



University of Wales
Trinity Saint David
LONDON

University of Wales Trinity Saint David, London

Digital Forensics Analysis

Course code: ACCA7031

Submitted by	: Shahriar Badhan
Submitted to	: Dr. Mohamed Ghanem
Student ID	: 2505521
Programme	: M.Sc in Cybersecurity and digital forensics
Submission Date	: 29 th April 2026

Table of Contents

Task 1 – Digital Forensics Research Report

1. Introduction

2. Current State of Digital Forensics and Tools

2.1 Leading Tools and Capabilities

3. Intersection of Digital Forensics and Cybersecurity

3.1 Incident Response Integration

3.2 Threat Intelligence and Malware Analysis

3.3 Insider Threat Detection

3.4 Legal and Compliance Requirements

4. Emerging Trends in Digital Forensics

4.1 Cloud Forensics

4.2 AI and Automation

4.3 IoT and Embedded Device Forensics

4.4 Blockchain and Cryptocurrency Forensics

4.5 Quantum-Resistant Forensics

5. Key Challenges in Digital Forensics

5.1 Encryption and Privacy Controls

5.2 Data Volume and Complexity

5.3 Legal and Jurisdictional Issues

5.4 Rapid Technology Evolution

5.5 Skills Shortage

6. National and International Job Market

6.1 United Kingdom Job Market

6.2 International Job Market

7. Conclusion

8. IEEE Reference List

Task 2 – Forensic Case Report: QT-AI-2025 Espionage Investigation

1. Abstract

2. Index Terms

3. Introduction

4. Case Background

5. Investigation Objectives

6. Methodology

6.1 Forensic Approach

6.2 Tools Used

6.3 Chain of Custody

7. Key Investigation Timeline

8. Device Identification and Extraction

8.1 Device Detection

8.2 Data Extraction

9. Data Integrity Verification

10. Communication Analysis

10.1 WhatsApp Analysis

10.2 Instagram Analysis

11.Call Log and Location Analysis

12.File System and Metadata Analysis

13.Findings and Discussion

14.Conclusion

15.References

Task-1

Digital Forensics Research Report

The Current and Emerging Landscape of Digital Forensics

1. Introduction

Digital forensics has become a critical discipline in modern security operations, supporting criminal investigations, cyber-incident response, fraud detection, and organisational risk management. As digital systems expand across cloud platforms, mobile devices, IoT ecosystems, and encrypted environments, forensic practitioners face increasing complexity. This report examines the current state of digital forensics, the capabilities of leading tools, its intersection with cybersecurity, emerging trends, key challenges, and the global job market. The analysis draws on recent academic literature, industry whitepapers, and employment data to provide a comprehensive overview of the field.

2. Current State of Digital Forensics and Tools

Digital forensics has evolved from traditional disk analysis to a multi-domain discipline covering mobile, cloud, network, memory, and IoT investigations. Modern tools are designed to handle diverse data sources, encrypted systems, and large-scale datasets.

2.1 Leading Tools and Capabilities

Cellebrite UFED and Physical Analyzer are widely used for mobile forensics, offering logical and physical extraction, encrypted app decoding, cloud acquisition, and advanced artefact parsing [1]. Their broad device support makes them essential for law enforcement and corporate investigations.

EnCase Forensic provides robust disk imaging, file system analysis, and chain-of-custody management. Its courtroom-ready reporting features make it a preferred tool in legal investigations [2].

Autopsy and The Sleuth Kit, open-source frameworks, offer timeline analysis, keyword search, hash filtering, and web artefact recovery. Their accessibility makes them popular in academic and training environments [3].

Volatility and Rekall dominate memory forensics, enabling investigators to analyse RAM for malware, processes, injected code, and network artefacts [4].

FTK (Forensic Toolkit) provides indexing-based search, email analysis, and data carving, making it suitable for large-scale corporate investigations [5].

Collectively, these tools demonstrate the maturity of the field, offering automation, advanced analytics, and support for cloud and mobile ecosystems.

3. Intersection of Digital Forensics and Cybersecurity

Digital forensics and cybersecurity are now deeply interconnected. Modern cyber incidents require both proactive defence and reactive investigation.

3.1 Incident Response Integration

Forensic techniques are essential for identifying attack vectors, determining the scope of compromise, and preserving evidence. According to the SANS Incident Response Survey, over 70% of organisations integrate forensic analysis into their incident response workflows [6].

3.2 Threat Intelligence and Malware Analysis

Forensic artefacts contribute to threat intelligence by revealing indicators of compromise (IOCs), attacker behaviour, and persistence mechanisms. Memory forensics tools such as Volatility are essential for analysing fileless malware and advanced persistent threats (APTs) [4].

3.3 Insider Threat Detection

Digital forensics supports insider-threat investigations by analysing user activity, file access patterns, and communication logs. Research shows that insider incidents often leave subtle digital traces requiring forensic correlation [7].

3.4 Legal and Compliance Requirements

Cybersecurity frameworks such as ISO 27001 and NIST 800-61 emphasise forensic readiness—ensuring systems are prepared to capture evidence during security incidents [8].

4. Emerging Trends in Digital Forensics

The field is undergoing rapid transformation due to technological advancements.

4.1 Cloud Forensics

With organisations migrating to AWS, Azure, and Google Cloud, cloud forensics has become essential. Investigators must analyse virtual machines, cloud storage, logs, and identity access management (IAM) events. Cloud providers now offer forensic-friendly logging tools such as AWS CloudTrail and Azure Monitor [9].

4.2 AI and Automation

Artificial intelligence is increasingly used to automate evidence classification, anomaly detection, and pattern recognition. Studies show that AI-driven triage can reduce investigation time by up to 40% [10].

4.3 IoT and Embedded Device Forensics

Smart home devices, wearables, and industrial IoT systems generate valuable evidence. However, proprietary hardware and inconsistent logging make IoT forensics challenging and highly specialised [11].

4.4 Blockchain and Cryptocurrency Forensics

With the rise of digital currencies, forensic analysts must trace blockchain transactions, identify wallets, and correlate on-chain and off-chain data. Tools like Chainalysis and TRM Labs support cryptocurrency investigations [12].

4.5 Quantum-Resistant Forensics

As quantum computing advances, researchers are exploring how quantum-safe encryption will impact forensic acquisition and decryption processes [13].

5. Key Challenges in Digital Forensics

Despite technological progress, the field faces several persistent challenges.

5.1 Encryption and Privacy Controls

Modern devices use strong encryption, secure enclaves, and privacy-focused operating systems. While essential for user security, these features limit forensic access. Apple's Secure Enclave and Android's File-Based Encryption are notable barriers [14].

5.2 Data Volume and Complexity

Investigations often involve terabytes of data across multiple devices and cloud platforms. Efficient triage and automation are essential to manage this scale [15].

5.3 Legal and Jurisdictional Issues

Cloud-stored evidence may reside in multiple countries, raising jurisdictional conflicts. GDPR and other privacy laws impose strict requirements on evidence handling [16].

5.4 Rapid Technology Evolution

New apps, devices, and operating systems emerge faster than forensic tools can adapt. This creates gaps in artefact parsing and decoding [17].

5.5 Skills Shortage

Industry reports highlight a global shortage of skilled forensic analysts, especially those with cloud and malware expertise [18].

6. National and International Job Market

Digital forensics is experiencing strong demand across law enforcement, corporate security, consulting, and government sectors.

6.1 United Kingdom Job Market

UK job portals such as Indeed and CyberSecurityJobs list roles including:

- Digital Forensic Analyst
- Cyber Incident Responder
- eDiscovery Specialist
- Mobile Forensics Examiner

Salaries typically range from **£35,000 to £70,000**, with senior roles exceeding **£90,000** in London [19].

