



Magnet Forensics Training

Magnet AXIOM Examinations (AX200)

STUDENT MANUAL

Copyright © 2021 Magnet Forensics
Magnet AXIOM – AXIOM Examinations (AX200) – Training
V2204

No part of this document may be copied or reproduced
without the written permission of Magnet Forensics

Magnet Forensics
2220 University Ave. E., Suite 300
Waterloo, ON, N2K 0A8, Canada
519-342-0195

magnetforensics.com

© 2022 Magnet Forensics Inc. All rights reserved. Magnet Forensics®, Internet Evidence Finder®, Magnet IEF™, Magnet ACQUIRE™ AXIOM®, Magnet AXIOM®, and related trademarks, names and logos are the property of Magnet Forensics and are registered and/or used in the U.S. and countries around the world. All other marks and brands may be claimed as the property of their respective owners.



TABLE OF CONTENTS

Module 1 – Course Introduction and Magnet AXIOM Installation	1
AX200 COURSE INTRODUCTION	3
WELCOME AND PERSONAL INTRODUCTIONS	3
COURSE OUTLINE	3
SYSTEM REQUIREMENTS.....	7
ABOUTMAGNET AXIOM	9
MAGNET AXIOM PROCESS.....	10
MAGNET AXIOM EXAMINE	10
WHAT'S NEW	11
PRODUCT INSTALLATION AND CLASSROOM COMPUTER SETUP	11
RUNNING EXERCISES	12
INSTALLATION OF MAGNET AXIOM.....	12
ACTIVATION OF THE SOFTWARE LICENSE KEY.....	12
REVIEW OF THE INSTALLATION FILES AND FOLDERS.....	13
CLASSROOM COMPUTER SETUP	13
DASHNER CASE SCENARIO.....	14
 Module 2 – Evidence Processing and Case Creation.....	 17
AXIOM OVERVIEW	19
HARDWARE RECOMMENDATIONS	19
PROCESSING OVERVIEW.....	23
CASE DETAILS.....	24
EVIDENCE SOURCES.....	25
PROCESSING DETAILS	33
ARTIFACT DETAILS	39
PARSING AND CARVING.....	42
SEARCH FOR CUSTOM FILE TYPES	43
ANALYZE EVIDENCE	43
RUNNING EXERCISES	44
CREATING A NEW CASE	44
ADDING EVIDENCE TO THE CASE	45
SETTING THE PROCESS OPTIONS	46
SELECTING ARTIFACTS TO PROCESS AND SETTING ARTIFACT OPTIONS	49
ENCRYPTED DRIVES	50
AXIOM EXAMINE SETTINGS	53
CASE DASHBOARD	57
ARTIFACT EXPLORER.....	64



Module 3 – Operating System	73
OS ARTIFACTS – PERSONAL COMPUTERS (PCS).....	75
WINDOWS REGISTRY	77
FILE SYSTEM INFORMATION	79
OPERATING SYSTEM INFORMATION	80
TIMEZONE INFORMATION.....	82
USER ACCOUNTS	83
SAM FILE – V KEY	87
SOFTWARE HIVE	88
RUNNING EXERCISE	89
OPERATING SYSTEM INFORMATION	89
TIMEZONE INFORMATION	89
USER ACCOUNTS.....	90
INSTALLED PROGRAMS / INSTALLED MICROSOFT PROGRAMS.....	91
RUNNING EXERCISE	92
INSTALLED APPLICATIONS	92
Module 4 – Encryption & Credentials	95
ENCRYPTION & CREDENTIALS.....	97
BITLOCKER RECOVERY KEY	100
POST-PROCESSING.....	101
RUNNING EXERCISE	104
POST-PROCESSING AND ENCRYPTED DRIVES	104
MODULE REVIEW.....	105
REVIEW QUESTIONS.....	106
STUDENT EXERCISE.....	107
Module 5 – Refined Results	109
REFINED RESULTS	111
HELP/DOCUMENTATION	112
GOOGLE SEARCHES.....	113
RUNNING EXERCISE	114
GOOGLE SEARCHES.....	114
PARSED SEARCH QUERIES.....	115
RUNNING EXERCISE	116
PARSED SEARCH QUERIES.....	116
CLASSIFIEDS URLs	117
RUNNING EXERCISE	118
CLASSIFIEDS URLs	118
CLOUD SERVICES URLs	119
RUNNING EXERCISE	119
CLOUD SERVICES URLs.....	119



FACEBOOK URLs	120
RUNNING EXERCISE	121
FACEBOOK URLs	121
SOCIAL MEDIA URLs	122
RUNNING EXERCISE	123
SOCIAL MEDIA URLs	123
GOOGLE MAP QUERIES	123
RUNNING EXERCISE	125
GOOGLE MAPS AND WORLD MAP VIEW	125
CONNECT TO AN OFFLINE MAP SERVER.....	125
LOCALLY ACCESSED FILES AND FOLDERS.....	126
IDENTIFIERS	126
PROFILES.....	127
RUNNING EXERCISE.....	129
CREATING A PROFILE.....	129
EDITING A PROFILE.....	130
MANAGING PROFILES	130
REBUILT DESKTOPS (WINDOWS)	131
MODULE REVIEW.....	132
REVIEW QUESTIONS	133
STUDENT EXERCISE.....	134
ADVANCED SEARCHING AND FILTERING	135
CREATING AND USING PROFILES	136
 Module 6 – Web Related	139
WEB RELATED ARTIFACTS.....	141
WHICH BROWSERS ARE IN PLAY?.....	142
BROWSER ARTIFACT HIERARCHY.....	142
HISTORY – GOOGLE CHROME.....	143
RUNNING EXERCISE	146
CHROME HISTORY.....	146
HISTORY – MOZILLA FIREFOX	147
RUNNING EXERCISE	149
FIREFOX HISTORY.....	149
HISTORY – MICROSOFT INTERNET EXPLORER & EDGE	150
DOWNLOADS.....	153
CHROME	153
FIREFOX.....	153
INTERNET EXPLORER AND EDGE.....	154
RUNNING EXERCISES	155
CHROME DOWNLOADS	155
BOOKMARKS.....	155
CHROME	155



FIREFOX.....	156
INTERNET EXPLORER AND EDGE.....	157
RUNNING EXERCISE	158
CHROME BOOKMARKS.....	158
FORM FILL INFORMATION AND SEARCH DATA	159
CHROME	159
FIREFOX.....	162
INTERNET EXPLORER AND EDGE.....	163
RUNNING EXERCISE	163
CHROME AUTOFILL.....	163
FIREFOX FORMHISTORY.....	163
INTERNET BROWSER CACHE.....	164
CACHE – CHROME	164
RUNNING EXERCISE	167
CHROME CACHE.....	167
CACHE – FIREFOX.....	168
CACHE – EDGE	169
SESSION RECOVERY	171
CHROME	171
FIREFOX.....	172
INTERNET EXPLORER AND EDGE.....	172
RUNNING EXERCISES	173
CHROME SESSION RECOVERY	173
COOKIES.....	174
CHROME	174
FIREFOX.....	175
INTERNET EXPLORER.....	176
EDGE	177
TYPEDURLS	178
CHROME AND FIREFOX.....	178
INTERNET EXPLORER AND EDGE.....	179
RUNNING EXERCISE	180
CHROME TYPED URLs	180
EDGE TYPED URLs	180
WEBKIT BROWSER DATA	181
MODULE REVIEW.....	182
REVIEW QUESTIONS.....	182
STUDENT EXERCISE.....	183
 Module 7 – Email	187
EMAIL ARTIFACTS	189
EMAIL CONTENT.....	190
EMAIL SOURCE LINKING	190



RUNNING EXERCISE	191
VIEWING EMAIL CONTENT.....	191
EMAIL SOURCE LINKING	191
EMAIL ATTACHMENTS.....	192
RUNNING EXERCISE	194
REVIEWING EMAIL ATTACHMENTS	194
SEARCHING EMAIL.....	194
RUNNING EXERCISE	195
SEARCHING EMAILS	195
MODULE REVIEW.....	195
REVIEW QUESTIONS	196
STUDENT EXERCISE.....	197
 Module 8 – Documents.....	199
DOCUMENTS ARTIFACTS	201
DOCUMENT CONTENT.....	202
EXPORTING DOCUMENTS TO A LOCAL DRIVE	204
RUNNING EXERCISE	205
VIEWING AND SEARCHING DOCUMENT CONTENT	205
EXPORTING DOCUMENT ARTIFACTS.....	205
DOCUMENT METADATA.....	206
RUNNING EXERCISE	207
VIEWING AND SEARCHING DOCUMENT METADATA.....	207
OPTICAL CHARACTER RECOGNITION	208
MODULE REVIEW.....	211
REVIEW QUESTIONS	212
STUDENT EXERCISE.....	213
 Module 9 – Operating System Part 2	215
USB DEVICES.....	217
RUNNING EXERCISE	218
USB DEVICES	218
LNK FILES	219
RUNNING EXERCISE	220
LNK FILES.....	220
RECENT DOCS	221
JUMP LISTS	223
RUNNING EXERCISE	226
JUMP LISTS.....	226
PREFETCH	226
RUNNING EXERCISE	228
WINDOWS PREFETCH FILES	228



WINDOWS TIMELINE	231
WINDOWS EVENT LOGS	232
WINDOWS EVENT LOG FILTERING.....	234
RUNNING EXERCISE	236
WINDOWS EVENT LOGS.....	236
MODULE REVIEW.....	237
REVIEW QUESTIONS	238
STUDENT EXERCISE.....	239
Module 10 – Media	243
MEDIA ARTIFACTS.....	246
PICTURES	248
VIDEOS.....	251
CATEGORIZING PICTURES USING MAGNET.AI.....	253
MAGNET.AI – CONTENT-BASED IMAGE RETRIEVAL (CBIR).....	256
RUNNING EXERCISE: CBIR.....	258
MANUAL CATEGORIZATION OF IMAGES USING MAGNET AXIOM	259
OFFICER WELLNESS FUNCTIONALITY.....	261
MEDIA EXPLORER	266
MEDIA FILTERS AND GROUPS	267
MEDIA FILTER GROUPS	267
HIT STACKING	269
RELATED ARTIFACTS	269
QUICK MEDIA PREVIEW	270
RUNNING EXERCISE	271
MEDIA EXPLORER	271
CONNECTIONS	271
RUNNING EXERCISE	276
CONNECTIONS	276
TIMELINE	277
RUNNING EXERCISE	278
TIMELINE.....	278
MODULE REVIEW.....	280
REVIEW QUESTIONS	280
STUDENT EXERCISE.....	282
Module 11 – Mobile Artifact Analysis	285
SMARTPHONE OPERATING SYSTEMS	287
IMAGING IN AXIOM	287
ANDROID DEBUG BRIDGE.....	289
DEVELOPER OPTIONS	290
USB DEBUGGING	290



ANDROID IMAGE TYPES.....	292
INSTRUCTOR DEMONSTRATION.....	296
ACQUIRING AN IOS DEVICE.....	296
ACQUIRING AN ANDROID DEVICE	297
LOADING MOBILE IMAGES	298
MOBILE ARTIFACTS.....	299
VIEWING ARTIFACTS.....	300
CONVERSATION VIEW	301
ANDROID SMS/MMS (CONTENT PROVIDER).....	303
ACCOUNTS INFORMATION	304
ANDROID CALL LOGS	305
ANDROID DEVICE INFORMATION.....	306
MANUALLY REVIEWING INFORMATION.....	308
COMMUNICATION ARTIFACTS	309
APPLICATION OPTIONS FOR COMMUNICATION ARTIFACTS.....	310
RUNNING EXERCISE.....	312
ENABLING MAGNET.AI	312
COMMUNICATION ARTIFACTS	313
ARTIFACTS – ROW VIEW	314
ARTIFACTS – CONVERSATION VIEW	315
ARTIFACTS – SOURCE LINKING	316
SKYPE	317
WINDOWS YOUR PHONE.....	319
YOUR PHONE SMS/MMS	320
RUNNING EXERCISE.....	324
YOUR PHONE SMS/MMS	324
REVIEW QUESTIONS	325
STUDENT EXERCISE.....	326
 Module 12 – Cloud	329
WHAT IS THE CLOUD?.....	331
ACQUIRING DATA WITH AXIOM CLOUD	333
TOKENS.....	335
FACEBOOK	336
DROPBOX.....	337
INSTRUCTOR-LED DEMONSTRATION - DROPBOX.....	337
GOOGLE	340
CLOUD ARTIFACTS	342
REVIEWING CLOUD DATA.....	343
CLOUD ACCOUNTS INFORMATION, PASSWORDS, AND TOKENS	344
DROPBOX.....	345
MICROSOFT ONEDRIVE.....	346
FACEBOOK	348



GOOGLE	351
RUNNING EXERCISE	356
REVIEWING CLOUD ARTIFACTS.....	356
MODULE REVIEW.....	356
REVIEW QUESTIONS.....	357
STUDENT EXERCISE.....	358
Module 13 – Reporting	361
EXPORTING – ARTIFACTS VIEW	363
RUNNING EXERCISE	369
REPORTING FROM THE FILE MENU	369
EXPORTING – PORTABLE CASE	369
MERGING PORTABLE CASES	371
MERGING PORTABLE CASES – TAGS	371
MANAGING PORTABLE CASES – COMMENTS.....	372
RUNNING EXERCISE	373
CREATING A PORTABLE CASE.....	373
CREATING A PORTABLE CASE FROM THE EVIDENCE PANE.....	374
MERGING A PORTABLE CASE	374
SPECIAL EXPORTS – PROJECT VIC	375
SPECIAL EXPORTS – IDENTIFIERS	376
EXPORTING – FILE SYSTEM EXPLORER.....	377
SAVING FILES – ARTIFACT AND FILE SYSTEM EXPLORERS	377
RUNNING EXERCISE	378
EXPORTING FILE DETAILS FROM THE FILE SYSTEM EXPLORER	378
SAVING FILES FROM THE ARTIFACTS EXPLORER.....	379
SAVING FILES FROM THE FILE SYSTEM EXPLORER.....	379
CASE REPORTING	379
CASE REPORTING – FINAL REPORT	380
REVIEW QUESTIONS	382
STUDENT EXERCISE.....	383
Appendix A – Cumulative Review Answers	385
MODULE 4: ENCRYPTION & CREDENTIALS	385
MODULE 5: REFINED RESULTS	386
MODULE 6: WEB RELATED.....	387
MODULE 7: EMAIL	387
MODULE 8: DOCUMENTS	388
MODULE 9: OPERATING SYSTEM PART 2.....	388
MODULE 10: MEDIA.....	389
MODULE 11: MOBILE ARTIFACT ANALYSIS	389
MODULE 12: CLOUD	390



PREFACE

Welcome to the Magnet Forensics® AXIOM Examinations (AX200) training course. Forensic examiners are navigating through an ever-changing technology landscape. The volume, velocity, and variety of Internet evidence entering the marketplace all pose unique challenges. For digital forensics professionals to meet these challenges to accomplish their mission, and uncover the truth, they must be equipped with the right combination of analytic tools and practical training.

Magnet AXIOM, from Magnet Forensics Inc., allows examiners to explore the evidence in great depth, while simplifying analysis activities by intuitively linking facts and data in a way that helps examiners draw insightful conclusions. Training from Magnet Forensics is designed and delivered by experts with decades of real-world experience in the field of digital forensics. The combination of AXIOM and AXIOM-based training from Magnet Forensics provides the perfect solution for students whose working environments demand they have the right tools and knowledge to accomplish their mission.

COURSE OVERVIEW

This four-day instructor-led course provides students with the knowledge and skill sets necessary to install, configure, and use Magnet Forensics, Inc. software tools. The forensic tools covered during this course include:

- Magnet AXIOM Process
- Magnet AXIOM Examine

AUDIENCE

This course is intended for users who are responsible for collecting and analyzing digital evidence artifacts stored on various media platforms, including PCs, mobile devices, and cloud services. Although designed for users who are new to Magnet AXIOM, experienced practitioners who have not attended formalized AXIOM training will also benefit greatly from the course materials.





MAGNET
FORENSICS®

MODULE 1:

Course Introduction and Magnet AXIOM Installation

LEARNING OBJECTIVES

In this module, students will review the course outline and introduce themselves to other participants of the course. Students will learn how to install the Magnet AXIOM platform, and its core components – AXIOM Process and AXIOM Examine. Additionally, students will learn about AXIOM system requirements and how to configure the software to best work with their machine.

GOALS

At the conclusion of this module, students will be able to demonstrate the proper installation of Magnet AXIOM and will be able to identify the core files and folders that can be shared between installations of Magnet AXIOM.



AX200 COURSE INTRODUCTION

Welcome to the Magnet AXIOM Examinations Course (AX200). This is an intermediate level course designed for students who are familiar with the principles of digital forensics and for students seeking to use AXIOM for their investigations. At the conclusion of the 4-day training event, students will have the knowledge and skills they need to acquire forensic images from computer and smartphone evidence, analyze data from cloud services, configure AXIOM Process to recover the most-relevant artifacts for their investigations, use AXIOM Examine to explore the evidence in greater depth, simplify analysis activities by intuitively linking facts and data, and prepare key artifacts for collaboration with other stakeholders. Each module of instruction employs extensive scenario-based and hands-on exercises to reinforce the learning objectives, and further enhance the student's understanding of AXIOM's functionality and its application within the forensic workflow.

WELCOME AND PERSONAL INTRODUCTIONS

- Who are you and where do you work?
- What's your primary role? Investigations? Forensics?
- What previous forensic training have you received?
- Which forensic software tools are you currently using?
- Look at the index in the beginning of this book and find one or two items that are most important to you and share this with your instructor.
- What would you like to take away from this course?

COURSE OUTLINE

MODULE 1: COURSE INTRODUCTION AND MAGNET AXIOM INSTALLATION

In this introductory module, students will be presented with the learning objectives and expected outcomes for the 4-day training event, and all related course materials. The module will conclude with a hands-on exercise during which students will install Magnet AXIOM and learn about its associated components – AXIOM Process and AXIOM Examine.

MODULE 2: EVIDENCE PROCESSING AND CASE CREATION



MAGNET AXIOM EXAMINATIONS (AX200)

© 2022 Magnet Forensics Inc. All rights reserved. May not be copied or reproduced without the written permission of Magnet Forensics Inc.

This module of instruction will focus on the many features available in AXIOM Process. The students will be shown how to successfully acquire forensic images from various evidence sources, configure case-specific and global settings in AXIOM Process for the recovery of key artifacts, and create a case for analysis in AXIOM Examine. After the creation of the case, students will be introduced to the AXIOM Examine interface. This module includes an instructor-led exercise to reinforce the learning objectives.

MODULE 3: OPERATING SYSTEM ARTIFACTS PART 1

In this module students will explore the vast array of system created artifacts parsed from Magnet AXIOM. This module will cover the file system, operating system, user accounts, installed applications, and other system related artifacts to assist the examiner in identifying user activity and the accounts associated with the activity. The student will utilize the registry and file system explorers to validate their findings.

MODULE 4: ENCRYPTION & ANTI-FORENSICS TOOLS

This module will briefly cover how to identify programs that may generate encrypted files as well as programs that are considered “anti-forensics.” Encrypted files will also be covered so that students can learn how AXIOM helps to identify these file types. Students will also cover Post-Processing in AXIOM and how to add additional data over time.

MODULE 5: REFINED RESULTS

Students will explore the Refined Results category of AXIOM and learn how data is generated and filtered within AXIOM for easier use. Artifacts such as Google Search Results and Parsed Search Queries will show students how multiple Web Related artifacts can be filtered simultaneously. Other artifacts that combine information from multiple areas of the disk such as the Rebuilt Desktop artifact will be covered.

MODULE 6: WEB RELATED

This module covers several supported browsers within Magnet AXIOM including Chrome, Firefox, and Microsoft Edge. Students will learn how the artifacts are structured and what source files generate these artifacts within the Windows operating system.

MODULE 7: EMAIL



This module teaches how AXIOM Examine displays EMAIL content and renders supported HTML from within these files. Several EMAIL programs such as Windows Mail and Microsoft Outlook will be examined.

MODULE 8: DOCUMENTS

Students will explore how AXIOM renders and parses documents from multiple categories including Microsoft Office documents, Open Office documents, CSV, TXT, and other document types. Students will learn how the data is indexed and searched for keywords in AXIOM, including document contents, metadata, and the OCR capabilities.

MODULE 9: OPERATING SYSTEM ARTIFACTS PART 2

Students will return the Operating System category to examine additional artifacts such as LNK Files, Jump Lists, USB Devices, and other artifacts that will help to show what files and devices have been accessed from the computer.

MODULE 10: MEDIA ARTIFACTS

This module will instruct students on how to deal with media artifacts including pictures and videos of varying types. Students will learn the differences between parsed and carved files, and the limitations of each. EXIF and metadata of these file types will be covered as well as several important features of AXIOM such as the Officer Wellness features, Media Explorer, Connections Explorer, and Timeline Explorer.

MODULE 11: MOBILE & CHAT ARTIFACT ANALYSIS

In this module students will explore smartphone evidence parsed by Magnet AXIOM from mobile operating systems. Additionally, this module will explore the device file systems and file structures to recover additional information, including device owner information, third party application data, core operating system data, Internet browser data, and more.

This module will explore how Magnet AXIOM handles chat artifacts from both computer and mobile platforms including features such as chat threading. Students will learn how the chats are grouped and tips and tricks for filtering through large chat extractions.

MODULE 12: CLOUD

In this module, students will learn about the cloud component of AXIOM Process and Examine. This feature allows examiners to extract valuable evidence from cloud sources such as Google, iCloud,



Dropbox, Microsoft Office 365, and others. Students will use hands-on exercises to learn how the information collected from these sources can integrate with other data recovered from live evidence sources and how it can play into their examinations.

MODULE 13: REPORTING

In this final instructional module of the course, students will explore the various exporting and reporting features available within AXIOM that can be used to present case evidence, and/or collaborate with other investigative stakeholders. Through the scenario-based, instructor-led, and student practical exercises, participants will learn how to manage the exporting of artifacts, produce and merge portable cases, and create a final investigative case report which is easily interpreted by both technical and non-technical recipients.



SYSTEM REQUIREMENTS

Figure 1.1 details the minimum and recommended hardware requirements for running AXIOM on a Microsoft Windows-based computer:

Item	Minimum requirement	Recommended requirement	Notes
Operating system	Windows Server 2019, Windows 10, Windows 8.1		Advanced Internet Security must be turned off for Windows Server 2019. Windows 7 is no longer be supported as of Magnet AXIOM 5.0.0.
Software framework	Microsoft .NET Framework 4.8.0 or later		
Display resolution	1280x720	1080p	
CPU	4 logical cores	8-16 logical cores	
GPU	Compute capability 3.5	Compute capability 5.0	<p>The GPU requirements are only applicable if you're using Magnet.AI picture categorization. This feature requires large amounts of processing power, and Magnet AXIOM has been designed to take advantage of the GPU for these processes. The GPU is not used for any other Magnet AXIOM functionality.</p> <p>Magnet.AI supports the following video cards:</p> <ul style="list-style-type: none"> • NVIDIA Tesla • NVIDIA Quadro • NVIDIA NVS • NVIDIA GeForce • NVIDIA TEGRA <p>Note: Magnet.AI does not support CUDA version 11.</p>
	NVIDIA CUDA version 9.0		
Memory	8 GB RAM	32 GB RAM	
Storage	HDD	SSD	The storage device requires enough space for storing images and cases from devices with large amounts of data (in some cases, these might be TBs in size)
Mobile devices	iOS devices: Latest version of iTunes Android devices: Mobile device drivers from each manufacturer (available through Windows Update or from the device manufacturers' websites)		If you're using Magnet AXIOM to create forensic images of mobile devices, you'll need to install this software.

Figure 1.1 Hardware system requirements



OPERATING SYSTEM: Windows Server 2019, Windows 8.1, Windows 10. Note that Windows 7 is no longer supported as of AXIOM 5.0.

SOFTWARE FRAMEWORK: Microsoft .NET 4.8 or later

STORAGE DEVICE: The storage device should have enough space to store images and cases from devices with large amounts of data (in some cases, these might be terabytes in size). You can also help prevent thread starvation by storing case data on a high-performance drive such as a Solid State Drive (SSD). SSDs have input/output operations per second (IOPs) that are much faster than Hard Disk Drives (HDDs). Faster IOPs are helpful when the system needs to read many small files.

MEMORY: As a general recommendation, you should allocate at least 2GB of RAM for every processing core in your system. Without enough memory to keep each core working constantly, your system might experience thread starvation. Thread starvation occurs when a processing core is sitting idle for an extended period because there isn't any RAM available to provide it with instructions.

CLOCK SPEED AND CORES: You can decrease scan times and increase performance by adding more CPU cores to your system and increasing the speed of those cores. Adding more cores will decrease scan time, as Magnet AXIOM is designed to create a separate thread for every core that's available on the system (currently, the upper limit is 32 cores). Due to the multi-threaded architecture of AXIOM, you'll initially see more significant improvements by adding cores instead of solely increasing clock speeds. However, after about 12 threads the speed of the cores matters more than the number due to the way Axiom allocates jobs to each thread. At this point, it would be worth maximizing core speed. Also note that the more cores that your system has, the more work it is for RAM to keep each core busy with new instructions to process.

You can manually set the number of cores that you want AXIOM Process to use via the **Search Speed** option accessed from the **Tools → Settings** menu. Select the number of cores AXIOM Process can use from the **Search Speed** drop-down list.

VIRTUALIZATION: The only part of Magnet AXIOM that cannot be used in a virtual machine is image acquisition. All other parts of Magnet AXIOM will function as normal.

ANTI-VIRUS: Some anti-virus software can interfere with the installation and operation of Magnet AXIOM. If errors are encountered, disable the anti-virus software. This is especially true when adding the Project VIC/CAID or similar large data sets. During the import process, changes are being made to the local SQLite database files associated with Magnet AXIOM and its installation. The anti-virus software can make this process very slow, because they are monitoring the safety of the local system.

ABOUT MAGNET AXIOM

AXIOM allows the examiner to explore evidence in greater depth and integrate digital data from multiple devices in one case. With AXIOM, you can acquire, process, analyze and report using just one tool. Intuitive linking will help you validate location data and find related artifact data quickly.

With AXIOM, your examinations will be faster and more thorough. You will uncover facts quickly, validate your findings with ease, and share the meaning of your results clearly. With advanced integration features, AXIOM allows you to examine data recovered through other tools as well.



MAGNET AXIOM PROCESS

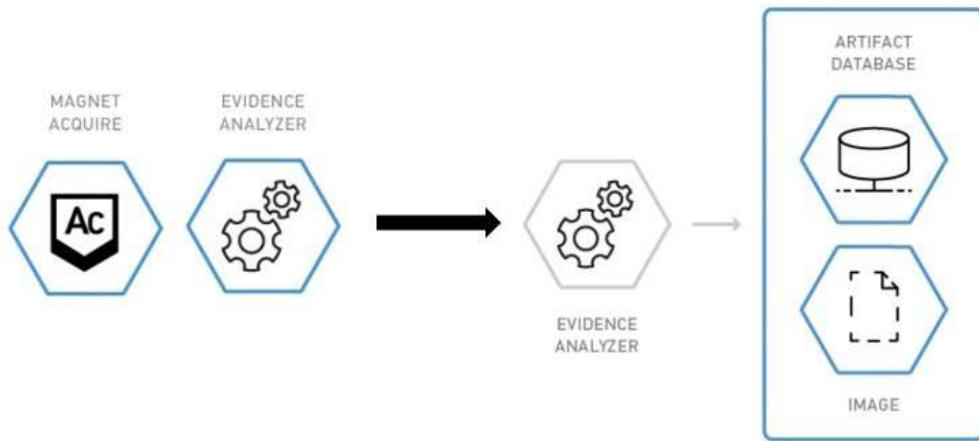


Figure 1.2 Magnet AXIOM core components – AXIOM Process

With AXIOM Process, users can search images, drives, files and folders, partitions, volume shadow copies, random-access memory (RAM), Android and iOS devices, Windows phones, Kindle Fire, media devices via the media transfer protocol (MTP), cloud services, search warrant returns, and other sources to find evidence that is relevant to the investigation. Users can customize and search for case-specific, or global needs by selecting specific artifacts or groups of artifacts. Keywords, regular expressions, and hash values can also be used to further refine the scope of the evidence included in the resulting case. AXIOM Process has the capability to create forensic images of iOS and Android devices, plus a variety of different types of drives including HDD, SSD, USB and SD flash, and more. Users can customize the type of image they want to acquire, depending on the evidence they are looking for, and time restraints. AXIOM Process is a seamless platform which allows an examiner to acquire and automatically process an image.

MAGNET AXIOM EXAMINE

After the collection and analysis of the evidence with AXIOM Process is complete, AXIOM Examine presents the evidence in a consumable and user-friendly manner. In addition to the Artifact explorer, users can drill down to the source of an artifact using the File system and Registry explorers. To view artifacts in a timeline, users can use the Timeline explorer. The Connections explorer will allow the user to see how one artifact is related to other artifacts, even throughout other sources of evidence. An enhanced search and filters bar also allows users to quickly narrow their focus to relevant artifacts, which can be tagged. Once the exam is complete, the next step is to share the findings. Using the enhanced export functionality of AXIOM Examine, users can create intuitive exports, portable cases, and final case reports for collaboration with other stakeholders.

WHAT'S NEW

When a new version of Magnet AXIOM is installed, a User Guide accompanies the installation. The User Guide includes a section explaining the newly added features and/or artifacts.

The User Guide can be accessed by either selecting the F1 key on the keyboard or selecting Help → Documentation → User Guide from the menu bar.

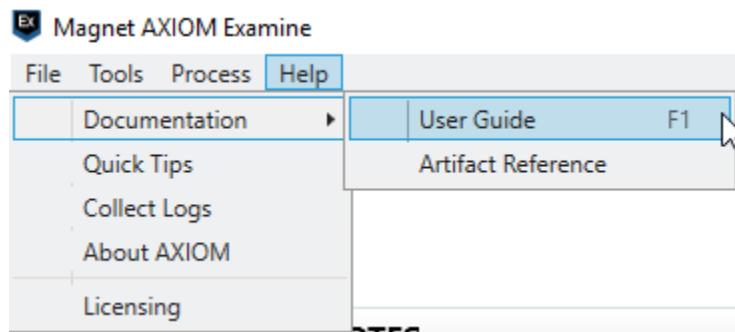


Figure 1.3 Accessing the User Guide

The User Guide itself contains many useful information items, however it is recommended every time AXIOM is updated, the examiner use this file to review the newly added features.

WHAT'S NEW	
VERSION	DESCRIPTION
	<ul style="list-style-type: none"> Added Viewing the timeline with information about the new Timeline explorer. Updated several Acquiring computer evidence topics with information about loading Mac evidence and support for APFS. Updated Decrypting evidence with information about decrypting macOS computers with an APFS file system. Updated Categorizing pictures and videos with information about how to load hash lists and configure hash sets in AXIOM Process, and how to manually categorizing pictures and videos in AXIOM Examine. Updated Keyboard shortcuts in AXIOM Examine with new shortcuts for categorizing media.

Figure 1.4 What's New

PRODUCT INSTALLATION AND CLASSROOM COMPUTER SETUP

The following instructor-led exercises are designed to familiarize students with the installation of Magnet AXIOM and its associated files, folders, and applications. The following steps will also prepare the classroom computers for all subsequent hands-on exercises.



NOTE: Depending on the classroom environment, the following installation steps may be performed during the introductory module using a USB device, or a software application installer (*.exe) for Magnet AXIOM from a location specified by the instructor.

RUNNING EXERCISES

INSTALLATION OF MAGNET AXIOM

- Open File Explorer and navigate to the location of the Magnet AXIOM installer. This will either be on the classroom computer or a USB device provided by your instructor.
- Double-click the Magnet AXIOM installation file.
- Follow the installation wizard steps, accepting the license agreement and default installation settings.
- Once the installation has completed, uncheck the option to Launch AXIOM Process, and click Finish.
- After the installation there will be two new desktop icons – AXIOM Process and AXIOM Examine.
- The temporary license key is in the same folder as the AXIOM installation file.

ACTIVATION OF THE SOFTWARE LICENSE KEY

- After successfully installing Magnet AXIOM, launch AXIOM Process from the desktop icon.
- A licensing menu will appear upon program launch, with a drop-down menu for different licensing options.
- From the drop-down menu, select Trial license.
- Browse to the location specified by your instructor and locate the AXIOM training license key.
- The license key is a plain text file. Open the file, copy the entire content to the clipboard and return to the Licensing window.
- Paste the key from the clipboard into the LICENSE KEY field and click **OKAY** to apply the temporary license.
- Confirmation of the license details should be listed at the top of the Licensing window under LICENSE INFORMATION.
- AXIOM Process will need to restart to apply the licensing changes.

REVIEW OF THE INSTALLATION FILES AND FOLDERS

- Open File Explorer and navigate to the folder
C:\Program Files\Magnet Forensics\Magnet AXIOM\
- Note the folders for AXIOM Process and AXIOM Examine.

CLASSROOM COMPUTER SETUP

- If they have not already been copied by the instructor, copy the following classroom folders to the desktop:
 - a. Cases
 - b. Evidence
- Create the following folders on the desktop:
- AX200 Reports
- AX200 Exports



MAGNET AXIOM EXAMINATIONS (AX200)

© 2022 Magnet Forensics Inc. All rights reserved. May not be copied or reproduced without the written permission of Magnet Forensics Inc.

DASHNER CASE SCENARIO

The instructor-led and student exercises throughout this course are based on evidence relating to the following case scenario:

The scenario is based on an investigation related to the possession, viewing and/or distribution of illicit material involving minors. The primary suspect is Isaiah Dashner who is on supervised release for prior offenses related to drug manufacturing and identify theft. As a condition of his release, Dashner is required to submit to searches of his residence and any electronic devices in his possession. Recently, the local police department responded to Dashner's residence for a noise complaint and found that he and another individual, Jeff Armstrong, were in possession of methamphetamine; both were arrested. While at the residence, officers noticed a running laptop computer with a contraband image displayed as the device wallpaper. The computer, along with two USB flash drives, which were on the desk next to the laptop, were seized as possible evidence. Dashner was also found to have an Android phone in his pocket, but he was unwilling to provide the passcode for the device to the officers on scene.

After learning of the arrest, Dashner's parole officer contacted the local police department and provided copies of his search waiver, which included a passcode for the Android phone. Additionally, the officers were able to download some of Dashner's cloud account information.

You have possession of the following items that were all acquired at Dashner's residence at the time of arrest, and full lawful authority to conduct a search:

- **Dashner's PC with one (1) internal hard drive**
- **Dashner's Google Pixel 3a phone**
- **Two USB devices found near Dashner's computer at the time of arrest. One was a SanDisk Cruzer, the other is a Lexar branded USB flash drive that is BitLocker encrypted.**
- **Dashner's cloud accounts**

The exercises throughout this course will focus on locating evidence relating to the possession, distribution, and viewing of illicit material involving minors, as well as narcotics related activity. This activity could include chat conversations, internet searches and browsing activity, and the possession of documents. By the end of the course, examiners should be able to provide information relating to Dashner's alleged activity and identify any potential leads for further investigation. Throughout the case scenario, images of puppies are to be regarded as contraband material which meet the statutory requirements in your jurisdiction.

Notes

Notes





MAGNET
FORENSICS®

MODULE 2:

Evidence Processing and Case Creation

LEARNING OBJECTIVES

In this lesson, students will take part in lecture, instructor-led exercises, and student practical exercises to learn the function of the AXIOM Process component of Magnet AXIOM, the steps of imaging devices using AXIOM Process, the steps of adding pre-imaged data to AXIOM Process, how to build a case using AXIOM Process, and how to configure AXIOM Examine. This lesson will also provide an overview of the AXIOM Examine interface and discuss the Case Dashboard content within AXIOM Examine.

GOALS

At the end of this lesson, students will be able to identify the steps required to set up the processing functionality of AXIOM Process, add evidence images to AXIOM Process, set up the imaging of devices if necessary, and be able to build a case within AXIOM Process.

AXIOM OVERVIEW

Magnet AXIOM is designed to help examiners by combining several steps of the case flow process into a single platform – from imaging, to searching and processing data, to analyzing the data, and finally to reporting the findings.

Instead of using separate tools to image the data and conduct the processing, AXIOM Process combines the two steps. Using AXIOM Process, computer, mobile, and cloud evidence can be imaged and processed in a single step and then reviewed within a single case file.

Evidence can either be imaged directly or added from other sources, then directly processed with specific items that the user requests. AXIOM Examine then allows the user to view the processed data in multiple views and add tags, generate reports, and create portable cases based on the processed data. In addition to displaying the parsed artifacts, AXIOM Examine also includes a case dashboard, artifacts explorer, registry explorer, file system explorer, timeline explorer, connections explorer, and media explorer which allow examiners to find and review even more data than ever before.

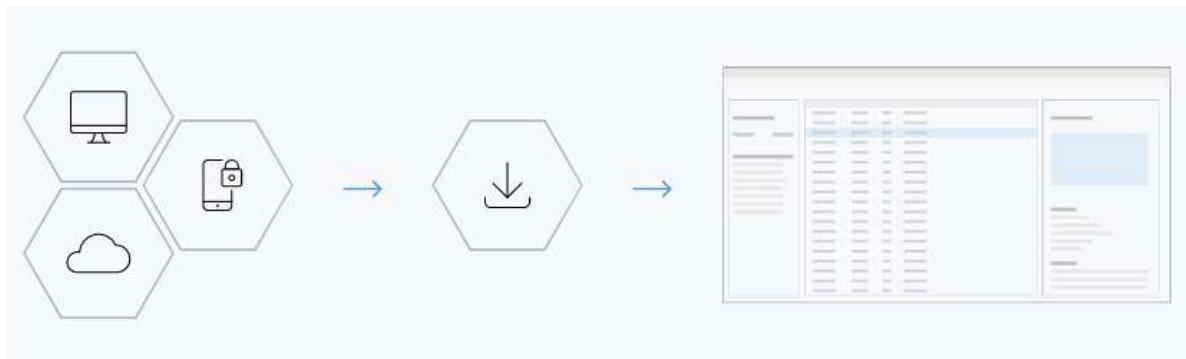


Figure 2.1 AXIOM Process extracts data from devices and displays it in AXIOM Examine

HARDWARE RECOMMENDATIONS

There are three recommendations we can suggest based on your forensic workstation budget. Hardware is constantly evolving and there is no perfect workstation. What you purchase today as the best hardware may change tomorrow.

We won't go into long term storage recommendations because there are too many options. You should choose your storage based on your needs, considering the number of cases you work per year and your amount of data being stored.

Separating your case files from your evidence files on physical media will allow you to obtain a significant improvement in the responsiveness and speed of processing and examining your cases. If you further



separate your TEMPORARY FILE LOCATION it will also assist in the processing speed of your cases by making sure you are not reaching the limit of your input/output operations per second (IOPS) on the physical disks you are using. You can change this feature in AXIOM Process by accessing the Tools → Settings option for the toolbar. By default, AXIOM Process uses your case file location as your temporary file location, however you can change this by selecting Custom location and browsing to another physical disk such as your operating system disk and choosing a temp path.

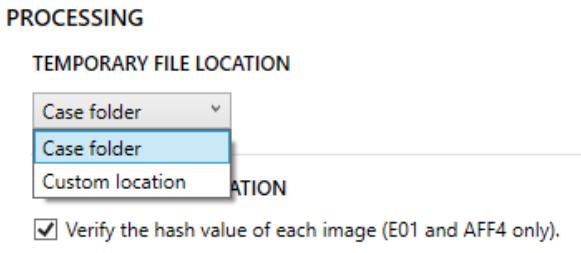


Figure 2.2 Setting temporary processing locations

AXIOM case files are stored with the **.MFDB** extension and are SQL databases. The number of reads and writes to that database, as well as reads from the evidence files will cause you to reach the physical limit of your physical disks on most high-speed modern computers.

If budget is no concern and you have the power to purchase your equipment, it is recommended to use NVME drives. A Samsung 960 NVME drive maintains 330,000 IOPS per physical disk (<https://www.storagereview.com/review/samsung-960-pro-m-2-nvme-ssd-review>) and when raided together in a RAID 0 configuration, you can expect about 900,000 IOPS. This is because there is some overhead when you RAID devices together, so you won't get exactly 990,000 IOPS.

A Samsung 850 EVO pro SATA drive maintains 98,000 IOPS per physical disk (<https://www.storagereview.com/review/samsung-ssd-850-pro-review>) and when raided together in a RAID 0 configuration can result in about 250,000 IOPS.

A 7200 RPM spinning drive maintains 35,000 IOPS and when raided together in a RAID 0 configuration can result in about 85,000 IOPS.

If budget is not a concern for you, it is recommended you consider Option 1 to get the most out of your forensic workstation.

Option 1:

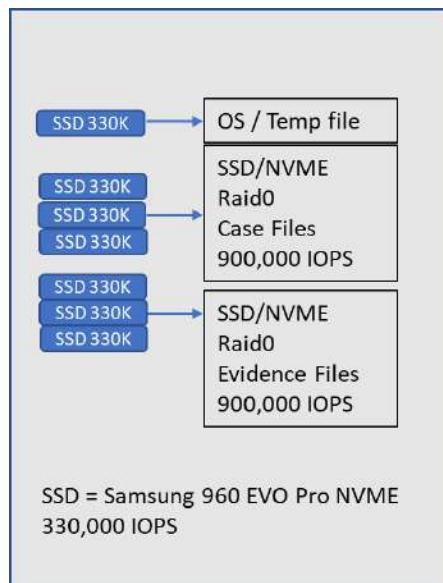


Figure 2.3 High-end configuration

If budget is somewhat of a concern for you, it is recommended you consider Option 2 to get the most out of your budget and forensic workstation.

Option 2:

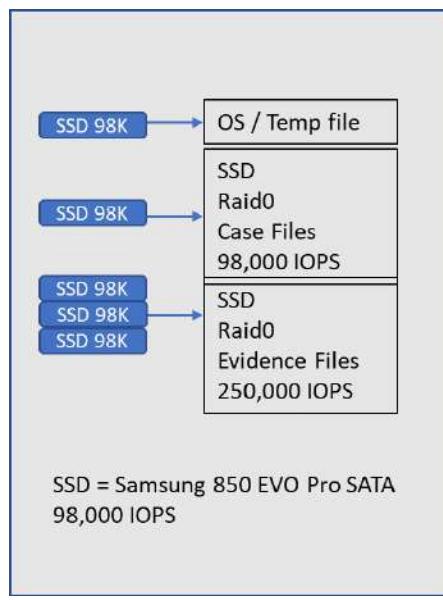


Figure 2.4 Mid-level configuration



Option 3:

If your budget is a large concern, or you don't have a budget to build/outfit a forensic machine, a baseline recommendation for lower-end systems is recommended below for efficiency.

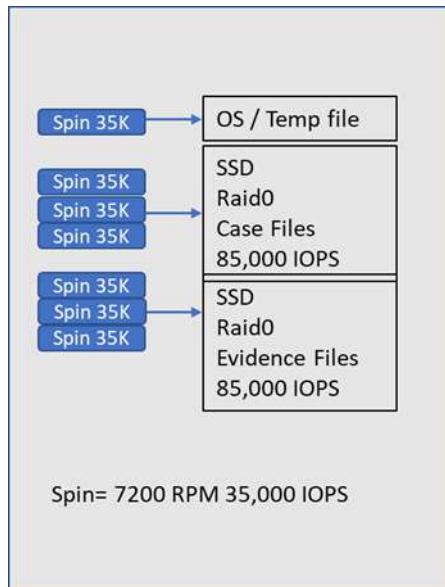


Figure 2.5 Low-end configuration

When processing in Magnet AXIOM Process, the CPU of the machine is a key factor in determining the speed of the processing. There is a balance between adding cores and the speed of those cores. AXIOM Process can create up to 32 threads for processing, one for each core of the machine. AXIOM will also only take advantage of one physical processing unit at a time. The more threads that Magnet AXIOM Process uses, the more the RAM of the system needs to keep up with assigning tasks to each thread. Users will notice a drastic performance increase up to 8 or 12 cores, and after 12 cores, the speed of the cores takes over in performance improvements. While adding additional cores beyond 12 will still increase performance, it will be a less noticeable amount than from 4 to 8 cores. When picking a CPU, focus on processors that have a higher clock speed versus pure number of cores. For example, an Intel i9 processor with 16 threads may perform better than a processor with more available threads but a slower speed available to each thread. For more information about increasing performance in Magnet AXIOM Process, please consult this knowledge base article on the Customer Support Portal: (<https://support.magnetforensics.com/s/article/Optimize-the-performance-of-Magnet-AXIOM>).

PROCESSING OVERVIEW

AXIOM Process allows the user to create a new case or add evidence to an existing case, as shown in Figure 2.6.

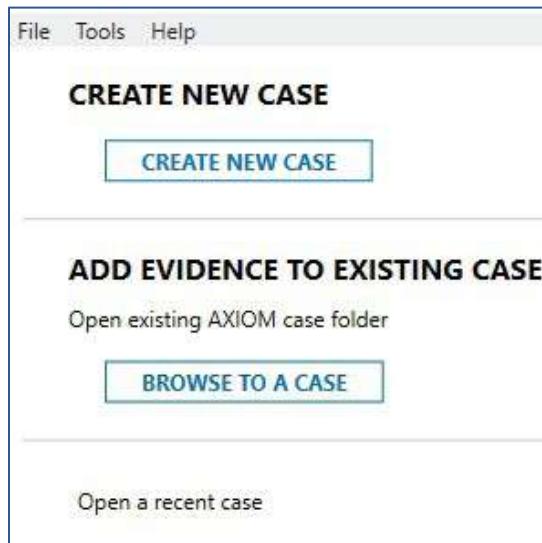


Figure 2.6 Create new or add evidence to existing case

Once a case has either been created or an existing case opened, AXIOM Process guides the user through each of the necessary steps until finally reaching the ANALYZE EVIDENCE stage. Users can also jump between each of the processing options by clicking the relevant option in the left-hand pane. The artifact details step will remain greyed out until at least one evidence source has been added and the method of processing has been selected. If the mandatory information for any step has not been provided, an orange exclamation point will appear in the window alerting the user that information is missing.

CASE DETAILS

CASE INFORMATION

Case number

Case type

LOCATION FOR CASE FILES

Folder name

File path

Available space: 278.10 GB

LOCATION FOR ACQUIRED EVIDENCE

Folder name

File path

Available space: 278.10 GB

SCAN INFORMATION

SCAN 1

Scanned by

Description

REPORT OPTIONS

Cover logo
Image resized to 150x150 pixels

Figure 2.7 Case details

In the CASE INFORMATION section of the CASE DETAILS, the user can specify where the case files will be saved as they are generated. Both the case files and the generated image files can be saved within the same folder structure, or they can be saved in separate locations. The File path location for either of these can be changed by selecting the **BROWSE** option beside the path listing.

By default, both the case files and acquired evidence files will be saved into the same folder. This folder will have the default name **AXIOM – DATE TIME** detailing when the case setup began for the case. The DATE TIME is in the format: month day year followed by a 24-hour time HHMMSS. The folder name can be changed to match the user's own standards and guidelines if desired.

Users can also set case information, including examiner name and any detailed notes, within the Scanned by and Description fields of the SCAN INFORMATION section. Because multiple scans can be performed to add additional evidence to a case, each scan will allow new examiner and description information to be included. Anything populated into these fields will appear in both the logs and the final case report.

In addition, a date created timestamp will be added to this information noting when the scan was conducted.

In the REPORT OPTIONS section, the user can specify a custom cover logo in place of the Magnet Forensics icon. To change the image, select the **BROWSE** option and navigate to a graphic file. Any selected file will be automatically resized to 150x150 pixels.

CASE INFORMATION	
Case number	<input type="text"/>
Case type	<input type="button" value="Select case type..."/> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> Border security assessments Child exploitation Civil case or investigation Counter terrorism Data exfiltration / IP theft Fraud HR / internal investigation Human trafficking Intrusion / incident response Major crimes (murder, drug trafficking, weapons trafficking) Military investigations Organized crime Policy violation / asset misuse Wrongful termination Other </div>
LOCATION FOR CASE FILE	Folder name <input type="button" value="BROWSE"/> File path <input type="button" value="BROWSE"/>
LOCATION FOR ACQUISITION	Folder name <input type="button" value="BROWSE"/> File path <input type="button" value="BROWSE"/>
SCAN INFORMATION	<input type="button" value="BROWSE"/>

Figure 2.8 Case type

Axiom Process allows the user to select the case type. This is an optional selection and will appear in the final case report. Users can also set a default case type within the AXIOM Settings menu that will auto-populate by default. Selecting a case type does not change any function of the software; it is only a reference for the examiner.

EVIDENCE SOURCES

In EVIDENCE SOURCES, users must first SELECT SOURCE PLATFORM for the evidence they are adding; the choices are COMPUTER, MOBILE, CLOUD, or VEHICLE-based evidence.



Figure 2.9 a depicts the flow of adding evidence. When choosing computer, the next option presented to the user is to select Windows, Mac, Linux, or Chromebook, and then to choose LOAD OR ACQUIRE evidence. When mobile based evidence is chosen (Figure 2.10), the next option presented to the user is to select the specific mobile platform (including SIM card), followed by the choice of either load or acquire the evidence (mobile acquisition and processing will be covered in more detail in Module 11). When cloud-based evidence is chosen, the user is again presented with the option to LOAD OR ACQUIRE evidence.

For computer-based evidence, the LOAD EVIDENCE option allows processing of locally connected drives (DRIVE), forensic image files (IMAGE), individual files and folders from a local drive (FILES & FOLDERS), Volume Shadow Copies from an image or a local drive (VOLUME SHADOW COPY) and RAM images (MEMORY).

Figure 2.9 Computer evidence source options

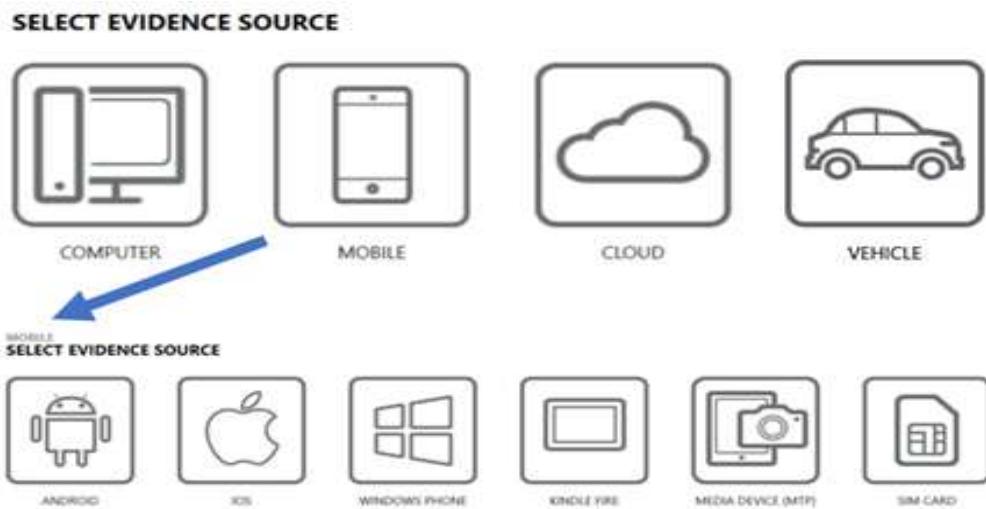
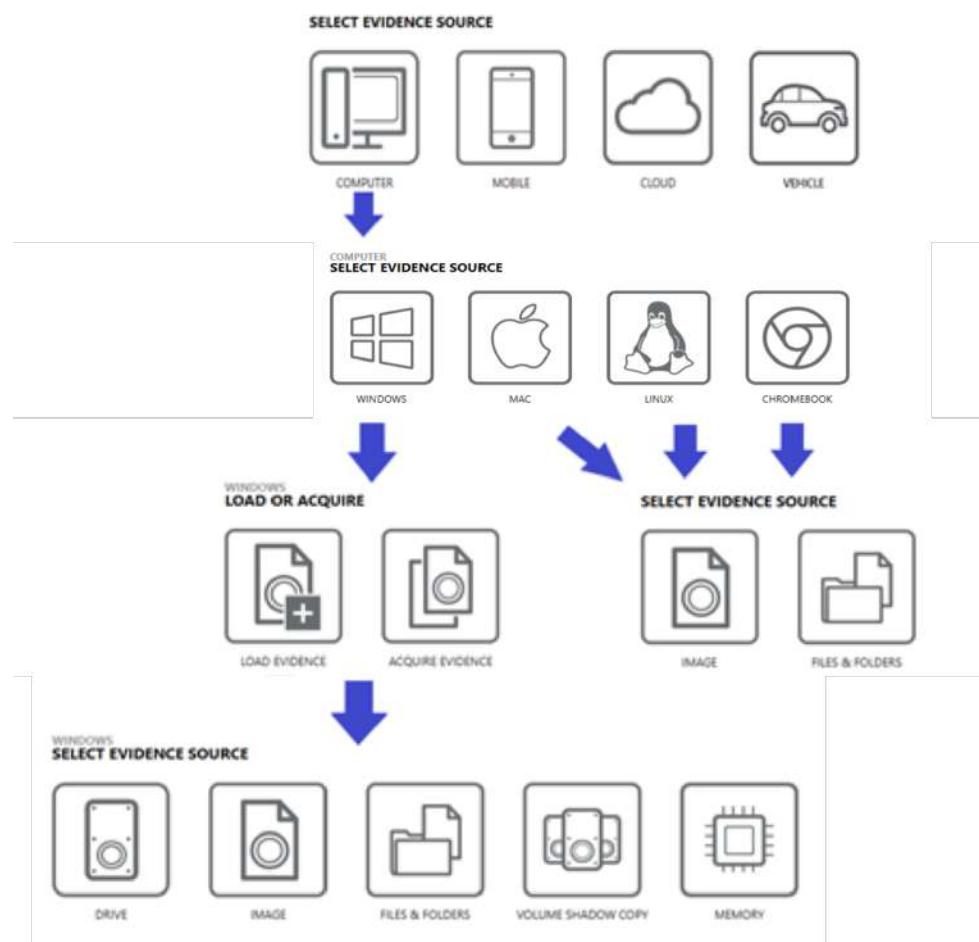


Figure 2.10 Mobile evidence source options

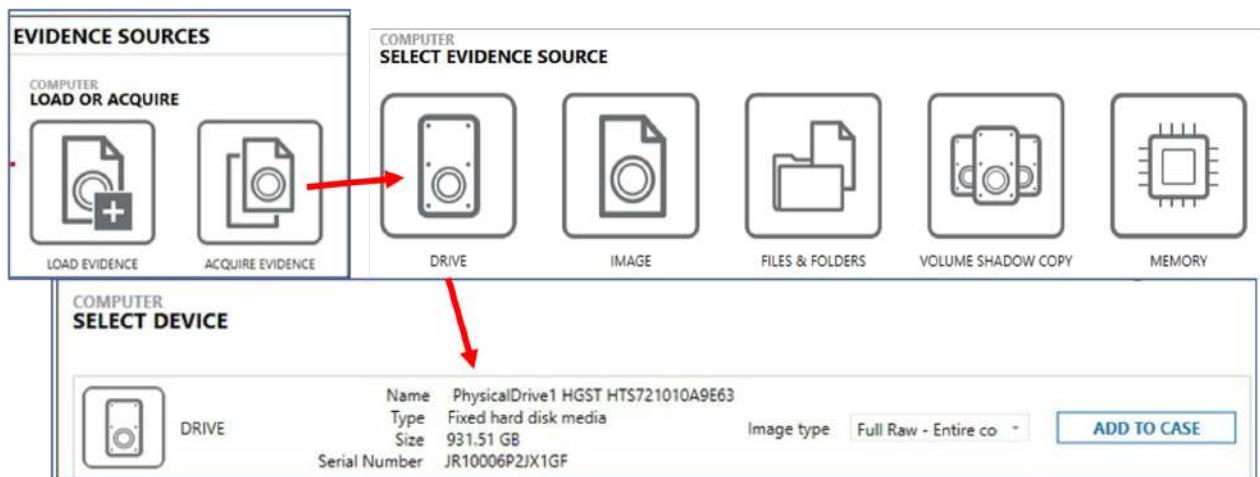


Figure 2.11 Computer evidence source options

As seen in Figure 2, if the option to ACQUIRE EVIDENCE is selected, AXIOM Process will present drive identification information such as the Name, Type, Size, and Serial Number of the attached drives that can be acquired. Both removable and fixed drives are listed with an icon resembling a hard drive. USB devices, connected hard drives, and media cards are also displayed.

The type and format of the acquired image can then be selected. The type of image and the formats available are:

- Full – Entire contents of the drive in E01 format
- Full – Entire contents of the drive in RAW format
- Full – All files and folders
- Quick – targeted acquisition

During creation of either an E01 or RAW format image with AXIOM Process, log files are created in the same folder designated for the newly created image file(s). These log files contain calculated hash values of the source evidence and acquired image files.

On smartphone devices, both iOS and Android devices will display for acquisition. Android devices will be marked with an icon representing the Android logo (Andy the Android), and iOS devices will be marked with an icon containing the Apple logo. Both device types will display the make, model, operating system version, and if they have privileged access.

Android devices can be acquired with both the Full and Quick options. Each of these options require the Android device to have USB Debugging options enabled, and the security prompt allowed. The Quick option will perform a standard Android logical acquisition which includes an APK injection type as well

as the ADB backup command. Android devices will also acquire data from the “getprops” or “dumpsyst” command in order to obtain live information from the device as well. The Full option preforms a full memory image but requires root access. AXIOM Process will attempt to perform a “shell” or temporary root of the device if it is running Android version 4.4.2 (KitKat) or lower.

Android Ice Cream Sandwich	Ice Cream Sandwich	4.0 – 4.0.2	October 18, 2011
		4.0.3 – 4.0.4	December 16, 2011
Android Jelly Bean	Jelly Bean	4.1 – 4.1.2	July 9, 2012
		4.2 – 4.2.2	November 13, 2012
		4.3 – 4.3.1	July 24, 2013
Android KitKat	Key Lime Pie	4.4 – 4.4.4	October 31, 2013
		4.4W – 4.4W.2	June 25, 2014
Android Lollipop	Lemon Meringue Pie	5.0 – 5.0.2	November 4, 2014
		5.1 – 5.1.1	March 2, 2015
Android Marshmallow	Macadamia Nut Cookie	6.0 – 6.0.1	October 2, 2015
Android Nougat	New York Cheesecake	7.0	August 22, 2016
		7.1 – 7.1.2	October 4, 2016
Android Oreo	Oatmeal Cookie	8.0	August 21, 2017
		8.1	December 5, 2017
Android Pie	Pistachio Ice Cream	9	August 6, 2018
Android 10	Quince Tart	10	September 3, 2019
Android 11	Red Velvet Cake	11	September 8, 2020
Android 12	Snow Cone	12	October 4, 2021
Android 12L	Snow Cone v2		March 7, 2022
Android 13	Tiramisu	13	Q3 2022

Figure 2.10 Android versions, release dates, and friendly names

iOS devices can also be acquired using both the Full and Quick options. Both require the iOS device to be connected to the PC and have the Trust this Computer dialog accepted on the device. Once the pairing between the two has been established, the iOS device will display for acquisition within AXIOM Process. The Quick option is the default for iOS devices and will attempt an iTunes backup along with obtaining information from the unprotected part of the filesystem (Camera Roll/Media/etc.).

The Full option can only be selected if the iOS device has already been jailbroken. This will allow the user to acquire a full file system extraction from the iOS device.

If, after selecting computer-based evidence, the option LOAD EVIDENCE is selected, the next screen presents the five options shown in Figure 2.9:

- DRIVE
- IMAGE
- FILES & FOLDERS
- VOLUME SHADOW COPY



- MEMORY

The DRIVE option allows the user to process any locally connected media such as hard drives and USB devices without first imaging them. The entire physical device can be selected, or just individual partitions on the device. Once the device or partition has been selected, clicking **NEXT** then displays the SELECT SEARCH TYPE options.

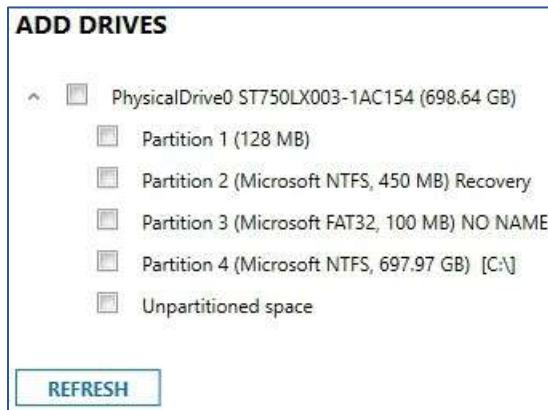


Figure 2.13 Physical drives

The IMAGE option allows the user to load a previously acquired forensic image. This option opens a Windows Browser dialog box for the user to locate and select the image file. Selecting the drop-down menu displays the image formats currently supported by AXIOM.

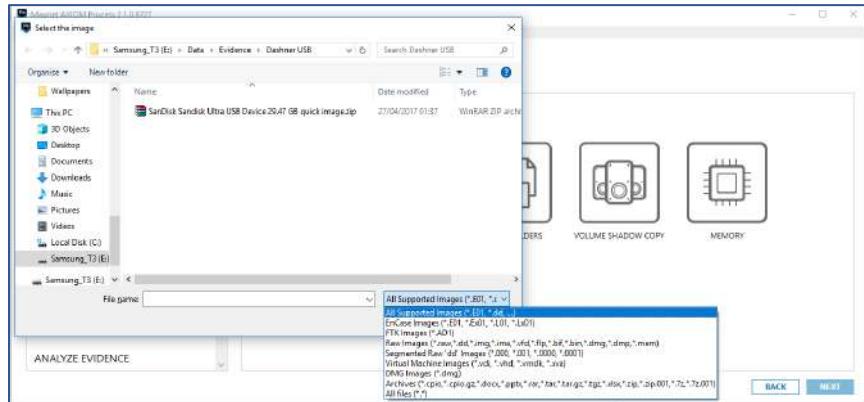


Figure 2.14 Supported image formats

NOTE: Other unlisted image types may also be supported. Select the All Files (*.*) option to locate and load the image file.

The FILES & FOLDERS option allows the user to scan individual files or folders stored on any connected disk or device. Selecting files and folders from the main ADD FILES AND FOLDERS window uses the AXIOM application programming interface (API) which accesses files directly from the disk/device. It reads the file system information directly from the disk and bypasses any Windows security, therefore protected system files, such as the Windows registry hives and the \$MFT etc. can be processed by AXIOM Process.

Alternatively, the FOLDER BROWSER or FILE BROWSER buttons at the bottom of the dialog window access the files and folders via the Windows API, therefore Windows Security will prevent access to system or protected files. However, anything that can be seen from File Explorer is visible to AXIOM Process via these options. Selecting one of these options and entering a UNC path in the address bar will allow access to the content of the remote location, provided the user has access credentials to view the content.

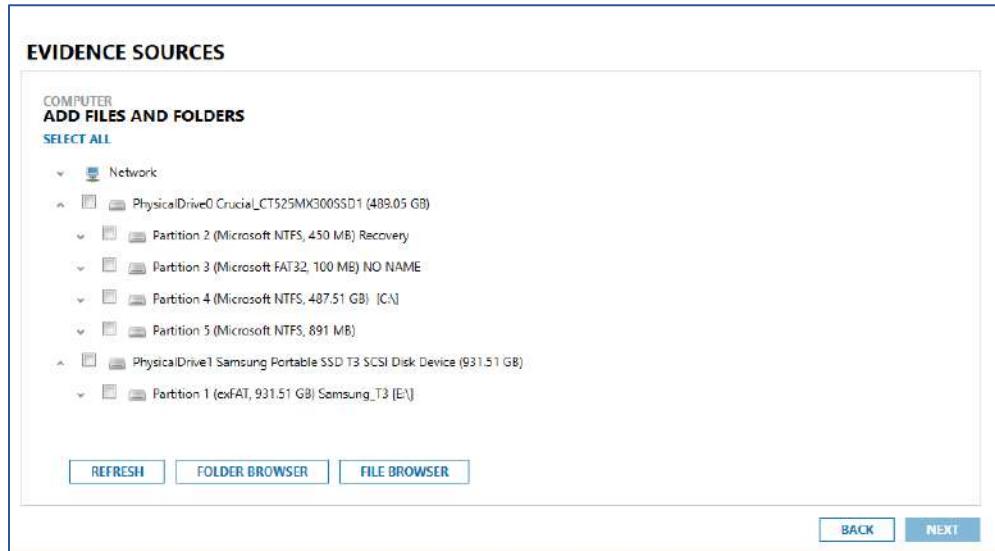


Figure 2.15 Adding files and folders

The MOBILE option allows the user to add smart phone data acquired from a separate source. There are six options available as seen in Figure 2.16. The six options are: Android, iOS, Windows Phone, Kindle Fire, Media Transfer Protocol (MTP), and SIM Card.

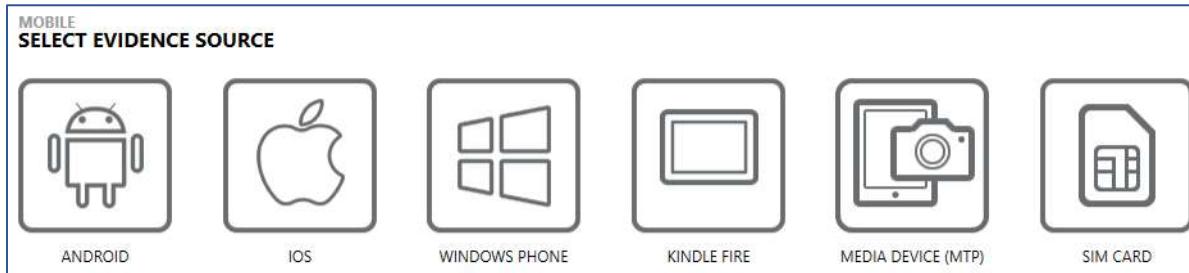


Figure 2.16 Mobile evidence sources

Data resides in different locations depending on the operating system. Specifying the operating system indicates to AXIOM Process which set of artifacts should be scanned and where they are located on the device/file system. Although some artifacts, e.g. Facebook, Twitter, WhatsApp, etc. can be parsed from different mobile OS types, the location and layout of the data may be different. Therefore, it is important to ensure the correct OS is selected at the time the evidence is added.

After selecting the operating system type, the user can specify whether to LOAD EVIDENCE or ACQUIRE EVIDENCE. Selecting LOAD EVIDENCE presents the choice of processing a previously acquired image or



just a selection of files & folders. Just as for the computer-based evidence, AXIOM supports images from mobile devices in many different formats and will process both physical and logical based images (full vs. quick). Mobile images generated using other tools can be added by selecting the raw data files (typically .bin files), or their proprietary files (.ufd.). If the proprietary files cannot be seen, ensure the filetype for the image is set as All Files (*.*). Images acquired with advanced procedures such as JTAG, Chip-Off, or ISP techniques can also be loaded directly into AXIOM Process.

The FILES & FOLDERS option can be used to analyze artifacts directly from the file system of a device, or from a collection of files such as an iTunes backup found on a PC. When using the FILES & FOLDERS option, AXIOM Process will scan each file individually to parse for the artifacts selected. Although this option is likely to be used less frequently than the image option, it can be used to obtain information when only certain files are provided or recoverable due to restrictions within the case.

When an image file is added to the case, regardless of type, the next option presented is SELECT SEARCH TYPE.

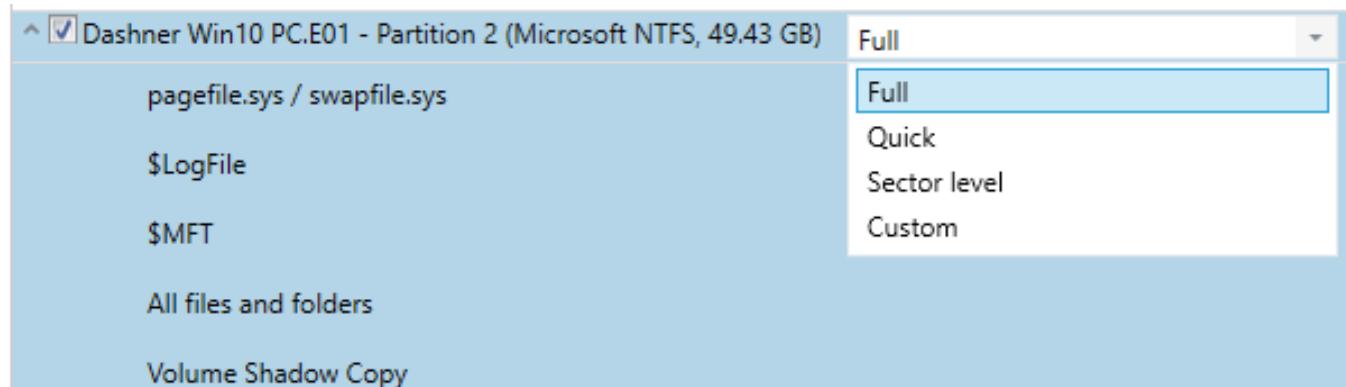


Figure 2.17 Search types

If a computer-based image is added there are four possible search types: Full, Quick, Sector level, and Custom. If mobile-based evidence is added, the search type will default to the OS.

The Full search type scans all areas of a drive or image for artifacts. This includes unallocated space, uninitialized space, and file slack space.

If the user does not wish to search all areas of the drive or image, the scan can be limited by selecting the Quick option. This searches the most common areas of your computer where AXIOM expects to find the evidence. Common areas include default application data directories (regardless of which language pack is installed), the Windows registry, user profiles, and My Documents. The list of common areas searched by AXIOM Process can be obtained from your instructor.

Alternatively, the search type can be set as Custom which allows the user to select which areas of the disk/image to search, e.g. only search the common areas, but also search unallocated space.

The Sector Level scan is the slowest of all the search types but can help rebuild information from systems that are unsupported, or images that may be corrupted. This can also be very helpful in a chip-off or JTAG acquisition of a mobile device where the imaging process was not able to pull the entire memory of the chip.

If you want to delete evidence from your case, you can do so by removing an evidence source and all associated evidence.

Warning: Removing an evidence source is a permanent action that cannot be undone.

- In AXIOM Examine, click Process > Remove evidence from case.
- Select the checkbox beside the evidence source you want to remove.
- Click Remove evidence source.

PROCESSING DETAILS

The PROCESSING DETAILS section is where the user can add any keywords to be searched for as part of the processing and add any hash sets for identification/elimination of files.

PROCESSING DETAILS	
Search archives and mobile backups	On
Add keywords to search	
Extract text from files (OCR)	
Calculate hash values	On
Categorize chats	
Categorize pictures and videos	
Add CPS data to search	
Find more artifacts	

Figure 2.18 Processing details

Any keywords to be searched for as part of the evidence processing are added using the ADD KEYWORDS TO SEARCH option.

Keywords can either be added as individual words, or as Keyword Lists. The keyword list should be a text document with a single word/phrase-per-line. These keyword lists can include both standard words



and/or Regex/GREP expressions. If an individual list is not needed for a case, de-select it by removing the check in the Enabled column for that word list and AXIOM Process will not search for those keywords. This allows the user to add keyword lists for specific types of examinations, e.g. child sexual abuse material (CSAM), fraud, or theft, and only select the keyword list(s) relevant to the individual case. Once a keyword list is enabled the content is displayed in the KEYWORDS window underneath.

NOTE: If the keyword list contains any Regex/GREP expressions, ensure the Regex/GREP checkbox is selected for that keyword in the KEYWORDS window.

KEYWORD LISTS			
ADD KEYWORD LIST		Lists added: 2	
Enabled	File source	Date loaded	Number of records
<input checked="" type="checkbox"/>	D:\Class Files\AE200\Evidence\Dashner Search Terms.txt	4/13/2017 1:47:58 PM	50
<input checked="" type="checkbox"/>	D:\PEDs.txt	6/14/2017 12:07:59 PM	4

KEYWORDS			
ADD KEYWORD		Items added: 54	
Keyword	Regex / GREP		
4[0-9]{12}(?:[0-9]{3})?	<input checked="" type="checkbox"/>		
5[1-5][0-9]{14}	<input checked="" type="checkbox"/>		
6(?:011 5[0-9]{2})[0-9]{12}	<input checked="" type="checkbox"/>		
amphetamine	<input type="checkbox"/>		

Figure 2.19 Keyword lists

The KEYWORD SEARCH TYPE, as displayed in Figure 2.20, is very important as it controls what areas of the evidence are searched for keywords. AXIOM Process can search for keywords during processing in one of two ways – at an Artifacts level, and across All content. By default, AXIOM Process will only search for the keywords at an artifact level, and this is the faster method. The second option instructs AXIOM Process to conduct an in-depth search across the entire disk/image. This includes all files within the file system, regardless of whether an artifact was extracted from the file, unallocated, and slack space. Any keyword hit results that are not associated with artifacts in the case, such as those found in unallocated space are displayed in the Artifacts explorer under the KEYWORD SNIPPETS category. Searching for keywords across all content will significantly increase processing time.

KEYWORD SEARCH TYPES

Select the type of keyword search you want to perform:

- Artifacts** — For quick results, search artifacts only.
- All content** — For more indepth results, search both the artifacts and all content. This increases processing time. Matches from the File system are displayed in the Artifact explorer as new Keyword snippets.

Figure 2.20 Keyword search types

The keywords that were searched for during processing are included in the Keyword List filter of AXIOM Examine. This allows the examiner to quickly identify the artifacts containing these keywords.

As of version 5.0, both “Artifacts” and “All Content” keyword searches can be performed after processing is completed from within AXIOM Examine.

Examiners can utilise Optical Character Recognition (OCR) technology to help them recover embedded text in PDFs, scanned documents, and images. Examiners have two options to enable OCR, the first during the processing options and later can also be applied to evidence as a post-processing option.

PROCESS FILES USING OPTICAL CHARACTER RECOGNITION

During a scan, Magnet AXIOM can extract text from certain files using optical character recognition (OCR). AXIOM Examine displays the extracted text in its own card, called Text extracted using OCR.

OCR is optimized to extract text from pictures in PDF documents, scanned documents, and pictures of documents. While OCR can extract text from other types of pictures, such as pictures of scenery, results might vary.

NOTE: Running OCR requires more processing time. To decrease processing time, consider running OCR from AXIOM Examine after your case finishes processing.

Extract text from the following types of artifacts:

- PDF documents
- Pictures

Figure 2.21 Optical Character Recognition

Within CALCULATE HASH VALUES is an option to CALCULATE HASH VALUES FOR ALL FILES. This option instructs AXIOM Process to generate a hash value (MD5, SHA1, or both) for all files within the case, regardless of Artifact status. This option is off by default because it increases processing time.



CALCULATE HASH VALUES FOR ALL FILES

Enable AXIOM Process to calculate hash values for each file in an evidence source so that AXIOM Examine displays the hash values for each file in the File system explorer Details section.

Configure hash settings to change the format that hashes are calculated in, to change where imported hash values are stored, and to limit the size of files hashed to decrease processing times.

- Calculate hash values for all files so that AXIOM Examine displays these values in the File system explorer.

CONFIGURE HASH SETTINGS

Figure 2.22 Calculating hash values

To mitigate this increase in processing time, if the user selects to calculate hashes for all files, a size limit can be set. By default, if this option is enabled, the size limit is set to 500MB. Therefore, any file larger than 500MB will not be hashed. The size limit applied can be changed or removed completely by selecting **CONFIGURE HASH SETTINGS**. If the option to **CALCULATE HASH VALUES FOR ALL FILES** is enabled, the hashes generated will be displayed in the File system explorer of AXIOM Examine.

NOTE: The option to **CALCULATE HASH VALUES FOR ALL FILES** cannot be disabled if one of the hash lists in the **TAG FILES WITH MATCHING HASH VALUES** or **IGNORE NON-RELEVANT FILES** sections is enabled.

The second option, **TAG FILES WITH MATCHING HASH VALUES**, instructs AXIOM Process to tag files based on their hash and display the tags in the File system explorer of AXIOM Examine. The hash list must be a plain text file with one hash (MD5 or SHA1) per line. Once the hash list has been added, the user can set the name of the Tag that will be applied to any matching files. If a list has been previously added for another case it can be Enabled for inclusion in the current case or disabled or deleted as necessary.

TAG FILES WITH MATCHING HASH VALUES

Import MD5 and SHA1 hash values for files that are of possible interest to your case so that Examine tags the matching files in the File system explorer.

For example, you can provide hash values for known documents or files so you can quickly determine if these files exist in your evidence. Each MD5 and SHA1 hash value must appear on its own line.
AXIOM calculates hash values for all files when this feature is enabled.

ADD FILE **DISABLE ALL FILES**

Records loaded: 3

Enabled	File source	Date loaded	Number of records	Tag
<input checked="" type="checkbox"/>	File Hashes to Match.txt	6/22/2018 11:43:21	3	Hash match

Figure 2.23 Tagging files with matching hash values



The third option, IGNORE NON-RELEVANT FILES, instructs AXIOM Process to disregard any file with a hash value that matches one listed in an enabled hash list. This option is commonly used to identify known system files, e.g. files associated with the Windows OS, and instructs AXIOM Process to undertake no further processing of the file. The file itself will still be displayed in the File system explorer of AXIOM Examine, but AXIOM Process will not search it for any artifacts. These hash lists are also plain text files with one hash (MD5 or SHA1) per line. This provides the ability for the user to generate their own hash lists, e.g. from a company's own standard or "gold" build, to eliminate the content of the standard build from the review, thus focusing on just user activity.

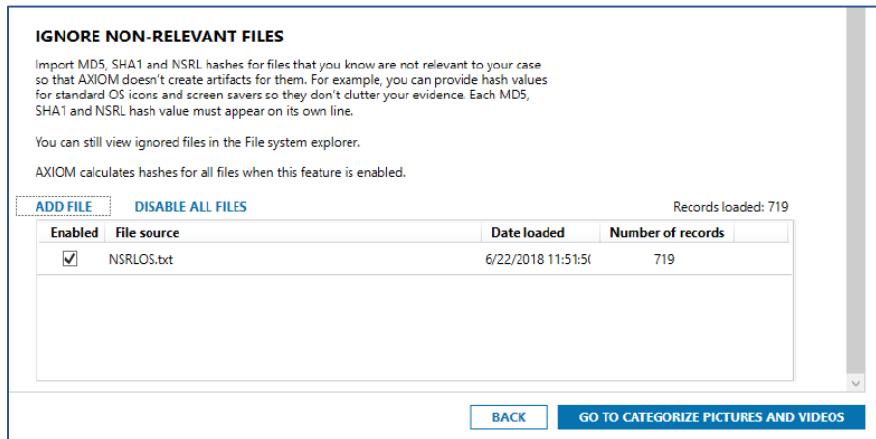


Figure 2.24 Ignoring non-relevant files

The National Software Reference Library (NSRL), generated by the National Institute for Standards and Technology (NIST), is a set of hash lists of known software. These hash lists can be downloaded from the Magnet Forensics website and added to AXIOM Process by selecting [ADD FILE](#). If a list has been previously added for another case it can be enabled for inclusion in the current case or disabled or deleted as necessary.

The CATEGORIZE CHATS section of PROCESSING DETAILS allows the user to enable the Magnet.AI feature to automatically categorize chat conversations based on selected categories. Note that this feature can also be enabled from within AXIOM Examine and will be covered in more detail in a later module.

The CATEGORIZE PICTURES AND VIDEOS section of PROCESSING DETAILS provides the user with three methods to categorize pictures and videos as part of the processing stage.

The BUILD PICTURE COMPARISON section processes media so that the examiner can find similar pictures based on a reference picture from within AXIOM Examine.

The CATEGORIZE PICTURES WITH MAGNET.AI section enables the Magnet.AI feature to automatically categorize and tag pictures within specified categories.

Note that BUILD PICTURE COMPARISON and MAGNET.AI can also be enabled from within AXIOM Examine and will be discussed in a later module.



If the Project VIC or CAID hash sets for pictures and videos are being used, these can be loaded by selecting **ADD HASH LIST** under CATEGORIZE PICTURES AND VIDEOS BY HASH VALUE as shown in Figure 2.25.

The PhotoDNA option is also located within this section and can be enabled by selecting **EDIT** and entering the passcode provided by Magnet Forensics. Access to the PhotoDNA database is for restricted to law enforcement.

CATEGORIZE PICTURES AND VIDEOS BY HASH VALUE

Import hash lists that contain MD5 or SHA1 hashes for pictures and videos so that AXIOM Examine automatically categorizes the pictures and videos it finds with matching hashes from these files. You can import JSON files from Project VIC and CAID organizations or your own text files. After you import a hash list, you can add the list to a hash set and select which categories you want to update in the hash set.

The order of the hash sets in the 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.

Each MD5 or SHA1 hash value must appear on its own line in the hash list.

PhotoDNA is currently deactivated [EDIT](#)

ADD HASH LIST

Records loaded: 0

Enabled	Hash set	Date updated	Categories	Number of records	Priority
<input type="checkbox"/>	sample.json				



Figure 2.25 Loading Project VIC / CAID files

NOTE: Artifacts within the Media category will be hashed even when the option CALCULATE HASH VALUES FOR ALL FILES is disabled.

Within FIND MORE ARTIFACTS is the option to USE THE DYNAMIC APP FINDER. Enabling the Dynamic app finder instructs AXIOM Process to search the evidence for any SQLite databases that are not associated with a known application, thereby identifying applications that are not natively supported. Even though the application may not be natively supported, AXIOM Process can still read the content of the SQL tables. The Dynamic App Finder provides the examiner with the ability to map selected database fields to artifact columns and display the content in AXIOM Examine. Dynamic App Finder will be covered in Module 11.

USE THE DYNAMIC APP FINDER

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

After AXIOM Process completes its search, it displays all the databases it discovers on the Customize artifacts screen. You can use the data that's displayed to configure your own custom artifacts.

Allow AXIOM to find more artifacts (this will increase processing time)

Figure 2.26 Using the Dynamic App Finder

The examiner also has the option to SEARCH FOR CUSTOM FILE TYPES using a CUSTOM FILE TYPES list. This list can be configured to allow AXIOM Process to create artifacts for file types that aren't currently supported by AXIOM artifacts. The examiner can edit the list by clicking [EDIT CUSTOM FILE TYPES LIST](#).

SEARCH FOR CUSTOM FILE TYPES

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

CUSTOM FILE TYPE LIST LOCATION

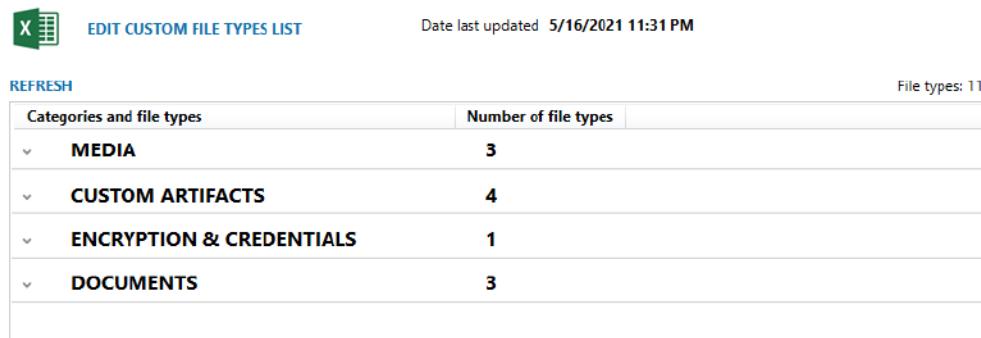
Optionally, change where the Custom file types list is stored.

File path [CHANGE LOCATION](#)

EDIT CUSTOM FILE TYPES

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

AXIOM Process will search for the categories and custom file types listed in the table below. To change this selection for each platform, go to Artifact details.



The screenshot shows a user interface for managing custom file types. At the top, there's a header with a refresh icon, the title 'EDIT CUSTOM FILE TYPES LIST', and a date/time stamp 'Date last updated 5/16/2021 11:31 PM'. On the right, it says 'File types: 11'. Below the header is a table with two columns: 'Categories and file types' and 'Number of file types'. The table lists four categories: MEDIA (3), CUSTOM ARTIFACTS (4), ENCRYPTION & CREDENTIALS (1), and DOCUMENTS (3). Each category row has a collapse/expand arrow to its left.

Categories and file types	Number of file types
▼ MEDIA	3
▼ CUSTOM ARTIFACTS	4
▼ ENCRYPTION & CREDENTIALS	1
▼ DOCUMENTS	3

Figure 2.27 Search for Custom File Types

ARTIFACT DETAILS

ARTIFACT DETAILS contain subcategories for each of the evidence types that can be added to AXIOM Process. AXIOM Process allows the user to set which artifacts will be scanned for. There are three subcategories, Computer, Mobile and Cloud artifacts.



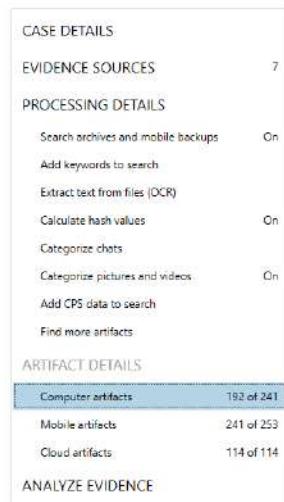


Figure 2.28 Artifact Details

Individual artifacts can be selected or deselected as required, or entire categories can be selected by placing a check in the box beside the category name.

