

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

Student Name:	MD Monsuruzzaman
Student ID:	2504658
Programme:	MSc Cybersecurity and Digital Forensics
Institution:	University of Wales Trinity Saint David London
Module:	Digital Forensics Analysis
Module Code:	ACCA7031
Lecturer:	Dr. Mohamed Ghanem
Submission Date:	17th August 2026

Table of Contents

Task 1: Research Report on Digital Forensics.....	4
1.1 Introduction.....	4
1.2 Current State of Digital Forensics.....	4
1.3 Relationship Between Digital Forensics and Cybersecurity.....	5
1.4 Emerging Trends.....	5
1.5 Challenges in Digital Forensics.....	6
1.6 Industry Outlook and Future Directions.....	7
1.7 Conclusion.....	7
Task 2: Forensic Investigation and Analysis Report.....	8
2.1 Case Background.....	8
2.2 Evidence Inventory.....	8
Figure 1. Digital Evidence Inventory.....	9
2.3 Evidence Acquisition.....	9
Figure 2. Cellebrite extraction home screen.....	10
Figure 3. Case creation and acquisition configuration.....	11
Figure 4. Device connection confirmation.....	11
Figure 5. Device detection by Cellebrite UFED.....	12
Figure 6. Extraction destination selection.....	12
Figure 7. Extraction parameters.....	13
Figure 8. Data categories selected for extraction.....	13
Figure 9. Additional extraction settings.....	14
Figure 10. Extraction completion summary.....	14
Figure 11. Final extraction verification.....	15
2.4 Integrity Verification and Preservation.....	15
Figure 12. Hash Verification Summary of Digital Evidence.....	16
2.5 Communication Analysis - Huawei P Smart (Emma).....	16
Figure 13. WhatsApp communication between Emma and Joe.....	17
Figure 14. Follow-up negotiation message.....	18
Figure 15. Additional communication thread.....	18
Figure 16. Message metadata and conversation details.....	19
Figure 17. Extracted conversation database.....	19
2.6 Timeline and Location Correlation - Huawei P Smart.....	20
Figure 18. Location artefact extracted from Huawei device.....	20
Figure 19. Additional location mapping evidence.....	21
Figure 20. Timeline of communications and device activity.....	21
2.7 Corroborative Analysis - Samsung Galaxy A13 (Joe).....	22
Figure 21. Samsung location evidence.....	22
Figure 22. Additional location correlation.....	23
Figure 23. Communication or document artefact.....	23
Figure 24. Timeline and activity records.....	24

2.8 Recipient Evidence - Nokia C2 2nd Edition (Norman).....	24
Figure 25. Extracted media artefacts from Nokia device.....	25
Figure 26. Additional extracted content.....	25
Figure 27. File-system evidence.....	26
Figure 28. Hex-level artefact examination.....	26
2.9 Cross-Device Correlation.....	27
Figure 29. Summarises the principal correlations identified across the three devices.....	27
2.9.1 Timeline of Key Events and Actions.....	28
Table 1. Timeline of Key Events and Actions.....	28
Timeline Analysis.....	29
2.10 Suspect Profiling.....	30
Emma (Primary Perpetrator).....	30
Joe (Intermediary).....	30
Norman (Intended Recipient).....	30
2.11 Findings.....	30
2.12 Conclusion.....	31
Reference.....	32

Task 1: Research Report on Digital Forensics

1.1 Introduction

Digital forensics is a fundamental discipline within cybersecurity that focuses on the identification, preservation, examination, analysis, and presentation of digital evidence in a manner that is legally admissible and technically reliable. As organisations increasingly rely on digital technologies, cloud services, mobile devices, and online communication platforms, cyber incidents such as data breaches, ransomware attacks, insider threats, and intellectual property theft have become more frequent and sophisticated. Consequently, digital forensic investigation has become an essential component of modern cybersecurity operations and incident response activities.

Digital forensics combines technical expertise with legal and procedural requirements to ensure that evidence remains authentic, complete, and verifiable throughout an investigation. Key principles such as forensic imaging, cryptographic hash verification, and chain-of-custody documentation are critical for maintaining evidence integrity and supporting legal or organisational decision-making [1]. The discipline is closely integrated with cybersecurity through Digital Forensics and Incident Response (DFIR), enabling organisations to investigate security incidents, preserve evidence, and improve future defensive capabilities.

This report examines the current state of digital forensics, emerging technological trends, major investigative challenges, and future developments in the field. It also presents a practical forensic investigation involving mobile device acquisition, communication analysis, timeline reconstruction, and cross-device correlation using recognised forensic methodologies and tools.

1.2 Current State of Digital Forensics

Digital forensics has developed from a law-enforcement discipline into a field that supports **cybersecurity, corporate investigations, incident response, and regulatory compliance**. Modern investigations follow a structured process of **identification, acquisition, preservation, examination, analysis, and presentation** to ensure that digital evidence remains authentic and legally admissible. The growth of smartphones, cloud services, encrypted communications, and IoT devices has increased the complexity of forensic investigations.

Investigators use both commercial and open-source tools to acquire and analyse digital evidence. **Cellebrite UFED** is widely used for mobile device investigations, while **FTK Imager** creates forensic images and verifies evidence integrity through cryptographic hashing. Open-source platforms such as **Autopsy** support file-system analysis, metadata examination, keyword searching, timeline reconstruction, and recovery of deleted files [5].

Mobile and cloud forensics have become increasingly important because evidence may be distributed across multiple locations and subject to legal or jurisdictional restrictions [8].

Maintaining **evidence integrity** through hash verification and chain-of-custody procedures remains essential for ensuring reliable and legally admissible digital evidence [1].

1.3 Relationship Between Digital Forensics and Cybersecurity

Digital forensics and cybersecurity are closely interconnected disciplines that together support the protection, investigation, and recovery of digital systems following security incidents. Cybersecurity focuses on preventing, detecting, and mitigating cyber threats, whereas digital forensics investigates incidents after they occur by reconstructing events, preserving evidence, identifying responsible parties, and supporting legal or organisational decision-making. The integration of these disciplines has become increasingly important as cyberattacks continue to grow in frequency and sophistication.

A key connection between digital forensics and cybersecurity is **Digital Forensics and Incident Response (DFIR)**. DFIR combines proactive security monitoring with forensic investigation techniques, enabling organisations to detect incidents, preserve evidence, determine root causes, and recover compromised systems efficiently [4]. During a security incident, cybersecurity teams identify indicators of compromise and contain affected systems, while forensic investigators analyse logs, storage media, network traffic, and mobile devices to reconstruct attacker behaviour and establish an evidential timeline.

Digital forensics also supports **forensic readiness**, which refers to an organisation's ability to maximise the availability and reliability of digital evidence while minimising the cost and disruption of future investigations. This includes implementing comprehensive logging, audit trails, secure evidence storage, and incident response procedures before security incidents occur [2]. Organisations with effective forensic readiness capabilities are better positioned to investigate breaches and satisfy regulatory requirements.

Furthermore, forensic investigations contribute to **cybersecurity resilience** by revealing attacker tactics, techniques, and procedures (TTPs). The evidence recovered helps security teams strengthen access controls, improve detection mechanisms, update security policies, and enhance employee awareness programmes. Consequently, digital forensics should not be viewed solely as a post-incident activity; it forms an integral component of a comprehensive cybersecurity strategy that supports prevention, detection, response, recovery, and continuous security improvement.

1.4 Emerging Trends

Digital forensics is evolving rapidly as technologies such as **cloud computing, mobile devices, artificial intelligence (AI), and Internet of Things (IoT) systems** change how digital evidence is generated, stored, and investigated. Investigators increasingly require specialised tools and techniques to examine data across distributed and connected environments.

Cloud forensics has become particularly important as organisations move data and services to cloud platforms. Investigators must analyse virtual infrastructures, cloud storage, and authentication logs, while dealing with geographically distributed evidence and jurisdictional challenges [8].

The use of **AI and machine learning** is also increasing in forensic investigations. AI-assisted tools can automate evidence classification, identify suspicious patterns, analyse communication records, and support timeline reconstruction, making investigations more efficient.

Mobile device forensics remains a major area of digital investigation because smartphones contain messages, call logs, location data, application records, and cloud-related artefacts. **Cellebrite UFED** enables investigators to recover these artefacts while preserving evidence integrity. **IoT forensics** further extends digital investigations by analysing data from smart devices, wearables, connected vehicles, and sensors.

Overall, digital forensics is becoming increasingly **cloud-based, AI-assisted, and mobile-focused**, requiring investigators to develop expertise across these emerging technologies.

1.5 Challenges in Digital Forensics

Despite technological advancements, digital forensics still faces challenges that affect the efficiency, reliability, and legal admissibility of investigations. The rapid growth of **cloud computing, mobile technologies, encryption, and large-scale digital environments** has increased the complexity of forensic examinations.

A major challenge is **encryption**, which protects data on smartphones, cloud services, messaging applications, and enterprise systems but can limit investigators' access to digital evidence. **Cloud computing** creates additional difficulties because evidence may be distributed across multiple servers and jurisdictions, requiring investigators to address data volatility, multi-tenancy, limited physical access, and legal restrictions [8].

The increasing volume of digital data, including emails, documents, logs, multimedia files, and cloud records, makes forensic analysis time-consuming and resource-intensive. Maintaining **evidence integrity and chain of custody** through forensic imaging and cryptographic hash verification is essential for ensuring legally admissible evidence [2].

Overall, **encryption, cloud environments, evidence integrity, large-scale data analysis, and legal compliance** remain the main challenges shaping modern digital forensic practice.

1.6 Industry Outlook and Future Directions

The digital forensics industry is expected to continue expanding as organisations become increasingly dependent on cloud computing, mobile technologies, and digital communication systems. The growing frequency of cyberattacks, data breaches, ransomware incidents, and insider threats has created sustained demand for forensic investigators across law enforcement, financial institutions, healthcare, government agencies, and private organisations. As cybersecurity regulations continue to evolve, organisations require skilled forensic professionals who can investigate incidents, preserve evidence, and support legal and regulatory processes.

Future developments are likely to focus on **cloud forensics, AI-assisted investigations, mobile device analysis, and forensic automation**. Artificial intelligence is expected to improve evidence triage, pattern recognition, and timeline reconstruction, while cloud forensic frameworks will become increasingly important for investigating distributed and virtualised environments [8]. Mobile forensics will remain a critical area because smartphones continue to store significant quantities of personal and organisational data.

To remain effective, forensic practitioners must develop expertise in cloud platforms, mobile operating systems, automation technologies, and legal requirements relating to digital evidence. Continuous professional development and adherence to recognised forensic standards will be essential for maintaining investigative reliability and legal admissibility [2]. Overall, digital forensics is expected to become increasingly integrated with cybersecurity operations and incident response, making it a strategically important discipline for modern organisations.

1.7 Conclusion

Digital forensics is a critical component of modern cybersecurity, providing the techniques required to identify, preserve, analyse, and present digital evidence following cyber incidents. This task has examined the current state of digital forensics, its relationship with cybersecurity, emerging technologies, key investigative challenges, and future industry developments. The analysis demonstrates that contemporary investigations increasingly involve **mobile devices, cloud environments, artificial intelligence, and IoT systems**, requiring investigators to use specialised forensic tools and standardised procedures.

