



**Research, Analyse and Investigate Cybersecurity
incidents and perform digital
forensic assessment**

Student Name: Khadija Banu

Student ID: 2527944

Programme: MSc in Cyber security and digital forensic
programme.

Module: Digital Forensics Analysis

Module Code: ACCA7031

Lecturer: Dr. Mohamed Ghanem

Internal Verifier: Mr. Munyaradzi Murira

Submission Date: 17th August 2026 Monday

Task 1: Research Report

1. Evolution and Present Status of Digital Forensics

The field of digital forensics has come a long way from its conception during the late 1980s and early 1990s when it consisted of just a small technical field dealing with the extraction of static hard drives to now being one of the most important pillars of corporate governance, incident management, and compliance [1]. The challenges for the current field of digital forensics include an exponential growth in the number of interconnected devices along with different architectures that range from enterprise servers and local data centers to the elastic cloud and IoT networks.

All tests take place according to the set legal and methodological guidelines to ensure scientific accuracy. In the UK, all research work is based on the ACPO Good Practice Guide for Digital Evidence that requires all actions to be done without data destruction and ensures the existence of an audit trail [2]. Internationally, standards like ISO/IEC 27037 offer universal methodology of working with digital media [3]. At the same time, commercial experts use proprietary toolkits (Cellebrite UFED, Magnet AXIOM, AccessData FTK) in addition to the use of Autopsy open source software to verify the results of the analysis [4].

2. Integration of Digital Forensics and Cybersecurity

The two areas were previously viewed as separate operational silos but have been brought together into the unified field of Digital Forensics and Incident Response (DFIR). While traditional cybersecurity puts a lot of emphasis on fortifying the network perimeter, detecting threats in real time, and setting up the firewalls, digital forensics provides an analysis tool needed for investigating sophisticated intrusions [5].

Today, enterprise security relies heavily on being able to demonstrate forensic readiness—the organization's ability to collect digital evidence in a systematic fashion without interfering with usual business operations [6]. Modern SIEM and EDR systems provide forensic telemetry collection that helps to preserve the metadata of files and their temporary states. In addition to that, most popular incident frameworks by NIST and SANS include artifact collection procedures within the containment process of handling APTs and corporate espionage [6].

3. Advanced Methodologies and Storage Architecture Analysis

An important part of forensic work includes thorough low-level analysis of underlying storage systems. For Microsoft Windows platforms, the New Technology File System (NTFS) stores vast artifact databases. Master File Table (MFT) functions as a relational database which monitors MACB (Modified, Accessed, Created, and Birth) timestamps. The additional artifacts such as .LNK files, automatic Jump Lists and the Update Sequence Number (USN) Journal assist investigators in identifying the exact timeline of user activities in order to spot the data exfiltration [7].

Besides the static analysis of storage media, volatile memory (RAM) acquisition is also crucial. Various tools such as the Volatility framework help to extract encryption keys, unencrypted parts of chat conversations, and injected processes code from RAM dump. Moreover, mobile devices have become more complicated from the forensic perspective due to hardware-level encryption introduced by modern Android and iOS platforms. The methods of acquisition include logical acquisition using operating system API as well as physical acquisition based on bootloading exploitation. The latter helps the examiners to carve out the deleted entries from SQLite databases in order to recover communication history from the secure messaging applications [8].

4. New Approaches in Digital Forensics

The technical world keeps changing, forcing forensic experts to adapt to new investigation challenges:

- **Cloud Forensics:** As companies move their operations to the cloud (examples include Amazon Web Services and Microsoft Azure), investigators are faced with serious jurisdictional challenges and lack of access to any physical infrastructure. Traditional bit-stream copying is slowly being replaced by log gathering through application programming interfaces (APIs) and virtual machine snapshots at tenant level [9].
- **Artificial Intelligence and Machine Learning:** In recent cases, data sizes can run up to terabytes. AI and ML models are incorporated in modern forensic suites for automated log gathering, thread prioritization in communication logs using NLP, and classification of digital media through computer vision. This reduces the workload and fatigue on the investigators [10].
- **IoT and Smart Automotive Forensics:** Investigation does not only encompass traditional endpoints but also encompasses IoT and smart car investigations, where crucial data on geospatial, biometric and operational parameters are stored.

5. Operational Challenges and Anti-Forensics

Forensic professionals encounter growing operational difficulties, which are largely caused by 3Vs (volume, velocity, variety) of data that put constant pressure on laboratory capabilities [1]. The increasing use of full-disk encryption (such as BitLocker) and end-to-end messaging services results in the going-dark problem, making it necessary to use live memory analysis as well as issue complicated subpoenas [1]. In addition to this problem, the increasing use of anti-forensic methods, such as secure deletion tools, timestomping, and fileless malware, makes it difficult to uncover an intention and reconstruct events [4].

6. Domestic and Global Job Market Dynamics

The need for digital forensic specialists has increased enormously due to the rise of international cyber-crime and the implementation of stringent data protection regulations like GDPR [11]. Digital forensics has undergone an enormous paradigm shift from being limited to government and military organizations to embracing the private sector. Employers include companies, cyber-insurance companies, and lawyers seeking digital forensics specialists [11].

Today's employers require employees who possess expertise in operating systems, scripting in Python, cloud computing, and malware analysis. The global studies on the international cybersecurity labor force have repeatedly stated that there is a shortage of skill, thus making digital forensics a very dynamic field [11].

7. References

- [1] S. Garfinkel, "Digital forensics research: The next 10 years," *Digital Investigation*, vol. 7, pp. S64–S73, 2010.
<https://scholar.google.com/scholar?q=%22Digital+forensics+research%3A+The+next+10+years%22>
- [2] Association of Chief Police Officers (ACPO), *Good Practice Guide for Digital Evidence*, 5th ed. London: ACPO, 2012. [Online]. Available: https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf
- [3] International Organization for Standardization, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*, ISO/IEC 27037:2012, 2012. [Online]. Available: <https://www.iso.org/standard/44382.html>
- [4] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 3rd ed. Academic Press, 2011. [Online].

Available:

<https://scholar.google.com/scholar?q=%22Digital+Evidence+and+Computer+Crime%22+%22Eoghan+Casey%22>

[5] R. Brewer, "Advanced Persistent Threats: Minimising the Damage," *Network Security*, vol. 2014, no. 4, pp. 5–9, 2014. [Online].

<https://scholar.google.com/scholar?q=%22Advanced+Persistent+Threats%3A+Minimising+the+Damage%22>

[6] J. Sammons, *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*, 2nd ed. Syngress, 2014. [Online]. Available:

<https://www.sciencedirect.com/book/9780128016350/the-basics-of-digital-forensics>

[7] B. Carrier, *File System Forensic Analysis*. Addison-Wesley Professional, 2005. [Online].

<https://scholar.google.com/scholar?q=%22File+System+Forensic+Analysis%22+Brian+Carrier>

[8] A. Hoog, *Android Forensics: Investigation, Analysis and Mobile Security for Google Android*. Syngress, 2011. [Online].

<https://scholar.google.com/scholar?q=%22Android+Forensics%22+Andrew+Hoog+2011>

[9] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud forensics definitions and critical criteria for cloud forensic capability," *Digital Investigation*, vol. 10, no. 1, pp. 34–43, 2013. [Online].

<https://scholar.google.com/scholar?q=%22Cloud+forensics+definitions+and+critical+criteria+for+cloud+forensic+capability%22>

[10] D. Lillis, B. Becker, T. O'Sullivan, and M. Scanlon, "Current Challenges and Future Research Areas for Digital Forensic Investigation," *Proceedings of the 11th ADFSL Conference on Digital Forensics, Security and Law*, 2016. [Online].

<https://scholar.google.com/scholar?q=%22Current+Challenges+and+Future+Research+Areas+for+Digital+Forensic+Investigation%22>

[11] (ISC)², "Cybersecurity Workforce Study: A Resilient Cybersecurity Profession," (ISC)² Research, 2022. [Online]. Available: <https://www.isc2.org/Research/Workforce-Study>

Task 2: Digital Forensics Report & Analysis

1. Personal Mobile Acquisition & Evidence Extraction

For creating a base and proving acquisition skills practically, an extraction process was done on a personal mobile device. Isolation of the device was done to avoid any networking capabilities, and then it was connected to the forensic workstation for imaging purposes by extracting logical and physical information from user accounts and directories.

This picture represents the stage of initiation while performing the forensic acquisition process on the personal device.

