

**CELLEBRITE 2023**  
**CAPTURE THE FLAG (CTF)**  
**FELIX IPHONE**

CTF Questions Only ..... 2

About This CTF Challenge ..... 4

Starting this challenge in Forensic Explorer ..... 5

Question 1 - Voicemail - level 1 - (10 points) ..... 6

Question 2 - Picture - level 1 (10 points) ..... 7

Question 3 - Confirmation - level 1 (10 points) ..... 9

Question 4 - Photo (10 points) ..... 11

Question 5 - Location (10 points) ..... 12

Question 6a - Size - Level1 (10 points) ..... 14

Question 6b - Time - Level 2 (30 points) ..... 15

Question 7 - Size - Level 2 (30 points) ..... 16

Question 8 - Missing - Level 2 (30 points) ..... 17

Question 9 - Wiped - Level 2 (30 points) ..... 19

Question 10 - Cruise - Level 2 (30 points) ..... 20

Question 11 - Data - Level 3 (50 points) ..... 23

Question 12 - H is mean - Level 3 (100 points) ..... 24

**CTF QUESTIONS ONLY**

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

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

## 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:

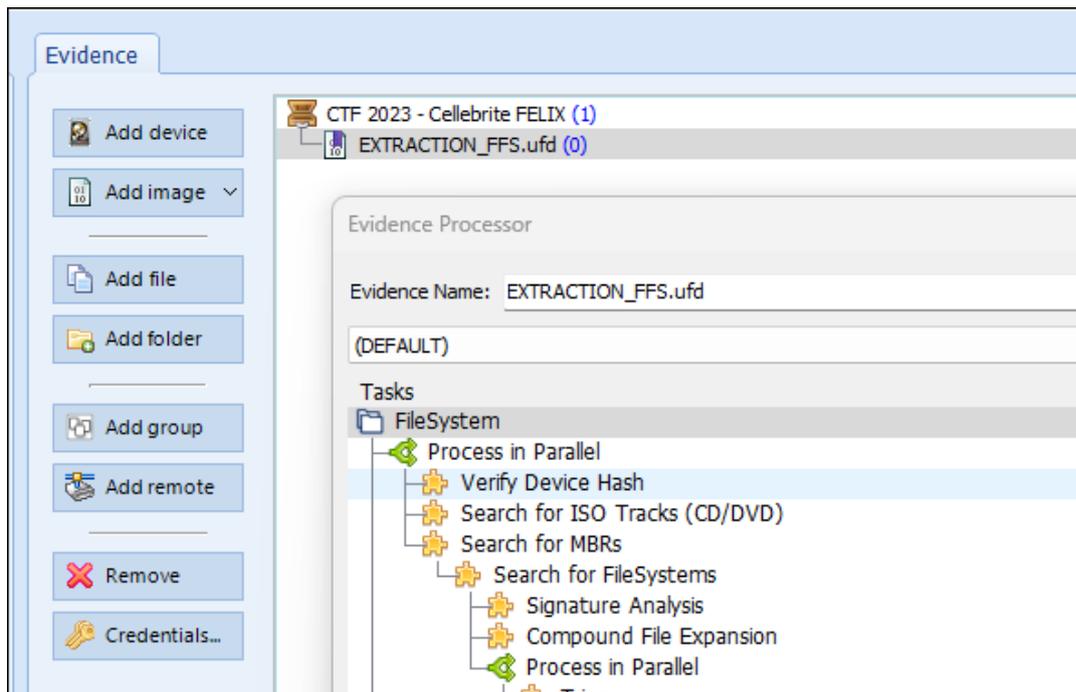
- <https://cellebrite.com/en/cellebrates-ctf-2023-recap-answers-for-felixs-iphone-device/>
- <https://www.stark4n6.com/2023/10/cellebrite-ctf-2023-felix.html>

