MAGNET AXIOM™

USER GUIDE

MAGNET FORENSICS®

CONTENTS

What's new 13

Getting started with Magnet AXIOM 16

Building your case in Magnet AXIOM 16

Acquiring mobile evidence 20

Acquiring an Android device 21

Access to data on Android devices 21

Supported acquisition methods for Android devices 21

Preparing an Android device for image acquisition 22

Turn on USB debugging for Android devices 23

Bypass the lock screen on an LG device 24

Downgrading apps 24

Device drivers for popular Android device manufacturers 25

Acquiring a locked Android device 25

Flashing a recovery image of a Samsung device 26

Acquire a Samsung device by flashing a recovery image 26

Acquire a Samsung device using MTP bypass 27

Acquire a Motorola device using bootloader bypass 28

Acquire an LG device using download mode 28

Acquire an MTK device using download mode 29

Acquire an MTK device using an SD card backup 30

Acquire a Qualcomm device using EDL mode 30

Flash a custom recovery image of an Android device 31

Acquire an unlocked Android device 31

Customizing Android acquisition settings 31

Create segments for Android images 31

Restore device state for Android devices 32

Acquiring an iOS device 32

Access to data on iOS devices 32

Supported acquisition methods for iOS devices 33

Prepare an iOS device for image acquisition 33

Acquire an encrypted iOS backup 34

Acquire a jailbroken iOS device 35

Connecting to a device using SSH 35

Acquire a full image from a jailbroken iOS device 35
Acquiring a Kindle Fire device 35
Acquiring media and files through MTP 36
Acquiring SIM cards 36
Loading evidence from mobile devices 37
Load a mobile image 37
Load files and folders from a mobile device 37
Load an encrypted iOS backup 38
Loading GrayKey images 38
Load a GrayKey image 39
Download an image from a GrayKey device on your network 39
Supported images and file types 40
Acquiring computer evidence 41
Search types 41
Acquiring a drive 42
Acquire a drive 42
Image options for drives 43
Loading a drive 44
Loading an image 44
Load an image 45
Supported images and file types 45
Loading files and folders 46
Load a file or folder 46
Supported file systems 47
Loading a volume shadow copy 47
Loading memory 48
Find the profile of a memory dump 48
Load a memory dump with a known profile 49
Load a memory dump with an unknown profile 49
Include memory artifacts in your search 50
Export memory artifacts 50
Supported memory profiles 51
Decrypting evidence 53
Decrypt evidence with a known password or recovery key 54
Decrypt a McAfee-encrypted evidence source with a machine key 54
Decrypt a FileVault-encrypted evidence source with a password and a wipe key 55
Decrypt a VeraCrypt-encrypted partition with a password and a PIM 55

Decrypt an evidence source by cracking the password 56
Supported encryption types 57

Acquiring cloud evidence 58

Changes to supported cloud services and content 58
Preparing a cloud account for acquisition 58
Acquiring evidence from a cloud-based user account 59
Acquiring evidence from an Amazon EC2 instance 61
Acquiring evidence from an Amazon S3 bucket 64
Acquiring public activity 65
Acquire public activity from Twitter or Instagram 65
Supported cloud platforms and services 66
Loading cloud evidence 75
Load a cloud image 76
Supported evidence sources 76

Adding keywords to a search 78

Add keywords to search 78
Keyword search types 79

Searching archives and mobile backups 80

Search archives and mobile backups 80
Decrypt mobile backups 80
Set the number of nested archive and mobile backup search layers 80
Turn off searching for archives and mobile backups 81

Calculating hash values 82

Calculate hash values for all files 82
Import hash lists for known files 82
Ignore non-relevant files in a search 83
Customizing hash settings 83
Set the format for hash values 83
Set a size limit for hash files 84
Set the location where you store hash values 84

Categorizing evidence with Magnet.AI 85

Categorizing chats 85
Start categorizing chats after processing completes 85
Categorize chats in your case 85

Categorizing pictures 86

Start categorizing pictures after processing completes 86

Categorize pictures in your case 87

Remove a tag from categorized chats and pictures 87

Finding similar pictures with Magnet.AI 88

Optimize the performance of Magnet.AI 88

Build picture comparison to find similar pictures 89

Build picture comparison automatically 89

Finding similar pictures 89

Find similar pictures using a picture in your case 90

Find similar pictures using an imported picture 90

Viewing similar pictures 90

Select the number of pictures to show 90

Categorizing pictures and videos 92

Categorizing pictures and videos automatically by hash value 92

Select hash sets to use to categorize media 92

Manage picture and video hash sets 93

Set the priority of hash sets 94

Enable PhotoDNA 94

Categorizing pictures and videos manually 94

Apply a media category to a picture or video 95

Apply a media category to uncategorized pictures or videos 95

Update hash sets with media categorizations from a case 96

Export media categorizations from a case to Project VIC or CAID 96

Managing media categorization lists 97

Select a media categorization list to use 97

Create a custom list of media categories 97

Import a media categorization list 98

Export a media categorization list 98

Reducing exposure to illicit content 99

Blur or hide illegal media items 99

Mute videos by default 99

Set a reminder to stop categorizing media 100

Set an end time for media categorization 100

Find pictures with PhotoDNA matches 100

Recategorize media files in your case 101

Adding CPS data to a case ... 102

- Search for evidence that matches data from the CPS ... 102
- Add evidence from the CPS to your case ... 102

Searching for custom file types ... 103

- Add custom file types ... 103
- Turn off searching for file types ... 104
- Custom file types list fields ... 104
- Searching for headers and footers in custom file types ... 106
- Change the location of the Custom file types list ... 107
- Import a Custom file types list ... 107

Searching for SQLite databases ... 108

- Search for SQLite databases using the Dynamic App Finder ... 108
- Creating custom artifacts from SQLite database hits ... 108

Selecting artifacts to include in a search ... 112

- Select artifacts to include in your search ... 112
- Search for custom artifacts ... 112
- Decrypting artifacts ... 112
- Configuring media artifact options ... 113
  - Save picture attachments to the case ... 113
  - Extract EXIF data from pictures ... 113
  - Detect skin tone in pictures and videos ... 114
  - Set the maximum dimensions for saved pictures ... 114
  - Create video previews using still frames ... 114
  - Save videos to your case ... 115
  - Customize the maximum size of saved carved videos ... 115
- Managing artifact profiles ... 116
  - Create an artifact profile ... 116
  - Update an artifact profile ... 116
  - Import an artifact profile ... 116
  - Export an artifact profile ... 117
  - Set a default artifact profile ... 117
  - Rename an artifact profile ... 117
  - Delete an artifact profile ... 118

Adding custom artifacts ... 119

What is a custom artifact? 119
Creating a custom artifact 119
Add custom artifacts to AXIOM Process 119
Confirm the artifact loaded correctly 120
Viewing custom artifacts in AXIOM Examine 120

Reviewing the evidence 121
Viewing artifact information 121
Reset your case view 123
Reviewing your case from the Case dashboard 124
Quickly drill down to key evidence in your case 124
Browsing the artifacts 126
Views in the Artifacts explorer 126
Reviewing Refined results 127
View evidence from around the same time as an artifact or file 127
Set the default explorer to view relative date/time filter results in 128
Change character encodings 128
View artifacts in an external application 128
Save artifacts 129
View artifacts on a map 129
View artifact details in the World map view 129
View chat threads 130
View chat threads in Conversation view 130
Export a chat thread 130
View artifacts on a histogram 131
Open the Histogram view 131
Save a histogram baseline 131
Load a histogram baseline 131
Exploring the file system 132
Viewing raw artifact data in Text and hex 132
Browse to a specific offset 132
Search for a text string or hex value 133
Decode hex values 133
Save or copy text or hex data 133
Create artifacts using raw data 134
Viewing database tables 134
View evidence from around the same time as an artifact or file 135
Set the default explorer to view relative date/time filter results in 135

View artifacts associated with a file 136
View file system artifacts in an external application 136
Add files from the File system explorer to the Artifacts explorer 136
Display files and folders recursively 136
Save files and folders 137
Saving databases 137
Create artifacts using file snippets 137
Viewing the registry 138
Viewing evidence details in the registry 138
Viewing raw artifact data in Text and hex 138
Browse to a specific offset 139
Search for a text string or hex value 139
Decode hex values 139
Save or copy text or hex data 139
Create artifacts using raw data 140
Discovering connections 141
Build connections 141
Build connections automatically 141
View connections 142
Navigating maps 142
Tips for navigating maps 143
Viewing matching results 144
Print a map 144
Save a map as an HTML file 144
Viewing the timeline 145
Build the timeline 145
Build the timeline automatically 146
View the timeline 146
Tips for navigating the timeline graph 146
Export timeline data 147
Timeline categories 147
Tagging evidence 150
Tag evidence 150
Add comments to an artifact 150
Understanding tag syncing between evidence in the Artifacts and File system explorers 151
Tagging evidence from the Artifacts explorer 151
Tagging evidence from the File system explorer 151

Removing tags from Tagged from file system artifacts 152
Exporting tagged evidence 152
Customizing tags 152
Create a custom tag 152
Import tags 153
Export tags 153
System tags 154
Organize evidence with profiles 154
Create a profile 154
Apply a profile 155
Import profiles 155
Export profiles 155
Filtering evidence 157
Types of filters 157
Filtering by date and time 159
Filter evidence by a specific date or time 159
Filter by relative date or time 160
Filtering by keywords 160
Filter by keyword list 160
Import a keyword list 160
Search by keyword 161
Search by keyword using advanced search options 161
Search by regular expression 162
Search by keyword snippet 162
Filter by accessible and inaccessible files 163
Filter by skin tone percentage 163
Filtering by column 164
Filter by column using a basic search 164
Filter a numeric column using an advanced search 164
Filter a string column using an advanced search 165
Adding more evidence to a case 167
Add new evidence to your case 167
Remove evidence from case 167
Add cloud evidence using recovered passwords and tokens 168
Acquire and decrypt a WhatsApp backup using a recovered decryption key 168

- Recategorize media files in your case 169
- Import CPS evidence 170

Viewing the source of evidence 171

- View the source of an artifact result 171
- View registry entries for an artifact result 171

Exporting and sharing evidence 173

- Exporting evidence using the exporting wizard 174
  - About the exporting wizard 174
  - Create an export 174
  - Export types 175
  - Items to include in your export 177
  - Configure artifact details 178
  - Format options 178
- Creating and managing column configurations 179
- Creating column configurations 179
  - Use the column configuration in your current view for your export 179
  - Create a column configuration 179
  - Import another user's column configuration 180
  - Export a column configuration 180
- Creating and managing templates 180
- Creating export templates 180
  - Save export settings as a template 181
  - Create a new template 181
  - Import a template 181
  - Export a template 182
  - Edit a template 182
- Exporting specialized outputs 182
  - Exporting specialized outputs using the exporting wizard 182
    - Export evidence that is in a different language 182
    - Export a chat thread 183
    - Export media categorizations from a case to Project VIC or CAID 183
  - Other types of exports 184
    - Export metadata 184
    - Export timeline data 185
    - Export memory artifacts 185
    - Export a connections map 186

Print or export a connections map as a PDF 186
Export a connections map as an HTML file 186
Collaborate on cases with others using portable case 187
Create a portable case 187
Sharing portable cases 187
Reviewing portable cases 187
Magnet AXIOM features available in portable case 188
Open a portable case 189
Merge a portable case 189
Keyboard shortcuts in AXIOM Examine 190
Customizing Magnet AXIOM 192
Customizing imaging settings 192
Create segments for Android and drive images 192
Create a hash value for evidence sources 192
Verify hash values for acquired images 192
Compress images 193
Restore mobile device state for Android devices 193
Customizing processing settings 193
Save temporary files to a custom location 193
Verify hash values for images 194
Deduplicating artifact results 194
Remove duplicate artifact results 195
Optimize search times 195
Customizing hashing settings 196
Set the format for hash values 196
Prevent hashing of large files 196
Set the location where you store hash values 196
Enable PhotoDNA 197
Customizing examining settings 197
Build connections automatically 197
Build timeline automatically 197
Set the default explorer to view relative date/time filter results in 198
Set the default explorer 198
Change the default view 198
Set the folder structure for saved files 198
Customizing general settings 199

Set a default case type 199
Collect log information 199
Send diagnostic information 199
Turn off software updates 200
Turn on Passware encryption features 200
Remove the Passware plugin 200
Connect to the internet using a system proxy 201
Change the display language 201

Updating Magnet AXIOM 202

Update Magnet AXIOM while online 202
Update Magnet AXIOM while offline 202

WHAT'S NEW

VERSION	DESCRIPTION
4.3.0	- Updated Calculating hash values with more information about ignoring non-relevant files. - Updated Reviewing the evidence with information about the JSON file previews. - Updated Finding similar pictures with Magnet.AI with more information about building picture comparison automatically.
4.2.0	- Updated Acquiring cloud evidence with information about acquiring WhatsApp accounts using QR codes. - Updated Loading cloud evidence with information about loading Skype warrant returns and Microsoft Office 365 Unified Audit Logs. - Updated Customizing Magnet AXIOM with more information about setting the folder structure of saved files and verifying the hash of processed AFF4 images. - Updated Finding similar pictures with Magnet.AI with information about building picture comparison automatically. - Updated Exporting evidence using the exporting wizard with more information about export types. - Updated Collaborate on cases with others using portable case. - Updated Loading an image and Loading evidence from mobile devices with information about AFF4 images.
4.1.0	- Updated Selecting artifacts to include in a search with more information about saving picture and video attachments in the case. - Updated Finding similar pictures with Magnet.AIwith information about selecting the number of pictures to show. - Updated Customizing Magnet AXIOM with information about setting the folder structure for saved .zip files. - Updated Acquiring an Android device with more information about downgrading apps.

VERSION	DESCRIPTION
4.0.0	• Updated Exporting evidence using the exporting wizard with information about the new exporting wizard. • Added Creating and managing column configurations. • Added Creating and managing templates. • Added Exporting specialized outputs. • Added Finding similar pictures with Magnet.AI. • Updated Acquiring cloud evidence to include information about Lyft and Microsoft Azure. • Updated Customizing Magnet AXIOM with more information about supported proxy types. • Updated Adding keywords to a search to include information about default encoding types.
3.11.0	• Updated Supported images and file types for loading evidence from mobile devices with support for .dar images. • Updated Adding more evidence to a case with information about the updated process for acquiring and decrypting WhatsApp backups. • Updated Acquiring cloud evidence with information about the difference between support for IMAP and POP acquisition.
3.10.0	• Updated Deduplicating artifact results with information about how AXIOM Process deduplicates FAT artifact results. • Updated Acquiring cloud evidence with information about acquiring an Uber account.
3.9.0	• Updated Reviewing the evidence and Collaborate on cases with others using portable case with information about how Magnet AXIOM handles executable files and scripts in your evidence. • Updated Tagging evidence with information about tag syncing between evidence in the Artifacts and File system explorers. • Updated Acquiring cloud evidence with more information about acquiring AWS EC2 instances and S3 buckets and information about the availability of Cloud platforms in AXIOM Cloud and AXIOM Cloud Premium. • Updated Loading cloud evidence with information about the availability of Cloud platforms in AXIOM Cloud and AXIOM Cloud Premium. • Updated Decrypting evidence with information about decrypting Windows 10 devices that have BitLocker Device Encryption turned on. • Updated Deduplicating artifact results with more information about how AXIOM Process deduplicates artifact results.

VERSION	DESCRIPTION
3.8.0	• Updated Exporting and sharing evidence and Reviewing your case from the Case dashboard with information about exporting case dashboard cards for media categorization summary and keyword matches. • Updated Customizing general settings with information about setting a default case type when creating a new case in AXIOM Process. • Updated Tagging evidence with information about the Exceptions system tag.
3.7.0	• Updated Loading cloud evidence with information about loading Google warrant returns. • Updated Loading memory with current list of supported memory profiles. • Updated Loading an image with information about support for Advanced Forensic File (AFF4) images.
3.6.0	• Updated Reviewing the evidence with information about viewing extended attributes and text and hex information in the APFS metadata card. • Updated Acquiring cloud evidence with information about acquiring public Instagram activity. • Updated Filtering evidence with information about new advanced column filtering options. • Updated Loading evidence from mobile devices with information about loading encrypted iOS backups.
3.5.0	• Updated Loading cloud evidence with information about loading Apple warrant returns • Updated Categorizing pictures with Magnet.AI with information about a new categorization option for searching for pictures of human faces and license plates. • Updated Filtering evidence with information about new advanced keyword filtering options. • Updated Customizing Magnet AXIOM with information about setting the location where you store hash values

GETTING STARTED WITH MAGNET AXIOM

Magnet AXIOM is a comprehensive, integrated digital forensics platform. It's the only platform that acquires and processes computer, smartphone, and cloud data in a single case file. Magnet AXIOM has two components: AXIOM Process and AXIOM Examine. Using AXIOM Process, you can acquire forensic images, load existing images, and run scans on those images all from the same interface. After processing is complete, you can review the evidence in AXIOM Examine.

Building your case in Magnet AXIOM

Learn more about building your case in AXIOM Process and reviewing the evidence in AXIOM Examine.

Step 1: Start a case

Your first step is to start your case. You can create a new case in AXIOM Process, or if you've already created a case, you can also add evidence to an existing case by browsing to a case or opening a recent case. If you choose to add evidence to an existing case, certain information—such as the case number, search type, keyword lists, and more—will be locked down based on the settings from the original search.

If you skip a step that's required, AXIOM Process flags it with a warning symbol !, and you won't be able to start processing until the step is complete.

Step 2: Provide case details

Specify basic information about your case such as the case number, the case type, where you want to save your case files and acquired evidence, and more.

The details you provide here are included in several reports or export types such as portable case, JSON, HTML, and PDF.

Step 3: Add your evidence sources

Add your evidence sources—computer, mobile, or cloud—and specify whether you are acquiring or loading evidence. Choose to acquire evidence if you want AXIOM Process to create an image of a computer drive, mobile device, or cloud-based social media platform. Choose to load evidence if you are uploading existing forensic images, files, or folders.

If you have multiple forensic images, you can add them all to the same case.

Acquiring evidence

AXIOM Process can acquire and process evidence from the following types of devices:

- Mobile devices including:
  - Android
  - iOS
  - Kindle Fire
  - Media devices that support the media transfer protocol (MTP)
  - SIM cards
- Computer drives including: HDD, SSD, USB, SD flash drives for the Windows operating system.
- Cloud-based social media platforms including: Amazon Web Services (AWS), Apple, Box.com, Dropbox, IMAP/POP Email, Facebook, Google, Instagram, Lyft, Microsoft, Microsoft Azure, Microsoft Teams, Slack, Twitter, Uber, and WhatsApp (Google Drive backups and QR code access).

Loading evidence

AXIOM Process can search many other types of evidence sources acquired using other tools:

- Computer sources including:
  - Connected drives
  - Files and folders
  - Images
  - Volume shadow copies
  - Memory dump files
- Mobile images and files and folders for: Android, iOS, Windows Phone, and Kindle Fire.
- Cloud sources including: AXIOM Cloud images, Apple warrant returns, Facebook warrant returns, Facebook Download Your Information archives, Instagram warrant returns, Google Takeout archives, Google warrant returns, iCloud backups, Microsoft Office 365 Unified Audit Logs, Skype warrant returns, Slack archives, and Snapchat warrant returns.

Step 4: Configure processing details

Configure advanced processing features so that you can use to get more out of your search:

- Add keywords and keyword lists to your search.
- Search archives and mobile backups.
- Calculate hash values for each file in an evidence source.
- Categorize picture and chat evidence using Magnet.AI.
- Categorize pictures and videos using hashes for known media files and .json files from Project VIC and CAID.
- Import CPS data so that AXIOM Process can search for matches in your case.
- Search for SQLite databases using the Dynamic App Finder.
- Search for custom file type artifacts.

Step 5: Configure artifact details

Select the artifacts that you want to include or exclude from your search. Depending on the type of Magnet AXIOM license that you have, you might have computer artifacts, mobile artifacts, cloud artifacts, or a combination.

Step 6: Analyze evidence

After you finish configuring each step in AXIOM Process, click **Analyze evidence** to start scanning the evidence. AXIOM Examine opens automatically to display any evidence that is recovered. The *Analyze evidence* screen indicates what percentage of the scan is complete along with information about search definitions and thread details.

After the search completes, there might be additional steps to complete. If you configured AXIOM Process to find more artifacts using the Dynamic App Finder, you might have to configure the artifacts that it discovers. For more information about turning this recovered data into custom artifacts, see Creating custom artifacts from SQLite database hits.

When a search completes, you can view a summary of the completed search—including any exceptions that might have occurred. You can also view the scan summary from the Case dashboard in AXIOM Examine. Unprocessed files are also tagged in AXIOM Examine with the *Exceptions* system tag.

Step 7: Examine the evidence

You can examine your evidence in a number of different ways:

- See an overview of your case using the Case dashboard.
- Browse the evidence using the Artifacts explorer, File system explorer, or Registry explorer.
- Analyze connections between attributes using the Connections explorer.
- Review and analyze timestamped evidence in the Timeline explorer.
- Filter evidence to narrow your focus.
- Tag and add comments to important evidence.
- Categorize media evidence with Project VIC or CAID hash lists or your own lists.
- Add more evidence to your case.

Step 8: Export or share the evidence

You can export your evidence to share with other stakeholders:

- Share evidence in many different formats, including Excel, XML, HTML, PST, PDF, and more.
- Collaborate on a case with other examiners and stakeholders by creating a portable case.

ACQUIRING MOBILE EVIDENCE

Using AXIOM Process, you can acquire mobile devices as well as load existing images, files, and folders previously acquired from mobile devices.

When you image a mobile device, specifying the operating system alerts AXIOM Process as to which set of artifacts should be scanned for, as data resides in different locations depending on the operating system. While some artifacts (i.e. Facebook, Twitter, WhatsApp, etc.) can be parsed from multiple mobile operating system types, the location and structure of the data can vary on each operating system.

METHOD	SUPPORTED EVIDENCE SOURCE	DESCRIPTION
Acquiring evidence	Android	Use this option to acquire evidence from an Android device. For Android devices running version 2.1 and later, AXIOM Process can obtain full images from rooted Android devices and quick images from other Android devices.
	iOS	Use this option to acquire evidence from an iOS device. AXIOM Process can obtain a quick image from iOS devices (version 5.0 and later) and full images from jailbroken iOS devices.
	Kindle Fire	Use this option to acquire evidence from a Kindle Fire device.
	Media devices that support MTP	Use this option to acquire evidence from media devices that support the media transfer protocol (MTP). Examples of media devices that typically support MTP include digital cameras, feature phones, and smartphones such as Android, iOS, BlackBerry, and Windows Phone.
Loading evidence	Images and files and folders	Use this option to load existing images, files, and folders from supported Android, iOS, Windows Phone, and Kindle Fire devices.

Acquiring an Android device

For Android devices running version 2.1 and later, AXIOM Process can obtain full images from rooted Android devices and quick images from other Android devices.

- A **quick** image is a comprehensive logical image that contains both user data and some native application data. AXIOM Process attempts multiple acquisition methods to get you as much information as possible from the device, as quickly as possible, so that you can start examining the evidence right away.
- A **full** image is a physical or file-system logical image. During this type of acquisition, AXIOM Process copies the entire contents of a device into a single file (either a .raw file or a .zip file, depending on the device). With a full image, you have a higher possibility of recovering data from unallocated space (that is, deleted files).

If you're unable to acquire either a quick or a full image, another option for some devices is to acquire media.

Review the Supported acquisition methods for Android devices topic for more information about which acquisition methods are available for specific Android versions.

In addition to acquiring evidence from an Android device, you can load existing images and files and folders.

Access to data on Android devices

The type of image that you can acquire from a device depends on the level of access that you have. Acquiring a full image requires that you have privileged access to the device. Privileged access indicates that you have an enhanced level of permissions which allow you to interact with the device in ways that a regular user can't.

On Android devices, having *root access* gives you enhanced permissions so that you can run apps that need access to certain system settings, flash custom images to the device, and more.

For full images, if an Android device is not rooted, AXIOM Process attempts to gain privileged access to the device using tested rooting methods. AXIOM Process creates a log file documenting the process, and indicates which roots are tried and whether any are successful.

Supported acquisition methods for Android devices

Full images are formatted as .raw files and quick images are formatted as .zip files.

	OS	METHOD	EVIDENCE
FULL	Android 2.1 and later**	Linux DD command	Recover a full physical image of the device's flash memory. Evidence collected includes all files, folders, user data, native data, and unallocated space.
QUICK	Android 2.1 to 8+	Android Debug Bridge (ADB) mode	Contents of any external storage (for example, an SD card).
	Android 2.1 to 8+	Agent application	Call logs, SMS/MMS, browser history, and user dictionary.
	Android 4.0 and later	ADB backup / agent application	Third-party application user data. Some native device data including SMS/MMS, browser history, calendar, call logs, BT devices, WiFi hot spots, user accounts, and user dictionary. Contents of any external storage (for example, an SD card).
	Android (Samsung models only)	MTP bypass	Pictures, videos, and any other files discoverable via MTP.

** Requires a rooted device. In some cases, AXIOM Process can root the device for you.

Preparing an Android device for image acquisition

Before you acquire an image from an Android device, verify that your computer and device are set up correctly.

To make sure AXIOM Process can connect to the Android device and acquire the most complete forensic image possible, there are several options that you need to set.

> Tip: If you don't want your search criteria to be saved in the recent search history on the device, don't use the magnifying glass on the mobile device to search for settings or other information.

- Turn on the device.
- Connect the device to the computer using a sync cable (not a charging cable).
- Charge the device to at least 50%.
- Unlock the device.
- Turn on airplane mode.

- Verify the device is running Android 2.1 or later.
- Set the USB option to charging. On some devices, you must set this option each time the USB cable is reconnected or the device is restarted.
- Turn off USB mass storage (on devices with micro SD capabilities). If this option is turned on, the device might unmount the SD card, resulting in less data being acquired during a quick image.
- Turn on USB debugging/developer mode. On most devices, you turn on developer mode by tapping on the build number until the "You are now a developer" message appears on the screen.
- Verify that USB debugging/develper mode is in turned on. On some devices, you must turn this setting on after you turn on USB debugging/developer mode. In **Settings** > **Developer options**, turn on **USB debugging**.
- Set the screen to stay awake. In **Settings** > **Developer** options, turn on **Stay awake**.
- Trust the computer that the device is connected to. When you connect the device to the computer, follow the device's on-screen instructions.
- Turn off the Verify apps via USB or Verify apps: Block or warn setting. In **Settings** > **Developer options**, turn off **Verify apps via USB**. The wording of the setting might vary depending on the device manufacturer.
- Allow the installation of applications from unknown sources. In **Settings** > **Security**, turn on **Unknown Sources**. The wording of the setting might vary depending on the device manufacturer.

> Tip: You must turn on USB debugging mode before you receive a prompt to trust the computer. To revoke the trust setting, in **Settings** > **Developer options** tap **Revoke USB debugging authorizations**.

Turn on USB debugging for Android devices

Depending on the type of Android device, there are different ways to turn on USB debugging or developer mode. Here's how you can turn on USB debugging for a few popular devices:

TYPE OF DEVICE	TURN ON USB DEBUGGING
Android 2.x+	In **Settings** > **Applications** > **Development**, tap the **Enable USB Debugging** option.
Android 4.2+	In **Settings** > **About phone**, tap the **Build Number** field approximately 7 times until “You are now a Developer” displays on the screen.
HTC One (M7/M8/M9)	In **Settings** > **About** > **Software information** > **More** > **Build number**, tap the **Build Number** field approximately 7 times until "You are now a Developer” displays on the screen.

TYPE OF DEVICE	TURN ON USB DEBUGGING
LG G2/G3 Samsung Galaxy	In **Settings** > **About phone** > **Software information** > **Build number**, tap the **Build Number** field approximately 7 times until “You are now a Developer” displays on the screen.
Stock Android	In **Settings** > **About phone**, tap the **Build Number** field approximately 7 times until “You are now a Developer” displays on the screen.

Bypass the lock screen on an LG device

If a LG Android device is locked and you don't have the passcode, you can attempt to bypass the lock screen in AXIOM Process. AXIOM Process supports bypassing the lock screen for many LG devices but does not currently support LG Nexus devices.

After successfully bypassing the lock screen, you can perform an acquisition of the device without needing the passcode.

1. In AXIOM Process, click **Evidence Sources** > **Mobile** > **Android** > **Acquire Evidence** > **Advanced (Lock Bypass)** > **LG Electronics** > **Lock bypass**.
2. Follow the instructions in AXIOM Process.
3. To start an acquisition of the device, click **Next** and select start an unlocked acquisition workflow for the device.

Downgrading apps

Some newer mobile device apps block access to their data. You can choose to temporarily install a previous version of the app that provided access to the data, acquire the evidence, and then install the original app back on the device again.

When acquiring a quick image of a device running Android 6.0 and earlier, you can turn on app downgrading in AXIOM Process.

> Warning: There are risks associated with app downgrading. You might change data on the device when you use this feature.

Device drivers for popular Android device manufacturers

If you're connected to the Internet while using AXIOM Process, AXIOM Process attempts to download the appropriate drivers for the mobile device that you're imaging. If the correct driver can't be found, you might have to visit the device manufacturer's website to download the driver. Here are the links to download drivers for a few popular devices:

- HTC: www.htc.com/us/software
- LG: www.lg.com/us/support
- Motorola: support.motorola.com
- Nexus: developer.android.com
- Samsung: developer.samsung.com
- Sony: developer.sony.com/develop/drivers/

Acquiring a locked Android device

As the development of smartphone software advances, it becomes increasingly difficult to gain privileged access to the device. When a device is locked, you might be prevented from being able to extract any data.

To help you acquire the most complete forensic image as possible, AXIOM Process supports several advanced mobile acquisition methods that increase your chances of getting a full image of the device. Some methods require that you flash the device with a recovery image, while others take advantage of download modes or device hardware features.

For more information about acquiring Android devices using Advanced lock bypass, review the acquisition methods for popular device manufacturers:

HARDWARE / MANUFACTURER	ACQUISITION METHOD	IMAGE TYPE
Samsung	Flash a recovery image	Full image
	MTP bypass	Quick image
Motorola	Bootloader bypass	Full image
LG	LG download mode	Full image

HARDWARE / MANUFACTURER	ACQUISITION METHOD	IMAGE TYPE
MTK chipsets	Download mode	Full image
	SD card backup	Logical image
Qualcomm chipsets	EDL mode	Full image
All Android devices	Flash a custom recovery image	Full image

Flashing a recovery image of a Samsung device

If a Samsung device is locked or is otherwise preventing you from gaining privileged access, you can flash a recovery image to the device to attempt to extract a full image.

Flashing a supported device with a recovery image allows AXIOM Process to grant itself root ADB access and bypass the device password. To prevent any loss of data integrity, the recovery image is flashed to a partition on the device that's separate from system and data partitions. The full image that gets extracted even gives you access to deleted data on the device, including data left behind after a factory reset. AXIOM Process offers recovery images for more than 1300 Samsung device models.

> Warning: There are risks associated with using third-party recovery packages. You might:
>
> - Void the device warranty.
> - Turn off the Knox security platform on Samsung devices.
> - Render the device completely or partially inoperable ("brick" the device).

Acquire a Samsung device by flashing a recovery image

When flashing a recovery image of a Samsung device, AXIOM Process can detect if the device is encrypted and prompts you to enter a password to decrypt the data. If the device is encrypted but has default encryption (no user password), AXIOM Process decrypts the data partition without prompting or requiring that you enter a password. Samsung devices allow you to enter up to 31 incorrect passwords before wiping the device. To help you keep track of attempts to decrypt the device, AXIOM Process displays the current password attempt count. If you don't know the device password, you can skip the decryption step and acquire the device with an encrypted user data partition.

> Note: This bypass method is only available for devices that have an unlocked bootloader and don't

> have FRP enabled.

