CELLEBRITE 2023

CAPTURE THE FLAG (CTF)
FELIX IPHONE

CTF QUESTIONS ONLY

1.	Question 1 - Voicemail - level 1 - (10 points) ***Please look at the following image: IMG_0026.HEIC. How many times do you see this picture on the device (including thumbnails)?***
2.	Question 2 - Picture - level 1 (10 points) ***Felix confirmed receiving "everything." When Felix sent the confirmation, which account did he sent it from?***
3.	Question 3 - Confirmation - level 1 (10 points) ***Felix confirmed receiving "everything." When Felix sent the confirmation, which account did he sent it from?***
4.	Question 4 - Photo (10 points) ***Private Photo Vault is an application that is installed on the phone. What is the passcode to the application?***
5.	Question 5 - Location (10 points) ***Felix always had an interest in the USA. What application did he use to search an address in New Jersey USA?***
6.	Question 6a - Size - Level1 (10 points) ***What is the size (in bytes) of the ChatStorage.sqlite-wal file? (Answer with numeric digit(s) only)***
7.	Question 7 - Size - Level 2 (30 points) ***What is the date and time the -WAL file from Felix 06a committed to the main database?***

8.	Question 8 - Missing - Level 2 (30 points) ***When was the SIM card information on Felix's phone last updated? (Raw data, not converted)***
9.	Question 9 - Wiped - Level 2 (30 points) ***The WhatsApp chat database appears to be missing some chat messages. Assuming the highest number is the last message, how many messages are missing?***
10.	Question 10 - Cruise - Level 2 (30 points) ***When was Felix's phone last wiped? [YYYY-MM-DD HH:MM:SS]***
11.	Question 11 - Data - Level 3 (50 points) ***Felix was researching / surveilling a ship as a possible target and downloaded a photo of it. What is the name of the cruise ship?***
12.	Question 12 - H is mean - Level 3 (100 points) ***Felix was referred information about pension reform. What is the SID associated with that artifact?***

ABOUT THIS CTF CHALLENGE

This challenge was created by Cellebrite (see: https://cellebrite.com/en/cellebrite-capture-the-flag-september-2023/).

FORENSIC IMAGE SOURCE

Download: CellebriteCTF23_Felix.zip

MD5: 996A913B1301AB011CA7DD8CA93A9400

OTHER ONLINE SOLUTIONS

The following other solutions can be found online:

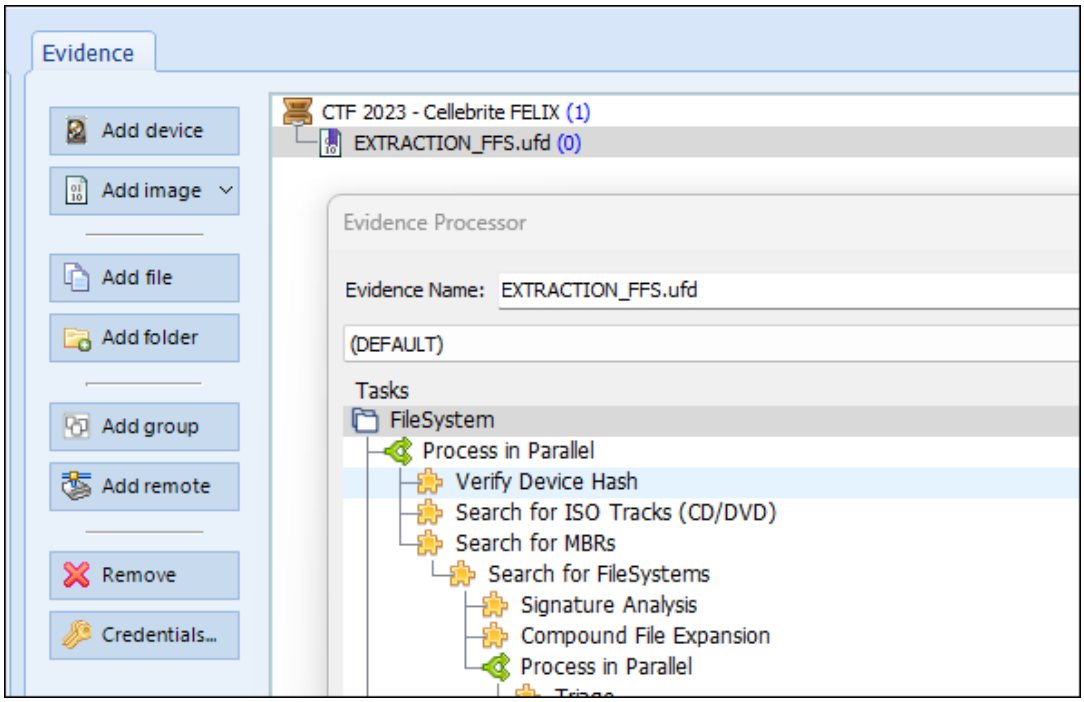
- https://cellebrite.com/en/cellebrites-ctf-2023-recap-answers-for-felixs-iphone-device/
- https://www.stark4n6.com/2023/10/cellebrite-ctf-2023-felix.html

STARTING THIS CHALLENGE IN FORENSIC EXPLORER

In the **Evidence** module:

1. Select the **New Case** button.
2. Enter investigator details (if required) and a **case name**.
3. Click the **Add Image** button.
4. Add the **Cellebrite** file: **EXTRACTION_FFS.ufd**
5. In the **Evidence Processor** window use the default options.

Figure 1: Evidence module > Add Image

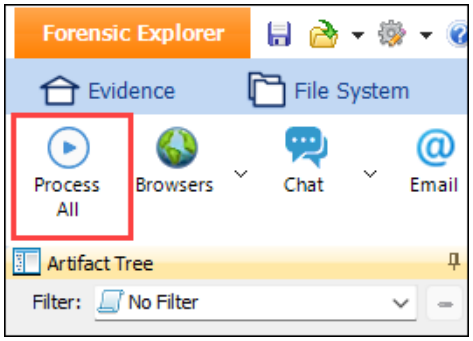


ARTIFACTS > PROCESS ALL

The Forensic Explorer **Artifacts module** extracts common forensic artifacts from SQLite, Plist, TXT, XML and other files. To populate artifacts:

1. Click the Artifacts module > **Process All** button.

Figure 2: Artifacts > Process All



QUESTION 1 - VOICEMAIL - LEVEL 1 - (10 POINTS)

Felix received a voicemail from +1-416-435-5684. How many seconds in length was the voicemail message?

