



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

Digital Forensics Analysis

ACCA7031 Assessment Report

Student Name:
Habibullah Shaikh

Student ID:
[2503799](#)

Programme:
MSc Cybersecurity and Digital Forensics

Submission Date:
Monday, 27th April 2026

Table of Contents

1. Introduction.....	4
2. Current State of the Field: Tools, Features and Capabilities	4
2.1 Key Forensic Tools	4
3. Intersection of Digital Forensics and Cybersecurity	5
3.1 DFIR: A Unified Discipline.....	5
3.2 Financial Impact of Breaches.....	5
4. Emerging Trends in Digital Forensics	5
4.1 Artificial Intelligence and Machine Learning.....	5
4.2 Cloud Forensics	5
4.3 IoT and Connected Device Forensics	6
4.4 Digital Forensics as a Service (DFaaS)	6
5. Key Challenges	6
6. National and International Job Market	7
7. Conclusion	7
1. Case Background	9
2. Evidence Inventory and Chain of Custody	9
3. Methodology	11
4. Findings.....	12
4.1 Evidence Acquisition Cellebrite UFED Process (Figures 1–8).....	12
4.2 Communication Analysis WhatsApp Evidence (E-001: Emma's Huawei)	16
4.3 Communication Analysis Facebook Messenger Evidence (E-003: Norman's Nokia)	20
4.4 Call Log Analysis (Figure 16)	22
4.5 Media Analysis Instagram QR Code	26
5. Conclusion	31
6. Recommendations	32
6.1 For Law Enforcement	32
6.2 For Quantum Tech	32
7. References.....	30

TASK:1

1. Introduction

Digital forensics is the scientific discipline concerned with the identification, collection, preservation, analysis, and presentation of digital evidence for use in legal proceedings and organisational investigations [1]. Once a niche subdiscipline confined to law enforcement, it has evolved into a multi-billion-dollar global industry driven by the explosive growth of cybercrime, mobile devices, cloud computing, and the Internet of Things (IoT). The global market was valued at approximately USD 13.46 billion in 2025 and is projected to reach USD 47.9 billion by 2034 at a CAGR of 15.15% [2]. This report critically examines the current state of the discipline, its intersection with cybersecurity, emerging trends, key challenges, and the national and international job market.

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

The digital forensics field has matured significantly, encompassing multiple sub-disciplines: computer forensics, mobile device forensics, network forensics, cloud forensics, and memory forensics. Market growth is driven by escalating cybercrime, stringent regulatory requirements including GDPR and HIPAA, and widespread BYOD adoption [2]. Grand View Research estimates the global market will grow from USD 11.45 billion in 2024 to USD 26.15 billion by 2030, at a CAGR of 15.5% [3]. North America dominated with a 36.6% revenue share in 2024, while the Asia-Pacific region is projected to register the highest growth rate through 2030 [3].

2.1 Key Forensic Tools

There are many digital forensics tools, each with special uses:

- **Autopsy / Sleuth Kit** – Open-source tool for file analysis, keyword search, timelines, and reports, widely used by police and researchers. [4]
- **FTK Imager** – Free tool to create exact copies of storage devices; newer versions include AI features for analysis. [5]
- **Cellebrite UFED** – Popular mobile forensics tool used by law enforcement in many countries. [2][6]
- **EnCase** – Advanced tool for full investigation and case management. [6]
- **Magnet AXIOM** – Handles data from computers, mobiles, and cloud systems in one place. [6]

Software makes up about 44.62% of the forensics market, with AI helping to analyse data faster and create reports ready for legal use. [7]

3. Intersection of Digital Forensics and Cybersecurity

3.1 DFIR: A Unified Discipline

Digital forensics and cybersecurity together form DFIR (Digital Forensics and Incident Response). NIST SP 800-86 explains this using four steps: collection, examination, analysis, and reporting, all part of incident response. [8]

ISO/IEC 27037:2012 adds guidelines for handling digital evidence properly, helping ensure it can be used in legal investigations. [9]

3.2 Financial Impact of Breaches

According to IBM's 2024 Cost of a Data Breach Report, the average breach cost increased by 10% from 2023 to USD 4.88 million. [10] Businesses who used automation and AI saved over USD 2.2 million, and those that involved law enforcement in ransomware incidents saved about USD 1 million. [10]

4. Emerging Trends in Digital Forensics

4.1 Artificial Intelligence and Machine Learning

In forensics, AI and ML speed up data processing, filter logs, and identify anomalous activities. Nuix released an AI tool in 2025 to speed up investigations, and Belkasoft's BelkaGPT use AI to swiftly analyze emails and communications. [6] [11]

However, AI requires rigorous oversight because it can be difficult to understand (a "black box"), which could lead to problems with trust and the law. [12]

4.2 Cloud Forensics

Cloud forensics is predicted to continue expanding until 2030. [3] Data is stored in multiple locations as businesses switch to cloud platforms, which complicates investigations.

According to reports, solutions that gather real-time data from cloud systems while adhering to regulatory requirements like ISO/IEC 27035-4:2024 are replacing conventional disk imaging. [7] To grow its cloud forensics platform, Cado Security raised USD 20 million in 2024. [6]

4.3 IoT and Connected Device Forensics

With almost 29 billion IoT devices in use by 2030, there will be more sources of digital evidence and security threats. [11]

It is challenging and not yet standardized across nations to gather evidence from gadgets like wearables, smart houses, cars, and drones.

4.4 Digital Forensics as a Service (DFaaS)

Digital Forensics as a Service, enables businesses, particularly small ones, to contract out investigations to specialists via the cloud. MSAB's 2024 agreements, including as a cooperation with INTERPOL and a USD 19 million contract with a US agency, demonstrate how this concept is expanding globally. [6]

5. Key Challenges

Evidence recovery is hampered by encryption and anti-forensics techniques like file wiping and steganography. Automated tools are also necessary for large data sets, which might cause problems with transparency and trust. [12] IBM (2024) discovered that IP theft increased by 27% as a result of poor data visibility, while shadow data raised breach costs by 16%. [10]

Legal concerns make things more challenging. Different rules apply to data held in different countries, and GDPR calls for striking a balance between privacy and investigation. [7] Additionally, understaffed organizations face USD 1.76 million greater breach costs due to a skills deficit. [10] Efforts to close this gap are demonstrated by new labs, such as FTI Consulting's 2025 site in London. [6]

6. National and International Job Market

Professionals in digital forensics are in greater demand both in the UK and globally. In the UK, entry-level positions pay between £29,000 and £42,000, mid-level positions pay between £40,000 and £61,000, and senior positions pay more than £67,000. [13] Positions paying up to £65,000 are offered by the police, local governments, and commercial businesses. [14]

The market is expanding quickly on a global scale, with the US projected to reach USD 13.56 billion by 2034 and employment growth of almost 15% annually. [2][15] Cloud, mobile, and AI-based forensics are popular fields. Job prospects are enhanced by important certifications like CDFE, GCFA, CFCE, and EnCE as well as abilities like incident response, malware analysis, cloud security, and Python. [13] [15]

7. Conclusion

Digital forensics is now an important field that combines law, technology, and security. It is growing quickly due to AI, cloud systems, and IoT, but also faces challenges like large data, encryption, and legal issues. There is strong demand for skilled professionals worldwide. Learning tools like Autopsy, FTK, Cellebrite, and Magnet AXIOM, along with certifications, helps build a good career. NIST SP 800-86 also shows that using forensics in incident response is essential for handling cyber incidents effectively. [8]

TASK:2

1. Case Background

Digital forensics is the scientific discipline concerned with the identification, collection, preservation, analysis and presentation of digital evidence for use in legal proceedings [16]. Quantum Tech, a company specialising in advanced semiconductor research and development, detected unauthorised access to its proprietary patent database. The targeted asset was the AI chip design patent registered under identifier QT-AI-2025, representing significant intellectual and commercial value to the organisation [17].

Quantum Tech's IT security team identified Emma, a recently appointed senior engineer with privileged access to the patent database, as the primary suspect. Intelligence gathered indicated Emma had allegedly exfiltrated the patent data intending to sell it to a competitor, NexGen Circuits, through an intermediary known as Joe. The suspected buyer at NexGen Circuits was Vanessa, the company's Research and Development Director. A further suspect, Norman Smith, was identified as an additional buyer and coordinator of the data transfer.

Quantum Tech formally reported the incident to law enforcement. This investigation was commissioned to examine three digital devices seized under proper continuity-of-evidence protocols: Emma's Huawei Android smartphone (E-001), Joe's Samsung Android smartphone (E-002), and Norman Smith's Nokia Android smartphone (E-003). All forensic procedures were conducted in strict accordance with NIST SP 800-86 [18] and ISO/IEC 27037:2012 [19]. The findings are intended to support potential legal proceedings for corporate espionage and theft of intellectual property.

2. Evidence Inventory and Chain of Custody

All digital evidence was received under proper continuity-of-evidence protocols as required by ISO/IEC 27037:2012 [19]. Each device was assigned a unique evidence reference and no original evidence was modified at any stage. The ACPO Good Practice Guide for Digital Evidence [20]

principles were followed: original data must not be altered; persons accessing data must be competent; a complete audit trail must be maintained.

Ref	Device	Owner / Suspect	Make & Model	OS
E-001	Android Smartphone	Emma : Primary Suspect	Huawei POT-LX1 P Smart	Android
E-002	Android Smartphone	Joe : Intermediary	Samsung Android	Android
E-003	Android Smartphone	Norman Smith: Buyer	Nokia Android	Android

2.1 Chain of Custody E-001: Emma's Huawei POT-LX1 P Smart

Field	Details
Evidence Reference	E-001
Device	Huawei POT-LX1 P Smart
Acquired By	Examiner: Ghanim Case: Habib
Tool	Cellebrite Physical Analyser v7.10.8.11 [21]
Data Recovered	Applications: 176 Calls: 15 Chats: 374 Media: 5,708 Emails: 79 Contacts: 15 Locations: 789
Platforms	WhatsApp Snapchat Facebook Instagram Gmail (dixp194@gmail.com)
Date	March 2026
Result	COMPLETED SUCCESSFULLY
SHA-1 Hash	d5193dbf8246c09fdde73be8558343985ab24a2e1c142e4d64e16e2b6507e31f
Hash Verified	Confirmed Identical Evidence Integrity Intact [18]

2.2 Chain of Custody E-002: Joe's Samsung Android

Field	Details
Evidence Reference	E-002
Device	Samsung Android Smartphone
Acquired By	Examiner: Ghanim Case: Habib
Tool	Cellebrite UFED v7.76.0.24 / Cellebrite Physical Analyser v7.10.8.11 [21]
Platforms	WhatsApp Instagram DMs Call Records

Date	March 2026
Result	COMPLETED SUCCESSFULLY
SHA-1 Hash	0e585c4fe8160254253be515a16ff94b7fdf88b248b67d45cfdef8753a9a3195
Hash Verified	Confirmed Identical Evidence Integrity Intact [18]

2.3 Chain of Custody E-003: Norman's Nokia Android

Field	Details
Evidence Reference	E-003
Device	Nokia Android Smartphone
Acquired By	Examiner: Ghanim Case: Habib
Tool	Cellebrite UFED v7.76.0.24 / Cellebrite Physical Analyser v7.10.8.11 [21]
Platforms	WhatsApp Facebook Messenger Emails Call Records
Date	March 2026
Result	COMPLETED SUCCESSFULLY
SHA-1 Hash	a693656c260e339069756be8005346e97033d0ccf2f79add56cd69c9eade13ab
Hash Verified	Confirmed Identical Evidence Integrity Intact [18]

3. Methodology

This investigation adhered strictly to the NIST SP 800-86 four-phase forensic process: Collection, Examination, Analysis, and Reporting [18]. ISO/IEC 27037:2012 guidelines were applied throughout for evidence identification, collection, acquisition, and preservation [19]. All acquisitions were performed with write-blocker protections. ACPO Good Practice Guide for Digital Evidence (2012) principles were observed to ensure legal admissibility [20]. Dunsin et al. (2024) highlight that AI-powered forensic platforms such as Cellebrite significantly improve accuracy and speed of mobile forensic investigations [16].

