MAGNET VIRTUAL SUMMIT 2024 CAPTURE THE FLAG (CTF) IOS

About 1	This CTF Challenge	2
Starting	g this challenge in Forensic Explorer	3
Questic	ons 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:

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

FORENSIC IMAGE SOURCE

Download: https://drive.google.com/drive/folders/1zynwO2BaccA2EOTcRYhKV5CjKuWWU2l6

OTHER ONLINE SOLUTIONS

The following solutions can be found on the web:

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

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

Evidence	
Add device	2024 Magnet CTF - iOS (1)
Add image 🗸	

ARTIFACTS > PROCESS ALL

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

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

Figure 2: Artifacts > Process All

Porensic Explorer	🚵 🔻 🎲 👻 🔮				
🔂 Evidence	File System				
Artifacts Process	Artifacts To CSV				
Process All					
G Process - Biome					
Process - Browsers					
👳 Process - Chat	(0) []				
Process - Cloud					
Process - Email					
S Process - Finance					
🗘 Process - Health					
Process - Locations					
🔹 Process - MAC OS					
Process - Mobile					
Process - Social Media					
Process - Tracking					
Process - Windows OS					

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 Al	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

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

Name:	Chadwick Elms
Phone:	Apple iPhone
Facebook Profile:	https://www.facebook.com/profile.php?id=61555027042760
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"

Search Artifacts Re	sults		– 🗆 X
Keyword Count:		1	
Artifacts Module:			
Bates ID	RegEx Search Term	Folder	Match Text
468913	meet	SMS v4 iOS	incredible. What's the earliest we
468914	meet	SMS v4 iOS	If your local we could meet up aroun
468916	meet	SMS v4 iOS	Sweet. I just happen to be in Burlin
468917	meet	SMS v4 iOS	What do you think about meeting at c
468920	meet	SMS v4 iOS	I'll bring the cash $\circ I$ look forward
468923	meet	SMS v4 iOS	It was so nice meeting you. Let me k
468929	meet	SMS v4 iOS	You're the goat! You want to meet at
Match Summary:			
RegEx Term		Hits	
meet		7	
Total Artifacts:		7	
Search Artifacts I	Results finished.		
Search Artifacts I	Results finished.		1
Time Taken: 00:00	:03		
			Copy to Clipboard Save CSV and Close Close

- 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"

III File List				
ş 🗆 🔯	B Date	B Date Read	is meet	AZT Tyj
	Date	Date Read	Text	Туре
1	17-Dec-2023 4:15:49 PM		incredible. What's the earliest we can we meet up?	Sent
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
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
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
5	17-Dec-2023 4:43:27 PM		I'll bring the cash ③I look forward to meeting you	Sent
6	17-Dec-2023 5:08:46 PM		It was so nice meeting you. Let me know when u want to play another	Sent
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

ChatGPT

A subreddit is a specific community within Reddit where users can share content, post comments, and engage in discussions on a particular topic or theme. Each subreddit is dedicated to a specific subject, ranging from broad topics like news, science, and technology, to very niche interests such as a particular hobby, TV show, or even a meme genre. Subreddits are denoted by the prefix "r/" followed by the community's name, for example, "r/science" for the science community or "r/gaming" for the gaming community.

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/"

Search Artifact	ts Results		- 0 X
Keyword Count:		1	A
Artifacts Modu	le:		
Bates ID	RegEx Search Term	Folder	Match Text
460257		Conformit Claused Table	
460257	reddit.com/r/	Safari Cloud Tabs	www.reddlt.com/r/iwitch/comments/ejqcor/g
460257	reddit.com/r/	Safari Vistory iOSS	https://www.reddit.com/r/iwitch/comments/
460373	reddit.com/r/	Safari History 1050	https://www.reddit.com/r/iwitch/comments/
460374	reddit.com/r/	Salari History 1050	https://www.reddit.com/r/iwitch/comments/
460375	reddit.com/r/	Safari Mistory 1050	https://www.reddit.com/r/iwitch/comments/
460376	reddit.com/r/	Salali History 1050	https://www.feddit.com/f/iwitch/comments/
			noops.//www.ieddio.com/i/intoch/commentos/
			
Match Summary:			
RegEx Term		Hits	
reddit.com/r/		7	
Total Artifact	5:	6	
Search Artifac	ts Results finished.		
Search Artifac	ts Results finished.		
Time Taken: 00	:00:03		
ĺ			
			Copy to Clipboard Save CSV and Close Close
		A	

- 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

🔢 Artifact Tree 🛛 🕂	🔠 File List			
Filter: 💭 No Filter 🗸 🗕	ig 🗆 🔯	8 Visit Date	AZ Hist	₩ https://www.reddit.com/r/
□ A Filename		Visit Date	History I	URL
2024 Magnet CTE (OS (10) []	1	21-Dec-2023 6:31:07 AM	17	https://www.reddit.com/r/Twitch/comments/ejqcof/goo
	2	21-Dec-2023 6:31:07 AM	18	https://www.reddit.com/r/Twitch/comments/ejqcof/goo
Browsers (11)	3	21-Dec-2023 6:31:08 AM	18	https://www.reddit.com/r/Twitch/comments/ejqcof/goo
	4	21-Dec-2023 6:32:04 AM	19	https://www.reddit.com/r/Twitch/comments/ejqcof/goo
Safari Carbe (25)				
Safari Cloud Tab Devices (1)				
Safari Cloud Tabs (11)				
Safari Cookies (78)				
Safari History iOS8 (93)				
- Safari Recent Searches (9)				

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

Search Artifacts R	Results		– 🗆 X
Keyword Count:		2	
Artifacts Module Bates ID	: RegEx Search Term	Folder	Match Text
472170 472209 472215 	annoyed myai myai	SnapChat Message (arroyo.d.) SnapChat Message (arroyo.d.) SnapChat User	Oh no, I'm really sorr: You can call me MyAI!] myai
Match Summary: RegEx Term myai annoyed		Hits 2 1	
Total Artifacts: Search Artifacts	Results finished.	3	
Search Artifacts Time Taken: 00:00	Results finished. 0:04		[
		Copy to Clipboard S	ave CSV and Close Close

- 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.dl	o)		
🔚 Artifact Tree 🛛 🖓	🧮 File List		
Filter: 🖉 No Filter 🗸 🖃	i 🔁 🖗	Creation Date	A₂▼ annoyed
A2 Filename		Creation Date	Message
2024 Magnet CTF - iOS (10) Browsers (11) Chat (5) Discord Chat (a) (25) Discord Chat (cache.db) (113) Discord Chat (fsCachedData) (3 SnapChat Message (arroyo.db) SnapChat User (4)	1	26-Dec-2023 11:27:46 PM	Oh no, I'm really sorry if I've annoyed you. T

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**.

📱 Artifact Tree म	🧮 File List		
Filter: 🔄 No Filter 🗸 😑	i 🖓 🖻 🔯	€ b42f1f70-5a8b-4c53-8c25-34e7ec9ed	SnapChat User
□		SnapChat User ID	SnapChat User Name
2024 Magnet CTF - iOS (10)	1	b42f1f70-5a8b-4c53-8c25-34e7ec9e6781	myai
H Browsers (11)			
Discord Chat (a) (25)			
Discord Chat (cache.db			
- Discord Chat (fsCached			
- SnapChat Message (an			
SnapChat User (4)			

Figure 10: Artifacts > Chat > SnapChat user

Q4. IMAGEINE 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

Salt4n6.com https://salt4n6.com > 2019/09/23 > ios-13-swipe-to-type

iOS 13 – Swipe to Type - Salt Forensics

23 Sept 2019 — This table seems pretty basic, it shows a total number or typed words and the number of words pathed, presumably this second value relates ...

