

Digital Forensic Investigation and Evidence Analysis

Keval Mahendra Motivaras

Student ID: 2515743

Module: Digital Forensics Analysis (ACCA7031)

*University of Wales Trinity Saint David (UWTSD)
London*

UWTSD

Objectives & Tool Used

- Extract data from multiple devices
- Verify integrity using hash values
- Analyse communication
- Identify suspicious activity

Tools:

- Cellebrite UFED
- Cellebrite Physical Analyzer
- MD5 / SHA-1 Hashing

Methodology

- 4 devices extracted individually
- Forensically sound acquisition
- Hash values generated (MD5/SHA-1)
- Integrity verified (no data alteration)

Acquisition

Hash Check

Extraction

Merge

Analysis

Extraction

The screenshot displays the Calibre Physical Analyzer 7.0.8.11 interface. The main window shows the 'Extraction Summary' for a device named 'Huawei_P20-LI2_P_Smart'. The interface is divided into several sections: 'Extraction Summary' at the top, 'Device Info' on the left, 'Content' in the center, and 'Insights from Installed Apps' on the right. The 'Extraction Summary' section shows a list of extracted files and their hashes. The 'Device Info' section provides details about the device, including its model, manufacturer, and hardware specifications. The 'Content' section lists various applications and files extracted from the device. The 'Insights from Installed Apps' section provides a summary of the installed applications and their associated data.

The screenshot displays the Calibre Physical Analyzer 7.0.8.11 interface. The main window shows the 'Extraction Summary' for a device named 'Detected Model_Nokia_C2'. The interface is divided into several sections: 'Extraction Summary' at the top, 'Device Info' on the left, 'Content' in the center, and 'Insights from Installed Apps' on the right. The 'Extraction Summary' section shows a list of extracted files and their hashes. The 'Device Info' section provides details about the device, including its model, manufacturer, and hardware specifications. The 'Content' section lists various applications and files extracted from the device. The 'Insights from Installed Apps' section provides a summary of the installed applications and their associated data.

The screenshot displays the Calibre Physical Analyzer 7.0.8.11 interface. The main window shows the 'Extraction Summary' for a device named 'Samsung GSM_SM-A12'. The interface is divided into several sections: 'Extraction Summary' at the top, 'Device Info' on the left, 'Content' in the center, and 'Insights from Installed Apps' on the right. The 'Extraction Summary' section shows a list of extracted files and their hashes. The 'Device Info' section provides details about the device, including its model, manufacturer, and hardware specifications. The 'Content' section lists various applications and files extracted from the device. The 'Insights from Installed Apps' section provides a summary of the installed applications and their associated data.

The screenshot displays the Calibre Physical Analyzer 7.0.8.11 interface. The main window shows the 'Extraction Summary' for a device named 'Detected Model_Note_14'. The interface is divided into several sections: 'Extraction Summary' at the top, 'Device Info' on the left, 'Content' in the center, and 'Insights from Installed Apps' on the right. The 'Extraction Summary' section shows a list of extracted files and their hashes. The 'Device Info' section provides details about the device, including its model, manufacturer, and hardware specifications. The 'Content' section lists various applications and files extracted from the device. The 'Insights from Installed Apps' section provides a summary of the installed applications and their associated data.

Device extraction & hash verification

Chats

The screenshot displays the Cellebrite Physical Analyzer 7.73.0.11 interface. The left sidebar shows the 'Analyzed Data' section with various categories like Application (179), Calls (15), Contacts (13), and Messages (75). The main window shows a table of chat events. The right-hand pane displays a detailed view of a chat conversation, showing messages and their metadata.

