CELLEBRITE 2023

CAPTURE THE FLAG (CTF)
ABE IPHONE

CTF QUESTIONS ONLY

1	iCloud - Level 1 ***Abe used a unique email address for his iCloud account. What is that email address?***	10
2	Comm App - Level 1 ***Abe used different types of communication channels, through different applications. What communication application was used the most?***	10
3	Wallet - Level 1 ***A payment card was used on Abe's device - Wallet. What are the last 4 digits of that card?***	10
4	iCloud Backup - Level 1 ***Abe's phone was setup using iCloudBackup method. What is the Date & Time for that (UTC+0 time)?***	10
5	Tracking - Level 1 ***Abe was suspicious about being tracked. After searching the rental vehicle he was using while in NJ, he found a device attached to his vehicle, what was the make/model (need to refine)?***	10
6	Steps - Level 2 ***Abe was not really active on 6/24/2023 local time. How many steps were recorded?***	30
7	BlueTooth - Level 2 ***Abe pairs his iPhone with few different Bluetooth devices. How many unique Bluetooth connections were paired?***	30

8	App Notification - Level 2 ***Abe got notified by Harold of a potential arrest, Abe then opened which app?***	30
9	Parked - Level 2 ***Abe went to a party at RAIN Event Space. What is the name of the street (just the street name) where he parked his vehicle?***	30
10	About - Level 2 ***What was Abe Rudder's About bio on WhatsApp?***	30
11	Permissions - Level 2 ***Abe is paranoid and not always giving access to everything. One of the apps Abe used on the iPhone received access to Photos however as an "Add Photos Only" permission. What is the name of the app (one word i.e.: Starbucks)?***	30
12	Email - Level 3 ***Abe used a specific method to find/check/share locations via an app. In order to keep privacy up, Abe signed up with a different email address which keeps it isolated to that vendor. What is that email address?***	50
13	Search - Level 3 ***Abe got suspicious when he had to deal with some shady people almost as if a crime was known to be committed and wanted to leave no traces. Abe wanted to create an anonymous email. Where did Abe search for that? (3 words)?***	50
14	Navigation - Level 3 ***Abe was navigating while driving, on June 26, 2023. What was the destination address on the navigation?***	50

15	Crypto - Level 2 ***Abe used MOB to send/receive crypto within Signal. Can you find the Recovery Phrase for Signal Mobile Coin wallet? What is it? (24 words)?***	30
16	Picture - Level 2 ***Abe loves taking pictures and videos on the iPhone, the problem is when Abe is trying to look for a picture, he is having hard time finding it therefore he utilizes the Search within the Apple Photos app. If Abe would have looked for a picture of: Myself, Pawel, and Hat he would end up with one photo. Can you name that filename?***	30
17	Location - Level 2 ***Abe went for some shady meeting on an island but tried to conceal as a vacation so he took a boat tour and tracked dolphins. He then decided to mark a location with "dolphins". What was the timestamp for that location? [HH:MM:SS] written in UTC time"?***	30
18	BokerTov ***Within the last month before Abe got arrested (and his device was extracted), Abe used to wake up naturally however, there was one day the phone did. What was the day and (local) time? [YYYY-MM-DD HH:MM:SS] e.g: 2021-09-19 08:35:00?Within the last month before Abe got arrested (and his device was extracted), Abe used to wake up naturally however, there was one day the phone did. What was the day and (local) time? [YYYY-MM-DD HH:MM:SS] e.g: 2021-09-19 08:35:00?Within the last month before Abe got arrested (and his device was extracted), Abe used to wake up naturally however, there was one day the phone did. What was the day and (local) time? [YYYY-MM-DD HH:MM:SS] e.g: 2021-09-19 08:35:00?***	100

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 (24gb):
https://drive.google.com/file/d/1dn5IRU1Sa3A9NokW5v5HhJsiRud3tYHa/view

OTHER ONLINE CELLEBRITE 2023 ABE SOLUTIONS

The following other solutions can be found online:

- https://cellebrite.com/en/cellebrites-ctf-2023-recap-answers-on-abes-iphone/
- https://www.stark4n6.com/2023/10/cellebrite-ctf-2023-abe.html
- https://forensafe.com/blogs/challenges/CellebriteCtfAbe.html

OTHER FORENSIC EXPLORER CTF WALKTHROUGHS

Other Forensic Explorer Capture the Flag walkthroughs are located on this page:
https://getdataforensics.com/capture-the-flag/

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**

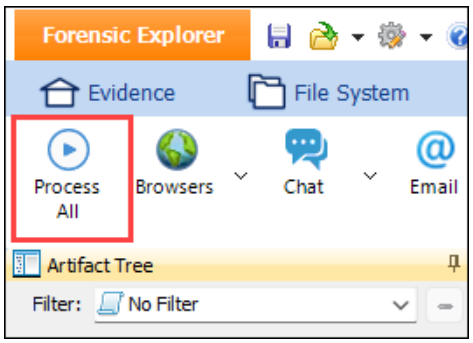
In the **Evidence Processor** window use the default options.

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 1: Artifacts > Process All



QUESTION 1 - ICLOUD - LEVEL 1 (10 POINTS)

Abe used a unique email address for his iCloud account. What is that email address?

Q1. ANSWER

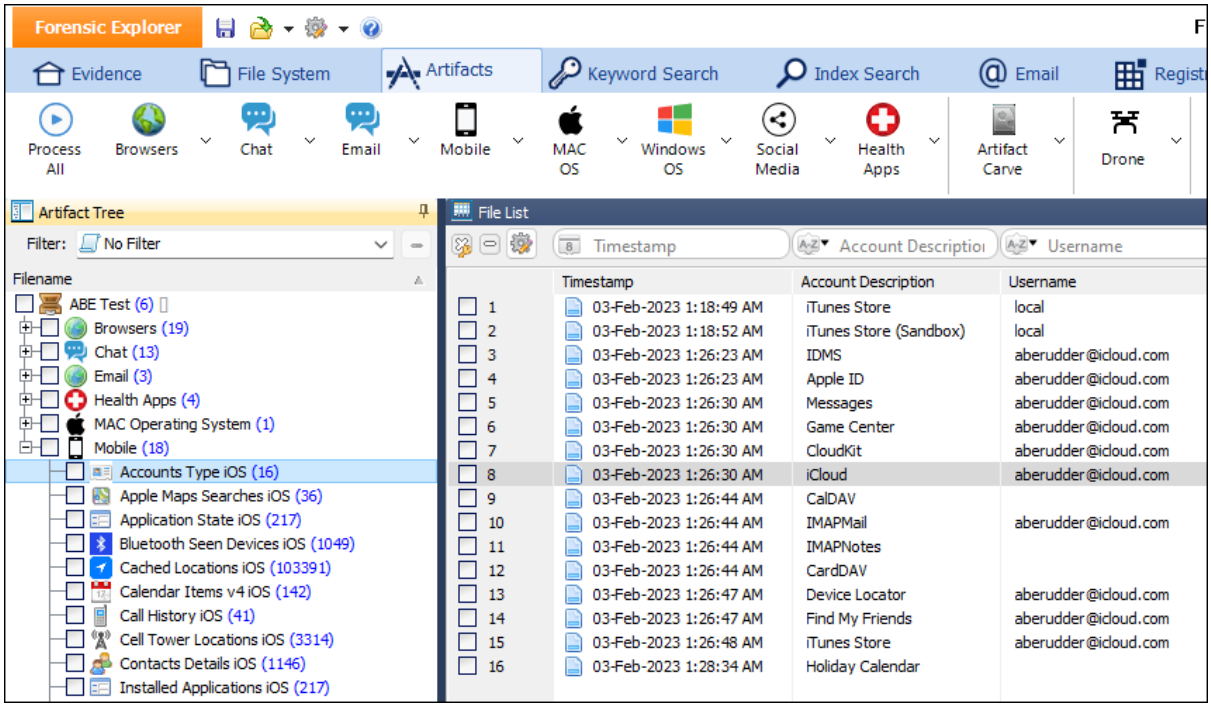
aberudder@icloud.com

Q1. FORENSIC EXPLORER METHODOLOGY

In the Forensic Explorer Artifacts module:

1. Select **Mobile > Accounts Type iOS**.
2. The **iCloud** account **Username** is listed as: **aberudder@icloud.com**.

Figure 2: Artifacts > Mobile > Account Types iOS



QUESTION 2 - COMM APP - LEVEL 1 (10 POINTS)

Abe used different types of communication channels, through different applications. What communication application was used the most?

Q2. ANSWER

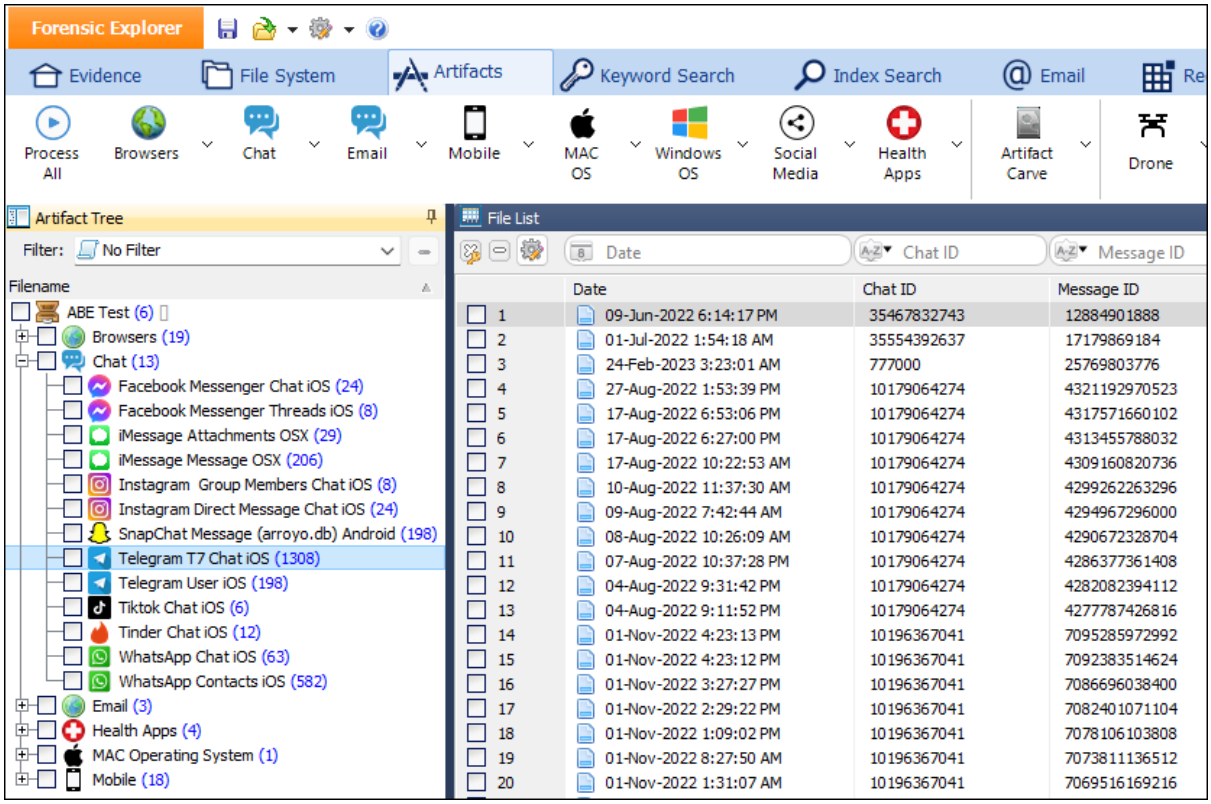
Telegram (1038 messages).

Q2. FORENSIC EXPLORER METHODOLOGY

In the Forensic Explorer **Artifacts module**:

1. Select **Chat**.
2. **Telegram T7 Chat IOS** has the most chat messages.

Figure 3: Artifacts > Chat > Telegram T7 Chat iOS



QUESTION 3 - WALLET - LEVEL 1 (10 POINTS)

A payment card was used on Abe's device - Wallet. What are the last 4 digits of that card?