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

≣	File List 🔋 Galler	ry View 🔋 Video View 🔒	Disk View	🕙 Category Graph			
F	🖻 😻 🐼 user_	_model_database.sqlite		AZ▼ File Category	A₂▼ File Sig	nature	AZ Extens
	Filename			File Category	File Signature	1	Extension Mi
	1 📄 user_	model_database.sqlite		Database	SQLite		No
	2 📄 user_	model_database.sqlite-shm		Database	Sqlite SHM		No
	3 📄 user_	model_database.sqlite-wal		Database	Sqlite WAL		No
-							
0 📄	0008110-000925383	620A01E_files_full.zip\privat	te\var\mobi	le\Library\Keyboard\user_model	_database.sq	lite	
3 of 4	442550 Visible [LS 2.	8 MB PS 2.8 MB]	1 H	lighlighted [LS 1.5 MB_PS 1.5 MB]	0 Checked	[LS 0 bytes PS (
~ .	Tables		ROWID *	KEY	VALUE	CREATION_DATE	LAST
	> properues		1	tium.totalWordsTyped	1797	1700963223.71662	17037
v usermodeldurablerecords 2		2	tium.totalWordsFromCandidate	26	1701285205.34421	17037	
CREATE TABLE usermodeldurablerecords (3			3	tium.totalWordsAutocorrected	175	1702662386.82841	17037
	> usermodeltransier	ntrecords					

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

Forensic Explorer	👌 - 🕸	+ 🕜						Forensic
🔂 Evidence	File Systen	n 🔥	Artifacts	P Ke	yword Search	P Index Set	arch 🔘 E	Email 🔠 Registr
Artifacts Process Carve	Artifac To CS	ts Art V Mag	ifacts oping	Search Artifact Results	Event × Logs			
Artifact Tree	Ļ	🛄 File List						
Filter: 🔄 No Filter	× =	🖗 🗆 🔯	AZ Pro	oduct Build	Product Copyr	Product	Product \	(A-Z ▼
			Product E	Build Version P	roduct Copyright	Product Name	Product Version	Source Name
Magnet 2024 CTE - iOS	(9) []	1	📄 20F7	75	1983-2023 Apple Inc	. iPhone OS	16.5.1	SystemVersion.plist
E- MAC Operating Syst	tem (1)							
System Version 1	MacOS (1)							

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: Sys	temVersion.plist				
III File I	ist 😨 Gallery View 😨 Video View 🔚 Disk	View	Categor	y Graph	
🥦 🖻 🏟	▼ SystemVersion.plist	\supset	lsDire	AZ Extensio	n 👰 🛛 File Sig
_	Filename		IsDirectory	Extension	File Signature
1	SystemVersion.plist		No	plist	XML
			c c :		P
000081	10-000925383620A01E_files_full.zip\System\Lib	orary	CoreServices	SystemVersion	.plist
1 of 442550	Visible [LS 572 bytes PS 572 bytes]	1	Highlighted	[LS 572 bytes P	S 572 bytes]
xml v</td <td>rersion="1.0" encoding="UTF-8"?</td> <td>></td> <td></td> <th></th> <td></td>	rersion="1.0" encoding="UTF-8"?	>			
DOCTS</td <td>PE plist PUBLIC "-//Apple//DTD</td> <td>PL</td> <td>IST 1.0//</td> <th>/EN" "http:</th> <td>//www.apple</td>	PE plist PUBLIC "-//Apple//DTD	PL	IST 1.0//	/EN" "http:	//www.apple
<plist< td=""><td>version="1.0"></td><td></td><td></td><th></th><td></td></plist<>	version="1.0">				
<dict></dict>					
	<key>BuildID</key>				
	<string>171F328C-0B65-11EE-94</string>	52-	F5DF3E711	LO1A <td>ıg></td>	ıg>
	<key>ProductBuildVersion<td>></td><td></td><th></th><td></td></key>	>			
	<string>20F75</string>				
	<key>ProductCopyright</key>				
	<pre><string>1983-2023 Apple Inc.<</string></pre>	/st	ring>		
	<key>ProductName</key>				
	<string>iPhone OS</string>				
	<key>ProductVersion</key>				
	<string>16.5.1</string>				
	<key>SystemImageID</key>				
	<string>02E5A322-DD97-4FE0-86</string>	8E-	EC626C4F7	127D <td>ig></td>	ig>
	•				
<td>></td> <td></td> <td></td> <th></th> <td></td>	>				

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. Ther are multiple hits referencing URLs containing the GUID **136986169563938816**:

Figure 16: Artifacts > Search Artifact Results > Guilds

Search Artifacts Res	ults		– 🗆 X
Keyword Count:		1	
Artifacts Module: Bates ID	RegEx Search Term	Folder	Match Text
447965 447895 447895 447891 447952 447952 447955 447956 447950 447913 447516 447516 447519 450754 	quilds quilds quilds quilds quilds quilds quilds quilds quilds quilds quilds quilds quilds	URL Cache Generic URL Cache Generic Discord Chat (cache.db)	<pre>https://discord.com/api/v9/users/@me/affinities/guilds https://discord.com/api/v9/guilds/18698169663930816/onboarding https://discord.com/api/v9/guilds/1869816965333816/achebuled-everificati https://discord.com/api/v9/guilds/1869816965333816/achebuled-everificati https://discord.com/api/v9/guilds/1869816966333816/achebuled-everificati https://discord.com/api/v9/guilds/1869816966338816/achebuled-everificati https://discord.com/api/v9/guilds/1869816966338816/achebuled-everificati https://discord.com/api/v9/guilds/1869816966338816/ache/4/1189329086 https://discord.com/api/v9/guilds/186981696633816/ach/4/11893337 https://discord.com/api/v9/guilds/186981696633816/preview https://discord.com/api/v9/guilds/18698169661898741/profile?with_mutu https://discord.com/api/v9/guilds/18698169661898741/profile?with_mutu ("user":("id":"1185636385107273755","username":"oneolick5664_28220","g</pre>
RegEx Term		Hits	
guilds		13	
Total Artifacts: Search Artifacts R	esults finished.	13	
Search Artifacts R Time Taken: 00:00:	esults finished. 04		
			Copy to Clipboard Save CSV and Close Close

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

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

	G	uild Look	up	
* 13698	6169563938816 F	etch Discord Informati	on	
8	Call of Duty • 55.662 Online • 544 • 245 Boosts (Level 3)	.967 Members		

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**.
- 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

Tree 4	🛄 File List			
Filter: 💭 No Filter 🗸 🖃	🖗 🖻 🏟	B Date	Date Read	fø▼ warning used data
	♥ 1 ♥ 2	Date 01-Dec-2023 9:51:43 PM 17-Dec-2023 12:27:48 AM	Date Read 21-Dec-2023 11:17:03 PM 17-Dec-2023 12:28:33 AM	Text Hi, your voice matters to us at Boost Mobile BOOST: You've <mark>used</mark> 4.27 GB of <mark>data</mark> . Once

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

6	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 🗋 Copy code
	(?=.*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

Search Artifacts Resu	lts					_		×
Keyword Count:	1							
Artifacts Module: Bates ID	RegEx Search Term	Folder			Match 1	lext		
455294	(?=.*yout)(?=.*chadwick) (Discord	Chat (a)		0{"id":	"1189;	3426047	651
Match Summary: RegEx Term 	H - wick) (?=.*chadwick)(?=.*yout) 1 	lits 						
-			Copy to Clipboard	Save	e CSV and Clo	ose	Close	•

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)

Forensic Explorer 🛛 🔒 🚵 🔹	- 🔅 - 🔞						Forensic Explor
合 Evidence 🛛 🛅 File Sy	ystem	Artifacts	P Keyword Searc	h 🔎 Ind	ex Search	(C) Email	Registry
Artifacts Artifacts Artifacts Carve	Artifacts To CSV	Artifacts So Mapping	earch Artifact Results	~			
🔚 Artifact Tree 🛛 🕂	🔠 File List						
Filter: 🔄 No Filter 🛛 🗸 🖃	🖗 🗆 🔯	Discord D	late	Author Ni	Alter https://you		
		Discord Date		Author Name	Message		
□ □	1	2023-12-26	T23:02:53.893000+00:00	chadwickgames	https://youtu.be _/	/xzfqVQWnf7s?si	=S4iMmfZHrMgzvdH8
- Discord Chat (cache.db)							

