ARTIFACT REFERENCE
4.3

MAGNET FORENSICS

CONTENTS

WINDOWS

Additional Sources

Android Backups

Description	Android Backups contains information about any backups of Android devices that are recovered from the computer. If an Android backup is recovered during a search, you can search the contents of the backup for additional artifacts.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the backup file.
File Path	The path where the backup was stored on the computer.
Encryption	The type of encryption (if any) that was used on the backup.
File System Created Date/Time - UTC (yyyy-mm-dd)	The creation date/time for the ab file from the file system.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date/time for the ab file from the file system.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date/time for the ab file from the file system.

Apple Disk Images

Description	Apple disk images are commonly stored as DMG or IMG files. These files are containers that may contain additional items of interest. This artifact identifies any Apple disk image found on the system.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the Apple disk image file.
File Path	The path where the Apple disk image was stored on the computer.

ATTRIBUTE	DESCRIPTION
File Type	The type of Apple disk image file (DMG or IMG).
File System Created Date/Time - UTC (yyyy-mm-dd)	The creation date/time for the file from the file system.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date/time for the file from the file system.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date/time for the file from the file system.

iOS Backups

Description	iOS Backups contains information about any backups of iOS devices that are recovered from the computer. If an iOS backup is recovered during a search, you can search the contents of the backup for additional artifacts.
Notes	

ATTRIBUTE	DESCRIPTION
Device Phone Name	The name of the iOS device from which the backup originated.
Device Phone Number	The phone number of the iOS device from which the backup originated.
IMEI	The IMEI of the iOS device from which the backup originated.
ICCID	The ICCID of the iOS device from which the backup originated.
Backup File Creation Date/Time	The Date/Time that the backup was created.
Product Name	The model of the iOS device from which the backup originated.
Product Version	The version of iOS of the device at the time of the backup creation.
Serial Number	The serial number of the iOS device from which the backup originated.

Virtual Machines

Description	Virtual Machine files that have been found on the object being searched.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the virtual machine.
Virtual Machine Software	The software that is associated with the virtual machine.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the virtual machine was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the virtual machine was last accessed.

ATTRIBUTE	DESCRIPTION
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the virtual machine was last modified

Chat

Adium Chat

Description	Adium is a multi-account chat application on Mac computers. It allows users to connect various accounts such as Google Talk, Facebook and generic Jabber accounts.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the message
Sender Nickname	The sender's nickname
Recipient	The message recipient
Message	The message content
Message Sent Date/Time UTC (yyyy-mm-dd)	The date and time the message was sent

AIM

Description	America OnLine Instant Messenger (AIM) is a desktop chat application that allows AOL account holders to chat with one another and transfer files.
Notes	

ATTRIBUTE	DESCRIPTION
Fragment	A HTML fragment of an AIM message
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

AIM Chat Messages

Description	America OnLine Instant Messenger (AIM) is a desktop chat application that allows AOL account holders to chat with one another and transfer files.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the AIM chat message.
Recipient	The recipient of the AIM chat message.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Message	The message body.

Chatroulette

Description	Chatroulette is a web-based video chat service that connects users with random users.
Notes	

ATTRIBUTE	DESCRIPTION
Type	The type of message
Content	The message content.
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Chatstep Messages

Description	Chatstep messages contains messages recovered from the Chatstep web portal.
Notes	If the Message attribute displays [Hidden Picture], this indicates that a picture was sent, but is in a hidden state (the user hasn't clicked the picture to view the content of the attachment. All data recovered for this artifact are from RAM, or RAM equivalent files.

ATTRIBUTE	DESCRIPTION
Sender	The message sender's username.
Direction	The direction of the message, if known.

ATTRIBUTE	DESCRIPTION
Message	The message body.
Message Sent Time - Local Time	The time when the message was sent or received in local time. There is no date information recovered.
Attachment Name	The name of the attachment.
MIME Type	The MIME type for the attachment.
Sender IP Address	The IP address of the sender.

Discord Messages

Description	Discord Messages contains information about messages and calls that are sent and received using Discord. Messages from some channels might be missing if they haven't been cached by the app. This artifact uses both parsing and carving techniques to recover messages.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The user name of the message sender.
Message	The message content.
Channel ID	The ID of the channel that the message was sent in. This attribute is always empty for android.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Last Edited Date/Time - UTC (yyyy-mm-dd)	If the message has been edited then this indicates the date and time when the last edit has occurred.
Attachment URL	If the message includes an attachment then this indicates the saved URL of the attachment. This attribute is always empty for android.
Attachment Name	If the message includes an attachment then this indicates the file name of the attachment. This attribute is always empty for android.
Embedded Content Title	If the message contains a link then this then this indicates the title that's displayed in the link preview.
Embedded Content Description	If the message contains a link then this indicates the description that's displayed in the link preview. This attribute is always empty for android.
Message Type	The type of the message, either a Message or a Call.
Call End Date/Time - UTC (yyyy-mm-dd)	If the message was a call, this indicates the date and time that the call ended.
Pinned	Indicates whether a message is pinned (True or False). This attribute is always empty for android.

Google Talk

Description	Google Talk is an instant messaging service that provides both text and voice communication.
Notes	

ATTRIBUTE	DESCRIPTION
Message ID	ID for the message
Sender	Email address of sender
Sender ID	ID of Sender
Recipient	Email address of recipient
Recipient ID	ID of Recipient
Message	Content of message
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

ICQ 10 Messages

Description	ICQ 10 Messages.
Notes	Currently, it's not possible to determine whether the timestamp associated with a message is the sent or received time. In addition, the recipient in a group conversation is the name of the group when the user first joined the group, and may not represent the current name of the group.

ATTRIBUTE	DESCRIPTION
Local User ID	The ICQ User ID of the local user.
Sender	The message sender's nickname.
Recipient	The message recipient's nickname. If the message is part of a group conversation, then it is the name of the group.
GroupChatID	The ID of the group chat, if the message is part of a group conversation.
Message Date/Time - UTC (yyyy-mm-dd)	The date/time of the message.
Message	The content of the message.
Direction	The direction of the message.
Type	The type of message.
Duration (Seconds)	The duration of a call, if the message type is a call.

ATTRIBUTE	DESCRIPTION
Media URL	A media URL link to any attachments sent.

ICQ Messages

Description	Messages that the user sent and received using the ICQ messaging application.
Notes	Status will only be retrieved for ICQ 6 and ICQ 7.

ATTRIBUTE	DESCRIPTION
Local User ID	The ID of the local user of the message.
Sender	The sender of the message.
Conversation Partner ID	The ID of the partner.
Sent Date/Time - UTC(yyyy-mm-dd)	The date and time the message was sent.
Received Date/Time - UTC(yyyy-mm-dd)	The date and time the message was received.
Message	The message's contents.
Direction	The direction of the message.
Type	The type of message
Status	The sent status of the message.
Group Chat ID	The ID of the group the message is associated with.

iMessage Chats

Description	iChat (now iMessage) is a chat application on Mac that allows users to communicate via text chat, video and audio. Users can also share files. iChat is standard on almost all Mac computers.
Notes	

ATTRIBUTE	DESCRIPTION
Recipient	The recipient of the message.
Sender	The sender of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Message	The message content.
Type	The type of message.
Status	The sent status of the message.

iMessage Messages

Description	iMessage (previously iChat) is a chat application for Apple products that allows users to communicate via text chat, video, and audio. Users can also share files. iMessage is standard on almost all Mac computers and iOS devices.
Notes	

ATTRIBUTE	DESCRIPTION
Recipient	The recipient of the message.
Sender	The sender of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Message	The message content.
Type	The type of message.
Status	The sent status of the message.

KakaoTalk Chat Rooms - Windows

Description	KakaoTalk Chat Rooms contains a list of all chat rooms that the KakaoTalk has open.
Notes	If the KakaoTalk data is acquired using a Files and Folders scan, some data might not be available.

ATTRIBUTE	DESCRIPTION
Chat ID	The ID of the chat room.
Room Name	The name of the room.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time the last message was sent to the room.
Last Message	The last message that was sent to the room.
Chat Type	The type of chat room.
Number of Participants	The number of users in the chat room.
Participant IDs	The user IDs of all participants in the chat room.
Link ID	The link ID of the chat room.
Room Status	The status messages for the room.
Room Status Author	The user ID of the last user to change the room status.
Status Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the status message was updated.

KakaoTalk Contacts - Windows

Description	KakaoTalk Contacts contains a list of all the users associated with the KakaoTalk account.
Notes	If the KakaoTalk data is acquired using a Files and Folders scan, some data might not be available.

ATTRIBUTE	DESCRIPTION
User ID	The user ID.
Account Type	The account type.
Screen Name	The user provided screen name.
Profile Image URL	A URL to the user's profile image.
Status Message	The status message of the contact.
Phone Number	The contacts phone number.
User Name	The known user name of the contact.
Nickname	The nickname provided to the contact by the current user.
Hidden	Whether or not the contact has been hidden.
Favorite	Whether or not the contact is a favorite.
Link ID	The link ID of the contact.

KakaoTalk Messages - Windows

Description	KakaoTalk Messages contains messages sent or received using the KakaoTalk account.
Notes	If the KakaoTalk data is acquired using a Files and Folders scan, some data might not be available.

ATTRIBUTE	DESCRIPTION
Sender ID	The ID of the sender.
Message ID	The message ID.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent
Message	The content of the message.
Message Type	The type of message.
Attachment	Any attachment information associated with the message.
Deleted	Whether or not the message has been deleted.

KakaoTalk Pictures

Description	KakaoTalk Pictures contains the decrypted pictures that have been shared using KakaoTalk. The formats that are supported are described in the Pictures artifacts.
Notes	If the KakaoTalk data is acquired using a Files and Folders scan, some data might not be available.

ATTRIBUTE	DESCRIPTION
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date/time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date/time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date/time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. "Complete" indicates that a full Exif extraction was performed. "Failed" indicates that the information may have been corrupted and could not be recovered. "Skipped" indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).

ATTRIBUTE	DESCRIPTION
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
Longitude	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the pciture was taken (extracted from Exif data).
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

KakaoTalk Shared Pictures - Windows

Description	KakaoTalk Shared Pictures contains pictures sent or received using the KakaoTalk account. The actual picture content is available if the user downloads the picture locally. If the user does not download the picture locally, the content remains encrypted. If it's possible to decrypt the picture, you can see the decrypted content in KakaoTalk Pictures.
Notes	If the KakaoTalk data is acquired using a Files and Folders scan, some data might not be available.

ATTRIBUTE	DESCRIPTION
Message ID	The ID of the message that included the picture.
Chat ID	The ID of the chat room where the picture was shared.

ATTRIBUTE	DESCRIPTION
Sender ID	The ID of the sender of the picture.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the picture was sent.
File Size (Bytes)	The size of the picture in bytes.
Thumbnail URL	A URL to a thumbnail of the picture.
Download Location	A filepath location to where the picture was saved.
Download Completed Date/Time - UTC (yyyy-mm-dd)	The date and time the picture was downloaded.
Deleted	Whether or not the picture has been deleted.
File Extension	The extension of the picture.
MIME Type	The MIME type of the picture.

Lync / OC Calls

Description	Lync/OC is a business grade communication application created by Microsoft.
Notes	

ATTRIBUTE	DESCRIPTION
Remote Participant Email	The email of the remote participant
Remote Participant Display Name	The display name of the remote participant
Call Started Date/Time - Local Time (yyyy-mm-dd)	The date and time when the call was started, local to the system
Call Ended Date/Time - Local Time (yyyy-mm-dd)	The date and time when the call ended, local to the system
Duration (Seconds)	The duration of the call in seconds

Lync / OC File Transfers

Description	Lync/OC is a business grade communication application created by Microsoft.
Notes	

ATTRIBUTE	DESCRIPTION
Type	The type of file
Sender	The sender of the file
Recipient	The recipient of the file
File	The file name or path

ATTRIBUTE	DESCRIPTION
File Size (Bytes)	The size of the file
Transfer Event Date/Time - Local Time (yyyy-mm-dd)	The start/end date time of the transfer

Lync / OC Fragments

Description	Lync/OC is a business grade communication application created by Microsoft.
Notes	

ATTRIBUTE	DESCRIPTION
HTML Fragment	The HTML Fragment of the conversation

Lync / OC Messages

Description	Lync/OC is a business grade communication application created by Microsoft.
Notes	

ATTRIBUTE	DESCRIPTION
Sender Email	The email address of the sender
Sender Display Name	The display name of the sender
Body	The body of the message
Sent Date/Time - Local Time (yyyy-mm-dd)	The date and time the message was sent, local to the system

Mail.ru

Description	Mail.ru is a webmail provider.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The name of the sender.
Reciever	The name of the receiver.
Message Sent Date/Time - Local Time	The date and time the message was sent.
Message	The actual message content.

Mail.ru Chat Non-Carved

Description	Mail.ru is a desktop communication application.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The name of the local user.
Name	The name of the group.
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Mail.ru Contacts

Description	Mail.ru is a desktop communication application.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The name of the local user.
First Name	The first name of the contact.
Last Name	The last name of the contact.
Email	The email address of the contact.
Last Seen Date/Time - UTC (yyyy-mm-dd)	The last time that user was seen online.
Location	The location of the contact.

Messenger Plus! Chat Logs

Description	MSN Plus! is a desktop chat application that allows Microsoft Acccount holders to chat with one another, transfer files and video conference. This is an older version of Windows Live Messenger.
Notes	

ATTRIBUTE	DESCRIPTION
Fragment	A HTML fragment of a MSN Plus! message

mIRC Chat Logs

Description	mIRC is a chat client that allows users to communicate and share files on the IRC network.
Notes	

ATTRIBUTE	DESCRIPTION
Fragment	A HTML fragment of a MIRC chat log
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

MSN Protocol Fragments

Description	MSN Messenger (also known as Windows Live Messenger) is a desktop chat application that allows Microsoft Account holders to chat with one another, transfer files, and video chat.
Notes	

ATTRIBUTE	DESCRIPTION
Fragment	A fragment of an MSN protocol message.

Omegle

Description	Omegle is a free online chat website that allows users to communicate with strangers without registering.
Notes	

ATTRIBUTE	DESCRIPTION
Type	The type of message.
Message	The content or body of the message
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

ooVoo Chat History

Description	ooVoo is a desktop communication application.
Notes	

ATTRIBUTE	DESCRIPTION
Message ID	The ooVoo unique message identifier.
Sender User ID	The ooVoo identifier of the sender.
Receiver User ID(s)	The ooVoo identifier of the recipient(s).
Chat Date/Time - UTC (yyyy-mm-dd)	The date and time of the conversation.
Message	The actual message content.
Message Type	The type of message that was sent. Some examples are: Chat, Video, Image, etc.
Message Direction	Indicates whether the message was sent (Outgoing) or received (Incoming).
Group Name	The name that is associated with a group conversation. If the chat is between two people the name will be empty.
Video URL	The address of the video that was sent in the message.
Image URL	The address of the image that was sent in the message.
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

ooVoo Contact List

Description	ooVoo is a desktop communication application.
Notes	

ATTRIBUTE	DESCRIPTION
Display Name	The contact display name
User ID	The contacts unique ooVoo identifier.
Status Message	A message set by the contact. This message can contain insight into how the person is feeling or share ideas/thoughts.
Birthday (yyyy-mm-dd)	The contact's birthday.
Phone Number	The contact's phone number.

ATTRIBUTE	DESCRIPTION
Password	The contact's password stored as plain text.
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

ooVoo Phone Book

Description	ooVoo is a desktop communication application.
Notes	

ATTRIBUTE	DESCRIPTION
Contact Name	The name of the contact.
Phone Number	The contacts phone number
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Pal Talk

Description	Paltalk is a desktop chat client.
Notes	

ATTRIBUTE	DESCRIPTION
Message	The message content.
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Pidgin Accelerators

Description	User-created keyboard shortcuts (accelerators) to perform actions within Pidgin more efficiently.
Notes	

ATTRIBUTE	DESCRIPTION
Window	An identifier for the application window.
Category	The category name of the acccelerator.
Data	A description of the accelerator that the user created.

Pidgin Accounts

Description	User information that's recovered from Pidgin accounts, such as the name, password, and display picture.
Notes	

ATTRIBUTE	DESCRIPTION
Protocol	The chat protocol of the account.
Name	The name of the account.
Password	The password of the account.
Alias	The user's nick name.
Status	The online status of the account.
Image	The user's display picture.

Pidgin Buddies

Description	Information about a user's Pidgin contacts.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the contact.
Friends With	The users that the contact is friends with.
Group	The group(s) that the contact belongs to, if any.
Protocol	The contact's chat protocol.
Alias	The contact's nick name.

ATTRIBUTE	DESCRIPTION
Last seen Date/Time - UTC (yyyy-mm-dd)	The last date and time the contact was seen online.
Image	The contact's display picture.
Source	The location of where the artifact was found.
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the source.
Evidence Number	The evidence number of the physical evidence that this artifact was recovered from.

Pidgin Chat

Description	Pidgin chat messages exchanged between users.
Notes	

ATTRIBUTE	DESCRIPTION
Participants	The chat participants.
Sender	The sender of the message.
Message Sent Date/Time - Local Time	The date and time the message was sent.
Message	The message content.
Image	The display picture of the sender, if found locally.
Downloaded Image	The display picture of the sender, downloaded from the Internet.
Source	The location of where the artifact was found.
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the source.
Evidence Number	The evidence number of the physical evidence that this artifact was recovered from.

Pidgin Custom Smileys

Description	Custom emoticons that a user creates and uses in Pidgin.
Notes	

ATTRIBUTE	DESCRIPTION
Shortcut	The keyboard shortcut to insert the custom smiley.

ATTRIBUTE	DESCRIPTION
Image	The custom smiley image.
Source	The location of where the artifact was found.
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the source.
Evidence Number	The evidence number of the physical evidence that this artifact was recovered from.

Pidgin OTR Fingerprints

Description	Pidgin is a multi-account desktop chat application. It allows users to connect various accounts such as Google Talk, Facebook, and generic Jabber accounts.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local user of the account.
Participant	The chat participant.
Protocol	The chat protocol of the account
Participant Fingerprint	The unique fingerprint belonging to the participant's account, used for Off-the-Record authentication.
Secure Conversation	Indicates whether the users used the Off-the-Record protocol to encrypt messages.

Pidgin OTR Users

Description	Pidgin is a multi-account desktop chat application. It allows users to connect various accounts such as Google Talk, Facebook, and generic Jabber accounts.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local user of the account.
Protocol	The chat protocol of the account.
Instance Tag	A 32-bit value that represents the user's login location. If the user logs in to the same account from multiple locations, each location will have a unique tag to identify it.
Private Key	The local user's private key, used for Off-the-Record encryption.

QQ Chat

Description	QQ is a chat application with a large user base. QQ is extremely popular in Asia and boasts about 800 million users. While the chat logs are encrypted, chat messages can still be recvoered if they are saved to RAM, pagefile.sys, hiberfil.sys and unallocated areas. Because the chat messages are retrieved from volatile locations, not all have a date/time associated with them.
Notes	

ATTRIBUTE	DESCRIPTION
Message	The message content

Second Life Chat

Description	Second Life is an online virtual world where users can create characters and interact with other users.
Notes	

ATTRIBUTE	DESCRIPTION
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent
From User	The sender of the message.
Chat Partner	The conversation partner
Message	The content of the message
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Skype Accounts

Description	Information about the Skype accounts that are recovered, such as user info and when the account was created.
Notes	

ATTRIBUTE	DESCRIPTION
Skype Name	Skype name of the account
Display Name	Display name of this account
Full Name	Full Name of this account
Birthday (yyyy-mm-dd)	Birthday of this account
Gender	Gender of this account
City	City where this account is located
State/Province	State/Province this account is located
Country	Country this account is located
Home Phone	Home phone of this contact
Office Phone	Office phone of this account
Mobile Phone	Mobile phone of this account
Email(s)	Email of this account
Homepage	Homepage of this contact
About Info	About info of this contact
Profile Created On Date/Time - UTC (yyyy-mm-dd)	The date when the profile was created
Profile Last Modified On Date/Time - UTC (yyyy-mm-dd)	The date when the profile was last modified
Mood Text	Text used to express mood
Last Online On Date/Time - UTC (yyyy-mm-dd)	Last time the account was online
Last used On Date/Time - UTC (yyyy-mm-dd)	Last time the account was used
Avatar Timestamp Date/Time - UTC (yyyy-mm-dd)	Avatar created time
Image	Image for this contact

Skype Activity

Description	Skype Activity contains interactions that occur between users on Skype. These interactions include messages, group interactions, calls, files sent/received, and SMS. Applies to Skype 8.1 and later.
Notes	

ATTRIBUTE	DESCRIPTION
Conversation ID	ID of this conversation.
Profile Name	The local user's profile name.
Sender	The username of the sender/initiator of the interaction.
Sender Email	The sender's email as given in the message (if available).
Recipient Name(s)	The recipients or targets of the interaction.

ATTRIBUTE	DESCRIPTION
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the interaction was initiated.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the interaction was last updated (for example, when a call ends).
Message Type	The type of the interaction.
Message	The content of the message or summary of the interaction.
Emotion Count	The number of reactions to the interaction (for example, likes, dislikes, emojis, and so on).
File Name	The name of any attached files associated with the interaction.
File Size (Bytes)	The size in bytes of any attached files.
File	The attachment file (if applicable).
Attachment Data Recovered	Whether the attached file was recovered from the local filesystem.
Thumbnail URL	A URL that directs to the thumbnail picture (if applicable).
Call Duration (Seconds)	The length of the call in seconds (if applicable).
Metadata	The content of the message, if it consisted of interpreted data (that is, XML or JSON data, rather than plain text).

Skype Calls

Description	Information about Skype calls that occur between users.
Notes	

ATTRIBUTE	DESCRIPTION
Local Username	The user logged into Skype at the time of the call.
Call Initiator	The user who started the call.
Initiator Display Name	The display name of the user. This might be different from the username.
Recipient(s)	The users who accepted a call from the call initiator and participated in the call for a period of time.
Call Participants	The users who accepted and participated in the call from the call initiator for some duration.
Started Date/Time - UTC (yyyy-mm-dd)	Start time of the call.
Duration	Total duration of the Skype call.
Metadata	Additional details about the call extracted in XML format. This includes the duration of time each participant was in the call.

Skype Chat Messages

Description	Skype messages sent from one user to another.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	Profile name of the caller
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent
Author	Author of the message
From Display Name	The display name of who sent the message
Message	The body of the message or a description of the action taken. For example, adding another participant to a group chat or sharing a file or picture.
Attachment Name	The name of the attachment that was sent. This attribute is populated when the Message Type is POSTED_FILE or POSTED_PICTURE. Otherwise, this attribute is empty.
Attachment Size (Bytes)	The size of the attached file, in bytes. This attribute is populated when the Message Type is POSTED_FILE or POSTED_PICTURE. Otherwise, this attribute is empty.
Metadata	Additional details about the action, extracted in its original XML format.
Message Status	The status of the message.
Message Type	Type of message
Chat ID	ID of this chat
Recipient	Recipient of the chat

Skype Chatsync Messages

Description	Skype messages sent from one user to another that are parsed from the chatsync directory.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local Skype user
Chat Initiator	The user that started the conversation
Chat Partner/Group Chat ID	The other user in the chat, or a group chat identifier
Message Type	Indicates the sent status of the message
Message	The content or body of the message
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent

Skype Chatsync Messages Carved

Description	Skype messages sent from one user to another that are carved from the chatsync directory.
Notes	

ATTRIBUTE	DESCRIPTION
Message Type	Indicates the sent status of the message
Message	The content or body of the message
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Skype Contacts

Description	Information about Skype contacts that are recovered, which may or may not be added contacts.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	Profile name of the user
Skype Name	Skype name of the contact
Display Name	Display name of this account
Is Blocked	Is this contact blocked?
Contact Added	Specifies whether the contact is an added contact or just cached into the database (1 if the contact was added, 0 otherwise). Contacts can be cached into the database for a variety of reasons (for example, as a 'suggested contact').
Full Name	Full Name of this account
Birthday (yyyy-mm-dd)	Birthday of this account
Gender	Gender of this account
City	City where this account is located
State/Province	State/Province this account is located
Country	Country this account is located
Home Phone	Home phone of this contact

ATTRIBUTE	DESCRIPTION
Office Phone	Office phone of this account
Mobile Phone	Mobile phone of this account
PSTN Number	PSTN number of this contact
Email(s)	Email of this account
Homepage	Homepage of this contact
About Info	About info of this contact
Profile Loaded Date/Time - UTC (yyyy-mm-dd)	Previously called "Profile Created On Date/Time", this attribute represents the date/time when a contact's profile is first created on the user's device. When the profile information is updated by the contact, the date in the database is also updated.
Mood Text	Text used to express mood
Last Online On Date/Time - UTC (yyyy-mm-dd)	Last time the account was online
Last used On Date/Time - UTC (yyyy-mm-dd)	Last time the account was used
Avatar Timestamp Date/Time - UTC (yyyy-mm-dd)	Avatar created time
Image	Image for this contact

Skype File Transfers

Description	Files that are transferred from one user to another using Skype.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	The name of the user.
Partner Handle	The user name of the file transfer partner.
Partner Display Name	The display name of the file transfer partner
File Name	The file name being transferred
Type	The type of file being transferred
File Path	The path to the local file
Transferred File	The file that was transferred
File Size (Bytes)	The size of the file being transferred
Bytes Transferred	The number of bytes that were transferred

ATTRIBUTE	DESCRIPTION
Transfer Start Date/Time - UTC (yyyy-mm-dd)	The date and time the file transfer was started
Transfer Finish Date/Time - UTC (yyyy-mm-dd)	The date and time the file transfer completed
Status	The status of the file (for example, transfer, transferring or cancelled)

Skype Group Chat

Description	Information about the Skype group chats that a user is a part of.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	The name of the user.
Chat ID	The group chat's unique identifier.
Participants	The participants of the chat.
Posters	The users that have posted to the chat.
Active Members	The currently active users of the group.
Chat name	The name of the chat.
Started Date/Time - UTC (yyyy-mm-dd)	The date and time the chat started.
Last Changed Date/Time - UTC (yyyy-mm-dd)	The date and time the chat was modified.
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Skype IP Addresses

Description	IP addresses that are associated with a Skype user account.
Notes	This artifact is no longer supported as of Skype 7.40.

ATTRIBUTE	DESCRIPTION
Username	Username of Skype accounts
IP Addresses	IP Addresses for the Skype user
Date/Time - UTC (yyyy-mm-dd)	Date and time
IP Address Type	Type of IP address Local or Public

Skype Media Cache

Description	Media content that gets sent from one Skype user to another.
Notes	

ATTRIBUTE	DESCRIPTION
Chat ID	The group chat's unique identifier.
Profile Name	The name of the user.
Author	The author of the media message.
Recipient(s)	The recipient(s) of the media message.
From Display Name	The display name of the sender.
Message Sent Date/Time	The Date/Time the media message was sent.
MIME Type	The MIME type of the media sent.
File Size (Bytes)	The size of the media file sent in bytes.
Is Thumbnail	Whether the particular media recovered is a thumbnail.
Media URL	The URL of the media as stored in the Skype cloud.
Thumbnail URL	The URL of the thumbnail as stored in the Skype cloud.
Media	The media that was recovered.
Thumbnail	The thumbnail if the media recovered was a video file.

Skype SMS

Description	SMS messages that a user sends or recieves using Skype.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	The name of the user.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Author	The author of the message

ATTRIBUTE	DESCRIPTION
Message	The message content.
Target Number(s)	The recipient phone numbers
Status	The status of the message.
Reply-to Number	A phone number the recipients can reply to

Skype Voicemails

Description	Voicemails that a user sends or recieves using Skype.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	The name of the user.
Partner Handle	The user name of the conversation partner
Partner Display Name	The display name of the conversation partner
Subject	Identifies the subject of the voicemail
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent
Duration	The length of the voicemail
Allowed Duration	The maximum length allowed for the voicemail
Size	The size of the recording
Path	The file path of the voicemail
Type	Identifies whether the voicemail was received or sent.
Status	The status of the voicemail, recording or played for example.

TorChat

Description	TorChat is a chat application that allows users to anonymously chat through the TOR (onion-routed) network. Chat logs are recovered when logging has been used or messages have been delayed on the TOR network.
Notes	

ATTRIBUTE	DESCRIPTION
Local Date/Time	The local date and time of the message
Sender	The sender of the message
Receiver	The receiver of the message
Message	The message content

Trillian

Description	Trillian is a multi-protocol chat client for Windows desktop.
Notes	

ATTRIBUTE	DESCRIPTION
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent
Type	The type of message.
From User	The sender of the message.
To User	The conversation partner
Message	The content of the message
Chat Network	The chat network the message was sent over. Trillian supports many chat networks.
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

WeChat Messages

Description	Stored messages for the WeChat app on Computer.
Notes	On OS X / Windows, the MD5 Hashed Partner Username, File, Call Duration, Latitude, Longitude, and Attachment Path attributes are always empty.

ATTRIBUTE	DESCRIPTION
Sender Username	The username or ID of the sender, as assigned by the application.
Sender Nickname	The display name of the sender, as defined by the user.
Recipient Username	The username of the person receiving the message.
Recipient Nickname	The nickname of the person receiving the message.
Group Chat Name	The name of the group chat, if the message is sent in a group chat.
Group Chat ID	The unique ID of the group chat, if the message is sent in a group chat.
Created Date/Time - UTC (yyyy-mm-dd)	The date/time that the message was created on the device.
Message	The content of the message.
Image	Image attachment associated with the message.

ATTRIBUTE	DESCRIPTION
File	Non-image attachment (such as audio, video) associated with the message.
Call Duration (Seconds)	Duration of voice and/or video call in seconds.
Type	The type of the message, such as text, audio, video etc.
Latitude	Latitude part of location data sent within the message.
Longitude	Longitude part of location data sent within the message.
Attachment Path	Absolute path to attachment(s) associated with the message if any were recovered.

WhatsApp Messages - Windows

Description	WhatsApp Messages contains information about the messages that are sent and received by the user. The data in this artifact is carved from RAM and/or unallocated space and can be created by the desktop application or the web.
Notes	

ATTRIBUTE	DESCRIPTION
Chat Type	The audience for the message/call. 'Individual' indicates one-on-one messages/calls and 'Group' indicates that the message/call involves more than one user.
Sender	The sender of the message. This value is a user ID for individual chats. If the message is recieved from a group, this value can be a group ID, or user ID of the sender. Messages sent by local user usually don't have a user ID.
Recipient	The message recipient. This fragment only used for group chats, using group ID value.
Message	The message text body.
ID	The unique message identifier.

Windows Live Messenger / MSN

Description	MSN Messenger (Windows Live Messenger) is a desktop chat application that allows Microsoft Acccount holders to chat with one another, transfer files and video conference.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The MSN Account of the sender.
Recipient	The MSN account of the recipient.

ATTRIBUTE	DESCRIPTION
Message Sent Date/Time - UTC (yyy-mm-dd)	The date and time the message was sent. This date time is stored as the local time of the system and cannot be timezone converted.
Message	The content of the chat message

Windows Live Messenger Chat - Mac

Description	MSN Messenger (Windows Live Messenger) is a desktop chat application that allows Microsoft Acccount holders to chat with one another, transfer files and video conference.
Notes	

ATTRIBUTE	DESCRIPTION
Message Sent Date/Time - Local Time (Date Format Unknown)	The date and time the message was sent. This date time is stored as the local time of the system and cannot be timezone converted.
Sender	The sender name.
Message	The content of the chat message.

Windows Viber Calls

Description	Windows Viber Calls contains details about calls sent or received using the Viber application.
Notes	

ATTRIBUTE	DESCRIPTION
Partner Phone Number	The number of the person or group the call was with.
Partner Name	The name of the person or group the call was with.
Partner Display Name	The display name of the person or group the call was with.
Date/Time - UTC (yyyy-mm-dd)	The date/time the call was sent/received.
Direction	The direction the call was made, can be 'Incoming' or 'Outgoing'.
Call Status	The status of the call, can be 'Answered', 'Unanswered', 'Missed' or 'Declined'.
Duration	The duration of the call.
Call Type	The type of the call, can be 'Audio', 'Video', and 'Viber Out'.

Windows Viber Chat Messages

Description	Viber Chat Messages contains details about chat messages sent or received using the Viber. This artifact applies to Viber 9.x and lower.
Notes	

ATTRIBUTE	DESCRIPTION
Partner Phone Number	The phone number of the person (or group) that the local user is chatting with.
Partner Name	The name of the person (or group) that the local user is chatting with.
Partner Display Name	The display name of the person (or group) that the local user is chatting with.
Subject	The subject of a message, currently only videos from a mobile device will have a subject.
Message Body	The body of the message.
Date/Time - UTC (yyyy-mm-dd)	The date/time the message was either sent or received.
Direction	The direction of the message, can be 'Incoming' or 'Outgoing'.
Read	Has the message been read by the user on the computer.
File Name	The name of the file attached to the message.
Attachment Path	The path to the attachment included with the message.
Attachment	The raw data for the attachment included with the message.
Latitude	The latitude of the user chatting with the local user.
Longitude	The longitude of the user chatting with the local user.

Windows Viber Contacts

Description	Contains details about a user's contacts in the Viber application.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the contact.
Display Name	The display name of the contact.
Avatar Path	The path to the user's avatar.
Avatar	The users avatar.
Number	The users telephone number.
Number Type	The type of the users number.

Windows Viber Group Members

Description	Viber Group Members contains details about group membership and group metadata for conversations made using Viber. It's important to note that group membership history is not recoverable, so it is hard to be certain of who may have received messages and attachments that were shared in a group chat.
Notes	

ATTRIBUTE	DESCRIPTION
Member Name	The name of the person that belongs to the group.
Member Phone Number	The phone number of the person that belongs to the group.
Admin	Specifies whether the person has Admin privileges for the group. Admins are usually the creators of the group, but they can also be added by another Admin.
Group Name	The name of the group the person belongs to. Group name is optional in the Viber application, so sometimes it can be blank.
Group Chat ID	The ID of the group. It can be used to sort or filter the member list to quickly see all members of any particular gorup. It can also be used to cross-reference with messages in the Windows Viber Messages artifact.
Group Type	The type of the group, can be 'Group', 'Community', or 'Public Account'.
Group Tagline	The tagline that is meant to describe the group. Only applies to groups of type 'Community' and 'Public Account'.
Group Origin	The country of origin of the group's creator. Only applies to groups of type 'Community' and 'Public Account'.

Windows Viber Messages

Description	Viber Messages contains details about messages sent or received using the Viber. This artifact applies to Viber 9.x and higher.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The phone number of the person (or group) that the local user is chatting with.
Sender Phone Number	The name of the person (or group) that the local user is chatting with.

ATTRIBUTE	DESCRIPTION
Recipient	The display name of the person (or group) that the local user is chatting with.
Recipient Phone Number	The subject of a message, currently only videos from a mobile device will have a subject.
Group Chat Name	The name of the group with which the message was shared.
Group Chat ID	The ID of the group. It can be used to cross-reference with members in the Windows Viber Group Members artifact.
Date/Time - UTC (yyyy-mm-dd)	The date/time the message was either sent or received.
Message Body	The body of the message.
Subject	The subject of the message. A subject usually appears in various media-type messages.
Type	The type of the interaction, can be 'Message', 'Picture', 'Video', 'Sticker', 'Attachment', 'Group Chat Membership', 'Set Group Name', 'Set Group Icon', or 'Set Background'.
Direction	The direction of the message, can be 'Incoming' or 'Outgoing'.
Read	Has the message been read by the user on the computer.
File Name	The name of the file exchanged.
Attachment Path	The path to the attachment on the local user's computer. Sometimes the File Name is present but the Attachment Path is empty, which might indicate that an incoming attachment was not downloaded by the local user.
Attachment	The raw data for the attachment included with the message.
Latitude	The latitude of the Sender.
Longitude	The longitude of the Sender.

World of Warcraft Chat

Description	World of Warcraft (WoW) is a massively multiplayer online role-playing game (MMORPG) created in 2004 by Blizzard Entertainment.Users can communicate via chat within the game.
Notes	

ATTRIBUTE	DESCRIPTION
Type	The type of message (private, public)
From Name	The name of the sender
To Name	The name of the recipient
Message	The message content.

ATTRIBUTE	DESCRIPTION
Channel	The channel the message was sent over
Local Player GUID	The local players GUID
Remote Player GUID	The remote players GUID
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Yahoo! Diagnostic Chats

Description	Yahoo! Messenger Chat is a desktop chat application that allows Yahoo! Account holders to chat with other Yahoo! users.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local Yahoo! Account user.
Sender	The sender of the chat message.
Recipient	The recipient of the chat message.
Chat Sent Date/Time - Local Time	The local date/time that the chat was sent.
Message	The chat message body.
Command	The command associated with the chat message.
Type	The type of the chat message.
Room Name	The name of the chat room.

Yahoo! Messenger (Mac)

Description	Yahoo! Messenger Chat is a desktop chat application that allows Yahoo! Account holders to chat with other Yahoo! users.
Notes	

ATTRIBUTE	DESCRIPTION
Sender User Name	The Yahoo! Account of the sender.
Sender Display Name	The Display Name of the Yahoo! Account of the sender.
Recipient User Name	The Yahoo! Account of the receiver.

ATTRIBUTE	DESCRIPTION
Recipient Display Name	The Display Name of the Yahoo! Account of the receiver.
Message Sent Date/Time - UTC (yyy-mm-dd)	The date and time the message was sent.
Message	The content of the chat message.

Yahoo! Messenger - Group Chat

Description	Yahoo! Messenger Chat is a desktop chat application that allows Yahoo! Account holders to chat with other Yahoo! users.
Notes	

ATTRIBUTE	DESCRIPTION
Username	The Yahoo! Account of the sender.
Message Sent Date/Time - Local Time	The date and time the message was sent. This date time is stored as the local time of the system and cannot be timezone converted.
Message	The content of the chat message.

Yahoo! Messenger - Non-encrypted Chat

Description	Yahoo! Messenger Chat is a desktop application that allows Yahoo! Account holders to chat with other Yahoo! users.
Notes	

ATTRIBUTE	DESCRIPTION
User name	The Yahoo! Account of the sender
Message Sent Date/Time - Local Time	The date and time the message was sent. This date time is stored as the local time of the system and cannot be timezone converted.
Sent Message Text	The content of the chat message.

Yahoo! Messenger Chat

Description	Yahoo! Messenger Chat is a desktop chat application that allows Yahoo! Account holders to chat with other Yahoo! users.
Notes	In Yahoo Messenger 11 and later, the user can save messages to the cloud or not at all. In either case, this prevents the recovery of actual message content for those versions of the app.

ATTRIBUTE	DESCRIPTION
Local user	The user account of the current system that is being searched.
Sender	The Yahoo! Account of the sender.
Recipient	The yahoo account of the receiver.
Message Sent Date/Time - UTC (yyy-mm-dd)	The date and time the message was sent.
Message	The content of the chat message.

Yahoo! Messenger Diagnostic Logs

Description	Yahoo! Messenger Chat is a desktop chat application that allows Yahoo! Account holders to chat with other Yahoo! users.
Notes	

ATTRIBUTE	DESCRIPTION
Image	A image that was pulled from the diagnostic log.
Log Created Date/Time - Local Time	The date and time the log entry was logged.
Local User	The local Yahoo! Account user.
Command	A number that represents a Yahoo! Diagnostic command.
Type	The type of the command.
Data	The data associated with the command.

Yahoo! Webmail Chat

Description	Yahoo! Webmail Chat is a browser chat application that allows Yahoo! Account holders to chat with other Yahoo! users.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the chat message.
Recipient	The recipient of the chat message.
Message	The message being sent.
Status	The status of the webmail message.
Version	The version of the webmail chat.
Vendor ID	The ID of the vendor.
Session ID	The ID of the chat session.

Your Phone Contacts

Description	Your Phone Contacts contains information about contacts synced from a mobile device to a computer using Your Phone. The Your Phone app can sync data from Android and iOS devices to computers running Windows 10.
Notes	

ATTRIBUTE	DESCRIPTION
Display Name	The contact's display name.
Nickname	The contact's nickname.
Phone Number	The contact's phone number.
Type	The type of phone number associated with the contact (for example, Home, Mobile, or Business).
Last Time Contacted Date/Time - UTC (yyyy-mm-dd)	The last time this contact either sent a message to or received a message from the synced device/local user since the Your Phone app was installed.
Number of Times Contacted	The number of times the synced device/local user either sent a message to or received a message from the contact since the Your Phone app was installed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time this contact's details were modified.

Your Phone Devices

Description	Your Phone Devices contains information about the devices that are synced to the user's computer by using the Your Phone application.
Notes	

ATTRIBUTE	DESCRIPTION
Application Version	The version of Your Phone running on the computer.
Last Run Date/Time - UTC (yyyy-mm-dd)	The date and time the application was last run on the computer.
Device Application Version	The version of the Your Phone companion app running on the device.
Device ID	A GUID identifier generated to uniquely identify devices within the Your Phone app.
Device Name	The name provided by the device and displayed in the user interface when referring to it.
Device Platform	The device's platform (Android or iOS).

ATTRIBUTE	DESCRIPTION
Device Messages Synced Date	The date and time the device last synchronized its messages data with Your Phone.
Computer Messages Synced Date	The date and time the computer last synchronized its messages data with Your Phone.
Device Contacts Synced Date	The date and time the device last synchronized its contacts data with Your Phone.
Computer Contacts Synced Date	The date and time the computer last synchronized its contacts data with Your Phone.
Device Photos Synced Date	The date and time the device last synchronized its picture data with Your Phone.
Computer Photos Synced Date	The date and time the computer last synchronized its picture data with Your Phone.

Your Phone Pictures

Description	Your Phone Pictures contains information about pictures synced from a mobile device to a computer using Your Phone. The Your Phone app syncs the 25 most recently taken photos from Android and iOS devices to computers running Windows 10.
Notes	

ATTRIBUTE	DESCRIPTION
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Device ID	A GUID identifier generated to uniquely identify devices synced using the Your Phone app.
Device Name	The name of the device (as provided by the device) which is displayed in the user interface for Your Phone.
Created Date/Time - UTC (yyyy-mm-dd)	The created date/time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date/time of the picture in the file system.

ATTRIBUTE	DESCRIPTION
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date/time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. "Complete" indicates that a full Exif extraction was performed. "Partial" indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. "Failed" indicates that the information may have been corrupted and could not be recovered. "Skipped" indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
GPS Longitude	The GPS longitude coordinates of where the picture was taken (extracted from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).

ATTRIBUTE	DESCRIPTION
GPS Latitude	The GPS Latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS Latitude (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the pciture was taken (extracted from Exif data).
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Potential Original Media	Indicating if the media is likely the original source.
Category	An integer that indicates the Project VIC category for the picture.

Your Phone SMS/MMS

Description	Your Phone SMS/MMS contains information about messages synced from a mobile device to a computer using Your Phone. The Your Phone app can sync data from Android and iOS devices to computers running Windows 10.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The phone number that sent the message.
Recipient(s)	The phone number(s) the message was sent to.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Message	The message content.
Message Direction	Indicates whether the message was sent or received by the synced device/local user.
Message Type	Indicates whether the message is SMS or MMS.
Message Status	Indicates whether the message has been read.
Attachment Name	The name of the attached file, if applicable (MMS only).

Zoom Chat Messages

Description	Contains details about Zoom chat messages sent outside of a meeting.
Notes	

ATTRIBUTE	DESCRIPTION
Sender Name	The name of the person who sent the message.
Sender ID	The ID of the person who sent the message.
Buddy ID	The ID of the person or group that the message was sent to.
Recipient Name	The name of the person who received the message.
Recipient ID	The ID of the person who received the message.
Group Chat ID	The ID of the group this message was sent in.
Message ID	The GUID of the message.
Message	The body of the message.
Message Date/Time - UTC (yyyy-mm-dd)	A timestamp that indicates when the message is sent or received, depending on whether the local user is the sender or receiver.
Sender	Whether the message was sent by the local user, or a remote user. Can be 'Local User' or 'Remote User'.
Read	Specifies whether the message has been read ('Yes' or 'No').
Message Type	The type of message that was sent. Can be 'Message', 'Picture', 'File', or 'Notification'.
Attachment Name	The name of the attachment that was sent.
Attachment Local File Path	The local path where the attachment was saved. This is empty if the attachment was not saved.
Attachment	The contents of the attachment if it can be recovered.

Zoom Meeting Messages

Description	Contains details about Zoom chat messages sent during a meeting.
Notes	

ATTRIBUTE	DESCRIPTION
Message ID	The GUID of the message.
Sender Name	The name of the person who sent the message.
Sender ID	The ID of the person who sent the message.

ATTRIBUTE	DESCRIPTION
Receiver Name	The name of the person who received the message. If blank, the message was sent to everyone in the meeting.
Receiver ID	The ID of the person who received the message. If zero, the message was sent to everyone in the meeting.
Message	The body of the message.
Message Date/Time - UTC (yyyy-mm-dd)	A timestamp that indicates when the message is sent or received, depending on whether the local user is the sender or receiver.
Sender	Whether the message was sent by the local user, or a remote user. Can be 'Local User' or 'Remote User'.
Read	Specifies whether the message has been read ('Yes' or 'No').
Message Type	The type of message that was sent.
Conference ID	The ID for the meeting the message was sent in.

Zoom User Accounts

Description	Contains details about the local user's zoom account.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The unique identifier for the user.
User Name	The account's user name.
Email	The email address associated with the account.
First Name	The user's first name.
Last Name	The user's last name.
Phone Number	The user's phone number.
Profile Image URL	The URL to the user's profile picture.
Downloaded Profile Image	The data for the profile picture.

Cloud

Carbonite Log File

Description	Carbonite is a cloud based automated backup program that is used for backing up a user's files and folders to the cloud. This search will return which files/folders have been or are pending to be backed up to the Carbonite cloud.

Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file that was backed up.
File Backup Date/Time - UTC (yyyy-mm-dd)	The date and time a file was backed up to the Carbonite service
File Size	The size of the backup file
Type	The type of the file that was backed up

Dropbox

Description	Dropbox contains information about files that users uploaded and synced to Dropbox.
Notes	

ATTRIBUTE	DESCRIPTION
Local File Name	The name of the file on the local machine
File Path	The path to the local file.
Updated File Name	The filename when updated.
Local Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time on the local machine.
Updated Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the updated file.
Local Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the local file.
Local File Size (bytes)	The size of the local file.
Updated File Size (bytes)	The size of the updated file
Local File Version Id	The file version id of the local file. Used to determine if there are any updates that need syncing.
Updated File Version Id	The file version id of the remote file.

Dropbox Configuration Data

Description	Dropbox Configuration Data contains information about users and the file that are uploaded and synced to Dropbox.
Notes	

ATTRIBUTE	DESCRIPTION
Dropbox User ID	The dropbox user id
Dropbox Email	The email addressed used with the dropbox service
Dropbox Folder Path	The folder path to the local dropbox folder.
Recently Changed Files	A list of recently changed files.

Flickr

Description	This search will recover artifacts left behind when using Flickr to upload files via the web. Data recovered can include file names, dates/times, user IDs, file sizes, URLs to files, descriptions, and more.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the media
Owner ID	The unique identifier of the Flickr media owner
Owner Name	The name of the media owner
URL	The URL to the picture on Flickr
Media	The type of media uploaded
Post Date/Time - UTC (yyyy-mm-dd)	The date and time the media was posted
Taken Date/Time - Local Time (yyyy-mm-dd)	The date and time the media was created/taken
Description	A description of the media uploaded

Google Docs

Description	Google Docs is a word processing suite available to all Google account holders.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file that was backed up.
Owner Email	The email address of the author of the file.
Owner Name	The name of the author of the file.
Last Edited Date/Time - UTC (yyyy-mm-dd)	The last date and time the file was edited.
Last Modified By Local User Date/Time - UTC (yyyy-mm-dd)	The date and time the document was edited locally.
File Size	The size of the file.

ATTRIBUTE	DESCRIPTION
Last Collaborator Name	The name of the last collaborator of the file.
Last Collaborator Email	The email address of the last collaborator of the file.

Google Drive

Description	Google Drive is a file hosting service that allows users to upload and sync files to a cloud service.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file that was backed up.
Author Name	The name of the author of the file.
Author Email	The email address of the author of the file.
File Size (Bytes)	The file size.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time the file was modified.
Last Modified Name	The last user to modified the file.
Last Modified Email	The last modifying user's email address.
Last Viewed Date/Time - UTC (yyyy-mm-dd)	The last date and time the file was viewed.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created.

OneDrive

Description	These are artifacts left behind using OneDrive to upload and view files via the web or through the OneDrive desktop application. Data recovered can include file names, dates/times, user IDs, file sizes, sharing settings, and more.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file that was backed up
File Size (Bytes)	The file size in bytes
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time the file was modified
Owner Name	The name of the owner of the file
Account Type	The type of the account (Personal or Business)
Account ID	The unique identifer of the owner of the account

ATTRIBUTE	DESCRIPTION
Owner ID	The unique identifer of the owner of the file
File Path	The path to the file that was backed up
URL	The URL to access the uploaded file. Usually this is a private URL
Last Modified Name	The last user to modify the file
Last Modified ID	The last modifying user's OneDrive identifier

SharePoint Discussions

Description	This table captures information related to discussions held on SharePoint
Notes	

ATTRIBUTE	DESCRIPTION
Subject	The subject of the discussion
Discussion Link	A link to the discussion
Fragment	A fragment of the discussion
Modified Date/Time - Local Time	The date and time when the content was last modified.
Created By	The user that created the content
Creator Link	A link to the user that created the content
Reply Count	The number of replies in the discussion

SharePoint Recycle Bin

Description	This table captures information about content in a SharePoint recycle bin.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the file in the recycle bin
Type	The type of the file in the recycle bin
Original Location	The file's original location
Creator Name	The user who created the file
Creator Email Address	The email address of the user who created the file
Deleted Date/Time - Local Time	The date and time that the file was deleted
Size	The size of the file

SharePoint Shared Documents

Description	This table captures information related to shared documents stored on SharePoint.
Notes	

ATTRIBUTE	DESCRIPTION
Content Type	The type of the content
Content Name	The name of the content
Content Link	A link to the content
Modified Date/Time - Local Time	The date and time when the content was last modified.
Modified By	The user that modified the content
Modified By Link	A link to the user that modified the content

Computer

Microsoft Teams Actiivty

Description	Microsoft Teams Activity contains interactions that occur between users on Teams. These interactions include messages, memers added/removed from meetings, and meeting start/end events.
Notes	

ATTRIBUTE	DESCRIPTION
Conversation ID	The unique identifier of the conversation.
Date/Time - UTC (yyyy-mm-dd)	The date and time the interaction was initiated.
Sender ID	The unique identifier of the sender.
Sender Display Name	The display name of the sender
Message Type	The type of the interaction.
Content	The content of the message or summary of the interaction.
Metadata	The json metadata from the database defining the interaction.

Microsoft Teams Messages

Description	Microsoft Teams Messages contains information about messages sent and received between Teams members, and which are recovered from the cloud.

Notes	

ATTRIBUTE	DESCRIPTION
Conversation ID	The unique identifier of the conversation.
Message ID	The unique identifier of the current message.
Sender ID	The unique identifier of the sender.
Sender Name	The name of the sender
Send Timestamp Date/Time - UTC (yyyy-mm-dd)	The UTC date time when the message was sent.
Content Type	The type of content in the message.
Message Text	The message text extracted from the HTML body.
HTML Body	The HTML body of the message.
Parent ID	The ID of the parent conversation.
_LocalUserAccount	The user name of the target user.
Attachment URL	The url of the attachment.
Attachments	The attachments.

Documents

Calc Documents

Description	Calc Documents are spreadsheets similar to Microsoft Excel spreadsheets, but created using OpenOffice Calc.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
File Name	The name of the document.
Created Date/Time - Local Time (yyyy-mm-dd)	The local date and time the file was created. This data is recovered from the <meta:creation-date> tag found in meta.xml.
Modified Date/Time - Local Time (yyyy-mm-dd)	The local date and time for when the file was modified. This data is recovered from the <dc:date> tag found in meta.xml.
Modified Date/Time - UTC (yyyy-mm-dd)	The UTC date and time for when the file was modified. This data is recovered from the local zip file header for meta.xml.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created on the filesystem.

ATTRIBUTE	DESCRIPTION
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified on the filesystem.
Recovered Size (Bytes)	The recovered size of the document in bytes.
Password Required	Indicates if the document is password protected.
Title	The title meta-data as set by the creator. This data is recovered from the <dc:-title> tag found in meta.xml. Note this can be different from the File Name.
Authors	The authors of the document. This data is recovered from the <meta:initial-creator> tag found in meta.xml.
Subject	The subject of the document as set by the creator. This data is recovered from the <dc:subject> tag found in meta.xml.
Keywords	The keywords meta-data in the document. This data is recovered from the <meta:keyword> tag found in meta.xml.
Comments	The comments meta-data. This data is recovered from the <dc:description> tag found in meta.xml.
Editing Cycle	The number of times the document has been edited. This data is recovered from the <meta:editing-cycles> tag found in meta.xml.
File	The actual file stored as an attachment.

CSV Documents

Description	CSV documents (.csv) that are located on the system.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
File Name	The name of the CSV document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was last modified.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was created.
File Content	The content of the CSV document.
Size (Bytes)	The size of the CSV document in bytes.
SHA1 Hash	The SHA1 hash of the contents of the document.
MD5 Hash	he MD5 hash of the contents of the document.

Excel Documents

Description	Microsoft Excel is a spreadsheet processor developed by Microsoft.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified on the filesystem.
Size (Bytes)	The size of the document in bytes.
Saved Size (Bytes)	The size of the document (in bytes) that was recovered. Extremely large documents may not be fully recovered.
File	The actual file.
Title	The title meta-data.
Subject	The subject meta-data.
Authors	The authors of the document.
Keywords	The keywords meta-data in the document.
Comments	The comments meta-data.
Last Author	The last author to edit the document.
Last printed Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last printed, extracted from meta-data within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last modified, extracted from meta-data within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the document was created, extracted from meta-data within the document.
Company	The company meta-data.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

Hangul Word Processor

Description	Specifies information about files created using Hangul Word Processor.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	Name of the found file.
Password Required	Whether the file requires a password to be opened.
Application Version	Version of the software used to create the file.
Preview Text	Preview of the file content that contains the first 1024 symbols.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was modified on the filesytem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the file was accessed on the filesytem.
File System Last Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created on the filesytem.
Title	Title field of the document.
Subject	Subject field of the document.
Author	Author field of the document.
Date String	Date field of the document.
Keyword	Keyword field of the document.
Additional Information	Any additional information that the author provided for the document. Appears as 'Other' field in the software.
Last Saved By	Username of the last user that saved the file.
Document Created Date/Time - Local Time (yyyy-mm-dd)	The date and time the file was originally created.
Preview Image	Preview image of the title page of the file.

Impress Documents

Description	Impress Documents are slide presentations similar to Microsoft PowerPoint presentations, but created using OpenOffice Impress.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
File Name	The name of the document.
Created Date/Time - Local Time (yyyy-mm-dd)	The local date and time the file was created. This data is recovered from the <meta:creation-date> tag found in meta.xml.
Modified Date/Time - Local Time (yyyy-mm-dd)	The local date and time for when the file was modified. This data is recovered from the <dc:date> tag found in meta.xml.
Modified Date/Time - UTC (yyyy-mm-dd)	The UTC date and time for when the file was modified. This data is recovered from the local zip file header for meta.xml.

ATTRIBUTE	DESCRIPTION
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified on the filesystem.
Recovered Size (Bytes)	The recovered size of the document in bytes.
Password Required	Indicates if the document is password protected.
Title	The title meta-data as set by the creator. This data is recovered from the <dc:title> tag found in meta.xml. Note this can be different from the File Name.
Authors	The authors of the document. This data is recovered from the <meta:initial-creator> tag found in meta.xml.
Subject	The subject of the document as set by the creator. This data is recovered from the <dc:subject> tag found in meta.xml.
Keywords	The keywords meta-data in the document. This data is recovered from the <meta:keyword> tag found in meta.xml.
Comments	The comments meta-data. This data is recovered from the <dc:description> tag found in meta.xml.
Editing Cycle	The number of times the document has been edited. This data is recovered from the <meta:editing-cycles> tag found in meta.xml.
File	The actual file stored as an attachment.

PDF Documents

Description	Portable Document Format (PDF) is a file format used to present documents in a manner independent of application software, hardware, and operating systems. This table captures documents in this file format, extracted from the filesystem and carved from unallocated space.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last accessed on the filesystem.

ATTRIBUTE	DESCRIPTION
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified on the filesystem.
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
Title	The title of the file.
Subject	The subject of the file.
Authors	The authors of the file.
Keywords	The keywords in the metadata of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the document was created, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last modified, extracted from metadata within the document.
File	The PDF file.
MD5 Hash	An MD5 hash of the PDF content.
SHA1 Hash	A SHA1 hash of the PDF content.

PowerPoint Documents

Description	Micrsoft PowerPoint is a presentation creator developed by Microsoft. This table captures documents created with PowerPoint, extracted from the filesystem and carved from unallocated space.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified on the filesystem.
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
File	The actual file.
Title	The title of the file.

ATTRIBUTE	DESCRIPTION
Subject	The subject of the file.
Authors	The authors of the file.
Keywords	The keywords in the metadata of the file.
Comments	The comments in the metadata of the file.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last modified, extracted from metadata within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the document was created, extracted from metadata within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

RTF Documents

Description	The information for each RTF document that was recovered from the search.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the RTF document.
File Size (Bytes)	The size of the RTF document in bytes.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the RTF document was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the RTF document was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the RTF document was last modified.
File Content	The contents of the RTF document.

Text Documents

Description	Text documents (.txt) that are located on the system.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the text document.

ATTRIBUTE	DESCRIPTION
Size (Bytes)	The size of the text document in bytes.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The Date/Time that the text document was last modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The Date/Time that the text document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The Date/Time that the text document was created.

Word Documents

Description	Microsoft Word is a word processor developed by Microsoft.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified on the filesystem.
Size (bytes)	The size of the document.
Saved Size (bytes)	The size of the document that was recovered. Extremely large documents may not be fully recovered.
File	The actual file.
Title	The title meta-data.
Subject	The subject meta-data.
Authors	The authors of the document.
Keywords	The keywords meta-data in the document.
Comments	The comments meta-data.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyy-mm-dd)	The date and time the document was last printed extracted from meta-data within the document.
Last Modified Date/Time - UTC (yyy-mm-dd)	The date and time the document was last modified, extracted from meta-data within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the document was created, extracted from meta-data within the document.
Company	The company meta-data.
MD5 Hash	The MD5 hash of the contents of the document.

ATTRIBUTE	DESCRIPTION
SHA1 Hash	The SHA1 hash of the contents of the document.
Source	The location of where the artifact was found.
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Writer Documents

Description	Writer Documents are documents similar to Microsoft Word documents, but created using OpenOffice Writer.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
File Name	The name of the document.
Created Date/Time - Local Time (yyyy-mm-dd)	The local date and time the file was created. This data is recovered from the <meta:creation-date> tag found in meta.xml.
Modified Date/Time - Local Time (yyyy-mm-dd)	The local date and time for when the file was modified. This data is recovered from the <dc:date> tag found in meta.xml.
Modified Date/Time - UTC (yyyy-mm-dd)	The UTC date and time for when the file was modified. This data is recovered from the local zip file header for meta.xml.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified on the filesystem.
Recovered Size (Bytes)	The recovered size of the document in bytes.
Password Required	Indicates if the document is password protected.
Title	The title meta-data as set by the creator. This data is recovered from the <dc:title> tag found in meta.xml. Note this can be different from the File Name.
Authors	The authors of the document. This data is recovered from the <meta:initial-creator> tag found in meta.xml.
Subject	The subject of the document as set by the creator. This data is recovered from the <dc:subject> tag found in meta.xml.

ATTRIBUTE	DESCRIPTION
Keywords	The keywords meta-data in the document. This data is recovered from the <meta:keyword> tag found in meta.xml.
Comments	The comments meta-data. This data is recovered from the <dc:description> tag found in meta.xml.
Editing Cycle	The number of times the document has been edited. This data is recovered from the <meta:editing-cycles> tag found in meta.xml.
File	The actual file stored as an attachment.

E-mail

Calendar Events (ICS)

Description	Calendar Events (ICS) contains information about events and appointments that are recovered from calendar .ics files. These files are used by many different email applications, including Outlook, Google Calendar, and Apple Calendar.
Notes	

ATTRIBUTE	DESCRIPTION
ID	A unique ID for the calendar entry.
Type	The type of event (for example, Event, TODO, Journal).
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the event was created.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the event starts.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the event ends.
Summary	A short summary of the event.
Description	Provides a more complete description of the event.
Latitude	The latitude coordinates of the event's venue.
Longitude	The longitude coordinates of the event's venue.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time in which the event was last modified.
Location Name	The name of the venue in which the event is held.
Organizer	The organizer of the calendar event.

ATTRIBUTE	DESCRIPTION
Status	The current pending status of the event (for example, NEEDS-ACTION, ACCEPTED, DECLINED, TENTATIVEB, DELEGATED, COMPLETED, IN-PROGRESS).
URL	The URL that is associated with the event.
Recurrence	Indicates whether the event is recurring.
Attendees	A list of attendees for the event.
Categories	The tags that are associated with the event.
Comment	A comment the organizer writes for to the user.
Contact Label	A reference of contacts associated with the event.
Resources	A list of resources and equipment required for the event.
Timezone	The timezone in which the event is held.

EML(X) Files

Description	Contains the emails in .eml and .emlx formats, that have been found on the device.
Notes	

ATTRIBUTE	DESCRIPTION
To	The recipients of the email.
From	The sender of the email.
Date/Time	The date and time the email was sent/received.
Subject	The subject of the email.
Body	The body of the email.
Cc	The recipients that receive the email by CC.
Bcc	The recipients that receive the email by BCC.
Headers	The raw email headers.
Importance	The email importance setting.
Last Read Date/Time - UTC (yyyy-mm-dd)	The date and time the email was last read, if the data is available.
Attachment Name(s)	A list of attachments on the email.

Gmail Email Fragments

Description	Contains the Gmail email fragments that were recovered from a Windows or OS X computer.
Notes	

ATTRIBUTE	DESCRIPTION
HTML Fragment	The HTML fragment of the email

Gmail Webmail

Description	Gmail is a webmail website that allows users to send and receive emails.
Notes	

ATTRIBUTE	DESCRIPTION
Email(s)	The email addresses involved with the email. If the email status is received it stores the email address of the sender otherwise it stores the emails that the message was sent to.
Subject	The subject of the email.
Snippet	A snippet of the message. It displays the first words as they were being displayed in the Gmail Inbox page
Sent Date/Time - Local Time	The local date and time of when the email was sent. This value is saved in the database as a string, so attempts to sort or filter the column may not behave as expected. Instead of sorting by date, the column sorts alphabetically.
Last Activity Date/Time	The date and time that the latest activity occurred. This value could represent the time that the email was sent or when it was received.
Status	The status of the email. Values can be 'sent' or 'received' for emails sent since 2018. Before 2018, values are 'read' or 'unread'.
Attachments	Contains information about attachments using the following format: file name (file type - file size).
Confidential	Indicates whether the email was sent in confidential mode.
Duration	For emails that are confidential, this attribute indicates how long that email is valid for (in days). This information is only recovered if all information about the confidential email is available.

Hotmail Webmail

Description	Hotmail is a web-based email client that allows users to send and receive emails. Hotmail was replaced by Outlook.com in 2012.
Notes	

ATTRIBUTE	DESCRIPTION
Type	The type of fragment found. Can be one of Contacts, Message, Folder view, Inbox Message, Edit Message, Plaintext Message Fragment, or Welcome Page

ATTRIBUTE	DESCRIPTION
HTML Fragment	The HTML fragment that was found

Hushmail Fragments

Description	Contains fragments of messages sent and received using Hushmail. Recovered data can include the sender, receiver, and message fragments.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the email.
Receiver	The receiver of the email.
Fragment	An HTML fragment of the email.

Hushmail Inbox

Description	Contains messages sent and received using Hushmail Webmail. Recovered data can include the sender, receiver, subject, and timestamps.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the email.
Receiver	The receiver of the email.
Message Received Date/Time - UTC (yyyy-mm-dd)	The UTC date and time the email was received.
Message Received Date/Time - Local Time	The local date and time the email was received.
Subject	The subject of the email.

Mailinator Inbox Access

Description	Instances when a user accesess their Mailinator inbox. Mailinator is webmail service that allows users to send and receive emails anonymously.
Notes	

ATTRIBUTE	DESCRIPTION
Inbox	The inbox that was accessed
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the inbox was accessed

Mailinator Snippets

Description	Fragments of email messages that are sent using Mailinator. Mailinator is webmail service that allows users to send and receive emails anonymously.
Notes	

ATTRIBUTE	DESCRIPTION
Sender Name	The name of the sender
Sender Address	The email address of the sender
Sender Mailserver IP	The IP of the sender's mail server
Recipient Address	The email address of the recipient
Subject	The subject of the email
Boddy Snippet	A snippet of the email body
Received Date/Time - UTC (yyyy-mm-dd)	The date and time the email was received

MBOX Emails

Description	MBOX is the default format used in Linux mail clients such as Thunderbird.
Notes	

ATTRIBUTE	DESCRIPTION
Folder Name	The folder where the email is stored
Sender	The sender of the email
To	The recipients of the email
CC	The recipients of the email that were CC'd
BCC	The recipients of the email that were BCC'd
Subject	The subject of the email
Body	The body of the email
Date/Time	The date and time the email was sent/received
Headers	The raw email headers
Importance	The email importance setting
Attachments	A list of attachments on the email

Offline Gmail webmail

Description	Gmail is a webmail website that allows users to send and receive emails.
Notes	

ATTRIBUTE	DESCRIPTION
From Address	The sender of the email
To Address(es)	The recipients of the email
cc Address(es)	The recipients of the email that were CC'd
bcc Address(es)	The recipients of the email that were BCC'd
Subject	The subject of the email
Date/Time - UTC (yyyy-mm-dd)	The date and time the email was sent/received
Status	The sent status of the email.
Email Body	The body of the email

Outlook Appointments

Description	Microsoft Outlook is a personal information manager and email client. This table captures information related to appointments scheduled in Outlook.
Notes	

ATTRIBUTE	DESCRIPTION
Sender Name	The person who requested the appointment
Sender Exchange Account	The sender's Exchange account name
Recipients	The recipients of the appointment invitation
Subject	The subject of the appointment
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the appointment starts
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the appointment ends
Body	The body of the appointment description
Recipients CC	The CC'd recipients of the appointment invitation
Recipients BCC	The BCC'd recipients of the appointment invitation
Companies	The companies involved in the appointment
Attachments	The attachments for the appointment
Location	The location of the appointment
Is All-Day Event	Indicates if the appointment is an all-day event
Is Recurring	Indicates if the appointment is recurring

ATTRIBUTE	DESCRIPTION
Recurrence Pattern Description	Describes the recurrence pattern of the appointment, if applicable
Sensitivity	Indicates if the appointment is sensitive
Is Hidden	Indicates if the appointment is hidden
Is Private	Indicates if the appointment is private
Priority	The priority of the appointment
Importance	The appointment importance setting

Outlook Contacts

Description	Microsoft Outlook is a personal information manager and email client. This table captures information related to contacts stored in Outlook.
Notes	

ATTRIBUTE	DESCRIPTION
Display Name	The contact's display name
Customer ID	The customer ID of the contact
Email Address 1	The contact's primary email address
Email Display As 1	The display string of the contact's primary email address
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the contact details were last modified
Company Name	The contact's company name
Department Name	The contact's department name
Title	The contact's job title
Profession	The contact's profession
Manager Name	The name of the contact's manager
Office Location	The contact's office location
Business Address	The physical address of the business
Business Phone	The contact's business phone number
Business Phone 2	The contact's secondary business phone number
Business Fax	The contact's business fax number
Business Homepage	The website of the contact's business
Email Display Name 1	The display name of the contact's primary email address
Email Address 2	The contact's secondary email address
Email Display As 2	The display string of the contact's secondary email address
Email Display Name 2	The display name of the contact's secondary email address
Email Address 3	The contact's tertiary email address

ATTRIBUTE	DESCRIPTION
Email Display As 3	The display string of the contact's tertiary email address
Email Display Name 3	The display name of the contact's tertiary email address
Cellular Phone	The contact's mobile phone number
Home Address	The contact's home address
Home Phone	The contact's home phone number
Home Phone 2	The contact's secondary home phone number
Home Fax	The contact's home fax number
FTP Site	The contact's FTP site
Body	More information about the contact
Attachments	Any attachments to the contact entry
Last Modifier Name	The name of the person who last modified the contact details

Outlook Journals

Description	Microsft Outlook is a personal information manager and email client from Microsoft. This table captures information related to journal entries stored in Outlook.
Notes	

ATTRIBUTE	DESCRIPTION
Creator Name	The name of the journal entry's creator
Last Modifier Name	The name of the person who last modified the journal entry
Subject	The subject of the journal entry
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the journal entry was last modified
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was created
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the journal entry was started
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the journal entry was finished
Type Description	The type of journal entry
Duration (minutes)	The length of the journal entry, in minutes
Body	The body of the journal entry
Attachments	List of attachments on the journal entry

Outlook Messages

Description	Microsft Outlook is a personal information manager and email client. This table captures information related to emails sent and received in Outlook.

Notes	

ATTRIBUTE	DESCRIPTION
Sender Name	The sender of the email
Sender Email	The email address of the sender
Recipients	The recipients of the email
Subject	The subject of the email
Sender Exchange Account	The sender's Exchange account name
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the email was created
Delivery Date/Time - UTC (yyyy-mm-dd)	The date and time the email was delivered
Body	The body of the email
Folder Name	The name of the folder where the email is stored
CC	The recipients of the email that were CC'd
BCC	The recipients of the email that were BCC'd
Attachments	The list of attachments on the email
Headers	The raw email headers
Priority	The priority of the email
Importance	The importance of the email
Sensitivity	The sensitivity of the email

Outlook Notes

Description	Microsoft Outlook is a personal information manager and email client. This table captures information related to notes written and stored in Outlook.
Notes	

ATTRIBUTE	DESCRIPTION
Creator Name	The name of the user who created the note
Last Modifier Name	The name of the person who last modified the journal entry
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the note was created
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the journal entry was last modified
Body	The body of the note

Outlook Tasks

Description	Microsoft Outlook is a personal information manager and email client. This table captures information related to tasks created in Outlook.
Notes	

ATTRIBUTE	DESCRIPTION
Owner	The owner of the task
Companies	The company the owner belongs to
Recipients	The recipients of the task
Subject	The subject of the task
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the task was last modified
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the task was created
Completed Date (yyyy-mm-dd)	The date the task was completed
Start Date (yyyy-mm-dd)	The date the task was started
Due Date (yyyy-mm-dd)	The due date of the task
Status	The status of the task
Percent Complete	The completeness of the task as a percentage
Body	The content of the task body
Attachments	Any attachments related to the task
Is Complete	Indicates if the task is complete
Actual Work (Minutes)	The actual amount of time it took to complete the task, in minutes
Total Work (Minutes)	The total amount of time for the task, in minutes
Mileage	The mileage that was travelled for the task
Billing Information	The billing information for the task
Delegator	The person who delegated this task to the user
Delgation State	Whether or not the task was delegated
Creator Name	The name of the person who created the task
Last Modifier Name	The name of the person who last modified the task
Is Hidden	Indicates if the task is hidden
Is Private	Indicates if the task is private
Is Read-Only	Indicates if the task is readable but not writable
Sensitivity	Indicates if the task is sensitive
Is Team Task	Indicates if the task is for a team
Is Recurring	Indicates if the task is recurring
Recurrence Pattern Description	Describes the recurrence pattern of the task, if applicable

ATTRIBUTE	DESCRIPTION
Is Reminder Set	Indicates if a reminder is set for the task
Reminder Date/Time - UTC (yyyy-mm-dd)	The date and time of the task reminder, if applicable
Priority	The priority of the task
Importance	The importance of the task

Outlook Web App Email Fragments

Description	Microsoft Outlook is a personal information manager and email client. This table captures information related to emails sent and received from Outlook's web application.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the email
Recipients	The recipient(s) of the email
Subject	The subject of the email
Server Timestamp	The timestamp of the email on the server
Is Draft	Indicates if the email is a draft
Fragment	The recovered raw email fragment

Outlook Web App Inbox

Description	Microsoft Outlook is a personal information manager and email client. This table captures information related to the inbox viewed from Outlook's web application.
Notes	

ATTRIBUTE	DESCRIPTION
Participants	The participants of the email
Subject	The subject of the email
Server Timestamp	The timestamp of the email on the server

Outlook Webmail Inbox

Description	Outlook.com (formerly hotmail.com) is a webmail website that allows users to send and receive emails.

Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the email
Date/Time - UTC (yyyy-mm-dd)	The date and time the email was sent/received
Displayed Date/Time - Local Time	The date and/or time the user was shown on the webpage
Subject	The subject of the message
Status	The sent status of the email

Windows Mail

Description	Email messages sent or received using Windows Mail.
Notes	

ATTRIBUTE	DESCRIPTION
To	The recipients of the email.
From	The sender of the email.
Date/Time	The date and time the email was sent/received.
Subject	The subject of the email.
Body	The body of the email.
CC	The recipients of the email that were CC'd.
BCC	The recipients of the email that were BCC'd.
Headers	The raw email headers.
Importance	The email importance setting.
Attachments	A list of attachments on the email.

Yahoo! Webmail

Description	Yahoo Mail is a web-based email client that allows users to send and receive emails.
Notes	

ATTRIBUTE	DESCRIPTION
Sender Name	The name of the sender
Sender Email	The email of the sender

ATTRIBUTE	DESCRIPTION
Receiver Name	The name of the receiver
Receiver Email	The email of the receiver
Subject	The email subject
Date/Time - UTC (yyyy-mm-dd)	The date and time the email was sent/received/drafted.
HTML Fragment	An HTML fragment of the email
Type	The type of message, some of which include the following: 'Folder Listing' indicates that the email was recovered from the Inbox view. 'Message' indicates that the user was looking at an individual email. 'Compose' indicates that the user was composing a message. 'Inbox Preview' indicates that the message was displayed as a preview.

Encryption

Encrypted Files

Description	Encrypted Files contains information about any files that have been recovered on the system that are encrypted. This artifact is not available in Magnet IEF.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the encrypted file.
File Size (Bytes)	The size of the encrypted file in bytes.
Detected File Type	The detected type of the encrypted file.
File Created Date/Time - UTC (yyyy-mm-dd)	The date and time the encrypted file was created on the filesystem.
File Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the encrypted file was last modified on the filesystem.
File Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the encrypted file was last accessed on the filesystem.
MD5 Hash	The MD5 hash of the file.
SHA1 Hash	The SHA1 hash of the file.

Encryption/Anti-forensics Tools

Description	Contains the encryption or anti-forensics tool(s) that have been found in the searched evidence.
Notes	You can find a list of the apps that are supported by this artifact at Encryption/Anti-forensics tools.

ATTRIBUTE	DESCRIPTION
Filename	The name of the executable for the encryption or anti-forensics tool.
Software	The name of the encryption or anti-forensics tool.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time the encryption or anti-forensics tool was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the encryption or anti-forensics tool was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the encryption or anti-forensics tool was last modified on the filesystem.

Media

Audio

Description	Audio files that are recovered that use the .mp3 or .wav formats.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
File Name	Name of the file.
File Extension	Extension of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the audio file was created.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the audio file was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the audio file was last modified.
File Size (Bytes)	The size of the audio file.
MD5 Hash	An MD5 hash of the audio content.
SHA1 Hash	A SHA1 hash of the audio content.

Carved Video

Description	Videos that are recovered using carving. Supported formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. Other container formats can also be recovered provided that their underlying packets are the same as one of the supported formats.
Notes	As of February 20 2020, this artifact will no longer be included under Videos. Carved Video functionality will be included in the 'Videos' artifact instead.

ATTRIBUTE	DESCRIPTION
Content Format	The format of the video.
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
File Size (Bytes)	The size of the container and file.
Container Format	The format of the video container.
Saved Video Size (Bytes)	The size of the video that was saved to the database.
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.

Pictures

Description	Pictures retrieved using either carving or parsing techniques.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date/time of the picture in the file system.

ATTRIBUTE	DESCRIPTION
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date/time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date/time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. "Complete" indicates that a full Exif extraction was performed. "Partial" indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. "Failed" indicates that the information may have been corrupted and could not be recovered. "Skipped" indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).

ATTRIBUTE	DESCRIPTION
GPS Longitude	The GPS longitude coordinates of where the picture was taken (extracted from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
GPS Latitude	The GPS Latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS Latitude (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the pciture was taken (extracted from Exif data).
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Potential Original Media	Indicating if the media is likely the original source.
Category	An integer that indicates the Project VIC category for the picture.

RealPlayer Library Assets

Description	RealPlayer Library Assets contains information about the items that have been added to the library. This artifact can reveal information about the user's interaction with the application.
Notes	

ATTRIBUTE	DESCRIPTION
Type	The type of asset, such as video, photo, or folder.
Path	The path to the asset.
Title	The asset's title.
Original Created Date/Time - UTC (yyyy-mm-dd)	The date and time the imported asset was original created.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time the asset was added to the library.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the asset was last accessed.
Exif Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time the imported asset was created according to its file metadata.
Private	Indicates whether the asset is marked private.

ATTRIBUTE	DESCRIPTION
Hidden	Indicates whether the asset is hidden.
Artist	The artist name associated with the asset, if applicable.
File Size (Bytes)	The size of the file in bytes.
Audio Format	The format of the asset's audio content (media files only).
Video Format	The format of the asset's video content (video files only).

RealPlayer Video History

Description	RealPlayer Video History contains information about the media files that were played using RealPlayer. This artifact can reveal information about the user's interaction with the application.
Notes	

ATTRIBUTE	DESCRIPTION
Video URL	URL of the video that was played, if streamed.
File Path	File path of the video, if it was played from the local filesystem.
File Name	File name of the video, if it was played from the local filesystem.
Last Viewed Date/Time - UTC (yyyy-mm-dd)	The date and time the video was last viewed.
First Viewed Date/Time - UTC (yyyy-mm-dd)	The date and time the video was first viewed.

Videos

Description	Videos that are recovered using parsing or carving. Supported formats for parsing include AVI, MP4, MOV, MPEG, DIVX, A3GP, ASF, WMV, DVR-MS, MKV, VOB, MOD, and WEBM. Supported carving formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. For more information about supported video formats, see Supported media and file types.
Notes	If AXIOM Process is configured to save only a specified amount of data from carved videos, any MD5 and SHA1 hashes that are generated are based on the data that's saved and not the full video. This behavior might cause issues when searching for known video hashes, as the hash for a carved video will differ from the actual video if it exceeds the size limit set in AXIOM Process.

ATTRIBUTE	DESCRIPTION
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
File Name	Name of the file.
File Extension	Extension of the file.

ATTRIBUTE	DESCRIPTION
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the video was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the video was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the video was last modified.
File Size (Bytes)	The size of the video.
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. "Complete" indicates that a full Exif extraction was performed, including potential metadata located at the end of the video. "Partial" indicates that only Exif information in the header section of the video file was recovered, which should only occur with very large videos (in excess of the limit set in the options screen). "Failed" indicates that the information may have been corrupted and could not be recovered. "Skipped" indicates that the extraction was skipped.
Media Duration (Seconds)	The duration of the video in seconds (extracted from Exif data).
Original Width	The resolution of the video (extracted from Exif data).
Original Height	The resolution of the video (extracted from Exif data).
Created Date/Time - Local Time	The local date and time when the video was first recorded (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the video was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the video being recored (extracted from Exif data).
Software	The software used to record or modify the video. This could either be the OS version of the phone used to record the video or name of the software used to edit the video in post-production (extracted from Exif data).

ATTRIBUTE	DESCRIPTION
Make	The manufacturer of the camera used to record the video (extracted from Exif data).
Model	The model of the camera used to record the video (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to record the video (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The GPS coordinates of the camera where the video was recorded (extracted from Exif data).
Longitude	The GPS coordinates of the camera where the video was recorded (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the video was recorded (extracted from Exif data).
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.
Content Format	The format of the carved video.
Container Format	The format of the carved video container.
Saved Video Size (Bytes)	The size of the carved video that was saved to the database.

VLC Recently Played Files

Description	VLC Recently Played Files contains information about the media files that are played using the VLC Media Player. This artifact can reveal information on the user's interaction with the application.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file that was played in the player.
File Path	The file path to the recently played file.
Resume Time (seconds)	The number of seconds played before the media file is paused or stopped. A value of -1 indicates that the file was watched completely. If the duration is less than 10 seconds, the Media Player will always set the value to 0.

Web Video Fragments

Description	This search recovers two distinct types of web-based video. Fragme nts of Flash video can be left behind by many video streaming sites, such as YouTube. RTMP Frame Fra gments are frames left behind by streaming sites using the RTMP protocol (widely used by webcam chat sites, including Chatroulette and Camstumble). In the case, a thumbnail from a recovered video is displayed, as well as any relevant metadata. Videos can be exported to .FLV format to be played. Due to the natur e of the data recovered, some video players will have issues playing the exported files. We recommen d trying ffmpeg, VLC, and the GOM player.
Notes	

ATTRIBUTE	DESCRIPTION
Preview	A thumbnail preview of the video
Content Recovered	The raw bytes that were recovered
Metadata	Any metadata about the video
Recovered Duration	The length of the video that was recovered

Memory

Active Network Info (sockets)

Description	The Active Network Info (sockets) artifact can be used to detect listening sockets and identify active networks. For more information about the sockets utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#sockets.
Notes	

ATTRIBUTE	DESCRIPTION
Process ID	The process ID, or PID.
Local Port	The port that was opened by the socket.
Protocol	The transport layer protocol that the socket is listening for.
IP Address	The IP address associated with the socket.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the socket was created.

API Hooks (apihooks)

Description	The API Hooks (apihooks) artifact detects various styles of programming hooks. For more information about the apihooks utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference-Mal#apihooks.
Notes	

ATTRIBUTE	DESCRIPTION
Process ID	The process ID, or PID.
Process Name	The name of the process where the hook is found.
Hook Mode	The hook mode that was used.
Hook Type	The hook type that was used.
Victim Module	The victim module.
Function	The function that called the hook.
Hook Address	The address in memory where the hook is located.
Hooking Module	The hooking module.
Assembly Instructions	The assembly instructions field.

Clipboard (clipboard)

Description	The Clipboard (clipboard) artifact recovers data that the user saves to their clipboard. For more information about the clipboard utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference-Gui#clipboard.
Notes	

ATTRIBUTE	DESCRIPTION
Text	The text that was saved to the clipboard.
Data	The hex representation of the data saved to the clipboard.
Session ID	The session ID associated.
Window Station	The window station field.
Format	The format of the data that is saved to the clipboard.
Handle ID	The handle ID field.
Object ID	The object ID field.

Command History (cmdscan)

Description	The Command History (cmdscan) artifact returns a history of commands that are run in the Command Prompt (cmd.exe). These results can help provide insight into an attack on the system. For more information about the cmdscan utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#cmdscan.
Notes	

ATTRIBUTE	DESCRIPTION
Process ID	The process ID, or PID.
Process Name	The name of the console host process (either csrss.exe or conhost.exe).
Command History Location	The location in memory where the command history is located.
Application Name	The name of the application (or the process that is using cmd.exe).
Flags	The flags field from cmdscan.
Command Count Total	The total number of commands that are recovered.
Last Added Command Number	The last added command number.
Last Displayed Command Number	The last displayed command number.
First Command	The first command.
Command Count Maximum	The maximum number of commands that the console saves (the default is 50).
Handles	The application process handle.
Command Number	The number for the command.
Command	A string that contains the command that was run.

Connection Scan (connscan)

Description	The Connection Scan (connscan) artifact contains information about network connections, both active and terminated. For more information about the connscan utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#connscan.
Notes	

ATTRIBUTE	DESCRIPTION
Local Address	The local IP address.
Remote Address	The remote IP address.
Process ID	The process ID, or PID.

Dynamically Loaded Libraries (dlllist)

Description	The Dynamically Loaded Libraries (dlllist) artifact contains information about the files that were loaded into memory. For more information about the dlllist utility, see https://-github.com/volatilityfoundation/volatility/wiki/Command-Reference#dlllist.
Notes	

ATTRIBUTE	DESCRIPTION
Process Name	
Process ID	The process ID, or PID.
File Path	The path to the executable.
Load Count	The load count. This value can help indicate whether the DLL was statically or dynamically loaded.
DLL Path	The path to the DLL.

Files (filescan)

Description	The Files (filescan) artifact contains information about the files that were loaded into memory. For more information about the psxview utility, see https://-github.com/volatilityfoundation/volatility/wiki/Command-Reference#filescan.
Notes	

ATTRIBUTE	DESCRIPTION
Pointers	The number of pointers to the file.
Handles	The number of handles to the object.
Permissions	The permissions set on the file.
File Path	The path to the file.
File Name	The name of the file.

Hidden Processes (psxview)

Description	The Hidden Processes (psxview) artifact can help reveal processes that were hidden. For more information about the psxview utility, see https://-github.com/volatilityfoundation/volatility/wiki/Command-Reference-Mal#psxview.
Notes	

ATTRIBUTE	DESCRIPTION
Process ID	The process ID, or PID.
Process Name	The name of the process.
Pslist	Indicates whether the process is found in Pslist.
Psscan	Indicates whether the process is found in Psscan.
Thrdproc	Indicates whether the process is found in Thrdproc.
Pspcid	Indicates whether the process is found in Pspcid.
Csrss	Indicates whether the process is found in Csrss.
Session	Indicates whether the process is found in Session.
Deskthrd	Indicates whether the process is found in Deskthrd.
End Date/Time	The date and time the process ends.

Hidden/Residual Modules (modscan)

Description	The Hidden/Residual Modules (modscan) artifact scans memory for pool tags to reveal unloaded drivers or drivers that have been hidden/unlinked by rootkits. For more information about the modscan utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#modscan.
Notes	

ATTRIBUTE	DESCRIPTION
Driver Name	The name of the driver.
Base Address	The base address for the driver.
Size	The size of the driver.
File Path	The path to the driver.

Hidden/Terminated Processes (psscan)

Description	The Hidden/Terminated Processes (psscan) artifact can help reveal processes that were terminated or were hidden or unlinked by a rootkit. For more information about the psscan utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#psscan.
Notes	

ATTRIBUTE	DESCRIPTION
Physical Offset	
Process Name	
Process ID	The process ID, or PID.

ATTRIBUTE	DESCRIPTION
Parent Process ID	The parent process ID.
PDB	The location of the PDB.
Process Start Date/Time	The date and time the process started.
Process Exit Date/Time	The date and time the process exited.

Image Info (imageinfo)

Description	The Image Info (imageinfo) artifact reveals high-level information about the memory image being scanned. For more information about the imageinfo utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#imageinfo.
Notes	

ATTRIBUTE	DESCRIPTION
Suggested Profiles	The suggested Volatility profiles you should use with this memory image.
KDBG Address	The address for the KDBG structure.
Image Date/Time	The date and time the image was created.
Image Date/Time - Local Time	The date and time the image was created, local time.

LDR Modules (ldrmodules)

Description	The LDR Modules (ldrmodules) artifact can help reveal DLLs that have been hidden with malicious intent. For more information about the ldrmodules utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference-Mal#ldrmodules.
Notes	

ATTRIBUTE	DESCRIPTION
Process ID	The process ID, or PID.
Process Name	The name of the process.
Base Address	The base address.
In Load	Indicates whether the PE file is found in the Load list.
In Init	Indicates whether the PE file is found in the Init list.
In Memory	Indicates whether the PE file is found in the Memory list.
Mapped Path	The mapped path to the PE file.
Load Path	The path to the Load file.
Init Path	The path to the Init file.

ATTRIBUTE	DESCRIPTION
Memory Path	The path to the Memory file.

Loaded Kernel Modules (modules)

Description	The Loaded Kernel Modules (modules) artifact shows the kernel drivers that are loaded on the system. For more information about the modules utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#modules.
Notes	

ATTRIBUTE	DESCRIPTION
Driver Name	The name of the driver.
Base Address	The base address.
Size	The size of the kernel.
File Path	The path to the kernel.

Malware Finder (malfind)

Description	The Malware Finder (malfind) artifact can help reveal hidden or injected code/DLLs in memory. For more information about the malfind utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference-Mal#malfind.
Notes	

ATTRIBUTE	DESCRIPTION
Process ID	The process ID, or PID.
Process Name	The name of the affected process.
Vad Tag	The VAD tag (virtual address descriptor) for the memory segment.
Protection	The protection level.
Flags	Flags that are set on the memory segment.
Assembly Instructions	The assembly language representation of the memory segment.

Network Connections (connections)

Description	The Network Connections (connections) artifact can be used to recover information about active TCP connections. For more information about the connections utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#connections.

Notes	

ATTRIBUTE	DESCRIPTION
Local IP Address	The local IP address.
Remote IP Address	The remote IP address.
Process ID	The process ID, or PID.

Network Connections (sockscan)

Description	The Network Connections (sockscan) artifact can be used to detect sockets used in network connections. For more information about the sockscan utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#sockscan.
Notes	

ATTRIBUTE	DESCRIPTION
Process ID	The process ID, or PID.
Local Port	The local port used by the socket.
Protocol	The transport layer protocol that the socket is listening for.
IP Address	The IP address associated with the socket.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the socket was created.

Network Info (netscan)

Description	The Network Info (netscan) artifact can be used to recover network details from memory, such as TCP or UDP listeners and endpoints. For more information about the netscan utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#netscan.
Notes	

ATTRIBUTE	DESCRIPTION
Protocol	The protocol used for communication.
Local IP Address	The local IP address.
Remote IP Address	The remote IP address.
State	The state of the connection.
Process ID	The process ID, or PID.
Owner	The application or process that owns the connection.
Created Date/Time	The date and time the connection was established.

Open Handles (handles)

Description	The Open Handles (handles) artifact can be used to show the active handles in a process. For more information about the handles utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#handles.
Notes	

ATTRIBUTE	DESCRIPTION
Process ID	The process ID, or PID.
Virtual Offset	The offset in memory.
Handle ID	An identifier for the handle.
Access	The access number.
Handle Type	The type of handle.
Details	Additional details about the handle.

Process Security Identifiers (getsids)

Description	The Process Security Identifiers (getsids) artifact can be used to recover the SIDs (security identifiers) associated with a process. SIDs can be useful in identifying processes that have their privileges escalated with malicious intent. For more information about the getsids utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#getsids.
Notes	

ATTRIBUTE	DESCRIPTION
Process ID	The process ID, or PID.
Application Name	The name of the application that the SID is associated with.
Security ID	The security ID, or SID.
Security Identifier	The security identifier level. Some examples include Users, Administrators, or Everyone.

Processes (pslist)

Description	The Processes (pslist) artifact contains information about the processes that are loaded into memory. For more information about the pslist utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#pslist.
Notes	

ATTRIBUTE	DESCRIPTION
Process Name	The name of the process.
Process ID	The process ID, or PID.
Parent Process ID	The ID of the parent process, or PPID.
Number of Threads	The number of threads that the process contains.
Handles	The number of handles that the process has.
Session ID	The session ID for the process.
WoW64 Process	Indicates whether the process is a WoW64 process.
Process Start Date/Time	The time the process started.
Process Exit Date/Time	The time the process exited.

Timeline (timeliner)

Description	The Timeline (timeliner) artifact scans a number of different sources in memory, such as processes, event logs, threads, and registry keys, and creates hits to help illustrate a timeline of the events. For more information about the timeliner utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#timeliner.
Notes	

ATTRIBUTE	DESCRIPTION
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the event starts.
Type	The source of the event.
Item Name	The name of the item, or a path to the item.
Details	Additional details about the item.

Operating System

$LogFile Analysis

Description	$LogFile Analysis provides a sequence analysis of the $LogFile data, condensing the data to draw definitive conclusions on file operations (i.e. file creation, deletion, moving, renaming, and writing).
Notes	

ATTRIBUTE	DESCRIPTION
File Operation	The file operation that occurred.

ATTRIBUTE	DESCRIPTION
Event Date/Time - UTC (yyyy-mm-dd)	The date and time that the file operation occurred.
MFT Record Number	The MFT Record number for the file in this operation.
MFT Reference Number	The MFT Reference number for the file in this operation.
Update Sequence Number	The Update Sequence Number (USN) associated with this file operation.
Starting LSN	The starting Log Sequence Number (LSN) associated with this operation.
Original Short File Name	The original state of the file name (8.3 filename format).
Original File Name	The original state of the file name (long filename format).
Original MFT Modified Date/Time - UTC (yyyy-mm-dd)	The original state of the MFT Modified Date/Time field as stored in the MFT.
Original Created Date/Time - UTC (yyyy-mm-dd)	The original state of the Created Date/Time as stored in the MFT.
Original Modified Date/Time - UTC (yyyy-mm-dd)	The original state of the Modified Date/Time field as stored in the MFT.
Original Accessed Date/Time - UTC (yyyy-mm-dd)	The original state of the Accessed Date/Time field as stored in the MFT.
Original Parent MFT Record Number	The original Parent MFT Record number as stored in the MFT.
Original Parent MFT Reference Number	The original Parent MFT Reference number as stored in the MFT.
Current Short File Name	The current state of the file name (8.3 filename format).
Current File Name	The current state of the file name (long filename format).
Current MFT Modified Date/Time - UTC (yyyy-mm-dd)	The current state of the MFT Modified Date/Time field as stored in the MFT.
Current Created Date/Time - UTC (yyyy-mm-dd)	The current state of the Created Date/Time field as stored in the MFT.
Current Modified Date/Time - UTC (yyyy-mm-dd)	The current state of the Modified Date/Time field as stored in the MFT.
Current Accessed Date/Time - UTC (yyyy-mm-dd)	The current state of the Accessed Date/Time field as stored in the MFT.
Current Parent MFT Record Number	The current Parent MFT Record Number as stored in the MFT.
Current Parent MFT Reference Number	The current Parent MFT Reference Number as stored in the MFT.

.DS_Store Records

Description	.DS_Store Records contains all the records extracted from .DS_Store files found on the computer. Each record represents a property of a file or a folder. The significance of this artifact is an indicator of high likelihood that the user of the computer was aware of these files and folders with a possibility of attributing a date to that awareness.
Notes	In the Apple macOS operating system, .DS_Store (Desktop Services Store) is a hidden file that stores the display information of its containing folder, similar to the file desktop.ini in Microsoft Windows. The file tracks information such as icon positions, view settings, cached file size, cached last modified date, and even the choice of a background image. The .DS_Store is created and maintained by the Finder application in any folder that it accesses, even on remote file systems mounted from servers that share files (for example, via Server Message Block (SMB) protocol or the Apple Filing Protocol (AFP)). .DS_Store files are also included in archives created by macOS users, such as ZIP files, and they are backed up by some cloud file backup services. This means that the presence of .DS_Store Records artifacts on non-Mac evidence such as Windows, Mobile, or Cloud indicates that some of the data may have originated or have been accessed from a macOS computer at some point. For more information on .DS_Store files and their forensic significance see: .DS_Stores: Like Shellbags but for Macs.

ATTRIBUTE	DESCRIPTION
Record Name	The name of the file or folder as stored in the .DS_Store file.
Record Type	The type of the record, or property, that is being logged in the .DS_Store file for a particular file or folder.
Record Value	The value of the property for the given file or folder.
Record Path	The full path to the file or folder
.DS_Store Created Date/Time - UTC (yyyy-mm-dd)	The created date of the .DS_Store file from which the record was extracted.
.DS_Store Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date of the .DS_Store file from which the record was extracted.
.DS_Store Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date of the .DS_Store file from which the record was extracted.

AmCache Device Containers

Description	AmCache Device Containers contains information recovered from the AmCache about the devices that are connected to the system (for example, printers, Bluetooth devices, and storage devices).
Notes	

ATTRIBUTE	DESCRIPTION
Model Name	The model name for the device.
Model Number	The model number of the device.
Key Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the registry key was last updated.
Categories	The category of the device. Some examples are display.monitor, input.mouse, printfax.fax, and printfax.printer.
Discovery Method	The DiscoveryMethod property recovered from the registry subkey (value is a string).
Friendly Name	A display name for the device.
Icon	The path to the icon for the device.
Active	Whether or not the device is active.
Connected	Whether or not the device is connected.
Machine Container	Whether or not the device is a machine container.
Networked	Whether or not the device is networked.
Paired	Whether or not the device is paired.
Manufacturer	The device manufacturer.
Model ID	The model ID of the device.
Primary Category	The PrimaryCategory property recovered from the registry subkey (value is a string).
State	The State property recovered from the registry subkey (value is an integer).

AmCache Driver Binaries

Description	AmCache Driver Binaries contains information recovered from the AmCache about driver binaries on the system. These records can contain information about when a driver is signed, the company associated with the driver, and what service it is associated with.
Notes	

ATTRIBUTE	DESCRIPTION
Driver Name	The name of the driver.
Key Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the registry key was last updated.
Driver Last Write Date/Time - UTC (yyyy-mm-dd)	The date and time the driver was last written to.
Key	The registry key value.
Driver In Box	The DriverInBox property recovered from the registry subkey (value is a string).

ATTRIBUTE	DESCRIPTION
Driver Is Kernel Mode	Whether the driver operates in kernel mode.
Driver Signed	Whether the driver is signed.
Driver Checksum	The checksum of the driver.
Driver Company	The company that produces the driver.
Driver ID	The ID of the driver.
Driver Package Strong Name	The DriverPackageStrongName property recovered from the registry subkey (value is a string).
Driver Timestamp	The DriverTimeStamp property recovered from the registry subkey (value is an integer).
Driver Type	The driver type.
Driver Version	The driver version.
Image Size	The size of the driver file.
Inf	The Inf property recovered from the registry subkey (value is a string).
Product	The product the driver is associated with.
Product Version	The product version.
Service	The service associated with the driver.
Wdf Version	The WdfVersion property recovered from the registry subkey (value is a string).

AmCache Driver Packages

Description	AmCache Driver Packages contains information recovered from the AmCache about driver packages on the system.
Notes	

ATTRIBUTE	DESCRIPTION
Key	The registry key value.
Key Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the registry key was last updated.
Date	The date of the driver package.
Class	The class of driver.
Directory	The directory where the driver can be located.
Driver In Box	The DriverInBox property recovered from the registry subkey (value is a string).
HWIDs	A list of associated hardware IDs.

ATTRIBUTE	DESCRIPTION
Inf	The Inf property recovered from the registry subkey (value is a string).
Provider	The driver provider.
Submission ID	The SubmissionId property recovered from the registry subkey (value is a string).
SYSFILE	The SYSFILE property recovered from the registry subkey (value is a string).
Version	The driver version.

AmCache File Entries

Description	AmCache File Entries contains information recovered from the AmCache about files that are used by executable programs.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the file.
Key Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the registry key was last updated.
File Extension	The extension of the file.
Program ID	The program ID of the program associated with the file.
Key	The registry key value.
Associated Application Name	The name of the application associated with the file.
SHA1 Hash:	The SHA1 hash of the file.
OS Component	Whether or not this file is an operating system component.
Full Path	The full path to the file.
Link Date	The link date of the file.
Product Name	The name of the product.
Size	The size of the file.
Version	The version of the file.
Product Version	The product version of the file.
Long Path Hash	The hash of the long path associated with the file.
Binary Type	The BinaryType property recovered from the registry subkey (value is a string).
PE File	Whether or not the file is a portable executable file.
Bin File Version	The binary file version.

ATTRIBUTE	DESCRIPTION
Bin Product Version	The binary product version.
Language	The language code of the file.

AmCache File Entries - Legacy

Description	AmCache File Entries contains information recovered from the AmCache about files that are used by executable programs. This version of the artifact is for the older, legacy version of the AmCache.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the file.
Key Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the registry key was last updated.
File Extension	The extension of the file.
Program ID	The program ID of the program associated with the file.
Key	The registry key value.
Associated Application Name	The name of the application associated with the file.
SHA1 Hash:	The SHA1 hash of the file.
Full Path	The full path to the file.
Link Date	The link date of the file.
Product Name	The name of the product.
Size	The size of the file.
Version	The version of the file.
Product Version	The product version of the file.
Language	The language code of the file.
Volume GUID	The guid of the volume where the file is located.
Publisher	The publisher of the file.
Switch Back Context	The 4 property recovered from the registry subkey (value is an integer).
Description	The description of the file.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created.
Last Modified 2 Date/Time - UTC (yyyy-mm-dd)	The 17 property recovered from the registry subkey (value is a UTC timestamp).

ATTRIBUTE	DESCRIPTION
PE Header Field Size Of Image	The field header size of the image for the portable executable.
Hash Of PE Header	The hash of the header of the portable executable.
PE Header Checksum	The checksum of the portable executable header.

AmCache Pnp Devices

Description	AmCache Pnp Devices contains information recovered from the AmCache about plug-n-play devices connected to the system.
Notes	

ATTRIBUTE	DESCRIPTION
Driver Name	The name of the driver.
Key Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the registry key was last updated.
Description	The description of the device.
Key	The registry key value.
Bus Reported Description	The BusReportedDescription property recovered from the registry sub-key (value is a string).
Class Value	The class of the device.
Class Guid	The guid of the device class.
COMPID	The COMPID property recovered from the registry subkey (value is a string).
Container ID	The ID of the device container.
Driver ID	The ID of the driver.
Driver Package Strong Name	The DriverPackageStrongName property recovered from the registry subkey (value is a string).
Driver Date	The date of the driver.
Driver Version	The driver version.
Enumerator	The Enumerator property recovered from the registry subkey (value is a string).
HWID	The hardware ID of the device.
Inf	The Inf property recovered from the registry subkey (value is a string).
Install State	The InstallState property recovered from the registry subkey (value is a string).
Manufacturer	The device manufacturer.
Matching ID	The MatchingId property recovered from the registry subkey (value is a string).

ATTRIBUTE	DESCRIPTION
Model	The device model.
Parent ID	The ParentId property recovered from the registry subkey (value is a string).
Problem Code	The ProblemCode property recovered from the registry subkey (value is a string).
Provider	The device provider.
Service	The Service property recovered from the registry subkey (value is a string).
STACKID	The STACKID property recovered from the registry subkey (value is a string).

AmCache Program Entries

Description	AmCache Program Entries contains information recovered from the AmCache about the applications that are run on the system.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the program.
Key Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the registry key was last updated.
Install Date	The date the program was installed.
Version	The program version.
Publisher	The program publisher.
Uninstall Date/Time - UTC (yyyy-mm-dd)	The date and time the program was uninstalled.
OS Version At Install Time	The version of the operating system when the program was installed.
Bundle Manifest Path	The path to the bundle manifest.
Hidden Arp	The HiddenArp property recovered from the registry subkey (value is an integer).
Inbox Modern App	The InboxModernApp property recovered from the registry subkey (value is an integer).
Language	The language code of the program.
Manifest Path	The path to the manifest file.
Msi Package Code	The msi package guid.
Msi Product Code	The msi product guid.
Package Full Name	The full name of the package.

ATTRIBUTE	DESCRIPTION
Program ID	The ID of the program.
Program Instance ID	The ID of the program instance.
Uninstall Registry Key Path	The path to the uninstall string in the registry.
Root Dir Path	The root directory path of the program.
Type	The type of program.
App Source	The source of the program.
Store App Type	The type of program in the store.
Uninstall String	The string that can be used to uninstall the program.

AmCache Program Entries - Legacy

Description	AmCache Program Entries contains information recovered from the AmCache about the applications that are run on the system. This version of the artifact is for the older, legacy version of the AmCache.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the program.
Key Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the registry key was last updated.
Install Date/Time - UTC (yyyy-mm-dd)	The date and time the program was installed.
Version	The program version.
Publisher	The program publisher.
Uninstall Date/Time - UTC (yyyy-mm-dd)	The date and time the program was uninstalled.
Language	The language code of the program.
Msi Package Code	The msi package guid.
Msi Product Code	The msi product guid.
Uninstall Registry Key Path	The path to the uninstall string in the registry.
Install Source	The source of the program installation.
File Entries	The file entries associated with the program.
File Paths	The file paths associated with the program.

AmCache Shortcuts

Description	AmCache Shortcuts contains information recovered from the AmCache about applications and file shortcuts are that are used on the system.

Notes	

ATTRIBUTE	DESCRIPTION
Key	The name of the registry key.
Key Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the registry key was last updated.
Shortcut Path	The path to the shortcut.

Autorun Items

Description	The Autorun Items artifact describes the programs that are configured to run automatically when a certain system event occurs.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the program.
File Path	The file path to the program.
Command	The command executed when the trigger condition is met. For Run items, this is the raw registry value.
Type	The type of autorun item.
Trigger Condition	The system event condition that triggers the autorun command.
Registry Key Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the registry key containing the autorun item was last modified
Metadata	Additional information about the autorun items.

Cortana Person Reminders

Description	Cortana Person Reminders are reminders that can be set for a specific contact. Cortana triggers the reminders when an interaction with that contact occurs (for example, when an email is received).
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the reminder.
Contact Name	The name of the contact associated with the reminder.
Status	The status of the reminder. The reminder can be Active (either has not been triggered yet or is an ongoing reminder), Deleted, or Completed.

ATTRIBUTE	DESCRIPTION
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the person reminder was created.
Last Update Date/Time - UTC (yyyy-mm-dd)	The date and time the person reminder was last updated.
Completion Date/Time - UTC (yyyy-mm-dd)	The date and time the person reminder was completed.

Cortana Place Reminders

Description	Cortana Place Reminders are virtual areas that you can define in Cortana to represent a real geographic place. Entering or leaving an area can trigger Cortana to display the reminder.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the reminder.
Location Name	The name of the location associated with the reminder.
Trigger Condition	The condition under which the reminder will be triggered, either arrival or departure.
Status	The status of the reminder. The reminder can be Active (either has not been triggered yet or is an ongoing reminder), Deleted, or Completed.
Recurrence	The recurrence of the reminder. Can recur on specific days of the week, or every time a user visits that location.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the place reminder was created.
Last Update Date/Time - UTC (yyyy-mm-dd)	The date and time the place reminder was last updated.
Completion Date/Time - UTC (yyyy-mm-dd)	The date and time the place reminder was completed.
Latitude	The latitudinal coordinates of the place reminder.
Longitude	The longitudinal coordinates of the place reminder.

Cortana Time Reminders

Description	Cortana Time Reminders are reminders that can be set for a specific time.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the reminder.
Trigger Date/Time - UTC (yyyy-mm-dd)	The date and time the time reminder is set to trigger.
Status	The status of the reminder. The reminder can be Active (either has not been triggered yet or is an ongoing reminder), Deleted, or Completed.
Recurrence	The recurrence of the reminder. Can recur on specific days of the week.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the time reminder was created.
Last Update Date/Time - UTC (yyyy-mm-dd)	The date and time the time reminder was last updated.
Completion Date/Time - UTC (yyyy-mm-dd)	The date and time the time reminder was completed.

File Associations

Description	Information about application associations for files. Users or applications can set associations for file types so that when a file of a specified file type is opened, a command gets triggered by Windows.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the program that is run when a file of the specified File Type is opened.
File Path	A path to the program that is run when a file of the specified File Type is opened.
Command	The command that is executed when a file of the specified File Type is opened.
File Type	The file type that triggers the associated Command to be executed.
Registry Key Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the registry key that contains the file association information was last modified.

File Signature Mismatch (Audio)

Description	File Signature Mismatch (Audio) contains identified mismatches between a known file signature header and the extension (or lack thereof) for an audio file. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.

File Signature Mismatch (Container)

Description	File Signature Mismatch (Container) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a container. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.

File Signature Mismatch (Document)

Description	File Signature Mismatch (Document) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a document. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.

File Signature Mismatch (Picture)

Description	File Signature Mismatch (Picture) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a picture. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file. If the mime type is unknown, this defaults to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file. If the mime type is unknown, this defaults to application/octet-stream. If there is no file extension, but the mime type is known, a mismatch is is returned.
File Path	The path to the mismatched file.

File Signature Mismatch (Video)

Description	File Signature Mismatch (Video) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a video. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.

File System Information

Description	Information pertaining to the File System that was searched
Notes	

ATTRIBUTE	DESCRIPTION
Volume Serial Number	This field only applies to FAT and NTFS file systems. This is a 32-bit unsigned int value that is stored in Bios Paramter Block (BPB) and is showed in a special hex format XXXX-XXXX e.g. EABB-6573. For other file systems, the value of this field should show "n/a".
Full Volume Serial Number	This field is a 64-bit volume serial number that is only present in BPB of NTFS file system, for example AABBCCDDEEFF0011. For non-NTFS file systems, "n/a" is displayed for this field.
File System	Shows the type of the file system, e.g "Microsoft NTFS"
Sectors per cluster	The number of sectors in a file system cluster, e.g. 8
Starting Sector	The starting sector for this partition.
Ending Sector	The ending sector for this partition.
Total Sectors	Encase shows different values for this field based on how a volume is added to the case. For example, if you add just a volume (e.g. your local C:\ drive), it shows 123410271 for the number of sectors, but if you add your local physical drive 0 to the case and then select your C:\ volume in the "Entries" tree (note: your C drive would most likely have another letter in this tree, e.g. E:), then total number of sectors would be one more that the other value, i.e. 123410272. the value show for this field is taken from BPB, which matches the first value. The other value is shown when the parent physical drive is present probably comes from the partition table, and it counts VBR as well.
Total Capacity	This value is calculated by Total Clusters * Cluster Size, which shows the capacity of the file system and not the volume containing it. The size of the volume would be higher than this value.

ATTRIBUTE	DESCRIPTION
Total Clusters	The number of clusters comprising the file system
Unallocated	Number of unallocated bytes on the file system, which is calculated by (Number of free clusters) * (cluster size)
Free clusters	Number of unallocated clusters in the file system
Allocated	(Number of allocated clusters) * (cluster size)
Volume Name	This is the volume label stored in Volume Boot Record (VBR)
Volume Offset	The offset (in bytes) of the volume containing this file system from beginning of the disk. "0" is displayed if the image and/or drive being searched is the image of one volume. Encase shows the number of sectors for this field instead of the number of bytes.

IME Suggestions (Japanese)

Description	IME Suggestions (Japanese) contains Japanese characters that have been suggested to the user as they use the Input Method Entry (IME) feature in Windows. This feature allows a user to provide a unicode string and returns the equivalent Japanese characters as a suggestion.
Notes	

ATTRIBUTE	DESCRIPTION
Created Time/Date - UTC (yyyy-mm-dd)	The date and time the entry was created.
Candidate 1	The first candidate that's provided in response to the characters typed by the user.
Candidate 2	The second candidate that's provided in response to the characters typed by the user.

Installed Microsoft Programs

Description	Applications installed on the machine which are published by Microsoft.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The name of the installed application.
Company	The publisher listed when the program was installed.

ATTRIBUTE	DESCRIPTION
Created Date	The date of installation or most recent update.
Key Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the key was last updated in the registry.
Install Size (Bytes)	The estimated install size of the installation. Calculated in bytes.
Version	The publisher provided version number of the application.
Potential Location	The potential location for the application's executable, as determined by the location where the icon for the application was found.

Installed Programs

Description	Applications installed on the machine which are not published by Microsoft.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The name of the installed application.
Company	The publisher listed when the program was installed.
Created Date	The date of installation or most recent update.
Key Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the key was last updated in the registry.
Install Size (Bytes)	The estimated install size of the installation. Calculated in bytes.
Version	The publisher provided version number of the application.
Potential Location	The potential location for the application's executable, as determined by the location where the icon for the application was found.

Jump Lists

Description	Jump lists are quick lists of recent applications or files that a user launched. The Dest List entries and shortcut entries are combined into a single table showing their joined structure.
Notes	

ATTRIBUTE	DESCRIPTION
App ID	The unique app identifier generated by Windows based on install location
Potential App Name	A potential app name from a list of common applications and install locations

ATTRIBUTE	DESCRIPTION
Linked Path	The path to the target file
Arguments	Any commands being passed to the target file
Volume Name	The name of the volume where the shortcut resides
Volume Serial Number	The serial number of the volume
Target File Created Date/Time - UTC (yyyy-mm-dd)	The date and time the shortcut target file was created
Target File Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the shortcut target file was last modified
Target File Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the shortcut target file was last accessed
Jump List Type	The type of jump list. ("Automatic" or "Custom")
Drive Type	The type of drive for the shortcut
Target NetBIOS Name	The machine name on the network the shortcut is on
Target MAC Address	The MAC address of the volume the shortcut is on
Target File Size (Bytes)	The size of the shortcut file
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last time the shortcut entry was accessed
Entry ID	The entry ID
Data	Other data within the shortcut entry
NetBIOS Name	The machine name on the network
Pin Status	If the shortcut was pinned in the dest list

Keyword Searches

Description	A list of keywords that were searched for on the system.
Notes	

ATTRIBUTE	DESCRIPTION
Search Term	The term that was searched.
Searched Date/Time - UTC (yyyy-mm-dd)	The date and time that the term was searched.

Known DLLs

Description	Known DLLs is a list of DLLs that have been cached by Windows and are known to be safe. The DLLs are assumed to be located at either the folder path found in DLL Directory or DLL Directory32. The list of Known DLLs can be found at the following registry location: SYSTEM\CurrentControlSet\Control\Session Manager\KnownDlls
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The filename of the known dll.
DLL Directory	The value stored under the DllDirectory value in the known dll registry key.
DLL Directory32	The value stored under the DllDirectory32 value in the known dll registry key.
Registry Key Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the known dll registry key was last modified.

Latent Wireless Geolocated WiFi Hotspots

Description	Latent Wireless Geolocated WiFi Hotspots contains information about WiFi hotspots that were discovered using a Latent Wireless device. Latent Wireless stores information about the hotspots in a database that Magnet AXIOM can parse for details about each hotspot.
Notes	

ATTRIBUTE	DESCRIPTION
MAC Address	The MAC address of the detected WiFi hotspot.
First Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was first discovered.
Last Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was last seen.
Strongest Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was detected at its highest strength.
Network Name (SSID)	The SSID of the WiFi hotspot.
Channel	The WiFi hotspot channel.
RSSI	The receieved signal strength indicator for the WiFi hotspot.
Latitude	The latitude where the WiFi hotspot was detected.
Longitude	The longitude where the WiFi hotspot was detected.
Secure	Indicates whether the wiFi hotspot is secure.

LNK Files

Description	LNK files are Windows shortcut files that point to other files on the system.
Notes	LNK files can be shortcuts to executables, media files, or any other type of file on the system. LNK files can be carved from many different areas of the OS, and the forensic importance of each type of LNK file varies from source to source.

ATTRIBUTE	DESCRIPTION
Linked Path	The path to the target file
Arguments	Any commands being passed to the target file
Target File Created Date/Time - UTC (yyyy-mm-dd)	The date and time the shortcut target file was created
Target File Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the shortcut target file was last modified
Target File Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the shortcut target file was last accessed
Target Attributes	Any file attributes of the target file
Drive Type	The type of drive for the shortcut
Volume Serial Number	The serial number of the volume
Volume Name	The name of the volume where the shortcut resides
Show Command	How the shortcut should show the target when opened, one of: SW_SHOWNORMAL, SW_SHOWMAXIMIZED, SW_SHOWMINNOACTIVE, or Unknown.
Net Bios Name	The machine name on the network
MAC Address	The MAC address of the volume the shortcut is on
Target File Size (Bytes)	The size of the shortcut file

LogMeIn Activity

Description	LogMeIn Activity records connection events that occur using the LogMeIn remote desktop client. These records can include remote sessions and file sharing events.
Notes	

ATTRIBUTE	DESCRIPTION
Date/Time Local Time	The time in local time when the log line was recorded.
Activity Type	The type of the activity that was recorded. The Session type indicates that the event is a remote session. The SessionDateReport indicates that the recorded event is a session summary. And, the FileShare type indicates that the recorded event was a file being shared with other users.
Connection Type	The type of connection that was used.
Status	Indicates the status of the file sharing event (only applies to FileShare activities).
Remote IP Address	The public IP address of the client server.
Local IP Address	The public IP address of the host server.
Connection State	The login/logout state of the connection.
OS Version	The OS version of the host.

McAfee Logs

Description	McAfee Logs identifies and collects any log files created by McAfee Antivirus and McAfee ePO.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the log file.
File Path	The path of the log file.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the log file was created.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the log file was last accessed.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the log file was last modified.

MRU Folder Access

Description	The MRU Folder Access artifact contains information about the folders that are accessed by a Windows application using Open/Save browsing dialogs. Windows versions above XP use PIDL to store file path. PIDL paths might contain GUIDs instead of relative path strings. Folder access data cis recovered from the following registry location: Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU (LastVisitedMRU for Windows XP).
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	Name of the application that was used to access a directory.
Folder Accessed	Full path to the folder that the application accesses while using a Windows dialog (such as an Open/Save dialog).
Registry Key Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the MRU registry key was last modified.
Registry Order	Order of recency in which specific directories have being accessed by specific applications. Values occur in an ascending order, with a value of 1 indicating that a directory was accessed the most recently.
Value Name	Name of the value associated with the record within registry key.

MRU Opened/Saved Files

Description	MRU Opened/Saved Files contains information about last files accessed by any application through 'Open File' or 'Save File' dialog window. Windows versions above XP use PIDL to store file path. PIDL paths might contain GUIDs instead of relative path strings. Opened/Saved files data can be found at the following registry location: Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\<subkey> (OpenSaveMRU for Windows XP).
Notes	

ATTRIBUTE	DESCRIPTION
File Name	Name of the file that was accessed using a Windows dialog (such as an Open/Save dialog)
File Path	Full path to the file.
Registry Key Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the mru registry key was last modified.

ATTRIBUTE	DESCRIPTION
Registry Order	Order of recency in which specific files were opened or saved by any applications. Values occur in an ascending order, with a value of 1 indicating that a file was opened/saved the most recently.
Value Name	Name of the value associated with the record within registry key.

MRU Recent Files And Folders

Description	The MRU Recent Files And Folders artifact contains information about files that were recently opened or saved and folders that were opened. This data is often related to items found in the Recent folder in the Users directory. Recent files and folders data is recovered from the following registry location: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs.
Notes	

ATTRIBUTE	DESCRIPTION
File/Folder Name	Name of the file or folder that was recently accessed.
File/Folder Link	A shortcut file name that is associated with the recently accessed file or folder.
Registry Key Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the MRU registry key was last modified.
Registry Order	Order of recency in which specific files or directories have being accessed by any applications. Values occur in an ascending order, with a value of 1 indicating that a file/directory was accessed the most recently.
Value Name	Name of the value associated with the record within registry key.

MRU Run Commands

Description	The MRU Run Commands artifact contains information about commands that a user runs using the Run utility for Windows. Run command data is recovered from the following registry location: Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU.
Notes	

ATTRIBUTE	DESCRIPTION
Run Command	A command string that a user provides in the Windows Run utility. This value can be a folder path, file path, or an command.
Registry Key Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the MRU registry key was last modified.

ATTRIBUTE	DESCRIPTION
Registry Order	Order of recency in which specific command was run through 'Run' application. Values occur in an ascending order, with a value of 1 indicating that a command was run the most recently.
Value Name	Name of the value associated with the record within registry key.

MUICache

Description	The MUICache artifact contains information about the files that are executed on the system, as parsed from the MUICache registry key.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file that is executed.
File Path	The path to the file that is executed. This value is stored in the Name field of the MUI registry.
Data	Additional information about the file (for example, the name or a description of the application it belongs to).

Network Interfaces (Registry)

Description	Contains a list of all of the Network Interfaces that the image has stored in the registry.
Notes	

ATTRIBUTE	DESCRIPTION
Description	A brief description of the interface.
MAC Address	The physical MAC address of the interface.
DHCP Enabled?	Whether or not DHCP is enabled on this interface. If it is, this will be 'Yes', otherwise this will be 'No'.
IPv4 Address	The IPv4 address of the interface.
IPv4 Subnet Mask	The IPv4 subnet mask of the interface
Lease Obtained Date/Time - UTC (yyyy-mm-dd)	The date and time that the lease was obtained on this interface.
Lease Expires Date/Time - UTC (yyyy-mm-dd)	The date and time that the lease will expire on this interface.
Default Gateway(s)	A comma separated list of the default gateways associated with this interface.

ATTRIBUTE	DESCRIPTION
DHCP Server	A comma separated list of the DHCP servers associated with this interface.
DNS Server(s)	A comma separated list of the DNS servers associated with this interface.
DHCP IPv4 Address	The DHCP assigned IPv4 address of the interface.
DHCP IPv4 Subnet Mask	The DHCP assigned IPv4 subnet mask of the interface
DHCP DNS Server(s)	A comma separated list of the DHCP assigned DNS servers associated with this interface.
DHCP Default Gateway(s)	A comma separated list of the DHCP assigned default gateways associated with this interface.
DNS Domain	The DNS domain of the interface
DHCP DNS Domain	The DHCP assigned DNS domain of the interface

Network Profiles

Description	A list of the saved Network Profiles on a machine.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	The name of the saved network profile.
Network Name (SSID)	The name of the network associated with the saved network profile.
Profile Created Date/Time - Local Time (yyyy-mm-dd)	The local date/time that the profile was created.
Last Connected Date/Time - Local Time (yyyy-mm-dd)	The last date/time that the network was connected to.
DNS	The DNS associated with this network connection.
Default Gateway MAC	The default gateway MAC associated with this network connection.
Broadcast SSID	Whether or not this network broadcasts its SSID.
Connection Type	The type of connection, either ESS or IBSS.
Connection Mode	How the network connects, either manual or auto.
Authentication	The authentication mode of the network.
Encryption	The method of encryption used.
Password	The password used to connect to the network.

Network Share Information

Description	This provides information about mapped network drives on Windows.
Notes	

ATTRIBUTE	DESCRIPTION
Network Name	The network share name
Mapped Drive Letter	The drive letter assigned to the share
Connection Type	The type of connection to the share
Provider Name	The share provider
Account	The account associated to the network share
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the share mapping was last modified

Network Usage - Application Data

Description	Network Usage - Application Data contains information about how an application sends or receives data over the network.
Notes	

ATTRIBUTE	DESCRIPTION
Process Name	The file name of the executable.
Type	The executable type (Process or App).
First Used Date/Time - UTC (yyyy-mm-dd)	The date and time the process was first run.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time the process was last run.
Last Connected Date/Time - UTC (yyyy-mm-dd)	The date and time the process last connected to a network.
WiFi Bytes Sent	The number of bytes sent over a WiFi connection.
WiFi Bytes Received	The number of bytes received over a WiFi connection.
Mobile Bytes Sent	The number of bytes sent over a mobile cellular network.
Mobile Bytes Received	The number of bytes received over a mobile cellular network.
Wired Bytes Sent	The number of bytes sent over a wired connection.
Wired Bytes Received	The number of bytes received over a wired connection.

Network Usage - Connections

Description	Network Usage - Connections contains information about the networks that a device connects to.
Notes	

ATTRIBUTE	DESCRIPTION
Network Name	The SSID or mobile network name.
Connection Type	Indicates the connection type (for example, WiFi or Cellular).
Cell ID/MAC Address	An identifier for the specific access point to the network, which can be either a cell tower identifier or a MAC address.
First Connected Date	The date that the device first connected to this network.
Last Connected Date	The date that the device last connected to this network.

Operating System Information

Description	This table provides information about the Windows installation.
Notes	

ATTRIBUTE	DESCRIPTION
Operating System	The operating system.
Version Number	The version number of the operating system.
Install Date/Time - UTC (yyyy-mm-dd)	The date and time that the operating system was installed.
Product Key	The product key used to license the operating system.
Owner	The owner of the operating system license.
Displayed Computer Name	The computer name that is displayed to the user of the system. This value is updated every time the system is restarted.
Computer Name	The name of the computer. This value can be can be different than the Displayed Computer Name if the user has changed their computer's name and not updated the system.

ATTRIBUTE	DESCRIPTION
DHCP DNS Server(s)	A comma separated list of the DHCP assigned DNS servers. This fragment represents the Domain Name Server(s) (DNS) provided from the DHCP service. This is stored in the registry as "DhcpNameServer".
Operating System Version	The version of the operating system.
Build Number	The build number of the operating system.
Product ID	The product ID of the operating system.
Last Service Pack	The last service pack that was installed.
Organization	The owner of the operating license organization.
Last Shutdown Date/Time - UTC (yyyy-mm-dd)	The date and time that the operating system was last shut down. In Windows, this comes from the ShutdownTime value which is found in the HKEY_LOCAL_MACHINE\SYSTEM\%ControlSet%\Control\Windows key. The software chooses the most recent date and time from the control sets as the CurrentControlSet may or may not reflect the last time the system was shut down.
System Root	The path to the system root.
Path	The path.
Last Access Time Enabled	Whether or not Last Accessed Times in NTFS are updated on this computer. If they are, this will be 'Yes', otherwise this will be 'No'.

Prefetch Files - Windows 8/10

Description	Prefetch files are used to speed up launching of frequently used executables. This table is for Windows 8 and 10.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The application that was run.
Application Path	The original path of the application that was run.
Application Run Count	The number of times the application was run. On some versions of Windows this count can be zero, while still having run date/time data.
File Created Date/Time - UTC (yyyy-mm-dd)	The date and time when prefetch file was created.
Last Run Date/Time - UTC (yyyy-mm-dd)	The last date and time that the application was run.

ATTRIBUTE	DESCRIPTION
File Hash	A hash of the file name and path, which is included in the file name for the prefetch file.
2nd Last Run Date/Time - UTC (yyyy-mm-dd)	The 2nd last date and time that the application was run.
3rd Last Run Date/Time - UTC (yyyy-mm-dd)	The 3rd last date and time that the application was run.
4th Last Run Date/Time - UTC (yyyy-mm-dd)	The 4th last date and time that the application was run.
5th Last Run Date/Time - UTC (yyyy-mm-dd)	The 5th last date and time that the application was run.
6th Last Run Date/Time - UTC (yyyy-mm-dd)	The 6th last date and time that the application was run.
7th Last Run Date/Time - UTC (yyyy-mm-dd)	The 7th last date and time that the application was run.
8th Last Run Date/Time - UTC (yyyy-mm-dd)	The 8th last date and time that the application was run.
Volume Name	The name of the first volume.
Volume Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the first volume was created.
Volume 2 Name	The name of the second volume.
Volume 2 Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the second volume was created.