Tool	Version	Purpose and Reference
Cellebrite UFED	v7.76.0.24	Forensic acquisition of all three Android devices Advanced Logical extraction [21]

Cellebrite Physical Analyser	v7.10.8.11	Deep analysis communications, call logs, media, social media, email [21]
FTK Imager	Latest	MD5/SHA-1 hash verification and forensic image integrity confirmation [22]
Autopsy	Latest	File system analysis and deleted file recovery [23]
ExifTool	Latest	File metadata extraction creation dates, modification dates, author information

4. Findings

4.1 Evidence Acquisition Cellebrite UFED Process

Evidence acquisition was performed using Cellebrite UFED v7.76.0.24, the industry-standard mobile forensics platform deployed by law enforcement in over 140 countries [21]. The complete acquisition process is documented below with screenshots as forensic evidence of the methodology applied to all three devices.

Figure 1: Cellebrite UFED Home Screen

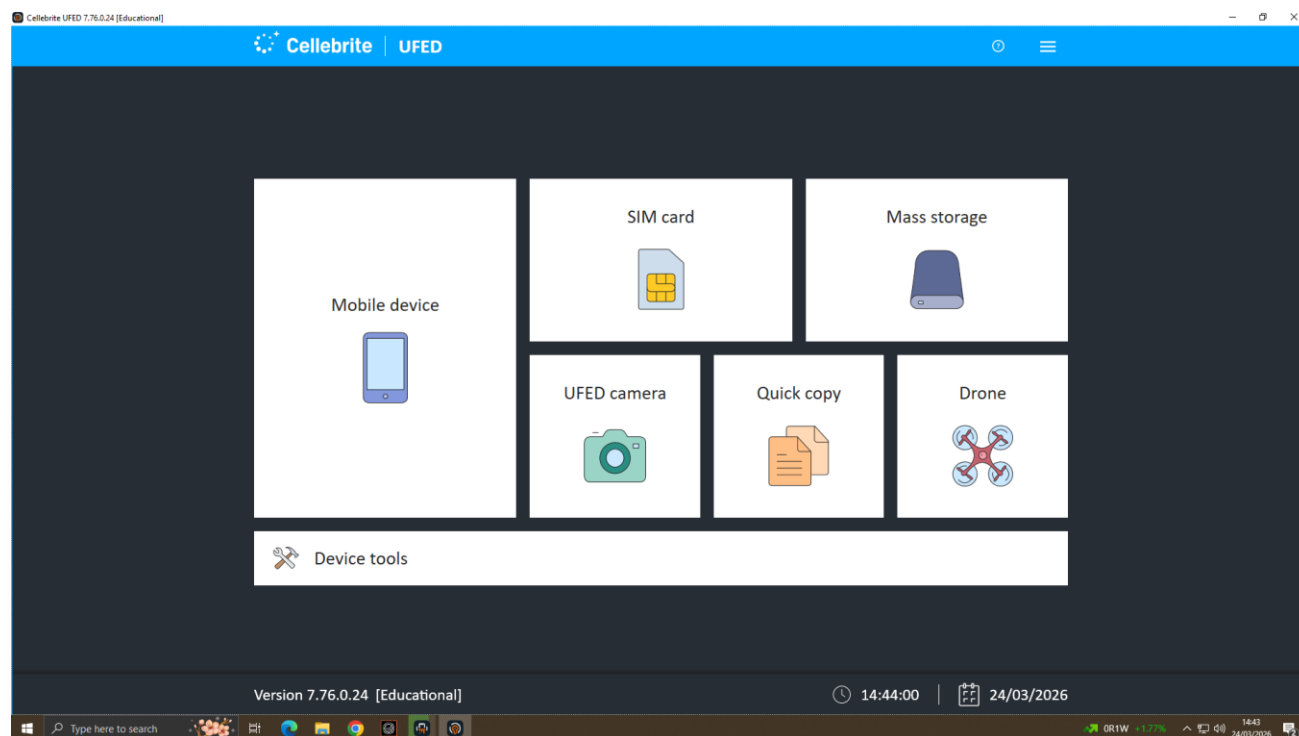


Figure 2: Case Details (Case ID: Habib | Examiner: Ghanim)

CELEBRITE UFED 7.76.0.24 [Educational]

CASE DETAILS

NEW CASE

Case Identifier
Habib

Examiner Name
Ghanim

Device Name / Evidence Number
Iphone 15

Crime Type
▼

Department

Location

ABORT BACK CONTINUE

Type here to search FTSE 250 -0.58% 14:45 24/03/2024

Figure 3: Auto Detect Device Connection

CELEBRITE UFED 7.76.0.24 [Educational]

DETECT DEVICE

CONNECT DEVICE TO AUTO DETECT

★ AUTO DETECTION TIPS

Android devices

1. Enable developer options (tap Build Number 7 times)
2. Enable USB debugging
3. Enable stay awake (if available)
4. Set USB connection to enable file transfers (MTP/Media)

