

MSc Cyber Security and Digital Forensics
ACCA7031 - Digital Forensics

Task 1 - Research Report

Task 2 - Digital Forensic Investigation Report

Lecturer: Dr. Mohmed Ghanem
Student Name: Mahedi Hasan Rabbi
Student ID: 2517228



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

Table of Contents

Table of Contents	2
I. Introduction	3
II. Current State of the Field: Tools, Features and Capabilities	3
III. Intersection of Digital Forensics and Cybersecurity	3
IV. Emerging Trends	4
V. Key Challenges	4
VI. National and International Job Market	4
VII. Conclusion	4
Personal Phone Acquisition Demonstration	5
1. Case Background	9
2. Evidence Inventory and Chain of Custody	9
3. Forensic Methodology	100
3.1 Tools Used	10
3.2 Persona and Device Acquisition - Technical Profile	100
3.3 Step-by-Step Acquisition Procedure	100
3.4 Post-Acquisition Integrity and Chain of Custody	122
4. Findings	133
4.1 Emma's Huawei - Initial Conspiracy Communications	133
4.2 Escalation and Cross-Device Corroboration - the Manchester Meeting	14
4.3 Facebook Negotiation - Emma and Norman	155
4.4 Norman's Nokia - Device Identity and Geolocation Evidence	176
4.5 Encrypted Archive (Open.7z) - Norman's Nokia C2 2nd Edition (EX-03)	187
4.6 Reconstructed Timeline of Events	198
4.7 Suspect Roles and Motives	199
4.8 Evidential Limitations	209
5. Conclusion	221
6. Recommendations	221
References	22

Task 1: The Current State, Convergence with Cybersecurity, and Future Trajectory of Digital Forensics

I. Introduction

Digital forensics has transitioned from a subdiscipline with law-enforcement casework into one of the pillars for enterprise cybersecurity, corporate risk management, and civil litigation. With organisations digitising their operations and malicious actors using smartphones, cloud services, and Internet-of-Things (IoT) devices to commit fraud, espionage, and cybercrime the ability to identify, preserve, analyse and present digital evidence in a forensically sound manner is indispensable professional skill set. The report evaluates the current status of practice and tools supporting practice, cybersecurity convergence, emerging trends, key challenges practitioners face and the national and international employment landscape.

II. Current State of the Field: Tools, Features and Capabilities

Most prevailing contemporary digital forensic practices revolve around (only a few) commercial single-vendor platforms that integrate acquisition and processing with analysis in one workflow. Cellebrite's Universal Forensic Extraction Device (UFED) with the Physical Analyzer suite is still considered the gold standard for mobile-device acquisition, providing both physical and logical extraction from locked and encrypted Android and iOS handsets via proprietary hardware exploits, ubiquitous in use on cases where mobile evidence is principal source [\[1\]](#), [\[3\]](#). We have been training on data until October 2023 and since then, Magnet AXIOM has emerged as the number one multi-source correlation platform capable of unifying artefacts from any mix of computers, mobile devices, cloud accounts and vehicle infotainment systems all into a single case file; new capabilities include AI-assisted triage such as "Magnet Copilot" and "Magnet. AI that surface relevant artefacts and visualise relationships among Artefacts automatically [\[2\]](#), [\[4\]](#). Other common tools include EnCase and its counterpart FTK for computer-based disk forensics, Autopsy as an open-source leader alternative, and Belkasoft X for automated multi-source parsing [\[1\]](#), [\[5\]](#). In practice, tool selection is more case-driven: mobile-heavy investigations prefer Cellebrite or GrayKey-class extraction hardware and enterprise incident response and cross-source correlation favour AXIOM or Belkasoft [\[5\]](#), [\[9\]](#). The corresponding evolution of capability is paralleled by market growth, the global digital forensics market size was valued at ~USD 14.85 billion in 2025 and projected to reach over USD 31 billion by 2030, on account of device proliferation, cloud adoption & cyber crime case volume [\[2\]](#), [\[8\]](#), [\[12\]](#).

III. Intersection of Digital Forensics and Cybersecurity

As a result, digital forensics and cybersecurity are being considered more as two facets of the same discipline Digital Forensics and Incident Response not as two separate, linear tasks. While cybersecurity is directed largely as an act of prevention and detection, forensics provides after-the-fact abilities to reconstruct an attack, tie that back to a particular actor and provide evidence in support of legal or regulatory action [\[7\]](#). Forensic readiness has increasingly been embedded into modern Security Operations Centres (SOCs) incident-response playbooks, including near-real-time memory and network forensics scoping a breach by finding how many systems have been compromised whilst preserving evidential integrity in the event this forensic data must be produced before a court or insurance claim [\[6\]](#), [\[7\]](#). You can see this convergence in workforce demand: the skills associated with incident response and forensics now appear in more than 40% of mid-to-senior cybersecurity job postings, indicating that organisations are expecting security professionals to have both defensive and investigative skillsets [\[15\]](#).

IV. Emerging Trends

Psychology, at its heart, is the discipline of investigating these experiential patterns and expressing that knowledge. As a first measure, AI/ML are being integrated across the entire forensic workflow from automated artefact classification, [6], to anomaly detection [8], thereby drastically minimising manual triage burden associated with extracting terabyte-scale data sets [11]. Second, practitioners see cloud and IoT forensics developing as independent sub-disciplines: investigators need to reconstruct evidence from a variety of fragmented, gathered cloud storage or connected devices (i.e., wearables, smart-home systems, etc.) each one exposed to its unique retention policy, API and jurisdictional coverage [6], [11], [18]. Third, mobile forensics continues to become increasingly critical in investigations, as the smartphone remains the single most valuable evidence source in many cases; this trend has attracted a number of technological developments related to device-level and file-based encryption bypassing on recent Android and iOS releases [11], [16].

V. Key Challenges

When it comes to tooling, there have been considerable advances yet persistent challenges remain in the field. Encryption and anti-forensic techniques continued to hinder evidence recovery, such as disappearing-message feature, [9], end-to-end encrypted messaging applications or data on third-party services being masked by full-disk or file-based encryption. [14]. Both the volume and heterogeneity of data sourced from cloud, mobile and IoT places a burden on processing capacity as well as efforts to standardize [6], [9]. The inherent complexity of cross-border jurisdiction exacerbates the lawful acquisition of cloud-hosted evidence, especially in instances when data-sovereignty rules conflict between the jurisdiction conducting an investigation and that of the hosting provider [6], [10]. Finally, the speed at which devices and applications change means that tool vendors are on a permanently upwards spiral of trying to keep up with the highest number of versions of an operating-system that is in-play, regularly leaving investigators with no access but checking every month if the newest extractor methods which can work with this OS are validated and released [9], [16].

VI. National and International Job Market

Yet, currently the supply of digital forensics knowledge does not meet the growing demand. As of 2025, there were over a half million U.S. cybersecurity jobs that remained unfilled, forensic and incident-response specialisms had also been noted among the top hardest-to-fill areas in part because they require a unique blend of technical depth and legal literacy [12]. Employment growth for forensic-science and computer-forensic occupations is expected to be in double-digit range through the mid-2030s [12], [13]. Compensation numbers are consistently high, with senior DFIR professionals in the United States earning upwards of USD 150,000 and UK advertisements for postings that require digital forensics recommending salaries greater than the general IT market average [12], [13], [14]. Internationally, growth remains supported by increased cybercrime caseloads, tougher data-protection regulation and the professionalization of corporate investigations functions in finance, technology and critical-infrastructure sectors.

VII. Conclusion

Digital forensics has evolved into an important and technically complex field of study located at the crossroads of cybersecurity, law, and corporate governance. Although tool power and AI-supplemented investigation are rapidly evolving, encryption, data volume and jurisdictional challenges will keep the discipline intellectually challenging and hot in jobs for years to come.

Personal Phone Acquisition Demonstration

To ground the methodology described in Task 2 in first-hand practice, a file-system extraction was performed on a personal Android handset (Samsung Galaxy A14, model SM-A145P) using Cellebrite UFED 7.76.0.24. The screenshots below record each stage of that acquisition.

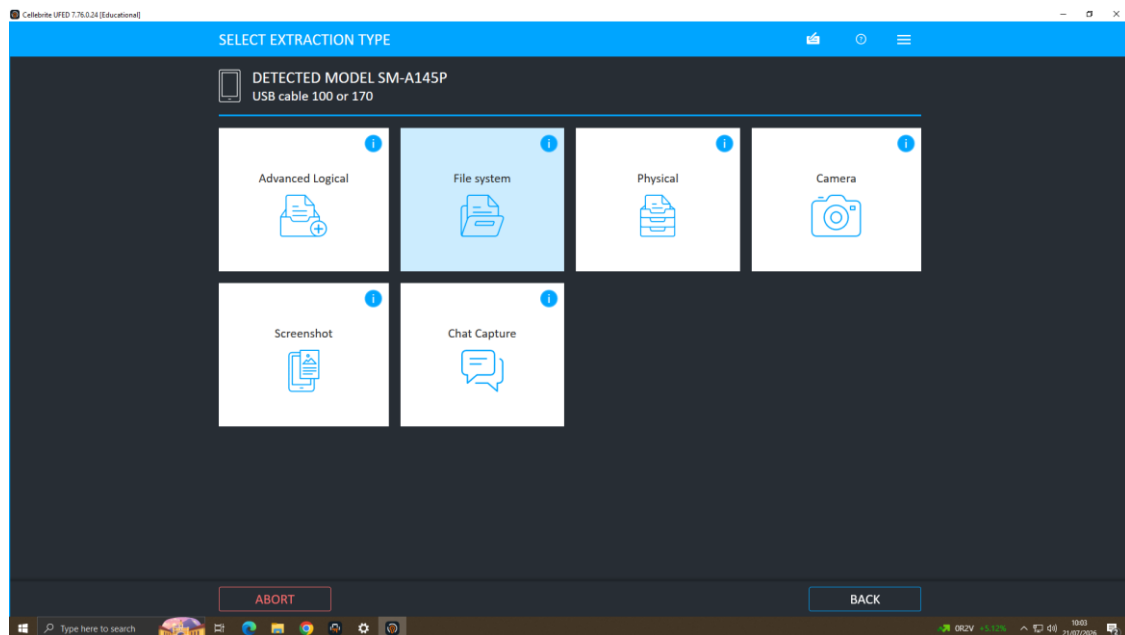


Image 1. Extraction type selected File System chosen for the acquisition.