Q3. ANSWER

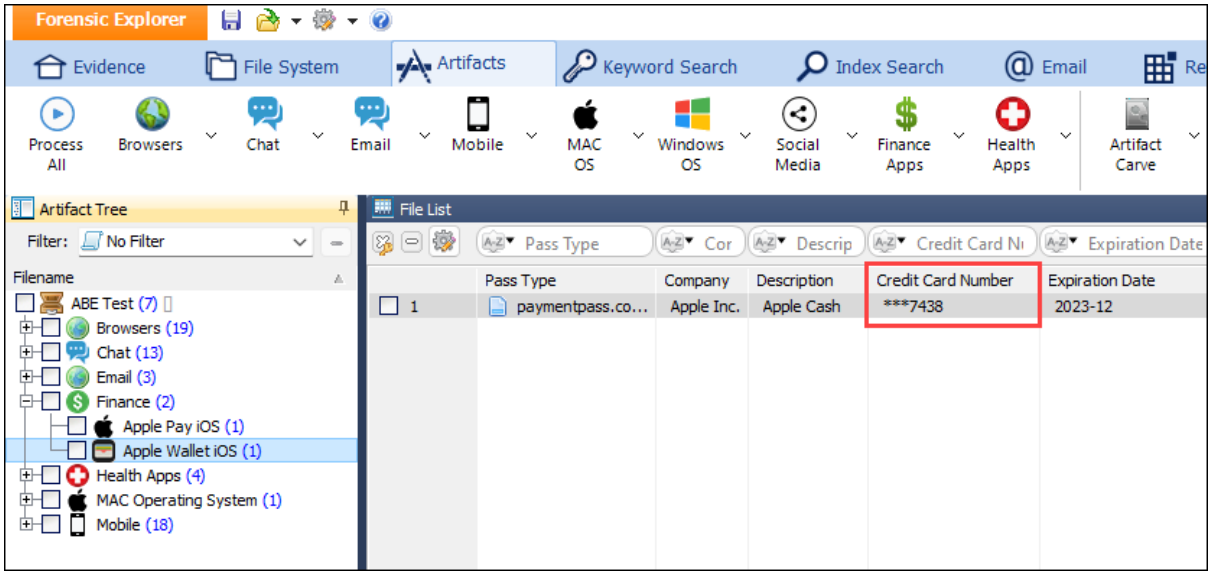
7438.

Q3. FORENSIC EXPLORER METHODOLOGY

In the Forensic Explorer **Artifacts module**:

1. Select **Finance** > **Apple Wallet**.
2. The last 4 digits of the **Credit Card Number** are listed as **7438**.

Figure 4: Artifacts > Finance > apple Wallet iOS



QUESTION 4 - ICLOUD BACKUP - LEVEL 1 (10 POINTS)

Abe's phone was setup using iCloudBackup method. What is the Date & Time for that (UTC+0 time)?

Q4. ANSWER

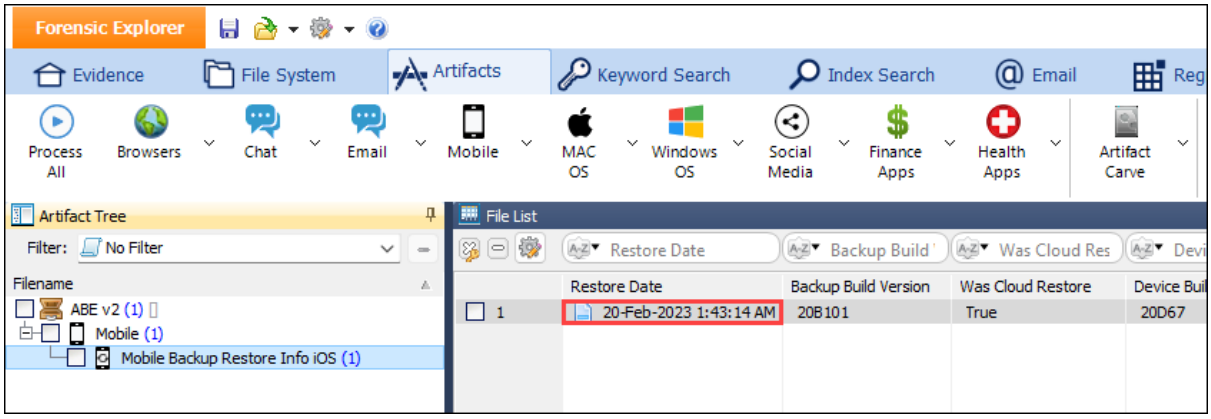
20-Feb-2023 1:43:14 AM.

Q4. FORENSIC EXPLORER METHODOLOGY

In the Forensic Explorer **Artifacts module**:

1. Select **Mobile** > **Mobile Backup Restore Info iOS**.
2. The **Restore Date** is listed as **20-Feb-2023 1:43:14 AM**.

Figure 5: Artifacts > Mobile > Mobile Backup Restore Info iOS



QUESTION 5 - TRACKING - LEVEL 1 (10 POINTS)

Abe was suspicious about being tracked. After searching the rental vehicle he was using while in NJ, he found a device attached to his vehicle, what was the make/model (need to refine)?

Q5. ANSWER

Geotab go9 lte or Geotab go9

Q5. FORENSIC EXPLORER METHODOLOGY

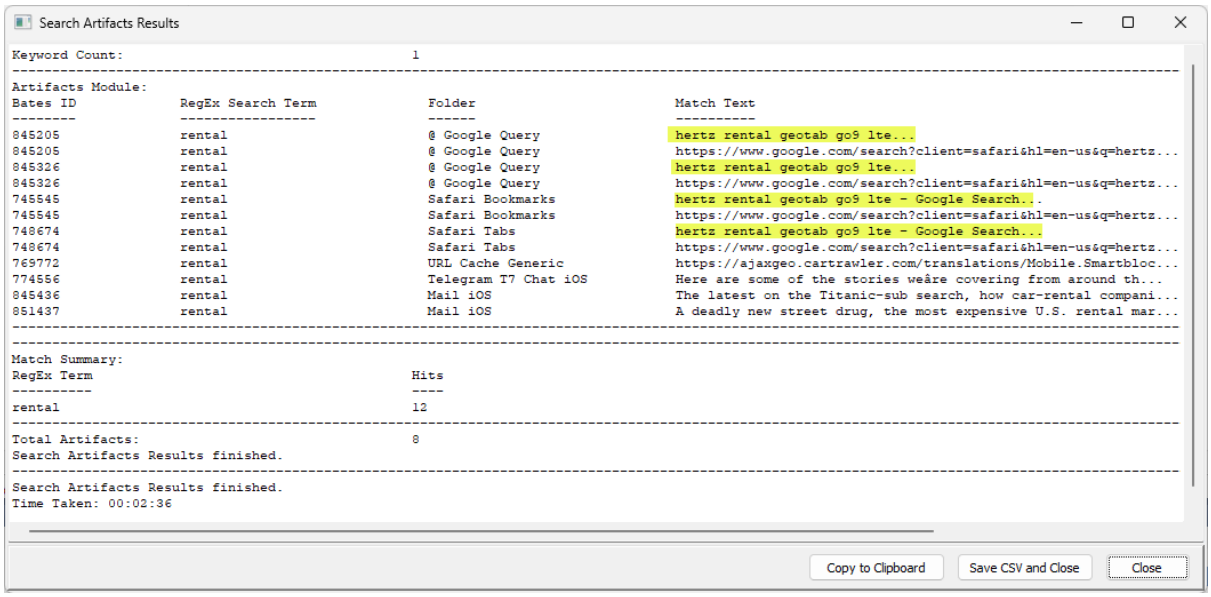
In the Forensic Explorer **Artifacts module**:

1. Use the **Search Artifact Results** toolbar button to search for **rental**.

Figure 6: Search Artifact Results

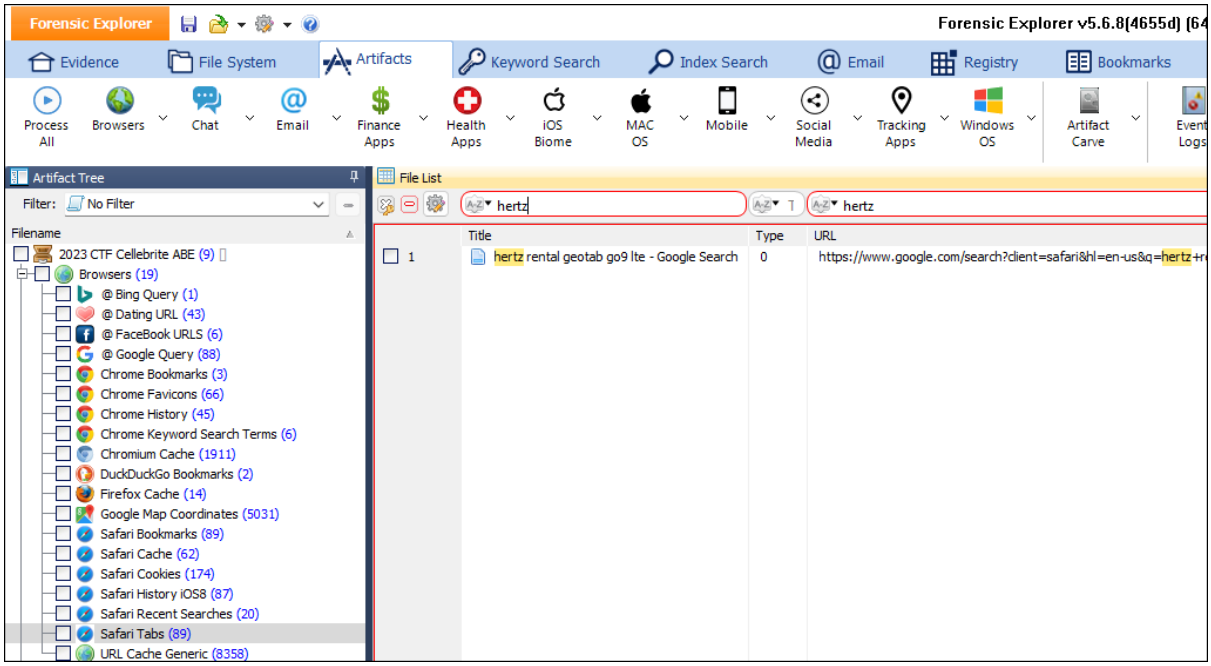
2. Search activity indicates that the **Safari Browser** was used to research **hertz rental**.

Figure 7: Search Artifact Results output



Safari Tabs shows a search activity relating to **Geotab go9 lte** and **Geotab go9**.

Figure 8: Artifacts > Browsers > Safari Tabs



QUESTION 6 - STEPS - LEVEL 2 (30 POINTS)

Abe was not really active on 6/24/2023 local time. How many steps were recorded?

Q6. ANSWER

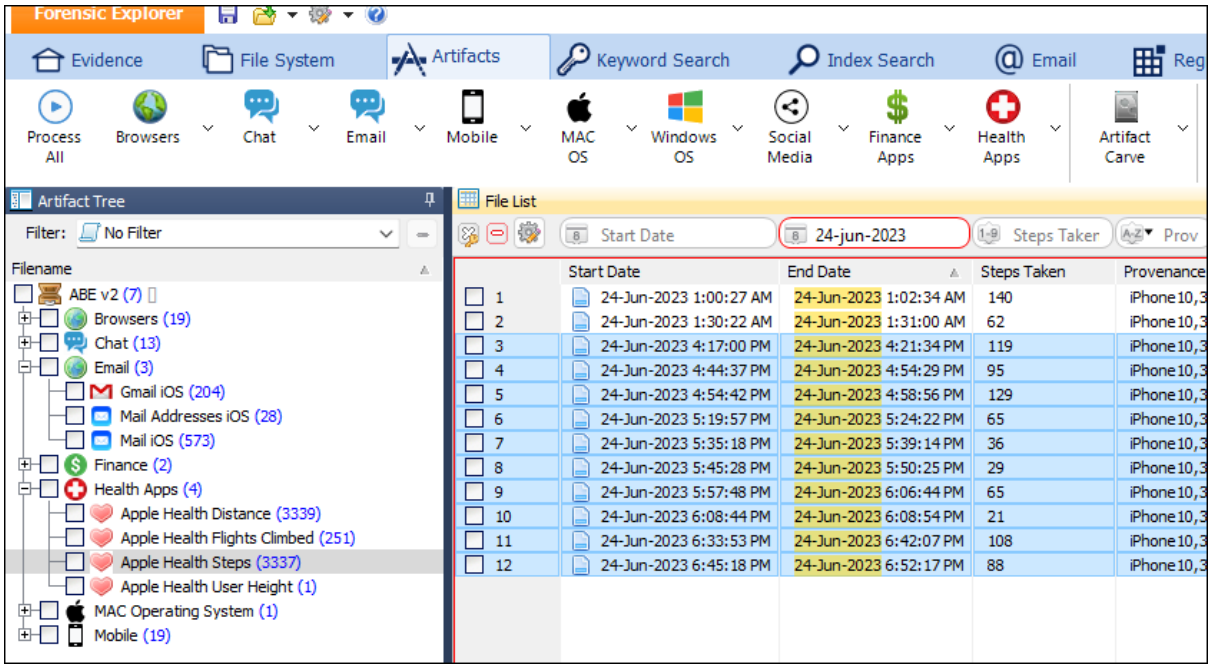
755.

Q6. FORENSIC EXPLORER METHODOLOGY

In the Forensic Explorer **Artifacts module**:

1. Select **Health Apps** > **Apple Health Steps**.
2. In the **End Date** column header, filter for **24 June 2023.**

Figure 9: Artifacts > Health Apps > Apple Health Steps



119
95
129
65
36
29
65
21
108
88
755

Note that **local time is requested**, so the displayed UTC dates must be adjusted.

The sum of steps on **24 June 2023** is **755**.

QUESTION 7 - BLUETOOTH - LEVEL 2 (30 POINTS)

Abe pairs his iPhone with few different Bluetooth devices. How many unique Bluetooth connections were paired?