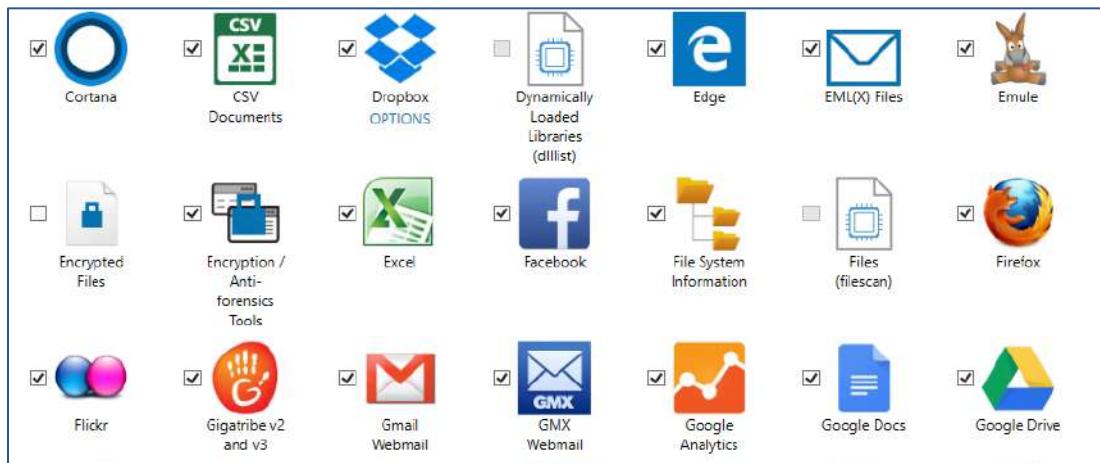


Figure 2.29 Individual computer artifacts

COMPUTER ARTIFACTS	MOBILE ARTIFACTS	CLOUD ARTIFACTS
CLEAR ALL	CLEAR ALL	CLEAR ALL
<input checked="" type="checkbox"/> ADDITIONAL SOURCES (4 of 4) <input checked="" type="checkbox"/> APPLICATION USAGE (7 of 7) <input checked="" type="checkbox"/> CLOUD STORAGE (6 of 6) <input type="checkbox"/> COMMUNICATION (23 of 36) <input checked="" type="checkbox"/> CONNECTED DEVICES (9 of 9) <input type="checkbox"/> CUSTOM ARTIFACTS (4 of 5) <input checked="" type="checkbox"/> DOCUMENTS (16 of 16) <input type="checkbox"/> EMAIL & CALENDAR (13 of 14) <input checked="" type="checkbox"/> ENCRYPTION & CREDENTIALS (5 of 5) <input checked="" type="checkbox"/> LOCATION & TRAVEL (1 of 1) <input type="checkbox"/> MEDIA (12 of 13) <input type="checkbox"/> MEMORY (0 of 21) <input type="checkbox"/> OPERATING SYSTEM (63 of 66) <input type="checkbox"/> PEER TO PEER (8 of 11) <input type="checkbox"/> SOCIAL NETWORKING (8 of 9) <input type="checkbox"/> WEB RELATED (14 of 19)	<input checked="" type="checkbox"/> APPLICATION USAGE (19 of 19) <input checked="" type="checkbox"/> CLOUD STORAGE (3 of 3) <input type="checkbox"/> COMMUNICATION (52 of 56) <input checked="" type="checkbox"/> CONNECTED DEVICES (15 of 15) <input type="checkbox"/> CUSTOM ARTIFACTS (4 of 5) <input checked="" type="checkbox"/> DOCUMENTS (17 of 17) <input checked="" type="checkbox"/> EMAIL & CALENDAR (13 of 13) <input checked="" type="checkbox"/> ENCRYPTION & CREDENTIALS (3 of 3) <input checked="" type="checkbox"/> LOCATION & TRAVEL (11 of 11) <input type="checkbox"/> MEDIA (15 of 16) <input type="checkbox"/> OPERATING SYSTEM (34 of 35) <input checked="" type="checkbox"/> PEER TO PEER (1 of 1) <input type="checkbox"/> SOCIAL NETWORKING (21 of 23) <input type="checkbox"/> WEB RELATED (33 of 36)	<input checked="" type="checkbox"/> APPLICATION USAGE (2 of 2) <input checked="" type="checkbox"/> CLOUD STORAGE (16 of 16) <input checked="" type="checkbox"/> COMMUNICATION (24 of 24) <input checked="" type="checkbox"/> CONNECTED DEVICES (2 of 2) <input checked="" type="checkbox"/> DOCUMENTS (2 of 2) <input checked="" type="checkbox"/> EMAIL & CALENDAR (9 of 9) <input checked="" type="checkbox"/> ENCRYPTION & CREDENTIALS (1 of 1) <input checked="" type="checkbox"/> LOCATION & TRAVEL (6 of 6) <input checked="" type="checkbox"/> MEDIA (5 of 5) <input checked="" type="checkbox"/> OPERATING SYSTEM (3 of 3) <input checked="" type="checkbox"/> SOCIAL NETWORKING (30 of 30) <input checked="" type="checkbox"/> WEB RELATED (14 of 14)

Figure 2.30 Computer, mobile, and cloud artifacts

Any artifacts that require or offer additional options will have a blue **OPTIONS** beneath them. Selecting **OPTIONS** opens a dialog window allowing additional information to be added or settings to be changed.

*Figure 2.31 Picture artifact options*

As seen in Figure 2.32, the examiners can select to Detect skin tone, and Create a preview using still frames which generates a filmstrip of the video content by taking a still frame from the video every 10%, and save a copy of the video files into the case. Selecting Save videos up to stores the full video content into the case rather than just a thumbnail or filmstrip. This allows the videos to be previewed within AXIOM Examine without having to extract them to the local machine first. If this option is selected, examiners can also set a maximum file size limit. The default setting for this option is 500MB, so only videos smaller than 500MB will be extracted from the evidence file and stored in the case. This setting can be changed by the examiner at the time of processing, if required.

AXIOM Process can carve, as well as parse video files and the examiner can also set a maximum size for these carved videos. By default, AXIOM Process will only carve the first 20MB of video files. For a complete list of supported media types, see the “Supported Media and File Types” section of the Artifact Reference.



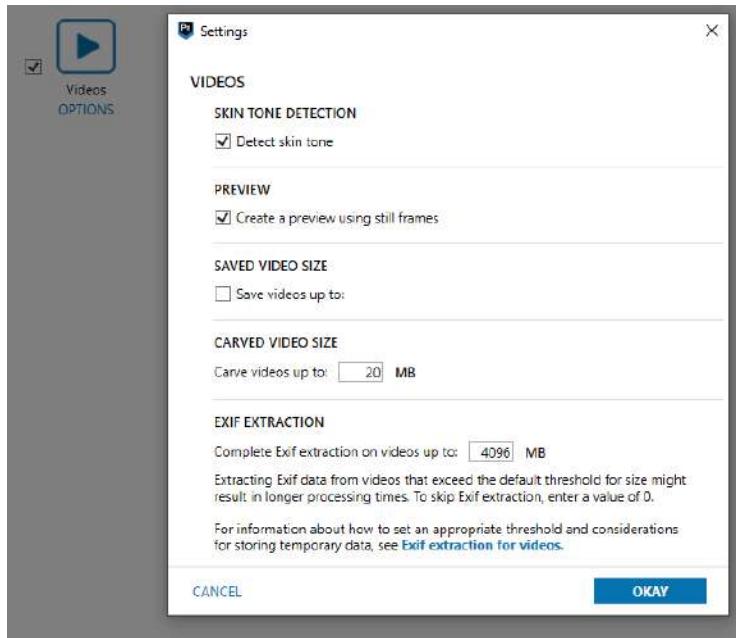


Figure 2.32 Video artifact options

PARSING AND CARVING

At this point, it is worth discussing two terms that are frequently used in digital investigations – **parsing** and **carving**.

Parsing is a method of interpreting structured information. Magnet AXIOM can parse videos, pictures, and other documents when it encounters a file with a known extension and format. And, for applications that store their data in a known structure (like a SQLite database), Magnet AXIOM can parse the information from the database into meaningful artifacts.

Carving involves searching raw data to identify headers or other patterns. For example, when a scan identifies the following stream of bytes \xFF \xD8 \xFF \xE0, this signifies the beginning of a **.jpg** picture. If the **.jpg** file is renamed with a different extension, Magnet AXIOM can still carve the picture even though it can no longer parse it. Unlike other forensic tools, carving does not necessarily indicate that the data came from unallocated space – carved artifacts can come from anywhere. It is common that SQLite databases will contain records that will be recovered via carving. These could be potential deleted records, but it could also be where the SQLite databases restructure information within the file container.

SEARCH 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 if multiple file types are added.

ANALYZE EVIDENCE

The Analyze Evidence section provides a summary of the imaging and processing that will be undertaken. The examiner has one last chance to review the devices and/or evidence added to the case for imaging and processing. Evidence items added to the case for processing display Ready or Ready to Search within the Status field, and items to be acquired display Ready to image.

ANALYZE EVIDENCE				
SOURCES TO PROCESS				
Type	Image / location name	Evidence number	Search type	Status
	DashnerWin10PC.E01 - Partition 1 (Microsoft NTFS, 5)	DashnerWin10PC.E01	Full	Ready
	DashnerWin10PC.E01 - Partition 2 (Microsoft NTFS, 4)	DashnerWin10PC.E01	Full	Ready
	DashnerWin10PC.E01 - Unpartitioned space	DashnerWin10PC.E01	Unpartitioned	Ready

Figure 2.33 Final review screen prior to analyzing evidence

Once the examiner has clicked the **ANALYZE EVIDENCE** button, AXIOM Process starts by acquiring any evidence items added via the ACQUIRE EVIDENCE option. Once all the images have been acquired, the processing phase begins. During processing the CURRENT SEARCH LOCATION screen, as shown in Figure 2.34, details which evidence item is currently being processed.



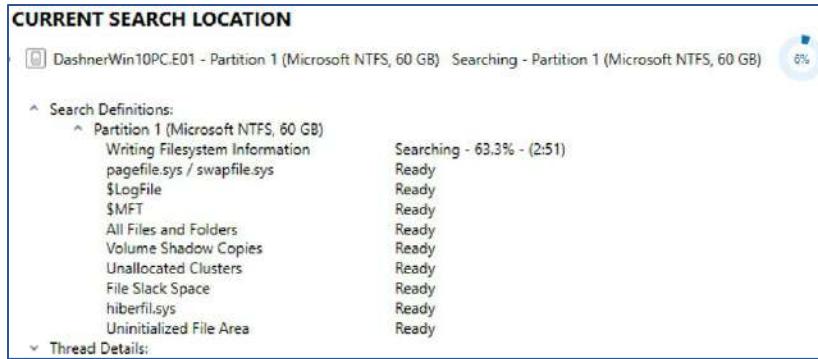


Figure 2.34 Search progress and current search location

AXIOM Process uses all the cores allocated to it in Tools → Settings → SEARCH SPEED to parse and carve the information as quickly as possible. The Thread Details section details the item being processed by each individual core at that moment. (Figure 2.35).

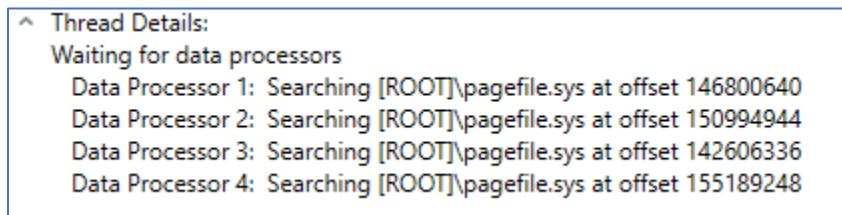


Figure 2.35 Thread details

RUNNING EXERCISES

CREATING A NEW CASE

- Start AXIOM Process from the icon on the Desktop
- Click the Create New Case button.
- The new case opens at the CASE DETAILS.
- In the CASE INFORMATION section, enter a Case number of your choosing.
- Under LOCATION FOR CASE FILES, change the Folder name to “Dashner Case”.
- Click BROWSE next to the File path and set the case folder location to be the \Cases\ folder on the Desktop.
- Under LOCATION FOR ACQUIRED EVIDENCE, also change the Folder name to “Dashner Case” and set the File path as the \Evidence\ folder on the Desktop.

- In the SCAN INFORMATION section, enter your name into the Scanned by field, and a short Description.

ADDING EVIDENCE TO THE CASE

- Click the **GO TO EVIDENCE SOURCES** button.
- This brings the user to the EVIDENCE SOURCES screen.
- Under SELECT EVIDENCE SOURCE, click the COMPUTER icon, then the WINDOWS icon.
- In the LOAD OR ACQUIRE window, click the LOAD EVIDENCE icon.
- Under SELECT EVIDENCE SOURCE, click the IMAGE icon.
- This opens a folder browser window to locate the evidence image.
- Navigate to the Desktop and locate the folder **\Evidence** Open the folder **\DashnerWin10PC**, select the **DashnerWin10PC.E01** file and click **Open**.
- Ensure all the partitions are selected, then click **NEXT**.
- On Partition 1, ensure the Search type is set to Full.
- Notice all the areas that will be searched.
- On Partition 2 change the Search type to Quick from the drop-down menu and compare it to Partition 1. What areas are no longer searched?

- Change the Search type for Partition 2 to Custom.
- This option allows the user to select just the areas they wish to search.
- Change the Search type back to Full and click **NEXT**.
- Each of the partitions in the image file are now listed under EVIDENCE SOURCES ADDED TO CASE, along with their Search type and Status.
- If required, the Evidence number can be changed by clicking into the field, changing the name, and clicking **SAVE**.
- Under SELECT EVIDENCE SOURCE, click the COMPUTER and WINDOWS icon again.
- In the LOAD OR ACQUIRE window, click the LOAD EVIDENCE icon.
- Under SELECT EVIDENCE SOURCE, click the IMAGE icon.



- Navigate to the Desktop and locate the folder **\Evidence** again. Open the folder **\SanDisk Cruzer**, select the **SanDisk Cruzer USB Device.E01** file and click **Open**.
- Under SELECT EVIDENCE SOURCE, click the COMPUTER and WINDOWS icon again.
- In the LOAD OR ACQUIRE window, click the LOAD EVIDENCE icon.
- Under SELECT EVIDENCE SOURCE, click the IMAGE icon.
- Navigate to the Desktop and locate the folder **\Evidence** again. Open the folder **\Lexar USB**, select the **Lexar USB Flash drive USB Device 7.46GB Full Image.E01** file and click **Open**.
- The padlock icon identifies it is an encrypted drive.
- Ensure the entire drive is selected and click **NEXT**.
- The Encryption Type has now been identified as BitLocker.
- The **NEXT** button is currently greyed-out.
- Notice that this drive is encrypted with BitLocker. At this point, we do not have the decryption key for this drive. Press the **BACK** button to remove this evidence item without processing it.
- Under SELECT EVIDENCE SOURCE, click the MOBILE and the ANDROID icon.
- In the LOAD OR ACQUIRE window, click the LOAD EVIDENCE icon.
- Under SELECT EVIDENCE SOURCE, click the IMAGE icon.
- Navigate to the Desktop and locate the folder **\Evidence** again. Open the folder **\Pixel 3a**, select the **Google Pixel 3a Quick Image** file and click **Open**.
- Under SELECT EVIDENCE SOURCE, click the CLOUD icon.
- In the LOAD OR ACQUIRE window, click the LOAD EVIDENCE icon.
- Under SELECT EVIDENCE SOURCE, click the MAGNET FORENSICS icon, then choose AXIOM CLOUD IMAGE on the next screen.
- Navigate to the Desktop and locate the folder **\Evidence** again. Open the folder **\Cloud**, select the **Dashner Cloud 12162019** file and click **Open**.
- Change the evidence number to **Dashner Cloud 12162019.zip**

SETTING THE PROCESS OPTIONS

- Click **GO TO PROCESSING DETAILS**.

- This steps the user to the PROCESSING DETAILS screen.
- Click the **ADD KEYWORDS TO SEARCH** button.
- In the KEYWORD SEARCH TYPES section, the default is set as Artifacts.
- In the KEYWORD LISTS section, click **ADD KEYWORD LIST**.
- Navigate to the **\Evidence** folder on the desktop, select the file **Dashner search terms.txt** and click **Open**.
- The keyword list is automatically Enabled.
- All the keywords/phrases are added to the KEYWORDS and will be searched for.
- Deselect the keyword list just added.
- All the keywords are removed from the KEYWORDS to be searched for.
- Ensure the keyword list is re-enabled, then ensure Regex/GREP is selected for the GREP terms for credit card numbers.
- Click the option to **GO TO SEARCH ARCHIVES AND MOBILE BACKUPS** from the left-hand navigation pane.
- Ensure both the options to **SEARCH ARCHIVES** and **SEARCH MOBILE BACKUPS** are selected.
- Click the option to **CALCULATE HASH VALUES** from the left-hand navigation.
- This steps the user to the Calculate hash values section of PROCESSING DETAILS.
- Under **CALCULATE HASH VALUES FOR ALL FILES**, select the **CONFIGURE HASH SETTINGS** link.
Scroll down in the Settings window that opens and locate the **HASH FORMATS** heading. What algorithms are available for hashing?

-
- Choose the option to calculate both MD5 and SHA1 hash values and then click on **OKAY** to exit the Settings window.
 - Under **TAG FILES WITH MATCHING HASH VALUES** click **ADD FILE**.
 - Navigate to the **\Evidence** folder on the desktop, select the file **File Hashes to Match.txt** and click **Open**.
 - The file containing the hashes is added to the list and details the date the hash list was loaded and how many hashes the file contains.
 - A Tag Hash Match is automatically applied to any matches encountered during case processing,



this tag can be changed if required.

- Click **GO TO CATEGORIZE CHATS** in the lower right corner of the screen.
- This section allows an examiner to enable the use of Magnet.AI categorization features for chat messages which may be found during case processing.
- Select the check-box under the **Enabled** column for the available chat categories.
- Notice the **Tag** column is now populated with a tag for any potential matches found during case processing. As before, this tag can be changed.
- Deselect both check-boxes under the **Enabled** column and then click on the **GO TO CATEGORIZE PICTURES AND VIDEOS** button.
- This steps the user to the Categorize pictures and videos section of PROCESSING DETAILS.
- The first section, PROCESS PICTURES WITH MAGNET.AI, includes BUILD PICTURE COMPARISON and CATEGORIZE PICTURES WITH MAGNET.AI. These features will be discussed in a later module.
- Under CATEGORIZE PICTURES AND VIDEOS BY HASH VALUE click **ADD HASH LIST**.
- From the Add hash sets window that is displayed, click on **SELECT HASH LIST** under Step 1.
- Navigate to the **\Evidence** folder on the desktop, select the file **sample.json** and click **Open**.
- The on-disk path for the selected hash list can now be seen under Step 1.
- Under 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 from the list.
- To add the imported hash list to a new hash set, click **ADD NEW HASH SET** and provide a name for the hash set, then click on the **ADD** button.
- 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**.
- 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**.
- When you've finished, click on **Update Hash Set** at the lower left, then click **Close** at the lower right. The updated hash set is added to the list and details the number of records and their categories.

- If a record has no pre-assigned category, AXIOM Process assigns it a category of -1.
- Click on the **GO TO ADD CPS DATA TO SEARCH** button in the lower-right corner of the screen.
- This steps the user to the Add CPS Data to Search section of PROCESSING DETAILS.
- If an examiner has data exported from the Child Protection System (CPS) website, that CSV file can be imported by clicking on the **ADD CPS EXPORT FILE** button and navigating to the appropriate location.
- Click the **GO TO FIND MORE ARTIFACTS** button at the lower right corner of the screen.
- This steps the user to the FIND MORE ARTIFACTS section of PROCESSING DETAILS.
- At the top of this screen are options for using the dynamic app finder. Do not enable dynamic app finder at this time, it will be covered during the mobile evidence module later in the course.
- The lower section is to enable searching for custom file types using the **EDIT CUSTOM FILE TYPES LIST**.

SELECTING ARTIFACTS TO PROCESS AND SETTING ARTIFACT OPTIONS

- Click **GO TO COMPUTER ARTIFACTS**.
- This steps the user to the COMPUTER ARTIFACTS section of the ARTIFACT DETAILS.
- A parent category that does not have a tick in the check box indicates one or more artifacts within that category are not selected.
- The MEMORY artifacts are greyed-out. These artifacts are only enabled if a memory evidence source is added to the case.
- Select the parent category MEDIA and click **OPTIONS** beneath the Videos artifact.
- Under SAVED VIDEO SIZE, enable the option Save videos up to.
- This will save all videos of 500MB or less into the case.
- Select the parent category CLOUD STORAGE and click **OPTIONS** beneath the Dropbox artifact.
- Enter Dashner's Windows password – **vikingsfan123**
- Click ANALYZE EVIDENCE on the left hand navigation pane, and then **ANALYZE EVIDENCE**
- This steps the user to ANALYZE EVIDENCE where the examiner can review the evidence to be imaged and/or searched.
- Due to the time required to process this case, it has been pre-processed for you. Therefore, close AXIOM Process **WITHOUT** starting the processing.



ENCRYPTED DRIVES

Support for encrypted drives was introduced with AXIOM 1.1. Often encrypted drives or volumes are only identified after the investigation has started. The ability to post-process data enables the examiner to search for and identify potential passwords within the current evidence, then add the encrypted drive or volume to the case once potential passwords have been determined.

Microsoft BitLocker is covered in the AX100 – Forensic Fundamentals course, so will not be covered in detail in this course; however, BitLocker is a high level of encryption using AES to encrypt the full drive/volume.

To acquire a USB device encrypted using BitLocker, using a write-blocker, plug the USB device into the imaging computer. As can be seen in Figure 2.36, Windows automatically recognizes a BitLocker encrypted drive based on information found in the volume boot record (VBR) of the encrypted drive and File Explorer displays the drive with a padlock.

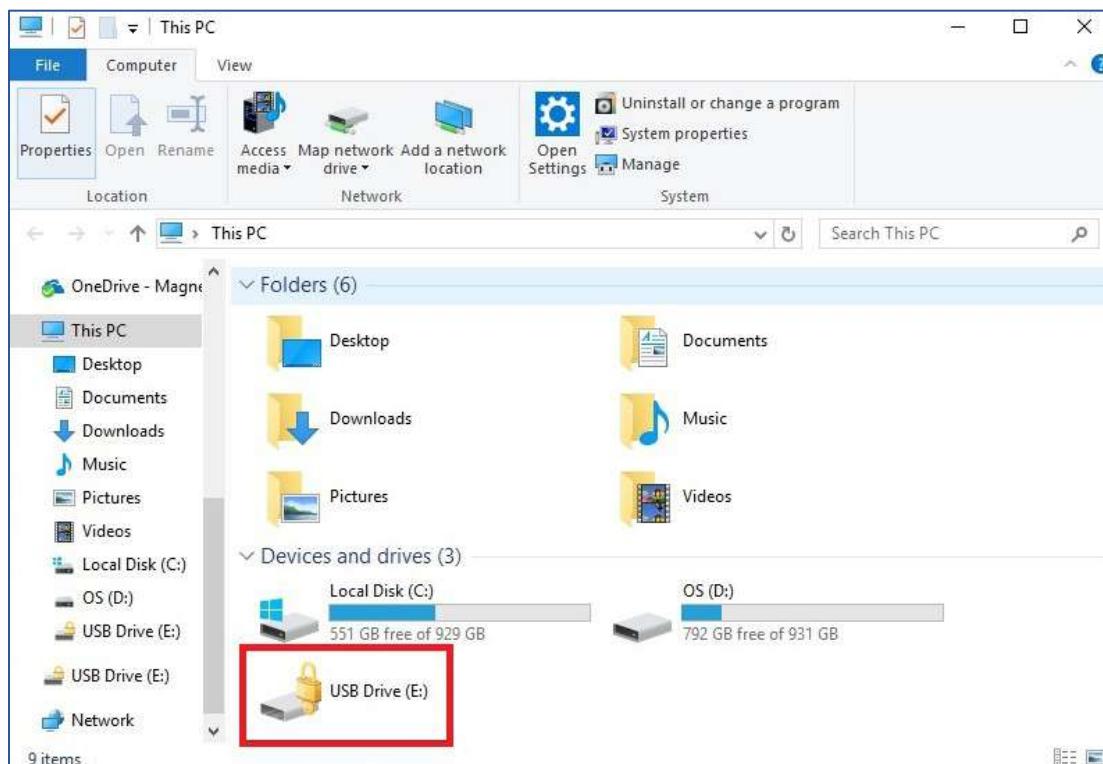


Figure 2.36 BitLocker encrypted USB device in File Explorer

Once the device is recognized, it can be acquired. If the password or recovery key is available, it can then be processed using AXIOM Process.

If an image is added to AXIOM Process and if the image was encrypted using one of the supported encryption types, AXIOM Process automatically recognizes the drive as encrypted and presents the examiner with DECRYPTION OPTIONS as shown in Figure 2.37.

WINDOWS DECRYPTION OPTIONS

Select the encrypted evidence sources you want to process by providing the necessary encryption details for each source. For some evidence sources, if you do not know the password or recovery key, AXIOM Process can attempt to crack the password using a password list of your choice. If password cracking is unsuccessful, that source will be skipped.

Partition 1 (7.46 GB)

Encryption type **Bitlocker**

Decryption option **I have the password / recovery key**

Password / Recovery key

Figure 2.37 BitLocker decryption options

AXIOM Process identifies the encryption type, which in this instance is BitLocker, and asks for the password or recovery key. When a password is entered, AXIOM Process displays **CHECK** as shown in Figure 2.38. The **NEXT** button will not activate until the correct password or recovery key is entered.

WINDOWS DECRYPTION OPTIONS

Select the encrypted evidence sources you want to process by providing the necessary encryption details for each source. For some evidence sources, if you do not know the password or recovery key, AXIOM Process can attempt to crack the password using a password list of your choice. If password cracking is unsuccessful, that source will be skipped.

Partition 1 (7.46 GB)

Encryption type **Bitlocker**

Decryption option **I have the password / recovery key**

>Password or recovery key is incorrect.

Password / Recovery key **password**

CHECK

Figure 2.38 Incorrect BitLocker password

If you do not have the correct password, review the computer evidence for the presence of a BitLocker Recovery Key text file. During the creation of a BitLocker encrypted drive, the encryption will not proceed until the user has saved a copy of the text file. The user could also print a hardcopy of the file, or print to PDF; however, AXIOM is looking for a text file. Many users save this to their Documents folder or their Desktop. This file contains a 48-digit recovery key that can be copied and pasted into the Password / Recovery key field and used instead of the password.

Once **ANALYZE EVIDENCE** is selected, AXIOM Process will first decrypt the drive, and then process the decrypted content.



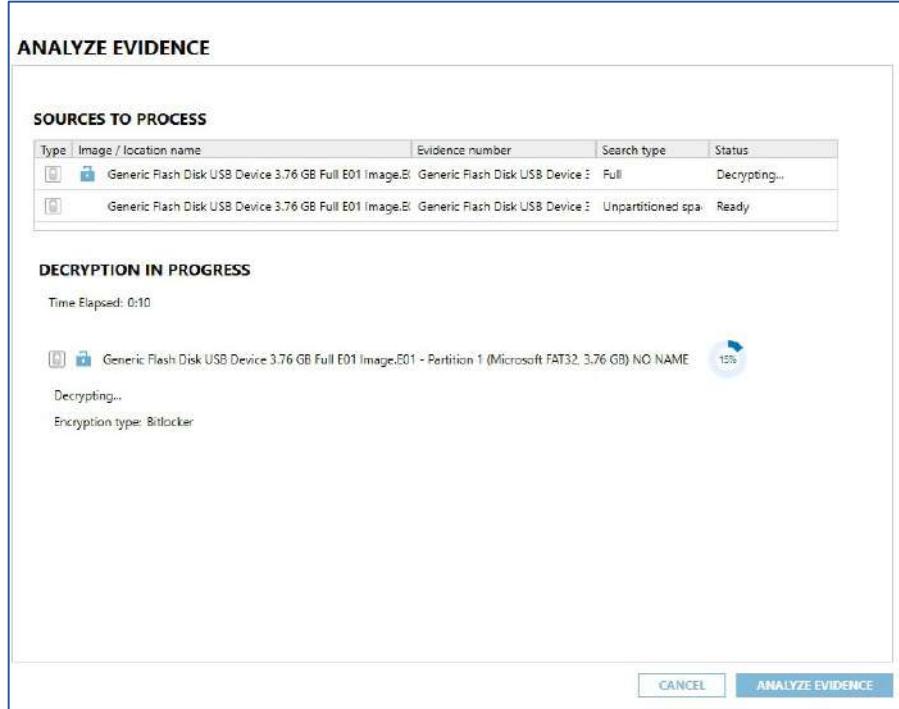


Figure 2.39 Decryption in progress

A full list of supported encryption types can be found in the AXIOM User Guide.

AXIOM EXAMINE SETTINGS

There are several configurable settings available from the Tools → Settings menu within AXIOM Examine which the examiner can change to customize how AXIOM Examine looks and behaves. By default, AXIOM Examine opens a case with the Case dashboard explorer open, however the DEFAULT EXPLORER to display when a case is first opened can be changed from the Tools → Settings menu. There are seven explorers in which to view the data:

- The Case dashboard explorer is the default view, and the command center of the case. It displays an overview of the evidence, artifacts, and tagged items.
- The Artifacts explorer displays the artifacts identified during the processing stage and displays them in a tabular form.
- The Connections explorer displays artifacts as nodes, connected by association lines which allow an examiner to easily discover how evidence is linked - even across multiple pieces of evidence.
- The File system explorer displays a tree directory structure of the file system or files stored on the evidence image.
- The Registry explorer displays a hierarchical view of all the registry files within the case.
- The Timeline explorer displays a graph showing artifact use.
- The Media explorer displays a media-focused view of the evidence within a case.

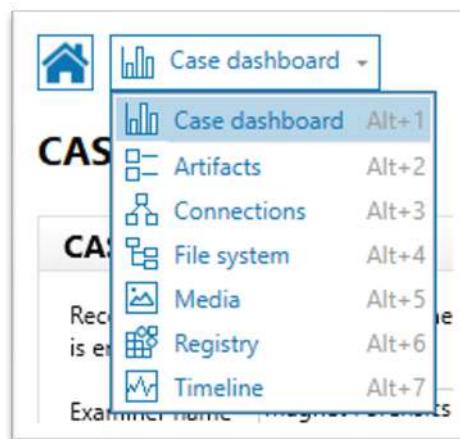


Figure 2.40 AXIOM Examine Explorers

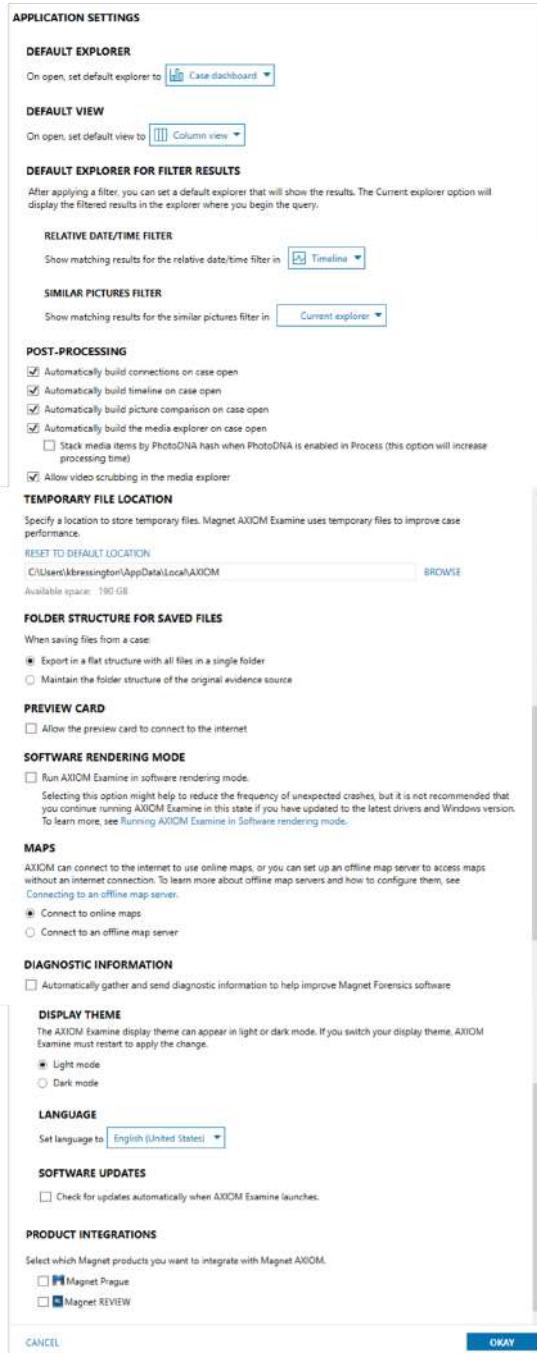


Figure 2.41 Default Explorer settings

As can be seen in Figure 2.41, the Settings menu allows examiners to change the display theme from Light Mode to Dark Mode. The settings also include the option to Automatically build connections, timeline, picture comparison and the media explorer that exist between artifacts within the case – connections will be covered in more detail in a later lesson. By default, the option to Automatically build

connections, timeline, media explorer and picture comparison is disabled, and the Build options process must be started manually from the menu option Tools → Build connections, as shown in Figure 2.42.

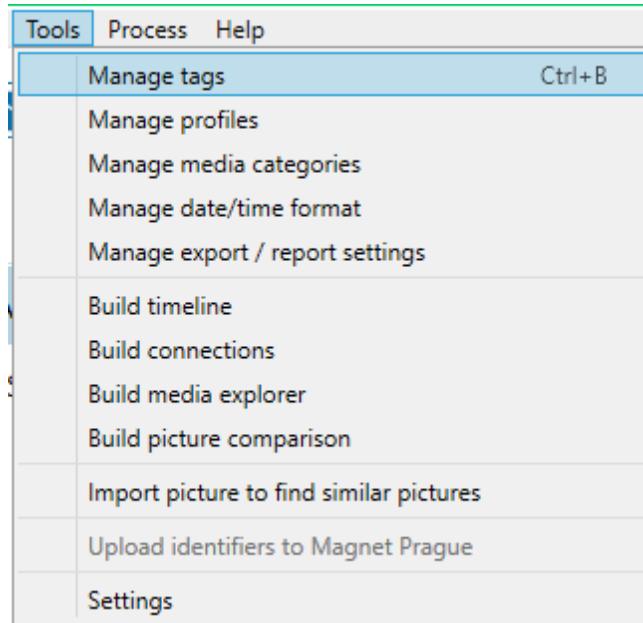


Figure 2.42 Manually building connections

If the option to Automatically build connections is enabled, AXIOM Examine will automatically start building connections between the artifacts once processing has completed. If new evidence is added post-processing, AXIOM Examine will again automatically build connections as soon as processing is complete. AXIOM Examine searches for connections between *all* artifacts within the case, not just connections between artifacts extracted from the same evidence item. If the option to automatically build connections is *not* enabled the examiner must remember to rebuild the connections each time new evidence is added to the case, and every time the examiner adds a user-defined artifact. User-defined artifacts will be covered in a later lesson. Connections are rebuilt from the menu option Tools → Build connections in AXIOM Examine. Similar functionality exists for building timeline and picture comparison.

The DEFAULT VIEW option controls how the artifacts are initially displayed in the EVIDENCE pane of the Artifact explorer. By default, the artifacts are displayed in Column view, but the view can be changed to either Classic view or Row view.



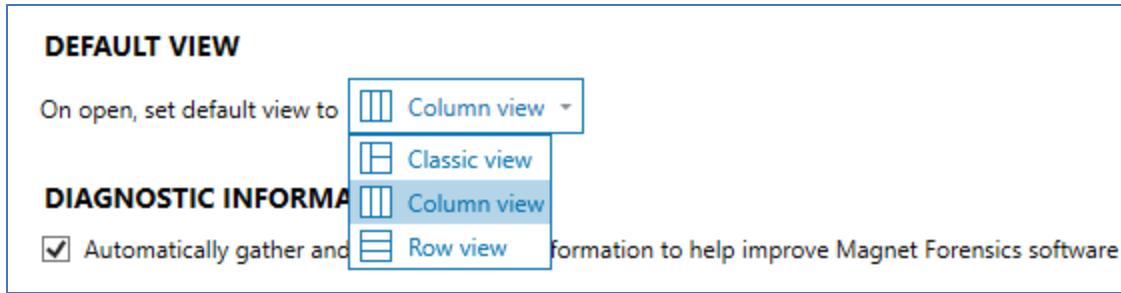


Figure 2.43 Default view settings in AXIOM Examine

The DIAGNOSTIC INFORMATION within Settings contains the option to Automatically gather and send diagnostics information to help improve Magnet Forensics software. If AXIOM is being used on a computer that is connected to the Internet, leaving this option enabled helps Magnet Forensics improve the user experience and identifies bugs in the software more quickly.

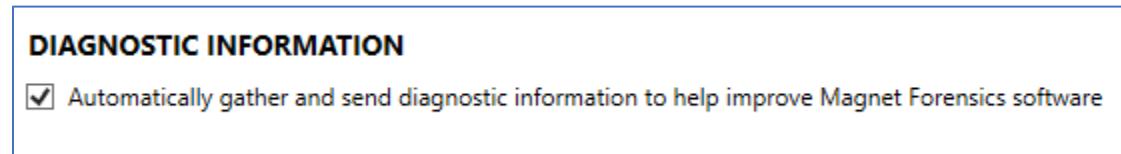


Figure 2.44 Sending diagnostic information

AXIOM also includes support for thirteen languages, as shown in Figure 2.45.

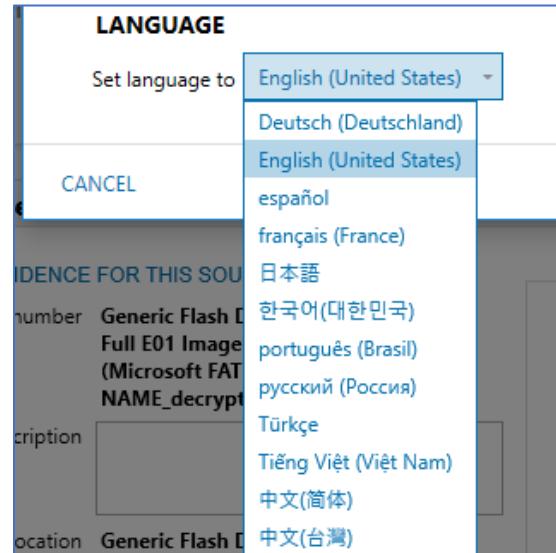


Figure 2.45 Language settings

CASE DASHBOARD

The Case dashboard was introduced to AXIOM Examine in version 2.0 and has been updated in version 6.0 to assist in Cloud insights. It is a central location where, once processing has completed, the examination and analysis process can begin. Unless the settings have been changed, upon completion of processing, AXIOM Examine displays the Case dashboard explorer, which contains a CASE OVERVIEW, EVIDENCE OVERVIEW, and PLACES TO START and CLOUD INSIGHTS.

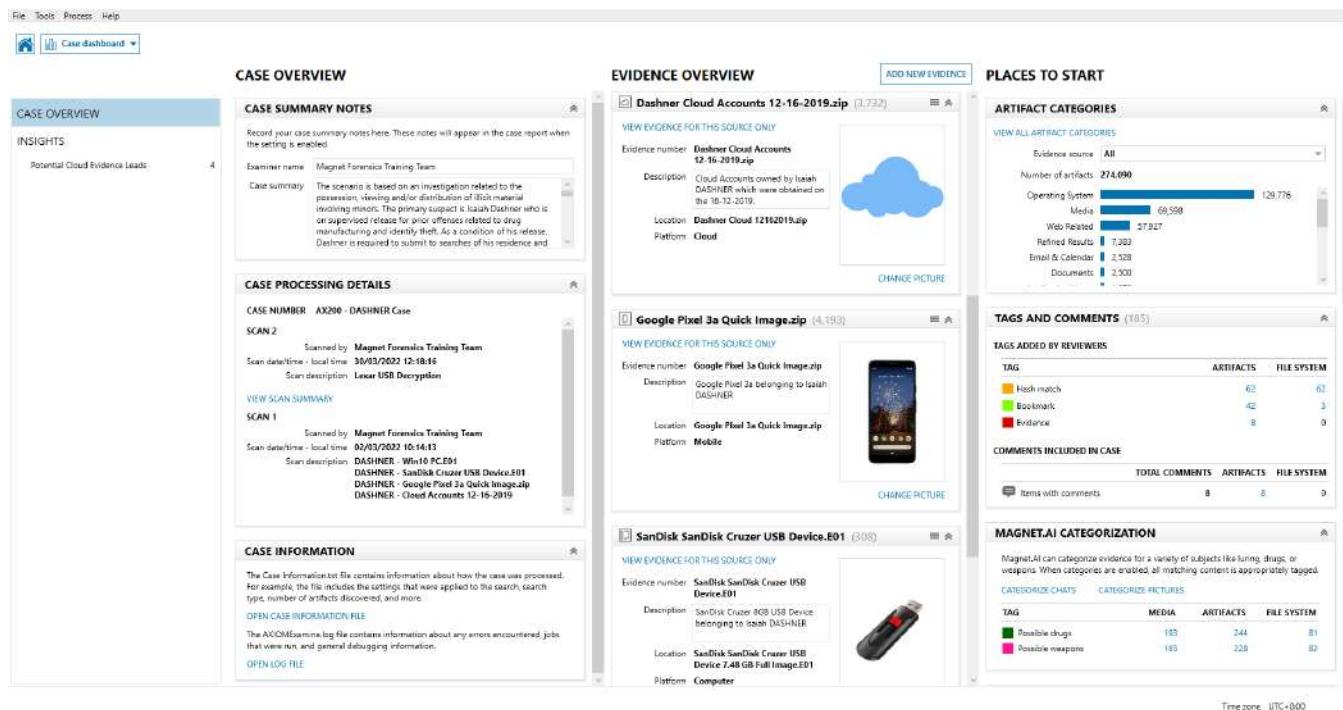


Figure 2.46 Case Dashboard

The INSIGHTS and POTENTIAL CLOUD EVIDENCE LEADS shown in Figure 2.47 was introduced in version 6.0 and allows users to take a deeper look into Cloud accounts and details, including passwords and tokens associated to an account within your evidence set. Examiners can also acquire cloud accounts based on the password and tokens.



Module 2 – Evidence Processing and Case Creation

The screenshot shows the 'POTENTIAL CLOUD EVIDENCE LEADS (4)' section. It lists four accounts: 'isaiyah.dashner@gmail.com' (Dropbox account), 'isaiyah.dashner@gmail.com' (Facebook account), 'isaiyah.dashner@gmail.com' (Google account), and 'isaiyah.dashner@gmail.com' (Microsoft account). The 'isaiyah.dashner@gmail.com' (Dropbox account) entry is expanded, showing 'ACCOUNT DETAILS' with a note about recovering the account from evidence, and 'ACCESS METHODS' which includes a 'User account' option. The 'POTENTIAL ARTIFACTS' section lists 'Cloud Dropbox Files'.

Figure 2.47 Cloud Insights Dashboard

The CASE OVERVIEW includes a CASE SUMMARY NOTES section where the examiner can add a case summary and any relevant case information. It can also be used to record case notes as the need arises, such as recording any relevant comments made by the suspect or recording any significant artifacts located during the examination. The case summary could also be used to record what investigations have been completed and what is left to review, or record if any examiners collaborating on the case have been provided with a portable case.

The screenshot shows the 'CASE SUMMARY NOTES' section. It contains a text area for 'Case summary' with the word 'de' typed into it. There are also fields for 'Examiner name' (set to 'Magnet Forensics') and 'Case summary'.

Figure 2.48 Case summary notes within the Case Overview

The CASE PROCESSING DETAILS section contains the following information: CASE NUMBER; Scanned by; Scan description and Scan date, of each AXIOM Process scan that has been carried out.



The CASE INFORMATION section contains two links to [OPEN CASE INFORMATION FILE](#) and [OPEN LOG FILE](#). The case information file includes information about how the case was processed such as the AXIOM Process settings and which artifacts were searched for. The log file includes information such as any errors encountered.

CASE INFORMATION

The Case Information.txt file contains information about how the case was processed. For example, the file includes the settings that were applied to the search, search type, number of artifacts discovered, and more.

[OPEN CASE INFORMATION FILE](#)

The AXIOMEExamine.log file contains information about any errors encountered, jobs that were run, and general debugging information.

[OPEN LOG FILE](#)

Figure 2.49 Case information within Case Overview

The EVIDENCE OVERVIEW lists each of the evidence items added to the case. The LOCATION details the name of the evidence item added to the case, and the Evidence number also displays the name of the evidence item unless it was changed by the examiner at the time of processing. The examiner has the option to add a Description and upload a picture for each individual item if desired. Within each entry is a link [VIEW EVIDENCE FOR THIS SOURCE ONLY](#). Selecting this link will cause AXIOM Examine to switch to the Artifact explorer and automatically apply a filter to display only artifacts sourced from that evidence item.

Dashner Win10 PC.E01 (248,692)

[VIEW EVIDENCE FOR THIS SOURCE ONLY](#)

Evidence number **Dashner Win10 PC.E01**

Description

Location **Dashner Win10 PC.E01**

Platform **Computer**

No picture added

[CHANGE PICTURE](#)

Figure 2.50 Evidence overview within Case Dashboard

The PLACES TO START displays a summary of key aspects of the case that could be of importance to the examiner. By default, any sections of the PLACES TO START that contain information will be expanded and any sections containing no information will be collapsed.



Module 2 – Evidence Processing and Case Creation

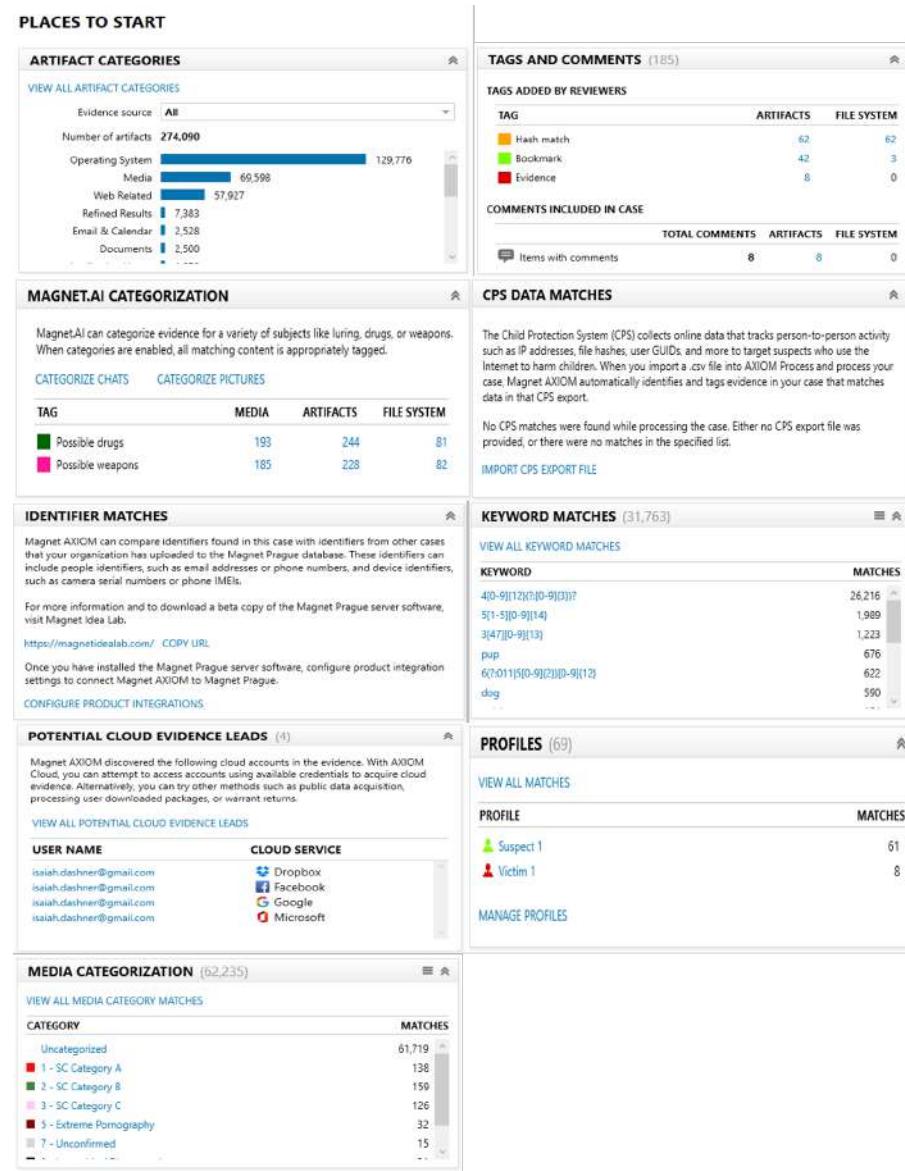


Figure 2.51 Places to Start within Case Dashboard view

The first section of PLACES TO START is the ARTIFACT CATEGORIES. This displays a histogram view of the recovered artifacts in the case. It displays each of the parent categories and details how many artifacts were recovered. Clicking any of the histogram bars automatically switches AXIOM Examine to the Artifact explorer with that category selected in the NAVIGATION pane. The Evidence Source drop-down within the ARTIFACT CATEGORIES section can be used to filter the results displayed in this window to just the artifacts from a specific evidence item.

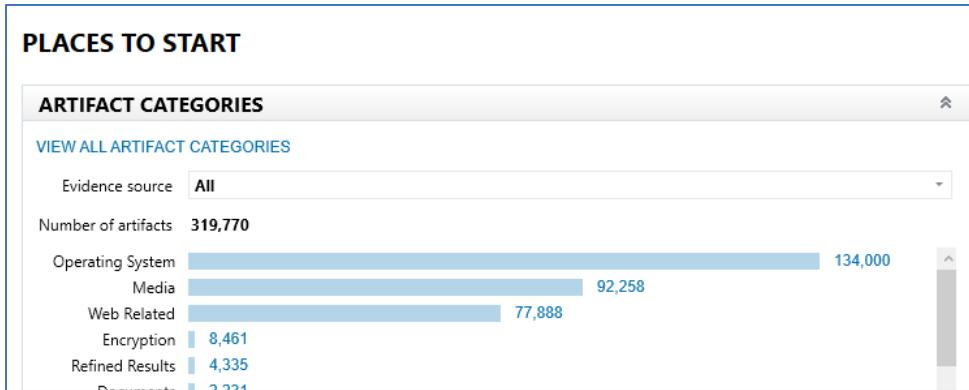


Figure 2.52 Case Dashboard Artifact Categories

The next section of PLACES TO START is the TAGS AND COMMENTS. Unless AXIOM Process identified any files with hashes matching those added in the TAG FILES WITH MATCHING HASH VALUES section, this window will be blank when a case is first opened. Once the examiner starts adding tags to items in the case, the content of this window displays how many total items have been tagged in both the artifact and file system explorers. Clicking the link automatically switches AXIOM Examine to the Artifact or File system explorer and applies the Tags and comments filter to display the files/items with that tag applied. In addition to the tags applied to items in the case, this section details how many items have comments, and again, clicking the link automatically switches AXIOM Examine to the Artifact or File system explorer with the Tags and comments filter applied.

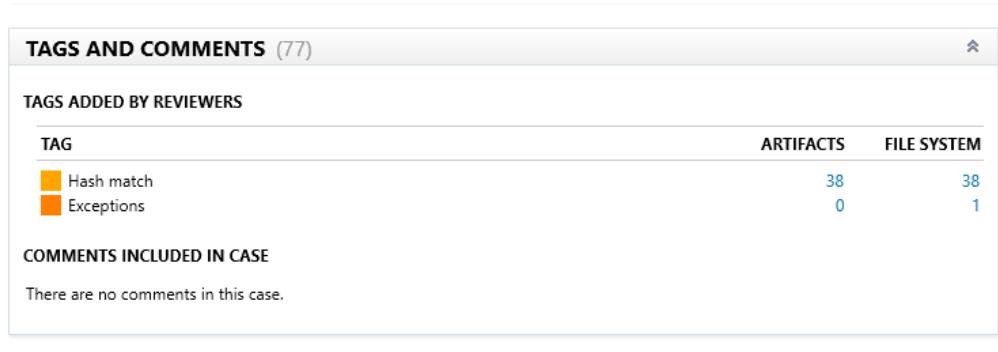


Figure 2.53 Case Dashboard Tags and Comments

The MAGNET.AI CATEGORIZATION section contains a link to start the chat and picture categorization utilizing AXIOM's artificial intelligence module – Magnet.AI. Any chats and pictures detected that match the built-in models will have the appropriate tags applied and the tag displayed in this section.

NOTE: Selecting to categorize pictures takes time. Each selected picture must be individually examined using Magnet.AI to determine if it contains any of the markers described in the categories.

The CHILD PROTECTIVE SERVICES (CPS) section offers the examiner to import data and track person-person activity of which, AXIOM will tag these items for the examiner to review.



IDENTIFIERS allow the examiner to compare identifiers such as names, email addresses, mobile phone numbers and device identifiers like serial numbers between multiple cases that have been updated and integrated to Magnet PRAGUE software.

KEYWORD MATCHES are only populated if there were hits for keywords added in the ADD KEYWORDS TO SEARCH section during processing. Clicking the link next to a KEYWORD automatically switches AXIOM Examine to the Artifact explorer with the Keyword lists filter applied.

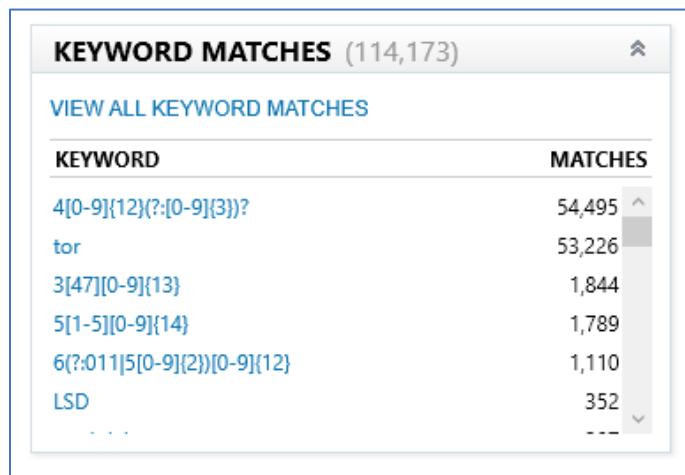


Figure 2.54 Keyword Matches within Case Dashboard

POTENTIAL CLOUD LEADS will identify cloud accounts within the evidence set that has been processed, clicking the cloud account depicted will automatically switch into the CLOUD INSIGHTS DASHBOARD (shown on [Figure 2.47](#)).

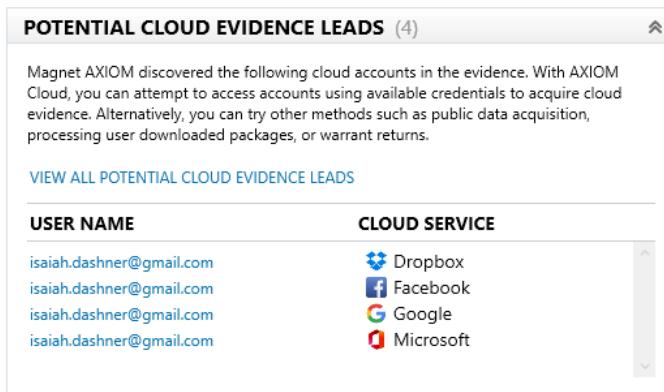


Figure 2.55 Potential Cloud Leads

If during processing the hash of any media files matched one listed in the CATEGORIZE PICTURES AND VIDEOS section, it is automatically categorized, and the categories are listed in the MEDIA CATEGORIES section. Selecting the link for a media category automatically switches AXIOM Examine to the Artifact explorer with the Media categories filter applied. Alternatively, the option to [VIEW ALL MEDIA CATEGORY MATCHES](#) can be selected.

MEDIA CATEGORIES (35)	
VIEW ALL MEDIA CATEGORY MATCHES	
CATEGORY	MATCHES
-1	31
Hash match	4

Figure 2.56 Media Categories within the Case Dashboard

The PROFILES section displays any Identifier profiles created within the case (profiles will be covered in a later lesson). Selecting the profile automatically switches AXIOM Examine to the Artifact explorer with the Profiles filter applied.

PROFILES (52)	
VIEW ALL PROFILES	
PROFILE	MATCHES
 Dashner	52

Figure 2.57 Profiles view within Case Dashboard

The content of these sections will evolve and reflect the case as it is worked and analyzed. The Case dashboard is meant to be a command center for the case and should be used throughout the entire case process from beginning to reporting.



ARTIFACT EXPLORER

The Artifacts explorer provides a tabular view of the artifacts identified during processing.

Figure 2.58 Artifacts explorer

On the left of the Artifacts explorer is the NAVIGATION pane, as shown in Figure 2.59 below. It lists the categories of artifacts found within the case, along with a count of the number of artifacts within that category. Axiom Examine does not display an artifact category if no artifacts of that type were found within the case. Therefore, you will never see a category with a zero count.

ALL EVIDENCE	230,481
REFINED RESULTS	3,362
█ Classified URLs	1,402
█ Cloud Services URLs	193
█ Facebook URLs	290
█ Google Analytics First Visit Cookies	7
█ Google Analytics Referral Cookies	7
█ Google Analytics Session Cookies	6
█ Google Searches	183
█ Identifiers	597
█ Locally Accessed Files and Folders	290
█ Malware/Phishing URLs	7
█ Parsed Search Queries	45
█ Passwords and Tokens	3
█ Rebuilt Webpages	223
█ Social Media URLs	108
█ Tax Site URLs	1
WEB RELATED	50,346

Figure 2.59 Navigation pane

In the center of the Artifacts explorer is the EVIDENCE pane, as shown in Figure 2.58. It displays the artifacts contained within the category highlighted in the NAVIGATION pane. How the data contained within the EVIDENCE pane is displayed is dictated by the View selected (the different views will be covered in later lessons) at the top-right of the EVIDENCE pane. By default, the EVIDENCE pane displays artifacts in COLUMNS VIEW which displays the data in a tabular list. The columns within the table display the fields of information extracted for each artifact.

To widen a column, simply drag the bar between the columns in the title row. To sort the content of a column, click the column title. Click the column title again to reverse sort the content. To hide a column, right-click the column title and select Hide column. To display the hidden columns again, right-click on any column title and select Show all columns. Column order can be changed via drag-and-drop on the column title.

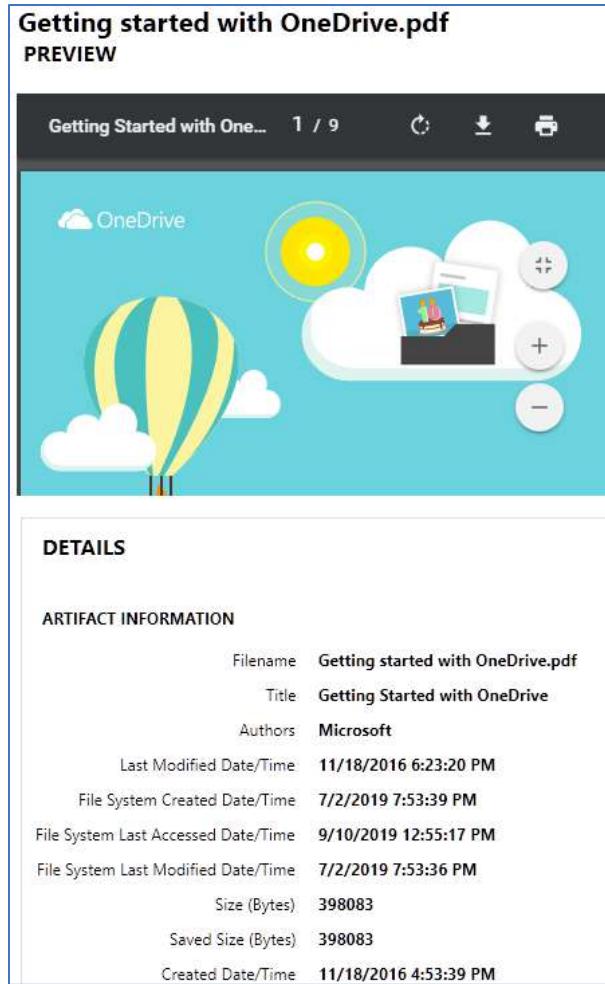
Users can right-click on the scroll bar in the EVIDENCE pane to easily navigate through large rows of data.



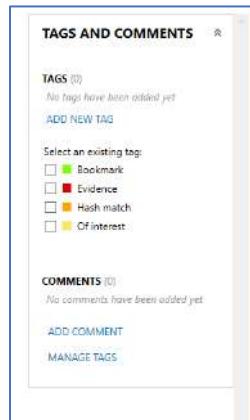
EVIDENCE (45)						
Search Term	URL	Date/Time	Date...	Searcher	Go	Column view +
how to find my windows product key site:microsoft...	https://www.bing.com/search?q=how%20to%20find...	7/3/2019 10:32:53 PM		Bing		
how to find my windows product key site:microsoft...	https://www.bing.com/search?q=how%20to%20find...	7/3/2019 10:32:53 PM		Bing		
gmx mail	https://www.bing.com/search?q=gmx+mail&form=...	8/29/2019 7:25:23 PM		Bing		
gmx mail	https://www.bing.com/search?q=gmx+mail&form=...	8/29/2019 7:25:24 PM		Bing		
gmx mail	https://www.bing.com/search?q=gmx+mail&form=...	8/29/2019 7:25:24 PM		Bing		
office 365 login	https://www.bing.com/search?q=office-365-login&...	8/30/2019 3:32:21 PM		Bing		
office 365 login	https://www.bing.com/search?q=office-365-login&...	8/30/2019 3:32:21 PM		Bing		
office 365 login	https://www.bing.com/search?q=office-365-login&...	8/30/2019 3:32:21 PM		Bing		
microsoft office download	https://www.bing.com/search?q=microsoft-office+...	8/30/2019 3:35:33 PM		Bing		
microsoft office download	https://www.bing.com/search?q=microsoft-office+...	8/30/2019 3:35:33 PM		Bing		
microsoft office download	https://www.bing.com/search?q=microsoft-office+...	8/30/2019 3:35:33 PM		Bing		
ebay	https://www.bing.com/search?q=ebay&form=EDGT...	8/30/2019 4:02:19 PM		Bing		
ebay	https://www.bing.com/search?q=ebay&form=EDGT...	8/30/2019 4:02:19 PM		Bing		
ebay	https://www.bing.com/search?q=ebay&form=EDGT...	8/30/2019 4:02:19 PM		Bing		
55829330959460	https://www.facebook.com/r/r.php?r=5582933095...	9/10/2019 8:27:13 PM		Facebook		
1531105787105294	https://www.facebook.com/r/b.php?p=1531105787...	9/11/2019 5:33:47 PM		Facebook		
paint	https://www.bing.com/search?q=paint&form=WMS...	12/18/2019 7:09:11 PM		Bing		
paint	https://www.bing.com/search?q=paint&form=WMS...	12/18/2019 7:09:11 PM		Bing		
paint	https://www.bing.com/search?q=paint&form=WMS...	12/18/2019 7:09:11 PM		Bing		
paint	https://www.bing.com/search?q=paint&form=WNS...	12/18/2019 7:09:19 PM		Bing		

Figure 2.60 Evidence pane

To the right of the Artifacts explorer is the DETAILS pane, as shown in Figure 2.58. It displays the details of the artifact currently highlighted in the EVIDENCE pane. This makes it easier to view the information relating to the artifact if the content of a field is extensive, e.g. the Source path. Each section of the DETAILS pane is a Card, and in Figure 2.61, the DETAILS pane includes a PREVIEW card displaying a preview of the artifact or file, and a DETAILS card displaying the artifact information.

*Figure 2.61 Details pane*

To the far right of the Artifacts explorer is a further pane, the TAGS, PROFILES & MEDIA CATEGORIES pane. By default, it is collapsed against the side bar out of view. To display this pane, click the words TAGS, PROFILES & MEDIA CATEGORIES.

*Figure 2.62 Tags, Profiles & Media Categories pane*

With the exception of the EVIDENCE pane, each of the panes has a double arrow icon in the top corner, as highlighted in Figure 2.63.

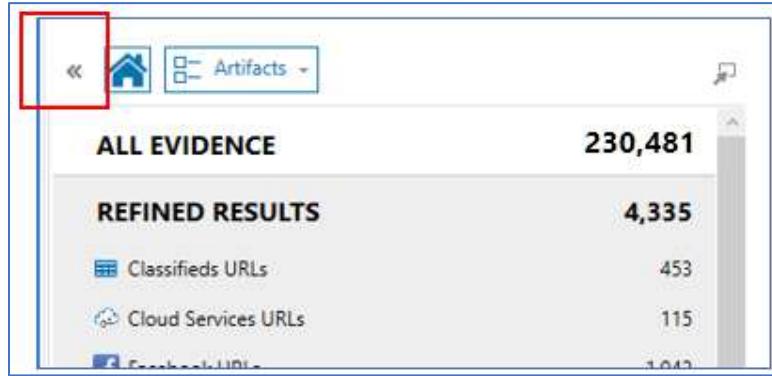


Figure 2.63 Collapse pane icon

Clicking the icon collapses the pane against the side bar allowing more space within the user interface for the EVIDENCE pane.

The screenshot shows the Magnet AXIOM interface with multiple panes collapsed on the side to expand the Evidence pane. The Evidence pane is now fully visible and expanded, displaying a large table of evidence items. The table has columns for Search Term, URL, Date/Time, Date..., Original Search Qu..., Search Sessi..., Web Page Title, Prev..., Artifact, and Artif... (partially visible). The table contains numerous rows of data, mostly related to Google searches for terms like '7zip', 'windows computer cleaner', 'cute puppy wallpaper', and 'soviet union trade with pepsi'. The right side of the interface shows collapsed panes for Tags, Profiles & Media Categories, and Details.

EVIDENCE (183)											
	Search Term	URL	Date/Time	Date...	Original Search Qu...	Search Sessi...	Web Page Title	Prev...	Artifact	Artif...	
7zip	https://www.google.com/search?q=7zip&oq=7zip&	6/30/2019 9:30:10 PM	7zip			T7zip - Google Search		WebKit Browser Web History (Carved)	183895		
windows computer cleaner	https://www.google.com/search?q=windows+computer+cleaner	8/29/2019 7:14:33 PM	windows computer cleaner			windows computer cleaner - Google Search		WebKit Browser Session/Tabs (Carved)	183895		
windows computer cleaner	https://www.google.com/search?q=windows+computer+cleaner	8/29/2019 7:14:33 PM	windows computer cleaner			windows computer cleaner - Google Search		Potential Browser Activity	183901		
windows computer cleaner	https://www.google.com/search?q=windows+computer+cleaner	8/29/2019 7:14:33 PM	windows computer cleaner			windows computer cleaner - Google Search		WebKit Browser Session/Tabs (Carved)	183903		
windows computer cleaner	https://www.google.com/search?q=windows+computer+cleaner	8/29/2019 7:14:33 PM	windows computer cleaner			windows computer cleaner - Google Search		Potential Browser Activity	183975		
cute puppy wallpaper	https://www.google.com/search?q=cute+puppy+wallpaper		cute puppy wallpaper			cute puppy wallpaper - Google Search		Chrome Favourites	184135		
cute puppy wallpaper	https://www.google.com/search?q=cute+puppy+wallpaper		cute puppy wallpaper			cute puppy wallpaper - Google Search		Chrome Favourites	184136		
soviet union trade with pepsi	https://www.google.com/search?q=soviet+union+tr...		soviet union trade with p...			soviet union trade with p...		Chrome Favourites	184238		
soviet union trade with pepsi	https://www.google.com/search?q=soviet+union+tr...		soviet union trade with p...			soviet union trade with p...		Chrome Favourites	184240		
cute puppy wallpaper	https://www.google.com/search?q=cute+puppy+wallpaper	10/31/2019 4:06:38...	cute puppy wallpaper			cute puppy wallpaper - Google Search		Chrome Web Visits	184255		
cute puppy wallpaper	https://www.google.com/search?q=cute+puppy+wallpaper	10/31/2019 4:06:39...	cute puppy wallpaper			cute puppy wallpaper - Google Search		Chrome Web Visits	184256		
cute puppy wallpaper	https://www.google.com/search?q=cute+puppy+wallpaper	10/31/2019 4:06:40...	cute puppy wallpaper			cute puppy wallpaper - Google Search		Chrome Web Visits	184258		
soviet union trade with pepsi	https://www.google.com/search?q=soviet+union+tr...	10/31/2019 4:12:24...	soviet union trade with p...			soviet union trade with pepsi - Google Search		Chrome Web Visits	184264		
soviet union trade with pepsi	https://www.google.com/search?q=soviet+union+tr...	10/31/2019 4:12:25...	soviet union trade with p...			soviet union trade with pepsi - Google Search		Chrome Web Visits	184265		
soviet union trade with pepsi	https://www.google.com/search?q=soviet+union+tr...	10/31/2019 4:12:25...	soviet union trade with p...			soviet union trade with pepsi - Google Search		Chrome Web Visits	184267		
cute puppy wallpaper	https://www.google.com/search?q=cute+puppy+wallpaper	10/31/2019 4:08:40...	cute puppy wallpaper			cute puppy wallpaper - Google Search		Chrome Web History	184269		
soviet union trade with pepsi	https://www.google.com/search?q=soviet+union+tr...	10/21/2019 4:12:25...	soviet union trade with p...			soviet union trade with pepsi - Google Search		Chrome Web History	184285		
cute puppy wallpaper	https://www.google.com/search?q=cute+puppy+wallpaper		cute puppy wallpaper			cute puppy wallpaper - Google Search		Chrome Keyword Search Terms	184289		
soviet union trade with pepsi	https://www.google.com/search?q=soviet+union+tr...		soviet union trade with p...			soviet union trade with pepsi - Google Search		Chrome Keyword Search Terms	184291		
cute puppy wallpaper	https://www.google.com/search?q=cute+puppy+wallpaper	10/31/2019 4:09:28...	cute puppy wallpaper			cute puppy wallpaper - Google Search		Chrome Shortcuts	184298		
soviet union trade with pepsi	https://www.google.com/search?q=soviet+union+tr...	10/31/2019 4:12:24...	soviet union trade with p...			soviet union trade with pepsi - Google Search		Chrome Shortcuts	184370		
pandora	https://www.google.com/search?q=pandora+lp&ie=...	8/29/2019 6:04:40 PM	pend			pandora - Google Search		Firefox Web Visits	185568		

Figure 2.64 Multiple panes collapsed on the side to expand the Evidence pane



At the top of the Artifacts explorer is the FILTERS bar. It is used to filter and search the artifacts being displayed.

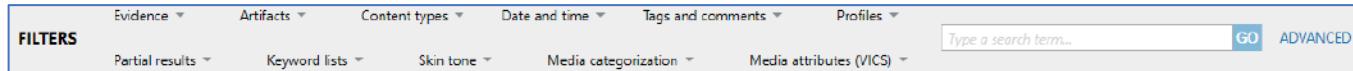


Figure 2.65 Filters bar

Applying any filter within AXIOM Examine turns the FILTERS bar yellow, as shown in Figure 2.66, to alert the examiner that not all artifacts are in view. The filtered criteria are displayed in bold. Hovering over the bold filter criteria will allow viewing the complete name of the filter.

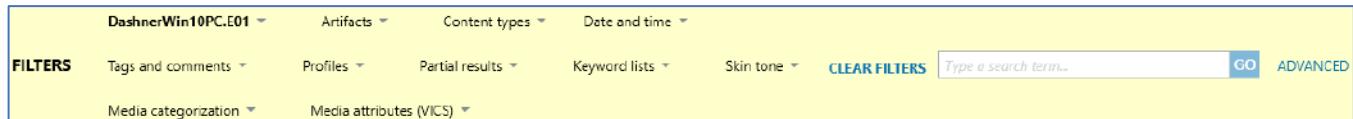


Figure 2.66 Filters bar with active filter in place



Notes



Notes

Notes





MODULE 3:

Operating System (Part 1)

LEARNING OBJECTIVES

In this lesson, students will take part in a lecture, hands-on exercises, instructor led exercises, and student practical exercises to gain an understanding of Magnet AXIOM's capability to recover artifacts from the File System and Registry of a computer running a Windows operating system. The computer artifact analysis section of this course is composed of several modules, each of which focuses on a specific set of key artifacts, which are commonly encountered during the analysis of the Windows Registry. Artifacts which reside in the Operating System category will be validated through use of the Registry Explorer. This lesson will also explore the tracking of USB devices, File System Information, Timezone Information, and User Accounts.

GOALS

At the conclusion of this lesson, students will be able to use Magnet AXIOM to conduct examinations of computers using the Windows Operating System to search for, recover, and tag key artifacts.

OS ARTIFACTS – PERSONAL COMPUTERS (PCS)

Operating system artifacts, from either PCs or mobile devices, can represent some of the most valuable evidentiary “puzzle pieces” available to an examiner when trying to rebuild a picture of device and user behavior. This category covers a wide range of behavioral artifacts and can include detailed information about software installations, network connections, file access, USB connections, changes to user accounts, and system settings - just to name a few. It is always beneficial for the examiner to include an analysis of operating system artifacts. Operating system artifacts are often generated automatically by the host system with little or no direct user control. In addition, the locations for most of the system files which track the activities are either unknown to the user or difficult to disable without the proper software or a deeper understanding of the operating system. Therefore, system level artifacts are not easily hidden or removed by the user in most cases.

As many of these operating system artifacts are created and updated through a user's normal interaction with the system, including its installed programs and files, their presence is expected. If an examiner finds these expected artifacts are not present on a piece of evidence, this can be an indicator that steps have been taken by a user to delete, or otherwise alter, this information. Third-party tools and native operating system functions are available which could be utilized to help a user hide traces of nefarious activity. Ironically, even if a user is successful in destroying a system level artifact, the operating system stores records of the software used to delete the artifact and the user who executed it. This information can be recovered in areas such as the Windows Event Logs and the Windows Registry.

In AXIOM Process, under the Computer Artifacts section, the user can select which operating system artifacts to recover and what options to use during processing. By default, AXIOM will attempt to recover specific operating system artifacts from a Windows or Mac evidence source. The examiner should review the OPERATING SYSTEM artifacts during case processing. Windows Event Logs are an extremely valuable resource for the examiner, and their inclusion can add hundreds of thousands of artifacts to the case but can increase the time it takes to load and process the case. Once the Event Logs are recovered, the searching and filtering capabilities of AXIOM Examine make analyzing the Windows Event Logs easily manageable. The increased processing time is worthwhile if searching Windows Event Logs is going to a part of your analysis.



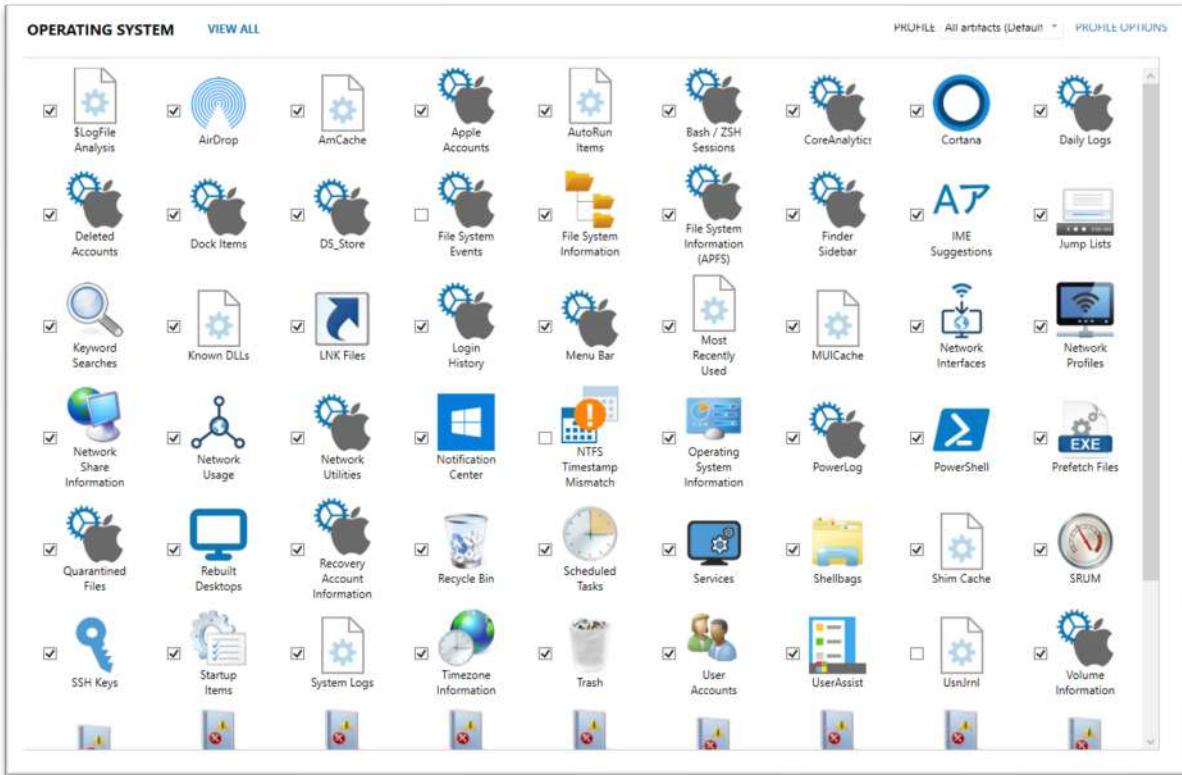


Figure 3.1 OPERATING SYSTEM ARTIFACT VIEW FROM MAGNET AXIOM PROCESS

On a computer running the Windows operating system, artifacts can be recovered from the Windows folder structure, the user profile folder structure, the Windows Registry, a restore point, the System Volume Information folder, or unallocated space. As with all artifacts in AXIOM, if an individual operating system artifact was not identified by AXIOM Process, then an empty category will not be displayed in Examine.

OPERATING SYSTEM	129,663		
\$LogFile Analysis	6,144	Scheduled Tasks	192
Accounts Information	7	Shellbags	57
AmCache Device Containers	13	Shim Cache	661
AmCache Driver Binaries	356	SRUM Application Resource Usage	4,873
AmCache File Entries	306	SRUM Energy Usage	62
AmCache Pnp Devices	74	SRUM Energy Usage (Long Term)	2
AmCache Program Entries	97	SRUM Network Connections	40
AmCache Shortcuts	94	SRUM Network Usage	895
Android Downloads	2	SRUM Push Notification Data	46
AutoRun Items	350	Startup Items	4
Cloud Accounts Information	7	System Services	598
File Associations	1,433	Timezone Information	1
File System Information	5	User Accounts	8
Jump Lists	225	UserAssist	93
Known DLLs	32	Windows Event Logs	108,568
LNK Files	753	Windows Event Logs - Firewall Events	865
MRU Folder Access	14	Windows Event Logs - Script Events	35
MRU Opened/Saved Files	55	Windows Event Logs - Service Events	304
MRU Recent Files & Folders	182	Windows Event Logs - System Events	24
MUICache	62	Windows Event Logs - User Events	1,759
Network Interfaces (Registry)	2	Windows Event Logs - User PNP Events	12
Network Profiles	1	Windows Notification Center	18
Operating System Information	1	Windows Timeline Activity	50
Prefetch Files - Windows 8/10	273		
Recycle Bin	8		

Figure 3.2 Windows OS Artifact Categories

WINDOWS REGISTRY

At the heart of most of the Operating System artifacts in AXIOM are the Windows Registry files. Microsoft defines its registry as “a hierarchical database that stores configuration information.” This registry contains profiles for each user of the computer, information about system hardware, installed programs, and property settings. Windows continually references this information during its operations. Unfortunately, even though the Windows Registry files contain some of the most valuable artifacts for an examiner, they are often not explored as a forensic resource. This can be due to a lack of understanding of their value or the inability of a forensic tool to access and analyze the registry files. AXIOM provides a solution to both challenges.



During the creation of the case within AXIOM Process, Windows registry files such as the **SAM**, **SECURITY**, **SOFTWARE**, and **SYSTEM** global hives are recovered from the **WINDOWS\System32\config** and the **Windows.Old** folders. Individual Windows user account registry hives such as **NTUSER.DAT** and **UsrClass.dat** are recovered from the user's profile folder, restore points, and volume shadow copies. Artifacts parsed from the registry hives are stored within the OPERATING SYSTEM category of AXIOM Examine. For examiners who are relatively new to the exploration of the Windows Registry files, and the data they contain, the Artifacts explorer within AXIOM Examine provides an intuitive and easily understood view of the data in both the EVIDENCE and DETAILS panes. To further their understanding of the source of the registry artifacts, examiners can follow the **LOCATION** hyperlinks in the ARTIFACT INFORMATION sections of the DETAILS pane. AXIOM Examine will automatically switch to the Registry explorer and allow the examiner to explore the associated hive and its key, sub-keys and values structures of the source registry files. For examiners who are more familiar with the Windows Registry, the Registry explorer in AXIOM Examine allows for a much deeper dive into the source hives, keys, sub-keys, and values that the artifact was populated from. In addition, the Registry explorer of AXIOM Examine allows the examiner to create user defined artifacts for a given value's data that is displayed in the HEX card view of the DETAILS pane. For example, using the Registry explorer in AXIOM Examine, an individual user defined artifact can be created and tagged for data within a specific value. The user defined registry artifact can be used for adding emphasis to a relevant artifact not automatically recovered by AXIOM.

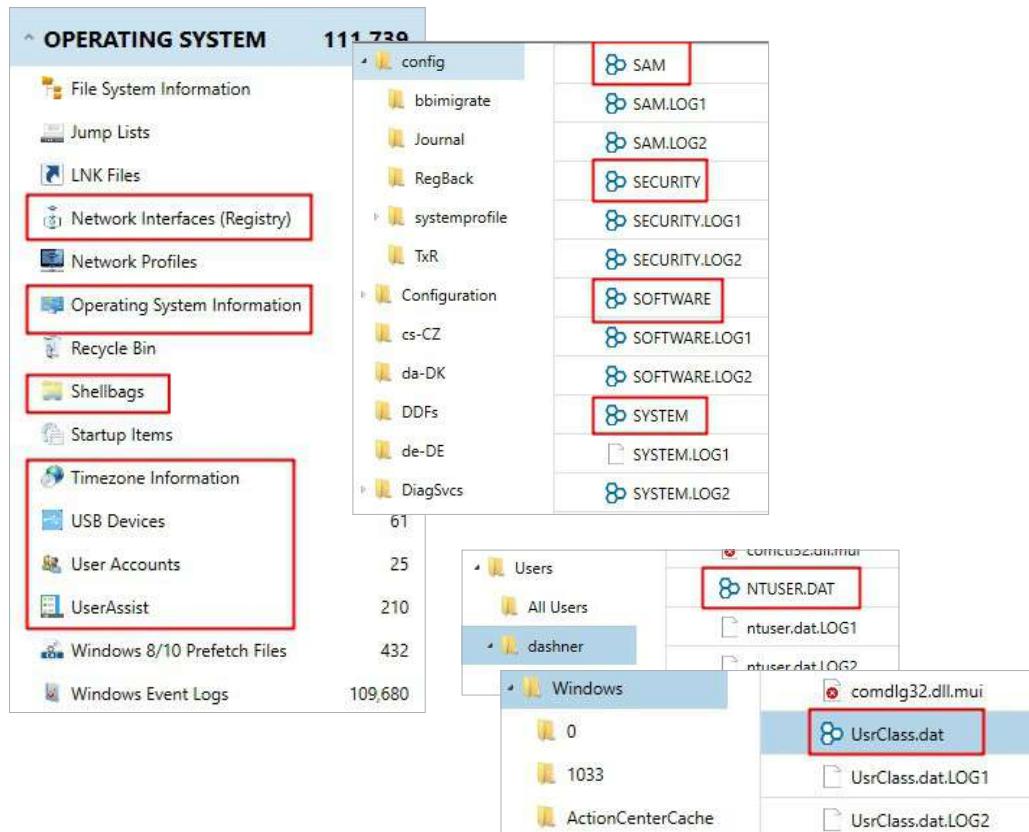


Figure 3.3 REGISTRY HIVES LOCATED IN WINDOWS OPERATING SYSTEM

Given the wide variety of operating system artifacts which can potentially be available in the Windows Registry and the depth in which each registry file can be explored, this module alone could encompass a week-long course. In the interest of time, this module will focus on some of the key OPERATING SYSTEM categories from the registry and other system-level files to illustrate the importance of operating system artifacts.

FILE SYSTEM INFORMATION

The File System Information artifact is a system level artifact, parsed from the Boot Record of the drive that was processed in AXIOM. The Volume Offset (Bytes) value can help the examiner determine if the artifact is from the Master Boot Record (MBR) or Volume Boot Record (VBR). The File System Information artifact provides technical information about the drive that was examined, including drive geometry, reported file system, volume serial number (VSN), and if the drive was fixed or removable.

