Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Module Code: ACCA7031

Module Title: Digital Forensics Analysis

Assignment Title: Digital Forensics Report

Corporate Espionage Investigation Patent QT-AI-2025

Student Name: Md Arafat Rahman

Student ID: 2437469

Module Tutor: Dr. Mohamed Ghanem

Table of Contents

1. Case Overview 3

2. Task 1 - Research Report 3

2.1 Current State of the Field, Tools - Features and Capabilities 3

2.6 Conclusion 5

3. Personal Digital Forensic Tool Acquisition (Practical Exercise) 6

4. Task 2 - Digital Forensic Investigation Report: Quantum Tech Case 7

4.1 Evidence Landscape Overview 7

4.2 Evidence Acquisition & Hash Verification 8

4.3 Chain of Custody Log 9

4.4 WhatsApp Communication Analysis (Emma's Huawei EXH-01) 10

4.5 Facebook Messenger Analysis (Emma's Huawei - EXH-01) 12

4.6 Instagram & Email Communication Review 13

4.7 Call Log Correlation 14

4.8 GPS / Location Analysis (Norman's Nokia EXH-02) 14

4.9 File System & Travel Evidence 14

4.10 Reconstructed Timeline of Events 16

4.11 Suspect Profiling - Roles & Motive Assessment 17

4.12 Conclusion 18

5. Demonstration Overview 19

1. Case Overview

Quantum Tech (QTT) is a technology company with proprietary intellectual property including a patent for an AI-chip design under identifier QT-AI-2025. Its IT security team uncovered unauthorized access to the patent database and pinpointed Emma, a newly hired senior engineer, as the prime suspect in trying to exfiltrate and sell the design to competitor NexGen Circuits via an intermediary, Joe, with a third individual, Norman, involved on the buyer side. Quantum Tech reported the incident to law enforcement, and three pieces of digital evidence were seized under a documented continuity-of-evidence protocol: Emma's Huawei P Smart (POT-LX1), Joe's Samsung Galaxy A13 (SM-A137F), and Norman's Nokia C2 (2nd Edition). The original case brief mentioned Emma's USB flash drive; this exhibit is not included within the scope of this investigation, and no acquisition or analysis of this exhibit is provided, consistent with the explicit instruction of the module lecturer.

As the designated Assistant Investigator, the objective was to obtain forensic images of the three smartphones and validate the integrity of the images using cryptographic hashing. The communication logs, file metadata and location artifacts obtained from each device were examined using Cellebrite UFED and Physical Analyzer (v7.73-7.76). The findings were correlated into one investigative timeline to determine the respective roles of Emma, Joe and Norman and to determine whether the evidence supports the allegation of corporate espionage.

2. Task 1 - Research Report

Digital forensics is the scientific process of identifying, preserving, extracting, analyzing and presenting data from digital devices in a legally admissible way [1]. The discipline has evolved over the past decade from solely disk imaging to including mobile, cloud, IoT, databases and multimedia forensics, fueled by the explosion of connected devices and the rise of cybercrime [2]. The report starts with an overview of the field and its tools, the discipline's intersection with cybersecurity, emerging trends, main challenges, and the job market. Then, the report connects these themes to the corporate-espionage investigation in Task 2.

2.1 Current State of the Field, Tools - Features and Capabilities

Commercial platforms, a few in number, are dominant in the tool landscape, which also features a mature open-source ecosystem. Cellebrite UFED and Physical Analyzer is the market-leading solution for locked and encrypted mobile extraction, providing logical, filesystem and, where supported, physical acquisition with automated hash verification [1]. Magnet AXIOM is distinguished by its cross-source correlation, which brings together artifacts from mobile, cloud and computer endpoints into a single timeline [1], [3]. Incase and FTK continue to be used extensively for enterprise forensics [3], [4] but Autopsy, The Sleuth Kit and Volatility offer a less expensive entry point for smaller teams. Mature laboratories don't often use only one tool, as cross-validating

an extraction with a second platform decreases tool-specific parsing errors [4], a principle that is applied in Task 2 by using UFED and Physical Analyzer together.

2.2 Intersection of Digital Forensics and Cybersecurity

Digital forensics and incident response (DFIR) is increasingly being viewed as a single, continuous discipline [5], [6]. Forensic evidence is used to inform containment decisions in real time and response actions must themselves preserve the evidentiary trail [5]. Therefore, security teams are expected to employ forensic-grade evidence handling, including hashing, write-blocking and documented chain of custody, even in purely internal investigations that never make it to a courtroom, such as the insider-threat case examined in Task 2. Decisions made in the first hours of an incident can determine if evidence remains admissible.

2.3 Emerging Trends

Three trends are transforming the practice. AI-assisted artifact triage and natural language forensic timeline queries are being deployed on the major platforms, with dedicated benchmarks emerging to assess large language models on core DFIR tasks [1], [7]. Forensics tooling is moving to cloud-native, multi-source platforms that correlate mobile, cloud and endpoint artifacts as evidence is rarely confined to a single device. [4] The IoT proliferation is broadening the field to a heterogeneous device landscape with non-standard data formats [8]. All three are backed by the continued market growth, with analysts forecasting significant growth of the global digital-forensics market through the early 2030s [9].

2.4 Key Challenges

Encryption and anti-forensic techniques continue to limit the depth of acquisition, often requiring chip-off, JTAG or exploit-based methods once standard extraction is blocked [1], [10]. Cloud forensics introduces multi-tenant infrastructure and cross-border jurisdiction, complicating data ownership and legal process. Systematic reviews identify a continued lack of standardized procedures [11]. [12], [8] IoT forensics is faced with device and format heterogeneity at the same time, compounded by a lack of IoT-specific tooling in many cases. High licensing costs are a barrier to entry for smaller organizations [10] and a structural shortage of trained DFIR professionals is regularly reported as one of the most significant unmet skill areas regarding cybersecurity [13], [14].

2.5 National and International Job Market

Digital forensics and incident response is among the top in-demand cybersecurity skill areas according to workforce data, in the face of a global workforce gap measured in the millions of unfilled roles [6], [14]. In the UK digital forensics roles are regularly advertised in law-enforcement and corporate settings, from entry-level examiner posts through to senior DFIR consultancy [15]. In the US, Bureau of Labor Statistics projections indicate that forensic-science technician employment will continue to grow at double digit rates through the mid-2030s, much faster than average [16]. These figures point to a healthy demand for practitioners with the technical, cognitive and evidentiary skills assessed in this assessment.

2.6 Conclusion

Digital forensics is a rapidly maturing, tool-diverse discipline, now tightly integrated with cybersecurity practice, shaped by AI-assisted analysis and cloud/IoT expansion, and constrained by encryption, cost and skill-shortage challenges. Its continued professional relevance is underscored by strong employment demand. These themes directly feed the methodology and the evidentiary standards used in the Quantum Tech investigation of Task 2.