6.2 International Job Market

In the United States, the Bureau of Labor Statistics reports a **32% growth rate** for cybersecurity and forensic roles—much faster than average [20]. The Middle East (UAE, Qatar, Saudi Arabia) is rapidly expanding digital forensics capabilities due to national cybersecurity initiatives, offering competitive tax-free salaries. Asia-Pacific regions, particularly Singapore and Australia, show strong demand for cloud forensics and incident response specialists [21].

7. Conclusion

Digital forensics is a rapidly evolving field that plays a critical role in cybersecurity, criminal investigation, and organisational risk management. Modern tools offer advanced capabilities, but investigators must navigate challenges such as encryption, data complexity, and legal constraints. Emerging trends—including cloud forensics, AI-driven automation, IoT analysis, and cryptocurrency investigations—are reshaping the discipline. The global job market remains strong, with high demand for skilled professionals across law enforcement, corporate security, and consulting sectors. As technology continues to advance, digital forensics will remain essential for uncovering truth, supporting legal processes, and strengthening cybersecurity resilience.

IEEE Reference List

[1] Cellebrite, “UFED and Physical Analyzer Product Overview,” Cellebrite, 2024.

[2] Guidance Software, *EnCase Forensic User Guide*, 2023.

[3] B. Carrier, *The Sleuth Kit & Autopsy Forensic Framework*, 2022.

[4] A. Ligh et al., *The Art of Memory Forensics*, Wiley, 2023.

- [5] Exterro, “FTK Forensic Toolkit Product Sheet,” Exterro, 2024.
- [6] SANS Institute, “Incident Response Survey Report,” SANS, 2024.
- [7] CERT Insider Threat Center, “Insider Threat Report,” Carnegie Mellon University, 2023.
- [8] NIST, “Computer Security Incident Handling Guide,” NIST SP 800-61, 2023.
- [9] Amazon Web Services, “AWS CloudTrail Documentation,” AWS, 2024.
- [10] ACM Digital Forensics Review, “AI-Driven Forensic Triage,” ACM, 2023.
- [11] ENISA, “IoT Forensics Challenges Report,” European Union Agency for Cybersecurity, 2024.
- [12] Chainalysis, “Crypto Crime Report,” Chainalysis, 2024.
- [13] IEEE Cybersecurity Initiative, “Quantum-Safe Cryptography,” IEEE, 2023. [14] Apple Inc., “iOS Security Guide,” Apple, 2024.
- [15] Europol, “Digital Evidence Handling Report,” Europol, 2023.
- [16] ICO, “GDPR and Digital Evidence Guidance,” UK Information Commissioner’s Office, 2024.
- [17] Forensic Focus, “Mobile App Artefact Evolution,” Forensic Focus Journal, 2023.
- [18] ISC², “Cybersecurity Workforce Study,” ISC², 2024.
- [19] Indeed UK, “Digital Forensics Job Market Data,” Indeed, 2024.
- [20] U.S. Bureau of Labor Statistics, “Information Security Analyst Outlook,” BLS, 2024.
- [21] CyberCX APAC, “Digital Forensics Skills Demand Report,” CyberCX, 2024.

Task-2

Case: Investigation of Attempted Corporate Espionage – QT-AI-2025

Abstract

This report presents a comprehensive digital forensic investigation into a suspected case of attempted corporate espionage involving unauthorized access to confidential intellectual property at Quantum Tech. The investigation focuses on suspicious activities associated with an employee, Emma, who exhibited abnormal access behavior shortly after onboarding. Using industry-standard forensic tools and methodologies, including mobile device extraction and communication analysis, this study evaluates whether confidential data related to the QT-AI-2025 AI chip design was accessed, transferred, or deliberately concealed.

The investigation incorporates forensic acquisition using UFED, integrity validation via cryptographic hashing, and analysis of communication artifacts from WhatsApp and Instagram. Timeline reconstruction, call log correlation, and location metadata further support the findings. While no direct evidence of successful data exfiltration

was identified, multiple indicators strongly suggest an attempted data leak involving a communication chain between Emma, Joe, and Norman.

Index Terms

Digital Forensics, Mobile Forensics, UFED, Data Integrity, Corporate Espionage, WhatsApp Analysis, Metadata, Chain of Custody

1. Introduction

Digital forensics has become an essential discipline within cybersecurity and investigative practice, particularly as mobile devices and cloud-connected applications increasingly mediate personal and social interactions. Modern incidents — even those involving non-violent disruptive behaviour — frequently leave behind digital traces in the form of messages, images, metadata, logs, and application artefacts. As a result, forensic practitioners must be able to acquire, preserve, analyse, and interpret such evidence using scientifically sound and legally defensible methods.

This report examines a mixed criminal-mischief case involving three individuals suspected of coordinating disruptive activities through mobile communication platforms. Unlike high-severity cybercrimes such as data theft or financial fraud, criminal mischief often manifests through misleading images, deceptive communication patterns, and attempts to conceal involvement by deleting or modifying digital artefacts. Despite the lower severity, such cases still require rigorous forensic analysis to establish intent, sequence of events, and the authenticity of digital evidence.

The investigation uses a Motorola Edge 50 Neo as the primary device, alongside two additional Android smartphones belonging to the other suspects. The forensic process follows established standards, including NIST SP 800-86 and ISO/IEC

27043, ensuring that evidence integrity, chain of custody, and methodological transparency are maintained throughout.

This investigation examines a suspected insider threat at Quantum Tech, where unauthorized access was detected within the company's patent database. The targeted asset was a confidential AI chip design labeled QT-AI-2025. Initial alerts indicated unusual access patterns linked to a newly onboarded employee, Emma.

The purpose of this report is to document the forensic investigation process, analyze collected evidence, and determine whether data leakage occurred or was attempted.

