

Digital Forensics Analysis

Student Name: Md Ashraful Islam

Student ID:2436063

Introduction

Digital forensics (DF) refers to the collection, preservation, analysis and presentation of digital evidence from computing devices, networks, cloud services, and other digital storage — for use in legal, corporate, or security contexts.

Digital forensics has become essential for incident response, cyber-crime investigations, regulatory compliance, and corporate security.

Image Acquisitions

Image acquisition is a foundational step in digital forensic investigations, involving the creation of an exact, bit-for-bit duplicate of digital storage media. This process preserves all data — including active files, metadata, and deleted information — while ensuring the original evidence remains unaltered.

Cellebrite Physical Analyzer 7.1.0.42

File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks

Search Advanced

Samsung GSM_SM-A13... Welcome Tips & Tricks Extraction Summary (1)

All Content File System

Extraction Summary

+ Add extraction + Add external file Project settings Generate report Open Virtual Analyzer

Extractions: 1



File System
Samsung GSM SM-A137F Galaxy A13
File System [Android Backup]
Selective apps decoding
Extraction start date/time: 28/10/2025 11:57:02
Extraction end date/time: 28/10/2025 12:36:47
[View details](#)

Image Hashes
Extraction images are verified.

Insights from Installed Apps
Unknown (4 apps)
[View all](#)

Device Info

[Generate preliminary device report](#)

Chipset	MT6769V/CT	Taken from UFD extraction file
Android ID	f50a68f1f9da28	Taken from UFD extraction file
IMEI1	357898921470825	Taken from UFD extraction file
IMEI2	357712351470827	Taken from UFD extraction file
Model	SM-A137F	Taken from UFD extraction file
OS	14	Taken from UFD extraction file
Security Patch Level	2023-06-01	Taken from UFD extraction file
Vendor	samsung	Taken from UFD extraction file

Hash set Info

Malware scanner

Malware scan performed: No

Content

Selected applications

Microsoft Outlook	Snapchat	Google Meet
Signal Private Messenger	Gmail	LinkedIn: Jobs & Business Ne...
Messenger	Samsung Gallery	Google Chrome: Fast & Secure
Samsung Health	Google	S Suggest
com.android.providers.settings	com.android.providers.userdi...	com.android.settings
com.sec.imsservice	com.android.phone	com.google.android.gsf
com.samsung.android.fnm	Android Advertising ID	StoortDumpPasswords
Android IDs	Keystore Secrets	AndroidID
Device Info IMEI	LGBackup	Build Prop