Q7. ANSWER

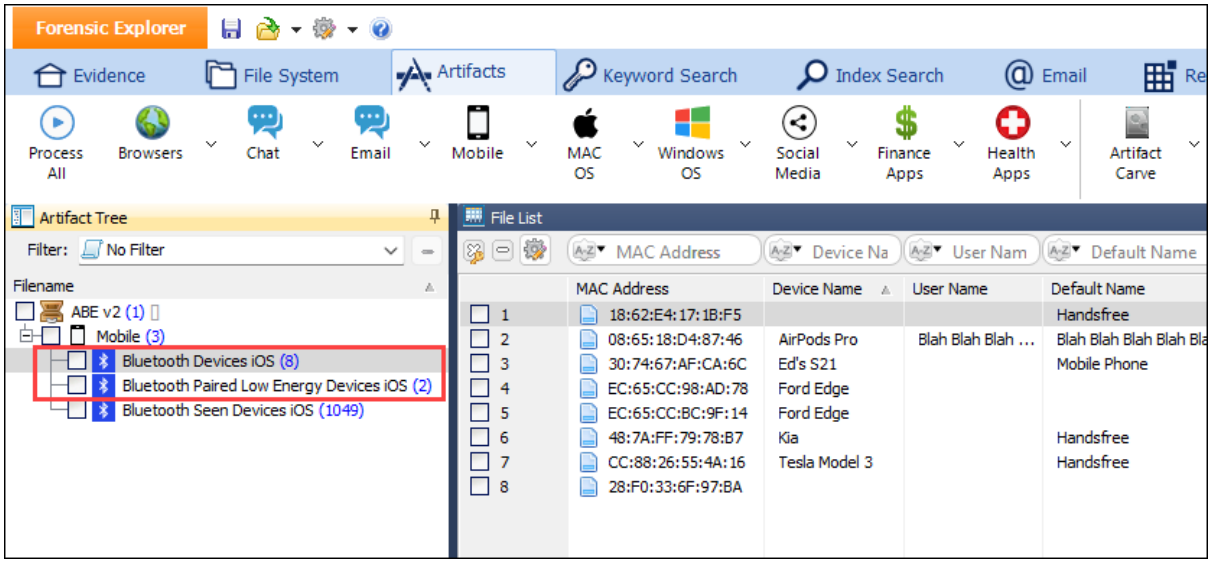
10.

Q7. FORENSIC EXPLORER METHODOLOGY

In the Forensic Explorer **Artifacts module**:

1. Examine results for **Mobile** > **Bluetooth Devices iOS** and **Bluetooth Paired Low Energy Devices iOS**.
2. The sum of these devices is **10**.

Figure 10: Artifacts > Mobile > Bluetooth



QUESTION 8 - APP NOTIFICATION - LEVEL 2 (30 POINTS)

Abe got notified by Harold of a potential arrest, Abe then opened which app?

Q8. ANSWER

Signal.

Q8. FORENSIC EXPLORER METHODOLOGY

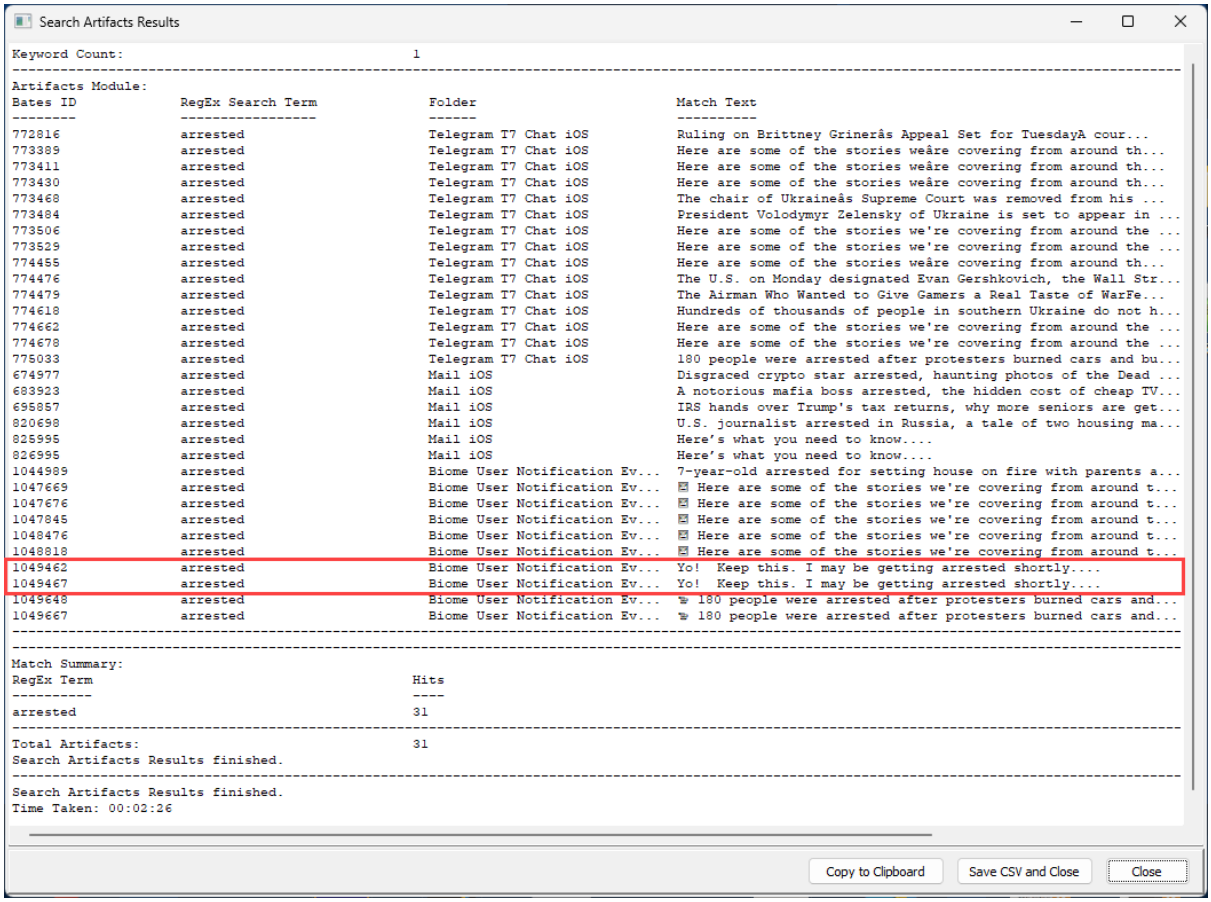
In the Forensic Explorer **Artifacts** module:

1. Use the **Search Artifact Results** toolbar button to search for **arrested**.

Figure 11: Artifacts > Search Artifact Results

2. The search results show hits in **Biome User Notification Events**.

Figure 12: Search Artifact Results



Search Artifacts Results

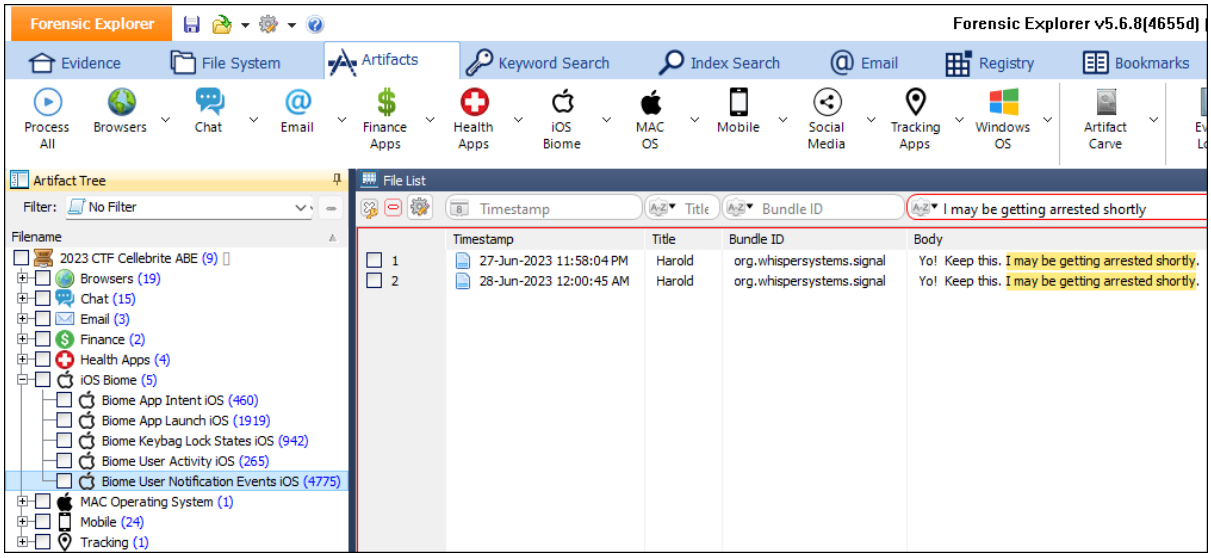
```
Keyword Count:                                  1
-------------------------------------------------------------------------------------------------------------------------------------------------------
Artifacts Module:
Bates ID            RegEx Search Term           Folder                          Match Text
--------            -----------------           ------                          ----------
772816              arrested                    Telegram T7 Chat iOS            Ruling on Brittney Grinerâs Appeal Set for TuesdayA cour...
773389              arrested                    Telegram T7 Chat iOS            Here are some of the stories weâre covering from around th...
773411              arrested                    Telegram T7 Chat iOS            Here are some of the stories weâre covering from around th...
773430              arrested                    Telegram T7 Chat iOS            Here are some of the stories weâre covering from around th...
773468              arrested                    Telegram T7 Chat iOS            The chair of Ukraineâs Supreme Court was removed from his ...
773484              arrested                    Telegram T7 Chat iOS            President Volodymyr Zelensky of Ukraine is set to appear in ...
773506              arrested                    Telegram T7 Chat iOS            Here are some of the stories we're covering from around the ...
773529              arrested                    Telegram T7 Chat iOS            Here are some of the stories we're covering from around the ...
774455              arrested                    Telegram T7 Chat iOS            Here are some of the stories weâre covering from around th...
774476              arrested                    Telegram T7 Chat iOS            The U.S. on Monday designated Evan Gershkovich, the Wall Str...
774479              arrested                    Telegram T7 Chat iOS            The Airman Who Wanted to Give Gamers a Real Taste of WarFe...
774618              arrested                    Telegram T7 Chat iOS            Hundreds of thousands of people in southern Ukraine do not h...
774662              arrested                    Telegram T7 Chat iOS            Here are some of the stories we're covering from around the ...
774678              arrested                    Telegram T7 Chat iOS            Here are some of the stories we're covering from around the ...
775033              arrested                    Telegram T7 Chat iOS            180 people were arrested after protesters burned cars and bu...
674977              arrested                    Mail iOS                        Disgraced crypto star arrested, haunting photos of the Dead ...
683923              arrested                    Mail iOS                        A notorious mafia boss arrested, the hidden cost of cheap TV...
695857              arrested                    Mail iOS                        IRS hands over Trump's tax returns, why more seniors are get...
820698              arrested                    Mail iOS                        U.S. journalist arrested in Russia, a tale of two housing ma...
825995              arrested                    Mail iOS                        Here's what you need to know....
826995              arrested                    Mail iOS                        Here's what you need to know....
1044989             arrested                    Biome User Notification Ev...   7-year-old arrested for setting house on fire with parents a...
1047669             arrested                    Biome User Notification Ev...   Here are some of the stories we're covering from around t...
1047676             arrested                    Biome User Notification Ev...   Here are some of the stories we're covering from around t...
1047845             arrested                    Biome User Notification Ev...   Here are some of the stories we're covering from around t...
1048476             arrested                    Biome User Notification Ev...   Here are some of the stories we're covering from around t...
1048818             arrested                    Biome User Notification Ev...   Here are some of the stories we're covering from around t...
1049462             arrested                    Biome User Notification Ev...   Yo!  Keep this. I may be getting arrested shortly....
1049467             arrested                    Biome User Notification Ev...   Yo!  Keep this. I may be getting arrested shortly....
1049648             arrested                    Biome User Notification Ev...   180 people were arrested after protesters burned cars and...
1049667             arrested                    Biome User Notification Ev...   180 people were arrested after protesters burned cars and...
-------------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------------------
Match Summary:
RegEx Term                                      Hits
----------                                      ----
arrested                                        31
-------------------------------------------------------------------------------------------------------------------------------------------------------
Total Artifacts:                                31
Search Artifacts Results finished.
-------------------------------------------------------------------------------------------------------------------------------------------------------
Search Artifacts Results finished.
Time Taken: 00:02:26
```

Copy to Clipboard | Save CSV and Close | Close

In the Forensic Explorer **Artifacts** module:

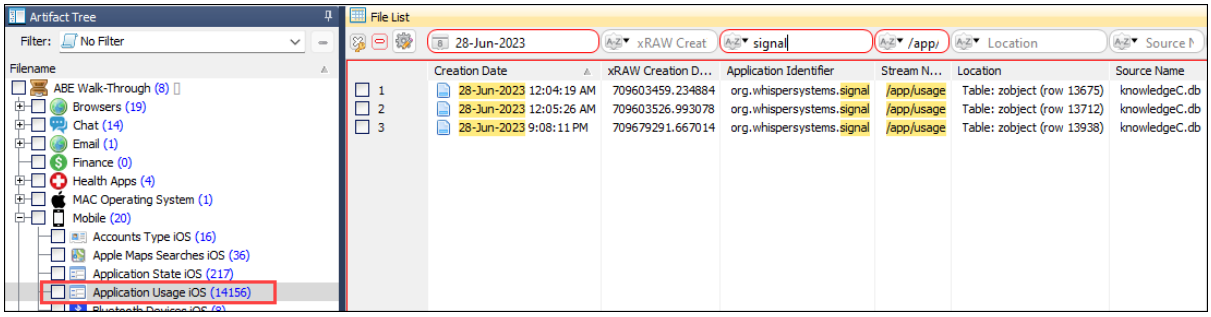
1. Select **iOS Biome**.
2. Use a **column filter** in the **Body** field for “I may be getting arrested shortly”.
3. This identifies a **Signal** message from **Harold.**

Figure 13: iOS Biome > Biome User Notification Events iOS



The **Mobile** > **Application Usage iOS** records also show use of **Signal** at that time.

