



University of Wales

Trinity Saint David

Department of Cyber Security and Digital Forensics
Master's Programme

Module: ACCA7031 – Digital Forensics Analysis

Assignment Title: Research, Analyse and Investigate Cybersecurity incidents and perform digital forensic assessment

Name:

Md Mahfuzur Rahman

ID:

2431582

Submission Date:

12 December 2025

Task-1: Research Report: The Evolving Field of Digital Forensics

1. Current State of the Field and Key Tools

Digital forensics has evolved from simple post-mortem hard-drive examination into a multidisciplinary field covering computer, mobile, network, cloud, IoT, and memory forensics. Contemporary research divides the field into specialised domains such as network forensics, cloud forensics, IoT forensics, and mobile forensics, each requiring unique methodologies and acquisition techniques (Zawoad & Hasan, 2015; Quick & Choo, 2018).

Key tools widely used in 2025 include FTK Imager, Autopsy/The Sleuth Kit, EnCase, X-Ways Forensics, Cellebrite UFED, and Wireshark. These tools support core functions:

Acquisition

Modern forensic imaging involves bit-for-bit duplication of disks, smartphone extractions, volatile-memory imaging, and cloud snapshot collection with hashing and write-blocking to maintain evidential integrity (Carrier, 2005; NIST, 2014).

Analysis

Forensic applications reconstruct file systems, generate timelines, carve deleted artefacts, and correlate logs and registry information across devices. Memory analysis frameworks such as Volatility remain critical for detecting fileless malware and unpacking volatile artefacts (Case et al., 2014).

Specialised Modules

Mobile forensics tools such as Cellebrite UFED and MSAB XRY extract app-level data, cloud synchronisation artefacts, and deleted items (Ayers, Brothers & Jansen, 2014). Tools like Wireshark support packet and flow analysis, while cloud forensic modules increasingly rely on API-based acquisition from services such as AWS and Microsoft 365 (Marty, 2011).

Reporting

Most forensic suites now offer automated reporting features with chain-of-custody tracking and court-ready evidence packaging (NIST, 2014).

A continuing trend is the shift toward integrated forensic-platform ecosystems, delivered as SaaS and designed to support remote collaboration and scalable multi-device investigations (Quick & Choo, 2018).

2. Intersection of Digital Forensics and Cybersecurity

Digital forensics is increasingly intertwined with cybersecurity through the rise of Digital Forensics and Incident Response (DFIR). During cyber incidents—such as ransomware outbreaks, insider breaches, or supply-chain compromises—DFIR teams collect volatile memory, endpoint artefacts, logs, and network captures to reconstruct intrusion paths and identify root causes (Casey, 2011).

Modern SOCs integrate digital-forensics tooling with SIEM, EDR, and XDR platforms, enabling automated evidence preservation when alerts are triggered (The MITRE Corporation, 2020).

Research at the intersection of AI, cybersecurity, and digital forensics explores machine-learning-driven anomaly detection, clustering, malware classification, and adversarial forensics related to AI-enabled systems (Bhardwaj et al., 2021).

Organisational Impact

- Faster and evidence-based incident response.
- Improved compliance with regulations such as GDPR, HIPAA, and breach-notification standards.
- Growth of hybrid cybersecurity–forensics roles such as DFIR Analyst, Threat Hunter (forensic-focused), and Cybercrime Investigator.

3. Emerging Trends in Digital Forensics

AI and Machine Learning

Due to massive increases in evidential volume, AI/ML is being used to automate triage, classify artefacts, detect anomalies, and accelerate review of multimedia and log datasets (Khan, Gani & Wahab, 2020).

Cloud and “As-a-Service” Forensics

Multi-tenant cloud infrastructures present unique technical and legal challenges. Forensic acquisition often relies on provider logs, snapshots, and API-driven collectors rather than physical access (Zawoad & Hasan, 2015). Cloud forensics has matured into a distinct subfield with its own frameworks and constraints.

Mobile, IoT, and Edge Forensics

As mobile devices dominate digital evidence, tools are continuously updated to handle encrypted apps, cloud-linked storage, and proprietary communication formats (Ayers et al., 2014). IoT devices—including vehicles, wearables, and smart-home systems—produce rich but fragmented data sources lacking standardisation (Oriwoh, Sant & Epiphaniou, 2013).

Integration with Cyber-Resilience and Zero-Trust

Zero-trust environments increasingly adopt forensic logging-by-design, enabling rapid detection and investigation of anomalous behaviour (UK NCSC, 2021).

4. Key Challenges

Encryption and Privacy

Widespread full-disk encryption and end-to-end encrypted communication present major obstacles for investigators. Legal debates continue around striking a balance between privacy and investigatory capability (Abelson et al., 2015).

Data Volume and Heterogeneity

Investigators frequently handle petabytes of logs, cloud artefacts and drive images. Scaling acquisition, indexing and correlation remains a major challenge despite automation (Bhardwaj et al., 2021).

Cloud and Jurisdictional Complexity

Distributed cloud environments raise issues related to legal authority, cross-border access, multi-tenant data, and chain-of-custody verification. Mutual Legal Assistance Treaties (MLATs) often delay investigations (Zawoad & Hasan, 2015).

Anti-Forensics and Ephemeral Artefacts

Adversaries employ secure deletion, log wiping, steganography, and memory-only malware to hide activity. Ephemeral cloud artefacts and volatile memory can vanish quickly without rapid acquisition (Case et al., 2014).

Skills Shortage

High-complexity investigations demand specialised expertise, and agencies worldwide face shortages of trained forensic practitioners (Interpol, 2022).

5. National and International Job Market

Market analyses estimate the global digital-forensics market at USD 10–13 billion in 2023–2025, projected to reach USD 22–48+ billion by 2030–2035, with a CAGR of 11–15% (MarketsandMarkets, 2023; Grand View Research, 2024).

Growth drivers include:

- Rising cybercrime and sophisticated threat actors.
- Regulatory pressures requiring forensic-ready auditing.
- Expansion of cloud, mobile, and IoT ecosystems.
- Increased integration of forensics with enterprise incident response.

Job portals show consistently high demand for roles such as Digital Forensics Analyst, DFIR Consultant, eDiscovery Specialist, and Cybercrime Investigator, with openings across government, financial institutions, law-enforcement, cloud providers, and Big-4 consultancies (Indeed, 2024; LinkedIn Jobs, 2024).

Typical required competencies include:

- Proficiency with EnCase, FTK, Autopsy, and Cellebrite.
- Experience in IR, malware analysis, and log forensics.
- Understanding of legal processes, disclosure rules and report writing for court.

Conclusion

Digital forensics has become a strategic discipline essential to both cybersecurity operations and criminal investigations. The field now encompasses cloud, mobile, IoT, and memory forensics, supported by powerful tools for acquisition, analysis, and reporting. While technological advancements improve investigator capability, challenges remain around encryption, data volume, cloud complexity, and anti-forensic techniques. Trends such as AI-driven analysis, forensic integration into zero-trust architectures, and growth of cloud forensics continue to reshape practice. Market projections and job-portal data confirm strong global demand for skilled practitioners, particularly those able to bridge technical forensics, cybersecurity, and regulatory compliance.

References

- Abelson, H. et al. (2015). *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*. MIT Computer Science and Artificial Intelligence Laboratory.
- Ayers, R., Brothers, S., & Jansen, W. (2014). *Guidelines on Mobile Device Forensics*. NIST Special Publication 800-101 Revision 1.
- Bhardwaj, A., Goundar, S., & Ray, S. (2021). AI-enabled digital forensics: challenges and future directions. *IEEE Access*, 9.
- Carrier, B. (2005). *File System Forensic Analysis*. Addison-Wesley.
- Case, A., Richard, G., & Walters, A. (2014). *Memory Forensics: The Art of Memory Analysis*. Wiley.
- Khan, M. N., Gani, A., & Wahab, A. W. (2020). Machine learning in digital forensics: applications, challenges, and future trends. *Journal of Network and Computer Applications*, 168.
- MarketsandMarkets. (2023). *Digital Forensics Market – Global Forecast to 2030*.
- Marty, R. (2011). Cloud application logging for forensics. *ACM Cloud Computing Security Workshop*.
- NIST. (2014). *Guide to Integrating Forensic Techniques into Incident Response*. SP 800-86.
- Oriwoh, E., Sant, P., & Epiphaniou, G. (2013). IoT forensics: Challenges and approaches. *IEEE Cyber Security Conference*.
- Quick, D., & Choo, K.-K. R. (2018). Digital forensics in the cloud era. *Forensic Science International: Digital Investigation*, 24.
- The MITRE Corporation. (2020). *ATT&CK® forensics integration guidance*.
- UK National Cyber Security Centre (NCSC). (2021). *Zero Trust Architecture Principles*.
- Zawoad, S., & Hasan, R. (2015). Cloud forensics: state-of-the-art and future directions. *Journal of Digital Forensics, Security and Law*, 10(4).

Task-2:Digital Forensics Investigation Report

Case ID: QT-DF-2025-11
Investigator: Md Mahfuzur Rahman
Organisation: Quantum Tech Incident Response Unit
Date: 12 December 2025

This report outlines the forensic acquisition of a Huawei POT-LX1 P Smart using Cellebrite UFED 4PC. It details each stage of the process, including device preparation, connection, extraction, hashing, and evidence verification. Screenshots accompany all steps to ensure transparency, authenticity, and evidential reliability for subsequent forensic analysis.

Figure 1: Collection Summart Report
The Collection Summary Report presents essential metadata from the extraction, including device identifiers, selected acquisition method, start and end times, and verification details. This information ensures transparency, supports chain-of-custody requirements, and confirms that the forensic process was conducted accurately and reliably.

Cellebrite Collection Summary

 Cellebrite
www.cellebrite.com

Collection Summary Report	
UFED 4PC ID	1136568878
UFED 4PC version	7.73.0.162
Extraction start time	2025-10-28 16:12:56
Extraction end time	2025-10-28 16:53:34
Selected vendor	Huawei
Selected model	POT-LX1 P Smart
Extraction type	File system
Extraction method	Kirin Live
Device Model	POT-LX1
OS Version	Android 10
Chipset	kirin710
Security Patch Level	2020-08-01
IMEI	860962043462662
IMEI2	860962043422658
Is Device Rooted	No
Number Of Installed Applications	263

Figure 2: Step 1

The UFED 4PC main interface serves as the starting point for acquisition, presenting multiple extraction categories and device options. It enables investigators to select appropriate methods and initiate a controlled, forensically sound data collection process.

