MAGNET VIRTUAL SUMMIT 2024 CAPTURE THE FLAG (CTF) ANDROID

UPDATED: 30 AUGUST 2024

About 1	This CTF Challenge	. 2
Questic	ons Only - Android	. 3
Starting	g this challenge in Forensic Explorer	. 5
Q1.	Warm Up (5 points)	. 8
Q2.	Press x to Respawn (5 points)	. 9
Q3.	Can you Handle this (5 points)	LO
Q4.	Need to reach those heights (5 points)	11
Q5.	Not to be basic but (5 points)	۱2
Q6.	Survival Mode Activated (5 points)	L3
Q7.	Sign me up! (5 points)	٤4
Q8.	Not so popular (5 points)	۱5
Q9.	You can never be too ready (10 points)	16
Q10.	Tag you're it! (10 points)	18
Q11.	A game of Cat and Mouse (10 points)	20
Q12.	Always achieving new heights (10 points)	22
Q13.	Remember your floaties (10 points)	25
Q14.	R-E-J-E-C-T-E-D Rejected (10 points)	26
Q15.	No two cents about them (10 points)	27
Q16.	LIVE your life (25 points)	28
Q17.	Out of Stock (25 points)	32
Q18.	So Salty! (25 points)	35
Q19.	Secrets Secrets are no Fun (25 points)	37
Q20.	Don't let them see you down (25 points)	38
Q21.	It's the eye of the tiger (25 points)	12
Q22.	Stalker Alert (50 points)	13

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

QUESTIONS ONLY - ANDROID

1.	Warm Up	What Southern state's sports team did Rocco search up?
2.	Can you Handle this	What was Rocco's Twitter account name?
3.	Need to reach those heights	What is the SIM operator name?
4.	Not to be basic but	What is the default Internet Browser?
5.	Survival Mode Activated	What conference did Rocco show interest in?
6.	Sign me up!	What email is associated with the device?
7.	Not so popular	How many messages were sent from Rocco in Twitter Direct Messages?
8.	No two cents about them	According to exCHANGEs in discord with Chad, what did Chad want back from Rocco?
9.	You can never be too ready	How many additional survival tips were provided in the \$9 book Rocco was looking into?
10.	Tag your're it!	What city was the user in when they identified an AirTag on them
11.	A game of Cat and Mouse	What game did two beloved cartoon characters promote in an Ad?
12.	Always achieving new heights	What was the new score achieved on the video game Rocco watched on YouTube?
13.	LIVE your life	What two sports did rocco capture in a photo (and)

14. Remember your floaties	What fun outdoor activity location was searched for?
15. R-E-J-E-C-T-E-D Rejected	When was the last shutdown that was initiated by Rocco? (YYYY- MM-DD HH:MM:SS) UTC 24 hour time.
16. Out of Stock	What is the most recent score in Subway Surfer
17. So Salty!	What is the handle of the person who is talking about how upset they are with Rocco?
18. Don't let them see you down	What was added using photoshop
19. It's the eye of the tiger	When is Rocco's Bday? (YYYY-MM-DD)
20. Secrets Secrets are no Fun	What did Rocco search in the App Store to download the app used to hide photos
21. Stalker Alert	Shortly after logging into Facebook with IP address 72.38.231.98, a photo was taken. Where was this photo taken?

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: Google Pixel 3a XL Logical Image Data.tar
- 5. In the Evidence Processor window use the default options.

Figure 1: Evidence > Add Image > Android - Google Pixel 3a XL Logical Image - Data.tar

Evidence	
· · · · · · · · · · · · · · · · · · ·	
	2024 Magnet CTF - Android (1)
Add device	Google Pixel 3a XL Logical Image - Data.tar (0)
ા: Add image 🗸	

PREPARATION: 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

PREPARATION: GRAPHICS OCR

Optical Character Recognition (OCR) extracts text content from graphics files so that it becomes available as text to be searched.

To perform **OCR**:

 In the File System module > File List, right-click and select OCR graphics files... from the dropdown menu:

Figure 3: File System > File List > OCR graphics files



2. In the OCR Files Options window, select the Searchable Items (all graphics).

Figure 4: OCR Files Options

🦉 OCR Files Options	_	\times
Source Searchable items (46481 items 18.16 GB) Highlighted items (1 items 2 KB) Checked items (5 items 7 KB)		

INDIVIDUALS OF INTEREST

The following profiles have been created from information contained within the evidence fi	iles:
--	-------

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. WARM UP (5 POINTS)

What Southern state's sports team did Rocco search up? (STATE ONLY)?

Q1. ANSWER

Louisiana (Louisiana Ragin Cajuns).

Q1. FORENSIC EXPLORER METHODOLOGY

The use of "Search up" in the question suggests web browsing. In the Artifacts module, a review of the Browsers > Google Query folder located search queries relating to a Louisiana football team.

Figure 5: Artifacts > Browsers > @ Google Query

Artifact Tree 🛛	🧮 File List		
Filter: 🔄 No Filter 🗸 😑	🖗 🗆 🎆	(AZ▼ URL	Query
□ Q Filename		URL	Query
Magnat 2024 CTE Andraid (E)	1	https://www.google.com/searc	call of duty mobile reviews 2023
	2	https://www.google.com/searc	ragin cajuns football record
Browsers (13)		https://www.google.com/searc	ragin cajuns football record
Google Query (266)	4	https://www.google.com/searc	ragin cajuns football roster
Chrome Autofill (2)			have be assured and allowed allowed a

The Origin Filename columns shows that these records come from Chrome History.

Figure 6: Artifact	s > Browsers	> Chrome History
--------------------	--------------	------------------

Artifact Tree	- ф	🛄 File List		
Filter: 🔄 No Filter 🗸 🗸		🖗 🖻 🔯	Last Visit Time	▲ football
Filename Magnet 2024 CTF Android (5) Browsers (13) G @ Google Query (266) G Chrome Autofill (2) G Chrome Bookmarks (6) G Chrome Cookies (3078) G Chrome Downloads (2) G Chrome Favicons (436) G Chrome History (398) G Chrome Keyword Search Terms	s (130)	1 2 3 4 5 6 7 8 9 9 10	Last Visit Time 15-Dec-2023 7:24:35 PM 15-Dec-2023 7:24:08 PM 15-Dec-2023 7:24:36 PM 15-Dec-2023 7:24:36 PM 15-Dec-2023 7:24:35 PM 15-Dec-2023 7:24:35 PM 15-Dec-2023 7:24:36 PM 15-Dec-2023 7:24:36 PM 15-Dec-2023 7:24:36 PM 15-Dec-2023 7:24:36 PM	URL https://www.google.com/search?q=ragin+cajuns+football+rec https://www.google.com/search?q=ragin+cajuns+football+rec https://ragincajuns.com/sports/football/roster https://ragincajuns.com/sports/football/roster/glenn-brown%2 https://www.google.com/search?q=ragin+cajuns+football+rec https://www.google.com/search?q=ragin+cajuns+football+rec https://www.google.com/search?q=ragin+cajuns+football+rec https://www.google.com/search?q=ragin+cajuns+football+rec https://ragincajuns.com/sports/football/roster https://ragincajuns.com/sports/football/roster https://ragincajuns.com/sports/football/roster https://ragincajuns.com/sports/football/roster/glenn-brown%2

The source path for Crome History data is:

• \data\data\com.android.chrome\app_chrome\Default\History

Q2. PRESS X TO RESPAWN (5 POINTS)

On what platform did Rocco share his Call of Duty Username?

|--|

Twitter.

Q1. FORENSIC EXPLORER METHODOLOGY

Artifacts > Search Artifact Results > Username returned hits from Twitter Direct Messages.



Figure 7: Artifacts > Search Artifact Results > Username

Search Artifacts Resul	ts						-		×
130122	username	Discord	Chat Android	[{"id":"11897038255(06979911"."channelI	d":"1189339	3735476	53172".	"me
130123	username	Discord	Chat Android	[{"id":"118970423654	40379146"."channell	d":"1189339	3735476	53172".	"me
130134	username	Facebook	Messenger Chat	Regardless I think	I'm signed in with	username Ch	adWickB	TWOOL	
130151	username	Facebook	Messenger Chat	Regardless I think	I'm signed in with	username Ch	adWickB	TW001	
130168	username	Facebook	Messenger Chat	Regardless I think	I'm signed in with	username Ch	adWickB	TW001	
130185	username	Facebook	Messenger Chat	Regardless I think	I'm signed in with	username Ch	adWickE	TW001	
123824	username	Twitter	Direct Messages An	Yeah I can show u I	'm not just talk.	My username	is OkCl	ick578	9.
123906	username	Twitter	Direct Messages An	Yeah I can show u I	'm not just talk.	My username	is OkCl	ick578	9.
Match Summary:									
RegEx Term		Hits							
			т						
username		56	Ţ						
Total Artifacts:		56							
Search Artifacts Res	sults finished.								
Search Artifacts Res Time Taken: 00:00:03	sults finished. 3								
					Copy to Clipboard	Save CSV and	Close	Clos	e

An Examination of Twitter Direct Messages shows user Rocco Sachs sending username OkClick5789.

🔚 Artifact Tree म	🔲 File List				
Filter: 🗾 No Filter 🗸 🕒	🖗 🖻 🔯	I Timestamp	₩2 vsername	A⊒▼ Sender Userr	Sender N
Magnet 2024 CTF Android (6) Magnet 2024 CTF Android (6) Browsers (13) Chat (5) Chat (5) Mobie (17) Mobie (17) Acostal Media (3) Facebook Contacts Android (4) Vitter Direct Messages Android (32) Witter Search Queries Android (20)	1 2	Timestamp 16-Dec-2023 11:17:51 PM 16-Dec-2023 11:17:51 PM	Text Yeah I can show u I'm not just talk. My <mark>username</mark> is OkClick5789. Yeah I can show u I'm not just talk. My <mark>username</mark> is OkClick5789.	Sender Username RoccoSachs96775 RoccoSachs96775	Sender Name Rocco Sachs Rocco Sachs

Figure 8: Artifacts >Twitter Direct Messages Android

Twitter Direct Messages source data is located in the following files:

- data\data\com.twitter.android\databases\1719897971716685824-66.db
- data\user\0\com.twitter.android\databases\1719897971716685824-66.db

Q3. CAN YOU HANDLE THIS (5 POINTS)

What was Rocco's Twitter account name?