Before you begin: Make sure the device does not have a locked bootloader and that the Factory Reset Protection (FRP) feature is not activated. Failing to do so might wipe the device or render it inoperable. FRP is a security feature on Android devices running Lollipop 5.1 and later. It is automatically activated when a user sets up a Google Account on the device. When activated, after a factory reset, FRP prevents use of the device until you log in to the Google Account that was previously set up. For more information about FRP, visit www.samsung.com/us/support/frp/. To determine if the device has a locked bootloader, in a browser, search for "check if bootloader is locked" for the device model. AT&T and Verizon devices often have locked bootloaders.

1. Download all three Samsung device Recovery Images .zip files from Downloads and Supported Devices.
2. Extract the contents to your computer using an extraction tool such as 7zip or WinRar.
3. Double-click **Magnet Recovery Images setup.exe** and follow the instructions in the wizard to install the programmers in your Magnet AXIOM directory.
4. After installation is complete, start the Recovery workflow in AXIOM Process: Click **Evidence Sources** > **Mobile** > **Android** > **Acquire Evidence** > **Advanced (Lock Bypass)** > **Samsung > Recovery (Full image)**.
5. Follow the instructions in AXIOM Process.
6. To continue setting up your case, click **Next**.

Acquire a Samsung device using MTP bypass

For Samsung devices that haven't received either the SMR-OCT-2017 or SMR-NOV-2017 security update (typically, devices from 2012 to 2017 running Android OS Android OS version 4.0.3 to 7), you can do an MTP (Media Transfer Protocol) bypass to attempt to extract a quick image.

When the device is encrypted, the bootloader is locked, or it's not possible to input a passcode, MTP bypass allows you to acquire a quick image of the /media/ partition on the Samsung device. The /media/ directory in the /data/ or /userdata/ partition mostly includes picture and video files but might include data such as documents, downloads from web browsers, WhatsApp chat backups, and third-party application data.

To use MTP bypass for Samsung devices, complete the following steps:

1. In AXIOM Process, click **Evidence Sources** > **Mobile** > **Android** > **Acquire Evidence** > **Advanced (Lock Bypass)** > **Samsung** > **MTP (Quick image)**.

2. Follow the instructions in AXIOM Process.
3. To continue setting up your case, click **Next**.

Acquire a Motorola device using bootloader bypass

AXIOM Process supports the ability to flash certain Motorola devices with a recovery image. By flashing a supported device with a recovery image, AXIOM Process can grant itself root ADB access and bypass the device password. To not affect the integrity of the data, the recovery image is flashed to a partition on the device that's separate from system and data partitions. The full image that gets extracted even gives you access to deleted data on the device, including data left behind after a factory reset.

> Note: This method does not work with all Motorola product lines and devices.

To use recovery images for Motorola devices, complete the following steps:

1. Download the **Recovery Images for Motorola devices .zip** file from Downloads and Supported Devices.
2. Extract the contents to your computer using an extraction tool such as 7zip or WinRar.
3. Double-click **Magnet Recovery Images for Motorola setup.exe** and follow the instructions in the wizard to install the programmers in your Magnet AXIOM directory.
4. After installation is complete, start the Bootloader Bypass workflow in AXIOM Process: Click **Evidence Sources** > **Mobile** > **Android** > **Acquire Evidence** > **Advanced (Lock Bypass)** > **Motorola** > **Bootloader Bypass (Full image)**.
5. Follow the instructions in AXIOM Process.
6. To continue setting up your case, click **Next**.

Acquire an LG device using download mode

On some LG devices, AXIOM Process can bypass the password and extract a full image by exploiting LAF (LG Advanced Flash). LAF is a tool that's used for downloading and uploading firmware for the device. Using LAF, AXIOM Process can put an LG device into download mode and extract its data.

This method works on devices that were released up until late 2017.

To use download mode for LG devices, complete the following steps:

1. Download the drivers for LG devices from Downloads and Supported Devices.
2. Double-click **LGMobileDriver_WHQL_Ver_X.X.X.exe** and follow the instructions in the wizard to install the programmers in your Magnet AXIOM directory.
3. After installation is complete, start the LG Download Mode workflow in AXIOM Process: Click **Evidence Sources** > **Mobile** > **Android** > **Acquire Evidence** > **Advanced (Lock Bypass)** > **LG Electronics** > **LG Download Mode (Full image)**.
4. Follow the instructions in AXIOM Process.
5. To continue setting up your case, click **Next**.

Acquire an MTK device using download mode

Some MediaTek (MTK) chipset hardware allows AXIOM Process to bypass the password on some Android devices that use certain chipsets. A successful bypass allows you to obtain a full image of the device.

To learn if your device is supported, click the *Compatible devices* link in the Downloads and Supported Devices page. You can also review the following websites to determine whether the device has an affected chipset:

- phonedb.net
- www.phonearena.com
- www.gsmarena.com
- www.phonescoop.com

To use download mode for MTK chipsets, complete the following steps:

1. Download the drivers for MTK chipsets from Downloads and Supported Devices.
2. Double-click **MTKDriverInstaller.exe** and follow the instructions in the wizard to install the programmers in your Magnet AXIOM directory.
3. After installation is complete, start the LG Download Mode workflow in AXIOM Process: Click **Evidence Sources** > **Mobile** > **Android** > **Acquire Evidence** > **Advanced (Lock Bypass)** > **Other** > **Mediatek (MTK)** > **Mediatek (MTK) (Full image)**.
4. Follow the instructions in AXIOM Process.
5. To continue setting up your case, click **Next**.

Acquire an MTK device using an SD card backup

MediaTek (MTK) based devices allow you to back up user data to an SD card—even on locked devices. Acquire and process these backups in AXIOM Process to attempt to gain access to device information using this method without requiring a device password.

To acquire an MTK device using an SD card backup, complete the following steps:

1. In AXIOM Process, click **Evidence Sources** > **Mobile** > **Android** > **Acquire Evidence** > **Advanced (Lock Bypass)** > **Other** > **Mediatek (MTK)** > **SD card backup (Logical image)**.
2. Follow the instructions in AXIOM Process.
3. To continue setting up your case, click **Next**.

Acquire a Qualcomm device using EDL mode

Emergency Download (EDL) mode is a Qualcomm feature that can allow you to perform tasks like unbricking or flashing a device, and downloading data. On supported devices, Magnet AXIOM can use EDL mode to extract a full image. You can read more about how to start a device in EDL mode at www.-magnetforensics.com/blog/qualcomm-phone-edl-mode.

Before you attempt to acquire a Qualcomm device using EDL mode, complete following steps:

1. Download the **EDL Drivers .zip** file from Downloads and Supported Devices.
2. Extract the contents to your computer using an extraction tool such as 7zip or WinRar.
3. Double-click **driver_installer.exe** and follow the instructions in the wizard.
4. Download the EDL Programmers installer from **Downloads and Supported Devices**.
5. Double-click the **Magnet EDL Programmers setup.exe** file and follow the instructions in the wizard to install the programmers in your Magnet AXIOM directory.
6. After installation is complete, start the EDL mode workflow in AXIOM Process: Click **Evidence Sources** > **Mobile** > **Android** > **Acquire Evidence** > **Advanced (Lock Bypass)** > **Other** > **Qualcomm**.
7. Follow the instructions in AXIOM Process.
8. To continue setting up your case, click **Next**.

After the EDL mode workflow starts, AXIOM Process attempts to select a compatible programmer based on the device type. While it's possible to manually select a programmer, it's recommended that you allow AXIOM Process to choose one for you.

Note: Programmers are not available for all Qualcomm devices. And some programmers can work with more than one device type.

Flash a custom recovery image of an Android device

If the Android device you want to acquire isn't supported by an existing recovery image, and you have your own recovery image for it, you can load a custom recovery image. AXIOM Process can attempt to acquire data from a device by flashing a custom recovery image to it, such as TWRP.

> Warning: Be careful loading your own recovery images as you will likely brick the device if the wrong recovery image is used.

1. Start the Custom Recovery workflow in AXIOM Process: Click **Evidence Sources** > **Mobile** > **Android** > **Acquire Evidence** > **Advanced (Lock Bypass)** > **Other** > **Recovery (Full Image)**.
2. Follow the instructions in AXIOM Process.
3. To continue setting up your case, click **Next**.

Acquire an unlocked Android device

If the Android device you want to acquire is unlocked, and you can turn on USB debugging, you can you attempt to acquire a full or a quick image of the device using Android Debug Bridge (ADB). Acquiring a full image requires privileged (root) access.

1. Start the ADB workflow in AXIOM Process: Click **Evidence Sources** > **Mobile** > **Android** > **Acquire Evidence** > **ADB (Unlocked)**.
2. Follow the instructions in AXIOM Process.
3. To continue setting up your case, click **Next**.

Customizing Android acquisition settings

Create segments for Android images

You can specify the size of the image segments that you want AXIOM Process to create when it acquires evidence from Android and drive images. Each option represents a different size that reflects its storage capabilities. By default, image segmentation is turned off.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Imaging** > **Image segmentation**, select a format from the drop-down list.
3. Click **Okay**.

Restore device state for Android devices

While AXIOM Process acquires evidence from Android devices, it installs an agent application onto the device to assist with recovering data. When the scan completes, AXIOM Process can remove the agent application from the device. By default, the agent application is left on the device.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Imaging** > **Restore mobile device state**, select the **Remove agent application** option.
3. Click **Okay**.

Acquiring an iOS device

AXIOM Process can obtain a quick image from iOS devices (version 5.0 and later) and full images from jailbroken iOS devices.

- A **quick** image is a comprehensive logical image that contains both user data and some native application data. AXIOM Process attempts multiple acquisition methods to get you as much information as possible from the device, as quickly as possible, so that you can start examining the evidence right away.
- A **full** image is a physical or file-system logical image. During this type of acquisition, AXIOM Process copies the entire contents of a device into a single file (either a .raw file or a .zip file, depending on the device). With a full image, you have a higher possibility of recovering data from unallocated space (that is, deleted files).

If you're unable to acquire either a quick or a full image, another option for some devices is to acquire media.

In addition to acquiring evidence from an iOS device, you can load existing images and files and folders such as including encrypted iOS backups and GrayKey images.

Access to data on iOS devices

The type of image that you can acquire from a device depends on the level of access that you have. Acquiring a full image requires that you have privileged access to the device. Privileged access indicates that you have an enhanced level of permissions which allow you to interact with the device in ways that a regular user can't. Gaining privileged access to an iOS device is often achieved by jailbreaking the device.

On iOS devices, a jailbreak uses an exploit or security vulnerability in the software to give you enhanced permissions to the operating system. For early iOS versions, these permissions allowed you to get a full image of the device, but for iOS 5.0 and later, the encryption allows only a logical image to be obtained.

Jailbreaks are often discovered after the release of a new iOS version. The timing of their availability depends on how difficult it is to find the vulnerability in the software. For many modern iOS devices, there are no public jalilbreaks available. You should monitor public jailbreaks to stay current.

Supported acquisition methods for iOS devices

Both full images and quick images from an iOS device are formatted as .zip files.

	OS	METHOD	EVIDENCE
FULL	iOS 5 to 10+ **	SSH	For jailbroken iOS devices, AXIOM Process recovers a full logical file system dump that includes all of the files, folders, user data, and native data.
QUICK	iOS 5 to 11+	iTunes backup process	Third-party application user data. Some native device data, including: SMS/MMS and iMessage, calendar, and call log.
	iOS 5 to 11+	Apple File Conduit	Camera pictures, ringtones, and iTunes books.
	iOS 8 and earlier	File relay	Some native device data, including: complete photo album, SMS/MMS and iMessage, address book, typing cache, geolocation cache, application screen shots, WiFi hot spots, voicemail, and native email metadata.

** Requires a jailbroken device.

Prepare an iOS device for image acquisition

Before you acquire an image from an iOS device, verify that your computer and device are set up correctly.

To allow AXIOM Process to connect to the iOS device and acquire the most complete forensic image possible, there are several options that you need to set.

> Tip: If you don't want your search criteria to be saved in the recent search history on the device, don't use the magnifying glass on the mobile device to search for settings or other information.

- Verify your computer is running the latest version of iTunes.
- Turn on the device.
- Connect the device to the computer using a sync cable (not a charging cable).
- Charge the device to at least 30%.
- Unlock the device.
- Turn on airplane mode.
- Verify that the device is running iOS 5 or later.
- Turn off screen lock or set it to the maximum amount of time.
- Set the screen timeout or sleep mode to stay awake, or to the maximum amount of time.
- Trust the computer that the device is connected to. When you connect the device to the computer, follow the device's on-screen instructions. On iOS 8 and later, to revoke trust, tap **Settings** > **General** > **Reset** > **Reset Location & Privacy**.

Acquire an encrypted iOS backup

AXIOM Process can often extract more evidence from an iOS device if it first creates an encrypted backup of the device. An encrypted backup can include information that isn't available in a normal quick image, such as saved passwords (iOS keychain), health data (HealthKit), smart home data (HomeKit), and more.

During the acquisition setup, AXIOM Process automatically prompts you for an encryption password if you choose the Quick image option. After the search starts, AXIOM Process creates an encrypted backup of the device and then decrypts the backup using the password that you provide. After imaging completes, AXIOM Process removes the password from the device.

1. In AXIOM Process, click **Evidence sources** > **Mobile** > **iOS** > **Acquire evidence**.
2. Select the device, and then click **Next**.
3. Select the **Quick** image type and click **Next**.
4. In the **Encrypted iTunes backups** dialog, provide a password to use for encryption and click **Okay**.
5. To continue setting up your case, click **Next**.

Acquire a jailbroken iOS device

You can extract a full image from an iOS device if the device is jailbroken, and SSH is installed. When SSH is configured, it allows you to interact with the device in ways that a regular user can't. You can run commands on the device, access the file system, or install third-party applications.

When you connect a jailbroken iOS device to AXIOM Process, it attempts to detect SSH automatically. If the device is supported, AXIOM Process indicates that it has *privileged access* to the device. If AXIOM Process can't connect to the device, only the Quick image option is available.

> Note: AXIOM Process no longer supports AFC2 as a service to communicate with iOS devices. This service was often used by jailbreak tools such as Cydia but is less commonly supported in newer jailbreaks.

Connecting to a device using SSH

When AXIOM Process detects that SSH is present on an iOS device, it attempts to connect to the device automatically by using the default SSH credentials (username: root, password: alpine).

If the SSH credentials are not set to the default values, AXIOM Process prompts you to provide the correct credentials to attempt to connect again.

Acquire a full image from a jailbroken iOS device

To acquire a full image of an iOS device, AXIOM Process must have privileged access to the device.

1. In AXIOM Process, click **Evidence sources** > **Mobile** > **iOS** > **Acquire evidence**.
2. Select the device to acquire, and then click **Next**.
3. Select the **Full** image type.
4. To continue setting up your case, click **Next**.

Acquiring a Kindle Fire device

AXIOM Process includes support for acquiring evidence from Kindle Fire devices. Kindle Fire uses a custom version of the Android operating system. While AXIOM Process supports acquisition of Android devices, using the Kindle Fire acquisition method provides support for Kindle-specific applications and artifacts. For example, Kindle Fire devices use the Amazon Silk browser, which uses Amazon Web Services (AWS) and stores browser-related artifacts differently than other Android devices. AXIOM Process searches the Amazon Silk browser for evidence such as remnants from AWS on the device.

In addition to acquiring evidence from a Kindle device, you can load existing images and files and folders previously acquired from the device.

To acquire evidence from a Kindle Fire device, complete the following steps:

1. In AXIOM Process, click **Evidence sources** > **Mobile** > **Kindle Fire** > **Acquire evidence**.
2. Select the device, and then click **Next**.
3. Select the type of image you want to acquire, and then click **Next**.
4. Continue setting up your case.

Acquiring media and files through MTP

Using the media transfer protocol (MTP), you can acquire media and files—including pictures, videos, audio files, documents, downloads, application data, and user data—from a media device. If other acquisition methods don't work for smartphones, MTP can sometimes bypass certain encryption methods and passwords so you can obtain a logical acquisition of the device.

You can use the MTP option with media devices that support the media transfer protocol (MTP), including: digital cameras, feature phones, and smartphones like Android, iOS, BlackBerry, and Windows Phone.

Before you begin: To acquire evidence from smartphones using MTP, the USB charging option must be set to Media Transfer Protocol.

1. In AXIOM Process, click **Evidence sources** > **Mobile** > **Media device (MTP)**.
2. Select the device, and then click **Next**.
3. Select the type of image you want to acquire, and then click **Next**.
4. Continue setting up your case.

Acquiring SIM cards

You can acquire mobile phone SIM cards and create a logical image of the SIM card files. This type of image contains all of the dedicated and elementary files available on the SIM card but is not a byte for byte copy of the SIM card.

Before you begin: Install the drivers required by your SIM card reader hardware and make sure that the SIM card reader is connected to your computer.

1. In AXIOM Process, click **Evidence sources** > **Mobile** > **SIM card**.
2. Select the SIM card, and then click **Next**.
3. Select the type of image you want to acquire, and then click **Next**.
4. Continue setting up your case.

Loading evidence from mobile devices

In addition to acquiring mobile devices, AXIOM Process can search previously acquired images, files, and folders from Android, iOS, Windows Phone, and Kindle Fire devices.

- Load a GrayKey image
- Download an image from a GrayKey device on your network

Load a mobile image

Use this option to process previously acquired images from mobile devices.

1. In AXIOM Process, click **Evidence sources** > **Mobile**.
2. Select the operating system for the image that you want to load.
3. Click **Load evidence** > **Image**.
4. Browse to the image you want to load and click **Open**.
5. Select the specific files and folders you want to load.
6. To continue setting up your case, click **Next**.

Load files and folders from a mobile device

Use this option to process previously acquired files and folders from mobile devices.

1. In AXIOM Process, click **Evidence sources** > **Mobile**.
2. Select the operating system for the files or folders that you want to load.
3. Click **Load evidence** > **Files and folders**.

4. Complete one of the following options:
    - From the displayed network or disks, browse to and select the files or folders you want to search. Click **Next**.
    - Click **Folder browser** to browse to a folder stored locally on your computer. Click **Select folder**.
    - Click **File browser** to browse to a file stored locally on your computer. Click **Open**.
5. Continue setting up your case.

Load an encrypted iOS backup

If you have an existing iOS backup that you created using iTunes, you can load the backup in AXIOM Process and provide the encryption password.

> Warning: Before you connect an iOS device to iTunes, you must first ensure that the **Prevent iPods, iPhones, and iPads from syncing automatically** option is turned on before you connect the device. If you don't turn this setting on first, there's a chance that you might contaminate your evidence by syncing external data to your device.

1. In AXIOM Process, click **Evidence sources** > **Mobile** > **iOS** > **Load evidence**.
2. Complete one of the following options:
    - To load an image of an encrypted iOS backup, click **Image**.
    - To load an encrypted backup file, click **Files and folders**.
3. Browse to the encrypted iTunes backup, and then click **Open**.
4. When prompted, provide the password, and then click **Check**.
5. Click **Okay**.
6. Continue setting up your case.

After AXIOM Process finishes searching the evidence, you'll see two evidence sources in AXIOM Examine—one for the original encrypted source and one for the decrypted backup.

Loading GrayKey images

For information about processing a GrayKey image, log in to the Customer Portal to view the Load a GrayKey image article

If you acquired an iOS device using GrayKey, you can load the images in to AXIOM Process. GrayKey provides three zip containers and a plist file:

- **files.zip**: Contains the entire file system structure of the iOS device and provides access to both system and user data.
- **backup.zip**: Contains similar information as files.zip and is structured similarly to an iTunes backup. While you can load the backup.zip file in AXIOM Process, files.zip includes the same data and more.
- **mem.zip**: Contains a memory dump of the iOS device.
- **keychain.plist**: Contains the user accounts, passwords, and keys for many of the apps that the user has saved or used.

Load a GrayKey image

To load a Graykey image, complete the following steps:

1. In AXIOM Process, click **Evidence sources** > **Mobile** > **iOS** > **Load evidence**.
2. Complete one of the following options:
    - To load the files.zip, backup.zip, or mem.zip, click **Image**.
    - To load the keychain.plist file, click **Files and folders**.
3. Browse to the GrayKey image and click **Open**.
4. To load additional GrayKey images, repeat steps 1-3.
5. To continue setting up your case, click **Next**.

Download an image from a GrayKey device on your network

Connect AXIOM Process to a GrayKey device on your network to easily download images stored on the device and add them to your case.

To connect to a GrayKey device for the first time, you'll need to provide the password for the device and authorize AXIOM Process to access the data stored on the device. After you connect to the GrayKey, you can view the results stored on the device and select the images you want to download.

> Note: AXIOM Process can only connect to an offline mode GrayKey device if the device has been updated to version 1.11.5 or later.

1. In AXIOM Process, click **Evidence sources** > **Mobile** > **iOS** > **Connect to GrayKey**.
2. In the **Hostname** field, provide the hostname for your network and click **Connect**.
3. If prompted, provide the password for the GrayKey device and click **Submit**.

4. If prompted to provide authorization for AXIOM Process to access the stored data on the GrayKey device, click **Allow**.
5. Click **Browse** and select the location where you want to save the downloaded GrayKey images. Click **Select folder**, and then click **Next**.
6. Select the device you want to view available images for, and then click **Next**.
7. Select the images you want to download from the GrayKey device, and then click **Next**.

AXIOM Process downloads the GrayKey images to the location you chose. When the download completes, AXIOM Process automatically verifies the image hashes, if applicable, and then adds the images to your case.

Supported images and file types

IMAGE/FILE TYPE	WHAT'S SUPPORTED
Advanced Forensics File images	.aff4 physical images
Archive files	.ab (Android only), .cpio, .cpio.gz, .dar (iOS only), .docx, .gz, .gzip, .pptx, .rar, .tar, .tar.gz, .tgz, .xlsx, .zip, .zip.001, .7z, .7z001
Cellebrite images	.ufd
EnCase images	.E01, Ex01, .L01, .Lx01
FTK images	.AD1
RAW images	.raw, .dd, .img, .ima, .vfd, .flp, .bif, .bin, .dmb, .dmp, .mem, .mdf
Segmented RAW dd images	.000, .001, .0000, .0001

ACQUIRING COMPUTER EVIDENCE

AXIOM Process supports acquiring and loading evidence from several computer evidence sources.

METHOD	SUPPORTED EVIDENCE SOURCE	DESCRIPTION
Acquiring evidence	Drives	Use this option to acquire evidence from drives, such as HDD, SSD, USB, and SD flash, and more. AXIOM Process supports Windows drives.
Loading evidence	Drives	Use this option to acquire evidence from drives, such as HDD, SSD, USB, and SD flash, and more. AXIOM Process supports Windows drives.
	Files and folders	Use this option to load evidence from files or folders that you have stored locally on your computer. This option supports files and folders from Windows or macOS (APFS, HFS+ and HFSX).
	Computer images	Use this option to load computer images. For information about the images that AXIOM Process supports, see the supported images and file types.
	Volume shadow copy	Use this option to locate Volume Shadow Copy files that are present on a connected Windows drive or image.
	Memory	Use this option to load Windows memory dump files.

Search types

Depending on your evidence type, you can select the type of search that you want AXIOM Process to run.

> Tip: If you don't know the type of file system that you're running a search on, the file system is not supported using a full or quick search, or you don't have a password to decrypt the drive, use the Sector level option. Selecting the Sector level option forces AXIOM Process to search an evidence source bit by bit, so it doesn't matter how the file system is structured.

SEARCH TYPE	DESCRIPTION
Full	Searches all areas of a drive or image for artifacts. This method processes fragmented files more effectively than other methods.
Quick	Searches the most common areas of your computer where evidence can be found. Common areas include default application data directories, the windows registry, user profiles, and My Documents.
Sector level	Reads raw data from the hard drive and searches for artifacts that can be carved out and pieced together from that data, with no understanding of the underlying files and folders.
Custom	A combination of any of the above options that you tailor to your specific needs.

Acquiring a drive

AXIOM Process can obtain images from many types of Windows-based external drives that are physically connected to your computer such as:

- HDD
- SSD
- USB
- SD flash drives
- Other external drives

AXIOM Process can't detect and image network-attached storage (NAS) devices over the network. If the computer that's running AXIOM Process is connected directly to the NAS with a USB cable, detection of the device and imaging work as expected.

Acquire a drive

You can search images on network drives by providing a path to the network drive using the format \\drive\-folder.

If you've installed the Passware plugin, AXIOM Process detects whether a drive is encrypted. For information about decrypting drives and cracking passwords, see Decrypting evidence.

1. In AXIOM Process, click **Evidence Sources** > **Computer** > **Windows** > **Acquire Evidence**.
2. Select a drive, and then click **Next**.
3. If prompted, provide encryption details for the drive.
4. Select the type of image you want to acquire, and then click **Next**.
5. From the **Search type** drop-down, select the type of search you want to complete for the drive.
6. To continue setting up your case, click **Next**.

Image options for drives

There are four imaging options for Windows-based drives that you can choose from. The option that you choose should reflect your time constraints and the type of data that you're looking for.

IMAGE TYPE		DESCRIPTION	EVIDENCE
Full	Entire contents of the drive in E01 format	These options represent a physical image of the drive. During this type of acquisition, AXIOM Process copies the entire contents of the drive into a single .E01 file or .raw file. These options typically take the longest.	A physical image of the entire drive.
	Entire contents of the drive in raw format		
	All files and folders	This option represents a logical image that contains all files and folders. During this type of acquisition, AXIOM Process copies all files and folders into a single, compressed .zip file. The .zip file maintains the original folder structure that existed on the drive. Depending on how many files are in the drive and the amount of logical data available, acquisition time will vary.	A full, logical file system image that includes all files and folders. This does not include deleted files and/or unallocated space.

IMAGE TYPE		DESCRIPTION	EVIDENCE
Quick	Targeted acquisition	This option represents a logical image of the drive. During this type of acquisition, AXIOM Process copies files such as system files, user profiles, and more into a single, compressed .zip file. The locations that AXIOM Process targets are typically the ones that are most likely to contain evidence. This option is typically the fastest.	Pagefile, Hibernation File, Master File Table, USN Journal, Event Logs, Setup API Logs, Windows Registry Hives, LNK Files, User Profiles, Prefetch Files

Loading a drive

You can search any locally connected Windows-based media such as computer and USB drives without first imaging them. Select any attached media or any partitions within the drive instead.

If you can't see mapped drives, you can make them visible by adding a DWORD value to the registry. For more information about creating the DWORD value, log in to the Customer Portal to review the following article: Show mapped drives in AXIOM Process.

If you've installed the Passware plugin, AXIOM Process detects whether a drive is encrypted. For information about decrypting drives and cracking passwords, see Decrypting evidence.

1. In AXIOM Process, click **Evidence Sources** > **Computer** > **Windows** > **Load evidence** > **Drive**.
2. Select the drives and partitions that you want to search, and then click **Next**.
3. If prompted, provide encryption details for the drive.
4. For each drive or partition, from the **Search type** drop-down, select the type of search you want to complete for the drive.
5. To continue setting up your case, click **Next**.

Loading an image

AXIOM Process can search Windows and macOS images from other evidence sources. For more information about the computer images that AXIOM Process supports, see the Supported images and file types.

You can also search images on network drives by providing a path to the network drive using the format \\drive\folder.

Load an image

When you load an image, if you've installed the Passware plugin, AXIOM Process can detect whether an evidence source is encrypted and the encryption method used (where possible). You can also attempt to decrypt software-encrypted evidence from an APFS-formatted macOS computer, without requiring the Passware plugin. For information about decrypting drives and cracking passwords, see Decrypting evidence.

1. In AXIOM Process, click **Evidence sources** > **Computer** > **Windows** or **Mac** > **Load evidence** > **Image**.
2. Browse to your file and click **Open**.
3. Select the partitions or specific files and folders that you want to include in your search.
4. If prompted, provide encryption details for the image.
5. To continue setting up your case, click **Next**.

Supported images and file types

IMAGE/FILE TYPE	PLATFORM	WHAT'S SUPPORTED
Advanced Forensics File images	Windows, Mac	.aff4 physical images
Archive files	Windows, Mac	.cpio, .cpio.gz, .docx, .gz, .gzip, .pptx, .rar, .tar, .tar.gz, .tgz, .xlsx, .zip, .zip.001, .7z, .7z001
EnCase images	Windows, Mac	.E01, Ex01, .L01, .Lx01
FTK images	Windows, Mac	.AD1
macOS disk images	Windows, Mac	.dmg
RAW images	Windows, Mac	.raw, .dd, .img, .ima, .vfd, .flp, .bif, .bin, .dmg, .dmp, .mem, .mdf
Segmented RAW dd images	Windows, Mac	.000, .001, .0000, .0001

IMAGE/FILE TYPE	PLATFORM	WHAT'S SUPPORTED
Virtual machine images	Windows, Mac	.vdi, .vhd, .vhdx, VMDK, XVA
UFED images	Windows, Mac	.ufd
Segmented images	Windows, Mac	.zip, .zip.001, .rar, .7z.001 When you load a segmented image, AXIOM Process automatically attempts to load all available segments.

Loading files and folders

AXIOM Process process specific files or folders that you might have stored locally on your computer. This option supports files and folders from Windows and macOS.

Load a file or folder

If you can't see mapped drives, you can browse to the mapped file's original location using the Folder browser, or you can make them visible by adding a DWORD value to the registry. For more information about creating the DWORD value, log in to the Customer Portal to review the following article: Show mapped drives in AXIOM Process.

> Note: For files and folders on a mobile operating system, use the mobile evidence source option instead.

1. In AXIOM Process, click **Evidence sources** > **Computer** > **Windows** or **Mac** > **Load evidence** > **Files and folders**.
2. Complete one of the following options:
    - From the displayed network or disks, browse to and select the files or folders you want to search, and then click **Next**.
    - Click **Folder browser** to browse to folder stored locally on your computer, and then click **Select folder**.
    - Click **File browser** to browse a file stored locally on your computer, and then click **Open**.

3. Continue setting up your case.

Supported file systems

FILE SYSTEM	TYPE	WHAT'S SUPPORTED
Linux	ext2, ext3, ext4, F2Fs	metadata
macOS	APFS, HFS+, HFSX	metadata
NAND	YAFFS2	metadata
Windows	NTFS	metadata (including metadata from the Master File Table and Windows Security), deleted files
	FAT12, FAT16, FAT32	metadata, deleted files
	exFAT	metadata

Loading a volume shadow copy

Volume shadow copy runs as a service (volume shadow service) on a Windows computer to create backups or snapshots of files or volumes (including user files).

When you complete a full search of a disk, volume shadow copies are included but sometimes provide only partial results. You can use the *Volume shadow copy* option in AXIOM Process to natively parse a volume shadow copy—this option provides more detail about where artifacts were recovered from. You can select entire volume shadow copies or expand the copy to select specific files that you want to search.

To load a volume shadow copy:

1. In AXIOM Process, click **Evidence sources** > **Computer** > **Windows** > **Load evidence** > **Volume shadow copy**.
2. Depending on your evidence source, choose one of the following options:
    - To select a connected disk, click **Drive**.
    - To select an existing image, click **Image** and browse to your file.
3. Select the shadow copies or specific files that you want to include in your search.
4. To continue setting up your case, click **Next**.

Loading memory

You can load Windows memory using the Volatility Framework. Memory dumps contain a record of all the data currently stored in memory at the time the dump occurs. These files can contain information about a user's activity on the computer that might have otherwise been lost when the system crashed or was shut down. The information available in a memory dump can be especially helpful in incident response investigations as they contain information about which processes are running and which files are opened by the user.

You can acquire a memory dump from a target's computer using Magnet RAM Capture or a third-party product.

In AXIOM Process, you can load Windows memory dumps in their native file format (for example, .raw or .bin) and scan them for artifacts just like you would with a drive. For example, you can use Volatility to search for known malware and recover the names of processes and IP addresses, giving you insight into malware investigations.

Find the profile of a memory dump

You can find the profile of a memory dump using the build number of its operating system. After you've located the build number, you can find a Volatility profile that matches the build at www.github.com/volatilityfoundation/volatility/wiki/2.6-Win-Profiles. To learn if the profile is supported by AXIOM Process, see Supported memory profiles.