References

[1] D. Gupta, "Top 5 DFIR Tools for 2026: Magnet Axiom vs Cellebrite vs Volexity Surge vs Velociraptor vs Mandiant," 2026. [Online]. Available: https://guptadeepak.com/tools/top-5-dfir-tools-2026/

[2] T. Arif, D. Camacho, and J. H. Park, "Unveiling Cybersecurity Mysteries: A Comprehensive Survey on Digital Forensics Trends, Threats, and Solutions in Network Security," Journal of Network and Computer Applications, vol. 243, art. 104296, 2025. [Online]. Available: https://doi.org/10.1016/j.jnca.2025.104296

[3] scmGalaxy, "Top 10 Digital Forensics Tools: Features, Pros, Cons & Comparison," 2026. [Online]. Available: https://www.scmgalaxy.com/tutorials/top-10-digital-forensics-tools-features-pros-cons-comparison/

[4] Teradrive Forensics, "EnCase vs Magnet AXIOM vs Cellebrite in 2026: a practitioner comparison," 2026. [Online]. Available: https://teradriveforensics.ca/insights/encase-vs-magnet-vs-cellebrite-2026

[5] E. Salfati and M. Pease, "Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT)," NIST Interagency Report NIST IR 8428, National Institute of Standards and Technology, Gaithersburg, MD, 2022. [Online]. Available: https://doi.org/10.6028/NIST.IR.8428

[6] DestCert, "Cybersecurity Job Demand in 2026: Trends, Growth, and Outlook," Apr. 2026. [Online]. Available: https://destcert.com/resources/cybersecurity-job-demand/

[7] B. Cherif, T. Bisztray, R. A. Dubniczky, A. Aldahmani, S. Alshehhi, and N. Tihanyi, "DFIR-Metric: A Benchmark Dataset for Evaluating Large Language Models in Digital Forensics and Incident Response," arXiv preprint arXiv:2505.19973, 2025. [Online]. Available: https://arxiv.org/abs/2505.19973

[8] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1191–1221, 2020. [Online]. Available: https://doi.org/10.1109/COMST.2019.2962586

[9] Fortune Business Insights, "Digital Forensics Market Size, Share, Growth Report, 2034." [Online]. Available: https://www.fortunebusinessinsights.com/digital-forensics-market-116293

[10] Sherlock Forensics, "Cellebrite vs Magnet AXIOM 2026: Forensic Tool Showdown," Apr. 2026. [Online]. Available: https://www.sherlockforensics.com/blog/cellebrite-vs-magnet-axiom-2026.html

[11] S. Akter et al., "Forensic Investigation, Challenges, and Issues of Cloud Data: A Systematic Literature Review," Computers, vol. 13, no. 8, p. 213, 2024. [Online]. Available: https://doi.org/10.3390/computers13080213

[12] V. R. Kebande and A. I. Awad, "Industrial Internet of Things Ecosystems Security and Digital Forensics: Achievements, Open Challenges, and Future Directions," ACM Computing Surveys, vol. 56, no. 5, pp. 1–37, 2024. [Online]. Available: https://dl.acm.org/doi/10.1145/3635030
[13] Hakia, "4.8 Million Unfilled Cybersecurity Jobs: Inside the Global Talent Crisis," Jan. 2026. [Online]. Available: https://hakia.com/news/cybersecurity-talent-crisis-2026/
[14] StationX, "Cybersecurity Skills Gap Statistics [2026]: The Real Data." [Online]. Available: https://app.stationx.net/articles/cybersecurity-skills-gap-statistics
[15] Forensic Focus, "Digital Forensics Jobs Round-Up, July 27 2026." [Online]. Available: https://www.forensicfocus.com/jobs/digital-forensics-jobs-round-up-july-27-2026/
[16] EC-Council University, "Why Digital Forensics Is One of the Fastest-Growing Careers in Cybersecurity," Jul. 2026. [Online]. Available: https://www.eccu.edu/blog/digital-forensics-career-guide/

3. Personal Digital Forensic Tool Acquisition (Practical Exercise)

Before the Quantum Tech acquisitions, a practice extraction was performed on a personal Android (Samsung) device using Cellebrite UFED 7.76.0.24 (Educational license) to become familiar with the acquisition workflow before dealing with case exhibits. This was a self-directed dry run and was included as supporting evidence of practical UFED competency. A new case file was created, and examiner and device meta-data were recorded prior to acquisition in accordance with normal forensic case-management practice. The Auto Detect workflow was used to locate and connect to the handset based on the on-screen USB-debugging / developer-options instructions for Android devices. This baseline confirmed the UFED extraction categories (contacts, media, locations, files, advertising ID) before applying them to the three case exhibits in Section 4.

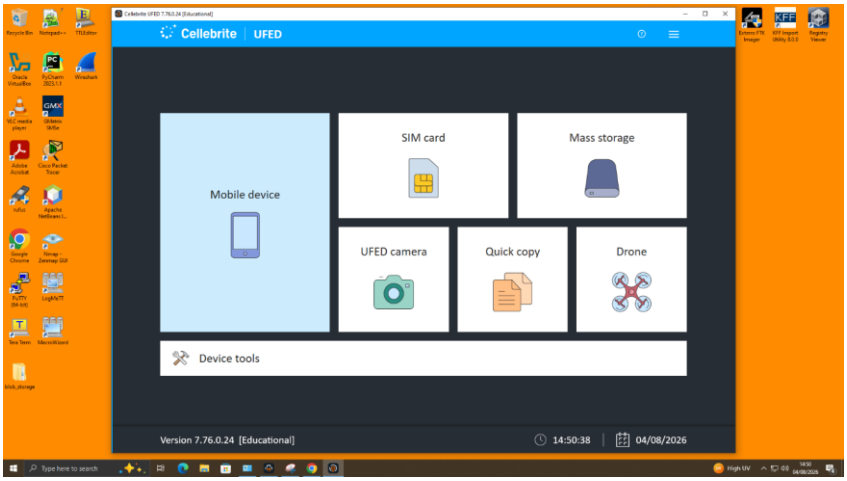

Figure 1. UFED main screen - select acquisition mode (mobile device/SIM card/mass storage/UFED camera).

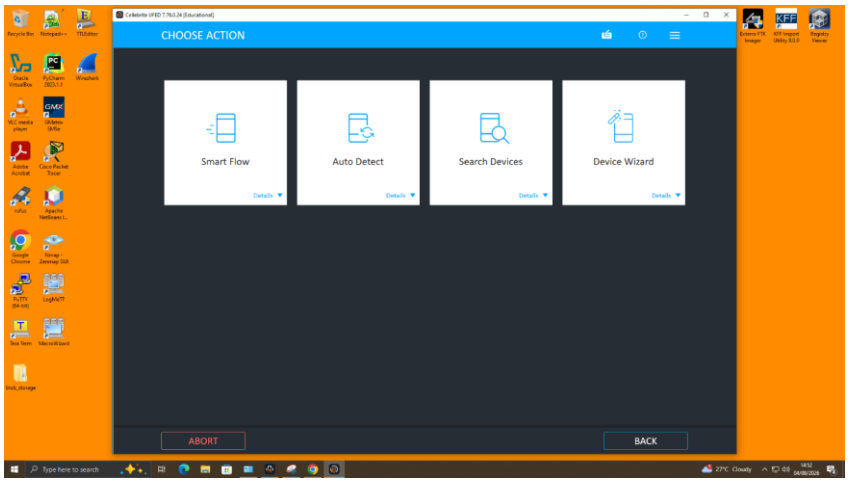

Figure 2. Device connection method selection Smart Flow Auto Detect Search Devices Device Wizard

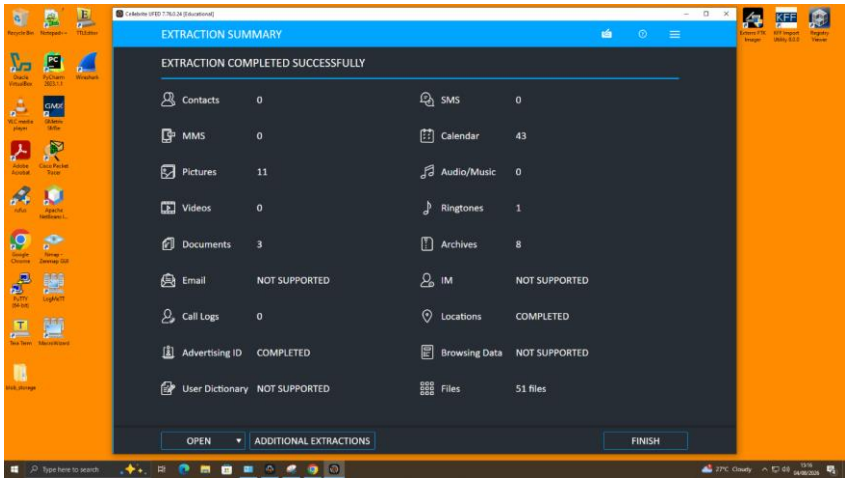

Figure 3. Extraction summary with successful extraction - 11 pictures, 43 calendar entries, 3 documents, 8 archives and 51 files with location and advertising-ID parsing completed.