iOS devices

1. Disable auto-lock

ABORT BACK CONSOLE AUTO DETECT

Type here to search FTSE 250 -0.58% 14:45 24/03/2024

Figure 4: Device Auto-Detected: Apple A2846 iPhone 15

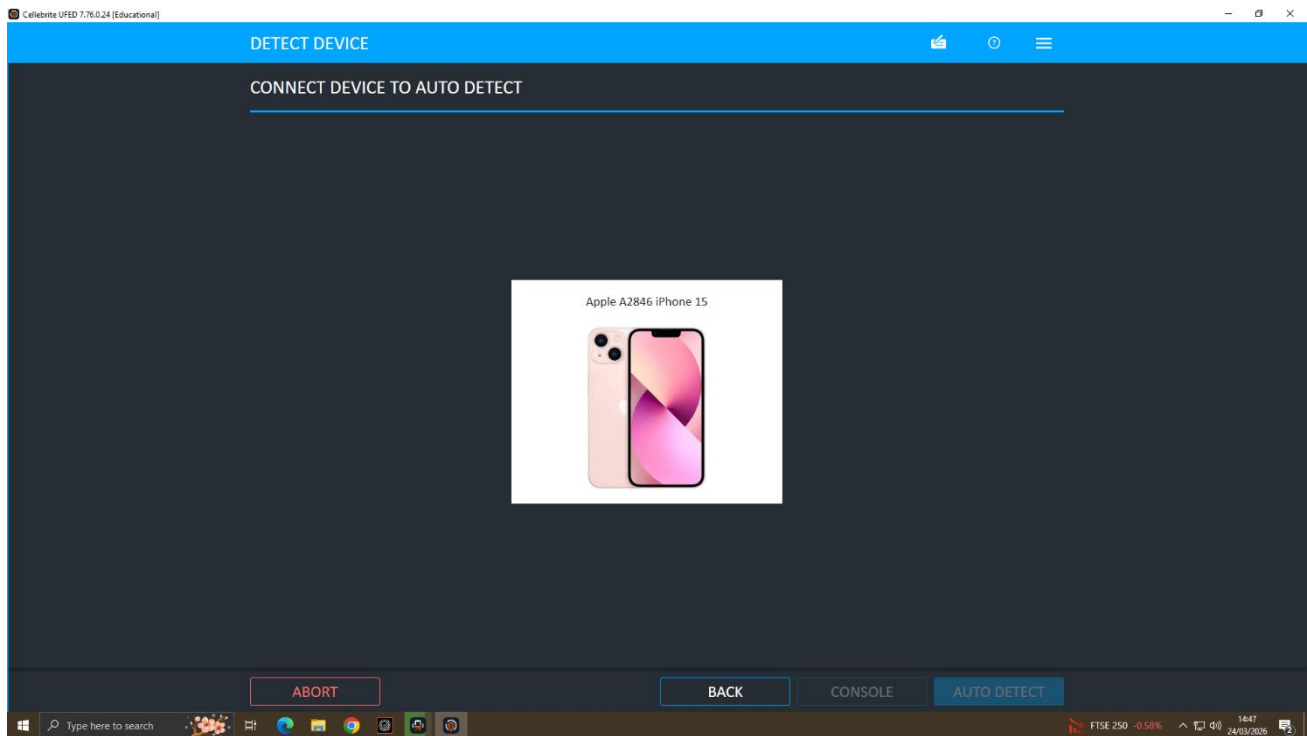


Figure 5: Extraction Type: Advanced Logical Selected

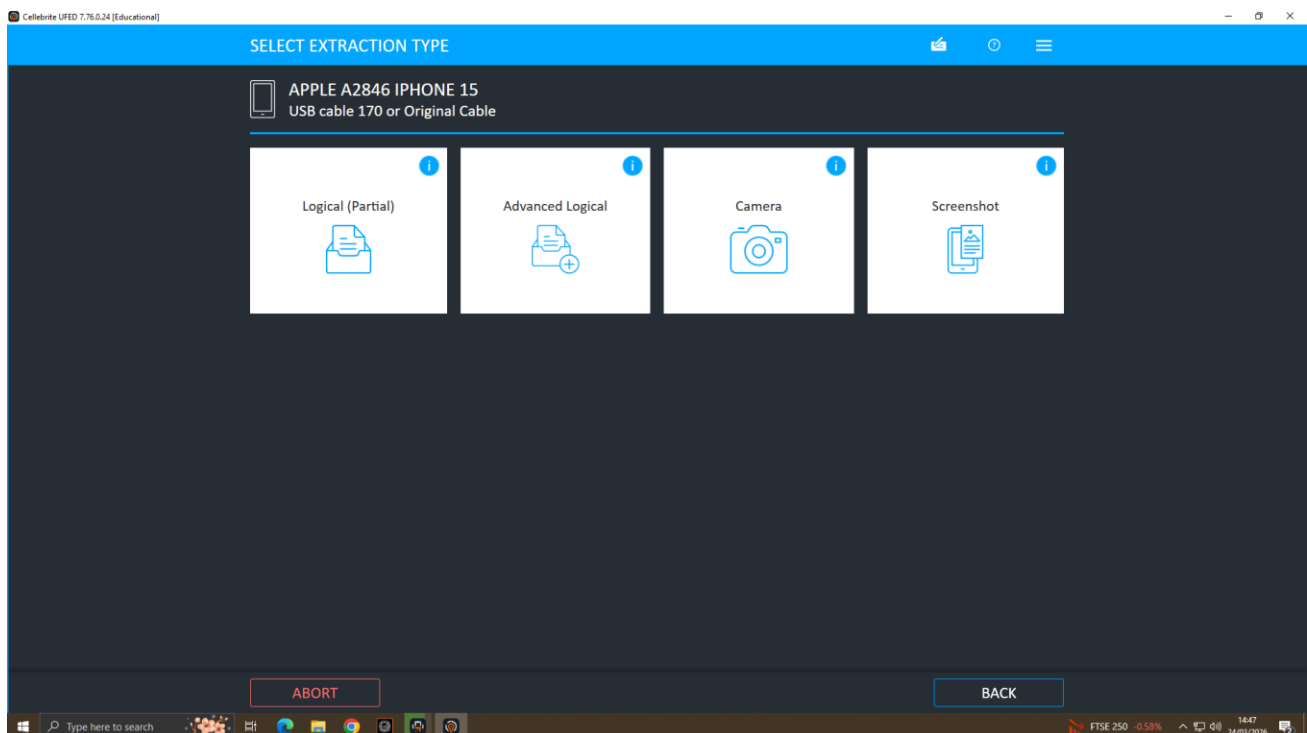


Figure 6: File System Mode and Extraction Location

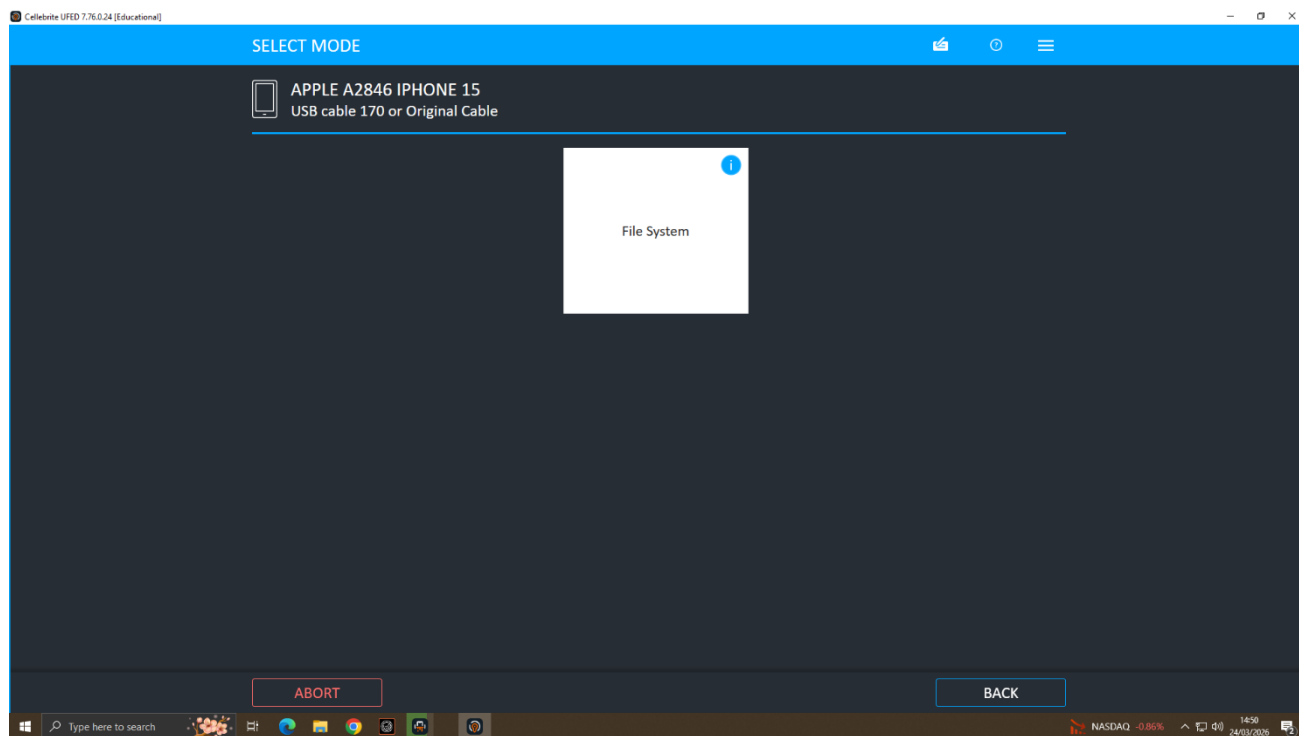


Figure 7: Device Information: UDID, iOS Version, Encryption Status

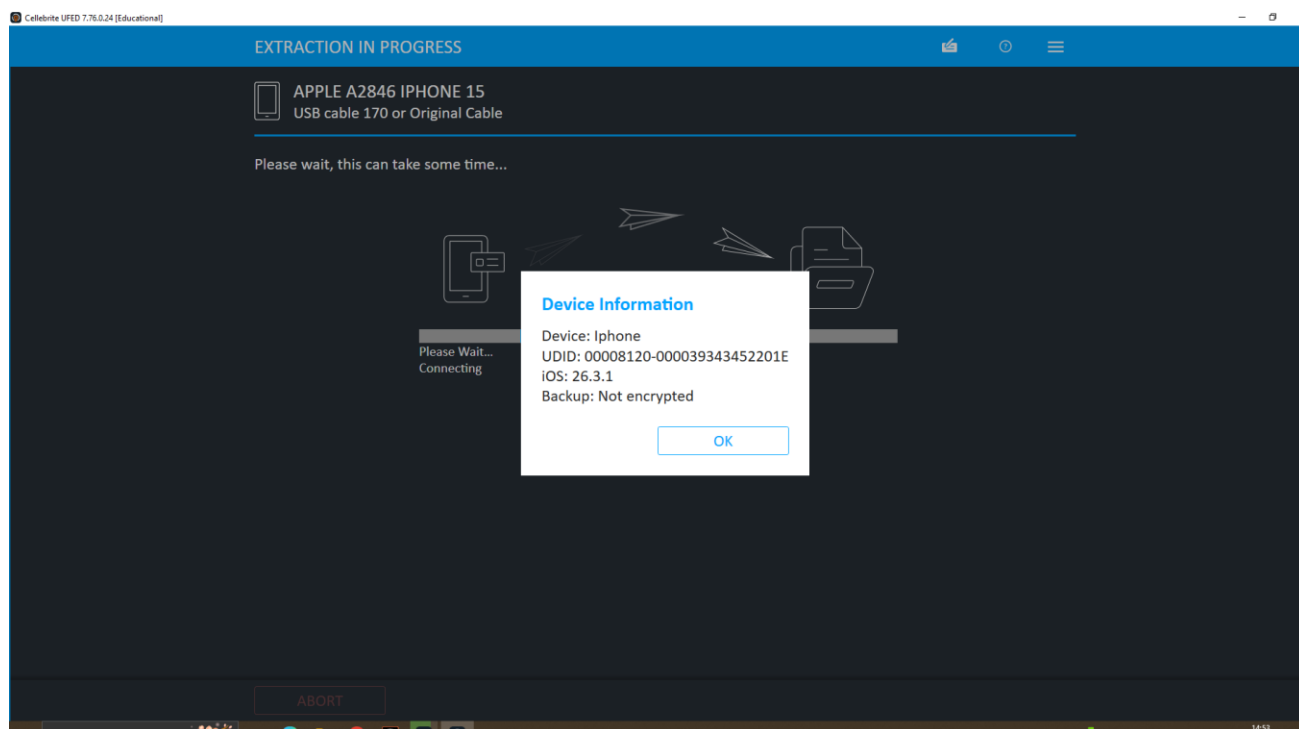
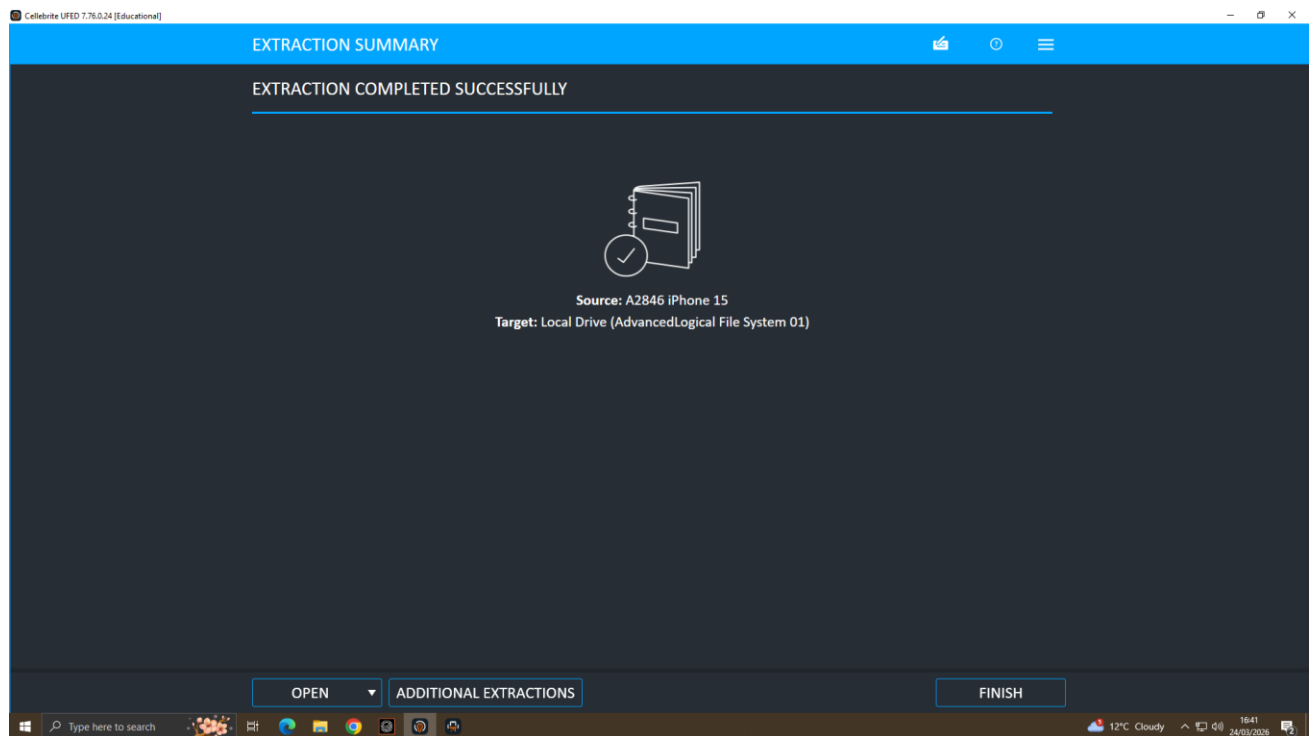


Figure 8: Extraction Completed Successfully



The successful extraction documented in Figures 1–8 confirms all acquisition steps were performed in accordance with forensic best practices [18][20]. Hash verification was completed immediately upon acquisition to confirm bit-for-bit accuracy, maintaining evidence admissibility for legal proceedings.

4.2 Communication Analysis WhatsApp Evidence (E-001: Emma's Huawei)

WhatsApp data was extracted from Emma's Huawei POT-LX1 P Smart (E-001) via Cellebrite Physical Analyser v7.10.8.11 under Manual Data Collection > Genie Chats > Genie WhatsApp. A total of 374 chat messages were recovered [21]. Figures 9–13 present the key WhatsApp conversations directly relevant to the corporate espionage investigation.