Q1. ANSWER

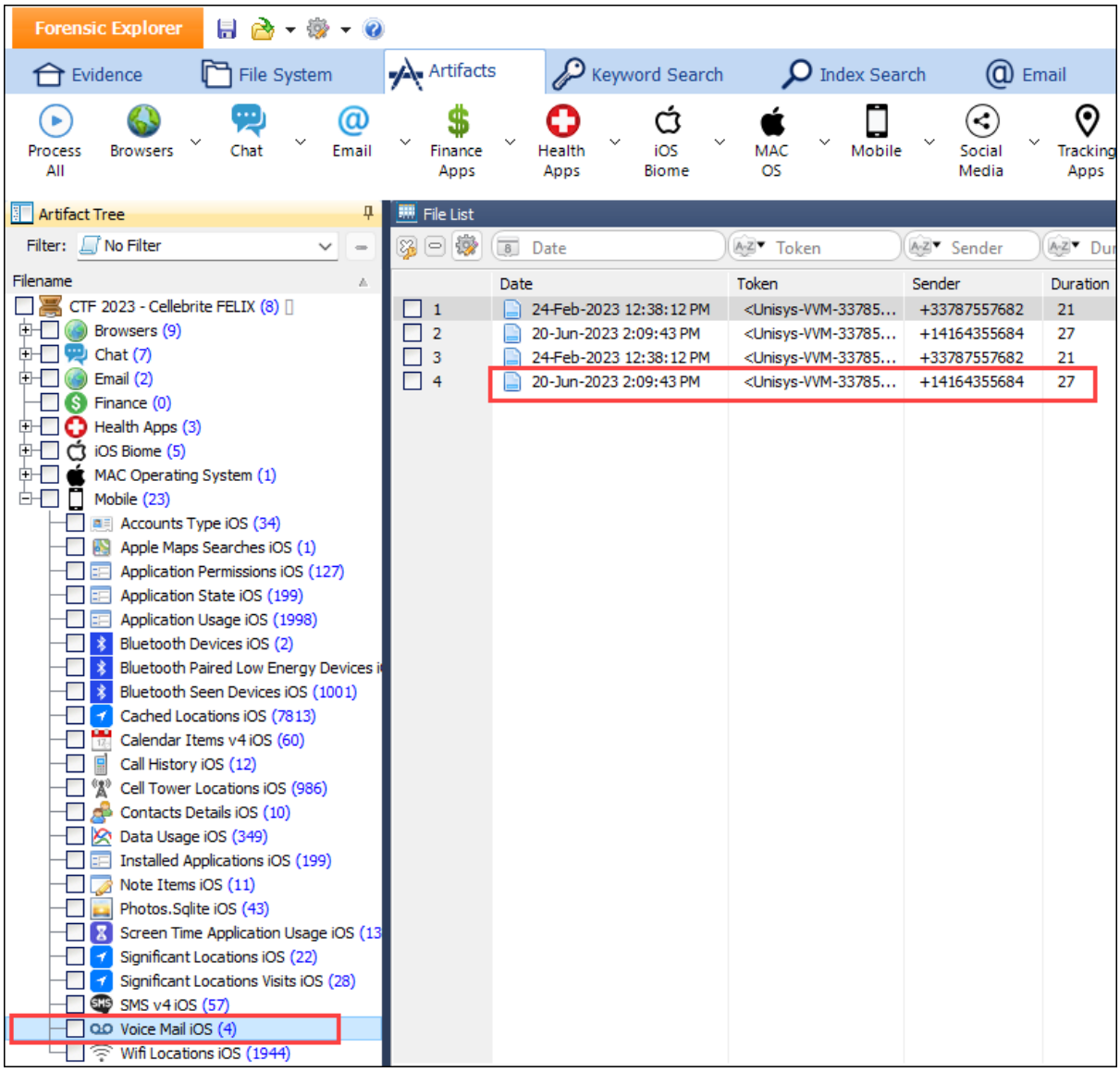
27 seconds.

Q1. FORENSIC EXPLORER METHODOLOGY

In the **Artifacts** module:

1. Select **Mobile** > **Voice Mail iOS**.

Figure 3: Artifacts > Mobile > Voice Mail iOS



QUESTION 2 - PICTURE - LEVEL 1 (10 POINTS)

Please look at the following image: IMG_0026.HEIC. How many times do you see this picture on the device (including thumbnails)?

Q2. ANSWER

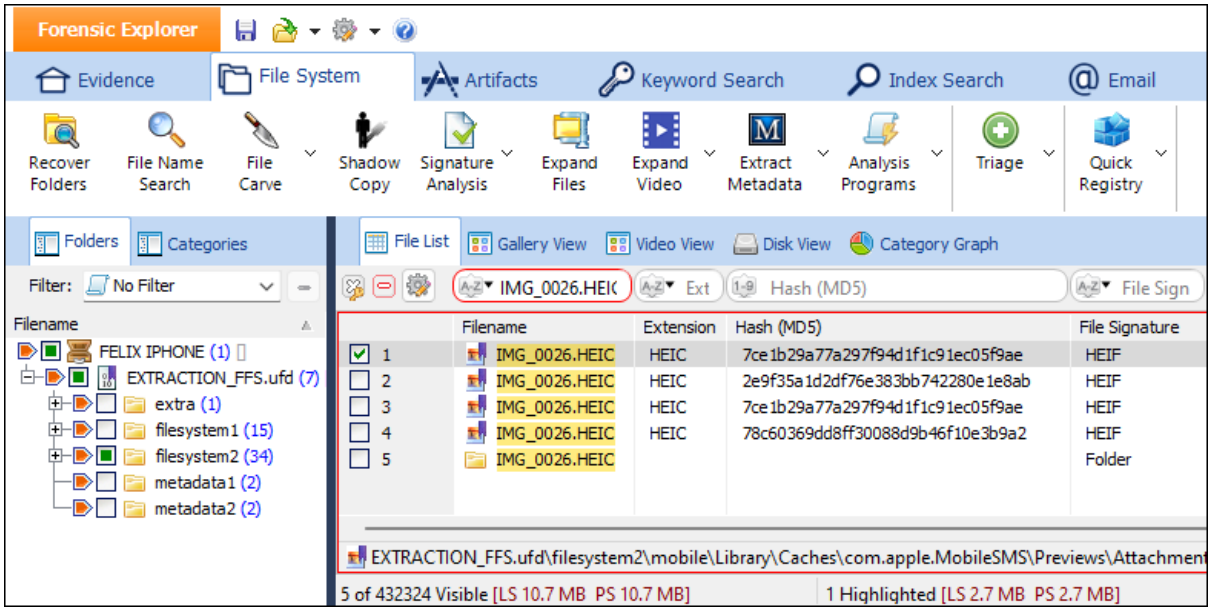
5 instances.

Q2. FORENSIC EXPLORER METHODOLOGY

Important: If HEIC files do not display in either Gallery View or display view, a HEIC drive is required. Install from: https://www.copytrans.net/copytransheic/.

To locate **IMG_0026.HEIC** files:

1. Branch plate [ ] the **entire case**.
2. In the File System > File List > Filename column filter, enter **IMG_0026.HEIC**.
3. This filter locates **four files**, plus **one folder**, of the same name.
4. Inside the **IMG_0026.HEIC** folder is an additional file called **5005.JPG**.



A search was also run using the **File Name Search** button.

Figure 4: File System > File Name Search

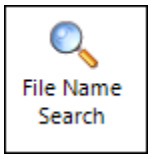
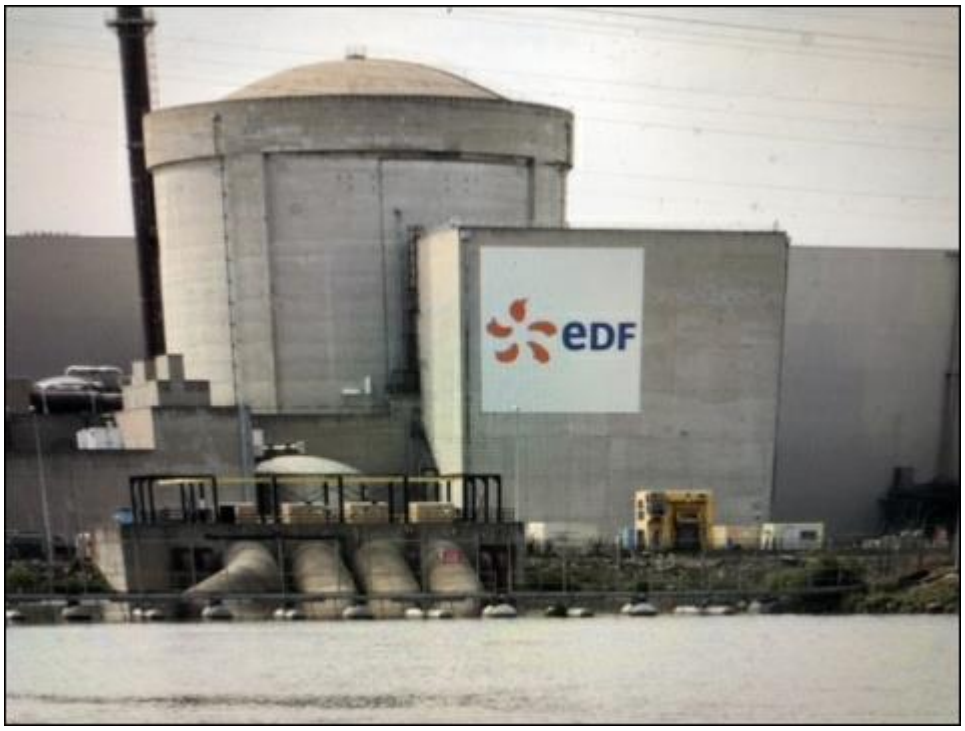