## 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

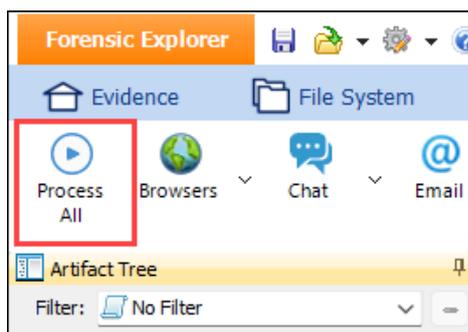


## ARTIFACTS > PROCESS ALL

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**

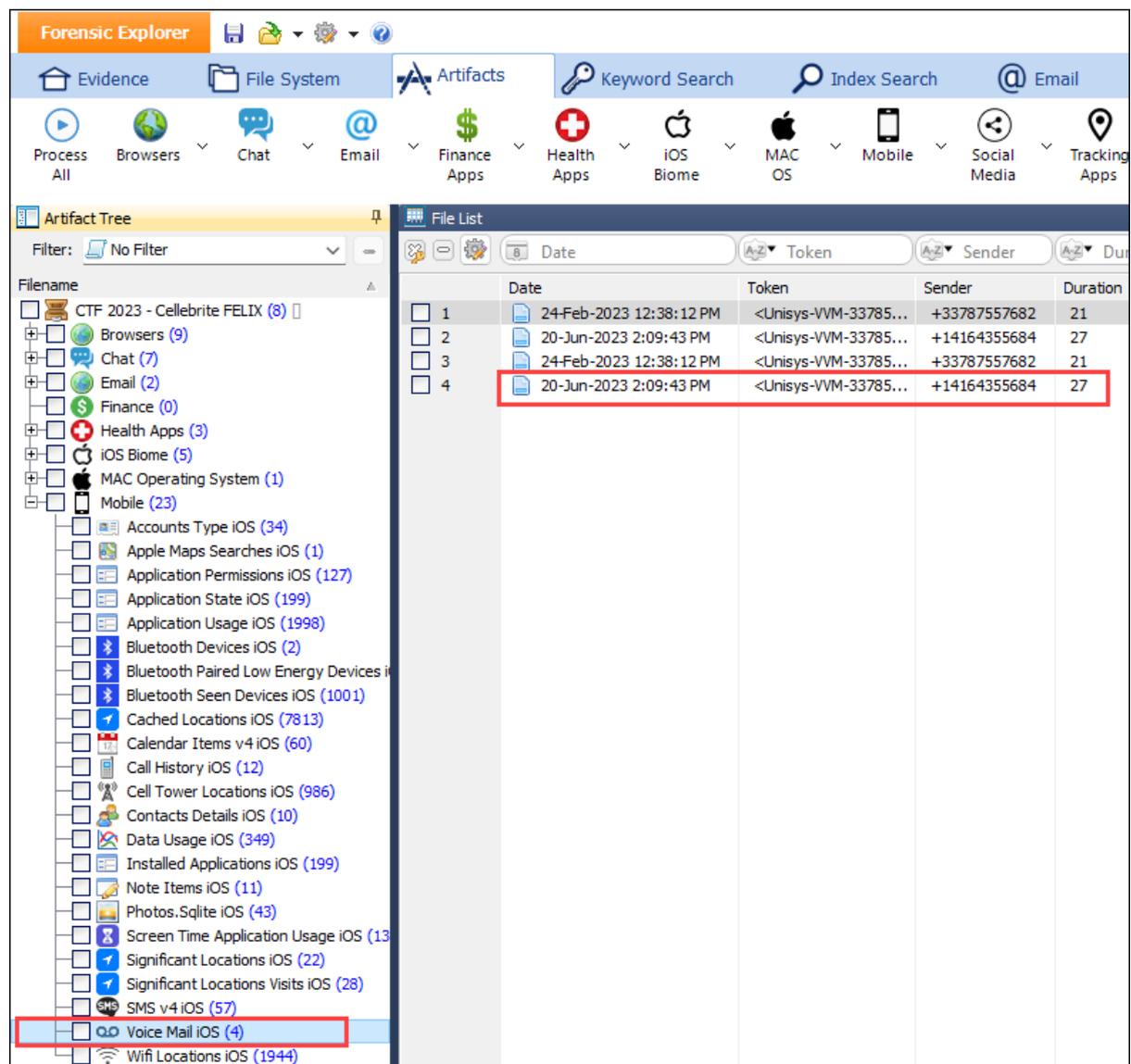
27 seconds.

**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**

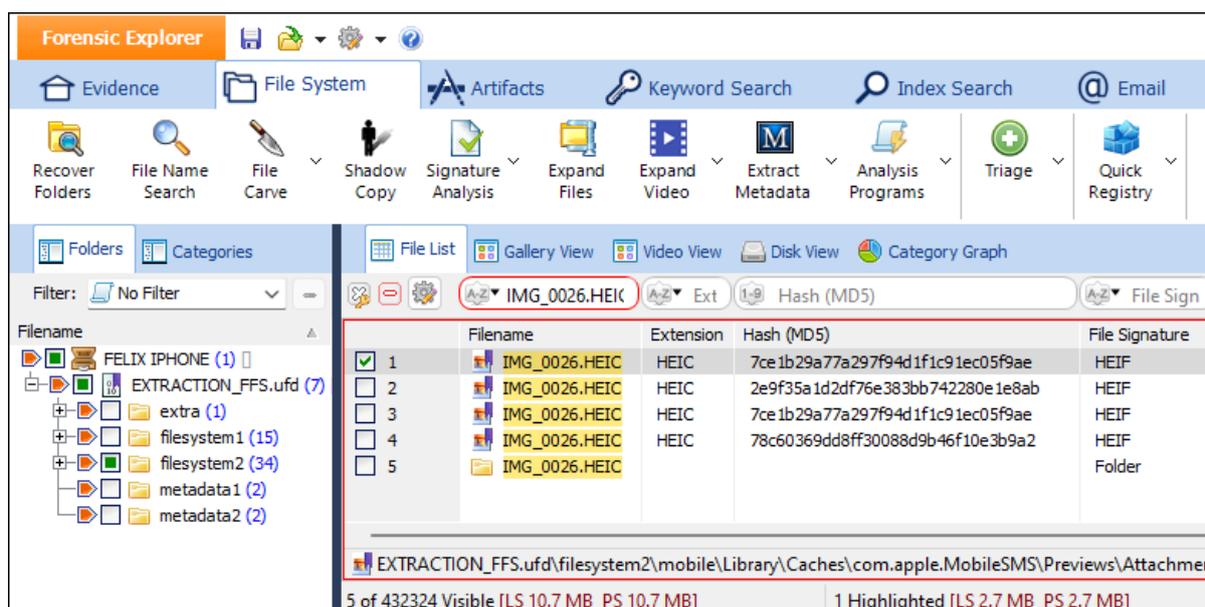
5 instances.