To find the build number, do one of the following:

- If the memory dump was recovered from a drive that was already processed using AXIOM Process, complete the following steps:
    1. Open the case in AXIOM Examine.
    2. In the Artifacts explorer, browse to the **Operating System Information** artifact and locate the **Version Number** fragment.
- If the memory dump is on a drive that hasn't been processed, complete the following steps:
    1. On the computer where the memory dump was created, press the **Windows key** + **R** to open the Run dialog.
    2. In the **Run** dialog, type **winver** and click **OK**.
    3. In the **About Windows** dialog, locate the **OS Build number**.

Load a memory dump with a known profile

If you know the profile of a memory image, you should manually select the profile to reduce scan time.

1. In AXIOM Process, click **Evidence sources** > **Computer** > **Windows** > **Load evidence** > **Memory** > **Load memory dump file**.
2. Browse to your file and click **Open**.
3. Select **I want to select the profile myself**.
4. In the **Image profile** drop-down list, select the appropriate image profile.
5. For faster memory analysis, in the **KDbg address** field, provide the Kernel Debug (KDbg) address of the profile.
6. To continue setting up your case, click **Next**.

Load a memory dump with an unknown profile

Each memory dump has a corresponding profile, based on its operating system. If you don't know the profile of a memory dump, AXIOM Process can perform a KDbg scan to attempt to find recommended profiles.

> Warning: Performing a KDbg scan can take a significant amount of time.

1. In AXIOM Process, click **Evidence sources** > **Computer** > **Windows** > **Load evidence** > **Memory** > **Load memory dump file**.
2. Browse to your file and click **Open**.
3. Select **I want AXIOM Process to provide a list of recommended image profiles**, and then click **Next**.

   AXIOM Process performs a KDbg scan to attempt to identify the profile. You can view the results of this scan in the case summary text file in your case folder.

   Once AXIOM Process finishes identifying profiles, its recommendations appear in the **Image profile** drop-down list. If more than one recommendation appears, you can click **Advanced images profile selection** to view details about the recommended profiles and make an informed selection.

4. In the **Image profile** drop-down list, select an image profile.
5. To continue setting up your case, click **Next**.

Include memory artifacts in your search

In AXIOM Process, you can specify the individual memory artifacts that you want to include in your search.

Each artifact corresponds to a Volatility command. For example, the Processes (pslist) artifact allows you to see which processes ran on a system, and the Process Security Identifiers (getsids) artifact allows you to view the Security Identifiers associated with processes. For more information about Volatility commands that correspond to memory artifacts, see the Volatility Foundation's Command Reference.

1. In AXIOM Process, click **Artifact details** > **Computer artifacts** > **Memory**.
2. Select the memory artifacts you want to search for.
3. Continue setting up your case.

Export memory artifacts

You can use AXIOM Examine to export memory artifacts from your case to import into other tools. You can choose to export files based on their type:

- Process executable files (procdump)
- Dynamic link library files loaded by the process (dlldump)
- Memory associated with a particular process (memdump)
- Open files in memory (dumpfiles)
- Range of pages described by a VAD node (vaddump)

To export memory artifacts, complete the following steps:

1. In AXIOM Examine, right-click the memory artifact you want to export, and then click **Export memory items**.
2. In the **Export memory items** dialog, complete the following actions:
    1. In **Export details**, provide the **Folder name** and **File path** that you want to use.
    2. In **Items to include**, select the memory items that you want to export.
3. Click **Export**.

Supported memory profiles

WINDOWS VERSION	PROFILES
Windows 10	Win10x64 Win10x64_10240_17770 Win10x64_10586 Win10x64_14393 Win10x64_15063 Win10x64_16299 Win10x64_17134 Win10x64_17763 Win10x64_18362 Win10x86 Win10x86_10240_17770 Win10x86_10586 Win10x86_14393 Win10x86_15063 Win10x86_16299 Win10x86_17134 Win10x86_17763
Windows 2016	Win2016x64_14393
Windows 2012	Win2012R2x64 Win2012R2x64_18340 Win2012x64

WINDOWS VERSION	PROFILES
Windows 8	Win81U1x64 Win81U1x86 Win8SP0x86 Win8SP1x64 Win8SP1x64_18340 Win8SP1x86
Windows 7	Win7SP0x64 Win7SP0x86 Win7SP1x64 Win7SP1x64_23418 Win7SP1x64_24000 Win7SP1x86 Win7SP1x86_23418 Win7SP1x86_24000
Windows 2008	Win2008R2SP0x64 Win2008R2sP1x64 Win2008R2SP1x64_23418 Win2008R2SP1x64_24000 Win2008SP1x64 Win2008SP1x86 Win2008SP2x64 Win2008SP2x86

WINDOWS VERSION	PROFILES
Windows Vista	VistaSP0x64 VistaSP0x86 VistaSP1x64 VistaSP1x86 VistaSP2x64 VistaSP2x86
Windows 2003	Win2003SP0x86 Win2003SP1x64 Win2003SP1x86 Win2003SP2x64 Win2003SP2x86
Windows XP	WinXPSP1x64 WinXPSP2x64 WinXPSP2x86 WinXPSP3x86

Decrypting evidence

For many evidence sources, if you installed the Passware plugin, AXIOM Process detects whether an evidence source is encrypted and, where possible, the type of encryption method that was used. You can also attempt to decrypt software-encrypted evidence from an APFS-formatted macOS computer, without requiring the Passware plugin.

For supported encryption types, you can provide known decryption credentials such as passwords and recovery keys, to decrypt the evidence source before AXIOM Process searches it. For some evidence sources, if you don't know the password, you can try cracking it—otherwise, AXIOM Process attempts a sector-level search of the drive.

For Windows 10 devices that have BitLocker Device Encryption turned on (including many Microsoft Surface Pro devices), AXIOM Process will automatically try to recover a clear key from the Master Boot Record (MBR). IfAXIOM Process finds a clear key in the MBR, it will then try to decrypt the device using that password. If AXIOM Process is unable to automatically decrypt the device, you're prompted to provide known decryption credentials for the device.

In AXIOM Process, a locked icon appears beside both decrypted and encrypted partitions, as it's not guaranteed that AXIOM Process will successfully decrypt the drive.

During a search, AXIOM Process adds the decrypted evidence source and the password that successfully decrypted the evidence source to the case folder. For decrypted evidence from a macOS computer with the APFS file system, you'll find a decrypted image for each partition. Before you attempt to decrypt an evidence source, make sure you have enough space for the decrypted images.

Decrypt evidence with a known password or recovery key

If you know the password or recovery key for an evidence source, you can attempt to decrypt it. For evidence from a macOS computer with the APFS file system, AXIOM Process supports user passwords or personal recovery keys, and, in some cases, might be able to display a password hint.

1. In the **Decryption option** drop-down list, click **I have the password/recovery key**.
2. In the **Password/Recovery key** field, provide a password or recovery key.
3. To verify that the password is correct, click **Check**.
4. To finish setting up your case, click **Next**.

Decrypt a McAfee-encrypted evidence source with a machine key

If you don't know the password for a McAfee-encrypted evidence source, you can attempt to decrypt it using a machine key. Machine keys are Base64 strings that must be 44 characters long and are unique to each computer. If you provide a machine key in the correct format but the key is incorrect (for example, the key is not associated with the evidence you are trying to decrypt), AXIOM Process attempts to decrypt the evidence source but creates an image without any results.

You obtain a machine key from the McAfee administrator. You find the key at the bottom of the XML file, between the <MfeEpeExportMachineKey> tags.

In AXIOM Process, when you attempt to decrypt a drive, only the largest partition appears to be available, as McAfee encrypts entire drives and not individual partitions.

1. In the **Decryption option** drop-down list, click **I have the machine key**.
2. In the **Machine key** field, paste the 44-character machine key from the XML file.
3. To verify that the password is correct, click **Check**.
4. To continue setting up your case, click **Next**.

Decrypt a FileVault-encrypted evidence source with a password and a wipe key

You need both a password and a wipe key to decrypt a macOS (HFS+ and HFSX) evidence source that is encrypted by FileVault. To recover the wipe key, search the recovery partition of the macOS computer.

1. In AXIOM Process, click **Evidence Sources** > **Computer** > **Mac** > **Files and folders**.
2. Select the check box beside the recovery partition.
3. Finish setting up your case.
4. Once processing is complete, extract the following file: **EncryptedRoot.plist.wipekey**. This file is usually stored at **\Recovery HD\-com.apple.boot.P\System\Library\Caches\com.apple.corestorage\EncryptedRoot.plist.wipekey**.

To decrypt the evidence source:

1. In AXIOM Process, click **Evidence Sources** > **Computer** > **Mac** > **Images** or **Files and folders**.
2. Browse to or select the evidence source you want to decrypt, and then click **Next**.
3. In the **Key file** field, provide the wipe key.
4. In the **Password** field, provide the known password.
5. To verify that the password is correct, click **Check**.
6. For each item, select the type of search you want to complete.
7. To continue setting up your case, click **Next**.

Decrypt a VeraCrypt-encrypted partition with a password and a PIM

You need both a password and a Personal Iterations Multiplier (PIM) to decrypt VeraCrypt-encrypted partitions. You can use Passware to recover the PIM.

> Note: If you enter the wrong PIM, VeraCrypt won't be able to decrypt the partition.

1. In the **Decryption option** drop-down list, select **I have the password**.
2. In the **Password** field, provide the known password.

3. In the **Personal iterations multiplier** field, provide the **PIM**.
4. To verify that the PIM and password are correct, click **Check**.
5. To continue setting up your case, click **Next**.

Decrypt an evidence source by cracking the password

To crack the password of a drive, you must be using AXIOM Process with the Passware plugin. You must also have a password list file in .txt format.

With the dictionary attack capabilities of the Passware plugin, you can use custom password lists, in .txt format, to attempt to decrypt drives, mobile devices, and images. Passware reads each new line as a separate password. Additionally, Passware reads spaces at any point in the line as part of the password.

You can use the AXIOM Wordlist Generator to retrieve a list of keywords from the devices in your case. This tool writes keywords to a .txt file that you can use to decrypt drives, mobile devices, and images.

McAfee, APFS, FileVault, and VeraCrypt-encrypted evidence sources can't be decrypted using password cracking.

> Warning: Password cracking can take a significant amount of time and system resources, and isn't guaranteed to work. To save time, consider cracking encrypted sources separately from sources with known passwords.

1. In the **Decryption option** drop-down list, select **I want to crack the password**.
2. Click **Browse** and browse to the location of the .txt file.
3. To continue setting up your case, click **Next**.

The Analyze evidence screen displays the cracking progress and the number of passwords that have been attempted. If the drive is successfully decrypted, the blue locked icon changes to the blue unlocked icon and AXIOM Process begins searching the drive immediately.

If password cracking is successful, that source is skipped during processing. You can find the correct password, decryption duration, and more in the Passware XML report file. This file is located in your case folder and will have a similar name to the decrypted image.

Supported encryption types

ENCRYPTION TYPE	WHAT'S SUPPORTED
BitLocker	All versions up to and including Windows 10, including BitLocker To Go
FileVault and FileVault 2	All versions of macOS formatted with HFS+ (non-system partitions are not supported) or APFS
McAfee Drive Encryption	McAfee 7.x and later (non-system partitions are not supported)
PGP Whole Disk Encryption (PGP WDE)	PGP Desktop 9.x - 10.x (encrypted drives can't currently be decrypted using administrator credentials)
TrueCrypt	TrueCrypt 5.0 and later (hidden and system partitions are not supported)
VeraCrypt	All current versions are supported Encryption ciphers supported: AES, Serpent, Twofish Encryption ciphers not supported: Kyznyechik, Magma, Carmellia Hash functions supported: RIPEMD-160, SHA256, SHA512, Whirlpool Hash functions not supported: Streebog

ACQUIRING CLOUD EVIDENCE

To acquire evidence from the cloud, you can sign in to an account with the target's user name and password, or—for some platforms—an authentication token that AXIOM Process discovers during a search or creates itself. For some cloud platforms, you can also acquire activity that is accessible to the public.

You can acquire evidence from the following cloud platforms and services: Amazon Web Services (AWS), Apple, Box.com, Dropbox, IMAP/POP Email, Facebook, Google, Instagram, Lyft, Microsoft, Microsoft Azure, Microsoft Teams, Slack, Twitter, Uber, and WhatsApp (Google Drive backups and QR code access). For more details about what type of information you can recover, see Supported cloud platforms and services.

AXIOM Cloud is available with a valid cloud license. To find out how to purchase a cloud license, contact sales@magnetforensics.com.

Changes to supported cloud services and content

> When acquiring evidence from a cloud-based user account, AXIOM Process acquires live data. If a supported platform makes a change to their product, this change might affect the types of services or content AXIOM Process can acquire and process. For a current list of any known changes to our ability to acquire data from our supported platforms (including specific artifacts that might be impacted), please log in to the Customer Portal to read the following article: Status of supported cloud acquisition platforms.
>
> For example, Google announced that it would begin blocking logins to Google accounts from embedded browser frameworks starting in June 2019. When this change comes into effect, AXIOM Process might not be able to support WhatsApp and the following data sources for Google accounts: Google Activity, Google Timeline Locations, Google Connected Apps, Recent Devices, Passwords, and Google Hangouts. For more information, log in to the Customer Portal to read the following article: Changes to supported data sources for Google accounts.

Preparing a cloud account for acquisition

Depending on the platform and the evidence you want to acquire, you might need administrator privileges and will need to configure the administrator account to allow AXIOM Process to access data from user accounts, grant consent for the application, and more.

For more information about preparing cloud accounts for acquisition, review the following Knowledge Base articles in the Magnet Forensics Customer Portal:

PLATFORM	RESOURCES
General	• Accessing cloud accounts that use two-factor authentication • Whitelisting URLs for cloud acquisition
Amazon Web Services (AWS)	• Find AWS authentication details • Prerequisites for acquiring an EC2 instance
Box.com	• Configure a Box.com account for acquisition
Google	• Configure the Google Admin console to give access to G Suite user accounts • Configure a Gmail account to allow access using IMAP/POP
Microsoft	• Configure Microsoft Azure to give access to Microsoft user accounts • Configure an Office 365 account for acquisition • Give examiners access to users' Office 365 Sharepoint and OneDrive accounts
Microsoft Azure	• Find Azure authentication details
Microsoft Teams	• Configure Microsoft Azure to give access to Microsoft Teams
Slack	• Configure Slack to allow access to AXIOM Process
Yahoo	• Configure a Yahoo account to allow access using IMAP/POP

Acquiring evidence from a cloud-based user account

When you create a new case in AXIOM Process, you can acquire a single account for each cloud platform or service. If you want to add additional accounts, add them as a new evidence source after the original search completes.

After your search completes, you can find the login credentials for each cloud account that you acquire in the **Cloud Accounts Information** artifact in AXIOM Examine so that you can easily acquire additional information from the account later. You can also acquire additional information from the cloud by using passwords and tokens found during a search or decrypting a WhatsApp backup using a recovered decryption key.

Acquired cloud data is saved as a .zip file. Each service and platform is saved in a separate folder, each containing an attachments folder. The files are saved in the same structure that appears in the account online and in the File system view in AXIOM Examine.

If your agency requires that you use AXIOM Process through a proxy server, you can still use AXIOM Cloud to acquire users' accounts for Box.com, Dropbox, Facebook, Google, Instagram, and Microsoft. For more information about how to use AXIOM Process through a proxy server, see Connect to the internet using a system proxy.

Step 1: Sign in to a cloud account

Acquire evidence from many cloud-based platforms by logging in to an account with a user's login information in AXIOM Process. For some platforms, you can also sign in to a user's account using a QR code or authentication tokens that AXIOM Process discovers during a search or creates itself—though some cloud platforms have services and content that can't be acquired when you use a token to authenticate. IMAP/POP email, Instagram, and Twitter don't support authentication tokens.

> Note: To acquire evidence for Microsoft Teams, make sure you sign in to the user account for the user you want to acquire chats from.

> Tip: If you are having trouble signing in to a Microsoft cloud account using the user name and password sign in method, try signing in to the account using external browser authentication. Audit logs can't be collected using this authentication method.

1. In AXIOM Process, click **Evidence sources** > **Cloud** > **Acquire evidence**.
2. Confirm that you have proper search authorization.
3. Click the platform that you want to sign in to.
4. Follow the instructions in AXIOM Process to sign in to the account. Depending on the platform or user account, you might be prompted to:
   - Provide login information (such as a user name and password)
   - Scan a QR code
   - Provide a token
   - Provide two-factor authentication information or a verification code
   - Provide additional details (for example, for IMAP/POP email, you must select a protocol and provide the Server port and Host name).

> Note: When AXIOM Process gains access to an account, the owner of the account might receive an e-

> mail notifying them that someone has signed in to their account.

Step 2: Select a date range

After you gain access to a cloud account, you can select a date range to acquire data from. By default, AXIOM Process acquires data from as far back in time as possible for the account. Acquiring some accounts can take a long time depending on the amount of data they contain, so you might want to narrow the date range to decrease the amount of time the acquisition takes.

1. In the **Date range** drop-down list, select one of the following options:
   - To acquire data *after* a specified date, click **After**.
   - To acquire data *before* a specified date, click **Before**.
   - To acquire data *between* two specified dates, click **Custom date range**.
2. Click the **calendar icon** and choose a date.

> Note: Some services don't use the date range for acquisition even if you specify one. In these cases, AXIOM Process allows you to specify a date range, but acquires and displays data for all available dates. This behavior applies to Apple iCloud backups and Google connected apps, passwords, and recent devices.

Step 3: Select services and content

After you gain access to a cloud account, you can specify which services and content you want to acquire. By default, AXIOM Process selects all available services and content.

1. In **Select services and content**, complete the following actions:
   - Services: In the **Service** column, select or clear the check box for each service.
   - Content: If available, in the **Content** column, click **Edit**. Select or clear the check box for each item, and then click **Next**.
2. When you've finished selecting services and content, click **Next** to continue setting up your case.

Acquiring evidence from an Amazon EC2 instance

When you create a new case in AXIOM Process, you can acquire a single EC2 instance with a single S3 bucket. If you want to acquire additional instances, add them as a new evidence source after the original search completes.

AXIOM Process supports acquiring EC2 instances for Amazon Linux and Ubuntu Server SSD volume types.

Amazon does not allow direct downloading from an EC2 instance, so to acquire evidence from an EC2 instance, AXIOM Process initiates an export in AWS which copies the EC2 instance and its associated drives to create an image. AWS then exports this image to an S3 bucket.

When acquiring an EC2 instance, you do not need to specify a date range. Date ranges are applicable to directly acquiring S3 buckets only.

> Note: There are typically costs associated with transferring data from AWS over the internet to a local machine. When you acquire evidence from AWS, you might be charged a nominal fee per GB of data downloaded based on your storage plan. For more information about specific charges you might incur, please consult the Amazon S3 pricing plans.

Prerequisites for acquiring an EC2 instance

To acquire evidence from an Amazon EC2 instance, there are several prerequisites and additional considerations you should be aware of. For detailed information about these prerequisites, review the Prerequisites for acquiring an EC2 instance article in the Magnet Forensics Customer Portal.

Step 1: Sign in to an AWS account

To sign in to and acquire an EC2 instance, you must provide authentication details for the AWS account required for your organization's AWS configuration. Depending on your organization's AWS configuration, you might be prompted to provide additional authentication details. You can find these authentication details in the AWS Management Console. For more information about how to find each of the required authentication details, review the Find AWS authentication details article in the Magnet Forensics Customer Portal.

1. In AXIOM Process, click **Evidence sources** > **Cloud** > **Acquire evidence**.
2. Confirm that you have proper search authorization.
3. Click **Amazon**.
4. Provide the required authentication details for the AWS account.
5. Click **Sign in**.

Step 2: Select services and content

After you gain access to the AWS account, you can specify that you want to acquire an EC2 instance, and then select the EC2 instance that you want to download.

1. In **Select services and content**, select the **Amazon EC2 instances** source type option.
2. In the **Content** column, click **Edit.**
3. In the **Select EC2 instances to download** section, search for the EC2 instance or click **View all instances**.
4. In the table, select the EC2 instance that you want to download, and then click **Next**.

Step 3: Define export details

To download an EC2 instance, AXIOM Process initiates an export in AWS. This export copies the EC2 instance and all of the drives associated with it to create an image. Next, AWS exports the image to an S3 bucket.

To export an image to an S3 bucket, you must provide some information about the export such as the disk image format and the S3 bucket you want to export the image to. To help organize your evidence in the S3 bucket, you can optionally provide a prefix to add to the name of the image of the EC2 instance. For example, you could add the target's name as the prefix value.

AXIOM Process supports VHD, VMDK, and RAW disc images formats for images of an EC2 instance.

1. In the **Export description** field, provide a description for the exported EC2 instance.
2. In the **Disk image format** drop-down, select a format for the image of the exported EC2 instance.
3. In the **S3 bucket** drop-down, select the S3 bucket you want to export the image of the EC2 instance to.
4. In the **S3 prefix** field, optionally provide a prefix to add to the name of the image of the EC2 instance.
5. When you've finished selecting services and content, click **Next** to continue setting up your case.

> Note: Storing an image of an EC2 instance in an S3 bucket might incur monthly costs. After you've successfully acquired the EC2 instance, consider removing the image from the S3 bucket to avoid additional expenses.

Acquiring evidence from an Amazon S3 bucket

Step 1: Sign in to an AWS account

To sign in to and acquire S3 buckets, you must provide authentication details for the AWS account required for your organization's AWS configuration. Depending on your organization's AWS configuration, you might be prompted to provide additional authentication details. You can find these authentication details in the AWS Management Console. For more information about how to find each of the required authentication details, review the Find AWS authentication details article in the Magnet Forensics Customer Portal.

1. In AXIOM Process, click **Evidence sources** > **Cloud** > **Acquire evidence**.
2. Confirm that you have proper search authorization.
3. Click **Amazon**.
4. Provide the required authentication details for the AWS account.
5. Click **Sign in**.

Step 2: Select a date range

After you gain access to the Amazon account, you can select a date range to acquire data from. By default, AXIOM Process acquires data from as far back in time as possible for the account. Acquiring some accounts can take a long time depending on the amount of data they contain, so you might want to narrow the date range to decrease the amount of time the acquisition takes.

1. In the **Date range** drop-down list, select one of the following options:
   - To acquire data *after* a specified date, click **After**.
   - To acquire data *before* a specified date, click **Before**.
   - To acquire data *between* two specified dates, click **Custom date range**.
2. Click the **calendar icon** and choose a date.

Step 3: Select services and content

After you gain access to the AWS account, you can specify that you want to acquire an S3 bucket, and then select the buckets or files that you want to download.

1. In **Select services and content**, select the **Amazon S3 files** source type option.
2. In the **Content** column, click **Edit.**
3. Select the buckets or files that you want to acquire.
4. To continue setting up your case, click **Next**

Acquiring public activity

You can acquire publicly available activity from Twitter and Instagram without requiring login information for specific users. When you create a new case in AXIOM Process, you can acquire a single date range and user name for each platform. If you want to search for additional date ranges and user names, you can add them as a new evidence source after the original search completes.

In some situations, Magnet AXIOM might not be able to acquire public Twitter activity, such as Retweets, content filtered by Twitter from public search results, protected Tweets, user accounts that are not completely configured, or Tweets that are not part of the supported history of the Twitter Standard Search API. Additionally, the returned results might vary depending on which Tweets the Twitter algorithms make available on the Advanced Search page at a given time. AXIOM Process might not be able to acquire some public Instagram activity, such as if the Instagram posts are private.

> Note: Depending on the amount of data available, acquiring public activity can take a long time, so you should narrow the date range to decrease the amount of time the acquisition takes and to find the most important evidence.

Acquire public activity from Twitter or Instagram

When you search for publicly available activity from a specific user name, include the complete handle. Make sure that you include the @ symbol (for example, @MagnetForensics) and format the user name correctly. For example, Twitter user names must be less than 15 characters and include only alphanumeric characters (letters A-Z and numbers 0-9) and underscores. Instagram user names must be less than 30 characters and can include letters, numbers, periods and underscores. When you search for publicly available activity from a specific hashtag, make sure that you include the # symbol (for example, #MagnetForensics).

1. In AXIOM Process, click **Evidence sources** > **Cloud** > **Acquire evidence**.
2. Confirm that you have proper search authorization.
3. Click **Instagram** or **Twitter**, and then select the **Public activity** access method.

4. In the **Date range** drop-down list, choose one of the following options:
    - To acquire data *after* a specified date, click **After**.
    - To acquire data *before* a specified date, click **Before**.
    - To acquire data *between* two specified dates, click **Custom date range**.
5. Click the **calendar icon** and choose a date.
6. In the **User name** or **Hashtag** field, provide the user name of the account whose public activity you want to acquire or provide the hashtag you want to search for.
7. Select the services and content you want to acquire.
8. To continue setting up your case, click **Next**.

Supported cloud platforms and services

PLATFORM / SERVICE	AXIOM CLOUD	MAGNET AXIOM CYBER	SERVICES / CONTENT	LAST ACTIVITY	SIZE	DATE RANGE LOGIC
Amazon Web Services		●	Amazon S3 Buckets Amazon EC2 Instances	—	—	Files modified or created within the date range
Apple	●	●	iCloud Backups (three most recent backups for each device in the account) iCloud Drive files and recently deleted files iCloud Mail iCloud Photos	Photos only	Includes all photos	Files modified, created, or accessed within the date range

PLATFORM / SERVICE	AXIOM CLOUD	MAGNET AXIOM CYBER	SERVICES / CONTENT	LAST ACTIVITY	SIZE	DATE RANGE LOGIC
Box.com (User)	●	●	Files and folders User Events	Last modified of any files or folders	Includes all files and folders	Files modified, created, or accessed within the date range
Box.com (Admin)		●	Files and folders from other accounts (if target has administrative privileges) Enterprise Events	Last modified of any files or folders	Includes all files and folders	Files modified, created, or accessed within the date range
Dropbox	●	●	Files and folders	Last modified of any files or folders	Includes all files and folders	Files with server last accessed, client accessed, or time taken within the date range, including files that match the "from" date and "to" date

PLATFORM / SERVICE	AXIOM CLOUD	MAGNET AXIOM CYBER	SERVICES / CONTENT	LAST ACTIVITY	SIZE	DATE RANGE LOGIC
Facebook	●	●	Facebook Friends Facebook Messenger Facebook Posts Facebook Profile Facebook Timeline	—	—	Posts and messages posted or sent within the date range

PLATFORM / SERVICE	AXIOM CLOUD	MAGNET AXIOM CYBER	SERVICES / CONTENT	LAST ACTIVITY	SIZE	DATE RANGE LOGIC
Google (User)	●	●	Gmail Messages Google Accounts (including activity, connected apps, passwords, recent devices, and timeline) Google Drive (files and folders) Google Hangouts Google Photos Google Takeout (including Activity, Calendar Events, Contacts, Hangouts, Location History, Mbox from Gmail, Chrome, Tasks, Activity, Keep, and Photos) Google Activ-	—	Includes Messages, Drive, and Photos	Files modified, created, or accessed within the date range

PLATFORM / SERVICE	AXIOM CLOUD	MAGNET AXIOM CYBER	SERVICES / CONTENT	LAST ACTIVITY	SIZE	DATE RANGE LOGIC
			ity (including activity and attachments)			
Google (G Suite Admin)		●	Services and content listed for Google (User) G Suite administrator and user accounts G Suite login audit logs for G Suite Basic, Business, and Enterprise G Suite Drive audit logs for G Suite Business and Enterprise	—	Includes Messages, Drive, and Photos	Files modified, created, or accessed within the date range
IMAP / POP	●	●	Emails and attachments Note: POP3 does not support folder acquisition and acquires the inbox only.	—	—	Emails modified, created, or accessed within the chosen date range

PLATFORM / SERVICE	AXIOM CLOUD	MAGNET AXIOM CYBER	SERVICES / CONTENT	LAST ACTIVITY	SIZE	DATE RANGE LOGIC
Instagram (User account)	●	●	Instagram Direct Messages Instagram Posts	Date of most recent post	Includes total amount of posts	Posts uploaded or messages sent within the date range
Instagram (Public activity)	●	●	Instagram Posts	—	—	Posts from the user name or hash tag posted within the date range
Lyft	●	●	Profile information Trip data	—	—	Trip data from within the date range

PLATFORM / SERVICE	AXIOM CLOUD	MAGNET AXIOM CYBER	SERVICES / CONTENT	LAST ACTIVITY	SIZE	DATE RANGE LOGIC
Microsoft (User)	●	●	Office 365/Microsoft Mail (including hosted services: Hotmail, Outlook, MSN, and Live) OneDrive files and folders Office 365 Outlook contacts Office 365 Outlook calendars	Newest of last modified, last accessed, and last created files (OneDrive only)	Includes all files and folders (OneDrive only)	Files modified, created, or accessed within the date range

PLATFORM / SERVICE	AXIOM CLOUD	MAGNET AXIOM CYBER	SERVICES / CONTENT	LAST ACTIVITY	SIZE	DATE RANGE LOGIC
Microsoft (Office 365 Admin)		●	Services and content listed for Microsoft (User) Audit logs Emails, OneDrive, Audit logs (if enabled) from other accounts (if target has administrative privileges) SharePoint files and folders	Newest of last modified, last accessed, and last created files (OneDrive only)	Includes all files and folders (OneDrive only)	Files modified, created, or accessed within the date range
Microsoft Azure		●	Virtual Machines	—	—	—
Microsoft Teams		●	Channels Chats	—	—	Messages sent within the date range.

PLATFORM / SERVICE	AXIOM CLOUD	MAGNET AXIOM CYBER	SERVICES / CONTENT	LAST ACTIVITY	SIZE	DATE RANGE LOGIC
Slack		●	Slack Public Channels Slack Private Channels Slack Direct Messages Slack Direct Group Messages Slack Users Slack Workspaces	—	—	Messages sent within the date range
Twitter (User account)	●	●	Twitter Direct Messages Twitter Posts Twitter Users (including followers, friends, and personal profile) information	Based on latest Tweets	Includes total amount of Tweets	Tweets posted within the date range
Twitter (Public activity)	●	●	Twitter Posts Twitter Users (including followers, friends, and personal profile) information	—	—	Tweets from the user name posted within the date range

PLATFORM / SERVICE	AXIOM CLOUD	MAGNET AXIOM CYBER	SERVICES / CONTENT	LAST ACTIVITY	SIZE	DATE RANGE LOGIC
Uber	●	●	Uber Trip History	—	—	Trip history within the date range
WhatsApp (Google Drive Backup)	●	●	WhatsApp backups	—	Includes all data backed up to Google Drive	Date that the backup was saved to Google Drive
WhatsApp (QR code access)	●	●	WhatsApp chats	—	—	Chats within the date range

Loading cloud evidence

You can load the following cloud-based evidence sources: AXIOM Cloud images, Apple warrant returns, Facebook warrant returns, Facebook Download Your Information archives, Instagram warrant returns, Google Takeout archives, Google warrant returns, iCloud backups, Microsoft Office 365 Unified Audit Logs, Skype warrant returns, Slack archives, and Snapchat warrant returns.

When you acquire a cloud evidence source, AXIOM Process creates a .zip file containing the hashed cloud image. You can load this cloud image into AXIOM Processif you want to process the evidence as a part of another case.

> Note: Magnet AXIOM allows you to load and process warrant return files provided by Apple, Facebook, Instagram, and Snapchat. Sometimes, the platform providing the warrant return file make changes to its format which might impact the ability for Magnet AXIOM to process the warrant return package.
>
> For a current list of any known changes to our ability to process warrant returns and the approximate dates of warrant returns Magnet AXIOM is known to support, please log in to the Customer Portal to read the following article: Status of supported cloud acquisition platforms. If you are unable to process a warrant return outside of these dates, please contact the Magnet Forensics Technical Support team.

Load a cloud image

Before you load a cloud image, make sure you have the appropriate user permissions to access the file.

If you're loading an Apple warrant return, make sure you decrypt the package using the instructions provided by Apple. After you've decrypted the package, AXIOM Process can decrypt encrypted backups contained within the decrypted warrant return.