Prefetch Files - Windows XP/Vista/7

Description	Prefetch files are used to speed up launching of frequently used executables. This table is for versions of Windows XP, Vista and 7.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The application that was run.
Application Path	The original path of the application that was run.
Application Run Count	The number of times the application was run. On some versions of Windows this count can be zero, while still having run date/time data.
File Created Date/Time - UTC (yyyy-mm-dd)	The date and time when prefetch file was created.

ATTRIBUTE	DESCRIPTION
Last Run Date/Time - UTC (yyyy-mm-dd)	The last date and time that the application was run.
File Hash	A hash of the file name and path, which is included in the file name for the prefetch file.
Volume Name	The name of the first volume.
Volume Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the first volume was created.
Volume 2 Name	The name of the second volume.
Volume 2 Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the second volume was created.

Recycle Bin

Description	Displays all items that were moved to the Recycle Bin.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file or folder that was deleted.
Deleted Date/Time - UTC (yyyy-mm-dd)	The local date and time the folder/file was deleted.
Security Identifier	The Security Identifier of the user who deleted the file/folder.
Original Path	The original location of the file/folder before deletion.
Type	Specifies if the deleted item was a file or folder.
Current Location	The current location/name of the file/folder in the Recycle Bin.
User	The user who deleted the file/folder, if we can retrieve it from the Security Identifier.
File Size (Bytes)	The size of the deleted file.

Remote Desktop Protocol

Description	The Remote Desktop Protocol artifact can indicate whether a device accesses external network devices, or was accessed by external network devices. The data collected by this artifact is recovered from the Windows Event Log, as well as the Windows Registry. To recover Windows Event RDP events, the Windows Event Log Artifact must be selected during the scan setup.
Notes	

ATTRIBUTE	DESCRIPTION
Event ID	The event ID from the Windows Event Log.
Created Date/Time - UTC (yyyy-mm-dd)	The Date/Time when the event was created.
Registry Key Modified Date/Time - UTC (yyyy-mm-dd)	The Date/Time when the Registry Key associated with the Remote Desktop Protocol (RDP) connection was modified.
Direction	The direction (outgoing or incoming) of the RDP connection.
Event Description Summary	The description of the event recovered.
Origin Service Name	The windows service or local account that initiated the RDP connection.
Origin Domain Name	The local domain name of the service or user that initiated the RDP connection.
Origin IP Address	The IP address of the device that initiated the RDP connection.
Origin Port	The IP Port of the device that initiated the RDP connection.
Destination User Name	The user name of the account that was remotely connected to.
Destination Domain Name	The user domain of the account that was remotely connected to.
Destination IP Address	The IP address of the device that was remotely connected to.
Destination Port	The IP Port of the device that was remotely connected to.
Event Data	The raw Windows Event Log data for the RDP connection.

Remote Desktop Protocol Bitmap Cache

Description	Remote Desktop Protocol Bitmap Cache provides a reconstruction of the RDP Bitmap Cache, which gives an indication of what may have been on screen during an RDP session.
Notes	

ATTRIBUTE	DESCRIPTION
Preview	A reconstructed image of the contents of the Remote Desktop Protocol bitmap cache. The image is produced by concatenating the individual cache bitmap tiles in the order that we find them, so the image is expected to look fragmented.

Scheduled Tasks

Description	The Scheduled Tasks artifact contains information about the scheduled tasks that are recovered from the computer. These records can be important to incident response investigations as malware often uses Scheduled Tasks to persist their content on an infected system.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The display name of the task.
Command	The path to the file used by the action that is performed by the task when it is triggered.
Author	The person who created the task.
Created Date/Time - Local Time	The local date and time of the local machine when the task was created.
Run As	The user account that the task runs as.
Last Run Date/Time - Local Time	The local date and time of the local machine when the task was last run.
Privilege Level	The privilege level that the task runs as. The options are 'LeastPrivilege' and 'HighestAvailable'
Description	A description of the purpose of the task.
Status	The status of the task at the time of recovery (can be Ready or Disabled).
Triggers	The actions that must occur for the task to perform its actions.
Actions	The actions the task will perform when it is triggered.
Run Options	The run options of the task.
Hidden	Indicates whether the task is hidden (true or false)
File	The xml markup defining the task.

Shellbags

Description	Windows Shellbags track folder access by keeping logs of the view mode of a folder. If a shellbag record exists for a path, it has been previously viewed.
Notes	

ATTRIBUTE	DESCRIPTION
Path	The path.
First Interaction Date/Time - UTC (yyyy-mm-dd)	The date and time that the folder was first interacted with.
Last Interaction Date/Time - UTC (yyyy-mm-dd)	The date and time the folder was last interacted with.
Mode	The view mode to which the path is currently set.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the entry on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed time of the entry on the filesystem.
File System Created Date/Time - UTC (yyyy-mm-dd)	The created time of the entry on the filesystem.
MFT Record Number	The MFT Record number of the folder.

Shim Cache

Description	The Shim Cache is used by Windows to track statistics about executables, such as the file path, size, and execution time (varies depending on the version of Windows). Only certain types of executable files are tracked and the data is only as recent as the last system reboot
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file.
File Path	The path to the file.
Last Run Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last accessed/explored.
Key Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the key was last updated.
File Size (Bytes)	The size of the file, in bytes.
Executed Flag	Whether or not the file is known to have been executed.

SRUM Application Resource Usage

Description	The SRUM Application Resource Usage artifact tracks information about an application's resource usage. This artifact indicates the number of CPU cycles an application uses, context switches (foreground to background), and information about I/O operations.
Notes	

ATTRIBUTE	DESCRIPTION
Entry ID	The entry ID.
Application Name	The name of the application.
Full Path	The full path to the application.
Recorded Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time the record was recorded in the database.
Security Identifier	The user ID of the account executing the application.
Foreground Cycle Time	The foreground cycle time.
Background Cycle Time	The background cycle time.
Foreground Context Switches	The number of foreground context switches.
Background Context Switches	The number of background context switches.
Foreground Bytes Read	The number of foreground bytes read.
Background Bytes Read	The number of background bytes read.
Foreground Bytes Written	The number of foreground bytes written.

ATTRIBUTE	DESCRIPTION
Background Bytes Written	The number of background bytes written.
Foreground Read Operations	The number of foreground read operations.
Background Read Operations	The number of background read operations.
Foreground Write Operations	The number of foreground write operations.
Background Write Operations	The number of background write operations.
Foreground Flushes	The number of foreground flushes.
Background Flushes	The number of background flushes.

SRUM Energy Usage

Description	The SRUM Energy Usage artifact contains information about the power expenditure for a device, as recovered from the SRUM database.
Notes	

ATTRIBUTE	DESCRIPTION
Entry ID	The entry ID.
Recorded Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time the record was recorded in the database.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time the event occurred.
State Transition	The type of state transition that occurred.
Designed Capacity	The original designed capacity of the device.
Full Charged Capacity	The actual full charged capacity of the device.
Charge Level	The current charge level of the device.
Cycle Count	The amount of power expended by the battery over the course of its life. A cycle represents the amount of power that a fully charged battery has.

SRUM Energy Usage (Long Term)

Description	The SRUM Energy Usage (Long Term) artifact contains information about the power expenditure for a device, as recovered from the SRUM database.
Notes	

ATTRIBUTE	DESCRIPTION
Entry ID	The entry ID.
Recorded Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time the record was recorded in the database.
Active AC Time	The Active AC time.
CS AC Time	The CS AC time.
Active DC Time	The Active DC time.
CS DC Time	The CS DC time.
Active Discharge Time	The Active Discharge time.
CS Discharge Time	The CS Discharge time.
Active Energy	The Active Energy amount.
CS Energy	The CS Energy amount.
Designed Capacity	The original designed capacity of the device.
Full Charged Capacity	The actual full charged capacity of the device.
Cycle Count	The amount of power expended by the battery over the course of its life. A cycle represents the amount of power that a fully charged battery has.

SRUM Network Connections

Description	The SRUM Network Connectivity artifact tracks information about the networks a device connects to and the length of time that it stays connected.
Notes	

ATTRIBUTE	DESCRIPTION
Entry ID	The entry ID.
Recorded Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time the record was recorded in the database.
Interface Type	The type of interface for the network connection.
Network Name (SSID)	The network name.
Connection Start Date/Time - UTC (yyyy-mm-dd)	The date and time a connection was made to the network.
Duration (Seconds)	The amount of time (in seconds) connected to the network.

SRUM Network Usage

Description	The SRUM Network Usage artifact contains information about the network activity for a device. This artifact can be useful in data theft investigations because it indicates the individual applications and processes that are responsible for uploading/downloading data.
Notes	

ATTRIBUTE	DESCRIPTION
Entry ID	The entry ID.
Application Name	The application name.
Full Path	The full path to the application.
Recorded Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time the record was recorded in the database.
Security Identifier	The user ID.
Interface Type	The type of interface for the network connection.
Network Name (SSID)	The network name.
Bytes Sent	The number of bytes sent.
Bytes Received	The number of bytes received.

SRUM Push Notification Data

Description	The SRUM Push Notification Data artifact contains information about Windows push notifications sent to the device.
Notes	

ATTRIBUTE	DESCRIPTION
Entry ID	The entry ID.
Recorded Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time the push notification was recorded in the database.
App ID	The application ID.
Security Identifier	The user ID.
Notification Type	The type of notification.
Payload Size	The size of the notification payload.
Network Type	The type of network.

Startup Items

Description	The configured auto-run programs for the system at startup.
Notes	

ATTRIBUTE	DESCRIPTION
Program Name	The name of the program
Path	The path to the program
Type	The type of autorun (one of 'Run', 'RunOnce', 'RunOnceEx', or 'Startup')
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the autorun was last modified

System Services

Description	The System Services artifact lists the current services that exist on the system.
Notes	

ATTRIBUTE	DESCRIPTION
Service Name	The service name.
Service Type	The service type.
Start Type	The service start type.
Service Location	The filepath to the service.
Group	The group the service belongs to.
Display Name	The service display name.
Dependencies	A list of service dependencies.
User Account	The user account to launch the service.
Description	A description of the service.
Service Details	A list of service details.
Hosted	Indicates whether the service is a hosted service (Yes or No).
Hosted Service	The hosted service.
Hosted Service Parameters	Parameters of the hosted service.
Registry Key Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the registry key that contains the startup item was last modified
Error Control	The method of error control for the service.
Tag	The tag for the service.

TeamViewer Activity

Description	TeamViewer Activity contains information about incoming and outgoing remote connections using TeamViewer remote desktop software.
Notes	

ATTRIBUTE	DESCRIPTION
Computer Name	The name of the local computer.
TeamViewer ID	The TeamViewer ID of the local computer.
Local User	The local computer user that was logged in during the connection.
Direction	The direction (incoming or outgoing) of the connection the activity was part of.
Remote Computer Name	The name of the remote computer associated with the connection.
Remote TeamViewer ID	The TeamViewer ID of the remote computer associated with the connection.
Session Type	The type of connection (remote control or file transfer).
Date/Time - UTC (yyyy-mm-dd)	The Date/Time of the activity.
Activity	The TeamViewer activity being reported.

Timezone Information

Description	The timezone information that is stored in the Windows registry.
Notes	

ATTRIBUTE	DESCRIPTION
Current Control Set	The current control set
Failure Control Set	The last control set with which the system did not boot correctly
Last Known Good Control Set	The last control set with which the system booted correctly
Current Timezone Offset (minutes)	The current timezone offset of the system, in minutes
Standard Timezone Name	The name of the standard timezone for the system
Standard Timezone Offset (minutes)	The offset of the standard timezone for the system, in minutes
Standard Timezone Start Date/Time - Local Time (yyyy-mm-dd)	The date and time at which the standard timezone of the system comes into effect
Daylight Timezone Name	The name of the daylight timezone for the system
Daylight Timezone Offset	The offset of the daylight timezone for the system, in minutes

ATTRIBUTE	DESCRIPTION
Daylight Timezone Start Date/Time - Local Time (yyyy-mm-dd)	The date and time at which the daylight timezone of the system comes into effect
Display	The name and offset of the currently active timezone, in a readable format

USB Devices

Description	A history of all USB devices that have been connected to the system.
Notes	

ATTRIBUTE	DESCRIPTION
Device Class ID	The class ID of the USB device
Serial Number	The USB device serial number
Class	The class of the device (USB, USBSTOR)
Last Connected Date/Time - UTC (yyyy-mm-dd)	The date and time the device was last connected to the computer
Device Description	The description of the device
Friendly Name	The friendly name of the device
Manufacturer	The manufacturer of the device
Last Assigned Drive Letter	The last drive letter that was assigned to the device by Windows
Volume GUID	The GUID of the volume
VSN Decimal	The volume serial number in decimal notation
VSN Hex	The volume serial number in hexadecimal notation
Associated User Accounts	Any user accounts that have used the device
First Connected Date/Time - Local Time (yyyy-mm-dd)	The date and time the device was first connected
First Connect Since Reboot Date/Time - UTC (yyyy-mm-dd)	The date and time the device was first connected since the last reboot
Install Date/Time - UTC (yyyy-mm-dd)	The date and time for each successive update of the device driver
First Install Date/Time - UTC (yyyy-mm-dd)	The date and time that specifies when the device instance was first installed in the system
Last Insertion Date/Time - UTC (yyyy-mm-dd)	The date and time the device was last inserted into the system. This value was added in Windows 8
Last Removal Date/Time - UTC (yyyy-mm-dd)	The date and time the device was last removed from the system. This value was added in Windows 8

User Accounts

Description	User accounts are pulled from the Windows registry.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The user name of the account
Full Name	The user's full name
Type of User	The type of user (either 'Domain User' or 'Built-in')
Account Description	A description of the account
Security Identifier	The security identifier of the account
User Group(s)	Any groups the user is a part of
Login Script	Any login scripts that get run when logging in as that user
Profile Path	The path to the profile folder
Last Login Date/Time - UTC (yyyy-mm-dd)	The date and time the user last logged in
Last Password Change Date/Time - UTC (yyyy-mm-dd)	The date and time the user last changed their password
Last Incorrect Password Login Date/Time - UTC (yyyy-mm-dd)	The date and time the user last entered the wrong password
Login Count	The number of times the user has logged in
Account Disabled	Indicates if the account is disabled
Password Required	Indicates if the account requires a password.
Password Hint	The user's password hint.
LM Hash	The LM hash for the local account password, if one can be recovered.
NTLM Hash	The NTLM hash for the local account password, if one can be recovered.

UserAssist

Description	The applications that are stored in the Microsoft Window's start menu.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The name of the user the UserAssist belongs to.
File Name	The name of the application that potentially executed.

ATTRIBUTE	DESCRIPTION
Application Run Count	The number of times the application has been launched from Windows Explorer or the Start menu shortcut.
Last Run Date/Time - UTC (yyyy-mm-dd)	The date and time the application was last executed.
Focus Count	The number of times application was brought in focus by the user. This fragment might be 0 for background apps.
Focus (Seconds)	The amount of time, in seconds, the app was in focus by the user. In some cases, such as when the user switches between apps, an app can still be receiving focus even if it's being displayed behind another app.

UsnJrnl

Description	The UsnJrnl artifact contains a listing of the records found in the $UsnJrnl:$J alternate data stream.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file or directory associated with this record.
Update Sequence Number	The update sequence number of this record.
Timestamp Date/Time - UTC (yyyy-mm-dd)	The standard UTC timestamp of this record.
Reason	Reasons for changes that have accumulated in this file or directory journal record since the file or directory opened.
MFT Record Number	The MFT Record number as stored in the MFT.
MFT Reference Number	The ordinal number of the file or directory for which this record applies.
Parent MFT Record Number	The parent MFT Record number as stored in the MFT.
Parent MFT Reference Number	The ordinal number of the parent directory or file for which this record applies.
File Attributes	The attributes for the file or directory associated with this record.
Source Information	Additional information about the source of the change.
Security ID	The unique security identifier assigned to the file or directory associated with this record.

Windows Defender Logs

Description	Windows Defender Logs identifies and collects any log files created by Windows Defender and Windows Security Essentials.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the log file.
File Path	The path of the log file.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the log file was created.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the log file was last accessed.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the log file was last modified.

Windows Event Logs

Description	Event logs are logs of events from any Windows application.
Notes	

ATTRIBUTE	DESCRIPTION
Event ID	The event ID
Event Type	The event type associated with the log. Event types are determined by the Event ID and, in some cases, a LoginType property indicated by the Event Data attribute. For example, an RDP event can have a number of different Event IDs, but must have a LoginType of 10.
Security Identifier	The security user ID
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the event was created
Event Description Summary	The description of the event recovered, if available.
Level	The level of error
Keywords	Event keywords
Provider Name	The name of the event provider

ATTRIBUTE	DESCRIPTION
Task category	The category the event falls under
Computer	The computer that generated the event
Event Data	Any event data

Windows Logon Banner

Description	This table contains the legal text a user must acknowledge in order to logon to the computer. This table contains legal text found in the group policy or set manually.
Notes	

ATTRIBUTE	DESCRIPTION
Legal Caption	The caption for the legal text that will be displayed to the user before they can logon to the computer.
Legal Text	The legal text being displayed to a user before they can logon to a computer.

Windows Notification Center

Description	The Windows Notification Center provides real-time notifications of events as they occur, such as received emails, calendar appointments, and more.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the notification center popup.
Subtext	The subtext of the notification center popup.
Message	The message text of the notification center popup.
Received Date/Time - UTC (yyyy-mm-dd)	The date/time when the notification was received.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date/time when the notification expires.

Windows Stored Credentials

Description	Windows Stored Credentials recover and decrypt the stored credentials for Windows Users. At this time, only non-domain users are supported.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file.
Entry ID	The name of the entry.
Description	The description of the entry.
User Name	The username of the user who is associated with the entry.
Password	The password of the entry.
Current Modified Date/Time - UTC (yyyy-mm-dd)	The modified date and time recovered from the metadata of the file.
File Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created.
File Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was modified.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last accessed on the iCloud Drive.

Windows Timeline Activity

Description	Windows Timeline Activity contains information about application usage, such as application start and end times and duration of usage.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The name of the executable reporting the timeline data.
Display Name	The title bar display text.
Content	The content the executable was displaying.
Activity Type	The activity type.
Focus (Seconds)	The number of seconds the user was engaged with the application.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time the activity started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time the activity ended.
Activity ID	The ID of the activity.
Platform	The platform related to the executable.
Created Time/Date - UTC (yyyy-mm-dd)	The date and time the entry was created.
Created In Cloud Date/Time - UTC (yyyy-mm-dd)	The date and time the activity was recorded in the cloud.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the entry was last modified.
Last Modified On Client Date/Time - UTC (yyyy-mm-dd)	The date and time the activity was last modified on the client.
Original Last Modified On Client Date/Time - UTC (yyyy-mm-dd)	The original date and time the activity was last modified on the client.

ATTRIBUTE	DESCRIPTION
Local Only	Whether or not the activity only occured locally.

Peer-to-Peer

Ares Download Folder

Description	Contains where Ares saves its downloads for each user on the system.
Notes	

ATTRIBUTE	DESCRIPTION
Download Folder	The location that Ares is saving its downloads to.

Ares Downloads

Description	Ares is a peer-to-peer file sharing application.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the media
Artist	The artist of the media.
Album	The album of the media.
Category	The category of the media.
Language	The language of the media.
Year	The year the media was created.
URL	The URL to the file.
Comment	Any comments about the file.
Downloaded Date/Time - Local Time (yyyy-mm-dd)	The local date and time of the system when the file was downloaded
Available for Download by Other Users	Whether or not other users can download this file
Corrupt	Whether or not the file is corrupt
SHA1 Hash	The SHA1 hash of the file.

Ares Incomplete Downloads

Description	Ares is a peer-to-peer file sharing application.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the media
Artist	The artist of the media.
Album	The album of the media.
Category	The category of the media.
Language	The language of the media.
Year	The year the media was created.
URL	The URL to the file.
Comment	Any comments about the file.
Keyword Genre	The genre of the media.
Subfolder	The subfolder where the file was downloaded.
Download Start Date/Time - Local Time (yyyy-mm-dd)	The local date and time of the system when the file was downloaded
SHA1 Hash	The SHA1 hash of the file.

Ares Search Keywords

Description	Ares is a peer-to-peer file sharing application
Notes	

ATTRIBUTE	DESCRIPTION
Search Keyword	The keyword that was searched for

Ares Shared Files

Description	Ares is a peer-to-peer file sharing application.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the media

ATTRIBUTE	DESCRIPTION
Artist	The artist of the media.
Album	The album of the media.
Category	The category of the media.
Language	The language of the media.
Year	The year the media was created.
URL	The URL to the file.
Comment	Any comments about the file.
File Size (Bytes)	The size of the file.
Video Info	Any information about the file if it is a video.
Corrupt	Whether or not the file is corrupt
SHA1 Hash	The SHA1 hash of the file.

Bitcoin Address

Description	Bitcoin wallet is an application that generates and stores private keys, and communicates with peers on the Bitcoin network to enable transactions.
Notes	

ATTRIBUTE	DESCRIPTION
Address	The Bitcoin address
Label	Any labels that were applied to this address by the user
Status	Whether or not the address is listed in the thread pool
Public Key	The public key
Encrypted Private Key	The encrypted private key

Bitcoin Debug Logs

Description	Bitcoin Debug Logs contain events related to bitcoin transactions performed by the user.
Notes	

ATTRIBUTE	DESCRIPTION
Event Type	The type of event that occurred in the log.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time the log event occurred.
Wallet Path	The path to the bitcoin wallet.
Transaction ID	The transaction identifier related to this event.

Bitcoin Logged Queries

Description	Bitcoin is a widely-used digital currency based on advanced encryption techniques. This search will return the Bitcoin addresses stored by the most common Bitcoin application, as well as transaction queries logged by older versions. These values are used to query Bitcoin servers for transaction history.
Notes	

ATTRIBUTE	DESCRIPTION
Query Type	The type of query on the network that was made - may or may not relate to the local user's activity
Object ID	The ID of the transaction or block that was queried
Query Date/Time - UTC (yyyy-mm-dd)	The date and time of the query

Cryptocurrency Clients

Description	Cryptocurrency Clients searches the system for known client applications that are used to transfer cryptocurrencies. Finding these applications can be helpful to investigations where cryptocurrency transactions might have been made using these applications.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name represents the name of the file that matched for known cryptocurrency clients.
Software	The name of the cryptocurrency client software.
Created Date/Time - UTC (yyyy-mm-dd)	The MAC creation time for the cryptocurrency client executable.
Accessed Date/Time - UTC (yyyy-mm-dd)	The MAC access time for the cryptocurrency client executable.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The MAC modified time for the cryptocurrency client executable.

Cryptocurrency Wallets

Description	Cryptocurrency Wallets searches the system for known cryptocurrency wallet formats. Recovering wallets can be helpful in an investigation where cryptocurrency transactions might have been made on the system and stored in the associated wallet.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file that matched for known cryptocurrency wallets.
File Type	The name of the cryptocurrency client software that created or manages the wallet.
Created Date/Time - UTC (yyyy-mm-dd)	The MAC creation time for the cryptocurrency wallet file.
Accessed Date/Time - UTC (yyyy-mm-dd)	The MAC access time for the cryptocurrency wallet file.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The MAC modified time for the cryptocurrency wallet file.

eMule Clients.met Records

Description	This search parses files used by the P2P file sharing application Emule. It will parse the following files: known.met, emfriends.met, clients.met, StoredSearches.met, sharedfiles.dat, shareddir.dat, and AC_SearchStrings.dat. Information recovered varies from file to file, but all fields available in each file format are recovered. Of particular evidential interest are the known.met, emfriends.met, StoredSearches.met, and AC_SearchStrings.dat files.
Notes	

ATTRIBUTE	DESCRIPTION
Client Hash	The hash of the client
Last Seen Date/Time - UTC (yyyy-mm-dd)	The last time the client was seen online
Uploaded Bytes	The number of bytes uploaded to that client
Downloaded Bytes	The number of bytes downloaded from that client

eMule EmFriends.met Records

Description	This search parses files used by the P2P file sharing application, Emule. It will parse the following files: known.met, emfriends.met, clients.met, StoredSearches.met, sharedfiles.dat, shareddir.dat, and AC_SearchStrings.dat. Information recovered varies from file to file, but all fields available in each file format are recovered. Of particular evidential interest are the known.met, emfriends.met, StoredSearches.met, and AC_SearchStrings.dat files.
Notes	

ATTRIBUTE	DESCRIPTION
Friend Name	The name of the friend on eMule
Last Used IP	The last IP address of that user
Last Used Port	The last port used by that user
Last Seen Date/Time - UTC (yyyy-mm-dd)	The last time the friend was seen online
Last Chatted Date/Time - UTC (yyyy-mm-dd)	The last date and time there was a conversation with the friend

eMule GUIDs

Description	This search parses files used by the P2P file sharing application, Emule. It will parse the following files: known.met, emfriends.met, clients.met, StoredSearches.met, sharedfiles.dat, shareddir.dat, and AC_SearchStrings.dat. Information recovered varies from file to file, but all fields available in each file format are recovered. Of particular evidential interest are the known.met, emfriends.met, StoredSearches.met, and AC_SearchStrings.dat files.
Notes	

ATTRIBUTE	DESCRIPTION
Network	The type of network
GUID	The GUID for the eMule Network

eMule Known.met Records

Description	This search parses files used by the P2P file sharing application, Emule. It will parse the following files: known.met, emfriends.met, clients.met, StoredSearches.met, sharedfiles.dat, shareddir.dat, and AC_SearchStrings.dat. Information recovered varies from file to file, but all fields available in each file format are recovered. Of particular evidential interest are the known.met, emfriends.met, StoredSearches.met, and AC_SearchStrings.dat files.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file on the KAD network
File Size (Bytes)	The total size of the file (in bytes)
Temp File Name	The name of the local .part file
Last Written Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last written or fully downloaded
Last Posted Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was posted or should be reposted on the KAD network
Last Shared Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last shared
Requests Total	The number of total requests from the other users in the KAD network
Requests Accepted	The number of accepted requests from other users in the KAD network
Bytes Uploaded	The number of bytes downloaded by other users in the KAD network
Upload Priority	Priority of the upload. eMule sets this value to "Auto" by default. The priorty can be changed manually by the user
Artist	The name of the artist (for media files)
Album	The name of the album (for media files)
Title	The title (for media files)
Length	The length of the media file in seconds
Bitrate	The bitrate of the media file
Codec	The codec of the media file
File Type	The type of the file, e.g. "Image", "Video", or "Doc"
File Hash	The eD2K has value of the original file

eMule Search Keywords

Description	This search parses files used by the P2P file sharing application Emule. It will parse the following files: known.met, emfriends.met, clients.met, StoredSearches.met, sharedfiles.dat, shareddir.dat, and AC_SearchStrings.dat. Information recovered varies from file to file, but all fields available in each file format are recovered. Of particular evidential interest are the known.met, emfriends.met, StoredSearches.met, and AC_SearchStrings.dat files.
Notes	

ATTRIBUTE	DESCRIPTION
Search Keyword	The keyword that was searched for

eMule Shared Files

Description	This search parses files used by the P2P file sharing application Emule. It will parse the following files: known.met, emfriends.met, clients.met, StoredSearches.met, sharedfiles.dat, shareddir.dat, and AC_SearchStrings.dat. Information recovered varies from file to file, but all fields available in each file format are recovered. Of particular evidential interest are the known.met, emfriends.met, StoredSearches.met, and AC_SearchStrings.dat files.
Notes	

ATTRIBUTE	DESCRIPTION
File	A user's file
Shared Status	Identifies whether or not the file is shared on the eMule network

eMule Shared Folders

Description	This search parses filesused by the P2P file sharing application Emule. It will parse the following files: known.met, emfriends.met, clients.met, StoredSearches.met, sharedfiles.dat, shareddir.dat, and AC_SearchStrings.dat. Information recovered varies from file to file, but all fields available in each file format are recovered. Of particular evidential interest are the known.met, emfriends.met, StoredSearches.met, and AC_SearchStrings.dat files.
Notes	

ATTRIBUTE	DESCRIPTION
Shared Folder	The name of the shared folder

eMule StoredSearches.met Records

Description	This search parses files used by the P2P file sharing application Emule. It will parse the following files: known.met, emfriends.met, clients.met, StoredSearches.met, sharedfiles.dat, shareddir.dat, and AC_SearchStrings.dat. Information recovered varies from file to file, but all fields available in each file format are recovered. Of particular evidential interest are the known.met, emfriends.met, StoredSearches.met, and AC_SearchStrings.dat files.
Notes	

ATTRIBUTE	DESCRIPTION
Search Expression	The keyword that was searched for
Special Title	An alternate title for the file

ATTRIBUTE	DESCRIPTION
Name of Matched File	The name of the file that was found
Hash of Matched File	The hash of the file that was found
File Type	The type of file that was found
File Rating	The file's rating on the eMule network

Frostwire

Description	Files and torrents downloaded with Frostwire version 5.
Notes	

ATTRIBUTE	DESCRIPTION
Torrent Name	The name of the torrent file.
Total Size (Bytes)	The total size of all files contained within the torrent.
Number of Pieces	The number of pieces needed to download the torrent (not number of files in the torrent).
Creation Date/Time - UTC (yyyy-mm-dd)	The creation date and time of the original torrent file.
Created By	The original author of the torrent file.
File Download Progress	The names of all files within the torrent along with their current download progress.
Download Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the download was started.
Download Completed Date/Time - UTC (yyyy-mm-dd)	The date and time that the download was completed.
Tracker Data	The list of ip addresses and ports connected to when downloading the torrent.

Frostwire.props Files

Description	This search finds fragments of Frostwire.props files. These files contain configuration data for the Frostwire peer to peer file sharing client and can include geo-locations, recent downloads, and many other useful items.
Notes	

ATTRIBUTE	DESCRIPTION
Fragment	The file contents

Gigatribe Chat Messages

Description	This search will recover Gigatribe chat messages saved by Gigatribe (versions 2 and 3). These logs are created when a user uses the chat feature of Gigatribe. Due to the way searches for these chat messages are performed, they can be recovered even if the log file has been deleted or a portion of the log file has been corrupted or overwritten. The chat messages can also be recovered from live memory dumps.
Notes	

ATTRIBUTE	DESCRIPTION
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent
From ID/Name	The unique ID or name for the user that sent the message
To ID/Name	The unique ID or name of the user who received the message
Message	The content of the message
Type	The visibility type of the message. Either "Private" or "Public"

Gigatribe Shared Files

Description	Gigatribe is a peer-to-peer file sharing network that allow users to download files from other users.
Notes	

ATTRIBUTE	DESCRIPTION
Filename	The name of the file being shared
File/Folder	Either "File" or "Folder"
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created
Folder Name	The name of the folder that contains the file
Folder Source	The source of the folder
Sub Directories	Whether or not the source has sub directories
Shared with group	Whether or not the source is shared with groups
Access	The file access permissions
Available from HTTP	Whether the file is available via URL or not
Folder Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the folder was created

Limerunner Shared Files

Description	Limewire is a P2P file sharing application.
Notes	

ATTRIBUTE	DESCRIPTION
Filename	The name of the file being shared
Shared	Whether or not the file is shared
Base32 Hash Value	The base32 hash of the file
SHA1 Hash Value	The SHA1 hash of the file
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time the file was modified
Additional Source	The additional source

Limewire Shared Files

Description	This search finds fragments of Limewire.props files. These files contain configuration data for the Limewire peer to peer file sharing client and can include geo-locations, recent downloads, and many other useful items.
Notes	

ATTRIBUTE	DESCRIPTION
Filename	The name of the file being shared
Shared	Whether or not the file is shared
Base32 Hash Value	The base32 hash of the file
SHA1 Hash Value	The SHA1 hash of the file
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time the file was modified
Additional Source	

Limewire v5.x Searches

Description	Search keywords left behind in live memory by Limewire. Search keywords/terms that are recovered have an associated number indicating how many search results were returned for that search term at the time the keyword was left in memory. The recovered search terms are search keywords that were entered by the local user. Other search keywords that were passed through the client ("Incoming Searches ") from other clients on the P2P network are not recovered.
Notes	

ATTRIBUTE	DESCRIPTION
Search Keyword	The keyword searched.
Search Category	The category searched, one of: All, Images, Videos, Documents, Audio, Program, or Other.
Number of Search Results	The number of search results found for the specific search keyword in the search category.

Limewire/Frostwire 4.x Searches

Description	Search keywords entered by the local user and left behind in live memory by Limewire. Search keywords that are recovered have an associated number indicating how many search results were returned for that search term at the time the keyword was left in memory. Other search keywords that were passed through the client (i.e. Incoming Searches) from other clients on the P2P network are not recovered
Notes	

ATTRIBUTE	DESCRIPTION
Search Keyword	The keyword searched
Number of Search Results	The number of search results found for the specific search keyword in the search category

Limewire.props Files

Description	This search finds fragments of Limewire.props files. These files contain configuration data for the Limewire peer to peer file sharing client and can include geo-locations, recent downloads, and many other useful items.
Notes	

ATTRIBUTE	DESCRIPTION
Fragment	The file contents

Luckywire Shared Files

Description	Luckywire is a P2P file sharing application.
Notes	

ATTRIBUTE	DESCRIPTION
Filename	The name of the file
Shared	Whether or not the file is shared
Base32 Hash Value	The base32 hash of the file
SHA1 Hash Value	The SHA1 hash of the file
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time the file was modified
Additional Source	The additional source

Shareaza GUIDs

Description	The GUIDs used by Shareaza. Shareaza is a peer-to-peer file sharing client that runs under Microsoft Windows. It supports supports the gnutella, Gnutella2 (G2), eDonkey, BitTorrent, FTP, HTTP and HTTPS network protocols.
Notes	

ATTRIBUTE	DESCRIPTION
Gnutella GUID	The GUID used for Gnutella.
Bittorrent GUID	The GUID used for Bittorrent.

Shareaza Library Files

Description	The files in the Shareaza library.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file.
Folder	The location of the file on.
Created Date/Time - UTC (yyy-mm-dd)	The date and time the file was created.
Shared	Whether the file is shared or not. This value can be explicit, or it can be inherited from a parent folder. Possible values include Yes, No, Inherited (Yes), Inherited (No), and Inherited (Unknown).
File Size (Bytes)	The size of the file in bytes.
MD5 Hash	The MD5 hash of the file.
SHA1 Hash	The SHA1 hash of the file.

ATTRIBUTE	DESCRIPTION
Hits	The number of times the file has appeared in other user's search results.
Uploads	The number of times the file has been uploaded to other users.
File Rating	The average rating of the file.
Comments	Comments left on the file by shareaza users.

Shareaza Search Keywords

Description	Shareaza is a peer-to-peer file sharing client that runs under Microsoft Windows. It supports supports the gnutella, Gnutella2 (G2), eDonkey, BitTorrent, FTP, HTTP and HTTPS network protocols.
Notes	

ATTRIBUTE	DESCRIPTION
Search Keyword	The keyword that was searched for.

Shareaza Search Results

Description	The results from a search conducted in Shareaza.
Notes	

ATTRIBUTE	DESCRIPTION
Search Keyword	The keyword that was searched for.
Name	The file name of the search result.
URL	The url to the peer serving the file.
File Size (Bytes)	The size of the file in bytes.
MD5 Hash	The MD5 hash of the file.
SHA1 Hash	The SHA1 hash of the file.

Torrent Active Transfers

Description	Information about the torrents that are active on the user's system.
Notes	

ATTRIBUTE	DESCRIPTION
Torrent Name	The name of the torrent file.
Potential App Name	The name of the application that the torrent was potentially downloaded with.
Download Start Date/Time - UTC (yyyy-mm-dd)	The date and time the torrent file download was started.
Download Completed Date/Time - UTC (yyyy-mm-dd)	The date and time the torrent file download was completed.
Download URL	The URL to download the torrent.
Downloaded Bytes	The total number of bytes that has been downloaded.
Download Location	The location on the disk to where the torrent was downloaded.
Bytes Uploaded	The total number of bytes that the system has uploaded for this torrent.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the active transfer was last modified.

Torrent Feeds

Description	Information about RSS feeds that a user subscribes to that contains torrents available for download.
Notes	

ATTRIBUTE	DESCRIPTION
Feed Name	The name of RSS subscription feed.
Feed URL	The URL of the RSS subscription feed.
Torrent Name	The name of the torrent available for download from the feed.
Download URL	The URL to download the torrent.
Description	A description of the contents of the torrent.
Published Date/Time - UTC (yyyy-mm-dd)	The date and time the torrent feed item was published.
Status	The status of the feed item, either 'Downloaded' or 'Not Downloaded'.

Torrent File Fragments

Description	Data that is carved or parsed from .torrent files that are used to download torrents from various networks on the Internet.

Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the torrent file
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the torrent file was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the torrent file was modified.
Torrent Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the torrent file was originally created.
Torrent Files	The files that are listed in the torrent to be downloaded.

Usenet Binary Files

Description	This search recovers uuencoded (ENC) encoded files that are used to transfer files on newsgroups (USENET). These files can have a wealth of header information and can be split into multiple files. Recovered files can be reconstructed in the Refined Results category in Report Viewer/AXIOM Examine. You can rebuild the files by clicking each item, or by right-clicking and selecting 'Rebuild All'.
Notes	

ATTRIBUTE	DESCRIPTION
Message ID	The message identifier of the Usenet file being downloaded
Organization	A string that describes the organization of the message sender or machine the file was on
Posted Date/Time - Local Time	The date and time the file was originally posted on the Usenet
Subject	Describes the message
Newsgroup	The list of newsgroups to which the message belongs
From	The email of the user who sent the message
Path	The path the message took to get to the local system
Keywords	Keywords that describe the message
Description	A description of the message
Original File Name	The original file name that is contained in the message
Image	The actual image
File Part	If a Usenet file is too large, it will be separated into pieces. This column will indicate which piece of the file was recovered
Original File Size (Bytes)	The size of the file
Received File Size (Bytes)	The number of bytes that have been downloaded

Refined Results

Rebuilt Desktops

Description	Rebuilt Desktops is an artifact that allows users to view an approximation of what a given Windows user's desktop looks like, including wallpapers, monitor configurations, and icon positioning, without having to virtualize the image.
Notes	This artifact is only supported for Windows 10 operating systems.

ATTRIBUTE	DESCRIPTION
User Account	The user account that the desktop belongs to.
Wallpaper Path	The path that the wallpaper/wallpapers were located at as identified by the Windows registry.
Background Type	The style of background the user has set, including single wallpaper, wallpaper slideshow, or color.
Display Configuration	Indicates whether the user had just a single screen, screens duplicated, or a screen extended across connected monitors.
Monitor Identifier	A record identifier from the Windows Registry that indicates the type of monitors that were connected for a given configuration.
Hidden Items	Indicates whether or not there are items on the desktop that have been manually hidden from view.
Preview	A preview of the rebuilt desktop image.

Social Networking

Bebo Live Chat

Description	Messages sent or received in Bebo live chat. Information found within these attributes can include the status of the message, the date/time, the sender username, target username, and the message itself.
Notes	

ATTRIBUTE	DESCRIPTION
Status	The sent status of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent
Source ID	The account of the source
Target ID	The account of the target

ATTRIBUTE	DESCRIPTION
Message	The content of the chat message

Facebook

Facebook, being one of the most popular social networking sites in the world, presents numerous opportunities for gathering evidence. You can recover messages that are sent and received, status updates and wall posts, and pages and pictures that the user views. On mobile devices, you can also recover user profiles and contacts.

Facebook can provide background information about a user, as well as evidence of who they are communicating with or associated with. Status and location updates can provide details about where a user has been and what they've been doing.

FORENSIC NOTES

The Facebook Pictures artifact represents cached pictures found on the system that originated from Facebook. When caching pictures, Facebook names the pictures using a particular format which allows forensic tools to know that they come from Facebook. These pictures can be user profile pictures, friends' pictures, or any other picture that gets cached while browsing Facebook.

ARTIFACTS

RELATED RESOURCES

How important are Facebook artifacts?

Recovering Facebook artifacts

Facebook Chat

Description	Messages sent and received using Facebook Chat.
Notes	

ATTRIBUTE	DESCRIPTION
Profile ID	The Facebook profile ID of the sender.
Message ID	The unique ID for a specific chat message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Sender ID	The Facebook ID of the sender.
Downloaded Sender Image	The profile picture of the sender, downloaded from the Internet based on the Sender ID.
Sender Name	The name of the sender.
Receiver ID(s)	The Facebook IDs of all the receivers of the message.
Downloaded Receiver Image	The profile picture of the receiver, downloaded from the Internet based on the Receiver ID.
Receiver Names(s)	The name of the receiver.
Message	The content of the chat message.
Sender Offline	The online status of the sender.

Facebook Email Snippets

Description	Snippets of email messages sent using Facebook.
Notes	

ATTRIBUTE	DESCRIPTION
Subject	The subject of the email.
Snippet	A text snippet of the body of the email.
Original Author	The author of the email.
Recent Author	The most recent author of the email.
Time Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the email was last updated.
Thread ID	The conversation ID.

Facebook Email

Description	Email messages sent using Facebook.
Notes	

ATTRIBUTE	DESCRIPTION
Logged-In User ID	The unique Facebook ID of the user that is currently logged in.

ATTRIBUTE	DESCRIPTION
Downloaded Logged-In User Image	The profile picture of the sender, downloaded from the Internet based on the Logged-In User ID
Author ID	The unique Facebook ID of the author of the email
Downloaded Author Image	The profile picture of the sender, downloaded from the Internet based on the Author ID
Author Name	The name of the author
Recipient(s)	The names of the recipients
Subject	The subject of the email
Time Rendered - Local Time (yyyy-mm-dd)	The time that was rendered in the web browser when the user viewed the email
Time Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time of when the email was last updated.
Original Author	The first author of the email.
Message	The content of the email message.
Thread ID	The unique ID that represents the email trail.
Mobile	Indicates whether this email was sent from a mobile device.
Attachments	Indicates whether this email has attachments.

Facebook Pages

Description	The content of the Facebook webpages that are cached.
Notes	

ATTRIBUTE	DESCRIPTION
Fragment	An HTML fragment of a Facebook webpage.

Facebook Status Updates/Wall Posts/Comments

Description	Information about Facebook status updates, wall posts, and comments that are cached.
Notes	

ATTRIBUTE	DESCRIPTION
Sender ID	The Facebook ID of the sender.
Downloaded Sender Image	If "Downloading Images from Web" is enabled, the sender's profile picture can be fetched using the Facebook Graph API.

ATTRIBUTE	DESCRIPTION
Sender Name	The name of the sender.
Receiver ID	The Facebook ID of the receiver.
Downloaded Receiver Image	If "Downloading Images from Web" is enabled, the receiver's profile picture can be fetched using the Facebook Graph API.
Receiver Name	The name of the receiver.
Status Update / Wall Post / Comment	The content of the status update, wall post, or comment.
Posted Date/Time - UTC (yyyy-mm-dd)	The date and time of the post.

Google+ Chat

Description	Google+ is a web-based social network that allows users to communicate publicly, share photos and videos and also message privately.
Notes	

ATTRIBUTE	DESCRIPTION
Type	Whether or not the message is a sent or received message
Email	The email address associated with the message
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent
Message	The content of the message

Instagram Pictures

Description	Instagram is a social media website where users share pictures.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Image	The profile picture of the poster
Downloaded Profile Image	The profile image of the poster, downloaded from the Internet
User ID	The user ID of the poster
User Name	The user name of the poster
Instagram Image	The picture that was posted, if found locally.
Downloaded Instagram Image	The picture that was posted, downloaded from the Internet.

Instagram Posts

Description	Instagram is a social media website where users share pictures.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Image	The profile picture of the poster
Download Profile image	The profile image of the poster, downloaded from the Internet
Text	The content of the post
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time the post was created.
User ID	The user ID of the poster
User Name	The user name of the poster
Posted Image	The picture that was posted, if found locally.
Downloaded Posted Image	The picture that was posted, downloaded from the Internet.

LINE Pictures

Description	LINE is a desktop application that allows users to exchange text messages, graphics, video and audio media, make free VoIP calls, and hold free audio or video conferences.
Notes	

ATTRIBUTE	DESCRIPTION
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date/time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date/time of the picture in the file system.

ATTRIBUTE	DESCRIPTION
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date/time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. "Complete" indicates that a full Exif extraction was performed. "Failed" indicates that the information may have been corrupted and could not be recovered. "Skipped" indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
Longitude	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the pciture was taken (extracted from Exif data).
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.

ATTRIBUTE	DESCRIPTION
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

LinkedIn Emails

Description	This search locates and carves emails that have been sent or received on LinkedIn. These email fragments can include the from/to names, subject, date/time, and full message. Please note that, depending on the browser, these emails might be compressed and are decompressed as they are viewed.
Notes	

ATTRIBUTE	DESCRIPTION
Fragment	An HTML fragment of the email

MySpace Chat - Messages

Description	Messages sent or received in MySpace live chat. Information found within these attributes can include the status of the message, the date/time, the sender ID, target ID, and the message itself. Some user info is also recoverable, such as the real name/username associated to a MySpace ID, image URL, and other information. This information is saved to a User Info report. This has been discontinued as of 2010.
Notes	

ATTRIBUTE	DESCRIPTION
Source ID	The account of the source
Target ID	The account of the target
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent
Message	The contents of the chat message
Status	The sent status of the message.

MySpace Chat - User Info

Description	MySpace is a social networking website popular with music lovers.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The MySpace user ID
UserName	The user name used on MySpace
Group	The group the user is associated to (if applicable)
Image	The user's display picture

MySpace Inbox Messages

Description	Messages sent or received in MySpace live chat. Information found within these attributes can include the status of the message, the date/time, the sender ID, target ID, and the message itself. Some user info is also recoverable, such as the real name/username associated to a MySpace ID, image URL, and other information. This information is saved to a User Info report. This has been discontinued as of 2010.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the message.
Subject	The subject of the message.
Message	The contents of the chat message.

Sina Weibo Carved Searches

Description	Sina Weibo is a Chinese microblogging (weibo) website. Akin to a hybrid of Twitter and Facebook, it is one of the most popular websites in China. This table carves for users' searches.
Notes	

ATTRIBUTE	DESCRIPTION
Search Term	The term that was searched.

Sina Weibo Microblogs

Description	Sina Weibo is a Chinese microblogging (weibo) website. Akin to a hybrid of Twitter and Facebook, it is one of the most popular websites in China. This table captures microblogging information.
Notes	

ATTRIBUTE	DESCRIPTION
Nickname	The blogger's nickname
User ID	The user ID of the blogger
Downloaded Profile Picture	The profile picture of the user, downloaded from the Internet based on the user ID
Microblog Text	The content of the blog
Posted From URL	The URL from which the blog was posted

Sina Weibo Search History

Description	Sina Weibo is a Chinese microblogging (weibo) website. Akin to a hybrid of Twitter and Facebook, it is one of the most popular websites in China. This table captures users' searches that have been parsed from the filesystem.
Notes	

ATTRIBUTE	DESCRIPTION
Search Term	The term that was searched.

Twitter

Description	Twitter is a social networking website that allows users to share status messages, known as tweets.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The full name of the user
Screen Name	The twitter handle of the user (eg. @username)
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the tweet was created
Tweet Text	The content of the tweet
In Reply To	This identifies if the tweet was a reply to another user
Status ID	The unique identifier for the tweet
Tweet Source	The type of device/application that was used to create the tweet
Geo	The geo-location of the user when they posted the tweet
Retweeted	This identifies whether the tweet was a retweet
Profile Img URL	The URL link to the profile picture of the user

VK Wall Posts

Description	The wall postings on social networking site VK.com.
Notes	

ATTRIBUTE	DESCRIPTION
Author	The author of the wall post.
Wall Text	The content of the wall text.
Message Date/Time - UTC (yyyy-mm-dd)	The date/time that the message was sent.
Message Relative Timestamp	A relative timestamp for the vk wall post.

VK Web Messages

Description	A combination of both VK instance messages and sent/received messages.
Notes	

ATTRIBUTE	DESCRIPTION
Message Sender	The sender of the message.
Message	The content of the message.
Message Date/Time - UTC (yyyy-mm-dd)	The date/time that the message was sent.
Message Relative Timestamp	A relative timestamp for the vk message.

Web Related

360 Safe Browser Archived Keyword Search Terms

Description	360 Safe Browser is a web browser developed by Qihoo.
Notes	

ATTRIBUTE	DESCRIPTION
Keyword Search Term	The keyword that was searched.
URL	The URL that was invoked because of the search.

360 Safe Browser Archived Web History

Description	Contains all of the websites the user has gone to. Along with when they last visited the site, and how often they have visited the site.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the website the user visited.
Title	The title of the website the user visited.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the user last visited the website.
Visit Count	The amount of times the user has visited the website.
Typed Count	The amount of times the user has manually types the website's URL.
ID	The 360 Safe Browser identifier of the website.

360 Safe Browser Autofill

Description	Contains all of the values that the user has saved to fill in fields at a later date and time.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the field to fill in.
Value	The value to perform the fill in with.
Count	The amount of times the autofill has been used.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill was first created.

360 Safe Browser Autofill Profiles

Description	Contains all of the profiles that are used to represent a person.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name the person goes by or uses.
Email	The email address to use to contact the person.

ATTRIBUTE	DESCRIPTION
Number	The telephone number to use to contact the person.
Company	The company the person works at.
Address Line 1	The first line of the person's address. E.g. 123 Fake Street, Fake Town, Fake Country.
Address Line 2	The second line of the person's address. E.g. Suite 123 or Apt. 123.
City	The city the person lives in.
State	The state or province the person lives in.
Zipcode	The zip code the person lives in.
Country	The country the person lives in.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time the person modified the profile.

360 Safe Browser Bookmarks

Description	Contains all of the websites the user has bookmarked.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the website.
URL	The URL of the website.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was last modified.
Is Folder	Is the bookmark a folder. Can be 'Yes', 'No' or '-Invalid-'.
Parent Folder	The parent folder of the bookmark.

360 Safe Browser Cache Records

Description	Contains all of the files and their information that has been cached by the browser.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL the file was downloaded from.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.

ATTRIBUTE	DESCRIPTION
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was first visited.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The last time the local cache was synced with the webserver.
File Type	The type of cache file.
Content Size (Bytes)	The size of the cache file.
Image	If the content file is an image, it will be displayed here.
Content	If the file is not an image, ie. A javascript file, the raw bytes will be stored here.

360 Safe Browser Cookies

Description	Contains all of the cookies saved to the browser.
Notes	

ATTRIBUTE	DESCRIPTION
Host	The host that created the cookie.
Name	The name of the cookie.
Value	The cookie value.
Accessed Date/Time - UTC(yyyy-mm-dd)	The date and time the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie was created.
Expiration Date/Time - UTC(yyyy-mm-dd)	The date and time the cookie expires.

360 Safe Browser Current Downloads

Description	Contains all of the files currently being downloaded.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file being downloaded.
Download Source	The source URL where the file was downloaded.
Saved To	The local file location.
State	The current state of the download.
Opened By User	If the downloaded file was opened by the user.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.

ATTRIBUTE	DESCRIPTION
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download finished.
Bytes Downloaded	The number of bytes download.
File Size (Bytes)	The size of the file being downloaded, in bytes.

360 Safe Browser Current Session

Description	Contains all of the sessions that are currently in use by the browser.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The web page URL.
Title	The title of the web page.
Last Visited Date/Time - (UTC)(yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.

360 Safe Browser Current Tabs

Description	Contains all of the open tabs in the browser.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The web page URL.
Title	The title of the web page.
Last Visited Date/Time - (UTC)(yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.

360 Safe Browser FavIcons

Description	Contains all of the icons that are belong to common web pages the user goes to.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	The URL of the web page.

ATTRIBUTE	DESCRIPTION
Icon URL	The URL to the icon image.
Last Updated Date/Time - UTC(yyyy-mm-dd)	The last date and time the icon was updated.
State	The current state of the download.
Opened By User	If the downloaded file was opened by the user.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download finished.
Bytes Downloaded	The number of bytes download.
File Size (Bytes)	The size of the file being downloaded, in bytes.

360 Safe Browser History Index

Description	Contains the browsing history of the user.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	The web page URL.
Title	The title of the web page.
Visited on Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Body	The HTML body of the web page.

360 Safe Browser Last Session

Description	Contains all of the sessions that were last open.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The web page URL.
Title	The title of the web page.
Last Visited Date/Time - (UTC) (yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable

360 Safe Browser Last Tabs

Description	Contains all of the tabs that were last open.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The web page URL.
Title	The title of the web page.
Last Visited Date/Time - (UTC) (yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable

360 Safe Browser Logins

Description	Contains all of the logins for web sites the user has saved.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The user name for the web page.
Password	The password for the login of the web page.
Created Date/Time - UTC (yyyy-mm-dd)	When the login information was created.
URL	The URL to the web page.

360 Safe Browser Saved Credit Cards

Description	Contains all of the credit card information the user has saved.
Notes	

ATTRIBUTE	DESCRIPTION
GUID	The identifier of the credit card.
Name On Card	The name on the credit card.
Expiry Date	The date the credit card is supposed to expire in format 'month-year'.
Card Number	The number of the credit card.

ATTRIBUTE	DESCRIPTION
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the credit card information was last modified.

360 Safe Browser Shortcuts

Description	Contains all of the shortcuts used by 360 Safe Browser for user entered URLs.
Notes	

ATTRIBUTE	DESCRIPTION
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.
Last Access Date/Time - (UTC) (yyyy-mm-dd)	The last access time of the shortcut.
Web Page Title	The title of the web page.
Times Used	The number of times the shortcut has been used.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Type	The type of shortcut (for example, 'typed url' or 'bookmark').

360 Safe Browser Top Sites

Description	Contains all of the web sites the user goes to most often.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL to the web page.
Title	The title of the web page.
Last Updated Date/Time - (UTC) (yyyy-mm-dd)	The last time the information for the top site was updated.
Thumbnail	The thumbnail of the web page.

360 Safe Browser Web History

Description	Contains all of the web sites the user has gone to.

Notes	

ATTRIBUTE	DESCRIPTION
Date Visited Date/Time - (UTC) (dd/MM/yy)	The date and time the URL was first visited.
URL	The URL that was accessed by the user.
Title	The title of the web page.
Visit Count	The number of times the user accessed the URL.
Typed Count	The number of times the user has navigated to this page by typing in the address.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Last Visited Date/Time - (UTC) (yyyy-mm-dd)	The date and time the URL was last visited.

360 Safe Browser Web Visits

Description	A history of the websites that the user visits (includes all visits).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited webpage.
Title	The title of the webpage that was visited.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Ashley Madison/Backpage Ads/Craigslist Ads/Plenty of Fish

Description	Recovered webpages from pagefile.sys.
Notes	

ATTRIBUTE	DESCRIPTION
Fragment	The fragment that was extracted.
Source	The location of where the artifact was found.
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Bing Toolbar - Map History

Description	Contains information about maps and locations that were searched for using the Bing Toolbar.
Notes	

ATTRIBUTE	DESCRIPTION
Location History	The previous location of the map
Default Location	The default location of the map.
Default lat/long	The default latitude and longitude of the default location.
Show Traffic	A True/False value of whether this feature was turned on.
Default Zoom Level	The default zoom level for the map
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Bing Toolbar - Search History

Description	Contains information about the search history for the Bing Toolbar.
Notes	

ATTRIBUTE	DESCRIPTION
Search Term	The keyword that was searched for
Search Date/Time - UTC (yyyy-mm-dd)	The date and time the keyword search was conducted.
Source	The location of where the artifact was found

ATTRIBUTE	DESCRIPTION
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Chrome

Google Chrome is free web browser developed by Google and is available on all major operating systems, for both mobile and desktop. As of 2016, Chrome usage represents over 70% of the world's total browser traffic.

Analyzing the websites a user visits and the time the visits occur can provide valuable insights about a user. One notable feature that Google Chrome has is that it allows users to sync their bookmarks, browsing history, and more across multiple platforms and devices by using cloud sync accounts.

FORENSIC NOTES

Web Visits vs Web History

Chrome has two distinct artifacts that are very similar nature: Chrome Web Visits and Chrome Web History. Both of these artifacts are recovered from the History database. Chrome Web History is parsed from the URLS table and only contains information for the last visited date of a particular website. Chrome Web Visits can contain multiple entries for the same website, giving the examiner a more complete look at browser usage if the user visited a website multiple times. For example, if a user visits www.magnetforensics.com six times, the Chrome Web History artifact displays only the last time the site is visited, while the Chrome Web Visits artifact potentially displays records for all six instances. Chrome Web Visits was added in a later version of Chrome than Chrome Web History.

Carved web history

The Chrome / 360 Safe Browser / Opera Carved Web History is essentially the same as Chrome Web History except that it's recovered using carving and you may find additional deleted hits with it. The 360 Safe and Opera browsers are included in this artifact because when the data is carved, it's not possible to tell which browser the hit comes from as they're all formatted the same way.

Autofill and profile data

Chrome stores field data that the user has previously input as autofill and profile settings. For example, if you visit magnetforensics.com and login to the customer portal, browsers automatically save your username (and other details) so that you don't have to type it in each time you visit the site. This data is helpful for recovering usernames and other information that your user has filled out on various sites.

Sessions and tabs

When the system has an active session available, Chrome stores the browsing activity as the Chrome Current Session and any tabs that are open as Chrome Current tabs. The previous session and tabs are maintained in Chrome Last Session and Chrome Last Tabs so that the user can restore the last session and tabs if Chrome is closed.

ARTIFACTS

RELATED RESOURCES

How does Chrome's 'incognito' mode affect digital forensics?

Forensic email analysis: browser artifacts you may find on a PC or laptop

Chrome Archived Keyword Search Terms

Description	Keyword search terms that were archived by the browser.
Notes	

ATTRIBUTE	DESCRIPTION
Keyword Search Term	The keyword search term the user entered.
URL	The URL of the keyword search.

Chrome Archived Web History

Description	An archived history of old webpage visits.

Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL where the archived web history is located.
Title	The title of the archived web history.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was visited.
Visit Count	Total visits to this URL.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
ID	ID for the web history archive.

Chrome Autofill Profiles

Description	Profiles that Chrome uses to fill in forms with saved values.
Notes	

ATTRIBUTE	DESCRIPTION
Name	Name for the autofill profile.
Email	Email used in the the autofill profile.
Number	Phone number used in the autofill profile.
Company	Company name used in the autofill profile.
Address Line 1	Address Line 1 used in the autofill profile.
Address Line 2	Address Line 2 used in the autofill profile.
City	City used in the autofill profile.
State	State used in the autofill profile.
Zipcode	Zipcode used in the autofill profile.
Country	Country used in the autofill profile.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the profile was last modified.

Chrome Autofill

Description	Chrome Autofill contains records of the autofill values that Chrome saves for different types of text fields.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the autofill value.
Value	The saved autofill value for this type of field.
Count	Count of this autofill.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill was last used.

Chrome Bookmarks

Description	Browser bookmarks that reference saved webpages.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was added.
Parent	The name of the parent folder of the bookmark.

Chrome Cache Records

Description	Content that Chrome downloads and caches to speed up rendering times. Cached content can include pictures, text, html, javascript, and more.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the cached item.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was first visited.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The date and time the cache was last synced with the cloud.
File Type	The type of file that was cached.
Content Size (Bytes)	The size of the cached file.
Image	The cached image if the file type is an image. Otherwise, this column is empty.
Content	The cached file contents if the file type is not an image. Otherwise, this column is empty.

Chrome Cookies

Description	Cookies that Chrome downloads from the Internet that contain information about the websites that a user visits.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie expires.
Path	The path of the cookie value.

Chrome Current Session

Description	Information about the browser session that's currently underway.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL.
Title	The title of the web page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Chrome Current Tabs

Description	Information about the tabs that are open in the current browser session.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL.
Title	The title of the web page.

ATTRIBUTE	DESCRIPTION
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.

Chrome Downloads

Description	Information about the files that a user downloads from the Internet.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	File name of the download.
Download Source	The URL of the file that was downloaded.
Saved To	Saved to location.
State	State of the download.
Opened By User	If the download is opened by the user.
Start Time Date/Time - UTC (yyyy-mm-dd)	Download start time.
End Time Date/Time - UTC (yyyy-mm-dd)	Download end time.
Bytes Downloaded	The bytes that were downloaded.
File Size(Bytes)	File size of the download.

Chrome Extensions

Description	Information about the extensions a user has installed on their Computer
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	Name of the Chrome plugin/extension
Version	Version number of the plugin/extension
Description	Description of the plugin/extension
Install Date/Time - UTC (yyyy-mm-dd)	Install time in Chrome/Webkit time
State	State of the plugin/extension on the google account (i.e enabled, disabled)
Installed by OEM	States whether the plugin/extension is installed by OEM (true or false)
Installed by Default	States whether the plugin/extension is installed by Default (true or false)
From Bookmark	States whether the plugin/extension was installed from a bookmark (true or false)

ATTRIBUTE	DESCRIPTION
From Webstore	States whether the plugin/extension was installed from the chrome webstore (true or false)
Author	The author.
Homepage	The homepage.

Chrome FavIcons

Description	Contains the favicons that Chrome displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	Page URL of the favicon.
Icon URL	Icon URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	Last time the favicon was updated.
Icon	A preview of the favicon.

Chrome History Index

Description	An index of the webpages the user has visited in the past.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	The URL of the webpage.
Title	The title of the webpage.
Visited On Date/Time - UTC (yyyy-mm-dd)	When the webpage was visited.
Body	A snippet of the webpage.

Chrome Keyword Search Terms

Description	Information about the keyword search terms that a user enters.
Notes	

ATTRIBUTE	DESCRIPTION
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.

Chrome Last Session

Description	Information about the previous browser session.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL.
Title	The title of the web page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Chrome Last Tabs

Description	Information about the tabs that were open during the previous session.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The web page URL.
Title	The title of the web page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Chrome Logins

Description	Login information that a user provides in Chrome. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the login page.
Username	The username entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the data was created.

Chrome Saved Credit Cards

Description	Chrome Saved Credit Cards contains information about the credit cards that a user has saved to their device.
Notes	

ATTRIBUTE	DESCRIPTION
Name On Card	The name of the person on the credit card.
Card Number	The number on the credit card.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the information was last modified.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time the credit card autofill information was last used.
GUID	An ID for the credit card.
Expiry Date	The date the credit card is supposed to expire in format 'month-year'.

Chrome Shortcuts

Description	Contains all of the shortcuts used by Google Chrome for user entered URLs.
Notes	

ATTRIBUTE	DESCRIPTION
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.
Last Access Date/Time - UTC (yyyy-mm-dd)	The last access time of the shortcut.
Web Page Title	The title of the web page.
Times Used	The number of times the shortcut has been used.

ATTRIBUTE	DESCRIPTION
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Type	The type of shortcut (for example, 'typed url' or 'bookmark').

Chrome Sync Accounts

Description	Chrome Sync Accounts contains information about the Chrome accounts that a user has logged in with. Chrome syncs data to the cloud so that a user can log in on multiple devices.
Notes	

ATTRIBUTE	DESCRIPTION
Sync Id	The unique id for the account that's used to sync data to the cloud.
Account Name	The name of the sync account.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the sync account was locally created.

Chrome Sync Data

Description	Chrome Sync Data contains information about the data that Chrome has synced to a user's account in the cloud.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the sync key.
Local Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the value on the local system.
Server Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the value on the server.
Local Created Date/Time - UTC (yyyy-mm-dd)	The created time of the value on the local system.
Server Created Date/Time - UTC (yyyy-mm-dd)	The created time of the value on the server.
Type	The type of data that is synced (bookmark, favicon, type URL, and so on).
Parsed Content	The type parsed data.
Favicon Image	The actual favicon image.

Chrome Top Sites

Description	A list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Notes	

ATTRIBUTE	DESCRIPTION
URL	URL of the site.
Title	Title of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the site was last updated.
Rank	A ranking of the website, in terms of how frequently it was visited. A value of 1 indicates the most frequent and values increment to 8 as frequency decreases. A value of -1 indicates a site that the user manually added to the list of top sites.
Thumbnail	Thumbnail of the site

Chrome Web History

Description	A history of the websites that the user visits (includes unique visits only).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

Chrome Web Visits

Description	A history of the websites that the user visits (includes all visits).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited webpage.
Title	The title of the webpage that was visited.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Edge Cache Data

Description	Information about cache data that was saved during browsing.
Notes	This artifact allows an investigator to see the content a user views, it's origin, and how often the content is reused by the browser. By clearing the cache, the user can effectively delete these records. In some cases, records do not get deleted from the database, but in cases where the files are deleted, the original files cannot be restored.

ATTRIBUTE	DESCRIPTION
Entry ID	The entry ID.
URL	The URL of the cache data source.
Creation Date/Time - UTC (yyyy-mm-dd)	Date and Time when cache data was saved on the machine.
Last Modified Date/Time - UTC (yyyy-mm-dd)	Date and Time when cache data was modified on the source side.
File Type	The file type.
Visit Count	Indicates the number of times the current cache file was accessed.
Content Size (Bytes)	Cache file size in bytes.
Image	The content of the file as an image, if the file is a supported image type.
File	The content of the file in raw bytes.
Original Path	Original absolute path to the cache file stored in the database.
Relative Path	A relative path to the file based on the location of the WebCache database, or [Doesn't exist] if the file is not found.

Edge Extensions

Description	Information about the extensions/plugins installed in the user's Edge browser

Notes	

ATTRIBUTE	DESCRIPTION
Package Name	The Package name for the extension
Application Name	The name of the extension
Version Number	The most recent version number of the extension
Created Date/Time - UTC (yyyy-mm-dd)	The time when this extension was created
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The most recent time the AppxManifest file for the extension was accessed (most likely the same as created time)
Last Modified Date/Time - UTC (yyyy-mm-dd)	The most recent time when the extension was updated

Edge Favorites

Description	Edge Favorites contains information about the websites a user favorites while browsing.
Notes	This artifact allows an investigator to see the content a user views, it's origin, and how often the content is reused by the browser. By clearing the cache, the user can effectively delete these records. In some cases, records do not get deleted from the database, but in cases where the files are deleted, the original files cannot be restored.

ATTRIBUTE	DESCRIPTION
Favorite Name	The name given to the favorite.
Is Folder	Indicates whether the item is a folder or a URL for a website (Yes if the item is a folder, and No if the item is a URL).
URL	The URL of the favorite.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the favorite was last modified.
Favicon URL	The URL of the favicon for the website.

Edge Last Session

Description	Information about the last snapshot Edge took of the user's browsing session.
Notes	At certain time intervals, Edge takes a snapshot of the user's browsing session. Using this artifact, an investigator is able to see exactly what the user was looking at, at the time of snapshot. The time interval between snapshots is unknown. Due to the interval, it's possible for a tab to be opened and closed quick enough that the tab isn't included in a snapshot.

ATTRIBUTE	DESCRIPTION
Page URL	The URL of the web page.
Page Title	The title of the web page.
Image	The browser generated snapshot of the page.
Body	The HTML body that was saved from the page.

Edge Reading Lists

Description	Edge Reading Lists contains collections of websites that the user has saved for offline viewing.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the Reading List page.
URL	The URL of the Reading List page.
Source Address	Other source information for the Reading List page.
Picture Path	A file path to pictures associated with the Reading List page.
Deleted	Indicates whether the user has deleted the Reading List page.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time the Reading List page was added.
Last Access Date/Time - UTC (yyyy-mm-dd)	The date and time the Reading List page was last accessed.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the Reading List page was updated.

Edge Top Sites

Description	Edge Top Sites lists the websites that the user visits frequently in the Edge browser. Top Sites can also be removed or added by the user.
Notes	

ATTRIBUTE	DESCRIPTION
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the page was added as a Top Site.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the Top Site was updated.
Favicon URL	The URL of the favicon for the Top Site.
Title	The title of the Top Site.
URL	The URL of the Top Site.

Edge/Internet Explorer 10-11 Content

Description	Content that the browser caches, including web pages, pictures and other resources.
Notes	

ATTRIBUTE	DESCRIPTION
Entry ID	The entry ID.
URL	The URL of the cache record.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The most recent visit to the URL.
Last Modified by Web Server Date/Time - UTC (yyyy-mm-dd)	The last time the content was modified on the web server. This time is reflective of when the website created the content on the page and can be before the system being examined was built.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the content was created on the local system.
Access Count	The number of times the content was accessed through the web browser.
Filename	The filename of the cached content.
File Size (Bytes)	The size of the cache file.
Image	If the content is an image, it will be displayed here.
Content	If the file is not an image, i.e. a javascript file, the raw bytes will be stored here.

Edge/Internet Explorer 10-11 Cookies

Description	Site usage information that websites send to the browser when a user visits their sites.
Notes	

ATTRIBUTE	DESCRIPTION
Entry ID	The entry ID.
User	The local user on the system.
URL	The URL that the cookie is for.
Accessed Date/Time - UTC (yyyy-mm-dd)	The most recent visit to the URL.
Updated Date/Time - UTC (yyyy-mm-dd)	The last date and time the cookie was updated by the website at the URL visited.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie was created.
Access Count	The number of times the cookie was accessed.

ATTRIBUTE	DESCRIPTION
Filename	The filename of the cookie.
File Size (Bytes)	The size of the cookie.

Edge/Internet Explorer 10-11 Daily/Weekly History

Description	Websites that a user visits using Internet Explorer, which are recovered from the Daily/Weekly history.
Notes	At the end of the week, all the daily .dat records are bundled into a weekly history and a new daily .dat file is created. This table represents a good secondary source for evidence if the main history is missing details or records.

ATTRIBUTE	DESCRIPTION
Entry ID	The entry ID.
URL	The URL that was accessed by the user.
User	The local user on the system.
Accessed Date/Time - Local (yyyy-mm-dd)	The most recent visit to the URL.
Access Count	The number of times the website was accessed.
Browser Source	The directory of the browser from where the history is extracted from.

Edge/Internet Explorer 10-11 Dependency Entries

Description	A history of the websites that the browser is required to load in order to render a page.
Notes	Records for this artifact are similar to the main history, the difference being that this artifact also includes dependencies for viewed websites (for example, if a viewed website contains pictures stored on another website).

ATTRIBUTE	DESCRIPTION
Entry ID	The entry ID.
URL	The URL visited by the user.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The most recent visit to the URL.

Edge/Internet Explorer 10-11 Downloads

Description	Information about the files a user downloads using the browser.
Notes	Internet Explorer 9 introduced a new integrated download manager which stores the details of downloaded files in a new download INDEX.DAT file. This file has a different structure to the standard INDEX.DAT files.

ATTRIBUTE	DESCRIPTION
Entry ID	The entry ID.
URL	The URL of the file download.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last time the user accessed the download URL.
Redirect URL	The previous URL that led the user to the download URL.
Download Location	The local path where the file was saved.
Temporary Download Location	The local path where the file was saved temporarily (usually while downloading).

Edge/Internet Explorer 10-11 Main History

Description	Records of the websites that a user visits using Internet Explorer, which are recovered from the main history.
Notes	The access count does not always accurately represent the real access count. These values should only be used as an estimate.

ATTRIBUTE	DESCRIPTION
Entry ID	The entry ID.
URL	The URL that was accessed by the user.
User	The local user on the system.
Accessed Date/Time - UTC (yyyy-mm-dd)	The most recent visit to the URL.
Page Title	The title of the webpage.
Access Count	The number of times the website was accessed.
Browser Source	The directory of the browser from where the history is extracted from.

Firefox Add-ons

Description	Contains the add-ons from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the add-on.
Version	The version the add-on.
Installed Date/Time - UTC (yyyy-mm-dd)	The date/time when the add-on was installed.
Updated Date/Time - UTC (yyyy-mm-dd)	The date/time when the add-on was updated.
Extension Enabled	Whether the add-on is enabled by the user.
Description	The description of the add-on.

Firefox Bookmarks

Description	Contains the bookmarks from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the website that was bookmarked.
Date Added Date/Time - UTC (yyyy-MM-dd)	The Date/Time the bookmark was created.
Last Modified Date/Time - UTC (yyyy-MM-dd)	The Date/Time the field was last modified.
Title	The title of the bookmark.
Bookmark Type	The type of bookmark, can be either 'Bookmark Item' or 'Bookmark Folder'.

Firefox Cache Records

Description	Contains all of the cached entries in the Firefox Cache Map.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the cache entry.

ATTRIBUTE	DESCRIPTION
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cache entry was created.
MIME Type	The MIME type of the cache data.
Content Size (Bytes)	The content size of the cached data.
Image	The image, should one be associated with the cache entry.
Content	The content, should any be associated with the cache entry.

Firefox Cookies

Description	Contains the cookies from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
Host	The host domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-MM-dd)	The Date/Time the cookie was last accessed.
Created Date/Time - UTC (yyyy-MM-dd)	The Date/Time the cookie was created.
Expiration Date/Time - UTC (yyyy-MM-dd)	The Date/Time the cookie will expire, if it is set to expire.
Path	The path to the cookie.

Firefox Downloads

Description	Contains the downloads from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file being downloaded.
Download Source	The URL of the file being downloaded.
Start Date/Time - UTC (yyyy-MM-dd)	The Date/Time the download was started.
End Date/Time - UTC (yyyy-MM-dd)	The Date/Time the download was ended.
Saved To	The path to where the file was downloaded to.
Temp Path	The path to where the file was saved during downloading.

ATTRIBUTE	DESCRIPTION
State	The state of the download can be 'Download In Progress', 'Download Complete', 'Download Stopped', or 'Download Paused'.
Referrer	If the web page used a mirror for downloading, the path to the original download URL.

Firefox FavIcons

Description	Contains the fav icons from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the icon.

Firefox FormHistory

Description	Contains the form history from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
Field Name	The name of the field.
Value	The value of the field.
First Used Date/Time - UTC (yyyy-MM-dd)	The Date/Time the field was first used.
Last Used Date/Time - UTC (yyyy-MM-dd)	The Date/Time the field was last used.
Times Used	The number of times the field has been used.
ID	The unique ID of the field.

Firefox Input History

Description	Contains the input to forms from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL the input was given to.
Input	The value that was given.

ATTRIBUTE	DESCRIPTION
Use Count	The number of times the input has been used.
ID	The unique ID of the input.

Firefox Logins

Description	Firefox Logins contains login information for websites that a user logs in to using the browser.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the login page.
Username	The username entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the data was created.

Firefox Private Browsing History

Description	Contains the URLs that were loaded during a Private Browsing session from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL.

Firefox SessionStore Artifacts

Description	Contains the web pages from the last active session from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the web page.
URL	The URL of the web page.
Referrer URL	The URL of the web page, if the web page was a redirect.

Firefox Web History

Description	Contains the web pages from the last active session from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the web page.
Last Visited Date/Time - UTC (yyyy-MM-dd)	The Date/Time the web page was last visited.
Title	The title of the web page.
Visit Count	The number of times the web page has been visited.
Is Typed	Did the user type the URL, can be 'Yes' or 'No'.

Firefox Web Visits

Description	Contains all of the non-archived URL visits for Firefox.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL that was visited.
Title	The title of the page that was visited.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the page was visited.
Is Typed	Did the user type the URL, can be 'Yes' or 'No'.
Transition Type	How the transition to the page happened.

Flash Cookies

Description	Flash cookies are Internet browser cookies that are saved when a user watches a flash video (e.g. Youtube)
Notes	

ATTRIBUTE	DESCRIPTION
Cookie Name	The name of the cookie

ATTRIBUTE	DESCRIPTION
Content	The flash content of the cookie. This content is essentially serialized ActionScript code. Primitive values such as integers and strings are shown, as well as more complicated data structures such as objects and arrays. A complex data structure's value is shown only once, along with an "object ID" that gets generated. For all subsequent references to that structure in the content, it's referred to by the generated object ID.
Domain	The domain/host that created the cookie
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Google Analytics First Visit Cookies

Description	Information about Google Analytics first-visit cookies that are discovered in other artifacts.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the URL.
Creation DateTime	Date/Time when the site was vist visited.
Most Recent Visit Date/Time	Date/Time of most recent session.
2nd Most Recent Visit Date/Time	Date/Time of previous session.
Hits	Number of visit.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Google Analytics First Visit Cookies Carved

Description	Information about Google Analytics first-visit cookies that are recovered using carving.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the URL.
Creation DateTime	Date/Time when the cookie was created.
Most Recent Visit Date/Time	Date/Time of most recent session.
2nd Most Recent Visit Date/Time	Date/Time of previous session.

ATTRIBUTE	DESCRIPTION
Hits	Number of visit.

Google Analytics Referral Cookies

Description	Information about Google Analytics referral cookies that are discovered in other artifacts.
Notes	

ATTRIBUTE	DESCRIPTION
Cookie Source	The source URL used to reach the site.
Host	Contains the domain of the URL.
Update Date/Time	The last time the cookie was updated.
Campaign	The method of referral.
Access Method	Whether the site was accessed organically or was referred.
Keyword	Keywords used to arrive at the site.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Google Analytics Referral Cookies Carved

Description	Information about Google Analytics referral cookies that are recovered using carving.
Notes	

ATTRIBUTE	DESCRIPTION
Cookie Source	The source URL used to reach the site.
Host	Contains the domain of the URL.
Update Date/Time	The last time the cookie was updated.
Campaign	The method of referral.
Access Method	Whether the site was accessed organically or was referred.
Keyword	Keywords used to arrive at the site.

Google Analytics Session Cookies

Description	Information about Google Analytics session cookies that are discovered in other artifacts.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the URL.
Page Views	The number of visits to this page from the user.
Start Current Session Date/Time	The start time of the current sesion.
Outbound Link Events Left	
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Google Analytics Session Cookies Carved

Description	Information about Google Analytics session cookies that are recovered using carving.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the URL.
Page Views	The number of visits to this page from the user.
Start Current Session Date/Time	The start Date/Time of the current sesion.
Outbound Link Events Left	

Google Analytics URLs

Description	URLs that are discovered in other artifacts that are related to Google Analytics.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the web site. If the url cannot be recovered, the source of the url containing all the metadata is displayed instead.
Page Title	The name of the web site. This value is carved from the source starting after 'utmdt=' and ending at '&'
Host Name	Contains the domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'
Artifact	The name of the artifact that the URL was discovered in.

ATTRIBUTE	DESCRIPTION
Artifact ID	The row ID of the URL in the original artifact table.

Google Analytics URLs Carved

Description	Information about Google Analytics URLs that are recovered using carving.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the web site. If the url cannot be recovered, the source of the url containing all the metadata is displayed instead.
Page Title	The name of the web site. This value is carved from the source starting after 'utmdt=' and ending at '&'
Host Name	Contains the domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'

Google Maps

Description	Google Maps is a free web service that allows users to get directions.
Notes	

ATTRIBUTE	DESCRIPTION
Search Query	The term that was searched for
Starting Location	The starting location for navigation/directions.
Center of Map	Where the map was centered
Business Latitude and Longitude	The latitude and longitude of the business location.
Source Address	The source physical address.
Destination Address	The user's desired destination
Route Type	How the user will travel (eg. Car, bus, bike)
Additional Address	Any additional addresses within the navigation
Street View Latitude/Longitude	The latitude and longitude information in street view.

Google Maps Tiles

Description	Google maps is a free web service that allows users to get directions.
Notes	

ATTRIBUTE	DESCRIPTION
Image	The actual picture content.
X Coordinate	The X coordinate value that Google uses to download the right tile.
Y Coordinate	The Y coordinate value that Google uses to download the right tile.
Zoom Level	The level that the user was zoomed in to the map. Can be understood as the Z coordinate value that Google uses to download the right tile.

Google Toolbar

Description	The Google toolbar is a browser add-on where a user can perform Google searches. While there are many different features to the Google Toolbar, search history is the focus. Search history can be either typed or done by autocomplete. It's also possible to determine where the user's search comes from, whether it is Google Search, YouTube, Google Maps, Google News, etc.
Notes	

ATTRIBUTE	DESCRIPTION
Search	The keyword that was searched for
Category	The category the search was conducted in (pictures, web, etc.)

Internet Explorer Cache Records

Description	Temporary Internet files that are written locally when the user views pages from the Internet.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the cache record.
User	The local user.
Last Modified by Web Server Date/Time - UTC (yyyy-mm-dd)	The last time the content was modified on the web server. This time is reflective of when the website created the content on the page and can be before the system being examined was built.

ATTRIBUTE	DESCRIPTION
Last Checked by Local Host Date/Time - UTC (yyyy-mm-dd)	The date and time the content was checked for recency on the local system.
Cache Retrieval Count	The number of times the cache record was requested by the browser.
Filename	The name of the file.
File Type	The filename of the cached content.
Content Size (Bytes)	The size of the cache file.
Image	If the content file is an image, it will be displayed here.
Content	If the file is not an image, ie. A javascript file, the raw bytes will be stored here.

Internet Explorer Cookie Records

Description	Site usage information that websites send to the browser when a user visits their sites.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL that created the cookie.
User	The user of the system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last date and time the URL was accessed.
Last Modified by Web Server Date/Time - UTC (yyyy-mm-dd)	The last date and time the URL record was modified.
Visit Count	The number of times the URL was visited.
Web Page Title	The title of the webpage.
File Name	The name of the cookie file.

Internet Explorer Cookies

Description	Site usage information that websites send to the browser when a user visits their sites.
Notes	

ATTRIBUTE	DESCRIPTION
Host	The host that created the cookie.
Name	The name of the cookie.
Value	The cookie value.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie was created.

ATTRIBUTE	DESCRIPTION
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie expires.
Flags	The flags associated with the cookie.

Internet Explorer Downloads

Description	Information about the files a user downloads using the browser.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL for the file download.
Date/Time - UTC (yyyy-mm-dd)	The date and time the file was downloaded.
Status	The download status.
Saved To	The local path where the file was saved.
Referrer URL	The previous URL that led the user to the download URL.
File Size (Bytes)	The size of the file in bytes.
Source IP	The IP address of the download URL.

Internet Explorer Favorites

Description	Web pages that the user has set as a favorite.
Notes	

ATTRIBUTE	DESCRIPTION
Favorite Name	The name of the favorite as it shows up in Internet Explorer.
URL	The URL of the favorite.
Modified Date/Time - UTC (yyyy-mm-dd)	The last time the user modified the favorite.
User	The user to whom the favourite belongs.
Favorites Root Location	The local path that is the root storage point for the favorite.
Folder Structure	The folder structure under which the favorite will show up in Internet Explorer.
Icon URL	The url of the icon for the favorite if an icon does exist.

Internet Explorer InPrivate/Recovery URLs

Description	URLs visited during InPrivate browsing that are saved in Internet Explorer recovery files (used to recover tabs in the event of a crash).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL that was visited.
File Create Date/Time - UTC (yyyy-mm-dd)	The date and time that the Internet record was created.
Description	The title of the website.
Local MAC address	The MAC address of the local machine.

Internet Explorer Leak Records

Description	Browser history records that are scheduled for deletion.
Notes	LEAK artifacts are created when an error occurs while the system attempts to delete a record and the Temporary Internet File is unavailable for some reason.

ATTRIBUTE	DESCRIPTION
URL	The URL visited.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time the URL record was modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last date and time the URL was accessed.
Visit Count	The number of times the URL was visited.

Internet Explorer Main History

Description	Websites that a user visits using Internet Explorer, which are recovered from the main history.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL that was visited.
User	The local user.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Last visited (2nd Timestamp) Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.

ATTRIBUTE	DESCRIPTION
Visit Count	The number of times the user accessed the URL.
Web Page Title	The webpage title.

Internet Explorer PrivacIE Records

Description	Websites that a user visits while having the privacy settings turned on.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL visited.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time the URL record was modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last date and time the URL was accessed.
Visit Count	The number of times the URL was visited.

Internet Explorer Typed URLs

Description	URLs that the user types directly into the address bar for Internet Explorer.
Notes	This includes data that a user pastes into the address bar, as well as instances when a user starts typing in the address bar and clicks on a suggestion from the browser. You may also see local paths and network locations here when the user types a location in Windows Explorer.

ATTRIBUTE	DESCRIPTION
URL	The URL that was typed into the address bar.
Last Entered Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last typed.

Internet Explorer Weekly History

Description	Websites that a user visits using Internet Explorer, which are recovered from the weekly history.
Notes	At the end of the week, all the daily .dat records are bundled into a weekly history and a new daily .dat file is created. This table represents a good secondary source for evidence if the main history is missing details or records.

ATTRIBUTE	DESCRIPTION
URL	The URL that was visited.
User	The local user.
Last Visited Date/Time (local time) (yyyy-mm-dd)	The date and time the URL was last visited. This date is local to the machine that visited the website.
Weekly History File Created Date/Time - UTC (yyyy-mm-dd)	The date and time the weekly history file was created.
Visit Count	The number of times the user accessed the URL.
Web Page Title	The webpage title.

IP Addresses - Audio/Video Calls

Description	IP Addresses of web audio/video calls that show who a user was communicating with. Each instance of this artifact represents a single hop in the communication chain. By showing the relationship between multiple hops, you can determine where a call originated from and what the final destination was.
Notes	

ATTRIBUTE	DESCRIPTION
Call ID	The ID of the call.
Message ID	The ID of the message.
Domain	The domain used for the call.
Connection Type	The type of connection.
Origin IP Address	The originating IP address for this hop in the call.
Origin Port	The originating port for this hop in the call.
Destination IP Address	The destination IP address for this hop in the call.
Destination Port	The destination port address for this hop in the call.
Date/Time - UTC (yyyy-mm-dd)	The timestamp associated with this hop in the call.
Remote User ID	Unique ID of the remote user.
Communication Protocol	The communication protocol for this call (either UDP or TCP).
Metadata	Additional details about the call.

Malware/Phishing URLs

Description	Records that are believed to be either malware or phishing related URLs.
Notes	

ATTRIBUTE	DESCRIPTION
Site Name	The name of the web site.
URL	The URL of the web site.
Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the artifact.
Artifact	The name of the artifact the URL belongs to.
Artifact ID	The row Id of the URL in the original artifact table.

Opera Archived Keyword Search Terms

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
Keyword Search Term	The keyword that was searched
URL	The URL that was invoked by the search

Opera Archived Web History

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was first visited
URL	The URL that was accessed by the user
Title	The title of the web page
Visit Count	The number of times the user accessed the URL
Typed Count	The number of times the user has navigated to this page by typing in the address
Transition Type	Describes how the browser navigated to a particular URL on a particular visit. For example, if a user visits a page by clicking a link on another page, the transition type is "Link".
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited

Opera Autofill Profiles

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the user
Email	The user's email
Number	The user's phone number
Company	The user's company
Address Line 1	The user's address
Address Line 2	The user's address
City	The user's city
State	The user's state
Zipcode	The user's zip code
Country	The user's country
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill profile was last modified

Opera Bookmarks

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the bookmark
URL	The URL that was bookmarked
Added Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was added
Parent	The parent bookmarks folder (if applicable)
Type	The type of bookmark

Opera Cache Records

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL the file was downloaded from
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was first visited
Last Sync Date/Time - UTC (yyyy-mm-dd)	The last time the local cache was synced with the webserver
File Type	The type of cache file
Content Size (Bytes)	The size of the cache file
Image	If the content file is an image, it will be displayed here
Content	If the file is not an image, e.g. a javascript file, the raw bytes will be stored here

Opera Cookies

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
Host	The host that created the cookie
Name	The name of the cookie
Value	The cookie value
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie was last accessed
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie was created
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie expires
Path	The path to the cookie

Opera Current Session

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL
Title	The title of the webpage
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited
Visit Count	The number of times the user accessed the URL
Redirect URL	The URL to use to redirect, if applicable

Opera Current Tabs

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL
Title	The title of the webpage
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited
Visit Count	The number of times the user accessed the URL
Redirect URL	The URL to use to redirect, if applicable

Opera Downloads

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file being downloaded
Download Source	The source URL where the file was downloaded

ATTRIBUTE	DESCRIPTION
Saved To	The local file location
State	The current state of the download
Opened By User	If the downloaded file was opened by the user
Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started
End Date/Time - UTC (yyyy-mm-dd)	The date and time when the download finished
Bytes Downloaded	The number of bytes downloaded
File Size (Bytes)	The total file size in bytes

Opera History Index

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	The webpage URL
Title	The title of the webpage
Visited On Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited
Body	The HTML body of the webpage

Opera Last Session

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL
Title	The title of the webpage
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited
Visit Count	The number of times the user accessed the URL
Redirect URL	The URL to use to redirect, if applicable

Opera Last Tabs

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL
Title	The title of the webpage
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited
Visit Count	The number of times the user accessed the URL
Redirect URL	The URL used to redirect, if applicable

Opera Logins

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL the autofill was extracted from
User Name	The user name to be auto-populated
Password	The password that was remembered
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill was saved

Opera Saved Credit Cards

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
GUID	A unique identifier for the credit card
Name On Card	The name on the credit card

ATTRIBUTE	DESCRIPTION
Expiry Date	The date the credit card is supposed to expire in format 'month-year'.
Card Number	The credit card number
Date Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time the credit card information was modified

Opera Search Field History

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
Search Entries	The term that was searched for

Opera Shortcuts

Description	Contains all of the shortcuts used by Opera for user entered URLs.
Notes	

ATTRIBUTE	DESCRIPTION
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.
Last Access Date/Time - (UTC) (yyyy-mm-dd)	The last access time of the shortcut.
Web Page Title	The title of the web page.
Times Used	The number of times the shortcut has been used.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Type	The type of shortcut (for example, 'typed url' or 'bookmark').

Opera Top Sites

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL
Title	The title of the webpage
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last date and time the top site was updated
Thumbnail	A thumbnail of the webpage

Opera Typed History

Description	Opera is a web browser developed by Opera Software. Web history are recently visited web pages. Opera stores a user's browsing history so that he or she can view it later. This search carves and parses web history from the Opera web browser, including the typed history (i.e. URLs or search terms entered by the user). The entire history file is not required; single records can be carved from live RAM captures and unallocated clusters, and so on.
Notes	

ATTRIBUTE	DESCRIPTION
Last Typed Date/Time - UTC (yyyy-mm-dd)	The last date and time the content was typed
Typed URL/Data	The content that was typed. Could be a URL or other data
Type	The type of content that was typed, e.g. URL

Opera Web History

Description	Opera is a web browser developed by Opera Software. Web history are recently visited web pages. Opera stores a user's browsing history so that he or she can view it later. This search carves and parses web history from the Opera web browser, including the typed history (i.e. URLs or search terms entered by the user). The entire history file is not required; single records can be carved from live RAM captures and unallocated clusters, and so on.
Notes	

ATTRIBUTE	DESCRIPTION
Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the user visited the website
URL	The URL accessed
Title	The webpage title
Visit Count	The amount of times the user has gone to the website.
Typed Count	The amount of times the user has typed out the website.

Pornography URLs

Description	Records that are believed to be pornography related URLs.
Notes	For a list of the URLs that are targeted by this artifact, see Pornography domains.

ATTRIBUTE	DESCRIPTION
Site Name	The name of the web site.
URL	The URL of the web site.
Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the artifact.
Artifact	The name of the artifact the URL belongs to.
Artifact ID	The row Id of the URL in the original artifact table.

Rebuilt Webpages

Description	Contains the data that allows for the reconstruction of web pages.
Notes	

ATTRIBUTE	DESCRIPTION
Page Title	The title.
URL	The URL.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the original record was created.
Domain	The domain.
Cache Table	The table the data to re-construct the page came from.
Cache RowID	The row id in the table that constructed the rebuilt web page.

Safari Bookmarks

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures information related to webpages that have been bookmarked.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The name of the bookmark.
URL	The URL that was bookmarked.

Safari Cache Records

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures information related to webpages that have been cached on the local system.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL from which the file was downloaded.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cache file was created.
File Type	The type of the cached file.
Content Size	The size of the cached file.
Image	If the content file is an image, it will be displayed in this column.
Content	If the file is not an image (e.g. if it is a javascript file), the raw file content will be stored here.

Safari Downloads

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures information related to files that have been downloaded from Safari.
Notes	

ATTRIBUTE	DESCRIPTION
Download URL	The URL of the downloaded file.
Saved to Path	The local path where the download was saved.
Download Identifier	The unique identifier for the download.
Amount Downloaded (Bytes)	The number of bytes downloaded.
Size of Download (Bytes)	The size of the download in bytes.

Safari History

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures history entries which have been parsed from the filesystem.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of a visited web page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Redirect URL	The URL the user was redirected to.
Title	The title of the web page.
Visit Count	The number of times the URL was visited.
Visit Source	Whether the website was viewed on the local device or on a synced device.

Safari iCloud Devices

Description	Safari iCloud Devices contains information about the devices that are synced to an iCloud account. Each device can access any browser tabs that are synced to the account.
Notes	

ATTRIBUTE	DESCRIPTION
Unique Device Identifier	A unique ID for the device that is accessing the tab.
Device Name	The name of the device that is linked to the iCloud account.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the device first synced to the iCloud account.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the device last synced with the iCloud account.

Safari iCloud Tabs

Description	Safari iCloud Tabs contains information about tabs that have been opened in the browser and synced to an iCloud account. Synchronized tabs are available to any device that logs in to the iCloud account.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the tab.
URL	The URL address of the tab.
Unique Device Identifier	A unique ID for the device that is accessing the tab.
Device Name	The name of the device that is accessing the tab.
Tab ID	The unique ID of the tab.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the tab was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the tab was last modified.
Modified By	The name of the device that last modified the tab.
Close Requested	Indicates whether a close request has been opened for the tab.
Close Request Date/Time - UTC (yyyy-mm-dd)	The date and time when the close request was created.

Safari Last Session

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures information related to the user's last session with Safari.
Notes	

ATTRIBUTE	DESCRIPTION
Tab URL	The webpage URL.
Tab Title	The title of the webpage.

Safari Top Sites

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures information related to the user's top sites
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL.
Title	The title of the webpage.
Feed Last Update Time	The date and time that the top site content was last updated.
Feed URL	The URL of the RSS feed.

WebKit Browser Session/Tabs (Carved)

Description	WebKit Browser Sessions/Tabs contains information about the browser sessions and tabs that the user has open, while using a browser built with WebKit. Some examples of browsers that use WebKit are Chrome, Opera, and 360 Safe Browser. This artifact consolidates the existing Chrome, Safe Browser, and Opera equivalents in a single artifact. Usage of other browsers, such as Firefox and Safari, aren't likely to appear under this artifact.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The web page URL.
Title	The title of the web page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

WebKit Browser Web History (Carved)

Description	WebKit Browser Web History contains information about the websites that a user visits while using a browser built with WebKit. Some examples of browsers that use WebKit are Chrome, Opera, and 360 Safe Browser. This artifact consolidates the existing Chrome, Safe Browser, and Opera equivalents in a single artifact. Usage of other browsers aren't likely to appear under this artifact, however, some URLs found by other browsers may also be found by this artifact.
Notes	

ATTRIBUTE	DESCRIPTION
URL	URL of the visited webpage.
Title	Title of the visited webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time this webpage was last visited
Visit Count	The number of times the webpage was visited.

ATTRIBUTE	DESCRIPTION
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

XBox 360 Internet Explorer Cache Records

Description	Internet explorer is a Windows-based desktop application for browsing the internet. All Windows computers are pre-loaded with this web-browser as the default internet browser.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the cache record
User	The local user
Last Modified by Web Server Date/Time - UTC (yyyy-mm-dd)	The last time the content was modified on the web server. This time is reflective of when the website created the content on the page and can be before the system being examined was built.
Last Checked by Local Host Date/Time - UTC (yyyy-mm-dd)	The date and time the content was checked for recency on the local system.
Cache Retrieval Count	The number of times the item was retrieved from the cache.
Filename	The name of the file.
File Type	The filename of the cached content.
Content Size (Bytes)	The size of the cache file.
Image	If the content file is an image, it will be displayed here.
Content	If the file is not an image, ie. A javascript file, the raw bytes will be stored here.

XBox 360 Internet Explorer Daily History

Description	Internet explorer is a Windows-based desktop application for browsing the Internet. All Windows computers are pre-loaded with this web-browser as the default Internet browser.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL that was visited
User	The local user
Last Visited Date/Time (local time) (yyyy-mm-dd)	The local Date and Time the URL was last visited

ATTRIBUTE	DESCRIPTION
Last Visited Date/Time - (UTC) (yyyy-mm-dd)	The Date and Time the URL was last visited
Visit Count	The number of times the URL was visted
Web Page Title	The webpage title

XBox 360 Internet Explorer Favorites/Recent/Featured Items

Description	Internet explorer is a Windows-based desktop application for browsing the Internet. All Windows computers are pre-loaded with this web-browser as the default Internet browser.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the item
Display Name	The name of the item

XBox 360 Internet Explorer Weekly History

Description	Internet explorer is a Windows-based desktop application for browsing the Internet. All Windows computers are pre-loaded with this web-browser as the default Internet browser.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL that was visited
User	The local user
Last Visited Date/Time (local time) (yyyy-mm-dd)	The local Date and Time the URL was last visited
Weekly History File Created Date/Time - UTC (yyyy-mm-dd)	The Date and Time the weekly history file was created
Visit Count	The number of times the URL was visted
Web Page Title	The webpage title

XBox Internet Explorer Main History

Description	Internet explorer is a Windows-based desktop application for browsing the Internet. All Windows computers are pre-loaded with this web-browser as the default Internet browser.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL that was visited
User	The local user
Last Visited Date/Time - (UTC) (yyyy-mm-dd)	The Date and Time the URL was last visited
Last Visited (2nd Timestamp) Date/Time - (UTC) (yyyy-mm-dd)	The Date and Time the URL was last visited
Visit Count	The number of times the URL was visted
Web Page Title	The webpage title

ANDROID

Advanced Search Tools

Dynamic Application Finder

Description	
Notes	

ATTRIBUTE	DESCRIPTION

Chat

AIM Buddies

Description	Contains the AIM buddies that were recovered from an Android device.
Notes	

ATTRIBUTE	DESCRIPTION
User AIM ID	The AIM ID of the local user.
Buddy Name	The name of the buddy.
Buddy Display ID	The display ID of the buddy.
Buddy AIM ID	The AIM ID of the buddy.
Buddy Icon URL	The URL of the buddy's icon.
Buddy Group	Identifies if the row is a buddy or group chat. The possible values are Buddies or groupcht.
Group Chat ID	The ID of the group chat, if applicable.

AIM Messages

Description	Contains the AIM messages that were recovered from and Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The AIM ID of the sender of the message
Receiver	The AIM ID of the user receiving the message or the group chat ID if in a chat.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the message.
Message	The message that was sent/received.
Latitude	The latitude of the message sender.
Longitude	The longitude of the message sender.

Android Burner Conversations

Description	Android Burner Conversations contains the Burner conversations that were recovered from an Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Burner Number	The Burner number on the device that is a part of the conversation.
Conversation Partner	The phone number of the other person in the conversation.
Message	The last message of the conversation.
Account Number	The Burner ID on the device that is a part of the conversation.
Conversation Date/Time - UTC (yyyy-mm-dd)	The date and time of the last message in the conversation.
Conversation Name	The name of the conversation.
Type	The type of the last interaction in the conversation. The possible values are Outgoing Text Message, Incoming Text Message, Incoming Phone Call, Missed Incoming Phone Call, Outgoing Phone Call, and Incoming Voice Mail.
Voice Mail URI	The URI to the voice mail, if applicable.

Android Burner Numbers

Description	Android Burner Numbers contains the Burner numbers that were recovered from an Android device.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The ID of the user's Burner account.
Burner ID	The ID of the Burner number.
Burner Number	The phone number that was generated by Burner.
Updated Date/Time - UTC (yyyy-mm-dd)	The last date and time when the Burner number was updated.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the Burner number was generated.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the Burner number will expire.
About	Information about the Burner number.

Android Google Hangouts Messages

Description	Android Google Hangouts Messages contains the messages from Google Hangouts from an Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Message	The body of the message.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the message.
Message Type	The type of the message. The message type value can be 'Sent Message', 'Received Message', 'Participant joined/left the Hangout', 'Video Chat Started', 'Video Chat Ended', 'History Turned Off', 'History Turned On', 'Participant left the Hangout', or 'Participant joined the Hangout'.
Sender Phone ID	The identifier of the device for who sent the message.
Sender Full Name	The full name of the sender who sent the message.
Sender Fall-back Name	The name of the sender, if they don't have a full name.
Sender Profile Photo URL	The URL to the profile photo of the sender of the message.
Recipient Phone ID	The identifier of the recipient of the message.
Recipient Full Name	The full name of the recipient of the message.

ATTRIBUTE	DESCRIPTION
Recipient Fallback Name	The name of the recipient, if they don't have a full name.
Recipient Profile Photo URL	The URL to the profile photo of the recipient of the message.
Remote Attachment URL	The URL to the attachment of a message.
Attachment Type	The type of the attachment.
Latitude	The latitude of the message. It has not been determined whether this is the sender of the message, the recipient of the message, or just where the device received the message.
Longitude	The longitude of the message. It has not been determined whether this is the sender of the message, the recipient of the message, or just where the device received the message.
Location URL	The URL to a location on Google maps of the image.
Location Thumbnail URL	The URL to a thumbnail picture of the location of the message on Google Maps.

Android Kik Messenger Attachments

Description	Android Kik Messenger Attachments contains the attachments of messages from Kik Messenger from an Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Media ID	The ID of the attachment.
Attachment	The attachment.
File Metadata	Any metadata from the file.

Android Kik Messenger Contacts

Description	Android Kik Messenger Contacts contains information about a user's Kik Messenger contacts.
Notes	

ATTRIBUTE	DESCRIPTION
Contact ID	The ID of the contact.
Display Name	The display name of the contact.
Local Name	The local name of the person on the device.
User Name	The username of the contact.
Photo URL	The URL to the profile photo of the contact.
Photo Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp of the contact's profile photo.
Group Member	Indicates whether the contact is a member of a group (Yes or No).
Blocked	Indicates whether the contact is blocked by the local user.

Android Kik Messenger Messages

Description	Android Kik Messenger Messages contains Kik Messenger messages that were sent or received by the local user.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local user of the device where the data was recovered from.
Partner	The person the local user sent a message to or received a message from.
Message Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp of the message.
Message Body	The body of the message.
Message Status	The status of the message. The possible values are Trying to establish connection, Message has been sent to recipient, Message has been delivered to recipient, Message has been read by recipient and Unknown message status.
Message Type	The type of the message. The possible values are Message Received, Message Sent and Unknown Message Type.
Media ID	The ID of the attachment.
Media Info	The description of the attached media.
Attachment	The attachment sent with the message.

Android Messages

Description	SMS/MMS messages sent and received using Android Messages.

Notes	

ATTRIBUTE	DESCRIPTION
Sender	The name of the sender or the phone number if the name is not available.
Phone Number	The phone number of the sender.
Message Sent Date/Time	The date and time when the message was sent.
Message Received Date/Time	The date and time when the message was received.
Message	The content of the message.
Recipient	The recipient of the message.
Message Status	The read status of the message.
Message Type	The message type. An example of message type is Text/plain.
Message Direction	Indicates whether the message was sent by or recieved on the local user's device.
Message ID	The ID used within the database to store the order in which messages come in.
Attachment Path	The path of an attachment.
Attachment Data Recovered	Indicates whether attachment data was recovered (Yes or No).
Subject	The optional subject line provided for an MMS message.
Target File Size (Bytes)	The size of attachments.
Longitude	The longitude associated with a location message.
Latitude	The latitude associated with a location message.
Avatar Path	The path to the contact icon used for the sender.

Android Messages SIM Card Information

Description	Android SIM Card Information is information about the device's SIM card that is recoverable if the user has the Android Messages application installed on the device.
Notes	

ATTRIBUTE	DESCRIPTION
ICCID	The ICCID (Integrated Circuit Card Identifier) is a serial number stored in the SIM card.
Service Provider Name	The name of the mobile service provider.
Phone Number	The phone number associated with the SIM card.
IMSI	The IMSI (International Mobile Subscriber Identity) is a unique number identifying a GSM (Global System for Mobile Communications) subscriber.

Android MMS

Description	MMS messages sent or received using an Android device. These messages are recovered from mmssms.db.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The phone number of the device that sent the message.
Recipient(s)	The phone numbers of the devices that received the message.
Message Direction	Indicates whether the message was incoming or outgoing. If the direction is not recognized, the value will be an integer.
Original Transmit Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was first sent from the sender.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent (only for outgoing messages).
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was received (only for incoming messages).
Message	The message body of the MMS message.
Attachments	The file names of all recovered attachments.
Attachment Data Recovered	Indicates whether attachment data was recovered (Yes, No, or Partial).

Android MMS (UFED Agent)

Description	Android MMS (UFED Agent) contains MMS messages sent or received using the Messages app on Android. These messages are recovered from <mms_messages> tags found in a UFED Report.xml
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local user of the device where the data was recovered from.
Partner Name	The name of the person who communicated with the local user. This data is retrieved from the <to> or <from> tags within mms_message elements in a UFED Report.xml.
Partner Phone Number	The phone number of the person who communicated with the local user. This data is retrieved from the <to> or <from> tags within mms_message elements in a UFED Report.xml.

ATTRIBUTE	DESCRIPTION
Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the message, though it is unclear whether this represents the sent or received time. This data is retrieved from the <timestamp> tag within mms_message elements in a UFED Report.xml.
Subject	The subject of the message. This data is retrieved from the <subject> tag within mms_message elements in a UFED Report.xml.
Message	The body of the message, excluding any attachments. This data is retrieved from the <body> tag within mms_message elements in a UFED Report.xml.
Message Direction	The direction of the message relative to the Local User. This data is retrieved from the <to> or <from> tags within mms_message elements in a UFED Report.xml.
Message Status	The status of the message. This data is retrieved from <status> tag within mms_message elements in a UFED Report.xml. However, if the value in the <folder> tag is Draft, this attribute will indicate Draft.
Priority	The priority of the message. This data is retrieved from <priority> tags within mms_message elements in a UFED Report.xml.
Attachment Name(s)	The attachment file name. This data is recovered from the <attachments> tag within mms_message elements in a UFED Report.xml.

Android SMS

Description	SMS messages sent using the Messages app on Android.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local user of the device where the data was recovered from.
Partner	An identifier for the person who communicated with the local user.
Received Date/Time-(UTC)(dd/MM/yyyy)	The time the message is recieved.
Sent Date/Time-(UTC)(dd/MM/yyyy)	The time the message is sent.
Original Transmit Date/Time-(UTC)(dd/MM/yyyy)	Original transmit timestamp
Message	The message body of the SMS message.
Message Direction	Indicates whether the message was incoming or outgoing.
Application	The application from which the message was sent.

Android SMS (UFED Agent)

Description	Android SMS (UFED Agent) contains SMS messages sent or received using the Messages app on Android. These messages are recovered from <sms_messages> tags found in a UFED Report.xml.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local user of the device where the data was recovered from.
Parnter Name	The name of the person who communicated with the local user. This data is retrieved from the <name> tag within sms_message elements in a UFED Report.xml.
Partner Phone Number	The phone number of the person who communicated with the local user. This data is retrieved from the <number> tag within sms_message elements in a UFED Report.xml.
Message Date/Time - UTC (yyyy-mm-dd)	A date and time associated with the message, though it is unclear whether this represents the sent or received time. This data is retrieved from the <timestamp> tag within the sms_message elements in a UFED Report.xml.
Message	The message content for the message. This data is retrieved from the <text> tag within sms_message elements in a UFED Report.xml.
Message Direction	The direction of the message (either incoming or outgoing). This data is retrieved from the <type> tag within sms_message elements in a UFED Report.xml.
Message Status	The status of the message. Values can be Read, Unread, or Sent. This data is retrieved from the <status> tag within sms_message elements in the UFED Report.xml.
SMSC	The Short Message Service Center (SMSC) associated with the message. This data is retrieved from the <smsc> tag within sms_message elements in a UFED Report.xml.

Android SMS/MMS (Content Provider)

Description	SMS/MMS messages sent or received using an Android device. Data for this artifact is recovered during the acquisition process using an Android Content Provider.
Notes	

ATTRIBUTE	DESCRIPTION
Participants	The phone numbers of the people in the conversation.
Original Transmit Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was first sent from the sender.
Message	The message body of the MMS message.
Message Status	The status of the message.

ATTRIBUTE	DESCRIPTION
MIME Type	The MIME type for the attachment.
Attachment	The recovered attachment.

Android SMS/MMS (Google Play Services)

Description	SMS and MMS messages sent or received using an Android device. These messages are recovered from icing_mmssms.db.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local user of the device where the data was recovered from.
Partner	An identifier for the person who communicated with the local user.
Sent Date/Time-(UTC) (dd/MM/yyyy)	The time the message is sent.
Received Date/Time-(UTC) (dd/MM/yyyy)	The time the message is received.
Message	The message body of the SMS message.
Message Type	The type of message. Possible values are MMS and SMS.
Message Direction	Indicates whether the message was incoming, outgoing, draft, sent, outbox, failed, or queued.
Message Status	The status of the message (Read or Unread).

Android Telegram Chats

Description	Information about the conversations that the suspect participates in using the Telegram application.
Notes	This table doesn't contain any of the actual text from the conversations that occur. However, the table does contain some useful metadata about group chats such as the RSA ID.

ATTRIBUTE	DESCRIPTION
Chat ID	The ID of the chat.
Chat Type	The type of the chat.
Chat Name	The name of the chat.
Unread Count	The number of unread messages.
Last Message ID	The ID of the last message in the chat.

ATTRIBUTE	DESCRIPTION
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the last message in the chat.
User ID	The ID of the other user in the chat.
RSA Key	The RSA key of the chat, if it is encrypted.
RSA Key Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the RSA key was created.

Android Telegram Contacts

Description	Information about a subject's contacts that are displayed in Telegram. The application pulls the list of potential contacts from Android Contacts, meaning that these users may or may not be Telegram users.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The ID of the user.
First Name	The user's first name.
Last Name	The user's last name.
Phone Number	The phone number associated with the user's account.
Second Phone Number	The second phone number associated with the user's account. If there is no second phone associated with the account, this value is the same as the above Phone column.
Deleted	Whether the suspect marked the user's information for deletion.

Android Telegram Messages

Description	Individual chat messages that are sent and received using the Telegram application.
Notes	

ATTRIBUTE	DESCRIPTION
Partner	The name of the conversation partner. In case the name is not available, it displays 'Chat Type:id', where the ID is the telegram ID of the partner (or conversation ID)
Chat Type	The type of chat that the message belongs to.
Direction	The direction of the message.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the message was created on the local device.

ATTRIBUTE	DESCRIPTION
Message Body	The body of the message.
Action	The action that occurred.
Type	The type of the message that was sent or received.
Call Duration (Seconds)	The duration of the call.
Latitude	The latitude of a location message.
Longitude	The longitude of a location message.
Local Media Path	The path to the content of the media file on the local phone.

Android Telegram Users

Description	Information about the users that a subject has interacted with using Telegram.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The ID of the user.
First Name	The user's first name.
Last Name	The user's last name.
User Name	The user's user name.
Phone Number	The phone number associated with the user's account.
Last Seen Date/Time	The date and time of the user's last seen.
Bot Account	Indicates whether the user is a bot account.
Added Contact	Indicates whether the subject has added the user as a contact.
Deleted	Indicates whether the contact was deleted by the subject.
Mutual Contact	Indicates whether the subject has a mutual contact with the user.
Self Contact	Indicates whether the contact is the subject's own user account.
Verified	Indicates whether the user has verified their account.

Android TextNow Calls

Description	Android TextNow Calls contains information about calls and voicemails that are sent and received through the TextNow application.
Notes	If the Contact Name cannot be determined, the Local Contact Key may be used to locate the corresponding entry in the iOS TextNow Contacts artifact.

ATTRIBUTE	DESCRIPTION
Call Type	The type of call or voicemail.
Direction	Whether the call was incoming or outgoing.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the call or voicemail.
Duration (Seconds)	The duration of the call.
Contact ID	The ID of the other call participant.
Contact Type	The other participant's contact type.
Conversation Partner	The name of the other call participant.
Voicemail URL	The URL of the voicemail.
Message Status	The status of the message ('Read' or 'Unread').
Attachment Path	The voicemail attachment path.

Android TextNow Chat

Description	Android TextNow Chat contains chat messages that are sent and received through the TextNow application.
Notes	If the Contact Name cannot be determined, the Local Contact Key may be used to locate the corresponding entry in the iOS TextNow Contacts artifact.

ATTRIBUTE	DESCRIPTION
Message	The body of the message.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the message.
Contact ID	The ID of the other message participant.
Contact Type	The other participant's contact type.
Message Partner	The phone number or username of the other participant.
Message Type	The type of message.
Message Direction	Whether the message was incoming or outgoing.
Group Name	The group name, if the message was sent to a group chat.
Message Status	The status of the message ('Read' or 'Unread').
Attachment Path	The attachment path.

Android TextNow Contacts

Description	Android TextNow Contacts contains the application, phone, email and group contacts that a user has in the TextNow application.
Notes	

ATTRIBUTE	DESCRIPTION
Contact ID	The name of the contact.
Contact Type	The contact's type.
Contact Name	The display name contact.

Android TextNow Groups

Description	Android TextNow Groups contains membership information for TextNow group chats.
Notes	

ATTRIBUTE	DESCRIPTION
Contact ID	The ID for the group.
Group	The name of the group.
Member Name	The username of a group member.
Type	The group member's contact type.
Display Name	The display name of the group member.
Contact Uri	The Android resource URI of the group member.

Android TextNow Profile

Description	Android TextNow Profile contains TextNow user profiles and application preference settings.
Notes	

ATTRIBUTE	DESCRIPTION
First Name	The first name of the TextNow user.
Last Name	The last name of the TextNow user.
Email	The email of the TextNow user.
User Name	The username of the TextNow user.
Phone Number	The phone number of the TextNow user.
Signature	The signature automatically appended to the end of each TextNow message sent by the user.
Last Number Called	The last number called using the TextNow application by the user.
TextNow Credit	The TextNow credit held by the user.
Balance	The TextNow cash balance held by the user.

Android TigerText Messages

Description	Android TigerText Messages contains messages from the TigerText Android application.
Notes	

ATTRIBUTE	DESCRIPTION
Message Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message Expiry Date/Time - UTC (yyyy-mm-dd)	The date and time that the message will expire.
Message Recalled	Whether the message was recalled. This value is 'True' for recalled, and 'False' for not recalled.
Attachment Type	The file type of the attachment (if any).
Attachment	Attachment data.
Message Text	The text content of the message.
Message Status	The status of the message (sent, delivered or read).
Sender First Name	The first name of the message sender.
Sender Last Name	The last name of the message sender.
Sender Display Name	The display name of the message sender.
Sender Phone Number	The phone number of the message sender.
Sender Email	The email address of the message sender.
Recipient First Name	The first name of the message recipient.
Recipient Last Name	The last name of the message recipient.
Recipient Display Name	The display name of the message recipient.
Recipient Phone Number	The phone number of the message recipient.
Recipient Email	The email address of the message recipient.

Android Tinder Accounts

Description	Android Tinder Accounts contains all of the recovered Android Tinder Accounts.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user ID of current account owner.
Biography	A brief written biography about the users account.
Birthday (yyyy-mm-dd)	The birthday of the account user.

ATTRIBUTE	DESCRIPTION
Distance (Miles)	The distance that the user is searching for matches.
Gender	The gender of the account user.
Name	The name of the account user.
Last Activity Date/Time - Local Time (dd/MM/yyyy)	The last date and time that the account user was active.

Android Tinder Matches

Description	Android Tinder Matches contains all of the recovered Android Tinder Matches.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user ID of the user whom you are matched with.
User Name	The name of the user whom you are matched with.
Gender	The gender of the matched user.
Created Date/Time	The creation date of the match entry in UTC.
Last Activity Date/Time	The last time that there was activity with the match in UTC.
Created Date/Time - Local Time (dd/MM/yyyy)	The creation date of the match entry.
Last Activity Date/Time - Local Time (dd/MM/yyyy)	The last time that there was activity with the match.
Message Count	The number of messages that were exchanged with the matched profile.
Viewed Profile	Whether or not the user has viewed the profile.
Draft Message	The contents of a pending draft message.

Android Tinder Messages

Description	Android Tinder Messages contains all of the recovered Android Tinder Messages.
Notes	

ATTRIBUTE	DESCRIPTION
Sender ID	The user ID of the user whom is part of this conversation and is sending.
Recipient ID	The user ID of the user whom is part of this conversation and is receiving.
Match ID	The ID of the match who the message is received from.

ATTRIBUTE	DESCRIPTION
Message Sent Date/Time - Local Time (dd/MM/yyyy)	The local date and time when the message was sent.
Message Sent Date/Time	The date and time when the message was sent in UTC.
Message Body	The body of the message.

Android Tinder Photos

Description	Android Tinder Photos contains all of the recovered Android Tinder Photos.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user ID of the user whom the picture belongs to.
User Name	The name of the user whom this picture belongs to.
Image URL	The URL to the Tinder photo.
Downloaded Image	The downloaded image.

BlackBerry Messenger Contacts

Description	Contains the BBM Contacts recovered from an Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Display Name	Contains the contacts display name.
BlackBerry PIN	Contains the contacts BlackBerry PIN.
Personal Message	Contains the contacts personal message.
Personal Message Last Update Date/Time - UTC (yyyy-mm-dd)	The data and time the contacts personal message was updated.
Avatar	The contacts avatar.
Avatar Content Type	The avatar content type. An example is 'image/jpeg'
Location	The contacts location.
Timezone	The contacts timezone.

BlackBerry Messenger File Transfers

Description	Contains the BBM File Transfers recovered from an Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Transfer Direction	Indicates whether a file was sent or received.
Transfer State	Indicates whether a file transfer is 'Pending Approval' or 'Complete'.
Display Name	Display name of the contact who the transfer is with.
BlackBerry PIN	BlackBerry PIN of the contact who the transfer is with.
Local File Path	The path on the device to the data transferred.
Content Type	The type of data that was transferred.
Transfer Description	Description of what is being transferred.
Attachment	The file that was transferred.
Total Transfer Size (Bytes)	The number of bytes the transferred file is.
Bytes Transferred	The number of bytes that were transferred.
Transfer Date/Time - UTC (yyyy-mm-dd)	The date and time the transfer took place.

BlackBerry Messenger Invitations

Description	BlackBerry Messenger Invitations contains BBM invite requests recovered from an Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Direction	This column states if the invite is a received invite or a sent invite.
Display Name	The display name of the user sending the invite request.
BlackBerry PIN	The BlackBerry PIN of the user sending the invite request.
Remote Email Address	
Local Email Address	
Invitation Status	Contains the status of the invite request. The value can be Pending Approval or Unknown.
Invite Method	The method used for sending the invite request. The value can be Via PIN or Unknown.
Subject	The subject used for the invite request.
Greeting	The message sent with the invite request.

ATTRIBUTE	DESCRIPTION
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date/time when the invite was sent/received.

BlackBerry Messenger Locations

Description	BlackBerry Messenger Locations contains BBM locations recovered from an Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Message Type	Indicates whether the message was sent or received.
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date/time when the location was sent/received.
Display Name	The display name of the location sender.
BlackBerry PIN	The BlackBerry PIN of the location sender.
Location Name	The name of the location
Latitude	The latitude of the location
Longitude	The longitude of the location
Altitude (meters)	
Accuracy (meters)	
Street	The street address of the location.
City	The city of the location.
State/Province	The state/province of the location.
Country	The country of the location.
ZIP/Postal Code	The postal code/ZIP of the location.

BlackBerry Messenger Messages

Description	Contains the BBM messages recovered from an Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Message Type	Contains the type of message that was sent. This can be one of the following: Message, Ping, File, Picture, Notification, Location.
Message Status	The status of the message (received or sent).
Message State	Contains the state of the message. This can be one of the following: 'Sent', 'Undelivered', 'Delivered, Unread', 'Read'.

ATTRIBUTE	DESCRIPTION
Display Name	The display name of who sent the message to the device or who's receiving a message from the device.
BlackBerry PIN	The BlackBerry PIN of who sent the message to the device or who's receiving a message from the device.
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent/received.
Message Content	The message sent/received.
Conversation ID	The conversation identifier.
Participants	The display names of the people in the conversation.
Attachment	The attachment that was sent/received.

BlackBerry Messenger Profile

Description	Contains the BBM Profiles recovered from an Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Display Name	The display name associated with the profile.
BlackBerry PIN	The BlackBerry PIN associated with the profile.
Personal Message	The profiles personal message.
Personal Message Last Update Date/Time - UTC (yyyy-mm-dd)	The date and time the profile message was last updated.
Avatar	The profiles avatar.
Avatar Content Type	The avatar content type. An example is 'image/jpeg'.
Location	The location of the profile.
Timezone	The timezone of the profile.
Keeps Chat History	Indicates whether or not the user keeps chat history.

Burner Contacts

Description	Burner Contacts contains information about a subject's Burner Contacts, as recovered from their Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Contact ID	The ID of the contact.
Contact Name	The name of the contact.
Phone Number	The phone number of the contact.
Burner ID	The ID of the Burner application associated with the contact.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the contact was created.

Burner Messages

Description	Burner Messages contains information about messages and calls that are sent and received using Burner.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The phone number of the sender.
Recipient	The phone number of the recipient.
Message	The body of the message.
Message Type	The type of message.
Media URL	The URL to the media file attached to the message
Voicemail URL	The URL of the voicemail.

Burner Numbers

Description	Burner Numbers contains information about the burner numbers that the local user created.
Notes	

ATTRIBUTE	DESCRIPTION
Burner ID	The ID of the Burner number.
Burner Number	The Burner phone number.
Display Name	The display name associated with the Burner number.
Created Date/Time	Indicates when the Burner number was created.
Expiration Date/Time	Indicates when the number will expire.
Mobile Number	The phone number used to sign in to the Burner App.
User ID	The user id of the signed in user.

Cake Local User Account

Description	Cake Local User Account contains information about the logged in local user.
Notes	

ATTRIBUTE	DESCRIPTION
Local User ID	The unique ID of the local user.
Local User Display Name	The display name of the local user.
Gender	The gender of the local user.
Birthday	The birthday of the local user.
Email Address	The email address of the local user.

Cake Messages

Description	Cake Messages contains messages sent and received by the local user.
Notes	

ATTRIBUTE	DESCRIPTION
Sender ID	The unique user ID of the sender.
Sender Display Name	The display name of the sender.
Recipient ID	The Cake ID of the message recipient. If the chat type is Group chat, the recipient ID is the group ID.
Recipient Display Name	The display name of the message recipient. If the chat type is Group chat, the recipient display name is the group display name.
Message	The body of the message.
Created Date/Time	The date and time when the message was created.
Chat Type	The type of chat where the message was sent (Group chat or One to one).
Picture URL	The URL of the picture, if one is attached to the message.

Chatous Chat Messages

Description	Chatous Chat Messages contains messages that were sent and received using the Chatous application.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The display name of the user who sent the message (Local User if it was the local user).
Recipient	The display name of the user who received the message (Local User if it was the local user).
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The body of the message.
Attachment Name	The name of the attachment that was sent.
Attachment Data Recovered	Indicates whether attachment data was recovered (Yes or No).

Chatous Chat Partners

Description	Chatous Chat Partners contains information about the users that the local user has communicated with.
Notes	

ATTRIBUTE	DESCRIPTION
Screen Name	The name of the chat partner.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the last message in the chat.
Age	The age of the chat partner.
Gender	The gender of the chat partner. A blank value indicates that the chat partner is the Team Chatous account.
Location	The location of the chat partner.
About	A summary of the chat partner.
Tag	The tag that matched the local user and the chat partner for a chat.
Profile Tags	The hashtags that the chat partner uses to describe themselves.

Discord Logged-in Account

Description	Discord Logged-in Account contains information about the user that is currently logged into Discord on the device. Information about other accounts that were previously logged into are not recoverable.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The ID of the logged-in user.
User Name	The name of the logged-in user.
Email	The email address of the logged-in user.
Locale	The locale of the logged-in user.
User Token	The authentication token of the logged-in user.

Discord Messages

Description	Discord Messages contains information about messages and calls that are sent and received using Discord. Messages from some channels might be missing if they haven't been cached by the application. This artifact uses both parsing and carving techniques to recover messages.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The username of the message sender.
Message	The message content.
Channel ID	The ID of the channel that the message was sent in. This attribute is always empty for Android.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Last Edited Date/Time - UTC (yyyy-mm-dd)	If the message has been edited then this indicates the date and time when the last edit has occurred.
Attachment URL	If the message includes an attachment then this indicates the saved URL of the attachment. This attribute is always empty for Android.
Attachment Name	If the message includes an attachment then this indicates the file name of the attachment. This attribute is always empty for Android.
Embedded Content Title	If the message contains a link then this then this indicates the title that's displayed in the link preview.
Embedded Content Description	If the message contains a link then this indicates the description that's displayed in the link preview. This attribute is always empty for Android.
Message Type	The type of message (Message or a Call).
Call End Date/Time - UTC (yyyy-mm-dd)	If the message was a call, this indicates the date and time that the call ended.
Pinned	Indicates whether a message is pinned (True or False). This attribute is always empty for Android.

Facebook Messenger Calls

Description	Facebook Messenger Calls contains call data recovered from Facebook Messenger.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The name of the application that generated the data (Facebook Messenger or Facebook Messenger Kids).
User Key	The user key of the call partner.
Thread Key	The thread key of the group where the call was made.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the call.
Call Duration (Seconds)	The duration of the call. If the call wasn't answered this field is Empty.
Call Type	The type of call. The types of calls are voice calls and group voice calls.
Answered	Indicates whether the call was answered or not.
Direction	The direction of the call.

Facebook Messenger Groups

Description	Facebook Messenger Groups contains data about group chats on Facebook Messenger.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The name of the application that generated the data (Facebook Messenger or Facebook Messenger Kids).
Thread Key	The thread key of the group.
Group Name	The display name of the group.
Participants	The users that are a part of the group.
Sender(s)	The users that recently participated in the group (for example, by sending a message).
Last Activity Date/Time - UTC (yyyy-mm-dd)	The date and time of the last activity recorded in the group.
Message Count	The approximate number of messages in the group.

Facebook Messenger Messages

Description	Facebook Messenger Messages contains messages recovered from Facebook Messenger.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The name of the application that generated the data (Facebook Messenger or Facebook Messenger Kids).
Sender Name	The display name of the person sending the message.
Receiver Name	The display name of the person receiving the message.
Date/Time - UTC (yyyy-mm-dd)	The date and time when message was sent.
Deleted Date/Time - UTC (yyyy-mm-dd)	The date and time the message was deleted from the application.
Text	The text of the message.
Thread ID	The thread ID of the message. This is also the Facebook ID of the remote party.
Media Type	The type of media that was sent with the message.
Media Info	The information about the media that is found. This value can be a URL to the media, a file name, or a sticker ID.
Send State	Represents whether the message was sent, received or queued. This field is always empty for Android.
Message ID	The internal unique message ID.
Receiver ID	The user ID of the person receiving the message.
Sender ID	The user ID of the person sending the message.
Message Source	The source of the message creation platform.
Latitude	The latitude portion of the location data that is sent with the message.
Longitude	The longitude portion of the location data that is sent with the message.