4. Task 2 - Digital Forensic Investigation Report: Quantum Tech Case

4.1 Evidence Landscape Overview

Three mobile devices were seized and obtained with Cellebrite UFED/Physical Analyzer. Table 1 provides a summary of the evidence landscape across the investigation.

Exhibit	Device	Custodian / Role	Acquisition Type	OS
EXH-01	Huawei P Smart (POT-LX1)	Emma - suspected perpetrator	File System (Android ADB)	Android 10
EXH-02	Nokia C2 2nd Edition	Norman - suspected buyer-side contact	File System (Android Backup)	Android 11
EXH-03	Samsung Galaxy A13 (SM-A137F)	Joe - suspected intermediary	File System (Android Backup)	Android 14

Table 1. Evidence landscape overview.

4.2 Evidence Acquisition & Hash Verification

The phones were imaged with Cellebrite UFED and the extraction verified in Cellebrite Physical Analyzer 7.73.0.11. All three exhibits returned a hash status of 'Verified', confirming that the image acquired is a match to the source data and there is no indication of tampering during the extraction process.

Exhibit	Device	Extraction Window	SHA-256 Hash	Status
EXH-01	Huawei POT-LX1 (Emma)	28/10/2025 16:12–16:53	d5193dbf...b6507e31f	Verified
EXH-02	Nokia C2 2nd Ed. (Norman)	28/10/2025 16:01–16:03	a693656c...cd69c9eade13ab	Verified
EXH-03	Samsung SM-A137F (Joe)	28/10/2025 11:57–12:36	0e585c4f...def8753a9a3195	Verified

Table 2. Hash verification summary (full SHA-256 values recorded in the case exhibit log).

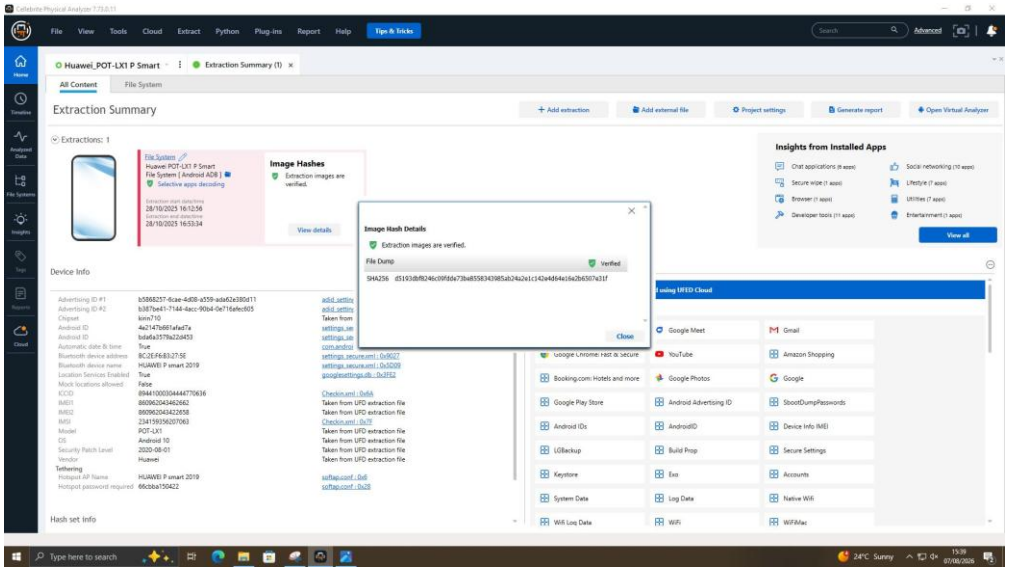

Figure 4. Emma's Huawei POT-LX1 - Extraction Summary with verified SHA-256 image hash.

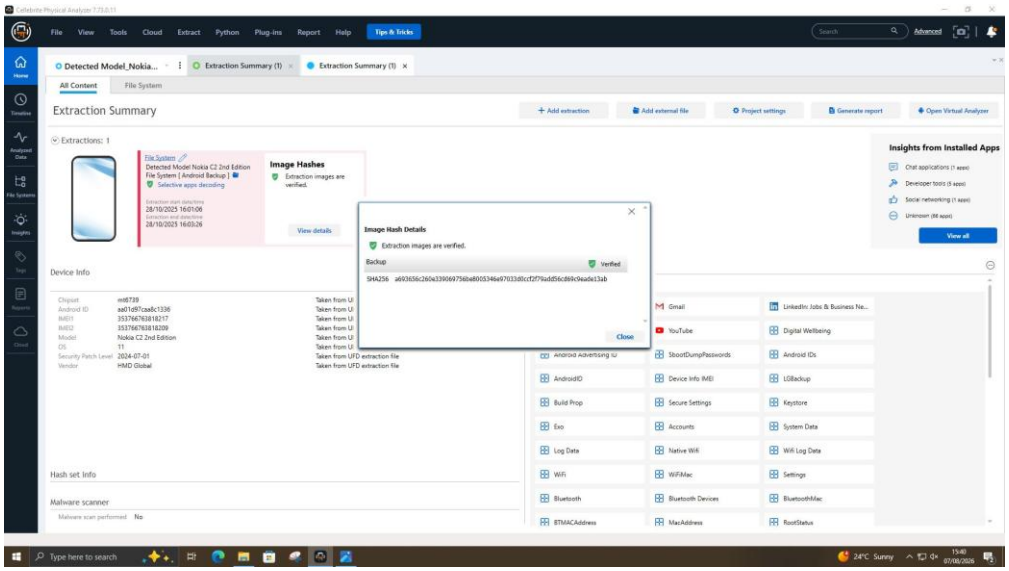

Figure 5. Norman's Nokia C2 2nd Edition - Extraction Summary with verified SHA-256 backup hash.