Q2. ANSWER

RoccoSachs96775.

Q2. FORENSIC EXPLORER METHODOLOGY

The **accounts_de.db** SQLite database securely stores data related to the accounts configured on the device, including, but not limited to, account types, names, and authentication tokens. A review of Artifacts > Mobile > Accounts DE Android shows the Twitter account name as **RoccoSachs96775**.



Forensic Explorer 📙 🚵 🔻 🎲 👻 🕜					Forensic Explore
合 Evidence 🛛 File System 🗚 A	rtifacts	P Keyword Search	🔎 Index Search	() E	mail 🔠 Registry
Artifacts Artifacts Carve Artifacts To CSV	acts Searc	ch Artifact Event × esults Logs			
🔲 Artifact Tree 🛛 🕂	🔠 File List				
Filter: 🔄 No Filter 🗸 🖃	🖗 🗆 🔯	Last Password Ent	AZ▼ Username		′ Туре
		Last Password Entry	Username	User ID Typ	e
Marrie 2024 CTE Andreid (6) D	1	14-Dec-2023 3:46	roccotsachs@gmail.com	1 cor	n.google
	2	14-Dec-2023 3:46	roccotsachs@gmail.com	1 cor	n.google
EL Chat (5)	3	15-Dec-2023 10:0	RoccoSachs96775	3 cor	n.twitter.android.auth.login
	4	22-Dec-2023 4:19	Facebook	4 cor	n.facebook.auth.login
	5	22-Dec-2023 4:21	61554919820462	5 cor	n.facebook.auth.login
AirTag Personal Safety Android (2)	6	26-Dec-2023 9:53	Reddit for Android	6 cor	n.reddit.account
	7	26-Dec-2023 9:54	NarrowEcho 136	8 cor	n.reddit.account
	8	26-Dec-2023 10:0	Messenger	9 cor	n.facebook.messenger
Accounts DE Android (9)					
Accounts Notifications Android (10)					

This information can also be viewed directly in the source file by examining **accounts_de.db** in the File System module:

File List 🕃 Gallery View 😨 Vide	eo View 🕒	Disk View Category C	Graph	A-Z▼	File Sia	nature
Filename 1 accounts_de.db 2 accounts_de.db-journa	al	Extension Gra db db-jou	phic Classification	File Si SQLi No si	ignature te ize	
Google Pixel 3a XL Logical Image - [2 of 123340 Visible [LS 64 KB PS 64 KB]	Data.tar\data	\system_de\0\accounts_ 1 Highlighted [L5 NAME roccotsachs@gmail.com RoccoSachs96775 Facebook 61554919820462 Reddit for Android NarrowEcho 136 Messenger	de.db 5 64 KB PS 64 KB] TYPE com.google com.twitter.android.auth.l com.facebook.auth.login com.facebook.auth.login com.reddit.account com.reddit.account com.facebook.messenger	ogin	0 Ch	LAST_PASSWORD_ENTRY 1702568766863 1702678030428 1703261999679 1703262103103 1703627593775 1703627651929 1703628416226

Figure 10: File System > File List > accounts_de.db > Display View

Q4. NEED TO REACH THOSE HEIGHTS (5 POINTS)

What is the SIM operator name?

Q3. ANSWER

Boost mobile.

Q3. FORENSIC EXPLORER METHODOLOGY

A review of Artifacts > Mobile > Device identifies the **US** sim card operator as **Boost Mobile**.

Forensic Explorer 🚦 📸 🔻 🐼	👻 🧭 Forensic Explor	rer v5.
合 Evidence 🛛 🛅 File System	Artifacts 🖉 Keyword Search 🔎 Index Search @ Email 🏢 Registry	==
Artifacts Process Artifacts Carve Artifacts	Artifacts Mapping	
🗌 Artifact Tree 🛛 🕂	📰 File List	
Filter: 🗾 No Filter 🗸 🖃	🖗 🖻 🍘 🐼 * Card ID 😥 * Carrie 🐼 * Display N 🐼 * ICC ID 🐼 * IMSI 😡	≩▼ ISO
	Card ID Carrier Name Display Name ICC ID IMSI IS	SO Count
Image: Magnet 2024 CTF - Android (6) Image: Magnet 2024 CTF - Android (6) Image: Magnet 2024 CTF - Android (7) Image: Magnet 2024 CTF - Android (7)	1 B89000000000000000000000000000000000000	e JS

Figure 11: Artifacts > Mobile > Device Info Android

This information can also be viewed in the File System module by examining the source file

• com.android.providers.telephony\databases\telephony.db

Figure 12: File System > File List > telephony.db > Display View

File List 🔋 Gallery View 🔋 Vide	eo View 🛛 🚨 Disk Vi	iew 🕙 Catego	ory Graph			
🖗 🖻 👹 🕡 telephony.db		Ext	Az▼ Gr	aphic Clas	sification	File Signature
Filename		Extension	Graphic	Classificatio	n	File Signature
1 Lelephony.db		db				SQLite
2 Elephony.db-journal		db-jou				No size
📄 Google Pixel 3a XL Logical Image - D)ata.tar\data\user_	_de\0\com.andr	roid.prov	iders.telep	hony\databases\t	elephony.db
2 of 123340 Visible [LS 28 KB PS 28 KB]		1 Highlighted	I [LS 28 k	(B PS 28 K	B]	0 Checked
✓ Tables	_ID * ICC_	ID		SIM_ID	DISPLAY_NAME	CARRIER_NAME
> android_metadata	1 8900	000000000000000000000000000000000000000	03	255	CARD	1
✓ siminfo	2 8935	3022222807229	13	255	3	T-Mobile — 3
CREATE TABLE siminfo(id INI	3 8901	24031072762528	81	0	Boost Mobile	
> sqlite_sequence						

Q5. NOT TO BE BASIC BUT... (5 POINTS)

What is the default Internet Browser?

Q4. ANSWER

Chrome.

Q4. FORENSIC EXPLORER METHODOLOGY

The **roles.xml** file on an Android phone is part of the system's framework that manages role-based permissions. It is located in the path:

• data\misc_de\0\apexdata\com.android.permission\roles.xml

An examination of **Artifacts > Mobile > Roes XML Android** shows the default browser to be **chrome**.

Figure 13: Artifacts > Mobile > Roles XML Android

III Artifact Tree	🗜 🧮 File List		
Filter: 💭 No Filter 🗸 🗸	- 🖗 - 🐲	kaz ▼ Role	AZ▼ Holder
🗢 👰 Filename		Role	Holder
■ 🧱 2024 Magnet CTF - Android (6) 🛛		android.app.role.ASSISTANT android.app.role.ASSISTANT	com.google.android.goo com.google.android.goo
	3	android.app.role.BROWSER	com.android.chrome
Email (1) Enail (1) Cocations (2)	5	android.app.role.CALL_REDIRECTION	contantarolatentonic
Mobile (18)		android.app.role.CALL_REDIRECTION	
Accounts DE Android (8)	8	android.app.role.CALL_\$VERENING android.app.role.COMPANION_DEVICE_WATCH	
Battery Event (turbo) Android (1137)	□ 10 □ 11	android.app.role.COMPANION_DEVICE_WATCH android.app.role.DIALER	com.google.android.dial
Bluetooth Adapter Android (1)	12	android.app.role.DIALER	com.google.android.dial
Device Info Android (3) Files External Android (373)	13	android.app.role.EMERGENCY	com.google.android.app
Files Internal Android (228)	15 16	android.app.role.HOME android.app.role.HOME	com.google.android.app com.google.android.app
Google Play Search Android (50)	17	android.app.role.SMS	com.google.android.app com.google.android.app
Installed Applications Android (168)	170	android.app.role.SYSTEM_ACTIVITY_RECOGNIZER	com.google.android.gm
- Roles XML Android (50)	20	android.app.role.SYSTEM_ACTIVITY_RECOGNIZER android.app.role.SYSTEM_AMBIENT_AUDIO_INTELLIGENCE	com.google.android.gm com.google.android.as

Q6. SURVIVAL MODE ACTIVATED (5 POINTS)

What conference did Rocco show interest in?

Q5. ANSWER

Preppercon.

Q5. FORENSIC EXPLORER METHODOLOGY

A search of Artifacts > Browsers > Google Query located references to preppercon.

Figure 14: Artifacts > Browsers > @ Google Query

🔲 Artifact Tree 🛛 🕂	🛄 File List		
Filter: 🔄 No Filter 🗸 😑	i 🔁 🖗	₩ URL	k⊒▼ prep
Filename		URL	Query
2024 Magnet CTF - Android (6) 3 2024 Magnet CTF - Android (6) 3 4	1 2 3 4 5 6 7 8 9 10 11 12 13 14	 https://www.google.com/search?q=preppercon+202 https://www.google.com/search?q=preppercod+202 	preppercon 2023 dates usa preppercod 2024 preppercod 2024 preppercon 2024 preppercon 2023 dates usa preppercod 2024 preppercod 2024 preppercon 2023 dates usa preppercod 2024 preppercod 2024 preppercod 2024 preppercon 2024 preppercon 2024 preppercon 2024 preppercon 2024 preppercon 2024
Firefox Cookies (272)	14 15 16	 https://www.google.com/search?q=preppercod+202 https://www.google.com/search?q=preppercod+202 https://www.google.com/search?q=preppercon+202 	preppercod 2024 preppercod 2024 preppercon 2024

ChatGPT identifies that PrepperCon is a yearly conference relating to personal survival.

