

Academic Research Project

Digital Forensic Investigation and Evidence Analysis

Submitted by: Rishabh Choudhary

Student ID: 2434332

Module: Digital Forensics Analysis (ACCA7031)

University: UWTSD London

Incident Overview & Objectives

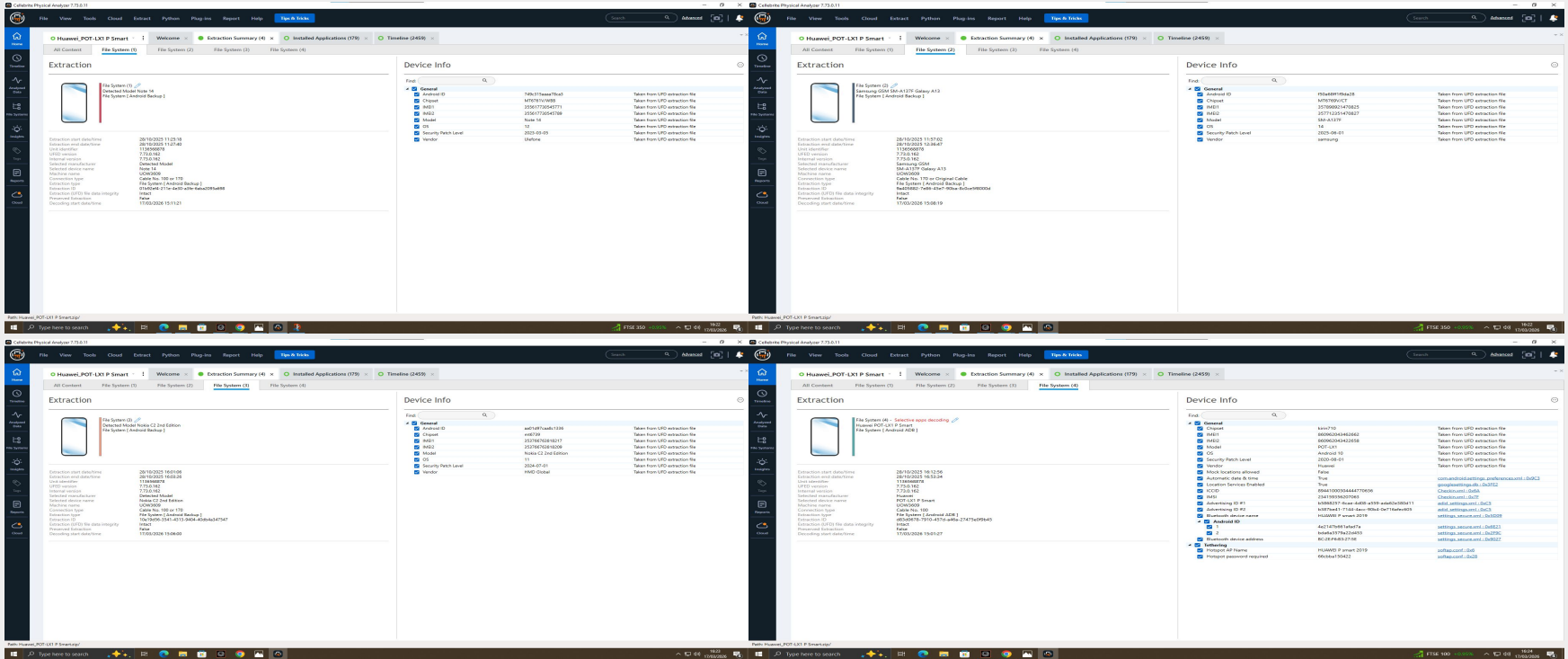
- Unauthorized access detected
- Patent QT-AI-2025 targeted
- Emma identified as suspect

Objectives:

- Identify communication
- Detect data transfer
- Reconstruct events
- Identify roles

Extractions

- Four devices forensically extracted
- Data integrity verified using hash values
- Analysis conducted using Cellebrite UFED



Evidence Acquisition

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

Huawei_POT-LX1 P Smart Welcome Extraction Summary (4)

All Content File System (1) File System (2) File System (3) File System (4)

Extraction Summary

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

Extractions: 4



File System (1)
Detected Model Note 14
File System [Android Backup]
Extraction start date/time: 28/10/2025 11:25:18
Extraction end date/time: 28/10/2025 11:27:40

Image Hashes
Extraction images are verified.

[View details](#)



File System (2)
Samsung GSM SM-A137F Galaxy A13
File System [Android Backup]
Extraction start date/time: 28/10/2025 11:57:02
Extraction end date/time: 28/10/2025 12:36:47

Image Hashes
Extraction images are verified.