EVIDENCE (4)						
Id	Volu...	Full Volume...	File Syst...	Sect...	Byte...	
S-1-5-21-3467557965-783750317-3214423210	B8B9-2072	34B8B95FB8B92072	Microsoft NTFS	8	512	
ARTIFACT INFORMATION						
Id	S-1-5-21-3467557965-783750317-3214423210					
Volume Serial Number	B8B9-2072					
Full Volume Serial Number	34B8B95FB8B92072					
File System	Microsoft NTFS					
Sectors per cluster	8					
Bytes per sector	512					
Total Sectors	103667711					
Total Capacity (Bytes)	53077864448					
Total Clusters	12958463					
Unallocated Area (Bytes)	30507716608					
Free Clusters	7448173					
Allocated Area (Bytes)	22570147840					
Volume Offset (Bytes)	608174080					
Drive Type	Fixed					

Figure 3.4 File system information about the main partition



OPERATING SYSTEM INFORMATION

Operating System Information				
EVIDENCE (1)				
Operating System	Version Number	Installed/Updated Date/Time	Product Key	
Windows 10 Pro (1903)	6.3	7/2/2019 7:39:35 PM	YGRNH-G8MJC-KKVV...	
EVIDENCE INFORMATION				
Source	Dashner Win10 PC.E01 - Partition 2 (Microsoft NTFS, 49.43 GB)\Windows\System32\config\SOFTWARE			
Recovery Method	Parsing			
Deleted source				
Location	Microsoft\Windows NT\CurrentVersion			
Evidence number	Dashner Win10 PC.E01			
EVIDENCE INFORMATION				
Source	Dashner Win10 PC.E01 - Partition 2 (Microsoft NTFS, 49.43 GB)\Windows\System32\config\SYSTEM			
Recovery Method	Parsing			
Deleted source				
Location	ControlSet001\Control\Windows			

Figure 3.5 OPERATING SYSTEM INFORMATION FROM THE SOFTWARE AND SYSTEM HIVES

The information parsed from the **SYSTEM** and **SOFTWARE** registry files, which compose the Operating System Information artifact, can provide valuable insight for the examiner. The version of the operating system installed can help the examiner identify the capabilities of the system being analyzed.

For example, if the OS is a Pro version, rather than a Home version, then the examiner may have to contend with BitLocker encryption. The build number of the operating system will tell the examiner if specific artifacts should exist on the computer media. For instance, in Build Number 1803, Microsoft introduced a timeline feature. By pressing the Windows+Tab keys at the same time prior to build number 1803, the open tiles in Windows will cascade on the screen. After the release of build number 1803, pressing Windows+Tab produces a timeline of activity by the user. Knowing the build number could explain why certain artifacts are or are not present on a given computer system.

In addition, the computer name value can be useful when examining the Windows Event Log artifacts and identifying activities associated with the host system performed by the user.

Information Parsed from SOFTWARE	
Information Parsed from SYSTEM	
ARTIFACT INFORMATION	
Operating System	Windows 10 Pro (1903)
Version Number	6.3
Installed/Updated Date/Time	7/2/2019 7:39:35 PM
Product Key	YGRNH-G8MJC-KKVW3-GGB9X-KQBP2
Owner	isaiah.dashner@gmail.com
Displayed Computer Name	DESKTOP-J37CE8J
Computer Name	DESKTOP-J37CE8J
DHCP Server	
Operating System Version	Professional
Build Number	18362
Product ID	00330-51276-65940-AAOEM
Last Shutdown Date/Time	10/8/2019 7:51:40 PM
System Root	C:\WINDOWS
Path	C:\WINDOWS
Last Access Time Enabled	No

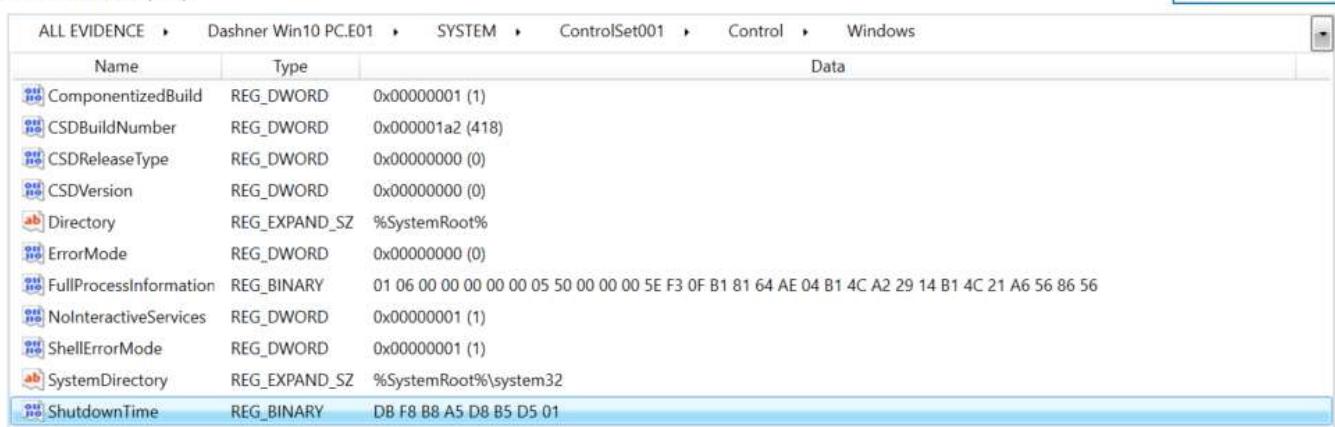
Figure 3.6 OPERATING SYSTEM ARTIFACT INFORMATION

Using Source Linking from the DETAILS card, examiners can view the values stored in the SOFTWARE\Microsoft\Windows NT\CurrentVersion key. AXIOM parses the following values displayed in the EVIDENCE and DETAILS panes from this key: version number, build number, installation date and time, digital product key information, installation path, product name, and registered owner for the operating system.

Within the SYSTEM hive, AXIOM parses the data from the ShutdownTime value, which is stored as an 8-byte Windows timestamp value, and converts the hexadecimal value to a human readable date and time which is shown as the Last Shutdown Date/Time field of the DETAILS pane, as seen in Figure 3.6.

To validate what AXIOM is interpreting for us, we can use Source Linking to review the registry location and see the registry information in hexadecimal. If you want to utilize the built-in functionality of AXIOM, you can highlight those 8 bytes and then scroll down to the DECODE card below the HEX card and look at the windows date and time LE (LittleEndian). Alternatively, we can use the Timestamp Converter program which will be introduced in a later module to decode the hex value of \x4A \xF0 \xBE \xCD \x11 \x7E \xD5 \x01. As you can see in the figure below, the Decode Format needs to be Windows 64-bit Hex value and the time decoded matches the figure below as interpreted by Magnet AXIOM.



EVIDENCE (11)


The screenshot shows a hierarchical registry path: ALL EVIDENCE > Dashner Win10 PC.E01 > SYSTEM > ControlSet001 > Control > Windows. The 'ShutdownTime' key is selected, and its value data is displayed in hexadecimal format as DB F8 B8 A5 D8 B5 D5 01. The table has columns for Name, Type, and Data.

Name	Type	Data
ComponentizedBuild	REG_DWORD	0x00000001 (1)
CSDBuildNumber	REG_DWORD	0x000001a2 (418)
CSDReleaseType	REG_DWORD	0x00000000 (0)
CSDVersion	REG_DWORD	0x00000000 (0)
Directory	REG_EXPAND_SZ	%SystemRoot%
ErrorMode	REG_DWORD	0x00000000 (0)
FullProcessInformation	REG_BINARY	01 06 00 00 00 00 05 50 00 00 00 05 F3 OF B1 81 64 AE 04 B1 4C A2 29 14 B1 4C 21 A6 56 86 56
NoInteractiveServices	REG_DWORD	0x00000001 (1)
ShellErrorMode	REG_DWORD	0x00000001 (1)
SystemDirectory	REG_EXPAND_SZ	%SystemRoot%\system32
ShutdownTime	REG_BINARY	DB F8 B8 A5 D8 B5 D5 01

Figure 3.7 Registry view of ShutdownTime, displayed as hexadecimal data

TIMEZONE INFORMATION

Following the SOFTWARE\Microsoft\Windows NT\CurrentVersion\TimeZones key will link to the SOFTWARE registry file. This key stores the data AXIOM parses in the Display field of the EVIDENCE and DETAILS panes of AXIOM Examine.

ARTIFACT INFORMATION

Standard Timezone Name	Central Standard Time
Current Timezone Offset (Minutes)	-360
Daylight Timezone Name	Central Daylight Time
Daylight Timezone Offset (Minutes)	-300
Daylight Timezone Start Date/Time - Local Time	2nd Sunday of March at 02:00:00 (Recurring)
Current Control Set	001
Failure Control Set	000
Last Known Good Control Set	001
Standard Timezone Offset (Minutes)	-360
Standard Timezone Start Date/Time - Local Time	1st Sunday of November at 02:00:00 (Recurring)
Display	(UTC-06:00) Central Time (US & Canada)

Figure 3.8 TIMEZONE INFORMATION FROM THE REGISTRY

The Time Zone Information artifacts are parsed from the SYSTEM and SOFTWARE registry files. Using the source link for the ControlSet##\Control\TimeZoneInformation key will allow the examiner to view the data parsed from the SYSTEM registry file. This data includes most of the values displayed in the EVIDENCE and DETAILS panes in AXIOM Examine. Identifying the local machine time

zone settings allows the examiner to adjust the time zone settings in their forensic software tools to reflect the time zone for the system they are examining.

USER ACCOUNTS

The User Accounts artifacts are parsed from the SAM and SOFTWARE hives of the Windows Registry, located at **WINDOWS\System32\config**, and the **Windows.Old** folders, as well as other restore points, volume shadow copies, and backup locations.

EVIDENCE INFORMATION	
Source	Dashner Win10 PC.E01 - Partition 2 (Microsoft NTFS, 49.43 GB)\Windows\System32\config\SAM
Recovery Method	Parsing
Deleted source	
Location	SAM\Domains\Account\Users\000003E9 SAM\Domains\Builtin\Aliases\00000220 SAM\Domains\Builtin\Aliases\00000221

Figure 3.9 SOURCE LINKING TO THE SAM REGISTRY HIVE

Details parsed from the SAM and SOFTWARE hives can include the user account name and description, dates and times associated with logins and password changes, account status, user security identifiers (SID), and the profile path for the specific user. The User Accounts artifacts can be very useful for the examiner. The User Name and Security Identifier values can be used for sorting, searching, and filtering in AXIOM Examine to help analyze Windows Event Logs category, or in the Identifiers category when creating profiles in AXIOM Examine to filter on user-specific artifacts.



ARTIFACT INFORMATION		User Accounts
User Name	isaia	
Full Name	Isaiah Dashner	
Type of User	Local User	
Security Identifier	S-1-5-21-3467557965-783750317-32144232 10-1001	
Profile Path	C:\Users\isaia	
Last Password Change Date/Time	7/2/2019 7:44:54 PM	
Password Required	True	
NTLM Hash	799C1DBBE06329B7055D8206E7C801B8	
User Group(s)	Administrators, Users	
Login Count	0	
Account Disabled	False	

Figure 3.10 USER ACCOUNT INFORMATION FROM THE SAM AND SOFTWARE REGISTRY HIVES

The User Group(s) information can help the examiner identify what local privileges the user has on the system being examined, as seen in Figure 3.10.

A registry file, such as the SAM file, is composed of 4096-Byte sections. The first block of data in every registry file begins with a header of “regf”, followed by the date/time the file was last modified, and the storage path for the file being examined. After the “regf” block are the 4096-Byte data blocks, which begin with a header value of “hbin.” The hbin blocks, which store the keys, sub keys, values and data for the registry file, have both allocated and unallocated space. The allocation status of the hbin blocks instructs the operating and file systems to treat the data area like any other storage area on the drive. Correspondingly, if a user account has been deleted, a forensic tool such as AXIOM may be able to recover data for the deleted account. The challenge lies in the version of the operating system being examined. For Windows XP and earlier, the likelihood of recovering data from the unallocated space of a registry file was good. However, beginning with Windows Vista and continuing through Windows 10, it is highly unlikely that data will be recoverable from the unallocated space of a registry file due to the improvements made in the way Windows handles the unallocated space in the registry files. As a result, other system-related files may need to be examined for the presence of legacy user account data from the registry, such as restore points, volume shadow copies, and Windows Event Logs. The `ProfileList` key of the SOFTWARE registry file may also maintain a `ProfileImagePath` value for the deleted user account.

Most details in User Accounts artifact are parsed from the “F” and “V” values of the user’s sub key, which is labeled with a hexadecimal value. The hex value for the key is the user’s Relative Identifier (RID), which is the last numeric value of the SID, and found at offset 48-51 of the F value:

Name	Type	
ComplexityLastUsed	REG_BINARY	00 00 00 00 00 00 00 00 0D 00 02 00
ComplexityPolicy	REG_BINARY	00 00 00 00 00 00 00 08 00 02 00
F	REG_BINARY	02 00 01 00 00 00 00 00 D8 8F AE D2
ForcePasswordReset	REG_BINARY	00 00 00 00
GivenName	REG_BINARY	49 00 73 00 61 00 6
InternetProviderGUID	REG_BINARY	8F 88 F9 D7 FC E3 8
InternetSID	REG_BINARY	01 0B 00 00 00 00 0
InternetUID	REG_BINARY	64 00 65 00 63 00 6
InternetUserName	REG_BINARY	69 00 73 00 61 00 6
Surname	REG_BINARY	44 00 61 00 73 00 6
UserPasswordHint	REG_BINARY	66 00 6F 00 6F 00 7
V	REG_BINARY	00 00 00 00 F4 00 0

ARTIFACT INFORMATION

User Name	isaia
Full Name	Isaiah Dashner
Type of User	Local User
Security Identifier	S-1-5-21-3467557965-783750317-32144232 10-1001
Profile Path	C:\Users\isaia
Last Password Change Date/Time	7/2/2019 7:44:54 PM
Password Required	True
NTLM Hash	799C1DBBE06329B7055D8206E7C801B8
User Group(s)	Administrators, Users
Login Count	0
Account Disabled	False

Figure 3.11 SAM FILE INFORMATION BEING PARSED

SAM FILE - F KEY

F KEY VALUE OFFSETS

8-15	Date and time of last login	64-bit Windows timestamp
24-31	Password reset timestamp	64-bit Windows timestamp
32-39	Account expiration date	64-bit Windows timestamp
40-47	Last unsuccessful login	64-bit Windows timestamp
48-51	Relative Identifier (RID)	4-byte Hex value
56	Account Status/Password	1-byte Hex value. The right nibble identifies account status: 0 = Account Active (Not-Disabled) 1 = Account Disabled

The left nibble identifies if a password has been set

0 = Password required

4 = Password not set

5 = Account not used yet, such as the Guest account

60-61	Country code	Default = 0000, U.S. = 0001, Canada = 0002
64-65	Number of invalid logins	2-byte Hex value
66-67	Number of valid logins	2-byte Hex value

This is OS-specific. For example, if Windows 8 or 10, then the count may not be incremented if the user logs in with their Windows LIVE ID credentials.

DETAILS

REGISTRY VALUE INFORMATION

Name	F
Type	REG_BINARY
Data	03 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 E0 7E 50 9F 0E 31 D5 01 FF FF FF FF FF FF 7F 00 00 00 00 00 00 00 E9 03 00 00 01 02 00 00 10 02 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00

EVIDENCE INFORMATION

Evidence source	Dashner Win10 PC.E01 - Partition 2 (Microsoft NTFS, 49.43 GB)\Windows\System32\config\SAM
Location	SAM\Domains\Account\Users\0000003E9
Evidence number	Dashner Win10 PC.E01

Figure 3.12 F KEY OF SAM FILE INTERPRETING THE RID AT OFFSET 48

SAM FILE – V KEY

V VALUE OFFSETS

12-15	Relative offset to windows user account from the end of the header	4-byte Hex value	Header is 204 bytes in length
16-19	Length of the field	4-byte Hex value	
24-27	Relative offset to the full name from the end of the header	4-byte Hex value	
28-31	Length of the field	4-byte Hex value	
36-39	Relative offset to the description	4-byte Hex value	
40-43	Length of the field	4-byte Hex value	
168-179	Pointer to LM password hash	12-byte Hex value	See note below
180-191	Pointer to NT password hash	12-byte Hex value	See note below

Note: In Windows 10 Release version 1607 Microsoft transitioned from using RC4 encryption to AES encryption for the NT hash of the user's password. In an instance where a system was updated to Windows 10 version 1607, or later, the NT hash of the password will remain secured via RC4 encryption.



until the user updates their password. To determine which encryption mechanism is being utilized for the NT hash of the user's password, examine the value of the first byte of the F value: 0x02 indicates RC4 encrypted, 0x03 indicates AES encryption (as seen in Figure 3.13).

GO TO	FIND	HIDE DECODING
432	01 02 00 00 00 00 00 00 05 20
441	00 00 20 02 00 00 69 00i.
450	73 00 61 00 69 00 61 00 00	s.a.i.a..
459	00 49 00 73 00 61 00 69 00	.I.s.a.i.
468	61 00 68 00 20 00 44 00 61	a.h. .D.a
477	00 73 00 68 00 6E 00 65 00	.s.h.n.e.
486	72 00 01 02 00 00 07 00 00	r.....

Figure 3.13 V KEY OF SAM HIVE SHOWING NAME OF USER PROFILE

SOFTWARE HIVE

The Profile Path value for the User Accounts artifact is parsed from the ProfileImagePath value of the SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\ key in the SOFTWARE registry file. As mentioned earlier, the ProfileList key may still be maintaining a record of deleted Windows user accounts, in the event the data is unavailable in the SAM file, due to the version of the operating system.

Name	Type	Value
ProfileImagePath	REG_EXPAND_SZ	C:\Users\saia
LocalProfileLoadTimeLow	REG_DWORD	0xf3284ad4 (4079504084)
LocalProfileUnloadTimeLow	REG_DWORD	0xca269956 (3391527254)
LocalProfileUnloadTimeHigh	REG_DWORD	0x01d57e11 (30768657)
LocalProfileLoadTimeHigh	REG_DWORD	0x01d57dee (30768622)

EVIDENCE INFORMATION

Evidence source: Dashner Win10 PC.E01 - Partition 2 (Microsoft NTFS, 49.43 GB)\Windows\System32\config\SOFTWARE

Location: Microsoft\Windows NT\CurrentVersion\ProfileList\{S-1-5-21-3467557965-783750317-3214423210-1001

Figure 3.14 PROFILEIMAGEPATH KEY WITHIN SOFTWARE HIVE SHOWING DASHNER IS USER WITH RID OF 1001

RUNNING EXERCISE

OPERATING SYSTEM INFORMATION

- Return to the Artifact explorer and in the NAVIGATION pane expand the Operating System category and then select the Operating System Information artifact.
- Select the entry listed in the EVIDENCE pane. In the DETAILS pane note this artifact comes from the path **Windows\System32\config**.
- Also in the DETAILS pane, note the **SOFTWARE** and **SYSTEM** files identified in the Source fields under EVIDENCE INFORMATION.
- Using the evidence information listed for the **SOFTWARE** file, select the Location field link `Microsoft\Windows NT\CurrentVersion`, and view the source in the Registry explorer.
- In the EVIDENCE pane, view the values from the `CurrentVersion` key displayed in the EVIDENCE pane.
- Return to the Artifacts explorer and with the Operating System Information artifact selected, note there are multiple entries listed under Location for the evidence information sourced from **SYSTEM**.
- Follow the link for the **SYSTEM** file Location field link `ControlSet01\ Control\Windows`.
- In the EVIDENCE pane, note the value for `ShutdownTime`. Select the artifact, then view the data in the DETAILS pane and the HEX card.
- Highlight the 8-byte value listed in the HEX card and scroll down in the DETAILS pane to the DECODE card. Note AXIOM identifies this 8-byte value as a Windows 64-bit little endian timestamp and makes the appropriate conversion. Compare the decoded value to the Last Shutdown Date/Time field listed in the in the DETAILS pane of the Artifacts explorer for the Operating System information artifact entry.

TIMEZONE INFORMATION

- Return to the Artifact explorer, select the Timezone Information artifact from the OPERATING SYSTEM category in the NAVIGATION pane.
- In the EVIDENCE pane, select the entry for **Central Standard Time**.
- In the DETAILS pane, note the data that is parsed from the SYSTEM and SOFTWARE registry hives.
- Find the EVIDENCE INFORMATION entry sourced from the SYSTEM hive. Click the location link listed for `ControlSet01\Control\TimeZoneInformation` and view the key values in



the Registry explorer of AXIOM.

- Return to the Artifacts explorer and follow the link for the Location field parsed from the SOFTWARE hive, Microsoft\Windows NT\CurrentVersion\Time Zones\Central Standard Time. In the Registry explorer, note the keys and values listed for “Display”, “Dlt”, and “Std”. Compare the values to those shown in the Artifact explorer for Display, Standard Timezone Name, and Daylight Timezone name, as shown in the Details pane.
- Use the Tools menu, and the Manage date/time format option to set AXIOM Examine to the time zone for the Dashner computer (UTC -06:00) and check the box to “Apply daylight saving time (DST).
- Notice the lower right corner of the Axiom Examine user interface now shows “Time zone UTC - 6:00”. Hover your mouse over this area of the display, then select the **EDIT** button which appears.
- This is an alternate method to access the “Manage date and time format” menu. Return the case time zone setting to UTC +0:00 and note the change in the lower right corner of the display.
- Tag the Timezone Information artifact using the “Dashner System Information” tag.

USER ACCOUNTS

- From the Artifact explorer, OPERATING SYSTEM category, select the User Accounts artifact.
- Select the Isaiah Dashner entry listed in the EVIDENCE pane and note the information parsed in the DETAILS pane. Notice the Security Identifier listed with its associated Relative Identifier of “1001”. Also notice the first part of the Security Identifier matches the ID value seen in the File System Information artifact.
- View the EVIDENCE INFORMATION entries for the SAM file, and the Locations from the keys within the SAM file.
- Follow the LOCATION link for the SAM\Account\Users\000003E9 key and view the data in the Registry explorer of Axiom Examine.
- In the EVIDENCE pane, select the individual values for GivenName, InternetUserName, and Surname, and view the data parsed in the DETAILS pane.
- In the EVIDENCE pane, select the “F” value and view the data in the DETAILS pane and the HEX card.
- In the HEX view, highlight offsets 24-31 of the F value. This contains the last password reset timestamp associated with the Isaiah Dashner user account. As before, scroll down to the DECODE pane and note that AXIOM detects this value as a possible Windows 64-bit little endian timestamp and makes the conversion.

- In the HEX view, now select offsets 48-51. This is the Relative Identifier (RID) associated with the Dashner user account, stored little endian. In this case “E9 03 00 00” would be read “00 00 03 E9”. We can drop leading zeros and are left with a value of 0x3E9. Open Windows calculator, switch to Programmer mode and HEX entry. Enter the HEX value found in the F Key of 0x3E9 and then switch to Decimal view (there are some variations on how to do this with different versions of the Windows Calculator. The result is a decimal value of 1001, which matches the Relative Identifier seen for the Isaiah Dashner user account.
- Select offset 56. The right nibble of this byte identifies the account status – enabled or disabled. The left nibble of this byte indicates whether a password is required. The value is set to 0x10, indicating this account is enabled and a password is required.
- Select offsets 66-67. This is the number of successful logins. It is a Hex value of 0x00 00. This should match the “Login Count” displayed in the DETAILS pane for the Dashner user account in Artifact view.
- Return to the Artifacts explorer. Add the Isaiah Dashner account information listed in the evidence pane to the “Dashner System Information” tag.

INSTALLED PROGRAMS / INSTALLED MICROSOFT PROGRAMS

In the APPLICATION USAGE category, there are two computer-related categories to help examiners quickly determine which applications are installed on a Windows computer. These are the Installed Programs and Installed Microsoft Programs artifact categories. The Installed Programs artifact includes applications installed on the machine which are not published by Microsoft. The INSTALLED MICROSOFT PROGRAMS artifact includes applications installed on the machine which are published by Microsoft. Both artifacts can be useful in allowing an examiner to quickly determine which programs are installed on a system and alert them to potential file types and artifacts to be looking for.

Application Name	Company	Created D...	Key Last Updat...	Insta...	Versi...	Potential Location
LibreOffice 6.2.5.2	The Document Foundation	17-Jul-19	17-Jul-19 10:07:50 AM	665850	6.2.5.2	
AxCrypt 2.1.1585.0	AxCrypt AB	29-Aug-19	29-Aug-19 3:17:46 PM	7828	2.1.1585.0	
7-Zip 19.00 (x64 edition)	Igor Pavlov	30-Aug-19	30-Aug-19 8:54:47 PM	5255	19.00.00.0	
Google Chrome	Google LLC	31-Oct-19	31-Oct-19 4:18:36 PM		78.0.3904.70	C:\Program Files (x86)\Google\Chrome\Application
Google Update Helper	Google LLC	31-Oct-19	31-Oct-19 4:17:38 PM	41	1.35.301	
CCleaner	Piriform		29-Aug-19 7:57:26 PM		5.61	C:\Program Files\CCleaner
Mozilla Firefox 70.0 (x64 en-US)	Mozilla		29-Oct-19 7:51:57 PM	198356	70.0	C:\Program Files\Mozilla Firefox
Mozilla Maintenance Service	Mozilla		07-Aug-19 12:56:28 PM	323	68.0.1	C:\Program Files (x86)\Mozilla Maintenance Service
VLC media player	VideoLAN		17-Jul-19 10:31:02 AM		3.0.7.1	C:\Program Files\VideoLAN\VLC
BHG Dog Lovers Screensaver			13-Sep-19 7:34:38 PM			
qBittorrent 4.1.7	The qBittorrent project		17-Jul-19 3:22:21 PM	117130	4.1.7	C:\Program Files\qBittorrent
AxCrypt 2.1.1585.0	AxCrypt AB		29-Aug-19 3:17:46 PM	11328	2.1.1585.0	C:\ProgramData\Package Cache\{32ab11f1-2681-42..



Figure 3.15 Installed applications on the Windows computer.

The listed artifact information can not only help determine what applications are installed, but potentially when the software may have been installed or updated. Not all software will update the associated registry keys with this information. The Created Date/Time columns and Key Last Updated Date/Time columns can provide some of this information.

RUNNING EXERCISE

INSTALLED APPLICATIONS

- With the pre-processed Dashner case opened in Axiom Examine, switch to the **Artifact Explorer**.
- In the filters bar, filter on the EVIDENCE drop-down to select only the DASHNER WIN10 PC.
- In the NAVIGATION pane, expand the APPLICATION USAGE category and select the Installed Programs category.
- Sort on the Application Name column then review the list of installed applications. Note the information listed for each in the DETAILS pane, including the Potential Location for the application installation.
- Create a new tag labelled Dashner Installed Applications and add any items of interest. Remember to consider the case scenario and alleged criminal activity when determining which applications to include in this tag. Further investigation of the Dashner evidence may lead you to return to this artifact category to refine items you may wish to include here.

Notes

Notes





MAGNET
FORENSICS®

MODULE 4:

Encryption & Credentials

LEARNING OBJECTIVES

In this lesson, students will take part in lecture, hands-on exercises, instructor-led exercises, and student practical exercises to gain an understanding of the Encryption and Credentials artifacts within AXIOM Examine. Students will also be introduced to decrypting BitLocker encrypted drives and AXIOM's integration with the Passware plugins.

GOALS

At the conclusion of this lesson, students will be able to discuss encryption and credentials artifacts, and use AXIOM Examine to identify encrypted files/containers and anti-forensics tools installed on a machine.

ENCRYPTION & CREDENTIALS

Encryption is becoming common place with free software that is readily available and easy to use. It is not unusual for everyday computer users to employ encryption to safeguard their data. Quickly identifying if encryption software is installed on a computer immediately alerts the examiner to be on the lookout for passwords or passphrases. Identifying encrypted files or containers on the evidence ensures the examiner has as much time as possible to obtain or break the password. Because of the potential value of these encrypted containers, recovery of stored user credentials can be critical to an investigation.

When a computer is in general use, traces of information are constantly being left behind. Analyzing this trace information is the role of the examiner. Anti-forensics tools are used to remove these traces of activity from a computer to mask what the user has been doing and disrupt the investigation of digital evidence.

These anti-forensics tools themselves also leave traces behind on the computer and the evidence of their presence on the machine is often relevant to a case in of itself. The Encryption & Credentials category quickly allows the examiner to locate information indicating that encryption or anti-forensics software has been installed.

In AXIOM Examine these artifacts are listed in the Computer artifacts → ENCRYPTION & CREDENTIALS artifact category. This category contains artifacts such as: Apple Keychain, BitLocker Recovery Key, Encrypted Files, Encryption/Anti-Forensics Tools, and Windows Stored Credentials. Axiom Process can identify if a BitLocker Recovery Key is located inside the evidence sources. When searching for Encrypted Files, AXIOM Process is using modules that are leased from Passware to detect encrypted files using several different techniques. Once an encrypted file is detected using the built-in Passware SDK, AXIOM will map the detected encryption type to a fragment within the artifact. The detected listing will be one of the following:

"Hard Disk Image"	"BestCrypt"	"Mail"
"McAfee Endpoint"	"ICQ"	"OneNote"
"Encrypted Container"	"Microsoft SQL Server"	"Outlook"
"DriveCrypt"	"Zip"	"PowerPoint"
"VeraCrypt"	"Rar"	"Money"
"FileVault"	"Lotus Notes Client Id"	"Access"
"TrueCrypt"	"Lotus Notes Id"	"Word"
"BitLocker"	"Lotus Organizer"	"Excel"
"Pgp"	"Lotus 1-2-3"	"Not Recognized"
"1Password"	"Acrobat"	"MsBackup"
"iWork"	"Act"	"Rdp"
"OpenDocument"	"WordPerfect"	"Project"
"KeePass"	"Lotus Word Pro"	"Schedule"
"Android Backup"	"FileMaker"	
"Ms Office 2013"	"Myob"	
"iTunes Backup"	"Quattro Pro"	
"7Zip"	"Paradox"	
"Ms Office 2010"	"Peachtree"	



"Ms Office 2007" "Norton Backup"	"QuickBooks" "Quicken"	
-------------------------------------	---------------------------	--

The screenshot shows the AXIOM Process software interface. On the left, under 'COMPUTER ARTIFACTS', there is a list of categories with checkboxes. The 'ENCRYPTION & CREDENTIALS' category is selected, highlighted with a blue background and a checked checkbox. On the right, under 'ENCRYPTION & CREDENTIALS', there are five artifacts listed with checkboxes: Apple Keychain, BitLocker Recovery Key, Encrypted Files, Encryption / Anti-forensics Tools, and Windows Stored Credentials. The 'Encryption / Anti-forensics Tools' artifact has its checkbox checked.

Figure 4.1 AXIOM Process ENCRYPTION artifacts

Selecting the Encryption / Anti-forensics Tools artifact instructs AXIOM Process to search the evidence in the case for the presence of known encryption or anti-forensics software. A list of the software that AXIOM Process currently identifies and the executable file it is searching for is provided in Table 4.1 below.

- aescrypt.exe|Crypt
- AESCrypt32.exe|AES Crypt
- AxCrypt.exe|AxCrypt
- AxCrypt2Go.exe|AxCrypt
- Asrar_2.exe|Asrar
- asrar-al-dardashah-0.8.1.exe|Asrar al-Dardashah
- bcveserv.exe|BestCrypt
- bcvetray.exe|BestCrypt
- BEDevCtl.exe|Sophos SafeGuard
- BEFCSvcn.exe|Sophos SafeGuard

- bestcrypt.exe|BestCrypt
- CCleaner64.exe|CCleaner
- DefenderDaemon.exe|Shadow Defender
- DFC.exe|Deep Freeze
- DFInit.exe|Deep Freeze
- EAFCRCLiManager.exe|Symantec Drive Encryption
- Eraser.exe|Eraser
- FreenetTray.exe|Freenet
- I2P.exe|i2p
- msu.exe|Mask Surf Pro
- OurSecret.exe|Our Secret
- pgp.exe|PGP
- pstartsr.exe|Check Point Encryption
- setmace64.exe
- SGNMasterServicen.exe|Sophos SafeGuard
- CCleaner.exe|CCleaner
- cptray.exe|Check Point Encryption
- DFAdmin.exe|Deep Freeze
- DFConsole.exe|Deep Freeze
- EACommunicatorSrv.exe|Symantec Drive Encryption
- EAFCRCLiStart.exe|Symantec Drive Encryption
- Folder Lock.exe|Folder Lock
- gpg.exe|GPG
- Kruptos2Pro.exe|Kruptos 2 Pro
- OpenPuff.exe|OpenPuff
- p95tray.exe|Check Point Encryption
- prot_srv.exe|Check Point Encryption
- setmace.exe
- SGNMaster.exe|Sophos SafeGuard
- Shredder.exe|File Shredder



- slacker.exe|Slacker
- steg.exe|Steg
- timestamp.exe|Timestamp
- Tracks Eraser Pro 9 & 10 - te.exe
- VeraCrypt.exe|Veracrypt
- SpotfluxAgent.exe|Spotflux
- SteganosHotKeyService.exe|Steganos Privacy Suite
- tor.exe|Tor
- truecrypt.exe|TrueCrypt
- WinClear.exe|Winclear

Table 4.1 List of Encryption / Anti-forensics Tools searched for by AXIOM Process

Once it has been established that these applications are installed on the computer, a further search across the evidence should be performed to include and identify other related artifacts (e.g. User Assist or Prefetch artifacts) identifying *when* the applications were run.

Filename	Soft...	Created Date/T...	Last Accessed...	Last Modified...
CCleaner.exe	CCleaner	15-Aug-19 11:29:58 AM	18-Dec-19 6:52:19 PM	29-Oct-19 7:31:24 PM
CCleaner64.exe	CCleaner	15-Aug-19 11:29:58 AM	18-Dec-19 6:58:35 PM	29-Oct-19 7:31:08 PM
AxCrypt.exe	AxCrypt	22-May-19 6:35:00 PM	18-Dec-19 7:02:21 PM	22-May-19 6:35:00 PM

Figure 4.2 Encryption / Anti-forensics Tools results

BITLOCKER RECOVERY KEY

One of the built-in Custom Artifacts lives within the ENCRYPTION & CREDENTIALS artifact category. This artifact, the BitLocker Recovery Key artifact, works by carving out information from saved text documents that contain the BitLocker Recovery Key. When a volume is created using Microsoft's BitLocker, either for full-disk protection or BitLocker-To-Go protection, it is Microsoft's recommendation that the BitLocker Recovery Key data is saved somewhere on an unencrypted drive for later recovery of a user's data. Users may choose to put these keys on their local drive, within cloud storage like OneDrive, or even on USB drives depending upon what is being encrypted to begin with.

Each BitLocker Recovery Key file is structured in the same way. Because of this, the custom artifact that is generated from AXIOM Process - SEARCH FOR CUSTOM FILES BY TYPE option allows AXIOM to carve

out these file entries across the loaded data. When reviewing this information, the examiner can find information such as the GUID identifier for this device as well as the saved Recovery Key which can be passed into AXIOM Process for decrypting this data.

The screenshot shows two windows from the AXIOM software interface. The top window is titled 'PREVIEW' and contains instructions for verifying a recovery key. It includes a text input field labeled 'Identifier:' containing '92987482-86D1-4E3A-97A1-F39C0F622914'. Below this is another text input field labeled 'Recovery Key:' containing '538835-168982-309023-303996-538087-711832-384351-416207', which is highlighted with a red box. The bottom window is titled 'DETAILS' and contains 'ARTIFACT INFORMATION' with fields for Size (Bytes: 1024), MD5 Hash (5f7ac64bb6e3efa17b9a983d5f3b8af2), and SHA1 Hash (554a3d35e3aff924cfa6768ffa394624d6a88c04). It also shows 'EVIDENCE INFORMATION' with a source path: 'Dashner Win10 PC.E01 - Partition 2 (Microsoft NTFS, 49.43 GB)\Users\isala\OneDrive\Documents\BitLocker Recovery Key 92987482-86D1-4E3A-97A1-F39C0F622914.TXT'.

Figure 4.3 Recovering a BitLocker Recovery Key from a OneDrive folder

This key can be applied just as a password could within AXIOM Process to create a decrypted copy of the drive.

POST-PROCESSING

Post-processing was introduced in AXIOM 1.1 and provides the examiner the ability to add additional evidence to the case without having to re-process the work that has already been completed. The additional evidence does not have to be added to a new separate case as it did in the past. The new evidence can now be added into an existing case and processed as part of the normal workflow of an investigation.

New evidence can be added to a case from both AXIOM Process and Examine. In AXIOM Process, open the case by either clicking the **BROWSE TO A CASE** button under ADD EVIDENCE TO EXISTING CASE, or select the case to add evidence to under Open a recent case, as shown in Figure 4.4.



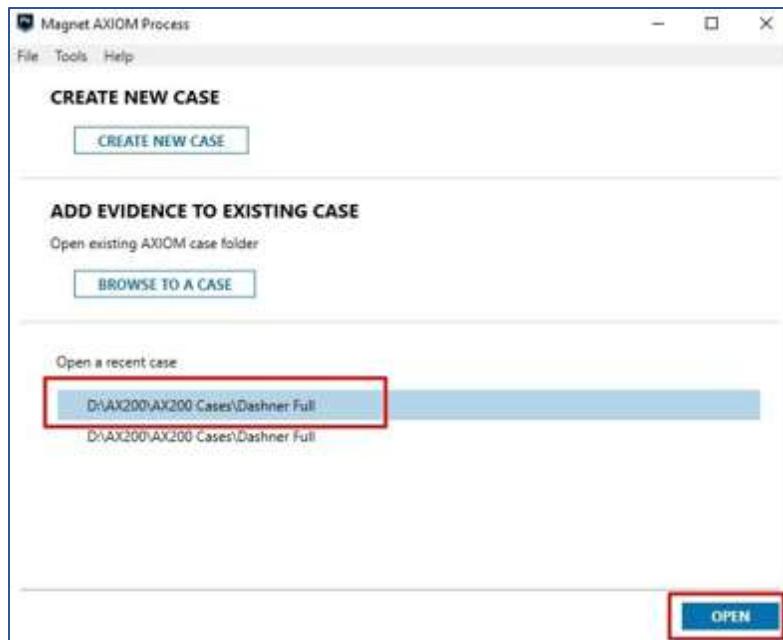


Figure 4.4 Adding new evidence to a case

When Axiom Examine first opens, the user is presented with a Quick Tips screen (see Figure 4.5). This can be turned off if the user does not want to see it again.



Figure 4.5 Quick Tips screen

The first sections of the CASE DETAILS are pre-populated and cannot be changed, as shown in Figure 4.6. Any previous scans are displayed in the SCAN INFORMATION below the current one. In Figure 4.6 the current scan is SCAN 2, and the information added for SCAN 1 is displayed below it. The Scanned By field will automatically pre-populate with the information from the previous scan but can be changed if required.

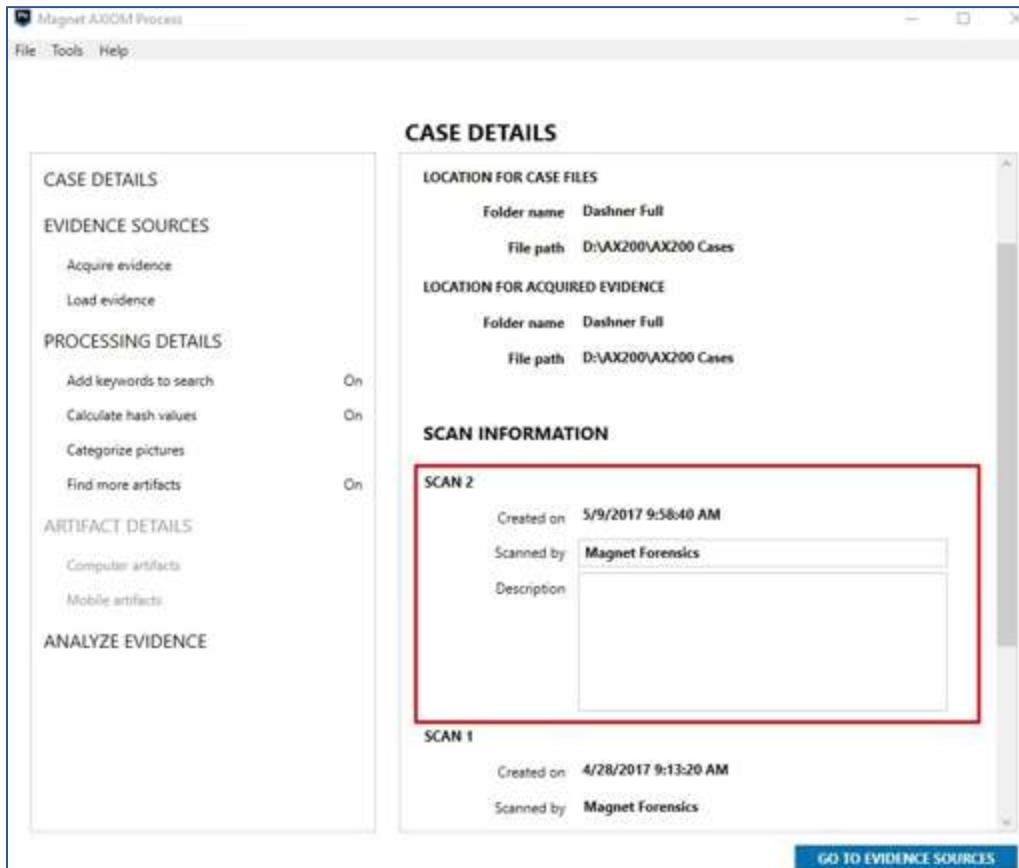


Figure 4.6 Case details of Scan 2

To add additional evidence to a case using AXIOM Examine, with the case already open, select the menu option Process → Add new evidence to case, as shown in Figure 4.7.



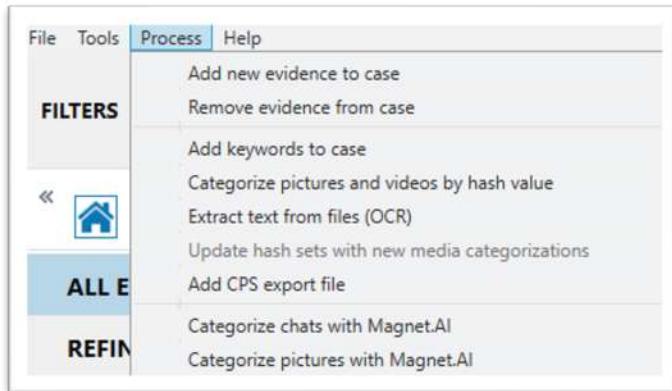


Figure 4.7 Adding new evidence to a case from AXIOM Examine

RUNNING EXERCISE

The image file created when Dashner’s Lexar USB drive was acquired will be used to demonstrate adding encrypted devices and post-processing in AXIOM Process.

POST-PROCESSING AND ENCRYPTED DRIVES

- From AXIOM Examine, select Process, Add new evidence to case
- Change the Scanned By information to your own name and add a Description.
- Click the **GO TO EVIDENCE SOURCES** button.
- Select the options COMPUTER, WINDOWS, LOAD EVIDENCE, IMAGE.
- Browse to the folder **\Evidence\Lexar Flash Drive** on the Desktop and open the file **Lexar USB Flash Drive USB Device 7.46 GB Full E01 Image.E01**.
- The padlock icon identifies it is an encrypted drive.
- Ensure the entire drive is selected and click **NEXT**.
- The Encryption Type has now been identified as BitLocker.
- The **NEXT** button is currently greyed-out.
- Enter the value “538835-168982-309023-303996-538087-711832-384351-416207” without the quotes and click **CHECK**.
- The **NEXT** button is now enabled.
- Click **NEXT**, then confirm the Search type for Partition 1 is set as Full, the search type of the

Unpartitioned space is set as Unpartitioned space, and click **NEXT**.

- Review the **EVIDENCE SOURCES ADDED TO CASE** section to confirm the BitLocker encrypted volume has been added to your case.
- There is no need to change settings for keyword searches or hash values because all the previously selected options from this case are still applied. Click **GO TO ANALYZE EVIDENCE** at the lower left corner of the screen.
- Confirm both Partition 1 and the Unpartitioned space for the **Lexar USB Flash Drive USB Device 7.46 GB Full Image.E01** evidence are present and the Status is Ready, then click **ANALYZE EVIDENCE** at the lower right corner of the screen.
- Once the decryption phase has completed AXIOM Examine automatically starts and displays Processing evidence in the bottom left corner with a progress indicator.
- Once the message Processing complete appears in AXIOM Examine, click **OKAY** to reload the case. Return to Axiom Process and click the **CLOSE** button at the lower right corner of the screen.

MODULE REVIEW

In this module the following topics were covered:

- How AXIOM Process identifies encrypted files.
- The use case and limitations of the Encrypted Files artifact.
- How to use the Encryption / Anti-forensics Tools category to identify traces of relevant software application.
- The use of BitLocker recovery artifacts to decrypt BitLocker evidence files.



REVIEW QUESTIONS

To help reinforce the learning objectives for this module, the following review questions have been provided:

1. How does AXIOM Process identify Encrypted Files?
2. Does an Encrypted Files artifact display what program was used to encrypt the files?
3. What does AXIOM Process search for when identifying Encryption / Anti-forensics Tools artifact?

STUDENT EXERCISE

This exercise is based on the Dashner case scenario from Module 1.

- From the **Artifacts** explorer in **AXIOM Examine**, clear any filters you may have applied.
 - Select the **ENCRYPTION & CREDENTIALS** → **Encryption / Anti-forensics Tools** category.
 - Ensure the Evidence pane is set to Column view.
 - Name the programs that are currently listed in this category.
-

- Using the **APPLICATION USAGE** → **Installed Programs** artifact, when does it appear the programs may have been installed? Do both programs appear to have a Created Date?
 - Using the **Encryption / Anti-forensics Tools** artifact category, what is last accessed time for each of the **.exe** files listed here?
-
-
-



Notes





MAGNET
FORENSICS®

MODULE 5:

Refined Results

LEARNING OBJECTIVES

In this lesson, students will take part in lecture, instructor-led exercises, and student practical exercises to learn the way in which Magnet AXIOM Examine organizes artifacts within the Refined Results category. This category includes items such as Cloud Service URLs, Classifieds URLs, Identifiers, Social Media URLs, and more. Students will also be shown how to create a profile using artifacts gathered in the Identifiers category and examine sources of searches such as Google Searches and Parsed Search Queries. Students will become familiar with the Artifact Reference to ensure if future changes occur in the artifacts supported by AXIOM, the students will have a source of reference to update their knowledge.

GOALS

At the conclusion of this lesson, students will be able to identify, discuss, and use artifacts found within the Refined Results category of AXIOM Examine to further a forensic examination. Students will also be able to create a Profile and use that profile to filter views of specific artifacts. Students will be able to show a depth of knowledge in artifacts relating to browser artifacts.

REFINED RESULTS

REFINED RESULTS is the first artifact in the NAVIGATION PANE of the Artifacts explorer. Figure 5.1 shows some of the categories included within Refined Results.

The Refined Results category organizes artifacts from other categories into useful and meaningful groups. Although many artifacts listed in Refined Results can also be found within the WEB RELATED parent category, they are organized within Refined Results to quickly identify artifacts of importance to expedite the examiner's investigation. Many of the artifacts from Refined Results are sourced from browser activity.

REFINED RESULTS	4,995
Classified URLs	1,689
Cloud Services URLs	383
Facebook URLs	375
Google Analytics First Visit Cookies	7
Google Analytics Referral Cookies	7
Google Analytics Session Cookies	6
Google Maps Queries	118
Google Searches	596
Identifiers	1,171
Locally Accessed Files and Folders	174
Malware/Phishing URLs	8
Parsed Search Queries	72
Passwords and Tokens	15
Rebuilt Desktops (Windows)	1
Rebuilt Webpages	239
Social Media URLs	132
Tax Site URLs	1
Torrent URLs	1

Figure 5.1 Refined Results

Figure 5.2 demonstrates three WEB RELATED artifacts that have also been compiled into one of the Refined Results categories. AXIOM Process reviews the URL content of the browser artifacts, regardless of the browser or evidence source, and compiles them into their respective Refined Results categories. When reviewing the artifacts in AXIOM Examine, this feature eliminates the need to search through individual browser results for Chrome, Firefox, Edge, etc. for the desired URLs.



NOTE: Because the source of much of the REFINED RESULTS categories originate from browser activity, many results will appear in both the compiled REFINED RESULTS as well as their individual browser artifact categories under WEB RELATED. Also, some artifacts could appear in more than one REFINED RESULTS category.

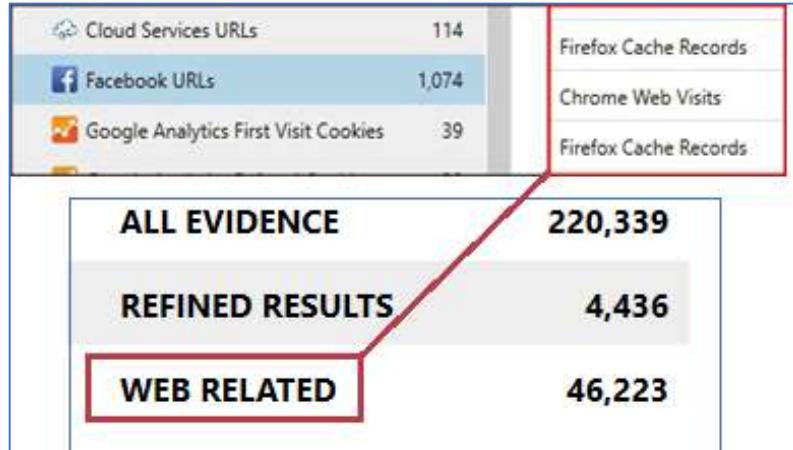


Figure 5.2 Relationship of a REFINED RESULTS originating from a WEB RELATED artifact

HELP/DOCUMENTATION

The Help → Documentation menu option in AXIOM Examine contains links to built-in documentation for Magnet AXIOM. The documentation includes the User Guide and the Artifact Reference – a guide to all the artifacts searched for and identified by AXIOM Process.

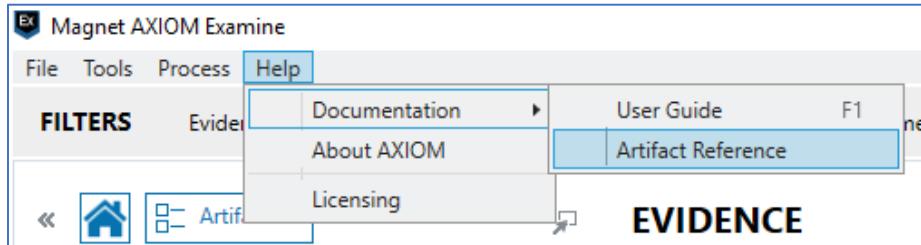


Figure 5.3 Help documentation available in AXIOM Examine

The Artifact Reference contains a listing of the REFINED RESULTS categories and a description of the columns displayed within each one, as shown in Figure 5.4. Where appropriate, the Artifact Reference also provides a link to documentation located on the Magnet Forensics website that details which URLs are included in the REFINED RESULT.

The screenshot shows the AXIOM Magnet software interface. On the left, there is a navigation tree under 'ARTIFACT REFERENCE' with categories like Windows, Android, iOS, macOS, Linux, Cloud, Windows Phone, Kindle, Refined Results, Media, and several sub-categories under Refined Results including 'Classifieds URLs'. The main content area is titled 'CLASSIFIEDS URLs' and contains a table with columns 'Attribute' and 'Description'. The 'Notes' row in this table includes a link 'classifieds sites domains' which is highlighted with a red arrow.

Figure 5.4 Artifact Reference showing link to view which URLs are included in the CLASSIFIEDS URLs category

GOOGLE SEARCHES

Any searches conducted via the Google webpage using any supported browser are compiled into the REFINED RESULTS → Google Searches category.

The DETAILS card on the DETAILS pane includes the following information:

ARTIFACT INFORMATION

Search Term	This information is imbedded in the URL itself; this is common to most search engine websites.
URL	The full URL from Google.
Date/Time	The date and time the search was executed. Whether the date and time information was recorded as UTC or Local Time is dependent on the browser that generated the artifact.
Webpage Title	The title of the webpage that appears in the browser's title bar/tab.
Original Artifact	The artifact category from which this refined result was compiled.
Original Search Query	The original search query supplied to google recorded by the URL.

EVIDENCE INFORMATION

Source	The directory path (including file name) where the artifact was found.
--------	--



Location The location of the data within the source file or object. The example shown in Figure 5.5 references a **History** SQLite database from the Chrome browser and details the specific database tables and records the artifact was extracted from. If the artifact is **not** sourced from a database, the offset from the beginning of the file or object is listed.

DETAILS

ARTIFACT INFORMATION

Search Term	tails bittorrent
URL	https://www.google.com/search?q=tails+bittorrent&rlz=1C1CHBD_enUS856US856&oq=tails+bit&aqs=chrome.2.69i57j0l5.3604j0j7&sourceid=chrome&ie=UTF-8
Date/Time	29/08/2019 2:04:11 PM
Original Search Query	tails bit
Web Page Title	tails bittorrent - Google Search
Original artifact	Chrome Web History

EVIDENCE INFORMATION

Source	Dashner Win10 PC.E01 - Partition 2 (Microsoft NTFS, 49.43 GB)\Users\isaia\AppData\Local\Google\Chrome\User Data\Default\History
Recovery Method	
Deleted source	
Location	Table: urls(id: 284)
Evidence number	Dashner Win10 PC.E01

Figure 5.5 DETAILS card showing SQLite table locations

RUNNING EXERCISE

GOOGLE SEARCHES

- Select the REFINED RESULTS → Google Searches category.
- Review the content of the URL column.
- All the search queries were performed on the Google webpage
- Click on the Search Term column to invoke a sort.
- The arrow is now pointing up, indicating an ascending sort.

- In the search box on the FILTERS bar, type “you” and click **Go**.
- The FILTERS bar has turned yellow and the keyword “you” is in bold.
- All instances of the word “you” are highlighted yellow.
- The filtered results are still sorted in ascending order by the Search Term.
- Scroll down in the Search Term column and locate the entries for the search “youtube”; select the first entry with a date of 8/29/2019.
- Notice the difference in the Search Term and the Original Search Query columns.
- In the DETAILS card of the DETAILS pane, view the URL field.
- The data following the “q=” is the actual search that was executed by the search engine.
- The data following the “oq=” is the original query that was entered by the user.
- A Google Search with an Original Search Query indicates the user clicked one of the auto-completed searches provided by Google rather than typed the Search Term into the search box.
- Click **CLEAR FILTERS** to clear all the filters.

PARSED SEARCH QUERIES

Searches conducted on sites other than Google are compiled into the REFINED RESULTS → Parsed Search Queries category. This includes searches performed on popular sites such as Yahoo, Facebook, Bing, YouTube, and others.



ARTIFACT INFORMATION

- Search Term: funny dog videos
- URL: https://www.youtube.com/results?search_query=funny+dog+videos
- Date/Time: 8/30/2019 5:22:57 PM
- Search Engine: Youtube
- Web Page Title: funny dog videos - YouTube
- Original artifact: Chrome Web Visits

EVIDENCE INFORMATION

- Source: Dashner Win10 PC:E01 - Partition 2 (Microsoft NTFS, 49.43 GB)\Users\jsain\AppData\Local\Google\Chrome\User Data\Default\History
- Recovery Method: Deleted source
- Location: Table: visits(id: 415)
Table: urls(id: 309)
- Evidence number: Dashner Win10 PC:E01

funny dog videos	https://www.youtube.com/results?search_query=funny+dog+videos	8/30/2019 5:22:57 PM	Youtube
funny dog videos	https://www.youtube.com/results?search_query=funny+dog+videos	8/30/2019 5:22:57 PM	Youtube

Figure 5.6 DETAILS card of Parsed Search Queries artifact

The DETAILS card on the DETAILS pane includes the following information:

ARTIFACT INFORMATION

Search Term	The information embedded in the URL itself; this is common to most search engine websites.
URL	The full URL.
Date/Time	The date and time the search was executed. Whether the date and time information was recorded as UTC or Local Time is dependent on the browser that generated the artifact.
Search Engine	The search engine used to search for the keyword(s)
Webpage Title	The title of the webpage that appears in the browser's title bar/tab.
Original Artifact	The artifact category from which this refined result was compiled.

RUNNING EXERCISE

PARSSED SEARCH QUERIES

- Select the REFINED RESULTS → Parsed Search Queries category.
- The Search Term column displays the search conducted by the user.
- The Search Engine column displays the different search engines used.

- The Artifact column details the WEB RELATED category this refined result has been sourced from.
 - In the search box on the FILTERS bar, type “you” and click **Go**.
 - All the results are from YouTube website searches as seen in the **Search Engine** column.
 - Locate the Artifact column, which indicates the original artifact this refined result was sourced from. Highlight the entry from the Chrome Web Visits category where the search term reflects “funny dog videos”.
 - Note the Table and record id information in the Location field of the DETAILS card.
-
- Expand the TAGS, PROFILES & MEDIA CATEGORIES pane.
 - Click **ADD NEW TAG** and apply a tag named “Refined Result – YouTube Search”.
 - A tag icon has been added to the entry in the EVIDENCE pane.
 - On the DETAILS card, click the Original Artifact link – [Chrome Web Visits](#).
 - AXIOM Examine automatically switches to the WEB RELATED → Chrome Web Visits category and highlights the corresponding artifact.
 - Review the Source and Location information in the DETAILS card and confirm this is the same artifact.
 - Although this is the same artifact it is **not** tagged. AXIOM Examine treats the artifacts within each category as separate items and does not cross-tag them.
 - Clear all filters.

CLASSIFIEDS URLs

URLs relating to websites that contain classified ad type content, such as items for sale, personal ads and services offered, are compiled into the REFINED RESULTS → Classifieds URLs category. There are currently in excess of 50 domains supported, some of which are shown in Figure 5.7. Refer to the Artifact Reference for a full list of supported domains.



Amazon	https://www.amazon.com/a/addresses/add?ref=ya_...
Amazon	https://www.amazon.com/a/addresses/add?ref=ya_...
Amazon	https://www.amazon.com/s/ref=nb_sb_noss [url fiel...
Amazon	https://www.amazon.com/a/addresses?ref_=ya_d_l_...
Amazon	https://www.amazon.com/ref=nav_logo
Craigslist	https://mail.google.com/mail/?view=cm&fs=1&to=... 8/29/2019 3:54:36 PM
Craigslist	https://bham.craigslist.org/grd/d/dora-siberian-hus... 8/29/2019 6:37:32 PM

Figure 5.7 Classifieds URLs

The DETAILS card on the DETAILS pane includes the following information:

ARTIFACT INFORMATION

Site Name	The name of the classified website.
URL	The full URL.
Date/Time	The date and time the webpage was visited. Whether the date and time information was recorded as UTC or Local Time is dependent on the browser that generated the artifact.
Original Artifact	The artifact category from which this refined result was compiled.

RUNNING EXERCISE

CLASSIFIEDS URLs

- From the **Artifacts** explorer in AXIOM Examine, clear any filters you have applied.
- Select the REFINED RESULTS → Classifieds URLs category.
- Right-click the Site Name column and select Filter on column.
- Enter “ebay” and click **SEARCH**.
- The results only contain eBay entries.
- The FILTERS bar has turned yellow and the filter criteria is in bold.
- Hover over the filter criteria on the FILTERS bar; the full filter criteria is displayed.
- Using the same steps, filter the URL column using “dog” as the search term.

- The matching results are eBay activity that include the word “dog” in the URL.
- Both filter criteria are in bold on the FILTERS bar.
- Clear all filters.

CLOUD SERVICES URLs

URLs relating to the use of cloud-based services are compiled into the REFINED RESULTS → Cloud Services URLs category. There are currently in excess of 60 domains supported, some of which are shown in Figure 5.8. Refer to the Artifact Reference for a full list of supported domains.

Site...	URL	Date/Time
Dropbox	https://www.dropbox.com/home/old%20flash%20dr...	10-Sep-19 7:55:52 PM
Dropbox	https://www.dropbox.com/home/old%20flash%20dr...	10-Sep-19 7:55:52 PM
Dropbox	https://photos-1.dropbox.com/t/2/AAAeTwq5JFnxD...	10-Sep-19 7:55:14 PM
Dropbox	https://assets.dropbox.com/www/en-us/help/emails...	10-Sep-19 7:55:14 PM

Figure 5.8 Cloud Services URLs

The DETAILS card on the DETAILS pane includes the following information:

ARTIFACT INFORMATION

Site Name	The name of the cloud service website.
URL	The full URL.
Date/Time	The date and time the webpage was visited. Whether the date and time information was recorded as UTC or Local Time is dependent on the browser that generated the artifact.
Original Artifact	The artifact category from which this refined result was compiled.

RUNNING EXERCISE

CLOUD SERVICES URLs

- Select the REFINED RESULTS → Cloud Services URLs category.
- Apply a filter of “dropbox” to the Site Name column.



- Apply an ascending sort to the URL column.
- Almost all the entries start with “https” denoting a secure connection.
- Use the keyboard shortcut CTRL+A to select all the entries.
- Expand the TAGS, PROFILES & MEDIA CATEGORIES pane.
- Click **ADD NEW TAG** and apply a tag named “Dropbox Activity”.
- A tag icon has been added to all the entries in the EVIDENCE pane.
- Hover over the tag icon in the far-left column of the EVIDENCE pane; the name of the tag is displayed.
- Using the search box in the FILTERS bar, conduct a search for “account”.
- Note that a file called “Accounting.ods” was downloaded using the Chrome web browser.
- There are also URLs containing “verifyemail” sourced from various Chrome artifacts. Review these URLs to determine the email address listed here, which appears to have authenticated to the Dropbox service.
- On the FILTERS bar, click the X next to “account” to remove just that part of the filter.
- The results are still filtered by Site Name contains “dropbox”.
- Clear all filters.

FACEBOOK URLs

The REFINED RESULTS → Facebook URLs category contains URLs relating to activity on the Facebook website. In some instances, the structure of the URL is such that the possible activity occurring on the website can also be identified, e.g. login attempts, viewing help pages, or looking at a Facebook profile. If the activity cannot be determined from the URL, the Potential Activity column is populated with Unknown.

URL	Date/Time	Potential Activity
https://www.facebook.com/CHOKLATE-1404311726...		Looking at Facebook profile with profile id: CHOKLATE-140431172675
https://www.facebook.com/aaronsprinklemusic		Looking at Facebook profile with profile id: aaronsprinklemusic
https://www.facebook.com/wearethegodsthemselves		Looking at Facebook profile with profile id: wearethegodsthemselves
http://www.facebook.com		At Facebook home page
https://graph.facebook.com		At Facebook home page
https://graph.{0}.facebook.com		At Facebook home page

Figure 5.9 Facebook URLs

The DETAILS card on the DETAILS pane includes the following information:

ARTIFACT INFORMATION

URL	The full URL.
Date/Time	The date and time the webpage was visited. Whether the date and time information was recorded as UTC or Local Time is dependent on the browser that generated the artifact.
Potential Activity	The potential activity occurring on the website.
Original Artifact	The artifact category from which this refined result was compiled.

RUNNING EXERCISE

FACEBOOK URLs

- From the **Artifacts** explorer in AXIOM Examine, clear any filters that you have applied.
- Select the REFINED RESULTS → Facebook URLs category.
- Filter on the URL column for “hounds”; then sort on the URL column.
- Select the first result and note the Potential Activity column.
- In the DETAILS card of the DETAILS pane, locate the URL field and highlight the string “HoundsLoungeNLR” (this is the Facebook username).
- An examiner could use the Facebook username to identify the Facebook ID for that account using the Facebook API.

NOTE: A Facebook user can change their vanity name/username, but not their Facebook ID number. This is important to remember when serving legal process. Also, bear in mind that a Facebook ID does not just refer to a user. All items within Facebook are given an ID including pictures, marketplace items, etc., so the IDs listed in the results for this case may not only be referring to a user account. Facebook could change their API at any time. The structure of these URLs was current at the time this manual was written.

- Highlight “HoundsLoungeNLR” within the DETAILS pane and copy the string by highlighting it, or by simply double-clicking the string.
- Paste the copied string into the search box of the FILTERS bar and click **Go**.
- The filtered results each have the search term highlighted in the URL and DETAILS pane.



- Select the WEB RELATED → Chrome Web History category.
- Note the Source information in the DETAILS card. The results are sourced from the **History** SQLite database file
- Web databases will be reviewed in Module 6.
- Clear all filters.

SOCIAL MEDIA URLs

URLs relating to activity on social media websites is compiled into the REFINED RESULTS → Social Media URLs category. It includes activity on websites such as: Friends Reunited, LinkedIn, Reddit and Twitter, some of which are shown in Figure 5.10. Refer to the Artifact Reference for a full list of supported domains.

NOTE: This category does not include activity on the Facebook website because Facebook has its own refined results category.

Site...	URL	Date/Time
Reddit	https://www.reddit.com/user/NewMaxx/comments/9yv0c6/ssd_buying_guide_wip/	31-Oct-19 6:48:14 PM
Reddit	https://www.reddit.com/r/buildapc/comments/cg68ec/best_m2_ssds/	31-Oct-19 6:48:21 PM
Twitter	https://twitter.com/intent/tweet?text=Check out today's homepage on Bing&url=ht...	

Figure 5.10 Social Media URLs

The DETAILS card on the DETAILS pane includes the following information:

ARTIFACT INFORMATION

- | | |
|-------------------|---|
| Site Name | The name of the social media website. |
| URL | The full URL. |
| Date/Time | The date and time the webpage was visited. Whether the date and time information was recorded as UTC or Local Time is dependent on the browser that generated the artifact. |
| Original Artifact | The artifact category from which this refined result was compiled. |

RUNNING EXERCISE

SOCIAL MEDIA URLs

- From the **Artifacts** explorer in AXIOM Examine, clear any filters you have applied.
- Select the **REFINED RESULTS** → Social Media URLs category
- Filter the Site Name column for “Reddit” entries.
- The **MATCHING RESULTS** details how many of the SOCIAL Media URLs meet the criteria.
- Sort the Date/Time column.
- Review the URL column. There are numerous entries relating to the Firefox web browser and an Alienware laptop.
- Filter the Artifact column to contain the word “Firefox.”
- Note that the user performed a search for “best m.2 ssd” on 31 Oct 19. After reviewing the URLs visited after this, it could show the user was interested in purchasing additional hard drives.
- Clear all filters.

GOOGLE MAP QUERIES

The **REFINED RESULTS** → Google Maps Queries artifacts are generated from browser activity on the Google Maps website – www.google.com/maps. Search data is compiled from activities such as searching for a specific street address, searching for restaurants near a specified location, clicking on a search result for a business near a specific location, searching for a city name, and searching for directions to a specific location.



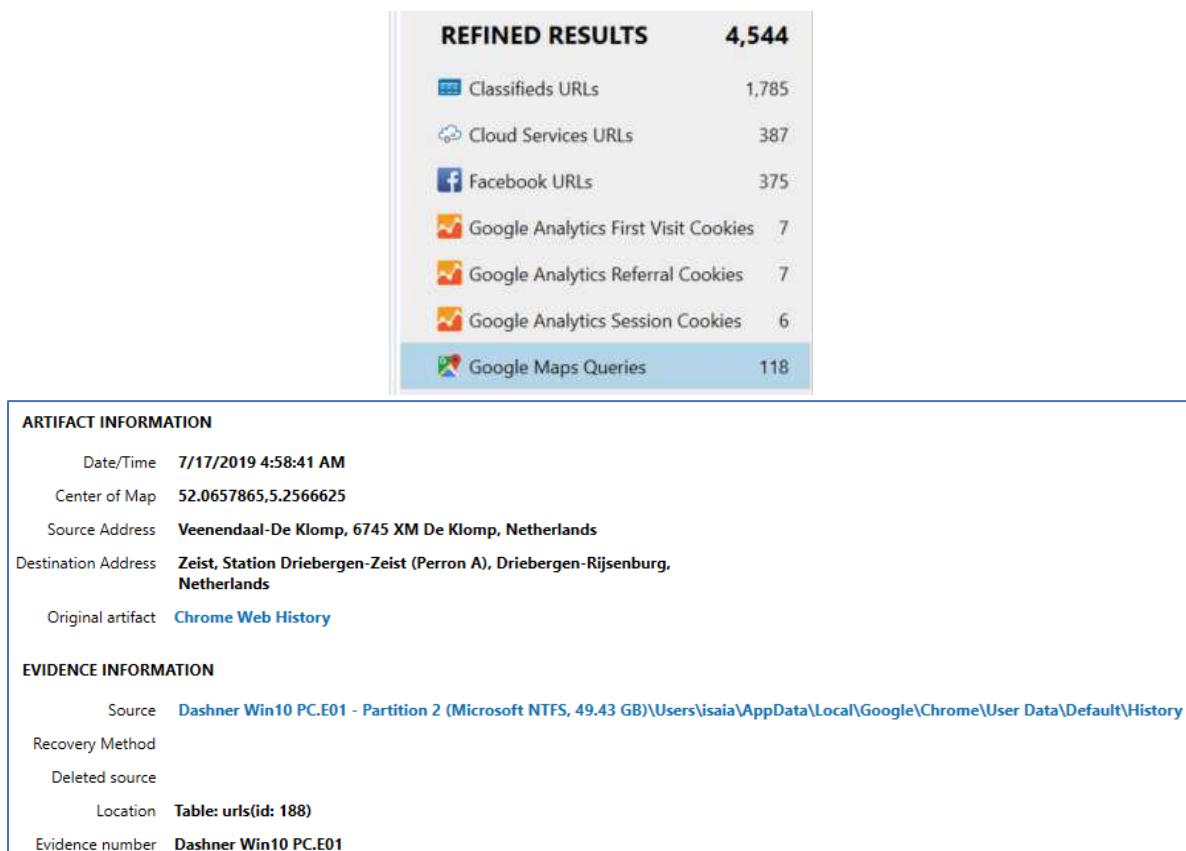


Figure 5.11 Google Map Queries

The DETAILS card on the DETAILS pane includes the following information:

ARTIFACT INFORMATION

Search Query	The place that was searched for.
Date/Time	The date and time the map was viewed. Whether the date and time information was recorded as UTC or Local Time is dependent on the browser that generated the artifact.
Starting Location	The starting location for navigation/directions.
Center of Map	Latitude and Longitude where the map was centered.
Business Latitude and Longitude	Latitude and Longitude of the business location.
Source Address	Starting point for directions.
Destination Address	Finishing point for directions.
Route Type	How the user selected to travel (car, bus, walk).
Additional Address	Any point the user selected to navigate via.

Street View Latitude/Longitude	The latitude and longitude displayed when in street view.
--------------------------------	---

RUNNING EXERCISE

GOOGLE MAPS AND WORLD MAP VIEW

- Select the Google Maps Queries artifact from the REFINED RESULTS category.
- Select the record where the Search Query column reflects: “enterprise car rental heathrow”
- Slide all the way to the far right in the EVIDENCE pane until a small red pin icon is visible for this record. Click on the red pin icon () for this record.
- This switches Examine to the World map view. Notice the DETAILS pane has been collapsed.
- Zoom into the points listed on the map for this artifact. Click on one of the red pins on the map. The pin will change to a green pin (). Click on **VIEW DETAILS** to see more information about the selected pin.
- The Center of Map fragment relays where the center of the loaded Google Maps query was found.
- Select the World map view in the dropdown at the top right of the Evidence pane and select Column view.

CONNECT TO AN OFFLINE MAP SERVER

If you're working on a computer without internet access, you can set up an offline map server. To connect to the server, follow the steps below.

Note: To learn about the offline map server requirements and recommendations, see the customer portal article, <https://www.magnetforensics.com/docs/axiom/html/Content/en-us/reviewing-evidence/views/view-map.htm>.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the **Settings** window, under **Maps**, select the option to **Connect to an offline map server**.
3. Provide a **Server address**, and then click **Connect to server**.

If the connection is successful, click **Okay**. If the connection is unsuccessful, see more tips about connecting to the server in <https://www.magnetforensics.com/docs/axiom/html/Content/en-us/reviewing-evidence/views/view-map.htm>.



LOCALLY ACCESSED FILES AND FOLDERS

This REFINED RESULTS category contains information about files and folders accessed on a computer via Windows File Explorer, including items stored on local drives, removable media, and network resources. The information contained within these artifacts is extracted from the **WebCacheV01.dat** database that also contains the Internet Explorer version 10 (and later) and Edge browsing history. Because this database is stored in the AppData area of the user account, the Windows user account in use when the activity occurred can be readily identified.

Path	Path...	Accessed Date...
E:\rides\20190907_141010_HDR.jpg	Drive	18-Dec-19 7:03:20 PM
E:\VHD for Hiding.docx	Drive	18-Dec-19 6:58:52 PM
C:\Users\isaia\OneDrive\Desktop\Sign.png	Drive	18-Dec-19 7:10:05 PM
E:\rides\20190907_142412_HDR.jpg	Drive	18-Dec-19 7:10:19 PM
E:\rides\20190907_141946_HDR.jpg	Drive	18-Dec-19 7:07:13 PM
E:\rides\20190907_141944_HDR.jpg	Drive	18-Dec-19 7:06:55 PM
E:\rides\20190907_141410_HDR.jpg	Drive	18-Dec-19 7:05:51 PM
E:\Wireshark_Display_Filters.pdf	Drive	18-Dec-19 6:58:42 PM
file:///	Drive	11-Sep-19 5:35:12 PM

Figure 5.12 Locally Accessed Files and Folders

For example, the artifact **E:\VHD for Hiding.docx** is sourced from the **WebCache** folder in **Users\isaia**, indicating the user accessing the volume. This is because the user navigated to the file path **E:\VHD for Hiding.docx** from the Windows File Explorer.

Artifacts displayed as “:Host: This PC” are also sourced from WebCache and navigated through File Explorer. The naming convention “:Host:” comes from native path variables (or environment variables).

Notice above, on 11-Sep-19 5:35:12PM, there is a listing for “file://”. Opening a PDF in Edge creates a safe container to view the PDF without the need for additional software.

IDENTIFIERS

There are two REFINED RESULTS → Identifiers categories: Identifiers – Device, and Identifiers – People. The Identifiers - People category contains information that can be used to help identify individuals e.g. email addresses, chat accounts and screen names, device user accounts, data extracted from document metadata, and information entered in web forms. The Identifiers – Device category contains information that can help identify devices that might have been attached to the computer at some point in time. These identifiers are extracted from other artifacts including those within the EMAIL and CHAT categories, and those within the OPERATING SYSTEM categories.

Identifier	Column Name	Artifact
Nunez, Raisa	Authors	Word Documents
Microsoft	Authors	PDF Documents
Kevin L. Brown	Authors	Word Documents
Kevin L. Brown	Authors	PowerPoint Documents
Kevin L. Brown	Authors	Excel Documents
Nunez, Raisa;Isaiyah Dashner	Authors	Excel Documents
live:griddlerheriddle	Display Name	Skype Contacts
Skype	Display Name	Skype Contacts
Echo / Sound Test Service	Display Name	Skype Contacts
george	Display Name	Skype Contacts
Wilfy Grunsell	Display Name	Skype Contacts
Jeff Armstrong	Display Name	Your Phone Contacts

Figure 5.13 Identifiers

The DETAILS card on the DETAILS pane includes the following information:

ARTIFACT INFORMATION

- Identifier The ID of the person.
- Column Name The artifact field containing the identifying information.
- Original Artifact The artifact the identifier was sourced from.

PROFILES

The data compiled into the REFINED RESULTS → Identifiers categories can be used to create a filter profile. A profile helps the examiner quickly identify all artifacts in the case associated with the Identifiers linked to the profile.

Profiles can either be created by selecting CREATE NEW PROFILE in the TAGS, PROFILES & MEDIA CATEGORIES pane, or by selecting **ADD PROFILE** from the Manage profiles dialog window, as shown in Figure 5.14. The Manage profiles window can be accessed from the Tools menu or the Profiles drop-down on the FILTERS bar.



Module 5 – Refined Results

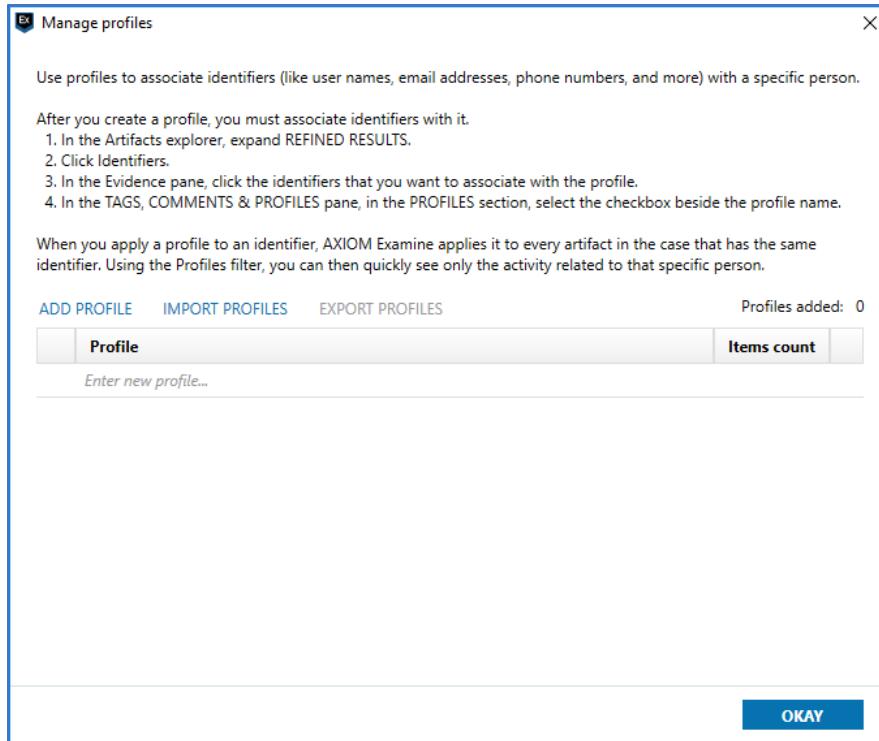


Figure 5.14 Managing profiles

NOTE: The PROFILES card only appears on the TAGS, PROFILES & MEDIA CATEGORIES pane when the REFINED RESULTS → Identifiers category is selected.

Once the profile has been created, Identifiers can be linked to it by highlighting the Identifier(s) and selecting the profile in the PROFILES card of the TAGS, PROFILES & MEDIA CATEGORIES pane.

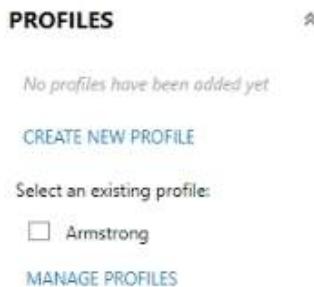


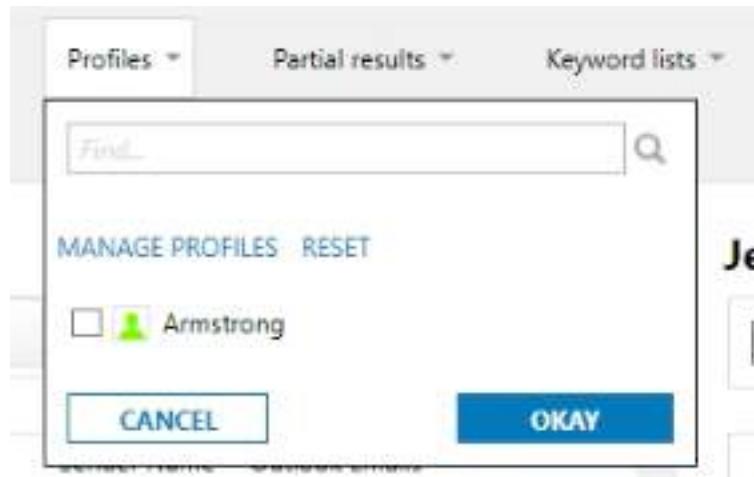
Figure 5.15 Profile card in Tags, Profiles & Media Categories pane

Identifiers linked to a profile display a silhouette icon in the EVIDENCE pane (left side of Figure 5.16)

Wilfred Grunsell <Wilfred.Grunsell@gmx.co.uk>	Sender Name	Outlook Emails
pandora@pandora.com <pandora@pandora.com>	Sender Name	Outlook Emails
Google Nest <googlenest.noreply@google.com>	Sender Name	Outlook Emails
Jeff Armstrong <armstrongjeff42@gmail.com>	Sender Name	Outlook Emails

Figure 5.16 Profile silhouette icon identifying a Profile

Once a profile has been created it can be used as a filter to display all artifacts associated with the Identifiers linked to the Profile. To filter using a profile, select the profile name from the Profiles drop-down menu on the FILTERS bar as shown in Figure 5.17 below.

*Figure 5.17 Filtering by a Profile*

RUNNING EXERCISE

CREATING A PROFILE

- Select the REFINED RESULTS → Identifiers-People category.
- Review the Artifact column which details the various sources of identifiers.
- The Column Name details the artifact field the Identifier has been extracted from.
- Locate the Identifier column, right-click on the column title and select Filter on column.
- Select the Advanced tab, and in the SEARCH BY TERM, leave the search as Include and enter the search term “Jeff”.
- Click ADD ANOTHER TERM and Include the search term “Armstrong”.



- Change the search logic to OR, and click **SEARCH**.
- This is a Regular Expression (RegEx) that will apply a filter to display only the Identifier fields containing the expression “Jeff” OR “Armstrong”.
- Highlight all the results.
- Expand the TAGS, PROFILES & MEDIA CATEGORIES pane.
- In the PROFILES card, click **CREATE NEW PROFILE**.
- Name the profile “Jeff Armstrong” and click **OKAY**.
- The selected items all now have a silhouette icon indicating they are linked to a profile.

EDITING A PROFILE

- In the EVIDENCE pane, highlight one of the Identifiers linked to the Jeff Armstrong Profile.
- In the TAGS, PROFILES & MEDIA CATEGORIES pane, on the PROFILES card, mouse over the Jeff Armstrong Profile and click the X that appears to the right.
- The Identifier has been removed from the Profile.
- With the removed Identifier still highlighted, find the heading “Select an existing profile:” on the PROFILES card and select the check-box next to the Jeff Armstrong Profile to replace this identifier in the profile.
- The Identifier is linked to the Jeff Armstrong Profile again.

MANAGING PROFILES

- In the TAGS, PROFILES & MEDIA CATEGORIES pane on the PROFILES Card, click **MANAGE PROFILES**.
- The number of Identifiers linked to the Profile is listed.
- Hover over the Profile name; a trash can appears, and the examiner could delete the profile if needed.
- Click on the Profile name – “Jeff Armstrong”, change it to just “Jeff” and click **UPDATE**.
- The Profile name has been updated.
- Close the Manage profiles window by clicking on **OKAY**.
- Clear all filters.
- From the Profiles drop-down on the FILTERS bar, select the Jeff profile and click **OKAY**.

- All artifacts in the case that contain the Identifiers linked to the Jeff profile are now displayed.
- Clear all filters.

NOTE: The Manage profiles option is also available from the Tools menu and the Profiles drop-down on the FILTERS bar.

REBUILT DESKTOPS (WINDOWS)

AXIOM can reconstruct the view of a user's Desktop on a Windows system. This combines several pieces of information from across the system in a single artifact for the examiner to review. In order to rebuild this information, AXIOM reads several keys from the user's **NTUSER.dat** registry hive, and keys from the SYSTEM and SOFTWARE registry hives. The Rebuilt Desktops (Windows) artifact even displays the user's chosen desktop wallpaper.

PREVIEW

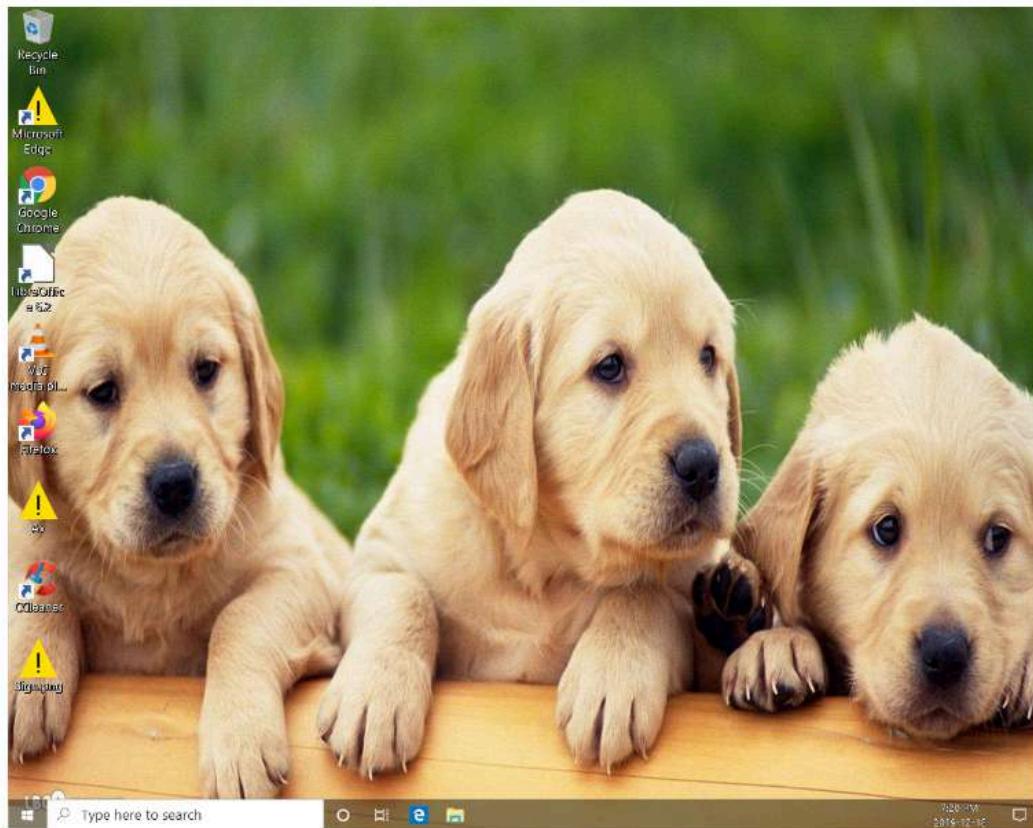


Figure 5.18 The user's rebuilt desktop



The PREVIEW card on the DETAILS pane displays a graphical representation of the user's Desktop including the picture(s) used as the backdrop, any Quick Launch icons on the taskbar, and any files, folders or shortcuts saved to the Desktop. However, it does not necessarily place the icons in their correct relative positions on the display. Icons are placed top-to-bottom starting at the top-left corner and then will create new columns, filling in the icons, as needed.

