



MAGNET FORENSICS TRAINING

# Magnet Forensics Digital Investigator

STUDENT MANUAL

Copyright © 2023 Magnet Forensics  
Magnet Forensics Digital Investigator – Training  
V2309

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](http://magnetforensics.com)

© 2023 Magnet Forensics Inc. All rights reserved. Magnet Forensics®, 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

<b>INTENDED AUDIENCE AND COURSE SUMMARY</b> .....	<b>VI</b>
<b>CASE SCENARIO</b> .....	<b>VI</b>
<b>MODULE 1: COURSE INTRODUCTION AND PORTABLE CASE OVERVIEW</b> .....	<b>2</b>
LEARNING OBJECTIVES AND GOALS: .....	3
MAGNET FORENSICS PORTABLE CASE COURSE INTRODUCTION .....	4
COURSE OUTLINE .....	5
SYSTEM REQUIREMENTS .....	7
GETTING STARTED WITH A PORTABLE CASE .....	7
TROUBLESHOOTING .....	9
RESOURCES.....	10
<b>MODULE 2: CASE DASHBOARD</b> .....	<b>14</b>
LEARNING OBJECTIVES AND GOALS: .....	15
CASE DASHBOARD .....	16
CASE OVERVIEW .....	17
<i>Case Summary Notes</i> .....	17
<i>Case Processing Details</i> .....	17
<i>Case Information</i> .....	17
<i>Evidence Overview</i> .....	18
<i>Artifact Categories (Places to Start)</i> .....	18
<i>Tags and Comments (Places to Start)</i> .....	19
<i>Identifier Matches (Places to Start)</i> .....	19
<i>CPS Data Matches (Places to Start)</i> .....	20
<i>Magnet.AI Categorization (Places to Start)</i> .....	20
<i>Keyword Matches (Places to Start)</i> .....	21
<i>Potential Cloud Evidence Leads (Places to Start)</i> .....	21
<i>Media Categorization (Places to Start)</i> .....	21
<i>Profiles (Places to Start)</i> .....	22
EVIDENCE SOURCES .....	22
INSIGHTS .....	23
STUDENT EXERCISE .....	25
<b>MODULE 3: ARTIFACTS EXPLORER</b> .....	<b>28</b>
LEARNING OBJECTIVES AND GOALS: .....	29
WHAT ARE ARTIFACTS? .....	30
ARTIFACTS EXPLORER LAYOUT .....	31
<i>Navigation Pane</i> .....	31
<i>Evidence Pane</i> .....	32
<i>Details Pane</i> .....	33
<i>Tags, Profiles, and Media Categories Pane</i> .....	34
<i>Filters Bar</i> .....	34
<i>Search Box</i> .....	35
STUDENT EXERCISE .....	37
<b>MODULE 4: TIMELINE EXPLORER</b> .....	<b>40</b>
LEARNING OBJECTIVES AND GOALS: .....	41
TIMELINE EXPLORER .....	42
<i>Timeline Graph</i> .....	42
<i>Evidence Pane</i> .....	43
<i>Details Pane</i> .....	43
<i>TIPS FOR NAVIGATING THE TIMELINE GRAPH</i> .....	44
STUDENT EXERCISE .....	45



<b>MODULE 5: OVERVIEW OF ARTIFACTS</b> .....	<b>50</b>
LEARNING OBJECTIVES AND GOALS:.....	51
REFINED RESULTS.....	52
<i>Cloud Passwords and Tokens, Passwords and Tokens, &amp; User Accounts</i> .....	52
<i>Google Searches &amp; Parsed Search Queries</i> .....	53
<i>Classifieds URLs</i> .....	53
<i>Facebook URLs</i> .....	53
<i>Identifiers - People</i> .....	53
STUDENT EXERCISE – REFINED RESULTS.....	54
WEB RELATED.....	55
<i>iOS Safari Recent Search Terms</i> .....	55
<i>Safari History</i> .....	55
STUDENT EXERCISE – WEB RELATED.....	55
COMMUNICATION.....	56
<i>Apple Contacts</i> .....	56
<i>iOS Call Logs</i> .....	56
<i>iOS iMessage/SMS/MMS</i> .....	56
STUDENT EXERCISE – COMMUNICATION.....	57
SOCIAL NETWORKING.....	57
<i>Instagram Direct Messages</i> .....	57
<i>iOS Tinder Messages</i> .....	57
STUDENT EXERCISE – SOCIAL NETWORKING.....	58
MEDIA.....	58
<i>iOS Snapshots</i> .....	58
<i>Live Photos &amp; Photos Media Information</i> .....	58
<i>Pictures</i> .....	59
<i>Videos</i> .....	59
STUDENT EXERCISE – MEDIA.....	60
EMAIL & CALENDAR.....	60
<i>Apple Mail</i> .....	60
<i>Calendar Events</i> .....	60
STUDENT EXERCISE – EMAIL & CALENDAR.....	61
DOCUMENTS.....	62
<i>Apple Notes</i> .....	62
STUDENT EXERCISE – DOCUMENTS.....	62
APPLICATION USAGE.....	63
<i>Installed Applications</i> .....	63
<i>iOS Device Information</i> .....	63
<i>KnowledgeC</i> .....	63
STUDENT EXERCISE – APPLICATION USAGE.....	64
OPERATING SYSTEM.....	65
<i>Apple Accounts &amp; Owner Information</i> .....	65
<i>Cell Tower Locations</i> .....	65
<i>PowerLog</i> .....	65
STUDENT EXERCISE – OPERATING SYSTEM.....	66
ENCRYPTION & CREDENTIALS.....	67
<i>Apple Keychain</i> .....	67
STUDENT EXERCISE – ENCRYPTION & CREDENTIALS.....	67
CONNECTED DEVICES.....	68
<i>Apple Health</i> .....	68
<i>Find My</i> .....	68
STUDENT EXERCISE – CONNECTED DEVICES.....	69
LOCATION & TRAVEL.....	70
<i>Cached Locations</i> .....	70
<i>Significant Locations &amp; Significant Locations Visits</i> .....	70
<i>WiFi Locations</i> .....	70
STUDENT EXERCISE – LOCATION AND TRAVEL.....	72



<b>MODULE 6: REPORTING.....</b>	<b>76</b>
LEARNING OBJECTIVES AND GOALS: .....	77
REPORTING INTRODUCTION.....	78
EXPORT / REPORT DETAILS.....	79
ITEMS TO INCLUDE.....	79
LEVEL OF DETAIL .....	79
EXCEL REPORT .....	80
PDF REPORT .....	81
HTML REPORT.....	83
STUDENT EXERCISE – CREATING REPORTS.....	85
EXCEL REPORT .....	85
PDF REPORT .....	85
WE WANT TO CREATE A .PDF OF ALL OF THE IOS MESSAGES BETWEEN CASEY NEWTON AND CHRIS AUSTIN .....	85
HTML REPORT .....	86
WE WANT TO CREATE A HTML REPORT OF ALL ITEMS THAT WE TAGGED DURING THE ANALYSIS. ....	86
<b>MODULE 7: MAGNET OUTRIDER.....</b>	<b>90</b>
LEARNING OBJECTIVES AND GOALS: .....	91
MAGNET OUTRIDER INTRODUCTION .....	92
KEY FEATURES OF OUTRIDER .....	92
UNDERSTANDING SYSTEM CHANGES .....	93
Changes Made to Windows Systems.....	93
Changes Made to macOS Systems .....	93
PREPARING A MAC DEVICE TO BE SCANNED.....	94
PREPARING AN ANDROID DEVICE TO BE SCANNED .....	95
ENCRYPTION DETECTION (WINDOWS SCANS ONLY) .....	95
CONFIGURING A SCAN TEMPLATE .....	95
SCANNING A WINDOWS SYSTEM.....	96
SCANNING A macOS SYSTEM .....	98
SCANNING AN ANDROID DEVICE .....	100
REVIEWING SCAN RESULTS.....	102
Understanding “No Hits Round” Results.....	102
View the Scan Report .....	103
<b>MODULE 8: PRACTICAL EXERCISE.....</b>	<b>106</b>
LEARNING OBJECTIVES AND GOALS: .....	107
PRACTICAL EXERCISE DESCRIPTION .....	108
PRACTICAL EXERCISE PORTABLE CASE .....	108
<b>APPENDIX - STUDENT EXERCISE ANSWERS .....</b>	<b>112</b>
MODULE 2: STUDENT EXERCISE .....	112
MODULE 3: STUDENT EXERCISE .....	112
MODULE 4: STUDENT EXERCISE .....	113
MODULE 5: STUDENT EXERCISE – REFINED RESULTS .....	113
MODULE 5: STUDENT EXERCISE – WEB RELATED.....	114
MODULE 5: STUDENT EXERCISE – COMMUNICATION .....	114
MODULE 5: STUDENT EXERCISE – SOCIAL NETWORKING .....	115
MODULE 5: STUDENT EXERCISE – MEDIA .....	115
MODULE 5: STUDENT EXERCISE – EMAIL & CALENDAR .....	116
MODULE 5: STUDENT EXERCISE – DOCUMENTS .....	116
MODULE 5: STUDENT EXERCISE – APPLICATION USAGE.....	117
MODULE 5: STUDENT EXERCISE – OPERATING SYSTEM.....	117
MODULE 5: STUDENT EXERCISE – CONNECTED DEVICES.....	118
MODULE 5: STUDENT EXERCISE – LOCATION AND TRAVEL .....	119



## INTENDED AUDIENCE AND COURSE SUMMARY

This is an introductory course designed for stakeholders, such as investigators, attorneys, and subject matter experts, who are responsible for reviewing digital forensics case data that has been provided by a digital forensics examiner in the form of a Magnet Forensics Portable Case. Students will learn and develop skills related to a Portable Case, including Portable Case navigation, searching and filtering data, analyzing artifacts, generating reports, and distributing findings. The course is designed for students who have limited, or no previous education or training related to digital forensics. Most of the instruction in this course is hands-on and requires that students be familiar with basic computer operation and navigation.

## CASE SCENARIO

This is a homicide investigation. The victim in the case, Christopher Austin, was killed when a drone hovered above his vehicle and detonated a bomb. During the investigation, two suspects were identified: Casey Newton and Ryan Jennings. Newton and Jennings admit to dating, but both deny being involved in the homicide. Moreover, both deny knowing Christopher Austin. After serving multiple search warrants, and seizing multiple items of evidence, you were provided with Portable Cases for the following items:

Item Number	Description	Owner
02-01	Apple iPhone 11. Full File System acquisition	Casey Newton – Suspect
03-01	Samsung Galaxy S20. Full File System acquisition	Christopher Austin - Victim





# MODULE 1

Course Introduction and Portable Case Overview

# MODULE 1: COURSE INTRODUCTION AND PORTABLE CASE OVERVIEW

- Magnet Forensics Portable Case Course Introduction
- Course Outline
- System Requirements
- Getting Started with a Portable Case
- Troubleshooting
- Resources





## **LEARNING OBJECTIVES AND GOALS:**

This module offers a comprehensive introduction to the course, providing students with a clear understanding of its purpose and significance. The course outline serves as a structured guide, ensuring a well-defined learning path by providing an overview of the topics covered. Students will become familiar with the system requirements, enabling them to effectively utilize the Portable Case. The module also focuses on developing troubleshooting skills to tackle potential challenges that may arise. Moreover, participants will be introduced to various available resources, empowering them to enhance their learning experience and further expand their knowledge of utilizing Portable Cases.



## MAGNET FORENSICS PORTABLE CASE COURSE INTRODUCTION

This course is specifically designed to introduce stakeholders, such as investigators, attorneys, and subject matter experts, to the utilization and review of digital forensics case data provided in the form of a Magnet Forensics Portable Case. It aims to equip students with the necessary skills to navigate, search, filter, analyze artifacts, generate reports, and distribute findings using the Portable Case.

Throughout the course, students will gain an understanding of the functionalities and capabilities of the Magnet Forensics Portable Case. You will learn how to efficiently navigate the interface, locate and retrieve specific data, and apply filtering techniques to narrow down your search results. By mastering these skills, students will be able to effectively identify relevant digital evidence for their investigations.

An important aspect of the course is the analysis of artifacts. Students will delve into the examination of various digital artifacts, such as metadata, internet browsing history, communication logs, and media. You will learn how to interpret these artifacts to reconstruct timelines, identify user activities, and uncover crucial evidence that may contribute to the overall investigation.

Furthermore, students will be guided on generating comprehensive reports based on their findings. You will understand the importance of documenting the investigative process, maintaining a chain of custody, and ensuring the accuracy and reliability of reports. The course emphasizes the significance of clear and concise reporting to effectively communicate findings to relevant parties, including legal professionals and other stakeholders.

It's worth noting that this course is tailored for students who have limited or no previous education or training in the field of digital forensics. However, basic computer operation and navigation skills are assumed, as most of the instruction involves hands-on practical exercises. Students will be required to interact with the Portable Case interface and perform various tasks using the provided tools and resources.

By the end of the course, students will have acquired fundamental skills in utilizing the Magnet Forensics Portable Case for reviewing digital forensics case data. You will be equipped to contribute effectively to investigations, legal proceedings, and other scenarios where the examination of digital evidence is essential.



## COURSE OUTLINE

Module 1: Course Introduction and Portable Case Overview

Module 2: Case Dashboard

Module 3: Artifacts Explorer

Module 4: Timeline Explorer

Module 5: Overview of Artifacts

Module 6: Reporting

Module 7: Magnet Outrider

Module 8: Practical Exercise

### MODULE 1: COURSE INTRODUCTION AND PORTABLE CASE OVERVIEW

Module 1 serves as an introduction to the Magnet Forensics Portable Case course. It covers the purpose and significant of the training, provides a structured course outline, presents system requirements, teaches participants how to get started with a Portable Case, develops troubleshooting skills, and highlights available resources for further learning.

### MODULE 2: CASE DASHBOARD

Module 2 introduces the student to the Case Dashboard of a Portable Case. The Case Dashboard is a graphical overview of the case, including the case summary, evidence overview, and places to start. This module includes exercises to reinforce the learning objectives.

### MODULE 3: ARTIFACTS EXPLORER

Module 3 introduces the student to the Artifacts Explorer of a Portable Case. Artifacts Explorer is a graphical view of all artifacts that have been recovered from the evidence. Students will learn how to navigate Artifacts Explorer, enabling them to effectively review information in a case. This will include creating tags, creating profiles, filtering data, and searching data. This module includes exercises to reinforce the learning objectives.

### MODULE 4: TIMELINE EXPLORER

Module 4 introduces the student to the Timeline Explorer of a Portable Case. Timeline Explorer is a visualization of time in an interactive graph where the student can examine specific timeframes, identify spikes in activity, focus on specific dates, and establish patterns of behavior. This module includes exercises to reinforce the learning objectives.

### MODULE 5: OVERVIEW OF ARTIFACTS

Module 5 provides a comprehensive exploration of significant digital artifacts commonly encountered in forensic investigations. This module covers a range of key points, including refined search results to efficiently extract relevant evidence. It delves into web-related artifacts, such as browsing history and downloaded files, along with communication artifacts, encompassing chat conversations and call logs. The module also examines artifacts from social networking platforms, media files, email and calendar data, documents, application usage, operating system artifacts, encryption and credential-related evidence, connected devices, and location and travel



information. By studying these artifacts, participants will gain a thorough understanding of the essential digital evidence sources and be equipped with valuable insights to conduct effective digital forensic investigations. This module includes exercises to reinforce the learning objectives.

#### MODULE 6: REPORTING

Module 6 explores the functionality of reporting within a Portable Case, equipping participants with the knowledge and skills to generate comprehensive and impactful reports in their investigations. This module covers the importance of reporting in documenting findings, supporting legal proceedings, and communicating results to stakeholders. Participants will learn how to utilize the reporting features within the Portable Case to create professional and customized reports that effectively present evidence and analysis. The module provides guidance on selecting relevant artifacts, organizing information, incorporating visual elements, and ensuring the accuracy and integrity of the generated reports. By mastering the art of reporting, participants will enhance their ability to convey their investigative findings clearly, concisely, and persuasively. This module includes exercises to reinforce the learning objectives.

#### MODULE 7: MAGNET OUTRIDER

Module 7 introduces the student to Magnet Forensics Outrider. Outrider is a powerful tool for quickly triaging and scanning Mac and Windows computers, external drives, and Android mobile devices. It provides automated insights and preconfigured artifact categories that enable both examiners and non-technical stakeholders to confidently use the software. With Outrider, investigators can swiftly scan computers and Android devices to automatically uncover various types of data such as SMS/MMS messages, illicit apps, device ID, contact lists, and call logs. The software is designed for speed and simplicity, offering a user-friendly interface and easy setup, allowing users to start running scans in the field or lab with just a few clicks.

#### MODULE 8: PRACTICAL EXERCISE

Module 8 offers a comprehensive practical exercise utilizing a new Portable Case. This provides an opportunity for students to reinforce their understanding of the course material, ensuring they have a solid grasp of the concepts and techniques covered. Participants will engage in a practical exercise where they independently examine a new piece of digital evidence using a Portable Case. This exercise allows students to apply their newly acquired skills to another piece of evidence, enhancing their confidence and proficiency in utilizing the Portable Case for digital forensic investigations. By conducting a hands-on practical experience, this module ensures that participants are well-prepared to effectively analyze and extract digital evidence using the Portable Case in their future investigations.

Each module of instruction during the course will have a similar structure. At the beginning of the module, the learning objectives will be identified and explained. Following the learning objectives, the content of the module will be presented through a combination of presentations and open discussions. During the presentation of materials, there will be various exercises. These exercises are designed to allow the student to demonstrate their knowledge of the material and skill navigating the program. At the conclusion of each module, there are Student Exercises. These exercises are designed to test the students' understanding and application of the learning concepts.



## SYSTEM REQUIREMENTS

To open and view a Portable Case, you don't need to have the complete Magnet Forensics AXIOM program installed on your computer. The Portable Case itself contains all the necessary files and applications to run without the need for AXIOM installation. However, to run AXIOM Examine within the Portable Case, certain dependencies are required. If these dependencies are not already present on your system, they will be automatically installed when you open the Portable Case.

When running a Portable Case, the following are the minimum system requirements. However, if the Portable Case is large and contains a substantial amount of data, a more powerful system might be necessary. Having system resources that exceed the minimum requirements will enhance the performance of the Portable Case, including tasks such as viewing, searching, and filtering.

Minimum Requirements	
Operating System	Windows 8.1 or later. 64-bit version
Software Framework	.NET version 4.8.0 or later
Visual C++ Visual Studio Redistribution Package	2008, 2012, 2013 or later. Packages can be downloaded from <a href="http://www.microsoft.com">www.microsoft.com</a> if needed
Processor	Intel Core i5 or equivalent. 4 logical cores
Memory	8 GB RAM
Disk Space	10 GB free disk space
Graphics Card	Supported graphics card with at least 2 GB of video memory

FIGURE 1-1: SYSTEM REQUIREMENTS

## GETTING STARTED WITH A PORTABLE CASE

When a forensics examiner generates a Portable Case in AXIOM, it results in the creation of a folder named "PortableCase." This folder encompasses several essential items that are crucial for the functionality of the Portable Case. Here's a breakdown of what you will find within the PortableCase folder:



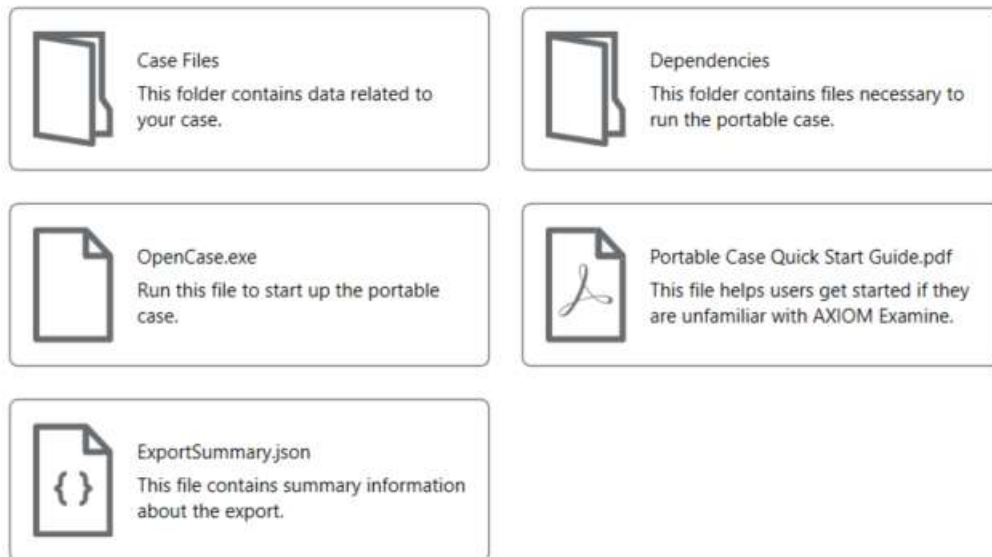


FIGURE 1-2: CONTENTS OF A PORTABLE CASE FOLDER

- **Case Files:** This folder contains all the data and case-specific files relevant to the investigation. It includes the required databases and any attachments associated with the case.
- **Dependencies:** Within this folder, you will find all the dependencies that are essential for the Portable Case to run smoothly. These dependencies ensure that the required software components and libraries are present to support the functionality of AXIOM and its associated features within the Portable Case. Among the items in this folder is the folder /Sandbox which is created when first opening the Portable Case.
- **ExportSummary:** This file serves as a comprehensive summary of the export process from AXIOM to the Portable Case. It provides a concise overview of the data that has been included and any pertinent details related to the export.
- **OpenCase:** The "OpenCase.exe" file is the executable that allows users to open and access the Portable Case. By executing this file, the examiner can launch the Portable Case environment and begin working on the investigation, utilizing the contained data and tools.
- **Portable Case Quick Start Guide:** To assist users in getting started with the Portable Case, a Quick Start Guide is included. This document provides fundamental information and instructions on how to navigate and utilize the features within the Portable Case. It serves as a helpful reference for users who are new to working with Portable Cases or need a quick refresher on its functionalities.

Name	Date modified	Type	Size
Case Files	7/15/2023 6:41 AM	File folder	
Dependencies	7/6/2023 4:40 PM	File folder	
ExportSummary	7/6/2023 4:39 PM	JSON File	1 KB
OpenCase	7/6/2023 4:39 PM	Application	26,556 KB
Portable Case Quick Start Guide	6/7/2023 6:15 PM	PDF Document	67 KB

FIGURE 1-3: CONTENTS OF PORTABLECASE FOLDER



To open a Portable Case, double-click on the file "OpenCase.exe." This will initiate the opening process. Once opened, the Portable Case will display the Case Dashboard. The Case Dashboard serves as the initial point of entry and provides a comprehensive overview of the Portable Case, allowing for seamless navigation and exploration of case contents.

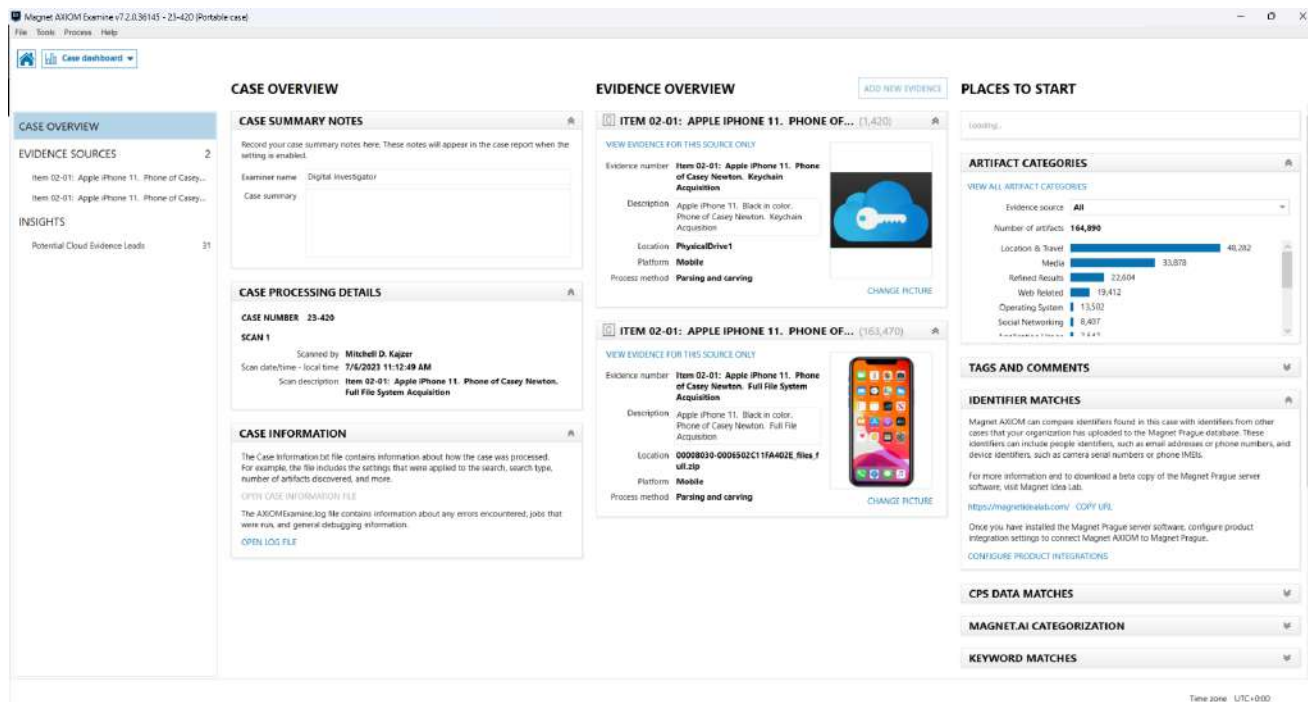


FIGURE 1-4: CASE DASHBOARD

## TROUBLESHOOTING

When working with Portable Cases, the most common issue that users encounter is the failure of a case to open or encountering an error after executing the "OpenCase.exe" file. If you encounter this situation, there are a few possible solutions you can try.

1. Copy the PortableCase folder to your local computer: If you are attempting to open the Portable Case from an external hard drive, thumb drive, or DVD, it is recommended to copy the entire PortableCase folder to your local computer drive. By executing the "OpenCase.exe" file from your local drive, the program can write essential information to a Sandbox folder within the Portable Case directory. Additionally, storing the Portable Case locally on your computer enhances performance since it eliminates the need for accessing external resources.
2. Delete the previous user's Sandbox folder: In situations where the Portable Case was previously opened by another user, it may be necessary to delete the Sandbox folder created for that specific user. The Sandbox folder is located within the Dependencies folder of the Portable Case. To resolve this, navigate to the Dependencies folder and locate the folder named "Sandbox." Delete this folder, and then proceed to execute the "OpenCase.exe" file once again.

