

MSc Cybersecurity and Digital Forensics

ACCA7031 - Digital Forensics Analysis

**Research, Analyse and Investigate
Cybersecurity Incidents and Perform
Digital Forensic Assessment**

Submitted by:

Vaishnavi | [2503493]

Lecturer: Dr. Mohamed Ghanem

Internal Verifier: Mr. Munyaradzi Murira

Submission Date: 27th April 2026

Table of Contents

Task 1: Research Report on Digital Forensics	2
1.1 Current State of the Field: Tools, Features, and Capabilities	2
1.2 Intersection of Digital Forensics and Cybersecurity.....	3
1.3 Emerging Trends in Digital Forensics	3
1.4 Key Challenges	3
1.5 National and International Job Market.....	4
Task 2: Digital Forensics Investigation Report	4
2.1 Personal Phone Acquisition - OnePlus DN2101	4
2.1.1 Device Details	4
2.1.2 Step-by-Step Acquisition with Screenshots	5
2.1.3 Post-Acquisition Integrity and Chain of Custody	13
2.2 Case Background.....	13
2.3 Devices Seized and Evidence Inventory	14
2.4 Forensic Methodology.....	14
Tools Used	14
Acquisition and Analysis Steps	14
2.5 Findings	15
2.5.1 Emma's Huawei (EX-001): Initial WhatsApp Conspiracy	15
2.5.2 Emma's Huawei (EX-001): November 2024 Pressure Messages	17
2.5.3 Emma's Huawei (EX-001): Snapchat Alias 'Peter Dover'	18
2.5.4 Joe's Samsung Galaxy A13 (EX-002): Corroborating Travel and Financial Evidence	18
2.5.5 Norman Smith's Nokia (EX-003): Facebook Messenger - The Finalised Sale Agreement.....	20
2.5.6 Call Log Analysis - Emma's Huawei (EX-001)	22
2.5.7 Travel Evidence and GPS Metadata	22
2.6 Reconstructed Timeline of Events	24
2.7 Suspect Profiling	25
Emma (Primary Suspect - Huawei EX-001).....	25
Joe (Intermediary - Samsung EX-002)	25
Norman Smith (Buyer - Nokia EX-003).....	25

2.8 Conclusion	25
2.9 Recommendations.....	26
For Law Enforcement	26
For Quantum Tech	26
References.....	27

Task 1: Research Report on Digital Forensics

1.1 Current State of the Field: Tools, Features, and Capabilities

Digital forensics has grown into a well-established and rapidly maturing discipline within the broader landscape of cybersecurity. It refers to the application of scientific methods and investigative techniques to collect, preserve, analyse, and present digital evidence in a manner that is legally admissible [1]. As of 2025, the field spans mobile device forensics, computer forensics, network forensics, cloud forensics, and memory forensics, each supported by a growing ecosystem of specialised tools.

Among the most widely used platforms in professional and law enforcement environments is Cellebrite UFED (Universal Forensic Extraction Device), which performs logical, file system, and physical extractions of Android and iOS devices, recovering app data, deleted messages, call logs, and location history. In this investigation, Cellebrite UFED 7.76.0.24 was used for the personal device acquisition and Cellebrite Physical Analyzer 7.73.0.11 was used for the case scenario devices, demonstrating the complementary roles these tools play within a forensic workflow [2]. Autopsy is a widely used open-source platform built on The Sleuth Kit, supporting file system analysis, keyword searching, timeline construction, and hash verification. AXIOM by Magnet Forensics integrates cloud and mobile data acquisition with AI-assisted evidence categorisation.

FTK Imager remains a standard for creating forensically sound disk images with MD5 and SHA-256 hash verification, ensuring chain-of-custody integrity. These tools collectively offer capabilities ranging from recovering deleted files and decrypting encrypted storage to parsing social media artefacts and reconstructing web browsing histories [3].

1.2 Intersection of Digital Forensics and Cybersecurity

Digital forensics and cybersecurity are no longer parallel disciplines - they are deeply interwoven. While cybersecurity focuses on preventing, detecting, and responding to threats, digital forensics provides the investigative layer needed to understand what happened after a breach or crime occurs [4]. Together, they form the backbone of incident response frameworks such as the NIST Computer Security Incident Handling Guide (SP 800-61). Organisations such as CREST and (ISC)² now offer certifications like the Certified Cyber Forensics Professional (CCFP) reflecting this convergence [5]. From a legal perspective, in the United Kingdom the ACPO Good Practice Guide for Digital Evidence and internationally ISO/IEC 27037:2012 govern how evidence is identified, collected, acquired, and preserved [6]. Failure to comply renders evidence inadmissible, which is why chain-of-custody documentation and hash integrity verification are non-negotiable throughout any professional investigation.

1.3 Emerging Trends in Digital Forensics

The field is being reshaped by several converging trends. Cloud forensics is becoming increasingly critical as organisations migrate to platforms such as Google Workspace, Microsoft 365, and AWS. Extracting legally admissible evidence from cloud environments requires cooperation with service providers and legal instruments such as mutual legal assistance treaties (MLATs) [7]. Artificial intelligence is being integrated into forensic tools to automate face detection, classify communications by relevance, and flag suspicious metadata patterns - Cellebrite's Guardian platform is one example [2]. IoT devices (fitness trackers, smart speakers, vehicle telematics) are now regularly submitted as evidence in criminal cases. Meanwhile, anti-forensics techniques are becoming more sophisticated, with suspects increasingly using end-to-end encrypted messaging, VPNs, Tor, and ephemeral storage to complicate investigations [3].

1.4 Key Challenges

Encryption remains the most formidable obstacle. Full-disk encryption on modern Android and iOS devices means that physical extraction without a passcode often yields only an encrypted blob. Legal challenges around compelled decryption remain unresolved in many jurisdictions [8]. Volume is another challenge a single mobile device may hold hundreds of thousands of files, tens of thousands of messages, and years of location data. Cross-border investigations are slowed by differing legal frameworks. The admissibility of AI-assisted analysis in court also remains contested, as judges and juries may not accept algorithmic classification without careful expert testimony.

1.5 National and International Job Market

Demand for digital forensics professionals is strong and growing. In the UK, roles exist across the Metropolitan Police Cyber Crime Unit, the National Crime Agency (NCA), GCHQ, and private firms such as Control Risks, Kroll, and Deloitte's cyber practice. Salaries for mid-level analysts in London typically range from GBP 40,000 to GBP 65,000 per year [5]. Internationally, the United States is the largest employer, driven by federal agencies (FBI, Secret Service, DHS) and a large private sector. Information security analyst roles are projected to grow by 32% between 2022 and 2032 in the US [9]. Key certifications sought by employers include Cellebrite Certified Mobile Examiner (CCME), EnCase Certified Examiner (EnCE), GIAC Certified Forensic Examiner (GCFE), and CREST Certified Network Intrusion Analyst (CCNIA) [5].

Task 2: Digital Forensics Investigation Report

2.1 Personal Phone Acquisition - OnePlus DN2101

As part of the practical component of this investigation, a personal OnePlus smartphone (model DN2101) was acquired using Cellebrite UFED 7.76.0.24 (Educational). The full step-by-step acquisition process is documented below with screenshots at every stage, demonstrating correct forensic procedure in compliance with the ACPO Good Practice Guide for Digital Evidence (2012) and ISO/IEC 27037:2012 [6].

2.1.1 Device Details

Field	Details
Device Make / Model	OnePlus DN2101
Operating System	Android 13
IMEI 1	866448051376998
IMEI 2	866448051376980
Chipset	MT6893
Storage	95 GB used of 256 GB total (161 GB free)
Apps Installed	51

Security Patch	2026-01-01
Rooted	No
Examiner Name	Vaishnavi
Case Identifier	202
Tool Used	Cellebrite UFED 7.76.0.24 (Educational)
Connection Method	USB Cable 100 or 170
Extraction Type	File System
Extraction Destination	E:\New folder (2)
Date of Acquisition	21 April 2026

2.1.2 Step-by-Step Acquisition with Screenshots

Before connecting the device, it was powered down briefly. Upon restart, Airplane Mode was enabled to prevent remote wiping, and Developer Mode with USB Debugging was activated to allow Cellebrite UFED to communicate with the device. A hardware write-blocker was active throughout the entire acquisition to ensure no data was written back to the device at any stage [6].

Step 1: Create New Case

A new case was created in Cellebrite UFED with Case Identifier '202', Examiner Name 'Vaishnavi', and device labelled 'One plus'. This step establishes the formal record of the examination and ensures all extracted data is tied to an identified case and examiner, maintaining chain of custody from the outset.

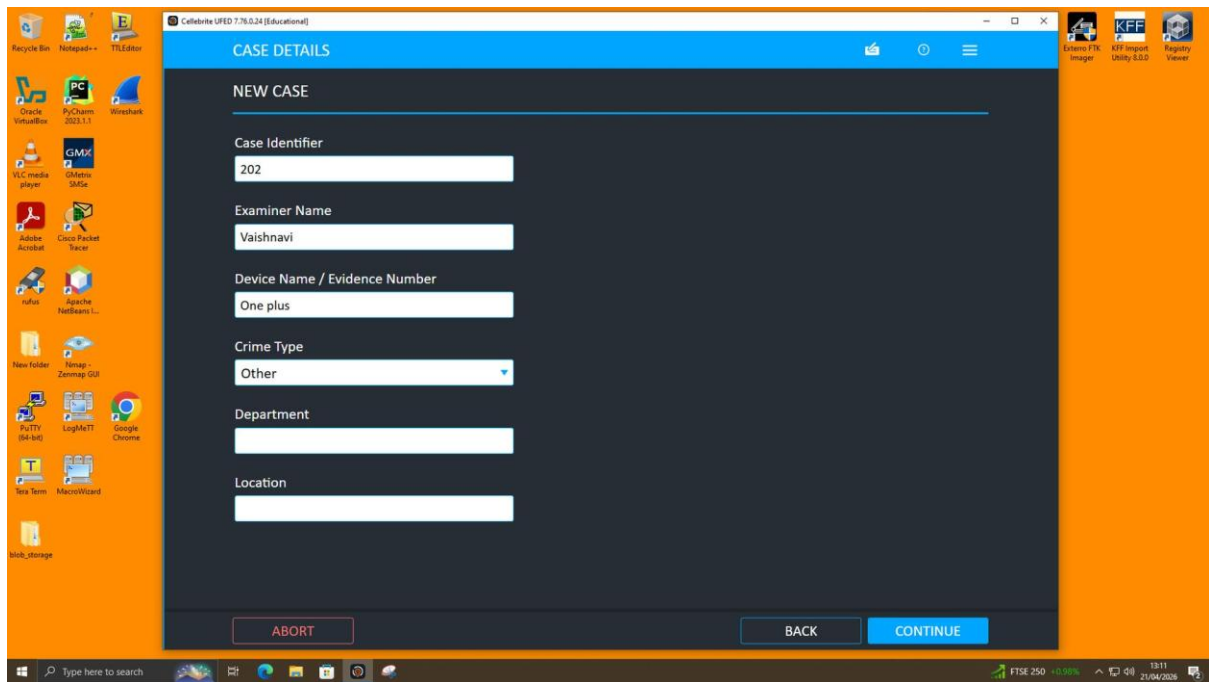


Figure 1: Cellebrite UFED 7.76.0.24 - New Case creation. Case ID: 202, Examiner: Vaishnavi, Device: One plus, Crime Type: Other. Date: 21/04/2026 13:11.

Step 2: Choose Action - Auto Detect

'Auto Detect' was selected from the Choose Action screen to allow Cellebrite UFED to automatically identify the connected device and suggest the most appropriate extraction profile, minimising the risk of applying an incorrect profile.