Facebook Messenger Users Contacted

Description	Facebook Messenger Users Contacted contains information about users contacted from the device using Facebook Messenger.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The name of the application that generated the data (Facebook Messenger or Facebook Messenger Kids).

ATTRIBUTE	DESCRIPTION
User Key	The user key of the user.
First Name	the first name of the user.
Last Name	The last name of the user.
Name	The display name of the user.
Username	The unique identifier of the user.
Profile Picture URL	The URL of the user's profile picture.
Is App User	Identifies whether the user is using Facebook Messenger or not.
Is Friend	Identifies whenever the user is a friend of the local user.
Rank	User's rank within the app.

Glide Messages

Description	Glide Messages contains messages sent and received by the local user.
Notes	

ATTRIBUTE	DESCRIPTION
Sender ID	The unique user ID of the sender.
Sender Name	The name of the sender.
Recipient ID(s)	The Glide IDs of the message recipients.
Recipient Name(s)	The names of the message recipients.
Message	The body of the message.
Message Type	The type of message.
Created Date/Time	The date and time when the message was created.
Read	The read status of the message.
Media URL	The URL to any media that's attached to the message.
Chat Type	The type of chat where the message was sent (group or oneToOne).

Glide Users

Description	Glide Users contains information about the contacts that the local user has added using Glide. The local user's contact information is also recovered by this artifact.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The unique ID of the user.
First Name	The first name of the user.
Last Name	The last name of the user.
Email Address	The email address of the user.
Gender	The gender of the user.
Account Type	The type of account associated with the user.
Last Seen Date/Time	The last time the user was seen online.

Google Duo Calls

Description	Google Duo Calls contains details about audio and video calls made by the user.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local user of the device where the data was recovered from.
Remote Username	The username of the remote participant of the call.
Remote User ID	The user ID or phone number of the remote participant of the call.
Direction	Indicates whether the call is outgoing or incoming.
Call Date/Time - UTC (yyyy-mm-dd)	The date and time that the user started the call.
Call Status	The status of the call.
Call Duration (seconds)	The duration of the call.
Call Type	Indicates Whether the call is an audio or video call.

Google Duo Messages

Description	Google Duo Messages contains details about audio, video, photo, and note messages sent and received by the user.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the message.
Recipient(s)	The recipient(s) of the message.
Direction	Whether the message is outgoing or incoming.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent or received.

ATTRIBUTE	DESCRIPTION
Attachment Name	The name of the message attachment.
Attachment	The attachment that was sent or received.

Google Hangouts Cached Images

Description	Google Hangouts Cached Images contains the cached images from Google Hangouts from an Android device.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the cached image.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the image. The significance of the date and time is unknown to us.
Image	The cached image.

Google Hangouts Voice Calls

Description	Google Hangouts Voice Calls contains a history of voice calls between the local user and other users.
Notes	

ATTRIBUTE	DESCRIPTION
Phone Number	The phone number of the call participant.
Call Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the call started.

Google Meet Accounts

Description	Google Meet Accounts contains the Google Meet accounts that are currently signed in on the device.
Notes	

ATTRIBUTE	DESCRIPTION
Account Name	The account name of the user.
Display Name	The display name of the user.

ATTRIBUTE	DESCRIPTION
Profile ID	The GAIA ID.
Profile Image URL	The URL for the user's profile image.

Google Meet Meeting History

Description	Google Meet Meeting History contains the meetings that any local user on the device has joined.
Notes	

ATTRIBUTE	DESCRIPTION
Meeting ID	The unique ID for the meeting.
Meeting Code	The code that was used to join the meeting.
URL	The URL for the meeting.
Joined Date/Time - Local Time	The local date and time that the local user joined the meeting.
Type	Whether the local user created or joined the meeting.

Grindr Buddies

Description	Grindr Buddies contains the buddies and their details that were extracted from the current user's Android data.
Notes	

ATTRIBUTE	DESCRIPTION
Public ID	The ID of the user in the buddy list.
Description	The description of the buddy.
Display Name	The display name of the buddy.
Age	The age of the buddy.
Height (cm)	The height of the buddy.
Weight (kg)	The weight of the buddy.
Ethnicity	The ethnicity of the buddy.
Distance	The distance of the buddy from the current user.
Favorited	Indicates whether the buddy is a favorite buddy of the current user.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the last message that was sent or received from this buddy.

Grindr Messages

Description	Grindr Messages contains the messages (and their details) that were extracted from a user's Android data.
Notes	

ATTRIBUTE	DESCRIPTION
Sender ID	The ID of the sender of the message.
Receiver ID	The ID of the receiver of the message.
Conversation Partner	The buddy's display name the message was with.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was received.
Message Body	The body of the message.
Read Status	The status of the message (Read or Unread).
Message Direction	Indicates whether the message was incoming to the device, or outgoing from the device.

GroupMe Accounts

Description	GroupMe Accounts contains information about the accounts that the local user has logged in with on the device.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user ID of the local user.
Display Name	The display name of the local user.
Email Address	The email address of the local user.
Phone Number	The phone number of the local user.
Created Date/Time	The date and time that the account was created (specific to iOS).
Login Date/Time	The date and time that the account was logged in on the device (specific to Android).
Profile Picture URL	The URL of the profile picture of the local user.
Password/Token	The local user password/token.

GroupMe Contacts

Description	GroupMe Contacts contains information about a user's contacts.

Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user ID of the contact.
Display Name	The display name of the contact.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the contact was added.

GroupMe Groups

Description	GroupMe Groups contains information about the groups that the logged-in user is a member of.
Notes	

ATTRIBUTE	DESCRIPTION
Group	The group number.
Group Name	The name of the group.
Topic	The topic of the group.
Creator ID	The creator identifier of the group.
Created Date/Time	The date and time when the group was created
Group Member ID(s)	The IDs of all of the group's participants.
Group Member Name(s)	The names of all of the group's participants.

GroupMe Messages

Description	GroupMe Messages contains the messages sent and received using GroupMe.
Notes	

ATTRIBUTE	DESCRIPTION
Sender Name	The name of the message sender.
Sender ID	The user ID of the message sender.
Recipient Name(s)	The user name(s) of the message recipient(s).
Recipient ID(s)	The user ID(s) of the message recipient(s).
Sent Date/Time	The date and time when the message was sent.
Message	The message text.
Photo URL	The URL to the photo associated with the message.
Video URL	The URL to the video associated with the message.

ATTRIBUTE	DESCRIPTION
Location	The name of the location in the location data sent with the message.
Latitude	The latitude part of location data sent with the message.
Longitude	The longitude part of location data sent with the message.
Event	The event sent with the message.
Document Title	The document details sent with the message.
Poll	The poll details sent with the message.

GROWLr Chat Messages

Description	GROWLr Chat Messages contains the messages on the device that were sent or received through Growlr.
Notes	

ATTRIBUTE	DESCRIPTION
Account ID	The ID of the other person that the message is with.
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent or received.
Message	The body of the message.
Message Type	Indicates whether the message was incoming or outgoing.
Message Status	The status of the message (Read or Unread).
Image Filename	The path to the image that is associated with the message.
Image	The attached image.
Voice Filename	The filename of the attached voice message.
Voice	The attached voice data.

GROWLr Notes

Description	GROWLr Notes contains the notes on Growlr that the user has made, and when they were last modified.
Notes	

ATTRIBUTE	DESCRIPTION
Text	The body of the note.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that the note was modified.

Gtalk Contacts

Description	Gtalk Contacts contains contact information that was recovered from Gtalk.
Notes	

ATTRIBUTE	DESCRIPTION
Username	The username/Gmail address of the contact.
Nickname	The nickname of the contact.
Local Account	The user account of the user logged into Gtalk.

Gtalk Message

Description	Gtalk Message contains the details of messages that were recovered from Gtalk.
Notes	

ATTRIBUTE	DESCRIPTION
Conversation ID	The ID of the conversation.
Message	The body of the message.
Sent/Received	The type of the message.
Date/Time - (UTC)(MM/dd/yyyy)	The timestamp for the message.
Local User	The local user ID.
Sender	The user who sent the message.
Receiver	The user who received the message.

imo Contacts

Description	imo Contacts contains information about a user's contacts.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The unique user ID of the contact.
Display Name	The display name of the contact.
Name	The full name of the contact.
Phone Number	The phone number of the contact.
Number of Times Contacted	The number of times that the local user has communicated with the contact.

imo Messages

Description	imo Messages contains information about sent and received messages, and calls made using the imo application.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	Indicates the local user identifier of the account.
Remote User ID	The user ID of the remote conversation partner.
Remote User Display Name	The display name of the remote conversation partner.
Direction	The direction of the message.
Message	The message content.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message Type	The type of the message (either messages or calls).
Attachment Path	The path to locate any attachments on the device.

Jott Groups

Description	Jott Groups contains information about the groups that the Jott user is a member of.
Notes	

ATTRIBUTE	DESCRIPTION
Group Chat ID	The ID of the group chat.
Group Name	The display name of the group.
Participants	The users that are a part of the group.
Picture Path	The path to the group's picture, if one exists.

Jott Messages

Description	Jott Messages contains information about the messages sent or received by the Jott user.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The username of the person sending the message.

ATTRIBUTE	DESCRIPTION
Recipient	The username of the person receiving the message, or the group chat ID if the message is being sent to a group.
Message	The message being sent.
Direction	The direction of the message being sent.
Read Status	Indicates whether or not the message has been read.
Group Chat	Indicates whether or not this is a group chat.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was received.
Attachment Path	The path to the attachment, if one exists.

KakaoTalk Calls

Description	KakaoTalk Calls contains audio calls and/or video calls sent or received using KakaoTalk.
Notes	Call Status and Sender information are not available for deleted calls.

ATTRIBUTE	DESCRIPTION
Call Status	Information about the call.
Duration (Seconds)	The duration of the call in seconds.
Sender ID	The KakaoTalk ID of the sender.
Sender Name	The name of the sender.
Chat ID	The ID of the KakaoTalk chat room session.
Call Type	Indicates whether the call was a voice call or a video call.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the call was made.
Deleted Date/Time - UTC (yyyy-mm-dd)	The date and time that the call was deleted from the application.
Direction	Indicates whether the call was incoming or outgoing.

KakaoTalk Chat Rooms

Description	KakaoTalk Chat Rooms contains KakaoTalk chat rooms that the user participates in.
Notes	

ATTRIBUTE	DESCRIPTION
Group Chat ID	The ID of the KakaoTalk chat room session.

ATTRIBUTE	DESCRIPTION
Other Participants	The names or KakaoTalk IDs of the other chat room participants.
Chat Type	The type of chat room session.
Last Message	The last message sent by any participant in the chat room session.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the chat room session was last updated.
Unsent Message	Messages that the local user has written, but not sent to the chat room.
Group Name	The name of the group, if the chat room session is a group chat.
Invitation Status	The status of any invitations to the chat room.

KakaoTalk Detected Wifi

Description	KakaoTalk Detected Wifi contains the network name of any WiFi networks detected by KakaoTalk.
Notes	As of KakaoTalk 8.4.0, the data in this artifact is no longer available.

ATTRIBUTE	DESCRIPTION
Network Name (SSID)	The network name.

KakaoTalk Friends

Description	KakaoTalk Friends contains the user's KakaoTalk friends and contacts.
Notes	

ATTRIBUTE	DESCRIPTION
ID	The KakaoTalk ID of the friend.
Name	The friend's name.
Contact Name	The friend's full contact name.
Nickname	The friend's nickname as set by the local user.
Favorite	Indicates whether the friend has been marked as a favorite.
Hidden	Indicates whether the friend has been hidden in the local user's application.
Phone Number	The friend's phone number.
Profile Picture URL	The URL for the friend's profile picture.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the friend's account was created.

ATTRIBUTE	DESCRIPTION
User ID	The friend's KakaoTalk user ID.
Group Chat ID	The chat room session IDs that the friend shares with the local user.

KakaoTalk Messages

Description	KakaoTalk Messages contains messages sent or received using KakaoTalk.
Notes	Message and Sender information are not available for deleted messages.

ATTRIBUTE	DESCRIPTION
Message	The message contents.
Sender ID	The KakaoTalk ID of the sender.
Sender Name	The name of the sender.
Chat ID	The ID of the KakaoTalk chat room session.
Message Type	The type of the message sent.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was created.
Deleted Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was deleted from the application.
Message Direction	Indicates whether the message was sent or received.
Additional Information	Additional information attached to the message.
Latitude	The latitude of location type messages.
Longitude	The longitude of location type messages.

Life360 Circle Members

Description	Life30 Circle Members contains information about the members of a circle. A circle is comprised of a group of individuals, such as a family, that the local user has created or has been added to by another circle member.
Notes	

ATTRIBUTE	DESCRIPTION
Member ID	The unique member ID of the circle member.
First Name	The first name of the member.
Last Name	The last name of the member.
Email Address	The email address of the member.

ATTRIBUTE	DESCRIPTION
Phone Number	The phone number of the member.
Circle Name	The name the circle.
Circle ID	The ID of the circle.

Life360 Local User Account

Description	Life360 Local User Account contains information about local user accounts.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The unique ID of the local user.
First Name	The first name of the local user.
Last Name	The last name of the local user.
Email Address	The email address of the local user.
Phone Number	The phone number of the local user.

Life360 Messages

Description	Life360 Messages contains messages sent and received by the local user within a circle that they're a member of.
Notes	

ATTRIBUTE	DESCRIPTION
Sender ID	The unique ID of the sender.
Sender Name	The name of the sender.
Recipient ID(s)	The ID(s) of the recipient(s).
Recipient Name(s)	The name(s) of the recipient(s).
Message Type	The type of the message.
Message	The message content.
Created Date/Time	The date and time when the message was created.
Picture URL	The URL of the picture on the Life360 server, if a picture is included in the message.
Read	The read status of the message.
Latitude	The latitude of the location, if the message is a map location.

ATTRIBUTE	DESCRIPTION
Longitude	The longitude of the location, if the message is a map location.
Location Name	The name of the location if the message is a map location.
Location Acquired Date/Time	The date and time when the location was acquired if the message is a map location.

Life360 Places

Description	Life360 Places indicates favorite locations that are saved by the user or the application.
Notes	

ATTRIBUTE	DESCRIPTION
Place Name	The name of the place. The name can be either user-defined or a default name defined by the application.
Place Address	The address of the place.
Circle ID	The ID of the circle where the place was found.
Owner ID	The owner ID of the place, if the place was created by user.
Latitude	The latitude of the place.
Longitude	The longitude of the place.

Life360 Trip Locations

Description	Life360 Trip Locations indicates the locations that the user visits (or passes by on the way to a destination). During a trip, the application will log locations at regular intervals along the way.
Notes	

ATTRIBUTE	DESCRIPTION
Updated Date/Time	The date and time that the trip details were last updated. Updates to the trip can be triggered by the user or the application.
Circle ID	The circle ID of the user who created this trip.
User ID	The unique ID of the user who created this trip.
Start Date	The date that the trip happened (days begin at 12:00 AM local time).
Latitude	The latitude of the location.
Longitude	The longitude of the location.

ATTRIBUTE	DESCRIPTION
Start Date/Time	The date and time when the user arrived at the location.
End Date/Time	The date and time when the user left the location.
Location Name	The name of the location if it is a user created place.
Location Address	The address of the location.

Mail.Ru Agent Contacts

Description	Mail.Ru Agent Contacts contains contact info for the Agent application on Android.
Notes	

ATTRIBUTE	DESCRIPTION
Contact ID	The user ID of contact.
Display Name	The display name of contact.
Account Type	The type of the contact. The value can be Agent ID or Agent Channel.
Local User ID	The unique ID of the local user.

Mail.Ru Agent Messages

Description	Mail.Ru Agent Messages contains messages sent or received by the Agent user on Android.
Notes	

ATTRIBUTE	DESCRIPTION
Local User ID	The unique ID of the local user.
Remote User ID	The user ID of the remote participant of the chat.
Remote Participant Display Name	The display name of remote participant.
Created Date/Time	The date and time that the message was created.
Message	The content of the message.
Type	The type of the message. The value can be Text Message, Voice Call, Video Call or File Transfer.
Duration (Seconds)	The duration of voice or video call.

ATTRIBUTE	DESCRIPTION
Direction	The direction of the message.
File Name	The file name of the attachment.

Mail.Ru Agent User Accounts

Description	Mail.Ru Agent User Accounts contains information about the Agent user accounts that are saved locally on the Android device.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The unique ID of the local user.
Active	Whether or not the account is currently logged in.
First Name	The first name of the account.
Last Name	The last name of the account.
Display Name	The display name of the account.
Birthday	The birthday of the account.
Phone Number	The phone number of the account.
Gender	The gender of the account.
Home Address	The home address of the account.

QQ File Transfers

Description	QQ File Transfers contains file transfers recovered from the QQ application.
Notes	

ATTRIBUTE	DESCRIPTION
Local User ID	The local user ID who the file was transferred with.
Chat Partner / Group Chat ID	The unique ID of the chat partner or group the file was transferred with.
Partner Display Name	The name displayed for the partner the file was transferred with.
File Name	The file name of the file transferred.
File Path	The file path of the file transferred.
Server Date/Time - UTC (yyyy-mm-dd)	The server date and time that the file was transferred.
File Size (bytes)	The size of the file transferred.

ATTRIBUTE	DESCRIPTION
Direction	Sent/Received: Indicates the direction of the file transfer relative to the local user.
MD5 Hash	The MD5 hash of the file.
SHA1 Hash	The SHA1 hash of the file.

QQ Local Users

Description	QQ Local Users contains local users recovered from the QQ application.
Notes	

ATTRIBUTE	DESCRIPTION
Local User ID	The user ID of the local user.
Local User Display Name	The name displayed for the local user.
Country	The country of the user.
City	The city of the user.
Age	The user's age in years.
Birthday (yyyy-mm-dd)	The user's birthday in YYYY-MM-DD format.
Email	The user's email address.

QQ Messages

Description	QQ Messages contains messages stored by the QQ application.
Notes	

ATTRIBUTE	DESCRIPTION
Local User ID	The unique ID of the local user.
Local User Display Name	The name displayed for the local user.
Chat Partner / Group Chat ID	The unique ID of the chat partner or group.
Sender User ID	The unique ID of the sender.
Sender Display Name	The name displayed for the sender.
Message	The text of the message.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the message.
Type	The type of content in the message.

ATTRIBUTE	DESCRIPTION
Sent/Received	Indicates whether the message is incoming or outgoing (Sent or Recieved).
Read	Indicates whether the message has been read (Read or Unread).

Samsung Text Message Logs

Description	Text message logs recovered from a Samsung Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local user of the device where data was recovered from.
Partner	An identifier for the person who communicated with the local user.
Partner Name	The name of the partner, as set by the local user.
Direction	The direction of the message, relative to the local device (Incoming or Outgoing).
Date/Time - UTC (yyyy-mm-dd)	The date and time of the text message.
Message Content	The text message content.
Subject	The subject of the text message. If message type is MMS this field has a value, otherwise is empty.
Message Type	The type of message. This can be 'SMS' or 'MMS'.

Signal

Signal is an encrypted messaging and voice calling application that's available for Android and iOS. The application enables a user to send content (messages, pictures, and videos) to other users and to groups of users. Signal also includes the capability for users to set a password on the application to protect their data.

Forensic notes

Signal for Android

Even though Signal uses encryption to protect its data, it's still possible to recover useful artifacts from Android devices. In cases where the user doesn't set a password, application data can often be recovered and decrypted. Even if decryption is not possible, group and user information, and information about messages can still be recovered (excluding the actual message and attachment content). In addition, latitude and longitude from location messages is also recoverable (these are messages that a user sends that includes their current location).

For instances when the user does set a password, you can provide a list of potential passwords for AXIOM Process or IEF to use as the key for decrypting the data. Once decrypted, message content and attachments are also available.

Artifacts

Signal Group Members

Description	Signal Group Memebers specifies the members from each of the Signal groups that the local user is a member of.
Notes	

ATTRIBUTE	DESCRIPTION
Group Member	The phone number of the group memeber.
Group Name	The name of the group.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the group was created (Empty for Android).
Group Avatar	The avatar of the group.

Signal Local User

Description	Signal local User contains information about the local user account.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The name of the local user.
Avatar	The avatar used by the local user account (Empty for Android).

Signal Messages

Description	Signal Messages contains information about the messages and calls that are exchanged between the local user and other users.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the message.
Recipient	The recipient of the message.
Partner	The partner of the call.
Message	The text contents of the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the the message was first attempted to be sent.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was received.
Attachment	The attachment of the message.
MIME Type	The MIME type of the attachment.
Type	The type of message.
Direction	The direction of the message.
Read	Indicates whether or not the message has been read by the local user.
Latitude	The latitude of the message.
Longitude	The longitude of the message.

Skype Accounts

Description	Skype Accounts contains information about the Skype accounts that are recovered, such as user information and when the account was created.
Notes	

ATTRIBUTE	DESCRIPTION
Skype Name	The Skype name of the account.
Display Name	The display name of the account.
Full Name	The full name of the account.
Birthday	The birthday of the account.
Gender	The gender of the account.
City	The city where the account is located.
State/Province	The state/province where the account is located.
Country	The country where the account is located.
Home Phone	The home phone of this contact.
Office Phone	The office phone of this account.
Mobile Phone	The mobile phone of this account.
Email(s)	The email of this account.

ATTRIBUTE	DESCRIPTION
Homepage	The homepage of this contact.
About Info	The about info of this contact.
Profile Created On Date/Time - UTC (yyyy-mm-dd)	The date when the profile was created.
Profile Last Modified On Date/Time - UTC (yyyy-mm-dd)	The date when the profile was last modified.
Mood Text	The text used to express mood.
Last Online On Date/Time - UTC (yyyy-mm-dd)	The last time that the account was online.
Last used On Date/Time - UTC (yyyy-mm-dd)	The last time that the account was used.
Avatar Timestamp Date/Time - UTC (yyyy-mm-dd)	The time that the avatar was created.
Image	The image for this contact.

Skype Activity

Description	Skype Activity contains interactions that occured between users on Skype. These interactions include messages, group interactions, calls, sent/received files, and SMS. This information is recovered for Skype 8.1 and later.
Notes	

ATTRIBUTE	DESCRIPTION
Conversation ID	The ID of this conversation.
Profile Name	The local user's profile name.
Sender	The username of the sender/initiator of the interaction.
Sender Email	The sender's email as given in the message (if available).
Recipient Name(s)	The recipients or targets of the interaction.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the interaction was initiated.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the interaction was last updated (for example, when a call ends).
Message Type	The type of the interaction.
Message	The content of the message or a summary of the interaction.
Emotion Count	The number of reactions to the interaction. Reactions include likes, dislikes, emojis and more.
File Name	The name of any attached files associated with the interaction.
File Size (Bytes)	The size in bytes of any attached files.
File	The attachment file (if applicable).
Attachment Data Recovered	Indicates whether the attached file was recovered from the local filesystem.
Thumbnail URL	A URL that directs to the thumbnail picture (if applicable).

ATTRIBUTE	DESCRIPTION
Call Duration (Seconds)	The length of the call in seconds (if applicable).
Metadata	The content of the message, if it consisted of interpreted data (XML or JSON data, rather than plain text).

Skype Calls

Description	Skype Calls contains information about Skype calls that occur between users.
Notes	

ATTRIBUTE	DESCRIPTION
Local Username	The user logged into Skype at the time of the call.
Call Initiator	The user who started the call.
Initiator Display Name	The display name of the user. This might be different from the username.
Recipient(s)	The users who accepted a call from the call initiator and participated in the call for a period of time.
Call Participants	The users who accepted and participated in the call from the call initiator for some duration.
Started Date/Time - UTC (yyyy-mm-dd)	The start time of the call.
Duration	The total duration of the Skype call.
Metadata	Additional details about the call extracted in XML format. This includes information on the amount of time that each participant was in the call.

Skype Chat Messages

Description	Skype Chat Messages contains Skype messages sent from one user to another.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	The profile name of the caller.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Author	The author of the message.
From Display Name	The display name of the message sender.

ATTRIBUTE	DESCRIPTION
Message	The body of the message or a description of the action taken. For example, adding another participant to a group chat or sharing a file or picture.
Attachment Name	The name of the attachment that was sent. This attribute is populated when the Message Type is POSTED_FILE or POSTED_PICTURE. Otherwise, this attribute is empty.
Attachment Size (Bytes)	The size of the attached file, in bytes. This attribute is populated when the Message Type is POSTED_FILE or POSTED_PICTURE. Otherwise, this attribute is empty.
Metadata	Additional details about the action, extracted in its original XML format.
Message Status	The status of the message.
Message Type	The type of message.
Chat ID	The ID of the chat.
Recipient	The recipient of the chat.

Skype Chatsync Messages

Description	Skype Chatsync Messages contains Skype messages that were sent from one user to another, and that are parsed from the chatsync directory.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local user of this message.
Chat Initiator	The initiator of the message.
Chat Partner/Group Chat ID	The other part of this message.
Message Type	The type of the message.
Message	The content or body of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.

Skype Contacts

Description	Skype Contacts contains information about Skype contacts that are recovered, which may or may not be added contacts.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	The profile name of the user.
Skype Name	The Skype name of the contact.
Display Name	The display name of this account.

ATTRIBUTE	DESCRIPTION
Is Blocked	Indicates whether the contact is blocked.
Contact Added	Specifies whether the contact is an added contact or just cached into the database (1 if the contact was added, 0 otherwise). Contacts can be cached into the database for a variety of reasons (for example, as a suggested contact).
Full Name	The full Name of this account
Birthday	The birthday of this account.
Gender	The gender of this account.
City	The city where this account is located.
State/Province	The state/province where this account is located.
Country	The country where this account is located.
Home Phone	The home phone of this contact.
Office Phone	The office phone of this account.
Mobile Phone	The mobile phone of this account.
PSTN Number	The PSTN number of this contact.
Email(s)	The email of this account.
Homepage	The homepage of this contact.
About Info	The about info of this contact.
Profile Loaded Date/Time - UTC (yyyy-mm-dd)	Previously called Profile Created On Date/Time, this attribute represents the date and time when a contact's profile is first created on the user's device. When the profile information is updated by the contact, the date in the database is also updated.
Mood Text	The text used to express mood.
Last Online On Date/Time - UTC (yyyy-mm-dd)	The last time that the account was online.
Last used On Date/Time - UTC (yyyy-mm-dd)	The last time that the account was used.
Avatar Timestamp Date/Time - UTC (yyyy-mm-dd)	The time that the avatar was created.
Image	The image for this contact.

Skype Emotions

Description	Skype Emotions contains the reactions of users to Skype messages.
Notes	

ATTRIBUTE	DESCRIPTION
Emotion	The type of emotion that the user reacted to the message with. The emotion is displayed using the shortcut from Skype (for example, cwl represents the emotion Crying With Laughter).
Message Content	The content of the message that the user reacted to. If the content of the message is plain text, this attribute matches the "Message" attribute from the "Skype Activity" artifact. Otherwise, this attribute matches the "Metadata" attribute.
Skype Name	The Skype name of the user who reacted to the message.
Date/Time - UTC (yyyy-mm-dd)	The date and time that the user reacted to the message.

Skype File Transfers

Description	Skype File Transfers contains files that are transferred from one user to another using Skype.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	The name of the user.
Partner Handle	The username of the file transfer partner.
Partner Display Name	The display name of the file transfer partner.
File Name	The name of the file that was being transferred.
Type	The type of file that was being transferred.
File Path	The path to the local file.
Transferred File	The file that was transferred.
File Size (Bytes)	The size of the file being transferred.
Bytes Transferred	The number of bytes that were transferred.
Transfer Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the file transfer was started.
Transfer Finish Date/Time - UTC (yyyy-mm-dd)	The date and time when the file transfer was completed.
Status	The status of the file (for example, transfer, transferring or cancelled).

Skype Group Chat

Description	Skype Group Chat contains information about the Skype group chats that a user is a part of.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	The name of the user.
Chat ID	The group chat's unique identifier.
Participants	The participants of the chat.
Posters	The users that have posted to the chat.
Active Members	The currently active user's of the group.
Chat name	The name of the chat.
Started Date/Time - (UTC) (yyyy-mm-dd)	The date and time that the chat started.
Last Changed Date/Time - (UTC) (yyyy-mm-dd)	The date and time that the chat was modified.

Skype IP Addresses

Description	Skype IP Addresses contains the IP addresses that are associated with a Skype user account.
Notes	

ATTRIBUTE	DESCRIPTION
Username	The username of Skype accounts.
IP Addresses	The IP addresses for the Skype user.
IP Address Type	The type of IP address (Local or Public).
Date/Time - UTC (yyyy-mm-dd)	The date and time.

Skype Notifications

Description	Skype Notifications contains notifications that were shown to users on Skype.
Notes	

ATTRIBUTE	DESCRIPTION
Read	Indiactes whether the user has read the notification.
Conversation ID	The ID of this conversation.
Profile Name	The local user's profile name.
Sender	The username of the sender/initiator of the interaction.
Recipient Name(s)	The recipients or targets of the interaction.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the interaction was initiated.

ATTRIBUTE	DESCRIPTION
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the interaction was last updated (for example, when a call ends).
Message Type	The type of the interaction.
Message	The content of the message or summary of the interaction.
Emotion Count	The number of reactions to the interaction. Reactions include likes, dislikes, emojis, and more.
File Name	The name of any attached files associated with the interaction.
File Size (Bytes)	The size in bytes of any attached files.
File	The attachment file (if applicable).
Attachment Data Recovered	Indicates whether the attached file was recovered from the local filesystem.
Thumbnail URL	A URL that directs to the thumbnail picture (if applicable).
Metadata	The content of the message, if it consisted of interpreted data (XML or JSON data, rather than plain text).

Slack Channel Messages

Description	Slack Channel Messages contains messages sent or received in channels in the user's Slack workspace.
Notes	

ATTRIBUTE	DESCRIPTION
Workspace ID	The unique identifier for the slack workspace.
Sender	The name or user ID of whoever sent the message.
Channel Name	The name of the channel that the message was sent to.
Message	The message text.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message Status	The delivered status of the message.

Slack Channels

Description	Slack Channels contains information about each of the channels and conversations that exist in a user's Slack workspace.
Notes	

ATTRIBUTE	DESCRIPTION
Channel Name	The name of a channel or message group.

ATTRIBUTE	DESCRIPTION
Channel ID	The ID of a channel or message group.
Workspace ID	The unique identifier for the slack workspace.
Created By	The name or user ID of whoever created the channel.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the channel was created.
Topic	The topic text for the channel.
Topic Author	The name or user ID of whoever last wrote the topic text.
Channel Type	The type of channel (Public, Private, General, Single User DM, Multi User DM.)
Last Read Date/Time - UTC (yyyy-mm-dd)	The date and time when the channel was last read.
Member	Represents whether or not the local user is a member of the channel.
Starred	Represents whether or not the local user has starred the channel.

Slack Direct Messages

Description	Slack Direct Messages contains information about direct messages sent or received in 1:1 chats or group chats.
Notes	

ATTRIBUTE	DESCRIPTION
Workspace ID	The unique identifier for the slack workspace.
Sender	The names or user IDs of the message recipients.
Message	The message text.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message Status	The delivered status of the message.

Slack Files

Description	Slack Files contains information about any files that have saved to the Slack workspace. Files may or may not have been shared with other users.
Notes	

ATTRIBUTE	DESCRIPTION
Workspace ID	The unique identifier for the slack workspace
Title	The title given to the file.

ATTRIBUTE	DESCRIPTION
File Name	The name of the file.
Created By	The name or user ID of whoever created the file.
Permanent Link	A permalink to the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was uploaded
FileSize	The size of the file
Deleted	Represents whether or not the file has been deleted.

Slack Users

Description	Slack Users contains information about each user in the Slack workspace.
Notes	

ATTRIBUTE	DESCRIPTION
Workspace ID	The unique identifier for the slack workspace.
Full Name	The full name of the user.
First Name	The first name of the user.
Last Name	The last name of the user.
User Name	The unique user name of the user.
Display Name	The slack display name of the user.
Email	The user email.
Phone Number	The user phone number.
Member ID	The user ID.
Title	The user title.
Status Message	The status message for the user
Account Type	The type of account the user has.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the user was last updated.
Timezone	The timezone that the user is in.

Slack Workspaces

Description	Slack Workspaces contains information about each of the workspaces that the local user is apart of.
Notes	

ATTRIBUTE	DESCRIPTION
ID	The unique identifier for the slack workspace.
Name	The name of the slack workspace.
Domain	The domain of the slack workspace.
Local User ID	The unique identifier of the local user.
Local User	The name of the local user.
Local User Display Name	The display name of the local user.
Local Email Address	The email address of the local user.
Password/Token	The local user password/token.

TamTam Messenger Channels - Android

Description	TamTam Messenger Channels contains messages that belong to channel conversations recovered from the local device (the channel type must be User Channel or Default Channel).
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The name of the channel in which the message originated.
Sender ID	The TamTam ID of the channel in which the message originated.
Recipient	The display name of the owner contact that received the message.
Recipient ID	The TamTam ID of the owner contact that received the message
Message	The content of the message. If the messages is a contact share, this attribute displays the text from the VCard.
Message Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp of the message.
Status	The delivery status of the message: Sent or Received.
Channel Type	The classification of the Channel. Channels created by TamTam users are displayed as 'User Channel' whereas 'Default Channel' describes channels that are created and managed by Tamtam. TamTam user are automatically signed up to some of these channels upon application download.
Message Type	The type of message content (Text, Picture, Audio, Video, File, Call, Geo Location or Contact Share). If the message is not in one of these formats, this attribute is empty.
Latitude	The latitude coordinate, if the message type is Geo location.
Longitude	The longitude coordinate, if the message type is Geo location.

ATTRIBUTE	DESCRIPTION
Attachment URL	A URL for any attachments that are sent or received. Attachments can be downloaded from this URL. However, to recover pictures properly, you must append '&fn=w_1440' manually to the end of the URL.
Attachment	The locally stored attachment, if the attachment was sent by the local user.

TamTam Messenger Contacts

Description	TamTam Messenger Contacts displays information about the TamTam contacts associated with the local user's account (including the local user).
Notes	

ATTRIBUTE	DESCRIPTION
Contact ID	A unique ID for the contact.
Profile Name	The profile name of the contact.
Website URL	The contact's TamTam website URL, if one exists.
About Info	Information that the user has provided about their self.
Avatar URL	A URL to the user's profile picture. A termination '&fn=w_1440' should be manually added to the URL to properly display the picture.
Updated Date/Time - UTC (yyyy-mm-dd)	The last time that the contact was updated on the local device. If the contact was not added by the local user, this does not display a value. Some contacts might be stored on the local user's device and may have not been added to their contact list. For example, this might occur when the local user belongs to a group but does not have all of the group participants as contacts. In these cases, TamTam adds the group contacts to the application database but they won't automatically be updated.

TamTam Messenger Conversations - Android

Description	TamTam Messenger Conversations contains information about all the chats recovered from the local device (includes individual, group, and channel messages).
Notes	

ATTRIBUTE	DESCRIPTION
Chat ID	A unique ID for the conversation.

ATTRIBUTE	DESCRIPTION
Chat Type	The type of conversation (Individual, Group, User Channel and Default Channel). Individual indicates one-to-one conversations, while Group indicates many-to-many conversations. User Channel indicates a one-to-many conversation created by a TamTam user. Default Channels are one-to-many conversations created and managed by TamTam.
Participants	A list of the participants that belong to the conversation. User Channels only display the local user as a participant whereas Default Channels do not display any participants.
Chat Name	The name of the conversation (only available in Groups and Channels).
Description	The description of the conversation (only available in Groups and Channels)
Address URL	The URL for the channel's webpage. Users can sign up to the channel using this page if the channel is public.

TamTam Messenger Groups - Android

Description	TamTam Messenger Groups contains all messages that belong to group conversations recovered from the local device.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The display name of the contact who sent the message.
Sender ID	The TamTam ID of the contact who sent the message. If the contact ID is not recovered, this attribute displays the chat ID of the conversation that the message belongs to.
Recipient	The name of the owner user who received the message.
Recipient ID	The TamTam ID of the owner user who received the message.
Message	The content of the message. If the messages is a contact share, this attribute displays the text from the VCard.
Message Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp of the message.
Status	The delivery status of the message: Sent or Received.
Message Type	The type of message content (Text, Picture, Audio, Video, File, Call, Geo Location or Contact Share). If the message is not in one of these formats, this attribute is empty.
Latitude	The latitude coordinate, if the message type is Geo location.
Longitude	The longitude coordinate, if the message type is Geo location.
Attachment URL	A URL for any attachments that are sent or received. Attachments can be downloaded from this URL. However, to recover pictures properly, you must append '&fn=w_1440' manually to the end of the URL.
Attachment	The locally stored attachment, if the attachment was sent by the local user.

TamTam Messenger Messages - Android

Description	TamTam Messenger Messages contains all individual messages (one-to-one) recovered from the local device.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The display name of the contact who sent the message.
Sender ID	The TamTam ID of the contact who sent the message. If the contact ID is not recovered this attribute displays the chat ID of the conversation that the message belongs to.
Recipient	The display name of the contact, group or channel that received the message.
Recipient ID	The TamTam ID of the contact, group or channel that received tha message.
Message	The content of the message. If the messages is a contact share, this attribute displays the text from the VCard.
Message Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp of the message.
Status	The delivery status of the message: Sent or Received.
Message Type	The type of message content (Text, Picture, Audio, Video, File, Call, Geo Location or Contact Share). If the message is not in one of these formats, this attribute is empty.
Latitude	The latitude coordinate, if the message type is Geo location.
Longitude	The longitude coordinate, if the message type is Geo location.
Attachment URL	A URL for any attachments that are sent or received. Attachments can be downloaded from this URL. However, to recover pictures properly, you must append '&fn=w_1440' manually to the end of the URL.
Attachment	The locally stored attachment, if the attachment was sent by the local user.

Textfree Attachments

Description	Textfree Attachments contains Attachments from the Android Textfree application.
Notes	The Metadata column is always empty for the Android version of the application.

ATTRIBUTE	DESCRIPTION
Message ID	The ID of the message.
Media URL	The URL from where the media could originaly be downloaded.
Type	The type of media (including picture, voicemail and video).

ATTRIBUTE	DESCRIPTION
Preview	The binary data of the attachment. If the attachment is a video, the preview is a frame from the video.
Metadata	Any metadata associated with the attachment. An example of this is VoicemailDuration.
Media ID	The internal ID used by the application. This value may point to other places where the attachment is used and/or contained.

Textfree Contacts

Description	Textfree Contacts contains contacts from the Android Textfree application.
Notes	Company Name, Email(s), Last Modified Date/Time will always be empty for the Android version of the application.

ATTRIBUTE	DESCRIPTION
First Name	The first name of the contact.
Last Name	The last name of the contact.
Company Name	The company name of the contact.
Phone Numbers	All phone numbers associated with the contact.
Email(s)	All emails associated with the contact.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that the contact was modified.
Contact ID	The internal ID used by the application. This value may point to other places where the attachment is used and/or contained.

Textfree Groups

Description	Textfree Groups contains information about group chats from the Android Textfree application.
Notes	The Group Name column will always be empty for the Android version of the application.

ATTRIBUTE	DESCRIPTION
Group	The group number.
Group Name	The name of the group.
Group Phone Number	The phone number of the group.
Group Member Name(s)	The names of all of the group participants.
Group Member Phone Number(s)	The phone numbers of all of the group participants.

Textfree Messages

Description	Messages from the Android Textfree application.
Notes	The Sender ID column is always left empty for Android.

ATTRIBUTE	DESCRIPTION
Message Partner	The name of the message partner.
Message Partner ID	The ID of the messaging partner. This value may contain the contact's phone number.
Sender Name	The name of the sender.
Sender ID	The ID of the sender.
Message ID	The ID of the message. This value can be used to find related attachments in the TextFree Attachments table.
Message Body	The content of the message.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that is associated with the message.
Attachment Type	The type of media file (for example: jpeg, png, wav).
Media URL	The URL from where the media could originally be downloaded.
Media ID	The internal ID used by the application. This value may point to other places where the attachment is used or contained, or both.
Read	The read status of the message.
Call Duration (Seconds)	The call duration in seconds, if the message is a call.

TextMe Calls

Description	TextMe Calls contains information about the calls that the suspect participates in using the TextMe application.
Notes	In some versions of TextMe, call logging does not behave as expected. If a suspect sends or receives a call, a database entry is created as normal. If another call occurs with the same user, without there being any messages in between, the timestamps from the first call are overwritten in the database with the timestamps from the second call. This behavior makes it seem as if the first call never occurred. The timestamps are repeatedly overwritten for each call until a message is sent, at which point a new database entry can be created for the next new call. For Android TextMe Calls, it is not possible to determine the display name of the recipient, so the 'Display Name' column will always be empty.

ATTRIBUTE	DESCRIPTION
Sender	The sender of the call.

ATTRIBUTE	DESCRIPTION
Recipient	The recipient of the call.
Display Name	The chosen display name for the call participant.
Call Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the call was initiated.
Call End Date/Time - UTC (yyyy-mm-dd)	The date and time when the call ended.
Direction	The direction of the call, either incoming or outgoing.
Status	Whether the call was unanswered, answered, or if the caller left a voicemail.
Call Type	Indicating if the call was an audio call or video call.
Voicemail	The associated voicemail message.

TextMe Messages

Description	TextMe Messages contains individual chat messages that are sent and received using the TextMe application.
Notes	

ATTRIBUTE	DESCRIPTION
Conversation Partner	The name of the other participant in the conversation. In some cases, when the owner of the device cannot be retrieved, this value is returned as "[sender], [recipient]".
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent, regardless of whether the message was sent or received.
Message	The body of the message.
Direction	Whether the message was sent or received.
Status	Whether the message was unsent, sent, delivered, or read.
Attachment Name	The name of the attachment, if one exists (can be pictures, videos, or URL links).
Attachment Path	The file path of the attachment, if one exists.
Attachment	The attachment data.

TextPlus Calls

Description	TextPlus Calls contains call information from TextPlus data on an Android device.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The username of the TextPlus account.
User	The identifier for the recipient of the call. This could be a GUID or phone number depending on the TextPlus version.
Display Name	The display name of the TextPlus account.
Date/Time - UTC (yyyy-mm-dd)	The date and time that the call was made.
Duration (Units Unknown)	The duration of the call (can be in milliseconds or seconds). To determine which unit of duration is being used, human inspection is required.

TextPlus Messages

Description	TextPlus Messages contains message information from TextPlus data on an Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Sender Name	The sender of the message.
Sender	The identifier for the sender of the message. This could be a GUID or phone number depending on the TextPlus version.
Recipient Name	The recipient of the message.
Recipient	The identifier for the recipient of the message. This could be a GUID or phone number depending on the TextPlus version.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent or received.
Message Body	The text contents of the message.
Message Type	Indicates if the message is incoming, outgoing, or an unknown message type.
Status	Indicates if the message was read ('Read'), unread ('Unread') or has an unknown status.

Touch Experiences

Description	Touch Experiences contains experiences in the Android Touch application. Similar to photo albums on Facebook except more private, users can post media to an experience and share it with friends, who can comment on the posted media and share media of their own.
Notes	

ATTRIBUTE	DESCRIPTION
Experience Name	The name of the experience.
Author	The author of the post.
Comment	A comment on the content of the experience. This comment can be seen by other users viewing the experience.
Media URL	The URL of a media item posted to the experience.
Status	The status of the post. Describes whether it was sent or received, and whether or not it was viewed/downloaded by the local user.
Downloaded Image	The raw content of the media in the post, downloaded from the URL specified in 'Media URL'.
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the post was sent/received.
Experience Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the experience was created.
Experience Owner	The user who created the experience.
Experience Members	All of the members in the experience.

Touch Friends

Description	Touch Friends contains contact information for friends of the local user in the Android Touch application.
Notes	

ATTRIBUTE	DESCRIPTION
First Name	The friend's first name.
Last Name	The friend's last name.
Touch ID	The friend's unique Touch ID.
Avatar URL	The URL of the friend's avatar.
Downloaded Image	The raw content of the friend's avatar, downloaded from the URL specified in 'Avatar URL'.

Touch Local User

Description	Touch Local User contains contact information for the local user in the Android Touch application.
Notes	

ATTRIBUTE	DESCRIPTION
First Name	The local user's first name.
Last Name	The local user's last name.
Touch ID	The local user's unique Touch ID.
Avatar URL	The URL of the local user's avatar.
Downloaded Image	The raw content of the local user's avatar, downloaded from the URL specified in 'Avatar URL'.

Touch Messages

Description	Touch Messages contain messages that were sent and received in the Android Touch application.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the message.
Recipients	The recipient(s) of the message. In a group conversation, recipients will be in a comma-delimited list.
Message Type	A phrase describing the content of the message. The possible values are 'Text', 'Image', 'Audio', 'Video', and 'Profile Picture Changed'.
Message	The content of the message.
Message Status	The status of the message. This value describes whether the message was sent or received by the local user, and describes the interactions that the user has had with it: whether or not it was viewed, or, in the case of media, whether or not it was downloaded.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Media URL	The URL of the media in the message, if it contains video, audio or an image.
Downloaded Image	The raw content of the media in the message, downloaded from the URL specified in 'Media URL'.
Local Media Path	The path to the content of the media in the message on the local phone.

Verizon Messages Messages

Description	Verizon Messages contains information about the messages sent or received by the local user.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The phone number of the device that sent the message.
Recipient(s)	The phone numbers of the devices that received the message.
Message Direction	Indicates whether the message was incoming or outgoing. If the direction is not recognized, the value will be an integer.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message	The text for the message.
Attachment Name	The attachment file name.

Viber Messages

Description	Viber Messages contains details about sent/received Android Viber messages.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the message.
Recipient(s)	The recipient(s) of the message. In a group chat, the recipients will be shown as a comma-delimited list.
Participant	The contact name of one of the participants of the record. It is up to the investigator to determine if this is the local user, or that of the chat partner.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The message that was sent. If the message type was a call this will identify if the call was outgoing, incoming or a missed call. For locations the message is a google maps link to the sent location. For images the message can be empty or a blurb of text.
Message Type	Identifies the type of message sent. The possible types are Text, Sticker, Call, Video, Location, Notification, or Image.
Message Status	The status of the message. This can be one of the following: 'Sent / Failed', 'Sent / Not Delivered', 'Sent / Delivered', or 'Received'.
Secret Chat	Indicates whether a message is sent in a secret chat (Yes if true).
Expiration	If the message is a secret chat message, this value represents the time limit that the message can be visible for before it disappears. The value is converted from seconds and reported as a timestamp in dd:hh:mm:ss format.
Repeat Count	If the message was a call, the number of times that the call was repeated.
File Path	If the message included an attachment, the path to the attachment on the local phone, in the form of a URL.

ATTRIBUTE	DESCRIPTION
Location Address	The address for the location that was sent.
Latitude	The map latitude location information.
Longitude	The map longitude location information.
Nearby Locations	The locations that are geographically close to the user when they use the Share Location feature within the application (these locations are cached even if a location is not actually shared).

WeChat Friends

Description	WeChat Friends contains stored contact information for the WeChat application on Android.
Notes	

ATTRIBUTE	DESCRIPTION
Username	The unique username of the friend.
MD5 Hashed Username	The MD5 hash of the friend's username.
Nickname	The nickname of the friend.
Gender	The friend's gender.
Phone Number	The friend's phone number.
Email	The friend's email address.
Full Name	The friend's full name.

WeChat Messages

Description	WeChat Messages contains stored messages for the WeChat application on Android.
Notes	

ATTRIBUTE	DESCRIPTION
Sender Username	The username or ID of the sender, as assigned by the application.
Sender Nickname	The display name of the sender, as defined by the user.
Recipient Username	The username of the person receiving the message.
Recipient Nickname	The nickname of the person receiving the message.
Group Chat Name	The name of the group chat, if the message is sent in a group chat.
Group Chat ID	The unique ID of the group chat, if the message is sent in a group chat.

ATTRIBUTE	DESCRIPTION
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was created on the device.
Message	The content of the message.
Image	The image attachment associated with the message.
File	The non-image attachment (such as audio, video) associated with the message.
Call Duration (Seconds)	The duration of voice and/or video call in seconds.
Type	The type of message, such as text, audio, and video.
Latitude	The latitude of the location data sent within the message.
Longitude	The longitude of location data sent within the message.
Attachment Path	The absolute path to the attachment associated with the message, if any were recovered.

WhatsApp

WhatsApp is a cross-platform mobile messaging app that is owned by Facebook and has over a billion registered users as of 2016. Magnet tools support the recovery of messages, contacts, and attachments from WhatsApp conversations on both Android and iOS. Information from these artifacts can help investigators identify who a user communicates with and what they talk about. This information can be important to many different types of investigations.

Artifacts

RELATED RESOURCES

Artifact Profile: WhatsApp Messenger

Android WhatsApp Chats

Description	WhatsApp Chats contains information about chat sessions that occur between the local user and another user or group. This artifact indicates the IDs of each participant as well as information about unread messages and the time when the last message was sent.
Notes	

ATTRIBUTE	DESCRIPTION
Individual Chat Name	If the chat is with an individual, this value indicates the name of the participant.
Group Chat Name	If the chat is a group chat, this value indicates the name of the group.
Chat ID	The ID of the individual or group involved in the chat.
Phone Number	The phone number associated with an individual contact.
Last Message	The text body of the last message sent in the chat.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time that the last message in the chat was sent.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the conversation was created.
Unread Message Count	The number of unread messages in the chat.
Missed Call Count	The number of missed calls in the chat.

Android WhatsApp Contacts

Description	Android WhatsApp Contacts contains contacts that were added to WhatsApp by the local user.
Notes	

ATTRIBUTE	DESCRIPTION
Image	The actual picture content.
ID	The unique identifier for the contact.
Phone Number	The contact's phone number.
Display Name	The contact's full name.
Given Name	The contact's given (i.e. first) name.
Family Name	The contact's family (i.e. last) name.
WhatsApp Name	The contact's name that is displayed to other users.
Status	The contact's status message.
Status Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the status message was updated.
Is WhatsApp User	Identifies whether the user is using WhatsApp or not.
Frequently Contacted	Indicates whether this contact is contacted frequently by the user.

Android WhatsApp Groups

Description	Android WhatsApp Groups contains information about the WhatsApp Group chats that the user participates in.
Notes	

ATTRIBUTE	DESCRIPTION
Picture	The profile picture associated with this group.
Group Chat ID	The unique identifier for group chats. The Group Chat ID format is creator phone number-creation epoch time@g.us.
Description	The description of the group.
Group Name	The name of the group that is seen by users in the chat list and the conversation view.
Admin IDs	The IDs of the administrators of the group chat.
Admin Names	The names of the administrators of the group chat.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the group was created.
Group Member(s)	The list of contact IDs for the members of the group.

Android WhatsApp Live Locations

Description	Android WhatsApp Live Locations captures Live Locations that are shared with the local device user. The coordinates in each result represent the sender's last shared location. Once a Live Location expires, it is no longer recoverable.
Notes	

ATTRIBUTE	DESCRIPTION
ID	The user ID of the contact that is sharing their live location.
Phone Number	The phone number of the contact.
Date Time - UTC (yyyy-mm-dd)	The date and time when the live location coordinate was captured.
Latitude	The latitude associated with the live location.
Longitude	The longitude associated with the live location.
Speed (m/s):	The speed of the contact at the time the live location was captured.
Direction	The direction of travel for the contact at the time the live location was captured.

Android WhatsApp Messages

Description	Android WhatsApp Messages contains messages that were sent and received using WhatsApp.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The phone number of the message sender.
Sender Nickname	The name of the message sender, retrieved from display_name.
Receiver	The phone number of the message recipient.
Receiver Nickname	The name of the message recipient, retrieved from display_name.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Message Received Date/Time - UTC (yyyy-mm-dd)	The date and time the message was received locally.
Server Received Date/Time - UTC (yyyy-mm-dd)	The date and time the message was received by the server.
Recipient Received Date/Time - UTC (yyyy-mm-dd)	The date and time the message was received by the remote recipient.
Message	The message text.
Type	The format of the message or the MIME type of the media attachment.
Chat Type	Defines the audience for the message/call. 'Individual' indicates one-on-one messages/calls, 'Group' indicates that the message/call involves more than one user, and 'Broadcast' indicates a message with multiple recipients.
Media Duration (Seconds)	The duration of the attached media.
Call Duration (Seconds)	The duration of the audio/video call.
Message Status	The sent/received status.
Latitude	The latitude of the location from which the message was sent.
Longitude	The longitude of the location from which the message was sent.
Thumbnail	The thumbnail of the media attached to the message. This can be a picture, video, or map.
Attachment	The media attached to the message.
Media URL	The source URL of the attached media.
Starred	Indicates whether the user bookmarked (or 'starred') a message.

ATTRIBUTE	DESCRIPTION
Forwarded	Indicates whether the user forwarded a message to another conversation

Android WhatsApp Profile Pictures

Description	Android WhatsApp Profile contains profile pictures that WhatsApp uses that are stored locally.
Notes	

ATTRIBUTE	DESCRIPTION
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date/time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date/time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date/time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. "Complete" indicates that a full Exif extraction was performed. "Failed" indicates that the information may have been corrupted and could not be recovered. "Skipped" indicates that the extraction was skipped.

ATTRIBUTE	DESCRIPTION
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera that was used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
Longitude	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

Android WhatsApp User Profiles

Description	WhatsApp User Profiles contains profile information about the local WhatsApp user.
Notes	

ATTRIBUTE	DESCRIPTION
Image	The user's profile image.
WhatsApp Name	The WhatsApp username that is associated with the account.

ATTRIBUTE	DESCRIPTION
Phone Number	The phone number used to register the account.
Status	The current status that the user shares
Version	The version of the WhatsApp application.
Latitude	The latitude associated with the last location the user shared.
Longitude	The longitude associated with the last location the user shared.
Private Key	The decryption key of the account.

WhatsApp Accounts Information

Description	WhatsApp Accounts Information Contains the login information for the user's account, including the private key used for authentication.
Notes	

ATTRIBUTE	DESCRIPTION
WhatsApp Name	The WhatsApp username that is associated with the account.
Phone Number	The phone number used to register the account.
Private Key	The decryption key of the account.

Wickr Me

Wickr Me is a private messaging application for iOS and Android, which provides end-to-end encryption of user communications, including texts, audio and video calls, transmitted locations and more. To ensure the security of your messages, Wickr Me encrypts every sent message with a unique key and gives you the option to control how long these messages will remain available to a recipient once read.

The content of a suspect’s sent and received messages can be valuable to an investigation, as well as their username and the usernames of their recipients. Other information can also be recovered, such as the date and time of when messages were sent, delivered and read, and a suspect's shared locations. This information can offer insight into the purpose of a suspect’s interactions, identify users who have been in contact with a suspect, and can be used to piece together a timeline of a suspect’s activity.

Decrypting messages

On Android, Wickr Me application data is stored in the SQLite database (wickr_db), which is fully encrypted using SQLCipher. Magnet AXIOM Process will search .wic files and Android system files for the components needed to recover the database decryption key.

Artifacts

Wickr Me Messages

Wickr Me Messages - Android

Description	Wickr Me Messages contains decrypted and decoded messages sent or received by a Wickr Me user on Android. These messages can include text messages, call logs, transmitted locations, attachments, voice messages, and more.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender's Wickr Me username.
Recipient	The recipient's Wickr Me username.
Message Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message	The message content.
Direction	Indicates whether the message was incoming or outgoing.
Read	Indicates whether the message was read.
Call Status	The status of the call, if applicable. The different statuses are 'Started', 'Completed', 'Missed' or 'Cancelled'.
Attachment Name	The file name of the attachment included in the message, if applicable.
Attachment	The decrypted attachment file, if applicable (can include photos, videos or voice messages).
Latitude	The latitude of the coordinates (for transmitted locations only).
Longitude	The longitude of the coordinates (for transmitted locations only).

Your Phone Companion Info

Description	Your Phone Companion Info contains information about the computers that are synced to the local device using Your Phone, and information about the types of data are synced from device to computer.
Notes	

ATTRIBUTE	DESCRIPTION
Application Version	The version of the Your Phone Companion application running on the device.

ATTRIBUTE	DESCRIPTION
Registered Date/Time - UTC (yyyy-mm-dd)	The date and time that the application was registered with Your Phone (this value should correspond to the install date).
Remote IDs	GUID identifiers generated within Your Phone to uniquely identify the remote computers this device synchronizes with.
Remote Computer Names	The names of the remote computers that this device synchronizes with.
Photo Sync Enabled	Indicates whether photos are synchronized between the device and the remote computer.
MMS Messages Enabled	Indicates whether MMS messages are synchronized between the device and the remote computer.
MMS Media Enabled	Indicates whether media sent via MMS are synchronized between the device and the remote computer.
SMS Messages Enabled	Indicates whether SMS messages are synchronized between the device and the remote computer.
Messaging Enabled	Indicates whether sending SMS/MMS messages using Your Phone on the remote computer is enabled.
Last Login Date/Time - UTC (yyyy-mm-dd)	The last time that the application signed in to the Your Phone servers (this value may not correspond to a user-initiated event).
Application Run Count	The number of times that the application has run.
Remote User Display Name	The display name of the user account on the remote system, which is typically the user's Windows account.
Remote Username	The username on the remote system, which is typically the user's Windows account.
Remote User ID	The user ID on the remote system, which is typically the user's Windows live account ID.
User First Seen Date/Time - UTC (yyyy-mm-dd)	The first time that the user entered the Your Phone ecosystem. This value may not correspond to the registered date if Your Phone was previously installed on other devices.

Zalo Contacts

Description	Zalo Contacts contains the user's Zalo contacts.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The contact's username.
User ID	The contact's unique user ID.
Profile Picture URL	The contact's profile picture URL.
Gender	The contact's gender.

ATTRIBUTE	DESCRIPTION
Phone Number	The contact's phone number.
Birthday (yyyy-mm-dd)	The contact's birthday.
Status	The contact's status message.
Last Activity Date/Time - UTC (yyyy-mm-dd)	The date and time when the contact was last active.
Is Friend	If the contact is friends with the user.
Type	The contact's type of account.

Zalo Groups

Description	Zalo Groups contains Zalo groups that the user participates in.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the group.
ID	The unique ID of the chat group.
Created By	The username of the person who created the chat room.
Group Members	The usernames of all of the members in the group.
Number of Participants	The number of participants in the group.

Zalo Messages

Description	Zalo Messages contains messages or calls sent or received using Zalo.
Notes	

ATTRIBUTE	DESCRIPTION
Sender User Name	The username of the person sending the message.
Recipient User Name	The username of the person receiving the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent on the device.
Direction	The direction that the message was sent.
Message	The content of the message.
Picture	Any picture attachments in the message.
Attachment	Any non-picture attachments in the message, including audio and video.

ATTRIBUTE	DESCRIPTION
Duration (Seconds)	The duration of calls.
Status	The status of calls. The status of some calls is ambiguous as it's not possible to distinguish whether calls are accepted or ended by the user receiving the call.
Message Type	The type of message. The different message types include text, audio, video and more.
Latitude	The latitude data sent within a message.
Longitude	The longitude data sent within a message.
Media URL	The URL of additional media attachments.
Attachment Path	The absolute path to recovered attachments in a message.

Zalo Profiles

Description	Zalo Profiles contains profile information of the local Zalo user.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The user's username.
User ID	The user's unique user ID.
Profile Picture URL	The user's profile picture URL.
Gender	The user's gender.
Birthday (yyyy-mm-dd)	The user's birthday.
Phone Number	The user's phone number.
Status	The user's status message.

Zoom Channels

Description	Zoom Channels contains information about the channels that the local user participates in.
Notes	

ATTRIBUTE	DESCRIPTION
Channel ID	The ID of the channel.
Channel Name	The display name of the channel.
Owner ID	The ID of the Zoom user that created the channel.
Participant IDs	The IDs of the participants of the channel.
Participant User Names	The names of the participants of the channel.
Description	A description of the channel, as provided by the creator of the channel.

Zoom Chat Messages

Description	Zoom Chat Messages contains details about Zoom chat messages sent outside of a meeting.
Notes	The Attachment Name column is always empty on Android.

ATTRIBUTE	DESCRIPTION
Sender Name	The name of the person who sent the message.
Sender ID	The ID of the person who sent the message.
Buddy ID	The ID of the person or group that the message was sent to.
Recipient Name	The name of the person who received the message.
Recipient ID	The ID of the person who received the message.
Group Chat ID	The ID of the group this message was sent in.
Message ID	The GUID of the message.
Message	The body of the message.
Message Date/Time - UTC (yyyy-mm-dd)	A timestamp that indicates when the message was sent or received, depending on whether the local user was the sender or receiver.
Sender	Whether the message was sent by the local user or a remote user.
Read	Specifies whether the message has been read. The displayed value is either 'Yes' or 'No'.
Message Type	The type of message that was sent. The message types are 'Message', 'Picture', 'File', or 'Notification'.
Attachment Name	The name of the attachment that was sent.
Attachment Local File Path	The local path where the attachment was saved. This is empty if the attachment was not saved.
Attachment	The contents of the attachment if it can be recovered.

Zoom Contacts

Description	Zoom Contacts contains information about a user's Zoom contacts.
Notes	

ATTRIBUTE	DESCRIPTION
Buddy ID	The user ID of the contact.
Email	The email address of the contact.
Display Name	The display name of the contact.
Description	A description of the contact, as provided by that user.

ATTRIBUTE	DESCRIPTION
Personal Meeting ID	An ID that can be used to start up a meeting with the contact.
Region	The default country or region where the contact is located.

Zoom Meeting Messages

Description	Zoom Meeting Messages contains details about Zoom chat messages sent during a meeting.
Notes	

ATTRIBUTE	DESCRIPTION
Message ID	The GUID of the message.
Sender Name	The name of the person who sent the message.
Sender ID	The ID of the person who sent the message.
Receiver Name	The name of the person who received the message. If blank, the message was sent to everyone in the meeting.
Receiver ID	The ID of the person who received the message. If zero, the message was sent to everyone in the meeting.
Message	The body of the message.
Message Date/Time - UTC (yyyy-mm-dd)	A timestamp that indicates when the message was sent or received, depending on whether the local user was the sender or receiver.
Sender	Whether the message was sent by the local user or a remote user.
Read	Specifies whether the message has been read. The displayed value is either 'Yes' or 'No'.
Message Type	The type of message that was sent.
Conference ID	The ID for the meeting the message was sent in.

Zoom User Accounts

Description	Zoom User Accounts contains details about the local user's zoom account.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The unique identifier for the user.
User Name	The username of the account.
Email	The email address associated with the account.
First Name	The first name of the user.

ATTRIBUTE	DESCRIPTION
Last Name	The last name of the user.
Phone Number	The phone number of the user.
Profile Image URL	The URL to the profile picture of the user.
Downloaded Profile Image	The data for the profile picture.

Cloud

Android Dropbox

Description	Android Dropbox contains Dropbox file information recovered from a Kindle device.
Notes	

ATTRIBUTE	DESCRIPTION
File Path	The path to the file.
Updated File Name	The name of the file/folder being updated.
Local Modified Date/Time - UTC (yyyy-mm-dd)	The local date and time that the file/folder was modified.
Updated Modified Date/Time - UTC (yyyy-mm-dd)	The updated date and time that the file/folder was modified.
Displayed Modified Date/Time	The displayed modified date and time.
Local File Size (Bytes)	The size of the file on the local machine.
Updated File Size (Bytes)	The updated size of the file.
Favorited	Indicates whether or not the file has been favorited.
File Version	The file version.

Android Dropbox Account Info

Description	Android Dropbox Account Info contains Dropbox account information recovered from a Kindle device.
Notes	

ATTRIBUTE	DESCRIPTION
Display Name	The Dropbox user account display name.
User ID	The Dropbox user account ID.
Country	The country that the user account is set for.

ATTRIBUTE	DESCRIPTION
Email	The email address associated with the account.

Cloud Storage

MEGA Accounts

Description	MEGA Accounts contains information about the accounts that the local user has logged in with on the device.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user ID of the local user.
Email Address	The email address of the local user.
First Name	The first name of the local user.
Last Name	The last name of the local user.
Summary	A summary of the the local user.

MEGA Chat

Description	MEGA Chat contains messages sent and received by the local user.
Notes	

ATTRIBUTE	DESCRIPTION
Sender ID	The ID of the sender.
Sender Email	The email address of the sender.
Sent Date/Time	The date and time that the message was sent.
Message Body	The body of the message.
Recipient ID	The user ID of the recipient.
Recipient Email	The email address of the recipient of the message.
Message Type	The type of the message.
Attachment Name	The file name of the attachment in a message.

MEGA Contacts

Description	MEGA Contacts contains information about MEGA users that have communicated with the local user account.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user ID of the contact.
Email Address	The email address of the contact.
First Name	The first name of the contact.
Last Name	The last name of the contact.

Documents

Evernote Accounts

Description	Evernote Accounts contains information about the user accounts that have been used to log in on the device.
Notes	

ATTRIBUTE	DESCRIPTION
Local User Display Name	The display name of the local user's account.
User ID	The user ID of the local user.
Created Date/Time	The date and time when the local user's account was created.
Login Date/Time	The date and time when the account was initially logged into on the device.

Evernote Contacts

Description	Evernote Contacts contains information about users that have communicated with the local user account.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user ID of the contact.

ATTRIBUTE	DESCRIPTION
Contact ID	The contact ID of the contact.
Account Name	The account name of the contact.

Evernote Notes

Description	Evernote Notes contains any notes associated with the local user, including notes shared from other users to the local user.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the note.
Content	The content of the note.
Type	The type of note.
File Name	The name of the attachment that was included with the note.
Created Date/Time	The date and time when the note was created.
Updated Date/Time	The date and time when the note was updated.
Deleted Date/Time	The date and time when the note was deleted.
Owner	The owner of the note. If a note is shared from one user to another, the owner is the user that shared the note.
Shared With	The accounts that the note was shared with.
Last Modifier Name	The username of the last modifier of the note.
Start Date/Time	The date and time of the starting time for the reminder of the note.
End Date/Time	The date and time of the end time for the reminder of the note.
Location	The location where the note was taken.
Longitude	The longitude of the location where the note was taken.
Latitude	The latitude of the location where the note was taken.
Notebook Name	The name of the notebook where the note was saved.

Evernote Work Chat

Description	Evernote Work Chat contains messages sent and received by the local user.
Notes	

ATTRIBUTE	DESCRIPTION
Sender ID	The unique ID of the sender.
Sender Name	The name of the sender.
Sent Date/Time	The date and time when the message was sent.
Message Body	The body of the message.
Participants	The participants of the chat.
Participant IDs	The IDs of the participants of the chat.

Excel Documents

Description	Microsoft Excel is a spreadsheet processor developed by Microsoft.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Extremely large documents may not be fully recovered.
File	The actual file.
Title	The title metadata.
Subject	The subject metadata.
Authors	The authors of the document.
Keywords	The keywords in the metadata of the document.
Comments	The comments metadata.
Last Author	The last author to edit the document.
Last printed Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last modified, extracted from metadata within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created, extracted from metadata within the document.

ATTRIBUTE	DESCRIPTION
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

Hangul Word Processor

Description	Hangul Word Processor specifies information about files that were created using Hangul Word Processor.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the found file.
Password Required	Indicates whether the file requires a password to be opened.
Application Version	The version of the software used to create the file.
Preview Text	A preview of the file content that contains the first 1024 symbols.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was modified on the filesytem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was accessed on the filesytem.
File System Last Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was created on the filesytem.
Title	The title field of the document.
Subject	The subject field of the document.
Author	The author field of the document.
Date String	The date field of the document.
Keyword	The keyword field of the document.
Additional Information	Any additional information that the author provided for the document. Appears as 'Other' field in the software.
Last Saved By	The username of the last user that saved the file.
Document Created Date/Time - Local Time (yyyy-mm-dd)	The date and time when the file was originally created.
Preview Image	An image preview of the title page of the file.

PDF Documents

Description	Portable Document Format (PDF) is a file format used to present documents in a manner independent of application software, hardware, and operating systems. This table captures documents in this file format, extracted from the filesystem and carved from unallocated space.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
Title	The title of the file.
Subject	The subject of the file.
Authors	The authors of the file.
Keywords	The keywords in the metadata of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last modified, extracted from metadata within the document.
File	The PDF file.
MD5 Hash	An MD5 hash of the PDF content.
SHA1 Hash	A SHA1 hash of the PDF content.

PowerPoint Documents

Description	Micrsoft PowerPoint is a presentation creator developed by Microsoft. This table captures documents created with PowerPoint, extracted from the filesystem and carved from unallocated space.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
File	The actual file.
Title	The title of the file.
Subject	The subject of the file.
Authors	The authors of the file.
Keywords	The keywords in the metadata of the file.
Comments	The comments in the metadata of the file.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last modified, extracted from metadata within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created, extracted from metadata within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

RTF Documents

Description	RTF Documents contains information for each RTF document that was recovered from the search.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the RTF document.
File Size (Bytes)	The size of the RTF document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the RTF document was created.

ATTRIBUTE	DESCRIPTION
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the RTF document was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the RTF document was last modified.
File Content	The contents of the RTF document.

Text Documents

Description	Text documents (.txt) that are located on the system.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the text document.
Size (Bytes)	The size of the text document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the text document was last modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the text document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the text document was created.

Thinkfree Office Viewer Files

Description	Thinkfree Office Viewer Files contains information about the files that the user has opened using Thinkfree Office Viewer. Even if the user has deleted the file from the device, this artifact can still recover information about the file if they opened it in the viewer.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file that was opened in Thinkfree Office Viewer.
File Size (Bytes)	The size of the file.
File System Created Date/Time	The date and time when the file was created on the filesystem.
Favorited	Indicates whether the file has been made a favorite.
File Path	The path to the local file.

Word Documents

Description	Microsoft Word is a word processor developed by Microsoft.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last modified on the filesystem.
Size (bytes)	The size of the document.
Saved Size (bytes)	The size of the document that was recovered. Extremely large documents may not be fully recovered.
File	The actual file.
Title	The title metadata.
Subject	The subject metadata.
Authors	The authors of the document.
Keywords	The keywords metadata in the document.
Comments	The comments metadata.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time that the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the document was last modified, extracted from metadata within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the document was created, extracted from metadata within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

E-mail

Android Emails

Description	Android Emails contains the email fragments that were recovered from an Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	Who sent the email.
Recipients	Who the email was sent to.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the email.
Subject	The subject of the email.
CC	Who was CC'd on the email.
BCC	Who was BCC'd on the email.
Email Body	The body of the email
Sync Server Date/Time - UTC (yyyy-mm-dd)	The date and time that the server synchronized the email.
Status	Identifies if the email was read or unread.
Attachments	The attachments in the email.

Android Gmail Conversations

Description	Android Gmail Conversations contains information about email conversations between the local user and others, as recovered from an Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Conversation Date/Time - UTC (yyyy-mm-dd)	The date and time when the first message in the conversation was sent.
Subject	The subject of the conversation.
Snippet	A snippet of text from the first message in the conversation.
Attachments	Any attachments that were sent during the conversation.
Permanent Link	A URL to the conversation.

Android Yahoo Mail Attachments

Description	Android Yahoo Mail Attachments contains attachments from emails stored by the Android Yahoo Mail application.
Notes	

ATTRIBUTE	DESCRIPTION
Message ID	The database key for the message. This key can be used to match up an attachment with an email found in Android Yahoo Mail Emails.
Attachment Name	The file name of the attachment.
Thumbnail URL	The URL of the thumbnail of the image attachment, if applicable.
Original Saved Location	The path at which this attachment was first saved, if any.
Attachment Size (bytes)	The size of the attached file.
Download State	The displayed value is either 'Complete' or 'Incomplete'.
MIME Type	The file type in MIME format.

Android Yahoo Mail Emails

Description	Android Yahoo Mail Emails contains carved and non-carved emails stored by the Android Yahoo Mail application.
Notes	

ATTRIBUTE	DESCRIPTION
Message ID	The database key for the message. This key can be used to match up an email with attachments found in Android Yahoo Mail Attachments.
Folder ID	The name of the folder that the email was stored in.
Subject	The subject line of the email.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was received.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was sent.
Last Viewed Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was last viewed on the local device.
From	The email address of the sender.

ATTRIBUTE	DESCRIPTION
Reply To	The email address to which replies to this email will be sent.
Recipients	A list of email addresses and labels for the intended recipients in the 'To' field of the email.
Cc	A list of email addresses and labels for the intended recipients in the 'Cc' field of the email.
Bcc	A list of email addresses and labels for the intended recipients in the 'Bcc' field of the email.
Body	The body of the email in plain text.
Snippet	A short preview of the text of the email body.
Favorited	Whether the email has been favorited locally. The displayed value is either 'Yes' or 'No'.
Replied	Whether the local user has replied to the email. The displayed value is either 'Yes' or 'No'.
Read Status	Whether the email has been opened locally. The displayed value is either 'Read' or 'Unread'.
Has Attachment	Whether the email has an attachment. The displayed value is either 'Yes' or 'No'.

Android Yahoo Mail User Accounts

Description	Android Yahoo Mail User Accounts contains local user accounts from the Android Yahoo Mail application.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The user ID of the account.
First Name	The first name of the person associated with the account.
Last Name	The last name of the person associated with the account.
Preferred Name	The user's custom preferred name.
Email Address	The account's email address.

Gmail Emails

Description	Gmail Emails contains the Gmail email fragments that were recovered from an Android device.
Notes	

ATTRIBUTE	DESCRIPTION
To Address(es)	The recipient(s) of the email.
From Address	The sender of the email.
Thread ID	The ID of the conversation the email is from. Emails with the same Thread ID belong to the same conversation.
Subject	The subject of the email.
Sent Date/Time - UTC (yyyy-mm-dd)	The date that the email was sent.
Received Date/Time - UTC (yyyy-mm-dd)	The time that the email was received.
Email Body	The body of the email.
Email Snippet	A snippet of the email.
cc Address(es)	The recipients of the email that were CC'd.
bcc Address(es)	The recipients of the email that were BCC'd.
Reply Address(es)	The reply-to address for the email.
Attachment Data Recovered	Indicates whether attachments for the email were recovered.
Attachments	The file names of any attachments for the email.
Saved Attachments	The file paths of any attachments for the email which were saved locally.

Outlook Accounts

Description	Outlook Accounts contains information about the user accounts that have been logged in to on the device.
Notes	

ATTRIBUTE	DESCRIPTION
Email Address	The email address associated with the account.
Description	A description of the account, as set by the user.
Display Name	The display name for the user.
Birthday	The user's birthday in yyyy-mm-dd format.

Outlook Appointments

Description	Microsoft Outlook is a personal information manager and email client. Outlook Appointments captures information related to appointments scheduled in Outlook.
Notes	

ATTRIBUTE	DESCRIPTION
Sender Name	The person who requested the appointment.
Sender Exchange Account	The sender's Exchange account name.
Recipients	The recipients of the appointment invitation.
Subject	The subject of the appointment.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the appointment starts.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the appointment ends.
Body	The body of the appointment description.
Recipients CC	The CC'd recipients of the appointment invitation.
Recipients BCC	The BCC'd recipients of the appointment invitation.
Companies	The companies involved in the appointment.
Attachments	The attachments for the appointment.
Location	The location of the appointment.
Is All-Day Event	Indicates if the appointment is an all-day event.
Is Recurring	Indicates if the appointment is recurring.
Recurrence Pattern Description	Describes the recurrence pattern of the appointment, if applicable.
Sensitivity	Indicates if the appointment is sensitive.
Is Hidden	Indicates if the appointment is hidden.
Is Private	Indicates if the appointment is private.
Priority	The priority of the appointment.
Importance	The appointment importance setting.

Outlook Contacts

Description	Microsoft Outlook is a personal information manager and email client. Outlook Contacts captures information related to contacts stored in Outlook.
Notes	

ATTRIBUTE	DESCRIPTION
Display Name	The contact's display name.
Customer ID	The customer ID of the contact.
Email Address 1	The contact's primary email address.
Email Display As 1	The display string of the contact's primary email address.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the contact details were last modified.
Company Name	The contact's company name.
Department Name	The contact's department name.

ATTRIBUTE	DESCRIPTION
Title	The contact's job title.
Profession	The contact's profession.
Manager Name	The name of the contact's manager.
Office Location	The contact's office location.
Business Address	The physical address of the business.
Business Phone	The contact's business phone number.
Business Phone 2	The contact's secondary business phone number.
Business Fax	The contact's business fax number.
Business Homepage	The website of the contact's business.
Email Display Name 1	The display name of the contact's primary email address.
Email Address 2	The contact's secondary email address.
Email Display As 2	The display string of the contact's secondary email address.
Email Display Name 2	The display name of the contact's secondary email address.
Email Address 3	The contact's tertiary email address.
Email Display As 3	The display string of the contact's tertiary email address.
Email Display Name 3	The display name of the contact's tertiary email address.
Cellular Phone	The contact's mobile phone number.
Home Address	The contact's home address.
Home Phone	The contact's home phone number.
Home Phone 2	The contact's secondary home phone number.
Home Fax	The contact's home fax number.
FTP Site	The contact's FTP site.
Body	More information about the contact.
Attachments	Any attachments to the contact entry.
Last Modifier Name	The name of the person who last modified the contact details.

Outlook Messages

Description	Microsoft Outlook is a personal information manager and email client. Outlook Messages captures information related to emails sent and received in Outlook.
Notes	

ATTRIBUTE	DESCRIPTION
Sender Name	The sender of the email.
Sender Email	The email address of the sender.

ATTRIBUTE	DESCRIPTION
Recipients	The recipients of the email.
Subject	The subject of the email.
Sender Exchange Account	The sender's Exchange account name.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was created.
Delivery Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was delivered.
Body	The body of the email.
Folder Name	The name of the folder where the email is stored.
CC	The recipients of the email that were CC'd.
BCC	The recipients of the email that were BCC'd.
Attachments	The list of attachments on the email.
Headers	The raw email headers.
Priority	The priority of the email.
Importance	The importance of the email.
Sensitivity	The sensitivity of the email.

Samsung Email Logs

Description	Samsung Email Logs contains the email logs that were recovered from a Samsung device.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the person/business the email is with.
Email Address	The email address of person/business the email is with.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the email.
Message Content	The email message content.
Subject	The subject of the email.

Internet of Things

Amazon Alexa Audio Activity

Description	Contains details about audio activity detected by the Amazon Alexa application.

Notes	The data in this artifact is retrieved from the application's cached data and may not represent a complete record of the user's activities. Accessing the web resource URL requires the user's Alexa login credentials.

ATTRIBUTE	DESCRIPTION
Text	The spoken audio as interpreted by the Alexa application.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the audio was recorded.
Resource URL	The web resource URL for the audio file.

Amazon Alexa Cached Audio

Description	Contains attached audio files recovered from the Amazon Alexa application.
Notes	The data in this artifact is retrieved from the application's cached data and may not represent a complete record of the user's activities.

ATTRIBUTE	DESCRIPTION
Audio	An audio file containing voice commands spoken by the user.

Amazon Alexa Device Information

Description	Contains details about Alexa-enabled devices.
Notes	The data in this artifact is retrieved from the application's cached data and may not represent a complete record of the user's activities.

ATTRIBUTE	DESCRIPTION
Device Name	The name of the device.
Customer ID	The Amazon customer identifier.
Device Type	The type of device.
Serial Number	The serial number of the device.
MAC Address	The MAC address of the device.
Network Name (SSID)	The network name to which the device is connected.
ZIP / Postal Code	The ZIP or postal code associated with the device.

Amazon Alexa Tasks

Description	Contains details about shopping lists or other tasks tracked by the Amazon Alexa application.
Notes	The data in this artifact is retrieved from the application's cached data and may not represent a complete record of the user's activities. Accessing the audio resource URL requires the user's Alexa login credentials.

ATTRIBUTE	DESCRIPTION
Text	The spoken task as interpreted by the Alexa application.
Type	The type of task.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the task was last updated.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the task was created.
Customer ID	The customer ID of the task creator.
Completed	Whether the task has been completed.
Deleted	Whether the task has been deleted.
Similar Text	Text that's similar to the text for the task, as determined by the Alexa application.
Resource URL	The web resource URL for the audio file.

Amazon Alexa User

Description	Contains details about user accounts recognized by the Amazon Alexa application.
Notes	The data in this artifact is retrieved from the app's cached data and may not represent a complete record of the user's activities.

ATTRIBUTE	DESCRIPTION
User Name	The username for the account.
Email	The email associated with the account.
Device Name	The name of the device.
Customer ID	The Amazon customer identifier.

Amazon Alexa Web Resource

Description	Contains details about Amazon API resources contacted by the Alexa application.

Notes	The data in this artifact is retrieved from the application's cached data and may not represent a complete record of the user's activities. Accessing the web resource URL requires the user's Alexa login credentials.

ATTRIBUTE	DESCRIPTION
Resource URL	The URL for the web resource.
Type	The type of data available from the resource.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the resource request was made.

Fitbit Floors

Description	Fitbit Floors specifies the number of floors a user has traveled up and down within a day.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user ID of the associated user profile.
Date	The date that the floor-traveling data was generated.
Floors	The number of floors traveled.

Fitbit Heart Rate

Description	Fitbit Heart Rate specifies the heart rate of the person wearing a Fitbit. Each record displays the average heart rate for a given 5 minute interval and the daily average resting heart rate.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user ID of the associated user profile.
Start Date/Time - UTC (yyyy-mm-dd)	The start date and time of the average heart rate calculation.
End Date/Time - UTC (yyyy-mm-dd)	The end date and time of the average heart rate calculation.
Average Heart Rate (BPM)	The average heart rate.
Type	Indicates whether the average heart rate is a periodic average (every 5 minutes) or a daily average resting heart rate.

Fitbit Profiles

Description	Fitbit Profiles specifies information from the Fitbit profiles that the user has set up on the device.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user ID of the associated user profile.
Full Name	The first and last name of the person associated with the profile.
Birthday (yyyy-mm-dd)	The birthday of the person associated with the profile.
Profile Image URL	The location of the profile image.
Height (cm)	The height of the person in centimeters.
Gender	The gender of the person.
Walking Stride Length (cm)	The walking stride length of the person in centimeters.
Running Stride Length (cm)	The running stride length of the person in centimeters.
Current Timezone Offset (Minutes)	The timezone offset in minutes of the profile.
Country	The country the profile user may be in. For example, if the person is from Canada the value would be en_CA.

Fitbit Sleep

Description	Fitbit Sleep contains information about the user's sleeping patterns.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user ID of the associated user profile.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the person went to bed.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the person got out of bed.
Time In Bed (Minutes)	The total time in minutes that the person was in bed (awake and asleep).
Time Awake (Minutes)	The total time in minutes that the person was awake in bed.
Time Asleep (Minutes)	The total time in minutes that the person was asleep.

Fitbit Steps

Description	Fitbit Steps specifies information about the number of steps a person takes while wearing a Fitbit. Steps are aggregated for a 15 minute interval and then stored.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user ID of the associated user profile.
Start Date/Time - UTC (yyyy-mm-dd)	The start date and time of the accumulated steps.
End Date/Time - UTC (yyyy-mm-dd)	The end date and time of the accumulated steps.
Steps Taken	The accumulated steps taken.

Pebble Activity Information

Description	Pebble Activity Information specifies the physical activities that were tracked by the Pebble watch.
Notes	The Active Calories column is always empty for Android.

ATTRIBUTE	DESCRIPTION
Start Date/Time - UTC (yyyy-mm-dd)	The start date and time of the activity.
End Date/Time - UTC (yyyy-mm-dd)	The end date and time of the activity.
Duration (Seconds)	The duration of the activity.
Steps Taken	The total number of steps taken during the activity.
Active Calories (Cal)	The number of calories being burned during the activity.
Serial Number	The serial number of the Pebble watch used to track the activity.

Pebble Applications

Description	Pebble Applications specifies the Pebble applications that are installed.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the Pebble Application.
Installed Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was installed.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was updated.
Created By	The creator of the application.

ATTRIBUTE	DESCRIPTION
Category	The category of the application in the Pebble application store.
Version	The version of the application.
Download URL	The URL where the application can be downloaded from.
Website URL	The URL of the application website.
Creator Email Address	The email of the creator for the application.
Companion Application	A companion application to the current application.
Companion Website	The website to the companion application.

Pebble Calendar Events

Description	Pebble Calendar Events contains calendar events that are displayed on the Pebble Watch Timeline.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the calendar event.
Description	A short description of the calendar event.
Location	The location of the event.
Calendar Display Name	The display name of the calendar to which the event belongs.
Start Date/Time - UTC (yyyy-mm-dd)	The start date and time of the event.
End Date/Time - UTC (yyyy-mm-dd)	The end date and time of the event.
Organizer Name	The organizer of the event.
Calendar Account	The calendar to which the event belongs.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the event was created on the Pebble application.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the event was updated.
User Account	The user account observing the event.
Attendees	The number of attendees to the event.
Is Recurring	Indicates whether the event is recurring.
Organizer	Indicates whether the user is the organizer of the event.

Pebble Contacts

Description	Pebble Contacts contains contact information that's accessible from the Pebble watch.

Notes	

ATTRIBUTE	DESCRIPTION
Display Name	The display name of the contact.
Phone Number	The phone number of the contact.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the last message from the contact.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the contact was created.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the contact was updated.

Pebble Detected Android Applications

Description	Pebble Detected Android Applications indicates the applications that were detected by the Pebble Android application.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The name of the detected application.
Last Message Received Date/Time - UTC (yyyy-mm-dd)	The date and time when a message or notification was last received from the application.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the application was detected by the Pebble application.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the detection was updated.
Application Version	The current version of the application.
Package Name	The package name of the application.

Pebble Device Information

Description	Pebble Device Information specifies the hardware information of the Pebble watch.
Notes	

ATTRIBUTE	DESCRIPTION
Friendly Name	The display name of the contact.
Last Connected Date/Time - UTC (yyyy-mm-dd)	The start date and time when the Pebble watch was last connected to the Android application.
MAC Address	The MAC address of the Pebble watch.
Serial Number	The serial number of the Pebble watch.

ATTRIBUTE	DESCRIPTION
Revision Number	The revision number of the Pebble watch.
Language	The user selected language of the Pebble watch.

Pebble Notifications

Description	Pebble Notifications specifies the notification that was sent to the Pebble watch.
Notes	

ATTRIBUTE	DESCRIPTION
Text	The content of the notification.
Title	The title of the notification.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the notification.
Original Date/Time - UTC (yyyy-mm-dd)	The original date and time of the notification.
Removed Date/Time - UTC (yyyy-mm-dd)	The date and time when the notification was removed.
Message Source	The source application of the notification.
Sent To Wearable	Indicates whether the notification was sent to the Pebble watch.
Dismissed	Indicates whether a notification was dismissed on the Pebble watch.

Pebble Physical Characteristics

Description	Pebble Physical Characteristics specifies the user's activity profile information.
Notes	

ATTRIBUTE	DESCRIPTION
Gender	The gender of the user.
Age	The age of the user.
Height (cm)	The height of the user in centimeters.
Weight (kg)	The weight of the user in kilograms.

Pebble Weather Locations

Description	Pebble Weather Locations contains location information that's tracked by the Pebble Watch.

Notes	The latitude and longitude are not a precise values, but they can place the Pebble Watch in a specific city.

ATTRIBUTE	DESCRIPTION
Location Name	The name of the tracked location.
Latitude	The latitude of the location.
Longitude	The longitude of the location.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time of the location data.
Updated Date/Time - UTC (yyyy-mm-dd)	The updated date and time of the location data.

Media

AMR Files

Description	AMR Files contains AMR files used for voicemail on both iOS and Android.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Audio	The contents of an AMR file.

Android Snapchat Accounts Information

Description	Android Snapchat Accounts Information contains information about the accounts that the user has logged in on the device with.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The ID of the user.
User Name	The username of the user.
Display Name	The display name of the user.
Email Address	The email address of the user.
Phone Number	The phone number of the user.
Location	The location of the user, specified by country.
Birthday	The birthday of the user.
Last Login Date	The most recent date and time that the user used the application.

ATTRIBUTE	DESCRIPTION
Account Creation Date/Time	The date and time that the user created the account

Android Snapchat Event Logs

Description	Android Snapchat Event Logs contains the events performed by the user.
Notes	

ATTRIBUTE	DESCRIPTION
Event	The event that the user performed.
Event Parameters	The parameters of the performed event.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time that the event occurred.

Android Snapchat Friends

Description	Android Snapchat Friends contains the friends of the user.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The username of the friend.
Display Name	The name that is displayed for that friend on the local device.
Added Me Date/Time - UTC (yyyy-mm-dd)	The date and time that the friend added the user on the device.
Added Them Date/Time - UTC (yyyy-mm-dd)	The date and time that the user on the device added the friend.

Android Snapchat Photo Transfers

Description	Android Snapchat Photo Transfers contains attributes of the photos sent between users.
Notes	

ATTRIBUTE	DESCRIPTION
Type	The type specifies if the photo was sent or received.
Sender	The person that sent the photo.
Receiver	The person that received the photo.
Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time that the photo was sent/received.

ATTRIBUTE	DESCRIPTION
Send Succeeded	Whether the message was successfully sent to the recipient.
Was Viewed	Indicates whether or not the receiver has viewed the sent photo.
Screenshot Taken	Indicates if a screenshot was taken or not.
Photo Id	The identifier of the photo.

Android Snapchat Received Images

Description	Android Snapchat Received Images contains the photos that the user on device has received.
Notes	

ATTRIBUTE	DESCRIPTION
Image	The actual picture content.
Size (Bytes)	The size of the picture
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Snapchat Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time of the picture according to Snapchat.
Skin Tone Percentage	The percentage of the image that is skin tone.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the picture was last accessed.
MD5 Hash	The MD5 hash of the image.
SHA1 Hash	The SHA1 hash of the image.
PhotoDNA Hash	The PhotoDNA hash of the image.
Category	An integer that indicates the Project VIC category for the picture.

Android Snapchat Received Snaps

Description	Android Snapchat Received Snaps contains Snaps containing pictures and videos that have been sent to the local user.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The user who sent the snap.
Picture	A picture or thumbnail of the video that was received as the snap.

ATTRIBUTE	DESCRIPTION
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the snap was sent.
Media Type	Whether the snap was a picture or video snap.
Skin Tone Percentage	The percentage of the video snap that contains what appears to be visible skin.
Status	The status of the snap.
Display Time (seconds)	Indicates how long the snap can be viewed for, in seconds.
Broadcast URL	The URL of a broadcasted snap.
Broadcast Text	The text of a broadcasted snap.

Android Snapchat Sent Snaps

Description	Android Snapchat Sent Snaps contains the snaps that have been sent by the user.
Notes	

ATTRIBUTE	DESCRIPTION
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the snap was sent.
Status	The status of the snap.
Recipient	The recipient of the snap.

Android Snapchat Stories

Description	Android Snapchat Stories contains information about Snapchat Stories that are recovered, along with any decrypted media content.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The username of the owner of the story.
Caption	The caption text associated with the story.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the story was first posted.
Last Viewed Date/Time - UTC (yyyy-mm-dd)	The date and time when the local user viewed the story.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the story expires.

ATTRIBUTE	DESCRIPTION
Screenshot Taken	Indicates the number of screenshots that the local user takes of the story.
Display Time (seconds)	The duration of the snap story.
Attachment Path	The path to an encrypted attachment.
Media URL	A URL to the location of the attachment. The URL will expire after some time.
Picture	The decrypted picture attachment.
Attachment	The decrypted attachment (if it's not a picture).

Audio

Description	Audio contains Audio files that are recovered and use .mp3 or .wav formats.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
File Name	The name of the file.
File Extension	The extension of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio file was created.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio file was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio file was last modified.
File Size (Bytes)	The size of the audio file.
MD5 Hash	An MD5 hash of the audio content.
SHA1 Hash	A SHA1 hash of the audio content.

Carved Video

Description	Carved Video contains videos that are recovered using carving. Supported formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. Other container formats can also be recovered provided that their underlying packets are the same as one of the supported formats.
Notes	As of February 20 2020, this artifact will no longer be included under Videos. Carved Video functionality will be included in the 'Videos' artifact instead.

ATTRIBUTE	DESCRIPTION
Content Format	The format of the video.
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.

ATTRIBUTE	DESCRIPTION
File Size (Bytes)	The size of the container and file.
Container Format	The format of the video container.
Saved Video Size (Bytes)	The size of the video that was saved to the database.
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.

Pictures

Description	Pictures contains pictures that were retrieved using either carving or parsing techniques. The supported picture formats are JPEG (.jpeg, .jpg, .jpe), PNG (.png), Bitmaps (.bmp), Graphics Interchange Format (.gif), Icons (.ico), and Tagged Image File Format (.tif, .tiff).
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Image	The image data that was recovered.
File Name	The name and extension of the that file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file that the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.

ATTRIBUTE	DESCRIPTION
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
GPS Longitude	The GPS longitude coordinates of where the picture was taken (extracted from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
GPS Latitude	The GPS latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS latitude (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).

ATTRIBUTE	DESCRIPTION
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Potential Original Media	Indicates whether the media is likely the original source.
Category	An integer that indicates the Project VIC category for the picture.

Private Photo Vault Albums

Description	Private Photo Vault Albums contains information about the albums a user creates to organize their media in the Private Photo Vault application. The album information can be useful intelligence for how a user might have organized encrypted media.
Notes	

ATTRIBUTE	DESCRIPTION
Album Title	The name of the album.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the album was created on the device.
Last Modified Date/Time - UTC (yyyy-mm-dd)	Not available on Android.
Decoy	Indicates whether the album is hidden (accessible with a different passcode) or not.
Password	The password protecting the album, if any. Does not affect encryption.
PIN	The value used to generate the encryption key. It can be either a numeric PIN (4 digits) or a sequence of values (2 to 9) of an unlock pattern.

Private Photo Vault Media

Description	Private Photo Vault Media contains information about encrypted media files that the user stores in the Private Photo Vault application. If decryption is successful, the decrypted media content is made available in this artifact. Metadata about the encrypted media files, such as timestamps, are always available. Users will often resort to encrypted media applications for storing illicit material. Being able to decrypt this media can be crucial to a case.
Notes	

ATTRIBUTE	DESCRIPTION
File Path	The path to the encrypted media file.
Media Type	The type of media (photo or video).
Album Title	The associated album title.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the media was created on the device.
Last Modified Date/Time - UTC (yyyy-mm-dd)	Not available on Android.
Thumbnail Path	Not utilized on Android - see the 'Private Photo Vault Thumbnails - Android' artifact instead.

Private Photo Vault Thumbnails - Android

Description	On Android, Private Photo Vault does not explicitly reference thumbnails in the database. Further, multiple resolutions can exist. This artifact will decrypt all of the thumbnails found in the thumbnails directory.
Notes	This artifact may be useful in situations where the original media or database rows have been deleted but thumbnail files remain. It is possible for the same encrypted media to have multiple thumbnails (different resolutions).

ATTRIBUTE	DESCRIPTION
FileName	The path to the encrypted thumbnail.
CreatedDateTimeUTC	The date and time when the media was created or imported into Private Photo Vault.

Snapchat Chat Messages

Description	Snapchat Chat Messages contains the chat messages sent between users.
Notes	

ATTRIBUTE	DESCRIPTION
Recipient	The recipient of the message.
Sender	The sender of the message.
Message ID	The ID of the message.
Message	The content of the sent message.
Type	The type of the sent message.
Saved by sender	Whether the message was saved by the sender (Yes or No).

ATTRIBUTE	DESCRIPTION
Saved by recipient	Whether the message was saved by the recipient (Yes or No).
Released by recipient	Whether the recipient let the chat message be deleted (Yes or No).
Message Status	The status of the message.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the chat message.

Snapchat Group Members

Description	Snapchat Group Members contains information about participants of the groups that the local user is a member of.
Notes	

ATTRIBUTE	DESCRIPTION
Group Chat ID	The ID of the group.
Group Name	The name of the group.
Group Member	The ID of the participant of the group.
Added Date/Time - UTC	The date and time that the participant joined the group.
Deleted	Whether the participant left the group (Yes or No)

Snapchat Memories

Description	Snapchat Memories contains pictures and videos that the Snapchat user saves as a memory.
Notes	

ATTRIBUTE	DESCRIPTION
Picture	The picture or video frames from the saved memory. The picture and the overlay for a snap are stored in separate locations, and are combined to reproduce the snap as it would appear in Snapchat.
Attachment	The attachment for the memory, if it's not a picture.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the snap was originally taken.
Timezone	The time zone of the device when the original snap was taken, or when the media was moved from the device's gallery to the My Eyes Only section of the application.
Type	Indicates whether the memory is saved as a regular snap or My Eyes Only, the latter being password protected.

ATTRIBUTE	DESCRIPTION
Media Type	The media type, either a picture or video.
Duration (seconds)	The duration of time before the snap expires.
Latitude	The latitude of the location where the snap was originally taken.
Longitude	The longitude of the location where the snap was originally taken.
Size (Bytes)	The encrypted size of the snap media. Any overlay that was added to the snap is not included when determining the size of the snap media.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Attachment Path	The file path of the media attachment on the device.
Skin Tone Percentage	The percentage of the picture that appears to be skin tone. Any overlay that was added to the snap is not included when calculating the skin tone.
MD5 Hash	The MD5 hash of the decrypted media. Any overlay that was added to the snap is not included when creating the hash signature.
SHA1 Hash	The SHA1 hash of the decrypted media. Any overlay that was added to the snap is not included when creating the hash signature.
PhotoDNA Hash	The PhotoDNA hash of the image.
Category	An integer that indicates the Project VIC category for the picture.

Snapchat Received Videos

Description	Snapchat Received Videos contains the videos sent to the user.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file.
File Extension	The extension of the file.
Image	A generated thumbnail of the video.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the video file was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the video file was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the video was last written to.
Skin Tone Percentage	The amount of skin tone found in the video.
File Size (Bytes)	The size of the video in bytes.
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.

ATTRIBUTE	DESCRIPTION
Category	An integer that indicates the Project VIC category for the video.

Videos

Description	Videos contains videos that are recovered using parsing or carving. Supported formats for parsing include AVI, MP4, MOV, MPEG, DIVX, A3GP, ASF, WMV, DVR-MS, MKV, VOB, MOD, and WEBM. Supported carving formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. For more information about supported video formats, see Supported media and file types.
Notes	If AXIOM Process is configured to save only a specified amount of data from carved videos, any MD5 and SHA1 hashes that are generated are based on the data that's saved and not the full video. This behavior might cause issues when searching for known video hashes, as the hash for a carved video will differ from the actual video if it exceeds the size limit set in AXIOM Process.

ATTRIBUTE	DESCRIPTION
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
File Name	The name of the file.
File Extension	The extension of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was last modified.
File Size (Bytes)	The size of the video.
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.

ATTRIBUTE	DESCRIPTION
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. "Complete" indicates that a full Exif extraction was performed, including potential metadata located at the end of the video. "Partial" indicates that only Exif information in the header section of the video file was recovered, which should only occur with very large videos (in excess of the limit set in the options screen). "Failed" indicates that the information may have been corrupted and could not be recovered. "Skipped" indicates that the extraction was skipped.
Media Duration (Seconds)	The duration of the video in seconds (extracted from Exif data).
Original Width	The resolution of the video (extracted from Exif data).
Original Height	The resolution of the video (extracted from Exif data).
Created Date/Time - Local Time	The local date and time when the video was first recorded (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the video was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the video being recored (extracted from Exif data).
Software	The software used to record or modify the video. This could either be the OS version of the phone used to record the video or name of the software used to edit the video in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to record the video (extracted from Exif data).
Model	The model of the camera used to record the video (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to record the video (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The GPS latitude coordinates of the camera where the video was recorded (extracted from Exif data).
Longitude	The GPS longitude coordinates of the camera where the video was recorded (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of the camera where the video was recorded (extracted from Exif data).
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.

ATTRIBUTE	DESCRIPTION
Category	An integer that indicates the Project VIC category for the video.
Content Format	The format of the carved video.
Container Format	The format of the carved video container.
Saved Video Size (Bytes)	The size of the carved video that was saved to the database.

Mobile

Activity Manager History

Description	Activity Manager History contains a list of recent activity manager events, identified by the package name that triggered the event.
Notes	

ATTRIBUTE	DESCRIPTION
Date/Time - Local Time (yyyy-mm-dd)	The date and time of the activity.
Type	The type of activity.
Event	The name of the event.
Package Name	The name of the package that triggered the event.
Process ID	The process ID of the package.

Camera History

Description	Camera History contains a list of the instances where applications have accessed the camera functionality on a device. This artifact can show when an application package accesses camera functionality, which can help the investigator determine when a suspect may have been using their device's camera.
Notes	

ATTRIBUTE	DESCRIPTION
Date/Time - Local Time (yyyy-mm-dd)	The local date and time of the event.
Action	The action that describes the event.

ATTRIBUTE	DESCRIPTION
Camera ID	An ID that can indicate the location of the camera on the phone. The location of the camera can be front, rear, or other.
Package Name	The package name for the application that's accessing the camera.
Process ID	The ID of the process accessing the camera.

Google Play Application Details

Description	Google Play Application Details contains more detailed information about the applications that a user has downloaded from Google Play. This information includes when the user last installed or updated an application, and how the user was referred to the application.
Notes	

ATTRIBUTE	DESCRIPTION
Package Name	The package name of the application that is installed.
Title	The name of the application as it is currently represented in the Google Play Store.
Account	The signed in Google Play Store account that is used to install the application.
Last Updated Date/Time	The date and time when the application was last updated through the Google Play Store.
Downloaded Date/Time	The date and time when the application was last downloaded through the Google Play Store.
Download Request Date/Time	The date and time when the application was last requested for installation through the Google Play Store.
First Installed Date/Time	The date and time when the application was first installed through the Google Play Store.
Update Discovered Date/Time	The last time Google Play discovered an available update for the installed application.
Automatically Updates	Indicates whether the application is set to automatically update in Google Play.
Referrer	The original source that referred the user to the application in Google Play.

Google Play Installed Applications

Description	Google Play Installed Applications lists each of the applications that were downloaded and installed from Google Play.
Notes	

ATTRIBUTE	DESCRIPTION
Package Name	The package name of the application that is installed.
Account	The signed in Google Play Store account that is used to install the application.
Purchased Date/Time	The time that the application was purchased from the Google Play Store.

Google Play Searches

Description	Google Play Searches contains the search queries that a user has performed in Google Play, and the date and time of when they were performed.
Notes	

ATTRIBUTE	DESCRIPTION
Search Query	The search query entered by the user.
Query Date/Time	The date and time when the user made the search.

Last Known Locations

Description	Last Known Locations contains a list of the last known locations of the Android device, as tracked by the GPS receiver and recovered using dumpsys.
Notes	

ATTRIBUTE	DESCRIPTION
Serial Number	The serial number of the Android device.
Type	The type of receiver.
Latitude	The latitude of the location.
Longitude	The longitude of the location.
Altitude (meters)	The altitude of the location.

SIM Card ICCID

Description	SIM Card ICCID contains the ICCID number that identifies the device's SIM card.
Notes	

ATTRIBUTE	DESCRIPTION
ICCID	The integrated circuit card identifier.

SIM Card IMSI

Description	SIM Card IMSI contains IMSI numbers used to identify the mobile subscriber, as recovered from the SIM card.
Notes	

ATTRIBUTE	DESCRIPTION
IMSI	The international mobile subscriber identity.

SIM Card Phone Numbers

Description	SIM Card Phone Numbers contains records of all the phone numbers saved to the device SIM card. The type of number is indicated by the record type.
Notes	

ATTRIBUTE	DESCRIPTION
Phone Number	The phone number for the specific record type.
Record Type	Identifies the type of record that the phone number is. The Record Type value can be Abbreviated dialing numbers (ADN), Emergency call codes (ECC), Last number dialed (LND), MSISDN, Service dialing numbers (SDN), or Fixed dialing numbers (FDN).

SIM Card Service Providers

Description	SIM Card Service Providers contains the names of mobile service providers that the device has connected with, and which are recovered from the SIM card.
Notes	

ATTRIBUTE	DESCRIPTION
Service Provider Name	The identity of the mobile phone service provider.

SIM Card SMS Messages

Description	SIM Card SMS Messages contains messages sent or received by the local user which were saved to the SIM card.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the SMS message.
Recipient	The recipient of the SMS message.
Message Date/Time	For incoming messages, this timestamp indicates when the message was received by the mobile service center. For outgoing messages, there is no data available for this field.
Message	The message body of the SMS message.
Deleted	Identifies whether the message has been deleted (Yes or No).
Message Status	Identifies whether the message has been read, unread, draft or sent.
SMSC	The short message service center number.

Wi-Fi Profiles

Description	Wi-Fi Profiles contains a list of the saved Wi-Fi Profiles on a mobile device.
Notes	

ATTRIBUTE	DESCRIPTION
Network Name (SSID)	The name of the network.
Security Mode	The security mode of the network.
Network Password	The password used to log onto the network.
User Name	The username that was used to log onto the network.
WEP Key	The WEP key used to log onto the network
MAC Address	The MAC Address of the network.
Network ID	An integer used to identify the network. As networks are added to the device, this value gets incremented (the first network added has an ID of 0, the second has an ID of 1, and so on). If a network is deleted and re-added at a later date, it receives the next new ID available instead of reassuming its original ID.
Profile Created Date/Time - Local Time (yyyy-mm-dd)	The date and time that the Wi-Fi profile was created.
Last Connected Date/Time - Local Time (yyyy-mm-dd)	The date and time of the last network connection.

ATTRIBUTE	DESCRIPTION
Connection Count	The number of times that the network was connected to by the device.

Operating System

.DS_Store Records

Description	.DS_Store Records contains all the records extracted from .DS_Store files found on the computer. Each record represents a property of a file or a folder. The significance of this artifact is an indicator of high likelihood that the user of the computer was aware of these files and folders with a possibility of attributing a date to that awareness.
Notes	In the Apple macOS operating system, .DS_Store (Desktop Services Store) is a hidden file that stores the display information of its containing folder, similar to the file desktop.ini in Microsoft Windows. The file tracks information such as icon positions, view settings, cached file size, cached last modified date, and even the choice of a background image. The .DS_Store is created and maintained by the Finder application in any folder that it accesses, even on remote file systems mounted from servers that share files (for example, via Server Message Block (SMB) protocol or the Apple Filing Protocol (AFP)). .DS_Store files are also included in archives created by macOS users, such as ZIP files, and they are backed up by some cloud file backup services. This means that the presence of .DS_Store Records artifacts on non-Mac evidence such as Windows, Mobile, or Cloud indicates that some of the data may have originated or have been accessed from a macOS computer at some point. For more information on .DS_Store files and their forensic significance see: .DS_Stores: Like Shellbags but for Macs.

ATTRIBUTE	DESCRIPTION
Record Name	The name of the file or folder as stored in the .DS_Store file.
Record Type	The type of the record, or property, that is being logged in the .DS_Store file for a particular file or folder.
Record Value	The value of the property for the given file or folder.
Record Path	The full path to the file or folder
.DS_Store Created Date/Time - UTC (yyyy-mm-dd)	The created date of the .DS_Store file from which the record was extracted.
.DS_Store Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date of the .DS_Store file from which the record was extracted.
.DS_Store Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date of the .DS_Store file from which the record was extracted.

Accounts Information

Description	Contains the login information for all accounts on the Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Username	The username associated with the account.
Package Name	The name of the application as the device sees it.
Password	The password stored on the device to connect to the account.
Last Login Date/Time - UTC (yyyy-mm-dd)	The date and time of the last successful login.

Android Cache.Cell

Description	Android Cache.Cell contains cached cell base station data recovered from an Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Key	The cell identifier. This identifier is constructed like [MCC]:[MNC]:[LAC]:[cell ID].
Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time when the information was gathered.
Range	The distance the phone is away from the cell base station.
Confidence	The confidence of the data.
Latitude	The latitude of the cell base station.
Longitude	The longitude of the cell base station.

Android Cache.Wifi

Description	Android Cache.Wifi contains the cached WiFi access points recovered from an Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Key	The WiFi access point MAC address.
Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time when the information was gathered.
Range	The distance the phone is away from the access point.

ATTRIBUTE	DESCRIPTION
Confidence	The confidence of the data.
Latitude	The latitude of the access point.
Longitude	The longitude of the access point.

Android Call Logs

Description	Android Call Logs contains information about the phone calls that occur using the Android Phone application.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local user of the device where the data was recovered from.
Partner	The phone number of the conversation partner.
Partner Name	The name of the conversation partner.
Direction	The direction of the call (Incoming or Outgoing).
Call Status	The status of the call (Answered, Unanswered, Missed or Declined).
Call Date/Time - UTC (yyyy-mm-dd)	The date/time of the call.
Call Duration (Seconds)	The duration of the call.
Partner Location	The location of the other participant of the call, can be a province or state.
Service Provider Country Code	The country code of the service provider that handled the call.
ICCID	The ICCID number of the SIM card inside the device.

Android Call Logs (UFED Agent)

Description	Android Call Logs (UFED Agent) contains calling logs from the Phone application on Android. These logs are recovered from <incoming_calls>, <outgoing_calls>, <missed_calls>, <unknown_calls> tags found in a UFED Report.xml.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local user of the device where the data was recovered from.
Type	The type of call (Incoming, Outgoing, or Missed). This data is retrieved from the <incoming_calls>, <outgoing_calls>, <missed_calls>, <unknown_calls> tags in a UFED Report.xml.
Partner Phone Number	The phone number of the conversation partner. This data is retrieved from the <number> tag within each call element in a UFED Report.xml.

ATTRIBUTE	DESCRIPTION
Partner Name	The name of the conversation partner. This data is retrieved from the <name> tag within each call element in a UFED Report.xml.
Date Time - UTC (yyyy-mm-dd)	The date/time of the call. This data is retrieved from the <timestamp> tag within each call element in a Report.xml.
Duration (Seconds)	The duration of the call. This data is retrieved from the <duration> tag within each call element in a Report.xml.

Android Contacts

Description	Android Contacts contains contact information from a recovered Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Display Name	The display name of the contact.
Source Account Name(s)	The name of the account.
Email Address(es)	The email address of the contact.
Phone Number(s)	The phone number of the contact.
Last Time Contacted Date/Time - UTC (yyyy-mm-dd)	The last date and time when the contact was contacted.
Notes	Notes associated with the contact.
Source Account Type(s)	The type of account that the contact information is for.
Number of Times Contacted	The number of times that the contact has been contacted.
Starred	Indicates whether or not the contact has been starred.
Deleted	Indicates whether or not the contact has been deleted.
Address	The postal address of the contact.
Website	The website of the contact.

Android Contacts (UFED Agent)

Description	Android Contacts (UFED Agent) contains information recovered from the Contacts application on Android. These contacts are recovered from <contacts> tag found in a UFED Report.xml.
Notes	

ATTRIBUTE	DESCRIPTION
Contact Name	The name of the contact. This data is retrieved from the <name> tag within contact elements in a UFED Report.xml.
Phone Numbers	The phone number of the contact. This data is retrieved from the <phone_number> tags within the contact elements in a UFED Report.xml.
Email Address(es)	Any email addresses associated with the contact. This data is retrived from the <extra_field> tags within the contact elements in a UFED Report.xml.
Company	The company name of the contact. This data is retrived from the <extra_field> tags within the contact elements in a UFED Report.xml.
Address	The mailing address of the contact. This data is retrieved from the <extra_field> tags within the contact elements in a UFED Report.xml.
Source Account Type(s)	The source from where the contact information is saved (that is, whether the contact is saved to the SIM card, the device, or another account). This data is retrieved from the <memory> tag within the contact elements in a UFED Report.xml.
Notes	The data from the notes field for the contact. This data is retrieved from the <extra_field> tag within calendar elements in a UFED Report.xml.
Additional Data	Any additional data that is recovered that's related to the contact. This field is in XML format as the data recovered is directly from the Report.xml without any further interpretation.

Android Device Information

Description	Android Device Information contains the phone identification values.
Notes	

ATTRIBUTE	DESCRIPTION
IMSI	The IMSI associated with the device.
IMEI	The IMEI associated with the device.
MEID	The MEID associated with the device.
Bluetooth Address	The Bluetooth hardware address of the device.
Bluetooth Name	The Bluetooth name that appears upon pairing the device.
Device Id	The unique identifier that is displayed when rooting the device.
ICCID	The ICCID associated with the device.
SIM Card State	The state of the SIM card when the device was acquired (for example, READY).
Service Provider Country Code	The country code associated with the service provider of the device.
Mobile Country Code	The mobile country code of the provider of the SIM.
Mobile Network Code	The mobile network code of the provider of the SIM.
Service Provider Name	The name of the SIM service provider.

ATTRIBUTE	DESCRIPTION
Device Phone Number	The phone number of the device.
Device Phone Type	The type of radio used to transmit voice calls (for example, GSM)
Voice Mail Identifier	The alphabetic identifier associated with the voice mail number.
Voice Mail Number	The phone number the device calls to access voice mail.
Current Network Country ISO Code	The ISO country code of the network that the device was registered on during acquisition.
Current Network Operator Name	The name of the network operator that the device was registered on during acquisition.
Network Type	The type of network that the device was registered on during acquisition.
Device Software Version	The software version of the device.
Roaming	Indicates whether the device was considered to be roaming during acquisition.
Serial Number	The serial number associated with the device.
Manufacturer	The manufacturer of the device.
Model	The model of the device.
Product Name	The secret codename that the manufacturer gave to the device.
Chip Name	The name of the processor within the device.
Bootloader	The bootloader associated with the device.
Host Name	The hostname associated with the device.
Security Patch	The current installed security patch of the device.
MAC Address	The WiFi hardware address of the device.
Timezone	The timezone for the device.
Advertising ID	The advertising ID of the primary user account.

Android KeyStore

Description	Android KeyStore contains passwords and tokens for websites and other internet services that are recovered from Android KeyStore.
Notes	

ATTRIBUTE	DESCRIPTION
Account	The user account that the keystore entry applies to.
File Name	The name of the keystore data file.
Type	The type of the keystore data.
Key	The private key found in the keystore data.
Value	The blob value.
Flags	The flags byte.

ATTRIBUTE	DESCRIPTION
Blob Info	The info byte.
Initialization Vector	The initialization vector.
AEAD Tag	The tag used for authentication encryption with associated data (used by KeyStore 3).
MD5 Hash	The MD5 hash used for encryption (used by KeyStore 2).

Android Usage History

Description	Android Usage History contains information about the usage and activity of applications that are running on the device.
Notes	

ATTRIBUTE	DESCRIPTION
Event Name	The category of event that is occurring.
Package Name	The package name defined by the publisher/developer of the application (for example, com.example.mypackage).
Event	The event that is running within the application.
Event Date/Time - UTC (yyyy-mm-dd)	The last time that the event was actively being engaged either by a user or by the system.
Last Active Date/Time - UTC (yyyy-mm-dd)	The last time that the package was active on the device.
Last System Active Date/Time - UTC (yyyy-mm-dd)	The last time that the package was being utilized on or by the system.
Total Time (Seconds)	The amount of time that the application/package was open and being interacted with by the user.
Type	The type of event representing a state of change, for example, configuration change or shortcut invocation. For a complete list of events, visit https://developer-.android.com/reference/android/app/usage/UsageEvents.Event.

Android Usage History (Dumpsys)

Description	Android Usage History (Dumpsys) contains information about the usage and activity of applications running on the device, recovered using the dumpsys utility. The dates and times that were recovered by this artifact reflect the local time of the device.

Notes	

ATTRIBUTE	DESCRIPTION
Event Name	The category of event that is occurring.
Package Name	The package name that was defined by the publisher/developer of the application (for example, com.example.mypackage).
Event	The event that is running within the application.
Configuration	The Android configuration that is currently active.
Time Range - Local Time (yyyy-mm-dd)	The time range that the data was aggregated within.
Total Time (Seconds)	The amount of time that the application/package was open and being interacted with by the user.
Event Date/Time - Local Time (yyyy-mm-dd)	The last time that the event was actively being engaged either by a user or by the system.
Last Active Date/Time - Local Time (yyyy-mm-dd)	The last time that the package was active on the device.
Last System Active Date/Time - Local Time (yyyy-mm-dd)	The last time that the package was being utilized on or by the system.
Type	The type of event representing a state of change, for example, configuration change or shortcut invocation. For a complete list of events, visit https://developer.android.com/reference/android/app/usage/UsageEvents.Event.

Android User Dictionary

Description	Contains the shortcuts and words the user has on his or her device.
Notes	

ATTRIBUTE	DESCRIPTION
Word	A word entered by a user to auto-complete a shortcut (a desired word or phrase). For example, a user may type the word, "Hello," prompting the shortcut, "Hello World."
Shortcut	The symbols that the user types to cause the word to be written.

Application Activity - Android

Description	Application Activity represents the applications that are active in the background of the operating system.

Notes	

ATTRIBUTE	DESCRIPTION
Package Name	The application package name.
First Active Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was first active.
Last Active Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was last active.
Last Moved Date/Time - UTC (yyyy-mm-dd)	The date and time when the application last changed positions in the list of running applications. An application moves to the front of the list when it starts.
Application Activity	The activity the application is performing.
Application Data	The application data.
Origin Activity	The Android activity where the currently running activity originated from. For example, if the current activity describes opening a website in the browser, the origin activity might be from a messaging application where the link was opened from.
Device User ID	A unique user ID associated with the user account.
Preview	The snapshot preview of the active application.

Application Power Usage

Description	Application Power Usage represents the amount of battery power consumed by each application since the device's last full charge.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The application package name.
Application ID	The unique ID associated with the application package.
Power Usage	The amount of power (in mAh) that the application consumes.

Bluetooth Devices

Description	Bluetooth Devices contains information about the Bluetooth devices that the iOS device has paired with.
Notes	

ATTRIBUTE	DESCRIPTION
MAC Address	The MAC address of the device.
Name	The name that has been assigned to the device.
Major Device Class	The major class of device/service as per the Bluetooth specification.
Minor Device Class	The minor class of device/service as per the Bluetooth specification.
Last Seen Date/Time - UTC (yyyy-mm-dd)	The last date and time when the device was seen.

Calendar Events

Description	The Android Calendar application is a default application on Android.
Notes	

ATTRIBUTE	DESCRIPTION
Summary	A summary of the calendar appointment.
Location	The location of the calendar appointment.
Notes	Notes about the calendar appointment.
Calendar	The name of the calendar from which the event was generated.
Attendees	The attendees of the event.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the appointment starts.
End Date/Time - UTC (yyyy-mm-dd)	The date and time when the appointment ends.
Timezone	The timezone the appointment is in.

Calendar Events (UFED Agent)

Description	Calendar Events (UFED Agent) contains details about a user's calendar events on Android. These messages are recovered from <calendar> tag found in a UFED Report.xml
Notes	

ATTRIBUTE	DESCRIPTION
Subject	The subject of the scheduled event. This data is retrieved from the <subject> tag within the calendar element in a UFED Report.xml.
Event Location	The location of the scheduled event. This data is retrieved from the <location> tag within the calendar element in a UFED Report.xml.
Notes	Notes about the scheduled event. This attribute is referred to as the <Description> in the evidence acquired from the UFED and is retrieved from the <description> tag within the calendar element in a UFED Report.xml.
Start Date/Time - UTC (yyyy-mm-dd)	The start date and time of the scheduled event. This data is retrieved from the <start> tag wihin the calendar element in a UFED Report.xml.
End Date/Time - UTC (yyyy-mm-dd)	The end date and time of the scheduled event. This data is retrieved from the <end> tag within the calendar element in a UFED Report.xml.
Repeat Until Date/Time - UTC (yyyy-mm-dd)	The date and time when this recurring scheduled event expires. This data is retrieved from the <repeat_until> tag within the calendar element in a UFED Report.xml.
Repeat Interval	Describes the type of recurring event. This data is retrieved from the <repeat_type> tag within the calendar element in a UFED Report.xml.
Repeat Every	Describes the frequency of the recurring event. This data is retrieved from the <repeat_every> tag within the calendar element in a UFED Report.xml.
Repeat On	Indicates the specific day of occurrence of the recurring event. This data is retrieved from the <repeat_position> tag within the calendar element in a UFED Report.xml.

Chrome

Google Chrome is free web browser developed by Google and is available on all major operating systems, for both mobile and desktop. As of 2016, Chrome usage represents over 70% of the world's total browser traffic.

Analyzing the websites a user visits and the time the visits occur can provide valuable insights about a user. One notable feature that Google Chrome has is that it allows users to sync their bookmarks, browsing history, and more across multiple platforms and devices by using cloud sync accounts.

FORENSIC NOTES

Web Visits vs Web History

Chrome has two distinct artifacts that are very similar nature: Chrome Web Visits and Chrome Web History. Both of these artifacts are recovered from the History database. Chrome Web History is parsed from the URLS table and only contains information for the last visited date of a particular website. Chrome Web Visits can contain multiple entries for the same website, giving the examiner a more complete look at browser usage if the user visited a website multiple times. For example, if a user visits www.magnetforensics.com six times, the Chrome Web History artifact displays only the last time the site is visited, while the Chrome Web Visits artifact potentially displays records for all six instances. Chrome Web Visits was added in a later version of Chrome than Chrome Web History.

Carved web history

The Chrome / 360 Safe Browser / Opera Carved Web History is essentially the same as Chrome Web History except that it's recovered using carving and you may find additional deleted hits with it. The 360 Safe and Opera browsers are included in this artifact because when the data is carved, it's not possible to tell which browser the hit comes from as they're all formatted the same way.

Autofill and profile data

Chrome stores field data that the user has previously input as autofill and profile settings. For example, if you visit magnetforensics.com and login to the customer portal, browsers automatically save your username (and other details) so that you don't have to type it in each time you visit the site. This data is helpful for recovering usernames and other information that your user has filled out on various sites.

Sessions and tabs

When the system has an active session available, Chrome stores the browsing activity as the Chrome Current Session and any tabs that are open as Chrome Current tabs. The previous session and tabs are maintained in Chrome Last Session and Chrome Last Tabs so that the user can restore the last session and tabs if Chrome is closed.

ARTIFACTS

RELATED RESOURCES

How does Chrome's 'incognito' mode affect digital forensics?

Forensic email analysis: browser artifacts you may find on a PC or laptop

Android Downloads

Description	Android Downloads contains file download information from a recovered Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Download Source	The URL of the file that was downloaded.
Save Location	The absolute path on the device to the file downloaded.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified.
Notification Package	The Android package name that the download was initiated in.
Bytes Downloaded	The bytes that were downloaded.
Total Bytes	The total bytes of the file.

Digital Wellbeing Events

Description	Digital Wellbeing Events contains information about events that are tracked by the Digital Wellbeing app. Events describe state changes such as when an application pauses or resumes. Digital Wellbeing is a system application that's available on most Android 9 and 10 devices. The app is used to track events and provide the user with options to limit their usage of applications and set up a sleep schedule to reduce device usage.
Notes	

ATTRIBUTE	DESCRIPTION
Event ID	The unique ID of the event.
Event Date/Time UTC	The date and time of the event.
Package Name	The package name of the application associated with the event.
Event Type	An event representing a state change in the application associated with the event.

ATTRIBUTE	DESCRIPTION
Source Package Name	The package name of the application that triggered the event. The application that triggers the event can be different from the application that the event is associated with. For example, opening one application might cause an activity in a tracked application to pause.

Digital Wellbeing Limits

Description	Digital Wellbeing Limits is used for restricting the amount of time for application usage. An application is suspended once the time limit has been reached.
Notes	

ATTRIBUTE	DESCRIPTION
Package Name	The package name of the application.
Time Limit (m)	The time limit configured for the application, in minutes (converted from milliseconds).
Suspended	Indicates whether the application is currently suspended.

File Signature Mismatch (Audio)

Description	File Signature Mismatch (Audio) contains identified mismatches between a known file signature header and the extension (or lack thereof) for an audio file. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.

File Signature Mismatch (Container)

Description	File Signature Mismatch (Container) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a container. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.

File Signature Mismatch (Document)

Description	File Signature Mismatch (Document) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a document. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type, we return a mismatch.
File Path	The path to the mismatched file.

File Signature Mismatch (Picture)

Description	File Signature Mismatch (Picture) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a picture. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file. If the mime type is unknown, this defaults to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file. If the mime type is unknown, this defaults to application/octet-stream. If there is no file extension, but the mime type is known, a mismatch is is returned.
File Path	The path to the mismatched file.

File Signature Mismatch (Video)

Description	File Signature Mismatch (Video) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a video. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.

File System Information

Description	File System Information contains all of the relevant information about the hard drives in use by the operating system.
Notes	

ATTRIBUTE	DESCRIPTION
Volume Serial Number	This field only applies to FAT and NTFS file systems. This is a 32-bit unsigned int value that is stored in Bios Paramter Block (BPB) and is showed in a special hex format – XXXX-XXXX e.g. EABB-6573. For other file systems, the value of this field should show "n/a".
Full Volume Serial Number	This field is a 64-bit volume serial number that is only present in BPB of NTFS file system, for example AABBCCDDEEFF0011. For non-NTFS file systems, "n/a" is displayed for this field.
File System	The type of the file system (e.g "Microsoft NTFS").
Sectors per cluster	The number of sectors in a file system cluster.
Bytes per sector	The number of bytes per sector.
Starting Sector	The starting sector for this partition.
Ending Sector	The ending sector for this partition.
Total Sectors	Encase shows different values for this field based on how a volume is added to the case. For example, if you add just a volume (e.g. your local C:\ drive), it shows 123410271 for the number of sectors, but if you add your local physical drive 0 to the case and then select your C:\ volume in the "Entries" tree (note: your C drive would most likely have another letter in this tree, e.g. E:), then total number of sectors would be one more that the other value, i.e. 123410272. the value show for this field is taken from BPB, which matches the first value. The other value is shown when the parent physical drive is present probably comes from the partition table, and it counts VBR as well.
Total Capacity (Bytes)	This value is calculated by (Total Clusters) x (Cluster Size), which shows the capacity of the file system and not the volume containing it. The size of the volume would be higher than this value.
Total Clusters	The number of clusters comprising the file system.
Unallocated Area (Bytes)	The number of unallocated bytes on the file system, which is calculated by (Number of free clusters) x (cluster size).
Free Clusters	The number of unallocated clusters in the file system.
Allocated Area (Bytes)	This value is calculated by (Number of allocated clusters) x (cluster size).