Figure 15



Q7. SIGN ME UP! (5 POINTS)

What email is associated with the device?

Q6. ANSWER

roccotsachs@gmail.com.

Q6. FORENSIC EXPLORER METHODOLOGY

A review of Artifacts > Chat Android Accounts identifies the email account as **roccotsachs@gmail.com**.

Figure 16: Artifacts > Chat > Android Accounts

Artifact Tree 🛛	🛄 File List				
Filter: 🔄 No Filter 🗸 😑	ig o 🔯	Account Name	Az Account	▲ Location	Source Na
■ A Filename		Account Name	Account Type	Location	Source Name
Magnet 2024 CTF - Android (6) Browsers (13) Chat (5) Android Accounts (2) Android Call Logs (18)	1 2	roccotsachs@gmail.com roccotsachs@gmail.com	com.google com.google	Table: accounts (row 0001) Table: accounts (row 0001)	contacts2.db contacts2.db

This information can also be viewed in the File System module by examining the source file:

• \data\com.android.providers.contacts\databases\contacts2.db

Figure 17: File System > File List > contacts2.db > Display View

I File Lis	t 😨 Gallery View 😨 Vide	o View 🛛 🔒 Disk View	🕙 Catego	ory Gra	ph				
i 🔁 🖗	▲ contacts2.db		€Z▼ Ext	Â-Z▼	Graphic Classification	n (Az ▼ File Si	gnature	
	Filename		Extension	Graph	ic Classification		File Signatur	e	
1	contacts2.db		db				SQLite		
2	contacts2.db-shm		db-shm				Sqlite SHM		
3	contacts2.db-wal		db-wal				Sqlite WAL		
4	contacts2.db		db				SQLite		
📄 Google P	Pixel 3a XL Logical Image - D	ata.tar\data\data\co	m.android.p	orovide	ers.contacts\database	es\contacts2	.db		
4 of 123340 \	/isible [LS 732 KB PS 733 KB]	1	Highlighte	d [LS 3	48 KB PS 348 KB]		0 C	hecked [LS	0 by
✓ ·Tables	c_state c_state_metadata unts CREATE TABLE accounts (exceptions presence	_ID * ACCOUN 1 roccotsa	NT_NAME hchs@gmail.co	om	ACCOUNT_TYPE com.google	DATA	SIM_SL	SIM_EF	

Q8. NOT SO POPULAR (5 POINTS)

How many messages were sent from Rocco in Twitter Direct Messages?

Q7. ANSWER

8.

Q7. FORENSIC EXPLORER METHODOLOGY

Twitter Direct Messages are located in:

- Artifacts > Social Media > Twitter Direct Message Android.
- Filter by Sender Username, Rocco.
- As data is sourced from two files, exclude the duplication to end with a result of 8.

Figure 18: Artifacts > Social Media > Twitter Direct Messages Android

📕 Artifact Tree म	🔠 File List				
Filter: 🔄 No Filter 🗸 😑	🖗 🖻 😻	8 Timestamp	AZ Text	AZ▼ rocco	Sender Na
Filename		Timestamp	Text 🔺	Sender Username	Sender Name
Manual 2024 CTE Andraid (6)	1	16-Dec-2023 9:11:26 PM	Absolutely! CoD is one of my favorites, especially CoD mobile it	RoccoSachs96775	Rocco Sachs
Magnet 2024 CTF Android (6)	2	16-Dec-2023 9:11:26 PM	Absolutely! CoD is one of my favorites, especially CoD mobile it	RoccoSachs96775	Rocco Sachs
E Chat (5)	3	16-Dec-2023 10:29:47 PM	I would say on a scale of 1 to 10 I'm a 7 or 8	RoccoSachs96775	Rocco Sachs
	4	16-Dec-2023 10:29:47 PM	I would say on a scale of 1 to 10 I'm a 7 or 8	RoccoSachs96775	Rocco Sachs
	5	16-Dec-2023 10:32:12 PM	Ive got these "vitamins" though that take me up to a 9 or 10	RoccoSachs96775	Rocco Sachs
	6	16-Dec-2023 10:32:12 PM	Ive got these "vitamins" though that take me up to a 9 or 10	RoccoSachs96775	Rocco Sachs
E- Social Media (3)	7	16-Dec-2023 10:42:52 PM	Lol not quite like Vitamin A. It makes you focus better, react fa	RoccoSachs96775	Rocco Sachs
Eacebook Contacts Android (4)	8	16-Dec-2023 10:42:52 PM	Lol not quite like Vitamin A. It makes you focus better, react fa	RoccoSachs96775	Rocco Sachs
Twitter Direct Messages Android (32)	9	16-Dec-2023 10:27:58 PM	Nice!	RoccoSachs96775	Rocco Sachs
Twitter Search Oueries Android (20)	10	16-Dec-2023 10:27:58 PM	Nice!	RottoSachs96775	Rocco Sachs
	11	26-Dec-2023 10:34:30 PM	t.co/IMxLe8z71xB%link.clashofclans.com/?action=	RoccoSachs96775	Rocco Sachs
	12	26-Dec-2023 10:34:30 PM	t.co/IMxLe8z71xB%link.clashofclans.com/?action=	RoccoSachs96775	Rocco Sachs
	13	17-Dec-2023 4:01:46 PM	They work for a bunch of games actually. And things outside o	RoccoSachs96775	Rocco Sachs
	14	17-Dec-2023 4:01:46 PM	They work for a bunch of games actually. And things outside o	RoccoSachs96775	Rocco Sachs
	15	16-Dec-2023 11:17:51 PM	Yeah I can show u I'm not just talk. My username is OkClick5789.	RoccoSachs96775	Rocco Sachs
	16	16-Dec-2023 11:17:51 PM	Yeah I can show u I'm not just talk. My username is OkClick5789.	RoccoSachs96775	Rocco Sachs
	📄 Social Me	edia\lwitter Direct Messages And	/bio/		

Q9. YOU CAN NEVER BE TOO READY (10 POINTS)

How many additional survival tips were provided in the \$9 book Rocco was looking into?

Q8.	ANSWER
-----	--------

72.

Q8. FORENSIC EXPLORER METHODOLOGY

In phone investigations evidence is frequently located in the DCIM\Cameras folder. The default File System module folders filter for Android Camera quickly isolates user pictures. The file PXL_20231215_202654750.jpg was immediately identified as relevant.



In the Keyword Search module, a search for **Survival Tips** was also conducted. As a result of running **Graphics OCR** in the preparation phase described above, keyword hits for **Survival Tips** were located in **OCR** output files (identified by ~OCR_eng in the screenshot below):

III Keywo	rd Result List 😨 Gallery View 😨 Video View								
🔯 🖻 🎆 🐼 Filename									
	Filename	Hits							
+ -	167.jpg~OCR_eng	1							
₽- □	167_reduced.jpg~OCR_eng	1							
⊕- □	230333cbab7d2f7b70188b879ae40e64e6f07340155d21ec660f540d811dde7a.0~OCR_eng	1							
⊕- □	230333cbab7d2f7b70188b879ae40e64e6f07340155d21ec660f540d811dde7a.0~OCR_eng	1							
₽- □	6fcf3764ada94070c76ffba92531067a7e2008b455021697d19159344d13b03d.0~OCR_eng	1							
₽- □	6fcf3764ada94070c76ffba92531067a7e2008b4550216974 9159344d13b03d.0~OCR_eng	1							
₽- □	9d9023ec29330150ac92aaf01c3ac92e4a81027a5a7028248d3b77d3c72df810.0~OCR_eng	1							
₽- □	9d9023ec29330150ac92aaf01c3ac92e4a81027a5a7028248d3b77d3c72df810.0~OCR_eng	1							
₽- □	de2b80410976b6e91086b698b4a100c4920a11a56362cee32e41a04235cf6dc5~OCR_eng	1							
₽- □	de2b80410976b6e91086b698b4a100c4920a11a56362cee32e41a04235cf6dc5~OCR_eng	1							
₽- □	f145c79b7fce98e38387bc86601a255dea79f3ffc020faa6eeb39a9bd32c50ef~OCR_eng	1							
÷-	f145c79b7fce98e38387bc86601a255dea79f3ffc020faa6eeb39a9bd32c50ef~OCR_eng	1							

Using the name of the OCR file of the keyword hit, a Filename column filter was used to find the parent graphic file:

Figure 21: Filtering for the parent file of OCR output



Figure 20: Keyword Search module > "Survival Tips"

Q10. TAG YOU'RE IT! (10 POINTS)

What city was the user in when they identified an AirTag on them?

Q9. ANSWER

Windsor, Ontario, Canada (42.3083344, -82.9654505).

Q9. FORENSIC EXPLORER METHODOLOGY

AirTag tracking information is located in **Artifacts > Location > AirTag Personal Safety Android**. The latitude and longitude of the located AirTag is 42.3083344, -82.9654505.

Figure 22: Artifacts > Locations > Air Tag Personal Safety Android

Artifact Tree 🕂	🛄 File List						
Filter: 🗾 No Filter 🗸 🚽	i 🖓 🖻 🎆	8 Timestamp	Last Updated Time	MAC Address	A-Z V State	AZ Latitude	Az Longitude
Filename		Timestamp	Last Updated Timestamp	MAC Address	State	Latitude	Longitude
Manual 2024 CTT Andreid (C) D	1	27-Dec-2023 10:40:00 PM	27-Dec-2023 10:40:0	CC:9C:0E:D8:0C:D0	STATE_STILL	42.3083344	-82.9654505
magnet 2024 CTF Android (6)	2	27-Dec-2023 10:40:00 PM	27-Dec-2023 10:40:0	CC:9C:0E:D8:0C:D0	STATE_STILL	42.3083344	-82.9654505
🗄 – 🛄 🗒 Chat (5)							
🕂 🔣 Email (1)							
E-Cocations (2)							
AirTag Personal Safety Android (2)							
🔄 🥥 AirTag Personal Safety Last Scan Android (
Mobile (17)							
⊕ 🔁 🧿 Social Media (3)							

This information can also be viewed in the File System module by examining the source file:

• data\com.google.android.gms\cache\personalsafety_db

However, in this case, the **DeviceData** table appears blank. This is because the data in the associated SQLite WAL (Write Ahead Logic) file has not yet been committed to the main database.