9°C Cloudy 11:16 04/12/2025

Fig:image extractions and verifications

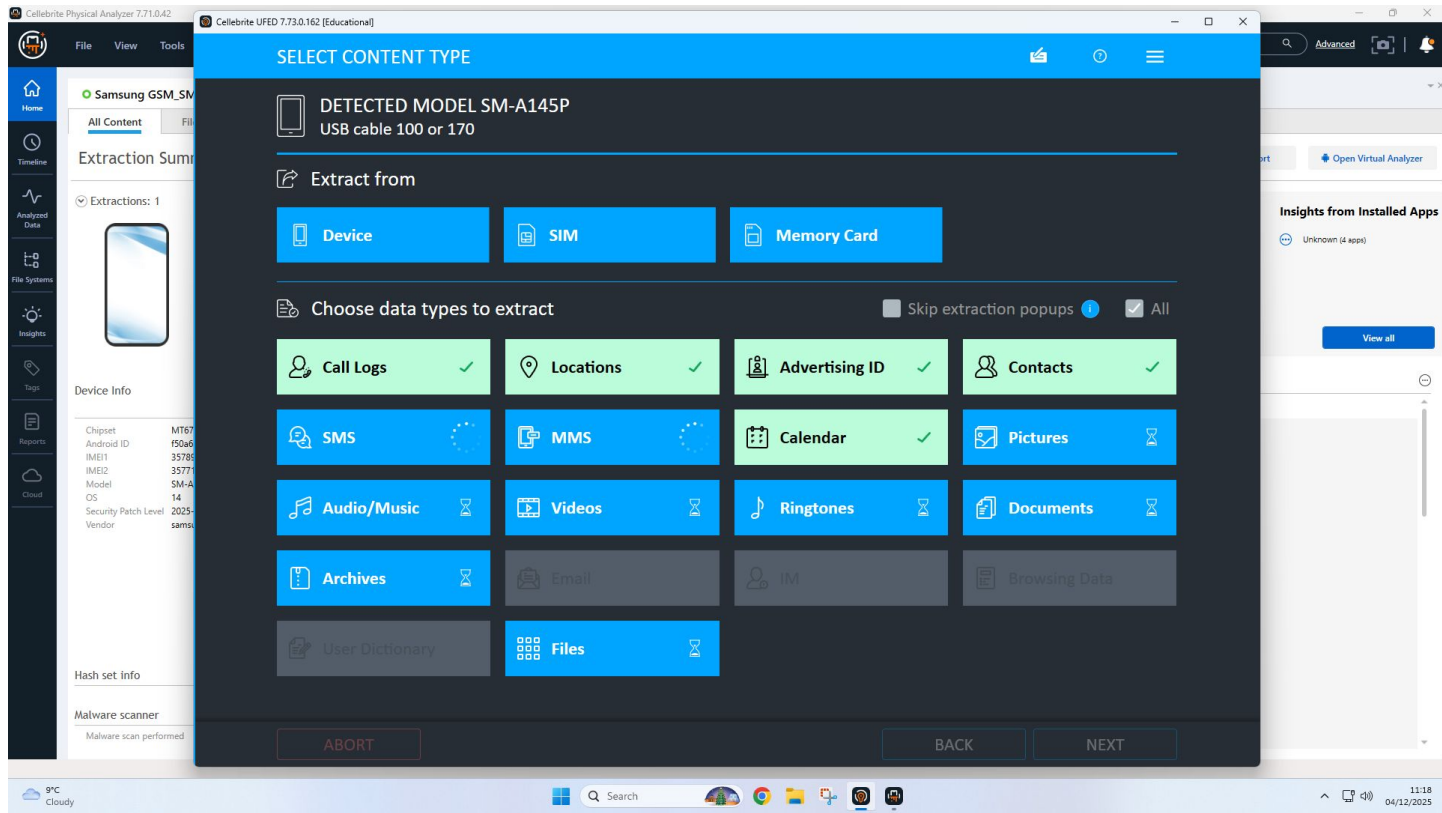
