4/18/2021

Adamentah Medical Center Information Technology Digital Forensics Report

Case 001

Jonathan Campbell, Digital Forensics Investigator
School of Computer and Information Science, University of the Cumberlands
MSDF 534: Wireless Security and Forensics
Dr. Rick Livingood

Contents

Executive Summary

On March 22, 2021, the Adamentah Medical Center Human Resources department requested an analysis of an Apple iPhone 4s (A1387). The acquisition goal was to extract and analyze all images, SMS, MMS, and application data to discover evidence related to a sexual harassment complaint by an Adamentah employee. After acquiring and analyzing data from the mobile device, the digital forensics investigator found no evidence supporting a sexual harassment claim. The investigator provided all files, data, and evidence to the Human Resources representative, Jack Opibus.

Background

The employee filing the sexual harassment complaint (Accuser) stated that an Adamentah employee in a leadership position (Accused) was sexting her, sending her sexually explicit pictures, and offering to help with promotion if she performed particular sexual activity. The accuser stated that she received the sexting MMS messages from a corporate cell phone number assigned to the accused.

Human Resources decided to retrieve the corporate cell phone for investigation. The accuser stated that her personal cell phone was the one that received the explicit material. She refused to allow Human Resources to investigate her cell phone. A Human Resources (HR) representative approached the accused and confiscated the corporate cell phone. The HR representative immediately turned off the cell phone. The HR representative stated that the accused was surprised by the confiscation, but once they heard the accusation had no problem turning over the device.

Mobile Device Forensics Process

This report will describe the mobile device forensics process in detail. The method includes all elements of the mobile device forensics process. The digital forensics investigator, Jonathan Campbell, provides step-by-step information related to the forensics method utilized. Mr. Campbell can answer any questions related to the digital forensics methodology.

Initial Contact and Intake

On March 22, 2021, the Adamentah Medical Center Information Technology department received an Apple iPhone 4s (A1387) from Human Resources. The mobile device was contained in a Faraday bag, signed by Jonathan Campbell and received from Jack Opibus, the Human Resources employee advocate.

Identification

Upon intake processing, the digital forensics investigator inspected the mobile device for specifications. The following are specifications retrieved from the mobile device.

Table 1: Mobile device specifications

Manufacturer	Apple
Model	iPhone 4s (A1387): MD236LL/A
Device Name	iPhone
Revision	9.1 (13B143)
IMEI	99 000193 389658 1
Serial Number	C8PJQKYMDTC1
ICCID	893144088513919209
IMSI	204043608658225
MEID	99000193389658
Bluetooth Address	64:a3:cb:cb:77:76
Wi-Fi Address	64:a3:cb:cb:77:75

Preparation

The digital forensics investigator prepared the following digital forensics tools and versions and the digital forensics workstation specifications for the mobile device forensics acquisition and analysis.

Table 2: Mobile forensics tools and versions

Mobile Device Forensics Acquisition Tool 1	Cellebrite UFED Touch2 Product Version: 7.42.0.82 , Internal Build: 7.42.0.82
Mobile Device Forensics Acquisition Tool 2	Magnet Axiom Process Product Version: 4.11.0.24063
Mobile Device Forensics Analysis Tool 1	Cellebrite Physical Analyzer Product Version: 7.41.0.8
Mobile Device Forensics Analysis Tool 2	Magnet Axiom Examine Product Version: 4.11.0.24063
Mobile Device Processing Workstation	Dell Inspiron-5548, i7 1TB SSD, 16GB
Operating System for Mobile Device Processing	Windows 10 Pro x64. Build 19041

Isolation Methods

Isolation methods used during the processing of the mobile device evidence. These included:

- Dark Mission Faraday bag – Used to transfer mobile devices between locations (Figure 1).
- Faraday Room – Used to perform all acquisitions and analysis.
- Device Settings – Configured on the mobile device to provide further isolation (Figure 2).

- Airplane Mode on
- Bluetooth off
- Wi-Fi off
- Cellular off
- Location Services off

Processing Methods

This section describes the step-by-step acquisition, analysis, and validation methods used to provide the Adamentah Medical Center Human Resources department with artifacts, data, and evidence related to the sexual harassment claim.

Processing Goals

The following goals set by the Adamentah Human Resources department regarding the acquisition and analysis of digital evidence retrieved from the accused's iPhone 4s include:

- Perform a file system and memory acquisition from the iPhone 4s.
- Use multiple tools to ensure the completeness of the acquisition.
- Analyze the file system for any photos, videos, SMS/MMS texts, chats, or emails associated with the accuser and accused.
- Analyze any deleted data found.
- Verify the analysis with another forensics tool to ensure completeness and accuracy.

Caveats to Acquisition and Analysis

Jonathan Campbell informed the Human Resources representative that the mobile device would need a 'Jail-Break' to retrieve a physical acquisition. Human Resources decided that they did not want the device tampered with if used in future investigations or litigation. The forensics investigator performed a logical extraction on the mobile device.

Acquisition Methods

The investigator used two forensics tools for data acquisition: Magnet Axiom Process and Cellebrite Touch2 UFED. The primary tool for data extraction was Cellebrite Touch2 UFED. The investigator used the Magnet Axiom tool as a secondary acquisition tool for data validation. The following is a step-by-step explanation of the acquisition process.

Cellebrite Touch2 UFED Acquisition Steps

1. The forensics investigator connected the iPhone 4s mobile device to the Cellebrite Touch2 UFED tool via Cellebrite cable number T-110.
2. The forensics investigator set the Cellebrite UFED tool to discover the mobile device model (Figure 3).
3. The investigator selected the Apple iPhone 4s (A1387) model as the device (Figure 4).
4. The first acquisition type, 'Advanced Logical,' was then selected (Figure 5).
5. The investigator could only acquire file system data; therefore, it was selected (Figure 6).
6. We used an external drive as the target device for extraction; therefore, 'Removable Drive' was selected as the target device (Figure 7).

7. Because the process included extracting user credentials, the investigator set a password for the encrypted backup of the user credentials
8. The Cellebrite UFED tool then extracted the file system to the target device under the 'AdvancedLogicalFile System 01' directory on the external drive.
9. Once the advanced logical acquisition was complete, the investigator returned to the iPhone acquisition screen and performed a 'Logical Acquisition.' The investigator selected all data types and media for extraction.
10. Once the logical extraction was complete, the following data type counts were produced (Figure 8).

Table 3: Cellebrite UFED data extraction counts

Contacts	390
Pictures	3825
Videos	2
Call Logs	316
Calendar	42
Ringtones	1
Instant Messages (IM)	33
Files	502

Magnet Axiom Process Acquisition Steps

At this point, the mobile device was disconnected from the Cellebrite Touch2 UFED tool and connected to the digital forensics Windows 10 workstation for validation acquisition. The following steps then took place with the Magnet Axiom Process application.

1. The digital forensics investigator added case details for the iPhone 4s extraction (Figure 9).
2. Set evidence source to 'iOS' (Figure 10).
3. Under 'Evidence Sources,' 'Acquire Evidence' was selected (Figure 11).
4. The iPhone 4s mobile device was then selected (Figure 12).
5. The investigator selected all data types and custom artifacts for acquisition. Since Axiom has a more robust capability of searching social media applications, this will produce a greater data count than Cellebrite (Figure 13).
6. Calculate hash values for all files was selected.
7. Upon completion of the extraction, the following data types and counts were produced (Figure 14).

Table 4: Magnet Axiom data extraction counts

Web Related	95
Chat	36
Media	9136
Mobile Application Data	1313
Operating System Files	116

Cloud Passwords and tokens	2
Custom	1

Analysis

As stated under the processing goals, the digital forensics investigator performed digital forensics analysis to locate any accuser and accused evidence. The evidence includes photos, pictures, videos, SMS/MMS messages, chats, emails, deleted files, and any other evidence that links the accused to activity associated with the accuser.

Cellebrite Physical Analyzer Analysis Steps

The following are the steps followed for analyzing evidence acquired from the Cellebrite UFED acquisition tool.

1. From the Cellebrite Physical Analyzer, open the .udx file system logical acquisition that was collected (Figure 15)
2. The investigator selected Hash sets, carve locations, and media classification for analysis (Figure 16).
3. Selecting the file system, we can view all media collected from the iPhone; the investigator exported this to a CSV file for Excel viewing. The investigator found deleted data in the initial analysis (Figure 17).
4. We are also presented with a summary of the original acquisition to include data categories found within the extracted file system (Figure 18).
5. Analyzing the photostream, we found 54 images. None of the pictures contain the accuser, nor do they have any pictures that could be of a sexual nature (Figure 19).
6. Next, the investigator analyzed the DCIM folder and found no images of the accuser nor any images of a sexual nature (Figure 20).
7. The investigator searched MMS messages for sexting messages. None were found (Figure 21).
8. From 'Analyzed Data,' the investigator searched FaceTime call logs for any calls between the accuser and the accused. No calls were found (Figure 22).
9. Under Calls, we drilled down to answered calls. The investigator found no deleted calls associated with the accuser (Figure 23).
10. The investigator then searched for the accuser's contact information in Contacts and found no data associated with the accuser (Figure 24).
11. Chats were then searched for any communications between the accuser and accused. None were found (Figure 25).
12. The investigator searched all SMS messages for communication related to sexting content or communications. None were found (Figure 26).
13. Next, the investigator analyzed the Email correspondence between the accused and accuser. None correspondence was found (Figure 27).
14. Finally, the investigator searched all volatile memory from the iPhone for keywords associated with the accuser's cellular phone number and name. None were found (Figure 28).

Validation Methods

Validation occurred by using an alternate digital forensics analysis tool. The tool used in this case was Magnet Axiom Examine. The purpose of verification was to ensure the completeness and accuracy of the data and evidence acquired and examined through the Cellebrite mobile forensics tools. One difference we notice between Cellebrite and Axiom is related to images. For example, we find multiple images associated with music albums in Axiom. The digital forensics investigator did see numerous photos in a contact list for a single contact related to LinkedIn. Therefore, the image count is much higher than Cellebrite. The following are the steps associated with validating data with the Magnet Axiom Examine tool.

1. After opening the Magnet Axiom Examine application and selecting the Axiom Process iPhone acquisition, a summary of the device, artifacts, and matching results are presented (Figure 29).
2. We then analyzed the chat data consisting of SMS, MMS, and iMessages. The investigator found no evidence relating to the accuser, nor was evidence found relating to sexting or anything of a sexual nature (Figure 30).
3. Next, we investigated the browser history. There was no evidence of anything inappropriate or associated with the accuser.
4. Call logs were then analyzed for calls between the accuser and accused. None were found (Figure 32).
5. Next, the investigator analyzed all images for photos of the accuser or sexually explicit pictures. No evidence was found (Figure 33).
6. The investigator then searched Contact lists for images or contact information related to the accused. In both cases, none were found (Figure 34).
7. Finally, the investigator found six videos in the acquired data. None of these contained any association to the accuser (Figure 35).

Documentation

The 128GB Flash drive labeled 'Case 001' contains all documentation related to the mobile device's acquisition and analysis. The documents include.