III File List III Gallery View III Video View 🕒 Disk View 🅙 Category Graph										
월 🖻 🛞 😡▼ personalsafety_db 🐼▼ File Cate 🐼▼ File Signatı 🐼▼ Ext 🐼▼ Path										
	Filename	Fil	e Category	File Signa	ture	Extension	Path			
1	personalsafety_db.lck			No size		lck	Google Pixel	3a XL Logica	al Image	- Data.ta
2	personalsafety_db	D	atabase	SQLite			Google Pixel	3a XL Logica	al Image	- Data.ta
3	personalsafety_db-shm	D	atabase	Sqlite SH	IM		Google Pixel 3a XL Logical Image - Data			- Data.ta
4	personalsafety_db-wal	D	atabase	Sqlite W	AL		Google Pixel	3a XL Logica	al Image	- Data.ta
📄 Google Pi	xel 3a XL Logical Image - Da	ata.tar\	data\data\c	om.google	android.gi	ms\databa	ses\personals	afety_db		
8 of 123340 Vi	isible [LS 941 KB PS 941 KB]			1 Highlight	ted [LS 32	KB PS 32 K	B]		700	Checked
✓ · Tables ✓ · Device ✓ · Scan ✓ · Scan ✓ · Scan ✓ · Scan ✓ · orom_	eData REATE TABLE `Scan` (`mac id_metadata master_table	Ro	`MACA	`CREA	`LAST	`STATE`	`BLESC	`LOCA	PRIMA	

Figure 23: File System > personalsafety_db > Display View

To view personalsafety_db in a third-party application:

- 1. highlight the three files:
 - a. personalsafety_db
 - b. personalsafety_db-shm (Shared Memory)
 - c. personalsafety_db-wal (Write Ahead Logic)
- 2. Right click and select **Export > Folders and Files:**

III File List 🛐 Gallery View 🛐 Video View 🖨 Disk View 🌒 Category Graph											
🖗 🖻 😻 🐼 personalsafety_d	P (reisonalsafety_db) (File Cate) File Signati) (
Filename File Category File Signature					Extension Mismatch	Exter	nsion	Path			
1 personalsafety_db	lck			No size			lck		Google Pixel 3a XL Logical Image - Data.tar\da		
2 personalsafety_db		Da	tabase	SQLite				1	Google Pixel 3a XL Logical Image - Data.tar\da		
3 personalsafety_db	shm	Da	tabase	Sqlite SHM		Add Bookmark			Google Pixel 3a XL Logical Image - Data.tar\da		
4 personalsafety_db	wal	Da	tabase	Sqlite WAL		Classify	•		Google Pixel 3a XL Logical Image - Data.tar\dat		
5 personalsafety_db	lck			No size		Flags	•		Google Pixel 3a XL Logical Image - Data.tar\da		
📄 Google Pixel 3a XL Logical Imag	e - Dat	a.tar\	data\data	\com.google.and	_	-		lb			
8 of 123340 Visible [LS 941 KB PS 94	1 KB1			3 Highlighted [g	Open 700 Checked II S 727 9 MB PS			700 Checked [LS 727.9 MB_PS 728.1 MB]		
						Open with	,		[]		
	1	(d	Туре	Name		Export	×		Export Rows (TAB, CSV, HTML, XLSX)		
						Send to module	•		Folders and Files		
						Determine file signature			Logical Evidence File (L01)		
					Expand compound file((s)		ZIP file (ZIP)			
				Hash		JavaScript Object Notation (JSON)					
						Morgo filos	L	—			

Then open the personalsafety_db with a tool like DB Browser for SQLite:

🗐 DB Browse	B Browser for SQLite - C:\Users\graha\Documents\Forensic Explorer v5\Cases\2024 Magnet CTF - Android\Exported\personalsafety_db											
<u>File E</u> dit <u>V</u> i	iew <u>T</u> ools I	<u>H</u> elp										
Gopen Project (Gave Project Gave Attach Database K Close Database K K Close Database K K Close Database K K Close Database K K K K K K K K K K K K K K K K K K K												
Database Structure Browse Data Edit Pragmas Execute SQL												
Table: Sca	Iable: 🗐 Scan 🗸 🛱 😵 💊 🖳 🖨 🖷 🖓 📾 🏂 Filter in any column											
mac	Address	creation	TimestampMillis	lastUpdatedTimestampMillis	state	bleScan	locationScan					
Filter		Filter		Filter	Filter	Filter	Filter					
1 CC:9C:0E	E:D8:0C:D0		1703716800000	1703716800000	STATE_STILL	BLOB	BLOB					

Q11. A GAME OF CAT AND MOUSE (10 POINTS)

What game did two beloved characters promote in an Ad?

Q10. ANSWER

Chase.

Q10. FORENSIC EXPLORER METHODOLOGY

"Cat and Mouse" and "beloved characters" could only mean Tom and Jerry. The "Ad" was likely to either be a video or a graphic.

To view videos:

- 1. In the File System module, branch plate [] the entire case.
- 2. Switch to Video View and browse the files.

Figure 24: File System > Video View > f034fda56f032783837c71b8a28635c0757e29c0



Figure 25: f034fda56f032783837c71b8a28635c0757e29c0



The path to the source file is:

• data\data\com.google.android.apps.tips\files\download\asset\f034fda56f032783837c71 b8a28635c0757e29c0

Q12. ALWAYS ACHIEVING NEW HEIGHTS (10 POINTS)

What was the new score achieved on the video game Rocco watched on YouTube?

Q11.	ANSWER
------	--------

5187.

Q11. FORENSIC EXPLORER METHODOLOGY

One of the great benefits of Chat GPT is the ability to quickly write more complex regex statements. A statement was created to find both **YouTube** and **video** within the same text.

Figure 26: Creating a RegEx statement in Chat GPT

GR	You create a regex statement where both the words "youtube" and "video" must appear in an sequence.	У
6	ChatGPT To create a regex statement where both the words "youtube" and "video" must appear in sequence, you can use positive lookahead assertions. This method checks for the prese both words without consuming any characters, allowing you to specify that both words r appear anywhere in the text, in any order. Here's how you can do it:	any nce of nust
	ruby (?=.*youtube)(?=.*video).*	Copy code

This regex statement was used in **Artifacts > Search Artifact Results** to locate items of interest.



Figure 27: Artifacts > Search Artifact Results

						-	~
Keyword Count:		1		Ţ			
Artifacts Module:				1			
Bates ID	RegEx Search Term	Folder		Match Text			
130090	^(?=.*voutube)(?=.*video)	Discord C	hat Android	[{"id":"118934	26047651	71913".	"ch
130115	^(?=.*voutube)(?=.*video)	Discord C	hat Android	[{"id":"118934	26047651	71913".	"ch
124045	^(?=.*youtube)(?=.*video)	Twitter T	weets Android	Where champion	is are ma	ade 2St	age
124413	^(?=.*youtube)(?=.*video)	Twitter T	weets Android	New Subway Sur	fers Hig	th Score	e1 (
125253	^(?=.*youtube)(?=.*video)	Twitter T	weets Android	Hey Gamers!	① Thin	king of	cr
125502	^(?=.*youtube)(?=.*video)	Twitter T	weets Android	Where champion	is are ma	ade 2St	age
125851	^(?=.*youtube)(?=.*video)	Twitter T	weets Android	New Subway Sur	fers Hig	jh Score	a1 (
126691	^(?=.*youtube)(?=.*video)	Twitter T	weets Android	A Hey Gamers!	① Thin	king of	cr
Match Summary:							
RegEx Term		Hits					
^(?=.*youtube)(?=	.*video).*	8					
Total Artifacts:		8					
Search Artifacts	Results finished.						
Search Artifacts	Results finished.						
Time Taken: 00:00	:04						
						5	
			Converte Clink	search Save CEV as	d Class	Close	

The results show that **Discord Chat Android** and/or **Twitter Tweets Android** are the likely source of the answer. A filter of these items located the following relevant entry:

📰 Artifact Tree म	🔠 File List				
Filter: 🗾 No Filter 🗸 –	🖗 🖻 🔯	Created	AZY_	AZ Author ID	Az▼ youtube
□ Agr Filename		Created	_ID	Author ID	Content
2024 Magnet CTE Andreid (6)	1	14-Dec-2023 6:00:47 PM	184	1166443278834659328	Where champions are m
	2	15-Dec-2023 3:37:01 PM	188	1166443278834659328	#CODMobile World Cha
	3	15-Dec-2023 3:00:27 PM	202	1648764058919657514	Snapdragon,https://t.c
	4	16-Dec-2023 3:33:14 PM	265	721704251962101764	LIVE NOW watching the
	5	📄 16-Dec-2023 4:45:32 PM	381	173571088961 792384	New Subway Surfers Hi
	6	15-Dec-2023 5:35:29 PM	383	1735710889611792384	COD Player here. How
	7	15-Dec-2023 3:00:58 PM	495	807726368444284928	THE WORLD CHAMPION
E- Sodal Media (5)	8	26-Dec-2023 4:48:54 AM	604	1735710889611792384	Pre-kill 🐔 https://t.co/)
Pacebook Contacts Android (4)	9	26-Dec-2023 11:31:20 PM	692	1735710889611792384	🖑 Hey Gamers! 🌒 Thir
Redait Accounts (2)	10	14-Dec-2023 6:00:47 PM	184	1166443278834659328	Where champions are m
Twitter Direct Messages Android (32)	11	15-Dec-2023 3:37:01 PM	188	1166443278834659328	#CODMobile World Cha
Twitter Search Queries Android (20)	12	15-Dec-2023 3:00:27 PM	202	1648764058919657514	Snapdragon,https://t.c
Twitter Tweets Android (736)	13	16-Dec-2023 3:33:14 PM	265	721704251962101764	LIVE NOW watching the
	14	16-Dec-2023 4:45:32 PM	381	1735710889611792384	New Subway Surfers Hi

The text related to a YouTube video:

New Subway Surfers High Score! https://t.co/K3y9DUC1kC via @YouTube Go check out my first video!,https://t.co/K3y9DUC1kC,youtu.be/dGhnVOpOoxQ?si...,YouTube

Playing this video on YouTube identified the highest score as 5,187.