[View details](#)

Insights from Installed Apps

- Chat applications (6 apps)
- Secure wipe (1 apps)
- Browser (1 apps)
- Developer tools (14 apps)
- Social networking (10 apps)
- Lifestyle (7 apps)
- Utilities (7 apps)
- Entertainment (1 apps)

[View all](#)

Device Info

[Generate preliminary device report](#)

File System (1)	File System (3)	File System (4)
Chipset MT6761V/WB8	Chipset mt6739	Advertising ID #1 b5868257-6cae-4d08-a559-ada62e380d11
Android ID 749c315aaaa78ca3	Android ID aa01497caa8c1336	Advertising ID #2 b387be41-7144-4acc-90b4-0e716afec605
IMEI1 355617730545771	IMEI1 353766763818217	Chipset kirin710
IMEI2 355617730545789	IMEI2 353766763818209	Android ID 4e2147b661afad7a
Model Note 14	Model Nokia C2 2nd Edition	
OS 12	OS 11	
Security Patch Level 2023-03-05	Security Patch Level 2024-07-01	
Vendor Ulfone	Vendor HMD Global	

Content

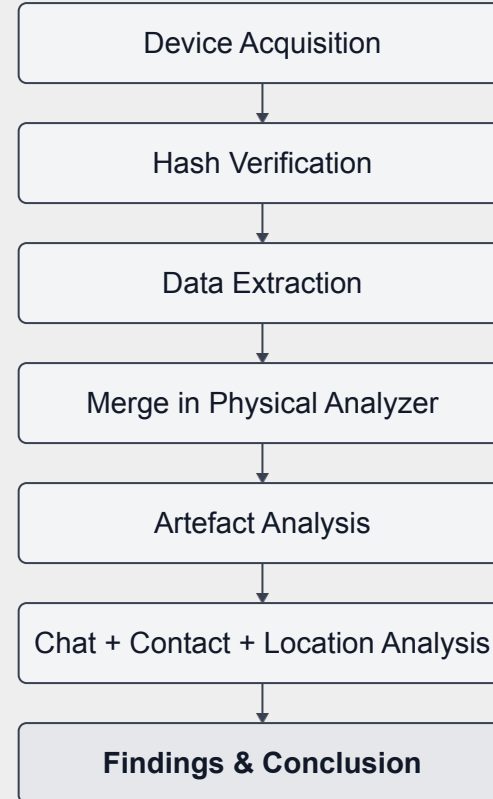
24 data sources can be extracted using UFED Cloud

Selected applications

Snapchat	Google Meet	Gmail
Google Chrome: Fast & Secure	YouTube	Amazon Shopping
Booking.com: Hotels and more	Google Photos	Google
Google Docs	Google Drive	Google Play Store
com.android.providers.settings	com.android.providers.useri...	com.android.settings
com.android.phone	com.android.email	com.google.android.gsf
com.android.providers.conta...	Android Advertising ID	SbootDumpPasswords
Android IDs	AndroidID	Device Info IMEI
LGBackup	Build Prop	Secure Settings

Investigation Approach

- Evidence Acquisition
- Hash Verification
- Data Integration
- Artefact Analysis
- Timeline Reconstruction
- Findings



Suspicious Messages

Coordination Messages:

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

These phrases suggest planning and transactional behavior, serving as a strong indicator of organized activity.

The screenshot displays the Cellebrite Physical Analyzer 2.73.0.11 interface. The left sidebar shows the 'Analyzed Data' section with a tree view of extracted information. The main window is divided into a 'Welcome' tab and a 'Chat' tab. The 'Chat' tab shows a conversation between Norman Smith and Peter Dover. The messages are as follows:

Sender	Message	Timestamp
Norman Smith	Almost.We need the Blueprint in chunks Too risky in one go.	3/10/2025 12:49:52(UTC+0)
Peter Dover	That wasn't the deal. Everything at once or no deal	3/10/2025 12:49:57(UTC+0)
Peter Dover	I do. But once we start there is no backtracking	3/10/2025 12:51:43(UTC+0)
Peter Dover	fine. Watch ur inbox in 48 hrs. After that we are ghosts	3/10/2025 12:53:09(UTC+0)

The interface also shows a list of analyzed data on the left, including Application Data (179), Calls (15), Contacts (13), Devices & Networks (11), Location Related (840), Manual Data Collection (475), Genie: Chats (12) (382 messages), Genie: Contacts (424), Genie: Passwords (31), Genie: User Accounts (8), Media (15877), Messages (75) (1), Chats (4) (34 messages), Snapchat (4) (34 messages), Emails (71), Search & Web (1159), Social Media (73) (73), and User Accounts & Details (257). The bottom status bar shows the total number of items and deduplications.