The artifact also lists the path to the wallpaper picture file(s), the type of background used, e.g. a static picture or slideshow, and whether the Desktop contained any hidden items.

ARTIFACT INFORMATION

User Account	The user account this desktop is associated with.
Wallpaper Path(s)	The path of the wallpaper's files on the computer.
Background Type	The type of displayed background, picture, slideshow, or single color.
Monitor Identifier	An identifier for which monitor is displaying this desktop.
Display Configuration	What type of configuration is used, either single or multiple displays.
Hidden Items	Whether or not there are hidden items on the desktop.

The date/time displayed within the taskbar is reflecting the time in which AXIOM processed the evidence item producing this artifact. For more information, please reference the Knowledge Base article: <https://support.magnetforensics.com/s/article/Artifact-profile-Rebuilt-Desktops>

MODULE REVIEW

In this module the following topics were covered:

- The purpose of the REFINED RESULTS categories and where the information is compiled from.
- The content of some of the REFINED RESULTS, such as Google Searches, Parsed Search Queries, Cloud Services URLs, Classifieds URLs, Social Media URLs, and Identifiers.
- How to create a Profile using information contained in the Identifiers category.
- How to sort and filter artifacts.
- How to filter artifacts pertaining to only specific Identifiers using a Profile.
- Accessing the built-in help resources such as the User Guide and Artifact Reference.

REVIEW QUESTIONS

To help reinforce the learning objectives for this module, the following review questions have been provided.

1. What is the purpose of the REFINED RESULTS artifact categories?
2. Explain the difference between the Google Searches and Parsed Search Queries artifacts.
3. What REFINED RESULTS artifacts are used to create a Profile?
4. Name at least three sources of information for the Identifiers artifacts.
5. What resource lists the various artifacts searched for by AXIOM and the meanings of the column values?



STUDENT EXERCISE

This exercise is based on the Dashner case scenario from Module 1.

- In the Artifacts drop-down on the FILTERS bar, type the word “search” into the *Find...* box at the top.
- Select the Google Searches and Parsed Search Queries artifact categories and click **OKAY**.
- The MATCHING RESULTS only contains these two categories.
- In the search box on the FILTERS bar, type “pup” and click **GO**.
- Select the REFINED RESULTS → Google Searches category.
- Locate the Artifact column, right-click the column title and select Filter on column.
- Select the Advanced tab, and in the SEARCH BY TERM, leave the search as Include and enter the search term “Chrome”.
- Click **ADD ANOTHER TERM** and Include the search term “Firefox”.
- Change the search logic to OR, and click **SEARCH**.
- Select the first result and Expand the TAGS, PROFILES & MEDIA CATEGORIES pane.
- In the TAGS card, click **ADD NEW TAG**.
- Name the TAG “Puppy Searches – Google” and click **OKAY**.
- Click on the second result, and select the remaining results using the Shift key.
- Right-click on the selected records, select Add / remove tag, and apply the newly created “Puppy Searches – Google” tag to the results.
- Click the down arrow  next to the Artifact contains “chro... on the FILTERS bar and select **REMOVE FILTER**.
- This removes just the column filter but leaves the remaining filter criteria in place.
- Select the Parsed Search Queries category.
- In the TAGS, PROFILES & MEDIA CATEGORIES pane, create a TAG named “Puppy Searches – YouTube” for the YouTube results.
- Highlight the first “YouTube” result, press **Ctrl+A**, to highlight all of the results.
- Right-click the highlighted results, select Add / remove tag and apply the newly created tag to the YouTube results.

- Select the first tagged YouTube result.
- On the TAGS, PROFILES & MEDIA CATEGORIES pane, in the COMMENTS card, click **ADD COMMENT**.
- Enter a comment with your initials, followed by “Puppy video from YouTube” and click **OKAY**.
- Click the X beside the keyword “pup” on the FILTERS bar.
- Filter the Search Term column:

How many Parsed Search Queries are there with a Search Term “pet”?

Which Search Engine was used to conduct these searches?

- Apply a TAG “Pet Related Searches – Facebook” to these results.
- Clear all filters.

ADVANCED SEARCHING AND FILTERING

- In the Artifacts drop-down on the FILTERS bar, select Google Searches and Parsed Search Queries and click **OKAY**.
- In the Keywords lists drop-down on the FILTERS bar, review the keywords and note the number in parenthesis.
- Select the keyword “dog” and click **OKAY**.

How many Parsed Search Queries results are there for “dog”?

- Uncheck the keyword “dog”, and select the keyword “pup” and click **OKAY**.

How many Google Searches results are there for “pup”?

- Create appropriate TAGS and apply them to the results.
- Return to the Keyword lists drop-down menu on the Filter bar and select both the “dog” and “pup” keywords.

How many Google Searches results are there with both keywords selected?

- Return to the Keyword lists drop-down menu on the Filter bar and select **RESET**.



- Enter “dog” in the Search box of the FILTERS bar and click **GO**.
- Enter “pup” in the Search box of the FILTERS bar and click **GO**.

When both keywords are applied at the same time, how many artifacts are found?

- Why is there a difference in the results? _____
- Clear all filters.

NOTE: Multiple search terms selected from the Keyword lists drop-down of the FILTERS bar list use OR logic by default. Multiple search terms entered using the Search box on the FILTERS bar use AND logic by default.

CREATING AND USING PROFILES

- From the Profiles drop-down on the FILTERS bar, click **MANAGE PROFILES**.
- Click **ADD PROFILE**, name the profile “Isaiah Dashner” and click **ADD**.
- Click **OKAY** to close the Manage profiles window.
- Select the REFINED RESULTS → Identifiers-People category.
- Right-click on the Identifier column and select Filter on column.
- Enter “Isaiah” and click **SEARCH**.

How many Identifiers result from using “Isaiah” as a filter?

- Link these Identifiers to the Isaiah Dashner Profile.
- Click the down arrow  next to Identifier **contains** on the Filters bar and replace “Isaiah” with “Dashner”, then click **SEARCH**.

How many Identifiers result from using “Dashner” as a filter?

- Click down arrow  next to Identifier **contains** on the Filters bar and replace “Dashner” with “isaia”, then click **SEARCH**.

Note: “isaia” was the value listed for the Windows user account associated with Isaiah Dashner on the Windows 10 computer.

- Link these Identifiers to the Dashner Profile.
- Clear the filter and using the Profiles drop-down on the FILTERS bar, filter the case using the Dashner profile.

How many matching results are displayed?

Notes

Notes





MAGNET
FORENSICS®

MODULE 6:

Web Related

LEARNING OBJECTIVES

In this lesson, students will take part in lecture, instructor-led exercises, and student practical exercises to gain an understanding of browser related artifacts and the databases used by browsers to store information such as browser history, typed URLs, bookmarks, download activity, and cached files.

GOALS

At the conclusion of this lesson, students will be able to identify and discuss the different artifacts associated with the most common browser applications and be able to use Magnet AXIOM to conduct examinations of web related artifacts. The student will be introduced to a possible workflow for investigation web related investigations and will also gain an understanding of how to use source linking to gain access to the browser databases.

WEB RELATED ARTIFACTS

AXIOM Process searches for and processes artifacts generated by the following browsers:

 Chrome Web History	544
 Chrome Web Visits	844
 Chrome/360 Safe Browser/Opera Carv...	52
 Edge Cache Data	819
 Edge Last Session	7
 Firefox Bookmarks	25
 Firefox Cache Records	9,891
 Firefox Cookies	762
 Firefox Downloads	12
 Firefox FavIcons	48
 Firefox FormHistory	4
 Firefox Input History	1
 Firefox SessionStore Artifacts	191
 Firefox Web History	735
 Firefox Web Visits	375
 Flash Cookies	66
 Google Analytics First Visit Cooki...	176
 Google Analytics Referral Cooki...	132
 Google Analytics Session Cooki...	138
 Google Analytics URLs Carved	17
 Google Maps	11
 IE InPrivate/Recovery URLs	7
 Internet Explorer 10-11 Content	5,664
 Internet Explorer 10-11 Cookies	279
 Internet Explorer 10-11 Daily/Wee...	50
 Internet Explorer 10-11 Dependen...	83

- 360 Safe Browser
- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Internet Explorer 10-11Internet Explorer Legacy versions (version 9 and earlier)
- Opera
- Apple Safari
- XBOX 360 Internet Explorer
- More than 20 browsers specific to mobile devices
- Android, iOS, Kindle, and Windows Phone

Figure 6.1 WEB RELATED category



This information is populated into the various categories within WEB RELATED and is grouped together by browser.

In addition, browser artifacts such as Google Analytics, Google Toolbar, Malware/Phishing URLs, eBay, Social Media, Classified Ads, and Searches are also identified and compiled into the various REFINED RESULTS categories.

AXIOM Examine provides various viewing options for artifacts generated from browsing activity.

WHICH BROWSERS ARE IN PLAY?

Most cases will involve multiple browsers. While modern Windows systems typically use the Edge browser, they also have the older Internet Explorer browser which may generate artifacts as well. However, neither of these browsers are the most common browser that is currently on the desktop platform. According to www.statcounter.com, the Google Chrome browser is the most popular browser used worldwide, followed by Safari.

For more information on what browser is currently in the lead on the desktop platform, please refer to: <https://gs.statcounter.com/browser-market-share/desktop/worldwide>.

Microsoft has also moved away from the legacy version of the Edge browser in modern Windows 10 systems in favor of a Chromium-based version of Edge. This Chromium engine uses the same functionality of the Google Chrome browser, but is skinned specifically for Edge. The Chromium engine is commonly used by many third-party browsers, such as the Brave browser.

BROWSER ARTIFACT HIERARCHY

Because there are many different types of browser artifacts, it is important to have a workflow while working through the artifacts. Each artifact displays different information within the Evidence pane, if one artifact does not have the data an examiner seeks, another artifact may allow them to recover some of the data. Depending on the case, some web related artifacts may be more important than others.

Some cases may find that the download of a specific program is key, while others may be more focused on what bookmarks are saved. Some investigations may focus more on what has been browsed to or what may be cached. Thanks to the way our browsers function, an examiner may find key artifacts within the browser cache. In each case, the order of operations in working through these artifacts may change, but this specific workflow is one efficient way to locate data within AXIOM.

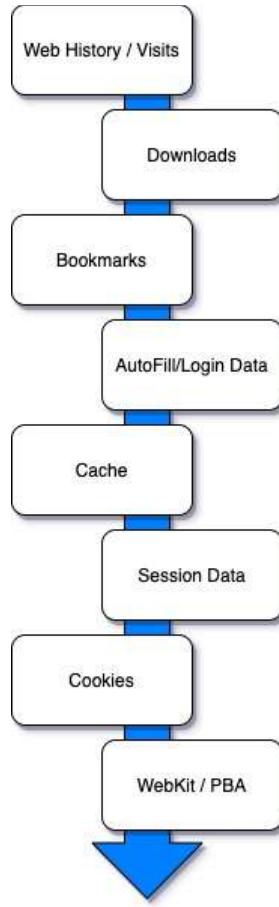


Figure 6.2 A suggested browser workflow

HISTORY – GOOGLE CHROME

Google Chrome can be configured with multiple browsing profiles, the first of which is named “Default”. Any additional profiles created will be named “Profile1”, “Profile2”, etc. The browser activity generated while a profile is in use is kept separate and discreet from the others in a subfolder named after the profile. These subfolders are stored in the following location:

`\Users\<username>\AppData\Local\Google\Chrome\User Data\`

So, the user data relating to the default profile is located at:

`\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\`

The Chrome browser history is stored in an SQLite database named **History** (note that this file has no extension). There are three database tables that store the history information: **urls**, **visits**, and **visit_source**. The **urls** table is a list of each unique URL stored in the database. The **visits** table contains a list of each time the browser has visited a URL, regardless of whether the URL has been accessed multiple times. The records contained in the **visits** table do not detail the URL accessed, but instead

contain a field **url** that cross-references the **urls** table. The **visit_source** refers to how each individual visit came to be in the database. The records in the **visit_source** table contain a field **id** that cross-references the **visits** table. A SQLite database is said to be a relational database because of these connected references.

DETAILS

ARTIFACT INFORMATION

- URL: https://www.youtube.com/results?search_query=nostalgia+critic
- Last Visited Date/Time: 23/08/2019 17:29:52
- Title: nostalgia critic - YouTube
- Visit Count: 2
- Typed Count: 0

EVIDENCE INFORMATION

- Source: DashnerWin10PC.E01 - Partition 1 (Microsoft NTFS, 59.56 GB)\Users\dashner\AppData\Local\Google\Chrome\User Data\Default\History
- Location: Table: urls(id: 68)
- Evidence number: DashnerWin10PC.E01

Figure 6.3 Chrome Web History artifact sourced from urls table

DETAILS

ARTIFACT INFORMATION

- URL: https://www.youtube.com/results?search_query=nostalgia+critic
- Date Visited Date/Time: 23/08/2019 17:29:52
- Title: nostalgia critic - YouTube
- Typed Count: 0
- Transition Type: LINK

EVIDENCE INFORMATION

- Source: DashnerWin10PC.E01 - Partition 1 (Microsoft NTFS, 59.56 GB)\Users\dashner\AppData\Local\Google\Chrome\User Data\Default\History
- Location: Table: visits(id: 81)
- Table: urls(id: 68)
- Evidence number: DashnerWin10PC.E01

Figure 6.4 Chrome Web Visits artifact sourced from urls and visits tables

The information from the **urls** table is extracted by AXIOM Process and placed in the WEB RELATED → Chrome Web History category, as shown in Figure 6.3, and the information from the **visits** table is extracted by AXIOM Process and placed in the WEB RELATED → Chrome Web Visits category (Figure 6.4). The records extracted from the **visits** table are cross-referenced with the **urls** and **visit_source** tables and the DETAILS card lists which records from each table have been used to compile the artifact, also shown in Figure 6.4.

The DETAILS card on the DETAILS pane of an artifact in the Chrome Web History category includes the following information:

ARTIFACT INFORMATION

URL	The URL visited.
Last Visited Date/Time	The date and time the URL was last visited.
Title	The title of the webpage as it appears in the browser's title bar/tab.
Visit Count	How many times the URL has been accessed.
Typed Count	The number of times Chrome deems this was a Typed URL. Typed URLs will be covered in more detail in a later section of this module.

EVIDENCE INFORMATION

Source	The directory path (including file name) where the artifact was found.
Location	The location of the data within the source file or object. If the artifact is not sourced from a database, the offset from the beginning of the file or object is listed.

The DETAILS card on the DETAILS pane of an artifact in the Chrome Web Visits category also includes:

ARTIFACT INFORMATION

Transition Type	How the browser navigated to the website.
Visit Source	The source of the visit entry in the database.

The possible values for the Transition Type are:

LINK	The user clicked a link in another page.
AUTO_TOPLEVEL	Any content that is automatically loaded in a top-level frame, e.g. opening the dev tools window, or opening web-based dialog boxes. It can also be the page passed to the command line.
AUTO_SUBFRAME	Any nested subframe that is loaded automatically by the parent page. This is often seen where frames contain ads – the ad URLs will have this transition type.
MANUAL_SUBFRAME	Any nested subframe that is loaded as a result of an explicit action by the user and generates new navigation entries in the back/forward page navigation list.
GENERATED	The user started typing in the address bar, then selected an entry that did NOT look like a URL. These are discrete from Typed URLs as the suggestion did not look like a URL. E.g. the entry in the database might be the URL of a google search but the user had typed Vikings in the address bar and selected the suggested entry “vikings – Google Search”.
KEYWORD	The URL was generated from keyword search configured by the user. This search might also generate an additional visit with a transition type of KEYWORD_GENERATED. If the user enters a search for “Wikipedia” the generated URL has a transition type of KEYWORD; a second URL for “wikipedia.org” with a transition type of KEYWORD_GENERATED might also be created.



KEYWORD_GENERATED	Corresponds to a visit generated for a keyword. See description of KEYWORD above.
FORM_SUBMIT	The user filled out values in a form and submitted it. NOTE: in some situations, such as when a form uses a script to submit its content, submitting a form does not result in this transition type.
RELOAD	The user reloaded the page using either the reload/refresh button or pressing enter in the address bar. This transition type is also used for session restore when reopening closed tabs.
TYPED	The user either entered the URL into the address bar or selected a URL from the autocomplete suggestions offered. This type is not used if the user selected a choice that didn't look like a URL; see GENERATED above.
AUTO_BOOKMARK	The user selected an entry from the User Interface. This includes bookmarks, or items in the browser history.

The possible values for the Visit Source are:

Synced	Synchronized from somewhere else.
User Browsed	User browsed will display Local.
Extension	Added by an extension.
Firefox Import	Imported from Firefox.
IE Import	Imported from Internet Explorer.
Safari Import	Imported from Safari.

RUNNING EXERCISE

CHROME HISTORY

- From the Artifacts explorer in AXIOM Examine, select the WEB RELATED → Chrome Web History category.
- Filter on the Title column for “pet”.
- Highlight the entry that begins “Ultimate FUNNY DOGS & CUTE PUPPIES of 2018”.
- The Source details this artifact has been extracted from the **History** database.
- It has been extracted from the **urls** table, record id **306**.

- Click the Source Link.
- This will switch to the File system explorer with the **History** database file selected and its contents displayed in the **SQLITE VIEWER** within the **DETAILS** pane.
- From the **Select table** drop-down menu, choose the **urls** table and locate record id **306**.
- The record details the URL and Title of the webpage, the Visit Count, and the Last Visited Date/Time.
- It also includes how many times Chrome deems this URL was Typed.
- This table of the database only details the last time the URL was accessed.
- Locate the `last_visit_time` field and record the content. _____
- Open the **Magnet Timestamp Converter** utility in the **\Tools** folder on the Desktop.
- In the Input field, type in the numerical timestamp value from previous step.
- Change the Format to GoogleChrome and click **Convert**.
- The decoded value matches the information displayed in AXIOM Examine.
- Return to the Artifacts explorer. Your **Title** column filter for “**pet**” should still be applied.
- Select the **WEB RELATED** → **Chrome Web Visits** category.
- Sort by **Title** and locate the same record we examined in the **Chrome Web History** artifact category, “Ultimate FUNNY DOGS & CUTE PUPPIES of 2018”.
- The Location lists the **urls** table record **id 306** again.
- It also lists the **visits** table record **id 409**.
- Click the Source link again to transition to the File system explorer and review the **History** SQLite database.
- View the **visits** table and locate record **id 409**.
- The **url** field contains **306**, the record just viewed in the **urls** table.

HISTORY – MOZILLA FIREFOX

Like Chrome, Firefox can also be configured with multiple browsing profiles, the first of which is named “default”. Any additional profiles created will be named using the profile name provided by the user. The



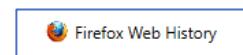
browser activity generated while a profile is in use is kept separate and discreet from the others in a subfolder named **xxxxxxxx.<profile name>**, where **xxxxxxxx** is a randomly generated alpha-numeric value prepended to the profile name. Most of the data is stored within the user's roaming profile and the subfolders are stored in the following location:

\Users\<username>\AppData\Roaming\Mozilla\Firefox\Profiles

So, the user data relating to the default profile (version 67 and later) is located at:

\Users\<username>\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxx.default-release

The Firefox browser history is stored in an SQLite database named **places.sqlite**. There are two database tables that store the history information: **moz_places**, and **moz_historyvisits**. The **moz_places** table is a list of each unique URL stored in the database and the **moz_historyvisits** table contains a list of each time the browser has visited a URL, regardless of whether the URL has been accessed multiple times. The records contained in the **moz_historyvisits** table do not detail the URL accessed, but instead contain a field **place_id** that cross-references the **moz_places** table.



DETAILS

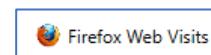
ARTIFACT INFORMATION

URL	https://www.screensaversplanet.com/screensavers/themes/dogs	
Last Visited Date/Time	13-Sep-19 7:30:13 PM	
Title	13 Dog Screensavers for Windows	
Visit Count	1	
Is Typed	No	

EVIDENCE INFORMATION

Source [Dashner Win10 PC.E01 - Partition 2 \(Microsoft NTFS, 49.43 GB\)\Users\isaia\AppData\Roaming\Mozilla\Firefox\Profiles\kcd9nxhs.default-release\places.sqlite](#)

Figure 6.5 Firefox Web History artifact sourced from *moz_places* table



DETAILS

ARTIFACT INFORMATION

URL	https://www.screensaversplanet.com/screensavers/themes/dogs	
Title	13 Dog Screensavers for Windows	
Date Visited Date/Time	13-Sep-19 7:30:13 PM	
Is Typed	No	

EVIDENCE INFORMATION

Source [Dashner Win10 PC.E01 - Partition 2 \(Microsoft NTFS, 49.43 GB\)\Users\isaia\AppData\Roaming\Mozilla\Firefox\Profiles\kcd9nxhs.default-release\places.sqlite](#)

Figure 6.6 Firefox Web Visits artifact sourced from *moz_places* and *moz_historyvisits* tables

The information from the **moz_places** table is extracted by AXIOM Process and placed in the WEB RELATED → Firefox Web History category, as shown in Figure 6.5 and the information from the **moz_historyvisits** table is extracted by AXIOM Process and placed in the WEB RELATED → Firefox Web Visits category (Figure 6.6). The records extracted from the **moz_historyvisits** table are cross-referenced with the **moz_places** table and the DETAILS card lists which records from each table have been used to compile the artifact, also shown in Figure 6.6.

The DETAILS card on the DETAILS pane of an artifact in the Firefox Web History category includes the following information:

ARTIFACT INFORMATION

URL	The URL visited.
Last Visited Date/Time	The date and time the URL was last visited.
Title	The title of the webpage as it appears in the browser's title bar/tab.
Visit Count	How many times the URL has been accessed.
Is Typed	A Boolean value detailing whether Firefox deems this URL has ever been Typed. Typed URLs will be covered in more detail in a later section of this module.

The possible values for the Transition Type are:

TRANSITION_LINK	User clicked on a link
TRANSITION_TYPED	User typed the URL into the address bar
TRANSITION_BOOKMARK	User clicked on a bookmark for the website
TRANSITION_EMBED	Content within a webpage was loaded (this would include imbedded images)
TRANSITION_REDIRECT_PERMANENT	Transition was a permanent redirect
TRANSITION_REDIRECT_TEMPORARY	Transition was a temporary redirect
TRANSITION_DOWNLOAD	A download link was clicked on

For more information on the Transition Types used by Mozilla and other browsers, please reference this link:

<https://developer.mozilla.org/en-US/docs/Mozilla/Add-ons/WebExtensions/API/webNavigation/TransitionType>

RUNNING EXERCISE

FIREFOX HISTORY

- From the Artifacts explorer in AXIOM Examine, select the WEB RELATED → Firefox Web History



category.

- Sort the Title column.
- Highlight the entry – “13 Dog Screensavers for Windows”.
- The artifact has been extracted from the **moz_places** table and the record id is **25**.
- The record details the URL and Title of the webpage, the Visit Count, and the Last Visited Date/Time.
- It also includes whether Firefox deems the URL was ever Typed.
- Switch to the **WEB RELATED** → Firefox Web Visits category.
- Sort by Title and locate the same record as before “13 Dog Screensavers for Windows”.
- The Location lists the **moz_places** table record id **25** again.
- It also lists the **moz_historyvisits** table record id **25**.

HISTORY – MICROSOFT INTERNET EXPLORER & EDGE

Microsoft Internet Explorer v9 and previous versions stored their browsing history in **Index.dat** files stored within the user profile in the following location:

\Users\<username>\AppData\Local\Microsoft\History\History.IE5

Internet Explorer v10 and v11 and Edge browsers stored their browsing history data in an Extensible Storage Engine (ESE) database, also commonly known as a “Jet Blue” database, named **WebCacheV01.dat** stored in the following location:

\Users\<username>\AppData\Local\Microsoft\Windows\WebCache

Internet Explorer v10 and v11 and Edge stored these histories as separate tables within the **WebCacheV01.dat** file. Older versions of Internet Explorer store them in separate **Index.dat** files contained within the **\History.IE5** folder detailed above.

Internet Explorer creates a new daily history the first time the browser is used after midnight each day. It contains the browsing history for a 24-hour period from midnight to midnight. The daily histories are stored in either a folder (older versions of IE) or a table (IE 10-11) named **MSHist01yyyymmddyyyymmdd**, where the first date is the start and the second date is the end of the history period, e.g. **MSHist012016101320161014**. In this example, the daily history file contains browsing activity from midnight on 13 Oct 2016 to midnight on 14 Oct 2016.

The first time Internet Explorer is used after midnight on a Monday, any daily histories are moved into a weekly history and the daily histories are either deleted (Index.dat files) or marked as defunct (WebCacheV01.dat tables). Each weekly history therefore contains browsing history for a seven-day period from 00:00:00 on Monday to 23:59:59 on Sunday. The weekly histories are also stored in either a folder or table named using the start and end date of the history period, e.g. **MSHist012016101020161017**. In this example the weekly history file contains browsing activity from midnight on 10 Oct 2016 to midnight on 17 Oct 2016.

Although Internet Explorer v10 and v11 store the history in the **WebCacheV01.dat** database, they also store a zero-byte file named **container.dat** in the relevant daily and weekly folders in place of the old **index.dat** file.

The cumulative history is created at the same time as the daily history and is simply stored in the History folder or table.

NOTE: The date and time information of Internet Explorer Daily and Weekly history is recorded in local time. The date and time information of Main history is recorded as UTC.

In AXIOM Examine, the three histories from Internet Explorer 10-11 are populated into two WEB RELATED categories: Internet Explorer 10-11 Main History, and Internet Explorer 10-11 Daily/Weekly History.

The three histories from older versions of Internet Explorer are populated into the two WEB RELATED categories: Internet Explorer Main History, and Internet Explorer Weekly History.

The cumulative main history is created at the same time as the daily history, so it is not unusual to see duplicate entries across these two categories – Daily/Weekly and Main.

Edge also stores its browser history in the **WebCacheV01.dat** stored in the folder:

\Users\username\AppData\Local\Microsoft\Windows\WebCache

This is the same database used by Internet Explorer (versions 10 and 11), however, there are separate tables within the database for the Internet Explorer Main, Daily, and Weekly Histories and the Edge History.

As Edge uses the same database as Internet Explorer v10-11, AXIOM Examine cannot determine whether the information in the **WebCacheV01.dat** file has been written by Internet Explorer v10-11 or Edge. Additionally, Edge does not store Main, Daily and Weekly histories in quite the same way, so all Edge browsing history is contained within the category WEB RELATED → Internet Explorer v10-11 Main History. It is therefore the responsibility of the examiner to determine which browser generated artifacts within this category if entries are of importance to the investigation, and this will be covered during the practical exercise that follows.



The DETAILS card on the DETAILS pane of an artifact in the Internet Explorer 10-11 Main History category includes the following information:

ARTIFACT INFORMATION

URL	The URL accessed by the browser.
User	The local Windows username.
Accessed Date/Time	The most recent visit to the URL.
Page title	The title of the webpage as it appears in the browser's title bar/tab.
Access Count	It is unclear all the actions that trigger this counter, but it is not necessarily the number of times the URL has been accessed.

EVIDENCE INFORMATION

Source	The directory path (including file name) where the artifact was found.
Location	The location of the data within the source file or object.

ARTIFACT INFORMATION	
Entry ID	100
URL	https://www.dropbox.com/home/old%20flash%20drive%20pics/pics%20to%20share
User	isaia
Accessed Date/Time	10-Sep-19 7:54:55 PM
Page Title	pics to share - Dropbox
Access Count	2
Browser Source	C:\Users\isaia\AppData\Local\Packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\#001\MicrosoftEdge\History

EVIDENCE INFORMATION	
Source	Dashner Win10 PC.E01 - Partition 2 (Microsoft NTFS, 49.43 GB)\Users\isaia\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat

Figure 6.7 Edge browser history listed as Internet Explorer 10-11 Main History

DOWNLOADS

Most browsers track information regarding file downloads and AXIOM Examine displays this information in categories specific to each browser.

CHROME

Chrome tracks download activity in the **History** database file stored in the profile folder. Therefore, for the default profile this file is stored in the following location:

\Users\<username>\AppData\Local\Google\Chrome\User Data\Default

The information is contained within two tables: **downloads** and **downloads_url_chains**, and the information from these tables is extracted by AXIOM Process and placed in the WEB RELATED → Chrome Downloads category,

The DETAILS card on the DETAILS pane includes the following information:

ARTIFACT INFORMATION

Download Source	The source URL of the downloaded file.
File Name	The name given to the file when it was saved to the local machine.
Start Time Date/Time	The date and time the download started.
End Time Date/Time	The date and time the download completed or stopped.
Saved To	The local path and filename where the file was saved.
State	Indicates whether the download completed successfully.
Opened by User	Indicates whether the file was opened by clicking the link at the bottom of the browser after download completed.
Bytes Downloaded	The number of bytes of the file downloaded.
File Size (Bytes)	The size of the fully downloaded file.

FIREFOX

Firefox tracks download activity in the **places.sqlite** database that stores the browsing history. The file is stored in the profile folder, so for the default profile this file is stored in the following location:



\Users\<username>\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxx.default-release

The information is contained within two tables: **moz_places** and **moz_anno**s, and the information from these two tables is extracted by AXIOM Process and placed in the WEB RELATED → Firefox Downloads category,

The DETAILS card on the DETAILS pane includes the following information:

ARTIFACT INFORMATION

File Name	The name given to the file when it was saved to the local machine.
Download Source	The source URL of the downloaded file.
Start Date/Time	The date and time the download was started.
End Date/Time	The date and time the download completed or stopped.
Saved To	The local path and filename where the file was saved.
Temp Path	The local path and filename where the file was temporarily stored during download, if applicable.
State	Indicates the download status: Download Complete, Download in Progress, Download Stopped, or Download Paused.
Referrer	If the webpage used a mirror for downloading, the path to the original download URL.
Bytes Downloaded	The number of bytes of the file downloaded.
File Size (Bytes)	The size of the fully downloaded file.

INTERNET EXPLORER AND EDGE

Internet Explorer v10-11 and Edge track download activity in the **WebCacheV01.dat** file that stores the browsing history. The file is stored in the folder:

\Users\<username>\AppData\Local\Microsoft\Windows\WebCache

For the same reasons previously discussed during the browser history section, AXIOM Examine displays download information extracted from both IE v10-11 and Edge in the WEB RELATED → Internet Explorer 10-11 Downloads category.

The DETAILS card on the DETAILS pane includes the following information:

ARTIFACT INFORMATION

URL	The source URL of the downloaded file.
-----	--

Last Accessed Date/Time	The date and time the download URL was last accessed.
Redirect URL	The previous URL which led the user to the download URL.
Download Location	The local path and filename where the file was saved.
Temp Download Location	The local path and filename where the file was temporarily stored during download. This is usually one of the cache folders.

RUNNING EXERCISES

CHROME DOWNLOADS

- From the **Artifacts** explorer in AXIOM Examine, clear any filters you may have in place.
- Select the WEB RELATED → Chrome Downloads category.
- Sort the File Name column and highlight the entry for the file “Pictures.7z”.
- The Download Source details the name of the file downloaded as “Pictures.7z” which appears to be a URL associated with Google Drive.
- The Saved To field details the file was saved to the local machine as **Pictures.7z** in the isaia Windows user account’s **\Downloads** folder.
- The download completed successfully, and the file was opened by the user.
- Note the record ID from the Downloads table. _____
- Tag this information as “Pictures.7z Download”

BOOKMARKS

Bookmarks, or Favorites, are used to mark websites for later return. They are often used for sites that are visited most frequently, or sites for which a user might need to quickly return. Every browser can create bookmarks, and these can provide useful information from an investigative standpoint. Most browsers can also save bookmarks in a tree-like structure within the bookmark folders.

CHROME

Chrome stores its bookmarks in a plain text JavaScript Object Notation (JSON) file named **Bookmarks**. The file is stored in the profile folder, so for the default profile the file is stored in the following location:

\Users\<username>\AppData\Local\Google\Chrome\User Data\Default



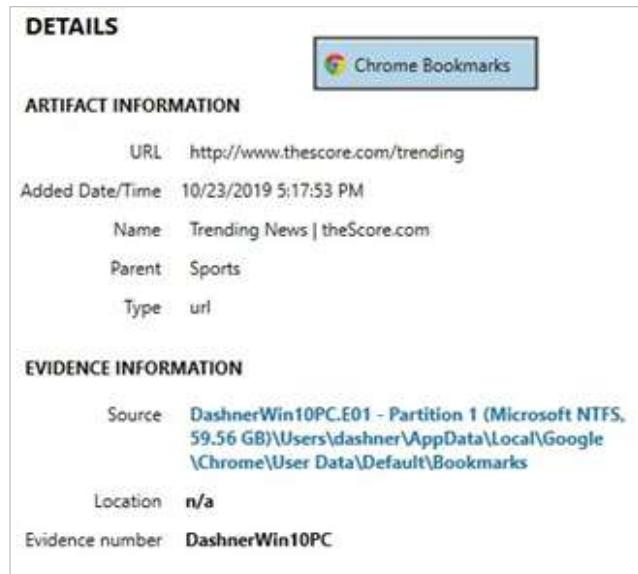


Figure 6.8 Chrome Bookmarks

The DETAILS card on the DETAILS pane includes the following information:

ARTIFACT INFORMATION

URL	The URL the bookmark points to.
Added Date/Time	The date and time the bookmark was added to Chrome.
Name	The name of the bookmark or bookmark folder as it appears in Chrome.
Parent	The parent bookmark folder in which the bookmark is located if applicable.
Type	Indicates whether the artifact is a URL or a parent folder.

FIREFOX

Firefox stores Bookmarks in the **places.sqlite** database that stores the browsing history. This file is stored in the profile folder, so for the default profile the file is stored in the following location:

\Users\<username>\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxx.default-release

The information is contained within the tables: **moz_places** and **moz_bookmarks**.

ARTIFACT INFORMATION

URL	https://tools.pdfforge.org/merge-pdf	
Date Added Date/Time	31-Oct-19 6:50:48 PM	
Last Modified Date/Time	31-Oct-19 6:50:53 PM	
Title	https://tools.pdfforge.org/merge-pdf	
Bookmark Type	Bookmark Item	

EVIDENCE INFORMATION

Source	Dashner Win10 PC.E01 - Partition 2 (Microsoft NTFS, 49.43 GB)\Users\isaia\AppData\Roaming\Mozilla\Firefox\Profiles\kcd9nxhs.default-release\places.sqlite	
--------	---	--

Figure 6.9 Firefox Bookmarks

The DETAILS card on the DETAILS pane includes the following information:

ARTIFACT INFORMATION

URL	The URL the bookmark points to.
Date Added Date/Time	The date and time the bookmark was added to Firefox.
Last Modified Date/Time	The date and time the bookmark was last modified.
Title	The name of the bookmark or bookmark folder as it appears in Firefox.
Bookmark Type	Indicates whether the artifact is a Bookmark Item (URL) or a Bookmark Folder.

INTERNET EXPLORER AND EDGE

Internet Explorer and Edge browsers refer to bookmarks as Favorites. Internet Explorer stores Favorites as individual files in the following location:

\Users\<username>\AppData\Favorites

The content of this folder and any subfolders is reflected in the Bookmarks within Internet Explorer, so if the user creates a bookmark folder within Internet Explorer, the folder is also created within the **\Favorites** folder on the disk.

Edge stores Favorites in two possible locations. Early versions of the browser stored Favorites in the folder:

\Users\<username>\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\User\Default\Favorites



Favorites that were migrated to Edge from Internet Explorer upon initial installation might also be found here.

Later versions of Edge moved the Favorites to an ESE database named **spartan.edb** that is stored in the following location:

\Users\<username>\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\User\Default\DataStore\Data\nouser1\120712-0049\DBStore

The entries are stored within the database in a table named **Favorites**.

The DETAILS card on the DETAILS pane for artifacts in the Internet Explorer Favorites category includes the following information:

ARTIFACT INFORMATION

Favorite Name	The name of the favorite as it appears in Internet Explorer.
URL	The URL the favorite points to.
Modified Date/Time	The date and time the favorite was last modified.
User	The user to whom the favorite belongs.
Favorites Root Location	The local path that is the root storage point for the favorite.
Folder Structure	The folder structure under which the favorite will appear in Internet Explorer.
Icon URL	The URL of the icon displayed next to the favorite if an icon exists.

RUNNING EXERCISE

CHROME BOOKMARKS

- From the **Artifacts** explorer in AXIOM Examine, clear any filters you may have in place.
- Select the WEB RELATED → Chrome Bookmarks category.
- Sort the Parent column.
- There are two Bookmark folders present on the Bookmarks bar (Pics and Videos), each containing Bookmarked URLs.
- Highlight the entry for “Cutest Puppies” that is in the “Videos” folder.

- Click the Source link shown for this entry in the DETAILS pane to transition to the File system explorer and review the content of the **Bookmarks** file.
- The DETAILS pane has three cards available which may be of use depending on the file type: the JSON Viewer, the PREVIEW card, and the TEXT AND HEX card. In this example, the **Bookmarks** file contains JSON data which is displayed in the JSON Viewer.
- In the JSON VIEWER, click **FIND**, and search for the text string “date_added”. Note the results are highlighted.
- Scroll down in the **DETAILS** Pane to the TEXT AND HEX card and switch the View to **TEXT**.
- Click **FIND** and search for the Text string “date_added”, pressing F3 on your keyboard will repeat the search and locate the next match.
- Highlight any of the numerical value that follows the “date_added” string, noting that these appear to be similar in format to Google Chrome timestamps seen earlier.
- Change the View back to **HEX** and scroll down to the DECODE card.
- Locate the DATE / TIME section, compare this value with the information seen in the DECODE card of the File System Explorer.

FORM FILL INFORMATION AND SEARCH DATA

Most browsers provide a means to store form information that would commonly be used to fill in basic information on multiple websites, such as name, phone number, address, etc.

Additionally, searches executed using the browser search box, or a search function on a website, will sometimes be stored as form information.

CHROME

Chrome will track a user’s profile once that user has signed into a website that uses a Google account or directly signs into the Chrome browser. This information is part of how Chrome will populate form data based on behalf the user. This information can be found within the Chrome Autofill Profile.



DETAILS

ARTIFACT INFORMATION

Name	Isaiah Dashner	
Number	(501) 237-0855	
Date Modified Date/Time	12-Sep-19 10:44:04 PM	
Address Line 1	250 S Locust	
City	North Little Rock	
State	AR	
Zipcode	72114	
Country	US	

EVIDENCE INFORMATION

Source	Dashner Win10 PC.E01 - Partition 2 (Microsoft NTFS, 49.43 GB)\Users\isaia\AppData\Local\Google\Chrome\User Data\Default\Web Data	
--------	--	--

Figure 6.10 Chrome Autocomplete Profile Information

Chrome refers to form data as “Autocomplete values” and saves them in an SQLite database named **Web Data** stored in the profile folder. Therefore, for the default profile this file will be found in the following location:

\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\

The information is contained within the table: **autocomplete**.

ARTIFACT INFORMATION

Name	Email	Chrome Autocomplete
Date Created Date/Time	8/22/2016 7:01:57 PM	
Value	isaih.dashner	
Count	1	

EVIDENCE INFORMATION

Source	DashnerWin10PC.E01 - Partition 1 (Microsoft NTFS, 59.56 GB)\Users\dashner\AppData\Local\Google\Chrome\User Data\Default\Web Data
Location	Table: autocomplete(rowid: 1)
Evidence number	DashnerWin10PC

Figure 6.11 Chrome Autocomplete

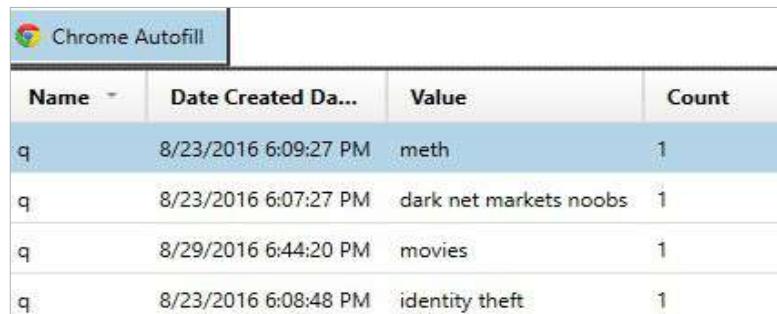
The DETAILS card on the DETAILS pane includes the following information:

ARTIFACT INFORMATION

Name	Name of the autofill field (email, address, etc.).
Date Created Date/Time	The date and time the autofill value was created.
Value	The autofill value stored in the database.
Count	The number of times the autofill value has been used/accessed.

In the example shown in the autofill Value stored in the **Web Data** database is “isaiah.dashner” and has a Count of 1. This Value contains a misspelling of Dashner’s name but to Chrome it does not matter, that is what the user typed and therefore Chrome saved it into the database as is.

Some searches conducted using Chrome are also tracked in the **Web Data** SQLite database. The items generated from searching populate the Name column with a query header. The query header comes from the search engine or website, and for many this is simply a “q”, but it varies depending on the specific site. Figure 6.12 shows search strings contained within the **Web Data** database.

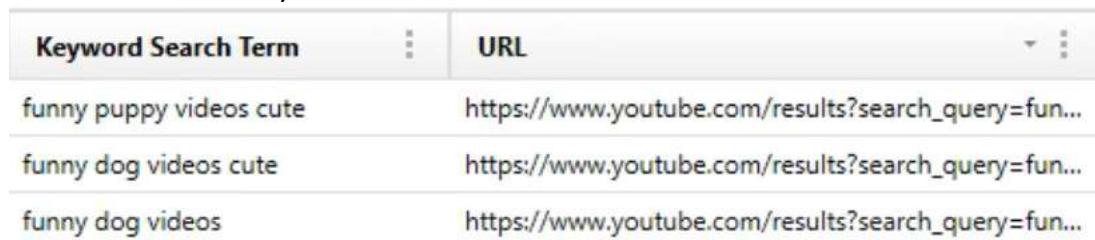


A screenshot of the AXIOM software interface showing a table titled "Chrome Autofill". The table has four columns: "Name", "Date Created Da...", "Value", and "Count". There are four rows of data:

Name	Date Created Da...	Value	Count
q	8/23/2016 6:09:27 PM	meth	1
q	8/23/2016 6:07:27 PM	dark net markets noobs	1
q	8/29/2016 6:44:20 PM	movies	1
q	8/23/2016 6:08:48 PM	identity theft	1

Figure 6.12 Entries in the Chrome Web Data database

Chrome also tracks information on the searches that are performed by the user within the browser’s ‘omnibox.’ As a user types information in the ‘omnibox’, or address bar, searches are captured separately in a table known as **keyword_search_terms** within the **History** database file. AXIOM will render this information as the Chrome Keyword Search Terms artifact.



A screenshot of the AXIOM software interface showing a table titled "Keyword Search Term". The table has two columns: "Keyword Search Term" and "URL". There are three rows of data:

Keyword Search Term	URL
funny puppy videos cute	https://www.youtube.com/results?search_query=fun...
funny dog videos cute	https://www.youtube.com/results?search_query=fun...
funny dog videos	https://www.youtube.com/results?search_query=fun...

Figure 6.13 Keyword search terms from Chrome



FIREFOX

Firefox stores form data in an SQLite database named `formhistory.sqlite` stored in the profile folder. Therefore, for the default profile the file is stored in the following location:

`\Users\<username>\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxx.default-release\`

The information is contained within the table: `moz_formhistory`.

The screenshot shows the Magnet Forensics interface with the 'DETAILS' card open. The card is divided into two sections: 'ARTIFACT INFORMATION' and 'EVIDENCE INFORMATION'. In the 'ARTIFACT INFORMATION' section, there are six data points: Field Name (searchbar-history), Value (when will windows 10 1909 release), First Used Date/Time (29-Oct-19 7:34:08 PM), Last Used Date/Time (29-Oct-19 7:34:08 PM), Times Used (1), and ID (23). Each data point has a small circular icon with a clock symbol to its right. In the 'EVIDENCE INFORMATION' section, there is one entry: Source (Dashner Win10 PC.E01 - Partition 2 (Microsoft NTFS, 49.43 GB)\Users\isaia\AppData\Roaming\Mozilla\Firefox\Profiles\kcd9nxhs.default-release\formhistory.sqlite), which is preceded by a small blue square icon.

Figure 6.14 Firefox Form History

The DETAILS card on the DETAILS pane includes the following information:

ARTIFACT INFORMATION

Field Name	The name of the form field.
Value	The form value stored in the database.
First Used Date/Time	The date and time the field was first used.
Last Used Date/Time	The date and time the field was last used.
Times Used	The number of times the field has been used.
ID	The unique ID of the field. This is essentially a number identifying the order in which the field values were written into the database.

Firefox stores search terms executed via the built-in browser search box in the `formhistory.sqlite` database. As can be seen in Figure 6.15, this usually populates the Field Name with “searchbar- history”. This data can be cross referenced with the Firefox artifacts in WEB RELATED, Parsed Search Queries, and Google Searches to possibly determine the source of the search.

Field N...	Value	First Used Dat...	Last Used Dat...	Time...
searchbar-history	isc2 training	29-Oct-19 7:25:59 PM	29-Oct-19 7:25:59 PM	1
searchbar-history	when will windows 10 1909 release	29-Oct-19 7:34:08 PM	29-Oct-19 7:34:08 PM	1
searchbar-history	big cigars	29-Oct-19 7:42:23 PM	29-Oct-19 7:42:23 PM	1
searchbar-history	synology ds1915+	29-Oct-19 8:14:30 PM	29-Oct-19 8:14:30 PM	1

Figure 6.15 Entries in the Firefox formhistory.sqlite database

INTERNET EXPLORER AND EDGE

Internet Explorer and Edge both store form data in the user registry hive – **NTUSER.DAT**. The information is stored in the registry key:

```
\SOFTWARE\Microsoft\Internet Explorer\Intelliforms\FormData
```

However, the information is encrypted using the Windows Data Protection API, which incorporates the Windows user password. Therefore, the content is not parsed by AXIOM.

RUNNING EXERCISE

CHROME AUTOFILL

- From the **Artifacts** explorer in AXIOM Examine, clear any filters you have applied.
- Select the WEB RELATED → Chrome Autofill category and sort the Date Created Date/Time column.
- Review the artifacts that AXIOM has extracted. There are two entries for “email”, and one for “code” that were accessed within a few minutes of each other. This could be a 2-factor authentication code (2FA) relating to access to the email account listed.
- Select the Chrome Autofill Profiles category and compare the information to this artifact.

FIREFOX FORMHISTORY

- From the **Artifacts** explorer in AXIOM Examine, clear any filters you have applied.
- Select the WEB RELATED → Firefox FormHistory category.
- Reverse-sort on the **Field Name** column.
- Locate the entries with a Field Name “searchbar-history”. This indicates the user searched for “isc2 training”, “when will windows 10 1909 release”, “big cigars”, and “synology ds1915+” using Firefox.
- Scroll through the remaining entries and note the data stored in the Value column. Several URLs



are displayed as part of the form history data showing that Firefox may encapsulate multiple types of information here.

INTERNET BROWSER CACHE

The browser cache is a temporary storage location on the local machine/device. It is used by the browser to store the component parts of a website that has been visited by the user. These files could include HTML files, JavaScript, cascading style sheets (CSS), as well as pictures and other multimedia content. Each time a website is visited, the browser checks to see if the site has been accessed before, and if it has, it checks with the host to ascertain if any content has been updated since the last visit. The browser only downloads files that have either been updated since the last visit or are not already stored in the cache. The purpose of the cache is to reduce network bandwidth usage which reduces the speed at which a webpage will load.

CACHE – CHROME

Chrome stores its cache in three different folder locations, all of which are in the user profile folder. Therefore, for the default profile the cached content is stored in the following locations:

`\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\Cache\`
`\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\GPUCache\`
`\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\Media Cache\`

Which folder a cached component is stored into is dependent on the content. Large media files such as video and audio are saved to the `\Media Cache\` folder; data that can utilize the video card's graphics processing unit are saved to the `\GPUCache\` folder; and everything else, such as HTML files, JavaScript, style sheets, and small graphics, are saved to the `\Cache\` folder.

Each cache folder contains an `index` file and four “block” files named `data_0`, `data_1`, `data_2` and `data_3`.

Name	Type	Size
data_0	File	44 KB
data_1	File	264 KB
data_2	File	1,032 KB
data_3	File	8 KB
index	File	257 KB

Figure 6.16 Sample Chrome cache folder

When a webpage component is stored in the cache, metadata information about the file is also stored. This metadata can include the host site, URL, the HTTP response, and when the file should expire and be deleted from the cache. The file content and its metadata are stored as two separate components; however, both are stored within the same cache folder. Therefore, if a video file is saved to the cache both the file content and the file's metadata will be saved into the **\Media Cache** folder.

If the data to be saved, whether that be the file content itself or its metadata, is less than 16384 bytes in size, it will be saved into one of the block files. Which block file the data is saved into is dependent on the size of the data as per Table 6.1.

Block File	Size of file content or metadata
data_0	Between 0 and 144 bytes.
data_1	Between 144 and 1024 bytes.
data_2	Between 1024 and 4096 bytes.
data_3	Between 4096 and 16384 bytes.

Table 6.1 Chrome cache block file data allocation

If the data to be saved is larger than 16384 bytes it is saved into an individual file named **f_0000xx** where **xx** is a hexadecimal value that simply increases by 1 for each new file written to the cache folder.

Consequently, small files, such as PNG or GIF files, are usually stored within one of the block files. Most large media files, such as videos, are stored as individual “f” files and most file metadata is found in the **data_1** block file.

The **index** file within the same cache folder stores the cross-reference between the cached file's content and its metadata.

Because the file content and metadata are tracked independently AXIOM Examine displays two EVIDENCE INFORMATION sections. The first details the Source and Location information of the metadata component. The second details the Source and Location for the data content of the cached file. The example shown in Figure 6.17 Chrome Cache RecordsFigure 6.17 is a small PNG file which has been saved to the **\Cache** folder. The metadata information is stored in the **data_1** block file so, from Table 6.1, must be between 144 and 1024 bytes in size. The actual PNG file content is stored in the **data_3** block file so, from Table 6.1, must be between 4096 and 16384 bytes in size. Reviewing the Content Size (Bytes) in the ARIFACT INFORMATION confirms the file size is 5969 bytes.



PREVIEW

The screenshot shows a digital forensic interface. At the top, there's a preview window displaying the Google logo. Below it, a "ZOOM 100%" button is visible. The main area is titled "DETAILS". Under "ARTIFACT INFORMATION", it lists the URL as https://www.google.com/images/branding/googlelogo/2x/googlelogo_color_92x30dp.png. It also shows the first visited date/time as 8/30/2019 8:54:12 PM, last visited date/time as 9/12/2019 10:31:22 PM, and last synced date/time as 8/30/2019 8:55:26 PM. The file type is listed as "png" and the content size as 3831 bytes. Under "EVIDENCE INFORMATION", it shows the source as "Dashner Win10 PC.E01 - Partition 2 (Microsoft NTFS, 49.43 GB)\Users\isaia\AppData\Local\Google\Chrome\User Data\Default\Cache\data_1" and the recovery method as "Parsing". A note indicates "Deleted source".

ARTIFACT INFORMATION

URL https://www.google.com/images/branding/googlelogo/2x/googlelogo_color_92x30dp.png

First Visited Date/Time 8/30/2019 8:54:12 PM

Last Visited Date/Time 9/12/2019 10:31:22 PM

Last Synced Date/Time 8/30/2019 8:55:26 PM

File Type png

Content Size (Bytes) 3831

EVIDENCE INFORMATION

Source Dashner Win10 PC.E01 - Partition 2 (Microsoft NTFS, 49.43 GB)\Users\isaia\AppData\Local\Google\Chrome\User Data\Default\Cache\data_1

Recovery Method Parsing

Deleted source

Figure 6.17 Chrome Cache Records

The DETAILS card on the DETAILS pane includes the following information:

ARTIFACT INFORMATION

URL	The URL of the cached item.
First Visited Date/Time	The date and time the URL was first visited.
Last Visited Date/Time	The date and time the URL was last visited.
Last Synced Date/Time	The date and time the cached item was last synced with the website.
File Type	The type of file that was cached.
Content Size (Bytes)	The size of the cached item in bytes.

RUNNING EXERCISE

CHROME CACHE

- From the **Artifacts** explorer in AXIOM Examine, clear any filters you may have in place.
- Select the **WEB RELATED** → Chrome Cache Records category.
- Right-click the Content Size (Bytes) column and select Filter on column.
- This column contains numerical information so the filter that can be applied is: A range, Equal to, Less than or equal to, or More than or equal to.
- Select A range, and filter for files between 1500 and 2000 bytes in size.
- Sort the Content Size (Bytes) column and locate the JPEG file that is 1708 bytes in size.
- This is a picture, so the DETAILS pane includes a PREVIEW of the file.
- Remove the Filter for files between 1500 and 2000 bytes in size.
- Filter on **File Type** column for “jpeg”, then reverse-sort on the **Content Size (Bytes)** column, to place the largest files at the top of the Evidence pane.
- Locate the largest JPEG file that is 2122986 bytes in size.
- Review the EVIDENCE INFORMATION listed in the DETAILS pane.
- Clear any filters you have applied.
- From the Artifacts drop-down on the FILTERS bar, select only the Chrome Cache Records and Pictures categories.
- In the search box on the FILTERS bar, run a search for the Chrome Cache Record filename “**f_000070**” and review the results shown in the NAVIGATION pane under the **WEB RELATED** → Chrome Cache Records and Media → Pictures categories.
- Notice that AXIOM also places media items recovered from web browser cache in the MEDIA → Pictures category.
- Clear all filters and select the Chrome Cache Records artifact again. Using the File Type column, filter on the column for “html”.
- Apply a descending sort on the Content Size (Bytes) column.
- Select a result for amazon.com and review the information displayed in the PREVIEW pane.



CACHE – FIREFOX

Most of the Firefox artifacts are extracted from files stored in the user's **Roaming** profile, but the Firefox cache is located within the user's Local profile. For the default Firefox profile, the cache is located at:

```
\Users\<username>\AppData\Local\Mozilla\Firefox\Profiles\xxxxxxx.default-release\cache2\
```

This folder contains a file named **index**, and two subfolders: **\entries**, and **\doomed**. The index includes information such as when each cached file was written into the cache, and when it will expire. The **\entries** folder contains the cached files themselves and the **\doomed** folder contains expired cached content that is usually deleted by Firefox when the browser closes or the next time it restarts.

Rather than store the file content and the metadata separately as Chrome does, Firefox appends the metadata information to the end of the cached file. The last 4 bytes of the file are a big-endian integer value that details the size of the cached content, and therefore where the metadata content starts within the logical file. In the Artifact explorer, the Content Size (Bytes) field details the size of the cached content only. It is *NOT* the size of the file stored in the Firefox cache folder on the disk/device. The logical file in the cache as displayed in the File system explorer also contains the metadata information, so it will always be larger. AXIOM Process extracts the metadata information from the file and displays it in the DETAILS pane in the Artifacts explorer.

The DETAILS card on the DETAILS pane includes the following information:

ARTIFACT INFORMATION

URL	The URL of the cached item.
Date Created Date/Time	The date and time the file was written to the cache.
MIME Type	The MIME type of the cached item.
Content Size (Bytes)	The size of the cached item in bytes (content only, not the metadata).

Figure 6.18 shows the DETAILS card of a Firefox Cache Records artifact as displayed in the Artifacts explorer.

PREVIEW

ZOOM 36%

DETAILS**ARTIFACT INFORMATION**

URL	https://content-images.p-cdn.com/images/public/int/4/2/1/074643811224_500W_500H.jpg	
Date Created Date/Time	29-Aug-19 6:22:01 PM	
MIME Type	image/jpeg	
Content Size (Bytes)	32158	

EVIDENCE INFORMATION

Source	Dashner Win10 PC.E01 - Partition 2 (Microsoft NTFS, 49.43 GB)\Users\isaia\AppData\Local\Mozilla\Firefox\Profiles\kcd9nxhs.default-release\cache2\entries\00149884C09BBEFBDE4789CC647C0F2B8E0DDAEC	
--------	---	--

Figure 6.18 Firefox Cache record in the Artifact explorer

TEXT AND HEX

View	TEXT	HEX
Source	Users\isaia\AppData\Local\Mozilla\Firefox\Profiles\kcd9nxhs.default-release\cache2\entries\00149884C09BBEFBDE4789CC647C0F2B8E0DDAEC	
Current offset	0	
Current selection	2	
GO TO	FIND	HIDE DECODING
		COPY SELECTION
		SAVE
00000	FF DB FF E0 00 10 4A	ÿØÿà...J
00007	46 49 46 00 01 01 00	FIF....
00014	00 01 00 01 00 00 FFÿ
00021	DB 00 43 00 08 06 06	Û.C....

Figure 6.19 Firefox Cache record in the File System explorer

CACHE – EDGE

Edge stores the metadata information and a cross-reference to the cached file itself in the **WebCacheV01.dat** file located in the folder:



\Users\<username>\AppData\Local\Microsoft\Windows\WebCache

The cached files are stored in the following folder location, where **xxxxxxxx** is a randomly named subfolder:

\Users\<username>\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\Cache\XXXXXXXX

Or subfolders within the same package, but with a number in the folder name.

\Users\<username>\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!001\MicrosoftEdge\Cache\XXXXXXXX

The screenshot shows the Magnet Forensics interface for examining Edge cache records. At the top, there's a preview window showing a person sitting on a couch. Below it, the word "ZOOM 100%" is visible. The main area is titled "DETAILS" and contains "ARTIFACT INFORMATION". The details listed are:

Entry ID	1621
URL	https://img-s-msn-com.akamaized.net/tenant/amp/entityid/BBY3iqJ.img?h=174&w=300&m=6&q=60&u=t&co=t&l=f&f-jpg
Creation Date/Time	18-Dec-19 6:58:53 PM
Last Modified Date/Time	16-Dec-19 7:37:50 PM
File Type	65
Visit Count	3
Content Size (Bytes)	5765
Original Path	C:\Users\isaia\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!002\MicrosoftEdge\Cache\D8WYBYWF\BBY3iqJ[1].jpg
Relative Path	Users\isaia\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!002\MicrosoftEdge\Cache\D8WYBYWF\BBY3iqJ[1].jpg

Figure 6.20 Edge Cache records

The DETAILS card on the DETAILS pane includes the following information:

ARTIFACT INFORMATION

URL	The URL of the cached item.
Creation Date/Time	The date and time the cached data was saved to the local machine.
Last Modified Date/Time	The date and time the cached item was last modified on the source side.
File Type	The file type of the cached item.

Visit Count	The number of times the cached file has been accessed.
Content Size (Bytes)	The size of the cached file in bytes.
Original Path	The original absolute path to the cached file.
Relative Path	The relative path to the file based on the location of the WebCacheV01.dat database file.

SESSION RECOVERY

Session Recovery files supply the means for a browser to return to the last pages or tabs open. These are used in the event of a crash or sudden power loss, to re-open tabs that were accidentally closed by the user, or to re-open any pages still open when the browser was closed if the browser settings are set to always pick-up where it left off.

These files can provide the examiner with additional useful information as they store evidence of web browsing activity that is stored independent of the normal history artifacts.

CHROME

Chrome stores this session recovery information in four files named: **Current Session**, **Current Tabs**, **Last Session**, and **Last Tabs**, which are all stored in the profile folder. Therefore, for the default profile these files are stored in the following location:

`\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\`

The **Current Session** file lists the tabs that were open during the most recent browsing session. The **Current Tabs** file list the tabs that were still open when the browsing session ended. The **Last Session** and **Last Tabs** files relate to the browsing session before the most recent/current one. The content of these files is parsed into the WEB RELATED categories: Chrome Current Session, Chrome Current Tabs, Chrome Last Session, and Chrome Last Tabs.

The DETAILS card on the DETAILS pane of the artifacts contained in these four categories include the following information:

ARTIFACT INFORMATION

URL	The URL of the webpage.
Last Visited Date/Time	The date and time the URL was last visited.
Title	The title of the webpage as it appears in the browser's title bar/tab.
Visit Count	The number of times the browser has accessed the URL.



Redirect URL	The URL to use for a redirect, if applicable.
--------------	---

FIREFOX

Firefox stores session recovery information from the most recent browsing session in a file named **sessionstore.js** stored in the profile folder. Therefore, for the default profile this file is stored in the following location:

\Users\<username>\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxx.default-release

From introduction through Firefox version 55, Firefox session store data was stored as plain text in a JSON file named **sessionstore.js** and **previous.js**.

With the introduction of Firefox 56 on September 28, 2017, Mozilla introduced the *mozlz4* file format, a proprietary variant of the lz4 compression format. This compression is present in different data stores utilized by Firefox; including files with an extension of **.jsonlz4**, which are essentially JSON files that have been compressed using Mozilla's proprietary implementation of the lz4 compression algorithm.

The DETAILS card on the DETAILS pane includes the following information:

ARTIFACT INFORMATION

Title	The title of the webpage as it appears in the browser's title bar/tab.
URL	The URL of the webpage.
Referrer URL	The URL of the referring website, if applicable.

INTERNET EXPLORER AND EDGE

Session recovery files for Internet Explorer and Edge are compound files with a naming convention **{GUID}.dat**. This file contains multiple entries known as Travel Logs numbered with a TL0, TL1, etc.

The session recovery files for Internet Explorer are stored in the folder:

\Users\<username>\AppData\Local\Microsoft\Internet Explorer\Recovery

The session recovery files for Edge are stored in the folder:

\Users\<username>\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\User\Default\Recovery

The Active session data is stored in a subfolder **\Active**, and the last session data is stored in a subfolder **\Last Active**. Additionally, there will sometimes be subfolders named **\High** and **\Low** within the **\Active** and **\Last Active** folders which relate to elevated security, e.g. Low – standard user, and High – administrator.

The DETAILS card on the DETAILS pane includes the following information:

ARTIFACT INFORMATION

Page URL	The URL of the webpage.
Page Title	The title of the webpage as it appears in the browser's title bar/tab.
Image	The browser generated snapshot of the webpage
Body	The HTML body saved from the webpage.

RUNNING EXERCISES

CHROME SESSION RECOVERY

- From the **Artifacts** explorer in AXIOM Examine, clear any filters you may have in place.
- Select the WEB RELATED → Chrome Current Session category.
- The last time Chrome was open there was one active tab.
- Select the WEB RELATED → Chrome Last Tabs category.
- There were multiple tabs open during the last browsing session when Chrome was closed. Review the **Title** column to see if any appear to be relevant to the case scenario.
- From the **Title** column, locate the entry which begins “Cutest Puppies Playing Around 2017” and note the File Offset listed in the Location link _____.
- Click the Source link which ends with \Last Tabs.
- In the DETAILS pane, scroll down to the TEXT AND HEX card.
- The Chrome session recovery files are a proprietary format with an ASCII “SNSS” file header.
- In the TEXT AND HEX card, click the Go To link and enter the File Offset noted in the earlier step.
- The information extracted is visible in plain text.
- Switch back to the Artifacts explorer and select the WEB RELATED → Chrome Last Session category.
- Sort the Last Visited Date column.
- The additional entries listed here are tabs that were closed during the last browsing session prior to closing Chrome.



COOKIES

Cookies are small files saved onto a local browsing machine by websites. The user might not have visited the website for which a cookie is present because another related website could have saved it to the local machine.

Cookies can store information about the user, their browsing activity, account information, and more.

CHROME

Chrome stores its cookies in a SQLite database named **Cookies** stored in the profile folder. Therefore, for the default profile this file will be stored in the following location:

\Users\<username>\AppData\Local\Google\Chrome\User Data\Default

The information is contained within the table: **cookies**.

DETAILS	
 Chrome Cookies	
ARTIFACT INFORMATION	
Host	www.tomsguide.com
Name	cmp
Accessed Date/Time	7/2/2019 8:47:42 PM
Created Date/Time	7/2/2019 8:47:42 PM
Expiration Date/Time	7/1/2020 8:47:42 PM
Path	/
EVIDENCE INFORMATION	
Source	Dashner Win10 PC.E01 - Partition 2 (Microsoft NTFS, 49.43 GB)\Users\isaia\AppData\Local\Google\Chrome\User Data\Default\Cookies
Recovery Method	Parsing
Deleted source	
Location	Table: cookies(rowid: 335)
Evidence number	Dashner Win10 PC.E01

Figure 6.21 Chrome cookies

The DETAILS card on the DETAILS pane includes the following information:

ARTIFACT INFORMATION

Host	The host domain of the cookie.
Name	The name of the cookie.
Value	The value contained in the cookie.
Accessed Date/Time	The date and time the cookie was last accessed.
Created Date/Time	The date and time the cookie was created.

Expiration Date/Time	The date and time the cookie expires.
Path	The path of the cookie value.

FIREFOX

Firefox stores cookies in a SQLite database named **cookies.sqlite** stored in the profile folder. Therefore, for the default profile the file is stored in the following location:

\Users\<username>\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxxx.default-release

The information is contained within the table: **moz_cookies**.

The screenshot shows a table titled "ARTIFACT INFORMATION" with the following data:

Host	.screensaversplanet.com
Name	sp_eu_ck
Value	OK
Accessed Date/Time	13-Sep-19 7:30:27 PM
Created Date/Time	13-Sep-19 7:30:13 PM
Expiration Date/Time	11-Sep-20 7:30:27 PM
Path	/

Below this is another table titled "EVIDENCE INFORMATION" with the following data:

Source	Dashner Win10 PC.E01 - Partition 2 (Microsoft NTFS, 49.43 GB)\Users\isaia\AppData\Roaming\Mozilla\Firefox\Profiles\kcd9nxhs.default-release\cookies.sqlite
--------	--

Figure 6.22 Firefox cookies

The DETAILS card on the DETAILS pane includes the following information:

ARTIFACT INFORMATION

Host	The host domain of the cookie.
Name	The name of the cookie.
Value	The value contained in the cookie.
Accessed Date/Time	The date and time the cookie was last accessed.
Created Date/Time	The date and time the cookie was created.
Expiration Date/Time	The date and time the cookie is set to expire.
Path	The path of the cookie value.



INTERNET EXPLORER

Internet Explorer stores cookie data as individual files on the local machine. Windows 7 and prior stored the cookie files in the folder:

\Users\<username>\AppData\Roaming\Microsoft\Windows\Cookies

In Windows 8 the Cookies moved to the folder:

\Users\<username>\AppData\Local\Microsoft\Windows\INetCookies

As with other Internet Explorer artifacts, there might also be a **\Low** folder present that relates to browser activity generated when the browser was started with standard, rather than elevated privileges.

In early versions of Internet Explorer, cookie files were named **user@hostname.txt**, e.g. **dashner@gmail.txt**. However, Microsoft recognized that in the event of a system breach, extensive useful information could be gained from cookie files and the format changed to a randomly generated 8-character alphanumeric value, e.g. **LG1FD45A.txt**.

Internet Explorer v10 and v11 store the information *about* the cookie (cookie metadata) and the cookie content in two different locations.

The cookie metadata information is contained within the **WebCacheV01.dat** file located in the folder:

\Users\<username>\AppData\Local\Microsoft\Windows\WebCache

It contains information such as when the cookie was created, last accessed, expires etc. It also contains the name of the individual cookie content file that is stored on the disk.

The individual cookie content file is stored in the folder:

\Users\<username>\AppData\Local\Microsoft\Windows\INetCookies

These cookie files are also named using a randomly generated 8-character alphanumeric value but can have either a **.txt** or **.cookie** extension.

The DETAILS card on the DETAILS pane of artifacts in the Internet Explorer 10-11 Cookies category include the following information:

ARTIFACT INFORMATION

User	The Windows user associated with the cookie.
URL	The host domain of the cookie.
Accessed Date/Time	The date and time the cookie was last visited.
Updated Date/Time	The date and time the cookie was last updated by the host domain.

Created Date/Time	The date and time the cookie was created.
Access Count	As with the browsing history, it is unclear all the actions that trigger this counter, but it is not necessarily the number of times the cookie has been accessed.
Filename	The name, including the full path, of the cookie content file.
File Size	The size of the cookie.

EDGE

Edge also stores the cookie metadata information in the **WebCacheV01.dat** file located in the folder:

\Users\<username>\AppData\Local\Microsoft\Windows\WebCache

The Edge cookie content files also have the name format **xxxxxxxx.txt** or **xxxxxxxx.cookie** and are either stored in the folder:

\Users\<username>\AppData\Local\Packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\MicrosoftEdge\Cookies

Or subfolders within the same package, but with a number in the folder name.

\Users\<username>\AppData\Local\Packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\#!001\MicrosoftEdge\Cookies

\Users\<username>\AppData\Local\Packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\#!002\MicrosoftEdge\Cookies

Other applications can also store cookies including: Windows Store, Windows Photos, Office Hub, Skype, and Cortana.

As with other artifacts extracted from the **WebCacheV01.dat** file, Edge cookies are listed under the Internet Explorer 10-11 cookie category.

The screenshot shows the 'DETAILS' tab of an artifact in Magnet AXIOM. The artifact is identified as an 'ARTIFACT INFORMATION' entry with ID 8, associated with the URL com.office365.outlook. It was updated on 03-Jul-19 at 6:34:58 PM. The 'EVIDENCE INFORMATION' section shows the source as Dashner Win10 PC.E01 - Partition 2 (Microsoft NTFS, 49.43 GB)\Users\isaia\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat. There are two small icons on the right side of the evidence information row.

Figure 6.23 Edge cookie located in the Internet Explorer 10-11 Cookies category

TYPED URLs

CHROME AND FIREFOX

Typed URLs need to be treated with a little caution. In the past, this field indicated when a URL had been typed (or copied/pasted) directly into the address bar of the browser. However, things are slightly more complicated now. If the user starts typing into the address bar, whether that be a URL or simply a search string, the browser will often provide autosuggestions for the user. If the user accepts one of these autosuggestions this will also appear as a Typed URL. This field does not necessarily mean the user has typed the URL directly into the address bar, it is more accurate to say that the user typed (or copied/pasted) *something* into the address bar.

Chrome stores Typed URLs in the **History** database, which for the default profile is located at:

\Users\<username>\AppData\Local\Google\Chrome\User Data\Default

Firefox stored Typed URLs in the **places.sqlite** database, which for the default profile is located at:

\Users\<username>\AppData\Local\Mozilla\Firefox\Profiles\xxxxxxx.default-release

AXIOM Examine displays this information in the respective Web History and Web Visits categories.

Chrome stores a numerical counter of how many times Chrome deems the URL was typed.

The screenshot shows the AXIOM Examine interface with the following details for a Chrome Typed URL:

- DETAILS** section:
 - Icon: Chrome Web History
- ARTIFACT INFORMATION** section:
 - URL: <https://www.google.com/>
 - Last Visited Date/Time: 9/11/2019 8:05:56 PM
 - Title: Google
 - Visit Count: 23
 - Typed Count: 8 (highlighted with a red border)
- EVIDENCE INFORMATION** section:
 - Source: Dashner Win10 PC.E01 - Partition 2 (Microsoft NTFS, 49.43 GB)\Users\isaia\AppData\Local\Google\Chrome\User Data\Default\History
 - Recovery Method: Parsing
 - Deleted source
 - Location: Table: urls(id: 2)
 - Evidence number: Dashner Win10 PC.E01

Figure 6.24 Chrome Typed URL

Firefox stores a Boolean Yes/No value detailing whether Firefox deems the URL has ever been typed.

The screenshot shows the 'DETAILS' tab in Magnet AXIOM. Under 'ARTIFACT INFORMATION', it displays:

- URL: <http://wikipedia.com/>
- Last Visited Date/Time: 29-Oct-19 8:12:19 PM
- Visit Count: 1
- Is Typed: Yes

Under 'EVIDENCE INFORMATION', it shows the source as:

Source: Dashner Win10 PC.E01 - Partition 2 (Microsoft NTFS, 49.43 GB)\Users\isaia\AppData\Roaming\Mozilla\Firefox\Profiles\kcd9nxhs.default-release\places.sqlite

Figure 6.25 Firefox Typed URL

INTERNET EXPLORER AND EDGE

Internet Explorer and Edge both track Typed URLs in the user registry.

Internet Explorer tracks Typed URLs in the main user registry hive – **NTUSER.dat**, that is stored in the following location:

\Users\<username>

The information is stored in the following 2 registry keys:

SOFTWARE\Microsoft\Internet Explorer\TypedURLs\

SOFTWARE\Microsoft\Internet Explorer\TypedURLsTime\

Edge tracks Typed URLs in the supplementary user registry hive – **UsrClass.dat**, that is stored in the following location:

\Users\<username>\AppData\Local\Microsoft\Windows

The information is stored in the following 3 registry keys:

LocalSettings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoftedge_8wekyb3d8bbwe\MicrosoftEdge\TypedURLs

LocalSettings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoftedge_8wekyb3d8bbwe\MicrosoftEdge\TypedURLsTime

LocalSettings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoftedge_8wekyb3d8bbwe\MicrosoftEdge\Typ



edURLsVisitCount

RUNNING EXERCISE

CHROME TYPED URLs

- From the **Artifacts** explorer in AXIOM Examine, clear any filters you may have applied.
- Select the WEB RELATED → Chrome Web History category.
- Reverse sort the Typed Count column.
- Filter the URL column for “dropbox.com”. Do a sort on the URL column so the listing for just “[https://www.dropbox.com/”](https://www.dropbox.com/) is at the top.
- The URL “[https://www.dropbox.com/”](https://www.dropbox.com/) has a Typed Count of 2 and a Visit Count of 5.
- The Last Visited Date/Time is 30 AUG 2019 at 18:22:29.
- Select the WEB RELATED → Chrome Web Visits category
- Sort on the URL column so the listing for “[https://www.dropbox.com/”](https://www.dropbox.com/) is at the top.
- The second and third entries have a Transition Type of TYPED. So, these are the two entries Chrome deems were Typed URLs.
- The fifth entry has a Transition Type of AUTO_BOOKMARK, so the user selected an entry from the user interface.
- The Typed Count for all five entries is 2. The Typed Count information is extracted from the single entry in the **urls** table which is being cross-referenced by each of the four entries in the **visits** table. It is *NOT* a running total; it is the total number of times the browser deems the URL has been TYPED.
- Clear all filters.

EDGE TYPED URLs

- From the **Artifacts** explorer in AXIOM Examine, clear any filters you have applied.
- Select the WEB RELATED → Edge Typed URLs category and then sort on the URL column.
- Note the path listed for the source of the two URLs associated with <http://www.google.com>.
- Typed URLs in Edge are stored in the **Spartan.edb** database along with the Favorites.

- Note the Accessed Date/Time listed for the two Google URLs.
- Using the Set relative time filter button  in the DETAILS card of the PREVIEW pane for the Accessed Date/Time value, check the box under SET RANGE to use the same range of time both before and after the defined date. Set a range of 5 minutes and select the option to view the results in the Current explorer.
- Review the Edge/Internet Explorer 10-11 Main History artifact.
- What was searched for after the user typed in Google.com?

WEBKIT BROWSER DATA

The WebKit engine is a web-browser engine designed by Apple for use in the Safari browser. Over time, many other browsers have adopted the use of the WebKit engine. The WebKit browser artifacts can often help to show other browsers that have been used by the user on a computer. AXIOM can often carve information that is stored within browsers that mimic the WebKit engine storage structure. By reviewing information in the source fragments within AXIOM, users may deduce what browser the data came from.

DETAILS

ARTIFACT INFORMATION

URL	https://www.google.com/search?q=golden +retriever +puppies&source=lnms&tbo=isch&sa=X&ved=0ahUKEwjj7J-4oKjkAhUIS60KHTfHAMsQ_AUIESgB&biw=1280&bih=917#imgrc=NiETBJmjfzPCtM	
Last Visited Date/Time	29-Aug-19 3:15:30 PM	
Title	golden retriever puppies - Google Search	
Visit Count	1	
Typed Count	0	

EVIDENCE INFORMATION

Source	Dashner Win10 PC.E01 - Partition 2 (Microsoft NTFS, 49.43 GB)\Users\isaia\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\History	
--------	--	---

Figure 6.26 WebKit Browser History (carved) from the Brave browser



As seen in Figure 6.26, the Source fragment shows this particular browser history record was carved from the storage relating to the Brave Browser. Brave is a Chromium-based privacy browser that is gaining popularity.

MODULE REVIEW

In this module the following topics were covered:

- Identifying browser artifacts generated by Chrome, Firefox, Internet Explorer and Edge. This included browsing history, bookmarks, download activity, and browser cache.
- Understanding source and location linking and viewing SQLite database content within AXIOM.

REVIEW QUESTIONS

To help reinforce the learning objectives for this module, the following review questions have been provided:

1. Firefox and Chrome store much of their data in SQLite databases. How can the content of SQLite databases be viewed in AXIOM Examine?
2. Name three pieces of information displayed in AXIOM Examine for a file downloaded using Chrome.
3. What is Session Recovery data?
4. Name the database file that stores/tracks most of the artifacts generated by Edge.

STUDENT EXERCISE

This exercise is based on the Dashner case scenario from Module 1.

- Review the results in the Chrome Bookmarks category. List any items of interest that you find. Tag these items appropriately.
- From the FILTERS bar, conduct a search for “torrent”. Review the results in the WEB RELATED → Chrome Web History and Chrome Downloads categories. What do these results indicate?
- On the filters bar, click the X next to the keyword filter “torrent” you just applied. Select the WEB RELATED → Edge/Internet Explorer 10-11 Daily/Weekly History category. Sort the Accessed Date/Time-Local Time column. What file was accessed on 2019-12-18 at 12:58:52? Where was this file located?
- From the FILTERS bar, select the Date and time filter with a Date range of All dates between. Apply a date/time filter for 29-Aug-2019, using this date for both the START DATE and END DATE. From the Time range drop-down menu choose the option for Custom time range. Use a start time of 1:56 PM and an end time of 1:57 PM.
- Select the WEB-RELATED → Chrome Web History artifact category.
- What activity does it appear Dashner was participating in between 1:56:56 PM and 1:57:00 PM? Tag these items appropriately.
- Review the WEB-RELATED → Chrome Downloads artifact category. Is there any relevant activity during this time frame?
- Clear the filters, then review the results in the WEB-RELATED → Chrome Downloads category for any items of relevance. Tag them as appropriate.
- Search the WEB-RELATED → Firefox Downloads category for any items of interest. Tag them as appropriate.



- What browser appears to have been used to search for “AxCrypt”? (Hint: Check *all* the WEB RELATED categories)
- Was the AxCrypt software downloaded and installed? (Hint: Check other categories outside of WEB RELATED)

Notes

Notes



MAGNET
FORENSICS®

MODULE 7:

Email & Calendar

LEARNING OBJECTIVES

In this lesson, students will take part in lecture, instructor led exercises, and student practical exercises to recover emails and email attachments from mail clients supported by Magnet AXIOM. Students will also gain an understanding of Source Linking as it relates to emails and understand the results found in the PREVIEW card as well as the DETAILS card.

GOALS

At the conclusion of this lesson, students will be able to identify and discuss different email artifacts, and use Magnet AXIOM to review, sort, filter, tag, and report on email and email attachments in furtherance of a successful investigation.

EMAIL ARTIFACTS

AXIOM Process searches for and categorizes a variety of types of email and the associated account calendar data into the EMAIL & CALENDAR artifact category. For a full list of the supported email clients and formats refer to the Artifact Reference.

AXIOM Process supports parsing of both traditional email client artifacts (POP, IMAP protocols, etc.) and those from web-based email. This can be useful as individuals might access the same email account differently on different computers and/or devices. Also, you may find email messages with delivery dates that predate the created dates by significant lengths of time. With the popularity of web-based mail clients and cloud storage of message by mail providers, it is very likely you will examine a device that has emails synced to it.

In addition, AXIOM may find Calendar Events pulled from data such as .ics files. These files are used by many different email applications, including Outlook, Google Calendar, and Apple Calendar.

NOTE: The content of compound mail structures such as Microsoft Outlook PST and OST files is also parsed.

Windows		
Additional Sources	Android	iOS
Chat	Advanced Search Tools	Advanced Search Tools
Cloud	Chat	Chat
Documents	Cloud	Cloud
E-mail	Cloud Storage	Cloud Storage
Calendar Events (.ICS)	Documents	Documents
EML(X) Files	E-mail	E-mail
Gmail Email Fragments	Android Emails	Apple Mail
Gmail Webmail	Android Gmail Conversations	Apple Mail Fragments
Hotmail Webmail	Android Yahoo Mail Attachments	Gmail Emails
Hushmail Fragments	Android Yahoo Mail Emails	iOS Yahoo Mail Contacts
Hushmail Inbox	Android Yahoo Mail User Accounts	iOS Yahoo Mail Messages
Mailinator Inbox Access	Gmail Emails	iOS Yahoo Mail User Accounts
Mailinator Snippets	Outlook Accounts	Outlook Appointments
MBOX Emails	Outlook Appointments	Outlook Contacts
Offline Gmail webmail	Outlook Contacts	Outlook Messages
Outlook Appointments	Outlook Messages	Samsung Email Logs
Outlook Contacts	Samsung Email Logs	Outlook Messages
Outlook Journals		
Outlook Messages		
Outlook Notes		
Outlook Tasks		
Outlook Web App Email Fragments		
Outlook Web App Inbox		
Outlook Webmail Inbox		
Windows Mail		
Yahoo! Webmail		

Figure 7.1 Supported EMAIL artifact



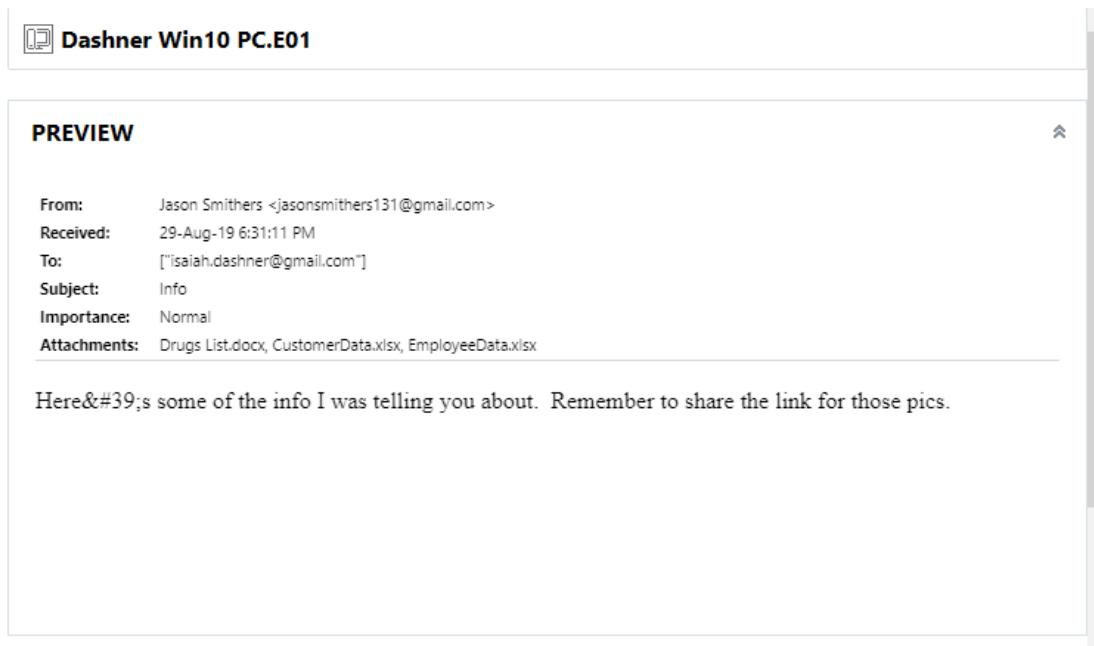
EMAIL CONTENT

When viewing the content of the EMAIL categories, the columns of the EVIDENCE pane include email specific information, such as: To, From, Sender, Recipient, Subject, Carbon Copy, etc. The exact columns displayed will differ depending on the email client being displayed.