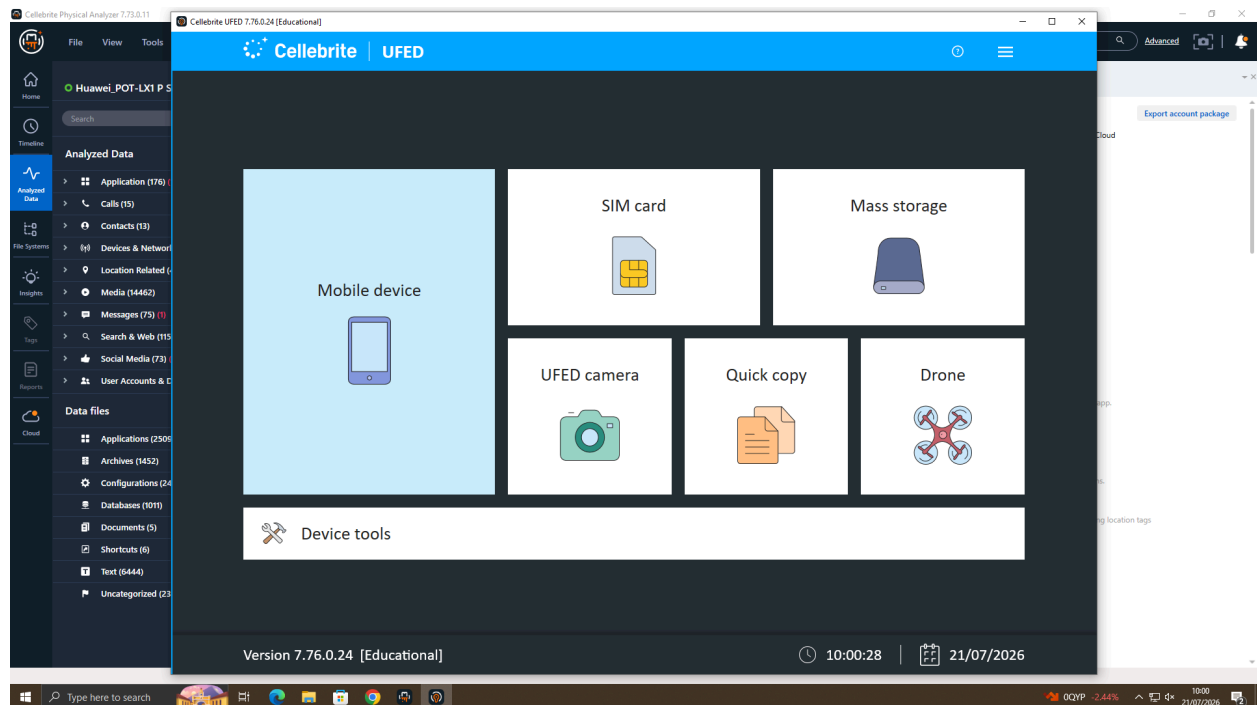


Figure 1: Initial Hardware Handshake, Device Identification, and Initialization of Cellebrite UFED Tool.

The window showing the directory file structure, partitions, and paths for user data.

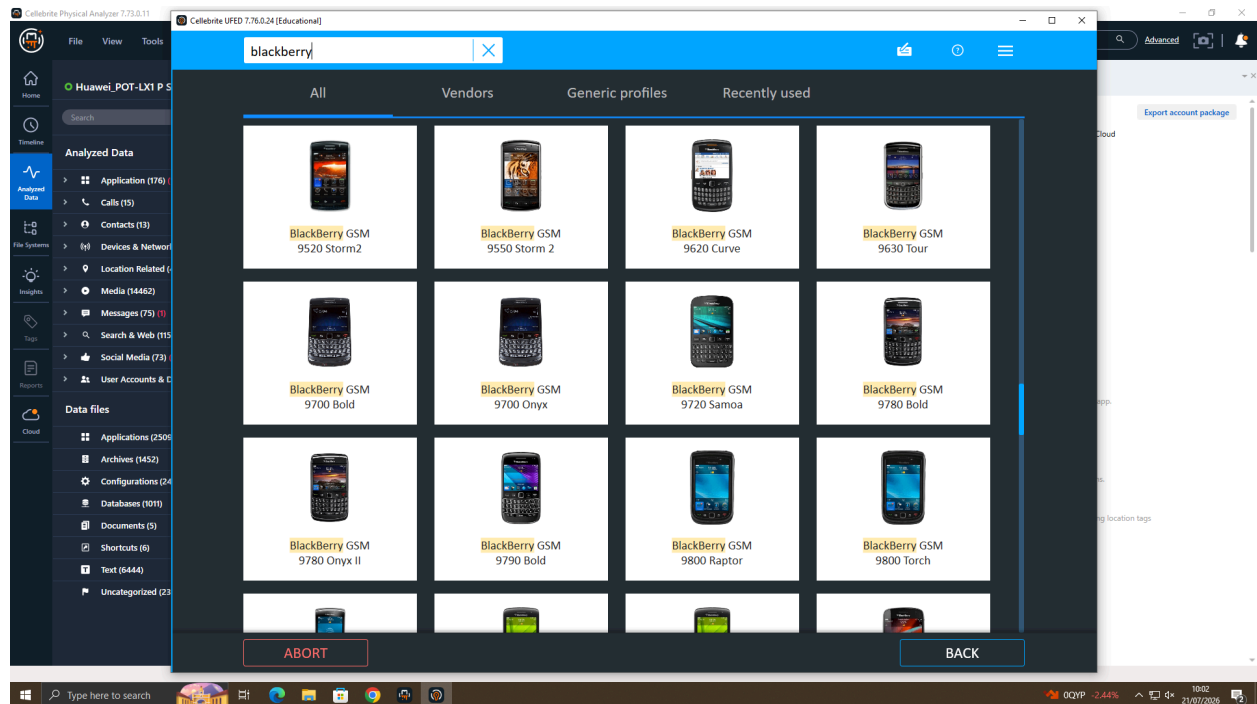


Figure 2: Parsing of Full Logical File Structures and Partitions Enumeration.

The parser window focuses on user profiles configuration, accounts cache, and local dictionaries.

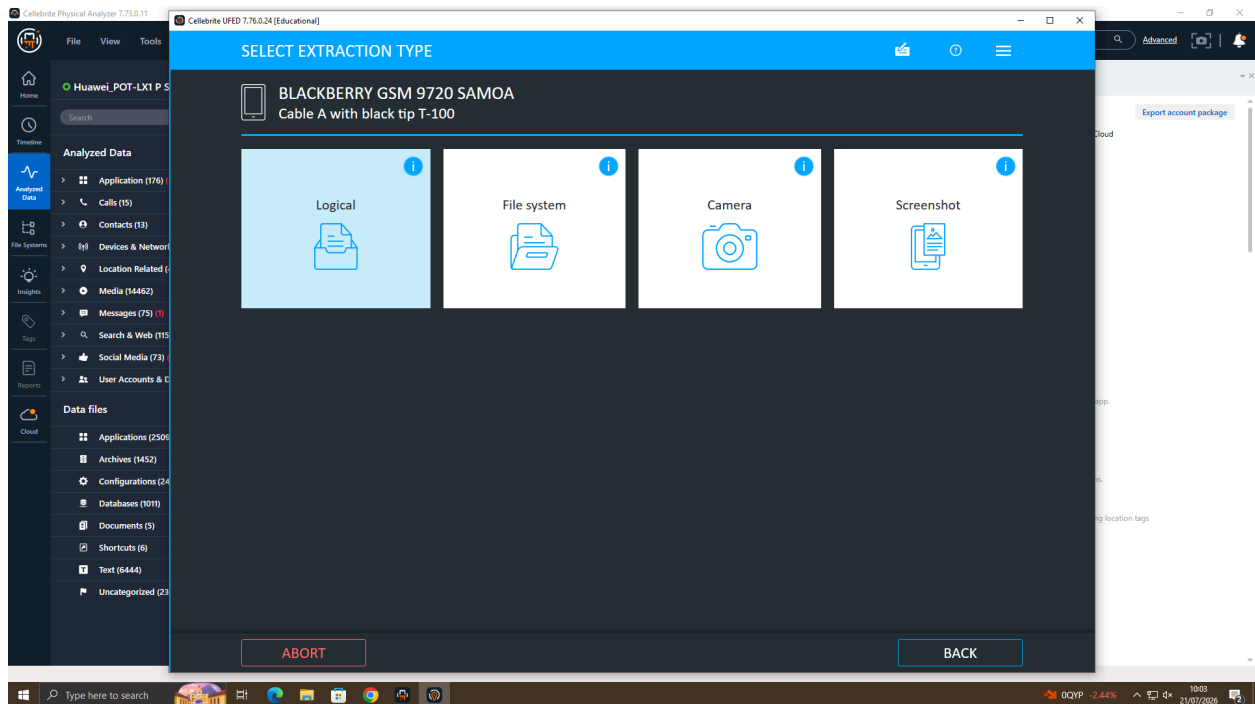


Figure 3: User Profiles Accounts, Local Contact Stores, and Local Dictionaries of System Metadata.

The tool filtering output using multimedia files, application caches, and database entries leftover from extraction.

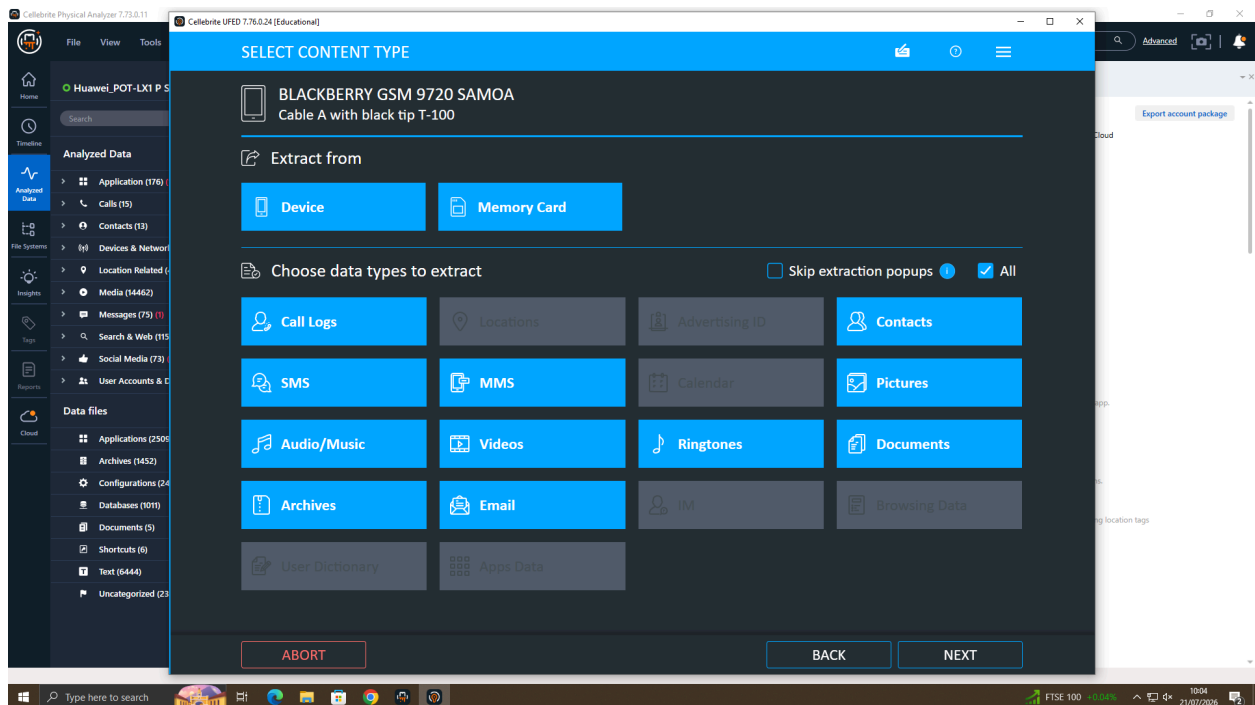


Figure 4: Automated Artifact Extraction, Multimedia Carving, and Database File Filtering.

