



Report on

Research, Analyse and Investigate Cybersecurity incidents and perform digital forensic assessment

Submitted By

Abdullah Al Noman

Student ID:

2520302

Module

Digital Forensics Analysis (ACCA7031_LON)

Department

MSC Cybersecurity and Digital Forensics

Table of Contents

Task 1	Page
1. Introduction	3
2. Current State of Digital Forensics and Forensic Tools	3
3. Intersection of Digital Forensics and Cybersecurity	3
4. Emerging Trends in Digital Forensics	4
5. Key Challenges in Digital Forensics	4
6. National and International Job Market	4
7. Conclusion	5
Task 2	
1. Case Background	5
2. Investigation Scope	5
3. Evidence Inventory	6
4. Chain of Custody and Evidence Integrity	6
5. Forensic Methodology	8
5.1 Evidence Acquisition	8
5.2 Examination Environment	9
6. Communication Analysis	11
6.1 Initial Contact	12
6.2 Discussion of Valuable Information	12
6.3 Buyer Identification Activities	13
6.4 Concealment and Secrecy	14
6.5 Location Coordination	15
6.6 Ongoing Negotiations	15
6.7 Financial Motivation	17
7. Correlation Between Digital and Physical Evidence	19
8. Timeline Reconstruction	22
9. Evidential Reliability Assessment	23
10. Suspect Profiling	24
11. Findings	25
12. Conclusion	26
13. Recommendations	26
References	26

Research, Analyse and Investigate Cybersecurity incidents and perform digital forensic assessment

Task 1

1.Introduction

Digital forensics has become one of the most important disciplines within cybersecurity due to the increasing number of cybercrimes, insider threats, data breaches, and cyber espionage incidents. Digital forensics refers to the identification, preservation, acquisition, examination, analysis, and presentation of digital evidence in a manner suitable for legal proceedings [1]. Cybersecurity professionals, private organizations, and law enforcement agencies all benefit from the discipline's assistance in investigating incidents involving digital communications, cloud platforms, computers, and mobile devices [2]. The significance of digital forensic investigations has skyrocketed in recent years [3]. This is due to the fact that modern businesses continue to heavily rely on digital technologies.

2.Current State of Digital Forensics and Forensic Tools

Digital forensics has evolved considerably over the last decade. Traditional investigations mainly focused on personal computers and storage devices, whereas modern investigations frequently involve smartphones, cloud environments, social media platforms, Internet of Things (IoT) devices, and virtual infrastructures [4]. Consequently, forensic investigators require sophisticated tools capable of processing large volumes of data while maintaining evidential integrity [5].

Cellebrite UFED, which facilitates the acquisition and analysis of mobile devices, is one of the most widely used tools. Cellebrite makes it possible for investigators to retrieve deleted messages, call logs, geolocation data, application data, multimedia content, and application data [6]. Similarly, EnCase is widely used in law enforcement and corporate investigations because of its powerful imaging, analysis, and reporting capabilities [7]. FTK Imager is commonly used for forensic acquisition and hash verification, while Autopsy provides a popular open-source platform supporting timeline generation, keyword searches, metadata analysis, and file recovery [8]. Although these tools provide comprehensive functionality, challenges remain when investigating encrypted devices, distributed cloud storage, and anti-forensic techniques designed to conceal digital evidence [9].

3.Intersection of Digital Forensics and Cybersecurity

Digital forensics and cybersecurity are closely related disciplines that complement one another. Cybersecurity primarily focuses on preventing, detecting, and responding to cyber threats, while digital forensics focuses on investigating incidents after they occur and determining how the attack was performed [10].

When organisations experience cybersecurity incidents such as ransomware attacks, insider threats, data breaches, or intellectual property theft, digital forensic investigators are often responsible for identifying the source of the attack and reconstructing the sequence of events [11]. The findings generated through forensic investigations assist organisations in improving security controls, strengthening incident response procedures, and supporting legal action against perpetrators [12].

Consequently, digital forensics has become an essential component of modern cybersecurity frameworks and incident response strategies [13].

4. Emerging Trends in Digital Forensics

Artificial intelligence (AI) and machine learning are increasingly being integrated into forensic investigations. These technologies help investigators analyse large datasets, identify patterns, automate repetitive tasks, and prioritise relevant evidence [14]. AI-assisted forensics may significantly reduce investigation times while improving analytical efficiency [15].

Cloud forensics has also emerged as a significant field of study. The widespread adoption of cloud computing means that digital evidence is frequently stored across geographically distributed infrastructures operated by third-party service providers [16]. This creates challenges relating to data acquisition, jurisdiction, and evidence preservation [17].

Another emerging trend is IoT forensics. Smart devices, wearable technologies, and connected sensors generate large volumes of potentially valuable evidence. However, device diversity, limited storage capabilities, and proprietary architectures often complicate forensic investigations [18].

Mobile device forensics continues to grow rapidly as smartphones increasingly become primary communication and storage platforms. Applications such as WhatsApp, Telegram, Signal, Instagram, and cloud storage services often contain critical evidential information during investigations [19].

5. Key Challenges in Digital Forensics

Despite technological advances, digital forensic investigators continue to face several significant challenges. Encryption remains one of the most prominent barriers because modern operating systems and applications increasingly implement strong security protections [20]. End-to-end encryption significantly limits access to communication records and may hinder evidence recovery efforts.

Another challenge is the increasing volume of data examined during investigations. Modern devices can store terabytes of information, requiring investigators to identify relevant evidence efficiently within vast datasets. Cloud storage services further complicate investigations because evidence may be distributed across multiple jurisdictions and owned by different service providers.

Additionally, anti-forensic techniques such as secure deletion, metadata manipulation, steganography, and anonymisation tools continue to evolve, making forensic investigations more complex and time-consuming.

6. National and International Job Market

The global demand for digital forensic professionals has increased substantially due to the growing frequency and sophistication of cybercrime. Organisations across both public and private sectors require specialists capable of investigating digital incidents, preserving evidence, and supporting legal proceedings.

Within the United Kingdom, opportunities exist within police digital forensic units, cybersecurity consulting firms, financial institutions, government agencies, and law enforcement organisations such as the National Crime Agency (NCA). Internationally, significant demand exists across North America, Europe, Australia, and Asia-Pacific regions, where organisations continue to invest heavily in cybersecurity capabilities.

Common job roles include Digital Forensic Analyst, Mobile Forensic Examiner, Incident Response Specialist, Cybercrime Investigator, Threat Intelligence Analyst, and Digital Forensic Consultant. Professional certifications such as CHFI, GCFA, CFCE, and EnCE often provide additional career advantages in the competitive job market.

7. Conclusion

Digital forensics has become an essential discipline for investigating cybercrime and supporting modern cybersecurity operations. Contemporary forensic tools such as Cellebrite, FTK, Autopsy, and EnCase enable investigators to analyse diverse forms of digital evidence while maintaining evidential integrity [6], [8]. Emerging technologies including artificial intelligence, cloud forensics, and IoT investigations continue to transform the field, although encryption, anti-forensic techniques, and growing data volumes remain major challenges [14], [20]. As cyber threats continue to increase globally, demand for skilled digital forensic professionals is expected to remain strong across both national and international job markets.

Task 2

1. Case Background

Quantum Tech reported a suspected insider-related security incident involving valuable AI-related corporate information. Emma, a recently appointed senior engineer, was identified as the primary subject of interest following concerns regarding potential disclosure of confidential information to external parties. Joe was identified as a possible intermediary involved in communications relating to external contacts and prospective meetings.

A digital forensic investigation was authorised to examine multiple mobile devices and identify evidence relating to communications, coordination activities, negotiation discussions, location information, travel records, and other artefacts relevant to the reported incident.

The purpose of the investigation was to determine whether recovered digital evidence demonstrated planning, coordination, communication, or attempts to disclose confidential corporate information.

2. Investigation Scope

The investigation focused on the following objectives:

- Identification and acquisition of digital evidence from seized mobile devices.
- Verification of evidence integrity through cryptographic hashing.
- Recovery and examination of communication artefacts.
- Correlation of communication records with travel-related and location-based evidence.
- Reconstruction of a forensic timeline.
- Identification of the roles of involved individuals based solely on recovered evidence.
- Preparation of a legally defensible forensic report.

3. Evidence Inventory

The investigation involved the examination of multiple digital devices recovered during the inquiry. Table 1 summarises the evidence sources and the primary artefacts identified during forensic analysis.

Evidence ID	Device	Uique Identifier	Relevant Artefacts Recovered
E01	Huawei POT-LX1 P Smart	Mobile Device Extraction	WhatsApp, Images, Timeline Data, Location Artefacts
E02	Nokia C2 2nd Edition	Mobile Device Extraction	Images, Documents, Metadata Artefacts
E03	Samsung Galaxy A13	Mobile Device Extraction	Images, Travel Artefacts, Hotel Photographs
E04	Samsung Galaxy A14	IMEI 358867374199958	Timeline Artefacts, Device Metadata, Images

Table 1. Evidence Inventory

The recovered evidence consisted of four mobile devices acquired using forensically sound procedures. Examination focused on communication artefacts, media files, timeline records, travel-related evidence, and device metadata. The collected artefacts were subsequently correlated to reconstruct events, identify communication patterns, and establish relationships between recovered digital evidence sources.

4. Chain of Custody and Evidence Integrity

Evidence integrity is essential within any digital forensic investigation because evidence must remain unchanged from acquisition through examination. Cryptographic hash verification is commonly used to demonstrate that digital evidence has not been modified following acquisition.

All acquired forensic images were verified using SHA256 cryptographic hash values within Cellebrite Physical Analyzer. Cryptographic hashing remains a recognised forensic approach for validating evidential integrity and admissibility.

Verification results confirmed that extracted data remained unchanged throughout the investigative process.

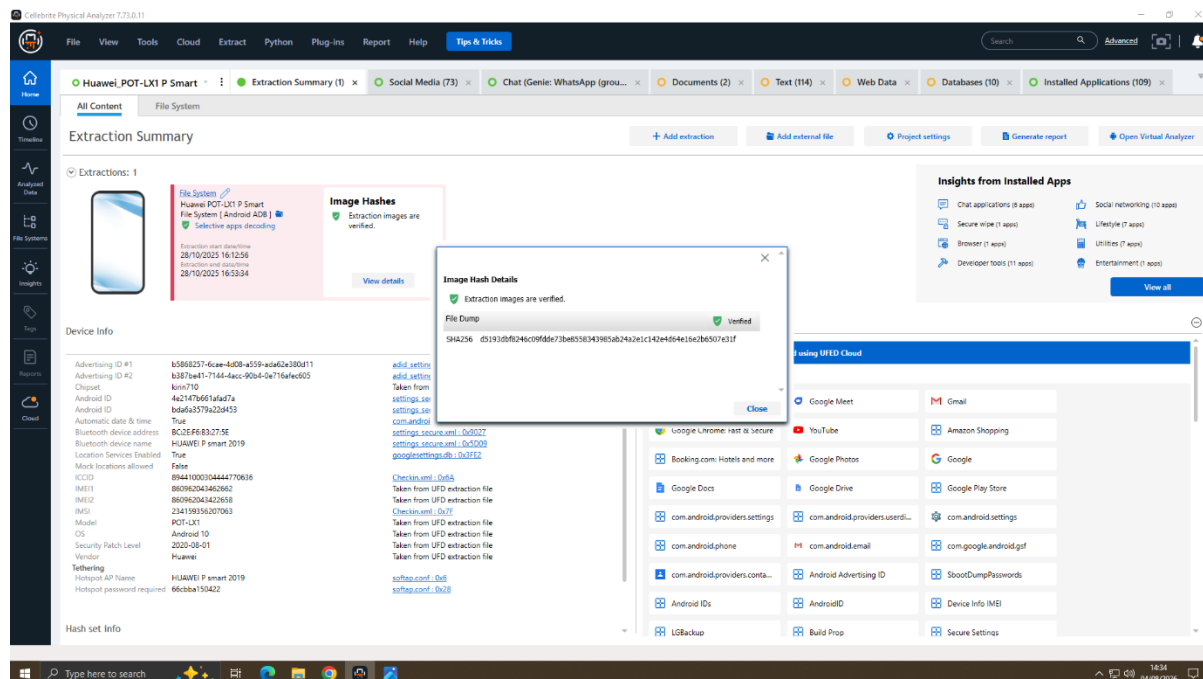


Figure 1. SHA256 Verification

Following acquisition, cryptographic hash verification was performed to ensure the integrity and authenticity of all forensic images. SHA256 hashing was utilised because it provides a reliable mechanism for detecting any modification to acquired evidence and is widely accepted within digital forensic investigations.

