

# MAGNET VIRTUAL SUMMIT 2024

## CAPTURE THE FLAG (CTF)

### IOS

About This CTF Challenge .....	2
Starting this challenge in Forensic Explorer.....	3
Questions Only - iOS .....	4
Q1. Why are your messages green? (5 points).....	7
Q2. Where /r u going on safari (5 points).....	9
Q3. Don't ghost me (5 Points) .....	11
Q4. IMAGEine living in pain (5 points).....	13
Q5. Your keyboard is salt-y (5 points) .....	14
Q6. Build me up, buttercup (5 points).....	15
Q7. Answer the call (5 points) .....	17
Q8. Warning Signs (5 points) .....	18
Q9. Watching streams to stay current (10 points) .....	19
Q10. One is The Lonliest Number (10 points) .....	22
Q11. Watch me sUAVely win this game (10 points).....	26
Q12. For when I cant Find My gear (10 points).....	27
Q13. Just a couple steps away (10 points) .....	28
Q14. Another regularly scheduled program (10 points) .....	30
Q15. I hear Stanley cups are all the rage (25 points) .....	33
Q16. Devil is in the details .....	36
Q17. Excuse Moi? What did you say (25 points) .....	38
Q18. Boost this server .....	40
Q19. Its been a long time (25 points) .....	42
Q20. Can anyone Kelp (25 points) .....	44
Q21. Chat GPT is my PREFERENCE for AI (25 points) .....	46
Q22. Read my mind (25 points).....	48
Q23. Seasons Greetings (25 points) .....	50
Q24. Follow the Breadcrumbs (50 points).....	54

## ABOUT THIS CTF CHALLENGE

This challenge was created by Magnet Forensics as part of their 2024 Virtual Summit.

Information about the next summit is available at:

- <https://magnetvirtualsummit.com/>
- <https://magnetvirtualsummit.com/capture-the-flag/>
- <https://www.magnetforensics.com/blog/2024-magnet-virtual-summit-ctf-winners-and-another-chance-to-play/>

## FORENSIC IMAGE SOURCE

Download: <https://drive.google.com/drive/folders/1zynwO2BaccA2EOTcRYhKV5CjKuWWU2I6>

## OTHER ONLINE SOLUTIONS

The following solutions can be found on the web:

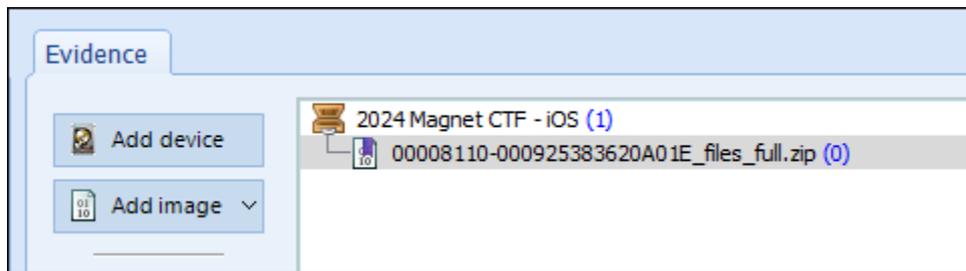
- <https://m-brumbelow.github.io/posts/MVS2024CTF/>
- <https://blog.kairostay.com/posts/magnet-virtual-summit-24/>
- <https://www.stark4n6.com/2024/03/magnet-virtual-summit-2024-ctf-android.html>
- <https://bakerstreetforensics.com/2024/03/12/magnet-virtual-summit-2024-capture-the-flag/>
- <https://dfir101.wordpress.com/2024/03/19/magnet-forensics-virtual-ctf-2024-android-challenges/>

## 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 evidence file: **00008110-000925383620A01E\_files\_full.zip**
5. In the **Evidence Processor** window use the default options.

Figure 1: Add Image > Add Zip file

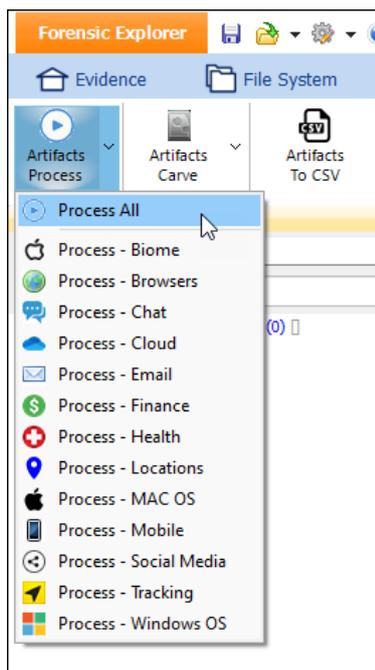


## ARTIFACTS > PROCESS ALL

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



**QUESTIONS ONLY - IOS**

Why are your messages green?	On what date did Rocco and Chadwick first meet in person according to their conversations? YYYY-MM-DD format
Where /r u going on safari?	What subreddit was visited in a browser?
Don't ghost me	At what time did Chadwick get annoyed at MYAI? YYYY-MM-DD HH:MM:SS UTC
IMAGEine living in pain	Chad seemed to be searching for pain relief medicine in a store, how much did it cost?
Your keyboard is salt-y	How many total words were typed on the device?
Build me up, buttercup	What is the current build version?
Answer the call	What is the guild ID of the discord server Chad was in?
Warning Signs	How many days did it take Chad to be warned about his Data Usage?
Watching streams to stay current	What is the name of Chad's streaming channel?
One is The Loneliest Number	What question did Chadwick ask to AI?
Watch me sUAVely win this game	How many kills did Chad have on his CoD Mobile winning game?
For when I can't Find My gear	What outdoor activity store did Chadwick Visit?
Just a couple steps away	How many steps did Chad take on 12/3/2023?

Another regularly scheduled program	What Tattoo shop was visited on 12/27/2023?
I hear Stanley cups are all the rage	What was the final score of the hockey game Chad went to? (home – away)
Devil is in the details	Whose bitmoji is dressed like a devil?
Excuse Moi? What did you say?	What is the content of the 2nd message that Chad deleted on Dec 18, 2023
Boost this server	What is the 16 character carrier code?
The easy way or the hard way	What is the timestamp of the message Chad sent to Rocco but was never received? YYYY-MM-DD HH:MM:SS UTC
Its been a long time	When did chad last login to Facebook? YYYY-MM-DD HH:MM:SS UTC
Can anyone Kelp?	What game was Chad asking to know the strategy to?
Chat GPT is my PREFERENCE for AI	What is the ChatGPT userID associated with chawickmr95@gmail.com
Read my mind	What message was sent to Rocco in a video game
Season’s Greetings	What was the first emoji that was sent to Susan?
Follow the Breadcrumbs	How many times did Chad’s keyboard become visible within the Amazon app on 12/24/2023?

INDIVIUDALS OF INTEREST

<b>Name:</b>	<b>Rocco Sachs</b>
<b>Phone:</b>	<b>Android</b>
Profile:	<a href="https://www.facebook.com/profile.php?id=61554919820462">https://www.facebook.com/profile.php?id=61554919820462</a>
Facebook Registration:	Saturday, December 16, 2023 at 11:29 AM UTC-05:00
Facebook Email:	<b>roccotsachs@gmail.com</b>
Facebook Birthday:	29 Sep 1974
Facebook Gender:	Male
Discord ID:	1185636389107273799
Discord Username:	oneclick5864_28820
Twitter Username	RoccoSachs96775
Twitter User ID:	1719897971716685824

<b>Name:</b>	<b>Chadwick Elms</b>
<b>Phone:</b>	<b>Apple iPhone</b>
Facebook Profile:	<a href="https://www.facebook.com/profile.php?id=61555027042760">https://www.facebook.com/profile.php?id=61555027042760</a>
Facebook Registration:	December 22, 2023
Facebook Email:	chawickmr95@gmail.com
Facebook Birthday:	
Facebook Gender:	
Discord ID:	1189069936618897431
Discord Username:	Chadwickgames
Twitter Username	GardenGamer95
Twitter User ID:	725408643810654

**Q1. WHY ARE YOUR MESSAGES GREEN? (5 POINTS)**

*On what date did Rocco and Chadwick first meet in person according to their conversations? YYYY-MM-DD format?*

**Q1. ANSWER**

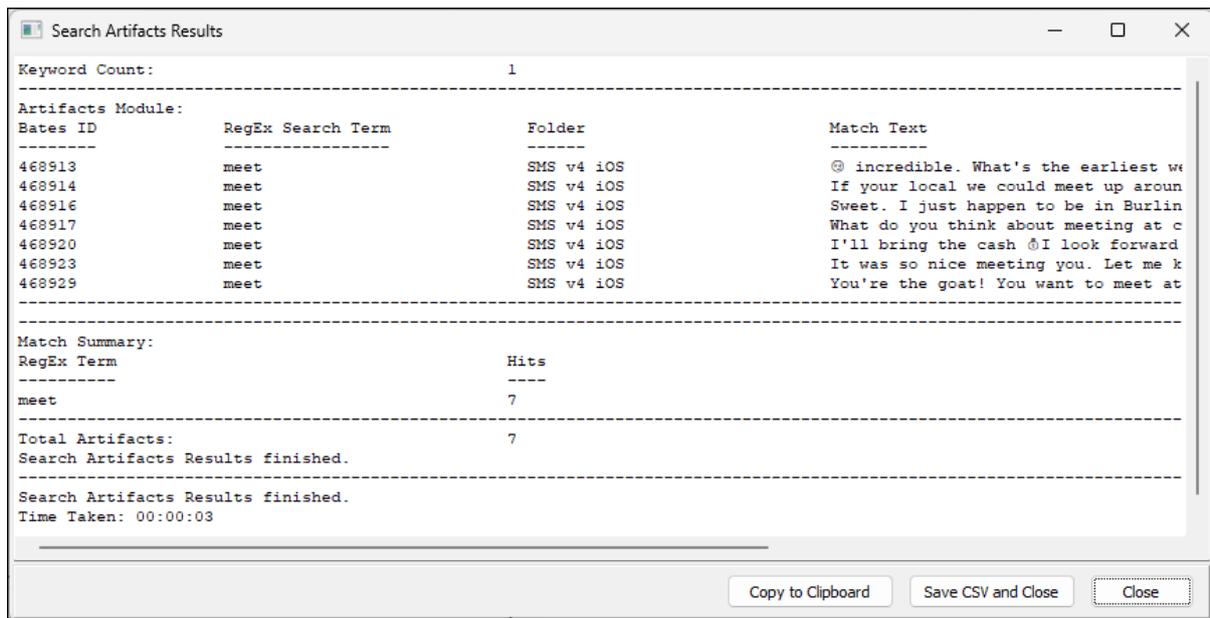
2023-12-17.

**Q1. FORENSIC EXPLORER METHODOLOGY**

In the **Artifacts** module:

1. Use the **Search Artifact Results** button to run a search for the keyword **meet**.
2. Search results indicate **SMS** to be the source.

Figure 3: Artifacts > Search Artifact Results > "Meet"



3. Select the **Mobile > SMS v4 iOS** folder.
4. Filter the **Text** column for the keyword **meet**. Messages indicate the first meeting to be on 2023-12-17.

Figure 4: Artifacts > SMS > column filter "meet"

	Date	Date Read	Text	Type
<input type="checkbox"/> 1	17-Dec-2023 4:15:49 PM		📍 incredible. What's the earliest we can we meet up?	Sent
<input type="checkbox"/> 2	17-Dec-2023 4:20:23 PM	17-Dec-2023 4:21:12 PM	If your local we could meet up around 12pm today. You in/near VT?	Received
<input type="checkbox"/> 3	17-Dec-2023 4:24:37 PM	17-Dec-2023 4:28:20 PM	Sweet. I just happen to be in Burlington too, I had another client to me...	Received
<input type="checkbox"/> 4	17-Dec-2023 4:25:52 PM	17-Dec-2023 4:28:20 PM	What do you think about meeting at city Hall park at 12pm?	Received
<input type="checkbox"/> 5	17-Dec-2023 4:43:27 PM		I'll bring the cash 📍 I look forward to meeting you	Sent
<input type="checkbox"/> 6	17-Dec-2023 5:08:46 PM		It was so nice meeting you. Let me know when u want to play another ...	Sent
<input type="checkbox"/> 7	18-Dec-2023 12:42:34 AM		You're the goat! You want to meet at the Ethan Allen Park?	Sent

**Q2. WHERE /R U GOING ON SAFARI (5 POINTS)**

*What subreddit was visited in a browser?*

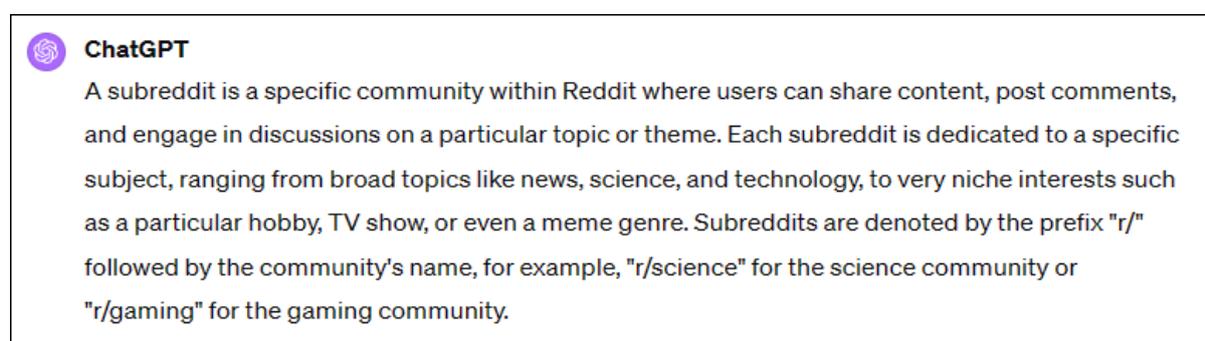
**Q2. ANSWER**

<https://www.reddit.com/r/Twitch/>

**Q2. FORENSIC EXPLORER METHODOLOGY**

ChatGPT was used to determine the structure of a **subreddit** URL as **reddit.com/r/**.

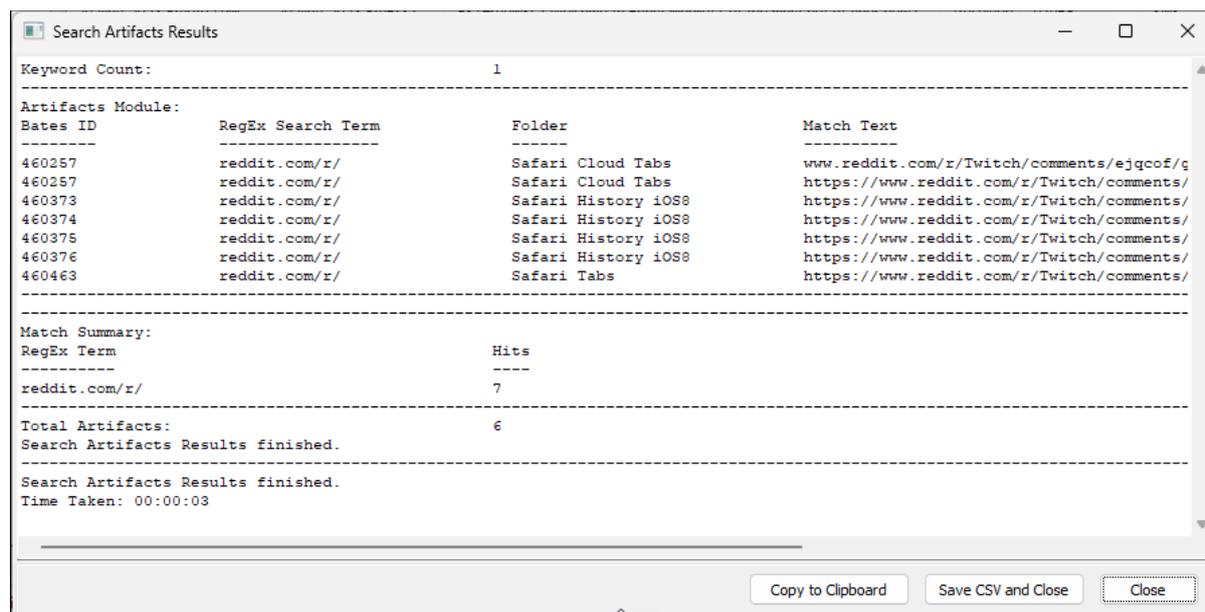
Figure 5: ChatGPT



In the **Artifacts** module:

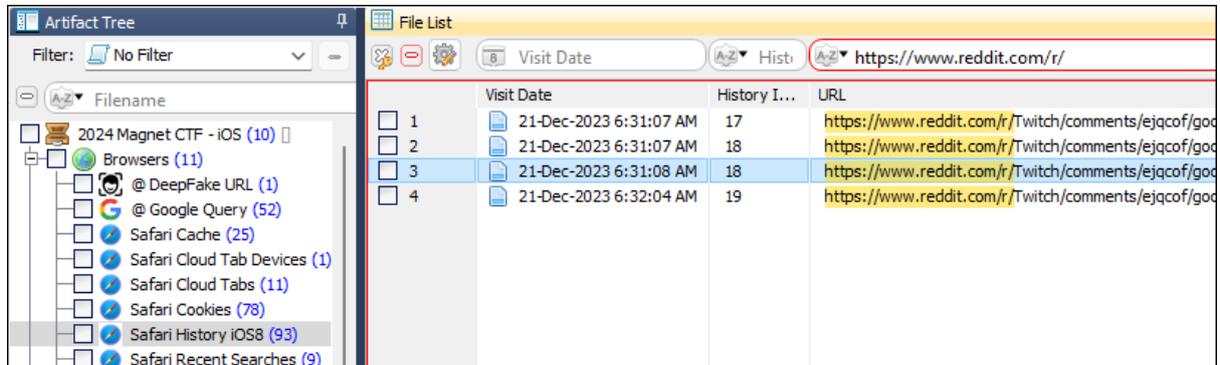
1. Click the **Search Artifact Results** button and search for keyword **reddit.com/r/**.
2. The **Safari** results show the answer to be **https://www.reddit.com/r/Twitch/**.

Figure 6: Search Artifacts Results > "reddit.com/r/"



3. Select the **Safari History iOS8** folder.
4. Filter the URL column for **https://www.reddit.com/r/** to examine the URLs in more detail.