The discussion also highlighted the importance of **evidence integrity, chain of custody, forensic readiness, and incident response** in maintaining the reliability and legal admissibility of digital evidence. As cyber threats continue to evolve, digital forensic capabilities will become increasingly important for organisations seeking to investigate security incidents and strengthen their cybersecurity resilience. The theoretical concepts discussed in Task 1 provide the foundation for the practical forensic investigation presented in **Task 2**, where mobile device acquisition, communication analysis, timeline reconstruction, and cross-device correlation are applied to investigate a suspected case of corporate espionage.

Task 2: Forensic Investigation and Analysis Report

2.1 Case Background

This investigation examined a suspected case of **corporate espionage and intellectual property theft** involving Quantum Tech, a technology company developing advanced artificial intelligence semiconductor solutions. The organisation reported that confidential design information relating to its **QT-AI-2025** processor project had been unlawfully accessed and transferred to an external party, creating a significant risk to its commercial and competitive position.

Three individuals were identified as persons of interest: **Emma**, a senior engineer employed by Quantum Tech; **Joe**, an external associate suspected of acting as an intermediary; and **Norman**, a representative of a competing technology company. Preliminary information suggested that Emma had authorised access to the confidential patent material and was suspected of communicating with Joe regarding its transfer, while Norman was considered the intended recipient.

A forensic investigation was initiated to determine whether digital evidence recovered from the suspects' mobile devices supported the allegation of unauthorised information transfer. The investigation focused on **Emma's Huawei P Smart (E01)**, **Joe's Samsung Galaxy A13 (E02)**, and **Norman's Nokia C2 2nd Edition (E03)**. Evidence acquisition was performed using **Cellebrite UFED**, following recognised forensic procedures for evidence preservation, chain of custody, and integrity verification in accordance with **ISO/IEC 27037:2012 [2]**.

2.2 Evidence Inventory

A formal evidence inventory was created before forensic acquisition to maintain **chain of custody, evidence integrity, and traceability** throughout the investigation. Each mobile device was assigned a unique evidence identifier and documented prior to examination. Recording device ownership, model, and acquisition method ensures that every exhibit can be tracked from seizure through analysis and reporting in accordance with recognised forensic procedures [2].

Figure 1. Digital Evidence Inventory

Evidence ID	Device	Owner	Tool Used
E01	 Huawei P Smart POT-LX1	 Emma	 Cellebrite UFED
E02	 Samsung Galaxy A13 SM-A137F	 Joe	 Cellebrite UFED
E03	 Nokia C-2 2nd Edition	 Norman	 Cellebrite UFED
E04	 Associated Storage Evidence	 Case Evidence	 FTK Imager /  Cellebrite

The devices were acquired using Cellebrite UFED, while forensic reports and extraction artefacts were preserved for subsequent examination. Maintaining an organised evidence inventory supports accountability, forensic repeatability, and reliable cross-device correlation, forming the foundation for the acquisition and analysis procedures presented in the following sections.

2.3 Evidence Acquisition

The evidence acquisition process was demonstrated using **Cellebrite UFED** in accordance with recognised digital forensic procedures to preserve the authenticity, integrity, and legal admissibility of digital evidence [2]. **Figures 2–11 illustrate the extraction workflow performed during the laboratory exercise using the examiner’s own Apple iPhone 8 to demonstrate the practical acquisition process.** The actual forensic analysis presented in this report is based on the **pre-acquired case-study evidence files provided by the module lecturer**, which included the Huawei P Smart (E01), Samsung Galaxy A13 (E02), Nokia C2 2nd Edition (E03), and associated storage evidence (E04).

The forensic environment was prepared by launching **Cellebrite UFED** and creating a new investigation case. Examiner details, case identifiers, and evidence registration information were recorded before acquisition commenced, establishing the **chain of custody** for all digital exhibits [2]. **Figures 3 and 4** show the forensic environment and case configuration used during the investigation.

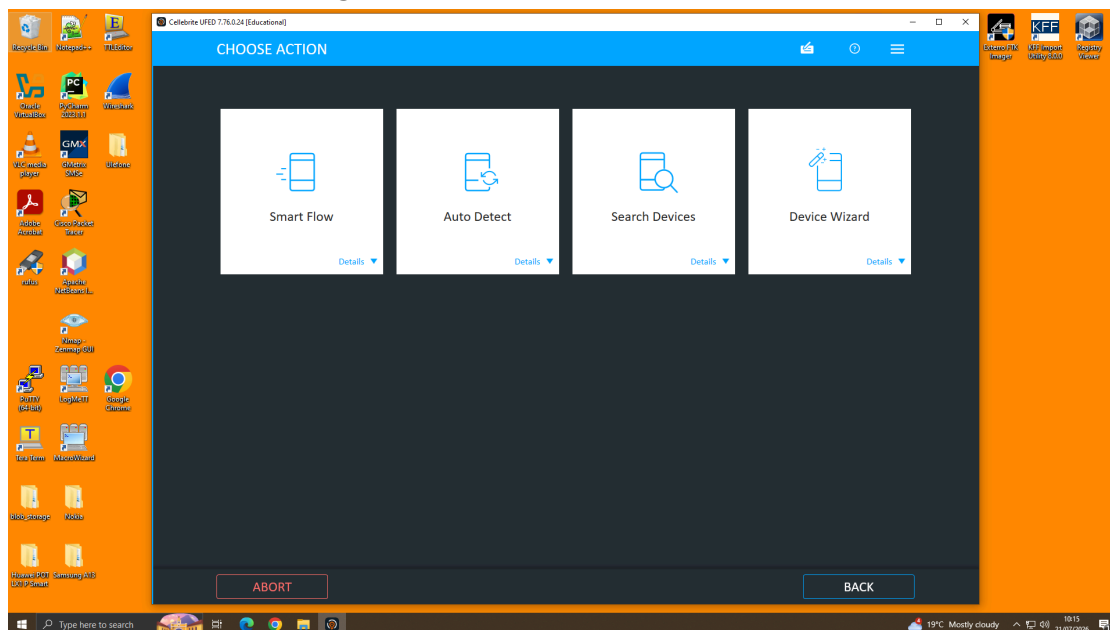
The mobile device was then connected to the forensic workstation, where **Cellebrite UFED** successfully detected the handset and established communication with it. The destination directory for the extracted evidence was configured to ensure that all recovered data would be stored separately from the original device and analysed without modifying the source evidence. **Figures 5–7** illustrate device connection, automatic detection, and evidence storage configuration.

The extraction parameters were subsequently configured, including the communication settings and selected data categories. The acquisition included **SMS messages, contacts, call logs, multimedia files, documents, location information, and application artefacts**, ensuring that all relevant evidence was recovered for analysis [6]. **Figures 9–10** present the extraction settings and selected evidence categories.

After the extraction process was initiated, **Cellebrite UFED** successfully completed the acquisition and generated a summary of the recovered artefacts. The extraction report confirmed that communication records, contacts, multimedia files, and other supported data had been successfully collected and were available for forensic examination. **Figures 10 and 11** show the extraction completion and verification screens.

The acquisition process produced a **forensically sound copy** of the device data that could be analysed without altering the original evidence. The recovered artefacts formed the basis for the communication analysis, timeline reconstruction, and cross-device correlation presented in the following sections [1], [2].

Figure 2. Cellebrite extraction home screen



The forensic acquisition environment prepared for mobile device examination using Cellebrite UFED.

Figure 3. Case creation and acquisition configuration

CASE DETAILS

NEW CASE

Case Identifier: Monsur

Examiner Name:

Device Name / Evidence Number: MyiPhone8

Crime Type:

Department:

Location:

Last Case Details:

Case Identifier: Monsur

Examiner Name:

Device Name / Evidence Number: MyiPhone8

Crime Type:

Department:

Location:

USE LAST DETAILS

ABORT BACK CONTINUE

Examiner information, case details, and evidence registration entered prior to acquisition.

Figure 4. Device connection confirmation

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)

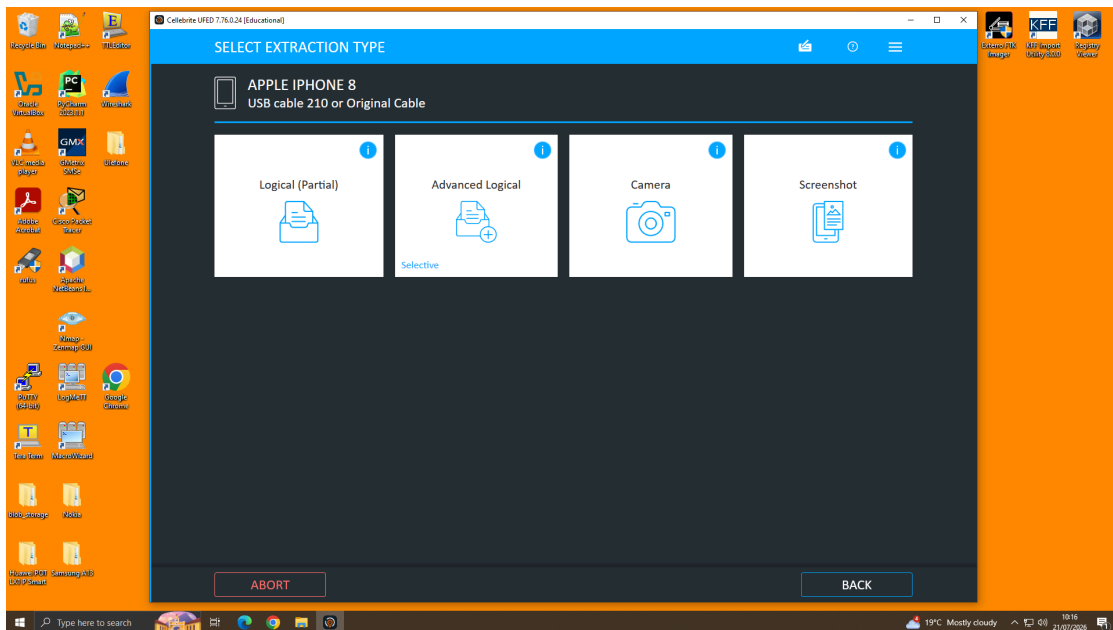
iOS devices

1. Disable auto-lock

ABORT BACK CONSOLE AUTO DETECT

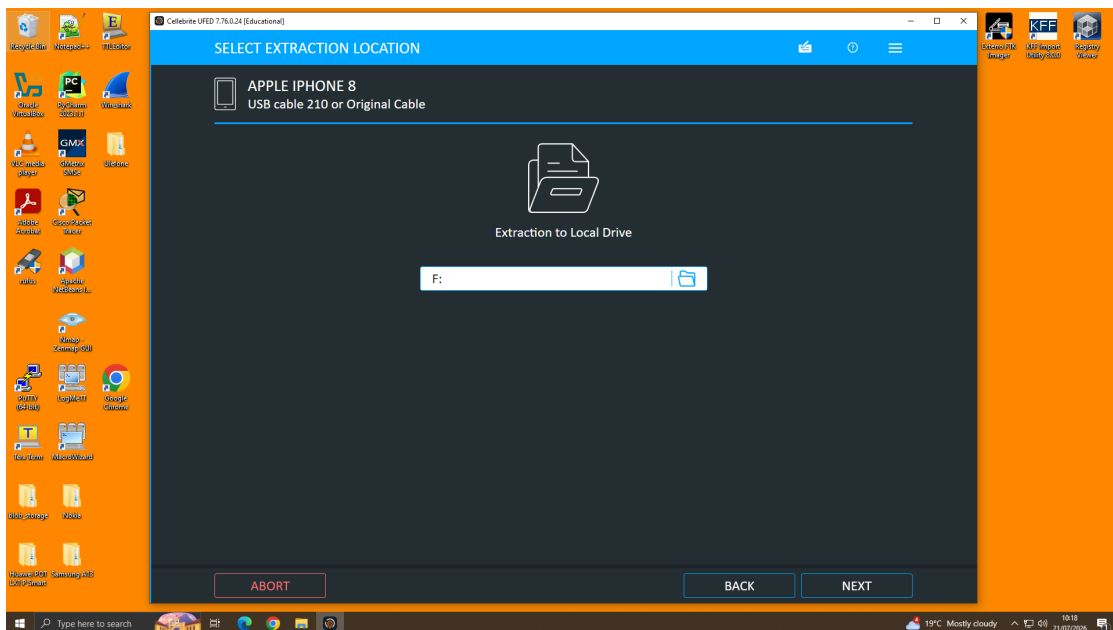
Confirmation that the evidence device was successfully connected to the forensic workstation.