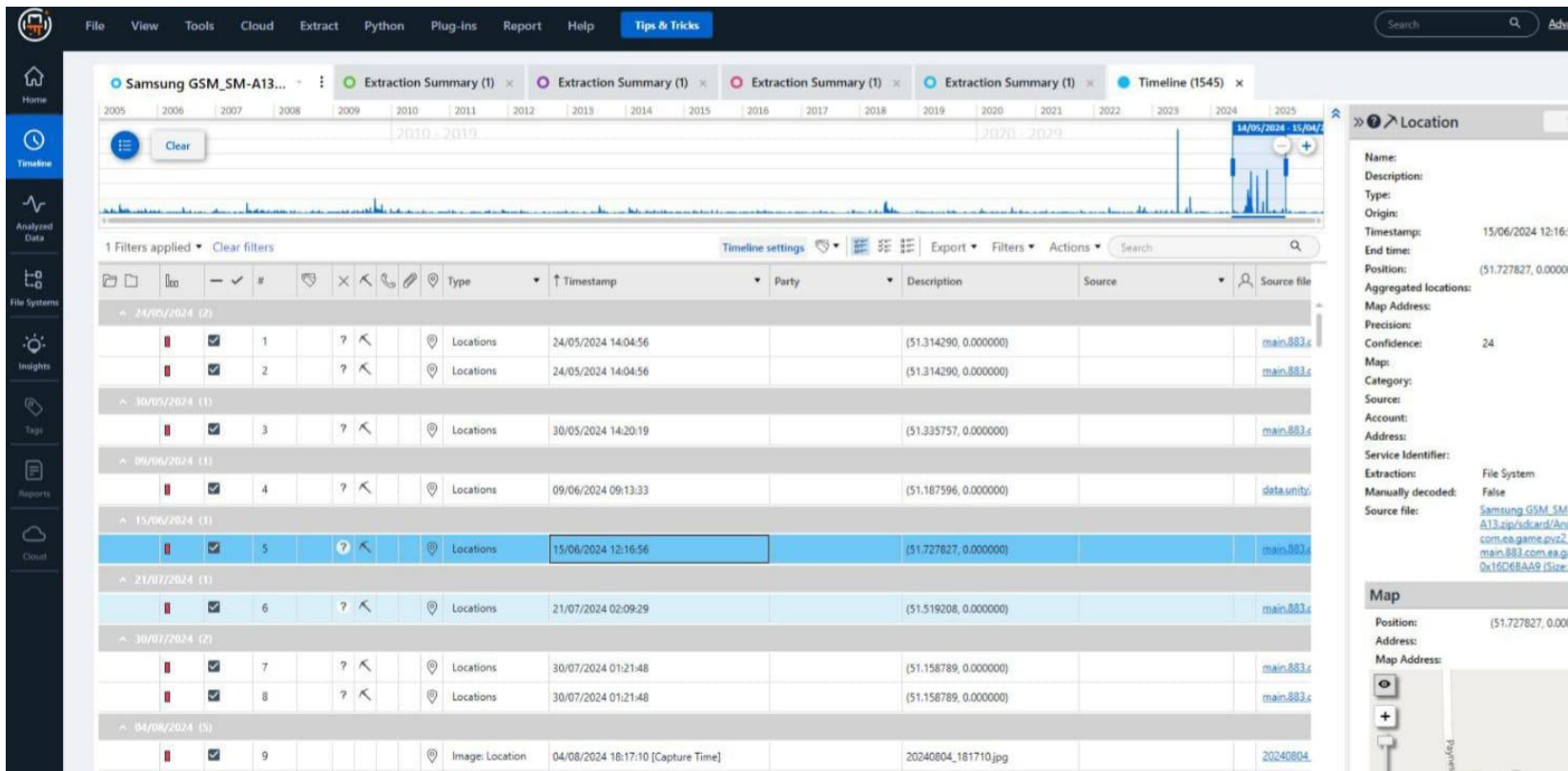
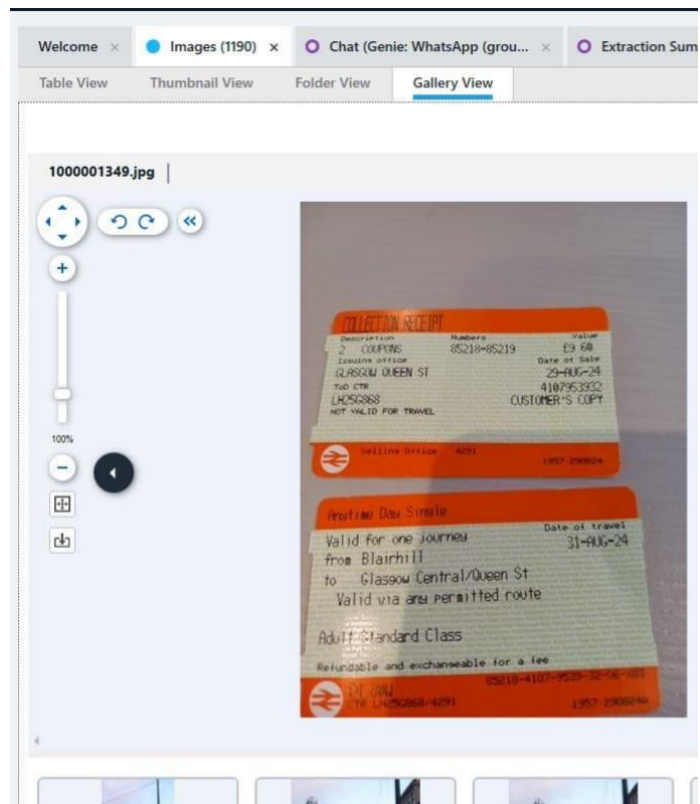