Negotiation & Coordination

The screenshot displays the Caliber Physical Analyzer 7.0.0.11 interface, which is used for analyzing digital evidence. The interface is divided into several sections:

- Top Bar:** Contains the application name, version (7.0.0.11), and a license expiration notice: "The license expires in 9 days. [License details](#)".
- Left Sidebar:** A navigation pane with various categories and sub-items:
 - Analyzed Data:** Application (179), Calls (15), Contacts (13), Devices & Networks (11), Location Related (840), Manual Data Collection (475), Genie Chats (12) (382 messages), Genie Contacts (424), Genie Passwords (31), Genie User Accounts (8), Media (15877), Messages (73) (1), Chats (4) (1) (4 messages), Snapchat (4) (1) (4 messages), Emails (7), Search & Web (1159), Autofill (1), Cookies (124), Searched Items (100), User Dictionary (176), Web Bookmarks (9), Web History (149), Social Media (77) (1), User Accounts & Details (257).
 - Data Files:** A section for managing data files.
- Main Chat View:** Displays a chat conversation with a search bar and a list of messages. The messages are filtered by "Select/Deselect all 273 messages". The chat shows a conversation between "Top-up" and "hustidate". The messages are in a "Conversation" view, with a "Details" tab also available. The chat content includes:

Top-up
hustidate: Hi no. Any update on the offer? It is disappointing that no response from u. I have managed to find someone with whom I am meeting over the next weeks.
translated: 0
20/11/2024 10:05:40UTC+0

Top-up
hustidate: I may go with someone if u r not interested.
translated: 0
20/11/2024 10:05:40UTC+0

Top-up
hustidate: Apologies Emma, I am in a final talks about it. Meeting the client this week at Manchester. Will update.
translated: 0
20/11/2024 10:05:40UTC+0

Top-up
hustidate: [Prenel Barcia Jagueros 2024](#)
[Alana Bonmati](#) and [Lamine Yana](#) have got their trophies
translated: 0
20/11/2024 11:05:40UTC+0

Top-up
hustidate: [BAPUNIRA'S DREAM II](#) @https://youtu.be/Fy_N30yQmhcI-1QZDPWraHnKZL
translated: 0
20/11/2024 20:06:30UTC+0
- Participants Table:** A table showing the participants in the chat. The table has columns for "Participants", "Messages", "Calls", "Contacts", "Location", "Manual Data Collection", "Genie Chats", "Genie Contacts", "Genie Passwords", "Genie User Accounts", "Media", "Messages", "Chats", "Snapchat", "Emails", "Search & Web", "Autofill", "Cookies", "Searched Items", "User Dictionary", "Web Bookmarks", "Web History", "Social Media", and "User Accounts & Details". The table is filtered by "1 Filters applied" and "Export" options. The table data is as follows:

Participants	Messages	Calls	Contacts	Location	Manual Data Collection	Genie Chats	Genie Contacts	Genie Passwords	Genie User Accounts	Media	Messages	Chats	Snapchat	Emails	Search & Web	Autofill	Cookies	Searched Items	User Dictionary	Web Bookmarks	Web History	Social Media	User Accounts & Details
Peter Dover	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2
SMS Service	9	1	2	8	47	1	2	8	47	1	2	8	47	1	2	8	47	1	2	8	47	1	2
SMS Service	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2
com.huawei.health	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2
Peter Dover	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2
SMS Service	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2
SMS Service	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2
Peter Dover	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2
Top-up	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2

Intermediary Role

- Repeated contact patterns identified
- Communication managed through a central contact
- Suggests role of intermediary (Joe)

The image displays four screenshots of the Humint POT-LXP Smart interface, arranged in a 2x2 grid. Each screenshot shows a detailed view of a contact's data, including a timeline, interaction status, and various details.

Top Left Screenshot (Norman Smith): The contact is Norman Smith, a female, born 1980, with a last name of Smith. The timeline shows a series of interactions, including a message from a contact named 'Joe' (ID: 1764504030201384) on 2020-10-10. The interaction status table shows a single entry for 'Joe' (ID: 1764504030201384) on 2020-10-10.