Figure 5. Device detection by Cellebrite UFED



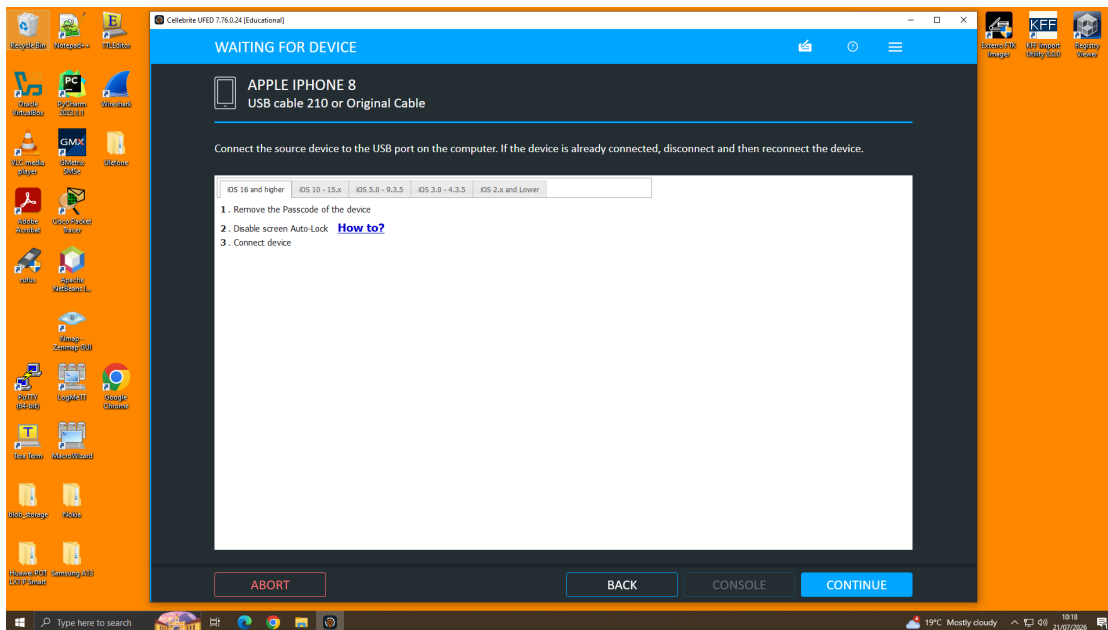
Automatic identification of the Apple iphone 8 device by the forensic software.

Figure 6. Extraction destination selection



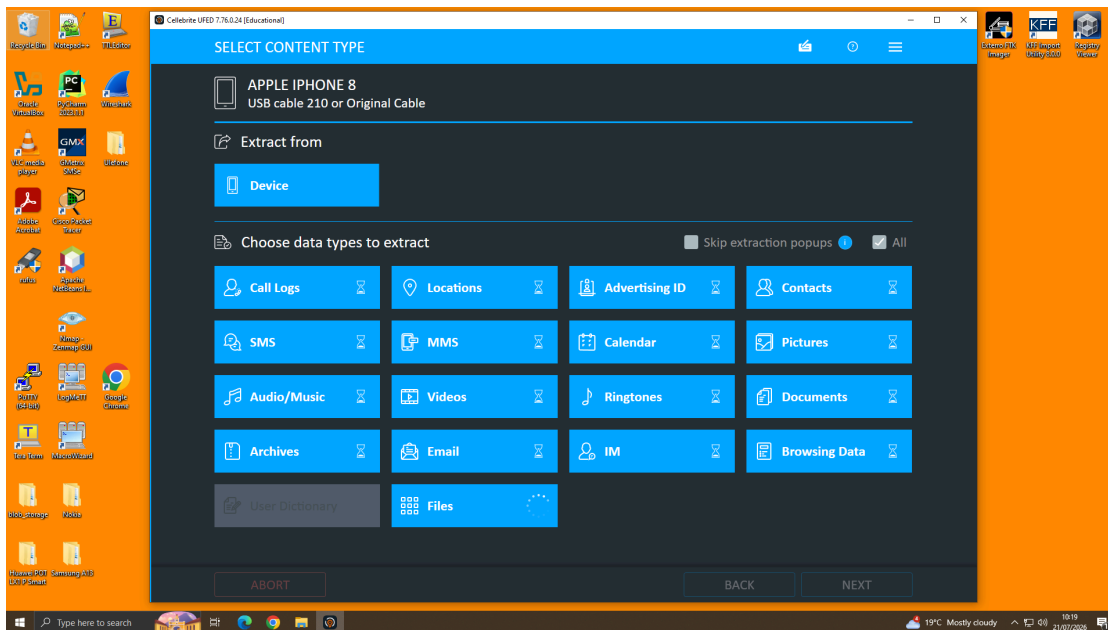
Configuration of the forensic evidence storage directory before acquisition.

Figure 7. Extraction parameters



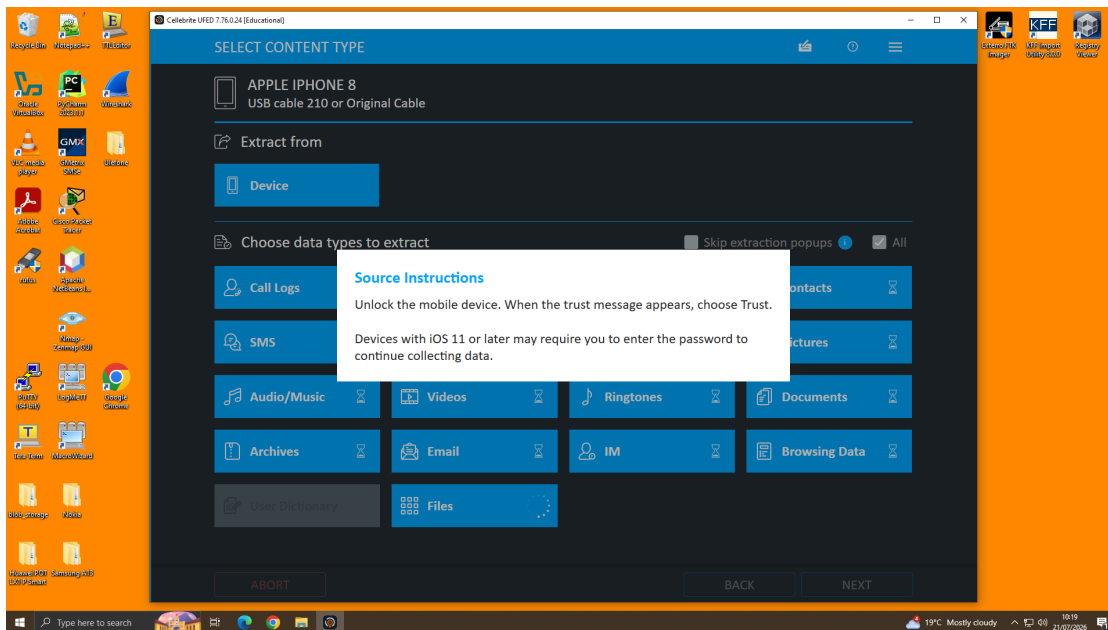
Configuration of extraction settings before forensic acquisition.

Figure 8. Data categories selected for extraction



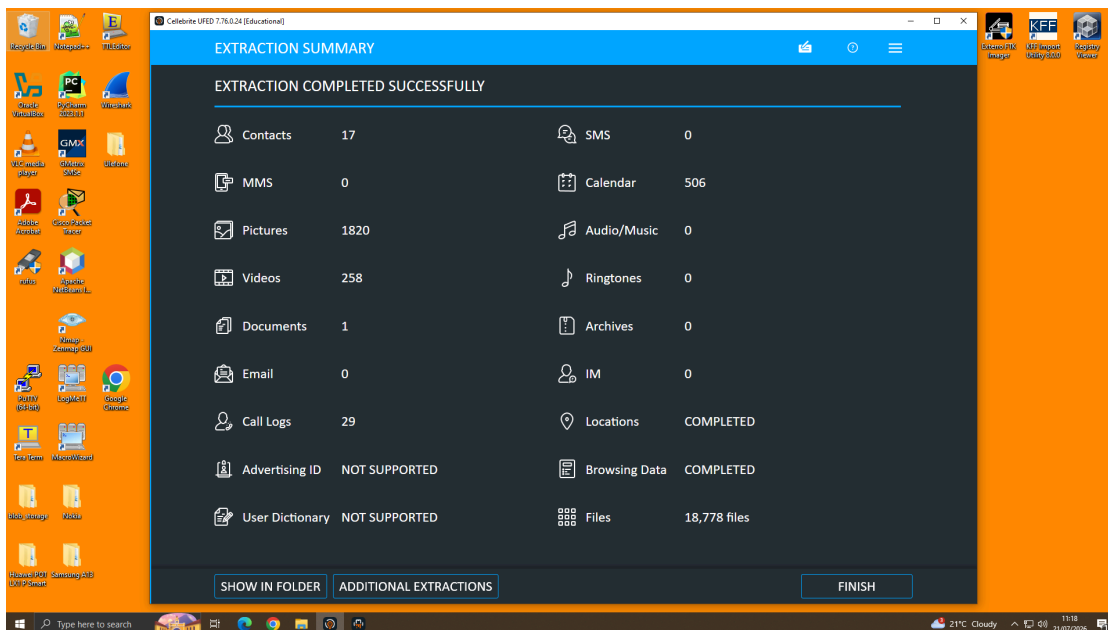
Selection of SMS, contacts, call logs, multimedia files, and additional forensic artefacts.