- Acquisition Files from Cellebrite UFED and Magnet Axiom Process tools
- All data files associated with Cellebrite Physical Analyzer and Magnet Axiom Examine tools
- Cellebrite Physical Analyzer generated report. See Figure 36 for an example.
- Magnet Axiom Examine generated report. See Figure 37 for an example.

Figures

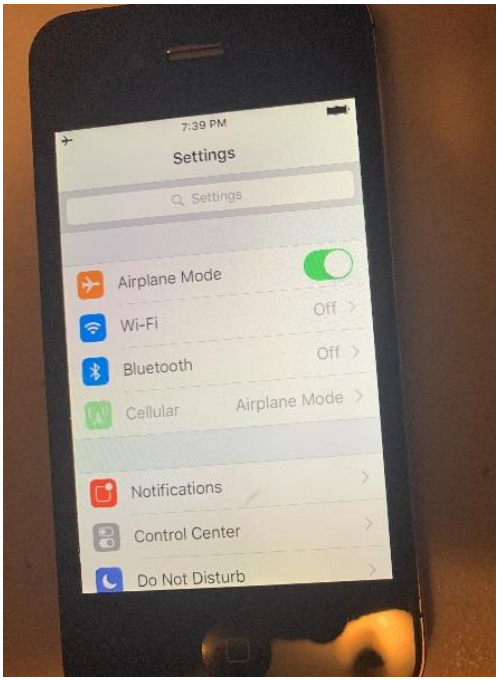


Figure 1: iPhone wireless status

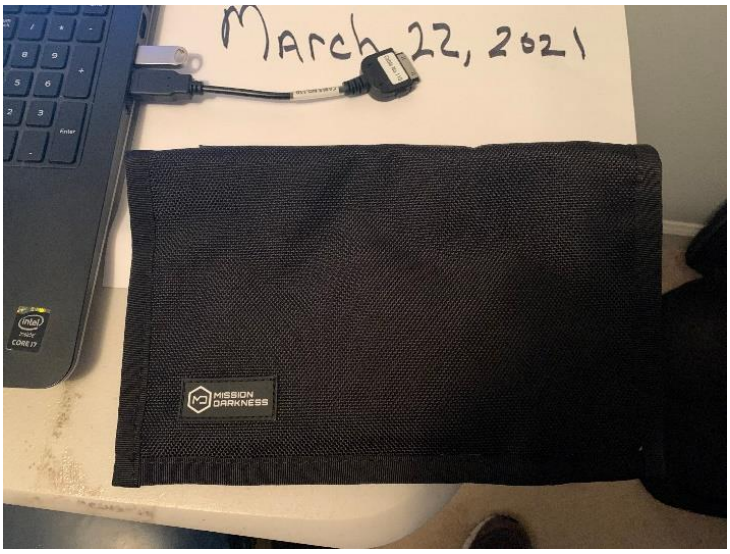


Figure 2: Faraday bag

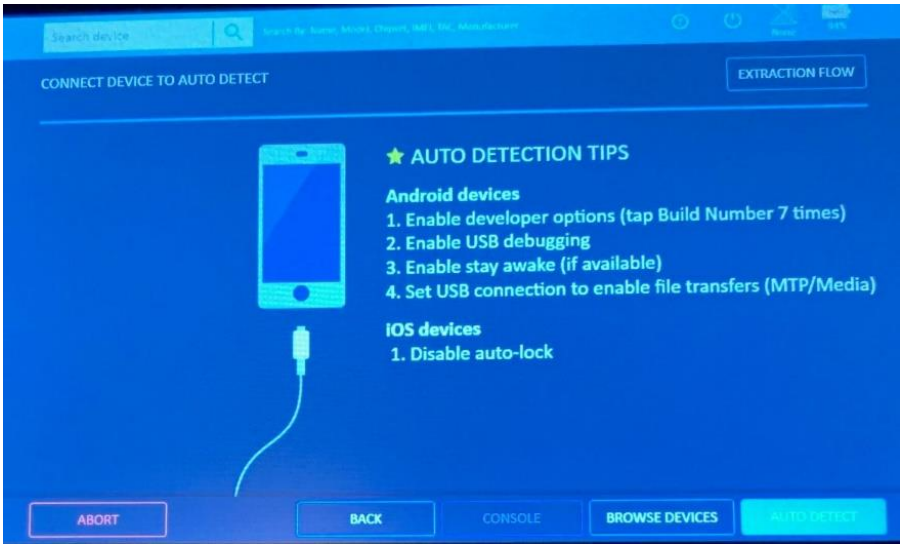


Figure 3: Cellebrite auto-detect screen

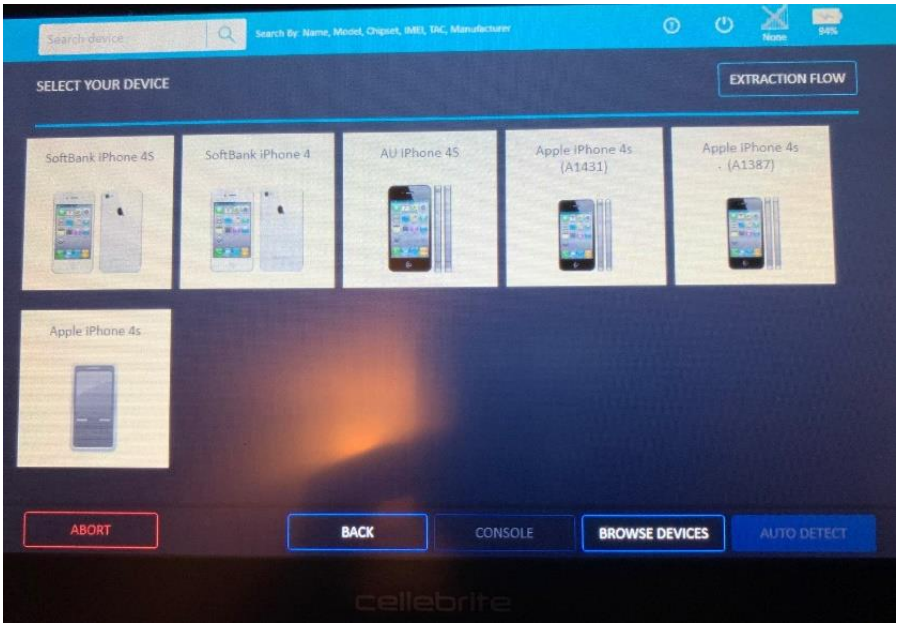


Figure 4: Cellebrite auto-detection output

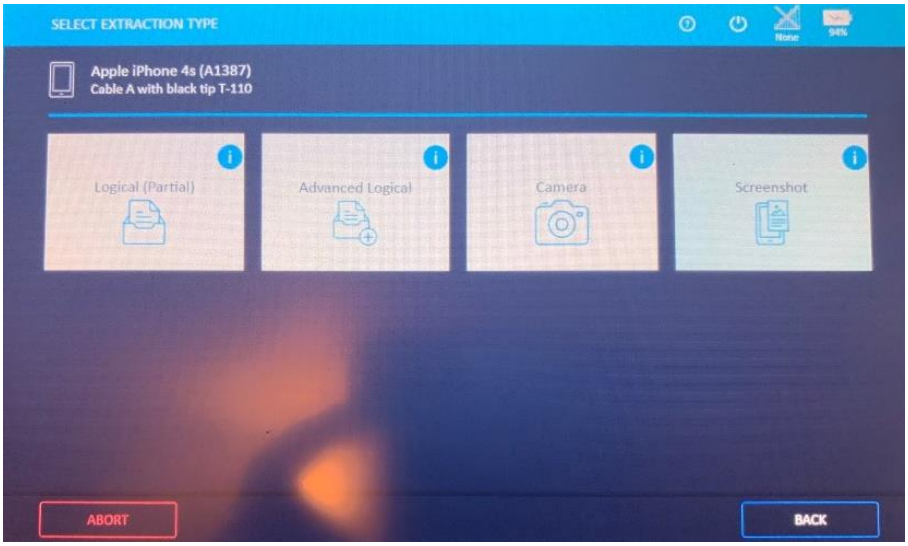


Figure 5: Cellebrite UFED acquisition options