Figure 14: Artifacts > Application Usage iOS



QUESTION 9 - PARKED - LEVEL 2 (30 POINTS)

Abe went to a party at RAIN Event Space. What is the name of the street (just the street name) where he parked his vehicle?

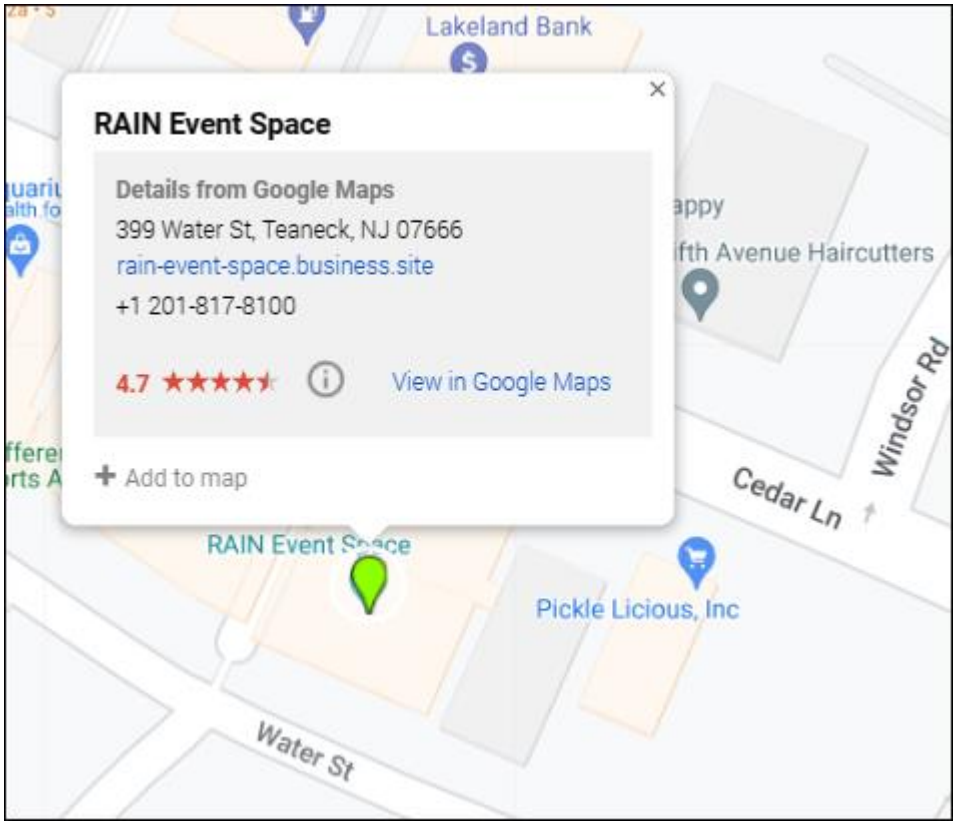
Q9. ANSWER

Water street.

Q9. FORENSIC EXPLORER METHODOLOGY

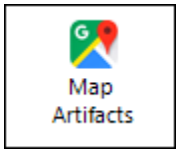
The first step is to locate the address of the **RAIN Event Space**. This is done using **Google My Maps**.

Figure 15: Google My Maps > RAIN Event Space



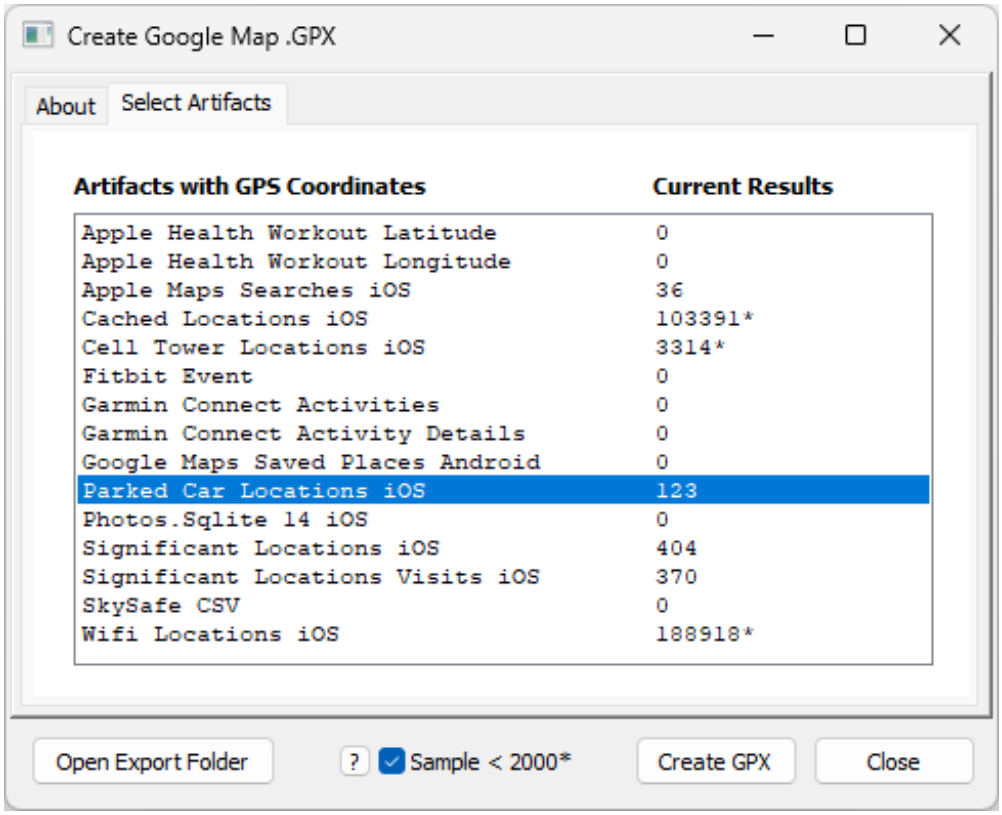
This question is likely to be answered using data from: **Artifacts > Mobile > Parked Car Locations**. Launch **Map Artifacts** from the toolbar button.

Figure 16: Artifacts > Map Artifacts



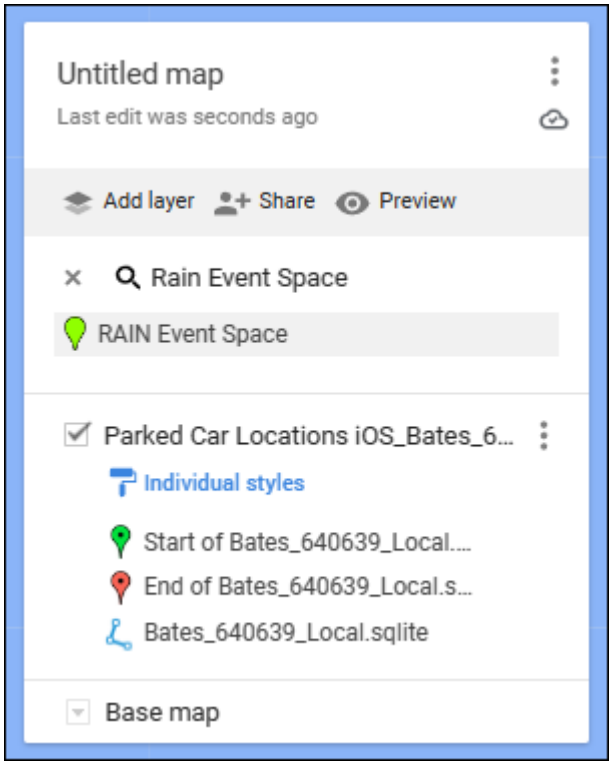
Select **Parked Car Locations iOS** from the list of available artifacts:

Figure 17: Map Artifacts



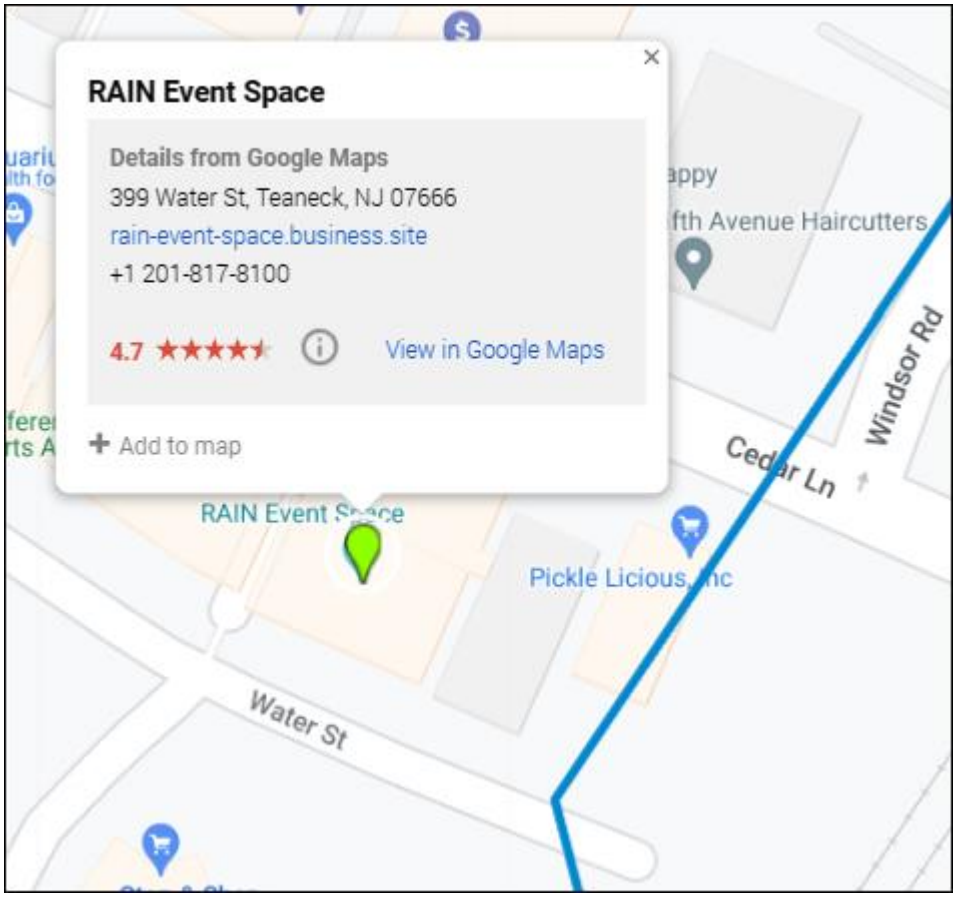
Create a **GPX** file and import into **Google My Maps** (or similar).

Figure 18: Google My Maps import



The map shows a data point on **Walter St** near the **Rain Event Space**.

Figure 19: Google My Maps



QUESTION 10 - ABOUT - LEVEL 2 (30 POINTS)

What was Abe Rudder's About bio on WhatsApp?