ATTRIBUTE	DESCRIPTION
Volume Name	The volume label stored in Volume Boot Record (VBR).
Volume Offset (Bytes)	The offset (in bytes) of the volume containing this file system from beginning of the disk. "0" is displayed if the image and/or drive being searched is the image of one volume. Encase shows the number of sectors for this field instead of the number of bytes.
ID	The identifier of the hard drive.
Drive Type	The type of the hard drive.

Installed Applications

Description	Installed Applications contains a list of all of the applications on an Android device, including their versions.
Notes	

ATTRIBUTE	DESCRIPTION
Package Name	The internal name of the application.
Installed Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was installed.
Display Name	The display name of the application.
Platform	The platform of the application.
Category	The category of the application (either System or User).
Internal Version	The internal version of the application.
Display Version	The display version of the application.

Latent Wireless Geolocated WiFi Hotspots

Description	Latent Wireless Geolocated WiFi Hotspots contains information about WiFi hotspots that were discovered using a Latent Wireless device. Latent Wireless stores information about the hotspots in a database that Magnet AXIOM can parse for details about each hotspot.
Notes	

ATTRIBUTE	DESCRIPTION
MAC Address	The MAC address of the detected WiFi hotspot.
First Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was first discovered.
Last Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was last seen.

ATTRIBUTE	DESCRIPTION
Strongest Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was detected at its highest strength.
Network Name (SSID)	The SSID of the WiFi hotspot.
Channel	The WiFi hotspot channel.
RSSI	The receieved signal strength indicator for the WiFi hotspot.
Latitude	The latitude where the WiFi hotspot was detected.
Longitude	The longitude where the WiFi hotspot was detected.
Secure	Indicates whether the WiFi hotspot is secure.

MPT Application Details

Description	MPT Application Details contains information about activities that are triggered by applications and logged in the MPT on LG devices.
Notes	

ATTRIBUTE	DESCRIPTION
Date/Time - Local Time (yyyy-mm-dd)	The date and time that the log was entered into MPT.
Package Name	The internal Android package name of this application.
Application Name	The name used to describe this application to users.
Activity Type	A description of the type of activity taking place that is recorded.
Group Name	The application group name (Phone, Multimedia, Utilities, System UI, or Other Apps).
Additional Information	Additional descriptive text about the logged activity.

MPT Application History

Description	MPT App Usage contains information about application launches, overall usage, and installation/update/deletion timestamps (as recovered from the MPT on LG devices).
Notes	

ATTRIBUTE	DESCRIPTION
Date/Time - Local Time (yyyy-mm-dd)	The date and time that this log was entered into MPT.
Package Name	The internal package name belonging to the application.

ATTRIBUTE	DESCRIPTION
Version	The version number of the application. This value is not available if the app has been updated or deleted and will report the value "deleted".
Status	An interpreted value for the status of the application package when the log was updated.
Installed Date/Time - Local Time (yyyy-mm-dd)	Indicates when the package was installed by either the device or the user.
Updated Date/Time - Local Time (yyyy-mm-dd)	Indicates when the package was updated by either the device or the user.
Deleted Date/Time - Local Time (yyyy-mm-dd)	Indicates when the package was deleted by the user.
Usage Time (milliseconds)	The usage, in seconds, that this application has on record.
Number of Launches	The number of launches that this application has on record.

MPT Cell Towers

Description	MPT Cell Towers contains records of which cell towers a device connects to at a given time. Records are recovered from the MPT on LG devices, and are defined in the following format: MCC:MNC:LAC:CID.
Notes	

ATTRIBUTE	DESCRIPTION
Date/Time - Local Time (yyyy-mm-dd)	The date and time that this log was entered into MPT.
Cell ID	A GSM Cell ID (CID) is a generally unique number used to identify each base tranceiver station (BTS) or sector of a BTS within a location area code (LAC) if not within a GSM network.
Location Area Code	Location Area Code (LAC) is a unique number describing the set of base stations that are grouped together to optimize signalling.
Mobile Country Code	Mobile Country Code (MCC) is used in combination with Mobile Network Code (MNC) to uniquely identify a mobile network operator (carrier).
Mobile Network Code	Mobile Network Code (MNC) is used in combination with Mobile Country Code (MCC) to uniquely identify a mobile network operator (carrier).

MPT Recent Activity

Description	MPT Recent Activity tracks when applications were launched and terminated (as recovered from the MPT on LG devices).

Notes	

ATTRIBUTE	DESCRIPTION
Date/Time - Local Time (yyyy-mm-dd)	The date and time that this log was entered into MPT.
Start Date/Time - Local Time (yyyy-mm-dd)	The date and time that this application was started.
End Date/Time - Local Time (yyyy-mm-dd)	The date and time that this application was terminated.
Package Name	The internal package name belonging to the application.

MPT Wifi Events

Description	MPT Wifi Events includes connection and disconnection events for device wireless networking (as recovered from the MPT on LG devices).
Notes	

ATTRIBUTE	DESCRIPTION
Date/Time - Local Time (yyyy-mm-dd)	The date and time that this log was entered into MPT.
State	The event state. Values can be decoded as follows: 0 = Disconnecting, 1 = Disconnected, 2 = Connecting, 3 = Connected, 4 = Suspended.
Additional Information	This field is not always populated, but includes (separated by newlines): BSSID, IP Address, Link Speed, RSSI, Supplicant State.

Wi-Fi Logs - Android

Description	Wi-Fi Logs - Android contains information about the Wi-Fi networks that a device has connected to.
Notes	

ATTRIBUTE	DESCRIPTION
Network Name (SSID)	The name of the saved network.
BSSID	A unique identifier for the specific access point, which is often represented as the MAC address for the access point's wireless adapter.
Date/Time - Local Time (yyyy-mm-dd)	The date and time of the network connection. In instances where the year is missing from the source data, this value is represented as a string instead of a date/-time.
First Connected Date/Time - Local Time (yyyy-mm-dd)	The date and time of the connection event.

Peer-to-Peer

Torrent Active Transfers

Description	Torrent Active Transfers contains information about the torrents that are active on the user's system.
Notes	

ATTRIBUTE	DESCRIPTION
Torrent Name	The name of the torrent file.
Potential App Name	The name of the application that the torrent was potentially downloaded with.
Download Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the torrent file download was started.
Download Completed Date/Time - UTC (yyyy-mm-dd)	The date and time that the torrent file download was completed.
Download URL	The URL to download the torrent.
Downloaded Bytes	The total number of bytes that has been downloaded.
Download Location	The location on the disk to where the torrent was downloaded.
Bytes Uploaded	The total number of bytes that the system has uploaded for this torrent.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the active transfer was last modified.

Torrent Feeds

Description	Torrent Feeds contains information about RSS feeds that a user subscribes to that contains torrents available for download.
Notes	

ATTRIBUTE	DESCRIPTION
Feed Name	The name of RSS subscription feed.
Feed URL	The URL of the RSS subscription feed.
Torrent Name	The name of the torrent available for download from the feed.
Download URL	The URL to download the torrent.
Description	A description of the contents of the torrent.

ATTRIBUTE	DESCRIPTION
Published Date/Time - UTC (yyyy-mm-dd)	The date and time that the torrent feed item was published.
Status	The status of the feed item, either 'Downloaded' or 'Not Downloaded'.

Torrent File Fragments

Description	Torrent File Fragments contains data that is carved or parsed from .torrent files that are used to download torrents from various networks on the Internet.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the torrent file
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the torrent file was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the torrent file was modified.
Torrent Creation Date/Time - UTC (yyyy-mm-dd)	The date and time that the torrent file was originally created.
Torrent Files	The files that are listed in the torrent to be downloaded.

Social Networking

Android Instagram Following

Description	Android Instagram Following contains information about the users that are being followed by the local user.
Notes	

ATTRIBUTE	DESCRIPTION
ID	The unique identification number of a user.
User Name	The username of the user account.
Full Name	The full name of the user.
Biography	The biography written by the user.
External Access	A URL to an external website, provided by the user.
Blocked	Indicates whether the user being followed is blocked by the local user.
Status	Indicates the follow status of the local user (Following, Requested, and Not following).

ATTRIBUTE	DESCRIPTION
Profile Picture URL	The URL to the profile picture of the user.
Account Type	The account status of the user (Private or Public).

Android Instagram Posts

Description	Android Instagram Posts contains the posts that a user has put onto Instagram.
Notes	

ATTRIBUTE	DESCRIPTION
Post ID	The post ID.
ID	The ID of the user who made the post.
Full Name	The full name of the user.
Profile Picture URL	The URL to the profile picture of the user.
Downloaded Profile Image	The downloaded profile picture.
User Name	The username on Instagram.
Posted Image URL	The URL to the image that was posted.
Downloaded Posted Image	
Text	The text for the given image.
Created Date/Time - UTC (yyyy-mm-dd)	The date that the image was created.
Posted Date/Time - UTC (yyyy-mm-dd)	The date that the post was made.
Device Date/Time - UTC (yyyy-mm-dd)	

Android Instagram Users

Description	Android Instagram Users contains information on users of Instagram.
Notes	

ATTRIBUTE	DESCRIPTION
ID	The ID of the user.
Full Name	The full name of the user.
Profile Picture URL	The URL to the profile picture of the user.
Downloaded Profile Image	The downloaded profile picture.
User Name	The username of the user on Instagram.

Android Meet24 Cache Records

Description	Android Meet24 Cache Records contains items cached by Meet24 to improve performance.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the cached item.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The last date and time that the URL was visited.
First Visited Date/Time - UTC (yyyy-mm-dd)	The first date and time that the URL was visited.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The last date and time that the URL cache was synced.
File Type	The type of file that was cached, if a file was cached.
Content Size	The size of the file that was cached, if a file was cached.
Image	The bytes of an image file, if an image file was cached.
Content	The bytes of a non-image file that was cached.

Android Meet24 Cookies

Description	Android Meet24 Cookies contains cookies that Meet24 uses for persistent data.
Notes	

ATTRIBUTE	DESCRIPTION
Host	The host of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie is supposed to expire.
Path	The path of the cookie.

Android Whisper Posts

Description	Android Whisper Posts contains the posts stored by the Whisper application.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The username of the person at the time when the post was posted.
Text	The content of the post.
Posted Date/Time - UTC (yyyy-mm-dd)	The date and time that the post was posted.
Image URL	The URL to the image of the post.
Downloaded Image	The downloaded image from the post, if the option is turned on in Report Viewer.
Location	The location of the user when the post was posted.
Latitude	The latitude of the user when the post was posted.
Longitude	The longitude of the user when the post was posted.
Hearts	The number of hearts the post has received.
Replies	The number of replies to the post.

Facebook

Facebook, being one of the most popular social networking sites in the world, presents numerous opportunities for gathering evidence. You can recover messages that are sent and received, status updates and wall posts, and pages and pictures that the user views. On mobile devices, you can also recover user profiles and contacts.

Facebook can provide background information about a user, as well as evidence of who they are communicating with or associated with. Status and location updates can provide details about where a user has been and what they've been doing.

FORENSIC NOTES

The Facebook Pictures artifact represents cached pictures found on the system that originated from Facebook. When caching pictures, Facebook names the pictures using a particular format which allows forensic tools to know that they come from Facebook. These pictures can be user profile pictures, friends' pictures, or any other picture that gets cached while browsing Facebook.

ARTIFACTS

RELATED RESOURCES

How important are Facebook artifacts?

Recovering Facebook artifacts

Android Facebook Messages

Description	Android Facebook Messages contains Facebook messages recovered from the Android device.
Notes	

ATTRIBUTE	DESCRIPTION
User Key	The facebook ID for the user sending a message.
Name	The display name of the user sending a message.
Email	The email of the user sending a message.
Message ID	The unique ID of the message that was sent.
Text	The content of the message.
Message Source	Indicates if the message was sent from the web, messenger, chat, or mobile.
Coordinates	A GPS location associated with the message.
Send Timestamp Date/Time	The time when the message was sent.
Delivery Timestamp Date/Time	The delivery time of the message.

Android Facebook Pictures

Description	Android Facebook Pictures contains Facebook pictures that are recovered from the Android device.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the Facebook picture.
Filename	The file's absolute path on the device.
Image	The picture that was recovered.

Facebook Contacts

Description	Facebook Contacts contains contact information stored by the Facebook application.
Notes	

ATTRIBUTE	DESCRIPTION
Profile ID	The Facebook profile ID of the contact.
First Name	The Facebook contact's first name.
Last Name	The Facebook contact's last name.
Display Name	The Facebook contact's display name.
Small Picture URL	The URL to the the small picture.
Big Picture URL	The URL to the big picture.
Huge Picture URL	The URL to the huge picture.
Phone Numbers	The contact's phone numbers.

Facebook User/Friends

Description	Facebook User/Friends contains profile information for the Facebook users and friends recovered from the Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Friend/User	Indicates if the information is for the user or a friend.
User ID	The user ID of the user/friend.
First Name	The first name of the user/friend.
Last Name	The last name of the user/friend.
Display Name	The display name of the user/friend.
User Image URL	The URL to the user/friends profile picture.
Image	The profile picture.
Phone Number	The user/friends phone number.
Other	
Email(s)	The user/friends email address(es).
Birthday (MM/DD/YYYY)	The user/friends birthday.

Foursquare Check-ins

Description	Foursquare Check-ins contains information about the user's check-ins.
Notes	

ATTRIBUTE	DESCRIPTION
User Id	The user ID
User First Name	The user's first name.
User Last Name	The user's last name.
User Email	The email address of the account used to check in.
Check-In Date/Time - UTC (yyyy-mm-dd)	The date and time when the user checked-in to the specified locaiton.
Location Name	The name of the location that the user checked into.
Comment	The comment a user left about their check-in for the location.
Address	The address of the check-in location.
Latitude	The latitude of the check-in location.
Longitude	The longitude of the check-in location.
City	The city of the check-in location.
State	The state of the check-in location.
Country	The country of the check-in location.
Been Here Count	The number of times that the user has checked into this location.
User Gender	The user's gender.

Foursquare Locations

Description	Foursquare Locations contains the location information viewed in Foursquare.
Notes	

ATTRIBUTE	DESCRIPTION
Location Name	The name of the location.
Address	The address of the location.
Latitude	The latitude of the location.
Longitude	The longitude of the location.
Distance (meters)	The distance the user is from the location.
City	The city of the location.
State	The state of the location.

ATTRIBUTE	DESCRIPTION
Country	The country of the location.

Foursquare Searches

Description	Foursquare Searches contains the search terms used in Foursquare.
Notes	

ATTRIBUTE	DESCRIPTION
Search Term	The search term used within Foursquare.

Houseparty Messages

Description	Houseparty Messages contains messages recovered from Houseparty.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The username of the person sending the message.
Recipient	The username of the person receiving the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The content of the sent message.
Read Status	Indicates whether or not the message has been read.

Houseparty Users

Description	Houseparty Users contains information about the users that were contacted from the device using Houseparty.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The username of the user.
Full Name	The full name of the user.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the user account was created.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the user account was last updated.

Instagram Direct Messages

Description	Instagram Direct Messages contains Instagram direct messages that are sent or received by the local user.
Notes	Attachments can only be retrieved when searching a full physical extraction of a device.

ATTRIBUTE	DESCRIPTION
Sender	The username of the sender of the message.
Recipient	The username of the recipient of the message.
Direction	The direction of the message, relative to the source of the hit.
Message	The message that was sent.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the message.
Picture	The picture attribute is empty for Android as recovered pictures are located in the Attachment attribute instead.
Attachment Path	The path to the attachment that was sent.
Media URL	The URL to the media of the message.
Type	The message type.
Status	The status of the message.
Latitude	The latitude of the message.
Longitude	The longitude of the message.
Caption	The original message of a forwarded post.
Original Author	The original author of a forwarded post.
Original Date/Time	The original date and time of a forwarded post.

Instagram Group Members

Description	Instagram Group Members contains information about the Instagram groups that the local user is a member of.
Notes	

ATTRIBUTE	DESCRIPTION
Group Member	The username of the group member.
Group Name	The name of the group.

Instagram Media

Description	Instagram Media contains the media files that have been found inside the Insatgram application.
Notes	

ATTRIBUTE	DESCRIPTION
Picture	The picture of the media, or a storyboard if the media is a video.
MIME Type	The MIME type of the media.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the media file.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

Instagram Profiles

Description	Instagram Profiles contains profile information for the users that the local user has had communications with, or has been referred to through direct message communications.
Notes	For Android devices, the Following attribute will always be empty.

ATTRIBUTE	DESCRIPTION
User Name	The username of the profile.
Name	The name that is associated with the profile.
User ID	The user ID associated with the profile.
Profile Picture URL	The profile picture of the user's profile.
Local User	Indicates whether the profile belongs to a user logged into the device.

ATTRIBUTE	DESCRIPTION
Is Private	Indicates whether the profile is private or not.
Biography	The biography of the user associated with the account.
Following	Indicates whether the user of the profile is following the local user.
Is Followed By	Indicates whether the local user is following the user profile.
Post Notifications	Indicates whether the local user has turned on post notifications for the user profile. This attribute is only populated if the local user is following this user profile.
Email	The public email address associated with this user profile.
Phone Number	The public phone number associated with the user profile.
Address	The public address associated with the user profile.
City	The city associated with the user profile.
ZIP/Postal Code	The ZIP/postal code associated with the user profile.
Latitude	The latitude of the location associated with the user profile.
Longitude	The longitude of the location associated with the user profile.

LINE Chats

Description	LINE Chats contains the chats that the local user is a part of.
Notes	

ATTRIBUTE	DESCRIPTION
Participants	The users in the chat (other than the local user).
Chat Name	The name of the chat.
Owner	The owner of the chat.
Last Message	The last message that was sent in the chat.
Sender	The user who sent the last message.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the last message was received.
Message Count	The number of messages that were sent in the chat.
Read Count	The number of messages that were read in the chat by the local user.

LINE Contacts

Description	LINE Contacts contains the user's LINE contacts.
Notes	

ATTRIBUTE	DESCRIPTION
Line ID	The LINE ID of the contact.
Name	The name of the LINE contact.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time that the user contact was added.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the contact was last updated.
Status Message	The status of the contact.
Hidden	Indicates whether the contact has been marked as hidden.
Favorite	Indicates whether the contact has been marked as favorite.

LINE Messages

Description	LINE Messages contains messages that were sent and received through LINE on Android.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the message. The sender value can be the sender's name or Local User.
Recipient(s)	The recipient(s) of the message.
Message Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was created.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message	The body of the message.
Message Type	The type of the message. The Message Type value can be Audio, Call, Contact Card, File, Location, Note, Picture, Sticker, or Text.
Contact Card Name	The first and last name of the contact.
Read Count	The number of times that the message has been read.
Location Address	The address of the location.
Latitude	The latitude of the location when message type is Location.
Longitude	The longitude of the location when the message type is Location.
Audio Length (Seconds)	The length of the audio in seconds when the message type column is Audio.

ATTRIBUTE	DESCRIPTION
Call Duration (Seconds)	The duration of the call in seconds when the message type is Call.
File Attachment	The name of the file that's sent when the message type is File.
File Size (Bytes)	The size of the file sent in bytes.
Thumbnail	A thumbnail of the image (if available).

LINE Pictures

Description	LINE Pictures contains pictures originating from LINE.
Notes	

ATTRIBUTE	DESCRIPTION
Image	The image data that was recovered.
File Name	The name and extension of the file that the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.

ATTRIBUTE	DESCRIPTION
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture, or the name of the software that was used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
Longitude	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

LinkedIn Connections

Description	LinkedIn Connections contains information about LinkedIn users that have communicated with the local user account.
Notes	

ATTRIBUTE	DESCRIPTION
Public ID	The public ID of the LinkedIn connection.
First Name	The first name of the LinkedIn connection.
Last Name	The last name of the LinkedIn connection.
Occupation	The occupation of the LinkedIn connection.

LinkedIn Messages

Description	LinkedIn Messages contains messages sent and received by the local user.
Notes	

ATTRIBUTE	DESCRIPTION
Sender Name	The name of the sender.
Recipient Name(s)	The name(s) of the recipient(s).
Sent Date/Time	The date and time when the message was sent.
Message	The body of the message.
Attachment Name	The name of attachment to the message.
Attachment URL	The URL of attachment to the message.
Attachment Type	The type of the attachment to the message.

LinkedIn Profile

Description	LinkedIn Profile contains information about the user accounts that the local user has used to log in on the device.
Notes	

ATTRIBUTE	DESCRIPTION
UserName	The username of local user.
First Name	The first name of the local user.
Last Name	The last name of the local user.
Full Name	The full name of the local user.
Summary	A summary of the local user. This information is provided by the user and can indicate a number of different things, including the user's position or status.

LinkedIn Searches

Description	LinkedIn Searches contains information about the searches that a LinkedIn user has made on the local device.
Notes	

ATTRIBUTE	DESCRIPTION
Search Keyword	The keyword used by the user as a search term.
Date/Time	The date and time when the search occurred.
Search Type	The type of the search. This fragment is only populated if the user has specified the type of search to execute.

Musical.ly Local Users

Description	Musical.ly Local Users contains all of the users that have logged in to Musical.ly on the local device.
Notes	The country code and language of the local user cannot be retrieved on Android devices.

ATTRIBUTE	DESCRIPTION
User Name	The user's login name.
User Nickname	The user's chosen nickname.
User ID	The ID of the user in Musical.ly systems.
Account Description	The description that the user has given themself.
Image URL	The URL of the user's profile picture.
Instagram Account	The user's Instagram account.
Google Account	The user's Google account.
YouTube Channel	The user's YouTube Channel.
IP Address	The public IP address of the device that the user logged in with.
Is Private	Indicates whether the user prevents others from discovering their profile (Yes or No).
Hide Location	Indicates whether the user keeps their geolocation inforomation hidden on their profile page (Yes or No).
Messaging Availablilty	Indicates who is able to message the user, as specified by the user (Public or Friends Only).
Country Code	The country code of the country that the user has set for themself.
Language	The language code of the language that the user has set for themself.

Musical.ly Messages

Description	Musical.ly Messages contains messages sent or received in Musical.ly.
Notes	The read status for messages cannot be retrieved from Android devices.

ATTRIBUTE	DESCRIPTION
Sender	The sender of the message.
Recipient	The recipient of the message.
Message	The body of the message. This value is empty if a picture message was sent.
Direction	The direction of the message, relative to the source database.
Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was either received or sent on the local device.
Picture	The picture that was sent or received. This value is empty if a text message has been sent.
Read	Indicates whether or not the message has been read by the local device (Yes or No).
Message Status	The status of the message (Delivered or Pending Internet Connection).

Musical.ly Posts

Description	Musical.ly Posts contains posts that Musical.ly has retrieved from the web.
Notes	The picture and cached video of posts cannot be retrieved on Android devices.

ATTRIBUTE	DESCRIPTION
User Name	The username of the poster.
User Nickname	The nickname of the poster.
User ID	The ID of the poster.
Caption	The caption the user wrote for their post.
Picture	The locally cached post's preview picture.
Cached Video Size (Bytes)	The size of the locally cached post's video.
Video URL	The URL of the post's video.
Picture URL	The URL of the post's preview picture.

Musical.ly Users

Description	Musical.ly Users contains all of the users that the local user has viewed in Musical.ly.
Notes	The country code and language of the user cannot be retrieved on Android devices.

ATTRIBUTE	DESCRIPTION
User Name	The user's login name.
User Nickname	The user's chosen nickname.
User ID	The ID of the user in Musical.ly systems.
Account Description	The description that the user has given themself.
Profile Picture URL	The URL of the user's profile picture.
Instagram Account	The user's Instagram account.
Google Account	The user's Google account.
YouTube Channel	The user's YouTube Channel.
Is Private	Indicates whether the user prevents others from discovering their profile (Yes or No).
Is Friend	Indicates whether the user is a friend of the local user in the source database (Yes or No).
Following	Indicates whether the local user in the source database is following this user (Yes or No).
Post Notifications	Indicates whether the local user wants to receive notifications when this user makes a post (Yes or No).
Hide Location	Indicates whether the user keeps their geolocation information hidden on their profile page (Yes or No).
Messaging Avail-ablilty	Indicates who is able to message the user, as specified by the user (Public or Friends Only).
Country Code	The country code of the country that the user has set for themself.
Language	The language code of the language that the user has set for themself.

Pinterest Accounts

Description	Pinterest Accounts contains information about the accounts that the local user has logged in with on the device.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user ID of the local user.
Full Name	The full name of the local user.

ATTRIBUTE	DESCRIPTION
Email Address	The email address of the local user.
Created Date/Time	The created date and time of the local user.
Gender	The gender of the local user.
Country	The country of the local user.
Location	The location of the local user.
Profile Image URL	The profile image URL of the local user.
Active	The current status of the local user indicates whether the account is coming from an active database.

Pinterest Boards

Description	Pinterest Boards contains information about the boards that were created by local user.
Notes	

ATTRIBUTE	DESCRIPTION
ID	The ID of the board.
Name	The name of the board.
Category	The category of the board.
Description	The description of the board.
Created Date/Time	The created date and time of the board.
Website URL	The URL of the board.
Owner ID	The owner ID of the board.
Active Account	Active Account indicates whether the board is from the account that's currently logged in on the device.

Pinterest Following

Description	Pinterest Following contains information about the people or boards that local user follows.
Notes	

ATTRIBUTE	DESCRIPTION
Type	Type indicates what is being followed (People or Board).
ID	The ID of the following.

ATTRIBUTE	DESCRIPTION
Name	The name of the following.
Description	The description of the following.
Email	The email address of the following.
Created Date/Time	The created date and time of the following.
Country	The country of the following.
Location	The location of the following.
Profile Image URL	The profile image URL of the following.
Website URL	The website URL of the following.
Active Account	Active Account indicates whether the following user is of the account that's currently logged in on the device.

Pinterest Messages

Description	Pinterest Messages contains messages or pins sent and received by the local user.
Notes	

ATTRIBUTE	DESCRIPTION
Sender ID	The ID of the sender.
Sender Name	The name of the sender.
Recipient ID(s)	The user ID(s) of the recipient(s).
Recipient Name(s)	The name(s) of the recipient(s).
Sent Date/Time	The date and time that the message was sent.
Message	The content of the message.
Pin Title	The title of the pin.
Pin Picture URL	The picture URL associated with the pin.
Attachment Name	The file name of the picture cache associated with the pin.
Active Account	Active Account indicates whether the following user is of the account that's currently logged in on the device.

Pinterest Pins

Description	Pinterest Pins contains information about the items that the local user has pinned to their own board.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the pin.
Description	The description of the pin.
Created Date/Time	The created date and time of the pin.
Website URL	The URL of the website associated with the pin.
Posted Image URL	The posted image URL associated with the pin.
Attachment Name	The name of the attachment associated with the pin.
Pinner ID	The pinner ID of the pin.
Active Account	Active Account indicates whether the following user is of the account that's currently logged in on the device.

Sina Weibo Posts

Description	Sina Weibo Posts contains Sina Weibo posts that are recovered from a device.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The unique identifier for the user posting.
User Nickname	The user's nickname.
Post Date/Time - UTC (yyyy-mm-dd)	The date and time that the content was posted.
Post	The content of the post.
Profile Image URL	The URL for the profile image of the user.
Downloaded Profile Image	The raw content of the user's profile image, downloaded from the URL shown in the Profile Image URL column.
Post Image URL	The URL of the image in the post, if applicable.
Downloaded Post Image	The raw content of the image in the post, if applicable, and is downloaded from the URL shown in the Post Image URL column.
Posted Source	Information that describes the device from where the post was made.

ATTRIBUTE	DESCRIPTION
Latitude	The latitude of the post's source device when the post was made.
Longitude	The longitude of the post's source device when the post was made.

Sina Weibo Private Messages

Description	Sina Weibo Private Messages contains Sina Weibo messages that are recovered from a device.
Notes	

ATTRIBUTE	DESCRIPTION
Conversation Partner ID	The unique ID of the conversation partner.
Conversation Partner	The name of the conversation partner.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent/received.
Message	The actual private message content.
Profile Image URL	The URL for the profile image of the user.
Downloaded Profile Image	The raw content of the user's profile image, downloaded from the URL shown in the Profile Image URL column.
Attachment Type	The type of attachment associated with the message.
Attachment Local File Path	The local path to the file attachment.

TikTok Contacts

Description	TikTok Contacts contains information about a user's contacts in TikTok.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The username of the contact.
Nickname	The nickname of the contact.
ID	The unique ID of the contact.
Profile Picture URL	The URL of the profile picture of the contact.

TikTok Messages

Description	TikTok Messages contains information about the messages that a user sends or receives using TikTok.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the message.
Recipient	The recipient of the message.
Message	The content of the message.
Message Type	The type of the message.
Media URL	The URL of any media attached to the message.
Created Date/Time	The time that the message was sent.
Read	Whether the recipient has read the message.
Deleted	Whether the message has been deleted.

TikTok Videos

Description	TikTok Videos contains videos that were either viewed or created by the user.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file.
File Extension	The extension of the file.
Image	A generated thumbnail of the video.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the video file was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the video file was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was last written to.
Type	The type of the video.
Skin Tone Percentage	The amount of skin tone found in the video.
File Size (Bytes)	The size of the video.
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.

Tumblr Blogs

Description	Tumblr Blogs contains information about the blogs that the user has interacted with. These blogs can include both followed and blocked blogs, though it's not currently possible to distinguish between the two.
Notes	

ATTRIBUTE	DESCRIPTION
Blog Title	The title of the blog.
Description	The description of the blog.
Creator Name	The name of the blog's creator.
URL	The URL to the blog.

Tumblr Chat Messages

Description	Tumblr Chat Messages contains messages that were sent and received using Tumblr.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The display name of the user who sent the message.
Recipient	The display name of the user who received the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The body of the message.
Media URL	The URL of any media attached to the message.

Tumblr Tags

Description	Tumblr Tags contains information about the subject tags that the local user has selected. Selecting a tags expresses the user's interest in a subject so they can see more content of that type.
Notes	

ATTRIBUTE	DESCRIPTION
Tag	The tag that the local user selected.

Twitter Direct Messages

Description	Twitter Direct Messages contains carved and noncarved direct messages from the Twitter application. Note: Carving will not retrieve the names and screen names of the sender and receiver. Also, carving may be unable to retrieve the message direction on newer versions of Twitter.
Notes	

ATTRIBUTE	DESCRIPTION
Text	The text of the direct message.
Sender ID	The Twitter ID of the sender.
Recipient ID(s)	The Twitter ID for the recipient(s).
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date and time that the direct message was sent or received.
Direction	Whether the message was sent or received.
Sender Name	The name of the person sending the direct message.
Sender Screen Name	The screen name or Twitter handle of the person sending the direct message.
Recipient Name(s)	The name(s) of the person(s) receiving the direct message.
Recipient Screen Name(s)	The screen name(s) or Twitter handle(s) of the person(s) receiving the direct message.

Twitter Tweets

Description	Twitter Tweets contains carved and noncarved tweets from the Twitter application.
Notes	

ATTRIBUTE	DESCRIPTION
Author ID	The numeric ID of the account that posted the tweet.
Status ID	The unique ID of the tweet.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the tweet was created.
Tweet	The text content of the tweet.
Tweet Source	The interface that was used to post the tweet.
Favorited	Whether the tweet has been favorited.
Latitude	The latitude of the location from which the tweet was posted.
Longitude	The longitude of the location from which the tweet was posted.
Retweet Count	The number of times that the tweet has been retweeted.

Twitter Users

Description	Twitter Users contains friend information in Twitter data.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The friend's Twitter user ID.
User Name	The friend's Twitter username.
Profile Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the friend's Twitter profile was created.
Description	The short profile description that the friend writes for themself.
Web URL	The friend's website URL.
Following	'Yes' if the local user is following this account, 'No' otherwise. If this attribute is empty, it's undetermined whether the local user is following this account.
Location	The location the friend is from.
Protected	
Followers	The number of followers that the friend has.
Friends	The number of friends that the friend has.
Statuses	The number of different statuses that the friend has had.
Image URL	The URL to the friend's profile picture.
Friend Metadata Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the friend's meta information was last updated.
Header URL	The URL to the friend's profile banner picture.

VK Messages

Description	VK Messages contains VK messages (either private or group messages) as well as the details about pictures, video, and audio that may have been sent.
Notes	

ATTRIBUTE	DESCRIPTION
Sender ID	The user ID of the message sender.
Receiver ID (s)	The user ID of the message recipient. This column can contain multiple user IDs if the message is from a group conversation.

ATTRIBUTE	DESCRIPTION
Message Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent/received.
Message Text	The message text that was sent/received.
Type	The type of message sent. The possible types are 'Private Message' for one-to-one conversations or 'Group Message' for one-to-many conversations.
Message Deleted	The deletion state of the message is unsupported in VK Android and will therefore be empty.
Read State	The read state of the message is unsupported in VK Android and will therefore be empty.
Forwarded Message Content	This column contains the original time that a message was sent, the user ID that originally sent the message, and the content (for example, text, video, or audio).
VK Attachment	This column contains details of the attachment that was sent. For picture attachments, a URL to a scaled picture is provided for downloading. When a video is sent, a thumbnail is provided with details of the video (title, date/time, duration and description). When audio is sent, a URL to the audio is provided as well as the title, artist, and duration.
Latitude	The latitude in VK Android will be contained within VK Attachment or Forwarded Message Content and this column will be empty.
Longitude	The longitude in VK Android will be contained within VK Attachment or Forwarded Message Content and this column will be empty.

VK Users

Description	VK Users contains the various users the data owner has been in communication with, as well as the users own profile.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user ID of the user.
Gender	Identifies whether the user is a male or female.
Birthdate (yyyy-mm-dd)	The birthdate of the user.
First Name	The first name/given name of the user.
Last Name	The last name/surname of the user.
Profile Image	The URL to the users profile image.

Whisper Messages

Description	Whisper Messages contains the messages that were sent and received between the local user and others.
Notes	

ATTRIBUTE	DESCRIPTION
Partner Name	The username of the person the chat was with.
Message Text	The content of the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Status	The status of the message (Received or Sent).
Read	Whether or not the message was read by its recipient.
Sender Name	The username of the person who sent the message.
Image	The image that was sent or received.

Transportation and Travel

OnStar RemoteLink Accounts

Description	Contains information about all the OnStar RemoteLink accounts found on the device.
Notes	

ATTRIBUTE	DESCRIPTION
Account Number	The OnStar account number of the suspect.
Account Key	A secondary identifier for the account on the device.
Created Date/Time	The date and time the account was created on the device.
Updated Date/Time	The date and time the account was updated on the device.
Country Code	The country code associated with the user account.
First Name	The first name of the account holder.
Last Name	The last name of the account holder.
Selected VIN	The VIN of the vehicle that was selected by the app at the time of extraction.

OnStar RemoteLink Hotspot Info

Description	Information about the vehicle Wi-Fi hotspots associated with an OnStar account.
Notes	

ATTRIBUTE	DESCRIPTION
Network Name(SSID)	The name of the vehicle's hotspot.
Network Password	The password of the vehicle's hotspot.
Created Date/Time	The date and time the hotspot was created.
Updated Date/Time	The date and time the hotspot was updated.
VIN	The Vehicle Identification Number that the hotspot is associated with.

OnStar RemoteLink Recent Location Searches

Description	OnStar RemoteLink Recent Location Searches contains the location searches and commands performed on the results of the searches.
Notes	

ATTRIBUTE	DESCRIPTION
Destination Address	The addresses searched for by the suspect.
Timestamp Date/Time	The date and time that the search was completed.
Created Date/Time	The date and time the entry was created on the device.
Updated Date/Time	The date and time the entry was updated on the device.
Command	The command used to send the address to the vehicle.
Command Status	The status of the command.
Destination Name	The name of the destination address if one was assigned.
VIN	The Vehicle Identification Number of the vehicle to which the command was sent.

OnStar RemoteLink Remote Commands

Description	OnStar RemoteLink Remote Commands contains information about commands sent from the device.
Notes	

ATTRIBUTE	DESCRIPTION
Requested Command	The command requested by the user.
Request State	The state of the request.
Sent Date/Time	The date and time that the command was sent to the vehicle.
Completion Date/Time	The date and time that the command was completed.
Command Description	The description of the command that was sent, if one is available.
VIN	The Vehicle Identification Number of the vehicle that the command was sent to.
Request ID	The ID of the request that was sent, if available.

OnStar RemoteLink Saved Places Of Interest

Description	OnStar RemoteLink Saved Places Of Interest contains addresses for places of interest saved in the OnStar RemoteLink application.
Notes	

ATTRIBUTE	DESCRIPTION
Address	The full address stored in the application.
State/Province	The state/province of the address.
Country	The country of the address.
Latitude	The latitude of the address to map on the world map.
Longitude	The longitude of the address to map on the world map.
Address URL	The URL of the address as stored by OnStar.
Created Date/Time	The date and time that the saved entry was created on the device.
Updated Date/Time	The date and time that the saved entry was updated on the device.
Name	The name of the saved address.

OnStar RemoteLink Saved Wireless Carrier

Description	OnStar RemoteLink Saved Wireless Carrier contains information about the wireless accounts associated with a vehicle.
Notes	

ATTRIBUTE	DESCRIPTION
Carrier Account ID	The account identifier of the carrier account.
Carrier Type Code	The code that represents the account type.

ATTRIBUTE	DESCRIPTION
Carrier Type Description	The carrier associated with the account.
Created Date/Time	The date and time that the account entry was created on the device.
Updated Date/Time	The date and time that the account entry was updated on the device.
Account Type	The type of wireless account.
Account Description	The description of the account type.
VIN	The Vehicle Identification Number of the vehicle that the wireless account is associated with.

OnStar RemoteLink Vehicle Diagnostics

Description	OnStar RemoteLink Vehicle Diagnostics contains information about the diagnostic values that were retrieved from the vehicle.
Notes	

ATTRIBUTE	DESCRIPTION
Diagnostic Name	The name of the diagnostic test that was retrieved.
Unit	The unit of measurement associated with the diagnostic test.
Value	The value associated with the diagnostic test.
Created Date/Time	The date and time that the diagnostic value was retrieved.
Updated Date/Time	The date and time that the diagnostic value was updated.
Completion Date/Time	The date and time that the server retrieved the diagnostic value from the vehicle.
VIN	The Vehicle Identification Number of the vehicle that the diagnostic value was retrieved from.

OnStar RemoteLink Vehicle Info

Description	OnStar RemoteLink Vehicle Info contains information about the vehicle associated with the account.
Notes	

ATTRIBUTE	DESCRIPTION
VIN	The Vehicle Identification Number of the vehicle associated with the account.
Vehicle Make	The make of the vehicle.

ATTRIBUTE	DESCRIPTION
Vehicle Model	The model of the vehicle.
Year	The year of production of the vehicle.
Created Date/Time	The date and time that the vehicle information was added to the device.
Updated Date/Time	The date and time that the vehicle information was updated on the device.
Phone Number	The phone number associated with the vehicle.
Account Number	The OnStar account number that the vehicle is associated with.

Uber Accounts

Description	Uber Accounts contains account information for riders, as recovered from the Uber application (passenger only).
Notes	

ATTRIBUTE	DESCRIPTION
First Name	The first name of the account holder.
Last Name	The last name of the account holder.
Mobile Phone	The mobile phone number associated with the acount.
Share Code	A unique share code associated with the rider.
User ID	The user ID uniquely identifying the account.
Latitude (On App Startup)	The latitude of the user when the application was last opened.
Longitude (On App Startup)	The longitude of the user when the application was last opened.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the user last opened the application.
Last Payment Profile ID	The ID of the payment profile that was last used by the user.
Profile Image URL	The URL of the profile image for the account.

Uber Cached Locations

Description	Uber Cached Locations contains information about locations that Uber caches, such as the initial location on the application's startup, or locations from a trip (passenger only).
Notes	

ATTRIBUTE	DESCRIPTION
Latitude	The GPS latitude of the cached location.
Longitude	The GPS longitude of the cached location.

ATTRIBUTE	DESCRIPTION
Address	The address of the cached location.
Date/Time - UTC (yyyy-mm-dd)	The date and time when the location was cached.
Tag	The user created tag given to the location.

Uber Payments

Description	Uber Payments contains payment information associated with a user's rides, as recovered from the Uber application (passenger only).
Notes	

ATTRIBUTE	DESCRIPTION
Rider Name	The name of the passenger/rider.
Share Code	A unique share code associated with the rider.
Cost	The cost of the trip.
Currency	The currency used to measure the cost of the trip.
Duration (Seconds)	The duration of the trip.
Distance (Kilometers)	The distance of the trip.
Payment Method	The method of payment.
Card Display Name	The payment card display name.

Uber Profiles

Description	Uber Profiles contains information about a user's Uber profiles, as recovered from the Uber application (passenger only).
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	The name of the profile.
Profile Email	The email associated with the profile.
Profile User ID	The unique user ID (UUID) associated with the profile.
Profile Payment User ID	The unique user ID that is the payment method for this profile.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the profile was created.

Uber Trips

Description	Uber Trips contains information about a user's Uber rides, as recovered from the Uber application (passenger only).
Notes	

ATTRIBUTE	DESCRIPTION
Booking Date/Time UTC (yyyy-mm-dd)	The date and time when the trip was booked.
Origin Address	The address of the original start location.
Destination Address	The address of the final destination.
Arrival Date/Time UTC (yyyy-mm-dd)	The date and time when the vehicle arrived at the destination address.
Duration (Seconds)	The duration of the trip.
Distance	The distance of the trip, units unknown.
Driver Name	The first name of the driver.
Vehicle Make	The make of the driver's vehicle.
Vehicle Model	The model of the driver's vehicle.
Vehicle Type	The type of Uber car service.
Driver Rating	The driver's rating.
Driver Picture URL	The URL to the driver's profile picture.
Cost	The cost of the trip.
Currency	The currency used to measure the cost of the trip.
Status	The status of the trip.
Route Map URL	The URL to the route taken in the trip.

Waze Events

Description	Waze Events can contain information about upcoming trips that a user has planned.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the place.
Address	The house number and street name of the place.
City	The city of the address.
State	The state/province of the address.
Country	The country of the address.
Start Date/Time	The start date and time that was recommended for the planned drive.

ATTRIBUTE	DESCRIPTION
End Date/Time	The date and time that the user planned to arrive at the destination.
Created Date/Time	The date and time when the event was created.
Is All-day Event	Indicates if the planned drive is an all-day event.
Latitude	The GPS latitude coordinates of the place.
Longitude	The GPS longitude coordinates of the place.

Waze Favorites

Description	Waze Favorites contains information about locations that a user has bookmarked as a favorite.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the place bookmarked as a favorite
Address	The house number and street name of the place.
City	The city of the address.
State	The state/province of the address.
Country	The country of the address.
Created Date/Time	The date and time that the address was added as a favorite.
Modified Date/Time	The date and time that the favorite location was last modified by the user.
Accessed Date/Time	The date and time that the favorite location was last accessed in Waze.
Latitude	The GPS latitude coordinates of the place.
Longitude	The GPS longitude coordinates of the place.

Waze Places

Description	Waze Places contains all of the places that the user has searched using Waze.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the place.
Address	The house number and street name of the place.
City	The city of the address.
State	The state/province of the address.
Country	The country of the address.

ATTRIBUTE	DESCRIPTION
Created Date/Time	The date and time when the address was entered in Waze.
Accessed Date/Time	The last date and time when the address was accessed in Waze.
Latitude	The GPS latitude coordinates of the place.
Longitude	The GPS longitude coordinates of the place.

Web Related

Aloha Browser Autofill

Description	Aloha Autofill contains records of the autofill values that Aloha saves for different types of text fields.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the autofill value.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill was last used.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Aloha Browser Bookmarks

Description	Aloha Bookmarks contains the webpages that a user has bookmarked.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was added.
Title	The name of the bookmark.
Parent	The name of the parent folder of the bookmark
Is Folder	Indicates whether the bookmark entry is a folder.

Aloha Browser Downloads

Description	Aloha Browser Downloads contains information about the files that a user downloads from the Internet.
Notes	

ATTRIBUTE	DESCRIPTION
Download URL	The URL of the file that was downloaded.
File Path	The absolute path on the device to the file downloaded.
URL	The URL of the site in which the file was downloaded.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was downloaded.

Aloha Browser History

Description	Aloha Browser History contains information about the websites that the user visits.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited page.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the user first visited the webpage.
Title	The title of the webpage.
Visit Count	The number of times the user has visited that webpage.

Android Browser Bookmarks

Description	Android Browser Bookmarks contians the webpages that a user has bookmarked.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the bookmark.
Name	The name of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date/time when the bookmark was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date/time when the bookmark was last modified.
Is Folder	Indicates whether the bookmark entry is a folder.

Android Browser Search Terms

Description	Android Browser Search Terms contains information about the keyword search terms a user has provided in the browser.
Notes	

ATTRIBUTE	DESCRIPTION
Search Term	The search term that the user entered.
Search Date/Time - UTC (yyyy-mm-dd)	The date/time when the search was entered.

Android Browser Web History

Description	Android Browser Web History contains information about the websites that the user has visited.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited page.
Title	The title of the webpage that was visited.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date/time when the webpage was last visited.
Visit Count	The number of times the webpage was visited.

Android Firefox Bookmarks

Description	Android Firefox Bookmarks contains bookmarks from the Firefox web browser on an Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the bookmark.
URL	The URL of the bookmark.
Keyword	Any keywords that have been associated with the bookmark. These keywords are user generated.
Description	A description of the bookmark.
Tags	Any tags that have been associated with the bookmarks. These tags are user generated.

ATTRIBUTE	DESCRIPTION
Date Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was last modified.
Deleted	Indicates whether the bookmark was deleted (Yes or No).

Android Firefox Web History

Description	Android Firefox Web History contains the webpage history from the Firefox web browser on an Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the webpage.
URL	The URL of the webpage.
Visit Count	The number of times that the user has visited that webpage.
First Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the person first visited the webpage.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage history was last modified.
Deleted	Indicates whether the webpage history was deleted (Yes or No).

Android Google Maps

Description	Android Google Maps contains information about the locations that a user searches for using Google Maps.
Notes	

ATTRIBUTE	DESCRIPTION
Search Query	The location that the user searched for
Latitude	The latitude associated with the search.
Longitude	The longitude associated with the search.
URL	The URL that contains the search query.

ATTRIBUTE	DESCRIPTION
CID	A unique ID - also known as ludocid - that Google assigns to a specific business location in order to identify it within its systems.
FID	A unique ID that relates to reviews that Google holds about a specific business.

Autofill

Description	Brave Autofill contains records of the autofill values that Brave saves for different types of text fields.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when autofill was last used.
Value	The saved autofill value for this type of field.
Count	The autofill count.

Baidu Searches

Description	Baidu Searches Contains information about the search history using the Baidu application.
Notes	

ATTRIBUTE	DESCRIPTION
Search Term	The term that was searched.
Picture Path	The path to the picture that was searched.
Picture URL	The URL of the picture that was searched.
Search Type	The type of search. The options are Text or Picture.
Search Date/Time	The date/time of the search.

Baidu Web Visits

Description	Baidu Web Visits contains a history of the websites that the user visited using the Baidu application.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the website.
Web Page Title	The title of the webpage.
Visited Date/Time	The date/time when the URL was visited

Brave Bookmarks

Description	Brave Bookmarks contain bookmarks that reference saved webpages.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Brave Cookies

Description	Brave Cookies contain cookies that Brave downloads from the Internet. These cookies contain information about the websites that a user visits.
Notes	

ATTRIBUTE	DESCRIPTION
Host	The domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Brave Downloads

Description	Brave Downloads contains information about the files that a user downloads from the Internet.

Notes	

ATTRIBUTE	DESCRIPTION
Download Source	The URL of the file that was downloaded.
File Name	The name of the downloaded file.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download finished.
Saved To	The absolute path on the device to the downloaded file.
State	The completion state of the download.
Opened By User	Indicates whether the user has opened the downloaded file or not.
Bytes Downloaded	The bytes that were downloaded.
Total Bytes	The file size of the download.

Brave Favicons

Description	Brave Favicons contains the favicons that Brave displays in the address bar when visiting a website. These icons are sometimes downloaded when you favorite/bookmark a website.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last date and time that the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Brave Keyword Search Terms

Description	Information about the keyword search terms that a user enters.
Notes	

ATTRIBUTE	DESCRIPTION
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.

Brave Tab History - Android

Description	A history of websites the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the tab file.
Tab ID	The unique ID of a tab entry in a tab file.
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request to open the web page (for example, the referrer source might be from Google or another third-party application).
Originating URL	The URL of the webpage that led the user to the current URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Search Term	The value the user entered into a search.

Brave Top Sites

Description	A list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Notes	

ATTRIBUTE	DESCRIPTION
URL	URL of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the site was last updated.
Title	The title of the site.
Thumbnail	The thumbnail of the site.

Brave Web History

Description	A history of the websites that the user visits (includes unique visits only).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

Brave Web Visits

Description	A history of the websites that the user visits (includes all visits).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Calc Vault Browser Bookmarks

Description	Calc Vault Browser Bookmarks contains the webpages a user has saved while using Calc Vault.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the bookmark.
URL	The URL of the bookmark.
User Added	Indicates whether the user added the bookmark (Yes if the user added the bookmark, or No if it is a default bookmark).

Calc Vault Browser History

Description	Calc Vault Browser History contains information about the webpages a user has visited using Calc Vault.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the webpage visited.
URL	The URL of the webpage visited.

Chrome

Google Chrome is free web browser developed by Google and is available on all major operating systems, for both mobile and desktop. As of 2016, Chrome usage represents over 70% of the world's total browser traffic.

Analyzing the websites a user visits and the time the visits occur can provide valuable insights about a user. One notable feature that Google Chrome has is that it allows users to sync their bookmarks, browsing history, and more across multiple platforms and devices by using cloud sync accounts.

FORENSIC NOTES

Web Visits vs Web History

Chrome has two distinct artifacts that are very similar nature: Chrome Web Visits and Chrome Web History. Both of these artifacts are recovered from the History database. Chrome Web History is parsed from the URLS table and only contains information for the last visited date of a particular website. Chrome Web Visits can contain multiple entries for the same website, giving the examiner a more complete look at browser usage if the user visited a website multiple times. For example, if a user visits www.magnetforensics.com six times, the Chrome Web History artifact displays only the last time the site is visited, while the Chrome Web Visits artifact potentially displays records for all six instances. Chrome Web Visits was added in a later version of Chrome than Chrome Web History.

Carved web history

The Chrome / 360 Safe Browser / Opera Carved Web History is essentially the same as Chrome Web History except that it's recovered using carving and you may find additional deleted hits with it. The 360 Safe and Opera browsers are included in this artifact because when the data is carved, it's not possible to tell which browser the hit comes from as they're all formatted the same way.

Autofill and profile data

Chrome stores field data that the user has previously input as autofill and profile settings. For example, if you visit magnetforensics.com and login to the customer portal, browsers automatically save your username (and other details) so that you don't have to type it in each time you visit the site. This data is helpful for recovering usernames and other information that your user has filled out on various sites.

Sessions and tabs

When the system has an active session available, Chrome stores the browsing activity as the Chrome Current Session and any tabs that are open as Chrome Current tabs. The previous session and tabs are maintained in Chrome Last Session and Chrome Last Tabs so that the user can restore the last session and tabs if Chrome is closed.

ARTIFACTS

RELATED RESOURCES

How does Chrome's 'incognito' mode affect digital forensics?

Forensic email analysis: browser artifacts you may find on a PC or laptop

Android Archived Web History

Description	Android Archived Web History contains an archived history of old webpage visits.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL where the archived web history is located.
Title	The title of the archived web history.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.
Visit Count	The total number of visits to the URL.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
ID	The ID for the web history archive.

Android Autofill

Description	Chrome Autofill contains records of the autofill values that Chrome saves for different types of text fields.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the autofill value.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill was last used.

Android Chrome Autofill Profiles

Description	Android Chrome Autofill Profiles contains profiles that Chrome uses to fill in forms with saved values.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name for the autofill profile.
Email	The email used in the the autofill profile.
Number	The phone number used in the autofill profile.
Company	The company name used in the autofill profile.
Address Line 1	The address Line 1 used in the autofill profile.
Address Line 2	The address Line 2 used in the autofill profile.

ATTRIBUTE	DESCRIPTION
City	The city used in the autofill profile.
State	The state used in the autofill profile.
Zipcode	The ZIP code used in the autofill profile.
Country	The country used in the autofill profile.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the profile was last modified.

Android Chrome Favicons

Description	Android Chrome Favicons contains the favicons that Chrome displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	The page URL of the favicon.
Icon URL	The icon URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last time the favicon was updated.
Icon	A preview of the favicon.

Android Chrome Logins

Description	Android Chrome Logins contains login information that a user provides in Chrome. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the login page.
Username	The username entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the data was created.

Android Chrome Saved Credit Cards

Description	Android Chrome Saved Credit Cards contains the credit card information saved by the user.
Notes	

ATTRIBUTE	DESCRIPTION
GUID	The GUID of the user.
Name On Card	The name of the person on the credit card.
Expiry Date	The date the credit card is supposed to expire in month-year format.
Card Number	The number on the credit card.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the information was last modified.

Android Chrome Top Sites

Description	Android Chrome Top Sites contains a list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the site.
Title	The title of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the site was last updated.
Rank	The rank of the website, where the rank is based on how frequently the website was visited. A value of 1 indicates the most frequent and values increment to 8 as frequency decreases. A value of -1 indicates a site that the user manually added to the list of top sites.
Thumbnail	The thumbnail of the site.

Android Chrome Web Visits

Description	Android Chrome Web Visits contains a history of the websites that the user visits (includes all visits).

Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited webpage.
Title	The title of the webpage that was visited.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is link.
Visit Source	The source of the visit.

Android Downloads

Description	Android Downloads contains information about the files that a user downloads from the Internet.
Notes	

ATTRIBUTE	DESCRIPTION
Download Source	The URL of the file that was downloaded.
Save Location	The absolute path on the device to the downloaded file.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified.
Notification Package	The Android package name that the download was initiated in.
Bytes Downloaded	The bytes that were downloaded.
Total Bytes	The file size of the download.

Chrome Bookmarks

Description	Chrome Bookmarks contains browser bookmarks that reference saved webpages.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.

ATTRIBUTE	DESCRIPTION
Type	The type of bookmark.

Chrome Cache Records

Description	Chrome Cache Records contains content that Chrome downloads and caches to speed up rendering times. Cached content can include pictures, text, HTML, javascript, and more.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the cached item.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was first visited.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The date and time when the cache was last synced with the cloud.
File Type	The type of file that was cached.
Content Size (Bytes)	The size of the cached file.
Image	The cached image if the file type is an image. If the file type is not an image, this column is empty.
Content	The cached file contents if the file type is not an image. If the file type is an image, this column is empty.

Chrome Cookies

Description	Chrome Cookies contains cookies that Chrome downloads from the Internet. These cookies contain information about the websites that a user visits.
Notes	

ATTRIBUTE	DESCRIPTION
Host	The domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.

ATTRIBUTE	DESCRIPTION
Path	The path of the cookie value.

Chrome Keyword Search Terms

Description	Chrome Keyword Search Terms contains information about the keyword search terms that a user enters.
Notes	

ATTRIBUTE	DESCRIPTION
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.

Chrome Sync Accounts

Description	Chrome Sync Accounts contains information about the Chrome accounts that a user has logged in with. Chrome syncs data to the cloud so that a user can log in on multiple devices.
Notes	

ATTRIBUTE	DESCRIPTION
Sync Id	The unique ID for the account that's used to sync data to the cloud.
Account Name	The name of the sync account.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the sync account was created.

Chrome Sync Data

Description	Chrome Sync Data contains information about the data that Chrome has synced to a user's account in the cloud.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the sync key.
Local Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the value on the local system.

ATTRIBUTE	DESCRIPTION
Server Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the value on the server.
Local Created Date/Time - UTC (yyyy-mm-dd)	The created time of the value on the local system.
Server Created Date/Time - UTC (yyyy-mm-dd)	The created time of the value on the server.
Type	The type of data that is synced (bookmark, favicon, type URL, and so on).
Parsed Content	The type of parsed data.
Favicon Image	The actual favicon image.

Chrome Tab History

Description	Chrome Tab History contains a history of websites that the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the tab file.
Tab ID	The unique ID of a tab entry in a tab file.
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request to open the webpage (for example, the referrer source might be from Google or another third-party application).
Originating URL	The URL of the webpage that led the user to the current URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Search Term	The value that the user entered into a search.

Chrome Web History

Description	Chrome Web History contains a history of the websites that the user visits (includes unique visits only).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

Dolphin Browser Bookmarks

Description	Dolphin Browser Bookmarks contains bookmarks from the Dolphin web browser on an Android device.
Notes	The Modified Date/Time field is always empty for Android.

ATTRIBUTE	DESCRIPTION
Title	The title of the bookmark.
URL	The URL of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was modified.
Visits	The number of times that the user visited this bookmark.

Dolphin Browser History

Description	Dolphin Browser History contains the webpage history from the Dolphin web browser on an Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the webpage.
URL	The URL of the webpage.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the user first visited the webpage.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the user last visited the webpage.
Visits	The number of times that the user has visited the webpage.

DuckDuckGo Bookmarks

Description	DuckDuckGo Bookmarks contains information about the webpages that a user has bookmarked.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the bookmark.
Name	The name of the bookmark.
Favorite	Indicates whether the link was added as a favorite. This value is not currently populated for Android.

DuckDuckGo Cookies

Description	DuckDuckGo Cookies contains cookies that DuckDuckGo downloads from the Internet. These cookies contain information about the websites that a user visits.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

DuckDuckGo Current Tabs

Description	DuckDuckGo Current Tabs contains information about the tabs that are open in the current browser session.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the webpage.
Title	The title of the webpage.

ATTRIBUTE	DESCRIPTION
Was Viewed	Whether the tab was viewed on the local device or not.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that URL was accessed.
Attachment Path	If a snapshot was saved for that tab, this fragment stores the path of the snapshot image file.

DuckDuckGo Whitelisted Websites

Description	DuckDuckGo Whitelisted Websites contains information about domains that are trusted or protected from deletion by the user.
Notes	

ATTRIBUTE	DESCRIPTION
Domain	The domain of the website.
Status	Whether the domain was whitelisted or fire proofed. Whitelisted indicates to DuckDuckGo that the domain should always be trusted. Fire proofed domains will keep the navigation data even if the user clicks the option 'Clear All Tabs and Data'.

Ecosia Autofill

Description	Ecosia Autofill contains records of the autofill values that Ecosia saves for different types of text fields.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when autofill was last used.
Value	The saved autofill value for this type of field.
Count	The count of the autofill.

Ecosia Bookmarks

Description	Ecosia Bookmarks contain browser bookmarks that reference saved webpages.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Ecosia Cookies

Description	Ecosia Cookies contains cookies that Ecosia downloads from the Internet. These cookies contain information about the websites that a user visits.
Notes	

ATTRIBUTE	DESCRIPTION
Host	The domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Ecosia Downloads

Description	Ecosia Downloads contains information about the files that a user downloads from the Internet.
Notes	

ATTRIBUTE	DESCRIPTION
Download Source	The URL of the file that was downloaded.
File Name	The name of the downloaded file.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download finished.
Saved To	The absolute path on the device to the downloaded file.
State	The completion state of the download.
Opened By User	Indicates whether the user has opened the downloaded file or not.

ATTRIBUTE	DESCRIPTION
Bytes Downloaded	The bytes that were downloaded.
Total Bytes	The file size of the download.

Ecosia Favicons

Description	Ecosia Favicons contains the favicons that Ecosia displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last date and time when the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Ecosia Keyword Search Terms

Description	Ecosia Keyword Search Terms contains information about the keyword search terms that a user enters.
Notes	

ATTRIBUTE	DESCRIPTION
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.

Ecosia Logins

Description	Ecosia Logins contains login information that a user provides in Ecosia. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the login page.

ATTRIBUTE	DESCRIPTION
Username	The username entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the data was created.

Ecosia Tab History

Description	Ecosia Tab History contains a history of websites that the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the tab file.
Tab ID	The unique ID of a tab entry in a tab file.
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request to open the webpage (for example, the referrer source might be from Google or another third-party application).
Originating URL	The URL of the webpage that led the user to the current URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Search Term	The value that the user entered into a search.

Ecosia Top Sites

Description	Ecosia Top Sites contains a list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the site was last updated.
Title	The title of the site.
Thumbnail	The thumbnail of the site.

Ecosia Web History

Description	Ecosia Web History contains a history of the websites that the user visits (includes unique visits only).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times that the webpage was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).

Ecosia Web Visits

Description	Ecosia Web Visits contains a history of the websites that the user visits (includes all visits).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Edge Chromium Bookmarks

Description	Browser bookmarks that reference saved webpages.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Edge Chromium FavIcons

Description	Contains the favicons that Chrome displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	The page URL of the favicon.
Updated Date/Time - UTC (yyyy-mm-dd)	The last time the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Edge Chromium Keyword Search Terms

Description	Information about the keyword search terms that a user enters.
Notes	

ATTRIBUTE	DESCRIPTION
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.

Edge Chromium Tab History

Description	A history of websites the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the tab file.
Tab ID	The unique ID of a tab entry in a tab file.
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request to open the web page (for example, the referrer source might be from Google or another third-party application).
Originating URL	The URL of the webpage that led the user to the current URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Search Term	The value the user entered into a search.

Edge Chromium Web History

Description	A history of the websites that the user visits (includes unique visits only).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

Edge Chromium Web Visits

Description	A history of the websites that the user visits (includes all visits).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.

ATTRIBUTE	DESCRIPTION
Title	The title of the webpage that was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Firefox Cache Records

Description	Firefox Cache Records contains the files that the Firefox web browser has cached on a device.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of file that was cached.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cache file was created.
MIME Type	The MIME type of the file.
Content Size (Bytes)	The size of the cached file.
Image	A preview of the cached file, if the cached file is anything but a picture.

Firefox Cookies

Description	Firefox Cookies contains the cookies from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
Host	The host domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-MM-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-MM-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-MM-dd)	The date and time when the cookie will expire, if it is set to expire.
Path	The path to the cookie.

Firefox FormHistory

Description	Firefox FormHistory contains the form history from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
Field Name	The name of the field.
Value	The value of the field.
First Used Date/Time - UTC (yyyy-MM-dd)	The date and time when the field was first used.
Last Used Date/Time - UTC (yyyy-MM-dd)	The date and time when the field was last used.
Times Used	The number of times that the field was used.
ID	The unique ID of the field.

Google Analytics First Visit Cookies

Description	Google Analytics First Visit Cookies contains information about Google Analytics first-visit cookies that are discovered in other artifacts.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the URL.
Creation DateTime	The date and time when the site was vist visited.
Most Recent Visit Date/Time	The date and time of most recent session.
2nd Most Recent Visit Date/Time	The date and time of previous session.
Hits	The number of visits.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Google Analytics First Visit Cookies Carved

Description	Google Analytics First Visit Cookies Carved contains information about Google Analytics first-visit cookies that are recovered using carving.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the URL.
Creation DateTime	The date and time when the cookie was created.
Most Recent Visit Date/Time	The date and time of the most recent session.
2nd Most Recent Visit Date/Time	The date and time of the second most recent session.
Hits	The number of visits.

Google Analytics Referral Cookies

Description	Google Analytics Referral Cookies contains information about Google Analytics referral cookies that are discovered in other artifacts.
Notes	

ATTRIBUTE	DESCRIPTION
Cookie Source	The source URL used to reach the site.
Host	Contains the domain of the URL.
Update Date/Time	The last time the cookie was updated.
Campaign	The method of referral.
Access Method	Indicates whether the site was accessed organically or was referred.
Keyword	The keywords used to arrive at the site.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Google Analytics Referral Cookies Carved

Description	Google Analytics Referral Cookies Carved contains information about Google Analytics referral cookies that are recovered using carving.
Notes	

ATTRIBUTE	DESCRIPTION
Cookie Source	The source URL used to reach the site.
Host	Contains the domain of the URL.
Update Date/Time	The last time the cookie was updated.
Campaign	The method of referral.
Access Method	Indicates whether the site was accessed organically or was referred.
Keyword	The keywords used to arrive at the site.

Google Analytics Session Cookies

Description	Google Analytics Session Cookies contains information about Google Analytics session cookies that are discovered in other artifacts.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the URL.
Page Views	The number of visits to this page from the user.
Start Current Session Date/Time	The start time of the current sesion.
Outbound Link Events Left	
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Google Analytics Session Cookies Carved

Description	Google Analytics Session Cookies Carved contains information about Google Analytics session cookies that are recovered using carving.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the URL.
Page Views	The number of visits to this page from the user.
Start Current Session Date/Time	The start date and time of the current sesion.
Outbound Link Events Left	

Google Analytics URLs

Description	Google Analytics URLs contains URLs that are discovered in other artifacts that are related to Google Analytics.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the website. If the URL cannot be recovered, the source of the URL containing all the metadata is displayed instead.

ATTRIBUTE	DESCRIPTION
Page Title	The name of the website. This value is carved from the source starting after 'utmdt=' and ending at '&'.
Host Name	Contains the domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'.
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'.
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Google Analytics URLs Carved

Description	Google Analytics URLs Carved contains information about Google Analytics URLs that are recovered using carving.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the website. If the URL cannot be recovered, the source of the URL containing all of the metadata is displayed instead.
Page Title	The name of the website. This value is carved from the source starting after 'utmdt=' and ending at '&'.
Host Name	Contains the domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'.
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'.
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'.

Google Maps Directions

Description	Google Maps Directions contains information about directions queries requested by the user using Google Maps.
Notes	

ATTRIBUTE	DESCRIPTION
Origin Address	The address where the direction starts from. This value can be an address, a business description or latitude/longitude coordinates.
Origin Latitude	The latitude associated with the origin address.
Origin Longitude	The longitude associated with the origin address.
Destination Address	The destination address where the direction goes to. Several destinations can be added to a direction but only the last one is displayed.
Destination Latitude	The latitude associated with the destination address.
Destination Longitude	The longitude associated with the destination address.
Number of Stops	The number of stops (if any) between origin and destination addresses.
URL	The URL associated with the direction query. Directions can be viewed in a browser by appending the URL to the end of 'www.google.com/maps'.

Iron Browser Autofill

Description	Iron Browser Autofill contains records of the autofill values that Iron Browser saves for different types of text fields.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill was last used.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Iron Browser Bookmarks

Description	Iron Browser Bookmarks contains browser bookmarks that reference saved webpages.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time that the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Iron Browser Cookies

Description	Iron Browser Cookies contains cookies that Iron Browser downloads from the Internet. These cookies contain information about the websites that a user visits.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Iron Browser Downloads

Description	Iron Browser Downloads contains information about the files that a user downloads from the Internet.
Notes	

ATTRIBUTE	DESCRIPTION
Download Source	The URL of the file that was downloaded.
File Name	The name of the downloaded file.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time that the downloaded was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time that the downloaded finished.
Saved To	The absolute path on the device to the file downloaded.
State	The completion state of the download.

ATTRIBUTE	DESCRIPTION
Opened By User	Indicates whether the user has opened the downloaded file or not.
Bytes Downloaded	The bytes that were downloaded.
Total Bytes	The file size of the download.

Iron Browser Favicons

Description	Iron Browser Favicons contains the favicons that Iron Browser displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last time that the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Iron Browser Keyword Search Terms

Description	Iron Browser Keyword Search Terms contains information about the keyword search terms that a user enters.
Notes	

ATTRIBUTE	DESCRIPTION
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.

Iron Browser Logins

Description	Iron Browser Logins contains login information that a user provides in Iron Browser. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the login page.
Username	The username entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the data was created.

Iron Browser Tab History

Description	Iron Browser Tab History contains a history of websites that the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the tab file.
Tab ID	The unique ID of a tab entry in a tab file.
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request to open the webpage (for example, the referrer source might be from Google or another third-party application).
Originating URL	The URL of the webpage that led the user to the current URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Search Term	The value that the user entered into a search.

Iron Browser Top Sites

Description	Iron Browser Top Sites contains a list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the site was last updated.
Title	The title of the site.
Thumbnail	The thumbnail of the site.

Iron Browser Web History

Description	Iron Browser Web History contains a history of the websites that the user visits (includes unique visits only).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

Iron Browser Web Visits

Description	Iron Browser Web Visits contains a history of the websites that the user visits (includes all visits).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Kiwi Browser Autofill

Description	Kiwi Browser Autofill contains records of the autofill values that Kiwi Browser saves for different types of text fields.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time that the autofill was last used.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Kiwi Browser Bookmarks

Description	Kiwi Browser Bookmarks contains browser bookmarks that reference saved webpages.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Kiwi Browser Cookies

Description	Kiwi Browser Cookies contains cookies that Kiwi Browser downloads from the Internet. These cookies contain information about the websites that a user visits.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Kiwi Browser Downloads

Description	Kiwi Browser Downloads contains information about the files that a user downloads from the Internet.
Notes	

ATTRIBUTE	DESCRIPTION
Download Source	The URL of the file that was downloaded.
File Name	The name of the downloaded file.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the downloaded was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the downloaded finished.
Saved To	The absolute path on the device to the file downloaded.
State	The completion state of the download.
Opened By User	Indicates whether the user has opened the downloaded file or not.
Bytes Downloaded	The bytes that were downloaded.
Total Bytes	The file size of the download.

Kiwi Browser Favicons

Description	Kiwi Browser Favicons contains the favicons that the Kiwi Browser displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last time that the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Kiwi Browser Keyword Search Terms

Description	Kiwi Browser Keyword Search Terms contains information about the keyword search terms that a user enters.
Notes	

ATTRIBUTE	DESCRIPTION
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.

Kiwi Browser Tab History

Description	Kiwi Browser Tab History a history of websites the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the tab file.
Tab ID	The unique ID of a tab entry in a tab file.
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request to open the web page (for example, the referrer source might be from Google or another third-party application).
Originating URL	The URL of the webpage that led the user to the current URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Search Term	The value the user entered into a search.

Kiwi Browser Top Sites

Description	Kiwi Browser Top Sites contains a list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the site was last updated.
Title	The title of the site.
Thumbnail	The thumbnail of the site.

Kiwi Browser Web History

Description	Kiwi Browser Web History contains a history of the websites that the user visits (includes unique visits only).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times that the webpage was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).

Kiwi Browser Web Visits

Description	Kiwi Browser Web Visits contains a history of the websites that the user visits (includes all visits).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Lunascape Autofill

Description	Lunascape Autofill contains records of the autofill values that Lunascape saves for different types of text fields.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the autofill value.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill was last used.
Value	The saved autofill value for this type of field.
Count	The number of times that the autofill has been applied.

Lunascape Bookmarks

Description	Lunascape Bookmarks contains the webpages that a user has bookmarked.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Title	The name of the bookmark.

Lunascape Cookies

Description	Lunascape Cookies contains information about the cookies that the browser downloaded from the websites that the user has visited.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Lunascape History

Description	Lunascape History contains information about the websites that the user visits.

Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.

Malware/Phishing URLs

Description	Malware/Phishing URLs contains records that are believed to be either malware or phishing related URLs.
Notes	

ATTRIBUTE	DESCRIPTION
Site Name	The name of the website.
URL	The URL of the website.
Date/Time - UTC (yyyy-mm-dd)	The date and time this is associated with the artifact.
Artifact	The name of the artifact that the URL belongs to.
Artifact ID	The row ID of the URL in the original artifact table.

Naver Web History

Description	Naver Web History contains a record of all the websites a user has visited using the Naver browser. This artifact tracks the first instance and last instance that a user has visited a site.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the website that the user visited.
URL	The URL of the website that the user visited.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the user last visited the website.
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the user first visited the website.

Opera Autofill

Description	Opera Autofill contains records of the autofill values that Opera saves for different types of text fields.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time that the autofill was last used.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Opera Bookmarks

Description	Opera Bookmarks contains browser bookmarks that reference saved webpages.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time that the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Opera Cookies

Description	Opera Cookies contain cookies that Opera downloads from the Internet. These cookies contain information about the websites that a user visits.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.

ATTRIBUTE	DESCRIPTION
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie expires.
Path	The path of the cookie value.

Opera Downloads

Description	Opera Downloads includes information about the files that a user downloads from the Internet.
Notes	

ATTRIBUTE	DESCRIPTION
Download Source	The URL of the file that was downloaded.
File Name	The name of the downloaded file.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time that the downloaded was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time that the downloaded finished.
Saved To	The absolute path on the device to the file downloaded.
State	The completion state of the download.
Opened By User	Indicates whether the user has opened the downloaded file or not.
Bytes Downloaded	The bytes that were downloaded.
Total Bytes	The file size of the download.

Opera Favicons

Description	Opera Favicons contains the favicons that Opera displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last time that the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Opera Keyword Search Terms

Description	Opera Keyword Search Terms contains information about the keyword search terms that a user enters.
Notes	

ATTRIBUTE	DESCRIPTION
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.

Opera Top Sites

Description	Opera Top Sites contains a list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the site was last updated.
Title	The title of the site.
Thumbnail	The thumbnail of the site.

Opera Web History

Description	Opera Web History contains a history of the websites that the user visits (includes unique visits only).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times that the webpage was visited.

ATTRIBUTE	DESCRIPTION
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).

Opera Web Visits

Description	Opera Web Visits contains a history of the websites that the user visits (includes all visits).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Indicates how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is link.
Visit Source	The source of the visit.

Pornography URLs

Description	Pornography URLs contains records of what are believed to be pornography related URLs.
Notes	You can find a list of the domains that are supported by this refined result at Pornography URLs.

ATTRIBUTE	DESCRIPTION
Site Name	The name of the website.
URL	The URL of the website.
Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the artifact.
Artifact	The name of the artifact that the URL belongs to.
Artifact ID	The row ID of the URL in the original artifact table.

Potential Browser Activity

Description	The Browser Activity artifact will recover browser-related URLs. This includes Chrome Incognito and Firefox Private Browsing URLs, HTTP request artifacts from multiple browsers, and regular web browsing artifacts. This does not include metadata such as the Windows username, dates/-times, and so on. Note that some recovered URLs can be from background browser processes related to certificate authorities, etc.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL that the request was sent to.
User Agent	The string that represents the browser that sent the request.

Puffin Browser Bookmarks

Description	Contains bookmarks from the Puffin Browser for Android.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the bookmark.
URL	The URL of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was added.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the user last visited the web page.
Visits	The number of times the user visited this bookmark.

Puffin Browser History

Description	Contains the web history for the Puffin Browser for Android.
Notes	Last Accessed Date/Time - Local Time is always empty for Android Puffin Browser History

ATTRIBUTE	DESCRIPTION
Title	The title of the web page.
URL	The URL of the web page.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the user last visited the web page.
Last Accessed Date/Time - Local Time (yyyy-mm-dd)	The date and time the user last visited the web page.

ATTRIBUTE	DESCRIPTION
Visits	The number of times the user has visited that web page.

Rebuilt Webpages

Description	Rebuilt Webpages contains the data that allows for the reconstruction of webpages.
Notes	

ATTRIBUTE	DESCRIPTION
Page Title	The title.
URL	The URL.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the original record was created.
Domain	The domain.
Cache Table	The table that the data to re-construct the page came from.
Cache RowID	The row ID in the table that constructed the rebuilt webpage.

Reddit Accounts

Description	Reddit Accounts contains information about the user accounts that are used to log in to the Reddit application on the device.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The Reddit user ID.
Created Date/Time - UTC (yyyy-mm-dd)	The creation date and time of the Reddit account.

Reddit Posts

Description	Reddit Posts contains information about the posts recovered from the device. These posts might be ones the user has read or created on their device.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the Reddit post.

ATTRIBUTE	DESCRIPTION
Subreddit Name	The subreddit name where the post was posted.
Author	The author of the post.
Over 18	Indicates whether or not the post was flagged as mature content.
Content Link	The URL to content from the post if applicable, or the URL to the post if there is no external content.
URL	The URL of the post.
Saved	Indicates whether or not the post was saved by the user.
Read Date/Time - UTC (yyyy-mm-dd)	The date and time that the user read the post.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the post was created.

Reddit Recently Visited Subreddits

Description	Reddit Recently Visited Subreddits contains information about the subreddits that a user has recently visited while on their device.
Notes	

ATTRIBUTE	DESCRIPTION
Subreddit Name	The name of the subreddit.
Sort Order	The order in which posts were sorted within the subreddit (e.g. New, Hot, Top, Controversial).
Sort Time Frame	The time frame in which posts were sorted within the subreddit (e.g. Day, Week, Month, Year).
Description	The public facing description of the subreddit.
User Name	The user who visited the subreddit.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the user last visited the subreddit.
Created Date/Time - UTC (yyyy-mm-dd)	The creation date and time of the subreddit.

Samsung Browser Archived Keyword Search Terms

Description	Keyword search terms that were archived by the browser.
Notes	

ATTRIBUTE	DESCRIPTION
Keyword Search Term	The keyword search term the user entered.
URL	The URL of the keyword search.

Samsung Browser Archived Web History

Description	Samsung Browser Archived Web History contains an archived history of old webpage visits.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL where the archived web history is located.
Title	The title of the archived web history.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was visited.
Visit Count	Total visits to this URL.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
ID	The ID for the web history archive.

Samsung Browser Autofill

Description	Samsung Browser Autofill contains a collection of saved values that were used to fill in forms and fields.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the autofill value.
Value	The value.
Count	The count of the autofill.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.

Samsung Browser Autofill Profiles

Description	Samsung Browser Autofill Profiles contains the profiles that Samsung Browser uses to fill in forms with saved values.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name for the autofill profile.
Email	The email used in the the autofill profile.
Number	The phone number used in the autofill profile.
Company	The company name used in the autofill profile.
Address Line 1	The address Line 1 used in the autofill profile.
Address Line 2	The address Line 2 used in the autofill profile.
City	The city used in the autofill profile.
State	The state used in the autofill profile.
Zipcode	The Zip Code used in the autofill profile.
Country	The country used in the autofill profile.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the profile was last modified.

Samsung Browser Bookmarks

Description	Samsung Browser Bookmarks contains browser bookmarks that reference saved webpages.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the bookmark.
Name	The title of the bookmarked page.
Account Name	The user account that created the bookmark.
Device ID	The ID of the device the bookmark was created on.
Device Name	The name of the device the bookmark was created on.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time whne the bookmark was last modified.
Deleted	Whether the bookmark has been deleted.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark (URL or Folder).

Samsung Browser Cache Records

Description	Content that Samsung Browser downloads and caches to speed up rendering times. Cached content can include pictures, text, html, javascript, and more.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the cached item.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was first visited.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The date and time the cache was last synced with the cloud.
File Type	The type of file that was cached.
Content Size (Bytes)	The size of the cached file.
Image	The cached image if the file type is an image. Otherwise, this column is empty.
Content	The cached file contents if the file type is not an image. Otherwise, this column is empty.

Samsung Browser Cached Thumbnails

Description	Samsung Browser Cached Thumbnails contains thumbnail previews of the web pages that a user visits while using the browser.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the cached item.
Thumbnail	A partial screenshot of the web page which is used as a thumbnail.
Preview Image	A full screenshot of the cached web page.

Samsung Browser Cookies

Description	Samsung Browser Cookies contains cookies that Samsung Browser downloads from the Internet. These cookies contain information about the websites that a user visits.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.

ATTRIBUTE	DESCRIPTION
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Samsung Browser Current Session

Description	Information about the browser session that's currently underway.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL.
Title	The title of the web page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Samsung Browser Current Tabs

Description	Information about the tabs that are open in the current browser session.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL.
Title	The title of the web page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.

Samsung Browser Downloads

Description	Information about the files that a user downloads from the Internet.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the download.
Download Source	The URL of the file that was downloaded.
Saved To	The location that the download was saved to.
State	The state of the download.
Opened By User	Whether the download is opened by the user.
Start Time Date/Time - UTC (yyyy-mm-dd)	The download start time.
End Time Date/Time - UTC (yyyy-mm-dd)	The download end time.
Bytes Downloaded	The bytes that were downloaded.
File Size(Bytes)	File size of the download.

Samsung Browser FavIcons

Description	Contains the favicons that Samsung Browser displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	Page URL of the favicon.
Icon URL	Icon URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	Last time the favicon was updated.
Icon	A preview of the favicon.

Samsung Browser History Index

Description	An index of the webpages the user has visited in the past.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	The URL of the webpage.
Title	The title of the webpage.
Visited On Date/Time - UTC (yyyy-mm-dd)	When the webpage was visited.
Body	A snippet of the webpage.

Samsung Browser Keyword Search Terms

Description	Information about the keyword search terms that a user enters.
Notes	

ATTRIBUTE	DESCRIPTION
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.

Samsung Browser Last Session

Description	Information about the previous browser session.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL.
Title	The title of the web page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Samsung Browser Last Tabs

Description	Information about the tabs that were open during the previous session.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The web page URL.
Title	The title of the web page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Samsung Browser Logins

Description	Login information that a user provides in Samsung Browser. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the login page.
Username	The username entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the data was created.

Samsung Browser Media History

Description	Samsung Browser Media History contains information about the media files (audio and video) that the user views in the browser.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	The URL of the page that contains the media file.
Video URL	The URL of the media file.
Title	The media title.
Thumbnail	The media thumbnail.
Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the user visited the page containing the media file.
Played (Seconds)	The duration of the media file that has been played, in seconds.
Duration (Seconds)	The full duration of the media file, in seconds.

Samsung Browser Saved Credit Cards

Description	Samsung Browser Saved Credit Cards contains information about the credit cards that a user has saved to their device.
Notes	

ATTRIBUTE	DESCRIPTION
Name On Card	The name of the person on the credit card.

ATTRIBUTE	DESCRIPTION
Card Number	The number on the credit card.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the information was last modified.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time the credit card autofill information was last used.
GUID	An ID for the credit card.
Expiry Date	The date the credit card is supposed to expire in format 'month-year'.

Samsung Browser Saved Pages

Description	Samsung Browser Saved Pages contains information about web pages that were saved for off-line viewing by the user. This includes basic page data, preview icon, user and device info. In addition, an .mhtml backup of the page is recovered, if it wasn't deleted.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the saved webpage.
Title	The title of the saved webpage.
Description	The brief description of the saved webpage.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the page was saved.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when saved page was last modified.
Icon	The preview icon for the saved page.
Deleted	Indicates whether saved page backup was deleted.
Account Name	The email account of the user that saved the page.
Device ID	The device ID.
Device Name	The device name.
Page Saved	The HTML content of the saved page. Uses .mhtml format instead of .html, which can affect display in various browsers.

Samsung Browser Shortcuts

Description	Contains all of the shortcuts used by Google Samsung Browser for user entered URLs.
Notes	

ATTRIBUTE	DESCRIPTION
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.
Last Access Date/Time - UTC (yyyy-mm-dd)	The last access time of the shortcut.
Web Page Title	The title of the web page.
Times Used	The number of times the shortcut has been used.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Type	The type of shortcut (for example, 'typed url' or 'bookmark').

Samsung Browser Tab History

Description	A history of websites the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the tab file.
Tab ID	The unique ID of a tab entry in a tab file.
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request to open the web page (for example, the referrer source might be from Google or another third-party application).
Originating URL	The URL of the webpage that led the user to the current URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Search Term	The value the user entered into a search.

Samsung Browser Tabs

Description	Samsung Browser Tabs contains information about the tabs that the user has opened in the browser (not including private browsing). This artifact can also recover tabs that were opened but deleted.
Notes	

ATTRIBUTE	DESCRIPTION
Tab ID	The ID of the tab. This value can be used to identify specific tab files.
Tab URL	The URL of the website open in the tab.
Tab Title	The title of the website that's open in the tab.
Deleted	Indicates whether the tab has been deleted in the browser.
Account Name	The email account of the user that opened the tab.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the tab was last modified.
Synced Date/Time - UTC (yyyy-mm-dd)	Indicates the date and time that the tab was last synced, if the browser on the local device is synced with another device.
Device Name	The device name.
Device ID	The device ID.

Samsung Browser Top Sites

Description	A list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Notes	

ATTRIBUTE	DESCRIPTION
URL	URL of the site.
Title	Title of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the site was last updated.
Thumbnail	Thumbnail of the site

Samsung Browser Web History

Description	A history of the websites that the user visits (includes unique visits only).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited.

ATTRIBUTE	DESCRIPTION
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

Samsung Browser Web Visits

Description	A history of the websites that the user visits (includes all visits).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited webpage.
Title	The title of the webpage that was visited.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Sleipnir Autofill

Description	Sleipnir Autofill contains records of the autofill values that Sleipnir saves for different types of text fields.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the autofill value.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill was last used.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Sleipnir Bookmarks

Description	Sleipnir Bookmarks contains the webpages that a user has bookmarked.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time that the bookmark was added.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the bookmark was last updated.
Name	The name of the bookmark.
Type	The type of bookmark.
Parent Folder	The name of the parent folder of the bookmark.

Sleipnir Cookies

Description	Sleipnir Cookies contains information about the cookies that the browser downloaded from the websites that were visted by the user.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie expires.
Path	The path of the cookie value.

Sleipnir Search Terms

Description	Sleipnir Search Terms contains information about the keyword search terms that a user has provided in the browser.
Notes	

ATTRIBUTE	DESCRIPTION
Search Term	The search term that the user entered.
URL	The URL of the keyword search.
Search Date/Time - UTC (yyyy-mm-dd)	The date and time when the keyword search took place.
Count	The number of times that the search occured.

Sleipnir Web History

Description	Sleipnir Web History contains information about the websites that the user visited.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times that the webpage was visited.

UC Browser Bookmarks

Description	UC Browser Bookmarks contains the webpages that a user has bookmarked.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Title	The title of the bookmark.
Is Folder	Indicates if the bookmark entry is a folder.

UC Browser Cookies

Description	UC Browser Cookies contains information about the cookies that the browser downloaded from the website that the user has visited.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

UC Browser Downloads

Description	UC Browser Downloads contains information about the files that a user downloads from the Internet.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the downloaded file.
Saved To	The absolute path on the device to the file downloaded.
Download URL	The URL of the file that was downloaded.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time when the downloaded finished.
File Size (Bytes)	The file size of the download.

UC Browser History

Description	UC Browser History contains information about the websites that the user visits.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited page.

WebKit Browser Session/Tabs (Carved)

Description	WebKit Browser Sessions/Tabs contains information about the browser sessions and tabs that the user has open, while using a browser built with WebKit. Some examples of browsers that use WebKit are Chrome, Opera, and 360 Safe Browser. This artifact consolidates the existing Chrome, Safe Browser, and Opera equivalents in a single artifact. Usage of other browsers, such as Firefox and Safari, aren't likely to appear under this artifact.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the webpage.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last visited.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

WebKit Browser Web History (Carved)

Description	WebKit Browser Web History contains information about the websites that a user visits while using a browser built with WebKit. Some examples of browsers that use WebKit are Chrome, Opera, and 360 Safe Browser. This artifact consolidates the existing Chrome, Safe Browser, and Opera equivalents in a single artifact. Usage of other browsers aren't likely to appear under this artifact, however, some URLs found by other browsers may also be found by this artifact.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited
Visit Count	The number of times that the webpage was visited.
Typed Count	The number of times that the webpage was accessed by the user typing the URL (as opposed to clicking a link).

Whale Autofill

Description	Whale Autofill contains records of the autofill values that Whale saves for different types of text fields.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill was last used.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Whale Bookmarks

Description	Whale Bookmarks contans browser bookmarks that reference saved webpages.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Whale Cookies

Description	Whale Cookies contains cookies that Whale downloads from the Internet. These cookies contain information about the websites that a user visits.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.

ATTRIBUTE	DESCRIPTION
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Whale Downloads

Description	Whale Downloads contains information about the files that a user downloads from the Internet.
Notes	

ATTRIBUTE	DESCRIPTION
Download Source	The URL of the file that was downloaded.
File Name	The name of the downloaded file.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was finished.
Saved To	The absolute path on the device to the downloaded file.
State	The completion state of the download.
Opened By User	Indicates whether the user has opened the downloaded file or not.
Bytes Downloaded	The bytes that were downloaded.
Total Bytes	The file size of the download.

Whale Favicons

Description	Whale Favicons contains the favicons that Whale displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last time that the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Whale Keyword Search Terms

Description	Whale Keyword Search Terms contains information about the keyword search terms that a user enters.
Notes	

ATTRIBUTE	DESCRIPTION
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.

Whale Logins

Description	Whale Logins contains login information that a user provides in Whale. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the login page.
Username	The username entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the data was created.

Whale Tab History

Description	Whale Tab History contains a history of websites that the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the tab file.
Tab ID	The unique ID of a tab entry in a tab file.
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request to open the webpage (for example, the referrer source might be from Google or another third-party application).

ATTRIBUTE	DESCRIPTION
Originating URL	The URL of the webpage that led the user to the current URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Search Term	The value that the user entered into a search.

Whale Top Sites

Description	Whale Top Sites contains a list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the site was last updated.
Title	The title of the site.
Thumbnail	The thumbnail of the site.

Whale Web History

Description	Whale Web History contains a history of the websites that the user visits (includes unique visits only).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times that the webpage was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).

Whale Web Visits

Description	Whale Web Visits contains a history of the websites that the user visits (includes all visits).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Yandex Autofill

Description	Yandex Autofill contains records of the autofill values that Yandex saves for different types of text fields.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when autofill was last used.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Yandex Bookmarks

Description	Yandex Bookmarks contains browser bookmarks that reference saved webpages.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time whne the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Yandex Cookies

Description	Yandex Cookies contains the cookies that Yandex downloads from the Internet. These cookies contain information about the websites that a user visits.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Yandex Downloads

Description	Yandex Downloads contains information about the files that a user downloads from the Internet.
Notes	

ATTRIBUTE	DESCRIPTION
Download Source	The URL of the file that was downloaded.
File Name	The name of the downloaded file.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download finished.
Saved To	The absolute path on the device to the downloaded file.
State	The completion state of the download.
Opened By User	Indicates whether the user opened the downloaded file or not.

ATTRIBUTE	DESCRIPTION
Bytes Downloaded	The bytes that were downloaded.
Total Bytes	The file size of the download.

Yandex Favicons

Description	Yandex Favicons contains the favicons that Yandex displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last date and time when the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Yandex Keyword Search Terms

Description	Yandex Keyword Search Terms contains information about the keyword search terms that a user enters.
Notes	

ATTRIBUTE	DESCRIPTION
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.

Yandex Logins

Description	Yandex Logins contains login information that a user provides in Yandex. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the login page.

ATTRIBUTE	DESCRIPTION
Username	The username entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the data was created.

Yandex Shortcuts

Description	Yandex Shortcuts contains all of the shortcuts used by Yandex for user entered URLs.
Notes	

ATTRIBUTE	DESCRIPTION
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.
Last Access Date/Time - UTC (yyyy-mm-dd)	The last access time of the shortcut.
Web Page Title	The title of the webpage.
Times Used	The number of times that the shortcut was used.
Transition Type	Describes how the browser navigated to the URL of the shortcut. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Type	The type of shortcut (for example, 'typed url' or 'bookmark').

Yandex Sync Data

Description	Yandex Sync Data contains information about the data that Yandex has synced to a user's account in the cloud.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the sync key.
Local Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the value on the local system.
Server Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the value on the server.
Local Created Date/Time - UTC (yyyy-mm-dd)	The created time of the value on the local system.

ATTRIBUTE	DESCRIPTION
Server Created Date/Time - UTC (yyyy-mm-dd)	The created time of the value on the server.
Type	The type of data that is synced (bookmark, favicon, type URL, and more).
Parsed Content	The type of parsed data.
Favicon Image	The actual favicon image.

Yandex Top Sites

Description	Yandex Top Sites contains a list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the site was last updated.
Title	The title of the site.
Thumbnail	The thumbnail of the site.

Yandex Web History

Description	Yandex Web History a history of the websites that the user visits (includes unique visits only).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times that the webpage was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).

Yandex Web Visits

Description	Yandex Web Visits contains a history of the websites that the user visits (includes all visits).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

IOS

Advanced Search Tools

Dynamic Application Finder

Description	
Notes	

ATTRIBUTE	DESCRIPTION

Chat

AIM Buddies

Description	Information about the local user's buddies in the iOS AIM app.
Notes	

ATTRIBUTE	DESCRIPTION
User AIM ID	The AIM ID of the local user.
Buddy Name	The name of the buddy.
Buddy Display ID	The display ID of the buddy.
Buddy AIM ID	The AIM ID of the buddy.
Buddy Icon URL	The URL of the buddy's icon.
Buddy Group	Identifies if the row is a buddy or group chat. The possible values are 'Buddies' or 'groupcht'.
Group Chat ID	The ID of the group chat, if applicable.

AIM Messages

Description	Messages sent and received from the iOS AIM app.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	Email address of the sender of the message.
Receiver	Email address of the receiver of the message.
Message Date/Time - UTC (yyyy-mm-dd)	Date/Time associated with the message.
Message	Message content, in HTML or plaintext format.
Latitude	Latitude of the location from which the message was sent.
Longitude	Longitude of the location from which the message was sent.

BlackBerry Messenger Contacts

Description	Contains the BBM Contacts recovered from an iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Display Name	Contains the contacts display name.
BlackBerry PIN	Contains the contacts BlackBerry PIN.
Personal Message	Contains the contacts personal message.
Personal Message Last Update Date/Time - UTC (yyyy-mm-dd)	The data and time the contacts personal message was updated.
Avatar	The contacts avatar.
Avatar Content Type	The avatar content type. An example is 'image/jpeg'
Location	The contacts location.
Timezone	The contacts timezone.

BlackBerry Messenger File Transfers

Description	Contains the BBM File Transfers recovered from an iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Transfer Direction	Indicates whether a file was sent or received.
Transfer State	Indicates whether a file transfer is 'Pending Approval' or 'Complete'.
Display Name	Display name of the contact who the transfer is with.
BlackBerry PIN	BlackBerry PIN of the contact who the transfer is with.
Local File Path	The path on the device to the data transferred.

ATTRIBUTE	DESCRIPTION
Content Type	The type of data that was transferred.
Transfer Description	Description of what is being transferred.
Attachment	The file that was transferred.
Total Transfer Size (Bytes)	The number of bytes the transferred file is.
Bytes Transferred	The number of bytes that were transferred.
Transfer Date/Time - UTC (yyyy-mm-dd)	The date and time the transfer took place.

BlackBerry Messenger Invitations

Description	Contains the BBM invite requests recovered from an iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Direction	This column states if the invite is a received invite or a sent invite.
Display Name	The display name of the user sending the invite request.
BlackBerry PIN	The BlackBerry PIN of the user sending the invite request.
Remote Email Address	
Local Email Address	
Invitation Status	Contains the status of the invite request. The value can be 'Pending Approval' or unknown.
Invite Method	Contains the method used for sending the invite request. The value can be 'Via PIN' or unknown.
Subject	The subject used for the invite request.
Greeting	The message sent along with the invite request.
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The data and time the invite was sent/received.

BlackBerry Messenger Locations

Description	Contains the BBM locations recovered from an iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Message Type	Contains if a location was sent or received.
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date and time the location was sent/received.

ATTRIBUTE	DESCRIPTION
Display Name	The display name of the location sender.
BlackBerry PIN	The BlackBerry PIN of the location sender.
Location Name	The name of the location
Latitude	The latitude of the location
Longitude	The longitude of the location
Altitude (meters)	
Accuracy (meters)	
Street	The street address of the location.
City	The city of the location.
State/Province	The state/province of the location.
Country	The country of the location.
ZIP/Postal Code	The postal code/zip of the location.

BlackBerry Messenger Messages

Description	Contains the BBM messages recovered from an iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Message Type	Contains the type of message that was sent. This can be one of the following: Message, Ping, File, Picture, Notification, Location.
Message Status	The status of the message (received or sent).
Message State	Contains the state of the message. This can be one of the following: 'Sent', 'Undelivered', 'Delivered, Unread', 'Read'.
Display Name	The display name of who sent the message to the device or who's receiving a message from the device.
BlackBerry PIN	The BlackBerry PIN of who sent the message to the device or who's receiving a message from the device.
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent/received.
Message Content	The message sent/received.
Conversation ID	The conversation identifier.
Participants	The display names of the people in the conversation.
Attachment	The attachment that was sent/received.

BlackBerry Messenger Profile

Description	Contains the BBM Profiles recovered from an iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Display Name	The display name associated with the profile.
BlackBerry PIN	The BlackBerry PIN associated with the profile.
Personal Message	The profiles personal message.
Personal Message Last Update Date/Time - UTC (yyyy-mm-dd)	The date and time the profile message was last updated.
Avatar	The profiles avatar.
Avatar Content Type	The avatar content type. An example is 'image/jpeg'.
Location	The location of the profile.
Timezone	The timezone of the profile.
Keeps Chat History	Indicates whether or not the user keeps chat history.

Burner Contacts

Description	Burner Contacts contains information about a subject's Burner Contacts, as recovered from their iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Contact ID	The id of the contact.
Contact Name	The name of the contact.
Phone Number	The phone number of the contact.
Burner ID	The ID of the Burner app associated with the contact.
Created Date/Time - UTC (yyyy-mm-dd)	Indicates When the contact was created.

Burner Messages

Description	Burner Messages contains information about messages and calls that are sent and received using Burner.

Notes	

ATTRIBUTE	DESCRIPTION
Sender	The phone number of the sender.
Recipient	The phone number of the recipient.
Message	The body of the message.
Message Type	The type of message.
Media URL	The URL to the media file attached to the message
Voicemail URL	The URL of the voicemail.

Burner Numbers

Description	Burner Numbers contains information about the burner numbers that the local user created.
Notes	

ATTRIBUTE	DESCRIPTION
Burner ID	The ID of the Burner number.
Burner Number	The Burner phone number.
Display Name	The display name associated with the Burner number.
Created Date/Time	Indicates when the Burner number was created.
Expiration Date/Time	Indicates when the number will expire.
Mobile Number	The phone number used to sign in to the Burner App.
User ID	The user id of the signed in user.

Chatous Chat Messages

Description	Messages sent and received using Chatous.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	Display name of the user who sent the message (Local User if it was the local user).
Recipient	Display name of the user who received the message (Local User if it was the local user).
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.

ATTRIBUTE	DESCRIPTION
Message	The body of the message.
Attachment Name	The name of the attachment that was sent.
Attachment Data Recovered	Indicates whether attachment data was recovered (Yes or No).

Chatous Chat Partners

Description	Chatous Chat Partners contains information about the users that the local user has communicated with.
Notes	

ATTRIBUTE	DESCRIPTION
Screen Name	The name of the chat partner.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the last message in the chat.
Age	The age of the chat partner.
Gender	The gender of the chat partner. A blank value indicates that the chat partner is the Team Chatous account.
Location	The location of the chat partner.
About	A summary of the chat partner.
Tag	The tag that matched the local user and the chat partner for a chat.
Profile Tags	The hashtags that the chat partner uses to describe themselves.

Discord Messages

Description	Discord Messages contains information about messages and calls that are sent and received using Discord. Messages from some channels might be missing if they haven't been cached by the app. This artifact uses both parsing and carving techniques to recover messages.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The user name of the message sender.
Message	The message content.
Channel ID	The ID of the channel that the message was sent in.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.

ATTRIBUTE	DESCRIPTION
Last Edited Date/Time - UTC (yyyy-mm-dd)	If the message has been edited then this indicates the date and time when the last edit has occurred.
Attachment URL	If the message includes an attachment then this indicates the saved URL of the attachment.
Attachment Name	If the message includes an attachment then this indicates the file name of the attachment.
Embedded Content Title	If the message contains a link then this then this indicates the title that's displayed in the link preview.
Embedded Content Description	If the message contains a link then this indicates the description that's displayed in the link preview.
Message Type	The type of the message, either a Message or a Call.
Call End Date/Time - UTC (yyyy-mm-dd)	If the message was a call, this indicates the date and time that the call ended.
Pinned	Indicates whether a message is pinned (True or False).

Facebook Messenger Calls

Description	Contains call data recovered from Facebook Messenger.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The name of the application that generated the data (Facebook Messenger or Facebook Messenger Kids).
User Key	User key of the call partner.
Thread Key	Thread key of the group where call was made.
Date/Time - UTC (yyyy-mm-dd)	Date and time of the call.
Call Duration (Seconds)	Duration of the call in seconds. Empty if call wasn't answered.
Call Type	Type of the call. Can be voice call or group voice call.
Answered	Whether the call was answered or not.
Direction	Direction of the call.

Facebook Messenger Groups

Description	Contains data about group chats on Facebook Messenger.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The name of the application that generated the data (Facebook Messenger or Facebook Messenger Kids).
Thread Key	Thread key of the group.
Group Name	Display name of the group.
Participants	The IDs of the users that are a part of the group.
Participants User Names	The user names associated with the participants of the group.
Sender(s)	The IDs of the users that recently participated in the group (for example, by sending a message).
Senders User Names	The user names associated with the respective senders in the group.
Last Activity Date/Time - UTC (yyyy-mm-dd)	Date and time of the last activity recorded in the group.
Message Count	Approximate number of messages in the group.

Facebook Messenger Messages

Description	Contains messages recovered from Facebook Messenger.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The name of the application that generated the data (Facebook Messenger or Facebook Messenger Kids).
Sender Name	Display name of the person sending the message.
Receiver Name	Display name of the person receiving the message.
Date/Time - UTC (yyyy-mm-dd)	Date and time when message was sent.
Deleted Date/Time - UTC (yyyy-mm-dd)	The date and time the message was deleted from the app.
Text	Text of the message. (If the message type is 'call' it will display an auto generated text with call details)
Thread ID	Thread ID of the message. This is also the Facebook ID of the remote party.
Message Type	Type of message that was sent (for example, call, sticker, etc.)
Media Info	Information about the media that is found. This value can be a URL to the media, a file name, or a sticker id.
Send State	Represents whether the message was queued. Always empty for Android.
Message ID	Internal unique message ID.
Receiver ID	User ID of the person receiving the message.
Sender ID	User ID of the person sending the message.

ATTRIBUTE	DESCRIPTION
Message Source	Source of the message creation platform.
Latitude	The latitude portion of the location data that is sent with the message.
Longitude	The longitude portion of the location data that is sent with the message.

Facebook Messenger Users Contacted

Description	Contains information about users contacted from the device using Facebook Messenger.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The name of the application that generated the data (Facebook Messenger or Facebook Messenger Kids).
User Key	User key of the user.
First Name	First name of the user.
Last Name	Last name of the user.
Name	Display name of the user.
Username	Unique identifier of the user.
Profile Picture URL	URL of the user's profile picture.
Is App User	Identifies whether the user is using Facebook Messenger or not.
Is Friend	Identifies whenever the user is a friend of the local user.
Rank	User's rank within the app.

Glide Messages

Description	Glide Messages contains messages sent and received by the local user.
Notes	

ATTRIBUTE	DESCRIPTION
Sender ID	The unique user ID of the sender.
Sender Name	The name of the sender.
Recipient ID (s)	The Glide identifier(s) of recipient(s)
Recipient Name(s)	The name(s) of the recipient(s).

ATTRIBUTE	DESCRIPTION
Message	The body of the message. Forwarded messages have had a Fwd: prefix added to help differentiate them from the original message.
Message Type	The type of the message.
Created Date/Time	The date and time when the message was created.
Read	The read status of the message.
Media URL	The URL to the media of the message.
Chat Type	The type of the chat.

Glide Users

Description	Information about the various users that the suspect has encountered using Glide.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	Unique ID of the user.
First Name	The first name of the user.
Last Name	The last name of the user.
Email Address	The email address of the user.
Gender	The gender of the user.
Account Type	The type of the user.
Last Seen Date/Time	The last time the user was seen online.

Google Duo Calls

Description	Google Duo Calls contains details about audio and video calls made by the user.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local user of the device where the data was recovered from.
Remote Username	The username of the remote participant of the call.
Remote User ID	The user ID or phone number of the remote participant of the call.
Direction	Whether the call is outgoing or incoming.
Call Date/Time - UTC (yyyy-mm-dd)	The date and time the user started the call.

ATTRIBUTE	DESCRIPTION
Call Status	The status of the call.
Call Duration (seconds)	The duration of the call.
Call Type	Whether the call is an audio or video call.

Google Duo Group Calls

Description	Google Duo Group Calls contains details about the video calls made and received by the user.
Notes	

ATTRIBUTE	DESCRIPTION
Session ID	The session ID of the group call.
Call Status	The status of the call. 'Incoming Initiated' indicates an incoming call request, 'Incoming Cancelled' indicates that the caller cancelled the request before connecting, and 'Call' indicates an incoming call that was connected or an outgoing call that is unknown if any participants joined the call.
Caller	The phone number of the caller.
Recipient(s)	The recipients of the call.
Call Date/Time - UTC (yyyy-mm-dd)	The date and time of the call.
Call Duration (Seconds)	The duration of the call.
Call Type	The type of call.

Google Duo Groups

Description	Google Duo Groups contains membership information of Google Duo Groups.
Notes	

ATTRIBUTE	DESCRIPTION
Group Chat ID	The ID of the group.
Group Name	The display name of the group.
Group Member Name(s)	The display names of the group members.
Group Member ID(s)	The IDs of the group members.

Google Duo Messages

Description	Google Duo Messages contains details about audio, video, photo, and note messages sent and received by the user.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the message.
Recipient(s)	The recipient(s) of the message.
Direction	Indicates whether the message is outgoing or incoming.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent or received.
Attachment Name	The name of the message attachment.
Attachment	The attachment that was sent or received.

Google Hangouts Voice Calls

Description	Google Hangouts Voice Calls contains a history of voice calls between the local user and other users.
Notes	

ATTRIBUTE	DESCRIPTION
Phone Number	The phone number of the call participant.
Call Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the call started.

Grindr Buddies

Description	Contains the buddies and their details within the current users extracted iOS data.
Notes	

ATTRIBUTE	DESCRIPTION
Public ID	The id of the user in the buddy list.
Description	The description of the buddy.
Display Name	The buddies display name.
Age	The age of the buddy.
Height (cm)	The height of the buddy.

ATTRIBUTE	DESCRIPTION
Weight (kg)	The weight of the buddy.
Ethnicity	The ethnicity of the buddy.
Distance	The distance how far the buddy is from the current user.
Favorited	States whether or not this buddy is a favorite buddy for the current user.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the last received message from this buddy.

Grindr Messages

Description	Contains the messages and their details within the current users extracted iOS data.
Notes	

ATTRIBUTE	DESCRIPTION
Sender ID	The ID of the sender of the message.
Receiver ID	The ID of the receiver of the message.
Conversation Partner	The buddy's display name the message was with.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time the message was received.
Message Body	The body of the message.
Read Status	The status of the message (read, unread, received, displayed or acknowledged).
Message Direction	If the was incoming to the device, or outgoing from the device.

GroupMe Accounts

Description	GroupMe Accounts contains information about the accounts that the local user has logged in with on the device.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user ID of the local user.
Display Name	The display name of the local user.
Email Address	The email address of the local user.
Phone Number	The phone number of the local user.
Created Date/Time	The date and time the account was created (specific to iOS).

ATTRIBUTE	DESCRIPTION
Login Date/Time	The date and time the account was logged in on this device (specific to Android).
Profile Picture URL	The URL of the profile picture of the local user.
Password/Token	The local user password/token.

GroupMe Contacts

Description	GroupMe Contacts contains information about a user's contacts.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user id of the contact.
Display Name	The display name of the contact.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time the contact was added.

GroupMe Groups

Description	GroupMe Groups contains information about the groups that the logged-in user is a member of.
Notes	

ATTRIBUTE	DESCRIPTION
Group	The group number.
Group Name	The name of the group.
Topic	The topic of the group.
Creator ID	The creator identifier of the group.
Created Date/Time	The date and time the group was created
Group Member ID(s)	IDs of all group participants.
Group Member Name(s)	Names of all group participants.

GroupMe Messages

Description	Messages sent and received using GroupMe.
Notes	

ATTRIBUTE	DESCRIPTION
Sender Name	The name of the message sender.
Sender ID	The user ID of the message sender.
Recipient Name(s)	The user name(s) of the message recipient(s).
Recipient ID(s)	The user ID(s) of the message recipient(s).
Sent Date/Time	The date and time the message was sent.
Message	The message text.
Photo URL	The URL to the photo associated with the message.
Video URL	The URL to the video associated with the message.
Location	The name of the location in the location data sent with the message.
Latitude	The latitude part of location data sent with the message.
Longitude	The longitude part of location data sent with the message.
Event	The event sent with the message.
Document Title	The document details sent with the message.
Poll	The poll details sent with the message.

GROWLr Chat Messages

Description	Messages stored by the iOS GROWLr app.
Notes	

ATTRIBUTE	DESCRIPTION
Account ID	The ID of the other person the message is with.
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent or received.
Message	The body of the message.
Message Type	If the message was incoming or outgoing.
Message Status	The status of the message (read or unread).
Image Filename	The path to the image of associated with the message.
Image	The attached image.
Voice Filename	The filename of the attached voice message.
Voice	The attached voice data.

GROWLr Notes

Description	Notes stored by the iOS GROWLr app.
Notes	

ATTRIBUTE	DESCRIPTION
Text	The note text.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the note was last modified.

iOS Burner Conversations

Description	Contains the Burner conversations that were recovered from an iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Message Body	The body of the last message in the conversation
Message Date/Time - UTC (yyyy-mm-dd)	The date/time of the last message in the conversation.
Burner Number	The Burner number on the device that is a part of the conversation.
Conversation Partner	Phone number of the other person in the conversation.
Conversation Name	The name of the conversation.
Duration (Seconds)	The duration of the conversation, in seconds
Status	The status of the message. Can be 'read', 'unread', 'Sent', 'Not Sent'
Type	The type of the last interaction in the conversation. Can be any of the following 'Outgoing Text Message', 'Incoming Text Message', 'Incoming Phone Call', 'Missed Incoming Phone Call', 'Outgoing Phone Call', 'Incoming Voice Mail'.
Voicemail URI	The URL to the voice mail, if applicable.

iOS Burner Numbers

Description	Contains the Burner numbers that were recovered from an iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Account Number	The phone number of the user's Burner account.
Burner Number	The phone number that was generated by Burner.

ATTRIBUTE	DESCRIPTION
Updated Date/Time - UTC (yyyy-mm-dd)	The last time the Burner number was updated.
Created Date/Time - UTC (yyyy-mm-dd)	When the Burner number was generated.
Expiration Date/Time - UTC (yyyy-mm-dd)	When the Burner number will expire.
About	Information about the Burner number.

iOS Google Hangouts Cached Images

Description	Contains the cached images from Google Hangouts from an iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Image URL	The URL of the cached image.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last Date/Time the image was accessed.
Local File Path	The location to the image on the user's device.
File Size (Bytes)	The size of the image in bytes.
Image	The cached image.

iOS Google Hangouts Contacts

Description	Contains the contacts of a person from Google Hangouts from an iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Display Name	The display name of the contact.
Google Hangouts ID	The ID of the user in Google Hangouts.
Avatar URL Suffix	The suffix of the user's avatar URL.
Is Blocked	Is the person blocked
Is Favorite	Is the person favourited.

iOS Google Hangouts Messages

Description	Contains the messages from Google Hangouts from an iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Event	The event that is the message. Can be 'Message', 'User Joined Group Conversation', 'User Left Group Conversation', 'Video Call Started', 'Video Call Ended', 'User Toggled History'.
Message	The body of the message.
Sender / Event Initiator	The sender/event initiator of the message.
Recipient(s)	The recipients of the message.
Event Date/Time - UTC (yyyy-mm-dd)	The Date/Time of the message/event.
Event Expiry Date/Time - UTC (yyyy-mm-dd)	The Date/Time the message/event expires.
Conversation Is Deleted	Is the conversation deleted.
Image URL	The URL to the image of the conversation.
Location	The location of the message.
Address	The address of the message.
Latitude	The latitude of the message.
Longitude	The longitude of the message.

iOS Kik Messenger Attachments

Description	Contains the attachments of messages from Kik Messenger from an iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Attachment Date/Time - UTC (yyyy-mm-dd)	The Date/Time of the message.
Attachment	The attachment.
Attachment (Plain Text)	The attachment, if its format is plain text (for example, a URL).

iOS Kik Messenger Messages

Description	Kik Messenger messages sent or received by the local user.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local user of the device where the data was recovered from.
Partner	The person the local user sent a message to or received a message from.
Partner Display Name	The partner's display name.
Message Body	The body of the message.
Message Type	The type of message. Possible values are 'Message Received', 'Message Sent', 'User Joined' and 'Unknown Message Type'.
Received (Device Time) Date/Time - UTC (yyyy-mm-dd)	When the message was received.
Sent (Device Time) Date/Time - UTC (yyyy-mm-dd)	When the message was sent from the device.
Sent (Server Time) Date/Time - UTC (yyyy-mm-dd)	When the message was sent from the server.
Anonymous Chat	Indicates whether message was part of an anonymous chat.
Anonymous Chat Expiry Date/Time - UTC (yyyy-mm-dd)	If the message was part of an anonymous chat, this indicates whether the anonymous chat has expired.
Attachment	The attachment sent with the message.

iOS Kik Messenger Users

Description	Information about a user's Kik Messenger contacts.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The identifier of the user.
Chat User ID	The chat user identifier of the user.
Username	The user name of the user.
First Name	The first name of the user.
Last Name	The last name of the user.
Display Name	The display name of the user.
Kik ID	The Kik identifier of the user.
Email	The email address of the user.
Image URL	The URL to the profile picture of the user.
Last Message	The last sent message of the user.
Last Sent Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp of the last sent message.

iOS Telegram Channel Chats

Description	Information about the channel chats that the suspect participates in using the Telegram app.
Notes	

ATTRIBUTE	DESCRIPTION
Chat ID	The ID number for the channel chat.
Title	The title of the channel chat.
Channel Type	The type of channel this chat happened in (persistent or temporary.)
Last Sender	The full name of the user that sent the last message in the chat.
Last Sender Id	The user ID of the user that sent the last message in the chat.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the last message in the chat.
Last Message	The last message that was sent in the channel chat.
Read Only (Yes/No)	Whether this channel chat is read only to the local user.
Flags	Status flags associated with the chat.
Attachment Name(s)	The names of any attachments included with the message.

iOS Telegram Chats

Description	Information about the chats that the suspect participates in using the Telegram app.
Notes	

ATTRIBUTE	DESCRIPTION
Chat ID	The ID number for the chat.
Title	The title of the chat.
Last Sender	The full name of the user that sent the last message in the chat.
Last Sender Id	The user ID of the user that sent the last message in the chat.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the last message in the chat.
Last Message	The last message that was sent in the channel chat.
Flags	Status flags associated with the chat.
Number of Participants	The number of people who have actively participated in the chat.
Participant Information	A list of users who have participated in the chat. This data consists of the full name and user ID of each participant.

iOS Telegram Messages

Description	Individual chat messages that are sent and received using the Telegram app.
Notes	

ATTRIBUTE	DESCRIPTION
Sender Name	The full name of the person who sent the message.
Sender ID	The user ID of the person who sent the message.
Recipient Name	The full name of the person who received the message.
Recipient ID	The user ID of the person who received the message.
Message	The content of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Image	The image that was sent or received.
Message Status	The status of the message (received or sent).
Read Status	Whether or not the message has been read when the message was received.
Message ID	The ID number of the message.
Chat ID	The ID number for the chat this message was sent in.
Flags	Status flags associated with the message.

iOS Telegram Users

Description	Information about the various users that the suspect has encountered using Telegram, either directly or as part of a channel chat.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The ID number for the user.
First Name	The first name of the user.
Last Name	The last name of the user.
User Name	The user name of the user.
Phone Number	The phone number of the user.
Local First Name	The localized first name of the user. This attribute is unavailable for versions newer than 3.2.2.

ATTRIBUTE	DESCRIPTION
Local Last Name	The localized last name of the user. This attribute is unavailable for versions newer than 3.2.2.
Gender	The gender of the user. This attribute is unavailable for versions newer than 3.2.2.
Last Seen Date/Time - UTC (yyyy-mm-dd)	The last time that the user was seen by the local user.

iOS Textfree Cache Records

Description	The web cache for the iOS Textfree app.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the cached content.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date the cached content was created on the local device.
File Type	The type of the cached file (html, js, css, jpeg, and so on).
Content Size (Bytes)	The size of the cached content, in bytes.
Image	The raw content of the cached image. This is blank if the content is not an image (i.e. it's html, js, css, etc.).
Content	The raw cached content. This is blank if the content is an image (in which case, the 'Image' column is populated instead).

iOS TigerText Messages

Description	Sent and received messages with attachments from iOS TigerText app.
Notes	

ATTRIBUTE	DESCRIPTION
Message Created Date/Time - UTC (yyyy-mm-dd)	Date/Time that the message was sent.
Message Expiry Date/Time - UTC (yyyy-mm-dd)	Date/Time that the message will expire.
Message Recalled	Yes/No, whether the message was recalled.
Message Deleted	Yes/No, whether the message was deleted.
Attachment Type	Type of the attached file, in MIME format.

ATTRIBUTE	DESCRIPTION
Attachment	The content of the attachment file.
Message Status	The status of the message (new/delivered/read).
Sender Display Name	Display name of the sender.
Sender Username	User ID of the sender.
Sender Email	Email address of the sender.
Sender First Name	First name of the sender.
Sender Last Name	Last name of the sender.
Sender Phone Number	Phone number of the sender.
Sender Organization Name	Name of the sender's organization, or 'Personal' if the user has none.
Recipient Display Name	Display name of the recipient.
Recipient Username	User ID of the recipient.
Recipient Email	Email address of the recipient.
Recipient First Name	First name of the recipient.
Recipient Last Name	Last name of the recipient.
Recipient Phone Number	Phone number of the recipient.
Recipient Organization Name	Name of the recipient's organization, or 'Personal' if the user has none.

iOS Tinder Accounts

Description	A table containing all of the recovered iOS Tinder Accounts.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user id of current account owner.
Local User	Indicates if this is the local user's account (Yes or No).
Biography	A brief written biography about the users account.
Birthday (yyyy-mm-dd)	The birthday of the account user.
Distance (Miles)	The distance (in miles) that the user is searching for matches.
Gender	The gender of the account user.
First Name	The first name of the account user.
Last Activity Date/Time - UTC (yyyy-mm-dd)	The last date/time that the account user was active.

iOS Tinder Matches

Description	A table containing all of the recovered iOS Tinder Matches.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user id of the user whom you are matched with.
User Name	The name of the user whom you are matched with.
Gender	The gender of the matched user.
Created Date/Time - UTC (yyyy-mm-dd)	The UTC creation date of the match entry.
Last Activity Date/Time - UTC (yyyy-mm-dd)	The last time there was activity with the match.
Message Count	The number of messages exchanged with the matched profile.
Viewed Profile	Whether or not the user has viewed the profile.
Draft Message	The contents of a pending draft message.

iOS Tinder Messages

Description	A table containing all of the recovered iOS Tinder Messages.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user id of the user whom is part of this conversation.
Match ID	The id of the match who the message is received from.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The UTC date/time timestamp of the message was sent.
Message Body	The body of the message.

iOS Tinder Photos

Description	A table containing all of the recovered iOS Tinder Photos.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user id of the user whom the picture belongs to.
User Name	The name of the user whom this picture belongs to.
Image URL	The URL to the Tinder photo.

ATTRIBUTE	DESCRIPTION
Downloaded Image	The downloaded image.

KakaoTalk Messages - iOS

Description	KakaoTalk Messages contains messages that are sent or received by the user.
Notes	Message and Sender information are not available for deleted messages.

ATTRIBUTE	DESCRIPTION
Sender ID	The KakaoTalk ID of the sender.
Sender Name	The name of the sender if available, or the nickname otherwise.
Recipient ID	The KakaoTalk ID of the recipient.
Recipient Name	The name of the recipient if available, the nickname otherwise.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was created.
Read Date/Time - UTC (yyyy-mm-dd)	The date and time the message was deleted from the app.
Message Direction	Indicates whether the message was sent or received.
Message	The message content.
Metadata	JSON data that contains additional information for message types other than text.

Life360 Circle Members

Description	Life30 Circle Members contains information about the members of a circle. A circle is comprised of a group of individuals, such as a family, that the local user has created or has been added to by another circle member.
Notes	

ATTRIBUTE	DESCRIPTION
Member ID	The unique member ID of the circle member.
First Name	The first name of the member.
Last Name	The last name of the member.
Email Address	The email address of the member.
Phone Number	The phone number of the member.
Circle Name	The name the circle.

ATTRIBUTE	DESCRIPTION
Circle ID	The ID of the circle.

Life360 Local User Account

Description	Life360 Local User Account contains information of local user account.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	Unique ID of the local user.
First Name	The first name of the local user.
Last Name	The last name of the local user.
Email Address	The email address of the local user.
Phone Number	The phone number of the local user.

Life360 Messages

Description	Life360 Messages contains messages sent and received by the local user within a circle they're a member of.
Notes	

ATTRIBUTE	DESCRIPTION
Sender ID	Unique ID of the sender.
Sender Name	The name of the sender.
Recipient ID(s)	The id(s) of the recipient(s).
Recipient Name(s)	The name(s) of the recipient(s).
Message Type	The type of the message.
Message	The message content.
Created Date/Time	The date and time when the message was created.
Picture URL	The URL of the picture on the Life360 server, if a picture is included in the message.
Read	The read status of the message.
Latitude	The latitude of the location, if the message is map location.
Longitude	The longitude of the location, if the message is map location.
Location Name	The name of the location if the message is map location.

ATTRIBUTE	DESCRIPTION
Location Acquired Date/Time	The date and time when the location was acquired if the message is a map location.

Life360 Places

Description	Life360 Places indicates favorite locations that are saved by the user or the application.
Notes	

ATTRIBUTE	DESCRIPTION
Place Name	The name of the place. The name can be either user-defined or a default name defined by the application.
Place Address	The address of the place.
Circle ID	The ID of the circle where the place was found.
Owner ID	The owner ID of the place, if the place was created by user.
Latitude	The latitude of the place.
Longitude	The longitude of the place.

Life360 Trip Locations

Description	Life360 Trip Locations indicates the locations that the user visits (or passes by on the way to a destination). During a trip, the application will log locations at regular intervals along the way.
Notes	

ATTRIBUTE	DESCRIPTION
Updated Date/Time	The date and time that the trip details were last updated. Updates to the trip can be triggered by the user or the application.
Circle ID	The circle id of the user who created this trip.
User ID	The unique id of the user who created this trip.
Start Date	The date that the trip happened (days begin at 12:00 AM local time).
Latitude	The latitude of the location.
Longitude	The longitude of the location.
Start Date/Time	The date and time when the user arrived the location.

ATTRIBUTE	DESCRIPTION
End Date/Time	The date and time when the user left the location.
Location Name	The name of the location if it is a user created place.
Location Address	The address of the location.

LINE Contacts

Description	The user's LINE contacts.
Notes	

ATTRIBUTE	DESCRIPTION
Line ID	The LINE id of the contact.
Name	The name of the LINE contact.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time the user contact was added.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the contact was last updated.
Status Message	The status of the contact.
Hidden	Whether the contact has been marked as hidden.
Favorite	Whether the contact has been marked as favorite.

LINE Local Users

Description	The local user accounts for LINE on the device.
Notes	

ATTRIBUTE	DESCRIPTION
Line ID	The LINE specific, unique identifier of the user.
User Name	The user's account name.
User Nickname	The user's nick name.
Status Message	The status the user has set for themselves.
Unread Message Count	The number of unread messages the user has.
Missed Call Count	The number of missed calls the user has.

LINE Messages

Description	The LINE messages that were recovered from an iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the message. Can be the sender name, or 'Local User'
Recipient(s)	The recipient(s) of the message.
Message Created Date/Time - UTC (yyyy-mm-dd)	The date and time the message was created.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Message	The body of the message.
Message Type	The type of message. This can be a 'Audio', 'Call', 'Contact Card', 'File', 'Location', 'Note', 'Picture', 'Sticker', 'Text'.
Contact Card Name	The contacts name (first and last name).
Read Count	The number of times the message has been read.
Location Address	The address of the location.
Latitude	Contains the latitude of the location when message type is 'Location'.
Longitude	Contains the longitude of the location when the message type is 'Location'.
Audio Length (Seconds)	Contains the length of the audio in seconds when message type column is 'Audio'.
Call Duration (Seconds)	Contains the duration of the call is seconds when the message type is 'Call'.
File Attachment	Contains the name of the file that's sent when the message type is 'File'.
File Size (Bytes)	Contains the size of the file sent in bytes.
Thumbnail	A thumbnail of the image (if available).

LINE Pictures

Description	The LINE pictures that were recovered from an iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.

ATTRIBUTE	DESCRIPTION
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date/time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date/time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date/time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. "Complete" indicates that a full Exif extraction was performed. "Failed" indicates that the information may have been corrupted and could not be recovered. "Skipped" indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).

ATTRIBUTE	DESCRIPTION
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
Longitude	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the pciture was taken (extracted from Exif data).
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

Mail.Ru Agent Contacts

Description	Mail.Ru Agent Contacts contains contact info for the Agent app on iOS.
Notes	

ATTRIBUTE	DESCRIPTION
Contact ID	The user ID of contact.
Display Name	The display name of contact.
Account Type	The type of the contact. The value can be Agent ID or Agent Channel.
Local User ID	Unique ID of the local user.

Mail.Ru Agent Messages

Description	Mail.Ru Agent Messages contains messages sent or received by the Agent user on iOS.
Notes	

ATTRIBUTE	DESCRIPTION
Local User ID	Unique ID of the local user.
Remote User ID	The user ID of the remote participant of the chat.

ATTRIBUTE	DESCRIPTION
Remote Participant Display Name	The display name of remote participant.
Created Date/Time	The date/time that the message was created.
Message	The content of the message.
Type	The type of the message. The value can be Text Message, Voice Call, Video Call or File Transfer.
Duration (Seconds)	The duration of voice or video call, in seconds.
Direction	The direction of the message.
File Name	The file name of the attachment.