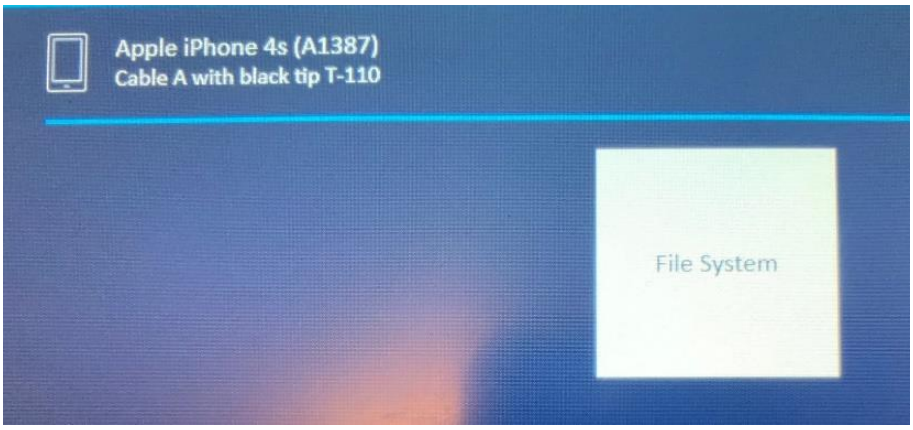


Figure 6: Cellebrite UFED advanced logical acquisition option

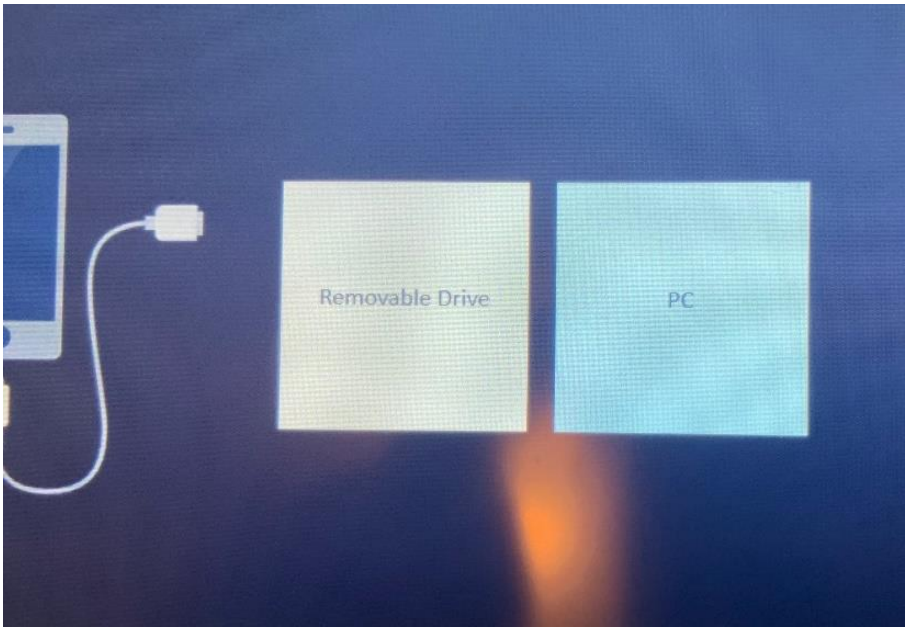


Figure 7: Cellebrite target device option

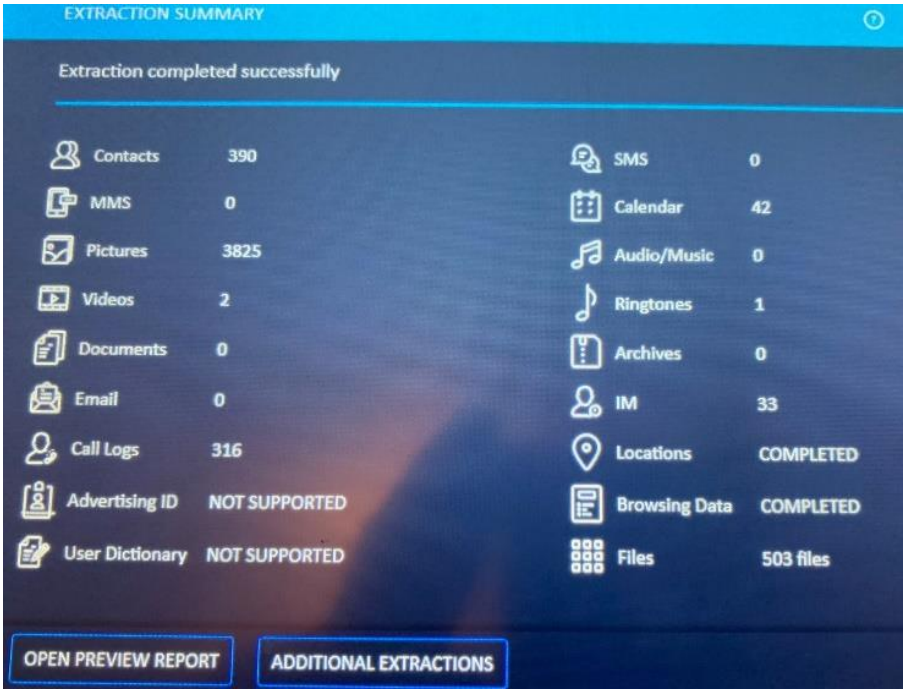


Figure 8: Cellebrite UFED logical extraction completion summary

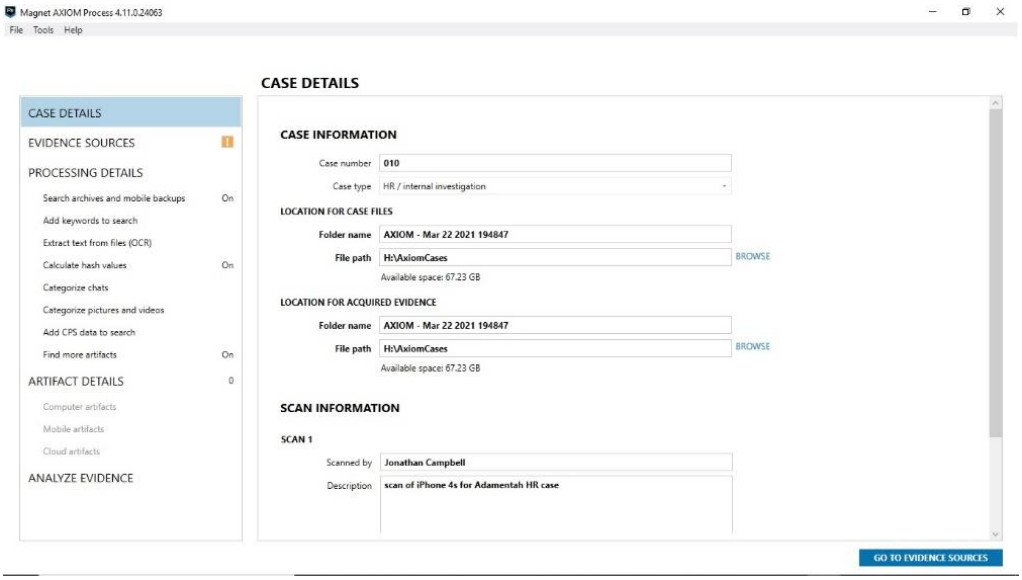


Figure 9: Axiom case details

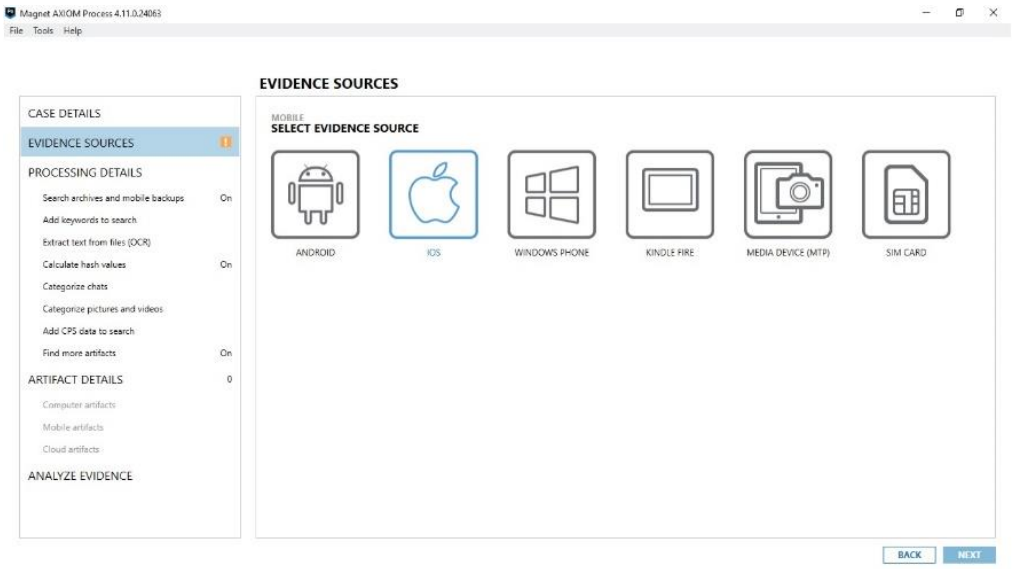


Figure 10: AXIOM iOS selection

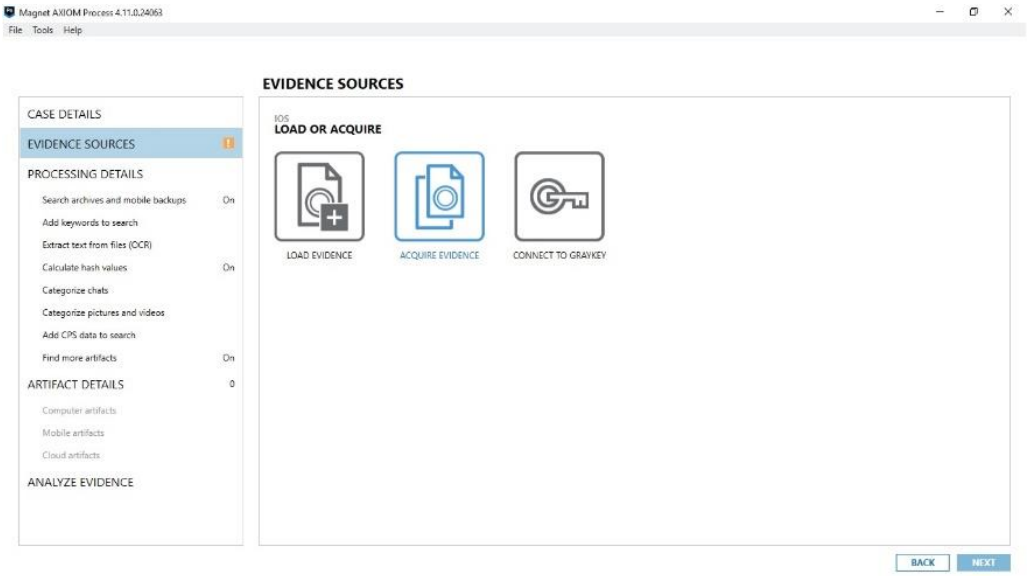


Figure 11: Axiom acquire evidence

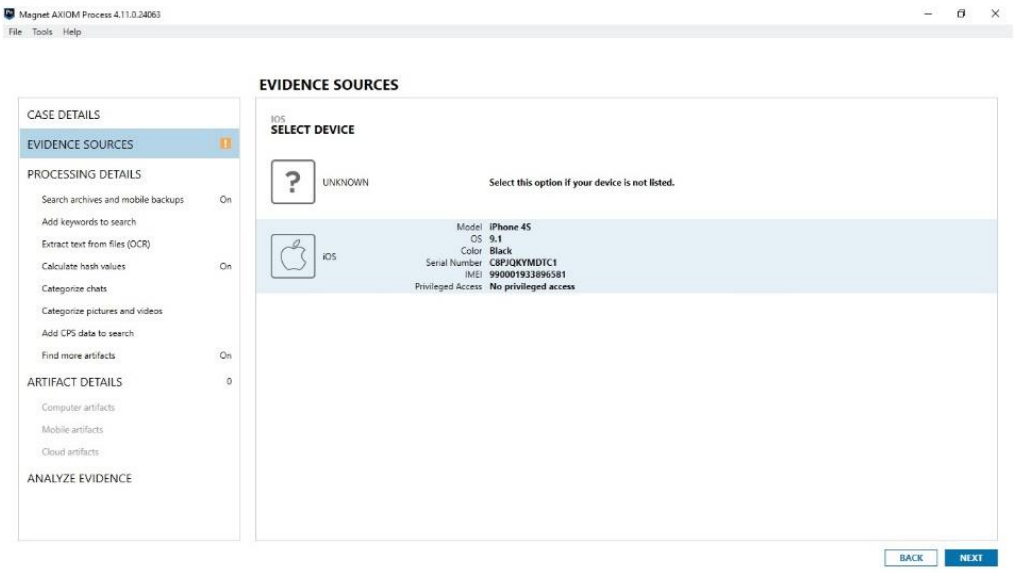


Figure 12: AXIOM iPhone device selection

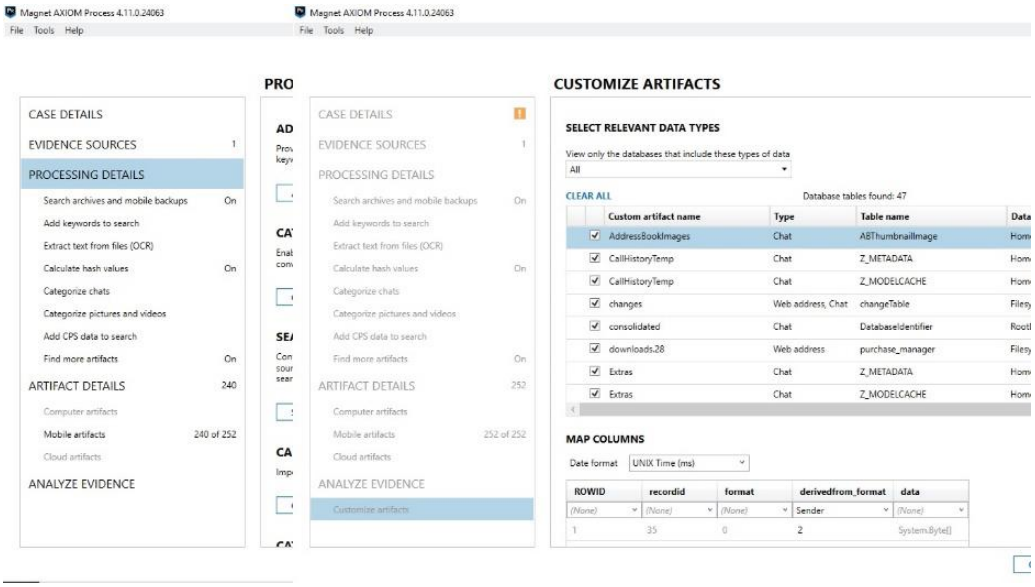


Figure 13: Selection of Axiom data acquisition custom artifacts

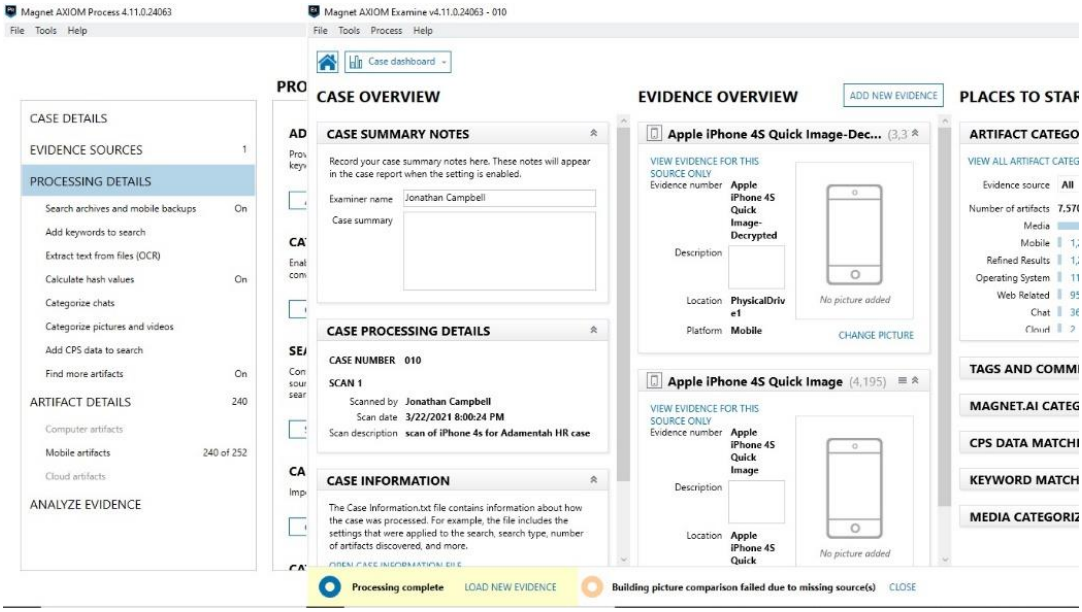