fig:UFED and Physical Analyzer,extraction and decoding process

FORENSIC INVESTIGATION

Quantum Tech recently reported a serious internal breach involving unauthorized access to a restricted patent: QT-AI-2025, a proprietary AI chip design. The company noticed abnormal access activity coming from inside the R&D network and immediately launched an internal investigation. The initial suspicion fell on Emma, a senior engineer who had recently joined the company. Internal logs indicated she accessed the patent files outside normal working hours. It was also believed she intended to sell the confidential design to NexGen Circuits, a long-time competitor. The proposed transfer appeared to involve a middleman — Joe — and possibly a third individual, Norman, believed to be connected to NexGen.





Cellebrite Physical Analyzer 7.71.0.42

File View Tools Cloud Extract Python Plug-ins Report Help **Tip & Tricks**

Home

Huawei_POT-LX1 P Smart

File Systems

- Memory Images
 - FileDump (Huawei_POT-LX1 P Smart)
- Memory Ranges
- File Systems
 - Google Photos dovp59@gmail.com
 - Huawei_POT-LX1 P Smart.zip (32192)

Timeline

Analyzed Data

File Systems

Insights

Tags

Reports

Cloud

FileDump (Huawei_POT-LX1 P Smart) x User Dictionary (176) x Genie: WhatsApp (grouped b... x Chat (Genie: Chats) (2) x Extraction Summary (1) x Extraction Summary (1) x

Hex View

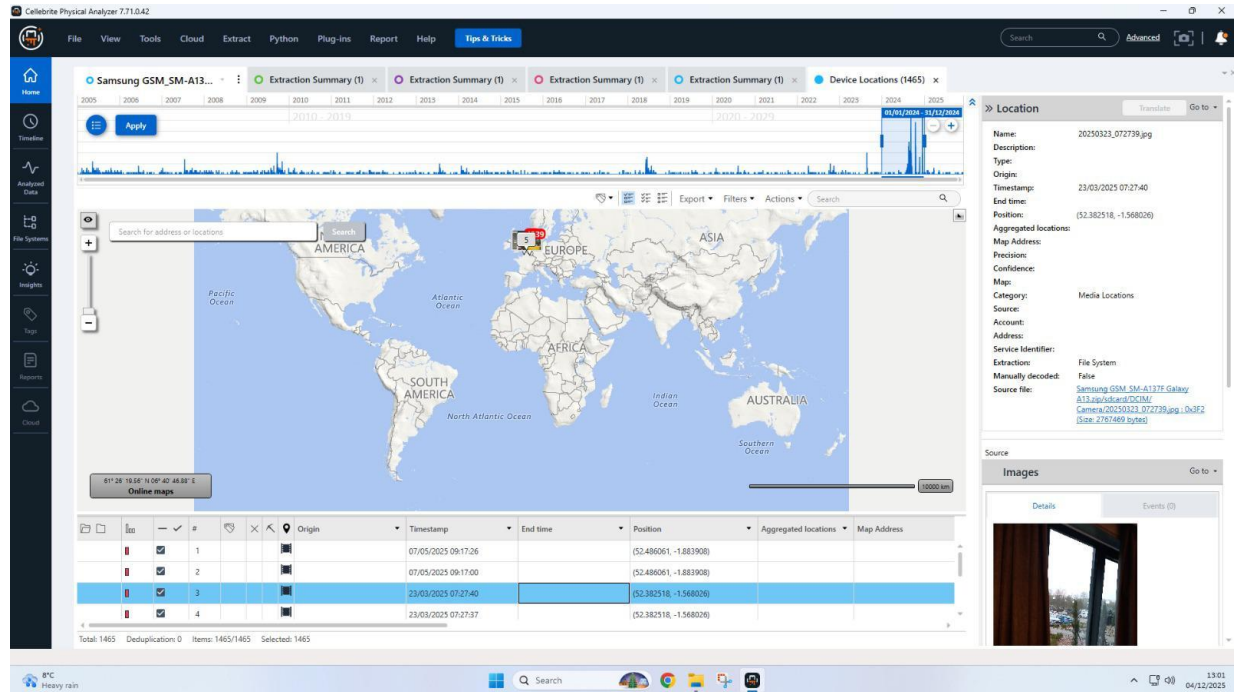
```
00000000 7F 45 4C 46 02 01 01 00 00 00 00 00 00 00 00 03 00 B7 00 01 00 00 00 00 C0 04 00 00 00 00 00 40 00 00 00 00
00000006 00 00 F8 7E 1A 00 00 00 00 00 00 00 00 00 40 00 38 00 09 00 00 00 1D 0B 00 06 00 00 00 00 00 40 00 00 00
0000000C 00 00 00 00 40 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00
00000012 00 00 00 00 00 01 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000018 8C B5 04 00 00 00 00 00 8C B5 04 00 00 00 00 10 00 00 00 00 00 00 01 00 00 00 01 00 00 00 C0 04 00 00 00
0000001E 00 00 00 C0 04 00 00 00 00 00 00 C0 04 00 00 00 00 80 79 13 00 00 00 00 00 80 79 13 00 00 00 00 00 10 00 00
00000024 00 00 00 01 00 00 00 00 06 00 00 00 00 40 18 00 00 00 00 00 00 40 18 00 00 00 00 40 18 00 00 00 40 78
0000002A 01 00 00 00 00 60 00 01 00 00 00 00 00 10 00 00 00 00 00 00 02 00 00 00 06 00 00 00 A1 19 00 00 00 00 00
00000030 60 A1 19 00 00 00 00 60 A1 19 00 00 00 00 02 00 00 00 00 00 02 00 00 00 02 00 00 00 00 08 00 00 00 00 00
00000036 00 00 52 B5 74 64 04 00 00 00 50 18 00 00 00 00 50 18 00 00 00 00 50 18 00 00 00 50 18 00 00 40 68 01 00
0000003C 00 00 00 00 70 01 00 00 00 00 01 00 00 00 00 00 50 B5 74 64 04 00 00 90 6F 02 00 00 00 00 00 90 6F
00000042 02 00 00 00 00 90 6F 02 00 00 00 00 44 68 00 00 00 00 00 00 44 68 00 00 00 00 00 00 04 00 00 00 00 00 00
00000048 51 B5 74 64 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000004E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 38 02 00 00 00 00 00 38 02 00 00
00000054 00 00 04 00 38 02 00 00 00 00 00 38 00 00 00 00 00 38 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00
0000005A 00 00 00 00 00 01 00 00 00 00 41 6E 64 72 6F 69 64 00 1D 00 00 00 00 00 00 10 00 00 00 03 00 00 47 4E 55 00
00000060 39 49 9E 99 C0 94 37 A7 25 D8 11 35 B9 CD 69 7E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000066 00 00 3B 00 00 12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 51 00 00 12 00 00 00 00 00 00 00 00
0000006C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000072 00 00 12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 72 00 00 12 00 00 00 00 00 00 00 00
00000078 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000007E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000084 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000008A 00 00 00 00 B4 00 00 12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 C4 00 00 12 00 00 00 00 00 00
```