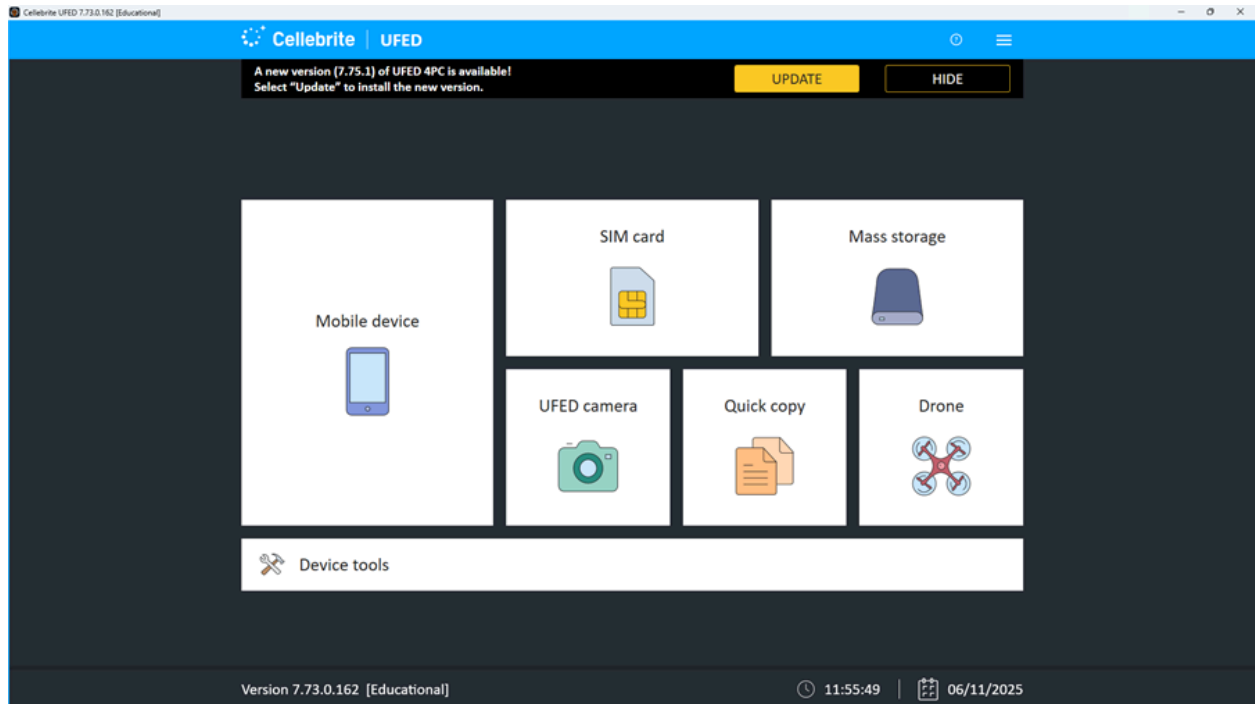


Figure 3: Step2

The case details entry screen records essential information such as examiner name, case ID, crime type, and evidence number. This ensures proper documentation, strengthens chain-of-custody, and links the extraction to a formally registered investigation.

Celebrite UFED 7.73.0.162 [Educational]

CASE DETAILS

NEW CASE

Case Identifier

Examiner Name

Device Name / Evidence Number

Crime Type

Department

Location

Use details from last case:

Case Identifier:
sdjyhf

Examiner Name:
gllndg

Device Name / Evidence Number:
1

Crime Type:
Theft

Department:
|Security

Location:
Alibaba kj gufa

USE LAST DETAILS

ABORT BACK CONTINUE

Figure 4: Step 4 acquisition paths. This step guides the workflow, ensuring the correct extraction method is applied based on device type and investigative requirements.

Celebrite UFED 7.73.0.162 [Educational]

CHOOSE ACTION

Smart Flow

Auto Detect

Search Devices

Device Wizard

ABORT BACK

Figure 5: Step 5

Auto Detect preparation instructions guide the examiner through enabling developer mode and USB debugging on the device. These steps ensure UFED 4PC can properly recognise the handset, establish communication, and perform a secure, forensically sound extraction without altering or compromising evidential data.

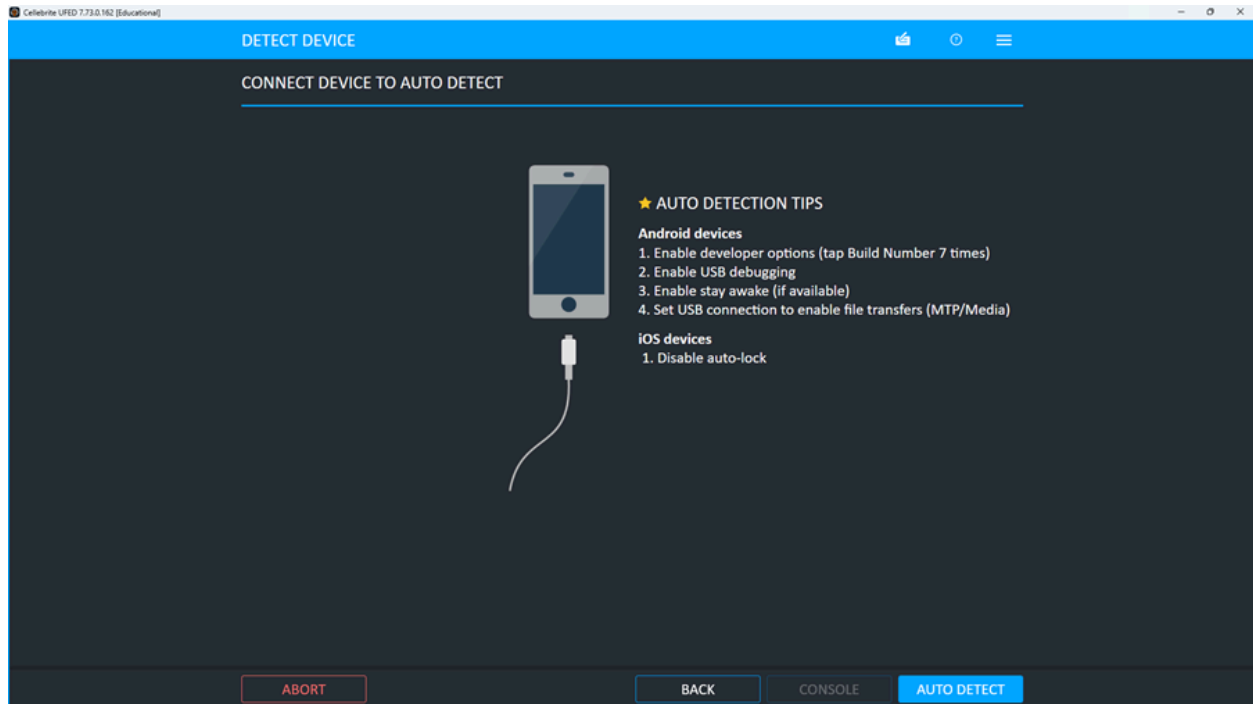


Figure 6: Step 6

Automatic detection of the Huawei device confirms the model, OS, and connection status, allowing UFED 4PC to initialize the appropriate extraction workflow. This step ensures accurate identification and prepares the system for a secure, validated data acquisition process.

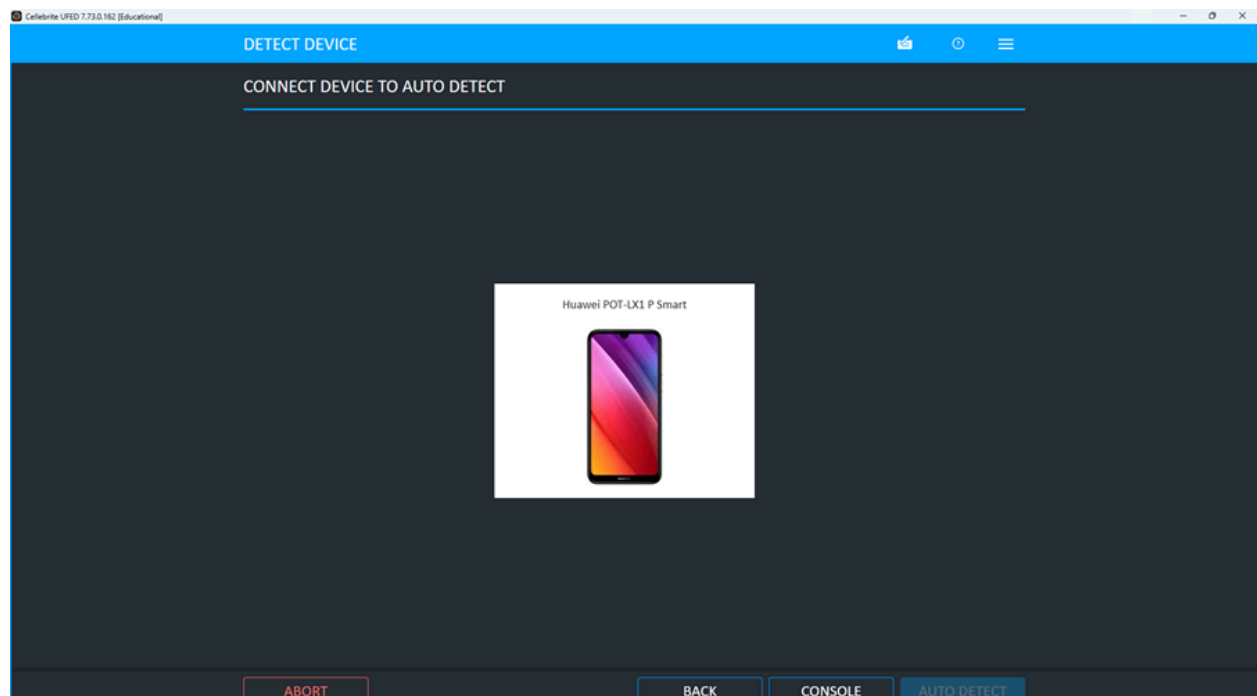


Figure 7: Step7

The extraction type selection screen allows the examiner to choose the most suitable method. File system extraction is selected to obtain deeper access to application data, system files, and artefacts essential for comprehensive forensic examination.