Figure 14: Axiom acquisition details

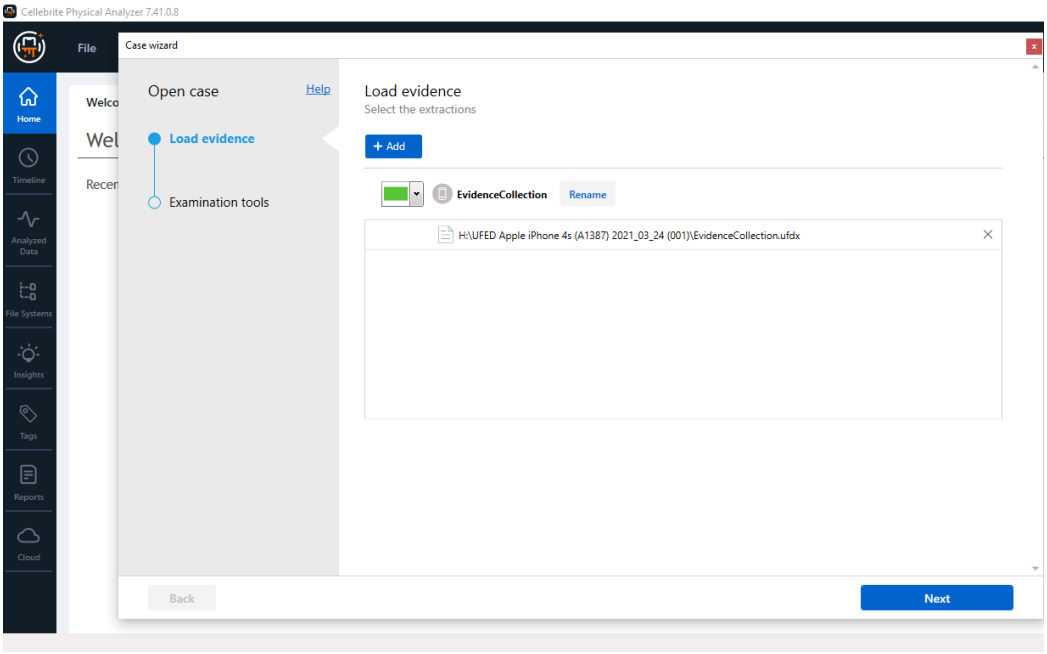


Figure 15: Cellebrite physical analyzer .udx selection

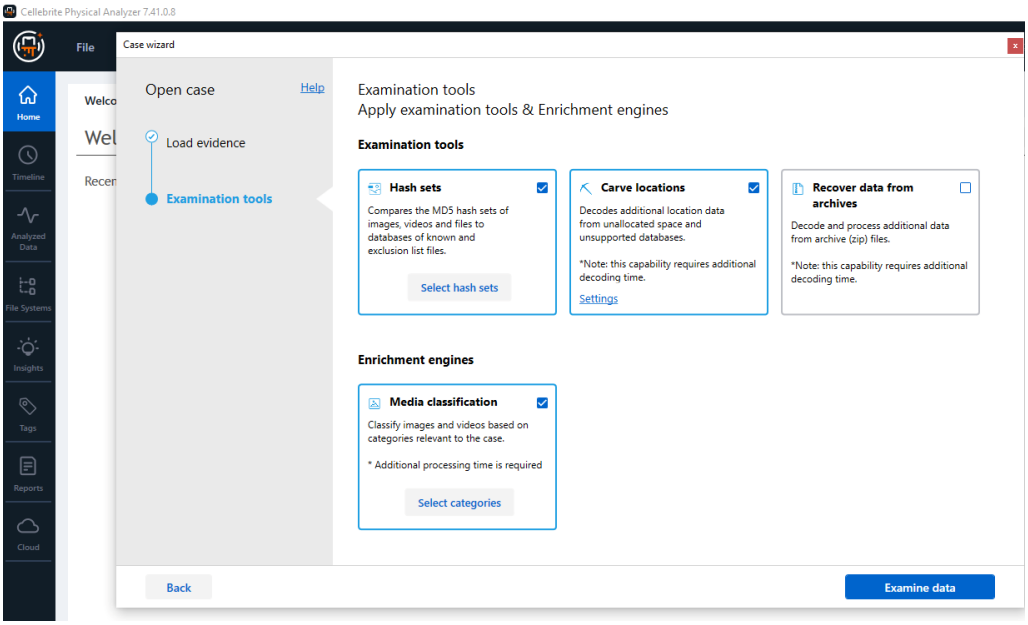


Figure 16: Cellebrite analysis toolset selection

	A	B
1	Data	
2	Calendar	192 (29)
3	Call Log	639 (7)
4	Carved Strings	1 (1)
5	Chats	241 (0)
6	Contacts	1162 (0)
7	Device Locations	458 (100)
8	Device Notifications	1 (0)
9	Emails	522 (0)
10	Installed Applications	63 (0)
11	Instant Messages	71 (0)
12	Log Entries	2 (0)
13	Searched Items	4 (0)
14	User Accounts	13 (0)
15	Web Bookmarks	112 (0)
16	Data Files	
17	Audio	1 (0)
18	Configurations	201 (0)
19	Databases	41 (0)
20	Images	5022 (0)
21	Text	2 (0)
22	Uncategorized	138 (0)
23	Videos	4 (0)
24		