Search [10479 results]

#	Offset	Length	Value	Source	More	Additional before	Additional after
1	0x0957A4	0x4	eMma	/apex/com.android.media.swcodec/lib64/libclang_rt...			
2	0x0987AF	0x4	eMma	/apex/com.android.media.swcodec/lib64/libclang_rt...			
3	0xA799A6	0x4	eMma	/apex/com.android.media.swcodec/lib64/libclang_rt...			
4	0xA799D8	0x4	eMma	/apex/com.android.media.swcodec/lib64/libclang_rt...			
5	0xA79A91	0x4	eMma	/apex/com.android.media.swcodec/lib64/libclang_rt...			
6	0xA79AC3	0x4	eMma	/apex/com.android.media.swcodec/lib64/libclang_rt...			
7	0xA79B37	0x4	eMma	/apex/com.android.media.swcodec/lib64/libclang_rt...			
8	0xA79B69	0x4	eMma	/apex/com.android.media.swcodec/lib64/libclang_rt...			
9	0x1F79C4D	0x4	eMma	/apex/com.android.media.swcodec@292103016/lib6...			
10	0x1F7CC58	0x4	eMma	/apex/com.android.media.swcodec@292103016/lib6...			
11	0x205DE4F	0x4	eMma	/apex/com.android.media.swcodec@292103016/lib6...			
12	0x205DE81	0x4	eMma	/apex/com.android.media.swcodec@292103016/lib6...			
13	0x205DEFA	0x4	eMma	/apex/com.android.media.swcodec@292103016/lib6...			

Values Tags Highlights **Search [10479 results]**

Length: 0x3BF5BA6CA | Offset: 0x0 | Selection: 0x0



Cellbrite Physical Analyzer 7.71.0.42
File View Tools Cloud Extract Python Plug-Ins Report Help **Tips & Tricks**
Search Advanced

Home

Timeline

Analyzed Data

File Systems

Insights

Tags

Reports

Cloud

Huawei_POT-LX1 P Smart

File Systems

- Memory Images
 - FileDump (Huawei_POT-LX1 P Smart...
- Memory Ranges
- File Systems
 - Google Photos d0vp59@gmail.com
 - Huawei_POT-LX1 P Smart.zip (32192...