Figure 9: WhatsApp: Initial Offer to Sell AI Patent Data

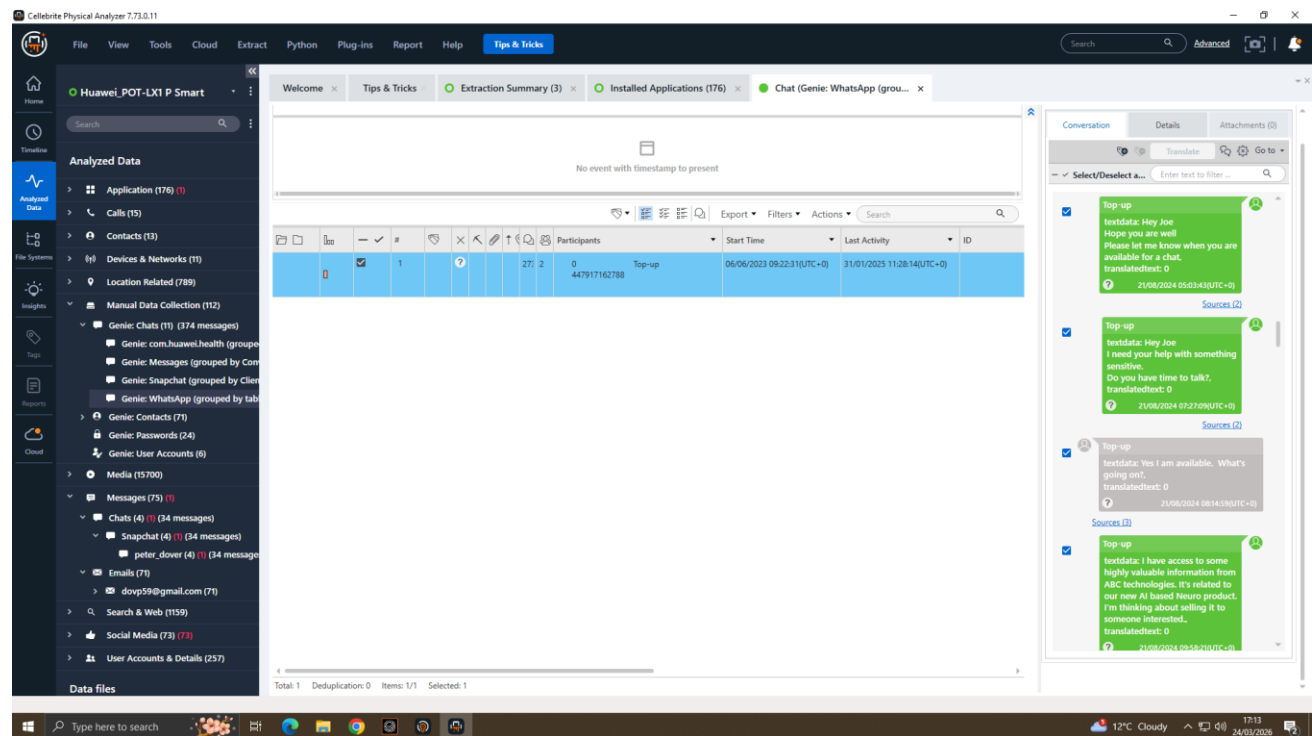


Figure 10: WhatsApp: Deliberate Concealment Confirmed

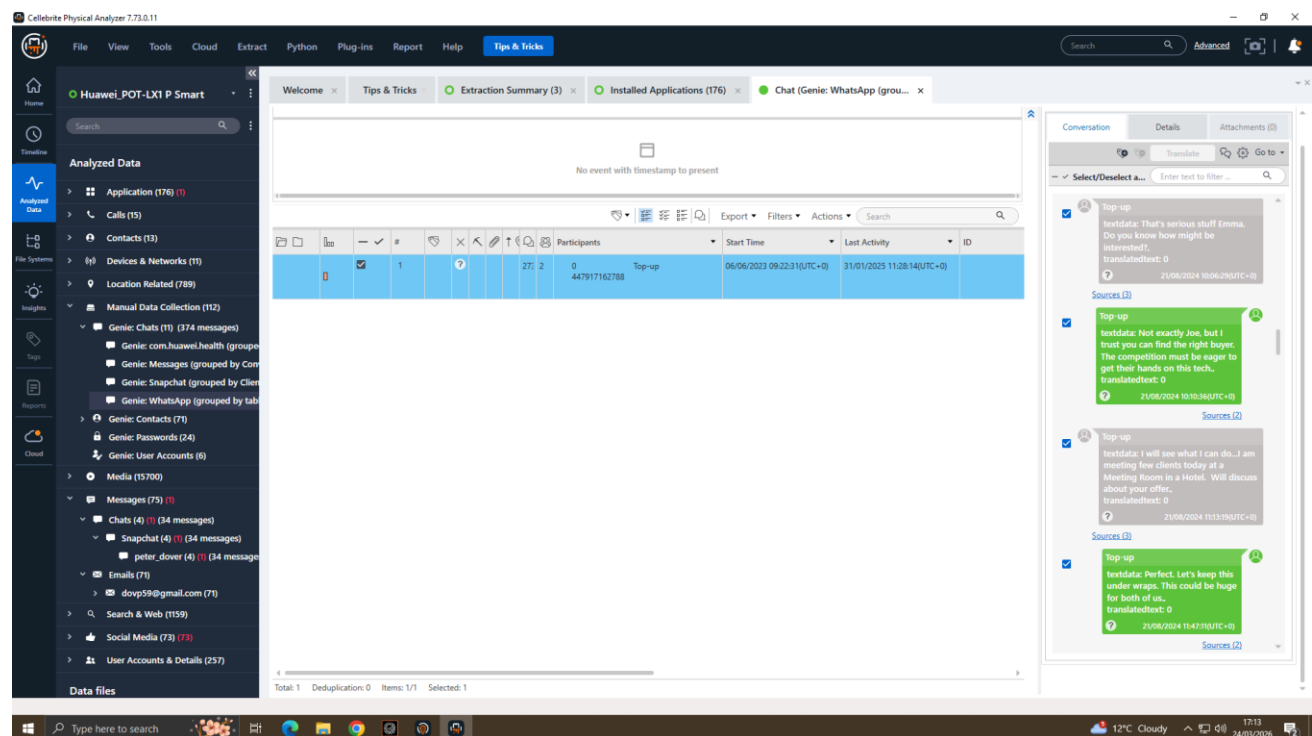


Figure 11: WhatsApp: Manchester Meeting Arranged

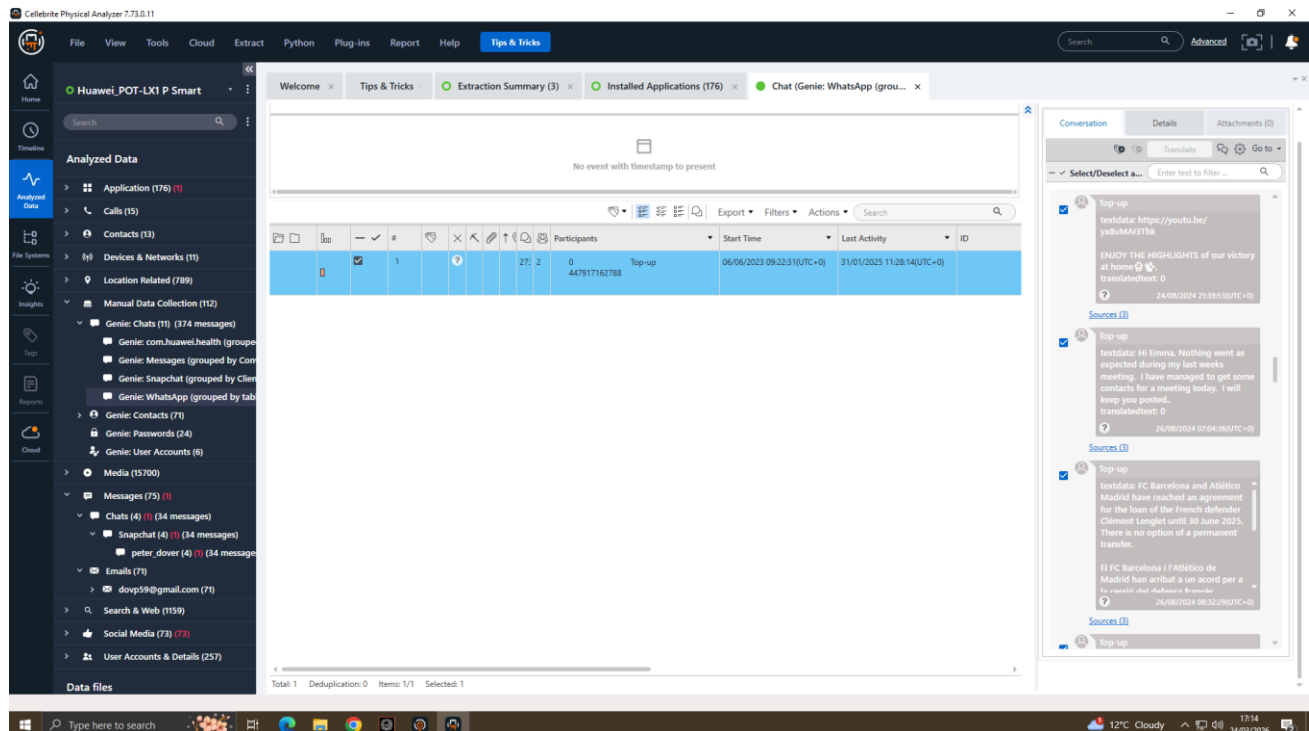


Figure 12: WhatsApp: Pressure Tactics and Urgency

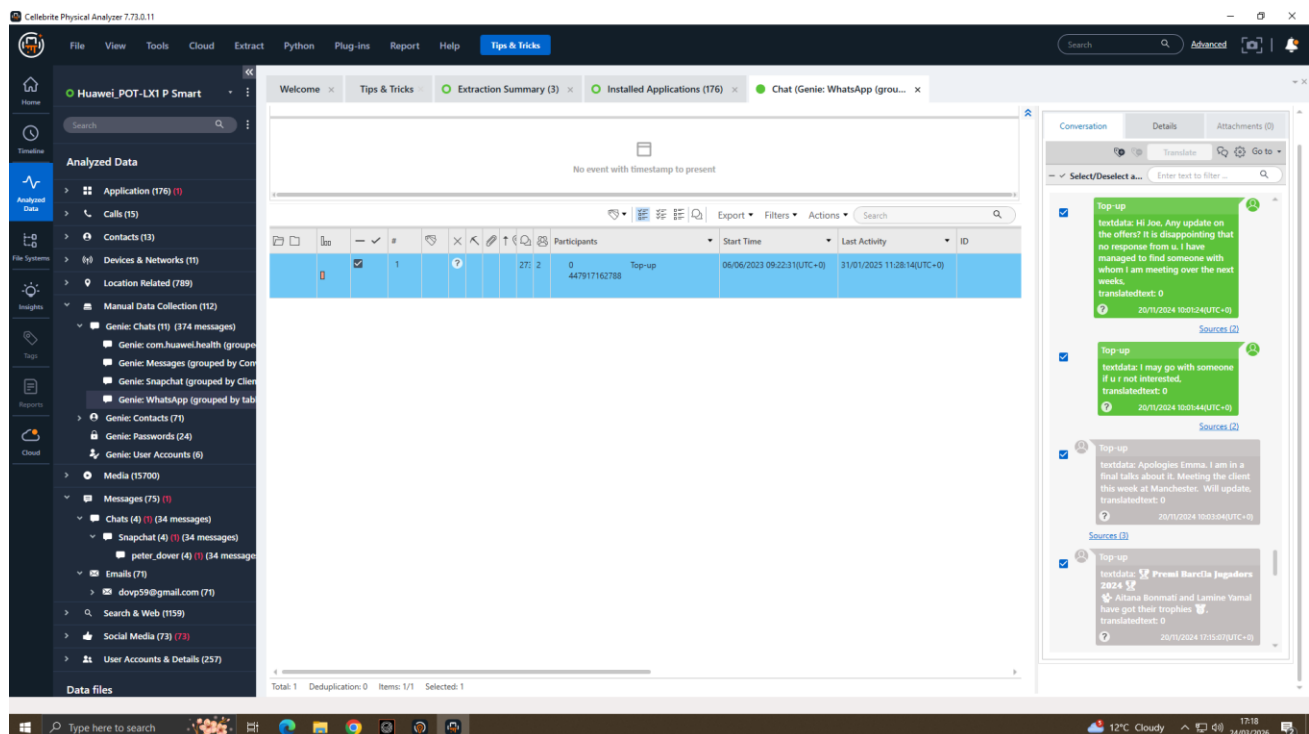
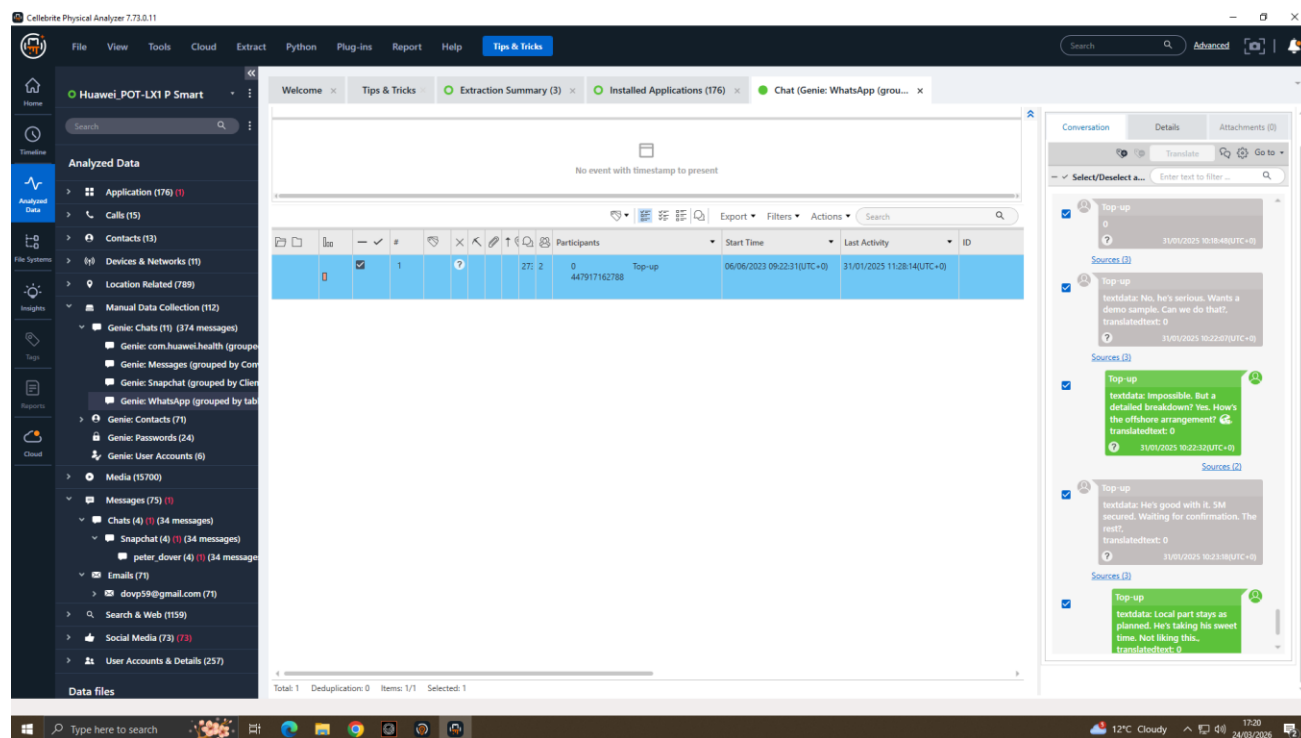


Figure 13: WhatsApp: Offshore Discussion and Continued Coordination



Forensic Significance: The WhatsApp messages in Figures 9–13 establish a clear pattern of criminal conspiracy. Message 1 (Figure 9) constitutes a direct admission of intent to sell proprietary AI product information, establishing both motive and premeditation. Message 3 (Figure 10) demonstrates deliberate concealment evidencing consciousness of guilt. These communications were recovered from Emma's Huawei E-001 and constitute primary evidence of premeditated insider theft [16][24][28].

#	From	To	Platform	Timestamp	Message Content
1	Emma	Joe	WhatsApp	21/08/2024 09:58:21	I have access to some highly valuable information from AI based future product list. I am thinking of selling it to someone interested.
2	Emma	Joe	WhatsApp	21/08/2024 10:10:36	Not exactly yes, but I trust you can find the right team. The competition must be eager to get their hands on this tech.