Device	SHA256 Hash Value	Verification Status
Huawei POT-LX1 P Smart	d5193dbf8246c09fdde73be8558343985ab24a2e1c142e4d64e16e2b6507e31f	Verified
Nokia C2 2nd Edition	a693656c260e339069756be8005346e97033d0ccf2f79add56cd69c9eae13ab	Verified
Samsung Galaxy A13	0e585c4fe8160254253be515a16ff94b7fdf88b248b67d45cfdef8753a9a3195	Verified
Samsung Galaxy A14	46c0872c1b8986c8d53069ddf4874f041e818e15bf89d64c9842dd0bb6c40c5e	Verified

Table 2. Hash Verification Summary

Table 2 demonstrates that all acquired forensic images successfully passed SHA256 verification. Matching hash values confirmed that no alterations occurred between acquisition and analysis. Consequently, the acquired evidence was considered authentic, reliable, and suitable for forensic examination. The integrity verification process supports the admissibility and evidential value of the recovered artefacts throughout the investigation.

5. Forensic Methodology

The investigation followed recognised digital forensic procedures consisting of identification, acquisition, preservation, examination, analysis and reporting stages. Consisting of acquisition, verification, extraction, analysis, correlation, and reporting.

5.1 Evidence Acquisition

The devices were acquired using Cellebrite UFED. Device information was recorded prior to acquisition to establish a reliable evidential reference and ensure accurate identification of the examination target.

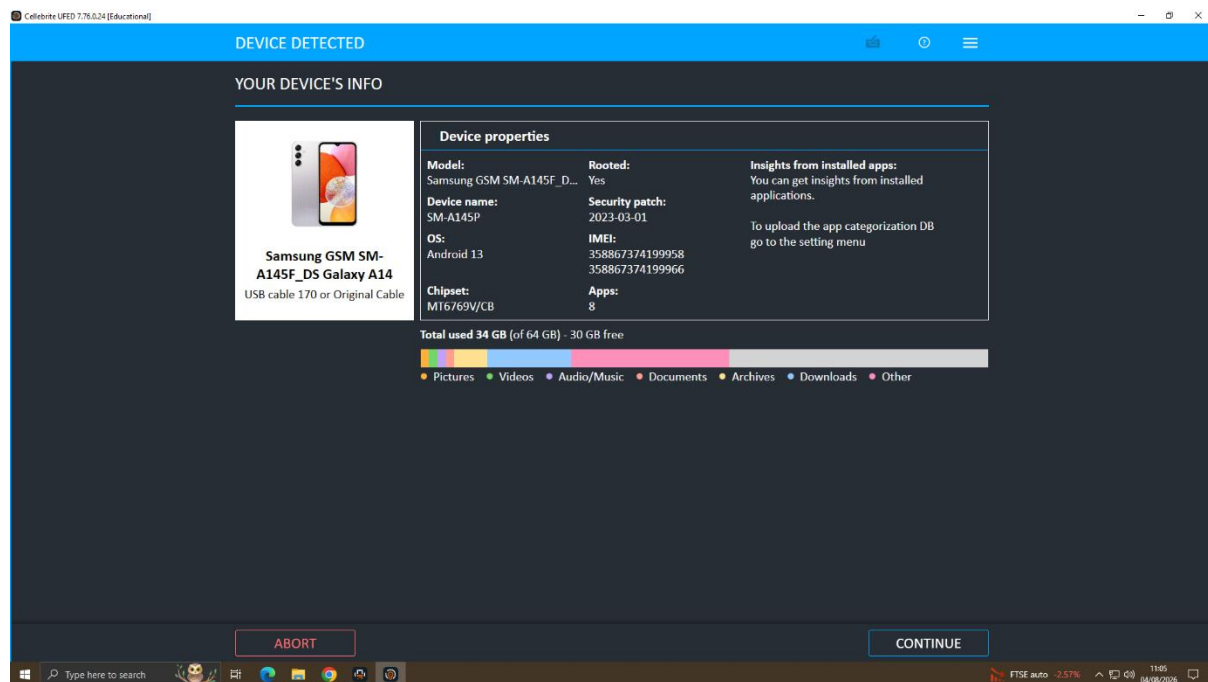


Figure 2. Device Identification Prior to Acquisition

The documented device characteristics provide traceability and support continuity of evidence throughout the investigation.

An appropriate extraction profile was selected to maximise the recovery of artefacts relevant to the investigation objectives.

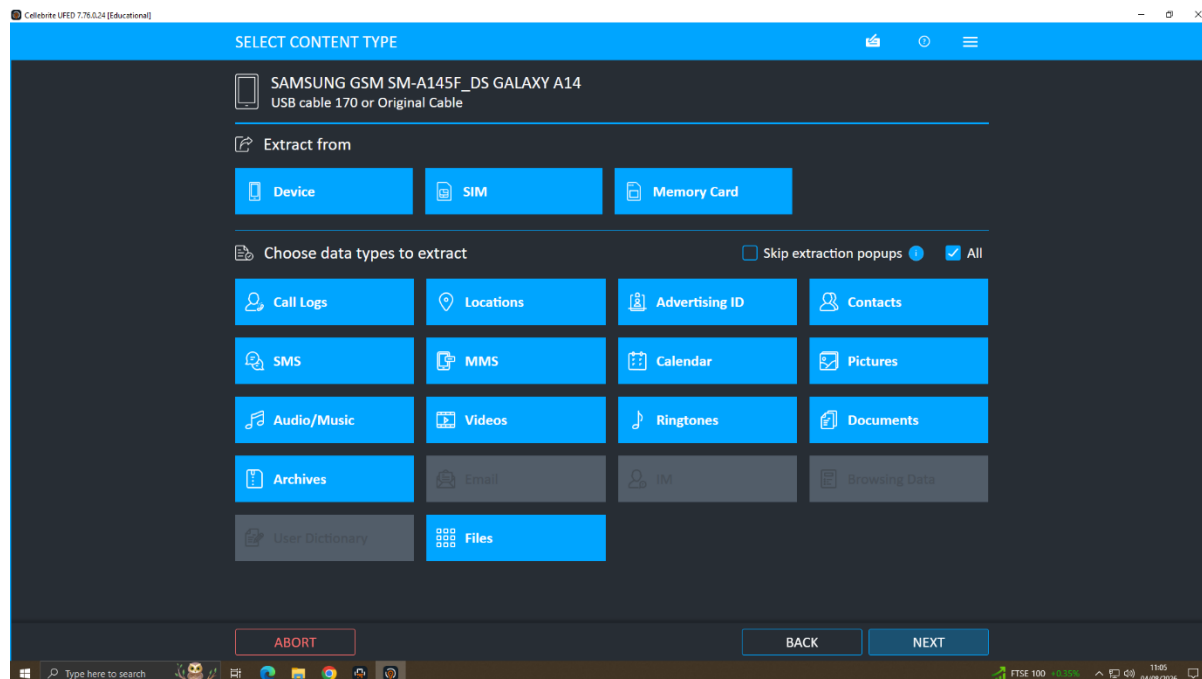


Figure 3. Extraction Scope Selection

The selected acquisition scope ensured that communications, media files, and supporting artefacts were available for examination.

5.2 Examination Environment

Analysis was conducted using Cellebrite Physical Analyzer. following acquisition, the forensic image was imported into the analysis environment for examination and artefact processing.

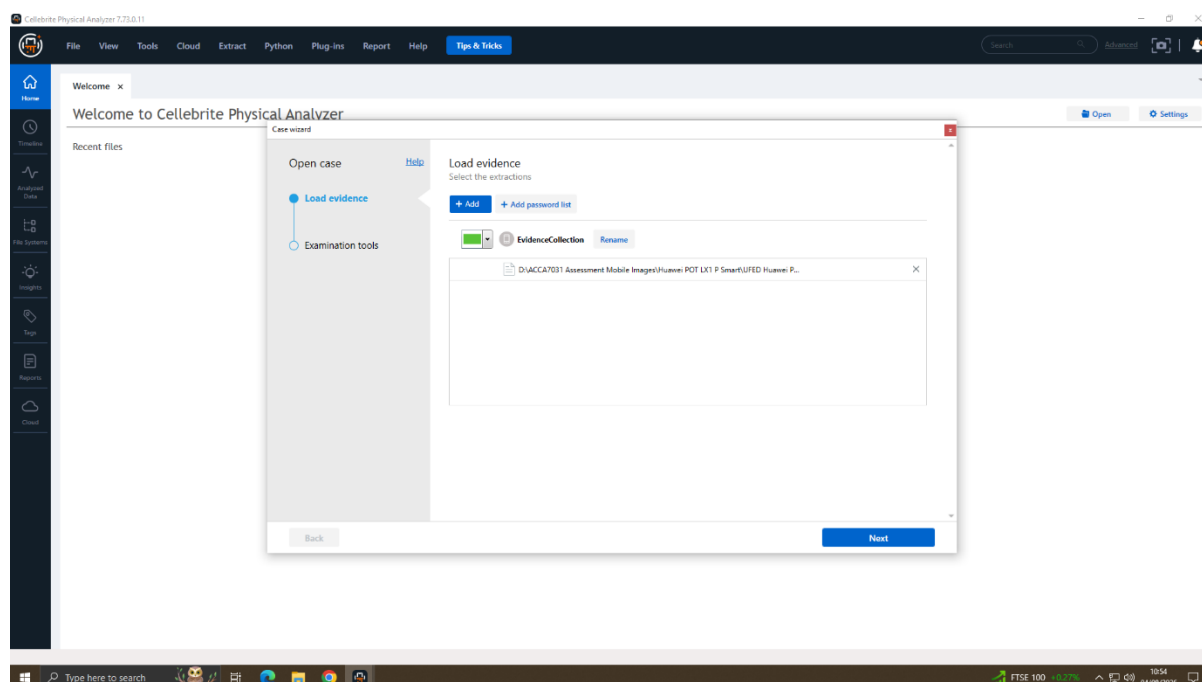


Figure 4. Loading Forensic Image into Physical Analyzer

Digital Forensics Analysis

Successful image loading enabled systematic analysis of recovered evidence and supporting metadata.