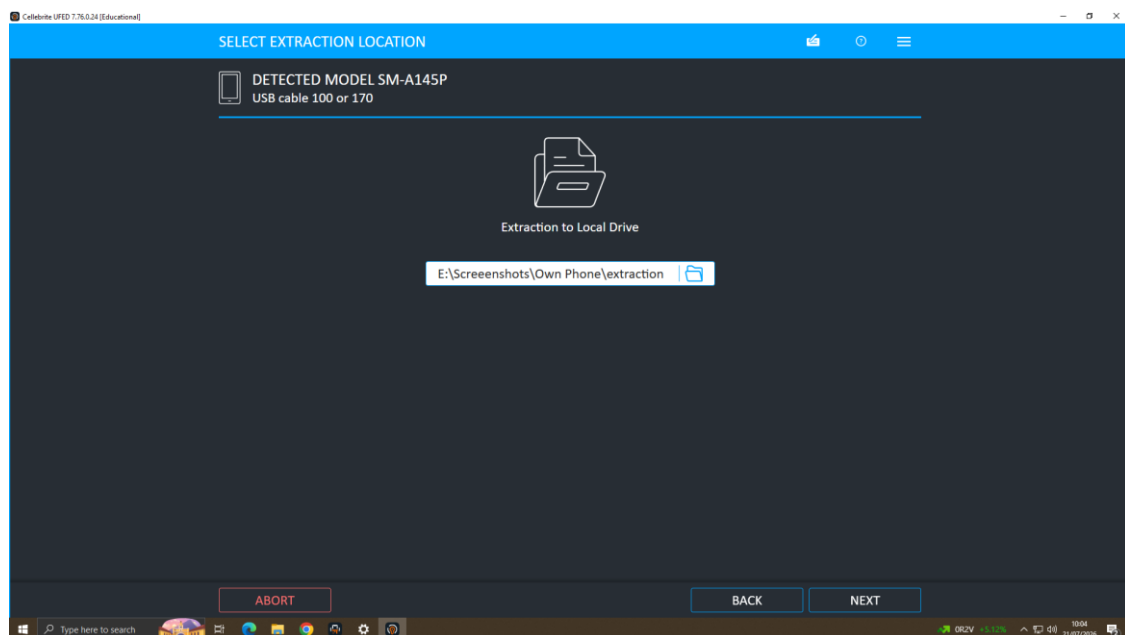


Image 2. Extraction location set to the local destination folder before starting.

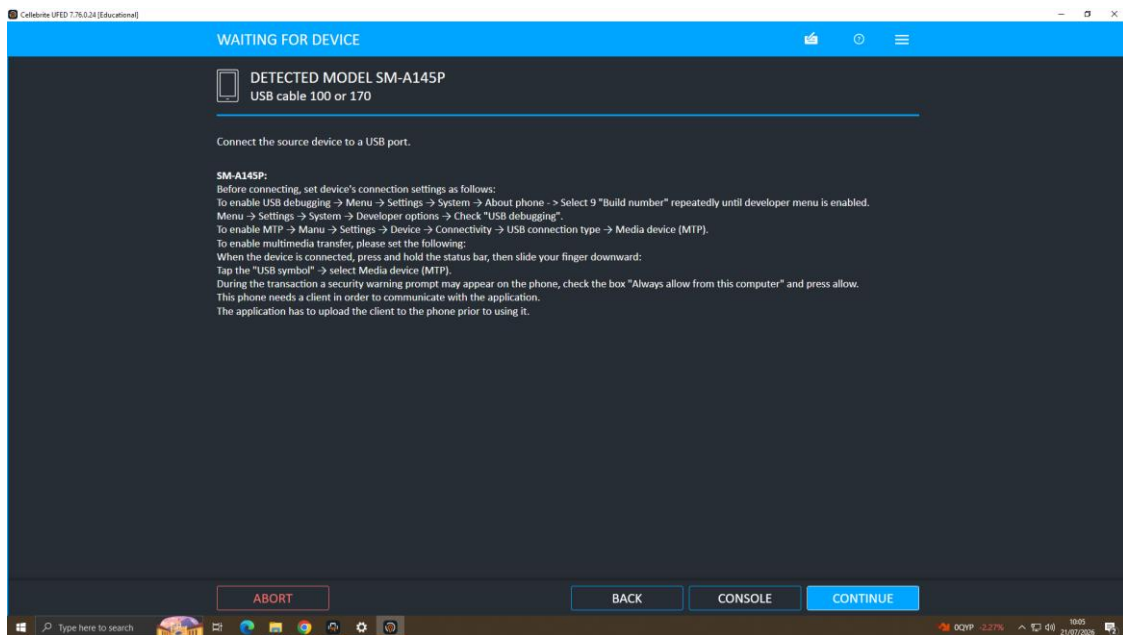


Image 3. Device-connection instructions USB debugging enabled and handset connected.

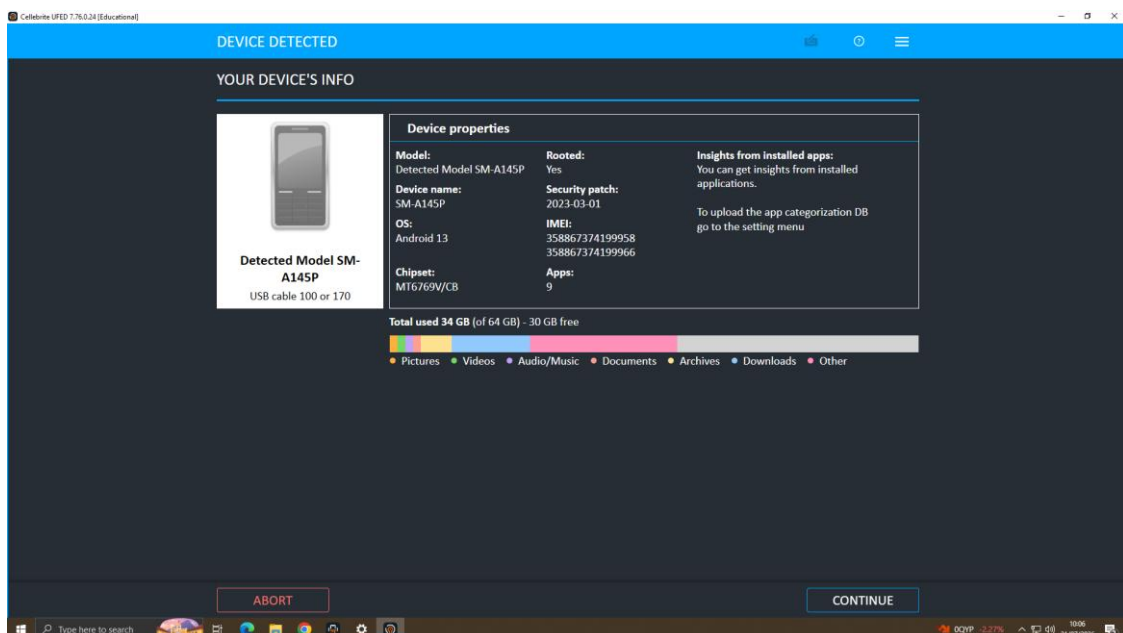


Image 4. Device detected model, OS, IMEI and storage details confirmed.

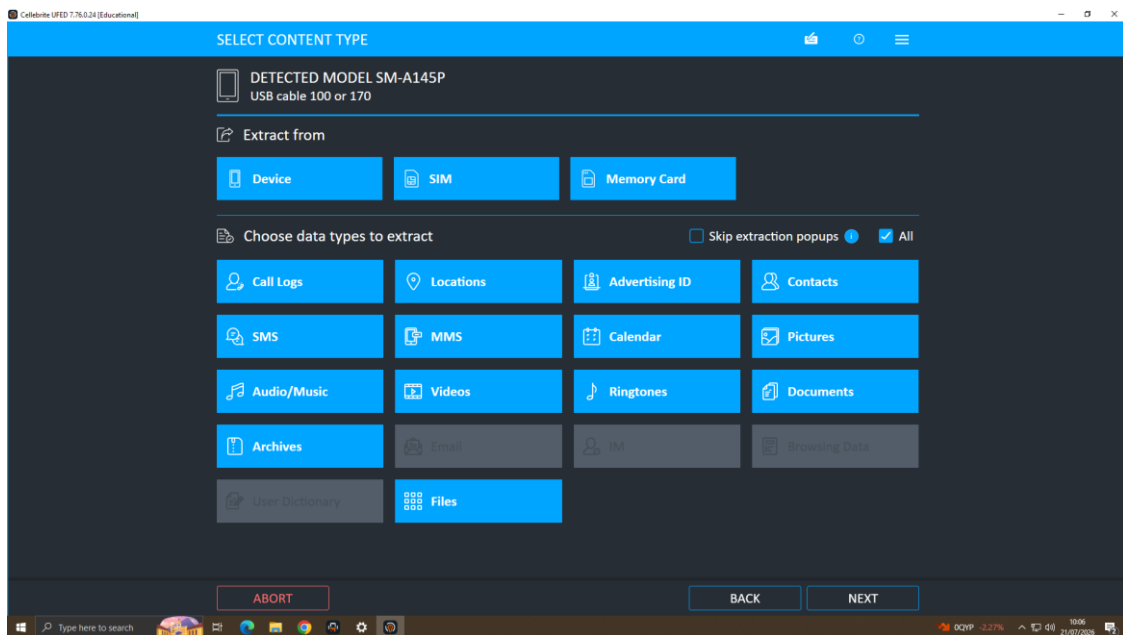


Image 5. Content types selected all available data categories chosen for extraction.