1. In AXIOM Process, click **Evidence sources** > **Cloud** > **Load evidence**.
2. Select the type of image you want to load.
3. Browse to the image and click **Open**.
4. To continue setting up your case, click **Next**.

> Note: If you load an AXIOM Cloud .zip file that was created in a newer version of AXIOM Process than the version you are currently using, it's possible that you might recover less evidence.

Supported evidence sources

You can load the following cloud evidence sources in AXIOM Process:

PLATFORM	AXIOM CLOUD	MAGNET AXIOM CYBER	IMAGE TYPE	DESCRIPTION
Apple	●	●	iCloud backup	Use this option to load manifest.plist files generated for encrypted and non-encrypted iTunes backups.
	●	●	Warrant return	Use this option to load .zip files provided by Apple for warrant returns.
Facebook	●	●	Warrant return	Use this option to load .zip files provided by Facebook for warrant returns.
	●	●	Download Your Information	Use this option to load .zip files generated from the Download Your Information (JSON) option in Facebook.

PLATFORM	AXIOM CLOUD	MAGNET AXIOM CYBER	IMAGE TYPE	DESCRIPTION
Google	●	●	Google Takeout	Use this option to load .mbox files, and .zip files that are generated when a Google Takeout archive is created.
	●	●	Warrant return	Use this option to load .zip files provided by Google for warrant returns.
Instagram	●	●	Warrant return	Use this option to load .zip files provided by Instagram for warrant returns.
Magnet Forensics	●	●	AXIOM Cloud image	Use this option to load an AXIOM Cloud image that has already been acquired.
Microsoft Office 365 Unified Audit Logs		●	Audit logs	Use this option to load Microsoft Unified Audit log .csv files generated using the Microsoft Security and Compliance Center.
Skype	●	●	Warrant return	Use this option to load .zip files provided by Skype / Microsoft for warrant returns.
Slack		●	Slack archives	Use this option to load .zip files of Slack archives (JSON) files generated from the standard and corporate workspace data exports in Slack.
Snapchat	●	●	Warrant return	Use this option to load .zip files provided by Snapchat for warrant returns.

ADDING KEYWORDS TO A SEARCH

Using keywords and regular expressions, you can quickly and precisely search large amounts of text in the evidence. You can add keywords and regular expressions to your search in AXIOM Process. Keywords that you include in your search are added to the Keywords filter in the Artifacts explorer in AXIOM Examine.

A regular expression is a pattern that you define using a sequence of letters, numbers, and special characters. Magnet AXIOM supports the .NET Framework syntax for creating regular expressions. For more information about creating regular expressions, see the Microsoft Regular Expression Language Quick Reference.

Add keywords to search

If you have a lot of search terms to filter on or want to search more than just artifacts, add keywords and regular expressions in AXIOM Process before you start a search. You can add individual search terms or keyword lists that contain multiple items.

Keyword lists must be .txt files and each search term must appear on a new line. A single file can contain both keywords and regular expressions. Keyword lists that contain ASCII characters default to the ASCII encoding type. If a keyword list contains non-ASCII characters, AXIOM Process defaults only those non-ASCII characters to be encoded as UFT-8.

1. In AXIOM Process, click **Processing details** > **Add keywords to search**.
2. Select the type of keyword search you want to perform.
3. Add keyword lists or individual keywords.
4. If applicable, in the **Encoding** drop-down list, select the encoding type of your keyword or keyword list. If you're not sure which encoding type to use, select them all.
5. For each keyword that is a regular expression, select the **Regex / GREP** option beside the term.
6. If you want to perform a case-sensitive search, select the **Case sensitive** option next to the search term or keyword list.
7. Continue setting up your case.

Keyword search types

TYPE OF SEARCH	DESCRIPTION
Artifacts	Artifact keyword searching looks for keywords in only the artifacts that AXIOM Process can recover. As part of this process, encrypted or encoded artifacts are decrypted into plain text that can be searched using keywords. Search results are limited to the artifacts that AXIOM Process supports, but hits are found quickly. In AXIOM Examine, each of the keywords and regular expressions that you get a result on are added to the Keywords filter. You can turn on or turn off an entire list of items by clicking on the file name.
All content	Searching for keywords in all content is a byte for byte search of data in the encoding type that you specify. AXIOM Process supports ASCII as well as UTF-7, UTF-8, UTF-16, and UTF-32 (Little Endian). AXIOM Process looks for keywords across the entire evidence source—not just the artifacts that it recovers. Searching all content for keywords can increase processing time significantly, but AXIOM Process can find hits in data (including deleted content) without a corresponding artifact type. In AXIOM Examine, in the Artifacts explorer, each of the keywords and regular expressions that you get a result on are added as new keyword snippets. If a keyword result is found on an item that is both an artifact and resides in the file system (for example a result on a document discovered in unallocated space) the keyword is counted twice. It appears as a result on the artifact itself and as a new Keyword Snippet.

SEARCHING ARCHIVES AND MOBILE BACKUPS

During processing, AXIOM Process can search archive files (such as .zip and .tar files) and mobile backup files (such as Android backup (.ab) files and iOS backup folders). To search mobile backups, the mobile backup files must be decrypted. You can provide potential passwords for AXIOM Process to use to decrypt the device. You can also choose the number of layers of nested archives and mobile backups that AXIOM Process searches.

After processing completes, you can open and search the contents of any discovered archives or mobile backups in AXIOM Examine.

Search archives and mobile backups

1. In AXIOM Process, click **Processing details** > **Search archives and mobile backups**.
2. To search archive files, click the **Search archives** option.
3. Tosearch mobile backups, click the **Search mobile backups** option. Make sure you add potential passwords for AXIOM Process to use to decrypt the device.
4. Continue setting up your case.

Decrypt mobile backups

For AXIOM Process to search mobile backups, the mobile backup files must be decrypted. Add potential passwords for AXIOM Process to use to decrypt the device.

1. In AXIOM Process, click **Processing details** > **Search archives and mobile backups**.
2. In the **Mobile backup passwords** field, provide each potential password on its own line.
3. Continue setting up your case.

Set the number of nested archive and mobile backup search layers

You can choose the number of layers of nested archives and mobile backups that AXIOM Process searches (to a maximum of 100 layers).

1. In AXIOM Process, click **Processing details** > **Search archives and mobile backups**.
2. In the **Nested archives and mobile backups** field, type the number of nested archive and mobile backup layers that you want AXIOM Process to search for.
3. Continue setting up your case.

Turn off searching for archives and mobile backups

If you turn off these settings, AXIOM Process will not search for nested archives or mobile backups.

1. In AXIOM Process, click **Processing details** > **Search archives and mobile backups**.
2. To turn off searching archives, clear the **Search archives** option.
3. To turn off searching mobile backups, clear the **Search mobile backups** option.
4. Continue setting up your case.

CALCULATING HASH VALUES

Evidence sources can contain thousands of files, including known files that are critical to an investigation and common files that are not relevant. Searching through and categorizing each file can be a very time consuming task.

By calculating hash values for all files and importing hash sets of known files, AXIOM Process automatically searches and categorizes evidence for you. AXIOM Process remembers your previous selections the next time you create a new case or add evidence to an existing case.

Calculate hash values for all files

During a search, AXIOM Process can calculate unique hash values for each file. In AXIOM Examine, you can then quickly search for, compare, or filter those files based on known hash sets (for example, NSRL hash sets).

Calculating hash values slows down processing times. By default, files larger than 500 MB will not be hashed though you can customize the file size limit for hashing.

1. In AXIOM Process, click **Processing details** > **Calculate hash values**.
2. In **Calculate hash values for all files**, select the **Calculate hash values for all files** option.
3. Continue setting up your case.

Import hash lists for known files

If you want to quickly see if known files exist in your evidence, you can import a list of hash values for files that might be of interest to your case.

Hash lists must be .txt files containing MD5 or SHA1 hashes (such as NSRL files), with each hash on a separate line. After you add a hash list, you can provide a tag that gets applied to the files. You can view the matching files in the File system explorer in AXIOM Examine.

1. In AXIOM Process, click **Processing details** > **Calculate hash values**.
2. In **Tag files with matching hash values**, click **Add file**.
3. Browse to the location where you saved the hash list and click **Open**.

4. If applicable, clear the **Enabled** option next to any previously imported hash list files that you don't want to use for this search.
5. In the **Tag** field, provide a name for the tag.
6. Continue setting up your case.

Ignore non-relevant files in a search

If you don’t want common operating system files like icons, wallpapers, system files, and so on to clutter up your evidence, you can exclude them by providing their hash values in a hash set. Ignoring non-relevant files is subject to the specified Set a size limit for hash files.

Hash lists must be .txt files containing MD5 hashes (such as NSRL files), with each hash declared on its own line. After you add a hash set, you can provide a tag that gets applied to the files. Even though the files are excluded from the Artifacts explorer, you can still view the files and the tag that is applied to them in the File system explorer.

1. In AXIOM Process, click **Processing details** > **Calculate hash values**.
2. In **Ignore non-relevant files**, click **Add file**.
3. Browse to the location where you saved the hash sets, and then click **Open**.
4. If applicable, clear the **Enabled** option next to any previously imported hash sets that you don't want to use for this search.
5. Continue setting up your case.

Customizing hash settings

Set the format for hash values

AXIOM Process can create hash values in MD5 and SHA1 formats.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Hashing** > **Hash formats**, in the drop-down list, select the hashing format that you want to use.

Set a size limit for hash files

When you set up a search, you can add files that contain hash values. AXIOM Process then uses these values to ignore non-relevant files or automatically categorize pictures. In either case, AXIOM Process must hash every file it encounters during a search to compare to the hash lists. Hashing very large files can take a long time, so you can set the maximum size of files to hash to help improve search times. The default value is 500 MB.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Hashing** > **File size limit for hashing**, select the **To optimize processing time, don't calculate hashes for files larger than** option.
3. Type the maximum file size (in MB) that you want to create hash values for.
4. Click **Okay**.

Set the location where you store hash values

You can change the location where imported hash sets are stored. If you change the location where imported hash values are stored, AXIOM Process must restart to apply the change.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Hashing** >**Hash value storage location**, browse to the location you want imported hash values to be stored and click **Select folder**.
3. Click **Okay**.

To apply the changed location of the hash set database, AXIOM Process must restart.

If the hash set on your computer isn't stored in the new location that you choose, AXIOM Process must move it to the new location before it restarts.

If there is no hash set on your computer, AXIOM Process creates an empty HashList.db file at the new location you choose before it restarts.

CATEGORIZING EVIDENCE WITH MAGNET.AI

Using machine learning models trained with real data sets, Magnet.AI helps you quickly identify chats and pictures of interest in your case. Magnet.AI tags content that it discovers in key artifacts, providing you with a convenient starting point for your investigation.

Categorizing chats

Magnet.AI chat categorization can detect possible grooming/luring and sexual content in chat messages. When Magnet.AI categorizes chat messages, it tags the entire conversation or a group of messages in the conversation.

Currently, Magnet.AI supports categorization of chat messages in English only.

Start categorizing chats after processing completes

You can configure AXIOM Process so that AXIOM Examine begins categorizing chats immediately after your case finishes processing.

1. In AXIOM Process, click **Processing details** > **Categorize chats**.
2. Under **Categorize chats with Magnet.AI**, select the chat categories you want Magnet.AI to categorize.
3. Continue setting up your case.

Categorize chats in your case

If you didn't previously configure AXIOM Process to categorize chats immediately after your case finished processing, you can start categorizing chats from AXIOM Examine.

Using Magnet.AI can be resource intensive. You can configure how Magnet AXIOM allocates system resources to either prioritize categorizing evidence with Magnet.AI quickly or to allow you to continue to reviewing evidence in AXIOM Examine while Magnet.AI is still processing.

1. In AXIOM Examine, on the **Process** menu, click **Categorize chats with Magnet.AI**.
2. In the **System resource allocation** drop-down list, choose how you want Magnet AXIOM to allocate system resources while categorizing chats.
3. Select the chat messages you want Magnet.AI to categorize, and then click **Next**.

4. Select the chat categories you want Magnet.AI to categorize.
5. Click **Categorize chats**.

While Magnet.AI categorization is in progress, you can view the evidence that has already been categorized. In the status bar, click **Show results**.

Categorizing pictures

Magnet.AI picture categorization can detect the following possible items in pictures or files that contain pictures (such as pictures embedded in a .doc file)

- Bedrooms
- Buildings (exterior)
- Child abuse
- Documents (cards and IDs)
- Documents (paper)
- Droves/UAVs
- Drugs
- Hate symbols
- Human faces
- License plates
- Militants
- Money
- Nudity
- Screen captures
- Vehicles (cars, trucks, vans, and buses)
- Weapons

Depending on the number of pictures being categorized in the case, categorizing pictures might take a while. Some categories, such as hate symbols, human faces, and license plates, require additional processing time. While Magnet.AI is still processing, you can continue to review the evidence in AXIOM Examine.

When you categorize pictures using Magnet.AI, if Magnet AXIOM detects a GPU on your computer, and the GPU has more than 126 MB of free memory, it automatically attempts to use it. Using a GPU instead of a CPU can significantly decrease the time it takes to categorize pictures.

Start categorizing pictures after processing completes

You can configure AXIOM Examine to categorize pictures immediately after your case finishes processing.

> Tip: When categorizing pictures with Magnet.AI, we recommend that you save picture attachments to the case rather than access them from the original source. For more information, see Save picture attachments to the case.

1. In AXIOM Process, click **Processing details** > **Categorize pictures and videos**.
2. Under **Categorize pictures with Magnet.AI**, select the picture categories you want Magnet.AI to categorize.
3. Continue setting up your case.

Categorize pictures in your case

If you didn't previously configure AXIOM Process to categorize pictures immediately after your case finished processing, you can start categorizing chats from AXIOM Examine.

Using Magnet.AI can be resource intensive. You can configure how Magnet AXIOM allocates system resources to either prioritize categorizing evidence with Magnet.AI quickly or to allow you to continue to reviewing evidence in AXIOM Examine while Magnet.AI is still processing.

1. In AXIOM Examine, on the **Process** menu, click **Categorize chats with Magnet.AI**.
2. In the **System resource allocation** drop-down list, choose how you want Magnet AXIOM to allocate system resources while categorizing pictures.
3. Select the pictures you want Magnet.AI to categorize, and then click **Next**.
4. Select the picture categories you want Magnet.AI to categorize.
5. Click **Categorize pictures**.

While Magnet.AI categorization is in progress, you can view the evidence that has already been categorized. In the status bar, click **Show results**.

Remove a tag from categorized chats and pictures

If you think that Magnet.AI has incorrectly categorized evidence, you can remove the tag.

1. In AXIOM Examine, right-click the tagged evidence.
2. Click **Add/remove tag**.
3. Click an existing tag to remove it.

FINDING SIMILAR PICTURES WITH MAGNET.AI

Using content-based image retrieval technology, Magnet.AI helps you identify pictures that are similar to each other in your case.

Before you can find similar pictures, you must build picture comparison so that Magnet.AI can analyze the content of each picture file. Once picture comparison is built, you can select a reference picture, and then find other pictures that have similar features.

Magnet.AI finds similar pictures based on a picture's general attributes, rather than specific details such as small objects or faces. Use Magnet.AI to help you find other pictures that are generally similar, such as pictures of the same room or pictures with similar scenery.

AXIOM Examine displays matching results in the Thumbnail view in the Artifacts explorer and sorts the pictures automatically so that the most similar pictures appear at the top.

Optimize the performance of Magnet.AI

To find similar pictures, Magnet.AI must create a large database. For optimal performance of this feature, follow the recommendations below.

- Make sure you have enough space to store the data. Each picture needs approximately 8 KB of space to store the data that Magnet.AI produces.
- Store your case files on an SSD rather than a fixed or external drive. While Magnet.AI can analyze pictures stored on fixed or external drives, performance will not be as efficient.
- Use a computer with a GPU. When you build picture comparison using Magnet.AI, if Magnet AXIOM detects a GPU on your computer with more than 126 MB of free memory, it automatically attempts to use it. Using a GPU instead of a CPU can significantly decrease the time it takes to build picture comparison.

For more information about the recommended system requirements in Magnet AXIOM, review the System requirements: Magnet AXIOM and Optimize the performance of Magnet AXIOM articles in the Customer Portal.

Build picture comparison to find similar pictures

Before you find similar pictures, you must build picture comparison in your case so that Magnet.AI can analyze each picture file.

If you haven't changed the setting to build picture comparison automatically, or performed any picture categorization using Magnet.AI, you must manually trigger building picture comparison in your case. If you add more evidence to your case, you must build picture comparison again for new picture files to be included in similar picture searches. Magnet.AI will only analyze the new picture files.

In AXIOM Examine, on the **Tools** menu, click **Build picture comparison**. Picture comparison will build in the background while you continue working in your case.

Build picture comparison automatically

By default, you must manually trigger building picture comparison in your case. You can also customize Magnet AXIOM to automatically build picture comparison for all cases going forward.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. Under **Post-processing**, select **Automatically build picture comparison on case open**.
3. Click **Okay**.

Or, you can set picture comparison to build automatically after you process your case.

1. In AXIOM Process, click **Categorize pictures and videos**.
2. Under **Build picture comparison**, select the checkbox.
3. Continue setting up your case

If you turn on this setting using either method, it will remain on for the next case unless you deselect it again.

Finding similar pictures

After you've built comparison for the pictures in your case, you can select a reference picture that you want to find similar pictures for. You can either select a reference picture from your case, or you can import an external picture.

> Note: Magnet.AI will search all uncorrupted picture files in your case. However, if the case contains more than 10,000 pictures, AXIOM Examine can only show a maximum of 10,000 of the most similar

> pictures in the search results.

Find similar pictures using a picture in your case

You can select a reference picture from your case or import an external picture. Select a picture from the Artifacts or File system explorers in Row, Column, Classic, or Thumbnail view.

1. In AXIOM Examine, right-click a picture.
2. Click **Find similar pictures** > **Select picture**.

Find similar pictures using an imported picture

You can import an external picture to use as a reference picture. Pictures that you import are not added to the case as evidence.

1. In AXIOM Examine, right-click a picture.
2. Click **Find similar pictures** > **Import picture**.
3. Select the picture file you want to import, and then click **Open**.
4. In the **Confirm selected picture** dialog, click **Okay**.

Viewing similar pictures

After Magnet.AI identifies similar pictures, you can view the matching results in the Thumbnail view in the Artifacts explorer. AXIOM Examine automatically sorts the results from most similar to least similar.

Matching results are sorted from most similar to least similar in the Thumbnail view only. If you examine the matching results in another view, the results will not be sorted. If you return to the Thumbnail view, the matching results will be sorted if you haven't removed the Similar pictures filter.

Select the number of pictures to show

After AXIOM Examine finds similar pictures, you can select the number of search results to show, up to a maximum of 10,000 pictures.

1. On the filters bar, click **Similar pictures**.
2. In the Similar pictures filter box, in the **Pictures to show** number box, use the arrows to increase or decrease the number. Or, enter a number.
3. Click **Okay**.

CATEGORIZING PICTURES AND VIDEOS

Categorizing pictures and videos automatically by hash value

When evidence sources contain thousands of pictures and videos, looking at every picture and video, and categorizing them one by one can be a very time consuming task. Import hash lists that contain known pictures and videos so that AXIOM Process automatically searches and categorizes these evidence sources for you.

In addition to your own .txt files, you can import .json files from organizations like Project VIC and CAID, which allow for the sharing of hash sets between law enforcement organizations for the purpose of identifying media related to child exploitation. When you import Project VIC hash lists, you can view additional VICS metadata in AXIOM Examine such as tags, series, distributed media, identified victims, and more.

You can also enable PhotoDNA to use *fuzzy matching* to help identify even more pictures. With PhotoDNA enabled, AXIOM Process can identify pictures that are similar in appearance to existing Project VIC pictures and categorize them in the same way.

Select hash sets to use to categorize media

You can select the hash sets you want to use to categorize pictures and videos found in your evidence sources. If you haven't previously imported hash lists, add hash lists and configure your hash sets first.

1. In AXIOM Process, click **Processing details** > **Categorize pictures and videos**.
2. In the **Categorize pictures and videos by hash value** table, select the hash sets you want AXIOM Process to use to categorize evidence.
3. If applicable, clear the **Enabled** option next to any hash sets that you don't want to use for this search.
4. Continue setting up your case.

When your search completes, AXIOM Examine adds each category number it gets hits for to the Media categorizations filter. When you categorize media using Project VIC hash lists, you can view VICS attributes and values in Media category details and filter by VICS attributes using the Media attributes (VICS) filter.

Manage picture and video hash sets

To automatically categorize picture and video evidence by hash value, import hash lists. These lists can be from organizations like Project VIC and CAID or your own files. Hash lists must be .json files or .txt files containing MD5, SHA1, or PhotoDNA hashes. For .txt files, each hash must be declared on its own line.

After you import a hash list, you can add the hash list to a new or existing hash set—for example, when you want to update a Project VIC or CAID hash set with incremental updates downloaded from Hubstream.

> Tip: If you haven't previously configured your hash sets in AXIOM Process, set up your media categorization profile in AXIOM Examine by choosing a media categorization list. You can choose pre-set media categorization profiles for Canada (Project VIC), International (Project VIC), the United States (Project VIC), and the United Kingdom (CAID), or you can add a new list or import a list of media categories. When you choose a media categorization list in AXIOM Examine, you'll see the category names and colors you're familiar with when managing picture and video hash sets in AXIOM Process.

1. In AXIOM Process, click **Processing details** > **Categorize pictures and videos**.
2. In **Categorize pictures and videos by hash value**, click **Add hash list**.
3. In **Step 1**, click **Select hash list**.
4. Browse to the hash list you want to import and click **Open**.
5. In **Step 2**, complete one of the following options:
    - To add the imported hash list to an existing hash set, select the hash set you want to update.
    - To add the imported hash list to a new hash set, click **Add new hash set**. Provide a name for the hash set and click **Add**.
6. In **Step 3**, complete one of the following options:
    - If the hash list you imported is a .txt file, from the drop-down, select the category you want to update in the hash set and click **Update hash set**. Repeat for other categories you want to update.
    - If the hash list you imported is a .json file, select the categories you want to update in the hash set and click **Update hash set**.
7. When you've finished updating your hash sets, click **Close**.

Set the priority of hash sets

The order of the hash sets in the Categorize pictures and videos by hash value table determines how AXIOM Process categorizes pictures and videos when a matching hash value appears in more than one hash set and has different categories applied to it. AXIOM Process will apply the assigned category from the hash set with a higher priority.

1. In AXIOM Process, click **Processing details** > **Categorize pictures and videos**.
2. In the **Categorize pictures and videos by hash value** table, click the hash set whose priority you want to change.
3. In the **Priority** column, click the up or down arrow to change the priority.

Enable PhotoDNA

If you import hash sets in AXIOM Process for the purpose of picture categorization, you can use PhotoDNA and fuzzy matching to help identify more pictures. When you enable PhotoDNA, AXIOM Process can identify pictures that have been modified to change their hash values and pictures that are similar in appearance to existing Project VIC pictures.

PhotoDNA is only available to law enforcement. To request a password, visit www.-magnetforensics.com/photodnaregistration.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Hashing** > **Enable photo DNA**, provide the password that you received from Magnet Forensics.
3. Click **Okay**.

Categorizing pictures and videos manually

In addition to automatically categorizing pictures and videos using hash sets, you can manually categorize or grade these artifacts in AXIOM Examine in the Thumbnail view. You can quickly grade images and videos using keyboard shortcuts and bulk categorization options. When you categorize a picture or video, AXIOM Examine automatically applies the same media category to any other media items in the case with a matching MD5 or SHA1 hash.

If you haven't previously configured a media categorization list, AXIOM Examine prompts you to choose one. You can choose pre-set media categorization profiles for Canada (Project VIC), International (Project VIC), the United States (Project VIC), and the United Kingdom (CAID) or you can add a new list or import a list of media categories. Pre-set media categorization profiles are automatically configured to include the categories, names, colors, and illegal status for media items specific to the organization or region.

When you begin categorizing media in the Thumbnail view, you can view your progress in the Media categorization progress bar. The progress bar displays the number of media items that have been categorized (by you or by hash sets) in each category and the number of uncategorized items.

You can reduce your exposure to illicit content while categorizing media by blurring or hiding media items in illegal categories, muting the sound in videos by default, and setting reminders to stop categorizing media after a period of time or after you've categorized a specified number of items.

Apply a media category to a picture or video

When you begin categorizing media in the Thumbnail view, you can view your progress in the Media categorization progress bar. The progress bar displays the number of media items that have been categorized (by you or by hash sets) in each category and the number of uncategorized items.

> Tip: Before you begin categorizing media, set up your reminder and media obfuscation options to reduce your exposure to illicit media content.

1. In AXIOM Examine, open the **Artifacts explorer**.
2. In the **View** drop-down list, click **Thumbnail view**.
3. Optionally, in the **Media categorization progress** bar, start the media categorization timer or configure the categorization goal for the case.
4. Select the pictures or videos you want to apply a media category to.
5. In **Media categories**, click the media category you want to apply, or press the keyboard shortcut (0-9) for the media category you want to apply.
6. Repeat Steps 4-5 for any other pictures and videos you want to categorize.

Apply a media category to uncategorized pictures or videos

You can quickly apply a media category to all uncategorized pictures or videos that are currently visible in the Thumbnail view. After you apply a category to all uncategorized media, AXIOM Examine automatically displays the next set of uncategorized evidence so that you can continue to applying media categories.

1. In AXIOM Examine, open the **Artifacts explorer**.
2. In the **View** drop-down list, click **Thumbnail view**.

3. In **Media categories**, in the **Set all visible uncategorized pictures to** drop-down, select a media category.
4. Click **Categorize** or press the **PLUS SIGN (+)**.

Update hash sets with media categorizations from a case

After you manually categorize pictures and videos in your case, you can add reviewer graded media back to your hash sets in the Magnet AXIOM hash database for use with future cases. The next time you create a case in AXIOM Process and search the evidence using these updated hash sets, AXIOM Process will automatically search and categorize evidence with matching hashes for you.

1. In AXIOM Examine, on the **Process** menu, click **Update hash set with new media categorizations**.
2. In **Step 1: Select a hash set to update**, complete one of the following options:
   - To add the hash list to an existing hash set, select the hash set you want to update.
   - To add the hash list to a new hash set, click **Add new hash set**. Provide a name for the hash set and click **Add**.
3. In **Step 2: Select the categories to update in the hash set**, select the categories you want to update in the hash set and click **Update hash set**.
4. When you've finished updating your hash sets, click **Close**.

Export media categorizations from a case to Project VIC or CAID

After you've categorized pictures and videos in your case, you can create a JSON export of the reviewer graded media to share with Project VIC or CAID. You can select the media items you want to include in the export such as graded media. For more information about choosing which media items to include, see Evidence export options. If you've enabled a pre-set media categorization country profile, the following categories are included in the export by default:

- Canada (Project VIC): Category 1
- International (Project VIC): Categories 1-2
- United Kingdom (CAID): All categories except 8
- United States (Project VIC): Categories 1-3

After you choose the category metadata you want to include, select the subset of categories you want to include attachments for in the export. Your export will include a .json file and a folder with attachments for included metadata items.

1. In AXIOM Examine, on the **File** menu, click **Create report / export**.
2. In the **Export type** drop-down list, click **VICS 1.3** or **VICS 2.0**.
3. Next to the **File path** field, click **Browse** and select where you want to save the export. Click **Select folder**.
4. In **Items to include**, select the media options you want to include in your export.
5. In **Contact information**, provide your contact information so that other organizations can contact you if they get a match on one of your identifiers.
6. Click **Create**.

Managing media categorization lists

If you haven't previously configured a media categorization list, AXIOM Examine prompts you to choose one. You can choose pre-set media categorization profiles for Canada (Project VIC), International (Project VIC), the United States (Project VIC), and the United Kingdom (CAID) or you can add a new list or import a list of media categories. Additionally, you can export your list of media categorizations to share with other examiners.

Select a media categorization list to use

The media categorization list you select determines which categories are available for media categorization in AXIOM Examine. You can choose pre-set media categorization profiles for Canada (Project VIC), International (Project VIC), the United States (Project VIC), and the United Kingdom (CAID), or you can add a new list or import a list of media categories.

1. In AXIOM Examine, on the **Tools** menu, click **Manage media categories**.
2. Select the media categorization list you want to use.
3. Click **Okay**.

Create a custom list of media categories

You can add a media categorizations list in AXIOM Examine to create a custom list of categories. Your list can contain up to 10 categories, and you can provide custom names and colors for each category.

1. In AXIOM Examine, click **Tools** > **Manage media categories**.
2. Click **Add new list**.

3. Click the **Active** option next to the list you created.
4. In the **List name** field, provide a name for your media categorization list.
5. Complete any of the following actions to customize your media categorization list:
    - To change the color of a category, click the current color, and then choose a new color.
    - To change the name of a category, click the current name and provide a new name.
    - To turn off any categories you don't want to use, clear the **Enabled** option.
    - To indicate that items in the category include illicit or illegal content, click the **Illegal** option.
6. Optionally, select the default category you want to use to assign all visible uncategorized pictures to.
7. Click **Okay**.

Import a media categorization list

You can import a list of media categorizations in AXIOM Examine. Files must be in XML format.

1. In AXIOM Examine, click **Tools** > **Manage media categories**.
2. Click **Import list**.
3. Browse to the XML file that you want to import, and then click **Open**.
4. Click the **Active** option next to the list you created.
5. In the **List name** field, provide a name for your media categorization list.
6. Complete any of the following actions to customize your media categorization list:
    - To change the color of a category, click the current color, and then choose a new color.
    - To change the name of a category, click the current name and provide a new name.
    - To turn off any categories you don't want to use, clear the **Enabled** option.
7. Optionally, select the default category you want to use to assign all visible uncategorized pictures to.
8. Click **Okay**.

Export a media categorization list

Export your list of media categorizations to share with other examiners. Media categorization lists export in XML format.

1. In AXIOM Examine, click **Tools** > **Manage media categories**.
2. Select the media categorization list that you want to export.

3. Click **Export list**.
4. Browse to the location where you want to save the list.
5. Click **Save**.

Reducing exposure to illicit content

To help reduce your exposure to illicit content, AXIOM Examine includes several options focused on your wellness: you can blur or hide illegal media items, automatically mute videos, and set reminders to stop categorizing media.

Blur or hide illegal media items

Choose whether you want to display, blur, or hide illicit media in thumbnail previews and in the Details card. To reduce your exposure to illegal media items, consider blurring or hiding media items in illegal categories.

1. In AXIOM Examine, click **Tools** > **Manage media categories**.
2. Click **Media options**.
3. In the **Select media obfuscation options** section, choose whether you want to display, blur, or hide media in illegal categories.
4. Click **Okay**.

Mute videos by default

Choose whether you want to mute the sound or keep the sound on when playing videos. If you choose to mute videos, turning the sound on for a single video in the Preview card does not affect this setting. All other videos remain muted by default.

1. In AXIOM Examine, click **Tools** > **Manage media categories**.
2. Click **Media options**.
3. In the **Select default sound level** section, choose whether you want to mute sound or keep sound on.
4. Click **Okay**.

Set a reminder to stop categorizing media

Consider setting a reminder to stop categorizing media after a specified amount of time or after you've categorized a specified number of items (for example, the number of media items required to make a conviction).

To use a timer-based reminder, choose the default amount of time that you want to categorize media for. When you start the timer in the Media categorization progress bar, AXIOM Examine begins counting down the amount of time you set.

To use a goal-based reminder, set a reminder to stop categorizing media after you've categorized a specific number of media items in a single media category, all media categories, or all illegal media categories. Illegal media categories are defined in the media categorization list.

1. In AXIOM Examine, click **Tools** > **Manage media categories**.
2. Click **Reminder options**.
3. In the **Set reminder type** section, choose the type of reminder you want to receive.
4. Click **Okay**.

Set an end time for media categorization

Consider setting a reminder to stop categorizing media, or avoid starting to categorize media, at a certain time of day (for example, if you want to take a break before the end of your work day). When you reach the time of day that you specify, AXIOM Examine will prompt you to stop categorizing media.