Figure 28



Q13. REMEMBER YOUR FLOATIES (10 POINTS)

What fun outdoor activity location was searched for?

Q12. ANSWER

Big Water Campground, Ontario 655, Timmins, ON.

Q12. FORENSIC EXPLORER METHODOLOGY

Google Maps Search show a recent search for "Big Water Campground, Ontario 655, Timmins, ON", which ties in with "Floaties".

Figure 29: Artifacts > Google Searches Android

I Artifact Tree	ф.	🛄 File List				
Filter: 🔄 No Filter 🗸 🗸	-	🖗 🗆 🔯	I Timestamp	M₂ ▼ Place	Az Latitude	AZ V Longitude
Filename			Timestamp	Place	Latitude	Longitude
New Creek (C) 0		1	26-Dec-2023 9:35	"Big Water Campground, Ontario 655, Timmins, ON"	48.6037654	-81.2903952
→ New Case (6) ⊕- ⊕ ⊕- ⊕ ⊕- ⊕ ⊕- ⊕ ⊕- ⊕ ⊕- ⊕ ⊕- ⊕ ⊕- ⊕ ⊕- ♥ Locations (3) ⊕		2	26-Dec-2023 9:35	"Big Water Campground, Ontario 655, Timmins, ON"	48.6037654	-81.2903952
Air Tag Personal Safety Android (2) AirTag Personal Safety Last Scan Android GoogleMaps Searches Android (2)	(2)					

A keyword identifies multiple other files referencing this address:

Figure 30: Keyword Search > Big Water Campground

Keywor	d Result List 📰 Gallery	View 😨	Video View		
i 🚳 🗆 🖗	Az▼ Filename	(19 H)		Hit Offset (I	Hit Offset (I
	Filename	Hits	Hit Text	Hit Offset (File)	Hit Offset (Parti
	directions_10977	13			
		1/13	Gg==éu.6 <mark>Big Water Campground</mark> , 6940 ON-655,	1104	1266762832
		2/13	Õ.RTÀ(<mark>Big Water Campground</mark> . 6940 ON-655,	1224	1266762952
		3/13	, ON P4N 7H9 <mark>Big Water Campground</mark> . 6940 ON-655,	1280	1266763008
		4/13	35ce33182c7c.6 <mark>Big Water Campground</mark> , 6940 ON-655,	1399	1266763127
		5/13	AQoAQ@.J8 <mark>Big Water Campground</mark> b llj4HPARjM98	1532	1266763260
		6/13	zNwujxN*6 <mark>Big Water Campground</mark> , 6940 ON-655,	1593	1266763321
		7/13	0 ON-655b <mark>Big Water Campground</mark> zJP	55731	1266817459
	2	8/13	onto2.EST <mark>Big Water Campground</mark> . 6940 ON-655,	56975	1266818703
	- 0	9/13	, ON P4N 7H9 <mark>Big Water Campground</mark> . 6940 ON-655,	57031	1266818759
		10/13	0 ON-655b <mark>Big Water Campground</mark> zJF	154928	1266916656
		11/13	onto2.ESTBig Water Campground. 6940 ON-655,	156172	1266917900
		12/13	, ON P4N 7H9 <mark>Big Water Campground</mark> . 6940 ON-655,	156228	1266917956
		13/13	Ü.ÌÂTÀ(u.6 <mark>Big Water Campground</mark> , 6940 ON-655,	303552	1267065280
₽-_	odelay_cache.cs	3			
		1/3	Big Water CampgroundOntario 655,	854	1267482966
		2/3	:	916	1267483028
		3/3	MH@!.ûèÔ.RTÀ". <mark>Big Water Campground</mark> j.BChIJpS-rM30	1023	1267483135
₽-□	new_recent_hist	2			
		1/2	.à	25	1267486233
		2/2	Timmins, ON <mark>Big Water Campground</mark> Ontario 655,	73	1267486281
₽-□	📄 gmm_storage.db	120			
		1/120	w u 6 <mark>Big Water Campground</mark> 6940 ON-655	47877	1267618123
📄 Google Pi	xel 3a XL Logical Image ·	- Data.tar\	data\user\0\com.android.chrome\app_chrome\Default\Offline P	ages\metadata\Off	linePages.db

Q14. R-E-J-E-C-T-E-D REJECTED (10 POINTS)

When was the last shutdown that was initiated by Rocco? (YYYY-MM-DD HH:MM:SS) UTC 24 hour time.?

Q13. ANSWER

2023-12-28 18:47:29.403 GMT-05:00 = 2023-12-28 23:47:29

Q13. FORENSIC EXPLORER METHODOLOGY

Shutdown Checkpoints are located at:

\data\system\shutdown-checkpoints\checkpoints-1703807249418

Figure 31: Artifacts > Shutdown Checkpoints Android

Forensic Explorer 🚦 🚵 👻 🎯						Forensic Explor	er v5.6.8(4894d) (64	lbit) Case: Mag
合 Evidence 🗋 File System 🗚	vrtifacts	🔑 Keyword Search	🔎 Index Se	arch	(C) Email	Registry	Bookmarks	Reports
Artifacts Process Artifacts Carve Artifacts Carve Artifacts To CSV Map	acts Search ping Re	h Artifact esults						
Artifact Tree 4	🔜 File List							
Filter: 🍠 No Filter 🗸 🚽	🖗 🖻 👹	Timestamp String	A	🖉 🛛 Reqi	AZ user			
Magnet 2024 CTF Android (5) Magnet 2024 CTF Android (5) Canada (5) Canada (1) Canada (1) Accounts DE Android (7) Accounts DE Android (10) Canadars Android (1137) Satury Event (turbo) Android (1137) Canadars Android (2) Canadars Android (2) Files External Android (238) Files External Android (238) Files Enternal Enternal Android (238) Files Enternal Enternal Android (238) Files Enternal Entern	1 2 3 4 5 6 6 7 8 9 10 11 12 13 14 15	Timestamp String 2023-12-15 05:29:21.0 2023-12-15 07:59:03.7 2023-12-15 07:59:00.0 2023-12-15 07:15:00.0 2023-12-18 10:18:35.8 2023-12-18 20:06:02.1 2023-12-20 22:38:54.8 2023-12-24 16:09:39.8 2023-12-24 16:21:93.3 2023-12-24 16:21:93.3 2023-12-24 16:21:93.3 2023-12-26 18:09:25.4 2023-12-26 18:09:25.4 2023-12-27 12:22:56.4 2023-12-27 12:22:56.4 2023-12-28 13:49:50.4 2023-12-28 13:49:10.4 2023-12-28 13:49:10.4 2023-12-28 13:49:10.4	A F GMT-05:00 97 GMT-05:00 95 GMT-05:00 25 GMT-05:00 21 GMT-05:00 10 GMT-05:00 10 GMT-05:00 13 GMT-05:00 31 GMT-05:00 31 GMT-05:00 46 GMT-05:00 4	Requestor BINDER BINDER BINDER BINDER BINDER BINDER BINDER BINDER BINDER BINDER BINDER BINDER BINDER BINDER BINDER BINDER	Entry Shutdown reques Shutdown reques	t from BINDER for reaso t from BINDER for reaso	n userrequested at 2023- n userrequested at 2023-	12-15 05:29:21.00., 12-15 07:59:03,79., 12-15 17:15:28.06., 12-18 10:18:35.82., 12-18 12:06:00.21.2., 12-20 22:38:54.86., 12-22 15:10:55.51., 12-24 16:21:94.33., 12-26 17:00:37.27., 12-26 18:09:26.43., 12-27 12:22:56.49., 12-27 12:22:56.49., 12-28 13:49:04.17., 12-28 13:49:05.23., 12-28 1
Google Play Search Android (50) Installed Applications Android (168) Installed Applications Google Play Android (170 Stuttops Secure Android (1) Stuttops Cecure Android (1) Google Play Android (43)	16	2023-12-28 18:47:29.4	03 GMT-05:00	BINDER	Shutdown reques	t from BINDER. for reaso	n <mark>user</mark> requested <mark>a</mark> t 2023-	12-28 18:47:29.40

The relevant checkpoint is:

Shutdown request from BINDER for reason userrequested at 2023-12-28 18:47:29.403 GMT-05:00 (epoch=1703807249403).

Q15. NO TWO CENTS ABOUT THEM (10 POINTS)

According to exCHANGEs in discord with Chad, what did Chad want back from Rocco?

Q14. ANSWER

Money.