Figure 7: Artifacts > Browsers > Safari History iOS8 > URL filter



**Q3. DON'T GHOST ME (5 POINTS)**

*At what time did Chadwick get annoyed at MYAI? YYYY-MM-DD HH:MM:SS UTC. 24 hour formatted timestamp?*

**Q3. ANSWER**

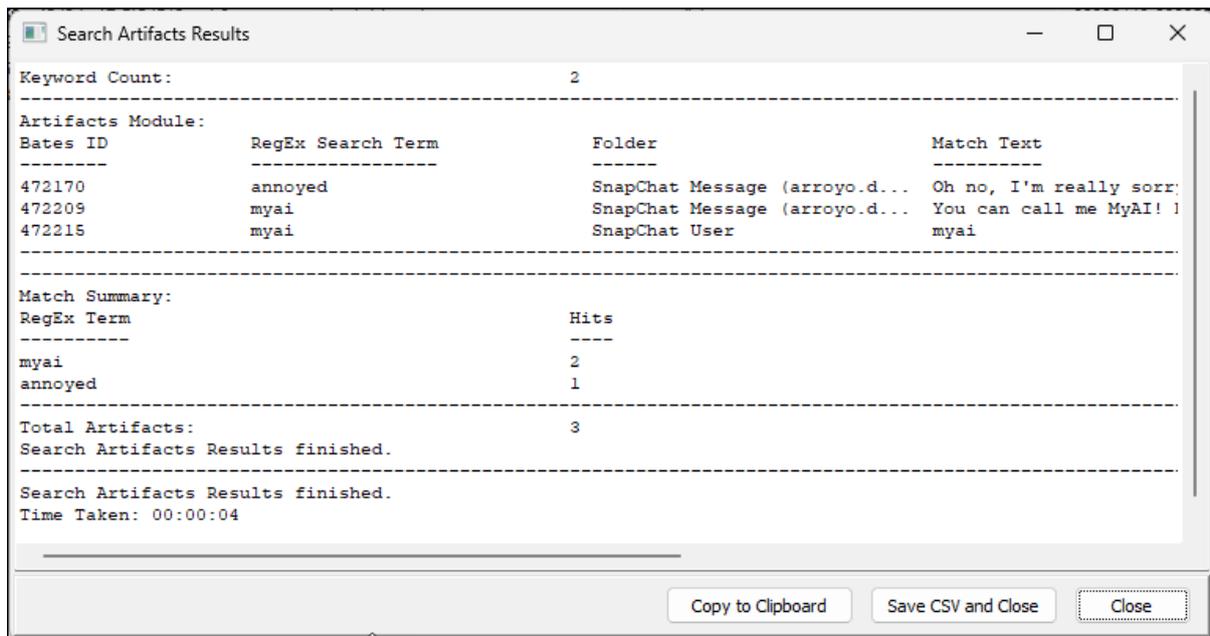
2023-12-26 23:27:45.

**Q3. FORENSIC EXPLORER METHODOLOGY**

In the **Artifacts** module:

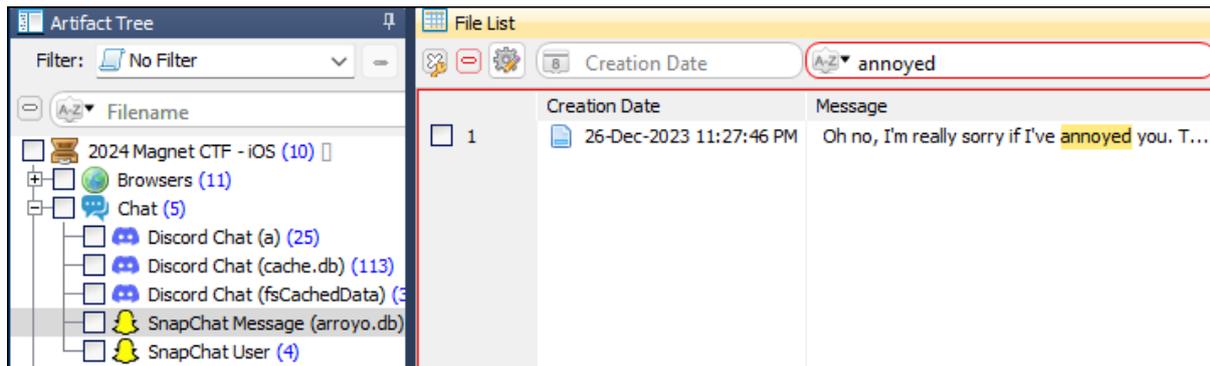
1. Click the **Search Artifact Results** button and search for keywords **myai** and **annoyed**.
2. Search results show **SnapChat** as the source.

Figure 8: Artifacts > Search Artifact Results



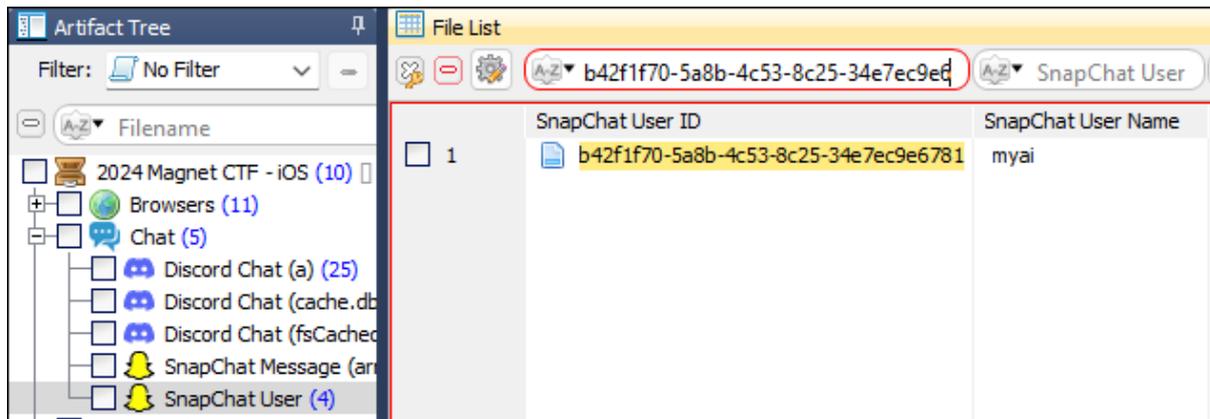
3. Select the folder **Chat > SnapChat Messages (arroyo.db)**.
4. Filter the **Messages** column for **annoyed** to examine the message in more detail.

Figure 9: Chat > SnapChat Message (arroyo.db)



5. The **Sender ID** column shows that the message has been sent by the SnapChat user **b42f1f70-5a8b-4c53-8c25-34e7ec9e6781**.
6. Select the **Chat > SnapChat User** folder to identify this user as **myia**.

Figure 10: Artifacts > Chat > SnapChat user



#### Q4. IMAGINE LIVING IN PAIN (5 POINTS)

*Chad seemed to be searching for pain relief medicine in a store, how much did it cost?*

#### Q4. ANSWER

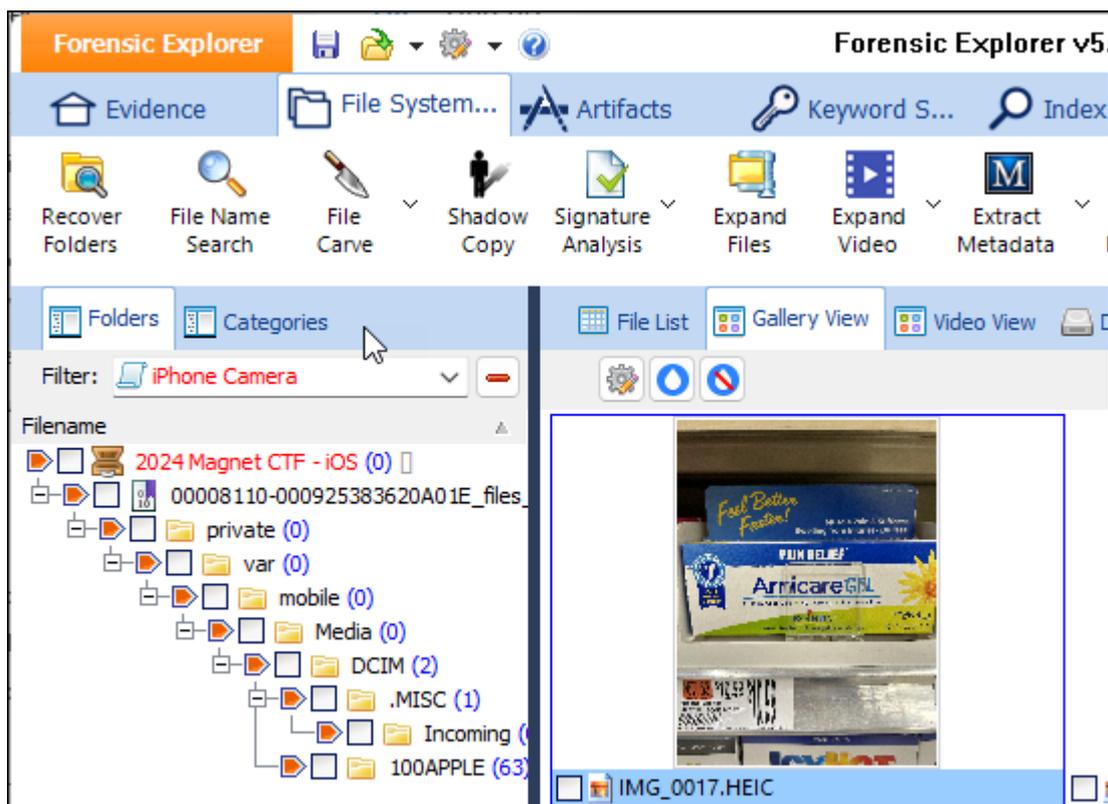
\$10.99.

#### Q4. FORENSIC EXPLORER METHODOLOGY

There is a clue in the title of this question “**IMAGE**ine” that indicates the answer is likely to be in a photograph.

1. In the **File System** module, branch plate [ ] the entire case.
2. Apply the **iPhone Camera** folders filter.
3. Switch to **Gallery View** and photograph **IMG\_0017.HEIC** is quickly identified.

Figure 11: \private\var\mobile\Media\DCIM\100APPLE\IMG\_0017.HEIC



**Q5. YOUR KEYBOARD IS SALT-Y (5 POINTS)**

*How many total words were typed on the device?*

**Q5. ANSWER**

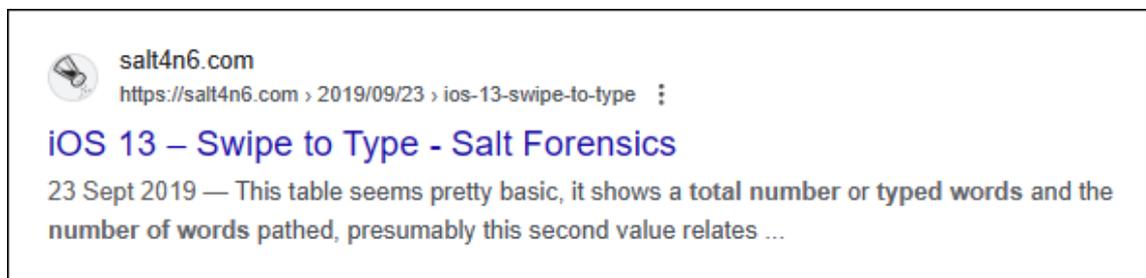
1797.

**Q5. FORENSIC EXPLORER METHODOLOGY**

A **Google search** for **iOS typed words** located research by **Salt4N6** relating to:

- **/private/var/mobile/Library/Keyboard/user\_model\_database.sqlite**

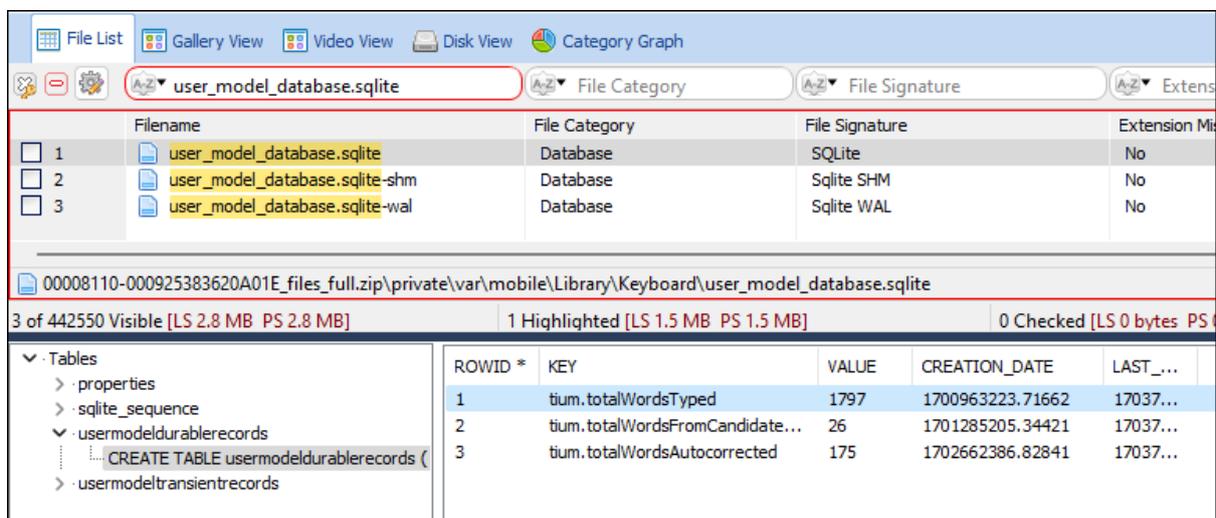
Figure 12: iOS total number of typed words



To locate and examine **user\_model\_database.sqlite**:

1. In the **File System** module, branch plate [  ] the entire case.
2. In the **Filename** column, filter for **user\_model\_database.sqlite**.
3. Change to **Display View** in the bottom tab to view the content of the SQLite database.
4. Select the **usermodeldurablerecords** table, **VALUE** column.

Figure 13: user\_model\_database.sqlite



**Q6. BUILD ME UP, BUTTERCUP (5 POINTS)**

*What is the current build version?*

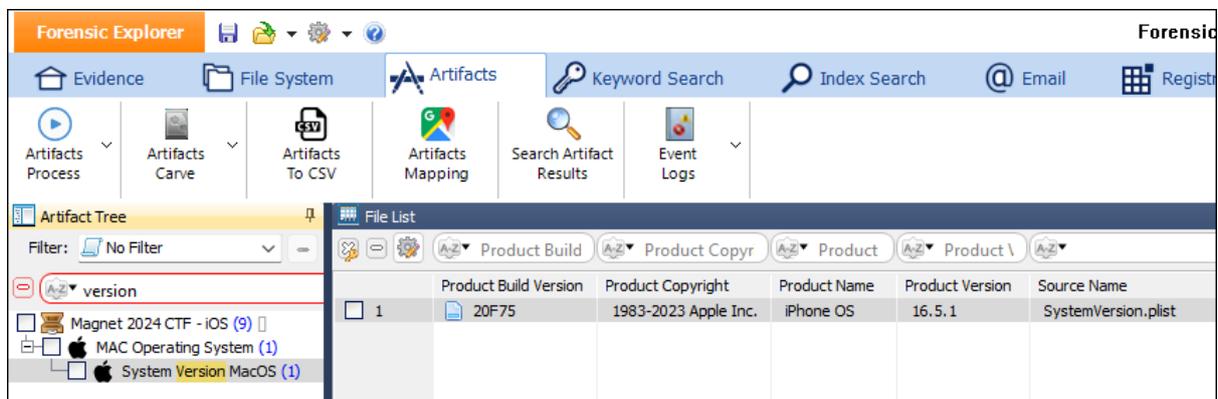
**Q6. ANSWER**

20F75.

**Q6. FORENSIC EXPLORER METHODOLOGY**

Build information is displayed in **Artifacts > MAC Operating System > System Version MacOS**. This shows the **Product Build Version** to be **20F75**.

Figure 14: Artifacts > MAC Operating System > System Version MacOS



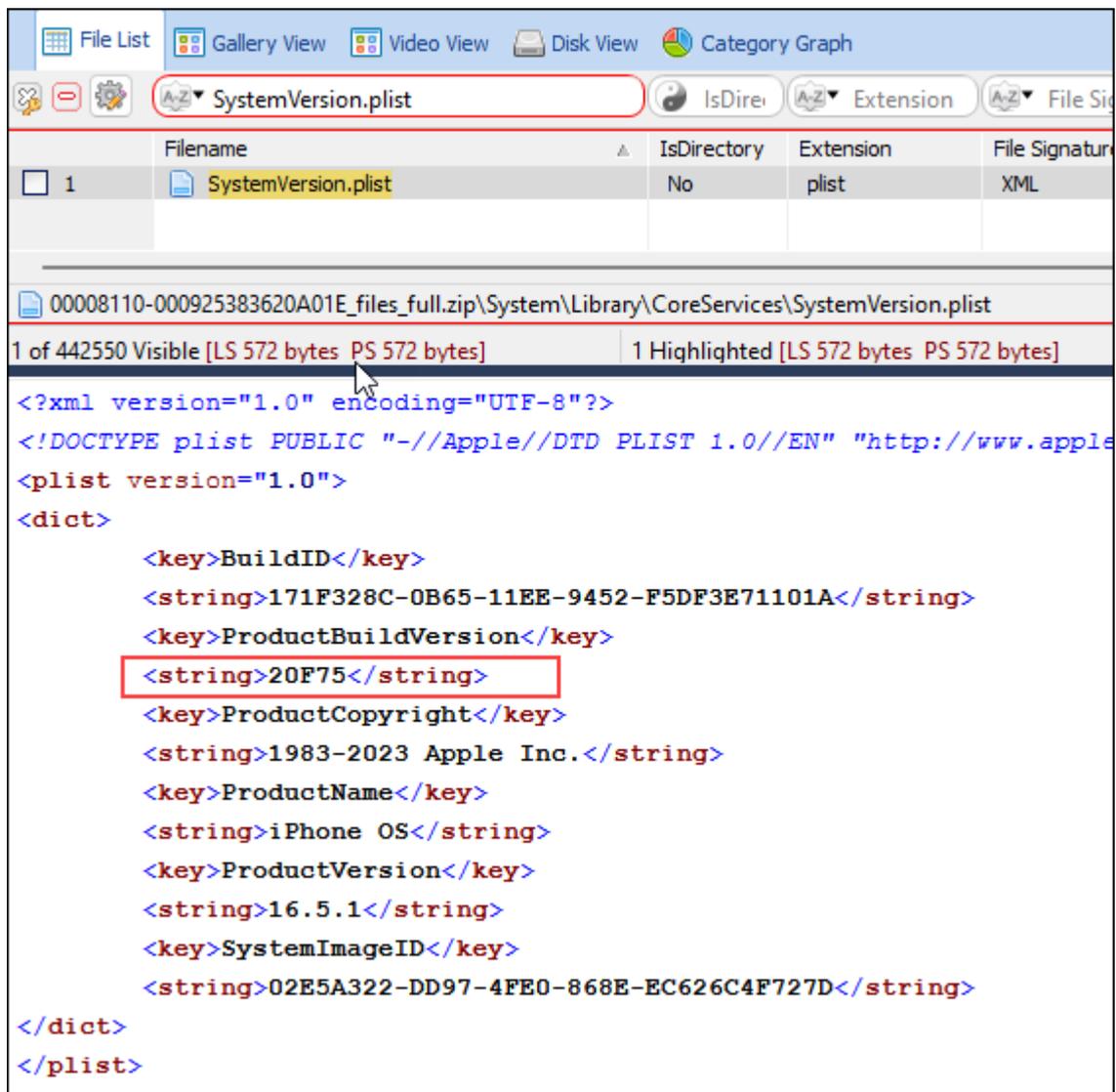
The source of this information is:

- `\System\Library\CoreServices\SystemVersion.plist`

To locate and examine **SystemVersion.plist**:

1. In the **File System** module, branch plate [  ] the entire case.
2. In the **Filename** column, filter for **SystemVersion.plist**.
3. Change to **Display View** in the bottom tab to view the content of the content of the file.