1. In AXIOM Examine, click **Tools** > **Manage media categories**.
2. Click **Reminder options**.
3. In the **Set media categorization end time** section, click the **Remind me to stop categorizing** option and choose the time of day you want to be reminded to stop categorizing media.
4. Click **Okay**.

Find pictures with PhotoDNA matches

When you enable PhotoDNA, AXIOM Process assigns a PhotoDNA hash to each valid picture in your case. In addition to finding matching pictures with identical hashes, PhotoDNA also uses fuzzy matching to find similar pictures with slight modifications. Using this technique, a user can modify a picture by re-sizing, cropping, drawing over, adding a watermark, or changing the resolution, and PhotoDNA can identify it as similar to the original picture. PhotoDNA works by converting pictures into a black-and-white format, dividing them into squares, and calculating a numerical value for each square. These values, which represent the shading in each square, are the PhotoDNA signature or hash of a picture.

1. In AXIOM Examine, in the **Artifacts explorer**, click a picture artifact.
2. In **Details** > **Artifact Information**, find the picture's PhotoDNA hash (alongside its MD5 and SHA1 hashes).
3. Right-click the artifact and click **Find pictures with PhotoDNA matches**.
4. In the **Find pictures with PhotoDNA matches** dialog, select one of the following options:
    - To find the exact same, unmodified pictures, click **Exact match**. This option has the same functionality as MD5 and SHA1 hashes.
    - To find a similar picture file that might be a modified version of the selected one, click **Similar match**.
5. Click **Search**.

AXIOM Examine filters on matching or similar pictures and shows you the results.

Recategorize media files in your case

If you categorized your media for Project VIC using a third-party tool, you can import the .json files to apply those categorizations to the media in your case after initial processing.

1. In AXIOM Examine, on the **Process** menu, click **Categorize pictures and videos by hash value**.
2. When AXIOM Process opens, browse to **Processing details** > **Categorize pictures and videos**.
3. In **Categorize pictures and videos by hash value**, click **Add file**.
4. Browse to the location where you saved the .json file and click **Open**.
5. If applicable, clear the **Enabled** option next to any previously imported .json files that you don't want to use for this search.
6. Click **Analyze evidence**.

ADDING CPS DATA TO A CASE

To help protect children that are targeted by suspects using the internet, the Child Rescue Coalition's Child Protection System (CPS) collects online data that tracks person-to-person activity such as IP addresses, file hashes, person-to-person user GUIDs, and more.

You can include CPS evidence in your search in AXIOM Process or add evidence from the CPS to your case in AXIOM Examine.

Search for evidence that matches data from the CPS

You can add evidence from the CPS to your case by importing the .csv files into AXIOM Process. Once you import the .csv file into AXIOM Process and process your case, Magnet AXIOM automatically identifies and tags evidence in your case that matches data in the CPS export.

1. In AXIOM Process, click **Processing details** > **Add CPS data to search**.
2. Click **Add CPS export file**.
3. Browse to the location of the CPS file you want to add, and then click **Open**.
4. Continue setting up your case.

After processing is complete, AXIOM Examine tags the matching data in the Artifacts and File system explorers.

Add evidence from the CPS to your case

You can add evidence from the CPS to your case by importing the .csv files into AXIOM Process.

1. In AXIOM Examine, on the **Process** menu, click **Add CPS export file**.
2. When AXIOM Process opens, browse to **Processing details** > **Add CPS data to search**.
3. Click **Add CPS export file**.
4. Browse to the .csv file that you want to add to your case and click **Open**.
5. Click **Analyze evidence**.

SEARCHING FOR CUSTOM FILE TYPES

During a search, AXIOM Process might discover file types that aren't currently supported by AXIOM artifacts. You can use the Custom file types list to configure AXIOM Process to create artifacts for these file types. Magnet Forensics provides several file types to get you started, and you can add your own custom file types.

If AXIOM Process recovers any custom file types, AXIOM Examine displays the hits in the Artifacts explorer under the category heading you configured in the Custom file types list. AXIOM Process does not index or search file type artifact hits that it discovers—you should review hits for file type artifacts manually.

You can change where the Custom file type list is saved or import a list configured by another examiner. You can also add more file types and choose which file types you want AXIOM Process to search for.

> Warning: Turning this feature on can increase search times significantly.

Add custom file types

Add file types to the Custom file types list so that AXIOM Process creates artifact hits for file types discovered during a search. After AXIOM Process completes its search, you can view recovered custom file type artifacts in AXIOM Examine.

You must have Microsoft Excel or an equivalent application installed on your computer to open the Custom file type list. If you do not have an application able to open a spreadsheet on your computer, you can move the Custom file types list to another location, such as a shared network, where you're able to open the file.

> Warning: Only one person can open the Custom file type list at a time. If the list is saved to a shared network, you must close the list on your computer before anyone else can open it.

1. In AXIOM Process, click **Processing details** > **Find more artifacts**.
2. Under **Edit custom file types**, click **Edit custom file types list**. AXIOM Process opens the file in your default spreadsheet application.
3. In the Custom file type list, add your file types. The file includes instructions about what data you should include. You can also review the Custom file type list fields topic for more information about each column in the spreadsheet.
4. Save and close the document.
5. To load the new file types in AXIOM Process, under **Find more artifacts** > **Edit custom file types**, click **Refresh**.

You can see the file types in the file type list in the Categories and file types table. The file types are organized into artifact categories. You can enable or turn off categories or specific file type artifacts from the Categories and file types table as well as the Artifact details screens.

Turn off searching for file types

You can turn off searching for file type categories or specific file type artifacts. If you turn off a category, AXIOM Process won't search for any of the file types grouped in the category.

1. In AXIOM Process, click **Processing details** > **Find more artifacts**.
2. Under **Edit custom file types**, in the **Categories and file types** table, expand the category with the file type you want to turn off searching for.
3. Clear the checkbox beside the category or file type you want to turn off searching for.

Custom file types list fields

COLUMN NAME	DESCRIPTION
Category	Choose an artifact category from the options provided. These categories correspond to the artifact categories available in AXIOM Examine. The category you choose determines where the file type artifact will appear in the Artifacts explorer in AXIOM Examine. You can't enter your own category name.
Name	Enter the name of the file type artifact, as you want it to appear in AXIOM Examine. To search for multiple headers and/or footers for the same file type, enter the file type multiple times in the list using the same Category and Name. AXIOM Examine will display hits for the file type as a single artifact. Note: AXIOM Process will not process custom file type artifacts that have the same name as artifacts already supported by AXIOM artifacts.
Description	A description of the custom file type you're searching for. Providing a description is helpful to other examiners who might be using the Custom file types list.
Extensions	To identify files by their file extension, or parse, enter one or more file extensions. To enter multiple extensions, separate each value by a semicolon. File extensions are not case sensitive and you can include or exclude a period.

COLUMN NAME	DESCRIPTION
Header	To identify files by their binary content, or carve, enter the hexidecimal byte header. Enter each byte as "\x" followed by the two-character hex header value. Specifying a header can improve the search performance of AXIOM Process because the software knows where to search. Warning: If you type a common header such as "00" or "F", search times increase significantly. You can enter a header value with or without providing a footer value. Depending on whether you specify just a header, just a footer, or both, AXIOM Process searches the file differently. For more information, see Searching for headers and footers in custom file types.
Header offset	If the file's header does not occur at the beginning of a file, enter the header offset. The header offset is expressed as a numeric value greater than zero. This is an optional value. If you do not provide a value, the header offset is assumed to be zero.
Footer	To identify files by their binary content, or carve, enter the hexidecimal byte footer. Enter each byte as "\x" followed by the two-character hex header value. Specifying a footer can improve the search performance of AXIOM Process because the software knows where to search. You can enter a footer value with or without providing a header value. Depending on whether you specify just a header, just a footer, or both, AXIOM Process searches the file differently. For more information, see Searching for headers and footers in custom file types.
Footer offset	If the file's footer does not occur at the end of a file, enter the footer offset. The footer offset is expressed as a numeric value greater than zero. This is an optional value. If you do not provide a value, the footer offset is assumed to be zero.

COLUMN NAME	DESCRIPTION
Maximum size of data to carve	In bytes, specify the maximum amount of data that you want to carve, beginning from the header offset, for a particular file type artifact hit. The maximum size of data to carve is expressed as a numeric value greater than zero. This is an optional value. If you don't provide a value, AXIOM Process will carve 1 KB of data. If you specify a maximum of 0 bytes to carve and turn on the Remove duplicates setting, AXIOM Examine will display a single artifact hit if the header signature is located in multiple locations in the file. Depending on whether you specify just a maximum file size, AXIOM Process searches the file differently. For more information, see Searching for headers and footers in custom file types.

Searching for headers and footers in custom file types

Depending on whether you specify just a header, just a footer, or both, Magnet AXIOM searches the file differently.

HEADER	FOOTER	RESULT
Yes	No	If you specify a maximum size of data to carve, AXIOM Process saves data from the beginning of the file to the number of bytes you specify. If you do not specify a maximum size, AXIOM Process saves data from the beginning of the file to up to 1 KB of data.
No	Yes	AXIOM Process saves only the footer data you specify.
Yes	Yes	AXIOM Process saves the file data from the header you specify to the footer you specify. If you specify a maximum size of data to carve, AXIOM Process saves data from the beginning of the file to the footer you specify. If you do not specify a maximum size, AXIOM Process saves data from the beginning of the file to up to 1 KB of data.

Change the location of the Custom file types list

You can move the Custom file types list to another location, such as a shared network to easily collaborate with other examiners.

1. In AXIOM Process, click **Processing details** > **Find more artifacts**.
2. Under **Custom file types list location**, click **Change location**.
3. Browse to the location you want to save the custom file type list to.
4. Click **Okay**.

Import a Custom file types list

If another examiner configured the Custom file types list in AXIOM Process and has made the file available to you, such as on a network share, you can change the location of the Custom file type list to use that list.

1. In AXIOM Process, click **Processing details** > **Find more artifacts**.
2. Under **Custom file types list location**, click **Change location**.
3. Browse to the location of the Custom file types list that you want to import, and then click **Okay**.
4. When prompted to use the file at the location you selected, click **Use file**.

SEARCHING FOR SQLITE DATABASES

During a search, AXIOM Process might discover SQLite databases for applications that aren't currently supported by Magnet AXIOM. You can configure AXIOM Process to extract data from these databases.

When you enable the Dynamic App Finder, AXIOM Process looks for databases that contain certain types of data (conversations, geolocation data, website URLs, and person identifiers). After the search completes, you can view and configure the recovered artifacts on the Customize artifacts screen.

Search for SQLite databases using the Dynamic App Finder

To recover more artifacts, you can configure AXIOM Process to extract data from SQLite databases for applications that aren't currently supported by Magnet AXIOM.

> Warning: Turning this feature on can increase search times significantly.

1. In AXIOM Process, click **Processing details** > **Find more artifacts**.
2. Select the **Allow AXIOM to search for more artifacts** option.
3. Continue setting up your case.

With the option turned on, AXIOM Process looks for databases that contain certain types of data (conversations, geolocation data, website URLs, and person identifiers).

After the search completes, you can view and configure the recovered artifacts in AXIOM Process on the Customize artifacts screen.

Creating custom artifacts from SQLite database hits

If you enable the Dynamic App Finder to allow AXIOM Process to search for more artifacts, after completing a search, AXIOM Process displays all the databases that it suspects contain useful data on the Customize artifacts screen.

The data that AXIOM Process displays is raw, and in many cases, the app name and columns it extracts might not be descriptive or user friendly. You can customize the data so that when results show up in AXIOM Examine, they make sense to you and others reviewing the data. You can change the name of the artifact (by default, AXIOM Process uses the name of the database).

You can also map each fragment in the artifact to a category that reflects the type of data. By mapping each fragment, you're providing AXIOM Process with instructions on how to handle and present the data. For example, fragments that you categorize as a Latitude or Longitude can be plotted on the World map view, while fragments that use Date/time can appear on the Timeline view.

Step 1: Select the data types and databases you want to create artifacts from

You can select the specific data types and databases that you want to create custom artifacts from. Only the databases that include the types of data you select will appear in AXIOM Examine, allowing you to filter the data that is relevant or irrelevant to your case.

You can then choose which databases you want to create custom artifacts from and specify a custom name for the artifact. By default, AXIOM Process names the artifacts using data identified from the database table, but you can change the name to something user-friendly.

When AXIOM Process completes its search, AXIOM Examine notifies you that you need to return to AXIOM Process to customize the artifacts.

1. InAXIOM Process, click **Customize artifacts**.
2. In the **Select relevant data types** drop-down, select the databases with the types of data that you want to view.
3. In the **Select relevant data types** table, select the databases that you want to create a custom artifact from. You must select at least one artifact to proceed with the remaining steps.
4. To rename an artifact, in the **Custom artifact name** column, click the existing artifact name. Provide a custom name.
5. Repeat Steps 3-4 for all remaining custom artifacts in the table.

Step 2: Map columns

Your next step is to configure the column names so that they're easier to understand. AXIOM Process attempts to name the column to reflect the type of data and content. If AXIOM Process can't identify a column or provide an accurate category for it, the column appears grayed out in the table. By default, these columns are excluded from the custom artifact until you provide a name.

You can provide a custom column name, or you can choose from the following categories:

- City
- Coordinates
- Country
- Date/Time
- Email
- Geolocation
- Latitude
- Longitude
- Message
- Phone
- Postal code/ZIP
- Recipient
- Sender
- State/Province
- Street
- URL/URI

For Date/Time fragments, AXIOM Process attempts to determine the format that the fragment is stored as and uses that value as the default. You can change the date format for the entire table by choosing an option from the *Date format* drop-down menu. The specified date format appears in the Preview table as well.

In some cases, for “Date/Time” fragments mapped from text-based SQL columns, you might be notified that the column does not support the type of data selected. To keep the column mapping and show the column values in AXIOM Examine, change the mapping option type to “Custom” and provide a new column name.

To configure the column names, complete the following action for each custom artifact you want to search for:

1. Select the artifact from the **Select relevant data types** table.
2. If applicable, under **Map columns**, in the **Date format** drop-down, select a date format for the fragment.
3. For each column in the **Map columns** table, click the column heading. Select one of the following options:
   - Select an existing column name.
   - Select **Custom** and provide your own column name.
   - If you don't want the column to be mapped, click **None**.
4. Repeat Steps 1-3 for all remaining custom artifacts.

Step 3: Preview your custom artifacts

The final step is to review the custom artifacts in the **Preview** section. This table lists all the columns that AXIOM Process will include in the final version of the custom artifact, along with the actual data that's recovered.

Step 4: Save selected artifacts

When you're satisfied with the content for the artifact, click **Save selected artifacts**. AXIOM Process only saves the custom artifacts that have their **Enabled** options selected in the **Select relevant data types** table.

AXIOM Process saves the artifact definitions to the AXIOM Process\plugins directory. The next time you run a search, the new artifact is available for selection by default.

SELECTING ARTIFACTS TO INCLUDE IN A SEARCH

Depending on your evidence sources and the type of license that you have, you might be able to search for computer artifacts, mobile artifacts, cloud artifacts, or a combination. If you've added custom artifacts in AXIOM Process or turned on searching for custom file type artifacts, you can also search for custom artifacts.

Select artifacts to include in your search

By default, AXIOM Process includes all available artifacts for your evidence sources in a search. You can select the specific artifacts or artifact categories that you want to include or exclude from your search.

1. In AXIOM Process, click **Artifact Details**.
2. Click **Customize computer artifacts**, **Customize mobile artifacts**, or **Customize cloud artifacts**.
3. Select the specific artifacts or artifact categories that you want to include in your search.
4. If necessary, configure the options for the artifacts that you want to include in your search.
5. Continue setting up your case.

Search for custom artifacts

You can search for custom artifacts if you've loaded custom artifacts in AXIOM Process or turned on searching for custom file type artifacts.

1. In AXIOM Process, click **Artifact details**.
2. Depending on what platform you specified for your custom artifact, click **Customize computer artifacts**, **Customize mobile artifacts**, or **Customize cloud artifacts**.
3. On the **Select artifacts to include in case screen**, select the **Custom artifacts** option.
4. Optionally, select or clear the check box for any specific custom artifacts.
5. Continue setting up your case.

Decrypting artifacts

For some artifacts, you can provide potential passwords or decryption keys to try to decrypt the user's account or data.

If this option is available for a specific artifact, you'll find an **Options** link below the artifact name with the ability to provide a password or decryption key.

Configuring media artifact options

Save picture attachments to the case

By default, AXIOM Process accesses picture attachments from the original source, rather than copy and save the pictures to the case folder. This behavior saves storage space in your case file, but requires that you have constant access to the evidence source to view the attachments while you work on your case. If the evidence source needs to be mounted (for example, with a volume shadow copy), if you plan on creating a portable case, or if you aren't concerned about storage space and longer processing times, you can turn off this setting.

If you choose to save picture attachments to your case, your case folder size can increase. The pictures will be saved to the attachments database in your case folder.

> Note: .tiff, .raw, and .3fr files, as well as carved pictures and thumbnails are saved to the case regardless of this setting.

1. In AXIOM Process, click **Artifact details** > **Computer or Mobile artifacts** > **Media**.
2. Under the **Pictures** artifact, click **Options**.
3. Clear the **Access pictures from the source (do not save to case)** option, and then click **Okay**.
4. Continue setting up your case.

Extract EXIF data from pictures

By default, AXIOM Process extracts EXIF (Exchangeable Image File Format) data from picture artifacts such as GPS longitude and latitude, original size, software, and more. You can use this data in AXIOM Examine in several ways such as filtering evidence or in the World map view (which plots all Google Maps, Google Maps Tiles, geo-enabled apps, and picture coordinates from EXIF data on a world map).

1. In AXIOM Process, click **Artifact details** > **Computer or Mobile artifacts** > **Media**.
2. Under the **Pictures** artifact, click **Options**.
3. Select or clear the **Extract EXIF data** option, and then click **Okay**.
4. Continue setting up your case.

Detect skin tone in pictures and videos

By default, AXIOM Process uses a skin tone detection algorithm to detect skin tone in picture, video, and carved video artifacts to help identify explicit content. For video artifacts, skin tone detection is limited to the still frames captured from the video.

1. In AXIOM Process, click **Artifact details** > **Computer or Mobile artifacts** > **Media**.
2. Under the **Pictures or Videos** artifact, click **Options**.
3. Select or clear the **Detect skin tone** option, and then click **Okay**.
4. Continue setting up your case.

When AXIOM Process finishes searching the evidence, you can filter evidence in the case by skin tone percentage in AXIOM Examine.

Set the maximum dimensions for saved pictures

To help save storage space in your case file, you can set a maximum width or height for saved pictures (while preserving the aspect ratio of the picture).

1. In AXIOM Process, click **Artifact details** > **Computer or Mobile artifacts** > **Media**.
2. Under the **Pictures or Videos** artifact, click **Options**.
3. Select the **Resize to a maximum width/height of** option and specify the maximum dimension (in pixels), and then click **Okay**.
4. Continue setting up your case.

Create video previews using still frames

You can configure AXIOM Process to create a preview of video files using still frames (static images taken from the video). If enabled, AXIOM Process will attempt to capture up to 10 still frames evenly spaced throughout the video. You can view the previews of video artifacts in AXIOM Examine.

1. In AXIOM Process, click **Artifact details** > **Computer or Mobile artifacts** > **Media**.
2. Under the **Pictures or Videos** artifact, click **Options**.
3. Select the **Create a preview using still frames** option.

4. Click **Okay**.
5. Continue setting up your case.

Save videos to your case

By default, AXIOM Process saves a thumbnail picture for the videos it recovers, not the full content. If you have access to the source image, you can always export the full content of the video even if you set AXIOM Process to save only thumbnail pictures, or, if you don't have enough space for the video files in the location where your case is saved. You can still stream the videos in AXIOM Examine. If you want AXIOM Process to include the full content of the videos it discovers, you can enable the option to save videos to your case.

If you choose to save video attachments to your case, your case folder size can increase. The videos will be saved to the attachments database in your case folder.

> Note: If the evidence in your case is from a VSC or ISO image, you must save the video to your case to get a preview of the video in the case. Consider exporting VSC and ISO images and processing them separately from the rest of your evidence.

1. In AXIOM Process, click **Artifact details** > **Computer or Mobile artifacts** > **Media**.
2. Under the **Videos** artifact, click **Options**.
3. Select the **Save videos up to** option and specify the maximum size for the videos. The default maximum size is 500 MB.
4. Click **Okay**.
5. Continue setting up your case.

Customize the maximum size of saved carved videos

AXIOM Process saves carved videos to your case. You can customize the maximum length of carved videos that you want to recover.

1. In AXIOM Process, click **Artifact details** > **Computer or Mobile artifacts** > **Media**.
2. Under the **Videos** artifact, click **Options**.
3. In the **Carved video size** field, specify the size of carved videos that you want to save. The default size is 20 MB.

4. Click **Okay**.
5. Continue setting up your case.

Managing artifact profiles

If you search for similar sets of artifacts regularly, you can create artifact profiles to help save you time when setting up your case. You can share the profiles you create with other examiners, and import profiles created by others.

Create an artifact profile

By default, AXIOM Process searches for all applicable artifacts each time you create a case. You can create your own custom artifact profiles to search for specific artifacts or artifact categories of your choosing. Creating custom artifact profiles can be particularly helpful if you regularly search for similar artifacts or artifact categories.

1. In AXIOM Process, click **Artifact Details**.
2. For each of **Computer artifacts**, **Mobile artifacts**, and **Cloud artifacts**, select the artifacts you want to include in the artifact profile.
3. Click **Profile options** > **Save profile as**.
4. In the **Save profile as** field, provide a name for your artifact profile.
5. Click **Okay**.

Update an artifact profile

You can add or remove artifacts from your artifact profile after you've created it.

1. In AXIOM Process, click **Artifact Details**.
2. For each of **Computer artifacts**, **Mobile artifacts**, and **Cloud artifacts**, select the artifacts you want to include in the artifact profile.
3. From the **Profile** drop-down, select the artifact profile you want to update.
4. Click **Profile options** > **Save profile**.

Import an artifact profile

You can import artifact profiles created by other examiners into AXIOM Process.

1. In AXIOM Process, click **Artifact Details**.
2. Click **Customize computer artifacts**, **Customize mobile artifacts**, or **Customize cloud artifacts**.
3. On the artifacts page, click **Profile options** > **Import profile**.
4. Browse to the location of the profile that you want to import.
5. Select the profile, and then click **Open**.

You can now find your imported artifact profile in the **Profile** drop-down list.

Export an artifact profile

You can share artifact profiles that you've created with other examiners by exporting the profile from AXIOM Process.

1. In AXIOM Process, click **Artifact Details**.
2. Click **Customize computer artifacts**, **Customize mobile artifacts**, or **Customize cloud artifacts**.
3. On the artifacts page, click **Profile options** > **Export profile**.
4. Browse to where you want to save the profile and click **Save**.

Set a default artifact profile

By default, AXIOM Process searches for all applicable artifacts each time you create a case using the artifact profile *All artifacts*. You can set a default artifact profile so that AXIOM Process automatically selects a specific group of artifacts to search when you create a case and load your evidence.

1. In AXIOM Process, click **Artifact Details**.
2. Click **Customize computer artifacts**, **Customize mobile artifacts**, or **Customize cloud artifacts**.
3. From the **Profile** drop-down, choose the artifact profile you want to set as the default selection.
4. Click **Profile options** > **Set as default**.

Rename an artifact profile

1. In AXIOM Process, click **Artifact Details**.
2. Click **Customize computer artifacts**, **Customize mobile artifacts**, or **Customize cloud artifacts**.
3. From the **Profile** drop-down, choose the artifact profile you want to rename.
4. Click **Profile options** > **Rename profile**.

5. In the **New name** field, provide the new name for the profile.
6. Click **Okay**.

Delete an artifact profile

1. In AXIOM Process, click **Artifact Details**.
2. Click **Customize computer artifacts**, **Customize mobile artifacts**, or **Customize cloud artifacts**.
3. From the **Profile** drop-down, select the artifact profile you want to update.
4. Click **Profile options** > **Delete profile**.

ADDING CUSTOM ARTIFACTS

With the frequency that new applications and services are released to the market, custom artifacts can help you keep up to date with artifacts that might not be supported by Magnet AXIOM. In a corporate environment, you can use custom artifacts to recover data from proprietary applications. In addition to creating your own artifacts, you can browse the Artifact Exchange to search for, download, and install custom artifacts that other organizations have created and uploaded.

In addition to adding custom artifacts in AXIOM Process, you can find more artifacts by enabling the Dynamic App Finder and configuring the Custom file types list to search for artifacts that aren't currently supported by Magnet AXIOM.

What is a custom artifact?

A custom artifact is an XML file or a Python script that contains instructions for recovering a particular type of evidence. Typically, custom artifacts are targeted towards new applications or features that Magnet AXIOM does not yet support. Because custom artifacts aren't developed and maintained by Magnet Forensics, they're not required to go through the same level of testing as fully supported Magnet AXIOM artifacts, so they can often be developed and released faster.

Custom artifacts can contain executable code and are run in an unsandboxed Python environment with administrator privileges. Running in an environment without restrictions gives custom artifacts a lot of power and flexibility, but you must ensure that the source from where you obtain a custom artifact is trusted.

Creating a custom artifact

For information about downloading, contributing, and creating your own custom artifacts, visit the Artifact Exchange.

Add custom artifacts to AXIOM Process

After you've created your own custom artifact or downloaded a custom artifact from the Artifact Exchange, you can load it into AXIOM Process.

1. In AXIOM Process, on the **Tools** menu, click **Manage custom artifacts**.
2. Click **Add new custom artifact** and browse to where you saved the artifact.
3. Select the artifact and click **Okay.**

AXIOM Process saves artifact definition templates to the *AXIOM Process/plugins* folder.

Confirm the artifact loaded correctly

1. In AXIOM Process, click **Artifact details**.
2. Depending on what platform you specified for your custom artifact, click **Customize computer artifacts**, **Customize mobile artifacts**, or **Customize cloud artifacts.** If you didn't specify a platform, the artifact is available in each option.
3. On the **Select artifacts to include in case screen**, select the **Custom artifacts** option.
4. Confirm that the custom artifacts you loaded to the plugins folder are visible.

If an artifact is not available, there might be a problem with the artifact schema. Check the log.txt file in the plugins folder for details.

When you've successfully loaded your custom artifacts in AXIOM Process, you can include them in a search.

Viewing custom artifacts in AXIOM Examine

AXIOM Examine displays custom artifacts in the Artifacts explorer under the **Custom** heading. When you add a custom artifact to a case for the first time, they don't appear under **Evidence** if AXIOM Examine is already open. To view your custom artifacts, you must close AXIOM Examine and reopen the case.

REVIEWING THE EVIDENCE

After processing is complete, AXIOM Examine presents your evidence in a consumable and user-friendly manner. Depending on your evidence sources, you can view the results in many different explorers.

GOAL	EXPLORER
Review your case and find places to start examining evidence	Case dashboard
Browse the artifacts	Artifacts explorer
Discover connections between evidence	Connections explorer
Explore the file system	File system explorer
View the registry	Registry explorer
View a timeline of file system and artifacts evidence	Timeline explorer

Viewing artifact information

AXIOM Examine allows you to view artifact information in a number of different ways, depending on the type and format of the artifact.

> Note: Often, the evidence that you examine includes executable files or scripts (including those embedded in other artifacts such as PDF files or documents). Please note that Magnet AXIOM never runs executable files or scripts contained in your evidence (whether examined from AXIOM Examine or a portable case)—including if you try to open an executable file with an external application.

Previews

In the Artifacts, File systems, and Timeline explorers, use Previews to see a visual representation of the artifact or file—similar to how the file actually appears to the suspect.

Previews support many types of document formats (such as .doc, .pdf, .xls, and .ppt), images, videos, and more. In some cases, an artifact might have more than one Preview (for example, PDF documents can have one Preview to show the actual PDF and another one to show highlighted keywords). JSON file previews appear in the File system explorer and allow you to search and copy text from the file.

Details

In the Artifacts, File system, and Timeline explorers, use Details to review the following information about the artifact or file:

- **Artifact information**: Includes general information such as file name, title, authors, and date/time information.
- **Evidence information**: Includes source and location information and links into the file system and registry (if applicable).

In the Artifacts and File systems explorers, Details displays a connections icon beside artifact attributes that you can draw a map of connections for. For more information about viewing connections between attributes, see Discovering connections.

APFS metadata

Files on macOS computers can contain a number of additional attributes associated with each file on the file system. For evidence from macOS computers with APFS, you can view additional attributes from the spotlight database as well as extended attributes in the APFS metadata card. View common attributes of interest in the Artifacts explorer and a full list of available attributes in the File system explorer. For attributes that have binary information, you can view the attribute text and hex data in the Text and hex viewer.

Media categorization details

In the Artifacts and Timeline explorers, use Media categorization details to view information about how the picture or video artifact was categorized (by a hash set or by a reviewer), the media category applied to the picture or video, MD5 and SHA1 hashes, and VICS attributes and values.

Media categories

In the Thumbnail view of the Artifacts explorer, use Media categories to apply a media category to a picture or video.

Text and hex

In the File system, Registry, and Timeline explorers, use Text and hex to view the raw data associated with a file system item. This view allows you to verify the results that Magnet AXIOM produces and manually parse out any additional data that might not be included in the Details for an artifact.

See Viewing raw artifact data in Text and hex for more information about using *Text and hex* to review file system evidence.

SQLite viewer

In the File system and Timeline explorers, use the SQLite viewer to view SQLite databases. See Viewing database tables for tips about examining databases in the SQLite viewer.

Tags and comments

In the Artifacts, File system, Connections, and Timeline explorers, use Tagging evidence to label evidence in a meaningful way for your investigation.

Reset your case view

You can revert your case view in AXIOM Examine back to what you see when you first open a case. Resetting your case view forces AXIOM Examine to revert any viewing customizations you set, such as collapsed or expanded information and applied filters.

1. In AXIOM Examine, on the **File** menu, click **Refresh case**.

Reviewing your case from the Case dashboard

Use the Case dashboard as a starting point to locate, and then browse directly to pieces of evidence that are potentially of interest in your case.

The Case dashboard displays summary information about your case, allowing you to gain insight into your evidence. You can customize the Case dashboard by collapsing or expanding individual sections.

The first two columns on the dashboard, Case overview and Evidence overview, provide you with a summary of your case and evidence sources. They include the following sections:

- **Case summary notes** displays the examiner name and case summary, which you can edit on the dashboard.
- **Case processing details** displays the case number and search information that you specified in AXIOM Process.
- **Case information** displays links to the Case Information.txt and AXIOMExamine.log files in your case folder.
- **Evidence overview** displays basic information about each evidence source in your case.

Information from these columns appears at the beginning of your PDF and HTML case reports. To learn more about exporting reports, see Exporting and sharing evidence.

The Case dashboard is the default explorer for AXIOM Examine. You can change the default explorer to another explorer such as the Artifacts or File system explorer.

Quickly drill down to key evidence in your case

In the Case dashboard, the *Places to start* column allows you to quickly see the most common types of evidence in your case—including categories, tags, keywords, and more—indicated by the number of matches displayed. You can click the links to filter on the type of evidence that you're interested in.

SECTION	DESCRIPTION
Artifact categories	Discover the number of hits for popular artifacts—like Chat, Web Related, Cloud, or Email—in your case.
Tags and comments	View the tags and comments in your case and where that evidence was tagged (in the Artifacts or File system explorers).

SECTION	DESCRIPTION
Magnet.AI categorization	View the chats and pictures that Magnet.AI identified as being off interest in your case.
CPS data matches	View the CPS data matches that AXIOM Process found while processing evidence.
Keyword matches	Discover the top keywords in your case and the number of matches, including both artifact keywords and binary keywords, and generate the keyword matches summary report.
Passwords and tokens	View the cloud passwords or tokens that AXIOM Process found while processing evidence.
Media categorizations	View the media categories in your case and the number of matches for pictures and videos in each category and generate the media categorization summary report.
Profiles	Discover the number of matches for the profiles in your case, including profiles from imported profile watchlists.