FileDump (Huawei_POT-LX1 P...

User Dictionary (176)

Genie: WhatsApp (grouped b...

Chat (Genie: Chats) (2)

Extraction Summary (1)

Extraction Summary (1)

Hex View

```

00000000 7F 45 4C 46 02 01 01 00 00 00 00 00 00 00 00 00 00 00 00 03 00 B7 00 01 00 00 00 00 C0 04 00 00 00 00 00 40 00 00 00 00
00000026 00 00 F8 7E 1A 00 00 00 00 00 00 00 00 00 00 40 00 38 00 09 00 40 00 1D 00 1B 00 06 00 00 00 04 00 00 40 00 00 00
0000004C 00 00 00 00 40 00 00 00 00 00 00 00 00 00 40 00 00 00 00 F8 01 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00
00000072 00 00 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000098 FC B5 04 00 00 00 00 00 FC B5 04 00 00 00 00 10 00 00 00 00 00 01 00 00 00 01 00 00 00 C0 04 00 00 00 00
000000BE 00 00 C0 04 00 00 00 00 C0 04 00 00 00 00 00 80 79 13 00 00 00 00 00 80 79 13 00 00 00 00 00 00 00 00 00 00
000000E4 00 00 00 01 00 00 00 06 00 00 00 00 00 40 18 00 00 00 00 00 40 18 00 00 00 00 00 00 40 18 00 00 00 00 40 78
0000010A 01 00 00 00 00 60 C5 01 00 00 00 00 00 00 10 00 00 00 00 00 02 00 00 00 06 00 00 60 A1 19 00 00 00 00 00 00
00000130 60 A1 19 00 00 00 60 A1 19 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000156 00 00 52 85 74 64 00 00 00 00 00 50 18 00 00 00 00 00 50 18 00 00 00 00 50 18 00 00 00 50 18 00 00 00 68 01
0000017C 00 00 00 00 70 01 00 00 00 00 01 00 00 00 00 00 50 85 74 64 04 00 00 00 50 85 74 64 04 00 00 00 50 85 74 64
000001A2 00 00 00 00 00 90 6F 02 00 00 00 00 00 44 6B 00 00 00 00 00 44 6B 00 00 00 00 00 00 04 00 00 00 00 00 00
000001C8 51 85 74 64 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001E2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000214 00 00 00 38 02 00 00 00 00 00 38 00 00 00 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000023A 00 00 04 00 00 01 00 00 00 41 6E 64 72 6F 69 64 00 1D 00 00 04 00 00 00 10 00 00 03 00 00 00 47 4E 55 00
00000260 39 49 8E 99 C0 94 37 A7 25 D8 11 35 89 CD 69 7E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000286 00 00 3D 00 00 12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000002AC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000002D2 00 00 12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000002F8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000031E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000344 00 00 00 00 84 00 00 00 12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

ELF.....e.....

.....8.....8.....

.....8.....8.....

.....y.....y.....

.....8.....8.....8.....

.....P.....P.....P.....

.....P.....P.....P.....

.....Dk.....Dk.....

.....Android.....GNU

9I.....7.....5.....

.....Q.....

.....f.....

.....

Search [10 results]

#	Offset	Length	Value	Source	More	Additional before	Additional after
1	0x20EDA380	0x8	password	/data/data/com.google.android.googlequicksearch...			
2	0x1E4ED1938	0x8	password	/data/app/com.huawei.appmarket-CGR33dm0zgoo...			
3	0x1E4ED8553	0x8	password	/data/app/com.huawei.appmarket-CGR33dm0zgoo...			
4	0x1E4ED845	0x8	password	/data/app/com.huawei.appmarket-CGR33dm0zgoo...			
5	0x1E4ED8F93	0x8	password	/data/app/com.huawei.appmarket-CGR33dm0zgoo...			
6	0x1E4ED8749	0x8	password	/data/app/com.huawei.appmarket-CGR33dm0zgoo...			
7	0x1E4ED8770	0x8	password	/data/app/com.huawei.appmarket-CGR33dm0zgoo...			
8	0x1E4ED879F	0x8	password	/data/app/com.huawei.appmarket-CGR33dm0zgoo...			
9	0x1E4ED8945	0x8	password	/data/app/com.huawei.appmarket-CGR33dm0zgoo...			