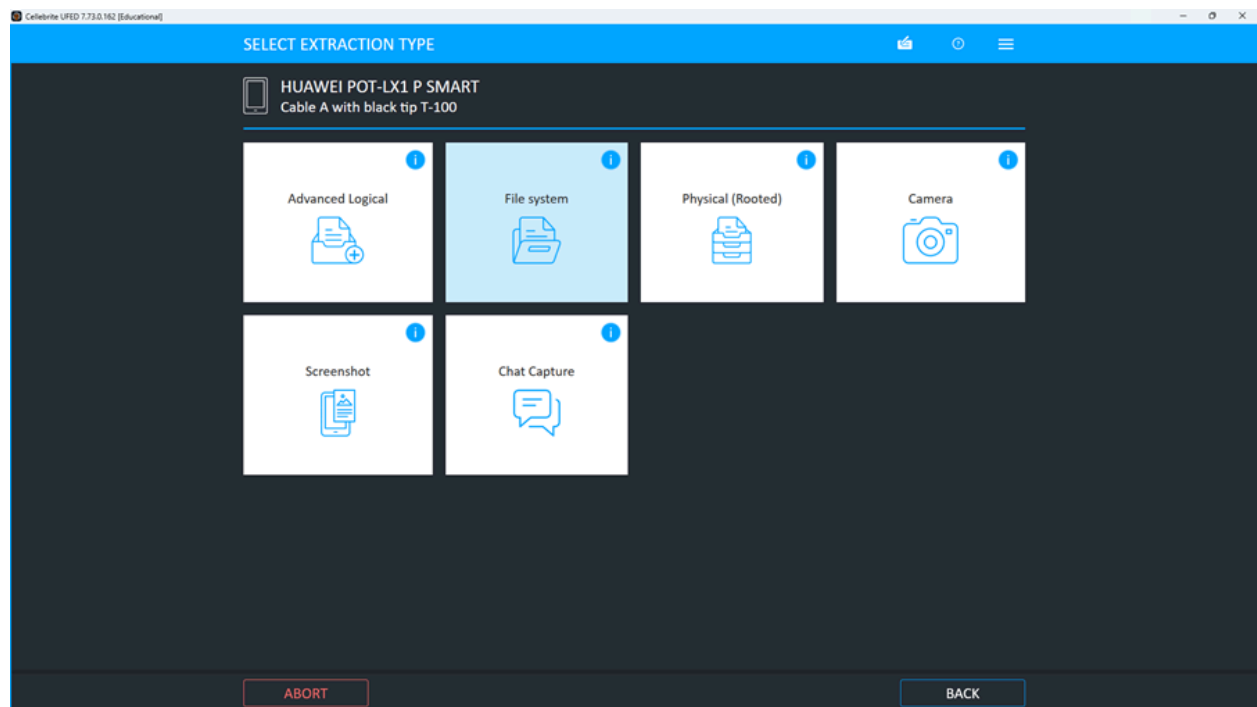


Figure 8: Step 8

The extraction mode selection screen presents options tailored to the device. Kirin Live mode is chosen specifically for Huawei devices using Kirin chipsets, enabling deeper data access while maintaining device integrity during the live forensic acquisition process.

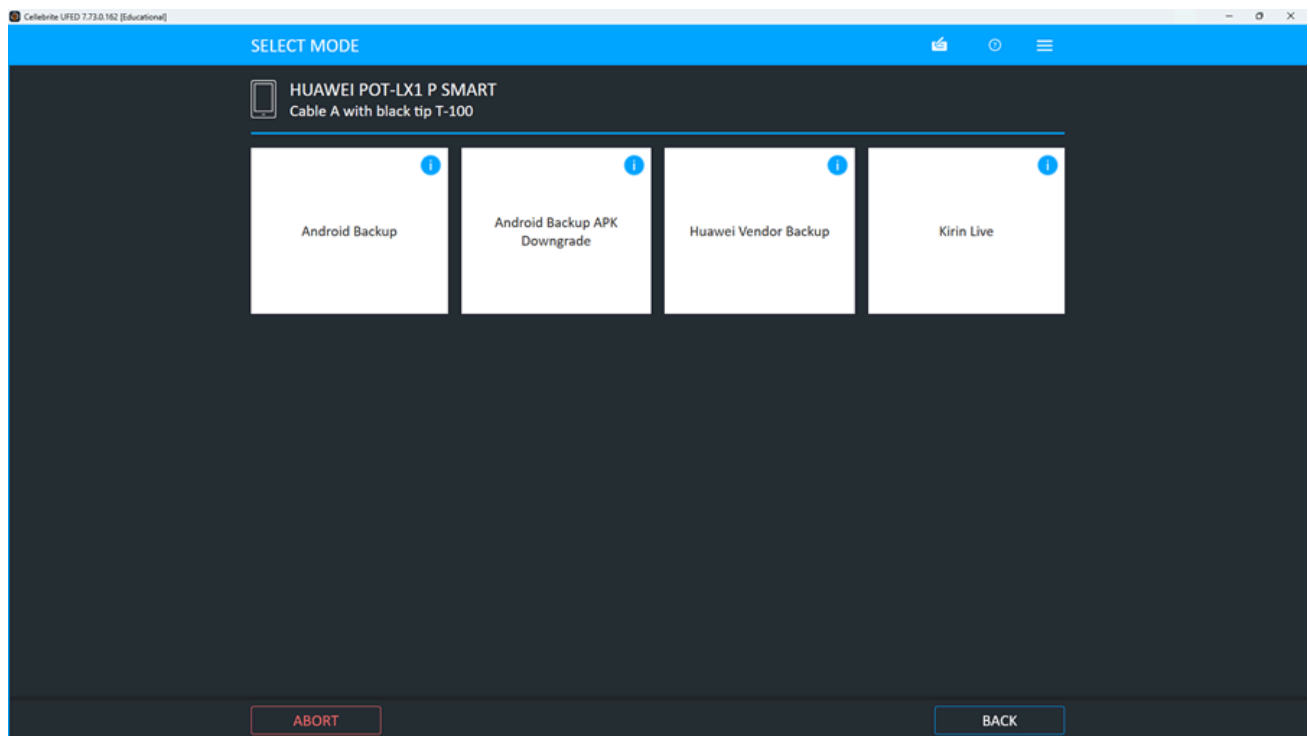


Figure 9: Step9

The examiner selects a secure extraction destination on the local machine, ensuring evidence is stored in an isolated, write-protected directory. This step preserves data integrity and maintains proper forensic handling throughout the acquisition process.

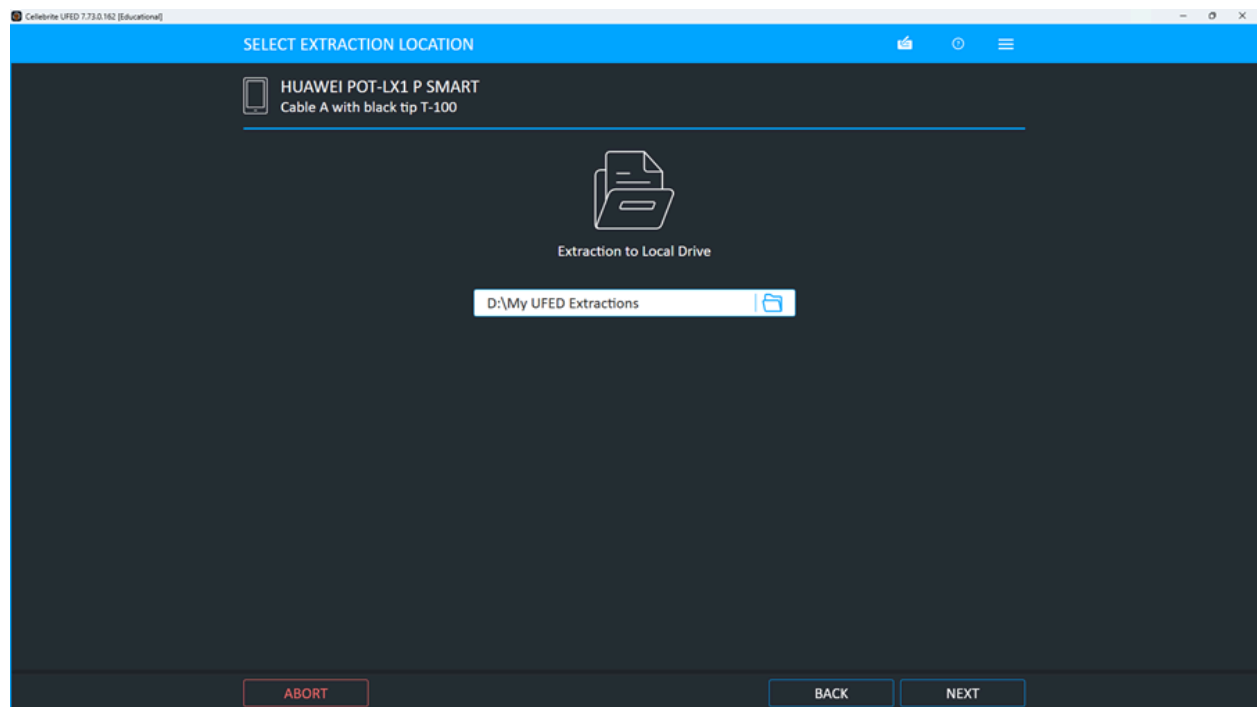


Figure 10: Step10

UFED provides device-side instructions to guide the user through enabling settings that ensure stable ADB communication. These steps help maintain a reliable connection throughout the extraction process, preventing interruptions and preserving the integrity of the collected forensic evidence.