Browsing the artifacts

In AXIOM Examine, use the Artifacts explorer to browse artifact groups and select the specific types of artifacts that you want to view in more detail.

Depending on the type of investigation you're doing, any one of the artifacts that Magnet AXIOM recovers might be important to your search. For example, in a corporate espionage investigation, you might want to focus your efforts on the operating system artifacts. In a fraud case, you might want to focus on email and web-related artifacts.

Views in the Artifacts explorer

Within the Artifacts explorer, you can customize how evidence is displayed using several Views:

VIEW	DESCRIPTION
Classic view	Stacks Evidence and Details vertically.
Column view	Displays all artifact data in a table format that allows you to sort on any column. This is the default view.
Conversation view	Displays messages as a back-and-forth dialog, in a format similar to the application that the messages are from. You can expand a conversation to see all the messages included in that conversation. This view uses an implicit filter to display only the content that is supported by chat threading.
Histogram view	Provides a graphical representation of all the results in your case for each type of artifact.
Row view	Displays an artifact result's most relevant pieces of data in a row format.
Thumbnail view	Displays media files as thumbnails. This view uses an implicit filter to display only the artifacts that contain media attachments. You can double-click the picture and video thumbnails to preview the content. Use this view to categorize pictures and videos manually in your case.
World map view	Plots artifact results as coordinates on a world map. This view uses an implicit filter to display only the artifacts that contain location information.

Reviewing Refined results

Use the *Refined results* category as a starting point when browsing the artifacts in your case. Refined results extract and highlight specific fragments from their artifact counterparts. These fragments are considered important depending on the type of case (for example, *Identifiers* is a refined results category that pulls out fragments which point to specific people involved in the case, allowing you to create profiles). Magnet AXIOM analyzes the evidence that's recovered from other artifact categories and creates a hit for each artifact that matches the criteria of a refined results artifact (for example, when AXIOM Process recovers a URL that contains a search query, it creates a refined result of the *Parsed search queries* type). Each refined result has a link to the parent artifact that the evidence was recovered from. You can browse to the parent by clicking the *Original artifact* link in Details.

Refined results categories:

- Classifieds URLs
- Cloud service URLs
- Dating sites URLs
- Facebook URLs
- Google searches
- Google translate
- Identifiers
- Parsed search queries
- Potentially unwanted apps
- Shipping site URLs
- Social media URLs
- Tax site URLs
- Torrent URLs
- Web chat URLs

View evidence from around the same time as an artifact or file

When you've found evidence relevant to your investigation, you might want to know what else occurred around the same time. You can use the Relative date/time filter to view evidence around the time of a specific date and choose which explorer you want to view the relative time results in—your current explorer or the Timeline explorer.

1. In AXIOM Examine, click an artifact or file that contains a date/time fragment.
2. In **Details**, click the clock icon beside the date/time fragment.
3. In the **Anchor relative to** section, select the date and time you want to use as the anchor.
4. In the **Set range** section, select the range of time you want to filter by.
5. In the **Explorer** drop-down, select the explorer you want to view the results in .
6. Click **Okay**.

Set the default explorer to view relative date/time filter results in

When you use the relative date/time filter to view evidence around the time of a specific date, you can choose which explorer you want to view the relative time results in—your current explorer or the Timeline explorer. By default, AXIOM Examine will show the results in the Timeline explorer.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. Under **Relative date/time** filter in the **Explorer** drop-down list, click the explorer you want to set as the default to view relative date/time results in.
3. Click **Okay**.

Change character encodings

Sometimes, Magnet AXIOM does not apply the correct encoding to an item, which causes some characters to become difficult to read. You can choose to change the encoding for a single item, a collection of items, or a whole artifact on a per-attribute basis.

1. In AXIOM Examine, in the **Artifacts explorer**, select the items you want to change character encodings for.
2. Right-click the selected items and click **Change encoding**.
3. In the **Items to encode** drop-down list, select the items that you want to change character encodings for.
4. In the **Attribute selection** drop-down list, select the attributes that you want to change character encodings for.
5. In the drop-down list beside each attribute, select the encoding you want to use.
6. Click **Okay**.

View artifacts in an external application

You can view the contents of artifacts using external applications such as HxD, Adobe Acrobat, Google Chrome, Microsoft Word, and more. The applications that Magnet AXIOM suggests for each artifact come from recently used Windows programs that are associated with each artifact type.

1. In AXIOM Examine, in the **Artifacts explorer**, right-click an artifact.
2. Click **Open with**.

3. Select the application that you want to open the artifact with and click **Okay**.

Save artifacts

When you save artifacts, AXIOM Examine saves the bytes of data that the specific artifact hit is associated with. If the hit is parsed, the entire source file gets saved. If the hit is carved, only a subset of the source file gets saved.

Saving the attachments for single artifacts is available only in the Row, Column, and Classic views.

1. In AXIOM Examine, in the **Artifacts explorer**, right-click an artifact group or type, or a single artifact.
2. Click **Save artifact to**.
3. Browse to the location where you want to save the files and click **Select folder**.

View artifacts on a map

The World map view plots all Google Maps, Google Maps Tiles, geo-enabled apps, and picture coordinates from Exif data on a world map. Clusters appear where a large number of plotted points exist. This view is useful if you have an idea of where an incident occurs and want to see if there are other artifact results that coincide with that area. Keep in mind that some artifacts do not have the required coordinates and can't be plotted.

View artifact details in the World map view

AXIOM Examine opens the world map and applies an implicit filter to display only the artifacts that have location information.

When you hover over a marker, basic details about the marker are displayed, including the date range and time of the result. To view the full details:

1. In AXIOM Examine, open the **Artifacts explorer**.
2. In the **View** drop-down list, click **World map view**.
3. In the **World map view**, click a pin on the map.
4. In the dialog that appears, click **View details**.

Details about all of the artifacts in the marker appear in a split screen below the world map view.

To switch back to a full-screen map, in the top-right corner of the map view, click the expand icon (⛶) .

View chat threads

Use Conversation view to quickly see the individual messages in a threaded conversation, in a format similar to the application that the messages are from. You can also view the details of the chat thread, including the number of participants, display names, number of messages in the chat thread, and more.

> Note: Not all chat artifacts currently support the Conversation view.

View chat threads in Conversation view

1. In AXIOM Examine, open the **Artifacts explorer**.
2. In the **View** drop-down list, click **Conversation view**.

Conversation view is sorted in chronological order based on most recent chat activity.

AXIOM Examine applies an implicit filter to display only the artifacts that support chat threads. To see the individual messages in the chat thread, expand the conversation.

Export a chat thread

When you save a chat thread to your case, the file is named with the name of the chat application and the date and time stamp of the last message in the thread. For example, "Skype Chat Messages - 7_05_2016 3_09_04 PM."

1. In AXIOM Examine, in the **Conversation view**, right click the chat thread that you want to export.
2. Click **Create report / export**.
3. In the **Export type** drop-down list, select **HTML** or **PDF**.
4. Next to the **File path** field, click **Browse** and select where you want to save the export. Click **Select folder**.
5. In **Items to include**, select the chat threads that you want to export.
6. In **Level of detail**, complete one of the following options:
   - To save the information to one report, select **High-level information**
   - To create individual reports for each artifact type (for example, one report for Skype Chat Messages and another for GoogleTalk messages), select **Detailed information** .
7. Click **Create**.

View artifacts on a histogram

You can use *Histogram view* to build a visual baseline for your case to compare with other cases. The histogram reveals differences between the baseline and another investigation, which can help you build a profile of common investigation types and identify cases that fall outside the norm. For example, if you're able to build a baseline of the common artifacts that are found in a case and then compare it with others, variations stand out and warrant further analysis.

Open the Histogram view

1. In AXIOM Examine, open the **Artifacts explorer**.
2. In the **View** drop-down list, click **Histogram view**.

Save a histogram baseline

1. In AXIOM Examine, in the **Histogram view**, click **Save as baseline**.
2. Provide a name and location for the saved baseline, and then click **Save**.

AXIOM Examine saves the baseline as a .ini file for comparison with later cases.

Load a histogram baseline

1. In AXIOM Examine, in the **Histogram view**, click **Load baseline**.
2. Select the histogram baseline that you want to load, and then click **Open**.

AXIOM Examine displays the baseline histogram alongside the current case to help visualize discrepancies between the current case and the baseline.

Exploring the file system

In AXIOM Examine, the *File system explorer* allows you to drill down through the file system tree of your evidence source, just like you can by using the File Explorer on your own computer. You can also use the File system explorer to view additional content such as unallocated space and volume slack.

Viewing raw artifact data in Text and hex

In the File system, Registry, and Timeline explorers, use Text and hex to view the raw data associated with a file system item. This view allows you to verify the results that Magnet AXIOM produces and manually parse out any additional data that might not be included in the Details for an artifact.

For information about viewing the raw data associated with a file system artifact, see Viewing raw artifact data in Text and hex.

For example, there might be data encoded in a picture that Magnet AXIOM might not be able to parse. By viewing the Hex source, you can manually extract the data yourself. You can also decode the hex values into common formats, including ASCII, binary, date/time, and more.

The *Text* view converts underlying bytes to ASCII text, which is generally a much cleaner view for text documents and for other ASCII-based data. As an examiner, you can use this feature to verify evidence and keywords. Text supports many different character encoding types that you can select from. The default character encoding is unicode (US-ASCII).

Browse to a specific offset

If you know the offset that you want to view, you can browse to it:

1. In AXIOM Examine, in the **File system** or **Registry explorer**, browse to the evidence item.
2. In **Evidence**, click the evidence item.
3. In **Text and hex**, click **Go to** and provide the offset that you want to view.
4. On your keyboard, press **ENTER**.

Search for a text string or hex value

1. In AXIOM Examine, in the **File system** or **Registry explorer**, browse to the evidence item.
2. In **Evidence**, click the evidence item.
3. In **Text and hex**, click **Find**.
4. Provide the string or hex value that you want to search for.
5. Select the search method that you want to use: **Text string** or **Hex value**.
6. On your keyboard, press **ENTER**.

Decode hex values

You can decode hex values into other formats to analyze the information in that specific format. When you decode hex values, the information appears in Decode at the bottom of Text and hex.

> Note: You can only decode up to 10 KB of data at one time.

1. In AXIOM Examine, in the **File system** or **Registry explorer**, browse to the evidence item.
2. In **Evidence**, click the evidence item.
3. In **Text and hex**, click **Decode**.
4. Click and select hex values to automatically decode that selection.

Save or copy text or hex data

You can save or copy a selection of text or hex data for use at a later time. To save or copy the data:

1. In AXIOM Examine, in the **File system** or **Registry explorer**, browse to the evidence item.
2. In **Evidence**, click the evidence item.
3. To select the data you want to save or copy, in **Text and hex**, click and drag text or hex values
4. Right-click and select **Save selection** or **Copy selection.**
5. If you chose to save the hex data, browse to the location where you want to save the data.
6. Provide a file name (ending in .txt), and then click **Save**.

Create artifacts using raw data

While using the File system or Registry explorers, you might come across important evidence that isn't already associated with an artifact. If you want to display this evidence alongside other artifacts and include it in your exports, you can save the content manually. After you create the new artifact, you can tag it, comment on it, and export it just like any other artifact. To save registry data as an artifact, do the following:

1. In AXIOM Examine, in the **File system** or **Registry explorer**, browse to the evidence item.
2. In **Evidence**, click the evidence item.
3. In **Text and hex** for that file, select the group of hex characters that you want to create an artifact for.
4. Right-click the selection and click **Display as artifact**.

The new artifact appears in the Artifacts explorer in the *Examiner defined* group. The *Details* for the new artifact list the name of the analyst / examiner who created the artifact.

You can also create artifacts from file snippets. To learn more, see Create artifacts using file snippets.

Viewing database tables

View SQLite databases in the SQLite viewer in the File system explorer. When you examine a database in the SQLite viewer, consider the following tips:

- Select the table in the database that you want to view from the **Select table** drop-down.
- Search all fields in the current table by clicking **Find** and providing a search term.
- Query the data by building and executing SQL queries directly in the SQLite viewer. Include JSON features in the query to look into JSON data within a cell and return data from inside that text block.
- Customize how you view data in the table by choosing which columns you want to show or hide or by reordering the columns by dragging the column headers to a new position.
- Freeze columns by dragging the vertical blue bar across the table. Columns to the left of the vertical blue bar will be visible while scrolling through the rest of the table.
- Refine the data you see in the table by applying one or more filters.
- Export the data in the table to a .csv or .xlsx file. If you apply a filter or query the data, only data currently shown in the table is included in the export.
- View BLOB (Binary Large Object) data by right-clicking the data and selecting one of the following options:

    - To preview the BLOB data, click **View as picture**. In the previewer, you can zoom in on the picture, rotate the picture, and more.
    - To view the BLOB data in an external viewer, click **Open with** and select a viewer.
    - To view BLOB data in a properly list (plist) viewer, click **View as plist**.
- Copy cell data or save BLOB image data by right-clicking the data and selecting **Copy** or **Save as**.
- Change the encoding of a column in the table by right-clicking the column header and selecting a new encoding type.

View evidence from around the same time as an artifact or file

When you've found evidence relevant to your investigation, you might want to know what else occurred around the same time. You can use the Relative date/time filter to view evidence around the time of a specific date and choose which explorer you want to view the relative time results in—your current explorer or the Timeline explorer.

1. In AXIOM Examine, click an artifact or file that contains a date/time fragment.
2. In **Details**, click the clock icon beside the date/time fragment.
3. In the **Anchor relative to** section, select the date and time you want to use as the anchor.
4. In the **Set range** section, select the range of time you want to filter by.
5. In the **Explorer** drop-down, select the explorer you want to view the results in .
6. Click **Okay**.

Set the default explorer to view relative date/time filter results in

When you use the relative date/time filter to view evidence around the time of a specific date, you can choose which explorer you want to view the relative time results in—your current explorer or the Timeline explorer. By default, AXIOM Examine will show the results in the Timeline explorer.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. Under **Relative date/time** filter in the **Explorer** drop-down list, click the explorer you want to set as the default to view relative date/time results in.
3. Click **Okay**.

View artifacts associated with a file

Similar to how you can view files or registry data associated with an artifact, you can also view artifacts associated with a file.

1. In AXIOM Examine, in the **File system explorer**, right-click a file in **Evidence**.
2. Click **View related artifacts**.

View file system artifacts in an external application

You can view the contents of artifacts using external applications such as HxD, Adobe Acrobat, Google Chrome, Microsoft Word, and so on. The applications that Magnet AXIOM suggests for each artifact come from recently used Windows programs that are associated with each artifact type.

1. In AXIOM Examine, in the **File system explorer**, right-click a file in **Evidence**.
2. Click **Open with**.
3. Select the application you want to open the artifact with.
4. Click **Okay**.

Add files from the File system explorer to the Artifacts explorer

You can add files from the File system explorer to the Artifacts explorer. Looking at all of your information in one explorer makes consolidating this information for reporting purposes easier.

1. In AXIOM Examine, in the **File system explorer**, right-click a file in **Evidence**.
2. Click **Save file as artifact**.

In the Artifacts explorer, you can see the new artifact in the Examiner defined group in Files.

Display files and folders recursively

By default, when you click a folder, the File system explorer behaves how you might expect a file system navigation tool to behave—when you click a folder, its immediate children are displayed in Evidence. However, you can change this behavior so that not only the selected folder's children are visible, but also its subfolders' children as well. This customization helps reduce the amount of clicking that you have to do to browse the file system hierarchy.

1. In AXIOM Examine, in the **File system explorer**, click the **Selected folder only** drop-down.
2. Select the **All subfolders** option.

Save files and folders

In the File system explorer, you can save files and folders locally to your computer. When you save files and folders, AXIOM Examine saves the original file along with any associated metadata.

1. In AXIOM Examine, in the **File system explorer**, right-click a file or folder in **Evidence**.
2. Click **Save file / folder to**.
3. Browse to where you want to save the file or folder and click **Select folder**.

Saving databases

While a database is in use on a live system, it creates temporary files to store data. To properly save this type of database to your computer, make sure that you save the temp files in addition to the .db file. If you save only the .db file, the database appears to be empty when you open it on your computer.

Create artifacts using file snippets

While using the File system explorer, you might come across important evidence that isn't already associated with an artifact. If you want to display this evidence alongside other artifacts and include it in your exports, you can save the content manually.

1. In AXIOM Examine, in the **File system explorer**, right-click a file in **Evidence**.
2. In **Text and hex** for that file, select the group of hex or text characters that you want to create an artifact for.
3. Right-click the selection and click **Display as artifact**.

The new artifact appears in the Artifacts explorer in the Examiner defined group. The Details for the new artifact lists the size of the file, the name of the analyst who added the artifact to the case, and the date that the artifact was added.

You can also create artifacts from registry data. To learn more, see Exploring the registry.

Viewing the registry

The Windows Registry stores important information about system hardware, installed programs and settings, and user profiles. Typically, the registry has a very large hierarchy, and can be difficult and time consuming to browse. AXIOM Examine helps remove some of these issues by linking artifacts and files directly to registry keys, decreasing the amount of time you spend traversing the tree. You can find all the separate registry hives in the registry on the left side of your screen. When you select a hive, its keys are displayed in Evidence and details about each key are visible on the right.

Viewing evidence details in the registry

AXIOM Examine allows you to view artifact information in a number of different ways, depending on the type and format of the artifact.

In the Registry explorer, you can use Details to review information about each registry hive key including:

- **Registry key information**: Includes general information such as the registry key name and type.
- **Evidence information**: Includes source information and links to the file system.

In addition to Details the Registry explorer uses Text and hex depending on the type of source.

Viewing raw artifact data in Text and hex

In the File system, Registry, and Timeline explorers, use Text and hex to view the raw data associated with a file system item. This view allows you to verify the results that Magnet AXIOM produces and manually parse out any additional data that might not be included in the Details for an artifact.

For example, there might be data encoded in a picture that Magnet AXIOM might not be able to parse. By viewing the Hex source, you can manually extract the data yourself. You can also decode the hex values into common formats, including ASCII, binary, date/time, and more.

The *Text* view converts underlying bytes to ASCII text, which is generally a much cleaner view for text documents and for other ASCII-based data. As an examiner, you can use this feature to verify evidence and keywords. Text supports many different character encoding types that you can select from. The default character encoding is unicode (US-ASCII).

Browse to a specific offset

If you know the offset that you want to view, you can browse to it:

1. In AXIOM Examine, in the **File system** or **Registry explorer**, browse to the evidence item.
2. In **Evidence**, click the evidence item.
3. In **Text and hex**, click **Go to** and provide the offset that you want to view.
4. On your keyboard, press **ENTER**.

Search for a text string or hex value

1. In AXIOM Examine, in the **File system** or **Registry explorer**, browse to the evidence item.
2. In **Evidence**, click the evidence item.
3. In **Text and hex**, click **Find**.
4. Provide the string or hex value that you want to search for.
5. Select the search method that you want to use: **Text string** or **Hex value**.
6. On your keyboard, press **ENTER**.

Decode hex values

You can decode hex values into other formats to analyze the information in that specific format. When you decode hex values, the information appears in Decode at the bottom of Text and hex.

> Note: You can only decode up to 10 KB of data at one time.

1. In AXIOM Examine, in the **File system** or **Registry explorer**, browse to the evidence item.
2. In **Evidence**, click the evidence item.
3. In **Text and hex**, click **Decode**.
4. Click and select hex values to automatically decode that selection.

Save or copy text or hex data

You can save or copy a selection of text or hex data for use at a later time. To save or copy the data:

1. In AXIOM Examine, in the **File system** or **Registry explorer**, browse to the evidence item.
2. In **Evidence**, click the evidence item.
3. To select the data you want to save or copy, in **Text and hex**, click and drag text or hex values
4. Right-click and select **Save selection** or **Copy selection.**
5. If you chose to save the hex data, browse to the location where you want to save the data.
6. Provide a file name (ending in .txt), and then click **Save**.

Create artifacts using raw data

While using the File system or Registry explorers, you might come across important evidence that isn't already associated with an artifact. If you want to display this evidence alongside other artifacts and include it in your exports, you can save the content manually. After you create the new artifact, you can tag it, comment on it, and export it just like any other artifact. To save registry data as an artifact, do the following:

1. In AXIOM Examine, in the **File system** or **Registry explorer**, browse to the evidence item.
2. In **Evidence**, click the evidence item.
3. In **Text and hex** for that file, select the group of hex characters that you want to create an artifact for.
4. Right-click the selection and click **Display as artifact**.

The new artifact appears in the Artifacts explorer in the *Examiner defined* group. The *Details* for the new artifact list the name of the analyst / examiner who created the artifact.

You can also create artifacts from file snippets. To learn more, see Create artifacts using file snippets.

Discovering connections

The Connections explorer provides a visual representation of how artifact attributes in your case are related. You set the focus on an attribute of interest, like a file name, and then AXIOM Examine draws a map of connections that might otherwise be time-consuming or difficult to discover.

By quickly finding and presenting connections between all the evidence in your case—including computer, mobile, and cloud-based sources—AXIOM Examine enables you to drill-down to the supporting pieces of evidence so you can:

- **Discover how the evidence got there**: See where an item—like a picture—originated from on the evidence source, where it was sent, who it was shared with, and more.
- **Demonstrate attribution**: Drill-down into shellbags, .lnk files, jump lists, and more to see when a folder was opened, which files were opened in which applications, shortcuts that were created, and so on.
- **Visualize communications**: Map out communication between a person of interest and the individuals that person communicates with across all recoverable communication platforms including email, instant messaging, SMS, call logs, and more.

Build connections

AXIOM Examine builds connections by comparing attributes for artifact and file system items. By default, connections don't build when you create a case. You can configure AXIOM Examine to build connections automatically.

1. In AXIOM Examine, on the **Tools** menu, click **Build connections**.
2. In the status bar, click **View details** to see the progress while connections are building.

While connections are building, you can continue to browse through your case and add tags, comments, filters, and profiles. Once you've built connections initially, AXIOM Examine refreshes the connections if you add new evidence.

Build connections automatically

By default, you must manually trigger building connections in your cases. You can change this setting to automatically build connections.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. Under **Post-processing**, select the **Automatically build connections on case open** check box.
3. Click **Okay**.

View connections

After connections are built, a connections icon appears in Details in the Artifacts and File system explorers beside the attributes that you can create maps for. You can view connections based on different attributes of an artifact, such as hash, file name, sender, recipient, or source.

1. In AXIOM Examine, in the **Artifacts** or **File system explorer**, select the artifact that you want to view connections for.
2. In **Details**, click the connections icon. If an artifact has multiple values (for example, multiple recipients), click an item from the drop-down list.

When you click the connections icon for an attribute, AXIOM Examine automatically switches to the Connections explorer and creates a map to show you how that attribute relates to other items in your case.

Navigating maps

In the Artifacts or File system explorers, when you click the connections icon for an attribute, AXIOM Examine automatically switches to the Connections explorer and creates a map to show you how that attribute relates to other items in your case. The more specific an attribute, the more precise your map will be. For example, if you click a file name, the map will be more precise than if you click a general application type.

The map is a series of nodes (based on artifact attributes) and connectors.

ITEM	DESCRIPTION	NODE COLOR
Primary node	The primary node is the anchor from which the connections are created. In the Artifacts or File system explorers, when you click the connections icon for a specific attribute, you make it the primary node. In the map, you double-click a node to make it the primary node.	hot pink

ITEM	DESCRIPTION	NODE COLOR
Direct node	Direct nodes are attributes with a direct connection to the primary node. To view only the connection between a primary node and a direct node, click the direct node.	blue
Selected nodes	When you click a direct node, it becomes selected. The matching results refresh so you only see artifacts that contain both attributes of the primary and selected node, for example file name and application name. When you select a node, you bring the indirect connections for that node into focus.	teal
Indirect nodes	Indirect nodes show all the nodes that will come into focus if you make a selected node the primary node. These nodes are not directly related to the primary node that is currently in focus.	gray
Connectors	Connectors are lines representing the type of connection between two nodes. These include accessed with, shares partial path, used in, and so on.	—

Tips for navigating maps

Depending on the attribute you are interested in, there might be a large number of connections for a specific node. When you examine a complex map consider the following tips:

- Peek at connections to help you decide where to focus your examination. To peek at the connections for a specific node, and not be required to redraw the map, hover your mouse over it.
- Reposition a node by clicking the node and dragging it to a new position.
- Pop out the map so you can maximize it on a separate monitor by clicking the pop out icon beside the Connections drop-down list.
- Save a node as a point of reference by clicking and holding a node to save it. As you explore connections in the map, click any node in the Saved nodes bar at the top of the map to return to that view.
- Refine the map using filters by applying one or more filters to the items on the map. Use the Evidence filter to limit which evidence sources to show connections for. Use the Connectors filter to indicate the specific types of connections that you want to see. Use the Attributes filter to specify which artifact attributes to include.

Viewing matching results

You can view all of the matching artifact results for the selected node as it relates back to the primary node. For example, if the primary node is a file name, the matching results show all artifacts that contain that file name. For example, if you select a direct node such as sender, the matching results show all artifacts that contain both the file name and the sender.

Print a map

If you want to include a map of connections in your report, you can print it to paper or PDF. When you print a map, the primary node and focus nodes get included.

1. In AXIOM Examine, in the **Connections explorer**, right-click a node.
2. Click **Print**.
3. Follow the instructions on screen to print the map.

Save a map as an HTML file

If you want to include a map of connections in your HTML report, you can save the connections map as an HTML file.

1. In AXIOM Examine, in the **Connections explorer**, right-click anywhere in the map.
2. Click **View source**.
3. In the .txt file that appears, on the **File** menu, click **Save as**.
4. Browse to the location where you want to save the file.
5. Provide a **File name** ending in **.html**.
6. Click **Save**.

Viewing the timeline

Get a singular view into what's happening in your case with the Timeline explorer where you can see a flat timeline of all timestamped evidence from the Artifacts and File system explorers. The Timeline explorer is useful if you have an idea of when an event occurs and want to see if there's a spike in a suspect's online activity during that time—or, you might have already identified an important piece of evidence and want to build a story around it using results that occur before and after.

The Timeline explorer includes a visualization of time in an interactive graph where you can examine specific timeframes, identify spikes in activity, focus on specific dates, and establish patterns in behavior.

Below the graph, you'll find timestamped evidence from the Artifacts and File system explorers ordered chronologically. To help you review and analyze the evidence with ease, you'll find additional details and high-level categorization of the evidence by timeline category—such as browser usage, file/folder opening, user event, and more.

When you click an evidence item, you can view more artifact information. Depending on whether the item originated from the Artifacts or File system explorer and the type and format of the artifact, you will have the option to view a preview of the artifact, review media categorization details, review artifact details, or view raw file system artifact data in text and hex.

To help decrease the scope of evidence to be searched, apply filters to the data, such as data types, timeline categories, date/time ranges, and more.

Build the timeline

AXIOM Examine builds the timeline from timestamped evidence from the Artifacts and File system explorers. By default, the timeline doesn't build when you create a case, but you can configure AXIOM Examine to build the timeline automatically.

1. In AXIOM Examine, on the **Tools** menu, click **Build timeline**.

You can see the progress while timeline is building in the Timeline explorer or the status bar.

While the timeline is building, you can continue to browse through your case and add tags, comments, filters, and profiles. Once you've built the timeline initially, AXIOM Examine refreshes the timeline if you add new evidence.

Build the timeline automatically

By default, you must manually trigger building the timeline in your case. You can change this setting to automatically build the timeline.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. Under **Post-processing**, select the **Automatically build timeline on case open** check box.
3. Click **Okay**.

View the timeline

After AXIOM Examine builds the timeline, you can view all timestamped evidence in your case from the Artifacts and File systems explorers—in chronological order—in the Timeline explorer.

1. In AXIOM Examine, open the **Timeline explorer**.
2. Select a date or date range of evidence that you'd like to zoom into as a starting point.
3. Click **Okay**.

Details about all the artifacts in the spike appear in the evidence table below the timeline graph. Items that have multiple timestamps appear in the Timeline explorer once for each timestamp, and you can quickly move between timestamps in the timeline for a single hit item when a hit has multiple timestamps.

Tips for navigating the timeline graph

- To get a closer look at a particular time in the graph, scroll the track wheel on your mouse or toggle the Zoom option.
- To move backward or forward in time, click the graph and drag your mouse left or right. To quickly jump backward or forward in time, you can also click through the *Next page* and *Previous page* options.
- To view the date and number of hits for a spike, hover over a node in the graph. The date/time format updates according to how you're viewing hits in the timeline (by year, month, week, day, hour, or minute).
- To analyze hits in a spike in the timeline, click a node in the timeline graph. AXIOM Examine automatically jumps to the first timestamped item for the activity spike in the evidence table below the timeline graph.

- To change how you view the timeline—by years, months, weeks, days, hours, or minutes—change the date type. The horizontal axis below the graph updates to reflect your selection.
- To focus the graph to a specific date range, click Go to date to choose your desired date range.
- To help decrease the scope of evidence to be searched, apply filters to the data, such as data types, timeline categories, date/time ranges, and more.

Export timeline data

If you want to share evidence from the timeline, export it to a .csv file.

1. In AXIOM Examine, in the **Timeline explorer**, select and right-click items that you want to export.
2. Click **Create report / export**.
3. In the **Export type** drop-down list, click **CSV**.
4. Next to the **File path** field, click **Browse** and select the location you want to save the export. Click **Select folder**.
5. Click **Create**.

Timeline categories

CATEGORY	DESCRIPTION	EXAMPLE
Account usage	Evidence of a user account or system account being accessed or used.	Login/logout Password changes
Browser usage	Evidence of the target using a browser or navigating web related activity on the computer or phone.	Browser last visit date/-time Cache/cookies from browsers
Deleted file	Indicates that a file has been deleted. While the file might not be accessible any more, there is a timed record representing its deletion.	Recycle Bin deletion date/time
Device interaction	Indicates the user or system interacted with an external device that was not the computer or phone being examined.	IoT devices such as Google Home, Amazon Echo, OnStar or other cars, and more.

CATEGORY	DESCRIPTION	EXAMPLE
External device/USB usage	Evidence of a USB or other external device being connected to the system.	USB first connect date/-time USB last connect date/-time
File download	Indicates that a file was downloaded from an external source.	Chrome download activity Skype file transfers
File knowledge	Indicates a user or system has interacted with the file in some way, but it might not be known whether the file was actually opened or not.	MAC times
File/folder opening	Evidence of a user opening a file or folder.	Jumplists Shellbags LNK files
Financial transactions	Indicates an exchange of currency or services has occurred.	Wallet transactions Samsung Pay
Network activity	A timestamp of a network action or activity that occurred on the computer or phone.	WiFi connections Authentications RDP activity
Physical location	A timestamp placing the user or device at a specific location at a given time based on GPS coordinates or a physical address.	iOS cached locations Significant locations
Program execution	Evidence of an application or program being run at a specific time.	Prefetch last run time
Social activity	Evidence of public interactions through applications or service.	Instagram posts Tweets Facebook Wall posts

CATEGORY	DESCRIPTION	EXAMPLE
User communication	Evidence of any sort of private or semi-private group chat through applications or services.	Chat messages Email Direct messages
User event	Evidence related to an event outside the system or user’s account usage.	Calendar events such as meetings or birthdays

TAGGING EVIDENCE

Tags and comments help you organize evidence and identify artifacts that are important to your investigation. For example, you might apply the *Of interest* tag to artifacts you want to have a closer look at later. You can view all of the tags and comments that are applied to an artifact in Tags, profiles & media categories.

AXIOM Examine includes a set of system tags that you can use, or you can create your own.

When you export artifacts or create a portable case, any tags or comments that you have applied also get exported.

Tag evidence

Use tags to label evidence in a meaningful way for your investigation. After you tag evidence, you can use the Tags and comments filter to show only those items that are of interest to you.

Tagging is available for artifacts that appear in the Artifacts, File system, Connections, and Timeline explorers.

1. In AXIOM Examine, in **Evidence**, right-click the artifact or group of artifacts that you want to tag.
2. Click **Add / Remove tag**.
3. Select the tags that you want to apply.