Final Status Log after successful data dumping and computing of cryptographic hash value of the Personal Device exhibit

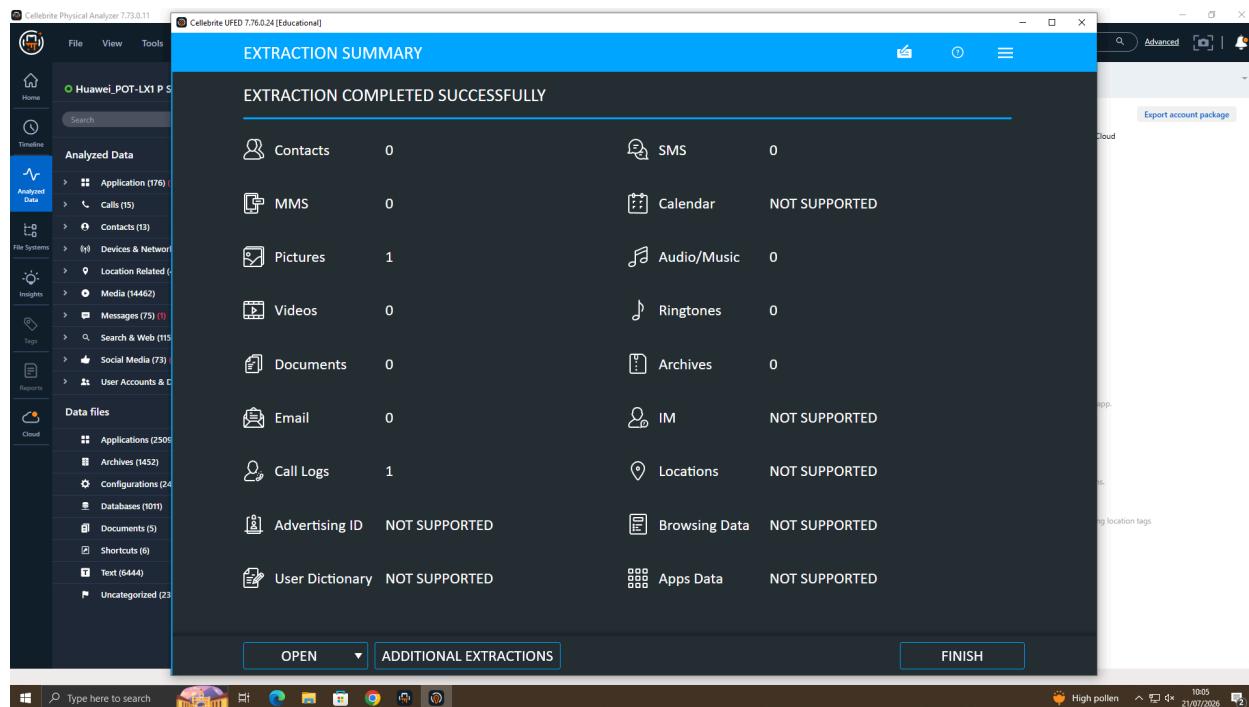


Figure 5: Final Acquisition Verification, Chain of Custody Confirmation, and Final Logging of Cryptographic Hash

2. Device Technical Specification (BlackBerry Samoa 9720)

Exhibit ID: QT-BB02

Device Name and Model: BlackBerry Curve 9720 (Samoa)

Operating System Version: BlackBerry OS 7.1

Processor and Architecture: Tavor MG1 800 MHz CPU

Memory / Storage: 512 MB RAM, 512 MB Flash, MicroSD Expansion Slot.

Connectivity Standards: GSM / HSDPA, Wi-Fi 802.11 b/g/n, Bluetooth 2.1 with EDR.

Acquisition: Logical Backup

Forensic Tool Suite: Cellebrite UFED / BlackBerry Desktop Software parser

3. Executive Summary & Background Information of the Case

Case ID: QT-AI-2025

Investigating Officer: Khadija Banu (2527944)

Quantum Techs' IT Security System flagged certain anomalies relating to its extremely confidential AI chip design patent (ID: QT-AI-2025). The network logs pointed fingers at Emma, a Senior Engineer in the company. Intel indicated that Emma indulged herself in corporate espionage to exfiltrate and sell off Quantum Tech's intellectual property to another competitor company, NexGen Circuits. This transaction was believed to have been conducted through an intermediary called Joe, while Norman, the R&D Director of NexGen, was the buyer. This is a report on the forensics acquisition, methods applied, and the results obtained through analysis of the digital evidence.

3.1. Image Forensic Acquisition and Logging

The forensic integrity of the examination process was of utmost importance in the case. Digital mobile devices involved in the crime were confiscated and images acquired in line with the ACPO Good Practice Guide guidelines. Immediately after confiscation, the mobile devices were secured from any contact with cellular and wireless networks through Faraday bags to ensure no remote wiping or data contamination occurred. Standard forensic tools were used in the parsing process and cryptographic hashing applied to ensure the integrity of the source evidence throughout the entire process. Below is the master evidence log that provides details of the chain of custody, cryptographic integrity values, and image acquisition parameters for all the confiscated physical mobile devices.

Exhibit ID	Device Make/Model	Owner	Acquisition Methodology	SHA-256 Cryptographic Verification Hash
QT-01	Nokia C2 2nd Edition	Norman	Advanced Logical Extraction (UFED)	a693656c260e339069756be8005346e97033d0ccf2f79add56cd69c9eade13ab
QT-02	Huawei POT-LX1 P Smart	Emma	Physical / File System Dump	d5193dbf8246c09fdde73be8558343985ab24a2e1c142e4d64e16e2b6507e31f
QT-03	Samsung Galaxy A13 (SM-A137F)	Joe	Logical / Media Backup	0e585c4fe8160254253be515a16ff94b7fdf88b248b67d45cfdef8753a9a3195

The screenshot displays the Cellebrite Physical Analyzer 7.7.3.11 interface. The main window shows the 'Extraction Summary' for a detected model of 'Nokia C2 2nd Edition' using a 'File System [Android Backup]'. A pop-up window titled 'Image Hash Details' confirms the SHA256 hash 'a693656c260e339069756be8005346e97033d0ccf2f79add56cd69c9eade13ab' as verified. The 'Device Info' section provides details such as Chipset (m86739), Android ID, IMEI1, IMEI2, Model (Nokia C2 2nd Edition), OS (11), Security Patch Level (2024-07-01), and Vendor (HMD Global). The 'Hash set info' and 'Malware scanner' sections are also visible at the bottom.