Figure 5: File Name Search result

```
File/Folder Name
----------------
EXTRACTION_FFS.ufd\filesystem2\mobile\Library\Caches\com.apple.MobileSMS\Previews\Attachments\ff\15\D4797FAC-8067-4768-A
EXTRACTION_FFS.ufd\filesystem2\mobile\Library\SMS\Attachments\97\07\64E43269-C3B4-4FFD-8A14-41FFD406EDA1\IMG_0026.HEIC
EXTRACTION_FFS.ufd\filesystem2\mobile\Library\SMS\Attachments\ff\15\D4797FAC-8067-4768-A5E7-EE3D325E5711\IMG_0026.HEIC
EXTRACTION_FFS.ufd\filesystem2\mobile\Media\DCIM\100APPLE\IMG_0026.HEIC
EXTRACTION_FFS.ufd\filesystem2\mobile\Media\PhotoData\Thumbnails\V2\DCIM\100APPLE\IMG_0026.HEIC
```

Figure 6: IMG_0026.HEIC



QUESTION 3 - CONFIRMATION - LEVEL 1 (10 POINTS)

Felix confirmed receiving "everything." When Felix sent the confirmation, which account did he sent it from?

Q3. ANSWER

felix.davey@orange.fr

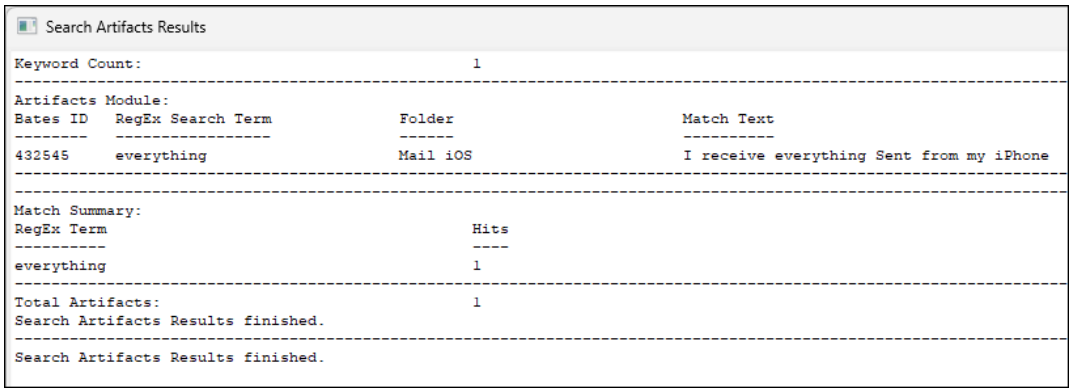
Q3. FORENSIC EXPLORER METHODOLOGY

In the **Artifacts** module:

1. Use the **Search Artifact Results** button to search for "**I received everything**".

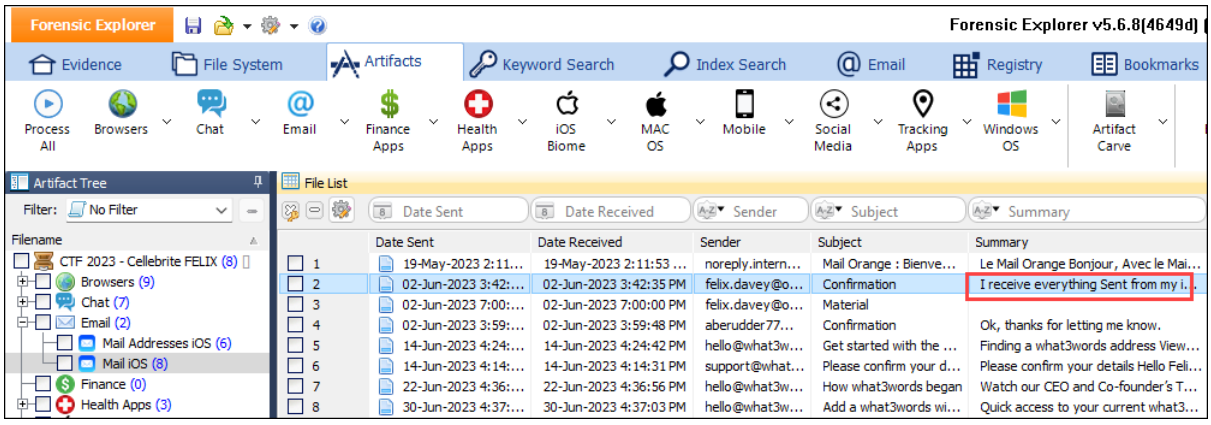
Figure 7: Artifacts > Search Artifact Results

Figure 8: Artifacts > Search Artifact Results > output



The search result identifies **Artifacts** > **Emil** > **Mail iOS** as a potential source:

Figure 9: Artifacts > Email > Mail iOS

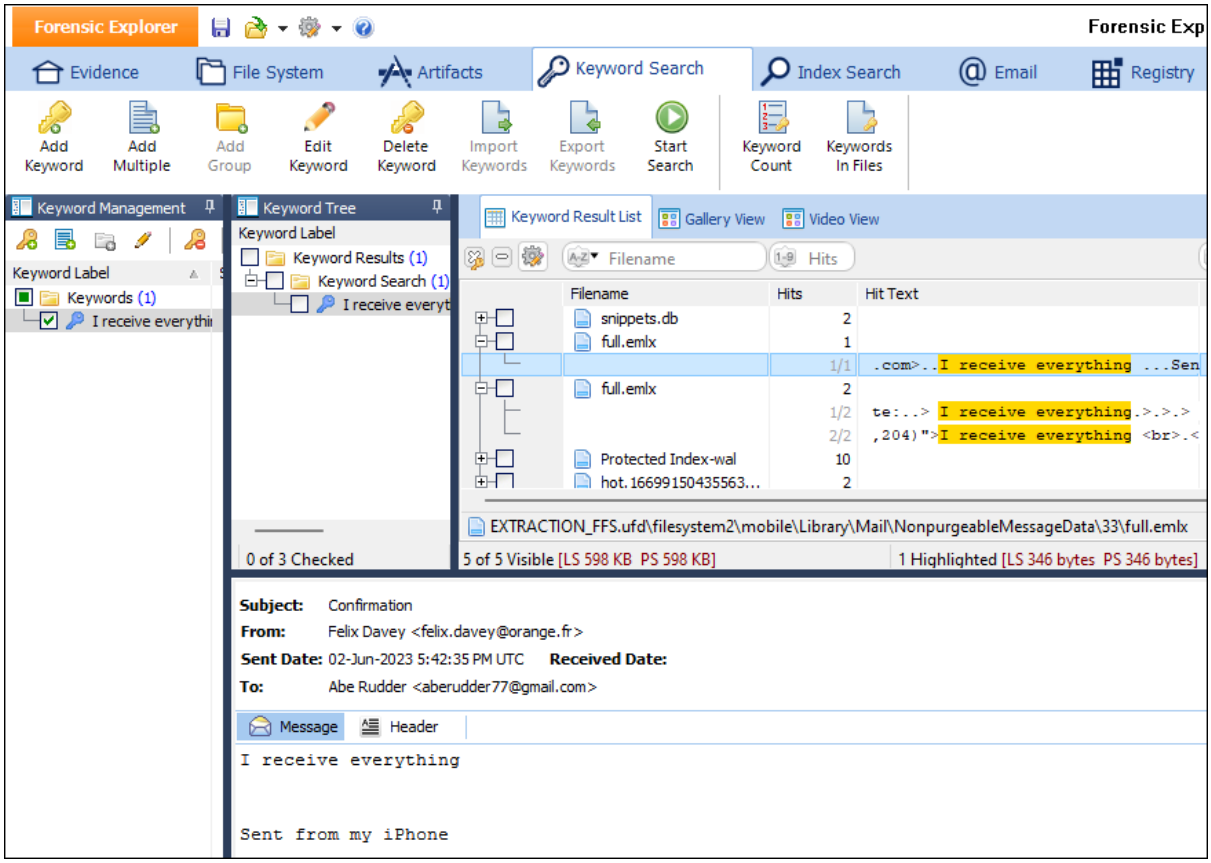


As a follow-up search, In the **Keyword Search** module:

1. Add the keyword phrase **"I received everything"**.

This search locates two files in the filesystem called **full.emlx**. These files can be displayed with the full email header.

Figure 10: Keyword Search > "I received everything"



QUESTION 4 - PHOTO (10 POINTS)

Private Photo Vault is an application that is installed on the phone. What is the passcode to the application?

Q4. ANSWER

2510.

Q4. FORENSIC EXPLORER METHODOLOGY

This answer is being updated. Check back soon.

QUESTION 5 - LOCATION (10 POINTS)

Felix always had an interest in the USA. What application did he use to search an address in New Jersey USA?

Q5. ANSWER

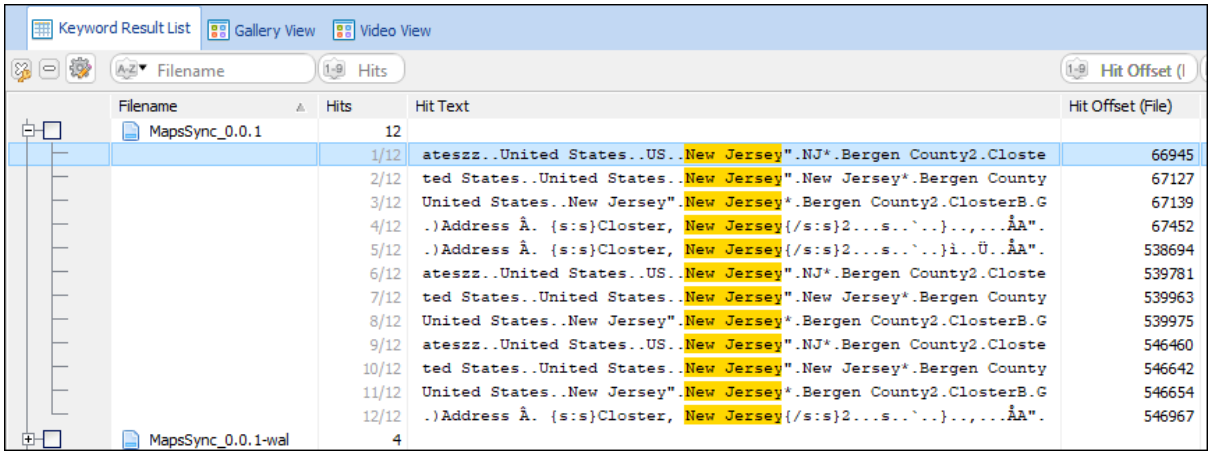
Apple Maps.

Q5. FORENSIC EXPLORER METHODOLOGY

Apple Maps is the usual suspect for navigation searches on an iPhone. In the **Keyword Search** module:

1. Search for the keyword **New Jersey**:

Figure 11: Keyword Search module



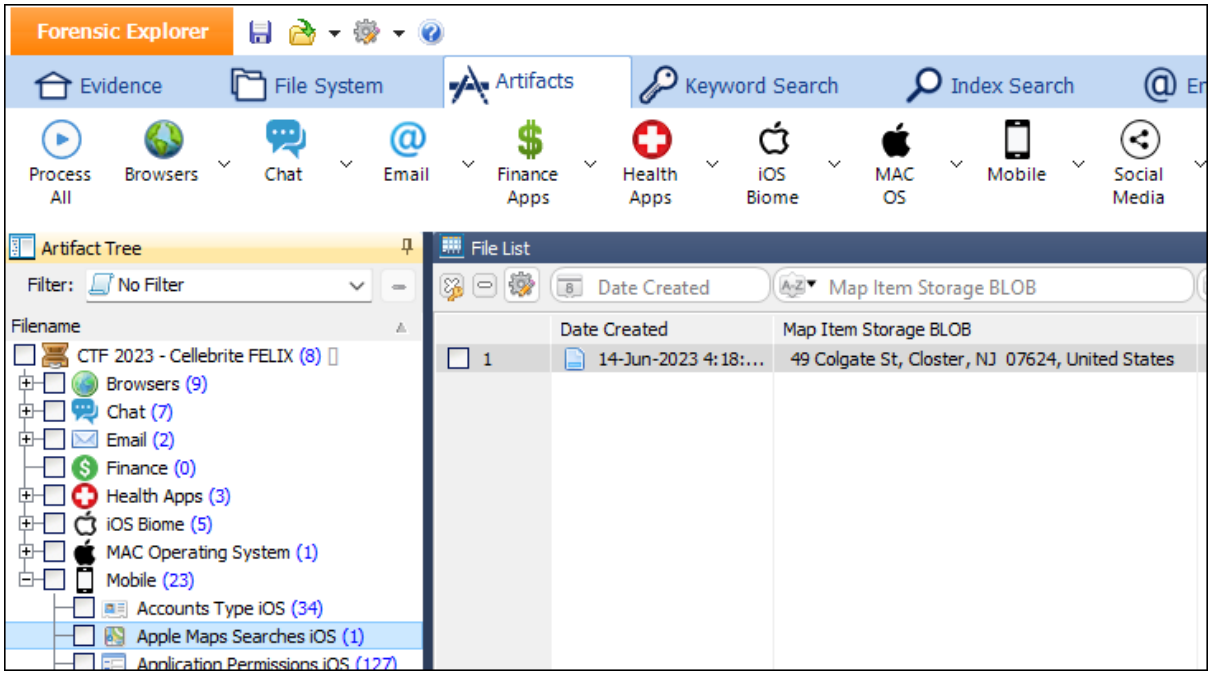
The search result identifies **MapsSync_0.0.1** (a known Apple Maps file) as a potential source.

In the **Artifacts** module:

1. Examine **Mobile** > **Apple Maps Searches iOS**.

This shows that the address **49 Colgate St, Closter, NJ 07624, United States**, was searched in Apple maps on 14 June 2023.