Figure 17: Cellebrite iOS data export to CSV

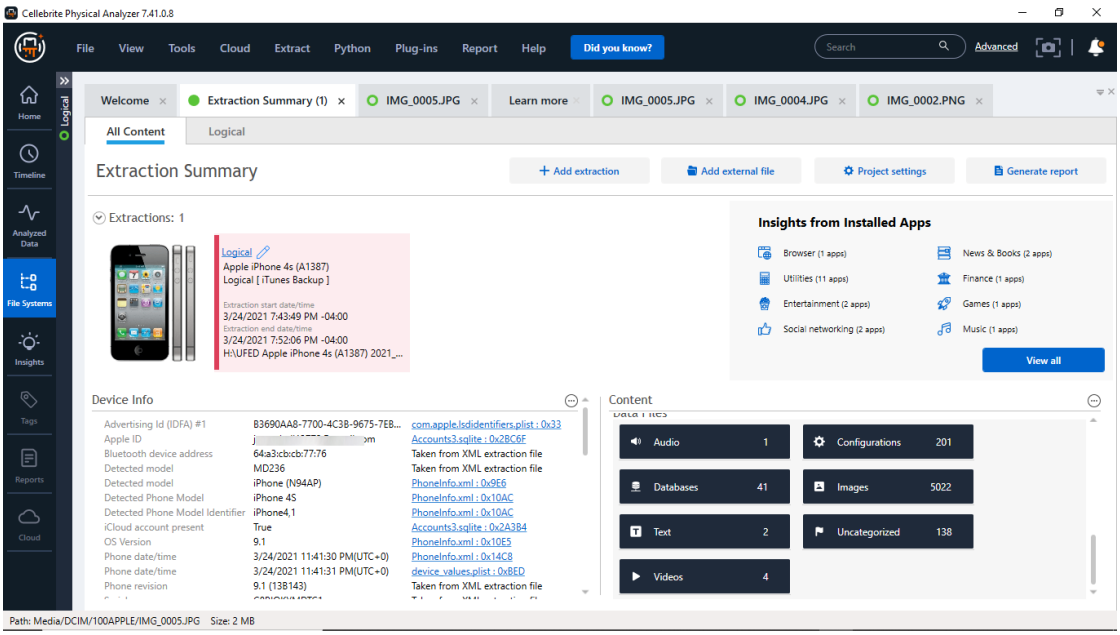


Figure 18: Summary of Cellebrite iOS data extraction for analysis

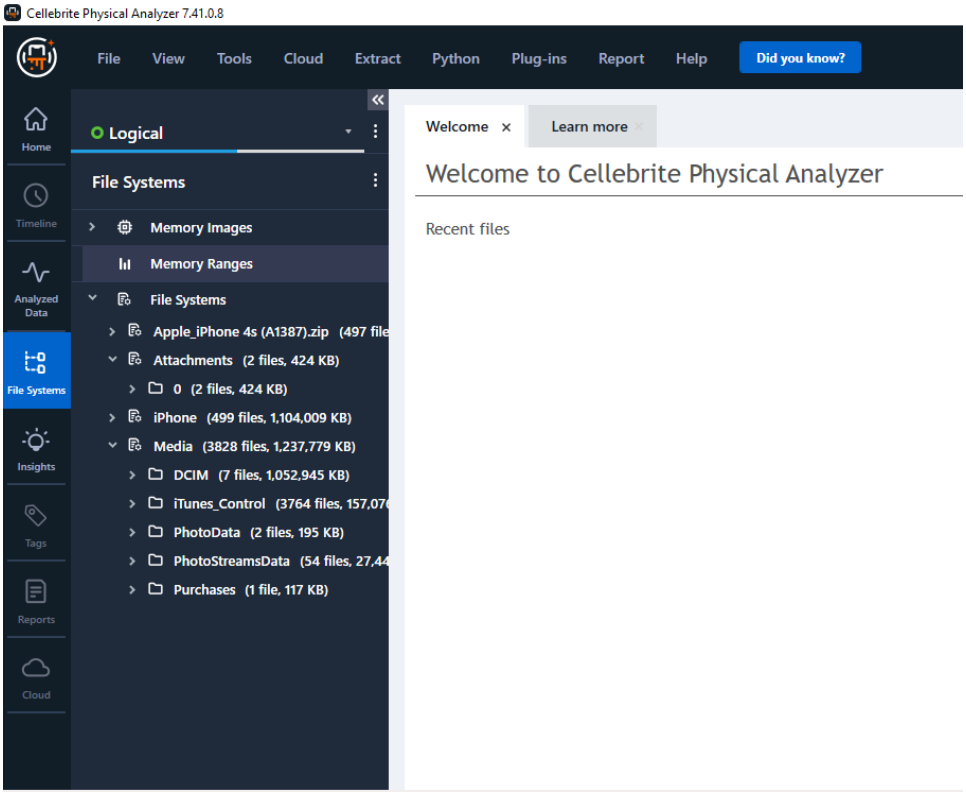


Figure 19: Cellebrite iOS photo stream count

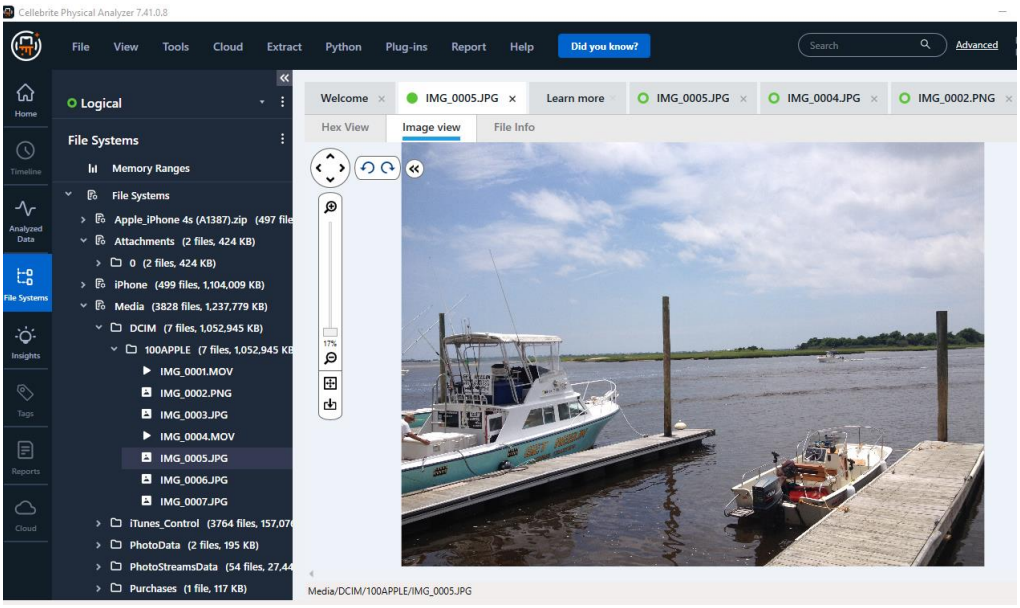


Figure 20: Cellebrite iOS DCIM images

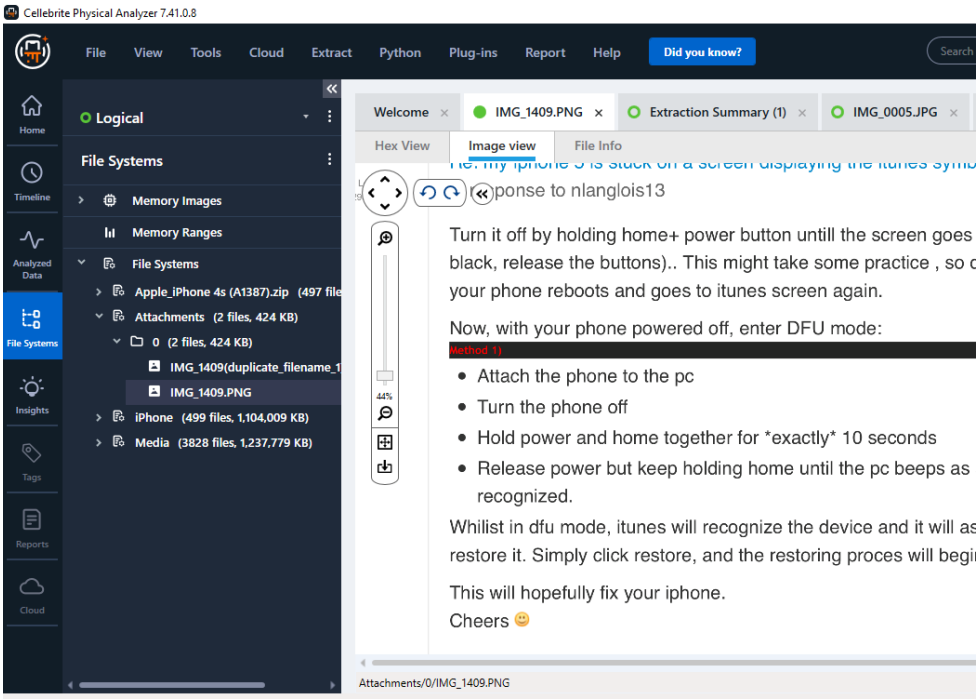


Figure 21: Cellebrite iOS MMS attachments

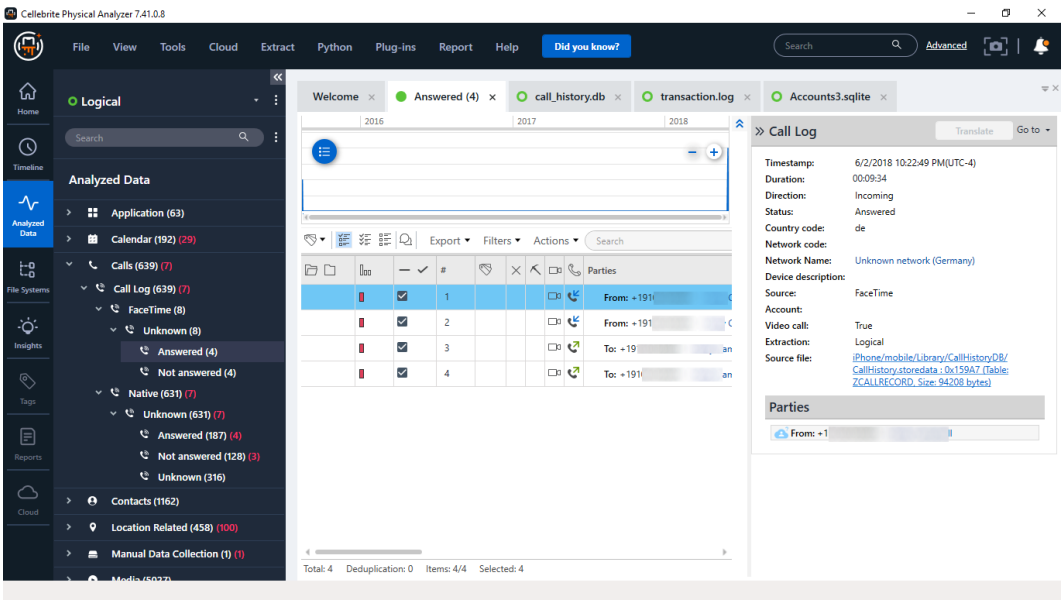


Figure 22: Cellebrite iOS FaceTime calls

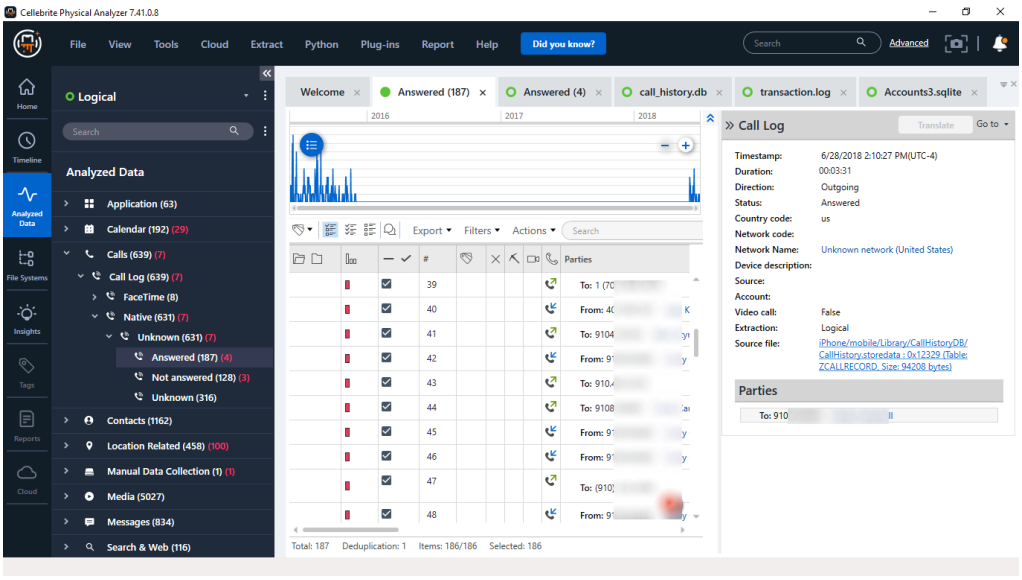


Figure 23: Cellebrite iOS call logs

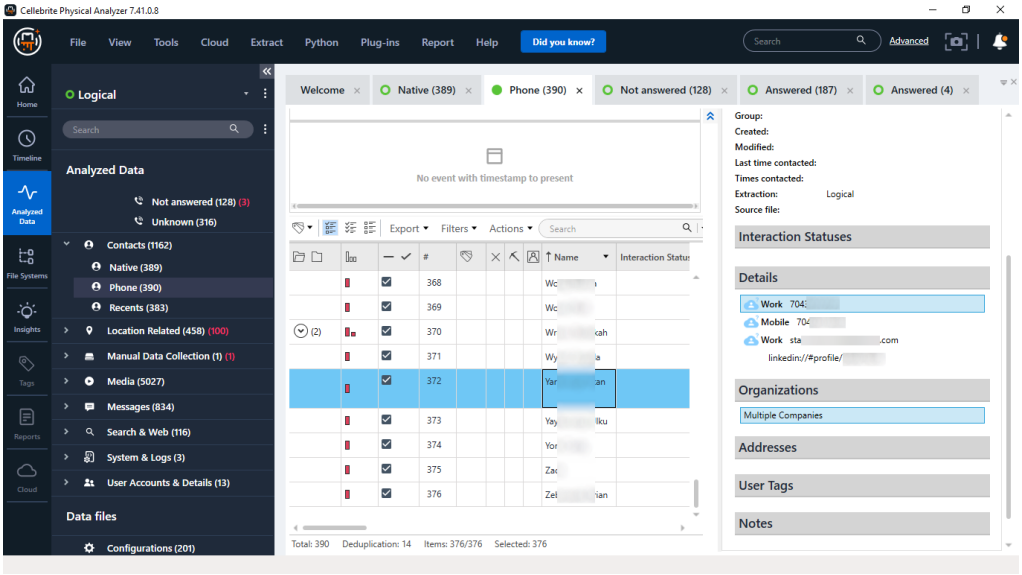


Figure 24: Cellebrite iOS contact lists

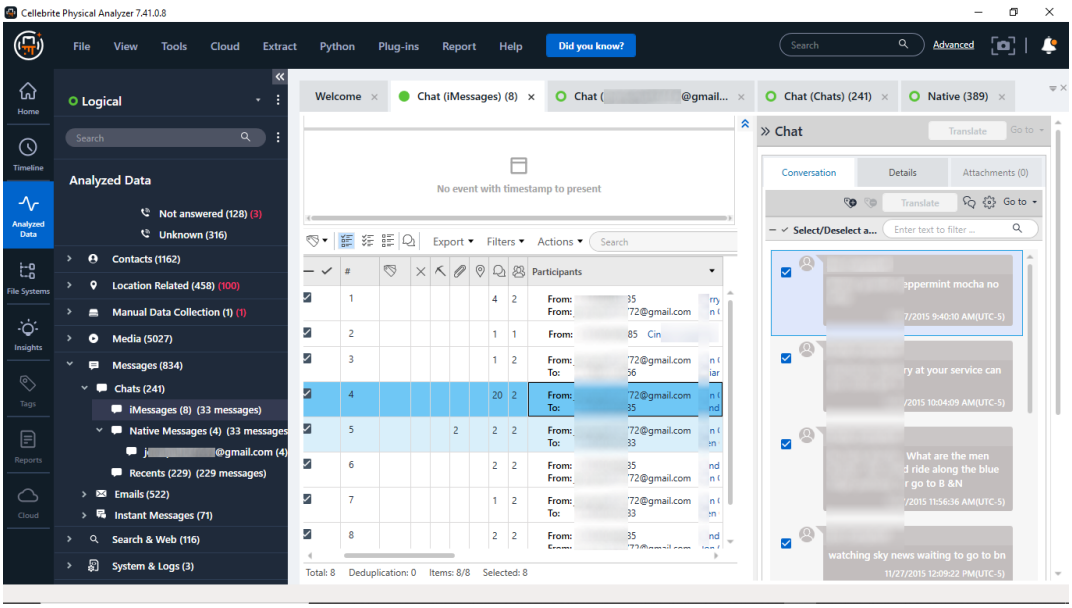


Figure 25: Cellebrite iOS iMessages