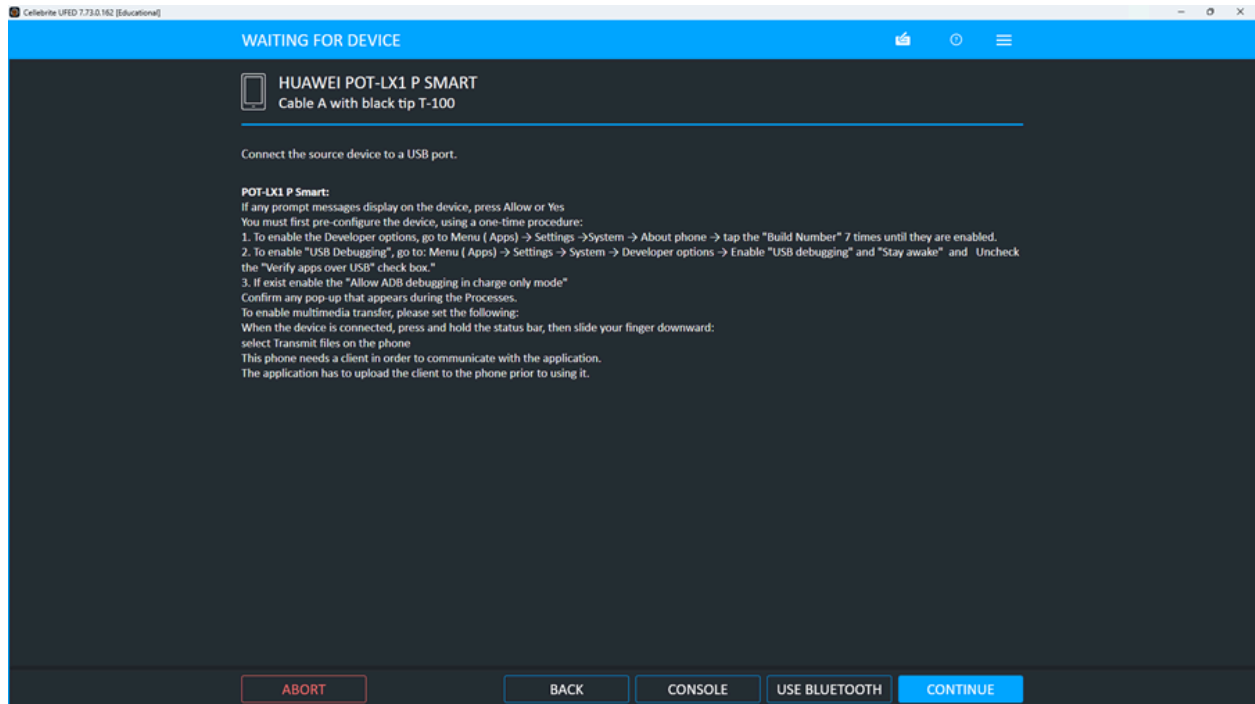


Figure 11: Step 11

The data content selection screen allows choosing what types of data to extract from the device.

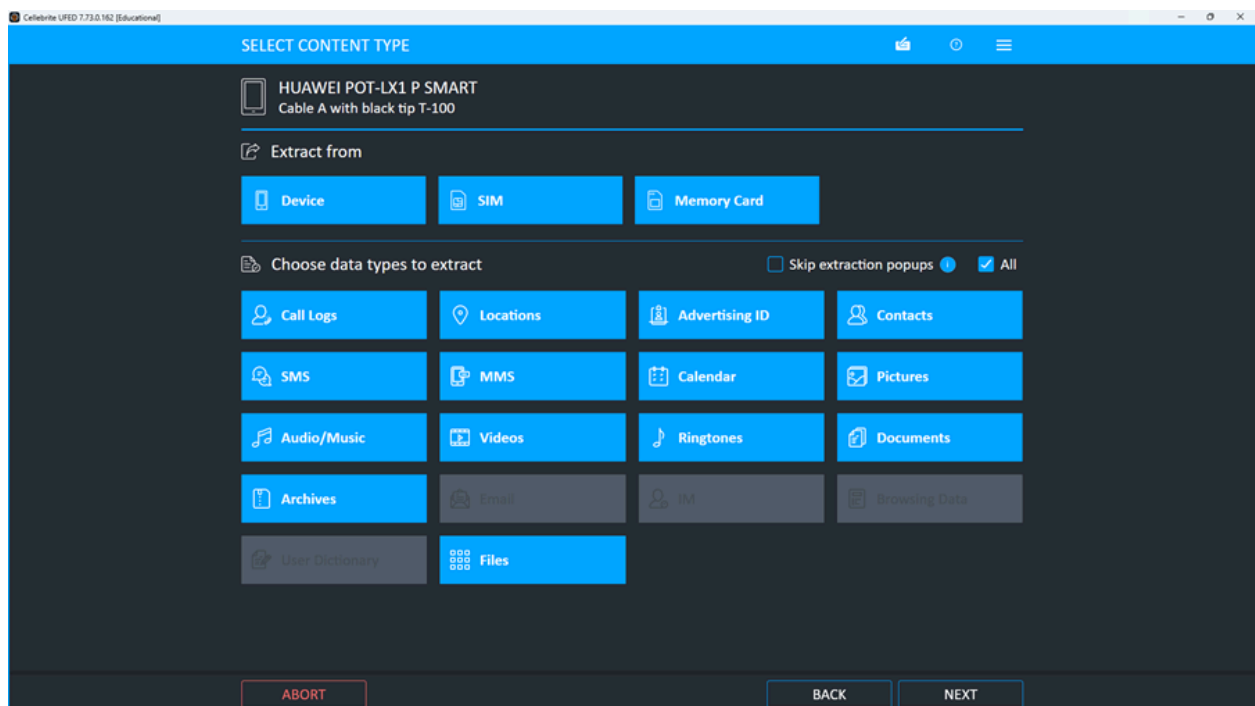


Figure 12: Step12

A warning message alerts the examiner that specific extraction methods may require a device restart. This notification ensures preparedness, prevents unexpected interruptions, and maintains a controlled forensic environment during the acquisition process.

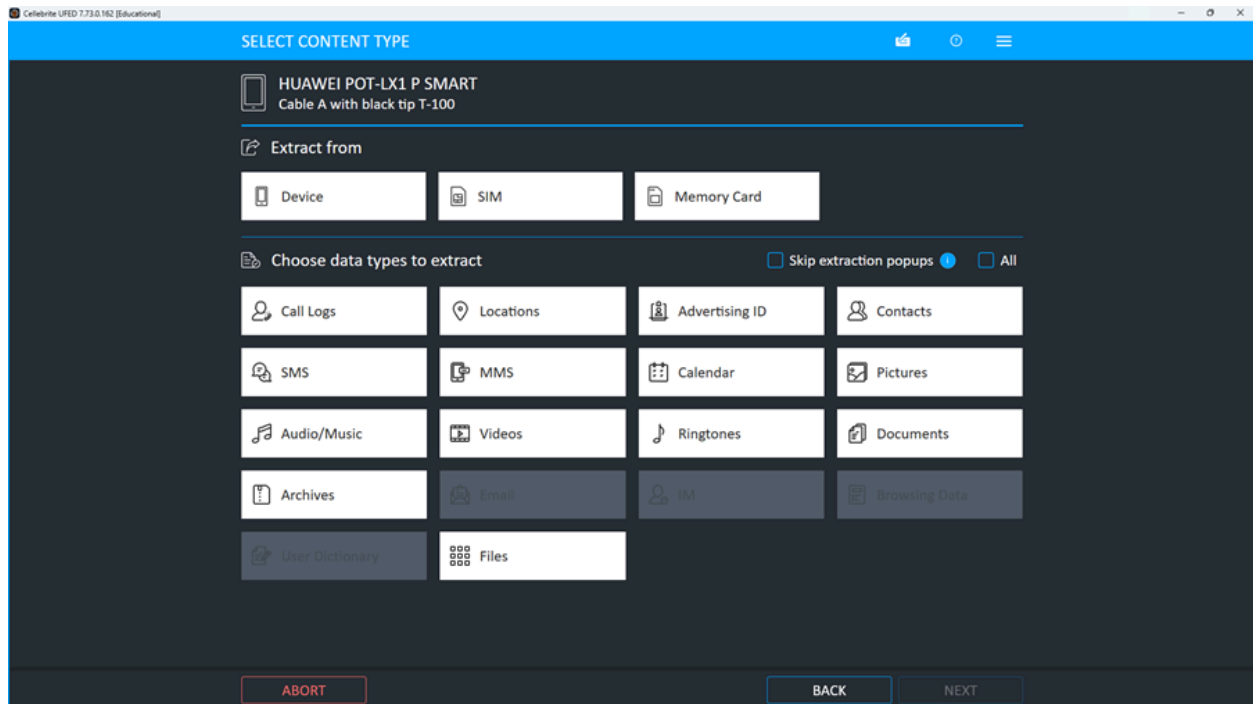


Figure 13: Step13

The extra info read failure message indicates UFED was unable to retrieve certain device details. It provides troubleshooting steps such as reconnecting the cable, enabling debugging, or restarting the device to restore stable communication and continue the forensic extraction process.

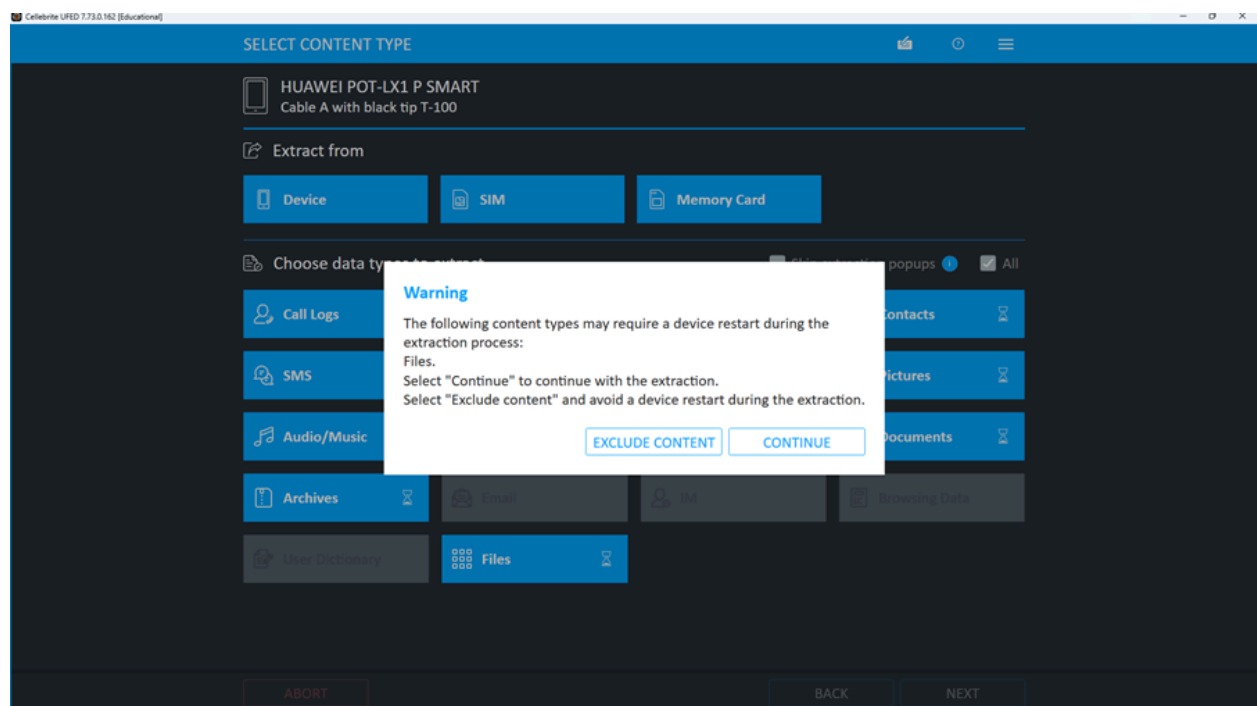


Figure 14: Step 14

A prompt displays the available multimedia extraction options, including photos, videos, and audio files, along with estimated data size and extraction time. This helps the examiner plan the acquisition and prioritise artefacts relevant to the investigation.