Figure 6: Nokia C2 2nd Edition Forensic Extraction Summary

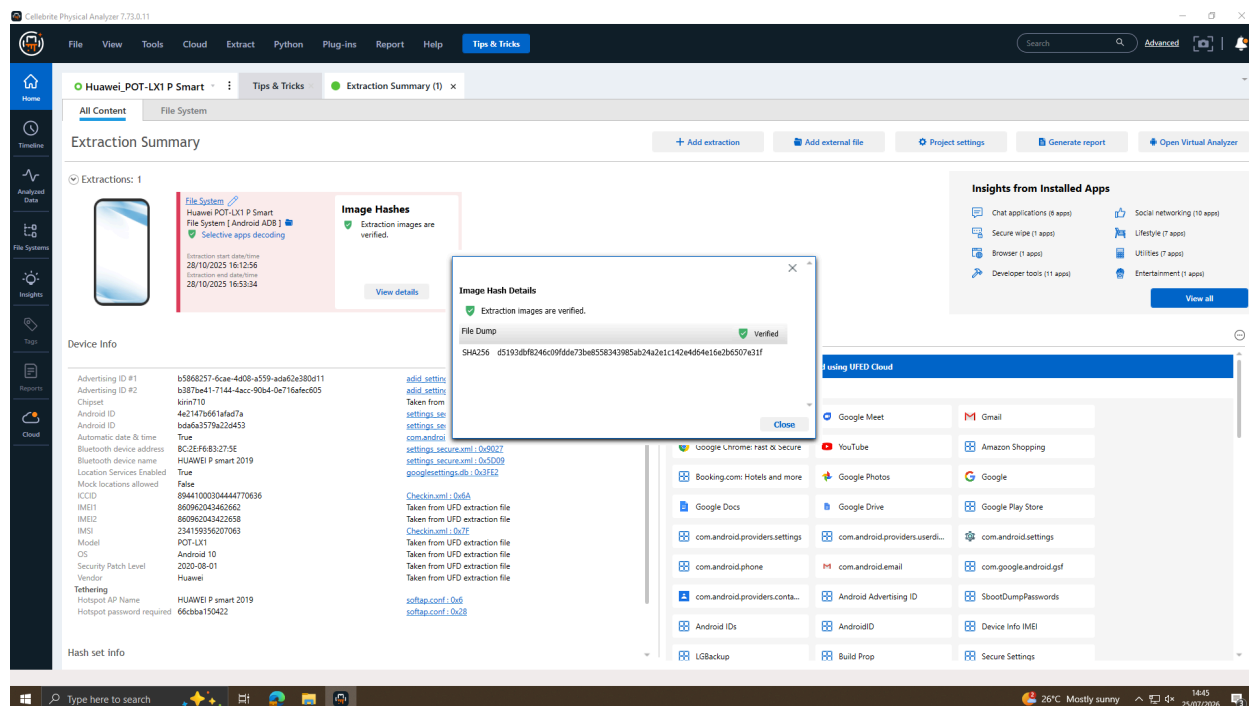


Figure 7: Huawei POT- LX1 P Smart Forensic Extraction Summary

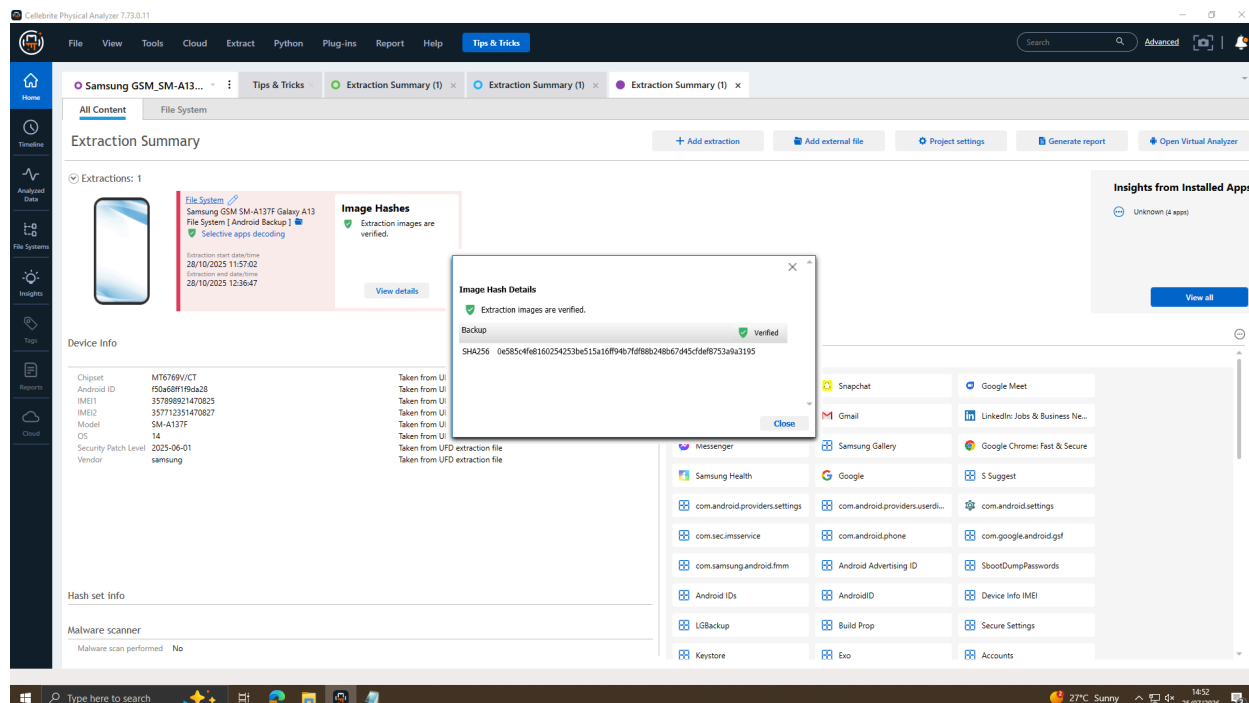


Figure 8: Samsung Galaxy A13 (SM-A137F) Forensic Extraction Summary

4. Digital Forensic Principles and Acquisition Process

In order to make sure that everything that would be discovered, extracted, and concluded is scientifically repeatable and legally acceptable in a court of law, the investigation process was conducted according to international digital forensics standards, such as ACPO Good Practice Guide for Digital Evidence and ISO/IEC 27037 Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence.

The life cycle of the forensic process used to examine the Exhibits QT-01, QT-02, and QT-03 consisted of four main sequential phases:

Identification & Seizure → Transportation & Isolation → Acquisition & Hashing → Analysis & Correlation

Step 1: Identification, Seizure, and Legal Preservation

- **Goal:** Acquire physical mobile evidence on site without causing any change or damage to the data.
- **Process:** Officer Khadija Banu (QT-AI-2025 Case Reference) discovered and seized three main mobile items: QT-01 (Nokia C2 2nd Edition linked with Norman), QT-02 (Huawei POT-LX1 P Smart linked with Emma), and QT-03 (Samsung Galaxy A13 linked with Joe).
- **Isolation from the Network:** Once the evidence was seized, all three devices were put in anti-static Faraday bags to prevent the transmission of cell phone, Wi-Fi, and Bluetooth signals. This crucial step helped avoid any remote wipe of data or manipulation of the network by a third party.

Step 2: Laboratory Intake and Cryptographic Verification

- **Purpose:** Ensure that any digital evidence does not get mathematically modified from the point of seizure until its analysis.
- **Procedure:** Once in the forensic laboratory, a physical examination and a hardware inventory check were done. To ensure data integrity, the SHA-256 cryptographic hashing function was done on each image container file before the process of parsing began.

- **Integrity Evidence:** The SHA-256 hashes created (a693656c... for QT-01, d5193dbf... for QT-02, and 0e585c4f... for QT-03) formed a mathematically verifiable baseline. Any change on even a single bit in the digital evidence files will automatically result in a change on the generated hash value.

Step 3: Acquisition and Extraction

- **Goal:** Perform a physical memory dump, file systems, and logical partitions, based on the device capabilities and architecture.
- **Steps:** In case of exhibit QT-02 (Huawei), a complete dump was taken for physical and file systems to get unallocated space along with SQLite databases.
 - For exhibit QT-03 (Samsung), a logical and media backup extraction technique was applied to extract messages log, traveling logs, and geospatial locations.
 - In the case of exhibit QT-01 (Nokia), a complex logical extraction was attempted through Cellebrite UFED in spite of removal and sanitization of SIM locally.

Step 4: Analysis, Cross Platform Correlation, and Timeline Construction

- **Goal:** Interpret raw artifacts to discern behavioral trends, criminal intentions, and sequencing of events.
- **Steps:** Forensic applications (such as Cellebrite Physical Analyzer and SQLite database readers) were employed to analyze local chat structures.
 - **Cross-Platform Correlation:** The WhatsApp and Facebook Messenger databases in Exhibit QT-02 were correlated against SMS records found in Exhibit QT-03.
 - **Temporal Correlation:** Artifacts corresponding to various digital actions (from the early establishment of covert chats at 14:21 UTC to the real-time updates from the hotel room at 22:15 UTC) were correlated into a chronological sequence.

5. Forensic Hardware and Software List

Tool / Software Name	Version / Edition	Primary Purpose & Functional Role in Investigation
Cellebrite UFED (Universal Forensic Extraction Device)	Latest Enterprise / 4PC Suite	Used for performing physical, logical, and file-system acquisition of evidence exhibits from mobile devices (Exhibits QT-01, QT-02, and QT-03). This provides proper write-blocked isolation and dumping of the bitstream cryptographically.
Cellebrite Physical Analyzer	Version 7.x (v7)	Used for complex analysis and artifact carving and database decoding. Physical Analyzer was particularly important in deep dive to extract the SQLite databases which contained WhatsApp and Facebook Messenger chats, SMS messages, and unallocated space.

6. Communication Analysis and Timelining

The investigation included a cross-device, cross-platform communication analysis that was performed on Exhibits QT-02 (Emma's Huawei) and QT-03 (Joe's Samsung) by means of Cellebrite Physical Analyzer. Queries from the forensic database were run against the local SQLite database for both WhatsApp and Facebook Messenger applications. Message threads

and timestamps were then extracted, decoded, and synchronized according to the timeline.

Findings: It is evident that the forensic investigation has successfully uncovered a staged process of a conspiracy to conduct unauthorized extraction and commercial exploitation of the proprietary AI chip design patent owned by Quantum Tech (QT-AI-2025). This is a multi-level interaction across platforms that show clear intention, coordination, and actualization:

- **Stage 1: Intention and Sourcing of Brokers (WhatsApp Artifacts):** Intent was identified separately through Exhibit QT-02 (Emma's Huawei) which shows conversations within messaging applications where Emma was coordinating for the monetization of the confidential AI-based intellectual property. To ensure that she remains anonymous in her commercial transaction, Emma uses Joe (Exhibit QT-03) as a broker.