Email headers can be an excellent source of information as they often include the source of an email, email servers the message has passed through, Internet Protocol (IP) addresses of the sender and pass-through servers, the sender's email client, and the true email address of the sender. If the message was sent from a group mailbox, the header will also include the email address of the person sending the message. Timestamps associated with the pass-through servers are also added to the header and can be trusted more than the sent date/time included in the email itself. If an individual has attempted to manipulate the date/time information stored in the computer, reviewing email headers could help ascertain the true date and time a message was sent and/or received.

The PREVIEW card on the DETAILS pane provides a rendered view of the email content if available.

NOTE: Not all HTML content can be rendered into an easily readable format in the PREVIEW Card.



The screenshot shows the AXIOM Examine software interface. At the top, there is a header bar with the text "Dashner Win10 PC.E01". Below this is a "PREVIEW" card. The card displays the following email metadata:

From:	Jason Smithers <jasonsmithers131@gmail.com>
Received:	29-Aug-19 6:31:11 PM
To:	["isaiyah.dashner@gmail.com"]
Subject:	Info
Importance:	Normal
Attachments:	Drugs List.docx, CustomerData.xlsx, EmployeeData.xlsx

Below the metadata, there is a rendered preview of the email body:

Here's some of the info I was telling you about. Remember to share the link for those pics.

Figure 7.2 PREVIEW card in the Details pane

EMAIL SOURCE LINKING

The Source Linking feature within AXIOM Examine can also be used for EMAIL artifacts. For EMAIL artifacts sourced from a flat database file such as MBOX Emails, the Source field details the filename and

directory location of the file the email was extracted from, and the Location field details the exact location within the source file, as shown in Figure 7.3. To view the source of the artifact, select either the Source or Location link. AXIOM Examine automatically switches to the File system explorer with the source file highlighted. If the Location link was selected, the cursor in the TEXT AND HEX card will be at the exact location within the file that the EMAIL artifact was found.

If the source of an EMAIL artifact is a compressed compound file, such as Microsoft Outlook PST and OST files, the exact location within the file cannot be directly mapped. Therefore, the Location link will simply display “n/a”, as shown in Figure 7.3.

EVIDENCE INFORMATION

Source	Dashner Win10 PC.E01 - Partition 2 (Microsoft NTFS, 49.43 GB)\Users\isaia\AppData\Local\Microsoft\Outlook\isaiah.dashner@gmail.com.ost
Recovery Method	Parsing
Deleted source	
Location	n/a
Evidence number	Dashner Win10 PC.E01

Figure 7.3 Source linking for compound file

RUNNING EXERCISE

VIEWING EMAIL CONTENT

- From the **Artifacts** explorer in AXIOM Examine, clear any filters you may have applied.
- In the Artifacts drop-down on the FILTERS bar, select EMAIL & CALENDAR.
- Select the EMAIL & CALENDAR → Outlook Emails category.
- Apply a filter to the Sender Name column for “Dropbox”.
- Sort on the Delivery Date / Time column and select the earliest email from Dropbox. Note the differences in the Delivery Date / Time and Creation Date / Time.
- The DETAILS pane includes a rendered view of the email in the PREVIEW card.
- Expand the Headers field to view the full content.

EMAIL SOURCE LINKING

- Scroll down in the DETAILS pane to the EVIDENCE INFORMATION.



- Note the Source of this email.

- Click the Source link to transition to the File system explorer within Axiom Examine.
- In the File system explorer, confirm the Source file is highlighted.
- Note the preview card is blank. Scroll down to the TEXT AND HEX card and review the file header information.
- In the TEXT AND HEX card, switch to TEXT view.
- This is a compound file (an .OST) and it may not be reviewable within the Hex/Text card.
- Switch back to the Artifacts explorer.

EMAIL ATTACHMENTS

If an EMAIL artifact contains a file attachment, the attachment name will be listed in the Attachments or Attachment Name(s) column in the EVIDENCE pane and listed on the DETAILS card in the DETAILS pane – the exact name of the field is dependent on the EMAIL category. An EMAIL ATTACHMENTS card is also included on the DETAILS pane listing the attachment name, as shown in Figure 7.4. If the content is viewable, the attachment name will be a link and when selected the attachment will display in a PREVIEW card embedded within the EMAIL ATTACHMENTS card.

The screenshot shows the Magnet AXIOM interface with the DETAILS pane open. The top section is titled "EMAIL ATTACHMENTS" and lists three attachments: "Drugs List.docx", "CustomerData.xlsx" (which is highlighted in blue), and "EmployeeData.xlsx". Below this, a "PREVIEW" card is embedded, showing the content of "CustomerData.xlsx". The preview shows a table with columns: id, first_name, last_name, email, gender, and Credit. The word "data" is visible above the table.

Figure 7.4 PREVIEW card embedded within the EMAIL ATTACHMENTS card on the DETAILS pane

Examiners can review all the email attachments by selecting the Email Attachments artifact within the EMAIL category. All attachments from all included and parsed email artifacts will be dropped within this single category.

The screenshot shows the Magnet AXIOM interface with the DETAILS pane open. The top section is titled "ARTIFACT INFORMATION" and lists various details about an artifact named "unicorn.jpg". The details include: File Name (unicorn.jpg), Subject (Re: new hobby), File Extension (.jpg), MD5 Hash (dd9805a2c5ae79d6e0d37cab592517b), SHA1 Hash (7e6f4f9b7f45a50de83ce706940d3b0e64a7a953), Skin Tone Percentage (1.4), To Address(es) (Isaiah Dashner), From Address (Jason Smithers <jasonsmithers131@gmail.com>), Email Timestamp Date/Time (12-Sep-19 10:01:42 PM), and Original artifact (Outlook Emails).

Figure 7.5 PREVIEW card embedded within the EMAIL ATTACHMENTS card on the DETAILS pane



In addition to displaying the Subject, Sender, and Recipient of the source email, there is also a secondary source link called Original artifact. This source link will direct the examiner to the email that contains the attachment.

RUNNING EXERCISE

REVIEWING EMAIL ATTACHMENTS

- In the Artifact explorer, select the EMAIL & CALENDAR → Email Attachments category.
- Sort on the File Name column and locate the attachment named “unicorn.jpg”.
- Review the Subject listing for this attachment.
- Review the From Address listing for this attachment.
- Click on the Original artifact link. This will take the examiner to the original email. Review the content of this email message.

SEARCHING EMAIL

The content and artifact attributes of EMAIL & CALENDAR artifacts can be searched in the same way as other artifact types. In the example shown in Figure 7.6, the Artifacts drop-down on the FILTERS bar was used to filter for “Email & Calendar” artifacts, then a keyword search was then conducted for the word “Smithers”.



The screenshot shows the Magnet AXIOM interface with a search results table. The table has columns for 'Sender Name' and 'Send...'. All entries in the 'Sender Name' column are identical, showing 'Jason Smithers <jasonsmithers131@gmail.com>'. The entire 'Sender Name' column is highlighted with a yellow background.

	Sender Name	Send...
	Jason Smithers <jasonsmithers131@gmail.com>	

Figure 7.6 Searching and filtering email

RUNNING EXERCISE

SEARCHING EMAILS

- Select Outlook Emails from the Artifacts drop-down menu on the FILTERS bar.
- Using the Search box on the FILTERS bar, search for the word “Smithers”
- The hits are contained within the email Sender and Recipients
- The hits are also highlighted in the rendered version of the email in the PREVIEW card.

MODULE REVIEW

In this module the following topics were covered:

- Viewing EMAIL information including the To, From, Subject, and date and times.
- Viewing EMAIL content and how AXIOM Examine renders the content in the DETAILS pane.
- EMAIL headers and the information contained within them.
- How to view EMAIL attachments.
- Source linking of EMAILS.
- Creating EMAIL artifact reports.



REVIEW QUESTIONS

To help reinforce the learning objectives for this module, the following review questions have been provided:

1. Where can EMAIL specific information such as Subject, To, From and Received Time be viewed in AXIOM Examine?
2. What is the potential investigative value of EMAIL Headers?
3. How can EMAILS with attachments be quickly identified?
4. If a keyword Search is conducted from the FILTERS bar, what parts of an EMAIL are searched?

STUDENT EXERCISE

This exercise is based on the Dashner case scenario from Module 1.

- Search for Emails from “googlenest”. What Internet of Things (IOT) device(s) did Dashner own?

- Who was Dashner receiving email(s) from on 29-Aug-2019? What were they discussing?

- What is the subject of the email thread sent from Jason Smithers to Dashner on 30-Aug-2019?

- Identify any encryption tool(s) referenced within the emails located in the Email category.

- Did any emails between Dashner and Smithers contain attachments and if so, what did they contain? Tag these items appropriately.

- Identify all emails sent by Dashner via Microsoft Outlook and export them as a PST. (Hint, look in the File menu).

- Were there any email links shared for online cloud services such as OneDrive or Dropbox?

- Type “AxCrypt” in the Filters Search bar and review the Windows Mail artifact. Run this email through an online translator such as <http://translate.google.com>. What is the email referencing?



Notes



MODULE 8:

Documents

LEARNING OBJECTIVES

In this lesson, students will take part in lecture, running exercises, and student practical exercises to gain an understanding of the different views for documents and the metadata of document files. Students will use Magnet AXIOM to create artifact reports and save artifacts externally from AXIOM. Students will explore the ability to search document content and metadata via the filters bar. Students will also discover AXIOM's ability to process documents/images using Optical Character Recognition (OCR).

GOALS

At the conclusion of this lesson, students will be able to identify and discuss document artifacts, use Magnet AXIOM to search the data and metadata of document files, and extract those recovered artifacts from AXIOM. Students will also be able to search and filter document content.

DOCUMENTS ARTIFACTS

AXIOM Process searches for and categorizes the following document formats into the DOCUMENTS category:

- CSV (comma-separated value)
- Hangul Word Processor (Includes support for Korean language)
- Microsoft Office Excel, PowerPoint and Word
- Apple Notes
- Google Docs
- Corel WordPerfect Documents
- OpenOffice Calc, Impress and Writer
- PDF (Portable Document Format)
- RTF (Rich Text Format)
- Text (Plain Text)



Figure 8.1 Document formats supported by Magnet AXIOM

In AXIOM Examine, these artifacts are grouped into the DOCUMENTS category, as shown in Figure 8.2.

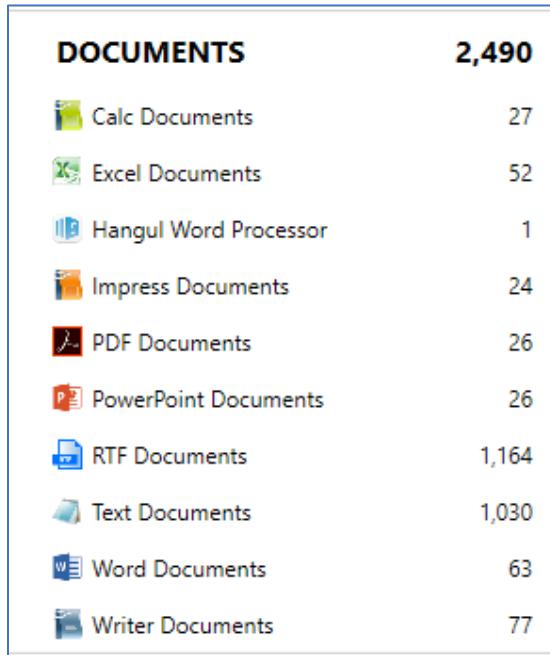


Figure 8.2 DOCUMENTS category

DOCUMENT CONTENT

When a document artifact is selected in the EVIDENCE pane, the DETAILS pane includes a PREVIEW card that displays the basic content of the document. When Microsoft Office documents are displayed each page/sheet/slide is separated by a grey, broken line. In some cases, such as PDF, there will be two preview cards. One will display the full PDF document while another will display just the flat text from the document.

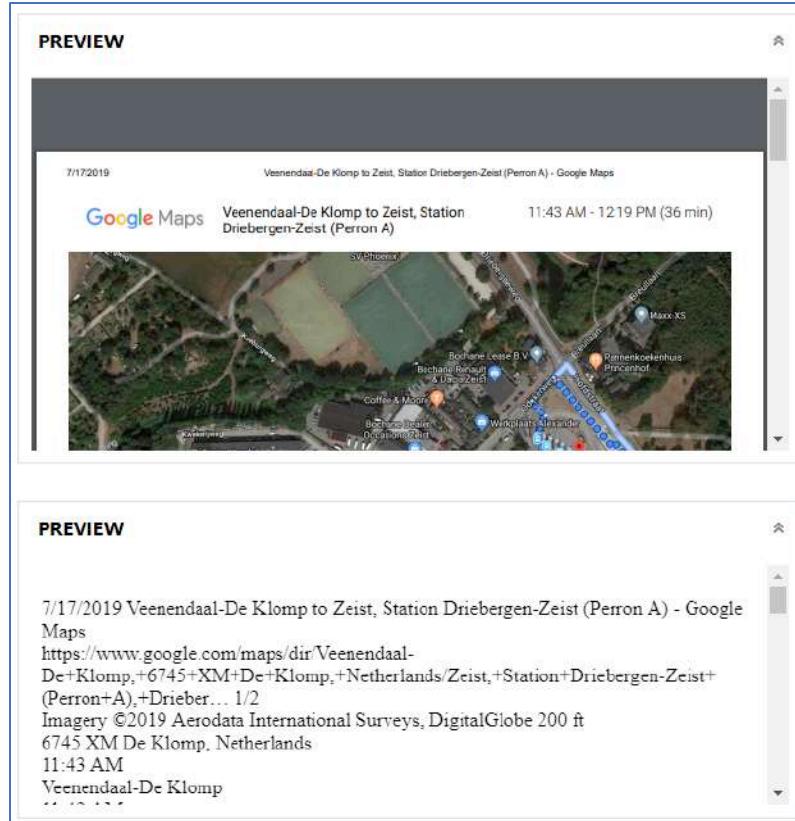


Figure 8.3 PREVIEW card in the DETAILS pane

The DETAILS card on the DETAILS pane includes the following:

ARTIFACT INFORMATION

Filename	The name of the document.
File System Created Date/Time	The date and time the file was created on the file system.
File System Last Accessed Date/Time	The date and time the file was last accessed on the file system.
File System Last Modified Date/Time	The date and time the file was last modified by the file system.
Size (Bytes)	The size of the file in bytes.
Saved Size (Bytes)	The size of the recovered file in bytes.
MD5 Hash	The MD5 hash of the document file.
SHA1 HASH	The SHA1 hash of the document file.

NOTE: Additional columns will be displayed for the document's metadata. These will be discussed in the next section.



EXPORTING DOCUMENTS TO A LOCAL DRIVE

Document artifacts parsed and carved by AXIOM Process can be exported from the case and saved to the local drive using AXIOM Examine.

To export a copy of the file, select the documents to be exported, right-click, and select Save artifact to..., as shown in Figure 8.4 Select the folder location for the exported files, and once the Files saved message appears in the bottom left of the AXIOM Examine interface, as shown Figure 8.5, click OPEN. The files are exported to the folder **Attachments** within the destination folder.

NOTE: Files can also be saved from the File system explorer, which will be covered in a later lesson.

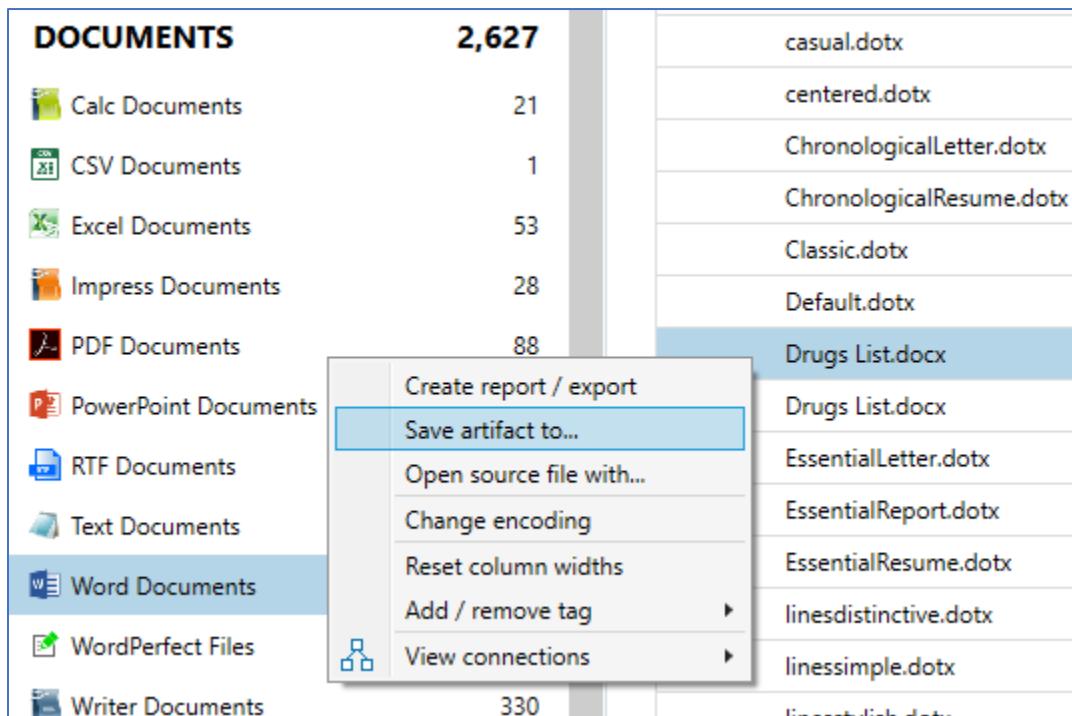


Figure 8.4 Saving document artifacts to the local drive



Figure 8.5 Artifacts exported successfully

RUNNING EXERCISE

VIEWING AND SEARCHING DOCUMENT CONTENT

- From the **Artifacts** explorer in AXIOM Examine, clear any filters you may have applied.
- From the Artifacts drop-down on the **FILTERS** bar, select the parent Documents category (the one above the bar).
- On the **FILTERS** bar hover over the **Artifacts** filter criteria, now displayed in bold.
- Because the parent category was selected, AXIOM Examine has automatically filtered on all available document types within the case.
- Select the DOCUMENTS → PDF Documents category.
- Sort the Filename column and locate “anarchistcookbook2000.pdf”.
- On the DETAILS pane there are two PREVIEW Cards
- The first contains a near-native view of the file, including the text and embedded graphics.
- The second contains just the text content.
- Using the Search box on the FILTERS bar, search for the word “recipe”.
- The keyword hits are highlighted in the second preview pane and can be seen by scrolling down.
- Searching from the FILTERS bar will locate keyword hits within the document content.
- Click the X next to recipe on the FILTERS bar to remove just the keyword search part of the filter.
- Switch to the DOCUMENTS → Excel Documents category.
- Sort the Filename column and highlight one of the files named **CustomerData.xlsx**.
- A rendered version of the file content is displayed in the PREVIEW card on the DETAILS pane.

EXPORTING DOCUMENT ARTIFACTS

- In the EVIDENCE pane, right-click on the previously selected file **CustomerData.xlsx** and select Save artifact to.... from the menu.
- Save the file to the **\Export** folder on the Desktop.
- Once the Files are saved a message appears in the bottom left of the AXIOM Examine interface, including a link which is labeled **OPEN**.



- Select **OPEN** and a File Explorer window opens the **\Export** folder. You will see a subfolder created by the file export named **\Attachments**.
- Open the **\Attachments** folder to view the saved file in Microsoft Excel.
- Compare the worksheet tab name shown in the lower portion of Microsoft Excel with the blue text shown in **DETAILS** pane within AXIOM Examine. This worksheet tab name corresponds to the blue text displayed in the PREVIEW card, which can be useful if there are multiple sheets in the spreadsheet document you are reviewing.
- Close Microsoft Excel and return to AXIOM Examine.

DOCUMENT METADATA

In addition to the ARTIFACT INFORMATION relating to the physical file, many document formats contain internal metadata. This information travels with the file and is independent of the file system. Metadata can often provide more accurate information regarding when a document was first created, as opposed to when the document was first written to the storage device. This can sometimes result in inconsistencies between the date and time information contained within the ARTIFACT INFORMATION. These inconsistencies should not be considered a bad thing, but rather as a source of additional information to include in a genesis timeline.

In addition to the ARTIFACT INFORMATION detailed in the previous section, The DETAILS card could also include the following information that has been extracted from the internal document metadata:

Title	The title of the document.
Subject	The subject of the document.
Authors	The document authors.
Last Author	The last author of the document.
Company	The company the software is registered to.
Keywords	Any keywords the user added to the document.
Comments	Any comments the user added to the document.
Created Date/Time	The date the document was created.
Last Modified Date/Time	The date and time the document was last modified.
Last Printed Date/Time	The date the document was last printed.

DETAILS	
ARTIFACT INFORMATION	
Filename	EmployeeData.xlsx
File System Last Modified Date/Time	29-Aug-19 6:34:42 PM
File System Last Accessed Date/Time	10-Sep-19 12:55:17 PM
File System Created Date/Time	29-Aug-19 6:31:52 PM
Size (Bytes)	75850
Saved Size (Bytes)	75850
Last Author	Isaiah Dashner
Last Modified Date/Time	29-Aug-19 6:34:42 PM
Created Date/Time	29-Aug-19 6:34:42 PM
MD5 Hash	04cf0abfe037575c78becdc3844457de
SHA1 Hash	9512b35846400e84fadcf4b1bab63813cfad223e

Figure 8.6 DETAILS card showing metadata extracted from document artifact

CSV, RTF, and Text documents do not have metadata. OpenOffice and PDF files contain metadata similar to Microsoft Office documents. Hangul Word Processor documents also have similar metadata to Microsoft Office documents but also include a few unique fields. The Artifact Reference contains a full list of metadata fields extracted for each document format.

RUNNING EXERCISE

VIEWING AND SEARCHING DOCUMENT METADATA

- From the **Artifacts** explorer in AXIOM Examine, clear any filters you may have in place.
- From the **Evidence** drop-down menu on the **Filters** bar, select only the **Dashner Win10 PC.E01** entry. This will apply a filter within AXIOM Examine and only show artifacts sourced from this evidence item.
- Select the DOCUMENTS → Word Documents category.
- Sort by Filename and highlight the file named **Pure Gold.docx**.
- In the DETAILS pane, scroll down to the DETAILS card.
- Compare the date and time information.
- The Last Modified Date/Time and Created Date/Time information is internal metadata that has been extracted from the file.



- The File System Created Date/Time, and File System Last Modified Date/Time information has been extracted from the file system. On an NTFS formatted volume this information is stored in the **\$MFT** file.
- From the Evidence drop-down menu on the Filters bar, select **RESET** to remove the previously applied evidence filter.
- Select the DOCUMENTS → PowerPoint Documents category.
- Sort the Filename column.
- Select the file named **Methamphetamine.ppt**.
- In the PREVIEW card on the DETAILS pane scroll down and locate the faint, grey broken line.
- This represents the next slide in the presentation.
- Using the Search box on the FILTERS bar, search for the word “supercourse”.
- Scroll down in the DETAILS pane and note the keyword hits are highlighted in yellow.
- Searching from the FILTERS bar will locate keyword hits within the document metadata.
- Clear all filters.

OPTICAL CHARACTER RECOGNITION

Examiners can leverage Optical Character Recognition (OCR) technology to help them recover embedded text in PDFs, scanned documents, and images. Examiners have two options to enable OCR.

Examiners can process PDFs and/or images during the initial scan of the evidence within AXIOM Process:

EXTRACT TEXT FROM FILES (OCR)

CASE DETAILS	
EVIDENCE SOURCES	4
PROCESSING DETAILS	
Search archives and mobile backups	On
Add keywords to search	
Extract text from files (OCR)	
Calculate hash values	On
Categorize chats	
Categorize pictures and videos	
Add CPS data to search	
Find more artifacts	
ARTIFACT DETAILS	188
Computer artifacts	188 of 237
Mobile artifacts	
Cloud artifacts	
ANALYZE EVIDENCE	

PROCESS FILES USING OPTICAL CHARACTER RECOGNITION

During a scan, Magnet AXIOM can extract text from certain files using optical character recognition (OCR). AXIOM Examine displays the extracted text in its own card, called Text extracted using OCR.

- PDF documents
- Pictures

Figure 7 OCR options at the point of processing within AXIOM Process

Alternatively, examiners can choose to post-process evidence within AXIOM Examine utilizing the OCR capability. To do this, an examiner needs to select Process – Extract text from files (OCR) from the Examine Menu:

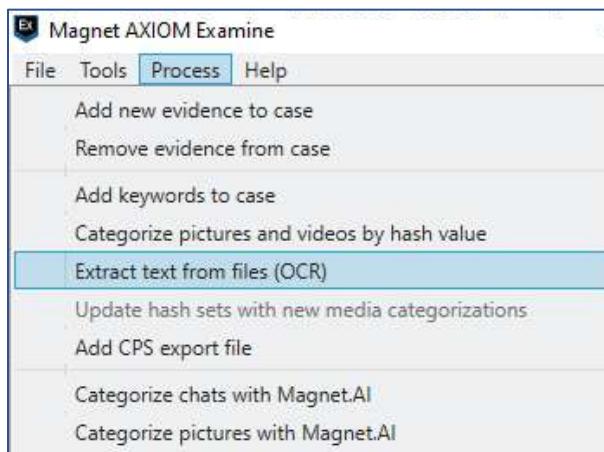


Figure 8.8 Menu selection to enable OCR post-processing



After selecting Extract text from files (OCR), and examiner will be presented with two options:

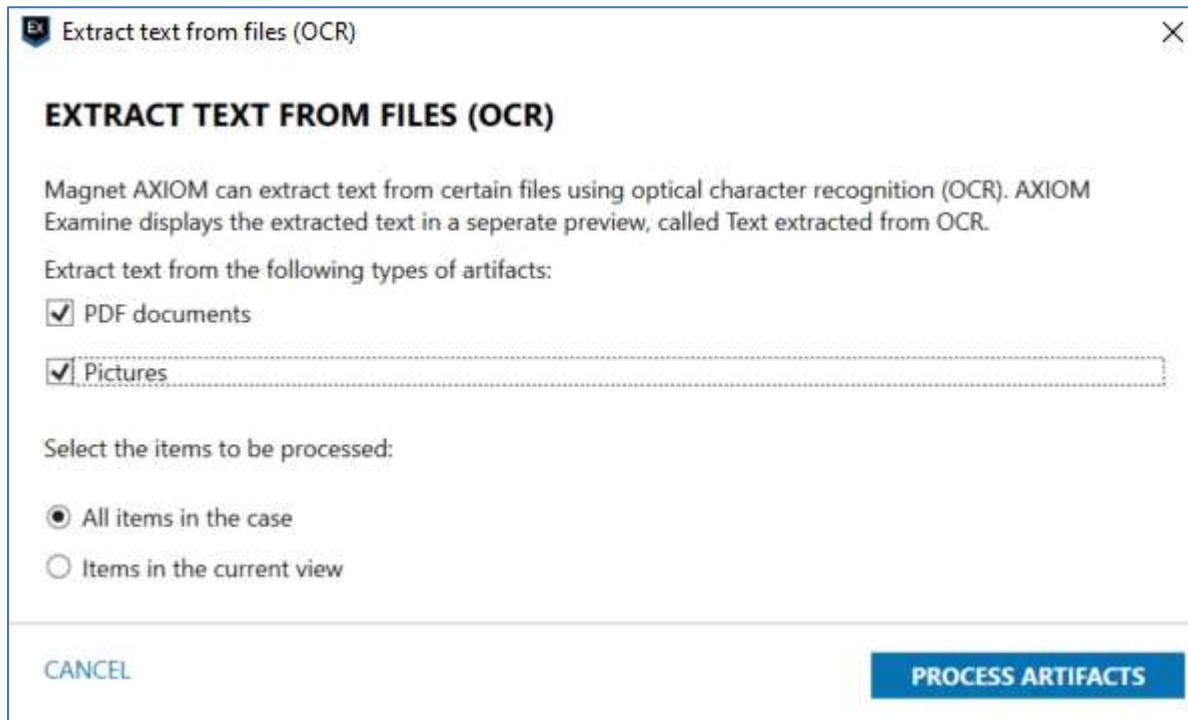


Figure 8 Configuring OCR text extraction

The examiner can use OCR to extract text from either PDF documents, Pictures, or both. Additionally, the examiner can choose all items in the case, or only items in the current view. Selecting the option for Items in the current view will significantly decrease processing time as it will avoid extraneous files.

After the OCR process is complete, the examiner can review the text extracted using the OCR preview card found within the Details panel of AXIOM Examine.

MODULE REVIEW

In this module, the following topics were covered:

- Viewing DOCUMENT details and previewing their content.
- Viewing DOCUMENT metadata.
- Exporting DOCUMENTS to the local machine using the Save artifact to... option.
- Creating artifact reports using the Create report / export option.
- Searching DOCUMENTS.



REVIEW QUESTIONS

To help reinforce the learning objectives for this module, the following review questions have been provided:

1. Where is the content of a document displayed in AXIOM Examine?
 2. When viewing a document's DETAILS, what is the difference between the Created Date/Time and the File System Created Date/Time?
 3. Name three document formats searched for and categorized by AXIOM.
 4. Will a keyword search find a word within a PDF Document using the OCR feature?



STUDENT EXERCISE

This exercise is based on the Dashner case scenario from Module 1.

- From the **Artifacts** explorer in AXIOM Examine, clear any filters you may have applied.
- Review the Word Documents for any items of interest (file name or content). How many files did you find and what are their names?

- Who was the last author of the **301.ppt** document? Where was this document located?

- Was the document **Golden Puppies.pdf** stored within a Cloud storage service? Hint: Compare the Source and Evidence number listed in the DETAILS pane for these items to confirm your findings.

- Tag this item(s) appropriately.
- Search for text documents created the afternoon of 29-Aug-2019. What kind of activity was taking place?
- Where was the **Methamphetamine.ppt** document stored?
- Search all documents for evidence related to AxCrypt. Were any items of evidentiary value located? Where were they located?
- Tag the item(s) appropriately
- How many authors were associated with the **Drugs List.docx** documents? Who were they?
- Were any Excel documents found to contain items of evidentiary value?



Notes





MAGNET
FORENSICS®

MODULE 9:

Operating System – Part 2

LEARNING OBJECTIVES

In this lesson, students will take part in lecture, hands-on exercises, instructor led exercises, and student practical exercises to gain an understanding of Magnet AXIOM's capability to recover artifacts from the File System and Registry of a computer running a Windows operating system. This continuation from Module 3 covers other commonly encountered operating system artifacts during the analysis of the Windows Registry. Artifacts which reside in the Operating System category will be validated through use of the Registry explorer. This lesson will also explore the tracking of USB devices, Jump Lists, Prefetch Files, LNK Files, Recent Documents, User Assist, Virtual Machines, Windows Event Logs, and Windows Timeline, and how the relationship between these artifacts can tell a story of computer usage and potentially attribute activity to a specific individual.

GOALS

At the conclusion of this lesson, students will be able to use Magnet AXIOM to conduct examinations of computers using the Windows operating system to search for, recover, and tag key artifacts. The ultimate purpose of this module is to help establish file use and knowledge.

USB DEVICES

When a user connects a USB device to a host system for the first time, a small popup window is often displayed in the lower right corner of the Task Bar with a dialog similar to, “Installing device driver software,” followed by, “Device driver software was successfully installed.” These popup windows are usually followed by the Windows AutoPlay popup window on the desktop, which lists a drive letter for the USB device, with options for the user on how they wish to interact with the newly-recognized drive.

ARTIFACT INFORMATION	
Device Class ID	Disk&Ven_SanDisk&Prod_SanDisk_Cruzer&Rev_8.02
Serial Number	10803209FCD0759D&0
Friendly Name	SanDisk SanDisk Cruzer USB Device
Associated User Accounts	isaia
Last Assigned Drive Letter	E:
Last Connected Date/Time	9/13/2019 2:49:15 PM
First Connected Date/Time - Local Time	2019-08-30 13:20:00
Install Date/Time	8/30/2019 1:19:57 PM
First Install Date/Time	8/30/2019 1:19:57 PM
Last Insertion Date/Time	9/13/2019 2:49:12 PM
Last Removal Date/Time	9/13/2019 2:59:31 PM
Device Description	@disk.inf.%disk_devdesc%;Disk drive
Manufacturer	@disk.inf.%genmanufacturer%;(Standard disk drives)
Volume GUID	{a5f1eedd-ca87-11e9-afbf-080027c8d2c5}
EVIDENCE INFORMATION	
Source	Dashner Win10 PC.E01 - Partition 2 (Microsoft NTFS, 49.43 GB)\Windows\System32\config\SYSTEM

Figure 9.1 SHOWING THE TRACKING OF USB DEVICES

For the user, this process may take only a few moments. For the examiner, those few moments are filled with writes to numerous system files and the Registry, which can be analyzed and recovered with AXIOM, and stored in the CONNECTED DEVICES → USB Devices artifact category. These source files can include the **SOFTWARE** and **SYSTEM** registry hives, **setupapi.dev.log** files, **pagefile.sys**, Windows Events Logs, **NTUSER.DAT** hives, and system files within restore points and volume shadow copies. The information can provide the examiner with the date and time the USB device was first connected, and when Windows installed the necessary device driver software, as well as descriptors such as the device name, manufacturer, and device identifiers. AXIOM can also recover the drive letter assigned by Windows, and which Windows user profile was associated with the connected device. This information can help an examiner understand how a USB device was utilized on a given system after it was connected, and possibly explain how a suspect might have used the USB device in the commission of a crime. For example, if a user accessed a file on the USB device through the File Explorer utility, artifacts may be recovered from the user’s recent items folder, **pagefile.sys**, **\$MFT**, prefetch, and user assist to name a



few. Also, an LNK file may exist on the computer system providing valuable information for the examiner which can be seen in the Operating System → LNK Files artifact category. The entry can include the drive letter assigned to the USB device, as well as the volume serial number (VSN) and volume name for the device. Using the VSN or volume name as a keyword search in AXIOM Examine, may result in matching values being found in the CONNECTED DEVICES → USB Devices category, allowing the examiner to associate the USB drive with the LNK File entry. Highlighting an entry in the OPERATING SYSTEM → USB Devices artifact category, and reviewing the associated **Location** and **Source** links in the DETAILS pane, reveals that OPERATING SYSTEM → USB Devices artifact entries are built with data recovered from the MountedDevices, USBSTOR, and DeviceClasses keys within the SYSTEM registry hive, and the class ID and volume GUID values for the USB device in the MountPoints2 key in the NTUSER.DAT file for a Windows user. The combination of data recovered from these locations can potentially indicate a specific user of a USB device, and the drive letter associated with a device.

Name	Type	Data
DeviceDesc	REG_SZ	@disk.inf%disk_devices%Disk drive
Capabilities	REG_DWORD	0x00000010 (16)
Address	REG_DWORD	0x00000001 (1)
ContainerID	REG_SZ	{cf2265a9-538d-5bab-aa0d-948b9f96005e}
HardwareID	REG_MULTI_SZ	USBSTOR\DiskLexar__USB_Flash_Drive_8.07 USBSTOR\DiskLexar_
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW GenDisk
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
Service	REG_SZ	disk
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0001
Mfg	REG_SZ	@disk.inf%disk\Manufacturer% (Standard disk drives)
FriendlyName	REG_SZ	Lexar USB Flash Drive USB Device
ConfigFlags	REG_DWORD	0x00000000 (0)

Figure 9.2 REGISTRY EXPLORER OF USBSTOR KEY TRACKING DEVICES BY THEIR NOMENCLATURE

The USBSTOR key of the SYSTEM registry hive provides several of the values categorized in the ARTIFACT INFORMATION fields displayed in the DETAILS pane.

RUNNING EXERCISE

USB DEVICES

- While still in the Artifact explorer, expand the CONNECTED DEVICES category and select the USB Devices category.
- Sort by the Friendly Name column.
- Does it appear all the USB devices connected to Dashner's computer have been submitted for analysis?

- Note the beginning Serial Number values for each device:

A227D	Lexar USB Flash Drive
10803	SanDisk Cruzer USB Device
900059	Verbatim Store N Go USB Device

- Switch to the Registry explorer in the NAVIGATION pane.
- Expand the **SYSTEM** hive and expand the ControlSet001 key and then expand the Enum and USBSTOR keys.
- Expand each Disk&Ven entry and note the sub keys named with the USB device Serial Number as seen in the Artifacts Explorer, identifying three different USB devices.
- Switch back to Artifacts Explorer, select the entries for the Lexar and SanDisk drives and create a new tag associated with those devices named “Dashner USB Devices”.
- Select the entry for the Verbatim USB drive and create a new tag named “Dashner USB Device – Not Submitted”.

LNK FILES

The LNK Files artifacts are parsed from numerous locations within the operating system. Which can include the **\$MFT**, **pagefile.sys**, Program Files folder, ProgramData folder, Program Files (x86) folder, and the user's Recent folder. In addition, data can be carved from unallocated space. LNK files are a relatively simple but valuable artifact for the forensic examiner. They are shortcut files that link to an application, folder, or file found on a user's system or removable media, and end with an extension of *.lnk. LNK files are named such because of the extension in the naming convention. LNK files can be created by the user or automatically by the Windows operating system. Each occurrence and file location have their own value and meaning. Windows-created LNK files are generated when a user opens a local or remote file or document, which can give an examiner valuable information and insight into a user's activities. LNK files are also excellent artifacts for forensic examiners who are trying to find files that may no longer exist on the system they're examining. The files might have been wiped or deleted, stored on a USB, or network share. Although the file may no longer exist, the LNK files associated with the original file could still exist on the system and provide valuable information as to what was accessed by the user. Information parsed for the LNK file can be useful when searching or filtering within a case, to help the examiner narrow the focus on a specific artifact or identify associations between multiple artifacts. For



example, the Volume Serial Number (VSN) value from an LNK file can be used to help identify an entry in the USB Devices artifacts category, and perhaps even associate a drive letter to a USB drive.

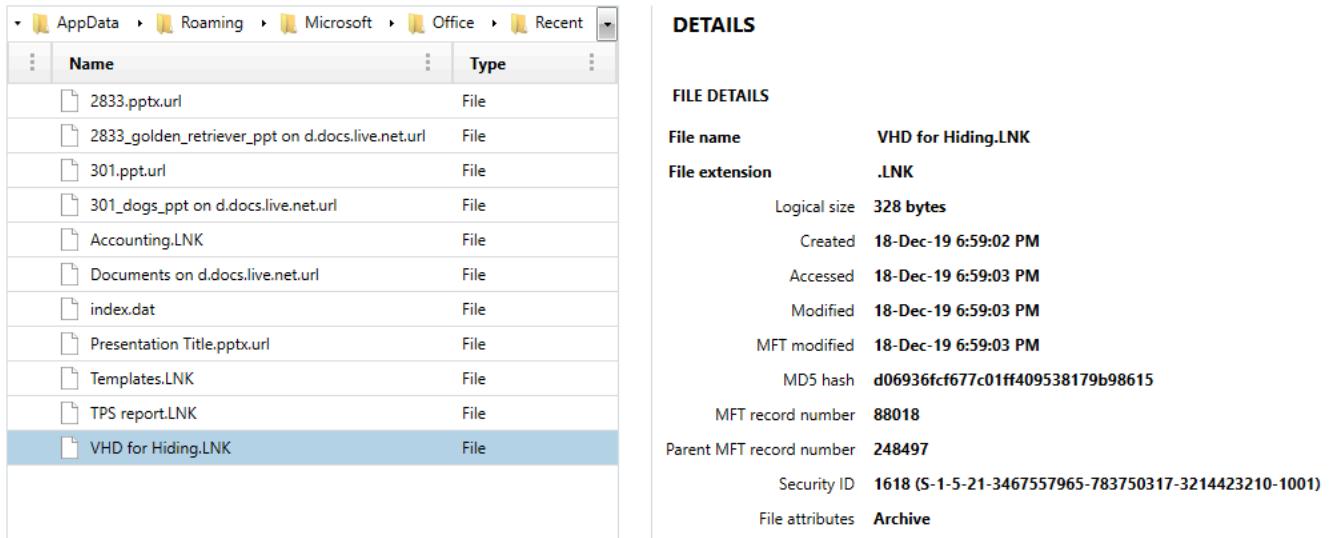


Figure 9.3 LNK FILES INTERPRETED BY MAGNET AXIOM

The LNK files parsed from the user's profile folder are found in the path: `Users\<profile>\AppData\Roaming\Microsoft\Windows\Recent\`. Within this folder are entries with the `*.lnk` file extensions. Information parsed by AXIOM from LNK files can include the linked path for the target item, timestamps associated with both the LNK file and the target file, target file size, volume name and volume serial number of the device the target file is stored on, NetBIOS name and MAC address of the host the target file is stored on, and network details if the target file was stored on a remote computer or network share.

RUNNING EXERCISE

LNK FILES

- Return to the Artifacts Explorer.
- In the FILTERS bar, open the Artifacts drop-down menu, check LNK Files, and click **OKAY**.
- The artifacts in the NAVIGATION pane should now show MATCHING RESULTS and be limited to LNK File entries only.
- Expand the OPERATING SYSTEM category and then select the **LNK Files** artifact in the NAVIGATION pane.

- In the keyword search window of the FILTERS bar, enter “Windows\Recent” and click **GO**.
- The EVIDENCE pane should now be limited to only LNK File entries from the Dashner user account Recent folder.
- Sort by the Linked Path column.
- Scroll through the list of artifacts and note the entries grouped together from the ‘C’, ‘E’, and ‘F’ volumes.
- Locate the Volume Name column in the evidence pane. Left-click and drag the Volume Name column to place it beside the Linked Path column. Sort by the Volume Name column and note the removable drive entries for “MYUSB” and “SANDISK.”
- Compare the Linked Path entries for the E:\ drive to the Volume Name column. Does it appear more than one USB device was assigned the E:\ drive letter?
- Select all of the artifacts with a Volume Name of MyUSB, and create a new tag for “MyUSB LNK Files”.
- Clear the filters to reset the view.

RECENT DOCS

The OPERATING SYSTEM → MRU Recent Files and Folders artifact category, displays the resources, files, and application shortcuts accessed by a specific Windows user account, utilizing data recovered from a user’s **NTUSER.DAT** hive key:

`Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs`

In the root of the `RecentDocs` key will be sub-keys named for the different file extensions (and one for folders) accessed by the Windows user account. The values stored within the sub-keys of the `RecentDocs` entries are listed numerically, beginning with “0” and incrementing up in value for each newly-added entry. Within each sub-key is an entry labeled `MRUList`, which Windows uses to keep track of the order of file access by the user. As a result, the entries in the `MRUListEx` can be compared to the listed values, to help identify the order. Viewing the corresponding value for the entry, an examiner can see the *.lnk file entry information, in both ASCII and Unicode.

Given the often-questionable efficiency with which Windows performs its housekeeping tasks, if a user deletes the entries within the Recent folder, it is possible that an investigation of the `RecentDocs` key



of the NTUSER.DAT file will reveal a listing of the files and folders accessed by the user, even if the original files and/or folders have been subsequently deleted.

File/Folder Name	File/Folder Link	Registry Key...	Regi...	Valu...
Videos.7z	Videos.lnk	10-Sep-19 3:47:35 PM	1	2
Pictures_2.7z	Pictures_2.lnk		3	1
flame.avi	flame.lnk	30-Aug-19 9:15:01 PM	1	0
Golden puppies-pdf.axx	Golden puppies-pdf.lnk	18-Dec-19 6:57:48 PM	1	1
Pure Gold-docx.axx	Pure Gold-docx.lnk		2	0
microsoft.com&form=B000...	https--www.bing.com-sear...	03-Jul-19 10:32:51 PM	1	0
www.mailvelope.com/	https--www.mailvelope.co...	29-Aug-19 7:23:37 PM	1	1

Figure 9.4 MRU Recent Files & Folders

The Windows operating system tracks files that are opened and saved through a standard Windows Open/Save dialogue. The information is presented in the Operating System → MRU Opened/Saved Files artifact category. It is common for Windows applications, both Microsoft and third-party, to have an Open/Save dialogue which allows the user to access or save a file. This is commonly achieved through an API (Application Programming Interface) made available to developers by Microsoft. Activity which utilizes the Open/Save dialogue is recorded in a user's **NTUSER.DAT** hive, within the key:

```
Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\
OpenSavePidMRU
```

Similarly to the RecentDocs key, the root of the OpenSavePidMRU key contains sub-keys named for the different file extensions accessed by the Windows user account associated with the particular **NTUSER.DAT** registry hive file. The values stored within the sub-keys of the OpenSavePidMRU entries are listed numerically, beginning with "0" and incrementing up in value for each newly added entry.

Details of the specific application executables that were used to open the files detailed within the OpenSavePidMRU key, are also tracked by Windows, and are presented in the artifact category OPERATING SYSTEM → MRU Folder Access. This data is recorded in a user's **NTUSER.DAT** hive, within the key:

```
Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\
LastVisitedPidIMRU
```

JUMP LISTS

Jump Lists were introduced in the Windows 7 operating system and continue to be an integral part of the Windows 10 operating system, providing valuable user activity information to examiners. Like the LNK File category, the Jump List artifacts are also parsed from the folder **Users\<profile>\AppData\Roaming\Microsoft\Windows\Recent**. Within the Recent folder are two sub folders, **AutomaticDestinations**, and **CustomDestinations**.

Jump List entries contain information for the resource accessed by the user including the path, the name of the application used to access the resource, the date and time the application was used, and the resource accessed. Jump Lists also track details of the drive the resource was accessed from including VSN and volume label and if the Jump List is an automated item created by the operating system or a custom item created by the user. The **AutomaticDestinations** folder contains entries generated by the operating system, and other default applications in Windows, while the **CustomDestinations** folder stores entries created by the user.

Jump Lists can be very useful for the examiner for a number of reasons. They can identify files and resources accessed by the user, including last accessed timestamps and file paths. Jump Lists store information on a user's most recently used files and applications. Jump lists also help the examiner identify applications the user has used to create, edit, or view specific files, such as graphic files and videos. They can help the examiner establish user history and timelines for user behavior and file access. Jump Lists can also provide detailed information on the object or volume on which the user accessed the files with an application. Finally, a Jump List entry, like an LNK File entry, may be the only remaining evidence that a file existed on a local system or removable media, as Jump List entries remain even after the original source file has been deleted.



ARTIFACT INFORMATION	
App ID	4cb9c5750d51c07f
Potential App Name	Microsoft Movies & TV
Linked Path	E:\Vids\Video of a Brown Puppy Playing with a Ball.mp4
Volume Name	MYUSB
Volume Serial Number	BC942E81
Target File Created Date/Time	30-Aug-19 9:07:14 PM
Target File Last Modified Date/Time	30-Aug-19 5:34:12 PM
Target File Last Accessed Date/Time	30-Aug-19 5:00:00 AM
Jump List Type	Automatic
Drive Type	DRIVE_REMOVABLE
Target File Size (Bytes)	5816586
Last Access Date/Time	30-Aug-19 9:08:06 PM
Entry ID	1
Data	E:\Vids\Video of a Brown Puppy Playing with a Ball.mp4
Pin Status	Not Pinned

Figure 9.5 Jump list data for a video file showing it was accessed and opened.

The **AutomaticDestinations** folder stores entries automatically generated by the Windows operating system when a user launches an application, accesses a file, or interacts with File Explorer to access a known resource. Each file is named with an application ID value, followed by **automaticDestinations-ms**. The application ID value is maintained by Microsoft and is unique to the application being tracked by the Jump List functionality of Windows. According to Microsoft, it represents a CRC64 hash of the path for the application. AXIOM uses the application ID (App ID) value for known applications to populate the Potential App Name column data within the EVIDENCE pane. A useful online resource for lists of application identifiers is:

https://forensicswiki.xyz/wiki/index.php?title=List_of_Jump_List_IDs

EVIDENCE (15)		
	Name	Ties to AppID
Recent		
AutomaticDestinations	469e4a7982cea4d4.automaticDestinations-ms	File
CustomDestinations	4cb9c5750d51c07f.automaticDestinations-ms	File
SendTo	5d696d521de238c3.automaticDestinations-ms	File

Figure 9.6 AUTOMATICDESTINATIONS APPID TO LINK TO ASSOCIATED PROGRAM

The **automaticDestinations-ms** file uses a compound binary file structure. Within the file is a destination list, **DestList** data stream, which serves as a Most Recently Used (MRU) or Most Frequently Used (MFU) list. Last accessed timestamps, target file names and paths, object and volume identifiers, and references to the Microsoft Shell Link (MS-SHLLINK) data streams are stored within the compound file itself. The MS-SHLLINK streams are commonly used to support the launching of an application, and links to other objects using Object Linking Embedding (OLE) functionality. For Jump List entries, the MS-SHLLINK functions as a reference to a target file, so it can be accessed more efficiently by the system. The combination of DestList and MS-SHLLINK data streams provide the information AXIOM uses to populate the columns of the EVIDENCE pane and ARTIFACT INFORMATION section of the DETAILS pane.

The **CustomDestinations** folder operates similarly to the **AutomaticDestinations** folder. Each entry uses the same naming convention for the files, with an alphanumeric prefix that represents a CRC64 hash for the application path, which AXIOM uses to identify the “Potential App Name” value. Unlike the automaticDestinations-ms files, which are generated by the operating system, the customdestinations-ms entries are created when a user pins an application to a specified location, such as the Task Bar. In addition, the customDestinations-ms file does not use the compound binary file format, but a more simplistic structure. The MS-SHLLINK data streams are still used, but the data is stored in a series of LNK-formatted sequential entries. Finally, unlike an automaticDestinations-ms entry, which is controlled by the operating system, additional metadata can be added to the customDestinations-ms data stream and is controlled by the application associated with the custom Jump List entry. Similar to the automaticDestinations-ms Jump List entries, the customDestinations-ms files can provide the examiner with valuable information which can be used to identify frequently-accessed applications (pinned), historical user data, timeline analysis data, and potential references to applications which may no longer be available on the local system being analyzed.

Name	Type
5d696d521de238c3.customDestinations-ms	File
6d2bac8f1edf6668.customDestinations-ms	File
7e4dca80246863e3.customDestinations-ms	File

Figure 9.7 CustomDestinations created when a user pins apps to a specific location (Taskbar, Start Menu)

RUNNING EXERCISE

JUMP LISTS

- Select the Jump Lists artifact in the NAVIGATION pane.
- In the EVIDENCE pane, sort on the Linked Path column.
- Right-click on the Linked Path column and select Filter on column. Enter “E:\” as a keyword to filter the list. Note the entries for the drive letter E:\ previously identified in the LNK File entries.
- Sort by the Volume Name column. Create new tags for “MYUSB USB Device Jump List”, “SanDisk USB Device Jump List” and another for “Verbatim USB Device Jump List” and associate the findings accordingly in each one of those newly created tags.
- Clear any filters.
- Sort by the Potential App Name column.
- Note the files that were accessed within the “isaia” Windows user account using Microsoft Movies & TV.
- Select the Microsoft Movies & TV entries with potentially relevant file names and create a new tag for “Microsoft Movies & TV Jump List Entries” and associate those artifacts with the newly created tag.
- Note the files that were accessed within the “isaia” Windows user account using VLC Media Player.
- Select the VLC Media Player entries with potentially relevant file names and create a new tag for “VLC Media Player Jump List Entries” and associate those artifacts with the newly created tag.

PREFETCH

AXIOM parses the Windows Prefetch artifacts from the Prefetch folder, located at **Windows\Prefetch**. The Windows Prefetch functionality was first introduced in Windows Server 2003, and Windows XP. There are two types of prefetching. **Boot prefetching** gathers data of files that were accessed during the boot process to make it faster the next time the computer boots. Forensically speaking boot prefetching has no value. **Application prefetching** tracks the application that was launched, and the last 8 dates and times the application was launched. By default, the Prefetch service tracks both types of operations, but the `EnablePrefetcher` value of the `PrefetchParameters` key in the `SYSTEM` hive can be modified to track one or the other, or be disabled entirely. When an application is launched on the host system for the first time, a corresponding `.pf` file is also created in the Prefetch folder. The purpose of

the application prefetch is to speed up the time it takes Windows to load applications. The files stored in the Prefetch folder are listed alphabetically, based on the name of the application that was launched.

The naming convention for the **.pf** file begins with the application name and extension, followed by a proprietary hash value, and the **.pf** extension. For example, the Prefetch file entry for QBittorrent.exe would be **QBITTORRENT.EXE17EBDC32-.pf**.

According to Microsoft, the Prefetch files are treated as data objects, and therefore a maximum storage capacity has been set for the Prefetch folder entries of 126 in Windows XP, and increased to 129 in Windows Vista, 7, 8, and 1024 in Windows 10.

Application Name	Application Path	Appl...	File Created...	Last Run Date...	File...	2nd Last Run...
QBITTORRENT.EXE	\VOLUME\01d53125b8d3...	3	17-Jul-19 3:19:52 PM	29-Aug-19 2:04:36 PM	17EBDC32	17-Jul-19 3:25:26 PM
QBITTORRENT_4.1.6_X64_SETUP.E		3	17-Jul-19 3:03:14 PM	17-Jul-19 3:03:04 PM	838A5150	17-Jul-19 3:02:59 PM
QBITTORRENT_4.1.7_X64_SETUP.E		3	17-Jul-19 3:21:44 PM	17-Jul-19 3:21:34 PM	186C0545	17-Jul-19 3:21:29 PM

Figure 9.8 Prefetch listing for QBittorrent.exe

Once the maximum number of entries has been reached, Windows will automatically delete all but 32 of the entries. There does not seem to be a factor which determines which 32 entries are retained, but it may follow a First in, First Out (FIFO) convention, in which the most recent entries would be retained.

As mentioned earlier, operating system artifacts can provide an examiner with a very clear picture of a user's behavior on a host system, provided the forensic tool deployed can recover the relevant data within the artifacts. Among the many key artifacts are the names of applications launched on the host system, the date and time they were most recently launched, and how many times they have been launched. An analysis of the **UserAssist** key in the **NTUSER.DAT** file provides this data as it relates to a specific Windows user profile. The Windows Prefetch files track similar information, but are system wide, rather than user specific.

The data stored within the Prefetch files, for versions of Windows prior to 10, was uncompressed, and relatively intuitive to interpret. Windows 10, Prefetch and SuperFetch files are compressed with the XPRESS HUFFMAN algorithm, a.k.a. the MAM format, which is not new. Windows 8.1 uses MAM to compress SuperFetch files, but not Prefetch files. Moreover, from what is known checksum is present only for SuperFetch files and never for Prefetch files.

AXIOM understands the compression mechanism and can decompress the data, and parse the application name, date and time of last launch, and the number of launches.



RUNNING EXERCISE

WINDOWS PREFETCH FILES

- Select the Artifact explorer in AXIOM Examine and clear any filters you may have in place.
- Expand the **OPERATING SYSTEM** category and select the Prefetch Files - Windows 8/10 artifact.
- Sort by the Application Name column.
- Locate the entry for “VLC.EXE”.
- The **VLC.EXE** application was last launched on **08/Oct/2019** at **19:22:16**. Create a new tag for “**VLC.EXE**” and include the **VLC.EXE** artifact.
- To understand the installation and use of **VLC.EXE** on the host system, we need to examine several artifact categories. From the Artifacts drop-down menu of the FILTERS bar, check the following categories:
 - LNK Files
 - Installed Programs
 - Prefetch Files – Windows 8/10
 - UserAssist
- Enter “**VLC**” in the search box on the FILTERS bar and click **GO**.
- In the NAVIGATION pane, expand the **OPERATING SYSTEM** category select the LNK Files artifact and note the entries in the EVIDENCE pane with a created date of 17/Jul/2019 at 10:18:17. One entry is from the Desktop, most likely after the application was downloaded and installed. Another is from the Start Menu, which is probably where VLC had an option to include in the Start Menu during the installation. The other LNK file entries appear to be associated with online documentation and weblinks relating to the Program. Take a moment to review those and note the recovery method listed.
- Select the UserAssist category. Note the entry for VLC.exe, the Last Run Date/Time and Application Run Count values. Also note a Userassist entry for the VLC-3.0.7.1-win64.exe installer.

Select the Installed Programs category and view the VLC entry in the EVIDENCE pane. Note the value listed in the **Version** column which matches the “VLC-3.0.7.1-win64.exe” installer associated with VLC.

- At the top of the **Navigation** pane, select MATCHING RESULTS so all items are listed in the **EVIDENCE** pane. Select all items listed in the **EVIDENCE** pane and add them to the VLC tag.

USERASSIST

Introduced in the Windows XP operating system, the UserAssist artifacts are parsed from the **NTUSER.DAT** Registry hive, from the key:

`Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\<GUID>\Count.`

Within the `Count` sub key are the values which track information for shortcuts created and accessed by the user, as well as applications launched by the user. Since the artifacts are parsed from the **NTUSER.DAT** file, they are unique to a specific Windows user profile, and can provide valuable insight for an examiner into a user's behavior on a system. The data parsed from the `Count` values includes the name of the application launched by the user, the number of times the application has been launched, and the date and time the application was last launched.

The following identifies the GUIDs within the UserAssist key, in the Windows 10 operating system:

Windows 10:

{FA99DFC7-6AC2-453A-A5E2-5E2AFF4507BD}	Link (*.lnk) entries
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	Application (*.exe) entries

MATCHING RESULTS (10 of 210)				
User Name	File Name	Application Run Cou...	Last Run Date/Time	Source
dashner	(9E3995AB-1F9C-4F13-B827-48B24B6C7174)\TaskBar\Google Chrome.lnk	12	10/20/2016 8:50:32 PM	DashnerW
dashner	(9E3995AB-1F9C-4F13-B827-48B24B6C7174)\TaskBar\Google Chrome.lnk	10	10/5/2016 9:34:16 PM	DashnerW
dashner	(7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E)\Google\Chrome\Application\chrome.exe	4	10/11/2016 1:28:45 AM	DashnerW
dashner	(7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E)\Google\Chrome\Application\chrome.exe	4	10/11/2016 1:28:45 AM	DashnerW
dashner	Chrome	23	10/20/2016 8:50:32 PM	DashnerW
dashner	Chrome	21	10/7/2016 5:33:29 PM	DashnerW
dashner	C:\Users\Public\Desktop\Google Chrome.lnk	11	10/7/2016 5:33:29 PM	DashnerW
dashner	C:\Users\Public\Desktop\Google Chrome.lnk	11	10/7/2016 5:33:29 PM	DashnerW

Figure 9.9 Artifact Explorer of the UserAssist registry entries



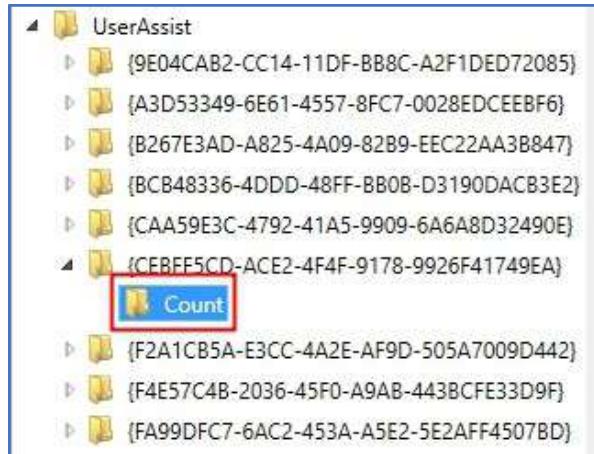


Figure 9.10 Raw registry view of UserAssist registry entries

The data within the Count values is stored using a ROT13 cipher in which the letters of the Roman alphabet are rotated 13 (Right on Table, “ROT”) positions. For example, an entry of “Puebzs” is the obfuscated form of “Chrome.” In the table below is a reconstructed alphabet based on ROT13.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

AXIOM decodes the ROT13 value for the File Name, the numeric value for the Application Run Count, and the 64-bit value for the timestamp in the Last Run Date/Time field in the ARTIFACT INFORMATION section. Given that the number of entries within UserAssist can be quite lengthy, if an examiner knows the name of the application of interest, the right-click Filter on column feature can be applied to the File Name column in the EVIDENCE pane, and a search can be conducted for the name of the application. The User Name and File Name columns in the EVIDENCE pane can also be sorted, to provide the examiner with a more manageable view of applications for a specific user if multiple users are present on a system.

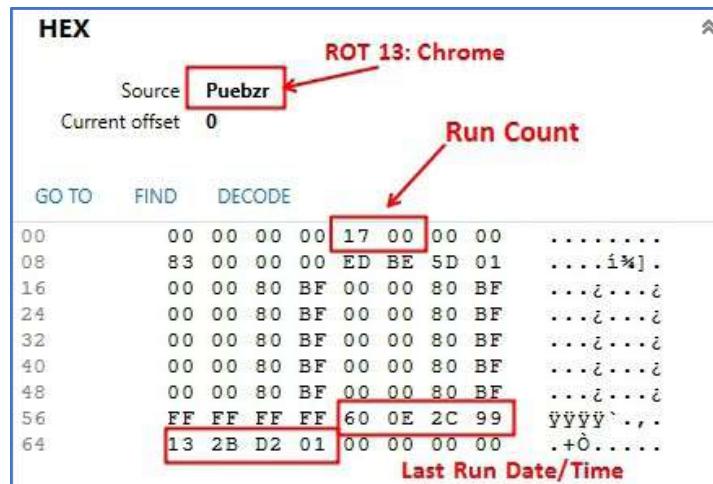


Figure 9.11 UserAssist entry for Chrome

WINDOWS TIMELINE

The Windows Timeline feature was introduced with the April 2018 update of Windows 10. Windows Timeline keeps a chronological list of user activities on a system. This artifact tracks various user actions including folders opened with File Explorer, recently opened files and their associated applications, and opened web pages. By default Windows Timeline retains 30 days of activity, with the most frequent activity shown as thumbnails in the Windows Timeline display. However, a user can select to see all the stored activity for a particular day by selecting the link next to the date, “See all xx activities”, where xx is the number of items stored for that particular day. Depending on the user’s account settings, if they are logged into the system with a Microsoft account, they can sync their Windows Timeline data across multiple devices. This synchronization feature is scheduled to be disabled by Microsoft from June 2021. Windows Timeline data is stored within each Windows user account’s AppData folder in an SQLite database named **ActivitiesCache.db**.



DETAILS	
 Windows Timeline Activity	
ARTIFACT INFORMATION	
Application Name	%windir%\system32\cmd.exe
Display Name	Command Prompt
Activity Type	Open App/File/Page
Focus (Seconds)	0
Start Date/Time	10/8/2019 1:32:18 PM 
Activity ID	aef1df71-61db-9079-2e4d-f13d388f01b2
Platform	windows_win32
Created Date/Time	10/8/2019 1:32:18 PM 
Last Modified Date/Time	10/8/2019 1:32:18 PM 
Last Modified On Client Date/Time	10/8/2019 1:32:18 PM 
EVIDENCE INFORMATION	
Source	Dashner Win10 PC.E01 - Partition 2 (Microsoft NTFS, 49.43 GB)\Users\isaia\AppData\Local\ConnectedDevicesPlatform\decd7e72d1f0dd2\ActivitiesCache.db
Recovery Method	Parsing
Deleted source	
Location	Table: ActivityOperation(OperationOrder: 39)
Evidence number	Dashner Win10 PC.E01

Figure 9.12 Windows Timeline Data

WINDOWS EVENT LOGS

The ability of the Windows operating system to log events has been available for system administrators since the early 1990's. Although the early event logs lacked the detail of today's logs, the event service provided system admins with a standardized format, and centralized location, for viewing important application and system activities recorded by the Windows operating system. In general, the event types include general information, warnings, errors, successes audits, and, failure audits. If necessary, the information from the early event logs could be used to help correct a problem or improve overall system performance.

EVIDENCE (104,503)				
	Even...	Even...	Secu...	Created Dat...
	4625			7/2/2019 4:35:47 PM
	1531		LocalSystem	7/2/2019 4:35:48 PM
	5615		LocalSystem	7/2/2019 4:35:51 PM

Figure 9.13 Windows Event Logs artifacts

Even though the more recent versions of the Windows operating system have expanded the degree of detail included in the event log files, increased the number of services which use the Windows Event Log Application Programming Interface (API), and improved the interoperability among the various services which can write to an event log, the basic underlying functionality remains the same.

AXIOM parses the Windows Event Logs artifacts from the **.evt/.evtx** files stored within the **Windows\System32\winevt\Logs** folder. The data parsed from the file includes the numeric Event ID value, the Security Identifier (SID) associated with the log entry, the created date/time for the log entry, a brief summary of the event, the level of the event (Information, Warning, Error etc.), the service that was associated with the log entry, the name of the computer, and detailed event data for the log entry.

Based on improvements to the Windows event logging functionality, and the capabilities of most forensic tools for parsing the event log entries, examiners are faced with several challenges. Rather than dealing with just the core system level event logs of the past (Application, Security, and System), the Logs folder may now contain over one hundred event logs. Those event logs are generated by the operating system and each containing potentially hundreds of individual entries. In addition to the Windows-based event logs, third-party applications are also allowed to generate their own custom event logs provided they comply with the Windows API requirements. Adding the functionality to third party applications to generate logs, compounds the challenge of reviewing such large volumes of information.

EVIDENCE (129)			
	Name	Type	File ext...
	Windows PowerShell.evtx	File	.evtx
	ThirdParty Diagnostics.evtx	File	.evtx
	System.evtx	File	.evtx
	Setup.evtx	File	.evtx
	Security.evtx	File	.evtx
	OAlerts.evtx	File	.evtx
	Microsoft-WindowsPhone-Connectivity-WiFiCon...	File	.evtx

Figure 9.14 Windows Event Logs



WINDOWS EVENT LOG FILTERING

What is the best way to find a needle in a haystack? Use a Magnet! AXIOM's searching and filtering functionality make it easy to find the information examiners are looking for in this avalanche of data. It's not uncommon for examiners to be presented with well over one hundred thousand individual Windows Event Logs artifacts in their case. The challenge for the examiner is to find a way of narrowing their focus to only the event log entries which are most relevant to their investigation, such as the number of times a laptop successfully connected to a wireless network, whether a user account was created or deleted, or if an application was installed, such as an anti-forensics tool capable of preventing the recovery of critical evidence. AXIOM Examine already categorizes certain Windows Event Logs as individual artifact categories:

- Networking Events
- Office Alert Events
- Scheduled Task Events
- Script Events
- Service Events
- System Events
- User Events
- User PNP Events

Additionally, using the filtering capabilities of AXIOM Examine, users can very quickly create a simple or compound filter condition that makes short work of identifying the key Windows Event Log entries. An examiner can filter by a user's RID in the Security Identifier column, or filter for keywords within the Event Data or Event Description Summary columns. If a user wants to narrow the results, a known value can be used as a filter on column criteria. For example, a filter for '1033' on the Event ID column will display event logs entries which relate to Windows Installer activity.

MATCHING RESULTS (17,531 of 108,568)		
	Event ID	Security Identifier
S-1-5-21-3467557965-783750317-3214423210-1001		
MATCHING RESULTS (4 of 108,568)		
	Event ID	Security Identifier
S-1-5-21-3467557965-783750317-3214423210-1001	1033	S-1-5-21-3467557965-783750317-3214423210-1001

Figure 9.15 Reduction from 17,000+ events for Security Identifier 1001 to just 4 that match Event ID 1033

In some cases, it may not be necessary to apply an additional filter condition to the results to identify the relevant log entries. Instead, simply using the column sorting functionality of AXIOM Examine may suffice. For example, if the initial filter results are relatively manageable, but they include entries associated with numerous SIDs on the local system, the examiner can left-click the Security User ID column, and sort numerically by user SID. The examiner can then use the up/down scroll bar to locate, examine, or tag the entries for a specific user's SID, which will all be displayed consecutively.

MATCHING RESULTS (17,531 of 108,568)		
	Event ID	Security Identifier
1097	S-1-5-21-3467557965-783750317-3214423210-1001	
1097	S-1-5-21-3467557965-783750317-3214423210-1001	
1097	S-1-5-21-3467557965-783750317-3214423210-1001	
505	S-1-5-21-3467557965-783750317-3214423210-1001	
500	S-1-5-21-3467557965-783750317-3214423210-1001	
505	S-1-5-21-3467557965-783750317-3214423210-1001	
500	S-1-5-21-3467557965-783750317-3214423210-1001	
505	S-1-5-21-3467557965-783750317-3214423210-1001	
505	S-1-5-21-3467557965-783750317-3214423210-1001	

Figure 9.16 Column sorting on Security Identifier column to find Event IDs grouped by user



RUNNING EXERCISE

WINDOWS EVENT LOGS

- Select the Artifact explorer in AXIOM Examine and clear any filters you may have in place.
- Expand the OPERATING SYSTEM category and select the Windows Event Logs artifact.
- We want to identify information related to one of the removable disks seen in the USB Devices artifact category. Currently, there are too many event log artifacts to manually review. We will use the sorting and filtering capabilities of AXIOM to reduce the number of event log entries.
- Return to the CONNECTED DEVICES → USB Devices artifact category and highlight the entry for the Verbatim USB drive.
- In the DETAILS pane, next to the timestamp for Last Connected Date/Time, click the relative time filter button  .
- De-select the check box under **SET RANGE**, then set the **Start range** to 1 minute before and **End range** to 30 minutes after this point. At the bottom of the **Set relative time** window, set the explorer to **Current explorer** and NOT **Timeline explorer**.
- Copy of the value of the Verbatim USB drive's serial number listed in the DETAILS pane, excluding the &0 at the end of the serial number.
- Return to the Windows Event Logs artifact. Locate the **Event Data** column and select the option to **Filter on column**. Apply a filter for the Verbatim USB device serial number "90005980CC384D12" located in the USB Devices artifact category.
- Take note that there could be multiple event logs generated from the connection of a USB device. If an examiner is looking for connection history of certain removable volumes, searching for device names or serial numbers within these logs can help to timeline this activity.
- Clear any active filters.
- We want to identify information relating to logon/ logoff information relating to the Dashner user account. Select the OPERATING SYSTEM → Windows Event Logs – User Events category. Locate the **Target User SID** column and select the option to **Filter on column**. Apply a filter for the term "1001", Dashner's relative identifier.
- Locate the **Event Description Summary** column and select the option to **Filter on column**. Select the Advanced option and under the **SEARCH BY TERM** options choose to Include the term "logged on".

- Select the **ADD ANOTHER TERM** option.
- Tick the radio button next to **Any of the following terms (OR)** and include the term “logged off” and click the **SEARCH** button.
- Review the results to identify logon and logoff activity for the user account with the relative identifier “1001” associated with Dashner.

MODULE REVIEW

In this module students learned about OS Artifacts, Registry Artifacts, USB tracking, LNK files, Recent Docs, and Jump Lists. Students also learned about Prefetch, Event Logs and how to filter on these items. These artifacts can help lead examiners to documents, devices, and media items that have been interacted with by the user on the system.



REVIEW QUESTIONS

To help reinforce the learning objectives for this module, the following review questions have been provided:

1. If a user is suspected of watching a video from an external drive connected to the host system, what OPERATING SYSTEM artifacts can help the examiner identify the name of the file, path for the file, and application used to watch the video?
2. The Windows Prefetch service provides examiners with which three key pieces of information?
3. What AXIOM Examine feature allows examiners to quickly identify the most relevant Windows Event Log entries?

STUDENT EXERCISE

This exercise is based on the Dashner case scenario from Module 1.

- From the **Artifacts** explorer in AXIOM Examine, clear any filters you may have in place.
 - Expand the **OPERATING SYSTEM** category and review the results in the Prefetch Files Windows 8/10 artifact.
 - According to the information in this artifact category, how many times was the executable for QBittorrent.exe ran? When was the last run date/time?
-

- In the LNK Files category, sort the artifacts by the Target File Created Date/Time column. What item(s) of interest appear on 18-Dec-2019? Hint: Look for a .docx file
-

- What is the volume name where these items are located? _____
 - Tag the item(s) appropriately.
 - Based on the Windows Timeline Activity artifact, what is the date/time that the Axcrypt program was used? _____
 - View the Windows Event Logs artifact. Filter the Event Description Summary for “logoff”. When was the last user initiated logoff? _____
 - What is the Event ID associated with this? Tag this item appropriately.
 - Search the User Assist artifact category for information related to the Brave browser. According to data from the NTUSER.DAT associated with the “isaia” Windows user account, how many times was the application ran? _____
 - Regarding the Brave browser, what were the Focus count and Focus seconds?
-



- In the Jump Lists artifact category, filter on the Volume Name column for “SANDISK”. After reviewing data contained in the Linked Path column, What appears to be the contents of the folder “New Friends”? _____
- What drive letter(s) can be associated to the device with a volume name of “SANDISK”? _____
- Reviewing information in the User Accounts artifact category, what is the user name associated with the RID of 500? _____
- Using the Recycle Bin artifact category, identify the date and time of deletion for the file “hanging-golden-retriever-puppy-statue-webp” and its original location on the evidence.

Notes

Notes





MAGNET
FORENSICS®

MODULE 10: Media



LEARNING OBJECTIVES

In this lesson, students will take part in lecture, instructor-led exercises, and student practical exercises to gain an understanding of what types of media files are parsed and carved by AXIOM Process and how the content of media files can be viewed in AXIOM Examine. Students will also learn about the Magnet artificial intelligence module (Magnet.AI), manual categorization of images, the Officer Wellness settings in AXIOM, and the various explorers used throughout the AXIOM software.

GOALS

At the conclusion of this lesson, students will be able to use AXIOM Examine to efficiently review media artifacts and determine the best view for the different artifact types. Students will be able to activate and process media artifacts using the Magnet.AI picture categorization modules and utilize the Officer Wellness functionality to reduce exposure to indecent and distressing media.



MEDIA ARTIFACTS

AXIOM Process can both parse and carve for multimedia files during the processing phase. AXIOM Process first parses any MEDIA artifacts from the evidence file(s), then it searches for and carves any MEDIA artifacts within other files on the disk, as well as from the file slack, uninitialized file areas, and unallocated space.

Some of the currently supported media formats are listed below. The examiner should refer to the Artifact Reference guide for a full list of supported media artifacts including raw picture formats.

PICTURES

Any pictures that Magnet AXIOM recovers are reported in the [Pictures](#) artifact. This artifact uses both parsing and carving techniques to recover a range of different picture formats. Magnet AXIOM can also recover many different types of RAW picture formats which are typically used with cameras.

Type	Extension	Parsing support	Carving support
BMP	.bmp	Yes	Yes
	.dib	Yes	Yes
JPEG	.jpg	Yes	Yes
	.jpe	Yes	Yes
	.jpeg	Yes	Yes
GIF	.gif	Yes	Yes
HEIC	.heic	Yes	No
HEIF	.heif	Yes	No
ICO	.ico	Yes	No
iThmb	.ithmb	Yes	No
PNG	.png	Yes	Yes
TIFF	.tiff	Yes	Yes

VIDEOS

Magnet AXIOM can supports a number of different video container formats, using both parsing and carving, and displays results in the [Videos](#) artifact. For information about what it means for a file to be parsed or carved, see [Parsing and carving](#).

Type	Extension	Parsing support	Carving support
Audio Video Interleave	.avi	Yes	Yes
DivX	.divx	Yes	No
Matroska	.mkv	Yes	No
MPEG-1, MPEG-2	.mpg, .mpg1, .mpg2, .mpeg, .mpeg1, .mpeg2, .m2v, .m2p, .mod, .vob	Yes	Yes
MPEG-4	.mp4, .mp4v, .f4v, .lrv, m4v	Yes	Yes
QuickTime	.3gp	Yes	Yes
	.3ga	Yes	No
	.3g2	Yes	No
	.m4a, .m4p	Yes	No
	.mov	Yes	Yes
	.qt	No	Yes
WebM	.webm	Yes	No
Windows Media Video	.wmv, .wm, .ASF, .dvr-ms	Yes	Yes

AUDIO

The [Audio](#) artifact contains the MP3 and WAV files that are recovered during a scan. On mobile devices, the [AMR Files](#) artifact contains voicemail messages.

Type	Extension	Parsing support	Carving support
AMR	.amr	No	Yes
MP3	.mp3	Yes	Yes
WAV	.wav	Yes	No

Figure 10.1 Picture, Video, and Audio Support



As can be seen in Figure 10.2, additional options are available in AXIOM Process for some of the MEDIA categories. Examiners should explore available options under each artifact that displays an [OPTIONS](#) hyperlink.

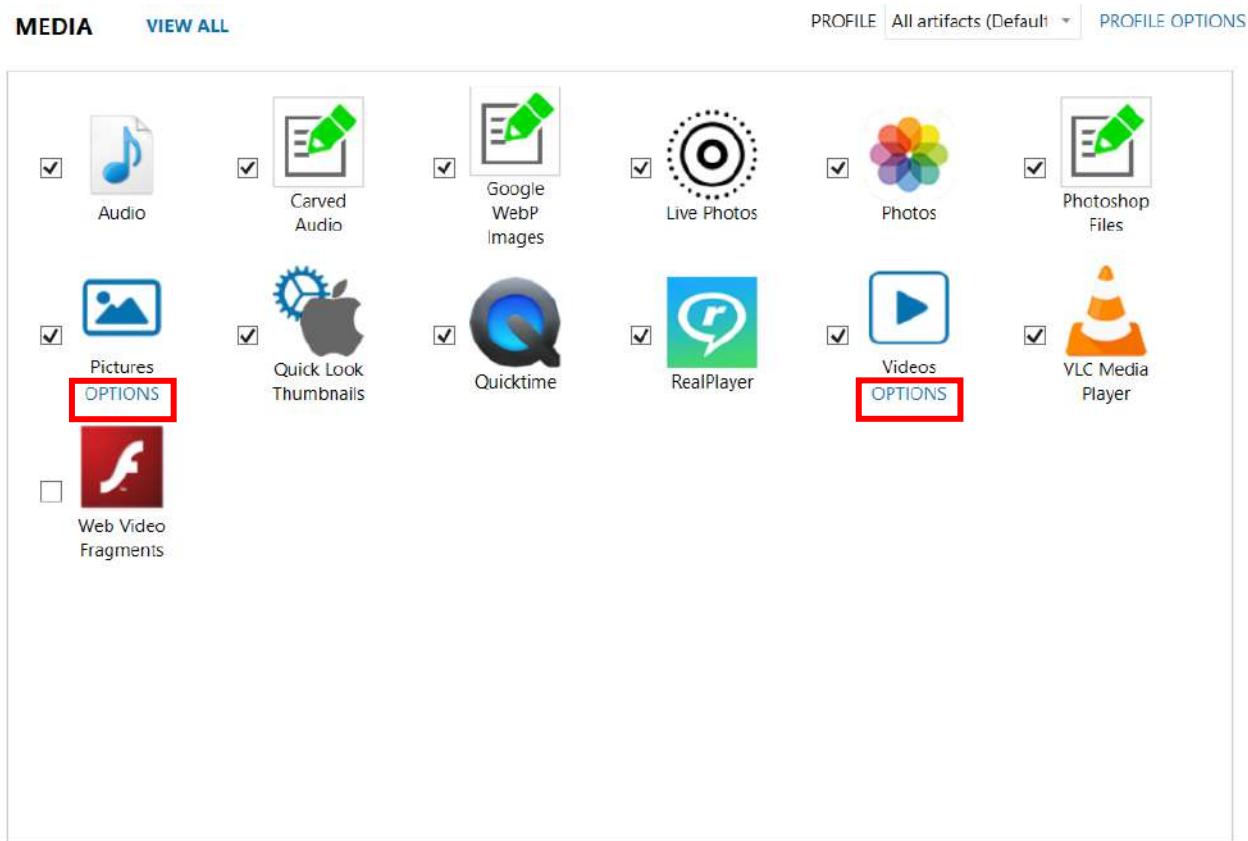


Figure 10.2 MEDIA artifacts and OPTIONS

Like the REFINED RESULTS, the MEDIA category can contain artifacts that are also included in other artifact categories. For example, if a user has been viewing pictures from a Facebook profile and they have been downloaded to the browser's cache, the picture will be contained within the relevant WEB RELATED cache category, and it will also be contained within the MEDIA → Pictures category.

PICTURES

By default, AXIOM Examine displays all artifacts in the Column view (the default view can be changed from the Tools → Settings → DEFAULT VIEW option). However, when reviewing Pictures, the artifacts

can be viewed using the Thumbnail view. To change the view, select Thumbnail view from the View drop-down in the EVIDENCE pane, as shown in Figure 10.3.

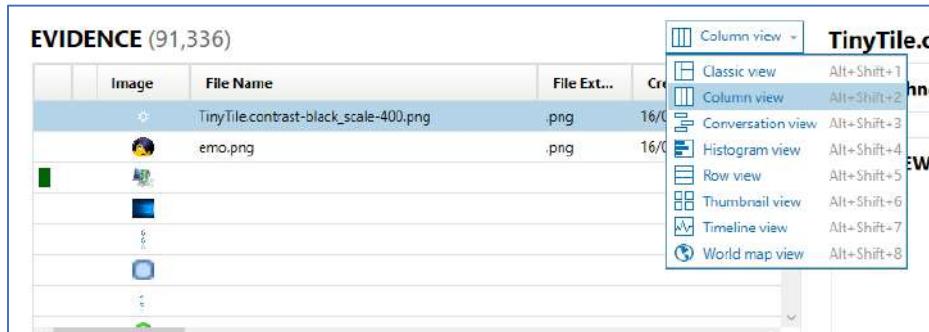


Figure 10.3 View drop-down

Changing to the Thumbnail View automatically applies a filter to display only artifacts that can be viewed as thumbnails. When Thumbnail view is selected, other drop-down filters appear that allow the examiner to set the size of the thumbnails being displayed as Small, Medium, or Large. Two additional drop-down menus appear, allowing the examiner to Filter and Sort by various options.

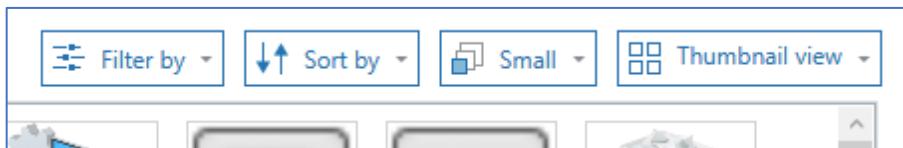


Figure 10.4 Thumbnail view and thumbnail resizing

Figure 10.5 shows the different artifact attributes to be sorted on.

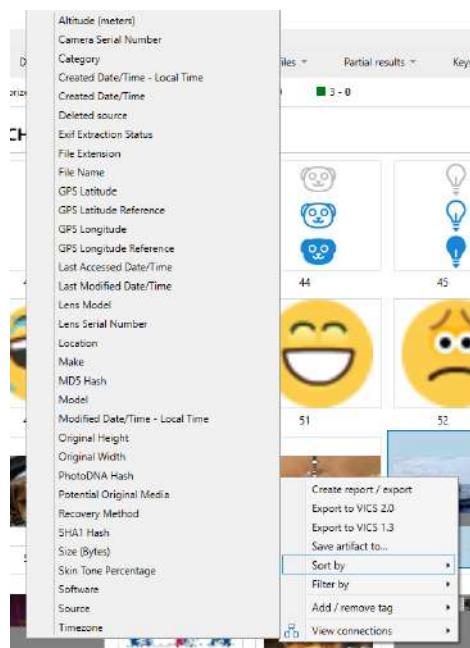


Figure 10.5 Sorting artifacts in Thumbnail view

Additional options are available for the Pictures artifacts during processing in AXIOM Process. One of the options is Extract EXIF data. If selected during processing, the DETAILS pane for each picture artifact will display some of the EXIF data contained within the file if this option is enabled.

EXIF data may contain important information such as GPS coordinates and make/model of the device capturing the photo, as seen in Figure 10.6.

DETAILS	
ARTIFACT INFORMATION	
File Name	2016-09-17 12.32.21.jpg
File Extension	.jpg
Created Date/Time	07/10/2016 16:31:26
Last Accessed Date/Time	07/10/2016 16:31:28
Last Modified Date/Time	17/09/2016 16:32:21
Size (Bytes)	2161666
Original Width	3264
Original Height	2448
Date/Time - Local Time	2016-09-17 12:32:21
Original Date/Time - Local Time	2016-09-17 12:32:21
Skin Tone Percentage	8.4
Make	Apple
Model	iPhone 5s
Software	9.3.3
GPS Longitude	82°17'41.3900"
GPS Longitude Reference	West
GPS Latitude	38°24'33.9100"
GPS Latitude Reference	North
MD5 Hash	e91528e665e8044d10dfc2dbf30ae18e
SHA1 Hash	a00c498796501dd9e86e9b05426dc8a77e26db38

Figure 10.6 EXIF data in DETAILS card

Other processing options for picture artifacts include whether to save the parsed and carved pictures to the case file, or whether to always access them from the evidence files. Accessing the pictures from the evidence file keeps the case database smaller but means the evidence file must always be available to AXIOM when reviewing picture artifacts. Saving picture artifacts to the case file allows them to be viewed without the original source evidence attached. If picture artifacts are saved to the case file, there is an additional option to resize the saved picture.