Mail.Ru Agent User Accounts

Description	Mail.Ru Agent User Accounts contains information about the Agent user accounts that are saved locally on the iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	Unique ID of the local user.
Active	Whether or not the account is currently logged in.
First Name	First Name of the account.
Last Name	Last Name of the account.
Display Name	Display Name of the account.
Birthday	Birthday of the account.
Phone Number	Phone number of the account.
Gender	Gender of the account.
Home Address	Home address of the account.

ooVoo Chat History

Description	This table contains the chat history between the data owner and their contacts.
Notes	

ATTRIBUTE	DESCRIPTION
Message ID	The ooVoo unique message identifier.
Sender User ID	The ooVoo identifier of the sender.

ATTRIBUTE	DESCRIPTION
Receiver User ID(s)	The ooVoo identifier of the recipient(s).
Chat Date/Time - UTC (yyyy-mm-dd)	The date and time of the conversation.
Message	The actual message content.
Message Type	The type of message that was sent. Some examples are: Chat, Video, Image, etc.
Message Direction	Indicates whether the message was sent (Outgoing) or received (Incoming).
Group Name	The name that is associated with a group conversation. If the chat is between two people the name will be empty.
Video URL	The address of the video that was sent in the message.
Image URL	The address of the image that was sent in the message.
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

ooVoo Contact List

Description	This table contains the list of contacts the data owner has on ooVoo.
Notes	

ATTRIBUTE	DESCRIPTION
Display Name	The contact display name
User ID	The contacts unique ooVoo identifier.
Status Message	A message set by the contact. This message can contain insight into how the person is feeling or share ideas/thoughts.
Birthday (yyyy-mm-dd)	The contact's birthday.
Phone Number	The contact's phone number.
Password	The contact's password stored as plain text.
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

ooVoo Phone Book

Description	This table contains the name and phone number of contacts from the data owners iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Contact Name	The name of the contact.
Phone Number	The contacts phone number
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

QQ File Transfers

Description	QQ file transfers recovered from the iOS QQ International app.
Notes	

ATTRIBUTE	DESCRIPTION
Local User ID	The local user ID who the file was transferred with.
Chat Partner / Group Chat ID	Either a unique ID for the chat partner or an ID for the group, if the transfer comes from a group conversation.
Partner Display Name	The name displayed for the partner the file was transferred with.
File Name	The file name of the file transferred.
File Path	The file path of the file transferred.
Server Date/Time - UTC (yyyy-mm-dd)	The server date and time the file was transferred.
File Size (bytes)	The size of the file transferred, in bytes.
Direction	The direction of the file transfer relative to the local user (Sent or Received).
MD5 Hash	The MD5 hash of the file.
SHA1 Hash	The SHA1 hash of the file.

QQ Local Users

Description	QQ local users recovered from the iOS QQ International app.

Notes	

ATTRIBUTE	DESCRIPTION
Local User ID	The user id of the local user.
Local User Display Name	The name displayed for the local user.
Country	The country of the user.
City	The city of the user.
Age	The user's age in years.
Birthday (yyyy-mm-dd)	The user's birthday in YYYY-MM-DD format.
Email	The user's email address.

QQ Messages

Description	Messages stored by the iOS QQ International app.
Notes	

ATTRIBUTE	DESCRIPTION
Local User ID	Unique ID of the local user.
Local User Display Name	The name displayed for the local user.
Chat Partner / Group Chat ID	Unique ID of the chat partner or group.
Sender User ID	Unique ID of the sender.
Sender Display Name	The name displayed for the sender.
Message	Text of the message.
Message Date/Time - UTC (yyyy-mm-dd)	Date/Time associated with the message.
Type	The type of content in the message.
Sent/Received	Sent/Received. Indicates whether this message is incoming or out-going.
Read	Read/Unread, whether this message has been read.

QQ Messages Carved

Description	Carved messages stored by the iOS QQ International app.
Notes	

ATTRIBUTE	DESCRIPTION
Local User ID	Unique ID of the local user.
Local User Display Name	The name displayed for the local user.
Chat Partner / Group Chat ID	Unique ID of the chat partner or group.
Sender User ID	Unique ID of the sender.
Sender Display Name	The name displayed for the sender.
Message	Text of the message.
Message Date/Time - UTC (yyyy-mm-dd)	Date/Time associated with the message.
Type	The type of content in the message.
Sent/Received	Sent/Received. Indicates whether this message is incoming or outgoing.
Read	Read/Unread, whether this message has been read.

Signal Contacts

Description	Signal Contacts lists all the contacts and profiles present in the app. This artifact usually recovers contact information for the local user, although it is not possible to indicate with certainty which contact is the local user.
Notes	

ATTRIBUTE	DESCRIPTION
Phone Numbers	The list of phone numbers associated with the contact.
Full Name	The full name of the contact as stored by the Signal app.
Profile Name	The profile name of the contact. This is usually a nickname.
Avatar	The avatar used by the contact.

Signal Group Members

Description	Signal Group Memebers specifies the members from each of the Signal groups that the local user is a member of.
Notes	

ATTRIBUTE	DESCRIPTION
Group Member	The phone number of the group memeber.
Group Name	The name of the group.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the group was created.

ATTRIBUTE	DESCRIPTION
Group Avatar	The avatar of the group.

Signal Local User

Description	Signal local User contains information about the local user account.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The name of the local user.
Avatar	The avatar used by the local user account.

Signal Messages - iOS

Description	Signal Messages - iOS contains information about the messages and calls that are exchanged between the local user and other users on an iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the message.
Recipient(s)	The message recipient(s)
Group Name	The name of the group the message was set in.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was received.
Message	The content of the message.
Attachment Name	The name of the message attachment if one was sent.
Attachment	The content of the attachment if one was sent.
Type	The type of the message.
Direction	The direction of the message (incoming, outgoing).
Call Status	The status of the call (connected, missed).
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the message is set to expire.
Expiration (dd hh:mm:ss)	The expiration policy that was set on the conversation at the time of sending the message.

Skype Accounts

Description	Information about the Skype accounts that are recovered, such as user info and when the account was created.
Notes	

ATTRIBUTE	DESCRIPTION
Skype Name	The Skype user name
Display Name	The visual display name
Full Name	The full name of the user
Birthday	The user's birthday
Gender	The gender of the user
City	The city in which the user has set
State / Province	The state/province in which the user has set
Country	The Country in which the user has set
Home Phone	The user's home phone number.
Office Phone	The user's office phone number
Mobile Phone	The user's mobile phone number
Email(s)	The user's email email address. Can be more than one
Homepage	The user's website
About Info	About the user
Profile Created On Date/Time - (UTC) (yyyy-mm-dd)	The date and time the profile was created
Profile Last Modified Date/Time - (UTC) (yyyy-mm-dd)	The date and time the profile was last modified
Mood Text	The user's mood
Last Online Date/Time - (UTC) (yyyy-mm-dd)	The date and time the user was last online
Last Used Date/Time - (UTC) (yyyy-mm-dd)	The last date and time the account was used
Avatar Timestamp Date/Time - (UTC) (yyyy-mm-dd)	The last date and time the user updated their display picture
Image	The display picture image

Skype Activity

Description	Skype Activity contains interactions that occur between users on Skype. These interactions include messages, group interactions, calls, files sent/received, and SMS. Applies to Skype 8.1 and later.

Notes	

ATTRIBUTE	DESCRIPTION
Conversation ID	ID of this conversation.
Profile Name	The local user's profile name.
Sender	The username of the sender/initiator of the interaction.
Sender Email	The sender's email as given in the message (if available).
Recipient Name(s)	The recipients or targets of the interaction.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the interaction was initiated.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the interaction was last updated (for example, when a call ends).
Message Type	The type of the interaction.
Message	The content of the message or summary of the interaction.
Emotion Count	The number of reactions to the interaction (for example, likes, dislikes, emojis, and so on).
File Name	The name of any attached files associated with the interaction.
File Size (Bytes)	The size in bytes of any attached files.
File	The attachment file (if applicable).
Attachment Data Recovered	Whether the attached file was recovered from the local filesystem.
Thumbnail URL	A URL that directs to the thumbnail picture (if applicable).
Call Duration (Seconds)	The length of the call in seconds (if applicable).
Metadata	The content of the message, if it consisted of interpreted data (that is, XML or JSON data, rather than plain text).

Skype Calls

Description	Information about Skype calls that occur between users.
Notes	

ATTRIBUTE	DESCRIPTION
Local Username	The user logged into Skype at the time of the call.
Call Initiator	The user who started the call.
Initiator Display Name	The display name of the user. This might be different from the username.
Recipient(s)	The users who accepted a call from the call initiator and participated in the call for a period of time.

ATTRIBUTE	DESCRIPTION
Call Participants	The users who accepted and participated in the call from the call initiator for some duration.
Started Date/Time - UTC (yyyy-mm-dd)	Start time of the call.
Duration	Total duration of the Skype call.
Metadata	Additional details about the call extracted in XML format. This includes the duration of time each participant was in the call.

Skype Chat Messages

Description	Skype messages sent from one user to another.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	Profile name of the caller
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent
Author	Author of the message
From Display Name	The display name of who sent the message
Message	The body of the message or a description of the action taken. For example, adding another participant to a group chat or sharing a file or picture.
Attachment Name	The name of the attachment that was sent. This attribute is populated when the Message Type is POSTED_FILE or POSTED_PICTURE. Otherwise, this attribute is empty.
Attachment Size (Bytes)	The size of the attached file, in bytes. This attribute is populated when the Message Type is POSTED_FILE or POSTED_PICTURE. Otherwise, this attribute is empty.
Metadata	Additional details about the action, extracted in its original XML format.
Message Status	The status of the message.
Message Type	Type of message
Chat ID	ID of this chat
Recipient	Recipient of the chat

Skype Chatsync Messages

Description	Skype messages sent from one user to another that are parsed from the chatsync directory.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local Skype user
Chat Initiator	The user that started the conversation
Chat Partner/Group Chat ID	The other user in the chat, or a group chat identifier
Message Type	Whether the message was sent or received
Message	The content or body of the message
Message Sent Date/Time - (UTC) (yyyy-mm-dd)	The date and time the message was sent

Skype Contacts

Description	Information about Skype contacts that are recovered, which may or may not be added contacts.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	The name of the contact
Skype Name	The Skype name of the contact
Display Name	The contact's display name
Is Blocked	Whether or not the contact is blocked
Contact Added	Specifies whether the contact is an added contact or just cached into the database (1 if the contact was added, 0 otherwise). Contacts can be cached into the database for a variety of reasons (for example, as a 'suggested contact').
Full Name	The contact's full name
Birthday (yyyy-mm-dd)	The contact's birthday
Gender	The contact's gender
City	The city the contact is from
State / Province	The state/province the contact is from
Country	The country that the contact is from
Home Phone	The contact's home phone number
Office Phone	The contact's office phone number
PSTN Number	The contact's public switched telephone network
Email(s)	The email address(es) of the contact
Homepage	The contact's homepage
About Info	About the contact
Profile Loaded Date/Time - (UTC) (yyyy-mm-dd)	Previously called "Profile Created On Date/Time", this attribute represents the date/time when a contact's profile is first created on the user's device. When the profile information is updated by the contact, the date in the database is also updated.

ATTRIBUTE	DESCRIPTION
Profile Last Modified Date/Time - (UTC) (yyyy-mm-dd)	the date and time the contact last modified their profile
Mood Text	The contact's mood
Last Online Date/Time - (UTC) (yyyy-mm-dd)	The last date and time the contact was seen online
Last Used Date/Time - (UTC) (yyyy-mm-dd)	The last date and time the contact accessed contacts
Avatar Timestamp Date/Time - (UTC) (yyyy-mm-dd)	The last date and time the contact updated their avatar

Skype Emotions

Description	Skype Emotions contains reactions from users on Skype messages.
Notes	

ATTRIBUTE	DESCRIPTION
Emotion	The type of emotion the user reacted to the message with. The emotion is displayed using the shortcut from Skype (for example, "cwl" represents the emotion "Crying With Laughter").
Message Content	The content of the message the user reacted to. If the content of the message is plain text, this attribute matches the "Message" attribute from the "Skype Activity" artifact. Otherwise, this attribute matches the "Metadata" attribute.
Skype Name	Skype Name of the user who reacted to the message.
Date/Time - UTC (yyyy-mm-dd)	Reacted Date/Time - UTC (yyyy-mm-dd)

Skype File Transfers

Description	Files that are transferred from one user to another using Skype.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	The name of the user
Partner Handle	The user name of the file transfer partner
Partner Display Name	The display name of the file transfer partner
File Name	The file name being transferred
Type	The type of file being transferred
File Path	The path to the local file
Transferred File	The file that was transferred
File Size (Bytes)	The size of the file being transferred
Bytes Transferred	The number of bytes that were transferred
Transfer Start Date/Time - UTC (yyyy-mm-dd)	The date and time the file transfer was started
Transfer Finish Date/Time - UTC (yyyy-mm-dd)	The date and time the file transfer completed
Status	The status of the file (for example, transfer, transferring or cancelled)

Skype Group Chat

Description	Information about the Skype group chats that a user is a part of.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	The name of the user
Chat ID	The group chat's unique identifier
Participants	The participants of the chat
Posters	The users that have posted to the chat
Active Members	The currently active user's of the group
Chat name	The name of the chat
Started Date/Time - (UTC) (yyyy-mm-dd)	The date and time the chat started
Last Changed Date/Time - (UTC) (yyyy-mm-dd)	The date and time the chat was modified

Skype IP Addresses

Description	IP addresses that are associated with a Skype user account.
Notes	

ATTRIBUTE	DESCRIPTION
Username	The Skype user name
IP Address	The IP address of that user
IP Address Type	The IP address type
Date/Time - (UTC) (yyyy-mm-dd)	The date and time of the IP address log

Skype Notifications

Description	Skype Notifications contains notifications shown to users on Skype.
Notes	

ATTRIBUTE	DESCRIPTION
Read	Whether the user has read the notification.
Conversation ID	ID of this conversation.
Profile Name	The local user's profile name.
Sender	The username of the sender/initiator of the interaction.
Recipient Name(s)	The recipients or targets of the interaction.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the interaction was initiated.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the interaction was last updated (for example, when a call ends).
Message Type	The type of the interaction.
Message	The content of the message or summary of the interaction.
Emotion Count	The number of reactions to the interaction (for example, likes, dislikes, emojis, and so on).
File Name	The name of any attached files associated with the interaction.
File Size (Bytes)	The size in bytes of any attached files.
File	The attachment file (if applicable).
Attachment Data Recovered	Whether the attached file was recovered from the local filesystem.
Thumbnail URL	A URL that directs to the thumbnail picture (if applicable).
Metadata	The content of the message, if it consisted of interpreted data (that is, XML or JSON data, rather than plain text).

Skype SMS

Description	SMS messages that a user sends or recieves using Skype.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	The name of the user
Message Sent Date/Time - (UTC) (yyyy-mm-dd)	The date and time the message was sent
Author	The author of the message
Message	The message content
Target Number(s)	The recipient phone numbers
Status	The status of the message.
Reply-to Number	A phone number the recipients can reply to

Skype Voicemails

Description	Voicemails that a user sends or recieves using Skype.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	The name of the user
Partner Handle	The user name of the conversation partner
Partner Display Name	The display name of the conversation partner
Subject	Identifies the subject of the voicemail
Message Sent Date/Time - (UTC) (yyyy-mm-dd)	The date and time the message was sent
Duration	The length of the voicemail
Allowed Duration	The maximum length allowed for the voicemail
Size	The size of the recording
Path	The file path of the voicemail
Type	Identifies whether the voicemail was received or sent.
Status	The status of the voicemail, recording or played for example.

Slack Channel Messages

Description	Slack Channel Messages contains messages sent or received in channels in the user's Slack workspace.
Notes	

ATTRIBUTE	DESCRIPTION
Workspace ID	The unique identifier for the slack workspace.

ATTRIBUTE	DESCRIPTION
Sender	The name or user ID of whoever sent the message.
Channel Name	The name of the channel that the message was sent to.
Message	The message text.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message Status	The delivered status of the message.

Slack Channels

Description	Slack Channels contains information about each of the channels and conversations that exist in a user's Slack workspace.
Notes	

ATTRIBUTE	DESCRIPTION
Channel Name	The name of a channel or message group.
Channel ID	The ID of a channel or message group.
Workspace ID	The unique identifier for the slack workspace.
Created By	The name or user ID of whoever created the channel.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the channel was created.
Topic	The topic text for the channel.
Topic Author	The name or user ID of whoever last wrote the topic text.
Channel Type	The type of channel (Public, Private, General, Single User DM, Multi User DM.)
Last Read Date/Time - UTC (yyyy-mm-dd)	The date and time when the channel was last read.
Member	Represents whether or not the local user is a member of the channel.
Starred	Represents whether or not the local user has starred the channel.

Slack Direct Messages

Description	Slack Direct Messages contains information about direct messages sent or received in 1:1 chats or group chats.
Notes	

ATTRIBUTE	DESCRIPTION
Workspace ID	The unique identifier for the slack workspace.

ATTRIBUTE	DESCRIPTION
Sender	The names or user IDs of the message recipients.
Message	The message text.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message Status	The delivered status of the message.

Slack Files

Description	Slack Files contains information about any files that have saved to the Slack workspace. Files may or may not have been shared with other users.
Notes	

ATTRIBUTE	DESCRIPTION
Workspace ID	The unique identifier for the slack workspace
Title	The title given to the file.
File Name	The name of the file.
Created By	The name or user ID of whoever created the file.
Permanent Link	A permalink to the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was uploaded
FileSize	The size of the file
Deleted	Represents whether or not the file has been deleted.

Slack Users

Description	Slack Users contains information about each user in the Slack workspace.
Notes	

ATTRIBUTE	DESCRIPTION
Workspace ID	The unique identifier for the slack workspace.
Full Name	The full name of the user.
First Name	The first name of the user.
Last Name	The last name of the user.
User Name	The unique user name of the user.
Display Name	The slack display name of the user.
Email	The user email.

ATTRIBUTE	DESCRIPTION
Phone Number	The user phone number.
Member ID	The user ID.
Title	The user title.
Status Message	The status message for the user
Account Type	The type of account the user has.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the user was last updated.
Timezone	The timezone the user is in.

Slack Workspaces

Description	Slack Workspaces contains information about each of the workspaces that the local user is apart of.
Notes	

ATTRIBUTE	DESCRIPTION
ID	The unique identifier for the slack workspace.
Name	The name of the slack workspace.
Domain	The domain of the slack workspace.
Local User ID	The unique identifier of the local user.
Local User	The name of the local user.
Local User Display Name	The display name of the local user.
Local Email Address	The email address of the local user.
Password/Token	The local user password/token.

TamTam Messenger Channels - iOS

Description	TamTam Messenger Channels contains messages that belong to channel conversations recovered from the local device. The user must be subscribed to the channel in order to receive the messages.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The name of the channel in which the message originated.
Sender ID	The TamTam ID of the channel in which the message originated.
Recipient	Display name of the owner contact that received the message.

ATTRIBUTE	DESCRIPTION
Recipient ID	The TamTam ID of the owner contact that received the message
Message	The content of the message. If the messages is a contact share, this attribute displays the text from the VCard.
Message Timestamp Date/Time - UTC (yyyy-mm-dd)	The time stamp of the message.
Latitude	The latitude coordinate, if the message type is Geo location.
Longitude	The longitude coordinate, if the message type is Geo location.
Attachment URL	A URL for any attachments that are sent or received. Attachments can be downloaded from this URL. However, to recover pictures properly, you must append '&fn=w_1440' manually to the end of the URL.
Attachment	The locally stored attachment, if the attachment was sent by the local user.

TamTam Messenger Contacts - iOS

Description	TamTam Messenger Contacts displays information about the TamTam contacts associated with the local user's account (including the local user).
Notes	

ATTRIBUTE	DESCRIPTION
Contact ID	A unique ID for the contact.
Profile Name	The profile name of the contact.
Website URL	The contact's TamTam website URL, if one exists.
About Info	Information that the user has provided about their self.
Avatar URL	A URL to the user's profile picture. A termination '&fn=w_1440' should be manually added to the URL to properly display the picture.
Updated Date/Time - UTC (yyyy-mm-dd)	The last time the contact was updated on the local device. If the contact was not added by the local user, this does not display a value. Some contacts might be stored on the local user's device and may have not been added to their contact list. For example, this might occur when the local user belongs to a group but does not have all of the group participants as contacts. In these cases, TamTam adds the group contacts to the app database but they won't automatically be updated.

TamTam Messenger Conversations - iOS

Description	TamTam Messenger Conversations contains information about all the chats recovered from the local device (includes individual, group, channel and draft messages).
Notes	

ATTRIBUTE	DESCRIPTION
Chat ID	A unique ID for the conversation.
Chat Type	The type of conversation (Individual, Group, User Channel and Default Channel). Individual indicates one-to-one conversations, while Group indicates many-to-many conversations. User Channel indicates a one-to-many conversation created by a TamTam user. Default Channels are one-to-many conversations created and managed by TamTam.
Participants	List of participants that belong to that conversation. User Channels only display the local user as a participant whereas Default Channels do not display any participants.
Chat Name	The name of the conversation (only available in Groups and Channels).
Description	Description of the conversation (only available in Groups and Channels). Channels may have more than one description in the blob data, the second occurrence is used by default. The first occurrence of the description may be used for default seeded channels.
Conversation Status	Indicates the state of the owner's participation in the conversation.
Last Sent Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time in which a message was last sent.
Address URL	The URL for the channel's webpage. Users can sign up to the channel using this page if the channel is public.

TamTam Messenger Groups - iOS

Description	TamTam Messenger Groups contains all messages that belong to group conversations recovered from the local device.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	Display name of the contact who sent the message. If the sender is not a contact and therefore unknown to the owner, TamTam Sender ID is displayed.
Sender ID	The TamTam ID of the contact who sent the message.

ATTRIBUTE	DESCRIPTION
Recipient	Display name of the owner user who received the message.
Recipient ID	The TamTam ID of the owner user who received the message.
Message	The content of the message. If the messages is a contact share, this attribute displays the text from the VCard.
Message Timestamp Date/Time - UTC (yyyy-mm-dd)	The time stamp of the message.
Status	Indicates whether the original message had been edited or deleted by the sender.
Latitude	The latitude coordinate, if the message type is Geo location.
Longitude	The longitude coordinate, if the message type is Geo location.
Attachment URL	A URL for any attachments that are sent or received. Attachments can be downloaded from this URL. However, to recover pictures properly, you must append '&fn=w_1440' manually to the end of the URL.
Attachment	The locally stored attachment.

TamTam Messenger Messages - iOS

Description	TamTam Messenger Messages contains all individual messages (one-to-one) recovered from the local device.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	Display name of the contact who sent the message.
Sender ID	The TamTam ID of the contact who sent the message.
Recipient	Display name of the contact that received the message.
Recipient ID	The TamTam ID of the contact that received the message.
Message	The content of the message. If the messages is a contact share, this attribute displays the text from the VCard.
Message Timestamp Date/Time - UTC (yyyy-mm-dd)	The time stamp of the message.
Status	Indicates whether the original message had been edited or deleted by the sender.
Latitude	The latitude coordinate, if the message type is Geo location.
Longitude	The longitude coordinate, if the message type is Geo location.
Attachment URL	A URL for any attachments that are sent or received. Attachments can be downloaded from this URL. However, to recover pictures properly, you must append '&fn=w_1440' manually to the end of the URL.

ATTRIBUTE	DESCRIPTION
Attachment	The locally stored attachment.

Textfree Attachments

Description	Attachments from the iOS Textfree app.
Notes	

ATTRIBUTE	DESCRIPTION
Message ID	The ID for the message.
Media URL	The URL from where the media could originaly be downloaded.
Type	The type of media (for example: picture, voicemail, video).
Preview	The binary data of the attachment. If the attachment is a video, the preview is a frame from the video.
Metadata	Any metadata associated with the attachment (for example, VoicemailDuration).
Media ID	The internal ID used by the app. This value may point to other places where the attachment is used and/or contained.

Textfree Contacts

Description	Contacts from the iOS Textfree app.
Notes	

ATTRIBUTE	DESCRIPTION
First Name	First name of the contact.
Last Name	Last name of the contact.
Company Name	Company name of the contact.
Phone Numbers	All phone numbers associated with the contact.
Email(s)	All emails associated with the contact.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time the contact was modified.
Contact ID	The internal ID used by the app. This value may point to other places where the attachment is used and/or contained.

Textfree Groups

Description	Information about group chats from the iOS Textfree app.
Notes	

ATTRIBUTE	DESCRIPTION
Group	The group number.
Group Name	The name of the group.
Group Phone Number	The phone number of the group.
Group Member Name(s)	Names of all group participants.
Group Member Phone Number(s)	Phone numbers of all group participants.

Textfree Messages

Description	Messages from the iOS Textfree application.
Notes	

ATTRIBUTE	DESCRIPTION
Message Partner	The name of the message partner.
Message Partner ID	The ID of the messaging partner. This value may contain the contact's phone number.
Sender Name	The name of the sender.
Sender ID	The ID of the sender.
Message ID	The ID of the message. This value can be used to find related attachments in the TextFree Attachments table.
Message Body	The content of the message.
Created Date/Time - UTC (yyyy-mm-dd)	The Date/Time associated with the message.
Attachment Type	The type of media file (for example: jpeg, png, wav).
Media URL	The URL from where the media could originally be downloaded.
Media ID	The internal ID used by the application. This value may point to other places where the attachment is used or contained, or both.
Message Type	The type of message (for example, call, voicemail, or message).
Chat Type	The type of a chat where the message originates from. Values can be individual, group, or system.
Direction	The direction of the message (for example, sent or received).

ATTRIBUTE	DESCRIPTION
Read	The read status of the message.
Call Duration (Seconds)	Call duration in seconds, if the message is a call.

TextMe Calls

Description	Information about the calls that the suspect participates in using the TextMe app.
Notes	For iOS TextMe Calls, we cannot determin whether a call was an audio or video call, and therefore the 'Call Type' column will always be empty.

ATTRIBUTE	DESCRIPTION
Sender	The sender of the call.
Recipient	The recipient of the call.
Display Name	The chosen display name for the call participant.
Call Start Date/Time - UTC (yyyy-mm-dd)	The date and time the call was initiated.
Call End Date/Time - UTC (yyyy-mm-dd)	The date and time the call ended.
Direction	The direction of the call, either incoming or outgoing.
Status	Whether the call was unanswered, answered, or if the user has listened to the attached voicemail.
Call Type	Whether the call was an audio or video call.
Voicemail	The associated voicemail message.

TextMe Messages

Description	Individual chat messages that are sent and received using the TextMe app.
Notes	For iOS TextMe Messages, the attachemnts are located at the same folder as the database, so the 'Attachment Path' column will always be empty.

ATTRIBUTE	DESCRIPTION
Conversation Partner	The name of the other participant in the conversation.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent, regardless of whether the message was sent or received.
Message	The body of the message.
Direction	Whether the message was sent or received.

ATTRIBUTE	DESCRIPTION
Status	Whether the message was unsent, sent, delivered, or read.
Attachment Name	The name of the attachment, if one exists (can be pictures, videos, or URL links).
Attachment Path	The file path of the attachment, if one exists.
Attachment	The attachment data.

TextNow Calls

Description	Information about calls and voicemails that are sent and received through the TextNow app.
Notes	If the Contact Name cannot be determined, the Local Contact Key may be used to locate the corresponding entry in the iOS TextNow Contacts artifact.

ATTRIBUTE	DESCRIPTION
Call Type	The type of call or voicemail.
Direction	Whether the call was incoming or outgoing.
Server Date/Time - UTC (yyyy-mm-dd)	The date and time the voicemail was registered by the TextNow server.
Device Date/Time - UTC (yyyy-mm-dd)	The date and time the call or voicemail was registered by the local device.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the call.
Duration (Seconds)	The duration of the call.
Contact ID	The ID for the other call participant.
Local Contact Key	The numeric key for the other call participant.
Contact Display Name	The display name of the other call participant.
Contact Type	The other participant's contact type.
Conversation Type	The type of conversation.
Conversation Partner	The name of the other call participant.
Voicemail URL	The URL of the voicemail.
Call Status	Whether the voicemail was received by the user.
Attachment Path	The voicemail attachment path.
Call ID	The SIP ID of the call.

TextNow Chat

Description	Chat messages that are sent and received through the TextNow app.

Notes	If the Contact Name cannot be determined, the Local Contact Key may be used to locate the corresponding entry in the iOS TextNow Contacts artifact.

ATTRIBUTE	DESCRIPTION
Message	The body of the message.
Server Date/Time - UTC (yyyy-mm-dd)	The date and time the message was registered by the TextNow server.
Device Date/Time - UTC (yyyy-mm-dd)	The date and time the message was registered by the local device.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the message.
Contact ID	The ID for the other message participant.
Local Contact Key	The numeric key for the other message participant.
Contact Display Name	The display name of the other message participant.
Contact Type	The other participant's contact type.
Message Type	The type of message.
Message Direction	Whether the message was incoming or outgoing.
Conversation Type	The type of conversation.
Author Name	The author of the message.
Message Status	The status of the message (read or unread).
Group Name	Group name, if the message was sent to a group chat.
Signature	The user's appended signature.
Attachment Path	The attachment path.
File Name	The file name of the attachment.
Attachment	The video or picture attachment file that was sent.

TextNow Contacts

Description	The app, phone, email and group contacts that a user has in the TextNow app.
Notes	

ATTRIBUTE	DESCRIPTION
Contact ID	The name of the contact.
Contact Type	The contact's type.
Local Contact Key	The numeric key for the contact.
Contact Display Name	The display name contact.
Contact Label	The descriptive label of the contact.

TextNow Groups

Description	Membership information for TextNow group chats.
Notes	

ATTRIBUTE	DESCRIPTION
Group Chat ID	The ID for the group.
Group Name	The name of the group.
Contact ID	The name of the group member.
Contact Display Name	The display name of the group member.
Contact Type	The group member's contact type.
Local Contact Key	The numeric key for the group member.
Contact Uri	The Android resource uri of the group member.

TextNow Profile

Description	TextNow user profile and app preference settings.
Notes	

ATTRIBUTE	DESCRIPTION
First Name	The first name of the TextNow user.
Last Name	The last name of the TextNow user.
Email	The email of the TextNow user.
User Name	The username of the TextNow user.
Phone Number	The phone number of the TextNow user.
Last Number Called	The last number called using the TextNow app by the user.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the profile information was last updated.
Gender	The gender of the TextNow user.
Birthday (yyyy-mm-dd)	The birthday of the TextNow user.
Forwarding Number	The forwarding number in use by the TextNow user.
Forwarding Expiry UTC (yyyy-mm-dd)	The date and time at which forwarding expires.
Signature	The signature automatically appended to the end of each TextNow message sent by the user.
TextNow Credit	The TextNow credit held by the user.

ATTRIBUTE	DESCRIPTION
Balance	The TextNow cash balance held by the user.

TextPlus Calls

Description	Contains call information from TextPlus data on an iOS device.
Notes	Group messages are not supported at this time, instead messages sent simultaneously to more than one recipient are displayed as separate hits.

ATTRIBUTE	DESCRIPTION
User Name	The user name of the TextPlus account.
User	The identifier for the recipient of the call. This could be a GUID or phone number depending on the TextPlus version.
Display Name	The display name of the TextPlus account.
Date/Time - UTC (yyyy-mm-dd)	The date/time the call was made.
Duration (Units Unknown)	The duration of the call. Can be in milliseconds or seconds. Requires human inspection and reasoning to determine which.

TextPlus Messages

Description	Contains message information from TextPlus data on an iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Sender Name	The sender of the message.
Sender	The identifier for the sender of the message. This could be a GUID or phone number depending on the TextPlus version.
Recipient Name	The recipient of the message.
Recipient	The identifier for the recipient of the message. This could be a GUID or phone number depending on the TextPlus version.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent or received.
Message Body	The text contents of the message.
Message Type	Indicates if the message is 'Incoming Message', 'Outgoing Message' or an unknown message type.

ATTRIBUTE	DESCRIPTION
Status	Indicates if the message was read ('Read'), unread ('Unread') or has an unknown status.

Threema

Threema is an instant messaging application for iOS and Android, which provides end-to-end encryption of all user communications, including texts, voice calls, media files and more. In addition to providing end-to-end encryption, Threema allows you to create an account without requiring personal information such as your phone number or email address.

The content of a suspect's sent and received messages can be valuable to an investigation, as well as their name and the names of their recipients. Other information can also be recovered, such as the shared location of a suspect, as well as when a message was sent, delivered, and read. This information can help to identify users who have been working with a suspect, the possible whereabouts of a suspect, and can offer insight into the purpose of a suspect's interactions.

Cryptography Details

Threema uses the NaCL Networking and Cryptography Library to provide end-to-end encryption and to secure the transport of incoming and outgoing messages.

Local Data encryption

All messages sent and received using Threema are encrypted and stored on a user's mobile device. On iOS devices, Threema stores a user's local data in a Core Data database, which is backed up by the files found in the application's private data directory. This data includes message history, contacts, and more, and is protected with an encryption key that is created from the device's UID key and passcode. To decrypt the data on an iOS device, the device must be jailbroken or you will need to acquire the device image using GrayKey.

Artifacts

Threema Messages

Threema Users

Threema Messages

Description	Threema Messages contains messages sent and received by the local Threema user.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The display name of the sender.
Recipient(s)	The display names of the recipients.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message	The content of the message.
Read Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was read.
Delivered Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was delivered.
Message Type	The type of message that was sent. This can include Audio, File, Image, Location, Text, or Video.
Message Direction	The direction of the message.
Duration	The duration in seconds of the Audio or Video.
Latitude	The latitude extracted from the location data that is sent with the message.
Longitude	The longitude extracted from the location data that is sent with the message.
File Name	The name of the file that was sent.

Threema Users

Description	Information about the various users that the suspect has encountered using Threema.
Notes	

ATTRIBUTE	DESCRIPTION
Display Name	The display name of the user.
First Name	The first name of the user.
Last Name	The last name of the user.
Avatar	The avatar of the user.

Viber Messages

Description	Contains details about sent/received Viber messages on an iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the message.
Recipient(s)	The recipient(s) of the message. In a group chat, the recipients will be shown as a comma-delimited list.
Participant	The phone number of one of the participants of the call. The owner of this number is not known at the time, and it is up to the investigator to determine if this is the local user, or that of the chat partner.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Message	The message that was sent. If the message type was a call this will identify if the call was outgoing, incoming or a missed call. For locations the message is a google maps link to the sent location. For images the message can be empty or a blurb of text.
Message Type	Identifies the type of message sent. The possible types are Text, Sticker, Call, Video, Location, Notification, or Image.
Message Status	The status of the message. This can be one of the following: 'Sent / Failed', 'Sent / Not Delivered', 'Sent / Delivered', or 'Received'.
Secret Chat	Indicates whether a message is sent in a secret chat (Yes if true).
Expiration	If the message is a secret chat message, this value represents the time limit that the message can be visible for before it disappears. The value is converted from seconds and reported as a timestamp in dd hh:mm:ss format.
Repeat Count	If the message was a call, the number of times that call was repeated.
File Path	If the message included an attachment, the path to the attachment on the local phone, in the form of a URL.
Location Address	The address for the location that was sent.
Latitude	Map latitude location information.
Longitude	Map longitude location information.

WeChat Friends

Description	Stored contact info for the WeChat app on iOS.
Notes	

ATTRIBUTE	DESCRIPTION
Username	The unique username of the friend.
MD5 Hashed Username	The MD5 hash of the friend's username.
Nickname	Nickname of the friend.
Gender	Friend's gender.
Phone Number	Friend's phone number.
Email	Friend's email address.
Full Name	Friend's full name.

WeChat Messages

Description	Stored messages for the WeChat app on iOS.
Notes	

ATTRIBUTE	DESCRIPTION
Sender Username	The username or ID of the sender, as assigned by the application.
Sender Nickname	The display name of the sender, as defined by the user.
Recipient Username	The username of the person receiving the message.
Recipient Nickname	The nickname of the person receiving the message.
Group Chat Name	The name of the group chat, if the message is sent in a group chat.
Group Chat ID	The unique ID of the group chat, if the message is sent in a group chat.
Created Date/Time - UTC (yyyy-mm-dd)	The date/time that the message was created on the device.
Message	The content of the message.
Image	Image attachment associated with the message.
File	Non-image attachment (such as audio, video) associated with the message.
Call Duration (Seconds)	Duration of voice and/or video call in seconds.
Type	The type of the message, such as text, audio, video etc.
Latitude	Latitude part of location data sent within the message.
Longitude	Longitude part of location data sent within the message.
Attachment Path	Absolute path to attachment(s) associated with the message if any were recovered.

WhatsApp

WhatsApp is a cross-platform mobile messaging app that is owned by Facebook and has over a billion registered users as of 2016. Magnet tools support the recovery of messages, contacts, and attachments from WhatsApp conversations on both Android and iOS. Information from these artifacts can help investigators identify who a user communicates with and what they talk about. This information can be important to many different types of investigations.

Artifacts

RELATED RESOURCES

Artifact Profile: WhatsApp Messenger

iOS WhatsApp Chats

Description	WhatsApp Chats contains information about chat sessions that occur between the local user and another user or group. This artifact indicates the IDs of each participant as well as information about unread messages and the time when the last message was sent.
Notes	

ATTRIBUTE	DESCRIPTION
Individual Chat Name	If the chat is with an individual, this value indicates the name of the participant.
Group Chat Name	If the chat is a group chat, this value indicates the name of the group.
Chat ID	The id of the individual or group involved in the chat.
Unread Message Count	The number of unread messages in the chat.
Last Message	The text body of the last message sent in the chat.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time that the last message in the chat was sent.

iOS WhatsApp Contacts

Description	Contacts added to WhatsApp by the local user.

Notes	

ATTRIBUTE	DESCRIPTION
ID	The unique identifier for the contact.
Phone Number	The contact's phone number.
Full Name	The contact's full name.
Given Name	The contact's given (i.e. first) name.
Is WhatsApp User	Identifies whether the user is using WhatsApp or not. This is determined by checking the user's status and status updated date/time because a WhatsApp user cannot have a null status.

iOS WhatsApp Groups

Description	WhatsApp Groups contains information about the group chats that the user participates in.
Notes	

ATTRIBUTE	DESCRIPTION
Group Chat ID	The ID of the group chat.
Group Name	A display name of the group chat.
Creator ID	The ID of the group's creator.
Creator Name	The name of the group's creator.
Admin IDs	The IDs of the administrators of the group chat.
Admin Names	The names of the administrators of the group chat.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the group chat was created.
Group Member Name(s)	The names of the members in the group.
Group Member ID(s)	The IDs of the members of the group.

iOS WhatsApp Messages

Description	WhatsApp Messages contains information about the messages, media, and calls that are sent and received by the user.
Notes	

ATTRIBUTE	DESCRIPTION
Chat Type	Defines the audience for the message/call. 'Individual' indicates one-on-one messages/calls, 'Group' indicates that the message/call involves more than one user, and 'Broadcast' indicates a message with multiple recipients.
Sender	The sender of the message. This value can be a phone number, if the message is sent by an individual. If the message is recieved from a group or a broadcast message, this value can be a Whatsapp ID. 'Local User <Evidence Number>' is used if the sender is the local user. For messages received from a group chat, you can cross reference this value with the Group Chat ID attribute in iOS WhatsApp Groups to identify the group it was sent from.
Sender Nickname	The name associated with the sender in the database. No value is displayed for the local user.
Receiver	The message recipient. This value can be a phone number or a Whatsapp ID for group or broadcast messages. 'Local User <Evidence Number>' is used if the recipient is the local user.
Receiver Nickname	The name associated with the recipient in the database. No value is displayed for the local user.
Conversation ID	An ID for the conversation that the WhatsApp message is associated with. This value is used to compile messages into chat threads.
Message	The message text body. This field can also contain additional information about the content that is sent or received, such as picture captions, contact card information or calls status.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the message. May be sent or received time.
Message Direction	Whether the message is incoming or outgoing.
Message Status	The status of the message (Sent/Delivered/Read/Unsent)
Type	The type of message or call (Text, Picture, Video, Voice record, Document, Geo-location, Contact, Broadcast, Call not answered, GIF, Deleted message for everyone, Audio call, Video call, Unknown).
Duration	If the type is audio or video, the duration in seconds.
Image	The raw data for the picture attached to the message. The data is loaded from the local media path stored in the database, if the path exists.
Location Address	The address of the location attached to the message. This attribute is only populated if the sender shares their location.
File	The raw data for the file attached to the message. The data is loaded from the local media path stored in the database, if the path exists.
Media URL	The URL for media that's included with the message.
Local Media Path	The local media path stored in the database. By default, this is ZMEDIALOCALPATH from the database, but if it's not available, ZTHUMBNAILLOCALPATH is used instead.

ATTRIBUTE	DESCRIPTION
Latitude	Latitude of the location from which the message was sent. This attribute is only populated if the message has type Geo-location.
Longitude	Longitude of the location from which the message was sent. This attribute is only populated if the message has type Geo-location.
Starred	Indicates whether the user bookmarked (or 'starred') a message.
Forwarded	Indicates whether the user forwarded a message to another conversation

Wickr Me

Wickr Me is a private messaging application for iOS and Android, which provides end-to-end encryption of user communications, including texts, audio and video calls, transmitted locations and more. To ensure the security of your messages, Wickr Me encrypts every sent message with a unique key and gives you the option to control how long these messages will remain available to a recipient once read.

The content of a suspect’s sent and received messages can be valuable to an investigation, as well as their username and the usernames of their recipients. Other information can also be recovered, such as the date and time of when messages were sent, delivered and read, and a suspect's shared locations. This information can offer insight into the purpose of a suspect’s interactions, identify users who have been in contact with a suspect, and can be used to piece together a timeline of a suspect’s activity.

Decrypting messages

Some artifact fragments including message type, read status, timestamps and more, can be viewed without decryption. To access encrypted Wickr Me application data, you will need to provide a key from the target device keychain, or the Wickr Me account password. A common way of obtaining the key is by recovering it from the keychain.plist file that GrayKey generates during an acquisition. To decrypt the application data, add the key to AXIOM Process when you set up your search.

Artifacts

Wickr Me Messages

Related Resources

Decrypt app data using the iOS Keychain and GrayKey

Recover the device keychain

Wickr Me Messages - iOS

Description	Wickr Me Messages contains decrypted and decoded messages sent or received by a Wickr Me user on iOS. These messages can include text messages, call logs, transmitted locations, attachments such as pictures and videos, voice messages, and more.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender's Wickr username.
Recipient(s)	The recipient's Wickr username.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time, in UTC, when this message was sent.
Message Type	The message type. This value is interpreted from the ZPRIMARYTYPE. Values can be: Text, Call, Attachment, Location, Key Verification, or Control (Group Conversation Events).
Message	The message content.
Direction	Indicates whether the message was incoming or outgoing.
Read	Indicates whether or not the message was read.
Call Status	The status of the call, if applicable (Started, Completed, Missed, Cancelled)
Attachment Name	The file name of the attachment included in the message, if applicable.
Attachment Path	The original file path of the encrypted attachment, if applicable.
Attachment	The decrypted attachment file, if applicable (can include photos, video or voice messages).
Latitude	The latitude of the coordinates (for transmitted locations only).
Longitude	The longitude of the coordinates (for transmitted locations only).

Zalo Contacts

Description	The user's Zalo contacts.
Notes	The Last Activity, Is Friend, and Type columns are empty for iOS.

ATTRIBUTE	DESCRIPTION
User Name	The contact's username.
User ID	The contact's unique user ID.
Profile Picture URL	The contact's profile picture URL.
Gender	The contact's gender.
Phone Number	The contact's phone number.

ATTRIBUTE	DESCRIPTION
Birthday (yyyy-mm-dd)	The contact's phone number.
Status	The contact's status message.
Last Activity Date/Time - UTC (yyyy-mm-dd)	The date/time of when the contact was last active.
Is Friend	If the contact is friends with the user.
Type	The contact's type of account.

Zalo Groups

Description	Zalo groups that the user participates in.
Notes	

ATTRIBUTE	DESCRIPTION
Name	Name of the group.
ID	Unique ID of the chat group.
Created By	The user name of the person who created the chat room.
Group Members	The user names of all the members in the group.
Number of Participants	Number of participants in the group.

Zalo Messages

Description	Messages or calls sent or received using Zalo.
Notes	

ATTRIBUTE	DESCRIPTION
Sender User Name	User name of the person sending the message.
Recipient User Name	User name of the person receiving the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date/time that the message was sent on the device.
Direction	The direction the message is being sent.
Message	The content of the message.
Picture	Picture attachment in the message.
Attachment	Non-picture attachments in the message (for example, audio or video).
Duration (Seconds)	Duration of calls.
Status	Status of calls.
Message Type	The type of the message, for example, text, audio, video etc.

ATTRIBUTE	DESCRIPTION
Latitude	The latitude data sent within a message.
Longitude	The longitude data sent within a message.
Media URL	The URL of additional media attachments.
Attachment Path	Absolute path to recovered attachments in a message.

Zalo Profiles

Description	Profile information for the local Zalo user.
Notes	On iOS devices, the value on the Birthday column is 12 hours behind the actual value. Report Viewer displays this as a 12 hour difference, but because Examine doesn't display hours for a birthday, the value appears as the previous day.

ATTRIBUTE	DESCRIPTION
User Name	The user's username.
User ID	The user's unique user ID.
Profile Picture URL	The user's profile picture URL.
Gender	The user's gender.
Birthday (yyyy-mm-dd)	The user's birthday.
Phone Number	The user's phone number.
Status	The user's status message.

Zoom Channels

Description	Zoom Channels contains information about the channels that the local user participates in.
Notes	

ATTRIBUTE	DESCRIPTION
Channel ID	The ID of the channel.
Channel Name	The display name of the channel.
Owner ID	The ID of the Zoom user that created the channel.
Participant IDs	The IDs of the participants of the channel.
Participant User Names	The names of the participants of the channel.
Description	A description of the channel, as provided by the creator of the channel.

Zoom Chat Messages

Description	Contains details about Zoom chat messages sent outside of a meeting.
Notes	The Attachment Name column is always empty on iOS.

ATTRIBUTE	DESCRIPTION
Sender Name	The name of the person who sent the message.
Sender ID	The ID of the person who sent the message.
Buddy ID	The ID of the person or group that the message was sent to.
Recipient Name	The name of the person who received the message.
Recipient ID	The ID of the person who received the message.
Group Chat ID	The ID of the group this message was sent in.
Message ID	The GUID of the message.
Message	The body of the message.
Message Date/Time - UTC (yyyy-mm-dd)	A timestamp that indicates when the message is sent or received, depending on whether the local user is the sender or receiver.
Sender	Whether the message was sent by the local user, or a remote user. Can be 'Local User' or 'Remote User'.
Read	Specifies whether the message has been read ('Yes' or 'No').
Message Type	The type of message that was sent. Can be 'Message', 'Picture', 'File', or 'Notification'.
Attachment Name	The name of the attachment that was sent.
Attachment Local File Path	The local path where the attachment was saved. This is empty if the attachment was not saved.
Attachment	The contents of the attachment if it can be recovered.

Zoom Contacts

Description	Zoom Contacts contains information about a user's Zoom contacts.
Notes	

ATTRIBUTE	DESCRIPTION
Buddy ID	The user ID of contact.
Email	The email address of contact.
Display Name	The display name of contact.
Description	A description of the contact, as provided by that user.

ATTRIBUTE	DESCRIPTION
Personal Meeting ID	An ID that can be used to start up a meeting with the contact.
Region	The default country or region where the contact is located

Zoom Meeting Messages

Description	Contains details about Zoom chat messages sent during a meeting.
Notes	

ATTRIBUTE	DESCRIPTION
Message ID	The GUID of the message.
Sender Name	The name of the person who sent the message.
Sender ID	The ID of the person who sent the message.
Receiver Name	The name of the person who received the message. If blank, the message was sent to everyone in the meeting.
Receiver ID	The ID of the person who received the message. If zero, the message was sent to everyone in the meeting.
Message	The body of the message.
Message Date/Time - UTC (yyyy-mm-dd)	A timestamp that indicates when the message is sent or received, depending on whether the local user is the sender or receiver.
Sender	Whether the message was sent by the local user, or a remote user. Can be 'Local User' or 'Remote User'.
Read	Specifies whether the message has been read ('Yes' or 'No').
Message Type	The type of message that was sent.
Conference ID	The ID for the meeting the message was sent in.

Zoom User Accounts

Description	Contains details about the local user's zoom account.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The unique identifier for the user.
User Name	The account's user name.
Email	The email address associated with the account.
First Name	The user's first name.

ATTRIBUTE	DESCRIPTION
Last Name	The user's last name.
Phone Number	The user's phone number.
Profile Image URL	The URL to the user's profile picture.
Downloaded Profile Image	The data for the profile picture.

Cloud

iOS Dropbox

Description	Information from the iOS Dropbox Database regarding the cached files.
Notes	

ATTRIBUTE	DESCRIPTION
Dropbox File Path	The relative path to the file in the Dropbox application.
Account ID	The ID number associated with the account.
Last Viewed Date/Time - UTC (yyyy-mm-dd)	The Date/Time that the file was last viewed.
Client Modified Date/Time - UTC (yyyy-mm-dd)	The Date/Time that the file was last modified on the client.
Modified Date/Time - UTC (yyyy-mm-dd)	The Date/Time that the file was last modified.
Size (Bytes)	The size of the file in bytes.
View Count	The number of times the file has been viewed.
Favorite	Whether or not the file has been favorited ('yes' or 'no').
Revision Number	The revision number for the file.
Local File Path	The local path on the disk to where the cached file was found.
Image	The image data for the file.

iOS Dropbox Carved

Description	File information from the iOS Dropbox app.
Notes	

ATTRIBUTE	DESCRIPTION
File Path	Path at which the file was stored, relative to the Dropbox folder.
Size (Bytes)	Size of the file in bytes.

ATTRIBUTE	DESCRIPTION
View Count	Number of times the file was viewed.
Last Viewed Date/Time - UTC (yyyy-mm-dd)	The Date/Time at which the file was last viewed.
Client Modified Date/Time - UTC (yyyy-mm-dd)	The Date/Time at which the local client last modified the file.
Modified Date/Time - UTC (yyyy-mm-dd)	The Date/Time at which the file was last modified.
Favourite	Whether or not the file is marked as a favourite.
Revision Number	The revision number of the file.
Image	The raw image content of the file.

Cloud Storage

MEGA Accounts

Description	MEGA Accounts contains information about the accounts that the local user has logged in with on the device.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user ID of the local user.
Email Address	The email address of the local user.
First Name	The first name of the local user.
Last Name	The last name of the local user.
Summary	A summary of the the local user.

MEGA Chat

Description	MEGA Chat contains messages sent and received by the local user.
Notes	

ATTRIBUTE	DESCRIPTION
Sender ID	The id of the sender.
Sender Email	The email address of the sender.
Sent Date/Time	The date and time the message was sent.
Message Body	The body of the message.

ATTRIBUTE	DESCRIPTION
Recipient ID(s)	The user ID(s) of the recipient(s).
Recipient Email(s)	The email addresses of the recipients of the message.
Message Type	The type of the message.
Attachment Name	The file name of attachment to the message.

MEGA Contacts

Description	MEGA Contacts contains information about MEGA users that have communicated with the local user account.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user ID of the contact.
Email Address	The email address of the contact.
First Name	The first name of the contact.
Last Name	The last name of the contact.

Documents

Evernote Accounts

Description	Evernote Accounts contains information about the user accounts that have been used to log in on the device.
Notes	

ATTRIBUTE	DESCRIPTION
Local User Display Name	The display name of local user's account.
User ID	The user ID of local user.
Created Date/Time	The date and time when this account was created.
Login Date/Time	The date and time that the account was initially logged in on the device.

Evernote Contacts

Description	Evernote Contacts contains information about users that have communicated with the local user account.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user ID of the contact.
Contact ID	The contact ID of the contact.
Account Name	The account Name of the contact.

Evernote Notes

Description	Evernote Notes contains any notes associated with the local user, including notes shared from other users to the local user.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the note.
Content	The content of the note.
Type	The type of note.
File Name	The name of the attachment that was included with the note.
Created Date/Time	The date and time when the note was created.
Updated Date/Time	The date and time when the note was updated.
Deleted Date/Time	The date and time when the note was deleted.
Owner	The owner of the note. If a note is shared from one user to another, the owner is the user that shared the note.
Shared With	The accounts the note was shared with.
Last Modifier Name	The user name of the last modifier of the note.
Start Date/Time	The date and time of the starting time for the reminder of the note.
End Date/Time	The date and time of the end time for the reminder of the note.
Location	The location where the note was taken.
Longitude	The Longitude of the location where the note was taken.

ATTRIBUTE	DESCRIPTION
Latitude	The Latitude of the location where the note was taken.
Notebook Name	The name of the notebook where the note was saved.

Evernote Work Chat

Description	Evernote Work Chat contains messages sent and received by the local user.
Notes	

ATTRIBUTE	DESCRIPTION
Sender ID	The unique ID of the sender.
Sender Name	The name of the sender
Sent Date/Time	The date and time when the message was sent.
Message Body	The body of the message.
Participants	The participants of the chat.
Participant IDs	The participant IDs of the chat.

Excel Documents

Description	Microsoft Excel is a spreadsheet processor developed by Microsoft.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified on the filesystem.
Size (Bytes)	The size of the document in bytes.
Saved Size (Bytes)	The size of the document (in bytes) that was recovered. Extremely large documents may not be fully recovered.
File	The actual file.
Title	The title meta-data.
Subject	The subject meta-data.

ATTRIBUTE	DESCRIPTION
Authors	The authors of the document.
Keywords	The keywords meta-data in the document.
Comments	The comments meta-data.
Last Author	The last author to edit the document.
Last printed Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last printed, extracted from meta-data within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last modified, extracted from meta-data within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the document was created, extracted from meta-data within the document.
Company	The company meta-data.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

PDF Documents

Description	Portable Document Format (PDF) is a file format used to present documents in a manner independent of application software, hardware, and operating systems. This table captures documents in this file format, extracted from the filesystem and carved from unallocated space.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified on the filesystem.
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
Title	The title of the file.
Subject	The subject of the file.
Authors	The authors of the file.
Keywords	The keywords in the metadata of the file.

ATTRIBUTE	DESCRIPTION
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the document was created, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last modified, extracted from metadata within the document.
File	The PDF file.
MD5 Hash	An MD5 hash of the PDF content.
SHA1 Hash	A SHA1 hash of the PDF content.

PowerPoint Documents

Description	Micrsoft PowerPoint is a presentation creator developed by Microsoft. This table captures documents created with PowerPoint, extracted from the filesystem and carved from unallocated space.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified on the filesystem.
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
File	The actual file.
Title	The title of the file.
Subject	The subject of the file.
Authors	The authors of the file.
Keywords	The keywords in the metadata of the file.
Comments	The comments in the metadata of the file.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last modified, extracted from metadata within the document.

ATTRIBUTE	DESCRIPTION
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the document was created, extracted from metadata within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

RTF Documents

Description	The information for each RTF document that was recovered from the search.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the RTF document.
File Size (Bytes)	The size of the RTF document in bytes.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the RTF document was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the RTF document was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the RTF document was last modified.
File Content	The contents of the RTF document.

Text Documents

Description	Text documents (.txt) that are located on the system.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the text document.
Size (Bytes)	The size of the text document in bytes.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The Date/Time that the text document was last modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The Date/Time that the text document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The Date/Time that the text document was created.

Word Documents

Description	Microsoft Word is a word processor developed by Microsoft.

Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified on the filesystem.
Size (bytes)	The size of the document.
Saved Size (bytes)	The size of the document that was recovered. Extremely large documents may not be fully recovered.
File	The actual file.
Title	The title meta-data.
Subject	The subject meta-data.
Authors	The authors of the document.
Keywords	The keywords meta-data in the document.
Comments	The comments meta-data.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last printed extracted from meta-data within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last modified, extracted from meta-data within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the document was created, extracted from meta-data within the document.
Company	The company meta-data.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

E-mail

Apple Mail

Description	Contains the emails that have been extracted from an iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Subject	The subject of the email.
To	Who the email was sent to.
CC	Who was CC'd on the email.
BCC	Who was BCC'd on the email.
Sender	Who sent the email.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the email was sent.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time the email was received.
Email Body	The body of the email.
Summary	A summary of the email.
Size	The size of the email.
Mailbox	The mailbox the email is in.
Read	States whether or not the email has been read.
Deleted	States whether or not the email has been deleted.

Apple Mail Fragments

Description	Contains the fragments of emails that have been extracted from an iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	Who sent the email
To	Who the email was sent to
CC	Who was CC'd on the email
BCC	Who was BCC'd on the email
Subject	The subject of the email
Body	The body of the email
Date/Time - UTC (yyyy-mm-dd)	The date of the email. This field can mean different things to different programs, so we have not defined what this column actually means
Header	The headers that are sent with the email
Importance	The importance of the email, set by the sender
Attachment Name (s)	The name of the attachments sent with the email. The names are not always Windows safe paths

Gmail Emails

Description	Contains the Gmail email fragments that were recovered from an Android device.
Notes	

ATTRIBUTE	DESCRIPTION
To Address(es)	The recipient(s) of the email.
From Address	The sender of the email.
Thread ID	The ID of the conversation the email is from. Emails with the same Thread ID belong to the same conversation.
Subject	The subject of the email.
Sent Date/Time - UTC (yyyy-mm-dd)	The date the email was sent.
Received Date/Time - UTC (yyyy-mm-dd)	The time the email was received.
Email Body	The body of the email.
Email Snippet	A snippet of the email.
cc Address(es)	The recipients of the email that were CC'd.
bcc Address(es)	The recipients of the email that were BCC'd.
Reply Address(es)	Reply-to address for the email.

iOS Yahoo Mail Contacts

Description	Contact details for local user accounts in iOS Yahoo Mail app.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Email	Email address of the local account.
Contact Email	Email address of the contact.
Contact Display Name	Display name of the contact. Note: The Yahoo Mail app may sometimes erroneously store the Contact Email in this column.
Contact Family Name	Family name of the contact.
Contact Family Name Sound	User-specified pronunciation guide for the contact's family name. Note: The Yahoo Mail app may sometimes erroneously store the Contact Family Name in this column.
Contact Given Name	Given name of the contact.

ATTRIBUTE	DESCRIPTION
Contact Given Name Sound	User-specified pronunciation guide for the contact's given name. Note: The Yahoo Mail app may sometimes erroneously store the Contact Given Name in this column.
Contact Middle Name	Middle name of the contact.

iOS Yahoo Mail Messages

Description	Emails stored by iOS Yahoo Mail app.
Notes	

ATTRIBUTE	DESCRIPTION
Account	Email address of the local account.
Sender	Email address or username of the sender.
Recipient	Email address or username of the recipient(s)in the 'To' field.
CC	Email address or username of the recipient(s)in the 'Cc' field.
BCC	Email address or username of the recipient(s)in the 'Bcc' field.
Subject	The subject line of the email.
Snippet	A short preview of the text of the email body.
HTML Body	The email body, in HTML format.
Content Type	The content type of the email body, in MIME format.
Folder	The name of the folder in which this email is stored.
Received Date/Time - UTC (yyyy-mm-dd)	The Date/Time at which the email was received.
Read	Yes/No, whether the email has been read.
Replied	Yes/No, whether the local account has replied to this email.
Forwarded	Yes/No, whether the local account has forwarded this email.
Flagged	Yes/No, whether the email has been flagged.
Erased	Yes/No, whether the email has been erased.
Draft	Yes/No, whether the email is a draft.
Attachment Name(s)	List of file names of the attachments on this email, if any.

iOS Yahoo Mail User Accounts

Description	Local user accounts for iOS Yahoo Mail app.
Notes	

ATTRIBUTE	DESCRIPTION
Email	Email address of the user account.
User	User ID of the user account.
Name	Full name of the user.
First Name	First name of the user.
Last Name	Last name of the user.

Outlook Appointments

Description	Microsoft Outlook is a personal information manager and email client. This table captures information related to appointments scheduled in Outlook.
Notes	

ATTRIBUTE	DESCRIPTION
Sender Name	The person who requested the appointment
Sender Exchange Account	The sender's Exchange account name
Recipients	The recipients of the appointment invitation
Subject	The subject of the appointment
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the appointment starts
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the appointment ends
Body	The body of the appointment description
Recipients CC	The CC'd recipients of the appointment invitation
Recipients BCC	The BCC'd recipients of the appointment invitation
Companies	The companies involved in the appointment
Attachments	The attachments for the appointment
Location	The location of the appointment
Is All-Day Event	Indicates if the appointment is an all-day event
Is Recurring	Indicates if the appointment is recurring
Recurrence Pattern Description	Describes the recurrence pattern of the appointment, if applicable
Sensitivity	Indicates if the appointment is sensitive
Is Hidden	Indicates if the appointment is hidden
Is Private	Indicates if the appointment is private
Priority	The priority of the appointment
Importance	The appointment importance setting

Outlook Contacts

Description	Microsoft Outlook is a personal information manager and email client. This table captures information related to contacts stored in Outlook.
Notes	

ATTRIBUTE	DESCRIPTION
Display Name	The contact's display name
Customer ID	The customer ID of the contact
Email Address 1	The contact's primary email address
Email Display As 1	The display string of the contact's primary email address
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the contact details were last modified
Company Name	The contact's company name
Department Name	The contact's department name
Title	The contact's job title
Profession	The contact's profession
Manager Name	The name of the contact's manager
Office Location	The contact's office location
Business Address	The physical address of the business
Business Phone	The contact's business phone number
Business Phone 2	The contact's secondary business phone number
Business Fax	The contact's business fax number
Business Homepage	The website of the contact's business
Email Display Name 1	The display name of the contact's primary email address
Email Address 2	The contact's secondary email address
Email Display As 2	The display string of the contact's secondary email address
Email Display Name 2	The display name of the contact's secondary email address
Email Address 3	The contact's tertiary email address
Email Display As 3	The display string of the contact's tertiary email address
Email Display Name 3	The display name of the contact's tertiary email address
Cellular Phone	The contact's mobile phone number
Home Address	The contact's home address
Home Phone	The contact's home phone number
Home Phone 2	The contact's secondary home phone number
Home Fax	The contact's home fax number
FTP Site	The contact's FTP site
Body	More information about the contact

ATTRIBUTE	DESCRIPTION
Attachments	Any attachments to the contact entry
Last Modifier Name	The name of the person who last modified the contact details

Outlook Messages

Description	Microsft Outlook is a personal information manager and email client. This table captures information related to emails sent and received in Outlook.
Notes	

ATTRIBUTE	DESCRIPTION
Sender Name	The sender of the email
Sender Email	The email address of the sender
Recipients	The recipients of the email
Subject	The subject of the email
Sender Exchange Account	The sender's Exchange account name
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the email was created
Delivery Date/Time - UTC (yyyy-mm-dd)	The date and time the email was delivered
Body	The body of the email
Folder Name	The name of the folder where the email is stored
CC	The recipients of the email that were CC'd
BCC	The recipients of the email that were BCC'd
Attachments	The list of attachments on the email
Headers	The raw email headers
Priority	The priority of the email
Importance	The importance of the email
Sensitivity	The sensitivity of the email

Encryption

Best Secret Folder Albums

Description	Best Secret Folder Albums contains information on the albums the user has created in the application.
Notes	

ATTRIBUTE	DESCRIPTION
Album Title	The title of the Album.
Created Date/Time - Local Time (yyyy-mm-dd)	The date/time when the album was created in local time.
Created Date/Time - UTC (yyyy-mm-dd)	The date/time when the album was created in UTC.
User ID	The username assigned to the folder by the application. This is either 'OtherUser', indicating a user without access, or 'VideoSafeValidUser' indicating a user with passcode access.
Type	The type of album (i.e. Photo, File or Video).

Best Secret Folder Configuration Data

Description	Best Secret Folder Configuration Data contains information about the configuration of the app, including the locations where hidden media is stored.
Notes	

ATTRIBUTE	DESCRIPTION
Password	The password used to access the app.
Password Hint	The hint for the password.
Root Notes Folder	The root folder in which all the user's notes are stored.
Root Photos Folder	The root folder in which all the user's photos are stored.
Root Videos Folder	The root folder in which all the user's videos are stored.

Best Secret Folder Media

Description	Best Secret Folder Media contains information about the media files that the user has added in the application.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the media file.
File Type	The type of the media file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the media was added in UTC.

ATTRIBUTE	DESCRIPTION
Created Date/Time - Local Time (yyyy-mm-dd)	The date and time when the media was added in local time.
Album Title	The title of the album.
User ID	The username assigned to the folder by the application. This is either 'OtherUser', indicating a user without access, or 'VideoSafeValidUser', indicating a user with passcode access.

Internet of Things

Amazon Alexa Audio Activity

Description	Contains details about audio activity detected by the Amazon Alexa app.
Notes	The data in this artifact is retrieved from the app's cached data and may not represent a complete record of the user's activities. Accessing the web resource URL requires the user's Alexa login credentials.

ATTRIBUTE	DESCRIPTION
Text	The spoken audio as interpreted by the Alexa app.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the audio was recorded.
Resource URL	The web resource URL for the audio file.

Amazon Alexa Device Information

Description	Contains details about Alexa-enabled devices.
Notes	The data in this artifact is retrieved from the app's cached data and may not represent a complete record of the user's activities.

ATTRIBUTE	DESCRIPTION
Device Name	The name of the device.
Customer ID	The Amazon customer identifier.
Device Type	The type of device.
Serial Number	The serial number of the device.
MAC Address	The MAC address of the device.
Network Name (SSID)	The network name to which the device is connected.

ATTRIBUTE	DESCRIPTION
ZIP / Postal Code	The ZIP or postal code associated with the device.

Amazon Alexa Tasks

Description	Contains details about shopping lists or other tasks tracked by the Amazon Alexa app.
Notes	Accessing the audio resource URL requires the user's Alexa login credentials.

ATTRIBUTE	DESCRIPTION
Text	The spoken task as interpreted by the Alexa app.
Type	The type of task.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the task was last updated.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the task was created.
Customer ID	The customer ID of the task creator.
Completed	Whether the task has been completed.
Deleted	Whether the task has been deleted.
Similar Text	Text that's similar to the text for the task, as determined by the Alexa app.
Resource URL	The web resource URL for the audio file.

Amazon Alexa User

Description	Contains details about user accounts recognized by the Amazon Alexa app.
Notes	The data in this artifact is retrieved from the app's cached data and may not represent a complete record of the user's activities.

ATTRIBUTE	DESCRIPTION
User Name	The user name for the account.
Email	The email associated with the account.
Device Name	The name of the device.
Customer ID	The Amazon customer identifier.

Amazon Alexa Web Resource

Description	Contains details about Amazon API resources contacted by the Alexa app.
Notes	The data in this artifact is retrieved from the app's cached data and may not represent a complete record of the user's activities. Accessing the web resource URL requires the user's Alexa login credentials.

ATTRIBUTE	DESCRIPTION
Resource URL	The URL for the web resource.
Type	The type of data available from the resource.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the resource request was made.

Apple Health Distance

Description	Apple Health Distances specifies the distances traveled during activities that were tracked by the iOS device. This data could be synced from another device, such as an Apple Watch. Data about the distance, steps, floors and heart rate of a user can be particularly useful as it provides a look at a user's activity level at any given time.
Notes	

ATTRIBUTE	DESCRIPTION
Distance (meters)	The distance of walking or running, in meters.
Start Date/Time	The date and time this activity started.
End Date/Time	The date and time this activity ended.
Duration (Minutes)	The duration of the activity, in minutes.
Model ID	The model ID of the device where the data synced from.

Apple Health Floors

Description	Apple Health Floors specifies the number of floors climbed during activities that were tracked by the iOS device. This data could be synced from another device, such as an Apple Watch. Data about the distance, steps, floors and heart rate of a user can be particularly useful as it provides a look at a user's activity level at any given time.
Notes	

ATTRIBUTE	DESCRIPTION
Floors	The floors climbed.
Start Date/Time	The date and time this activity started.
End Date/Time	The date and time this activity ended.
Model ID	The model ID of the device where the data synced from.

Apple Health Heart Rate

Description	Apple Health Heart Rate specifies the average heart rate during activities that were tracked by the iOS device, which will be synced from an Apple Watch. Data about the distance, steps, floors and heart rate of a user can be particularly useful as it provides a look at a user's activity level at any given time.
Notes	

ATTRIBUTE	DESCRIPTION
Heart Rate	The average heart rate during the activity rounded to the first decimal place.
Start Date/Time	The date and time that the activity started.
End Date/Time	The date and time that the activity ended.
Unit	The unit used to measure the heart rate.
Model ID	The model ID of the device where the data synced from. This may not be available since the data is synced from an Apple Watch.

Apple Health Steps

Description	Apple Health Steps specifies the number of steps taken during activities that were tracked by the iOS device. This data could be synced from another device, such as an Apple Watch. Data about the distance, steps, floors and heart rate of a user can be particularly useful as it provides a look at a user's activity level at any given time.
Notes	

ATTRIBUTE	DESCRIPTION
Steps Taken	The total number of steps taken during the activity.
Start Date/Time	The date and time this activity started.
End Date/Time	The date and time this activity ended.
Duration (Minutes)	The duration of the activity, in minutes.

ATTRIBUTE	DESCRIPTION
Model ID	The model ID of the device where the data synced from.

Fitbit Activity Log

Description	Specifies the activities that were tracked by the Fitbit.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user ID of the associated user profile.
Type	The type of physical activity.
Start Date/Time - UTC (yyyy-mm-dd)	The start date and time of the average heart rate calculation.
End Date/Time - UTC (yyyy-mm-dd)	The end date and time of the average heart rate calculation.
Average Heart Rate (BPM)	The average heart rate.
Steps Taken	The total number of steps taken during the activity.
Distance (Kilometers)	The total distance travelled during the activity.
Duration (Seconds)	The duration of the activity.

Fitbit Floors

Description	Analyzing this data can help identify the number of floors a user has traveled within a day.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user ID of the associated user profile.
Date	The date that the floor-traveling data was generated.
Floors	The number of floors traveled.

Fitbit Profiles

Description	Specifies information from the Fitbit profiles that the user has set up on the device.
Notes	The Birthday (yyyy-mm-dd) column is always null for iOS devices.

ATTRIBUTE	DESCRIPTION
User ID	The user ID of the associated user profile.
Full Name	The first and last name of the person associated with the profile.
Birthday (yyyy-mm-dd)	The birthday of the person associated with the profile.
Profile Image URL	The location of the profile image.
Height (cm)	The height of the person in centimeters.
Gender	The gender of the person.
Walking Stride Length (cm)	The walking stride length of the person in centimeters.
Running Stride Length (cm)	The running stride length of the person in centimeters.
Current Timezone Offset (Minutes)	The timezone offset from GMT, in minutes. This value represents the timezone specified in the user's profile, and does not necessarily represent the user's current location.
Country	The country the profile user may be in.

Fitbit Sleep

Description	Contains information about the user's sleep patterns.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user ID of the associated user profile.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the person went to bed.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the person got out of bed.
Time In Bed (Minutes)	The total time in minutes that the person was in bed (awake and asleep).
Time Awake (Minutes)	The total time in minutes that the person was awake in bed.
Time Asleep (Minutes)	The total time in minutes that the person was asleep.

Fitbit Steps

Description	Specifies information about the number of steps a person takes while wearing the Fitbit. Steps are aggregated for a 60 minute interval and then stored.

Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user ID of the associated user profile.
Start Date/Time - UTC (yyyy-mm-dd)	The start date and time of the accumulated steps.
End Date/Time - UTC (yyyy-mm-dd)	The end date and time of the accumulated steps.
Steps Taken	The accumulated steps taken.

Nest Location Configuration

Description	Contains configuration and settings related to the structure housing the Nest system.
Notes	

ATTRIBUTE	DESCRIPTION
Location Name	The name of the location.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the location configuration was created.
City	The local city.
State / Province	The local state or province.
Country Code	The local country code.
ZIP / Postal Code	The local ZIP or postal code.
Latitude	The local latitude.
Longitude	The local longitude.
Structure Area (Square Meters)	The floor size of the structure, in square meters.
Emergency Contact Description	The description of the emergency contact.
Emergency Contact Phone	The phone number for the emergency contact.

Nest Temperature Adjustment

Description	Contains details about thermostat temperature adjustments made through the Nest app.
Notes	

ATTRIBUTE	DESCRIPTION
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the adjustment was made.
User ID	The identifier for the user.
Temperature (Celsius)	The temperature setting.

ATTRIBUTE	DESCRIPTION
Scheduled Time (Local)	The local time of day at which the temperature adjustment is to take effect.
Scheduled Day	The day of the week at which the temperature adjustment is to take effect.

Nest User

Description	Contains details about Nest user accounts.
Notes	

ATTRIBUTE	DESCRIPTION
Email	The user's email.
Name	The user's name.
User ID	The user identifier.
Device Location	The location of the primary Nest device.
Profile Image URL	The URL for the user's profile image.

Pebble Activity Information

Description	Specifies the physical activities that were tracked by the Pebble watch.
Notes	

ATTRIBUTE	DESCRIPTION
Start Date/Time - UTC (yyyy-mm-dd)	The start date and time of the activity.
End Date/Time - UTC (yyyy-mm-dd)	The end date and time of the activity.
Duration (Seconds)	The duration of the activity.
Steps Taken	The total number of steps taken during the activity.
Active Calories (Cal)	The number of calories being burned during the activity.
Serial Number	The serial number of the Pebble watch used to track the activity.

Pebble Calendar Events

Description	Calendar events that are displayed on the Pebble Watch Timeline.

Notes	The Organizer Name, Owner Account, Created Date/Time, Updated Date/Time, Calendar Account, Attendees, Is Recurring, Organizer columns are always null for iOS devices.

ATTRIBUTE	DESCRIPTION
Title	The title of the calendar event.
Description	A short description of the calendar event.
Location	The location of the event.
Calendar Display Name	The display name of the calendar to which the event belongs.
Start Date/Time - UTC (yyyy-mm-dd)	The start date/time of the event.
End Date/Time - UTC (yyyy-mm-dd)	The end date/time of the event.
Organizer Name	The organizer of the event.
Calendar Account	The calendar to which the event belongs.
Created Date/Time - UTC (yyyy-mm-dd)	The date/time the event was created on the Pebble application.
Updated Date/Time - UTC (yyyy-mm-dd)	The date/time the event was updated.
User Account	The user account observing the event.
Attendees	The number of attendees to the event.
Is Recurring	Whether the event is recurring.
Organizer	Whether the user is the organizer of the event.

Pebble Physical Characteristics

Description	Specifies the user's activity profile information.
Notes	

ATTRIBUTE	DESCRIPTION
Gender	The gender of the user.
Age	The age of the user.
Height (cm)	The height of the user in centimeters.
Weight (kg)	The weight of the user in kilograms.

Pebble Steps

Description	Specifies the steps information tracked by the Pebble smart watch.
Notes	

ATTRIBUTE	DESCRIPTION
Start Date/Time - UTC (yyyy-mm-dd)	The start date/time of the steps occurance.
Steps Taken	The number of steps taken during a one minute duration from the start time.
Active Calories (Cal)	The number of active calories burned in the one minute.

Pebble Weather Locations

Description	Contains location information that's tracked by the Pebble Watch.
Notes	The latitude and longitude are not a precise values, but they can place the Pebble Watch in a specific city.

ATTRIBUTE	DESCRIPTION
Location Name	The name of the tracked location.
Latitude	The latitude of the location.
Longitude	The longitude of the location.
Created Date/Time - UTC (yyyy-mm-dd)	The date/time of the location data.
Updated Date/Time - UTC (yyyy-mm-dd)	The updated date/time of the location data.

Media

'Private Photo Vault Media

Description	Private Photo Vault Media contains information about encrypted media files that the user stores in the Private Photo Vault application. If decryption is successful, the decrypted media content is made available in this artifact. Metadata about the encrypted media files, such as timestamps, are always available. Users will often resort to encrypted media applications for storing illicit material. Being able to decrypt this media can be crucial to a case.
Notes	

ATTRIBUTE	DESCRIPTION
File Path	The path to the encrypted media file.
Media Type	The type of media (photo, video, or live photo).
Album Title	The associated album title.

ATTRIBUTE	DESCRIPTION
Created date and time - UTC (yyyy-mm-dd)	The date and time when the media was created on the device.
Last Modified date and time - UTC (yyyy-mm-dd)	The date and time when the album was modified on the device.
Thumbnail Path	The path to the encrypted thumbnail media file

AMR Files

Description	AMR files used for voicemail on both iOS and Android.
Notes	

ATTRIBUTE	DESCRIPTION
Audio	The contents of an AMR file.

Audio

Description	Audio files that are recovered that use the .mp3 or .wav formats.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
File Name	Name of the file.
File Extension	Extension of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the audio file was created.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the audio file was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the audio file was last modified.
File Size (Bytes)	The size of the audio file.
MD5 Hash	An MD5 hash of the audio content.
SHA1 Hash	A SHA1 hash of the audio content.

Carved Video

Description	Videos that are recovered using carving. Supported formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. Other container formats can also be recovered provided that their underlying packets are the same as one of the supported formats.

Notes	As of February 20 2020, this artifact will no longer be included under Videos. Carved Video functionality will be included in the 'Videos' artifact instead.

ATTRIBUTE	DESCRIPTION
Content Format	The format of the video.
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
File Size (Bytes)	The size of the container and file.
Container Format	The format of the video container.
Saved Video Size (Bytes)	The size of the video that was saved to the database.
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.

iOS Snapchat Conversations

Description	iOS Snapchat Conversations contain information about all the chats recovered from the local device.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The unique ID for the local user.
Chat ID	A unique ID for the conversation.
Participants	A list of participants that belong to the conversation.
Last Sent Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time in which a message was last sent.

iOS Snapchat My Story

Description	iOS Snapchat My Story contains information about a collection of Snaps which can exist for a 24 hour period.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The unique ID for the local user.
Posted Date/Time - UTC (yyyy-mm-dd)	The Date/Time when the Snapchat Story was originally created.

ATTRIBUTE	DESCRIPTION
Expiration Date/Time - UTC (yyyy-mm-dd)	The Date/Time the Snapchat Story expires and will be automatically deleted.
URL	The URL for the local user's Snapchat Story.

Live Photos

Description	Live Photos retrieved using parsing. Supports all Ios versions
Notes	

ATTRIBUTE	DESCRIPTION
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
UUID	The id of the picture and video. If the uuid is different for picture and a video, it is not associated with each other
Created Date/Time - UTC (yyyy-mm-dd)	The created date/time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date/time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date/time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.

ATTRIBUTE	DESCRIPTION
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. "Complete" indicates that a full Exif extraction was performed. "Failed" indicates that the information may have been corrupted and could not be recovered. "Skipped" indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
GPS Longitude	The GPS longitude coordinates of where the picture was taken (extracted from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
GPS Latitude	The GPS Latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS Latitude (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the pciture was taken (extracted from Exif data).
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

Photos Albums

Description	Photos Albums contains information about the albums that contain pictures and media in the Photos app on iOS.
Notes	

ATTRIBUTE	DESCRIPTION
Album Title	The title of the album.
Created Date/Time	The date/time when the album was created on the local device.
Photo Count	The number of photos in the album.
Video Count	The number of videos in the album.
UUID	The UUID of the album.
Owner Name	The full name of the owner. This is only available when the album is a Shared Album.
Shared	Indicates if the album is a Shared Album. The value "Yes" is displayed when the album is shared.
Invitees	The full names of those invited to view the Shared Album.

Photos Media Information

Description	Photos Media Information contains metadata about pictures and media stored in the Photos app on iOS.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the media file.
Type	The type of media. The value can be Picture or Video.
Album Title	The title of the media file's album.
Hidden	Indicates if a photo has been hidden.
Favorited	Indicates if a photo has been favorited.
Deleted	Indicates if a file has been recently deleted. Recently deleted files remain accessible for 30 days.
Directory	The directory the media file resides in.
Created Date/Time	The date/time when the media was created on the local device.
UUID	The UUID of the media.
Latitude	The latitude of the location where the media was taken.

ATTRIBUTE	DESCRIPTION
Longitude	The longitude of the location where the media was taken.
Modified Date/Time	The date/time when the media was modified on the local device.
Deleted Date/Time	The date/time when the media was deleted from the local device.

Pictures

Description	Pictures retrieved using either carving or parsing techniques.
Notes	The supported formats are as follows: JPEG (.jpeg, .jpg, .jpe), PNG (.png), Bitmaps (.bmp), Graphics Interchange Format (.gif), Icons (.ico), and Tagged Image File Format (.tif, .tiff). For more information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date/time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date/time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date/time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.

ATTRIBUTE	DESCRIPTION
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. "Complete" indicates that a full Exif extraction was performed. "Partial" indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. "Failed" indicates that the information may have been corrupted and could not be recovered. "Skipped" indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
GPS Longitude	The GPS longitude coordinates of where the picture was taken (extracted from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
GPS Latitude	The GPS Latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS Latitude (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the pciture was taken (extracted from Exif data).
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.

ATTRIBUTE	DESCRIPTION
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Potential Original Media	Indicating if the media is likely the original source.
Category	An integer that indicates the Project VIC category for the picture.

Private Photo Vault Albums

Description	Private Photo Vault Albums contains information about the albums a user creates to organize their media in the Private Photo Vault application. The album information can be useful intelligence for how a user might have organized encrypted media.
Notes	

ATTRIBUTE	DESCRIPTION
Album Title	The name of the Album.
Created date and time - UTC (yyyy-mm-dd)	The date and time when the album was created on the device.
Last Modified date and time - UTC (yyyy-mm-dd)	The date and time when the album was last modified on the device.
Decoy	Indicates whether the album is hidden (accessible with a different passcode) or not.
Password	The password protecting the album, if any. Does not affect encryption.
PIN	The value used to generate the encryption key. It can be either a numeric PIN (4 digits) or a sequence of values (2 to 9) of an unlock pattern.

Secret Photo Vault Albums

Description	Secret Photo Vault Albums contains information about the albums a user creates to organize their media in the Secret Photo Vault application. Users can create a fake account as a distraction from the content they want to hide in their main account.
Notes	

ATTRIBUTE	DESCRIPTION
Album Title	The name of the album.
Created date and time - UTC (yyyy-mm-dd)	The date and time that the album was created on the device.

ATTRIBUTE	DESCRIPTION
Account Type	Indicates whether the album is in the user's main account or their fake account.

Secret Photo Vault Bookmarks

Description	Secret Photo Vault Bookmarks contains information about the webpages that a user has bookmarked while using the browser of the Secret Photo Vault application.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the bookmark.
Added date and time - UTC (yyyy-mm-dd)	The date and time that the bookmark was added.
Name	The name of the bookmark.

Secret Photo Vault Contacts

Description	Secret Photo Vault Contacts contains information about the contacts a user saved in the Secret Photo Vault application. Users can create a fake account as a distraction from the content they want to hide in their main account.
Notes	

ATTRIBUTE	DESCRIPTION
First Name	The first name of the saved contact.
Last Name	The last name of the saved contact.
Company	The company information of the saved contact.
Email Address	The email address of the saved contact.
Home Phone	The home phone number of the saved contact.
Business Phone	The busines or work phone number of the saved contact.
Mobile Phone	The mobile phone number of the saved contact.
Created date and time - UTC (yyyy-mm-dd)	The date and time that the contact was added.
Notes	The notes added to the contact's information by the user.
URL	The URL added to the contact's information by the user.
Account Type	Indicates whether the saved contact is in the user's main account or their fake account.

Secret Photo Vault Media

Description	Secret Photo Vault Media contains information about the picture and video files that the user stores in the Secret Photo Vault application. Users can create a fake account as a distraction from the content they want to hide in their main account.
Notes	

ATTRIBUTE	DESCRIPTION
File Path	The path to the media file.
Media Type	The type of media (photo or video).
Album Title	The associated album title.
Created date and time - UTC (yyyy-mm-dd)	The date and time that the media was created on the device.
Deleted	Indicates whether or not the media file was deleted by the user.
Path	The path to the media file on the device.
Account Type	Indicates whether the saved contact is in the user's main account or their fake account.

Secret Photo Vault Saved Passwords

Description	Secret Photo Vault Saved Passwords contains information about the passwords a user has saved while using the browser of the Secret Photo Vault application. Users can create a fake account as a distraction from the content they want to hide in their main account.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the webpage that the saved password is associated with.
User Name	The saved username.
Password	The saved password.
Created date and time - UTC (yyyy-mm-dd)	The date and time that the password was saved on the device.
Account Type	Indicates whether the saved password is in the user's main account or their fake account.

Snapchat Chat Messages

Description	Contains the chat messages sent between users.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the message.
Recipient(s)	The recipients of the message.
Message ID	The unique ID for the message.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the chat message.
Message	The content of the sent message.
Type	The type of the message
Saved By Sender	Whether the message was saved by the sender (either Yes or No).
Saved By Recipient	Whether the message was saved by the recipient (either Yes or No).
Released By Recipient	Whether the recipient let the chat message be deleted (either Yes or No).
Message Status	The status of the message.
Skin Tone Percentage	The calculated percentage of skin tone in the attachment.
MD5 Hash	An MD5 hash of the attachment content.
SHA1 Hash	A SHA1 hash of the attachment content.
Attachment	The attachment content that was decrypted.

Snapchat Memories

Description	Pictures and videos that the Snapchat user saves as a memory.
Notes	

ATTRIBUTE	DESCRIPTION
Picture	The picture or video frames from the saved memory. The picture and the overlay for a snap are stored in separate locations, and are combined to reproduce the snap as it would appear in Snapchat.
Attachment	The attachment for the memory, if it's not a picture.
Created Date/Time - UTC (yyyy-mm-dd)	The date/time when the snap was originally taken.

ATTRIBUTE	DESCRIPTION
Timezone	The time zone of the device when the original snap was taken, or when the media was moved from the device's gallery to the My Eyes Only section of the app.
Type	Indicates whether the memory is saved as a regular snap or My Eyes Only, the latter being password protected.
Media Type	The media type, either Picture, Video, or Video (First Frame). Video (First Frame) indicates that the full video was not recovered.
Duration (seconds)	The duration of time before the snap expires.
Latitude	The latitude of the location where the snap was originally taken.
Longitude	The longitude of the location where the snap was originally taken.
Size (Bytes)	The encrypted size of the snap media. Any overlay that was added to the snap is not included when determining the size of the snap media.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Attachment Path	The file path of the media attachment on the device.
Skin Tone Percentage	The percentage of the picture that appears to be skin tone. Any overlay that was added to the snap is not included when calculating the skin tone.
MD5 Hash	The MD5 hash of the decrypted media. Any overlay that was added to the snap is not included when creating the hash signature.
SHA1 Hash	The SHA1 hash of the decrypted media. Any overlay that was added to the snap is not included when creating the hash signature.
PhotoDNA Hash	The PhotoDNA hash of the image.
Category	An integer that indicates the Project VIC category for the picture.

Snapchat Received Videos

Description	Videos stored by the Snapchat app on iOS
Notes	

ATTRIBUTE	DESCRIPTION
File Name	Name of the file.
File Extension	Extension of the file.
Image	A generated thumbnail of the video.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the video file was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the video file was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the vidoe was last written to.

ATTRIBUTE	DESCRIPTION
Skin Tone Percentage	The amount of skin tone found in the video.
File Size (Bytes)	The size of the video in bytes.
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.

Snapchat Stories - iOS

Description	Snapchat Stories contains information about a collection of snaps, which can exist for a 24 hour peroid.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the story.
Group	Whether the story is a group story (either Yes or No).
Creator ID	The unique ID of the user that created the story.
Creator Name	The username of the user that created the story.
Created Date/Time - UTC (yyyy-mm-dd)	The Date/Time the story was originally created.
Last Posted Date/Time - UTC (yyyy-mm-dd)	The Date/Time that content was last posted to the story.
Group Member ID(s)	The unique IDs of members of this story.
Group Member(s)	The usernames of members of this story.
Group Member Name(s)	The display names of members of this story.
Shared	Whether the story is shared with others (either Yes or No).
Geofenced	Whether the story is geofenced, meaning only users within a fixed radius of a certain lat/long coordinate can post to and view the story.
Latitude	For geofenced stories, the latitude of the center of the geofence.
Longitude	For geofenced stories, the longitude of the center of the geofence.

Snapchat Story Snaps - iOS

Description	Snapchat Story Snaps contains information about snaps that have been posted to a story.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The username of the user that posted the snap.
Display Name	The display name of the user that posted the snap.
Story Name	The name of the story the snap was posted to.
Caption	A caption that was added to the snap.
Attachment URL	The URL of any additional attachment linked to the snap.
Recorded Date/Time - UTC (yyyy-mm-dd)	The Date/Time the snap was recorded.
Posted Date/Time - UTC (yyyy-mm-dd)	The Date/Time the snap was posted to the story.
Expiration Date/Time - UTC (yyyy-mm-dd)	The Date/Time the snap will expire.
Screenshot Taken	Whether a screenshot of the snap was taken (Yes or No).
Saved By User	Whether the local user saved the snap (Yes or No).
Private	Whether the snap has been posted to a private story.
Attachment Name	The name of the attachment file associated with the snap.
Attachment Path	The path to the attachment file.
Skin Tone Percentage	The calculated percentage of skin tone in the attachment.
MD5 Hash	An MD5 hash of the attachment content.
SHA1 Hash	A SHA1 hash of the attachment content.
Attachment	The attachment content that was decrypted.

Videos

Description	Videos that are recovered using parsing or carving. Supported formats for parsing include AVI, MP4, MOV, MPEG, DIVX, A3GP, ASF, WMV, DVR-MS, MKV, VOB, MOD, and WEBM. Supported carving formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. For more information about supported video formats, see Supported media and file types.
Notes	Supported formats include AVI, MP4, MOV, MPEG, DIVX, A3GP, ASF, WMV, DVR-MS, MKV, VOB, MOD, and WEBM. For more information about supported video formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
File Name	Name of the file.
File Extension	Extension of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the video was created.

ATTRIBUTE	DESCRIPTION
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the video was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the video was last modified.
File Size (Bytes)	The size of the video.
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. "Complete" indicates that a full Exif extraction was performed, including potential metadata located at the end of the video. "Partial" indicates that only Exif information in the header section of the video file was recovered, which should only occur with very large videos (in excess of the limit set in the options screen). "Failed" indicates that the information may have been corrupted and could not be recovered. "Skipped" indicates that the extraction was skipped.
Media Duration (Seconds)	The duration of the video in seconds (extracted from Exif data).
Original Width	The resolution of the video (extracted from Exif data).
Original Height	The resolution of the video (extracted from Exif data).
Created Date/Time - Local Time	The local date and time when the video was first recorded (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the video was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the video being recored (extracted from Exif data).
Software	The software used to record or modify the video. This could either be the OS version of the phone used to record the video or name of the software used to edit the video in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to record the video (extracted from Exif data).
Model	The model of the camera used to record the video (extracted from Exif data).

ATTRIBUTE	DESCRIPTION
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to record the video (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The GPS coordinates of the camera where the video was recorded (extracted from Exif data).
Longitude	The GPS coordinates of the camera where the video was recorded (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the video was recorded (extracted from Exif data).
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.
Content Format	The format of the carved video.
Container Format	The format of the carved video container.
Saved Video Size (Bytes)	The size of the carved video that was saved to the database.

Mobile

SIM Card ICCID

Description	SIM Card ICCID contains the ICCID number that identifies the device's SIM card.
Notes	

ATTRIBUTE	DESCRIPTION
ICCID	The integrated circuit card identifier.

SIM Card IMSI

Description	SIM Card IMSI contains IMSI numbers used to identify the mobile subscriber, as recovered from the SIM card.
Notes	

ATTRIBUTE	DESCRIPTION
IMSI	The international mobile subscriber identity.

SIM Card Phone Numbers

Description	SIM Card Phone Numbers contains records of all the phone numbers saved to the device SIM card. The type of number is indicated by the record type.
Notes	

ATTRIBUTE	DESCRIPTION
Phone Number	The phone number for the specific record type.
Record Type	Identifies the type of record the phone number is. Can be 'Abbreviated dialing numbers(ADN)', 'Emergency call codes (ECC)', 'Last number dialed (LND)', 'MSISDN', 'Service dialing numbers (SDN)', or 'Fixed dialing numbers (FDN)'

SIM Card Service Providers

Description	SIM Card Service Providers contains the names of mobile service providers that the device has connected with, and which are recovered from the SIM card.
Notes	

ATTRIBUTE	DESCRIPTION
Service Provider Name	The identity of the mobile phone service provider.

SIM Card SMS Messages

Description	SIM Card SMS Messages contains messages sent or received by the local user which were saved to the SIM card.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the SMS message.
Recipient	The recipient of the SMS message.

ATTRIBUTE	DESCRIPTION
Message Date/Time	For incoming messages, this timestamp indicates when the message was received by the mobile service center. For outgoing messages, there is no data available for this field.
Message	The message body of the SMS message.
Deleted	Identifies whether the message has been deleted. Can be 'Yes' or 'No'
Message Status	Identifies whether the message has been read, unread, draft or sent.
SMSC	The short message service center number.

Operating System

.DS_Store Records

Description	.DS_Store Records contains all the records extracted from .DS_Store files found on the computer. Each record represents a property of a file or a folder. The significance of this artifact is an indicator of high likelihood that the user of the computer was aware of these files and folders with a possibility of attributing a date to that awareness.
Notes	In the Apple macOS operating system, .DS_Store (Desktop Services Store) is a hidden file that stores the display information of its containing folder, similar to the file desktop.ini in Microsoft Windows. The file tracks information such as icon positions, view settings, cached file size, cached last modified date, and even the choice of a background image. The .DS_Store is created and maintained by the Finder application in any folder that it accesses, even on remote file systems mounted from servers that share files (for example, via Server Message Block (SMB) protocol or the Apple Filing Protocol (AFP)). .DS_Store files are also included in archives created by macOS users, such as ZIP files, and they are backed up by some cloud file backup services. This means that the presence of .DS_Store Records artifacts on non-Mac evidence such as Windows, Mobile, or Cloud indicates that some of the data may have originated or have been accessed from a macOS computer at some point. For more information on .DS_Store files and their forensic significance see: .DS_Stores: Like Shellbags but for Macs.

ATTRIBUTE	DESCRIPTION
Record Name	The name of the file or folder as stored in the .DS_Store file.
Record Type	The type of the record, or property, that is being logged in the .DS_Store file for a particular file or folder.
Record Value	The value of the property for the given file or folder.
Record Path	The full path to the file or folder
.DS_Store Created Date/Time - UTC (yyyy-mm-dd)	The created date of the .DS_Store file from which the record was extracted.

ATTRIBUTE	DESCRIPTION
.DS_Store Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date of the .DS_Store file from which the record was extracted.
.DS_Store Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date of the .DS_Store file from which the record was extracted.

AirDrop Available Recipients

Description	AirDrop Available Recipients lists all available recipients for an AirDrop transfer outgoing from the local device. The devices need to be in Bluetooth and Wi-Fi range to connect to each other. You can recover up to one week of AirDrop activity history as it is stored in the Apple Unified Logs.
Notes	Available users are only recorded in the Apple Unified Logs when the local user opens the AirDrop view in Finder or tries to send a file using the AirDrop sharing option. There is a record for each time a person "bubble" appears in the respective interface. This artifact can help place other devices in proximity of the device being investigated.

ATTRIBUTE	DESCRIPTION
Name	The name of the user or the user's device.
User ID	The ID of the user as tracked by the AirDrop service.
Contact Added	Indicates whether the user is a contact on the local user's device.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the log entry.
Transaction Log	The log message extracted from Unified Logs.

AirDrop Background Activity

Description	Airdrop Background Activity is a collection of logs that capture background events triggered by the Airdrop service.
Notes	This artifact does not capture every single background event that is described in the log. This artifact extracts what look to be the most relevant pieces of data, but it's up to the examiner to determine their forensic significance. If there are logs that are not included in this artifact that should be, please reach out to Tech Support.

ATTRIBUTE	DESCRIPTION
Date/Time - UTC (yyyy-mm-dd)	The date and time of the log entry.
Transaction Log	The log message extracted from Unified Logs.

AirDrop Discoverability

Description	AirDrop Discoverability lists changes to the discoverability status of device.
Notes	While this artifact reflects changes that the user initiates a change to their discoverability, it does also capture system changes. The AirDrop service periodically resets which causes the status to toggle between the current status and off, typically within one second of each other. These changes are background system activities that are not representative of an action by the user.

ATTRIBUTE	DESCRIPTION
Mode Change Date/Time - UTC (yyyy-mm-dd)	The date and time of the log entry.
Mode	Mode is an indication of who can share files with the local machine (values include Off, Contacts Only, or Everyone).
Transaction Log	The log message extracted from Unified Logs.

AirDrop Incoming Transfers

Description	AirDrop Incoming Transfers lists information about AirDrop transfers incoming to the local device. The devices need to be in Bluetooth and Wi-Fi range to connect to each other. You can recover up to one week of AirDrop activity history as it is stored in the Apple Unified Logs.
Notes	Incoming transfers are records pertaining to the files received on the local machine. A single transaction with multiple files will get split into multiple hits in AXIOM Examine and can be grouped by sorting on Transaction ID.

ATTRIBUTE	DESCRIPTION
Item Type	Typically these values are displayed as mime types. However, if Apple doesn't have a friendly name reserved for a particular file type, you might see values like dyn.ah62d4rv4ge80nqbv.
Number of Items	The number of items of that type included in the transfer.
Is File	Indicates whether the items being transferred are files or not (e.g. folder, link, etc.).
Sender Name	The name of the sender.
Sender Device	The name of the sender's device.
Destination Folder	The location chosen by the user to save the incoming transfer to.
Status	Indicates whether the transfer is accepted, declined, or incomplete. Incomplete could mean either the transaction timed out, or the sender cancelled the transaction on their end.

ATTRIBUTE	DESCRIPTION
Transfer Start Date/Time - UTC (yyyy-mm-dd)	The date of the first log entry associated with the transfer.
Transfer Finish Date/Time - UTC (yyyy-mm-dd)	The date of the last log entry associated with the transfer.
Sender is Me	Indicates whether the sender is logged in under the same account as the recipient.
Auto Accepted	Indicates if the transfer was auto-accepted.
Sender ID	The Id of the sender as tracked by the AirDrop service.
Verifiable Identity	Indicates whether the identity of the user is verifiable, this is an internal flag and its up to the examiner to determine its forensic significance.
Partial Recovery	Identifies whether the transfer transaction log was incomplete. 'Yes' indicates that some of the transaction log lines were missing before the end of the log file was encountered, so some fragment lines were left empty because they could not be properly recovered.
Transaction ID	An identifier for a given transaction. If multiple files are selected and transferred together, they're listed as separate hits but will have the same transaction ID.
Transaction Log	A raw dump of the logs between the first and last log relating to the transaction.

AirDrop Outgoing Transfers

Description	AirDrop Outgoing Transfers lists information about AirDrop transfers outgoing from the local device. The devices need to be in Bluetooth and Wi-Fi range to connect to each other. You can recover up to one week of AirDrop activity history as it is stored in the Apple Unified Logs.
Notes	Outgoing transfers are records pertaining to the files sent by the local machine. A single transaction with multiple files will get split into multiple hits in AXIOM Examine and can be grouped by sorting on Transaction ID.

ATTRIBUTE	DESCRIPTION
Item Name	The file or folder name.
Item Type	Typically, these values are displayed as mime types. However, if Apple doesn't have a friendly name reserved for a particular file type, you might see values like dyn.ah62d4rv4ge80nqbv.
Is File	Indicates whether the items being transferred are files or not (e.g. folder, link, etc.).
Recipient Name	The name of the recipient.

ATTRIBUTE	DESCRIPTION
Recipient Device	The name of the recipient's device.
Status	Indicates whether the transfer is accepted, declined, or incomplete. A Declined/Incomplete status could indicate the transfer was cancelled, declined, or the transfer timed out transfer.
Transfer Start Date/Time - UTC (yyyy-mm-dd)	The date of the first log entry associated with the transfer.
Transfer Finish Date/Time - UTC (yyyy-mm-dd)	The date of the last log entry associated with the transfer.
Recipient ID	The Id of the recipient as tracked by the AirDrop service.
Verifiable Identity	Indicates whether the identity of the user is verifiable, this is an internal flag and its up to the examiner to determine its forensic significance.
Partial Recovery	Identifies whether the transfer transaction log was incomplete. 'Yes' indicates that some of the transaction log lines were missing before the end of the log file was encountered, so some fragment lines were left empty because they could not be properly recovered.
Transaction ID	An identifier for a given transaction. If multiple files are selected and transferred together, they're listed as separate hits but will have the same transaction ID.
Transaction Log	A raw dump of the logs between the first and last log relating to the transaction.

Apple Accounts

Description	Apple Accounts contains information about the Apple ID accounts used on the macOS computer. The account details contained can help investigators recover and correlate account information across applications and provide information on what accounts to review and get more information from.
Notes	

ATTRIBUTE	DESCRIPTION
Local Account	The local user's account name, this attribute is only available for macOS computers
User Name	The email address or user name used to log into the account.
Account ID	The UID used to identify accounts and files tied to a specific account.
Account Added Date/Time - UTC (yyyy-mm-dd)	The date and time that the account was added to the database.

ATTRIBUTE	DESCRIPTION
Parent Account ID	The UID used to match the account to its parent account if it has one.
Account Description	A description of the account, as provided by the user.
Account Type	The type of user account
Account Credential Type	The type of credentials used by the account. The account credential type can help to indicate which methods might be of use for recovering the credentials (and possibly aiding with a cloud acquisition of the account).
Owning Bundle ID	The unique bundle ID of the application that the account was setup with.
Last Credential Expiry Date/Time - UTC (yyyy-mm-dd)	The date and time of when the credentials had to be re-entered for the account due to a password change or expiry of the token/credentials.

Apple Contacts - iOS

Description	Apple Contacts contains information about the contacts a user has saved to their device.
Notes	

ATTRIBUTE	DESCRIPTION
First Name	The first name of the contact.
Last Name	The last name of the contact.
Picture	The profile picture of the contact, in its full size.
Phone Number(s)	The phone numbers associated with the contact.
Email(s)	The email addresses associated with the contact.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the contact's information was created.
Address	The physical address associated with the contact.
Website	The website associated with the contact.
Middle Name	The middle name of the contact.
Organization	The organization or business associated with the contact.
Organization Phonetic	The phonetic spelling of the organization.
Department	The department associated with the contact.
Notes	Notes associated with the contact.
Favorited	Indicates whether a contact has been set as a favorite by the user.
Favorite Contact Entry	An entry for the contact (such as a phone number) that the user has set as the preferred contact method. This attribute also indicates the default action used by the device when the entry is used

ATTRIBUTE	DESCRIPTION
Birthday (yyyy-mm-dd)	The birthday of the contact.
Alternate Birthday	The alternate birthday of the contact.
Job Title	The job title associated with the contact.
Nickname	The nickname associated with the contact.
Thumbnail	The profile picture of the contact, in thumbnail size.
Prefix	The prefix of the contact's name. E.g. Mr., Mrs., Dr.
Suffix	The suffix of the contact's name. E.g. PH.D, Ed.D, LL.D.
User Accounts	A comma separated list all the social media accounts associated with this contact.
First Name Phonetic	The phonetic spelling of the contact's first name.
First Name Pronunciation	The pronunciation of the contact's first name.
Middle Name Phonetic	The phonetic spelling of the contact's middle name.
Middle Name Pronunciation	The pronunciation of the contact's middle name.
Last Name Phonetic	The phonetic spelling of the contact's last name.
Last Name Pronunciation	The pronunciation of the contact's last name.
Previous Last Name	The previous last name of the contact.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the contact's information was last modified.

Apple Keychain Generic Passwords

Description	Apple Keychain Generic Passwords contains passwords for applications and services that are saved to the Keychain app. Analyzing results from this artifact can reveal valuable passwords and tokens that are associated to the user's accounts.
Notes	

ATTRIBUTE	DESCRIPTION
Service Name	The name of the service that has stored data in the keychain.

ATTRIBUTE	DESCRIPTION
Value	The secret value that's associated with the account. Values that have non-printable characters are converted to hex strings. To see what the raw data looks like before conversion, export the hit with attachments.
Account	The account identifier of the keychain item.
Access Group	The access group that the keychain item belongs to.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the keychain item was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the keychain item was last modified.
Original Location	The associated location of the keychain item in the original SQLite database on the original iOS device.

Apple Keychain Internet Passwords

Description	Apple Keychain Internet Passwords contains passwords for websites and internet services that are saved to the Keychain app. Analyzing results from this artifact can reveal valuable passwords and tokens that are associated to the user's accounts.
Notes	

ATTRIBUTE	DESCRIPTION
Label	The label of the keychain item.
Description	The description of the keychain item.
Account	The account identifier of the keychain item.
Value	The secret value that's associated with the account. Values that have non-printable characters are converted to hex strings. To see what the raw data looks like before conversion, export the hit with attachments.
Access Group	The access group that the keychain item belongs to.
DSID	The Destination Signaling Identifier is a unique identifier assigned to a user when they register an iCloud account.
Server	The server address for an internet password item.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the keychain item was created.

ATTRIBUTE	DESCRIPTION
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the keychain item was last modified.
Original Location	The associated location of the keychain item in the original SQLite database on the original iOS device.

Apple Keychain Saved Credit Cards

Description	Credit card entries saved to the Keychain app.
Notes	

ATTRIBUTE	DESCRIPTION
Name On Card	Name of the credit card owner as displayed in the card.
Card Number	Credit card number (if available)
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the credit card entry was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the credit card entry was last modified.
Expiry Date	Expiry date of the credit card in the format 'month-year'.

Apple Maps Trips

Description	Apple Maps Trips contains trips generated by Apple Maps. Instances of this artifact can be suggested routes as well as trips that the user actually takes.
Notes	

ATTRIBUTE	DESCRIPTION
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the trip was created on the device. This value does not reflect the time that the user took the trip. This value can also represent the time that the app suggested a route.
Origin Address	The full address of the origin point.
Destination Address	The full address of the destination point.
Origin Latitude	The latitude portion of the origin coordinate. This value is used to mark the location in the World Map view.
Origin Longitude	The longitude portion of the origin coordinate. This value is used to mark the location in the World Map view.

ATTRIBUTE	DESCRIPTION
Destination Latitude	The latitude portion of the destination coordinate. The World Map view doesn't use this value.
Destination Longitude	The longitude portion of the destination coordinate. The World Map view doesn't use this value.

Apple Notes

Description	Apple Notes contains information about the notes a user has created on their iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the note.
Folder	The folder the note is stored in.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the note was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the note was last modified.
Summary	The summary of the note.
Encrypted	Indicates whether or not the note has been encrypted.
Password Hint	The hint to encryption password.
Body	The note body.
Attachments	A list of attachments contained in the note
Note ID	The notes unique identifier.

Apple Notes - Voice

Description	Contains the recovered voice notes from an iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Audio	The saved voice note.
Saved Date/Time - UTC (yyyy-mm-dd)	The date and time that the voice note was saved.
Duration (seconds)	The duration of the voice note in seconds.
Path	The path to the voice note on the device.

ATTRIBUTE	DESCRIPTION
Version	The version of the note: Original, Duplicate (duplicate copy of the original), Duplicate - Edited (duplicate copy of the original and partly modified), Edited (edited copy of an original note).
Original Path	The path to the original version of an edited note.
Note ID	The ID of the note.
Label	The label of the note.

Application Install States

Description	Application Install States contains a list of state changes that occur while an application installs or is uninstalled on an iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Date/Time	The date and time that the event occurred.
Package Name	The internal name of the application.
Action	The type of change that occurred to the application.
Path	The file path to the package of the application.

Application Permissions

Description	Application Permissions contains information about the app permissions that a user is prompted to accept or decline while using iOS applications.
Notes	

ATTRIBUTE	DESCRIPTION
Application	The application that requests the permission.
Service Name	The permission service name.
Allowed	Indicates whether the application is allowed to use the service/permission.
Prompt Count	The number of times the user was prompted to give the permission to the application.

Bluetooth Devices

Description	Contains the Bluetooth devices that the iOS device has paired with.
Notes	

ATTRIBUTE	DESCRIPTION
Address	The MAC address of the device.
Name	The name that has been assigned to the device.
Major Device Class	The major class of device/service as per the Bluetooth specification.
Minor Device Class	The minor class of device/service as per the Bluetooth specification.
Last Seen Date/Time - UTC (yyyy-mm-dd)	The last date and time the device was seen.

Cached Locations

Description	Cached Locations stores a sample of locations that the iOS device has cached. Each instance contains the location, speed, and direction of travel at that particular point in time. The frequency that location samples are cached can vary depending on device usage, where some applications (for example, Maps) can result in samples being cached very frequently.
Notes	

ATTRIBUTE	DESCRIPTION
Latitude	The latitude of the stored location.
Longitude	The longitude of the stored location.
Accuracy (m)	The radius of horizontal accuracy of the latitude and longitude values.
Altitude (m)	The altitude of the stored location.
Altitude Accuracy (m)	The accuracy of the altitude value.
Direction	The direction of travel of the stored location, measured in degrees and relative to due north.
Speed (m/s)	The instantaneous speed captured for the stored location sample.
Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time that the location was recorded.

Calendar Events

Description	The iOS calendar app is a default app on iOS.
Notes	

ATTRIBUTE	DESCRIPTION
Summary	A summary of the calendar appointment

ATTRIBUTE	DESCRIPTION
Location	The location of the calendar appointment
Notes	Notes about the calendar appointment
Calendar	The name of the calendar from which the event was generated
Attendees	The attendees for the event
Start Date/Time - UTC (yyyy-mm-dd)	The date and time the appointment starts
End Date/Time - UTC (yyyy-mm-dd)	The date and time the appointment ends
Timezone	The timezone the appointment is in.
URL	A URL associated with the event

Cell Tower Locations

Description	Cell Tower Locations contains records of which cell towers a device connects to at a given time.
Notes	

ATTRIBUTE	DESCRIPTION
Cell ID	A GSM Cell ID (CID) is a generally unique number used to identify each base tranceiver station (BTS) or sector of a BTS within a location area code (LAC) if not within a GSM network.
Location Area Code	Location Area Code (LAC) is a unique number describing the set of base stations that are grouped together to optimize signalling.
Mobile Country Code	Mobile Country Code (MCC) is used in combination with Mobile Network Code (MNC) to uniquely identify a mobile network operator (carrier).
Mobile Network Code	Mobile Network Code (MNC) is used in combination with Mobile Country Code (MCC) to uniquely identify a mobile network operator (carrier).
Date/Time - Local Time (yyyy-mm-dd)	The date and time that this log was entered into cache.
Latitude	The latitude of the mobile device.
Longitude	The longitude of the mobile device.
Range	The distance the phone is away from the cell base station.
Confidence	The confidence of the data.

File Signature Mismatch (Audio)

Description	File Signature Mismatch (Audio) contains identified mismatches between a known file signature header and the extension (or lack thereof) for an audio file. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.

Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.

File Signature Mismatch (Container)

Description	File Signature Mismatch (Container) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a container. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.

File Signature Mismatch (Document)

Description	File Signature Mismatch (Document) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a document. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.

File Signature Mismatch (Picture)

Description	File Signature Mismatch (Picture) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a picture. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file. If the mime type is unknown, this defaults to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file. If the mime type is unknown, this defaults to application/octet-stream. If there is no file extension, but the mime type is known, a mismatch is is returned.
File Path	The path to the mismatched file.

File Signature Mismatch (Video)

Description	File Signature Mismatch (Video) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a video. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.

File System Events

Description	File System Events contains informaiton about the changes to file system objects, occuring on an iOS device. This artifact contains all system event files recovered from the '.fseventsd' folder.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the system object affected by the event.
File Path	The full path to the system object affected by the event.
Flags	Flags that indicate the type of system object and the changes that occured to the object.
Event ID	An Event ID for the record.
File ID	A system ID for the file system object that was affected by the event.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the event file is initially created. This file is recovered from the .fseventsd directory and can contain records for many different events, so this timestamp may not coincide with when the event actually occurred.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the event file was last updated. This file is recovered from the .fseventsd directory and can contain records for many different events, so this timestamp may not coincide with when the event actually occurred.

File System Information

Description	Contains all of the relevant information about the hard drives in use by the operating system.
Notes	

ATTRIBUTE	DESCRIPTION
Volume Serial Number	This field only applies to FAT and NTFS file systems. This is a 32-bit unsigned int value that is stored in Bios Paramter Block (BPB) and is showed in a special hex format – XXXX-XXXX e.g. EABB-6573. For other file systems, the value of this field should show "n/a".
Full Volume Serial Number	This field is a 64-bit volume serial number that is only present in BPB of NTFS file system, for example AABBCCDDEEFF0011. For non-NTFS file systems, "n/a" is displayed for this field.
File System	Shows the type of the file system, e.g "Microsoft NTFS".
Sectors per cluster	The number of sectors in a file system cluster, e.g. 8.
Bytes per sector	The amount of bytes per sector.
Starting Sector	The starting sector for this partition.
Ending Sector	The ending sector for this partition.
Total Sectors	Encase shows different values for this field based on how a volume is added to the case. For example, if you add just a volume (e.g. your local C:\ drive), it shows 123410271 for the number of sectors, but if you add your local physical drive 0 to the case and then select your C:\ volume in the "Entries" tree (note: your C drive would most likely have another letter in this tree, e.g. E:), then total number of sectors would be one more that the other value, i.e. 123410272. the value show for this field is taken from BPB, which matches the first value. The other value is shown when the parent physical drive is present probably comes from the partition table, and it counts VBR as well.
Total Capacity (Bytes)	This value is calculated by (Total Clusters) x (Cluster Size), which shows the capacity of the file system and not the volume containing it. The size of the volume would be higher than this value.
Total Clusters	The number of clusters comprising the file system.
Unallocated Area (Bytes)	Number of unallocated bytes on the file system, which is calculated by (Number of free clusters) x (cluster size).
Free Clusters	Number of unallocated clusters in the file system.
Allocated Area (Bytes)	(Number of allocated clusters) x (cluster size).
Volume Name	This is the volume label stored in Volume Boot Record (VBR).
Volume Offset (Bytes)	The offset (in bytes) of the volume containing this file system from beginning of the disk. "0" is displayed if the image and/or drive being searched is the image of one volume. Encase shows the number of sectors for this field instead of the number of bytes.
ID	The identifier of the hard drive.
Drive Type	The type of the hard drive.

Installed Applications

Description	A list of all of the applications on an iOS device, including their versions.
Notes	

ATTRIBUTE	DESCRIPTION
Package Name	The internal name of the application.
Installed Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was installed.
Display Name	The display name of the application.
Platform	The platform of the application.
Category	The category of the application, either System or User.
Internal Version	The internal version of the application.
Display Version	The display version of the application.

InteractionC

Delete this text and replace it with your own content.

InteractionC Contacts

Description	InteractionC Contacts contains information about the contacts that have been recorded as having interacted with the local user. This artifact can reveal a high-level view of how the local user communicates with a contact across multiple applications, provided that the contact uses the same identifier (for example, a phone number or email address).
Notes	

ATTRIBUTE	DESCRIPTION
Identifier	The identifier of the contact being communicated with. This value can be an email, a phone number, or another unique identifier for the contact.
Display Name	The display name of the contact.
Created Date/Time - UTC (yyyy-mm-dd)	The date/time that the contact was first recorded in the database. This value can coincide with the date/time of the first interaction, but in some cases, it appears that this value gets recorded without an interaction having occurred.
First Incoming Interaction Date/Time - UTC (yyyy-mm-dd)	The first recorded date/time of an incoming interaction.

ATTRIBUTE	DESCRIPTION
Last Incoming Interaction Date/Time - UTC (yyyy-mm-dd)	The last recorded date/time of an incoming interaction.
First Outgoing Interaction Date/Time - UTC (yyyy-mm-dd)	The first recorded date/time of an outgoing interaction.
Last Outgoing Interaction Date/Time - UTC (yyyy-mm-dd)	The last recorded date/time of an outgoing interaction.
Incoming Interaction Count	The number of incoming interactions recorded between the local user and the contact.
Outgoing Interaction Count	The number of outgoing interactions recorded between the local user and the contact.

InteractionC Interactions

Description	InteractionC Interactions contains information about the individual interactions that occurred with a contact, and were tracked in the InteractionC database. Interactions can be phone calls, emails, or messages from one of many different applications (native and third-party).
Notes	

ATTRIBUTE	DESCRIPTION
Bundle ID	The application bundle through which the interaction was initiated.
Display Name	The display name of the contact that was interacted with.
Sender	The sender of the interaction.
Created Date/Time - UTC (yyyy-mm-dd)	The date/time that an interaction was first recorded.
Start Date/Time - UTC (yyyy-mm-dd)	The first recorded date/time of an interaction.
End Date/Time - UTC (yyyy-mm-dd)	The last recorded date/time of an interaction.

iOS App Cache

Description	Cache of web content from various applications on an iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the cached content.

ATTRIBUTE	DESCRIPTION
Date Created Date/Time - UTC (yyyy-mm-dd)	The date the cached content was created on the local device.
File Type	The type of the cached file (html, js, css, jpeg, and so on).
Content Size (Bytes)	The size of the cached content, in bytes.
Image	The raw content of the cached image. This is blank if the content is not an image (i.e. it's html, js, css, etc.).
Content	The raw cached content. This is blank if the content is an image (in which case, the 'Image' column is populated instead).

iOS Call Logs

Description	Call logs from the iOS native phone app.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local user of the device where the data was recovered from.
Partner	The phone number of the conversation partner.
Partner Name	The name of the conversation partner.
Call Type	The type of iOS call, either FaceTime (Audio or Video), or regular phone call.
Call Status	The status of the call, either answered or unanswered.
Direction	The direction of the call, either incoming or outgoing.
Call Date/Time - UTC (yyyy-mm-dd)	Date and time at which the call was placed.
Call Duration (Seconds)	Duration of the call in seconds.
Service Provider	The service provider that handled the call.
Location	The location of the other participant of the call, which is either a full address or a Mobile Country Code (MCC).

iOS Device Information

Description	iOS Device Information contains information about the physical device, such as model information, the software version, timezone information, and the IMEI.
Notes	

ATTRIBUTE	DESCRIPTION
IMEI	The IMEI associated with the device.
Unique Device Identifier	A SHA1 hash that represents a unique identifier for the device.
Serial Number	The serial number of the device.
Device Name	The name of the device.
Display Name	The display name of the device.
Model	The device model.
Model ID	The ID of the model.
Build Version	The version of the build.
ICCID	The ID of the integrated circuit card.
Is Encrypted	True if the phone is encrypted, false otherwise.
Location Services Enabled	True if the location services have been enabled on this device, false otherwise.
Backup File Creation Date/Time	The date and time that most recent backup file was created (this might represent an iTunes backup or iCloud backup).
Last iTunes Backup Date/Time	The date and time that the most recent iTunes backup file was created.
Last Cloud Backup Date/Time	The date and time that the most recent cloud backup file was created.
OS Version	The iOS version number.
iCloud Account Present	Indicates whether an iCloud account is present on the device.
iTunes Version	The iTunes version number.
Was Passcode Set	Indicates whether a password was set on the device.
Find My iPhone Enabled	Indicates whether Find My iPhone is enabled.
Bluetooth Address	The bluetooth address of the device.
Device Class	The class of device (iPhone).
MEID	The MEID associated with the device.
Service Provider Country Code	The country code given by the service provider.
Mobile Network Code	The network code for the device.
Model Number	The model number of the device hardware.
Timezone	The timezone for the device.
UTC Offset	The timezone offset from UTC for the device.
MAC Address	The MAC address of the device.

iOS iMessage/SMS/MMS

Description	Contains all of the iMessages, SMSs and MMSs sent by the user.
Notes	

ATTRIBUTE	DESCRIPTION
Recipient	The recipient of the message.
Sender	The sender of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Message	The message that was sent.
Type	The direction of the message.
Status	The status of the message.
Message Delivered Date/Time - UTC (yyyy-mm-dd)	The date and time the message was delivered.
Message Read Date/Time - UTC (yyyy-mm-dd)	The date and time the message was read.
Attachments	The list of files attached to the message.
Attachment Data Recovered	The data of any files attached to the message.
Sent by Siri	Indicates whether the message was sent by the user through Siri.

iOS Maps

Description	The iOS maps images recovered from the device.
Notes	

ATTRIBUTE	DESCRIPTION
Local Modified Date/Time - UTC (yyyy-mm-dd)	The local modified date and time of the map image.
Size (Bytes)	The size of the map image.
Image	The map image.

iOS PowerLog App Usage

Description	iOS PowerLog App Usage contains information about the apps that were running on the device during a specified interval.
Notes	

ATTRIBUTE	DESCRIPTION
Interval Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the interval started. The time stated in this fragment represents an approximate time, and might vary from the exact time by up to 30 seconds.
Interval Length (Seconds)	The length of the interval in seconds.
Bundle ID	The ID of the app bundle.
Focus (Seconds)	The number of seconds the app was on the screen during the interval.
Background (Seconds)	The number of seconds the app was running in the background during the interval.

iOS PowerLog Battery Level

Description	iOS PowerLog Battery Level contains information about the phone's battery.
Notes	

ATTRIBUTE	DESCRIPTION
Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time that the battery level was recorded.
Battery Level	The battery level displayed in the UI.
Raw Battery Level	The true battery level.
Charging	Indicates whether the phone is charging (yes if charging, no otherwise).
Fully Charged	Indicates whether the battery is fully charged (yes if charged, no otherwise).

iOS PowerLog Camera State

Description	iOS PowerLog Camera State contains information about changes to the camera state which indicate when a device's camera is in use.
Notes	

ATTRIBUTE	DESCRIPTION
Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time that the camera usage was recorded.
Bundle ID	The ID of the app bundle.
State	Indicates whether the camera was On or Off.
Camera Type	Indicates which camera was being used (Front or Back).

iOS PowerLog Device Lock State

Description	iOS PowerLog Device Lock State contains information about when the phone was locked or unlocked.
Notes	

ATTRIBUTE	DESCRIPTION
Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time that the device lock state change was recorded.
State	The state of the phone (Locked or Unlocked).

iOS PowerLog Process Data Usage

Description	iOS PowerLog Process Data Usage contains information about the processes that were running on the device, and the amount of data that sent and received during the specified interval.
Notes	

ATTRIBUTE	DESCRIPTION
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time period started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time period ended.
Bundle ID	The ID of the app bundle.
Process Name	The name of the application that ran during the diagnostic period.
Mobile Bytes Received	The number of bytes received over a mobile cellular network.
Mobile Bytes Sent	The number of bytes sent over a mobile cellular network.
WiFi Bytes Received	The number of bytes received over a WiFi connection.
WiFi Bytes Sent	The number of bytes sent over a WiFi connection.

iOS PowerLog Screen Autolock

Description	iOS PowerLog Screen Autolock contains information about when the phone autolocked.
Notes	

ATTRIBUTE	DESCRIPTION
Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time that the device autolocked. The time stated in this fragment represents an approximate time, and might vary from the exact time by up to 30 seconds.

iOS PowerLog Timezone Information

Description	iOS PowerLog Timezone Information contains information about the timezones that were registered on the device.
Notes	

ATTRIBUTE	DESCRIPTION
Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time that the timezone was recorded.
Name	The name of the timezone.
Country Code	The code of the timezone's country.
Locale	The locale of the timezone.
GMT Offset	The number of hours the timezone is away from Greenwich Mean Time (GMT).

iOS Spotlight

Description	Contains the iMessage/SMS/MMS messages that have been saved by the Spotlight application.
Notes	

ATTRIBUTE	DESCRIPTION
Message	The content of the iMessage/SMS/MMS.
Summary	The summary of the content of the iMessage/SMS/MMS.
Partner	The partner of the iMessage/SMS/MMS.

iOS User Shortcut Dictionary

Description	Contains the shortcuts and phrases the user have on their device.
Notes	

ATTRIBUTE	DESCRIPTION
Shortcut	The sequence of characters that indicate when a phrase should be written.
Phrase	The phrase that the user wants typed when a sequence of characters are typed.

ATTRIBUTE	DESCRIPTION
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the shortcut and phrase were created.

iOS User Word Dictionary

Description	Contains the words the user has typed on the device.
Notes	

ATTRIBUTE	DESCRIPTION
Word	The word the user has typed.

iOS Voice Mail

Description	iOS Voice Mail contains messages left on the voicemail for the iOS device, along with any greetings messages recorded by the local user.
Notes	

ATTRIBUTE	DESCRIPTION
Audio	The raw audio content of the voicemail.
Sender	The sender of the voicemail.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the voicemail was sent.
Type	The type of voicemail. The Message type indicates a voicemail message left by a caller and the Greeting type indicates the greeting recorded by the local user.
Transcript	A text transcript of the voicemail message.
Duration (seconds)	The duration of the voicemail in seconds.

KnowledgeC Activity Level

Description	KnowledgeC Activity Level provides information about the KnowledgeC stream type of activity level.
Notes	

ATTRIBUTE	DESCRIPTION
Activity Type	The activity level.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Application Activities

Description	KnowledgeC Application Activities contains information about activities associated with specific applications.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The bundle name of the application associated with activity.
Activity	The description associated with the activity.
Activity Type	The type of activity that occurred. This value displays the package where the activity orginates from.
URL	The URL associated with the activity, if one exists.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time the activity occurred.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Application Focus

Description	KnowledgeC Application Focus provides information about the applications that were in focus on the device screen, within a recorded interval.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The bundle name of the application in focus.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Application Install States

Description	KnowledgeC Application Install States provides information about when applications were installed or uninstalled on the device.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The bundle name of the application that was installed or deleted.
Install State	The install state of the application (Installed or Uninstalled).
State Changed Date/Time - UTC (yyyy-mm-dd)	The date and time that install state last changed.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Application Intents

Description	KnowledgeC Application Intents bring additional context and detail to user interactions with the device. Application Intents are recorded by the system and are not always initiated by user interaction. For example, an intent is recorded when the user initiates a call and also when a call is received but isn't answered.
Notes	

ATTRIBUTE	DESCRIPTION
Intent Type	The type of interaction intent as recorded by the device.
Intent Class	The class of the intent.
Intent Action	The action the user intended.
Bundle ID	The application bundle through which the action was initiated.
Metadata	Additional details of the intent. This can include items such as alarm times and details spoken to Siri.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time of the intent as recorded by the device.