Q10. ANSWER

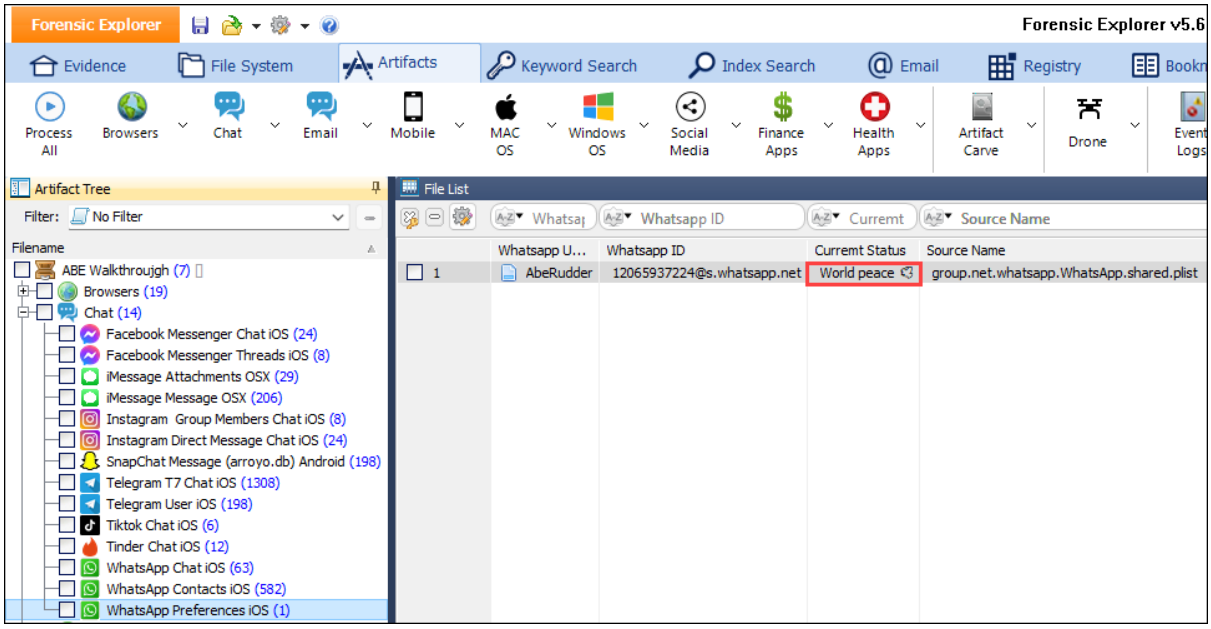
World peace.

Q10. FORENSIC EXPLORER METHODOLOGY

In the Forensic Explorer **Artifacts module**:

1. Select **Chat** > **WhatsApp Preferences iOS**.
2. **Current Status** is set to **World Peace**.

Figure 20: Artifacts > Chat > WhatsApp Preferences iOS



QUESTION 11 - PERMISSIONS - LEVEL 2 (30 POINTS)

Abe is paranoid and not always giving access to everything. One of the apps Abe used on the iPhone received access to Photos however as an "Add Photos Only" permission. What is the name of the app (one word i.e.: Starbucks)?

Q11. ANSWER

Chrome.

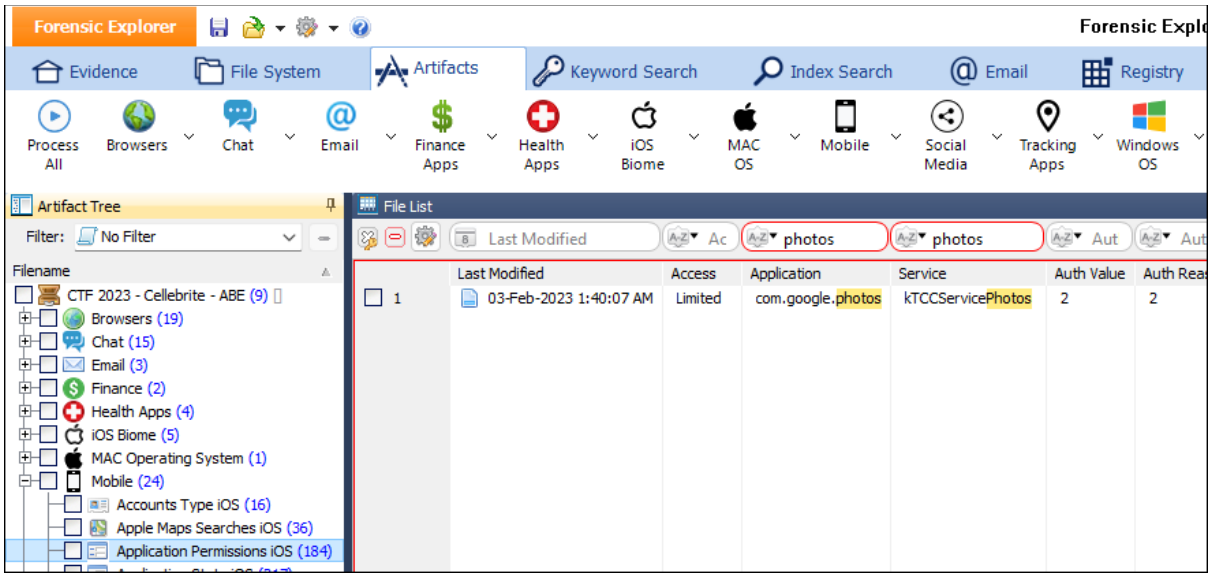
Q11. FORENSIC EXPLORER METHODOLOGY

In the Forensic Explorer **Artifacts module**:

1. Select **Mobile** > **Application Permissions iOS**.
2. Apply a column filter in the **Application** and **Service** columns for **photos**.

A single entry for Chrome is associated with the **kTCCServicePhotosAdd** access permission. The **Auth Value** of **2** indicates that the application was granted permission (see https://www.rainforestqa.com/blog/macos-tcc-db-deep-dive).

Figure 21: Artifacts > Mobile > Application Permissions iOS



QUESTION 12 - EMAIL - LEVEL 3 (50 POINTS)

Abe used a specific method to find/check/share locations via an app. In order to keep privacy up, Abe signed up with a different email address which keeps it isolated to that vendor. What is that email address?

Q12. ANSWER

j9by422yjc@privaterelay.appleid.com

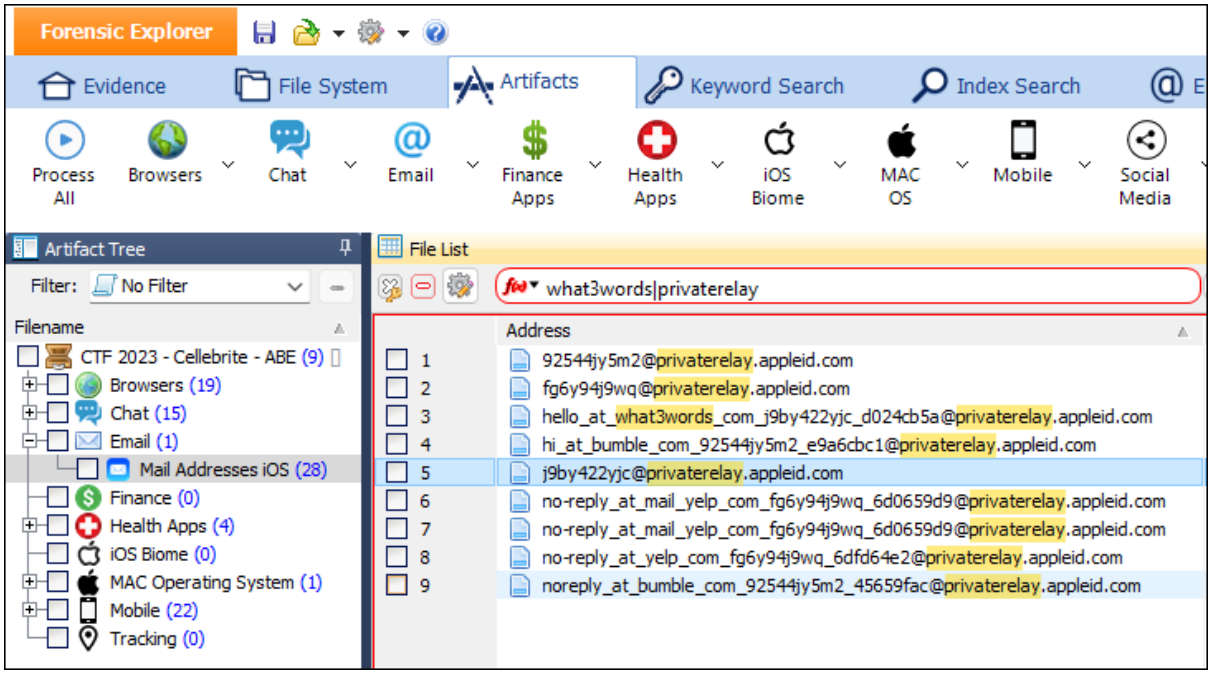
Q12. FORENSIC EXPLORER METHODOLOGY

There are several ways to approach this question. The biggest clues are **privacy** and **email address**.

To examine email addresses used on the iPhone:

1. In the Artifacts module, select **Email** > **Mail Addresses iOS**.
2. Of the 28-email address listed, the domain **privaterelay.appleid.com** stands out as a potential candidate.
3. One of the entries related to **priveaterelay** is **what3words**, and its Wikipedia entry indicates that it is geocode system used to share location information.

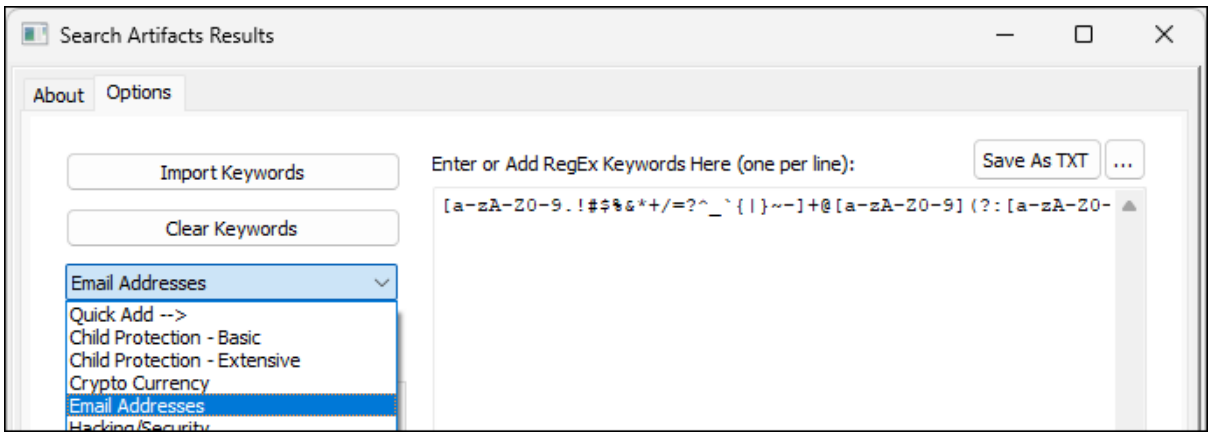
Figure 22: Artifacts > Mail Addresses > iOS



A broader search of all **Artifact module** results for email addressed can be done using the **Search Artifact Results** button.

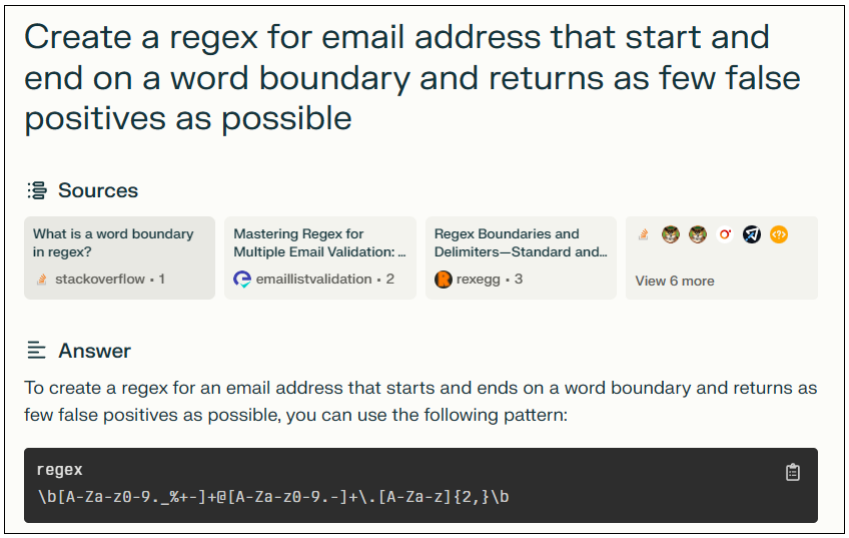
1. Use the **Quick Add** menu option to add a regular expression for email addresses.

Figure 23: Artifacts module > Search Artifact Results > Quick Add > email regex



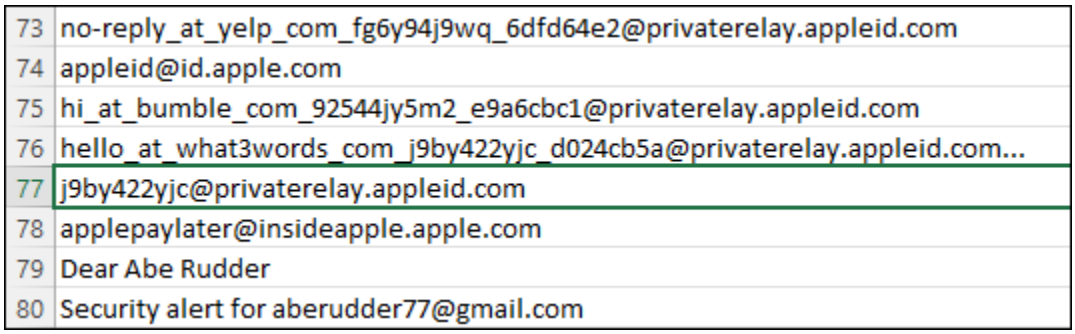
Artificial Intelligence websites, like Perplixity.com have made the creation and/or refinement of regular expression statements much simpler.