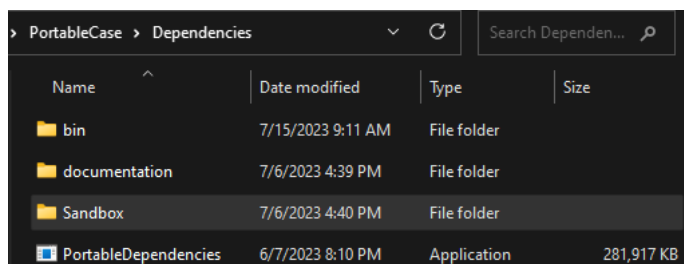


FIGURE 1-5: SANDBOX FOLDER

By implementing these recommended solutions, you can effectively troubleshoot and resolve most issues commonly experienced when opening Portable Cases. However, if the problem persists even after attempting these steps, it is recommended that you contact to your Office of Information Technology for further assistance. It is possible that your computer may have specific security restrictions or limitations imposed by your organization, which could hinder the successful execution of the Portable Case. Alternatively, you can seek support and request assistance through Magnet Forensics Support at [support.magnetforensics.com](mailto:support.magnetforensics.com).

## RESOURCES

Within the Portable Case, there are two resources available to assist the user with the Portable Case and the contents of the case. The User Guide and Artifact Reference are both located under the menu Help > Documentation.

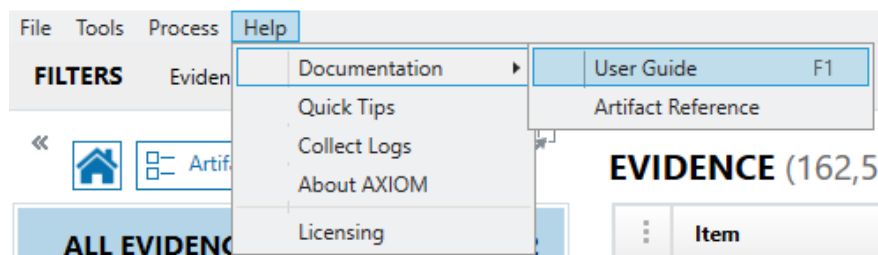


FIGURE 1-6: USER GUIDE AND ARTIFACT REFERENCE

The User Guide provides comprehensive information on how to examine artifacts within the Portable Case. It covers various topics essential to the investigative process, including tagging, creating profiles, conducting searches, applying filters, and exporting artifacts. By referring to the User Guide, users can gain a thorough understanding of these functionalities and effectively utilize them to analyze the artifacts contained within the Portable Case. The User Guide is saved within the Dependencies folder of the Portable Case and does not require internet connectivity to view.

The Artifact Reference serves as a comprehensive list of applications from which Magnet AXIOM can retrieve data. This data, once recovered, is presented in the form of artifacts. An artifact can be defined as a structured representation of data that Magnet AXIOM utilizes to organize and present the evidence it uncovers. Each artifact consists of a collection of attributes, each with its own data type and the potential to contain specific information (e.g., names, timestamps, locations, messages, etc.).

This Artifact Reference effectively categorizes artifacts based on the platform they belong to (iOS, Android, OS X / Windows, Windows Phone) as well as their application type (e.g., chat, document, social media). By examining the attributes associated with each artifact, one can begin to piece together a comprehensive narrative regarding users' online activities and their communication patterns with others. The Artifact Reference is an online resource and requires internet connectivity to view.









# MODULE 2

Case Dashboard

## MODULE 2: CASE DASHBOARD

- Case Dashboard
- Case Overview
- Evidence Sources
- Insights
- Student Exercise



## **LEARNING OBJECTIVES AND GOALS:**

The primary learning objective and goal of this module is to ensure students become familiar with the Case Dashboard in a Portable Case. The Case Dashboard offers a visual representation of the case, featuring essential components such as Case Overview, Evidence Overview, Places to Start, and Insights. Throughout the module, each of these topics will be thoroughly presented and discussed. By the end of this module, students will possess a comprehensive understanding of the Case Dashboard's various elements, empowering them to navigate the Portable Case efficiently and effectively, leveraging the insights provided by the Case Dashboard.



## CASE DASHBOARD

When you open a Portable Case, it will automatically open to the Case Dashboard. The Case Dashboard is one of three explorers accessible in a Portable Case. By clicking on the drop-down menu for the Case Dashboard, you can choose to switch to the Artifacts Explorer or Timeline Explorer. The remaining explorers are grayed out and unavailable because they require a full AXIOM license to be activated.

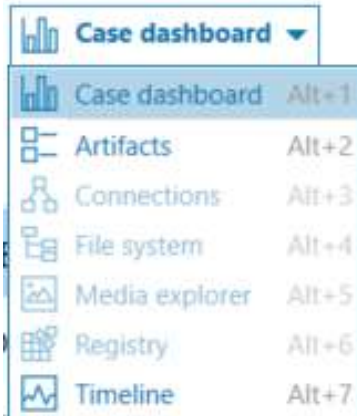


FIGURE 2-1: PORTABLE CASE EXPLORERS

The Case Dashboard in a Portable Case is a centralized graphical interface that acts as the main starting point for investigators. It provides a comprehensive overview of the case and enables access to various case components and features. This visual and informational hub offers key information and functionalities to aid in case management and analysis. By serving as a holistic view of the case, the Case Dashboard facilitates efficient case navigation, data exploration, and analysis for digital forensic investigators.

The Case Dashboard is comprised of two panes, the Navigation Pane and the Evidence Pane. Clicking on a category in the Navigation Pane will display the results in the Evidence Pane.

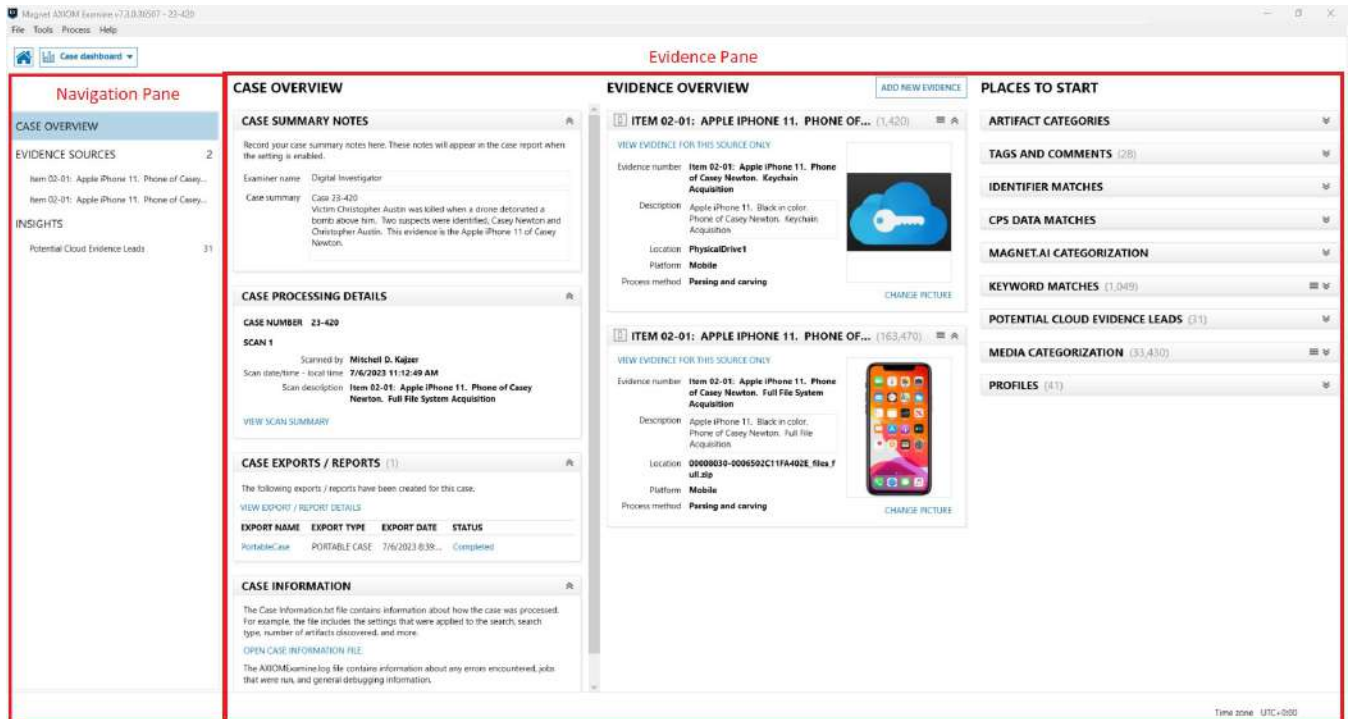


FIGURE 2-2: CASE DASHBOARD

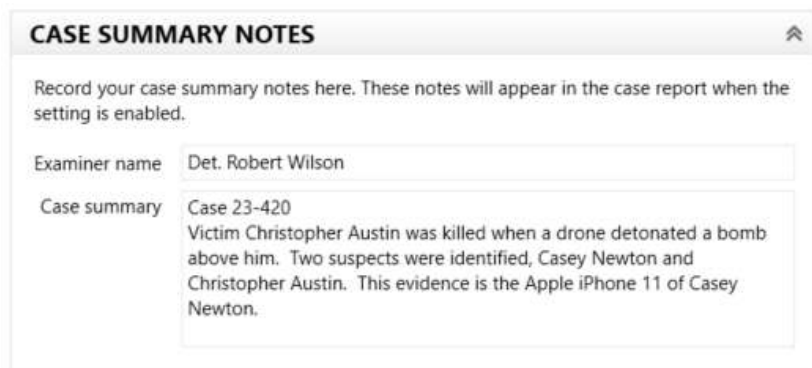


## CASE OVERVIEW

The Case Overview section provides a brief overview of the case, including relevant details such as case name, case number, examiner name, and case description. It helps investigators quickly identify and refer to essential case information. The Evidence Pane for Case Overview contains the following evidence items:

### Case Summary Notes

The Case Summary Notes section includes editable fields for the Examiner Name and a summary of the case investigation. These fields can be updated to include relevant information specific to your investigation. As an investigator, you can modify and add details within these sections to ensure that the Case Summary accurately reflects the necessary information for your case.



**CASE SUMMARY NOTES**

Record your case summary notes here. These notes will appear in the case report when the setting is enabled.

Examiner name: Det. Robert Wilson

Case summary: Case 23-420  
Victim Christopher Austin was killed when a drone detonated a bomb above him. Two suspects were identified, Casey Newton and Christopher Austin. This evidence is the Apple iPhone 11 of Casey Newton.

FIGURE 2-3: CASE SUMMARY NOTES

### Case Processing Details

The Case Processing Details section provides information pertaining to the scanning process of the digital evidence with AXIOM. It includes essential details such as the case number, forensic examiner name, date and time of the scanning, and a description of the scan. It's important to note that this information is not editable once the scanning process is completed. The Case Processing Details serve as a record and reference of the specific scan performed, ensuring transparency and accuracy in the forensic investigation process.



**CASE PROCESSING DETAILS**

**CASE NUMBER** 23-420

**SCAN 1**

Scanned by **Mitchell D. Kajzer**

Scan date/time - local time **7/6/2023 11:12:49 AM**

Scan description **Item 02-01: Apple iPhone 11. Phone of Casey Newton. Full File System Acquisition**

FIGURE 2-4: PROCESSING DETAILS

### Case Information

The Case Information section includes information on the file Case Information.txt along with a link to the file AXIOMExamine.log. The log file contains valuable information regarding encountered errors, executed jobs, and general debugging details. However, it is important to note that the Case Information.txt file is not directly viewable within the Portable Case. To access and review the Case Information File, you need to contact the forensic examiner responsible for the case. They will be able to provide you with the information contained within the Case Information File.



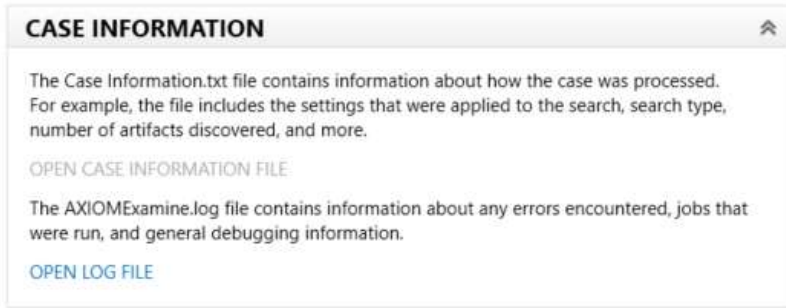


FIGURE 2-5: CASE INFORMATION

## Evidence Overview

The Evidence Overview section provides a comprehensive summary of the evidence sources within the case. Each evidence item added to the case is listed. The Evidence number typically displays the name of the evidence item, unless modified by the examiner during processing. Additionally, examiners have the option to include a Description and upload or change a picture for each individual item. Within each entry, there is a link to "VIEW EVIDENCE FOR THIS SOURCE ONLY." Selecting this link transitions to the Artifact Explorer in AXIOM Examine, automatically applying a filter to display only the artifacts sourced from that specific evidence item. This feature enables investigators to focus their analysis and easily explore the artifacts associated with each evidence source.

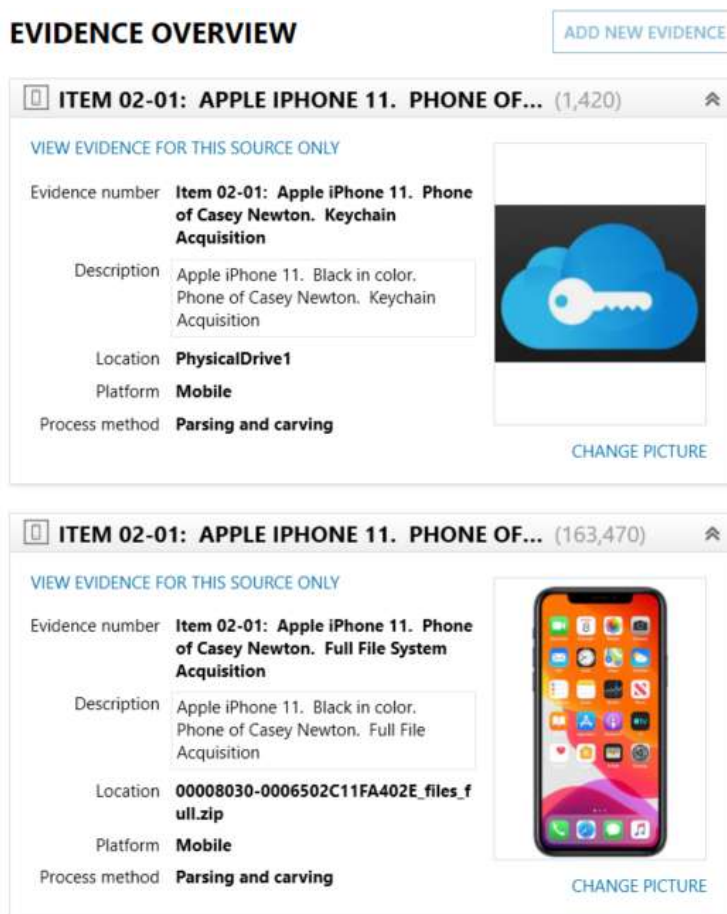


FIGURE 2-6: EVIDENCE OVERVIEW

## Artifact Categories (Places to Start)

The Artifact Categories section presents a concise summary of the quantity of artifacts within each category of information. The categories are listed in descending order, starting from the largest artifact category and descending to the smallest. By clicking on a specific artifact category, the user is seamlessly directed to the Artifact explorer. Upon transition, a filter is automatically applied to display only the artifacts belonging to the selected





category. This feature streamlines the investigative process, allowing users to focus specifically on the artifacts within their desired category for further analysis and examination.

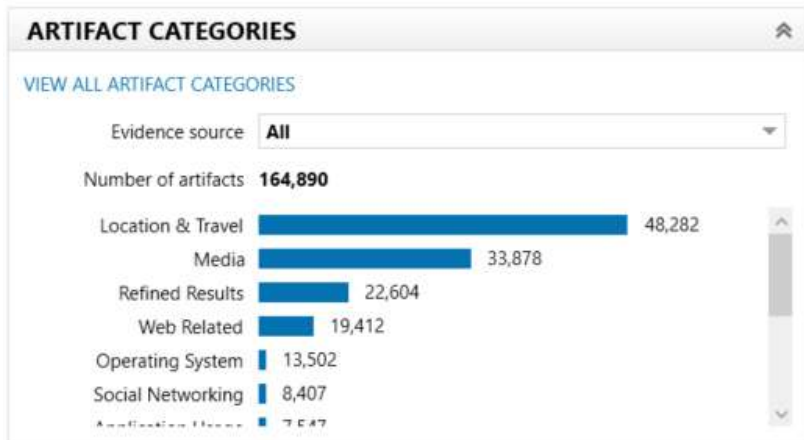


FIGURE 2-7: ARTIFACT CATEGORIES

### Tags and Comments (Places to Start)

The Tags and Comments section displays tags that were assigned (if any) to artifacts by the forensic examiner before generating the Portable Case. This area will dynamically change as tags are added to the case. This section includes the tag name and the number of artifacts associated with each tag. By clicking on the number of tags, AXIOM will transition to the Artifact Explorer. Upon switching, a filter will be automatically applied to display only the artifacts tagged with the selected tag.



FIGURE 2-8: TAGS AND COMMENTS

### Identifier Matches (Places to Start)

AXIOM offers the capability to compare identifiers discovered within a case with identifiers from other cases uploaded to the Magnet Prague database by the forensic examiner. These identifiers encompass various types, including people identifiers like email addresses or phone numbers, as well as device identifiers such as camera serial numbers or phone IMEIs. It is important to note that for information in Identifier Matches to be populated, the forensic examiner must be utilizing the Magnet Prague product. This functionality enhances the ability to establish connections and identify potential correlations between cases, leveraging the shared information in the Magnet Prague database.



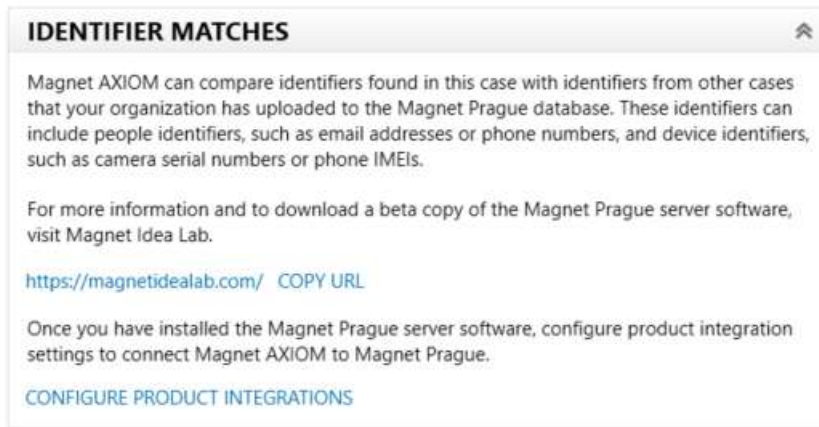


FIGURE 2-9: IDENTIFIER MATCHES

### CPS Data Matches (Places to Start)

The Child Protection System (CPS) is designed to gather online data that monitors peer-to-peer, computer-to-computer interactions, including IP addresses, file hashes, user GUIDs, and other relevant information. Its purpose is to identify individuals who exploit the internet to harm children. When a forensic examiner imports a .csv file into AXIOM Processes and subsequently processes the case, AXIOM automatically identifies and tags evidence that corresponds to the data exported from the CPS. It is important to note that for information in CPS Data Matches to be populated, the forensic examiner must be utilizing the Child Protection System. This functionality enhances the examiner's ability to identify potential matches and evidence related to individuals involved in child exploitation cases.



FIGURE 2-10: CPS DATA MATCHES

### Magnet.AI Categorization (Places to Start)

Magnet.AI provides the capability to use artificial intelligence to search and categorize artifacts based on various categories, such as drugs, weapons, faces, buildings, and bedrooms. If the forensic examiner ran Magnet.AI during the case processing, any identified matches will be listed in this section. The information displayed includes the applied tag for each category and the corresponding number of artifacts that were identified through Magnet.AI. By clicking on the number of artifacts, AXIOM transitions to the Artifact Explorer. During the transition, a filter is automatically applied to display only the artifacts that match the selected category. This feature streamlines the examination process, allowing investigators to focus on the specific artifacts that match their desired category for further analysis and investigation.



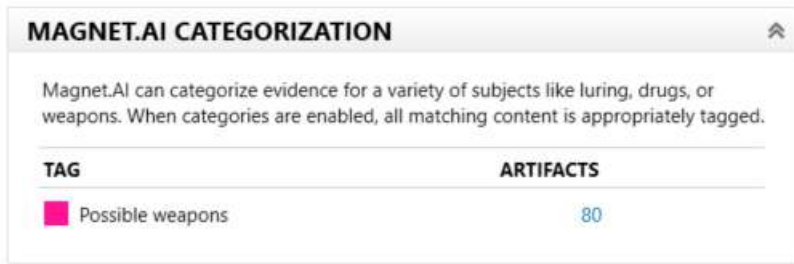


FIGURE 2-11: MAGNET.AI CATEGORIZATION

### Keyword Matches (Places to Start)

During the processing phase, forensic examiners can run keyword searches against the evidence. If keywords were utilized, any corresponding hits will be displayed in the Keyword Matches section. The provided information includes the specific keyword that was searched and the total number of matches found. By clicking on a keyword, AXIOM transitions to the Artifact Explorer. This transition applies an automatic application of a filter, resulting in the display of only the artifacts that match the selected keyword. This functionality enables investigators to conveniently explore and examine artifacts relevant to specific keywords for further analysis and investigation.



FIGURE 2-12: KEYWORD MATCHES

### Potential Cloud Evidence Leads (Places to Start)

During processing, AXIOM conducts searches for user credentials associated with online services like Apple, Facebook, and Google. When a user name is discovered, it is listed in the Potential Cloud Evidence Leads section. This information not only provides investigators with previously unknown account details but also presents a compilation of cloud accounts that potentially hold additional evidence relevant to the investigation. The inclusion of Potential Cloud Evidence Leads assists investigators in identifying accounts that may contain additional evidence related to the investigation.



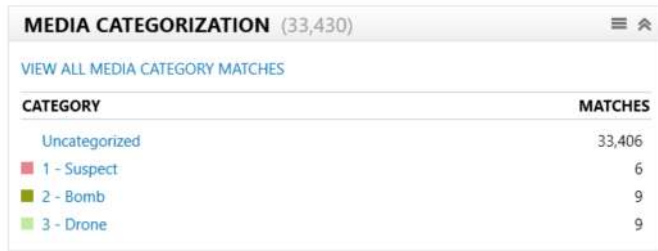
FIGURE 2-13: POTENTIAL CLOUD EVIDENCE LEADS

### Media Categorization (Places to Start)

The Media Categorization section displays the names of media categories that were assigned to artifacts by the forensic examiner prior to generating the Portable Case. Each category is accompanied by the number of artifacts



associated with that specific category. By selecting a category name, AXIOM transitions to the Artifact Explorer. As the transition occurs, a filter is automatically applied to display artifacts that correspond to the chosen media category. This functionality streamlines the investigation process by allowing users to focus on specific media categories and efficiently explore the artifacts relevant to those categories for further analysis and examination.



CATEGORY	MATCHES
Uncategorized	33,406
1 - Suspect	6
2 - Bomb	9
3 - Drone	9

FIGURE 2-14: MEDIA CATEGORIZATION

## Profiles (Places to Start)

A profile is comprised of identifying information that can be attributed to a specific individual. This information includes items such as real names, screen names, social media accounts, phone numbers, and address details. Any artifact that can be linked to a particular person contributes to their profile. By utilizing this collected information, investigators can construct a comprehensive profile on an individual. If the Portable Case contains one or more profiles, they will be listed under the Profiles section. The information displayed includes the name of each profile and the corresponding number of matches associated with that profile. Clicking on a profile name within AXIOM will transition to the artifact explorer. During this transition, a filter will be automatically applied, resulting in the display of only the artifacts specifically linked to the selected profile. This feature allows investigators to focus their analysis on the artifacts directly associated with the profile they are examining.



PROFILE	MATCHES
Ryan Jennings	6,806

FIGURE 2-15: PROFILES

## EVIDENCE SOURCES

In the Navigation Pane of the Portable Case, all the evidence is listed under "Evidence Sources." Clicking on Evidence Sources will display each individual item of evidence in the Evidence Pane. For every evidence item listed, there are multiple links available to the examiner. These links provide the option to either view artifacts exclusively associated with that evidence item or access the detailed information pertaining to that evidence item. This functionality enables examiners to efficiently navigate through the evidence sources, view specific artifacts, and access comprehensive details related to each item of evidence within the Portable Case.



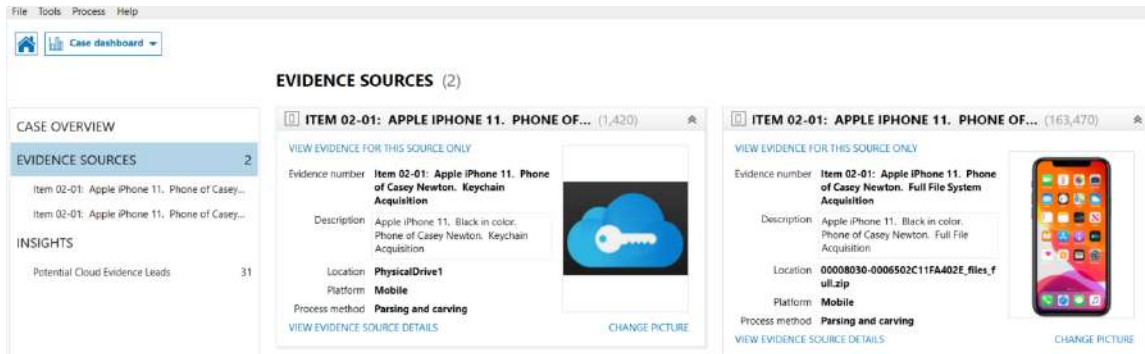


FIGURE 2-16: EVIDENCE SOURCES

By clicking on the individual evidence sources listed in the Navigation Pane, all relevant information associated with that specific item will be displayed in the Evidence Pane. This includes comprehensive details and metadata pertaining to the evidence item. Additionally, the Evidence Pane provides multiple links that allow users to conveniently filter, search, and view artifacts specifically related to the selected evidence source. These links enhance the examiner's ability to explore and analyze artifacts within the context of the chosen evidence source, providing a focused and efficient approach to investigating the Portable Case.