KnowledgeC Application Usage

Description	KnowledgeC Application Usage provides information about the applications that were used on the device, within a recorded interval.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The bundle name of the application used.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Application Web Usage

Description	KnowledgeC Application Web Usage provides information about the applications that were used to access webpages on a iOS device, within a recorded interval.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The bundle name of the application that accessed the webpage.
Domain	The domain name of the webpage.
URL	The URL of the webpage.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Device Lock States

Description	KnowledgeC Device Lock States provides information about whether the device is locked or unlocked within recorded intervals. An absence of a recorded interval might mean that device was turned off during that time.
Notes	

ATTRIBUTE	DESCRIPTION
State	The lock state of the device (Locked or Unlocked).
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Device Orientation States

Description	KnowledgeC Device Orientation States provides information about the orientation of the device within recorded intervals. An absence of a recorded interval might mean that device was turned off during that time.
Notes	

ATTRIBUTE	DESCRIPTION
State	The orientation state of the device (Vertical or Sideways).
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Device Plugged-in States

Description	KnowledgeC Device Plugged-in States provides information about the plugged-in state of a device within recorded intervals. An absence of a recorded interval might mean that device was turned off during that time. Knowing whenever a device is connected to charger or computer using USB can help identify how the device is used.
Notes	

ATTRIBUTE	DESCRIPTION
State	The plugged-in state of the device. This value shows whether a device is plugged in and/or connected via USB (Plugged in or Unplugged).
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Do Not Disturb Usage

Description	KnowledgeC Do Not Disturb Usage contains system activity information for the Do Not Disturb setting on the device.
Notes	

ATTRIBUTE	DESCRIPTION
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Keybag Lock States

Description	KnowledgeC Keybag Lock States provides information about whether the device's keybag is locked or unlocked within recorded intervals. An absence of a recorded interval might mean that device was turned off during that time.
Notes	

ATTRIBUTE	DESCRIPTION
State	The lock state of the keybag (Locked or Unlocked).
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Media History

Description	KnowledgeC Media History provides information about what type of audio/video media the user was engaging with at what time, as recovered from KnowledgeC.db
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The bundle name of the application used to play the specified media
Album	The album name of the specified media
Title	The title of the specified media
Artist	The artist of the specified media
Duration (Seconds)	The duration of the specified media in seconds
Start Date/Time - UTC (yyyy-mm-dd)	The date and time the media started playing
End Date/Time - UTC (yyyy-mm-dd)	The date and time the media stopped playing

KnowledgeC Notification Usage

Description	KnowledgeC Activity Level provides information about the KnowledgeC stream type of activity level.
Notes	

ATTRIBUTE	DESCRIPTION
Bundle ID	The bundle ID.
Type	The type of notification.
Device ID	The device ID.
Process ID	The process ID.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Safari History

Description	KnowledgeC Safari History provides information about web pages that were accessed using the Safari browser, as recovered from knowledgeC.db
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the web page that was accessed with Safari browser.
Title	The title of the web page that was accessed with Safari browser.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the web page was accessed with Safari browser.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Screen Backlight States

Description	KnowledgeC Screen Backlight States provides information about the device backlight within recorded intervals. An absence of a recorded interval might mean that device was turned off during that time. This information can help identify whether a device was in active use within a specific interval.
Notes	

ATTRIBUTE	DESCRIPTION
State	The screen backlight state of the device. This value indicates whether the screen backlight is on or off (Screen on or Screen off).
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Siri UI Usage

Description	KnowledgeC logs the time windows that the Siri UI is in use.
Notes	

ATTRIBUTE	DESCRIPTION
Value	Indicates either the start or the end of a Siri UI session.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Latent Wireless Geolocated WiFi Hotspots

Description	Latent Wireless Geolocated WiFi Hotspots contains information about WiFi hotspots that were discovered using a Latent Wireless device. Latent Wireless stores information about the hotspots in a database that Magnet AXIOM can parse for details about each hotspot.
Notes	

ATTRIBUTE	DESCRIPTION
MAC Address	The MAC address of the detected WiFi hotspot.
First Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was first discovered.
Last Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was last seen.
Strongest Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was detected at its highest strength.
Network Name (SSID)	The SSID of the WiFi hotspot.
Channel	The WiFi hotspot channel.

ATTRIBUTE	DESCRIPTION
RSSI	The receieved signal strength indicator for the WiFi hotspot.
Latitude	The latitude where the WiFi hotspot was detected.
Longitude	The longitude where the WiFi hotspot was detected.
Secure	Indicates whether the wiFi hotspot is secure.

Network Usage - Application Data

Description	Network Usage - Application Data contains information about how an application sends or receives data over the network.
Notes	

ATTRIBUTE	DESCRIPTION
Process Name	The file name of the executable.
Type	The executable type (Process or App).
First Used Date/Time - UTC (yyyy-mm-dd)	The date and time the process was first run.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time the process was last run.
Last Connected Date/Time - UTC (yyyy-mm-dd)	The date and time the process last connected to a network.
WiFi Bytes Sent	The number of bytes sent over a WiFi connection.
WiFi Bytes Received	The number of bytes received over a WiFi connection.
Mobile Bytes Sent	The number of bytes sent over a mobile cellular network.
Mobile Bytes Received	The number of bytes received over a mobile cellular network.
Wired Bytes Sent	The number of bytes sent over a wired connection.
Wired Bytes Received	The number of bytes received over a wired connection.

Network Usage - Connections

Description	Network Usage - Connections contains information about the networks that a device connects to.
Notes	

ATTRIBUTE	DESCRIPTION
Network Name	The SSID or mobile network name.
Connection Type	Indicates the connection type (for example, WiFi or Cellular).
Cell ID/MAC Address	An identifier for the specific access point to the network, which can be either a cell tower identifier or a MAC address.

ATTRIBUTE	DESCRIPTION
First Connected Date	The date that the device first connected to this network.
Last Connected Date	The date that the device last connected to this network.

Owner Information

Description	Owner Information contains information about the iOS device and the device owner. Information includes the device name, the phone number associated with the phone, and other details associated with iOS.
Notes	

ATTRIBUTE	DESCRIPTION
Device Phone Name	The name of the device.
Device Phone Number	The phone number associated with the device.
Apple ID	The Apple ID associated with this owner.
iTunes Version	The version of iTunes installed on the device.
Setup Date	The date and time that the iOS device was setup.
Setup Type	Indicates the method used for setting up the device (for example, using the setup assistant, iTunes, or by iCloud backup).

Parked Car Locations

Description	Parked Car Locations contains locations of a user's vehicle that they've saved and which are tracked by the iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Date/Time - Local Time (yyyy-mm-dd)	The date and time that this log was entered into cache.
Latitude	The latitude of the Parked Car Location.
Longitude	The longitude of the Parked Car Location.

Screen Time Application Usage

Description	Screen Time Application Usage contains usage and notification information for all applications tracked by Screen Time. The application (and this artifact) tracks data in 60 minute intervals, so any usage and notification data applies only to that segment of time. This artifact can help identify when an application was in use and for how long, both on the local device and other devices that are synced under the same Apple ID/Family Account.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The bundle name of the application that's being tracked using Screen Time.
Domain	The name of the domain associated to the webpage the user was visiting.
Interval Start Date/Time - UTC (yyyy-mm-dd)	The start date and time of the 60 minute interval. Screen time tracks usage in these hour-long blocks.
Total Time (Seconds)	The total time that was spent using the application within the time interval.
Notifications	The number of notifications received by the application within the time interval.
Pickups	The number of times the application receives focus (when the app starts, or the user switches contexts, etc.) within the time interval.
Device Name	The name of the device where the application was used. It can be empty for cloud-synched data or all devices data.
Given Name	The given name of the user associated with the device.
Family Name	The last name of the user associated with the device.

Screen Time Synced Applications

Description	Screen Time Synced Applications contains list of all the applications that are being tracked using Screen Time. This list includes applications that are installed on the local user's device, or are installed on other devices connected to the same family account or use the same Apple ID.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The bundle name of the application that's being tracked using Screen Time.
Unique Device Identifier	The ID of the device where the application is installed.
Device Name	The name of the device where the application was installed.
Given Name	The given name of the user associated with the device.
Family Name	The last name of the user associated with the device.

ATTRIBUTE	DESCRIPTION
Account Type	The family account type of the user associated with the device. The value is Unknown if a family account wasn't set.

Seen Bluetooth Devices

Description	Seen Bluetooth Devices keep a track of Bluetooth devices that may have been seen by the host device.
Notes	

ATTRIBUTE	DESCRIPTION
Device Name	Name of the Bluetooth device.
Bluetooth Address	The MAC address of the Bluetooth device.
UUID	The Universially Unique Identifier of the record.

Significant Locations

Description	Significant Locations contains information about places that are deemed to be significant in some way to the user. These locations can be manually added by the user (such as a home or work address) or are automatically added by Apple. This data is used to help make more personalized predictions.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local user of the device where the data was recovered from.
Location Name	The name of location.
Address	The address of the location.
City	The city of the location.
Country	The country of the location.
State/Province	The state or province of the location.
ZIP/Postal Code	The ZIP or postal code of the location.
Location Type	The type of location set by the user
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the location was saved.
Latitude	The latitude of the location.
Longitude	The longitude of the location.

Significant Locations Visits

Description	Significant Locations Visits contains information about the saved significant locations that the user visits. These location visits are automatically tracked by the device when the user is in the vicinity.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local user of the device where the data was recovered from.
Address	The address of the location visited.
City	The city of the location.
Country	The country of the location.
State/Province	The State/Province of the location.
ZIP/Postal Code	The ZIP/Postal Code of the location.
Vicinity Entry Date/Time - UTC (yyyy-mm-dd)	The date and time that the user entered the vicinity of the location.
Vicinity Exit Date/Time - UTC (yyyy-mm-dd)	The date and time that the user exited the vicinity of the location.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the visit entry was saved.
Latitude	The latitude of the location visited.
Longitude	The longitude of the location visited.
Accuracy	The distance from the original geographic coordinate that could yield the user's actual location. The unit of measurement is presumed to be meters.

SIM Card Activity

Description	SIM Card Activity contains information about the SIM cards that have been used in an iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
ICCID	The unique identifier for the SIM card.
Phone Number	The phone number associated with the SIM card.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the SIM card data was updated.
SIM Card Slot	The slot on the phone that the SIM card was inserted in.

Siri Message Search Suggestions

Description	Siri Message Search Suggestions contains the sent or received messages that Siri provides to the user as search results for a query. Queries can be typed in the search bar or spoken using Siri voice commands.
Notes	

ATTRIBUTE	DESCRIPTION
Message	The message that appeared as a suggestion for a user's search
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Message Direction	The direction the message was sent, either sent or received.
Conversation ID	The identifier of the conversation the message is a part of.

Wallet Passes

Description	Wallet Passes contains information on passes (boarding passes, coupons, event tickets, store cards, and others) that have been saved to the user's Wallet app.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local user of the device where the data was recovered from.
Organization	The organization that issued this pass.
Description	A description of the pass.
Serial Number	The serial number of the pass. This is vendor-specific, so cannot be assumed to be unique across passes.
Type	The type of the pass, e.g. Boarding Pass.
Effective Date/Time - UTC (yyyy-mm-dd)	The date/time that the pass becomes relevant, e.g. a start date, or boarding time.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date/time that the pass is no longer relevant.
Header Fields	Content of the dynamic header fields structure in the file, which are supplied by the vendor. These are presented as (key) label : value and delimited with a newline.
Primary Fields	Content of the dynamic primary fields structure in the file, which are supplied by the vendor. These are presented as (key) label : value and delimited with a newline.
Secondary Fields	Content of the dynamic secondary fields structure in the file, which are supplied by the vendor. These are presented as (key) label : value and delimited with a newline.

ATTRIBUTE	DESCRIPTION
Auxiliary Fields	Content of the dynamic auxiliary fields structure in the file, which are supplied by the vendor. These are presented as (key) label : value and delimited with a newline.
Back Fields	Content of the dynamic back fields structure in the file, which are supplied by the vendor. These are presented as (key) label : value and delimited with a newline.

Wallet Payment Cards

Description	Wallet Payment Cards contains information on payment cards that have been saved to the user's Wallet app.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local user of the device where the data was recovered from.
Issuer	The organization that issued this payment card (typically a bank).
Payment Method	The payment method, i.e. credit or debit.
Last Four Digits	The card's last four digits.
Expiry Date	The expiry month and year as indicated on the card.
Account Description	A description of the account that backs this payment card.
DPAN	The Device Primary Account Number linking the device and bank account/credit card.
Country Code	The two-character country code in which this card was issued.

Wallet Transactions

Description	Wallet Transactions contains information about transactions that have been completed with the Apple Wallet application. This artifact can also recover transactions with cards that are associated with the wallet but aren't made through the wallet application.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local user of the device where the data was recovered from.
Transaction Date/Time - UTC (yyyy-mm-dd)	The date/time the transaction was initiated.
Name	The merchant's name.
Cost	The amount of the transaction.
Currency	The currency of the transaction.

ATTRIBUTE	DESCRIPTION
Latitude	The latitude of the first location acquisition after the transaction was conducted (may be inaccurate if there's a large time gap between the two).
Longitude	The longitude of the first location acquisition after the transaction was conducted (may be inaccurate if there's a large time gap between the two).
Accuracy	The distance from the original geographic coordinate that could yield the user's actual location. The unit of measurement is presumed to be meters.
Altitude (meters)	The altitude in meters of the first location acquisition after the transaction was conducted (may be inaccurate if there's a large time gap between the two).
Location Acquired Date/Time - UTC (yyyy-mm-dd)	The date/time the location was acquired.
Status	The transaction status (raw data - uninterpreted).
Type	The transaction type (raw data - uninterpreted).
DPAN	The Device Primary Account Number linking the device and bank account/credit card.
Categories	The merchant's primary business category, e.g. restaurant.
Street	The merchant's street address.
City	The merchant's city.
State/Province	The merchant's state/province.
Country	The merchant's country.
ZIP/Postal Code	The merchant's ZIP or postal code.
Business Phone	The merchant's phone number.

Wi-Fi Profiles

Description	A list of the saved Wi-Fi Profiles on a mobile device.
Notes	

ATTRIBUTE	DESCRIPTION
Network Name (SSID)	The name of the network.
Security Mode	The security mode of the network.
MAC Address	The MAC Address of the network.
Last Auto Joined Date/Time - UTC (yyyy-mm-dd)	The last date and time that the wireless network was automatically joined by the device.
Last Joined Date/Time - UTC (yyyy-mm-dd)	The last date and time that the wireless network was manually joined by the device.

WiFi Locations

Description	WiFi Locations contains records of WiFi Location detected by the mobile device at a given time.
Notes	

ATTRIBUTE	DESCRIPTION
MAC Address	The MAC Address of the WiFi Location.
Channel	The channel the WiFi Location.
Date/Time - Local Time (yyyy-mm-dd)	The date and time that this log was entered into cache.
Latitude	The latitude of the mobile device.
Longitude	The longitude of the mobile device.
Accuracy (meters)	The accuracy of the position information.
Confidence	The confidence of the data.

Peer-to-Peer

Torrent File Fragments

Description	Data that is carved or parsed from .torrent files that are used to download torrents from various networks on the Internet.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the torrent file
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the torrent file was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the torrent file was modified.
Torrent Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the torrent file was originally created.
Torrent Files	The files that are listed in the torrent to be downloaded.

Refined Results

iOS Snapshots

Description	Stored snapshots of an application's state taken by iOS when the application is suspended.

Notes	This artifact can only return hits if the Pictures artifact is turned on.

ATTRIBUTE	DESCRIPTION
Application Package Name	The package name of the application.
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date/time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date/time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date/time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

Social Networking

Facebook

Facebook, being one of the most popular social networking sites in the world, presents numerous opportunities for gathering evidence. You can recover messages that are sent and received, status updates and wall posts, and pages and pictures that the user views. On mobile devices, you can also recover user profiles and contacts.

Facebook can provide background information about a user, as well as evidence of who they are communicating with or associated with. Status and location updates can provide details about where a user has been and what they've been doing.

FORENSIC NOTES

The Facebook Pictures artifact represents cached pictures found on the system that originated from Facebook. When caching pictures, Facebook names the pictures using a particular format which allows forensic tools to know that they come from Facebook. These pictures can be user profile pictures, friends' pictures, or any other picture that gets cached while browsing Facebook.

ARTIFACTS

RELATED RESOURCES

How important are Facebook artifacts?

Recovering Facebook artifacts

iOS Facebook Friends

Description	Contact information stored by the Facebook app.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	Integer unique ID for the friend.
Member Email	Email address of the friend.
Member Name	Full name of the friend.
Nickname	The friend's nickname, if applicable.
Image URL	The URL of the friend's avatar.
Read Receipt Message ID	The message ID of the last read message from the friend.
Read Receipt Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time the last message from the friend was read.

iOS Facebook Messages

Description	Facebook messages recovered from the device.

Notes	

ATTRIBUTE	DESCRIPTION
User ID	Integer unique ID for the sender.
Name	The sender's name.
Email	The sender's email address.
Message ID	A string which uniquely identifies the message.
Text	Text message content.
Message Source	Indicates which facebook platform was used to send the message.
Coordinates	Latitude and Longitude of the location from which the message was sent.
Send Timestamp Date/Time - UTC (yyyy-mm-dd)	The Date/Time at which the message was sent.
Send State	0/2. 0 indicates a successful send, and 2 indicates a failed send.
Timestamp Date/Time - UTC (yyyy-mm-dd)	Second timestamp associated with the message.

Foursquare Check-ins

Description	Check-ins made by the iOS Foursquare app.
Notes	

ATTRIBUTE	DESCRIPTION
User Id	The user id.
User First Name	The users first name.
User Last Name	The users last name.
User Email	Email address of the account used to check in.
Check-In Date/Time - UTC (yyyy-mm-dd)	The date and time when the user checked-in to the specified locaiton.
Location Name	The name of the location the user checked into.
Comment	The comment a user left about their check-in for the location.
Address	The address of the check-in location.
Latitude	The latitude of the check-in location.
Longitude	The longitude of the check-in location.
City	The city of the check-in location.
State	The state of the check-in location.

ATTRIBUTE	DESCRIPTION
Country	The country of the check-in location.
Been Here Count	The number of times the user has checked into this location.
User Gender	The users gender.

Foursquare Locations

Description	Locations cached by the iOS Foursquare app.
Notes	

ATTRIBUTE	DESCRIPTION
Location Name	The name of the location.
Address	The address of the location.
Latitude	The latitude of the location.
Longitude	The longitude of the location.
Distance (meters)	The distance the user is from the location.
City	The city of the location.
State	The state of the location.
Country	The country of the location.

Houseparty Messages

Description	Contains messages recovered from Houseparty.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The username of the person sending the message.
Recipient	The username of the person receiving the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The content of the sent message.
Read Status	Whether or not the message has been read.

Houseparty Users

Description	Contains information about the users contacted from the device using Houseparty.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	User name of the user.
Full Name	Full name of the user.
Created Date/Time - UTC (yyyy-mm-dd)	Date and time when the user account was created.
Updated Date/Time - UTC (yyyy-mm-dd)	Date and time when the user account was last updated.

Instagram Direct Messages

Description	Instagram direct messages that are sent or received by the local user.
Notes	Attachment Path, Latitude, and Longitude are not recoverable on iOS devices. The Media URL attribute is only available for messages of the Forwarded Post type.

ATTRIBUTE	DESCRIPTION
Sender	The user name of the sender of the message.
Recipient	The user name of the recipient of the message.
Direction	The direction of the message, relative to the source of the hit.
Message	The message that was sent.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the message.
Picture	Either the picture that was sent, or a storyboard of the video that was sent.
Attachment Path	The path to the attachment that was sent.
Media URL	The URL to the media of the message.
Type	The message type.
Status	The status of the message.
Latitude	The latitude of the message.
Longitude	The longitude of the message.
Caption	The original message of a forwarded post.
Original Author	The original author of a forwarded post.
Original Date/Time	The original date and time of a forwarded post.

Instagram Group Members

Description	Information about the Instagram groups that the local user is a member of.
Notes	

ATTRIBUTE	DESCRIPTION
Group Member	The user name of the group member.
Group Name	The name of the group.

Instagram Media

Description	The media files that have been found inside the Insatgram app.
Notes	

ATTRIBUTE	DESCRIPTION
Picture	The picture of the media, or a storyboard if the media is a video.
MIME Type	The MIME type of the media.
Created Date/Time - UTC (yyyy-mm-dd)	The created date/time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date/time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date/time of the picture in the file system.
Size (Bytes)	The size of the media file, in bytes
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

Instagram Profiles

Description	All the profile information that the local user has had communications with, or have been referred to through Direct Messages communication.

Notes	For iOS devices, the 'Post Notifications' attribute will always be empty.

ATTRIBUTE	DESCRIPTION
User Name	The user name of the profile.
Name	The name associated with the profile.
User ID	The User ID associated with the profile.
Profile Picture URL	The profile picture of the user's profile.
Local User	Indicates if the profile belongs to a user logged into the device.
Is Private	Indicates if the profile is private or not.
Biography	The biography of the user associated with the account.
Following	Indicates whether the user of this profile is following the local user.
Is Followed By	Indicates whether the local user is following this user profile.
Post Notifications	Indicates whether the local user has turned on post notifications for this user profile. This attribute is only populated if the local user is following this user profile.
Email	The public email address associated with this user profile.
Phone Number	The public phone number associated with the user profile.
Address	The public address associated with the user profile.
City	The city associated with the user profile.
ZIP/Postal Code	The ZIP/Postal associated with the user profile.
Latitude	The latitude of the location associated with the user profile.
Longitude	The longitude of the location associated with the user profile.

iOS Instagram Posts

Description	Instagram Posts contains information about posts that a user has recently viewed on Instagram as well as comments that are present on those posts.
Notes	The Device Date/Time and Downloaded Posted Images fragments are only available on Android.

ATTRIBUTE	DESCRIPTION
ID	The post ID.
Full Name	The full name of the user.
Profile Picture URL	The URL to the profile picture of the user.
Downloaded Profile Image	The downloaded profile picture.

ATTRIBUTE	DESCRIPTION
User Name	The user name on Instagram.
Posted Image URL	The URL to the picture that was posted.
Downloaded Posted Image	The downloaded picture from the post.
Text	The text for the given image.
Created Date/Time - UTC (yyyy-mm-dd)	The date the post was created.
Device Date/Time - UTC (yyyy-mm-dd)	The date the user viewed the post

iOS Whisper Posts

Description	Contains the posts stored by the Whisper app.
Notes	

ATTRIBUTE	DESCRIPTION
Poster Nickname	The username of the person at the time the post was posted.
Post Date/Time - UTC (yyyy-mm-dd)	The date and time the post was posted.
Message Text	The content of the post.
Local Device Post	Whether the post was created on the local device (yes or no).
Location	The location of the user when the post was posted.
Image URL	The URL to the image of the post.
Downloaded Image	The downloaded image from the post, if the option is turned on in Report Viewer.
Heart Count	The number of hearts the post has received.
Reply Count	The number of replies to the post.
Hearted	Whether the local user has hearted the post (yes or no).

LinkedIn Messages

Description	LinkedIn Messages contains messages sent and received by the local user.
Notes	

ATTRIBUTE	DESCRIPTION
Sender Name	The name of the sender.
Recipient Name(s)	The name(s) of the recipient(s).

ATTRIBUTE	DESCRIPTION
Sent Date/Time	The date and time when the message was sent.
Message	The body of the message.
Attachment Name	The name of attachment to the message.
Attachment URL	The url of attachment to the message.
Attachment Type	The type of attachment to the message.

LinkedIn Profile

Description	LinkedIn Profile contains information about the user accounts that the local user has used to log in on the device.
Notes	

ATTRIBUTE	DESCRIPTION
UserName	The username of local user.
First Name	The first name of local user.
Last Name	The last name of local user.
Full Name	The full name of local user.
Summary	A summary of the local user. This information is provided by the user and could indicate a number of different things including their position or status.

Musical.ly Local Users

Description	All of the users that have logged in to Musical.ly on the local device.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The user's login name.
User Nickname	The user's chosen nick name.
User ID	The ID of the user in Musical.ly systems.
Account Description	The description the user has given for themself.
Image URL	The URL of the user's profile picture.
Instagram Account	The user's Instagram account.
Google Account	The user's Google account.
YouTube Channel	The user's YouTube Channel.

ATTRIBUTE	DESCRIPTION
IP Address	The public IP address of the device the user logged in with.
Is Private	Has the user prevented others from discovering their profile (Yes or No)?
Hide Location	Does the user keep their geolocation information hidden on their profile page (Yes or No)?
Messaging Availablilty	Indicates who is able to message the user, as specified by the user (Public or Friends Only).
Country Code	The country code of the country that the user has set for themself.
Language	The language code of the language that the user has set for themself.

Musical.ly Messages

Description	The messages sent or received via the in-app message system of Musical.ly.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the message.
Recipient	The recipient of the message.
Message	The body of the message. This value is empty if a picture message was sent.
Direction	The direction of the message, relative to the source database.
Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time the message was either received or sent on the local device.
Picture	The picture that was sent or received. This value is empty if a text message has been sent.
Read	Whether or not the message has been read by the local device. Can be displayed as 'Yes' or 'No'.
Message Status	The status of the message. Can be 'Delivered' or 'Pending Internet Connection'.

Musical.ly Posts

Description	Posts that Musical.ly retrieved from the web.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The user name of the poster.
User Nickname	The nick name of the poster.
User ID	The ID of the poster.
Caption	The caption the user wrote for their post.
Picture	The locally cached post's preview picture.
Cached Video Size (Bytes)	The size of the locally cached post's video.
Video URL	The URL of the post's video.
Picture URL	The URL of the post's preview picture.

Musical.ly Users

Description	All the users that the local user has viewed in Musical.ly.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The user's login name.
User Nickname	The user's chosen nick name.
User ID	The ID of the user in Musical.ly systems.
Account Description	The description the user has given for themself.
Profile Picture URL	The URL of the user's profile picture.
Instagram Account	The user's Instagram account.
Google Account	The user's Google account.
YouTube Channel	The user's YouTube Channel.
Is Private	Has the user prevented others from discovering their profile (Yes or No)?
Is Friend	Is the user a friend of the local user in the source database (Yes or No)?
Following	Is the local user in the source database following this user (Yes or No)?
Post Notifications	Does the local user want to receive notifications when this user makes a post (Yes or No)?
Hide Location	Does the user keep their geolocation information hidden on their profile page (Yes or No)?
Messaging Avail-ablilty	Indicates who is able to message the user, as specified by the user (Public or Friends Only).
Country Code	The country code of the country that the user has set for themself.
Language	The language code of the language that the user has set for themself.

Pinterest Accounts

Description	Pinterest Accounts contains information about the accounts that the local user has logged in with on the device.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user ID of the local user.
Full Name	The full name of the local user.
Email Address	The email address of the local user.
Created Date/Time	The created date/time of the local user.
Gender	The gender of the local user.
Country	The country of the local user.
Location	The location of the local user.
Profile Image URL	The profile image url of the local user.
Active	The current status of the local user. It indicated if the account is coming from an active database.

Pinterest Boards

Description	Pinterest boards contains information about the boards created by local user.
Notes	

ATTRIBUTE	DESCRIPTION
ID	The id of the board.
Name	The name of the board.
Category	The category of the board.
Description	The description of the board.
Created Date/Time	The created date/time of the board.
Website URL	The url of the board.
Owner ID	The owner ID of the board.
Active Account	Indicates whether the board is from the account that's currently logged in on the device.

Pinterest Messages

Description	Pinterest Messages contains messages or pins sent and received by the local user.
Notes	

ATTRIBUTE	DESCRIPTION
Sender ID	The id of the sender.
Sender Name	The name of the sender.
Recipient ID (s)	The user ID(s) of the recipient(s). For iOS, there is not reliable way to get the recipient information. User need to infer that from the sender information.
Recipient Name(s)	The name(s) of the recipient(s). For iOS, there is not reliable way to get the recipient information. User need to infer that from the sender information.
Sent Date/Time	The date and time the message was sent.
Message	The content of the message.
Pin Title	The title of the pin.
Pin Picture URL	The picture URL associated with the pin.
Attachment Name	The file name of the picture cache associated with the pin.
Active Account	Indicates whether the following user is of the account that's currently logged in on the device.

Pinterest Pins

Description	Pinterest Pins contains information about the items that the local user has pinned to their own board.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the pin.
Description	The description of the pin.
Created Date/Time	The created date/time of the pin.
Website URL	The website utl associated with the pin.
Posted Image URL	The posted image url associated with the pin.

ATTRIBUTE	DESCRIPTION
Attachment Name	The name of the attachment associated with the pin.
Pinner ID	The pinner ID of the pin.
Active Account	Indicates whether the following user is of the account that's currently logged in on the device.

Sina Weibo Posts

Description	User posts (similar to Twitter's tweets) on the Sina Weibo app on iOS.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The unique identifier for the user posting.
User Nickname	The user's nickname.
Post Date/Time - UTC (yyyy-mm-dd)	The date/time that the content was posted.
Post	The content of the post.
Profile Image URL	The URL for the profile image of the user.
Downloaded Profile Image	The raw content of the user's profile image, downloaded from the URL shown in the 'Profile Image URL' column.
Post Image URL	The URL of the image in the post, if applicable.
Downloaded Post Image	The raw content of the image in the post, if applicable. Downloaded from the URL shown in the 'Post Image URL' column.
Posted Source	Information describing the device from where the post was made.
Latitude	Latitude of the post's source device when the post was made.
Longitude	Longitude of the post's source device when the post was made.

Sina Weibo Private Messages

Description	Stored data from private messages on the iOS Sina Weibo app.
Notes	

ATTRIBUTE	DESCRIPTION
Conversation Partner ID	The unique ID of the conversation partner.
Conversation Partner	The name of the conversation partner.
Message Date/Time - UTC (yyyy-mm-dd)	The date/time that the message was sent/received.

ATTRIBUTE	DESCRIPTION
Message	The actual private message content.
Profile Image URL	The URL for the profile image of the user.
Downloaded Profile Image	The raw content of the user's profile image, downloaded from the URL shown in the 'Profile Image URL' column.
Attachment Type	The type of attachment associated with the message.
Attachment Local File Path	The local path to the file attachment.

TikTok Contacts

Description	TikTok Contacts contains information about a user's contacts in TikTok.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The username of the contact.
Nickname	The nickname of the contact.
ID	The unique ID of the contact.
Profile Picture URL	The URL of the profile picture of the contact.

TikTok Messages

Description	TikTok Messages contains information about the messages a user sends or receives using TikTok.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the message.
Recipient	The recipient of the message.
Message	The content of the message.
Message Type	The type of the message.
Media URL	The URL of any media attached to the message.
Created Date/Time	The time the message was sent.
Read	Whether the recipient has read the message.
Deleted	Whether the message has been deleted

TikTok Videos

Description	TikTok Videos contains videos that were either viewed or created by the user.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	Name of the file.
File Extension	Extension of the file.
Image	A generated thumbnail of the video.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the video file was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the video file was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the vidoe was last written to.
Type	The type of the video.
Skin Tone Percentage	The amount of skin tone found in the video.
File Size (Bytes)	The size of the video in bytes.
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.

Tumblr Blocked Blogs

Description	Tumblr Blocked Blogs contains information about the blogs blocked by the local user.
Notes	

ATTRIBUTE	DESCRIPTION
Blog Title	The title of the blog.
Creator Name	The name of the blog's creator.
Blocked Date/Time - UTC (yyyy-mm-dd)	The date and time the blog was blocked.

Tumblr Chat Messages

Description	Messages sent and received using Tumblr.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	Display name of the user who sent the message.
Recipient	Display name of the user who received the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Message	The body of the message.
Media URL	The URL of any media attached to the message.

Tumblr Created Posts

Description	Tumblr Created Posts contains information about the blog posts created by the local user.
Notes	

ATTRIBUTE	DESCRIPTION
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the post was created.
Summary	The title of the post.
URL	The URL to the blog post.
Blog Title	The title of the post's blog.
Creator Name	The name of the post's creator.
Reblogged From	The name of the original creator, if this post was reblogged.

Tumblr Followed Blogs

Description	Tumblr Followed Blogs contains information about the blogs followed by the local user.
Notes	

ATTRIBUTE	DESCRIPTION
Blog Title	The title of the blog.
Description	The description of the blog.
Creator Name	The name of the blog's creator.
URL	The URL to the blog.

Tumblr Tags

Description	Tumblr Tags contains information about the subject tags the local user has selected. Selecting a tags expresses the user's interest in a subject so they can see more content of that type.

Notes	

ATTRIBUTE	DESCRIPTION
Tag	The tag that the local user selected.

Twitter Direct Messages

Description	Carved and noncarved direct messages from the Twitter app. Note: Carving may not retrieve the name and screen name of sender and receiver.
Notes	

ATTRIBUTE	DESCRIPTION
Text	The text of the direct message.
Sender ID	The twitter ID for the sender.
Recipient ID(s)	The twitter ID for the recipient(s).
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date and time that the direct message was sent or received.
Direction	Whether the message was sent or received.
Sender Name	Name of the person sending the direct message.
Sender Screen Name	Screen name or twitter handle of the person sending the direct message.
Recipient Name(s)	Name(s) of the person(s) receiving the direct message.
Recipient Screen Name(s)	Screen name(s) or twitter handle(s) of the person(s) receiving the direct message.

Twitter Tweets

Description	Carved and noncarved tweets from the Twitter app. Note: Carving older versions of the app will only recover the Tweet column.
Notes	This artifact can recover Tweet data locally in versions up to Twitter 8.2.1.0. In later versions, Tweet data is stored in the cloud and cannot be recovered unless you're running a cloud acquisition.

ATTRIBUTE	DESCRIPTION
Author ID	The numeric ID of the account that posted the tweet.
Status ID	The unique ID of the tweet.
Created Date/Time - UTC (yyyy-mm-dd)	The Date/Time at which the tweet was created.

ATTRIBUTE	DESCRIPTION
Tweet	The text content of the tweet.
Tweet Source	The interface used to post the tweet.
Favorited	Whether the tweet has been favorited.
Latitude	The latitude of the location from which the tweet was posted.
Longitude	The longitude of the location from which the tweet was posted.
Retweet Count	The number of times the tweet has been re-tweeted.

Twitter Users

Description	Contains friend information in Twitter data.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The friend's twitter user ID.
User Name	The friend's twitter username.
Profile Created Date/Time - UTC (yyyy-mm-dd)	The date and time the friend's Twitter profile was created.
Description	Short profile description the friend puts about themselves.
Web URL	The friend's website URL.
Following	'Yes' if the current Twitter user is following this account, 'No' otherwise.
Location	The location the friend is from.
Protected	
Followers	The number of followers the friend has.
Friends	The number of friends the friend has.
Statuses	The number of different status the friend has had.
Image URL	The URL to the friend's profile picture.
Friend Metadata Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the friend's meta information was last updated.
Header URL	The URL to the friend's profile banner picture.

VK Messages

Description	This artifact contains VK messages (either private or group messages) as well as the details about pictures, video, and audio that may have been sent.
Notes	

ATTRIBUTE	DESCRIPTION
Sender ID	The user ID of the message sender.
Receiver ID (s)	The user ID of the message recipient. This column can contain multiple user IDs if the message is from a group conversation.
Message Date/Time - UTC (yyyy-mm-dd)	The date/time the message was sent/received.
Message Text	The message text that was sent/received.
Type	The type of message sent. The possible types are 'Private Message' for one-to-one conversations or 'Group Message' for one-to-many conversations.
Message Deleted	Identifies whether or not a message has been deleted.
Read State	Identifies whether or not a message has been read.
Forwarded Message Content	This column contains the original time a message was sent, the user ID that originally sent the message, and the content (for example, text, video, or audio).
VK Attachment	This column contains details of the attachment that was sent. For picture attachments a URL to a scaled picture is provided for downloading. When a video is sent a thumbnail is provided with details of the video (title, date/time, duration and description). When audio is sent, a URL to the audio is provided as well as the title, artist, and duration.
Latitude	The latitude sent by the user. This point may represent the device's current location or a point the user selected from the world map.
Longitude	The longitude sent by the user. This point may represent the device's current location or a point the user selected from the world map.

VK Users

Description	This artifact contains the various users the data owner has been in communication with, as well as the users own profile.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The user ID of the user.
Gender	Identifies whether the user is a male or female.
Birthdate (yyyy-mm-dd)	The birthdate of the user.
First Name	The first name/given name of the user.
Last Name	The last name/surname of the user.

ATTRIBUTE	DESCRIPTION
Profile Image	The URL to the users profile image.

Whisper Messages

Description	Contains the messages that were sent and received between the local user and others.
Notes	

ATTRIBUTE	DESCRIPTION
Partner Name	The user name of the person the chat was with.
Message Text	The content of the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Status	The status of the message (received, sent, or send failed).
Read	Whether or not the message has been read when the message was received.
Image	The image that was sent or received.

Yik Yak Notifications

Description	Contains the notifications that have been generated for the user.
Notes	

ATTRIBUTE	DESCRIPTION
Thing Content	The content of the object the notification is about.
User ID	The identifier of the user the notification belongs to.
Thing Created Date/Time - UTC (yyyy-mm-dd)	The date and time the thing the notification is about was created.
Notification ID	The identifier of the notification.
Thing ID	The identifier of the thing the notification is about.
Thing Type	The type of the object the notification is about (for example, a Yak or a Comment).
Subject	The subject of the notification.
Notification Body	The body of the notification.
Reason	The reason for the notification (for example, a Vote or a Comment).
Status	The status of the notification (New, Unread, or Read).

Yik Yak Yaks

Description	Contains the Yaks the user has viewed on their home page.
Notes	

ATTRIBUTE	DESCRIPTION
Message	The content of the Yak.
Poster ID	The ID of the user who posted the Yak.
Posted Date/Time - UTC (yyyy-mm-dd)	The date and time the Yak was posted.
Message ID	The ID of the Yak.
Image URL	The URL to the image associated with the Yak (if one exists).
Downloaded Image	The image of the Yak that was downloaded.
User Vote	Indicates whether the user has voted on the Yak (Down, None, or Up).
Latitude	The latitude of the Yak.
Longitude	The longitude of the Yak.
Likes Count	The number of likes the Yak has.
Re-Yaked Count	The number of times the Yak has been Re-Yaked.
Comments Count	The number of comments the Yak has.

Transportation and Travel

Lyft Account Information

Description	Lyft Account Information stores information associated with the user's account.
Notes	

ATTRIBUTE	DESCRIPTION
First Name	The first name of the account holder.
Last Name	The last name of the account holder.
Email	The email associated with the account.
Phone Number	The phone number associated with the acount.
Share Code	A unique share code associated with the rider.
User ID	The user ID uniquely identifying the account.

Lyft Last Known Location

Description	Lyft Last Known Location contains the app user's last known location as recorded by the app.
Notes	

ATTRIBUTE	DESCRIPTION
Latitude	The GPS latitude of the last known location.
Longitude	The GPS longitude of the last known location.
Altitude (m)	The altitude in meters of the last known location.
Date/Time	The date and time when the location was recorded.

Lyft Rider Payment Details

Description	Lyft Rider Payment Details contains information about the user's payment profile.
Notes	

ATTRIBUTE	DESCRIPTION
Payment Method	The method of payment made (Apple Pay, etc.).
Payment Type	The type of payment made (Visa, MasterCard, etc.).
Payment Profile ID	The ID of the payment profile.
Card Display Name	The payment card display name.

OnStar RemoteLink Hotspot Info

Description	Information about the vehicle Wi-Fi hotspots associated with an OnStar account.
Notes	

ATTRIBUTE	DESCRIPTION
Network Name(SSID)	The name of the vehicle's hotspot.
Network Password	The password of the vehicle's hotspot.
Created Date/Time	The date and time the hotspot was created.
Updated Date/Time	The date and time the hotspot was updated.
VIN	The Vehicle Identification Number that the hotspot is associated with.

OnStar RemoteLink Remote Commands

Description	Information about commands sent from the device.
Notes	

ATTRIBUTE	DESCRIPTION
Requested Command	The command requested by the user.
Request State	The state of the request.
Sent Date/Time	The date and time the command was sent to the vehicle.
Completion Date/Time	The date and time the command was completed.
Command Description	The description of the command that was sent, if available.
VIN	The Vehicle Identification Number of the vehicle the command was sent to.
Request ID	The ID of the request that was sent, if available.

OnStar RemoteLink Saved Wireless Carrier

Description	Information about the wireless accounts associated with a vehicle.
Notes	

ATTRIBUTE	DESCRIPTION
Carrier Account ID	The account identifier of the carrier account.
Carrier Type Code	The code that represents the account type.
Carrier Type Description	The carrier associated with the account.
Created Date/Time	The date and time the account entry was created on the device.
Updated Date/Time	The date and time the account entry was updated on the device.
Account Type	The type of wireless account.
Account Description	The description of the account type.
VIN	The Vehicle Identification Number of the vehicle the wireless account is associated with.

OnStar RemoteLink Searches

Description	Possible locations searched.
Notes	

ATTRIBUTE	DESCRIPTION
Original Search Query	The original search query requested by the user.
Search Date/Time	The date and time of the search.
GPS Latitude	The GPS latitude where the search was performed.
GPS Longitude	The GPS longitude where the search was performed.
Location Name	The name or address of the result destination.
Type	The type of returned search results.
Distance (meters)	The distance, in meters, to the result destination.
Destination Latitude	The latitude of the result destination.
Destination Longitude	The longitude of the result destination.

OnStar RemoteLink Vehicle Diagnostics

Description	Information about the diagnostic values retrieved from the vehicle.
Notes	

ATTRIBUTE	DESCRIPTION
Diagnostic Name	The name of the diagnostic test that was retrieved.
Unit	The unit of measurement associated with the diagnostic test.
Value	The value associated with the diagnostic test.
Created Date/Time	The date and time the diagnostic value was retrieved.
Updated Date/Time	The date and time the diagnostic value was updated.
Completion Date/Time	The date and time the server retrieved the diagnostic value from the vehicle.
VIN	The Vehicle Identification Number of the vehicle that the diagnostic value was retrieved from.

OnStar RemoteLink Vehicle Info

Description	Information about the vehicle associated with the account.
Notes	

ATTRIBUTE	DESCRIPTION
VIN	The Vehicle Identification Number of the vehicle associated with the account.
Vehicle Make	The make of the vehicle.

ATTRIBUTE	DESCRIPTION
Vehicle Model	The model of the vehicle.
Year	The year of production of the vehicle.
Created Date/Time	The date and time the vehicle information was added to the device.
Updated Date/Time	The date and time the vehicle information was updated on the device.
Phone Number	The phone number associated with the vehicle.
Account Number	The OnStar account number that the vehicle is associated with.

Uber Accounts

Description	Uber Accounts contains account information for riders, as recovered from the Uber app (passenger only).
Notes	

ATTRIBUTE	DESCRIPTION
First Name	The first name of the account holder.
Last Name	The last name of the account holder.
Mobile Phone	The mobile phone number associated with the acount.
Share Code	A unique share code associated with the rider.
User ID	The user ID uniquely identifying the account.
Latitude (On App Startup)	The latitude of the user when the app was last opened.
Longitude (On App Startup)	The longitude of the user when the app was last opened.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the user last opened the app.
Last Payment Profile ID	The ID of the payment profile last used by the user.
Profile Image URL	The URL of the profile image for the account.

Uber Cached Locations

Description	Uber Cached Locations contains information about locations that Uber caches, such as the initial location on app startup or locations from a trip (passenger only).
Notes	

ATTRIBUTE	DESCRIPTION
Latitude	The GPS latitude of the cached location.
Longitude	The GPS longitude of the cached location.

ATTRIBUTE	DESCRIPTION
Address	The address of the cached location.
Date/Time - UTC (yyyy-mm-dd)	The date and time when the location was cached.
Tag	The user created tag given to the location.

Uber Locations

Description	Uber Locations contains the latitude and longitude of various locations, as recovered from the Uber app (passenger only).
Notes	

ATTRIBUTE	DESCRIPTION
Latitude	The recorded GPS latitude.
Longitude	The recorded GPS longitude.
Altitude (meters)	The altitude recorded for the current location.
Date/Time - UTC (yyyy-mm-dd)	The date and time the current location was saved.

Uber Payments

Description	Uber Payments contains payment information associated with a user's Uber rides, as recovered from the Uber app (passenger only).
Notes	

ATTRIBUTE	DESCRIPTION
Rider Name	The name of the passenger/rider.
Share Code	A unique share code associated with the rider.
Cost	The cost of the trip.
Currency	The currency used to measure the cost of the trip.
Duration (Seconds)	The duration of the trip, in seconds.
Distance (Kilometers)	The distance of the trip, in Kilometers.
Payment Method	The method of payment.
Card Display Name	The payment card display name.

Uber Profiles

Description	Uber Profiles contains information about a user's Uber profiles, as recovered from the Uber app (passenger only).
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	The name of the profile.
Profile Email	The email associated with the profile.
Profile User ID	The unique user ID (UUID) associated with the profile.
Profile Payment User ID	The unique user ID that is the payment method for this profile.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the profile was created.

Uber Rider Payment Details

Description	Uber Rider Payment Details contains information about the user's payment profile, such as their payment method and fare-splitting info (passenger only).
Notes	

ATTRIBUTE	DESCRIPTION
Card Display Name	The payment card display name.
Payment Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the payment is set to expire.
Payment Profile ID	The ID of the payment profile.
Status	The status of the payment
Payment Method	The type of payment made (Visa, MasterCard, etc.)
Country	The country associated with the payment profile.
ZIP/Postal Code	The zip code associated with the payment profile.
Last Fare Split Name	The name of the person who the user last split a ride fare with.
Last Fare Split Phone Number	The number of the person who the user last split a ride fare with.

Uber Trips

Description	Uber Trips contains information about a user's Uber rides, as recovered from the Uber app (passenger only).
Notes	

ATTRIBUTE	DESCRIPTION
Booking Date/Time UTC (yyyy-mm-dd)	The date/time when the trip was booked.
Origin Address	The address of the original start location.
Destination Address	The address of the final destination.
Arrival Date/Time UTC (yyyy-mm-dd)	The date/time when the vehicle arrived at the destination address.
Duration (Seconds)	The duration of the trip, in seconds.
Distance	The distance of the trip, units unknown.
Driver Name	The first name of the driver.
Vehicle Make	The make of the driver's vehicle.
Vehicle Model	The model of the driver's vehicle.
Vehicle Type	The type of uber car service.
Driver Rating	The driver's rating.
Driver Picture URL	URL to the driver's profile picture.
Cost	The cost of the trip.
Currency	The currency used to measure the cost of the trip.
Status	The status of the trip.
Route Map URL	URL to the route taken in the trip.

Waze Events

Description	Waze Events can contain information about upcoming trips that a user has planned.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the place.
Address	The house number and street name of the place.
City	The city of the address.
State	The state/province of the address.
Country	The country of the address.
Start Date/Time	The start date and time recommended for the planned drive.

ATTRIBUTE	DESCRIPTION
End Date/Time	The date and time the user has planned to arrive at the destination.
Created Date/Time	The date and time the event was created.
Is All-day Event	Indicates if the planned drive is an all-day event.
Latitude	The GPS Latitude coordinates of the place.
Longitude	The GPS Longitude coordinates of the place.

Waze Favorites

Description	Waze Favorites contains information about locations that a user has bookmarked as a favorite.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the place bookmarked as Favorite
Address	The house number and street name of the place.
City	The city of the address.
State	The state/province of the address.
Country	The country of the address.
Created Date/Time	The date and time the address was added as a favorite.
Modified Date/Time	The date and time that the favorite location was last modified by the user.
Accessed Date/Time	The date and time that the favorite location was last accessed in Waze.
Latitude	The GPS Latitude coordinates of the place.
Longitude	The GPS Longitude coordinates of the place.

Waze Places

Description	All the places the user has searched using Waze.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the place.
Address	The house number and street name of the place.
City	The city of the address.
State	The state/province of the address.
Country	The country of the address.

ATTRIBUTE	DESCRIPTION
Created Date/Time	The date and time the address was entered in Waze.
Accessed Date/Time	The last date and time the address was accessed in Waze.
Latitude	The GPS Latitude coordinates of the place.
Longitude	The GPS Longitude coordinates of the place.

Web Related

Bolt Browser Bookmarks

Description	Bolt Browser Bookmarks contains stored bookmark entries for the Bolt browser on iOS.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of a bookmarked webpage.
Title	The title of the webpage.
Created Date/Time	The date and time when the URL was bookmarked.

Bolt Browser History

Description	Bolt Browser History contains stored history entries for the Bolt browser on iOS.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of a visited webpage.
Title	The title of the webpage.
Created Date/Time	The date and time when the URL was visited.

Brave Tab History

Description	Brave Tab History contains the websites that the user visits in a particular tab, sorted by order they were visited.
Notes	

ATTRIBUTE	DESCRIPTION
Tab ID	The unique ID of the tab.
Visit Order	The order in which this URL was visited in the tab. Values start at 1 and increase with recency.
URL	The URL of the site visited in the tab.
Title	The title of the most recent webpage visited in the tab.

Brave Web History - iOS

Description	Brave Web History contains a history of all the websites the user visits (includes unique visits only).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Domain	The title of the domain associated to the webpage.
Domain Visit Count	The number of times the domain was visited.

Chrome

Google Chrome is free web browser developed by Google and is available on all major operating systems, for both mobile and desktop. As of 2016, Chrome usage represents over 70% of the world's total browser traffic.

Analyzing the websites a user visits and the time the visits occur can provide valuable insights about a user. One notable feature that Google Chrome has is that it allows users to sync their bookmarks, browsing history, and more across multiple platforms and devices by using cloud sync accounts.

FORENSIC NOTES

Web Visits vs Web History

Chrome has two distinct artifacts that are very similar nature: Chrome Web Visits and Chrome Web History. Both of these artifacts are recovered from the History database. Chrome Web History is parsed from the URLS table and only contains information for the last visited date of a particular website. Chrome Web Visits can contain multiple entries for the same website, giving the examiner a more complete look at browser usage if the user visited a website multiple times. For example, if a user visits www.magnetforensics.com six times, the Chrome Web History artifact displays only the last time the site is visited, while the Chrome Web Visits artifact potentially displays records for all six instances. Chrome Web Visits was added in a later version of Chrome than Chrome Web History.

Carved web history

The Chrome / 360 Safe Browser / Opera Carved Web History is essentially the same as Chrome Web History except that it's recovered using carving and you may find additional deleted hits with it. The 360 Safe and Opera browsers are included in this artifact because when the data is carved, it's not possible to tell which browser the hit comes from as they're all formatted the same way.

Autofill and profile data

Chrome stores field data that the user has previously input as autofill and profile settings. For example, if you visit magnetforensics.com and login to the customer portal, browsers automatically save your username (and other details) so that you don't have to type it in each time you visit the site. This data is helpful for recovering usernames and other information that your user has filled out on various sites.

Sessions and tabs

When the system has an active session available, Chrome stores the browsing activity as the Chrome Current Session and any tabs that are open as Chrome Current tabs. The previous session and tabs are maintained in Chrome Last Session and Chrome Last Tabs so that the user can restore the last session and tabs if Chrome is closed.

ARTIFACTS

RELATED RESOURCES

How does Chrome's 'incognito' mode affect digital forensics?

Forensic email analysis: browser artifacts you may find on a PC or laptop

Chrome Archived Keyword Search Terms

Description	Keyword search terms that were archived by the browser.
Notes	

ATTRIBUTE	DESCRIPTION
Keyword Search Term	The keyword search term the user entered.
URL	The URL of the keyword search.

Chrome Archived Web History

Description	An archived history of old webpage visits.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL where the archived web history is located.
Title	The title of the archived web history.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was visited.
Visit Count	Total visits to this URL.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
ID	ID for the web history archive.

Chrome Autofill Profiles

Description	Profiles that Chrome uses to fill in forms with saved values.
Notes	

ATTRIBUTE	DESCRIPTION
Name	Name for the autofill profile.
Email	Email used in the the autofill profile.
Number	Phone number used in the autofill profile.
Company	Company name used in the autofill profile.
Address Line 1	Address Line 1 used in the autofill profile.

ATTRIBUTE	DESCRIPTION
Address Line 2	Address Line 2 used in the autofill profile.
City	City used in the autofill profile.
State	State used in the autofill profile.
Zipcode	Zipcode used in the autofill profile.
Country	Country used in the autofill profile.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the profile was last modified.

Chrome Autofill

Description	Chrome Autofill contains records of the autofill values that Chrome saves for different types of text fields.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the autofill value.
Value	The saved autofill value for this type of field.
Count	Count of this autofill.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill was last used.

Chrome Bookmarks

Description	Browser bookmarks that reference saved webpages.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the bookmark.
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was added.
Parent	The name of the parent folder of the bookmark.

Chrome Cache Records

Description	Content that Chrome downloads and caches to speed up rendering times. Cached content can include pictures, text, html, javascript, and more.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the cached item.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was first visited.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The date and time the cache was last synced with the cloud.
File Type	The type of file that was cached.
Content Size (Bytes)	The size of the cached file.
Image	The cached image if the file type is an image. Otherwise, this column is empty.
Content	The cached file contents if the file type is not an image. Otherwise, this column is empty.

Chrome Cookies

Description	Cookies that Chrome downloads from the Internet that contain information about the websites that a user visits.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie expires.
Path	The path of the cookie value.

Chrome Current Session

Description	Information about the browser session that's currently underway.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL.
Title	The title of the web page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.

Chrome Current Tabs

Description	Information about the tabs that are open in the current browser session.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL.
Title	The title of the web page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.

Chrome Downloads

Description	Information about the files that a user downloads from the Internet.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	File name of the download.
Download Source	The URL of the file that was downloaded.
Saved To	Saved to location.
State	State of the download.
Opened By User	If the download is opened by the user.
Start Time Date/Time - UTC (yyyy-mm-dd)	Download start time.
End Time Date/Time - UTC (yyyy-mm-dd)	Download end time.

ATTRIBUTE	DESCRIPTION
Bytes Downloaded	The bytes that were downloaded.
File Size(Bytes)	File size of the download.

Chrome Favlcons

Description	Contains the favicons that Chrome displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	Page URL of the favicon.
Icon URL	Icon URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	Last time the favicon was updated.
Icon	A preview of the favicon.

Chrome History Index

Description	An index of the webpages the user has visited in the past.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	The URL of the webpage.
Title	The title of the webpage.
Visited On Date/Time - UTC (yyyy-mm-dd)	When the webpage was visited.
Body	A snippet of the webpage.

Chrome Keyword Search Terms

Description	Information about the keyword search terms that a user enters.
Notes	

ATTRIBUTE	DESCRIPTION
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.

Chrome Last Session

Description	Information about the previous browser session.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL.
Title	The title of the web page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Chrome Last Tabs

Description	Information about the tabs that were open during the previous session.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The web page URL.
Title	The title of the web page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Chrome Logins

Description	Login information that a user provides in Chrome. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the login page.
Username	The username entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the data was created.

Chrome Saved Credit Cards

Description	Contains the credit card information saved by the user.
Notes	

ATTRIBUTE	DESCRIPTION
GUID	GUID of the user.
Name On Card	The name of the person on the credit card.
Expiry Date	The date the credit card is supposed to expire in format 'month-year'.
Card Number	The number on the credit card.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the information was last modified.

Chrome Shortcuts

Description	Contains all of the shortcuts used by Google Chrome for user entered URLs.
Notes	

ATTRIBUTE	DESCRIPTION
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.
Last Access Date/Time - UTC (yyyy-mm-dd)	The last access time of the shortcut.
Web Page Title	The title of the web page.
Times Used	The number of times the shortcut has been used.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Type	The type of shortcut (for example, 'typed url' or 'bookmark').

Chrome Tab History

Description	A history of websites the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Notes	

ATTRIBUTE	DESCRIPTION
Tab ID	The unique ID of a tab entry in a tab file.
Entry ID	The unique ID of a web page entry in a tab.
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request to open the web page (for example, the referrer source might be from Google or another third-party application).
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.

Chrome Top Sites

Description	A list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Notes	

ATTRIBUTE	DESCRIPTION
URL	URL of the site.
Title	Title of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the site was last updated.
Rank	A ranking of the website, in terms of how frequently it was visited. A value of 1 indicates the most frequent and values increment to 8 as frequency decreases. A value of -1 indicates a site that the user manually added to the list of top sites.
Thumbnail	Thumbnail of the site

Chrome Web History

Description	A history of the websites that the user visits (includes unique visits only).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited page.

ATTRIBUTE	DESCRIPTION
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

Chrome Web Visits

Description	A history of the websites that the user visits (includes all visits).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited webpage.
Title	The title of the webpage that was visited.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Dolphin Browser Bookmarks

Description	Contains bookmarks from the Dolphin web browser on an iOS device.
Notes	The Visits field is always empty for iOS.

ATTRIBUTE	DESCRIPTION
Title	The title of the bookmark.
URL	The URL of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was added.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was modified.
Visits	The number of time the user visited this bookmark.

Dolphin Browser History

Description	Contains the web page history from the Dolphin web browser on an iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the web page.
URL	The URL of the web page.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the user first visited the web page.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the user last visited the web page.
Visits	The number of times the user has visited that web page.

DuckDuckGo Bookmarks

Description	DuckDuckGo Bookmarks contains information about the webpages that a user has bookmarked.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the bookmark.
Name	The name of the bookmark.
Favorite	Indicates whether the link was added as a favorite.

DuckDuckGo Current Tabs

Description	DuckDuckGo Current Tabs contains information about the tabs that are open in the current DuckDuckGo browser session.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the webpage.
Title	The title of the webpage.
Was Viewed	Indicates whether the tab was viewed or not.
Accessed Date/Time - UTC (yyyy-mm-dd)	This fragment is only populated for Android.
Attachment Path	This fragment is only populated for Android.

DuckDuckGo Whitelisted Websites

Description	DuckDuckGo Whitelisted Websites contains information on domains that have been added by the user to the whitelist or fireproof list of domains.
Notes	

ATTRIBUTE	DESCRIPTION
Domain	The domain that was added by the user to either the whitelist or fireproof list of domains.
Status	The whitelisted or fireproofed status of a domain. The same domain may be added to one or both domain lists. A whitelisted domain allows for third-party trackers and a fireproofed domain saves cookies even after the application has been closed.

Ecosia Bookmarks

Description	Ecosia Bookmarks contains the webpages that a user has bookmarked in the browser.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark

Ecosia Current Tabs

Description	Ecosia Current Tabs contains information about the tabs that the user currently has open in the browser.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL.
Title	The title of the web page.
Last Opened Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last opened.
Visit Count	The number of times the user accessed the URL.

Ecosia Web History

Description	Ecosia Web History contains information about the webpages that a user has visited (includes unique visits only).
Notes	

ATTRIBUTE	DESCRIPTION
Tab ID	The unique ID of the tab.
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.

Edge Chromium Bookmarks

Description	Browser bookmarks that reference saved webpages.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Edge Chromium FavIcons

Description	Contains the favicons that Chrome displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	The page URL of the favicon.
Updated Date/Time - UTC (yyyy-mm-dd)	The last time the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Edge Chromium Logins

Description	Login information that a user provides in Chrome. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The user name entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the data was created.
URL	The URL of the login page.

Edge Chromium Web History

Description	A history of the web sites that a user has visited. Each artifact hit represents a unique web page visit, whereas subsequent visits to the same page are tracked by its Visit Count.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited. The value for this fragment is interpreted to show the actual visit count. Whereas the source data starts counting at 0 (0 indicates a single visit occurred) the value that is displayed here is the actual visit count (1 indicates a single visit).
Typed Count	This fragment is not populated for iOS.

Google Analytics First Visit Cookies

Description	Information about Google Analytics first-visit cookies that are discovered in other artifacts.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the URL.
Creation DateTime	Date/Time when the site was vist visited.
Most Recent Visit Date/Time	Date/Time of most recent session.
2nd Most Recent Visit Date/Time	Date/Time of previous session.
Hits	Number of visit.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Google Analytics First Visit Cookies Carved

Description	Information about Google Analytics first-visit cookies that are recovered using carving.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the URL.
Creation DateTime	Date/Time when the cookie was created.
Most Recent Visit Date/Time	Date/Time of most recent session.
2nd Most Recent Visit Date/Time	Date/Time of previous session.
Hits	Number of visit.

Google Analytics Referral Cookies

Description	Information about Google Analytics referral cookies that are discovered in other artifacts.
Notes	

ATTRIBUTE	DESCRIPTION
Cookie Source	The source URL used to reach the site.
Host	Contains the domain of the URL.
Update Date/Time	The last time the cookie was updated.
Campaign	The method of referral.
Access Method	Whether the site was accessed organically or was referred.
Keyword	Keywords used to arrive at the site.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Google Analytics Referral Cookies Carved

Description	Information about Google Analytics referral cookies that are recovered using carving.
Notes	

ATTRIBUTE	DESCRIPTION
Cookie Source	The source URL used to reach the site.
Host	Contains the domain of the URL.
Update Date/Time	The last time the cookie was updated.
Campaign	The method of referral.
Access Method	Whether the site was accessed organically or was referred.
Keyword	Keywords used to arrive at the site.

Google Analytics Session Cookies

Description	Information about Google Analytics session cookies that are discovered in other artifacts.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the URL.
Page Views	The number of visits to this page from the user.
Start Current Session Date/Time	The start time of the current sesion.
Outbound Link Events Left	
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Google Analytics Session Cookies Carved

Description	Information about Google Analytics session cookies that are recovered using carving.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the URL.
Page Views	The number of visits to this page from the user.
Start Current Session Date/Time	The start Date/Time of the current sesion.

ATTRIBUTE	DESCRIPTION
Outbound Link Events Left	

Google Analytics URLs

Description	URLs that are discovered in other artifacts that are related to Google Analytics.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the web site. If the url cannot be recovered, the source of the url containing all the metadata is displayed instead.
Page Title	The name of the web site. This value is carved from the source starting after 'utmdt=' and ending at '&'
Host Name	Contains the domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Google Analytics URLs Carved

Description	Information about Google Analytics URLs that are recovered using carving.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the web site. If the url cannot be recovered, the source of the url containing all the metadata is displayed instead.
Page Title	The name of the web site. This value is carved from the source starting after 'utmdt=' and ending at '&'
Host Name	Contains the domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'

ATTRIBUTE	DESCRIPTION
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'

iOS Google Map Coordinates

Description	Google map coordinates viewed on an iOS device.
Notes	

ATTRIBUTE	DESCRIPTION
X Coordinate	The map X coordinate.
Y Coordinate	The map Y coordinate.
Zoom Level	The zoom level within the map.
Image	The Google map image for the location specified by the X, Y coordinates.
Last Touched Date/Time - UTC (yyyy-mm-dd)	The last date and time the coordinates were touched.

iOS Safari Cache

Description	Locally cached content from the Safari browser on iOS.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the cached content.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date the cached content was created on the local device.
File Type	The type of the cached file (html, js, css, jpeg, etc.)
Content Size (Bytes)	The size of the cached content, in bytes.
Image	The raw content of the cached image. Blank if the content is not an image (i.e. it's html, js, css, etc.)
Content	The raw cached content. Blank if the content is an image (in which case, the 'Image' column will be populated instead).

iOS Safari Recent Search Terms

Description	iOS Safari Recent Search Terms contains the search terms that a user runs in the Safari browser.
Notes	

ATTRIBUTE	DESCRIPTION
Search Term	The term that was searched.
Search Date/Time	The date and time of the search.

Malware/Phishing URLs

Description	Records that are believed to be either malware or phishing related URLs.
Notes	

ATTRIBUTE	DESCRIPTION
Site Name	The name of the web site.
URL	The URL of the web site.
Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the artifact.
Artifact	The name of the artifact the URL belongs to.
Artifact ID	The row Id of the URL in the original artifact table.

Pornography URLs

Description	Records that are believed to be pornography related URLs.
Notes	You can find a list of the domains that are supported by this refined result at Pornography URLs.

ATTRIBUTE	DESCRIPTION
Site Name	The name of the web site.
URL	The URL of the web site.
Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the artifact.
Artifact	The name of the artifact the URL belongs to.
Artifact ID	The row Id of the URL in the original artifact table.

Potential Browser Activity

Description	The Browser Activity artifact will recover browser-related URLs. This includes Chrome Incognito and Firefox Private Browsing URLs, HTTP request artifacts from multiple browsers, and regular web browsing artifacts. This does not include metadata such as the Windows username, dates/-times, and so on. Note that some recovered URLs can be from background browser processes related to certificate authorities, etc.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL that the request was sent to.
User Agent	The string that represents the browser that sent the request.

Puffin Browser Bookmarks

Description	Contains bookmarks from the Puffin Browser for iOS.
Notes	Created Date/Time, Last Accessed Date/Time, and Visits are empty for iOS Puffin Browser Bookmarks.

ATTRIBUTE	DESCRIPTION
Title	The title of the bookmark.
URL	The URL of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was added.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the user last visited the web page.
Visits	The number of times the user visited this bookmark.

Puffin Browser History

Description	Contains the web history for the Puffin Browser for iOS.
Notes	Last Accessed Date/Time - UTC and Visits are empty for iOS Puffin Browser History.

ATTRIBUTE	DESCRIPTION
Title	The title of the web page.
URL	The URL of the web page.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the user last visited the web page.

ATTRIBUTE	DESCRIPTION
Last Accessed Date/Time - Local Time (yyyy-mm-dd)	The date and time the user last visited the web page.
Visits	The number of times the user has visited that web page.

Rebuilt Webpages

Description	Contains the data that allows for the reconstruction of web pages.
Notes	

ATTRIBUTE	DESCRIPTION
Page Title	The title.
URL	The URL.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the original record was created.
Domain	The domain.
Cache Table	The table the data to re-construct the page came from.
Cache RowID	The row id in the table that constructed the rebuilt web page.

Reddit Accounts

Description	Reddit Accounts contains information about the user accounts that are used to log in to the Reddit app on the device.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The Reddit user ID.
Created Date/Time - UTC (yyyy-mm-dd)	The creation date time of the Reddit account.

Reddit Posts

Description	Reddit Posts contains information about the posts recovered from the device. These posts might be ones the user has read or created on their device.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the Reddit post.
Subreddit Name	The subreddit name where the post was posted.
Author	The author of the post.
Over 18	Indicates whether or not the post was flagged as mature content.
Content Link	The URL to content from the post if applicable, or the URL to the post if there is no external content.
URL	The URL of the source. This URL is not recovered from the source as is, but is constructed using the Post ID.
Saved	Indicates whether or not the post was saved by the user.
Read Date/Time - UTC (yyyy-mm-dd)	The date and time that the user read the post.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the post was created.

Reddit Recently Visited Subreddits

Description	Reddit Recently Visited Subreddits contains information about the subreddits a user has recently visited while on their device.
Notes	

ATTRIBUTE	DESCRIPTION
Subreddit Name	The name of the subreddit.
Sort Order	The order in which posts were sorted within the subreddit (e.g. NEW, HOT, TOP, CONTROVERSIAL).
Sort Time Frame	The time frame in which posts were sorted within the subreddit (e.g. DAY, WEEK, MONTH, YEAR).
Description	The public facing description of the subreddit.
User Name	The user who visited the subreddit.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the user last visited the subreddit.
Created Date/Time - UTC (yyyy-mm-dd)	The creation date and time of the subreddit.

Safari Bookmarks

Description	Stored bookmarks for the Safari browser on iOS.

Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the bookmarked webpage.
Title	The title of the webpage.
Type	The type of bookmark (ie. Bookmark, Favourite, Reading List Item, etc.)
Read	If the bookmark type is a Reading List Item, this indicates whether the item has been read. This attribute is empty for all other types.
Date Added Date/Time - UTC (yyyy-mm-dd)	If the bookmark type is a Reading List Item, this indicates the date and time that the webpage was added. This attribute is empty for all other types.
Last Visited Date/Time - UTC (yyyy-mm-dd)	If the bookmark type is a Reading List Item, this indicates the date and time that the item was last visited. This attribute is empty for all other types.
Locally Added	Indicates whether the bookmark was created on the local device or a synced device with the same Apple ID.

Safari Downloads

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures information related to files that have been downloaded from Safari.
Notes	

ATTRIBUTE	DESCRIPTION
Download URL	The URL of the downloaded file.
Saved to Path	The local path where the download was saved.
Download Identifier	The unique identifier for the download.
Amount Downloaded (Bytes)	The number of bytes downloaded.
Size of Download (Bytes)	The size of the download in bytes.

Safari History

Description	Stored history entries for the Safari browser on iOS.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of a visited web page.

ATTRIBUTE	DESCRIPTION
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Redirect URL	The URL the user was redirected to.
Title	The title of the web page.
Visit Count	The number of times the URL was visited.
Visit Source	Whether the website was viewed on the local device or on a synced device.

Safari iCloud Devices

Description	Safari iCloud Devices contains information about the devices that are synced to an iCloud account. Each device can access any browser tabs that are synced to the account.
Notes	

ATTRIBUTE	DESCRIPTION
Unique Device Identifier	A unique ID for the device that is accessing the tab.
Device Name	The name of the device that is linked to the iCloud account.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the device first synced to the iCloud account.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the device last synced with the iCloud account.

Safari iCloud Tabs

Description	Safari iCloud Tabs contains information about tabs that have been opened in the browser and synced to an iCloud account. Synchronized tabs are available to any device that logs in to the iCloud account.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the tab.
URL	The URL address of the tab.
Unique Device Identifier	A unique ID for the device that is accessing the tab.
Device Name	The name of the device that is accessing the tab.
Tab ID	The unique ID of the tab.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the tab was created.

ATTRIBUTE	DESCRIPTION
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the tab was last modified.
Modified By	The name of the device that last modified the tab.
Close Requested	Indicates whether a close request has been opened for the tab.
Close Request Date/Time - UTC (yyyy-mm-dd)	The date and time when the close request was created.

Safari Tabs

Description	Safari Tabs contains the web page history of each browser tab that is currently open on the device.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The web page URL.
Title	The title of the web page.
Last Viewed Date/Time	The date and time the tab was last opened. Only the web page that is currently opened in the tab will contain a value for this attribute.
Visit Order	The browsing order of the pages viewed in the tab. 0 indicates the most recent view.
Private Browsing	Indicates whether the web page was viewed using the private browsing setting.
Tab ID	The ID of the tab that the web page was visited in.

WebKit Browser Session/Tabs (Carved)

Description	WebKit Browser Sessions/Tabs contains information about the browser sessions and tabs that the user has open, while using a browser built with WebKit. Some examples of browsers that use WebKit are Chrome, Opera, and 360 Safe Browser. This artifact consolidates the existing Chrome, Safe Browser, and Opera equivalents in a single artifact. Usage of other browsers, such as Firefox and Safari, aren't likely to appear under this artifact.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The web page URL.
Title	The title of the web page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.

ATTRIBUTE	DESCRIPTION
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

WebKit Browser Web History (Carved)

Description	WebKit Browser Web History contains information about the websites that a user visits while using a browser built with WebKit. Some examples of browsers that use WebKit are Chrome, Opera, and 360 Safe Browser. This artifact consolidates the existing Chrome, Safe Browser, and Opera equivalents in a single artifact. Usage of other browsers aren't likely to appear under this artifact, however, some URLs found by other browsers may also be found by this artifact.
Notes	

ATTRIBUTE	DESCRIPTION
URL	URL of the visited webpage.
Title	Title of the visited webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time this webpage was last visited
Visit Count	The number of times the webpage was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

Whale Autofill

Description	Whale Autofill contains records of the autofill values that Whale saves for different types of text fields.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill was last used.
Value	The saved autofill value for this type of field.
Count	Count of this autofill.

Whale Bookmarks

Description	Browser bookmarks that reference saved webpages.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark

Whale Cookies

Description	Cookies that Whale downloads from the Internet that contain information about the websites that a user visits.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie expires.
Path	The path of the cookie value.

Whale Downloads

Description	Information about the files that a user downloads from the Internet.
Notes	

ATTRIBUTE	DESCRIPTION
Download Source	The URL of the file that was downloaded.
File Name	The name of the downloaded file.

ATTRIBUTE	DESCRIPTION
Start Time Date/Time - UTC (yyyy-mm-dd)	Date and time the downloaded was started.
End Time Date/Time - UTC (yyyy-mm-dd)	Date and time the downloaded finished.
Saved To	Absolute path on the device to the file downloaded.
State	The completion state of the download.
Opened By User	Indicates whether the user has opened the downloaded file or not.
Bytes Downloaded	The bytes that were downloaded.
Total Bytes	File size of the download.

Whale Favicons

Description	Contains the favicons that Whale displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	Page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	Last time the favicon was updated.
Icon URL	Icon URL of the favicon.
Icon	A preview of the favicon.

Whale Keyword Search Terms

Description	Information about the keyword search terms that a user enters.
Notes	

ATTRIBUTE	DESCRIPTION
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.

Whale Logins

Description	Login information that a user provides in Whale. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the login page.
Username	The username entered.
Password	The encrypted password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the data was created.

Whale Top Sites

Description	A list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Notes	

ATTRIBUTE	DESCRIPTION
URL	URL of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the site was last updated.
Title	Title of the site.
Thumbnail	Thumbnail of the site

Whale Web History

Description	A history of the websites that the user visits (includes unique visits only).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

Whale Web Visits

Description	A history of the websites that the user visits (includes all visits).

Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Yandex Autofill

Description	Yandex Autofill contains records of the autofill values that Yandex saves for different types of text fields.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill was last used.
Value	The saved autofill value for this type of field.
Count	Count of this autofill.

Yandex Bookmarks

Description	Browser bookmarks that reference saved webpages.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.

ATTRIBUTE	DESCRIPTION
Type	The type of bookmark

Yandex Cookies

Description	Cookies that Yandex downloads from the Internet that contain information about the websites that a user visits.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie expires.
Path	The path of the cookie value.

Yandex Downloads

Description	Information about the files that a user downloads from the Internet.
Notes	

ATTRIBUTE	DESCRIPTION
Download Source	The URL of the file that was downloaded.
File Name	The name of the downloaded file.
Start Time Date/Time - UTC (yyyy-mm-dd)	Date and time the downloaded was started.
End Time Date/Time - UTC (yyyy-mm-dd)	Date and time the downloaded finished.
Saved To	Absolute path on the device to the file downloaded.
State	The completion state of the download.
Opened By User	Indicates whether the user has opened the downloaded file or not.
Bytes Downloaded	The bytes that were downloaded.
Total Bytes	File size of the download.

Yandex Favicons

Description	Contains the favicons that Yandex displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	Page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	Last time the favicon was updated.
Icon URL	Icon URL of the favicon.
Icon	A preview of the favicon.

Yandex Keyword Search Terms

Description	Information about the keyword search terms that a user enters.
Notes	

ATTRIBUTE	DESCRIPTION
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.

Yandex Logins

Description	Login information that a user provides in Yandex. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the login page.
Username	The username entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the data was created.

Yandex Shortcuts

Description	Contains all of the shortcuts used by Yandex for user entered URLs.
Notes	

ATTRIBUTE	DESCRIPTION
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.
Last Access Date/Time - UTC (yyyy-mm-dd)	The last access time of the shortcut.
Web Page Title	The title of the web page.
Times Used	The number of times the shortcut has been used.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Type	The type of shortcut (for example, 'typed url' or 'bookmark').

Yandex Sync Data

Description	Yandex Sync Data contains information about the data that Yandex has synced to a user's account in the cloud.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the sync key.
Local Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the value on the local system.
Server Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the value on the server.
Local Created Date/Time - UTC (yyyy-mm-dd)	The created time of the value on the local system.
Server Created Date/Time - UTC (yyyy-mm-dd)	The created time of the value on the server.
Type	The type of data that is synced (bookmark, favicon, type URL, and so on).
Parsed Content	The type parsed data.
Favicon Image	The actual favicon image.

Yandex Top Sites

Description	A list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Notes	

ATTRIBUTE	DESCRIPTION
URL	URL of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the site was last updated.
Title	Title of the site.
Thumbnail	Thumbnail of the site

Yandex Web History

Description	A history of the websites that the user visits (includes unique visits only).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

Yandex Web Visits

Description	A history of the websites that the user visits (includes all visits).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.

ATTRIBUTE	DESCRIPTION
Title	The title of the webpage that was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

MACOS

Additional Sources

Android Backups

Description	Android Backups contains information about any backups of Android devices that are recovered from the computer. If an Android backup is recovered during a search, you can search the contents of the backup for additional artifacts.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the backup file.
File Path	The path where the backup was stored on the computer.
Encryption	The type of encryption (if any) that was used on the backup.
File System Created Date/Time - UTC (yyyy-mm-dd)	The creation date/time for the ab file from the file system.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date/time for the ab file from the file system.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date/time for the ab file from the file system.

Apple Disk Images

Description	Apple disk images are commonly stored as DMG or IMG files. These files are containers that may contain additional items of interest. This artifact identifies any Apple disk image found on the system.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the Apple disk image file.
File Path	The path where the Apple disk image was stored on the computer.

ATTRIBUTE	DESCRIPTION
File Type	The type of Apple disk image file (DMG or IMG).
File System Created Date/Time - UTC (yyyy-mm-dd)	The creation date/time for the file from the file system.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date/time for the file from the file system.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date/time for the file from the file system.

iOS Backups

Description	iOS Backups contains information about any backups of iOS devices that are recovered from the computer. If an iOS backup is recovered during a search, you can search the contents of the backup for additional artifacts.
Notes	

ATTRIBUTE	DESCRIPTION
Device Phone Name	The name of the iOS device from which the backup originated.
Device Phone Number	The phone number of the iOS device from which the backup originated.
IMEI	The IMEI of the iOS device from which the backup originated.
ICCID	The ICCID of the iOS device from which the backup originated.
Backup File Creation Date/Time	The Date/Time that the backup was created.
Product Name	The model of the iOS device from which the backup originated.
Product Version	The version of iOS of the device at the time of the backup creation.
Serial Number	The serial number of the iOS device from which the backup originated.

Chat

iMessage Archived Chats

Description	iMessage Archived Chats contains information from messages that have been archived on the macOS computer. iMessage allows users to chat using text, video, and audio and is a standard on almost all iOS and macOS devices.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the message.
Recipient	The recipient of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Message	The message content.
Read Status	The read status of the message.
Attachment Name(s)	The attachment file names, recovered from the ichat file.

iMessage Archived Messages

Description	iMessage Archived Chats contains information from messages that have been archived on the macOS computer. iMessage allows users to chat using text, video, and audio and is a standard on almost all iOS and macOS devices.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the message.
Recipient	The recipient of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Message	The message content.
Read Status	The read status of the message.

iMessage Chats

Description	iMessage (previously iChat) is a chat application for Apple products that allows users to communicate via text chat, video, and audio. Users can also share files. iMessage is standard on almost all Mac computers and iOS devices.
Notes	

ATTRIBUTE	DESCRIPTION
Recipient	The recipient of the message.
Sender	The sender of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Message	The message content.
Type	The type of message.
Status	The sent status of the message.

iMessage Messages

Description	iMessage (previously iChat) is a chat application for Apple products that allows users to communicate via text chat, video, and audio. Users can also share files. iMessage is standard on almost all Mac computers and iOS devices.
Notes	

ATTRIBUTE	DESCRIPTION
Recipient	The recipient of the message.
Sender	The sender of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Message	The message content.
Type	The type of message.
Status	The sent status of the message.

Skype Accounts

Description	Information about the Skype accounts that are recovered, such as user info and when the account was created.
Notes	

ATTRIBUTE	DESCRIPTION
Skype Name	Skype name of the account
Display Name	Display name of this account
Full Name	Full Name of this account
Birthday (yyyy-mm-dd)	Birthday of this account
Gender	Gender of this account
City	City where this account is located
State/Province	State/Province this account is located
Country	Country this account is located
Home Phone	Home phone of this contact
Office Phone	Office phone of this account
Mobile Phone	Mobile phone of this account
Email(s)	Email of this account
Homepage	Homepage of this contact
About Info	About info of this contact

ATTRIBUTE	DESCRIPTION
Profile Created On Date/Time - UTC (yyyy-mm-dd)	The date when the profile was created
Profile Last Modified On Date/Time - UTC (yyyy-mm-dd)	The date when the profile was last modified
Mood Text	Text used to express mood
Last Online On Date/Time - UTC (yyyy-mm-dd)	Last time the account was online
Last used On Date/Time - UTC (yyyy-mm-dd)	Last time the account was used
Avatar Timestamp Date/Time - UTC (yyyy-mm-dd)	Avatar created time
Image	Image for this contact

Skype Activity

Description	Skype Activity contains interactions that occur between users on Skype. These interactions include messages, group interactions, calls, files sent/received, and SMS. Applies to Skype 8.1 and later.
Notes	

ATTRIBUTE	DESCRIPTION
Conversation ID	ID of this conversation.
Profile Name	The local user's profile name.
Sender	The username of the sender/initiator of the interaction.
Sender Email	The sender's email as given in the message (if available).
Recipient Name(s)	The recipients or targets of the interaction.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the interaction was initiated.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the interaction was last updated (for example, when a call ends).
Message Type	The type of the interaction.
Message	The content of the message or summary of the interaction.
Emotion Count	The number of reactions to the interaction (for example, likes, dislikes, emojis, and so on).
File Name	The name of any attached files associated with the interaction.
File Size (Bytes)	The size in bytes of any attached files.
File	The attachment file (if applicable).
Attachment Data Recovered	Whether the attached file was recovered from the local filesystem.
Thumbnail URL	A URL that directs to the thumbnail picture (if applicable).
Call Duration (Seconds)	The length of the call in seconds (if applicable).

ATTRIBUTE	DESCRIPTION
Metadata	The content of the message, if it consisted of interpreted data (that is, XML or JSON data, rather than plain text).

Skype Contacts

Description	Information about Skype contacts that are recovered, which may or may not be added contacts.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	Profile name of the user
Skype Name	Skype name of the contact
Display Name	Display name of this account
Is Blocked	Is this contact blocked?
Contact Added	Specifies whether the contact is an added contact or just cached into the database (1 if the contact was added, 0 otherwise). Contacts can be cached into the database for a variety of reasons (for example, as a 'suggested contact').
Full Name	Full Name of this account
Birthday (yyyy-mm-dd)	Birthday of this account
Gender	Gender of this account
City	City where this account is located
State/Province	State/Province this account is located
Country	Country this account is located
Home Phone	Home phone of this contact
Office Phone	Office phone of this account
Mobile Phone	Mobile phone of this account
PSTN Number	PSTN number of this contact
Email(s)	Email of this account
Homepage	Homepage of this contact
About Info	About info of this contact
Profile Loaded Date/Time - UTC (yyyy-mm-dd)	Previously called "Profile Created On Date/Time", this fragment represents the date/time when a contact's profile is first created on the user's device. When the profile information is updated by the contact, the date in the database is also updated.
Mood Text	Text used to express mood
Last Online On Date/Time - UTC (yyyy-mm-dd)	Last time the account was online

ATTRIBUTE	DESCRIPTION
Last used On Date/Time - UTC (yyyy-mm-dd)	Last time the account was used
Avatar Timestamp Date/Time - UTC (yyyy-mm-dd)	Avatar created time
Image	Image for this contact

Skype Group Chat

Description	Information about the Skype group chats that a user is a part of.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	The name of the user.
Chat ID	The group chat's unique identifier.
Participants	The participants of the chat.
Posters	The users that have posted to the chat.
Active Members	The currently active users of the group.
Chat name	The name of the chat.
Started Date/Time - UTC (yyyy-mm-dd)	The date and time the chat started.
Last Changed Date/Time - UTC (yyyy-mm-dd)	The date and time the chat was modified.
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Documents

CSV Documents

Description	CSV documents (.csv) that are located on the system.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
File Name	The name of the CSV document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was last modified.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was created.
File Content	The content of the CSV document.
Size (Bytes)	The size of the CSV document in bytes.
SHA1 Hash	The SHA1 hash of the contents of the document.
MD5 Hash	he MD5 hash of the contents of the document.

Excel Documents

Description	Microsoft Excel is a spreadsheet processor developed by Microsoft.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified on the filesystem.
Size (Bytes)	The size of the document in bytes.
Saved Size (Bytes)	The size of the document (in bytes) that was recovered. Extremely large documents may not be fully recovered.
File	The actual file.
Title	The title meta-data.
Subject	The subject meta-data.

ATTRIBUTE	DESCRIPTION
Authors	The authors of the document.
Keywords	The keywords meta-data in the document.
Comments	The comments meta-data.
Last Author	The last author to edit the document.
Last printed Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last printed, extracted from meta-data within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last modified, extracted from meta-data within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the document was created, extracted from meta-data within the document.
Company	The company meta-data.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

PDF Documents

Description	Portable Document Format (PDF) is a file format used to present documents in a manner independent of application software, hardware, and operating systems. This table captures documents in this file format, extracted from the filesystem and carved from unallocated space.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified on the filesystem.
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
Title	The title of the file.
Subject	The subject of the file.
Authors	The authors of the file.
Keywords	The keywords in the metadata of the file.

ATTRIBUTE	DESCRIPTION
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the document was created, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last modified, extracted from metadata within the document.
File	The PDF file.
MD5 Hash	An MD5 hash of the PDF content.
SHA1 Hash	A SHA1 hash of the PDF content.

PowerPoint Documents

Description	Micrsoft PowerPoint is a presentation creator developed by Microsoft. This table captures documents created with PowerPoint, extracted from the filesystem and carved from unallocated space.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified on the filesystem.
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
File	The actual file.
Title	The title of the file.
Subject	The subject of the file.
Authors	The authors of the file.
Keywords	The keywords in the metadata of the file.
Comments	The comments in the metadata of the file.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last modified, extracted from metadata within the document.

ATTRIBUTE	DESCRIPTION
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the document was created, extracted from metadata within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

RTF Documents

Description	The information for each RTF document that was recovered from the search.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the RTF document.
File Size (Bytes)	The size of the RTF document in bytes.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the RTF document was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the RTF document was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the RTF document was last modified.
File Content	The contents of the RTF document.

Text Documents

Description	Text documents (.txt) that are located on the system.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the text document.
Size (Bytes)	The size of the text document in bytes.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The Date/Time that the text document was last modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The Date/Time that the text document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The Date/Time that the text document was created.

Word Documents

Description	Microsoft Word is a word processor developed by Microsoft.

Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified on the filesystem.
Size (bytes)	The size of the document.
Saved Size (bytes)	The size of the document that was recovered. Extremely large documents may not be fully recovered.
File	The actual file.
Title	The title meta-data.
Subject	The subject meta-data.
Authors	The authors of the document.
Keywords	The keywords meta-data in the document.
Comments	The comments meta-data.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyy-mm-dd)	The date and time the document was last printed extracted from meta-data within the document.
Last Modified Date/Time - UTC (yyy-mm-dd)	The date and time the document was last modified, extracted from meta-data within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the document was created, extracted from meta-data within the document.
Company	The company meta-data.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.
Source	The location of where the artifact was found.
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

E-mail

Calendar Events (ICS)

Description	Calendar Events (ICS) contains information about events and appointments that are recovered from calendar .ics files. These files are used by many different email applications, including Outlook, Google Calendar, and Apple Calendar.
Notes	

ATTRIBUTE	DESCRIPTION
ID	A unique ID for the calendar entry.
Type	The type of event (for example, Event, TODO, Journal).
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the event was created.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the event starts.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the event ends.
Summary	A short summary of the event.
Description	Provides a more complete description of the event.
Latitude	The latitude coordinates of the event's venue.
Longitude	The longitude coordinates of the event's venue.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time in which the event was last modified.
Location Name	The name of the venue in which the event is held.
Organizer	The organizer of the calendar event.
Status	The current pending status of the event (for example, NEEDS-ACTION, ACCEPTED, DECLINED, TENTATIVEB, DELEGATED, COMPLETED, IN-PROGRESS).
URL	The URL that is associated with the event.
Recurrence	Indicates whether the event is recurring.
Attendees	A list of attendees for the event.
Categories	The tags that are associated with the event.
Comment	A comment the organizer writes for to the user.
Contact Label	A reference of contacts associated with the event.
Resources	A list of resources and equipment required for the event.
Timezone	The timezone in which the event is held.

Email

Calendar Events (ICS)

Description	Calendar Events (ICS) contains information about events and appointments that are recovered from calendar .ics files. These files are used by many different email applications, including Outlook, Google Calendar, and Apple Calendar.
Notes	

ATTRIBUTE	DESCRIPTION
ID	A unique ID for the calendar entry.
Type	The type of event (for example, Event, TODO, Journal).
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the event was created.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the event starts.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the event ends.
Summary	A short summary of the event.
Description	Provides a more complete description of the event.
Latitude	The latitude coordinates of the event's venue.
Longitude	The longitude coordinates of the event's venue.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time in which the event was last modified.
Location Name	The name of the venue in which the event is held.
Organizer	The organizer of the calendar event.
Status	The current pending status of the event (for example, NEEDS-ACTION, ACCEPTED, DECLINED, TENTATIVEB, DELEGATED, COMPLETED, IN-PROGRESS).
URL	The URL that is associated with the event.
Recurrence	Indicates whether the event is recurring.
Attendees	A list of attendees for the event.
Categories	The tags that are associated with the event.
Comment	A comment the organizer writes for to the user.
Contact Label	A reference of contacts associated with the event.
Resources	A list of resources and equipment required for the event.
Timezone	The timezone in which the event is held.

Media

Audio

Description	Audio files that are recovered that use the .mp3 or .wav formats.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
File Name	Name of the file.
File Extension	Extension of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the audio file was created.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the audio file was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the audio file was last modified.
File Size (Bytes)	The size of the audio file.
MD5 Hash	An MD5 hash of the audio content.
SHA1 Hash	A SHA1 hash of the audio content.

Carved Video

Description	Videos that are recovered using carving. Supported formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. Other container formats can also be recovered provided that their underlying packets are the same as one of the supported formats.
Notes	As of February 20 2020, this artifact will no longer be included under Videos. Carved Video functionality will be included in the 'Videos' artifact instead.

ATTRIBUTE	DESCRIPTION
Content Format	The format of the video.
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
File Size (Bytes)	The size of the container and file.
Container Format	The format of the video container.
Saved Video Size (Bytes)	The size of the video that was saved to the database.
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.

Live Photos

Description	Live Photos retrieved using parsing.
Notes	

ATTRIBUTE	DESCRIPTION
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
UUID	The id of the picture and video. If the uuid is different for picture and a video, it is not associated with each other
Created Date/Time - UTC (yyyy-mm-dd)	The created date/time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date/time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date/time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. "Complete" indicates that a full Exif extraction was performed. "Failed" indicates that the information may have been corrupted and could not be recovered. "Skipped" indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).

ATTRIBUTE	DESCRIPTION
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
GPS Longitude	The GPS longitude coordinates of where the picture was taken (extracted from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
GPS Latitude	The GPS Latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS Latitude (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the pciture was taken (extracted from Exif data).
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

Photos Albums

Description	Photos Albums contains information about the albums that contain pictures and media in the Photos app on macOS.
Notes	

ATTRIBUTE	DESCRIPTION
Album Title	The title of the album.
Created Date/Time	The date/time when the album was created on the local device.
Photo Count	The number of photos in the album.
Video Count	The number of videos in the album.
UUID	The UUID of the album.
Owner Name	The full name of the owner. This is only available when the album is a Shared Album.
Shared	Indicates if the album is a Shared Album. The value "Yes" is displayed when the album is shared.
Invitees	The full names of those invited to view the Shared Album.

Photos Media Information

Description	Photos Media Information contains metadata about pictures and media stored in the Photos app on macOS.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the media file.
Type	The type of media. The value can be Picture or Video.
Album Title	The title of the media file's album.
Hidden	Indicates if a photo has been hidden.
Favorited	Indicates if a photo has been favorited.
Deleted	Indicates if a file has been recently deleted. Recently deleted files remain accessible for 30 days.
Directory	The directory the media file resides in.
Created Date/Time	The date/time when the media was created on the local device.
UUID	The UUID of the media.
Latitude	The latitude of the location where the media was taken.
Longitude	The longitude of the location where the media was taken.
Modified Date/Time	The date/time when the media was modified on the local device.
Deleted Date/Time	The date/time when the media was deleted from the local device.

Pictures

Description	Pictures retrieved using either carving or parsing techniques. The supported formats are as follows: JPEG (.jpeg, .jpg, .jpe), PNG (.png), Bitmaps (.bmp), Graphics Interchange Format (.gif), Icons (.ico), and Tagged Image File Format (.tif, .tiff).
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date/time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date/time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date/time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. "Complete" indicates that a full Exif extraction was performed. "Partial" indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. "Failed" indicates that the information may have been corrupted and could not be recovered. "Skipped" indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).

ATTRIBUTE	DESCRIPTION
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
GPS Longitude	The GPS longitude coordinates of where the picture was taken (extracted from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
GPS Latitude	The GPS Latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS Latitude (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the pciture was taken (extracted from Exif data).
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Potential Original Media	Indicating if the media is likely the original source.
Category	An integer that indicates the Project VIC category for the picture.

Quicktime Player History

Description	Quicktime Player History provides information about the files a user has viewed using the player. Quicktime is the default video player for macOS computers.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file played with Quicktime.
File Path	The full path to the file played with Quicktime.
Drive Name	The name of the drive where the played file was located.
Volume UUID	The UUID of volume where the played file was located.

Videos

Description	Videos that are recovered using parsing or carving. Supported formats for parsing include AVI, MP4, MOV, MPEG, DIVX, A3GP, ASF, WMV, DVR-MS, MKV, VOB, MOD, and WEBM. Supported carving formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. For more information about supported video formats, see Supported media and file types.
Notes	Supported formats include AVI, MP4, MOV, MPEG, DIVX, A3GP, ASF, WMV, DVR-MS, MKV, VOB, MOD, and WEBM. For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
File Name	Name of the file.
File Extension	Extension of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the video was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the video was last accessed.

ATTRIBUTE	DESCRIPTION
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the video was last modified.
File Size (Bytes)	The size of the video.
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. "Complete" indicates that a full Exif extraction was performed, including potential metadata located at the end of the video. "Partial" indicates that only Exif information in the header section of the video file was recovered, which should only occur with very large videos (in excess of the limit set in the options screen). "Failed" indicates that the information may have been corrupted and could not be recovered. "Skipped" indicates that the extraction was skipped.
Media Duration (Seconds)	The duration of the video in seconds (extracted from Exif data).
Original Width	The resolution of the video (extracted from Exif data).
Original Height	The resolution of the video (extracted from Exif data).
Created Date/Time - Local Time	The local date and time when the video was first recorded (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the video was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the video being recored (extracted from Exif data).
Software	The software used to record or modify the video. This could either be the OS version of the phone used to record the video or name of the software used to edit the video in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to record the video (extracted from Exif data).
Model	The model of the camera used to record the video (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to record the video (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).

ATTRIBUTE	DESCRIPTION
Latitude	The GPS coordinates of the camera where the video was recorded (extracted from Exif data).
Longitude	The GPS coordinates of the camera where the video was recorded (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the video was recorded (extracted from Exif data).
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.
Content Format	The format of the carved video.
Container Format	The format of the carved video container.
Saved Video Size (Bytes)	The size of the carved video that was saved to the database.

VLC Recently Played Files

Description	VLC Recently Played Files contains information about the media files that are played using the VLC Media Player. This artifact can reveal information on the user's interaction with the application.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file that was played in the player.
File Path	The file path to the recently played file.
Resume Time (seconds)	The number of seconds played before the media file is paused or stopped. If the duration is less than 5% or more than 95% of the total runtime, this value is set to 0.

Web Video Fragments

Description	This search recovers two distinct types of web-based video. Fragme nts of Flash video can be left behind by many video streaming sites, such as YouTube. RTMP Frame Fra gments are frames left behind by streaming sites using the RTMP protocol (widely used by webcam chat sites, including Chatroulette and Camstumble). In the case, a thumbnail from a recovered video is displayed, as well as any relevant metadata. Videos can be exported to .FLV format to be played. Due to the natur e of the data recovered, some video players will have issues playing the exported files. We recommen d trying ffmpeg, VLC, and the GOM player.

Notes	

ATTRIBUTE	DESCRIPTION
Preview	A thumbnail preview of the video
Content Recovered	The raw bytes that were recovered
Metadata	Any metadata about the video
Recovered Duration	The length of the video that was recovered

Operating System

.DS_Store Records

Description	.DS_Store Records contains all the records extracted from .DS_Store files found on the computer. Each record represents a property of a file or a folder. The significance of this artifact is an indicator of high likelihood that the user of the computer was aware of these files and folders with a possibility of attributing a date to that awareness.
Notes	In the Apple macOS operating system, .DS_Store (Desktop Services Store) is a hidden file that stores the display information of its containing folder, similar to the file desktop.ini in Microsoft Windows. The file tracks information such as icon positions, view settings, cached file size, cached last modified date, and even the choice of a background image. The .DS_Store is created and maintained by the Finder application in any folder that it accesses, even on remote file systems mounted from servers that share files (for example, via Server Message Block (SMB) protocol or the Apple Filing Protocol (AFP)). .DS_Store files are also included in archives created by macOS users, such as ZIP files, and they are backed up by some cloud file backup services. This means that the presence of .DS_Store Records artifacts on non-Mac evidence such as Windows, Mobile, or Cloud indicates that some of the data may have originated or have been accessed from a macOS computer at some point. For more information on .DS_Store files and their forensic significance see: .DS_Stores: Like Shellbags but for Macs.

ATTRIBUTE	DESCRIPTION
Record Name	The name of the file or folder as stored in the .DS_Store file.
Record Type	The type of the record, or property, that is being logged in the .DS_Store file for a particular file or folder.
Record Value	The value of the property for the given file or folder.
Record Path	The full path to the file or folder
.DS_Store Created Date/Time - UTC (yyyy-mm-dd)	The created date of the .DS_Store file from which the record was extracted.
.DS_Store Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date of the .DS_Store file from which the record was extracted.

ATTRIBUTE	DESCRIPTION
.DS_Store Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date of the .DS_Store file from which the record was extracted.

AirDrop Available Recipients

Description	AirDrop Available Recipients lists all available recipients for an AirDrop transfer outgoing from the local device. The devices need to be in Bluetooth and Wi-Fi range to connect to each other. You can recover up to one week of AirDrop activity history as it is stored in the Apple Unified Logs.
Notes	Available users are only recorded in the Apple Unified Logs when the local user opens the AirDrop view in Finder or tries to send a file using the AirDrop sharing option. There is a record for each time a person "bubble" appears in the respective interface. This artifact can help place other devices in proximity of the device being investigated.

ATTRIBUTE	DESCRIPTION
Name	The name of the user or the user's device.
User ID	The ID of the user as tracked by the AirDrop service.
Contact Added	Indicates whether the user is a contact on the local user's device.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the log entry.
Transaction Log	The log message extracted from Unified Logs.

AirDrop Background Activity

Description	Airdrop Background Activity is a collection of logs that capture background events triggered by the Airdrop service.
Notes	This artifact does not capture every single background event that is described in the log. This artifact extracts what look to be the most relevant pieces of data, but it's up to the examiner to determine their forensic significance. If there are logs that are not included in this artifact that should be, please reach out to Tech Support.

ATTRIBUTE	DESCRIPTION
Date/Time - UTC (yyyy-mm-dd)	The date and time of the log entry.
Transaction Log	The log message extracted from Unified Logs.

AirDrop Discoverability

Description	AirDrop Discoverability lists changes to the discoverability status of device.
Notes	While this artifact reflects changes that the user initiates a change to their discoverability, it does also capture system changes. The AirDrop service periodically resets which causes the status to toggle between the current status and off, typically within one second of each other. These changes are background system activities that are not representative of an action by the user.

ATTRIBUTE	DESCRIPTION
Mode Change Date/Time - UTC (yyyy-mm-dd)	The date and time of the log entry.
Mode	Mode is an indication of who can share files with the local machine (values include Off, Contacts Only, or Everyone).
Transaction Log	The log message extracted from Unified Logs.

AirDrop Incoming Transfers

Description	AirDrop Incoming Transfers lists information about AirDrop transfers incoming to the local device. The devices need to be in Bluetooth and Wi-Fi range to connect to each other. You can recover up to one week of AirDrop activity history as it is stored in the Apple Unified Logs.
Notes	Incoming transfers are records pertaining to the files received on the local machine. A single transaction with multiple files will get split into multiple hits in AXIOM Examine and can be grouped by sorting on Transaction ID.

ATTRIBUTE	DESCRIPTION
Item Type	Typically these values are displayed as mime types. However, if Apple doesn't have a friendly name reserved for a particular file type, you might see values like dyn.ah62d4rv4ge80nqbv.
Number of Items	The number of items of that type included in the transfer.
Is File	Indicates whether the items being transferred are files or not (e.g. folder, link, etc.).
Sender Name	The name of the sender.
Sender Device	The name of the sender's device.
Destination Folder	The location chosen by the user to save the incoming transfer to.
Status	Indicates whether the transfer is accepted, declined, or incomplete. Incomplete could mean either the transaction timed out, or the sender cancelled the transaction on their end.

ATTRIBUTE	DESCRIPTION
Transfer Start Date/Time - UTC (yyyy-mm-dd)	The date of the first log entry associated with the transfer.
Transfer Finish Date/Time - UTC (yyyy-mm-dd)	The date of the last log entry associated with the transfer.
Sender is Me	Indicates whether the sender is logged in under the same account as the recipient.
Auto Accepted	Indicates if the transfer was auto-accepted.
Sender ID	The Id of the sender as tracked by the AirDrop service.
Verifiable Identity	Indicates whether the identity of the user is verifiable, this is an internal flag and its up to the examiner to determine its forensic significance.
Partial Recovery	Identifies whether the transfer transaction log was incomplete. 'Yes' indicates that some of the transaction log lines were missing before the end of the log file was encountered, so some fragment lines were left empty because they could not be properly recovered.
Transaction ID	An identifier for a given transaction. If multiple files are selected and transferred together, they're listed as separate hits but will have the same transaction ID.
Transaction Log	A raw dump of the logs between the first and last log relating to the transaction.

AirDrop Outgoing Transfers

Description	AirDrop Outgoing Transfers lists information about AirDrop transfers outgoing from the local device. The devices need to be in Bluetooth and Wi-Fi range to connect to each other. You can recover up to one week of AirDrop activity history as it is stored in the Apple Unified Logs.
Notes	Outgoing transfers are records pertaining to the files sent by the local machine. A single transaction with multiple files will get split into multiple hits in AXIOM Examine and can be grouped by sorting on Transaction ID.

ATTRIBUTE	DESCRIPTION
Item Name	The file or folder name.
Item Type	Typically, these values are displayed as mime types. However, if Apple doesn't have a friendly name reserved for a particular file type, you might see values like dyn.ah62d4rv4ge80nqbv.
Is File	Indicates whether the items being transferred are files or not (e.g. folder, link, etc.).
Recipient Name	The name of the recipient.

ATTRIBUTE	DESCRIPTION
Recipient Device	The name of the recipient's device.
Status	Indicates whether the transfer is accepted, declined, or incomplete. A Declined/Incomplete status could indicate the transfer was cancelled, declined, or the transfer timed out transfer.
Transfer Start Date/Time - UTC (yyyy-mm-dd)	The date of the first log entry associated with the transfer.
Transfer Finish Date/Time - UTC (yyyy-mm-dd)	The date of the last log entry associated with the transfer.
Recipient ID	The Id of the recipient as tracked by the AirDrop service.
Verifiable Identity	Indicates whether the identity of the user is verifiable, this is an internal flag and its up to the examiner to determine its forensic significance.
Partial Recovery	Identifies whether the transfer transaction log was incomplete. 'Yes' indicates that some of the transaction log lines were missing before the end of the log file was encountered, so some fragment lines were left empty because they could not be properly recovered.
Transaction ID	An identifier for a given transaction. If multiple files are selected and transferred together, they're listed as separate hits but will have the same transaction ID.
Transaction Log	A raw dump of the logs between the first and last log relating to the transaction.

Apple Accounts

Description	Apple Accounts contains information about the Apple ID accounts used on the macOS computer. The account details contained can help investigators recover and correlate account information across applications and provide information on what accounts to review and get more information from.
Notes	

ATTRIBUTE	DESCRIPTION
Local Account	The local user's account name, this attribute is only available for macOS computers
User Name	The email address or user name used to log into the account.
Account ID	The UID used to identify accounts and files tied to a specific account.
Account Added Date/Time - UTC (yyyy-mm-dd)	The date and time that the account was added to the database.

ATTRIBUTE	DESCRIPTION
Parent Account ID	The UID used to match the account to its parent account if it has one.
Account Description	A description of the account, as provided by the user.
Account Type	The type of user account
Account Credential Type	The type of credentials used by the account. The account credential type can help to indicate which methods might be of use for recovering the credentials (and possibly aiding with a cloud acquisition of the account).
Owning Bundle ID	The unique bundle ID of the application that the account was setup with.
Last Credential Expiry Date/Time - UTC (yyyy-mm-dd)	The date and time of when the credentials had to be re-entered for the account due to a password change or expiry of the token/credentials.

Apple Contacts - macOS

Description	Apple Contacts contains information about the contacts a user has saved to their device.
Notes	

ATTRIBUTE	DESCRIPTION
First Name	The first name of the contact.
Last Name	The last name of the contact.
Picture	The profile picture of the contact, in its full size.
Home Phone	The home phone numbers associated with the contact.
Mobile Phone	The mobile phone numbers associated with the contact.
Office Phone	The office phone numbers associated with the contact.
Phone Number(s)	Any additional phone numbers associated with the contact.
Home Email	The home email addresses associated with the contact.
Office Email	The office email addresses associated with the contact.
Email(s)	Any additional email addresses associated with the contact.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the contact's information was created.
Address	The physical addresses associated with the contact.
Website	The websites associated with the contact.
Middle Name	The middle name of the contact.
Source Account	The linked account that the contact was imported from.
Organization	The organization or business associated with the contact.
Company	Whether or not the contact is a company.
Department	The department associated with the contact.

ATTRIBUTE	DESCRIPTION
Note	Notes associated with the contact.
Birthday (yyyy-mm-dd)	The birthday of the contact.
Job Title	The job title associated with the contact.
Nickname	The nickname associated with the contact.
Prefix	Any prefix applied to the contact's name (for example, Mr., Mrs., Dr.).
Suffix	Any suffix applied to the contact's name (for example, PH.D, Ed.D, LLD).
User Accounts	A comma separated list all the social media accounts associated with this contact.
First Name Phonetic	The phonetic spelling of the contact's first name.
Middle Name Phonetic	The phonetic spelling of the contact's middle name.
Last Name Phonetic	The phonetic spelling of the contact's last name.
Previous Last Name	The previous last name of the contact.
Relationship	Relationships that the contact shares with others. E.g. Mother, Father, Spouse
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the contact's information was last modified.

Apple Contacts Groups

Description	Apple Contacts Groups contains information about the groups that the user creates to organize their contacts.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the contact group.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the group's information was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the group's information was last modified.
Group Member(s)	The contacts that have been added to the group.
Source Account	The linked account that the contact group was imported from.

Apple Keychain Generic Passwords

Description	Apple Keychain Generic Passwords contains passwords for applications and services that are saved to the Keychain app. Analyzing results from this artifact can reveal valuable passwords and tokens that are associated to the user's accounts.

Notes	

ATTRIBUTE	DESCRIPTION
Service Name	The name of the service that has stored data in the keychain.
Value	The secret value that's associated with the account. Values that have non-printable characters are converted to hex strings. To see what the raw data looks like before conversion, export the hit with attachments.
Account	The account identifier of the keychain item.
Access Group	The access group that the keychain item belongs to.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the keychain item was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the keychain item was last modified.
Original Location	The offset of the keychain item in the keychain database.

Apple Keychain Internet Passwords

Description	Apple Keychain Internet Passwords contains passwords for websites and internet services that are saved to the Keychain app. Analyzing results from this artifact can reveal valuable passwords and tokens that are associated to the user's accounts.
Notes	

ATTRIBUTE	DESCRIPTION
Label	The label of the keychain item.
Description	The description of the keychain item.
Account	The account identifier of the keychain item.
Value	The secret value that's associated with the account. Values that have non-printable characters are converted to hex strings. To see what the raw data looks like before conversion, export the hit with attachments.
Access Group	The access group that the keychain item belongs to.
DSID	The Destination Signaling Identifier is a unique identifier assigned to a user when they register an iCloud account.
Server	The server address for an internet password item.

ATTRIBUTE	DESCRIPTION
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the keychain item was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the keychain item was last modified.
Original Location	The offset of the keychain item in the keychain database.

Apple Notes

Description	Apple Notes contains information about the notes a user has created on their macOS computer.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the note.
Folder	The folder the note is stored in.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the note was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the note was last modified.
Summary	The summary of the note.
Encrypted	Indicates whether or not the note has been encrypted.
Password Hint	The hint to encryption password.
Body	The note body.
Attachments	A list of attachments contained in the note
Note ID	The notes unique identifier.

Apple Notes - Voice

Description	Contains the recovered voice notes from a macOS computer.
Notes	

ATTRIBUTE	DESCRIPTION
Audio	The saved voice note.

ATTRIBUTE	DESCRIPTION
Saved Date/Time - UTC (yyyy-mm-dd)	The date and time that the voice note was saved.
Duration (seconds)	The duration of the voice note in seconds.
Path	The path to the voice note on the device.
Version	The version of the note: Original, Duplicate (duplicate copy of the original), Duplicate - Edited (duplicate copy of the original and partly modified), Edited (edited copy of an original note).
Original Path	The path to the original version of an edited note.
Note ID	The ID of the note.
Label	The label of the note.

Bash / ZSH Sessions

Description	Bash / ZSH Sessions contains information about terminal/Bash/ZSH sessions on a macOS computer, and the commands that are run during each session.
Notes	

ATTRIBUTE	DESCRIPTION
Session ID	The ID of the session.
User	The user that started the session.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the session started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the session ended.
Session Command History	The command history of the session.

Bluetooth Devices - macOS

Description	Bluetooth Devices contains information about the Bluetooth devices that have been connected to the user's macOS computer
Notes	

ATTRIBUTE	DESCRIPTION
Address	The MAC address of the associated Bluetooth Device that's connected to the macOS computer
Type	The type of Bluetooth device

ATTRIBUTE	DESCRIPTION
Last Seen Date/Time - UTC (yyyy-mm-dd)	The last date and time that the Bluetooth device was connected to the macOS computer
UUID	The username GUID that's associated with the Bluetooth device

CoreAnalytics

Description	CoreAnalytics contains information about macOS system usage and application execution history. This artifact gives an overview of applications and processes used during historical and current activity periods.
Notes	

ATTRIBUTE	DESCRIPTION
Process Name	The name of the application that ran during the diagnostic period.
Bundle ID	The unique bundle identifier for the application.
Application Version	The build and release versions for the application. Formatted as: Build Version (Release Version)
Ran in Foreground	Indicates whether the application had run in the foreground.
Number of Activations	The number of times that the application was brought to the foreground.
Uptime (seconds)	The total time that the application was awake including running in the background and foreground.
Active Time (seconds)	The number of seconds that the application was run in the foreground.
Number of Launches	The number of times that the application was launched during the diagnostic reporting period. The value of launches will remain at zero if the application was launched prior to the beginning of the diagnostic period.
Diagnostic Period Began	The date and time that the diagnostic log was started.
Diagnostic Period Ended	The date and time that the diagnostic log ended or will end.

Daily Logs - Disk Status

Description	Daily Logs - Disk Status contains information about daily disk status logs on a macOS computer.
Notes	

ATTRIBUTE	DESCRIPTION
Log Date/Time - Local Time	The local date and time that the log was created.
Disk Device	The disk device that the log was created for.
Disk Size	The full size of the disk.
Disk Space Used	The amount of disk space that's used.
Disk Space Available	The amount of disk space that's still available.
Mount Point	The path the mounted disk.

Daily Logs - Local System Status

Description	Daily Logs - Local System Status contains information about daily system status logs on a macOS computer.
Notes	

ATTRIBUTE	DESCRIPTION
Log Date/Time - Local Time	The local date and time that the log was created.
System Up Time	The system up time at the time the log was created.
Number of Logged In Users	The number of logged in users.
Load Average (1 min)	Load average value over the last 1 minute.
Load Average (5 min)	Load average value over the last 5 minutes.
Load Average (15 min)	Load average value over the last 15 minutes.

Daily Logs - Network Interfaces Status

Description	Daily Logs - Network Interfaces Status contains information about daily network interfaces status logs on a macOS computer.
Notes	

ATTRIBUTE	DESCRIPTION
Log Date/Time - Local Time	The local date and time that the log was created.

ATTRIBUTE	DESCRIPTION
BSD Name	The BSD name assigned to the network adapter.
MTU	Maximum Transmission Unit value.
Network	The network interface type.
Address	The address of the newwork interface.
Incoming Packets	The number of packets received on this network interface.
Outgoing Packets	The number of packets sent on this network interface.

Deleted Accounts

Description	Quarantined Files contains information about the files that were flagged as quarantined in the macOS computer.
Notes	

ATTRIBUTE	DESCRIPTION
Quarantined Date/Time - UTC (yyyy-mm-dd)	The date and time the file was flagged as quarantined.
Application Name	The name of the application used to access/download the file.
Package Name	The package name of the application used to access/download the file.
Quarantined File identifier	Unique identifier of the quarantine event saved in the extended attributes of the quarantined file.
Download URL	Exact URL the file was downloaded from.
Sender Name	The Sender Name of the email, when the flagged quarantined file originated from an email.
Sender Address	The Sender Email Address, when the flagged quarantined file originated from an email.
Origin	Either the original URL the file was downloaded from or the email message id, when the flagged quarantined file originated from an email.
Origin Title	The Subject of the email, when the flagged quarantined file originated from an email.

Dock Items

Description	Dock Items contains information about the applications that have appeared in the dock. Usually, these items are recently or often used apps.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The name of the application.
Package Name	The package name of the application.
State	The positioning of the application in the dock (Persistent App, Recent App or Persistent Others).
User Name	The user name of the account from where the dock items were parsed.
Folder Path	The folder path of the application.
GUID	The GUID of the application.

File Signature Mismatch (Audio)

Description	File Signature Mismatch (Audio) contains identified mismatches between a known file signature header and the extension (or lack thereof) for an audio file. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.

File Signature Mismatch (Container)

Description	File Signature Mismatch (Container) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a container. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.

ATTRIBUTE	DESCRIPTION
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.

File Signature Mismatch (Document)

Description	File Signature Mismatch (Document) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a document. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.

File Signature Mismatch (Picture)

Description	File Signature Mismatch (Picture) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a picture. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.

ATTRIBUTE	DESCRIPTION
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file. If the mime type is unknown, this defaults to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file. If the mime type is unknown, this defaults to application/octet-stream. If there is no file extension, but the mime type is known, a mismatch is is returned.
File Path	The path to the mismatched file.

File Signature Mismatch (Video)

Description	File Signature Mismatch (Video) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a video. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.

File System Events

Description	File System Events contains information about the changes to file system objects, occurring in volumes mounted on a macOS computer. This artifact contains all system event files recovered from the '.fseventsd' folder.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the system object affected by the event.

ATTRIBUTE	DESCRIPTION
File Path	The full path to the system object affected by the event.
Flags	Flags that indicate the type of system object and the changes that occured to the object.
Event ID	An Event ID for the record.
File ID	A system ID for the file system object that was affected by the event.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the event file is initially created. This file is recovered from the .fseventsd directory and can contain records for many different events, so this timestamp may not coincide with when the event actually occurred.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the event file was last updated. This file is recovered from the .fseventsd directory and can contain records for many different events, so this timestamp may not coincide with when the event actually occurred.

File System Information (APFS)

Description	File System Information (APFS) contains information about the file system of the macOS computer.
Notes	

ATTRIBUTE	DESCRIPTION
Container GUID	The file system's container GUID.
Volume GUID	The file system's volume GUID.
Block Size	The block size of the file system.
Volume Name	The name of the volume of the file system.
Volume Size (bytes)	The size of the volume of the file system.
Next Object ID	The next allocated object id in the file system.
Unmounted Date/Time - UTC (yyyy-mm-dd)	The date and time the file system was last unmounted.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file system was created.
Volume Creator Program	The name of the program used to create the volume of the file system.
File Count	The number of files in the file system.
Symlink Count	The number of symbolic links in the file system.
Directory Count	The number of directories in the file system.
Snapshot Count	The number of snapshots in the file system.
Filesystem Object Count	The file system's object count.
Volume Count	The volume count.

Finder MRU

Description	Finder MRU lists the recently accessed paths from the Finder application on macOS.
Notes	

ATTRIBUTE	DESCRIPTION
Path	The path that was accessed through the Finder.
Accessed Order	The order in which certain paths are accessed. 1 represents the location that was most recently accessed. The numbers then increase by 1 for each previous accessed location.
MRU Type	The type of MRU that is being reported.
Creator Name	The creator name for the path that was accessed.

Finder Sidebar Items

Description	Finder Sidebar Items contains information about each of the items featured in the Finder Sidebar on macOS. Items in the sidebar are often commonly-used items, and the user can customize the types of items they want to appear.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the sidebar item.
Type	The type of the sidebar item.
Category	The category that the sidebar item belongs to (Devices, Favorites, Shared, Tags).
Bookmark Data	The raw data contained within the sidebar item.

iCloud Downloads

Description	iCloud Downloads show a list of files that have been either recently downloaded or are pending download.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the iCloud file.
Download State	Indicates whether the file is available on the local drive or is pending download.

ATTRIBUTE	DESCRIPTION
FileSize (bytes)	The size of the file in bytes.
Download Request Date/Time - UTC (yyyy-mm-dd)	The date and time that the download was requested.

iCloud Local Files

Description	iCloud Local Files are files that have been imported from the local computer or synced remotely from the iCloud Drive folder on a macOS machine.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the iCloud file.
Original File Name	The name of the file when it was first loaded to the iCloud Drive.
Package Name	The package ID of the application used to interact with the file.
FileSize (Bytes)	The size of the file in bytes.
Item Type	Indicates whether an item is a file, a folder, or a hidden iCloud File. Hidden iCloud files are used as markers for upload/download sync states and are .iCloud files.
File Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created.
File Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was modified.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last accessed on the iCloud Drive.

iCloud Uploads

Description	iCloud Uploads show a list of files that have been either recently uploaded or are pending upload.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the iCloud file.
Upload State	Indicates whether the file is available on the local drive or is pending upload.
FileSize (Bytes)	The size of the file in bytes.

ATTRIBUTE	DESCRIPTION
Upload Request Date/Time - UTC (yyyy-mm-dd)	The date and time that the upload was requested.

Installed Applications - macOS

Description	Applications that are installed on the computer that's running macOS.
Notes	

ATTRIBUTE	DESCRIPTION
Display Name	The display name of the installed application.
Package Name(s)	The application bundle(s), which represent the application package identifier(s) in the App Store.
Display Version	The version number of the application provided via the App Store.
Internal Version	The long version string of the application.
Installed/Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the application was last installed or updated.
App Store Action	The App Store action further describes the application installation or update.

KnowledgeC Activity Level

Description	KnowledgeC Activity Level provides information about the KnowledgeC stream type of activity level.
Notes	

ATTRIBUTE	DESCRIPTION
Activity Type	The activity level.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Application Activities

Description	KnowledgeC Application Activities contains information about activities associated with specific applications.

Notes	

ATTRIBUTE	DESCRIPTION
Activity	The description associated with the activity.
Application Name	The bundle name of the application associated with activity.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time the activity occurred.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Application Focus

Description	KnowledgeC Application Focus provides information about the applications that were in focus on the device screen, within a recorded interval.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The bundle name of the application in focus.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Application Install States

Description	KnowledgeC Application Install States provides information about when applications were installed or uninstalled on the device.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The bundle name of the application that was installed or deleted.
Install State	The install state of the application (Installed or Uninstalled).
State Changed Date/Time - UTC (yyyy-mm-dd)	The date and time that install state last changed.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Application Usage

Description	KnowledgeC Application Usage provides information about the applications that were used on the device, within a recorded interval.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The bundle name of the application used.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Application Web Usage

Description	KnowledgeC Application Web Usage provides information about the applications that were used to access webpages on a iOS device, within a recorded interval.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The bundle name of the application that accessed the webpage.
Domain	The domain name of the webpage.
URL	The URL of the webpage.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Device Lock States

Description	KnowledgeC Device Lock States provides information about whether the device is locked or unlocked within recorded intervals. An absence of a recorded interval might mean that device was turned off during that time.
Notes	

ATTRIBUTE	DESCRIPTION
State	The lock state of the device (Locked or Unlocked).

ATTRIBUTE	DESCRIPTION
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Device Orientation States

Description	KnowledgeC Device Orientation States provides information about the orientation of the device within recorded intervals. An absence of a recorded interval might mean that device was turned off during that time.
Notes	

ATTRIBUTE	DESCRIPTION
State	The orientation state of the device (Vertical or Sideways).
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Device Plugged-in States

Description	KnowledgeC Device Plugged-in States provides information about the plugged-in state of a device within recorded intervals. An absence of a recorded interval might mean that device was turned off during that time. Knowing whenever a device is connected to charger or computer using USB can help identify how the device is used.
Notes	

ATTRIBUTE	DESCRIPTION
State	The plugged-in state of the device. This value shows whether a device is plugged in and/or connected via USB (Plugged in or Unplugged).
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Media History

Description	KnowledgeC Media History provides information about what type of audio/video media the user was engaging with at what time, as recovered from KnowledgeC.db
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The bundle name of the application used to play the specified media
Album	The album name of the specified media
Title	The title of the specified media
Artist	The artist of the specified media
Duration	The duration of the specified media in seconds
Start Date/Time - UTC (yyyy-mm-dd)	The date and time the media started playing
End Date/Time - UTC (yyyy-mm-dd)	The date and time the media stopped playing

KnowledgeC Notification Usage

Description	KnowledgeC Activity Level provides information about the KnowledgeC stream type of activity level.
Notes	

ATTRIBUTE	DESCRIPTION
Bundle ID	The bundle ID.
Type	The type of notification.
Device ID	The device ID.
Process ID	The process ID.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Safari History

Description	KnowledgeC Safari History provides information about web pages that were accessed using the Safari browser, as recovered from knowledgeC.db
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the web page that was accessed with Safari browser.
Title	The title of the web page that was accessed with Safari browser.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the web page was accessed with Safari browser.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Screen Backlight States

Description	KnowledgeC Screen Backlight States provides information about the device backlight within recorded intervals. An absence of a recorded interval might mean that device was turned off during that time. This information can help identify whether a device was in active use within a specific interval.
Notes	

ATTRIBUTE	DESCRIPTION
State	The screen backlight state of the device. This value indicates whether the screen backlight is on or off (Screen on or Screen off).
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Latent Wireless Geolocated WiFi Hotspots

Description	Latent Wireless Geolocated WiFi Hotspots contains information about WiFi hotspots that were discovered using a Latent Wireless device. Latent Wireless stores information about the hotspots in a database that Magnet AXIOM can parse for details about each hotspot.
Notes	

ATTRIBUTE	DESCRIPTION
MAC Address	The MAC address of the detected WiFi hotspot.
First Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was first discovered.
Last Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was last seen.

ATTRIBUTE	DESCRIPTION
Strongest Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was detected at its highest strength.
Network Name (SSID)	The SSID of the WiFi hotspot.
Channel	The WiFi hotspot channel.
RSSI	The receieved signal strength indicator for the WiFi hotspot.
Latitude	The latitude where the WiFi hotspot was detected.
Longitude	The longitude where the WiFi hotspot was detected.
Secure	Indicates whether the wiFi hotspot is secure.

Login History

Description	Login History contains information about the date and time when a user logged in or out of the macOS system.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The account user name.
Date/Time - UTC (yyyy-mm-dd)	The date and time the user logged in or out of the system in UTC format. These records are recovered from the .asl logs.
Date/Time - Local Time	The date and time the user logged in or out of the system, in local time. Note: These records do not contain the year, so the exact date can only be inferred by using the Modified Date/Time of the respective accountpolicy.log file.
Status	The logon/logoff event status.

LogMeIn Activity

Description	LogMeIn Activity records connection events that occur using the LogMeIn remote desktop client. These records can include remote sessions and file sharing events.
Notes	

ATTRIBUTE	DESCRIPTION
Date/Time Local Time	The time in local time when the log line was recorded.

ATTRIBUTE	DESCRIPTION
Activity Type	The type of the activity that was recorded. The Session type indicates that the event is a remote session. The SessionDateReport indicates that the recorded event is a session summary. And, the FileShare type indicates that the recorded event was a file being shared with other users.
Connection Type	The type of connection that was used.
Status	Indicates the status of the file sharing event (only applies to FileShare activities).
Remote IP Address	The public IP address of the client server.
Local IP Address	The public IP address of the host server.
Connection State	The login/logout state of the connection.
OS Version	The OS version of the host.

Menu Bar Apps

Description	Menu Bar Items lists the applications that are listed in the menu bar on macOS. The menu bar appears at the top of the screen and allows the user to open and interact with the applications that are displayed. Some menu bar items are displayed by default, while others might be added by the user.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The internal name of the application that's displayed in the menu bar

Network Interfaces - macOS

Description	Network Interfaces contains information about each of the network the macOS computer has been connected to.
Notes	

ATTRIBUTE	DESCRIPTION
BSD Name	The BSD name for the network.
MAC Address	The MAC Address for the network interface.

ATTRIBUTE	DESCRIPTION
Network Type	The type of network, which can be ethernet or IEEE80211 (wireless).
Network Name (SSID)	The SSID for the network.
USB Product Name	The name of any device that's connected to the Computer and is utilizing network connectivity. The value will be empty if there aren't any eternal devices connected.
Service Path	Service path details

Network Profiles - macOS

Description	Network Profiles contains information about networks that have been saved to the device. This artifact can reveal current networks that are frequently in use, as well as archived networks.
Notes	

ATTRIBUTE	DESCRIPTION
Network Name (SSID)	The name of the saved network.
Last Connected Date/Time - UTC (yyyy-mm-dd)	The date and time of the last network connection.
Security Mode	The security mode of the network.
MAC Address	The list of MAC addresses that were accessed with the network.
Status	The network record status. 'Active' indicates an up-to-date record from KnownNetworks, and 'Archived' an old record from UpdateHistory.

Network Utilities

Description	Network Utilities contains information about tools run in the Network Utilities app on macOS (Info, Ping, Netstat, Lookup, etc). Each instance of the artifact indicates the utility that's used and the query (or URL) passed in to the utility. The results of running the utility are not recoverable.
Notes	

ATTRIBUTE	DESCRIPTION
Utility Tab	The specific utility that's used in the Network Utility app. The utilities include Ping Address, Lookup Address, Traceroute Address, Whois Address, User Finger Lookup Address, and Portscan Address.
Search Query	The query, or URL, that is run using the specified network utility.