**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

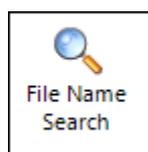
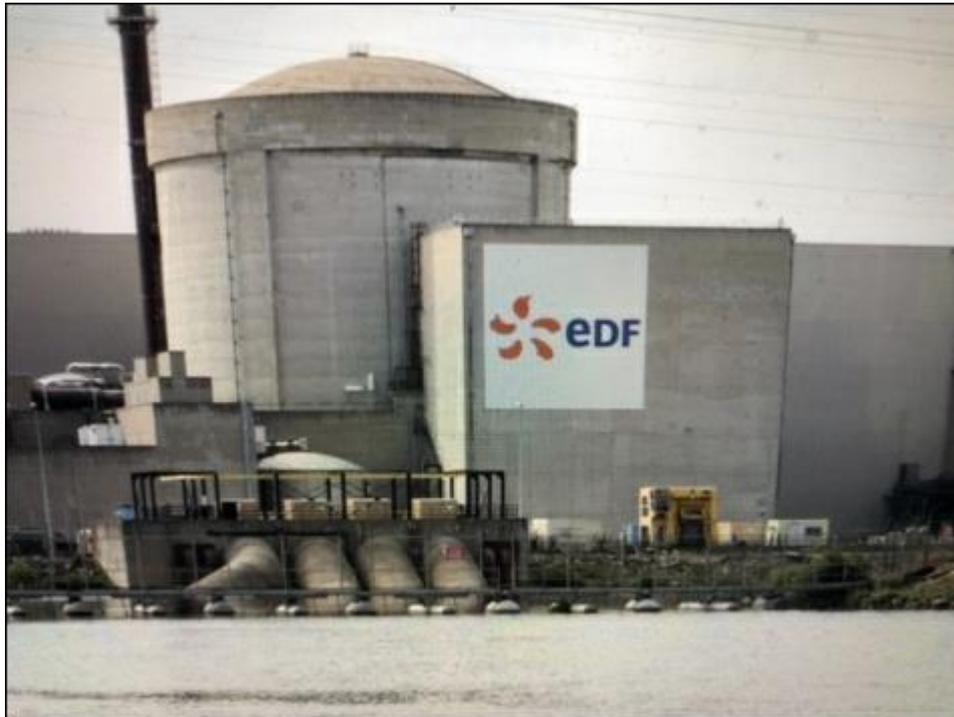


Figure 5: File Name Search result

```
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-8A14-41FFD406ED1\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



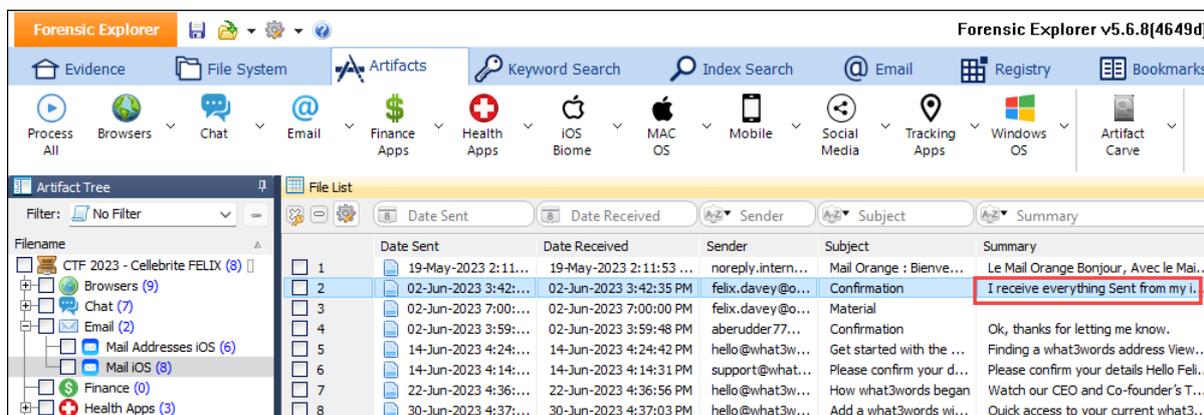
Figure 8: Artifacts > Search Artifact Results > output

```

Search Artifacts Results
-----
Keyword Count:                               1
-----
Artifacts Module:
Bates ID  RegEx Search Term                Folder                Match Text
-----
432545    everything                               Mail iOS              I receive everything Sent from my iPhone
-----
Match Summary:
RegEx Term                Hits
-----
everything                1
-----
Total Artifacts:                1
Search Artifacts Results finished.
-----
Search Artifacts Results finished.
    