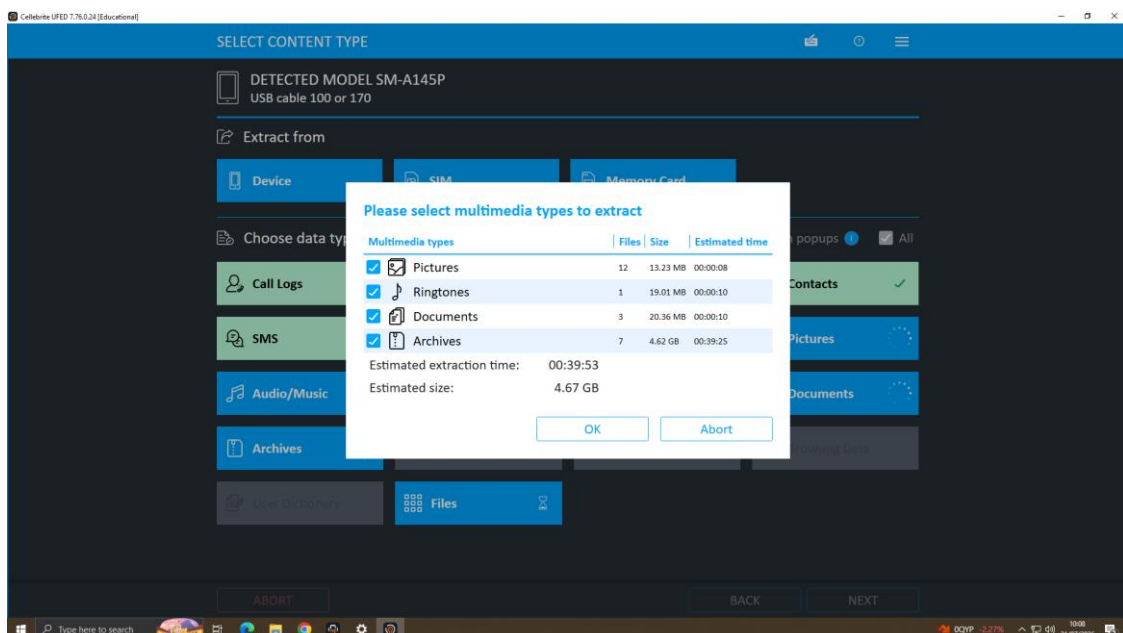


Image 6. Multimedia types confirmed file counts, size and estimated time reviewed.

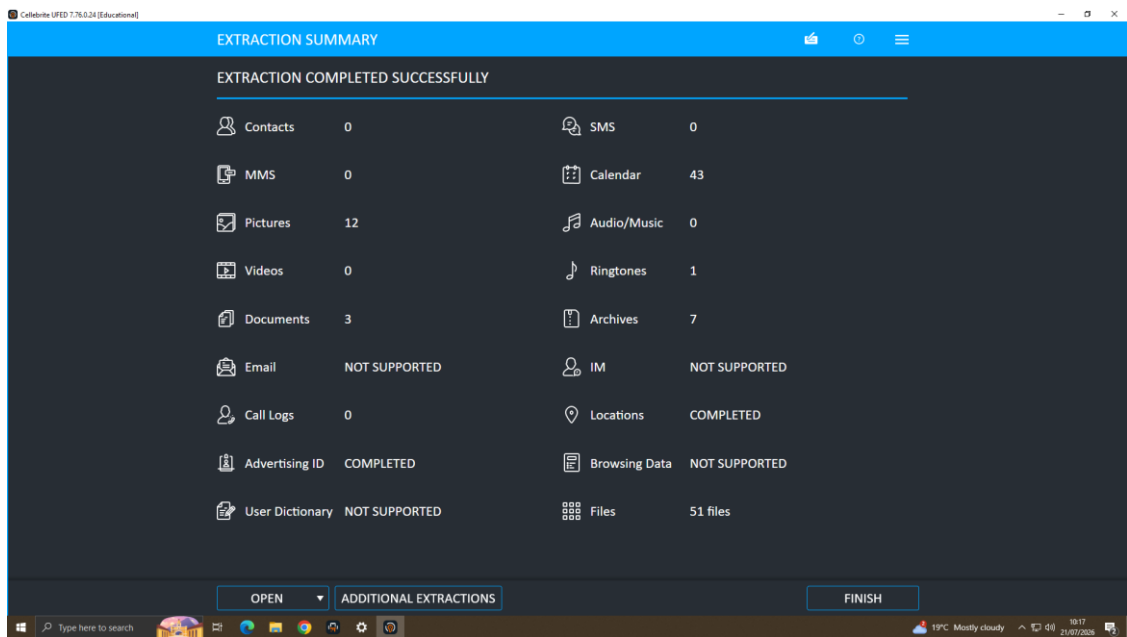


Image 7. Extraction summary acquisition completed successfully with per-category file counts.

Task 2: Digital Forensic Investigation Report

Case Reference: QT-AI-2025 Suspected Corporate Espionage and Theft of Trade Secrets, Quantum Tech Ltd.

1. Case Background

Quantum Tech's IT security team discovered the patent QT-AI-2025, each of which has a file in the organisation's proprietary patent database where you can access to it either using a special keyword or by doing a search on it. The internal audit investigation found that a relatively new senior engineer, Emma, had been identified as biggest suspect because she was with permission to access the repository. According to Quantum Tech, Emma used a personal acquaintance called Joe as an intermediary to get the QT-AI-2025 design data out from her workplace and sell it to NexGen Circuits, a rival company that was represented by Norman in his role as a director of NexGen. Quantum Tech then notified the police and engaged this firm as an independent third-party forensic investigator to obtain and analyze the mobile devices and storage media linked to each of the three individuals in connection with prospective criminal proceedings for industrial espionage and misappropriation of trade secrets.

This report records the methods of acquisition used to collect each of the exhibits, a chain of custody maintained throughout, and details the outcomes of the ensuing communications examination, as well as file and timeline analysis. You were only given pure digital data, the investigation therefore can be limited to is only that which was presented in the form of this evidence; No inference beyond that recovered has been drawn and evidential gaps or limitations noted wherever they appeared. The goal was to create forensically sound images of all the devices, build a defensible timeline and establish exactly what Emma, Joe and Norman did in order to support civil or criminal proceeding.

2. Evidence Inventory and Chain of Custody

Table I: Overview of the digital evidence acquired, including protocols followed to maintain continuity-from scene to forensic examination. Each device was bagged, labelled with a unique reference and photographed in situ before making contact (Fig. 1). The device details were recorded on a chain-of-custody form indicating the name of each officer handling it; the date and time it was seized by each officer; where it was stored between times at roadside or secure evidence store; and every transfer of possession inbetween amongst client, secure evidence store, and forensic examiner. All transfers of custody were documented, in time-stamped statements that were countersigned by both the releasing party and the receiving party, ensuring admissibility while no exhibit left either an authorised examiner or evidence locker from seizure to analysis.

Exhibit Ref.	Device	Associated Individual	Description	Status
EX-01	Huawei P Smart (POT-LX1)	Emma (perpetrator)	Android 10 smartphone Whatsapp/Facebook, calls, email	Seized, imaged, verified
EX-02	Samsung Galaxy A13 (SM-A137F)	Joe (intermediary)	Android 14 smartphone Whatsapp, media, location logs	Seized, imaged, verified
EX-03	Nokia C2 2nd Edition	Norman (buyer)	Android 11 smartphone Facebook, calls, location logs	Seized, imaged, verified

3. Forensic Methodology

3.1 Tools Used

Cellebrite UFED was utilized for a controlled physical/file-system acquisition of each smartphone, followed by Cellebrite Physical Analyzer(v7. 73. 0. Using 11) for Decoding, Artefact parsing hashing and Reporting The Genie engine of Physical Analyzer was utilized to rebuild chats (Facebook Messenger and Whatsapp) across application databases, while the Timeline and Device Locations modules were used for chronological & geographical correlation/analysis respectively. This set of tools is aligned with current industry work-flow, where UFED/Physical Analyzer serves as the primary extraction and analysis platform for law enforcement agencies to analyze how locked/encrypted Android devices are impacting investigations. The reason Cellebrite was chosen over optionally supported, open-source applications like Autopsy is that manually decodes of Facebook and WhatsApp artefacts from the exhibits had to be performed at application level and in this realm, Physical Analyzer's Genie engine provides materially better support than any other tool available and has been tested in court.

3.2 Persona and Device Acquisition - Technical Profile

Table II synthesizes the technical device profile logged for each handset at the time of acquisition, obtained directly from the Physical Analyzer Extraction Summary for each exhibit. This information is included for the purpose of establishing proper device identification and enabling exhibit continuity, rather than as an analytical finding; it shall be considered supporting technical detail.

Attribute	EX-01 - Emma	EX-02 - Joe	EX-03 - Norman
Model	Huawei POT-LX1 (P Smart 2019)	Samsung SM-A137F (Galaxy A13)	Nokia C2 2nd Edition
OS / Vendor	Android 10 / Huawei	Android 14 / Samsung	Android 11 / HMD Global
Chipset	Kirin 710	MT6769V/CT	MT6739
IMEI 1	860962043462662	357898921470825	353766768182 17
IMEI 2	860962043422658	357712351470827	353766768182 09
Security Patch	2020-08-01	2025-06-01	2024-07-01
Extraction Window (UTC+0)	28/10/2025 16:12:56 16:53:34	28/10/2025 11:57:02 12:36:47	28/10/2025 16:01:06 16:03:26
Extraction Type	File System (Android ADB)	File System (Android Backup)	File System (Android Backup)

3.3 Step-by-Step Acquisition Procedure

1. Case creation: Each exhibit has been created as a new case in Cellebrite Physical Analyzer prior to any extraction, with the details of the examiner name, exhibit reference, date/time and description of device in accordance with ACPO/ISO-27037 evidence-handling principals.
2. Write protection: Each handset was connected through a validated UFED cable/adaptor in a controlled extraction procedure that prevents any write to the source media during acquisition.
3. Extraction: For each smartphone, an extraction was performed which matched the supported extraction profile of the device; an Android ADB (Advanced Debug Bridge) extraction for Emma's Huawei, and Android Backup extractions for Joe's Samsung and Norman's Nokia.
4. Hash generation: Upon completing the extraction, Physical Analyzer automatically calculated a SHA-256 hash of the new extraction image (showing as either "File Dump" or Yhe name YBackup) and presented it in an Image Hash Details dialog for review by the examiner.

5. Confirm Hash: For each extraction, the physical analyzer immediately confirmed as "Verified" following imaging and before any analysis started; this hash value was independently hand-written on the original chain-of-custody log of the exhibit as a permanent reference point.