Figure 24: Perplexity



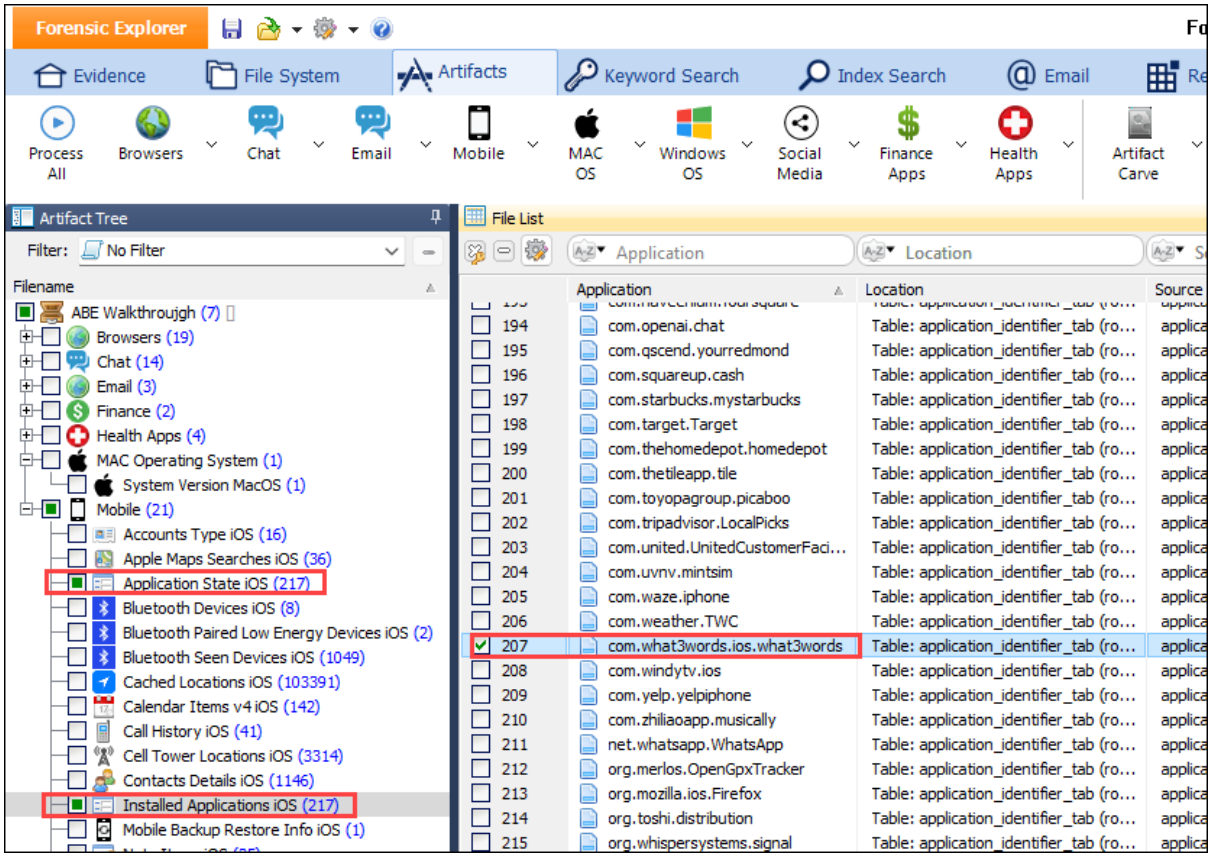
Save the search result to CSV and refine in Microsoft Excel (i.e. remove duplicates) to identify candidates.

Figure 25: Refine results in Microsoft Excel



Artifacts > Application State iOS and **Artifacts > Installed Applications iOS** can be used to confirm the presence of the what3words application on the iPhone.

Figure 26: Mobile > Application State and Installed Applications



QUESTION 13 - SEARCH - LEVEL 3 (50 POINTS)

Abe got suspicious when he had to deal with some shady people almost as if a crime was known to be committed and wanted to leave no traces. Abe wanted to create an anonymous email. Where did Abe search for that? (3 words)?

Q13. ANSWER

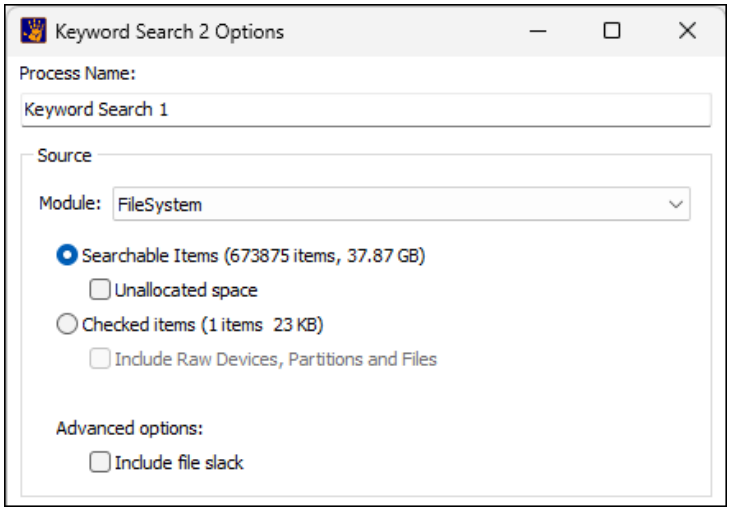
Duck Duck Go

Q13. FORENSIC EXPLORER METHODOLOGY

In the Forensic Explorer **Keyword Search** module:

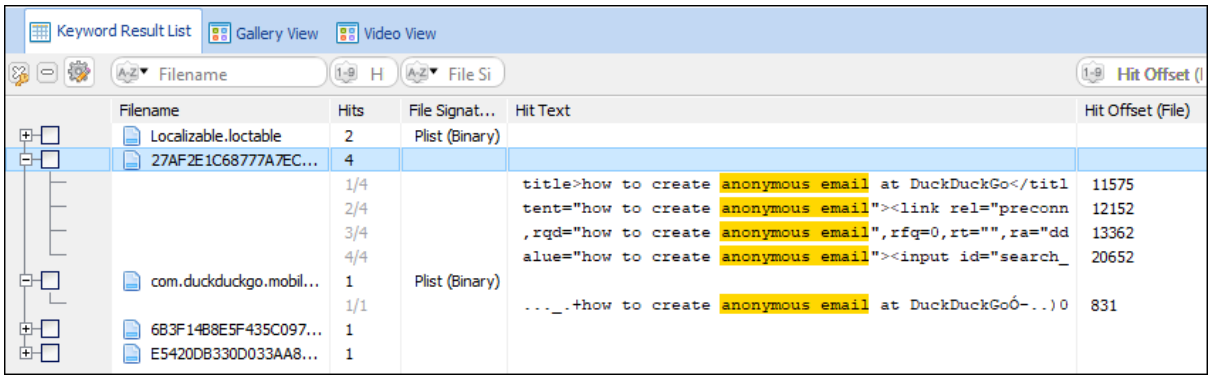
1. Add the keyword **anonymous email.**
2. Run the keyword search across all **FileSystem searchable items**.

Figure 27: Keyword Search



Keyword search hits are located that relate to the web browser **DuckDuckGo**. DuckDuckGo is considered good for anonymous browsing due to its strong privacy focus.

Figure 28: Keyword Search results



Artifacts > Mobile > Application State iOS confirms that DuckDuckGo is installed:

Figure 29: Artifacts > Mobile > Application State iOS

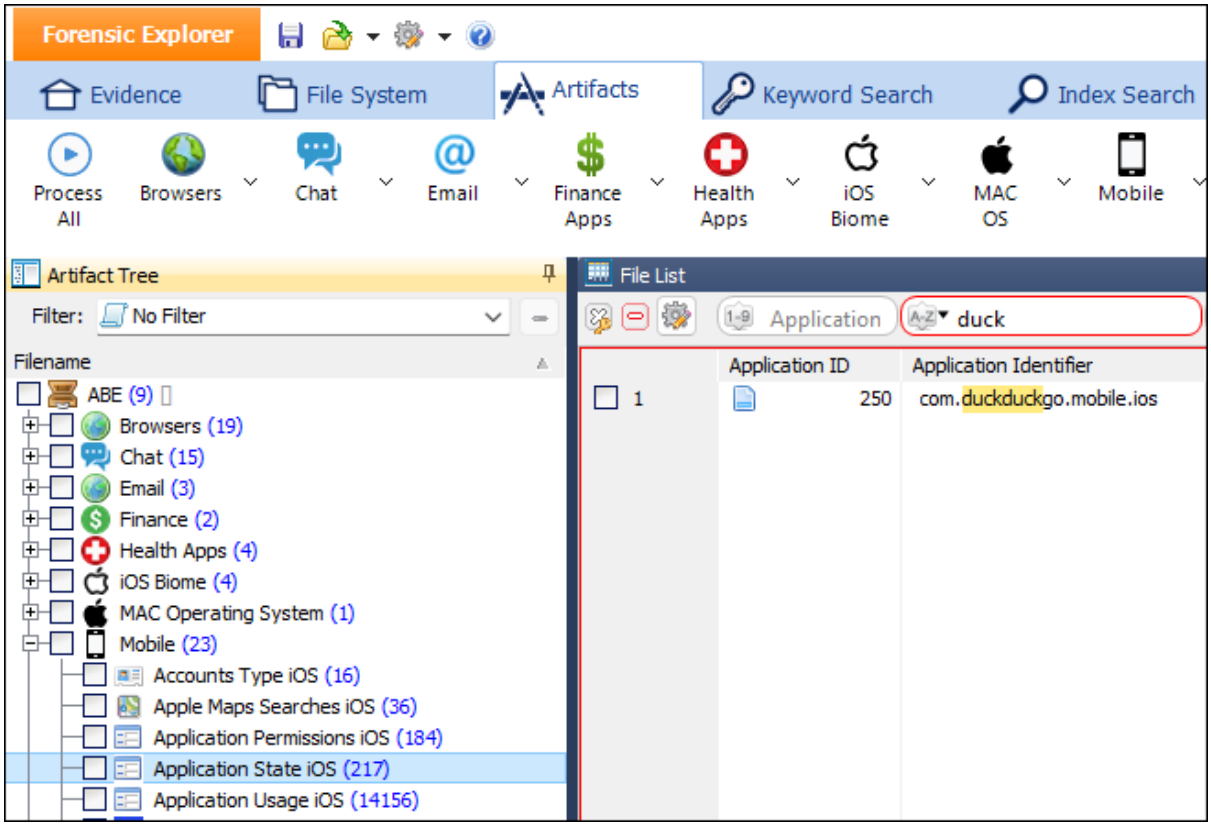
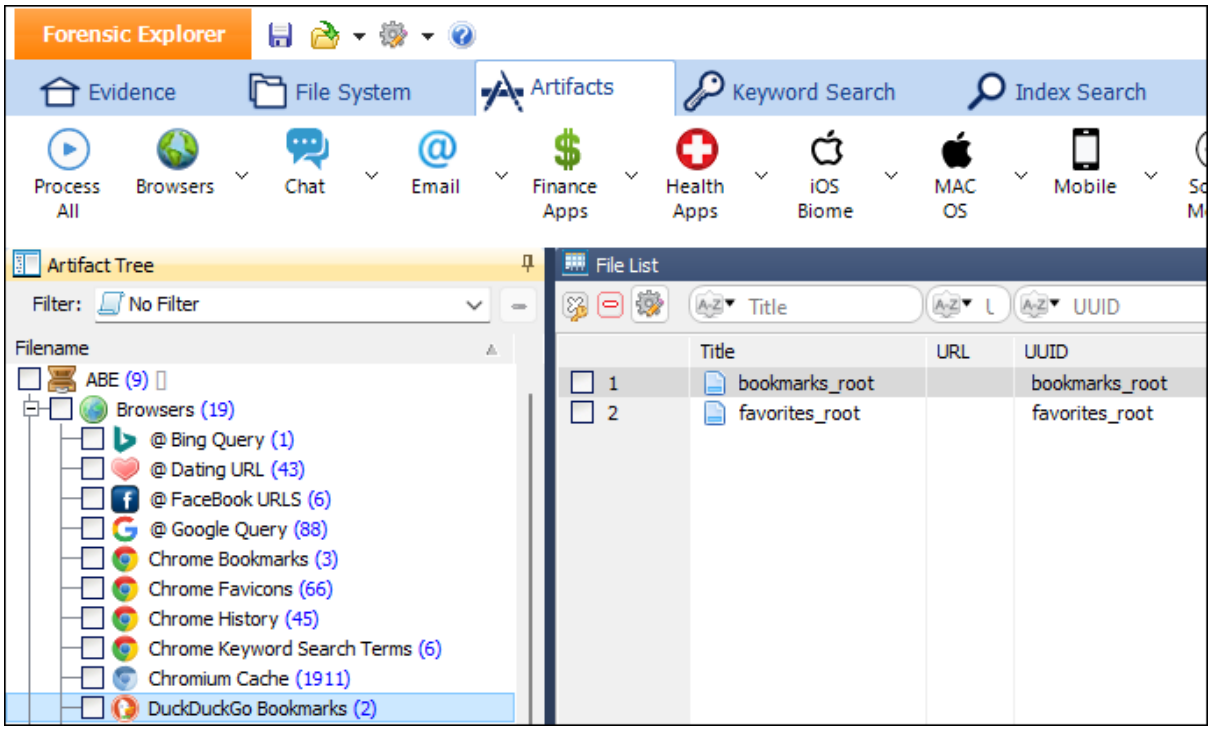


Figure 30: Artifacts > Browsers > DuckDuckgo



QUESTION 14 - NAVIGATION - LEVEL 3 (50 POINTS)

Abe was navigating while driving, on June 26, 2023. What was the destination address on the navigation?