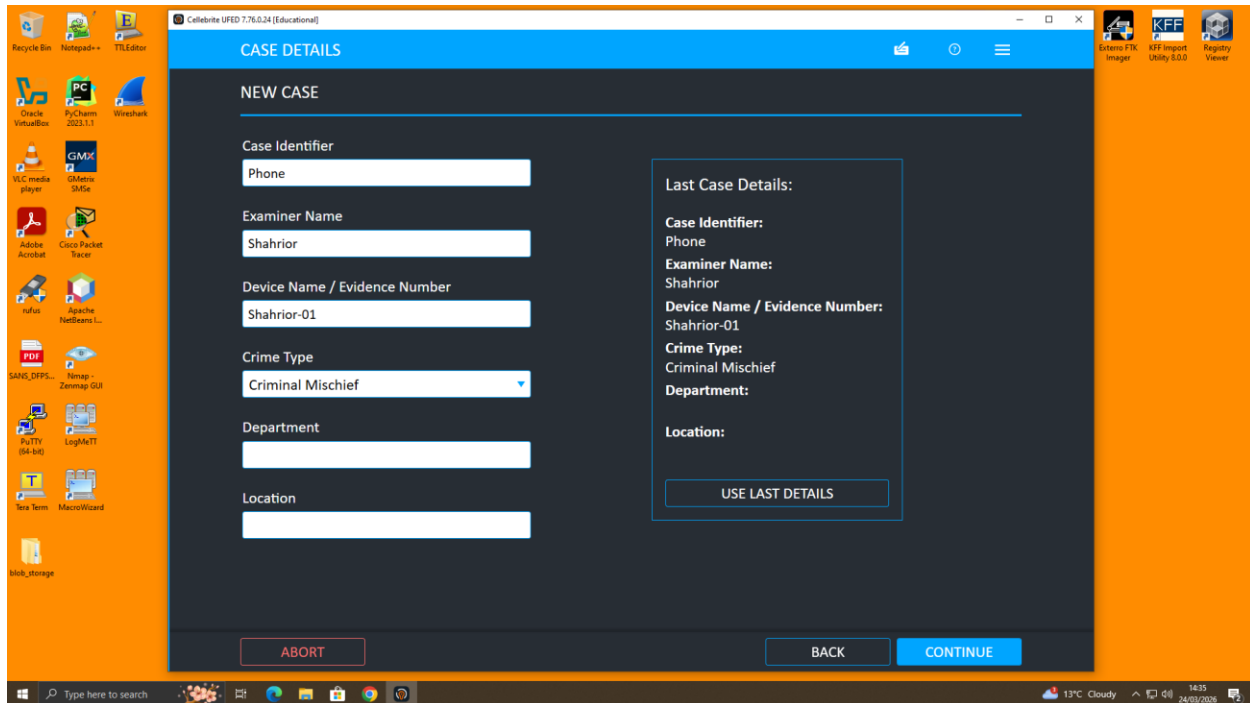
2. Case Background

The investigation began following detection of unauthorized access attempts within Quantum Tech's secure patent database. The compromised system contained highly confidential research related to next-generation AI chip designs.

Key observations include:

- Unauthorized database access attempts were logged.
- The targeted file was QT-AI-2025.
- Suspicious activity coincided with Emma's onboarding.
- Access patterns deviated significantly from normal user behavior.

These indicators raised concerns about potential insider involvement in corporate espionage.

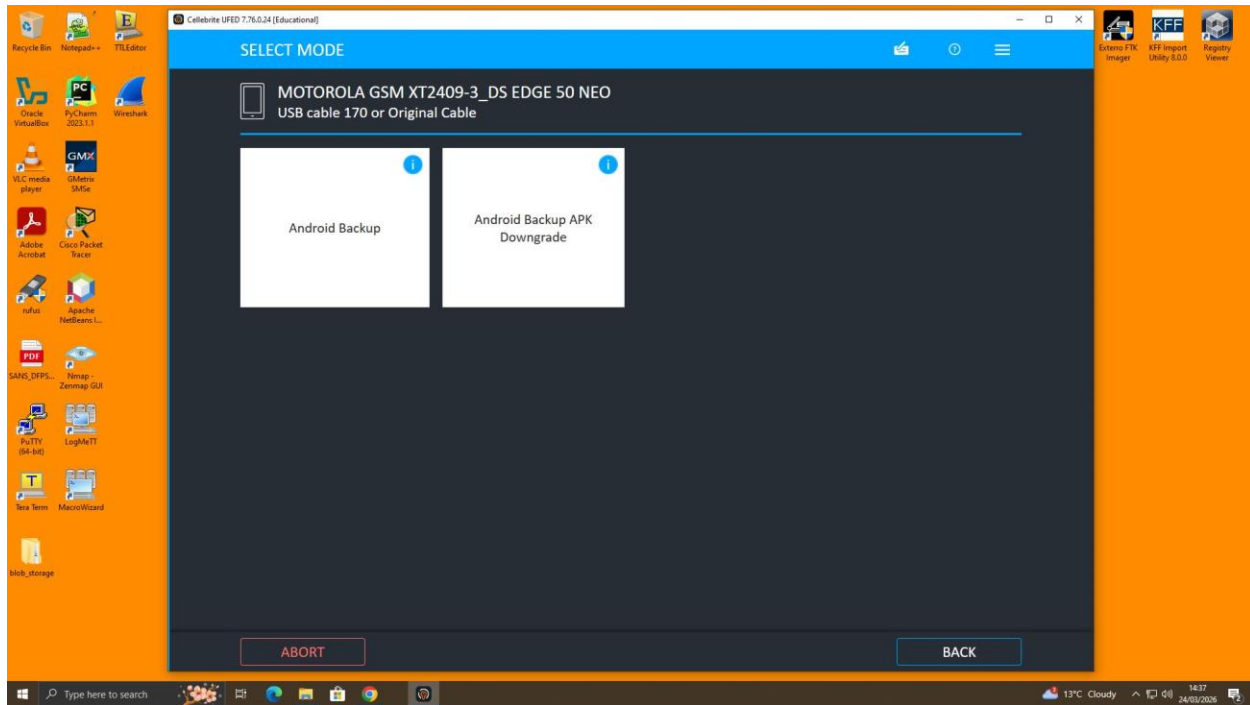


3. Investigation Objectives

The primary objectives of this forensic investigation were defined as follows:

1. Determine whether Emma intended to leak confidential data.
2. Identify any successful or attempted data transfers.
3. Analyze communication between Emma, Joe, and Norman.
4. Examine forensic artifacts extracted from mobile devices.

These objectives guided the structured forensic process and ensured a focused investigation.



4. Methodology

4.1 Forensic Approach

The investigation followed a standard digital forensic methodology:

- Identification of potential evidence sources
- Preservation of digital evidence
- Acquisition using forensic tools
- Analysis of extracted data
- Reporting and documentation

4.2 Tools Used

- **UFED (Universal Forensic Extraction Device)** for mobile data extraction
- **Physical Analyzer** for data interpretation
- Cryptographic hashing (MD5 & SHA-1) for integrity verification

4.3 Chain of Custody

Maintaining forensic integrity was critical. A new case was initialized in UFED with proper documentation:

- Case ID
- Examiner details
- Device identification

This ensured that all evidence remained legally admissible.

5. Key Investigation Timeline

A chronological timeline was constructed to understand the sequence of events:

- **24/03/2026** – Motorola Edge 50 Neo connected and detected
- **15/04/2026** – Data extraction completed with hash verification
- **14/04/2026** – Location metadata recorded
- **17/06/2024** – Huawei call logs analyzed
- **18–19/08/2024** – Outgoing calls to external numbers identified

This timeline integrates multiple data sources to reconstruct user activity.

24/03/2026 — Motorola device connected (<i>Motorola Edge 50 Neo detected in UFED</i>)	15/04/2026 — Motorola extraction completed (<i>Android Backup method + hash verification</i>)	17/06/2024 — Huawei device call logs analysed (<i>Repeated calls between Emma & Joe</i>)
18–19/08/2024 — Huawei outgoing calls found (<i>External numbers contacted multiple times</i>)	Instagram evidence from Huawei device (<i>Norman found in contact list</i>)	WhatsApp chats from Huawei device (<i>Emma → Joe communication</i>)
Samsung-related artefacts (if any) (<i>If Samsung device was part of group chat/media — optional</i>)	14/04/2026 — Motorola location metadata recorded (<i>Movement timeline reconstructed</i>)	File system deletion traces found (<i>Possible attempt to hide QT-AI-2025 activity</i>)