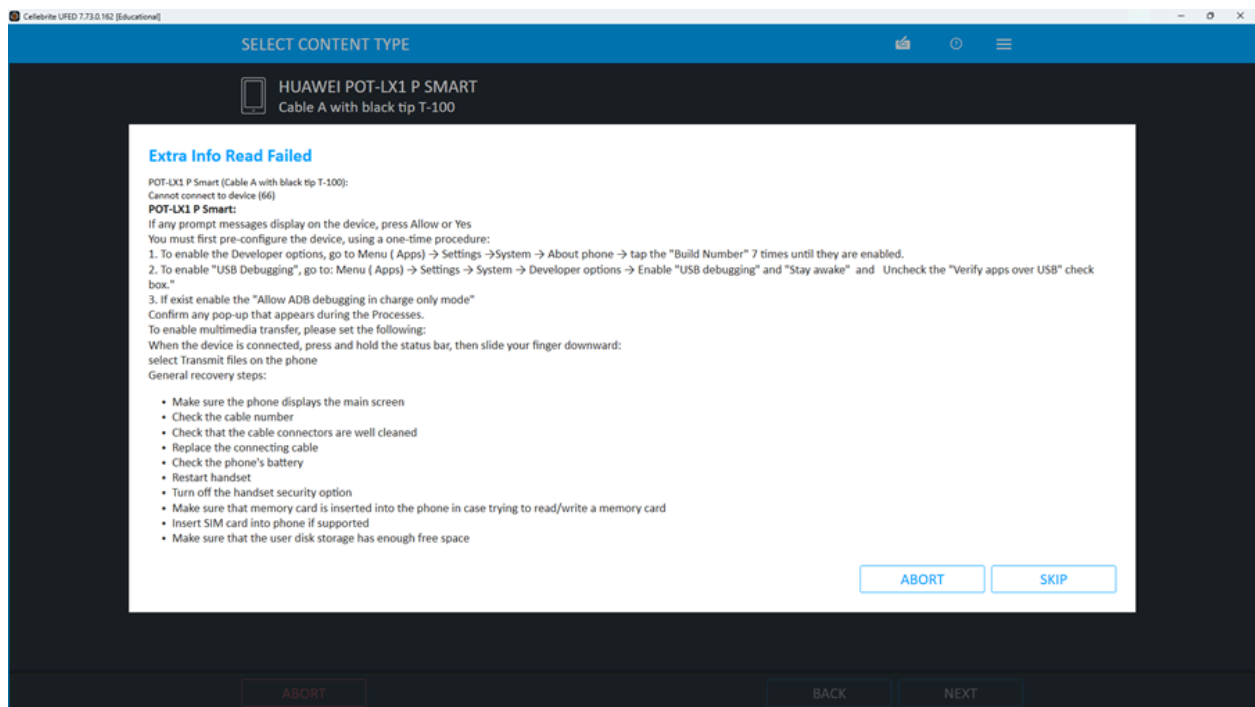


Figure 15: Step 15
Extraction Summary displaying successful and unsuccessful extracted data categories.

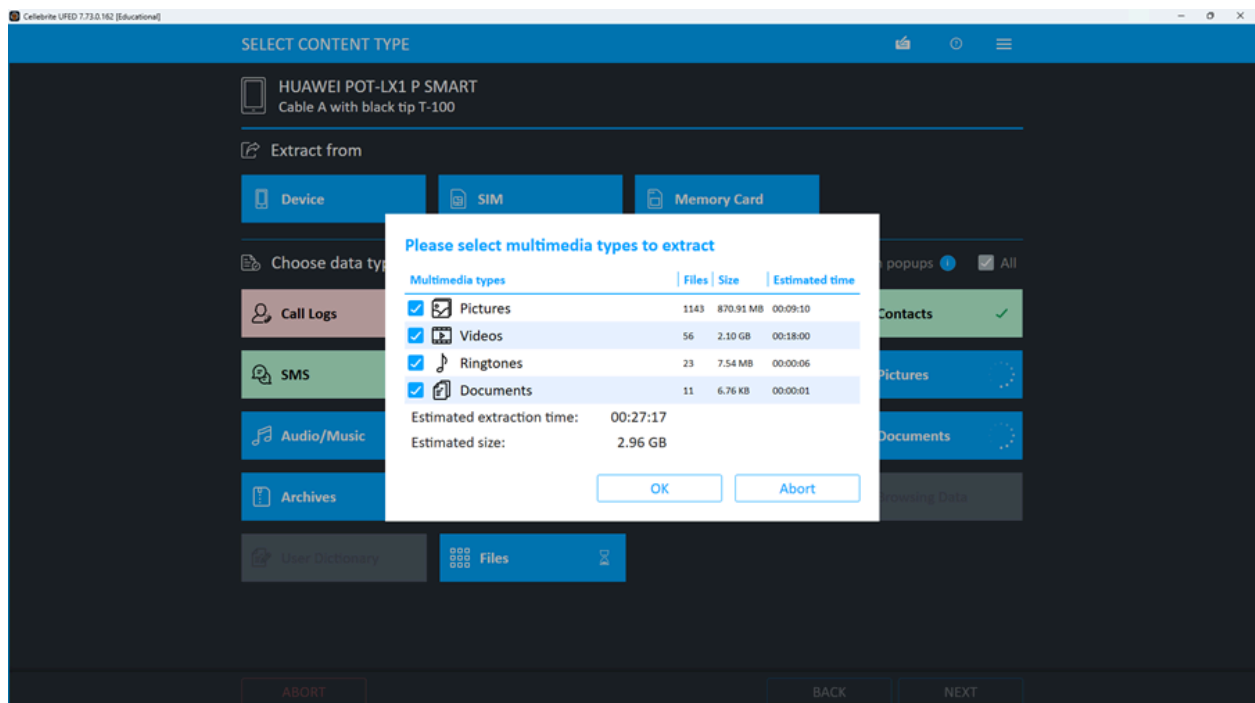


Figure 16: Step 16

Android Backup APK downgrade warning, used for older or restricted Android versions.

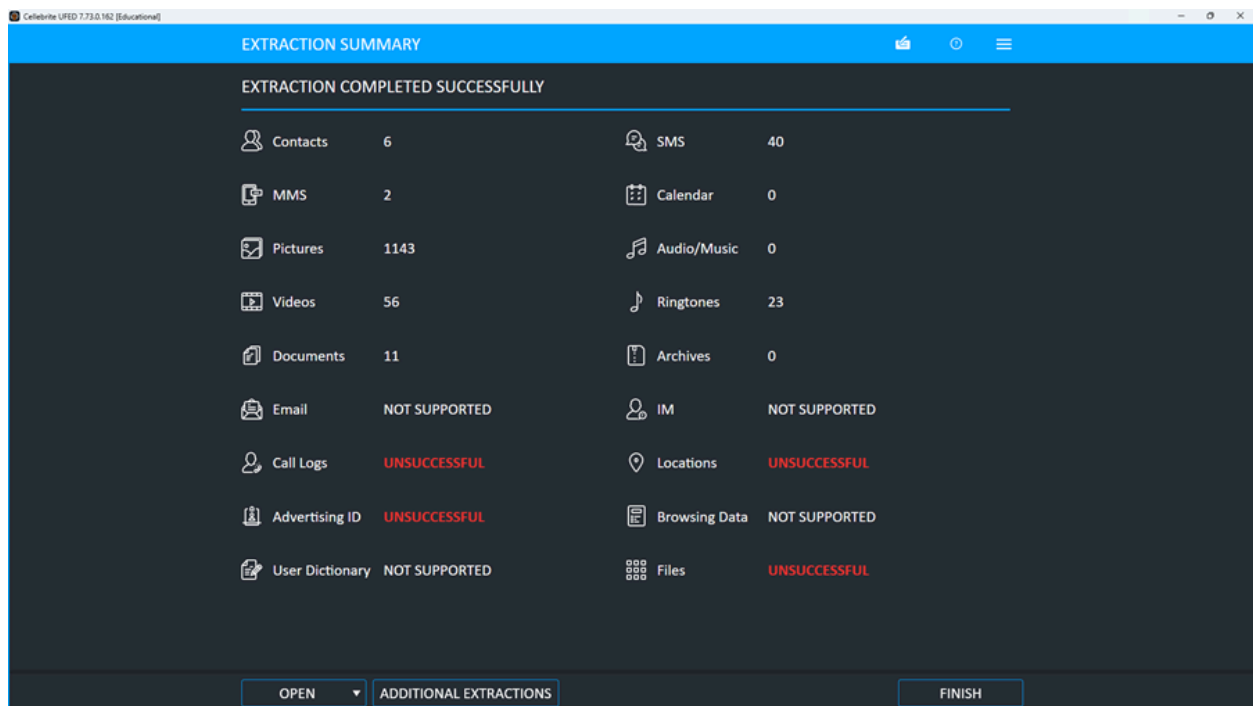


Figure 17: Step 17

The final extraction folder structure displays the organised output of the acquisition, including advanced logical data and file system dumps. This structure allows the examiner to easily locate artefacts, verify completeness, and proceed with detailed forensic analysis using compatible tools.