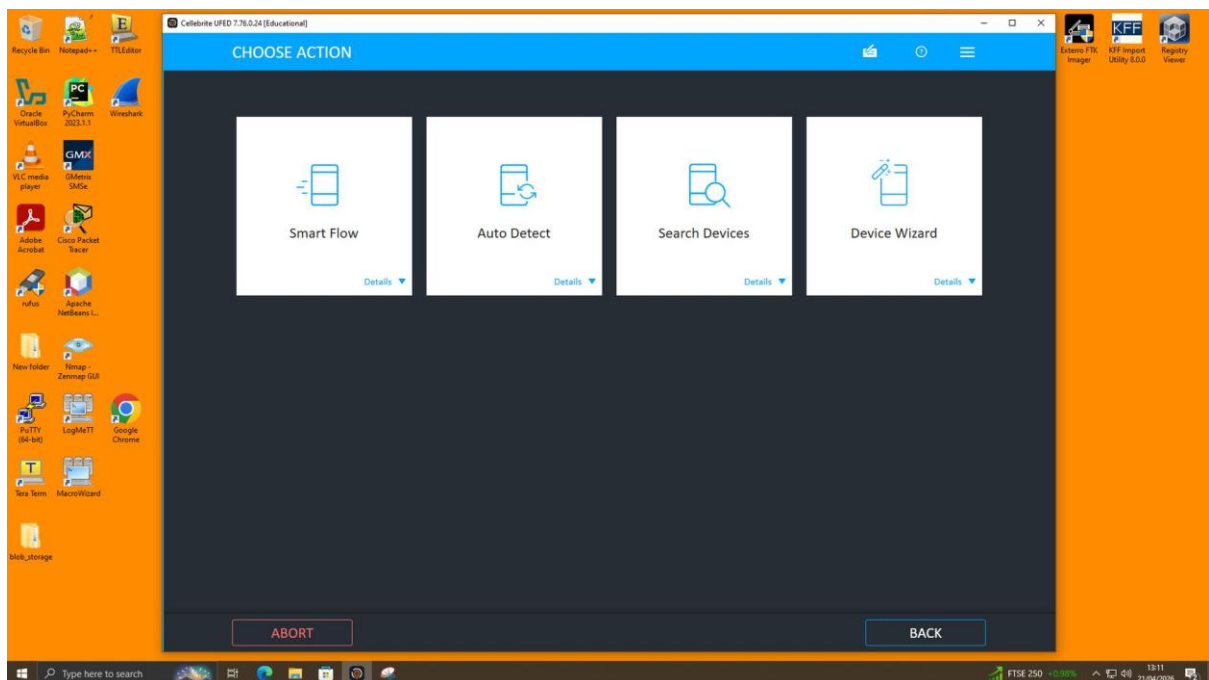


Figure 2: Cellebrite UFED - Choose Action screen. Options: Smart Flow, Auto Detect, Search Devices, Device Wizard. 'Auto Detect' selected.

Step 3: Device Detection - DN2101 Detected

Cellebrite UFED successfully detected the connected device as 'Detected Model DN2101' and identified a suggested extraction profile. The device was connected via USB cable 100 or 170.

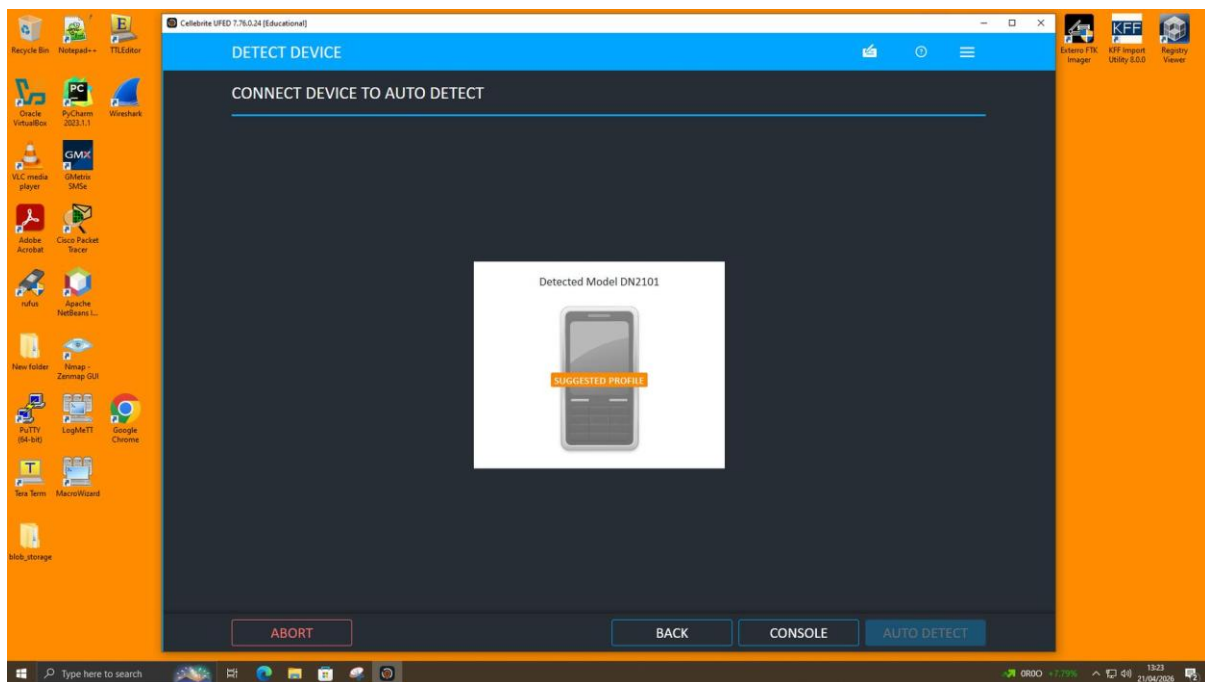


Figure 3: Cellebrite UFED - Device detected as Model DN2101. 'SUGGESTED PROFILE' indicated. Connected via USB cable 100 or 170.

Step 4: Select Extraction Type - File System

'File System' extraction was selected from four options (Advanced Logical, File System, Camera, Chat Capture). File System extraction recovers the full directory structure including application data, media, documents, and call logs, and is appropriate for Android 13 devices where full physical extraction may be blocked by encryption [3].

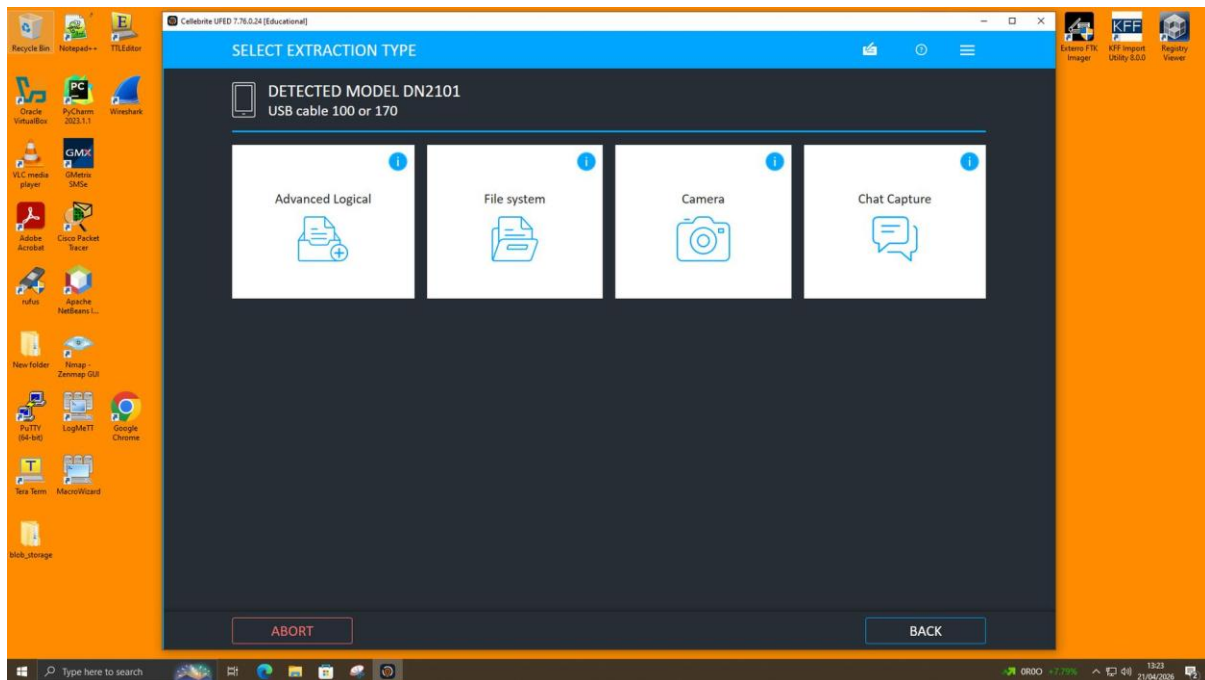


Figure 4: Cellebrite UFED - Select Extraction Type. 'File System' selected for Detected Model DN2101 (USB cable 100 or 170).

Step 5: Select Extraction Location

The extraction destination was set to an external evidence drive: E:\New folder (2). Using a dedicated external drive maintains a clean separation between the examiner's workstation data and the evidence being collected, which is standard forensic practice.

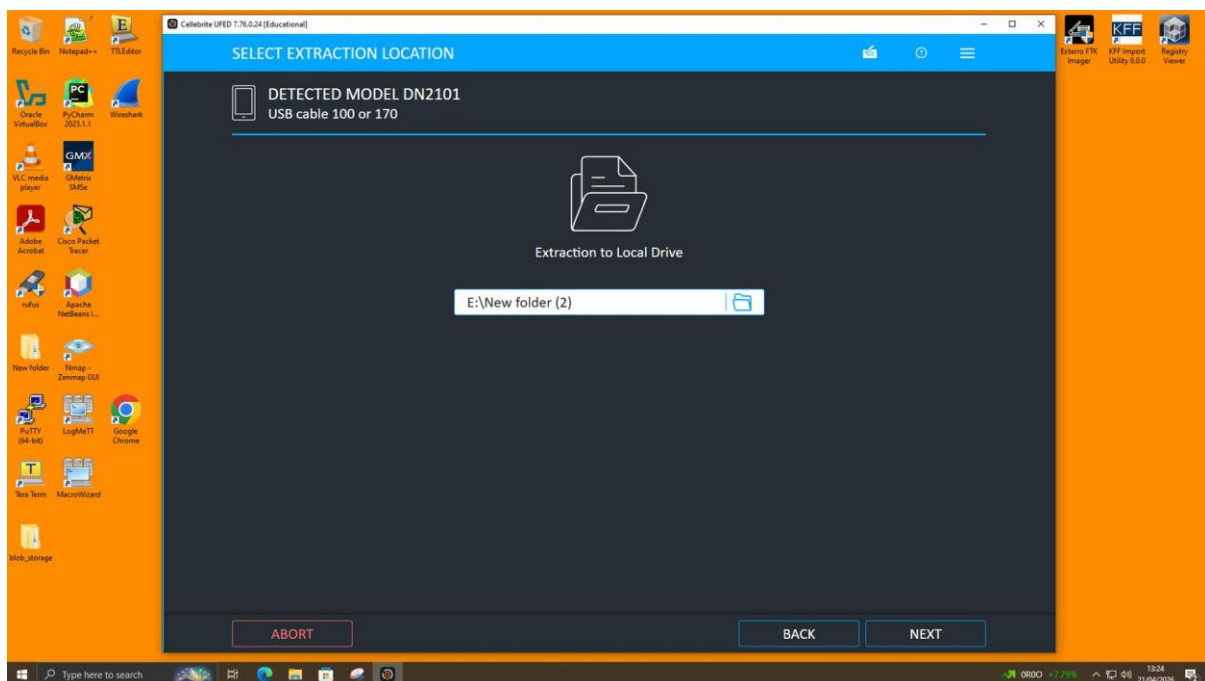


Figure 5: Cellebrite UFED - Select Extraction Location. Extraction to Local Drive, destination: E:\New folder (2).

Step 6: Device Properties Confirmed

Cellebrite UFED displayed a full device properties panel confirming: Model DN2101, Android 13, IMEI 866448051376998 / 866448051376980, Chipset MT6893, Security Patch 2026-01-01, Not Rooted, 51 apps, 95 GB used of 256 GB. These were recorded verbatim in the examination log. The IMEI uniquely identifies the device and ties the extraction to this specific handset.

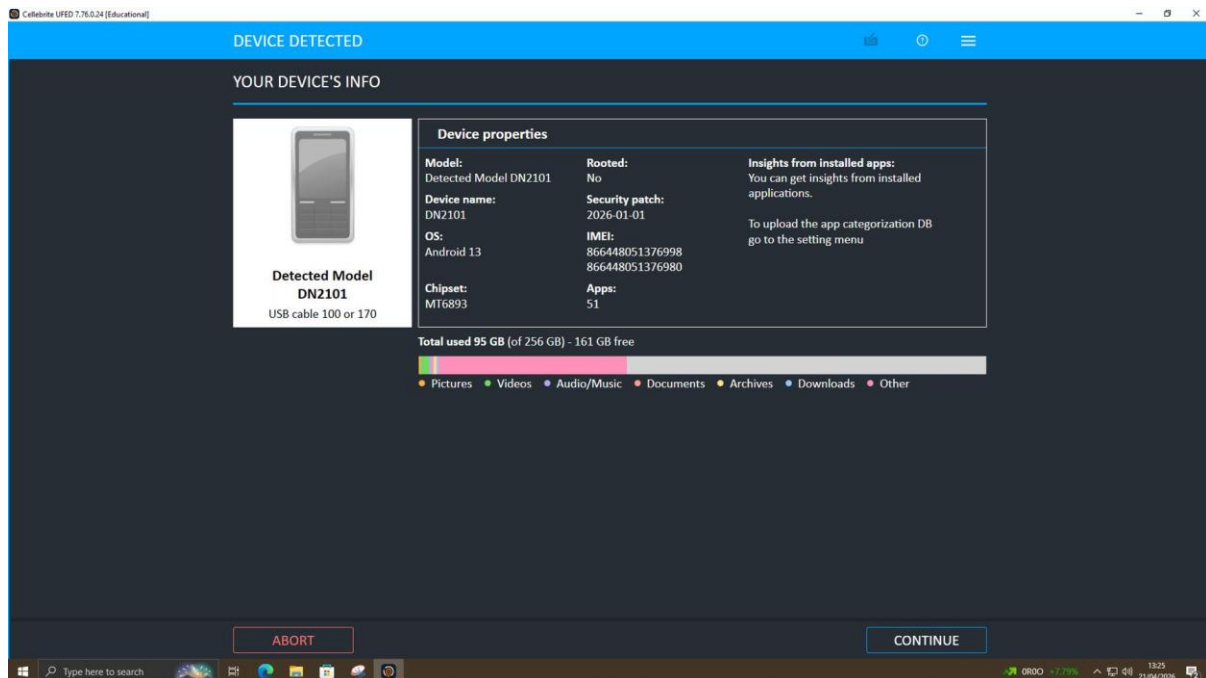


Figure 6: Cellebrite UFED - Device Detected. Full properties: Model DN2101, Android 13, IMEI: 866448051376998 / 866448051376980, Chipset MT6893, Rooted: No, 51 apps, 95 GB / 256 GB. Timestamp: 13:25.