Figure 12: Artifacts > Mobile > apple Maps Searches iOS



QUESTION 6A - SIZE - LEVEL1 (10 POINTS)

What is the size (in bytes) of the ChatStorage.sqlite-wal file? (Answer with numeric digit(s) only)

Q6A. ANSWER

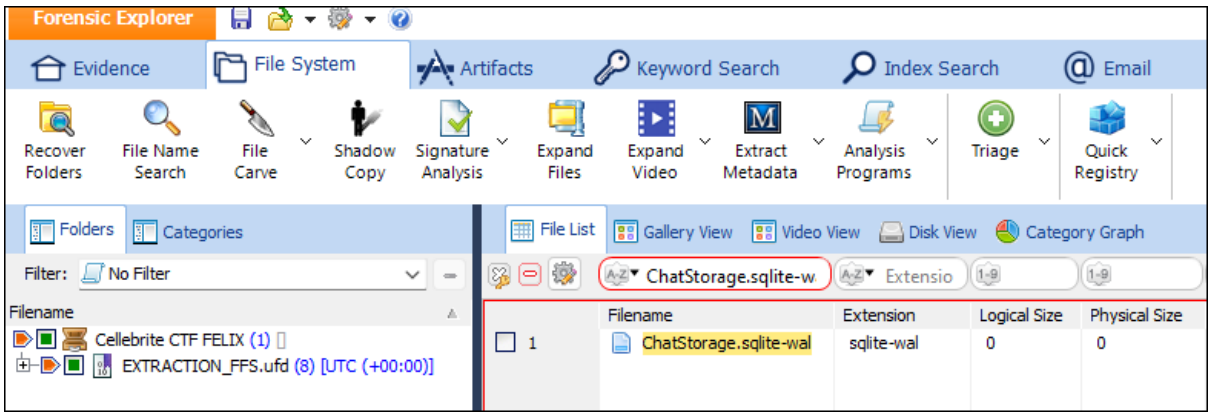
0 bytes.

Q6A. FORENSIC EXPLORER METHODOLOGY

In the **File System** module:

1. Branch plate [ ] the **entire case**.
2. Enter **ChatStorage.sqlite-wal** in the **Filename** column filter.
3. Examine the **Logical Size** column.

Figure 13: File System > Filename column filter



QUESTION 6B - TIME - LEVEL 2 (30 POINTS)

What is the date and time the -WAL file from Felix 06a committed to the main database?

Q6B. ANSWER

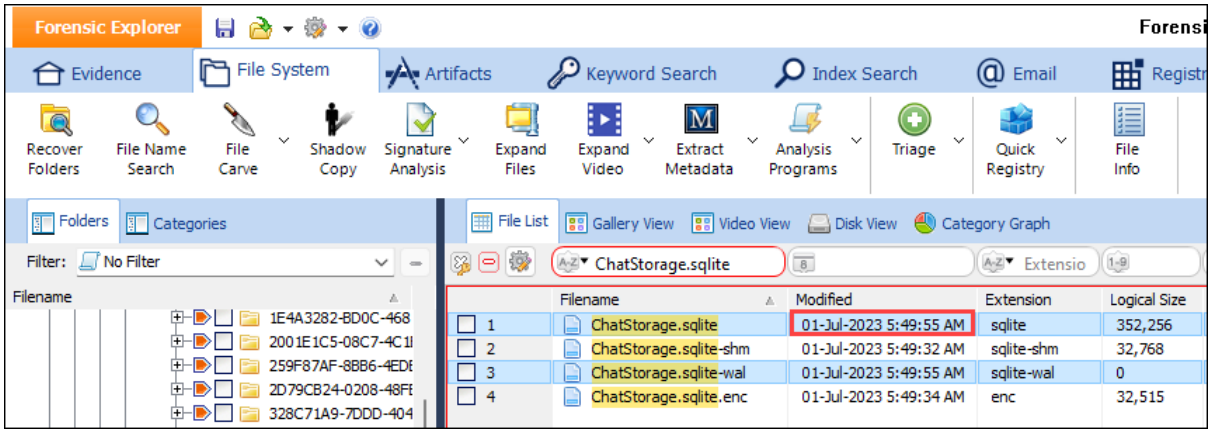
2023-07-01 05:49:55.

Q6B. FORENSIC EXPLORER METHODOLOGY

In the **File System** module:

1. Branch plate [ ] the **entire case**.
2. Enter **ChatStorage.sqlite** in the **Filename** column filter.
3. Examine the **Logical Size** column of the filtered results.

Figure 14: File System > Filename column filter



The **modified** date of **ChatStorage.sqlite** and **ChatStorage.sqlite-wal** files are the same. This is indicative of the commit from the -wal to the database.

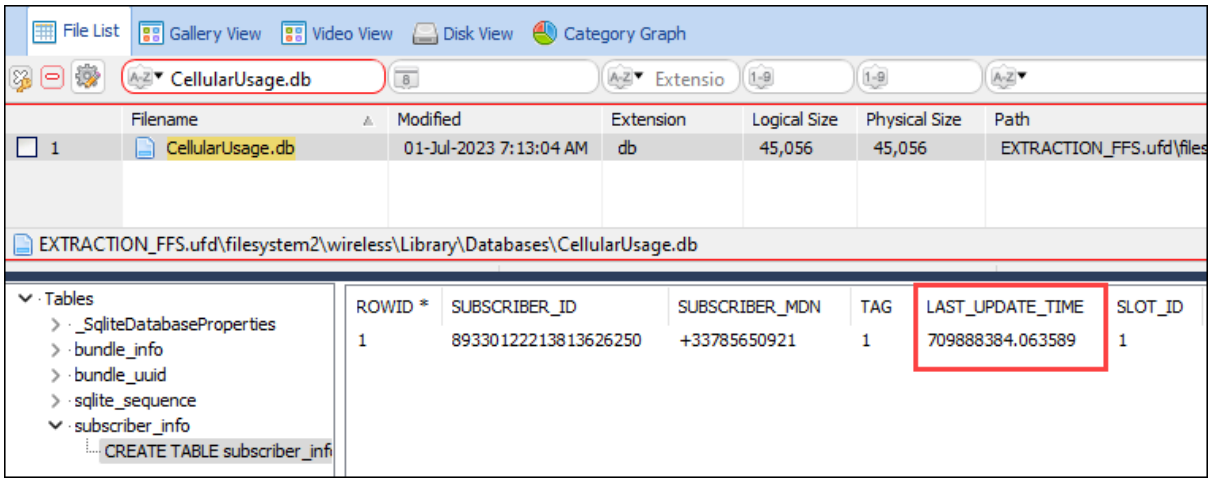
QUESTION 7 - SIZE - LEVEL 2 (30 POINTS)

When was the SIM card information on Felix's phone last updated? (Raw data, not converted)

Q7. ANSWER

709888384.063589.

Q7. FORENSIC EXPLORER METHODOLOGY



QUESTION 8 - MISSING - LEVEL 2 (30 POINTS)

The WhatsApp chat database appears to be missing some chat messages. Assuming the highest number is the last message, how many messages are missing?