Visiting <u>https://www.youtube.com/watch?v=xzfqVQWnf7s</u> 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

Tree 4	🔜 File List			
Filter: 🗾 No Filter 🗸 🚽	🖗 🖻 🔯	Created (UTC)	✓ Transition Type	Az▼ ai
Filename		Created (UTC)	Transition Type	Bundle ID
2024 Magnet CTE - iOS (10) []	1	20-Dec-2023 6:44	com.apple.SpringBoard.transitionRe	com.apple.mobilem <mark>ai</mark> l
	2	20-Dec-2023 6:47	com.apple.SpringBoard.transitionRe	com.apple.mobilem <mark>ai</mark> l
Chart (E)	3	24-Dec-2023 8:33	com.apple.SpringBoard.transitionRe	com.apple.mobilem <mark>ai</mark> l
	4	24-Dec-2023 8:33	com.apple.SpringBoard.transitionRe	com.apple.mobilem <mark>ai</mark> l
	5	24-Dec-2023 8:52	com.apple.SpringBoard.transitionRe	com.apple.mobilem <mark>ai</mark> l
	6	24-Dec-2023 8:52	com.apple.SpringBoard.transitionRe	com.apple.mobilem <mark>ai</mark> l
	7	24-Dec-2023 8:54	com.apple.SpringBoard.transitionRe	com.apple.mobilem <mark>ai</mark> l
	8	24-Dec-2023 8:54	com.apple.SpringBoard.transitionRe	com.apple.mobilem <mark>ai</mark> l
App Folder UUID IOS (1/4)	9	25-Dec-2023 7:40	com.apple.SpringBoard.transitionRe	com.open <mark>ai</mark> .chat
App Permissions IOS (108)	10	25-Dec-2023 7:40	SBFullScreenSwitcherSceneLiveCont	com.open <mark>ai</mark> .chat
App State IOS (182)	11	25-Dec-2023 7:40	SBFullScreenSwitcherSceneLiveCont	com.open <mark>ai</mark> .chat
Biome App Intent iOS (154)	12	25-Dec-2023 7:42	com.apple.SpringBoard.transitionRe	com.open <mark>ai</mark> .chat
Biome App Launch iOS (1043)	13	26-Dec-2023 10:4	com.apple.SpringBoard.transitionRe	com.apple.mobilemail
Biome Keybag Lock States iOS (149)	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.

Figure 23: Artifacts > Mobile > Application Folder UUID iOS

🔚 Artifact Tree 🛛 🕂	🧮 File List		
Filter: 🔄 No Filter 🗸 🚽	🖗 🖻 🔯	K₂▼ UUID	AZ▼ openai
		UUID	Application Name
2024 Magnet CTF - iOS (9)	1	6BFA5EA3-61CB-4652-A60A-2A955B651E05	com. <mark>openai</mark> .chat
+ Browsers (10)			
🗄 🗔 👼 Chat (5)			
🕀 🖂 Email (2)			
🕀 💽 Finance (1)			
🕀 🔂 Health Apps (3)			
🕂 🗌 🧰 iOS Biome (4)			
🕀 🔽 💡 Locations (2)			
🕀 💼 💼 MAC Operating System (1)			
🗄 🔲 🗋 Mobile (16)			
Accounts Type iOS (38)			
- Application Folder UUID iOS (174)			
Application Permissions iOS (108)		N	

To search the data folder 6BFA5EA3-61CB-4652-A60A-2A955B651E05 for relevant files:

- 1. In the **File System** module, branch plate [**b**] the entire case.
- 2. Filter the Filename column for 6BFA5EA3-61CB-4652-A60A-2A955B651E05.
- 3. Place a check next to this folder.
- 4. In the tree, follow the green boxes to the location of the **6BFA5EA3-61CB-4652-A60A-**

2A955B651E05. Examine the sub-folders and their content.

5. The sub-folder **conversations-b5c12911-e3c0-4961-bbe7-aec0a3ec3dd6** contains three JSON files.

gories	III File List 🚦 Gallery View 📳 Video View 🦲 Disk View 🅙 Category Graph
V	🚱 🖻 👹 🐼 🕈 Filename 🐼 🐨 Ext 🐼 File Signatu
B→D→ B→D→ <t< th=""><th>Filename Ext & File Signature 1 A0724901-AAEA-4F6A-85F3-7146F87EC139.json json JSON 2 B00981C1-4A49-4F45-84D8-59DFF84412CA.json json JSON 3 DC21BA37-9C8D-4FAD-A67F-B318D1752F24.json json JSON</th></t<>	Filename Ext & File Signature 1 A0724901-AAEA-4F6A-85F3-7146F87EC139.json json JSON 2 B00981C1-4A49-4F45-84D8-59DFF84412CA.json json JSON 3 DC21BA37-9C8D-4FAD-A67F-B318D1752F24.json json JSON
E-ID is Library (9)	00008110-000925383620A01E_files_full.zip\private\var\mobile\Containers\Data\Application
Conversations-b5c12911-e3c0-4961-bbe7-aec0a3ec3dd6 (3)	3 of 3 Visible [LS 15 KB PS 15 KB] 1 Highlighted [LS 3 KB PS 3 KB]
	<pre>], "created_at" : 725410981.34251106 }, "BE070EAF-516A-4E78-9AF2-138CB9A281ED" : { "parent" : "7C149DCB-8714-48CB-90F4-86027E0CD121", "id" : "BE070EAF-516A-4E78-9AF2-138CB9A281ED", "content" : { "id" : "9C4CBC90-9E52-48A0-A14A-CACD507DA38D", "author" : { "role" : "user" }, "content" : { "parts" : ["How to make online friends"]]]</pre>
B-D B 70A45E19-4DF2-4C73-B17D-9E0321564598 (5) B-D B 71310B1A-E4CE-4566-B3E2-64FACE1DB5E1 (5)], "content type" : "text"
B-D Image: 73400697-9065-4683-9EE5-F0146E6AB851 (5) FD Image: 73400697-9065-4683-9EE5-F0146E5AB851 (5) FD Image: 73400697-9065-4683-9EE5-F0146E5AB851 (5) FD Image: 73400697-9065-4683-9EE5-F0146E5AB851 (5) FD Image: 73400697-9065-4683-9EE5-F01465-48851 (5) FD Image: 73400697-9065-4683-9EE5-F01465-48851 (5) FD Image: 73400697-9065-4683-9EE5-701465-48851 (5) FD Image: 73400697-9065-4683-9EE5-701465-48851 (5) FD Image: 73400697-9065-4683-9EE5-701465-48851 (5) FD Image: 73400697-9065-7065-7065-7065-7065-7065-7065-7065-7	},

Figure 24: OpenAi data folder > conversations...

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

1.

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

• "Write a short snarky twitter post about friend betrayal in Canada"

2.

File B00981C1-4A49-4F45-B4D8-59DFF84412CA.json:

- · "How to make online friends"
- З.

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.

0007

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** (<u>https://www.swiftforensics.com/2020/07/ktx-to-png-in-python-for-ios-snapshots.html</u>).

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: <u>https://www.youtube.com/watch?v=xzfqVQWnf7s</u>. 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



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.