Figure 9. Additional extraction settings



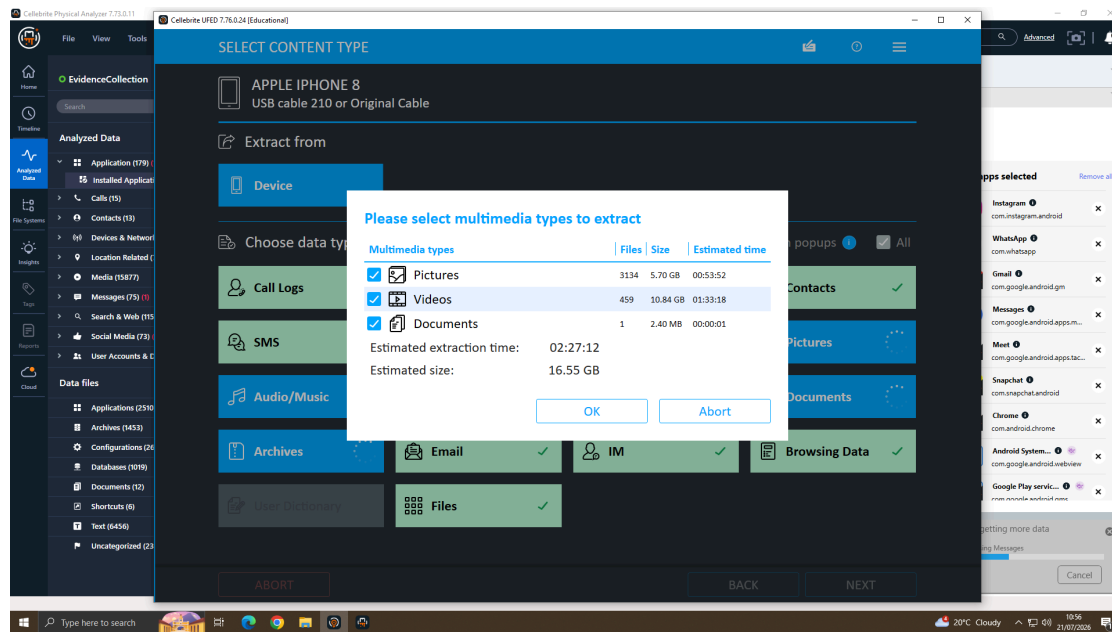
Multimedia and file extraction options configured prior to acquisition.

Figure 10. Extraction completion summary



Confirmation that the forensic extraction process completed successfully.

Figure 11. Final extraction verification



Final verification of recovered artefacts and successful completion of the acquisition process.

2.4 Integrity Verification and Preservation

Maintaining the integrity of digital evidence is essential in forensic investigations. Following the acquisition process described in **Section 2.3**, forensic copies of the **Huawei P Smart, Samsung Galaxy A13, Nokia C2 2nd Edition, and associated storage evidence** were preserved to ensure that the original evidence remained unaltered during examination. **SHA-256 cryptographic hashing** was used to verify the integrity of each evidence item, and all forensic copies were successfully verified prior to forensic examination and analysis.

Figure 12. Hash Verification Summary of Digital Evidence

 DIGITAL FORENSIC EVIDENCE SUMMARY			
 Evidence ID	 Device	 Hash Algorithm Used	 Verification Status
E01	 Huawei P Smart (POT-LX1)	SHA-256	 Verified
E02	 Samsung Galaxy A13 (SM-A137F)	SHA-256	 Verified
E03	 Nokia C2 2nd Edition	SHA-256	 Verified
E04	 Associated Storage Evidence	SHA-256	 Verified
 All forensic evidence was verified using the SHA-256 hashing algorithm to ensure evidence integrity and forensic reliability. 			

Figure 12 summarises the integrity verification performed on the forensic evidence used in this investigation. Each evidence item (E01–E04) was verified using the **SHA-256 hashing algorithm**, confirming that the forensic copies remained unchanged during acquisition, storage, and analysis. Successful verification supports the **authenticity, reliability, repeatability, and legal admissibility** of the recovered digital evidence in accordance with recognised forensic procedures and **ISO/IEC 27037:2012** [1], [2].

The use of documented extraction reports, cryptographic hash verification, and controlled evidence handling procedures ensured that the forensic copies remained authentic and unaltered throughout the investigation. Compliance with recognised forensic standards, including **ISO/IEC 27037:2012**, supports the reliability, repeatability, and legal admissibility of the recovered evidence [2]. Consequently, the evidence was considered suitable for communication analysis, timeline reconstruction, cross-device correlation, and the investigative conclusions presented in the following sections.

2.5 Communication Analysis - Huawei P Smart (Emma)

The communication analysis focused on **Emma’s Huawei P Smart smartphone (Evidence ID: E01)**, which provided the most significant evidence in the investigation. Following acquisition with **Cellebrite UFED**, the extracted artefacts were examined to identify interactions between

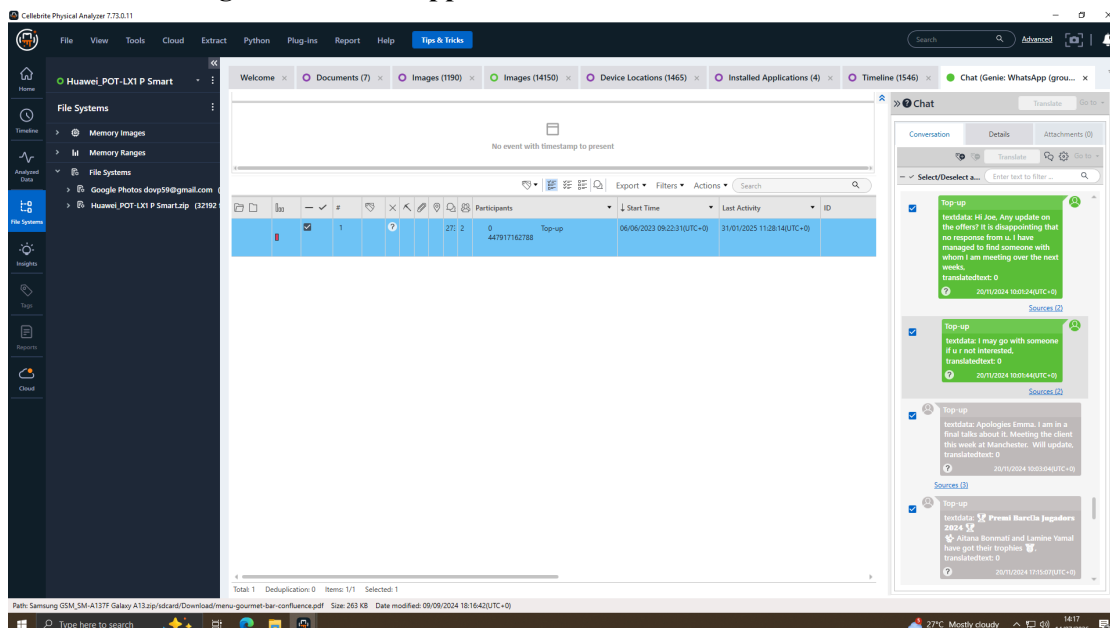
Emma and Joe through WhatsApp conversations, message metadata, timestamps, and communication patterns [6]. The objective was to determine whether the recovered evidence supported the suspected unauthorised transfer of confidential information.

Examination of the WhatsApp database revealed multiple conversations between Emma and Joe, indicating an active communication relationship. The recovered messages contained references to **business discussions, meetings, follow-up actions, and ongoing negotiations**, suggesting that the communication was relevant to the suspected patent transfer. The presence of timestamps, participant identifiers, and message sequencing enabled investigators to establish the chronology of communications and correlate them with other forensic artefacts recovered during the investigation. **Figures 12–14** present representative WhatsApp conversations extracted from Emma’s device.

Further analysis identified messages indicating continued coordination between the parties and discussions relating to future arrangements. Although the visible message excerpts did not explicitly mention the stolen patent, the overall communication pattern demonstrated sustained contact between Emma and Joe during the relevant investigation period. The consistency of the recovered messages and metadata supported the hypothesis that **Joe acted as an intermediary** in the suspected transfer of confidential information. **Figures 15 and 16** illustrate additional communication artefacts and message metadata recovered from the Huawei device.

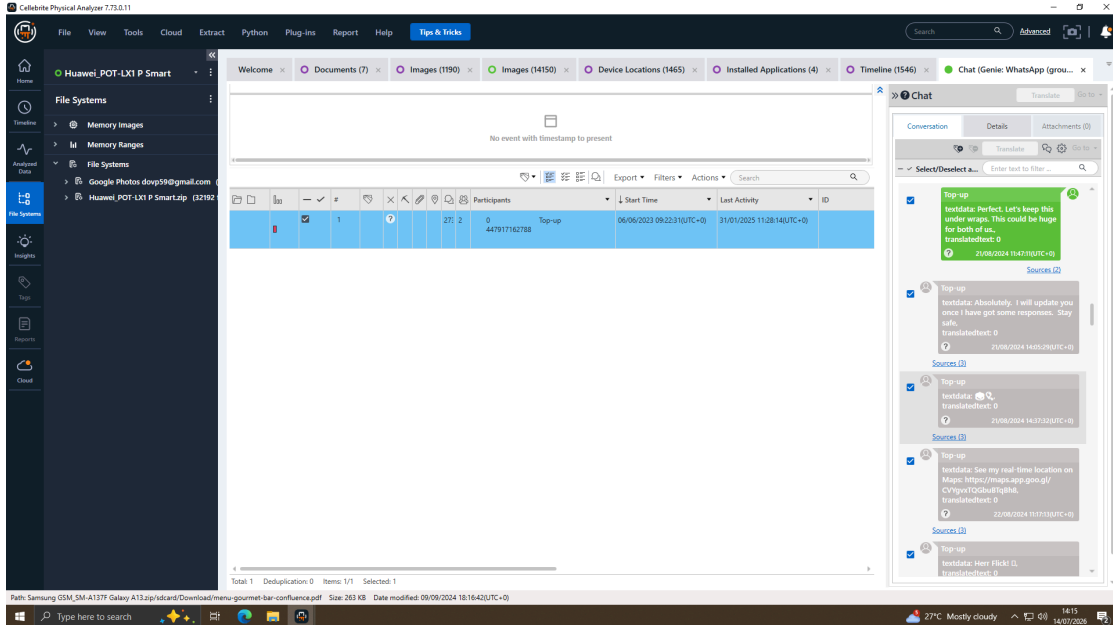
Overall, the Huawei examination established that Emma maintained regular contact with Joe throughout the relevant period and provided the **strongest communication evidence** recovered during the investigation. The recovered WhatsApp records formed the foundation for the timeline reconstruction and cross-device correlation presented in the subsequent sections.