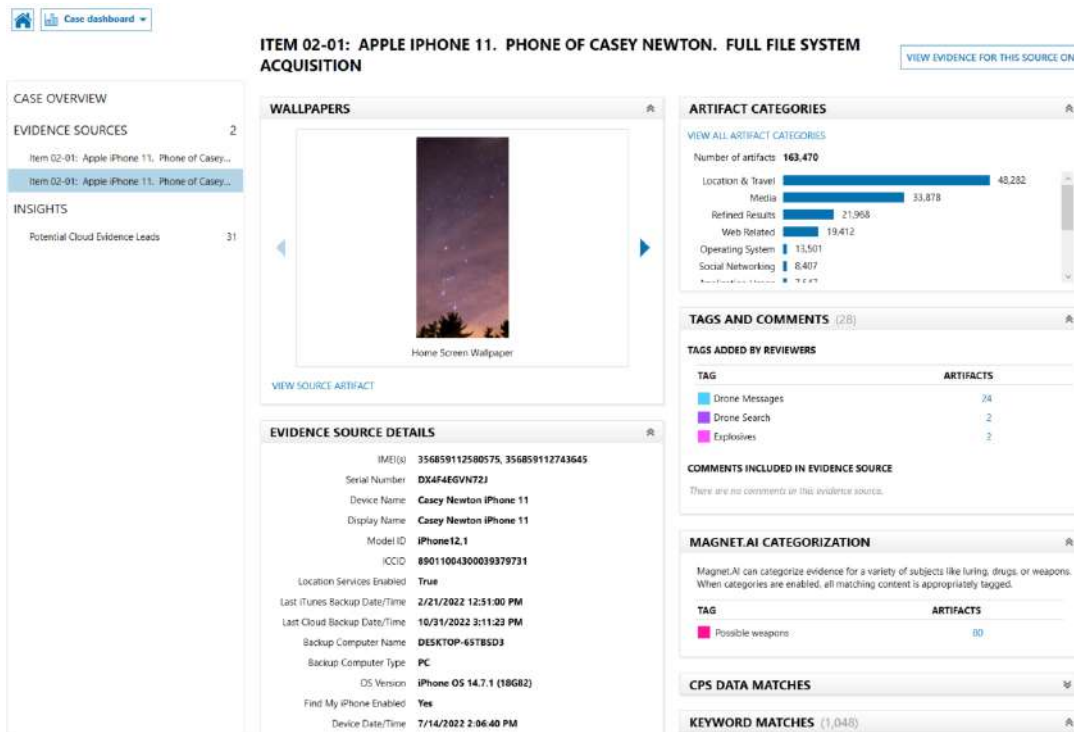


FIGURE 2-17: EVIDENCE ITEM DETAILS

## INSIGHTS

The final option within the Navigation pane of the Case Dashboard is labeled INSIGHTS. Insights primarily encompass Potential Cloud Evidence Leads. During the processing phase, AXIOM searches for any cloud accounts associated with the user. This process retrieves various information such as screen names, email addresses, and passwords linked to these accounts. The Insights section provides comprehensive details about any located cloud accounts, offering valuable information that can aid in obtaining additional evidence to the investigation.

Furthermore, the Insights section offers advanced features that can be triggered. For example, investigators can utilize AXIOM to connect to an online account and download the associated cloud data, subject to proper search authorization. It is important to note that these advanced features require a full AXIOM license and can be



conducted by the forensic examiner who created the Portable Case. These capabilities provide additional avenues for investigation and enhance the examiner's ability to gather relevant evidence from cloud sources within the scope of the case.

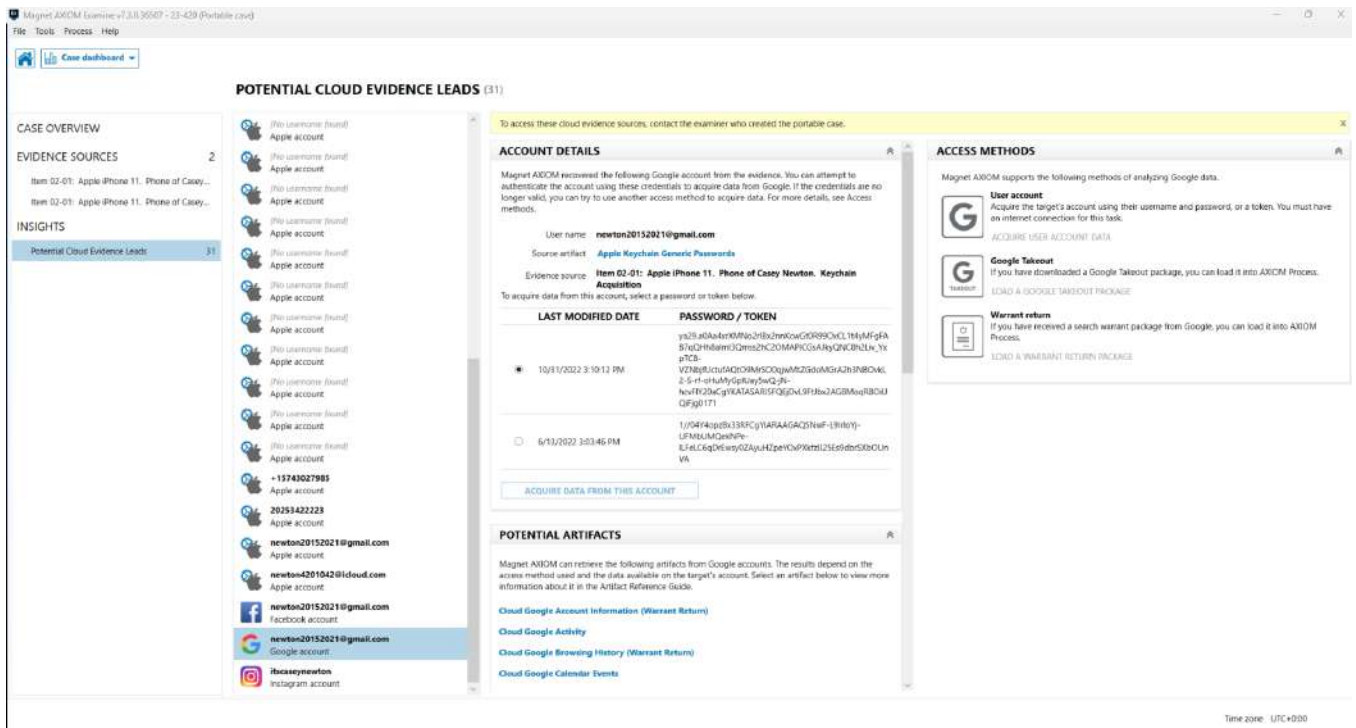


FIGURE 2-18: PLACES TO START



## STUDENT EXERCISE

From the Case Dashboard of the Portable Case, answer the following questions:

1. What are the two items of evidence in the Portable Case?
2. Who is the owner of the phone?
3. What is the phone number for the phone?
4. What is the name of the phone?
5. Are location services enabled on the phone?
6. What is the Apple ID associated with the phone?
7. When was the last time that a cloud backup was done on the phone?
8. What operating system is on the phone?
9. Are location services enabled on the phone?
10. Has the phone ever been backed up to a computer?
11. If so, what is the name of the computer?
12. What is the DSID for the phone?
13. What is the user's Instagram username?
14. What is the user's password for her Instagram account?
15. What is the user's password for her Facebook account?
16. Which artifact category contains the largest number of artifacts?
17. Which drive on the forensic examiner's computer contains the original AXIOM Case? Hint: View the log file.









# MODULE 3

## Artifacts Explorer

## MODULE 3: ARTIFACTS EXPLORER

- What are artifacts?
- Artifacts Explorer Layout
  - Navigation Pane
  - Evidence Pane
  - Details Pane
  - Tag, Profiles, & Media Categories
  - Filters Bar
  - Search Box
- Student Exercise



## LEARNING OBJECTIVES AND GOALS:

The primary learning objective and goal of this module is to familiarize students with the Artifacts Explorer in a Portable Case. The Artifacts Explorer provides a visual representation of all artifacts within the case, organized by categories, such as Communication, Media, Documents, and more. Students will learn about the different components of the Artifacts Explorer, including the Navigation Pane, Evidence Pane, Details Pane, and Tags/Profiles/Media Pane. Additionally, they will be introduced to the Filters Bar, a feature that enables advanced filtering, sorting, and searching of artifacts. By the end of this module, students will have a comprehensive understanding of the Artifact Explorer and its various elements. This knowledge will empower them to efficiently navigate the Portable Case and leverage the insights provided by the Artifacts Explorer.



## WHAT ARE ARTIFACTS?

An artifact can be defined as a structured representation of data that is retrieved by Magnet AXIOM from the file system of the item of digital evidence. Artifacts that are supported by AXIOM are listed in the Artifact Reference. These artifacts are used by AXIOM to organize and present the evidence it uncovers during digital investigations. Each artifact consists of a collection of attributes, each with its own data type and the potential to contain specific information such as names, timestamps, locations, messages, and more.

The Artifact Reference (Help > Documentation > Artifact Reference) serves as a comprehensive catalog or list of applications from which Magnet AXIOM can retrieve data. It categorizes artifacts based on the platform they belong to (iOS, Android, OS X / Windows, Windows Phone) and their application type (e.g., Chat, Document, Social Media). By examining the attributes associated with each artifact, investigators can piece together a comprehensive narrative about users' online activities and their communication patterns with others.

It is important to note that all artifacts come from somewhere in the file system of the evidence, but not everything in the file systems gets an artifact created from it. Only applications that are supported by AXIOM result in the creation of artifacts.

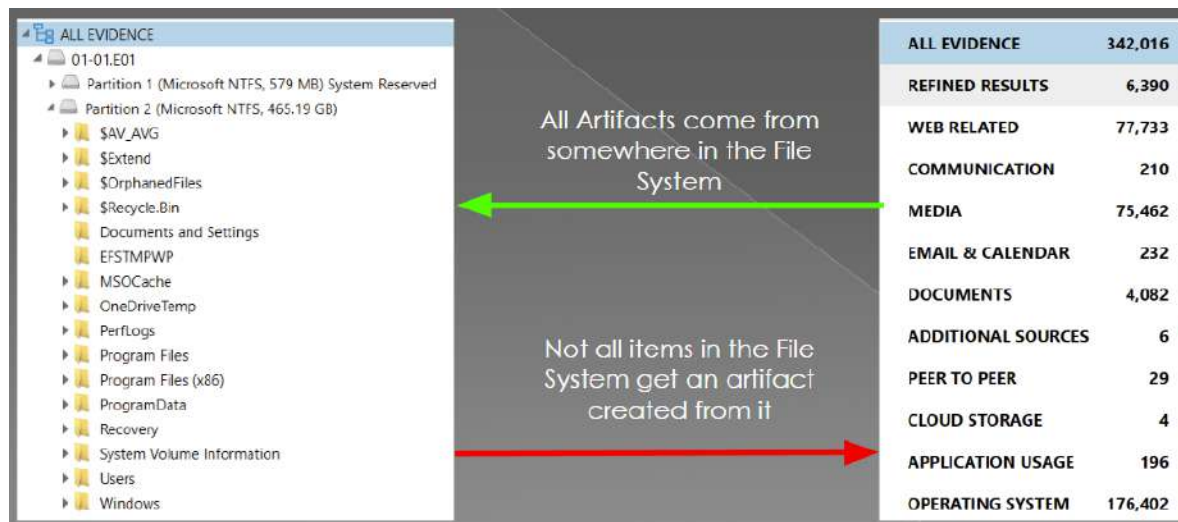


FIGURE 3-1: ARTIFACT CREATION

Understanding the distinction between artifacts and the file system is crucial in investigations involving Portable Cases. In a Portable Case, only artifacts are included, and not the complete file system from the evidence source. It is essential to note this because if you are investigating and searching for specific information, such as the location history from a Fitbit, and you cannot find it within the Portable Case, it might indicate that AXIOM does not support the application, resulting in the absence of an artifact for that particular data.

To verify this, you can consult the Artifact Reference, which serves as a resource listing the supported artifacts. If the Artifact Reference does not indicate support for the artifact you are looking for, it is advisable to contact the forensic examiner and request a search of the file system of the evidence. This is because the desired data might be present in the file system but not as an artifact within the Portable Case. By reaching out to the forensic examiner, you can ensure a comprehensive search for the required information.



## ARTIFACTS EXPLORER LAYOUT

The Artifacts Explorer provides a tabular view of the artifacts that were identified during processing. The Artifacts Explorer consists of the Filters Bar, Navigation Pane, Evidence Pane, Details Pane, and Tags and Comments Pane.

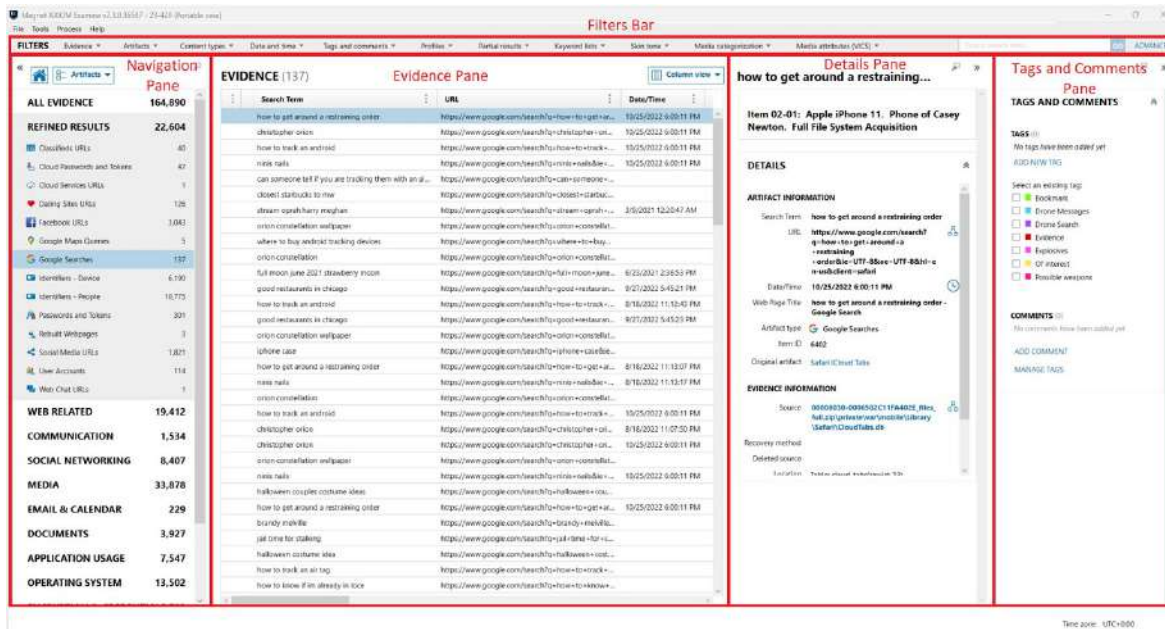


FIGURE 3-2: ARTIFACT EXPLORER LAYOUT

### Navigation Pane

The Navigation Pane, located on the left side of the Artifacts Explorer, provides a list of artifact categories present in the Portable Case. It shows the name of each artifact category along with the corresponding number of artifacts within that category. The artifact categories are organized into main categories, displayed in bold text, followed by subcategories specific to each main category.

If a case does not contain any artifacts of a particular type, AXIOM will not display that artifact category in the Navigation Pane. Therefore, you will never come across an artifact category with a zero count. By clicking on an artifact category in the Navigation Pane, you can view all the associated artifacts in the Evidence Pane.

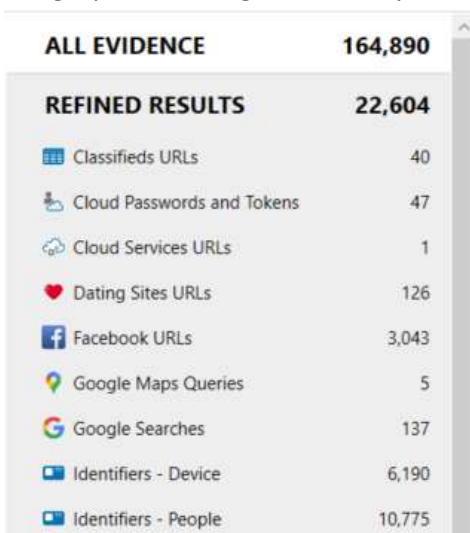


FIGURE 3-3: NAVIGATION PANE



## Evidence Pane

The Evidence Pane, positioned at the center of the Artifacts Explorer screen, displays the artifacts that belong to the highlighted artifact category in the Navigation Pane. It provides a focused view of the specific artifacts relevant to the selected category.

**EVIDENCE (137)** Column view ▾

Search Term	URL	Date/Time	Original Search Query
how to get around a restraining order	https://www.google.com/search?q=how+to+get+ar...	10/25/2022 6:00:11 PM	
christopher orion	https://www.google.com/search?q=christopher+ori...	10/25/2022 6:00:11 PM	
how to track an android	https://www.google.com/search?q=how+to+track+...	10/25/2022 6:00:11 PM	
ninis nails	https://www.google.com/search?q=ninis+nails&ie=...	10/25/2022 6:00:11 PM	
can someone tell if you are tracking them with an ai...	https://www.google.com/search?q=can+someone+...		
closest starbucks to mw	https://www.google.com/search?q=closest+starbuc...		
stream oprah harry megan	https://www.google.com/search?q=stream+oprah+...	3/9/2021 12:20:47 AM	
orion constellation wallpaper	https://www.google.com/search?q=orion+constellat...		orion constellation wallap
where to buy android tracking devices	https://www.google.com/search?q=where+to+buy+...		
orion constellation	https://www.google.com/search?q=orion+constellat...		
full moon june 2021 strawberry moon	https://www.google.com/search?q=full+moon+june...	6/23/2021 2:36:53 PM	
good restaurants in chicago	https://www.google.com/search?q=good+restauran...	9/27/2022 5:45:21 PM	
how to track an android	https://www.google.com/search?q=how+to+track+...	8/18/2022 11:12:43 PM	
good restaurants in chicago	https://www.google.com/search?q=good+restauran...	9/27/2022 5:45:23 PM	
orion constellation wallpaper	https://www.google.com/search?q=orion+constellat...		
iphone case	https://www.google.com/search?q=iphone+case&ie=...		

FIGURE 3-4: EVIDENCE PANE

The Evidence Pane offers customizable content and layout options to suit user preferences. By default, artifacts are displayed in Column View. However, depending on the type of artifact being viewed, it can be advantageous to switch to a different view. AXIOM provides the following alternative views:

- **Classic View:** This view presents artifacts in columns, with the Details Pane located below the Evidence Pane.
- **Column View:** Artifacts are displayed in columns, and the Details Pane is positioned next to the Evidence Pane.
- **Conversation View:** Communications evidence is organized in a threaded conversation format, grouping artifacts by the subjects involved.
- **Histogram View:** This view represents each artifact category as a bar graph, visually indicating the number of artifacts in each category.
- **Row View:** Artifacts are shown as individual rows in the Evidence Pane.
- **Thumbnail View:** Media artifacts are presented as thumbnail images, allowing a quick visual overview of the full-size artifact.
- **World Map View:** If artifacts contain geolocation data, this view plots the artifacts as points on a world map, providing a geographical perspective.

These different views cater to diverse analysis needs and offer alternative ways to explore and interpret artifacts within the Evidence Pane. Users can choose the most suitable view based on the nature of the artifacts and their investigative requirements.



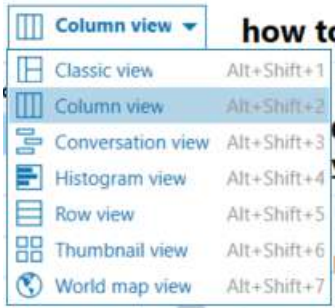


FIGURE 3-5: ARTIFACT VIEWS

### Details Pane

The Details Pane in AXIOM provides information about the artifact currently selected in the Evidence Pane. The details presented in the pane vary depending on the type of artifact being viewed. Common details typically include date/time stamps, the source of the artifact, and the method of recovery.

In addition to these common details, specific artifact types may have additional information. For example, for artifacts like Google Searches, a Search Term field might be available. Cached Locations may include GPS coordinates, and application artifacts may contain application metadata related to the specific application.

For certain artifact types such as pictures, videos, and documents, a preview of the artifact itself is displayed within the Details Pane. This allows users to quickly assess the content of the artifact without opening it separately.

The Details Pane in AXIOM provides users with contextual information and relevant details for each artifact, helping them understand the artifact's properties and aiding in their investigative analysis.

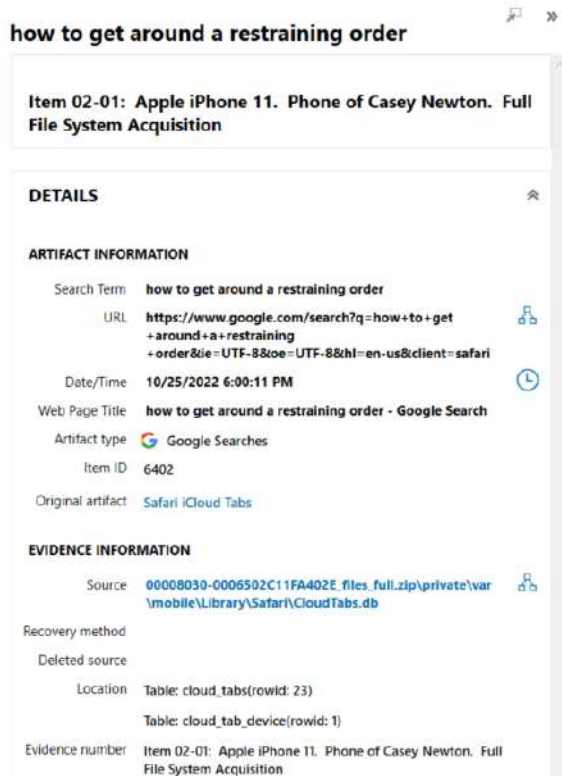


FIGURE 3-6: DETAILS PANE



## Tags, Profiles, and Media Categories Pane

Situated on the far right of the screen, the Tags, Profiles, and Media Categories Pane provides functionality related to tags, comments, and profiles. By default, this pane is collapsed against the side bar and hidden from view. To expand and display this pane, simply click on the words TAGS, PROFILES & MEDIA CATEGORIES.

Once expanded, the Tags and Comments Pane allows users to create or view tags, comments, and profiles associated with the case. Users can create tags to categorize and label artifacts, add comments to provide additional information or analysis notes, and manage profiles related to individuals or entities involved in the investigation.

The Tags, Profiles, and Media Categories Pane serves as a convenient and accessible area for organizing and documenting important details and observations within the case, enhancing collaboration and analysis capabilities.

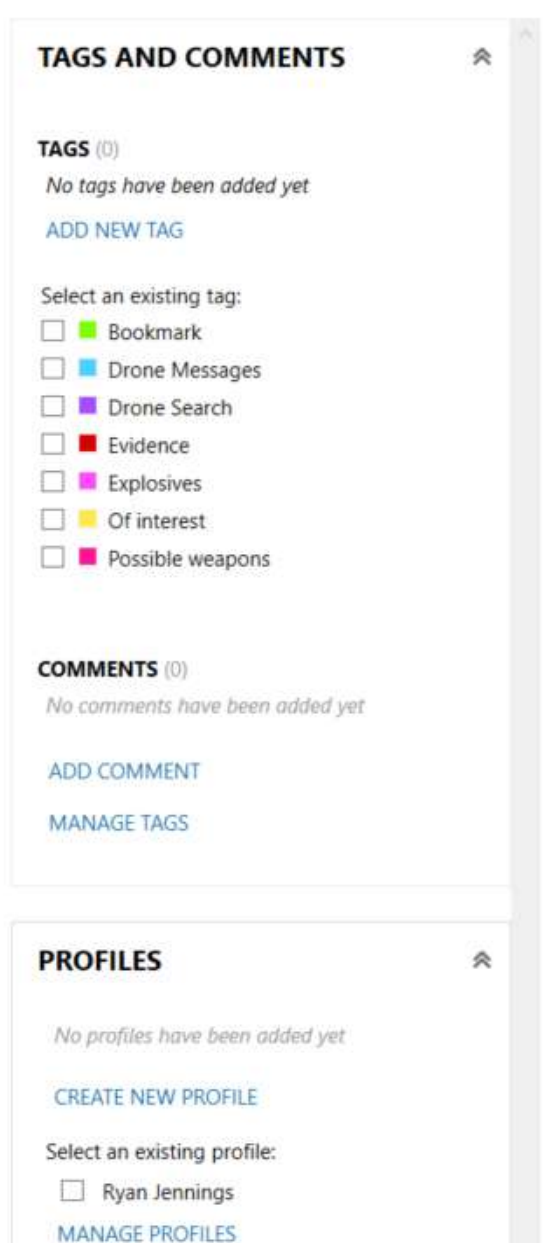


FIGURE 3-7: TAGS, COMMENTS, AND PROFILES PANE

## Filters Bar

In a Portable Case, the Filters Bar is a highly adaptable and effective tool that enables users to apply various filters to focus on pertinent case data. When a filter is applied, the Filters Bar changes to a yellow color, indicating that





the displayed artifacts are filtered results rather than the complete set of artifacts in the case. Additionally, the applied filter is highlighted in bold text within the Filters Bar, allowing the examiner to easily identify the specific filter in use.

If you want to remove a filter, simply click on the "CLEAR FILTERS" option. This action clears all applied filters, restoring the view to show all artifacts in the case without any filtering applied.

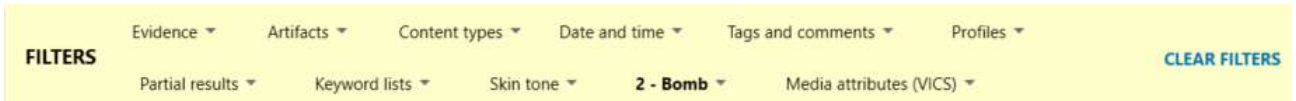


FIGURE 3-8: FILTERS BAR WITH A FILTER APPLIED

## Search Box

Positioned on the far right of the Filters Bar, the Search Box provides users with the ability to perform both basic and advanced keyword searches. Conducting a basic search is straightforward: enter the desired search term into the search box and click GO. Subsequently, only artifacts that match the search term will be displayed.