Q14. FORENSIC EXPLORER METHODOLOGY

A column filter in **Artifacts module > Chat > Discord Chat Android** was used to locate the following message:

Figure 32: Artifacts module > Chat > Discord Chat Android

Artifact Tree 4	I File List			
Filter: 🔄 No Filter 🗸 🚽	🖗 🖻 🎆 I	Mer Timestamp String	AZY Sender	😥 🕶 money þack
🖻 🐼 🕶 Filename	_	Timestamp String	Sender	Message
Magnet 2024 CTE Android (5)		2023-12-27T22:35:37.628000+00:00	chadwickgames	well now "stalking" is a strong word I prefer keeping an eye on you ?? I will get my money back of
+ Browsers (13)	2	2023-12-27T22:35:37.628000+00:00	chadwickgames	well now "stalking" is a strong word I prefer keeping an eye on you ?? I will get my money back of
E-F (Chat (5)	3	2023-12-27T22:57:28.026000+00:00	oneclick5864_28820	You are seriously crazy No way I'm giving you that money back. Even if I wanted to you know I'm
Android Accounts (2)	4	2023-12-27T22:57:28.026000+00:00	oneclick5864_28820	You are seriously crazy No way I'm giving you that money back. Even if I wanted to you know I'm
Android Call Logs (18)			N	
Android Messages (218)			his	
Discord Chat Android (50)				
- Facebook Messenger Chat (68)				
Email (1)				

The Discord source file is an SQLite database. The message content is contained in a Binary Large Object, which can be exported and examined in a SQLite application such as DB Browser.

Figure 33: Discord Chat source data

Fo	Iders Categories	I File List	🔋 Gallery View	🔋 Video	View 🔒	Disk View 🕘 Category Grap
Filter:	🔄 No Filter 🗸 📼	🖗 🖻 🚳	f⊌ ▼ ^a\$	Az▼ Ext	Az▼ Fil	e Signature
Filename	A		Filename	Extensior	n File Signa	ature
	atastore (1)				SOLite	
	🖃 🕒 📴 kv-storage (1)				COLita	
	@account. 1185636389107273799 (3)		<u> </u>		SQUILE	
	🗄 🕒 📄 otas (2)					
	— 🖻 📄 no_backup (4)	Google Pi	vel 3a XI. Logical II	mage - Da	ta tar\data	\data\com_discord\files\by-
	🕒 🕒 📴 shared_prefs (20)	✓ · Tables			PowID	
	🕀 🕒 📄 com.einnovation.temu (12)	> ·kv0			ROWID	
	🗄 🕒 📄 com.facebook.katana (60)	> ·kv_cache0			85	Binary Large OBject
	+- D a com.facebook.orca (43)				86	Binary Large OBject
	com.google.android.accessibility.soundamplifier (5)	CF	EATE TABLE messa	ges0 (a,	87	Binary Large OBject
+-> Com.google.android.apps.camera.services (6)		> meta			88	Binary Large OBject
	+ Com.google.android.apps.carrier.carrierwifi (6)				89	Binar Aarge OBject
	+- D = com.google.android.apps.carrier.log (2)				90	Binary Large OBject

Q16. LIVE YOUR LIFE (25 POINTS)

What two sports did rocco capture in a photo (__ and __)?

Q15. ANSWER

Golfers and skiers.

Q15. FORENSIC EXPLORER METHODOLOGY

Clearly this question relates to photo that are likely to be taken by the Android phone. A fast way to examine photos is to:

- 1. In the File System module, branch plate [] the entire case.
- 2. Use the File System > Android > folders filters:

Forensic	Explorer	8 👌 🖥	- 🎲 🖵 🍳		
合 Evid	ence	File Sy	stem	Artifa	cts
Recover Folders	C File Name Search	File Carve	Shadow Copy	Signature ~ Analysis	Expa File
Folders	Catego	ories			
Filter: 🗐 I	No Filter				× •
Filename	Androw Andro	id 12)			_
	And And And And And	roid Camera roid Moving Pi roid Screensh roid Snapshot	ctures ots s		

A filter for **Android** Camera and a manual review of the camera photos in File System > Gallery View did not locate any obvious photos containing sports.

A filter for **Android Moving Pictures** did identify the following picture of potential value as it appears to contain text in the embedded video.



Figure 34: File System > Folders Filter > Android Moving Photos

The text in the picture is not clear in the Display View, so additional steps were required to extract the video segment and examine it in more detail:

- 1. In the File System module > Folder Tree > right-click and **Clear All Checks**.
- 2. Check the file PXL_20231220_234032213.MP.jpg.
- 3. Click on the File System > Toolbar > File Carve button.
 - a. Carve Checked items (1 items 12.1 MB).
 - b. Change the Search Mode to Byte (slow).
 - c. Checkbox Video.
- 4. Click **OK** to launch the carve. Note that the carve process may take up to 30 seconds to finish.

Forensic Explorer 🚦 🚵 👻 💭	0
🔂 Evidence 🔂 File System	Artifacts 🖉 Keyword Search 🔎 Index Search
Recover File Name Folders Search	w Signature Expand Expand Extract Analysis Tria
🐺 Folders 📱 Categories	📰 File List 🔋 Gallery View 🔋 Video View 🖳 Disk View 🌯 Category
Filter: 🔄 Android Moving Pictures 🗸 두	🖗 🖻 👹 🐼 Filename 🐼 Extensic
Filename	Filename Extension
Magnet 2024 CTF - Android (0)	1 m PXL 20231217 165129946.MP.jpg jpg
E B ata (0)	Z ■ PXL_20231220_234032213.MP.jpg jpg J = PXL_20231220_235235170 MP ing ing
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	4 PXL 20231222 154741911.MP.jpg jpg
白- 🖻 🔲 🚞 0 (0)	5 pXL_20231227_235408812.MP.jpg jpg
Ė- 🖻 🔳 📴 DCIM (0)	
— 🖻 🔳 🔂 Camera (5)	File Carve Options
	Process Name:
	File Carve
	Source
	Unallocated space (0 items 0 bytes)
	Checked items (1 items 12.1 MB)
	Include Raw Devices, Partitions and Files
	Search Mode: Byte (slow) \checkmark Byte Offset: 0
	File types to carve:
	E Documents
	📲 🕀 💭 💭 Email
	🕀 🗍 🔛 Text (WARNING: Slows Search)
	🗉 🔽 妇 Video
	🕀 🗍 💼 Apple OS

Figure 35: File System > File Carve (byte level) a checked item for embedded video

The result of the carve will appear in the File System module tree in the **File Carve** folder. Click on the carved .mov file to view the video in the **Display View**. If the Display View is not clear, right click on the file and open it in a external video program like **VLC**. The relevant text is located at the start of the video, as shown below:

Forensic Explorer	🔒 👌 🕶 🎲 🕶 🔇				
Evidence	File System	Artifacts	P Keyword Search	₽ Index Search	h
Recover File Name Folders Search	File Carve	Signature Kap Analysis Fil	and Expand Video	 Analysis Programs Tria) age
Folders Categ	ories	File	List Gallery View 😨 Vide	o View 🔚 Disk View	🕙 c
Filter: 🗐 No Filter		🗸 🖃 🛄 File Lis	t		
Filename		× 🖗 🖻 🖗	Filename)(4	€Z* E
Nagnet 2024 0	TTF - Android (1) []		Filename	E	Extens
	el 3a XL Logical Image - Dat ve (1)	'a.tar (2)	Carved_Mov_52262486	s.mov	mov
E-D data (4	(E)				
		-			
			LANDMAR	sik.	
			CRUENZ		
			Frequentes		
			oy gould to be		
			ummerage s	>	

Figure 36: File System > File Carve results folder

Q17. OUT OF STOCK (25 POINTS)

What is the most recent score in Subway Surfer?

Q16. ANSWER

1899.

Q16. FORENSIC EXPLORER METHODOLOGY

Method 1:

In the Artifacts module:

- 1. Select Mobile > Application Usage Android.
- 2. Filter the **Package Name** column for **subwaysurf**.
- 3. Double-click on the **Timestamp** column heading to sort by date.
- 4. Activity on subway surfer last stopped on **28-Dec-2023 at 10:49:19pm**.

Figure 37: Artifacts > Mobile > Application Usage Android

Artifact Tree 4	🚟 File List			
Filter: 🔄 No Filter 🗸 🧧	🖗 🖻 😻	Timestamp	com.kiloo.subway	Event Type
□ Image: Filename		Timestamp 🔺	Package Name	Event Type
■ 2024 Magnet CTF - Android (6) [56 57 58 59 60 61 62 63	28-Dec-2023 10:44:03 PM 28-Dec-2023 10:44:04 PM 28-Dec-2023 10:44:05 PM 28-Dec-2023 10:44:05 PM 28-Dec-2023 10:44:05 PM 28-Dec-2023 10:44:05 PM	com.kiloo.subwaysurf com.kiloo.subwaysurf com.kiloo.subwaysurf com.kiloo.subwaysurf com.kiloo.subwaysurf com.kiloo.subwaysurf com.kiloo.subwaysurf	ACTIVITY_PAUSED ACTIVITY_STOPPED ACTIVITY_STOPPED ACTIVITY_STOPPED ACTIVITY_STOPPED ACTIVITY_RESUMED ACTIVITY_RESUMED ACTIVITY_PAUSED
Accounts Notifications Android (10)	64 65	 28-Dec-2023 10:49:18 PM 28-Dec-2023 10:49:19 PM 28-Dec-2023 10:49:19 PM 	com.kiloo.subwaysurf com.kiloo.subwaysurf	ACTIVITY_PAUSED ACTIVITY_STOPPED
Battery Event (turbo) Android (1137)		E 20-DEC-2023 10:49:19 PM	com.kioo.subwaysuri	ACTIVITI_STOPPED

In the File System module:

- 1. Branch plate [] the entire case.
- 2. Double-click on the Modified column header to sort by Modified.
- 3. Apply a column filter for **28-Dec-2023 10:4**.