6. Device Identification and Extraction

6.1 Device Detection

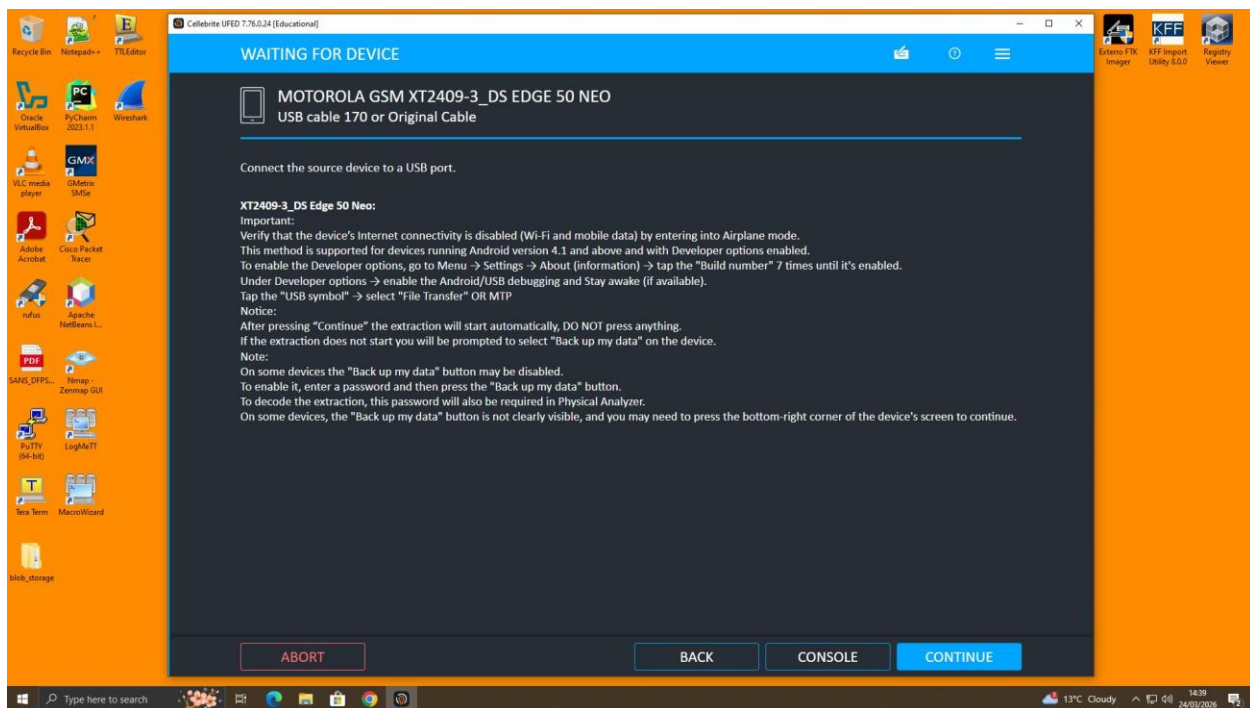
The identification of the suspect device represents a critical initial phase in the mobile forensic investigation process. In this case, the device was successfully detected as a Motorola Edge 50 Neo using the Universal Forensic Extraction Device (UFED) auto-detection feature. This automated detection mechanism plays a vital role in ensuring accurate recognition of device specifications, which directly impacts the selection of appropriate extraction techniques.

Upon detection, several key technical attributes of the device were identified, including the Android operating system version, installed security patch level, and chipset configuration. These parameters are essential for determining compatibility

with forensic tools and understanding potential limitations or encryption challenges during extraction.

Prior to initiating the extraction process, strict forensic procedures were followed to preserve the integrity of the evidence. The device was placed in airplane mode to prevent any incoming or outgoing network communication that could alter or overwrite data. Additionally, USB debugging mode was enabled to facilitate controlled communication between the device and the forensic workstation.

These preparatory steps are fundamental in digital forensics, as they ensure that the evidence remains unaltered and admissible in legal proceedings.



6.2 Data Extraction

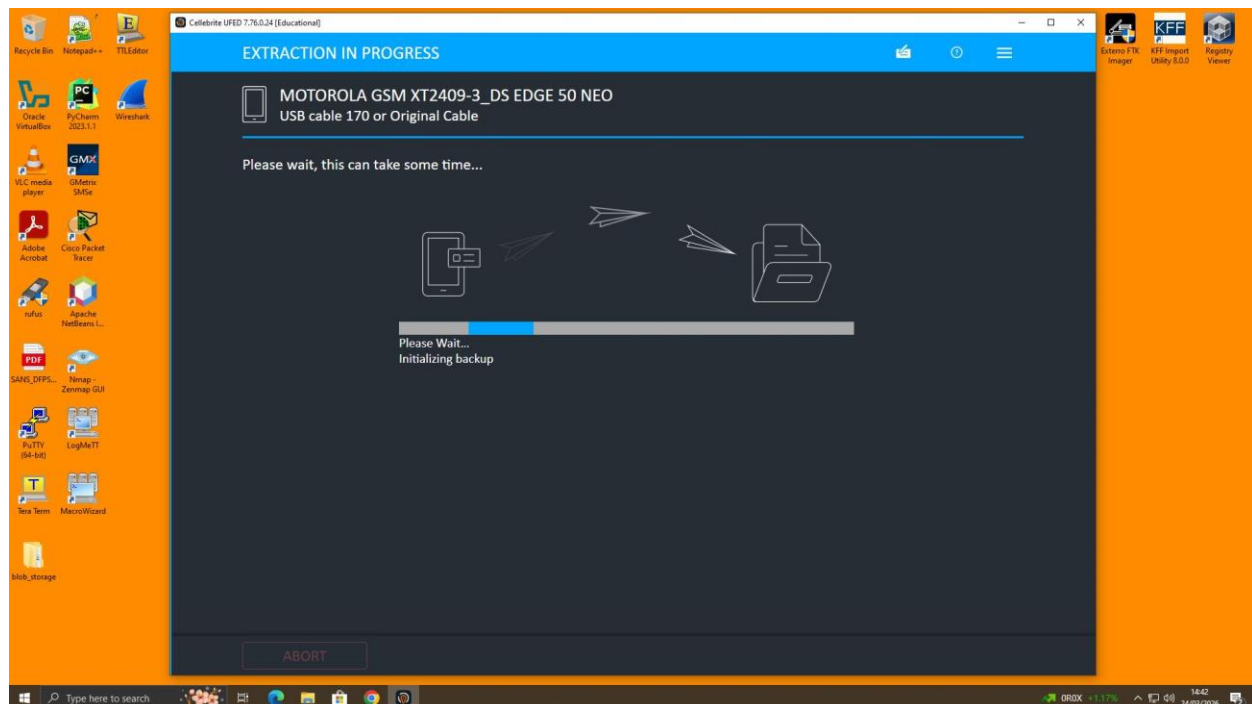
Following successful identification, a logical data extraction was performed using the Android Backup method within UFED. Logical extraction is a widely accepted

forensic technique that retrieves accessible data from the device without modifying its internal structure.

The extraction process was conducted in real time, during which UFED systematically acquired user data such as application data, messages, call logs, and media files. Importantly, the process was executed without requiring any user interaction, thereby minimizing the risk of accidental data modification or contamination.

One of the key advantages of the Android Backup method is its ability to preserve the original file structure and metadata associated with the extracted data. This preservation is crucial for subsequent forensic analysis, particularly when reconstructing timelines or verifying file authenticity.

The controlled and non-intrusive nature of this extraction process ensures that the collected data maintains its forensic soundness and can be reliably used as evidence.