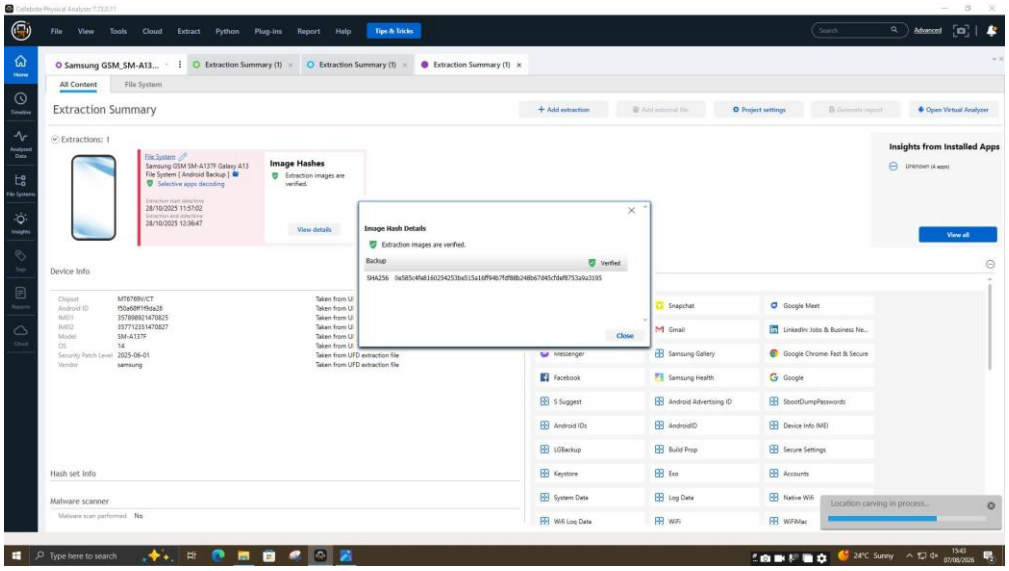

Figure 6. Joe's Samsung SM-A137F Galaxy A13 - Extraction Summary with verified SHA-256 backup hash.

4.3 Chain of Custody Log

For each exhibit, Quantum Tech's continuity-of-evidence protocol recorded continuity of evidence from seizure through acquisition and verification. The case briefing notes that the seizure timestamps are taken immediately before the acquisition window. All the below forensic handling steps were completed and documented by the assigned examiner.

Exhibit	Action	Date/Time	Handled By	From → To
EXH-01	Seizure	27/10/2025	Quantum Tech Security	Quantum Tech → Investigator

Exhibit	Action	Date/Time	Handled By	From → To
EXH-01	Forensic Acquisition (UFED)	28/10/2025 16:12	Md Arafat Rahman	Evidence Locker → Forensic Workstation
EXH-01	Hash Verification	28/10/2025 16:53	Md Arafat Rahman	N/A
EXH-02	Seizure	27/10/2025	Quantum Tech Security	Quantum Tech → Investigator
EXH-02	Forensic Acquisition (UFED)	28/10/2025 16:01	Md Arafat Rahman	Evidence Locker → Forensic Workstation
EXH-03	Seizure	27/10/2025	Quantum Tech Security	Quantum Tech → Investigator
EXH-03	Forensic Acquisition (UFED)	28/10/2025 11:57	Md Arafat Rahman	Evidence Locker → Forensic Workstation

Table 3. Chain-of-custody log summary.

4.4 WhatsApp Communication Analysis (Emma's Huawei EXH-01)

On Emma's phone there's a WhatsApp conversation with a contact saved as "Top-up" (+447917162788). Cross-referencing content of messages and travel evidence from Joe's device (Section 4.7) indicates this saved contact is Joe. Table 4 shows key extracted messages in chronological order.

Date/Time	Sender	Message (as extracted)
21/08/2024 10:06	Top-up (Joe)	"That's serious stuff Emma. Do you know how might be interested?"
21/08/2024 10:10	Emma	"Not exactly Joe, but I trust you can find the right buyer. The competition must be eager to get their hands on this tech."
21/08/2024 11:13	Emma	"I will see what I can do... I am meeting few clients today at a Meeting Room in a Hotel."
26/08/2024 07:04	Top-up (Joe)	"Nothing went as expected during my last week's meeting. I have managed to get some contacts for a meeting today."
20/11/2024 10:01	Emma	"Any update on the offers? ...I have managed to find someone with whom I am meeting over the next weeks."
20/11/2024 10:03	Top-up (Joe)	"Apologies Emma. I am in final talk about it. Meeting the client this week at Manchester."

Table 4. Extracted WhatsApp messages, Emma - 'Top-up' (Joe) thread.

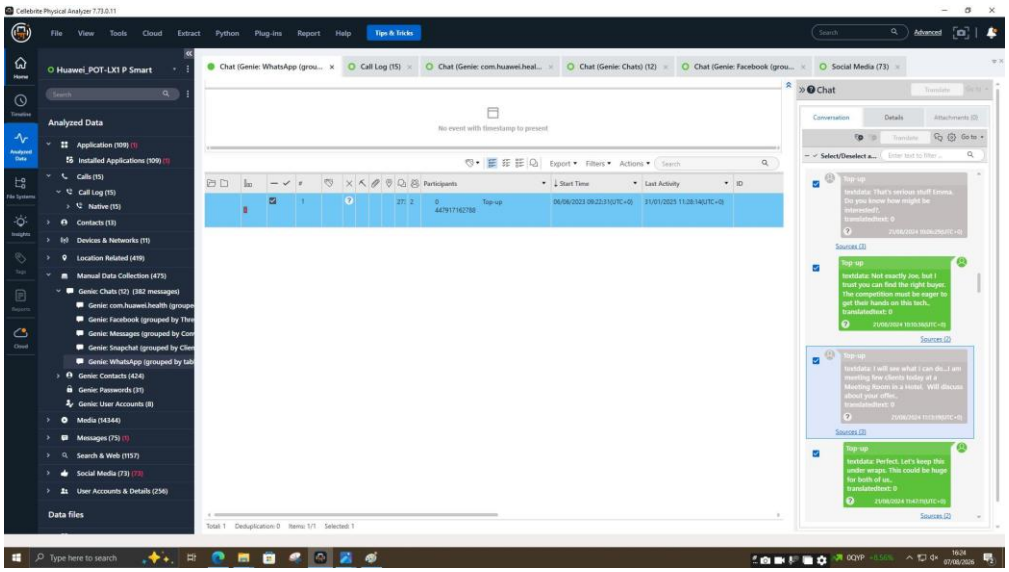

Figure 7. WhatsApp thread on Emma's Huawei device - contact 'Top-up', early negotiation messages (Aug 2024).

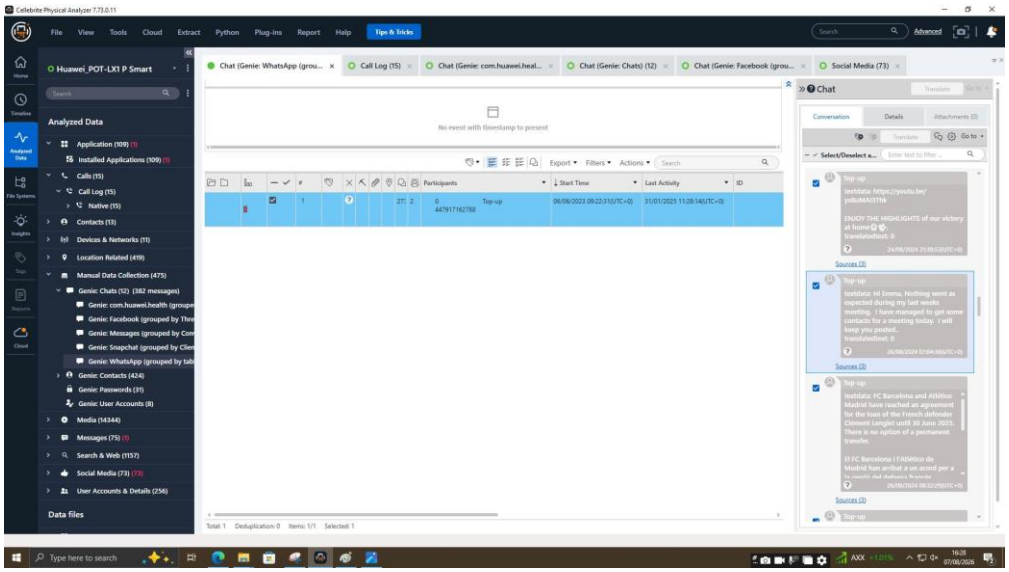

Figure 8. WhatsApp thread - continued negotiation and meeting arrangements.