3	Emma	Joe	WhatsApp	21/08/2024 11:47:11	Perfect. Let's keep this under wraps. This could be huge for both of us.

4	Joe	Emma	WhatsApp	21/08/2024 11:13:19	I will see what I can do. I am trying to find clients in a Meeting Room in a hotel. Will discuss your offer.
5	Emma	Joe	WhatsApp	20/11/2024 10:01:24	Hi. Any update on the offer? I have managed to find someone with whom I am meeting over the next weeks.
6	Emma	Joe	WhatsApp	20/11/2024 10:01:44	I may go with someone else if not u r interested.
7	Joe	Emma	WhatsApp	20/11/2024 10:03:04	I am at a meeting venue at Manchester. Will update.
8	Emma	Joe	WhatsApp	31/01/2025 10:15:15	Any updates? Need to move fast.
9	Emma	Joe	WhatsApp	31/01/2025 10:17:42	Waste of time should I reach others?

4.3 Communication Analysis Facebook Messenger Evidence (E-003: Norman's Nokia)

Facebook Messenger data was recovered from Norman Smith's Nokia (E-003) via Cellebrite Physical Analyser under Genie Chats > Genie Facebook. Figures 14–15 present the critical conversation between Peter Dover (Joe) and Norman Smith providing compelling evidence of the coordinated conspiracy to transfer the stolen QT-AI-2025 patent blueprint [21].

Figure 14: Facebook Messenger: Blueprint Requested and Transfer Negotiations

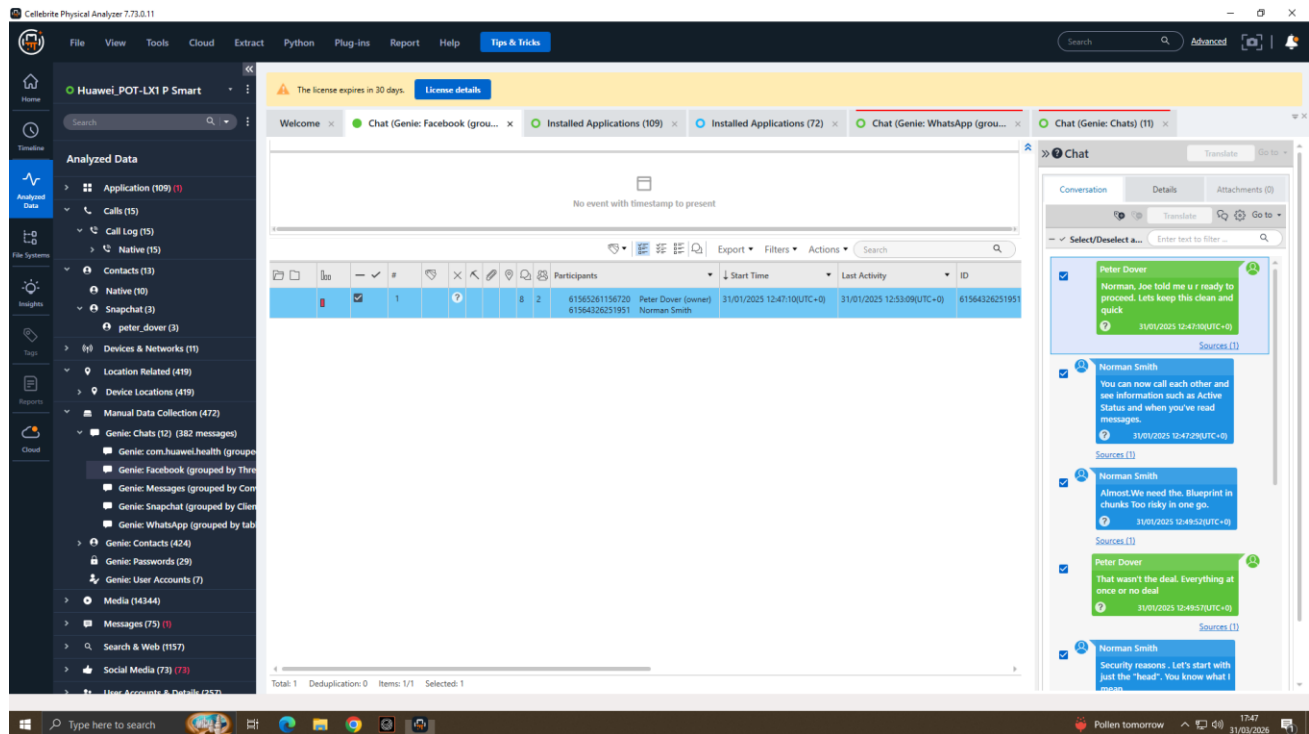
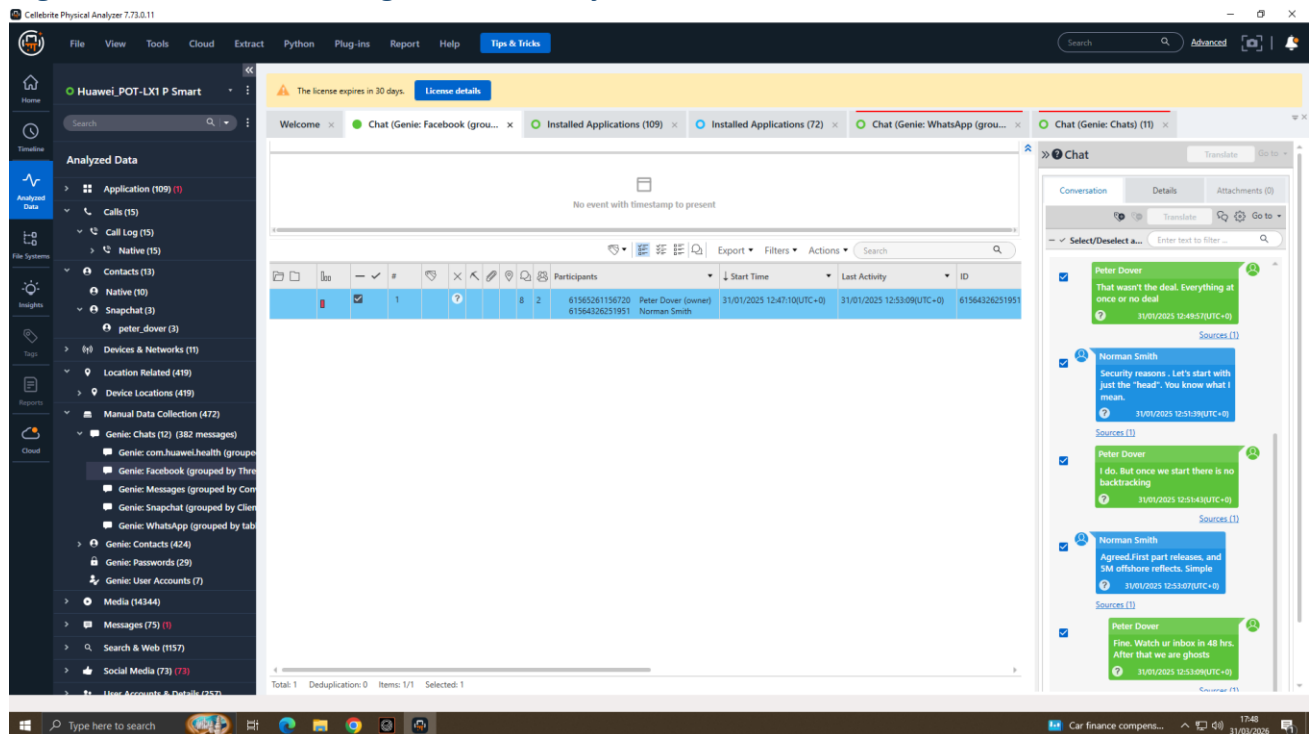