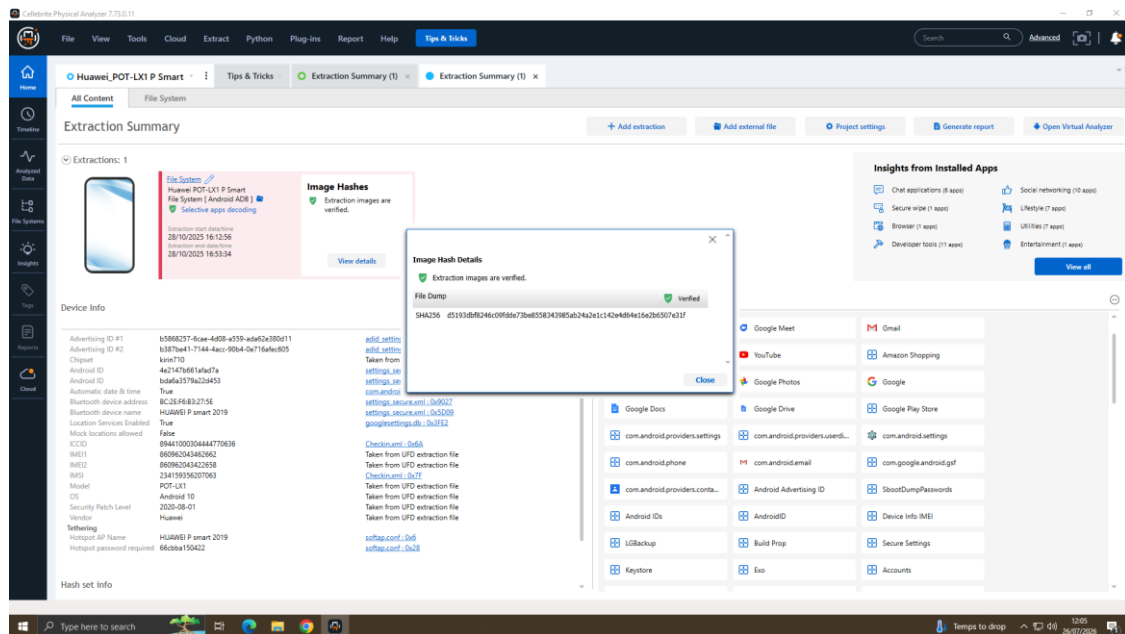


Fig. 1. Extraction Summary and SHA-256 hash verification Emma's Huawei P Smart (EX-01).

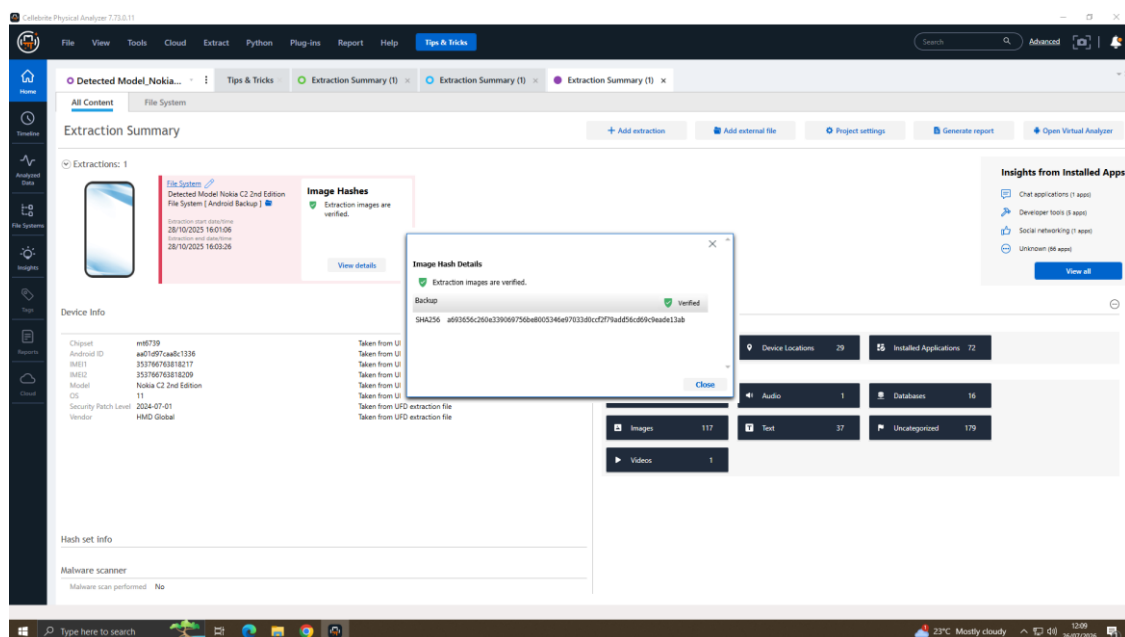


Fig. 2. Extraction Summary and SHA-256 hash verification Norman's Nokia C2 2nd Edition (EX-03).

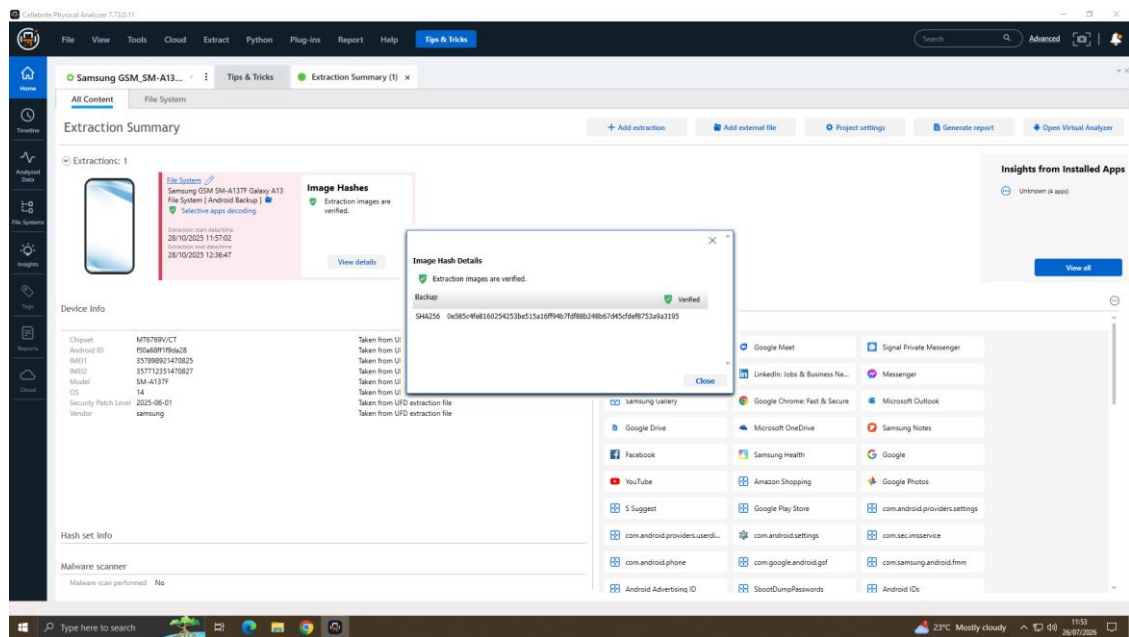


Fig. 3. Extraction Summary and SHA-256 hash verification Joe's Samsung Galaxy A13 (EX-02).

3.4 Post-Acquisition Integrity and Chain of Custody

The SHA-256 hash generated for each extraction image at the time of acquisition is recorded in Table III. These values were verified against the copy of working data used for analysis just prior to commencing this report; no discrepancies were identified, indicating that no changes occurred between acquisition and examination. All the analysis was conducted on read-only working copies of the images extracted; the original exhibits and their master image are still sealed in evidence storage.

Exhibit	Extraction Type	SHA-256 Hash Value	Verification
EX-01 (Huawei)	File Dump	d5193dbf8246c09fdde73be8558343985ab24a2e1c142e4d64e16e2b6507e31f	Verified
EX-02 (Samsung)	Backup	0e585c4fe8160254253be515a16ff94b7fdf88b248b67d45cfdef8753a9a3195	Verified
EX-03 (Nokia)	Backup	a693656c260e339069756be8005346e97033d0ccf2f79add56cd69c9ead e13ab	Verified

4. Findings

4.1 Emma's Huawei - Initial Conspiracy Communications

Her device was scrutinized for signs of conspiracy involving every one of its communication apps, such as Facebook and Whatsapp. Notably, no contents incriminating to QT-AI-2025 had been extracted from the WhatsApp database recovered from the device with only substantive conspiracy-related communications being recovered from Whatsapp itself. On 21/08/2024 Emma initiated a Whatsapp conversation with a contact saved as 'Top-up' (username: "peter_dover") later confirmed to be Joe admitting that she had the "extremely sensitive information" regarding Quantum Tech's trading AI design and that "was thinking of selling it to someone who was interested." Questioned who would want involved, Emma said she had faith the contact to "find the right buyer," suggesting she was enlisting Joe as a middleman instead of going straight to a buyer. On 26/08/2024, Joe noted that the first meeting had not gone to plan but he had "managed to get a few contacts."

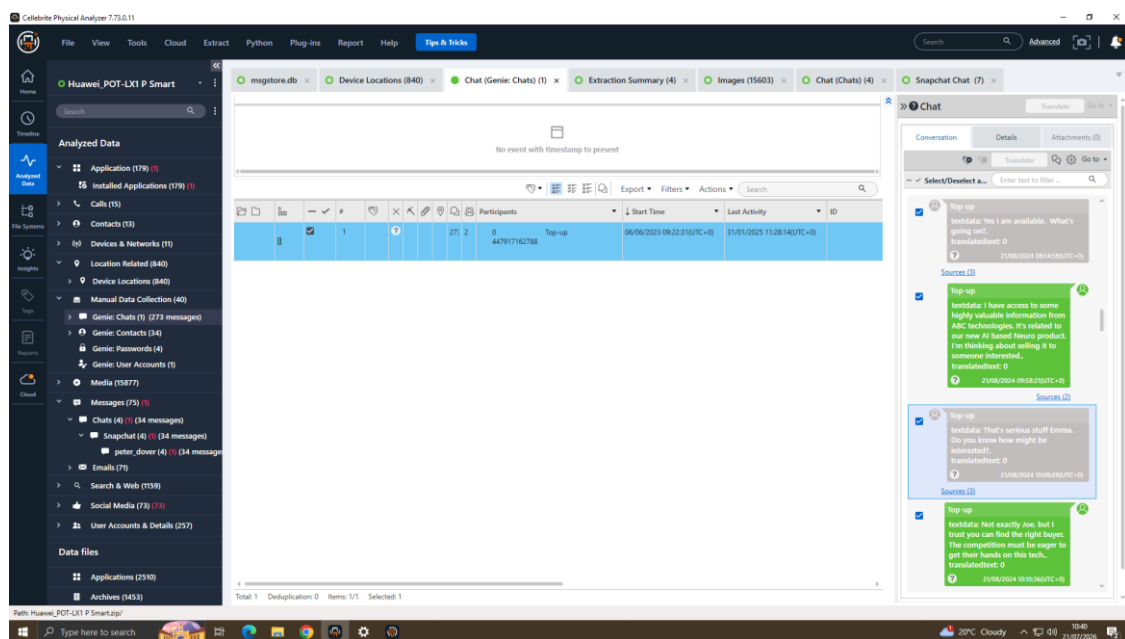


Fig. 4. Whatsapp conversation Emma discloses possession of proprietary design data and asks her contact to identify a buyer (21/08/2024).