Figure 15: SystemVersion.plist



**Q7. ANSWER THE CALL (5 POINTS)**

*What is the guild ID of the discord server Chad was in?*

Q7. ANSWER

136986169563938816.

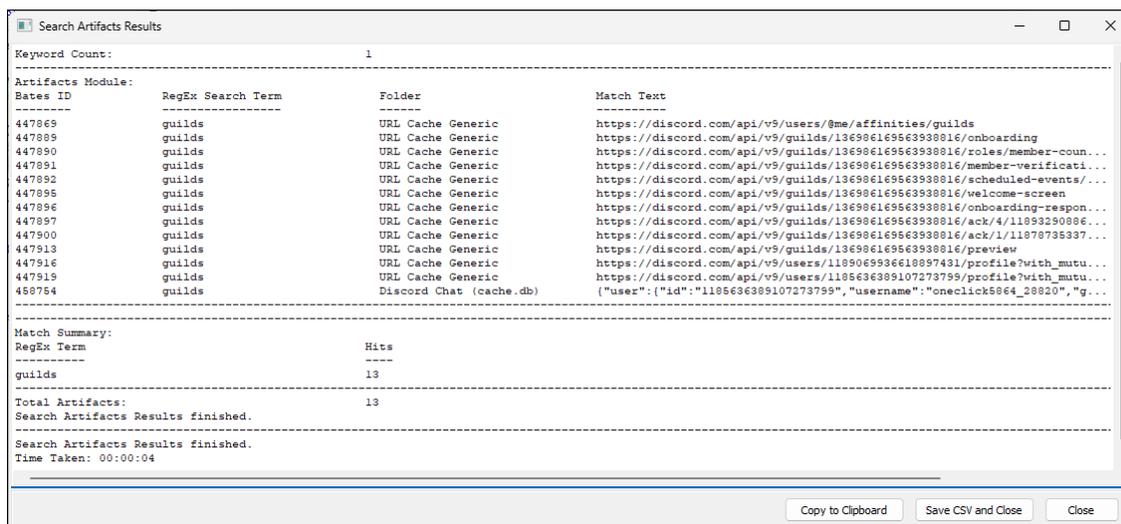
**Q7. FORENSIC EXPLORER METHODOLOGY**

**Answer The Call** is likely to be a reference to **Call of Duty**.

In the **Artifacts** module:

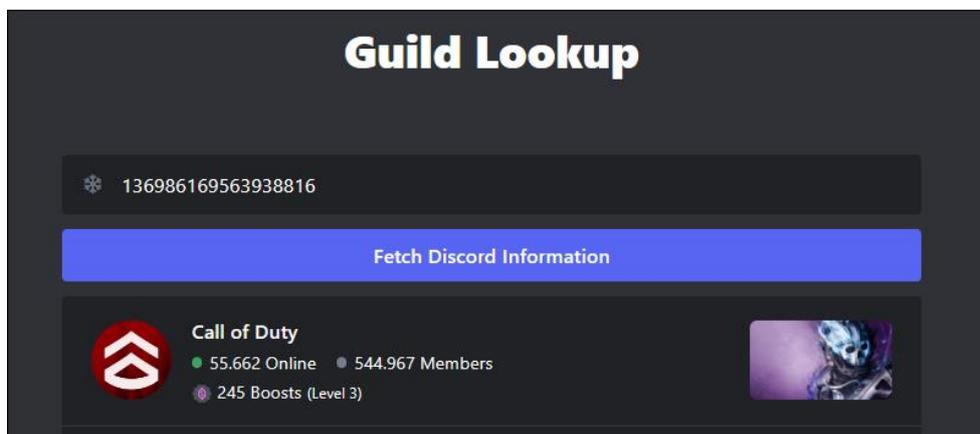
1. Click the **Search Artifact Results** button and search for keyword **guild**.
2. There are multiple hits referencing URLs containing the GUID **136986169563938816**:

Figure 16: Artifacts > Search Artifact Results > Guilds



A **Discord guild lookup** website confirms the guild ID to be for **Call of Duty**:

Figure 13: <https://discordlookup.com/guild/136986169563938816>



**Q8. WARNING SIGNS (5 POINTS)**

*How many days did it take Chad to be warned about his Data Usage?*

**Q8. ANSWER**

Activated 1/12/2023, warning on 17/12/2023.

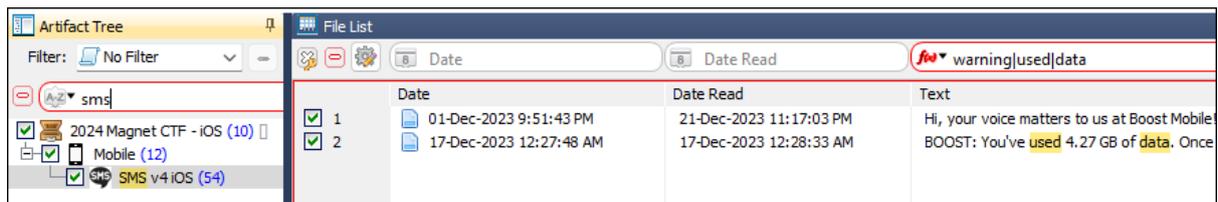
**Q8. FORENSIC EXPLORER METHODOLOGY**

Messages relating to cell phone data usage are usually delivered by SMS.

In the **Artifacts Module**:

1. Locate and select **Mobile > SMS v4 iOS**.
2. Filter the **Text** column for relevant keywords (In the screenshot below, a **RegEx** column filter has been used for **warning|used|data**).

Figure 17: Artifacts > Mobile > SMS v4 iOS > RegEx filter for warning|used|data



## Q9. WATCHING STREAMS TO STAY CURRENT (10 POINTS)

*What is the name of Chad's streaming channel?*

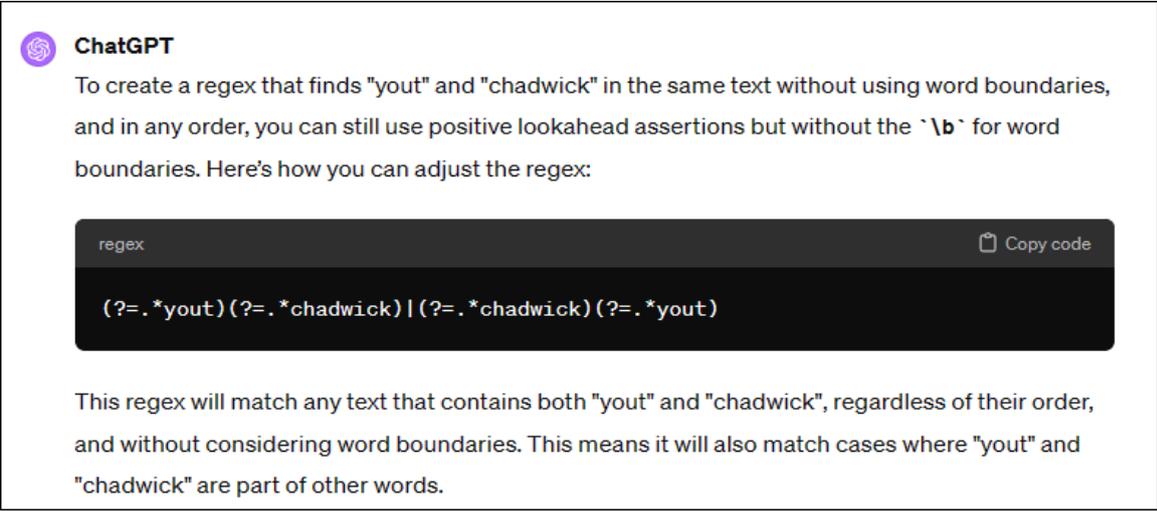
### Q9. ANSWER

ChadwickGames (<https://www.youtube.com/watch?v=xzfqVQWnf7s>).

## Q9. FORENSIC EXPLORER METHODOLOGY

YouTube is the most likely candidate for a streaming channel. To narrow the search, a regex statement can be used to filter artifacts containing both **yout** (YouTube truncate their streaming URLs) and **chadwick**. ChatGPT can be used to create complex regex statements:

Figure 18: ChatGPT > Create a regex statement to locate yout and chadwick



**ChatGPT**

To create a regex that finds "yout" and "chadwick" in the same text without using word boundaries, and in any order, you can still use positive lookahead assertions but without the `\b` for word boundaries. Here's how you can adjust the regex:

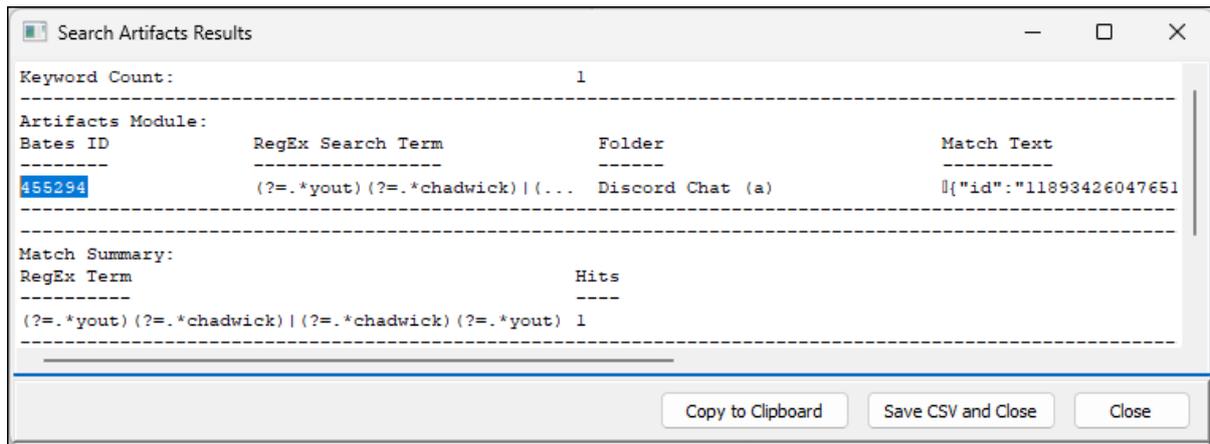
```
regex (?. *yout)(?. *chadwick)|(?. *chadwick)(?. *yout)
```

This regex will match any text that contains both "yout" and "chadwick", regardless of their order, and without considering word boundaries. This means it will also match cases where "yout" and "chadwick" are part of other words.

In the **Artifacts** module:

1. Click the **Search Artifact Results** button and search for the regex statement.
2. The search identifies **Discord Chat** as a potential source.

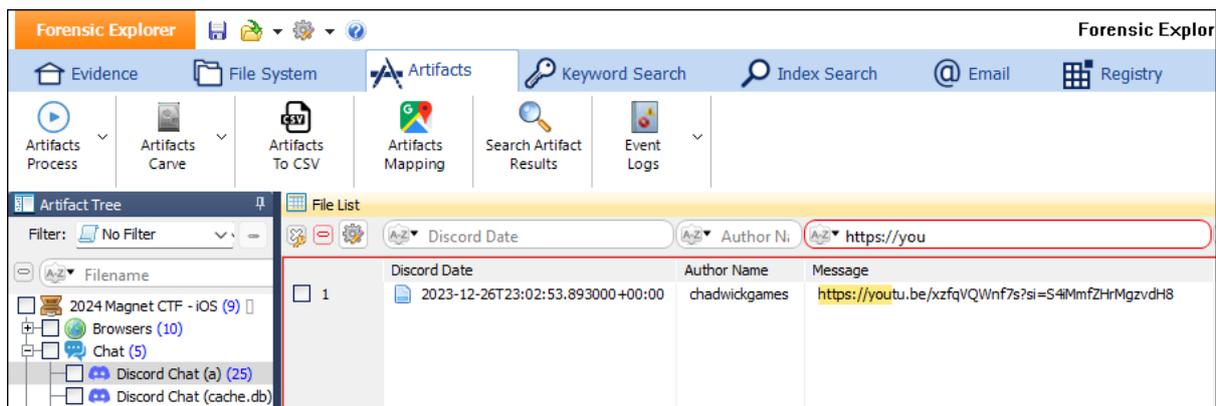
Figure 19: Artifacts > Search Artifact Results



In the **Artifacts** module:

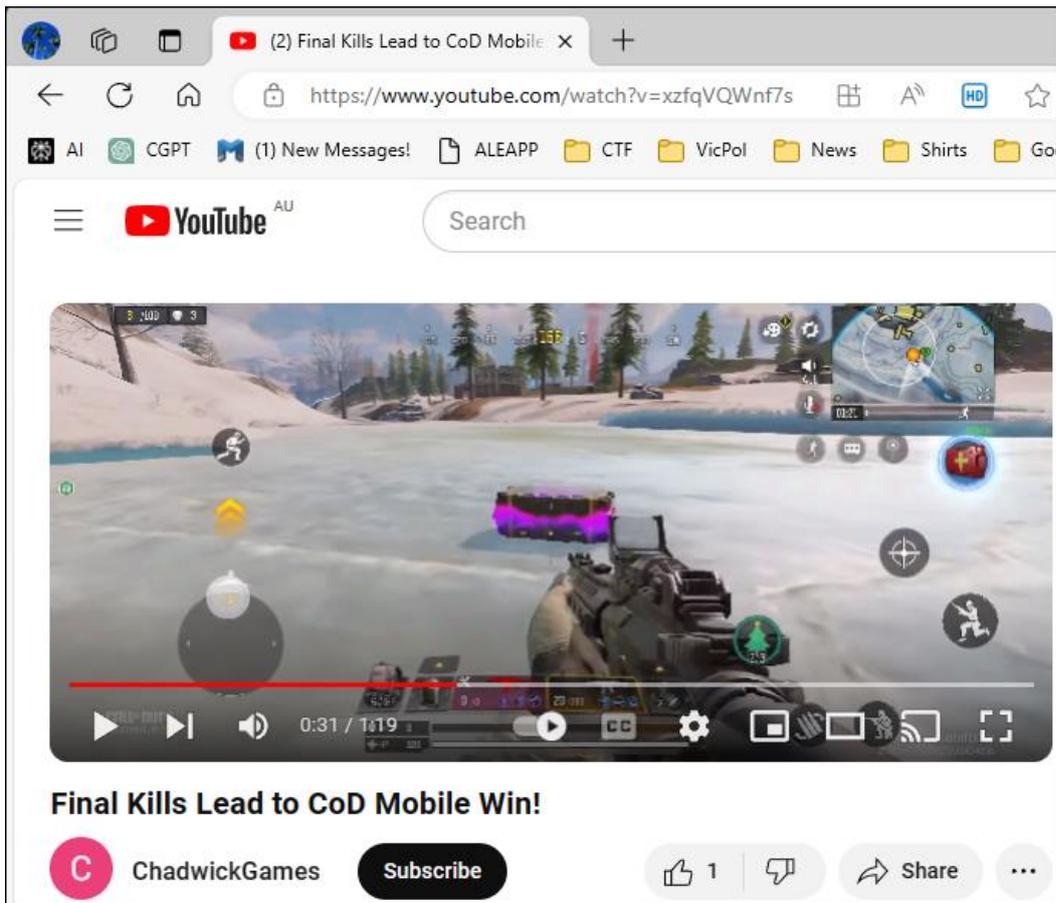
1. Locate and select **Chat > Discord Chat (a)** in the tree.
2. Filter the **Message** column for **yout**.
3. The following URL is located: **https://www.youtube.com/watch?v=xzfqVQWnf7s**

Figure 20: Artifacts > Discord Chat (a)



Visiting <https://www.youtube.com/watch?v=xzfqVQWnf7s> identifies it as the **ChadwickGames** channel.

Figure 21: YouTube > <https://www.youtube.com/watch?v=xzfqVQWnf7s>



**Q10. ONE IS THE LONLIEST NUMBER (10 POINTS)**

*What question did Chadwick ask to AI?*

**Q10. ANSWER**

The following questions were asked of OpenAI:

- "How to make online friends"
- "What is doxing"
- "How to subtly dox without getting caught"
- "How to be a good gamer"

**Q10. FORENSIC EXPLORER METHODOLOGY**

In the **Artifacts** module:

1. Select iOS Application > Biome App Launch iOS to detail programs in use on the iPhone.
2. In the Bundle ID column, filter for ai.
3. Results identify that **com.openai.chat** is in use.

Figure 22: Artifacts > Search Artifact Results

	Created (UTC)	Transition Type	Bundle ID
1	20-Dec-2023 6:44...	com.apple.SpringBoard.transitionRe...	com.apple.mobilemail
2	20-Dec-2023 6:47...	com.apple.SpringBoard.transitionRe...	com.apple.mobilemail
3	24-Dec-2023 8:33...	com.apple.SpringBoard.transitionRe...	com.apple.mobilemail
4	24-Dec-2023 8:33...	com.apple.SpringBoard.transitionRe...	com.apple.mobilemail
5	24-Dec-2023 8:52...	com.apple.SpringBoard.transitionRe...	com.apple.mobilemail
6	24-Dec-2023 8:52...	com.apple.SpringBoard.transitionRe...	com.apple.mobilemail
7	24-Dec-2023 8:54...	com.apple.SpringBoard.transitionRe...	com.apple.mobilemail
8	24-Dec-2023 8:54...	com.apple.SpringBoard.transitionRe...	com.apple.mobilemail
9	25-Dec-2023 7:40...	com.apple.SpringBoard.transitionRe...	com.openai.chat
10	25-Dec-2023 7:40...	SBFullScreenSwitcherSceneLiveCont...	com.openai.chat
11	25-Dec-2023 7:40...	SBFullScreenSwitcherSceneLiveCont...	com.openai.chat
12	25-Dec-2023 7:42...	com.apple.SpringBoard.transitionRe...	com.openai.chat
13	26-Dec-2023 10:4...	com.apple.SpringBoard.transitionRe...	com.apple.mobilemail
14	26-Dec-2023 10:4...	com.apple.SpringBoard.transitionRe...	com.apple.mobilemail

Settings and output relating to **com.openai.chat** are likely to be stored in the **data** folder of that application. To identify the data folder:

1. Select **iOS Application > App Folder UUID iOS**.
2. Filter the **Application Name** column for **com.openai.chat**.
3. The com.openai.chat data folder is identified as **6BFA5EA3-61CB-4652-A60A-2A955B651E05**.