Table of Chat Events:

Participants	Start Time	Last Activity	ID
Top-up 447917162788	06/06/2023 09:22:31(UTC+0)	31/01/2025 11:28:14(UTC+0)	

Chat Conversation Details:

- Message 1:** textdata: Hi Joe, Any update on the offers? It is disappointing that no response from u. I have managed to find someone with whom I am meeting over the next weeks. translatedtext: 0
20/11/2024 10:01:24(UTC+0)
- Message 2:** textdata: I may go with someone if u r not interested, translatedtext: 0
20/11/2024 10:01:44(UTC+0)
- Message 3:** textdata: Apologies Emma, I am in a final talks about it. Meeting the client this week at Manchester. Will update, translatedtext: 0
20/11/2024 10:03:04(UTC+0)
- Message 4:** textdata: **Premi Barclia Jugadors 2024**
Aitana Bonmati and Lamine Yamal have got their trophies. translatedtext: 0
20/11/2024 17:15:07(UTC+0)

Merged data analysis

Suspicious Messages

Messages indicating coordination:

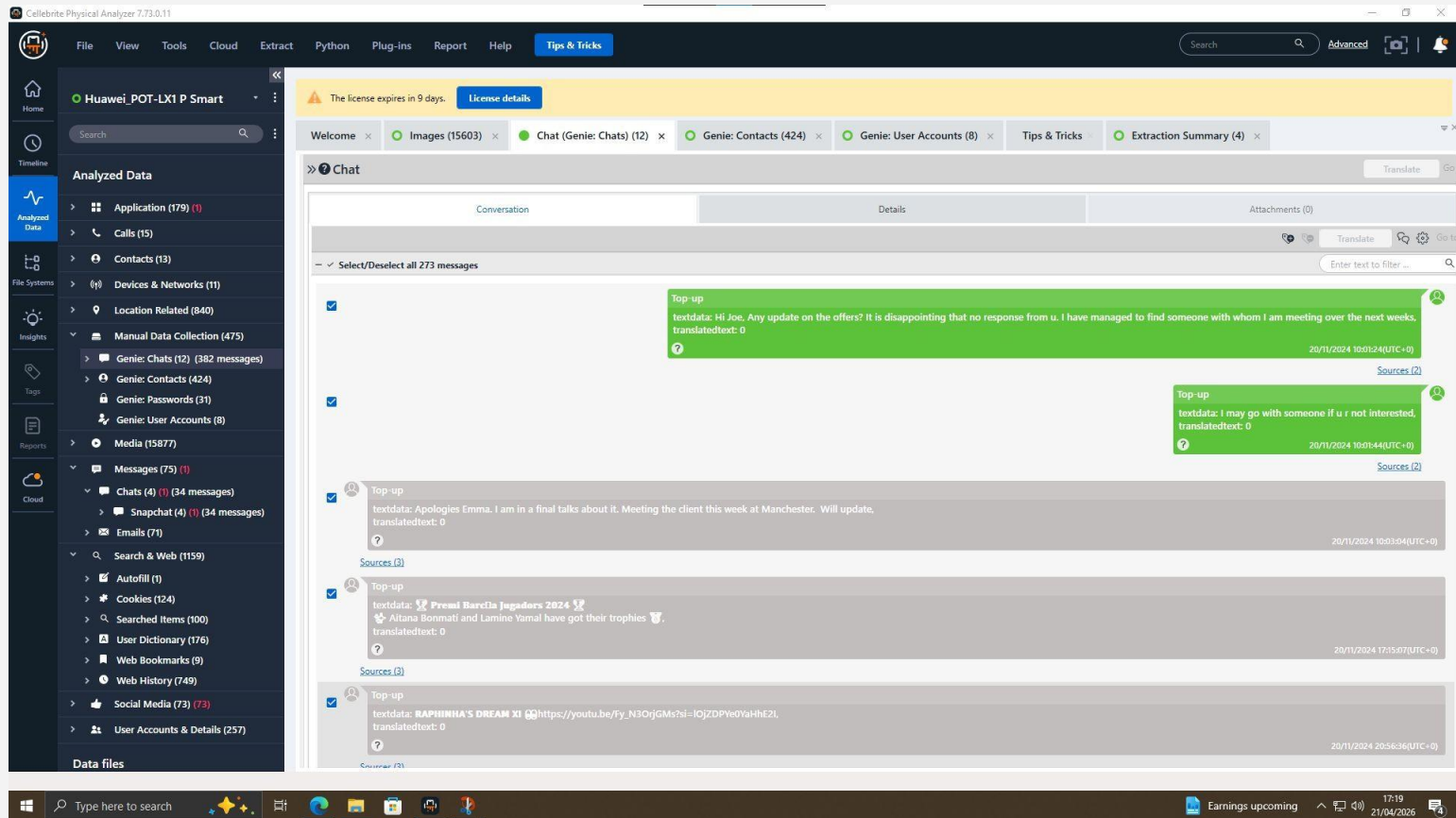
- “5M secured”
- “Local part stays as planned”
- “Keep me posted”