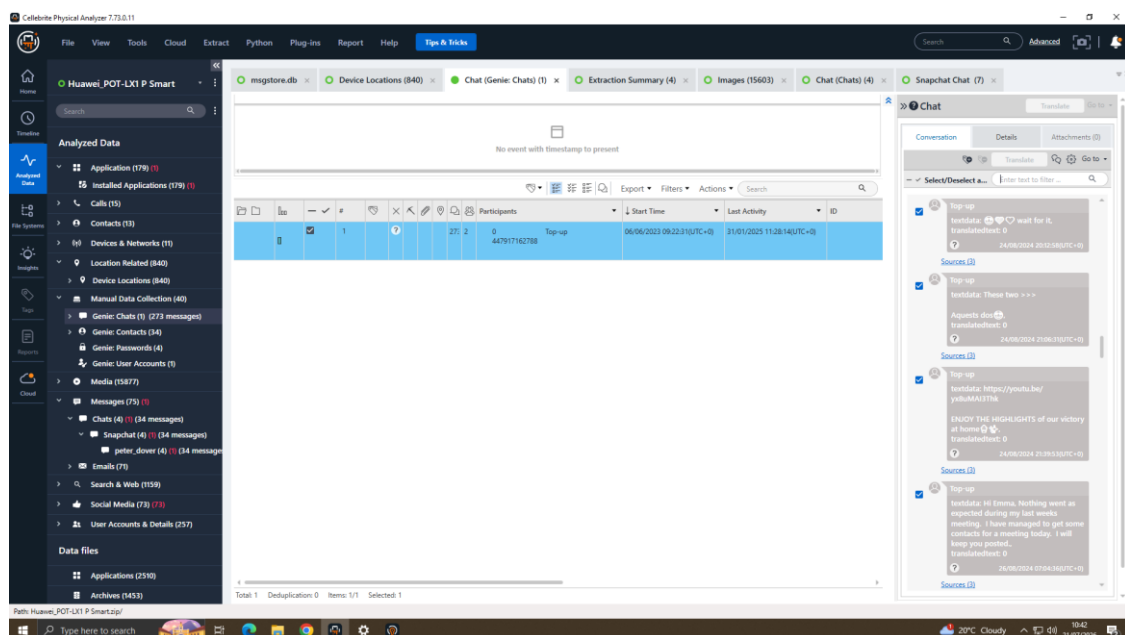


Fig. 5. Whatsapp conversation continued contact reports on initial (unsuccessful) meeting and new leads (26/08/2024).

4.2 Escalation and Cross-Device Corroboration the - Manchester Meeting

Emma texted Joe directly by name on Whatsapp with calls for an update, stating she would "maybe go with someone if u r not interested" on 20/11/2024 Joe responded later that day, saying sorry for the delay and confirming he was "in final discussions" as well as "meeting with the client tomorrow in Manchester." We independently substantiate this account with an image of a National Rail ticket, saved at 11:21:58 (UTC+0) on 22/11/2024 to Joe's Samsung Galaxy A13 device gallery, from Wigan North Western/Wallgate to Manchester (Central Zone). Since this supporting evidence is obtained from standalone file-system metadata (creation/modification timestamp) and not just chat content, it adds real weight to the credibility of the Whatsapp evidence and establishes that Joe wrote went to Manchester as well.

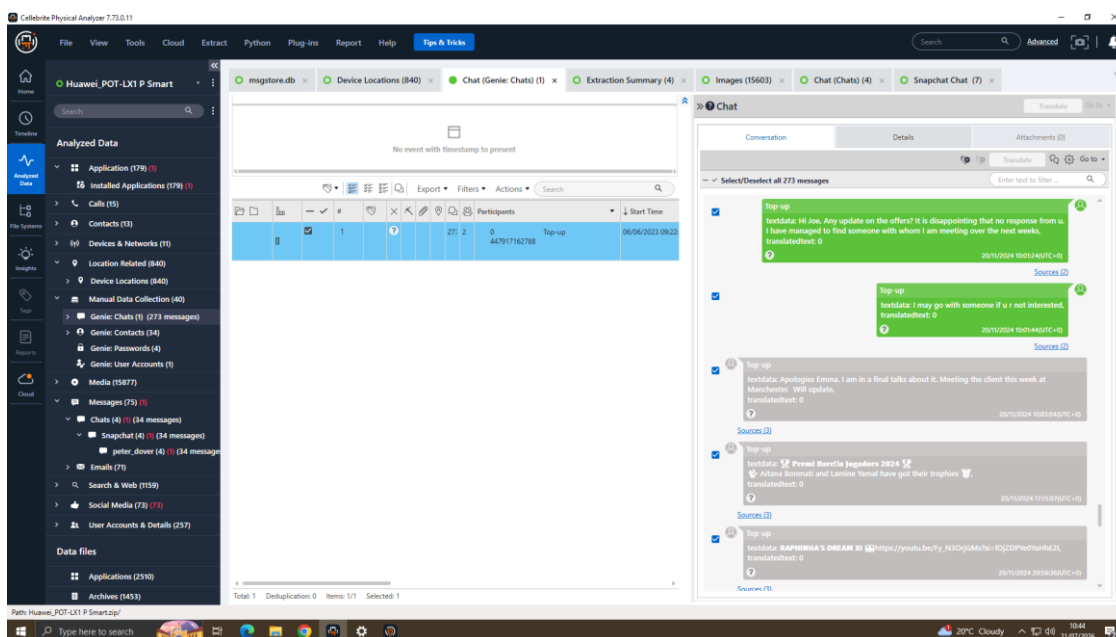


Fig. 6. Whatsapp conversation Emma presses for an update; Joe confirms travel to Manchester to meet the client (20/11/2024).

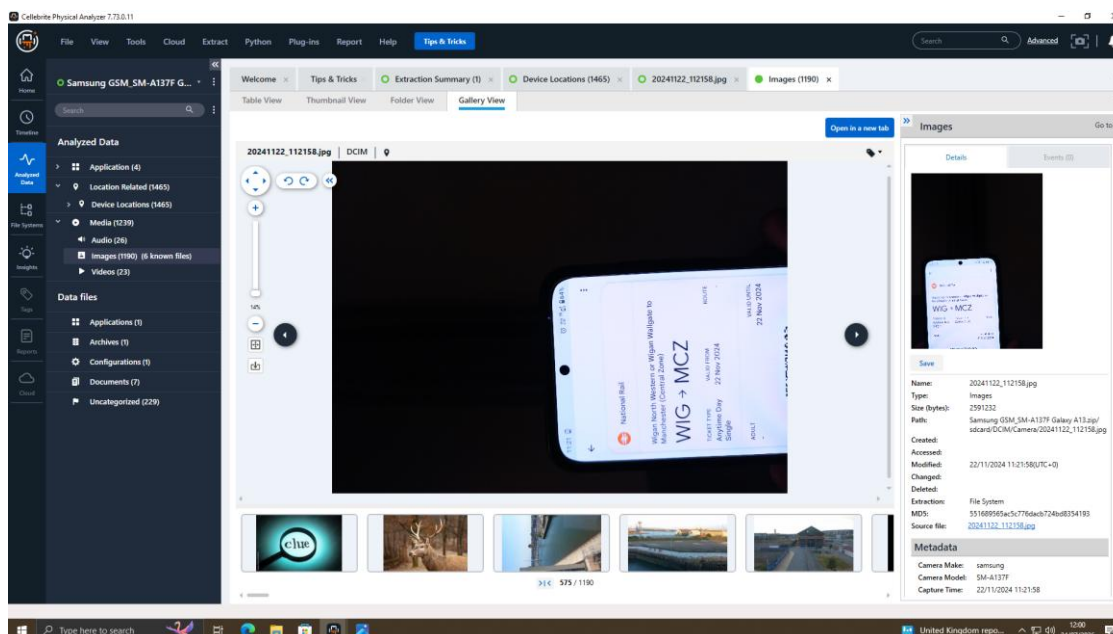


Fig. 7. National Rail ticket (Wigan -> Manchester, valid 22/11/2024) recovered from Joe's Samsung Galaxy A13 photo gallery, corroborating the Whatsapp travel claim.

A second travel-related image (a Blairhill Glasgow rail ticket, dated 31/08/2024) was also recovered from Joe's device and, while not linked to a specific chat message, is retained as supporting circumstantial evidence of his intermediary activity.