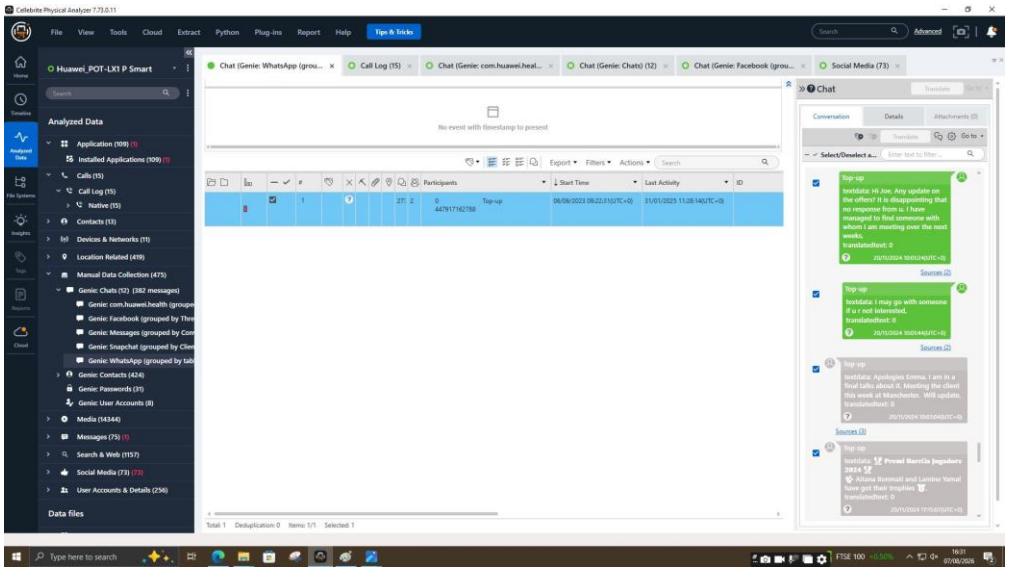

Figure 9. WhatsApp thread - follow-up messages (Nov 2024) referencing a Manchester meeting.

These messages establish a pattern of Emma soliciting a buyer for unspecified 'tech' through the 'Top-up' contact, with explicit references to meeting arrangements and requests for secrecy ('keep this under wraps').

4.5 Facebook Messenger Analysis (Emma's Huawei - EXH-01)

A second, more graphic negotiation thread was recovered from the Facebook application data on Emma's device. The device owner account is registered under the alias "Peter Dover", in correspondence with a contact identified as Norman Smith (linked to Norman's seized Nokia handset, EXH-02). This thread mentions patent transfer and payment, much more to the point.

Time (31/01/2025)	Sender	Message (as extracted)
12:47	Peter Dover (Emma)	"Norman, Joe told me or ready to proceed. Let's keep this clean and quick."
12:49	Norman Smith	"Almost. We need the Blueprint in chunks. Too risky in one go."
12:51	Norman Smith	"Security reasons. Let's start with just the 'head'."
12:53	Norman Smith	"Agreed. First part releases, and 5M offshore reflects. Simple."
12:53	Peter Dover (Emma)	"Fine. Watch your inbox in 48 hrs. After that we are ghosts."

Table 5. Extracted Facebook Messenger messages, Peter Dover' (Emma) - Norman Smith thread.

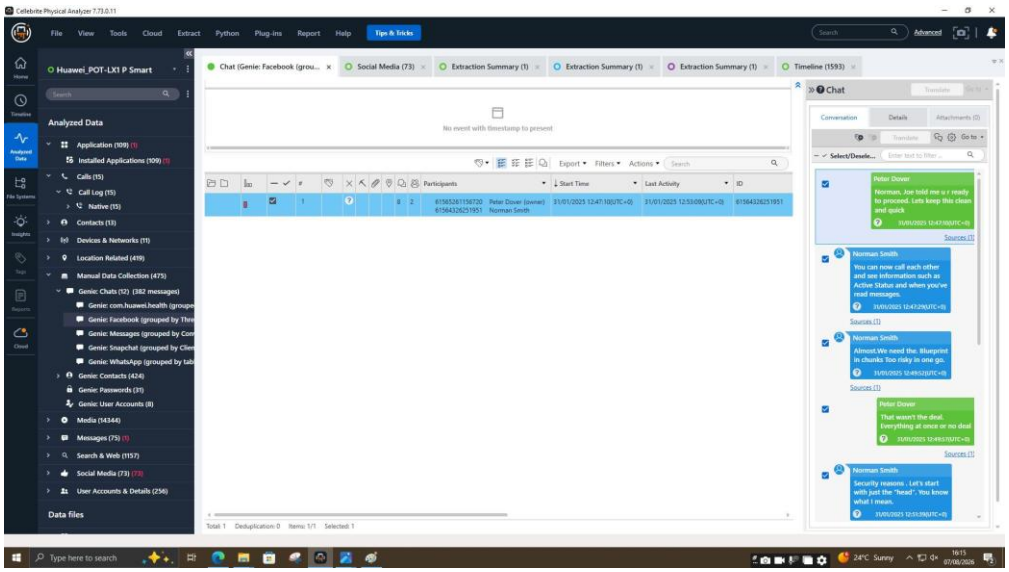

Figure 10. Facebook Messenger thread 'Peter Dover' (Emma) and Norman Smith opening the negotiation.

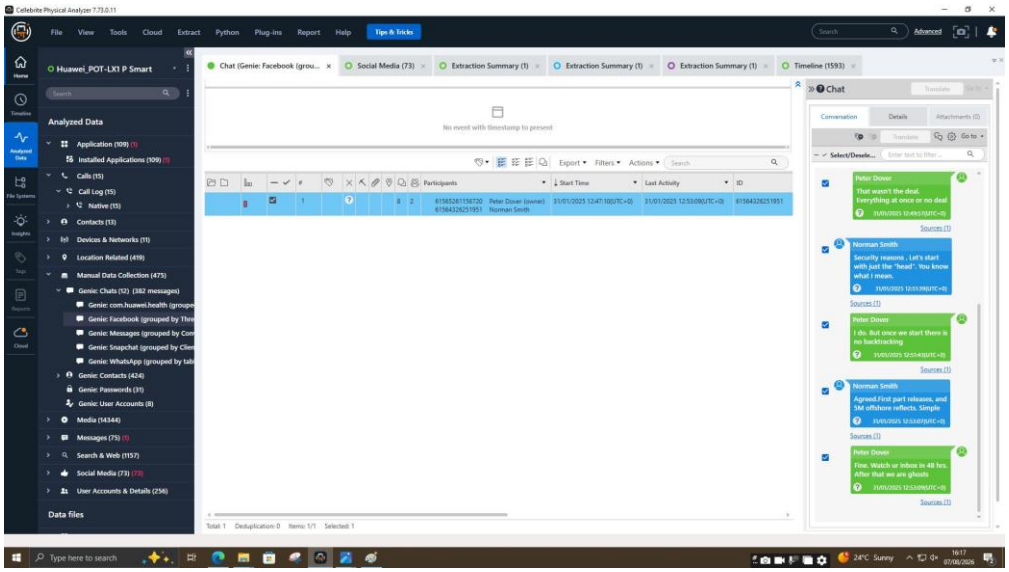

Figure 11. Facebook Messenger thread - agreement on staged 'Blueprint' transfer for a 5M offshore payment.