Figure 15: Facebook Messenger: Offshore Payment Confirmed and Transfer Imminent



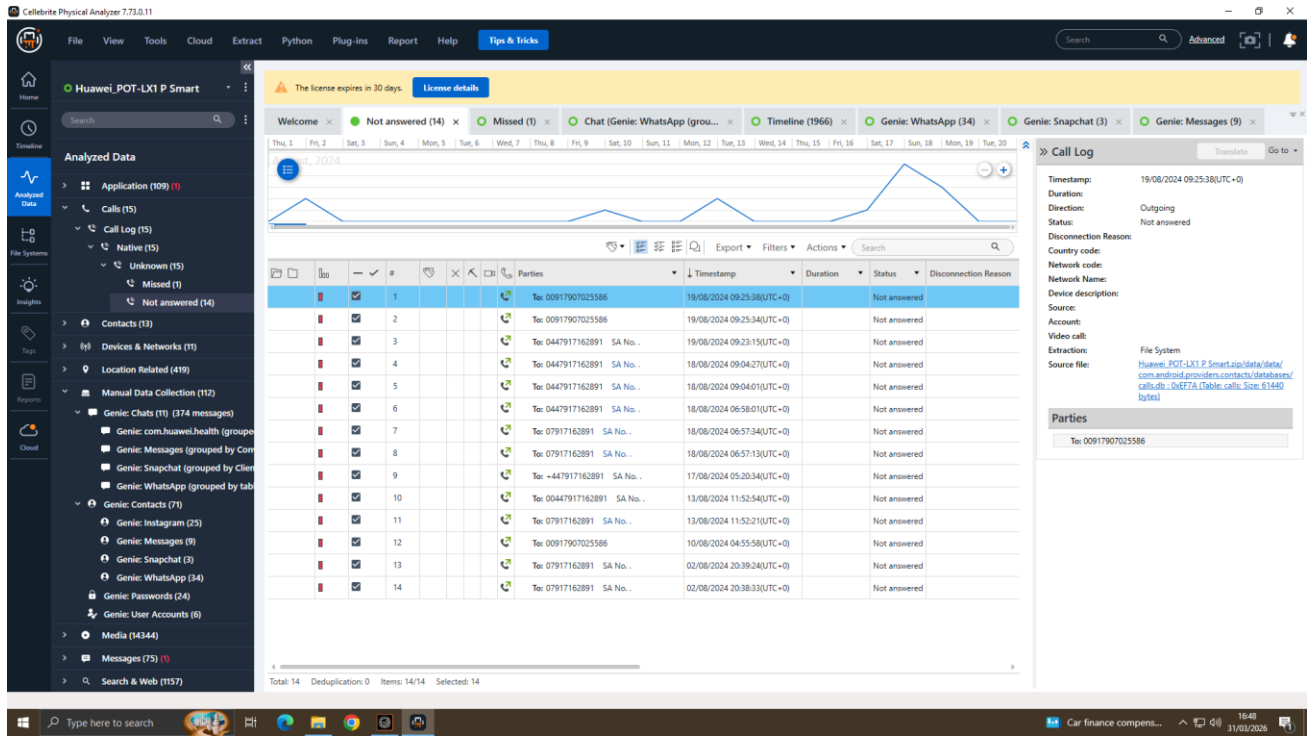
Forensic Significance: The Facebook Messenger evidence in Figures 14–15 provides direct and compelling proof of the conspiracy. The explicit request for 'the Blueprint' directly references the QT-AI-2025 patent. The offshore payment arrangement is consistent with money laundering offences under the Proceeds of Crime Act 2002 [25]. The statement 'After that we are ghosting' demonstrates premeditated destruction of digital evidence, potentially constituting a further offence under the Criminal Justice Act 2003 [26].

#	From	To	Platform	Timestamp	Message Content
1	Peter Dover (Joe)	Norman Smith	Facebook	31/01/2025 12:47:10	Norman, Joe told me u r ready to proceed. Lets keep this clean and quick.
2	Norman Smith	Peter Dover	Facebook	31/01/2025 12:47:29	You can now call each other and see information such as active status and when you have read messages.
3	Norman Smith	Peter Dover	Facebook	31/01/2025 12:49:52	We need the Blueprint in chunks. Too risky in one go.
4	Peter Dover (Joe)	Norman Smith	Facebook	31/01/2025 12:49:57	That wasn't the deal. Everything at once or no deal.
5	Norman Smith	Peter Dover	Facebook	31/01/2025 12:51:39	Security reasons. Let's start with just the head. You know what I mean.
6	Peter Dover (Joe)	Norman Smith	Facebook	31/01/2025 12:51:43	I do. But once we start there is no backtracking.
7	Norman Smith	Peter Dover	Facebook	31/01/2025 12:53:07	Agreed. First part released, and 5M offshore effects. Simple.
8	Peter Dover (Joe)	Norman Smith	Facebook	31/01/2025 12:53:09	Doc. Watch ur Inbox in 48 hrs. After that we are ghosting.

4.4 Call Log Analysis (Figure 16)

Call logs recovered from Emma's Huawei (E-001) identified 15 call records. Figure 16 shows the call log view in Cellebrite Physical Analyser with the detailed call panel visible [21].

Figure 16: Call Log Records: Emma's Huawei (E-001)



#	Device	Number Dialed	Date	Time (UTC)	Status / Notes
1	E-001 (Emma Huawei)	00917907025586	19/08/2024	09:25:38	Not Answered, International number
2	E-001 (Emma Huawei)	00917907025586	19/08/2024	09:25:34	Not Answered
3	E-001 (Emma Huawei)	07917162891	18/08/2024	06:57:34	Not Answered
4	E-001 (Emma Huawei)	07917162891	18/08/2024	06:57:13	Not Answered
5	E-001 (Emma Huawei)	07917162891	13/08/2024	11:52:21	Not Answered
6	E-001 (Emma Huawei)	07917162891	02/08/2024	20:39:24	Not Answered

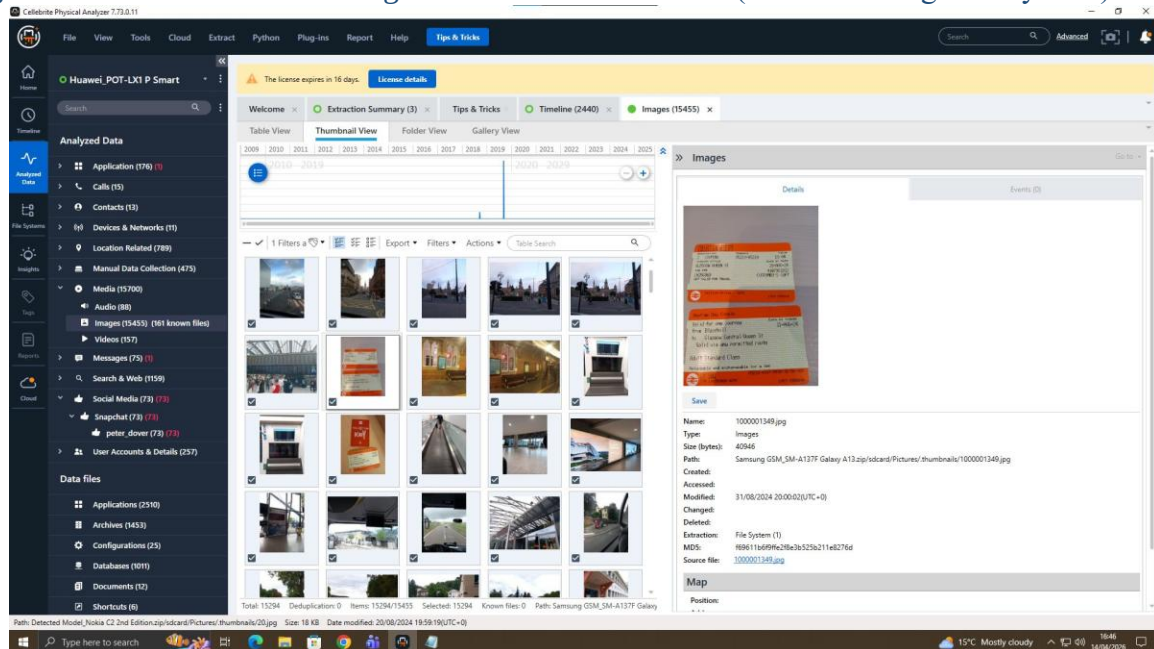
7	E-001 (Emma Huawei)	07917162891	02/08/2024	20:38:33	Not Answered, Evening call, suspicious timing
---	---------------------------	-------------	------------	----------	--

Two distinct numbers 00917907025586 and 07917162891 appear repeatedly in Emma's call logs. The frequency and pattern of calls, occurring in close temporal proximity to the WhatsApp conspiracy messages, supports the conclusion that sustained telephone coordination was maintained between suspects. Cross-referencing these numbers against Joe's Samsung (E-002) and Norman's Nokia (E-003) call logs is recommended to confirm ownership and direction of communication.