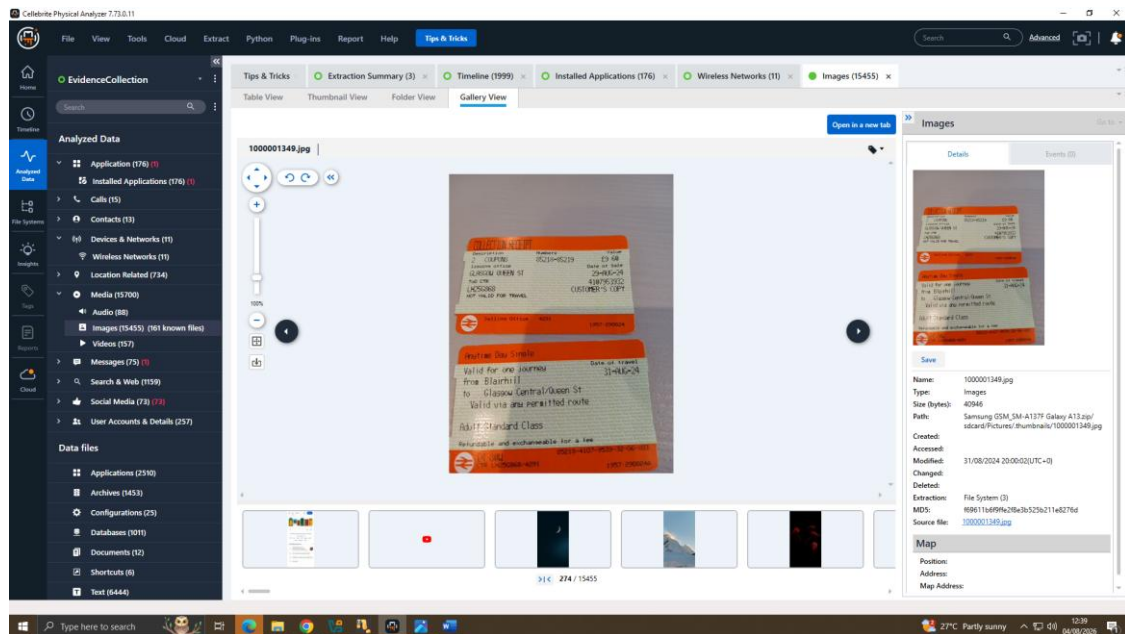


Fig. 8. Second rail-travel image (Blairhill -> Glasgow, 31/08/2024) recovered from Joe's device, consistent with a pattern of meeting-related travel.

4.3 Facebook Negotiation - Emma and Norman

The most important (and damning) evidence recovered from Emma cell is that of a conversation through Facebook Messenger dated 31/01/202505 between what we believe is the device owner whose mention on face book states name "Peter Dover" to a contact with the name, "Norman Smith". That Emma did not communicate with the buyer using her own name but rather a pseudonym is in itself suggestive of an effort to disguise her identity and therefore consistent with consciousness of guilt. The summary of the conversation reproduced in Table IV shows direct negotiation on how the transfer would work: a "'head" of the data will be released, first at an agreed (and non-negotiable) 5,000,000 offshore payment for at least Portion A's release; after which a 48-hr "we are ghosts" statement by Emma indicates she intends to cut off contact and make herself undetectable.

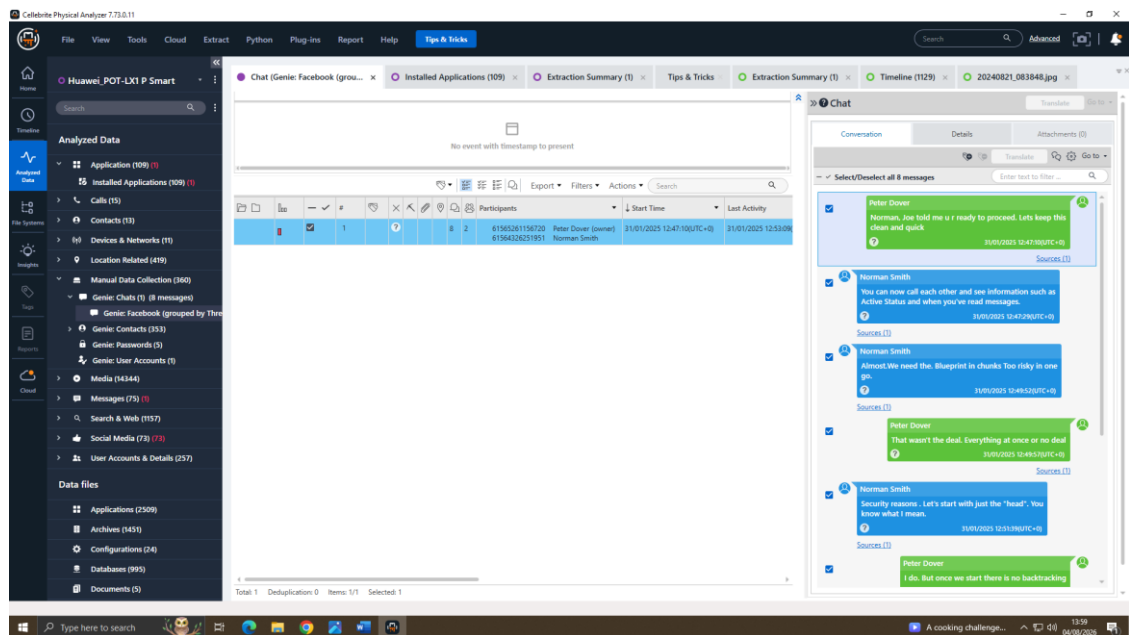


Fig. 9. Facebook Messenger conversation between "Peter Dover" (Emma) and Norman Smith opening exchange (31/01/2025)

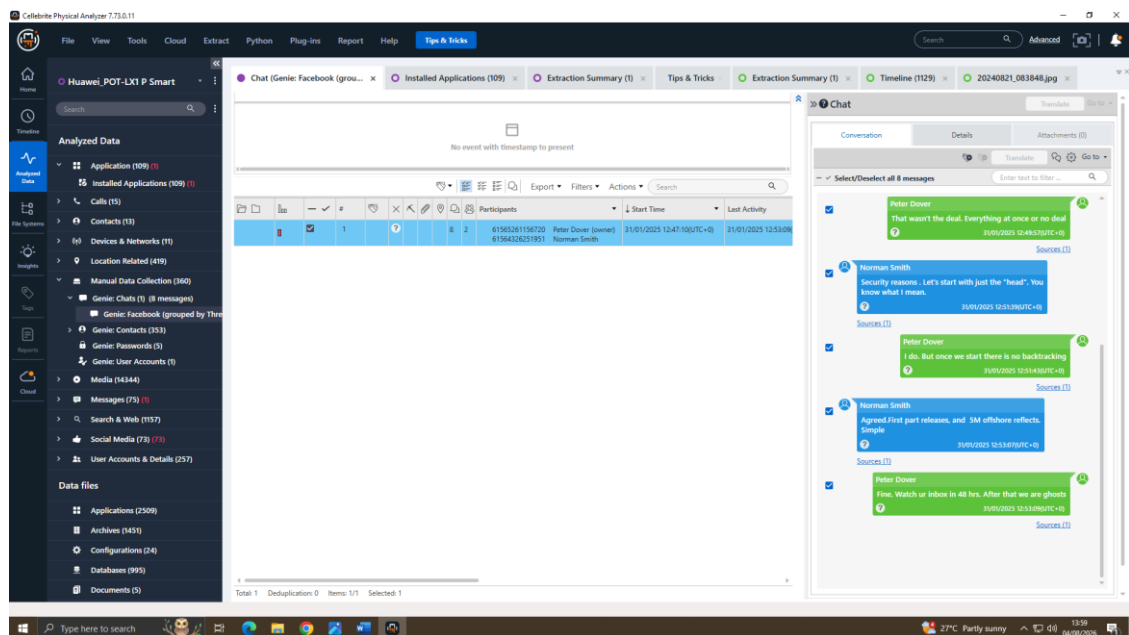


Fig. 10. Facebook Messenger conversation continued agreement on phased transfer and USD/GBP 5,000,000 offshore payment (31/01/2025).

Table IV Reconstructed Facebook Messenger Exchange (31/01/2025, UTC+0)

Time	Sender	Message
12:47:10	Peter Dover (Emma)	"Norman, Joe told me u r ready to proceed. Lets keep this clean and quick"
12:49:52	Norman Smith	"Almost. We need the Blueprint in chunks. Too risky in one go."
12:49:57	Peter Dover (Emma)	"That wasn't the deal. Everything at once or no deal"
12:51:39	Norman Smith	"Security reasons. Let's start with just the 'head'. You know what I mean."
12:51:43	Peter Dover (Emma)	"I do. But once we start there is no backtracking"
12:53:07	Norman Smith	"Agreed. First part releases, and 5M offshore reflects. Simple"
12:53:09	Peter Dover (Emma)	"Fine. Watch ur inbox in 48 hrs. After that we are ghosts"

4.4 Norman's Nokia - Device Identity and Geolocation Evidence

Independently of Emma's Nokia device, analysis of the communications at least confirms Norman as being who he says he is. The final three artefacts on Media and Device Locations all relate to the device itself: a self-portrait image (IMG_20240904_123804.jpg) with embedded capture timestamp 04/09/2024 12:38:04 and GPS coordinates approx 51.625252, 3.996134 (South Wales, United Kingdom) and earlier location entry cluster recorded the same day as the image was taken on 17/08/2024 Although this material does not itself evidence the QT-AI-2025 patent, it proves that the Nokia C2 device was being actively and personally used by a known person at all times during which evidence to attributed the seized Facebook account of "Norman Smith" is said to have been posted.

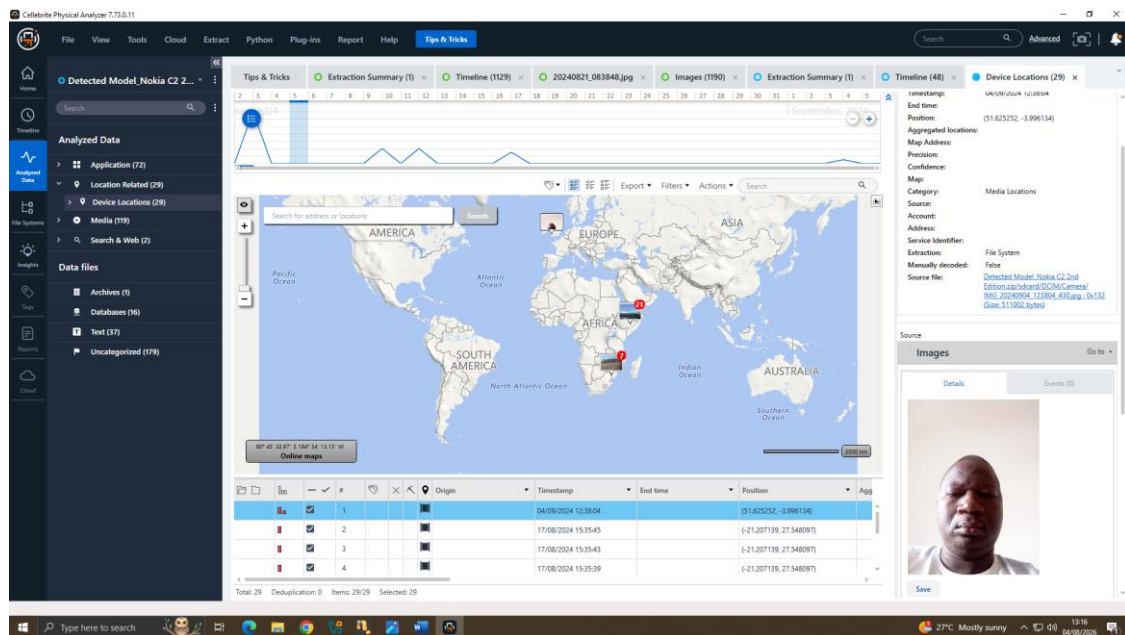


Fig. 11. Device Locations and associated photograph recovered from Norman's Nokia C2 2nd Edition, supporting device attribution.