```

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

Figure 9: Artifacts > Email > Mail iOS

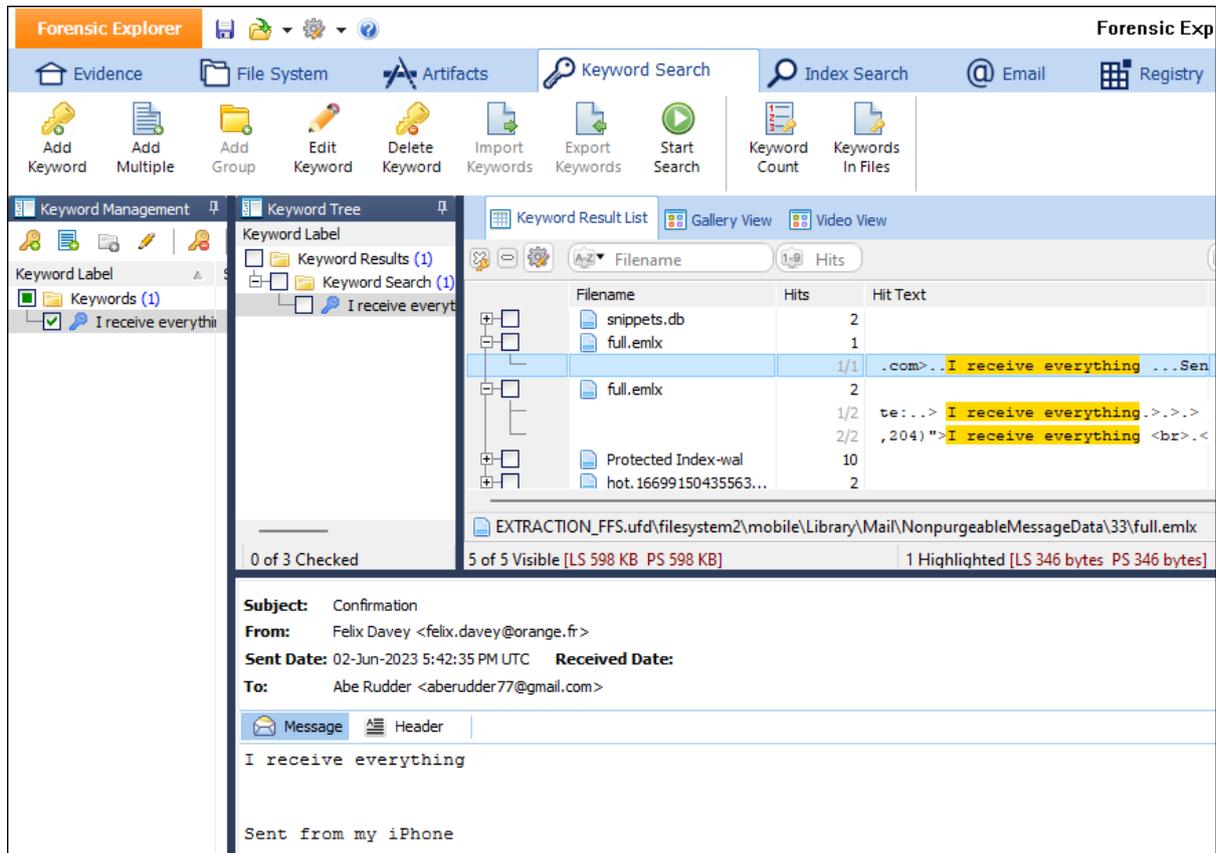


As a follow-up search, In the **Keyword Search** module:

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 screenshot shows the Keyword Search module interface with a search for 'New Jersey'. The results table is as follows:

Filename	Hits	Hit Text	Hit Offset (File)
MapsSync_0.0.1	12		
	1/12	ateszz..United States..US..New Jersey".NJ*.Bergen County2.Closte	66945
	2/12	ted States..United States..New Jersey".New Jersey*.Bergen County	67127
	3/12	United States..New Jersey".New Jersey*.Bergen County2.ClosterB.G	67139
	4/12	.)Address Å. {s:s}Closter, New Jersey{/s:s}2...s...`...}...ÅA".	67452
	5/12	.)Address Å. {s:s}Closter, New Jersey{/s:s}2...s...`...}i..Ü..ÅA".	538694
	6/12	ateszz..United States..US..New Jersey".NJ*.Bergen County2.Closte	539781
	7/12	ted States..United States..New Jersey".New Jersey*.Bergen County	539963
	8/12	United States..New Jersey".New Jersey*.Bergen County2.ClosterB.G	539975
	9/12	ateszz..United States..US..New Jersey".NJ*.Bergen County2.Closte	546460
	10/12	ted States..United States..New Jersey".New Jersey*.Bergen County	546642
	11/12	United States..New Jersey".New Jersey*.Bergen County2.ClosterB.G	546654