Furthermore, the Search Box allows users to add additional search terms to refine their query. When multiple search terms are entered through the Search Box, the Boolean logic "AND" is employed to execute the search. As a result, only artifacts that match all of the specified search terms will be returned.

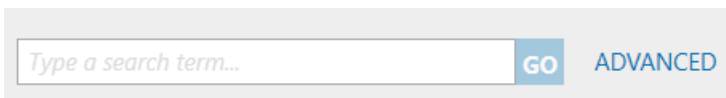


FIGURE 3-9: SEARCH BOX

In addition to the basic search option, you can perform an advanced search by clicking on the ADVANCED link. This action will open the Advanced Search window, providing additional functionality to fine-tune your search.

With the advanced search feature, you gain access to various tools that enable further refinement of your search query. These tools include:

- **Adding Multiple Terms:** You can include multiple search terms within a single query to narrow down the search results.
- **Selecting Boolean Operators:** You have the option to specify the Boolean operator (AND, OR) to define the relationship between multiple search terms.
- **Including/Excluding Terms:** You can specify whether the search should include or exclude specific terms to fine-tune the search results.
- **Search Term Proximity:** You can specify the proximity between search terms to refine the search results based on their relative position within the text.
- **Whole Word Search:** You can specify that the search should only match whole words, disregarding partial matches.
- **Regex Search:** You can choose to perform a regular expression (Regex) search, which provides advanced pattern matching capabilities.

By utilizing these advanced search features, you can create search queries that are highly specific to the information you are seeking. This allows for more precise and targeted search results, enhancing the efficiency and effectiveness of your investigation.



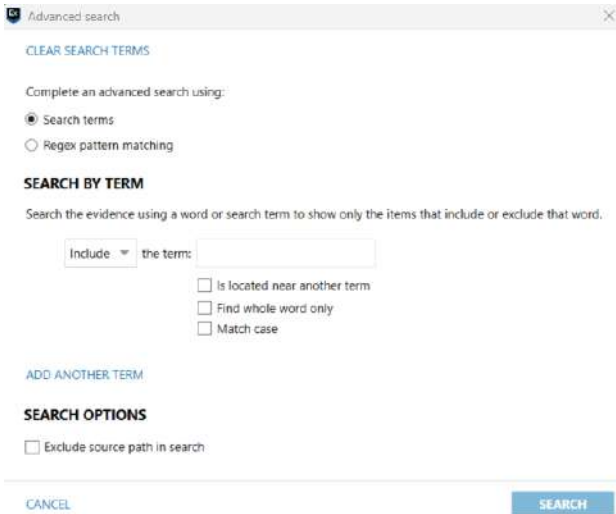


FIGURE 3-10: ADVANCED SEARCH

With the exception of the Evidence Pane, each pane in Artifacts Explorer includes a double-arrow icon. Clicking on this icon collapses the respective pane against the side bar, creating more space for the Evidence Pane. When a pane is collapsed, it is hidden from view.

To display a collapsed pane, simply click on the vertical text representing the pane. This action expands and reveals the pane again, making its contents visible.

The double-arrow icon provides a convenient way to customize the layout of Artifacts Explorer, allowing users to prioritize and allocate space according to their needs. By collapsing and expanding panes as necessary, users can optimize their workspace and focus on the specific areas of the application that are most relevant to their investigation.

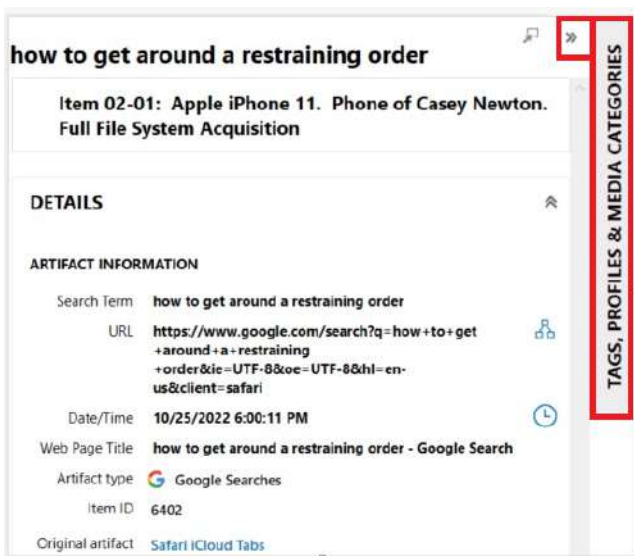


FIGURE 3-11: COLLAPSING AND DISPLAYING PANES



## STUDENT EXERCISE

From the Artifacts Explorer of the Portable Case, answer the following questions:

1. What are the seven views available in Artifacts Explorer?
2. What are the three main panes in Artifacts Explorer?
3. If you want to view mapped GPS data, which view should you use?
4. If you are reviewing pictures and videos, what is the most beneficial view to use?
5. You want to view only Communication evidence in a case. How can you do this?
6. Where can you view all media files that have been categorized by the forensic examiner?
7. Where can you view all of the artifacts that were tagged by the forensic examiner?
8. If you conduct a basic keyword search using two terms, that Boolean logic does AXIOM use to conduct the search?
9. True or False. You can conduct a Regex search in the Portable Case.
10. If a Portable Case contains more than one item of evidence, how can you view artifacts for only one evidence item at a time?







# MODULE 4

## Timeline Explorer

## MODULE 4: TIMELINE EXPLORER

- Timeline explorer
  - Timeline Graph
  - Evidence Pane
  - Details Pane
  - Tips for Navigating the Timeline Explorer
- Student Exercise



## **LEARNING OBJECTIVES AND GOALS:**

The main objective and goal of this module is to introduce students to the Timeline Explorer in a Portable Case, enabling them to become familiar with its functionalities. The Timeline Explorer presents artifacts in an interactive graph based on their timestamps, offering a visual representation of the data.

Throughout this module, students will learn how to navigate the Timeline Explorer effectively and employ various filtering techniques to focus on relevant information. By the conclusion of this module, students will possess a comprehensive understanding of the Timeline Explorer and its components. This knowledge will empower them to efficiently explore the Portable Case and utilize the valuable insights provided by the Timeline Explorer.



## TIMELINE EXPLORER

The Timeline Explorer offers a comprehensive timeline representation of all time-stamped evidence gathered from the Artifacts and File System Explorers. It serves as a valuable tool when you have a specific timeframe in mind and wish to determine if there are notable spikes in user activity during that period.

Within the Timeline Explorer, you will find a visual depiction of time through an interactive graph. This graph allows you to examine specific timeframes, identify spikes in activity, focus on particular dates, and establish behavioral patterns.

The Timeline Explorer comprises three main panes:

- **Timeline Graph:** This pane presents an interactive graph that visually represents a designated period of time. It offers an intuitive overview of events and activities within that timeframe.
- **Evidence Pane:** In this pane, you can explore a chronological listing of all artifacts and file system events that occurred during the selected time period from the Timeline Graph. It provides a structured view of the evidence, facilitating easy navigation and exploration.
- **Details Pane:** Clicking on an artifact or file system event in the Evidence Pane opens the Details Pane, which provides specific information and additional details about the selected item. This pane offers a closer examination of individual artifacts or events for a more comprehensive understanding.

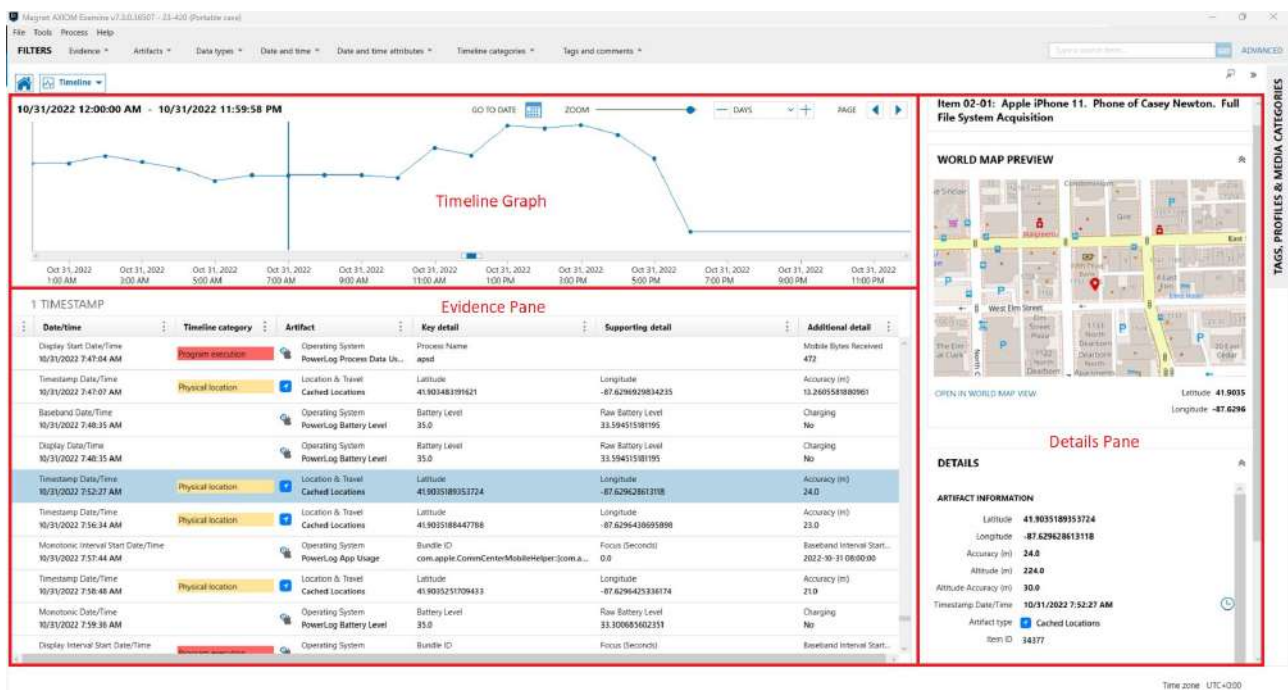


FIGURE 4-1: TIMELINE EXPLORER

### Timeline Graph

The Timeline Graph is an interactive visual representation of a specific timeframe. It provides a user-friendly overview of events and activities that occurred during that period, facilitating easy comprehension and analysis. Within the Timeline Graph, users have the ability to apply time filters, allowing them to limit the data displayed on the graph. These time filters can range from filtering by years down to filtering by minutes.

Presenting the data in a visual format helps to uncover patterns within the data. For instance, in Figure 4-2, it is easy to see that on Oct 27, 2022, there was a notable increase in user activity related to the specific item of evidence. This heightened activity persisted for the subsequent six days. Then on Oct 31, 2022, the activity





abruptly dropped to minimal levels and remained at that level for the rest of the graph's duration. Such visualizations enhance the understanding of the data by enabling users to easily identify significant shifts and trends.

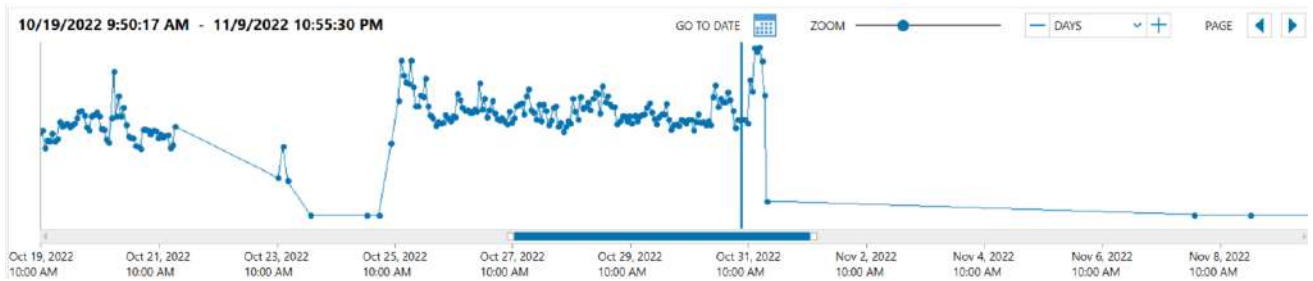


FIGURE 4-2: TIMELINE GRAPH

### Evidence Pane

Within the Evidence Pane, you can navigate through a chronological list of all artifacts and file system events that took place within the selected time period from the Timeline Graph. It offers a structured view of the evidence, allowing for convenient navigation and exploration. To aid in the review and analysis of the evidence, the Evidence Pane also includes supplementary details and high-level categorization of the evidence based on timeline categories. These categories encompass various aspects such as program execution, browser usage, file and folder openings, user events, and more.

1 TIMESTAMP						
Date/time	Timeline category	Artifact	Key detail	Supporting detail	Additional detail	
Display Start Date/Time 10/31/2022 7:47:04 AM	Program execution	Operating System PowerLog Process Data Us...	Process Name apsd		Mobile Bytes Received 472	
Timestamp Date/Time 10/31/2022 7:47:07 AM	Physical location	Location & Travel Cached Locations	Latitude 41.903483191621	Longitude -87.6296929834235	Accuracy (m) 13.260558180961	
Baseband Date/Time 10/31/2022 7:48:35 AM		Operating System PowerLog Battery Level	Battery Level 35.0	Raw Battery Level 33.594515181195	Charging No	
Display Date/Time 10/31/2022 7:48:35 AM		Operating System PowerLog Battery Level	Battery Level 35.0	Raw Battery Level 33.594515181195	Charging No	
Timestamp Date/Time 10/31/2022 7:52:27 AM	Physical location	Location & Travel Cached Locations	Latitude 41.9035189353724	Longitude -87.629628613118	Accuracy (m) 24.0	
Timestamp Date/Time 10/31/2022 7:56:34 AM	Physical location	Location & Travel Cached Locations	Latitude 41.9035188447788	Longitude -87.6296438695898	Accuracy (m) 23.0	
Monotonic Interval Start Date/Time 10/31/2022 7:57:44 AM		Operating System PowerLog App Usage	Bundle ID com.apple.CommCenterMobileHelper[com.a...	Focus (Seconds) 0.0	Baseband Interval Start...	2022-10-31 08:00:00
Timestamp Date/Time 10/31/2022 7:58:48 AM	Physical location	Location & Travel Cached Locations	Latitude 41.9035251709433	Longitude -87.6296425336174	Accuracy (m) 21.0	
Monotonic Date/Time 10/31/2022 7:59:36 AM		Operating System PowerLog Battery Level	Battery Level 35.0	Raw Battery Level 33.300685602351	Charging No	
Display Interval Start Date/Time	Program execution	Operating System	Bundle ID	Focus (Seconds)	Baseband Interval Start...	

FIGURE 4-3: EVIDENCE PANE

### Details Pane

The Details Pane provides specific information and additional details about selected artifacts or file system events. It offers a closer examination of individual artifacts, enhancing the understanding of their significance. By clicking on an artifact or event in the Evidence Pane, users can access the Details Pane to gain deeper insights and contextual information. This pane allows for a comprehensive analysis, providing valuable metadata, timestamps, and associated actions or interactions.



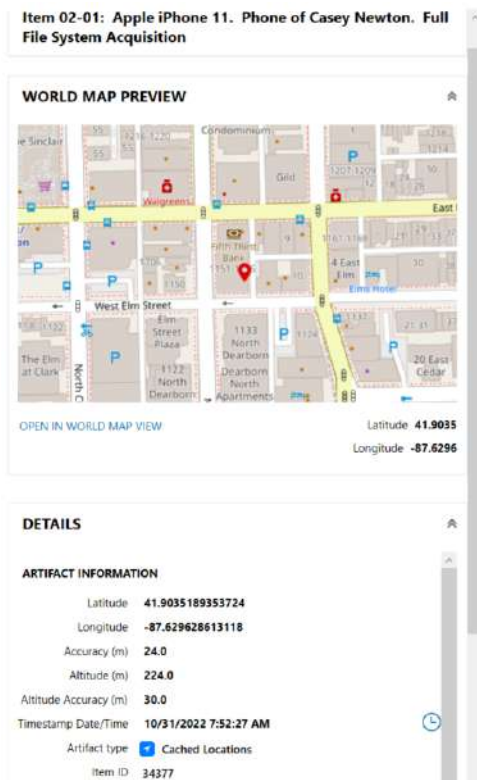


FIGURE 4-4: DETAILS PANE

## TIPS FOR NAVIGATING THE TIMELINE GRAPH

To effectively navigate the Timeline Graph, consider the following suggestions:

- **Zoom in and explore:** To examine a specific time period in detail, utilize the scroll wheel on your mouse or toggle the Zoom option. This allows you to get a closer look at the graph and its events.
- **Time navigation:** To move backward or forward in time, click and drag your mouse left or right on the graph. For quick jumps in time, utilize the Next page and Previous page options.
- **Hover for details:** Hovering over a node on the graph displays the date and number of hits for a spike. The date/time format adjusts based on your selected view (year, month, week, day, hour, or minute).
- **Analyze activity spikes:** Clicking a node on the timeline graph enables you to analyze hits within a spike. AXIOM Examine automatically directs you to the first time-stamped item related to the activity spike in the evidence table below the graph.
- **Adjust date type:** Toggle the date type to change how the timeline is displayed—whether by years, months, weeks, days, hours, or minutes. The horizontal axis below the graph updates accordingly.
- **Focus on specific date range:** Utilize the "Go to date" feature to concentrate the graph on a particular date range. Simply click the option and select your desired date range.
- **Apply filters:** Narrow down the scope of the evidence by applying filters such as data types, timeline categories, date/time ranges, and more. This helps streamline the search process and focus on relevant information.

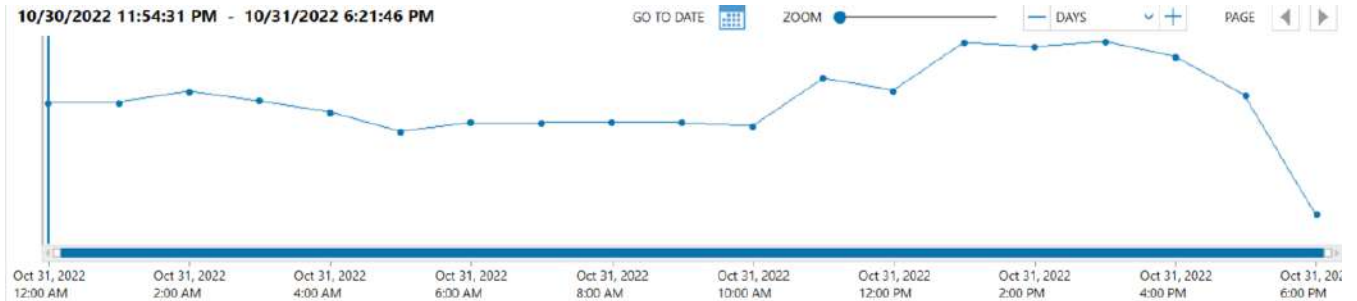
By following these suggestions, you can effectively navigate the Timeline Graph, zoom in on specific time periods, analyze spikes in activity, adjust the date display, and apply filters to streamline your investigation process.



## STUDENT EXERCISE

In this module, we saw that there was a significant drop in user activity on the iPhone after 10/31/2022. Using Timeline Explorer, explore this further.

1. Go to Timeline explorer.
2. Apply a date range so that online timeline information from 10/31/2022 is displayed. From the initial graph, we can see that activity on the phone picked up around 10:00 AM and then dropped rapidly after 5:00 PM.



3. In the Timeline Graph, switch from DAYS to HOURS. Scroll to the right of the graph and then use your mouse wheel to zoom in around 5:00 PM. By zooming in, we can see that activity on the phone stopped right around 5:21 PM.



5. Based on this information, let's modify the date filter and add a specific time period. Click on the filter for Date/Time. Leave the date 10/31/2022 and select Custom Time Range for the time range. Use a Start Time of 3:30 PM and an End Time of 5:30 PM.
7. To drill into the data further, from the Filters Bar, under Artifacts, filter so that you are only viewing Communications and Location & Travel artifacts. Review the timeline
8. From this information, we can see multiple text messages with Ryan Jennings. We can also see the physical location of Casey Newton when the messages were sent. The reason that there are multiple copies of the same messages is due to the fact that they are parsed from different locations.
9. At approximately 3:53:49 PM, Ryan Jennings sent Casey Newton a picture. From Artifacts in the Filters Bar, add in the artifact Media. Return to the timeline and view the activity around the time the picture was sent. What was the picture? It is also a Live Photo. Play the associated video.
10. At approximately 3:58:22, another picture was sent. What is that picture?
11. At approximately 4:04:36, Ryan Jennings sent a message telling Casey Newton to "Go ahead



and make the call.” What phone number did she call?

12. The final message sent by Ryan Jennings says that he is coming to Casey’s house. Casey replies that she will see him soon. Approximately where is Casey’s house?
13. Return to Artifacts Explorer and clear all filters.









# MODULE 5

Overview of Artifacts

## MODULE 5: OVERVIEW OF ARTIFACTS

- Refined Results
- Web Related
- Communication
- Social Networking
- Media
- Email & Calendar
- Documents
- Application Usage
- Operating System
- Encryption & Credentials
- Connected Devices
- Location and Travel
- Student Exercise





## LEARNING OBJECTIVES AND GOALS:

The main objective of this module is to introduce students some of the common artifact types found in the Portable Case. These artifacts are grouped into distinct categories, and throughout the module, students will learn about the most prevalent types in each category. They will understand what these artifacts are, their significance, and how to interpret them effectively.

By the end of the module, students will understand the various artifact types in the Portable Case. This knowledge will empower them to conduct more successful investigations and improve their overall proficiency in this field.

This module serves as an introduction to some of the most common artifact types. For a more in-depth, detailed analysis of artifacts, it is recommended that the student attend an advanced course such as AX200.



## REFINED RESULTS

In the Navigation Pane, the second parent category displayed is known as Refined Results. Its main purpose is to efficiently organize data from different artifacts, making it easier for examiners to identify evidence quickly.

The content within the Refined Results category mainly comes from browser activity. While some of these artifacts can also be found in the Web Related parent category, they are intelligently grouped under meaningful categories within Refined Results to enhance the examiner's efficiency and reduce effort.

Since a significant portion of the artifacts in Refined Results stem from browser activity, it's common for results to appear both within the consolidated Refined Results category and their respective browser artifact category under Web Related. Additionally, certain artifacts may appear in multiple categories within Refined Results. It is important to note that tagging an artifact in Refined Results will not tag the corresponding artifact in another artifact category. Each category operates independently in this regard.

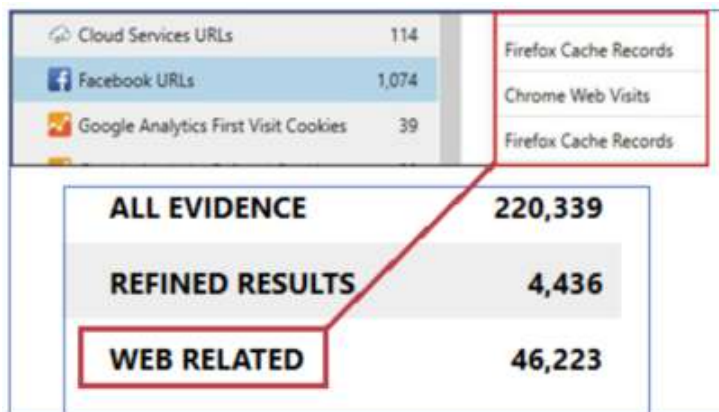


FIGURE 5-1: RELATIONSHIP OF A 'REFINED RESULTS' ORIGINATING FROM A 'WEB RELATED' ARTIFACT

## Cloud Passwords and Tokens, Passwords and Tokens, & User Accounts

These three artifact categories offer valuable information about recovered user accounts and passwords from the evidence:

- Cloud Passwords and Tokens:** This category includes any cloud-related passwords and tokens that have been found on the system during the investigation. Cloud passwords are credentials used to access cloud-based services or platforms, while tokens are authentication mechanisms used to verify a user's identity without revealing their actual password. These accounts and tokens are crucial as they can potentially grant access to data stored in cloud services like cloud storage, email accounts, or other cloud-based applications. Investigators can use these credentials to gather more evidence from the associated cloud accounts and better understand the user's activities, communications, and stored files within those services.
- Passwords and Tokens:** In this category, you will find passwords and tokens associated with user accounts on the local system. User accounts often require passwords or tokens for authentication purposes. These could be local user accounts used to log in to the operating system or any locally installed applications. These artifacts are significant because they can provide insights into the user's activity on the local machine and possibly grant access to other sensitive data or services that rely on these credentials.
- User Accounts:** This category encompasses all the application accounts of local users that have been identified on the system during the investigation. These application accounts can belong to various installed software or services, such as email clients, web browsers, messaging apps, productivity tools, and more. Analyzing these accounts can provide a comprehensive understanding of the user's digital footprint,



the applications they interacted with, and the potential avenues they used to communicate, access information, or conduct activities.

By analyzing these artifact categories, investigators can gain a deeper understanding of the user's digital presence, online activities, and potential access points to acquire additional evidence pertinent to the case at hand.

## Google Searches & Parsed Search Queries

These two artifact categories offer valuable insights into the search behavior of users:

- **Google Searches:** Within the Google Searches artifact, you can find a comprehensive list of URLs linked to searches performed using the Google search engine. This includes records of the search terms or keywords entered by users, as well as the date and time when each search occurred. By analyzing this data, investigators can gain a deeper understanding of the specific information users were seeking and the timelines of their searches on Google.
- **Parsed Search Queries:** The Parsed Search Queries artifact comprises URLs associated with search engines other than Google. This encompasses a variety of search engines, such as Bing and DuckDuckGo, as well as searches conducted on other platforms like Facebook and YouTube. This category provides a broader view of users' search activities beyond just Google, shedding light on their interests and exploration patterns across multiple search engines and online platforms.

Both artifact categories play a crucial role in digital investigations, enabling investigators to uncover significant insights into users' search preferences, information needs, and online activities across a diverse range of search engines and platforms.

## Classifieds URLs

The artifact category Classifieds URLs comprises a comprehensive collection of URLs linked to classifieds websites. These websites are known for hosting content such as items available for sale, personal ads, and offered services. The Classifieds URLs artifact group encompasses domains that primarily feature classifieds-type content. Examples of such domains include popular sites like Amazon, eBay, and Craigslist.

By examining this artifact, investigators can gain insights into users' interactions with various classifieds platforms and their engagement with the listed types of content, such as buying or selling items, seeking personal connections, or exploring services available on these websites.

## Facebook URLs

Facebook URLs contains a list of URLs associated with activities on the Facebook website. These URLs are gathered from various web browsers, capturing users' interactions and engagements on the platform. By examining the URLs within this artifact, investigators can potentially determine the nature of the activities taking place on Facebook. The information extracted from the URLs can provide valuable insights into users' actions, content interactions, and other relevant activities carried out on the social media platform.