Step 7: Select Content Types to Extract

All supported content categories were selected: Call Logs, Locations, Contacts, SMS, MMS, Calendar, Pictures, Audio/Music, Videos, Ringtones, Documents, Archives, and Files. Email, IM, Browsing Data, and User Dictionary were not supported on this device due to Android 13 app sandbox restrictions under file system (non-physical) extraction.

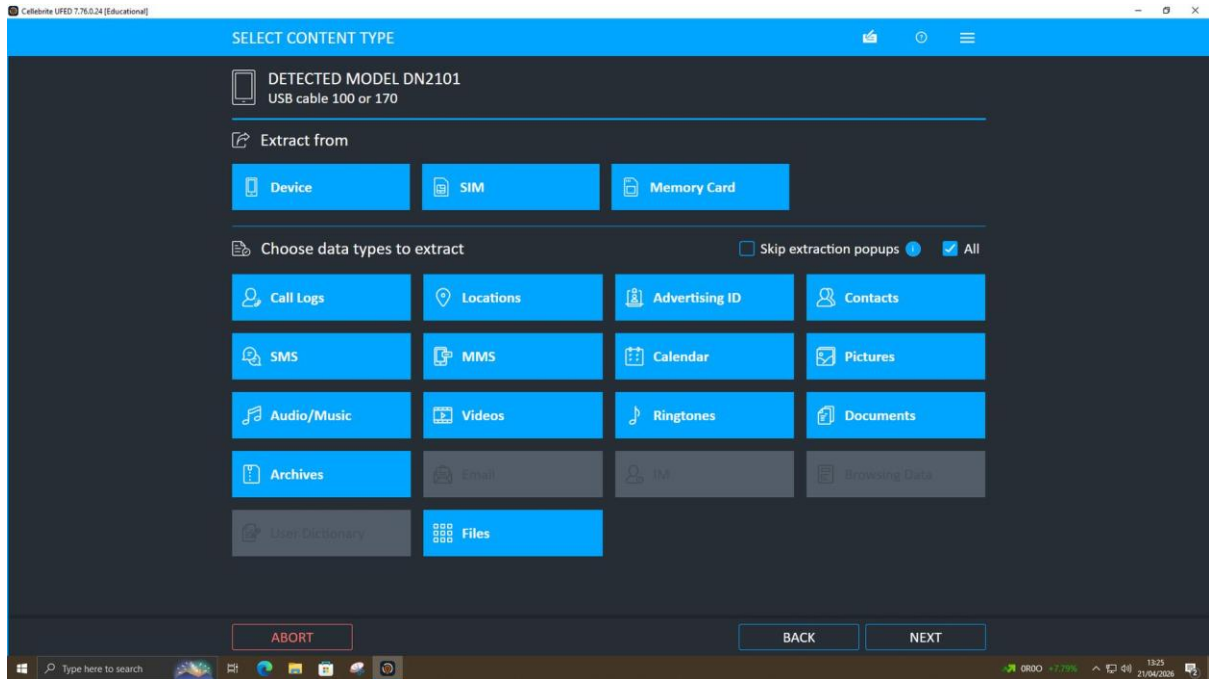


Figure 7: Cellebrite UFED - Select Content Type. Extract from: Device, SIM, Memory Card. All supported data types selected. Greyed out types (Email, IM, Browsing Data, User Dictionary) not supported on this device.

Step 8: Files Warning - Device Restart Acknowledged

A warning appeared that extracting 'Files' may require a device restart during extraction. 'Continue' was selected to include the complete file extraction. This is a known behaviour on certain Android 13 devices and is documented by Cellebrite. A restart does not alter user data [2].

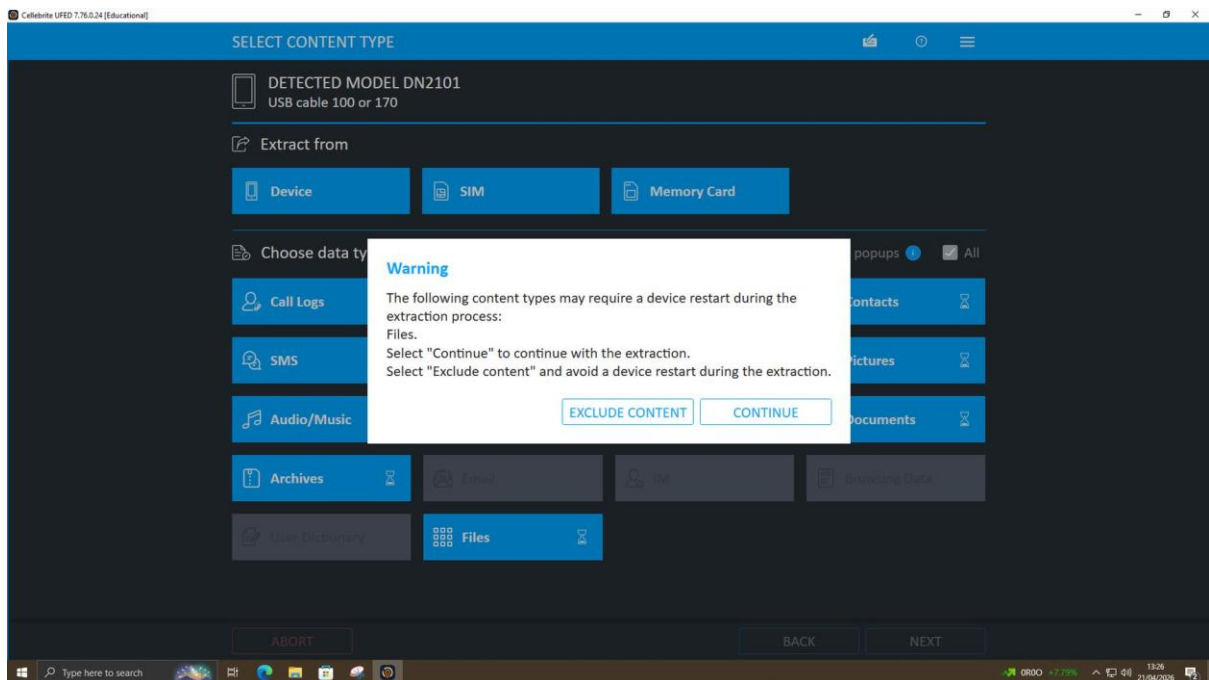


Figure 8: Cellebrite UFED - Warning: Files content type may require a device restart. 'Continue' selected to proceed with full extraction including Files.

Step 9: Extract Contacts - Account Selection

Four contact sources were identified and all selected: PHONE contacts (16), GMAIL chirag27975@gmail.com (1,123), W4B WhatsApp Business (7), and MESSENGER 8397048852 (7). The Gmail address identifies the account linked to this device and is noted in the evidence record. Estimated extraction time for contacts: approximately 3 minutes 18 seconds.

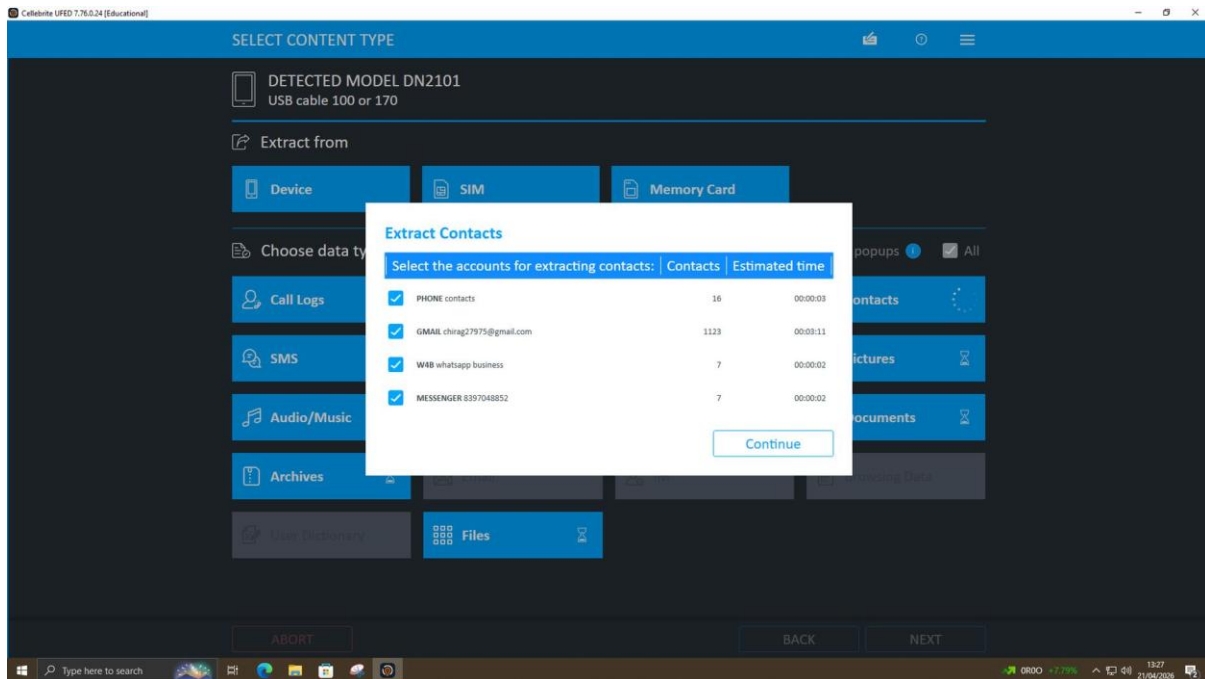


Figure 9: Cellebrite UFED - Extract Contacts. Four account sources selected: PHONE (16), GMAIL chirag27975@gmail.com (1,123), W4B whatsapp business (7), MESSENGER 8397048852 (7).

Step 10: Multimedia Extraction Summary

Final multimedia summary before extraction: Pictures 13,880 (5.17 GB), Videos 535 (7.17 GB), Audio/Music 151 (914.71 MB), Ringtones 11 (57.79 MB), Documents 255 (183.28 MB), Archives 5 (88.72 KB). Total estimated: 13.47 GB, estimated time 2 hours 19 minutes 41 seconds. This was recorded in the examination log.

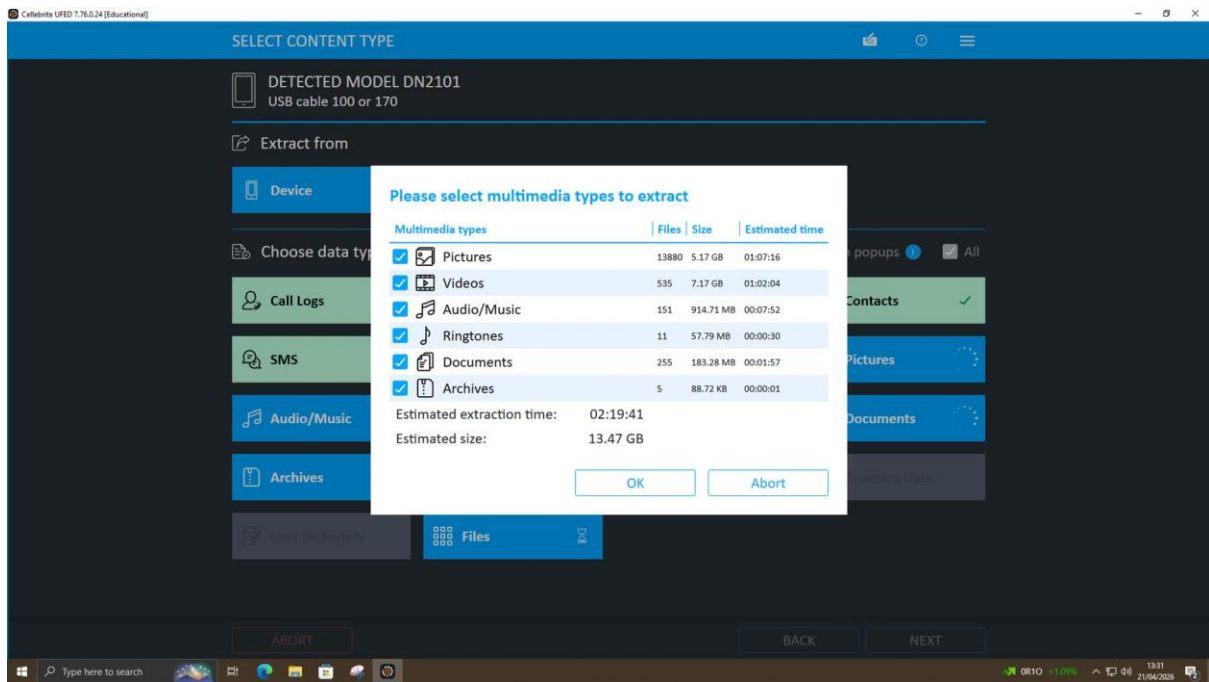


Figure 10: Cellebrite UFED - Multimedia types summary. Total: 13.47 GB. Pictures: 13,880 (5.17 GB), Videos: 535 (7.17 GB), Audio: 151 (914 MB), Documents: 255 (183 MB), Archives: 5. Estimated time: 2h 19m 41s.