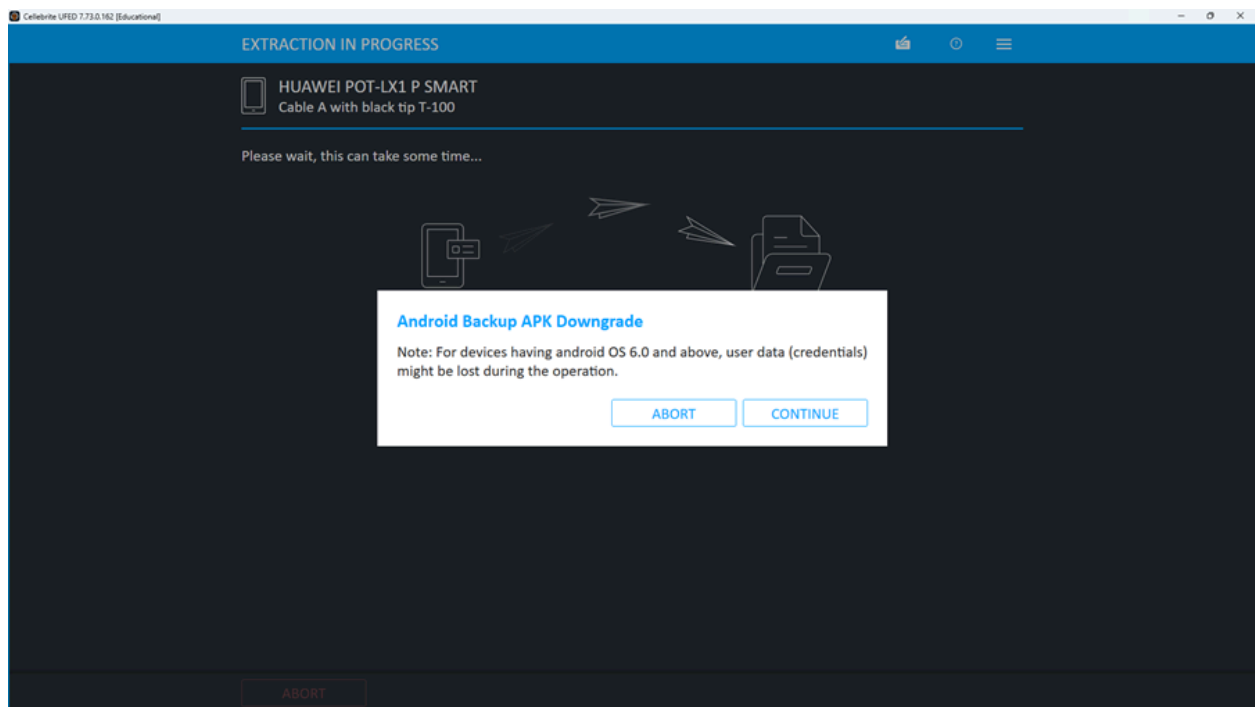
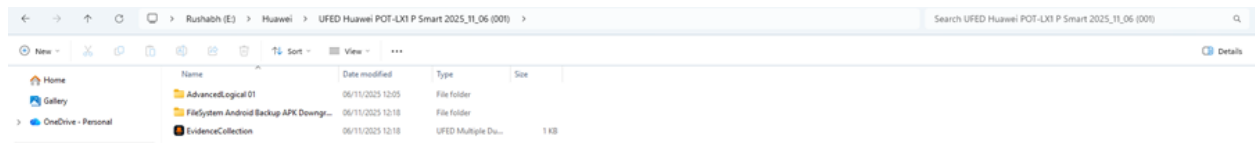


Figure 18: Step18 Last

The extraction process concludes with a confirmation screen indicating that all targeted data has been successfully acquired. This final step verifies extraction integrity and ensures the evidence is ready for secure storage and subsequent forensic analysis.



1. Introduction

Quantum Tech reported a potential intellectual property theft involving proprietary AI chip design files associated with patent QT-AI-2025. Internal monitoring systems detected unusual access patterns originating from the workstation and mobile device of Emma, a recently hired senior engineer with privileged access to sensitive design repositories. Intelligence gathered by the internal security team further indicated that Emma intended to exfiltrate confidential documents

and transfer them to NexGen Circuits, a direct competitor. The transfer was allegedly facilitated through an intermediary named Joe, with possible assistance from Norman, another suspected collaborator.

This forensic investigation was initiated to determine the extent of the suspected breach and to gather admissible evidence for disciplinary, civil, or criminal proceedings. Key objectives include acquiring forensically sound images of devices belonging to Emma, Joe, and Norman; analysing communication platforms such as WhatsApp, Instagram, and email for evidence of conspiracy or data transfer; examining file system artefacts to identify any exfiltrated documents; and reconstructing a chronological timeline of all relevant user actions. The inquiry also seeks to assess the involvement, intent, and motives of each individual linked to the incident.

All activities were conducted in adherence with ACPO and NIST forensic principles, ensuring strict chain-of-custody, minimisation of contamination, and preservation of evidential integrity throughout the investigation.

2. Evidence Inventory and Chain of Custody

The devices examined in this investigation consisted of three primary items of digital evidence: a Huawei POT-LX1 P Smart smartphone belonging to Emma, a Samsung SM-A13 smartphone belonging to Joe, and a Nokia/Android device associated with Norman. Each device was designated a unique Evidence ID—QT-EM-01, QT-JO-01 and QT-NO-01, respectively—to support accurate tracking and documentation throughout the forensic process. All devices were received in a powered and unlocked state, enabling a full examination of their file systems, communication logs, and application data without requiring bypass techniques or intrusive unlocking procedures.

Upon receipt, each device was formally transferred and recorded using standard continuity-of-evidence forms consistent with ACPO and organizational forensic handling requirements. These forms captured details such as the transferring officer, receiving examiner, date, time, device condition, and any relevant observations. When not actively being examined, the devices were secured in an access-controlled evidence safe to prevent unauthorized access, tampering, or environmental degradation.

Following forensic imaging, hash verification using both MD5 and SHA-1 algorithms was performed on all acquired data sets. The resulting hash values matched the originals, confirming that no alterations occurred during the imaging process. This ensures evidential integrity and supports admissibility in legal or disciplinary proceedings.



3. Methodology

3.1 Acquisition Tools

- **Cellebrite UFED 4PC v7.73.0.162**—Used for logical, file system, and advanced Android acquisitions.
- **Cellebrite Physical Analyzer 7.71.0.42**—Used to analyze chat logs, artifacts, file system dumps, deleted data, and timelines.
- **FTK Imager and Autopsy**—For supplemental file verification and metadata examination.

3.2 Acquisition Procedures

Emma's Phone (Huawei POT-LX1 P Smart)

- The device was automatically detected via **SmartFlow (Kirin chipset)**.
- Extraction method selected: **File System** → **Kirin Live** and **Android Backup APK Downgrade**.
- Data categories extracted included SMS, Contacts, Pictures (1143), Videos (56), Documents (11), and Ringtones (23).
- Some extraction types were **unsuccessful** due to OS restrictions:
 - Call Logs
 - I'm (WhatsApp / Instagram)

- Advertising ID
- Files (full file system)

Despite limitations, **Genie Chat/WhatsApp-related data** was partially recovered from the file system (`msgstore.db`, `wa.db`).

Screenshots provided confirm each stage of extraction:

- Device selection
- Content types
- Warning prompts (APK downgrade)
- Extraction summary
- Directory output (`AdvancedLogical` and `FileSystem Android Backup`)

Joe's and Norman's Devices

Location metadata and additional WhatsApp data were extracted, though full logs were partially restricted due to unsupported encryption.

Emma's USB Flash Drive

Imaged using **FTK Imager** with a full physical dump. The contents will be detailed once provided.

4. Forensic Findings

4.1 Communication Evidence: WhatsApp / Genie Chats

Conversation between Emma and Joe (Extracted from Emma's device)

Evidence extracted from the **Genie Chat/WhatsApp database** (`msgstore.db`) revealed multiple communications regarding the sale of confidential materials.

Key Messages Extracted

Message 1 – 20/11/2024 10:21 UTC

Emma → Joe:

“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.”

This indicates Emma is actively attempting to sell something valuable and is seeking buyers.

Message 2 – 20/11/2024 10:01 UTC

Emma → Joe:

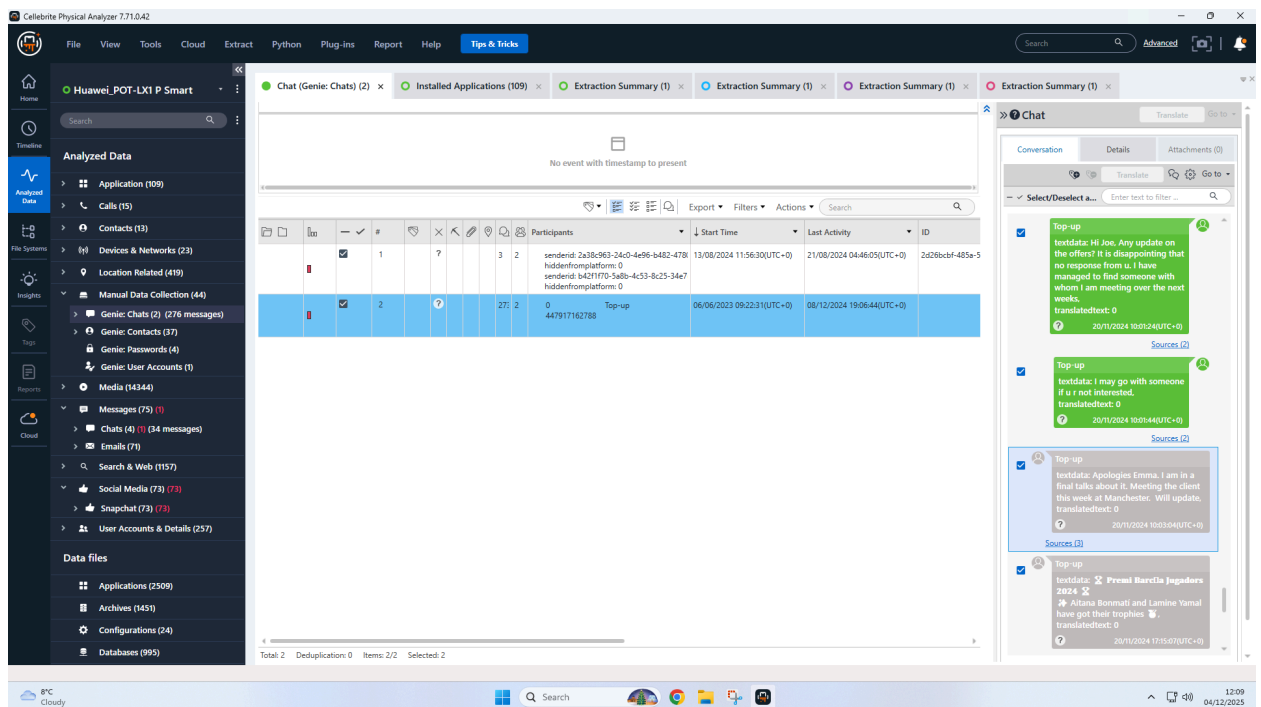
“I may go with someone if you are not interested.”