	III File List	8	Gallery View 🔋 Video View 🦲 Disk View	🕙 Catego	ory Graph	
B	- 🖗 (A-Z	▼ Filename	AZ▼ Ext	38-Dec-2023 10:4	<u>A</u> ₂▼
		File	name	Extension	Modified 🛛	Path
	2086		u_notification_data_47.xml	xml	28-Dec-2023 10:49:18 PM	God
	2087		u_notification_data_48.xml	xml	28-Dec-2023 10:49:18 PM	Goo
	2088		u_notification_data_49.xml	xml	28-Dec-2023 10:49:18 PM	God
	2089		u_notification_data_50.xml	xml	28-Dec-2023 10:49:18 PM	God
	2090		u_notification_data_51.xml	xml	28-Dec-2023 10:49:18 PM	God
	2091		u_notification_data_52.xml	xml	28-Dec-2023 10:49:18 PM	God
	2092		u_notification_data_53.xml	xml	28-Dec-2023 10:49:18 PM	Goo
	2093		u_notification_data_54.xml	xml	28-Dec-2023 10:49:18 PM	Goo
	2094		u_notification_data_55.xml	xml	28-Dec-2023 10:49:18 PM	Goo
	2095		adc_events_db		28-Dec-2023 10:49:19 PM	Goo
	2096		network_requests		28-Dec-2023 10:49:19 PM	God
	2097		persistent_postback_cache.json	json	28-Dec-2023 10:49:19 PM	God
	2098		com.applovin.sdk.1.xml	xml	28-Dec-2023 10:49:19 PM	Goo
	2099		256.jpg	jpg	28-Dec-2023 10:49:19 PM	Goo
	2100	Ħ	256_reduced.jpg	jpg	28-Dec-2023 10:49:19 PM	Goo
	2101		adc_events_db		28-Dec-2023 10:49:19 PM	Goo

Figure 38: File System > Filter by Modified date

Switching to Gallery View, two Subway Surfer snapshots dated 28-Dec-2023 at 10:49 were located:

- \data\system_ce\0\snapshots\256.jpg
- \data\system_ce\0\snapshots\256_reduced.jpg

Figure 39: \data\system_ce\0\snapshots\256.jpg



Method 2:

Recent activity is commonly tracked on stock Android phones at path:

• \data\system_ce\0\recent_tasks

Decoding of these binary XML file currently underway. Check back soon.

Figure 40: File System > recent_taks

Folders Categories	III File List	😨 Gallery View 😨 Video View 🔒	Disk View	🕙 Catego	ory Graph
Filter: 🔄 Android Recent Tasks 🗸 🗢	🖗 🗆 🔯 I	Ilename		Az ▼ Ext	File Signature
Filename		Filename		Extension	File Signature
🗈 🔳 🚟 Magnet 2024 CTF - Android (0) 🛛	✓ 1	116_task.xml		xml	Unknown
🗄 💽 🔳 💀 Google Pixel 3a XL Logical Image - Data, tar (0)	✓ 2	135_task.xml		xml	Unknown
🖻 💽 🔲 🚞 data (0)	✓ 3	136_task.xml		xml	Unknown
🗄 💽 🔳 📴 system_ce (0)	✓ 4	140_task.xml		xml	Unknown
Ė-🖸 🔲 📴 0 (0)	✓ 5	158_task.xml		xml	Unknown
🕒 💽 🔽 📴 recent_tasks (37)	6	167_task.xml		xml	Unknown
	7	172_task.xml		xml	Unknown
	8	177_task.xml		xml	Unknown
	9	180_task.xml		xml	Unknown
	✓ 10	📄 185 task.xml		xml	Unknown

Q18. SO SALTY! (25 POINTS)

What is the handle of the person who is talking about how upset they are with Rocco?

Q17. ANSWER

@larissajenna9.

Q17. FORENSIC EXPLORER METHODOLOGY

In the Artifacts module **Search Artifact Results** for **Salty** to identify **Twitter Tweets Android** as the potential source.



Figure 41: Artifacts > Search Artifacts Results > "Salty"

Search Artifacts Re	sults		N	-		×
Keyword Count:		1	2			
Artifacts Module: Bates ID	RegEx Search Term	Folder	Match Text			
125241 126678	salty salty	Twitter Tweets Android Twitter Tweets Android	For all of you wondering why I've been in such a salty mood th For all of you wondering why I've been in such a salty mood th	is holid is holid		
Match Summary: RegEx Term		Hits				
salty		2				
Total Artifacts: Search Artifacts H	Results finished.	2				
Search Artifacts F Time Taken: 00:00:	Results finished. :03					
						Ŧ
			Copy to Clipboard Save CSV ar	d Close	Close	

In the Artifacts module, run a column filter on Twitter Tweets Android Content column for Salty.

Filter: 🔄 No Filter 🛛 🗸 👄	😼 🖻 🐯	Created	A-Z T	AZ Author ID	AZ▼ salty
		Created	ID	Author ID	Content
🕒 🥶 Fliename		26-Dec-2023 9:56:24 PM	680	1739363969809227776	For all of you wondering why I've been in such a salty m
🔲 🚟 Magnet 2024 CTF - Android (6) 🛛		26-Dec-2023 9:56:24 PM	680	1739363969809227776	For all of you wondering why I've been in such a salty m
🗄 🗌 🎯 Browsers (14)	L ~		000	1/0/00000000000000000000000000000000000	i di di or you vondening viry 1 ve beer in baer a barry
🕀 🛄 💬 Chat (5)					
🛨 🔂 Email (1)					
🕀 🔽 💙 Locations (3)					
🕂 🛄 Mobile (20)					
🗄 🔲 💿 Social Media (5)					
				45	
— 🔂 😁 Reddit Accounts (2)					
—— 🔰 Twitter Direct Messages Android					
—— 🔰 Twitter Search Queries Android (
🖵 🔰 Twitter Tweets Android (736)					

The **Author ID** column lists the author as **1739363969809227776**. There are multiple online sites online, such as <u>https://commentpicker.com/twitter-id.php</u>. that resolve a Twitter ID. This shows the handle to be **@larissajenna9**.

Figure 43: https://commentpicker.com/twitter-id.php

TWITTER ID & USERNAME	
TWITTER ID / X ID	
1739363969809227776 📋	
TWITTER USERNAME	
<u>(@larissajenna9</u> 🗷	
NAME	
Larissa Jenna	

A Keyword Search for Salty Mood located a number of OCR hits:

Figure 44: Keyword Search for "Salty Mood"

E Keyw	ord Result List 😨 Gallery View 😨 Video View	
5 o 🐯	€2 Filename	19 Hits
	Filename	Hits
+ -	8odv6TQHebCMedZrtO1PAhQ0UBQ~OCR_eng	1
₽-	hBtmvONwE1t4w3pXWAXJctROjHc~OCR_eng	1
∲- □	screenshot3245726116852701563.png~OCR_eng	1
₽- □	screenshot6545948068700152483.png~OCR_eng	1

Which identify the png source file in the Twitter cache folder:

Figure 45: data\user\0\com.twitter.android\cache\screenshot3245726116852701563.png



Q19. SECRETS SECRETS ARE NO FUN (25 POINTS)

What did Rocco search in the App Store to download the app used to hide photos?

Q18. ANSWER

Calculator vault.

Q18. FORENSIC EXPLORER METHODOLOGY

Artifacts > Mobile > Installed Applications Android shows that Calculator Lock is installed.

Figure 46: Artifacts > Mobile > Installed Applications Android



Artifacts > Mobile > Google Play Search Android shows the search term used was calculator vault.

Tree 4	III File List				
Filter: 🗾 No Filter 🗸 🧧	🖗 🖻 🎆	TimeStamp	<pre> calc </pre>	Query	
□ 👰 Filename		TimeStamp	Display	Query	
Magnet 2024 CTF Android (5) Imagnet 2024 CTF Android (7) Imagnet 2024 CTF Android (7) Imagnet 2024 CTF Android (7) Imagnet 2024 CTF Android (8) Imagnet 2024 CTF Android (10) Imagnet 2024 CTF Android (2) Imagnet 2024 CTF Android (2) Imagnet 2024 CTF Android (3) Imagnet 2024 CTF Android (223)	□ 1 □ 2	 24-Dec-2023 7:52:37 PM 24-Dec-2023 7:52:37 PM 	calculator vault calculator vault	calculator vault calculator vault	
Files Master Android (161) Google Play Search Android (50)					

Figure 47: Artifacts > Mobile > Google Play Search Android

Q20. DON'T LET THEM SEE YOU DOWN (25 POINTS)

What was added using photoshop?

Q19. ANSWER

Good Job! Success.

Q19. FORENSIC EXPLORER METHODOLOGY

Attempt 1:

My first instinct in this question was to see which files have been edited with Photoshop by extracting metadata and looking at the **Exif 305: Software** value for **Photoshop**.

Figure 48: File System > Extract Metadata



This methodology did indeed locate pictures that appear to have been manipulated, as shown below:

Figure 49: File System > filter by Exif 305: Software > photoshop



Whilst the above file may be a technically correct answer to this question, as it is an Android phone, it seemed rather improbable that the edit would involve using the full Photoshop software.

Attempt 2:

In the File System module:

- 4. Branch plate [] the entire case.
- 5. Apply a **Filename** column filter for **photoshop**.

This identifies a **Photoshop Express** folder in the path: **Google Pixel 3a XL Logical Image -**Data.tar\data\media\0\Pictures\.