Application decoding was performed to identify relevant user-generated artefacts and communication records.

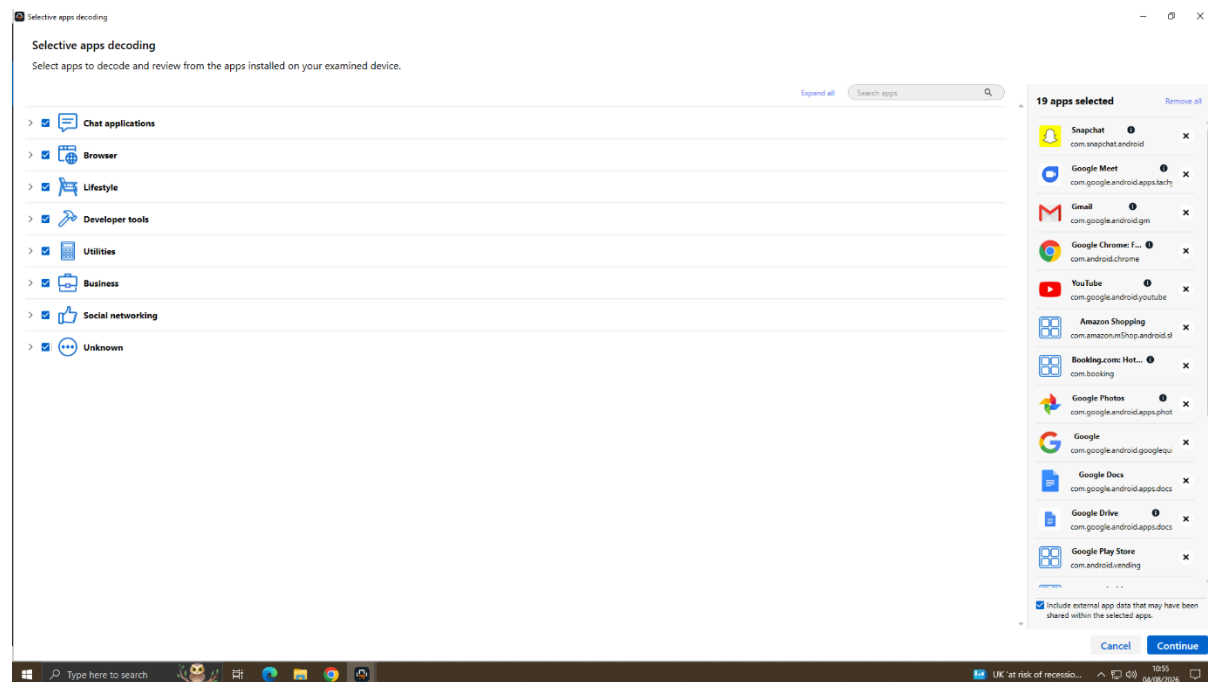


Figure 5. Selective Application Decoding

The decoding process improved visibility of application data and facilitated detailed investigative analysis.

The forensic dashboard provided an overview of recovered artefacts and device information.

Digital Forensics Analysis

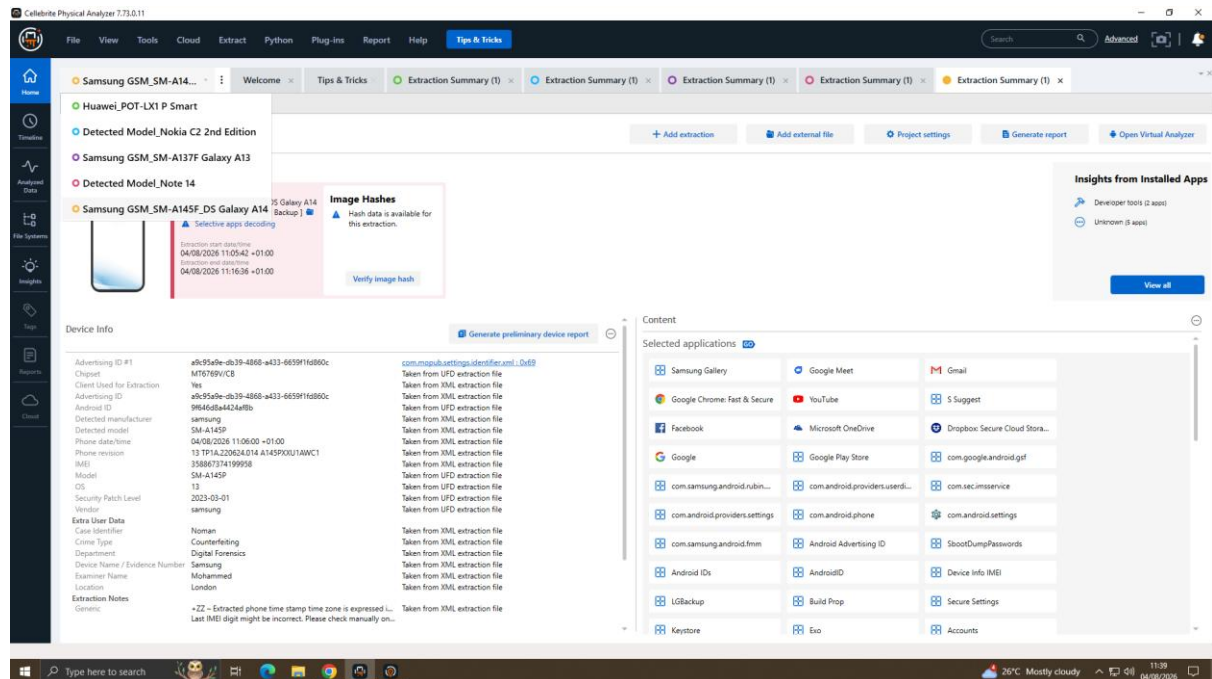


Figure 6. Examination Dashboard

The selected methodology ensured evidence preservation while maximising artefact recovery and analytical repeatability. The dashboard confirmed successful processing and readiness for detailed forensic examination.

6. Communication Analysis

Recovered WhatsApp artefacts provided the most significant body of evidence within the investigation. Communication artefacts were prioritised during analysis due to their potential evidential value within the investigation.

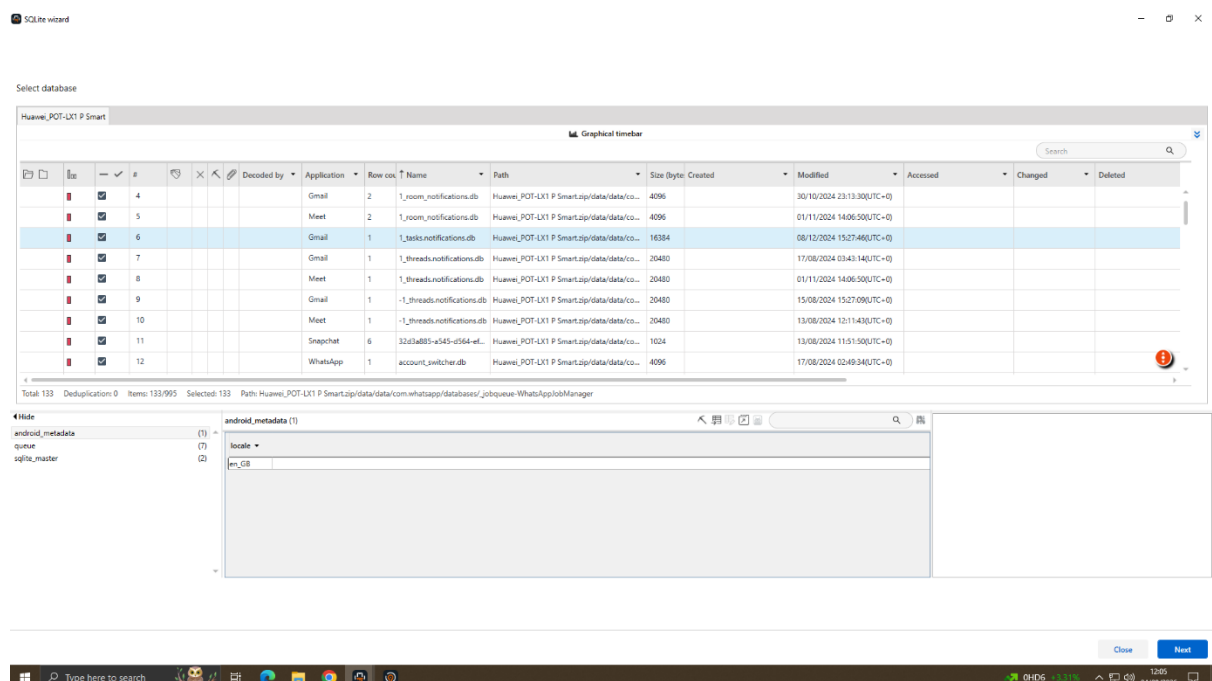


Figure 7. WhatsApp Database Artefacts

The recovered databases confirmed that communication records were available for forensic analysis. The recovered databases confirmed the availability of communication records suitable for further examination.

6.1 Initial Contact

The communication timeline began with the identification of direct interactions between involved individuals.

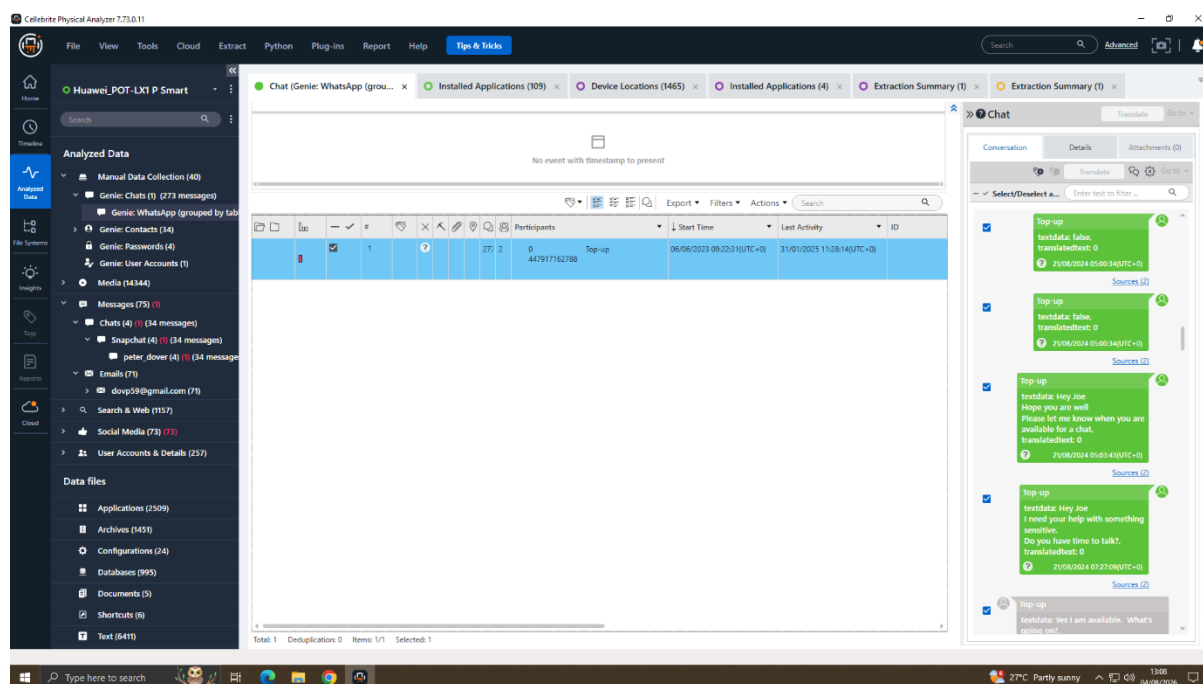


Figure 8. Initial Contact Between Emma and Joe

The recovered communication demonstrates direct contact between Emma and Joe and establishes the starting point for subsequent events. This communication established the initial connection and provided the starting point for timeline reconstruction.