ChatGPT can be used to read the JSON files:

Figure 25: ChatGPT > Read uploaded JSON files

 **ChatGPT**

Across the provided JSON files, the questions asked by the user and the corresponding user IDs and names (if available) are as follows:

### Questions Asked by the User

- File A0724901-AAEA-4F6A-B5F3-7146F87EC139.json:**

  - "Write a short snarky twitter post about friend betrayal in Canada"
- File B00981C1-4A49-4F45-B4D8-59DFF84412CA.json:**

  - "How to make online friends"
- File DC21BA37-9CBD-4FAD-A67F-B318D1752F24.json:**

  - "How to be a good gamer"
  - "How to subtly dox without getting caught"
  - "Write a tweet asking if people would be interested in a clash of clans YouTube video"
  - "What is doxing"

### User IDs and Names

The JSON files structure does not explicitly provide a user name for the questions asked. User interactions are identified by node IDs and roles within the interaction tree, but these do not translate directly to user names or static IDs that would commonly represent a user's identity in plain text. Each `author` field is specified with a `role`, indicating whether the content was generated by a `user`, `assistant`, or `system`, without further identifying information.

Hence, it's not possible to extract a specific user's name or ID beyond the roles mentioned in the interaction data from the provided files.

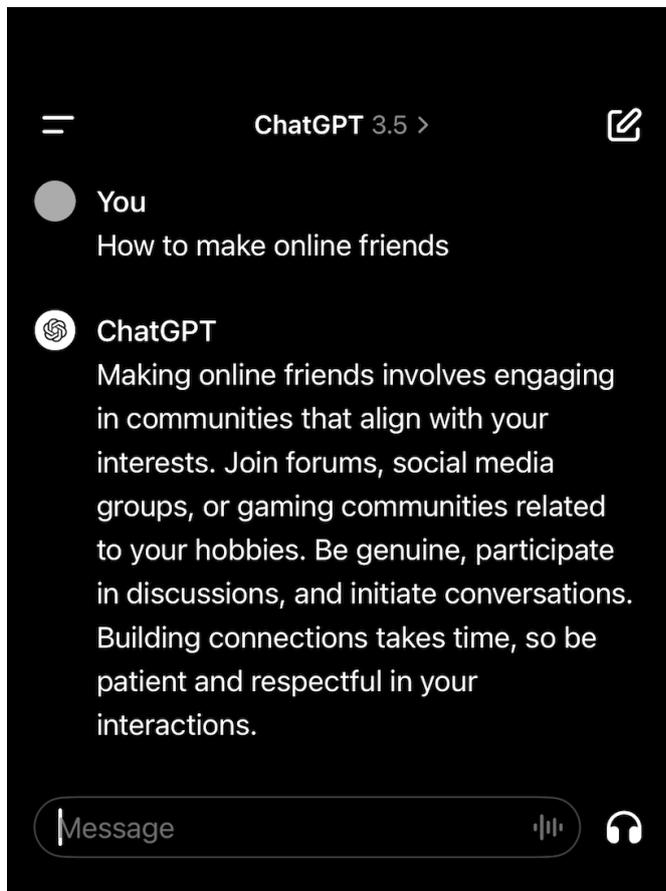
### KTX Screenshot File

iPhone store screenshots in a .KTX format. Forensic Explorer does not currently display .KTX graphics (check back for updates).

KTX files need to be exported and converted to PNG using a stand-alone executable, **ios\_ktx2png.exe** (<https://www.swiftforensics.com/2020/07/ktx-to-png-in-python-for-ios-snapshots.html>).

The following KTX screenshot was located:

Figure 26: private\var\mobile\Containers\Data\Application\6BFA5EA3-61CB-4652-A60A-2A955B651E05\Library\SplashBoard\Snapshots\sceneID:com.openai.chat-default\downscaled\7661E3A8-D25A-46B5-8B27-E9CDB9E810CD@3x.ktx



**Q11. WATCH ME SUAVELY WIN THIS GAME (10 POINTS)**

*How many kills did Chad have on his CoD Mobile winning game?*

**Q11. ANSWER**

7.

**Q11. FORENSIC EXPLORER METHODOLOGY**

A Call of Duty video was located in a previous question at **ChadwickGames** YouTube streaming channel: <https://www.youtube.com/watch?v=xzfqVQWnf7s>. There are 7 kills in this video.

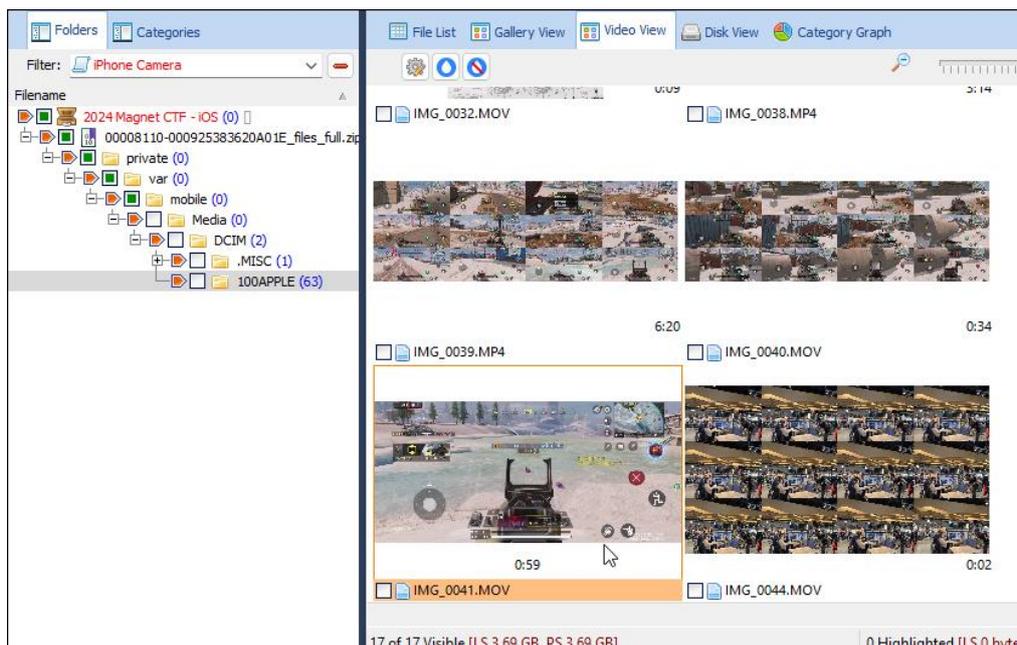
Figure 27: IMG\_0041.MOV



To search for a local copy of the video:

1. In the File System module, branch plate [ ] the entire case.
2. Switch to Video view.
3. The Folder filter for **iPhone Camera** can also be applied to narrow the search.
4. The video is located at: **private\var\mobile\Media\DCIM\100APPLE\IMG\_0041.MOV**

Figure 28: private\var\mobile\Media\DCIM\100APPLE\IMG\_0041.MOV



**Q12. FOR WHEN I CANT FIND MY GEAR (10 POINTS)**

*What outdoor activity store did Chadwick Visit?*

**Q12. ANSWER**

Neptune Mountaineering, 633 S Broadway unit a, Boulder, CO 80305, United States.

**Q12. FORENSIC EXPLORER METHODOLOGY**

The use of “Find My” in the question title is likely a hint to the iOS **Find My** function to track devices.

**Artifacts > Locations > Find My Devices iOS** provides a latitude and longitude of **39.9840754545505, -105.249818957094**.

Figure 29: Artifacts > Locations > Find My Devices

Timestamp	Model Display Name	Map Address	Latitude	Longitude
27-Dec-23 11:00:27 PM	iPhone	613 S Broadway, Boulder, CO 80305	39.984075454...	-105.249818957094

Entering these co-ordinates into **Google Maps** shows the location to be close to **Neptune Mountaineering**, 633 S Broadway unit a, Boulder, CO 80305, United States.

Figure 30: Google Maps > 39.9840754545505, -105.249818957094



**Q13. JUST A COUPLE STEPS AWAY (10 POINTS)**

*How many steps did Chad take on 12/3/2023?*

Q13. ANSWER

$272 + 299 + 175 + 222 = 968$

**Q13. FORENSIC EXPLORER METHODOLOGY**

In the Artifacts module, select **Health Apps > Apple Health Steps**.

Figure 31: Artifacts > Health Apps > Apple Health Steps

	Start Date	End Date	Steps Taken	Provenance
<input type="checkbox"/> 1	03-Dec-2023 6:47:37 PM	03-Dec-2023 6:50:22 PM	272	iPhone14,7
<input type="checkbox"/> 2	03-Dec-2023 7:18:44 PM	03-Dec-2023 7:21:28 PM	299	iPhone14,7
<input type="checkbox"/> 3	03-Dec-2023 9:11:59 PM	03-Dec-2023 9:15:43 PM	175	iPhone14,7
<input type="checkbox"/> 4	03-Dec-2023 11:36:34 PM	03-Dec-2023 11:38:30 PM	222	iPhone14,7

The **Source Name** and **Path** columns identify the source file as:

- `\private\var\mobile\Library\Health\healthdb_secure.sqlite`

To locate and examine the source `healthdb_secure.sqlite`:

1. In the **File System** module, branch plate [  ] the entire case.
2. In the **Filename** column, filter for `healthdb_secure.sqlite`.
3. Change to **Display View** to show the content of the SQLite **samples** table.

Figure 32: File System > healthdb\_secure.sqlite > Display View

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

- Navigation Bar:** File List, Gallery View, Video View, Disk View, Category Graph.
- Address Bar:** healthdb\_secure.sqlite
- Filtering:** Ext, File Signature, Extension.
- File List Table:**

	Filename	Ext...	File Signature	Extension Mism
<input type="checkbox"/> 1	healthdb_secure.sqlite	sqlite	SQLite	No
<input type="checkbox"/> 2	healthdb_secure.sqlite-shm	sqlite-...	SQLite SHM	No
<input type="checkbox"/> 3	healthdb_secure.sqlite-wal	sqlite-wal	SQLite WAL	No
- Path:** 00008110-000925383620A01E\_files\_full.zip\private\var\mobile\Library\Health\healthdb\_secure.sqlite
- Summary:** 3 of 442550 Visible [LS 3.7 MB PS 3.7 MB] | 1 Highlighted [LS 2.0 MB PS 2.0 MB] | 1 Checked
- Database Contents Table:**

	DATA_ID *	START_DATE	END_DATE	DATA_TYPE
> .quantity_samples				
> .quantity_series_data				
> .sample_aggregate_caches				
> <b>samples</b>	1	722076460.531398	722076743.617333	8
	2	722076460.531398	722076743.617333	7
	3	722076493.985648	722077335.502489	9
> .schema_user_versions				

**Q14. ANOTHER REGULARLY SCHEDULED PROGRAM (10 POINTS)**

*What Tattoo shop was visited on 12/27/2023?*

**Q14. ANSWER**

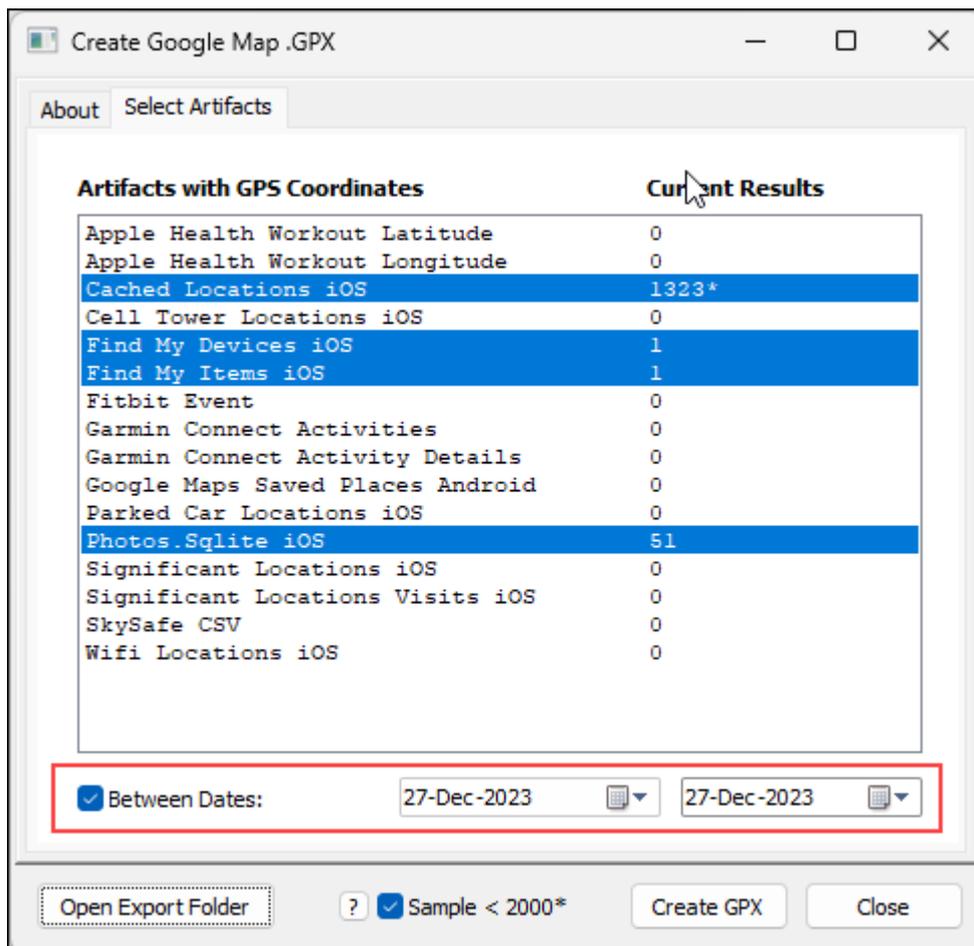
Auspicious Tattoo, 635 S Broadway G, Boulder, CO 80305, United States.

**Q14. FORENSIC EXPLORER METHODOLOGY**

The **Artifacts > Artifacts Mapping** toolbar button can be used to show location activity between dates:

1. In the **Artifacts** module, launch **Artifact Mapping**.
2. Select the items that have current GPS results.
3. Set the required date range for **27 December 2023** and click the **Create GPX** button.