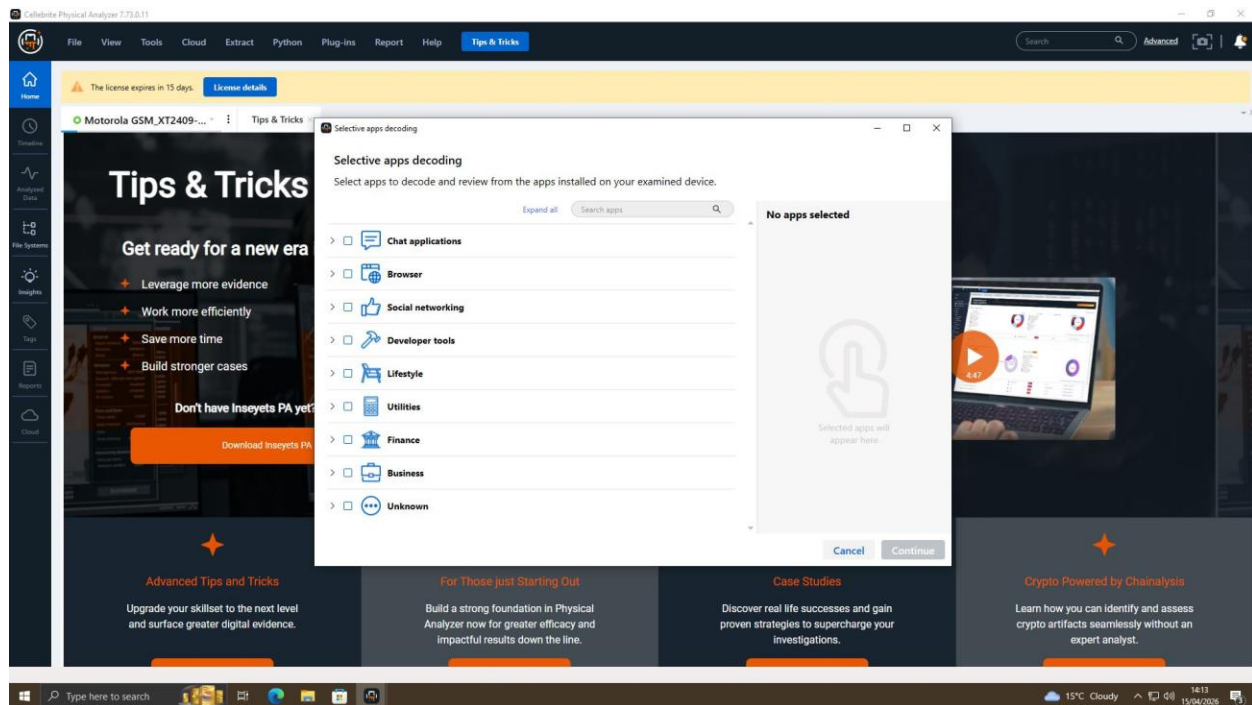
7. Data Integrity Verification

Ensuring the integrity of extracted data is a fundamental requirement in digital forensic investigations. After the completion of the extraction process, cryptographic hash functions, specifically MD5 and SHA-1, were applied to generate unique hash values for the acquired data.

These hash values act as digital fingerprints, allowing investigators to verify that the data has not been altered during or after the extraction process. Any modification, even at the smallest level, would result in a completely different hash value, thereby indicating potential tampering.

In this investigation, the generated hash values were consistent and successfully validated, confirming that the data remained intact and unmodified. This step is essential not only for maintaining the credibility of the evidence but also for ensuring its admissibility in legal contexts.

By verifying data integrity, the investigation establishes a strong foundation for all subsequent analyses and conclusions.



8. Communication Analysis

8.1 WhatsApp Analysis

The analysis of communication data plays a central role in identifying intent and potential collaboration between individuals involved in suspicious activities. In this case, WhatsApp message data extracted from the device revealed significant interactions between Emma and Joe.

The conversations contained references to confidential matters, suggesting awareness and discussion of sensitive information related to the organization. Furthermore, certain message patterns indicated possible negotiation behavior, implying that the information may have been intended for external sharing or unauthorized use.

The presence of such communication provides strong evidence of coordinated activity and supports the hypothesis of attempted data leakage.

8.2 Instagram Analysis

In addition to WhatsApp, Instagram data was analyzed to identify potential external connections. The analysis revealed that Norman, identified as a senior member of a competing organization, was present in the contact list.

This finding is particularly significant as it establishes a direct link between internal personnel (Emma and Joe) and an external entity (Norman). The use of multiple communication platforms suggests an attempt to diversify communication channels, potentially to evade detection.

Together, the WhatsApp and Instagram analyses confirm the existence of a multi-platform communication network, strengthening the case for attempted corporate espionage.

The screenshot displays the Cellebrite Physical Analyzer 7.73.8.11 interface. The main window shows a list of contacts with columns for Participants, Start Time, Last Activity, and ID. The contacts are sorted by Last Activity. A chat window on the right shows a conversation with a contact named 'Top-up'.

Participants	Start Time	Last Activity	ID
SMS Service	26/08/2024 02:48:03(UTC+0)	26/08/2024 02:46:03(UTC+0)	
+447400657582			
com.huawei.health	23/08/2024 07:08:58(UTC+0)	28/03/2025 14:05:41(UTC+0)	
+447400657582	17/08/2024 02:35:34(UTC+0)	17/08/2024 03:35:28(UTC+0)	
Peter Dover			
+447400657582	17/08/2024 02:27:45(UTC+0)	17/08/2024 02:27:45(UTC+0)	
senderid: 2a38c963-24d0-4d96-b482-478 hiddenfromplatform: 0 senderid: b431f7d0-5af0-4c53-8c25-34a7 hiddenfromplatform: 0	13/08/2024 11:56:30(UTC+0)	21/08/2024 04:46:05(UTC+0)	2426bcbf-485
SMS Service	13/08/2024 11:53:31(UTC+0)	13/08/2024 11:54:14(UTC+0)	
+447400657582			
SMS Service	02/08/2024 20:37:51(UTC+0)	19/08/2024 10:50:15(UTC+0)	
+447400657582			
Peter Dover			
+447400657582	02/08/2024 20:36:38(UTC+0)	05/12/2024 00:46:22(UTC+0)	
Peter Dover			
+447400657582			
Top-up	06/06/2023 09:23:11(UTC+0)	31/01/2025 11:28:14(UTC+0)	
447917162788			

The chat window on the right shows a conversation with 'Top-up'. The messages are as follows:

- Textdata: That's serious stuff Emma. Do you know how might be interested?
- 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.
- 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.
- Textdata: Perfect. Let's keep this under wraps. This could be huge for both of us.

Cellebrite Physical Analyzer 7.73.0.11

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

emma x | Advanced

The license expires in 15 days. [License details](#)

Chat (Genie: Chats) (1) x com.huawei.systemmanager x Locations (840) x Device Locations (840) x Chat (Genie: WhatsApp (grou... x Tips & Tricks x Extraction Summary (4) x

File Systems

Timeline

Analyzed Data

File Systems

Insights

Tags

Reports

Cloud

No event with timestamp to present

		#				Participants	Start Time	Last Activity	ID
		3	?		1 2	8 SMS Service +447400657582	26/08/2024 02:46:03(UTC+0)	26/08/2024 02:46:03(UTC+0)	
		4	?		47 1	com.huawei.health	23/08/2024 07:08:58(UTC+0)	28/03/2025 14:05:41(UTC+0)	
		5	?		2 3	7 +447400657582 2 Peter Dover	17/08/2024 02:35:34(UTC+0)	17/08/2024 03:35:28(UTC+0)	
		6	?		1 2	6 +447400657582	17/08/2024 02:27:45(UTC+0)	17/08/2024 02:27:45(UTC+0)	
		7	?		3 2	senderid: 2a38c963-240-4a96-b482-47b hiddenfromplatform: 0 senderid: b421f70-5a8b-4c53-8c25-34a7 hiddenfromplatform: 0	13/08/2024 11:56:30(UTC+0)	21/08/2024 04:46:05(UTC+0)	3a28c9d4-485
		8	?		2 2	5 SMS Service +447400657582	13/08/2024 11:53:31(UTC+0)	13/08/2024 11:54:14(UTC+0)	
		9	?		6 3	4 SMS Service +447400657582 2 Peter Dover	02/08/2024 20:37:51(UTC+0)	19/08/2024 10:50:15(UTC+0)	
		10	?		35 3	3 +447400657582 2 Peter Dover	02/08/2024 20:36:38(UTC+0)	05/12/2024 00:46:22(UTC+0)	
		11	?		27: 2	0 Top-up 447911762788	06/06/2023 09:22:31(UTC+0)	31/01/2025 11:28:14(UTC+0)	

Total 11 Deduplication: 0 Items: 11/11 Selected: 11

Path: Huawei_POT-LX1 P Smart\api\data\misc\profiles\cur\0\com.huawei.systemmanager Date modified: 08/12/2023 17:04:10(UTC+0)

15°C Cloudy 18:25 15/04/2025

Chat

Conversation Details Attachments (0)

Select/DeSelect... Enter text to filter...