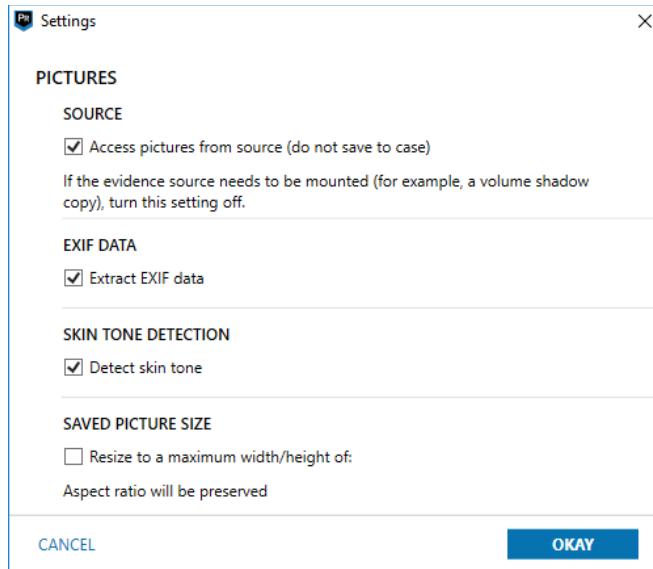


Figure 10.7 PICTURES options in AXIOM Process

VIDEOS

If, at the time of processing, “Create a preview using still frames” was selected in the VIDEO options, as shown in Figure 10.8. The DETAILS pane for each VIDEO artifact will include a PREVIEW card that is a filmstrip of the video content. This option is enabled by default in the [OPITONS](#) for Video artifacts in AXIOM Process.

If, at the time of processing, Save videos up to was selected in the VIDEOS options, the DETAILS pane for each VIDEO artifact will also include a playable PREVIEW card. To play a video file within the PREVIEW card, simply click the play button. The playable PREVIEW card also includes a mute button.



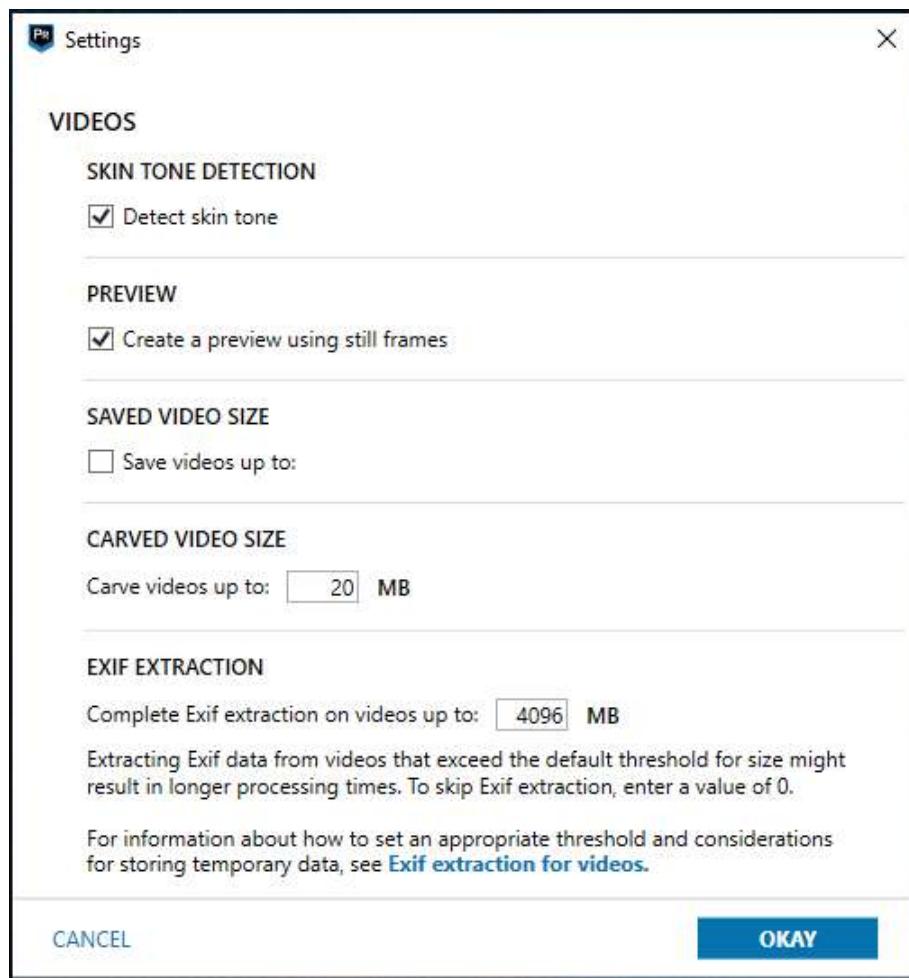


Figure 10.9 VIDEO options in AXIOM Process

78

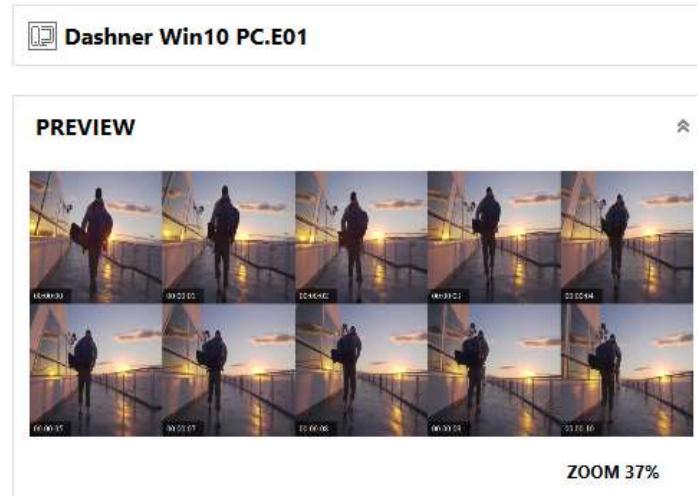


Figure 10.10 Filmstrip preview of a video artifact

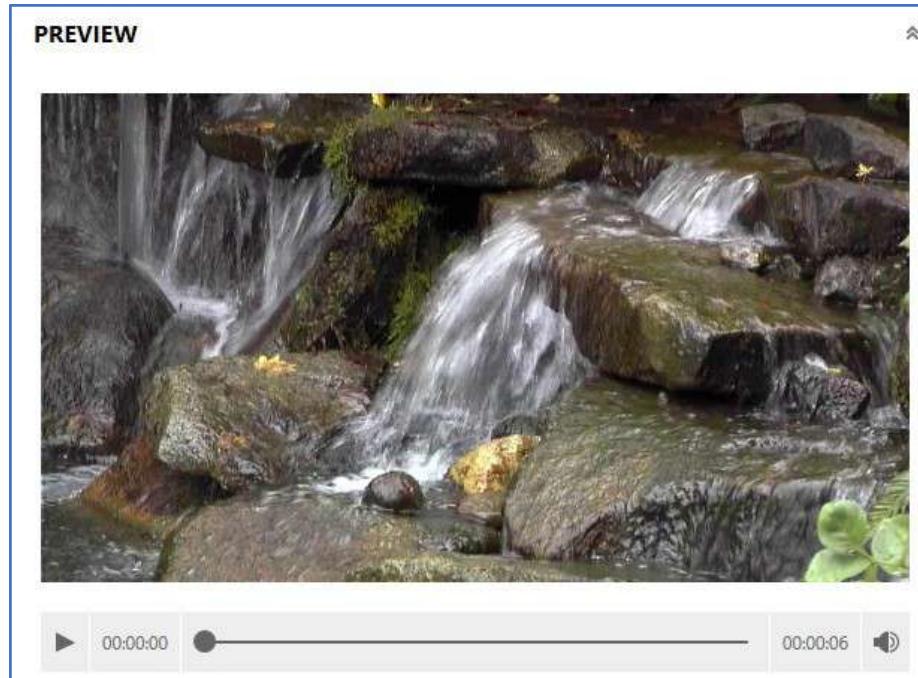


Figure 10.11 Playable PREVIEW

CATEGORIZING PICTURES USING MAGNET.AI

The Magnet artificial intelligence module, Magnet.AI, can be used to help identify picture content of a specified type within the case. During categorization, Magnet.AI identifies and tags picture content that matches the selected criteria, thereby reducing the need to manually sort through numerous pictures.

The CATEGORIZE PICTURES option can be selected during processing. If selected, it will categorize all pictures in the case. Alternatively, the CATEGORIZE PICTURES process can be started from within AXIOM Examine once all processing has completed. It can be started from the Case dashboard by selecting **CATEGORIZE PICTURE** within PLACES TO START → MAGNET.AI CATEGORIZATION, or it can be started by selecting the menu option PROCESS → CATEGORIZE PICTURES WITH MAGNET.AI.

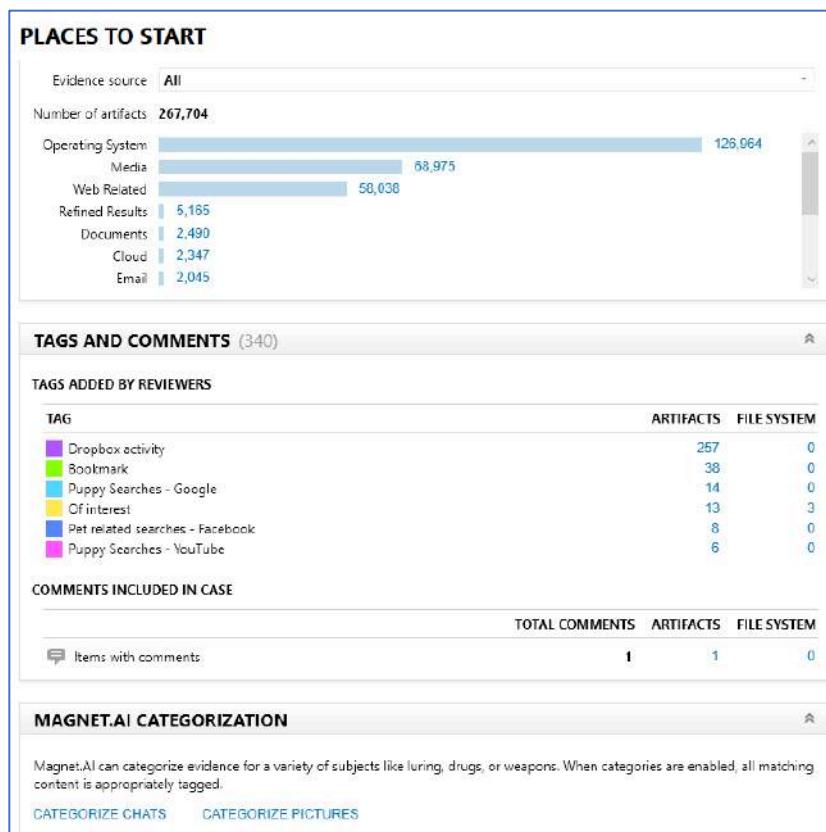


Figure 10.12 Magnet.AI Categorize Pictures

Selecting to run picture categorization from the Case dashboard will automatically attempt to categorize all the pictures in the case. If a more granular approach is required, the pictures must first be filtered within the Artifacts explorer.

From the Artifacts explorer, first apply any necessary filters to restrict which pictures should be categorized, then select the menu option Process → Categorize pictures with Magnet.AI. The Categorize pictures with Magnet.AI dialog then provides the option to categorize just the pictures in the current view, or all pictures.

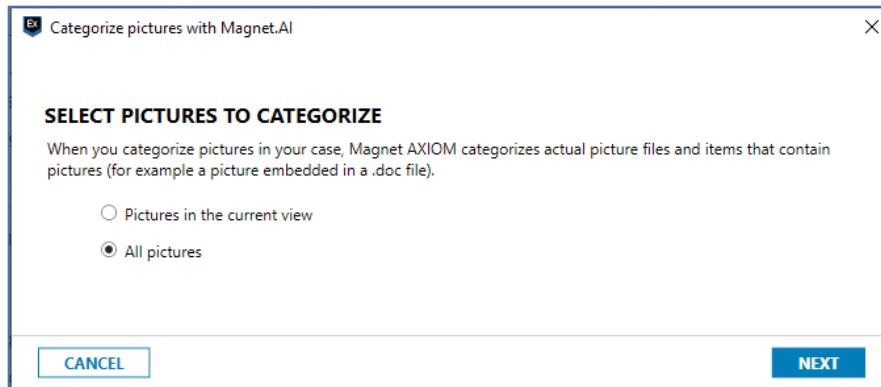


Figure 10.13 Categorize pictures dialog

Clicking **NEXT** then opens MAGNET.AI PICTURE CATEGORIZATION table listing the categories of content MAGNET.AI can search for.

Enabled	Category	Tag
<input checked="" type="checkbox"/>	Hate symbols	
<input type="checkbox"/>	Human faces	
<input type="checkbox"/>	License plates	
<input type="checkbox"/>	Militants	
<input type="checkbox"/>	Money	

Figure 10.14 PICTURE CATEGORIZATION categories

As of the time of writing, the current categories of pictures that Magnet.AI can categorize include: Bedrooms, Buildings (exterior), Child abuse, Documents (cards/ID), Documents (paper), Drones/UAVs, Drugs, Hate symbols, Human faces, License plates, Militants, Money, Nudity, Screen captures, Vehicles (cars/trucks/vans/buses), and Weapons. Categories may be updated and added over time.

Once a category is enabled, the Tag name can be changed by clicking into the text, changing the tag name, then selecting **UPDATE**.

Once the Categories are selected and Tag names changed as desired, click **CATEGORIZE PICTURES** to start the process.

After processing, the Case dashboard updates with the Magnet.AI results:

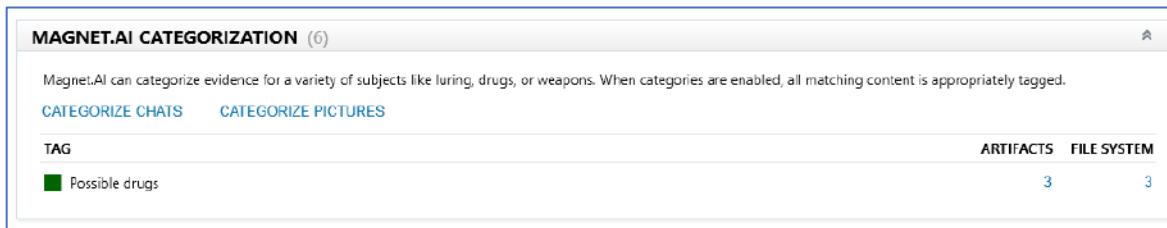


Figure 10.15 TAGS added by MAGNET.AI picture categorization

MAGNET.AI – CONTENT-BASED IMAGE RETRIEVAL (CBIR)

Starting with Magnet AXIOM version 4.0, examiners can use Content-Based Image Retrieval (CBIR) as part of the Magnet.AI offering. Using Magnet.AI, an examiner can either import a picture, or select a current picture in their case as a reference, to find similar pictures across the evidence set.

The idea behind CBIR is the application of computer vision techniques to search digital images within databases for relevant or matching content within the data. The term “content” may refer to colors, shapes, textures, or other information that can be derived from the original source image. The benefit of using the CBIR engine within Magnet AXIOM is that the content search can be performed entirely offline allowing for the searching of suspect or contraband material on the host system.

Examiners must build the comparison database prior to using CBIR functionality. To begin the picture comparison, examiners should select the Tools menu at the top, then Build picture comparison. Examiners can also trigger this to autorun within the settings by checking the box for Automatically build picture comparison on case open. The process could take many hours depending on how many media items are within the case as well as the processing power of the computer.

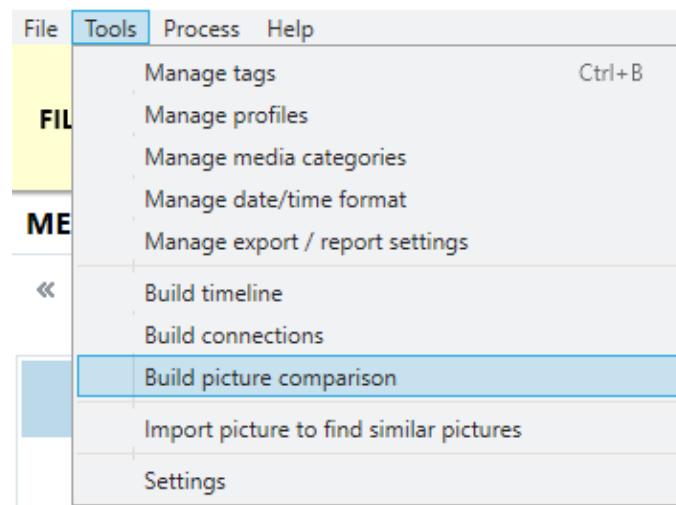


Figure 10.16 Building picture comparison

Once the picture comparison database has been established, examiners have two ways of triggering the search: either use an image already in their case data or import an image from outside their case. Importing an image from outside the case does not add the image as evidence; however, an examiner may want to add the image to the case by adding a file in AXIOM Process.

To search the current case data for similar images, examiners simply need to right-click on their specific image and select Find similar pictures → Select picture. Examine will use the selected image as the source image to scan against.

After the search is performed, AXIOM will then display the 100 (by default) most relevant images to the selected source image.

This number is configurable from the dropdown menu. These images are represented in Thumbnail view with the most relevant being displayed first and the images deemed least relevant being displayed last.

The screenshot shows the AXIOM software's main interface. On the left, there is a sidebar with navigation icons and a tree view of 'REFINED RESULTS' (1 item), 'WEB RELATED' (1,417 items), 'CHAT' (10 items), 'MEDIA' (8,308 items), 'EMAIL' (19 items), and 'CLOUD' (245 items). The central area is titled 'MATCHING RESULTS (10,000 of 267,762)' and shows a grid of 35 thumbnail images. The first thumbnail is highlighted with a blue border. The thumbnails are numbered 0 through 35. At the top right, there are buttons for 'Sort by', 'Small', and 'Thumbnail view'. The bottom right corner shows a small watermark for Magnet Forensics.

Figure 10.17 Find similar pictures

Examiners can also take an image from their computer and run the CBIR functionality against it. To do this, examiners can select the Import picture to find similar pictures option from the Tools menu or from a right-click menu of an image. The filter bar's Similar pictures dropdown can also be selected so that examiners can select the **IMPORT PICTURE** option. Once the IMPORT PICTURE option is selected a selection box will open so examiners can point to the selected image file.

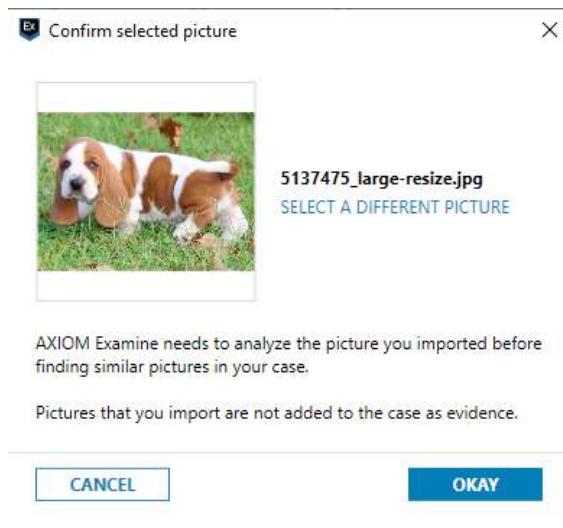


Figure 10.18 Importing a similar image

RUNNING EXERCISE: CBIR

- From the **Artifacts** explorer in AXIOM Examine, clear any filters you may have applied.
- Select the Tags and comments drop-down menu on the **FILTERS** bar and choose the tag listed for Hash match.
- Select the MEDIA → Pictures artifact category and sort on the File Name column.
- Select the first image, "00404_3TMiaAMuyS3_1200x900.jpg" and then right-click on the data for this artifact in the **EVIDENCE** pane.
- Select Find similar pictures → Build Picture Comparison. Note: To save time, this step may have already been performed.
- Once Build picture comparison completes, right-click on the image again and choose Select picture.
- You will be taken to the EVIDENCE pane with Thumbnail view selected and the heading MATCHING RESULTS will be visible at the top.

- Take note of the returned image set that many of the copies of the image are appearing first with other images of the same/similar dogs in a similar environment appearing next.
- Using the Similar pictures dropdown in the FILTERS bar, select **IMPORT PICTURE**.
- Navigate to the path **AX200\Evidence\CBIR** and select the file **Toby.jpg**.
- Review the returned results. Clear all filters when finished.

MANUAL CATEGORIZATION OF IMAGES USING MAGNET AXIOM

Magnet.AI categorizes pictures within the case based on the graphical content, but AXIOM can also categorize pictures and videos based on their hash values. Hash sets can be added to AXIOM Process to automatically categorize media files during the processing stage in accordance with a pre-defined list of categories. Pictures and videos can also be categorized manually within AXIOM Examine as part of the evidence review. Pre-categorizing media files based on their calculated hash value reduces the number of artifacts that must be reviewed and categorized manually. The media categories can be setup and customized within the Tools → Manage media categories menu option.

STEP 1: SELECT A MEDIA CATEGORIZATION LIST

Select a list to determine which categories are available for media categorization. You can select a list from the table below, add a new list, or import a list.

[ADD NEW LIST](#) [IMPORT LIST](#) [EXPORT LIST](#)

Active	Name
<input type="radio"/>	Canada (Project VIC)
<input checked="" type="radio"/>	International (Project VIC)
<input type="radio"/>	United Kingdom (CAID)
<input type="radio"/>	United States (Project VIC)

STEP 2: CUSTOMIZE THE MEDIA CATEGORIZATION LIST

List name

Customize this list to represent the category names and colors applicable to your organization or region. You can turn off any categories that your organization does not use.

Enabled	Category	Name	Keyboard shortcut	Illegal
<input checked="" type="checkbox"/>	■ 0	Non-Pertinent	0	<input type="checkbox"/>
<input checked="" type="checkbox"/>	■ 1	Child Pornography	1	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	■ 2	Images of Investigative Interest	2	<input type="checkbox"/>
<input checked="" type="checkbox"/>	■ 3	Other Material	3	<input type="checkbox"/>

Select the default category to use to assign all visible uncategorized pictures to:

Figure 10.19 Manage media categorization



The default installed lists relate to Canada (Project Vic), United States (Project Vic), the United Kingdom (Child Abuse Image Database, CAID), and a generic International Categorization list. Selecting one of the pre-defined lists, displays the categories defined in that list.

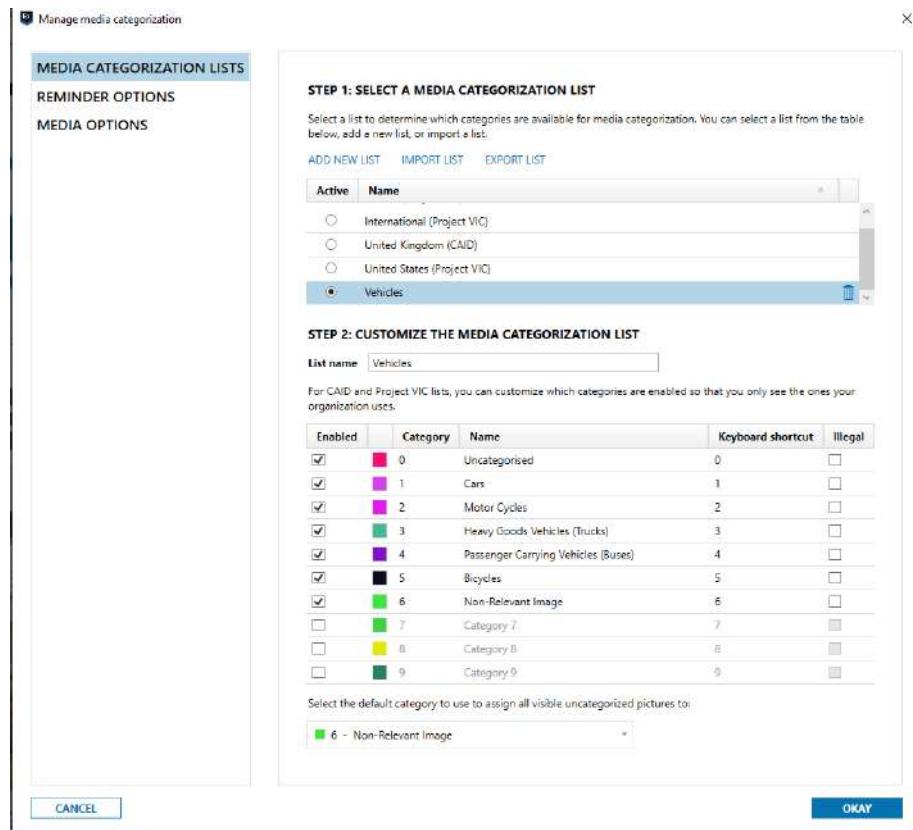


Figure 10.20 Categorizing new lists

The examiner can create their own custom list of categories by selecting ADD NEW LIST. An examiner may choose to create their own list to “grade” privileged or intellectual property in a corporate environment or other scenario outside of simply grading child abuse cases. For example, AXIOM could be used to identify pictures and videos of different types of vehicles, flag documents as safe or unsafe to share, etc. The above shows a custom list, the user renamed a category to “Vehicles” and configured it with different brands of vehicles.

Active	Name
<input checked="" type="radio"/>	My custom list
<input type="radio"/>	Canada (Project VIC)
<input type="radio"/>	International (Project VIC)
<input type="radio"/>	United Kingdom (CAID)

Figure 10.21 Selecting categorization lists

Once created and configured, this Custom list can be exported for use by other AXIOM users. Selecting the EXPORT LIST option creates a .xml formatted file. Similarly, categorization lists that have been created on another instance of AXIOM can be imported using the IMPORT LIST option.

When configuring the media categorization lists, the examiner should always define a category for Non-Relevant Images, which can be used to bulk identify any irrelevant/unrelated files. As it is likely to be the most used category, it can be assigned the status of “default category”. Once a default category has been set, pressing the “+” key will automatically assign the default category to all pictures in view. Pressing the “-“ key while on selected images will remove that category.

This feature is used in the context of CSAM / IIOC images and could be allocated to whichever category is of no interest to the examiner, i.e., for USA Project Vic – Category 0 and for UK CAID – Category 8.

There is also an option to check which Categories can be marked as “Illegal”. Numeric keyboard shortcuts are assigned to the categories, and during manual categorization/grading the examiner can select the file(s) and use the numeric keyboard shortcut to quickly assign a category.

OFFICER WELLNESS FUNCTIONALITY

Exposure to child abuse and other disturbing imagery can take a toll on examiners and image graders. Though exposure may be reduced using hash sets, such as Project Vic and CAID, it will always be necessary for examiners to view potentially harrowing and disturbing images. To further minimize exposure to this material, there are Officer Wellness features in AXIOM, which can be configured from the Tools → Manage media categories setting.



Categorizing/grading illicit pictures and videos for a long period of time can induce stress for examiners. The REMINDER OPTIONS within Manage media categorization allows the examiner to set a timed reminder to trigger after a specified time, for example, two hours as shown in Figure 10.22. Once the timer has expired, AXIOM Examine will suggest the examiner takes a break from media categorization.

The second REMINDER OPTION can be set to warn the examiner to stop categorization activities at a specified time at the end of the working day. This helps ensure the last thing on their mind is not disturbing imagery.

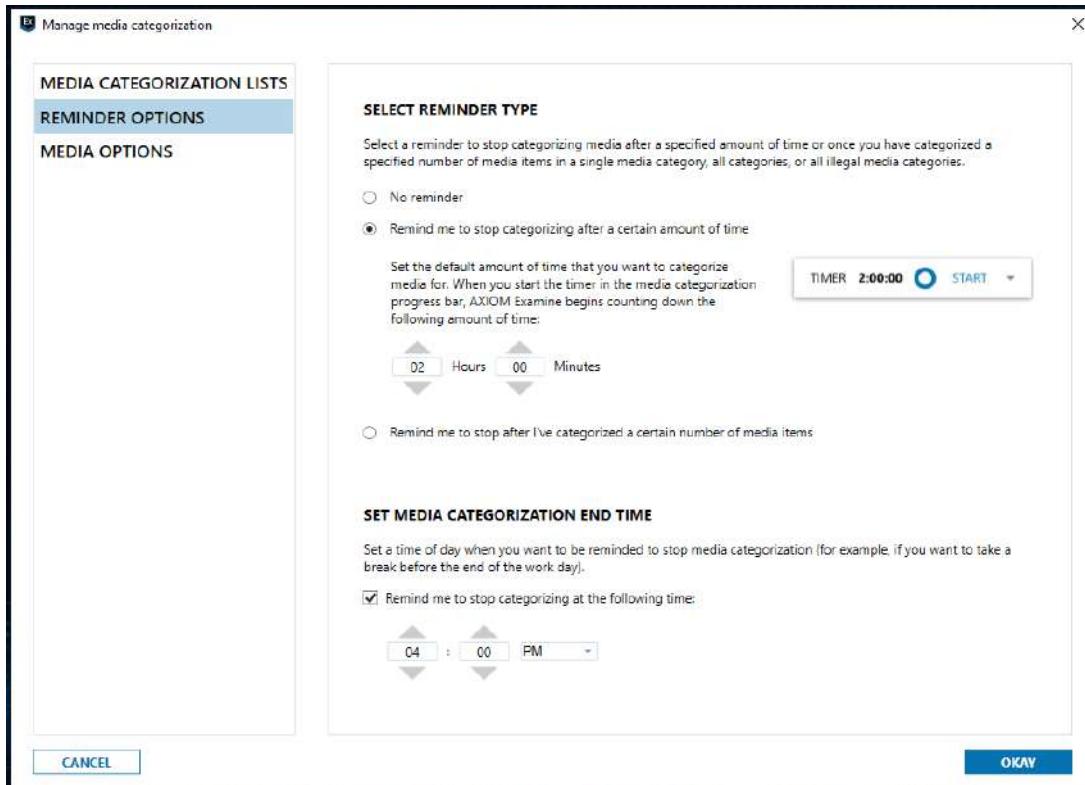


Figure 10.22 Officer wellness reminders

The MEDIA OPTIONS within Manage media categorization provides the ability to automatically blur, or completely block from view, any media files categorized as one of the categories marked as “Illegal”, as shown below:

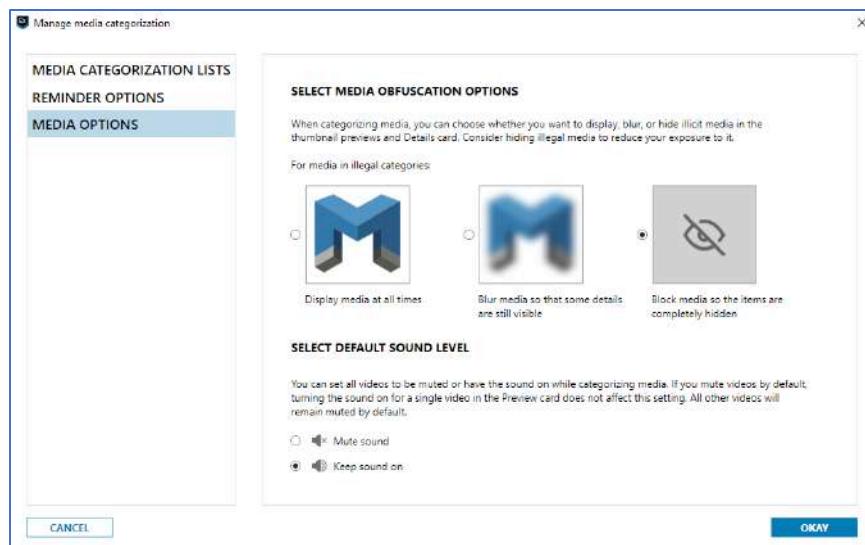


Figure 10.23 Media blurring

The MEDIA OPTIONS will also provide the ability to mute the sound of any video during playback, again to minimize exposure to distressing media both for the examiner and anyone else working nearby.

If a picture or video is categorized, any files with the same hash value will automatically have the same category applied. Therefore, if a media file is categorized as one of the illegal categories, all matching files will also automatically be blurred or blocked from view. In Figure 10.24 the highlighted puppy picture was categorized as an illegal picture. AXIOM blurred the thumbnail picture and automatically blurred the two other pictures with the same hash value.

Blurring or blocking the picture from view is only a display mask, the content of the picture is not changed or removed from the case. If the categorization/grading needs to be checked later, either the MEDIA OPTIONS can be changed to display the pictures again, or simply clicking the PREVIEW card in the DETAILS pane will display the original content.

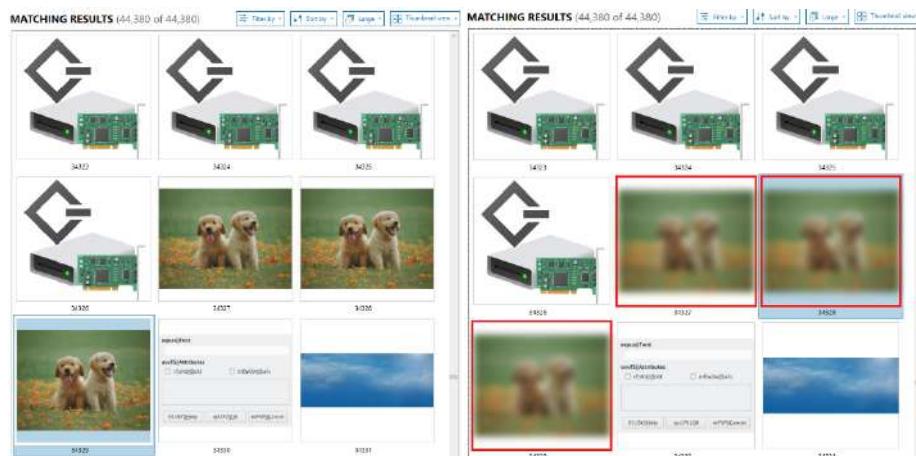


Figure 10.24 Blurring with the Officer Wellness feature



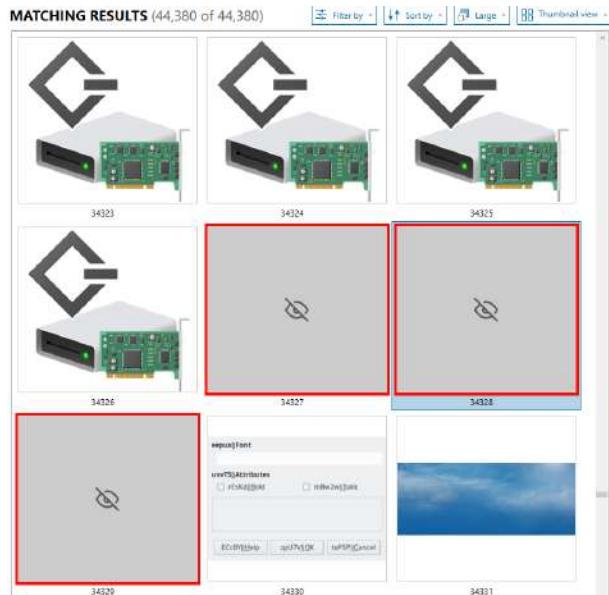


Figure 10.25 Blocking images with the Officer Wellness feature

To facilitate the grading/categorization of media files by other officers/staff, it is recommended that Portable Cases be created. These portable cases can be handed to other graders, and once they have completed their grading, the results from the Portable Cases can be imported back into the master case file. For more information on the creation of Portable Cases please refer to Module 13.

EXPORTING THE CATEGORIZED DATA

Once all the categorization is complete and any portable cases have been merged back into the original case, the pictures, along with their metadata, can be exported as a JSON file to allow their ingestion into other tools and databases where required.

To create the JSON export, select the pictures to export and right-click. Select the relevant version of VICS. The version selected dictates the format of the output file and is dependent on the target system, i.e., Project VIC or CAID.

Figure 10.27 displays the report information window, where the examiner can select which categories of files to include in the export. The CONTACT INFORMATION fields in bold must be completed before the CREATE button activates.

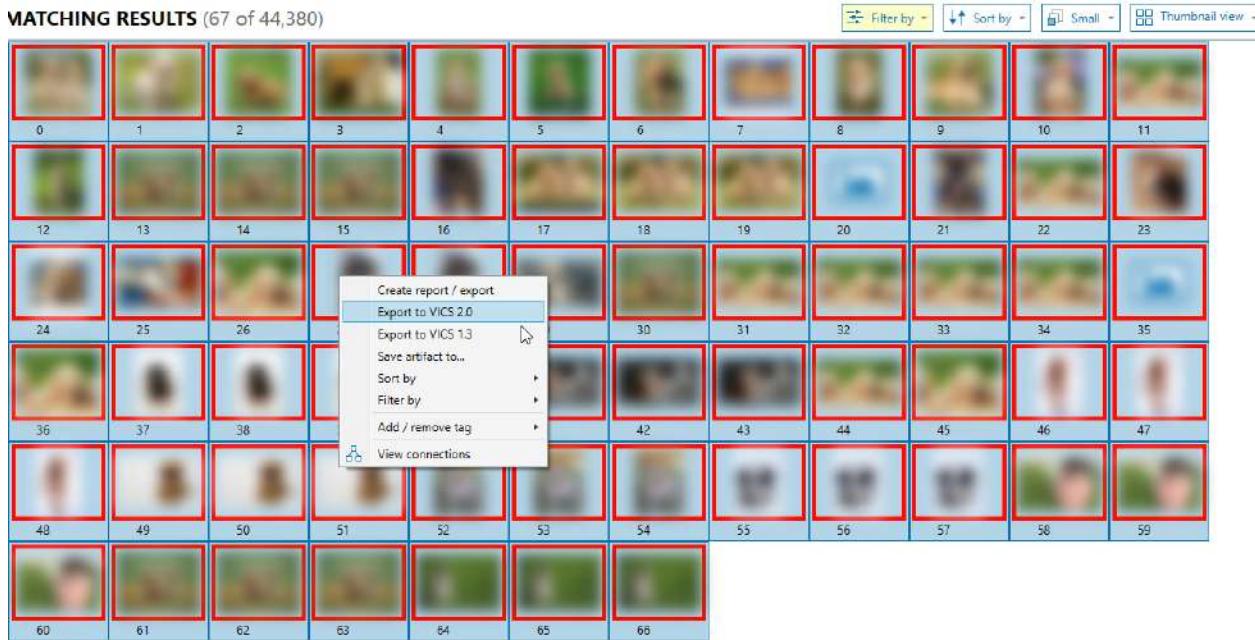


Figure 10.26 Exporting the JSON

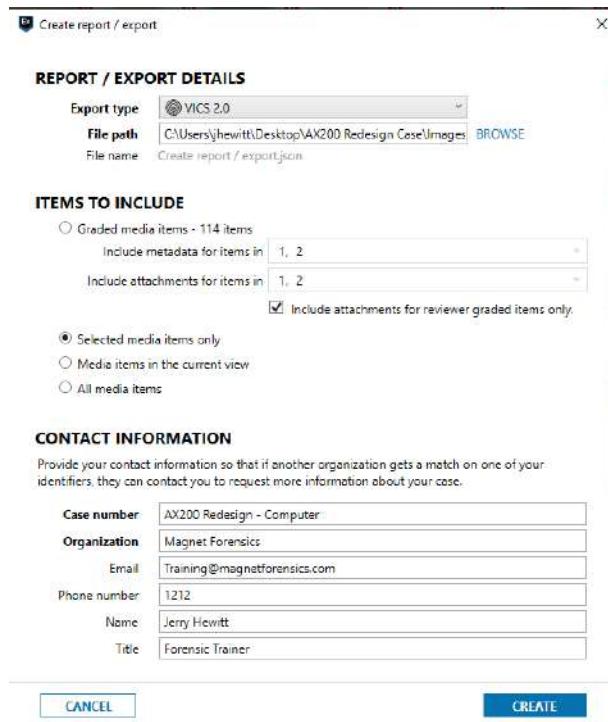


Figure 10.27 JSON options for export



MEDIA EXPLORER

New for AXIOM version 5.0, the Media explorer was designed to provide examiners with a media-focused view of the evidence within a case, instead of strictly relying on the Artifact explorer. The Media explorer offers several different features over the traditional Artifact explorer. In order to use the Media explorer, examiners must select the Media explorer from the explorer drop-down as seen in Figure 10.28 below:

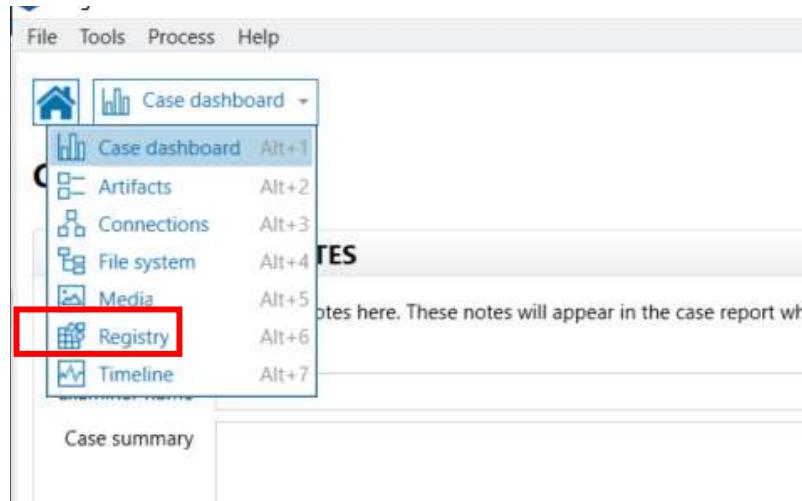


Figure 10.28 Newly added Media Explorer

When the examiner selects the Media explorer in the explorer drop down, they will be presented with a prompt to build the explorer, unless already enabled under Tools → Settings → Automatically build the media explorer on case open (Figure 10.29)

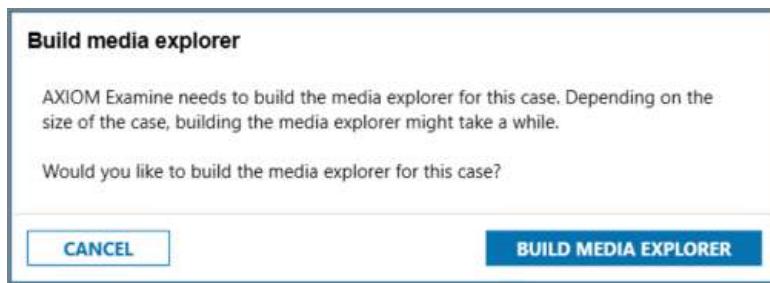


Figure 10.29 Build media explorer

MEDIA FILTERS AND GROUPS

The Media explorer introduces a brand-new filter panel designed to allow the examiner to create complex filters with a few clicks. With the AXIOM 5.5 update, global searches can now be performed within the Media Explorer.

Examiners are also able to group media together by accessed date, creation date, evidence source, file extension, and modified dates. There are sorting features such as size in bytes, skin tone percentage, and more, which are like the thumbnail sorting options in the Artifact explorer.

By default, images are “stacked” by hash value but can also be displayed individually. Image stacking is referred to as “hit stacking” and is discussed later.

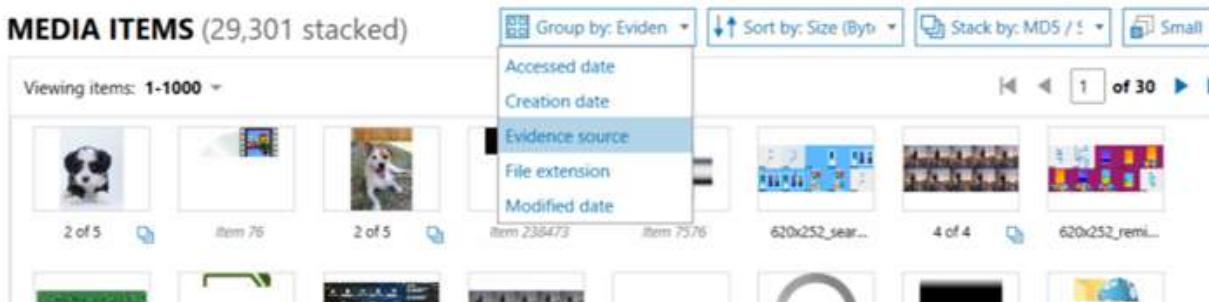


Figure 10.30 Media filters and groups

MEDIA FILTER GROUPS

The left-hand side of the Evidence pane displays the new media filter groups.

FILTERS Artifacts Date and time Tags and comments Keyword lists Similar pictures Type a search term... GO

MEDIA CATEGORIZATION PROGRESS

INVESTIGATION LEADS

- Items with an Exif created date
- Items with geolocation data

CAMERA DETAILS

- Camera make
- Camera model
- Camera serial numbers
- Lens model
- Lens serial numbers

DISTRIBUTION INDICATORS

- File names matching social media patterns

MEDIA ATTRIBUTES

- Size (bytes)
- Skin tone percentage

VIDEO ATTRIBUTES

- Carved video file size
- Container format
- Content format
- Media duration

FILE ATTRIBUTES

- Accessible items
- Deleted source
- Exif extraction status
- File extension
- MIME type
- Recovery method

MEDIA ITEMS (30,577 stacked)

Viewing items: 1-1000

Win 10PC (58,245 individual items)

Group by: Evidence source Sort by: Size (Bytes) Stack by: MD5 / SHA1 Small

Blur media Sound on SET UP REMINDER

Tags, Profiles & Media Categories

INVESTIGATION LEADS

CAMERA DETAILS

DISTRIBUTION INDICATORS

MEDIA ATTRIBUTES

VIDEO ATTRIBUTES

FILE ATTRIBUTES

CLEAR FILTERS APPLY FILTER

Figure 10.31 Media filter groups

INVESTIGATION LEADS – These filters are designed to quickly identify items that could provide additional case leads including surfacing details of original creation dates, geolocation data, and media that may have come from social media sites.

CAMERA DETAILS – The camera details filter uses available EXIF metadata to identify the type of device the media was originally created with.

VICS ATTRIBUTES – If the evidence was processed with a known Project VIC hash set and matching results were found in the evidence, examiners can use these filters to narrow results for known media.

MEDIA ATTRIBUTES – Allows the examiner to filter by size (bytes) and known skin tone percentage.

VIDEO ATTRIBUTES – These filters allow the examiner to filter videos by length, format, and carving size.

FILE ATTRIBUTES – This filter can be used to look for content from deleted sources, EXIF extraction status, file extensions, and the recovery method.

HIT STACKING

Hit stacking is the process of combining media that has the same MD5/SHA1 hash into a single “stacked” item, regardless of how many copies of that file exist across the evidence items. This is useful to ensure the same file is graded consistently, while also preventing examiners from being repeatedly exposed to the same content throughout their review.

When a stack is graded or tagged within the media categories, the value is applied to all copies of the file across the evidence. In the example below, the stack is represented by the icon in the lower right corner of the thumbnail.

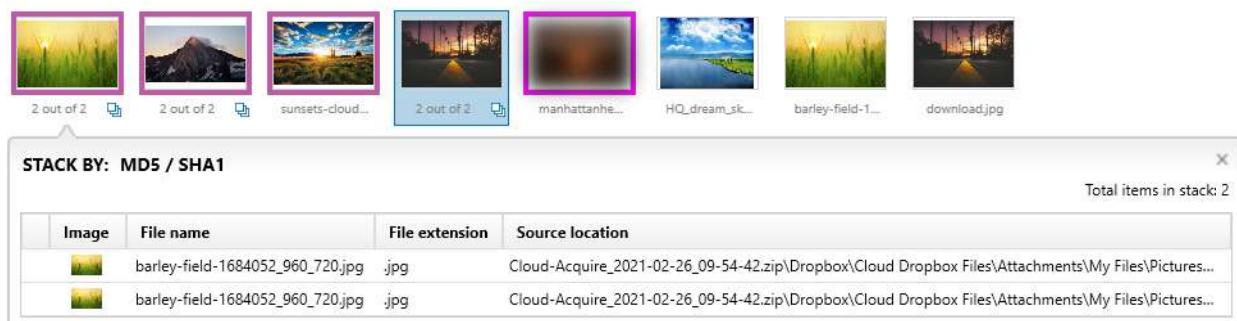


Figure 10.32 Hit Stacking and source information

Selecting the small, stacked icon in the bottom right of an image will bring up a list of all the images along with their file extension and source location, as seen above.

RELATED ARTIFACTS

Clicking on the image in a stack will bring up the details in the details pane, including a hyperlink which allows examiners to see the related artifacts to that image.

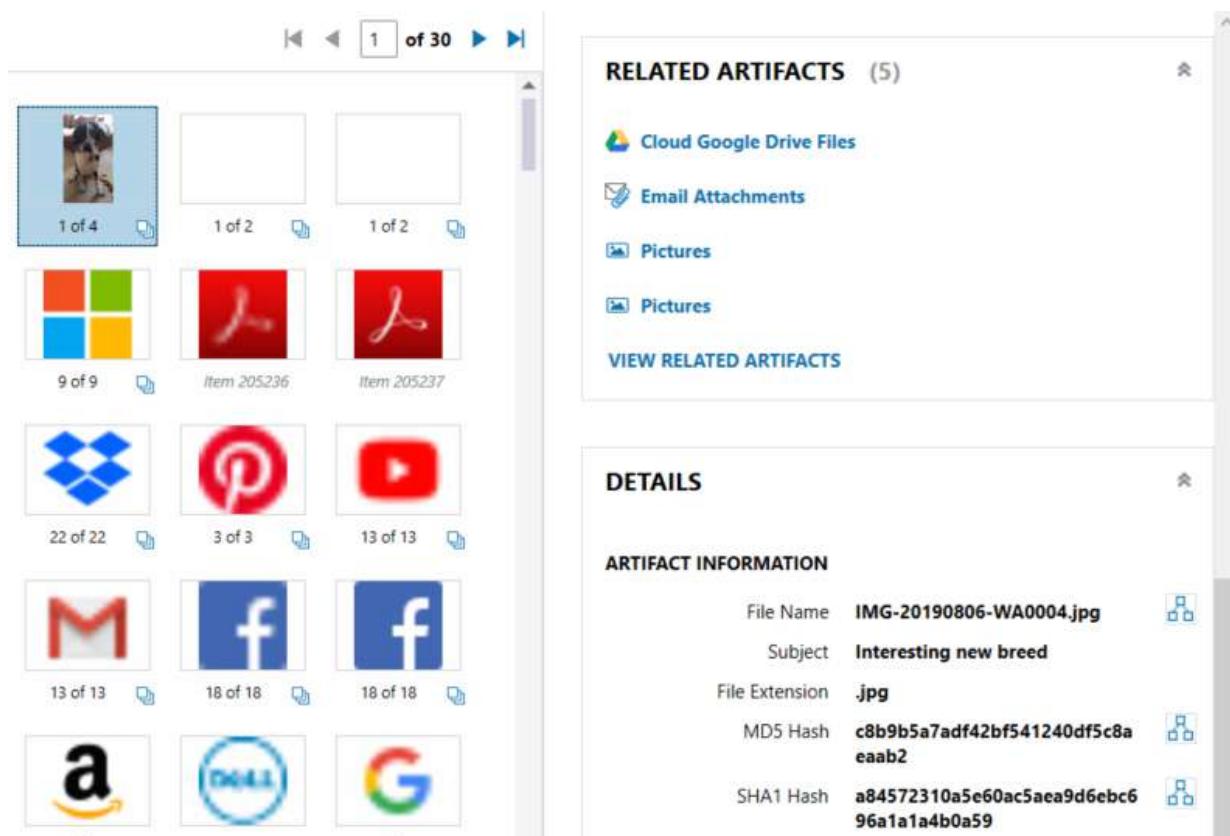


Figure 10.33 Details pane and related artifacts

The figure above shows the RELATED ARTIFACTS card in the Details pane. The option to view related artifacts is also presented when a user right-clicks on an image in the Evidence pane.

QUICK MEDIA PREVIEW

Hovering over an image or video will show a pop-up preview of the media unless the media is blurred/blocked. For an image, the examiner can pan and zoom on the image using the standard mouse functions. For a video, the examiner can “scrub” the video for a quick preview by moving the mouse left to right across the preview. This feature allows the examiner to quickly preview the entire contents of the video, even if the video is lengthy.

RUNNING EXERCISE

MEDIA EXPLORER

- Navigate to the **Media** explorer in AXIOM Examine.
- If not already built, click the dialog to build the Media explorer.
- Apply the filter to Group by: Creation date and under INVESTIGATION LEADS, apply a filter for Items with an Exif created date. Hit APPLY FILTER
- Click on the stacked icon for any image with multiple stacks, review the source data.
- CLEAR FILTERS in the left-hand navigation pane
- Search for video “VID_20190818_102332.MP4”
- Hover the mouse over the video until the preview shows, move the mouse to observe the quick video preview.

CONNECTIONS

Connection information is collected from all evidence items in the case regardless of the source. Links are built between the artifacts telling the examiner how they were connected, and the artifacts are displayed in a network diagram within the Connections explorer.

The Connections explorer displays these connections visually, making it faster and easier to identify and understand how various pieces of the investigative puzzle fit together. With the ever-growing mountain of evidence examiners must deal with on a day-to-day basis, CONNECTIONS provide a way of connecting the dots and identifying key related information in a more expedient manner. The Connections explorer will help examiners establish the who, what, when, where, why, and how of the investigation. It is expected that the examiner will return to the Connections explorer many times throughout the life of the case.

WHO Who was involved? Understanding who owns a suspect file; who put it in that location; who, if anyone, has looked at or executed the file (depending on the filetype); who deleted it; who emailed/ transferred it; who did they email/transfer it to; and who was using the machine at the time the offence occurred, who else has been using the machine are all questions that could help answer the key question – Who was involved?

WHAT What happened? Understanding what other files this is related to; what applications have been used; what additional information does the metadata provide (Word docs - when was it



last printed, Pictures – What camera was used); what other files were stored in the same folder/on the same device; what was the sequence of events, are all questions that could help answer the key question – What happened?

- WHEN When did it occur? Understanding when a picture was taken (EXIF data); when was this file viewed, emailed/shared/transferred, when was this file deleted, when was this file executed or last accessed are all questions that could help answer the key question – When did it occur?
- WHERE Where did it take place? Understanding where else a file is located, was it saved locally, to other devices, to the cloud; where was it downloaded from; where was it distributed to; are there logs to show where a device been used, are all questions that could help answer the key question – Where did it take place?
- WHY Why did it happen? The content of correspondence in the form of chat, email, instant messaging communications etc.; or the content of machine activity logs could help answer the key question – Why did it happen?
- HOW How did it happen? How did this file get onto this device; how was the file shared with other people; how did this person communicate with other key people; the content of correspondence in the form of chat, email, instant messaging communications etc. could all help answer the key question – How did it happen?

Connections are built by manually selecting Tools → Build Connections but can be set to automatically rebuild every time new evidence is added to the case by enabling the Automatically build connections on case open option in Tools → Settings → Connections.

Once the connections have been built, AXIOM Examine displays a CONNECTIONS icon beside any artifact attribute that has been connected in some way, as shown in Figure 10.35. The CONNECTIONS icon automatically switches AXIOM Examine to the Connections explorer with the selected artifact attribute as the PRIMARY NODE.

ARTIFACT INFORMATION	
File Name	s-l1600.jpg
File Extension	.jpg
Created Date/Time	12 Sep 2019 21:28:56
Last Accessed Date/Time	18 Dec 2019 05:00:00
Last Modified Date/Time	30 Aug 2019 15:55:24
Size (Bytes)	109014
Skin Tone Percentage	57.7
Original Width	1000
Original Height	1000
Exif Extraction Status	Complete
MD5 Hash	39ca952b844546ac73aaefe16eba42a4
SHA1 Hash	25550643003b8b3d8bf5d7cad495e7cf8b44f424

EVIDENCE INFORMATION	
Source	SanDisk SanDisk Cruzer USB Device 7.48 GB Full Image.E01 - Partition 1 (Microsoft FAT32, 7.48 GB) MYUSB\Pics\s-l1600.jpg

Figure 10.34 CONNECTIONS icons

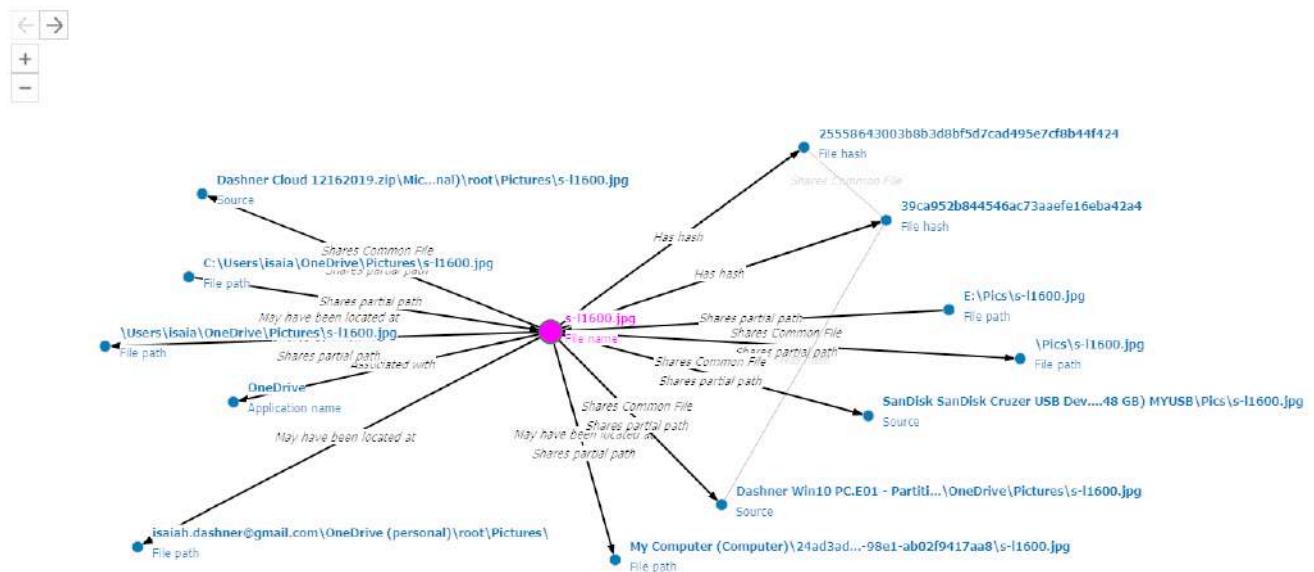


Figure 10.35 Primary nodes (pink) and direct nodes (blue)

There are four types of nodes within the Connections explorer:



PRIMARY NODES are displayed in **HOT PINK**. This is the anchor point from which the connections are being made. In the Artifacts or File system explorers, selecting a CONNECTIONS icon for a specific artifact attribute switches AXIOM Examine to the Connections explorer with that artifact attribute set as the primary node. Double-clicking any node withing the Connections explorer sets it as the primary node.

DIRECT NODES are displayed in **BLUE**. These are artifact attributes with a direct connection to the primary node. To view only connections between a primary node and a direct node, click the direct node.

SELECTED NODES are displayed in **TEAL**. When a direct node is selected, it becomes a selected node. The matching results displayed in the Connections explorer refresh to display only artifacts that contain both attributes of the primary and selected node, e.g., filename and application name. When a direct node becomes a selected node, indirect connections come into focus.

INDIRECT NODES are displayed in **GREY**. When a direct node becomes a selected node all other direct connections to the primary node become indirect nodes and turn grey. All direct connections to the selected node are also now displayed as indirect nodes.

CONNECTORS are the lines representing connections between two nodes. Types of connections include: shares partial path, accessed with, transferred to, source, etc.

The MATCHING RESULTS pane displays the artifacts relating to the primary node. If a direct node is selected, the MATCHING RESULTS updates to display just the artifacts in common between the primary node and the selected node. Selecting one of the MATCHING RESULTS displays the artifact information in the DETAILS pane and the artifact can be tagged or a comment added in the usual way.

To navigate the connections map, individual nodes can be selected to view where connections exist. In the example shown in Figure 10.36 the file name **s-l1600.jpg** is the primary node and has several linked attributes identified by the direct nodes. A copy of the same file is stored in multiple locations and shares a partial path with the **E:** drive. Selecting the File path attribute **E:\Pics\s-l1600.jpg** makes that direct node a selected node and the indirect connections are now displayed.

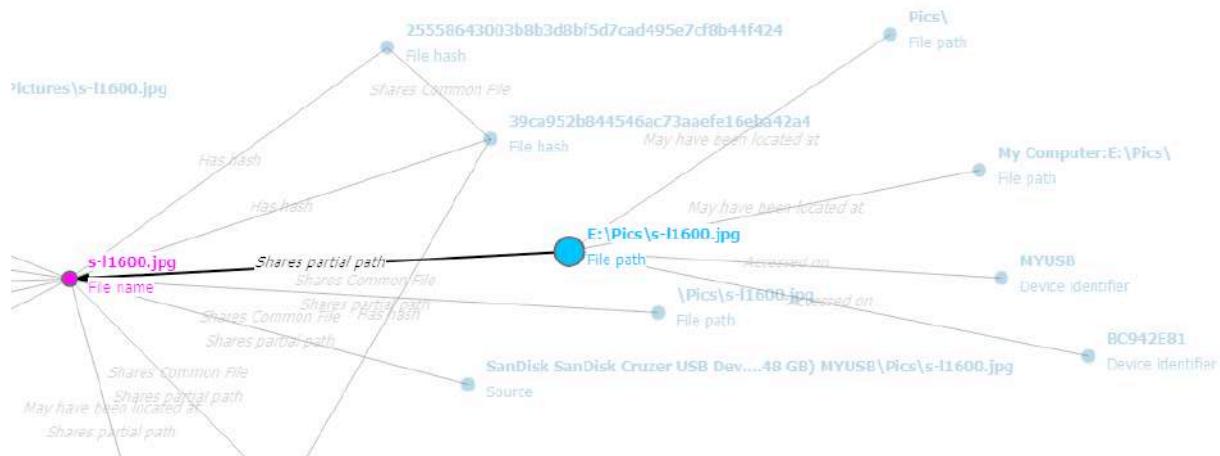


Figure 10.36 Primary (pink), selected (light blue), and indirect (faded) nodes

By selecting this node, it immediately becomes apparent that an external storage device with a volume name **MyUSB** and a volume serial number **BC942E81** was inserted into the computer and assigned the drive letter **E:**. This graphical representation makes it easier to see that the file **S-l1600.jpg** was accessed from a USB drive with these two properties.

The content displayed in the Connections explorer can be refined by filtering by Evidence source, Connectors type, or Attributes. The layout of the CONNECTIONS map can also be customized simply by dragging nodes around on the screen. This is sometimes necessary if the map contains many artifacts.

To print a copy of the CONNECTIONS map, simply right-click anywhere in the map and select Print...



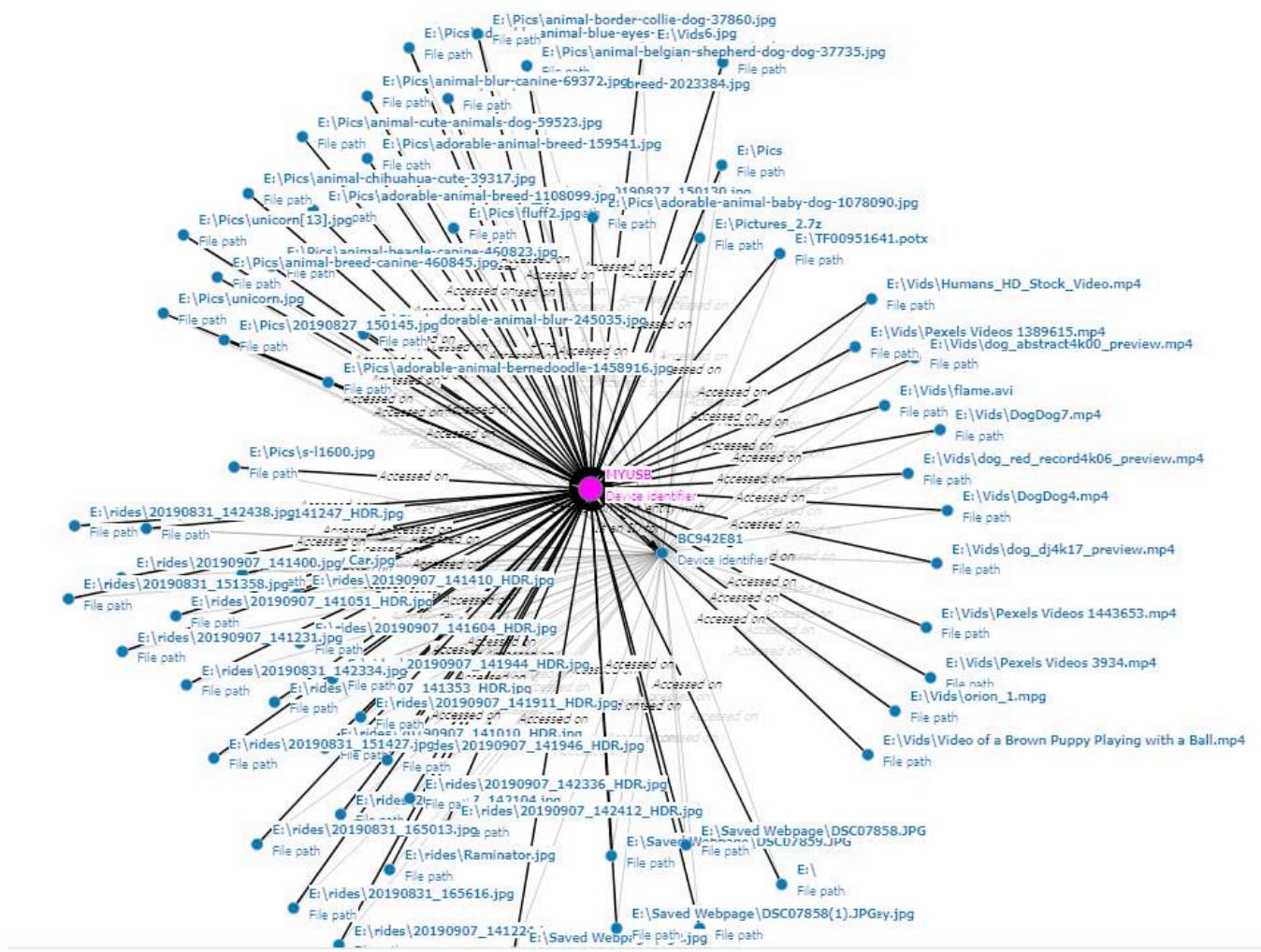


Figure 10.37 Complex connections map

RUNNING EXERCISE

CONNECTIONS

- From the **Artifacts** explorer in AXIOM Examine, clear any filters you may have applied.
 - From the Evidence drop-down menu on the FILTERS bar, select the two USB devices.
 - Select the MEDIA → Pictures category.
 - Filter the Filename column for the word “unicorn”.

- Select the file **unicorn.jpg**.
- There are CONNECTIONS icons next to the Filename, MD5 and SHA1 attributes.
- Click on the CONNECTIONS icon next to the Filename.

Who was this file transferred by?

Transferred with?

- Using the listed nodes take note of the various locations this file was stored.
 - What applications are associated with this picture?
-
- Clear all filters

TIMELINE

The Timeline explorer, as shown in Figure 10.38, provides a visualization of events in an interactive graph making it easy to conduct specific timeline examinations. The examiner can identify spikes in activity, focus on specific dates, and establish patterns in behavior. This view can be helpful in showing the sequence of events that occurred prior to, and after a particular event.

Like Connections, the Timeline must first be built using the option Tools → Build timeline. Alternatively, the Timeline can be set to automatically rebuild every time new evidence is added to the case by enabling the Automatically build timeline on case open option in Tools → Settings → POST-PROCESSING.

The graph shown below is a chronological representation of timestamped artifacts. The Timeline category column includes high-level categorization such as browser usage, file/folder opening, user event and more, and can be used to filter the information displayed. Other filter options are available in the FILTERS bar.





Figure 10.38 Timeline explorer

The date range displayed can be modified by selecting GO TO DATE at the top of the graphic, as shown in Figure 10.39. The next option, ZOOM, narrows or expands the dates displayed in the graph, and the dropdown modifies the axis points to years, months, days, hours, or minutes. See below:

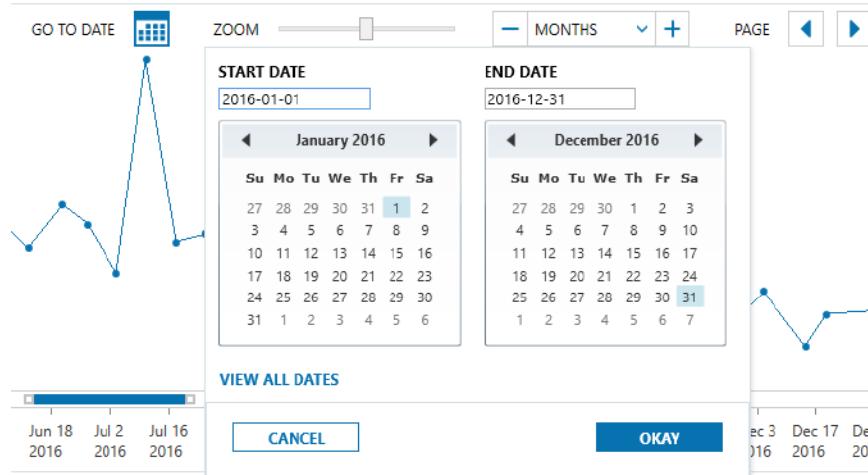


Figure 10.39 Timeline explorer date selection

If an individual artifact in the Timeline explorer is selected, the PREVIEW pane displays the artifact details.

RUNNING EXERCISE

TIMELINE

- From the **Artifacts** explorer in **AXIOM Examine**, clear any filters you may have applied.

- Switch to Timeline explorer. From the **FILTERS** bar, select the Date and Time drop-down. In **SET DATE RANGE**, change the Date range to All dates between, and set the range as 29 Aug 2019 to 29 Aug 2019. This filter will display only activity on 29 Aug 2019.
- From the **FILTERS** bar, use the **Timeline Categories** drop-down to filter for just Browser usage.
- From the **FILTERS** bar, use the Artifacts drop-down to filter for just Google Searches. Review the web searches made on this day.
- Find the first search for “golden retriever puppies.”
- Select the time icon  next to the Date/Time for this listing. In SET RANGE, deselect Use the same range of time both before and after the defined date. Set the range as 0 minutes before and 5 minutes after this time.
- Remove the filters for the Artifact (Google Searches) and Timeline (Browser Usage) category.
- From the **FILTERS** bar, select Data types and choose Artifacts only.
- Review the results.
- Clear all filters



MODULE REVIEW

In this module the following topics were covered:

- Media formats supported by Magnet AXIOM, for a full list, refer to the Artifact Reference.
- The different views available to review MEDIA artifacts.
- How the filmstrip is created and how it can be used to speed-up the investigative process.
- How to use Magnet.AI Picture Categorization to help quickly identify pictures of interest within the case.
- How to use Magnet Media Categorization to grade images to Project VIC or CAID.
- How to make use of the Officer Wellness functionality in AXIOM including activity timers, blurring and redacting illegal images.
- How to view artifacts in the Timeline, Connections, and Media explorers.

REVIEW QUESTIONS

To help reinforce the learning objectives for this module, the following review questions have been provided:

1. What types of data are categorized within the MEDIA artifact categories within AXIOM Examine?
2. What two PREVIEWS are available to help examiners quickly review VIDEO artifacts?
3. At what percentage of a VIDEO file does AXIOM Process take still frames to create the filmstrip PREVIEW?

4. MAGNET.AI can search for and categorize pictures within the case. Name five of the current categories searched for.
5. Which keyboard button can be used to grade all visible uncategorized images?
6. When exporting user graded media, what export type should be selected?
7. Which three methods are available to reduce exposure to pictures and videos that could be distressing or illegal?



STUDENT EXERCISE

This exercise is based on the Dashner case scenario from Module 1.

- From the **Artifacts** explorer in AXIOM Examine, clear any filters you may have applied.
 - Select the MEDIA → Pictures category.
 - Ensure the **EVIDENCE** pane is set to Column view.
 - Sort the Model column.
List some of the detected Models.
-

- Switch to the **File system** explorer and select the Lexar USB Flash Drive USB Device Decrypted.
- In the Evidence pane, double-click the “Entire Disk” entry to expand it.
- Highlight the ...\\New Friends\\ folder, right-click and select View related artifacts.
How many items are listed within the MEDIA → Pictures category? _____
- Create a Tag named “Dashner Pictures” and apply it to these Pictures.
- Switch back to the File system explorer and on the decrypted Lexar USB evidence, navigate into the folder \\old flash drive pics\\old flash drive pics\\
- Highlight the folder \\hugsnotdrugs\\, right-click, and select View related artifacts.
- Select the MEDIA → Pictures category.
- Select the file named **spice_1-2.jpg**.
- Click the CONNECTIONS icon next to the Filename in the DETAILS pane.
- Locate the MD5 hash (beginning in 973) and select the node. View the DETAILS pane.

Which Cloud Storage is associated with this file?

- Select the Media explorer from the explorer drop-down
- On the left-hand navigation pane, select the CAMERA DETAILS filter and select the checkbox for “iPhone5s” and hit APPLY FILTER
How many Pictures were taken using an iPhone? _____
Where were these Pictures parsed/carved from?

-
- Clear all filters.
 - Switch to the File system explorer.
 - In the NAVIGATION pane, select **ALL EVIDENCE**.
 - In the EVIDENCE pane, right click the **SanDisk Sandisk Cruzer USB Device 7.48 GB full image.e01** entry and select View related artifacts.
 - From the Artifacts drop-down menu on the FILTERS bar, select MEDIA.
 - Select the MEDIA → Videos category.

What is the Created Date/Time of the Video **DogDog4.mp4**?

- Using just the filmstrip PREVIEW
What is the approximate run time of the Video? _____
What is depicted in the video? _____
- Click the CONNECTIONS icon next to the Source of the Video.
- Select the direct node for **DogDog4.mp4**.
- Does it appear this file was accessed on Dashner's computer from an external device? If so, what were the device identifiers for this device and which program was used to view it?

- Switch back to the Artifacts explorer and clear all filters.
- On the FILTERS bar, from the EVIDENCE drop-down, select the **SanDisk Cruzer USB Device** only.
- From the NAVIGATION pane, select the MEDIA category
- Select the menu option Process → Categorize pictures with Magnet AI.
- Select Pictures in the current view and click **NEXT**.
- Select the categories for Drugs and Vehicles then click **CATEGORIZE PICTURES**.
How many pictures are categorized as:
Possible Drugs _____
Possible Vehicles _____
- Did Magnet.AI TAG the hits? _____



Notes





MAGNET
FORENSICS®

MODULE 11:

Mobile Artifact Analysis

LEARNING OBJECTIVES

In this lesson, students will take part in lecture, instructor-led exercises, and student practical exercises to gain an understanding of the capabilities of Magnet AXIOM in recovering artifacts from mobile devices. Supported mobile operating systems will be discussed in detail, and how to acquire the data into evidence files as well as how to process the artifacts from the mobile phone images. In addition to Mobile artifacts, Chat artifacts will also be discussed. Students will learn the artifact types accessible from mobile sources and how to use AXIOM Examine to discover additional data that is not a natively parsed artifact.

GOALS

At the conclusion of this lesson, students will be able to identify supported mobile operating systems and will be able to add data from mobile sources to identify artifact types. Students will gain an understanding of how to use Magnet AXIOM to conduct forensic examinations on mobile devices.

SMARTPHONE OPERATING SYSTEMS

Magnet AXIOM can use and process images from multiple smartphone platforms. iOS, Android, Windows Phones, Kindle Fire, media devices via the media transfer protocol (MTP), and SIM cards are all supported for loading and processing with AXIOM Process and AXIOM Examine. Additionally, AXIOM Process can accept images from other forensic platforms. To load images or file dumps for any of these mobile operating systems, choose MOBILE from the SELECT EVIDENCE SOURCE screen. At that point, AXIOM will present options for the four supported mobile operating systems to the user.

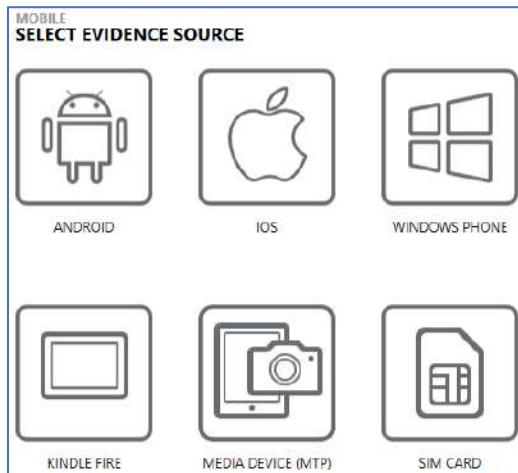


Figure 11.1 Supported mobile operating systems in AXIOM Process

IMAGING IN AXIOM

Dashner is in possession of a Pixel 3a Android device. To examine this device users need to select the evidence source Mobile → Android → Acquire Evidence. There are two further options to acquire data. One will utilize exploits to try to circumvent the security measures put in place by Android, while the other will grab data from a regular, unlocked device. While some of these exploits can obtain a full physical image, for the purposes of this course we will be examining the standard Quick imaging process.

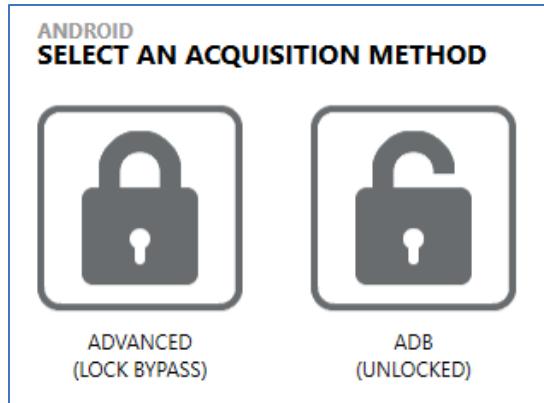


Figure 11.2 Android acquisition methods

Selecting the ADB (UNLOCKED) option will display devices that are currently connected to the machine. In order to obtain an image from an Android device, several things must be in place first:

1. The correct driver needs to be installed on the host machine to allow communication with the mobile device.
2. Android devices also require the USB debugging function to be enabled in order to communicate with the computer.
3. Root access on the device may also be required to gain full access to the system files.

Drivers are a vital to the communication process. Each Android device will have a set of drivers that can be used – often manufacturer dependent. There may be a driver for the modem, one for the COM port communication, another for special software installation from the carrier, etc. The driver that matters the most for forensics is the Android Debug Bridge (ADB) driver. This is a separate driver that allows for ADB communication to complete. Best practice would be to use a dedicated ADB driver, although others may work. Once the device is placed into USB debugging mode, the ADB debug driver can be installed by a manufacture source or by a third-party vendor, i.e. a generic or vendor-neutral driver.



Figure 11.3 ADB driver installation for Android

ANDROID DEBUG BRIDGE

Android Debug Bridge (ADB) is the communication protocol developed for Android. It allows for the communication of devices to a host machine using a client/server environment. The ADB is three distinct parts: client, server, and daemon (a background service). The client and server run on the forensic machine, whilst the ADB daemon runs on the Android device. The client will send ADB commands which the server will facilitate by communicating to and from the daemon, ultimately returning results to the client. All forensic tools use the ADB protocol to communicate with Android devices in one way or another.

It is possible to obtain the ADB setup by downloading the Android SDK for Google from <https://developer.android.com>. In addition, Magnet AXIOM has also included a version of the ADB setup to allow it to communicate with plugged in devices. This is found under:

C:\Program Files\Magnet Forensics\Magnet AXIOM\AXIOM Process\ADB

AXIOM will use this version of the ADB commands to communicate with the connected device and perform several functions such as installing a custom application, performing backups, attempting software exploits, and extracting files from the file system.

The ADB package in the above folder can function independently of AXIOM for advanced troubleshooting of the connection and extraction functionality.

DEVELOPER OPTIONS

For the ADB protocol to work, Developer Options must be enabled on the device. Since Android version 4.2, the developer options area was hidden from the end user. To re-enable this menu, locate the **About Device** area under the device's settings. Scroll down until **Build Number** is displayed. **Tap on Build Number 7 times** until a pop-up window displays **Developer mode has been turned on**. Once developer options are enabled, a separate menu will be available under the Settings area:

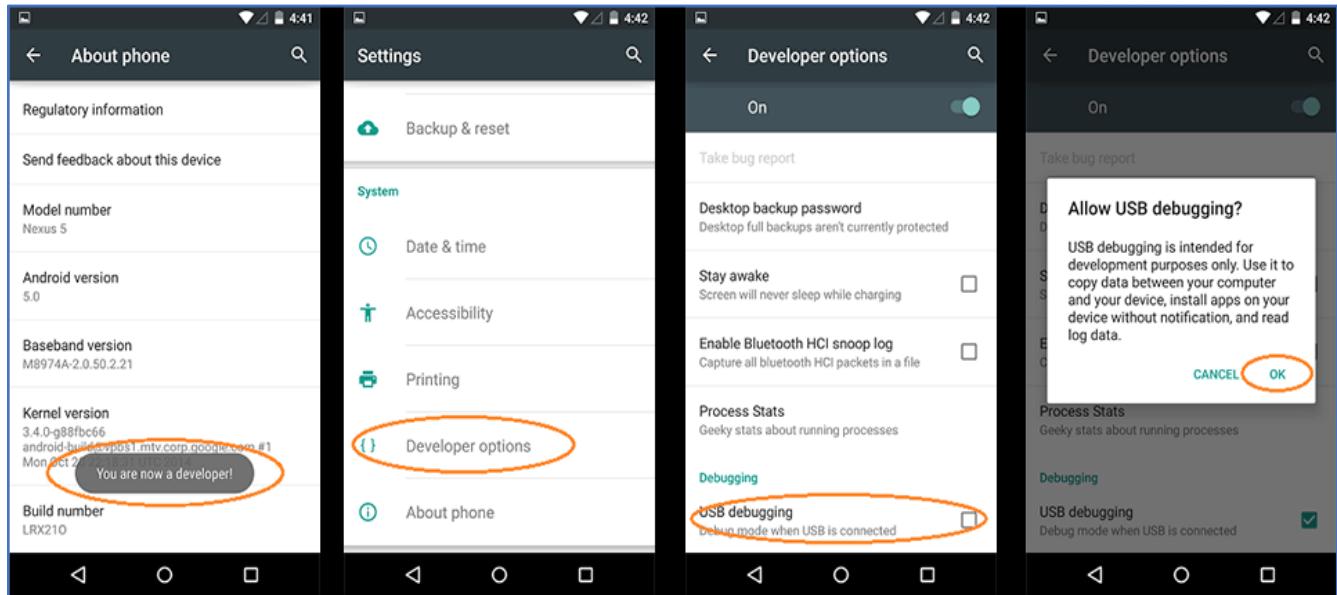


Figure 11.4 Enabling Android USB debugging

USB DEBUGGING

By default Android USB Debugging is switched off for security. The ADB protocol being left open could allow users unauthorized access to a device. USB debugging can only be activated through an unlocked device. This is problematic for forensic examiners as without the debugging option ADB communication is not available. Once the developer options are enabled, USB debugging can be turned on.

If the device is unlocked, USB debugging can be enabled by using the menus to navigate to **Settings → Developer Options → USB Debugging**. Select the checkbox for this option to enable it. In newer versions of Android, a separate pop-up is displayed warning against enabling this option, making it less likely a user would enable it.

Also, under this option menu is a **Stay Awake** option. This option keeps the device screen on and keeps the device from locking with a handset password if it is connected to power. This option should be enabled by first responders if available.

An additional security prompt was added with the release of Android version 4.2.2 to reduce unauthorized access. Once developer options have been enabled and USB debugging turned on, an additional prompt will appear. This prompt will appear for each computer the device connects to as it uses unique RSA keys for each computer. These RSA keys are stored on the device under **/data/misc/adb/adb_keys**. New keys are appended to this file.

While the previous options are needed to enable communication, side loading applications is blocked by default on Android, allowing only approved sources to install applications. The whitelist is provided as part of the Google Play store. To install applications from additional sources, the **Unknown Sources** option must be enabled. In most versions of Android, this can be found under **Settings → Security**.

This option allows for the installation of applications from third party application stores and the side loading of applications. This means that any application can be installed into an Android device with this option enabled. Forensic suites use this option to inject a custom application to recover data from the Android device.

The **Verify apps** option should also be unchecked. This option will check applications before they run, which is good for applications that may include malicious code. However, some of the commands used by forensic applications can also trigger this warning.

Once the device has all the options needed to maintain connection, it will appear within the Evidence Sources area of AXIOM.

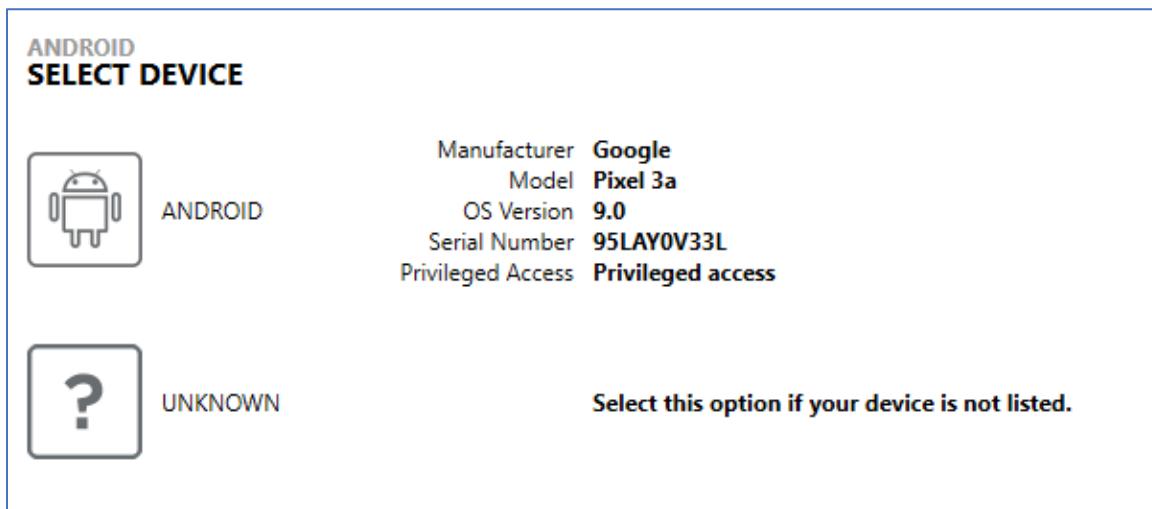


Figure 11.5 Reviewing device details before acquisition

Once listed, some of the information displayed includes Manufacturer, Model, OS Version, Serial Number, and the Privileged Access level. The Privileged Access level determines whether the device has gained root access. Without root access, only the Quick imaging type will be available instead of a full imaging type. This will be the most common scenario that examiners come across.