10	0x1E4ED8A66	0x8</					

File View Tools Cloud Extract Python Plug-Ins Report Help **Tips & Tricks** Search

Huawei_POT-LX1 P Smart

Search

Analyzed Data

- Application (109)
- Calls (15)
- Call Log (15)
- Contacts (13)
- Devices & Networks (23)
- Device Events (12)
- Wireless Networks (11)
- Location Related (419)
- Manual Data Collection (44)
- Genie: Chats (2) (276 messages)
- Genie: Contacts (37)
- Genie: Passwords (4)
- Genie: User Accounts (1)
- Media (14344)
- Audio (61)
- Images (14150) (156 known files)
- Videos (133)
- Messages (75) (1)
- Search & Web (1157)
- Autofill (1)
- Cookies (122)
- Searched Items (100)
- User Dictionary (176)
- Web Bookmarks (9)
- Web History (749)
- Social Media (72)

Genie: WhatsApp (grouped b... x Chat (Genie: Chats) (2) x Extraction Summary (1) x Extraction Summary (1) x Extraction Summary (1) x Extraction Summary (1) x

Conversation View Messages View

Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov De

2024

Participants (2)

- Top-up 0
- Unknown 447917162768

Conversation

Select/Deselect all 273 messages

Top-up
textdata: That's serious stuff Emma. Do you know how might be interested?
translatedtext: 0
21/08/2024 10:06:29(UTC+0)
Sources (3)

Top-up
textdata: Not exactly Joe, but I trust you can find the right buyer. The competition must be eager to get their hands on this tech..
translatedtext: 0
21/08/2024 10:30:36(UTC+0)
Sources (2)

Top-up
textdata: I will see what I can do..I am meeting few clients today at a Meeting Room in a Hotel. Will discuss about your offer..
translatedtext: 0
21/08/2024 11:13:16(UTC+0)
Sources (2)

Top-up
textdata: Perfect. Let's keep this under wraps. This could be huge for both of us..
translatedtext: 0
21/08/2024 11:13:16(UTC+0)
Sources (2)

Source:
Subject:
Timestamps:
Status:
Message Type:
SMSC:
Device description:
Folder:
Message Deleted F
Self Destruct Durat
Priority:
Service Identifier:
Extraction:
Manually decoded
Source file:

From
0 Top-up

To
44791716276

CC

BCC

Label

No event with timestamp to present

Export Filters Actions Search											
Participants											
Start Time Last Activity											
0 447917162788 Top-up 06/06/2023 09:22:31(UTC+0) 08/12/2024 19											

Total: 1 Deduplication: 0 Items: 1/1 Selected: 1

Translate

Go to

Select/Deselect a... Enter: text to filter ...

☒

Top-up

textdata: Olmo showing his skills 🤖
#LaLigaHighlights,
translatedtext: 0
28/08/2024 16:05:26(UTC+0)

Source (3)

☒

Top-up

textdata: 🎵 DREAM DEBUT
🔗 https://youtu.be/pgM5peJl_N0?
si=v8kd3KG19IRANTz0,
translatedtext: 0
28/08/2024 21:39:27(UTC+0)

Source (3)

☒

Top-up

textdata: These two 🏆❤️,
translatedtext: 0
29/08/2024 11:50:59(UTC+0)

Source (3)

☒

Top-up

textdata: Hi there, just nearing to
some wonderful offers. I am flying to
Glasgow to meet a contact over there
for a meeting. Will keep you posted,
translatedtext: 0
29/08/2024 14:10:34(UTC+0)

Source (3)

☒

Top-up

textdata: ★ Our opponents for the
Champions League! ★

What can i find :

Evidence Inventory and Chain of Custody

n No.	Device	Owner	Evidence Type	Acquisition Method	Hash Verification
001	Huawei POT-LX1 P Smart	Emma (Perpetrator)	Smartphone Text	Acquired using UFED	MD5 & SHA-256
002	Samsung Galaxy A13 (GSM_SM-A13F	Joe (Intermediary)	Smartphone Image	Acquired using UFED	MD5 & SHA-256
003	Norman's Android Device	Norman (Buyer)	Smartphone Image	Acquired using UFED	MD5 & SHA-256

Thank you