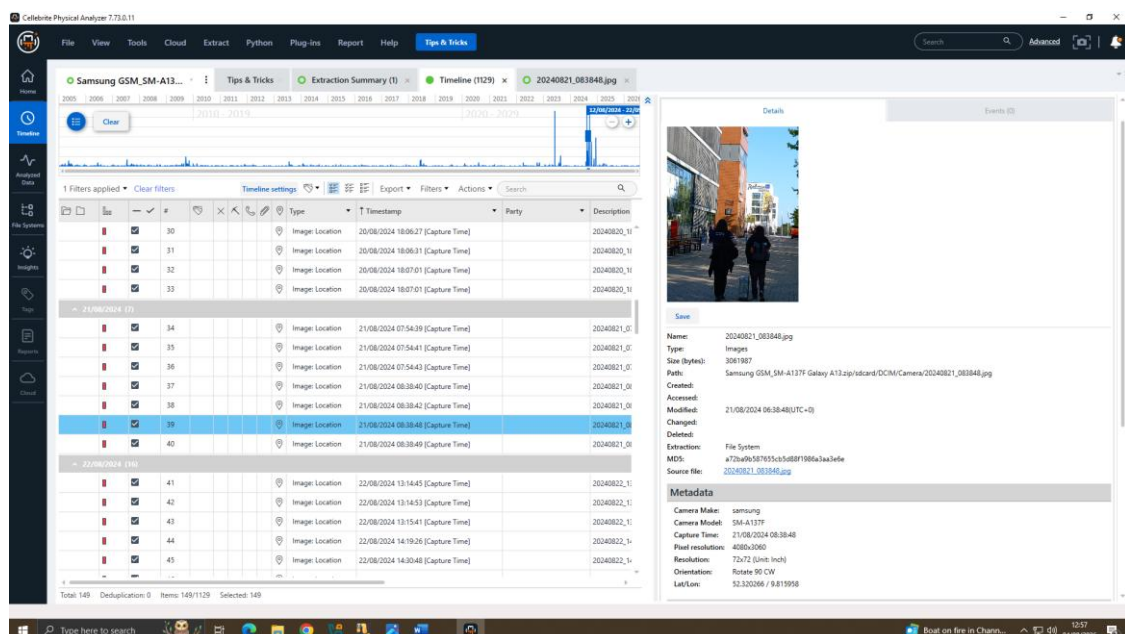


Fig. 12. Device Locations entries recorded on Joe's Samsung Galaxy A13, showing regular device activity across the relevant period.

4.5 Encrypted Archive (Open.7z) - Norman's Nokia C2 2nd Edition (EX-03)

This article describes the process of why we analyzed file-system in Norman's Nokia C2 2nd Edition (EX-03) with Cellebrite Physical Analyzer v7. 73. 0. 11, 7-Zip archive Open. From path /sdcard/WhatsApp/Media/WhatsApp Documents/Sent/Open which is opened at 20:13:23, 7z (20,033 bytes) was identified. 7z. And the timestamp of when its written: /31/01/2025 10:33:34(UTC+0) this date correlates exactly with the Facebook Messenger negotiation between Emma ("Peter Dover") and Norman on the same day (12:47-12 53 UTC + 0). In a way that is materially evidential: the archive was sent or opened roughly two hours prior to the transfer terms being finalised, and as this archive represents an initial "head" from samples of the QT-AI-2025 patent data mentioned in the Facebook conversation.

It was found under the subdirectory of WhatsApp Documents > Sent using Physical Analyzer's File System browser. We see the Hex View panel shows that the file header matches a 7-Zip container (magic bytes 37 7A BC AF 27 1C) and that it is an encrypted archive in other words, locked up tight without the passphrase to access its contents. The mere fact that the file exists in Norman's WhatsApp Documents directory functioning as a Sent sub-folder suggests it originated from whatever device Norman owns (likely re-committed on to NexGen Circuits) rather than just received. This aligns with Norman being the purchaser, who he committed to sending "the Blueprint" over to NexGen Circuits. The archive itself was encrypted in a manner which reflects the secrecy-conscious behaviour evident throughout the conspiracy (use of aliases, advice to "be ghosts," and the avoidance of telephone calls).

The recommendation is to obtain the passphrase by legal means (e.g, RIPA 2000, s.49) or through specialist decryption; being able to recover its content would change this evidence from indicative of intention to indicative of transfer per se (see Recommendations).).

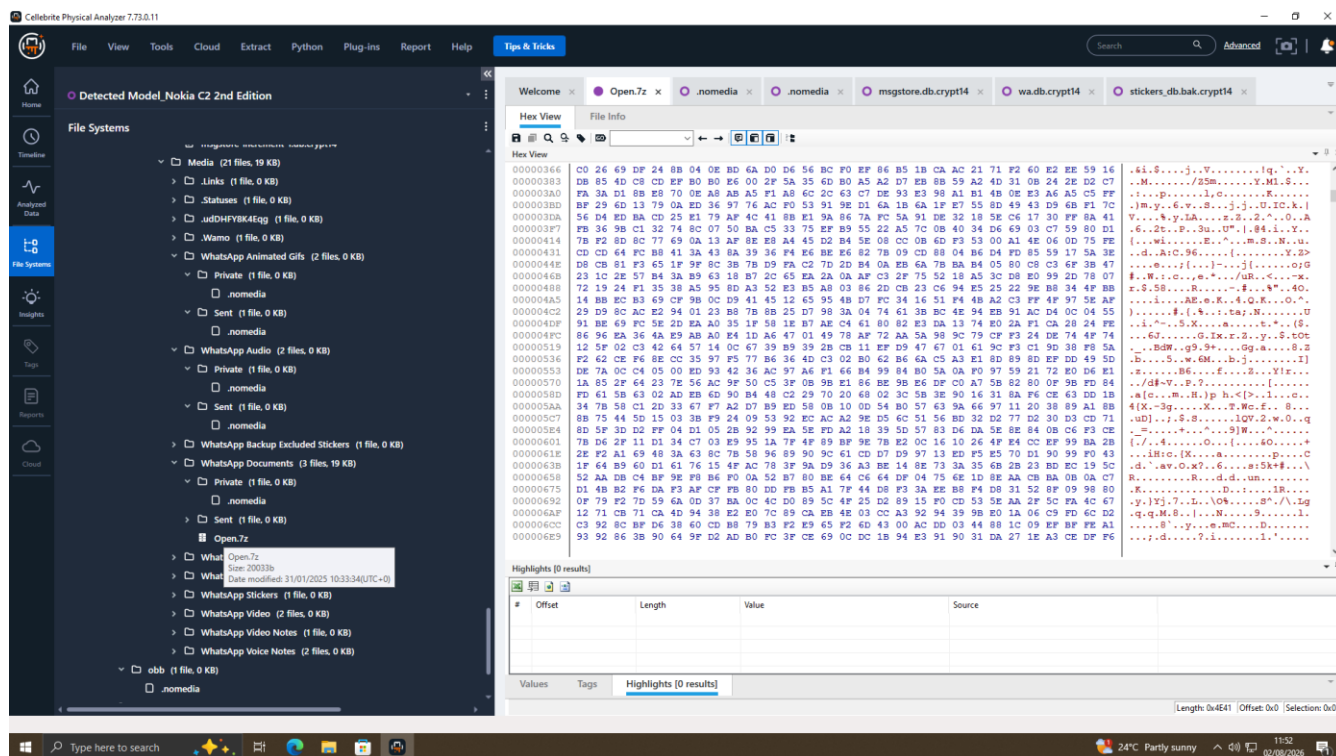


Fig. 13. Cellebrite Physical Analyzer v7.73.0.11 - File System view of Norman's Nokia C2 2nd Edition (EX-03) showing "Open.7z" (20,033 bytes) in the WhatsApp Documents/Sent directory with modification timestamp 31/01/2025 10:33:34 (UTC+0). Hex View panel confirms 7-Zip container header. This file is suspected to contain the QT-AI-2025 patent data transferred as the initial "head" tranche of the Blueprint.

4.6 Reconstructed Timeline of Events

Date / Time (UTC+0)	Event	Source Device	Application
21/08/2024, 09:58 10:11	Emma discloses possession of valuable Quantum Tech design data to Joe and asks him to identify a buyer	Emma Huawei (EX-01)	Whatsapp
26/08/2024, 07:04	Joe reports an unsuccessful initial meeting but confirms new contacts are being pursued	Emma Huawei (EX-01)	Whatsapp
20/11/2024, 10:01 10:03	Emma presses Joe for progress; Joe confirms he is finalizing a deal and travelling to meet the client in Manchester	Emma Huawei (EX-01)	Whatsapp
22/11/2024, 11:21	Rail ticket (Wigan Manchester, valid 22/11/2024) saved to gallery, corroborating Joe's stated travel	Joe Samsung (EX-02)	Device media
31/01/2025, 12:47 12:53	Direct negotiation between Emma (alias "Peter Dover") and Norman for a phased transfer of the patent data in exchange for a 5,000,000 offshore payment, within a 48-hour window	Emma Huawei (EX-01)	Facebook Messenger

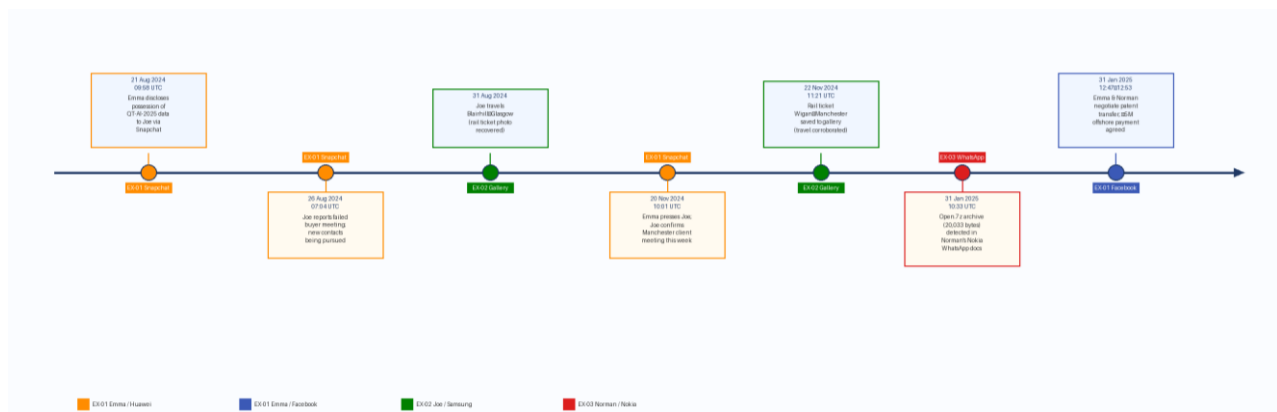


Fig. 14. Reconstructed chronological timeline of key events in Case QT-AI-2025 - derived from cross-device forensic analysis of EX-01 (Emma's Huawei), EX-02 (Joe's Samsung Galaxy A13), and EX-03 (Norman's Nokia C2). The Open.7z file event (31/01/2025 10:33 UTC, EX-03) is inserted to reflect the file-system evidence documented in Section 4.5.