## Identifiers - People

Earlier in the course, we learned about Profiles and their significance in filtering case data that pertains to a particular individual. A Profile consists of identifiable information attributed to a specific person, encompassing real names, screen names, internet accounts, phone numbers, addresses, and other relevant details. Any artifact associated with a specific individual adds to their profile.

The artifact category Identifiers - People stores information and identifications of all individuals discovered within the evidence. This data is valuable in constructing a profile that enables a focused investigation on data related to



a specific user. By using these profiles, investigators can efficiently drill down into relevant data linked to particular individuals, streamlining the process of analyzing and understanding their activities and digital presence during the course of the investigation

## STUDENT EXERCISE – REFINED RESULTS

1. What is the user's Instagram User Name and password?
2. What is the user's Facebook User Name and password?
3. The user logged into a WiFi AirPort service. What is the password of that wireless network?
4. The user has a WhatsApp account. What is her User ID?
5. Is there any evidence that the user was searching for information about tracking someone?
6. On Amazon, the user viewed a book related to building explosives and weapons. What is the title of that book?
7. The user viewed Facebook event 1052515771967336. What was that event and what date was it being held?
8. While on Facebook, the user viewed the profile and several photos related to a BBQ business. What is the name of that business?
9. In Identifiers, what is the DSID for the Owner Information of the iPhone?
10. Clear all filters



## WEB RELATED

Web-related evidence pertains to digital artifacts extracted from the internet, shedding light on an individual's online activities. This encompasses a range of elements, such as visited websites, conducted searches, downloaded files, bookmarked webpages, cookies, and records of viewed content stored on their computer.

### iOS Safari Recent Search Terms

The artifact iOS Safari Recent Search Terms maintains a record of the search terms executed by the user through the Safari browser on an iOS device. These search terms are collected from any search engine that the user accessed via Safari.

By examining this artifact, investigators can gain insights into the recent search activities of the user, regardless of the search engine used. It allows them to understand the topics, interests, and information the user was seeking during a specific period of time, providing valuable evidence for digital investigations.

### Safari History

The Safari History artifact encompasses stored internet history records from the Safari browser on iOS devices. Within this artifact, investigators may find crucial information, including the URLs visited by the user, the respective dates of each visit, the titles of the web pages accessed, and the frequency of visits to specific pages. This data provides valuable insights into the user's browsing activities, preferences, and recurring site visits.

By analyzing the Safari History, investigators can reconstruct the user's web browsing journey, understand their interests, and potentially uncover essential evidence related to their online actions.

## STUDENT EXERCISE – WEB RELATED

1. In the previous exercise, we saw that the user viewed a specific book on Amazon related to building explosives and weapons. Is there any information in iOS Safari Recent Search Terms indicating how the user found the book on Amazon?
2. What type of club was the user search for in Chicago?
3. In general, is there any evidence in iOS Safari Recent Search Terms related to this investigation?
4. On 9/27/2022 at 5:45:21 PM, the user conducted a search for 'good restaurants in Chicago.' What is the title of the first web page that the user viewed after that search?
5. Based on the restaurant search, what specific restaurant did the user view on tripadvisor.com?
6. The user searched 'mountain cabins nearby with waterfalls.' This led to viewing a specific rental site on VRBO. What is that rental site?
7. Is there any evidence that the user booked a cabin through VRBO?
8. Clear all filters



## COMMUNICATION

Communication evidence is any information that shows how someone has talked to or communicated with someone else. This could include things like phone calls, email addresses, text messages, social media messages, or even contacts. It can also include things like recordings of conversations or screenshots of messages. Communication evidence can be used to indicate that someone talked to someone else, or to find out what they talked about. It can also be used to find out when someone talked to someone else, or how often they talked.

### Apple Contacts

The Apple Contacts artifact contains information about the contacts that a user has saved on their Apple device. This includes details such as the contact's name, phone number, and email address. Additionally, the artifact records the date when each contact was created and, if applicable, the date of any modifications made to the contact information.

By examining the Apple Contacts artifact, investigators gain access to a comprehensive list of the user's saved contacts, along with the timeline of their creation and any subsequent changes. This data can be instrumental in understanding the user's communication patterns, identifying individuals with whom they have been in contact, and establishing potential connections in a digital investigation.

### iOS Call Logs

The iOS Call Logs artifact stores a comprehensive history of calls on the iOS device. This includes not only traditional telephone calls but also FaceTime calls and calls made through third-party apps such as Facebook Messenger. The artifact provides essential information such as the contact number of the call partner, the date when the call occurred, the direction of the call (incoming or outgoing), and the duration of the call.

By analyzing the "iOS Call Logs" artifact, investigators can gain insights into the user's communication activities, including whom they have been in contact with, the frequency and duration of their calls, and the various communication platforms they used. This data can be instrumental in establishing connections, understanding communication patterns, and providing valuable leads in digital investigations.

### iOS iMessage/SMS/MMS

The iOS iMessage/SMS/MMS artifact serves as a comprehensive record of all iMessages, SMS messages, and MMS messages sent and received by the user. This data includes information such as contact details of the individuals the user communicated with, the dates of each communication, and the content of the messages exchanged. Additionally, if any media files like pictures or videos were sent or received as part of the messages, this multimedia information will also be available within this artifact.

By carefully examining the iOS iMessage/SMS/MMS artifact, investigators gain deep insights into the user's communication activities, including their conversations with specific contacts, the content shared, and the overall frequency and nature of their messaging interactions. This artifact plays a central role in digital investigations, providing a clear picture of the user's communication behavior and establishing connections with others. The comprehensive information present within the iOS iMessage/SMS/MMS artifact proves instrumental in piecing together crucial evidence, revealing communication patterns, and understanding the user's social interactions on their iOS device.

## STUDENT EXERCISE – COMMUNICATION

1. What is the contact name associated with the phone number 572-276-1969?
2. There is a contact name of 'Off The Grid.' What two lakes is 'Off The Grid' between?
3. What date/time did Casey Newton add Ryan Jennings as a contact?
4. What is the phone number for Dolan Shaver?
5. How many phone calls did the user place to 572-276-1969?
6. Has Casey Newton ever talked on the phone with Ryan Jennings?
7. On 9/15/2022 at 10:36:11, Ryan Jennings sent Casey Newton a message with a video attached. What is depicted in this video?
8. Using the answer in Question 5, is there any evidence in the text messages between Casey Newton and Ryan Jennings related to Casey Newton making a phone call?
9. When Casey Newton and Chris Austin first met in-person, where did they agree to meet?
10. Clear all filters

## SOCIAL NETWORKING

Social networking evidence is any information that is stored on social media websites or applications. This could include things like posts, profiles, friends, and messages. Social networking evidence can be used to prove that someone was at a certain place, or that they knew someone else. It can also be used to find out what someone was thinking or what they were doing.

### Instagram Direct Messages

Instagram Direct Messages include all private, direct messages sent or received by the user through the Instagram platform. This artifact contains valuable information, including the usernames of the individuals the user is communicating with, the dates of each message exchange, and the content of the messages.

By examining the Instagram Direct Messages artifact, investigators gain insights into the user's private conversations on the platform, identifying the contacts with whom they communicate, the frequency of their interactions, and the content shared in their direct messages.

### iOS Tinder Messages

The iOS Tinder Messages artifact encompasses all private, direct messages sent or received by the user within the Tinder app. This artifact holds crucial information, including the User ID of the individuals the user is communicating with, the dates of each message exchange, and the content of the messages.

By carefully analyzing the iOS Tinder Messages artifact, investigators gain valuable insights into the user's private conversations on the Tinder platform. The data reveals the contacts with whom the user communicates, the frequency of their interactions, and the specific content shared in their direct messages. This artifact proves essential in digital investigations, as it sheds light on the user's social connections, communication behavior, and potentially relevant information related to the case.



## STUDENT EXERCISE – SOCIAL NETWORKING

1. Using the information in Instagram Direct Messages, what date did Ran Jennings and Casey Newton get a drink?
2. What date did Casey Newton match with Ryan Jennings on Tinder?
3. What is the User Name of the only other user that Casey matched with on Tinder?
4. What is the User ID of Case Newton's Tinder account?
5. How did Casey Newton learn Ryan Jennings's phone number?
6. What is the Twitter User ID for Miley Cyrus?
7. Clear all filters

## MEDIA

Media evidence refers to audio or video information stored in various formats such as recordings, pictures, screenshots, and videos. It serves the purpose of demonstrating occurrences or determining events that took place. Additionally, media evidence aids in identifying individuals involved in incidents or ascertaining their actions. An item of digital evidence can contain tens of thousands of pictures and videos. To filter to those only on the camera roll of the device, the user can conduct a search for 'DCIM.' DCIM stands for Digital Camera Image and is the location where most user-generated pictures and videos are stored.

### iOS Snapshots

The iOS Snapshots artifact consists of stored snapshots taken by iOS when an application is suspended. This occurs when the application is sent to the background on a device, either by minimizing the application or switching to a different one.

When an application is suspended, iOS captures a snapshot of its current state before temporarily pausing its execution. These snapshots serve as a frozen image of the application's interface and content at the moment of suspension. They allow users to resume their interactions seamlessly when returning to the application.

For digital investigations, analyzing the iOS Snapshots artifact can provide valuable information about the user's recent activities within specific applications. Investigators can gain insights into the application's appearance, content, and potentially sensitive data displayed when it was last in use. This data can be crucial for understanding the user's actions and the context surrounding their interactions with the application, assisting in piecing together the user's digital activities and behavior on the iOS device.

### Live Photos & Photos Media Information

iOS Live Photos is an Apple feature that enhances traditional still photographs by adding a dynamic element. When activated on an iOS device, Live Photos records 1.5 seconds of video and audio both before and after capturing the photo. This results in a short, animated clip that not only preserves the static image but also captures the surrounding movement and sound, providing a more immersive and vivid representation of the moment. AXIOM presents this information in Live Photos and Photos Media Information

For digital forensics, the inclusion of Live Photos in iOS devices can be highly beneficial. These dynamic photo clips can provide valuable context and additional evidence surrounding a particular moment or event. Investigators can analyze the Live Photos to gain insights into the environment and atmosphere when the photo was taken, potentially revealing critical details that may have been missed in a static image alone. Live Photos can be



particularly useful in understanding the sequence of events, verifying the authenticity of images, and reconstructing timelines during investigations.

## Pictures

The Pictures artifact comprises all images recovered from the evidence, including both carved and parsed pictures. While an iOS device may have tens of thousands of pictures, only a small fraction of them may be present in the Camera Roll.

When examining the Pictures artifact, the examiner should pay attention to the Source of each picture. This helps determine if the picture was accessible by the user or if it was stored in a location not directly accessible through the device's regular user interface.

By noting the Source of each picture, the examiner can distinguish between images that were part of the user's regular collection and those that might have been hidden, stored in encrypted files, or originating from other sources like app-specific folders or temporary caches. This analysis aids in understanding the user's image usage patterns and can potentially uncover relevant evidence hidden within the device's image repository. The Pictures artifact plays a critical role in digital forensics investigations, allowing examiners to explore the user's visual data, identify potential sources of evidence, and provide a deeper understanding of the user's image-related activities and behaviors.

## Videos

The Videos artifact includes all video files recovered from the evidence, including both carved and parsed videos. iOS devices may have a significant number of videos, exceeding what's visible in the Camera Roll.

When examining the Videos artifact, the examiner should review the Source of each video to determine its accessibility to the user. This helps differentiate between videos in the user's regular collection, easily viewable, and those potentially hidden in encrypted files, app-specific folders, or temporary caches.

Careful Source analysis allows for insights into the user's video habits, identifying potential evidence sources and uncovering hidden information. The Videos artifact is critical in digital forensics, providing a comprehensive view of the user's video content and activities.



## STUDENT EXERCISE – MEDIA

1. On 10/31/2022, at approximately 4:20:16, an iOS Snapshot was captured. What is the significance of this Snapshot?
2. From iOS Snapshots, who was Casey Newton having dinner with on 9/13/2022?
3. View the live information associated with the picture IMG\_0057.HEIC. What is being discussed while this picture was taken?
4. What address was the user near when this picture was taken?
5. Conduct a search for '5005.jpg.' In the results, view the Source of the results. What is this information indicating?
6. From the 5005.jpg pictures, it is possible to determine the name of the full-size picture?
7. For the picture IMG\_0053.HEIC, what is the Make, Model, and Software for the camera that was used to take the picture?
8. When was the video IMG\_0138. MOV taken?
9. What Make and Model of camera was used to take IMG\_0138.mov?
10. Clear all filters

## EMAIL & CALENDAR

Email and calendar evidence encompass information stored within email and calendar programs. This comprises email messages, attachments, and calendar events. Such evidence serves to establish actions undertaken by individuals or to ascertain the specifics of those actions. Moreover, it aids in identifying parties involved or determining the timing of events.

### Apple Mail

The Apple Mail artifact stores emails that the user has both sent and received, along with comprehensive details related to each email. Common information available for each email includes the sender's and recipient's details, the subject of the email, the body of the message, and any attachments that were included.

In addition to the standard email content, this category also includes additional information such as email headers. Email headers provide valuable metadata about the email, including details about the route the email took through the internet, the email servers involved in its transmission, and other technical information related to the message.

For digital forensics, analyzing the Apple Mail artifact is essential as it offers a comprehensive overview of the user's email communication. It allows investigators to trace communication patterns, identify contacts, verify the authenticity of emails, and gather relevant evidence related to the case. The inclusion of email headers is particularly useful for validating the origin and legitimacy of emails and can be crucial in verifying the accuracy of the provided information.

### Calendar Events

The Calendar Events artifact stores information from the default iOS calendar. This encompasses both prepopulated events, such as holidays, and any calendar events created by the user. For each calendar event, the

artifact includes a summary of the event, along with the start date and end date.

By examining the Calendar Events artifact, investigators gain insights into the user's scheduled activities, appointments, and important dates. It provides a comprehensive view of both system-generated and user-created events, enabling a better understanding of the user's daily routine and plans.

The artifact proves valuable in digital forensics as it assists in reconstructing timelines, verifying the user's activities, and corroborating other evidence gathered during the investigation. Moreover, it helps establish the user's engagement with specific events, shedding light on their commitments and potential connections to significant occurrences.

## STUDENT EXERCISE – EMAIL & CALENDAR

1. On 9/9/2022, Ryan Jennings sent Casey Newton an email with the subject line “So Many Options.” What attachment was included with this email?
2. What attachment was included in the email with the subject line “Check this out”?
3. On 9/19/2022, Ryan Jennings sent an email to himself and to Casey Newton. This email had the subject line of “Cool video” and contained an attachment of IMG\_0051.MOV. Due to the size of the attachment, it could not be included as an attachment and instead a download link was generated by Apple. What location did this download link point to?
4. Casey Newton received a notification email from Facebook that someone wanted to be friends with her. Who wanted to be friends with her?
5. How many user-created Calendar Events are there?
6. Clear all filters



## DOCUMENTS

Document evidence encompasses information stored in various document formats, including word processing documents, text files, spreadsheet files, presentation files, and user-created notes. It serves the purpose of demonstrating occurrences or determining events that took place. Additionally, document evidence aids in identifying individuals involved in incidents or ascertaining their actions.

### Apple Notes

The Apple Notes artifact holds information about the notes created by a user on their iOS device. Each Apple Note contains essential details, including the title, the content of the note (referred to as the body), and the date when the note was created.

Additionally, the Apple Notes artifact indicates whether a user has encrypted a particular note. If a note is encrypted, it means that the content is protected by encryption to secure its confidentiality. Depending on the type of forensic acquisition, encrypted notes may or may not be recoverable.

For digital forensics investigations, the Apple Notes artifact is significant as it allows investigators to access and analyze the user's written thoughts, reminders, or any other information stored in notes. Examining the contents of Apple Notes can provide valuable insights into the user's intentions, plans, and activities. Moreover, if encrypted notes can be successfully recovered, they may contain crucial information relevant to the investigation.

## STUDENT EXERCISE – DOCUMENTS

1. Review the Apple Note with the title To do 9/13/22. Does this note look familiar?
2. Are any of the Apple Notes encrypted? If so, can you still read the content?
3. Review the encrypted note. What is the significance of the phone number in the note?
4. Review the document data.csv. The document is referring to a specific location. What city is that location near?
5. Review the document attachment.pptx. Who is the original author of the document and where did she work?
6. Who is the last author of attachment.pptx and when was it last modified?
7. What date was the file Anarchist Cookbook – William Powell.pdf saved on the phone?
8. Clear all filters



## APPLICATION USAGE

Application usage evidence refers to information that reveals the installed programs and applications on an individual's computer, the permissions granted to them, and their usage patterns. This evidence can establish the utilization of specific programs or applications or shed light on the activities performed within them. Furthermore, it can aid in identifying the party responsible for installing a particular program or application and determining the permissions assigned to it.

### Installed Applications

The Installed Applications artifact compiles a comprehensive list of all applications installed on the device. This includes both system and user-installed apps. The artifact provides essential information, such as the package name (a unique identifier for the app), the display name (the name visible to the user), and the date when each application was installed.

For digital forensics, analyzing the Installed Applications artifact is valuable in understanding the user's app usage and preferences. It offers insights into the types of applications the user has installed, potentially revealing their interests, activities, and even their profession or hobbies. Furthermore, the artifact aids in establishing a timeline of events or user behavior, as the installation dates of certain apps can be indicative of specific activities or changes in the device's usage pattern.

### iOS Device Information

The iOS Device Information artifact stores comprehensive details related to the device itself. This information includes the make, model, and serial number of the iOS device, providing crucial identifiers for the specific hardware in question. Additionally, the artifact contains the device's name, which is the user-assigned name to identify the device.

Moreover, the iOS Device Information artifact includes data on whether location services are enabled on the device. Location services allow various apps and features to access the device's location, and this information can be relevant for digital forensics investigations.

Furthermore, the artifact holds data related to the device's wallpapers, which are the background images displayed on the device's home screen and lock screen. These wallpapers can offer insights into the user's preferences and personalization choices.

Finally, the iOS Device Information artifact contains detailed backup information. This includes data related to device backups, which are copies of the device's data stored on iCloud or a computer. Backup information can be crucial in recovering lost or deleted data and can be essential for digital forensics investigators to access and analyze.

### KnowledgeC

KnowledgeC is a database that stores a wide range of information related to various processes running within an iOS device. Its purpose is to track and record diverse activities occurring on the device, offering valuable insights for digital forensics investigations.

The database keeps records of crucial events, such as when the device was plugged in or unplugged, providing a timeline of power-related activities. It also tracks the device's orientation, keeping a record of how the device was positioned at specific times.

KnowledgeC goes beyond basic activities and captures significant data about the device's lock state, notifications received, application usage patterns, and even the backlight status. This information helps investigators understand the user's interactions with the device, app usage behavior, and their attention to notifications.



In AXIOM, the data from KnowledgeC is divided into multiple sub-categories, facilitating a structured and systematic examination of the device's activities. By analyzing this wealth of data, digital forensics experts can build a comprehensive pattern-of-life analysis, gaining valuable insights into the user's behavior, routine, and habits on the iOS device.

Overall, KnowledgeC plays a crucial role in digital forensics investigations by providing a detailed and comprehensive overview of the user's interactions and activities on the iOS device, ultimately contributing to a more thorough examination and a deeper understanding of the user's digital footprint.

## STUDENT EXERCISE – APPLICATION USAGE

1. Is the program Snapchat installed on the device? If so, when was it installed?
2. Snap Chat and TikTok both have Package Names that are different from their Display Names. What are the package names of each?
3. What is the Display Version of Tinder that is installed on the device?
4. Are location services enabled on the phone?
5. What is the Serial Number for the phone?
6. What is the name of the phone?
7. On 10-/31/2022, at 4:30 PM, was the phone locked or unlocked?
8. On 10/31/2022, between 4:05:06 and 4:05:20, what application was in use?
9. On 10/31/2022 at 4:19:42 PM, the user received a notification on the phone. What was the notification for?
10. Clear all filters



## OPERATING SYSTEM

Operating system evidence encompasses information that provides insights into the functioning of a computer or mobile device. This evidence includes details such as the file system, owner information, configured accounts, cell tower and Wi-Fi connections, as well as device state information like time settings, battery level, and lock state.

### Apple Accounts & Owner Information

Apple Accounts and Owner Information artifacts hold detailed information about all Apple accounts associated with the device, as well as essential data about the device's owner.

These artifacts include specific information about the owner, including the Device Name, Phone Number, and Apple ID. Furthermore, they also contain the DSID (Directory Services/Storage Identification) of the device's owner. The DSID serves as a unique method of identifying Apple ID accounts. It functions as an equivalent to a serial number for the device but is exclusively assigned to an Apple ID or iCloud account.

The DSID plays a crucial role in accurately identifying and distinguishing Apple ID or iCloud accounts. For example, if a user changes the Apple ID email address associated with the device, the DSID does not change.

The Apple Accounts and Owner Information artifact are a vital resource for digital forensics investigations, as they provide critical insights into the user's Apple account usage, iCloud-related activities, and establishes a direct link between the device and its owner through the DSID. Understanding this information allows investigators to gain a deeper understanding of the user's digital behavior and interactions within the Apple ecosystem.

### Cell Tower Locations

The Cell Tower Locations artifact stores records of the cell towers to which the device has connected at various times. Each connection to a cell tower generates detailed information that is captured and stored. However, it should be noted that information is written to this database at set intervals, not when the device has connected to a cell tower. As such, this information provides an estimate of the area that a device has been in. It cannot be used for precise location information. It should also be noted that the database containing Cell Tower Locations only has a retention period of seven days.

This information includes the approximate date and time of the connection, providing a timeline of the device's cellular activity. Additionally, the GPS coordinates of the cell tower are recorded, allowing investigators to pinpoint the tower's geographical location.

The mobile network code associated with the cell tower is also included in the data. This code can be used to identify the specific cellular provider associated with the tower, giving insights into the user's network service provider.

Furthermore, the Cell Tower Locations artifact records a confidence interval, indicating the level of certainty or accuracy of the cell tower's location data. This helps assess the reliability of the location information.

Additionally, the approximate distance (Range) between the device and the cell tower is documented, which aids in understanding the device's proximity to the tower at the time of connection.

For digital forensics investigations, analyzing the Cell Tower Locations artifact is crucial in understanding the user's movements and patterns of cellular connectivity. By examining this data, investigators can reconstruct the device's location history, track its movements, and establish a timeline of the user's cellular activities. This information can be invaluable in determining the user's whereabouts and actions during the course of an investigation.

### PowerLog

PowerLog is a database that records battery usage details on the device, including data on power consumption by



various applications. Apple utilizes PowerLog to offer users a summarized view of their device's battery health and a list of applications consuming battery power. This database provides valuable insights into power usage patterns, revealing which applications are utilizing how much power.

In AXIOM, PowerLog artifacts are categorized into multiple sub-categories, encompassing essential information such as battery level, camera state, lock state, cable status, and autolock. This information can be used to develop a comprehensive understanding of the user's pattern-of-life.

By examining the PowerLog data, investigators gain valuable knowledge about the user's app usage and power consumption patterns over time. This information sheds light on the user's typical device behavior and daily routines. Moreover, it allows investigators to delve deeper into the user's app preferences and overall battery performance.

Overall, PowerLog provides crucial insights for digital forensics investigations, facilitating a more profound analysis of the user's digital behavior, usage habits, and app interactions, ultimately contributing to a better understanding of the user's overall device usage patterns.

## STUDENT EXERCISE – OPERATING SYSTEM

1. What is the DSID for the user?
2. Review all of the Cell Tower Locations that were recorded in the database on 10/26/2022 at 1:47:09 PM. What is the general location of the user?
3. Review all of the Cell Tower Locations that were recorded in the database 10/30/2022 at 9:50:23 PM. What is the general location of the user?
4. On 10/30/2022, at 9:14:28 PM, one Cell Tower Location was recorded in the database. What Mobile Network was the phone connected to? Include the Mobile Network Code and the Cellular provider?
5. What is the lowest battery percentage ever on the phone and what is the Display Date/Time of when this happened?
6. What is the last Display Date/Time that the lightning cable was connected to the phone?
7. What two Timezone has this phone been in during the month of October 2022?
8. What application has sent the most data via the cellular network?
9. Clear all filters





## ENCRYPTION & CREDENTIALS

Encryption and credentials evidence encompass information related to how individuals safeguard their files and accounts. This evidence includes encrypted files, password-protected files, as well as user login names, passwords, and tokens used to access user accounts.

### Apple Keychain

The Apple Keychain serves as the password management system on an iOS device, securely storing account passwords and tokens in an encrypted container. The information stored in the Keychain is protected by a separate encryption scheme, different from the encryption used for other files on the device.

Within AXIOM, Keychain information is organized into two artifact categories:

- **Apple Keychain Generic Passwords:** This category contains login information for various accounts and WiFi networks. While most of the data in the Value column is not in plain text, making it challenging to determine passwords, the password for WiFi networks is typically listed in plain text.
- **Apple Keychain Internet Passwords:** In this category, Safari saves values when users choose to store their login credentials. Although most of the information is not in plain text, there may be account information and passwords in plain text.

During digital forensics investigations, analyzing the Keychain data is essential for understanding the user's stored credentials and passwords, especially when conducting encrypted logical acquisitions. However, due to the encryption measures in place, not all data in the Keychain may be accessible in plain text form. Nonetheless, the available information can still provide valuable insights into the user's login behavior and usage of encrypted credentials on the iOS device.

## STUDENT EXERCISE – ENCRYPTION & CREDENTIALS

1. List the Account Names and Passwords for the following:

Service	Account	Password
Instagram		
Facebook		
TikTok		
Twitter		
LolaGranola Wireless		
ATT-WIFI-6WVL Wireless		



## CONNECTED DEVICES

Connected devices evidence refers to information that demonstrates how individuals utilize their Internet of Things (IoT) devices. This evidence includes data such as the timestamp and duration of device connections, geographical locations, and transferred data. Connected devices encompass a range of examples, such as Amazon Alexa, Apple Watch, Fitbit, Nest, Bluetooth devices, and also encompass relevant details about the device's SIM card.

### Apple Health

Apple Health data is an automatically collected dataset on iOS devices that encompasses various health-related metrics about the user's physical activities and physiological measurements. This data includes the number of steps taken, the count of floors climbed, and the distance walked, all of which are tracked passively by the device. For users who have an Apple Watch, additional health-related information is available, such as heart rate data, which is actively monitored by the watch.

The Apple Health data serves as a valuable resource for digital forensics investigations, as it allows examiners to examine the user's physiological data and gain insights into their health and activity patterns. By analyzing this information, investigators can understand movement of the user along with physical exertion.