ATTRIBUTE	DESCRIPTION
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the source file was last updated. The source file contains information about all user activity in the Network Utility app, so this timestamp may not represent the time that the event occurs, just the time that the file was last updated.

Operating System Information - macOS

Description	Operating System Information contains details about the macOS instance that's running on the user's computer.
Notes	

ATTRIBUTE	DESCRIPTION
Operating System	The name of the operating system.
Version Number	The operating system version number.
Build Number	The operating system build number.
iOS Support Version	The version of iOS that the operating system supports.
Install Date/Time - UTC (yyyy-mm-dd)	The date and time the operating system was installed.
Serial Number	The serial number of the drive the operating system is installed on.
Computer Name	The name of the computer.
Local Hostname	The local hostname of the computer.
Timezone	The current timezone of the computer.
Country Code	The current country code of the computer.
Locale	The current locale of the computer.
Languages	The installed languages on the computer.

Quick Look Thumbnails

Description	Quick Look Thumbnails contains thumbnail previews that the macOS device creates and displays for items in the file system.
Notes	

ATTRIBUTE	DESCRIPTION
Thumbnail	The thumbnail of the associated file.
Folder	The folder from which the thumbnail was generated.
File Name	The name of the file that the thumbnail was created for.

ATTRIBUTE	DESCRIPTION
Filesystem ID	The unique ID provided to the file. This value can be used to verify file system attributes for the file.
Thumbnail Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the thumbnail was generated
Thumbnail Size (bytes)	The thumbnail size in bytes. Negative values are ommitted until further investigation.
Thumbnail Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time in that thumbnail was last accessed by the user.
Thumbnail Access Count	The number of times the thumbnail has been accessed.

Recently Used Items

Description	Recently Used Items lists the most recently accessed items from a variety of sources. Each data source stores its recently used information in a separate file. For example, RecentDocuments aggregates information about all the documents that are opened, regardless of the app. RecentApplications contains information about each app that runs. And, app-specific sources can contain information specific to a particular app.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file that was accessed.
File Path	The full path of where the file was located.
UUID	The UUID of the accessed file.
Accessed Order	The order in which the Microsoft Office files are accessed. 1 represents the location that was most recently accessed. The numbers then increase by 1 for each previously accessed file.
MRU Type	The type of MRU that is being reported.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the file was accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created.
Creator Name	The creator name of the file.
Volume Name	The name of the physical volume the file was recovered from.
Volume UUID	The UUID of the physical volume the file was recovered from.
Volume Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the physical volume where the file was recovered from.
Volume Size (bytes)	The size of the volume in bytes where the file was recovered from.

ATTRIBUTE	DESCRIPTION
File System	The type of file system the file was recovered from.

Recovery Account Information

Description	Recovery Account Information lists the user accounts that have privileges to decrypt a FileVault encrypted volume in APFS.
Notes	

ATTRIBUTE	DESCRIPTION
UUID	The unique identifier for the user.
Full Name	The full display name of the user.
Password Hint	The user's password hint.
Picture	The users profile image.
Is Admin Account	Indicates if the user has administrative privileges on the computer.

Resumed Apps - macOS

Description	Resumed Apps has information about the applications that are set to reopen after the macOS computer restarts or resumes after going to sleep
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The name of the application that will be resumed when the computer resumes operations.
Bundle ID	The bundle name of the application, used to uniquely identify it in the App Store
Background State	A number that indicates the background state of the app. The values for this field are not translated into human-readable values, as it's not currently clear what each value represents

Spotlight Shortcuts

Description	Spotlight Shortcuts contains information about the searches that a user performs in the Spotlight application on macOS. The display name can indicate a local file/folder, application, or online search results.
Notes	

ATTRIBUTE	DESCRIPTION
Search Query	The query provided by the user.
Diplay Name	The name of the suggested result, provided by Spotlight.
URL	The URL associated with the suggested result.
Accessed Date/Time - UTC (yyyy-mm-dd)	Indicates when the displayed item was last accessed.

Startup Items - macOS

Description	Startup Items contains information about the processes and applications that are set to run at startup on a macOS computer.
Notes	

ATTRIBUTE	DESCRIPTION
Application Package Name	A label that identifies the package name of the launch agent or daemon.
Startup Process Arguments	Any command line arguments that are run automatically when the application starts.
Type	The type of startup item (LaunchAgent if the plist file was found in the LaunchAgents folder and LaunchDaemon if the file is found in the LaunchDaemons folder).
Process Type	The type of process that's being launched (Background, Standard, Adaptive or Interactive).
Disabled	Indicates whether the job is enabled or disabled.

Trash Items

Description	Trash Items contains information about the items that a user has sent to the trash. There is also a potential of recovering items that have been cleared from the trash. This artifact does not recover folder/directory objects unless they're listed in the .DS_Store file.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file or directory that's been deleted.
Type	The extension of the file. This attribute is not populated for directories and files with no extensions.
File Size (bytes)	The size of the file or directory in bytes.
Original Path	The original path of a file or directory recovered from the .DS_Store file. This path is used for restoring files to their original location

ATTRIBUTE	DESCRIPTION
Added Date/Time - UTC (yyyy-mm-dd)	The date and time that a file or directory was added to the trash bin. This attribute is not populated for files and directories that are not present in the filesystem but are mentioned in the .DS_Store file
Data	The Preview Card

USB Connection History

Description	USB Connection History contains a history of the USB devices that have been connected to the macOS computer.
Notes	

ATTRIBUTE	DESCRIPTION
Connection Start Date/Time - UTC (yyyy-mm-dd)	The date and time a connection was made to the macOS computer.
Serial Number	The serial number of the connected USB device.
Vendor ID	The vendor ID of the connected USB device.
Product ID	The product ID of the connected USB device.
Device Release Number	The release number of the connected USB device.

User Accounts - macOS

Description	User Accounts contains information about the users that have logged in to the macOS computer, as recovered from the settings file.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The account user name.
Full Name	The full display name of the user.
User ID	The users ID.
UUID	The unique identifier for the user.
Profile Created Date/Time - UTC (yyyy-mm-dd)	The date and time the profile was created.
Home Directory	The user's home directory.
Password Hash	A hash of the user's password.

ATTRIBUTE	DESCRIPTION
Password Hash Algorithm	The algorithm used to generate the user's password hash.
Password Hint	The user's password hint.
Login Failure Count	The number of failed logins for the account.
Last Incorrect Password Login Date/Time - UTC (yyyy-mm-dd)	The last date and time an incorrect password was attempted.
Last Password Change Date/Time - UTC (yyyy-mm-dd)	The date and time the password was last changed.
Profile Image	The users profile image.
Profile Image Path	The path to the users profile image.

Volume Information

Description	Volume Information contains information about the volumes that are connected to the macOS computer. Volumes can include mounted drives, CD/DVDs, DMG files, external drives, or anything else that the computer detects as a mounted volume/device). You can find information about mapped networks volumes in the macOS Most Recently Used artifact.
Notes	

ATTRIBUTE	DESCRIPTION
Volume Name	The volume name.
Volume Created Date/Time - UTC (yyyy-mm-dd)	The date and time when volume was created on the system.

Wi-Fi Logs

Description	Wi-Fi Logs contains log entries extracted from the wifi log on a macOS computer. This artifact can reveal wifi activities, such as attempts to connect, autoconnect, and connection errors. This artifact can include data from networks that the user hasn't saved.
Notes	

ATTRIBUTE	DESCRIPTION
Line	The line number within the log file where this record exists.
Network Name (SSID)	The name of the network that's associated with log entry.
Type	The type of event for the log entry.
Date/Time - Local Time (yyyy-mm-dd)	The local date and time for when the log entry was written.
Event	A brief description of the event from the log entry.

ATTRIBUTE	DESCRIPTION
Original Text	The full text of the log entry.

Social Networking

Houseparty Messages

Description	Contains messages recovered from Houseparty.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The username of the person sending the message.
Recipient	The username of the person receiving the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The content of the sent message.
Read Status	Whether or not the message has been read.

Houseparty Users

Description	Contains information about the users contacted from the device using Houseparty.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	User name of the user.
Full Name	Full name of the user.
Created Date/Time - UTC (yyyy-mm-dd)	Date and time when the user account was created.
Updated Date/Time - UTC (yyyy-mm-dd)	Date and time when the user account was last updated.

Web Related

Chrome Archived Keyword Search Terms

Description	Keyword search terms that were archived by the browser.

Notes	

ATTRIBUTE	DESCRIPTION
Keyword Search Term	The keyword search term the user entered.
URL	The URL of the keyword search.

Chrome Archived Web History

Description	An archived history of old webpage visits.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL where the archived web history is located.
Title	The title of the archived web history.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was visited.
Visit Count	Total visits to this URL.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
ID	ID for the web history archive.

Chrome Autofill

Description	A collection of saved values that were used to fill in forms and fields.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the autofill value.
Value	The value
Count	Count of this autofill.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill value was created.

Chrome Autofill Profiles

Description	Profiles that Chrome uses to fill in forms with saved values.

Notes	

ATTRIBUTE	DESCRIPTION
Name	Name for the autofill profile.
Email	Email used in the the autofill profile.
Number	Phone number used in the autofill profile.
Company	Company name used in the autofill profile.
Address Line 1	Address Line 1 used in the autofill profile.
Address Line 2	Address Line 2 used in the autofill profile.
City	City used in the autofill profile.
State	State used in the autofill profile.
Zipcode	Zipcode used in the autofill profile.
Country	Country used in the autofill profile.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the profile was last modified.

Chrome Bookmarks

Description	Browser bookmarks that reference saved webpages.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was added.
Parent	The name of the parent folder of the bookmark.

Chrome Cache Records

Description	Content that Chrome downloads and caches to speed up rendering times. Cached content can include pictures, text, html, javascript, and more.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the cached item.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.

ATTRIBUTE	DESCRIPTION
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was first visited.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The date and time the cache was last synced with the cloud.
File Type	The type of file that was cached.
Content Size (Bytes)	The size of the cached file.
Image	The cached image if the file type is an image. Otherwise, this column is empty.
Content	The cached file contents if the file type is not an image. Otherwise, this column is empty.

Chrome Cookies

Description	Cookies that Chrome downloads from the Internet that contain information about the websites that a user visits.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie expires.
Path	The path of the cookie value.

Chrome Current Session

Description	Information about the browser session that's currently underway.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL.
Title	The title of the web page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.

ATTRIBUTE	DESCRIPTION
Redirect URL	The URL to use to redirect if applicable.

Chrome Current Tabs

Description	Information about the tabs that are open in the current browser session.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL.
Title	The title of the web page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.

Chrome Downloads

Description	Information about the files that a user downloads from the Internet.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	File name of the download.
Download Source	The URL of the file that was downloaded.
Saved To	Saved to location.
State	State of the download.
Opened By User	If the download is opened by the user.
Start Time Date/Time - UTC (yyyy-mm-dd)	Download start time.
End Time Date/Time - UTC (yyyy-mm-dd)	Download end time.
Bytes Downloaded	The bytes that were downloaded.
File Size(Bytes)	File size of the download.

Chrome Extensions

Description	Information about the extensions a user has installed on their Computer
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	Name of the Chrome plugin/extension
Version	Version number of the plugin/extension
Description	Description of the plugin/extension
Install Date/Time - UTC (yyyy-mm-dd)	Install time in Chrome/Webkit time
State	State of the plugin/extension on the google account (i.e enabled, disabled)
Installed by OEM	States whether the plugin/extension is installed by OEM (true or false)
Installed by Default	States whether the plugin/extension is installed by Default (true or false)
From Bookmark	States whether the plugin/extension was installed from a bookmark (true or false)
From Webstore	States whether the plugin/extension was installed from the chrome web-store (true or false)
Author	The author.
Homepage	The homepage.

Chrome FavIcons

Description	Contains the favicons that Chrome displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	Page URL of the favicon.
Icon URL	Icon URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	Last time the favicon was updated.
Icon	A preview of the favicon.

Chrome History Index

Description	An index of the webpages the user has visited in the past.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	The URL of the webpage.
Title	The title of the webpage.

ATTRIBUTE	DESCRIPTION
Visited On Date/Time - UTC (yyyy-mm-dd)	When the webpage was visited.
Body	A snippet of the webpage.

Chrome Keyword Search Terms

Description	Information about the keyword search terms that a user enters.
Notes	

ATTRIBUTE	DESCRIPTION
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.

Chrome Last Session

Description	Information about the previous browser session.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL.
Title	The title of the web page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Chrome Last Tabs

Description	Information about the tabs that were open during the previous session.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The web page URL.
Title	The title of the web page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.

ATTRIBUTE	DESCRIPTION
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Chrome Logins

Description	Login information that a user provides in Chrome. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the login page.
Username	The username entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the data was created.

Chrome Saved Credit Cards

Description	Chrome Saved Credit Cards contains information about the credit cards that a user has saved to their device.
Notes	

ATTRIBUTE	DESCRIPTION
Name On Card	The name of the person on the credit card.
Card Number	The number on the credit card.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the information was last modified.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time the credit card autofill information was last used.
GUID	An ID for the credit card.
Expiry Date	The date the credit card is supposed to expire in format 'month-year'.

Chrome Shortcuts

Description	Contains all of the shortcuts used by Google Chrome for user entered URLs.
Notes	

ATTRIBUTE	DESCRIPTION
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.
Last Access Date/Time - UTC (yyyy-mm-dd)	The last access time of the shortcut.
Web Page Title	The title of the web page.
Times Used	The number of times the shortcut has been used.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Type	The type of shortcut (for example, 'typed url' or 'bookmark').

Chrome Sync Accounts

Description	Chrome Sync Accounts contains information about the Chrome accounts that a user has logged in with. Chrome syncs data to the cloud so that a user can log in on multiple devices.
Notes	

ATTRIBUTE	DESCRIPTION
Sync Id	The unique id for the account that's used to sync data to the cloud.
Account Name	The name of the sync account.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the sync account was created.

Chrome Sync Data

Description	Chrome Sync Data contains information about the data that Chrome has synced to a user's account in the cloud.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the sync key.
Local Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the value on the local system.
Server Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the value on the server.
Local Created Date/Time - UTC (yyyy-mm-dd)	The created time of the value on the local system.
Server Created Date/Time - UTC (yyyy-mm-dd)	The created time of the value on the server.
Type	The type of data that is synced (bookmark, favicon, type URL, and so on).
Parsed Content	The type parsed data.
Favicon Image	The actual favicon image.

Chrome Top Sites

Description	A list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Notes	

ATTRIBUTE	DESCRIPTION
URL	URL of the site.
Title	Title of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the site was last updated.
Rank	A ranking of the website, in terms of how frequently it was visited. A value of 1 indicates the most frequent and values increment to 8 as frequency decreases. A value of -1 indicates a site that the user manually added to the list of top sites.
Thumbnail	Thumbnail of the site

Chrome Web History

Description	A history of the websites that the user visits (includes unique visits only).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

Chrome Web Visits

Description	A history of the websites that the user visits (includes all visits).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited webpage.
Title	The title of the webpage that was visited.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Firefox Add-ons

Description	Contains the add-ons from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the add-on.
Version	The version the add-on.
Installed Date/Time - UTC (yyyy-mm-dd)	The date/time when the add-on was installed.
Updated Date/Time - UTC (yyyy-mm-dd)	The date/time when the add-on was updated.
Extension Enabled	Whether the add-on is enabled by the user.

ATTRIBUTE	DESCRIPTION
Description	The description of the add-on.

Firefox Bookmarks

Description	Contains the bookmarks from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the website that was bookmarked.
Date Added Date/Time - UTC (yyyy-MM-dd)	The Date/Time the bookmark was created.
Last Modified Date/Time - UTC (yyyy-MM-dd)	The Date/Time the field was last modified.
Title	The title of the bookmark.
Bookmark Type	The type of bookmark, can be either 'Bookmark Item' or 'Bookmark Folder'.

Firefox Cache Records

Description	Contains all of the cached entries in the Firefox Cache Map.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the cache entry.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cache entry was created.
MIME Type	The MIME type of the cache data.
Content Size (Bytes)	The content size of the cached data.
Image	The image, should one be associated with the cache entry.
Content	The content, should any be associated with the cache entry.

Firefox Cookies

Description	Contains the cookies from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
Host	The host domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-MM-dd)	The Date/Time the cookie was last accessed.
Created Date/Time - UTC (yyyy-MM-dd)	The Date/Time the cookie was created.
Expiration Date/Time - UTC (yyyy-MM-dd)	The Date/Time the cookie will expire, if it is set to expire.
Path	The path to the cookie.

Firefox Downloads

Description	Contains the downloads from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file being downloaded.
Download Source	The URL of the file being downloaded.
Start Date/Time - UTC (yyyy-MM-dd)	The Date/Time the download was started.
End Date/Time - UTC (yyyy-MM-dd)	The Date/Time the download was ended.
Saved To	The path to where the file was downloaded to.
Temp Path	The path to where the file was saved during downloading.
State	The state of the download can be 'Download In Progress', 'Download Complete', 'Download Stopped', or 'Download Paused'.
Referrer	If the web page used a mirror for downloading, the path to the original download URL.

Firefox FavIcons

Description	Contains the fav icons from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the icon.

Firefox FormHistory

Description	Contains the form history from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
Field Name	The name of the field.
Value	The value of the field.
First Used Date/Time - UTC (yyyy-MM-dd)	The Date/Time the field was first used.
Last Used Date/Time - UTC (yyyy-MM-dd)	The Date/Time the field was last used.
Times Used	The number of times the field has been used.
ID	The unique ID of the field.

Firefox Input History

Description	Contains the input to forms from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL the input was given to.
Input	The value that was given.
Use Count	The number of times the input has been used.
ID	The unique ID of the input.

Firefox Private Browsing History

Description	Contains the URLs that were loaded during a Private Browsing session from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL.

Firefox SessionStore Artifacts

Description	Contains the web pages from the last active session from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the web page.
URL	The URL of the web page.
Referrer URL	The URL of the web page, if the web page was a redirect.

Firefox Web History

Description	Contains the web pages from the last active session from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the web page.
Last Visited Date/Time - UTC (yyyy-MM-dd)	The Date/Time the web page was last visited.
Title	The title of the web page.
Visit Count	The number of times the web page has been visited.
Is Typed	Did the user type the URL, can be 'Yes' or 'No'.

Firefox Web Visits

Description	Contains all of the non-archived URL visits for Firefox.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL that was visited.
Title	The title of the page that was visited.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the page was visited.
Is Typed	Did the user type the URL, can be 'Yes' or 'No'.
Transition Type	How the transition to the page happened.

Google Analytics First Visit Cookies

Description	Information about Google Analytics first-visit cookies that are discovered in other artifacts.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the URL.
Creation DateTime	Date/Time when the site was vist visited.
Most Recent Visit Date/Time	Date/Time of most recent session.
2nd Most Recent Visit Date/Time	Date/Time of previous session.
Hits	Number of visit.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Google Analytics First Visit Cookies Carved

Description	Information about Google Analytics first-visit cookies that are recovered using carving.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the URL.
Creation DateTime	Date/Time when the cookie was created.
Most Recent Visit Date/Time	Date/Time of most recent session.
2nd Most Recent Visit Date/Time	Date/Time of previous session.
Hits	Number of visit.

Google Analytics Referral Cookies

Description	Information about Google Analytics referral cookies that are discovered in other artifacts.
Notes	

ATTRIBUTE	DESCRIPTION
Cookie Source	The source URL used to reach the site.
Host	Contains the domain of the URL.
Update Date/Time	The last time the cookie was updated.

ATTRIBUTE	DESCRIPTION
Campaign	The method of referral.
Access Method	Whether the site was accessed organically or was referred.
Keyword	Keywords used to arrive at the site.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Google Analytics Referral Cookies Carved

Description	Information about Google Analytics referral cookies that are recovered using carving.
Notes	

ATTRIBUTE	DESCRIPTION
Cookie Source	The source URL used to reach the site.
Host	Contains the domain of the URL.
Update Date/Time	The last time the cookie was updated.
Campaign	The method of referral.
Access Method	Whether the site was accessed organically or was referred.
Keyword	Keywords used to arrive at the site.

Google Analytics Session Cookies

Description	Information about Google Analytics session cookies that are discovered in other artifacts.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the URL.
Page Views	The number of visits to this page from the user.
Start Current Session Date/Time	The start time of the current sesion.
Outbound Link Events Left	
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Google Analytics Session Cookies Carved

Description	Information about Google Analytics session cookies that are recovered using carving.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the URL.
Page Views	The number of visits to this page from the user.
Start Current Session Date/Time	The start Date/Time of the current sesion.
Outbound Link Events Left	

Google Analytics URLs

Description	URLs that are discovered in other artifacts that are related to Google Analytics.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the web site. If the url cannot be recovered, the source of the url containing all the metadata is displayed instead.
Page Title	The name of the web site. This value is carved from the source starting after 'utmdt=' and ending at '&'
Host Name	Contains the domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Google Analytics URLs Carved

Description	Information about Google Analytics URLs that are recovered using carving.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the web site. If the url cannot be recovered, the source of the url containing all the metadata is displayed instead.
Page Title	The name of the web site. This value is carved from the source starting after 'utmdt=' and ending at '&'
Host Name	Contains the domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'

Google Maps

Description	Google Maps is a free web service that allows users to get directions.
Notes	

ATTRIBUTE	DESCRIPTION
Search Query	The term that was searched for
Starting Location	The starting location for navigation/directions.
Center of Map	Where the map was centered
Business Latitude and Longitude	The latitude and longitude of the business location.
Source Address	The source physical address.
Destination Address	The user's desired destination
Route Type	How the user will travel (eg. Car, bus, bike)
Additional Address	Any additional addresses within the navigation
Street View Latitude/Longitude	The latitude and longitude information in street view.

Google Maps Tiles

Description	Google maps is a free web service that allows users to get directions.
Notes	

ATTRIBUTE	DESCRIPTION
Image	The actual picture content.
X Coordinate	The X coordinate value that Google uses to download the right tile.
Y Coordinate	The Y coordinate value that Google uses to download the right tile.

ATTRIBUTE	DESCRIPTION
Zoom Level	The level that the user was zoomed in to the map. Can be understood as the Z coordinate value that Google uses to download the right tile.

Malware/Phishing URLs

Description	Records that are believed to be either malware or phishing related URLs.
Notes	

ATTRIBUTE	DESCRIPTION
Site Name	The name of the web site.
URL	The URL of the web site.
Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the artifact.
Artifact	The name of the artifact the URL belongs to.
Artifact ID	The row Id of the URL in the original artifact table.

Pornography URLs

Description	Records that are believed to be pornography related URLs.
Notes	For a list of the URLs that are targeted by this artifact, see Pornography URLs.

ATTRIBUTE	DESCRIPTION
Site Name	The name of the web site.
URL	The URL of the web site.
Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the artifact.
Artifact	The name of the artifact the URL belongs to.
Artifact ID	The row Id of the URL in the original artifact table.

Rebuilt Webpages

Description	Contains the data that allows for the reconstruction of web pages.
Notes	

ATTRIBUTE	DESCRIPTION
Page Title	The title.
URL	The URL.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the original record was created.
Domain	The domain.
Cache Table	The table the data to re-construct the page came from.
Cache RowID	The row id in the table that constructed the rebuilt web page.

Safari Bookmarks

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures information related to webpages that have been bookmarked.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The name of the bookmark.
URL	The URL that was bookmarked.
Locally Added	Indicates whether the bookmark was created on the local device or a synced device with the same Apple ID. On Mac OS Safari, this fragment is not available for every link.

Safari Cache Records

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures information related to webpages that have been cached on the local system.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL from which the file was downloaded.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cache file was created.
File Type	The type of the cached file.
Content Size	The size of the cached file.
Image	If the content file is an image, it will be displayed in this column.
Content	If the file is not an image (e.g. if it is a javascript file), the raw file content will be stored here.

Safari Downloads

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures information related to files that have been downloaded from Safari.
Notes	

ATTRIBUTE	DESCRIPTION
Download URL	The URL of the downloaded file.
Saved to Path	The local path where the download was saved.
Download Identifier	The unique identifier for the download.
Amount Downloaded (Bytes)	The number of bytes downloaded.
Size of Download (Bytes)	The size of the download in bytes.

Safari History

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures history entries which have been parsed from the filesystem.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of a visited web page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Redirect URL	The URL the user was redirected to.
Title	The title of the web page.
Visit Count	The number of times the URL was visited.
Visit Source	Whether the website was viewed on the local device or on a synced device.

Safari iCloud Devices

Description	Safari iCloud Devices contains information about the devices that are synced to an iCloud account. Each device can access any browser tabs that are synced to the account.
Notes	

ATTRIBUTE	DESCRIPTION
Unique Device Identifier	A unique ID for the device that is accessing the tab.
Device Name	The name of the device that is linked to the iCloud account.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the device first synced to the iCloud account.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the device last synced with the iCloud account.

Safari iCloud Tabs

Description	Safari iCloud Tabs contains information about tabs that have been opened in the browser and synced to an iCloud account. Synchronized tabs are available to any device that logs in to the iCloud account.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the tab.
URL	The URL address of the tab.
Unique Device Identifier	A unique ID for the device that is accessing the tab.
Device Name	The name of the device that is accessing the tab.
Tab ID	The unique ID of the tab.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the tab was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the tab was last modified.
Modified By	The name of the device that last modified the tab.
Close Requested	Indicates whether a close request has been opened for the tab.
Close Request Date/Time - UTC (yyyy-mm-dd)	The date and time when the close request was created.

Safari Last Session

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures information related to the user's last session with Safari.
Notes	

ATTRIBUTE	DESCRIPTION
Tab URL	The webpage URL.
Tab Title	The title of the webpage.

Safari Preferences

Description	Safari Preferences contains important Safari Browser settings.
Notes	

ATTRIBUTE	DESCRIPTION
Homepage	The URL of the user's homepage.
Search Engine	The search engine used by the user to perform searches. The default search engine is Google.
Download Location	The folder location where downloaded items get saved. The user can specify a folder, or they may choose to manually select a download location with each download.
Remove Download Items Frequency	Indicates how frequently Safari should clear the download history. The default value is "Manually".
Clear History Frequency	Indicates how frequently Safari should clear the browser history. The default value is "Manually".
Open Safe Downloads	An option to automatically open "safe" download files, such as movies, pictures, sounds, PDF, text documents, and archives. Default is true.

Safari Recently Closed Tabs

Description	Safary Recently Closed Tabs contains a history of recently closed tabs in the Safari browser.
Notes	

ATTRIBUTE	DESCRIPTION
Tab URL	The webpage URL.
Tab Title	The title of the webpage.
Close Requested	The date and time that the tab close request was made. This date time is stored as either UTC or local time format.

Safari Top Sites

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures information related to the user's top sites
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL.
Title	The title of the webpage.
Feed Last Update Time	The date and time that the top site content was last updated.
Feed URL	The URL of the RSS feed.

WebKit Browser Session/Tabs (Carved)

Description	WebKit Browser Sessions/Tabs contains information about the browser sessions and tabs that the user has open, while using a browser built with WebKit. Some examples of browsers that use WebKit are Chrome, Opera, and 360 Safe Browser. This artifact consolidates the existing Chrome, Safe Browser, and Opera equivalents in a single artifact. Usage of other browsers, such as Firefox and Safari, aren't likely to appear under this artifact.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The web page URL.
Title	The title of the web page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

WebKit Browser Web History (Carved)

Description	WebKit Browser Web History contains information about the websites that a user visits while using a browser built with WebKit. Some examples of browsers that use WebKit are Chrome, Opera, and 360 Safe Browser. This artifact consolidates the existing Chrome, Safe Browser, and Opera equivalents in a single artifact. Usage of other browsers aren't likely to appear under this artifact, however, some URLs found by other browsers may also be found by this artifact.
Notes	

ATTRIBUTE	DESCRIPTION
URL	URL of the visited webpage.
Title	Title of the visited webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time this webpage was last visited
Visit Count	The number of times the webpage was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

CLOUD

Chat

Cloud Google Hangouts Messages

Description	Google Hangouts messages that are sent or received by the logged in user and recovered from the cloud.
Notes	

ATTRIBUTE	DESCRIPTION
Conversation Name	The name of the conversation.
Sender Username	The user name of the sender of the message.
Text	The message that was sent.
Sent Date/Time	The date and time of the message.
Participants	The name of the participants in that conversation.
Message Type	The message type.
Latitude	The latitude of a location shared through a message or attachment.
Longitude	The longitude of a location shared through a message or attachment.
Conversation Status	The status of the conversation.
Conversation View	Indicates where the conversation is located (Inbox or Archive).
Conversation ID	The conversation ID.
Attachments	The names of the locally downloaded files.

Cloud Slack Channels

Description	Cloud Slack Channels contains information about each of the channels and conversations that exist in a user's Slack workspace.
Notes	

ATTRIBUTE	DESCRIPTION
Channel Name	The name of a channel or message group.
Channel ID	The ID of a channel or message group.
Channel Type	The type of the channel.
Created By	The name or user ID of whoever created the channel.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the channel was created.
Topic	The topic text for the channel.
Topic Author	The name or user ID of whoever last updated the topic text.
Purpose	The purpose of the channel.
Purpose Author	The author that set the channel purpose.
Channel Members	The user names of the members in the channel.
Members Count	The number of members in the channel.
Last Read Date/Time - UTC (yyyy-mm-dd)	The date and time when the channel was last read.
Member	Indicates whether or not the local user is a member of the channel.

Cloud Slack Messages

Description	Slack Messages contains messages sent or received in channels in the user's Slack workspace.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The user name of whoever sent the message.
Recipient(s)	If the message is a direct message, this attribute indicates the recipient's user name. If the message is a group message, this attribute indicates the group or channel name.
Direction	The direction of the conversation relative to the signed in user.
Message Type	The type of message.
Conversation ID	The Slack conversation ID for the chat.
Message	The message text.

ATTRIBUTE	DESCRIPTION
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Workspace ID	The unique identifier for the slack workspace.
Attachment URL	The URL associated with any link attachments to the message.
Attachment Name	The name of any attachment associated with the message.
Attachment ID	The Slack ID used to identify the file.

Cloud Slack Users

Description	Cloud Slack Users contains information about each user in the Slack workspace.
Notes	

ATTRIBUTE	DESCRIPTION
Workspace ID	The unique identifier for the slack workspace.
Full Name	The full name of the user.
User Name	The unique user name of the user.
Display Name	The slack display name of the user.
Email	The user email.
Phone Number	The user phone number.
Member ID	The user ID.
Title	The user title.
Status Message	The status message for the user
Account Type	The type of account the user has.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the user was last updated.
Timezone	The timezone the user is located in.

Cloud Slack Workspaces

Description	Cloud Slack Workspaces contains information about each of the workspaces that the user is a member of.
Notes	

ATTRIBUTE	DESCRIPTION
ID	The unique identifier for the slack workspace.

ATTRIBUTE	DESCRIPTION
Name	The name of the slack workspace.
Domain	The domain of the slack workspace.
Email Domain	The email domain of the slack workspace.
Enterprise ID	If the team belongs to an Enterprise Grid, this field represents the enterprise ID for the organization.
Enterprise Name	If the team belongs to an Enterprise Grid, this field represents the enterprise name for the organization.

Cloud

Cloud Amazon EC2 Instances

Description	EC2 instances are virtual machines that corporations use for hosting secure services and storing data securely in the cloud. To acquire this data, Magnet AXIOM exports this instance to Amazon's S3 service and downloads it from there.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file after it's exported from EC2.
Instance ID	The unique ID of the EC2 instance.
Instance State	The status of the EC2 instace (running, stopped, or terminated).
Owner ID	The numerical ID of the user who launched the EC2 instance.
Instance Creation Date/Time	The date and time when the user launched the EC2 instance.
IP Address	The private IP address of the user who launched the EC2 instance.
Region	The region where the instance was launched.
Instance Type	The type of EC2 instance.
AMI ID	The ID of the AMI (Amazon Machine Image) with which the instance was launched.
Key Name	The name of the key pair that must be used to login to the instance securely.
File Path	The path from the root of S3 to the exported image.
Attachment	The path to the downloaded file.

Cloud Azure Virtual Machine Snapshots

Description	Azure virtual machines are on-demand computing resources used by organizations for hosting services and storing data securely in the cloud. To acquire this data, Magnet AXIOM creates snapshots of all disks attached to a given virtual machine, and downloads the snapshots for analysis.
Notes	

ATTRIBUTE	DESCRIPTION
Resource ID	The fully-qualified ID of the virtual machine resource.
Snapshot Name	The name of the snapshot created during processing.
Parent Virtual Machine Name	The name of the virtual machine that this disk belongs to.
Region	The region the targeted virtual machine was deployed to.
Disk Type	Indicates whether the targeted disk is an operating system disk or an attached data disk.
Disk Capacity in Gigabytes	Maximum capacity for the targeted disk in gigabytes.
Disk Creation Date/Time - UTC (yyyy-mm-dd)	The date/time the disk was created and assigned to the targeted virtual machine (in UTC).
Snapshot Creation Date/Time - UTC (yyyy-mm-dd)	The date/time that the disk snapshot was created (in UTC).
Attachment	The name of the snapshot downloaded as a VHD file.

Cloud Box.com Enterprise Events

Description	The Cloud Box Enterprise event contains information about administrative events that are triggered by user actions. Some examples of events include new user creation, successful login, and item syncs. You can see a full list at https://developer.box.com/v2.0/reference#enterprise-events.
Notes	

ATTRIBUTE	DESCRIPTION
Initiator Email	The email address of the user the initiated the event.
Event Type	The type of the event that was created (for example, 'NEW_USER').
Subject Email	The email address of the user that was the subject of the event.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the event was initiated.
Event ID	The ID of the event.
IP Address	The IP address of the user that initiated the event.

ATTRIBUTE	DESCRIPTION
Type	The type of the item that was targeted by the event (always a user or nothing).
Initiator Name	The name of the user that initiated the event.
Initiator ID	The ID of the user that initiated the event.
Subject Name	The name of the user that was the subject of the event.
Subject ID	The ID of the user that was the suject of the event.

Cloud Box.com Files

Description	Files that are stored in Box that are recovered from the cloud. Box is a file hosting service that allows users to upload and sync files to the cloud and access or share them from multiple locations.
Notes	

ATTRIBUTE	DESCRIPTION
Attachments	The path to the downloaded file.
File Created Date/Time	The file upload date.
Creator Email Address	The email address of the original uploader of the file.
Creator ID	The unique Box ID of the original uploader of the file.
Creator Name	The name of the original uploader of the file.
Description	The description attached to a file through Box.
Download Count	The number of times the file has been downloaded via a share link. This does not include downloads performed by API calls.
File Hash	The file's SHA1 hash, provided by Box.
File ID	The file's unique Box ID.
Last Modified Date/Time	The file's last modified date and time.
Last Modifier Email	The email address of the latest user to modify the file.
Last Modifier ID	The unique Box ID of the latest user to modify the file.
Last Modifier Name	The name of the latest user to modify the file.

ATTRIBUTE	DESCRIPTION
Owner Email	The email address of the owner of the file.
Owner ID	The unique Box ID of the owner of the file.
Owner Name	The name of the owner of the file.
Box File Path	The filepath of the file.
Preview Count	The number of times the file has been previewed via a share link.
Access	The permissions setting a file's share link. Null if no share link exists, 'open' if anyone with the link can access, and 'collaborators' if only collaborators on the file can access.
Download Permissions	True if users can download the file through a share link.
Preview Permissions	True if users can preview the file through a share link.
File Size (Bytes)	The size of the file, in bytes, according to Box.
Type	The type of the file. Value is either 'file' or 'folder'.

Cloud Box.com User Events

Description	The Cloud Box User Events artifact contains information about actions that are triggered by the user. Some examples of events include item creation, upload, and download. You can see a full list of events at https://developer.box.com/v2.0/reference#user-events.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the user that caused the event creation.
Event Type	The type of event that occurred (for example, 'ITEM_CREATE').
File Name	The name of the file that was targeted by the action/event.
File Path	The path to the folder that was targeted by the action/event.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time in which the event was created.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time in which the event was recorded.
User Email	The email address of the user that initiated the event.
User ID	The ID of the user that initiated the event.

ATTRIBUTE	DESCRIPTION
Type	The type of the item that was targeted by the action (usually file or folder).
Source ID	The ID of the item that was targeted by the action.
Event ID	The ID of the event.

Cloud Dropbox Files

Description	Files that are stored in Dropbox that are recovered from the cloud. Dropbox is a file hosting service that allows users to upload and sync files to the cloud and access them from multiple locations.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The original name of the file.
File ID	A unique identifier for the file.
Dropbox File Path	Path of the file in Dropbox
Updated File Name	The name of the file, if it's been updated.
Server Modified Date/Time - UTC (yyyy-mm-dd)	The file's last modified date and time on the Dropbox server.
Client Modified Date/Time - UTC (yyyy-mm-dd)	The file's last modified date and time on the client application.
Photo Timestamp Date/Time - UTC (yyyy-mm-dd)	If the file is a photo, the date and time the photo was originally taken
File Hash	The hash of the file generated by Dropbox. For more information, see https://www.dropbox.com/developers/reference/content-hash.
File Version ID	The version ID of the file. This value is used to determine if there are any updates on the server that need to be synced locally.
File Type	The type of file
Attachments	The path to the downloaded file.

Cloud Facebook Messenger Messages (Warrant Return)

Description	Facebook Messenger Messages (Warrant Return) contains individual messages that are parsed from chat threads that Facebook has included in a warrant return. The 'messages' in a chat thread can include messages, shared files or links, calls, and audio messages.
Notes	

ATTRIBUTE	DESCRIPTION
Author Name	The name of sender of the message.
Author ID	The Facebook ID of the author.
Participant	The participants of the chat thread.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Body	The text of the message.
Owner	The name of the ower of the chat (identifies the local user for chat threading).
Owner ID	The Facebook ID of the owner of the chat (identifies the local user for chat threading).
Thread ID	The ID of the chat thread that the message is from.
IP	The IP address of the sender of the message.
Attachments	A ZIP of any attachments to this message.
Attachment Name(s)	A list of the filenames of the attachments to this message.
Last Shared Date/Time - UTC (yyyy-mm-dd)	If the message was shared outside the chat, this value indicates the last date and time when it was shared.
Sharing Link	A link to the file, if the message contains a shared file.
Sharing Summary	A summary of the shared item, if the message contains a shared file or URL.
Sharing Text	A description of the shared item, if the message contains a shared file or URL.
Sharing Title	A title for the shared item, if the message contains a shared file or URL.
Sharing Url	A URL to the shared page, if the message contains a shared file or URL.
Call Type	If the message type is a call, this indicates whether the call is an audio or a video call.
Call Missed	A boolean value indicates whether the call was missed.
Call Duration	The duration of the call.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the chat thread was accessed by Facebook during the generation of the warrant return.

Cloud Google Activity

Description	Google Activity entries retrieved from the Google Activity website.
Notes	

ATTRIBUTE	DESCRIPTION
Action	The type of activity that occurred. For example, visited, searched for, and so on.
Description	Information about the activity. For example, the title of the website or the search criteria used.

ATTRIBUTE	DESCRIPTION
Date/Time - UTC (yyyy-mm-dd)	The date and time when the activity occurred.
URL	The URL associated with the activity.
Platform	The operating system or platform where the activity occurred. For example: Windows, Chrome OS, Apple iPhone, and so on.
Latitude	The latitude of the location where the activity occurred.
Longitude	The longitude of the location where the activity occurred.
Attachments	The path to the downloaded file.

Cloud Google Calendar Events

Description	Cloud Google Calendar Events contains information about the entries a user has saved to their Google Calendar.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the event.
Calendar Display Name	The name of the calendar.
Calendar Owner	The email of the owner of the calendar.
Status	The status of the event (Confirmed, Tentative, or Cancelled).
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the event was created in the calendar.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the event was last updated.
Description	A more complete description of the event.
Location	A free-form text description of the location/venue of the event.
Created By	The email of the user who created the event.
Organizer	The organizer's email of the calendar event.
Start Date/Time - Local	The local date and time that the event is scheduled to start.
Event Start Timezone	The timezone of the start date/time.
End Date/Time - Local	The local date and time that the event is scheduled to end.
Event End Timezone	The timezone of the end date/time.
Attendees	The list of attendee emails associated with the event.
User Response	The user response for the calendar event (Needs Action, Accepted, Declined, Tentative).
Recurrence	The recurrence rules for the event.

ATTRIBUTE	DESCRIPTION
Visibility	The visibility of the event (Default, Public, Private, or Confidential).
Web URL	The URL associated with the event.
Hangout URL	An absolute link to the Google+ hangout associated with this event.
Private	Indicates whether the event is private.
Locked	Indicates whether the event is locked.
Guests Can Invite Others	Indicates whether guests can invite others to the event.
Guests Can Modify	Indicates whether guests can modify the event.
Guests Can See Other Guests	Indicates whether guests can see the list of other guests that are attending.
Source URL	Source url from which the event was created.
ID	Unique ID within the calendar for this event.
Calendar ID	Unique ID for this calendar.

Cloud Google Calendar Events (Takeout)

Description	Cloud Google Calendar Events (Takeout) contains information about the entries a user has saved to their Google Calendar.
Notes	

ATTRIBUTE	DESCRIPTION
ID	Unique ID within the calendar for this object.
Type	The Calendar entry type, one of: Event, Todo or Journal.
Created Date/Time	Date and Time in UTC for which the entry was created in the calendar.
Start Date/Time	Date and Time in UTC when this entry is scheduled to start.
End Date/Time	Date and Time in UTC when this entry is scheduled to end.
Summary	A short summary of the entry.
Description	A more complete description of the entry.
Latitude	The latitude attached to the entry. This could be where the event will occur.
Longitude	The longitude attached to the entry. This could be where the event will occur.
Last Modified Date/Time	Date and Time in UTC when this entry was last modified.
Location Name	Free form text defining the intended venue for the entry.
Organizer	The organizer's email of the calendar entry.
Status	The status of the entry within the calendar, one of: Needs Action, Accepted, Declined, Tentative, Delegated, Completed, In Progress.

ATTRIBUTE	DESCRIPTION
URL	A URL associated with the event.
Recurrence	Indicates if the event is recurring.
Attendees	List of Attendee emails associated with the entry.
Categories	Tags associated with this event.
Comment	Specifies a comment to the user for this entry.
Contact Label	Contact information or alternately a reference to contact information associated with the entry.
Resources	Equipment or resources required for the entry.
Timezone	Timezone name associated with this entry.

Cloud Google Chats (Warrant Return)

Description	Google Chats parsed from a Google Warrant Return archive.
Notes	

ATTRIBUTE	DESCRIPTION
Message	The message that was sent.
Sender Email	The sender's email address.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time of the message.
Participants	The email addresses of all participants in the conversation.
Attachments	The name of the locally downloaded file.

Cloud Google Chrome Autofill

Description	Cloud Google Chrome Autofill contains information used in Google Chrome to automatically fill out contact information forms on the web. A user's account can contain multiple sets of autofill data, and this artifact creates a hit for each set it discovers.
Notes	

ATTRIBUTE	DESCRIPTION
Name	Full names that the user has saved to this autofill identity.
First Name	First names that the user has saved to this autofill identity.
Last Name	Last names that the user has saved to this autofill identity.
Middle Name	Middle names that the user has saved to this autofill identity.
Email Address	Email addresses that the user has saved to this autofill identity.

ATTRIBUTE	DESCRIPTION
Home Phone	Phone numbers that the user has saved to this autofill identity.
Home Address	The home street address that the user has saved to this autofill identity.
Address Line 1	The address line 1 that the user has saved to this autofill identity.
Address Line 2	The address line 2 that the user has saved to this autofill identity.
City	The city of residence that the user has saved to this autofill identity.
State/Province	The State or Province of residence that the user has saved to this autofill identity.
Zip/Postal Code	The ZIP or Postal code that the user has saved to this autofill identity.
Country Code	The country code that the user has saved to this autofill identity.
Sorting Code	The sorting code that the user has saved to this autofill identity. The sorting code serves as additional information around the postal code, such as a CEDEX code.
Dependent Locality	The dependent locality that the user has saved to this autofill identity. More specific city locations such as village, township, neighbourhood, and district belong here.
Language Code	The abbreviated language code that the user has saved to this autofill identity.
Company	The company of employment that the user has saved to this autofill identity.
Use Count	How many times this autofill identity has been used.
Last Used Date/Time - UTC (yyyy-mm-dd)	The time when this autofill identity was last used.
Source Information	The origin of this autofill identity. Usually the URL of website on which this information was first entered, or 'Chrome Settings' if it was entered through Chrome's autofill page.
GUID	A unique ID for this autofill identity.

Cloud Google Chrome Bookmarks

Description	Cloud Google Chrome Bookmarks contains information about the bookmarks a user has saved to their Google Account. Saved bookmarks can be synced across multiple devices.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The name of the bookmark or bookmark folder.
URL	The URL for the bookmark.
Icon URL	The icon URL for the bookmark.
Path	The absolute folder path to the bookmark.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time the bookmark was modified.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was added.

Cloud Google Chrome Browser History

Description	Cloud Google Chrome Browser History contains information about all URLs visited using Google Chrome.
Notes	

ATTRIBUTE	DESCRIPTION
Event Type	The event that caused this page to be visited, eg. LINK, TYPED, FORM_SUBMIT.
Title	Title of the web page.
URL	URL of the web page.
Timestamp Date/Time - UTC (yyyy-mm-dd)	The time when this page visit occurred
ID	The ID of the client which caused this visit. Unique per installation of Google Chrome.
Favicon URL	The URL for the favicon of the web page.

Cloud Google Chrome Extension Settings

Description	Cloud Google Chrome Extension Settings contains configuration settings for Chrome Extensions.
Notes	

ATTRIBUTE	DESCRIPTION
ID	The ID of the extension. Unique per extension, and is the same between users with the same extension.
Key	The name of the setting.
Value	The value of the setting.

Cloud Google Chrome Extensions

Description	Cloud Google Chrome Extensions contains information about installed Chrome Extensions.
Notes	

ATTRIBUTE	DESCRIPTION
Extension Name	The extension name.

ATTRIBUTE	DESCRIPTION
ID	The ID of the extension. Unique per extension, and is the same between users with the same extension.
Version Number	The version number of the extension.
Extension Enabled	Whether the extension is enabled by the user.
Incognito Enabled	Whether the extension is enabled in incognito browsing mode by the user.
Disable Reasons	The reason why the extension has been disabled. Possible values are as follows: DISABLE_USER_ACTION: Disabled by the user DISABLE_PERMISSIONS_INCREASE: Disabled due to an increase in required permissions DISABLE_RELOAD: Disabled until extension is reloaded DISABLE_UNSUPPORTED_REQUIREMENT: Disabled because of an unsupported requirement DISABLE_SIDELOAD_WIPEOUT: Disabled during a mass disabling of 3rd party extensions DEPRECATED_DISABLE_UNKNOWN_FROM_SYNC: Disabled because of synced disable state DISABLE_NOT_VERIFIED: Disable because Chrome could not verify the install DISABLE_GREYLIST: Disabled because the extension is blacklisted in the Windows registry DISABLE_CORRUPTED: Disabled because the extension is corrupted DISABLE_REMOTE_INSTALL: Disabled because it was remotely installed and must be enabled by the user DISABLE_EXTERNAL_EXTENSION: Disabled because it is an external extension and must be enabled by the user DISABLE_UPDATE_REQUIRED_BY_POLICY: Disabled because an update is required for the extension DISABLE_CUSTODIAN_APPROVAL_REQUIRED: Disabled because user requires approval by custodian DISABLE_BLOCKED_BY_POLICY: Disabled because management policy blocks the extension
Remote Install	Whether this extension was remotely installed from an android device.
Installed by Custodian	Whether this extension was installed by the custodian managing this user.
Update URL	The update URL for this extension.

Cloud Google Chrome Search Engines

Description	Cloud Google Chrome Search Engines contains information about search engines the user has used.
Notes	

ATTRIBUTE	DESCRIPTION
Short Name	The name of the search engine.
URL	The URL of the search engine.
Suggestions URL	The URL which returns suggested searches.
Originating URL	The URL of the XML configuration file for the search engine.

ATTRIBUTE	DESCRIPTION
Instant URL	The URL used by the Chrome Instant feature.
New Tab URL	The URL for the search engine upon opening a new browser tab.
Alternate URL	A list of alternate URLs for the search engine.
Favicon URL	The URL for the favicon associated with the search engine.
Picture URL	The URL for the image associated with the search engine.
Image URL Post Params	The POST parameters to be used with the image URL.
Search Terms Replacement Key	Keyword for activating Chrome Instant feature.
Show in Default List	Whether this search engine will appear in the default search engines list in Chrome.
Created Date/Time - UTC (yyyy-mm-dd)	The time when this search engine was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time for this search engine.
Sync GUID	Unique ID for this search engine.
Keyword	A keyword used to activate this search engine in Chrome.
Input Encodings	Encodings for the input into this search engine, such as UTF-8.

Cloud Google Chrome Sync Settings App Settings

Description	Cloud Google Chrome Sync Settings - App Settings contains information about Chrome app settings to sync between devices.
Notes	

ATTRIBUTE	DESCRIPTION
ID	The ID of the app. Unique per app, and is the same between users with the same app.
Key	The name of the setting.
Value	The value of the setting.

Cloud Google Chrome Sync Settings Apps

Description	Cloud Google Chrome Sync Settings - Apps contains information about Chrome apps to sync between devices.
Notes	

ATTRIBUTE	DESCRIPTION
Extension Name	The app name.
ID	The ID of the app. Unique per app, and is the same between users with the same app.
Version Number	The version number of the app.
Extension Enabled	Whether the app is enabled by the user.
Incognito Enabled	Whether the app is enabled in incognito browsing mode by the user.
Disable Reasons	The reason why the app has been disabled. Possible values are as follows: DISABLE_USER_ACTION: Disabled by the user DISABLE_PERMISSIONS_INCREASE: Disabled due to an increase in required permissions DISABLE_RELOAD: Disabled until app is reloaded DISABLE_UNSUPPORTED_REQUIREMENT: Disabled because of an unsupported requirement DISABLE_SIDELOAD_WIPEOUT: Disabled during a mass disabling of 3rd party apps DEPRECATED_DISABLE_UNKNOWN_FROM_SYNC: Disabled because of synced disable state DISABLE_NOT_VERIFIED: Disable because Chrome could not verify the install DISABLE_GREYLIST: Disabled because the app is blacklisted in the Windows registry DISABLE_CORRUPTED: Disabled because the app is corrupted DISABLE_REMOTE_INSTALL: Disabled because it was remotely installed and must be enabled by the user DISABLE_EXTERNAL_EXTENSION: Disabled because it is an external app and must be enabled by the user DISABLE_UPDATE_REQUIRED_BY_POLICY: Disabled because an update is required for the app DISABLE_CUSTODIAN_APPROVAL_REQUIRED: Disabled because user requires approval by custodian DISABLE_BLOCKED_BY_POLICY: Disabled because management policy blocks the app
Remote Install	Whether this app was remotely installed from an android device.
Installed by Custodian	Whether this app was installed by the custodian managing this user.
Update URL	The update URL for this app.

Cloud Google Chrome Sync Settings Preferences

Description	Cloud Google Chrome Sync Settings - Preferences contains information about Chrome settings to sync between devices.
Notes	

ATTRIBUTE	DESCRIPTION
Key	The name of the setting.
Value	The value of the setting.

Cloud Google Connected Apps

Description	Google Connected Apps recovered from the Cloud.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The name of the application.
Permissions	The application access permissions.
Authorization Date - Local Time	The date that authorization to use the application was granted.
Source	The location of where the application was found.
Location	A byte offset within the source where the Google Connected Apps data has been acquired.

Cloud Google Contacts

Description	Cloud Google Contacts contains information about the contacts and services that a user has saved to their Google account.
Notes	

ATTRIBUTE	DESCRIPTION
Display Name	The display name of the contact.
Nickname	The nickname of the contact.
Gender	The gender of the contact
Email Address (es)	The email addresses of the contact.
Mobile Phone	The mobile phone number of the contact.
Home Phone	The home phone number of the contact.
Home Address	The home address of this contact.
Title	The job title of this contact.
Organization	The organization or business associated with the contact.
Business Phone	A business phone number for the contact.
Business Address	The physical address of the business associated with the contact.
Phone Numbers	Any other phone numbers that are associated with the contact, excluding any home, business or cell phone number.

ATTRIBUTE	DESCRIPTION
Website URL	A list of website URLs associated with the contact.
Tags	Any tags that are associated with the contact (also known as labels).

Cloud Google Devices (Warrant Return)

Description	Google Device (Warrant Return) contains information about the target account of the warrant return.
Notes	

ATTRIBUTE	DESCRIPTION
Gaia (Google Accounts and ID Administration) ID	The Google Accounts and ID Administration (GAID) ID.
Device Type	The type of device used to access the Google Account.
Brand	The brand of the device used to access the Google Account.
Device Model	The model of the device used to access the Google Account.
Operating System	The operating system of the device used to access the Google Account.
Device Last Country	The last country the device was used to access the Google Account.
Device Last Location Time	The last location time that the device was used to access the Google Account.
Device First Activity Time	The first time the device was used to access the Google Account.
Device Last Activity Time	The last time the device was used to access the Google Account.

Cloud Google Drive Files

Description	Files that are stored in Google Drive that are recovered from the cloud. Google Drive is a file hosting service that allows users to upload and sync files to the cloud and access them from multiple locations.
Notes	

ATTRIBUTE	DESCRIPTION
Id	The ID of the file assigned by Google Drive.
File Name	The name of the file on Google Drive.
Folder Structure	The folder structure the file resides in.

ATTRIBUTE	DESCRIPTION
Drive Owner	The owner of the google drive (e.g. testing@gmail.com).
Owner Name	The name of the author of the file.
Owner Email	The email address of the author of the file.
Shared	The number of accounts the file is shared with.
MIME Type	An identifier used to described the type and format of the file (for example text/plain). For more information, see https://en.wikipedia.org/wiki/Media_type.
File Size (Bytes)	The file size.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created.
Last Viewed By Me Date/Time - UTC (yyyy-mm-dd)	The last date and time the file was viewed by the user.
Last Modified By Me Date/Time - UTC (yyyy-mm-dd)	The last date and time the file was modified by the user.
Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time the file was modified.
Last Modified Name	The last user to modified the file.
Last Modified Email	The last modifying user's email address.
Shared With Me Date/Time - UTC (yyyy-mm-dd)	The time at which the file was shared with the user.
Trashed Date/Time (Team Drives) - UTC (yyyy-mm-dd)	The time the file was trashed. Only populated for Team Drive files.
Source Locations	A list of the spaces where the file exists. Supported values are drive, appDataFolder, and photos.
Parent Folder	The parent of the folder where the file resides.
Web URL	The direct URL to the file.
Download URL	The direct URL to download the file.
Attachments	The raw data of the file.

Cloud Google Keep

Description	The Cloud Google Keep artifact contains notes and lists the user wrote and saved to their Google account.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the note, when specified.
Modified Date/Time - Local Time	The date and time the note was modified.
Body	The body content of the note
Pinned	Indicates wether the note was pinned.
Archived	Indicates wether the note was archived.
Labels	Any labels added to the note.
Has Attachments	Indicates wether the note has attachments.

Cloud Google Login History (Warrant Return)

Description	Google Login History (Warrant Return) contains information about the logins and logouts made by the user account of the warrant return.
Notes	

ATTRIBUTE	DESCRIPTION
IP Address	The IP address of the device on which the action was executed.
Type	The type of action executed.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the action.
Details	Information about the action that occurred.

Cloud Google Passwords

Description	Google Passwords recovered from the Cloud.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The name of the application that saved the passwords.
User Name	The username associated to the application
Password	The saved password.
Source	The location of where the passwords were found.
Location	A byte offset within the source where the Google Passwords data has been acquired.

Cloud Google Photos (Warrant Return)

Description	Google Photos (Warrant Return) contains information about pictures recovered from the target user's Google account.
Notes	

ATTRIBUTE	DESCRIPTION
Hex Id	The Hex ID of the photo in the warrant return.
Created Date/Time - Local Time	The local date and time the photo was created.
Modified Date/Time - Local Time	The local date and time the photo was last modified.
Upload IP	The IP address of the user who uploaded the photo.
Title	The title of the photo.
Status	The status of the user who uploaded the photo.
Caption	The caption of the photo.
Location	The location the photo was taken.
Album ID	The ID of the photo album.
Album Title	The title of the photo album.
Comments	The comments associated with the photo.
Tags	The tags associated with the photo.
People	The people identified in the photo.
EXIF - Camera	The camera used to take the photo (as extracted from the picture's EXIF Data).
EXIF - Width	The width of the image (as extracted from the picture's EXIF Data).
EXIF - Length	The length of the image (as extracted from the picture's EXIF Data).

Cloud Google Recent Devices

Description	Google Recent Devices recovered from the Cloud.
Notes	

ATTRIBUTE	DESCRIPTION
Device Name	The name of the device.
Device Location	The location of the device.
Last Access Date/Time - Local Time	The last time Google was accessed from the device.
Device Status	The last time the device was synced to Google.

ATTRIBUTE	DESCRIPTION
Browser Name	The name of the browser the device accessed.
Device Model	The device model number.
Computer Name	The name of the computer the device was synced to.

Cloud Google Tasks

Description	Cloud Google Tasks contains information about the tasks that a user has saved to their Google account.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the task.
Type	The type of entry (a tasklist, a task or a subtask)
Task List	The title of the tasklist the task belongs to.
Parent Task	The title of the parent task.
Status	Indicates whether a task has been completed (values are either need-sAction or completed).
Last Modified Date/Time - UTC (yyyy-mm-dd):	The last date and time the task was modified.
Due Date - UTC (yyyy-mm-dd)	The date and time the task is due to be completed.
Completed Date - UTC (yyyy-mm-dd)	The data and time the task was completed.
Notes	The notes describing the task.
ID	The ID of the task assigned by the system.
Parent ID	The ID of the task's parent task.
Version	The version tag of the task.
Content Link	The URL pointing to the task.

Cloud iCloud Mail

Description	Cloud iCloud Mail contains the messages and attachments recovered from an iCloud Mail account.
Notes	

ATTRIBUTE	DESCRIPTION
To	The recipients of the email.

ATTRIBUTE	DESCRIPTION
From	The sender of the email.
Date/Time	The date and time the email was created.
Subject	The subject of the email.
Body	The body of the email.
CC	The recipients of the email that were CC'd.
BCC	The recipients of the email that were BCC'd.
Folder Path	The folder path of where the email is stored.
Headers	The raw email headers.
Attachments	The list of attachments on the email.

Cloud Instagram Account Actions (Warrant Return)

Description	Instagram Account Actions (Warrant Return) contains the list of actions made by the user that Instagram has included in a warrant return.
Notes	

ATTRIBUTE	DESCRIPTION
Action	A description of the action executed on the account.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the action.
IP Address	The IP address of the device on which the action was executed.
Account Name	The handle of the user.
ID	The unique ID of the account.

Cloud Instagram Comments (Warrant Return)

Description	Instagram Comments (Warrant Return) contains the list of comments that Instagram has included in a warrant return.
Notes	

ATTRIBUTE	DESCRIPTION
Author ID	The ID of the target user.
Author Name	The name of the target user.
Comment ID	The ID of the comment.
Content	The content of the comment.

ATTRIBUTE	DESCRIPTION
Date/Time Created - UTC (yyyy-mm-dd)	The UTC date time the comment was posted.
Status	The status of the comment.
Media ID	The ID of the media related to the comment.
Media Owner Name	The owner name of the media related to the comment.
Media Owner ID	The owner ID of the media related to the comment.

Cloud Instagram Direct Shares (Warrant Return)

Description	Instagram Direct Shares (Warrant Return) contains the list of direct shares of the user that Instagram has included in a warrant return.
Notes	

ATTRIBUTE	DESCRIPTION
Picture	The picture data that was recovered.
Content	The content of the direct share message.
Author Name	The name of the author of the direct share message.
Author ID	The Instagram ID of the author of the direct share message.
Participants	The participants of the direct share.
Date/Time - UTC (yyyy-mm-dd)	The date and time the direct share message was sent.
Type	The type of the direct share message.
IP Address	The IP Address of the user that sent the direct share message.
URL	The URL of the content that was shared.
Local Name	The name of the local user.
Local User ID	The Instagram ID of the local user.
ID	The ID of the direct share message.
Thread ID	The ID of the thread the direct share was a part of.

Cloud Instagram Direct Stories (Warrant Return)

Description	Instagram Direct Stories (Warrant Return) contains the list of direct stories sent by the user that Instagram has included in a warrant return.
Notes	

ATTRIBUTE	DESCRIPTION
Author Name	The name of the author of the story.
Author ID	The Instagram ID of the author of the story.
Recipient(s)	The recipient(s) of the direct story.
Date/Time - UTC (yyyy-mm-dd)	The date and time the story was sent.
Media ID	The ID of the picture or video featured in the story.
Attachment Name	The picture or video featured in the story.

Cloud Instagram Followers and Following (Warrant Return)

Description	Instagram Followers and Following (Warrant Return) provides information about who the user is following and who their followers are, which is parsed from an Instagram warrant return.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The Instagram handle for the user.
Display Name	The name of the Instagram user, as they've provided in their user profile.
User ID	The unique identifier for this User.
Followed By	Nullable. User Name of the user that is following this account.
Following	Nullable. User Name of the user that this account is following.

Cloud Instagram Photos (Warrant Return)

Description	Instagram Photos (Warrant Return) contains the list of all of the user's photos and any comments attached to the photo. Each comment is displayed as an individual hit and you can view a thread of the comments in the chat threading view in AXIOM Examine. You can identify the photo that a comment belongs to using the Photo ID attribute.
Notes	

ATTRIBUTE	DESCRIPTION
Picture	The picture data that was recovered.
Comment	A comment posted on the photo (by another user or the photo's author).
Author Name	The name of the author of the comment.
Author ID	The ID of the author of the comment.

ATTRIBUTE	DESCRIPTION
Comment Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the comment was posted on the photo.
Comment ID	The ID of the comment.
Message Status	The status of the comment. The values of this attribute might indicate cases where a comment has been edited or removed, but this has not been verifiable.
Photo Id	The ID of the photo that the user posted to Instagram.
Image Date/Time - UTC (yyyy-mm-dd)	The date and time that the photo was uploaded.
IP Address	The IP Address of the user that uploaded the photo.
Web Url	The Instagram URL of the photo that was uploaded
Draft	publicly or is still in draft (Yes indicates that the post is still in draft, and No indicates that it's been posted publicly).
Shared	Indicates whether the photo was shared with another user.
Status	The status of the photo.
Source Locations	The device or location from which the photo was uploaded.
Image Filter	The Instagram filter that was applied to the photo.
Local Name	The name of the local user.
Local User ID	The Instagram ID of the local user.
Type	Indicates whether this instance is a comment or a photo.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
MD5 Hash	An MD5 hash of the picture content.
SHA1 Hash	A SHA1 hash of the picture content.
PhotoDNA Hash	The hash of the picture content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

Cloud Lyft Profile Information

Description	Lyft profile information recovered from the cloud.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The unique ID of the user.
First Name	The first name of the user.
Last Name	The last name of the user.
Email	The email address of the user.

ATTRIBUTE	DESCRIPTION
Phone Number	The phone number of the user.
Email Verification Date/Time	The date and time the user verified their account with their registered email.
Has Taken Ride	Indicates whether the user has taken a ride.
Photo URL	The URL of the user's profile photo.

Cloud Lyft Trip Information

Description	Lyft Trips contains summaries of the trips taken by a Lyft user, and recovered from the cloud using their account credentials.
Notes	

ATTRIBUTE	DESCRIPTION
Ride ID	The unique ID for the ride.
Pickup Address	The pickup location address, as specified by the user.
Pickup Latitude	The GPS Latitude coordinates of the specified pickup location.
Pickup Longitude	The GPS Longitude coordinates of the specified pickup location.
Departure Date/Time - UTC (yyyy-mm-dd)	The date and time the rider was picked up from their pickup location.
Dropoff Address	The address specified by the rider for drop-off.
Dropoff Latitude	The GPS Latitude coordinates of the specified drop-off location.
Dropoff Longitude	The GPS Longitude coordinates of the specified drop-off location.
Arrival Date/Time - UTC (yyyy-mm-dd)	The date and time the rider was dropped off at their destination.
Origin Address	The original address specified by the rider for pickup.
Origin Latitude	The original GPS Latitude coordinates of the specified pickup location.
Origin Longitude	The original GPS Longitude coordinates of the specified pickup location.
Destination Address	The original address specified by the rider for drop-off.
Destination Latitude	The original GPS Latitude coordinates of the specified drop-off location.
Destination Longitude	The original GPS Longitude coordinates of the specified drop-off location.
Driver ID	The unique ID of the driver.
Driver Name	The first name of the driver.
Driver Phone Number	The phone number of the driver.

ATTRIBUTE	DESCRIPTION
Account Activation Date/Time - UTC (yyyy-mm-dd)	The date and time the driver activated their account.
Driver Picture URL	The URL of the driver's picture.
Vehicle Make	The make of the driver's vehicle.
Vehicle Model	The model of the driver's vehicle.
Vehicle Year	The year of the driver's vehicle.
License Plate Number	The license plate number of the driver's vehicle.
License Plate State	The license plate state of the driver's vehicle.
Cost	The cost of the rider's trip and the currency used.
Distance	The distance in miles covered on the rider's trip.
Duration	The duration in hours, mins and seconds of the rider's trip.
Trip Status	The status of the trip at the time of acquisition.

Cloud Microsoft Teams Conversations

Description	Cloud Microsoft Teams Conversations contains information about each of the channels and group messages that exist in a user's Teams environment.
Notes	

ATTRIBUTE	DESCRIPTION
Conversation Name	The name of a channel or message group.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the message group was created.
Description	The optional description for the channel.
Participants	The names of the users in the message group. Channels do not have a participant list.
Email	The email address for sending messages to the channel.
Web URL	The URL for the channel in Microsoft Teams.
Conversation ID	The ID of a channel or message group.
Team ID	The team ID of the channel.

Cloud Microsoft Teams Messages

Description	Microsoft Teams Messages sent and received between Teams members which are recovered from the cloud.
Notes	

ATTRIBUTE	DESCRIPTION
Conversation ID	The unique identifier of the conversation.
Message ID	The unique identifier of current message.
Sender ID	The unique identifier of the sender.
Sender Name	The name of the sender
Send Timestamp Date/Time - UTC (yyyy-mm-dd)	The UTC date time when the message was sent.
Content Type	The type of the content.
HTML Body	The HTML body of the message.
Parent ID	The ID of the parent conversation.
_LocalUserAccount	The user name of the target user.
Attachment URL	The url of the attachment.
Attachments	The attachments.

Cloud Microsoft Teams Teams

Description	Cloud Microsoft Teams Membership contains information about Microsoft Teams as recovered from the cloud.
Notes	

ATTRIBUTE	DESCRIPTION
Team ID	Unique identifier for the team.
Team Name	Name of the team.
Description	Description associated with the team.

Cloud Office 365 Audit Logs

Description	Office 365 Audit Logs recovered from the cloud. This artifact collects information from SharePoint, Azure, and Exchange. SharePoint collects ItemType, SiteUrl, SourceFileName, and DestinationFileName information. Azure collects ResultStatus, and Client information. Exchange collects ClientInfoString, LogonType, MailboxOwnerUPN, Subject, and ExternalAccess information.
Notes	

ATTRIBUTE	DESCRIPTION
ID	The unique identifier of an audit record [Available on SharePoint, Azure, and Exchange].

ATTRIBUTE	DESCRIPTION
Type	The type of operation indicated by the record. See the AuditLogRecordType table for details on the types of audit log records [Available on SharePoint, Azure, and Exchange].
User	The User Principal Name (UPN) of the user who performed the action (specified in the operation property) that resulted in the record being logged; for example, my_name@my_domain_name. The records for activity performed by system accounts (such as SHAREPOINT/system or NT AUTHORITY/SYSTEM) are also included [Available on SharePoint, Azure, and Exchange].
Action	The name of the user or administrative activity. For a description of the most common activities, see Search the audit log in the Office 365 Protection Center. For Exchange administrative activity, this property identifies the name of the cmdlet that was run. For DLP events, this can be DlpRuleMatch, DlpRuleUndo or DlpInfo [Available on SharePoint, Azure, and Exchange].
Created Date/Time	Created Date/Time - UTC (yyyy/mm/dd) The date and time when the user performed the activity [Available on SharePoint, Azure, and Exchange].
Object ID	The full path name of the file or folder accessed by the user on SharePoint and OneDrive Business activity. The name of the object that was modified by the cmdlet on Exchange administrative audit logging.[Available on SharePoint, Azure, and Exchange].
IP Address	The IP address of the device that was used when the activity was logged. The IP address is displayed in either an IPv4 or IPv6 address format [Available on SharePoint, Azure, and Exchange].
Content Type	The type of object that was accessed or modified. See the ItemType table for details on the types of objects [Available on SharePoint].
Resource URL	The URL of the site where the file or folder accessed by the user is located.
Status	Indicates whether the action (specified in the Operation property) was successful or not. For SharePoint and Azure, possible values are Succeeded, PartiallySucceded, or Failed. For Exchange admin activity, possible values are True or False [Available on SharePoint, Azure, and Exchange].
Client	The client device information, provided by the browser performing the login [Available on Azure].
Device Description	Information about the email client that was used to perform the operation, such as a browser version, Outlook version, and mobile device information [Available on Exchange].
Access Method	Indicates the type of user who accessed the mailbox and performed the operation that was logged [Available on Exchange].
Owner Email	The email address of the user who is associated to the mailbox that was accessed [Available on Exchange].
Subject	The subject line of the message that was accessed [Available on Exchange].
External Access	Specifies whether the cmdlet was run by a user in your organization, by Microsoft datacenter personnel or a datacenter service account, or by a delegated administrator. The value False indicates that the cmdlet was run by someone in your organization. The value True indicates that the cmdlet was run by datacenter personnel, a datacenter service account, or a delegated administrator [Available on Exchange]
Data	Multi-value data for multiple properties from the audit log record. Each of the multi-value properties has value pairs [Available on SharePoint, Azure, and Exchange]
Source	The location of where the Office 365 Audit Logs were found.

ATTRIBUTE	DESCRIPTION
Location	A byte offset within the source where the Office 365 Audit Logs data has been acquired.

Cloud Office 365 Outlook Calendars

Description	Cloud Office365 Outlook Calendar contains information about the entries a user has saved to their Outlook Calendar.
Notes	

ATTRIBUTE	DESCRIPTION
Event ID	The unique identifier of a calendar event.
Subject	The subject of the event.
Body	A more complete description of the entry.
Created Date/Time - UTC (yyyy-mm-dd)	Date and Time in UTC for which the entry was created in the calendar.
Last Modified Date/Time - UTC (yyyy-mm-dd)	Date and Time in UTC when this entry was last modified.
Start Date/Time - UTC (yyyy-mm-dd)	Date and Time in UTC when this entry is scheduled to start.
End Date/Time - UTC (yyyy-mm-dd)	Date and Time in UTC when this entry is scheduled to end.
Attendees	List of Attendee emails associated with the entry.
Has Attachements	Indicates if there is an attachemnt with the entry
All-Day Event	Indicates if it is an all-day event
Sent By Organizer	indicates if the sender of the event is the organizer
Event Location	Free form text defining the intended venue for the entry.
Organizer	The organizer's email of the calendar event.
Recurrence	Indicates if the event is recurring.
Sensitivity	Indicates the sensitivity of the event.
Importance	Indicates the importance of the entry

Cloud Office 365 Outlook Contacts

Description	Cloud Office 365 Outlook Contact contains information about the entries a user has saved to their Outlook Contacts.
Notes	

ATTRIBUTE	DESCRIPTION
Contact Owner	The owner account of the contact.
Contact Display Name	The display name of the contact.
Contact Family Name	The family name of the contact.
Contact Middle Name	The middle name of the contact.
Contact Given Name	The given name of the contact.
Created Date/Time - UTC (yyyy-mm-dd)	Date and Time in UTC that the contact was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	Date and Time in UTC that the contact was last modified.
Contact Email	Email addresses of the contact.
Contact ID	A unique identifier of a contact.
Profession	The profession of the contact.
Company	The company of the contact
Department	The department of the contact.
Job Title	The job title of the contact.
Manager	The manager of the contact.
Office Location	A free form description of the contact's office location
Business Homepage	The business homepage of the contact.
Business Address	The business adress of the contact.
Business Phone	The business phone numbers of the contact.
Home Address	The home adress of the contact.
Home Phone	The home phone numbers of the contact.
Mobile Phone	The mobile phone numbers of the contact.

Cloud OneDrive Files

Description	Files that are stored in OneDrive that are recovered from the cloud. OneDrive is a file hosting service that allows users to upload and sync files to the cloud and access them from multiple locations.
Notes	

ATTRIBUTE	DESCRIPTION
File ID	File ID on OneDrive.
File Name	The name of the file on OneDrive.
File Type	The type of file.
File Path	Path to the file on OneDrive.
File Size (Bytes)	The file size in bytes.

ATTRIBUTE	DESCRIPTION
Owner ID	The unique identifer of the owner of the file.
Owner Name	The name of the owner of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time the file was modified.
Attachments	Path to the downloaded file.

Cloud SharePoint Content

Description	content that is hosted on a SharePoint service and is recovered from the cloud. SharePoint is a web-based, collaborative platform that integrates with Microsoft Office.
Notes	

ATTRIBUTE	DESCRIPTION
ID	Content ID hosted by SharePoint services.
File Name	The name of the content that is hosted by SharePoint service.
File Type	The type of content.
File Path	The path to the content on the SharePoint service.
Creator ID	A unique identifier for the content Creator.
Creator Name	The name of the content creator.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the the content was created.
Last Modified ID	An ID for the individual that last modified the content.
Last Modified Name	The name of the individual that last modified the content.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the content was last modified.
Web URL	A direct URL to the content
Attachments	A path to the downloaded content.

Cloud SharePoint Documents

Description	Files that are stored in SharePoint Documents library that are recovered from the cloud. SharePoint is a web-based, collaborative platform that integrates with Microsoft Office.
Notes	

ATTRIBUTE	DESCRIPTION
File ID	File ID in SharePoint Documents library.

ATTRIBUTE	DESCRIPTION
File Name	The name of the file in the SharePoint Documents library.
File Type	The type of file.
File Path	Path to the file in the SharePoint Documents library.
File Size (Bytes)	The file size in bytes.
Owner ID	The unique identifer of the owner of the file.
Owner Name	The name of the owner of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time the file was modified.
Attachments	Path to the downloaded file.

Cloud Sharepoint Site Pages

Description	Site pages that are hosted on a SharePoint service and are recovered from the cloud. SharePoint is a web-based, collaborative platform that integrates with Microsoft Office.
Notes	

ATTRIBUTE	DESCRIPTION
ID	SharePoint ID of the site page.
File Name	The name of the site page.
File Path	The path to the site page on the SharePoint service. It the sites hierarchy of the site page that is hosted by SharePoint services
Creator ID	A unique ID for the page Creator.
Creator Name	The name of the site page creator.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the the site page was created.
Last Modified ID	An ID for the individual that last modified the site page.
Last Modified Name	The name of the individual that last modified the site page.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the site page was last modified.
Web URL	A direct URL to the site page
Attachments	A path to the downloaded site page.

Cloud Skype Account Details (Warrant Return)

Description	Cloud Skype Account Details (Warrant Return) contains information about the target account of the warrant return.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The username of the user.
Account Creation Date/Time	The date and time that the account was created.
Account Creation IP Address	The IP Address of the device on which the account was created.
User Email	The email address of the user.
Language	The shortcode of the user account's language.
First Name	The first name of the user.
Last Name	The last name of the user.
Profile User ID	The unique ID that is associated with the profile.

Cloud Skype Chat History Records (Warrant Return)

Description	Cloud Skype Chat History Records contains the chat history of a user, including calls and shared attachments.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the message.
Recipient(s)	The recipient(s) of the message.
Message	The body of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Attachment Name	The name of the attachment that was sent.
Attachment Size (bytes)	The size of the attached file in bytes.
Message Type	The type of the message.
Metadata	Additional details about the record in XML format.

Cloud Skype Connection History (Warrant Return)

Description	Cloud Skype Connection History contains information regarding account activity extracted from warrant returns provided by Skype.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The full username of the account holder.
First Name	The first name of the account holder.
Last Name	The surname of the account holder.
Record Type	The record descriptor for this action.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the account activity occurred.
Action	The type of account activity that occurred.
IP Address	The IP address associated with the account action.
Service Name	The Microsoft service used for this action.

Cloud Skype Contacts (Warrant Return)

Description	Cloud Skype Contacts contains the contacts of a user.
Notes	

ATTRIBUTE	DESCRIPTION
User	The username of the user.
Type	The type of contact. The GUID of the contact is displayed for Service contacts.
Contact	The user ID of the contact.

Cloud Slack Files

Description	Slack Cloud Files contains information about files a user has downloaded locally from URLs they've viewed within Slack. Data about the downloads are recovered from Slack Workspace Corporate exports.
Notes	

ATTRIBUTE	DESCRIPTION
Attachments	The name of the attached file.

ATTRIBUTE	DESCRIPTION
Attachment URL	The download URL of the attached file.
Attachment ID	The unique ID of the attached file assigned to it by Slack.
Channel Name	The name of the Slack Channel in which the file was shared.

Cloud Snapchat Account Information (Warrant Return)

Description	Snapchat Account Information (Warrant Return) contains information about the target account of the warrant return.
Notes	

ATTRIBUTE	DESCRIPTION
Account ID	The handle of the account target account of the warrant return.
Email Address	The registered email address of the target account of the warrant return.
Account Creation Date/Time (yyyy-mm-dd)	The date and time the account was created.
Account Creation IP Address	The IP Address of the device on which the account was created.
Phone Number	The registered phone number of the target account of the warrant return.
Display Name	The display name of the target account of the warrant return.

Cloud Snapchat Friends (Warrant Return)

Description	Snapchat Friends (Warrant Return) contains information about the user's friends, which are parsed from a warrant return.
Notes	

ATTRIBUTE	DESCRIPTION
Target ID	The account handle of the target account for the warrant return.
Friend ID	The account handle of target's friend.

Cloud Snapchat Group Chat Messages (Warrant Return)

Description	Snapchat Group Chat Messages (Warrant Return) contains information about the messages sent and received by users participating in a group chat thread, and which are parsed from a warrant return.
Notes	

ATTRIBUTE	DESCRIPTION
Message Type	The contents of the sent message.
From	The handle of the sender of the message.
Owner ID	The handle of the target account for the warrant return.
Group Chat ID	The unique identifier of the group chat thread.
Group Chat Name	The name of the group chat thread.
Body	The text that was included in the message.
HREF	The contents of the href column from the warrant return .CSV file.
Attachments	Media attached to the message.
MediaID	The sender and unique ID information for all media attached to a message.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.

Cloud Snapchat IP History (Warrant Return)

Description	Snapchat IP History (Warrant Return) contains information about the IP addresses that are associated with a user's account logins, as recovered from a warrant return.
Notes	

ATTRIBUTE	DESCRIPTION
User Account	The account name for the Snapchat user.
IP	The IP address of the device that logged in or out of the account.
Type	The type of account action the user performed (login or logout).
Date/Time - UTC (yyyy-mm-dd)	The date and time the action was performed.

Cloud Snapchat Messages (Warrant Return)

Description	Snapchat Messages (Warrant Return) contains information about the messages that are sent or received by a user and which are parsed from a warrant return.
Notes	

ATTRIBUTE	DESCRIPTION
From	The account that sent the message.
To	The account that received the message.
Body	The text that was included in the message.
Media ID	The identifier for any photo(s) that were sent in the message.
Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Saved	The saved column found in the chat.
HREF	The href column found in the chat.
Chat ID	An ID for the chat, which combines the account names of the two users participating in the chat.
UserAccount	The main user account name.
Attachments	Paths to any photo and video attachments included in the message.

Cloud Uber Trip History

Description	Uber Trips contains summaries of the trips taken by an Uber user, and recovered from the cloud using their account credentials.
Notes	

ATTRIBUTE	DESCRIPTION
Origin Address	The pickup location address, as specified by the user.
Origin Latitude	The GPS Latitude coordinates of the specified pickup location.
Origin Longitude	The GPS Longitude coordinates of the specified pickup location.
Departure Date/Time - UTC (yyyy-mm-dd)	The date and time the rider was picked up from their pickup location.
Destination Address	The address specified by the rider for drop-off.
Destination Latitude	The GPS Latitude coordinates of the specified drop-off location.
Destination Longitude	The GPS Longitude coordinates of the specified drop-off location.
Arrival Date/Time - UTC (yyyy-mm-dd)	The date and time the rider was dropped off at their destination.

ATTRIBUTE	DESCRIPTION
Rider ID	The unique ID assigned to the rider's account.
Distance	The distance covered on the rider's trip.
Duration	The duration of the rider's trip.
Cost	The cost of the rider's trip and the currency used.
Trip Status	The status of the trip at the time of acquisition.
Trip ID	The unique ID for the trip.
Driver Name	The first name of the driver.
Driver ID	The unique ID of the driver.
Vehicle Make	The make of the driver's vehicle.
Vehicle Year	The year of the driver's vehicle.
Map Tile URL	The URL of the map tile that displays the route taken.
Attachment	The name of the downloaded Map Tile displaying the route taken.

Cloud WhatsApp Backups

Description	Cloud WhatsApp Backups contains information about backups that are created by WhatsApp and stored in the cloud. Each backup is a database that contains information from the WhatsApp for Android app, such as the user's message history. Backups are recovered from the cloud through the user's Google Drive account.
Notes	

ATTRIBUTE	DESCRIPTION
File ID	The unique ID for the WhatsApp backup recovered from Google Drive.
File Path	The parent folder and file name of the backup.
File Type	The MIME type of the file.
Description	The description of the file.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was uploaded to Google Drive.
File Hash	The unique MD5 hash calculated when uploaded to Google Drive.
File Size	Total byte size of the file.

Cloud WhatsApp Chats

Description	Cloud WhatsApp Chats are messages retrieved from a subject's account using their WhatsApp QR code login.
Notes	

ATTRIBUTE	DESCRIPTION
Message	The content of the message.
Author ID	The unique ID of the message author.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent (UTC).
Conversation Name	The name of the conversation.
Attachments	The file names of any locally downloaded files.

G Suite Drive Events

Description	G suite Drive Events contains event information about the Google Drive activity on a G Suite domain.
Notes	

ATTRIBUTE	DESCRIPTION
Event Type	Type of the event.
Event Name	Name of the event.
Event Date/Time - UTC (yyyy-mm-dd)	Time of occurrence of the activity.
Event ID	Unique identifier for each activity record.
Actor Email	The primary email address of the actor. May be absent if there is no email address associated with the actor.
Actor Profile ID	The unique G Suite profile ID of the actor. May be absent if the actor is not a G Suite user.
Actor Caller Type	The type of actor.
Actor Key	The consumer_key of the requestor for OAuth 2LO API requests or an identifier for robot accounts.
Owner Domain	The domain that is affected by the report's event. For example domain of Admin console or the Drive application's document owner.
IP Address	The IPv4 or IPv6 IP address of the user performing the action.
Document Type	The type of the document.
Document Title	The document title.

ATTRIBUTE	DESCRIPTION
Document ID	The document Id.
Originating App ID	The Google Cloud Project ID of the application that performed the action.
Owner	Email address of the document's owner.
Owner Is Team Drive	Indicates whether the document's owner is a team drive.
Team Drive ID	The unique identifier of the Team Drive. Only populated for for events relating to a Team Drive or item contained inside a Team Drive.
Visibility	The current visibility setting of the target file.
Old Visibility	The previous visibility setting of the target file.
Visibility Change	The change in visibility setting of the target file.
Destination Folder ID	The destination folder Id.
Destination Folder Title	The destination folder title.
Old Value	The old name of the event.
New Value	The new name of the event.
Target Domain	The domain for which the acccess scope was changed.
Membership Change Type	The type of change in Team Drive membership for the user or group.
Removed Role	The membership role that was removed for a user or group in a Team Drive.
Target	The target user or group.
Target User	The email address of the user or group whose access permissions were changed, or the name of the domain for which access permissions were changed.
New Settings State	The new state of team drive settings.
Old Settings State	The old state of team drive settings.
Team Drive Settings Change Type	The type of change that occurred to the team drive settings.

G Suite Login Events

Description	G Suite Login Events contains information about the events and parameters for login activity on a G Suite domain.
Notes	

ATTRIBUTE	DESCRIPTION
Event Type	The type of event that occurred.
Event Name	The name of the event.

ATTRIBUTE	DESCRIPTION
Event Date/Time - UTC (yyyy-mm-dd)	The date and time that the event occurred.
Event ID	Unique identifier for each activity record.
Actor Email	The primary email address of the actor that initiated the event. This value may be absent if there is no email address associated with the actor.
Actor Profile Id	The unique G Suite profile ID of the actor. This values may be absent if the actor is not a G Suite user.
Actor Caller Type	The type of actor.
Actor Key	The consumer_key of the requestor for OAuth 2LO API requests or an identifier for robot accounts.
Owner Domain	The domain that is affected by the report's event. For example, the domain could be for the Admin console or the Drive application's document owner.
IP Address	IPv4 or IPv6 IP address of the user doing the action.
Login Failure Type	The reason for the login failure.
Login Type	The type of credentials used to attempt login.
Login Challenge Status	Whether the login challenge succeeded or failed.
Is Suspicious	The login attempt had some unusual characteristics, for example the user logged in from an unfamiliar IP address.

Google Browsing History (Warrant Return)

Description	Google Browsing History (Warrant Return) contains information about the target account of the warrant return.
Notes	

ATTRIBUTE	DESCRIPTION
Browsing History Event	The website that the user visited or the browsing history event that occurred.
URL	The URL of the website the user visited.
Search Date Time UTC	The date and time that the website was visited.

Google Maps Activity (Warrant Return)

Description	Google Maps Activity (Warrant Return) contains information about the Google Maps actions executed by the account holder found within a Warrant Return package.
Notes	

ATTRIBUTE	DESCRIPTION
Description	A description of the Google Maps action made by the subject of the Warrant Return.
URL	The Google Maps URL associated with the action.
Search Date Time UTC	The date and time the action was made.
Latitude	The GPS Latitude coordinate of the area viewed, or the journey destination (depending on the action).
Longitude	The GPS Longitude coordinate of the area viewed, the location searched for, or the journey destination (depending on the action).

Google Search History

Description	Google Search History contains information about the searches made by the account holder, and found within a Warrant Return or Takeout package.
Notes	

ATTRIBUTE	DESCRIPTION
Search Type	The type of Google search the user used.
Search Term	The search term the user used.
URL	The URL of the search generated by Google.
Search Date Time UTC	The date and time the google search was made.
Latitude	The GPS Latitude coordinates of the location at which the search was made.
Longitude	The GPS Longitude coordinates of the location at which the search was made.

Google Snapchat Account Information (Warrant Return)

Description	Google Account Information (Warrant Return) contains information about the target account of the warrant return.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the user who created the account.
Email Address	The registered email address of the target account of the warrant return.
Services	The list of Google services associated with the user account.
Recovery Email	The recovery email address of the target account of the warrant return.
Account Creation Date/Time UTC	The date and time that the account was created.
Terms Of Service IP	The IP Address of the device on which the account was created.

ATTRIBUTE	DESCRIPTION
Terms Of Service Date/Time UTC	The date and time that the user accepted Google's Terms of Service.
SMS	The phone number associated with the target account of the warrant return.
Account ID	The handle of the account target account of the warrant return.
Last Login Date Time UTC	The last login date and time.
Youtube URL	The YouTube URL associated with the target account of the warrant return.
Youtube Creation Date Time UTC	The date and time that the user created the associated YouTube account.
Youtube Creation IP	The IP Address of the device on which the YouTube account was created.

iCloud Backups

Description	Backups of iOS devices that the user creates, and which are recovered from the cloud.
Notes	

ATTRIBUTE	DESCRIPTION
Created Date	The date and time the backup was created.
User Name	The Apple ID used to sign in to the account.
Cloudkit User ID	User ID for the CloudKit account - can be paired with the CloudkitToken to make authenticated requests to Cloudkit services.
Cloudkit Token	Token for the CloudKit account - can be used to make authenticated requests to Cloudkit services.
iCloud Account ID	The ID of the iCloud account.
Mme Auth Token	Token can be paired with the iCloud Account ID to make requests for other iCloud services.
Device Name	Name of the iOS device used to make the backup.
Device Hash	A unique hash value for the device (created by Apple).
Device Class	The type of device (for example, iPhone or iPad).
Model	The device model (for example, N61AP).
Friendly Name	A more friendly, recognizable name for the device model (for example, iPhone 6).
Product Type	An internal product identifier used by Apple (for example, iPhone7,2 which actually corresponds to the iPhone 6).
Quota Used	The number of bytes used by the backup.
Serial Number	Serial number of the device.
Snapshot Hash	Unique identifier of the backup (created by Apple).
System Domains Version	Backup system version.
Version	Backup version.

ATTRIBUTE	DESCRIPTION
Password Set	Indicates whether the device was locked when the backup was created (True or False).
Attachment	The path to the downloaded backup file.

iCloud Drive Files

Description	Files that are stored in iCloud Drive that are recovered from the cloud. iCloud Drive is a file hosting service that allows users to upload and sync files to the cloud and access them from multiple locations.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file on iCloud Drive.
File Path	The folder path the file resides in.
Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time the file was modified.
Uploaded Date/Time - Local Time (yyyy-mm-dd)	The local date and time the file was uploaded to iCloud Drive.
File Size (Bytes)	The file size.
Type	The file type, like 'FILE' or 'FOLDER'
Download URL	The direct URL to download the file.
Id	The ID of the file assigned by iCloud Drive.
Attachments	The raw data of the file.

iCloud Photos

Description	Photos that are stored in iCloud Photo Library that are recovered from the cloud.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the photo in iCloud Photo Library.
File Size (Bytes)	The file size.
Taken Date/Time - UTC (yyyy-mm-dd)	The time the photo was taken.
Added Date/Time - UTC (yyyy-mm-dd)	The time the photo was added to the phone.
Published Date/Time - UTC (yyyy-mm-dd)	The time the photo was published to iCloud Photo Library.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time the photo was changed on iCloud Photo Library.

ATTRIBUTE	DESCRIPTION
Caption	The description user added in iCloud Photo Library to describe the photo.
Albums	The albums the photo belongs to.
Id	The ID of the file assigned by iCloud Photo Library.
Attachments	The raw data of the file.

E-Mail

Cloud Google Gmail Messages

Description	Contains Gmail message contents, and Gmail attachments recovered from the cloud.
Notes	

ATTRIBUTE	DESCRIPTION
Id	An Id for the message.
Label	A list of the labels applied to the email (for example, IMPORTANT, SENT, UNREAD).
To Address(es)	The recipient(s) of the email.
From Address	The sender of the email.
CC	The recipients of the email that were CC'd.
BCC	The recipients of the email that were BCC'd.
Subject	The subject of the email.
Date/Time	The UTC date and time of when the email was sent.
Headers	The header information of the email.
Email Body	The body of the email.
HTML Body	The body of the email in HTML format where applicable.
Attachments	List of files attached to the email.
Source	A path to a location within the recovered evidence that contains the recovered email.
Location	A byte offset within the source where the Gmail data has been acquired.

Cloud IMAP / POP Emails

Description	Messages and attachments from an IMAP / POP account that are recovered from the cloud.
Notes	

ATTRIBUTE	DESCRIPTION
Sender Name	The sender of the email
Recipients	The recipients of the email
Subject	The subject of the email
Delivery Date/Time - UTC (yyyy-mm-dd)	The date and time the email was delivered
Body	The body of the email
Folder Name	The name of the folder where the email is stored
CC	The recipients of the email that were CC'd
BCC	The recipients of the email that were BCC'd
Attachments	The list of attachments on the email
Headers	The raw email headers
Importance	The importance of the email

Cloud MBOX Emails

Description	Cloud MBOX Emails contains the messages and attachments recovered from an MBOX file.
Notes	

ATTRIBUTE	DESCRIPTION
To	The recipients of the email.
From	The sender of the email.
Date/Time	The date and time the email was created.
Subject	The subject of the email.
Body	The body of the email.
CC	The recipients of the email that were CC'd.
BCC	The recipients of the email that were BCC'd.
Headers	The raw email headers.
Attachments	The list of attachments on the email.

Cloud Office 365 Hotmail/Outlook Emails

Description	Email messages and attachments sent and received using Microsoft mail services such as Office 365, Hotmail, or Outlook which are recovered from the cloud.
Notes	

ATTRIBUTE	DESCRIPTION
Sender Name	The sender of the email
Recipients	The recipients of the email
Subject	The subject of the email
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the email was created
Delivery Date/Time - UTC (yyyy-mm-dd)	The date and time the email was delivered
Body	The body of the email
Folder Name	The name of the folder where the email is stored
CC	The recipients of the email that were CC'd
BCC	The recipients of the email that were BCC'd
Attachments	The list of attachments on the email
Headers	The raw email headers
Importance	The importance of the email

Email

Cloud MBOX Emails

Description	Cloud MBOX Emails contains the messages and attachments recovered from an MBOX file.
Notes	

ATTRIBUTE	DESCRIPTION
To	The recipients of the email.
From	The sender of the email.
Date/Time	The date and time the email was created.
Subject	The subject of the email.
Body	The body of the email.
CC	The recipients of the email that were CC'd.
BCC	The recipients of the email that were BCC'd.
Headers	The raw email headers.
Attachments	The list of attachments on the email.

Media

Cloud Google Photos

Description	Pictures stored in Google Photos which are recovered from the cloud. Google Photos is a cloud-based photo storage service that allows users to store, view and share their photos.
Notes	

ATTRIBUTE	DESCRIPTION
Id	The ID of the photo.
File Name	Name of the file
Published Date/Time - UTC (yyyy-mm-dd)	The date the photo was published to Google Photos.
Updated Date/Time - UTC (yyyy-mm-dd)	The date the photo was last updated.
Photo Timestamp Date/Time - UTC (yyyy-mm-dd)	The photo's timestamp. Contains the date of the photo either set externally or retrieved from the Exif data.
Exif Timestamp Date/Time - UTC (yyyy-mm-dd)	The date/time the photo was taken.
Album	Album the photo is stored in.
Description	A description of the photo, if one exists.
Make	The make of the camera used to take the picture, as recovered from the EXIF data.
Model	The model of the camera used to take the picture, as recovered from the EXIF data.
Latitude	The GPS Latitude coordinates of where the picture was taken, as recovered from the EXIF data.
Longitude	The cardinal coordinates of the GPS longitude, as recovered from the EXIF data.
Access	Current sharing permission assigned to the photo.
File Size (Bytes)	The size of the photo in bytes.
Image Unique Id	Unique ID assigned to the photo
Download URL	A download URL for the photo.
Attachments	The name of the locally downloaded file.

Cloud Google Photos - AXIOM 2.8

Description	Pictures stored in Google Photos which are recovered from the cloud. Google Photos is a cloud-based photo storage service that allows users to store, view and share their photos. This artifact applies to Magnet AXIOM 2.8 and earlier.
Notes	

ATTRIBUTE	DESCRIPTION
Id	The ID of the photo.
File Name	Name of the file
Published Date/Time - UTC (yyyy-mm-dd)	The date the photo was published to Google Photos.
Updated Date/Time - UTC (yyyy-mm-dd)	The date the photo was last updated.
Photo Timestamp Date/Time - UTC (yyyy-mm-dd)	The photo's timestamp. Contains the date of the photo either set externally or retrieved from the Exif data.
Exif Timestamp Date/Time - UTC (yyyy-mm-dd)	The date/time the photo was taken.
Album	Album the photo is stored in.
Description	A description of the photo, if one exists.
Make	The make of the camera used to take the picture, as recovered from the EXIF data.
Model	The model of the camera used to take the picture, as recovered from the EXIF data.
Latitude	The GPS Latitude coordinates of where the picture was taken, as recovered from the EXIF data.
Longitude	The cardinal coordinates of the GPS longitude, as recovered from the EXIF data.
Access	Current sharing permission assigned to the photo.
File Size (Bytes)	The size of the photo in bytes.
Image Unique Id	Unique ID assigned to the photo
Download URL	A download URL for the photo.
Attachment Path	The location of the Attachment
Attachments	The name of the locally downloaded file.

Social Networking

Cloud Facebook Account Actions (Warrant Return)

Description	Facebook Account Actions (Warrant Return) contains the list of actions made by the user that Facebook has included in a warrant return.
Notes	

ATTRIBUTE	DESCRIPTION
Action	A description of the action executed on the account.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the action.
IP Address	The IP address of the device on which the action was executed.

Cloud Facebook Audit Logs (Warrant Return)

Description	Facebook Audit Logs (Warrant Return) contains information activities the user has performed on Facebook which are parsed from a warrant return.
Notes	

ATTRIBUTE	DESCRIPTION
Type	The type of activity that occurred.
Summary	A summary of what happened.
Date/Time - UTC	The time the activity occurred.
Object ID	The ID of the activity.

Cloud Facebook Friend Requests (Warrant Return)

Description	Facebook Friend Requests (Warrant Return) contains friend requests that are parsed from friend_requests file that Facebook has included in a warrant return.
Notes	

ATTRIBUTE	DESCRIPTION
Sender Name	The name of the sender of the friend request.
Sender ID	The Facebook ID of the sender.

ATTRIBUTE	DESCRIPTION
Recipient Name	The name of the recipient of the friend request.
Recipient ID	The Facebook ID of the recipient.
Sent Date/Time	The UTC time the friend request was sent.
Requests Accepted	Indicates whether the friend request is accepted.
Is Rejected	Indicates whether the friend request is rejected.
Marked As Spam	Indicates whether the friend request is marked as spam.
Hidden	Indicates whether the friend request is hidden.

Cloud Facebook Friends

Description	Cloud Facebook Friends contains information about the user's Facebook friends that was recovered from the cloud.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the user's friend.
HTML Body	An HTML card for the friend, which appears in the user's Friends list.
FriendTagLine	A string containing a tagline for the friend (this can contain the friend count for that user, the mutual friend count, or another piece of information about the friend).
Permanent Link	The URL of the friend's profile.
Attachments	The profile picture of the friend.
Date/Time	The date and time that the friend was added, deleted or requested.
Status	The friend's relationship status with the user (for example 'deleted friends' if the user is no longer a friend, or 'friends' if they are currently friends).

Cloud Facebook Friends (Warrant Return)

Description	Facebook Friends (Warrant Return) contains information about a user's Facebook friends which are parsed from a warrant return.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the user's friend.
ID	The Facebook ID of the user's friend.

Cloud Facebook Messenger Messages

Description	Cloud Facebook Messenger Messages contains Facebook Messages recovered from the cloud.
Notes	In cases where the sender account is suspended by Facebook pending a user ID verification, the body of a message is not recoverable. Only the sender name, sender ID, participants, and timestamp for the message is available.

ATTRIBUTE	DESCRIPTION
Thread ID	The unique ID for the message thread that the message is recovered from.
Local User Account	The unique Facebook ID associated with the local user account.
Sender Name	The username of the person who sent the message.
Author ID	The unique Facebook ID of the author of the message.
Text	The content of the message.
HTML Body	The HTML body of the message.
Participants	The display names of the participants in the conversation.
Date/Time	The date and time when the message was sent.
Attachments	The file names of any locally downloaded files.
Message Type	The type of the message (examples include 'Generic' which indicates a standard message, 'Call', and 'Share').
Source	The location of where the artifact was found.
Location	A byte offset within the source where the Facebook Message data has been acquired.

Cloud Facebook Messenger Messages (Warrant Return)

Description	Facebook Messenger Messages (Warrant Return) contains individual messages that are parsed from chat threads that Facebook has included in a warrant return. The 'messages' in a chat thread can include messages, shared files or links, calls, and audio messages.
Notes	

ATTRIBUTE	DESCRIPTION
Sender Name	The name of sender of the message.
Author ID	The Facebook ID of the author.
Participants	The participants of the chat thread
Sent Date/Time	The date and time the message was sent.
Body	The text of the message.
Owner	The name of the ower of the chat. (Identifies the local user for chat threading)

ATTRIBUTE	DESCRIPTION
Owner ID	The Facebook ID of the owner of the chat. (Identifies the local user for chat threading)
Thread ID	The ID of the chat thread that the message is from.
Sender IP	The IP address of the sender of the message.
Attachments	A zip of any attachments to this message.
Last Shared Date/Time	If the message was shared outside the chat, this indicates the last date and time it was shared.
Sharing Link	A link to the file, if the message contains a shared file.
Sharing Summary	A summary of the shared item, if the message contains a shared file or URL.
Sharing Text	A description of the shared item, if the message contains a shared file or URL.
Sharing Title	A title for the shared item, if the message contains a shared file or URL.
Sharing Url	A URL to the shared page, if the message contains a shared file or URL.
Call Type	If the message type is a call, this indicates whether the call is an audio or video call
Call Missed	A boolean value indicates if the call was missed.
Call Duration	The duration of the call.
Date/Time	The UTC time the chat thread was created

Cloud Facebook Photos (Warrant Return)

Description	Facebook Photos (Warrant Return) contains information about the pictures that a user has posted to Facebook, which are parsed from a warrant return.
Notes	

ATTRIBUTE	DESCRIPTION
Picture	The image data that was recovered.
Album	The name of the album that the picture belongs to.
Title	The title of the picture.
ID	The Facebook ID of the picture.
Photo URL	The URL of the picture on Facebook.
Web URL	The URL of the picture post on Facebook.
IP	The IP address of the device that was used to upload the photo.
Uploaded Date/Time UTC	The date and time the photo was uploaded to Facebook.
Modified Date/Time UTC	The modification date and time of the photo as reported by Facebook.
Make	The make of the camera used to take the picture, as recovered from the Facebook data.

ATTRIBUTE	DESCRIPTION
Model	The model of the camera used to take the picture, as recovered from the Facebook data.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.
Tags	Any Facebook tags applied to the picture by the user.

Cloud Facebook Profile Info

Description	Cloud Facebook Profile Info contains Facebook profile information recovered from the cloud.
Notes	

ATTRIBUTE	DESCRIPTION
Address	The full address of the user.
Additional Address	The name of the neighborhood that the user lives in.
Email Address(es)	A list of the user's email addresses.
Public Key	The user's PGP public key.
Phone Number	A list of the user's phone numbers.
Website URL	A list of website URLs that are associated with the user's profile.
Website	A list of other websites and account names that are associated with the user's profile.
Birthday	The user's birthday.
Gender	The user's gender.
Sexual Orientation	The user's sexual orientation (Men, Women, or Men and Women).
Language	A list of the languages that the user has specified.
Religion	A title and description indicating the user's religious views.
Political Party	A title and description indicating the user's political views.
HTML Body	The HTML of the user's profile info page.

Cloud Facebook Status Updates (Warrant Return)

Description	Facebook Status Updates (Warrant Return) contains status updates and comments from a user's status update that Facebook has included in a warrant return.
Notes	

ATTRIBUTE	DESCRIPTION
Author ID	The Facebook ID of the author of the status update or comment.
Name	The name of the author of the status update or comment.
Type	Indicates whether this instance is a status update or comment.
Status/Comments	The content of the status update or comment.
Posted Date/Time - UTC	The date and time when the status update or comment was made.
Mobile	Indicates if the status update was posted via mobile phone
Attachment	A ZIP of any attachemnts to this status update or comment.

Cloud Facebook Timeline

Description	Cloud Facebook Timeline contains Facebook timelines and their content, which are recovered from the cloud.
Notes	

ATTRIBUTE	DESCRIPTION
Message ID	The Facebook ID of the post.
Poster ID	The Facebook ID of the authenticated user.
Name	The authenticated user's name.
Type	The type of post (for example: photo, video, status, or link).
Text	The content of the post.
Permanent Link	A URL to the post that is intented to remain unchanged for many years.
Web URL	The URL of a link that is attached to the post.
Picture URL	The URL to a picture from any link included with the post.
Video URL	The URL to a video from any link included with the post.
Created Date/Time	The date and time when the post was created.
Updated Date/Time	The date and time when the post was last updated.
Attachments	A list of relative file paths to downloaded media.
Source	A path to a location within the recovered evidence that contains the recovered post.
Location	A byte offset within the source where the Facebook post data has been acquired.

Cloud Facebook Wallposts (Warrant Return)

Description	Facebook Wallposts (Warrant Return) contains posts and comments from a user's wall that Facebook has included in a warrant return.
Notes	

ATTRIBUTE	DESCRIPTION
Sender ID	The Facebook ID of person who made the post.
Sender Name	The name of the person who made the post.
Recipient ID	The Facebook ID of the post recipient.
Recipient Name	The name of the post recipient.
Date/Time - UTC	The time that the post was made.
Content	The content of the post.
Message ID	The ID of the post. Both posts and comments on a post share the same ID.
Message Type	Indicates whether this instance is a wall post or a comment on a post.

Cloud Instagram Direct Messages

Description	Instagram direct messages that are sent or received by the logged in user and recovered from the cloud.
Notes	

ATTRIBUTE	DESCRIPTION
Thread Title	The title of the conversation.
Sender Username	The user name of the sender of the message.
Author	The user name of the original author of the message.
Text	The message that was sent.
Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time of the message.
Participants	The user name of the participants in that conversation.
Message Type	The message type.
Direction	The direction of the message, relative to the source of the hit.
Latitude	The latitude of a location shared through the message or attachment.
Longitude	The longitude of a location shared through the message or attachment.

ATTRIBUTE	DESCRIPTION
Thread ID	The conversation ID.
Message ID	The message ID.
Attachments	The name of the locally downloaded file(s).

Cloud Instagram Posts

Description	Instagram posts that are published by the logged in user and recovered from the cloud.
Notes	

ATTRIBUTE	DESCRIPTION
ID	The post ID.
Sender Username	The user name of the publisher of the post.
Sender Full Name	The full name of the publisher of the post.
Sender ID	The user ID of the publisher of the post.
Taken Date/Time - UTC (yyyy-mm-dd)	The date and time the picture or video was taken.
Archived	Indicates whether the post was archived.
Text	The caption of the post.
Likes Count	The number of likes the post has.
Likers	The user names of users that like the post.
Comments Count	The number of comments the post has.
Comments Preview	A preview of the comments on the post.
Tagged Users	Users that were tagged in the post.
Permanent Link	The direct link to the post.
Latitude	The latitude of a location added to the post.
Longitude	The longitude of a location added to the post.
Attachments	The names of any locally downloaded files attached to the post.

Cloud Instagram Posts - AXIOM 2.1

Description	Instagram posts that are published by the logged in user and recovered from the cloud.
Notes	This version of the artifact was supported on Magnet AXIOM 2.1 and earlier. In the latest versions of AXIOM, the Cloud Instagram Posts artifact uses a different recovery method and now recovers a more comprehensive set of data.

ATTRIBUTE	DESCRIPTION
Message ID	The post ID.
Name	The user name of the publisher of the post.
Text	The caption of the post.
Permanent Link	The direct link to the post.
Web URL	The web url of the post.
Created Date/Time - UTC (yyyy-mm-dd)	The creation date and time of the post.
HTML Body	The HTML body of the post.
Attachments	The names of any locally downloaded files attached to the post.

Cloud Twitter Direct Messages

Description	Direct messages between an authenticated Twitter user and another user, which are recovered from the cloud (limited to 20 sent and 20 received messages).
Notes	

ATTRIBUTE	DESCRIPTION
Message ID	Unique identifier for the direct message.
Sender Screen Name	The Twitter handle for the message sender.
Recipient Screen Name	The Twitter handle for the message recipient.
Text	The content of the direct message.
Sent/Received Date/Time	The UTC date and time that the message was sent.
Sender ID	Unique identifier for the sender.
Sender Name	The name of the Twitter sender, as they've defined it, not necessarily the person's name.
Sender Location	Human readable name of the place from where the message was sent.
Recipient ID	Unique identifier for the recipient.
Recipient Name	The name of the Twitter recipient, as they've defined it, not necessarily the person's name.
Recipient Location	Human readable name of the place from where the message was received.
Media URL	A list of media URLs attached to the message.
Media Type	A list of media types corresponding to each media URL.
Attachments	A list of relative file paths to the media downloaded from Twitter servers.
Source	A path to a location within the recovered evidence that contains the recovered message.
Location	Byte offset within Source where the Twitter data has been acquired.

Cloud Twitter Posts

Description	An authenticated Twitter user's tweets, recovered from the cloud (limited to 1200 of the user's most recent Tweets).
Notes	

ATTRIBUTE	DESCRIPTION
Status ID	Unique identifier for the Twitter Tweet.
User ID	Unique identifier for the Twitter user.
Screen Name	The Twitter handle for the user (ie. @username).
Name	The name of the Twitter user, as they've provided in their user profile.
Tweet Text	The content of the tweet.
Posted Date/Time	The UTC date and time that the tweet was posted.
Favorited	Whether this Tweet was liked by the authenticated user.
Retweet Count	The number of times this Tweet has been retweeted.
Tweet Source	The type of device/application that was used to create the tweet.
URL	URL for the Tweet.
Location Name	Human-readable name of the place where the Tweet was posted.
Country	Name of the country where the Tweet was posted.
Latitude	Latitude of the location where the Tweet was posted (values are between -90.0 to +90.0, where North is positive).
Longitude	Longitude of the location where the Tweet was posted (values are between -180.0 to +180.0 where East is positive).
Location Bounding Box	A series of longitude and latitude points, defining a box around around the Tweet location.
Media Type	A list of media types for media posted in the Tweet.
Media URL	A list of media URLs for media posted in the Tweet.
Attachments	A list of relative file paths to downloaded media attached to the Tweet.
Source	A path to a location within the recovered evidence that contains the recovered Tweet.
Location	Byte offset within Source where the Tweet data has been acquired.

Cloud Twitter Posts Public

Description	Twitter Posts contains publicly-accessible tweets which are recovered from the cloud. The data structure is defined in https://github.com/twintproject/twint/blob/master/twint/tweet.py
Notes	

ATTRIBUTE	DESCRIPTION
Screen Name	The Twitter handle for the user (@username).
Name	The name of the Twitter user, as they've provided in their user profile.
Place	The geocoded location where the tweet was sent from (if available).
Tweet Text	The content of the tweet.
Retweeted by Target User	Indicates the Sceen Name of the targetted user that retweeted the original tweet.
Posted Date/Time - UTC (yyyy-mm-dd)	The date and time when the tweet was originally created.
Attachments	A list of relative file paths to downloaded media attached to the Tweet.
Reply Count	The number of times that people replied to this tweet.
Retweet Count	The number of times this Tweet has been retweeted.
Likes Count	The number of times this Tweet has been liked.
Location	The location of the tweet's author.
Mentions	An array of user's that were mentioned within this post.
Status ID	Unique identifier for the Twitter Tweet.
Conversation ID	Unique identifier for the conversation of the Twitter Tweet.
User ID	Unique identifier for the Twitter user.
Location Name	The human-readable name of the place where the Tweet was posted.
Web URL	An array of URLs contained inline within this tweet.
Photo URL	An array of URLs to photos contained inline within this tweet.
HashTags	An array of hashtags used within this tweet.
URL	URL for the Tweet.
Retweeted	Indicates whether this tweet is a retweet of another user's tweet.
Quote URL	The URL to the a tweet which is being quoted in this user's tweet.
Has Video	Indicates that this tweet has an inline video included.

Cloud Twitter Users

Description	Twitter users (followers, friends, and personal profile) information. Data structure from https://dev.twitter.com/overview/api/users
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The integer representation of the unique identifier for this User. Int64.
Name	The name of the Twitter user, as they've provided in their user profile.

ATTRIBUTE	DESCRIPTION
User Name	The screen name, handle, or alias that this user identifies themselves with. screen_names are unique but subject to change.
Profile Created Date/Time	The UTC datetime that the user account was created on Twitter.
Description	Nullable . The user-defined UTF-8 string describing their account.
Web URL	Nullable . A URL provided by the user in association with their profile.
Location	Nullable . The user-defined location for this account's profile. Not necessarily a location, nor machine-parseable.
Protected	When true, indicates that this user has chosen to protect their Tweets.
Followers	The number of followers this account currently has. Under certain conditions of duress, this field will temporarily indicate 0.
Friends	The number of users this account is following. Under certain conditions of duress, this field will temporarily indicate 0.
Statuses	The number of Tweets (including retweets) issued by the user.
Timezone	Nullable . A string describing the Time Zone this user declares themselves within.
Following	Nullable. Screen name of a user that this account is following.
Followed By	Nullable. Screen name of a user that is following this account.
Profile Picture URL	A HTTP-based URL pointing to the user's profile image.
Profile Background Picture URL	A HTTP-based URL pointing to the background image the user has uploaded for their profile.
Profile Banner URL	The HTTPS-based URL pointing to the standard web representation of the user's uploaded profile banner.

Cloud Twitter Users Public

Description	Twitter Users contains information about publicly-accessible Twitter users (followers, friends, and personal profile) which are recovered from the cloud. The data structure is defined in https://-github.com/twintproject/twint/blob/master/twint/user.py
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The integer representation of the unique identifier for this User. Int64.
Name	The name of the Twitter user, as they've provided in their user profile.
User Name	The screen name, handle, or alias that this user identifies themselves with. screen_names are unique but subject to change.
Biography	Nullable . The user-defined UTF-8 string describing their account.
Bio URL	Nullable . A URL provided by the user in association with their profile.

ATTRIBUTE	DESCRIPTION
Location	Nullable . The user-defined location for this account’s profile. Not necessarily a location, nor machine-parseable.
Statuses	The number of Tweets (including retweets) issued by the user.
Friends	The number of users this account is following. Under certain conditions of duress, this field will temporarily indicate 0.
Followers	The number of followers this account currently has. Under certain conditions of duress, this field will temporarily indicate 0.
Likes Count	The number of tweets that this user has liked.
Media Count	Indicates the number of posts with media embedded in them, such as all Twitter posts that contain inline photos or video.
Protected	Indicates whether a user has chosen to protect their Tweets.
Verified	Indicates whether this user has been marked as verified by Twitter.
Profile Picture URL	A HTTP-based URL pointing to the user’s profile image.
Following	Nullable. Screen name of users that this account is following.
Is Followed By	Nullable. Screen name of users that are following this account.
Web URL	The HTTPS-based URL pointing to the user's profile.
Profile Created Date/Time	The UTC datetime that the user account was created on Twitter.

Transportation and Travel

Cloud Google Timeline Locations

Description	Locations that a user visits that are captured by Google Timeline, and recovered from the cloud. Google Timeline is a web service that allows a user to view the locations they travel and the routes they take.
Notes	

ATTRIBUTE	DESCRIPTION
Location Name	The name of the location.
Location Address	Address of the location.

ATTRIBUTE	DESCRIPTION
Arrival Date/Time UTC (yyyy-mm-dd)	The time the user arrived at the location.
Last Seen Date/Time - UTC (yyyy-mm-dd)	The time the user was last seen at this location.
Latitude	The GPS Latitude coordinates of the location.
Longitude	The GPS Longitude coordinates of the location.
Location Type	A description of the location, as determined by Google (for example, home, bar, cafe, or generic).
Location Type Inference	Indicates how the location type was determined. A value of inferred suggests that Google inferred the location type based on the person's position and the types of places nearby (for example, Google might infer that a person is at a restaurant if there's a restaurant at the same approximate location). A value of inferred-alias is used when the person visits a place they explicitly set as destination type (i.e. home or work).

WINDOWS PHONE

Advanced Search Tools

Dynamic Application Finder

Description	
Notes	

ATTRIBUTE	DESCRIPTION

Chat

Lync / OC Calls

Description	Lync/OC is a business grade communication application created by Microsoft.
Notes	

ATTRIBUTE	DESCRIPTION
Remote Participant Email	The email of the remote participant
Remote Participant Display Name	The display name of the remote participant
Call Started Date/Time - Local Time (yyyy-mm-dd)	The date and time when the call was started, local to the system
Call Ended Date/Time - Local Time (yyyy-mm-dd)	The date and time when the call ended, local to the system
Duration (Seconds)	The duration of the call in seconds

Lync / OC File Transfers

Description	Lync/OC is a business grade communication application created by Microsoft.
Notes	

ATTRIBUTE	DESCRIPTION
Type	The type of file
Sender	The sender of the file
Recipient	The recipient of the file
File	The file name or path
File Size (Bytes)	The size of the file
Transfer Event Date/Time - Local Time (yyyy-mm-dd)	The start/end date time of the transfer

Lync / OC Fragments

Description	Lync/OC is a business grade communication application created by Microsoft.
Notes	

ATTRIBUTE	DESCRIPTION
HTML Fragment	The HTML Fragment of the conversation

Lync / OC Messages

Description	Lync/OC is a business grade communication application created by Microsoft.
Notes	

ATTRIBUTE	DESCRIPTION
Sender Email	The email address of the sender
Sender Display Name	The display name of the sender
Body	The body of the message
Sent Date/Time - Local Time (yyyy-mm-dd)	The date and time the message was sent, local to the system

Skype Accounts

Description	Information about the Skype accounts that are recovered, such as user info and when the account was created.
Notes	

ATTRIBUTE	DESCRIPTION
Skype Name	The Skype user name
Display Name	The visual display name
Full Name	The full name of the user
Birthday	The user's birthday
Gender	The gender of the user
City	The city in which the user has set
State / Province	The state/province in which the user has set
Country	The Country in which the user has set
Home Phone	The user's home phone number.
Office Phone	The user's office phone number
Mobile Phone	The user's mobile phone number
Email(s)	The user's email email address. Can be more than one
Homepage	The user's website
About Info	About the user
Profile Created On Date/Time - UTC (yyyy-mm-dd)	The date and time the profile was created
Profile Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the profile was last modified
Mood Text	The user's mood
Last Online Date/Time - UTC (yyyy-mm-dd)	The date and time the user was last online
Last Used Date/Time - UTC (yyyy-mm-dd)	The last date and time the account was used
Avatar Timestamp Date/Time - UTC (yyyy-mm-dd)	The last date and time the user updated their display picture
Image	The display picture image

Skype Calls

Description	Information about Skype calls that occur between users.
Notes	

ATTRIBUTE	DESCRIPTION
Local Username	The user logged into Skype at the time of the call.
Call Initiator	The user who started the call.
Initiator Display Name	The display name of the user. This might be different from the username.
Recipient(s)	The users who accepted a call from the call initiator and participated in the call for a period of time.

ATTRIBUTE	DESCRIPTION
Call Participants	The users who accepted and participated in the call from the call initiator for some duration.
Started Date/Time - UTC (yyyy-mm-dd)	Start time of the call.
Duration	Total duration of the Skype call.
Metadata	Additional details about the call extracted in XML format. This includes the duration of time each participant was in the call.

Skype Chat Messages

Description	Skype messages sent from one user to another.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	Profile name of the caller
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent
Author	Author of the message
From Display Name	The display name of who sent the message
Message	The body of the message or a description of the action taken. For example, adding another participant to a group chat or sharing a file or picture.
Attachment Name	The name of the attachment that was sent. This attribute is populated when the Message Type is POSTED_FILE or POSTED_PICTURE. Otherwise, this attribute is empty.
Attachment Size (Bytes)	The size of the attached file, in bytes. This attribute is populated when the Message Type is POSTED_FILE or POSTED_PICTURE. Otherwise, this attribute is empty.
Metadata	Additional details about the action, extracted in its original XML format.
Message Status	The status of the message.
Message Type	Type of message
Chat ID	ID of this chat
Recipient	Recipient of the chat

Skype Chatsync Messages

Description	Skype messages sent from one user to another that are parsed from the chatsync directory.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local Skype user
Chat Initiator	The user that started the conversation
Chat Partner/Group Chat ID	The other user in the chat, or a group chat identifier
Message Type	Whether the message was sent or received
Message	The content or body of the message
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent

Skype Chatsync Messages Carved

Description	Skype messages sent from one user to another that are carved from the chatsync directory.
Notes	

ATTRIBUTE	DESCRIPTION
Message Type	Whether the message was sent or received
Message	The content or body of the message
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent

Skype Contacts

Description	Information about Skype contacts that are recovered, which may or may not be added contacts.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	The name of the contact
Skype Name	The Skype name of the contact
Display Name	The contact's display name
Is Blocked	Whether or not the contact is blocked
Contact Added	Specifies whether the contact is an added contact or just cached into the database (1 if the contact was added, 0 otherwise). Contacts can be cached into the database for a variety of reasons (for example, as a 'suggested contact').
Full Name	The contact's full name
Birthday (yyyy-mm-dd)	The contact's birthday
Gender	The contact's gender
City	The city the contact is from

ATTRIBUTE	DESCRIPTION
State / Province	The state/province the contact is from
Country	The country that the contact is from
Home Phone	The contact's home phone number
Office Phone	The contact's office phone number
PSTN Number	The contact's public switched telephone network
Email(s)	The email address(es) of the contact
Homepage	The contact's homepage
About Info	About the contact
Profile Loaded Date/Time - UTC (yyyy-mm-dd)	Previously called "Profile Created On Date/Time", this attribute represents the date/time when a contact's profile is first created on the user's device. When the profile information is updated by the contact, the date in the database is also updated.
Profile Last Modified Date/Time - UTC (yyyy-mm-dd)	the date and time the contact last modified their profile
Mood Text	The contact's mood
Last Online Date/Time - UTC (yyyy-mm-dd)	The last date and time the contact was seen online
Last Used Date/Time - UTC (yyyy-mm-dd)	The last date and time the contact accessed contacts
Avatar Timestamp Date/Time - UTC (yyyy-mm-dd)	The last date and time the contact updated their avatar

Skype File Transfers

Description	Files that are transferred from one user to another using Skype.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	The name of the user
Partner Handle	The user name of the file transfer partner
Partner Display Name	The display name of the file transfer partner
File Name	The file name being transferred

ATTRIBUTE	DESCRIPTION
Type	The type of file being transferred
File Path	The path to the local file
Transferred File	The file that was transferred
File Size (Bytes)	The size of the file being transferred
Bytes Transferred	The number of bytes that were transferred
Transfer Start Date/Time - UTC (yyyy-mm-dd)	The date and time the file transfer was started
Transfer Finish Date/Time - UTC (yyyy-mm-dd)	The date and time the file transfer completed
Status	The status of the file (for example, transfer, transferring or cancelled)

Skype Group Chat

Description	Information about the Skype group chats that a user is a part of.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	The name of the user
Chat ID	The group chat's unique identifier
Participants	The participants of the chat
Posters	The users that have posted to the chat
Active Members	The currently active user's of the group
Chat name	The name of the chat
Started Date/Time - UTC (yyyy-mm-dd)	The date and time the chat started
Last Changed Date/Time - UTC (yyyy-mm-dd)	The date and time the chat was modified

Skype IP Addresses

Description	IP addresses that are associated with a Skype user account.
Notes	

ATTRIBUTE	DESCRIPTION
Username	The Skype user name
IP Address	The IP address of that user

ATTRIBUTE	DESCRIPTION
IP Address Type	The IP address type
Date/Time - UTC (yyyy-mm-dd)	The date and time of the IP address log

Skype SMS

Description	SMS messages that a user sends or recieves using Skype.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	The name of the user
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent
Author	The author of the message
Message	The message content
Target Number(s)	The recipient phone numbers
Status	The status of the message.
Reply-to Number	A phone number the recipients can reply to

Skype Voicemails

Description	Voicemails that a user sends or recieves using Skype.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	The name of the user
Partner Handle	The user name of the conversation partner
Partner Display Name	The display name of the conversation partner
Subject	Identifies the subject of the voicemail
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent
Duration	The length of the voicemail
Allowed Duration	The maximum length allowed for the voicemail
Size	The size of the recording
Path	The file path of the voicemail
Type	Identifies whether the voicemail was received or sent.
Status	The status of the voicemail, recording or played for example.

Documents

Excel Documents

Description	Microsoft Excel is a spreadsheet processor developed by Microsoft.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified on the filesystem.
Size (Bytes)	The size of the document in bytes.
Saved Size (Bytes)	The size of the document (in bytes) that was recovered. Extremely large documents may not be fully recovered.
File	The actual file.
Title	The title meta-data.
Subject	The subject meta-data.
Authors	The authors of the document.
Keywords	The keywords meta-data in the document.
Comments	The comments meta-data.
Last Author	The last author to edit the document.
Last printed Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last printed, extracted from meta-data within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last modified, extracted from meta-data within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the document was created, extracted from meta-data within the document.
Company	The company meta-data.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

PDF Documents

Description	Portable Document Format (PDF) is a file format used to present documents in a manner independent of application software, hardware, and operating systems. This table captures documents in this file format, extracted from the filesystem and carved from unallocated space.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified on the filesystem.
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
Title	The title of the file.
Subject	The subject of the file.
Authors	The authors of the file.
Keywords	The keywords in the metadata of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the document was created, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last modified, extracted from metadata within the document.
File	The PDF file.

PowerPoint Documents

Description	Microsoft PowerPoint is a presentation creator developed by Microsoft.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created on the filesystem.

ATTRIBUTE	DESCRIPTION
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified on the filesystem.
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Extremely large documents may not be fully recovered.
File	The actual file.
Title	The title meta-data.
Subject	The subject meta-data.
Authors	The authors of the document.
Keywords	The keywords meta-data in the document.
Comments	The comments meta-data.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last printed, extracted from meta-data within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last modified, extracted from meta-data within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the document was created, extracted from meta-data within the document.
Company	The company meta-data.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

RTF Documents

Description	The information for each RTF document that was recovered from the search.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the RTF document.
File Size (Bytes)	The size of the RTF document in bytes.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the RTF document was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the RTF document was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the RTF document was last modified.
File Content	The contents of the RTF document.

Text Documents

Description	Text documents (.txt) that are located on the system.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the text document.
Size (Bytes)	The size of the text document in bytes.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The Date/Time that the text document was last modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The Date/Time that the text document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The Date/Time that the text document was created.

Word Documents

Description	Microsoft Word is a word processor developed by Microsoft.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified on the filesystem.
Size (bytes)	The size of the document
Saved Size (bytes)	The size of the document that was recovered. Extremely large documents may not be fully recovered.
File	The actual file.
Title	The title meta-data.
Subject	The subject meta-data.
Authors	The authors of the document.
Keywords	The keywords meta-data in the document.
Comments	The comments meta-data.
Last Author	The last author to edit the document.