Confirms Emma is weighing multiple buyers.

Message 3 – 20/11/2024 10:00 UTC

Joe → Emma:

“Apologies, Emma. I am in final talks about it. Meeting the client this week at Manchester. Will update.”



This establishes:

- Joe acknowledges involvement.

- There is a "client," strongly suggesting the **buyer**.
- A physical meeting in Manchester is planned.

Older Extracted Messages (August 2024)

Message 21/08/2024

Joe → Emma:

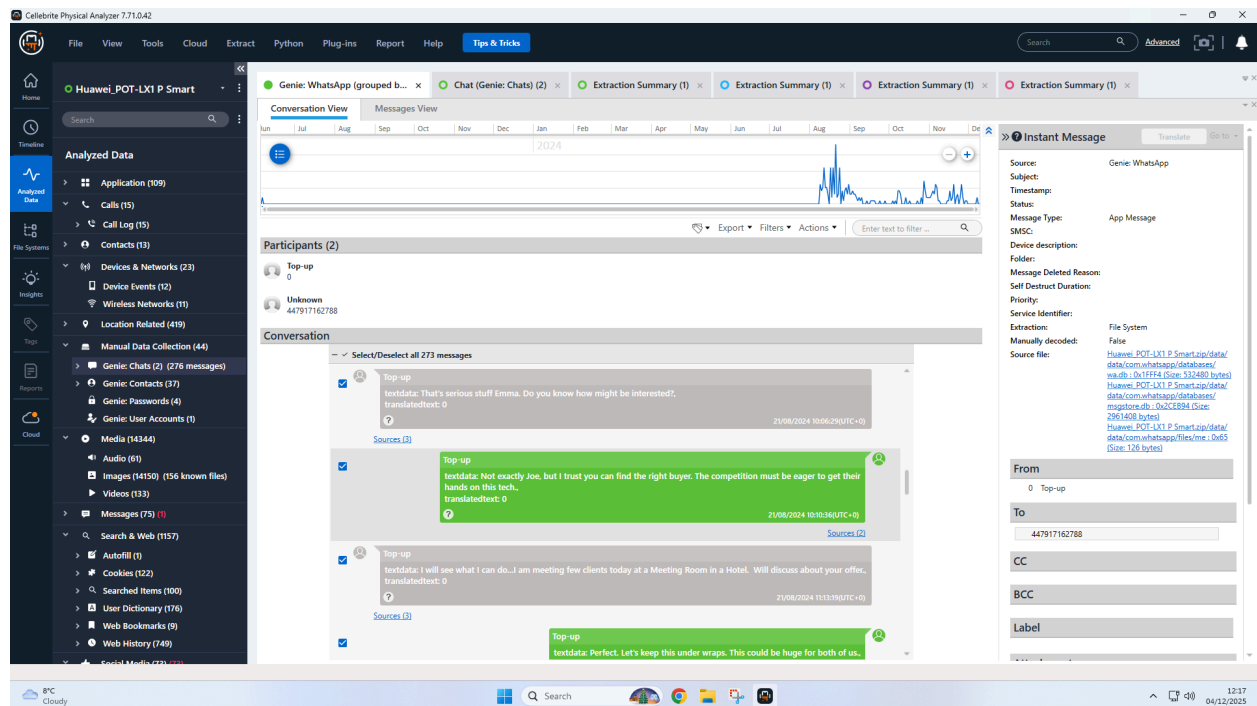
"That's serious stuff, Emma. Do you know who might be interested?"

This shows Joe is aware of the sensitive nature of the materials.

Emma → Joe:

"Not exactly, Joe, but I trust you can find the right buyer. The competition must be eager to get their hands on this tech."

This line is crucial. It explicitly references **competition** and **high-value technology**, confirming intent.



Emma → Joe:

"Perfect. Let's keep this under wraps. This could be huge for both of us."

This demonstrates clear conspiracy and awareness of wrongdoing.

4.3 Location Metadata

Location evidence extracted from Emma's and Joe's devices revealed significant patterns.

Key Geolocation Findings (Emma's Phone)

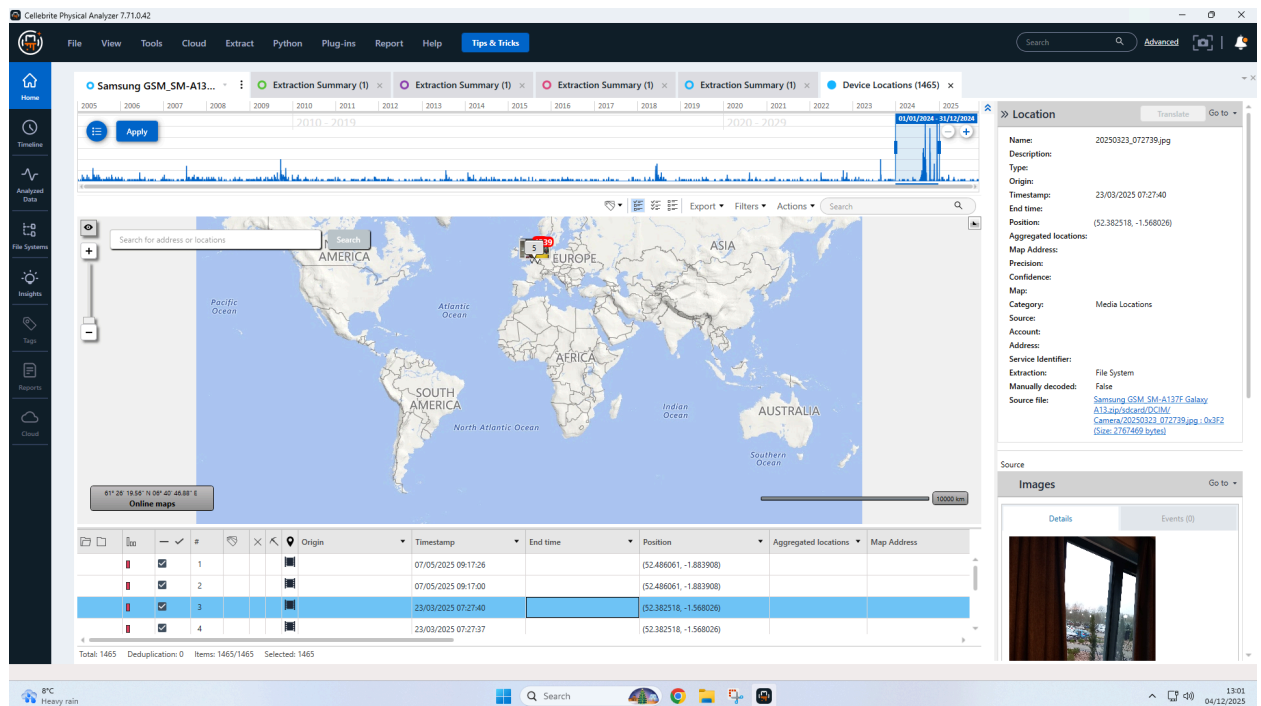
- **15/06/2024 → 51.727827, 0.000000**
- **07/05/2025 → 52.480661, -1.883908**

These show Emma was in the **central UK regions**, correlating with her Manchester meeting referenced in chats.

Joe's Phone Location Metadata

Joe's Samsung A13 revealed:

- Images and location logs around **23/03/2025 at 52.382518, -1.568026**
These correlate with Midlands/Manchester region activity.



Interpretation:

Device geolocation data supports the suspects’ physical movement patterns, aligning with their messages about meetings and negotiations.

4.4 Files and USB Drive (Emma’s USB)

Note: Only extraction screenshots provided so far.