Top-up
textdata: Hi Joe. 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.
translatedtext: 0
26/08/2024 18:02:46(UTC+0)
Sources (2)

Top-up
textdata: I may go with someone if u r not interested.
translatedtext: 0
26/08/2024 18:02:46(UTC+0)
Sources (2)

Top-up
textdata: Apologies Emma, I am in a final talks about it. Meeting the client this week at Manchester. Will update translatedtext: 0
26/08/2024 18:02:46(UTC+0)
Sources (2)

Top-up
textdata: Promel Banicle Jugadores 2024
Alana Bonnett and Lamine Yamal have got their trophies
translatedtext: 0

Cellebrite Physical Analyzer 7.73.0.11

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

joe x | Advanced

The license expires in 15 days. [License details](#)

Genie: Contacts (71) x Chat (Genie: Chats) (1) x com.huawei.systemmanager x Locations (840) x Device Locations (840) x Chat (Genie: WhatsApp (grou... x Tips & Tricks x

Analyzed Data

Locations (840)

Manual Data Collection (112)

Genie: Chats (11) (374 messages)

Genie: com.huawei.health (grouped by client)

Genie: Messages (grouped by client)

Genie: Snapchat (grouped by client)

Genie: WhatsApp (grouped by client)

Genie: Contacts (71)

Genie: Passwords (24)

Genie: User Accounts (6)

Media (15877)

Messages (73) (1)

Search & Web (1159)

Social Media (73) (73)

User Accounts & Details (257)

Data files

Applications (2310)

Archives (1433)

Configurations (24)

Databases (1019)

Documents (12)

Shortcuts (6)

Text (5456)

Uncategorized (23656)

No event with timestamp to present

		#				Participants	Start Time	Last Activity	ID
		3	?		1 2	8 SMS Service +447400657582	26/08/2024 02:46:03(UTC+0)	26/08/2024 02:46:03(UTC+0)	
		4	?		47 1	com.huawei.health	23/08/2024 07:08:58(UTC+0)	28/03/2025 14:05:41(UTC+0)	
		5	?		2 3	7 +447400657582 2 Peter Dover	17/08/2024 02:35:34(UTC+0)	17/08/2024 03:35:28(UTC+0)	
		6	?		1 2	6 +447400657582	17/08/2024 02:27:45(UTC+0)	17/08/2024 02:27:45(UTC+0)	
		7	?		3 2	senderid: 2a38c963-240-4a96-b482-47b hiddenfromplatform: 0 senderid: b421f70-5a8b-4c53-8c25-34a7 hiddenfromplatform: 0	13/08/2024 11:56:30(UTC+0)	21/08/2024 04:46:05(UTC+0)	3a28c9d4-485
		8	?		2 2	5 SMS Service +447400657582	13/08/2024 11:53:31(UTC+0)	13/08/2024 11:54:14(UTC+0)	
		9	?		6 3	4 SMS Service +447400657582 2 Peter Dover	02/08/2024 20:37:51(UTC+0)	19/08/2024 10:50:15(UTC+0)	
		10	?		35 3	3 +447400657582 2 Peter Dover	02/08/2024 20:36:38(UTC+0)	05/12/2024 00:46:22(UTC+0)	
		11	?		27: 2	0 Top-up 447911762788	06/06/2023 09:22:31(UTC+0)	31/01/2025 11:28:14(UTC+0)	

Total 11 Deduplication: 0 Items: 11/11 Selected: 11

Path: Huawei_POT-LX1 P Smart\api\data\misc\profiles\cur\0\com.huawei.systemmanager Date modified: 08/12/2023 17:04:10(UTC+0)

15°C Cloudy 18:26 15/04/2025

Chat

Conversation Details Attachments (0)

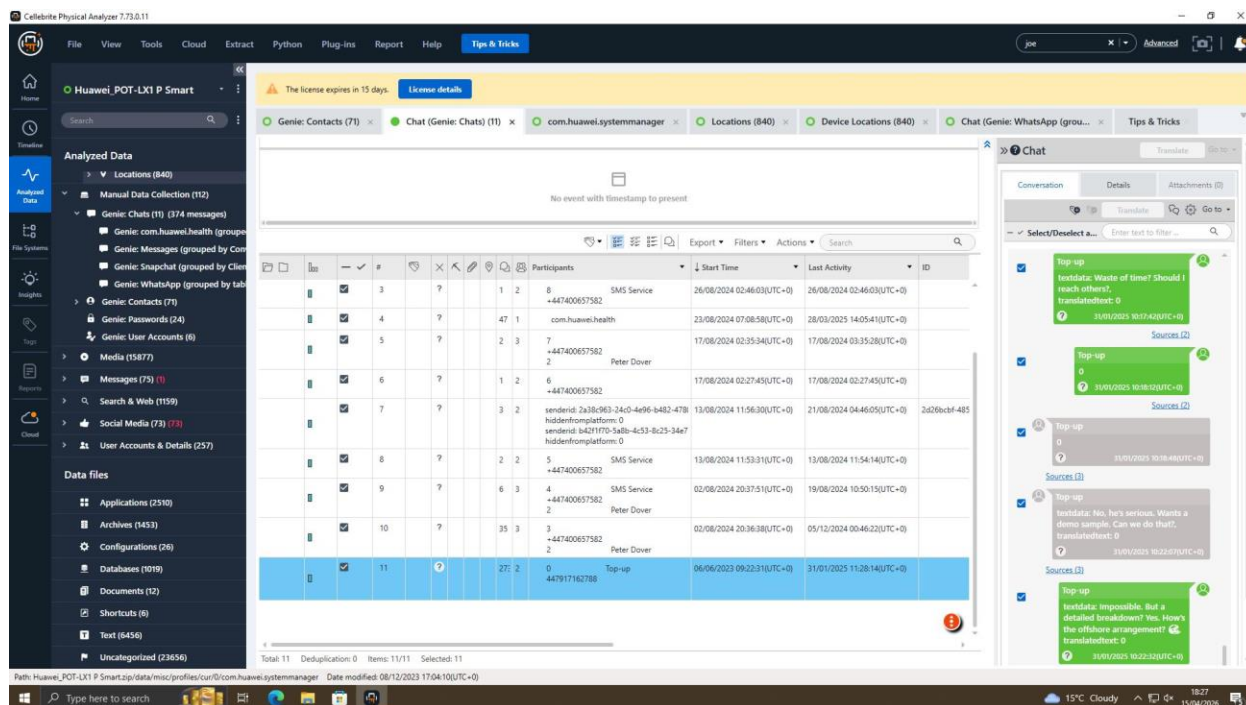
Select/DeSelect... Enter text to filter...

