

Module: Digital Forensics Analysis
MSc Cybersecurity and Digital Forensics

Submitted By-

Name: MD. Mashrurul Haque

ID: 2435257

Contents

List of Figures.....	3
Task - 1: Research Report Digital Forensics	4
Introduction	4
Current state of the field: tools, features, and capabilities	4
Intersection of digital forensics and cybersecurity	4
Emerging trends in digital forensics	5
Key challenges in digital forensics	5
National and international job market	5
Conclusion	6
References	6
Task – 2	8
2.1 Device Collection	8
2.2 Case Background	10
2.3 Evidence Inventory	11
2.4 Methodology	11
2.5 Findings	13
2.5.1 Communication evidence involving Emma and Joe	13
2.5.2 Buyer-side communication involving Norman.....	19
2.5.3 Corroborative location and travel artefacts.....	20
2.5.4 Call log Analysis.....	23
2.6 Suspect role assessment	23
2.7 Conclusion	23
2.8 Recommendations	24

List of Figures

Figure 1. Device connected to the computer using Cellebrite adapter -----	08
Figure 2. Device detection and identification in Cellebrite UFED -----	08
Figure 3. UFED extraction workflow and content selection -----	09
Figure 4. Successful extraction summary in Cellebrite UFED -----	10
Figure 5. Huawei POT-LX1 device hash verification -----	11
Figure 6. Nokia C2 device hash verification -----	12
Figure 7. Samsung Galaxy A13 device hash verification -----	12
Figure 8. Note 14 device hash verification -----	13
Figure 9. Contact artefact identifying Joe Marsh within Cellebrite Physical Analyzer -----	14
Figure 10. Initial WhatsApp communication in which Emma initiates a sensitive discussion --	15
Figure 11. Emma’s disclosure of access to highly valuable AI-related information -----	16
Figure 12. Emma instructs Joe to locate a suitable buyer -----	17
Figure 13. Message indicating travel to Glasgow for a meeting with a contact -----	18
Figure 14. Discussion of controlled disclosure and offshore payment structure -----	19
Figure 15. Message reflecting structured financial negotiation -----	20
Figure 16. Buyer-side communication linking Norman to the planned transaction-----	21
Figure 17. Buyer-side discussion of staged blueprint release and offshore payment -----	22
Figure 18. Geo-tagged image placing a device at a hotel during the relevant meeting period --	23
Figure 19. Geo-tagged image placing a device in Glasgow during the negotiation period -----	24
Figure 20. Travel-related image artefact showing train ticket photographs -----	25
Figure 21. Call Log of Emma’s Phone -----	23

Task - 1: Research Report Digital Forensics

Introduction

Digital forensics is the discipline concerned with identifying, preserving, examining, interpreting, and presenting digital evidence in a technically reliable and legally defensible way. In practice, the field now extends well beyond traditional hard-disk analysis. Investigations routinely span smartphones, cloud platforms, memory artefacts, network traces, multimedia, Internet of Things (IoT) devices, and application ecosystems. A ten-year review of DFRWS Europe publications shows how the field has expanded into device forensics, artefact forensics, multimedia, memory, and network forensics, reflecting the fact that modern evidence is distributed across many technologies rather than stored in one place [1].

Current state of the field: tools, features, and capabilities

The current state of digital forensics is shaped by a tension between growing technical capability and growing technical resistance. On the capability side, specialist tools such as Cellebrite, Magnet, FTK, EnCase, Autopsy, Volatility, and cloud-focused collection frameworks allow investigators to acquire and analyse messages, call logs, browser artefacts, file metadata, memory structures, deleted fragments, and timeline data across multiple platforms. Official NIST mobile device forensic testing specifications illustrate the range of expected capabilities, including extraction, interpretation, and reporting of time-stamped mobile artefacts and application-related activity [2]. NIST's wider Computer Forensics Tool Testing programme also exists because forensic tools must be evaluated systematically rather than trusted blindly [3]. This is an important point academically and professionally: digital forensic software is powerful, but it is never infallible.

At the same time, the field faces more technical barriers than before. Strong encryption, secure enclaves, locked bootloaders, multi-factor authentication, rapid operating-system updates, and the migration of evidence into cloud services all restrict visibility. Recent mobile-forensics literature stresses that no single tool provides complete coverage and that investigators often need multiple tools, validation steps, and careful interpretation to avoid over-claiming what the artefacts prove [4]. The modern state of the field is therefore not simply "better tools"; it is better tools operating in a harder environment.