The screenshot displays the Cellebrite Physical Analyzer 7.73.0.11 interface. The left sidebar shows the 'Analyzed Data' tree with categories like 'Snapchat (3)', 'Devices & Networks (11)', 'Location Related (840)', 'Manual Data Collection (112)', 'Genie: Chats (11) (374 messages)', 'Genie: Contacts (71)', 'Genie: Passwords (24)', 'Genie: User Accounts (6)', 'Media (15077)', 'Messages (75) (1)', 'Chats (4) (1) (34 messages)', 'Snapchat (4) (1) (34 messages)', 'Emails (71)', 'Search & Web (1159)', 'Autofill (1)', 'Cookies (124)', 'Searched Items (100)', 'User Dictionary (176)', and 'Web Bookmarks (9)'. The main window shows a 'Timeline (2125)' view with a table of events. The table has columns for 'Participants', 'Start Time', and 'Last Activity'. A single event is visible, dated 06/06/2023 09:22:31(UTC+0), with participants 'Top-up' and '447917162768'. The right sidebar shows a 'Select/Deselect all 273 messages' view with a list of messages. The messages are grouped by source and include timestamps and translated text. The messages are:

- Top-up: textdata: He's good with it. 5M secured. Waiting for confirmation. The rest, translatedtext: 0. 31/01/2025 10:23:18(UTC+0). Sources (3).
- Top-up: textdata: Local part stays as planned. He's taking his sweet time. Not liking this., translatedtext: 0. 31/01/2025 10:23:19(UTC+0). Sources (2).
- Top-up: textdata: It's all about patience. We can push harder., translatedtext: 0. 31/01/2025 10:23:56(UTC+0). Sources (3).
- Top-up: textdata: OK. Keep me posted. I have others waiting., translatedtext: 0. 31/01/2025 10:24:11(UTC+0). Sources (2).
- Top-up: textdata: We'll be watching..., translatedtext: 0. 31/01/2025 11:28:14(UTC+0). Sources (3).

Chat communication

Suspicious Messages



Suspicious coordination messages

Duplicate Contact

The screenshot displays the XosRoject Hybrid Analyzer interface, which is used for analyzing mobile device data. The interface is split into two panes, each showing a list of contacts and a detailed view of a specific contact.

Left Pane:

- Contacts List:** A table with columns for Name, Device description, Source, Account, Group, Contact, and Modified. It shows a list of contacts, with the contact 'Pete Oliver' highlighted in blue.
- Contact Details:** A detailed view of the contact 'Pete Oliver'. It includes fields for Name, Device description, Source, Account, Group, Contact, and Modified. The contact is identified as 'Pete Oliver' with a device description of 'Generic Facebook'.

Right Pane:

- Contacts List:** A table with columns for Name, Device description, Source, Account, Group, Contact, and Modified. It shows a list of contacts, with the contact 'Pete Oliver' highlighted in blue.
- Contact Details:** A detailed view of the contact 'Pete Oliver'. It includes fields for Name, Device description, Source, Account, Group, Contact, and Modified. The contact is identified as 'Pete Oliver' with a device description of 'Generic Facebook'.

The interface also includes a sidebar on the left with various analysis tools and a top menu bar with options like File, View, Tools, Cloud, Extract, Python, Plug Ins, Report, and Help. The bottom status bar shows the total number of contacts (424) and the number of selected contacts (424).

Location Evidence

- Reference to meeting location
- Identified in Manchester
- Links digital communication to real-world activity
- Supports timeline reconstruction

The screenshot displays the Cellebrite Physical Analyzer 7.73.0.11 interface. The left sidebar shows the 'File Systems' section with a list of files. The main window features a map of Manchester, England, with a search bar and a list of extracted location data. The map shows various locations including Bolton, Rochdale, Huddersfield, and Manchester. The list below the map contains columns for Source, Account, Source file information, Service Identifier, and Extraction.