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

🚺 Artifact Tree म	III File List	
Filter: 🗾 No Filter 🗸 🖃	🙀 🖻 😻 🖲 03-Dec 💽 End Date 🕼 Steps	• Provenance
Filename	Start Date End Date Steps Take	n Provenance
2024 Magnat CTE (OS (0)]	1 03-Dec-2023 6:47:37 PM 03-Dec-2023 6:50:22 PM 2	72 iPhone 14, 7
□	2 03-Dec-2023 7:18:44 PM 03-Dec-2023 7:21:28 PM 2	99 iPhone 14,7
Browsers (11)	3 03-Dec-2023 9:11:59 PM 03-Dec-2023 9:15:43 PM 1	75 iPhone 14,7
Chat (5)	4 03-Dec-2023 11:36:34 PM 03-Dec-2023 11:38:30 PM 2	22 iPhone 14,7
Apple Health Distance (252		
- Apple Health Flights Climber		
Apple Health Steps (252)		
Health Apps (3) Apple Health Distance (252 Apple Health Flights Climber Apple Health Steps (252)		

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

I File List	😨 Gallery View 😨 Video View 🔒 D	Disk View) Category G	Graph			
i 🔁 🕺	✓ healthdb_secure.sqlite		€Z▼ Ext	► File Sign	ature	A-Z	• Extension
	Filename		Ext 🔺	File Signature		Ext	ension Misma
1	healthdb_secure.sqlite		sqlite	SQLite		No	1
2	healthdb_secure.sqlite-shm		sqlite	Sqlite SHM		No	
3	healthdb_secure.sqlite-wal		sqlite-wal	Sqlite WAL		No	
00008110	000925383620A01E_files_full.zip\private	\var\mobile\	Library\Hea	alth\healthdb_s	ecure.sqlite		
3 of 442550 V	isible [LS 3.7 MB PS 3.7 MB]	1 Hig	hlighted [LS	2.0 MB PS 2.0	MB]		1 Checked
> · quant	ity_samples	DATA_ID *	START	_DATE	END_DATE		DATA_TYPE
> quant	ity_series_data	1	72207	6460.531398	722076743.617333		8
> sampl	es	2	72207	6460.531398	722076743.617333		7
> scher	a_user_versions	3	72207	6493.985648	722077335.502489		9

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

Create Google Map .GPX	_		×
About Select Artifacts			
Artifacts with GPS Coordinates	Cur ant Result	ts	
Apple Health Workout Latitude	0		
Apple Health Workout Longitude	0		_
Cached Locations iOS	1323*		
Cell Tower Locations iOS	0		_
Find My Devices iOS	1		
Find My Items iOS	1		
Fitbit Event	0		
Garmin Connect Activities	0		
Garmin Connect Activity Details	0		
Google Maps Saved Places Android	0		
Parked Car Locations iOS	0		_
Photos.Sqlite 10S	51		
Significant Locations 10S	0		
Significant Locations Visits 105	0		
Skysare CSV	0		
WITI LOCATIONS 105	0		
Between Dates: 27-Dec-2023		3	•
Open Export Folder ? Sample < 2000*	Create GPX	Clos	æ

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"

Search Artifacts Result	ults		- 0 X
Keyword Count:		1	
Artifacts Module: Bates ID	RegEx Search Term	Folder	Match Text
456472	hockey	SnapChat Message (arroyo.d	Wow, that looks like an ele
Match Summary: RegEx Term		Hits 	
hockey		1	
		Copy to Clipboard	Save CSV and Close Close

 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.

🔚 Artifact Tree	Ъ,	🧮 File List				
Filter: 🔄 No Filter 🗸 🔹	-	🖗 🗆 🔯	Creation Date	Read Timestamp	AZY Co	Message
■ AZ▼ Filename		1.1.61	Creation Date	Read Timestamp	Conten	Message
2024 Magnet CTF - iOS (10)		25	26-Dec-2023 11:19:33 PM	26-Dec-2023 11:19:33 PM	Text	Ditto!
+- Browsers (11)		26	26-Dec-2023 11:19:34 PM	26-Dec-2023 11:19:35 PM	Text	No way, that's awesome! Go Avs! 🍕 🕲 What do you lov
🔁 🗐 💬 Chat (5)		27	26-Dec-2023 11:20:01 PM	26-Dec-2023 11:20:01 PM	Text	mikko rantanen!! He's goated. Do you know what that m
Discord Chat (a) (25)		28	26-Dec-2023 11:20:02 PM	26-Dec-2023 11:20:03 PM	Text	Oh, absolutely! Mikko Rantanen is an incredible player, n
Discord Chat (cache.db) (113)		29	26-Dec-2023 11:20:16 PM	26-Dec-2023 11:20:16 PM	Text	Heck yea! Who's your favorite player
Discord Chat (fsCachedData) (381)		30	26-Dec-2023 11:20:17 PM	26-Dec-2023 11:20:18 PM	Text	I'm so glad you asked! My favorite player on the Colorad
SnapChat Message (arroyo.db) (65)		31	26-Dec-2023 11:20:36 PM	26-Dec-2023 11:20:36 PM	Text	Dawg. Did u see what he did the other night? The night I
SnapChat User (4)		32	26-Dec-2023 11:20:37 PM	26-Dec-2023 11:20:38 PM	Text	No way, dawg! I'm so stoked you downloaded Snapchat
+ Email (2)		33	26-Dec-2023 11:21:28 PM	26-Dec-2023 11:21:28 PM	Text	The Avs won 6-4 Mackinnon made 4 of our 6 total points
+		34	26-Dec-2023 11:21:30 PM	26-Dec-2023 11:21:31 PM	Text	No way, that sounds absolutely insane! 🕷 Nathan MacK
🕂 🔄 🛟 Health Apps (3)		35	26-Dec-2023 11:21:47 PM	26-Dec-2023 11:21:47 PM	Text	Yea you rly missed out
🕂 🗌 💰 iOS Application (13)		36	26-Dec-2023 11:21:48 PM	26-Dec-2023 11:21:49 PM	Text	Aw, man! I wish I could have been there to witness it to
App Folder UUID iOS (174)		37	26-Dec-2023 11:21:55 PM	26-Dec-2023 11:21:55 PM	Text	So u don't have access to the internet to see these thing
App Permissions iOS (108)		38	26-Dec-2023 11:21:57 PM	26-Dec-2023 11:21:58 PM	Text	Oh, my bad! I misunderstood your question. Yes, I do ha
App State iOS (182)		39	26-Dec-2023 11:22:43 PM	26-Dec-2023 11:22:43 PM	Media	
Biome App Intent iOS (154)		40	26-Dec-2023 11:22:47 PM	26-Dec-2023 11:22:48 PM	Text	Wow, that looks like an electric atmosphere at the hocke
Biome App Launch iOS (1043)		41	26-Dec-2023 11:23:01 PM	26-Dec-2023 11:23:01 PM	Text	Why can you see photos but ChatGPT can't?
Biome Keybag Lock States iOS (149)		42	26-Dec-2023 11:23:03 PM	26-Dec-2023 11:23:04 PM	Text	Oh, I see what you mean! Well, the thing is, as a virtual
Biome Plugged-in States iOS (72)		43	26-Dec-2023 11:23:29 PM	26-Dec-2023 11:23:29 PM	Text	So can you send me pictures?

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. Apple 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**.

- a Created	2023:12:21 20:23:06	2023:12:21 20:23:06	AString	30376
— a Tag 316 (Computer)	iPhone 14	iPhone 14	AString	30396
	216	216	UInt32	30316
Ė– EXIF				
- 🔢 Tag 33434 (ExposureTime)	0.00233100233100233	0.00233100233100233	Double	30808
— 🛒 Tag 33437 (FNumber)	1.5	1.5	Double	30816
-123 Tag 34850 (ExposureProgram)	2	2	Word	30440
-123 Tag 34855 (ISOSpeedRatings)	50	50	Word	30452
Tag 36864 (ExifVersion)	48 50 51 50	48 50 51 50	Byte (4)	30464
— a Tag 36867 (DateTimeOriginal)	2023:12:21 20:23:06	2023:12:21 20:23:06	AString	30824
— a Tag 36868 (DateTimeDigitized)	2023:12:21 20:23:06	2023:12:21 20:23:06	AString	30844
— a 36880	-07:00	-07:00	AString	30864
— <u>a</u> Tag 36881	-07:00	-07:00	AString	30872
— <u>a</u> 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\mo	bile\Media\DCIM\100APPLE	\IMG_0030.HEIC		2
🗰 Hex 🚍 Text 🚍 Info 🔢 Bookmark 📠 Byte P	lot 📑 Display 😑 Filesyste	em Record 🗵 File Metadata	🚔 File Exte	nt 喜 Per

Figure 41: File System > File Metadata

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).