Figure 33: Artifacts > Artifacts Mapping



4. Drag and drop the created GPX files into **Google Earth** or **Google My Maps**.

Figure 34: Google Earth location activity

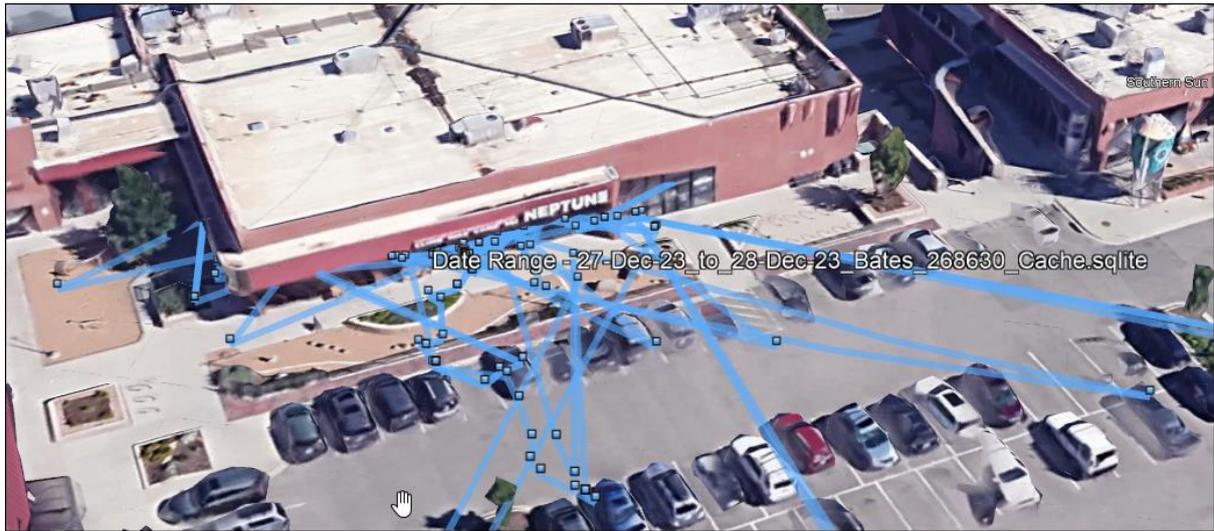


Figure 35: Google Maps showing the location of Auspicious Tattoo

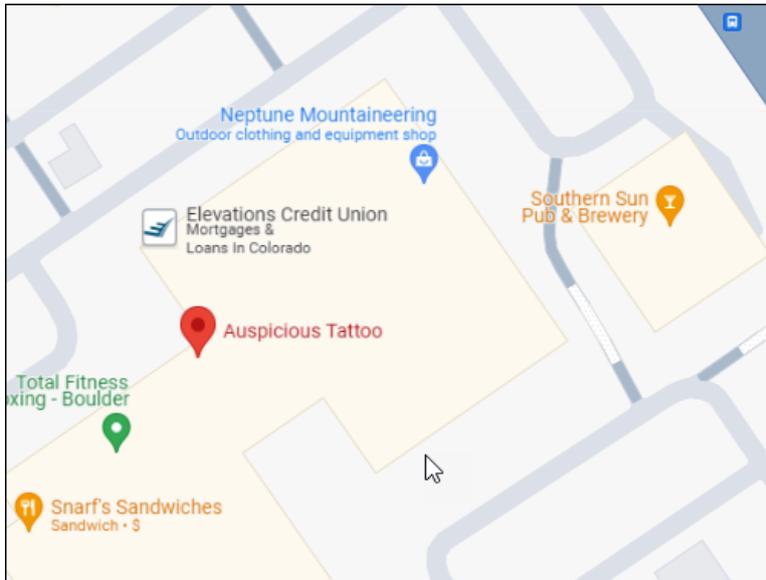
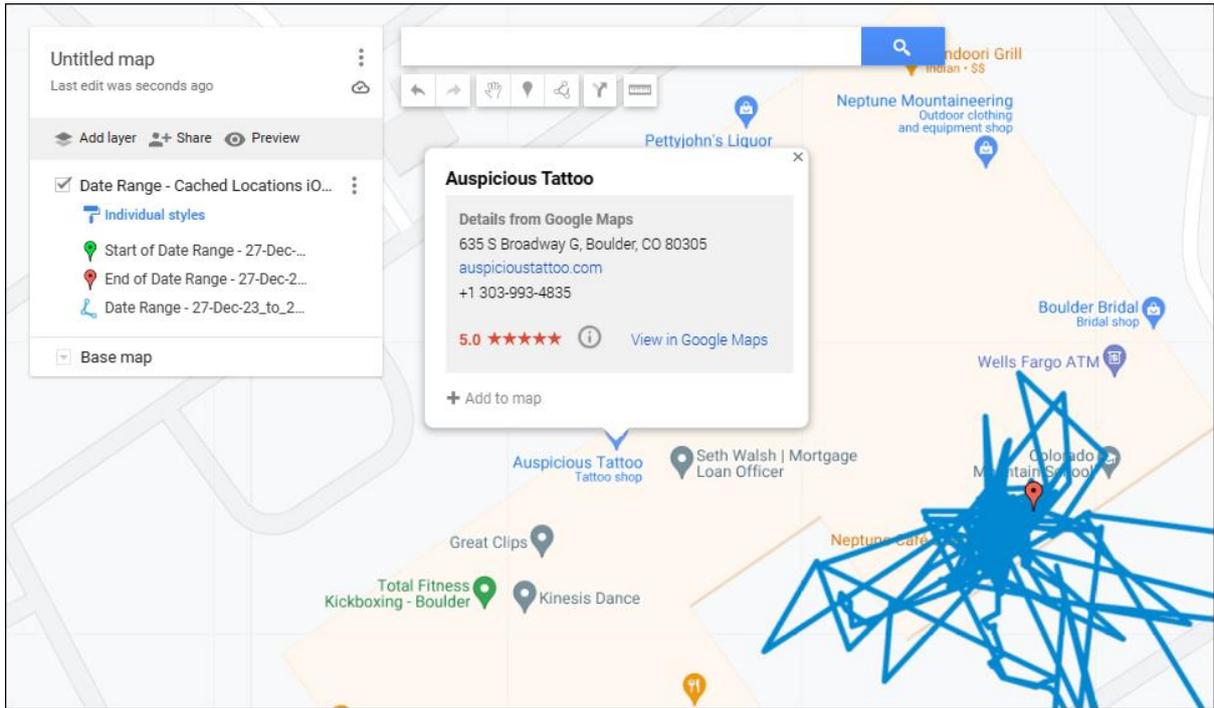


Figure 36: Google Maps > Auspicious Tattoo



Figure 37: Google My Maps > Auspicious Tattoo



**Q15. I HEAR STANLEY CUPS ARE ALL THE RAGE (25 POINTS)**

*What was the final score of the hockey game Chad went to? (home - away)?*

**Q15. ANSWER**

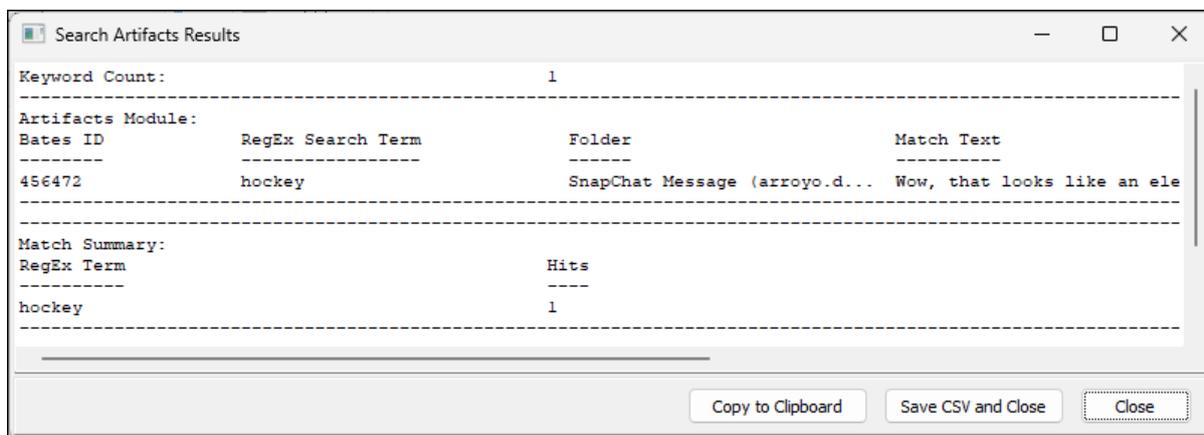
6-4 Senators.

**Q15. FORENSIC EXPLORER METHODOLOGY**

In the **Artifacts** module:

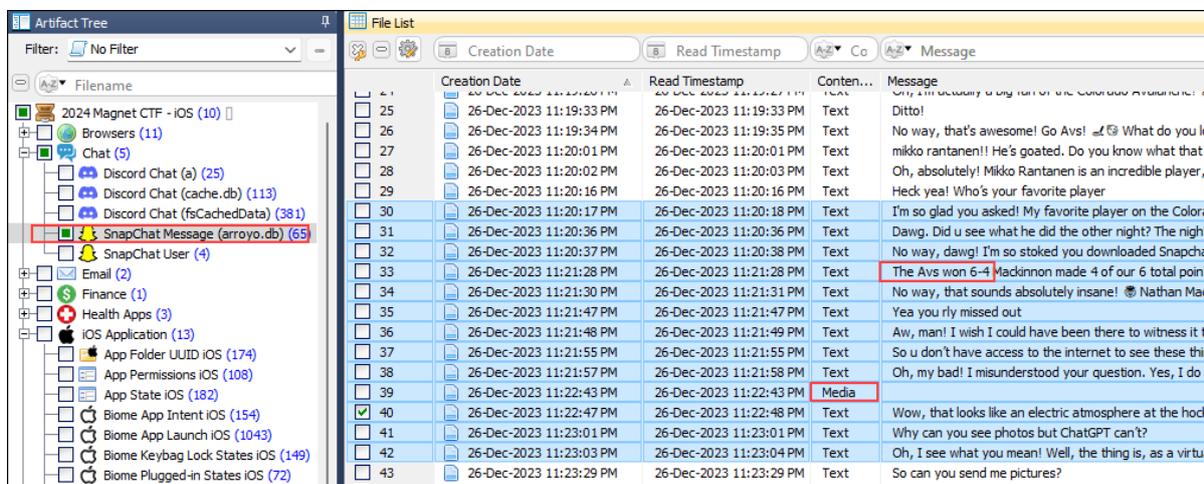
1. Click the **Search Artifact Results** button and search for **hockey**.
2. Results indicate relevant information in Snapchat.

Figure 38: Search Artifact Results > "hockey"



3. Locate the **SnapChat Message (arroyo.db)** folder and filter the **Message** column. Messages located include: *"The Avs won 6-4..."*. Message also references that photos were taken.

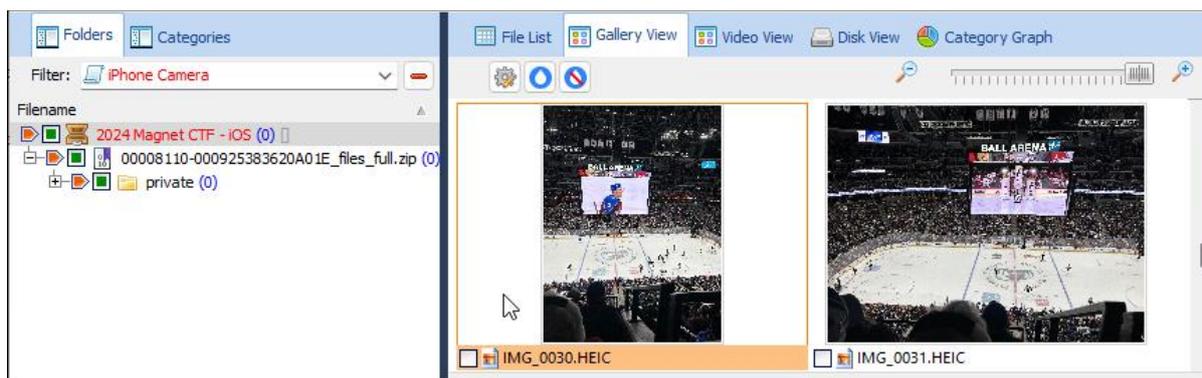
Figure 39: Artifacts > Chat > SnapChat Message (arroyo.db)



To search for photos from this event, In the **File System** module:

1. Branch plate [ ] the entire case.
2. Apply the **iPhone Cameras** folders filter.
3. Switch to **Gallery View** to examine the photos.
4. Photos **IMG\_0030.HEIC** and **IMG\_0031.HEIC** of a hockey match are located. “**Ball Arena**” can be seen on the stadium screen.

Figure 40: File System > Gallery View, IMG\_0030.HEIC, IMG\_0031.HEIC



5. Switch to **File Metadata** in the bottom table to locate the **HEIC metadata**.
6. The date time attributes show the pictures be take on the evening of **21 December 2023**.

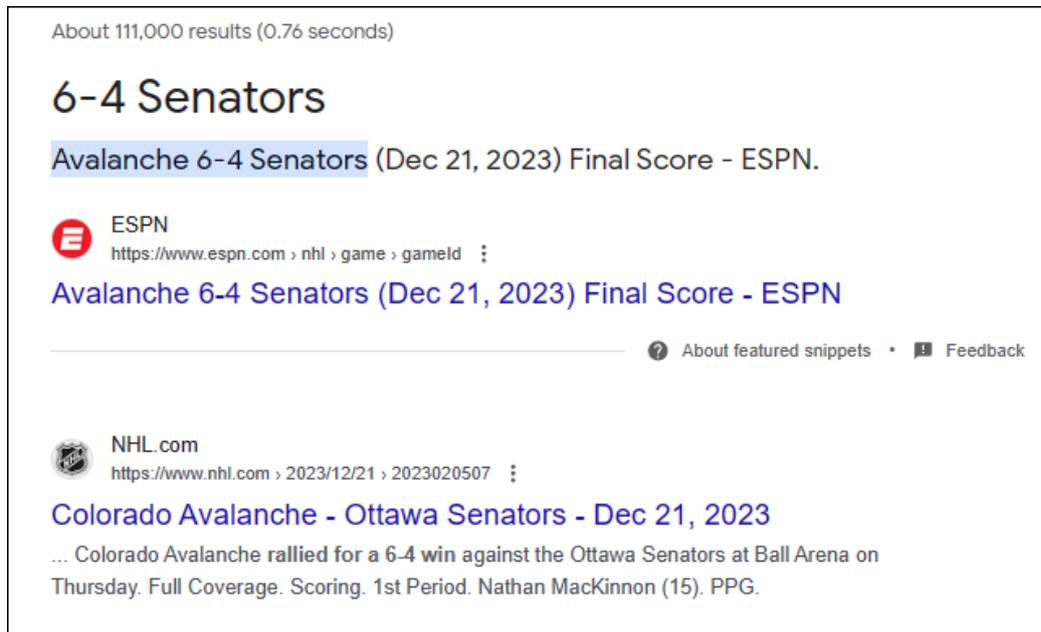
Figure 41: File System > File Metadata

Tag	Value	Value	Type	Offset
Created	2023:12:21 20:23:06	2023:12:21 20:23:06	AString	30376
Tag 316 (Computer)	iPhone 14	iPhone 14	AString	30396
Tag 34665 (ExifTag)	216	216	UInt32	30316
EXIF				
Tag 33434 (ExposureTime)	0.00233100233100233	0.00233100233100233	Double	30808
Tag 33437 (FNumber)	1.5	1.5	Double	30816
Tag 34850 (ExposureProgram)	2	2	Word	30440
Tag 34855 (ISOSpeedRatings)	50	50	Word	30452
Tag 36864 (ExifVersion)	48 50 51 50	48 50 51 50	Byte (4)	30464
Tag 36867 (DateTimeOriginal)	2023:12:21 20:23:06	2023:12:21 20:23:06	AString	30824
Tag 36868 (DateTimeDigitized)	2023:12:21 20:23:06	2023:12:21 20:23:06	AString	30844
Tag 36880	-07:00	-07:00	AString	30864
Tag 36881	-07:00	-07:00	AString	30872
Tag 36882	-07:00	-07:00	AString	30880
Tag 37377 (ShutterSpeedValue)	8.74483528754886	8.74483528754886	Double	30888
Tag 37378 (ApertureValue)	1.16992500210668	1.16992500210668	Double	30896

00008110-000925383620A01E\_files\_full.zip\private\var\mobile\Media\DCIM\100APPLE\IMG\_0030.HEIC

7. A Google search confirms the score from this event to be **Avalanche 6, Senators 4**.

Figure 42: Google search



## Q16. DEVIL IS IN THE DETAILS

*Whose bitmoji is dressed like a devil?*

## Q16. ANSWER

Sofiakhan ([https://images.bitmoji.com/render/panel/10226594-482842799\\_5-s5-v1.png](https://images.bitmoji.com/render/panel/10226594-482842799_5-s5-v1.png)).

## Q16. FORENSIC EXPLORER METHODOLOGY

A **Search Artifact Results** for **bitmoji** did not return relevant information.

A **Keyword Search** for **bitmoji** returned several hits containing the URL reference <https://images.bitmoji.com/render/panel/>.

Figure 43: Keyword Search > “bitmoji”

Filename	Hits	Hit Text
DeliveredNotifications.plist	8	
	1/8	fProcessedByNSE ..suppress bitmojiIn_idVsender ..arroyo_convoy
	2/8	idUtitleXdt_token ..sender bitmoji_url local_message0.S...T.U
	3/8	this!Rdt_Uhttps://images.bitmoji.com/render/panel/10226428-
	4/8	arroyo_convoy_id ..suppress bitmoji ..suppress_in_app ..sender
	5/8	fProcessedByNSE ..suppress bitmoji ..arroyo_convoy_id*ab_cnoti
	6/8	.sender_selfie_id ..sender bitmoji_url local_message0.S...i.U
	7/8	tch this!_Thhttps://images.bitmoji.com/render/panel/10226594-
8/8	reator_icon_url ..suppress bitmoji ..suppress_in_app ..sender	
installed_app_whitelist_url	1	moji\": [{\"bundle_name\": \"Bitmoji\", \"encoding_id\": 1244, \"m
correction_dict_url	9	
	1/9	\"c\": {\"lamodeise\": 0}, {\"q\": \"bitmoji\", \"c\": {\"bitem\": 0, \"bimo\": 0, \"
	2/9	max\", \"c\": {\"baax\": 0}, {\"n\": \"bitmoji free\", \"c\": {\"bitmogi\": 0, \"bi

A second **Keyword Search** for <https://images.bitmoji.com/render/panel/> identified web references to **.png** and **.webp** graphics.

Figure 44: Keyword Search > “https://images.bitmoji.com/render/panel/”

Filename	Hits	Hit Text
DeliveredNotifications.plist	2	
	1/2	6428 ..Chadwick, Watch this!Rdt_Uhttps://images.bitmoji.com/render/panel/10226420-197920250_17-s5-v1.png?tr
	2/2	0226594 ..Chadwick, Watch this!_Thhttps://images.bitmoji.com/render/panel/10226594-482842799_5-s5-v1.png?tra
DuetActivitySchedulerCl...	1	
aps.db	1/1	6594 ..Chadwick, Watch this!Rdt_Uhttps://images.bitmoji.com/render/panel/10226594-482842799_5-s5-v1.png?tra
app_group_plist_storage	2	
	1/2	push.mp3RdpRdtZfrom My AIUfalse_Thhttps://images.bitmoji.com/render/panel/10226021-101443429406_1-s5-v1.webp
	2/2	push.mp3RdpRdtZfrom My AIUfalse_Thhttps://images.bitmoji.com/render/panel/10226021-101443429406_1-s5-v1.webp
	4	
	1/4	..8`aWNS.base[NS.relative.....Thhttps://images.bitmoji.com/render/panel/10226021-101443429406_1-s5-v1.webp
	2/4	le=00..deUNURL.d 0).^8`i.....chhttps://images.bitmoji.com/render/panel/10226021-bbs-101443429406_1-s5-v1.
	3/4	.....*(..0).^8`È.....)Thhttps://images.bitmoji.com/render/panel/10226021-101443429406_1-s5-v1.webp
	4/4	nsparent=l&scale=00).^8`I.....+_chhttps://images.bitmoji.com/render/panel/10226021-bbs-101443429406_1-s5-v1.

Visiting these URLs located the following bitmoji:

Figure 45: [https://images.bitmoji.com/render/panel/10226594-482842799\\_5-s5-v1.png?](https://images.bitmoji.com/render/panel/10226594-482842799_5-s5-v1.png?)



A Keyword Search for **10226594-482842799\_5-s5-v1.png** identified communication from a user called **Sofiakhan**.