Figure 13. WhatsApp communication between Emma and Joe



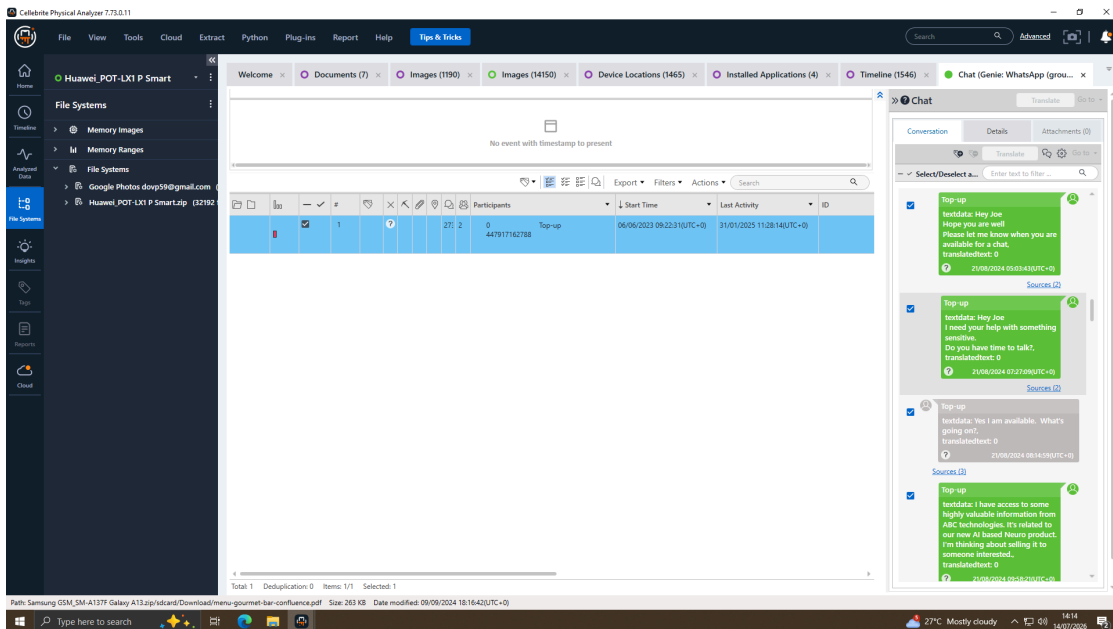
Recovered WhatsApp conversation showing direct communication between the primary suspect (Emma) and Joe.

Figure 14. Follow-up negotiation message



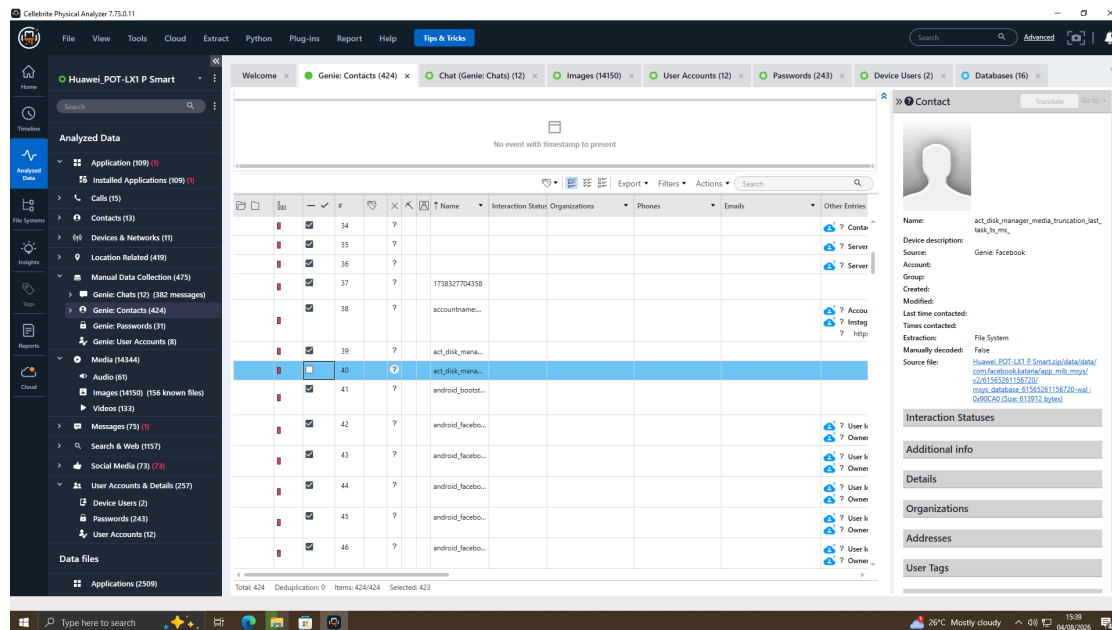
Additional WhatsApp communication demonstrating ongoing coordination between Emma and Joe.

Figure 15. Additional communication thread



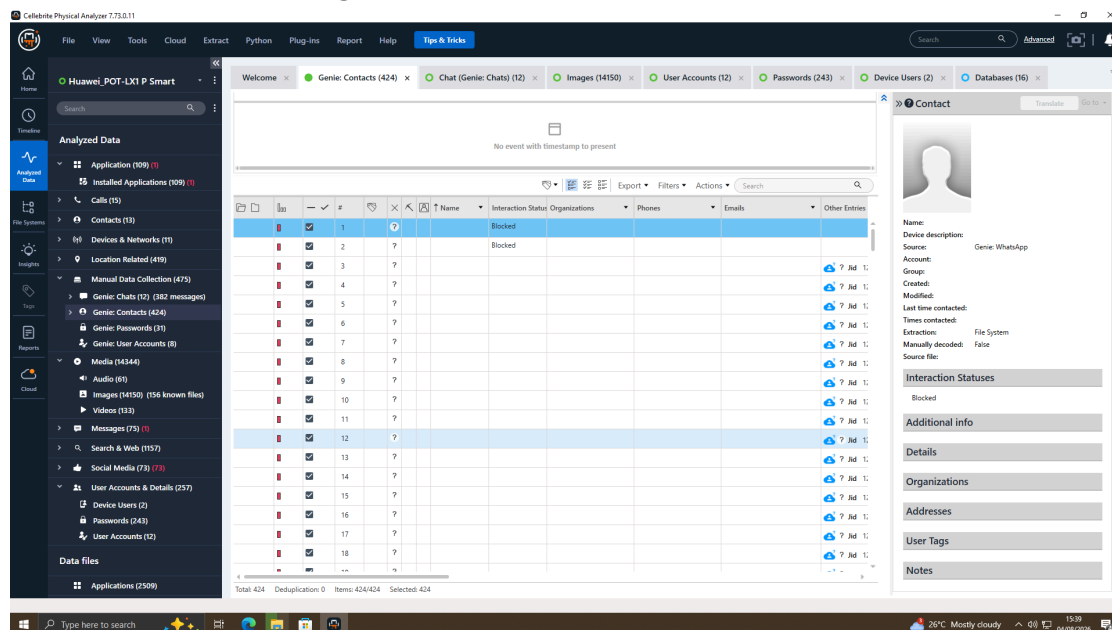
Extended communication history demonstrating repeated interaction between the suspects.

Figure 16. Message metadata and conversation details



Recovered timestamps, participant information, and message metadata associated with the communication records.

Figure 17. Extracted conversation database



Recovered WhatsApp database and communication artefacts extracted from Emma's Huawei P Smart device.

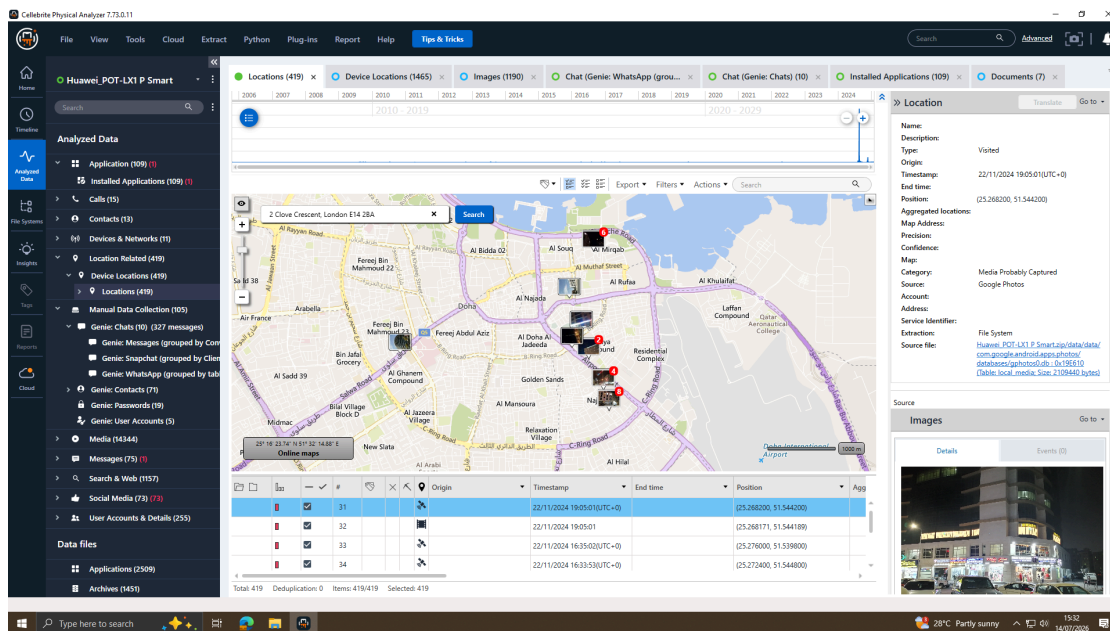
2.6 Timeline and Location Correlation - Huawei P Smart

Timeline reconstruction was performed using **location artefacts and timestamped communication records** recovered from Emma's Huawei P Smart. Correlating these artefacts enabled investigators to reconstruct the sequence of events and determine whether Emma was present in locations relevant to the suspected meetings with Joe. **Figures 18–20** present representative location and timeline artefacts recovered from the Huawei device [1].

The recovered timestamps showed that communication between **Emma and Joe** occurred during the same period in which relevant location information was recorded on the device. The consistency between communication records and location artefacts provided **corroborative evidence** supporting the reconstructed timeline and linking the communication analysis in Section 2.5 with the cross-device examination conducted later in the investigation.

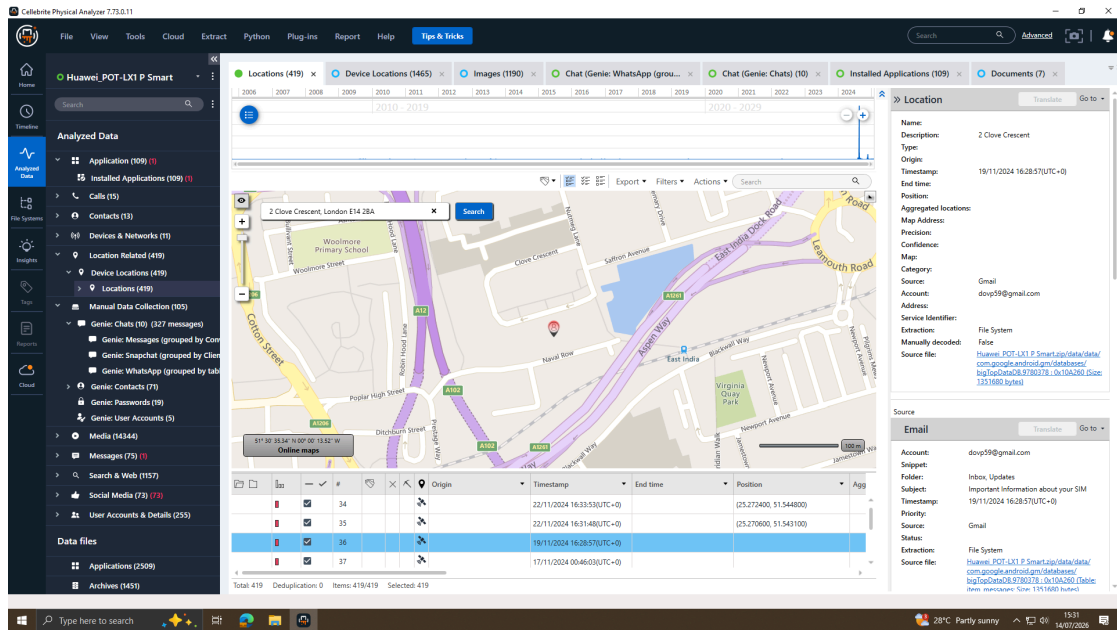
Overall, the timeline and location analysis strengthened the reliability of the investigation by demonstrating a temporal relationship between **communications, movements, and suspected meeting activity** during the relevant investigation period.