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"

E Gallery View E Video View						
Ş — 🔅	Interview Filename	19 H				
	Filename	Hits	Hit Text			
₽-	DeliveredNotifications.plist	8				
		1/8	fProcessedByNSEsuppress_bitmojiTn_idVsenderarroyo_convo			
		2/8	idUtitleXdt_tokensender_ <mark>bitmoji</mark> _url]local_messageÒ.ST.U			
		3/8	this!RdtU <mark>https://images.bitmoji</mark> .com/render/panel/10226428-			
		4/8	arroyo_convo_idsuppress_bitmojisuppress_in_appsender			
		5/8	fProcessedByNSEsuppress_bitmojiarroyo_convo_id^ab_cnoti			
		6/8	.sender_selfie_idsender_ <mark>bitmoji</mark> _url]local_messageÒ.Si.U			
		7/8	tch this!Thttps://images.bitmoji.com/render/panel/10226594-			
		8/8	reator_icon_urlsuppress_bitmojisuppress_in_appsender			
₽-□	installed_app_whitelist_url	1				
		1/1	<pre>moji\":[{\"bundle_name\":\"Bitmoji\",\"encoding_id\":1244,\"m</pre>			
₽-□	correction_dict_url	9				
		1/9	"c":{"lamodeise":0}}.{"q":" <mark>bitmoji</mark> ","c":{"bitem":0,"bimo":0,"			
		2/9	<pre>max","c":{"baax":0}}.{"[3]:"bitmoji free","c":{"bitmogi":0,"bi</pre>			

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

📰 Keywo	rd Result List 🔋 Gallery View	📰 Video '	/iew
i 🖓 🖻 🔯	€2 Filename	19 H	
	Filename	Hits	Hit Text
₽-₽	DeliveredNotifications.plist	2	
		1/2	🔗 6428Chadwick, Watch this!RdtU <mark>https://images.bitmoji.com/render/panel/</mark> 10226428-197928258_17-s5-v1.png?tr
		2/2	0226594Chadwick, Watch this!Thttps://images.bitmoji.com/render/panel/10226594-482842799_5-s5-v1.png?tra
	DuetActivitySchedulerCl	1	
		1/1	6594Chadwick, Watch this!RdtT <mark>https://images.bitmoji.com/render/panel/</mark> 10226594-482842799_5-s5-v1.png?tra
⊨	aps.db	2	
		1/2	push.mp3RdpRdtZfrom My AIUfalse`https://images.bitmoji.com/render/panel/10226021-101443429406_1-s5-v1.webp
		2/2	push.mp3RdpRdtZfrom My AIUfalse` <mark>https://images.bitmoji.com/render/panel/</mark> 10226021-101443429406_1-s5-v1.webp
Ė- 	app_group_plist_storage	4	
		1/4	.^8`aWNS.base[NS.relative`https://images.bitmoji.com/render/panel/10226021-101443429406_1-s5-v1.webp
-		2/4	l==00deUNSURL.d 0j.^8`idhttps://images.bitmoji.com/render/panel/10226021-bbs-101443429406_1-s5-v1.
		3/4	*,.(Ó].^8`Ê)` <mark>https://images.bitmoji.com/render/panel/</mark> 10226021-101443429406_1-s5-v1.webp
		4/4	nsparent=1&scale=06].^8`\+d <mark>https://images.bitmoji.com/render/panel/</mark> 10226021-bbs-101443429406_1-s5-v1.

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

Visiting these URLs located the following bitmoji:

Figure 45: 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"

Keyword Tree	٦, T	I Keywor	d Result List 📰 Gallery View	👬 Video \	liew		
Keyword Label	Search	_					
E Keyword Results (1)		🖗 🗆 🔯	Filename	(19 H			
E- 🔄 🔚 Keyword Search 4 (1)			Filename	Hite	Hit Text		
10226594-482842799 5-s5-v1 (2)	10226		Fliename	HILS	nitiext		
		P-L	DeliveredNotifications.plist	1			
				1/1	Thttps://images.bitmoji.com/rend		
		Ė- □	DuetActivitySchedulerCl	1			
				1/1	Thttps://images.bitmoji.com/rend		
		00008110-	000925383620A01E_files_full.zip	o\private\	$var\\DuetActivitySchedulerClassC.db-wal$		
0 of 3 Checked		2 of 2 Visible [[LS 3.9 MB PS 3.9 MB]		1 Highlighted [LS 25 KB PS 25 KB]		
0226594Chadwick, Watch this!Thttps://images.bitmoji.com/render/panel/10226594-482842799_5-s5-v1.p							
?transparent=lo.*.S.o.f.1.a.k.h.a	<u>.n</u> . Ø	>YvØ>Yu	a.d.d.e.dav.1.(d.e.o.	.t.oS.p.o.t.l.i.g.h.t.!0		
\$.ò;."4/O							
. AttachmentOptionsThumbnailHidde	n]Att:	achmentURL	^AttachmentType'Att	tachmen	tHiddenFromDefaultExpandedV		
w Kawatar h395elfhad7d5377345de7	52580	27679aeh44	ddeba8a25b5fd2001713	9db1ba0	6 a 6 Oprov		

Figure 47: Keyword Search > File Metadata

Chadwick, Watch this!	
Sofiakhan 🕲 🎯 added a video to Spotlight!	
spotlight_feed_subscription_story	
generic_push.mp3	
{"dt_resend_mode":"disabled","dt_rid":"22da020f-058a-43d8-baf7-5f3d518aecb0","dt	{"dt_resend_mode":
1703784158264	
482842799_5-s5	
79e540d6-964d-4981-bd72-05231ff0e206	
10226594	
Chadwick, Watch this!	
https://images.bitmoji.com/render/panel/10226594-482842799_5-s5-v1.png?transpar	https://images.bitmo
Sofiakhan 🕲 🏶 added a video to Spotlight!	
444	
202 Aug Alexa Mila Mila Mila Mila Mila A DOT77006, DA27, 4020, A260, 270,40001207A), D. J.	INT ALC AND A REAL
e\var\mobile\Library\UserNotifications\BC777900-DA27-4839-A209-37D489012B7A\Delivered	divotifications.plist
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

=	File List				
Ş	0 🔯	B Date	B Date Read	Az ▼ Text	Attributed Body Carve
		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 ge
	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		0	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 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