6.2 Discussion of Valuable Information

Subsequent communications were analysed to determine the nature and significance of the information being discussed.

Digital Forensics Analysis

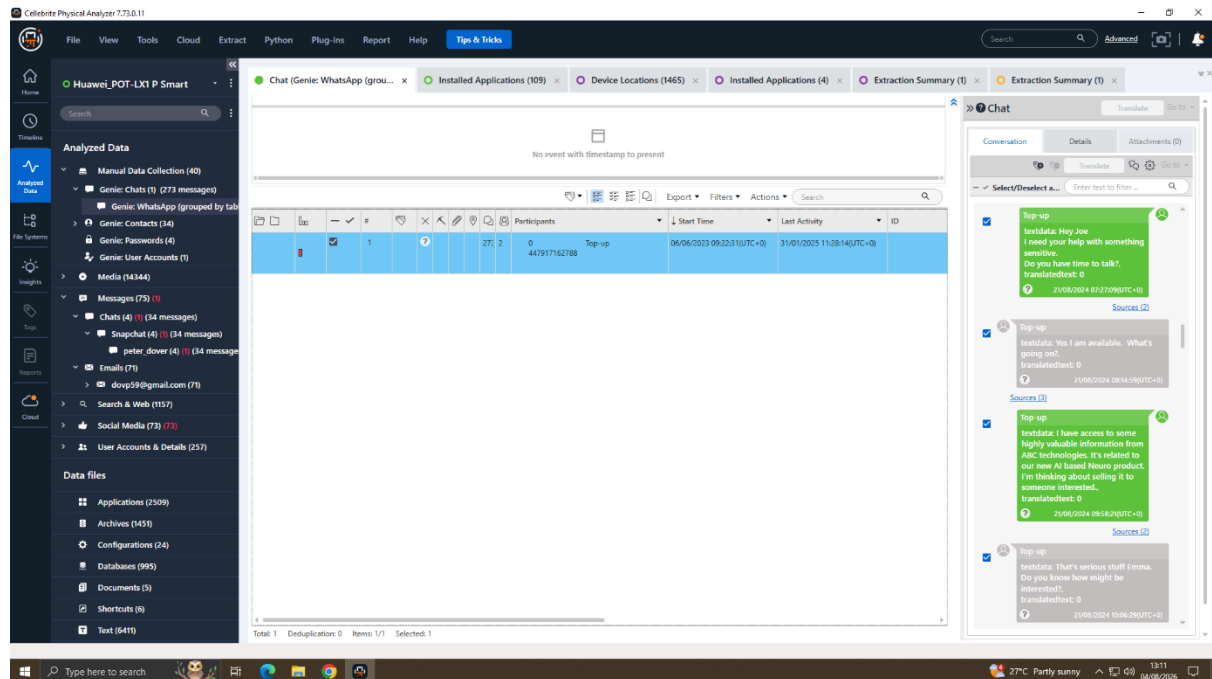


Figure 9. Communication referencing valuables

The recovered messages indicate that Emma described possessing highly valuable information associated with an AI-based product. The messages demonstrated awareness of information considered valuable by the sender.

6.3 Buyer Identification Activities

The investigation examined whether communications referenced external contacts or potential third parties.

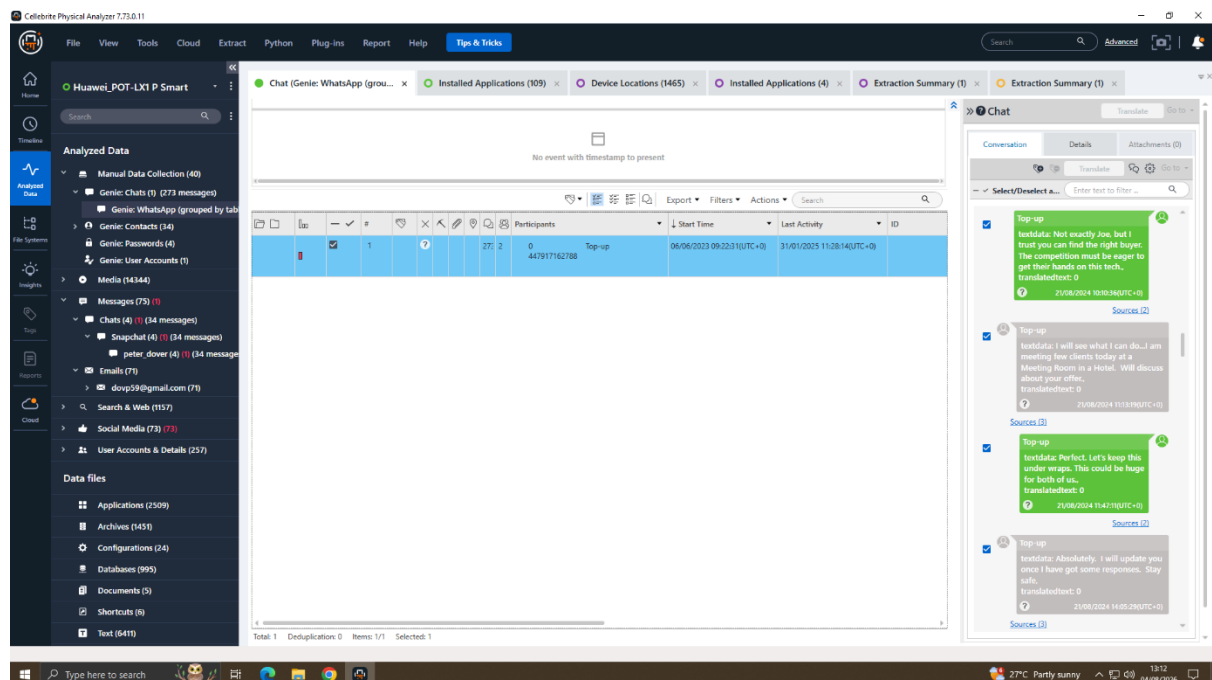


Figure 10. Search for Potential Buyers

Digital Forensics Analysis

The communication demonstrates efforts to identify parties potentially interested in obtaining the information. The recovered discussion indicated efforts to identify individuals potentially interested in the information.

6.4 Concealment and Secrecy

Communication records were also reviewed for indications of confidentiality or concealment.

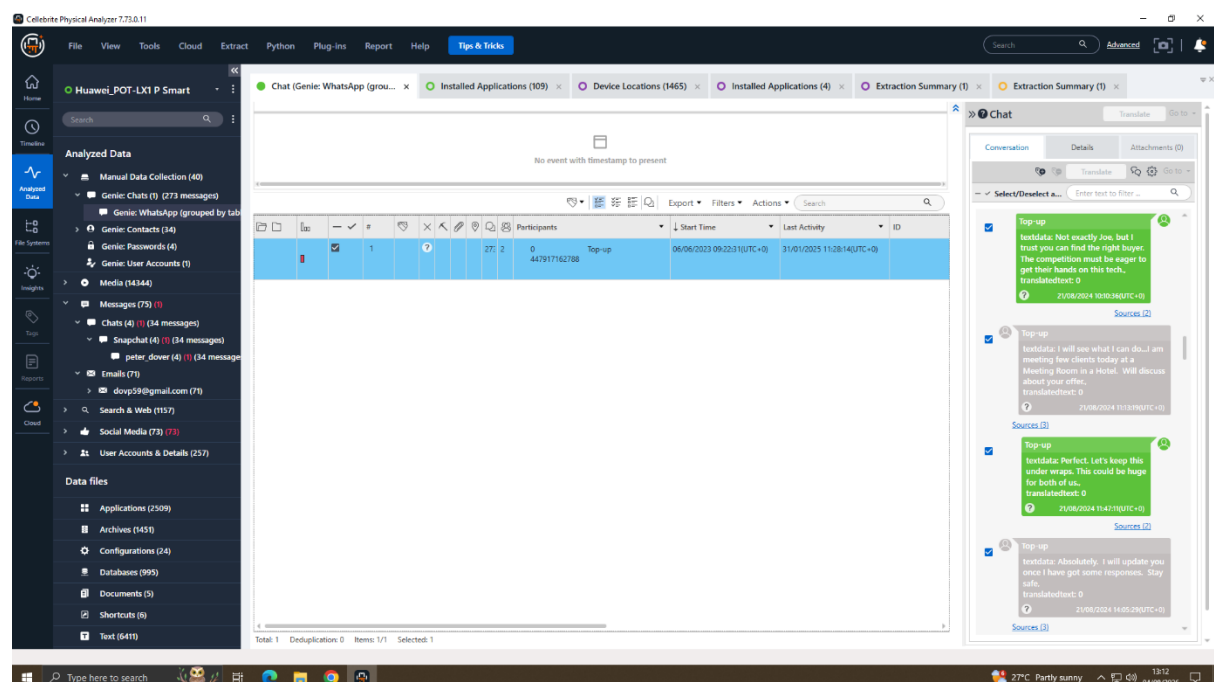


Figure 11. Confidentiality Discussion

The recovered communication includes references indicating that the activities should remain hidden from others. References to secrecy provided important context regarding the sensitivity of the discussions.

6.5 Location Coordination

Location-based artefacts were analysed to determine whether communication records could be supported by movement-related evidence.