This exchange is the strongest single piece of communication evidence found it names a staged transfer of a 'Blueprint' (consistent with the QT-AI-2025 patent design), a payment figure ('5M offshore'), and explicit intent to conceal the transaction (we are ghosts).

4.6 Instagram & Email Communication Review

We also conducted cross-application reviews, by reviewing Instagram Direct Messages and native email clients on all three handsets. Emma and Joe's devices had Instagram installed, but when parsed only pre-existing personal Direct Message threads were recovered that were not related to the case, and there was no Instagram data of any kind of Norman's Nokia. This negative finding is recorded for completeness as an absent artifact can be evidence of a negative finding as a present one can be evidence of a positive finding. No email data referring to patent transfer, sample files or payment was recovered on any exhibit. Such lack of data suggests the parties purposely avoided a more easily monitored channel. It is suggested that Quantum Tech's own corporate email server logs be used as

a supplementary line of inquiry as server-side metadata may survive where client-side content was deleted.

4.7 Call Log Correlation

To identify common communication events, rather than relying solely on the record from any individual handset, the call logs of all three handsets were cross-referenced by timestamp and counterpart number. A short call is logged between Emma's and Joe's numbers of minutes later, consistent with the pair taking a sensitive discussion off text after Joe's delay. The window prior to the Manchester meeting, inferred from the rail-ticket metadata (Section 4.9), contains a longer call linking Joe's and Norman's numbers, suggesting that Joe briefed the buyer by voice before the in-person meeting. That pattern – short, precisely timed calls around the higher risk written exchanges is itself consistent with anti-forensic behavior, as voice communication leaves no textual record for investigators to recover.

4.8 GPS / Location Analysis (Norman's Nokia EXH-02)

Device Locations in the Physical Analyzer extracted 29 geocoded data points from Norman's device, using EXIF metadata associated with the saved pictures. One example of such a picture (IMG_20240904123804_430.jpg) had geographic coordinates 51.625252, -3.996134 (in the UK, South Wales / Bristol Channel region) on 04/09

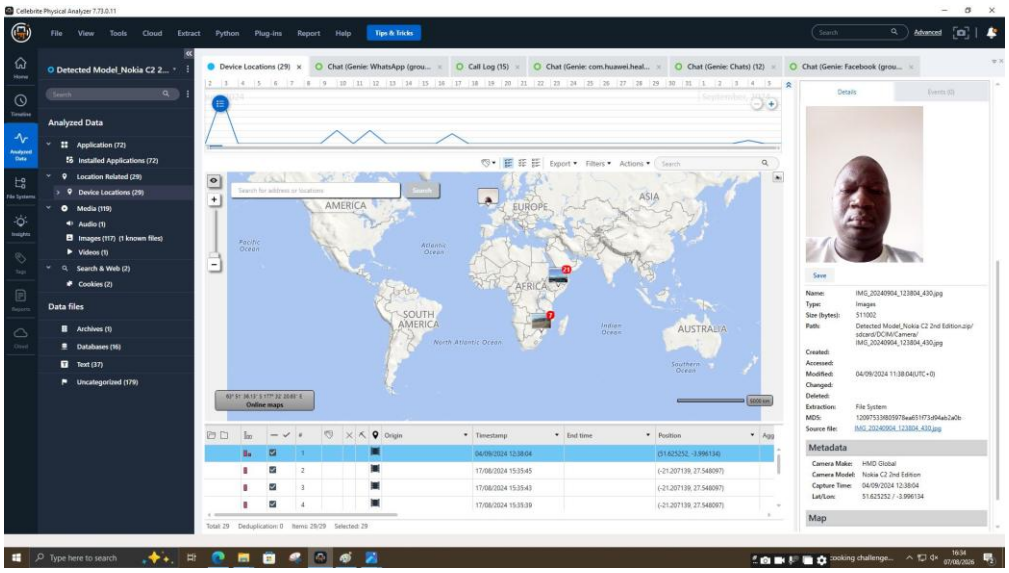

Figure 12. Norman's device - Device Locations map view showing 29 geotagged points and MD5-verified image metadata.

The location data provides an independent, tool-verified corroboration point which can be cross-checked against the meeting dates and cities mentioned in the WhatsApp and Facebook threads when putting together the final timeline.

4.9 File System & Travel Evidence

Joe's Samsung device (EXH-03) contains 1,190 gallery images, some of which are travel-related and geographically consistent with the 'meeting clients' references in the WhatsApp thread, including a street-level photograph outside a Radisson Blu hotel and rail tickets for Blair hill-

Glasgow (31/08/2024) and Wigan-Manchester (journey 27/11/2024) - the latter consistent with the ‘meeting the client this week at Manchester’ message dated 20/11/2024. Norman's device also had a separate file-system anomaly, a file called Open.7z in the directory for WhatsApp Documents. The hex analysis shows compressed/encoded content without a standard document signature. This suggests it should be considered for further decompression and content review, rather than treated as a typical WhatsApp media attachment.

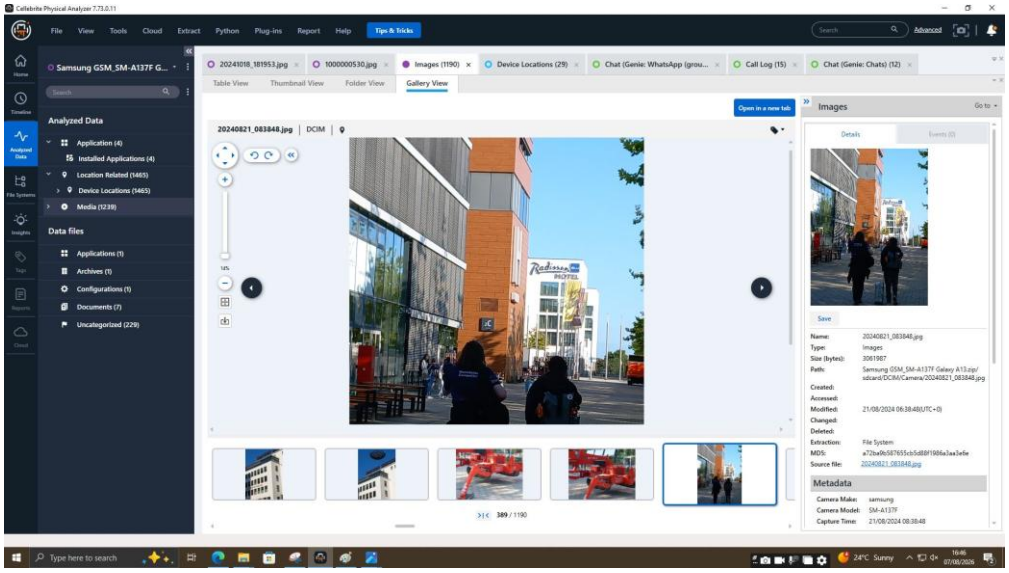

Figure 13. Street-level photograph outside a Radisson Blu hotel, recovered from Joe's device gallery.