Figure 18. Location artefact extracted from Huawei device



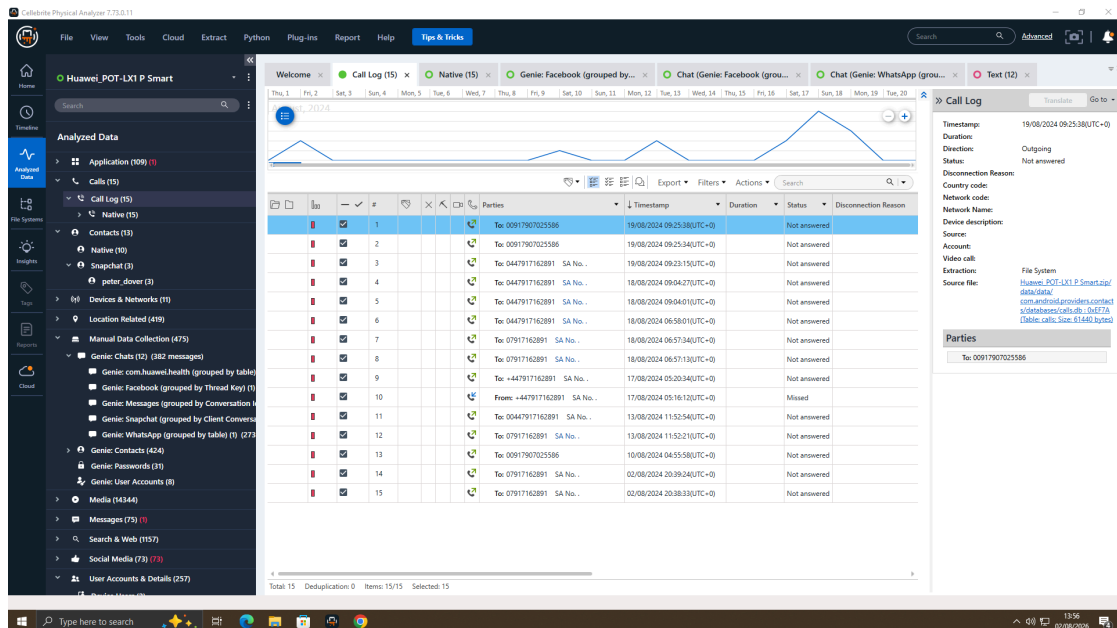
Recovered location information associated with Emma's Huawei P Smart smartphone.

Figure 19. Additional location mapping evidence



Supplementary geographic evidence recovered from the Huawei device.

Figure 20. Timeline of communications and device activity



Chronological reconstruction of communication and device activity extracted from the Huawei P Smart.

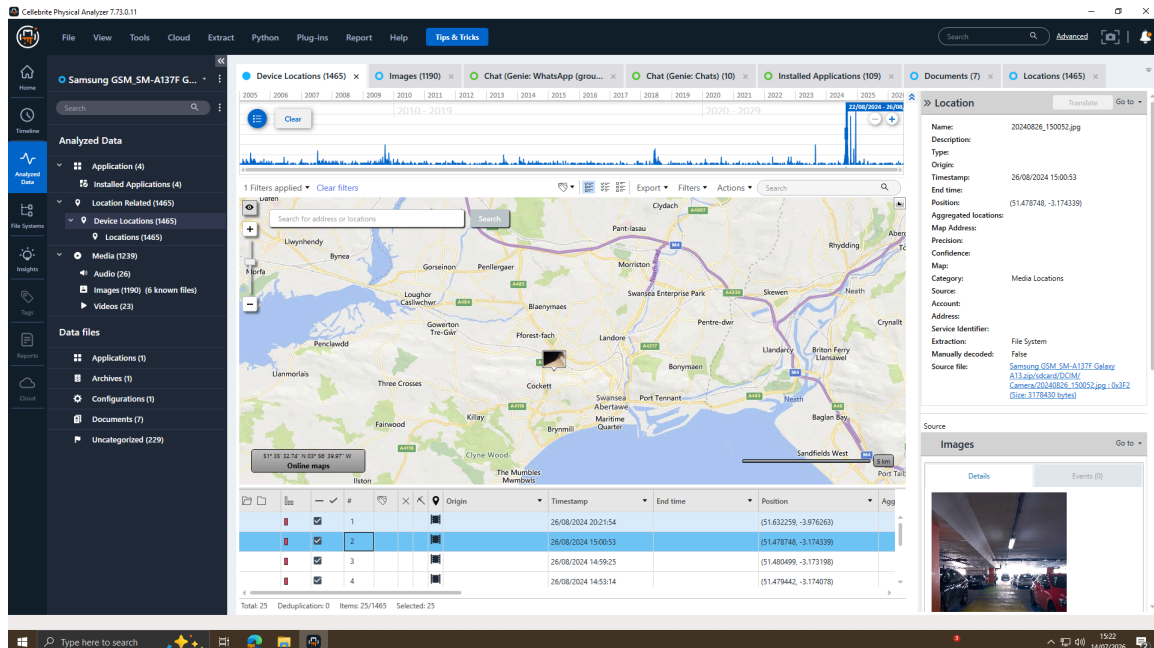
2.7 Corroborative Analysis - Samsung Galaxy A13 (Joe)

The forensic examination of **Joe's Samsung Galaxy A13 smartphone (Evidence ID: E02)** was conducted to determine whether evidence recovered from **Emma's Huawei device** could be independently corroborated. The Samsung device was analysed for **location records, communication artefacts, timeline information, and recovered data** that could be compared with the communications identified between Emma and Joe. **Figures 19–22** present representative location and timeline artefacts extracted from the Samsung device.

Analysis of the recovered artefacts showed that **Joe's device was active during the same period in which communication occurred between Emma and Joe**, providing independent corroboration of the Huawei findings. The consistency between the Samsung timeline records and the Huawei communication evidence strengthened the reliability of the reconstructed sequence of events and supported the conclusion that **Joe acted as an intermediary** during the suspected transfer of confidential information [1].

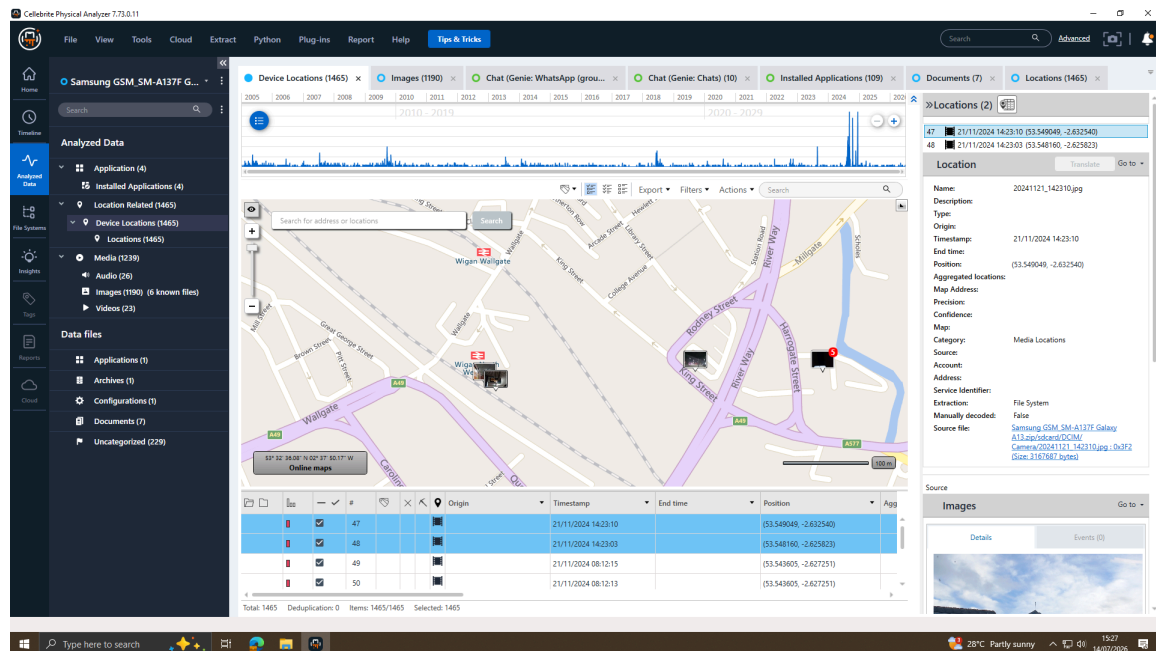
Overall, the Samsung examination provided **corroborative evidence** that supported the communication and timeline analysis established from Emma's Huawei device and reinforced the cross-device findings presented later in this report.

Figure 21. Samsung location evidence



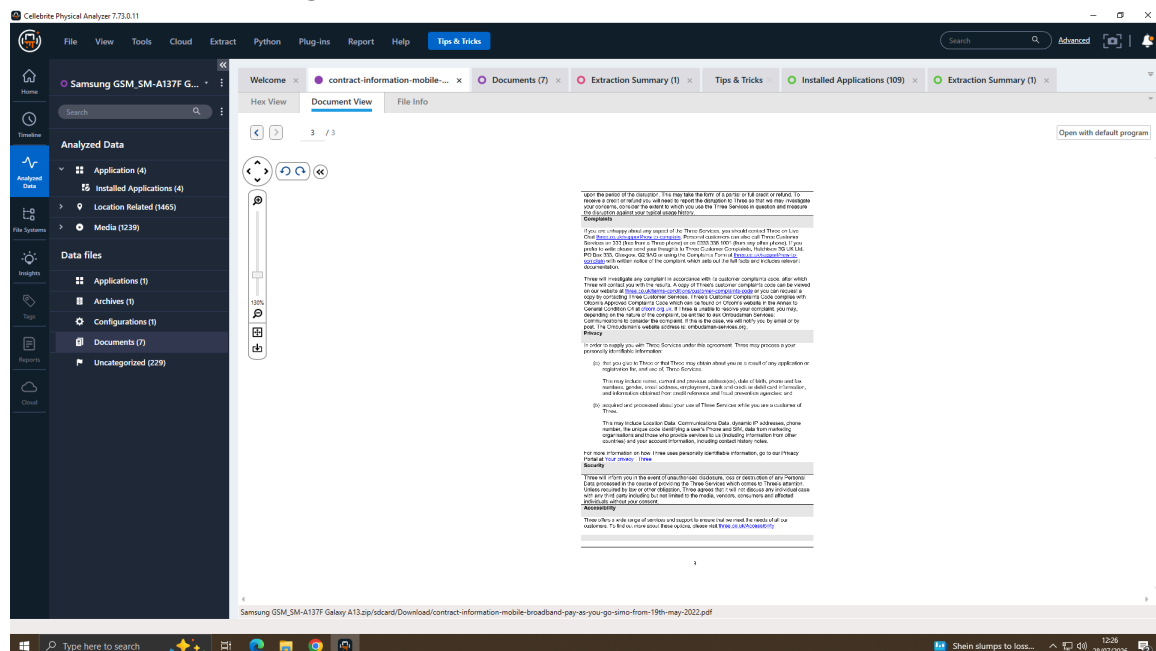
Location information recovered from Joe's Samsung Galaxy A13 smartphone.