Figure 50:

Forensic Explorer	🔒 🚵 🕶 🎲 🕶 🔮					
Evidence	File System	Artifacts	P Keyword	Search	Index Search	
Recover File Name Folders Search	File Carve Copy	Signature Analysis File	nd Expand Video	<mark>M</mark> Extract → An Metadata Prog	alysis v Triage v	
Folders Categories				t 🔋 Gallery View	📰 Video View 🛛 🔒 Disk	
Filter: 🔄 No Filter 🗸 🕒			🖗 🖻 🚳	🖗 🖻 🔯 🕡 photoshop		
Filename		Filename				
Magnet 2024 (1	Photoshop Exp	press			
🗄 🕒 🔜 🚮 Google Pixe	1					

3. Branch plate [▶] jus the Photoshop Express folder and it appears to contain pictures that have been manipulated.

Folders Categories	File List 🔋 Gallery View 🔋 Vid	eo View 🛛 🔒 Disk View 🏾 🅙 Category Graph
Filter: 🗾 No Filter 🗸 🗢	🌼 🔿 🚫	P
Filename 	PSX_20231226_155813.png	Good Jobi , Good Jobi ,
\square \square \square \square $property (1)$	F3A_20231220_133039.phg	F3A_20251220_100220.prig
-D is resource-cache (61) D-D is rollback (1)	4 of 4 Visible [LS 1.3 MB PS 1.3 MB]	0 Highli

Figure 51: File System > Photoshop Express folder > Gallery View

To locate the source file, in the **File System** module a **Hash Files** was run to give each graphic a **Differential Hash**:

Figure 52: File System > Hash Files > Differential Hash

# # # Hash Hash Hash Set Files Match Create	tual Boot	Cisco Clam Anti Virus	(y) Yara Rules
 Hash Files Options Source Searchable items (123341 items 25 Unallocated space Checked items (1 items 12.1 MB) Include Raw Devices, Partitions 	.38 GB) and Files	- 0	×
Crypto Hash Methods MD5 Hash SHA1 Hash SHA256 Hash SHA512 Hash CRC32 Hash xxHash64 Hash	graphics only) raphics only) quired for graph	iics)	

By using the files in the **Photoshop Express** folder, and running a **Match Visually Similar Graphics** (Differential Hash) the source file was identified as Screenshot_20231226-154230.png

Figure 53: File System > Hash Match > Match Visually Similar Graphics (Differential Hash)



From File System module > Tools > Add 3rd Party Tools, Beyond Compare was selected to compare the source file against the edit file.

Figure 54: 3rd Party Tools > Beyond Compare



Beyond Compare identifies the edits to be Good Job and Success.

Figure 55: Beyond Compare



Q21. IT'S THE EYE OF THE TIGER (25 POINTS)

When is Rocco's Bday? (YYYY-MM-DD)?

Q20. ANSWER

1974-09-29.

Q20. FORENSIC EXPLORER METHODOLOGY

This information is provided in the Facebook source file: *facebook-61554919820462-2024-01-06-49fzodcA.zip*, under the section *personal_information\profile_information\profile_information.html*.

Figure 56: facebook-61554919820462-2024-01-06-49fzodcA.zip

Name	Rocco Sachs
Profile	https://www.facebook.com/profile.php?id=61554919820462
Registration date	Saturday, December 16, 2023 at 11:29 AM UTC-05:00
Emails	roccotsachs@gmail.com
Birthday	Sep 29, 1974
Gender	Male
Blood donor settings	unregistered

Q22. STALKER ALERT (50 POINTS)

Shortly after logging into Facebook with IP address 73.38.231.98, a photo was taken. Where was this photo taken?

Q21. ANSWER

Devonshire Mall, 3100 Howard Ave, Windsor, Ontario, Canada.

Q21. FORENSIC EXPLORER METHODOLOGY

Searching for hits on the I.P. address **73.38.231.98** returned no results. A double-check of the CTF question confirmed the I.P. address provided:

Figure 57: Magnet CTF Question > Android > Stalker Alert

Challenge	45 Solves	×					
Stalker Alert							
	50						
Shortly after logging into Facebook with IP address 73.38.231.98, a photo was taken. Where was this photo taken?							
Flag		Submit					

A search of the source file *facebook-61554919820462-2024-01-06-49fzodcA.zip* identified that the actual I.P. address as **72.38.231.98**.

Figure 58: Facebook source file facebook-61554919820462-2024-01-06-49fzodcA.zip > IP address activity

IP address activity Your recent activity from specific IP addresses Generated by Rocco Sachs on Wednesday, January 3, 2024 at 4:09 PM UTC-05:00 Contains data from January 3, 2023 at 10:21 AM to January 3, 2024 at 4:09 PM				
Login				
IP 174.94.45.94 address				
Browser [FBAN/FB4A;FBAV/444.0.0.31.114;FBBV/546214382;FBDM/{density=2.5,width=1080,height=2040};FBLC/en_US;FBRV/0;FBCR/;FBMF/G oogle;FBBD/google;FBPN/com.facebook.katana;FBDV/Pixel 3a XL;FBSV/12;FBOP/1;FBCA/arm64-v8a;]				
Dec 22, 2023 11:19:58am				
Login				
IP 72.38.231.98				
Browser Mozilla/5.0 (Linux; Android 12; Pixel 3a XL Build/SP2A.220305.012; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/120.0.6099.43 Mobile Safari/537.36				
Dec 27, 2023 11:16:01am				

Once the date of Dec 27, 2023 11:16:01am was determined, a sort of graphics files in the File System module by **Modified date** identified the picture **PXL_20231227_163049844.jpg**.

Figure 59: File System (sorted by Modified) > PXL_20231227_163049844.jpg

III File List	😨 Gallery View 😨 Video View 🔒 Disk	View 🌖 Category Graph						
🖗 🖻 🔯	€2 Filename	Exif 305: Software	Exif 36867: DateTime(3 27-Dec-2023	GPS Long	AZ Extensio	AZ* gra	GPS Lat. (
	Filename	Exif 305: Software	Exif 36867: DateTimeOriginal	Modified 🔺	GPS Long. (calc)	Extension Mis	File Cate	GPS Lat. (calc)
	NvFSK46JCd9t7sa53H7BbF-YY.cnt			27-Dec-2023 11:17:02 AM		Yes	Graphics	
- 2	NixsIs98kv0_EMAkSN4ihvc2W3E.cnt			27-Dec-2023 11:17:02 AM		Yes	Graphics	
- 3	NVFSK46JCd9t7sa53H7BbF-YY.cnt			27-Dec-2023 11:17:02 AM		Yes	Gra phics	
- 4	NixsIs98kv0_EMAkSN4ihvc2W3E.cnt			27-Dec-2023 11:17:02 AM		Yes	Graphics	
- 5	5rfVZhCh41cRILdamaJUBYwbnqw.cnt			27-Dec-2023 11:24:35 AM		Yes	Graphics	
- 6	🐋 RL5zBBvcXOYPufP3Ppj-KBV-UYc.cnt			27-Dec-2023 11:24:35 AM		Yes	Graphics	
- 7	5rfVZhCh41cRILdamaJUBYwbngw.cnt			27-Dec-2023 11:24:35 AM		Yes	Graphics	
8	射 RL5zBBvcXOYPufP3Ppj-KBV-UYc.cnt			27-Dec-2023 11:24:35 AM		Yes	Graphics	
9	0586a383f90cf405da2df89acc57f515			27-Dec-2023 11:24:37 AM		Yes	Graphics	
- 10	6ae54aa6e86219e0a9a2f717432a4e			27-Dec-2023 11:24:37 AM		Yes	Graphics	
- 11	10586a383f90cf405da2df89acc57f515			27-Dec-2023 11:24:37 AM		Yes	Graphics	
12	6ae54aa6e86219e0a9a2f717432a4e			27-Dec-2023 11:24:37 AM		Yes	Graphics	
13	PXL_20231227_163049844.jpg	HDR + 1.0.450594208zd	2023:12:27 11:30:49	27-Dec-2023 11:30:56 AM	-83.0026	No	Graphics	42.2746
- 14	PXL_20231227_163055783.jpg	HDR+ 1.0.450594208zd	2023:12:27 11:30:55	27-Dec-2023 11:31:01 AM	-83.0019	No	Graphics	42.2748
- 15	n 78986223c15174e9a6ad9399412293			27-Dec-2023 11:31:01 AM		Yes	Graphics	
16	18986223c15174e9a6ad9399412293			27-Dec-2023 11:31:01 AM		Yes	Graphics	
- 17	15121d0e769c1731db14352b8cc8c79			27-Dec-2023 4:32:04 PM			Graphics	
18	15121d0e769c1731db14352b8cc8c79			27-Dec-2023 4:32:04 PM			Graphics	
- 19	important system file dont delete 906	HDR + 1.0.450594208zd	2023:12:27 16:31:58	27-Dec-2023 4:32:11 PM		Yes	Graphics	
- 20	6acd503856ffed601e3aacbcc87c6b50			27-Dec-2023 4:32:14 PM		Yes	Graphics	
21	6acd503856ffed601e3aacbcc87c6b50			27-Dec-2023 4:32:14 PM		Yes	Graphics	
			21227 102040044					
Google Pi	xel 3a XL Logical Image - Data.tar\data\me	dia\0\DCIM\Camera\PXL_202	31227_163049844.jpg	101 Charles HUG 1 O MD DC 1 O M	101	DVI 20	21227 16204	0044 in a
2811 of 12030	a visible [LS 109.2 IVIB PS 109.9 IVIB]	T Highlighted [LS 2.0 IVIB	PS 2.0 IVIB]	191 Checked [LS 1.9 MB PS 1.9 M	IB]	PXL_20	231227_10304	as44'lbd

Using **Extract Metadata** information already populated in the metadata columns (or located in the Metadata Tab) for **GPS Lat. (calc)** and **GPS Long. (calc)**, the location was entered into Google Maps:

https://www.google.com/maps/place/42%C2%B016'28.6%22N+83%C2%B000'09.4%22W/@42.2745 476,-83.0028256,51m/data=!3m1!1e3!4m4!3m3!8m2!3d42.2746!4d-83.0026?entry=ttu



Figure 60: Google Maps, Latitude 42.2746, Longitude -83.0026