Top Right Screenshot (Norman Smith): The contact is Norman Smith, a female, born 1980, with a last name of Smith. The timeline shows a series of interactions, including a message from a contact named 'Joe' (ID: 1764504030201384) on 2020-10-10. The interaction status table shows a single entry for 'Joe' (ID: 1764504030201384) on 2020-10-10.

Bottom Left Screenshot (Peter Dover): The contact is Peter Dover, a male, born 1980, with a last name of Dover. The timeline shows a series of interactions, including a message from a contact named 'Joe' (ID: 1764504030201384) on 2020-10-10. The interaction status table shows a single entry for 'Joe' (ID: 1764504030201384) on 2020-10-10.

Bottom Right Screenshot (Peter Dover): The contact is Peter Dover, a male, born 1980, with a last name of Dover. The timeline shows a series of interactions, including a message from a contact named 'Joe' (ID: 1764504030201384) on 2020-10-10. The interaction status table shows a single entry for 'Joe' (ID: 1764504030201384) on 2020-10-10.

Location Evidence

- GPS/location data extracted from device
- Movement aligns with meeting discussions
- Supports real-world coordination

The screenshot displays the Cellebrite Physical Analyzer 7.72.0.31 interface. The main window shows a map of Manchester and surrounding areas, with a timeline of location data points. The timeline is labeled '2020-2023' and shows a series of location points. A table below the map lists extracted location data with columns for Source, Account, Source file information, Service Identifier, and Extraction.

Source	Account	Source file information	Service Identifier	Extraction
ably Captured	Google Photos	gphotos0.db : 0x198738		File System (4)
ions		IMG_20241122_190504.jpg : 0x233A		File System (4)
ably Captured	Google Photos	gphotos0.db : 0x19E810		File System (4)
ions		IMG_20241122_190458.jpg : 0x233A		File System (4)
ably Captured	Google Photos	gphotos0.db : 0x19E750		File System (4)
ably Captured	Google Photos	gphotos0.db : 0x19E713		File System (4)
ably Captured	Google Photos	gphotos0.db : 0x19E866		File System (4)

Metadata for the selected image file (20241122_112158.jpg):

- Name: 20241122_112158.jpg
- Type: Images
- Size (Bytes): 2591232
- Path: Samsung GSM_SM_A1377 Galaxy A13.zip\sdcard\DCIM\Camera\20241122_112158.jpg
- Created: 22/11/2024 11:21:58(UTC+0)
- Modified:
- Changed:
- Deleted:
- Extraction: File System (2)
- MD5: 551689185ac3c776dab724bd854193
- Source file: 20241122_112158.jpg

Metadata for the selected image file (20241122_112158.jpg):

- Camera Make: samsung
- Camera Model: SM-A1377
- Capture Time: 22/11/2024 11:21:58
- Pixel resolution: 4096x3060
- Resolution: 72x72 (Units: Inch)
- Orientation: Rotate 90 CW
- Lat/Lon: 53.543655 / -2.627303

Map Address:

USB Device Activity

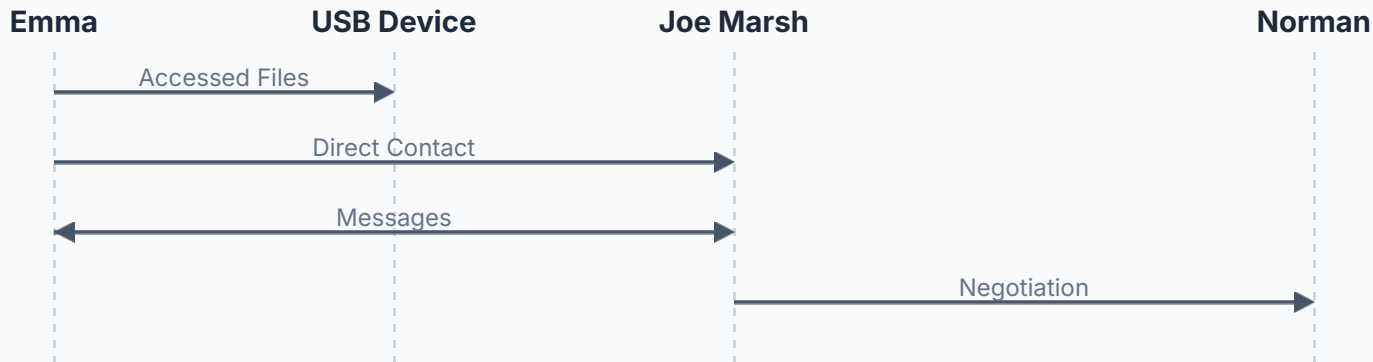
- USB flash device detected in system
- Indicates use of external storage
- Possible method for data transfer

The screenshot displays the Forensic Toolkit (FTK) interface, version 8.2.0.596. The main window is titled "System Summary" and shows a list of system components on the left and a detailed "Property Value" table on the right. The "Property Value" table lists various attributes of a USB device, including its Object ID, Name, Friendly Name, Device Serial/Instance ID, Last User Mount Time, User Name, Vendor, Vendor ID, Product, Product ID, Revision, Provenance, Data Provenance, Description, and Timestamp Time.