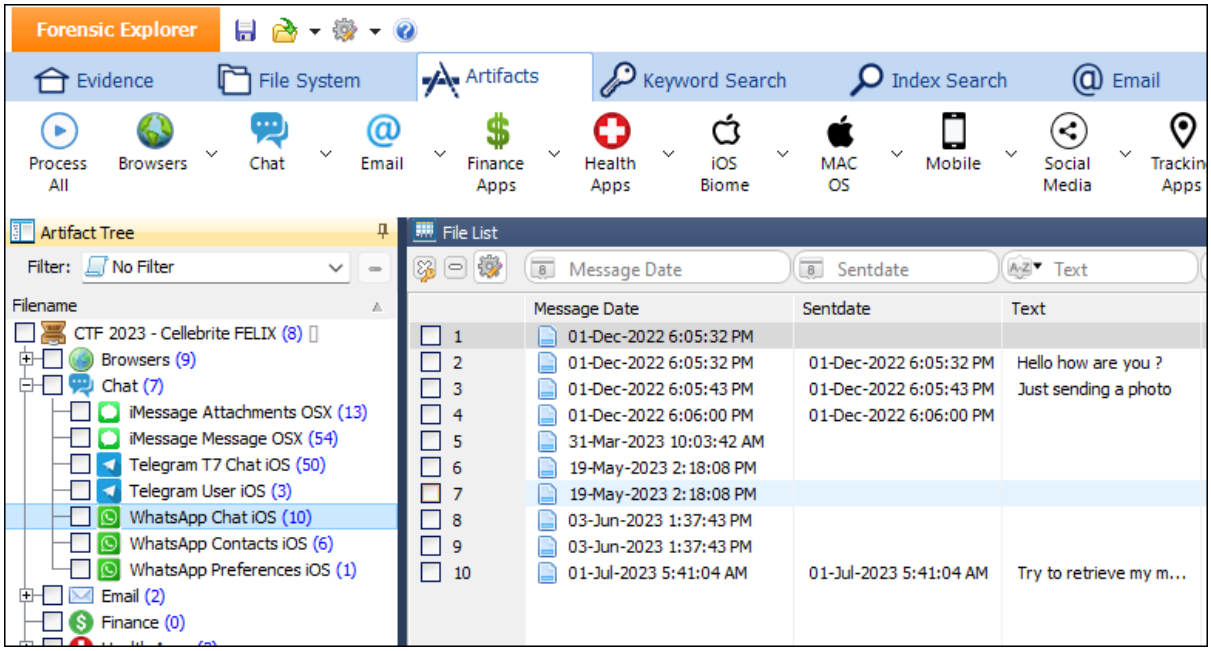
Q8. ANSWER

19 messages are missing.

Q8. FORENSIC EXPLORER METHODOLOGY

Artifacts > **Chat** > **WhatsApp Chat iOS** shows 10 messages:

Figure 15: WhatsApp Chat iOS

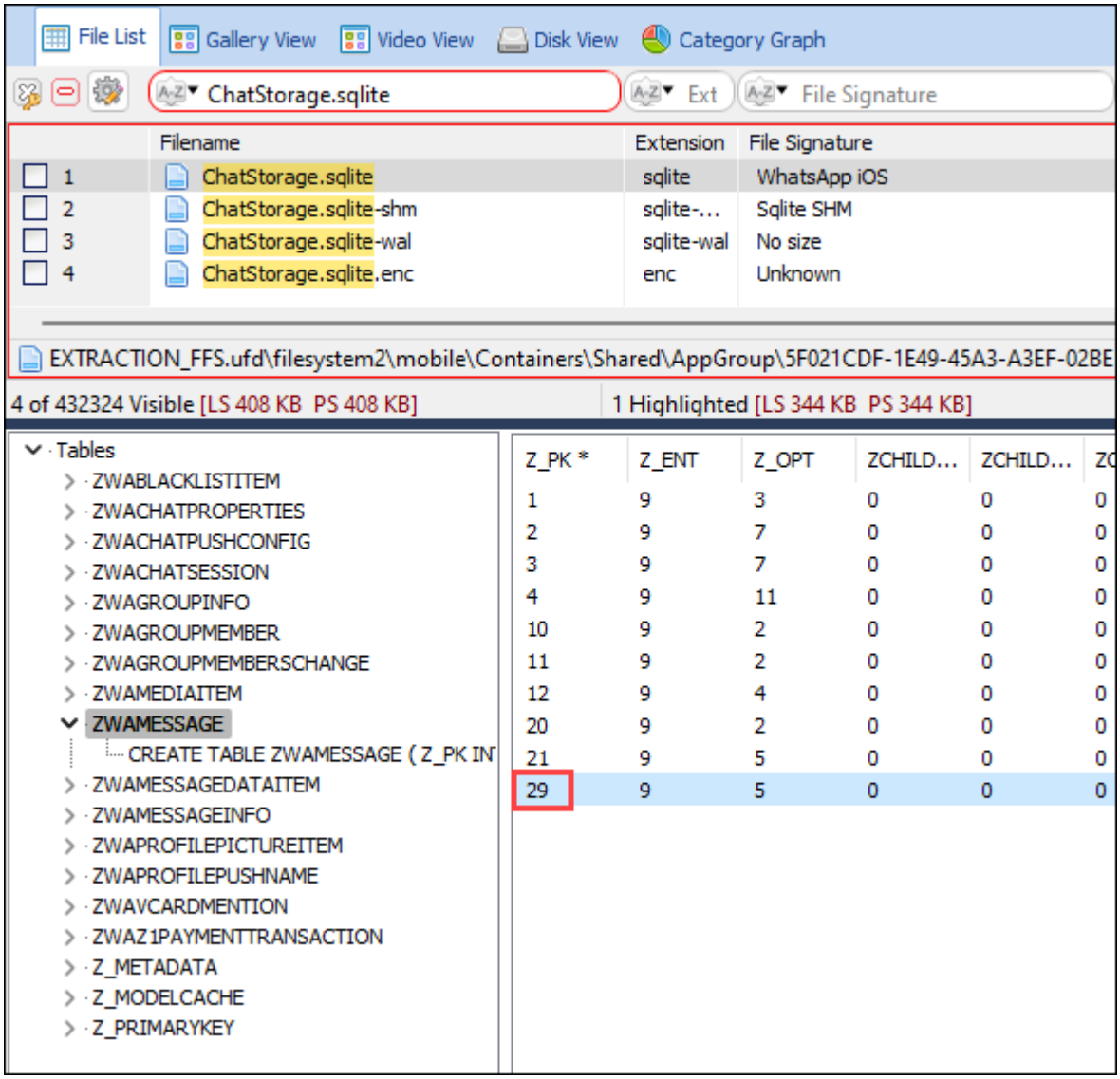


The **Source Path** and **Source Name** columns show **ChatStorage.sqlite** to be the source. The **Location** column lists the primary SQL Table as **zwamessage**.

To examine the **ChatStorage.sqlite, zwamessage** table:

1. In the **File System** module, Branch plate [ ] the **entire case**.
2. Enter **ChatStorage.sqlite** in the **Filename** column filter.
3. In the **Display View**, locate the **ZWAMESSAGE** table.

Figure 16: File System > ChatStorage.sqlite > Display View ZWAMESSAGE table



The **Z_PK** column shows **29** as the highest numbered message. Subtract the 10 visible messages and there are 19 missing items.

QUESTION 9 - WIPED - LEVEL 2 (30 POINTS)

When was Felix's phone last wiped? [YYYY-MM-DD HH:MM:SS]

Q9. ANSWER

2022-12-01 17:16:55.

Q9. FORENSIC EXPLORER METHODOLOGY

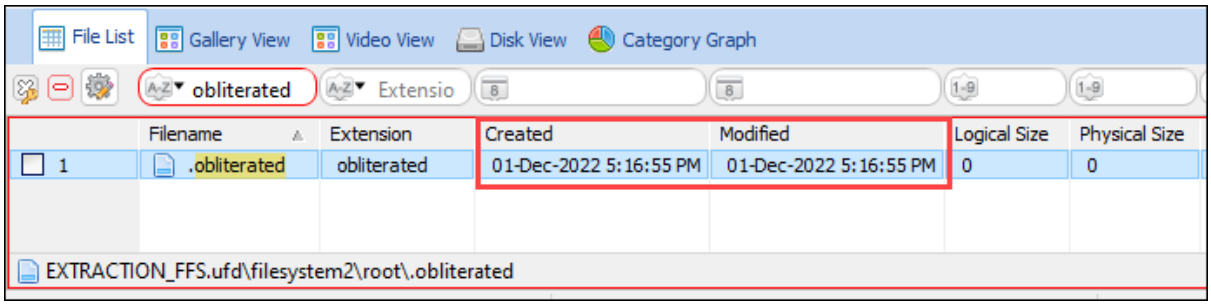
A common file that is used to identify an iOS device wipe is **root\.obliterated** (see: https://dfir.pubpub.org/pub/6i7d593n/release/1). This is a zero-byte file created by the device upon booting after a wipe.