Figure 22. Additional location correlation



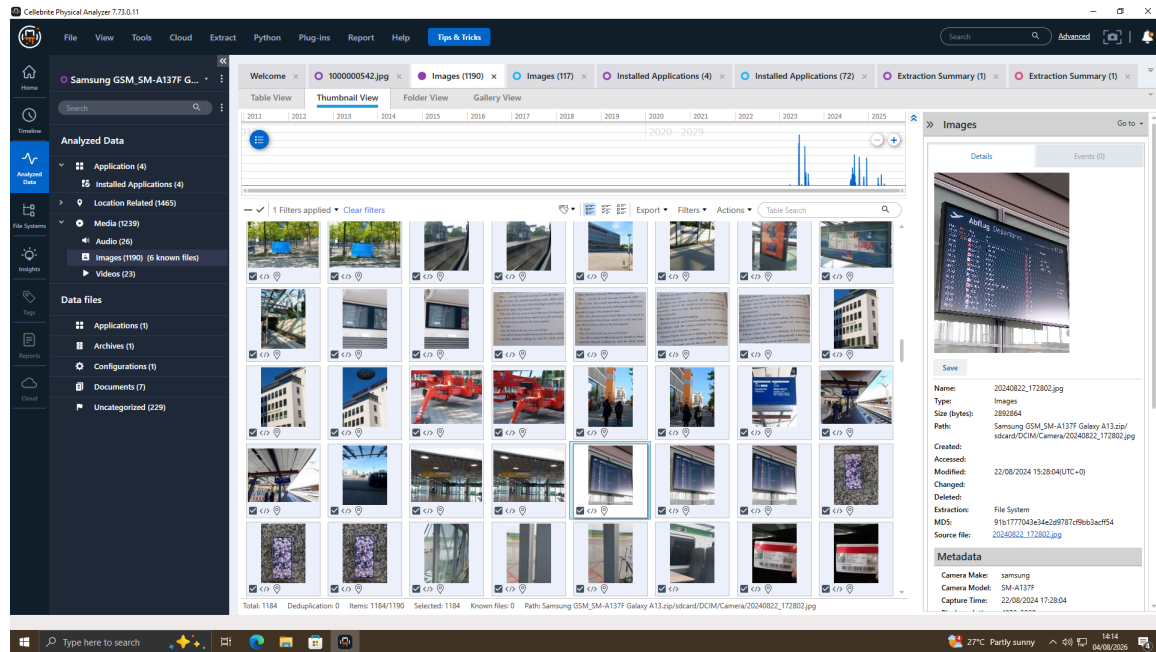
Supplementary geographic evidence extracted from the Samsung device.

Figure 23. Communication or document artefact



Chronological activity records recovered from the Samsung Galaxy A13.

Figure 24. Timeline and activity records



Chronological activity records recovered from the Samsung Galaxy A13.

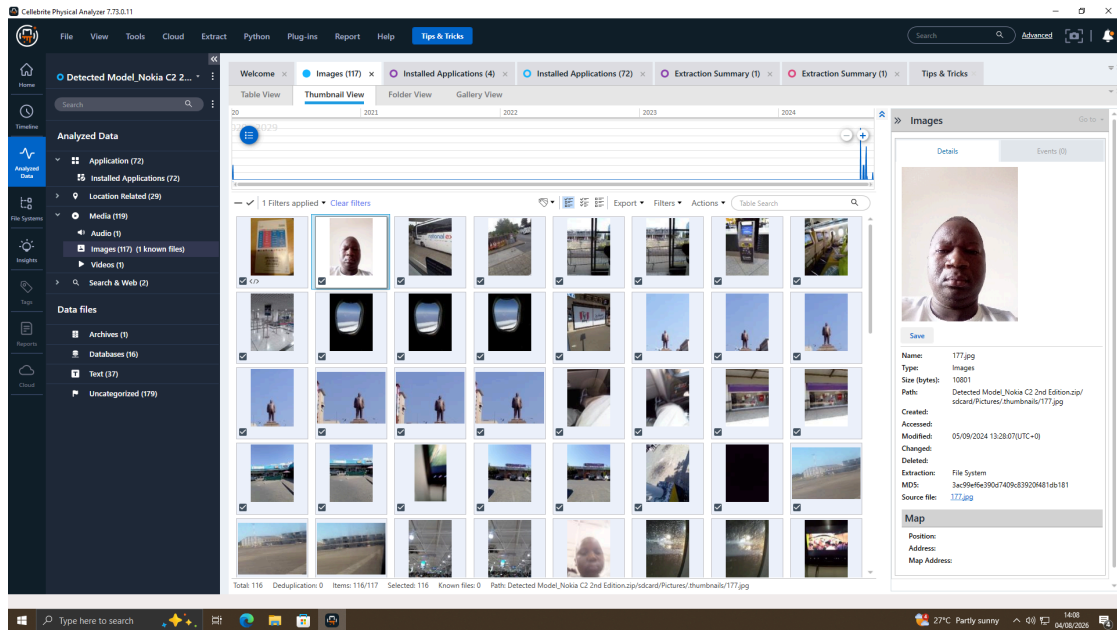
2.8 Recipient Evidence - Nokia C2 2nd Edition (Norman)

The forensic examination of **Norman's Nokia C2 2nd Edition smartphone (Evidence ID: E03)** was conducted to determine whether the recipient device contained evidence consistent with the communication and timeline analysis established from **Emma's Huawei** and **Joe's Samsung** devices. The examination focused on **media files, documents, file-system artefacts, and other recovered data** relevant to the suspected transfer of confidential information. **Figures 25–28** present representative artefacts recovered from the Nokia device.

Analysis of the recovered files confirmed that relevant media and file-system artefacts had been successfully extracted and preserved for forensic examination. Although the Nokia device contained less extensive communication evidence than the Huawei and Samsung devices, the recovered artefacts were **consistent with recipient-side evidence** and supported the overall reconstruction of events established through cross-device correlation [2].

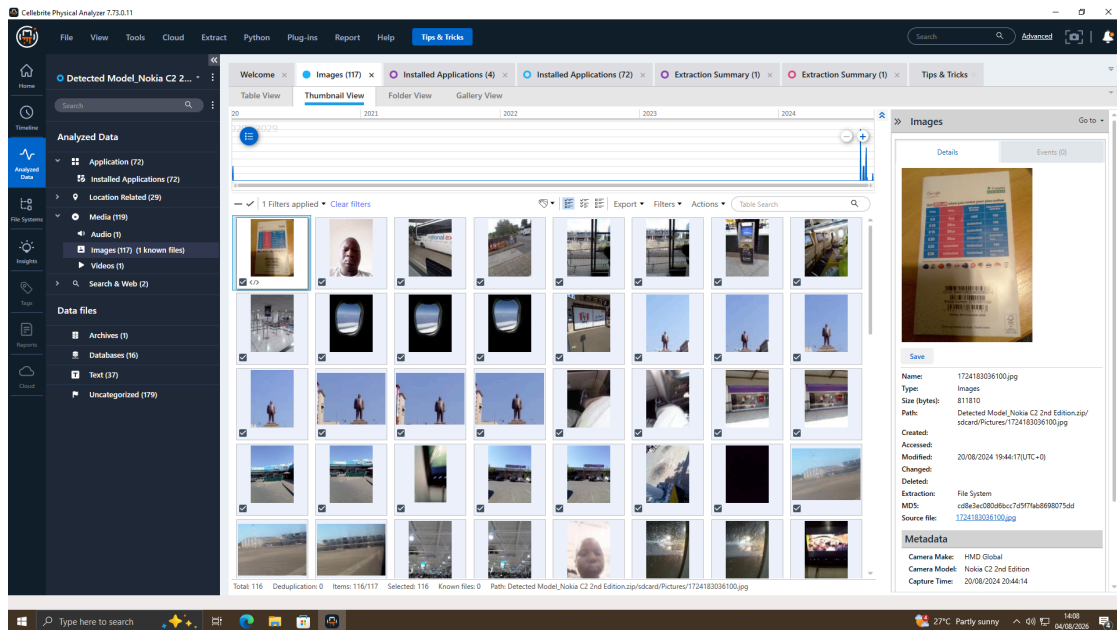
Overall, the Nokia examination provided supporting evidence that reinforced the communication and timeline findings recovered from the other devices and strengthened the conclusion that **Norman was the intended recipient** of the confidential information.

Figure 25. Extracted media artefacts from Nokia device



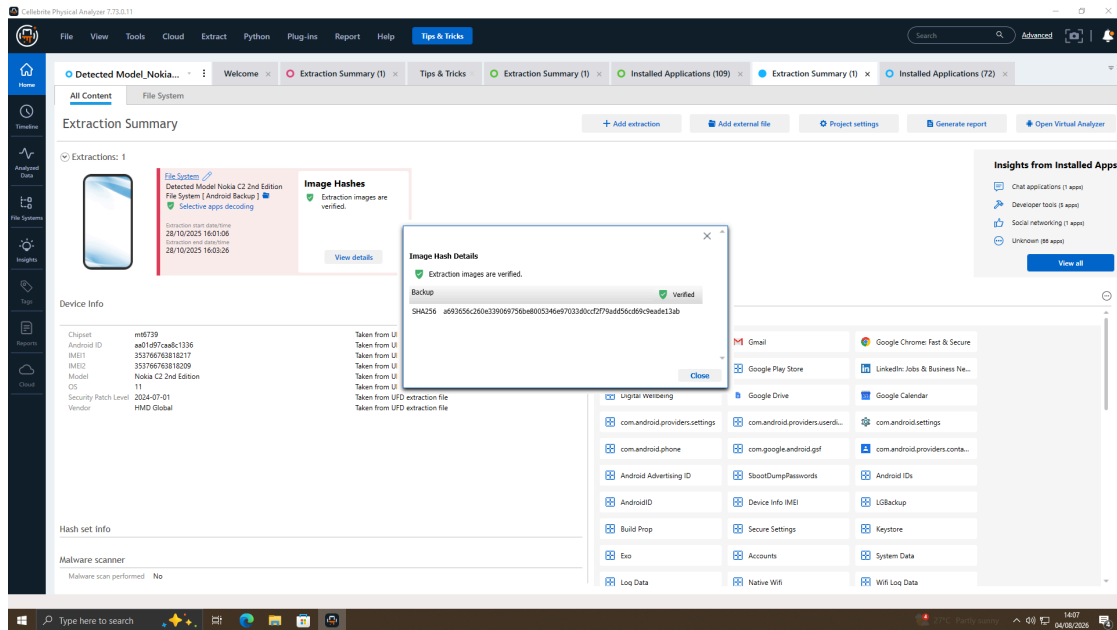
Recovered media and file artefacts extracted from Norman's Nokia C2 2nd Edition smartphone.