	12/12	.)Address Å. {s:s}Closter, New Jersey{/s:s}2...s...`...}...ÅA".	546967
MapsSync_0.0.1-wal	4		

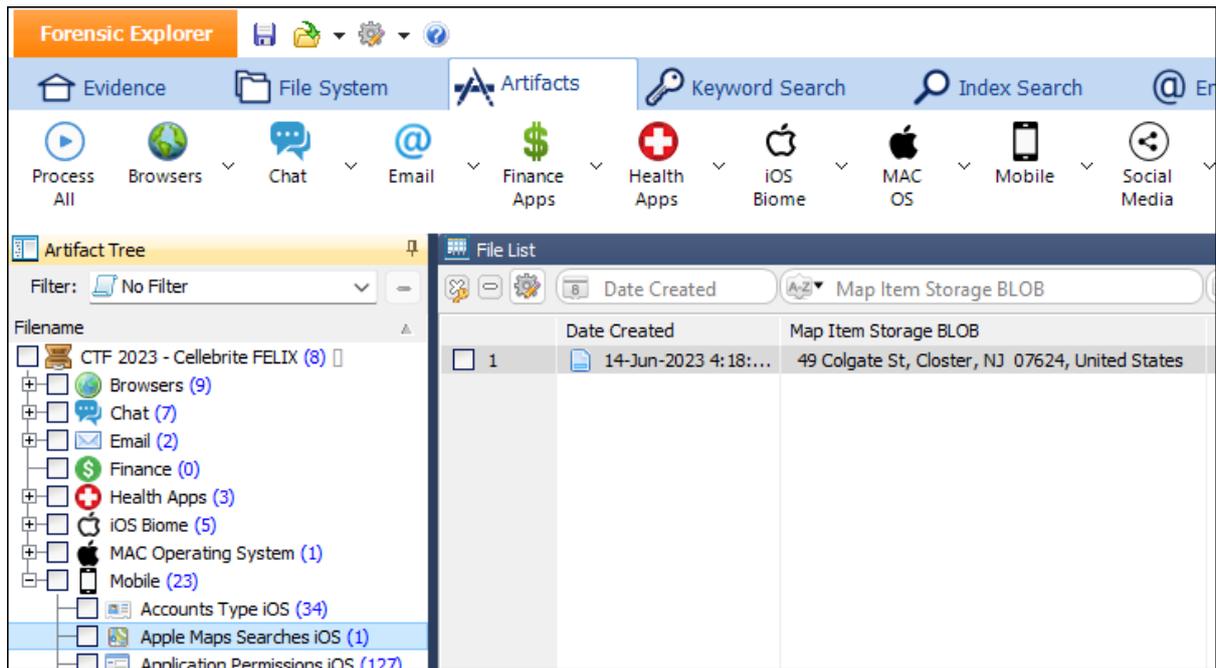
The search result identifies **MapsSync\_0.0.1** (a known Apple Maps file) as a potential source.

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**

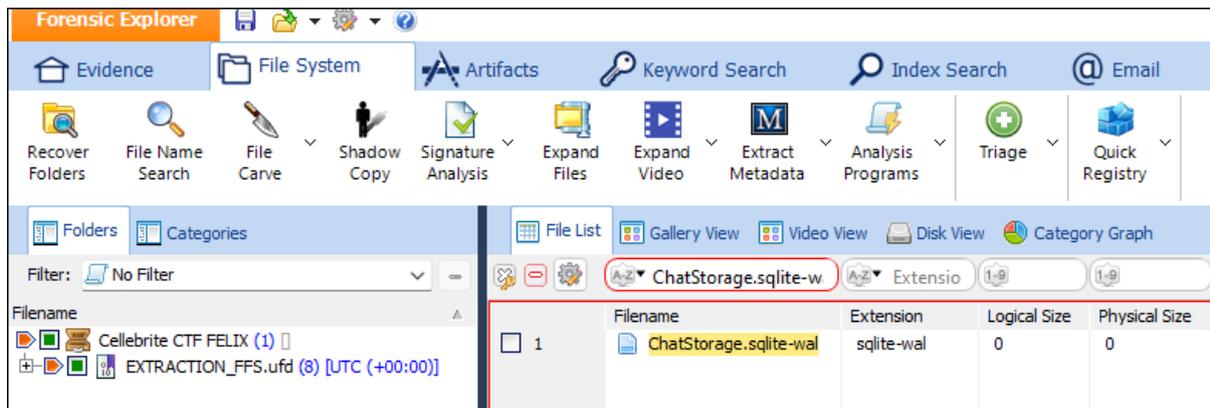
0 bytes.

**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**

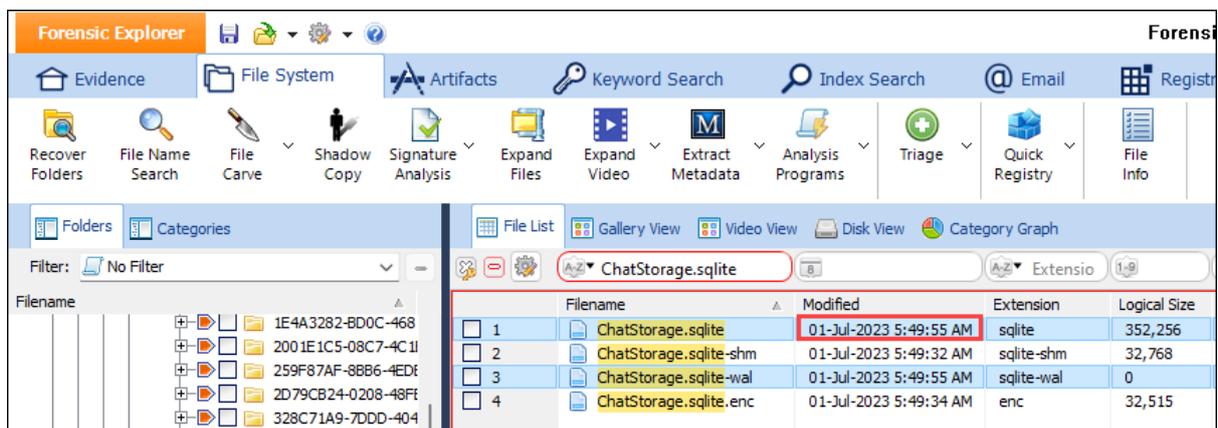
2023-07-01 05:49:55.

**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.

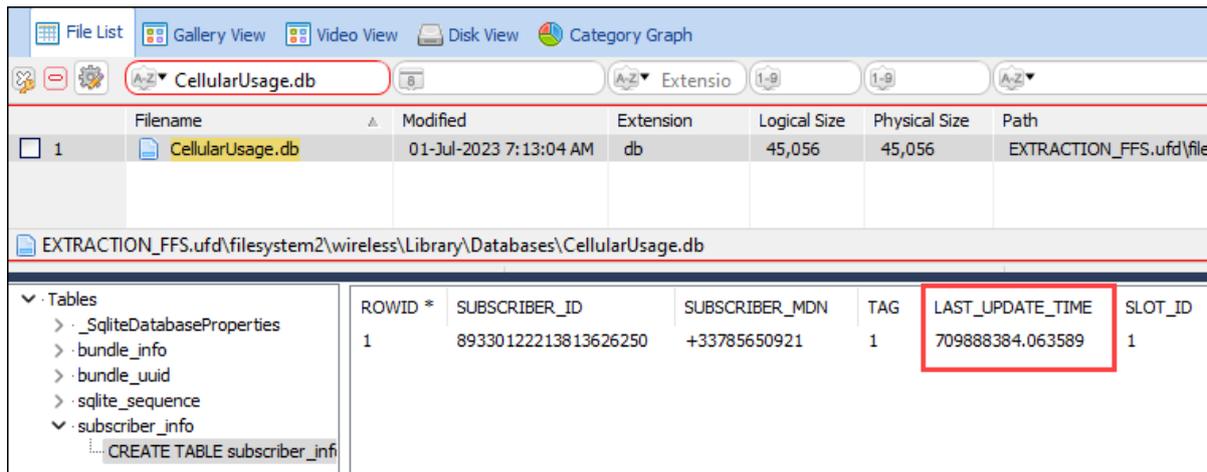
**QUESTION 7 - SIZE - LEVEL 2 (30 POINTS)**

*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?*

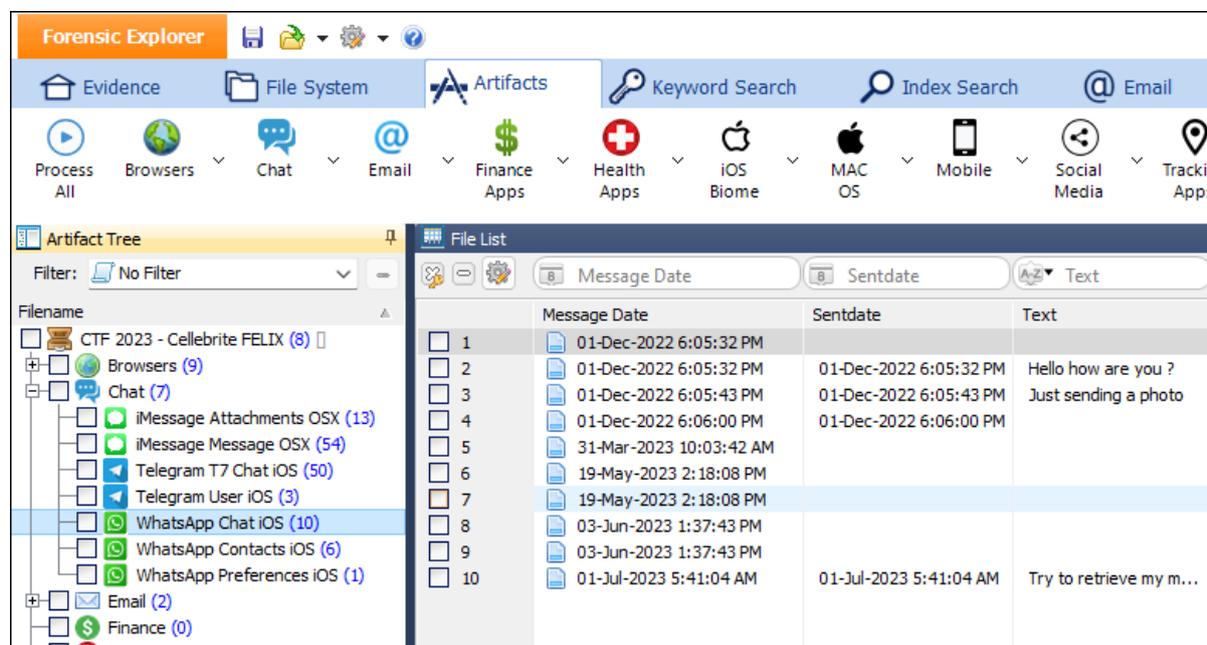
**Q8. ANSWER**

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 ZWMESSAGE table

The screenshot shows a file explorer interface with the following elements:

- Navigation tabs: File List, Gallery View, Video View, Disk View, Category Graph.
- File name: ChatStorage.sqlite (highlighted with a red box).
- File Signature: WhatsApp iOS.
- Table list (expanded):
 

Filename	Extension	File Signature
1 ChatStorage.sqlite	sqlite	WhatsApp iOS
2 ChatStorage.sqlite-shm	sqlite-...	SQLite SHM
3 ChatStorage.sqlite-wal	sqlite-wal	No size