To search for **.obliterated**:

1. In the File System module, branch plate [ ] the **entire case**.
2. In the **Filename column header**, filter by **obliterated**.

The filter identified a **.obliterated** file with a created and modified date of 1 December 2022.

Figure 17: File System column filter



QUESTION 10 - CRUISE - LEVEL 2 (30 POINTS)

Felix was researching / surveilling a ship as a possible target and downloaded a photo of it. What is the name of the cruise ship?

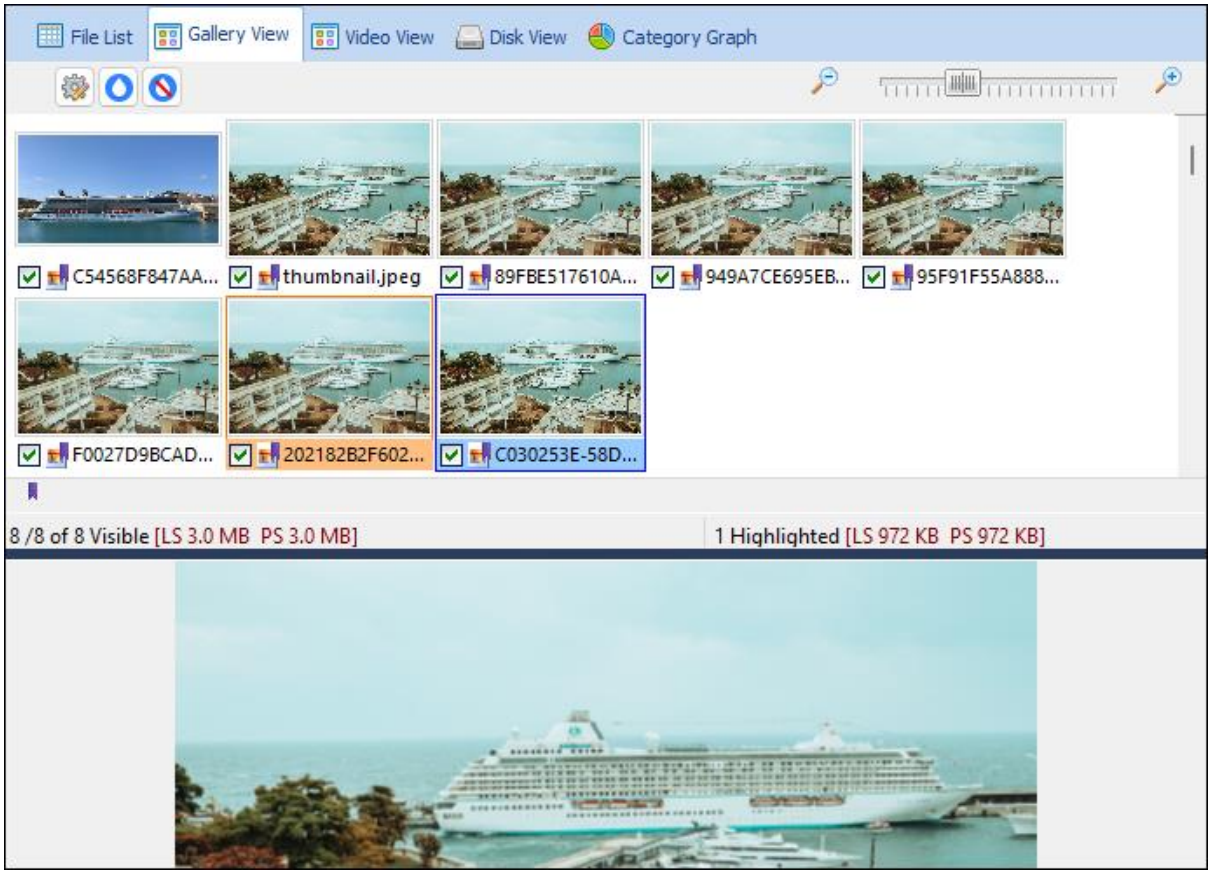
Q10. ANSWER

Q10. FORENSIC EXPLORER METHODOLOGY

A visual scan of File System > Gallery View was conducted:

3. In the File System module, branch plate [ ] the **entire case**.
4. Switch to Gallery View to examine the photos.

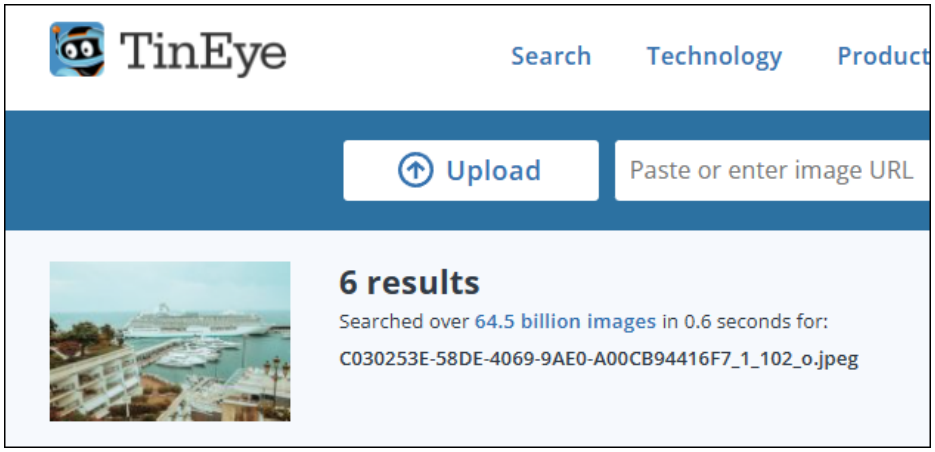
The following ship photos were located:



However the **Display View** resolution was too low to make our the ship name.

The highest resolution image was then exported from the Forensic Explorer case and uploaded to https://tineye.com/ Reverse Image Search.

Figure 18: TinEye Reverse Image lookup



From the TinEye results the following picture was identified: https://pixabay.com/photos/cruise-ship-dock-boats-yachts-6145828/ identifying the cruise ship as the **Crystal Serenity**.

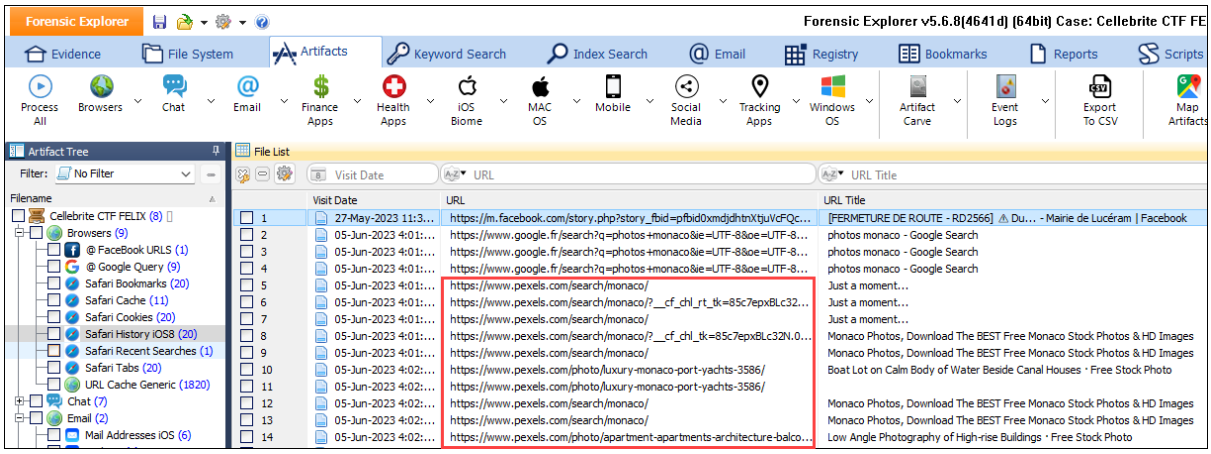
Figure 19: https://pixabay.com/photos/cruise-ship-dock-boats-yachts-6145828/