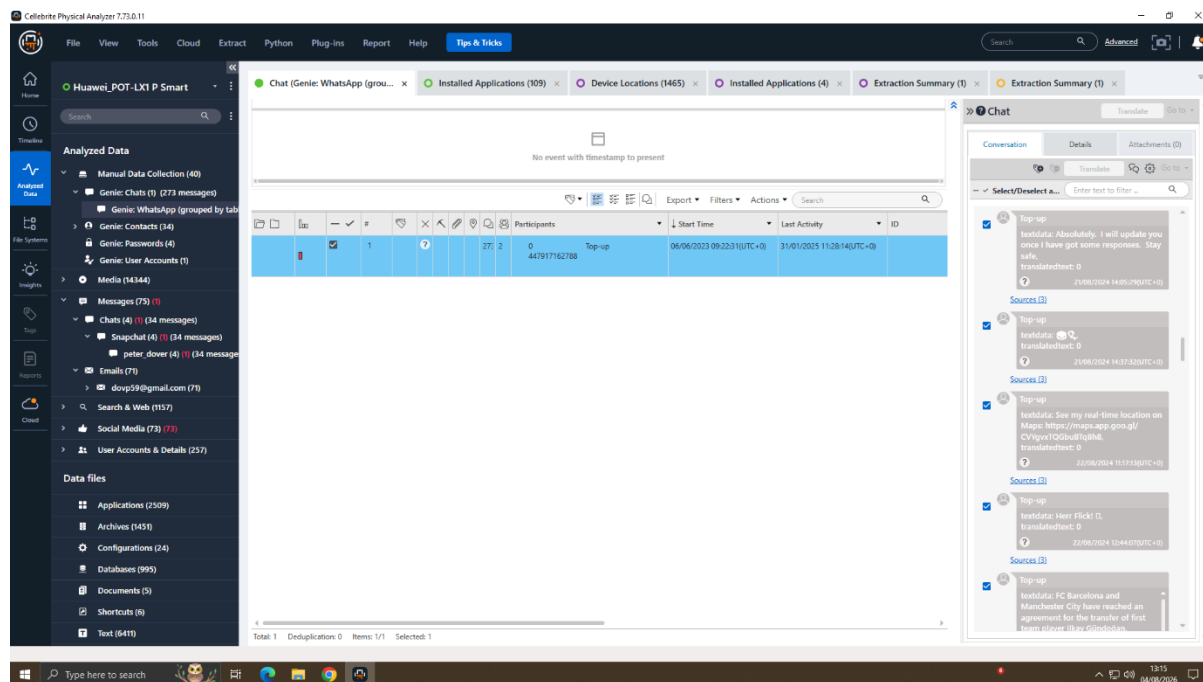


Figure 12. Location Sharing Activity

This artefact demonstrates coordination of physical meetings between involved parties. The recovered location-sharing activity demonstrated coordination between the involved parties.

6.6 Ongoing Negotiations

Additional communications revealed continued interaction over an extended period and provided insight into planning activities.

Digital Forensics Analysis

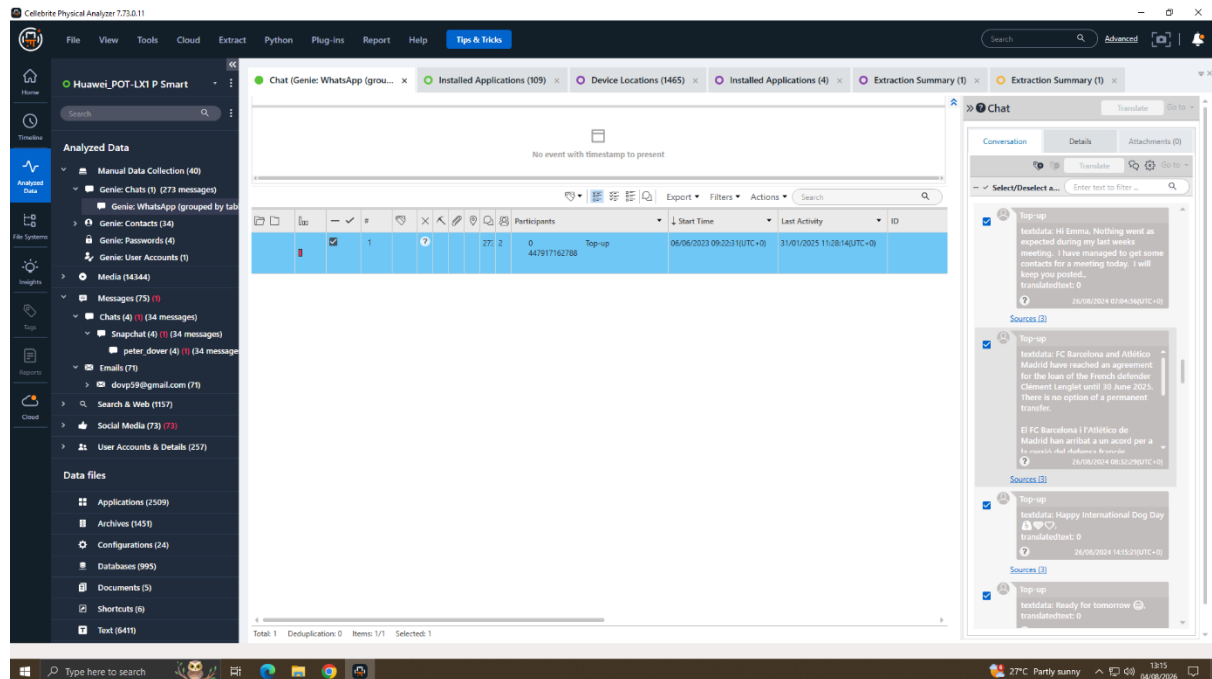


Figure 13. Follow-Up Communication Activity

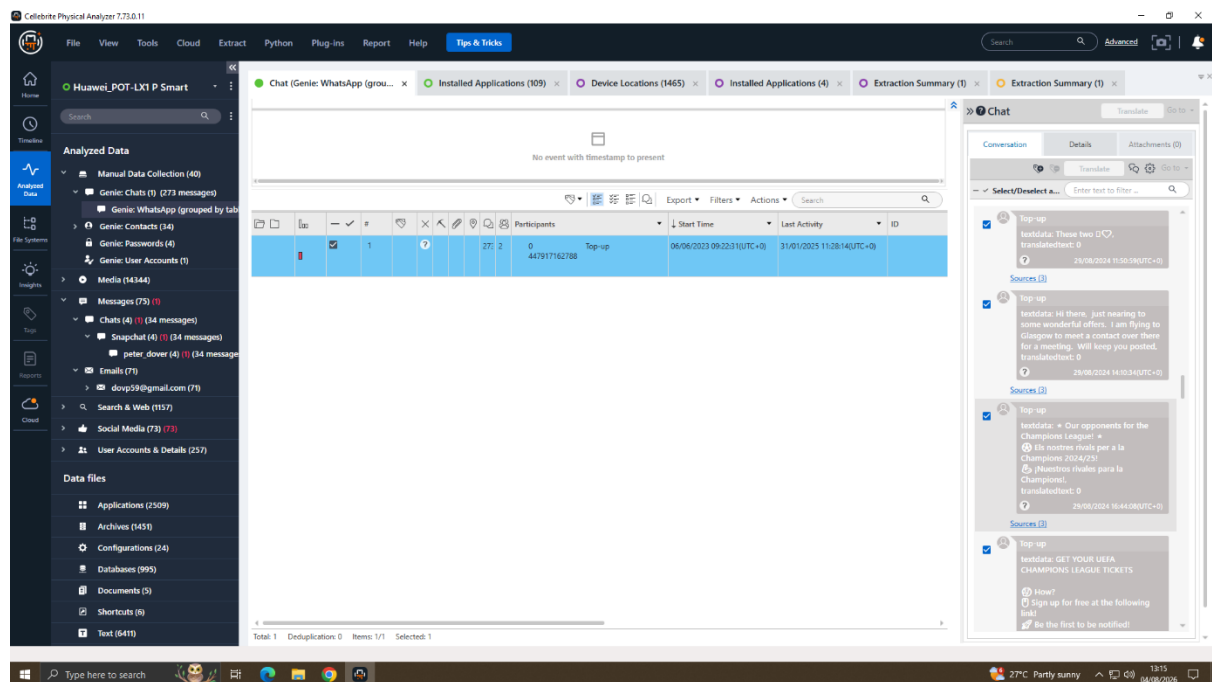


Figure 14. Glasgow Meeting Arrangements

Digital Forensics Analysis

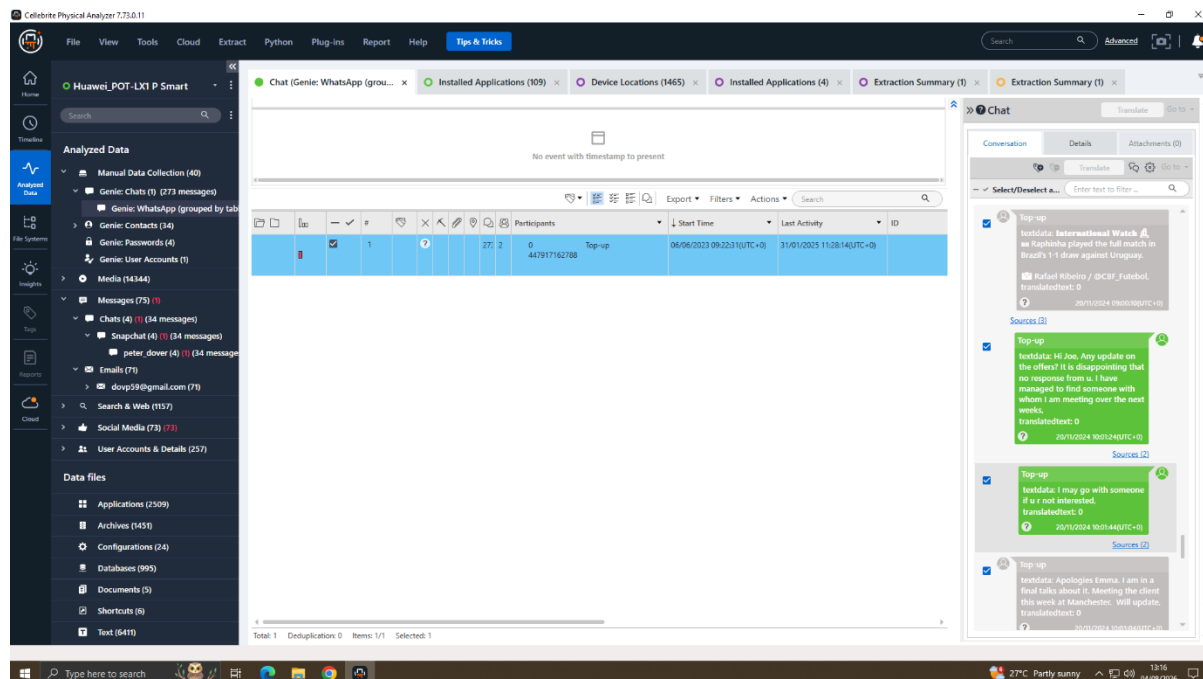


Figure 15. Manchester Meeting Discussions

The recovered communications indicate sustained discussions over an extended period and demonstrate continued efforts to arrange meetings with external parties. Collectively, the recovered messages demonstrate sustained communication and ongoing coordination efforts.

6.7 Financial Motivation

The final communication review focused on discussions that could indicate motivation for the identified activities.