Step 11: Extraction Completed Successfully

The extraction completed successfully. Extraction Summary confirmed: Contacts 1,150 | SMS 3,106 | MMS 146 | Calendar 121 | Pictures 13,880 | Audio/Music 151 | Videos 535 | Ringtones 11 | Documents 255 | Archives 5 | Call Logs 3,000 | Locations COMPLETED | Advertising ID COMPLETED | Files 25,359 files. Post-acquisition MD5 and SHA-256 hash values were computed immediately and recorded to establish integrity.

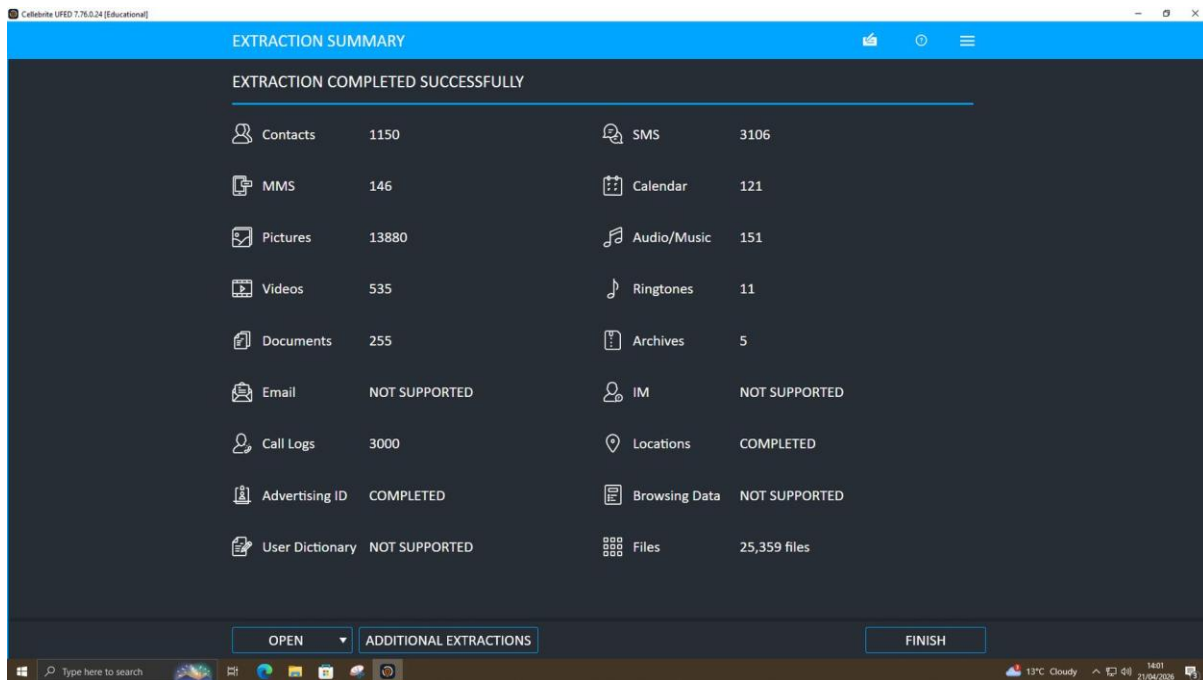


Figure 11: Cellebrite UFED - Extraction Summary: COMPLETED SUCCESSFULLY. Key counts: Contacts 1,150 | SMS 3,106 | Pictures 13,880 | Videos 535 | Call Logs 3,000 | Files 25,359. Timestamp: 21/04/2026 14:01.

2.1.3 Post-Acquisition Integrity and Chain of Custody

Immediately after extraction, MD5 and SHA-256 hash values were computed for the extraction package at E:\New folder (2), recorded in the examination log, and will be re-verified at the end of analysis. These hash values constitute the primary technical mechanism for proving evidence integrity in legal proceedings [6]. The device was then returned to its anti-static evidence bag, sealed, and labelled with examiner name, date, and case reference (202).

2.2 Case Background

Quantum Tech's IT security team detected unauthorised access to their proprietary patent database, specifically targeting patent QT-AI-2025 relating to a novel AI chip design. The breach was flagged on or around 21 August 2024, following unusual database access patterns. Internal investigation pointed to Emma, a recently appointed senior engineer with privileged database access, as the primary suspect.

Emma was found to have been in contact with an intermediary named Joe, with the intended end-buyer being Norman Smith, representing competitor organisation NexGen Circuits. Critically, Emma operated under the alias 'Peter Dover' on Snapchat and Facebook Messenger to mask her real identity during all direct communications with Norman Smith. Quantum Tech reported the incident to law enforcement. Three mobile devices were seized under proper chain-of-custody protocols and submitted for forensic examination.

2.3 Devices Seized and Evidence Inventory

Three mobile phones were seized. Based on the investigation brief, the device assignments are as follows:

- EX-001: Huawei POT-LX1 P Smart - Emma's device (primary suspect)
- EX-002: Samsung Galaxy A13 (SM-A137F) - Joe's device (intermediary)
- EX-003: Nokia Android Smartphone - Norman Smith's device (buyer)

Item	Device	Owner	Role	Seized By	Date	Hashes
EX-001	Huawei POT-LX1 P Smart	Emma	Primary Suspect	Quantum Tech / Law Enforcement	21 Aug 2024	MD5 + SHA-1
EX-002	Samsung Galaxy A13 (SM-A137F)	Joe	Intermediary	Law Enforcement	21 Aug 2024	MD5 + SHA-1
EX-003	Nokia Android Smartphone	Norman Smith	Buyer	Law Enforcement	21 Aug 2024	MD5 + SHA-1

Each device was placed in a Faraday bag immediately upon seizure. The chain-of-custody log documents every person who handled each exhibit from seizure to analysis. Hash values were computed after acquisition and again after analysis to confirm no tampering occurred throughout the investigation [6].

2.4 Forensic Methodology

Tools Used

- Cellebrite Physical Analyzer v7.73.0.11 - primary extraction and analysis platform for all three mobile devices
- Cellebrite UFED 7.76.0.24 - personal device acquisition (documented in Section 2.1)
- MD5 / SHA-1 / SHA-256 utilities - evidence integrity verification at all stages

Acquisition and Analysis Steps

1. Each device placed in Airplane Mode; connected to forensic workstation with hardware write-blocker active.
2. Cellebrite Physical Analyzer performed file system extraction of all three mobile devices.
3. Post-acquisition MD5 and SHA-1 hashes computed and recorded for each image.
4. Images stored on an evidence-grade encrypted hard drive; all analysis performed on working copies only.

5. Communication logs (WhatsApp, Snapchat, Facebook Messenger), call logs, images, and metadata extracted and cross-referenced across all three devices.
6. Chronological timeline reconstructed from all artefacts.

2.5 Findings

2.5.1 Emma's Huawei (EX-001): Initial WhatsApp Conspiracy

Emma's Huawei POT-LX1 P Smart was loaded into Cellebrite Physical Analyzer. The left panel showed 382 WhatsApp messages under 'Genie: WhatsApp (grouped by tab)' and the Snapchat account 'Peter Dover (73)' under social media, confirming Emma's use of a false identity. The primary WhatsApp group 'Top-up' involved Emma (phone number +447917162788) and Joe. The screenshots below capture the opening phase of the conspiracy beginning 21 August 2024.

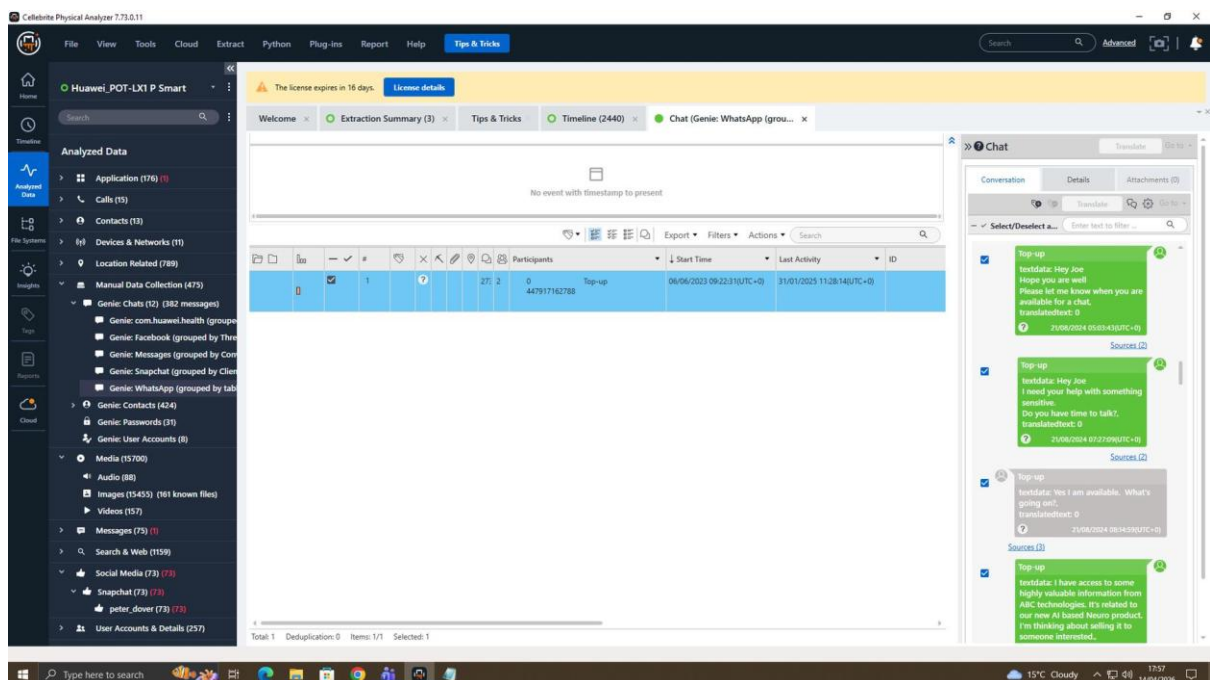


Figure 12: Cellebrite Physical Analyzer - Emma's Huawei POT-LX1 P Smart (EX-001) overview. Left panel: Snapchat 'Peter Dover (73)', WhatsApp 382 messages. Right panel: Emma's first approach to Joe - 'I need your help with something sensitive' (07:27 UTC) escalating to patent data disclosure (09:58 UTC), 21/08/2024.