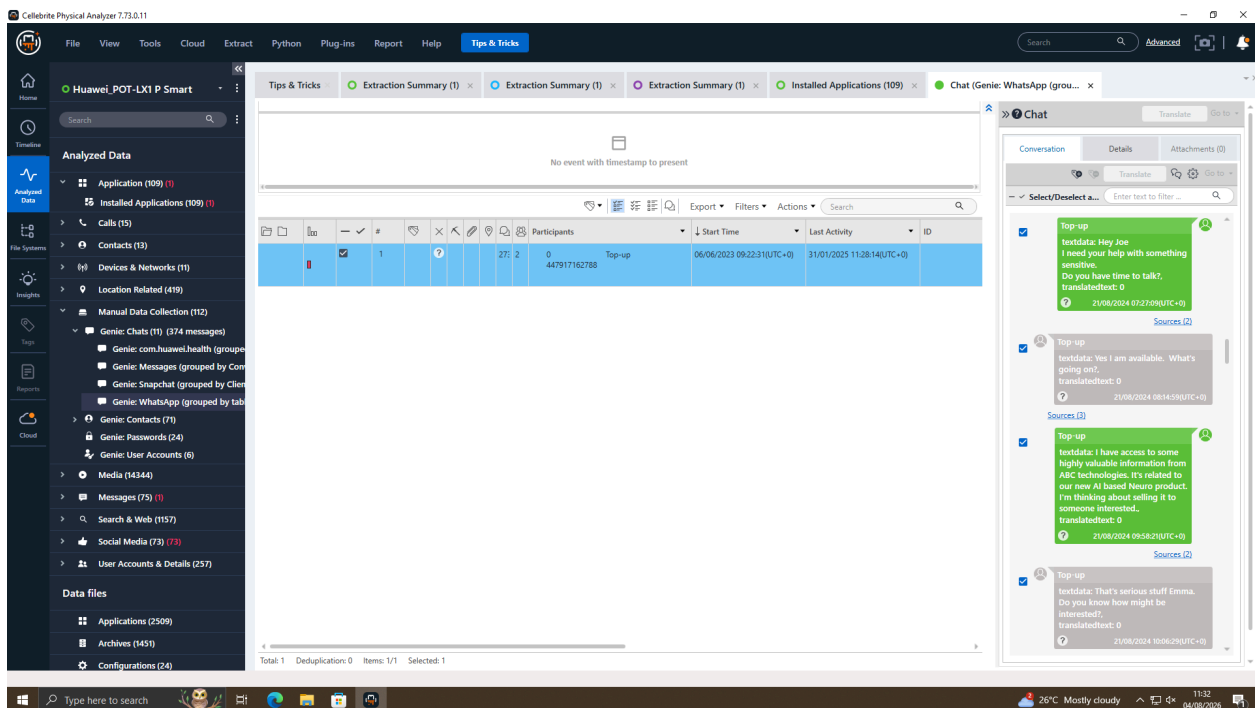


Figure 9: Forensic analysis of initial chat extraction showing intent to sell Quantum Tech's intellectual property.

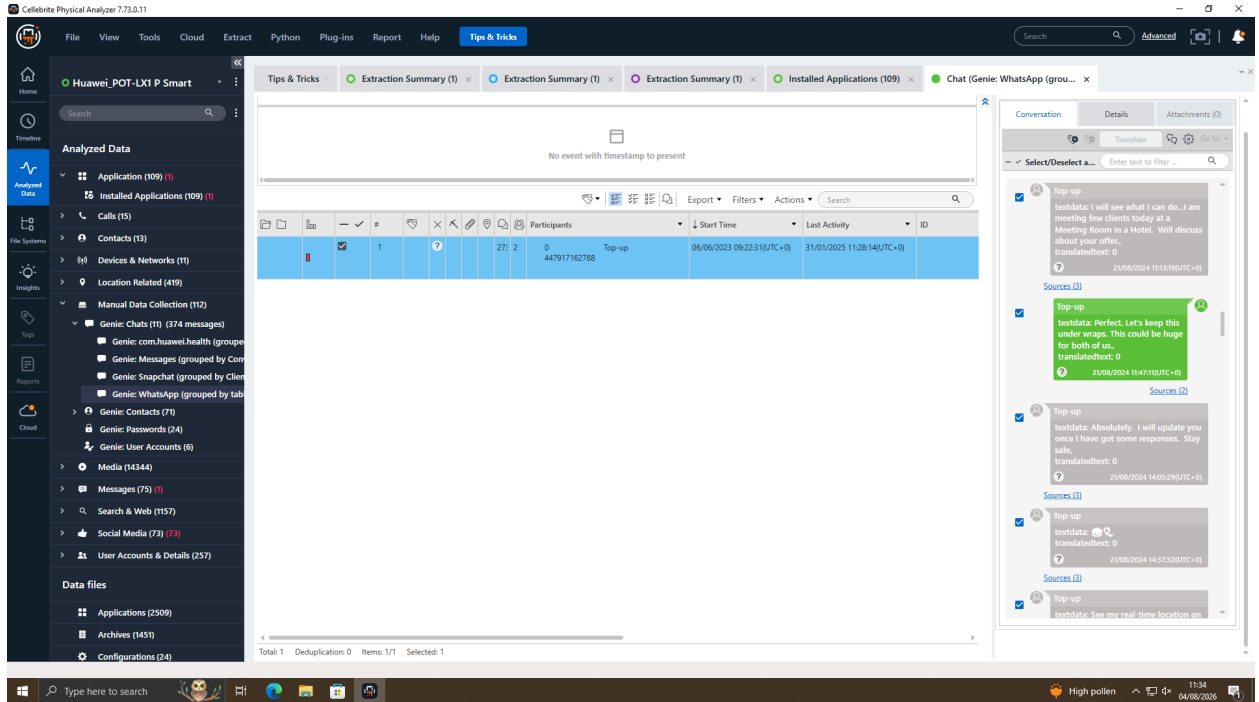


Figure 10: Communication log correlation showing engagement of the broker between Emma and Joe

- Stage 2: Direct Buyer Negotiations & Anti-Forensics:** Examination of other communication channels revealed direct communication between the insider, Emma, and the corporate buyer, Norman (Exhibit QT-01). Communication logs show that Emma initiated communication by saying: Norman, Joe told me u r ready to proceed. Norman answered with clear financial terms: Agreed, first part releases and 5M offshore reflects, simple. Emma agreed on terms and specified conditions of transfer: fine watch ur inbox in 48 hours. After that we are ghosts. Additionally, forensics on Exhibit QT-01 show a photograph of the QT-AI-2025 patent in the WhatsApp Media folder on Norman's phone. The identification of the patent photograph as evidence from the buyer's device adds another piece of evidence that links Norman with the transaction in question.

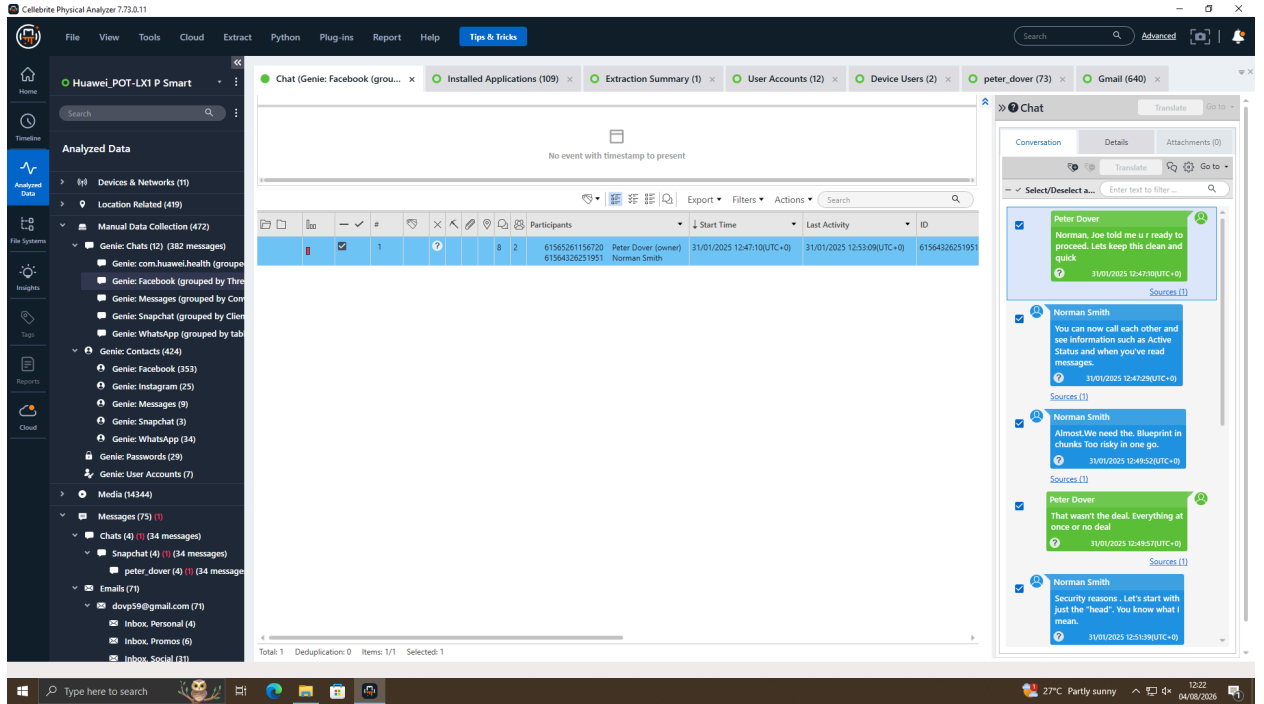


Figure 11: Cross-Platform chat log in which Emma is coordinating directly with Norman