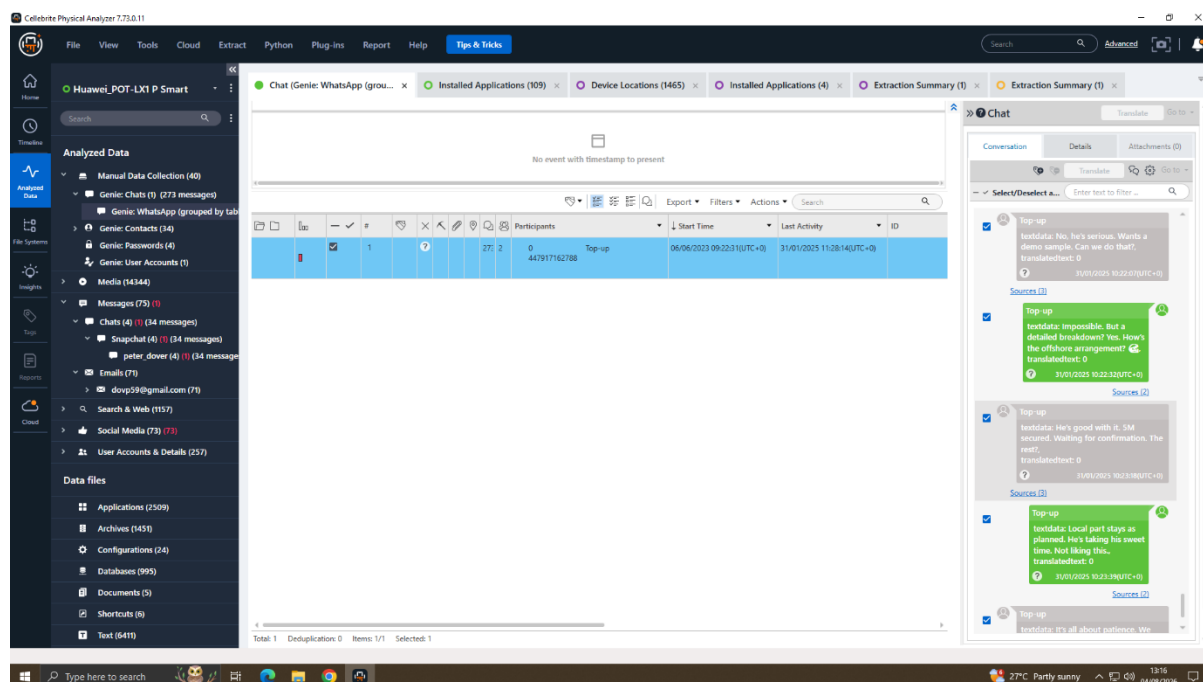


Figure 16. Discussion Relating to Information Disclosure

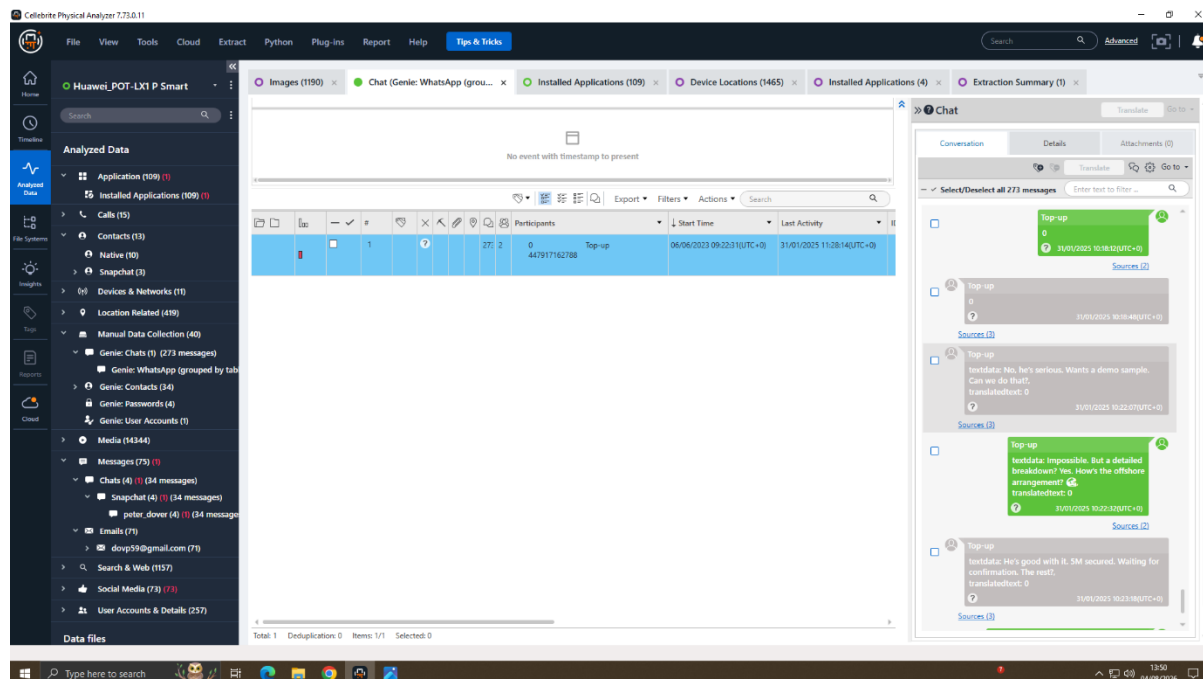


Figure 17. Offshore Arrangement Discussion

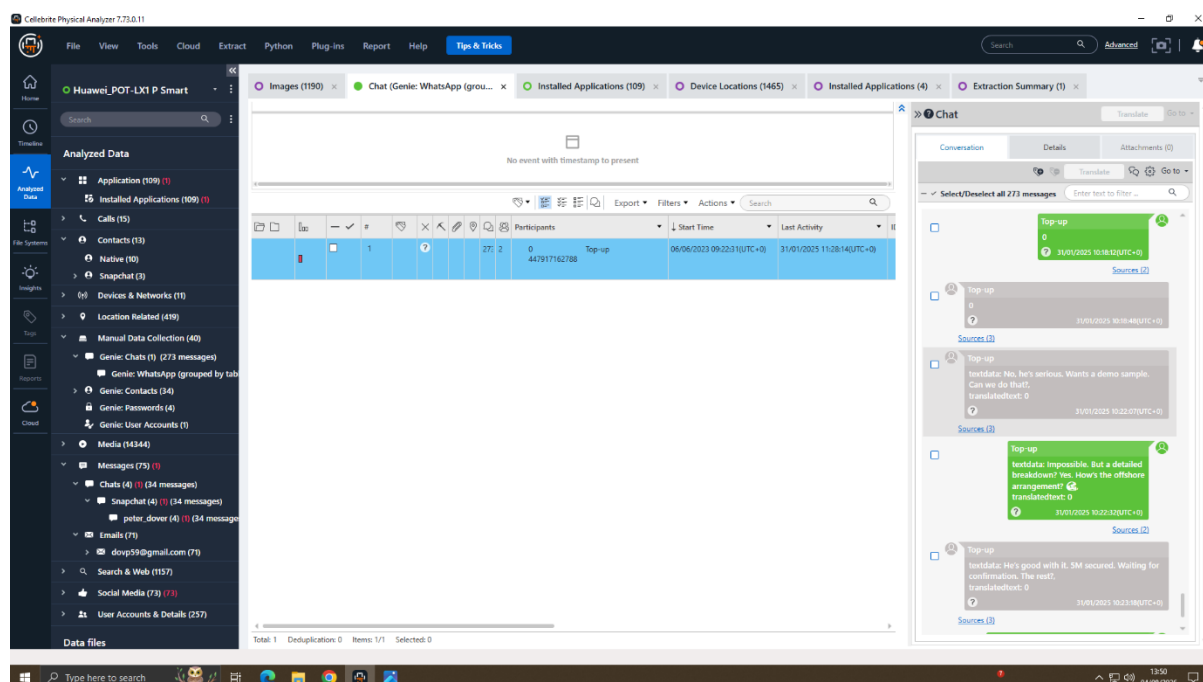


Figure 18. Financial Negotiation Discussion

The financial discussions identified within the communications suggest that commercial gain was a motivating factor behind the activities being discussed. These discussions suggest that potential financial gain may have influenced the ongoing interactions.

7. Correlation Between Digital and Physical Evidence

One of the strongest aspects of the investigation involved correlating communication artefacts with independent physical evidence recovered from the devices.

Hotel-Related Evidence

Media artefacts recovered from the devices were examined to identify evidence capable of corroborating communication records.

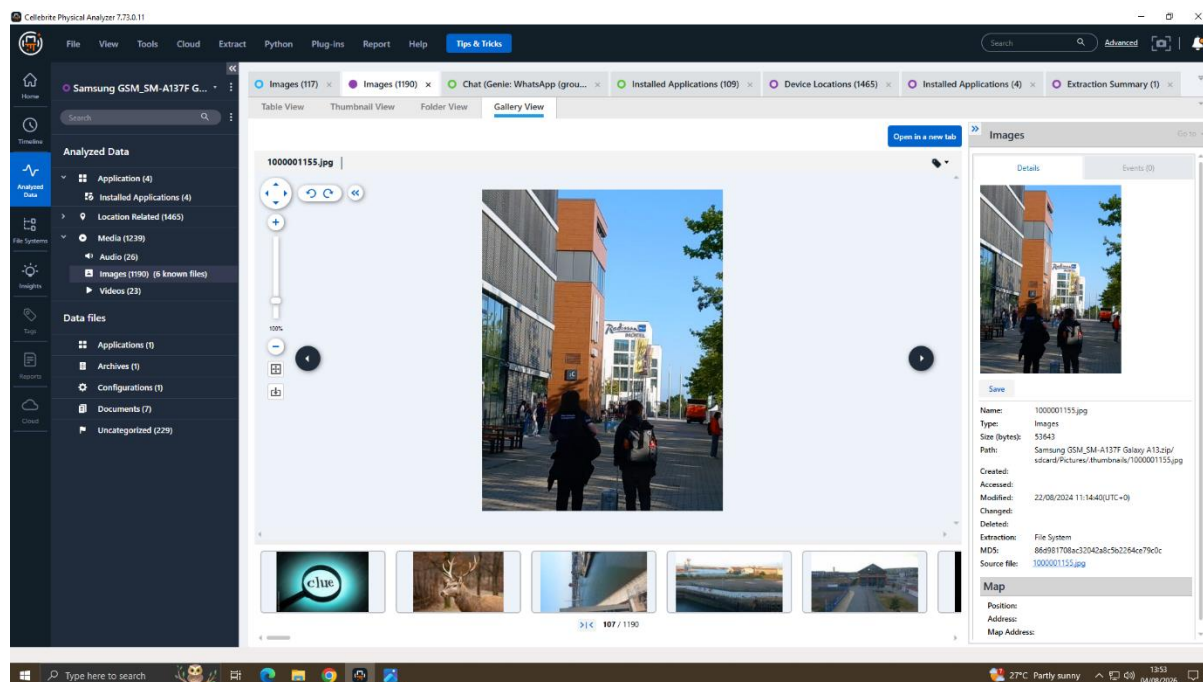


Figure 19. Hotel Photograph

The photograph provides supporting evidence for discussions involving meetings at hotel locations. The recovered image provides supporting context for meeting-related discussions identified during analysis.

Travel-related evidence was reviewed to determine whether movement records aligned with communication activity.