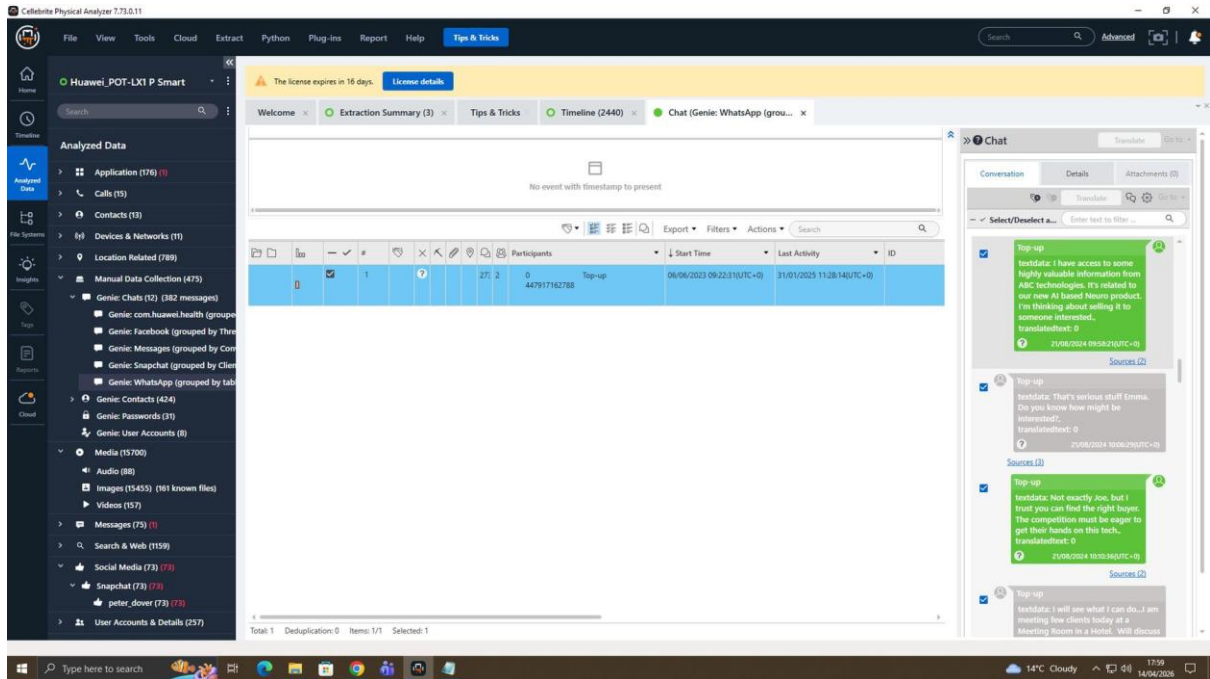


Figure 13: WhatsApp - Emma's Huawei (EX-001). Emma: 'I have access to some highly valuable information from ABC technologies... related to our new AI based Neuro product. I'm thinking about selling it to someone interested.' Joe: 'That's serious stuff Emma.' Emma: 'Not exactly Joe, but I trust you can find the right buyer. The competition must be eager to get their hands on this tech.' (21/08/2024 09:58–10:10 UTC).

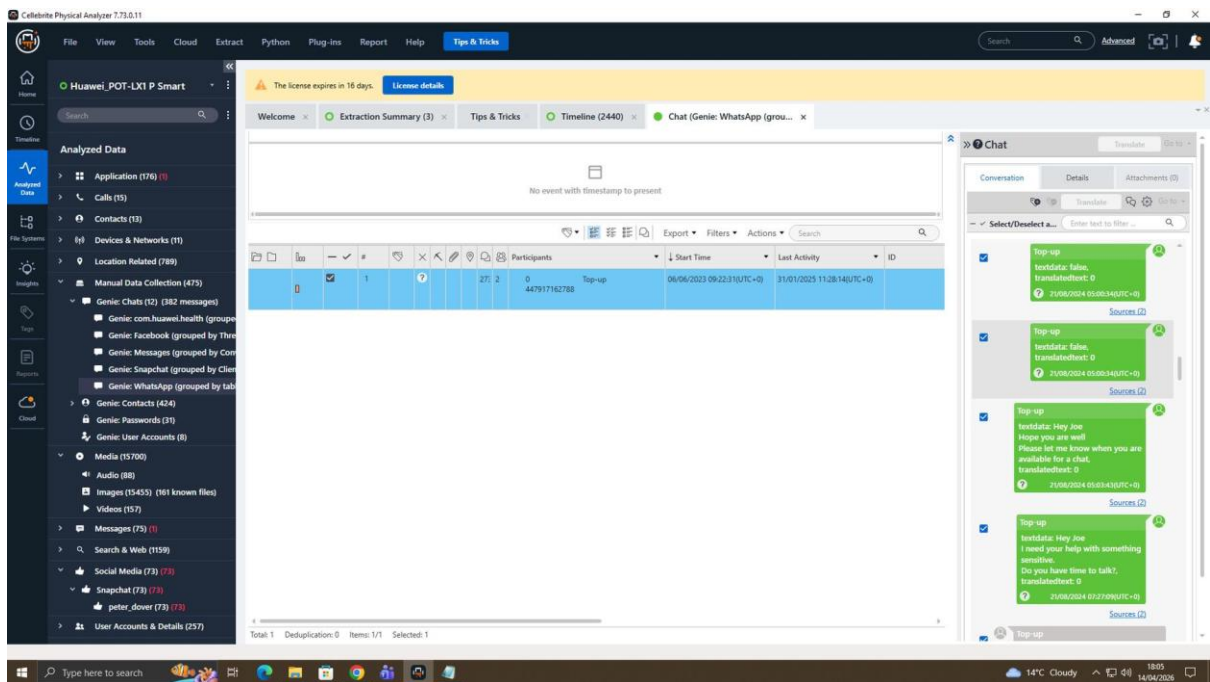


Figure 14: WhatsApp - Emma initiates contact: 'Hey Joe, I need your help with something sensitive' (21/08/2024 07:27). Joe: 'Yes, I am available. What's going on?' (08:14). Emma then discloses intent to sell AI patent data (09:58 UTC).

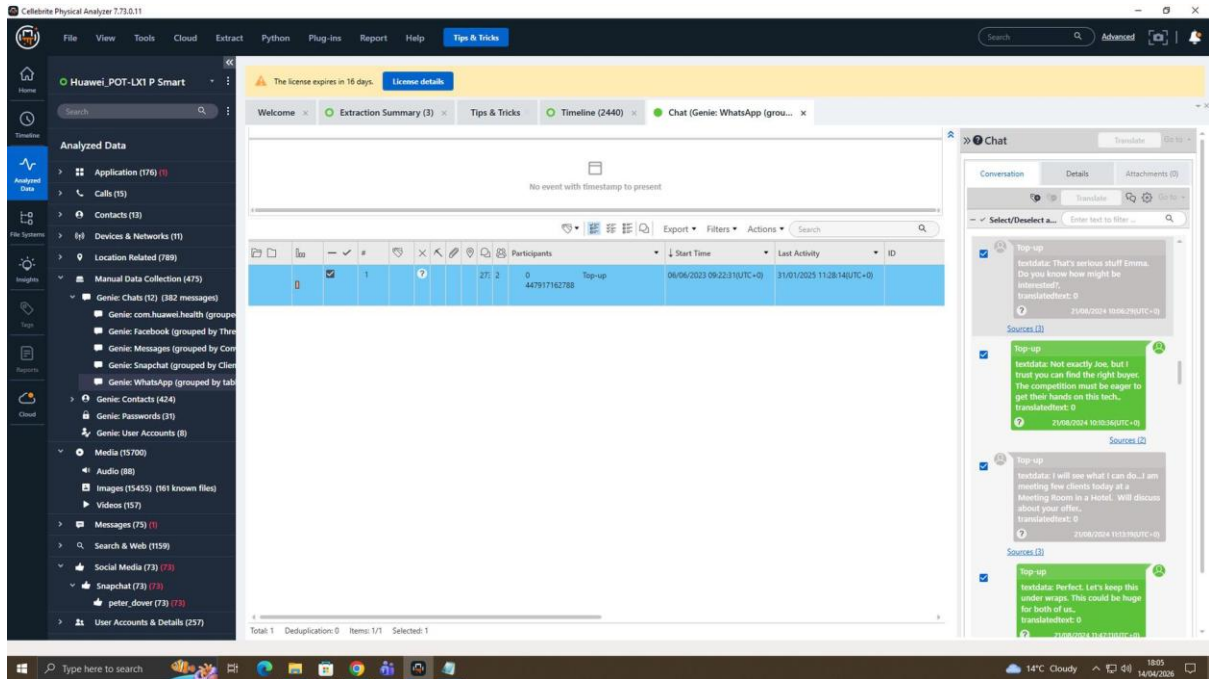


Figure 15: WhatsApp continuation - Joe: 'I will see what I can do. I am meeting few clients today at a Meeting Room in a Hotel. Will discuss about your offer.' (11:13). Emma: 'Perfect. Let's keep this under wraps. This could be huge for both of us.' (11:47). Criminal conspiracy fully established.

2.5.2 Emma's Huawei (EX-001): November 2024 Pressure Messages

By November 2024, Emma grew impatient and threatened to bypass Joe. Joe's response confirmed he was in final negotiations and was travelling to Manchester to meet the client.

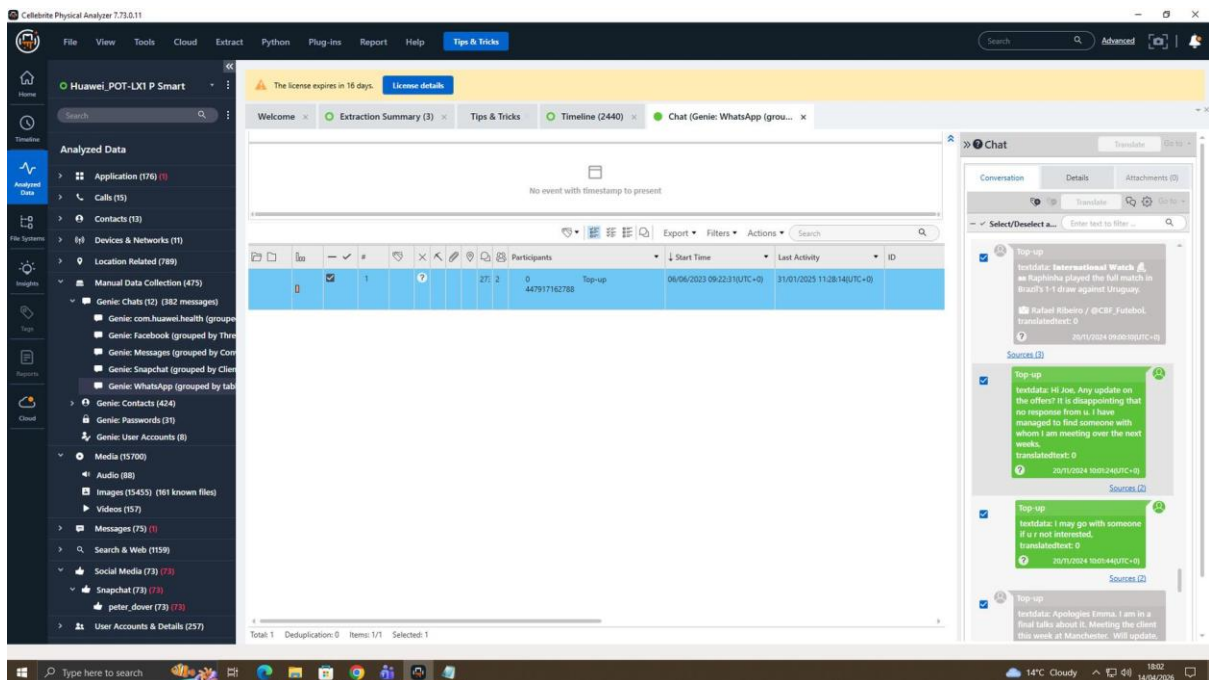


Figure 16: WhatsApp (20/11/2024 10:01) - Emma: 'Hi Joe. Any update on the offers? It is disappointing that no response from u. I have managed to find someone with whom I am meeting over the next weeks.' Clear evidence of continued criminal intent and parallel negotiations.

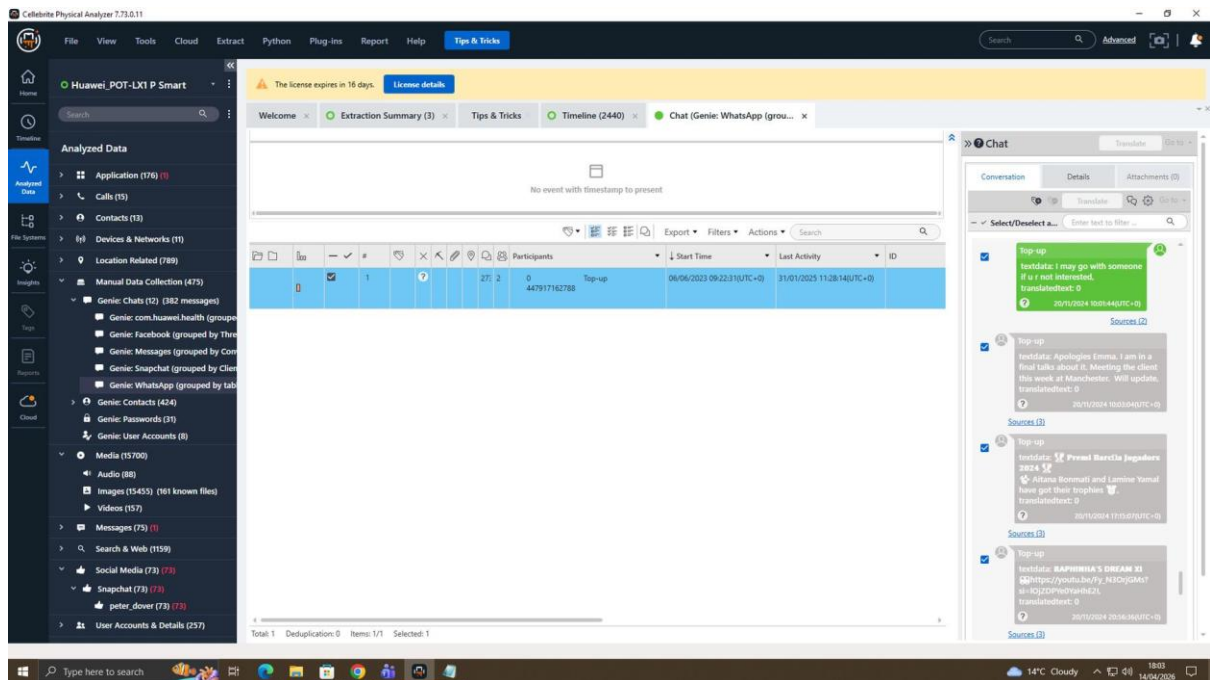


Figure 17: WhatsApp (20/11/2024 10:03) - Joe: 'Apologies Emma. I am in a final talk about it. Meeting the client this week at Manchester. Will update.' This directly corroborates the train ticket evidence showing travel to Manchester on 22 November 2024.