📑 DB Br	📳 DB Browser for SQLite - C:\Users\graha\Documents\Forensic Explorer v5\Cases\2024 Magnet CTF - iOS\Exported\sms.db					
File Edit	View Tools Help				_	
() Open	Project 😭 Save Project 😹 Attach Database 🗙 Clos	se Database				
Database	Structure Browse Data Edit Pragmas Execute SQL			Edit Database Cell		
-0 [Mode: Binary 🗸 🎯	Ð,	
🔍 SQL	1 🛛					
1 2 3 4 5 6 7 8 9 10 11	<pre>SELECT ROWID, text, attributedBody, datetime(date / 1000000000 + 978307200, 'ur FROM message WIERE DecodedDate >= '2023-12-18 00:00:00' AND DecodedDate < '2023-12-15 00:00:00' GRDER BY</pre>	iixepoch') AS De	codedDate	0000 04 0b 73 74 72 65 61 61 74 79 70 65 64 81 e8 03 streamtyped 0010 84 01 40 84 94 19 49 65 34 d7 57 46 16 25 65 NSMutable 0020 41 74 74 72 69 62 75 74 65 64 53 74 72 69 68 67 NSMutable 0030 00 84 84 12 45 34 17 74 72 69 62 75 74 65 64 53 74 72 69 68 67 NSMutable 0040 53 74 72 69 62 67 00 84 84 08 42 53 44 75 74 61 62 66 55 NSMutable 0050 06 65 53 74 72 69 62 67 01 84 84 09 42 53 44 75 74 61 62 60 55 NSMutable 0060 07 72 69 62 67 01 98 84 01 2b 81 96 00 45 78 63 75		
12	DecodedDate;			00c0 6f 20 77 61 6c 6b 65 64 20 61 77 61 79 20 77 69 6 walked away wi 00d0 74 68 20 61 20 62 6c 61 63 6b 20 65 79 65 20 61 th a black eye a		
RC)WID text	attributedBody	DecodedDate	00e0 6e 64 20 73 70 65 6e 74 20 24 33 30 20 6t 61 73 nd spent \$30 las 00f0 74 20 6e 69 67 68 74 20 6f 6e 20 70 72 6f 64 75 t night on produ 0100 63 74 73 20 74 6f 20 61 76 6f 69 64 20 6f 6e 65 tots to avoid one		
1	26 You're the goat! You want to meet at the Ethan	BLOB	2023-12-18 00:42:34	0110 21 20 86 84 02 69 49 01 6d 92 84 84 84 0c 4e 53 !iI.mNS		
2	27 For sure, 20 pieces for \$100	BLOB	2023-12-18 00:50:09	0130 92 84 98 98 1d 5f 5f 6b 49 4d 4d 65 73 73 61 67 kIMMessag		
3	28 Let me know when you are heading over there a	BLOB	2023-12-18 00:51:07	0140 65 50 61 72 74 41 74 74 72 69 62 75 74 65 4e 61 ePartAttributeNa		
4	29 NULL	BLOB	2023-12-18 01:34:30	0150 60 65 56 92 54 54 54 55 46 55 46 75 60 62 65 72 meNSNumber 0160 00 84 84 07 4e 53 56 61 6c 75 65 00 95 84 01 2aNSNalue*		
5	30 Alright I'll be there	BLOB	2023-12-18 01:36:47	0170 84 9b 9b 00 86 86 99 02 03 92 84 9a 9b 02 92 9b		
6	31 Just got here	BLOB	2023-12-18 01:59:22	0180 92 9C 92 84 98 98 17 51 51 60 49 4d 4d 61 66 65 kimione 0190 79 41 74 74 72 69 62 75 74 65 4e 61 6d 65 86 92 yAttributeName		
7	32 How dare you!! Come back here and face me lik	BLOB	2023-12-18 02:14:25	01a0 84 84 84 0d 4e 53 4d 75 74 61 62 6c 65 44 61 74NSMutableDat		
8	33 No shot after what you did, this money is for pai	BLOB	2023-12-18 02:38:38	Type of data currently in cell: Binary		
9	34 NULL	BLOB	2023-12-18 10:05:26	1350 byte(s)		
10	35 BOOST: Got it! We've received your payment of	BLOB	2023-12-18 14:28:16	SQL Log		
				Show SQL submitted by Application 267 order by DecodedDate LIMIT 0, 49999; 268 ROLLACK TO SAVEPOINT "RESTOREPOINT"; 269 PRACMA database_list; 270 SBLBCT type,name,sql,tbl_name FROM "main".sqlite_master;		