4 ChatStorage.sqlite.enc	enc	Unknown
- Database table list (expanded):
 

Table Name	Z_PK *	Z_ENT	Z_OPT	ZCHILD...	ZCHILD...	ZC...
> ZWABLACKLISTITEM						
> ZWACHATPROPERTIES	1	9	3	0	0	0
> ZWACHATPUSHCONFIG	2	9	7	0	0	0
> ZWACHATSESSION	3	9	7	0	0	0
> ZWAGROUPINFO	4	9	11	0	0	0
> ZWAGROUPMEMBER	10	9	2	0	0	0
> ZWAGROUPMEMBERSCHANGE	11	9	2	0	0	0
> ZWAMEDIAITEM	12	9	4	0	0	0
▼ ZWMESSAGE	20	9	2	0	0	0
... CREATE TABLE ZWMESSAGE ( Z_PK IN	21	9	5	0	0	0
> ZWMESSAGEDATAITEM	29	9	5	0	0	0
> ZWMESSAGEINFO						
> ZWAPROFILEPICTUREITEM						
> ZWAPROFILEPUSHNAME						
> ZWAVCARDMENTION						
> ZWAZIPAYMENTTRANSACTION						
> Z_METADATA						
> Z_MODELCACHE						
> Z_PRIMARYKEY						

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**

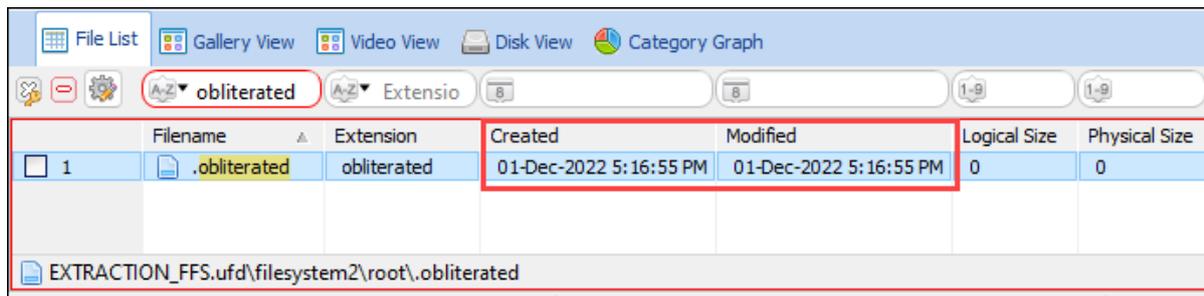
A common file that is used to identify an iOS device wipe is **root\obfuscated** (see: <https://dfir.pubpub.org/pub/6i7d593n/release/1>). This is a zero-byte file created by the device upon booting after a wipe.

To search for **.obfuscated**:

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

The filter identified a **.obfuscated** 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?*

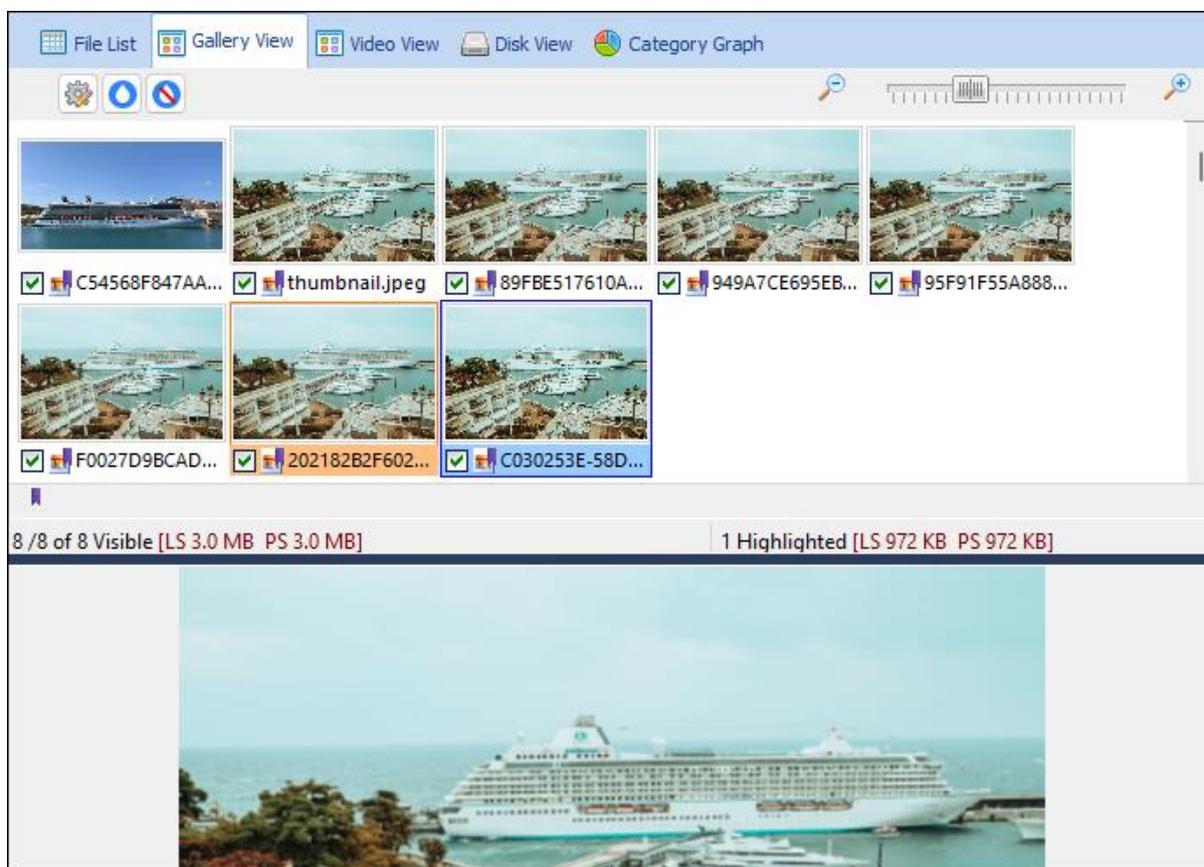
**Q10. ANSWER**

**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.

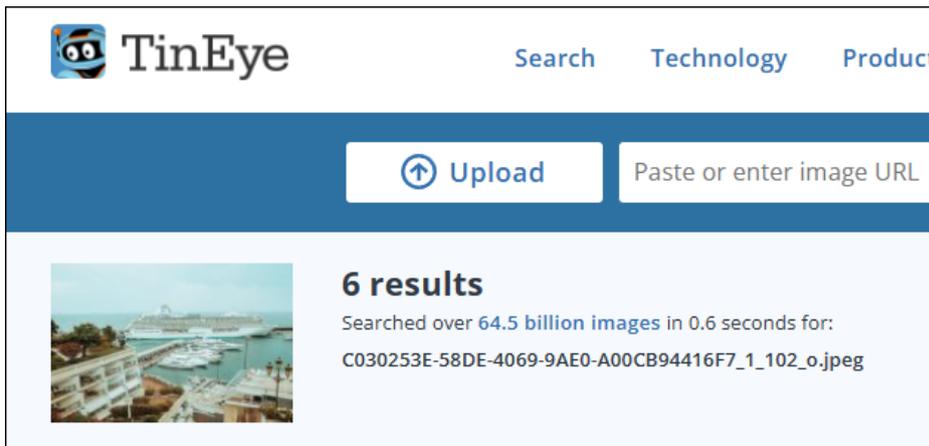