Apple Health data can provide a window into the owner's physical activity levels, enhancing the digital forensics examination by offering an understanding of the user's physiological data and overall activity during an event under investigation.

### Find My

Find My is a comprehensive asset tracking service developed by Apple Inc. It allows users to track the real-time location of various Apple devices, including iPhones and AirTags. This tracking functionality is made possible through a connected iCloud account.

With Find My, users have the ability to not only track their own devices but also share their GPS locations with others who have Apple devices. This feature enables seamless location sharing among family members, friends, or colleagues. Additionally, users can view the real-time location of individuals who have chosen to share their location with them.

Find My offers a robust and integrated solution for people and asset tracking, enhancing user convenience and security by ensuring the ability to locate and monitor their devices and accessories efficiently.



## STUDENT EXERCISE – CONNECTED DEVICES

1. From earlier data, we know that on 10/31/2022, at 4:05:20: PM, Casey Newton made a phone call to detonate the drone bomb. Around that time, from Apple Health data, does it appear that she was physically active?
2. What is the largest number of Steps Taken by Casey Newton on 10/31/2022?
3. Does it appear that Casey Newton wears an Apple Watch?
4. What is the furthest distance that Casey Newton has walked and what date did this occur?
5. What is the last location recorded by Find My Devices for Casey Newton iPhone 11 and when was this recorded?
6. In iOS Messages, Chris Austin accused Casey Newton of planting an AirTag on him. Is there any evidence of this in Connected Devices?
7. What was the last location recorded by this AirTag and when was it recorded?
8. Apply a Relative Time Filter and view activity for five minutes prior to and after the time that the location of the AirTag was recorded. View iOS Messages. Do you see any evidence indicating that Casey is tracking Chris?
9. Remove the Relative Time filter and return to Connected Devices.
10. Is there any evidence in Find My Locations confirming that the last recorded location for the AirTag planted on Chris was at University Park Mall?
11. Clear all filters



## LOCATION & TRAVEL

Location and travel evidence encompass various types of information that shed light on an individual's whereabouts. Historical GPS locations reveal the past tracking of a device's GPS, providing insights into their previous locations. Map searches offer data on locations searched for using map applications, indicating areas of interest, or intended destinations. Significant locations denote places marked as significant by the device, which may include frequently visited spots like home, school, or workplace. Wi-Fi locations comprise information about Wi-Fi networks recognized or connected to by the device, as these networks are often specific to certain places such as coffee shops, libraries, or schools. Lastly, rideshare application data discloses details about rides taken using rideshare services, enabling the determination of specific locations visited as rides typically have identifiable start and end points. Collectively, these sources of evidence help establish a comprehensive understanding of an individual's movements and travel patterns.

### Cached Locations

Cached Locations is an artifact of the iOS device's location data. When location services are enabled on the device, it records location points over time, with the frequency depending on the device's activity. For instance, if the device is locked and idle, Cached Locations may be collected every 15 to 60 minutes, while during active use, it could be as frequent as once per second.

Some apps that have been granted Location Services permissions also may record speed data (in Meters per Second) for each Cached Location point. Apps like Maps, Snapchat, Weather, and Camera are likely to record speed data. However, other applications, such as SMS, will not record this data.

For digital forensics investigations, analyzing iOS Cached Locations can provide valuable location-based evidence, helping investigators understand the device's movements and usage patterns over time. This data can be crucial in establishing a timeline of the device owner's activities and whereabouts during a specific period. However, in order to recovery Cached Locations, a full file system acquisition within seven days of the offense is required. Cached Locations are only maintained in the database for a period of seven days.

### Significant Locations & Significant Locations Visits

iOS Significant Locations is an artifact that stores locations that an Apple algorithm deems significant to the user. The exact workings of the algorithm are undisclosed, but the locations are determined based on the frequency and recency of visits. The retention period for records in this database is not explicitly known, but they are typically retained for several months.

iOS Significant Locations Visits is an artifact that keeps a historical record of visits to locations that have been designated as Significant Locations. These locations are considered important based on the user's visitation patterns.

For digital forensics investigations, analyzing Significant Locations and Significant Locations Visits can provide valuable insights into the user's frequently visited places and routine movements. By examining this data, investigators can establish a pattern of the user's activities, preferred locations, and potential points of interest. This information can be useful in reconstructing the user's timeline, understanding their behavior, and identifying significant places related to the investigation.

### WiFi Locations

WiFi Locations is an artifact of locations of Wi-Fi networks that the device has encountered. It records the locations of Wi-Fi networks that the device has come across, even if the device did not connect to them; it is sufficient for the device to detect the network.

Similar to Cached Locations, this database is accessible through a full file system acquisition of the device. However, it's worth noting that WiFi Locations has a retention period of approximately seven days, meaning that older data may not be available.



For digital forensics investigations, analyzing WiFi Locations can provide valuable information about the device's past interactions with various Wi-Fi networks. By examining this data, investigators can gain insights into the device's movements and the locations it has been in proximity to. This can be useful for establishing the user's whereabouts or tracking the device's travels over a specific time frame.



## STUDENT EXERCISE – LOCATION AND TRAVEL

1. Casey Newton was interviewed regarding the killing of Chris Austin. During her interview, she stated that she was not involved and was in Chicago the entire day on 10/31/2022. Using Cached Locations, can her alibi be verified?
2. When Casey was in Chicago on 10/31/2022, what is the name of the building that she was staying at?
3. Prior to the killing, Casey Newton walked from one building to another on the campus of Notre Dame. What building did she start out at and where did she walk to?
4. View all of the Significant Locations in the State of North Carolina. What city are they associated with?
5. Casey still denies that she was in South Bend during the time of the killing and she states that she has never been to Duncan Student Center. Using Significant Locations Visits, can her alibi be verified?
6. Apply a date filter of 10/31/2022. View Cached Locations. In general, notice where Casey began in Chicago, the route she took to South Bend, and where she ended near Notre Dame. Now switch to WiFi Locations and view the mapping. Does this information correspond with the Cached Locations?
7. While still in WiFi Locations, zoom into the area of Notre Dame and South Bend. The data should begin to form two groups. One group is at Notre Dame. What is the significance of the other group?
8. Clear all filters











# MODULE 6

Reporting

## MODULE 6: REPORTING

- Reporting Introduction
- Excel Report
- PDF Report
- HTML Report
- Student Exercise



## LEARNING OBJECTIVES AND GOALS:

This module will introduce students to the reporting capabilities of the Portable Case. Students will learn techniques for generating shareable documents and files from the case, enabling effective presentation of their findings to stakeholders or team members. By understanding the available reporting features, students will be well-prepared to distribute the results of their analysis with clarity and efficiency. These skills will prove invaluable in effectively communicating analysis results and supporting decision-making processes during investigations or projects.



## REPORTING INTRODUCTION

Upon concluding an analysis, effective communication and distribution of the results are vital. The reasons for generating reports may vary for each case, such as additional analysis requirements, legal process directives, presentations to prosecutors, collaboration with stakeholders, or providing crucial intelligence during ongoing investigations. Regardless of the purpose, The Portable Case offers investigators the capability to generate reports in multiple formats for distribution.

For distribution purposes, an examiner can create one of three types of reports from the Portable Case: 1) An Excel report, 2) A PDF report, or 3) an HTML report. Each of these reports contains the same information from the Portable Case but presented in different formats. The choice of which report type to use depends on the specific needs of the target audience. In the sections below, we will introduce each type of report and demonstrate how to generate reports from the Portable Case.

Regardless of the type of report that is generated, they each are initiated in one of two ways. First, reports can be initiated from the File menu by selecting Create export / report:

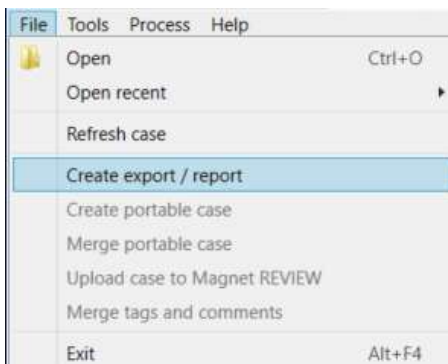


FIGURE 6-1: INITIATING A REPORT VIA THE FILE MENU

The second way to initiate a report is by right-clicking on any artifact or artifact category and selecting Create export report:

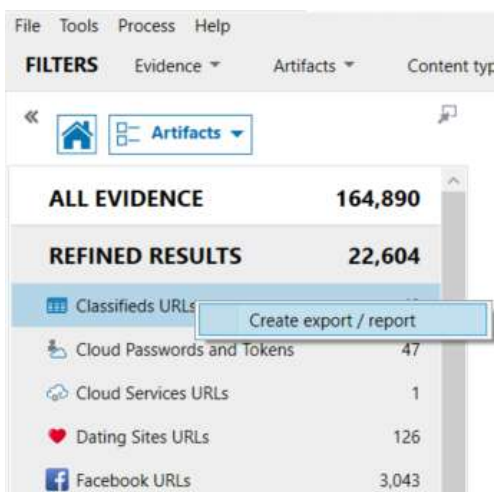


FIGURE 6-2: INITIATING A REPORT VIA RIGHT-CLICKING

When selecting either method for initiating a report, both will open the Create export / report box where the user then selects the type of report that you wish to generate:

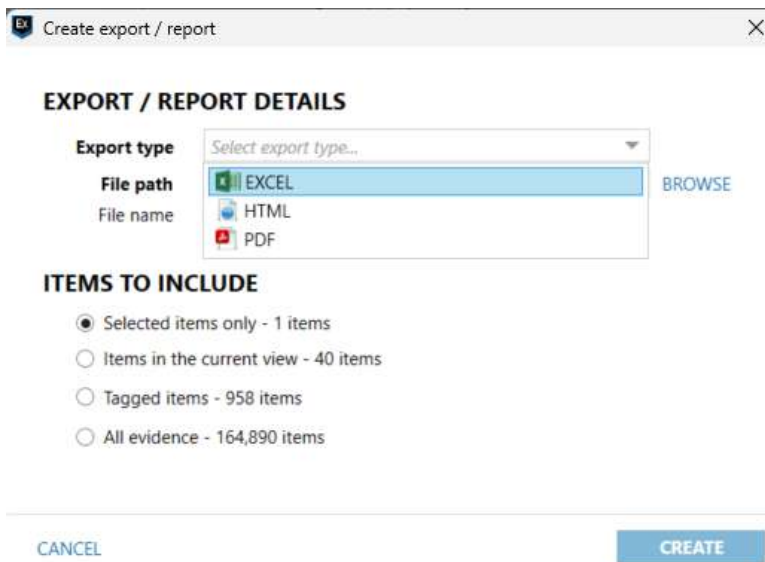


FIGURE 6-3: SELECTING THE TYPE OF REPORT

Once selecting the type of report (Export type), the user is then required to select a number of options:

## EXPORT / REPORT DETAILS

- **Export Type:** The type of report that the user wishes to generate.
- **File Path:** This is the location on the user's computer where the report, along with all supporting files, is saved. By default, the report is saved to the same folder as the Portable Case. The user can specify a different location by selecting the BROWSE button.
- **File Name:** The File name field will be automatically populated based on the Export type chosen by the user. PDF and HTML reports will be named Report while Excel reports will be named Exported results.xlsx. Once the report is saved to the local hard drive of the user's computer, these file names can be changed if desired.

## ITEMS TO INCLUDE

- **Selected items only:** Only the artifacts that are selected and highlighted in the Portable Case
- **Items in the current view:** The artifacts currently being displayed in the Evidence Pane
- **Tagged items:** The artifacts that the user tagged in the Portable Case. When selecting Tagged item, users will also be presented with a drop-down menu to include or exclude each tag type.
- **All evidence:** All artifacts from the case
- **Don't include previews or file attachments in the report:** By checking this checkbox, previews or file attachments for the artifacts will not be saved to the report that is generated. This option is commonly used when the Portable Case contains contraband files such as Child Sexual Abuse Materials (CSAM). In some situations, such as the production of reports for defense counsel, these files are excluded.

## LEVEL OF DETAIL

- **High-level information in one report:** Selecting this option will generate one report that contains all of the artifacts selected from ITEMS TO INCLUDE.



- Detailed information with individual reports per artifact type – Selecting this option will generate individual reports for each artifact type selected from ITEMS TO INCLUDE.

Once the user selects the options for report, hitting the CREATE button will generate the report and save it to the location specified by the user.

## EXCEL REPORT

Excel spreadsheets offer numerous advantages for data management, reporting, and distribution. They provide an organized layout for viewing data, along with powerful calculation capabilities using formulas and functions. Data can be visually represented through charts and graphs, making it easier to interpret patterns and trends. Excel also allows for data filtering, sorting, and validation. Its versatility enables seamless collaboration with external stakeholders.

When producing a report in Excel format, a spreadsheet will be generated containing comprehensive data related to the selected artifacts. This includes essential artifact information, along with additional details such as date/time stamps, the artifact's storage location, and the specific item of evidence from which it was recovered. The Excel report provides a thorough and organized summary of the selected artifacts, making it a valuable tool for distribution of results to stakeholders.

	A	B	C	D
	Search Term	Original Search Query	URL	Date/Time - UTC+00:00 (M/d/yyyy)
1	how to get around a restraining order		https://www.google.com/search?q=how+to+get+around+a+restraining+order&ie=UTF-	10/25/2022 6:00:11 PM
2	christopher orion		https://www.google.com/search?q=christopher+orion&ie=UTF-8&oe=UTF-8&hl=en-us&	10/25/2022 6:00:11 PM
3	how to track an android		https://www.google.com/search?q=how+to+track+an+android&ie=UTF-8&oe=UTF-8&h	10/25/2022 6:00:11 PM
4	ninias nails		https://www.google.com/search?q=ninias+nails&ie=UTF-8&oe=UTF-8&hl=en-us&client=	10/25/2022 6:00:11 PM
5	can someone tell if you are tracking them w		https://www.google.com/search?q=can+someone+tell+if+you+are+tracking+them+wit	10/25/2022 6:00:11 PM
6	closest starbucks to mw		https://www.google.com/search?q=closest+starbucks+to+mw&ie=UTF-8&oe=UTF-8&hl	10/25/2022 6:00:11 PM
7	stream oprah harry megghan		https://www.google.com/search?q=stream+oprah+harry+megghan&ie=UTF-8&oe=UTF-8	3/9/2021 12:20:47 AM
8	orion constellation wallpaper	orion constellation wallpap	https://www.google.com/search?q=orion+constellation+wallpaper&tbm=isch&ved=2a	3/9/2021 12:20:47 AM
9	where to buy android tracking devices		https://www.google.com/search?q=where+to+buy+android+tracking+devices&ie=UTF-	3/9/2021 12:20:47 AM
10	orion constellation		https://www.google.com/search?q=orion+constellation&ie=UTF-8&oe=UTF-8&hl=en-u	3/9/2021 12:20:47 AM
11	full moon june 2021 strawberry moon		https://www.google.com/search?q=full+moon+june+2021+strawberry+moon&client=s	6/23/2021 2:36:53 PM
12	good restaurants in chicago		https://www.google.com/search?q=good+restaurants+in+chicago&ie=UTF-8&oe=UTF-8	9/27/2022 5:45:21 PM
13	how to track an android		https://www.google.com/search?q=how+to+track+an+android&ie=UTF-8&oe=UTF-8&h	8/18/2022 11:12:43 PM
14	good restaurants in chicago		https://www.google.com/search?q=good+restaurants+in+chicago&ie=UTF-8&oe=UTF-8	9/27/2022 5:45:23 PM
15	orion constellation wallpaper		https://www.google.com/search?q=orion+constellation+wallpaper&tbm=isch&hl=en-u	9/27/2022 5:45:23 PM
16	iphone case		https://www.google.com/search?q=iphone+case&ie=UTF-8&oe=UTF-8&hl=en-us&clie	9/27/2022 5:45:23 PM
17	how to get around a restraining order		https://www.google.com/search?q=how+to+get+around+a+restraining+order&ie=UTF-	8/18/2022 11:13:07 PM
18	ninias nails		https://www.google.com/search?q=ninias+nails&ie=UTF-8&oe=UTF-8&hl=en-us&client=	8/18/2022 11:13:17 PM
19	orion constellation		https://www.google.com/search?q=orion+constellation&client=safari&hl=en-us&prmc	8/18/2022 11:13:17 PM
20	how to track an android		https://www.google.com/search?q=how+to+track+an+android&ie=UTF-8&oe=UTF-8&h	10/25/2022 6:00:11 PM
21	christopher orion		https://www.google.com/search?q=christopher+orion&ie=UTF-8&oe=UTF-8&hl=en-us&	8/18/2022 11:07:50 PM
22	christopher orion		https://www.google.com/search?q=christopher+orion&ie=UTF-8&oe=UTF-8&hl=en-us&	10/25/2022 6:00:11 PM
23	orion constellation wallpaper		https://www.google.com/search?q=orion+constellation+wallpaper&tbm=isch&hl=en-u	10/25/2022 6:00:11 PM
24	ninias nails		https://www.google.com/search?q=ninias+nails&ie=UTF-8&oe=UTF-8&hl=en-us&client=	10/25/2022 6:00:11 PM
25	halloween couples costume ideas		https://www.google.com/search?q=halloween+couples+costume+ideas&ie=UTF-8&oe	10/25/2022 6:00:11 PM

FIGURE 6-4: EXCEL REPORT OF GOOGLE SEARCHES

Finally, when producing an Excel report that contains artifacts such as pictures and videos, a thumbnail picture of the original file will be produced on the spreadsheet and the full-size files will also be exported with the report and saved to a folder named /Attachments. These full-size files can then be reviewed or used as exhibits in legal proceedings.





	A	B	C	D
1	<b>File Name</b>	<b>File Extensio</b>	<b>Image</b>	<b>Created Date/Time - UTC+00:00 (M/d/yyyy)</b>
2	IMG_0138	.HEIC		10/31/2022 3:53:52 PM
3	IMG_0364	.HEIC		10/31/2022 3:58:28 PM

FIGURE 6-5: EXCEL REPORT WITH THUMBNAILS

## PDF REPORT

PDF report also offer certain advantages. These include universal compatibility across platforms, preservation of formatting, data security through encryption and password protection, print-friendliness, compact file size for easy sharing, and non-editable format to maintain integrity. PDF reports support embedding media and hyperlinks, facilitating interactive elements. They are suitable for archiving and long-term storage, ensuring accessibility and consistency over time. Overall, PDF reports offer a secure, professional, and accessible format for sharing critical information.

When producing a report in PDF format, depending on the artifacts selected for the report, multiple documents may be created. Each PDF report will include a page of basic case information, including the Case Overview and Evidence Overview.



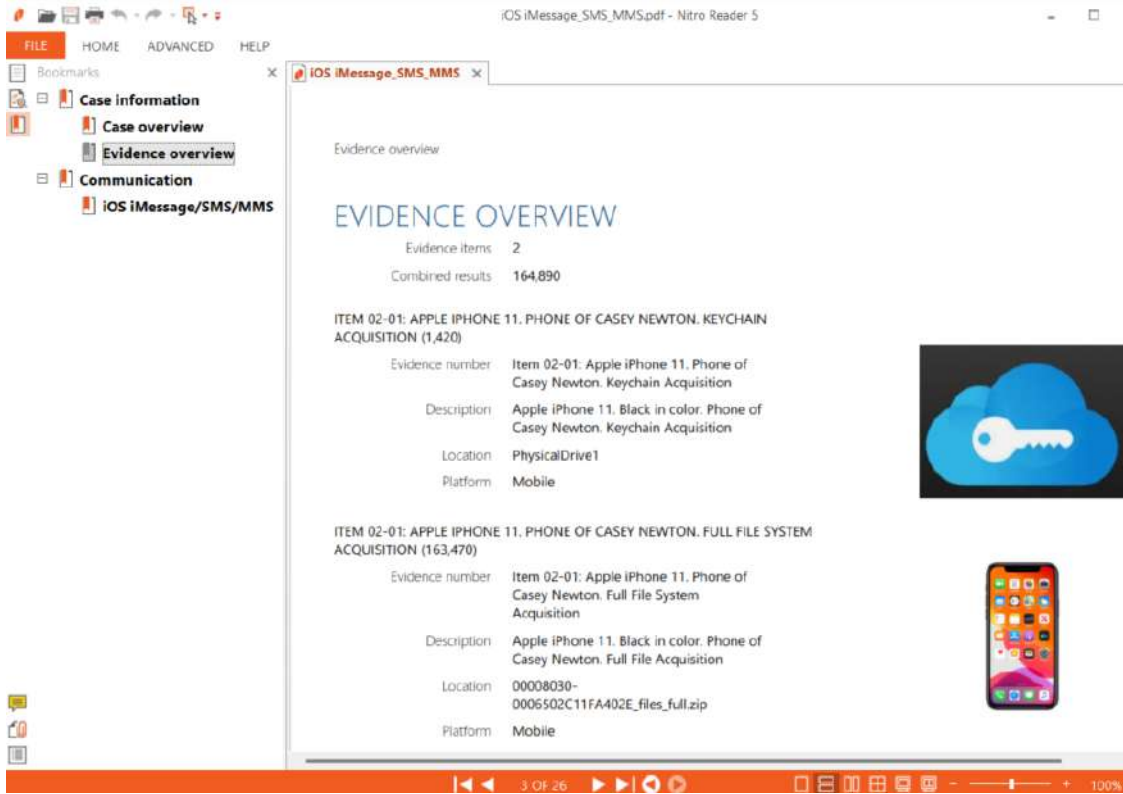


FIGURE 6-6: PDF REPORT EVIDENCE OVERVIEW

Similar to the Excel report, if the PDF report contains any artifacts such as pictures, videos, or documents, the original artifact will be exported and saved into a folder named /Attachments. Also, if the PDF report contains any conversations, a separate page for each conversation will be created and saved to the folder /Chat preview report.

**IOS IMESSAGE/SMS/MMS**

CHAT PARTICIPANTS	
Number of participants	3
Display names	+15742209526 Dolan Shaver (+15742209526) Local User
Local user	Local User
CONVERSATION DETAILS	
Number of messages	28
First message sent date/time	10/11/2022 5:50:23 PM
Last message sent date/time	10/13/2022 5:24:15 PM
Case time zone	(UTC) Coordinated Universal Time



FIGURE 6-7: PDF CHAT PREVIEW REPORT





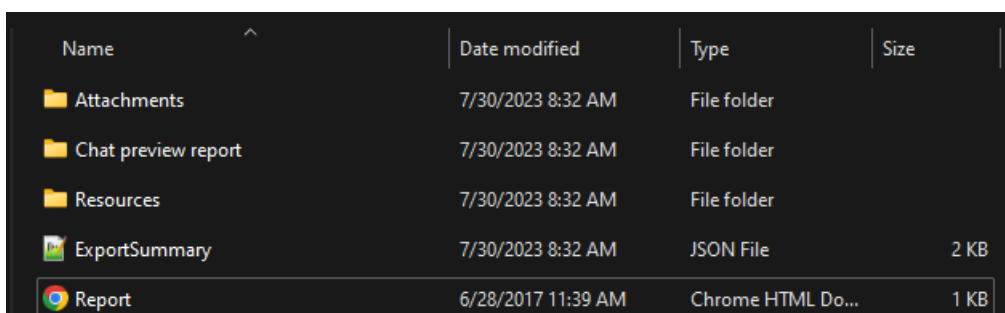
## HTML REPORT

HTML reports offer numerous advantages that make them an excellent choice for presenting and distributing analysis results. One key advantage is their cross-platform compatibility, enabling viewing on various platforms and browsers without compatibility issues. Furthermore, HTML reports allow for interactive and dynamic content, enabling users to interact with multimedia elements and hyperlinks, facilitating easy navigation and data exploration.

Another prominent advantage of HTML reports is their ease of sharing and distribution. They can be shared via email, uploaded to websites, or distributed through external media like thumb drives or hard drives. This flexibility ensures that the report can reach a wide audience, regardless of the preferred distribution method. Overall, HTML reports provide a versatile and user-friendly option for effectively presenting analysis findings, engaging stakeholders, and facilitating easy access to information across different platforms and devices.

When producing a report in HTML format, AXIOM will generate multiple files:

- **Report.html** — Contains the main page of the report. The .html report is opened by double-clicking this file.
- **Resources** — Contains any resources needed to display the report. These include items such as images, style sheets, Java script, etc.
- **Attachments** — Contains any file attachments needed for the report. This folder will include any pictures or documents that were exported during the creation of the report.
- **Chat Preview Report** — Contains .html pages of individual threaded chat conversations. This folder will only be presented if chat conversations were included as part of the report.
- **ExportSummary.json** — Contains a summary of the settings used when generating the report.



Name	Date modified	Type	Size
Attachments	7/30/2023 8:32 AM	File folder	
Chat preview report	7/30/2023 8:32 AM	File folder	
Resources	7/30/2023 8:32 AM	File folder	
ExportSummary	7/30/2023 8:32 AM	JSON File	2 KB
Report	6/28/2017 11:39 AM	Chrome HTML Do...	1 KB

FIGURE 6-8: .HTML REPORT FOLDER STRUCTURE

When the document "Report.html" is double-clicked, it will open the case report in a web browser. The report's layout comprises two main sections: Navigation Pane (left side) and the Evidence Pane (right side).

The Navigation Pane allows for easy navigation through different sections or items within the report. Users can click on specific items in the menu to access more detailed information about them.

The Evidence Pane displays the specific details corresponding to the item selected in the Navigation Pane. As users click on different items in the menu, the content in the Evidence Pane dynamically updates to show relevant information, ensuring a seamless and focused reading experience.



Record	Tags	Comments	Search Term	URL
1	Google Search		how to get around a restraining order	https://www.google.com/search?q=how+to+get+around+a+restraining+order&ie=UTF-8&oe=UTF-8&hl=en-us&client=safari
2	Google Search		christopher orion	https://www.google.com/search?q=christopher+orion&ie=UTF-8&oe=UTF-8&hl=en-us&client=safari
3	Google Search		how to track an android	https://www.google.com/search?q=how+to+track+an+android&ie=UTF-8&oe=UTF-8&hl=en-us&client=safari

FIGURE 6-9: .HTML REPORT

This navigation setup in the HTML report enables users to explore and review the report's content in a structured and user-friendly manner, enhancing their understanding and analysis of the case information.