Digital Forensics Analysis

Glasgow Travel Evidence

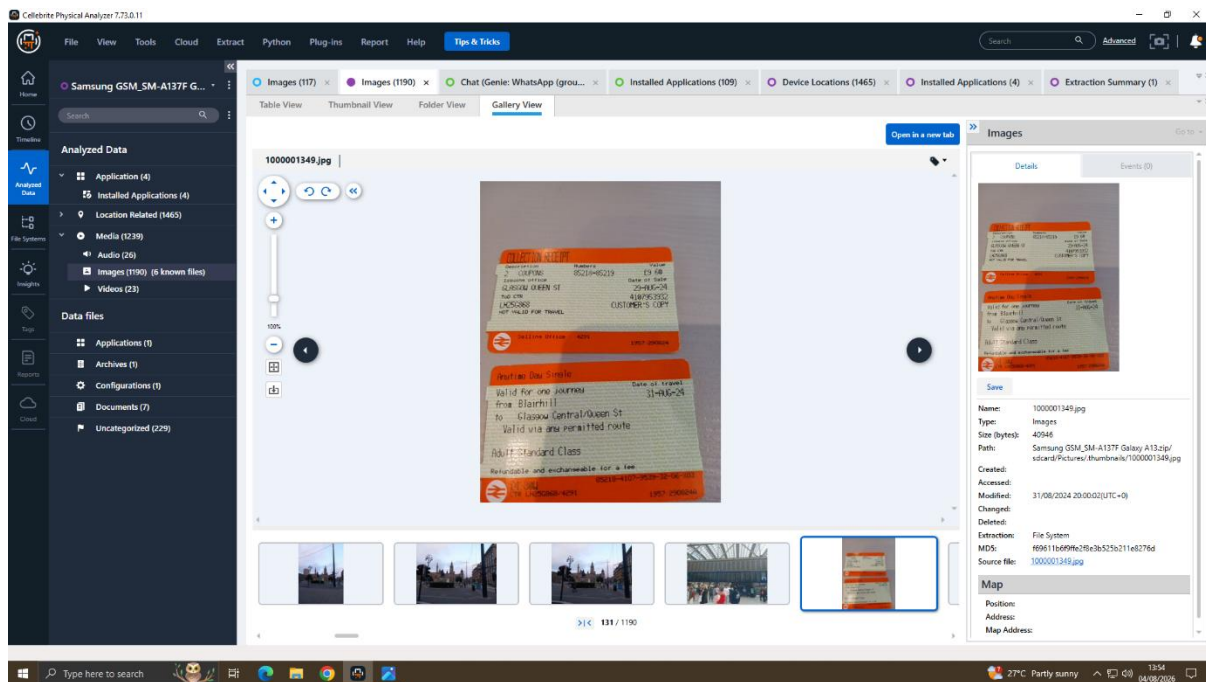


Figure 20. Glasgow Travel Ticket

The travel artefact supports the timeline reconstructed from recovered communications.

Accommodation Evidence

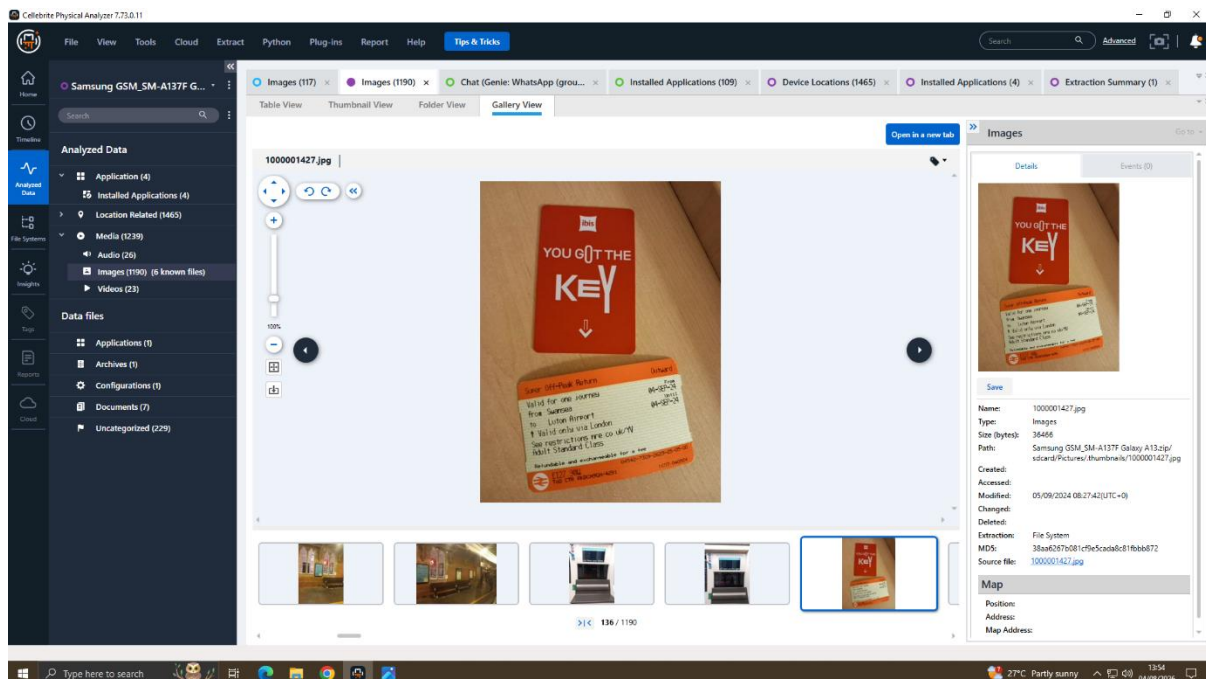


Figure 21. Manchester Travel Ticket in media

Digital Forensics Analysis

Manchester Travel Evidence

Additional transport-related artefacts were recovered during examination of media evidence.

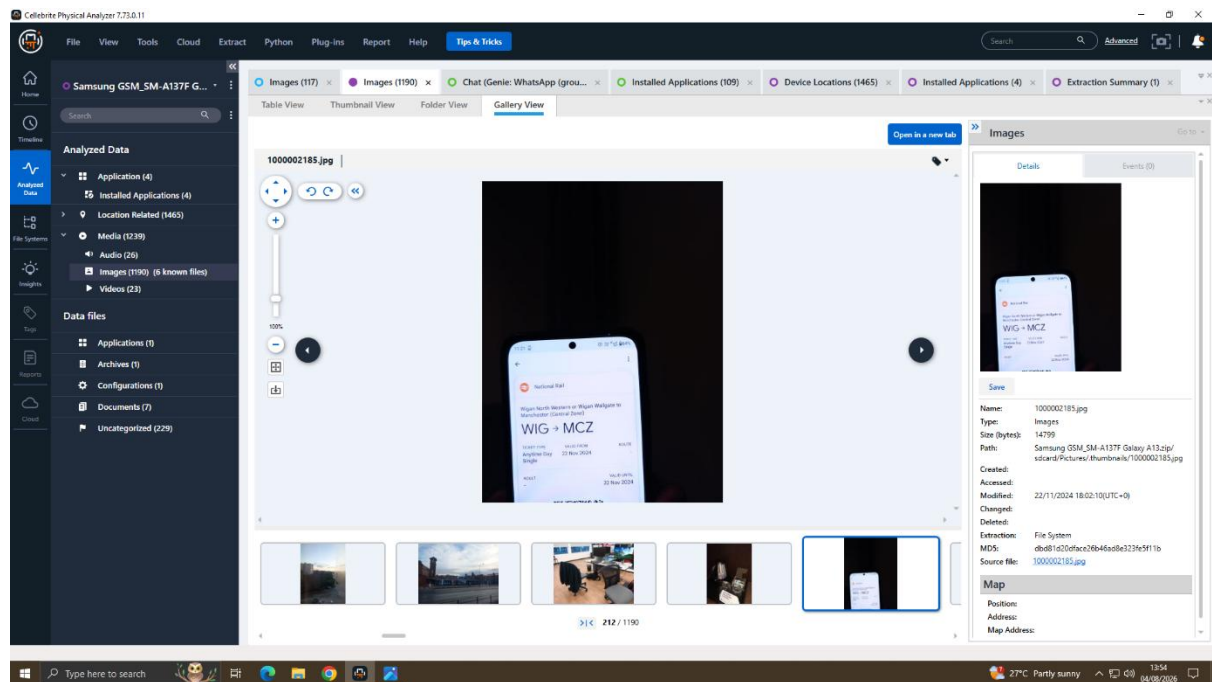


Figure 22. Manchester Travel Ticket

These records provide further support for meeting arrangements and travel activity identified in the investigation.

Communication records were compared against independently recovered artefacts to assess consistency and reliability across evidence sources.

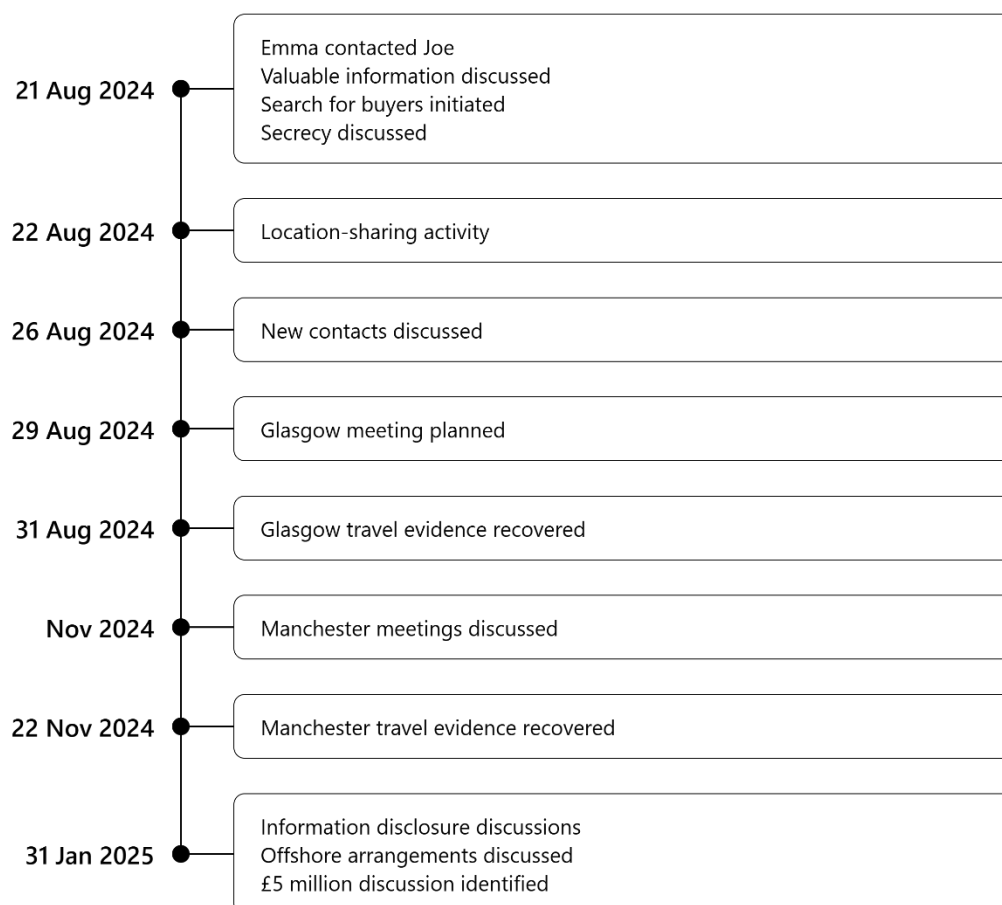
Communication Evidence	Supporting Evidence	Significance	Strength
Glasgow meeting discussion	Glasgow rail ticket	Confirms travel linked to meeting activity	High
Manchester client meeting	Manchester travel ticket	Supports external meeting arrangements	High
Hotel meeting references	Radisson Blu image	Corroborates reported meeting location	High
Negotiation discussions	Travel & accommodation artefacts	Indicates meeting preparation and attendance	Medium-High
Location sharing activity	Timeline location artefacts	Demonstrates coordination between parties	High
Buyer-search communications	Travel and hotel evidence	Supports external contact activities	High
Long-term communication pattern	Timeline artefacts	Demonstrates continuity over time	High

Table 3. Evidence Correlation Matrix

The consistency between communications and recovered travel-related artefacts significantly strengthens the reliability of the investigative findings. The correlation results demonstrate strong agreement between communications, travel records, location artefacts, and media evidence.