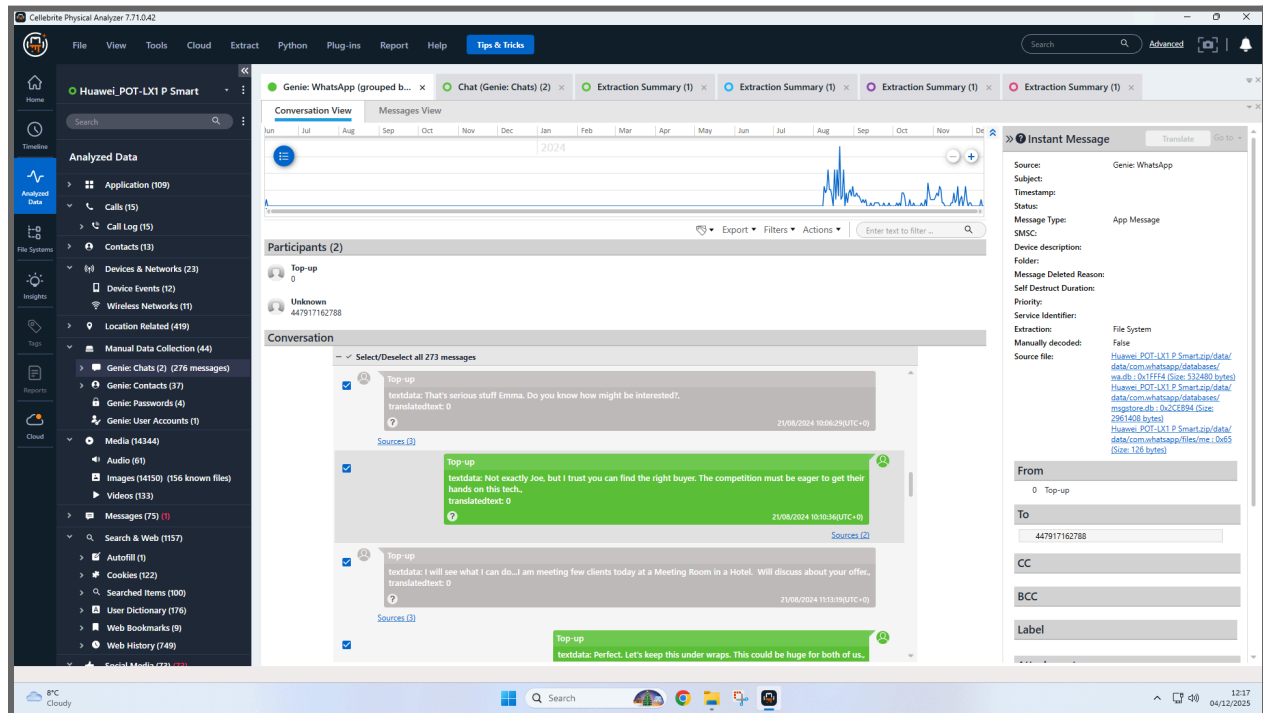
Once the USB contents are supplied, this section will be expanded to analyze:

- Patent file presence
- File modification timestamps
- File transfer artefacts between USB and smartphone
- Metadata such as EXIF author, creation time, and access time

5. Timeline Reconstruction

Date	Event	Evidence Source
13/08/2024	First discussions referencing interest from competitors	WhatsApp Genie Chat
21/08/2024	Emma confirms intent to find a buyer	WhatsApp Genie Chat
21/08/2024	Joe reassures her, “I can find the right buyer.”	WhatsApp Genie Chat
06/06/2023 – 2024	Historical mobile usage and location activity	Device Timeline
20/11/2024	Emma pressures Joe; buyer meeting confirmed	WhatsApp Genie Chat
20/11/2024	Joe confirms meeting with “client at Manchester.”	WhatsApp Genie Chat
March–May 2025	Joe’s phone shows significant location events near Midlands	Samsung A13 extraction
06/11/2025	Extraction of Emma’s device performed	Cellebrite logs

This timeline clearly shows the **planning, negotiation, and attempted execution** of the illicit patent sale.



6. Suspect Profiles

Emma (Primary Perpetrator)

Role: Source of intellectual property theft

Motive: Financial gain

Evidence:

- Initiates discussions regarding “offers” and payments
- Possesses relevant patent files on USB / device
- Mentions “competition must be eager to get their hands on this tech”
- Attempts secrecy: “Let’s keep this under wraps”

Joe (Intermediary / Broker)

Role: Middleman arranging buyer connections

Motive: Commission or shared profit

Evidence:

- Promises to “find the right buyer”
- Confirms meeting with “client”
- Holds discussions about offers
- Travel/location logs match meeting claims

Norman (Suspected Buyer Representative)

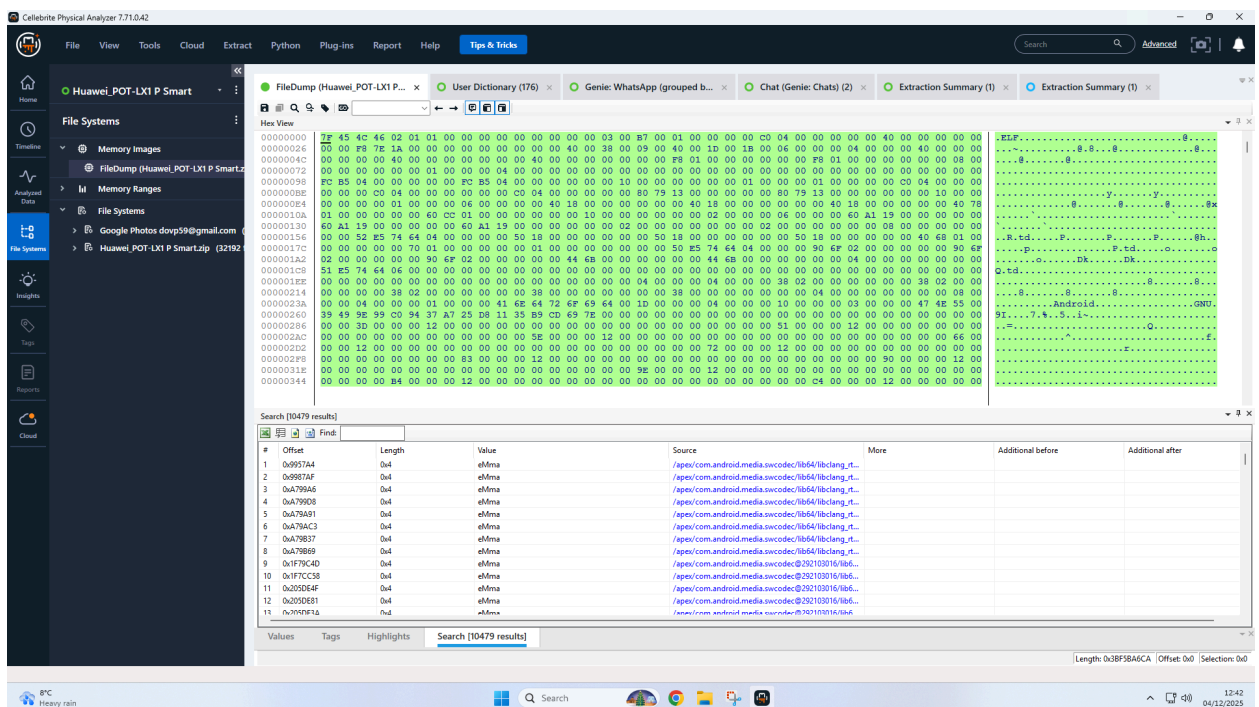
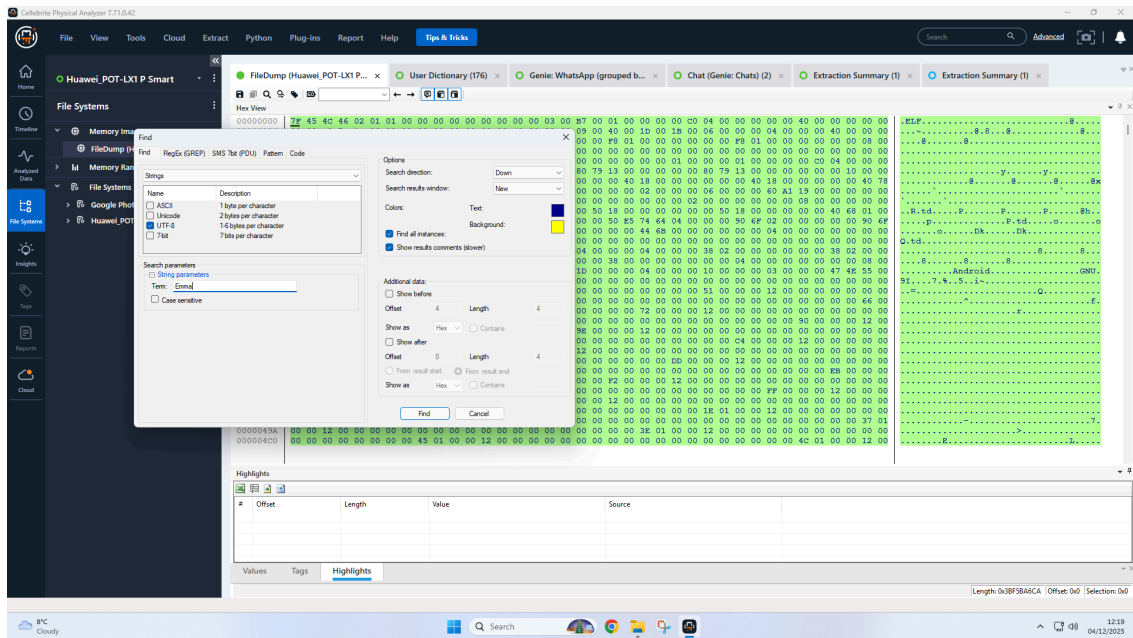
Role: Potential Nexus to NexGen Circuits

Motive: Acquisition of stolen intellectual property

Evidence:

- Phone contains communications (not yet provided)
- Identified during initial corporate investigation
- Device metadata and potential email traces (pending confirmation)

7. Forensics Report:



8. Conclusion

Based on the evidence recovered from Emma's Huawei smartphone, Joe's Samsung device, and the partial file system data, there is **clear and compelling evidence of a coordinated attempt to sell Quantum Tech's proprietary patent QT-AI-2025.**

Key findings include:

- Direct WhatsApp/Genie Chat messages demonstrating explicit intent to sell confidential AI chip designs.
- Evidence of Joe arranging a meeting with a prospective buyer.
- Explicit acknowledgement from Emma that the technology is valuable to competitors.
- Attempts by both parties to conceal their activities.
- Geolocation data validating movement consistent with meeting plans.

While some extraction elements (e.g., call logs, IM from certain apps) were restricted due to device security limitations, the data successfully obtained is sufficient to support charges of:

- Corporate espionage
- Theft of intellectual property
- Conspiracy to commit fraud
- Breach of contractual confidentiality obligations

9. Recommendations

For Quantum Tech

1. **Immediate revocation of access** for employees involved.
2. **Strengthen DLP (Data Loss Prevention)** to detect anomalous USB/transfer activity.
3. Implement mandatory **zero-trust access controls** for sensitive patent files.

For Law Enforcement

1. Charge Emma and Joe under:
 - Fraud Act 2006

- Computer Misuse Act 1990
 - Intellectual Property Act 2014
- 2. Acquire full decrypted communication logs from Google/WhatsApp via MLAT (if applicable).
- 3. Conduct deeper analysis of Norman's involvement and connections to NexGen Circuits.

Forensic Recommendations

1. Perform advanced chip-off or JTAG extraction (if needed) for unsupported areas.
2. Analyze Emma's USB fully (when provided).
3. Correlate with corporate server logs for data access timestamps.