After you apply a tag, the tag color appears beside the artifact.

Add comments to an artifact

Commenting is available for artifacts that appear in the Artifacts, File system, Connections, and Timeline explorers.

1. In AXIOM Examine, in **Evidence**, click the artifact that you want to comment on.
2. In **Tags, profiles & media categories**, click **Add comment**.
3. Type a comment and click **Okay**.

Understanding tag syncing between evidence in the Artifacts and File system explorers

For cases processed in Magnet AXIOM 3.9 and higher, tags that you apply to evidence automatically sync between the Artifacts and File system explorers. Depending on which explorer you tag the evidence from, AXIOM Examine will tag related evidence differently.

> Note: If you're examining a case processed with an earlier version of Magnet AXIOM, and you have not previously applied any tags to your case, tags that you apply to evidence also automatically sync between the Artifacts and File system explorers following the logic above. However, if you're examining a case processed with an earlier version of Magnet AXIOM, and you have previously applied tags to evidence in the case, tags do not automatically sync between the Artifacts and File system explorers. To enable tag syncing, you must untag all of your existing evidence in the case, and then reopen the case.

Tagging evidence from the Artifacts explorer

When you tag an artifact in the Artifacts explorer or when evidence is automatically tagged by AXIOM Process during a search, AXIOM Examine looks for corresponding files in the File system explorer using the source ID for the hit.

- If there is a one-to-one relationship between the artifact and a file in the File system explorer (i.e. a single source for the hit), AXIOM Examine automatically applies the same tag to both items—syncing the tags between the Artifacts and File system explorers.
- If there are multiple sources for an artifact hit, AXIOM Examine does not sync the tags.
- Note: AXIOM Examine will not sync tags for refined results, carved items, or items that have a location offset.

Tagging evidence from the File system explorer

When you tag an evidence item in the File system explorer or when evidence is automatically tagged by AXIOM Process during a search, AXIOM Examine looks for a corresponding parsed artifact hit in the Artifacts explorer.

- If there is a one-to-one relationship between the file in the File system explorer and a parsed artifact hit, AXIOM Examine automatically applies the same tag to both evidence items (syncing the tags between the Artifacts and File system explorers).

- If there are multiple artifact hits for the source evidence item, AXIOM Examine automatically creates a new artifact from the file in the file system and applies the same tag to both the evidence item in the File system explorer and the new artifact (syncing the tags between the Artifacts and File system explorers). You can quickly view these artifacts in the *Tagged from file system* artifact category in the Artifacts explorer.
- Note: AXIOM Examine will not sync tags for refined results, carved items, or items that have a location offset.

Removing tags from Tagged from file system artifacts

If you remove all tags from an artifact hit created from a tagged file in the File system explorer, the artifact hit is permanently deleted from the case, and the tag is removed from the file in the File system explorer. You can re-tag the file in the File system explorer, and AXIOM Examine will automatically create a new artifact from the file again.

Exporting tagged evidence

When you create an export or report from tagged items, AXIOM Examine exports evidence items from the Artifacts explorer only. Because your tags from the File system are synced with the Artifacts explorer (either in a one-to-one relationship or from newly created artifacts), your tags from the File system explorer are included in the report.

> Note: Artifacts created from a tagged file in the File system explorer are included in portable cases. If you remove all tags from an artifact created from a tagged file in the File system explorer, the artifact is permanently deleted from the portable case. However, when you merge the portable case back in to the original case, these artifact hits reappear in the in the Tagged from file system artifact category in the Artifacts explorer.

Customizing tags

Create a custom tag

You can create custom tags that are specific to your investigation and then apply those tags to evidence in your case. Each tag must have a unique name. You can customize the colors and shortcuts for your tags.

1. In AXIOM Examine, on the **Tools** menu, click **Manage tags**.
2. Click **Add tag**.
3. In the **Enter new tag** field, type a name for the tag, and then click **Add**.
4. If you want to change the color associated with the tag, click the current color, and then choose a new color.
5. If you want to change the shortcut assigned to the tag, in the **Shortcut** drop-down list, choose a different option.
6. Click **Okay**.

Import tags

You can import a list of tags in AXIOM Examine. Files must be .json or .txt format and each tag value must appear on its own line.

1. In AXIOM Examine, on the **Tools** menu, click **Manage tags**.
2. Click **Import tags**.
3. Browse to the .json or .txt file you want to import, and then click **Open**.
4. Optionally, customize the name, color, and shortcut for the tags.
5. Click **Okay**.

Export tags

You can export your list of tags to share with other examiners. You can export your list of tags to either .json or .txt format.

1. In AXIOM Examine, on the **Tools** menu, click **Manage tags**.
2. Click **Export tags**.
3. Browse to the location you want to save your tags.
4. In the **File name** field, provide a name for the file.
5. From the **Save as type** drop-down, select the file format you want to use, and then click **Save**.
6. Click **Okay**.

System tags

In addition to creating your own tags, AXIOM Examine includes a set of system tags that you can use or customize.

TAG	DEFAULT KEYBOARD SHORTCUT
Bookmark	Spacebar
Evidence	CTRL + 1
Of interest	CTRL + 3
Possible luring	No shortcut
Exceptions	No shortcut

> Note: When a search completes, you can view a summary of any files that were not fully processed due to artifact timeouts. These files are tagged in AXIOM Examine with the Exceptions system tag. The Exceptions system tag is not included in any exports/reports.

ORGANIZE EVIDENCE WITH PROFILES

Profiles help you organize evidence and identify artifacts that are important to your investigation. For example, you might create a profile called *Target A* to group the various user names and phone numbers used by that person of interest and then filter evidence to see only activity related to that person. You can view all of the profiles that are applied to an artifact in Tags, profiles & media categories.

> Note: Profiles are available only when you select the Identifiers artifact.

Create a profile

Create and apply profiles to associate identifiers (for example, user names and email addresses) with persons of interest. After you apply profiles, you can use the Profiles filter to show only the evidence that is associated with that individual.

1. In AXIOM Examine, on the **Tools** menu, click **Manage profiles**.
2. Click **Add profile** and provide a name for the profile.

3. Click **Add**.
4. Click **Okay**.

Apply a profile

When you apply a profile to a specific identifier, AXIOM Examine applies that profile to every artifact in the case that has that exact identifier.

1. In AXIOM Examine, in the **Artifacts explorer**, expand the **Refined results** group, and click **Identifiers**.
2. In Evidence, select the identifier or group of identifiers you want to apply a profile to.
3. In **Tags, profiles & media categories**, select the check boxes beside the profiles that you want to associate the identifier with.

Import profiles

You can import a list of profiles in AXIOM Examine. Files must be JSON or TXT format and each profile value must appear on its own line.

1. In AXIOM Examine, on the **Tools** menu, click **Manage profiles**.
2. Click **Import profiles**.
3. Browse to the JSON or TXT file you want to import.
4. Click **Open**.
5. Optionally, customize the profile names.
6. Click **Okay**.

Export profiles

You can export your list of profiles to share with other examiners. You can export your list of profiles to either JSON or TXT format.

1. In AXIOM Examine, on the **Tools** menu, click **Manage profiles**.
2. Click **Export profiles**.
3. Browse to the location you want to save your profiles.
4. In the **File name** field, provide a name for the file.
5. From the **Save as type** drop-down, select the file format you want to use.

6. Click **Save**.
7. Click **Okay**.

FILTERING EVIDENCE

You might have thousands, or even millions of hits in your case. Browsing through these results might seem like a time consuming task, but you can make it much more manageable by applying filters.

In AXIOM Examine, the filter bar allows you to create specific conditions for the results that you want to display. You can also stack filters so that each additional filter that you apply refines the displayed results even further.

Types of filters

Depending on the explorer you're using to view your evidence, you'll have a variety of filters available for you to use.

FILTER	DESCRIPTION	EXPLORER AVAILABILITY
Attributes	Show evidence in the Connections explorer by attribute of interest such as file name, identifier, sender, and more.	Connections
Artifacts	Show evidence by artifact type or artifact group.	Artifacts Timeline
Connectors	Show evidence based on how artifact attributes are related, such as accessed by, transferred to, child of, and more.	Connections
Content types	Show evidence based on a specific content type (for example, pictures, video, and audio). There is also an option to filter by files that are either accessible or inaccessible to users.	Artifacts
Data types	Show evidence in the Timeline explorer based on whether it originated from the Artifacts explorer or the File system explorer.	Timeline
Date and time	Show evidence based on date and time. You can search by absolute date/time (a specific range of dates and times) or by relative date/time (around the time of a specified date).	Artifacts File system Timeline

FILTER	DESCRIPTION	EXPLORER AVAILABILITY
Date and time attributes	Show evidence in the Timeline explorer based on date and time attributes.	Timeline
Evidence	Show evidence based on the source. For example, if you have evidence from both computer and iOS images, you can view evidence from the computer, the iOS, or both evidence sources.	Artifacts Connections Timeline
File attributes	Show evidence by file attribute. For example, you can opt to show only the files that are archived, deleted, hidden, or encrypted. To see all the attributes that a particular file has, see the File attributes property in Details.	File system
File size	Show evidence by file size (in bytes). You can specify an exact value, a range, or more than/less than values.	File system
Keyword lists	Show evidence based on keywords or keyword lists. You can stack keywords or keyword lists to refine your results even further. If you added keywords or keyword lists to your search in AXIOM Process, those lists and keywords appear as filtering options.	Artifacts
Keywords / search terms	Show evidence based on keywords and regular expressions that you provide in the search box.	Artifacts File system Registry
Media categorization	Show evidence based on the media categories that you apply to pictures and videos or that were applied by hash sets.	Artifacts
Media attributes (VICS)	Show evidence based on Video Image Classification Standard (VICS) media attributes and values.	Artifacts
Partial results	Show evidence based on whether a result is complete or partial. Because AXIOM Process searches both allocated and deleted space, recovered artifacts can be a mix of complete and partial results. Partial results are valuable but often require a manual investigation of the underlying data.	Artifacts
Profiles	Show evidence that you've assigned a profile to.	Artifacts

FILTER	DESCRIPTION	EXPLORER AVAILABILITY
Similar pictures	After you find similar pictures, this filter appears. You can adjust the scale to only view the most similar pictures, or broaden the results. You can also view the reference photo that you're currently using.	Artifacts (Thumbnail view only)
Skin tone	Show evidence based on the overall percentage of skin tone—for all different skin colors—in media files.	Artifacts
Tags and comments	Show evidence that you've tagged or commented on or evidence that has been tagged by Magnet.AI. Tags are labels that you manually apply to artifacts of interest. For more information about tags, see Tagging evidence.	Artifacts File system Timeline
Timeline categories	Show evidence by timeline category.	Timeline

Filtering by date and time

The Date and time filter allows you to specify the range of dates and times that you want to show artifact results for. You can filter by absolute date/time (a specific range of dates or times) or by relative date/time (evidence around a date or time). Any dates and times inside the specified range are displayed.

Filter evidence by a specific date or time

You can view evidence within a specific range of dates and times such as before a date, on a specific day of the week, in a custom time range, and more.

The Date and time filter is available in the Artifacts explorer and the File system explorer.

1. In AXIOM Examine, on the **Filters** bar, click **Date and time**.
2. Click **Absolute date/time**.
3. Set the **date range** and/or **time range** you want to filter by.
4. Click **Okay**.

Filter by relative date or time

When you've found evidence relevant to your investigation, you might want to know what else occurred around the same time. You can use the Relative date/time filter to view evidence around the time of a specific date.

The Date and time filter is available in the Artifacts explorer and the File system explorer.

1. In AXIOM Examine, on the **Filters** bar, click **Date and time**.
2. Click **Absolute date/time**.
3. In the **Anchor relative to** section, select the date and time you want to use as the anchor.
4. In the **Set range** section, select the range of time you want to filter by.
5. Click **Okay**.

Filtering by keywords

Filter by keyword list

If you added keywords or keyword lists to your search in AXIOM Process, those lists and keywords appear as filtering options in AXIOM Examine. To refine your results even further, you can stack keywords or keyword lists.

The Keyword list filter is available in the Artifacts explorer.

1. In AXIOM Examine, on the **Filters** bar, click **Keyword lists**.
2. Select the keywords or keyword lists you want to filter on.
3. Click **Okay**.

Import a keyword list

You can import a list of keywords, and then filter your evidence using those keywords.

1. In AXIOM Examine, on the **Filters** bar, click **Keyword lists**.
2. Click **Import keyword list**.

3. Browse to the keyword list you want to import.
4. Click **Open**.

Search by keyword

You can search the evidence using keywords or search terms to only show the items that contain those keywords. You can type a keyword that acts as a filter on the evidence. Keywords can include letters, numbers, or both letters and numbers. When a match occurs, AXIOM Examine highlights the matching text in Evidence and in Details.

You can search for keywords in the Artifacts explorer, the File system explorer, and Registry explorer.

- In the Artifacts explorer, AXIOM Examine searches all fragments (except for date and time fragments), and content of media and documents for the keyword.
- In the File system explorer, AXIOM Examine searches only within an item's file path for keyword matches—it doesn't search the contents of the file.
- In the Registry explorer, you can complete an advanced search by keys, values, and data and specify to match the whole string or match case.

To search by keyword, do the following:

1. In AXIOM Examine, on the **Filters** bar search box, provide the keyword you want to filter on.
2. Click **Go**.

Search by keyword using advanced search options

When you search the evidence in the Artifacts explorer using an advanced keyword search, you can search using multiple words or search terms and choose whether you want to see results for all (and "AND" search) or any (and "OR" search) of the search terms. For each keyword that you specify, you can choose to show only the items that include or exclude that word. You can further specify if you want to search for the whole word only, match the case, and search for the term if it appears near another word or set of characters..

To search by keyword using advanced search options in the Artifacts explorer, do the following:

1. In AXIOM Examine, on the **Filters** bar, click **Advanced**.
2. Select the **Search terms** option.

3. In the **Search by term** section, select whether you want to **include** or **exclude** the search term, and then provide the keyword you want to filter on.
4. To search for the term if it appears near another word or set of characters, select **Is located near another term** and provide the details for the secondary term.
5. To search for the whole word rather than partial instances, select **Find whole word only**.
6. To search for instances of the word with the same letter case, select **Match case**.
7. To add another search term, click **Add another term**. Choose whether you want to see results for all or any of the search terms, and then complete Steps 3-6.
8. Optionally, select the **Exclude source path in search** option.
9. Click **Search**.

Search by regular expression

Search by regular expression (regex) to narrow your search results. AXIOM Examine supports the .NET regex format.

1. In AXIOM Examine, on the **Filters** bar, click **Advanced**.
2. Select the **Regex pattern matching** option.
3. In the **Regex** field, provide the regular expression you want to filter on.
4. Optionally, select the **Exclude source path in search** option.
5. Click **Search**.

Search by keyword snippet

You can filter by keyword snippets to see all of the evidence—not just artifacts—that contains a specific keyword. If you turned on keyword search for all content when you set up your case in AXIOM Process, any keyword with a result appears in Keyword snippets. To provide additional context, the keyword snippet includes the 50 bytes that appear before and after the keyword. For more detailed information about a specific keyword result, click the source link to go to the original file.

1. Expand Keyword snippets.
2. Click the keyword that you want to refine your results with.

Filter by accessible and inaccessible files

Use the Content types filter to discover which files are accessible to users and which ones aren't. The filter option only appears if there are inaccessible files in the evidence that you are examining.

The Content types filter is available in the Artifacts explorer.

1. In AXIOM Examine, on the **Filter** bar, click **Content types**.
2. Select the **Items accessible by users** or **Items inaccessible by users** option.

Inaccessible files are files recovered from the following locations:

- pagefile.sys
- hiberfil.sys
- swapfile.sys
- $Mft
- $MftMirr
- $Logfile
- $Volume
- $AttrDef
- $Bitmap
- $Boot
- $BadClus
- $Secure
- $Upcase
- $Extend
- Unallocated space
- Unpartitioned space
- File slack
- Uninitialized file area
- Orphaned files
- Overwritten files
- Deleted files

Files recovered from all other locations are considered accessible.

Filter by skin tone percentage

To help detect explicit content in media like pictures, video, and carved video, AXIOM Process uses a skin tone detection algorithm. By converting data to an advanced color space and isolating clusters of pixels that appear to be skin, AXIOM Examine filters content based on the overall percentage of skin tone—for all different skin colors—in a specific media file. Values are within a range of 0% and 100%. A value of 0% indicates that there is no skin tone present, while 100% indicates there's only skin tone present.

The *Skin tone percentage* filter is available in the Artifacts explorer.

1. In AXIOM Examine, on the **Filters** bar, click **Skin tone**.
2. Set the skin tone percentage range you want to detect.
3. Click **Okay**.

> Tip: You can optimize this filter by importing hash lists for files like standard operating system icons and

> screen savers that are not relevant to your case. AXIOM Examine will ignore these files so that they don't clutter your evidence. For more information, see Ignore non-relevant files.

Filtering by column

Filter by column using a basic search

When using Column view, you can set filters on individual columns that are independent of any global filters that you specify. For columns that are numeric values or dates, you can specify the range of values to include, or a specific value to match. For columns that are strings, you specify a keyword or regex string.

1. In AXIOM Examine, right-click the header of a column and select **Filter on column**.
2. Depending on the type of column, complete one of the following options:
    - For date and time columns, select a start and end date and time.
    - For numeric columns, specify a range or an exact value to filter on.
    - For string columns, specify a search term.
3. Click **Search**.

> Note: If you sort on a column that contains a string that begins with special characters (i.e. not numbers or letters), you can find this evidence at the top or bottom of the column.

Filter a numeric column using an advanced search

When using Column view in the Artifacts and File systems explorer, you can set advanced filters on numeric columns and complete an advanced search using search terms or regex pattern matching.

To filter numeric columns using advanced search terms in the Artifacts and File systems explorer, do the following:

1. In AXIOM Examine, on a numeric column name, click **More options** > **Filter on column**.
2. On the **Advanced** tab, select the **Search terms** option.
3. In the **Search by number** section, select whether you want to **include** or **exclude** the number, and then specify a range or an exact value to filter on.
4. To add another search term, click **Add another number**, and then complete Steps 3-4.
5. Click **Search**.

To filter numeric columns using regex pattern matching, in the Artifacts and File systems explorer, do the following:

1. In AXIOM Examine, on a numeric column name, click **More options** > **Filter on column**.
2. On the **Advanced** tab, select the **Regex pattern matching** option.
3. In the **Regex** field, provide the regular expression you want to filter on.
4. Click **Search**.

Filter a string column using an advanced search

When using Column view in the Artifacts and File systems explorer, you can set advanced filters on string columns and complete an advanced search using search terms or regex pattern matching. Search using multiple words or search terms and choose whether you want to see results for all (and "AND" search) or any (and "OR" search) of the search terms. For each keyword that you specify, you can choose to show only the items that include or exclude that word. You can further specify if you want to search for the whole word only, match the case, and search for the term if it appears near another word or set of characters.

To filter string columns using advanced search terms in the Artifacts and File systems explorer, do the following:

1. In AXIOM Examine, on a string column name, click **More options** > **Filter on column**.
2. On the **Advanced** tab, select the **Search terms** option.
3. In the **Search by term** section, select whether you want to **include** or **exclude** the search term, and then provide the keyword you want to filter on.
4. To search for the term if it appears near another word or set of characters, select **Is located near another term** and provide the details for the secondary term.
5. To search for the whole word rather than partial instances, select **Find whole word only**.
6. To search for instances of the word with the same letter case, select **Match case**.
7. To add another search term, click **Add another term**. Choose whether you want to see results for all or any of the search terms, and then complete Steps 3-6.
8. Optionally, select the **Exclude source path in search** option.
9. Click **Search**.

To filter string columns using regex pattern matching, in the Artifacts and File systems explorer, do the following:

1. In AXIOM Examine, on a string column name, click **More options** > **Filter on column**.
2. On the **Advanced** tab, select the **Regex pattern matching** option.
3. In the **Regex** field, provide the regular expression you want to filter on.
4. Optionally, select the **Exclude source path in search** option.
5. Click **Search**.

ADDING MORE EVIDENCE TO A CASE

During a search, Magnet AXIOM might recover evidence that could help you find additional evidence. You can add this new evidence to your case.

> Tip: When you add new evidence to a case, make sure to provide Scan information in AXIOM Process > *Case details*. This allows you to keep track of the separate acquisition instances in a case.

- Recategorize media files in your case
- Import CPS evidence

Add new evidence to your case

If you discover new digital evidence sources, you can easily add them to an existing case. You can add new evidence to an existing case from either AXIOM Examine or AXIOM Process .

1. Complete one of the following options:
    - In AXIOM Examine, on the **Process** menu, click **Add new evidence to case**.
    - In AXIOM Process, click **Browse to case** and select the case you want to add evidence to.
2. When AXIOM Process opens, choose how to search the evidence the same way that you would for any new case.
3. To load new results while the evidence is being processed, in AXIOM Examine, click **Load new results**.
4. To load the new results when processing is complete, click **Okay**.
5. If the new evidence includes chat messages, click **Okay** to update the chat threads.

Remove evidence from case

To delete evidence from your case, remove an evidence source and all associated evidence.

> Warning: Removing an evidence source is a permanent action that can't be undone.

1. In AXIOM Examine, on the **Process** menu, click **Remove evidence from case**.
2. Select the evidence source you want to remove and click **Okay**.
3. To confirm you want to remove the evidence, click **Remove evidence source**.

Add cloud evidence using recovered passwords and tokens

During a search, if AXIOM Process encounters tokens or passwords for a cloud account, it creates an artifact for them. From the Artifacts explorer in AXIOM Examine, you can use these passwords and tokens to open AXIOM Process and add a cloud evidence source. IMAP/POP email and Apple accounts can't be accessed using this method.

1. In AXIOM Examine, in the **Artifacts** explorer, browse to **Cloud** > **Cloud passwords and tokens**.
2. Right-click the password or token that you want to use and click **Add new cloud evidence using passwords/tokens**.
3. In AXIOM Process, confirm that you proper search authorization, as described in Sign in to a cloud account. A spinner appears while AXIOM Process attempts to access the account using the token or password you chose.
4. If the login is successful, select the services and sub-services that you want to acquire.
5. After the search starts, click **Load new results** in AXIOM Examine to view the results.

If the login attempts are unsuccessful, AXIOM Process notifies you that you've entered an incorrect password and does not proceed past the sign-in screen. An unsuccessful attempt can be due to one of the following reasons:

- The target changed their password
- The token expired

Acquire and decrypt a WhatsApp backup using a recovered decryption key

After you acquire an Android image, you can attempt to recover the user's WhatsApp decryption key and use the key to decrypt their WhatsApp cloud backups. In some cases, the decryption key might not be available if you acquired a quick image of the Android device. If the WhatsApp data is missing from the quick image, attempt to acquire a full image.

Before you begin: To acquire and decrypt a user's WhatsApp backups from the cloud, you'll require the following information:

- Google credentials (user name and password) and multi-factor authentication details if required
- Phone number associated with the account
- Decryption key

To acquire and decrypt a WhatsApp backup:

1. In AXIOM Examine, in the **Artifacts** explorer, browse to **Mobile** > **Android WhatsApp User Information**.
2. Find the **Private Key** and **Phone Number**.
3. On the **Process** menu, click **Add new evidence to case**.
4. In AXIOM Process, click **Evidence sources** > **Cloud** > **Acquire evidence**.
5. Confirm that you have the proper search authorization.
6. Click **WhatsApp**.
7. Provide the user's Google email address, and then click **Next**.
8. Provide the user's Google password, and then click **Next**.
9. If applicable, provide 2-step verification details.
10. When prompted to trust Magnet Forensics International, Inc., click **Allow**.
11. Provide the target's phone number, including country code, and then click **Next**.
12. Select the backups you want to acquire, and then click **Next**.
13. Browse to **Artifact details** > **Cloud artifacts** > **Cloud WhatsApp Backups** artifact, and click **Options**.
14. In the **Options for decrypting WhatsApp** dialog, provide the **Private Key** listed in the **Android WhatsApp User Information** artifact in AXIOM Examine and click **OK**.
15. Click **Go to Analyze evidence** and click **Analyze evidence**.

Recategorize media files in your case

If you categorized your media for Project VIC using a third-party tool, you can import the .json files to apply those categorizations to the media in your case after initial processing.

1. In AXIOM Examine, on the **Process** menu, click **Categorize pictures and videos by hash value**.
2. When AXIOM Process opens, browse to **Processing details** > **Categorize pictures and videos.**
3. In **Categorize pictures and videos by hash value**, click **Add file**.
4. Browse to the location where you saved the .json file and click **Open**.
5. If applicable, clear the **Enabled** option next to any previously imported .json files that you don't want to use for this search.
6. Click **Analyze evidence**.

Import CPS evidence

To help protect children that are targeted by suspects using the internet, the Child Rescue Coalition's Child Protection System (CPS) collects online data that tracks person-to-person activity such as IP addresses, file hashes, person-to-person user GUIDs, and more.

You can add evidence from the CPS to your case by importing the .csv files into AXIOM Process.

1. In AXIOM Examine, on the **Process** menu, click **Add CPS export file**.
2. When AXIOM Process opens, browse to **Processing details** > **Add CPS data to search**.
3. Click **Add CPS export file**.
4. Browse to the .csv file that you want to add to your case and click **Open**.
5. Click **Analyze evidence**.

VIEWING THE SOURCE OF EVIDENCE

Source linking provides a way to quickly browse between the Artifacts, File system, and Registry explorers without having to click through large file and folder structures. Source linking saves you time and can help you verify artifacts and dig deeper into the raw data. The following sections describe how to view the source and registry data for an artifact. For more information about viewing the artifact associated with a file, see Exploring the file system.

View the source of an artifact result

For some types of artifacts, you might require more information than is available in the Artifacts explorer. For example, you might want to view the hex source or database for an artifact to identify and retrieve additional information. If this functionality is available for an artifact result:

1. In AXIOM Examine, in the **Artifacts explorer**, browse to an evidence item.
2. In **Evidence**, click the evidence item.
3. In **Details** > **Evidence information**, click the **Source** link.

> Note: Some artifacts might have more than one source link, which means that the artifact is comprised of data from more than one location.

When you click the source link, AXIOM Examine switches to the File system explorer and opens the correct location in the file system. If the source of the artifact is a database, you can view the database tables and their content. For other file types, you can use Text and hex to look at the source of the file and decode the hex values into different formats.

View registry entries for an artifact result

For artifacts that Magnet AXIOM creates from the Windows registry, you can view the original registry keys where the artifacts come from. Many of the Windows operating system artifacts come from the registry, such as USB Devices, Network Interfaces, User Accounts, and more.

1. In AXIOM Examine, in the **Artifacts explorer**, browse to an evidence item.
2. In **Evidence**, click the evidence item.
3. In **Details** > **Evidence information**, click the **Location** link.

> Note: Not all artifacts have associated registry data. Some artifacts might have more than one location

> link, meaning that the artifact contains information from more than one registry location.

When you click the location link, AXIOM Examine switches to the Registry explorer and opens the registry key associated with the artifact.

EXPORTING AND SHARING EVIDENCE

In AXIOM Examine, you can create various types of exports and reports in order to share evidence and collaborate on your cases.

The exporting wizard allows you to customize which items and details to include in your export / report. You can also create and import column configurations and templates to avoid selecting the same details for multiple exports.

You can also use specialized exports to share information such as Project VIC categorized media and connections maps. Create portable cases to send to your stakeholders so they can examine selected evidence items.

ACTION	DESCRIPTION
Exporting evidence using the wizard	Share evidence in a number of different formats, including Excel, XML, HTML, PST, PDF, and more. Customize which items and details to include, or use templates and column configurations to streamline the exporting process.
Create and manage column configurations	When you create your export, you can use pre-set column configurations. In AXIOM Examine, you can create, import, and export column configurations.
Create and manage templates	When you create your export, you can use pre-set artifacts to include, columns, and format options. In AXIOM Examine, you can create, import, and export templates.
Exporting specialized outputs	Use different outputs to create specialized exports. Using the exporting wizard, export evidence in a different language, chat threads, and Project VIC / CAID categorized media items. You can also export metadata, timeline data, memory artifacts, and connections maps using other explorers and exporting capabilities in AXIOM Examine.
Working with portable cases	Collaborate on a case with other examiners and stakeholders by creating a portable case in AXIOM Examine.

Exporting evidence using the exporting wizard

About the exporting wizard

Use the exporting wizard to create and customize exports and reports in AXIOM Examine. When you create an export, the wizard walks you through a series of steps that are customized to the type of export you're creating.

First, you can choose the type of export / report you want to create. You can share evidence in many formats, including Excel, XML, HTML, PST, PDF, and more.

Next, you can choose which items you want to include in your export / report (such as tagged items, Case dashboard cards, etc.), or you can choose to use a template. When you use a template, the export / report options are automatically configured based on the settings in your template—so you can either proceed right to building your report, or you can modify the settings during the rest of the workflow.

Depending on the export type, you can also choose which artifact categories (or specific artifacts) you want to include, configure additional artifact details, configure columns to include or use column configurations, customize the title page, and customize formatting options.

Finally, you can preview the names and sizes of all the files that will be included in your export.

Create an export

1. In AXIOM Examine, click **File** > **Create export / report**. Or, if you want to export a specific selection in the current view, select and right-click an artifact group or specific evidence items, then click **Create export / report**.
2. Under **Export / report format**, click a format and then click **Next**.
3. In **Items to include**, select what you want to export and then click **Next**.
4. If applicable to your export type, **Select artifacts** or artifact categories you want to include and then click **Next**.
5. If applicable to your export type, **Configure the artifact details** and then click **Next**.
6. If applicable to your export type, follow the steps to **Customize title page**, **Customize formatting options**, and **Provide additional information**, then click **Next**.
7. On the **Preview and save** screen, click **Browse** and select the location where you want to save the

export. Click **Select folder**.

8. On the **Preview and save** screen, click **Save**.

> Note: AXIOM Examine saves exports to your case folder, with a UTC time stamp. Depending on the archive explorer you use to view the exported .zip file, the times of the artifacts might be converted to your local time. You can use tools such as 7-Zip to convert the artifact times back to what you see in AXIOM Examine.

Export types

You can create exports and reports that include different types of evidence, details, attachments, and more. AXIOM Examine supports ten different export formats that are useful in different situations. The table below describes each export type, some possible use cases, and possible limitations that you should keep in mind.

EXPORT TYPE	DESCRIPTION AND USE CASES
CSV	This option exports evidence, including timeline data, to a comma-separated value (CSV) file that you can open in text editor or spreadsheet applications. As the name suggests, each fragment in an artifact is separated by a comma. This option does not include any attachments with the export. Use this export type to export metadata and timeline data, for example. This export is not recommended for exports that include chat messages in a different language than the UI, or other multiline UTF-8 encoded text (Excel exports are a recommended alternative to CSV in these instances).
Excel	This option exports evidence to an .xlsx file. Use this export type to prevent display errors that are common in .csv file exports of multiline UTF-8 encoded text (for example, chat messages in a different language than the UI).
HTML	This option exports evidence to a package of user-friendly HTML files with built-in navigation and includes attachments. If your case includes media categorizations, the HTML export includes a summary of media categorization results. Double-click the Report.html file to open the export in a web browser. Use this export type to export chat threads, connections maps (from the Connections explorer), case dashboard cards, and evidence in a different language than the UI.

EXPORT TYPE	DESCRIPTION AND USE CASES
Identifiers	This option exports all of the identifiers in a case to a .json file so that you can share the information with other organizations. The export requires that you provide your organization name and contact information so that if another organization gets a match on one of your identifiers they can contact you to request more information about your case.
Magnet REVIEW	This option exports all evidence you selected to an .xml file with attachments. This option exports in UTC time and in English only. Use this export type to export content from AXIOM Examine to Magnet REVIEW.
PDF	This option exports all evidence you selected to PDF, a read-only format that's easily printable. This option does not include any attachments with the export. If your case includes media categorizations, the PDF export includes a summary of media categorization results. Use this export type to export chat threads, connections maps (from the Connections explorer), case dashboard cards, and evidence in a different language than the UI.
PST	This option exports Microsoft Outlook email messages to a .pst file that you can open in a PST viewer. This option does not include content like calendar items, contacts, or tasks. PST exports are designed for Microsoft Outlook, but this export type also supports the following email artifacts: • Outlook Emails • Cloud IMAP/POP Emails • Cloud iCloud Mail • Cloud MBOX Emails • Cloud Gmail Messages
Portable case	This option exports all your evidence to a portable case that users without a full version of Magnet AXIOM can use with limited capabilities. A portable case contains the artifact database and evidence sources, combined with a lightweight version of AXIOM Examine. Certain features are unavailable to create a more streamlined experience for non-technical users. For more information, see the portable case quick start guide.