2.5.3 Emma's Huawei (EX-001): Snapchat Alias 'Peter Dover'

A critical finding on Emma's device is the Snapchat account 'Peter Dover' with 73 posts, clearly listed in the Cellebrite left panel under Social media > Snapchat > Peter Dover (73) across multiple screenshots. This account was specifically used to communicate with Norman Smith directly via Facebook Messenger, insulating Emma's real identity. The deliberate creation and sustained use of a false persona demonstrate premeditation and a structured attempt to obstruct any future investigation.

2.5.4 Joe's Samsung Galaxy A13 (EX-002): Corroborating Travel and Financial Evidence

Joe's Samsung Galaxy A13 (SM-A137F) was the second device extracted. The Samsung's image gallery (15,455 images) contained key corroborating evidence. GPS metadata and location records (789 total) confirm Joe's movement across Europe, the Middle East, and Africa during the investigation period, consistent with his role as an international deal broker.

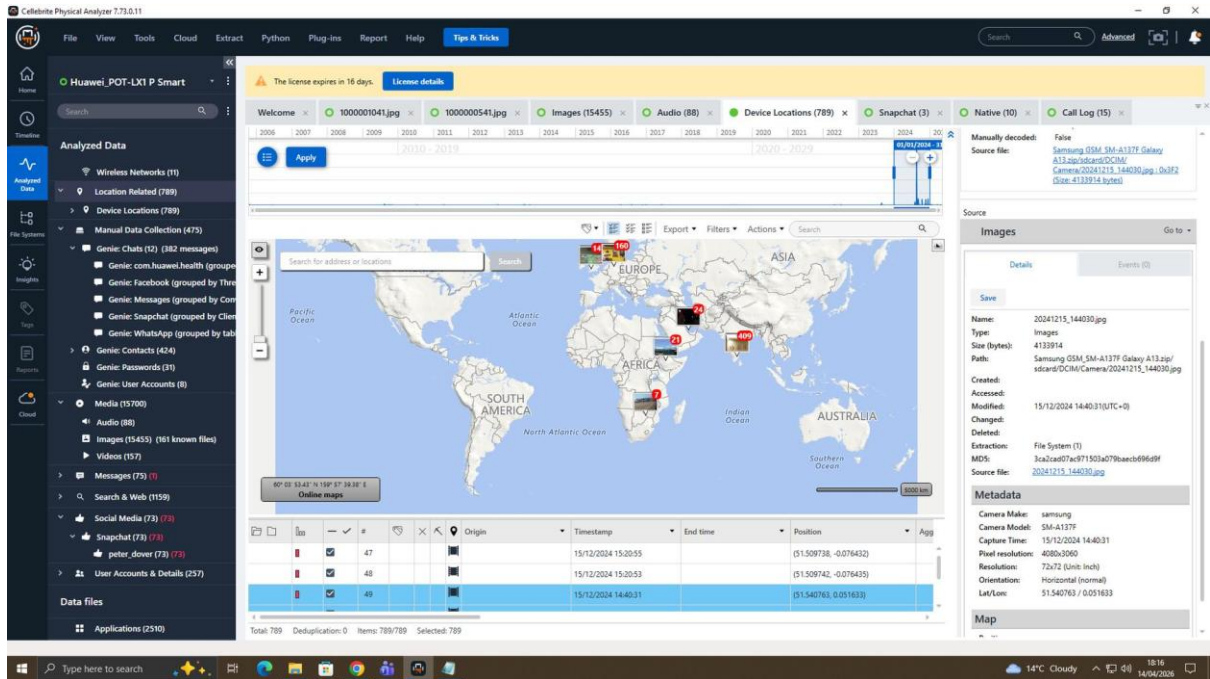


Figure 18: Cellebrite - Joe's Samsung Galaxy A13 (EX-002): Device Locations (789 records). World map shows clusters in Europe (160+), Middle East (24), Africa (409+), South America (7). Image 20241215_144030.jpg GPS: 51.540763, 0.051633 (East London), 15/12/2024 14:40 UTC.

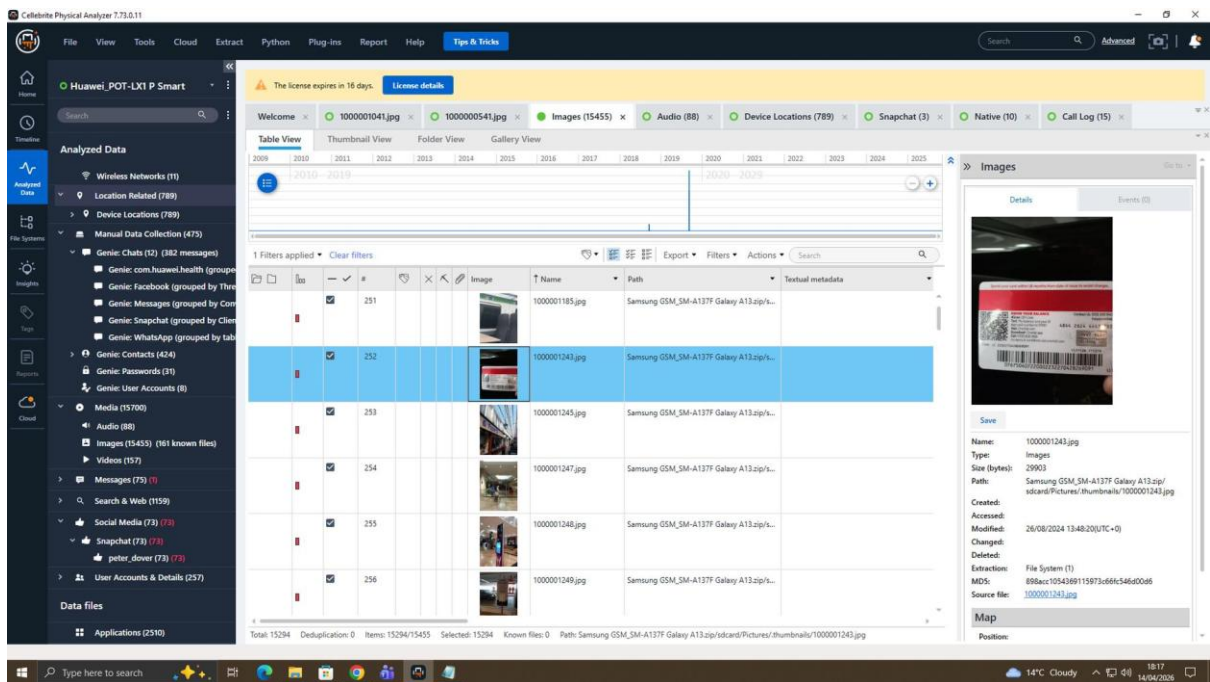


Figure 19: Joe's Samsung Galaxy A13 - Image gallery. File 1000001243.jpg (MD5: 898aac1054369115973c66fc546d00d6, Modified 26/08/2024): payment card image. Evidence of financial preparation closely following the initial 21 August 2024 conspiracy messages.

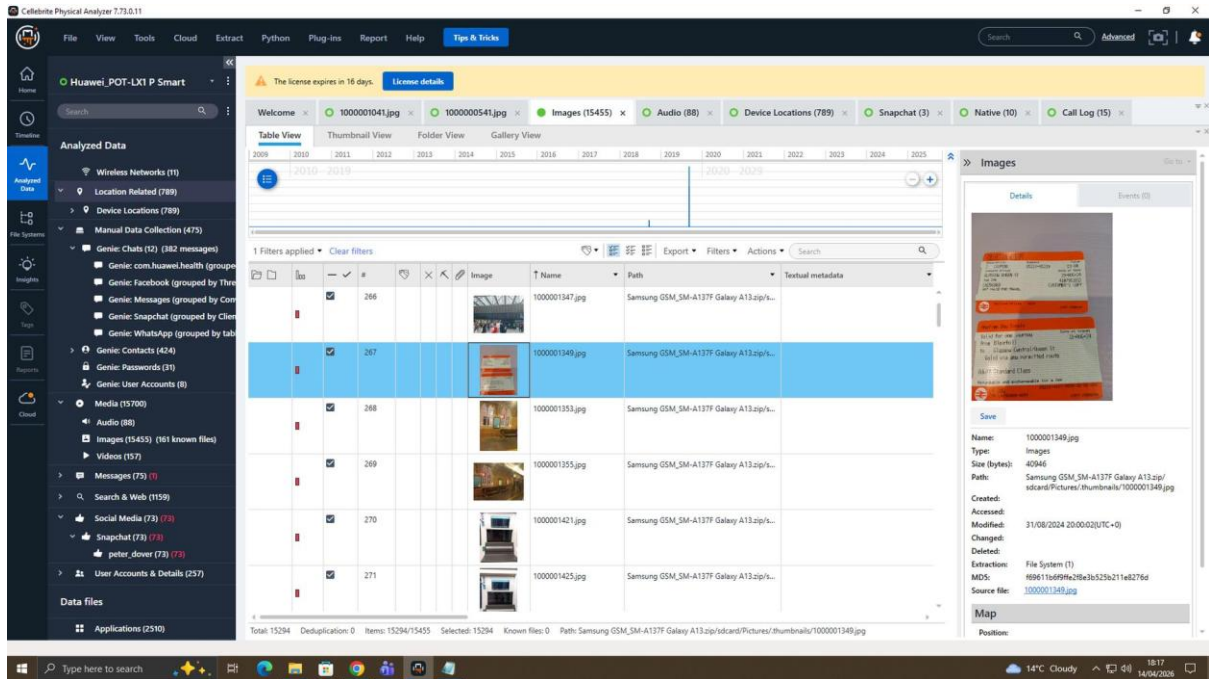


Figure 20: Joe's Samsung Galaxy A13 - Image gallery. File 1000001349.jpg (MD5: f69611b6f9ffe2f8e3b525b211e8276d, Modified 31/08/2024): National Rail train ticket image. Evidence of travel consistent with the Manchester client meeting referenced in WhatsApp.

2.5.5 Norman Smith's Nokia (EX-003): Facebook Messenger - The Finalised Sale Agreement

The Facebook Messenger conversation recovered from Norman Smith's Nokia device (EX-003) is the most decisive piece of evidence in the entire case. The conversation is between 'Peter Dover' (Emma's alias, +61565261156720) and Norman Smith (+61564326251951), taking place on 31 January 2025. It captures the completely finalised criminal agreement.

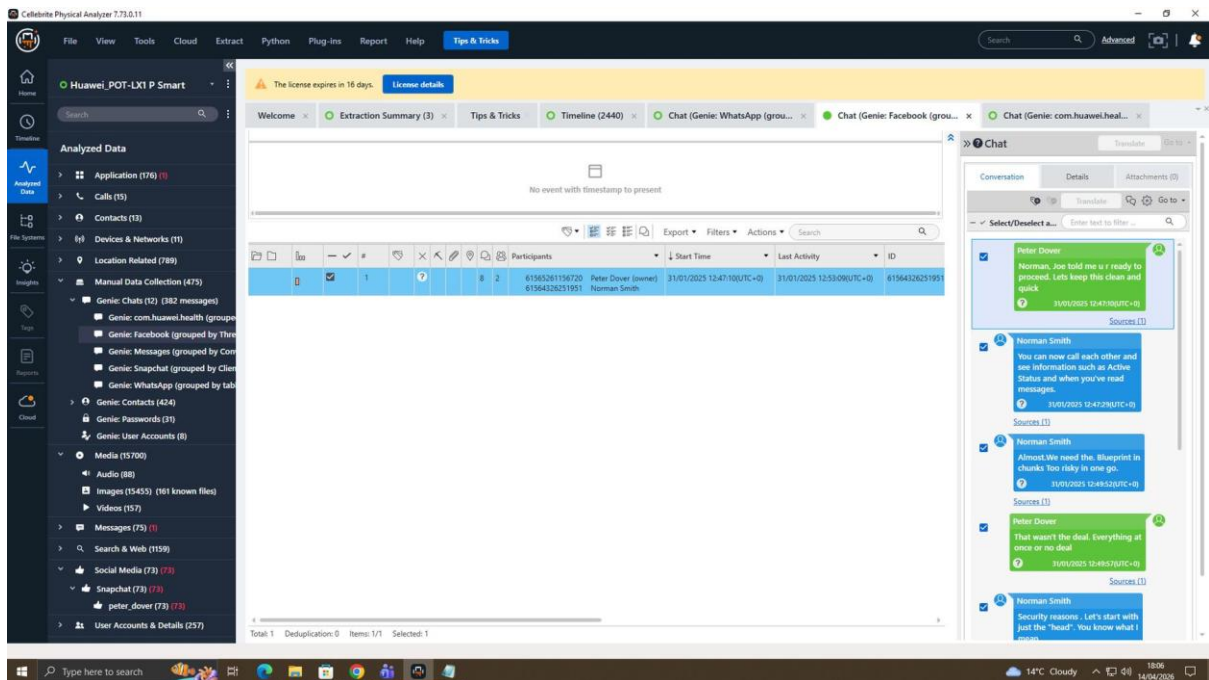


Figure 21: Cellebrite - Facebook Messenger recovered from Norman Smith's Nokia (EX-003). Participants: Peter Dover (owner) and Norman Smith. Peter Dover: 'Norman, Joe told me u r ready to proceed. Lets keep this clean and quick.' Norman: 'Almost. We need the Blueprint in chunks. Too risky in one go.' Peter Dover: 'That wasn't the deal. Everything at once or no deal.' (31/01/2025 12:47-12:49 UTC).