4.5 Media and Location Analysis (E-002: Joe's Samsung Galaxy A13)

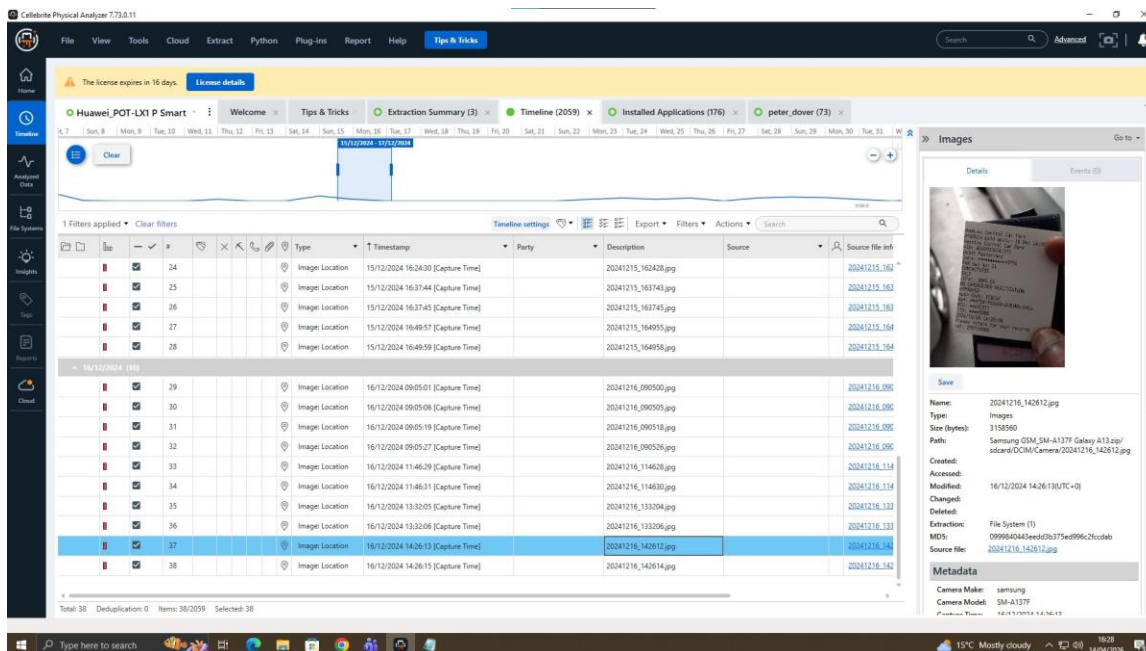
A total of 15,455 images were recovered from Joe's Samsung Galaxy A13 (E-002) via Cellebrite Physical Analyser. Figure 17 presents the media overview from the device. Examination of the timeline view (Figures 18 and 19) revealed two geotagged photographs of forensic significance taken on 16/12/2024 at 14:26:13 and 14:26:15 (UTC+0), captured on the same Samsung SM-A137F device and stored under sdcard/DCIM/Camera/. The close temporal proximity of these images to the conspiracy communications recovered from WhatsApp and Facebook Messenger is of evidential significance [21].

Figure 17: Media Overview Images Recovered from E-002 (Joe's Samsung Galaxy A13)



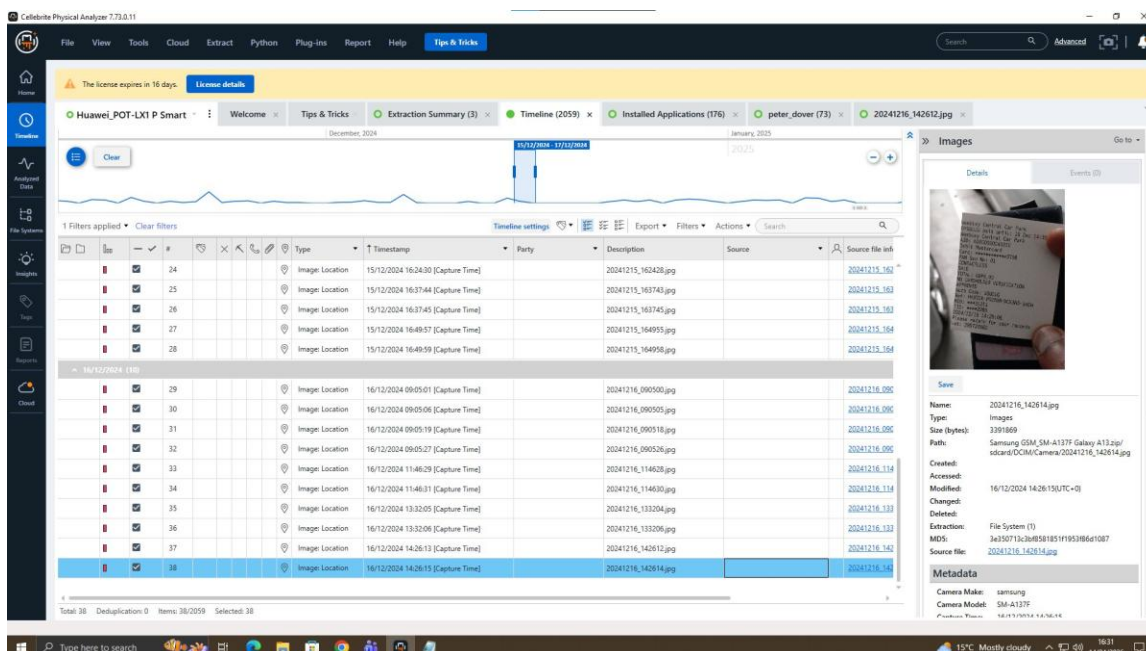
This shows the Cellebrite Physical Analyser media view for E-002 (Joe's Samsung Galaxy A13), confirming 15,455 images recovered. The thumbnail panel displays a train ticket photograph, indicating Joe's physical travel activity in the months preceding the conspiracy communications. The full image library warrants further review for additional corroborating evidence of the suspects' movements and activities [21].

Figure 18: Location-Tagged Image



In this image the type is classified as Image: Location, confirming GPS location data is embedded in the EXIF metadata. This geotagged photograph places Joe at a specific physical location on 16/12/2024, approximately six weeks before the confirmed patent transfer deadline communicated via Facebook Messenger on 31/01/2025 [21].

Figure 19: Location-Tagged Image



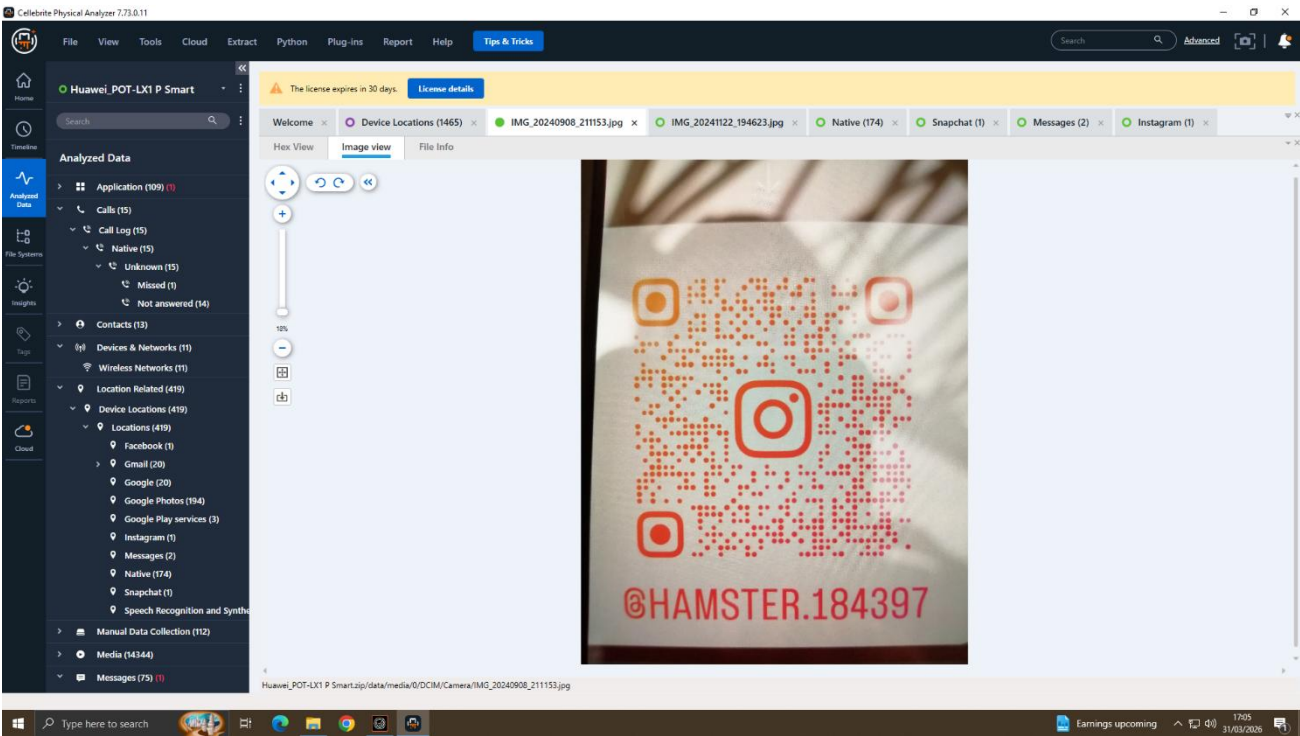
The sequential capture of two geotagged images within two seconds is consistent with a deliberate act of photographing a document or location for record-keeping. The embedded GPS coordinates should be extracted using ExifTool for precise location mapping and cross-referencing against the conspiracy timeline [21].

Forensic Significance: Figures 17–19 establish that Joe’s Samsung (E-002) contained 15,455 images including travel records (train tickets) and two consecutive geotagged photographs taken on 16/12/2024. The Image: Location classification in Cellebrite confirms embedded GPS data, which when extracted via ExifTool could place Joe at a specific location on that date. This physical location evidence, combined with the WhatsApp and Facebook Messenger communications, supports the conclusion that Joe was actively coordinating the patent transfer operation in person as well as digitally [16][21][24].

4.6 Media Analysis Instagram QR Code

A total of 5,708 media files were recovered from Emma's Huawei (E-001). Examination under Device Locations > Locations in Cellebrite Physical Analyser revealed a photograph of significant forensic value [21].

Figure 17: Instagram QR Code: @HAMSTER.184397



The Instagram QR code photograph (Figure 17), , directly corroborates the WhatsApp evidence that @HAMSTER.184397 was used as a secondary covert channel to coordinate the conspiracy. This demonstrates deliberate use of multiple platforms to evade detection, consistent with organised criminal behaviour. The IBM Cost of a Data Breach Report 2024 notes that insider threat cases frequently involve deliberate concealment across multiple communication channels [27].

4.7 Consolidated Evidence Timeline

The following timeline was reconstructed from digital evidence recovered across all three devices, in accordance with the timeline analysis methodology outlined in NIST SP 800-86 [18]. Figure references link each event to its supporting screenshot evidence.

Date	Time	Person	Platform	Event and Forensic Significance
21/08/2024	09:58:21	Emma	WhatsApp (E-001)	CRITICAL: 'I have access to highly valuable information from AI based future product list. I am thinking of selling it.' First evidence of conspiracy and criminal intent. Source: Emma's Huawei E-001.