Alternate Method

The word '**researching'** in the questions suggests web browser activity. A search of **Artifacts > Browsers > Safari History** identified browsing activity at the site:

https://www.pexels.com/photo/luxury-monaco-port-yachts-3586/

Figure 20: Artifacts > Browsers > Safari History



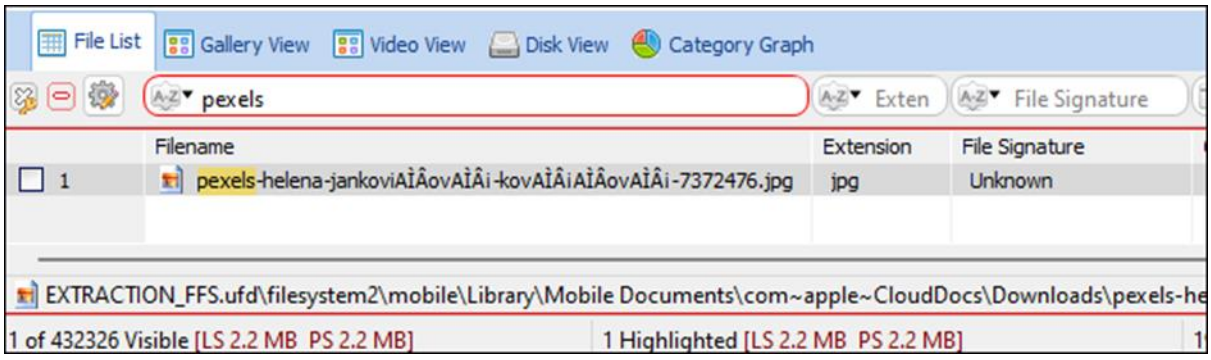
At https://www.pexels.com/photo/luxury-monaco-port-yachts-3586/ a high resolution version of the Crystal Serenity image was found.

https://www.pexels.com/photo/white-and-blue-cruise-ship-on-the-sea-7372476/

Figure 21: https://images.pexels.com/photos/7372476/pexels-photo-7372476.jpeg

A filename search for **pexels** located the following image in the **apple~CloudDocs\Downloads** folder:

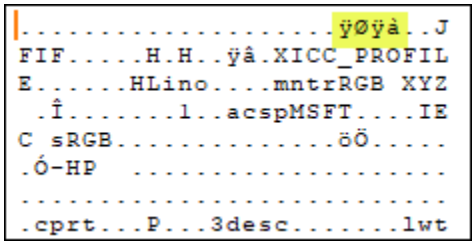
Figure 22: File System > Filename column filter for 'pexels'



This file has a **jpg** extension, but an **unknown** signature, and does not display in Forensic Explorer.

A HEX examination of the file shows that it has additional characters before the standard JPG header:

Figure 23: pexels-helena-.... file header



A **right-click > open** with programs including Snagit and Irfan view, shows it to be the high-resolution Crystal Serenity picture.

QUESTION 11 - DATA - LEVEL 3 (50 POINTS)

Which process on Felix's phone used the most cellular data (network traffic INTO the device)?

Q11. ANSWER

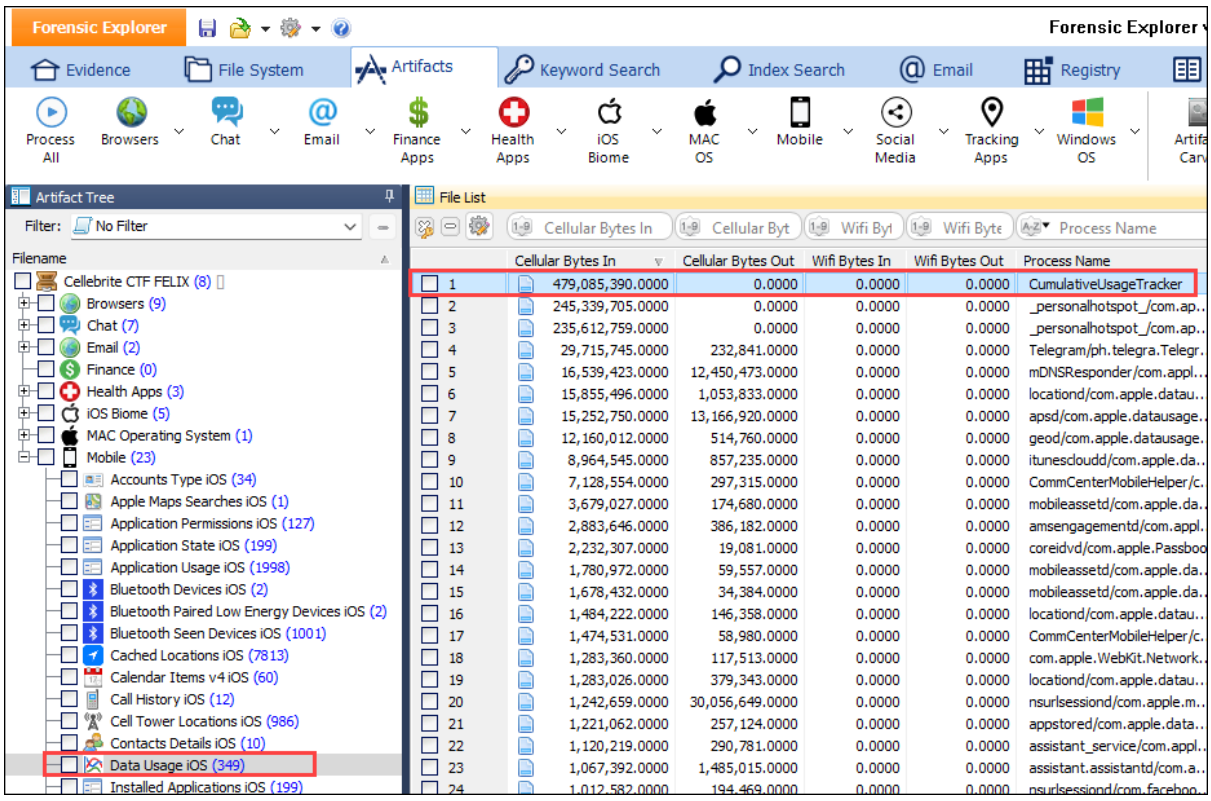
CumulaltiveUsageTracker.

Q11. FORENSIC EXPLORER METHODOLOGY

In the Artifacts module:

1. Select **Mobile** > **Data Usage iOS**.
2. Double click on the Cellular Bytes In column header to sort by size.
3. The process with the most bytes is **CumulaltiveUsageTracker**.

Figure 24: Artifacts > Mobile > Data Usage iOS



QUESTION 12 - H IS MEAN - LEVEL 3 (100 POINTS)

Felix was referred information about pension reform. What is the SID associated with that artifact?

Q12. ANSWER

c5141308-e98c-11ed-8f70-ea4e37ab9147

Q12. FORENSIC EXPLORER METHODOLOGY

This question is obscure. Please see the official Cellebrite solution on this page:

https://cellebrite.com/en/cellebrites-ctf-2023-recap-answers-for-felixs-iphone-device/