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
```

III Artifact Tree 4	🔜 File List						
Filter: 🔄 No Filter 🗸 🚽	🖗 – 🍪	AZ▼ IMEI	AZY Last Good IM!	Last Known ICCID	Apple Carrier	Phone Nun	AZ▼
Agy apple comm		IMEI	Last Good IMSI	Last Known ICCID	Apple Carrier	Phone Number	Source Name
2024 Magnet CTE - iOS (10)	1	352013407827333	310380777899377	8901240147139955363	310240_GID1-6432	16802424161	com.apple.commcenter.plist
□ = 202+Magnet C11 + 103 (10) □							
Apple Comm Center iOS (1)							

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

🏢 File List	🔋 Gallery View 🔋 Video View 🔔 Disk View 🌒 Category	Graph					
🖗 🖻 😻 🌔	🤯▼ com.apple.commcenter.plist	AZT Ext	File Signature				
	Filename	Extension	File Signature				
1	com.apple.commcenter.plist	plist	Plist (Binary)				
			1				
00008110-0	00925383620A01E_files_full.zip\private\var\wireless\Library\P	references\@	com.apple.commcenter.plist				
			-				
xml ver:</td <th>sion="1.0" encoding="UTF-8"?></th> <th></th> <th></th>	sion="1.0" encoding="UTF-8"?>						
DOCTYPE</td <th>plist PUBLIC "-//Apple Computer//DTD PLI</th> <th>IST 1.0/</th> <th>/EN" "http://www.apple.c</th>	plist PUBLIC "-//Apple Computer//DTD PLI	IST 1.0/	/EN" "http://www.apple.c				
<plist td="" ve:<=""><th>rsion="1.0"></th><th></th><th></th></plist>	rsion="1.0">						
<dict></dict>	<dict></dict>						
<key></key>	EnhancedLQMTrafficClassRegistration	>					
<true></true>							
<pre><key>EnhancedLQMLinkQualityFingerPrintRegistration</key></pre>							
<true></true>							
<key>EnhancedLQMLinkStateRegistration</key>							
<true,< td=""><td colspan="7"><true></true></td></true,<>	<true></true>						
<key></key>	EnhancedLQMNRServingCellTypeRegistration<		I				

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	
-----------	--------	--------	---	----------	--------	-----------	--

III File List	🔋 Gallery View 🔋 Video View 🦲 Disk View 🅙 Cate	egory Graph	
🖗 🖻 🎆 I	🦗 🕶 carrier	AZ▼ Ext	A₂▼ File Signat
	Filename	Extension	File Signature
10	device + carrier + 310240_GID1-6432+D27+54.1.plist	plist	Plist (Binary)
11	device +carrier +310380_GID1-39+D27+54.0.plist	plist	Plist (Binary)
12	device+carrier+310410+D27+54.0.1.plist	plist	Plist (Binary)
13	device +carrier +311480 +D27+54.0.1.plist	plist	Plist (Binary)
14	device+carrier+311580+D27+54.0.1.plist	plist	Plist (Binary)
15	device+carrier+313100+D27+54.0.1.plist	plist	Plist (Binary)
16	device+carrier+bs-310380+D27+54.0.plist	plist	Plist (Binary)
17	device+carrier+Default.bundle+D27+54.0.1.plist	plist	Plist (Binary)
18	device+carrier+Unknown.bundle+D27+54.0.plist	plist	Plist (Binary)
19	device +mvno +carrier +310240_GID 1-6432 +M:3102	plist	Plist (Binary)
20	device +mvno +carrier +310240_GID 1-6432 +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/fac	ebook/id284882215					
	/private/var/mobile/Container Internal App Path	rs/Data/Application/ <app_guid> File Name</app_guid>	File Type				
	/Documents/	time_in_app_ <user_id>.db</user_id>	SQLite				
	/Library/Caches/com.facebook. Facebook.MosaicIGImageDiskCache/	*	Various				
	/Library/Caches/graphStoreDB/	GraphStore_ <user_id>.sqlite3</user_id>	SQLite				
	/Library/Caches/messenger_contacts. <guid>/</guid>	fbsyncstore.db	SQLite				
	/Library/Caches/search_bootstrap. <guid>/search/</guid>	graph_search_entity_bootstrap.data	File				
	/Library/Caches/video_cache. <guid>/storage/</guid>	*	Plist				
	/Library/Preferences/	com.facebook.Facebook.plist	Plist				
Facebook							
	REFERENCES: https://www.academia.edu/10726810/Social_Medi https://www.tandfonline.com/doi/abs/10.1080/00-	a_Forensics_on_Mobile_Devices 450618.2015.1066854?src=recsys&journa	lCode=tajf20				
	https://www.fbiic.gov/public/2011/jul/Facebook_F	orensics-Finalized.pdf					
	https://www.researchgate.net/publication/224221519_Third_Party_Application_Forensics_on_ Apple_Mobile_Devices						
	https://www.diva-portal.org/smash/get/diva2:6516	693/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"

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.

File List 😨 Gallery View 😨 Video View 🖨 Disk Vie	ew 🅙 C	ategory Graph			
🖗 🖻 🎆 🕢 time_in_app	Az▼ Exti	AZT sqlite	■ BF2FEA88-C397-405D-90	DEE-A56B2720896C	
Filename A Extension File Signature Path 1 time_in_app_61554675133740.db db SQLite 00008110-000925383620A01E_files_full.zip\private\va 2 time_in_app_61554675133740.db db SQLite 00008110-000925383620A01E_files_full.zip\private\va 3 time_in_app_61555027042760.db db SQLite 00008110-000925383620A01E_files_full.zip\private\va 4 time_in_app_61555027042760.db-shm db-shm Sqlite 00008110-000925383620A01E_files_full.zip\private\va 5 time_in_app_61555027042760.db-wal db-wal Sqlite WAL 00008110-000925383620A01E_files_full.zip\private\va 00008110-000925383620A01E_files_full.zip\private\var\mobile\Containers\Data\Application\BF2FEA88-C397-405D-90EE-A56B2720896 SQLite 00008110-000925383620A01E_files_full.zip\private\var\mobile\Containers\Data\Application\BF2FEA88-C397-405D-90EE-A56B2720896					
5 of 443156 Visible [LS 667 KB PS 667 KB]	1 Highli	ghted [LS 20 KB	PS 20 KB]	0 Checked [LS 0	
✓ · Tables		KEY * last_logging_tim last_eviction_tim	VALUE estamp 1703448852 nestamp 1703448852		

- In the File System Display View, the metadata table identifies the last_loggin_timestamp as 1703448852.
- Decode this timestamp in Digital Detectives DCode software to be Unix Seconds (UTC), 2023-12-27 21:34:55.0000000 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"

I Keywor	rd Result List 🔋	Gallery Vie	v 🚦 Video View	
Ş — 🔯	Filenam	19 Hit		
	Filename	Hits	Hit Text	
₽--	FBF7F88	1		1
		1/1	having many different types. No gun overpowers another, only in the strategy required.	. Both I
₽-□	📄 G1%3a3	2		
		1/2	vrangesstext.@Does anyone know the strategy to Terran	rium? O
		2/2	essageTextWithEntities.stext@Does anyone know the strategy to Terrar	rium? O
₽-□	📄 G1%3a1	1		
		1/1	essageTextWithEntities.stext@Does anyone know the strategy to Terrar	rium? O.
₽-□	173FF94	1		1
	_	1/1	s, you can get cool stuff like Sacred and Void Shards for free. The strategy matters t	the mos
₽- ₽	7DDEF5	1		
		4/4		n nrotti.
00008110	-00092538362040	N1E files fu	II zin\nrivate\var\mohile\Containerc\Data\Annlication\RE2E_\G1%3a38163057137705668072843833128%3a077155603	27667250056
	000525505020A	vic_nes_re	maip (private (var (mobile (containers/outa (Application (b) 21 (c) volabor (5005 / 15 / 05005 / 20 / 5055 / 20 / 20	11001255050
6 of 6 Visible	[LS 338 KB PS 33	88 KB]	1 Highlighted [LS 46 KB PS 46 KB] 0 Checked [LS 0 bytes PS 0 bytes]	
BCDB	E F 10 11 1	2 13 14	15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21	Disassembly
72 5F 72 6	1 6E 67 65 7	3 01 01	00 00 00 00 00 00 00 00 76 0E 00 00 00	Graphic
00 00 00 0	0 00 00 76 0	6 00 00 i	00 72 61 65 65 73 01 01 00 00 00 00 ranges	Data Inspect
78 74 01 0	1 40 00 00 0	0 00 00	00 00 44 6F 65 73 20 61 6E 79 6F 6E 65stext@Does anyone	bata inspect
74 72 61 7	4 65 67 79 2	0 74 EF 3	20 54 65 72 72 61 72 69 75 6D 3F 20 4F know the strategy to Terrarium? O D	ata Type
20 72 61 6	E 64 6F 6D 3	F 00 76 :	25 00 00 00 6D 65 73 73 61 67 65 5F 72 r is it all random?.v%message_r	Fil
61 74 69 6	5 55 52 4C 0	4 69 6D 1 01 86	bb 6C 69 6K 65 22 29 01 01 00 00 00 icntext(location:"\$imeline")	Ur
CD 00 00 0	0 00 02 40 0	1 01 00	to be be be be be be in it is in an interesting of the best in the	Lie

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.





A check of the previously identified Facebook account of chadwick,

<u>https://www.facebook.com/profile.php?id=61555027042760</u>, finds a message relating to Terrarium on the main page:

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

Posts			≌₀. Filters
Chadwick Elms December 28, 20/	23 · 🕲		
Does anyone l random?	know the strategy	to Terrarium?	Or is it all
🖒 Like	Comment	🕓 Send	🖒 Share

ChatGPT identified the full name of Terrarium to be "Terrarium: Garden Idle".

Figure 60: ChatGPT

GR	You What is the ios game Terrarium?
6	ChatGPT " The iOS game "Terrarium: Garden Idle" is a free-to-play idle gardening game where players start with some oxygen points and use them to plant and upgrade various cute plants, which in turn produce more oxygen points. The game includes options for decoration and a VIP subscription for additional features. However, it features frequent ads that can be bypassed by making in-game purchases. The game is developed by Green Panda Games and is available on devices running iOS 12.5 or later (App Store). ()* () ()