The "File List" pane at the bottom shows a list of files and folders, including "USB Devices" and "USB Mass Storage Device". The "Device - USB Devices" pane is active, displaying a table of USB devices with columns for Name, Label, Item #, Friendly Name, Device ID, First Connect Setup API, First Connect, Last Connect, Last Removal, and Last User Mount.

Name	Label	Item #	Friendly Name	Device ID	First Connect Setup API	First Connect	Last Connect	Last Removal	Last User Mount
CBM Flash Disk USB Device		61462	CBM Flash Disk USB Device	150037...					06/07/2008 08:19:27.76 (06/07/2008 07:19:27.76...)
Digital Still Camera.html		61464	Digital Still Camera	b54422...					
Generic USB Flash Drive...		61463	Generic USB Flash Drive...	78162...					
Generic USB Hub.html		61465	Generic USB Hub	581f8f...					
Generic USB Hub.html		61466	Generic USB Hub	6837e...					
USB Composite Device...		61468	USB Composite Device	6837e...					
USB Composite Device...		61467	USB Composite Device	581f8f...					
USB Human Interface D...		61469	USB Human Interface D...	6829cb...					
USB Human Interface D...		61470	USB Human Interface D...	78525c...					
USB Human Interface D...		61471	USB Human Interface D...	6829cb...					
USB Human Interface D...		61472	USB Human Interface D...	78525c...					
USB Mass Storage Devic...		61473	USB Mass Storage Device	68385...					

Evidence Correlation



Suspect Roles

Emma

Data Source

Joe

Intermediary

Norman

Buyer

Timeline of Activities & Conclusion

Date	Activity
August 2024	Initial communication established
November 2024	Active negotiation with multiple parties
January 2025	Financial confirmation and coordination

Conclusion:

Circumstantial evidence that strongly suggests a coordinated attempt to steal data through:

- communication,
- timeline,
- location, and
- USB operations

All of which imply the motive, intermediary, and possible buyer participation

The artefacts don't individually point to any data theft but the combination supports the idea of corporate espionage.

Practical Demonstration

- Personal device extraction performed
- Demonstrates real-world forensic capability
- Use of Cellebrite Physical Analyzer for analysis

The screenshot displays the 'Extraction Summary' window in Cellebrite Physical Analyzer. The interface shows a list of extractions with two main categories: 'File System' and 'Advanced Logical'. The 'File System' section lists various data types such as Calendar, Call Log, Contacts, Installed Applications, Instant Messages, Archives, Audio, Configurations, Databases, Documents, Images, Text, and Videos, each with a count. The 'Advanced Logical' section provides details about the extraction process, including the device model (SM-M22SF), the extraction date (14/04/2023), and the extraction time (16:41:05 UTC+1). The interface also includes a 'Device Info' section on the left, which provides details about the device, such as the model, manufacturer, and version.

The screenshot displays the 'Analyzed Data' window in Cellebrite Physical Analyzer. The interface shows a list of analyzed data items, including Applications, Calendar, Calls, Contacts, SIM, Manual Evidence, Image Carving Results, Media, Audio, Images, and Instant Messages. The 'Images' section is highlighted, showing a gallery view of extracted images. The gallery view displays a grid of images, with a selected image shown in a larger view on the right. The larger view shows a photo of a man in a white shirt. The interface also includes a 'Data Files' section on the left, which lists various data files such as Applications, Archives, Configurations, Databases, Documents, Images, Text, and Videos, each with a count. The 'Analyzed Data' section also includes a 'Data Files' list, which shows the files extracted from the device.

Recommendations & References

- Enforce restrictive access to data by employees using least privilege concept
- Limit usage of USB devices to avoid exfiltration of company data
- Continuous monitoring of communication activities of employees

References:

- N. Soni, “Digital Forensics: Confronting Modern Cyber Crimes,” 2025
- R. Shapland, “Digital Forensics Tools for Enterprises,” TechTarget, 2025
- Proofpoint, “Digital Forensics Process,” 2025