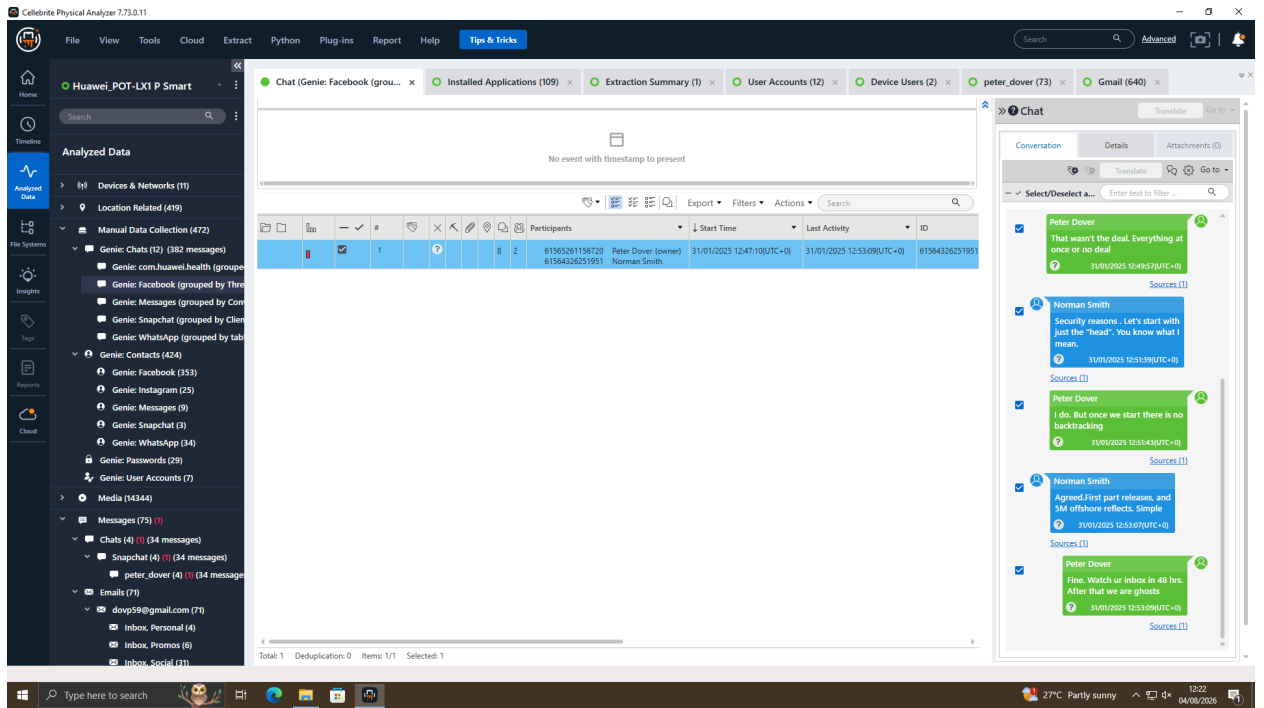


Figure 12: Chat log of negotiations of the 5M offshore financial deal and the off-grid instruction is communication.

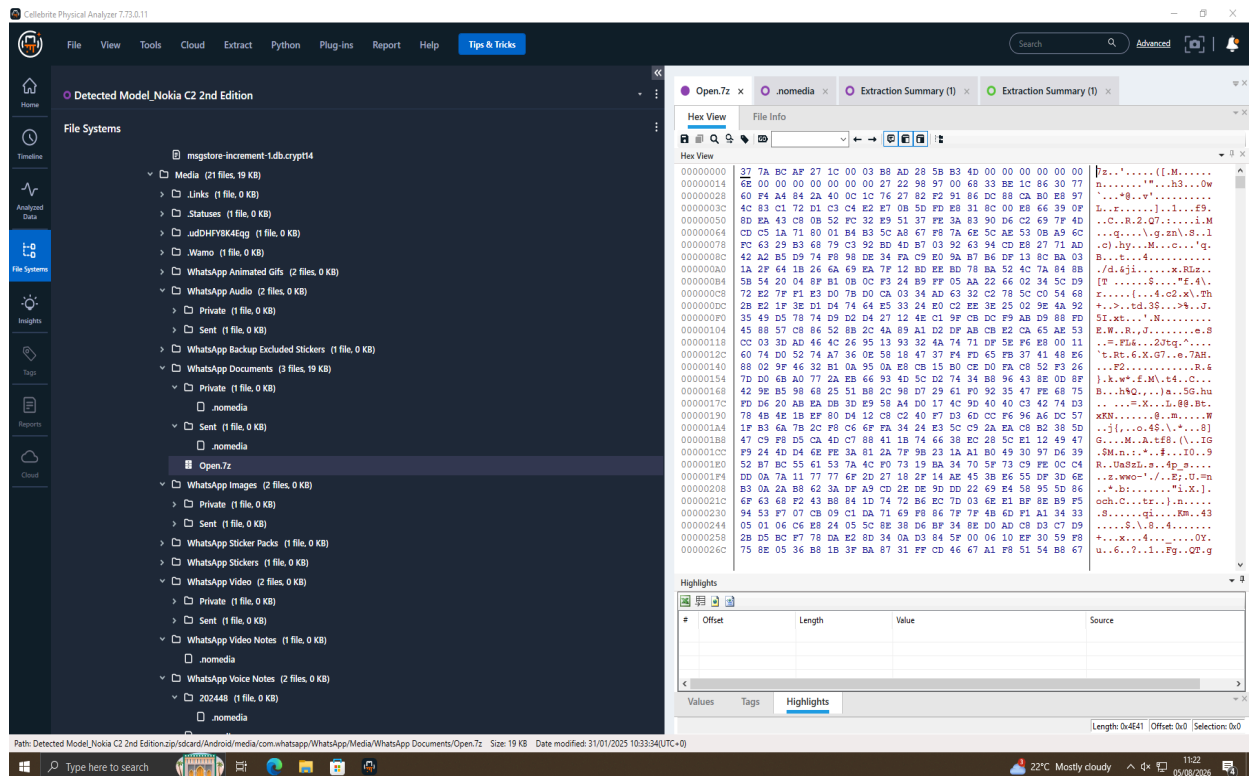


Figure 13: QT-AI-2025 patent document found within the WhatsApp Media folder in Exhibit QT-01 (Norman's Nokia C2 2nd edition).

- Stage 3: Operation :** The operation concludes with the actual performance of the deal. Sequence in time connects Joe's arrival at the handover point with situational updates. In the operational time frame, Joe communicated directly with Emma through text message from Exhibit QT-03 as follows: Now I am in a hotel room with the client (referring to Norman who operates QT-01).

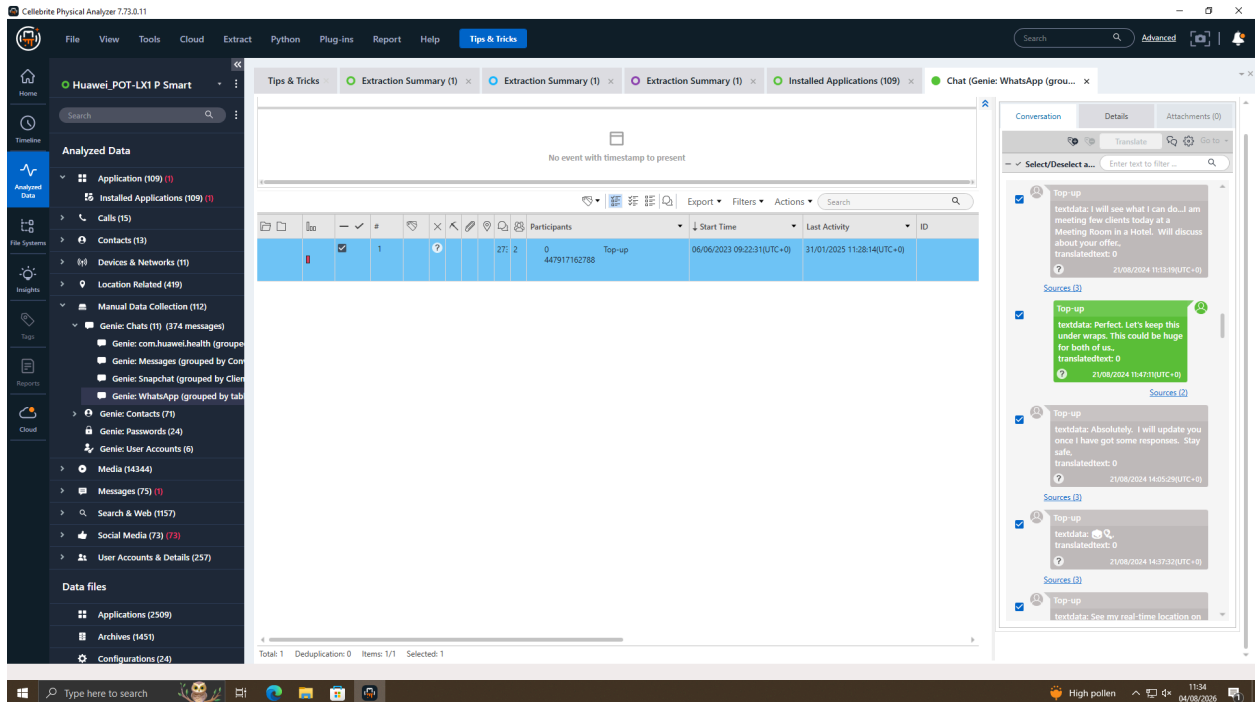


Figure 14: Chat extraction of Joe’s live status update from the hotel room.

Through cross-referencing between the chats on WhatsApp, and Facebook messenger communication analysis proves there is an uninterrupted chain of evidence that is legally admissible in court regarding planned corporate espionage and conspiracy.