8. Timeline Reconstruction

Recovered artefacts were organised chronologically to reconstruct the sequence of investigative events.



The completed timeline provides a structured overview of communications, travel activity, and supporting evidence.

9. Evidential Reliability Assessment

The reliability of the investigation findings was assessed by examining the consistency, integrity, and corroborative value of all recovered evidence sources. During the examination process, multiple independent artefact categories were identified and analysed, including communication records, timeline data, location information, travel documentation, media files, and cryptographically verified forensic images. The use of multiple evidence sources reduced dependency on any single artefact and strengthened the overall reliability of the investigation findings.

Several factors contributed to the evidential reliability of this investigation:

- **Cryptographically Verified Forensic Images:** All acquired device images successfully passed SHA256 hash verification, confirming that the evidence remained unchanged throughout acquisition and analysis.
- **Recovered WhatsApp Communications:** The communication artefacts provided direct records of interactions, meeting arrangements, coordination activities, and negotiation-related discussions.
- **Timeline Artefacts:** More than 1,500 timeline artefacts were recovered and used to establish the chronological sequence of events.
- **Location and Coordination Records:** Location-sharing activities and recovered geographical artefacts provided additional support for communication records and movement patterns.
- **Travel Documentation:** Recovered rail tickets and travel-related images independently corroborated discussions relating to meetings and external contacts.
- **Hotel and Accommodation Artefacts:** Photographs of hotel locations and accommodation-related items provided supporting evidence for meeting arrangements identified within the communication data.

Cross-Validation of Evidence Sources

A significant strength of the investigation was the ability to correlate communications with independent physical artefacts. For example, discussions concerning Glasgow and Manchester meetings were supported by corresponding travel records, while hotel-related communications were reinforced by recovered hotel photographs. This cross-validation process increased confidence in the reconstructed timeline and reduced the likelihood that individual artefacts were being interpreted in isolation.

Consistency Assessment

No significant inconsistencies were identified between the recovered communications, travel artefacts, location records, and timeline data. The examined artefacts demonstrated a high degree of consistency across multiple evidence categories, indicating that the reconstructed sequence of events was supported by several independent sources.

Reliability Conclusion

Based on the successful hash verification of all forensic images, the consistency of artefacts across multiple evidence sources, and the strong correlation between communication records and supporting physical evidence, the investigation findings are considered reliable and forensically sound. The use of

independently corroborating artefacts significantly strengthens the evidential value of the investigation and supports the conclusions presented within this report [1], [2].

10. Suspect Profiling

Emma

Role Assessment

Primary Subject

Supporting Evidence

- Initiated communication.
- Referenced valuable information.
- Discussed external disclosure.
- Requested confidentiality.
- Participated in negotiation discussions.

Joe

Role Assessment

Intermediary

Supporting Evidence

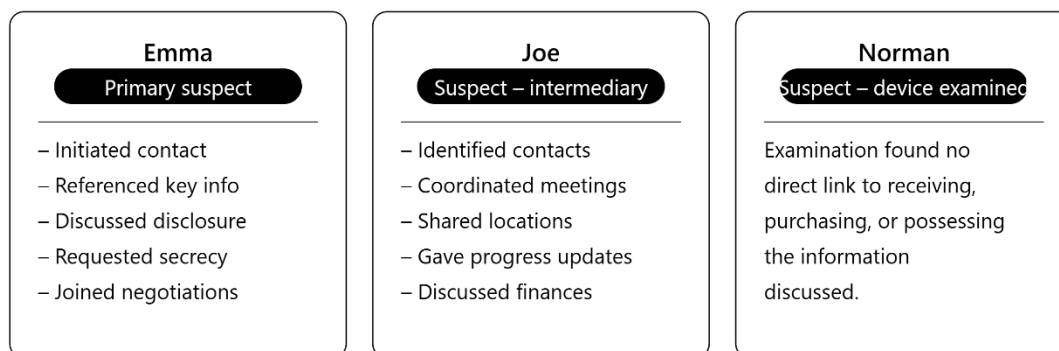
- Identified potential contacts.
- Coordinated meetings.
- Shared locations.
- Provided progress updates.
- Participated in financial discussions.

Norman

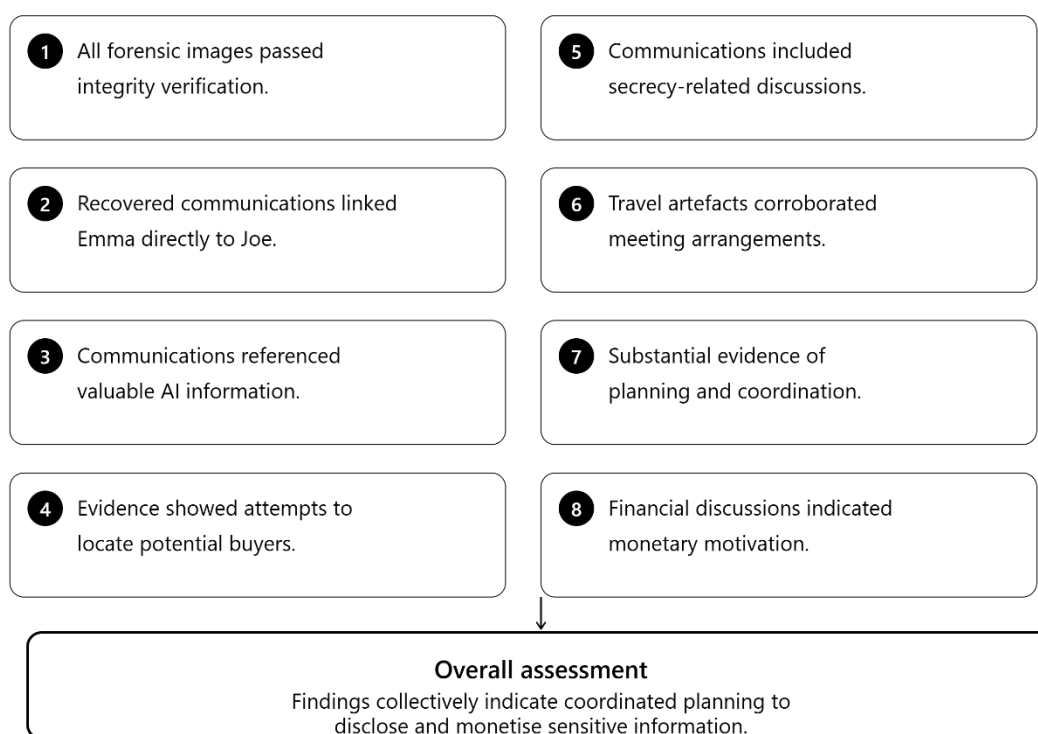
Role Assessment

Device Examined

The recovered evidence does not provide sufficient information to directly associate Norman with receiving, purchasing, or possessing the information discussed in the communications.

**Figure 23. Comparative Suspect Profiling**

11. Findings

**Figure 24. Graphical View of overall findings**

12. Conclusion

The forensic examination identified substantial evidence demonstrating communication, coordination, planning, negotiation activity, secrecy, and financial motivation relating to valuable AI-related information.

Recovered communications established that Emma and Joe maintained sustained discussions concerning potential interested parties, meeting arrangements, and proposed commercial opportunities. Independent travel artefacts, location-sharing records, and hotel-related images corroborated several of the activities identified within the communications.

Based on the available evidence, Emma appears to have acted as the primary initiator of the activities discussed, while Joe appears to have acted as an intermediary by communicating with potential external contacts and coordinating meetings.

The overall evidence supports findings relating to planning, coordination, negotiation activities, and attempts to identify external parties interested in confidential information.

13. Recommendations

Recommendations for Enterprise

- Implement Data Loss Prevention (DLP) controls.
- Strengthen insider-threat monitoring.
- Restrict access to sensitive intellectual-property repositories.
- Conduct additional employee awareness training.
- Review privileged-access assignments.

Recommendations for Law Enforcement

- Examine cloud-based accounts associated with involved devices.
- Obtain telecommunications records where appropriate.
- Investigate associated financial records.
- Conduct interviews with identified individuals.
- Continue monitoring for additional supporting evidence.

References

- [1] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 4th ed. London, UK: Academic Press, 2020.
- [2] K. Kent, S. Chevalier, T. Grance, and H. Dang, *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication 800-86. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2022.
- [3] National Institute of Standards and Technology (NIST), *Security and Privacy Controls for Information Systems and Organizations*, NIST SP 800-53 Rev. 5. Gaithersburg, MD, USA, 2023.

- [4] Cellebrite, *Mobile Forensics Fundamentals Guide*. Petah Tikva, Israel: Cellebrite Digital Intelligence, 2024.
- [5] OpenText, *EnCase Forensic Investigator User Guide*. Waterloo, ON, Canada: OpenText Corporation, 2024.
- [6] AccessData, *FTK Imager User Guide*. Lindon, UT, USA: AccessData, 2023.
- [7] B. Carrier, *File System Forensic Analysis*. Boston, MA, USA: Addison-Wesley Professional, 2021.
- [8] S. Garfinkel, "Digital Forensics Research: The Next Decade," *Digital Investigation*, vol. 42, pp. 1-14, 2023.
- [9] M. Rogers and P. Seigfried-Spellar, *Digital Forensics and Investigations: People, Process, and Technologies to Defend the Enterprise*. New York, NY, USA: McGraw-Hill Education, 2023.
- [10] ENISA, *Threat Landscape Report 2025*. Athens, Greece: European Union Agency for Cybersecurity, 2025.
- [11] INTERPOL, *Global Cybercrime Trend Report 2024*. Lyon, France: INTERPOL Publications, 2024.
- [12] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2025*. The Hague, Netherlands: Europol, 2025.
- [13] IBM Security, *Cost of a Data Breach Report 2025*. Armonk, NY, USA: IBM Corporation, 2025.
- [14] Verizon, *2025 Data Breach Investigations Report*. New York, NY, USA: Verizon Enterprise Solutions, 2025.
- [15] Microsoft, *Microsoft Digital Defense Report 2025*. Redmond, WA, USA: Microsoft Corporation, 2025.
- [16] Check Point Research, *Cyber Security Report 2025*. Tel Aviv, Israel: Check Point Software Technologies, 2025.
- [17] CrowdStrike, *Global Threat Report 2025*. Austin, TX, USA: CrowdStrike, 2025.
- [18] Cisco Systems, *Cybersecurity Readiness Index 2025*. San Jose, CA, USA: Cisco Systems, 2025.
- [19] A. Martini and K. K.-R. Choo, "Cloud Forensics: Challenges and Opportunities," *Digital Investigation*, vol. 36, pp. 112-125, 2022.
- [20] I. Ahmed, Y. Ruan, H. Shehab, and E. Bertino, "Cloud Forensics: Challenges and Future Directions," *IEEE Security & Privacy*, vol. 21, no. 2, pp. 78-85, 2023.