Figure 46: Keyword Search > “10226594-482842799\_5-s5-v1.png”

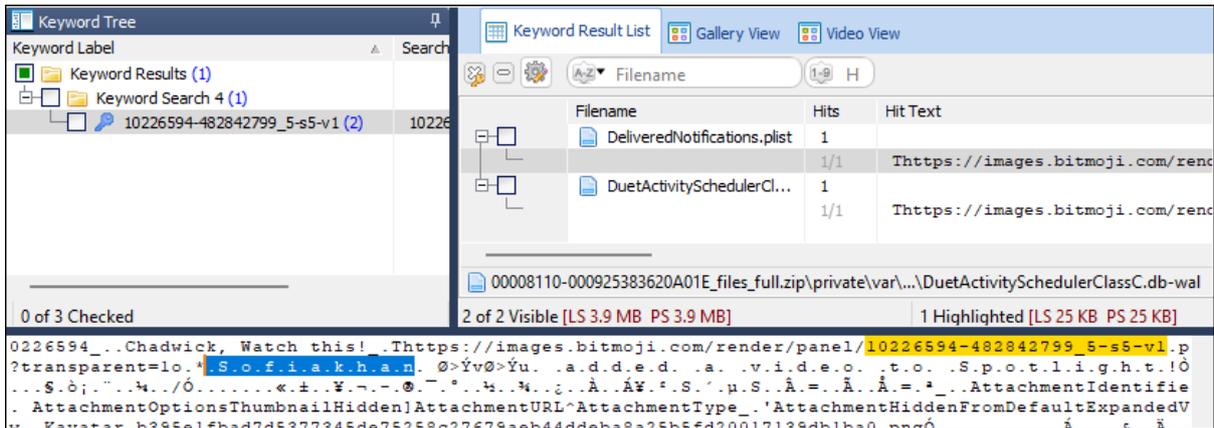
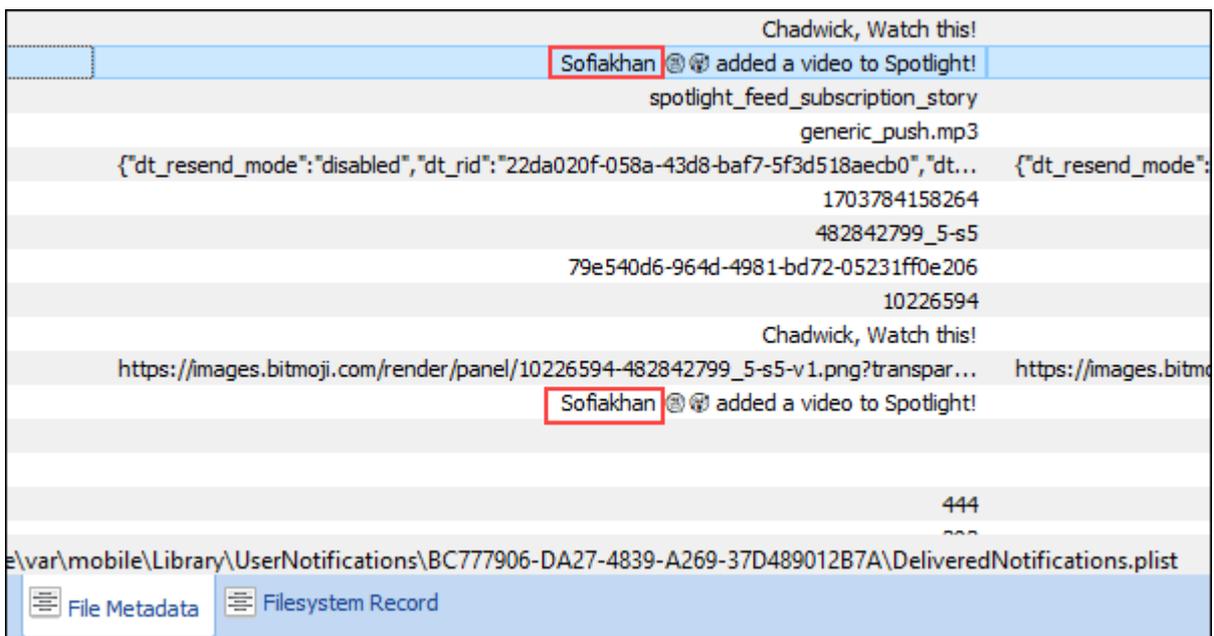


Figure 47: Keyword Search > File Metadata



**Q17. EXCUSE MOI? WHAT DID YOU SAY (25 POINTS)**

*What is the content of the 2nd message that Chad deleted on Dec 18, 2023?*

**Q17. ANSWER**

*That's quite a bold statement considering I'm the one who walked away with a black eye and spent \$30 last night on products to avoid one!*

**Q17. FORENSIC EXPLORER METHODOLOGY**

The message is likely to be a SMS text message. In the Artifacts module:

1. Select **Mobile > SMS v4 iOS**.
2. A deleted message is usually indicated by a blank **Text** column, with message text shown only in the **Attribute Body Carve** column.

Figure 48: Artifacts > Mobile > SMS v4 iOS

	Date	Date Read	Text	Attributed Body Carve
25	17-Dec-2023 11:51:55 PM	18-Dec-2023 12:14:37 AM	Tonight is the last night I can get ...	Tonight is the last night I can get ...
26	18-Dec-2023 12:42:34 AM		You're the goat! You want to mee...	You're the goat! You want to m...
27	18-Dec-2023 12:50:09 AM	18-Dec-2023 1:34:12 AM	For sure, 20 pieces for \$100	For sure, 20 pieces for \$100
28	18-Dec-2023 12:51:07 AM	18-Dec-2023 1:34:12 AM	Let me know when you are headin...	Let me know when you are hea...
29	18-Dec-2023 1:34:30 AM		1	Let's meet there at 9pm in 26m...
30	18-Dec-2023 1:36:47 AM	18-Dec-2023 2:12:24 AM	Alright I'll be there	Alright I'll be there
31	18-Dec-2023 1:59:22 AM	18-Dec-2023 2:12:24 AM	Just got here	Just got here
32	18-Dec-2023 2:14:25 AM		How dare you!! Come back here a...	How dare you!! Come back her...
33	18-Dec-2023 2:38:38 AM	18-Dec-2023 10:04:09 AM	No shot after what you did, this m...	No shot after what you did, thi...
34	18-Dec-2023 10:05:26 AM		2	Excuse me?! That's quite a bold...
35	18-Dec-2023 2:28:16 PM		BOOST: Got it! We've received yo...	BOOST: Got it! We've received...
36	20-Dec-2023 6:48:57 PM		Rocco. I will turn you into the polic...	Rocco. I will turn you into the p...
37	20-Dec-2023 10:06:05 PM	21-Dec-2023 6:28:17 AM	Oh yeah? Turn the person you bo...	Oh yeah? Turn the person you...
38	20-Dec-2023 10:07:32 PM	21-Dec-2023 6:28:17 AM	I could also tell them how you basi...	I could also tell them how you b...

**DB Browser For SQLite**

To test this result in a stand-alone SQLite program:

1. In the **File System** module, highlight the **sms.db**, **sms.db-shm**, and **sms.db-wal**, right-click and **Export Folder and Files...**
2. Once exported, navigate to the **sms.db** and open the **sms.db** file with **DB Browser For SQLite** (or similar).
3. The following SQLite query can be used in the **Execute SQL** tab to extract full data with decoded date and times:

Figure 49: SQL query

```

SELECT
  ROWID,
  text,
  attributedBody,
  datetime(date / 1000000000 + 978307200, 'unixepoch') AS DecodedDate
FROM
  message
WHERE
  DecodedDate >= '2023-12-18 00:00:00'
  AND DecodedDate < '2023-12-19 00:00:00'
ORDER BY
  DecodedDate;
    
```

The relevant data is located in the **attributeBody BLOB**.

Figure 50: SMS.db > attributeBody BLOB

The screenshot shows the DB Browser for SQLite interface. On the left, a SQL query is executed, resulting in a table with columns ROWID, text, attributedBody, and DecodedDate. Row 9 is highlighted, showing a NULL text field and a BLOB attributedBody field. On the right, the hex editor view shows the binary data of the BLOB field, which is 1350 bytes long. The hex data is displayed in a grid format, with the first few bytes being 0000 04 0b 73 74 72 65 f1 6d 74 79 70 65 64 81 e8 03.

ROWID	text	attributedBody	DecodedDate
1	26	You're the goat! You want to meet at the Ethan ...	2023-12-18 00:42:34
2	27	For sure, 20 pieces for \$100	2023-12-18 00:50:09
3	28	Let me know when you are heading over there a...	2023-12-18 00:51:07
4	29	NULL	2023-12-18 01:34:30
5	30	Alright I'll be there	2023-12-18 01:36:47
6	31	Just got here	2023-12-18 01:59:22
7	32	How dare you! Come back here and face me lik...	2023-12-18 02:14:25
8	33	No shot after what you did, this money is for pai...	2023-12-18 02:38:38
9	34	NULL	2023-12-18 10:05:26
10	35	BOOST: Got it! We've received your payment of ...	2023-12-18 14:28:16

**Q18. BOOST THIS SERVER**

*What is the 16 character carrier code?*

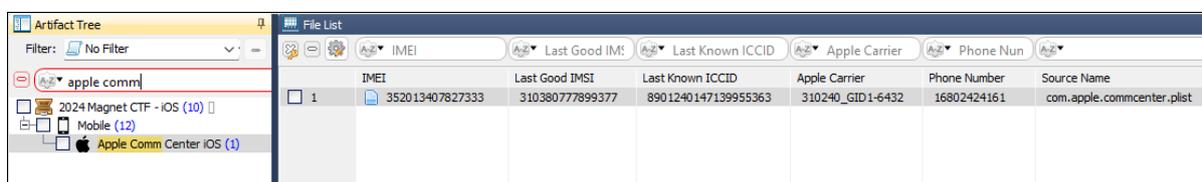
**Q18. ANSWER**

310240\_GID1-6432.

**Q18. FORENSIC EXPLORER METHODOLOGY**

Apple iOS carrier information, including IMEI, IMSI, ICCID and phone number are parsed in the Artifacts module under **Mobile > Apple Comm Center iOS**. This lists the **Apple Carrier** as **310240\_GID1-6432**.

Figure 51: Artifacts > Mobile > Apple Comm Center iOS > Apple Carrier



The screenshot shows the Artifacts module in Forensic Explorer. The left pane shows the artifact tree with 'Apple Comm Center iOS' selected. The right pane shows a table of artifacts with the following data:

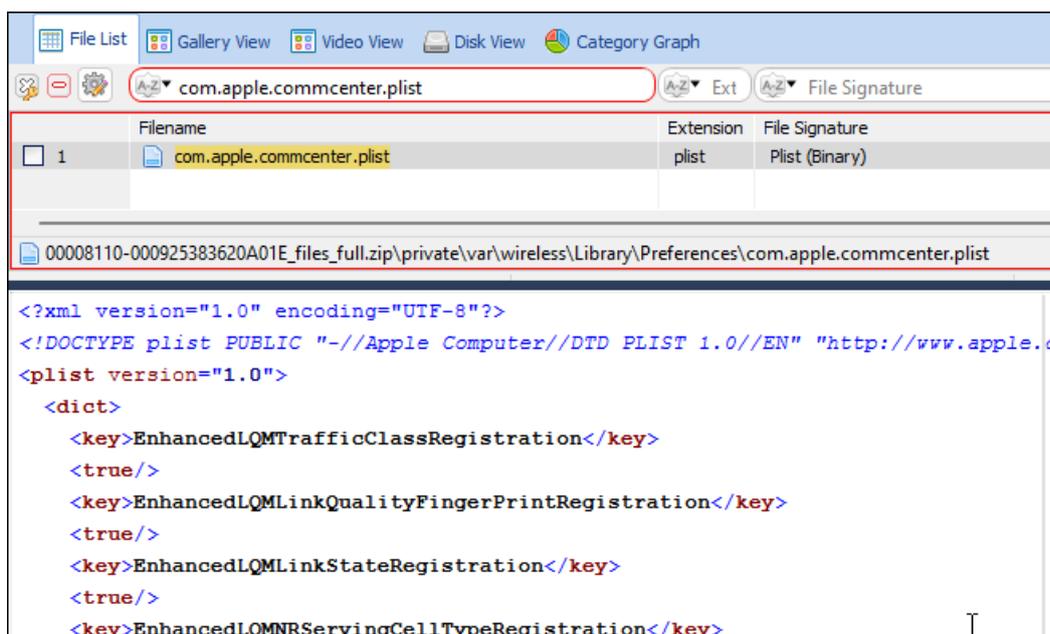
IMEI	Last Good IMSI	Last Known ICCID	Apple Carrier	Phone Number	Source Name
352013407827333	310380777899377	8901240147139955363	310240_GID1-6432	16802424161	com.apple.commcenter.plist

The source of this data is the file:

- **wireless\Library\Preferences\com.apple.commcenter.plist**

The file can be filtered and examined in the File System module in its XML format:

Figure 52: File System > wireless\Library\Preferences\com.apple.commcenter.plist > Display view