Source	Account	Source file information	Service Identifier	Extraction
ibly Captured	Google Photos	gphotos0.db; 0x19E728		File System (4
ions		IMG_20241122_190504.jpg; 0x232A		File System (4
ibly Captured	Google Photos	gphotos0.db; 0x19E610		File System (4
ions		IMG_20241122_190455.jpg; 0x233A		File System (4
ibly Captured	Google Photos	gphotos0.db; 0x19E768		File System (4
ibly Captured	Google Photos	gphotos0.db; 0x19E713		File System (4
ibly Captured	Google Photos	gphotos0.db; 0x19E886		File System (4

Path: Samsung GSM_SM-A137F Galaxy A13 zip(sicard)/DCIM/Camera/20241122_112158.jpg Size: 2 MB Date modified: 22/11/2024 11:21:58(UTC+0)

Findings & Conclusion

- Evidence integrity successfully verified
- Coordinated communication identified
- Duplicate contacts detected (identity obfuscation)
- Real-world meeting planned
- Cross-device linkage established

Conclusion:

- Successful forensic investigation conducted
- Multi-device analysis provided deeper insights
- Digital evidence supports coordinated behaviour
- Demonstrates importance of forensic tools in cybersecurity

Findings

Suspect roles:

Emma

Data Source

Joe

Intermediary

Norman

Buyer

Timeline

Timeline:

- August 2024 ->Initial chat
- November 2024 -> meeting and deal
- January 2025 -> payment confirmation

Practical Demonstration

Cellebrite Physical Analyzer 7.73.0.11

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

Home Timeline Analyzed Data File Systems Insights Tags Reports Cloud

The license expires in 9 days. [License details](#)

EvidenceCollection Welcome Videos (40) Phone (116) Calendar (126) Tips & Tricks Extraction Summary (2) Images (2067) Contacts (142) Installed Applications (4)

All Content Advanced Logical File System

Extraction Summary

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

Extractions: 2



Advanced Logical
Detected Model SM-M325F
Advanced Logical
Extraction start date/time
14/04/2026 16:49:46 +01:00
Extraction end date/time
14/04/2026 16:53:13 +01:00
[View details](#)



Image Hashes
Extraction images are verified.
[View details](#)



File System
Detected Model SM-M325F
File System [Android Backup]
Extraction start date/time
14/04/2026 16:41:05(UTC+1)
Extraction end date/time
14/04/2026 16:48:50(UTC+1)
[View details](#)



Image Hashes
Extraction images are verified.
[View details](#)

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

Device Info

[Generate preliminary device report](#)

File System	Chipset	MT6769V/CT	Taken from UFD extraction file
Android ID	4699b009b1a49bba	Taken from UFD extraction file	
IMEI1	357674432063494	Taken from UFD extraction file	
IMEI2	357915402063497	Taken from UFD extraction file	
Model	SM-M325F	Taken from UFD extraction file	
OS	13	Taken from UFD extraction file	
Security Patch Level	2025-05-01	Taken from UFD extraction file	
Vendor	samsung	Taken from UFD extraction file	

Advanced Logical	Chipset	MT6769V/CT	Taken from UFD extraction file
Client Used for Extraction	Yes	Taken from XML extraction file	
Advertising ID	6f495d44-a0b6-4fd6-91ae-95129473e7f3	Taken from XML extraction file	
Android ID	4699b009b1a49bba	Taken from XML extraction file	
Detected manufacturer	samsung	Taken from XML extraction file	
Detected model	SM-M325F	Taken from XML extraction file	
Phone date/time	14/04/2026 16:50:16 +01:00	Taken from XML extraction file	
Phone revision	13 TP1A.220634.014 M325FXSDDYE3	Taken from XML extraction file	
IMEI	357674432063494	Taken from XML extraction file	
Model	SM-M325F	Taken from UFD extraction file	
MSISDN	+919001500120	Taken from XML extraction file	

Content

Data

Calendar	126	Call Log	293	Contacts	142
Installed Applications	4	Instant Messages	359		

Data Files

Applications	4	Archives	8	Audio	36
Configurations	1	Databases	2	Documents	33
Images	2067	Text	108	Uncategorized	553
Videos	40				

Windows taskbar: Type here to search, 12°C Sunny, 18:10, 21/04/2026