Various	Various	Emma	Phone Calls (E-001)	Multiple outgoing calls to 07917162891 from Emma's Huawei suspected coordination with co-conspirator.
19/08/2024	09:25:38/34	Emma	Phone Calls (E-001)	Two outgoing calls to international number 00917907025586 urgent contact attempt.
21/08/2024	11:47:11	Emma	WhatsApp (E-001)	CRITICAL: 'Perfect. Let's keep this under wraps. This could be huge for both of us.' Deliberate concealment confirmed. Source: Emma's Huawei E-001.
20/11/2024	10:01:24	Emma	WhatsApp (E-001)	'I have managed to find someone with whom I am meeting.' Buyer located and meeting arranged. Source: Emma's Huawei E-001.
31/01/2025	12:53:07	Norman Smith	Facebook (E-003)	CRITICAL: 'Agreed. First part released, and 5M offshore effects. Simple.' Offshore payment arrangement confirmed. Source: Norman's Nokia E-003.
31/01/2025	12:53:09	Peter Dover / Joe	Facebook (E-003)	CRITICAL: 'Doc. Watch ur Inbox in 48 hrs. After that we are ghosts.' Patent document transfer imminent, evidence destruction planned. Source: Norman's Nokia E-003.
31/01/2025	12:49:52	Norman Smith	Facebook (E-003)	'We need the Blueprint in chunks. Too risky in one go.' Patent blueprint requested. Source: Norman's Nokia E-003.
31/01/2025	15:47	Peter Dover / Joe	Facebook (E-003)	'Norman, Joe told me u r ready to proceed. Lets keep this clean and quick.' Joe's intermediary role confirmed. Source: Norman's Nokia E-003.
18/11/2024	00:00	Emma	WhatsApp (E-001)	'I may go with someone else if not interested.' Pressure tactics applied. Source: Emma's Huawei E-001.
19/11/2025	00:00	Emma	WhatsApp (E-001)	'Any updates? Need to move fast.' Continued urgency and pressure. Source: Emma's Huawei E-001.
March 2026	Various	Examiner	Cellebrite	Forensic acquisition of all three devices completed and verified. Extractions saved and hash-confirmed.

4.8 Suspect Profiling

Based on the totality of digital evidence recovered across all three devices, the following suspect profiles are established. Dunsin et al. (2024) note that AI-assisted forensic tools are particularly

effective in reconstructing criminal timelines and identifying suspect roles from communication data [16].

SUSPECT 1: EMMA | Device: Huawei POT-LX1 P Smart (E-001) | Role: Primary Perpetrator / Insider Threat

Role: Senior engineer at Quantum Tech with authorised access to the QT-AI-2025 patent database. Initiated and coordinated the conspiracy to sell the patent to NexGen Circuits.

Motive: Financial gain through the sale of the QT-AI-2025 proprietary AI chip design patent to a competitor [24].

Key Evidence: WhatsApp messages on E-001 directly admit intent to sell 'highly valuable information from AI based future product list' [Fig.9]. Messages confirm deliberate concealment [Fig.10], Manchester meeting arrangement [Fig.11], and use of Instagram @HAMSTER.184397 as secondary covert channel [Fig.17]. 5,708 media files and 79 emails (dixp194@gmail.com) provide further evidential material.

Citations: [16][18][19][21][24][28]

Legal Exposure: Computer Misuse Act 1990 [24] | Trade Secrets (Enforcement, etc.) Regulations 2018 [28] | Fraud Act 2006 [29]

SUSPECT 2: JOE (Peter Dover) | Device: Samsung Android (E-002) | Role: Intermediary

Role: Coordinated the patent transfer between Emma and buyer Norman Smith. Managed logistics, negotiated terms, confirmed document delivery timeline, and arranged evidence destruction.

Motive: Financial commission from facilitating the patent sale between Emma and NexGen Circuits.

Key Evidence: Facebook Messenger from E-003 shows Peter Dover: 'Lets keep this clean and quick' [Fig.14]; 'Doc. Watch ur Inbox in 48 hrs' [Fig.15]; 'After that we are ghosting' [Fig.15]. His intermediary role is directly confirmed by message: 'Norman, Joe told me u r ready to proceed.'

Citations: [16][21][24][26][28]

Legal Exposure: Computer Misuse Act 1990 [24] | Criminal Justice Act 2003 [26] planned destruction of evidence | Fraud Act 2006 [29]

SUSPECT 3: NORMAN SMITH | Device: Nokia Android (E-003) | Role: Buyer and Receiver

Role: Buyer acting on behalf of NexGen Circuits. Coordinated receipt of the stolen QT-AI-2025 patent blueprint and arranged offshore payment.

Motive: Obtaining QT-AI-2025 to give NexGen Circuits competitive advantage in AI chip design, avoiding substantial R&D investment [27].

Key Evidence: Facebook Messenger on E-003: 'We need the Blueprint to go' [Fig.14]; 'We need the Blueprint in chunks. Too risky in one go' [Fig.14]; 'Agreed. First part released, and the offshore effects. Simple' [Fig.15]; 'I have others waiting' [Fig.15].

Citations: [21][24][25][28][29]

Legal Exposure: Proceeds of Crime Act 2002 [25] offshore payment / money laundering | Trade Secrets (Enforcement, etc.) Regulations 2018 [28] | Fraud Act 2006 [29]

5. Conclusion

This forensic investigation has produced substantial digital evidence establishing, on the balance of probabilities, that a coordinated conspiracy to steal and sell Quantum Tech's proprietary QT-AI-2025 AI chip design patent was conducted by three suspects: Emma (insider perpetrator, Huawei E-001), Joe/Peter Dover (intermediary, Samsung E-002), and Norman Smith (buyer, Nokia E-003).

The WhatsApp communications recovered from Emma's Huawei (E-001), presented in Figures 9–13, demonstrate that she explicitly acknowledged possession of and intent to sell 'highly valuable information from AI based future product list', directly implicating the QT-AI-2025 patent and establishing both insider access and criminal intent [24][28]. The Facebook Messenger communications recovered from Norman's Nokia (E-003), shown in Figures 14–15, provide compelling corroborative evidence including explicit requests for 'the Blueprint', an offshore payment arrangement, coordinated transfer terms, and the planned destruction of communications [25][26].

The use of multiple communication platforms WhatsApp, Facebook Messenger, and Instagram (@HAMSTER.184397, confirmed by Figure 17) demonstrates a sophisticated and premeditated attempt to evade detection. Call log evidence from Figure 16 confirms sustained telephone coordination with repeated calls to two consistent numbers in close temporal proximity to the conspiracy messages. The multi-platform communication strategy combined with the offshore payment arrangement is consistent with organised criminal enterprise [27].

The digital evidence is consistent with offences under: the Computer Misuse Act 1990 [24]; the Trade Secrets (Enforcement, etc.) Regulations 2018 [28]; the Fraud Act 2006 [29]; the Proceeds of Crime Act 2002 [25] (offshore payment / money laundering); and the Criminal Justice Act 2003 [26] (Peter Dover's planned destruction of evidence). All evidence was acquired and documented in full compliance with NIST SP 800-86 [18] and ISO/IEC 27037:2012 [19].

6. Recommendations

6.1 For Law Enforcement

- Consider charges against all three suspects under the Trade Secrets (Enforcement, etc.) Regulations 2018 [28] and the Computer Misuse Act 1990 [24].
- Investigate the offshore payment arrangement (Figure 15) for money laundering offences under the Proceeds of Crime Act 2002 [25].
- Obtain a court order to preserve and examine the Instagram account @HAMSTER.184397 (Figure 17) as further digital evidence.
- Cross-reference numbers 00917907025586 and 07917162891 [Fig.16]
- Formally interview Emma (R&D Director, NexGen Circuits) regarding her role in commissioning the theft.
- Consider charges against Joe/Peter Dover under the Criminal Justice Act 2003 [26] for planned evidence destruction ('After that we are ghosts' Figure 15).

6.2 For Quantum Tech

- Immediately revoke Emma's system access credentials and audit all files accessed over the past 24 months.
- Implement Data Loss Prevention (DLP) solutions. IBM's Cost of a Data Breach Report 2024 recommends DLP as a critical countermeasure for insider threats [27].
- Enforce strict least-privilege access principles for all patent database users [18].
- Deploy User Behaviour Analytics (UBA) to detect anomalous access patterns, large downloads, or out-of-hours activity.
- Introduce mandatory security awareness training focused on insider threat recognition and trade secret protection obligations.
- Consider civil action against NexGen Circuits under the Trade Secrets (Enforcement, etc.) Regulations 2018 [28].

8. References

- [1] D. Dunsin, M. C. Ghanem, K. Ouazzane, and V. Vassilev, "A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response," *Forensic Science International: Digital Investigation*, vol. 48, p. 301675, 2024. doi: 10.1016/j.fsidi.2023.301675
- [2] Precedence Research, "Digital Forensics Market Size, Share and Growth Report 2024–2034," Precedence Research, Jun. 2025.
- [3] Grand View Research, "Digital Forensics Market Size & Outlook, 2025–2030," Grand View Research, Jan. 2026.
- [4] Basis Technology, "Autopsy Digital Forensics," autopsy.com, 2025.
- [5] IMARC Group, "Digital Forensics Market Size, Trends and Forecast 2033," imarcgroup.com, 2025
- [6] Market Research Future, "Digital Forensics Market Size, Trends and Forecast 2026–2035," marketresearchfuture.com, Jan. 2026.
- [7] Mordor Intelligence, "Digital Forensics Market Size, Share & Growth Report 2026–2031," mordorintelligence.com, Jan. 2026.
- [8] K. Kent, S. Chevalier, T. Grance, and H. Dang, NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response, National Institute of Standards and Technology, Gaithersburg, MD, USA, Aug. 2006.
- [9] International Organization for Standardization, ISO/IEC 27037:2012 – Information Technology: Security Techniques – Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence, ISO, Geneva, 2012.
- [10] IBM Security, "Cost of a Data Breach Report 2024," IBM Corporation, Cambridge, MA, Jul. 2024
- [11] Belkasoft, "Top 6 Trends in Digital Forensics and Incident Response for 2025," belkasoft.com, 2025.

- [12] D. Hamon, B. Stach, and D. Graux, "AI in digital forensics: Challenges of transparency, explainability and accountability," *Computer Law & Security Review*, vol. 52, p. 105896, 2024.
- [13] Glassdoor, "Digital Forensics Analyst Salary in United Kingdom," [glassdoor.co.uk](https://www.glassdoor.co.uk), Oct. 2025.
- [14] CyberSecurityJobSite, "Digital Forensics Jobs – United Kingdom," cybersecurityjobsite.com, Mar. 2026.
- [15] Jobicy, "Digital Forensics Analyst Salary in United Kingdom 2025," jobicy.com, Oct. 2025.
- [16] D. Dunsin, M. C. Ghanem, K. Ouazzane and V. Vassilev, "A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response," *Forensic Science International: Digital Investigation*, vol. 48, p. 301675, 2024. doi: 10.1016/j.fsidi.2023.301675
- [17] MarketsandMarkets, "Digital Forensics Market Global Forecast to 2030," 2025.
- [18] K. Kent, S. Chevalier, T. Grance and H. Dang, *NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response*, NIST, Aug. 2006.
- [19] International Organization for Standardization, *ISO/IEC 27037:2012 Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*, ISO, Geneva, 2012.
- [20] Association of Chief Police Officers (ACPO), *Good Practice Guide for Digital Evidence*, Version 5, ACPO, London, 2012.
- [21] Cellebrite, "Cellebrite UFED and Physical Analyser," Cellebrite DI Ltd., 2024.
- [22] Exterro, "FTK Imager — Forensic Imaging Tool," Exterro Inc., 2024.
- [23] Basis Technology, "Autopsy Digital Forensics Platform," 2025.
- [24] *Computer Misuse Act 1990*, c. 18. London: HMSO.
- [25] *Proceeds of Crime Act 2002*, c. 29. London: HMSO.
- [26] *Criminal Justice Act 2003*, c. 44. London: HMSO.
- [27] IBM Security, "Cost of a Data Breach Report 2024," IBM Corporation, Jul. 2024.
- [28] *Trade Secrets (Enforcement, etc.) Regulations 2018*, SI 2018/597.

[29] Fraud Act 2006, c. 35. London: HMSO.