## STUDENT EXERCISE – CREATING REPORTS

### EXCEL REPORT

1. We want to create an Excel report of all phone calls sent or received on the device.
2. Select the artifact category iOS Call Logs
3. From File, select 'Create export / report'
4. Export type: Excel
5. File path: Browse to where you want to save the report
6. File Name: Default name
7. Items to Include: Items in current view – 51 items
8. Level of Detail: Detailed information with individual reports per artifact type
9. Hit CREATE
10. Open the folder where the report was saved. There should be two files present. ExportSummary contains a summary of the export. iOS Call Logs.xlsx contains records in the report.
11. Open and view iOS Call Logs.xlsx
12. Return to the Portable Case and clear any filters.

### PDF REPORT

We want to create a .pdf of all of the iOS Messages between Casey Newton and Chris Austin

1. Select the artifact category iOS iMessage/SMS/MMS
2. Switch to Conversation View
3. In the Evidence Pane, select the conversation between Chris Austin and Casey Newton. Tag all of the messages as "Conversation with Ryan Jennings."
4. Return to Column View, right-click on any message in the Evidence Pane, select 'Create export/ report.'
5. Export Type: PDF
6. File path: Browse to where you want to save the report
7. File Name: Default name
8. Items to Include: Tagged items. From the drop-down that opens, uncheck everything except for the tag "Conversation with Ryan Jennings."
9. Level of Detail: Detailed information with individual reports per artifact type
10. Hit CREATE
11. Open the folder where the report was saved. There should be four files/folders present.
12. Attachments – Any files that were sent with the text messages



13. Chat preview report – A PDF document of the threatened conversation
14. ExportSummary – A summary of the export
15. iOS Message\_SMS\_MMS – The PDF report that was generated
16. Open and view iOS Message\_SMS\_MMS.pdf
17. Navigate to the folder Chat preview report. Open and view the PDF document in that folder
18. Return to the Portable Case and clear any filters.

## HTML REPORT

We want to create a HTML report of all items that we tagged during the analysis.

1. From File, select 'Create export / report'
2. Export type: HTML
3. File path: Browse to where you want to save the report
4. File Name: Default name
5. Items to Include: Tagged items
6. Level of Detail: Detailed information with individual reports per artifact type
7. Hit CREATE
8. Open the folder where the report was saved and open the file Report.html
9. Navigate through the HTML report
10. Return to the Portable Case and clear all filters









# MODULE 7

Magnet OUTRIDER

## MODULE 7: MAGNET OTRIDER

- Magnet OTRIDER Introduction
- Key Features of OTRIDER
- Understanding System Changes
- Preparing a Mac Device to be Scanned
- Preparing an Android Device to be Scanned
- Encryption Detection (Windows Scan Only)
- Configuring a Scan Template
- Scanning a Windows System
- Scanning a macOS System
- Scanning an Android Device
- Reviewing Scan Results





## **LEARNING OBJECTIVES AND GOALS:**

In this module, students will be introduced to Magnet Forensics Outrider, a powerful tool for triaging mobile devices and computers. They will learn about the program's capabilities and how to effectively use it to expedite the process of identifying actionable evidence. Magnet Outrider is specifically designed to optimize speed and efficiency, enabling investigators to quickly identify and prioritize relevant data for further analysis. By the end of this module, students will be equipped with essential skills to leverage Magnet Outrider for efficient and effective digital forensic investigations.



## MAGNET OTRIDER INTRODUCTION

Law enforcement agencies are grappling with the ever-increasing volume and complexity of digital evidence, presenting a daunting challenge for investigators. Whether they are conducting on-site triage of mobile devices and computers or dealing with a backlogged collection of evidence in the lab, the time taken to process this data is of utmost importance. Magnet OTRIDER was developed to address these issues.

Magnet OTRIDER is designed to run from an external drive and maximize speed and simplicity in the process of identifying actionable evidence. This tool equips examiners and non-technical stakeholders with the capability to swiftly access information that is critical for cases. By efficiently navigating through vast volumes of digital data, OTRIDER streamlines the investigation process, allowing for timely and effective decision-making, thereby increasing the overall efficiency of digital forensics workflows.

One of the key advantages of OTRIDER is the significant time-saving it offers in the field or lab. Examiners can uncover critical hits on various digital devices, such as mobile phones, Mac and Windows computers, and external hard drives, in just minutes. This rapid processing ability ensures that crucial evidence is promptly identified, enabling investigators to focus their efforts on analyzing and prioritizing pertinent data swiftly.

Magnet OTRIDER addresses the challenges faced by law enforcement agencies in managing and analyzing digital evidence. By providing unparalleled speed, simplicity, and accuracy in identifying actionable evidence, OTRIDER empowers investigators to make informed decisions swiftly and effectively, optimizing the overall investigative process.

## KEY FEATURES OF OTRIDER

Magnet OTRIDER is designed for evidence triage. It provides automated insights for quick identification of actionable evidence on Android devices and Windows systems. The tool offers customizable reports, simultaneous scanning of multiple devices, and cross-referencing of live computer IPs for more efficient investigations.

1. **Triage for Illicit Content:** Magnet OTRIDER allows for efficient triaging of devices, both in the field and the lab, to identify illicit content, such as Child Sexual Abuse Material (CSAM). Its automated insights enable examiners and non-technical stakeholders to confidently use the tool.
2. **Scan Android Devices:** OTRIDER eliminates the need for manual scans on Android devices. It automatically searches through SMS/MMS messages, device ID, recently used apps, contact lists, call logs, and more to find actionable evidence in minutes, leaving a minimal footprint on the device. The tool can also detect secure folders and multiple user accounts. Additionally, it supports scanning multiple devices simultaneously, saving time during field operations.
3. **Search Using Customizable Keyword Lists & NCMEC Reports:** Investigators can edit OTRIDER's existing keyword list or import their own keywords, such as account names, device IDs, browser terms, and URLs, to expedite the search for evidence. Leveraging common or known keywords is particularly effective in locating Contraband or CSAM. The tool also allows scanning of internet browser history for keywords using a National Center for Missing & Exploited Children (NCMEC) CyberTip report to bring in URLs and file names as keywords.
4. **Live System Scans Including RAM Capture:** OTRIDER performs live system scans on Windows operating systems, collecting valuable artifacts and capturing RAM. It can also take a screenshot of the desktop and obtain the external IP address for the system, providing critical insights for investigators.
5. **Preserve & Report Evidence:** Once scans are complete, OTRIDER generates comprehensive reports containing details about the scan, used keywords, and any saved files of interest from the device. Separate



reports can be created for each device when parallel scans are conducted. The generated reports are compatible with Magnet AXIOM and other third-party forensic tools for further analysis of the evidence.

6. **Device Identification:** OTRIDER provides the external IP address of a live computer, facilitating cross-referencing with other intelligence systems, such as the Child Protection System (CPS) or ICACCOPS. This feature enhances the potential for broader investigative insights and collaboration.

In summary, Magnet OTRIDER offers a robust set of features designed to expedite the triage process for digital evidence, identify illicit content efficiently, and produce comprehensive reports for further analysis. Its capabilities cater to the needs of both experienced examiners and non-technical stakeholders, streamlining digital forensic investigations and enhancing collaboration among law enforcement agencies.

## UNDERSTANDING SYSTEM CHANGES

Magnet OTRIDER is designed to run from external media (thumb drive or hard drive). For compatibility, it is recommended that the external media be formatted as exFAT. During execution of Magnet OTRIDER, the program may interact with the operating system to gather and process information. Depending on the specific operating system in use, the tool may make certain changes or modifications to access and extract data effectively. It is important that you understand changes that may be made.

### Changes Made to Windows Systems

Magnet OTRIDER operates in a non-modifying mode, meaning it does not make any changes or generate new files on the system where it is executed. However, a few automatic files are created by the Windows system during its execution. Subsequently examining the system's evidence using a forensic tool like Magnet AXIOM would reveal registry keys and prefetch files that came into existence when a USB drive was connected and Magnet OTRIDER was launched.

The following are the automatic files created on a Windows system:

- Registry keys are generated when Magnet OTRIDER is run from a USB dongle. These registry keys are specifically associated with the hardware ID of the connected USB drive.
- Prefetch files, such as "MAGNET OTRIDER.EXE-<value>.pf," are created in C:\Windows\Prefetch when Magnet OTRIDER is executed on a computer.

These files are inherent to the normal functioning of the Windows system and are produced as part of the routine operations when using Magnet OTRIDER via a USB drive. As an investigator, it is important to be aware of these artifacts and consider them while analyzing evidence from a system where Magnet OTRIDER has been utilized.

### Changes Made to macOS Systems

Upon the initial execution of Magnet OTRIDER on a macOS system, dynamic libraries are extracted to the designated installation folder and remain there for subsequent runs of the application. Within the Magnet OTRIDER X.X macOS folder, files are created, modified, and deleted in the Logs, Resources, and Reports directories, and these files persist across different sessions.

Temporary files are also generated at specific locations during the application's runtime. While these temporary files are removed upon a graceful exit of the application, they may remain if Magnet OTRIDER terminates unexpectedly. The locations where these temporary files are created are as follows:

- /System/Volumes/Data/private/var/folders/cl/
- /System/Volumes/Data/Users/[username]/Library/Saved Application State/-com.magnetforensics.outrider.savedState



Examples of the temporary files created in these locations include:

- CASESENSITIVETESTf3be3efe5b8447bda29e003a8905d265
- dotnet-diagnostic-8334-1634696265-socket
- clr-debug-pipe-8334-1634696265-in
- clr-debug-pipe-8334-1634696265-out

To access folders on the system, Magnet OTRIDER adds entries to the Transparency, Consent, and Control (TTC) database, with the bundle ID being com.magnetforensics.otrider. It's essential for forensic examiners to be aware of these file operations and locations while analyzing data from systems where Magnet OTRIDER has been utilized.

## PREPARING A MAC DEVICE TO BE SCANNED

By default, Magnet OTRIDER lacks the necessary permissions to scan protected system paths and private user folders. To enable such access, you must grant full disk access for Terminal and execute the Magnet OTRIDER admin script. This procedure ensures that the tool can effectively analyze and examine the designated areas on the system.

### Step 1: Allow Full Disk Access for Terminal

Prior to begging, consider running an initial scan on the device without full disk access enabled. This will detect all running applications.

Before you proceed, ensure that any open instances of Terminal are closed. Follow these steps to grant full disk access to Terminal, allowing Magnet OTRIDER to scan protected system paths and private user folders:

1. Open "System Preferences" on the macOS device.
2. In "System Preferences," click on "Security & Privacy," then "Privacy."
3. Under "Privacy", select "Full Disk Access," and click on the lock icon at the bottom left corner of the window.
4. Enter the username and password of an administrator account on the device to make changes.
5. Now, you have two options to allow Terminal access:
  - a. If "Terminal" is already listed among the allowed apps, select the checkbox next to "Terminal."
  - b. If "Terminal" is not in the list of allowed apps, click the "+" (Add) button, and navigate to "Applications/Utilities/Terminal." Click "Open" to add Terminal to the list.
6. Close the "Security & Privacy" window.

Finally, once you have finished scanning the device with Magnet OTRIDER, you can remove full disk access from Terminal to return the device to its previous state.

### Step 2: Run the Magnet OTRIDER Admin Script

1. Navigate to your Magnet OTRIDER installation folder and locate the file named "Start OTRIDER for macOS (admin).command."
2. Double-click on the file to open it. This action will launch a Terminal window.
3. Within the Terminal window, you will be prompted to enter the root password. Type in the root password and press Enter to proceed.



4. Keep the Terminal window open throughout your Magnet OTRIDER usage.
5. Once you have finished using Magnet OTRIDER, close the Terminal window to conclude the session.

## PREPARING AN ANDROID DEVICE TO BE SCANNED

Prior to scanning a target Android device, Developer Mode must be enabled and USB Debugging must be turned on. These settings allow OTRIDER to communicate with the Android device. Depending on the specific device, some of these settings may be found in different locations.

1. Enable Developer Mode by going to Settings > About Phone > Software Information. Tap Build Number seven times. You may then be prompted to enter the device PIN. Once the PIN is entered, Developer Mode is enabled.
2. Return to Settings and navigate to Developer options > USB Debugging. Hit the switch to turn on USB debugging. The Android device is now configured.

## ENCRYPTION DETECTION (WINDOWS SCANS ONLY)

When Magnet OTRIDER is launched, it automatically loads the available drives for scanning and conducts a check to identify any Bitlocker encryption on the computer and attached drives. While configuring your scan template, you have the option to include encryption detection information in the scan report.

If Magnet OTRIDER detects a drive that has been encrypted and password-locked using Bitlocker, you will receive a notification specifying which drive has been recognized as a Bitlocker-locked drive.

In case decryption is identified, you will be presented with the choice to proceed with the scan or close Magnet OTRIDER. The report on encryption, along with available recovery keys and passwords for detected Bitlocker drives, will be automatically placed in the case folder.

It is important to note that if Magnet OTRIDER does not detect any encryption, it does not guarantee the absence of encryption on the system. The tool might not be able to detect certain types of encryption.

If encryption is detected, it is advisable not to shut down your device unless you possess the password required to decrypt the encrypted containers or drives. Instead, consider preserving files or creating a live forensic image of the drive while the computer is powered on and you have decrypted access to the data.

## CONFIGURING A SCAN TEMPLATE

Scan templates come equipped with pre-configured options that offer a convenient and swift way to scan a specific target. These options can be tailored to match the requirements of different operating systems. If you are configuring a scan template for a particular operating system, you have the flexibility to filter the available options accordingly, streamlining the process of selecting the appropriate settings during template configuration.

1. Choose one of the following actions:
  - a. To create a new template, navigate to the Scan setup page and click "Add new template."
  - b. To edit an existing template, select the desired scan template and click "Edit template."
2. Provide a name for the scan template or modify the existing template name as needed.
3. Specify the operating system for which you want to view the scan options.
4. Configure the scan options to include in the template according to your requirements.



## SCANNING A WINDOWS SYSTEM

When conducting a scan on a Windows System, it's important to understand the implications of the Last Accessed date/time stamps enabled on the target system. If Last Accessed is enabled, this can lead to certain timestamps being changed and updated during the scan process, potentially affecting the integrity of the evidence if a forensic examination is conducted at a later date. It's important to be aware of this when executing OUTRIDER on a Windows system.

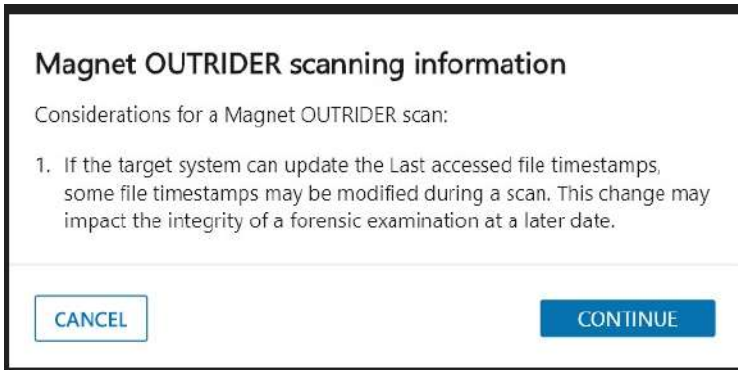


FIGURE 7-1: LAST ACCESSED TIMESTAM WARNING

To scan a Windows System, execute the batch file Start OURTIDER for Windows:

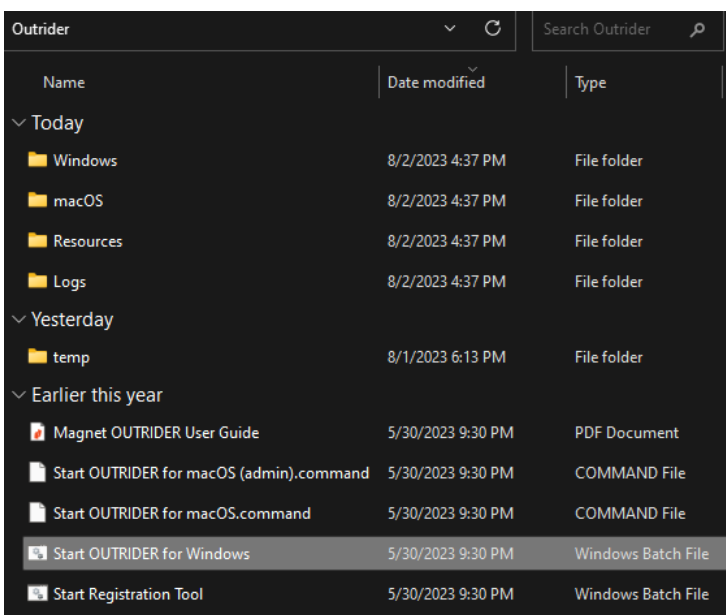


FIGURE 7-2: STARTING OUTRIDER ON A WINDOWS SYSTEM

Once OURTIDER opens, complete the following:

### Step 1: Enter a case number



FIGURE 7-3: ENTER CASE NUMBER

### Step 2: Select a Scan Template

The default template listed is name Default. By selecting EDIT TEMPLATE, you can view scan options for all supported operating systems. Select the option for Windows and review the settings. Change any setting

based on the specific circumstance of your case.

FIGURE 7-4: SELECT A SCAN TEMPLATE

**Step 3: Select Evidence**

All evidence available for scanning will be listed in Step 3. Should an item of evidence not be present, hit the REFRESH ALL link.

SELECT ALL REFRESH ALL

Location	Name	Description	Size
<input type="checkbox"/> Local Drive	C:\	OS	1.00 TB
<input checked="" type="checkbox"/> Local Drive	D:\	Cases	1.02 TB
<input checked="" type="checkbox"/> Local Drive	E:\		0.00 KB
<input checked="" type="checkbox"/> Local Drive	F:\		0.00 KB

FIGURE 7-5: SELECT EVIDENCE

Once the program is configured and the evidence is selected, hit the START SCAN button. OUTRIDER will scan the evidence and provide a summary once complete. From this summary, you can navigate to each of the categories that contained hits or you can click on the link OPEN REPORT to open the report for the Scan. By defaults, all reports are saved to the Outrider folder in a folder named Reports.





FIGURE 7-6: SCAN RESULTS

## SCANNING A macOS SYSTEM

To scan a macOS System, first ensure that all steps have been taken to prepare the Mac for scanning. Then execute the file Start OURTIDER for macOS.command:

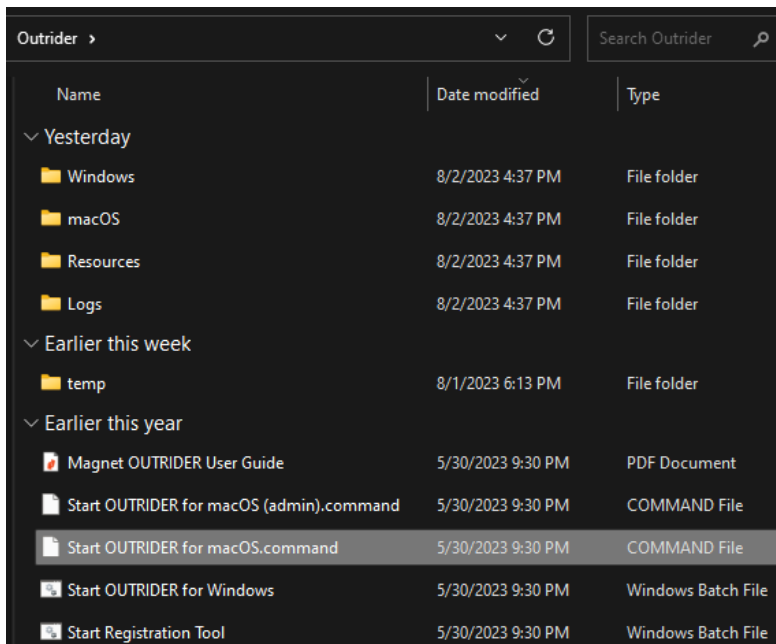


FIGURE 7-7: STARTING OURTIDER ON A MAC SYSTEM

Once OURTIDER opens, complete the following:

### Step 1: Enter a case number



FIGURE 7-8: ENTER CASE NUMBER





### Step 2: Select a Scan Template

The default template listed is name Default. By selecting EDIT TEMPLATE, you can view scan options for all supported operating systems. Select the option for OSX and review the settings. Change any setting based on the specific circumstance of your case.

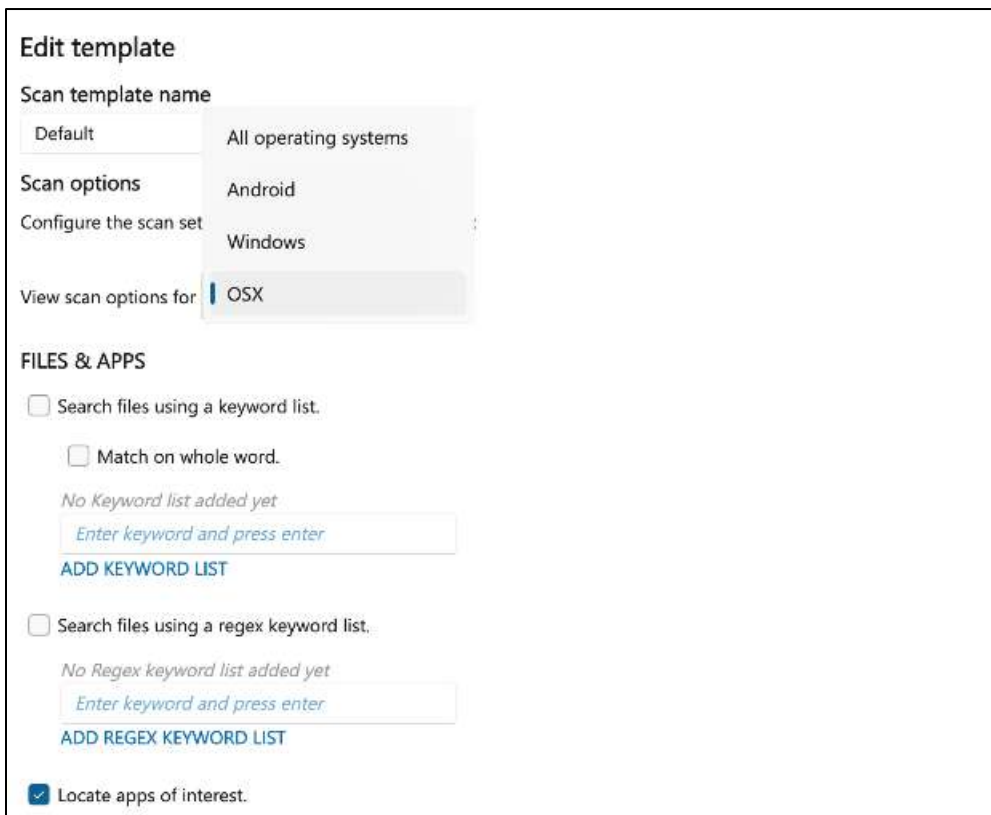


FIGURE 7-9: SELECT A SCAN TEMPLATE

### Step 3: Select Evidence

All evidence available for scanning will be listed in Step 3. Should an item of evidence not be present, hit the REFRESH ALL link.

SELECT ALL		REFRESH ALL	
Location	Name	Description	Size
<input checked="" type="checkbox"/> Local Drive	/	/	251 GB
<input type="checkbox"/> Removable Drive	/Volumes/Outrider/	/Volumes/Outrider	30.8 GB

FIGURE 7-10: SELECT EVIDENCE

Once the program is configured and the evidence is selected, hit the START SCAN button. OUTRIDER will scan the evidence and provide a summary once complete. From this summary, you can navigate to each of the categories that contained hits or you can click on the link OPEN REPORT to open the report for the Scan. By defaults, all reports are saved to the Outrider folder in a folder named Reports.



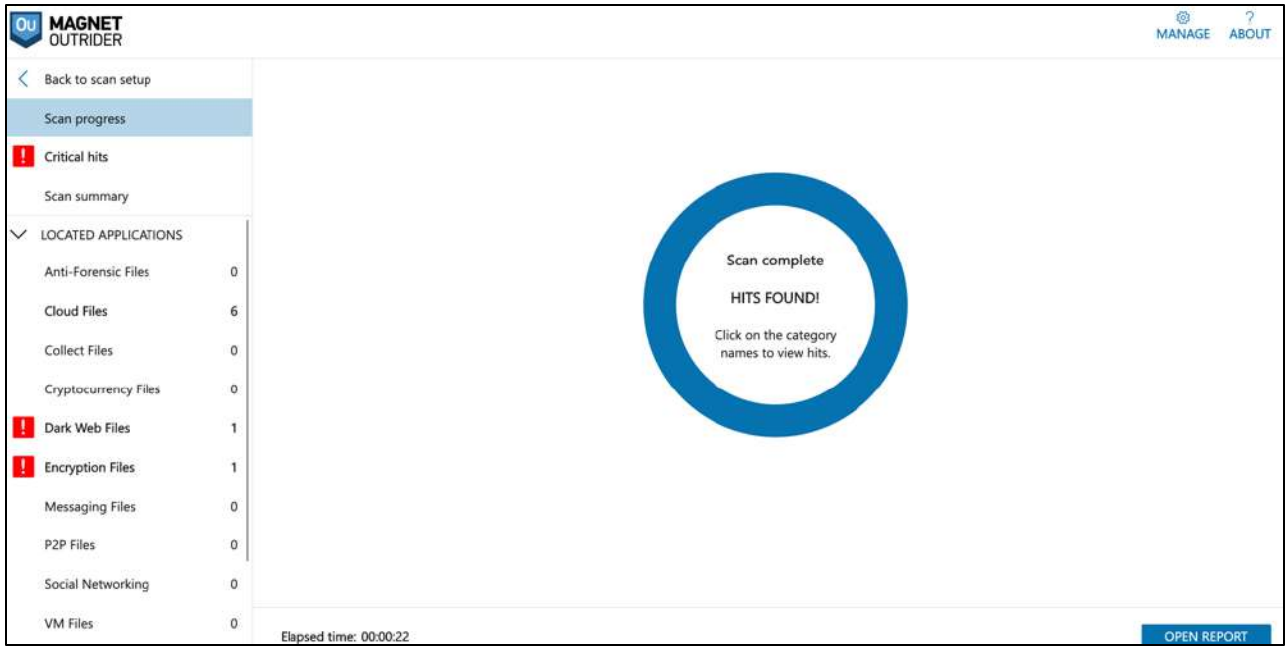


FIGURE 7-11: SCAN RESULTS

## SCANNING AN ANDROID DEVICE

To scan an Android, first ensure that all steps have been taken to prepare the Android for scanning. Once prepared, attach the Android device to the computer and then execute the file Start OURTIDER for Windows:

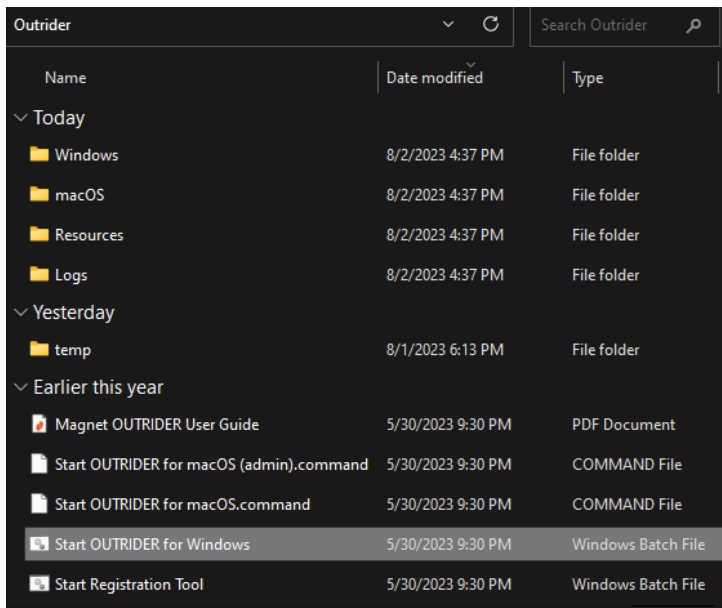


FIGURE 7-12: STARTING OURTIDER ON A WINDOWS SYSTEM

Once OURTIDER opens, complete the following:

### Step 1: Enter a case number



FIGURE 7-13: ENTER CASE NUMBER



### Step 2: Select a Scan Template

The default template listed is name Default. By selecting EDIT TEMPLATE, you can view scan options for all supported operating systems. Select the option for Android and review the settings. Change any setting based on the specific circumstance of your case.