The following ship photos were located:



However the **Display View** resolution was too low to make out 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/>

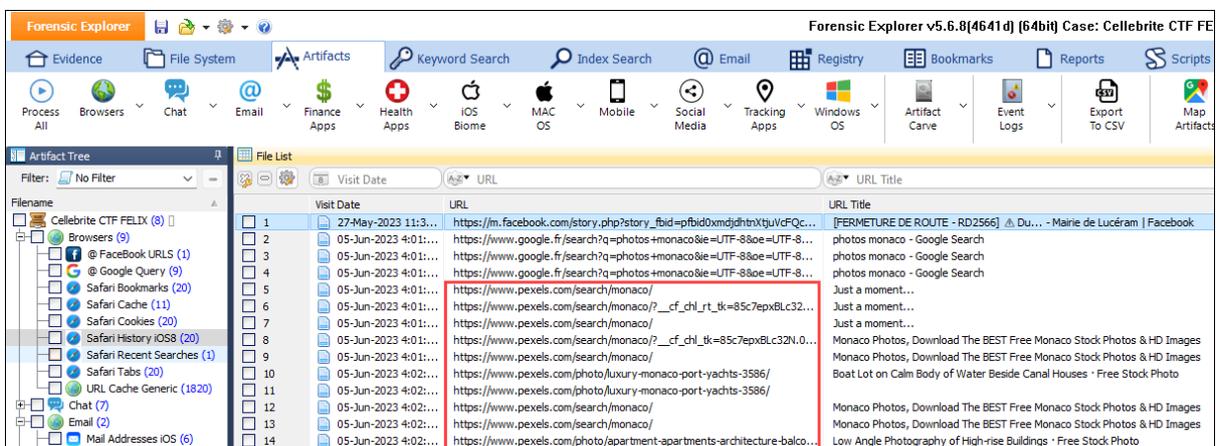


### Alternate Method

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.

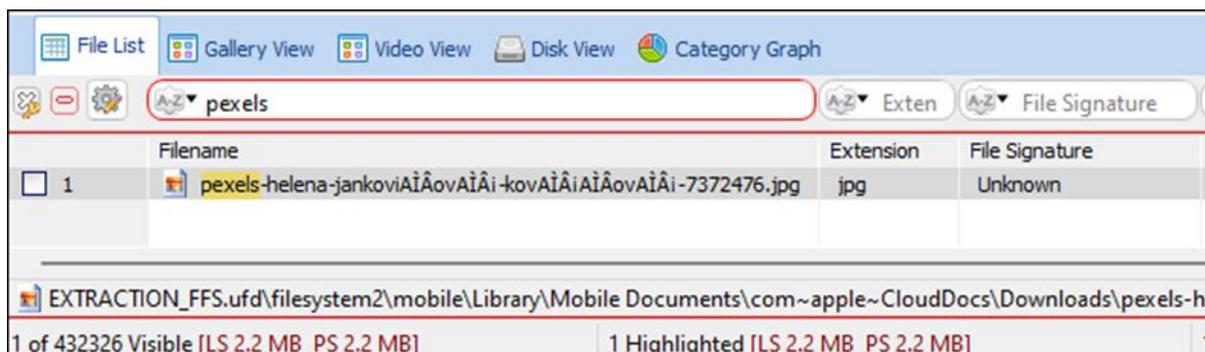
<https://www.pexels.com/photo/white-and-blue-cruise-ship-on-the-sea-7372476/>

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:

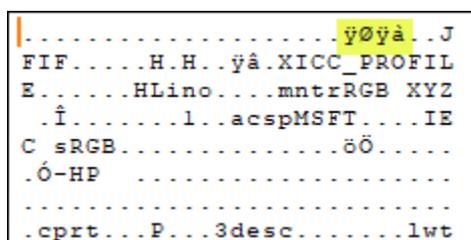
Figure 22: File System > Filename column filter for 'pexels'



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

	Cellular Bytes In	Cellular Bytes Out	Wifi Bytes In	Wifi Bytes Out	Process Name
1	479,085,390.0000	0.0000	0.0000	0.0000	CumulativeUsageTracker
2	245,339,705.0000	0.0000	0.0000	0.0000	_personalhotspot_/com.ap...
3	235,612,759.0000	0.0000	0.0000	0.0000	_personalhotspot_/com.ap...
4	29,715,745.0000	232,841.0000	0.0000	0.0000	Telegram/ph.telegra.Telegr...
5	16,539,423.0000	12,450,473.0000	0.0000	0.0000	mDNSResponder/com.appl...
6	15,855,496.0000	1,053,833.0000	0.0000	0.0000	locationd/com.apple.datau...
7	15,252,750.0000	13,166,920.0000	0.0000	0.0000	apsd/com.apple.datausage...