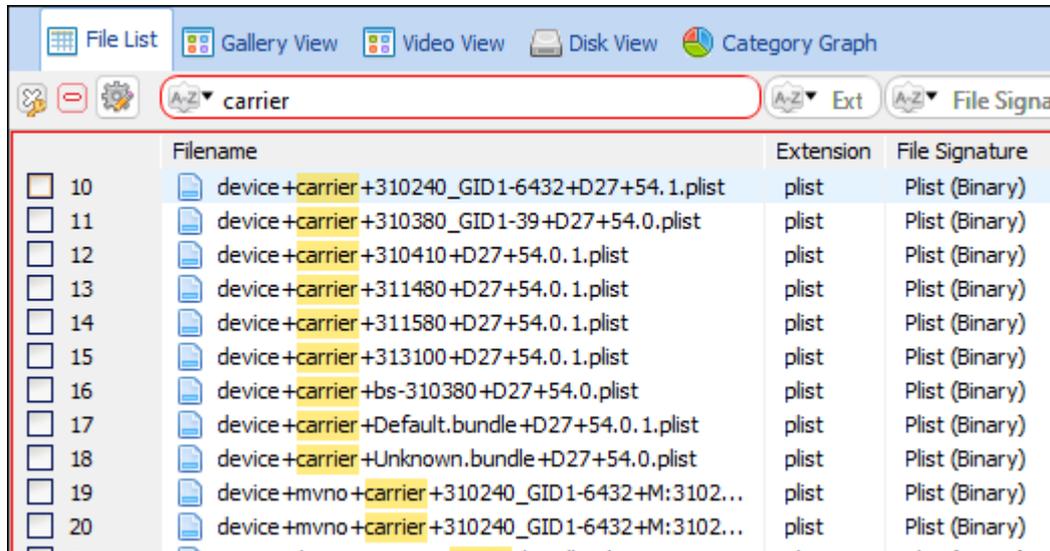


The screenshot shows the File System module in Forensic Explorer. The file 'com.apple.commcenter.plist' is selected, and its XML content is displayed in the main pane. The XML content is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN" "http://www.apple.c
<plist version="1.0">
  <dict>
    <key>EnhancedLQMTrafficClassRegistration</key>
    <true/>
    <key>EnhancedLQMLinkQualityFingerprintRegistration</key>
    <true/>
    <key>EnhancedLQMLinkStateRegistration</key>
    <true/>
    <key>EnhancedLQMNRServingCellTypeRegistration</key>
```

It was also noted that a **File System** module > **Filename** filter for **carrier** located a number of potentially relevant hits:

Figure 53: File System > Filename filter > carrier



The screenshot shows a file system search interface with a search bar containing the text 'carrier'. Below the search bar is a table of search results. The table has four columns: 'Filename', 'Extension', and 'File Signature'. The search results are as follows:

	Filename	Extension	File Signature
<input type="checkbox"/> 10	device+carrier+310240_GID1-6432+D27+54.1.plist	plist	Plist (Binary)
<input type="checkbox"/> 11	device+carrier+310380_GID1-39+D27+54.0.plist	plist	Plist (Binary)
<input type="checkbox"/> 12	device+carrier+310410+D27+54.0.1.plist	plist	Plist (Binary)
<input type="checkbox"/> 13	device+carrier+311480+D27+54.0.1.plist	plist	Plist (Binary)
<input type="checkbox"/> 14	device+carrier+311580+D27+54.0.1.plist	plist	Plist (Binary)
<input type="checkbox"/> 15	device+carrier+313100+D27+54.0.1.plist	plist	Plist (Binary)
<input type="checkbox"/> 16	device+carrier+bs-310380+D27+54.0.plist	plist	Plist (Binary)
<input type="checkbox"/> 17	device+carrier+Default.bundle+D27+54.0.1.plist	plist	Plist (Binary)
<input type="checkbox"/> 18	device+carrier+Unknown.bundle+D27+54.0.plist	plist	Plist (Binary)
<input type="checkbox"/> 19	device+mvno+carrier+310240_GID1-6432+M:3102...	plist	Plist (Binary)
<input type="checkbox"/> 20	device+mvno+carrier+310240_GID1-6432+M:3102...	plist	Plist (Binary)

**Q19. ITS BEEN A LONG TIME (25 POINTS)**

*When did chad last login to Facebook? YYYY-MM-DD HH:MM:SS UTC?*

Q19. ANSWER

2023-12-27 21:34:55.

**Q19. FORENSIC EXPLORER METHODOLOGY**

The **SANS DFPS iOS Apps** poster indicates a potential source as **time\_in\_app\_<User\_ID>.db** stored in the Facebook application data folder.

Figure 54: SANS\_DFPS\_iOS-APPS-v1.2\_09-22.pdf

APPSTORE URL: <https://apps.apple.com/us/app/facebook/id284882215>

Internal App Path	File Name	File Type
/Documents/	time_in_app_<User_ID>.db	SQLite
/Library/Caches/com.facebook.Facebook.MosaicGImageDiskCache/	*	Various
/Library/Caches/graphStoreDB/	GraphStore_<User_ID>.sqlite3	SQLite
/Library/Caches/messenger_contacts.<GUID>/	fbsyncstore.db	SQLite
/Library/Caches/search_bootstrap.<GUID>/search/	graph_search_entity_bootstrap.data	File
/Library/Caches/video_cache.<GUID>/storage/	*	Plist
/Library/Preferences/	com.facebook.Facebook.plist	Plist

REFERENCES:

- [https://www.academia.edu/10726810/Social\\_Media\\_Forensics\\_on\\_Mobile\\_Devices](https://www.academia.edu/10726810/Social_Media_Forensics_on_Mobile_Devices)
- <https://www.tandfonline.com/doi/abs/10.1080/00450618.2015.1066854?src=recsys&journalCode=tajf20>
- [https://www.fbiic.gov/public/2011/jul/Facebook\\_Forensics-Finalized.pdf](https://www.fbiic.gov/public/2011/jul/Facebook_Forensics-Finalized.pdf)
- [https://www.researchgate.net/publication/224221519\\_Third\\_Party\\_Application\\_Forensics\\_on\\_Apple\\_Mobile\\_Devices](https://www.researchgate.net/publication/224221519_Third_Party_Application_Forensics_on_Apple_Mobile_Devices)
- <https://www.diva-portal.org/smash/get/diva2:651693/fulltext01.pdf>

The Artifacts module **iOS Application > App Folder UUID iOS** shows the Facebook data folder to be **BF2FEA88-C397-405D-90EE-A56B2720896C**.

Figure 55: Artifacts > iOS Application > filter by Application Name > "Facebook"

Artifact Tree: Filter: No Filter

- 2024 Magnet CTF - iOS (10)
- Browsers (11)
- Chat (5)
- Email (2)
- Finance (1)
- Health Apps (3)
- iOS Application (13)
  - App Folder UUID iOS (174)
  - App Permissions iOS (108)

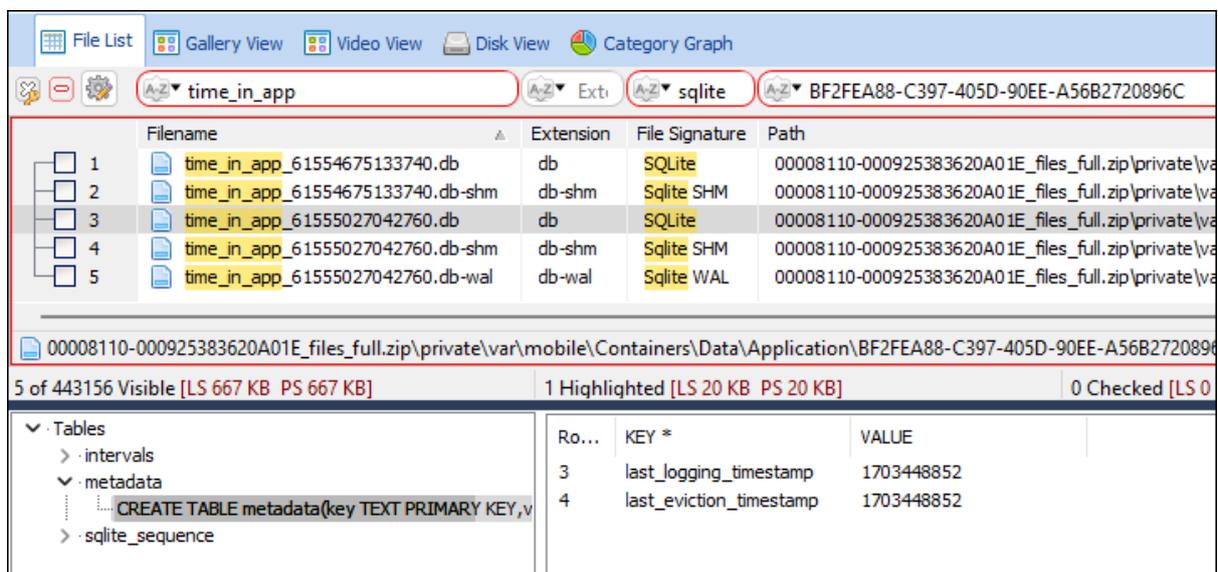
File List: Filter: UUID, Application Name: facebook

UUID	Application Name
BF2FEA88-C397-405D-90EE-A56B2720896C	com.facebook.Facebook

To locate the relevant **time\_in\_app** files:

1. In the **File System** module, branch plate [  ] the entire case.
2. Filter the **Filename** column for **time\_in\_app**.
3. Filter the **File Signature** column for **SQLite**.
4. Filter the **Path** column for **BF2FEA88-C397-405D-90EE-A56B2720896C**.
5. The UUID in filename **time\_in\_app\_61555027042760.db** is known to be the Facebook account of **Chadwick Elms** which can be resolved at URL <https://www.facebook.com/profile.php?id=61555027042760>.

Figure 56: Locating Facebook time\_in\_app files.



6. In the **File System Display View**, the **metadata** table identifies the **last\_login\_timestamp** as **1703448852**.
7. Decode this timestamp in **Digital Detectives DCode** software to be **Unix Seconds (UTC)**, **2023-12-27 21:34:55.000000 Z**.

**Q20. CAN ANYONE KELP (25 POINTS)**

*What game was Chad asking to know the strategy to?*

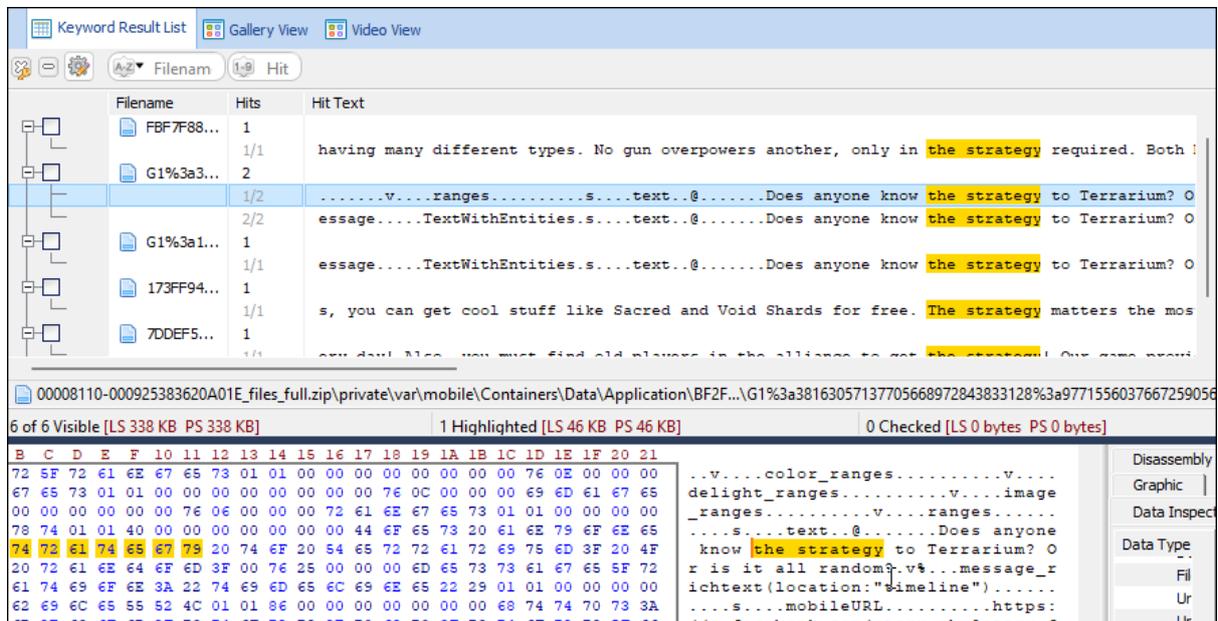
**Q20. ANSWER**

Terrarium: Garden Idle.

**Q20. FORENSIC EXPLORER METHODOLOGY**

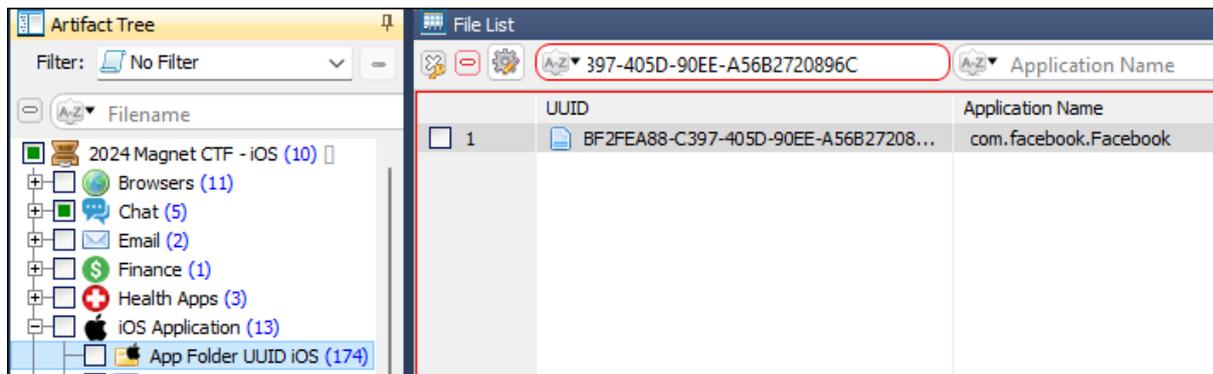
In the **Keyword Search** module, run a keyword search for “**the Strategy**”. Hits are located relating to **Terrarium**.

Figure 57: Keyword Search > “the strategy”



The path to the keyword hit files contain the directory **BF2FEA88-C397-405D-90EE-A56B2720896C**. The Artifacts module > **iOS Application** > **App Folder UUID iOS** identifies this as the Facebook data folder.

Figure 58: Artifacts > iOS Application > App Folder UUID iOS



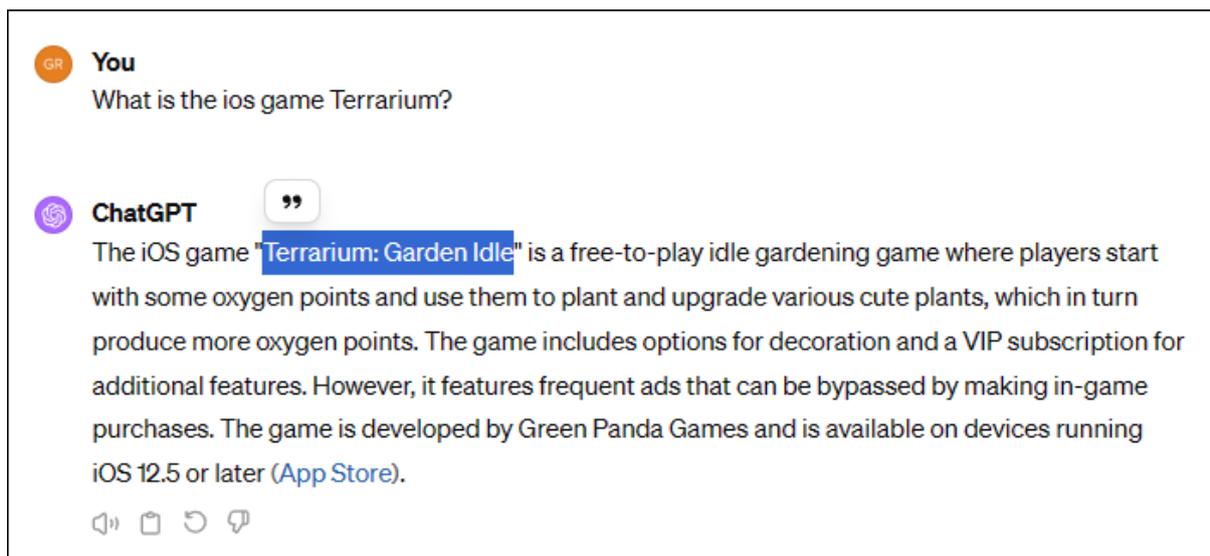
A check of the previously identified Facebook account of chadwick, <https://www.facebook.com/profile.php?id=61555027042760>, finds a message relating to Terrarium on the main page:

Figure 59: Facebook > <https://www.facebook.com/profile.php?id=61555027042760>



ChatGPT identified the full name of Terrarium to be “**Terrarium: Garden Idle**”.

Figure 60: ChatGPT



**Q21. CHAT GPT IS MY PREFERENCE FOR AI (25 POINTS)**

*What is the ChatGPT userID associated with chawickmr95@gmail.com?*

**Q21. ANSWER**

user-xurgQQxumvrujH5ESG17Yhcw.

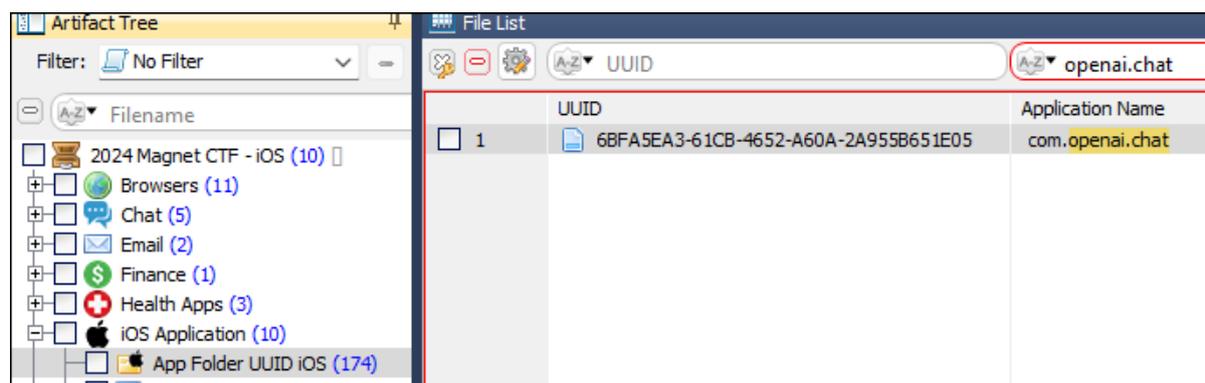
**Q21. FORENSIC EXPLORER METHODOLOGY**

It is likely that user ID configuration for an iOS application will be located within the data folder for that application. iPhones usually store this type of information in a plist.

To locate the data folder:

1. Select **Artifacts > iOS Application > App folder UUID iOS**.
2. Filter the **Application Name** column for AI names to locate **com.openai.chat**.
3. The data folder for **com.openai.chat** is **BF2FEA88-C397-405D-90EE-A56B2720896C**.

Figure 61



In the **File System** module:

1. In the **File System** module Branch plate [  ] the entire case and in the **Filename** column, filter for **BF2FEA88-C397-405D-90EE-A56B2720896C**.
2. Check this folder and use the green checkbox to locate the folder in the tree.
3. Branch plate [  ] just the **BF2FEA88-C397-405D-90EE-A56B2720896C** folder so that its content, including sub-folder content, is displayed in the **File List** on the right-hand side.
4. Right-click in the folder tree and **clear all checks**. Then check the entire content of the **BF2FEA88-C397-405D-90EE-A56B2720896C** folder.
5. In the **Keyword Search** module, run a keyword search on **checked items only** for **chawickmr95@gmail.com**. Two files are located:

Figure 62

Filename	Hits	File Signat...	Hit Text
com.openai.chat.StatsigService.plist	1	Plist (Binary)	vrujH5ESG17Yhcw_..chadwickmr95@gmail.com_..
Cache.db-wal	13	Sqlite WAL	hcw",. "email": "chadwickmr95@gmail.com",
	1/13		"Personal org for chadwickmr95@gmail.com",
	2/13		G17Yhcw", "email": "chadwickmr95@gmail.com",
	3/13		

Examine the metadata of **com.openai.chat.StatsigService.plist** to reveal the **userID** to be **user-xurgQ0xumvrujH5ESG17Yhcw**.

Figure 63: com.openai.chat.StatsigService.plist

The screenshot shows the Magnet AXIOM interface. On the left, a file tree is visible with a red circle '1' highlighting a folder. In the center, a file list shows 'com.openai.chat.StatsigService.plist' highlighted with a red circle '3'. On the right, the metadata for this file is displayed, with a red circle '4' highlighting the 'userID' property value: 'user-xurgQ0xumvrujH5ESG17Yhcw'.

Property	Value	Raw
[-] PList (Binary)		
accountID	b5c12911-e3c0-4961-bbe7-aec0a3ec3dd6	b5
planType	free	
userID	user-xurgQ0xumvrujH5ESG17Yhcw	
userEmail	chadwickmr95@gmail.com	

**Q22. READ MY MIND (25 POINTS)**

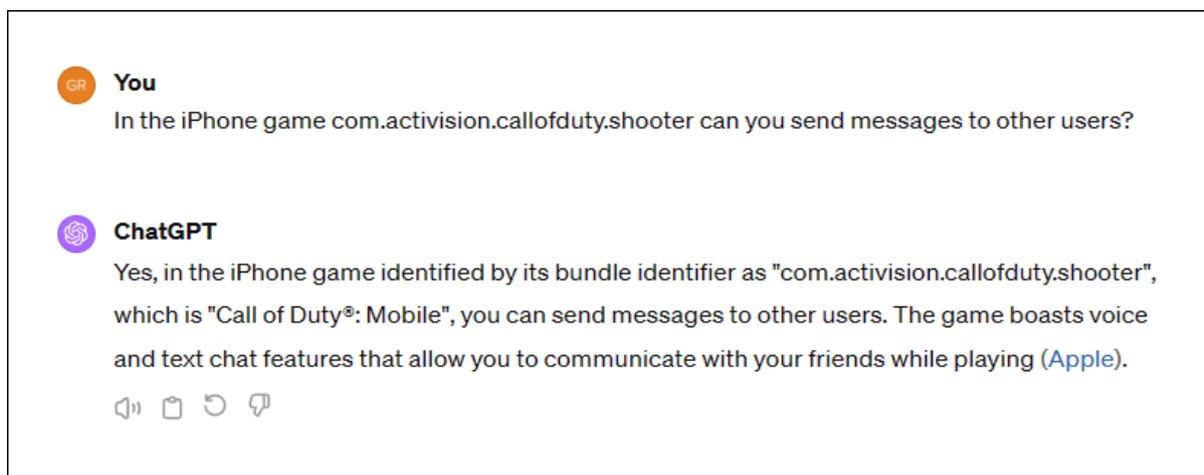
*What message was sent to Rocco in a video game?*

**Q22. ANSWER**

*I know youre reading my messages.*

**Q22. FORENSIC EXPLORER METHODOLOGY**

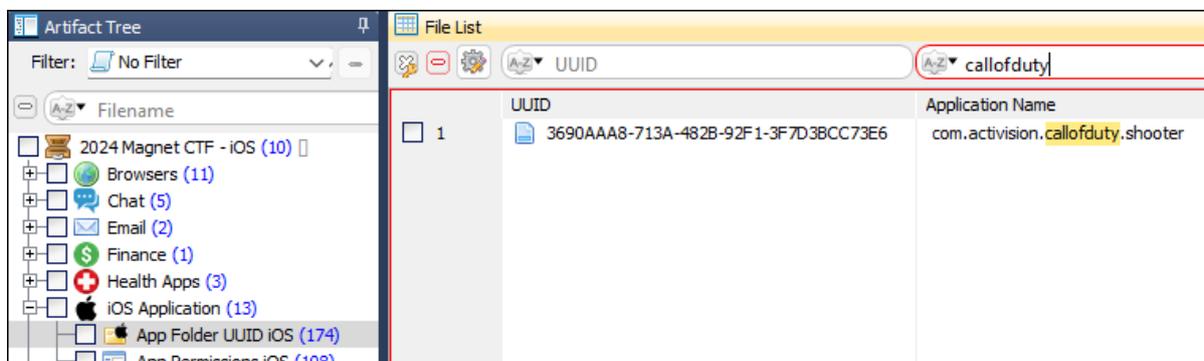
**Call of Duty** is the game that is most noticeable in the artifacts produced. ChatGPT confirms that Call of Duty has in-game messaging capabilities:



The message was therefore likely to be in the Call of Duty data folder. To determine the data folder name:

1. In Artifacts > iOS Applications > select **App Folder UUID iOS**.
2. Filter in the Application name for **callofduty**.
3. The folder UUID is **3690AAA8-713A-482B-92F1-3F7D3BCC73E6**.

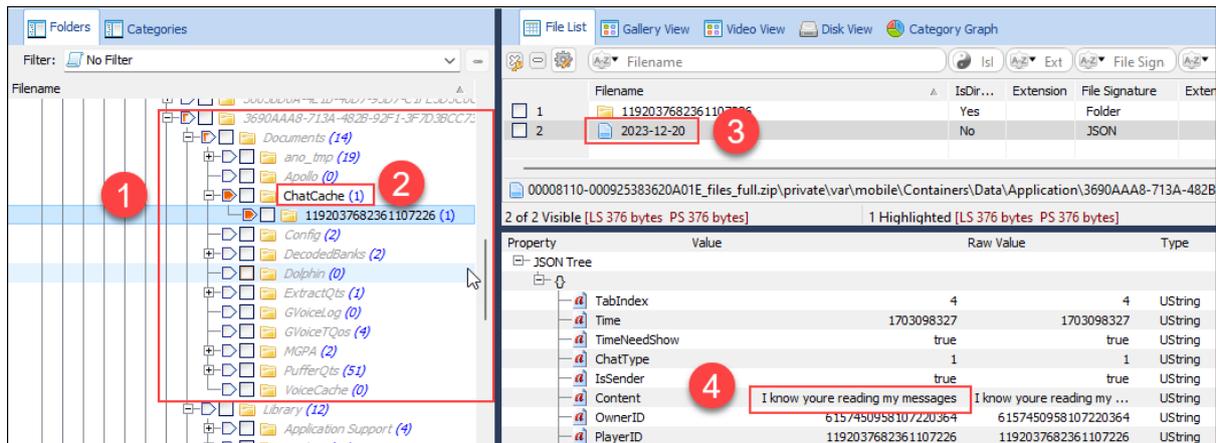
Figure 64: Locating the folder UUID of CallOfDuty



There is no detail in the question as to the potential source file or content of the message. To browse the Call of Duty data folder:

1. In the File System module, filter for the folder: **3690AAA8-713A-482B-92F1-3F7D3BCC73E6**.
2. Perusing the sub-folder structure identifies **ChatCache** as a likely candidate. Branch plate [  ] just that folder to display its contents in the **File List**.
3. The **JSON** file **2023-12-20** looks to hold details of a conversation on that date.
4. In the Hex, Text, Display, or Metadta view the content of the message is shown:

Figure 65: Call of Duty data folder (690AAA8-713A-482B-92F1-3F7D3BCC73E6) > ChatCache > 2023-12-20



**Q23. SEASONS GREETINGS (25 POINTS)**

*What was the first emoji that was sent to Susan?*

**Q23. ANSWER**

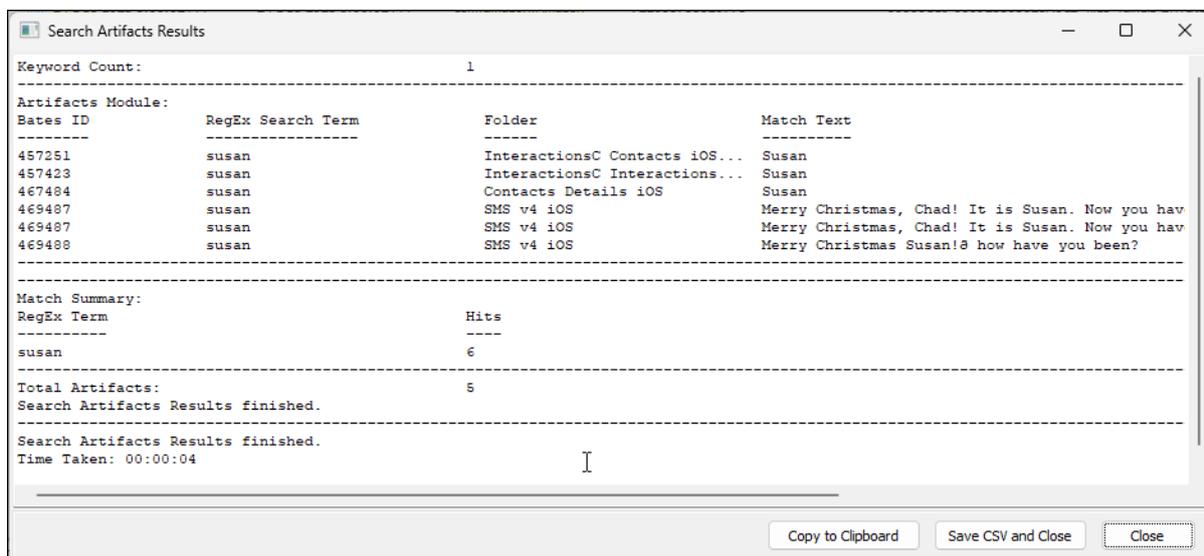
Christmas tree (or possibly a Potted Plant [see below]).

**Q23. FORENSIC EXPLORER METHODOLOGY**

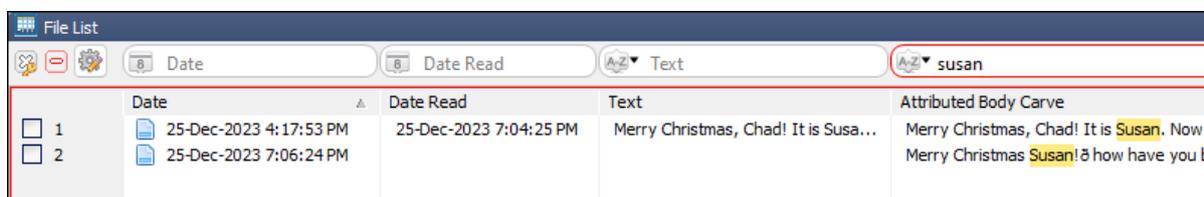
In the **Artifacts** module:

1. Use the **Search Artifact Results** button to run a search for the keyword **susan**.
2. Search results indicate **SMS** to be the source.

Figure 66: Artifacts > Search Artifact Results > “susan”



3. Select **Mobile > SMS v4 iOS** and filter on the **Text** and **Attribute** body columns for **susan**:



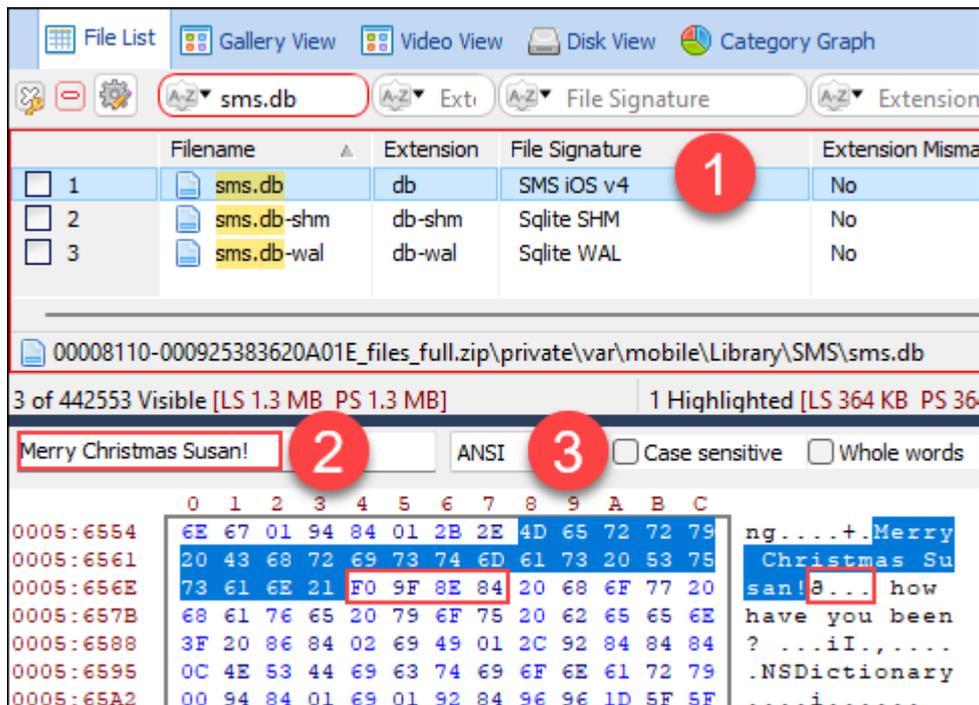
The message dated **25-Dec-2023 7:06:24 PM** contains and emoji. In order to determine the exact emoji, it is necessary to read the raw data. The **source** data is:

- `\private\var\mobile\Library\SMS\sms.db`

To locate and examine **sms.db**:

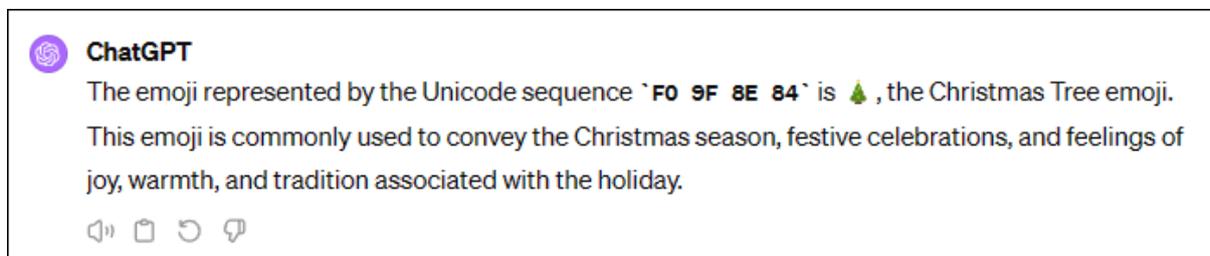
6. In the **File System** module Branch plate [  ] the entire case and in the **Filename** column, filter for **sms.db**.
7. Switch to **Hex** in the bottom window. In the Hex view, press **CTRL F** to open the find bar. Enter the text **Merry Christmas Susan!**
8. Change the search type to **ANSI**. Press the **Find** to locate the text.
9. The first 4 bytes after Merry Christmas Susan! are **F0 9F 8E 84**.

Figure 67: File System > Filename filter for sms.db



10. Search online for the emoji equivalent of **F0 9F 8E 84**.

Figure 68: ChatGPT > “What is the emoji F09F 8E 84?”

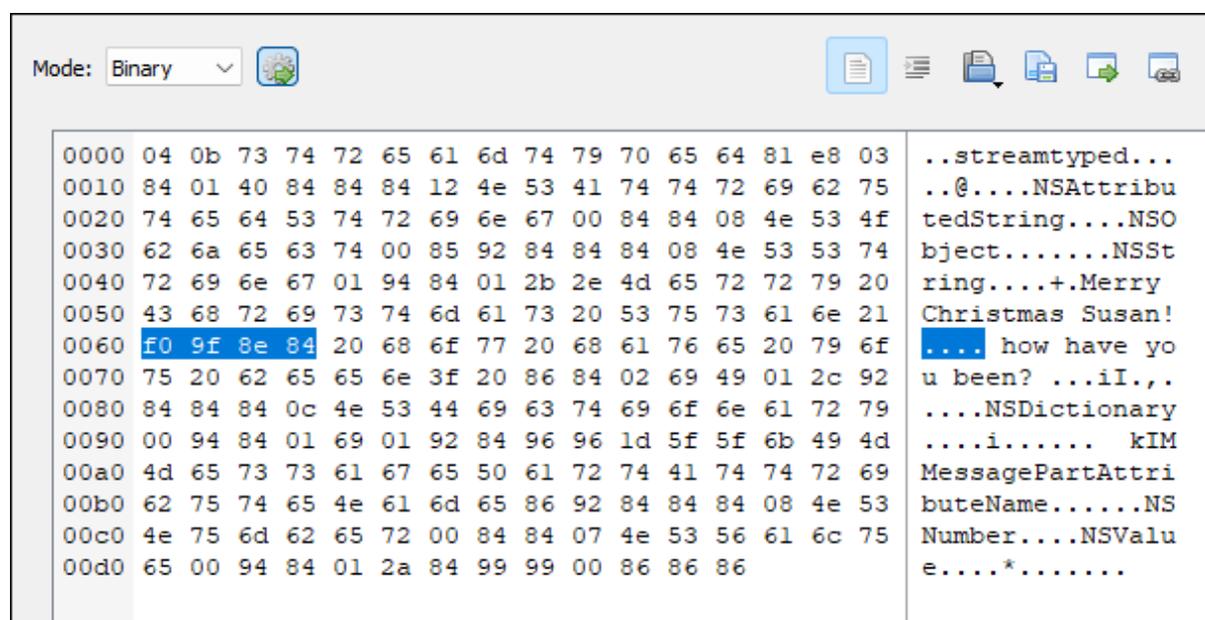


## DB Browser For SQLite

As the data is stored in an SQLite database, which uses -wal (Write Ahead Logic) and -shm (Shared Memory File) it is prudent to undergo the same test using an SQLite program.\

1. In the **File System** module, highlight the **sms.db**, **sms.db-shm**, and **sms.db-wal**, right-click and **Export Folder and Files...**
2. Once exported, navigate to the **sms.db** and open the file with **DB Browser For SQLite**.
3. Using the reference information from the **Artifacts** module **Location** column, navigate to the **message** table, **row 50** and examine the blob data for the **attributedBody** column.
4. The hex data for the emoji is also **F0 9F 8E 84**.

Figure 69: DB Browser for SQLite



## Other SMS data sources

iOS SMS message details are known to be replicated in other files in an iOS device. A **Keyword Search** for **Christmas Susan!** identifies additional files as:

- `_ATXDataStore.db`
- `knowledgeC.db`
- `722972402610564`

It should be noted that in **sms.db**, **sms.db-wal**, and the additional files, there is a variation of how the emoji is stored:

- **F0 9F AA B4** (the third character is stored as AA not 8E).

Figure 70: Keyword Search > Christmas Susan!

Filename	Hits	Hit Text	Hit Offset (File)
_ATXDataStore.db	1	'UbytesO...*-.+.)Christmas Susan! @... how have yo	615530
knowledgeC.db	2	<UbytesO...*-.+.)Christmas Susan! @... how have yo	2285957
	1/2	O..ñ...ê.....)Christmas Susan! @... how have yo	2287959
sms.db	3	tring....+.Merry Christmas Susan!@... how have you	353634
	1/3	tring....+.Merry Christmas Susan!@... how have you	353634
	2/3	...NSString....+)Christmas Susan! @... how have yo	353967
sms.db-wal	3	tring....+.Merry Christmas Susan!@... how have you	354206
	3/3	tring....+.Merry Christmas Susan!@... how have you	354206
	1/3	tring....+.Merry Christmas Susan!@... how have you	965514
	2/3	...NSString....+)Christmas Susan! @... how have yo	965847
	3/3	tring....+.Merry Christmas Susan!@... how have you	966086
722972402610564	2	<UbytesO...*-.+.)Christmas Susan! @... how have yo	262500
	1/2	O..ñ...ê.....)Christmas Susan! @... how have yo	264502
	2/2	O..ñ...ê.....)Christmas Susan! @... how have yo	264502

00008110-000925383620A01E\_files\_full.zip\private\var\mobile\Library\SMS\sms.db

5 of 5 Visible [LS 6.5 MB PS 6.5 MB] 1 Highlighted [LS 364 KB PS 364 KB] 0 Checked [LS 0]