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

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

Q21. ANSWER

user-xurgQ0xumvrujH5ESG17Yhcw.

Q21. FORENSIC EXPLORER METHODOLOGY

It is likely that user ID configuration for an iOS application will be located withing 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

Artifact Tree 4	🛲 File List		
Filter: 🔄 No Filter 🗸 🖃	i 🔁 🖗	€ UUID	A₂▼ openai.chat
Filename		UUID	Application Name
2024 Magnet CTF - iOS (10)	1	68FA5EA3-61CB-4652-A60A-2A955B651E05	com. <mark>openai.chat</mark>
+ Browsers (11)			
🕂 🗍 🕺 Chat (5)			
🕂 🔄 🖂 Email (2)			
🕂 🗌 🔇 Finance (1)			
🕂 🗌 🛟 Health Apps (3)			
- iOS Application (10)			
App Folder UUID iOS (174)			
Ann Derminsings (OC (100)			

In the File System module:

- 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.
- Right-click in the folder tree and clear all checks. Then check the entire content of the BF2FEA88-C397-405D-90EE-A56B2720896C folder.
- In the Keyword Search module, run a keyword search on checked items only for chawickmr95@gmail.com. Two files are located:

Figure 62

Keywor	d Result List 😨 Gallery View 😨 Video	View		
i 🖓 🗆 🔯	€Z▼ Filename	<u>1</u> 9 н	File Si	
	Filename	Hits	File Signat	Hit Text
	com.openai.chat.StatsigService.plist	1	Plist (Binary)	
		1/1		vrujH5ESG17Yhcw <mark>chadwickmr95@gmail.com</mark>
<u> </u>	Cache.db-wal	13	Sqlite WAL	
<u> </u>	_	1/13		hcw",. "email": " <mark>chadwickmr95@gmail.com</mark> ",
-		2/13		"Personal org for <mark>chadwickmr95@gmail.com</mark> ",
		3/13		G17Yhcw","email":"chadwickmr95@gmail.com",

Examine the metadata of **com.openai.chat.StatsigService.plist** to reveal the **userID** to be **userxurgQ0xumvrujH5ESG17Yhcw**.

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



Q22. READ MY MIND (25 POINTS)

What message was sent to Rocco in a video game?

Q22. ANSWER

Γ

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:

GR	You In the iPhone game com.activision.callofduty.shooter can you send messages to other users?
\$	ChatGPT
	Yes, in the iPhone game identified by its bundle identifier as "com.activision.callofduty.shooter",
	which is "Call of Duty®: Mobile", you can send messages to other users. The game boasts voice
	and text chat features that allow you to communicate with your friends while playing (Apple).
	C C C

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

Folders Categories	File List 😨 Gallery View 🔋 Video	View 🔚 Disk View 🍓 Category Grap	h	
Filter: 🔄 No Filter 🗸 🕒	🖗 🖻 👹 🕡 🖓 Filename) 🖉 Is	I 🐼▼ Ext 🐼▼ File Sig	n A-ZV
Filename	Filename 1 119203768236110 2 2023-12-20 00008110-000925383620A01E_files_full.	▲ IsDir Yes No zip\private\var\mobile\Containers\Da	Extension File Signature Folder JSON	Exten
□ □ 1192037682361107226 (1)	2 of 2 Visible [LS 376 bytes PS 376 bytes]	1 Highlighted [LS 37	6 bytes PS 376 bytes]	
	Property Value ⊡ JSON Tree ⊡ - ⊕	Raw	v Value	Туре
$\begin{array}{c} \begin{array}{c} \begin{array}{c} \begin{array}{c} \begin{array}{c} \begin{array}{c} \end{array}\\ \end{array}\\ \end{array} \\ \begin{array}{c} \begin{array}{c} \end{array}\\ \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \begin{array}{c} \end{array}\\ \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \begin{array}{c} \end{array}\\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \begin{array}{c} \end{array}\\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \end{array} \\ \end{array} \\ \begin{array}{c} \end{array} \\ \end{array} \\ \begin{array}{c} \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \end{array} \\ \end{array} $	a) TabIndex	4 1703098327	4 1703098327	UString UString
⊕-D ⊇ MGPA (2) ⊕-D ⊇ AufferQts (51) ⊕-D ⊇ AufferQts (51)	- a ChatType - a IsSender	true 1 true	true 1 true	UString UString UString
	- a Content - a OwnerID - a PlayerID	I know youre reading my messages I know youre reading my messages 1 know 15/45/0958107220364 1192037682361107226	now youre reading my 6157450958107220364 1192037682361107226	UString UString UString

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"

Search Artifacts Result	ts		– 🗆 X
Keyword Count:		1	
Artifacts Module:			
Bates ID	RegEx Search Term	Folder	Match Text
457251	susan	InteractionsC Contacts iOS	Susan
457423	susan	InteractionsC Interactions	Susan
467484	susan	Contacts Details iOS	Susan
469487	susan	SMS v4 iOS	Merry Christmas, Chad! It is Susan. Now you hav
469487	susan	SMS v4 iOS	Merry Christmas, Chad! It is Susan. Now you hav
469488	susan	SMS v4 iOS	Merry Christmas Susan!ð how have you been?
Match Summary:			1
RegEx Term		Hits	
susan		6	
Total Artifacts:		5	
Search Artifacts Res	ults finished.		1
Search Artifacts Res	sults finished.		
Time Taken: 00:00:04		т	
		Ť	
			Copy to Clipboard Save CSV and Close Close

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

	🛲 File List				
(🥦 🖻 🎆 (B Date	B Date Read	Az▼ Text	AZ▼ susan
Γ		Date 🔺	Date Read	Text	Attributed Body Carve
l	1	25-Dec-2023 4:17:53 PM	25-Dec-2023 7:04:25 PM	Merry Christmas, Chad! It is Susa	Merry Christmas, Chad! It is Susan. Now y
	2	25-Dec-2023 7:06:24 PM			Merry Christmas <mark>Susan</mark> !ð how have you be

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**:

- In the File System module Branch plate [▶] the entire case and in the Filename column, filter for sms.db.
- 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**.
- 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

ode: Bir	nary	~													[ì	= 🖹 🔓 📮 🗔
0000	04	0b	73	74	72	65	61	6d	74	79	70	65	64	81	e8	03	streamtyped
0010	84	01	40	84	84	84	12	4e	53	41	74	74	72	69	62	75	@NSAttribu
0020	74	65	64	53	74	72	69	6e	67	00	84	84	08	4e	53	4f	tedStringNSO
0030	62	6a	65	63	74	00	85	92	84	84	84	08	4e	53	53	74	bjectNSSt
0040	72	69	6e	67	01	94	84	01	2b	2e	4d	65	72	72	79	20	ring+.Merry
0050	43	68	72	69	73	74	6d	61	73	20	53	75	73	61	6e	21	Christmas Susan!
0060	fO	9f	8e	84	20	68	6f	77	20	68	61	76	65	20	79	6f	how have yo
0070	75	20	62	65	65	6e	3f	20	86	84	02	69	49	01	2c	92	u been?iI.,.
0800	84	84	84	0c	4e	53	44	69	63	74	69	6f	6e	61	72	79	NSDictionary
0090	00	94	84	01	69	01	92	84	96	96	1d	5f	5f	6b	49	4d	kIM
00a0	4d	65	73	73	61	67	65	50	61	72	74	41	74	74	72	69	MessagePartAttri
00b0	62	75	74	65	4e	61	6d	65	86	92	84	84	84	08	4e	53	buteNameNS
00c0	4e	75	6d	62	65	72	00	84	84	07	4e	53	56	61	6c	75	NumberNSValu
00d0	65	00	94	84	01	2a	84	99	99	00	86	86	86				e*

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!

E Keywor	I Keyword Result List Gallery View S Video View								
🖗 o 🔯	AZ▼ Filename	(19 H		Hit Offset (I					
	Filename	Hits	Hit Text	Hit Offset (File)					
₽-□	_ATXDataStore.db	1							
		1/1	'Ubytes0*+.)Christmas Susan! 8 how have yo	615530					
₽-Ę-	knowledgeC.db	2							
		1/2	<ubytes0*+.)christmas 8="" have="" how="" susan!="" th="" yo<=""><th>2285957</th></ubytes0*+.)christmas>	2285957					
		2/2	Oñê)Christmas Susan! Ə how have yo	2287959					
₽-□	📄 sms.db	3							
		1/3	tring+.Merry Christmas Susan!8 how have you	353634					
-		2/3	NSString+) Christmas Susan! 8 how have yo	353967					
		3/3	tring+.Merry Christmas Susan!8 how have you	354206					
₽-□	📄 sms.db-wal	3							
		1/3	tring+.Merry Christmas Susan!8 how have you	965514					
		2/3	NSString+) Christmas Susan! 8 how have yo	965847					
	_	3/3	tring+.Merry Christmas Susan!8 how have you	966086					
	22972402610564	2							
_		1/2	<ubytes0*+.) 8="" christmas="" have="" how="" susan!="" th="" yo<=""><th>262500</th></ubytes0*+.)>	262500					
		2/2	Oñê)Christmas Susan! Ə how have yo	264502					
00008110-	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 1	B 1C 1D 1E 1F 20 21 22						
69 73 74 ED	61 73 20 53 75 73	61 6E 2	1 20 F0 9F AA B4 20 68 String+) Christmas Sus	an! 8.ª1 h					
6E 3F 20 86	84 02 69 49 01 27	92 84 8	4 84 0C 4E 53 44 69 63 ow have you been?iI.'	NSDic					
96 96 1D 5F	5F 6B 49 4D 4D 65	73 73 6	1 67 65 50 61 72 74 41 tionary i kIMMe	ssagePartA					

Emoji F0 9F AA B4 represents a Potted Plant.

GR	You What is the emoji represented by the Unicode sequence F0 9F AA B4 Ø
6	ChatGPT The Unicode sequence `FO 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

Z▼ Source Name
ource Name
722655735826773
722655735826773
777