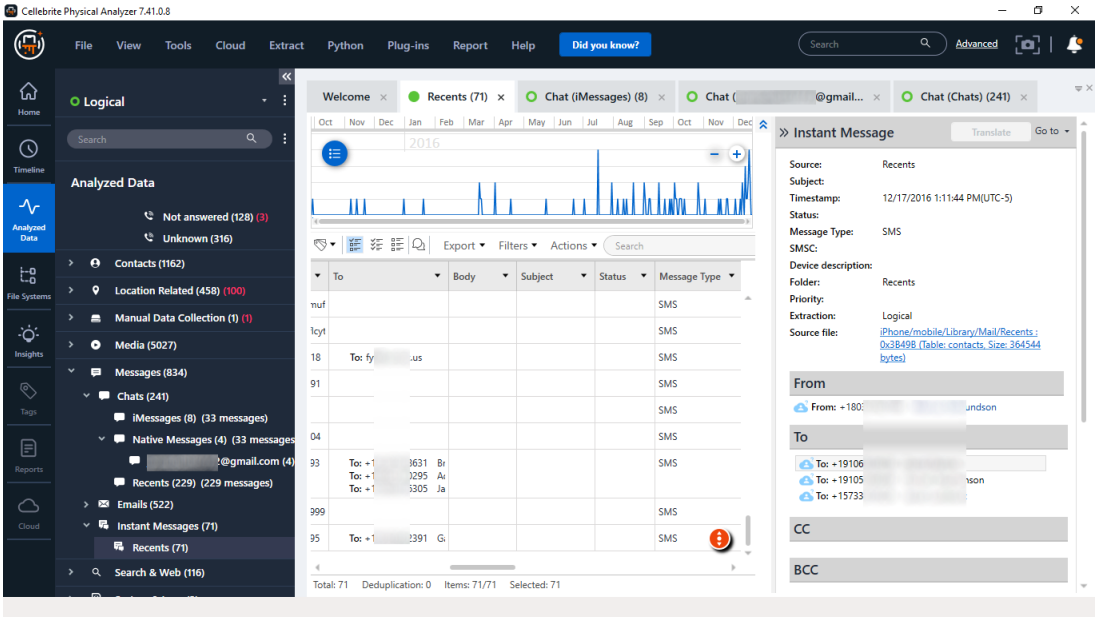


Figure 26: Cellebrite iOS SMS messages

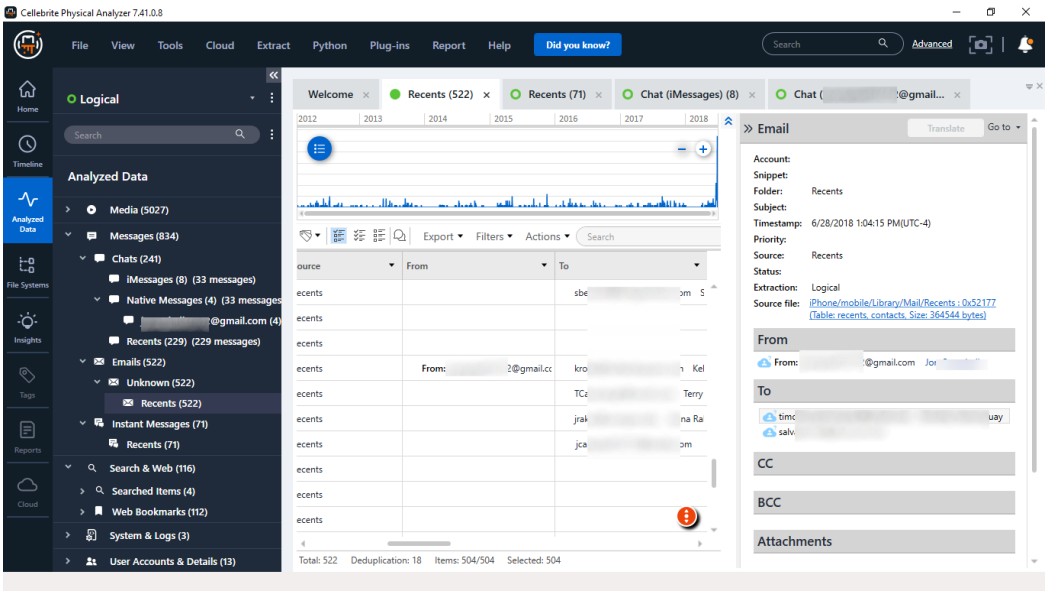


Figure 27: Cellebrite iOS Email messages

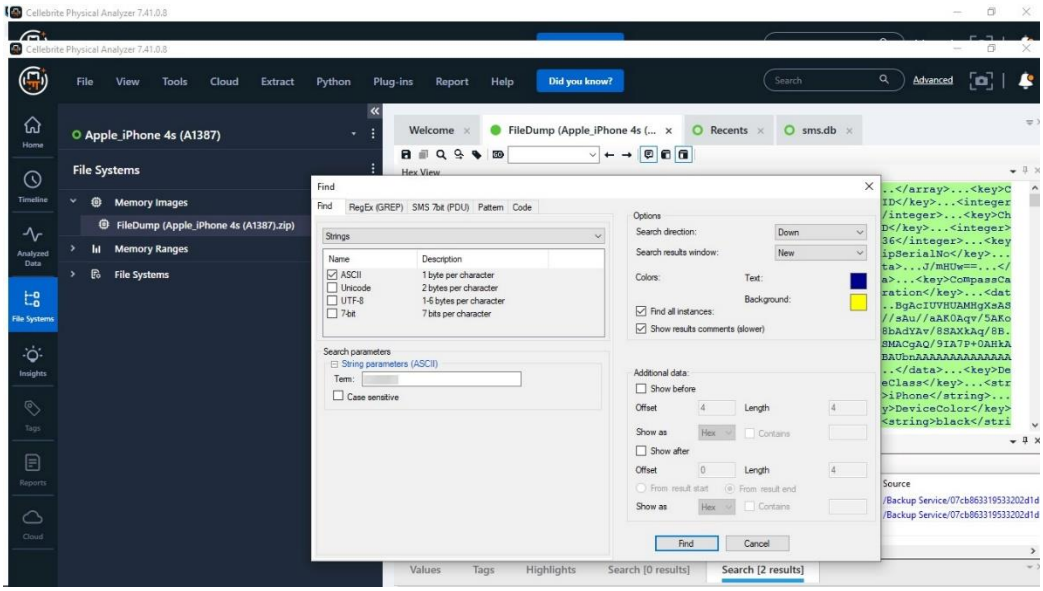


Figure 28: Cellebrite iOS volatile memory analysis

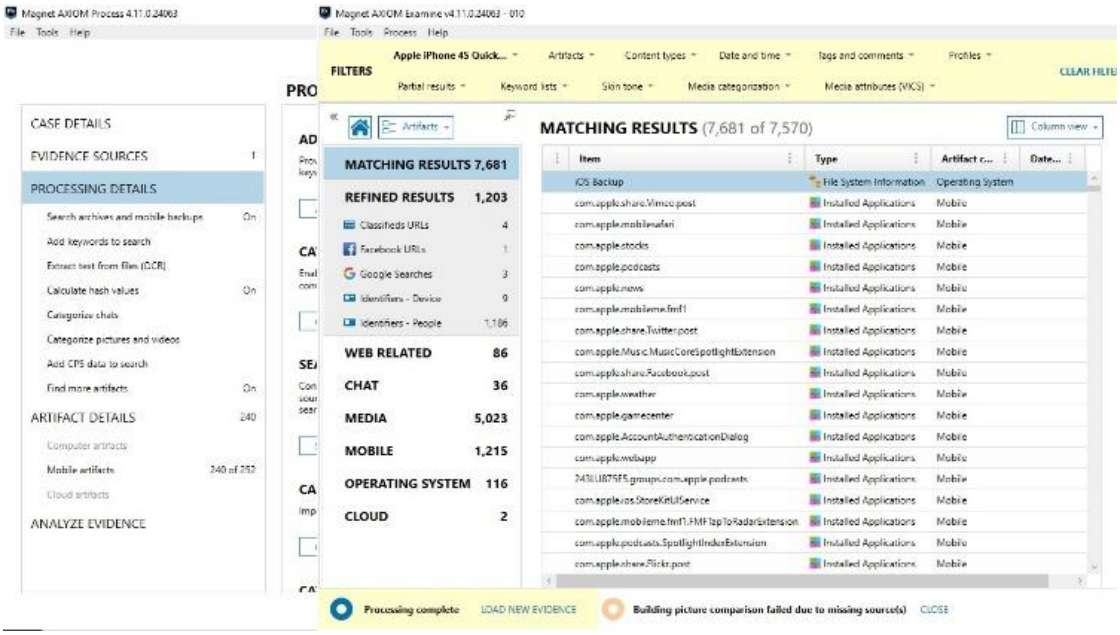


Figure 29: Axiom data processing overview

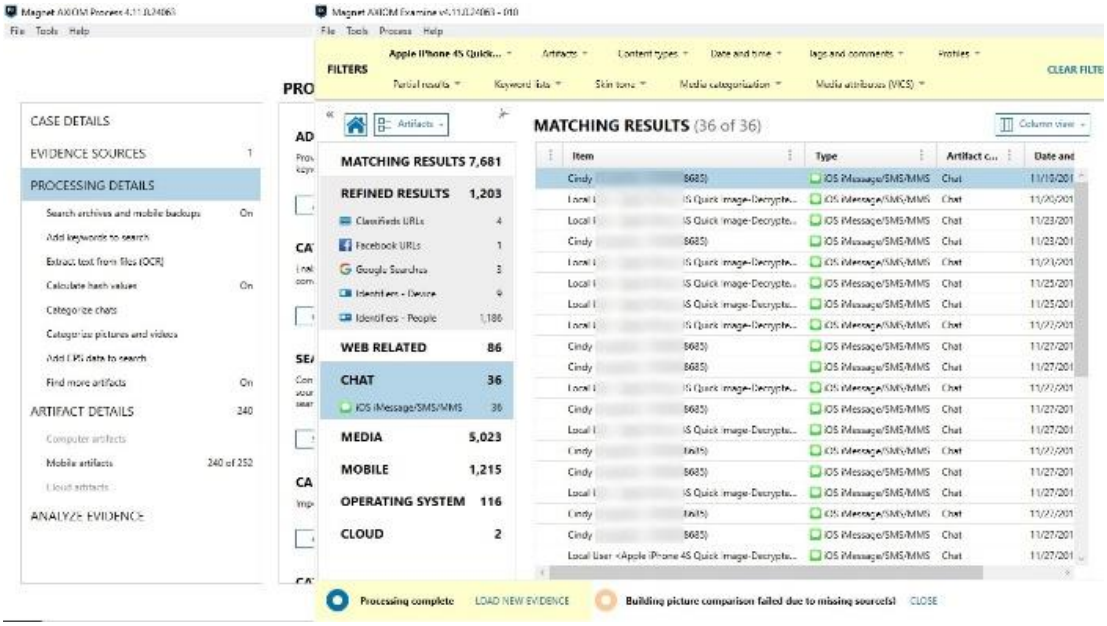


Figure 30: Axiom SMS/MMS messages

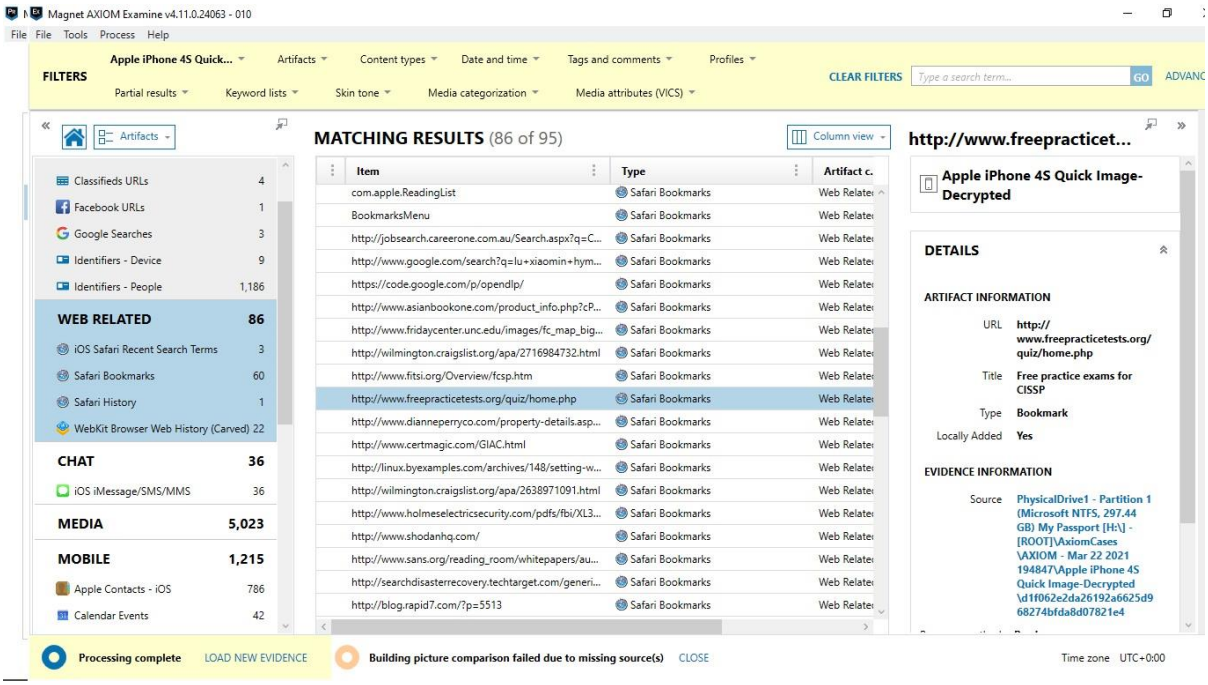


Figure 31: Axiom Safari browser data

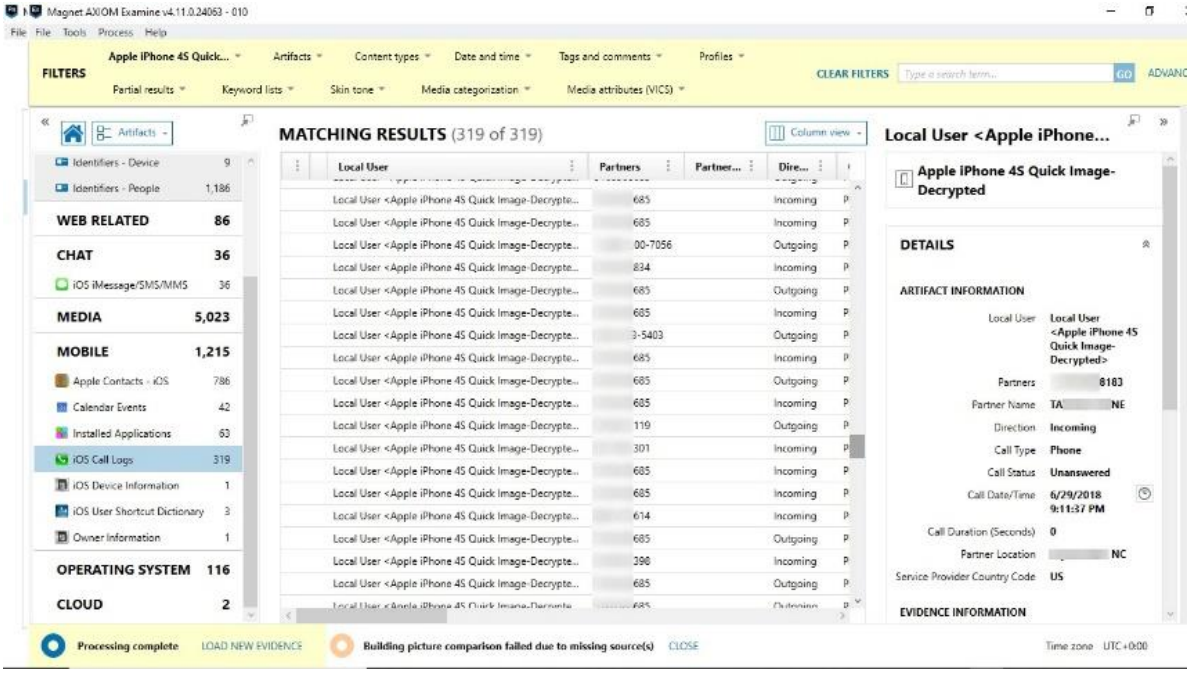


Figure 32: Axiom iOS call logs

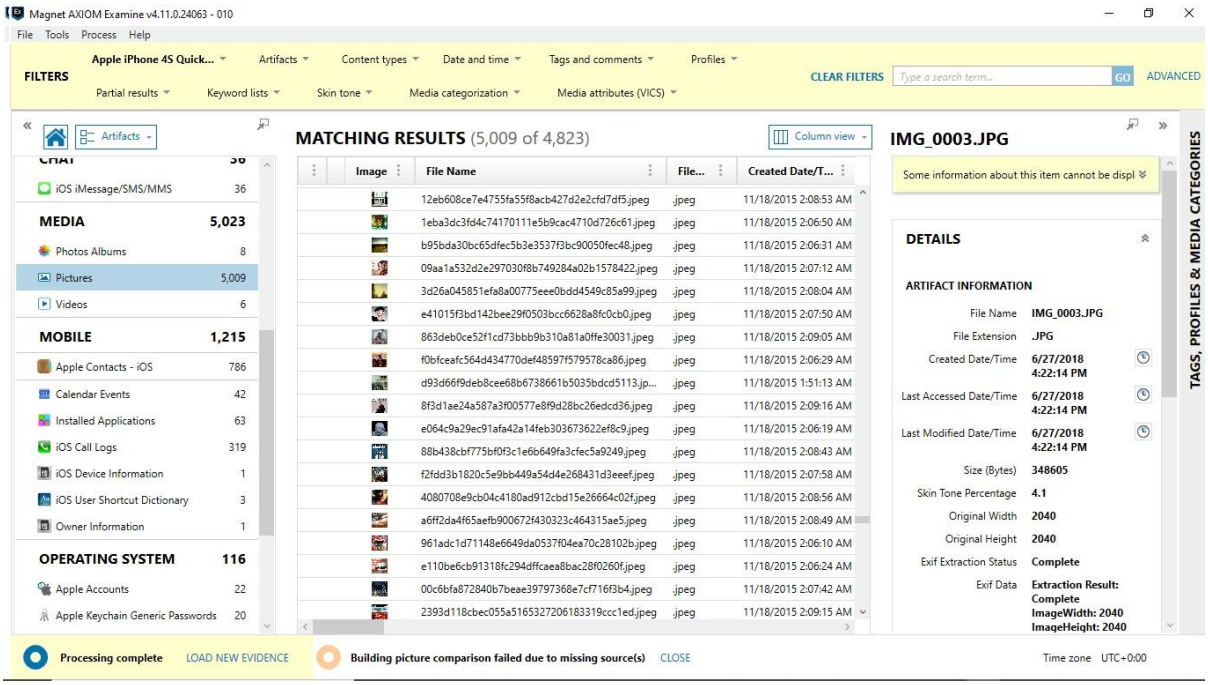


Figure 33: Axiom images found

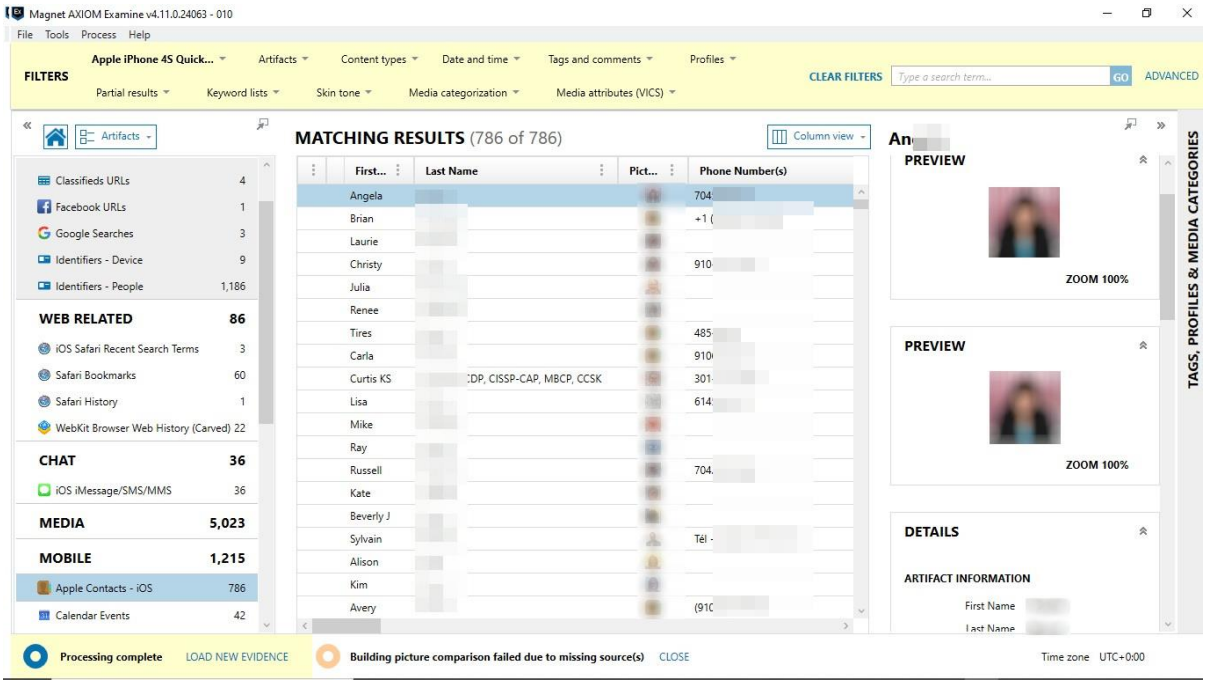


Figure 34: Axiom iOS contacts