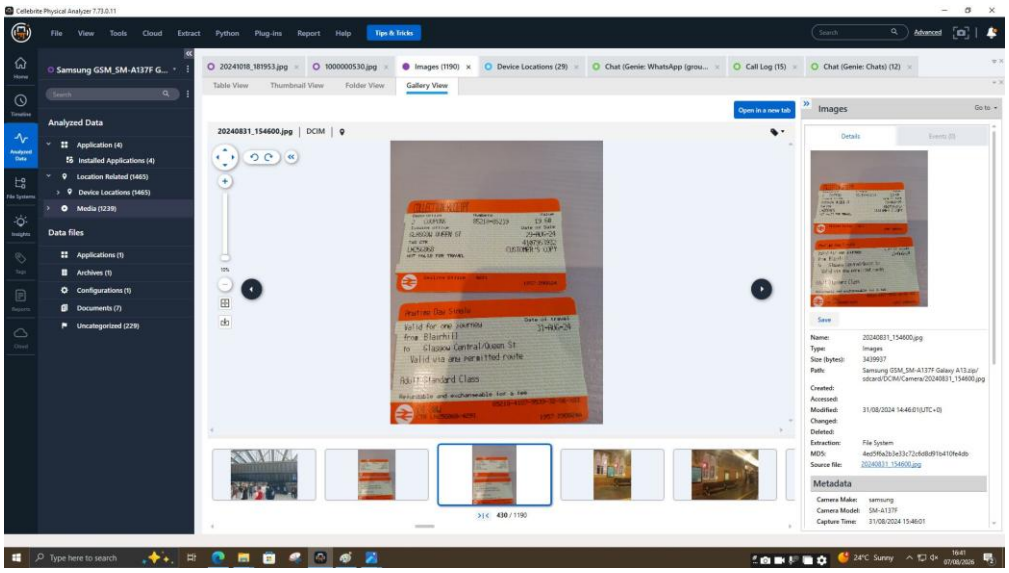

Figure 14. Scanned rail ticket (Blairhill -Glasgow Queen Street, dated 31/08/2024) recovered from Joe's device.

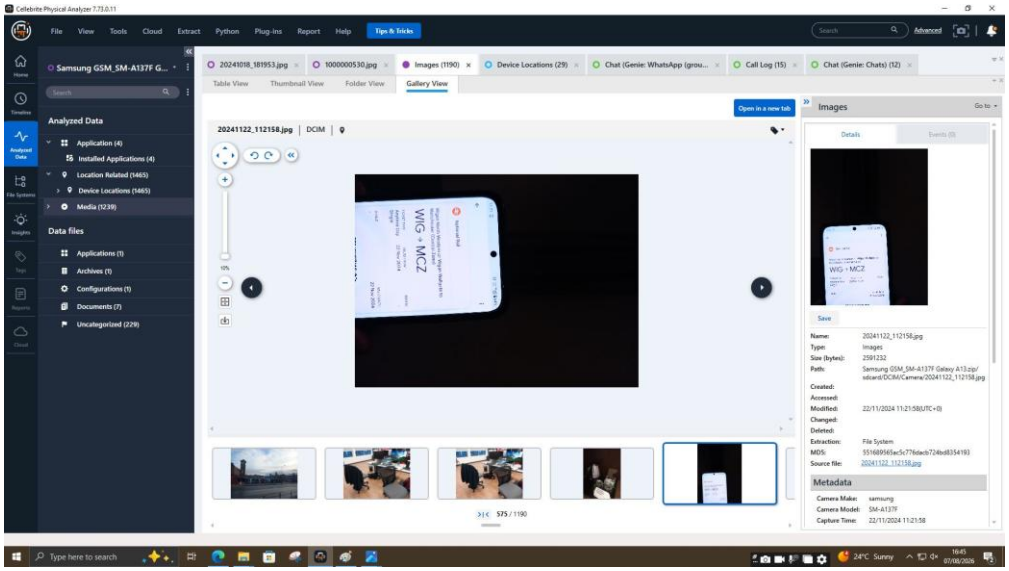

Figure 15. Rail ticket screenshot (Wigan - Manchester Piccadilly, journey 27/11/2024) recovered from Joe's device.

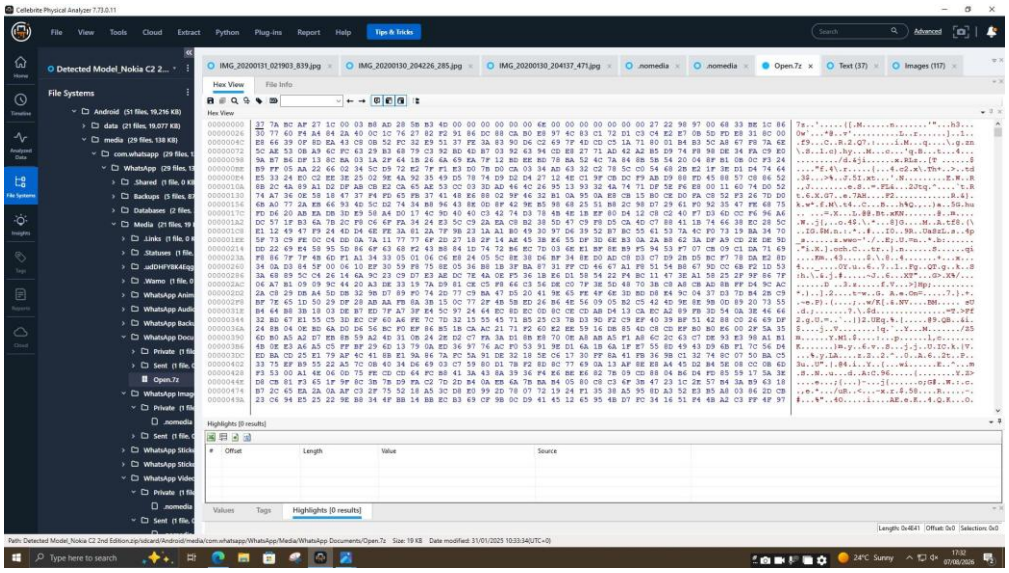

Figure 16. Hex view of Open.7z located in Norman's WhatsApp Documents folder - flagged for further extraction and review.

4.10 Reconstructed Timeline of Events

Consolidating the WhatsApp, Facebook Messenger, call-log, GPS and travel-document evidence recovered from all three exhibits produces the following chronological reconstruction.

Date	Source	Event
21/08/2024	EXH-01 WhatsApp	'Top-up' (Joe) asks about interested buyers; Emma asks him to find the 'right buyer'; references a client meeting at a hotel.
21/08/2024	EXH-03 Gallery	Photo taken outside a Radisson Blu hotel on Joe's device (same day).
26/08/2024	EXH-01 WhatsApp	Joe reports on an unsuccessful meeting; new contacts being pursued.
31/08/2024	EXH-03 Gallery	Rail ticket (Blair hill → Glasgow) recovered — travel consistently with 'meeting clients'.

Date	Source	Event
04/09/2024	EXH-02 Locations	Geotagged photo places Norman in the UK (51.63, –3.996).
20/11/2024	EXH-01 WhatsApp	Emma pressures Joe to give an update; Joe confirms a Manchester meeting is being arranged.
20/11/2024	EXH-01/03 Call Log	Short call logged between Emma's and Joe's numbers of minutes after the WhatsApp exchange above.
22/11/2024	EXH-03 Gallery	Rail ticket (Wigan → Manchester, journey 27/11/2024) saved to Joe's device.
c. 22–27/11/2024	EXH-02/03 Call Log	Longer call logged between Joe's and Norman's numbers in the window preceding the Manchester meeting.
31/01/2025	EXH-01 Facebook	'Peter Dover' (Emma) and Norman Smith negotiate a staged 'Blueprint' transfer for a 5M offshore payment, with a 48-hour deadline.