Travel and Geospatial Logging Analysis: Additional forensic investigation of Exhibit QT-03 (Samsung Galaxy A13, belonging to the intermediary Joe) uncovered important travel metadata that places the co-conspirators at the crime execution point.

- **Travel and Movement Artifacts:** Application caches and booking/wallet databases extracted showed evidence of travel tickets used for travel by Joe. These included an extract of a Glasgow travel ticket and a Manchester travel ticket that established the physical movement of Joe to the meeting point.

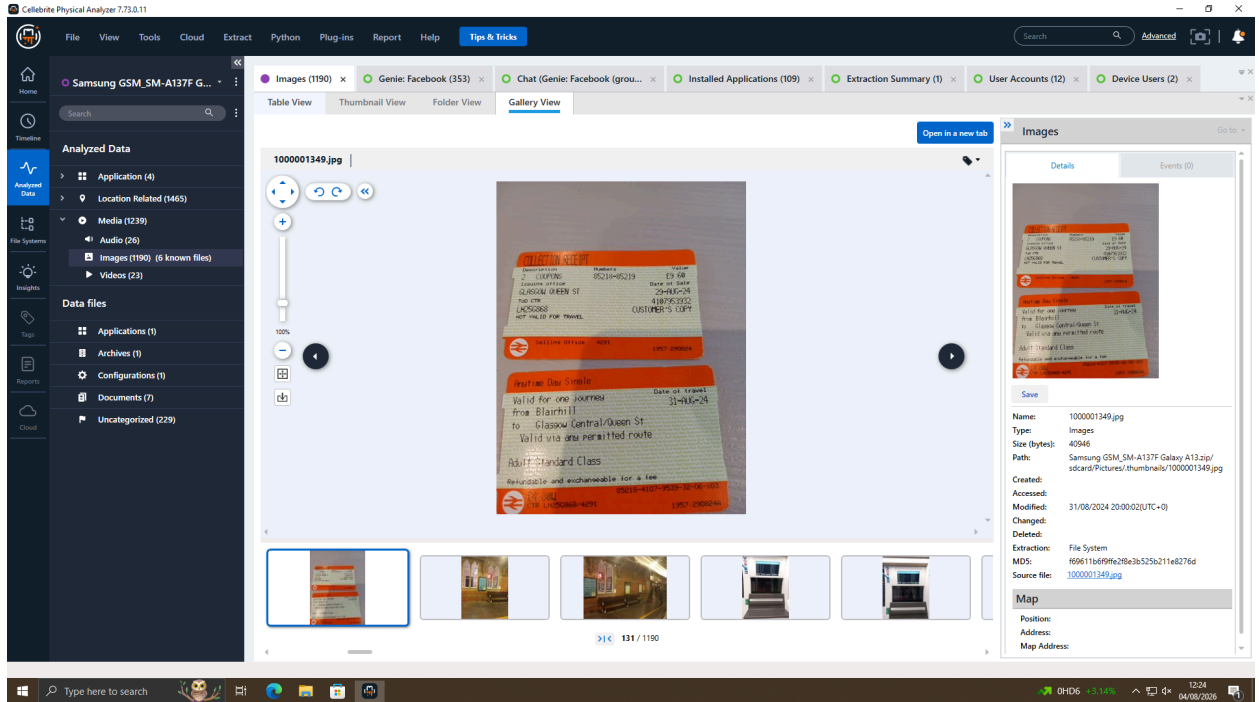


Figure 15: Extract of digital travel ticket from Glasgow as exhibited in QT-03

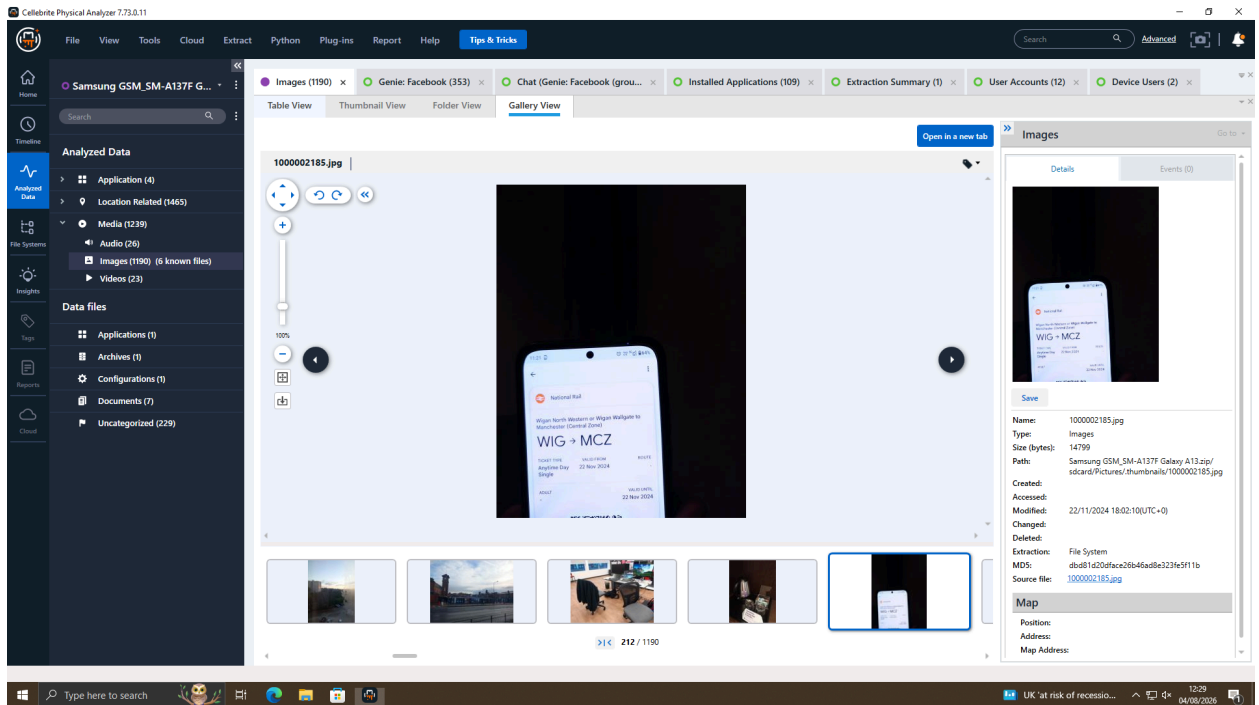


Figure 16 Extract of digital Manchester travel ticket establishing

suspect travel route

- **Geospatial Attribution of Hotel Room Location:** Geospatial metadata and location-based applications logs extracted from the device established the arrival of Joe at the target destination. The location artifact mapped the physical presence of Joe to the hotel room location where the transfer of the QT-AI-2025 patent was conducted.

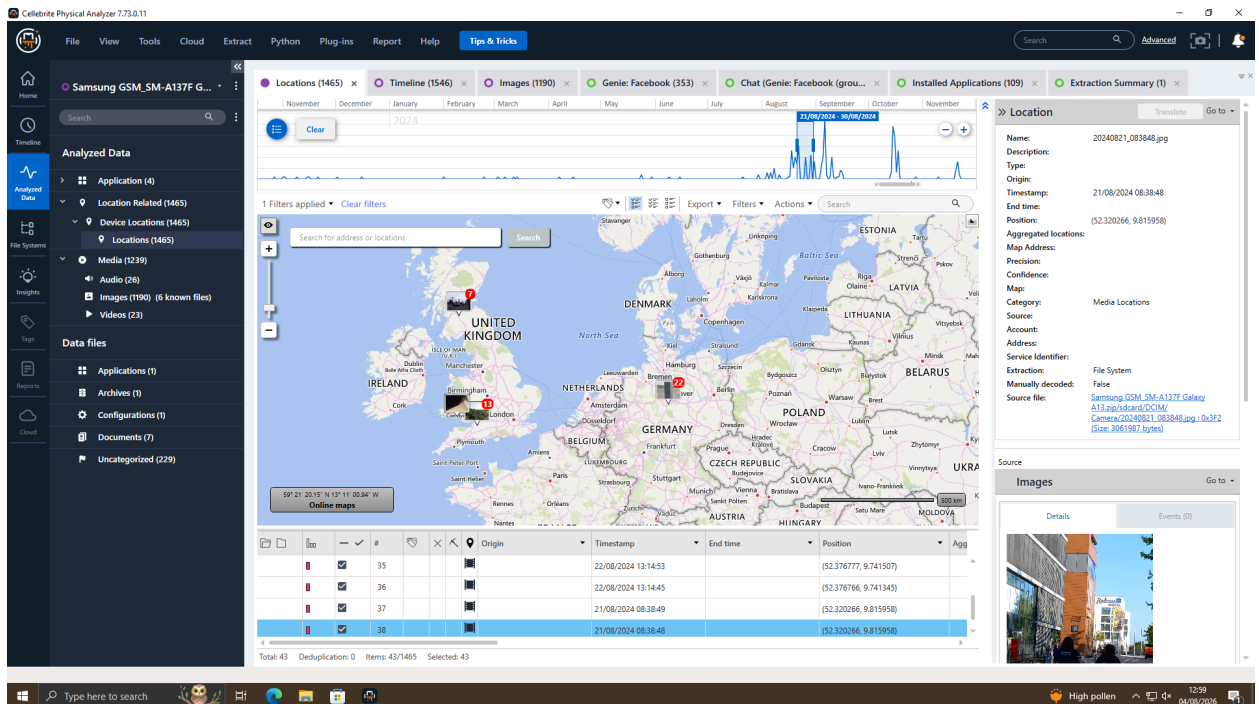


Figure 17: Artifact mapping for geospatial location Exhibit QT-03 to the hotel room

- **Travel and rendezvous geospatial attribution of Norman's Travel and Rendezvous:** Additional geospatial analysis of Exhibit QT-01 (Nokia C2 2nd Edition, attributable to the corporate purchaser Norman) has produced simultaneous location artifacts and GPS routing records. This geospatial data demonstrates that Norman travelled to the operational area, which coincides exactly with Joe's travel route to rendezvous at the location of the handover of the QT-AI-2025 patent.