8	12,160,012.0000	514,760.0000	0.0000	0.0000	geod/com.apple.datausage...
9	8,964,545.0000	857,235.0000	0.0000	0.0000	itunescloud/com.apple.da...
10	7,128,554.0000	297,315.0000	0.0000	0.0000	CommCenterMobileHelper/c...
11	3,679,027.0000	174,680.0000	0.0000	0.0000	mobileassetd/com.apple.da...
12	2,883,646.0000	386,182.0000	0.0000	0.0000	amsengagementd/com.appl...
13	2,232,307.0000	19,081.0000	0.0000	0.0000	coreidvd/com.apple.Passbo...
14	1,780,972.0000	59,557.0000	0.0000	0.0000	mobileassetd/com.apple.da...
15	1,678,432.0000	34,384.0000	0.0000	0.0000	mobileassetd/com.apple.da...
16	1,484,222.0000	146,358.0000	0.0000	0.0000	locationd/com.apple.datau...
17	1,474,531.0000	58,980.0000	0.0000	0.0000	CommCenterMobileHelper/c...
18	1,283,360.0000	117,513.0000	0.0000	0.0000	com.apple.WebKit.Network...
19	1,283,026.0000	379,343.0000	0.0000	0.0000	locationd/com.apple.datau...
20	1,242,659.0000	30,056,649.0000	0.0000	0.0000	nsurlsessiond/com.apple.m...
21	1,221,062.0000	257,124.0000	0.0000	0.0000	appstored/com.apple.data...
22	1,120,219.0000	290,781.0000	0.0000	0.0000	assistant_service/com.appl...
23	1,067,392.0000	1,485,015.0000	0.0000	0.0000	assistant.assistantd/com.a...
24	1,012,582.0000	194,469.0000	0.0000	0.0000	nsurlsessiond/com.faceboo...

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/>