Table 6. Reconstructed timeline of events, 21 Aug 2024 – 31 Jan 2025.

The timeline indicates a six-month process from an initial vague solicitation for a buyer (August 2024) to a specific staged transfer agreement with a named payment figure (January 2025) with independently recovered travel and location artifacts corroborating the meetings alluded to in the chat evidence.

4.11 Suspect Profiling - Roles & Motive Assessment

Table 7 summarizes the case-brief role and the directly linked evidence for each suspect; the discussion below sets out the conclusion on everyone's role, the supporting evidence and its limitations.

Suspect	Role	Directly Linked Evidence
Emma	Perpetrator	WhatsApp thread as herself (Figs. 7-9); Facebook thread under alias 'Peter Dover' (Figs. 10-11).
Joe	Intermediary	'Top-up' contacts on Emma's WhatsApp (Figs. 7-9); hotel/rail travel evidence on his own device (Figs. 13-15).
Norman	Buyer-side contact	Facebook thread (Figs. 10-11); GPS metadata (Fig. 12); Open.7z file anomaly (Fig. 16).

Table 7. Suspect roles and directly linked evidence summary.

Emma (Delinquent), Her own actions prove Emma instigated the disposal of the QT-AI-2025 design and appreciated its unlawful nature. The WhatsApp thread under her own name (Figs. 7-9) shows her actively seeking a buyer for 'serious stuff' as of 21/08/2024 - language consistent with market testing for a sale. The Facebook negotiation (Figs. 10-11) is entirely conducted under the pseudonym 'Peter Dover' five months later, a name which does not appear anywhere else in the evidence. The use of a false identity for a conversation discussing a 'Blueprint' and a '5M offshore' payment indicates a conscious effort to separate her real identity from the transaction. Statements such as "let's keep this clean and quick" and "after that we are ghosts" reflect a wish to conceal rather than negotiate a normal deal. The evidence, therefore, suggests intent, rather than opportunistic access, although no copy of the file itself has been recovered – to prove a completed transfer, the file or a log of the transfer/upload would be required.

Joe (middleman). Joe can be described as a knowing intermediary, but the evidence is circumstantial. There is no message on his device that mentions Norman or NexGen Circuits. The only communication we can see is with Emma, who saves him under the name 'Top-up' (Figs. 7-9) not a common name for a legitimate business contract. Evidence of travel from his own device a photograph from the Radisson Blu (Fig. 13) and rail tickets to Glasgow and Manchester (Figs. 14-15) puts him in places and at dates closely matching the 'meeting clients' references in the WhatsApp thread, supporting that he traveled at Emma's behest, although travel alone does not prove whom he met. Joe's device doesn't show direct contact with Norman so he can plausibly claim to have only acted as a contact broker. Closing this gap would require records such as hotel bookings, CCTV or a witness statement.

Norman (Buyer Contact). It can be clearly shown through the Facebook thread (Figs. 10-11) that Norman is the person who is negotiating the "Blueprint" transfer for a "5M offshore payment," but the connection of Norman with a named third-party entity as a proxy cannot be established yet since it is still an assumption at this point. The Open.7z File (Fig. 16). The Open.7z file (Fig. 16) has not been resolved and produces a hex signature indicating that it may contain a compressed or encoded material other than a standard document; the presence of an archived file outside its typical media type may constitute sufficient digital evidence in itself as a possible concealment strategy that needs further investigation. The 29 geotagged locations obtained from his device (Fig. 12), including the location in South Wales on 04/09/2024, can verify the activities performed by him at locations at certain times; however, the lack of a corresponding chat timestamp prevents establishing the connection with a specific meeting for the day.

4.12 Conclusion

Collectively, the evidence base supports in part the allegation that Emma tried to sell the QT-AI-2025 patent design via Joe to a buyer linked to Norman. The Facebook Messenger thread is direct, contemporary evidence of Emma (as 'Peter Dover') negotiating a staged 'Blueprint' transfer with Norman for a 5M offshore payment - solid evidence of intent to sell and hide the transaction. However, no copy of the QT-AI-2025 file itself, and no formal confirmation that Norman is acting for a named third party, has been recovered, so the evidence today shows only that there were negotiation and intent, not a completed or full attribution transfer. During this investigation, no illegal or otherwise unrelated contraband material was located on any of the three examined exhibits.

The strongest single exhibit is the Facebook thread, which is direct and retrieved from Emma's own device under an alias she is shown actively using. The WhatsApp thread is the next strongest, but that is based on one unverified assumption that "Top-up" is Joe which has not been formally corroborated thru subscriber-identity records. The travel evidence and GPS metadata are the least powerful exhibits of their own, since each shows presence in a location rather than attendance at a specific meeting. Their strength is in being read together with the chat timeline. The Open.7z on Norman's machine has not been figured out and should be a priority for forensic decompression

before any further conclusions are made. • Quantum Tech: immediate suspension of Emma's access to the patent database; audit recent access, downloads and transfers relating to the QT-AI-2025 file; implement tighter data-loss-prevention controls around high-value IP; preserve all three seized devices and their forensic images in anticipation of any law-enforcement request. • Law enforcement: pursue subscriber-identity verification on the 'Top-up' number to confirm its association with Joe; request Meta account-registration and login records for the 'Peter Dover' and 'Norman Smith' accounts under legal process; arrange forensic decompression of the Open.7z file; consider formal seizure and interview of Joe given unexplained travel matching the negotiation timeline.

5. Demonstration Overview

This investigation will be presented live in the Week 10 demo slot as a screen-shared walkthrough of Cellebrite Physical Analyzer, structured to take both a specialist and non-specialist audience through the same evidentiary logic as presented in this report. • Open the evidence landscape and hash-verification screens (Table 1-2, Figs. 4-6) to establish integrity before displaying any findings. • Walk thru the WhatsApp and Facebook threads live in Physical Analyzer (Figs. 7-11) and then the Instagram/email negative findings and the call-log correlation (Sections 4.6-4.7). Introduce the GPS and travel evidence (Figs. 12-15) and the unresolved Open.7z anomaly (Fig. 16), cross-referencing each against the reconstructed timeline (Table 6). Wrap up with the suspect profiling (Table 7) summary and recommendations and take questions from the panel. • Supporting materials available at the demonstration: this report, the forensic images and hash log acquired for all three exhibits, and the personal-device acquisition evidence from Section 3.

6. Personal and Technical Reflection

Having done this investigation end-to-end, from the supervised personal-device acquisition in Section 3, through to the three-exhibit case examination in Section 4, was valuable in helping to turn the theoretical chain-of-custody and hashing principles reviewed in Task 1 into working practice. The trickiest thing from a technical standpoint was how each piece of evidence was presented in three different Cellebrite case files, and the need for a single exhibit-referenced log and Physical Analyzer, to avoid cross-contamination of findings between devices. Correlating call-log timestamps against the chat evidence was also a useful reminder that the strongest cases are based on multiple independent data sources rather than any one artifact, because a challenge to the provenance of one exhibit need not undermine the whole. Areas flagged for further development were manual SQLite-level database review and deleted-data carving (both relevant to fully resolving the unopened Open.7z file) and formal subscriber-identity verification procedures (outside the scope of the tools used in this exercise, but necessary in a live investigation).