4.7 Suspect Roles and Motives

Emma (perpetrator): a senior engineer who had been given privileged access to QT-AI-2025. Actual evidence obtained indicates Bitcoin where she solicited to sell proprietary design data, directly negotiated price and terms with the buyer and dictated timing and structure of the transfer ("Watch ur inbox in 48 hrs"). Her use of the alias "Peter Dover" in her dealings with Norman suggests a conscious attempt to obscure her identity, consistent with an awareness that she was engaging in illegal conduct.

Joe (intermediary): The connecting party between Emma and the ultimate buyer The Whatsapp records also show him soliciting a buyer, giving updates on meeting developments and from travel to Manchester where he met an interested client supported by the image of the rail ticket found on his own device. It also confirms that Joe was responsible for introducing Emma to Norman, because when negotiating with Emma over Facebook, she said: "Joe told me u r ready."

Norman (buyer): Facebook evidence states that Norman negotiated with Emma about how the transfer would work, and how it was to be received in "chunks" for "security reasons," starting with the "head" (the

actual design files themselves) and Offshore payment number 5,000.00 upon release of tranche 1 (the first batch of materials). This serves as direct proof that Norman was the acquirer and had negotiated price and delivery method.

4.8 Evidential Limitations

The limitations of the current authorship evidence base, which are intrinsically linked to the methods used in it, should be made available openly. The initial analysis of the communications evidence possessed by the three smartphones supports negotiation and intent but, taken alone, does not contain any QT-AI-2025 design files; any supplemental storage media connected to Emma that would hold those files are beyond the scope of evidence provided for this evaluation and should be sought out in a separate acquisition if such devices exist. Second, the published Facebook system message timestamped on 31/01/2025 at 12:47:29 ("You can now call each other and see...") is an automatically generated notice used by the platform itself so that users are aware of their functionalities; not a message written by Norman himself therefore excluded from substantive negotiation analysis in Table IV for the same reason. Third, as detailed in the extraction summaries that follow, no deleted-item recovery was uniquely identified; owing to the clear security interest of the parties herein, additional carving of unallocated space is recommended (placing details in Recommendations below).

5. Conclusion

The integrated communications and device evidence obtained from all three smartphones manifests a coherent and mutually-reinforcing story: Emma instigated an unauthorised disclosure of patent data relating to Quantum Tech's QT-AI-2025, solicited Joe as the vehicle for procuring someone to buy it and negotiated directly with Norman via Facebook Messenger for the information in tranches (amounts) in return for a each time payment of 5,000,000 into offshore accounts. This cross-device corroboration here highlighted by the fact that Joe, in his Whatsapp statement where he and Phil were travelling to Manchester at different times, went on to tell investigators the rail ticket retrieved from his photo gallery belonged to him considerably enhances the reliability of the communications evidence as it is based solely on file-system metadata rather than chat content. All three of the smartphone extraction images were hash-verified (SHA-256) immediately after acquiring them and no issues were found during re-verification before starting any analysis, thus confirming the integrity and admissibility of the evidence base. Both Emma and Norman's references to the "Blueprint" and its "head" during Facebook negotiation identify the artefact that is truly at issue, such that any file level inquiry into Emma's access and manipulation of QT-AI-2025 should be guided accordingly.

6. Recommendations

1. Quantum Tech should immediately revoke Emma's access to the patent repository and maintain complete audit/access logs of her activity in the patent repository to support that she exfiltrated files containing QT-AI-2025 information.
2. Law enforcement should be provided this report, plus the hash-verified forensic images and chain-of-custody documentation in preparation for charges against Emma for theft of trade secrets/corporate espionage and Joe and Norman for conspiracy to possess stolen proprietary data.
3. Quantum Tech should be requested to submit their QT-AI-2025 repository/file-server access logs, with subsequent citation against the timeline in Table V (Section 4.6) that indicates when Emma accessed or exported the underlying design files (i.e., the "back-end").
4. Relevant financial records regarding the proposed 5,000,000 transfer overseas discussed over Facebook and any other payment attempt related to Norman or NexGen Circuits but not attempted in connection with Norman's alleged crimes may be available through additional compulsory processes.
5. Investigations involving "ghosts," for example, aliases (e.g., "Peter Dover") and security conscious language ("no backtracking," "we are ghosts"), warrant a lawful request to Meta and Snap Inc. for records related at the platform level that authenticate account access and data deleted from the devices that have not been previously extracted.
6. The same evidential limitation needs to be applied if any content produced is encrypted or deleted and cannot be recovered through the existing extractions, and advanced level (for example physical/chip-off extraction) should only be considered on a case by case basis, subject to proportionality and further legal authorization.

References

- [1] DigitalEdge, "Corporate Investigation Software Solutions in 2026: Essential Tools for Modern Digital Forensics," DigitalEdge, Apr. 2025. [Online]. Available: <https://digitaledge.org/corporate-investigation-software-solutions-in-2025/>
- [2] SkyQuest Technology, "Digital Evidence Management Market Size & Share, Industry Growth Report 2032," SkyQuest, 2025. [Online]. Available: <https://www.skyquestt.com/report/digital-evidence-management-market>
- [3] Computer Forensics Lab, "Top Mobile Device Forensic Tools Expert Comparison 2025," Nov. 2025. [Online]. Available: <https://computerforensicslab.co.uk/mobile-device-forensic-tools-comparison/>
- [4] Cotocus, "Top 10 Digital Forensics Tools in 2025: Features, Pros and Cons Comparison," Feb. 2026. [Online]. Available: <https://www.cotocus.com/blog/top-10-digital-forensics-tools-in-2025-features-pros-cons-comparison/>
- [5] Sherlock Forensics, "Cellebrite vs Magnet AXIOM 2026: Forensic Tool Showdown," May 2026. [Online]. <https://www.sherlockforensics.com/blog/cellebrite-vs-magnet-axiom-2026.html>
- [6] Computer Forensics Lab, "Digital Forensic Trends 2025: AI, Cloud, and Risk," Feb. 2026. [Online]. Available: <https://computerforensicslab.co.uk/digital-forensic-trends-2025/>
- [7] Belkasoft, "Top 6 Trends in Digital Forensics and Incident Response for 2025," Belkasoft Blog, 2025. [Online]. Available: <https://belkasoft.com/dfir-trends-2025>
- [8] SalvationData, "Key Trends in Digital Forensics 2025: Challenges and Innovations," Sep. 2025. [Online]. Available: <https://www.salvationdata.com/knowledge/key-trends-in-digital-forensics-for-2025/>
- [9] IJRASET, "Digital Forensic: Techniques, Challenges, and Future Direction," Int. J. Res. Appl. Sci. Eng. Technol., 2025. [Online]. Available: <https://www.ijraset.com/research-paper/digital-forensic-techniques-challenges-and-future-direction>
- [10] P. Narasimhan, "Emerging Trends in Digital Forensics: Investigating Cybercrime," Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 11, no. 1, pp. 3645 3652, Jan. Feb. 2025. [Online]. Available: https://www.researchgate.net/publication/389631795_Emerging_Trends_in_Digital_Forensics_Investigating_Cybercrime
- [11] Oxygen Forensics, "Key Trends Shaping the Future of Digital Forensics in 2025," Dec. 2025. [Online]. Available: <https://www.oxygenforensics.com/resources/digital-forensics-trends-2025/>
- [12] EC-Council University, "Why Digital Forensics Is One of the Fastest-Growing Careers in Cybersecurity," ECCU Blog, 2026. [Online]. Available: <https://www.eccu.edu/blog/digital-forensics-career-guide/>
- [13] SANS Institute, "Digital Forensics Salary, Skills, and Career Path," Jan. 2026. [Online]. Available: <https://www.sans.org/blog/digital-forensics-salary-skills-and-career-path>
- [14] IT Jobs Watch, "Digital Forensics Job Trends, Salaries & Related Skills," Jun. 2026. [Online]. Available: <https://www.itjobswatch.co.uk/jobs/uk/digital%20forensics.do>
- [15] SQ Magazine, "Cybersecurity Job Statistics 2026: Salaries, Gaps & Growth," Oct. 2025. [Online]. Available: <https://sqmagazine.co.uk/cybersecurity-job-statistics/>
- [16] Eclipse Forensics, "The Future of Digital Forensics: Emerging Trends and Technologies," Jan. 2025. [Online]. Available: <https://eclipseforensics.com/the-future-of-digital-forensics-emerging-trends-and-technologies/>
- [17] ISO/IEC 27037:2012, Information technology, Security techniques, Guidelines for identification, collection, acquisition and preservation of digital evidence, International Organization for Standardization, Geneva, 2012.
- [18] National Institute of Standards and Technology, SP 800-101 Rev. 1, Guidelines on Mobile Device Forensics, NIST, Gaithersburg, MD, 2014. [Online]. Available: <https://csrc.nist.gov/pubs/sp/800/101/r1/final>