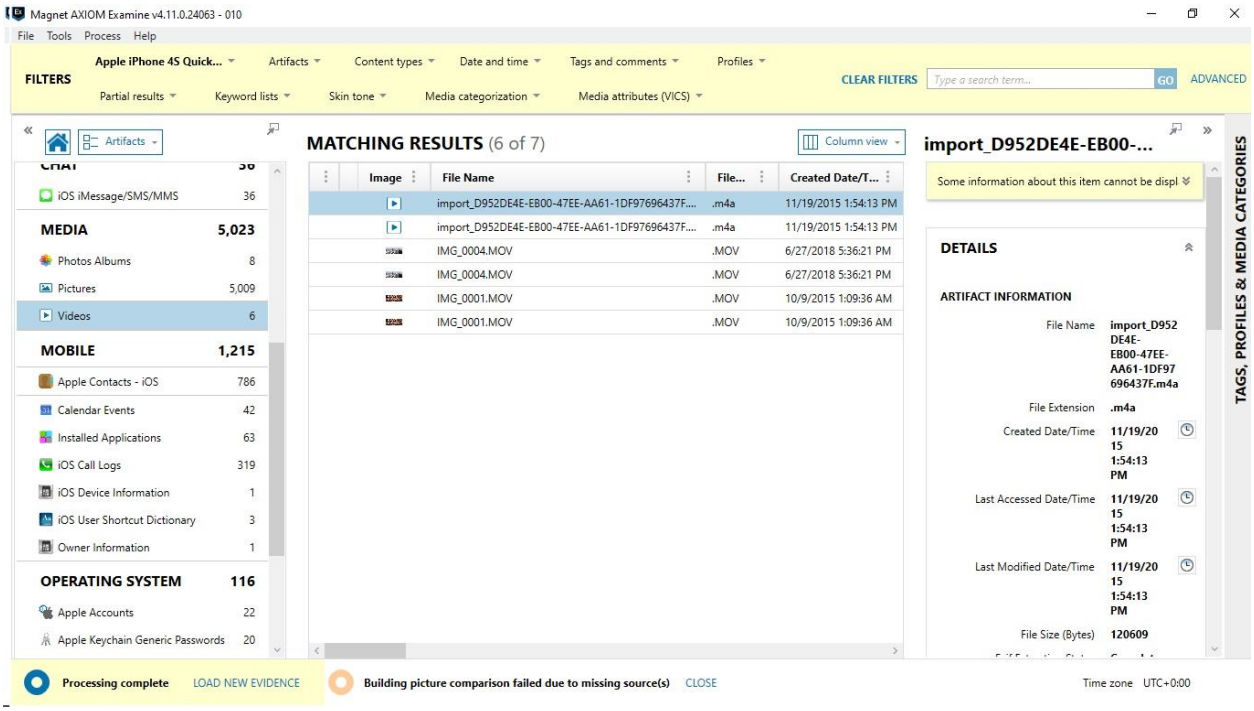
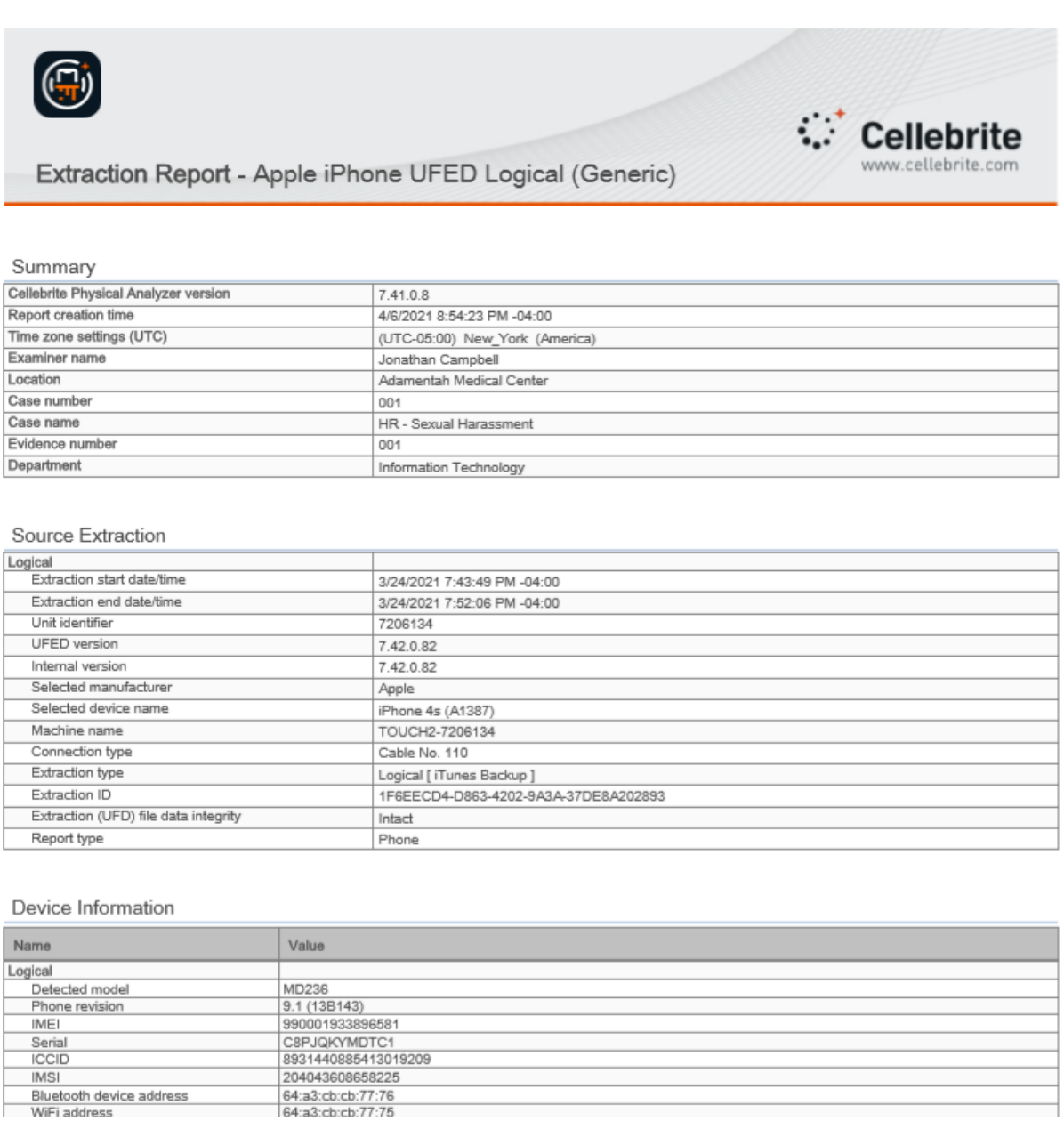


Figure 35: Axiom iOS videos



Extraction Report - Apple iPhone UFED Logical (Generic)

Cellebrite
www.cellebrite.com

Summary

Cellebrite Physical Analyzer version	7.41.0.8
Report creation time	4/6/2021 8:54:23 PM -04:00
Time zone settings (UTC)	(UTC-05:00) New_York (America)
Examiner name	Jonathan Campbell
Location	Adamentah Medical Center
Case number	001
Case name	HR - Sexual Harassment
Evidence number	001
Department	Information Technology

Source Extraction

Logical	
Extraction start date/time	3/24/2021 7:43:49 PM -04:00
Extraction end date/time	3/24/2021 7:52:06 PM -04:00
Unit identifier	7206134
UFED version	7.42.0.82
Internal version	7.42.0.82
Selected manufacturer	Apple
Selected device name	iPhone 4s (A1387)
Machine name	TOUCH2-7206134
Connection type	Cable No. 110
Extraction type	Logical [iTunes Backup]
Extraction ID	1F6EECD4-D863-4202-9A3A-37DE8A202893
Extraction (UFD) file data integrity	Intact
Report type	Phone

Device Information

Name	Value
Logical	
Detected model	MD236
Phone revision	9.1 (13B143)
IMEI	990001933896581
Serial	C8PJQKYMDTC1
ICCID	8931440885413019209
IMSI	204043608658225
Bluetooth device address	64:a3:cb:cb:77:76
WiFi address	64:a3:cb:cb:77:75

Figure 36: Cellebrite report example

FORENSIC EXAMINATION REPORT

CASE NUMBER 001

Examiner	Jonathan Campbell
Case generated	Friday, March 26, 2021
Report generated	Friday, March 26, 2021

Figure 37: Axiom report example