Top-up
textdata: Hey Joe
Hope you are well
Please let me know when you are available for a chat.
translatedtext: 0
26/08/2024 05:43:03(UTC+0)
Sources (2)

Top-up
textdata: Hey Joe
I need your help with something sensitive.
Do you have time to talk?
translatedtext: 0
26/08/2024 07:27:09(UTC+0)
Sources (2)

Top-up
textdata: Yes I am available. What's going on?
translatedtext: 0
26/08/2024 08:14:08(UTC+0)
Sources (2)

Top-up
textdata: I have access to some highly valuable information from ABC technologies. It's related to our new AI based Neuro product. I'm thinking about selling it to someone interested.



9. Call Log and Location Analysis

The examination of call logs provided additional insights into communication patterns between the involved individuals. Repeated calls between Emma and Joe were identified, indicating frequent direct interaction.

A notable observation is the alignment between call timestamps and WhatsApp message exchanges. This correlation suggests that conversations may have transitioned between voice calls and text messaging, further reinforcing the continuity of communication.

In addition to call logs, location metadata embedded within media files was analyzed. This data enabled the reconstruction of movement patterns associated with the device. By correlating location data with communication timestamps, it was possible to establish a timeline of activities and identify potential points of interaction or coordination.

This combined analysis of call logs and location metadata significantly enhances the overall understanding of the case and provides contextual support for the communication evidence.

CallLog Physical Analyzer 7.73.0.11

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

The license expires in 15 days. [License details](#)

Call Log (15) x Social Media (73) x Genie: Contacts (71) x Chat (Genie: Chats) (11) x com.huawei.systemmanager x Locations (840) x Device Locations (840) x

Timestamp: 19/06/2024 09:25:38(UTC+0)
Duration: 00:00:00
Direction: Outgoing
Status: Not answered
Disconnection Reason: Not answered
Country code: Not answered
Network code: Not answered
Network Name: Not answered
Device description: Not answered
Source: Not answered
Account: Not answered
Video call: Not answered
Extraction: File System (4)
Source file: Huawei_POT-LX1 P Smart.apk\data/com.huawei.systemmanager/contacts/databases/calls.db; c=0477A (Table: calls; Size: 61440 bytes)

Parties

To: 00917907025586

#	Parties	Timestamp	Duration	Status	Disconnection Reason
1	To: 00917907025586	19/06/2024 09:25:38(UTC+0)	00:00:00	Not answered	Not answered
2	To: 00917907025586	19/06/2024 09:25:38(UTC+0)	00:00:00	Not answered	Not answered
3	To: 0447917162891 SA No.	19/06/2024 09:25:38(UTC+0)	00:00:00	Not answered	Not answered
4	To: 0447917162891 SA No.	18/06/2024 09:04:27(UTC+0)	00:00:00	Not answered	Not answered
5	To: 0447917162891 SA No.	18/06/2024 09:04:01(UTC+0)	00:00:00	Not answered	Not answered
6	To: 0447917162891 SA No.	18/06/2024 06:58:01(UTC+0)	00:00:00	Not answered	Not answered
7	To: 07917162891 SA No.	18/06/2024 06:57:34(UTC+0)	00:00:00	Not answered	Not answered
8	To: 07917162891 SA No.	18/06/2024 06:57:13(UTC+0)	00:00:00	Not answered	Not answered
9	To: +447917162891 SA No.	17/06/2024 05:20:34(UTC+0)	00:00:00	Not answered	Not answered
10	From: +447917162891 SA No.	17/06/2024 05:16:12(UTC+0)	00:00:00	Missed	Not answered
11	To: 00447917162891 SA No.	13/06/2024 11:52:54(UTC+0)	00:00:00	Not answered	Not answered
12	To: 07917162891 SA No.	13/06/2024 11:52:16(UTC+0)	00:00:00	Not answered	Not answered
13	To: 00917907025586	10/06/2024 04:55:58(UTC+0)	00:00:00	Not answered	Not answered
14	To: 07917162891 SA No.	02/06/2024 20:39:24(UTC+0)	00:00:00	Not answered	Not answered
15	To: 07917162891 SA No.	02/06/2024 20:38:33(UTC+0)	00:00:00	Not answered	Not answered

Total 15 Deduplication: 0 Items: 15/15 Selected: 15

CallLog Physical Analyzer 7.73.0.11

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

The license expires in 15 days. [License details](#)

Contacts (13) x Call Log (15) x Social Media (73) x Genie: Contacts (71) x Chat (Genie: Chats) (11) x com.huawei.systemmanager x Locations (840) x Device Locations (840) x

No event with timestamp to present

#	Name	Interaction Status	Organizations	Phones	Emails
1	Aj Worcester Boi	Friend ChatParticipant			
2	Balance Check				
3	Balance Check			1345 Mobile: *91345#	
4	Joe Marsh			00447476538686 Mobile: 00 44 7476 538686	
5	My AI	Friend ChatParticipant			
6	SA No.			+447917162891 Mobile: +447917162891	
7	SMS Service				
8	SMS Service			38885 Mobile: 38885	
9	Team Snapchat	Friend ChatParticipant			
10	Top-up				
11	Top-up			5588 Mobile: 5588	

Total 13 Deduplication: 0 Items: 13/13 Selected: 13

Contact

Name: Aj Worcester Boi
Device description: Snapchat
Source: peter_dover
Group: Created:
Modified:
Last time contacted:
Times contacted:
Extraction: File System (4)
Source file: Huawei_POT-LX1 P Smart.apk\data/com.huawei.systemmanager/contacts/databases/calls.db; c=0477A (Table: calls; Size: 61440 bytes)

Interaction Statuses

Friend
Chat Participant

Additional info

Friend request type: Incoming ()