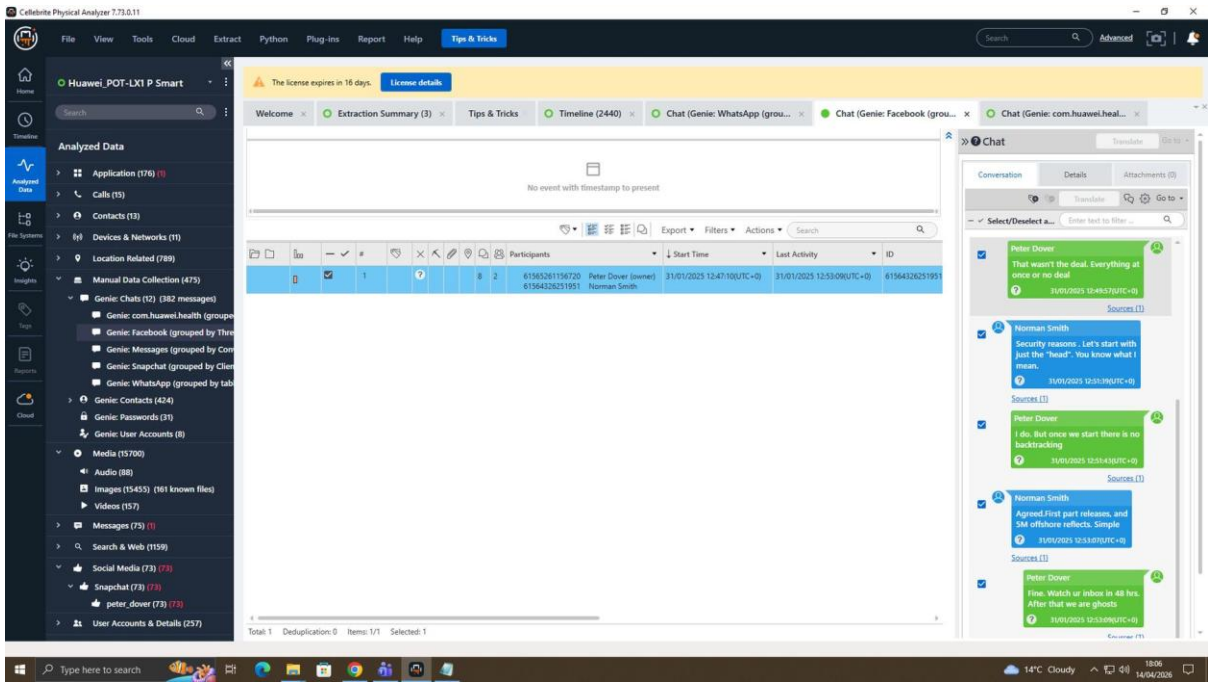


Figure 22: Facebook Messenger continuation (31/01/2025 12:51–12:53 UTC). Norman: 'Security reasons. Let's start with just the head. You know what I mean.' Peter Dover: 'I do. But once we start there is no backtracking.' Norman: 'Agreed. First part releases, and 5M offshore reflects. Simple.' Peter Dover: 'Fine. Watch ur inbox in 48 hrs. After that we are ghosts.' — \$5M offshore payment agreed; 48-hour delivery window confirmed.

Timestamp (UTC+0)	Sender	Message
31/01/2025 12:47:10	Peter Dover (Emma)	Confirms Joe vouched for Norman; instructs to proceed cleanly
31/01/2025 12:49:52	Norman Smith	Requests blueprint in chunks, citing security concerns
31/01/2025 12:49:57	Peter Dover (Emma)	Refuses staged delivery: 'Everything at once or no deal'
31/01/2025 12:51:39	Norman Smith	Requests 'just the head' first for security reasons
31/01/2025 12:51:43	Peter Dover (Emma)	Agrees: 'once we start there is no backtracking'
31/01/2025 12:53:07	Norman Smith	'Agreed. First part releases, and 5M offshore reflects. Simple.'
31/01/2025 12:53:09	Peter Dover (Emma)	'Fine. Watch Ur inbox in 48 hrs. After that we are ghosts.'

2.5.6 Call Log Analysis - Emma's Huawei (EX-001)

Emma's call log contained 15 entries, predominantly outgoing unanswered calls to Joe's number (+447917162891) and a third number (00917907025586), spanning 02 August to 19 August 2024. This pattern of repeated failed contact attempts immediately precedes the WhatsApp escalation on 21 August 2024, establishing that Emma had been urgently trying to reach Joe by voice before resorting to text-based communication.

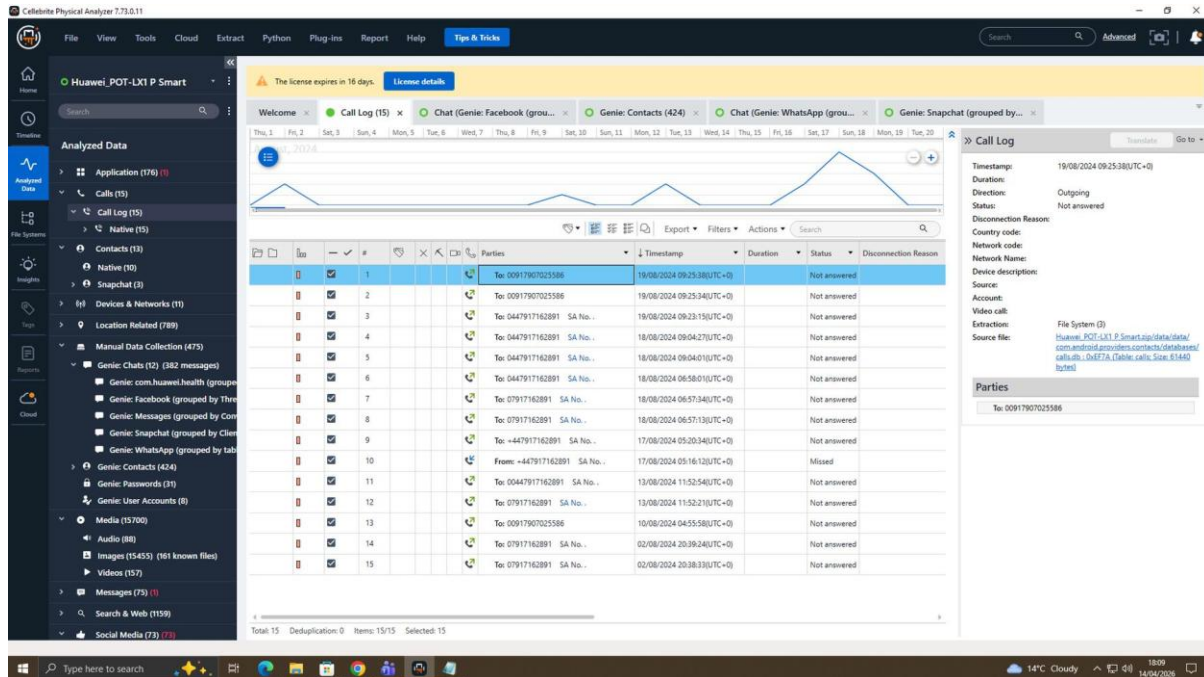


Figure 23: Cellebrite - Call Log from Emma's Huawei (EX-001). 15 entries total, predominantly outgoing unanswered/missed calls to +447917162891 (Joe) and 00917907025586, spanning 02/08/2024 to 19/08/2024. Directly precedes the WhatsApp conspiracy messages beginning 21/08/2024.

2.5.7 Travel Evidence and GPS Metadata

A National Rail digital train ticket (file 20241122_112158.jpg) was recovered from Joe's Samsung Galaxy A13 (EX-002). Route: Wigan Northwestern / Wigan Wall gate to Manchester Central Zone (WIG to MCZ), Anytime Day Single, valid 22 November 2024. GPS metadata in the file: 53.543655, -2.627383 (Wigan, UK). MD5: 551689565ac5c776dacb724bd835. This directly corroborates Joe's WhatsApp message on 20/11/2024 that he was 'Meeting the client this week at Manchester.'

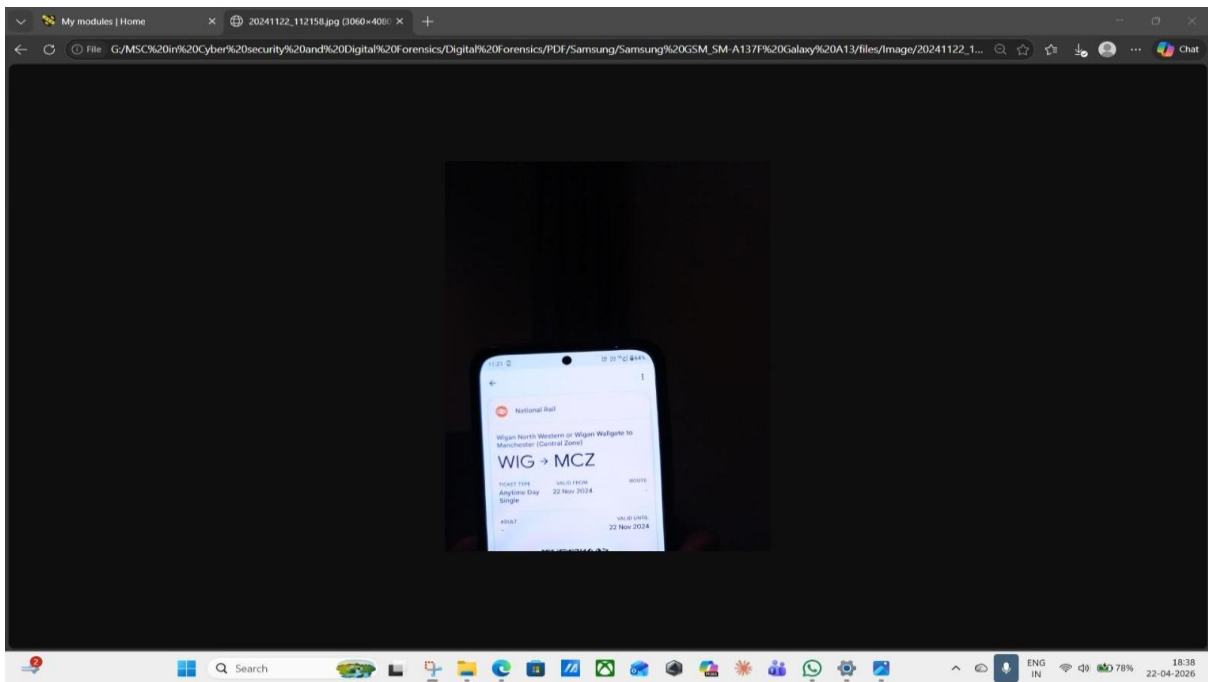


Figure 24: National Rail train ticket recovered from Joe's Samsung Galaxy A13 (EX-002) - file 20241122_112158.jpg. Route: WIG → MCZ (Wigan North Western → Manchester Central Zone). Anytime Day Single. Valid: 22 Nov 2024. GPS: Wigan, UK (53.5437N, 2.6274W).