ATTRIBUTE	DESCRIPTION
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last printed, extracted from meta-data within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last modified, extracted from meta-data within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the document was created, extracted from meta-data within the document.
Company	The company meta-data.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

E-mail

Gmail Email Fragments

Description	Contains the Gmail email fragments that were recovered from a Windows Phone device.
Notes	

ATTRIBUTE	DESCRIPTION
HTML Fragment	The HTML fragment of the email

Gmail Webmail

Description	Contains the Gmail email that was recovered from a Windows Phone device.
Notes	

ATTRIBUTE	DESCRIPTION
Email(s)	The email addresses involved with the email.
Status	The status of the email.
Subject	The subject of the email.
Snippet	A snippet of the email.
Attachments	The name of any attachments.
Sent Date/Time - Local Time	The local date and time of when the email was sent. This value is saved in the database as a string, so attempts to sort or filter the column may not behave as expected. Instead of sorting by date, the column sorts alphabetically.

ATTRIBUTE	DESCRIPTION
Last Modified or Viewed Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was last modified.

Hotmail Webmail

Description	Hotmail is a web-based email client that allows users to send and receive emails. Hotmail was replaced by Outlook.com in 2012.
Notes	

ATTRIBUTE	DESCRIPTION
Type	The type of fragment found. Can be one of Contacts, Message, Folder view, Inbox Message, Edit Message, Plaintext Message Fragment, or Welcome Page
HTML Fragment	The HTML fragment that was found

Hushmail Webmail

Description	Carved fragments of messages that are sent or recieved using Hushmail. Uses inbox listings to recover the emails received by a user.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the email
Receiver	The reciever of the email
Subject	The subject of the email
Received Date/Time - UTC (yyyy-mm-dd)	The date and time the email was received

Mailinator Inbox Access

Description	Instances when a user accesess their Mailinator inbox. Mailinator is webmail service that allows users to send and receive emails anonymously.
Notes	

ATTRIBUTE	DESCRIPTION
Inbox	The inbox that was accessed.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the inbox was accessed.

Mailinator Snippets

Description	Snippets of email messages that are sent using Mailinator. Mailinator is webmail service that allows users to send and receive emails anonymously.
Notes	

ATTRIBUTE	DESCRIPTION
Sender Name	The sender of the email.
Sender Address	The sender's email address.
Sender Mailserver IP	The sender's mailserver IP address.
Recipient Address	The receiver of the email.
Subject	The subject of the email.
Boddy Snippet	A snippet of the email body.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time the email was received.

Offline Gmail webmail

Description	Gmail is a web-based email website that allows users to send and receive emails.
Notes	

ATTRIBUTE	DESCRIPTION
From Address	The sender of the email.
To Address(es)	The recipients of the email.
cc Address(es)	The recipients of the email that were CC'd.
bcc Address(es)	The recipients of the email that were BCC'd.
Subject	The subject of the email.
Date/Time - UTC (yyyy-mm-dd)	The date and time the email was sent/received.
Status	The sent status of the email.
Email Body	The body of the email.

Outlook Appointments

Description	Microsoft Outlook is a personal information manager and email client from Microsoft.
Notes	

ATTRIBUTE	DESCRIPTION
Sender Name	The sender name
Recipients	The recipients of the appointment
Recipients CC	The CC'd recipients of the appointment
Recipients BCC	The BCC'd recipients of the appointment
Companies	The companies involved
Subject	The subject of the appointment
Body	The body of the appointment
Attachments	If there are any attachments on the appointment
Start Date/Time - UTC (yyyy-mm-dd)	The date and time the appointment starts
End Date/Time - UTC (yyyy-mm-dd)	The date and time the appointment ends
Location	The location of the appointment
Is All-day Event	Indicates if the appointment is a full date event
Is Recurring	Indicates if the appointment is recurring
Recurrence Pattern Description	The recurring pattern, if applicable
Sensitivity	Indicates if the appointment is sensitive
Is Hidden	Indicates if the appointment is hidden
Is Private	Indicates if the appointment is private
Sender Exchange Account	The senders Exchange Account name
Priority	The priority of the appointment
Importance	The appointment importance setting

Outlook Contacts

Description	Microsoft Outlook is a personal information manager and email client from Microsoft.
Notes	

ATTRIBUTE	DESCRIPTION
Display Name	The contact's display name
Company Name	The contact's company name
Department Name	The contact's department name

ATTRIBUTE	DESCRIPTION
Title	The contact's job title
Profession	The contact's profession
Manager Name	The contact's managers name
Office Location	The contact's office location
Business Phone	The contact's business phone number
Business Phone 2	The contact's business phone number
Business Fax	The contact's business fax number
Business Homepage	The contact's business' website
Email Address 1	The contact's email address
Email Display As 1	How the contact's email should be displayed
Email Display Name 1	The contact's email display name
Email Address 2	The contact's email address
Email Display As 2	How the contact's email should be displayed
Email Display Name 2	The contact's email display name
Email Address 3	The contact's email address
Email Display As 3	How the contact's email should be displayed
Email Display Name 3	The contact's email display name
Cellular Phone	The contact's mobile phone number
Home Address	The contact's address
Home Phone	The contact's home phone number
Home Phone 2	The contact's home phone number
Home Fax	The contact's home fax number
FTP Site	The contact's FTP site
Body	More information about the contact
Attachments	Any attachments on the contact entry
Customer ID	The customer ID of the contact
Last Modifier Name	The person that last modified the contact details
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the contact was last modified

Outlook Journals

Description	Microsoft Outlook is a personal information manager and email client from Microsoft.
Notes	

ATTRIBUTE	DESCRIPTION
Type Description	The type of journal entry

ATTRIBUTE	DESCRIPTION
Subject	The subject of the journal
Start Date/Time - UTC (yyyy-mm-dd)	The start date and time of the journal
End Date/Time - UTC (yyyy-mm-dd)	The end date and time of the journal
Duration (minutes)	The length of the journal entry in minutes
Body	The body of the journal
Attachments	List of attachments on the journal
Creator Name	The journal creators name
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the journal was created
Last Modifier Name	The user that last modified the journal
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the journal was last modified

Outlook Messages

Description	Microsoft Outlook is a personal information manager and email client from Microsoft.
Notes	

ATTRIBUTE	DESCRIPTION
Folder Name	The folder where the email is stored
Sender Name	The sender of the email
To	The recipients of the email
CC	The recipients of the email that were CC'd
BCC	The recipients of the email that were BCC'd
Subject	The subject of the email
Body	The body of the email
Attachments	List of attachments on the email
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the email was created
Delivery Date/Time - UTC (yyyy-mm-dd)	The date and time the email was delivered
Sender Exchange Account	The senders Exchange Account name
Headers	The raw email headers
Priority	The priority of the message
Importance	The email importance setting
Sensitivity	The email sensitivity setting

Outlook Notes

Description	Microsoft Outlook is a personal information manager and email client from Microsoft.
Notes	

ATTRIBUTE	DESCRIPTION
Body	The body of the note
Creator Name	The creator's name of the note
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the note was created
Last Modifier Name	The user that last modified the note
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the note was last modified

Outlook Tasks

Description	Microsoft Outlook is a personal information manager and email client from Microsoft.
Notes	

ATTRIBUTE	DESCRIPTION
Subject	The subject of the task
Due Date (yyyy-mm-dd)	The due date of the task
Status	The status of the task
Percent Complete	The percent the task is complete
Owner	The owner of the task
Body	The content of the task body
Attachments	Any attachments that are attached to the task
Recipients	The recipients of the task
Start Date (yyyy-mm-dd)	The date the task was started
Completed Date (yyyy-mm-dd)	The date the task was completed
Is Complete	Indicates if the task is complete
Actual Work (Minutes)	The actual time it took to finish the task
Total Work (Minutes)	The number of working minutes it took to finish the task
Mileage	The mileage that was travelled for the task
Billing Information	Any billing information for the task
Delegator	The person who delegated this task to the user
Delegation State	If the task was delegated
Creator Name	The creator of the task

ATTRIBUTE	DESCRIPTION
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the task was created
Last Modifier Name	The user that last modified the task
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the task was last modified
Is Hidden	Indicates if the task is hidden
Is Private	Indicates if the task is private
Is Read-Only	Indicates if the task is read-only
Sensitivity	Indicates if the task is sensitive
Is Team Task	Indicates if the task is for a team
Is Recurring	Indicates if the task is recurring
Recurrence Pattern Description	The recurring pattern, if applicable
Is Reminder Set	Indicates if the task has a reminder
Reminder Date/Time - UTC (yyyy-mm-dd)	The date and time of the task reminder
Priority	The priority of the task

Outlook Web App Email Fragments

Description	Microsoft Outlook is a personal information manager and email client. This table captures information related to emails sent and received from Outlook's web application.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the email
Recipients	The recipient(s) of the email
Subject	The subject of the email
Server Timestamp	The timestamp of the email on the server
Is Draft	Indicates if the email is a draft
Fragment	The recovered raw email fragment

Outlook Web App Inbox

Description	Microsoft Outlook is a personal information manager and email client. This table captures information related to the inbox viewed from Outlook's web application.
Notes	

ATTRIBUTE	DESCRIPTION
Participants	The participants of the email
Subject	The subject of the email
Server Timestamp	The timestamp of the email on the server

Outlook Webmail Inbox

Description	Outlook.com (formerly hotmail.com) is a webmail website that allows users to send and receive emails.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the email
Date/Time - UTC (yyyy-mm-dd)	The date and time the email was sent/received
Displayed Date/Time - Local Time	The date and/or time the user was shown on the webpage
Subject	The subject of the message
Status	The sent status of the email

Windows Phone Emails

Description	Contains the emails that were recovered from a Windows Phone device.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the email. Both the pretty name and the email address.
Subject	The subject of the email.
Snippet	The snippet of the email body.
Email Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the email.

Yahoo! Webmail

Description	Yahoo Mail is a web-based email client that allows users to send and receive emails.
Notes	

ATTRIBUTE	DESCRIPTION
Type	One of: 'Folder Listing', which means the email was recovered from the Inbox view or 'Message' which means the user was looking at an individual email, 'Compose', which means the user was composing a message.
Sender Name	The name of the sender
Sender Email	The email of the sender
Receiver Name	The name of the receiver
Receiver Email	The email of the receiver
Subject	The email subject
HTML Fragment	A HTML fragment of the email

Media

Audio

Description	Audio files that are recovered that use the .mp3 or .wav formats.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
File Name	Name of the file.
File Extension	Extension of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the audio file was created.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the audio file was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the audio file was last modified.
File Size (Bytes)	The size of the audio file.
MD5 Hash	An MD5 hash of the audio content.
SHA1 Hash	A SHA1 hash of the audio content.

Carved Video

Description	Videos that are recovered using carving. Supported formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. Other container formats can also be recovered provided that their underlying packets are the same as one of the supported formats.
Notes	As of February 20 2020, this artifact will no longer be included under Videos. Carved Video functionality will be included in the 'Videos' artifact instead.

ATTRIBUTE	DESCRIPTION
Content Format	The format of the video.
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
File Size (Bytes)	The size of the container and file.
Container Format	The format of the video container.
Saved Video Size (Bytes)	The size of the video that was saved to the database.
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.

Pictures

Description	Pictures retrieved using either carving or parsing techniques. The supported formats are as follows: JPEG (.jpeg, .jpg, .jpe), PNG (.png), Bitmaps (.bmp), Graphics Interchange Format (.gif), Icons (.ico), and Tagged Image File Format (.tif, .tiff).
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date/time of the picture in the file system.

ATTRIBUTE	DESCRIPTION
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date/time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date/time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. "Complete" indicates that a full Exif extraction was performed. "Partial" indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. "Failed" indicates that the information may have been corrupted and could not be recovered. "Skipped" indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).

ATTRIBUTE	DESCRIPTION
GPS Longitude	The GPS longitude coordinates of where the picture was taken (extracted from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
GPS Latitude	The GPS Latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS Latitude (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the pciture was taken (extracted from Exif data).
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Potential Original Media	Indicating if the media is likely the original source.
Category	An integer that indicates the Project VIC category for the picture.

Videos

Description	Videos that are recovered using parsing or carving. Supported formats for parsing include AVI, MP4, MOV, MPEG, DIVX, A3GP, ASF, WMV, DVR-MS, MKV, VOB, MOD, and WEBM. Supported carving formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. For more information about supported video formats, see Supported media and file types.
Notes	Supported formats include AVI, MP4, MOV, MPEG, DIVX, A3GP, ASF, WMV, DVR-MS, MKV, VOB, MOD, and WEBM. For more information about supported video formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
File Name	Name of the file.
File Extension	Extension of the file.

ATTRIBUTE	DESCRIPTION
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the video was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the video was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the video was last modified.
File Size (Bytes)	The size of the video.
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. "Complete" indicates that a full Exif extraction was performed, including potential metadata located at the end of the video. "Partial" indicates that only Exif information in the header section of the video file was recovered, which should only occur with very large videos (in excess of the limit set in the options screen). "Failed" indicates that the information may have been corrupted and could not be recovered. "Skipped" indicates that the extraction was skipped.
Media Duration (Seconds)	The duration of the video in seconds (extracted from Exif data).
Original Width	The resolution of the video (extracted from Exif data).
Original Height	The resolution of the video (extracted from Exif data).
Created Date/Time - Local Time	The local date and time when the video was first recorded (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the video was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the video being recored (extracted from Exif data).
Software	The software used to record or modify the video. This could either be the OS version of the phone used to record the video or name of the software used to edit the video in post-production (extracted from Exif data).

ATTRIBUTE	DESCRIPTION
Make	The manufacturer of the camera used to record the video (extracted from Exif data).
Model	The model of the camera used to record the video (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to record the video (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The GPS coordinates of the camera where the video was recorded (extracted from Exif data).
Longitude	The GPS coordinates of the camera where the video was recorded (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the video was recorded (extracted from Exif data).
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.
Content Format	The format of the carved video.
Container Format	The format of the carved video container.
Saved Video Size (Bytes)	The size of the carved video that was saved to the database.

Web Video Fragments

Description	This search recovers two distinct types of web-based video. Fragments of Flash video can be left behind by many video streaming sites, such as YouTube. RTMP Frame Fragments are frames left behind by streaming sites using the RTMP protocol (widely used by webcam chat sites, including Chatroulette and Camstumble). While viewing the case, a thumbnail from a recovered video is displayed, as well as any relevant metadata. Videos can be exported to .FLV format to be played. Due to the nature of the data recovered, some video players will have issues playing the exported files. In these cases, you should try ffmpeg, VLC, and the GOM player.
Notes	

ATTRIBUTE	DESCRIPTION
Preview	A thumbnail preview of the video
Content Recovered	The raw bytes that were recovered
Metadata	Any metadata about the video
Recovered Duration	The length of the video that was recovered

Mobile

SIM Card ICCID

Description	SIM Card ICCID contains the ICCID number that identifies the device's SIM card.
Notes	

ATTRIBUTE	DESCRIPTION
ICCID	The integrated circuit card identifier.

SIM Card IMSI

Description	SIM Card IMSI contains IMSI numbers used to identify the mobile subscriber, as recovered from the SIM card.
Notes	

ATTRIBUTE	DESCRIPTION
IMSI	The international mobile subscriber identity.

SIM Card Phone Numbers

Description	SIM Card Phone Numbers contains records of all the phone numbers saved to the device SIM card. The type of number is indicated by the record type.
Notes	

ATTRIBUTE	DESCRIPTION
Phone Number	The phone number for the specific record type.
Record Type	Identifies the type of record the phone number is. Can be 'Abbreviated dialing numbers(ADN)', 'Emergency call codes (ECC)', 'Last number dialed (LND)', 'MSISDN', 'Service dialing numbers (SDN)', or 'Fixed dialing numbers (FDN)'

SIM Card Service Providers

Description	SIM Card Service Providers contains the names of mobile service providers that the device has connected with, and which are recovered from the SIM card.
Notes	

ATTRIBUTE	DESCRIPTION
Service Provider Name	The identity of the mobile phone service provider.

SIM Card SMS Messages

Description	SIM Card SMS Messages contains messages sent or received by the local user which were saved to the SIM card.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the SMS message.
Recipient	The recipient of the SMS message.
Message Date/Time	For incoming messages, this timestamp indicates when the message was received by the mobile service center. For outgoing messages, there is no data available for this field.
Message	The message body of the SMS message.
Deleted	Identifies whether the message has been deleted. Can be 'Yes' or 'No'
Message Status	Identifies whether the message has been read, unread, draft or sent.
SMSC	The short message service center number.

Operating System

.DS_Store Records

Description	.DS_Store Records contains all the records extracted from .DS_Store files found on the computer. Each record represents a property of a file or a folder. The significance of this artifact is an indicator of high likelihood that the user of the computer was aware of these files and folders with a possibility of attributing a date to that awareness.

Notes	In the Apple macOS operating system, .DS_Store (Desktop Services Store) is a hidden file that stores the display information of its containing folder, similar to the file desktop.ini in Microsoft Windows. The file tracks information such as icon positions, view settings, cached file size, cached last modified date, and even the choice of a background image. The .DS_Store is created and maintained by the Finder application in any folder that it accesses, even on remote file systems mounted from servers that share files (for example, via Server Message Block (SMB) protocol or the Apple Filing Protocol (AFP)). .DS_Store files are also included in archives created by macOS users, such as ZIP files, and they are backed up by some cloud file backup services. This means that the presence of .DS_Store Records artifacts on non-Mac evidence such as Windows, Mobile, or Cloud indicates that some of the data may have originated or have been accessed from a macOS computer at some point. For more information on .DS_Store files and their forensic significance see: .DS_Stores: Like Shellbags but for Macs.

ATTRIBUTE	DESCRIPTION
Record Name	The name of the file or folder as stored in the .DS_Store file.
Record Type	The type of the record, or property, that is being logged in the .DS_Store file for a particular file or folder.
Record Value	The value of the property for the given file or folder.
Record Path	The full path to the file or folder
.DS_Store Created Date/Time - UTC (yyyy-mm-dd)	The created date of the .DS_Store file from which the record was extracted.
.DS_Store Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date of the .DS_Store file from which the record was extracted.
.DS_Store Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date of the .DS_Store file from which the record was extracted.

File Signature Mismatch (Audio)

Description	File Signature Mismatch (Audio) contains identified mismatches between a known file signature header and the extension (or lack thereof) for an audio file. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.

ATTRIBUTE	DESCRIPTION
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.

File Signature Mismatch (Container)

Description	File Signature Mismatch (Container) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a container. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.

File Signature Mismatch (Document)

Description	File Signature Mismatch (Document) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a document. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.

ATTRIBUTE	DESCRIPTION
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.

File Signature Mismatch (Picture)

Description	File Signature Mismatch (Picture) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a picture. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file. If the mime type is unknown, this defaults to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file. If the mime type is unknown, this defaults to application/octet-stream. If there is no file extension, but the mime type is known, a mismatch is is returned.
File Path	The path to the mismatched file.

File Signature Mismatch (Video)

Description	File Signature Mismatch (Video) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a video. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.

ATTRIBUTE	DESCRIPTION
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.

Jump List Dest List Entries

Description	Jump lists are quick lists of recent applications or files that a user launched. The Dest List entries correspond to a list of shortcuts that are generated on a per app basis.
Notes	

ATTRIBUTE	DESCRIPTION
App ID	The unique app identifier generated by Windows based on install location
Potential App Name	A potential app name from a list of common applications and install locations
Entry ID	The entry ID
Data	Other data within the shortcut entry
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last time the shortcut entry was accessed
Pin Status	If the shortcut was pinned in the dest list
Birth Volume MAC Address	The MAC address of the volume the shortcut was created on
New Volume MAC Address	The MAC address of the volume the shortcut is on
NetBios Name	The machine name on the network

Jump List Shortcut Entries

Description	Jump lists are quick lists of recent applications or files that a user can use.
Notes	

ATTRIBUTE	DESCRIPTION
App ID	The unique app identifier generated by Windows based on install location
Potential App Name	A potential app name from a list of common applications and install locations
Jump List Type	The type of jump list. ("Automatic" or "Custom")

ATTRIBUTE	DESCRIPTION
Linked Path	The path to the target file
Arguments	Any commands being passed to the target file
Target File Created Date/Time - UTC (yyyy-mm-dd)	The date and time the shortcut target file was created
Target File Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the shortcut target file was last modified
Target File Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the shortcut target file was last accessed
Target Attributes	Any file attributes of the target file
Drive Type	The type of drive for the shortcut
Serial Number	The serial number of the drive
Volume Name	The name of the volume where the shortcut resides
Net Bios Name	The machine name on the network
MAC Address	The MAC address of the volume the shortcut is on
Target File Size (Bytes)	The size of the shortcut file

LNK Files

Description	LNK files are Windows shortcut files to other files on the system.
Notes	

ATTRIBUTE	DESCRIPTION
Linked Path	The path to the target file
Arguments	Any commands being passed to the target file
Target File Created Date/Time - UTC (yyyy-mm-dd)	The date and time the shortcut target file was created
Target File Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the shortcut target file was last modified
Target File Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the shortcut target file was last accessed
Target Attributes	Any file attributes of the target file
Drive Type	The type of drive for the shortcut
Serial Number	The serial number of the drive
Volume Name	The name of the volume where the shortcut resides

ATTRIBUTE	DESCRIPTION
Show Command	How the shortcut should show the target when opened, one of: SW_SHOWNORMAL, SW_SHOWMAXIMIZED, SW_SHOWMINNOACTIVE, or Unknown.
Net Bios Name	The machine name on the network
MAC Address	The MAC address of the volume the shortcut is on
Target File Size (Bytes)	The size of the shortcut file

Network Share Information

Description	This provides information about mapped network drives on Windows.
Notes	

ATTRIBUTE	DESCRIPTION
Network Name	The network share name
Mapped Drive Letter	The drive letter assigned to the share
Connection Type	The type of connection to the share
Provider Name	The share provider
Account	The account associated to the network share
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the share mapping was last modified

Operating System Information

Description	This table provides information about the Windows installation.
Notes	

ATTRIBUTE	DESCRIPTION
Operating System	The operating system.
Version Number	The version number of the operating system.
Install Date/Time - UTC (yyyy-mm-dd)	The date and time that the operating system was installed.
Product Key	The product key used to license the operating system.
Owner	The owner of the operating system license.
Displayed Computer Name	The computer name that is displayed to the user of the system. This value is updated every time the system is restarted.
Computer Name	The name of the computer. This value can be can be different than the Displayed Computer Name if the user has changed their computer's name and not updated the system.

ATTRIBUTE	DESCRIPTION
DHCP DNS Server (s)	A comma separated list of the DHCP assigned DNS servers. This fragment represents the Domain Name Server(s) (DNS) provided from the DHCP service. This is stored in the registry as "DhcpNameServer".
Operating System Version	The version of the operating system.
Build Number	The build number of the operating system.
Product ID	The product ID of the operating system.
Last Service Pack	The last service pack that was installed.
Organization	The owner of the operating license organization.
Last Shutdown Date/Time - UTC (yyyy-mm-dd)	The date and time that the operating system was last shut down.
System Root	The path to the system root.
Path	The path.
Last Access Time Enabled	Whether or not Last Accessed Times are updated on this computer. If they are, this will be 'Yes', otherwise this will be 'No'.

Prefetch Files - Windows 8/10

Description	Prefetch files are used to speed up launching of frequently used executables. This table is for Windows 8 and 10.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The application that was run.
Application Run Count	The number of times the application was run. On some versions of Windows this count can be zero, while still having run date/time data.
File Created Date/Time - UTC (yyyy-mm-dd)	The date and time when prefetch file was created.
Last Run Date/Time - UTC (yyyy-mm-dd)	The last date and time that the application was run.
File Hash	A hash of the file name and path, which is included in the file name for the prefetch file.
2nd Last Run Date/Time - UTC (yyyy-mm-dd)	The 2nd last date and time that the application was run.
3rd Last Run Date/Time - UTC (yyyy-mm-dd)	The 3rd last date and time that the application was run.

ATTRIBUTE	DESCRIPTION
4th Last Run Date/Time - UTC (yyyy-mm-dd)	The 4th last date and time that the application was run.
5th Last Run Date/Time - UTC (yyyy-mm-dd)	The 5th last date and time that the application was run.
6th Last Run Date/Time - UTC (yyyy-mm-dd)	The 6th last date and time that the application was run.
7th Last Run Date/Time - UTC (yyyy-mm-dd)	The 7th last date and time that the application was run.
8th Last Run Date/Time - UTC (yyyy-mm-dd)	The 8th last date and time that the application was run.
Volume Name	The name of the first volume.
Volume Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the first volume was created.
Volume 2 Name	The name of the second volume.
Volume 2 Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the second volume was created.

Prefetch Files - Windows XP/Vista/7

Description	Prefetch files are used to speed up launching of frequently used executables. This table is for versions of Windows XP, Vista and 7.
Notes	

ATTRIBUTE	DESCRIPTION
Application Name	The application that was run.
Application Run Count	The number of times the application was run. On some versions of Windows this count can be zero, while still having run date/time data.
File Created Date/Time - UTC (yyyy-mm-dd)	The date and time when prefetch file was created.
Last Run Date/Time - UTC (yyyy-mm-dd)	The last date and time that the application was run.
File Hash	A hash of the file name and path, which is included in the file name for the prefetch file.
Volume Name	The name of the first volume.
Volume Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the first volume was created.
Volume 2 Name	The name of the second volume.

ATTRIBUTE	DESCRIPTION
Volume 2 Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the second volume was created.

Shellbags

Description	Windows Shellbags track folder access by keeping logs of the view mode of a folder. If a shellbag record exists for a path, it has been previously viewed.
Notes	

ATTRIBUTE	DESCRIPTION
Path	The path
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the path view was modified
Mode	The view mode to which the path is currently set
Registry Key Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the shellbags registry key was last modified

Startup Items

Description	The configured auto-run programs for the system at startup.
Notes	

ATTRIBUTE	DESCRIPTION
Program Name	The name of the program
Path	The path to the program
Type	The type of autorun (one of 'Run', 'RunOnce', 'RunOnceEx', or 'Startup')
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the autorun was last modified

Timezone Information

Description	The timezone information that is stored in the Windows registry.
Notes	

ATTRIBUTE	DESCRIPTION
Current Control Set	The current control set
Failure Control Set	The last control set with which the system did not boot correctly
Last Known Good Control Set	The last control set with which the system booted correctly
Current Timezone Offset (minutes)	The current timezone offset of the system, in minutes
Standard Timezone Name	The name of the standard timezone for the system
Standard Timezone Offset (minutes)	The offset of the standard timezone for the system, in minutes
Standard Timezone Start Date/Time - Local Time (yyyy-mm-dd)	The date and time at which the standard timezone of the system comes into effect
Daylight Timezone Name	The name of the daylight timezone for the system
Daylight Timezone Offset	The offset of the daylight timezone for the system, in minutes
Daylight Timezone Start Date/Time - Local Time (yyyy-mm-dd)	The date and time at which the daylight timezone of the system comes into effect
Display	The name and offset of the currently active timezone, in a readable format

USB Devices

Description	A history of all USB devices that have been connected to the system.
Notes	

ATTRIBUTE	DESCRIPTION
Device Class ID	The class ID of the USB device
Serial Number	The USB device serial number
Class	The class of the device (USB, USBSTOR)
Last Written Date/Time - UTC (yyyy-mm-dd)	The date and time the device was last written to
Device Description	The description of the device
Friendly Name	The friendly name of the device
Manufacturer	The manufacturer of the device
Last Assigned Drive Letter	The last drive letter that was assigned to the device by Windows
Volume GUID	The GUID of the volume
VSN Decimal	The volume serial number in decimal notation
VSN Hex	The volume serial number in hexadecimal notation
Associated User Accounts	Any user accounts that have used the device

ATTRIBUTE	DESCRIPTION
First Connected Date/Time - UTC (yyyy-mm-dd)	The date and time the device was first connected

User Accounts

Description	User accounts are pulled from the Windows registry.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The user name of the account
Full Name	The user's full name
Type of User	The type of user (either 'Domain User' or 'Built-in')
Account Description	A description of the account
Security Identifier	The security identifier of the account
User Group(s)	Any groups the user is a part of
Login Script	Any login scripts that get run when logging in as that user
Profile Path	The path to the profile folder
Last Login Date/Time - UTC (yyyy-mm-dd)	The date and time the user last logged in
Last Password Change Date/Time - UTC (yyyy-mm-dd)	The date and time the user last changed their password
Last Incorrect Password Login Date/Time - UTC (yyyy-mm-dd)	The date and time the user last entered the wrong password
Login Count	The number of times the user has logged in
Account Disabled	Indicates if the account is disabled
Password Required	Indicates if the account is password protected

Windows Event Logs

Description	Event logs are logs of events from any Windows application.
Notes	

ATTRIBUTE	DESCRIPTION
Level	The level of error
Keywords	Event keywords

ATTRIBUTE	DESCRIPTION
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the event was created
Provider Name	The name of the event provider
Event ID	The event ID
Task category	The category the event falls under
Computer	The computer that generated the event
Security User ID	The security user ID
Event Data	Any event data

Windows Phone Call Logs

Description	Contains the call logs on a Windows Phone 8 device.
Notes	

ATTRIBUTE	DESCRIPTION
Phone Number	The phone number of the other device the phone call was with.
Partner Name	The name of the other person the phone call was with.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the call was started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the call was ended.
Call Status	The status of the call. Can be 'Outgoing Call', 'Incoming Call', or 'Missed Call'

Windows Phone Contacts

Description	Contains the contacts on a Windows Phone 8 device.
Notes	

ATTRIBUTE	DESCRIPTION
Contact Name	The name of the contact.
Phone Number	The phone number of the contact.
Email Address	The email address of the contact.
Address	The street address of the contact.
City	The city of the contact.
State/Province	The state/province of the contact.

ATTRIBUTE	DESCRIPTION
Country	The country of the contact.
Zip/Postal Code	The zip/postal code of the contact.
Occupation	The occupation of the contact.
Employer	The employer of the contact.
Profile Image URL	The URL of the profile image associated with the contact.

Windows Phone Contacts Carved Fragments

Description	Contains the carved contacts fragments from a Windows Phone 8 device.
Notes	

ATTRIBUTE	DESCRIPTION
Fragment	The carved contact fragment. This information is presented as-is and is not formatted or separated.

Windows Phone SMS/MMS

Description	Contains the call logs on a Windows Phone 8 device.
Notes	

ATTRIBUTE	DESCRIPTION
Type	The type of the message, either SMS or MMS.
Direction	The direction of the message, either Incoming or Outgoing.
Message Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the message.
Conversation Partner	The number or identifier of the conversation partner.
Status	The status of the message (read/sent/unknown).
Message	The message content of the SMS or MMS.

Social Networking

Bebo Live Chat

Description	Messages sent or received in Bebo live chat. Information found within these attributes can include the status of the message, the date/time, the sender username, target username, and the message itself.
Notes	

ATTRIBUTE	DESCRIPTION
Status	The sent status of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent
Source ID	The account of the source
Target ID	The account of the target
Message	The content of the chat message

Facebook

Facebook, being one of the most popular social networking sites in the world, presents numerous opportunities for gathering evidence. You can recover messages that are sent and received, status updates and wall posts, and pages and pictures that the user views. On mobile devices, you can also recover user profiles and contacts.

Facebook can provide background information about a user, as well as evidence of who they are communicating with or associated with. Status and location updates can provide details about where a user has been and what they've been doing.

FORENSIC NOTES

The Facebook Pictures artifact represents cached pictures found on the system that originated from Facebook. When caching pictures, Facebook names the pictures using a particular format which allows forensic tools to know that they come from Facebook. These pictures can be user profile pictures, friends' pictures, or any other picture that gets cached while browsing Facebook.

ARTIFACTS

RELATED RESOURCES

How important are Facebook artifacts?

Recovering Facebook artifacts

Facebook Chat

Description	Messages sent and received using Facebook Chat.
Notes	

ATTRIBUTE	DESCRIPTION
Profile ID	The Facebook profile ID of the sender.
Message ID	The unique ID for a specific chat message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Sender ID	The Facebook ID of the sender.
Downloaded Sender Image	The profile picture of the sender, downloaded from the Internet based on the Sender ID.
Sender Name	The name of the sender.
Receiver ID(s)	The Facebook IDs of all the receivers of the message.
Downloaded Receiver Image	The profile picture of the receiver, downloaded from the Internet based on the Receiver ID.
Receiver Names(s)	The name of the receiver.
Message	The content of the chat message.
Sender Offline	The online status of the sender.

Facebook Email Snippets

Description	Snippets of email messages sent using Facebook.
Notes	

ATTRIBUTE	DESCRIPTION
Subject	The subject of the email.
Snippet	A text snippet of the body of the email.
Original Author	The author of the email.

ATTRIBUTE	DESCRIPTION
Recent Author	The most recent author of the email.
Time Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the email was last updated.
Thread ID	The conversation ID.

Facebook Email

Description	Email messages sent using Facebook.
Notes	

ATTRIBUTE	DESCRIPTION
Logged-In User ID	The unique Facebook ID of the user that is currently logged in.
Downloaded Logged-In User Image	The profile picture of the sender, downloaded from the Internet based on the Logged-In User ID
Author ID	The unique Facebook ID of the author of the email
Downloaded Author Image	The profile picture of the sender, downloaded from the Internet based on the Author ID
Author Name	The name of the author
Recipient(s)	The names of the recipients
Subject	The subject of the email
Time Rendered - Local Time (yyyy-mm-dd)	The time that was rendered in the web browser when the user viewed the email
Time Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time of when the email was last updated.
Original Author	The first author of the email.
Message	The content of the email message.
Thread ID	The unique ID that represents the email trail.
Mobile	Indicates whether this email was sent from a mobile device.
Attachments	Indicates whether this email has attachments.

Facebook Pages

Description	The content of the Facebook webpages that are cached.
Notes	

ATTRIBUTE	DESCRIPTION
Fragment	An HTML fragment of a Facebook webpage.

Facebook Pictures

Description	Any cached pictures that are recovered that originate from Facebook.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name and extension of the file the picture came from.
Image	The actual picture content.
Size (Bytes)	The size of the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Potential Profile ID or Picture ID	The potential Facebook profile ID or picture ID.
Tags	The tags associated with the picture content.
Skin Tone Percentage	The percentage of the image that is skin tone.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the picture was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the picture was last accessed.
MD5 Hash	The MD5 hash of the picture content.
SHA1 Hash	The SHA1 hash of the picture content.
PhotoDNA Hash	The PhotoDNA hash of the picture content.
Category	An integer that indicates the Project VIC category for the picture.

Facebook Status Updates/Wall Posts/Comments

Description	Information about Facebook status updates, wall posts, and comments that are cached.
Notes	

ATTRIBUTE	DESCRIPTION
Sender ID	The Facebook ID of the sender.
Downloaded Sender Image	If "Downloading Images from Web" is enabled, the sender's profile picture can be fetched using the Facebook Graph API.
Sender Name	The name of the sender.

ATTRIBUTE	DESCRIPTION
Receiver ID	The Facebook ID of the receiver.
Downloaded Receiver Image	If "Downloading Images from Web" is enabled, the receiver's profile picture can be fetched using the Facebook Graph API.
Receiver Name	The name of the receiver.
Status Update / Wall Post / Comment	The content of the status update, wall post, or comment.
Posted Date/Time - UTC (yyyy-mm-dd)	The date and time of the post.

Google+ Chat

Description	Google+ is a web-based social network that allows users to communicate publicly, share photos and videos and also message privately.
Notes	

ATTRIBUTE	DESCRIPTION
Type	Whether or not the message is a sent or received message
Email	The email address associated with the message
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent
Message	The content of the message

Instagram Pictures

Description	Instagram is a social media website where users share pictures.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Image	The profile picture of the poster
Downloaded Profile Image	The profile image of the poster, downloaded from the Internet
User ID	The user ID of the poster
User Name	The user name of the poster
Instagram Image	The picture that was posted, if found locally.
Downloaded Instagram Image	The picture that was posted, downloaded from the Internet.

Instagram Posts

Description	Instagram is a social media website where users share pictures.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Image	The profile picture of the poster
Download Profile image	The profile image of the poster, downloaded from the Internet
Text	The content of the post
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time the post was created.
User ID	The user ID of the poster
User Name	The user name of the poster
Posted Image	The picture that was posted, if found locally.
Downloaded Posted Image	The picture that was posted, downloaded from the Internet.

LinkedIn Emails

Description	Fragments of emails send or received using LinkedIn. These email fragments can include the from/to names, subject, date/time, and full message. Please note that, depending on the browser, these emails will be in a compressed gzipped form which gets decompressed on-the-fly.
Notes	

ATTRIBUTE	DESCRIPTION
Fragment	An HTML fragment of the email.

MySpace Chat - User Info

Description	MySpace is a social networking website popular with music lovers.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The MySpace user ID
UserName	The user name used on MySpace
Group	The group the user is associated to (if applicable)

ATTRIBUTE	DESCRIPTION
Image	The user's display picture

MySpace Live Chat

Description	Messages sent or received in MySpace live chat. Information found within these attributes can include the status of the message, the date/time, the sender ID, target ID, and the message itself. Some user info is also recoverable, such as the real name/username associated to a MySpace ID, image URL, and other information. This information is saved to a User Info report. This has been discontinued as of 2010.
Notes	

ATTRIBUTE	DESCRIPTION
Status	The sent status of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent
Source ID	The account of the source
Target ID	The account of the target
Message	The contents of the chat message

Sina Weibo Carved Searches

Description	Sina Weibo is a Chinese microblogging (weibo) website. Akin to a hybrid of Twitter and Facebook, it is one of the most popular websites in China.
Notes	

ATTRIBUTE	DESCRIPTION
Search Term	The keyword that was searched for

Sina Weibo Microblogs

Description	Sina Weibo is a Chinese microblogging (weibo) website. Akin to a hybrid of Twitter and Facebook, it is one of the most popular websites in China.
Notes	

ATTRIBUTE	DESCRIPTION
Nickname	The nickname
User ID	The user ID of the blogger
Downloaded Profile Picture	The profile picture of the user, downloaded from the Internet based on the user ID
Microblog Text	The content of the blog
Posted From URL	The URL from which the blog was posted

Sina Weibo Search History

Description	Sina Weibo is a Chinese microblogging (weibo) website. Akin to a hybrid of Twitter and Facebook, it is one of the most popular websites in China.
Notes	

ATTRIBUTE	DESCRIPTION
Search Term	The keyword that was searched for

Twitter

Description	Twitter is a social networking website that allows users to share status messages, known as tweets.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The full name of the user
Screen Name	The twitter handle of the user (eg. @username)
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the tweet was created
Tweet Text	The content of the tweet
In Reply To	This identifies if the tweet was a reply to another user
Status ID	The unique identifier for the tweet
Tweet Source	The type of device/application that was used to create the tweet
Geo	The geo-location of the user when they posted the tweet
Retweeted	This identifies whether the tweet was a retweet
Profile Img URL	The URL link to the profile picture of the user

Web Related

360 Safe Browser Archived Keyword Search Terms

Description	360 Safe Browser is a web browser developed by Qihoo.
Notes	

ATTRIBUTE	DESCRIPTION
Keyword Search Term	The keyword that was searched.
URL	The URL that was invoked because of the search.

360 Safe Browser Archived Web History

Description	Contains all of the websites the user has gone to. Along with when they last visited the site, and how often they have visited the site.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the website the user visited.
Title	The title of the website the user visited.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the user last visited the website.
Visit Count	The amount of times the user has visited the website.
Typed Count	The amount of times the user has manually types the website's URL.
ID	The 360 Safe Browser identifier of the website.

360 Safe Browser Autofill

Description	Contains all of the values that the user has saved to fill in fields at a later date and time.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the field to fill in.

ATTRIBUTE	DESCRIPTION
Value	The value to perform the fill in with.
Count	The amount of times the autofill has been used.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill was first created.

360 Safe Browser Autofill Profiles

Description	Contains all of the profiles that are used to represent a person.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name the person goes by or uses.
Email	The email address to use to contact the person.
Number	The telephone number to use to contact the person.
Company	The company the person works at.
Address Line 1	The first line of the person's address. E.g. 123 Fake Street, Fake Town, Fake Country.
Address Line 2	The second line of the person's address. E.g. Suite 123 or Apt. 123.
City	The city the person lives in.
State	The state or province the person lives in.
Zipcode	The zip code the person lives in.
Country	The country the person lives in.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time the person modified the profile.

360 Safe Browser Bookmarks

Description	Contains all of the websites the user has bookmarked.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the website.
URL	The URL of the website.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was last modified.

ATTRIBUTE	DESCRIPTION
Is Folder	Is the bookmark a folder. Can be 'Yes', 'No' or '-Invalid-'.
Parent Folder	The parent folder of the bookmark.

360 Safe Browser Cache Records

Description	Contains all of the files and their information that has been cached by the browser.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL the file was downloaded from.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was first visited.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The last time the local cache was synced with the webserver.
File Type	The type of cache file.
Content Size (Bytes)	The size of the cache file.
Image	If the content file is an image, it will be displayed here.
Content	If the file is not an image, ie. A javascript file, the raw bytes will be stored here.

360 Safe Browser Cookies

Description	Contains all of the cookies saved to the browser.
Notes	

ATTRIBUTE	DESCRIPTION
Host	The host that created the cookie.
Name	The name of the cookie.
Value	The cookie value.
Accessed Date/Time - UTC(yyyy-mm-dd)	The date and time the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie was created.
Expiration Date/Time - UTC(yyyy-mm-dd)	The date and time the cookie expires.

360 Safe Browser Current Downloads

Description	Contains all of the files currently being downloaded.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file being downloaded.
Download Source	The source URL where the file was downloaded.
Saved To	The local file location.
State	The current state of the download.
Opened By User	If the downloaded file was opened by the user.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download finished.
Bytes Downloaded	The number of bytes download.
File Size (Bytes)	The size of the file being downloaded, in bytes.

360 Safe Browser Current Session

Description	Contains all of the sessions that are currently in use by the browser.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The web page URL.
Title	The title of the web page.
Last Visited Date/Time - (UTC)(yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.

360 Safe Browser Current Tabs

Description	Contains all of the open tabs in the browser.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The web page URL.
Title	The title of the web page.

ATTRIBUTE	DESCRIPTION
Last Visited Date/Time - (UTC)(yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.

360 Safe Browser FavIcons

Description	Contains all of the icons that are belong to common web pages the user goes to.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	The URL of the web page.
Icon URL	The URL to the icon image.
Last Updated Date/Time - UTC(yyyy-mm-dd)	The local file location.
State	The current state of the download.
Opened By User	If the downloaded file was opened by the user.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download finished.
Bytes Downloaded	The number of bytes download.
File Size (Bytes)	The size of the file being downloaded, in bytes.

360 Safe Browser History Index

Description	Contains the browsing history of the user.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	The web page URL.
Title	The title of the web page.
Visited on Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Body	The HTML body of the web page.

360 Safe Browser Last Session

Description	Contains all of the sessions that were last open.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The web page URL.
Title	The title of the web page.
Last Visited Date/Time - (UTC) (yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable

360 Safe Browser Last Tabs

Description	Contains all of the tabs that were last open.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The web page URL.
Title	The title of the web page.
Last Visited Date/Time - (UTC) (yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable

360 Safe Browser Logins

Description	Contains all of the logins for web sites the user has saved.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The user name for the web page.
Password	The password for the login of the web page.
Created Date/Time - UTC (yyyy-mm-dd)	When the login information was created.
URL	The URL to the web page.

360 Safe Browser Saved Credit Cards

Description	Contains all of the credit card information the user has saved.
Notes	

ATTRIBUTE	DESCRIPTION
GUID	The identifier of the credit card.
Name On Card	The name on the credit card.
Expiry Date	The date the credit card is supposed to expire in format 'month-year'.
Card Number	The number of the credit card.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the credit card information was last modified.

360 Safe Browser Shortcuts

Description	Contains all of the shortcuts used by 360 Safe Browser for user entered URLs.
Notes	

ATTRIBUTE	DESCRIPTION
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.
Last Access Date/Time - (UTC) (yyyy-mm-dd)	The last access time of the shortcut.
Web Page Title	The title of the web page.
Times Used	The number of times the shortcut has been used.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Type	The type of shortcut (for example, 'typed url' or 'bookmark').

360 Safe Browser Top Sites

Description	Contains all of the web sites the user goes to most often.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL to the web page.
Title	The title of the web page.
Last Updated Date/Time - (UTC) (yyyy-mm-dd)	The last time the information for the top site was updated.
Thumbnail	The thumbnail of the web page.

360 Safe Browser Web History

Description	Contains all of the web sites the user has gone to.
Notes	

ATTRIBUTE	DESCRIPTION
Date Visited Date/Time - (UTC) (yyyy-mm-dd)	The date and time the URL was first visited.
URL	The URL that was accessed by the user.
Title	The title of the web page.
Visit Count	The number of times the user accessed the URL.
Typed Count	The number of times the user has navigated to this page by typing in the address.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Last Visited Date/Time - (UTC) (yyyy-mm-dd)	The date and time the URL was last visited.

360 Safe Browser Web Visits

Description	A history of the websites that the user visits (includes all visits).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited webpage.
Title	The title of the webpage that was visited.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Bing Toolbar - Search History

Description	Bing toolbar is a toolbar that can be used to search the Internet using Bing.

Notes	

ATTRIBUTE	DESCRIPTION
Search Term	The keyword that was searched for
Search Date/Time - UTC (yyyy-mm-dd)	The date and time the keyword search was conducted.
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Chrome

Google Chrome is free web browser developed by Google and is available on all major operating systems, for both mobile and desktop. As of 2016, Chrome usage represents over 70% of the world's total browser traffic.

Analyzing the websites a user visits and the time the visits occur can provide valuable insights about a user. One notable feature that Google Chrome has is that it allows users to sync their bookmarks, browsing history, and more across multiple platforms and devices by using cloud sync accounts.

FORENSIC NOTES

Web Visits vs Web History

Chrome has two distinct artifacts that are very similar nature: Chrome Web Visits and Chrome Web History. Both of these artifacts are recovered from the History database. Chrome Web History is parsed from the URLS table and only contains information for the last visited date of a particular website. Chrome Web Visits can contain multiple entries for the same website, giving the examiner a more complete look at browser usage if the user visited a website multiple times. For example, if a user visits www.magnetforensics.com six times, the Chrome Web History artifact displays only the last time the site is visited, while the Chrome Web Visits artifact potentially displays records for all six instances. Chrome Web Visits was added in a later version of Chrome than Chrome Web History.

Carved web history

The Chrome / 360 Safe Browser / Opera Carved Web History is essentially the same as Chrome Web History except that it's recovered using carving and you may find additional deleted hits with it. The 360 Safe and Opera browsers are included in this artifact because when the data is carved, it's not possible to tell which browser the hit comes from as they're all formatted the same way.

Autofill and profile data

Chrome stores field data that the user has previously input as autofill and profile settings. For example, if you visit magnetforensics.com and login to the customer portal, browsers automatically save your username (and other details) so that you don't have to type it in each time you visit the site. This data is helpful for recovering usernames and other information that your user has filled out on various sites.

Sessions and tabs

When the system has an active session available, Chrome stores the browsing activity as the Chrome Current Session and any tabs that are open as Chrome Current tabs. The previous session and tabs are maintained in Chrome Last Session and Chrome Last Tabs so that the user can restore the last session and tabs if Chrome is closed.

ARTIFACTS

RELATED RESOURCES

How does Chrome's 'incognito' mode affect digital forensics?

Forensic email analysis: browser artifacts you may find on a PC or laptop

Chrome Autofill

Description	Chrome Autofill contains records of the autofill values that Chrome saves for different types of text fields.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the autofill value.
Value	The saved autofill value for this type of field.
Count	Count of this autofill.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill was last used.

Chrome Web Visits

Description	A history of the websites that the user visits (includes all visits).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the visited webpage.
Title	The title of the webpage that was visited.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Edge Cache Data

Description	Information about cache data that was saved during browsing.
Notes	This artifact allows an investigator to see the content a user views, it's origin, and how often the content is reused by the browser. By clearing the cache, the user can effectively delete these records. In some cases, records do not get deleted from the database, but in cases where the files are deleted, the original files cannot be restored.

ATTRIBUTE	DESCRIPTION
Entry ID	The entry ID.
URL	The URL of the cache data source.
Creation Date/Time - UTC (yyyy-mm-dd)	Date and Time when cache data was saved on the machine.

ATTRIBUTE	DESCRIPTION
Last Modified Date/Time - UTC (yyyy-mm-dd)	Date and Time when cache data was modified on the source side.
File Type	The file type.
Visit Count	Indicates the number of times the current cache file was accessed.
Content Size (Bytes)	Cache file size in bytes.
Image	The content of the file as an image, if the file is a supported image type.
File	The content of the file in raw bytes.
Original Path	Original absolute path to the cache file stored in the database.
Relative Path	A relative path to the file based on the location of the WebCache database, or [Doesn't exist] if the file is not found.

Edge Extensions

Description	Information about the extensions/plugins installed in the user's Edge browser
Notes	

ATTRIBUTE	DESCRIPTION
Package Name	The Package name for the extension
Application Name	The name of the extension
Version Number	The most recent version number of the extension
Created Date/Time - UTC (yyyy-mm-dd)	The time when this extension was created
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The most recent time the AppxManifest file for the extension was accessed (most likely the same as created time)
Last Modified Date/Time - UTC (yyyy-mm-dd)	The most recent time when the extension was updated

Edge Favorites

Description	Edge Favorites contains information about the websites a user favorites while browsing.
Notes	This artifact allows an investigator to see the content a user views, it's origin, and how often the content is reused by the browser. By clearing the cache, the user can effectively delete these records. In some cases, records do not get deleted from the database, but in cases where the files are deleted, the original files cannot be restored.

ATTRIBUTE	DESCRIPTION
Favorite Name	The name given to the favorite.
Is Folder	Indicates whether the item is a folder or a URL for a website (Yes if the item is a folder, and No if the item is a URL).
URL	The URL of the favorite.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the favorite was last modified.
Favicon URL	The URL of the favicon for the website.

Edge Last Session

Description	Information about the last snapshot Edge took of the user's browsing session.
Notes	At certain time intervals, Edge takes a snapshot of the user's browsing session. Using this artifact, an investigator is able to see exactly what the user was looking at, at the time of snapshot. The time interval between snapshots is unknown. Due to the interval, it's possible for a tab to be opened and closed quick enough that the tab isn't included in a snapshot.

ATTRIBUTE	DESCRIPTION
Page URL	The URL of the web page.
Page Title	The title of the web page.
Image	The browser generated snapshot of the page.
Body	The HTML body that was saved from the page.

Edge Reading Lists

Description	Edge Reading Lists contains collections of websites that the user has saved for offline viewing.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the Reading List page.
URL	The URL of the Reading List page.
Source Address	Other source information for the Reading List page.
Picture Path	A file path to pictures associated with the Reading List page.
Deleted	Indicates whether the user has deleted the Reading List page.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time the Reading List page was added.
Last Access Date/Time - UTC (yyyy-mm-dd)	The date and time the Reading List page was last accessed.

ATTRIBUTE	DESCRIPTION
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the Reading List page was updated.

Edge Top Sites

Description	Edge Top Sites lists the websites that the user visits frequently in the Edge browser. Top Sites can also be removed or added by the user.
Notes	

ATTRIBUTE	DESCRIPTION
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the page was added as a Top Site.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the Top Site was updated.
Favicon URL	The URL of the favicon for the Top Site.
Title	The title of the Top Site.
URL	The URL of the Top Site.

Edge/Internet Explorer 10-11 Content

Description	Content that the browser caches, including web pages, pictures and other resources.
Notes	

ATTRIBUTE	DESCRIPTION
Entry ID	The entry ID.
URL	The URL of the cache record.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The most recent visit to the URL.
Last Modified by Web Server Date/Time - UTC (yyyy-mm-dd)	The last time the content was modified on the web server. This time is reflective of when the website created the content on the page and can be before the system being examined was built.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the content was created on the local system.
Access Count	The number of times the content was accessed through the web browser.
Filename	The filename of the cached content.
File Size (Bytes)	The size of the cache file.
Image	If the content is an image, it will be displayed here.
Content	If the file is not an image, i.e. a javascript file, the raw bytes will be stored here.

Edge/Internet Explorer 10-11 Cookies

Description	Site usage information that websites send to the browser when a user visits their sites.
Notes	

ATTRIBUTE	DESCRIPTION
Entry ID	The entry ID.
User	The local user on the system.
URL	The URL that the cookie is for.
Accessed Date/Time - UTC (yyyy-mm-dd)	The most recent visit to the URL.
Updated Date/Time - UTC (yyyy-mm-dd)	The last date and time the cookie was updated by the website at the URL visited.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie was created.
Access Count	The number of times the cookie was accessed.
Filename	The filename of the cookie.
File Size (Bytes)	The size of the cookie.

Edge/Internet Explorer 10-11 Daily/Weekly History

Description	Websites that a user visits using Internet Explorer, which are recovered from the Daily/Weekly history.
Notes	At the end of the week, all the daily .dat records are bundled into a weekly history and a new daily .dat file is created. This table represents a good secondary source for evidence if the main history is missing details or records.

ATTRIBUTE	DESCRIPTION
Entry ID	The entry ID.
URL	The URL that was accessed by the user.
User	The local user on the system.
Accessed Date/Time - UTC (yyyy-mm-dd)	The most recent visit to the URL.
Access Count	The number of times the website was accessed.
Browser Source	The directory of the browser from where the history is extracted from.

Edge/Internet Explorer 10-11 Dependency Entries

Description	A history of the websites that the browser is required to load in order to render a page.
Notes	Records for this artifact are similar to the main history, the difference being that this artifact also includes dependencies for viewed websites (for example, if a viewed website contains pictures stored on another website).

ATTRIBUTE	DESCRIPTION
Entry ID	The entry ID.
URL	The URL visited by the user.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The most recent visit to the URL.

Edge/Internet Explorer 10-11 Downloads

Description	Information about the files a user downloads using the browser.
Notes	Internet Explorer 9 introduced a new integrated download manager which stores the details of downloaded files in a new download INDEX.DAT file. This file has a different structure to the standard INDEX.DAT files.

ATTRIBUTE	DESCRIPTION
Entry ID	The entry ID.
URL	The URL of the file download.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last time the user accessed the download URL.
Redirect URL	The previous URL that led the user to the download URL.
Download Location	The local path where the file was saved.
Temporary Download Location	The local path where the file was saved temporarily (usually while downloading).

Edge/Internet Explorer 10-11 Main History

Description	Records of the websites that a user visits using Internet Explorer, which are recovered from the main history.
Notes	The access count does not always accurately represent the real access count. These values should only be used as an estimate.

ATTRIBUTE	DESCRIPTION
Entry ID	The entry ID.
URL	The URL that was accessed by the user.
User	The local user on the system.
Accessed Date/Time - UTC (yyyy-mm-dd)	The most recent visit to the URL.
Page Title	The title of the webpage.
Access Count	The number of times the website was accessed.
Browser Source	The directory of the browser from where the history is extracted from.

Firefox Bookmarks

Description	Contains the bookmarks from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the website that was bookmarked.
Date Added Date/Time - UTC (yyyy-MM-dd)	The Date/Time the bookmark was created.
Last Modified Date/Time - UTC (yyyy-MM-dd)	The Date/Time the field was last modified.
Title	The title of the bookmark.
Bookmark Type	The type of bookmark, can be either 'Bookmark Item' or 'Bookmark Folder'.

Firefox Cache Records

Description	Contains all of the cached entries in the Firefox Cache Map.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the cache entry.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cache entry was created.
MIME Type	The MIME type of the cache data.
Content Size (Bytes)	The content size of the cached data.
Image	The image, should one be associated with the cache entry.

ATTRIBUTE	DESCRIPTION
Content	The content, should any be associated with the cache entry.

Firefox Cookies

Description	Contains the cookies from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
Host	The host domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-MM-dd)	The Date/Time the cookie was last accessed.
Created Date/Time - UTC (yyyy-MM-dd)	The Date/Time the cookie was created.
Expiration Date/Time - UTC (yyyy-MM-dd)	The Date/Time the cookie will expire, if it is set to expire.
Path	The path to the cookie.

Firefox Downloads

Description	Contains the downloads from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file being downloaded.
Download Source	The URL of the file being downloaded.
Start Date/Time - UTC (yyyy-MM-dd)	The Date/Time the download was started.
End Date/Time - UTC (yyyy-MM-dd)	The Date/Time the download was ended.
Saved To	The path to where the file was downloaded to.
Temp Path	The path to where the file was saved during downloading.
State	The state of the download can be 'Download In Progress', 'Download Complete', 'Download Stopped', or 'Download Paused'.
Referrer	If the web page used a mirror for downloading, the path to the original download URL.

Firefox FavIcons

Description	Contains the fav icons from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the icon.

Firefox FormHistory

Description	Contains the form history from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
Field Name	The name of the field.
Value	The value of the field.
First Used Date/Time - UTC (yyyy-MM-dd)	The Date/Time the field was first used.
Last Used Date/Time - UTC (yyyy-MM-dd)	The Date/Time the field was last used.
Times Used	The number of times the field has been used.
ID	The unique ID of the field.

Firefox Input History

Description	Contains the input to forms from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL the input was given to.
Input	The value that was given.
Use Count	The number of times the input has been used.
ID	The unique ID of the input.

Firefox Private Browsing History

Description	Contains the URLs that were loaded during a Private Browsing session from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL.

Firefox SessionStore Artifacts

Description	Contains the web pages from the last active session from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The title of the web page.
URL	The URL of the web page.
Referrer URL	The URL of the web page, if the web page was a redirect.

Firefox Web History

Description	Contains the web pages from the last active session from the Firefox web browser on a device.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the web page.
Last Visited Date/Time - UTC (yyyy-MM-dd)	The Date/Time the web page was last visited.
Title	The title of the web page.
Visit Count	The number of times the web page has been visited.
Is Typed	Did the user type the URL, can be 'Yes' or 'No'.

Firefox Web Visits

Description	Contains all of the non-archived URL visits for Firefox.

Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL that was visited.
Title	The title of the page that was visited.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the page was visited.
Is Typed	Did the user type the URL, can be 'Yes' or 'No'.
Transition Type	How the transition to the page happened.

Flash Cookies

Description	Flash cookies are internet browser cookies that are saved when a user watches a flash video (eg. Youtube)
Notes	

ATTRIBUTE	DESCRIPTION
Cookie Name	The name of the cookie
Content	The flash content of the cookie. This content is essentially serialized ActionScript code. Primitive values such as integers and strings are shown, as well as more complicated data structures such as objects and arrays. A complex data structure's value is shown only once, along with an "object ID" that gets generated. For all subsequent references to that structure in the content, it's referred to by the generated object ID.
Domain	The domain/host that created the cookie
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Google Analytics First Visit Cookies

Description	Information about Google Analytics first-visit cookies that are discovered in other artifacts.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the URL.
Creation DateTime	Date/Time when the site was vist visited.

ATTRIBUTE	DESCRIPTION
Most Recent Visit Date/Time	Date/Time of most recent session.
2nd Most Recent Visit Date/Time	Date/Time of previous session.
Hits	Number of visit.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Google Analytics First Visit Cookies Carved

Description	Information about Google Analytics first-visit cookies that are recovered using carving.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the URL.
Creation DateTime	Date/Time when the cookie was created.
Most Recent Visit Date/Time	Date/Time of most recent session.
2nd Most Recent Visit Date/Time	Date/Time of previous session.
Hits	Number of visit.

Google Analytics Referral Cookies

Description	Information about Google Analytics referral cookies that are discovered in other artifacts.
Notes	

ATTRIBUTE	DESCRIPTION
Cookie Source	The source URL used to reach the site.
Host	Contains the domain of the URL.
Update Date/Time	The last time the cookie was updated.
Campaign	The method of referral.
Access Method	Whether the site was accessed organically or was referred.
Keyword	Keywords used to arrive at the site.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Google Analytics Referral Cookies Carved

Description	Information about Google Analytics referral cookies that are recovered using carving.
Notes	

ATTRIBUTE	DESCRIPTION
Cookie Source	The source URL used to reach the site.
Host	Contains the domain of the URL.
Update Date/Time	The last time the cookie was updated.
Campaign	The method of referral.
Access Method	Whether the site was accessed organically or was referred.
Keyword	Keywords used to arrive at the site.

Google Analytics Session Cookies

Description	Information about Google Analytics session cookies that are discovered in other artifacts.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the URL.
Page Views	The number of visits to this page from the user.
Start Current Session Date/Time	The start time of the current sesion.
Outbound Link Events Left	
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Google Analytics Session Cookies Carved

Description	Information about Google Analytics session cookies that are recovered using carving.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the URL.
Page Views	The number of visits to this page from the user.
Start Current Session Date/Time	The start Date/Time of the current sesion.

ATTRIBUTE	DESCRIPTION
Outbound Link Events Left	

Google Analytics URLs

Description	URLs that are discovered in other artifacts that are related to Google Analytics.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the web site. If the url cannot be recovered, the source of the url containing all the metadata is displayed instead.
Page Title	The name of the web site. This value is carved from the source starting after 'utmdt=' and ending at '&'
Host Name	Contains the domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Google Analytics URLs Carved

Description	Information about Google Analytics URLs that are recovered using carving.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the web site. If the url cannot be recovered, the source of the url containing all the metadata is displayed instead.
Page Title	The name of the web site. This value is carved from the source starting after 'utmdt=' and ending at '&'
Host Name	Contains the domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'

ATTRIBUTE	DESCRIPTION
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'

Google Maps

Description	Google maps is a free web service that allows users to get directions.
Notes	

ATTRIBUTE	DESCRIPTION
Search Query	The term that was searched for
Starting Location	The starting location for navigation/directions.
Center of Map	Where the map was centered
Business Latitude and Longitude	The latitude and longitude of the business location.
Source Address	The source physical address.
Destination Address	The users desired destination
Route Type	How the user will travel (eg. Car, bus, bike)
Additional Address	Any additional addresses within the navigation
Street View Latitude/Longitude	The latitude and longitude information in street view.

Google Maps Tiles

Description	Google maps is a free web service that allows users to get directions.
Notes	

ATTRIBUTE	DESCRIPTION
Image	The actual picture content.
X Coordinate	The X coordinate value that Google uses to download the right tile.
Y Coordinate	The Y coordinate value that Google uses to download the right tile.
Zoom Level	The level that the user was zoomed in to the map. Can be understood as the Z coordinate value that Google uses to download the right tile.

Google Toolbar

Description	The Google toolbar is a browser add-on where a user can perform Google searches. While there are many different features to the Google Toolbar, search history is the focus. Search history can be either typed or done by autocomplete. It's also possible to determine where the user's search comes from, whether it is Google Search, YouTube, Google Maps, Google News, etc.
Notes	

ATTRIBUTE	DESCRIPTION
Search	The keyword that was searched for
Category	The category the search was conducted in (pictures, web, etc.)

Internet Explorer Cache Records

Description	Temporary Internet files that are written locally when the user views pages from the Internet.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the cache record.
User	The local user.
Last Modified by Web Server Date/Time - UTC (yyyy-mm-dd)	The last time the content was modified on the web server. This time is reflective of when the website created the content on the page and can be before the system being examined was built.
Last Checked by Local Host Date/Time - UTC (yyyy-mm-dd)	The date and time the content was checked for recency on the local system.
Cache Retrieval Count	The number of times the cache record was requested by the browser.
Filename	The name of the file.
File Type	The filename of the cached content.
Content Size (Bytes)	The size of the cache file.
Image	If the content file is an image, it will be displayed here.
Content	If the file is not an image, ie. A javascript file, the raw bytes will be stored here.

Internet Explorer Cookie Records

Description	Site usage information that websites send to the browser when a user visits their sites.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL that created the cookie.
User	The user of the system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last date and time the URL was accessed.
Last Modified by Web Server Date/Time - UTC (yyyy-mm-dd)	The last date and time the URL record was modified.
Visit Count	The number of times the URL was visited.
Web Page Title	The title of the webpage.
File Name	The name of the cookie file.

Internet Explorer Cookies

Description	Site usage information that websites send to the browser when a user visits their sites.
Notes	

ATTRIBUTE	DESCRIPTION
Host	The host that created the cookie.
Name	The name of the cookie.
Value	The cookie value.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie expires.
Flags	The flags associated with the cookie.

Internet Explorer Downloads

Description	Information about the files a user downloads using the browser.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL for the file download.
Date/Time - UTC (yyyy-mm-dd)	The date and time the file was downloaded.
Status	The download status.
Saved To	The local path where the file was saved.
Referrer URL	The previous URL that led the user to the download URL.
File Size (Bytes)	The size of the file in bytes.
Source IP	The IP address of the download URL.

Internet Explorer Favorites

Description	Web pages that the user has set as a favorite.
Notes	

ATTRIBUTE	DESCRIPTION
Favorite Name	The name of the favorite as it shows up in Internet Explorer.
URL	The URL of the favorite.
Modified Date/Time - UTC (yyyy-mm-dd)	The last time the user modified the favorite.
User	The user to whom the favourite belongs.
Favorites Root Location	The local path that is the root storage point for the favorite.
Folder Structure	The folder structure under which the favorite will show up in Internet Explorer.
Icon URL	The url of the icon for the favorite if an icon does exist.

Internet Explorer InPrivate/Recovery URLs

Description	URLs visited during InPrivate browsing that are saved in Internet Explorer recovery files (used to recover tabs in the event of a crash).
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL that was visited.
File Create Date/Time - UTC (yyyy-mm-dd)	The date and time that the Internet record was created.
Description	The title of the website.
Local MAC address	The MAC address of the local machine.

Internet Explorer Leak Records

Description	Browser history records that are scheduled for deletion.
Notes	LEAK artifacts are created when an error occurs while the system attempts to delete a record and the Temporary Internet File is unavailable for some reason.

ATTRIBUTE	DESCRIPTION
URL	The URL visited.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time the URL record was modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last date and time the URL was accessed.
Visit Count	The number of times the URL was visited.

Internet Explorer Main History

Description	Websites that a user visits using Internet Explorer, which are recovered from the main history.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL that was visited.
User	The local user.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Last visited (2nd Timestamp) Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.
Web Page Title	The webpage title.

Internet Explorer PrivacIE Records

Description	Websites that a user visits while having the privacy settings turned on.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL visited.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time the URL record was modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last date and time the URL was accessed.
Visit Count	The number of times the URL was visited.

Internet Explorer Typed URLs

Description	URLs that the user types directly into the address bar for Internet Explorer.

Notes	This includes data that a user pastes into the address bar, as well as instances when a user starts typing in the address bar and clicks on a suggestion from the browser. You may also see local paths and network locations here when the user types a location in Windows Explorer.

ATTRIBUTE	DESCRIPTION
URL	The URL that was typed into the address bar.
Last Entered Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last typed.

Internet Explorer Weekly History

Description	Websites that a user visits using Internet Explorer, which are recovered from the weekly history.
Notes	At the end of the week, all the daily .dat records are bundled into a weekly history and a new daily .dat file is created. This table represents a good secondary source for evidence if the main history is missing details or records.

ATTRIBUTE	DESCRIPTION
URL	The URL that was visited.
User	The local user.
Last Visited Date/Time (local time) (yyyy-mm-dd)	The date and time the URL was last visited. This date is local to the machine that visited the website.
Weekly History File Created Date/Time - UTC (yyyy-mm-dd)	The date and time the weekly history file was created.
Visit Count	The number of times the user accessed the URL.
Web Page Title	The webpage title.

Malware/Phishing URLs

Description	Records that are believed to be either malware or phishing related URLs.
Notes	

ATTRIBUTE	DESCRIPTION
Site Name	The name of the web site.
URL	The URL of the web site.
Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the artifact.
Artifact	The name of the artifact the URL belongs to.
Artifact ID	The row Id of the URL in the original artifact table.

Opera Archived Keyword Search Terms

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
Keyword Search Term	The keyword that was searched
URL	The URL that was invoked by the search

Opera Archived Web History

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was first visited
URL	The URL that was accessed by the user
Title	The title of the web page
Visit Count	The number of times the user accessed the URL
Typed Count	The number of times the user has navigated to this page by typing in the address
Transition Type	Describes how the browser navigated to a particular URL on a particular visit. For example, if a user visits a page by clicking a link on another page, the transition type is "Link".
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited

Opera Autofill Profiles

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the user
Email	The user's email
Number	The user's phone number
Company	The user's company
Address Line 1	The user's address
Address Line 2	The user's address
City	The city the user is from
State	The state the user is from
Zipcode	The zipcode of the user
Country	The user's country
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill profile was last modified

Opera Bookmarks

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
Name	The name of the bookmark
URL	The URL that was bookmarked
Added Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was added
Parent	The parent bookmarks folder (if applicable)
Type	The type of bookmark

Opera Cache Records

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL the file was downloaded from
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited

ATTRIBUTE	DESCRIPTION
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was first visited
Last Sync Date/Time - UTC (yyyy-mm-dd)	The last time the local cache was synced with the webserver
File Type	The type of cache file
Content Size (Bytes)	The size of the cache file
Image	If the content file is an image, it will be displayed here
Content	If the file is not an image, e.g. a javascript file, the raw bytes will be stored here

Opera Cookies

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
Host	The host that created the cookie
Name	The name of the cookie
Value	The cookie value
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie was last accessed
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie was created
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie expires
Path	The path to the cookie

Opera Current Session

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL
Title	The title of the webpage
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited
Visit Count	The number of times the user accessed the URL

ATTRIBUTE	DESCRIPTION
Redirect URL	The URL to use to redirect, if applicable

Opera Current Tabs

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL
Title	The title of the webpage
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited
Visit Count	The number of times the user accessed the URL
Redirect URL	The URL to use to redirect, if applicable

Opera Downloads

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name of the file being downloaded
Download Source	The source URL where the file was downloaded
Saved To	The local file location
State	The current state of the download
Opened By User	If the downloaded file was opened by the user
Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started
End Date/Time - UTC (yyyy-mm-dd)	The date and time when the download finished
Bytes Downloaded	The number of bytes downloaded
File Size (Bytes)	The total file size in bytes

Opera History Index

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
Page URL	The webpage URL
Title	The title of the webpage
Visited On Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited
Body	The HTML body of the webpage

Opera Last Session

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL
Title	The title of the webpage
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited
Visit Count	The number of times the user accessed the URL
Redirect URL	The URL to use to redirect, if applicable

Opera Last Tabs

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL
Title	The title of the webpage
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited

ATTRIBUTE	DESCRIPTION
Visit Count	The number of times the user accessed the URL
Redirect URL	The URL used to redirect, if applicable

Opera Logins

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL the autofill was extracted from
Username	The user name to be auto-populated
Password	The password that was remembered
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill was saved

Opera Saved Credit Cards

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
GUID	A unique identifier for the credit card
Name On Card	The name on the credit card
Expiry Date	The date the credit card is supposed to expire in format 'month-year'.
Card Number	The credit card number
Date Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time the credit card information was modified

Opera Search Field History

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
Search Entries	The term that was searched for

Opera Shortcuts

Description	Contains all of the shortcuts used by Opera for user entered URLs.
Notes	

ATTRIBUTE	DESCRIPTION
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.
Last Access Date/Time - (UTC) (yyyy-mm-dd)	The last access time of the shortcut.
Web Page Title	The title of the web page.
Times Used	The number of times the shortcut has been used.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Type	The type of shortcut (for example, 'typed url' or 'bookmark').

Opera Top Sites

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL
Title	The title of the webpage
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last date and time the top site was updated
Thumbnail	A thumbnail of the webpage

Opera Typed History

Description	Opera is a web browser developed by Opera Software. Opera Typed History includes those addresses that have been entered explicitly, as opposed to addresses that were visited via a link. This search will carve and parse web history from the Opera web browser, including carving/-parsing the typed history (URLs or search terms entered by the user). The entire history file is not required, single records can be carved from live RAM captures and unallocated clusters, etc.
Notes	

ATTRIBUTE	DESCRIPTION
Last Typed Date/Time - UTC (yyyy-mm-dd)	The last date and time the content was typed
Typed URL/Data	The content that was typed. Could be a URL or other data
Type	The type of content that was typed, e.g. URL

Opera Web History

Description	Opera is a web browser developed by Opera Software. Web history are recently visited web pages. Opera stores a user's browsing history so that he or she can view it later. This search will carve and parse web history from the Opera web browser, including carving/parsing the typed history (URLs or search terms entered by the user). The entire history file is not required, single records can be carved from live RAM captures and unallocated clusters, etc.
Notes	

ATTRIBUTE	DESCRIPTION
Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the user visited the website
URL	The URL accessed
Title	The webpage title

Pornography URLs

Description	Records that are believed to be pornography related URLs.
Notes	You can find a list of the domains that are supported by this refined result at Pornography URLs.

ATTRIBUTE	DESCRIPTION
Site Name	The name of the web site.

ATTRIBUTE	DESCRIPTION
URL	The URL of the web site.
Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the artifact.
Artifact	The name of the artifact the URL belongs to.
Artifact ID	The row Id of the URL in the original artifact table.

Potential Browser Activity

Description	The Browser Activity artifact will recover browser-related URLs. This includes Chrome Incognito and Firefox Private Browsing URLs, HTTP request artifacts from multiple browsers, and regular web browsing artifacts. This does not include metadata such as the Windows username, dates/-times, and so on. Note that some recovered URLs can be from background browser processes related to certificate authorities, etc.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL that was accessed either programmatically or by the user
User Agent	The application used to request the URL. Often this is the browser type (eg. Google Chrome)

Rebuilt Webpages

Description	Viewable webpages that are rebuilt from data that's been recovered from the cache.
Notes	

ATTRIBUTE	DESCRIPTION
Page Title	The title of the page
URL	The cached URL
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the cache entry was created
Domain	The domain for the cache entry
Cache Table	The table the cache entry originates from
Cache RowID	The row id the cache entry originates from

Safari Bookmarks

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows.
Notes	

ATTRIBUTE	DESCRIPTION
Title	The name of the bookmark
URL	The URL that was bookmarked

Safari Cache Records

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL the file was downloaded from
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cache file was created
File Type	The type of the cache file
Content Size	The size of the cache file
Image	If the content file is an image, it will be displayed here
Content	If the file is not an image, i.e. A javascript file, the raw bytes will be stored here

Safari Downloads

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows.
Notes	

ATTRIBUTE	DESCRIPTION
Download URL	The URL of the file download
Saved to Path	The local path where the download was saved
Download Identifier	The unique identifier for the download

ATTRIBUTE	DESCRIPTION
Amount Downloaded (Bytes)	The number of bytes downloaded
Size of Download (Bytes)	The size of the download

Safari History

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of a visited web page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Redirect URL	The URL the user was redirected to.
Title	The title of the web page.
Visit Count	The number of times the URL was visited.
Visit Source	Whether the website was viewed on the local device or on a synced device.

Safari Last Session

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows.
Notes	

ATTRIBUTE	DESCRIPTION
Tab URL	The webpage URL
Tab Title	The title of the webpage

Safari Top Sites

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The webpage URL
Title	The title of the webpage
Feed Last Update Time	The last date and time the top site content was updated
Feed URL	The URL of the RSS feed

WebKit Browser Session/Tabs (Carved)

Description	WebKit Browser Sessions/Tabs contains information about the browser sessions and tabs that the user has open, while using a browser built with WebKit. Some examples of browsers that use WebKit are Chrome, Opera, and 360 Safe Browser. This artifact consolidates the existing Chrome, Safe Browser, and Opera equivalents in a single artifact. Usage of other browsers, such as Firefox and Safari, aren't likely to appear under this artifact.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The web page URL.
Title	The title of the web page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

WebKit Browser Web History (Carved)

Description	WebKit Browser Web History contains information about the websites that a user visits while using a browser built with WebKit. Some examples of browsers that use WebKit are Chrome, Opera, and 360 Safe Browser. This artifact consolidates the existing Chrome, Safe Browser, and Opera equivalents in a single artifact. Usage of other browsers aren't likely to appear under this artifact, however, some URLs found by other browsers may also be found by this artifact.
Notes	

ATTRIBUTE	DESCRIPTION
URL	URL of the visited webpage.
Title	Title of the visited webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time this webpage was last visited
Visit Count	The number of times the webpage was visited.

ATTRIBUTE	DESCRIPTION
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

KINDLE

Advanced Search Tools

Dynamic Application Finder

Description	
Notes	

ATTRIBUTE	DESCRIPTION

Chat

AIM

Description	America OnLine Instant Messenger (AIM) is a desktop chat application that allows AOL account holders to chat with one another and transfer files.
Notes	

ATTRIBUTE	DESCRIPTION
Fragment	A HTML fragment of an AIM message

AIM Chat Messages

Description	America OnLine Instant Messenger (AIM) is a desktop chat application that allows AOL account holders to chat with one another and transfer files.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the AIM chat message.
Recipient	The recipient of the AIM chat message.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.

ATTRIBUTE	DESCRIPTION
Message	The message body.

Skype Accounts

Description	Information about the Skype accounts that are recovered, such as user info and when the account was created.
Notes	

ATTRIBUTE	DESCRIPTION
Skype Name	Skype name of the account
Display Name	Display name of this account
Full Name	Full Name of this account
Birthday	Birthday of this accoutn
Gender	Gender of this account
City	City where this account is located
State/Province	State/Province this account is located
Country	Country this account is located
Home Phone	Home phone of this contact
Office Phone	Office phone of this account
Mobile Phone	Mobile phone of this account
Email(s)	Email of this account
Homepage	Homepage of this contact
About Info	About info of this contact
Profile Created On Date/Time - (UTC)(yyyy-mm-dd)	The date when the profile was created
Profile Last Modified On Date/Time - (UTC)(yyyy-mm-dd)}	The date when the profile was last modified
Mood Text	Text used to express mood
Last Online On Date/Time - (UTC)(yyyy-mm-dd)	Last time the account was online
Last used On Date/Time - (UTC)(yyyy-mm-dd)	Last time the account was used
Avatar Timestamp Date/Time - (UTC)(yyyy-mm-dd)	Avatar created time
Image	Image for this contact

Skype Calls

Description	Information about Skype calls that occur between users.
Notes	

ATTRIBUTE	DESCRIPTION
Local Username	The user logged into Skype at the time of the call.
Call Initiator	The user who started the call.
Initiator Display Name	The display name of the user. This might be different from the username.
Recipient(s)	The users who accepted a call from the call initiator and participated in the call for a period of time.
Call Participants	The users who accepted and participated in the call from the call initiator for some duration.
Started Date/Time - UTC (yyyy-mm-dd)	Start time of the call.
Duration	Total duration of the Skype call.
Metadata	Additional details about the call extracted in XML format. This includes the duration of time each participant was in the call.

Skype Chat Messages

Description	Skype messages sent from one user to another.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	Profile name of the caller
Message Sent Date/Time - (UTC) (yyyy-mm-dd)	The date and time the message was sent
Author	Author of the message
From Display Name	The display name of who sent the message
Message	The body of the message or a description of the action taken. For example, adding another participant to a group chat or sharing a file or picture.
Attachment Name	The name of the attachment that was sent. This attribute is populated when the Message Type is POSTED_FILE or POSTED_PICTURE. Otherwise, this attribute is empty.
Attachment Size (Bytes)	The size of the attached file, in bytes. This attribute is populated when the Message Type is POSTED_FILE or POSTED_PICTURE. Otherwise, this attribute is empty.
Metadata	Additional details about the action, extracted in its original XML format.
Message Status	The status of the message.
Message Type	Type of message
Chat ID	ID of this chat
Recipient	Recipient of the chat

Skype Chatsync Messages

Description	Skype messages sent from one user to another that are parsed from the chatsync directory.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local user of this message
Chat Initiator	Initiator of the message
Chat Partner/Group Chat ID	the other part of this message
Message Type	Type of the message
Message Sent Date/Time - (UTC)(yyyy-mm-dd)	Date and time the message was sent

Skype Contacts

Description	Information about Skype contacts that are recovered, which may or may not be added contacts.
Notes	

ATTRIBUTE	DESCRIPTION
Profile Name	Profile name of the user
Skype Name	Skype name of the contact
Display Name	Display name of this account
Is Blocked	Is this contact blocked?
Contact Added	Specifies whether the contact is an added contact or just cached into the database (1 if the contact was added, 0 otherwise). Contacts can be cached into the database for a variety of reasons (for example, as a 'suggested contact').
Full Name	Full Name of this account
Birthday	Birthday of this accoutn
Gender	Gender of this account
City	City where this account is located
State/Province	State/Province this account is located
Country	Country this account is located
Home Phone	Home phone of this contact
Office Phone	Office phone of this account
Mobile Phone	Mobile phone of this account
PSTN Number	PSTN number of this contact
Email(s)	Email of this account

ATTRIBUTE	DESCRIPTION
Homepage	Homepage of this contact
About Info	About info of this contact
Profile Loaded Date/Time - (UTC)(yyyy-mm-dd)	Previously called "Profile Created On Date/Time", this attribute represents the date/time when a contact's profile is first created on the user's device. When the profile information is updated by the contact, the date in the database is also updated.
Mood Text	Text used to express mood
Last Online On Date/Time - (UTC)(yyyy-mm-dd)	Last time the account was online
Last used On Date/Time - (UTC)(yyyy-mm-dd)	Last time the account was used
Avatar Timestamp Date/Time - (UTC)(yyyy-mm-dd)	Avatar created time
Image	Image for this contact

Skype IP Addresses

Description	IP addresses that are associated with a Skype user account.
Notes	

ATTRIBUTE	DESCRIPTION
Username	Username of Skype accounts
IP Addresses	IP Addresses for the Skype user
IP Address Type	Type of IP address Local or Public
Date/Time - (UTC)(yyyy-mm-dd)	Date and time

Cloud

Android Dropbox

Description	Contains Dropbox file information recovered from a Kindle device.
Notes	

ATTRIBUTE	DESCRIPTION
File Path	The path to the file.
Updated File Name	The name of the file/folder being updated.
Local Modified Date/Time - UTC (yyyy-mm-dd)	Local date and time the file/folder was modified.
Updated Modified Date/Time - UTC (yyyy-mm-dd)	The updated date and time the file/folder was modified.
Displayed Modified Date/Time	The displayed modified date and time.
Local File Size (Bytes)	The size of the file on the local machine.
Updated File Size (Bytes)	The updated size of the file.
Favorited	States whether or not the file has been favorited.
File Version	The file version.

Android Dropbox Account Info

Description	Contains Dropbox account information recovered from a Kindle device.
Notes	

ATTRIBUTE	DESCRIPTION
Display Name	The Dropbox user account display name.
User ID	The Dropbox user account ID.
Country	The country the user account is set for.
Email	The email address associated with the account.

Documents

Excel Documents

Description	Microsoft Excel is a spreadsheet processor developed by Microsoft.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified on the filesystem.
Size (Bytes)	The size of the document in bytes.
Saved Size (Bytes)	The size of the document (in bytes) that was recovered. Extremely large documents may not be fully recovered.
File	The actual file.
Title	The title meta-data.
Subject	The subject meta-data.
Authors	The authors of the document.
Keywords	The keywords meta-data in the document.
Comments	The comments meta-data.
Last Author	The last author to edit the document.
Last printed Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last printed, extracted from meta-data within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last modified, extracted from meta-data within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the document was created, extracted from meta-data within the document.
Company	The company meta-data.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

PDF Documents

Description	Portable Document Format (PDF) is a file format used to present documents in a manner independent of application software, hardware, and operating systems. This table captures documents in this file format, extracted from the filesystem and carved from unallocated space.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified on the filesystem.
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
Title	The title of the file.
Subject	The subject of the file.
Authors	The authors of the file.
Keywords	The keywords in the metadata of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the document was created, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last modified, extracted from metadata within the document.
File	The PDF file.
MD5 Hash	An MD5 hash of the PDF content.
SHA1 Hash	A SHA1 hash of the PDF content.

PowerPoint Documents

Description	Micrsoft PowerPoint is a presentation creator developed by Microsoft. This table captures documents created with PowerPoint, extracted from the filesystem and carved from unallocated space.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified on the filesystem.
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
File	The actual file.
Title	The title of the file.
Subject	The subject of the file.
Authors	The authors of the file.
Keywords	The keywords in the metadata of the file.
Comments	The comments in the metadata of the file.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last modified, extracted from metadata within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the document was created, extracted from metadata within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

RTF Documents

Description	The information for each RTF document that was recovered from the search.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the RTF document.
File Size (Bytes)	The size of the RTF document in bytes.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the RTF document was created.

ATTRIBUTE	DESCRIPTION
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the RTF document was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the RTF document was last modified.
File Content	The contents of the RTF document.

Text Documents

Description	Text documents (.txt) that are located on the system.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the text document.
Size (Bytes)	The size of the text document in bytes.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The Date/Time that the text document was last modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The Date/Time that the text document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The Date/Time that the text document was created.

Word Documents

Description	Microsoft Word is a word processor developed by Microsoft.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified on the filesystem.
Size (bytes)	The size of the document.
Saved Size (bytes)	The size of the document that was recovered. Extremely large documents may not be fully recovered.
File	The actual file.
Title	The title meta-data.
Subject	The subject meta-data.

ATTRIBUTE	DESCRIPTION
Authors	The authors of the document.
Keywords	The keywords meta-data in the document.
Comments	The comments meta-data.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last printed extracted from meta-data within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last modified, extracted from meta-data within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the document was created, extracted from meta-data within the document.
Company	The company meta-data.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

E-mail

Android Emails

Description	Contains the email attributes that were recovered from an Kindle device.
Notes	

ATTRIBUTE	DESCRIPTION
Sync Server Date/Time - UTC (yyyy-mm-dd)	The date and time that the server synchronized the email.
Date/Time - UTC (yyyy-mm-dd)	Contains a date and time of the email.
Subject	The subject of the email.
Status	Identifies if the email was 'read' or 'unread'.
Sender	Who sent the email.
Recipients	Who the email was sent to.
CC	Who was CC'd on the email.
BCC	Who was BCC'd on the email.
Attachments	The attachments in the email.
Email Body	The body of the email

Android Gmail

Description	Contains the Gmail email fragments that were recovered from a Kindle device.
Notes	

ATTRIBUTE	DESCRIPTION
From Address	The sender of the email.
To Address(es)	The recipient(s) of the email.
cc Address(es)	The recipients of the email that were CC'd.
bcc Address(es)	The recipients of the email that were BCC'd.
Reply Address(es)	Reply-to address for the email.
Sent Date/Time - UTC (yyyy-mm-dd)	The date the email was sent.
Received Date/Time - UTC (yyyy-mm-dd)	The time the email was received.
Subject	The subject of the email.
Email Snippet	A snippet of the email.
Email Body	The body of the email.

Samsung Email Logs

Description	Contains the email logs that were recovered from an Kindle device.
Notes	

ATTRIBUTE	DESCRIPTION
Email Address	The email address of person/business the email is with.
Date/Time - UTC (yyyy-mm-dd)	Contains a date and time of the email.
Name	The name of the person/business the email is with.
Subject	The subject of the email.
Message Content	The email message content.

Media

Audio

Description	Audio files that are recovered that use the .mp3 or .wav formats.
Notes	For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
File Name	Name of the file.
File Extension	Extension of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the audio file was created.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the audio file was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the audio file was last modified.
File Size (Bytes)	The size of the audio file.
MD5 Hash	An MD5 hash of the audio content.
SHA1 Hash	A SHA1 hash of the audio content.

Carved Video

Description	Videos that are recovered using carving. Supported formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. Other container formats can also be recovered provided that their underlying packets are the same as one of the supported formats.
Notes	As of February 20 2020, this artifact will no longer be included under Videos. Carved Video functionality will be included in the 'Videos' artifact instead.

ATTRIBUTE	DESCRIPTION
Content Format	The format of the video.
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
File Size (Bytes)	The size of the container and file.
Container Format	The format of the video container.
Saved Video Size (Bytes)	The size of the video that was saved to the database.
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.

Pictures

Description	Pictures retrieved using either carving or parsing techniques. The supported formats are as follows: JPEG (.jpeg, .jpg, .jpe), PNG (.png), Bitmaps (.bmp), Graphics Interchange Format (.gif), Icons (.ico), and Tagged Image File Format (.tif, .tiff).
Notes	

ATTRIBUTE	DESCRIPTION
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date/time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date/time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date/time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. "Complete" indicates that a full Exif extraction was performed. "Partial" indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. "Failed" indicates that the information may have been corrupted and could not be recovered. "Skipped" indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).

ATTRIBUTE	DESCRIPTION
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
GPS Longitude	The GPS longitude coordinates of where the picture was taken (extracted from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
GPS Latitude	The GPS Latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS Latitude (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the pciture was taken (extracted from Exif data).
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Potential Original Media	Indicating if the media is likely the original source.
Category	An integer that indicates the Project VIC category for the picture.

Videos

Description	Videos that are recovered using parsing or carving. Supported formats for parsing include AVI, MP4, MOV, MPEG, DIVX, A3GP, ASF, WMV, DVR-MS, MKV, VOB, MOD, and WEBM. Supported carving formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. For more information about supported video formats, see Supported media and file types.
Notes	Supported formats include AVI, MP4, MOV, MPEG, DIVX, A3GP, ASF, WMV, DVR-MS, MKV, VOB, MOD, and WEBM. For information about supported formats, see Supported media and file types.

ATTRIBUTE	DESCRIPTION
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
File Name	Name of the file.
File Extension	Extension of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the video was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the video was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the video was last modified.
File Size (Bytes)	The size of the video.
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. "Complete" indicates that a full Exif extraction was performed, including potential metadata located at the end of the video. "Partial" indicates that only Exif information in the header section of the video file was recovered, which should only occur with very large videos (in excess of the limit set in the options screen). "Failed" indicates that the information may have been corrupted and could not be recovered. "Skipped" indicates that the extraction was skipped.
Media Duration (Seconds)	The duration of the video in seconds (extracted from Exif data).
Original Width	The resolution of the video (extracted from Exif data).
Original Height	The resolution of the video (extracted from Exif data).
Created Date/Time - Local Time	The local date and time when the video was first recorded (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the video was edited (extracted from Exif data).

ATTRIBUTE	DESCRIPTION
Timezone	The timezone setting on the camera at the time of the video being recored (extracted from Exif data).
Software	The software used to record or modify the video. This could either be the OS version of the phone used to record the video or name of the software used to edit the video in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to record the video (extracted from Exif data).
Model	The model of the camera used to record the video (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to record the video (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The GPS coordinates of the camera where the video was recorded (extracted from Exif data).
Longitude	The GPS coordinates of the camera where the video was recorded (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the video was recorded (extracted from Exif data).
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.
Content Format	The format of the carved video.
Container Format	The format of the carved video container.
Saved Video Size (Bytes)	The size of the carved video that was saved to the database.

Mobile

Android Kik Messenger Attachments

Description	Contains the attachments of messages from Kik Messenger from an Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Message ID	The ID of the message.

ATTRIBUTE	DESCRIPTION
Attachment	The attachment.
File Metadata	Any metadata from the file.

Android Kik Messenger Contacts

Description	Information about a user's Kik Messenger contacts.
Notes	

ATTRIBUTE	DESCRIPTION
Contact ID	The ID of the contact.
Display Name	The display name of the contact.
Local Name	The local name of the person on the device.
User Name	The user name of the contact.
Photo URL	The URL to the profile photo of the contact.
Photo Timestamp Date/Time - UTC (yyyy-mm-dd)	The time stamp of the contacts profile photo.
Group Member	Indicates whether the contact is a member of a group (Yes or No).
Is User Blocked	Indicates whether the contact is blocked by the local user.

Android Kik Messenger Messages

Description	Kik Messenger messages sent or received by the local user.
Notes	

ATTRIBUTE	DESCRIPTION
Local User	The local user of the device where the data was recovered from.
Partner	The person the local user sent a message to or received a message from.
Message Timestamp Date/Time - UTC (yyyy-mm-dd)	The time stamp of the message.
Message Body	The body of the message.

ATTRIBUTE	DESCRIPTION
Message Status	The status of the message (possible values are 'Trying to establish connection', 'Message has been sent to recipient, 'Message has been delivered to recipient', 'Message has been read by recipient' and 'Unknown message status').
Message Type	The type of message. Possible values are 'Message Received', 'Message Sent' and 'Unknown Message Type'.
Attachment	The attachment sent with the message.

SIM Card ICCID

Description	SIM Card ICCID contains the ICCID number that identifies the device's SIM card.
Notes	

ATTRIBUTE	DESCRIPTION
ICCID	The integrated circuit card identifier.

SIM Card IMSI

Description	SIM Card IMSI contains IMSI numbers used to identify the mobile subscriber, as recovered from the SIM card.
Notes	

ATTRIBUTE	DESCRIPTION
IMSI	The international mobile subscriber identity.

SIM Card Phone Numbers

Description	SIM Card Phone Numbers contains records of all the phone numbers saved to the device SIM card. The type of number is indicated by the record type.
Notes	

ATTRIBUTE	DESCRIPTION
Phone Number	The phone number for the specific record type.

ATTRIBUTE	DESCRIPTION
Record Type	Identifies the type of record the phone number is. Can be 'Abbreviated dialing numbers(ADN)', 'Emergency call codes (ECC)', 'Last number dialed (LND)', 'MSISDN', 'Service dialing numbers (SDN)', or 'Fixed dialing numbers (FDN)'

SIM Card Service Providers

Description	SIM Card Service Providers contains the names of mobile service providers that the device has connected with, and which are recovered from the SIM card.
Notes	

ATTRIBUTE	DESCRIPTION
Service Provider Name	The identity of the mobile phone service provider.

SIM Card SMS Messages

Description	SIM Card SMS Messages contains messages sent or received by the local user which were saved to the SIM card.
Notes	

ATTRIBUTE	DESCRIPTION
Sender	The sender of the SMS message.
Recipient	The recipient of the SMS message.
Message Date/Time	For incoming messages, this timestamp indicates when the message was received by the mobile service center. For outgoing messages, there is no data available for this field.
Message	The message body of the SMS message.
Deleted	Identifies whether the message has been deleted. Can be 'Yes' or 'No'
Message Status	Identifies whether the message has been read, unread, draft or sent.
SMSC	The short message service center number.

Operating System

.DS_Store Records

Description	.DS_Store Records contains all the records extracted from .DS_Store files found on the computer. Each record represents a property of a file or a folder. The significance of this artifact is an indicator of high likelihood that the user of the computer was aware of these files and folders with a possibility of attributing a date to that awareness.
Notes	In the Apple macOS operating system, .DS_Store (Desktop Services Store) is a hidden file that stores the display information of its containing folder, similar to the file desktop.ini in Microsoft Windows. The file tracks information such as icon positions, view settings, cached file size, cached last modified date, and even the choice of a background image. The .DS_Store is created and maintained by the Finder application in any folder that it accesses, even on remote file systems mounted from servers that share files (for example, via Server Message Block (SMB) protocol or the Apple Filing Protocol (AFP)). .DS_Store files are also included in archives created by macOS users, such as ZIP files, and they are backed up by some cloud file backup services. This means that the presence of .DS_Store Records artifacts on non-Mac evidence such as Windows, Mobile, or Cloud indicates that some of the data may have originated or have been accessed from a macOS computer at some point. For more information on .DS_Store files and their forensic significance see: .DS_Stores: Like Shellbags but for Macs.

ATTRIBUTE	DESCRIPTION
Record Name	The name of the file or folder as stored in the .DS_Store file.
Record Type	The type of the record, or property, that is being logged in the .DS_Store file for a particular file or folder.
Record Value	The value of the property for the given file or folder.
Record Path	The full path to the file or folder
.DS_Store Created Date/Time - UTC (yyyy-mm-dd)	The created date of the .DS_Store file from which the record was extracted.
.DS_Store Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date of the .DS_Store file from which the record was extracted.
.DS_Store Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date of the .DS_Store file from which the record was extracted.

Accounts Information

Description	Contains the login information for all accounts on the Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Username	The username associated with the account.
Package Name	The name of the application as the device sees it.
Password	The password stored on the device to connect to the account.
Last Login Date/Time - UTC (yyyy-mm-dd)	The UTC Date/Time of the last successful login.

Android Downloads

Description	Contains file download information from a recovered Android device.
Notes	

ATTRIBUTE	DESCRIPTION
Download Source	The URL of the file that was downloaded.
Save Location	Absolute path on the device to the file downloaded.
Last Modified Date/Time - UTC (yyyy-mm-dd)	Date and time the file was last modified.
Notification Package	Android package name the download was initiated in.
Bytes Downloaded	The bytes that were downloaded.
Total Bytes	The total bytes of the file.

File Signature Mismatch (Audio)

Description	File Signature Mismatch (Audio) contains identified mismatches between a known file signature header and the extension (or lack thereof) for an audio file. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.

File Signature Mismatch (Container)

Description	File Signature Mismatch (Container) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a container. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.

File Signature Mismatch (Document)

Description	File Signature Mismatch (Document) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a document. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.

File Signature Mismatch (Picture)

Description	File Signature Mismatch (Picture) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a picture. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file. If the mime type is unknown, this defaults to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file. If the mime type is unknown, this defaults to application/octet-stream. If there is no file extension, but the mime type is known, a mismatch is is returned.
File Path	The path to the mismatched file.

File Signature Mismatch (Video)

Description	File Signature Mismatch (Video) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a video. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.

File System Information

Description	Contains all of the relevant information about the hard drives in use by the operating system.
Notes	

ATTRIBUTE	DESCRIPTION
Volume Serial Number	This field only applies to FAT and NTFS file systems. This is a 32-bit unsigned int value that is stored in Bios Paramter Block (BPB) and is showed in a special hex format – XXXX-XXXX e.g. EABB-6573. For other file systems, the value of this field should show "n/a".
Full Volume Serial Number	This field is a 64-bit volume serial number that is only present in BPB of NTFS file system, for example AABBCCDDEEFF0011. For non-NTFS file systems, "n/a" is displayed for this field.
File System	Shows the type of the file system, e.g "Microsoft NTFS".
Sectors per cluster	The number of sectors in a file system cluster, e.g. 8.
Bytes per sector	The amount of bytes per sector.
Starting Sector	The starting sector for this partition.
Ending Sector	The ending sector for this partition.
Total Sectors	Encase shows different values for this field based on how a volume is added to the case. For example, if you add just a volume (e.g. your local C:\ drive), it shows 123410271 for the number of sectors, but if you add your local physical drive 0 to the case and then select your C:\ volume in the "Entries" tree (note: your C drive would most likely have another letter in this tree, e.g. E:), then total number of sectors would be one more that the other value, i.e. 123410272. the value show for this field is taken from BPB, which matches the first value. The other value is shown when the parent physical drive is present probably comes from the partition table, and it counts VBR as well.
Total Capacity (Bytes)	This value is calculated by (Total Clusters) x (Cluster Size), which shows the capacity of the file system and not the volume containing it. The size of the volume would be higher than this value.
Total Clusters	The number of clusters comprising the file system.
Unallocated Area (Bytes)	Number of unallocated bytes on the file system, which is calculated by (Number of free clusters) x (cluster size).
Free Clusters	Number of unallocated clusters in the file system.
Allocated Area (Bytes)	(Number of allocated clusters) x (cluster size).

ATTRIBUTE	DESCRIPTION
Volume Name	This is the volume label stored in Volume Boot Record (VBR).
Volume Offset (Bytes)	The offset (in bytes) of the volume containing this file system from beginning of the disk. "0" is displayed if the image and/or drive being searched is the image of one volume. Encase shows the number of sectors for this field instead of the number of bytes.
ID	The identifier of the hard drive.
Drive Type	The type of the hard drive.

Social Networking

Android Instagram Posts

Description	The posts that a user has put onto Instagram.
Notes	

ATTRIBUTE	DESCRIPTION
ID	The post ID.
Full Name	The full name of the user.
Profile Picture URL	The URL to the profile picture of the user.
Downloaded Profile Image	The downloaded profile picture.
User Name	The user name on Instagram.
Posted Image URL	The URL to the image that was posted.
Downloaded Posted Image	
Text	The text for the given image.
Created Date/Time - UTC (yyyy-mm-dd)	The date the image was created.
Taken Date/Time - UTC (yyyy-mm-dd)	The date the image was taken.
Device Date/Time - UTC (yyyy-mm-dd)	

Android Instagram Users

Description	The posts that a user has put onto Instagram.
Notes	

ATTRIBUTE	DESCRIPTION
ID	The ID of the user.
Full Name	The full name of the user.
Profile Picture URL	The URL to the profile picture of the user.
Downloaded Profile Image	The downloaded profile picture.
User Name	The user name on Instagram.

Android Sina Weibo Posts

Description	Sina Weibo posts, recovered from a device.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The Sina Weibo user ID.
User Nickname	The users Sina Weibo nickname.
Profile Image URL	The URL to the users profile image.
Downloaded Profile Image	
Post	Text that the user has posted.
Post Date/Time - UTC (yyyy-mm-dd)	The date and time the user made the post.
Post Image URL	Contains the URL to an image that was posted.
Downloaded Post Image	
Posted Source	Contains the source of the post.
Longitude	The longitude of the poster.
Latitude	The latitude of the poster.

Android Sina Weibo Private Messages

Description	Sina Weibo posts, recovered from a device.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The Sina Weibo user ID.
Recipient Nickname	The recipient's Sina Weibo nickname.
Profile Image URL	The URL to the users profile image.
Downloaded Profile Image	

ATTRIBUTE	DESCRIPTION
Message	The text that the user has sent as a message.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time the user sent the message.
Attachment Type	The MIME type of the attachment.
Attachment Local File Path	The path to the attachment on the device.

Facebook

Facebook, being one of the most popular social networking sites in the world, presents numerous opportunities for gathering evidence. You can recover messages that are sent and received, status updates and wall posts, and pages and pictures that the user views. On mobile devices, you can also recover user profiles and contacts.

Facebook can provide background information about a user, as well as evidence of who they are communicating with or associated with. Status and location updates can provide details about where a user has been and what they've been doing.

FORENSIC NOTES

The Facebook Pictures artifact represents cached pictures found on the system that originated from Facebook. When caching pictures, Facebook names the pictures using a particular format which allows forensic tools to know that they come from Facebook. These pictures can be user profile pictures, friends' pictures, or any other picture that gets cached while browsing Facebook.

ARTIFACTS

RELATED RESOURCES

How important are Facebook artifacts?

Recovering Facebook artifacts

Android Facebook Pictures

Description	Facebook pictures that are recovered from the device.

Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the Facebook picture.
Filename	The file's absolute path on the device.
Image	The picture that was recovered.

Facebook Contacts

Description	Contact information stored by the Facebook app.
Notes	

ATTRIBUTE	DESCRIPTION
Profile ID	The Facebook profile ID of the contact.
First Name	The Facebook contact's first name.
Last Name	The Facebook contact's last name.
Display Name	The Facebook contact's display name.
Small Picture URL	The URL to the the small picture.
Big Picture URL	The URL to the big picture.
Huge Picture URL	The URL to the huge picture.
Phone Numbers	The contact's phone numbers.

Facebook User/Friends

Description	Profile information for the Facebook user and friends recovered from the device.
Notes	

ATTRIBUTE	DESCRIPTION
Friend/User	Indicates if the information is for the user or a friend.
User ID	The user ID of the user/friend.
First Name	The first name of the user/friend.
Last Name	The last name of the user/friend.
Display Name	The display name of the user/friend.
User Image URL	The URL to the user/friends profile picture.
Image	The profile picture.

ATTRIBUTE	DESCRIPTION
Phone Number	The user/friends phone number.
Other	
Email(s)	The user/friends email address(es).
Birthday (MM/DD/YYYY)	The user/friends birthday.

Twitter Tweets

Description	Carved and noncarved tweets from the Twitter app.
Notes	

ATTRIBUTE	DESCRIPTION
Author ID	The numeric ID of the account that posted the tweet.
Status ID	The unique ID of the tweet.
Created Date/Time - UTC (yyyy-mm-dd)	The Date/Time at which the tweet was created.
Tweet	The text content of the tweet.
Tweet Source	The interface used to post the tweet.
Favorited	Whether the tweet has been favorited.
Latitude	The latitude of the location from which the tweet was posted.
Longitude	The longitude of the location from which the tweet was posted.
Retweet Count	The number of times the tweet has been re-tweeted.

Twitter Users

Description	Contains friend information in Twitter data.
Notes	

ATTRIBUTE	DESCRIPTION
User ID	The friend's twitter user ID.
User Name	The friend's twitter username.
Profile Created Date/Time - UTC (yyyy-mm-dd)	The date and time the friend's Twitter profile was created.
Description	Short profile description the friend puts about themselves.
Web URL	The friend's website URL.

ATTRIBUTE	DESCRIPTION
Following	'Yes' if the local user is following this account, 'No' otherwise. If this attribute is empty, it's undetermined whether the local user is following this account.
Location	The location the friend is from.
Protected	
Followers	The number of followers the friend has.
Friends	The number of friends the friend has.
Statuses	The number of different status the friend has had.
Image URL	The URL to the friend's profile picture.
Friend Metadata Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the friend's meta information was last updated.
Header URL	The URL to the friend's profile banner picture.

Web Related

Google Analytics First Visit Cookies

Description	Information about Google Analytics first-visit cookies that are discovered in other artifacts.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the URL.
Creation DateTime	Date/Time when the site was vist visited.
Most Recent Visit Date/Time	Date/Time of most recent session.
2nd Most Recent Visit Date/Time	Date/Time of previous session.
Hits	Number of visit.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Google Analytics First Visit Cookies Carved

Description	Information about Google Analytics first-visit cookies that are recovered using carving.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the URL.
Creation DateTime	Date/Time when the cookie was created.
Most Recent Visit Date/Time	Date/Time of most recent session.
2nd Most Recent Visit Date/Time	Date/Time of previous session.
Hits	Number of visit.

Google Analytics Referral Cookies

Description	Information about Google Analytics referral cookies that are discovered in other artifacts.
Notes	

ATTRIBUTE	DESCRIPTION
Cookie Source	The source URL used to reach the site.
Host	Contains the domain of the URL.
Update Date/Time	The last time the cookie was updated.
Campaign	The method of referral.
Access Method	Whether the site was accessed organically or was referred.
Keyword	Keywords used to arrive at the site.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Google Analytics Referral Cookies Carved

Description	Information about Google Analytics referral cookies that are recovered using carving.
Notes	

ATTRIBUTE	DESCRIPTION
Cookie Source	The source URL used to reach the site.
Host	Contains the domain of the URL.
Update Date/Time	The last time the cookie was updated.
Campaign	The method of referral.
Access Method	Whether the site was accessed organically or was referred.
Keyword	Keywords used to arrive at the site.

Google Analytics Session Cookies

Description	Information about Google Analytics session cookies that are discovered in other artifacts.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the URL.
Page Views	The number of visits to this page from the user.
Start Current Session Date/Time	The start time of the current sesion.
Outbound Link Events Left	
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Google Analytics Session Cookies Carved

Description	Information about Google Analytics session cookies that are recovered using carving.
Notes	

ATTRIBUTE	DESCRIPTION
Host	Contains the domain of the URL.
Page Views	The number of visits to this page from the user.
Start Current Session Date/Time	The start Date/Time of the current sesion.
Outbound Link Events Left	

Google Analytics URLs

Description	URLs that are discovered in other artifacts that are related to Google Analytics.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the web site. If the url cannot be recovered, the source of the url containing all the metadata is displayed instead.
Page Title	The name of the web site. This value is carved from the source starting after 'utmdt=' and ending at '&'

ATTRIBUTE	DESCRIPTION
Host Name	Contains the domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Google Analytics URLs Carved

Description	Information about Google Analytics URLs that are recovered using carving.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the web site. If the url cannot be recovered, the source of the url containing all the metadata is displayed instead.
Page Title	The name of the web site. This value is carved from the source starting after 'utmdt=' and ending at '&'
Host Name	Contains the domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'

Google Maps

Description	Google maps is a free web service that allows users to get directions.
Notes	

ATTRIBUTE	DESCRIPTION
Search Query	The term that was searched for
Starting Location	The starting location for navigation/directions.
Center of Map	Where the map was centered
Business Latitude and Longitude	The latitude and longitude of the business location.

ATTRIBUTE	DESCRIPTION
Source Address	The source physical address.
Destination Address	The user's desired destination
Route Type	How the user will travel (eg. Car, bus, bike)
Additional Address	Any additional addresses within the navigation
Street View Latitude/Longitude	The latitude and longitude information in street view.

Google Maps Tiles

Description	Google maps is a free web service that allows users to get directions.
Notes	

ATTRIBUTE	DESCRIPTION
Image	The actual picture content.
X Coordinate	The X coordinate value that Google uses to download the right tile.
Y Coordinate	The Y coordinate value that Google uses to download the right tile.
Zoom Level	The level that the user was zoomed in to the map. Can be understood as the Z coordinate value that Google uses to download the right tile.

Kindle Silk Web History

Description	Contains the browsing history from the Silk web browser recovered from a Kindle device.
Notes	

ATTRIBUTE	DESCRIPTION
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time which the URL was last visited.
URL	The URL that was recorded in the web history for Silk.
Title	The title that the web page displayed.
Visit Count	The number of visits to the web page using the Silk browser.
Is Bookmarked	Whether or not the URL has been bookmarked in the browser.
Is Favorited	Whether or not the URL has been favorited in the browser.

Malware/Phishing URLs

Description	Records that are believed to be either malware or phishing related URLs.

Notes	

ATTRIBUTE	DESCRIPTION
Site Name	The name of the web site.
URL	The URL of the web site.
Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the artifact.
Artifact	The name of the artifact the URL belongs to.
Artifact ID	The row Id of the URL in the original artifact table.

Pornography URLs

Description	Records that are believed to be pornography related URLs.
Notes	You can find a list of the domains that are supported by this refined result at Pornography URLs.

ATTRIBUTE	DESCRIPTION
Site Name	The name of the web site.
URL	The URL of the web site.
Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the artifact.
Artifact	The name of the artifact the URL belongs to.
Artifact ID	The row Id of the URL in the original artifact table.

REFINED RESULTS

Media

Potential Facebook Pictures

Description	Any cached pictures that are recovered that potentially originate from Facebook.
Notes	

ATTRIBUTE	DESCRIPTION
File Name	The name and extension of the file the picture came from.
Image	The actual picture content.
Size (Bytes)	The size of the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Potential Profile ID or Picture ID	The potential Facebook profile ID or picture ID.
Tags	The tags associated with the picture content.
Skin Tone Percentage	The percentage of the picture that is likely to be skin tone.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the picture was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the picture was last accessed.
MD5 Hash	The MD5 hash of the picture content.
SHA1 Hash	The SHA1 hash of the picture content.
PhotoDNA Hash	The PhotoDNA hash of the picture content.
Category	The category that the picture is assigned if known hashes were loaded for categorization.
Artifact	The artifact the picture is from.
Artifact ID	The ID of the artifact where the picture comes from.

Refined Results

Classifieds URLs

Description	Contains all of the URLs that are associated with classifieds websites.
Notes	You can find a list of the domains that are supported by this refined result at Classifieds sites domains.

ATTRIBUTE	DESCRIPTION
Site Name	The name of the classifieds website.
URL	The URL of the classifieds website.
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Artifact	The artifact the classifieds URL is from.
Artifact ID	The ID of the artifact where the classifieds URL comes from.

Cloud Passwords and Tokens

Description	Cloud passwords and tokens that are found on the system. These accounts and their corresponding tokens can be used to acquire more evidence from the cloud.
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The user name for the cloud account.
Password/Token	The password/token for the cloud account.
Platform	The application/platform for which the account is used (e.g. Facebook, Twitter, Google, etc).
Artifact	The artifact the cloud account is from.
Artifact ID	The ID of the artifact where the cloud account comes from.

Cloud Service URLs

Description	Contains all of the URLs that are associated with cloud service websites.
Notes	You can find a list of the domains that are supported by this refined result at Cloud service domains.

ATTRIBUTE	DESCRIPTION
Site Name	The name of the cloud service website.
URL	The URL of the cloud service website.
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Artifact	The artifact the cloud service URL is from.
Artifact ID	The ID of the artifact where the cloud service URL comes from.

Dating Sites URLs

Description	Contains all of the URLs that are associated with dating sites websites.
Notes	You can find a list of the domains that are supported by this refined result at Dating site domains.

ATTRIBUTE	DESCRIPTION
Site Name	The name of the dating sites website.
URL	The URL of the dating sites website.
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Artifact	The artifact the dating sites URL is from.
Artifact ID	The ID of the artifact where the dating sites URL comes from.

Email Attachments

Description	Email Attachments contains any information about email attachments that have been discovered within other recovered artifacts.
Notes	

ATTRIBUTE	DESCRIPTION
Subject	The subject of the email.
File Name	The name of the attachment.
File Extension	The extension of the attachment.
Created Date/Time	The date and time that the attachment was originally created.
Accessed Date/Time	The date and time that the attachment was last accessed.
Modified Date/Time	The date and time that the attachment was last modified.
MD5 Hash	An MD5 hash of the attachment.

ATTRIBUTE	DESCRIPTION
SHA1 Hash	A SHA-1 hash of the attachment.
Skin Tone Percentage	The percentage that appears to be visible skin (if the attachment is a picture or video).
To Address(es)	The recipient(s) of the email.
From Address	The sender of the email.
Email Timestamp Date/Time	The date of the email. This field can mean different things to different email hits, so we have not defined what this column actually means.
CC	The recipients that receive the email by CC.
BCC	The recipients that receive the email by BCC.

Facebook URLs

Description	Contains all of the URLs that are associated with facebook websites.
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the facebook website.
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Potential Activity	The activity that may have been performed at the URL.
Artifact	The artifact the facebook URL is from.
Artifact ID	The ID of the artifact where the facebook URL comes from.

Google Searches

Description	Contains all of the URLs that are associated with the google search engine.
Notes	

ATTRIBUTE	DESCRIPTION
Search Term	The string that was searched.
URL	The URL of the google search.
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Original Search Query	The query at the start of the search session.
Search Session Start Date/Time - (UTC) (yyyy-mm-dd)	The date and time when the search session started. This fragment originates from the 'ei' value in the search URL.

ATTRIBUTE	DESCRIPTION
Previous Page Load Date/Time - (UTC) (yyyy-mm-dd)	The date and time when the page prior to the returned search result was loaded. This fragment originates from the 'sxsrf' value in the search URL.
Page Load Date/Time - (UTC) (yyyy-mm-dd)	The date and time when the returned search page was loaded. This fragment originates from the 'ved' value in the search URL.
Web Page Title	The title of the web page.
Previous Queries	Other queries that were searched during the search session.
Artifact	The artifact the URL is from.
Artifact ID	The ID of the artifact where the URL comes from.

Google Translate

Description	Contains all of the translations done using google translate.
Notes	

ATTRIBUTE	DESCRIPTION
Language Translated From	The original language of the translation string.
Language Translated To	The language the translation string was translated to.
Translation String	The string that was translated.
Date/Time - (UTC) (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Artifact	The artifact the URL is from.
Artifact ID	The ID of the artifact where the URL comes from.

Human Trafficking Site URLs

Description	Identifies any URLs that are affiliated with escort services which is often associated to human trafficking operations. Many classified ad sites also provide escort services but the primary purpose of the sites in this list are providing escort services.
Notes	You can find a list of the domains that are supported by this refined result at Human Trafficking sites.

ATTRIBUTE	DESCRIPTION
URL	The URL of human trafficking/escort site.
Site Name	The name of the site.

ATTRIBUTE	DESCRIPTION
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Date/Time - Local Time (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Artifact	The artifact the URL comes from
Artifact ID	The ID of the artifact where the human trafficking/escort URL comes from.

Identifiers

Description	Contains all of the IDs of the people that are found on the system.
Notes	

ATTRIBUTE	DESCRIPTION
Identifier	The ID of the person.
Column Name	The column where the ID is discovered.
Artifact	The artifact the ID comes from
Artifact ID	The ID of the artifact where the identifier comes from.

Identifiers - Device

Description	Contains all of the IDs of the unique devices that are found on the system.
Notes	

ATTRIBUTE	DESCRIPTION
Identifier	The ID of the device.
Column Name	The column where the ID is discovered.
Artifact	The artifact the ID comes from
Artifact ID	The ID of the artifact where the identifier comes from.

Identifiers - People

Description	Contains all of the IDs of the people that are found on the system.
Notes	

ATTRIBUTE	DESCRIPTION
Identifier	The ID of the person.
Column Name	The column where the ID is discovered.
Artifact	The artifact the ID comes from
Artifact ID	The ID of the artifact where the identifier comes from.

Locally Accessed Files and Folders

Description	Locally Access Files and Folders is a refined result that contains information about local and network resources that have been accessed by the user.
Notes	This refined result is primarily sourced from Windows IE WebCache. Windows Explorer and Internet Explorer are tightly coupled together, which allows us find Windows Explorer history in the IE Web Cache.

ATTRIBUTE	DESCRIPTION
Path	The path to the file or folder being accessed, which might be located on a drive or on the network.
Path Type	The type of path to the file or folder. 'Drive' indicates that the accessed resource was located on a locally mounted drive, a mapped network drive, or an attached USB drive. 'Network' indicates that the accessed resource was located on the network. 'Virtual' indicates that the resource may have been accessed using a shortcut like 'Windows Explorer' from the task bar, 'Win+E', 'F1', or a scripted event during a 3rd party program execution.
Accessed Date/Time - UTC (yyyy-mm-dd)	The last recorded date that the resource was accessed.
Accessed Date/Time - Local time (yyyy-mm-dd)	The last recorded date that the resource was accessed.
User	The local user on the system.
Access Count	The number of times the resource was accessed.
Artifact	The type of artifact where this refined result was recovered from.
Artifact ID	The ID of the individual artifact hit where this refined result was recovered from.

Parsed Search Queries

Description	Contains all of the URLs that are associated with search engines, Google excepted.
Notes	You can find a list of the domains that are supported by this refined result at Parsed Search Queries domains.

ATTRIBUTE	DESCRIPTION
Search Term	The string that was searched.
URL	The URL of the search.
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Search Engine	The search engine used to perform the search.
Google Original Search Query	The query at the start of the search session.
Web Page Title	The title of the web page.
Artifact	The artifact the URL is from.
Artifact ID	The ID of the artifact where the URL comes from.

Passwords and Tokens

Description	Passwords and Tokens is a refined result that collects passwords and tokens that are associated with user accounts. This refined results only applies to accounts recovered from mobile and computer sources. For accounts that are recovered from cloud sources, see Cloud Passwords and Tokens).
Notes	

ATTRIBUTE	DESCRIPTION
User Name	The user name associated with the account.
Password/Token	The password/token for the account.
Service	The application/website for which the account is used.
Artifact	The artifact where the account is recovered from.
Artifact ID	The ID of the artifact where the account is recovered from.

Potentially Unwanted Apps

Description	Records that are believed to be potentially unwanted, or spyware, applications.
Notes	You can find a list of the domains that are supported by this refined result at Potentially unwanted applications.

ATTRIBUTE	DESCRIPTION
Application Name	The name of the application.
Package Name	The name of the package.
Artifact	The name of the artifact the potentially unwanted application belongs to.
Artifact ID	The row Id of the potentially unwanted application in the original artifact table.

Shipping Site URLs

Description	Contains all of the URLs that are associated with shipping websites.
Notes	You can find a list of the domains that are supported by this refined result at Shipping site domains.

ATTRIBUTE	DESCRIPTION
Site Name	The name of the shipping website.
URL	The URL of the shipping website.
Tracking Number	The tracking number associated with the URL.
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Artifact	The artifact the shipping website URL is from.
Artifact ID	The ID of the artifact where the shipping website URL comes from.

Social Media URLs

Description	Contains all of the URLs that are associated with social media websites.
Notes	You can find a list of the domains that are supported by this refined result at Social media domains.

ATTRIBUTE	DESCRIPTION
Site Name	The name of the social media website.
URL	The URL of the social media website.
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Artifact	The artifact the social media URL is from.
Artifact ID	The ID of the artifact where the social media URL comes from.

Tax Site URLs

Description	Contains all of the URLs that are from a list of websites approved by IRS tax forms.
Notes	You can find a list of the domains that are supported by this refined result at Tax site domains.

ATTRIBUTE	DESCRIPTION
Site Name	The name of the tax website.
URL	The URL of the tax website.
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Artifact	The artifact the URL comes from
Artifact ID	The ID of the artifact where the tax website URL comes from.

Tor URLs

Description	Identifies any .onion sites access via Tor or Tor proxy
Notes	

ATTRIBUTE	DESCRIPTION
URL	The URL of the Tor/Onion site.
Site Name	The name of the site.
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Date/Time - Local Time (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Artifact	The artifact the URL comes from
Artifact ID	The ID of the artifact where the Tor URL comes from.

Torrent URLs

Description	Contains all of the URLs that are associated with torrent websites.
Notes	You can find a list of the domains that are supported by this refined result at Torrent site domains.

ATTRIBUTE	DESCRIPTION
Site Name	The name of the torrent website.
URL	The URL of the torrent website.

ATTRIBUTE	DESCRIPTION
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Artifact	The artifact the torrent URL is from.
Artifact ID	The ID of the artifact where the torrent URL comes from.

Web Chat URLs

Description	Contains all of the URLs that are associated with web chat websites.
Notes	You can find a list of the domains that are supported by this refined result at Web chat domains.

ATTRIBUTE	DESCRIPTION
Site Name	The name of the web chat website.
URL	The URL of the web chat website.
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Artifact	The artifact the web chat URL is from.
Artifact ID	The ID of the artifact where the web chat URL comes from.

LEARN MORE ABOUT ARTIFACTS

Parsing and carving

Parsing is a method of interpreting structured information. Magnet AXIOM can parse videos, pictures, and other documents when it encounters a file with a known extension and format. And, for applications that store their data in the known structure (like a SQLite database), Magnet AXIOM can parse the information from the database into meaningful artifacts.

Carving involves searching raw data to identify headers or other patterns. For example, when a scan identifies the following stream of bytes xFF xD8 xFF[xC0 xC4 xDB xE0- xE3 xE8 xEA xEE xFE], this signifies the beginning of a .jpg picture and is what allows Magnet AXIOM to recover artifacts even when they're recovered from unallocated space. However, carving does not necessarily indicate that the data came from unallocated space – carved artifacts can come from anywhere.

Parsing almost always recovers more data about an item than with carving. Carved results often don't include metadata about a file, such as datestamps and file locations that parsing otherwise recovers.

Supported media and file types

Magnet AXIOM can recover many different file and media types. This section highlights the artifacts that contain file and media content, identifies the file types that each artifact supports, and indicates whether Magnet AXIOM can parse or carve each type.

Videos

Magnet AXIOM can supports a number of different video container formats, using both parsing and carving, and displays results in the Videos artifact. For information about what it means for a file to be parsed or carved, see Parsing and carving.

TYPE	EXTENSION	PARSING SUPPORT	CARVING SUPPORT
Audio Video Interleave	.avi	Yes	Yes
DivX	.divx	Yes	No
Matroska	.mkv	Yes	No
MPEG-1, MPEG-2	.mpg, .mpg1, .mpg2, .mpeg, .mpeg1, .mpeg2, .m2v, .m2p, .mod, .vob	Yes	Yes
MPEG-4	.mp4, .mp4v, .f4v, .lrv, m4v	Yes	Yes
QuickTime	.3gp	Yes	Yes
	.3ga	Yes	No
	.3g2	Yes	No
	.m4a, .m4p	Yes	No
	.mov	Yes	Yes
	.qt	No	Yes

TYPE	EXTENSION	PARSING SUPPORT	CARVING SUPPORT
WebM	.webm	Yes	No
Windows Media Video	.wmv, .wm, .asf, .dvr-ms	Yes	Yes

Pictures

Any pictures that Magnet AXIOM recovers are reported in the Pictures artifact. This artifact uses both parsing and carving techniques to recover a range of different picture formats. Magnet AXIOM can also recover many different types of RAW picture formats which are typically used with cameras.

TYPE	EXTENSION	PARSING SUPPORT	CARVING SUPPORT
BMP	.bmp	Yes	Yes
	.dib	Yes	Yes
JPEG	.jpg	Yes	Yes
	.jpe	Yes	Yes
	.jpeg	Yes	Yes
GIF	.gif	Yes	Yes
HEIC	.heic	Yes	No
HEIF	.heif	Yes	No
ICO	.ico	Yes	No
iThmb	.ithmb	Yes	No
PNG	.png	Yes	Yes
TIFF	.tiff	Yes	Yes

Raw pictures

EXTENSION	PARSING SUPPORT	CARVING SUPPORT
.3fr	Yes	No
.arw	Yes	No
.cr2	Yes	No
.crw	Yes	No
.dcr	Yes	No
.dng	Yes	No
.erf	Yes	No
.k25	Yes	No
.kdc	Yes	No
.mef	Yes	No
.raw	Yes	No
.rw2	Yes	No
.sr2	Yes	No
.srf	Yes	No
.x3f	Yes	No
.tif	Yes	Yes
.tiff	Yes	Yes

Audio

The Audio artifact contains the MP3 and WAV files that are recovered during a scan. On mobile devices, the AMR Files artifact contains voicemail messages.

TYPE	EXTENSION	PARSING SUPPORT	CARVING SUPPORT
AMR	.amr	No	Yes
MP3	.mp3	Yes	Yes
WAV	.wav	Yes	No

Documents

Documents are recovered in the following artifacts: Calc Documents , CSV Documents , Excel Documents , Hangul Word Processor , Impress Documents , PDF Documents , PowerPoint Documents , RTF Documents , Text Documents , Word Documents , Writer Documents .

TYPE	EXTENSION	PARSING SUPPORT	CARVING SUPPORT
CSV	.csv	Yes	No
Hangul Word	.hml .hwpx .hwp .hwt	Yes	Yes

TYPE	EXTENSION	PARSING SUPPORT	CARVING SUPPORT
Microsoft Excel	.xlm .xls .xlsx .xlt .xltx .xlsm	Yes	Yes
Microsoft PowerPoint	.pot .potm .potx .ppam .pps .ppsm .ppsx .ppt .pptm .pptx .sldm .sldx	Yes	Yes
Microsoft Word	.doc .docm .docx .dot .dotx .dotm	Yes	Yes

TYPE	EXTENSION	PARSING SUPPORT	CARVING SUPPORT
Open Office Calc	.odf .odf .sxc .stc	Yes	Yes
Open Office Impress	.odp .otp .sxi .sti	Yes	Yes
Open Office Writer	.odm .odt .ott .swx .stw	Yes	Yes
PDF	.pdf	Yes	Yes
RTF	.rtf	Yes	Yes
Text	.txt	Yes	No

Magnet Forensics

156 Columbia Street West, Unit #2, N2L 3L3

Waterloo, ON, N2L 3L3

1 (519) 342-0195