Q14. ANSWER

284 Central Way, Kirkland

Q14. FORENSIC EXPLORER METHODOLOGY

This question is in progress. Check back soon.

QUESTION 15 - CRYPTO - LEVEL 2 (30 POINTS)

Abe used MOB to send/receive crypto within Signal. Can you find the Recovery Phrase for Signal Mobile Coin wallet? What is it? (24 words)?

Q15. ANSWER

pet element blast mix trumpet usual leg aim office jaguar emerge fatigue tent volcano other unfair absent hope power annual banana speak initial gold

Q15. FORENSIC EXPLORER METHODOLOGY

This question is in progress. Check back soon.

QUESTION 16 - PICTURE - LEVEL 2 (30 POINTS)

Abe loves taking pictures and videos on the iPhone, the problem is when Abe is trying to look for a picture, he is having hard time finding it therefore he utilizes the Search within the Apple Photos app. If Abe would have looked for a picture of: Myself, Pawel, and Hat he would end up with one photo. Can you name that filename?

Q16. ANSWER

IMG_1100.HEIC

Q16. FORENSIC EXPLORER METHODOLOGY

The Photos.sqlite database on an iPhone contains a wealth of information about all the photos and videos stored on the device, including their metadata such as creation date, modified date, location data, and more. It also stores information about face recognition and the relationships between photos and the applications they were created with. The database can be challenging to work with due to its complex structure, but it provides valuable insights for forensic investigations.

In Forensic Explorer, to **identify names attributed to iPhone photos**:

1. Select **Artifacts** > **Mobile** > **Photos.Sqlite Person iOS**.
2. In the **Display Name** or **Full Name** columns, change the column filter to **RegEx**.
3. Filter the column by **Myself|Pawel** (Myself OR Pawel).
4. **Double-click** on the **File Name** column header to sort the filtered result by **File Name**.
5. Search in the sorted File Name list for a file that contains both **Myself** and **Powell**. This identifies **IMG_1100.HEIC** as a candidate.
6. **Right-click** and **Copy cell** to copy the **Filename**.
7. In the **File System** module, **branch plate** [ ] the **entire case** and paste the copied filename into the **Filename** column.
8. In the bottom window, change to the **Display View** to view the photo.

Figure 31: Artifacts > Photos.sqlite

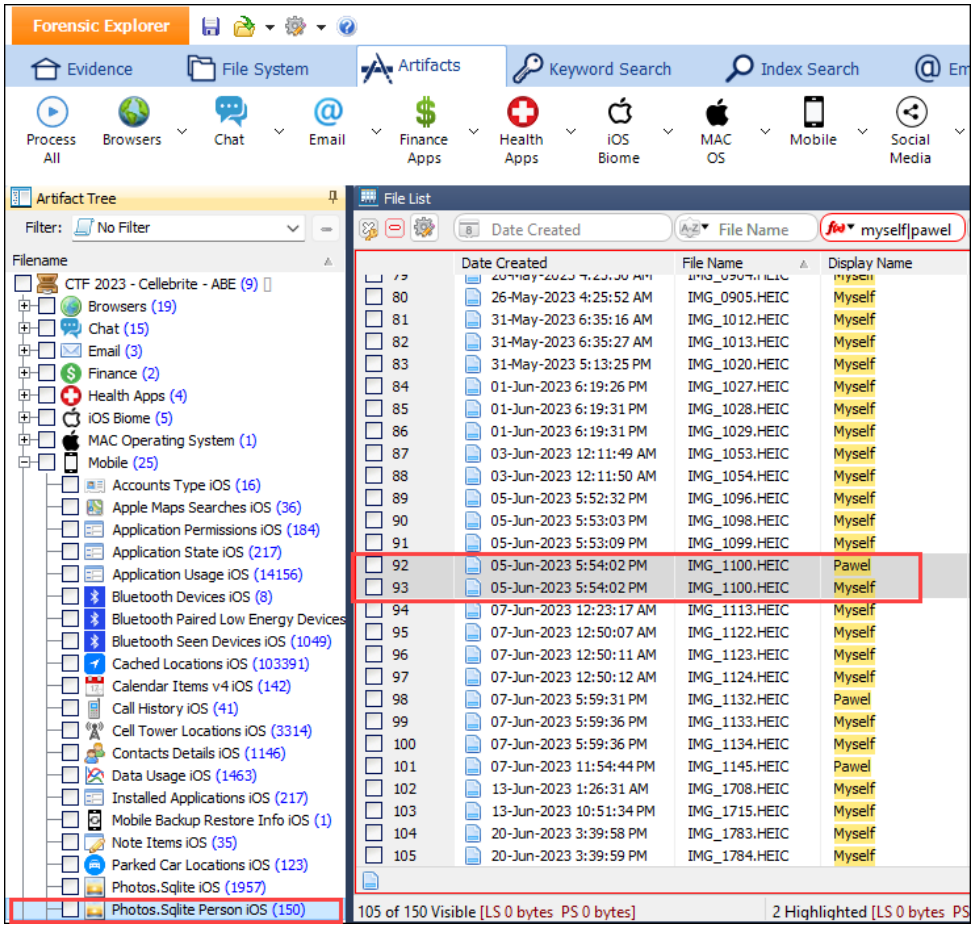
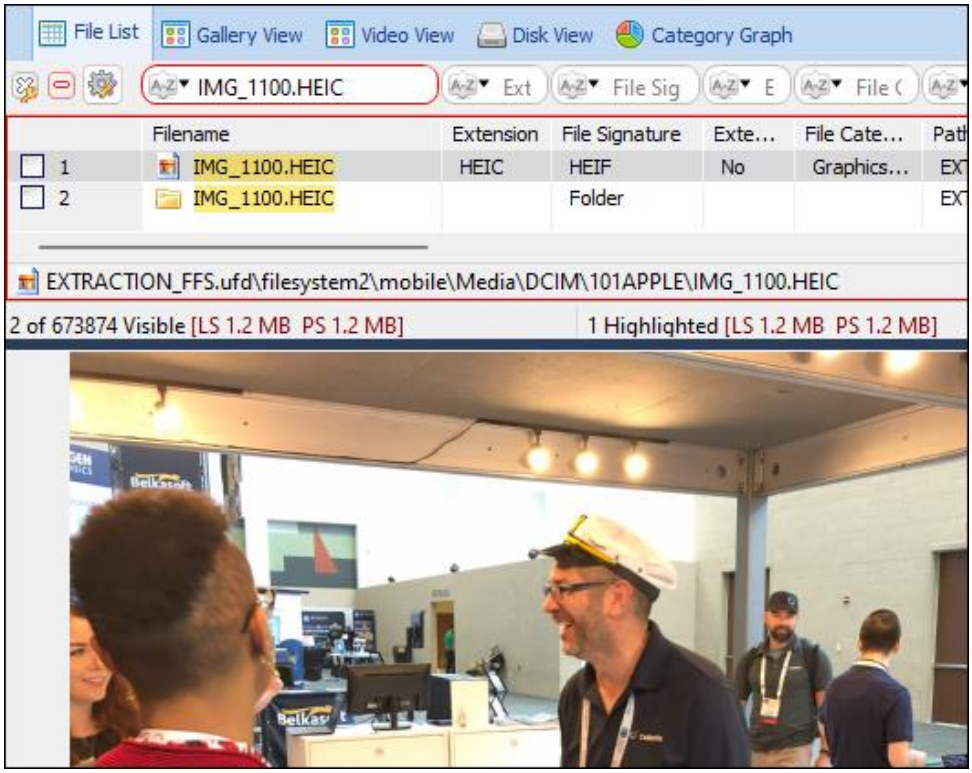


Figure 32: File System > column filter > Display View > IMG_1100.HEIC

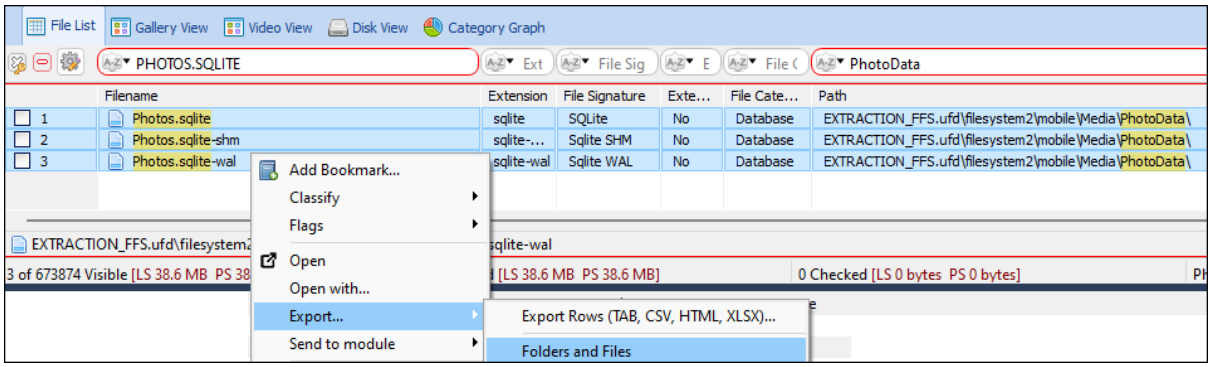


Alternate Method – Custom SQLite Query

As the question asks for specific information that is drawn from sever different SQLite tables inside Photos.sqlite, a custom SQLite query is an effective method of locating the filename of interest. To perform a custom SQLite search:

1. In the Forensic Explorer **File System** module, **branch plate** [ ] the **entire case** and use the **column filter** to locate the **Photos.sqlite** file and its associated **-wal** and **-shm** files.
2. Highlight the files, right-click and **Export > Files and folders**.

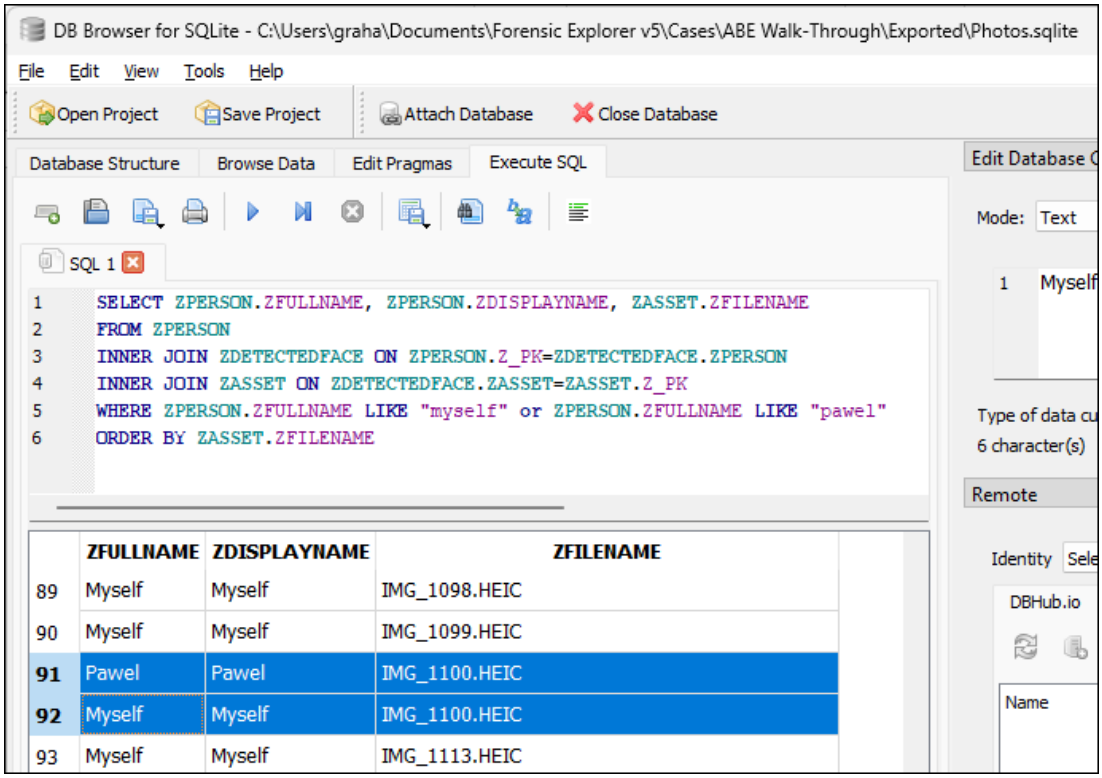
Figure 33: Open the raw Photos.sqlite database (and associated -shm and -wal)



3. Use the shortcut folder at the top of Forensic Explorer to navigate to the **Exported** folder of the current case.
4. **Open Photos.sqlite** with a **3rd party application**, e.g. DB browser for SQLite.
5. The SQLite query suggested by STARK-4n6 is:

```
SELECT DISTINCT ZPERSON.ZFULLNAME AS FULL_NAME, ZASSET.ZFILENAME AS FILENAME,
ZASSET.ZDATECREATED + 978307200 AS DATECREATED
FROM ZPERSON
INNER JOIN ZDETECTEDFACE ON ZPERSON.Z_PK=ZDETECTEDFACE.ZPERSON
INNER JOIN ZASSET ON ZDETECTEDFACE.ZASSET=ZASSET.Z_PK
WHERE ZPERSON.ZFULLNAME LIKE "Pawel"
ORDER BY ZASSET.ZDATECREATED DESC
```

Figure 34: DB Browser for SQLite (Query source: https://www.stark4n6.com/2023/10/cellebrite-ctf-2023-abe.html)



QUESTION 17 - LOCATION - LEVEL 2 (30 POINTS)

Abe went for some shady meeting on an island but tried to conceal as a vacation so he took a boat tour and tracked dolphins. He then decided to mark a location with "dolphins". What was the timestamp for that location? [HH:MM:SS] written in UTC time"?