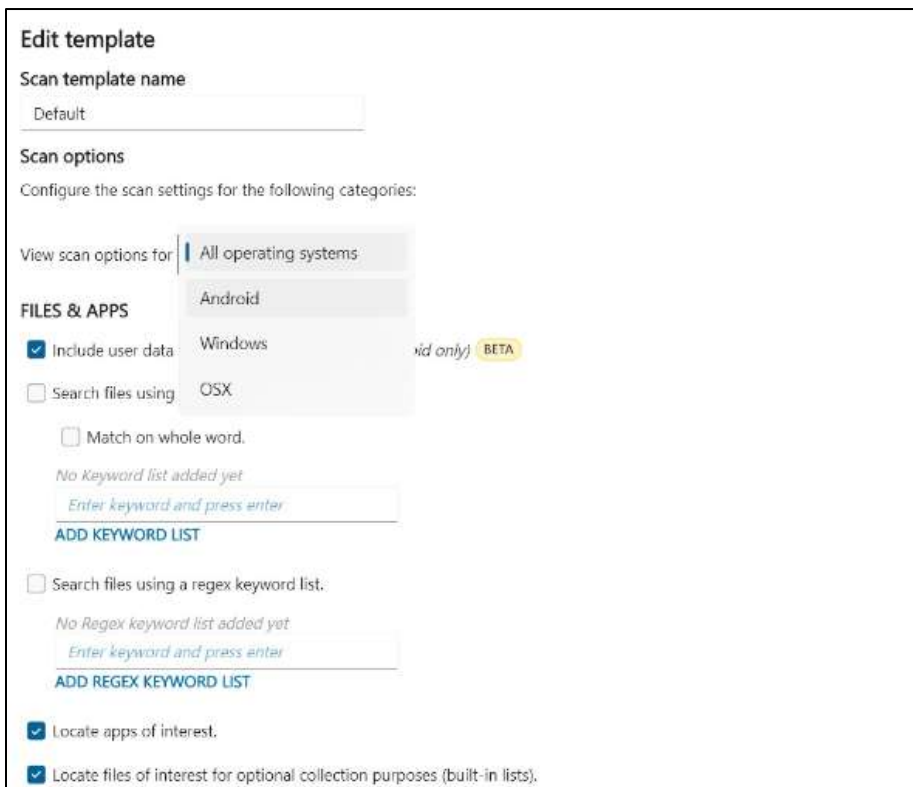


FIGURE 7-14: SELECT A SCAN TEMPLATE

### Step 3: Select Evidence

All evidence available for scanning will be listed in Step 3. Should an item of evidence not be present, hit the REFRESH ALL link.

SELECT ALL		REFRESH ALL		
	Location	Name	Description	Size
<input type="checkbox"/>	Local Drive	C:\	OS	1.00 TB
<input type="checkbox"/>	Local Drive	D:\	Cases	1.02 TB
<input type="checkbox"/>	Local Drive	E:\		0.00 KB
<input type="checkbox"/>	Local Drive	F:\		0.00 KB
<input type="checkbox"/>	Removable Drive	G:\	Outrider	30.8 GB
<input checked="" type="checkbox"/>	Mobile Device	Galaxy S20 FE 5G	SM-G781U	116 GB

FIGURE 7-15: SELECT EVIDENCE

Once the program is configured and the evidence is selected, hit the START SCAN button. OUTRIDER will scan the evidence and provide a summary once complete. From this summary, you can navigate to each of the categories that contained hits or you can click on the link OPEN REPORT to open the report for the Scan. By defaults, all reports are saved to the Outrider folder in a folder named Reports.





FIGURE 7-16: SCAN RESULTS

## REVIEWING SCAN RESULTS

During the scanning process, Magnet OTRIDER provides real-time updates on the progress, displaying the number of artifacts processed and items scanned. As the scan continues, you can begin to examine the identified hits through the following actions:

- Click on an application category to view new hits or to refresh the category. When hits are discovered, category names will be highlighted in bold.
- Pay special attention to critical hits, which are marked with an exclamation mark next to the title, indicating their significance.
- To access more information about a specific hit, right-click on a file result. From here, you can choose to open the source location of the file or save the source file for further analysis.

### Understanding “No Hits Round” Results

When Magnet OTRIDER produces a result of "No hits found," it does not necessarily imply that the drive is completely clear of relevant apps, keyword matches, or content related to Child Sexual Abuse Material (CSAM). It's important to be aware that some users have the ability to conceal files from the application, which may lead to undetected items. Nevertheless, scanning devices using Magnet OTRIDER remains valuable as it helps in prioritizing among multiple target devices.

There are instances where Magnet OTRIDER might not recover hits due to the file names on the scanned device not matching any of the loaded keywords. To reduce the risk of false positives, Magnet OTRIDER reports only whole-word keyword hits.

Positive hits in Magnet OTRIDER serve as a significant indicator that further investigation of a specific device is warranted. However, it's crucial to understand that negative hits do not necessarily mean that no evidence is present. Comprehensive analysis and examination may still be required to uncover relevant information on the device.



## View the Scan Report

Once Magnet OTRIDER completes its scanning process, you can access a comprehensive report providing valuable insights into the scan results. Even if you decide to cancel the scan, the report will include the items scanned up to the point of cancellation.

To view your report, you can follow either of these two methods:

- Within the Magnet OTRIDER application, click on "Open report."
- Alternatively, manually browse to the "Magnet OTRIDER\_<X.X.X.XXX>\Reports" directory to access the report.







# MODULE 8

## Practical Exercise

## MODULE 8: PRACTICAL EXERCISE

- Practical Exercise Description
- Practical Exercise Portable Case





## **LEARNING OBJECTIVES AND GOALS:**

This module offers a practical exercise using a new Portable Case, allowing students to reinforce their understanding of the course material. Participants will independently examine digital evidence, applying their newly acquired skills to another case scenario. This hands-on experience enhances their confidence and proficiency in utilizing the Portable Case for digital forensic investigations, ensuring they are well-prepared for future analyses.



## PRACTICAL EXERCISE DESCRIPTION

This practical exercise is centered around the analysis of a new Portable Case. This exercise serves as a crucial opportunity for students to solidify their understanding of the course material by actively applying the concepts and techniques covered throughout course. Through hands-on experience, students will engage in an independent examination of a new piece of digital evidence using the Portable Case.

This practical exercise is thoughtfully designed to reinforce and expand students' knowledge of the materials learned. By navigating through the Portable Case and analyzing the information, students gain valuable insights into the intricacies of digital forensics investigations. The exercise challenges them to identify relevant artifacts, extract valuable information, and draw meaningful conclusions based on the evidence at hand.

The practical nature of this module fosters a deeper comprehension of the Portable Case's functionalities and strengthens the students' abilities to make informed decisions during investigations. By working independently on the exercise, participants gain confidence in their proficiency and technical competence, empowering them to handle complex digital evidence with assurance and accuracy.

By the conclusion of the practical exercise, participants will have honed their digital forensics skills, making them adept at leveraging the Portable Case effectively. Armed with this valuable hands-on experience, students will be equipped to tackle real-world digital forensic challenges with a heightened level of proficiency, ensuring their contributions to the field are both impactful and efficient.

## PRACTICAL EXERCISE PORTABLE CASE

Throughout this course, our focus was on analyzing the Apple iPhone 11 belonging to the suspect, Casey Newton. Now, for the practical exercise, we will shift our attention to examining the phone of the victim, Christopher Austin, who owned a Samsung Galaxy S20. This device was recovered at the scene of the bombing, and a full file system acquisition was successfully performed on it. The acquired data, along with the associated Android Keystore file, were parsed in AXIOM, resulting in the generation of a Portable Case.

Given that Christopher Austin is deceased, there is no expectation of privacy, allowing for an extensive scope of analysis. You are free to examine all artifacts from any dates without limitations. Your task is to thoroughly analyze the Portable Case and identify and tag any artifacts that you consider to be of evidentiary value in the context of the case.

You should explore the data and leverage AXIOM's advanced features to uncover critical insights from the Samsung Galaxy S20. Your analysis may encompass various aspects, including communications, applications, files, and any other data relevant to the investigation. Once your analysis is complete, your next step is to produce an HTML report of all items that you tagged as evidence.

Through this practical exercise, you will have the opportunity to apply the knowledge and skills acquired during the course. By analyzing the digital evidence from Christopher Austin's phone, you will gain hands-on experience, honing your expertise in digital forensics and evidence examination.









# APPENDIX

Student Exercise - Answers

# Appendix - Student Exercise Answers

## MODULE 2: STUDENT EXERCISE

From the Case Dashboard of the Portable Case, answer the following questions:

1. What are the two items of evidence in the Portable Case? **An Apple iPhone 11 full file system and the keychain from the Apple iPhone**
2. Who is the owner of the phone? **Casey Newton**
3. What is the phone number for the phone? **574-302-7985**
4. What is the name of the phone? **Casey Newton iPhone 11**
5. Are location services enabled on the phone? **Yes**
6. What is the Apple ID associated with the phone? **newton20152021@gmail.com**
7. When was the last time that a cloud backup was done on the phone? **10/31/2022 3:11:23**
8. What operating system is on the phone? **14.7.1**
9. Are location services enabled on the phone? **Yes**
10. Has the phone ever been backed up to a computer? **Yes**
11. If so, what is the name of the computer? **DESKTOP-65TBSD3**
12. What is the DSID for the phone? **20253422223**
13. What is the user's Instagram user name? **itscaseynewton**
14. What is the user's password for her Instagram account? **holyguacomole44**
15. What is the user's password for her Facebook account? **LatteLover44**
16. Which artifact category contains the largest number of artifacts? **Location & Travel**
17. Which drive on the forensic examiner's computer contains the original AXIOM Case? Hint: View the log file. **D:\**

## MODULE 3: STUDENT EXERCISE

From the Artifacts Explorer of the Portable Case, answer the following questions:

1. What are the seven views available in Artifacts Explorer? **Classic View, Column View, Conversation View, Histogram View, Row View, Thumbnail View, World Map View**
2. What are the three main panes in Artifacts Explorer? **Navigation Pane, Evidence Pane, and Details Pane**
3. If you want to view mapped GPS data, which view should you use? **World Map View**
4. If you are reviewing pictures and videos, what is the most beneficial view to use? **Thumbnail View**
5. You want to view only Communication evidence in a case. How can you do this? **In the Filters Bar, under Artifacts, apply a filter for Communication**
6. Where can you view all media files that have been categorized by the forensic examiner? **In**



the Filters Bar, under Media Categorization

7. Where can you view all of the artifacts that were tagged by the forensic examiner? **Either in the Filters Bar, under Tags and Comments or in the Tags, Profiles & Media Categories Pane**
8. If you conduct a basic keyword search using two terms, that Boolean logic does AXIOM use to conduct the search? **AND**
9. True or False. You can conduct a Regex search in the Portable Case. **True. Advanced search**
10. If a Portable Case contains more than one item of evidence, how can you view artifacts for only one evidence item at a time? **In the Filter Bar, under Evidence, select the item of evidence that you wish to view**

## MODULE 4: STUDENT EXERCISE

9. At approximately 3:53:49 PM, Ryan Jennings sent Casey Newton a picture. From Artifacts in the Filters Bar, add in the artifact Media. Return to the timeline and view the activity around the time the picture was sent. What was the picture? It is also a Live Photo. Play the associated video. **A picture of a white vehicle in a field**
10. At approximately 3:58:22, another picture was sent. What is that picture? **The drone**
11. At approximately 4:04:36, Ryan Jennings sent a message telling Casey Newton to “Go ahead and make the call.” What phone number did she call? **542-276-1969**
12. The final message sent by Ryan Jennings says that he is coming to Casey’s house. Casey replies that she will see him soon. Approximately where is Casey’s house? **Near Irish Way and Willis Street**

## MODULE 5: STUDENT EXERCISE – REFINED RESULTS

1. What is the user’s Instagram User Name and password? **Name: itscaseynewton. Password: holyguacamole44**
2. What is the user’s Facebook User Name and password? **Name: newton20152021@gmail.com. Password: LatteLover44**
3. The user logged into a WiFi AirPort service. What is the password of that wireless network? **Opus420Penguin#**
4. The user has a WhatsApp account. What is her User ID? **15743027985@s.whatsapp.net**
5. Is there any evidence that the user was searching for information about tracking someone? **Yes. Multiple searches related to tracking an Android and an AirTag**
6. On Amazon, the user viewed a book related to building explosives and weapons. What is the title of that book? **The Anarchist Cookbook**



7. The user viewed Facebook event 1052515771967336. What was that event and what date was it being held? **June MSB Market. Michiana Small Businesses. June 26, 2022**
8. While on Facebook, the user viewed the profile and several photos related to a BBQ business. What is the name of that business? **Evelyn Mae's BBQ**
9. In Identifiers, what is the DSID for the Owner Information of the iPhone? **20253422223**

## MODULE 5: STUDENT EXERCISE – WEB RELATED

1. In the previous exercise, we saw that the user viewed a specific book on Amazon related to building explosives and weapons. Is there any information in iOS Safari Recent Search Terms indicating how the user found the book on Amazon? **Yes. A search for 'the anarchist cookbook' on 9/8/2022 7:29:01**
2. What type of club was the user search for in Chicago? **Blues Clubs**
3. In general, is there any evidence in iOS Safari Recent Search Terms related to this investigation? **Yes. Multiple searches related to killing, bombs and tracing drones/bombs**
4. On 9/27/2022 at 5:45:21 PM, the user conducted a search for 'good restaurants in Chicago.' What is the title of the first web page that the user viewed after that search? **The 38 Essential Restaurants in Chicago**
5. Based on the restaurant search, what specific restaurant did the user view on tripadvisor.com? **The Capital Grille**
6. The user searched 'mountain cabins nearby with waterfalls.' This led to viewing a specific rental site on VRBO. What is that rental site? **Roaring Fork Waterfalls vacation rentals**
7. Is there any evidence that the user booked a cabin through VRBO? **No**

## MODULE 5: STUDENT EXERCISE – COMMUNICATION

1. What is the contact name associated with the phone number 572-276-1969? **Boom**
2. There is a contact name of 'Off The Grid.' What two lakes is 'Off The Grid' between? **Elk Lake and Lake Skegemog**
3. What date/time did Casey newton add Ryan Jennings as a contact? **6/1/2021 10:28:16**
4. What is the phone number for Dolan Shaver? **574-220-9526**
5. How many phone calls did the user place to 572-276-1969? **Two. Both on 10/31/2022**
6. Has Casey Newton ever talked on the phone with Ryan Jennings? **No**
7. On 9/15/2022 at 10:36:11, Ryan Jennings sent Casey Newton a message with a video attached.





- What is depicted in this video? **A drone flying and carrying a package**
8. Using the answer in Question 5, is there any evidence in the text messages between Casey Newton and Ryan Jennings related to Casey Newton making a phone call? **Yes. On 10/31/2022 at 4:04:36, Ryan tells her to 'go ahead and make the call'**
  9. When Casey Newton and Chris Austin first met in-person, where did they agree to meet? **Brothers Bar by Notre Dame**

## MODULE 5: STUDENT EXERCISE – SOCIAL NETWORKING

1. Using the information in Instagram Direct Messages, what date did Ran Jennings and Casey Newton get a drink? **9/6/2022**
2. What date did Casey Newton match with Ryan Jennings on Tinder? **8/25/2022**
3. What is the User Name of the only other user that Casey matched with on Tinder? **Richard**
4. What is the User ID of Case Newton's Tinder account? **6307ada3ba03c001005d0b1b**
5. How did Casey Newton learn Ryan Jennings's phone number? **He provided it to her in the Tinder messages**
6. What is the Twitter User ID for Miley Cyrus? **268414482**

## MODULE 5: STUDENT EXERCISE – MEDIA

1. On 10/31/2022, at approximately 4:20:16, an iOS Snapshot was captured. What is the significance of this Snapshot? **It is a Snapshot of the end of the text message conversation between Ryan and Casey, indicating that Chris has been blown up**
2. From iOS Snapshots, who was Casey Newton having dinner with on 9/13/2022? **Irelyn and Ellen**
3. View the live information associated with the picture IMG\_0057.HEIC. What is being discussed while this picture was taken? **Chiropractor**
4. What address was the user near when this picture was taken? **6300 Royal Aberdeen Ct, Charlotte, NC**
5. Conduct a search for '5005.jpg.' In the results, view the Source of the results. What is this information indicating? **5005.jpg are all thumbnails of full-size pictures**
6. From the 5005.jpg pictures, it is possible to determine the name of the full-size picture? **Yes, it is contained in the Source path**
7. For the picture IMG\_0053.HEIC, what is the Make, Model, and Software for the camera that was used to take the picture? **Apple iPhone 11, iOS 16.0**



8. When was the video IMG\_0138. MOV taken? **9/15/2022**
9. What Make and Model of camera was used to take IMG\_0138.mov? **Apple iPhone XR**

## MODULE 5: STUDENT EXERCISE – EMAIL & CALENDAR

1. On 9/9/2022, Ryan Jennings sent Casey Newton an email with the subject line “So Many Options.” What attachment was included with this email? **Anarchist Cookbook – William Powell.pdf**
2. What attachment was included in the email with the subject line “Check this out”? **Drone Receipt.pdf**
3. On 9/19/2022, Ryan Jennings sent an email to himself and to Casey Newton. This email had the subject line of “Cool video” and contained an attachment of IMG\_0051.MOV. Due to the size of the attachment, it could not be included as an attachment and instead a download link was generated by Apple. What location did this download link point to? **cvws.icloud-content.com. This can be seen by expanding the headers of the email.**
4. Casey Newton received a notification email from Facebook that someone wanted to be friends with her. Who wanted to be friends with her? **Philip Das**
5. How many user-created Calendar Events are there? **None**

## MODULE 5: STUDENT EXERCISE – DOCUMENTS

1. Review the Apple Note with the title To do 9/13/22. Does this note look familiar? **Yes. There was an iOS Snapshot of this note**
2. Are any of the Apple Notes encrypted? If so, can you still read the content? **Yes, the note with the Title ‘Important details for the operation’ is an encrypted note. It is still readable. It is readable because a full file system acquisition was acquired. This included the encryption key for Apple Notes**
3. Review the encrypted note. What is the significance of the phone number in the note? **That is the phone number to activate the bomb. This number was called by Casey Newton**
4. Review the document data.csv. The document is referring to a specific location. What city is that location near? **Munich, Germany. 48.186405, 11.608580**
5. Review the document attachment.pptx. Who is the original author of the document and where did she work? **Erin. Aldridge Electric**
6. Who is the last author of attachment.pptx and when was it last modified? **Ryan Jennings 9/12/2022 5:03:40 PM**
7. What date was the file Anarchist Cookbook – William Powell.pdf saved on the phone? **9/9/2022**



## MODULE 5: STUDENT EXERCISE – APPLICATION USAGE

1. Is the program Snapchat installed on the device? If so, when was it installed? **Yes. Installed 10/13/2022**
2. Snap Chat and TikTok both have Package Names that are different from their Display Names. What are the package names of each? **Snapchat = Picaboo. TikTok = musically**
3. What is the Display Version of Tinder that is installed on the device? **13.17.0**
4. Are location services enabled on the phone? **Yes**
5. What is the Serial Number for the phone? **DX4F4EGVN72J**
6. What is the name of the phone? **Casey Newton iPhone 11**
7. On 10-/31/2022, at 4:30 PM, was the phone locked or unlocked? **Locked**
8. On 10/31/2022, between 4:05:06 and 4:05:20, what application was in use? **Mobile Phone. This matches with the phone call that was placed to 572-276-1969 at 4:05:20**
9. On 10/31/2022 at 4:19:42 PM, the user received a notification on the phone. What was the notification for? **Receiving a text message**

## MODULE 5: STUDENT EXERCISE – OPERATING SYSTEM

1. What is the DSID for the user? **20253422223**
2. Review all of the Cell Tower Locations that were recorded in the database on 10/26/2022 at 1:47:09 PM. What is the general location of the user? **South Bend, IN**
3. Review all of the Cell Tower Locations that were recorded in the database 10/30/2022 at 9:50:23 PM. What is the general location of the user? **Chicago, IL**
4. On 10/30/2022, at 9:14:28 PM, one Cell Tower Location was recorded in the database. What Mobile Network was the phone connected to? Include the Mobile Network Code and the Cellular provider? **Mobile Network Code is 410. Searching at [mcc-mnc-list.com/list](http://mcc-mnc-list.com/list) indicates that MCC 310/MNC 410 is AT&T Mobility.**
5. What is the lowest battery percentage ever on the phone and what is the Display Date/Time of when this happened? **5.0%. 10/25/2022 1:37:30 PM**
6. What is the last Display Date/Time that the lightning cable was connected to the phone? **10/31/2022 4:52:18**
7. What two Timezone has this phone been in during the month of October 2022? **Central (Chicago) and Eastern (Indianapolis/New York)**
8. What application has sent the most data via the cellular network? **com.apple.mobileslideshow. The Photos app**



## MODULE 5: STUDENT EXERCISE – ENCRYPTION & CREDENTIALS

Service	Account	Password
Instagram	Itscaseynewton	holylguacamole44
Facebook	Newton20152021@gmail.com	LatteLover44
TikTok	Itscaseynewton	3CheesePizza!
Twitter	Newton20152021@gmail.com	ZucchiniZoodle22
LolaGranola Wireless		Opus420Penguin#
ATT-WIFI-6WVL Wireless		362WxLXV

## MODULE 5: STUDENT EXERCISE – CONNECTED DEVICES

- From earlier data, we know that on 10/31/2022, at 4:05:20: PM, Casey Newton made a phone call to detonate the drone bomb. Around that time, from Apple Health data, does it appear that she was physically active? **No. There are no Steps or Distance during that time period.**
- What is the largest number of Steps Taken by Casey Newton on 10/31/2022? **1149**
- Does it appear that Casey Newton wears an Apple Watch? **No. There is no heart rate data recorded.**
- What is the furthest distance that Casey Newton has walked and what date did this occur? **968.92 meters on 2/15/2022**
- What is the last location recorded by Find My Devices for Casey Newton iPhone 11 and when was this recorded? **1744 Irish Way, South Bend, IN 10/31/2022 4:00:02PM**
- In iOS Messages, Chris Austin accused Casey Newton of planting an AirTag on him. Is there any evidence of this in Connected Devices? **Yes. There is an AirTag named Chris listed under Find My Items.**
- What was the last location recorded by this AirTag and when was it recorded? **University Park Mall, W. University Dr, Mishawaka, IN 46545 on 10/31/2022 at 3:40:51 PM**
- Apply a Relative Time Filter and view activity for five minutes prior to and after the time that the location of the AirTag was recorded. View iOS Messages. Do you see any evidence indicating that Casey is tracking Chris? **Yes, she sent a text message to Ryan Jennings at 3:41:52 stating "Ok looks like he's at the mall!"**
- Remove the Relative Time filter and return to Connected Devices.
- Is there any evidence in Find My Locations confirming that the last recorded location for the AirTag planted on Chris was at University Park Mall? **Yes. The device named Chris is mapped to**



University Park Mall on 10/31/2022 at 3:40:51.

## MODULE 5: STUDENT EXERCISE – LOCATION AND TRAVEL

1. Casey Newton was interviewed regarding the killing of Chris Austin. During her interview, she stated that she was not involved and was in Chicago the entire day on 10/31/2022. Using Cached Locations, can her alibi be verified? **No, it cannot. Apply a date filter for 10/31/2023. She was in Chicago earlier in the day but traveled back to South Bend. At the time of the killing, she was in South Bend.**
2. When Casey was in Chicago on 10/31/2022, what is the name of the building that she was staying at? **Elm Tower. This can be viewed in Cached Locations**
3. Prior to the killing, Casey Newton walked from one building to another on the campus of Notre Dame. What building did she start out at and where did she walk to? **Started at Hammes Mowbray Hall. Walked to Duncan Student Center. This can also be viewed in Cached Locations**
4. View all of the Significant Locations in the State of North Carolina. What city are they associated with? **Charlotte**
5. Casey still denies that she was in South Bend during the time of the killing and she states that she has never been to Duncan Student Center. Using Significant Locations Visits, can her alibi be verified? **No, it cannot. There are four Significant Locations Visits recorded for 10/31/2022. The first three show that she was in Chicago. The fourth shows that she was at Duncan Student Center. She arrived at 1:18:24 PM and left at 2:43:24 PM**
6. Apply a date filter of 10/31/2022. View Cached Locations. In general, notice where Casey began in Chicago, the route she took to South Bend, and where she ended near Notre Dame. Now switch to WiFi Locations and view the mapping. Does this information correspond with the Cached Locations? **Yes, she started in Chicago, drove to South Bend via the Indiana Toll Road, and then went to Notre Dame.**
7. While still in WiFi Locations, zoom into the area of Notre Dame and South Bend. The data should begin to form two groups. One group is at Notre Dame. What is the significance of the other group? **The other group is near Irish Way. That is where Casey's residence is and where she was when the killing took place**





[magnetforensics.com/training](https://magnetforensics.com/training)