EXPORT TYPE	DESCRIPTION AND USE CASES
VICS 1.3, VICS 2.0 (JSON)	This option exports reviewer graded media in a .json file using the Project VIC specification. For more information about Project VIC, see www.projectvic.org. Use this export type to share reviewer graded media with Project VIC or CAID.
XML	This option exports all evidence you selected to an .xml file. You can choose to include external files. For more information about the structure of the .xml file, see Sample XML output. Use this export type to export chat threads, evidence that you want to use with another tool or script, and evidence that includes external files.

Items to include in your export

When you share evidence, you choose which evidence items you want to include. Depending on the export type that you've chosen, different options will be available.

OPTION	DESCRIPTION
Graded media items	For VICS 1.3 and VICS 2.0 export types, export the graded media metadata and attachments in the case. You can choose to export attachments for reviewer graded items only. If you enabled a pre-set media categorization profile for Canada (Project VIC), the United States (Project VIC), or the United Kingdom (CAID), the following categories are included in the export by default: • Canada (Project VIC): Category 1 • International (Project VIC): Categories 1-2 • United Kingdom (CAID): All categories except 8 • United States (Project VIC): Categories 1-3
Selected items only	Export only the items you selected in Evidence.
Items in the current view	Export all the items or media items currently visible in Evidence. The items that AXIOM Examine displays depend on which artifacts you select and the filters that you apply. For example, you can select a specific artifact (such as Skype Messages) and apply a date filter to include only the messages in the last six months.

OPTION	DESCRIPTION
Tagged items	Export only the items you tagged. You can select all tagged items in the case, or only items that you have applied specific tags to.
All evidence	Export all the evidence or all media items in the case.
Case dashboard cards only	For HTML and PDF reports, export only the case information from the selected case dashboard cards.

Configure artifact details

Under **Configure artifact details**, certain export types allow you to select or deselect various options about what information you want to include in your export.

DETAIL	DESCRIPTION
Include attachments	If email or other messaging artifacts are exported, attachments will be listed with the message in the report itself, and will be exported in a separate folder.
Include chat threads	If you export messages that are available in conversation view, your export will include these threaded conversations in addition to the report with the metadata you've chosen to include.
Make external links click-able	If any of the artifact data in your export includes external links, you'll be able to click on them and view the external webpage.
Blur / hide categorized media	The report will blur or hide sensitive pictures or videos in your report. Blurring and blocking is based on the existing media categorization in your case.

Format options

For HTML and PDF reports, you can choose to create one report that includes all artifact types, or create separate reports for each artifact type. If you create one report, you can choose how you want to order the evidence items. If you create separate reports, each artifact type will save to a separate file.

For Excel reports, you can choose to create one report that includes all artifact types on separate pages, or create separate workbooks for each artifact type.

Creating and managing column configurations

Creating column configurations

Column configurations help to streamline the exporting process by predetermining which columns will be displayed in applicable reports. Certain columns might be more useful for different types of cases, so it is helpful to create column configurations that can be reused in these cases. When you create an export, you can save the column configuration settings for use in future exports. You can also import other users' column configurations.

Use the column configuration in your current view for your export

If you're using the Column view in the Artifacts explorer, you can maintain the customizations that you make to the Column view in your export. For example, if you reorder or hide columns under Evidence, your export does the same.

1. In AXIOM Examine, right-click an artifact and click **Create export / report**.
2. Follow the instructions in the **Create export / report** window to select your export / report format and customize the items you want to include.
3. In **Configure artifact details**, under **Customize columns to include**, click **Manage column configurations**.
4. In the **Manage column configurations** window, click **Use columns from current view in AXIOM Examine**.
5. Click **Save and close**.
6. Follow the rest of the instructions in the **Create export / report** window to export your evidence.

Create a column configuration

When you create an export, you can create a new column configuration for use in future exports. The order of the columns in the report will reflect the order of the columns as they currently appear in AXIOM Examine.

1. In AXIOM Examine, click **Tools** > **Manage export / report settings**.
2. Under **Manage column configurations**, click **Create new**.

3. Select an artifact from the left navigation menu and select the columns you want to include. Repeat for all applicable artifacts.
4. Enter a name for the column configuration, and then click **Save and close**.

Import another user's column configuration

You can import another user's column configuration to use for your own exports.

1. In AXIOM Examine, click **Tools** > **Manage export / report settings**.
2. Under **Manage column configurations**, click **Import**.
3. Browse to the JSON file that contains the column configuration and click **Open**.

When you create your export / report, on the **Configure artifact details** screen, under **Configure columns to include**, select **Specific columns only** and then select the imported column configuration in the drop-down list.

Export a column configuration

You can export a column configuration so that other examiners can use it in their own exports.

1. In AXIOM Examine, click **Tools** > **Manage export / report settings**.
2. Under **Manage column configurations**, hover the mouse over the column configuration you want to export and click **Export**.
3. Browse to the folder where you want to save the JSON file.
4. Enter a name for the file, and then click **Save**.

Creating and managing templates

Creating export templates

Templates help to streamline the exporting process by predetermining the export's artifact types, columns, and format options. When you create an export, you can save the settings for use in future exports. You can also use Magnet AXIOM's system templates, or import other users' templates. When you use templates, you can edit the selections during the export workflow.

> Note: Templates are not available for Identifiers, PST, and VICS export formats. These formats are

> more streamlined, so you don't need to use templates to save time.

Save export settings as a template

When you create an export, you can save the settings for use in future exports of the same format. Magnet AXIOM saves your selected artifact types, column configuration, and formatting options, if applicable.

1. In AXIOM Examine, click **File** > **Create export / report**.
2. Follow the instructions in the **Create export / report** window to select your export / report format and customize the items you want to include.
3. In **Preview and save**, click **Save settings to template**.
4. In the **Create new template** window, type a template name and click **Create**.

Create a new template

You can create a new template directly from AXIOM Examine. Magnet AXIOM saves your selected artifact types, column configuration, and formatting options, if applicable.

1. In AXIOM Examine, click **Tools** > **Manage export / report settings**.
2. Under **Manage templates**, click **Create new**.
3. Follow the instructions in the **Create export / report** window to select your export / report format and customize the items you want to include.
4. In **Preview and save**, click **Save settings to template**.
5. In the **Create new template** window, type a template name and click **Create**.

Import a template

You can import another user's template to use for your own exports of the same format.

1. In AXIOM Examine, click **Tools** > **Manage export / report settings**.
2. Under **Manage templates**, click **Import**.
3. Browse to the JSON file that contains the template and click **Open**.

When you create your export / report, on the Items to include screen select **Use a template**, then select the imported template from the dropdown menu.

Export a template

You can export a template so that other examiners can use it in their own exports.

1. In AXIOM Examine, click **Tools** > **Manage export / report settings**.
2. Under **Manage templates**, hover the mouse over the template you want to export and click **Export**.
3. Browse to the folder where you want to save the JSON file, enter a name for the file, and click **Save**.

Edit a template

You can edit all user-created templates, but not system-created ones.

1. In AXIOM Examine, click **Tools** > **Manage export / report settings**.
2. Under **Manage templates**, hover the mouse over the template you want to edit and click **Edit**.

   > Tip: If you want to create a template using any template as the basis, including a system-created template, you can **Duplicate** the template first, and then edit the copy.

3. In the **Manage export / report settings** window, follow the steps to make changes to the template.
4. On the **Format options** screen, click **Save template**.
5. To rename the template, under **Template name**, double-click the current name. Enter a new name, then click **Update**.

Exporting specialized outputs

Exporting specialized outputs using the exporting wizard

You can use the exporting wizard in AXIOM Examine to create exports for specific purposes.

Export evidence that is in a different language

If you want to share evidence that's in a different language, export it to an Excel, HTML, or PDF file. Excel spreadsheets, HTML files, and PDF files support multi-line UTF-8 encoded text (for example, chat messages in different languages), so you won't see display errors that are common in other types of exports (like .csv files).

1. In AXIOM Examine, select and right-click an artifact group or items that you want to export.
2. Click **Create export / report**.
3. Under **Export / report format**, click **Excel**, **HTML**, or **PDF**.
4. Follow the instructions to customize and create your export.

> Tip: If you created an Excel report and the evidence contains content that appears on multiple lines, for example chat messages, turn on the wrap text feature in Microsoft Excel. (In Excel, press **CTRL + A**. On the toolbar, click **Wrap Text**.)

Export a chat thread

When you save a chat thread to your case, the file is named with the name of the chat application and the date and time stamp of the last message in the thread. For example, "Skype Chat Messages - 7_05_2016 3_09_04 PM."

1. In AXIOM Examine, in the **Conversation view**, right click the chat thread that you want to export.
2. Click **Create report / export**.
3. In the **Export type** drop-down list, select **HTML** or **PDF**.
4. Next to the **File path** field, click **Browse** and select where you want to save the export. Click **Select folder**.
5. In **Items to include**, select the chat threads that you want to export.
6. In **Level of detail**, complete one of the following options:
    - To save the information to one report, select **High-level information**
    - To create individual reports for each artifact type (for example, one report for Skype Chat Messages and another for GoogleTalk messages), select **Detailed information** .
7. Click **Create**.

Export media categorizations from a case to Project VIC or CAID

After you've categorized pictures and videos in your case, you can create a JSON export of the reviewer graded media to share with Project VIC or CAID. You can select the media items you want to include in the export such as graded media. For more information about choosing which media items to include, see Evidence export options. If you've enabled a pre-set media categorization country profile, the following categories are included in the export by default:

- Canada (Project VIC): Category 1
- International (Project VIC): Categories 1-2
- United Kingdom (CAID): All categories except 8
- United States (Project VIC): Categories 1-3

After you choose the category metadata you want to include, select the subset of categories you want to include attachments for in the export. Your export will include a .json file and a folder with attachments for included metadata items.

1. In AXIOM Examine, on the **File** menu, click **Create report / export**.
2. In the **Export type** drop-down list, click **VICS 1.3** or **VICS 2.0**.
3. Next to the **File path** field, click **Browse** and select where you want to save the export. Click **Select folder**.
4. In **Items to include**, select the media options you want to include in your export.
5. In **Contact information**, provide your contact information so that other organizations can contact you if they get a match on one of your identifiers.
6. Click **Create**.

Other types of exports

Some export types allow you to export specific kinds of data from various different explorers and views in AXIOM Examine. These export types don't use the exporting wizard because there are fewer options to choose from.

Export metadata

In the File system explorer, you can export the metadata associated with files or folders to a .csv file. By default, AXIOM Examine saves exported metadata to your case folder.

1. In AXIOM Examine, in the **File system view**, browse to the file or folder of interest.
2. In **Evidence**, right-click the item you want to export metadata for. To select multiple items, press **CTRL** and click the items. Then, right-click one of the highlighted items.
3. Click **Export details**.
4. Click **Browse to location** and select the location where you want to save the export. Enter a file name.
5. Click **Save file**.

Export timeline data

If you want to share evidence from the timeline, export it to a .csv file.

1. In AXIOM Examine, in the **Timeline explorer**, select and right-click items that you want to export.
2. Click **Create report / export**.
3. In the **Export type** drop-down list, click **CSV**.
4. Next to the **File path** field, click **Browse** and select the location you want to save the export. Click **Select folder**.
5. Click **Create**.

Export memory artifacts

You can use AXIOM Examine to export memory artifacts from your case to import into other tools. You can choose to export files based on their type:

- Process executable files (procdump)
- Dynamic link library files loaded by the process (dlldump)
- Memory associated with a particular process (memdump)
- Open files in memory (dumpfiles)
- Range of pages described by a VAD node (vaddump)

To export memory artifacts, complete the following steps:

1. In AXIOM Examine, right-click the memory artifact you want to export, and then click **Export memory items**.
2. In the **Export memory items** dialog, complete the following actions:
    1. In **Export details**, provide the **Folder name** and **File path** that you want to use.
    2. In **Items to include**, select the memory items that you want to export.
3. Click **Export**.

Export a connections map

Print or export a connections map as a PDF

If you want to include a map of connections in your report, you can print it to paper or PDF. When you print a map, the primary node and focus nodes get included.

1. In AXIOM Examine, in the **Connections explorer**, right-click a node.
2. Click **Print**.
3. Follow the instructions on screen to print the map.

Export a connections map as an HTML file

If you want to include a map of connections in your HTML report, you can save the connections map as an HTML file.

1. In AXIOM Examine, in the **Connections explorer**, right-click anywhere in the map.
2. Click **View source**.
3. In the .txt file that appears, on the **File** menu, click **Save as**.
4. Browse to the location where you want to save the file.
5. Provide a **File name** ending in **.html**.
6. Click **Save**.

Collaborate on cases with others using portable case

To collaborate on a case with other examiners and stakeholders, you can create a portable case in AXIOM Examine.

When you share a portable case with other stakeholders, they can explore the evidence, and add their own comments, tags, media categorizations, and bookmarks. Stakeholders don't need to have Magnet AXIOM installed to review a portable case. When they complete their reviews, you can merge their findings back into the original case.

Create a portable case

Create a portable case to share evidence from an investigation with stakeholders who might not be forensic examiners and might not have access to a full version of Magnet AXIOM. You can choose which evidence items you want to include, share all of the evidence you recovered with Magnet AXIOM, or choose specific evidence items such as tagged evidence.

Timeline data is not included in the portable case. To view the timeline, the reviewer can build the timeline in the portable case.

1. In AXIOM Examine, right-click an artifact group or items that you want to include in the portable case.
2. Click **Create export / report**.
3. Under **Export / report format**, select **Portable case**.
4. Follow the instructions to customize and create your portable case.

Sharing portable cases

When you create a portable case in AXIOM Examine, the portable case export includes several files and folders. Because stakeholders do not need to have Magnet AXIOM installed to open the portable case, the export includes an executable file for AXIOM Examine as well as other dependencies.

When you share a portable case with your stakeholders, make sure you provide them with the entire export folder in a read/write format.

Reviewing portable cases

Use a portable case to collaborate on a case with other examiners, investigators, and stakeholders.

When you share a portable case with other stakeholders, they can explore the evidence, and add their own comments, tags, media categorizations, and bookmarks. When they complete their reviews, you can merger their findings back into the original case.

Magnet AXIOM features available in portable case

FEATURE	AVAILABILITY IN PORTABLE CASE
Bookmarks	Yes
Column filtering	No
Comments	Yes
Connections explorer	No
Create a portable case	No
Create export / report	No
File system explorer	No
Filter bar	Yes
Hex decoder	No
Histogram view	No
Located at columns	No
Media categorization in Thumbnail view	Yes
Merge case	No
Profiles	Yes
Registry explorer	No
Search - Basic	Yes
Search - Advanced	No
Text and hex view	No
Timeline explorer	Yes (artifacts only)

FEATURE	AVAILABILITY IN PORTABLE CASE
CSV, tab-separated, and XML exports	No

Open a portable case

1. Browse to the portable case folder provided to you by the examiner.
2. In the **Export** folder, double-click the **OpenCase.bat** file.

When the portable case opens in AXIOM Examine, you can review the artifacts, add tags and comments, search and filter evidence, manage profiles, and export information.

> Note: Often, the evidence that you examine includes executable files or scripts (including those embedded in other artifacts such as PDF files or documents). Please note that Magnet AXIOM never runs executable files or scripts contained in your evidence (whether examined from AXIOM Examine or a portable case)—including if you try to open an executable file with an external application.

When you've completed reviewing the evidence, you can send the send the Portable Case folder back to the owner of the original case.

Merge a portable case

In AXIOM Examine, you can merge a portable case into your case. Merging a portable case allows you to import tags and comments (including those applied in the Timeline explorer), media categorizations, and profiles that other stakeholders have added to the portable case, and combine them with your own notes in the case.

> Note: You can't merge two portable cases together. The portable case must be merged with the master case it was created from.

1. In AXIOM Examine, click **File** > **Merge portable case**.
2. In the **Merge portable case** dialog, click **Browse**.
3. Select the portable case and click **Open**.
4. Click **Next**.
5. Select the information you want to merge into the case from the portable case.
6. In the **Merge portable case** wizard, follow the rest of the steps to choose what to include from the portable case and click **Merge**.

KEYBOARD SHORTCUTS IN AXIOM EXAMINE

Keyboard shortcuts allow you to complete actions by using a key or a combination of keys instead of your mouse.

AXIOM Examine supports keyboard shortcuts on standard QWERTY keyboards.

CTRL + A	Select all
CTRL + C	Copy
CTRL + V	Paste
CTRL + X	Cut
CTRL + B	Manage tags in the Evidence window
CTRL + D	Apply the *Bookmark* tag
CTRL + O	Open a case you have saved on your computer
CTRL + R	Go to the next page in the timeline graph
CTRL + L	Go to the previous page in the timeline graph
CTRL + G	Go to a date range in the timeline
CTRL + PLUS SIGN (+)	Zoom in to the timeline
CTRL + MINUS SIGN (–)	Zoom out in the timeline
CTRL + 1	Apply the *Evidence* tag
CTRL + 3	Apply the *Of interest* tag
F1	Open the online Magnet AXIOM User Guide
SPACEBAR	Click a button, select a check box, select an option or apply the *Bookmark* tag (depending on active user interface control)
ENTER	Equivalent to clicking **Okay** when an option is selected in a menu
ESC	Exit or close a window or filter

PLUS SIGN (+)	Set all visible uncategorized pictures in Thumbnail view to a media category you choose.
0 - 9	Apply a media category to the selected the picture or pictures in Thumbnail view
ALT + F4	Quit application
ALT + ENTER	Start a new paragraph line in the **Comments** field
ALT + Number	Switch between explorers. View the number that corresponds to each explorer in the explorer drop-down list.
ALT + SHIFT + Number	Switch between views (for example, Conversation view, Column view, and so on). View the number that corresponds to each view in the view drop-down list.
ALT + Left arrow	Expand or collapse **Navigation**
ALT + Down arrow	Expand or collapse **Tags, profiles & media categories**
ALT + Right arrow	Expand or collapse **Details**

CUSTOMIZING MAGNET AXIOM

You can customize settings in Magnet AXIOM like whether you want to provide diagnostic information to Magnet Forensics, receive software updates automatically, prevent your computer from entering sleep mode during a search, and more. You can also set up how you want to run your searches, including whether to compress images, create hash values, and more.

Customizing imaging settings

Create segments for Android and drive images

You can specify the size of the image segments that you want AXIOM Process to create when it acquires evidence from Android and drive images. Each option represents a different size that reflects its storage capabilities. By default, image segmentation is turned off.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Imaging** > **Image segmentation**, select a format from the drop-down list.
3. Click **Okay**.

Create a hash value for evidence sources

AXIOM Process can create hash values for each evidence source that it acquires. By default, image hashing is turned off.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Imaging** > **Image hashing**, select the **Calculate a hash value for each evidence source that's being acquired** option.
3. Click **Okay**.

Verify hash values for acquired images

AXIOM Process can create a hash value for acquired E01 images and compare it to the hash value of the source E01 image. This process verifies that the image has not been altered. Hash verification information gets written to the Case Information.txt and .xml files. By default, image hash verification is turned off.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Imaging** > **Image hashing**, select the **Verify the hash value of each acquired image file (E01 image files only)** option.

Compress images

You can compress the E01 images that AXIOM Process acquires. The **Fast** option provides some compression in a reasonable amount of time. The **Best** option provides the best possible compression, but can take much longer than the fast option. By default, image compression is turned off.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Imaging** > **Compression**, select a compression method.
3. Click **Okay**.

Restore mobile device state for Android devices

While AXIOM Process acquires evidence from Android devices, it installs an agent application onto the device to assist with recovering data. When the scan completes, AXIOM Process can remove the agent application from the device. By default, the agent application is left on the device.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Imaging** > **Restore mobile device state**, select the **Remove agent application** option.
3. Click **Okay**.

Customizing processing settings

Save temporary files to a custom location

By default, AXIOM Process stores all temporary files associated with a case to the Cases folder.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Processing** > **Temporary file location**, in the drop-down list, click **Custom location**.
3. Click **Browse** and select the folder where you want to save all temporary files associated with a case.
4. Click **Okay**.

Verify hash values for images

AXIOM Process can create a hash value for each image that it processes. This hash value acts like a digital fingerprint for the image, and you can use it to verify that the file has not been tampered with. Hash verification information gets written to the Case Information.txt and .xml files. By default, creating hash values for processed images is turned off.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Processing** > **Image hash verification**, select the **Verify the hash value of each image file (E01 only)** option.
3. Click **Okay**.

Deduplicating artifact results

When scanning an evidence source, AXIOM Process parses allocated space and carves data from across the entire image (whether it's allocated or unallocated, and a recognized file system or not). By carving data from the entire image, AXIOM Process can uncover files or fragments of data vital to your investigation—however, you're more likely to have duplicate data in your case. Most commonly, AXIOM Process could report the same file recovered through both parsing and carving techniques.

By default, Magnet AXIOM deduplicates artifact results in your case to help reduce the amount of data you need to examine.

As part of the deduplication process, AXIOM Process looks at the essential information fragments for each artifact and the source of the artifact (the source representing where the data is found and is presented by the Source column in AXIOM Examine), and then assigns a unique value to the artifact. When AXIOM Process encounters a duplicate of an existing unique value, only the first artifact with a unique value is kept. Other artifacts with the identical unique value are discarded as duplicates. For example, with pictures, the unique value is based on the hash of picture. If two pictures are found with the same hash and source, they would be deduplicated.

While parsed hits are always kept (they always have a different source), AXIOM Process will discard duplicates of the hit with the same unique value that were recovered through carving (carved hits will often be incomplete and contain only partial data).

If an identical artifact is found in two different locations (i.e. the source is different), AXIOM Process will not discard the artifact from one location. AXIOM Process treats each path as a unique source, so the artifact will appear in both locations. For example, if an identical picture is discovered in two different places—a downloads folder and a temp folder—the artifact wouldn't be discarded as a duplicate from one location.

For deleted files recovered from unallocated space, only the first artifact with a unique value is kept. If the same artifacts are found in unallocated space on different drives, both artifacts are kept because the sources are different.

For searches of NTFS and FAT file systems, AXIOM Process will automatically deduplicate results from unallocated space if they are covered by a range of space that's occupied by a known deleted file. Only the deleted file hit with an existing $MFT record will be shown in AXIOM Examine. If no $MFT record exists, the hit will be carved from unallocated space.

Remove duplicate artifact results

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Processing** > **Duplicates**, select the **Remove duplicates** option.
3. Click **Okay**.

Optimize search times

The easiest way to decrease scan times and increase performance is to add more CPU cores to your system. Magnet AXIOM is designed to create a separate thread for every core that's available in your system (currently, the upper limit is 32 cores). For the fastest search time, AXIOM Process uses all logical cores on your computer (to a maximum of 32 cores). If you want to use your computer for other tasks during a search, reduce the number of cores. Increasing the clock speed of your CPU is another way that you can improve performance.

In AXIOM Process, you can manually set the number of cores that you want to use:

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. Under **Processing** > **Search speed**, in the **Number of cores** drop-down list, select the number of cores you want to use.
3. Click **Okay**.

> Note: Adding additional cores does not improve performance in a linear way. The more cores that your system has, the more work it is for RAM to keep each core busy with new instructions to process. As the number of cores increases, the returns on performance diminish. Whereas increasing the number of

> cores from 4 to 8 will yield significant improvements, increasing from 8 to 16 has a less noticeable effect. After 8 cores, the easiest way to improve performance is by increasing clock speed.

Customizing hashing settings

Set the format for hash values

AXIOM Process can create hash values in MD5 and SHA1 formats.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Hashing** > **Hash formats**, in the drop-down list, select the hashing format that you want to use.

Prevent hashing of large files

When you set up a search, you can add files that contain hash values. AXIOM Process then uses these values to ignore non-relevant files or automatically categorize pictures. In either case, AXIOM Process must hash every file it encounters during a search to compare to the hash lists. Hashing very large files can take a long time, so you can set the maximum size of files to hash to help improve search times. The default value is 500 MB.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Hashing** > **File size limit for hashing**, select the **To optimize processing time, don't calculate hashes for files larger than** option.
3. Type the maximum file size (in MB) that you want to create hash values for.
4. Click **Okay**.

Set the location where you store hash values

You can change the location where imported hash sets are stored. If you change the location where imported hash values are stored, AXIOM Process must restart to apply the change.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Hashing** >**Hash value storage location**, browse to the location you want imported hash values to be stored and click **Select folder**.
3. Click **Okay**.

To apply the changed location of the hash set database, AXIOM Process must restart.

If the hash set on your computer isn't stored in the new location that you choose, AXIOM Process must move it to the new location before it restarts.

If there is no hash set on your computer, AXIOM Process creates an empty HashList.db file at the new location you choose before it restarts.

Enable PhotoDNA

If you import hash sets in AXIOM Process for the purpose of picture categorization, you can use PhotoDNA and fuzzy matching to help identify more pictures. When you enable PhotoDNA, AXIOM Process can identify pictures that have been modified to change their hash values and pictures that are similar in appearance to existing Project VIC pictures.

PhotoDNA is only available to law enforcement. To request a password, visit www.magnetforensics.com/photodnaregistration.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Hashing** > **Enable photo DNA**, provide the password that you received from Magnet Forensics.
3. Click **Okay**.

Customizing examining settings

Build connections automatically

By default, you must manually trigger building connections in your cases. You can change this setting to automatically build connections.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. Under **Post-processing**, select the **Automatically build connections on case open** check box.
3. Click **Okay**.

Build timeline automatically

By default, you must manually trigger building the timeline in your case. You can change this setting to automatically build the timeline.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. Under **Post-processing**, select the **Automatically build timeline on case open** check box.
3. Click **Okay**.

Set the default explorer to view relative date/time filter results in

When you use the relative date/time filter to view evidence around the time of a specific date, you can choose which explorer you want to view the relative time results in—your current explorer or the Timeline explorer. By default, AXIOM Examine will show the results in the Timeline explorer.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. Under **Relative date/time** filter in the **Explorer** drop-down list, click the explorer you want to set as the default to view relative date/time results in.
3. Click **Okay**.

Set the default explorer

Although you can use any explorer to browse the evidence in your case, by default, AXIOM Examine opens the Case dashboard explorer. You can change your default explorer.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the **Default explorer** drop-down list, click the explorer that you want to make your default.
3. Click **Okay**.

Change the default view

By default, AXIOM Examine opens the Column view. You can change your default view.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the **Default view** drop-down list, click the view that you want to make your default.
3. Click **Okay**.

Set the folder structure for saved files

When you save files from your case to a file / folder, you can set AXIOM Examine to export them in a flat structure with all files in a single folder or maintain the folder structure of the original evidence source.

Choose to maintain the original folder structure if your investigation requires that you preserve all time stamps and file locations.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. Under **Folder structure for saved files**, select one of the options.
3. Click **Okay**.

Customizing general settings

Set a default case type

When adding Case details, use the Case type field to specify the type of case you're processing. You can set a default Case type when creating new cases in AXIOM Process.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Preferences** > **Case type**, select a default case type.
3. Click **Okay**.

Collect log information

While it's running, AXIOM Process can collect log information that you can use to help track progress and troubleshoot potential issues. Turning on logging can slow down performance, so you should only turn it on when necessary. You can find the log file for AXIOM Process at: C:\AXIOM\Cases\<*case name*>.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Processing > Logging**, select the **Turn on logging** option.
3. Click **Okay**.

Send diagnostic information

You can choose to share information about how you use Magnet AXIOM with Magnet Forensics. This information can help us improve our products. The type of information that gets sent can include data about how long it took to perform a search and the processing options you used in the search. The information that gets sent *never* includes actual data from the evidence sources that you search.

By default, the collection of diagnostic information is turned off.

1. In Magnet AXIOM, on the **Tools** menu, click **Settings**.
2. In **Diagnostic information**, select the **Automatically gather and send diagnostic information** option.
3. Click **Okay**.

Turn off software updates

Each time AXIOM Process starts, it automatically checks for software updates. If you turn this option off, you must manually check the Customer Portal for updates.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **AXIOM Process settings** > **Software updates**, clear the **Check for updates automatically** option.
3. Click **Okay**.

Turn on Passware encryption features

Using a third-party plugin available from Passware, Inc., AXIOM Process supports the recognition and full disk decryption of drives with a known password or recovery key. When you turn this feature on, future Magnet AXIOMsoftware updates will also include updates to the Passware plugin.

1. Install the latest version of Magnet AXIOM.
2. In AXIOM Process, on the **Tools** menu, click **Settings**.
3. In **AXIOM Process settings** > **Passware encryption features**, select the **Turn on encryption and drive decryption features using the Passware plugin** option.
4. Click **Okay**.

Remove the Passware plugin

When you turn off the recognition and full disk decryption of drives feature and restart AXIOM Process, you remove all of the Passware plugin components from your computer. Future Magnet AXIOM software updates will no longer include updates to the Passware plugin.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **AXIOM Process settings** > **Passware encryption features**, clear the **Turn on encryption and drive decryption features using the Passware plugin** option.
3. Click **Okay**.

4. When prompted to remove the Passware plugin, click **Remove**.
5. When prompted, manually restart AXIOM Process.

Connect to the internet using a system proxy

If your agency requires that you use Magnet AXIOM through a proxy server, you can still use AXIOM Cloud to acquire users' accounts for the following platforms: Box.com, Dropbox, Facebook, Google, Instagram, and Microsoft. When AXIOM Process detects a proxy internet connection, it automatically connects to the server using the proxy settings on your computer or prompts you to type your credentials for the server if applicable.

> Note: Magnet AXIOM currently supports HTTP proxies and not SOCKS4/5 proxies.

To change your proxy settings:

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **AXIOM Process settings** > **Local area network (LAN) connection settings**, select one of the following settings:
   - If your proxy settings are configured on your computer, select **User system proxy settings**.
   - If you have more than one proxy server available, select **Manual proxy configuration** and provide the hostname and port number.
3. Click **Okay**.

Change the display language

Changing the display language for AXIOM Process also changes the display language for AXIOM Examine (and the other way around). When you change languages, you must restart Magnet AXIOM.

1. In Magnet AXIOM, on the **Tools** menu, click **Settings**.
2. In the **Language**drop-down list, click the language that you want to use, and then click **Okay**.
3. To restart Magnet AXIOM and apply the change, click **Now**.

UPDATING MAGNET AXIOM

To update to the latest version of Magnet AXIOM, download and run the incremental update. Incremental updates include only the changes that have been made to the software since you last updated it, which decreases the time it takes to update Magnet AXIOM.

Only recent versions of Magnet AXIOM support incremental updates. If you're running a version of Magnet AXIOM that is more than six months old, you must download the entire update from the Customer Portal.

Update Magnet AXIOM while online

1. In AXIOM Process, on the **Help** menu, click **Check for updates**.
2. In the **Update available** window, click **Update**.
3. Follow the instructions in the setup wizard.

Update Magnet AXIOM while offline

If your computer does not have an internet connection, you can download the update on another computer, copy it onto a USB drive, and then transfer it to your computer.

1. In AXIOM Process, on the **Help** menu, click **Check for updates**.
2. Copy the download link from the **Check for updates** window.
3. On a computer that is connected to the internet, open a web browser and paste the link into the address bar.
4. Download the .zip file.
5. Copy the .zip file to a storage device such as a USB key.
6. Connect the USB key to the offline computer and extract the contents of the .zip file.
7. Double-click the installer and follow the instructions in the setup wizard.

Magnet Forensics

2220 University Ave. E., Suite 300

Waterloo, ON, N2K 0A8

1 (519) 342-0195

This document was published on 7/22/2020.