ANDROID IMAGE TYPES

After all the needed communication steps have taken place and the device is seen by AXIOM Process, there are multiple types of images that can be acquired. A Quick image will capture active data on the device including SMS, Contacts, Call Logs, and more using an Android application package (APK) installation to capture information. It will also perform an ADB backup command to gather information.

A Full Image will capture the entire block of memory of the device; however this requires root level access. This is done by installing a security exception which removes the protection put in place by the operating system designers.

In the case of devices that are protected using Android's File Based Encryption released in Android version 7 and higher, a Full Image will not be available, and it will be replaced by the option for a Logical Image. This is a **true** logical extraction where it obtains all available files and folders from the device. The full or logical extraction will only be available when a device is found to have privileged access.

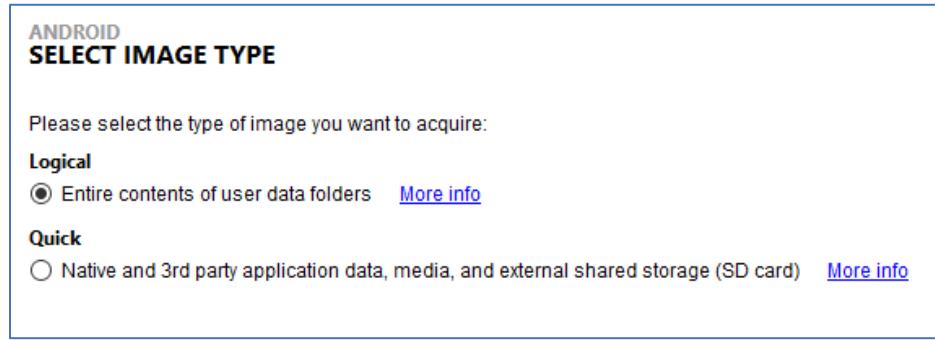


Figure 11.6 Selecting image type

NOTE: If privileged access exists, conduct a Full/Logical Image.

Within the settings for AXIOM Process, the user can set an option for Restore Device State. By default, the APK file that is installed for a quick image is left on the device after the acquisition process is complete. This will leave the Acquire application on the device, as well as the data that it gathers under the directory **/data/com.magnetforensics.acquire/**. By checking the Restore Device State within the AXIOM settings, this will trigger the software to be uninstalled after the data is gathered.

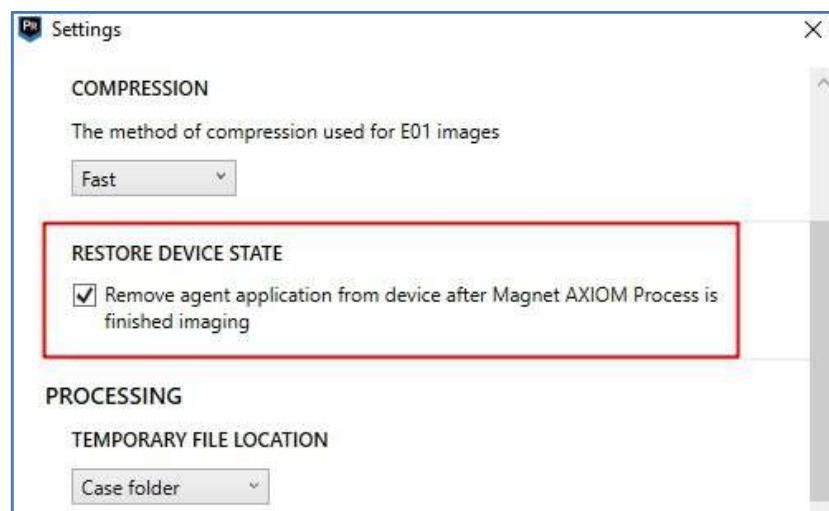


Figure 11.7 Restoring device state from AXIOM Process

When using the Quick image, two sets of data are recovered. The first, Agent Data, will show information that has been recovered using the Magnet AXIOM APK agent. The agent will acquire SMS/MMS data from the **mmssms.db** file and contact/call logs will be recovered from the **Contacts3.db** file. The actual database files will not be acquired due to the security of the device, however, copies of the active information of the data from the database will be extracted. For more information on what the Android agent can extract, please see the following list:

- * For each account on the device:
 - * Name
 - * Account type
- * For each Bluetooth device known by the device:
 - * Name
 - * MAC address
 - * Bluetooth class
 - * Bond (pairing) status
- * For each website in the device's browser history
 - * URL
 - * Name
 - * Number of visits
 - * Date of last visit
- * For each calendar on the device:
 - * ID
 - * Name
 - * Display name
 - * Whether or not the calendar has been deleted
 - * Time zone
 - * Account which owns the event
 - * Owner's account type
 - * Whether or not the calendar has local changes that aren't synced
- * For each event in each calendar on the device:
 - * ID



- * Title
 - * Description
 - * Start date and time
 - * End date and time
 - * Location
 - * Time zone
 - * Recurrence rule
 - * Recurrence dates
 - * Recurrence exception rule
 - * Recurrence exception dates
 - * ID of the parent recurring event (For exceptions to recurring events)
 - * Instance time of the parent recurring event (For exceptions to recurring events)
 - * Whether or not the event has local changes that aren't synced
 - * Whether or not the event has been deleted
 - * ID of calendar that the event's in
 - * Display name of calendar that the event's in
- * For each attendee for each event in each calendar on the device:
- * ID
 - * Name
 - * Email
 - * Relationship of the attendee to the user
 - * Whether the attendee is required, optional, etc.
 - * RSVP status of the attendee
- * For each phone call made by the device:
- * Phone number of the device on the other end
 - * Type (incoming, outgoing, missed, blocked, voicemail, etc.)
 - * Date and time of the call
 - * Duration of call
 - * Caller ID of device on the other end
- * For each contact on the device:
- * ID
 - * Display name
 - * Name and type of each account that the contact has
 - * Phone numbers (including deleted phone numbers)
 - * Email addresses (including deleted email addresses)
 - * Note (including deleted notes)
 - * Photo (including deleted photos)
 - * Websites (including deleted websites)
 - * Number of times contacted
 - * Date and time of last contact
 - * Whether the contact is "starred"
- * For all downloads:
- * URI
 - * Date and time of last modification
 - * Size
 - * Contents of the file in binary
- * For each SMS and MMS message:
- * ID

- * ID of thread
- * Date and time that the message was sent
- * Date and time that the message was received
- * Whether or not the notification for the message has been seen
- * Whether or not the message has been read
- * The body of the message
- * Address of the other party
- * Service center which the message was sent through
- * Whether or not the message is locked
- * List of attachments on the message
- * For the device's SIM card:
 - * State (locked, unlocked, absent, error, etc.)
 - * Serial number
 - * Country code of SIM
 - * Network code of the SIM provider
 - * Name of the SIM provider
 - * Cellular network user ID (IMSI or equivalent)
 - * Phone number
 - * Radio type
 - * Voicemail ID
 - * Voicemail number
 - * Device ID (IMEI or equivalent)
 - * Country code of current cellular network
 - * Name of operator of current cellular network
 - * Type of current cellular network (GSM, LTE, etc.)
 - * Software version of SIM firmware
 - * Whether the device is considered to be roaming or not
- * For the device's customized spellcheck dictionary:
 - * Each word in the dictionary
 - * Each series of characters that spellcheck should suggest the word as a replacement for
- * For the device's WiFi data:
 - * MAC address of the device
 - * SSID for each stored network
 - * Security key system (PSK, EAP, or none) for each stored network
 - * ID number for each stored network

A second set of data, **adb-data.tar**, will include information from the ADB backup information. There are two folders within this tar file, Shared and Apps. Shared will contain information from the operating system and the internal (emulated) or external microSD cards. The Apps folder will contain information that developers have chosen to be backed up from core and third-party applications. This is not a true file system copy of the device, only what developers have chosen to be backed up, and areas of the file system that are not protected.

Magnet AXIOM will also acquire “Live” device data through ADB commands against the device. Information acquired from this technique could give information that would not traditionally be available



from devices that are not rooted or have privileged access. Data contained as “Live Data” is stored as .txt files that are then parsed for various artifacts such as:

- Device DateTime UTC
- Device Properties
 - IP Information
 - Roaming information
 - SIM information
 - Timezone
 - Serial Number
 - Encryption Type (Yes/No | FDE/FBE)
- Task statistics
- Usage Statistics (app usage and movement)
- WiFi Statistics

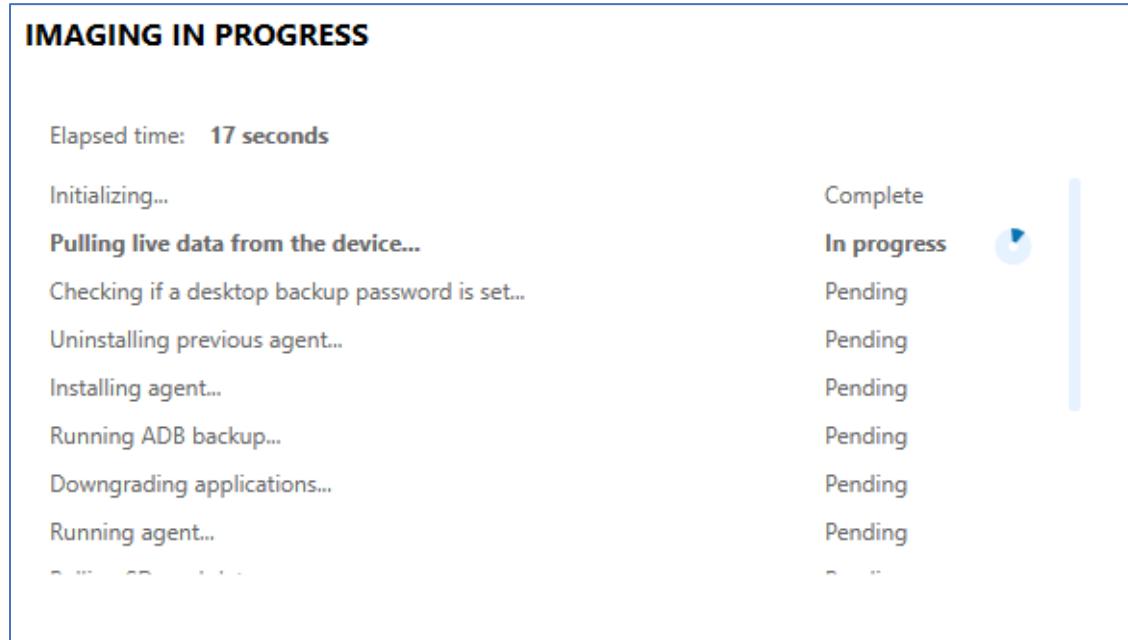


Figure 11.8 Reviewing the imaging process

The data from these extraction techniques will be covered in more detail later within this chapter.

INSTRUCTOR DEMONSTRATION

ACQUIRING AN IOS DEVICE

- Connect the device to the examination machine.

- Unlock the iOS device and press the “Trust” option on the dialog.
- Open AXIOM Process from the Desktop.
- In the CASE DETAILS pane, assign the file paths and case name.
- In the EVIDENCE SOURCES, under SELECT EVIDENCE SOURCE, choose MOBILE.
- Under SELECT EVIDENCE SOURCE, choose iOS.
- Under iOS LOAD OR ACQUIRE, choose ACQUIRE EVIDENCE.
- Select the device when it appears and click **NEXT**.
- Unless the device is Jailbroken, leave the IMAGE TYPE as Quick.
- AXIOM Process then provides the option to create an encrypted backup. If a password is added, additional information such as the Home data and keychain will be acquired.
- Jump to the Mobile artifacts section.
- Press **CLEAR ALL**.
- Under the OPERATING SYSTEM section, select the File System Information artifact.
- Press **GO TO ANALYZE EVIDENCE**, then press **ANALYZE EVIDENCE**.
- This will create our “Quick” image of the device with no artifacts being parsed but the File System Explorer artifacts.

ACQUIRING AN ANDROID DEVICE

- Connect the device to the examination machine.
- Ensure USB debugging is enabled by swiping down from the top of the screen and pressing the “Cog” icon.
- In Settings, scroll down to Developer Options. In this menu, ensure USB Debugging has been checked.
- Open AXIOM Process from the Desktop.
- When prompted with a security prompt on the device, press “Always allow from this computer” and then “Ok.”
- In the CASE DETAILS pane assign the file paths and case name.
- In the EVIDENCE SOURCES, under SELECT EVIDENCE SOURCE, choose MOBILE.



- Under SELECT EVIDENCE SOURCE, choose Android.
- Under ANDROID LOAD OR ACQUIRE, choose ACQUIRE EVIDENCE.
- Select the device when it appears and click **NEXT**.
- At the SELECT IMAGE TYPE screen select a Quick image.
- Jump to the Mobile artifacts section.
- Press **CLEAR ALL**.
- Under the OPERATING SYSTEM section, select the File System Information artifact
- Press **GO TO ANALYZE EVIDENCE**, then press **ANALYZE EVIDENCE**.
- This will create our “Quick” images of the device with no artifacts being parsed but the File system explorer being available.

LOADING MOBILE IMAGES

Magnet AXIOM can accept several images from different sources including other forensic tools. If an examiner is using a toolbox approach and using multiple mobile forensic tools to extract data, these extractions can then be loaded into AXIOM Process for additional artifacts and validation purposes. In order to load the extraction into AXIOM Process, the workflow used is to select Mobile -> iOS / Android -> Load Evidence.



Figure 11.9 Loading or acquiring a mobile phone

Within the Load Evidence option, users can then choose to load a pre-acquired image or just a collection of files or folders. When selecting an image, there are multiple choices that an examiner can select from other tools.

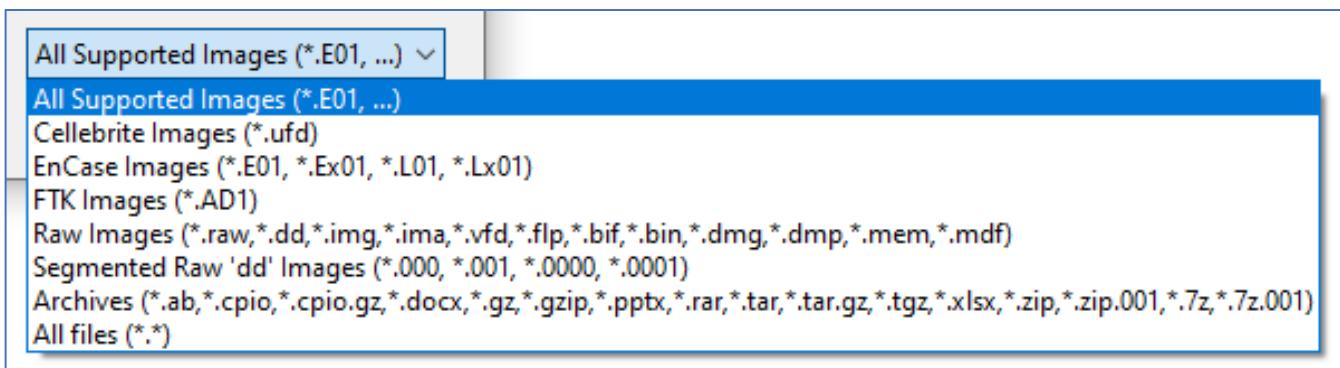


Figure 11.10 Supported image format types

Examiners can choose to add a standard RAW/DD image, a segmented image or archive container, or could choose a vendor-specific container like a UFD file. In the case of choosing a vendor-specific file like a UFD file, the data may not be within the file, and if the UFD does not work, adding the raw data files could also be an option.

Other forensic tools may produce images that are not directly supported. However, there are steps that examiners can take in order to make these files ingestible. For more information please refer to this blog post on the Magnet Forensics website: <https://www.magnetforensics.com/blog/how-to-ingest-images-from-various-tools-and-acquisition-methods/>. From here, articles are available to walk users through loading Cellebrite, Oxygen, XRY, and GrayKey image types.

MOBILE ARTIFACTS

AXIOM Process will enable Mobile artifacts to be selected when it encounters a mobile evidence source loaded. There are fourteen categories of mobile artifacts available. To select an entire category the user need only place a check in the box beside that category. Highlighting the category allows the examiner to individually select artifacts for processing.



Figure 11.11 Example of mobile artifacts in AXIOM Process



Some artifacts will have an [OPTIONS](#) link as seen in Figure 11.12 Video artifact options. These links allow the user to set specific options about that artifact. For example, the [OPTIONS](#) button on the Videos artifact will allow the user to export the video files as part of the evidence processing step.

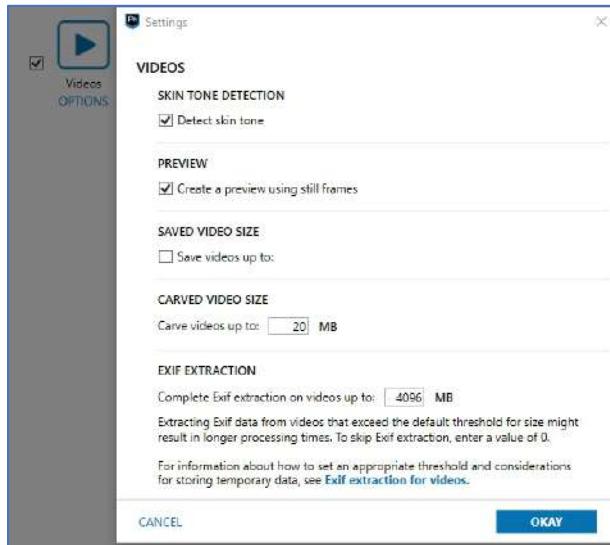


Figure 11.12 Video artifact options

VIEWING ARTIFACTS

AXIOM Examine offers several helpful ways to review the data that comes from mobile operating systems. Users have the option to see the data in several different ways within the Artifacts explorer, including viewed in Row, Column, or Classic view. Changing the view to Thumbnail view for example can help filter the acquired data. Examiners can be benefited by seeing data sorted by time, geolocations, or by a threaded view for chat artifacts, for example.

In addition to the Artifacts explorer, the File system explorer allows examiners to scrutinize PLIST and SQLite database files.

The screenshot shows the Magnet AXIOM interface with the 'Evidence pane' open. On the left, there is a table titled 'Call...' with columns for 'Call Date/Time' and 'Duration'. The table lists several 'Missed Call' entries. On the right, a context menu is displayed under the heading 'Local User' with options: 'Column view' (selected), 'Classic view', 'Conversation view' (with keyboard shortcut Alt+Shift+3), 'Histogram view' (with keyboard shortcut Alt+Shift+4), 'Row view' (with keyboard shortcut Alt+Shift+5), 'Thumbnail view' (with keyboard shortcut Alt+Shift+6), and 'World map view' (with keyboard shortcut Alt+Shift+7).

Call...	Call Date/Time	Duration
Missed Call	22-Aug-19 6:43:49 PM	0
Missed Call	22-Aug-19 6:41:54 PM	0
Missed Call	22-Aug-19 4:36:48 PM	0
Missed Call	22-Aug-19 3:59:50 PM	0
Missed Call	21-Aug-19 8:44:00 PM	0

Figure 11.13 Evidence pane views

CONVERSATION VIEW

The Conversation view is one of the most helpful views and will automatically filter the available results into an easy to read conversation. Each threaded chat will display the data as it appears on the device. This allows the user to view the chats as they would have appeared, sorted based upon the time and date of the message. It is also easy for the user to export the data in this view into both PDF and HTML formatted reports.

The screenshot shows the 'COMMUNICATION' section of the Magnet AXIOM interface. It displays three categories: 'Android SMS/MMS (Content Provider)' (101 messages), 'Cloud Facebook Messenger Messages' (3 messages), and 'Skype Activity' (42 messages). To the right, the 'Conversation view' is shown for the first category, displaying two threads. The top thread is for '+15012370855, Martin Clemons (+18705179483)' with 32 chat messages. The bottom thread is for '+18318512510' with 1 chat message.

COMMUNICATION		146
	Android SMS/MMS (Content Provider)	101
	Cloud Facebook Messenger Messages	3
	Skype Activity	42

Figure 11.14 Conversation view for chats

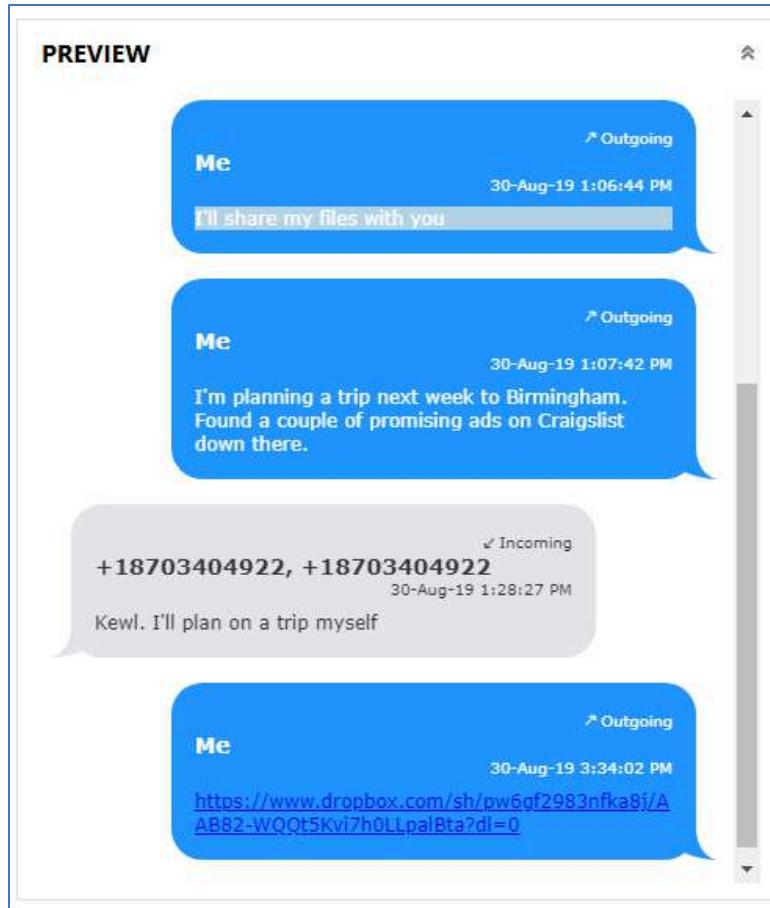


Figure 11.15 Conversation view in the PREVIEW card

Images and videos that are embedded into conversations will also be available within the chat threaded preview. Examiners can review this information within the threaded view, however using the Column view of AXIOM can reveal more information about the attachments that are embedded.

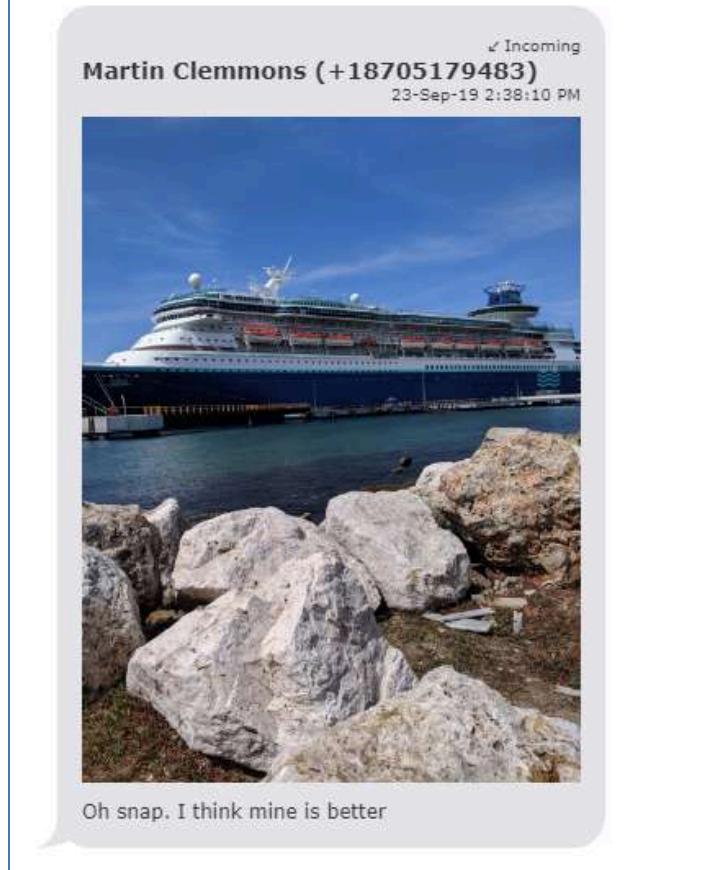
PREVIEW

Figure 11.16 Image previews within conversation view

ANDROID SMS/MMS (CONTENT PROVIDER)

There are multiple sources of SMS/MMS messages on an Android device. When acquiring data via a Quick image type, the data is pulled from the agent application installed onto the device during processing. The data populated in AXIOM comes from the **mmssms.db** database on the Android device, however this is only the active information that is available to the application. Whilst the database cannot be extracted through this acquisition type, the data held within is output to a new database - **agent_mmssms.db**.

The artifact will track several relevant columns for the examiner including the Participants of the message, Original Transmit Date/Time, the body of the message, and its status (incoming or outgoing). If an attachment is included a column called MIME Type will record the type, for example “image/jpeg” or “image/gif”. MIME stands for Multipurpose Internet Mail Extension and it simply indicates the format of a document or assortment of bytes.

ARTIFACT INFORMATION	
Participants	Jeff Armstrong (+18652323212)
Original Transmit Date/Time	30-Aug-19 3:45:15 PM
Message	A few more
Message Status	Incoming
MIME Type	image/jpeg
EVIDENCE INFORMATION	
Source	Google Pixel 3a Quick Image.zip\Agent Data\agent_mmssms.db
Recovery Method	Parsing
Deleted source	
Location	Table: mmssms(rowid: 19) Table: data(rowid: 13)
Evidence number	Google Pixel 3a Quick Image.zip

Figure 11.17 Reviewing SMS messages within the DETAILS pane

ACCOUNTS INFORMATION

Within the Android quick image, the Accounts Information artifact can reveal information that was captured from the Android device using the “dumpsys” ADB commands. This information is captured as part of AXIOM’s Live Data acquisition on the Android outside of the agent acquisition and ADB backup processes. The source file for this information is saved to a .txt file because it is live information from the device and is not captured as part of a file.

User Name	Package Name
isaiah.dashner@gmail.com	com.google
jasonsmithers131@gmail.com	com.google
Facebook	com.facebook.auth.login
Messenger	com.facebook.messenger
isaiah.dashner@gmail.com	com.dropbox.android.account
WhatsApp	com.whatsapp
Skype	com.skype.raider

Figure 11.18 User accounts on the Android device

The artifact will capture the username and the package the username is associated with. However, as this information typically comes back to the **accounts.db** on a full file system/physical image of a device,

the application or service may not keep the username listed, and may only reflect that the service itself was in use, e.g. WhatsApp, Facebook, or Skype.

ANDROID CALL LOGS

The Android Call Logs artifact allows the user to review the call logs that are currently active on the device. These records are encapsulated into an SQLite database to mimic the information as it appears on the device. The call logs will store the partner's number, the direction of the call, the call's status (whether the call is answered or unanswered), the date/time of the call, and the duration of the call, recorded in seconds.

ARTIFACT INFORMATION	
Local User	Local User <Google Pixel 3a Quick Image.zip>
Partner	+15015881514
Partner Name	King Financial Group LLC
Direction	Incoming
Call Status	Missed Call
Call Date/Time	11-Nov-19 2:19:45 PM
Call Duration (Seconds)	0

Figure 11.19 Android call logs

When using AXIOM's connections feature, examiners can press the connector icon beside the Local User fragment to see a mapping of all the users the device has called.



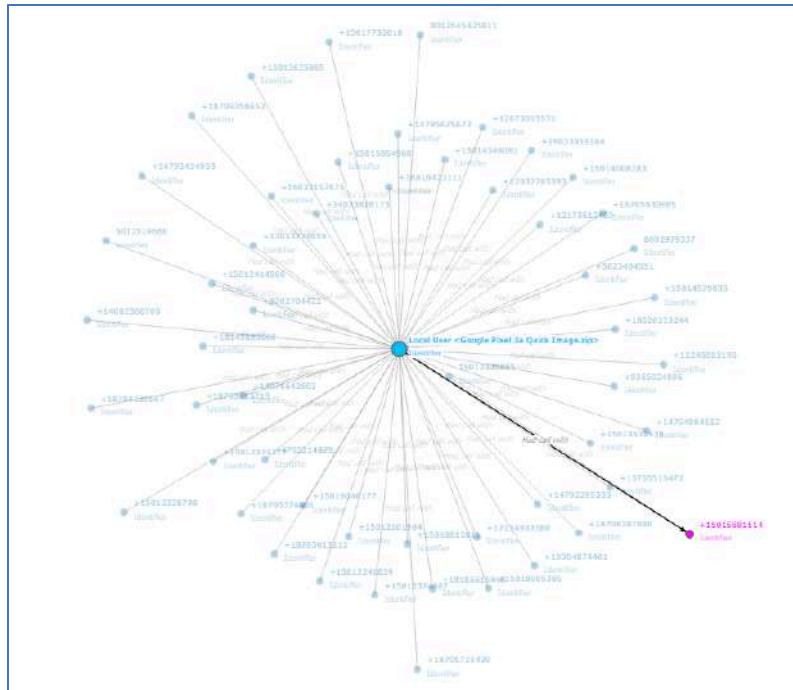


Figure 11.20 Mobile connections view

ANDROID DEVICE INFORMATION

The Android Device Information artifact is crucial because the user can find information about the device as well as the owner of the device. In order to get all the information, there are two separate sources for the evidence file. One comes from the agent data from the APK file pushed to the device while the other comes from the live data acquisition.

If a SIM card (UICC) is inserted into the Android device, the agent can acquire several pieces of information about both the device and the SIM.

ARTIFACT INFORMATION	
Device ID	359677096510187
IMSI	310260974463809
IMEI	359677096510187
ICCID	8901260971144638093
SIM Card State	READY
Service Provider Country Code	us
Mobile Country Code	310
Mobile Network Code	260
Service Provider Name	Google Fi
Device Phone Number	+15012370855
Device Phone Type	GSM
Voice Mail Identifier	Voicemail
Voice Mail Number	+16505034700
Network Type	Unknown
Device Software Version	04
Roaming	No

Figure 11.21 Android device information

The device's ID as well as identifiers such as IMEI, ICCID, and IMSI are captured from the SIM. In addition, the network type and currently assigned device phone number are listed within this artifact. This information may only be available from the SIM card being inserted into the device. The information that is available on the SIM may differ from device to device depending on the carrier.

ARTIFACT INFORMATION	
Serial Number	94SAY0SJSY
Manufacturer	Google
Model	Pixel 3a
Product Name	sargo
Bootloader	b4s4-0.1-5653622
SIM Card State	LOADED
Current Network Country ISO Code	us
Current Network Operator Name	Google Fi
Device Software Version	9
Security Patch	2019-08-01
Roaming	false
Bluetooth Address	58:CB:52:81:89:06
Bluetooth Name	Pixel 3a
Timezone	America/Chicago

Figure 11.22 More mobile device information

When reviewing the device information from the live data source, the information is acquired directly from the Android device using an ADB command. This grabs slightly different information about the device itself instead of the network and its identifiers. This data grab can tell us what version of security and version the device is running for future exploit use, but also the device's currently set time zone for applying proper time zone offsets.

MANUALLY REVIEWING INFORMATION

If an examiner wants to see if third-party application data has been captured from the ADB backup command or what other information may be available from the emulated SD-card storage, it is possible to review the data within the File System explorer of AXIOM. By switching to the explorer and opening the Google Pixel 3a Quick Image.zip image file, examiners will see how the data is segmented after acquisition.

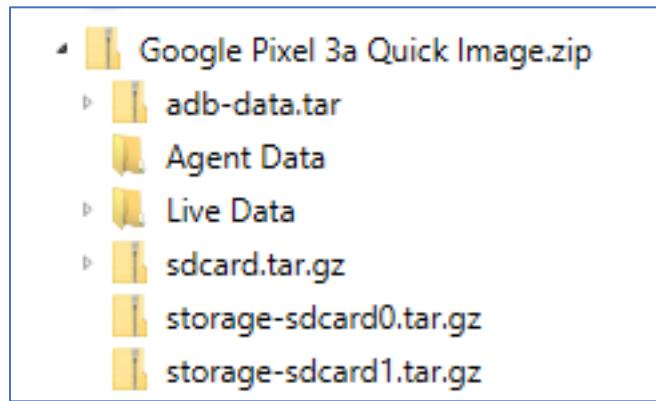


Figure 11.23 Android file system view

The device image is divided into several sections:

- **Adb-data.tar:** This is the information acquired from the ADB backup command. This will include two subfolders: Apps and Shared.
 - Apps: Data from applications on the device that the developers have allowed to be backed up.
 - Shared: Information from the emulated SD card area of the device that is backed up by the ADB backup command.
- **Agent Data:** This is the information acquired from the custom Android application. The databases in this folder are set to mimic their original source files but are not copies of the databases themselves.

- **Live Data:** This is a collection of .txt files that are pulled from running ADB commands against a live device. This information will typically exist in other files and formats on the actual device but can only be acquired by running ADB commands against the live device if it is not rooted.
- **Sdcard.tar.gz:** A secondary collection of the emulated SD card data that is saved as a tar.gz archive file.

If the examiner would like to eliminate some duplicated information or chooses to focus on just one section of data at a time, the examiner can highlight any of these files/folders and right-click View related artifact from the File System explorer.

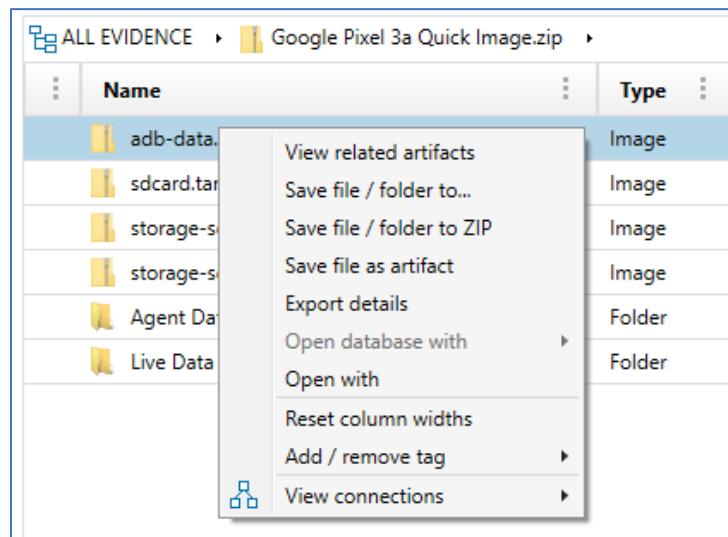


Figure 11.24 Viewing related artifacts

COMMUNICATION ARTIFACTS

AXIOM Process supports over 300 known types of Internet artifacts, many of which are instant messaging, or chat clients. Magnet AXIOM can recover communication data from a wide variety of evidence sources, including PC, Mac, and mobile platforms. When possible, AXIOM will also recover data from deleted chat client activities. Supported chat clients can be found in the COMMUNICATION section in AXIOM Process, under the ARTIFACT DETAILS section where the examiner can make selections for both PC (Windows and Mac) and mobile (Android, iOS, Windows, Kindle Fire) evidence. Depending on the platform of the evidence source selected (computer or mobile), the list of COMMUNICATION evidence may differ.



Figure 11.25 Example of communication artifacts

APPLICATION OPTIONS FOR COMMUNICATION ARTIFACTS

AXIOM Process may have an [OPTIONS](#) hyperlink enabled for some messaging artifacts to assist in potentially decrypting the data. It is important to note that these [OPTIONS](#) may also differ between the COMMUNICATION selections from within the Computer artifacts or Mobile artifacts options in the ARTIFACT DETAILS section of AXIOM Process.

Figure 11.26 Zoom options within Computer artifacts

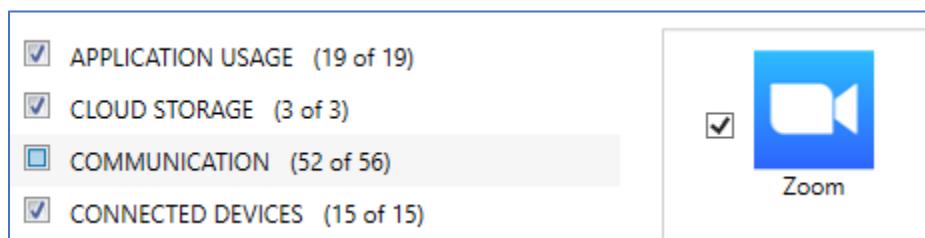


Figure 11.27 Zoom within Mobile artifacts

Evidence recovered from WhatsApp can include messages, images, audio, and video but an email address or decryption key may be needed to decrypt the data depending on the version. In some other versions of chat software, a key or token value may be needed from a mobile device to decrypt the data.

The Signal application is an encrypted communications application used primarily on Androids and iOS products. Signal can also be used as a desktop client for Linux, Windows and MacOS. Users can send one-to-one and group messages, including voice, files, videos, and images. Signal can be utilized to make one-to-one voice and video calls. In order to decrypt the Signal database in AXIOM Process, a password or key (depending upon the operating system) is required.

Regardless of the messaging client, if **OPTIONS** is enabled, ensure the dialog box is read thoroughly to provide the most appropriate information to AXIOM Process for proper decryption. When more than one password, email address or other data is given, each entry will need to be provided on a separate line as shown in Figure 11.28.

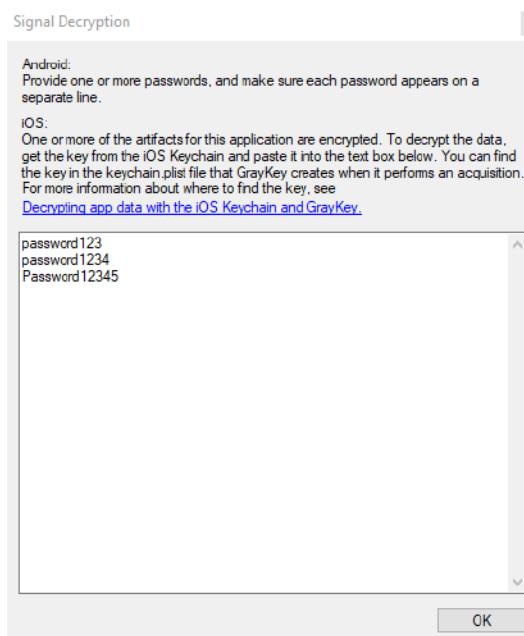


Figure 11.28 Decrypting Signal messages using a password within the artifact options

Use of the Magnet Forensics free program AXIOM Wordlist Generator and the IDENTIFIERS artifact category in AXIOM can help you discover the email addresses and passwords for an application like Signal. If the application is installed on a device, but the data was not parsed due to encryption, use the data obtained from these two resources to process the case again only with the desired artifact selected.

MAGNET.AI – CATEGORIZE CHATS

AXIOM uses Magnet.AI capabilities when searching chat artifacts to analyze the content for possible evidence of enticement or sex-related content. Magnet.AI technology attempts to identify chat content where activities such as grooming, luring, sex-related conversations, enticement, etc., may be occurring. Possible grooming/luring content or Possible sex-related content are the default naming tags, which can be modified by the examiner. To review the artifacts associated with the categorization, these tags are available from the Tags and comments drop-down of the FILTERS bar. A hyperlink to the tagged chats is available from the MAGNET.AI CATEGORIZATION card under PLACES TO START on the Case Dashboard explorer.

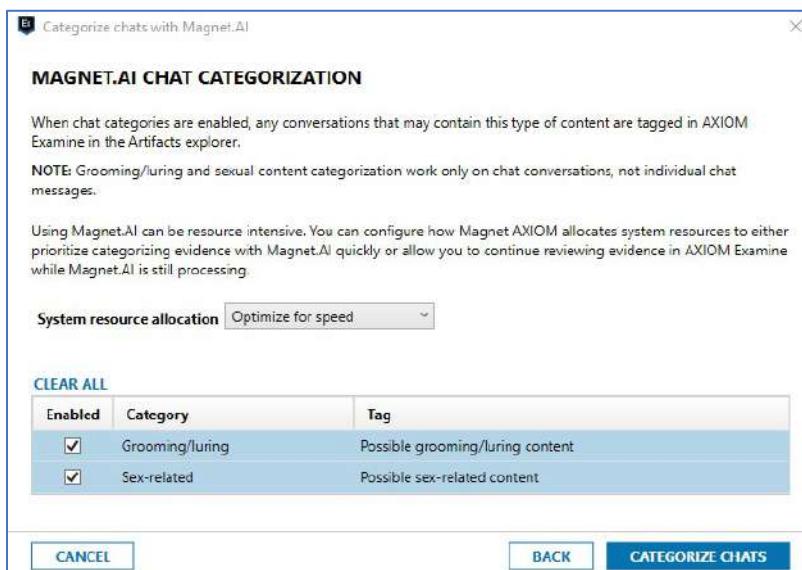


Figure 11.29 Magnet.AI chat categorization

RUNNING EXERCISE

ENABLING MAGNET.AI

- In AXIOM Examine, select the menu option Process → Categorize chats.
- Select which chats you want to categorize.

- Click **NEXT**.
- Select which categories of content you want Magnet.AI to search for. To change the name of a tag, click the default label, type a new name, and then click **UPDATE**.
- Click **CATEGORIZE CHATS**.

COMMUNICATION ARTIFACTS

When the Artifacts explorer is selected in AXIOM Examine, the COMMUNICATION category will display the total number of chat-related artifacts recovered during the creation of the case, based on the user's configuration settings in AXIOM Process and the presence of recoverable artifacts within the evidence. Expanding the COMMUNICATION category will display all the subcategories, organized by client name, with application-specific artifacts including call logs and contacts. The artifact subcategories that appear are based on the format the various clients store data on the devices, and whether artifacts within the various categories are recoverable by AXIOM from allocated and unallocated space. Chat client artifact categories may include local user screen name, profile information, contact lists, messages exchanged, phone calls, and file transfers or Internet Protocol (IP) addresses.

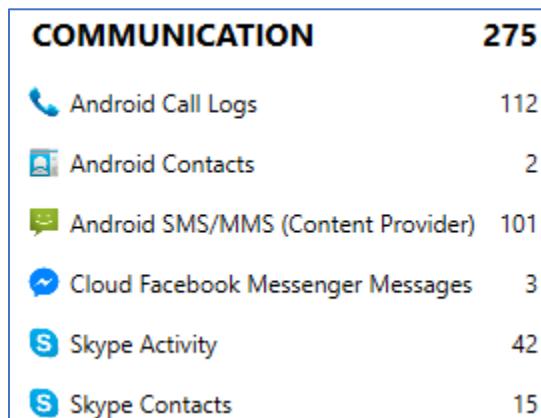


Figure 11.30 COMMUNICATION artifacts

By default, the artifact listed within the various COMMUNICATION categories will be displayed from all evidence sources simultaneously. If a case includes PC and mobile evidence the COMMUNICATION category and subcategories for each client will be a combination of PC and mobile results.

To limit the view to COMMUNICATION artifacts from either the PC, or mobile evidence, select the desired evidence item from the Evidence drop-down menu of the FILTERS bar. After making the selection, AXIOM Examine will only display the artifacts associated with the checked evidence.



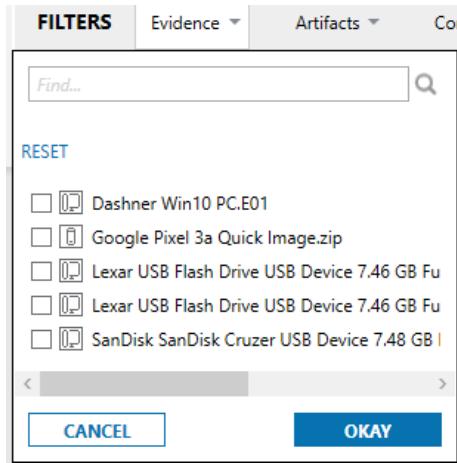


Figure 11.31 Filtering by evidence source

AXIOM Examine enables the user to explore the messenger-related artifacts, using either the Artifacts or File system explorers in the NAVIGATION pane. The Artifacts explorer is the default view providing a breakdown of the messenger clients and their associated categories. Selecting the category within the NAVIGATION pane will display its contents in the EVIDENCE pane.

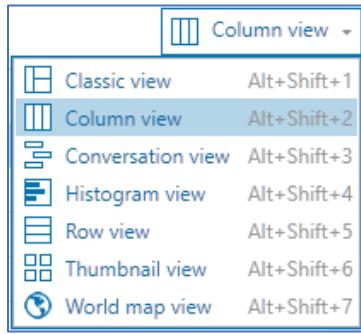


Figure 11.32 EVIDENCE pane view options

The default view for the EVIDENCE pane is the Column view, but the user can configure the default view in the Tools → Settings menus of AXIOM Examine to Column view, Classic view, or Row view. The view within the EVIDENCE pane can also be changed at any time using the drop-down menu in the upper right corner of the EVIDENCE pane. The viewing options available are Classic view, Column view, Conversation view, Histogram view, Row view, Thumbnail view, and World map view. Each of these viewing options offers a unique way of allowing the user to interact with the COMMUNICATION artifacts within the EVIDENCE pane, based on the examiner's investigative needs.

ARTIFACTS – ROW VIEW

Another useful view for examining chat artifacts is the Row view, also available from the EVIDENCE pane drop-down menu. In this view, the details of the selected artifact category are displayed in a format that's

easily presented to a non-technical stakeholder in the investigation and can also provide the examiner with a quick overview of the artifacts in each category. When a user selects individual or multiple artifacts from the Row view, the **CREATE REPORT / EXPORT** option allows the selected artifacts to be exported from the case. The Export type drop-down menu lets the user identify the format for the exported artifact(s). When a single artifact is selected from Row view, the **OPEN SOURCE FILE WITH...** option allows for an external application to open the source file containing the selected artifact.

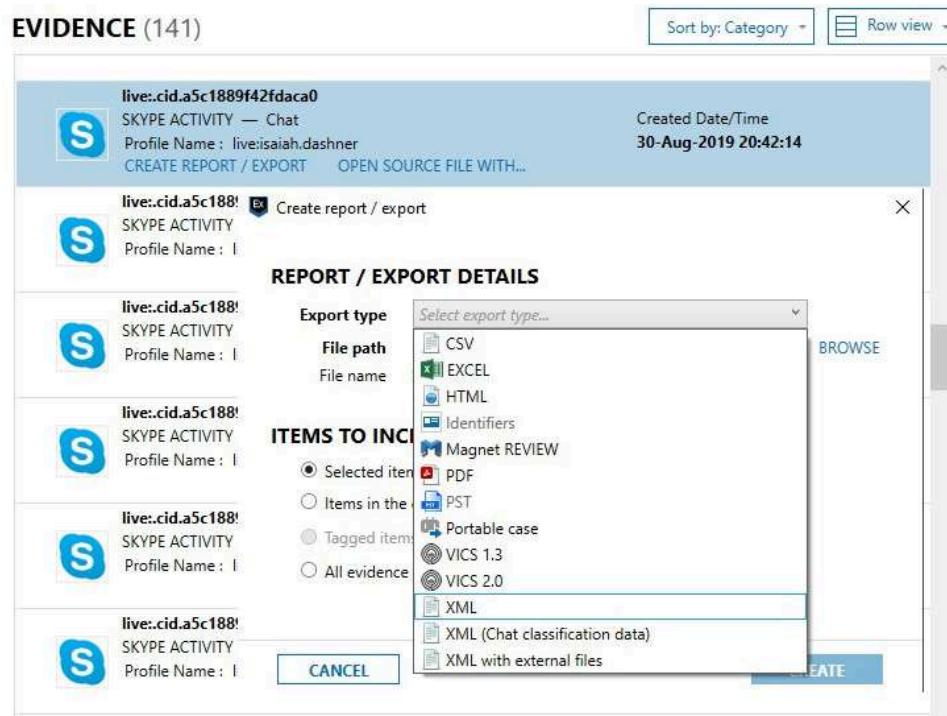


Figure 11.33 Row view for communication artifacts

Artifacts can also be tagged from within the EVIDENCE pane, in the Row view, by right-clicking on the artifact and selecting Add / remove Tag. For chat client message artifacts, the Row view will display basic information for each of the individual message thread, while the Conversation view reconstructs the entire conversation.

ARTIFACTS – CONVERSATION VIEW

The Conversation view in the EVIDENCE pane, is another extremely useful feature when examining chat messages and their relevance to an investigation. AXIOM reconstructs the chat conversations from clients, using individual message threads parsed from the chat client artifacts of both allocated and unallocated space. The rethreaded conversations are displayed in the EVIDENCE pane; each thread can be expanded to view the individual posts within the thread. When an individual post is selected, it will also be highlighted in the PREVIEW card of the DETAILS pane to provide context.

The screenshot shows the AXIOM Examine interface. On the left, there's a list of conversations under 'Conversation view'. One conversation is expanded, showing messages from '+17755991240, Local User <Dashner Win10 PC.E01>' and '+18652323212, Local User <Dashner Win10 PC.E01>'. The messages include text like 'Hey it's Jeff trying again think I had the wrong number before...what...', file attachments (User sent image (jpeg)), and timestamps (e.g., 29-Aug-2019 22:59:48). To the right, a 'PREVIEW' pane shows a message from '+18652323212' with the text 'Hey it's Jeff trying again think I had the wrong number before...what's up freak.' and a blue box indicating 'User sent image (jpeg)'.

Figure 11.34 Conversation view

The entire conversation thread or individual posts can be exported using the right-click, Create report / export to formats listed. A conversation can also be assigned to a pre-existing tag, or a new tag can be created from the TAGS, PROFILES & MEDIA CATEGORIES pane of AXIOM Examine, and applied to the selected conversation. A tag applied to a thread or individual post in Conversation view will also display in Column view.

This screenshot shows the same AXIOM interface as Figure 11.34. A context menu is open over the second conversation in the list. The menu options are 'Create report / export' (which is highlighted with a red box) and 'Add / remove tag'. The conversation list includes three entries: one with 37 messages from 29-Oct-2019 19:50:45, one with 3 messages from 10-Sep-2019 15:59:17, and one with 1 message from 29-Aug-2019 15:14:43.

Figure 11.35 Conversation view, create report / export

The Chat Threading of AXIOM is done once the processing is completed by AXIOM Process. If an examiner is previewing data while it is still being processed, they will not see any of the threaded chats until the job completes. This job will only begin running after all the loaded data has completed processing.

ARTIFACTS – SOURCE LINKING

As presented in earlier modules, the Source Linking feature of AXIOM Examine enables the user to quickly locate the source of an artifact in either the File system or Registry Explorer of the NAVIGATION pane. For COMMUNICATION artifacts, this feature can be particularly useful when examiners need to locate an artifact parsed from an SQLite database table. When a chat thread entry within the EVIDENCE pane is selected, the contents are displayed in the DETAILS pane. Within the DETAILS card are two important fields

for the examiner, the Source and Location fields. If selected, each field will take the examiner to either the source, or the location of the data within the evidence source.

SKYPE

Within the ever-expanding digital ecosystem examiners must navigate, there are hundreds of instant messaging (chat) clients. Each client offers its own unique set of features for the user and poses an equally unique set of challenges for the examiner attempting to recover evidence in support of their case. Among the available Windows chat clients, Skype is one of the most popular. The architecture used by Skype has been modified several times over the years, causing artifacts from various Skype versions to be stored differently. As such, presentation of Skype artifacts within AXIOM may different between versions.

While each chat artifact set may be different, it will be common for the program or application to store not only the message activity, but also potentially the contacts. These will be separated into different artifacts for review within the CHAT section.

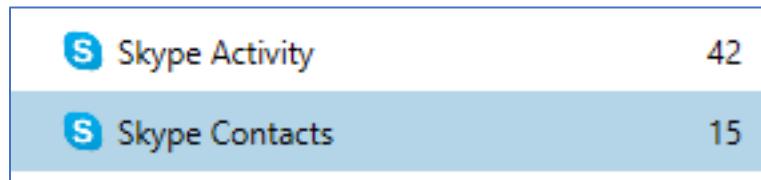


Figure 11.36 Skype artifacts

Within the Skype Contacts artifact, AXIOM will recover and display all the saved contacts from within the SQLite database responsible for storing this data. While each application may keep different information within its contact artifact, Skype will keep a listing of the local user's Profile Name, the contact's Skype name, display name, and other information about the user such as their gender, email address, other phone number, and potentially when the profile was loaded. This information will be used to identify and track users within the kept messages, activities, or calls from the other part of this application.

Profile Na...	Skype Name	Full Name	Display Name	Is Blo...	Contact Added
live:isaiah.dashner	live:.cid.a5c1889f42fdaca0	Jason Smithers	Jason Smithers	No	Yes
live:isaiah.dashner	live:monicaneff4		live:monicaneff4	No	Yes
live:isaiah.dashner	luthorfelix	Luthor Felix	Luthor Felix	No	Yes
live:isaiah.dashner	live:giddletheriddle		live:giddletheriddle	No	Yes
live:isaiah.dashner	concierge	Skype	Skype	No	Yes
live:isaiah.dashner	echo123	Echo / Sound Test Service	Echo / Sound Test Service	No	Yes
live:isaiah.dashner	+13048405011		george	No	Yes
live:isaiah.dashner	live:.cid.5a0356233a02f82c	Wilfy Grunsell	Wilfy Grunsell	No	Yes

Figure 11.37 Skype contacts

In the case of newer Skype IDs that were created after Microsoft’s shift to “Microsoft IDs” or “Live Accounts”, they Skype ID will have the prefix “live:”. It is important to note that the “live:” portion is NOT part of the username, but simply how the data is recorded within Skype’s database. In the case of some other usernames, it may contain a Windows UID or Internet User ID.

Skype’s chat and call activity in newer versions of Skype for Windows 10 is parsed by the Skype Activity artifact recovered by Magnet AXIOM. This singular artifact will record both the messages exchanged with users as well as the duration of calls that were placed. If files were transmitted, the information about the files will be included in this artifact as well.

Sender	Message	Created Date/...	Recipient(s)	Message Type
live:isaiah.dashner	Still up to the same tricks?	29-Aug-19 3:14:43 PM	luthorfelix	RichText
live:.cid.a5c1889f42fdaca0	got any more	30-Aug-19 6:52:33 PM	live:isaiah.dashner	RichText
live:isaiah.dashner	Try this	30-Aug-19 6:51:29 PM	live:.cid.a5c1889f42fdaca0	RichText
live:isaiah.dashner	live:isaiah.dashner shared Golden puppies....	30-Aug-19 6:51:29 PM	live:.cid.a5c1889f42fdaca0	RichText/Media_GenericFile

Figure 11.38 Reviewing Skype messages

If there are multiple participants involved in the chat or call, this information will be reflected within the Recipient(s) and Conversation ID columns. Using the Message Type column allows an examiner to filter through the different types of messages recovered. Some examples would include:

- RichText – A message of text. This could include Emojis and Stickers and may also reflect ‘Text’ in the type.
- RichText/Media_Album – The sharing of a media album via chat.

- RichText/Generic_File – The sharing of generic files such as PDF, Archives, and more.
- RichText/UriObject – The sharing of pictures or links.
- Event/Calls – Calls between users.
- ThreadActivity – Group activity like adding a member or changing channel settings.

Recipient(s)	Message Type	File Name
live:isaiah.dashner	RichText/UriObject	Funny Jack.JPG
live:.cid.a5c1889f42fdaca0	RichText/UriObject	animal-beagle-canine-460823.jpg
live:.cid.a5c1889f42fdaca0	RichText/UriObject	adorable-animal-breed-1108099.jpg
live:.cid.a5c1889f42fdaca0	RichText/Media_GenericFile	Golden puppies.pdf
live:.cid.5a0356233a02f82c	RichText/Media_GenericFile	Videos.7z
live:.cid.a5c1889f42fdaca0	RichText/Media_Album	
live:.cid.a5c1889f42fdaca0	RichText/Media_Album	
luthorfelix	RichText	

Figure 11.39 Sorting by Message Type in Skype

WINDOWS YOUR PHONE

Syncing data across multiple devices is a rapidly expanding function for many platforms. In Windows 10, Microsoft introduced “Your Phone” as a means for users to share data between mobile devices and Windows PCs. This has given examiners an opportunity to examine mobile data on a Windows PC that may or may not still reside on the originating device.

In this module, we will explore Your Phone artifacts that were native to a Google Pixel 3a phone. Specifically, artifacts from Your Phone Contacts, Your Phone Devices and Your Phone SMS/MMS will be explored.



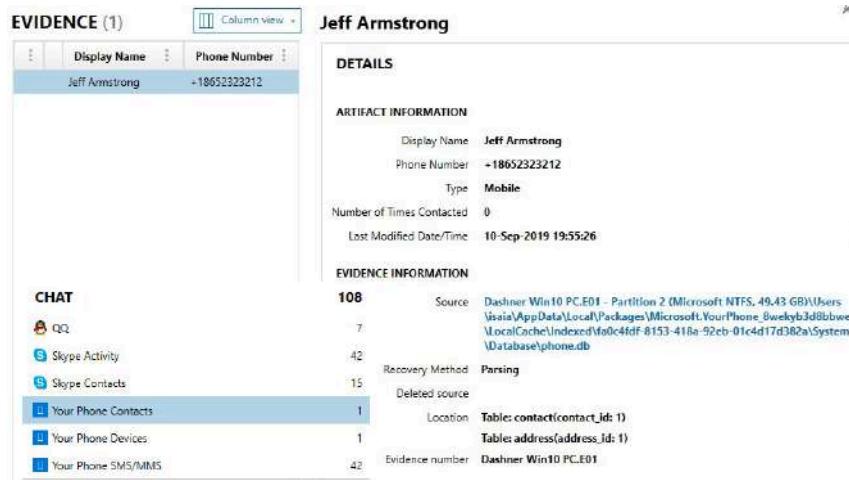


Figure 11.40 Windows Your Phone

AXIOM parses many of the Your Phone artifact categories from the **phone.db** file, which is located within the **Modern Application** folder for Your Phone. The **phone.db** file is a SQLite database, composed of tables which store data such as the user's contacts in the contact and address tables and messages in the message table.

The Your Phone Contacts artifacts are parsed from the **contact** and **address** tables of the **phone.db** file. These tables store data synced with a mobile device and the data contained within may vary depending on the version of the mobile device operating system and syncing options. The column view of the EVIDENCE pane, and the DETAILS card of the DETAILS pane will list data from these tables. Evidentiary items from the table(s) can include the contact's Display Name, Phone Number, Type of Phone Number and the last time the contact was modified. Two additional details about the contact (Number of Time Contacted and Last Time Contacted) are representative of data since the Your Phone application was installed or configured and do not indicate instances prior to such.

YOUR PHONE SMS/MMS

The CONNECTED DEVICES → Your Phone SMS/MMS artifacts are parsed from the **message** table of the **phone.db** database. Using the source linking functionality of Examine, a user can follow the link to the **phone.db** file and use the File system explorer within the NAVIGATION pane to explore the table structure, and values within the **phone.db** database much like the previous example for the contact and address tables in the same database.

The screenshot shows a file system view on the left with several database files listed, including notifications.db, notifications.db-shm, notifications.db-wal, phone.db, phone.db-shm, phone.db-wal, photos.db, photos.db-shm, photos.db-wal, settings.db, settings.db-shm, and settings.db-wal. To the right, the SQLite Viewer interface is open, displaying the 'message' table. The table has columns: #, message_id, thread_id, status, from_address, type, subject, body, and timestamp. The data shows various messages with their details and timestamps.

#	message_id	thread_id	status	from_address	type	subject	body	timestamp
12	16	14	2	+18652323212	1		Oh yeah I'll have some original stuff for u soon	13211601
13	18	14	2	+18652323212	1		Whos motherload keep em coming	13211654
14	19	14	2	+18652323212	1		Oh you talking a hand to hand to keep off the radar? I get down that way sometimes and would be inter...	13211654
15	26	14	2	+18652323212	1		Well count me in trying to get you some original stuff	13211654
16	28	14	2	+18652323212	1		Is he cool	13211665
17	29	14	2	+18652323212	1		He gonna share... That what u mean	13211665
18	30	14	2	+18652323212	1		Wait what's his name?	13211666
19	35	14	2	+18652323212	1		Oh I know that dude he's solid	13211666
20	36	14	2	+18652323212	1		Yeah it's good	13211666
21	37	14	2	+18652323212	1		But freaky deaky	13211667
22	40	14	2	+18652323212	1		Ok let me know oohl puppy	13211936
23	41	14	2	+18652323212	1		Lol to pppptppp usu	13211936
24	42	14	2	+18652323212	1		Pypop I speak on to you	13211936
70	44	16	2	+17755351297	1		Damian you are able to see all the pictures you want now.	13211936

Figure 11.41 Your Phone phone.db database

Within the **message** table, Your Phone stores several fields including the author (sender) of the message, the status of the message (read/unread), the type of message (SMS/MMS), the timestamp of the message, the direction of the message (sent / received) and the body of the message.

The id values are used to link associated messages to conversation threads. The **thread_id** value links the **message** table to the **conversation** table, to help identify the other party with whom the chat message occurred as seen in Figure 11.42.

The screenshot shows the SQLite Viewer interface with the 'conversation' table selected. The table has columns: #, thread_id, recipient_list, and timestamp. The data shows various conversations with their timestamps.

#	thread_id	recipient_list	timestamp
1	5	7759423174	132104310320560000
2	6	+13613214034	132105856843360000
3	7	47543	132105868121870000
4	8	+19563046997	132106968163380000
5	9	+14017154990	132113908277120000
6	10	+17755351299	132113908290580000
7	11	+17757992976	132113908306170000

Figure 11.42 Conversation table linking to the message table

In order to manually review the photos that are cached locally that were sent/received as part of Your Phone, locate the **photos.db** file that is stored in the same path as the previously covered **phone.db**. To find this file use the File System explorer to navigate to the path:

`Users\isaia\AppData\Local\Packages\Microsoft.YourPhone_8wekyb3d8bbwe\LocalCache\Index ed\fa0c4fdf-8153-418a-92eb-01c4d17d382a\System\Database\`



Within the photo table of this database, a listing of all the cached photos will be available. This table will store the name of the photo, the time the photo was last updated, the size, a storage path of where it came from on the synced device, and a thumbnail and full-size image.

SQLITE VIEWER

Select table **photo**

FIND BUILD QUERY EXPORT

#	photo_id	name	last_updated_time	size	uri	thumbnail	blob
1	1	IMG_20...	132114073160000000	918558	file:///storage/emulated/0/DCIM/Camera/IMG_20190827_142153.jpg	?????ExifMM*	????Exif...
2	3	IMG_20...	132114041130000000	997342	file:///storage/emulated/0/DCIM/Camera/IMG_20190827_132831.jpg	?????ExifMM*	????Exif...
3	4	IMG_20...	132114028380000000	965631	file:///storage/emulated/0/DCIM/Camera/IMG_20190827_130715.jpg	?????ExifMM*	????Exif...

Figure 11.43 Reviewing the photo table

In order to have this table make more sense to the examiner, some of the listed columns can be reflected differently. By right-clicking on columns there are several options to transform the display of the data depending upon what is in there. For example, the **last_updated_time** column can be changed to Windows file time.

The screenshot shows a table with a context menu open over the 'last_updated_time' column. The menu includes options like Date / time, Unix time, ASCII, Base64 decoded hex, Base64 decoded text, Hex, Unicode, URL encoded, URL decoded, Booleans, Picture, and Reset. The 'Windows file time' option is highlighted.

last_updated_time	size	uri	thumbnail
13211...	Date / time	Unix time	
13211...	ASCII	Unix time (milliseconds)	?ExifMM*
13211...	Base64 decoded hex	Unix time (microseconds)	
13211...	Base64 decoded text	Apple time	?ExifMM*
13211...	Hex	macOS time (HFS+)	
13211...	Unicode	macOS time (APFS)	?ExifMM*
13211...	URL encoded	Google Chrome time	
13211...	URL decoded	Windows file time	
13211...	Booleans	M/Camera/_20190827_130712.jpg	?????ExifMM*
13211...	Picture	file:///storage/emulated/0/M/...	
13211...	Reset	IMG_20190827_130708.ipa	?????ExifMM*

Figure 11.44 Converting timestamps

By right-clicking the thumbnail and blob columns, these columns can be adjusted to display the picture stored within the blob (Binary Large Object) data. After changing both columns to reflect the Picture setting, the data will look like the following:

SQLITE VIEWER

Select table ▾

FIND BUILD QUERY EXPORT

#	photo_id	name	last_updated_time	size	uri	thumbnail	blob
1	1	IMG_20...	27-Aug-19 7:21:56 PM	918558	file:///storage/emulated/0/DCIM/Camera/IMG_20190827_142153.jpg		

Figure 11.45 Displaying BLOB data as an image

It is also possible to right click each photograph in order to save the photo out directly, view it within AXIOM's picture viewer, or open it with a different tool.

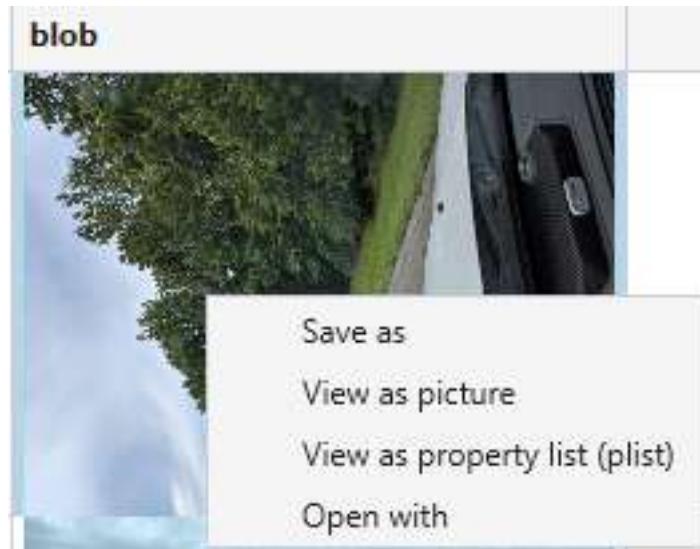


Figure 11.46 Right-clicking a photo within a SQLite database

RUNNING EXERCISE

YOUR PHONE SMS/MMS

- From the **Artifacts** explorer in **AXIOM Examine**, clear any filters you may have applied.
- Select the CONNECTED DEVICES → Your Phone SMS/MMS artifact category and view the artifacts in the **Conversation** view
- Locate the conversation dated September 2, 2019 and expand the messages.
- Click the **Source** link for the location of the **phone.db** file, to view the artifacts in the File system explorer.
- Select the **message** table from the drop-down in the SQLITE VIEWER. Review the records for **message_id: 14** to see the data shown in the message from the Artifacts explorer.
- Note the numeric value in the column **thread_id** (14). This is the ID value for the conversation and could be used to find the related data in the **conversation** table.
- Select the **mms_part** table from the drop-down in the SQLITE VIEWER. Review the records for **message_id: 14**. Note the data contained in the various fields of this table, paying particular attention to the **blob** and **size** fields. Right-click on the data in the **blob** field for message_id: 14 and choose **View as picture** from the menu.
- Return to the **Artifacts** explorer. The conversation will still be selected in the **Evidence** pane.

REVIEW QUESTIONS

To help reinforce the learning objectives for this module, the following review questions have been provided:

1. Name two different types of information that may be entered in the **OPTIONS** in AXIOM Process to help decrypt CHAT data.
2. What free Magnet AXIOM tool can help you discover user information to gain access to otherwise encrypted data?
3. What two Magnet.AI features can be enabled for searching chat artifacts?
4. What is the name of the view in the Artifacts explorer that displays chat messages in a threaded format?
5. What is the name of the Your Phone database that provides most of the artifacts in AXIOM?
6. What built in AXIOM tool is available in the File system explorer to assist with viewing databases?



STUDENT EXERCISE

- From the **Artifacts** explorer in **AXIOM Examine**, clear any filters you may have applied.
- From the **Evidence** drop-down menu on the **Filters** bar, select the item, **Google Pixel 3a Quick Image.zip** and answer the following questions.
- What is the Google Account that appears to be associated with Isaiah Dashner on this device?

- What is the phone number for this device? _____
- What contacts has Isaiah Dashner saved into his contacts?

- Is there any evidence of images having been shared between Dashner and Jeff Armstrong?

- Look for the Videos that have timestamps for 18-Aug-19. Is there location data for these videos?

- What country were these videos taken in? _____ (Hint: Use **World Map View** in the **Evidence** pane)
- According to geo-location data, what states within the United States were there photos on the device?

- From the **Artifacts** explorer in **AXIOM Examine**, clear any filters you may have applied.
- Review the **CONNECTED DEVICES** → **Your Phone SMS/MMS messages** artifact category.

What cloud storage service is being discussed? _____

What is the thread_id from the database of the conversation containing this information?
 (Hint: note the Location information for the message and review the thread_id field in the associated SQLite database table.)

- How many times is the word “puppy” mentioned in CHAT artifacts?
 (Hint – Filter for COMMUNICATION artifacts – use search box on Filters bar)

What is the phone number of the sender? _____

- Tag these results with “Puppy Chat”.
- Using the Skype Activity artifact, who sent the file “Golden Puppies.pdf”? _____
- What is the Skype Name of the user who received this file? _____
- Using the Skype Contacts artifact, what was this user’s Display Name? _____
- Using the Your Phone SMS/MMS artifact, was there evidence of files being sent or received?

- Using the Your Phone Devices artifact, what kind of device was Dashner using?

Dashner Win10 PC.E01\Partition 2\

Users\isaia\AppData\Local\Packages\Microsoft.YourPhone_8wekyb3d8bbwe\LocalCache\Indexed\fa0c4fdf-8153-418a-92eb-01c4d17d382a\System\Database\.

- Select the **photos.db** file, and from within the SQLITE VIEWER in the DETAILS pane select the **photo** table. Converting the blob column to show the picture, what is depicted in the photo matching **photo_id 155**? _____
- Converting the last_updated_time column to Windows file time, what is the time and date listed for **photo_id 155**? _____



Notes





MAGNET
FORENSICS®

MODULE 12:

Cloud

LEARNING OBJECTIVES

In this lesson, students will take part in lecture, instructor-led exercises, and student practical exercises to gain an understanding of AXIOM Cloud. Students will learn how it can assist in an investigation, how to acquire data from the cloud, and learn some of the information/data that can be collected.

GOALS

At the conclusion of this lesson, students will be able to discuss the circumstances when acquiring cloud data should be considered, how to obtain data from the cloud, and how to add this acquired cloud evidence to a case for review in AXIOM Examine.

WHAT IS THE CLOUD?



There is no cloud
it's just someone else's computer

Figure 12.1 There is no cloud

While the cloud sounds mysterious, examiners should understand that it's not very mysterious at all. Data coming from the cloud simply refers to information that is coming from server-stored locations as opposed to data stored on a local device. As many like to joke, "There is no cloud, it's just someone else's computer".

One of the fastest growing sources of data in forensic examinations is not on locally acquirable devices, but rather data stored on cloud servers. While there are several litigation issues around these acquisition methods that can impact your ability to acquire the data, even in consent cases alone the data available to an examiner can justify the use of cloud acquisitions. Many cloud storage providers offer free storage and not collecting this evidence would be the same as an examiner ignoring gigabytes, or even terabytes of evidential data. As more devices begin to rely on cloud data, along with high speed mobile connectivity on 4G and 5G networks, cloud data can no longer be ignored.

At the time of writing AXIOM has a specialized module that can be used to acquire and analyze data from cloud platforms including:

- Apple
- AWS
- Azure
- Box

- Dropbox
- Facebook
- Google
- IMAP / POP email
- Instagram
- Lyft
- Mega
- Microsoft / Office 365 / One Drive
- Microsoft Teams
- Slack
- Twitter
- Uber
- WhatsApp

Undoubtedly, the number of cloud platforms will increase as more become available and adopted for use at both personal and corporate level. For example, due to recent changes in the General Data Protection Requirement (GDPR), many providers have begun allowing users to download their own data. As services comply with this requirement, AXIOM will evolve to support those services, e.g. Snapchat, TikTok, etc.

There are data points available from these acquisition sources that may not be available from any physical device, and if required for review during an investigation this information may only be available from the cloud. By combining the data from the cloud with data stored locally, missing pieces of the puzzle could be uncovered. The use of the AXIOM Connections Module can help reveal the relevance of this type of data.

It should be noted that none of the methods employed by AXIOM to obtain cloud data should be considered as covert; traces will be left. Emails may be sent to the account holder to show that access has been given to “Magnet Forensics Inc”, just as you would expect if a user signed on from a new device or browser. User accounts and passwords, in most cases, will still be required to access cloud data and there may be issues with two-factor or multi-factor authentication (2FA).

ACQUIRING DATA WITH AXIOM CLOUD

To acquire data from these cloud sources using AXIOM Cloud, an examiner must have the correct license installed which will enable the option to select CLOUD from the evidence source selection screen.

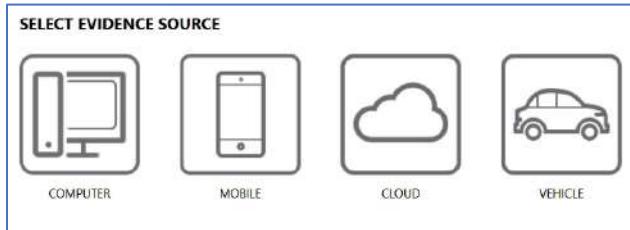


Figure 12.2 Select CLOUD from EVIDENCE SOURCES

After selecting the CLOUD option, the examiner is then given the choice of either acquiring new evidence or loading previously acquired data.



Figure 12.3 ACQUIRE or LOAD Cloud Evidence

If the examiner selects ACQUIRE EVIDENCE, a prompt is displayed asking them for confirmation that they have proper legal authority to use these acquisition techniques. This acts as an important reminder to the examiner to ensure they have proper authority from their area before using this option, as laws and procedures differ widely between regions.

EVIDENCE SOURCES	
CLOUD	
SELECT EVIDENCE SOURCE	
<input type="checkbox"/> I have proper search authorization to access the target's information stored in the cloud.	

Figure 12.4 Authorization to access cloud evidence

Once the examiner confirms that proper authority exists by checking the box, the available cloud platforms are then displayed. When a platform is selected the examiner can choose services and options specific to that platform.

The LOAD EVIDENCE option in Figure 12.3 ACQUIRE or LOAD Cloud Evidence allows the examiner to add data previously acquired using AXIOM Cloud. They can also add data from other sources such as Google Takeout, Facebook Download My Data, or Apple Warrant Returns.

When the **LOAD EVIDENCE** option is selected the examiner then chooses from the following options:

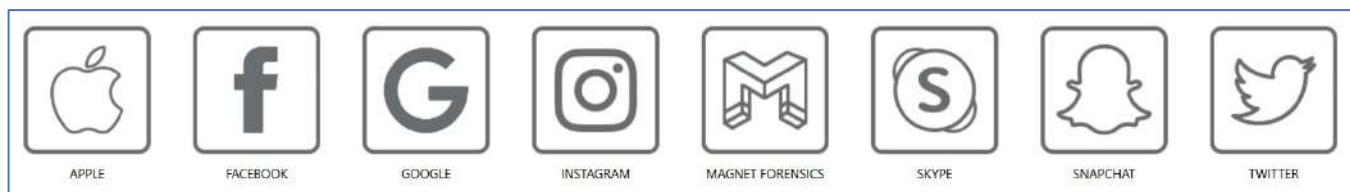


Figure 12.5 Sample of platform selection screen for loading cloud evidence

When the evidence has been obtained using Magnet AXIOM software, select the MAGNET FORENSICS option. This will take the examiner to this screen:



Figure 12.6 Platform selection screen for loading Cloud Evidence obtained by AXIOM

It will then be necessary to find the downloaded file location of the data and select it to be ingested into AXIOM. Because not every agency will have their forensic computers on an open network, it is possible to acquire the data on a separate machine and then ingest that cloud data into an AXIOM case that has already been processed containing the local evidence items such as Windows, macOS, iOS, or Android.

Where the data has been obtained directly from the site or provider, i.e. Google Takeout, Facebook – Download My Data, or as the result of a warrant return, then the appropriate platform as shown in Figure 12.7 should be used.



Figure 12.7 Platform selection screen for loading Cloud Evidence obtained from the service provider or as a result of a Warrant Return.

Remember, if it has been downloaded directly by Magnet AXIOM software, the examiner would use the MAGNET AXIOM as in Figure 12.17

Use of several of these cloud platforms was identified during the Dashner case scenario exercises so far. The next step is to establish if there is cloud data present and if so, should it and can it be acquired? Any additional information obtained from the cloud could help connect more of the data that we already have.

Once a platform is selected, the user is prompted to enter either the account credentials, such as username and password, or use a previously acquired token.



Figure 12.8 Providing credentials to access the cloud platform

TOKENS

While the data can be accessed by entering the username and password combination of the account, this information may not necessarily be available to an examiner. Instead it may be possible to use information in the form of a digital key stored on one of the local devices already in possession of the

examiner, such as a mobile device. A token is part of a procedure known as Token Based Authentication where a service will generate a key that can be used to re-authenticate to a service without the user constantly needing to enter their credentials over and over within the same session. These tokens are not permanent; they can last for extended periods of time or for only a few minutes depending on the service. The other benefit of using tokens is that it does not need two-factor authentication (2FA), nor does it rely on security checks that could alert the end user when someone is accessing their data. They are used on the basis that the user has already been authenticated by another trusted service. It is worth reiterating this method is NOT to be considered as covert as other traces may be left.

The token for each platform or service will differ in length, structure, and ability. Some tokens only provide access to certain parts of a service and not the entire authentication model, whereas others provide access to all the user's stored content within that platform. Additionally, each token is generated by that specific platform or service and how and where they choose to store it may differ. Most commonly, tokens can be recovered from an Android's **accounts.db** file or the iOS/macOS **Keychain**.

FACEBOOK

The incredibly popular social media platform Facebook is available as a cloud service from which AXIOM Process can acquire data. To authenticate to the Facebook platform, the user's account credentials or a previously acquired token are needed. When using credentials, AXIOM Cloud will open a webpage pop-up displaying the Facebook login page for the examiner to enter the username and password information. Once authenticated, all the available services from Facebook are displayed.

SELECT SERVICES AND CONTENT					
Select the services and level of content that you want to acquire from the cloud. By default, AXIOM Process will acquire all available content for the user who is signed in.					
CLEAR ALL					
SERVICE	DATE RANGE	LAST ACTIVITY (UTC)	ACCOUNT SIZE	CONTENT	
<input checked="" type="checkbox"/> Facebook Profile Info	All dates	Not available	Not available	All content from signed-in user	
<input checked="" type="checkbox"/> Facebook Messenger Messages	All dates	Not available	Not available	All content from signed-in user	
<input checked="" type="checkbox"/> Facebook Timeline	All dates	Not available	Not available	All content from signed-in user	
<input checked="" type="checkbox"/> Facebook Friends	All dates	Not available	Not available	All content from signed-in user	

Figure 12.9 Services available for acquisition from the FACEBOOK platform

None of the Facebook services have editable options but each of the services can be enabled or disabled depending upon the scope of the investigation. The Facebook acquisitions are widely based on scraping the available web data. This can take a long time depending upon how much information is being stored.

Messenger Messages and Friends can take several hours depending on how many messages are being stored and to how many friends the user is connected.

DROPBOX

The Dropbox remote storage platform has over 700 million users worldwide. It is also seen in many child exploitation and data exfiltration cases as a popular way to remotely hide, store, and share data between individuals and computers. After selecting the DROPBOX platform and authenticating to the account using either the account credentials or a previously acquired token, AXIOM Cloud displays a service for the Cloud Dropbox Files of the account. The service also details the date of the LAST ACTIVITY on the account and the current ACCOUNT SIZE.

INSTRUCTOR-LED DEMONSTRATION - DROPBOX

- Open AXIOM PROCESS and Create a New Case – Call it DASHNER DROPBOX

CASE DETAILS	
CASE INFORMATION	
Case number	<input type="text" value="DASHNER DROPBOX"/>
Case type	<input type="text" value="Select case type..."/>
LOCATION FOR CASE FILES	
Folder name	<input type="text" value="DASHNER DROPBOX"/>
File path	<input type="text" value="C:\"/> BROWSE
Available space: 36.93 GB	
LOCATION FOR ACQUIRED EVIDENCE	
Folder name	<input type="text" value="DASHNER DROPBOX"/>
File path	<input type="text" value="C:\"/> BROWSE
Available space: 36.93 GB	

Figure 12.10 Creating a new case

- Then select the GO TO EVIDENCE SOURCES option.
- Select the CLOUD icon and then ACQUIRE EVIDENCE.
- When asked about having proper authorization, select the check box. This will display the cloud options



EVIDENCE SOURCES

CLOUD SELECT EVIDENCE SOURCE

I have proper search authorization to access the target's information stored in the cloud.

Figure 12.11 Cloud acquisition authorization checkbox.

EVIDENCE SOURCES

CLOUD
SELECT EVIDENCE SOURCE

I have proper search authorization to access the target's information stored in the cloud.

To obtain evidence from the cloud, sign in to the account with the target's user name and password or an authentication token. For some cloud platforms, you can also acquire activity that is accessible to the public.

AMAZON APPLE AZURE BOX.COM DROPBOX FACEBOOK GOOGLE IMAP / POP EMAIL

INSTAGRAM LYFT MEGA MICROSOFT MICROSOFT TEAMS SLACK TWITTER UBER

WHATSAPP

Figure 12.12 Available platforms for acquisition

- After selecting the DROPBOX platform, the account needs to be authenticated using either the account credentials, Email and Password, or a previously acquired token. It can be noted that access is requested by Magnet Forensics International Inc. and not the examiners agency / Department.

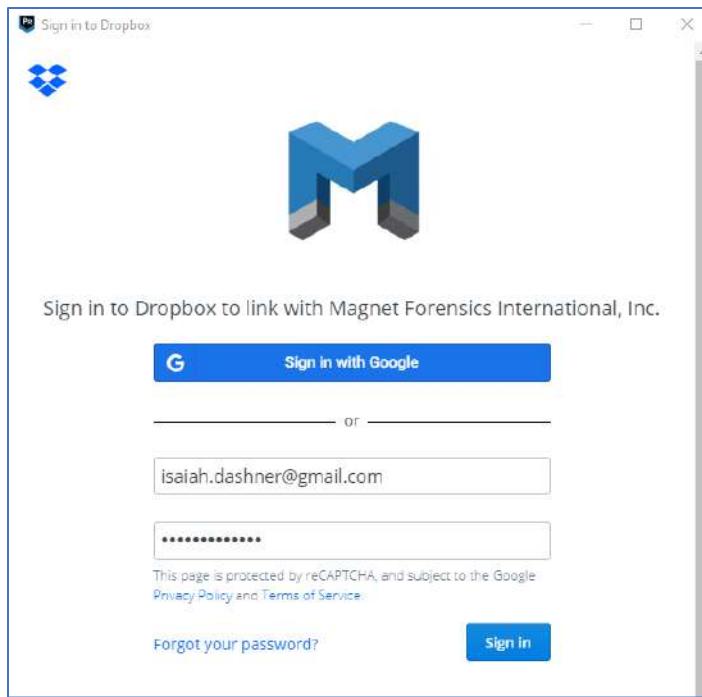


Figure 12.13 Authenticating Magnet Forensics Inc to acquire data.

- AXIOM Cloud displays a service for the Cloud Dropbox Files of the account. The service also details the date of the LAST ACTIVITY on the account and the current ACCOUNT SIZE.

EVIDENCE SOURCES

CLOUD SELECT DROPBOX SERVICES

Platform: Dropbox
User name: isaiah.dashner@gmail.com

SELECT DATE RANGE
Set the period of time that you want to access data from the cloud
Date Range: All dates

SELECT SERVICES AND CONTENT
Select the services and level of content that you want to acquire from the cloud. By default, AXIOM Process will acquire all available content for the user who is signed in.
SELECT ALL

SERVICE	DATE RANGE	LAST ACTIVITY (UTC)	ACCOUNT SIZE	CONTENT
<input type="checkbox"/> Cloud Dropbox Files	All dates	Not available	406.94 MB	No content selected EDIT

Figure 12.14 Setting filters and targeting data within Dropbox

- Selecting **EDIT** within the CONTENT column displays a files and folder selection window as shown in Figure 12.15, that allows the examiner to select which items to acquire from Dropbox.



- This will include files and folders that are contained within a different Dropbox account but are shared with this Dropbox user and those that the user is sharing with others.
- It should also be noted that the folder structure can also be reviewed at this stage for any relevant data.