```

F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22
69 73 74 6D 61 73 20 53 75 73 61 6E 21 20 F0 9F AA B4 20 68 String....+)Christmas Susan! @.*" h
6E 3F 20 86 84 02 69 49 01 27 92 84 84 84 0C 4E 53 44 69 63 ow have you been? ...iI.'.....NSDic
66 96 1D 5F 5F 6B 49 4D 4D 65 73 73 61 67 65 50 61 72 74 41 tionary i kIMessagePartA
    
```

Emoji **F0 9F AA B4** represents a **Potted Plant**.

**You**

What is the emoji represented by the Unicode sequence F0 9F AA B4

**ChatGPT**

The Unicode sequence `F0 9F AA B4` represents the emoji 🌿, which is the "Potted Plant" emoji.

Anecdotally it seems more likely that a Christmas message on 25 December would be accompanied by a Christmas tree emoji rather than a potted plant.

**Q24. FOLLOW THE BREADCRUMBS (50 POINTS)**

*How many times did Chad's keyboard become visible within the Amazon app on 12/24/2023?*

**Q24. ANSWER**

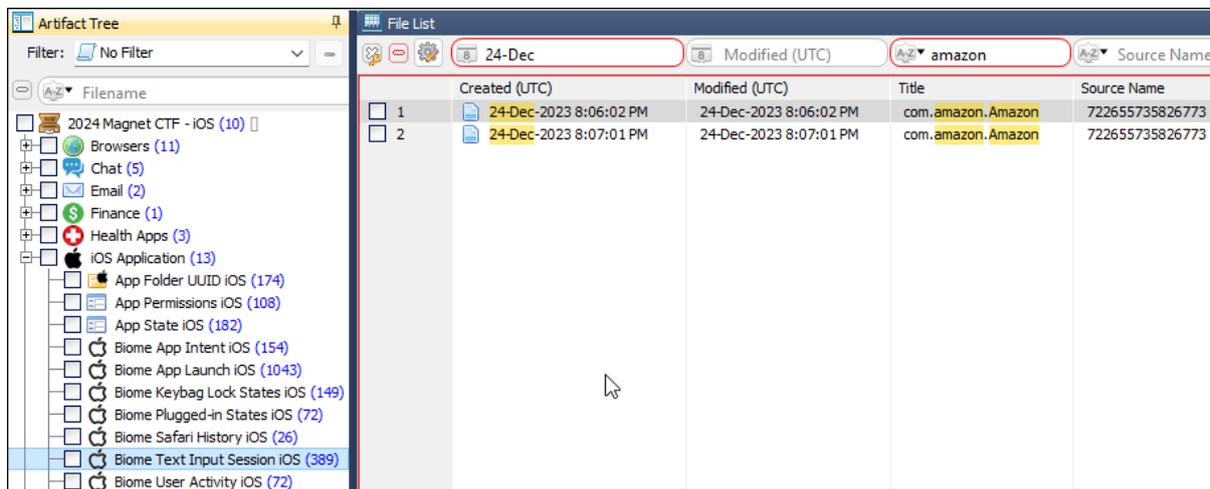
2 times.

**Q24. FORENSIC EXPLORER METHODOLOGY**

In the **Artifacts** module:

1. Select **iOS Application > Biome Text Input Session iOS**.
2. Apply a column filter for **Created (UTC)** and **Title**.

Figure 71: Artifacts > iOS Application > Biome Text Input Session iOS



	Created (UTC)	Modified (UTC)	Title	Source Name
<input type="checkbox"/> 1	24-Dec-2023 8:06:02 PM	24-Dec-2023 8:06:02 PM	com.amazon.Amazon	722655735826773
<input type="checkbox"/> 2	24-Dec-2023 8:07:01 PM	24-Dec-2023 8:07:01 PM	com.amazon.Amazon	722655735826773