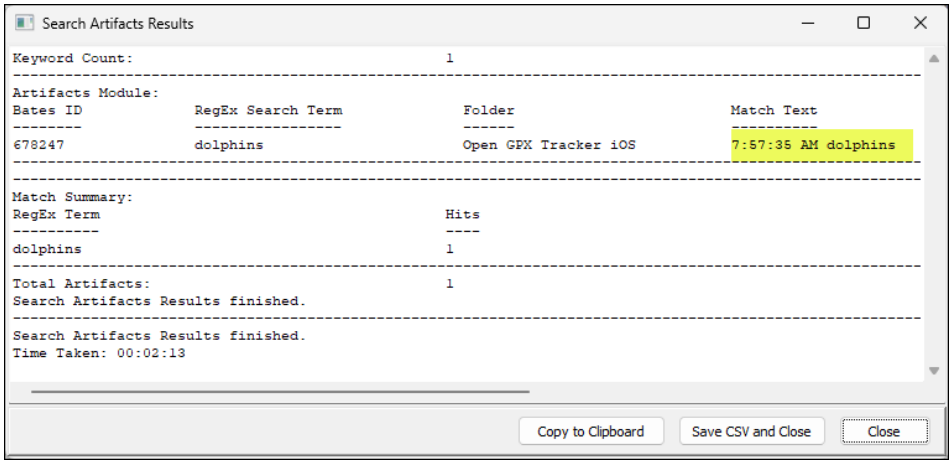
Q17. ANSWER

17:57:35.

Q17. FORENSIC EXPLORER METHODOLOGY

Figure 35: Artifacts > Search Artifact Results

Figure 36: Artifacts > Search Artifact Results > Dolphin



In the **Artifacts** module, select **Tracking** > **Open GPX Tracker iOS** and examine the **Waypoint Name**. To confirm the **UTC time**:

1. The **Artifacts** > **Source Name** column identifies **open-gpx-tracker-session.sqlite** as the source file. Right-click to copy the **Source Name**.
2. In the **File System** module, branch plate [ ] the **entire case**, and use the column filter to locate **open-gpx-tracker-session.sqlite**.
3. In **Display View**, locate the **ZCDWAYPOINT** table, and for **dolphins** entry, copy the raw **ZTIME** integer value.
4. Enter this value into a time decoding program (e.g. DCode) to confirm that the time value is in **UTC**.

Figure 37: Artifacts > Tracking > Open GPX Tracker iOS

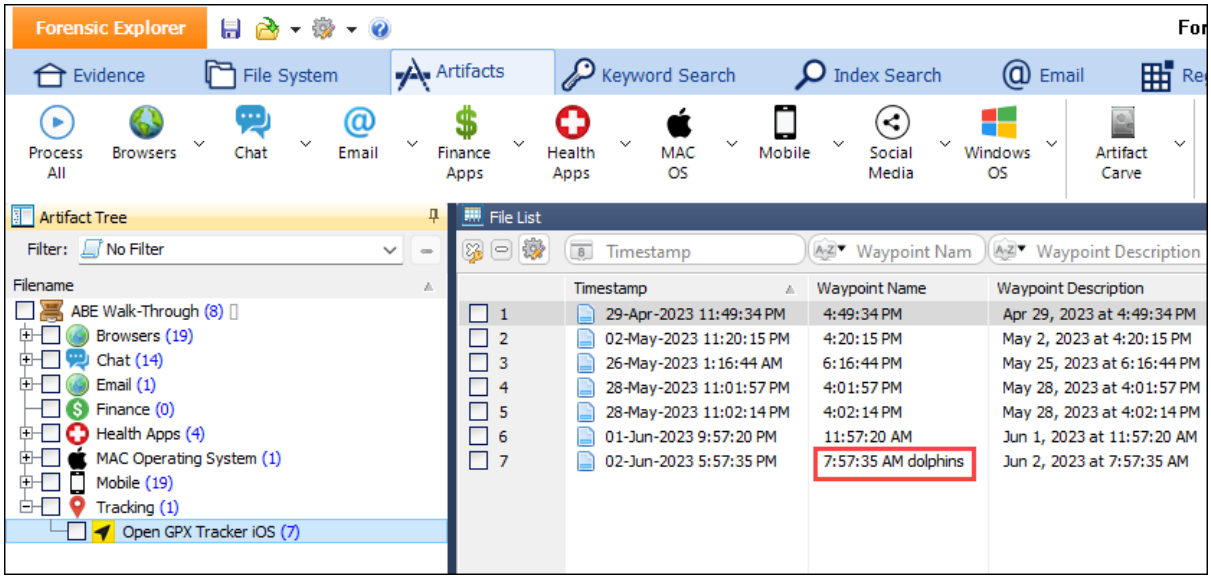


Figure 38: open-gpx-tracker-session.sqlite

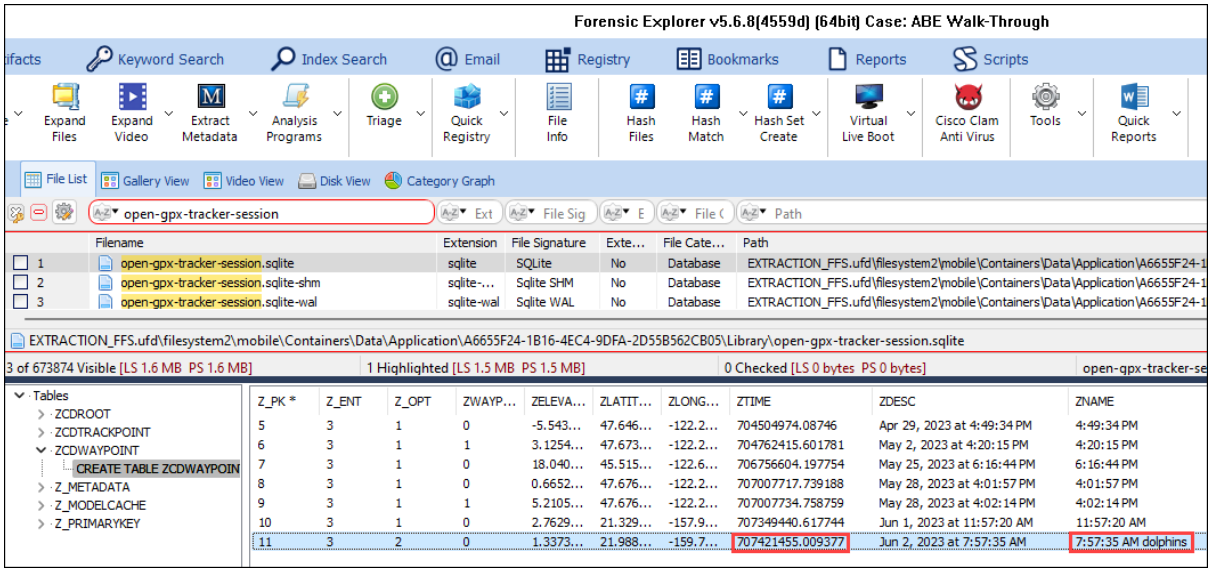
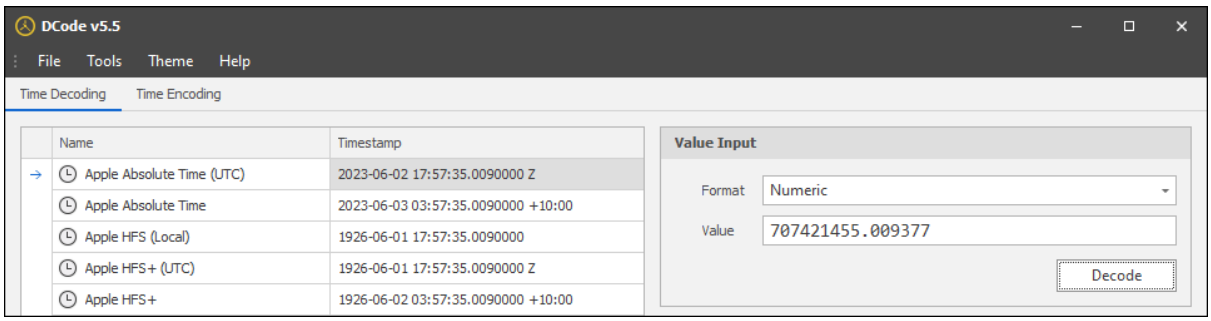


Figure 39: DCode (https://www.digital-detective.net/dcode/)



QUESTION 18 - BOKERTOV - LEVEL 3 (100 POINTS)

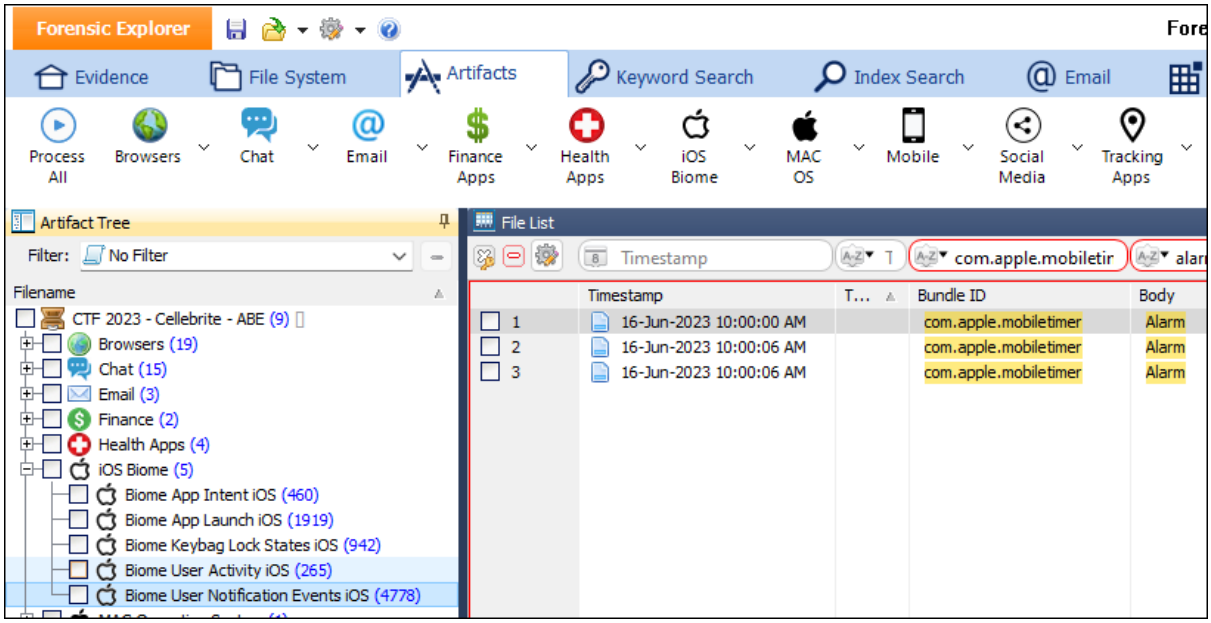
Within the last month before Abe got arrested (and his device was extracted), Abe used to wake up naturally however, there was one day the phone did. What was the day and (local) time? [YYYY-MM-DD HH:MM:SS] e.g: 2021-09-19 08:35:00?

Q18. ANSWER

2023-06-16 06:00:00.

Q18. FORENSIC EXPLORER METHODOLOGY

Figure 40: Artifacts > Biome > User Notification Events iOS



Screen Snapshot:

There is a screenshot in the following path:

> ***filesystem2\mobile\Containers\Data\Application\73B09176-74A6-4676-AE95-0769BC8603D3\Library\SplashBoard\Snapshots\sceneID_com.apple.mobiletimer-default\17FA1799-E1EF-42E8-A76F-91F7E63319E4@3x.ktx***

Forensic Explorer does not currently view .ktx files. This feature is currently in development.