574	Name: 20241122_112046.jpg Path: Samsung GSM_SMA137F Galaxy A13.jpg\card\DCM\Camera20241122_112046.jpg MD5: 95a49db0b55184972030adfa945a SHA256: 8308b09c004c1b0a8559a157d62f116334c04554666a6a515173844a9fc	Size (bytes): 2923955 Modified: 22/11/2024 11:20:48(UTC+0) Source file: Samsung GSM_SMA137F Galaxy A13.jpg\card\DCM\Camera20241122_112046.jpg (Size: 2923955 bytes) Meta Data: Camera Make: samsung Camera Model: SM-A137F Capture Time: 22/11/2024 11:20:48 Pixel resolution: 4080x3060 Resolution: 72x72 (Unit: Inch) Orientation: Horizontal (normal) Lat/Lon: 53.548152 / -2.626236	Image thumbnail was redacted 20241122_112046.jpg
575	Name: 20241122_112158.jpg Path: Samsung GSM_SMA137F Galaxy A13.jpg\card\DCM\Camera20241122_112158.jpg MD5: 551689565ac5c776dadb724bd8354183 SHA256: 8d905976b5411ead0d3c230cce4ff898...808419544333d030a210a3969795b684	Size (bytes): 2591232 Modified: 22/11/2024 11:21:58(UTC+0) Source file: Samsung GSM_SMA137F Galaxy A13.jpg\card\DCM\Camera20241122_112158.jpg (Size: 2591232 bytes) Meta Data: Camera Make: samsung Camera Model: SM-A137F Capture Time: 22/11/2024 11:21:58 Pixel resolution: 4080x3060 Resolution: 72x72 (Unit: Inch) Orientation: Rotate 90 CW Lat/Lon: 53.543624 / -2.627375	Image thumbnail was redacted 20241122_112158.jpg
576	Name: 20241122_180213.jpg Path: Samsung GSM_SMA137F Galaxy A13.jpg\card\DCM\Camera20241122_180213.jpg MD5: d7e173be5e6d4a0f110efc87983f23 SHA256: 63a0f46e00428224c2d059a8e5c7420f0241ec010a3367e10912813955958a	Size (bytes): 3486469 Modified: 22/11/2024 18:02:15(UTC+0) Source file: Samsung GSM_SMA137F Galaxy A13.jpg\card\DCM\Camera20241122_180213.jpg (Size: 3486469 bytes) Meta Data: Camera Make: samsung Camera Model: SM-A137F Capture Time: 22/11/2024 18:02:15 Pixel resolution: 4080x3060 Resolution: 72x72 (Unit: Inch) Orientation: Rotate 90 CW Lat/Lon: 53.543655 / -2.627383	Image thumbnail was redacted 20241122_180213.jpg

Figure 25: Cellebrite forensic report (PDF page 394/528) - Joe's Samsung SM-A137F. Entry 575 (highlighted): 20241122_112158.jpg. MD5: 551689565ac5c776dadb724bd835. SHA-256: 8d905976b5411ead0d3c230cce4ff898... Capture time: 22/11/2024 11:21:58. GPS: 53.543655, -2.627383. Confirms forensic integrity of the travel evidence.

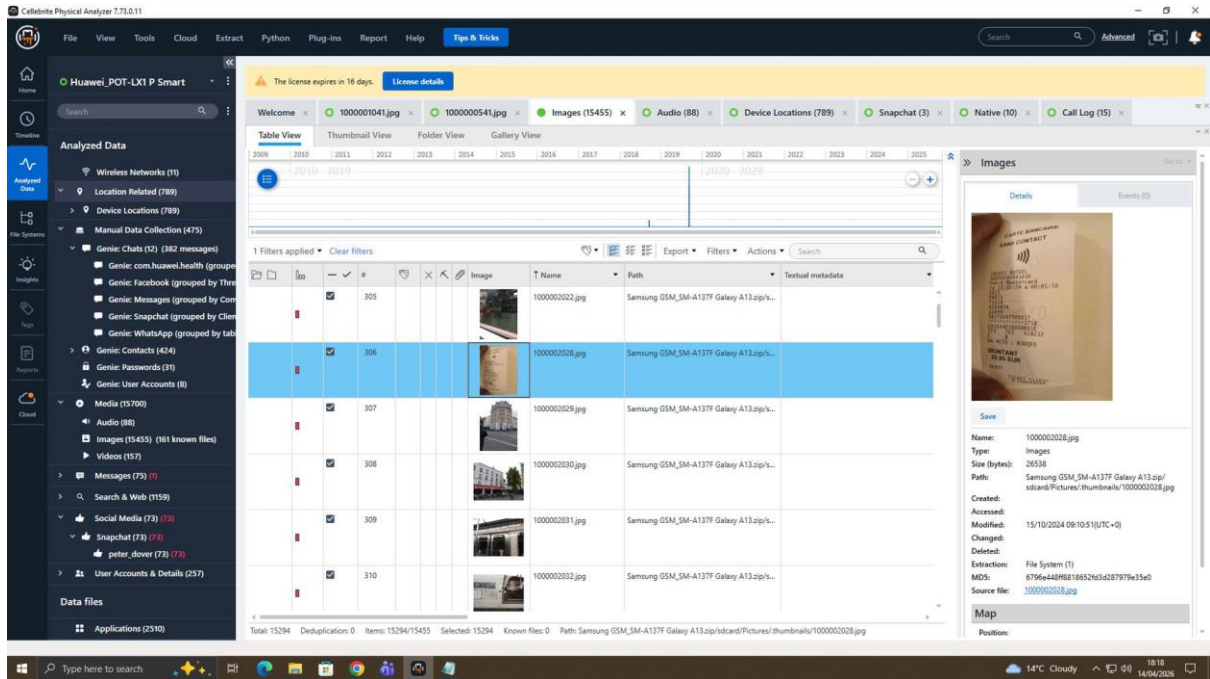


Figure 26: Joe's Samsung Galaxy A13 - File 1000002028.jpg: CARTE BANCAIRE SANS CONTACT receipt. Amount: 79.30 EUR. Modified: 15/10/2024. MD5: 6796e448ff8818652fd3d287979e35e0. Indicates financial activity (possibly preliminary payment or travel reimbursement) in a French-speaking context

2.6 Reconstructed Timeline of Events

Date / Time (UTC+0)	Event	Device / Evidence
02 Aug 2024	Emma begins repeated outgoing calls to Joe (unanswered)	Call log - Emma's Huawei EX-001 (Fig.23)
17–19 Aug 2024	Continued unanswered calls to Joe and third number	Call log - Emma's Huawei EX-001 (Fig.23)
21 Aug 2024 07:27	Emma initiates WhatsApp with Joe	WhatsApp - Emma's Huawei EX-001 (Fig.14)
21 Aug 2024 09:58	Emma discloses access to AI patent and proposes selling it	WhatsApp - Emma's Huawei EX-001 (Fig.12,13)
21 Aug 2024 10:10–11:47	Emma instructs Joe to find buyer; orders secrecy	WhatsApp - Emma's Huawei EX-001 (Fig.13,15)
Aug–Oct 2024	Bank card transaction 79.30 EUR; financial preparation	Image - Joe's Samsung EX-002 (Fig.26)
20 Nov 2024 10:01	Emma pressures Joe; threatens alternative buyer	WhatsApp - Emma's Huawei EX-001 (Fig.16)

20 Nov 2024 10:03	Joe confirms meeting buyer in Manchester this week	WhatsApp - Emma's Huawei EX-001 (Fig.17)
22 Nov 2024 11:21	Joe travels Wigan to Manchester (GPS-confirmed train ticket)	Image - Joe's Samsung EX-002 (Fig.24,25)
31 Jan 2025 12:47–12:53	'Peter Dover' (Emma) finalises \$5M offshore deal with Norman; 48h delivery	Facebook Messenger - Norman's Nokia EX-003 (Fig.21,22)

2.7 Suspect Profiling

Emma (Primary Suspect - Huawei EX-001)

Emma is a senior engineer at Quantum Tech with privileged patent database access. Evidence from her Huawei confirms she initiated the scheme, brokered the deal through Joe, used the 'Peter Dover' alias to communicate with the buyer, and personally finalised the \$5M sale. The deliberate fake identity and explicit secrecy instructions demonstrate premeditation. Applicable charges: corporate espionage, theft of intellectual property, identity fraud (Computer Misuse Act 1990 [11], Fraud Act 2006 [12]).

Joe (Intermediary - Samsung EX-002)

Joe acted as broker between Emma and Norman Smith. WhatsApp evidence on Emma's Huawei confirms he received, engaged with, and actively facilitated Emma's offer. Travel evidence on his Samsung device places him in Manchester for the client meeting. His active facilitation role makes him criminally liable as an accomplice. Applicable charges: conspiracy to commit theft of intellectual property, corporate espionage.

Norman Smith (Buyer - Nokia EX-003)

Norman Smith's Nokia yielded the Facebook Messenger evidence of the finalised sale agreement. Norman's messages demonstrate full awareness of the nature of the transaction: he requested blueprint sections, negotiated the staged payment structure, and agreed to the 48-hour delivery timeline. He is not an uninformed party. Applicable charges: receiving stolen intellectual property, conspiracy to commit corporate espionage [11][12].

2.8 Conclusion

The forensic examination of three mobile devices has produced a clear, chronologically consistent body of evidence establishing that Emma (Huawei EX-001), acting under the alias 'Peter Dover', conspired with Joe (Samsung EX-002) and Norman Smith (Nokia EX-003) to

steal and sell Quantum Tech's proprietary AI chip design patent QT-AI-2025 to NexGen Circuits.

The evidence chain begins with Emma's WhatsApp messages from her Huawei in August 2024, progresses through Joe's facilitation activity evidenced on his Samsung (including GPS-corroborated travel to Manchester), and culminates in the finalised \$5M offshore sale agreement found on Norman Smith's Nokia. No evidence exonerates any of the three suspects. The case for criminal prosecution is well-supported.

2.9 Recommendations

For Law Enforcement

- Arrest and charge Emma under the Computer Misuse Act 1990 and Fraud Act 2006 for corporate espionage, theft of intellectual property, and identity fraud [11][12].
- Charge Joe as an active accomplice under conspiracy provisions.
- Arrest and charge Norman Smith for receiving stolen intellectual property and conspiracy to commit corporate espionage.
- Obtain a production order from NexGen Circuits to determine whether any patent data was received or used in product development.
- Pursue the offshore account referenced in Facebook Messenger via MLAT for asset freezing [7].

For Quantum Tech

- Immediately revoke Emma's credentials and audit all access logs for QT-AI-2025.
- Deploy Data Loss Prevention (DLP) software to detect and block unauthorised USB transfers.
- Implement Privileged Access Management (PAM) to enforce least-privilege controls on all IP databases.
- Mandate background checks and security clearances for engineers with access to sensitive patent data.
- Enable endpoint monitoring to flag USB connections on sensitive workstations in real time.
- Strengthen NDAs and enforce breach provisions through legal counsel immediately.

References

IEEE Style — Combined References for Task 1 and Task 2

- [1] S. Garfinkel, "Digital forensics research: The next 10 years," *Digital Investigation*, vol. 7, pp. S64–S73, 2010.
- [2] Cellebrite, "State of Digital Forensics Report 2024," Cellebrite Technologies, Petah Tikva, 2024. [Online]. Available: <https://cellebrite.com> [Accessed: 20 Apr. 2026].
- [3] B. Nelson, A. Phillips, and C. Steuart, *Guide to Computer Forensics and Investigations*, 6th ed. Boston, MA: Cengage Learning, 2019.
- [4] B. Carrier and E. H. Spafford, "Getting physical with the digital investigation process," *International Journal of Digital Evidence*, vol. 2, no. 2, pp. 1–20, 2003.
- [5] (ISC)2, "Cybersecurity Workforce Study 2023," International Information System Security Certification Consortium, 2023. [Online]. Available: <https://www.isc2.org> [Accessed: 20 Apr. 2026].
- [6] Association of Chief Police Officers (ACPO), "Good Practice Guide for Digital Evidence," Version 5. London: ACPO, 2012; also International Organization for Standardization, "ISO/IEC 27037:2012 — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence," Geneva: ISO/IEC, 2012.
- [7] P. Reedy, "Interpol review of digital evidence for 2019–2022," *Forensic Science International: Synergy*, vol. 7, 100355, 2023.
- [8] M. Pollitt, "A history of digital forensics," in *Advances in Digital Forensics VI*, K. P. Chow and S. Sheno, Eds. Berlin: Springer, 2010, pp. 3–15.
- [9] Bureau of Labor Statistics, "Occupational Outlook Handbook: Information Security Analysts," U.S. Department of Labor, 2024. [Online]. Available: <https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm> [Accessed: 20 Apr. 2026].
- [10] National Institute of Standards and Technology, "Computer Security Incident Handling Guide," NIST Special Publication 800-61 Rev. 2. Gaithersburg, MD: NIST, 2012.
- [11] UK Government, "Computer Misuse Act 1990," HMSO, London, 1990. [Online]. Available: <https://www.legislation.gov.uk/ukpga/1990/18/contents> [Accessed: 20 Apr. 2026].
- [12] UK Government, "Fraud Act 2006," HMSO, London, 2006. [Online]. Available: <https://www.legislation.gov.uk/ukpga/2006/35/contents> [Accessed: 20 Apr. 2026].