The screenshot shows the 'EVIDENCE SOURCES' interface in AXIOM. Under the 'CLOUD' tab, the 'ADD FILES AND FOLDERS' section is active. A service icon for 'Cloud Dropbox Files' and the user name 'isaiah.dashner@gmail.com' are displayed. Below this, a list of selected items is shown, each with a checkbox and a small icon:

- My Files (selected)
- Camera Uploads (selected)
- New Friends (selected)
- Fun Docs (selected)
- old flash drive pics (selected)
- Mobile Uploads (selected)
- csi-miami_o_951813.jpg (selected)
- Accounting.ods (selected)
- Drugs List.docx (selected)
- Sharing (selected)

Figure 12.15 Targeting specific data from Dropbox

- This would then Acquire the DROPBOX data into the case.

GOOGLE

The search engine and technology giant, Google, stores an incredible amount of information about its users, most of which can be acquired using AXIOM Cloud. The volume of data stored will depend on the number of Google services used. For example, if the user starts the Chrome browser and signs into Chrome using their Google account, information from that browser, e.g. bookmarks and browsing history, will be synced to the cloud. If the device in use is running an Android operating system there will be additional information about the device and its activities logged by Google.

Google stores a token file on Android devices within the **accounts.db** database file. This token can often be used to access almost all the information stored by Google. Additionally, this token does not seem to

expire for an extended period, so it is a prime example of using a token to access information stored in the cloud.

Once authenticated, the services available for acquisition within the GOOGLE platform are displayed. Several of these services have further customization options. Hover over the service and if additional options are available the **EDIT** button appears within the CONTENT column.

SERVICE	DATE RANGE	LAST ACTIVITY (UTC)	ACCOUNT SIZE	CONTENT
<input checked="" type="checkbox"/>  Google Account	All dates	Not available	Not available	All content from signed-in user EDIT
<input checked="" type="checkbox"/>  Gmail Messages	All dates	Not available	27.65 MB	All content from signed-in user
<input checked="" type="checkbox"/>  Google Drive	All dates	Not available	27.65 MB	All content from signed-in user
<input checked="" type="checkbox"/>  Google Photos	All dates	Not available	0 GB	All content from signed-in user
<input checked="" type="checkbox"/>  Google Hangouts	All dates	Not available	Not available	All content from signed-in user

Figure 12.16 Services available for acquisition from the GOOGLE Platform

Selecting **EDIT** for the Google Account service displays several additional subservices, as shown in Figure 12.17.

SERVICE	DATE RANGE	CONTENT
<input checked="" type="checkbox"/>  Google Activity	All dates	All content from signed-in user
<input checked="" type="checkbox"/>  Google Timeline Locations	All dates	All content from signed-in user
<input checked="" type="checkbox"/>  Google Connected Apps	All dates	All content from signed-in user
<input checked="" type="checkbox"/>  Recent Devices	All dates	All content from signed-in user
<input checked="" type="checkbox"/>  Passwords	All dates	All content from signed-in user

Figure 12.17 Google Account sub services

The Google Account subservices include Google Activity (searches and browsing history), Google Timeline Locations, Google Connected Apps, Recent Devices that have signed into the account, and any saved Passwords stored in the cloud.



Selecting the **EDIT** option for Google Drive launches an ADD FILES AND FOLDERS window to select which areas of the Google Drive should be acquired. The Gmail Messages, Google Photos, and Google Hangouts services do not have any configurable options and selecting these services will acquire all the available content within the service including attachment files for messages and mail.

CLOUD ARTIFACTS

Once each of the platforms to be acquired have been added to the case, AXIOM Process lists them as Ready to image along with the account that will be used to acquire the content.

EVIDENCE SOURCES ADDED TO CASE				
Type	Image - location name	Evidence number	Search type	Status
	Cloud - Google	Google - isaiah.dashner@gmail.com	Full	Ready to image
	Cloud - Apple	Apple - isaiah.dashner@gmail.com	Full	Ready to image
	Cloud - Facebook	Facebook - isaiah.dashner@gmail.com	Full	Ready to image
	Cloud - Dropbox	Dropbox - isaiah.dashner@gmail.com	Full	Ready to image

Figure 12.18 Cloud Platforms Ready to image

As of the writing of this manual, AXIOM can recognize and extract data from over 100 different cloud artifacts.

The screenshot shows a grid of 60+ cloud artifacts supported by AXIOM. The artifacts are categorized into several groups:

- Cloud Accounts:** Cloud Accounts Information, Cloud Amazon EC2 Instances, Cloud Amazon S3 Files, Cloud Azure Virtual Machine Snapshots, Cloud Box.com Enterprise Events, Cloud Box.com Files, Cloud Box.com User Events, Cloud Dropbox Files, Cloud Facebook Friends.
- Cloud Facebook:** Cloud Facebook Messenger Messages, Cloud Facebook Mobile Timeline, Cloud Facebook Profile Info, Cloud Facebook Timeline, Cloud Gmail Messages, Cloud Google Account Information (Warrant Return), Cloud Google Activity, Cloud Google Browsing History (Warrant Return), Cloud Google Calendar Events.
- Cloud Google:** Cloud Google Calendar Events (Takeout), Cloud Google Chats (Warrant Return), Cloud Google Chrome Autofill, Cloud Google Chrome Bookmarks, Cloud Google Chrome Browser History, Cloud Google Chrome Extension Settings, Cloud Google Chrome Extensions, Cloud Google Chrome Search Engines, Cloud Google Chrome Sync Settings - App Settings.
- Cloud Google Sync:** Cloud Google Chrome Sync Settings - Apps, Cloud Google Chrome Sync Settings - Preferences, Cloud Google Connected Apps, Cloud Google Contacts, Cloud Google Devices (Warrant Return), Cloud Google Drive Files, Cloud Google G Suite Drive Audit Events, Cloud Google G Suite Login Audit Events, Cloud Google Hangouts Messages.
- Cloud Google Keep:** Cloud Google Keep.
- Cloud Google Location:** Cloud Google Location.
- Cloud Google Login:** Cloud Google Login History.
- Cloud Google Maps:** Cloud Google Maps Activity.
- Cloud Google Photos:** Cloud Google Photos.
- Cloud Google Recent:** Cloud Google Recent.

Figure 12.19 Some of the CLOUD ARTIFACTS supported by AXIOM Process

Because there are often files stored in cloud services such as photos, videos, documents, and even full backups which could include SMS/MMS data and/or third-party application data, in addition to these 100+ artifacts, AXIOM will also automatically select and search for all computer or mobile across the cloud evidence added to the case.

REVIEWING CLOUD DATA

Once the cloud evidence source is acquired and/or loaded, AXIOM Process will parse and carve the data for artifacts just as for computer and mobile evidence. AXIOM Examine is then used to review the results. Analyzing acquired cloud data in AXIOM Examine is no different to reviewing PC, RAM, or mobile data.

In AXIOM Examine, the cloud specific artifacts are integrated into existing categories but are mostly recognizable through the Cloud prefix.



REFINED RESULTS		7
 Cloud Passwords and Tokens		7
COMMUNICATION		3
 Cloud Facebook Messenger Messages		3
SOCIAL NETWORKING		14
 Cloud Facebook Friends		10
 Cloud Facebook Timeline		4
MEDIA		100
 Cloud Google Photos		100
EMAIL & CALENDAR		440
 Cloud Gmail Messages		440
CLOUD STORAGE		338
 Cloud Dropbox Files		266
 Cloud Google Drive Files		8
 Cloud OneDrive Files		64
APPLICATION USAGE		1,339
 Cloud Google Activity		1,330
 Cloud Google Connected Apps		9
OPERATING SYSTEM		7
 Cloud Accounts Information		7
CONNECTED DEVICES		3
 Cloud Google Recent Devices		3
LOCATION & TRAVEL		96
 Cloud Google Timeline Locations		96

Figure 12.20 An example of cloud data available view for review in AXIOM Examine

CLOUD ACCOUNTS INFORMATION, PASSWORDS, AND TOKENS

AXIOM Cloud captures any username and password account credentials entered and/or any tokens used to gain access to the platform or service. These passwords and tokens are then populated into their own artifact category within AXIOM Examine – Refined Results → Cloud Passwords and Tokens, as shown in figures 12.20 and 12.21. This category contains information from the OPERATING SYSTEM → Cloud Accounts Information category and other sources such as the Android **Accounts.db** file.

If a password was used to log into the account to acquire the data, the Password/Token field displays the password entered. If the examiner accessed the service with a token, the Password/Token field does not display the user's password, but instead displays the content of the token. These password credentials can be useful if an examiner needs to gain access to the account again at a later date to

acquire additional data. Additionally, many people are creatures of habit and use their passwords for multiple accounts and/or files. Therefore, if any encrypted backups or files have been located within the case, it is prudent to check if the passwords contained within this category will open them.

User Name	Password/Tokens	Platf...
isaiah.dashner@gmail.com	1//04okgbk0ul70ECgYIARAAGAQSNwF-L9lrR5p-vao...	Google
isaiah.dashner@gmail.com	3I5klY7m4PAAAAAAAAABQUhS2uUd3Ue6j1U8hGJQ...	Dropbox
isaiah.dashner@gmail.com	vikingsfan123	Microsoft
isaiah.dashner@gmail.com	P4\$\$w0rd	Facebook
isaiah.dashner@gmail.com	vikingsfan123	Dropbox
isaiah.dashner@gmail.com	GoBuckeyes123	Google
isaiah.dashner@gmail.com	MCflarVd9ErLppFzFdKxYas2Dh!UDsuCGpCqhaeZP5...	Microsoft

Figure 12.21 An Example of Passwords and Tokens artifacts detailing stored credentials and tokens

DROPBOX

The CLOUD STORAGE → Cloud Dropbox Files category contains any files and folders that were captured from the acquired Dropbox account. The ARTIFACT INFORMATION includes: the location of the file within the Dropbox account, a File ID, a File Version ID, the server and client last modified date and time, the original photo timestamp if present, and a preview of the file content.



File Name	File ID	Dropbox File Path	Server Last...
00404_3TMiaAMuyS3_1200x900.jpg	id:VzCxAbOCF2AAAAAAAQKQ	/My Files/New Friends/00404_3TMiaAMuyS3_1200x9...	29/08/2019 18:02:
00404_dsQfMtdB47X_1200x900.jpg	id:VzCxAbOCF2AAAAAAAQKg	/My Files/New Friends/00404_dsQfMtdB47X_1200x9...	29/08/2019 18:02:
00c0c_8tjyn038hn_1200x900.jpg	id:VzCxAbOCF2AAAAAAAAGw	/My Files/New Friends/00c0c_8tjyn038hn_1200x900...	29/08/2019 18:02:
00dd4_8ZnN0nP9xF_1200x900.jpg	id:VzCxAbOCF2AAAAAAAALHA	/My Files/New Friends/00dd4_8ZnN0nP9xF_1200x9...	29/08/2019 18:02:
00KKM_cj2ih3xxor_1200x900.jpg	id:VzCxAbOCF2AAAAAAAALHC	/My Files/New Friends/00KKM_cj2ih3xxor_1200x900...	29/08/2019 18:02:
00101_6e32bzjsqF3_1200x900.jpg	id:VzCxAbOCF2AAAAAAAALAHw	/My Files/New Friends/00101_6e32bzjsqF3_1200x900...	29/08/2019 18:02:
00101_6e32bzjsqF3_50x50c.jpg	id:VzCxAbOCF2AAAMAAAAAAlg	/My Files/New Friends/00101_6e32bzjsqF3_50x50c.jpg	29/08/2019 18:02:
00M0M_3cDnDdPdR0P_1200x900.jpg	id:VzCxAbOCF2AAAMAAAAAAlA	/My Files/New Friends/00M0M_3cDnDdPdR0P_1200...	29/08/2019 18:02:
00q0q_87jEMIScNC_1200x900.jpg	id:VzCxAbOCF2AAAMAAAAAAlQ	/My Files/New Friends/00q0q_87jEMIScNC_1200x9...	29/08/2019 18:02:
00Q0Q_lrsAA6RHnW_1200x900.jpg	id:VzCxAbOCF2AAAAAAAAlg	/My Files/New Friends/00Q0Q_lrsAA6RHnW_1200x9...	29/08/2019 18:02:
00V0V_bzxOtyRInH_1200x900.jpg	id:VzCxAbOCF2AAAMAAAAAAlw	/My Files/New Friends/00V0V_bzxOtyRInH_1200x9...	29/08/2019 18:02:
00X0K_InglvOBg84o_1200x900.jpg	id:VzCxAbOCF2AAAMAAAAAAlA	/My Files/New Friends/00X0K_InglvOBg84o_1200x9...	29/08/2019 18:02:
00y0y_66q82qMpE6L_1200x900.jpg	id:VzCxAbOCF2AAAAAAAAlQ	/My Files/New Friends/00y0y_66q82qMpE6L_1200x9...	29/08/2019 18:02:
05_drugs-ledc_neww710.h473.jpg	id:VzCxAbOCF2AAAMAAAAAATg	/My Files/old flash drive pics/hugsnctdrugs/05_drug...	10/09/2019 19:54:
05ce42060aae047121c954e10bdb3...	id:VzCxAbOCF2AAAMAAAAAAARg	/My Files/old flash drive pics/bonksticks/05ce42060a...	10/09/2019 19:54:
1015555.jpeg	id:VzCxAbOCF2AAAMAAAAAAAdw	/My Files/old flash drive pics/pics to share/1015555.j...	10/09/2019 19:54:
105598.jpeg	id:VzCxAbOCF2AAAMAAAAAAAE	/My Files/old flash drive pics/pics to share/105598.jp...	10/09/2019 19:54:
1164848.jpeg	id:VzCxAbOCF2AAAMAAAAAAeQ	/My Files/old flash drive pics/pics to share/1164848.jp...	10/09/2019 19:54:
116675.jpeg	id:VzCxAbOCF2AAAMAAAAAAeg	/My Files/old flash drive pics/pics to share/116675.jp...	10/09/2019 19:54:
122908_wenger_1.jpg	id:VzCxAbOCF2AAAMAAAAAAAxQ	/My Files/old flash drive pics/stabbythings/122908_...	10/09/2019 19:54:
1254752.jpeg	id:VzCxAbOCF2AAAMAAAAAAAw	/My Files/old flash drive pics/pics to share/1254752.j...	10/09/2019 19:54:
1280x720-b3o.jpg	id:VzCxAbOCF2AAAMAAAAAAAZQ	/My Files/old flash drive pics/noods/1280x720-b3o.j...	10/09/2019 19:54:
12912644_1685266541725915_1070..	id:VzCxAbOCF2AAAMAAAAAAATA	/My Files/old flash drive pics/rootycooty/poointandho...	10/09/2019 19:54:
132548.jpeg	id:VzCxAbOCF2AAAMAAAAAAAlA	/My Files/old flash drive pics/pics to share/132548.jp...	10/09/2019 19:54:
1358396965_9c18eeccab9_lo-c12fc7f...	id:VzCxAbOCF2AAAMAAAAAAATw	/My Files/old flash drive pics/hugsnctdrugs/1358396...	10/09/2019 19:54:
1367002.jpeg	id:VzCxAbOCF2AAAMAAAAAAAlQ	/My Files/old flash drive pics/pics to share/1367002.j...	10/09/2019 19:54:
1453621807849.jpg	id:VzCxAbOCF2AAAMAAAAAAAUUA	/My Files/old flash drive pics/hugsnctdrugs/1453621...	10/09/2019 19:54:
1454806.jpg	id:VzCxAbOCF2AAAMAAAAAAAfA	/My Files/old flash drive pics/pics to share/1454806.j...	10/09/2019 19:54:

Figure 12.22 Cloud Dropbox Files artifacts

MICROSOFT ONEDRIVE

In addition to third-party cloud storage services like Dropbox, there are ones built-in natively to the Windows OS. Microsoft's OneDrive is a built-in service to all Windows 10 computers that not only allows its users free cloud storage, it is actively encouraged to allow for users to recover from unwanted damage or destruction to data such as ransomware attacks.

AXIOM can pull information from both the cloud storage of Microsoft's OneDrive and from local file artifacts that exist on the device. If an examiner discovers an artifact "OneDrive" under the CLOUD STORAGE section, this means that the user of the computer was storing files locally in their OneDrive folders. This information can be found within the OneDrive folder, but information about the files are parsed from a .ini file found within the user's AppData folder relating to OneDrive.



Figure 23 Cloud and locally recovered OneDrive artifacts

ARTIFACT INFORMATION	
File Name	animal-chihuahua-cute-39317.jpg
File Size (Bytes)	1943326
Last Modified Date/Time	30-Aug-19 5:26:57 PM
Owner Name	Isaiah Dashner
Account Type	Personal
Account ID	decdd7e72d1f0dd2
File Path	\Users\isaia\OneDrive\Pictures\Shared\Pictures\animal-chihuahua-cute-39317.jpg
EVIDENCE INFORMATION	
Source	Dashner Win10 PC.E01 - Partition 2 (Microsoft NTFS, 49.43 GB)\Users\isaia\AppData\Local\Microsoft\OneDrive\settings\Personal\decdd7e72d1f0dd2.ini

Figure 12.24 Reviewing the source location of OneDrive files

If data is acquired directly from Microsoft’s OneDrive cloud storage using AXIOM Cloud’s capabilities, the artifact will be stored as Cloud OneDrive Files. This artifact stores similar information as the local artifact however this may contain files that are not stored locally. This artifact can also show an examiner if a file has been shared with another user, whereas the locally stored data does not.

ARTIFACT INFORMATION	
File ID	DECDD7E72D1F0DD2!542
File Name	animal-chihuahua-cute-39317.jpg
File Type	File
File Path	isaiah.dashner@gmail.com\OneDrive (personal)\root\Pictures\Shared\Pictures\
File Size (Bytes)	1943326
Owner ID	decdd7e72d1f0dd2
Owner Name	Isaiah Dashner
Created Date/Time	30-Aug-19 8:59:07 PM
Modified Date/Time	30-Aug-19 8:59:15 PM
Shared With Root User	0
Attachments	animal-chihuahua-cute-39317.jpg

Figure 12.25 Reviewing the data pulled directly from AXIOM Cloud

As with other artifacts in AXIOM Examine, there may be connections available for the files obtained from CLOUD STORAGE options using file names or other values. These can be used to ascertain if the cloud stored files are also stored on other devices such as hard disks, removable drives, or mobile devices. In this example the relevant file has been stored on Microsoft’s OneDrive but clicking on the connection for the file name reveals that this hit is listed on both the local drive but also remote drives. The file hash goes to help confirm that this file is the exact file stored on the hard drive, USB drive, and Cloud storage.



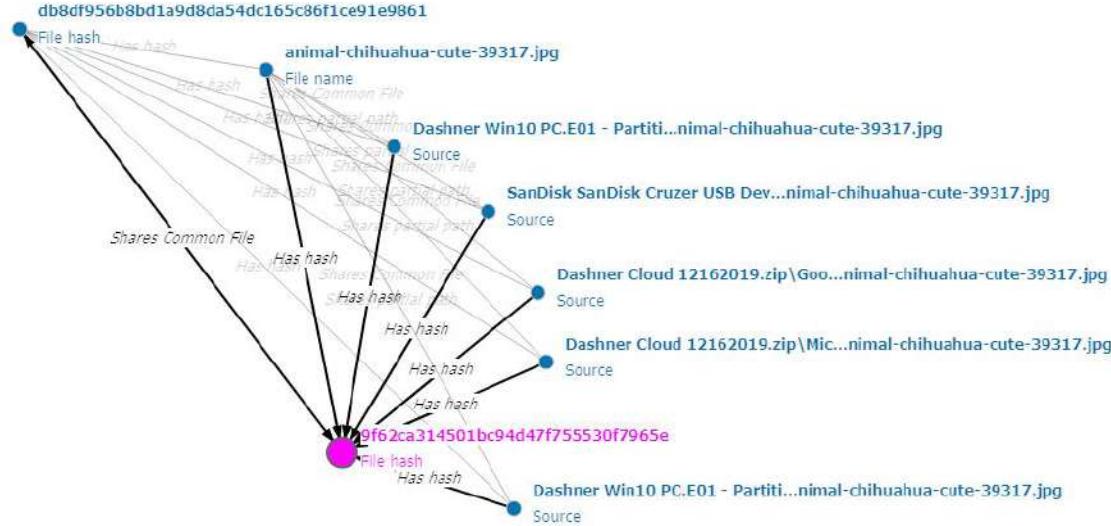


Figure 12.26 MD5 connections of files acquired from OneDrive

FACEBOOK

Though not shown in the current scenario case files, the Cloud Facebook Profile Info artifact is worthy of the examiner's attention. It includes a copy of the Facebook page of the account at the time of acquisition. This is not a live stream of currently available data, but a scrape of the website that saves the data as an encapsulation in time. This will include profile information about the user such as:

- Address
- Email Address(es)
- Phone Number
- Website
- Birthday
- Gender

AXIOM Cloud also captures and stores the raw HTML data from the page thereby making it searchable within AXIOM Examine. A preview window is generated based on the captured data, allowing the examiner to review the content as it would have appeared if they had logged into Facebook website on the day it was acquired.

The SOCIAL NETWORKING → Cloud Facebook Friends artifact displays the Facebook users linked as friends to the acquired account at the time of collection. The ARTIFACT INFORMATION includes the name of the friend, how many friends that person has, and a URL to the friend's homepage. The PREVIEW card within the DETAILS pane displays the profile photo of the user if available.

Name	Tagli...	Permanent Link
Terry Bunch	6 friends	https://www.facebook.com/profile.php?id=1000133...
Lily Duncan	6 friends	https://www.facebook.com/lily.duncan.1481169?fref...
Patricia Swain	7 friends	https://www.facebook.com/patricia.swain.3576?fref...
Scott Berner	1 friend	https://www.facebook.com/scott.berner.528?fref=pr...
Chris Donovan	5 friends	https://www.facebook.com/chris.donovan.3705?fref...

Figure 12.27 Cloud Facebook Friends artifacts

The Facebook Timeline includes information such as, status updates, tagged posts, check-ins, uploaded photos, profile changes, and posts from other users. The Cloud Facebook Timeline category displays this timeline data for the acquired Facebook account. The ARTIFACT INFORMATION includes the original Message ID used by Facebook, the name and Facebook ID of the user making the post, the type of post, the text of the post, the permanent link of the post, and when the post was created.

The Type field displays whether the artifact relates to a post to the timeline, a photo or video uploaded to the timeline, status updates, or generic timeline updates such as job or profile changes. Attachments to the post are also captured and displayed within AXIOM Examine for the examiner to review. These attachments can be reviewed in the File system explorer as well as the Artifact explorer allowing the examiner to quickly review any attachments that were captured by the cloud acquisition.

AXIOM Examine also renders the captured HTML data from each timeline posting and displays it in the PREVIEW card of the DETAILS pane. The rendered view includes some of the comments, and names of people who have interacted with the post on the Facebook website.



Message ID	Name	Text	Type	Permanent Link	Created Date	HTML Body
73231415882376	Isaiah Dashner		photo	https://www.facebook.com/photo.php?fbid=732314...	30/08/2019 20:52:53	<link type="text/css" rel="stylesheet" href="https://www.facebook.com/photo.php?fbid=732314..."/>
73231420549313	Isaiah Dashner		photo	https://www.facebook.com/photo.php?fbid=732313...	30/08/2019 20:51:01	<link type="text/css" rel="stylesheet" href="https://www.facebook.com/photo.php?fbid=732313..."/>
73231657215958	Isaiah Dashner		photo	https://www.facebook.com/photo.php?fbid=732312...	30/08/2019 20:51:40	<link type="text/css" rel="stylesheet" href="https://www.facebook.com/photo.php?fbid=732312..."/>
732313783862612	Isaiah Dashner		photo	https://www.facebook.com/photo.php?fbid=732313...	30/08/2019 20:52:02	<link type="text/css" rel="stylesheet" href="https://www.facebook.com/photo.php?fbid=732313..."/>

Figure 12.28 An example of the PREVIEW card of Facebook Timeline artifact

NOTE: On an Internet connected workstation, clicking on any link in the HTML preview will take you to the live Facebook login page. This should be avoided.



Figure 12.29 Live link to Facebook login page

The COMMUNICATION → Cloud Facebook Messenger Messages category includes any message data associated with the Facebook account that was acquired. It also includes any attachments or links that were shared using the Messenger service. In addition to displaying each individual message, the PREVIEW card in the DETAILS pane displays a chat threaded view allowing the examiner to review the information in a back-and-forth manner just like chat data from other platforms.

EVIDENCE (3)						
Sender...	Author ID	Text	HTML Body	Partici...	Date/Ti...	cid.c.100013119909406:100015386043920
Isaiah Dashner	100013119909406		<div class="z69" data-store="[""timestamp&...>	Isaiah Dashner	11/09/201	
Isaiah Dashner	100013119909406	Hey man	<div class="z69" data-store="[""timestamp&...>	Isaiah Dashner	29/08/201	
Isaiah Dashner	100013119909406	Got any files to share? Trying to find some new stuff.	<div class="z69" data-store="[""timestamp&...>	Isaiah Dashner	29/08/201	

Figure 12.30 Facebook Messenger

The Cloud Facebook Messenger Messages captured by AXIOM Cloud are processed the same as chat messages sourced from other platforms. Identifiers are extracted and compiled into the REFINED RESULTS → Identifiers - People category, Connections are created to map links between individuals, and the content can be displayed in Conversation view to quickly review threaded conversations including chats categorized by Magnet.AI.

GOOGLE

Artifacts acquired from the Google platform contain some of the most useful information due to the sheer volume and type of information Google stores about its users. A good starting point when reviewing cloud data is the REFINED RESULTS → Cloud Passwords and Tokens artifacts as it can contain passwords for many other cloud accounts that have been accessed by the user.

MEDIA	100
Cloud Google Photos	100
EMAIL & CALENDAR	440
Cloud Gmail Messages	440
CLOUD STORAGE	8
Cloud Google Drive Files	8
APPLICATION USAGE	1,339
Cloud Google Activity	1,330
Cloud Google Connected Apps	9
CONNECTED DEVICES	3
Cloud Google Recent Devices	3
LOCATION & TRAVEL	96
Cloud Google Timeline Locations	96

Figure 12.31 Artifacts extracted from a Google account

The CONNECTED DEVICES → Cloud Google Recent Devices artifact details other devices used to access the Google account, and therefore identifies other relevant devices to seize and acquire as part of the forensic investigation. This artifact also records the location of the device and when that device last utilized the synced services.

The APPLICATION USAGE → Cloud Google Connected Apps artifact details any additional applications that have access to the Google account.

NOTE: Where Magnet AXIOM was used to capture the data then there will always be at least one entry present – “Magnet Forensics International, Inc.”. This artifact relates to the AXIOM Cloud application.

If the user signs into their Google account from an Android device or utilizes Google location services, e.g. Google Maps or location-based searching, any information recorded by Google will be in the LOCATION & TRAVEL → Cloud Google Timeline Locations category. These timeline locations help establish places the user has either visited or passed through, or locations the user has searched for. Depending on the platform, the time and date of this activity might also be available. While not necessarily a direct map of where the user was at a specific point, these artifacts can demonstrate that the user was in a geographic region on or around a specific date and time. Due to the way in which Google passes this information from a mobile device to Google’s web services, these locations are often logged without any outside action by the user.



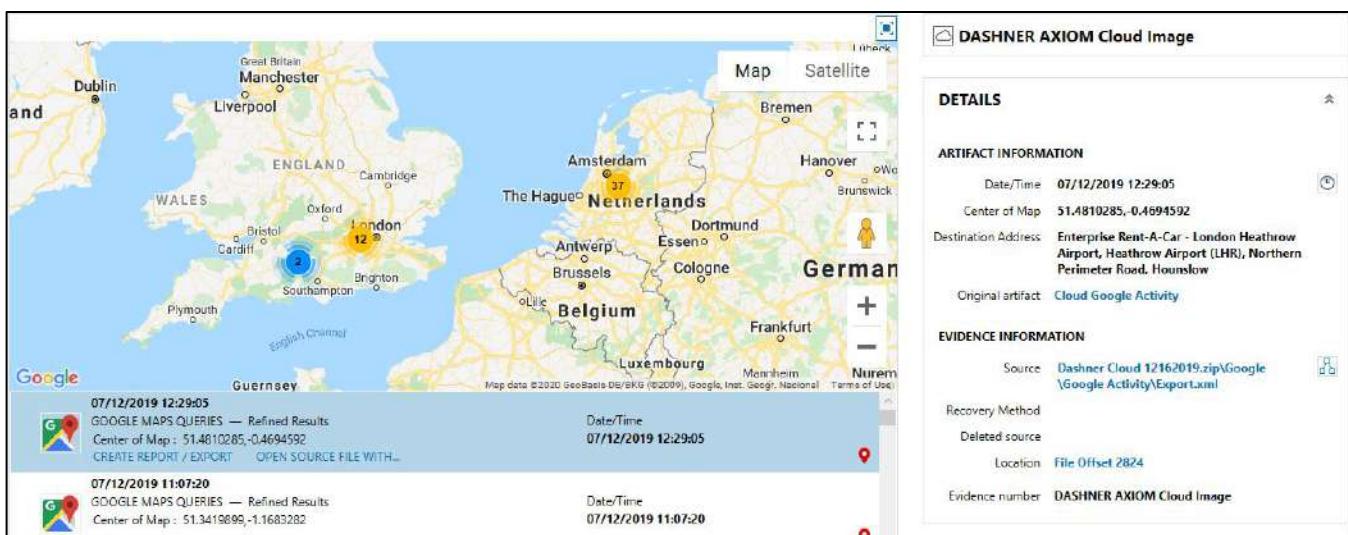


Figure 12.32 World Map view of Google Activity Locations

When a user accesses one of the services within the Google platform while logged into their Google account, a large amount of data is recorded and stored. The user can review this stored information from their My Activity webpage, and if acquired by AXIOM Cloud it is parsed into the APPLICATION USAGE → Cloud Google Activity category. It includes Internet browsing history and searches, YouTube search and watch history, searches for locations or directions, Google Assistant activity from Google Home devices, and if the device is running the Android OS, applications that were downloaded and used. Many of these actions include date and timestamps, and in some cases geolocation data detailing where the device was when the activity occurred.

Action	Description	Date/Time	Platform	Latitude	Longitude
Said	who Let The Dogs Out	29-Aug-19 4:00:14 PM	Google App	34.712159	-92.345763
Visited	Best Phoenix Dog Parks Pet Sitting Phoenix Arizona...	15-Sep-19 10:37:04 PM	Google Pixel 3a		
Searched for	funny dog videos cute	30-Aug-19 5:23:04 PM	Web		
Searched for	funny dog videos	30-Aug-19 5:22:58 PM	Web		
Watched	10 SMALLEST Dog Breeds In The World!	29-Aug-19 6:57:45 PM	Web		
Watched	Ultimate FUNNY DOGS & CUTE PUPPIES of 2018 Tr...	29-Aug-19 6:38:52 PM	Web		
Visited	https://www.k9convenience.com/best-phoenix-dog-...	15-Sep-19 10:37:04 PM			
Searched for	dog parks downtown phoenix	15-Sep-19 10:36:59 PM		34.720898	-92.21383

Figure 12.33 Google activity across multiple services

The CLOUD STORAGE → Cloud Google Drive Files category contains details of files that were acquired from the user's Google Drive account. These files can be viewed from the Artifact explorer, or the entire file/folder structure of the acquired data can be reviewed from the File system explorer. Within the File system explorer these files are stored within the folder \Google\Drive Files\Attachments\.

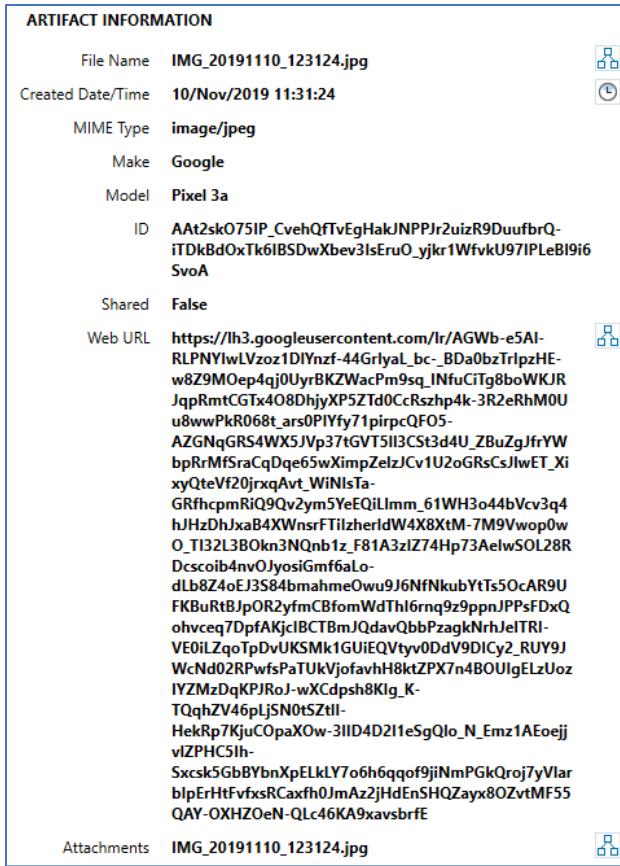
ARTIFACT INFORMATION	
ID	1_ilKh-HrmipJX74C-mhgZLXRHbx5-TtN
File Name	Videos.7z
Folder Structure	isaiah.dashner@gmail.com\Shared With Me\
Drive Owner	isaiah.dashner@gmail.com
Owner Name	Jason Smithers
Owner Email	jasonsmithers131@gmail.com
Shared	1
MIME Type	application/x-7z-compressed
File Size (Bytes)	203002043
Created Date/Time	30/Aug/2019 20:54:30
Last Viewed By Me Date/Time	30/Aug/2019 21:03:17
Modified Date/Time	30/Aug/2019 21:01:16
Last Modified Name	Jason Smithers
Last Modified Email	jasonsmithers131@gmail.com
Shared With Me Date/Time	30/Aug/2019 21:03:17
Source Locations	drive
Parent Folder	SharedFolder
Web URL	https://drive.google.com/uc?id=1_ilKh-HrmipJX74C-mhgZLXRHbx5-TtN&export=download
Download URL	https://www.googleapis.com/drive/v3/files/1_ilKh-HrmipJX74C-mhgZLXRHbx5-TtN?alt=media
Attachments	Videos.7z
Attachment Path	isaiah.dashner@gmail.com\Shared With Me\

Figure 12.34 Reviewing Google Drive attachments

The artifact for Google Drive (Cloud Google Drive Files) can also help to show if someone else is attached to the file. In the example above, the Videos.7z recovered from Dashner's Google Drive is owned by a separate user - Jason Smithers and shared to Dashner. By using the File System Explorer, the contents of this shared **7z** file can be reviewed.

The MEDIA → Cloud Google Photos category contains any photos or pictures that have been uploaded to the Google Photos service linked to the user's Google account. These photos and pictures may, or may not, also be stored in the user's Google Drive, dependent on the account settings. Many Android devices will automatically stream photos to the user's Google Photos without interaction from the user. Additional information such as when the photo was taken, when the photo or picture was uploaded, the make and model of the device used to take the picture, and any geolocation data are also uploaded with the file if available. The artifact displayed in AXIOM Examine also details in which photo album the pictures were stored.





The EMAIL & CALENDAR → Cloud Gmail Messages category contains any emails acquired from the Gmail account mailbox. If a date and time filter was applied at the time of acquisition, this category might not include all the messages that were stored in the mailbox at the time of collection. AXIOM Cloud retains any status flags applied to the messages and when the artifacts are reviewed in AXIOM Examine this information is recorded in the Label field, e.g. UNREAD, IMPORTANT, etc. Like other email artifacts in AXIOM Examine, Cloud Gmail Messages artifacts include sender and recipient details, any CC or BCC information, the message subject, and a rendering of the email content.

EVIDENCE (440)

ID	Label	To Adc
1610ff790be03:ca5	UNREAD,CATEGORY_PERSONAL,INBOX	isaiyah.dcl
1610ff93693fc90c	UNREAD,CATEGORY_UPDATES,INBOX	isaiyah.dcl
1610f74250ba46576	UNREAD,CATEGORY_SOCIAL,INBOX	isaiyah.dcl
1610c156a5dd7294	UNREAD,CATEGORY_SOCIAL,INBOX	isaiyah.dcl
1610f5be558bcdf7	UNREAD,CATEGORY_UPDATES,INBOX	isaiyah.dcl
1610e0f6739c14a3	CATEGORY_PROMOTIONS,UNREAD,INBOX	isaiyah.dcl
1610e1c965483a2	UNREAD,CATEGORY_UPDATES,INBOX	isaiyah.dcl
161073662a04d444	CATEGORY_PROMOTIONS,UNREAD,INBOX	isaiyah.dcl
1610f71270a5b437	UNREAD,CATEGORY_SOCIAL,INBOX	isaiyah.dcl
161013f9f87ad3b2	CATEGORY_PROMOTIONS,UNREAD,INBOX	<isaiyah.dcl>
16afe991b543abb0	UNREAD,CATEGORY_SOCIAL,INBOX	isaiyah.dcl
16efd3dc72232024	UNREAD,CATEGORY_UPDATES,INBOX	isaiyah.dcl
16afc9f092aa8c0b	UNREAD,CATEGORY_SOCIAL,INBOX	isaiyah.dcl

16f0671270a5b437

PREVIEW

From: Facebook <notification@facebookmail.com>
Sent: 14-Dec-19 12:04:24 PM
To: [Isaiyah Dashner <isaiyah.dashner@gmail.com>]
Subject: You have 6 new Page suggestions including Leyte TOP Models 2012.

Facebook

Figure 12.36 PREVIEW card of a Gmail messages cloud artifact

Any attachments to Cloud Gmail Messages are listed in the ATTACHMENTS card on the DETAILS pane. If the content can be displayed within AXIOM Examine e.g. pictures and documents, the attachment name is a hyperlink, as shown in the figure below. Selecting the link opens an embedded PREVIEW card displaying the content of the attachment file. Additionally, any attachments are parsed into their respective categories within AXIOM Examine and they can be reviewed from the artifact category based on the attachment file type, e.g. PDF Documents.

Thread ID	Attachments	Source
157b14e5650e035a	130179_Secrets_of_Meth_Manufacture_StevenPreisler.pdf	Cloud_2
15796ac9d3bb2d4f	images.jpg	Cloud_2
15796ac9d3bb2d4f	images.jpg	Cloud_2
15796aca04475eac	images.jpg	Cloud_2
15796aca04475eac	images.jpg	Cloud_2

ATTACHMENTS

- 130179_Secrets_of_Meth_Manufacture_StevenPreisler.pdf
- The Great Big Narcotics Cookbook.pdf

Figure 12.37 Gmail message with attachments

DOCUMENTS 6

- Calc Documents 1
- PDF Documents 4

EVIDENCE (4)

Filename
The Great Big Narcotics Cookbook.pdf
Getting started
130179_Secrets_of_Meth_Manufacture_StevenPreisler.pdf

Figure 12.38 Gmail message attachments are also contained within the respective artifact category



RUNNING EXERCISE

REVIEWING CLOUD ARTIFACTS

- From the **Artifacts** explorer in **AXIOM Examine**, clear any filters you may have applied.
- From the FILTERS bar, use the Evidence drop-down to select the Dashner Cloud evidence item.
- Select the OPERATING SYSTEM → Cloud Accounts Information artifact category, and sort by the Platform column.
- The passwords and tokens used to acquire the data from each platform are listed.
- DASHNER uses the same password for both the Microsoft and Dropbox accounts.
- Switch to the CLOUD STORAGE → Cloud Dropbox Files artifact category. Review the findings.
- Switch to the APPLICATION USAGE → Cloud Google Activity artifact category. Review the findings.

MODULE REVIEW

In this module the following topics were covered:

- A review of the cloud platforms from which AXIOM can collect and process data.
- Understanding how to use AXIOM Cloud to collect cloud data using passwords or tokens.
- The data recovered from popular cloud platforms such as Google, Facebook, and Dropbox.

REVIEW QUESTIONS

To help reinforce the learning objectives for this module, the following review questions have been provided:

1. List some of the cloud platforms that AXIOM Cloud can collect data from.
2. What two authentication methods can AXIOM Cloud use to access data from a cloud account?
3. When collecting Facebook data, are the messages sent via Facebook Messenger available for review? If so, what is the artifact named?
4. When obtaining data from a Google account and the Gmail Messages are collected, are any message attachments available to be viewed?



STUDENT EXERCISE

This exercise is based on the Dashner case scenario from Module 1.

- From the **Artifacts** explorer in **AXIOM Examine**, clear any filters you may have applied.
- Select the APPLICATION USAGE → Cloud Google Activity artifact category.
- List three applications that Isaiah DASHNER **Used**:

- List three things DASHNER has **Searched for**:

- Select the MEDIA → Cloud Google Photos artifact category.
- From the EXIF information, does it appear that these photos were generated using DASHNERS phone? If so which Phone?

- Select the CLOUD STORAGE → Cloud Dropbox Files artifact category.
- Were any files shared with Dashner from someone else? _____
- Select the CLOUD STORAGE → Cloud OneDrive Files artifact category.
- Locate the file called fluff2.jpg and select the connections icon located next to the file name.
- Using connections, answer the following questions:
- Does it appear this file was ever associated with applications other than OneDrive?

- Does it appear Dashner tried to delete or remove this file? _____

- Is there evidence this file was accessed from a USB or external drive? _____

- What was the volume name of the external drive? _____

- Does it appear another file contained this file inside of it? _____

- If so, which service does it relate to? _____
- Using the CLOUD STORAGE artifacts within the Artifact Explorer, who is the owner of the original container? _____



Notes



MAGNET
FORENSICS®

MODULE 13:

Reporting

LEARNING OBJECTIVES

In this lesson, students will take part in a lecture, instructor-led exercises, and student practical exercises to gain an understanding of the capabilities of Magnet AXIOM in order to export key artifacts for additional analysis. Students will create and manage portable cases for stakeholder review and collaboration and generate a final report with all investigative results.

GOALS

At the conclusion of this lesson, students will be able to extract key artifacts and create a portable case for additional analysis by the case investigating officer or legal counsel and subsequently author a final report using the tags discussed in previous lessons.

EXPORTING – ARTIFACTS VIEW

There may be times throughout an investigation when an examiner needs to export key artifacts from the case. Reasons for exporting the artifacts may include additional analysis requirements, legal process directives, prosecution requests for supporting exhibits during preliminary hearings, collaborating and reviewing key evidence with case stakeholders, or providing key intelligence during open/active investigations. Regardless of the necessity, AXIOM Examine allows examiners to save the actual artifact or export attributes and details from the artifacts, as displayed within the EVIDENCE pane.

To understand the exporting feature of AXIOM Examine, it is important to note the distinction between the export and save options. Exporting from the case involves creating an output file, in various formats, which contains attributes or details about the artifact, as parsed and displayed within the EVIDENCE and DETAILS panes of AXIOM Examine. For example, right-clicking on a picture displayed in the EVIDENCE pane, with the Column view selected, can create an output file containing the column values along with the actual picture. However, selecting the Save artifact to option, from the right-click menu, will save a copy of the picture to a location specified by the user.

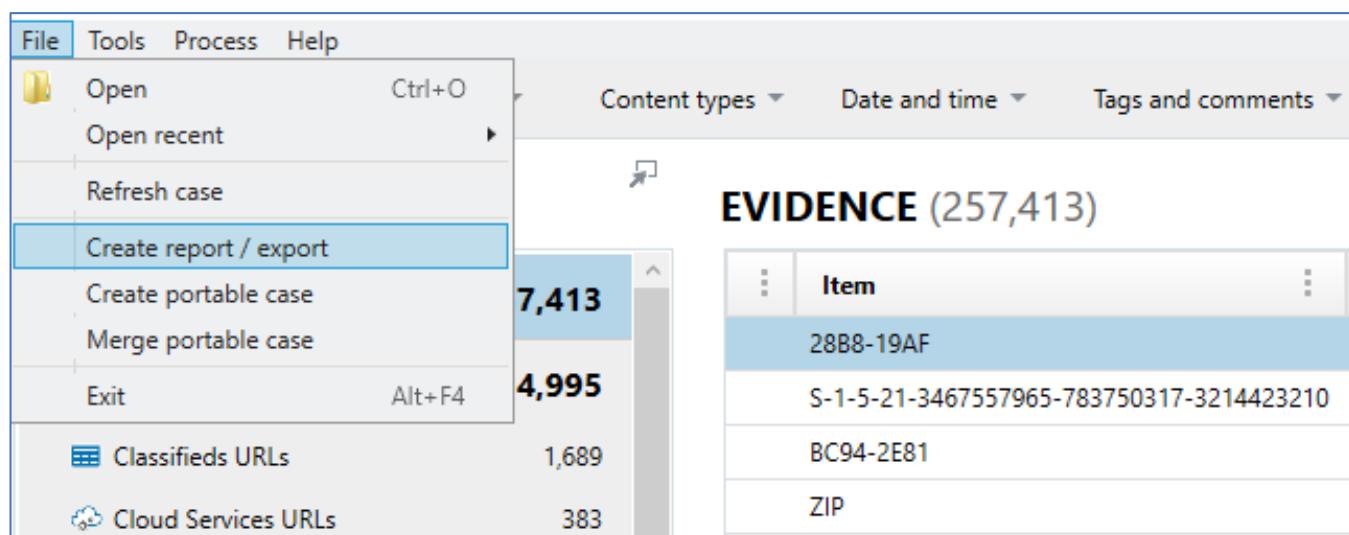


Figure 13.1 Exporting reports

A new reporting and exporting wizard was introduced in AXIOM version 4.0. This menu appears once a user selects the Create export/report option from anywhere within AXIOM Examine. This window allows for users to set up templates for report generation and have granular control over what information is included in their final report of choice.



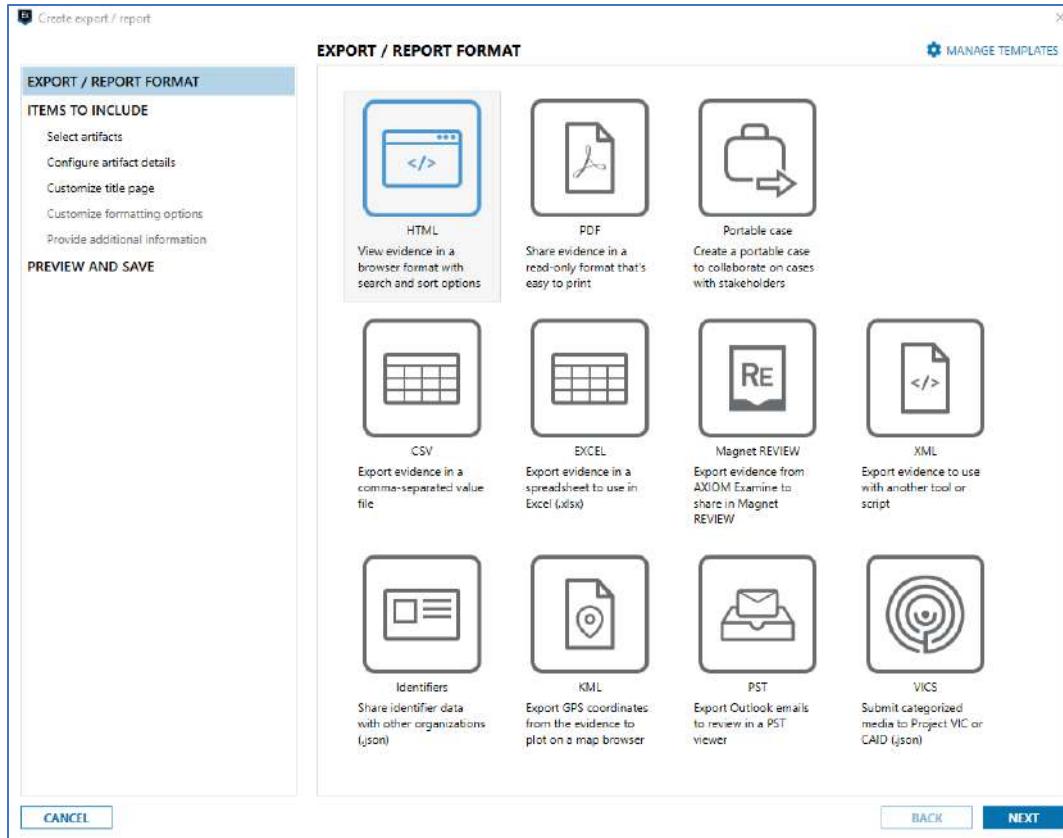


Figure 13.2 Export report formatting within Examine

The first window allows the examiner to select which type of report the user should generate. Currently examiners can select any of the following types:

- HTML
- PDF
- Portable Case
- CSV
- Excel
- Magnet REVIEW
- XML
- Identifiers
- KML
- PST
- VICS

Once a type is selected, users can modify the options in the ITEMS TO INCLUDE section. In the main area of the ITEMS TO INCLUDE section examiners can choose information to include in their report from Selected items only, Items in the current view, All evidence, Tagged items (with a dropdown selector to control which tags are included), or Use a template (includes specific artifact types, columns, and format options). The Use a template option allows the examiner to select one of their pre-created templates for including information such as a defense discovery report which may automatically exclude any Media items.

The screenshot shows the 'Create export / report' interface. On the left, a sidebar lists 'EXPORT / REPORT FORMAT' and 'ITEMS TO INCLUDE' sections with various options like 'Select artifacts', 'Configure artifact details', etc. The 'ITEMS TO INCLUDE' section is expanded. At the top right of this section is a 'MANAGE TEMPLATES' button. The main content area is titled 'ITEMS TO INCLUDE' and contains a sub-section titled 'ITEMS TO INCLUDE'. It says 'Select which items from the case you want to include in your export / report.' Below this are five radio button options: 'Use a template (includes specific artifact types, columns, and format options)' (selected, labeled 'Default'), 'All evidence (269,784)', 'Items in the current view (269,784)', 'Tagged items (38)', and 'Selected items only (1)'. A dropdown arrow is shown next to the 'Default' label.

Figure 13.3 Selecting items to include in the chosen report

To create a template, users should click the MANAGE TEMPLATES option in the top right corner of the Create export / report window. Users can create their own templates from a blank slate, import one that another examiner has already created, or even duplicate one of the existing templates for modification. These templates allow examiners to set which artifacts will/will not be included in a specific report type, what artifact details will be included, how the title page will be formatted, and what reporting format to follow. This could allow an agency to create templates for each of their examiners to follow.

Once the items to include have been selected, the next part of the workflow, SELECT ARTIFACTS, allows the examiner to pick and choose which artifacts and categories they would like to appear in the report by using a checkbox. These will only display the results recovered within the report and give the users a choice to selectively ignore artifacts or entire categories that may contain false-positive information.



SELECT ARTIFACTS

Confirm which artifacts from the case you want to include in your export / report.

Artifact selected from template

[CLEAR ALL](#) [EXPAND ALL](#)

- ↳ Additional Sources (1)
- ↳ Application Usage (1,978)
- ↳ Cloud Storage (398)
- ↳ Communication (275)
 - ↳ Android Call Logs (112)
 - ↳ Android Contacts (2)
 - ↳ Android SMS / MMS (101)
 - ↳ Cloud Facebook Messenger Messages (3)
 - ↳ Skype (57)
- ↳ Connected Devices (201)
- ↳ Custom (1,101)
- ↳ Documents (2,484)

Figure 13.4 Selecting artifacts to appear in the report

After examiners select which artifacts to appear within the case, they can then CONFIGURE ARTIFACT DETAILS. There are two components to the CONFIGURE ARTIFACT DETAILS screen: the ability to configure artifact options and the ability to configure which columns to include for each artifact. The CONFIGURE ARTIFACT OPTIONS area allows the examiners to pick several options including to remove file previews and attachments (for redacting contraband or privileged material), to include/not include chat threads, to enable external links to be clickable in the report, or to apply their blur/hide picture options on media items that have been categorized.

CONFIGURE ARTIFACT DETAILS

Customize how you want artifacts to display in the export / report.

CONFIGURE ARTIFACT OPTIONS

Include previews and file attachments
 Blur previews for items in illegal categories

Include chat threads as HTML
For each conversation in the export:
 Include only the individual messages I selected
 Include the full conversation history

Make external links clickable

CONFIGURE COLUMNS TO INCLUDE

All columns
 Visible columns and column sorting from current view
 Specific columns only (advanced)

Default ▼ [MANAGE COLUMN CONFIGURATIONS](#)

Figure 13.5 Configuring options for the reports

If the radio button for Specific columns only (advanced) is selected, users can then pick and choose which template (or to create a new template) for which columns to be included for each artifact selected. Creating a new, or modifying an existing column configuration, will load the MANAGE COLUMN CONFIGURATIONS window. This window will allow users to select any artifact in the current case and select which columns they would like to export for the final report. Once set, examiners can also export these configurations for deployment to other machines in their environment.



MANAGE COLUMN CONFIGURATIONS

Column configuration Default IMPORT CONFIGURATION EXPORT CONFIGURATION

Select an artifact type from the list below, and then select which columns you want to include in the export / report. You can also drag and drop columns to reorder them.

Find an artifact...

Only view artifacts in the current case

APPLE DISK IMAGES

CLEAR ALL

Include	Column name	Sort order
<input checked="" type="checkbox"/>	Tags	None
<input checked="" type="checkbox"/>	Comments	None
<input checked="" type="checkbox"/>	File Name	None
<input checked="" type="checkbox"/>	File Path	None
<input checked="" type="checkbox"/>	File Type	None
<input checked="" type="checkbox"/>	File System Created Date/Time - UTC (yyyy-mm-dd)	None
<input checked="" type="checkbox"/>	File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	None
<input checked="" type="checkbox"/>	File System Last Modified Date/Time - UTC (yyyy-mm-dd)	None
<input checked="" type="checkbox"/>	Source	None
<input checked="" type="checkbox"/>	Location	None
<input checked="" type="checkbox"/>	Evidence number	None
<input checked="" type="checkbox"/>	Deleted source	None
<input checked="" type="checkbox"/>	Recovery method	None

CANCEL **SAVE** **SAVE AND CLOSE**

Figure 13.6 Managing columns to appear in the final report

The next part of the exporting workflow allows the examiner to customize the title page of the report. This allows them to place an agency or group logo, organization name, and examiner name.

The CUSTOMIZING FORMATTING OPTIONS area of the workflow is only available for PDF, EXCEL and VICS report types. It will allow the user to set the option using radio buttons between creating one report that includes all artifact types, or to create separate reports for each artifact type. Please note, that if the Create one report that includes all artifact types option is selected, then only the columns shared by all the artifacts will be included in the final report.

RUNNING EXERCISE

REPORTING FROM THE FILE MENU

- From the Artifacts explorer in AXIOM Examine, clear any filters you may have applied.
- From the Artifacts drop-down menu on the FILTERS bar, check the artifacts for the Chrome Downloads, Firefox Downloads, and Edge/Internet Explorer 10-11 Downloads categories.
- From the File Menu and select **Create export / report**.
- In the Create export / report window, select HTML as the report type, then **NEXT**.
- On the ITEMS TO INCLUDE screen, select the radio button for Items in the current view then **NEXT**.
- Leave all the artifacts selected on the next screen, then press **NEXT**.
- On the CONFIGURE ARTIFACT DETAILS screen, leave the default selections then press **NEXT**.
- On the CUSTOMIZE TITLE PAGE screen, fill in the Organization and Examiner name boxes before pressing **NEXT**.
- In the File Location area, click **BROWSE** next to the File Path and create a new folder on the desktop called **\Dashner Case Exports** then press **SAVE FILE**.
- When complete, click **OPEN** from the Status Bar to view the export folder and files. Launch the export report using the **Report.html** file.

EXPORTING – PORTABLE CASE

Portable cases can be created for many uses. Similar to the requirements for exporting artifacts and saving files, the need for a portable case can include responding to legal process directives, such as a discovery order, managing larger case data sets by assigning smaller artifact analysis duties to other examiners, providing training to new members of the examination team, collaborating and reviewing case evidence with other stakeholders, or allowing examiners without an AXIOM license, but with the most knowledge about the case, perform the analysis. Regardless of the reasons, examiners can use the Create portable case option from the File menu in AXIOM Examine to create and manage custom case data sets within the overall investigative workflow. Portable cases can be accessed by both licensed and non-licensed users of AXIOM. When launching the lightweight version of AXIOM Examine to work with the portable case, a non-licensed user will not have access to the following features: File system explorer, Registry explorer, TEXT AND HEX card, DECODE card, Create portable case, and Merge portable case.

The Create portable case option, from the File menu, opens the Create report / export window, which is also used for the exporting operations. The Export type drop-down menu is what allows the examiner to



create the portable case data set. By default, the ITEMS TO INCLUDE option is set to Items in the current view. So, prior to creating the portable case, the examiner must determine which artifacts they wish to have included in the resulting data set.

Other options which can be selected include Tagged items and All Evidence. If the All Evidence option is selected, AXIOM will create a portable case containing the same categories and artifacts that were part of the “parent” case viewed in AXIOM Examine.

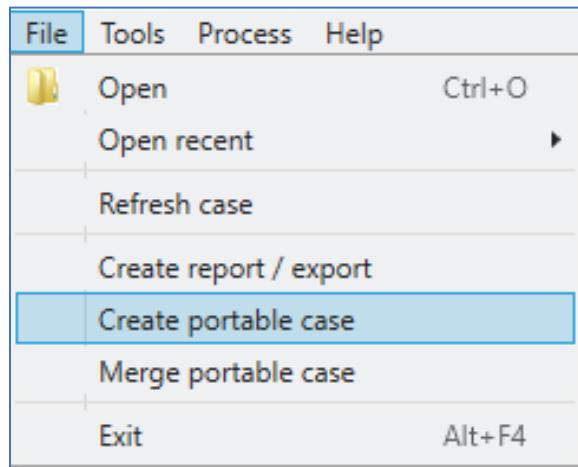


Figure 13.7 Create a portable case

The portable case folder will contain two database files. One file, with a hash-like file name and a **.attachments** extension, will contain data pointers and other details about the artifacts within the case. The second file, which is the larger of the two, is the main case database and the file that AXIOM Examine (for a licensed user) or the **OpenCase.bat** file (for a non-licensed user) will use to display the case data in AXIOM Examine. If a licensed user of AXIOM wishes to open a portable case, they can navigate to the portable case folder from the Open option of the File menu and use the Select folder option to open the case. Or, the licensed examiner can double-click the **Case.mfdb** file, which will also open the portable case in AXIOM Examine. For a non-licensed user, double-clicking the **OpenCase.bat** file will automatically open the **Case.mfdb** file in the lightweight version of AXIOM Examine.



Figure 13.8 Folder structure with .bat file and portable case folder contents

MERGING PORTABLE CASES

After they have been processed by another examiner or stakeholder, portable cases can be merged back into the parent case itself. An example of this scenario might be when a case is too large for one examiner to process in a timely manner. The lead examiner can create smaller portable cases containing specific artifact categories, which can then be assigned to other members of the forensics team for processing. After the examiner has completed their analysis, they can return the portable case to the lead examiner for merging into the parent case.

From the File menu, the Merge portable case option begins the process. Next, the examiner needs to navigate to and select the Portable Case sub folder within the main portable case folder itself.

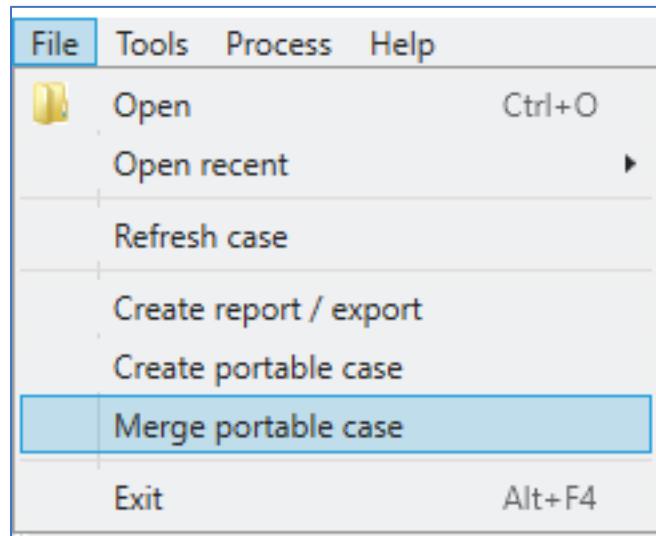


Figure 13.9 Merge portable case options

MERGING PORTABLE CASES – TAGS

During the merge process, examiners have the option to include all Tags, Comments, and Profiles (default), or to select which case attributes they want to include in the merging process. If Tags are selected, AXIOM will display the tags from both the original (parent) case and the portable case. AXIOM will list the results of the tag merge process. AXIOM, by default, will also have the Show conflicts only option checked. If there are no conflicting tag names, the Merge Tags window will be empty. If the option is unchecked, AXIOM will display all tags that will be part of the merge process, regardless of conflicts. If there are conflicts, AXIOM gives the examiner the option of renaming the tags prior to the merge.

Merge portable case

SELECT MERGE OPTIONS

Select the types of information you want to include in the merge.

Tags
 Comments
 Profiles

Merge portable case

MERGE TAGS

When a tag that's created in the portable case has the same name as a tag that's created in the original case, you can either merge the tags together or rename the portable case tag to separate them. Show conflicts only

Original case	Portable case	Action	New label	Merge result
Bookmark	Bookmark	Merge		Bookmark
Evidence	Evidence	Merge		Evidence
Of interest	Of interest	Merge		Of interest
Portable Case Bookma		Merge		Portable Case Bookma

Figure 13.10 Options for merging a portable case back into the full axiom case

MANAGING PORTABLE CASES – COMMENTS

If Comments are included as part of the merge process, AXIOM will allow the examiner to apply a unique User ID to the comments from the portable case. After the merge process is completed, the User ID is applied to all the comments from the portable case to identify the user who applied the artifact comments. Tags and/or comments for both the original and portable cases can be managed from the Tags and comments drop-down on the FILTERS bar, further assisting the examiner with their case evidence management.

Merge portable case

MERGE COMMENTS

If you'd like to include an ID with portable case comments (such as the user's initials), provide one in the field below. This ID can help differentiate portable case comments from the original case's comments.

User ID

Figure 13.11 MERGE COMMENTS User ID option

RUNNING EXERCISE

CREATING A PORTABLE CASE

- From the Artifacts explorer in AXIOM Examine, clear any filters you may have applied.
- From the File menu, select Create portable case.
- From the EXPORT / REPORT FORMAT screen, note the Portable case option is selected, press **NEXT**.
- Select the radio button for All evidence and press the **NEXT** button.
- In the SELECT ARTIFACTS screen, press the **CLEAR ALL** option. Expand the categories to select the individual artifact types:
 - a. Communication → Android SMS/MMS
 - b. Communication → Skype
 - c. Connected Devices → Your Phone
- Press **NEXT**.
- Press **BROWSE** on the PREVIEW AND SAVE screen.
- For the File path, create a new folder on the desktop for **\Dashner Chat Artifacts**.
- Press **SAVE FILE**.
- When complete select **OPEN** from the Status Bar to review the contents of the **\Dashner Chat Artifacts** folder.
- Return to AXIOM Examine.
- From the File menu, select Open and navigate to the **\Dashner Chat Artifacts** folder.
- Double-click the **\PortableCase\Case Files** folder and then choose the **Case.MFDB** file to open the portable case.
- From the NAVIGATION pane, select the CONNECTED DEVICES → Your Phone Devices artifact category.
- Create a new tag for the artifact listed in the Your Phone Devices artifact category. Because we are working in a portable case, make sure to use your initials in front of the tag name. For example, “XX Dashner Your Phone Devices”. Add a comment to the tag for, “Isaiah Dashner Your Phone device info”.



- Create a new tag for the Your Phone Contacts, “Dashner Your Phone Contacts”, also using your initials in the tag name.
- Create a new tag for the Your Phone SMS/MMS, “Dashner Your Phone SMS/MMS”, also using your initials in the tag name.
- Close the portable case by using the File menu and selecting Exit, or clicking the X in the upper-right corner of the window.

CREATING A PORTABLE CASE FROM THE EVIDENCE PANE

- From the **Artifacts** explorer in **AXIOM Examine**, clear any filters you may have applied.
- Select **EMAIL** → **Outlook Emails** artifact category.
- In the **EVIDENCE** pane, sort by the **Attachments** column.
- Select only the emails with attachments.
- Right-click on the selected items, select **Create export / report**
- When the **Create export / report** window opens, select **Portable Case**, then press **NEXT**.
- Select the radio button for **Selected items only** then press **NEXT**.
- On the **SELECT ARTIFACTS** screen, leave all the artifacts selected then press **NEXT**.
- On the **PREVIEW AND SAVE** screen, select **BROWSE** and create a new folder in the **Dashner Case Exports** folder called **\Outlook Email with Attachments**.
- Press the button.
- When complete, click **OPEN** from the Status Bar to view the export folder and files. Launch the portable case using the **OpenCase.bat** file. Notice AXIOM will not open the Portable Case with a valid AXIOM license already on the machine. Instead, open the Portable Case from **\Portable Case\Case Files**

MERGING A PORTABLE CASE

- Return to the original full Dashner case in Examine.
- From the File menu, select **Merge portable case**.
- From the **SELECT CASE TO MERGE** window, click **BROWSE** and navigate to the **\PortableCase\Case Files** folder.

- Select the Case.MFDB file, choose Open, then click **NEXT** to begin the merge operation.
- In the SELECT MERGE OPTIONS window, check only the option for Tags and **Comments** then click **NEXT**.
- In the MERGE TAGS window, uncheck the option for Show conflicts only.
- Note the tags to be added from the Portable case with the unique tag names and initials. Click **NEXT**.
- In the MERGE COMMENTS window, enter your initials and the date into the User ID field e.g. CSV-05072021.
- From the MERGE SUMMARY screen, AXIOM details the portable case location, case name, evidence items, and the number of tags to merge. Complete the merge operation by clicking **MERGE**.
- From the NAVIGATION pane of the Artifacts explorer, select the CONNECTED DEVICES → Your Phone Devices artifact category.
- In the EVIDENCE pane, hover over the block indicating this artifact has been tagged. The tag name displayed should match that entered from the portable case.
- Expand the TAGS, PROFILES & MEDIA CATEGORIES pane.
- The User ID has been applied to the comment during the merge operation.

SPECIAL EXPORTS – PROJECT VIC

For the Pictures and Videos artifacts in AXIOM Examine, the option of creating a Project Vic 2.0 or 1.3 data set is available from the Artifacts and File system explorers. When selected, AXIOM will create an Open Data (OData) JavaScript object notation (JSON) file formatted for a Project Vic data set, which contains details for the creation of a special export file format.

Project Vic is spearheaded by the International Center for Missing and Exploited Children (ICMEC) and the Department of Homeland Security (DHS) and is an initiative to create a standardized, shared, central hash database that examiners can use to locate and/or categorize child exploitation images. The Project Vic Website states, “The purpose of Project VIC is to create an ecosystem of information and data sharing between domestic and international law enforcement agencies all working on crimes facilitated against children and the sexual exploitation of children.” In AXIOM Process, Project Vic JSON data sets can be imported and used in the CATAGORIZE PICTURES function for identifying pictures and videos from the case with hash values that match those from the Project Vic data. In addition, using the Create report / export feature in AXIOM Examine, examiners can create a custom Project Vic (2.0/1.3) data set from picture and video artifacts in the case. The exported Project Vic data set (JSON) can be used in third party



media analysis tools, such as Griffeye Analyze DI, or provided to other users of Magnet IEF and AXIOM, who can then import the exported .JSON Project Vic file and take advantage of the media hash comparison capabilities of both tools.

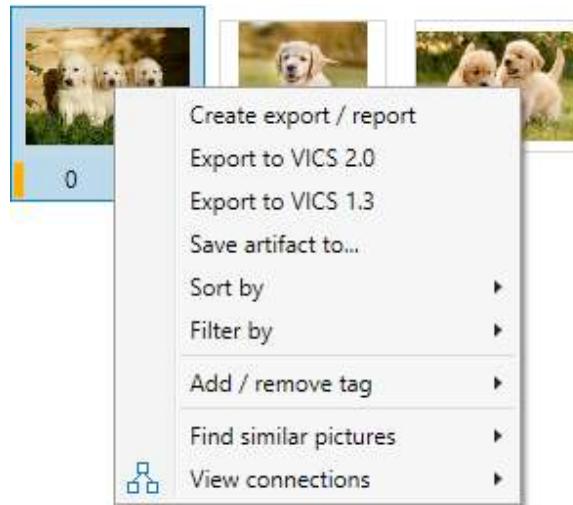


Figure 13.12 Export of images to a report in Project Vic format

SPECIAL EXPORTS – IDENTIFIERS

Another special export available in AXIOM Examine is the option to export the Identifiers from the case. AXIOM parses the Identifiers artifacts from across the evidence sources when the case is created. The Identifiers can include unique biographical information for the user, system level identifiers, such as SIDs, chat client screen names, email addresses, and any value that uniquely identifies a given user on the system. When the Identifiers option is selected as the Export type, AXIOM will create a JSON file which can be shared between installations of AXIOM for the purposes of comparing identifiers between cases. The Create report / export dialog window allows the examiner to include information about their agency, so the recipient of the exported identifiers can use to contact the agency should they need additional assistance or wish to collaborate on any matching identifiers.

ITEMS TO INCLUDE

Format: **Identifiers**
Items to include: **Selected Identifiers only**
Artifact count:

PROVIDE ADDITIONAL INFORMATION

Provide the following information so that others can contact your organization when they have a case with the same identifiers.

Case number	AX200 Full
Organization	Magnet Forensics
Email	training@magnetforensics.com
Phone number	304-867-5309
Name	Training Team
Title	Forensic Instructor

Figure 13.13 Create export / report for Identifiers

EXPORTING – FILE SYSTEM EXPLORER

Using the right-click Export details option in the File system explorer only allows for the creation of a **.csv** format for the export operation. In addition, unlike the export option from the File menu, which gives the examiner several choices in the ITEMS TO INCLUDE section of the export window, the right-click export option limits the export operation to Selected items only. So, prior to using the right-click menu option, the examiner should select all artifacts that they wish to include in the export.

SAVING FILES – ARTIFACT AND FILE SYSTEM EXPLORERS

The files themselves can also be saved out of the case for additional analysis or collaboration and review with other stakeholders. In the Artifacts explorer, the Save artifact to option is only available by right-clicking on an artifact within the EVIDENCE pane. In addition, the save option only applies to artifacts that are actual files, rather than those representing the attributes or details of an actual file. A similar operation for saving files from the case is available from within the File system explorer in AXIOM Examine. From the File system explorer, when a file is selected, and the right-click menu is opened, Save file / folder to and Save file / folder to ZIP options are presented to the examiner. The Save file / folder to copies the file from the case to a directory location specified by the examiner. During this operation, the original file type of the artifact is retained, such as **.jpg** or **.pdf**. The Save file / folder to ZIP adds the selected files to a **.zip** archive instead.



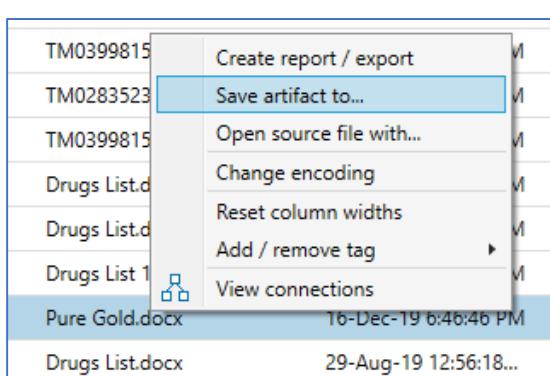


Figure 13.14 Save artifact to option details

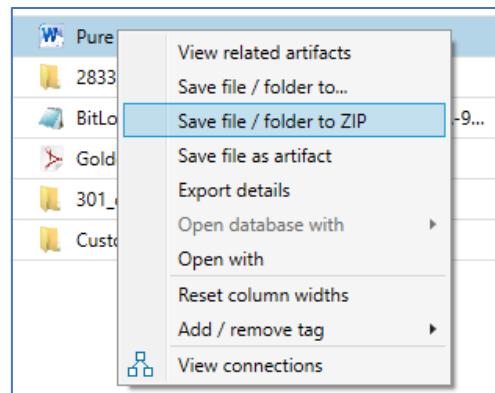


Figure 13.15 Save file / folder to ZIP and Export

Note: When using the Save file / folder to option, the saved files are listed with the local machine timestamps. The Save files / folders to ZIP option will retain the timestamps from the evidence for the files within the .zip file and will not apply local timestamps until the files are extracted.

RUNNING EXERCISE

EXPORTING FILE DETAILS FROM THE FILE SYSTEM EXPLORER

- Switch to the File system explorer.
- Navigate to the following path:
Dashner Win10 PC.E01\Partition 2\Users\isaia\Downloads
- In the EVIDENCE pane, select all the listed items. Right-click and select Export details.
- Select the **\Dashner Case Exports** folder as the destination. Create a new sub folder called **\Dashner Downloads**. Note the CSV file format is the only option available and the default file name of **Export.csv**.
- Press the CREATE button to generate the report.
- When complete, click **OPEN** from the Status Bar to view the export folder and file. Open the **Export.csv** in Microsoft Excel by double-clicking on it.
- Review the information contained in the CSV file. When complete, change the file name to **Dashner Downloads.csv**.

SAVING FILES FROM THE ARTIFACTS EXPLORER

- From the Artifacts explorer in AXIOM Examine, clear any filters you may have applied.
- Select the DOCUMENTS → PDF Documents category.
- In the EVIDENCE pane, sort by the Filename column.
- Locate the entries for **Golden puppies.pdf** file and find the file recovered from the Dashner Win10 PC evidence item.
- Right-click on the file name in the EVIDENCE pane and select Save artifact to.
- Select the **\Dashner Case Exports** folder as the destination. Create a new sub folder called **\Dashner Documents** and choose Select Folder.
- When complete, click **OPEN** from the Status Bar to view the export folder. Note AXIOM creates an **\Attachments** folder within the selected destination and places the exported file inside.
- Open the **Attachments** folder, then double-click on the **Golden Puppies.pdf** file.

SAVING FILES FROM THE FILE SYSTEM EXPLORER

- From the Artifacts explorer in AXIOM Examine, click the Source link in the DETAILS pane for the **Golden puppies.pdf** file to view the file's location in the File system Explorer.
- From the EVIDENCE pane, right-click the file and select Save file / folder to ZIP.
- Select the **\Dashner Documents** folder for the export and label the **ZIP** file with the file name of the PDF you are exporting, **Golden puppies**.
- When complete select **OPEN** from the Status Bar to confirm the export of the ZIP archive.

CASE REPORTING

Once the investigation with AXIOM has been completed, the examiner may need to generate a final case report. When generating the case report, it is important for the examiner to create a format which not only identifies the key artifacts that are relevant to the investigation, but also presents the artifacts in a manner that is easy to understand and interpreted by both technical and non-technical recipients. From the File menu in AXIOM Examine, the Create report / export menu option can also be used to create the case report. Once the Create report / export window opens, the examiner has the option of selecting the output format from the Export type drop-down menu. The HTML format is probably one of the most common, but other formats available include PDF, Portable case, CSV, Excel, Magnet REVIEW, and XML. Like the export operation, the examiner also has the same three choices available under the ITEMS TO



INCLUDE section of the export window when creating the case report. The default is Items in the current view (EVIDENCE pane) but can be changed to Tagged items or All evidence items. The CUSTOMIZE FORMATTING OPTIONS is what that enables the examiner to further decide whether they would like the report to be one single report from beginning to end, or an individual report for each artifact type.

Once generated, the report folder can contain the following files and folders: **front.html**, **index.html**, **nav.html**, **\Attachments**, **\ChatThreads** (if present in the exported artifacts), **\resources**, and **\webpages**. The **front.html** and **nav.html** files are used to aid in the report header and artifact category panes as viewed from the **index.html** file, while the **\resources** folder contains the **.css**, **.js**, and images used to create the structure and format of the report.

Name	Date modified	Type	Size
Attachments	20-Mar-20 1:03 PM	File folder	
Chat preview report	20-Mar-20 1:02 PM	File folder	
Resources	20-Mar-20 1:00 PM	File folder	
Report	28-Jun-17 11:39 AM	Microsoft Edge H...	1 KB

Figure 13.16 Contents of folder containing exported case

CASE REPORTING – FINAL REPORT

Opening the **Report.html** file will open the final HTML report, see Figure 13.17

Chrome Web Visits				
Record	Tags	Comments	URL	
1	AxCrypt Story		http://www.axcrypt.net/documentation/get-started/	
2	AxCrypt Story		https://account.axcrypt.net/en/Home/Activate?Email=isaiyah.dashner%40gmail.com&Code=123759	
3	AxCrypt Story		http://www.axantium.com/	

Figure 13.17 Final report format

Within the HTML report, individual column headers can be sorted by numerical order, alphabetical order, or timestamp. In addition, a filter option also exists for each column, which allows the viewer to enter a keyword and filter on the column values. This can be especially useful for report categories with large numbers of associated artifacts, such as Windows Event Logs, email messages, or chat conversations.

Chrome Web Visits			
Record	Tags	Comments	URL
Filter	Filter	Filter	Filter

Figure 13.18 Final report filters within browser



REVIEW QUESTIONS

To help reinforce the learning objectives for this module, the following review questions have been provided:

1. True/False. Exporting in AXIOM can be performed from the Registry view?
2. What option from the File system explorer allows a user to export artifact details from the case?
3. What is the file format for a Project VIC 1.3/2.0 export?
4. From the File system explorer, what are the options available for saving files from the case?
5. When a non-licensed user wants to open a portable case, what file can they use to launch the case in AXIOM Examine?
6. What is the name of the HTML file that will launch the case report?
7. In the HTML version of the case report, what features can assist the viewer in managing the listed artifacts?

STUDENT EXERCISE

This exercise is based on the Dashner case scenario from Module 1.

- From the **Artifacts** explorer in **AXIOM Examine**, clear any filters you may have applied.
- Create a **.csv** file containing all the Pixel 3a images. This can be useful for additional processing or review with examiners.
- Export any potentially relevant videos from Dashner’s SanDisk USB device.
- Create a **.html** report for all Dashner’s browser downloads.
- Create a Project VIC 2.0 export for all the pictures from Dashner’s SanDisk USB device.
- Create a portable case containing just the Chat artifacts, which can be provided to the case examiner for additional review.
- Open the portable case.
- Create a tag for all the conversations between Dashner and Martin Clemons.
- Merge the portable case back to the main case.
- Within the main case, create a tag for any relevant documents in the DOCUMENTS → Word Documents and the DOCUMENTS → PDF Documents artifact categories.
- Create an HTML case report which includes only the tags, and comments from the student exercises.



Notes



MAGNET
FORENSICS®

APPENDIX A:

Module Review Question Answers

MODULE 4: ENCRYPTION & CREDENTIALS

1. How does AXIOM Process identify Encrypted Files?

Utilizing Passware plugins.

2. Does an Encrypted Files artifact display what program was used to encrypt the files?

No

3. What does AXIOM Process search for when identifying Encryption / Anti-forensics Tools artifacts?

Known executables and data structures.

MODULE 5: REFINED RESULTS

1. What is the purpose of the REFINED RESULTS artifact categories?

To help the examiner expedite their investigation by placing useful artifacts in one category.

2. Explain the difference between the Google Searches and Parsed Search Queries artifacts.

Google Searches is only for searches conducted on Google. Parsed Search Queries is for all other search engines, like Bing, Yahoo, etc.

3. What REFINED RESULTS artifacts are used to create a Profile?

ONLY Identifiers-People and Identifiers-Devices.

4. Name at least three sources of information for the Identifiers artifacts.

Any of the columns from either Identifiers-People or Identifiers-Devices will suffice.

5. What resource lists the various artifacts search for by AXIOM and the meanings of the column values?

The Artifact Reference, accessed from Help > Documentation > Artifact Reference.

MODULE 6: WEB RELATED

1. Firefox and Chrome store much of their data in SQLite databases. How can the content of SQLite databases be viewed in AXIOM Examine?

From the SQLite Viewer within the File System Explorer.

2. Name three pieces of information displayed in AXIOM Examine for a file downloaded using Chrome.

Any of the columns from the Evidence Pane or Details Pane will suffice.

3. What is Session Recovery data?

Information such as last opened tabs, etc. This is the information that may be stored should the browser quit unexpectedly, or crash.

4. Name the database that stores/tracks most of the artifacts generated by Edge and Internet Explorer v10 and v11.

WebCacheV01.dat

MODULE 7: EMAIL

1. Where can EMAIL specific information such as Subject, To, From, and Received Time be viewed in AXIOM Examine?

The Evidence Pane or the Details Pane.

2. What is the potential investigative value of EMAIL Headers?

Headers main contain accurate timestamps from the email servers, IP addresses, true sender information, and more.

3. How can EMAILS with attachments be quickly identified?

Either by viewing the Attachments column for data, or by accessing the Email Attachments artifact category.



4. If a keyword Search is conducted from the FILTERS bar, what parts of an EMAIL are searched?

All Parts

MODULE 8: DOCUMENTS

1. Where is the content of a document displayed in AXIOM Examine?

The Preview Card in the Details Pane.

2. When viewing a document's DETAILS, what is the difference between the Created Date/Time and the File System Created Date/Time?

The Created Date/Time comes from the document metadata, whereas the File System Created Date/Time comes from the filesystem itself.

3. Name three document formats searched for and categorized by AXIOM.

One could utilize the Artifact Reference and list any three here, examples include Word documents, Excel documents, Hangul Word Processor, and others.

4. Will a keyword search conducted across the DOCUMENTS artifact category find a word within a PDF document?

Yes in the flat-text preview, and an examiner may use the OCR functionality to process those PDF documents.

MODULE 9: OPERATING SYSTEM PART 2

1. If a user is suspected of watching a video from an external drive connected to the host system, what OPERATING SYSTEM artifacts can help the examiner identify the name of the file, path for the file, and application used to watch the video?

Prefetch, LNK files, Jump Lists, and User Assist can all aid the examiner in identifying those artifacts.

2. The Windows Prefetch service provides examiners with which three key pieces of information?

Name of the application, run count, and times.

3. What AXIOM Examine feature allows examiners to quickly identify the most relevant Windows Event Log entries?

Filtering and sorting.

MODULE 10: MEDIA

1. What types of data are categorized within the MEDIA artifact categories within AXIOM Examine?

Using the Artifact Reference, there are many, including but not limited to: Pictures, videos, and audio files.

2. What two PREVIEWS are available to help examiners quickly review VIDEO artifacts?

The actual video preview, and the filmstrip preview.

3. At what percentage of a VIDEO file does AXIOM Process take still frames to create the filmstrip preview?

Every 10%

4. Magnet.AI can search for and categorize pictures within the case. Name five of the current categories searched for.

Process > Categorize Pictures with Magnet.AI: Possible weapons, Possible drugs, Militants, Vehicles, Human faces, etc.

5. Which keyboard button can be used to grade all visible uncategorized images?

The + key. The – key will remove a category from one image.

MODULE 11: MOBILE ARTIFACT ANALYSIS

1. Name two different types of information that may be entered in the OPTIONS in AXIOM Process to help decrypt Chat data.



MAGNET AXIOM EXAMINATIONS (AX200)

© 2022 Magnet Forensics Inc. All rights reserved. May not be copied or reproduced without the written permission of Magnet Forensics Inc.

Reviewing different applications will produce different answers but some examples are the application password and email address.

2. What free Magnet AXIOM tool can help you discover user information to gain access to otherwise encrypted data?

The AXIOM Wordlist Generator, which can be downloaded from the Magnet support portal.

3. What two Magnet.AI features can be enabled for searching chat artifacts?

Sex-related chats, and Grooming/Luring chats.

4. What is the name of the view in the Artifacts Explorer that displays chat messages in a threaded format?

Conversation view

5. What is the name of the Your Phone database that provides most of the artifacts in AXIOM?

Phone.db

6. What built in AXIOM tool is available in the File System Explorer to assist with viewing databases?

SQLite Viewer

MODULE 12: CLOUD

1. List some of the cloud platforms that AXIOM Cloud can collect data from.

Instagram, Twitter, Snapchat, Apple, and Google. There are a few others.

2. What two authentication methods can AXIOM Cloud use to access data from a cloud account?

Passwords and/or Tokens

3. When collecting Facebook data, are the messages sent via Facebook Messenger available for review? If so, what is the artifact named?

Yes – Cloud Facebook Messenger Messages

4. When obtaining data from a Google account and the Gmail Messages are collected, are any message attachments available to be viewed?

Yes – there is an Attachments card in the Cloud Gmail Messages artifact.

MODULE 13: REPORTING

1. True/False. Exporting in AXIOM can be performed from the Registry View.

False

2. What option from the File System Explorer allows a user to export artifact details from the case?

Right-click, Export details

3. What is the file format for a Project VIC 1.3/2.0 export?

JSON

4. From the File System Explorer, what are the options available for saving files from a case?

Save file / folder to...

Save file / folder to ZIP

5. When a non-licensed user wants to open a portable case, what file can they use to launch the case in AXIOM Examine?

OpenCase.bat

6. What is the name of the HTML file that will launch the case report?

Report.html



7. In the HTML version of the case report, what features can assist the viewer in managing the listed artifacts?

Filtering, sorting, and searching