Figure 26. Additional extracted content



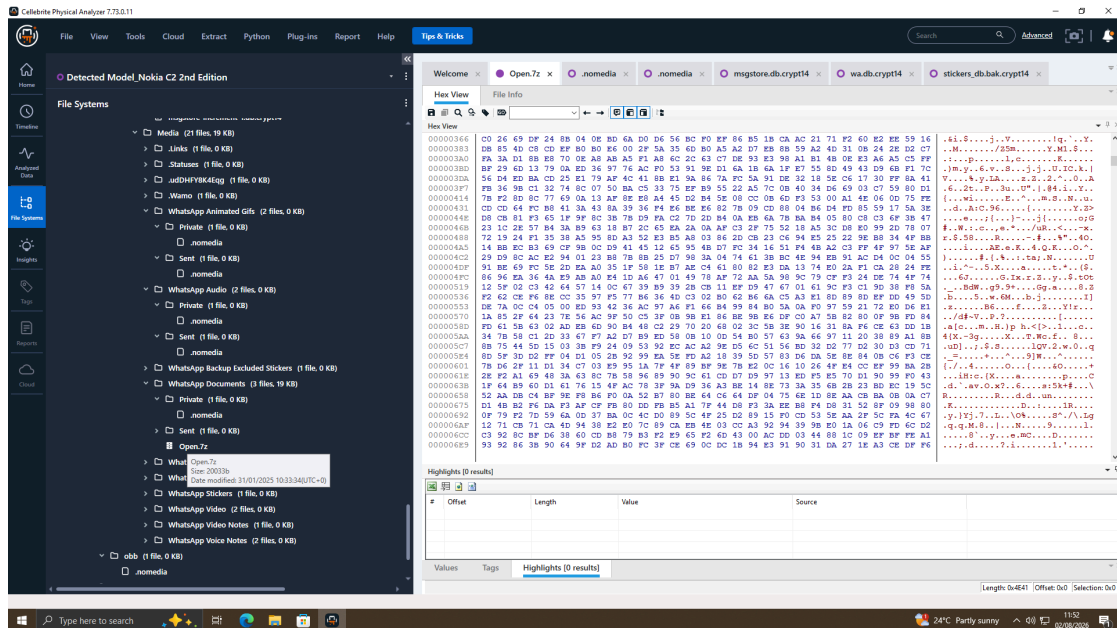
Supplementary artefacts recovered from the Nokia device.

Figure 27. File-system evidence



File-system level evidence recovered from Norman's device.

Figure 28. Hex-level artefact examination



Low-level forensic examination of recovered data from the Nokia C2 2nd Edition.

2.9 Cross-Device Correlation

The final stage of the investigation involved **cross-device correlation**, comparing evidence recovered from **Emma's Huawei P Smart**, **Joe's Samsung Galaxy A13**, and **Norman's Nokia C2 2nd Edition** to reconstruct the sequence of events associated with the suspected transfer of confidential information. Communication records, timestamps, location artefacts, and recovered files were examined across the three devices to identify consistent patterns and determine whether the evidence collectively supported the investigative hypothesis.

The comparison demonstrated a **consistent relationship** between the three devices. Emma's Huawei device provided the strongest communication evidence, Joe's Samsung device contained timeline and location artefacts corresponding to the communication period, and Norman's Nokia device contained media and file-system artefacts consistent with recipient-side evidence[1]. The chronological alignment of these artefacts strengthened the reliability of the reconstructed timeline and reduced the likelihood that the findings resulted from isolated or unrelated activity.

Figure 29. Summarises the principal correlations identified across the three devices.

Event	Emma (Huawei POT-LX1)	Joe (Samsung SM-A137F)	Norman (Nokia C-2 2nd Edition)
Initial contact	✓ Yes	✓ Yes	✗ No
Negotiation	✓ Yes	✓ Yes	✗ No
Meeting arrangement	✓ Yes	✓ Yes	✓ Yes
Location evidence	✓ Yes	✓ Yes	✓ Yes
Recovered files	✓ Yes	? Possible	✓ Yes
✓ Yes: Evidence found / Correlated ? Possible: Partial / Indirect Evidence ✗ No: No Evidence / Not Correlated			

Overall, the **cross-device correlation** showed that the evidence recovered from the three devices was **mutually supportive**, providing a coherent reconstruction of events and strengthening the evidential reliability of the investigation [1]. This integrated analysis formed the basis for the timeline reconstruction and suspect profiling presented in the following sections.

2.9.1 Timeline of Key Events and Actions

A chronological timeline was constructed by correlating **WhatsApp communications, message metadata, and location artefacts** recovered from Emma’s Huawei and Joe’s Samsung devices. The timeline assisted investigators in reconstructing the sequence of events associated with the suspected transfer of confidential information and demonstrated the relationship between communication activity and the physical proximity of the suspects [1].

Table 1. Timeline of Key Events and Actions

Date/Time (UTC)	Event	Description	Participants	Evidence Source	Additional Details
20/11/2024, 10:01:24	Initial follow-up communication	Emma requests an update regarding the proposed patent transaction and indicates that she has identified another potential contact.	Emma, Joe	Huawei WhatsApp (Figure 11)	Demonstrates Emma’s active involvement in pursuing the transaction.
20/11/2024, 10:03:04	Response from Joe	Joe apologises for the delay and states that he is meeting a client in Manchester.	Joe, Emma	Huawei WhatsApp (Figure 12)	Indicates that Joe is engaged in negotiations and coordinating with a third party.
20/11/2024, 10:04:44	Continued negotiation	Emma informs Joe that she may proceed with another party if progress is not made.	Emma, Joe	Huawei WhatsApp (Figure 13)	Suggests urgency and the existence of alternative buyers.
20/11/2024, 11:03:59	Confidential agreement	Joe agrees to continue the matter discreetly and emphasises confidentiality.	Joe, Emma	Huawei WhatsApp (Figure 14)	Supports the inference that the transaction was intended to remain concealed.

23/03/2025, 07:27:37	Location correlation (Joe)	Location records place Joe near the suspected meeting area during the relevant investigation period.	Joe	Samsung Location Data (Figure 19)	Correlates with Emma's recorded location and supports the possibility of a meeting.
23/03/2025, 07:27:40	Location correlation (Emma)	Emma's device records indicate presence in the same geographical area during communication activity.	Emma	Huawei Location Data (Figure 16)	The close temporal and geographical proximity strengthens cross-device correlation.
23/03/2025, 07:28:00	Timeline synchronisation	Device activity and communication records from Huawei and Samsung show chronological consistency across both devices.	Emma, Joe	Huawei Timeline (Figure 18); Samsung Timeline (Figure 22)	Supports the reconstructed sequence of events presented in the investigation.

Timeline Analysis

The timeline demonstrated a progressive pattern of communication and coordination between **Emma and Joe**, with discussions relating to meetings, negotiations, and confidentiality. The location artefacts recovered from both devices indicated that the suspects were in close geographical proximity during the relevant period, providing **corroborative evidence** that supported the reconstructed sequence of events and the overall investigative findings.

2.10 Suspect Profiling

The forensic investigation enabled profiles to be developed for the three principal suspects using **communication records, location artefacts, recovered files, and cross-device correlations** recovered from their mobile devices[1].

Emma (Primary Perpetrator)

Emma was identified as the **primary suspect** because she had authorised access to Quantum Tech's confidential patent information. The Huawei examination recovered WhatsApp conversations, message metadata, timeline records, and location artefacts indicating regular communication with Joe during the relevant investigation period (**Figures 11–18**).

Joe (Intermediary)

Joe was identified as an **intermediary** between Emma and Norman. Evidence recovered from the Samsung Galaxy A13, including location and timeline artefacts, corresponded with the communications identified on Emma's device (**Figures 19–22**).

Norman (Intended Recipient)

Norman was identified as the **intended recipient** of the confidential information. The Nokia C2 2nd Edition contained media and file-system artefacts consistent with recipient-side evidence and the reconstructed timeline (**Figures 23–26**).

Overall, the forensic evidence indicated a coordinated relationship between the three individuals, with Emma acting as the source of the information, Joe facilitating communication, and Norman functioning as the intended recipient.

2.11 Findings

The forensic investigation successfully acquired and analysed evidence from the **Huawei P Smart, Samsung Galaxy A13, and Nokia C2 2nd Edition** devices using Cellebrite UFED. Communication records, timeline information, location artefacts, and recovered files were correlated across the three devices to reconstruct the suspected sequence of events. The evidence showed consistent communication between **Emma and Joe**, corroborative timeline and location records on Joe's Samsung device, and recipient-side artefacts on Norman's Nokia device. Collectively, these findings support the allegation of **unauthorized transfer of confidential information** and provide a coherent reconstruction of the suspected corporate espionage incident [1].

2.12 Conclusion

This investigation applied recognised digital forensic procedures, including **evidence acquisition, preservation, examination, analysis, and cross-device correlation**, to investigate a suspected case of corporate espionage [1], [2]. **Cellebrite UFED** enabled the recovery of communication records, location artefacts, and digital files from multiple mobile devices while maintaining **evidence integrity and chain of custody**. Correlation of evidence across the **Huawei, Samsung, and Nokia** devices produced a consistent timeline that supported the investigative findings and demonstrated the value of systematic mobile forensic analysis in reconstructing cyber-enabled incidents. The recovered evidence provides a reliable basis for further legal or organisational proceedings and highlights the importance of digital forensic methodologies in modern cybersecurity investigations [2].

Reference

- [1] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3rd ed. Amsterdam, The Netherlands: Academic Press, 2011.
<https://www.sciencedirect.com/book/9780123742681/digital-evidence-and-computer-crime>
- [2] ISO/IEC 27037:2012, *Information Technology-Security Techniques-Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*. Geneva, Switzerland: International Organization for Standardization, 2012.
<https://www.iso.org/standard/44381.html>
- [3] National Institute of Standards and Technology (NIST), *Guide to Integrating Forensic Techniques into Incident Response (Special Publication 800-86)*. Gaithersburg, MD, USA: NIST, 2006. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>
- [4] National Institute of Standards and Technology (NIST), *Computer Security Incident Handling Guide (Special Publication 800-61 Rev. 2)*. Gaithersburg, MD, USA: NIST, 2012.
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>
- [5] B. Carrier, *File System Forensic Analysis*. Boston, MA, USA: Addison-Wesley, 2005.
<https://www.pearson.com/en-us/subject-catalog/p/file-system-forensic-analysis/P200000003161>
- [6] Cellebrite, *UFED User Guide and Mobile Device Forensics Documentation*. Petah Tikva, Israel: Cellebrite, 2025. <https://docs.cellebrite.com/>
- [7] AccessData, *FTK Imager User Guide*. Lindon, UT, USA: AccessData Group, 2024.
<https://accessdata.com/product-download/ftk-imager-version-4-5>
- [8] R. Al-Mugren, A. Alqahtani, and M. Alshammari, "A Cloud Forensics Framework to Identify, Gather and Analyze Cloud Computing Incidents," *Engineering, Technology & Applied Science Research*, vol. 14, no. 3, 2024. <https://etasr.com/index.php/ETASR/article/view/7610>

Author's Note: All graphical illustrations, infographics, diagrams, and visual figures included in this report were designed and created by the author using **Adobe Illustrator**.