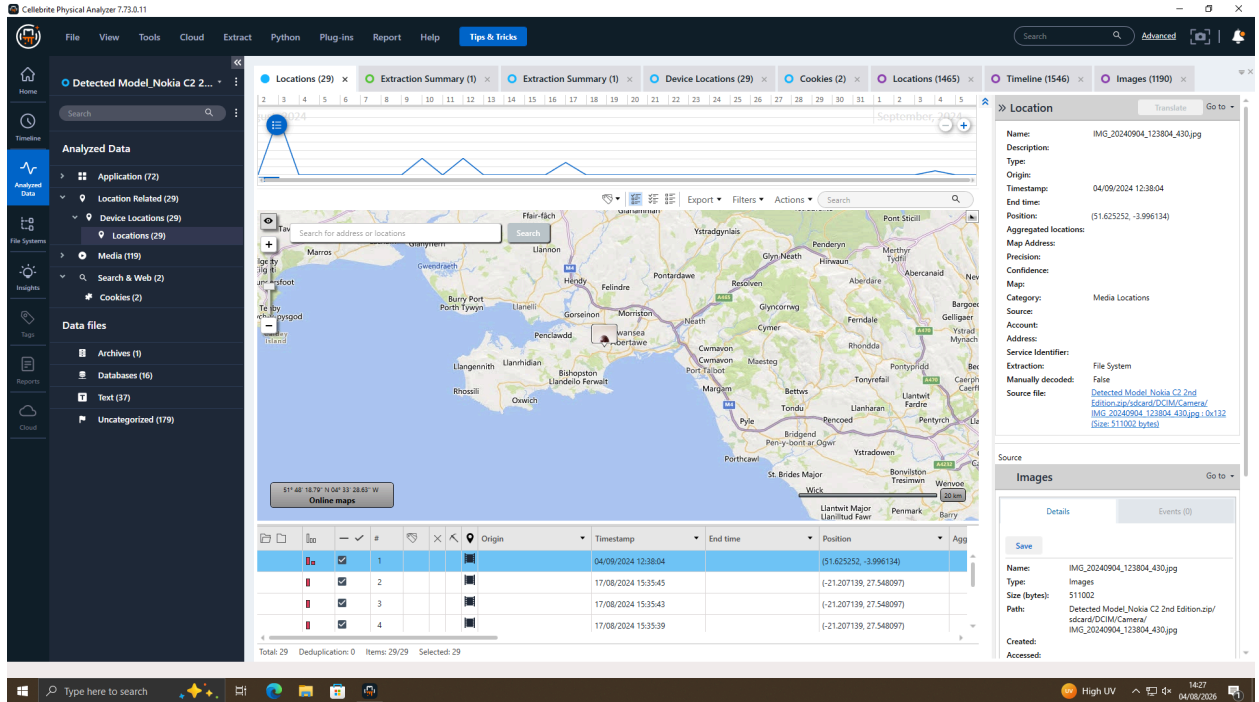


Figure 18: Artifact mapping for geospatial location Exhibit QT-01 to Norman's travel and rendezvous route

7. Chronological Timeline of the Conspiracy (Case QT-AI-2025)

Timestamp	Exhibit ID	Suspect Involved	Evidence Source	Event Description
2024-11-20	QT-02	Emma	Huawei System Logs / Genie Chats	Original configuration of covert channel and user account under pseudonym -Peter Dover.

2024-08-21	QT-02 & QT-03	Emma & Joe	WhatsApp	Emma gets in touch with Joe, informing about her intention to sell the classified Neuro system (QT-AI-2025) and asking for an external buyer.
2024-08-31	QT-02 & QT-01	Emma & Norman	Direct Messaging Channel	Emma starts a conversation with the buyer of the corporation, saying: Norman, Joe told me u r ready to proceed.
2024-08-31	QT-01 & QT-02	Norman & Emma	Direct Messaging Channel	Norman specifies payment terms: Agreed, first part releases and 5M offshore reflects, simple.
2025-08-25	QT-02	Emma & Norman	Direct Messaging Channel	Emma sets parameters for transferring data and anti-forensic measures: fine watch ur inbox in 48

				hours. After that we are ghosts.
2024-08-21	QT-03	Joe (Intermediary)	Samsung Travel Database & Wallet	Record from Joe's transit tracking demonstrating movement via first Glasgow ticket.
2024-11-22	QT-03	Joe	Samsung Transit Routing Database	Artifact from secondary transit tracking depicting Joe's transit to Manchester.
2024-08-21	QT-03	Joe	Samsung Geospatial Logs	Metadata of geolocation artifact locating Joe at the target destination hotel.
2024-08-21	QT-03	Joe & Emma	SMS / Cellular Database	Live situational update sent by Joe to Emma: Now I am in a hotel room with the client (Norman, QT-01).

2024-09-04	QT-01	Norman (Buyer)	Nokia Geospatial / GPS Logs	Artifact from geolocation mapping depicting Norman's transit route to the hotel venue.
------------	-------	-------------------	-----------------------------------	--

8. Profiling and Behavioral Analysis of the Suspect

From the forensic extractions conducted in multiple devices, the communication patterns through different platforms, and the geospatial maps obtained in the exhibits QT-01, QT-02, and QT-03 (Case Reference: QT-AI-2025), profiling of the specific role and motivation of each of the people involved in the case is as follows:

A. Emma (The Insider)

- **Function:** Main insider threat and perpetrator of the corporate espionage crime. She abused her privileged access as an engineer at Quantum Tech by targeting, accessing, and preparing for the extraction of the confidential AI chip design patent (QT-AI-2025 / AI-based Neuro product).
- **Motivation:** Greed and intellectual property violation.
- **Evidence:** Forensic extractions in Exhibit QT-02 (Huawei POT-LX1 P Smart) showed evidence of the secret Genie Chats conversations where she communicated using a pseudonym name Peter Dover. Logs from WhatsApp as well as cross platform messages confirm Emma's involvement in persuading the middleman, Joe, to arrange an outside buyer for their product.
The logs from direct communications show Emma negotiating a deal with the buyer, Norman, settling on a \$5M offshore transfer along with anti-forensic advice (fine watch ur inbox in 48 hours. after that we are ghosts).

B. Joe (The Intermediary / Broker)

- **Function:** Illegal broker/intermediary and logistics provider. Joe served as a mediator between the insider (Emma) and the corporate buyer (Norman) to create confusion about the channels of communication and protect both sides from detection by the corporation.
- **Motivation:** Money from commission gained as part of the illegal transaction.
- **Evidence:**
Extracted logs from Exhibit QT-03 (Samsung Galaxy A13) proved Joe's involvement in arranging the terms for the meeting.
Movement data and travel records, consisting of initial travel tickets from Glasgow and transit routes from Manchester, showed the physical movements of Joe in regions before the meeting.
Geographical tracking data clearly identified the geographical presence of Joe in the targeted hotel room. This is confirmed by the smoking gun message sent to Emma: Now I am in a hotel room with the client.

C. Norman (The Buyer / Corporate Competitor)

- **Function:** External buyer and Research & Development Director for the competing company NexGen Circuits. Norman attempted to illegally obtain Quantum Tech's QT-AI-2025 patent to save his firm from conducting expensive research and development efforts.
- **Motive:** Corporate gain, market domination, and industrial espionage.
Evidence Supporting the Claim:
- **Evidence:**
Messages collected as evidence from Exhibit QT-01 (cross-device messages) prove that Norman agreed to the illegal deal on account of financial logistics: Agreed, first part releases and 5M offshore reflects, simple.

- **Evidence Countering the Claim / Counter-forensics:**

Analysis of Exhibit QT-01 (Nokia C2 2nd Edition) revealed vital anti-forensic artifacts: the phone was confiscated in the absence of its local SIM card and with major sanitization of local communication databases. The above measures point at mens rea and destruction of local evidence by Norman.

9. Conclusion

Conducting an extensive digital forensic examination of case QT-AI-2025, we have managed to prove a legally acceptable timeline of the corporate espionage act. Cross-device and geolocation analysis prove that Emma, Joe, and Norman are responsible for participating in the plot. The recovery of the hidden intent from Exhibit QT-02, along with operational transit tracking (Exhibits QT-01 and QT-03) and the confirmation message regarding the transfer, provides conclusive evidence of the planned theft of the QT-AI-2025 patent.

10. Recommendations

1. **For Quantum Tech Legal & Management:**

Submit these results to law enforcement to begin criminal prosecution for Corporate Espionage and Conspiracy to Commit Fraud against Emma, Joe, and Norman. Establish tighter data loss prevention measures and limit access privileges on the classified R&D data archives.

2. **For Law Enforcement Investigators (Technical Follow-up):**

For legally overcoming the anti-forensic sanitization done by Norman on his Nokia C2 (QT-01), submit a request for Call Detail Records (CDRs) and IMEI number from network log data of the corresponding Mobile Network Operators (MNOs) within the period of operations, which can be compared against the physical IMEI number of Exhibit QT-01.