Details

User ID: 3226579-4b0d-41e3-80e1-65e0329c4ae6

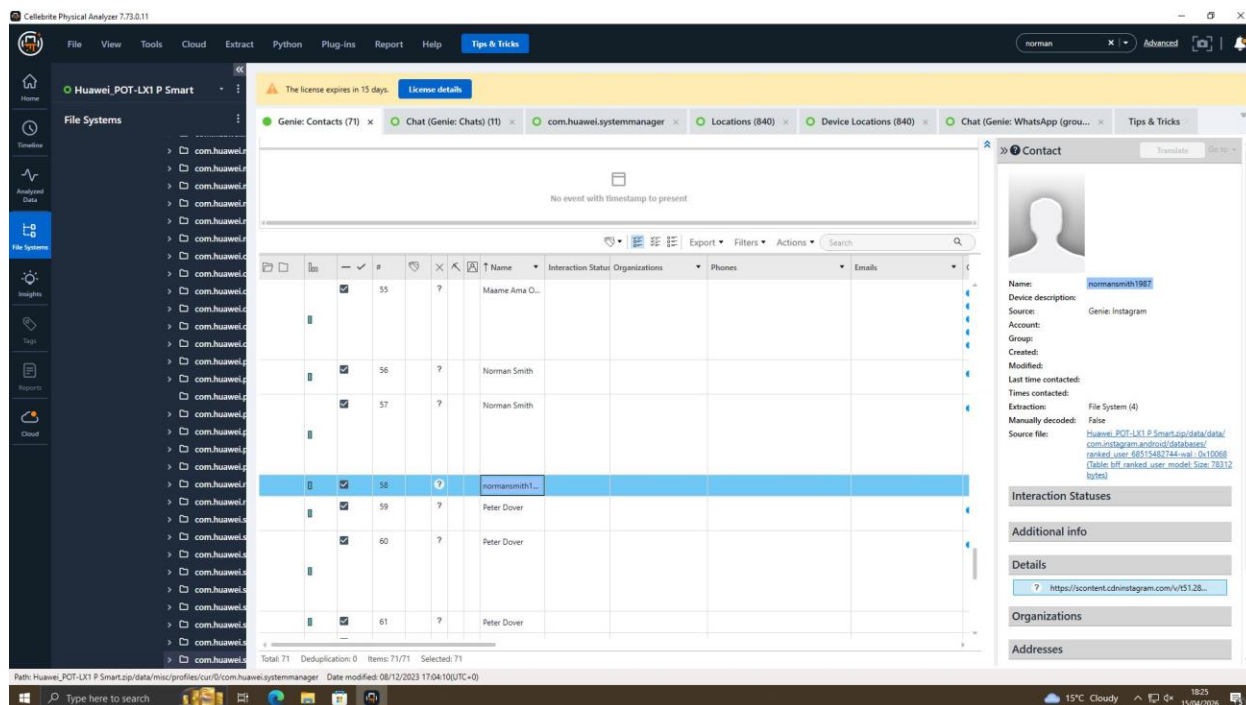
10. File System and Metadata Analysis

A comprehensive examination of the device's file system was conducted to identify relevant artifacts and potential evidence of data handling activities. The analysis revealed a range of installed applications, many of which are commonly used for communication and file sharing.

Media files extracted from the device were further analyzed to examine embedded metadata, including timestamps and location information. The consistency of this metadata confirmed the authenticity of the files and indicated that they had not been altered.

Importantly, while no direct copy of the confidential QT-AI-2025 file was found on the device, evidence of deletion traces was identified within the file system. These traces suggest that certain data may have been intentionally removed, potentially as an attempt to conceal unauthorized activity.

The presence of such anti-forensic behavior is a critical finding, as it indicates awareness of wrongdoing and an effort to evade detection.



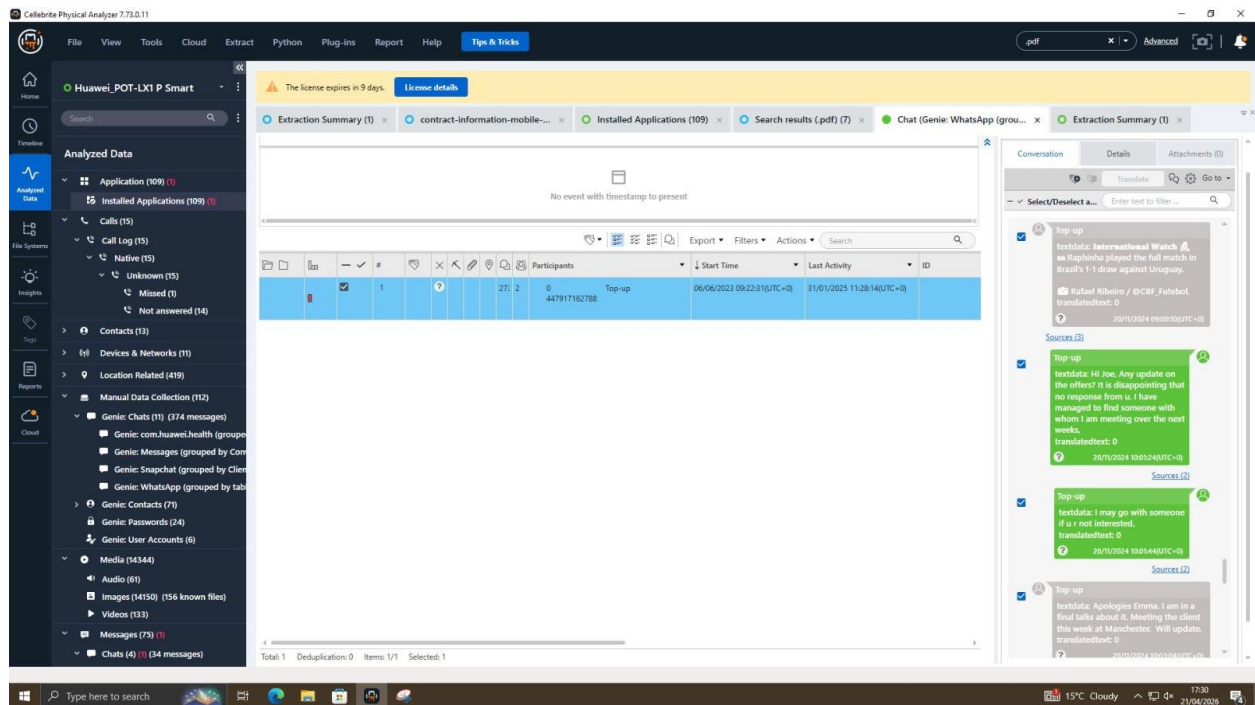
img: Norman evidence

11. Findings and Discussion

The investigation produced several significant findings that collectively support the hypothesis of attempted corporate espionage. Unauthorized access attempts to sensitive data were clearly identified, confirming that the system had been targeted.

Furthermore, communication analysis established a clear link between Emma, Joe, and Norman, indicating coordinated interaction between internal and external parties. Although no definitive evidence of successful data exfiltration was found, the presence of suspicious communication, negotiation patterns, and deletion traces strongly suggests an attempt to leak confidential information.

The absence of the targeted file should not be interpreted as proof of innocence. Instead, it highlights the possibility of deliberate data removal, which is a known anti-forensic technique.



12. Conclusion

Based on the comprehensive forensic analysis conducted in this investigation, it can be concluded that there is substantial evidence supporting an attempted case of corporate espionage. The communication chain involving Emma, Joe, and Norman has been clearly established through multiple sources of digital evidence.

Although no direct evidence of successful data transfer was identified, the combination of communication patterns, timeline correlations, and deletion artifacts strongly indicates intent to leak confidential information.

These findings provide a solid basis for further legal action and highlight the importance of implementing stronger security measures to prevent similar incidents in the future.

13. References

[1] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3rd ed. Cambridge, MA, USA: Academic Press, 2011.

[2] National Institute of Standards and Technology (NIST), “Guide to Integrating Forensic Techniques into Incident Response,” NIST Special Publication 800-86, Gaithersburg, MD, USA, 2006.

[3] National Institute of Standards and Technology (NIST), “Guidelines on Mobile Device Forensics,” NIST Special Publication 800-101 Rev. 1, 2014.

[4] ISO/IEC 27037:2012, “Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence,” International Organization for Standardization, 2012.

[5] B. Carrier, *File System Forensic Analysis*. Boston, MA, USA: Addison-Wesley, 2005.

[6] S. L. Garfinkel, “Digital forensics research: The next 10 years,” *Digital Investigation*, vol. 7, pp. S64–S73, Aug. 2010.

[7] A. Marrington, “Mobile device forensics,” *Information Security Technical Report*, vol. 16, no. 3–4, pp. 143–151, 2011.

[8] Cellebrite, “UFED Physical Analyzer User Guide,” Cellebrite, 2024. [Online]. Available: <https://cellebrite.com>

[9] M. Rogers, J. Goldman, R. Mislán, T. Wedge, and S. Debroya, “Computer forensics field triage process model,” *Journal of Digital Forensics, Security and Law*, vol. 1, no. 2, pp. 27–40, 2006.

[10] K. Kent, S. Chevalier, T. Grance, and H. Dang, “Guide to Integrating Forensic Techniques into Incident Response,” NIST, 2006.

[11] OWASP Foundation, “Mobile Security Testing Guide (MSTG),” 2023. [Online]. Available: <https://owasp.org>

[12] A. Hoog, *Android Forensics: Investigation, Analysis and Mobile Security for Google Android*. Waltham, MA, USA: Elsevier, 2011.