Intersection of digital forensics and cybersecurity

Digital forensics and cybersecurity are now deeply intertwined. Traditionally, cybersecurity focused on prevention and defence, while forensics focused on post-incident investigation and court presentation. That separation is no longer realistic. In modern practice, forensic methods are central to incident response, threat hunting, insider-threat investigations, malware analysis, ransomware triage, and breach reconstruction. When an organization suffers a cyber incident, forensic analysis helps answer the questions that defensive tools alone cannot fully resolve what happened, how it happened, what systems were affected, what data may have been exfiltrated, and which artefacts can support remediation, disciplinary action, or prosecution.

The 2024 DFPulse practitioner survey is useful here because it shows that forensic practitioners operate in environments shaped by live operational pressures, diverse technologies, and a constant need to make research relevant to real investigations [5]. This demonstrates that digital forensics is

not a detached laboratory exercise. It is a practical cybersecurity capability that supports evidencebased decision-making. In SOC and incident-response settings, this intersection is especially important because forensic findings can confirm attacker behavior, validate containment steps, and provide the factual basis for lessons learned after an incident.

Emerging trends in digital forensics

One of the most important emerging trends is cloud forensics. As organizations move data, collaboration, identity, and logging into cloud environments, investigators increasingly rely on provider-generated logs, API-based collection, and distributed evidence sources. Recent research on cloud digital forensics argues that the problem is no longer limited to tools; it is also about evidence preservation, attribution, validation, and cross-jurisdictional access in virtualized and multi-tenant environments [6].

A second major trend is IoT forensics. Smart devices generate evidence across embedded hardware, companion mobile apps, edge gateways, and cloud platforms. A recent review of IoT forensics highlights that this heterogeneity creates both investigative opportunity and complexity because conventional forensic workflows do not map neatly onto IoT ecosystems [7]. As a result, investigators increasingly need hybrid thinking that combines device, cloud, app, and network evidence.

A third trend is the growing use of artificial intelligence, especially large language models, in forensic workflows. Recent scholarship suggests that LLMs may support triage, summarization, search, and review of large volumes of artefacts [8]. However, the same literature warns that explainability and reproducibility remain critical. Forensics is an evidential discipline, so any AIassisted output must still be verified by a human investigator. The likely future direction is augmentation rather than replacement: AI can speed analysis, but human judgment remains central.

Key challenges in digital forensics

Several major challenges continue to define the field. The first is scale. Investigators are now dealing with far more data, more devices per case, and more sources of evidence than in earlier forensic practice. DFPulse 2024 highlights the practical strain this creates for investigators, especially when academic outputs are not always aligned with operational needs [5]. The second challenge is trust and validation. Since forensic findings can influence criminal liability, civil claims, and organizational sanctions, methods and tools must be defensible. NIST's testing work exists precisely because software limitations can shape investigative outcomes [2], [3].

The third challenge is encryption and platform security. Stronger privacy protections are valuable for users, but they also reduce evidential access for lawful investigations. Mobile environments are a particularly strong example of this tension [4]. The fourth challenge is jurisdiction and legality, especially in cloud contexts where data may be distributed across multiple countries and controlled by third-party providers [6]. A final challenge is skills. The field needs professionals who understand both technical artefacts and evidential reasoning. That combination is harder to develop than narrow tool familiarity, which is one reason the profession still reports capability gaps.

National and international job market

The job market for digital-forensics-related skills remains strong, although the roles are often embedded inside wider cybersecurity, incident response, e-discovery, and investigative functions. In

the UK, the Department for Science, Innovation and Technology reported an average of 2,698 core cybersecurity job postings per month in 2024, with a median salary of GBP55,000, while also noting continuing skills shortages [9]. Although not all these roles are labelled "digital forensics", the report is relevant because forensic expertise is increasingly required in cyber investigation, insider-threat response, and incident management. UK career guidance also continues to describe forensic computer analysis as an area with good prospects due to sustained demand for organizations that need to investigate security incidents and evidential misuse of technology [10].

Internationally, the outlook is also favorable. In the United States, the Bureau of Labor Statistics projects 29% growth for information security analysts from 2024 to 2034, with around 16,000 openings per year [11]. Again, this is broader than pure forensic work, but it matters because modern digital-forensics capability is frequently embedded inside security analyst, incident responder, DFIR, and cyber investigator roles. At the global level, ISC2 reported a cybersecurity workforce of 5.5 million professionals in 2024 alongside a workforce gap of 4.8 million, showing that demand for security-related expertise remains high worldwide [12]. For postgraduate students, this means digital forensics is valuable both as a specialist in its own right and as a pathway into adjacent areas such as SOC analysis, cyber investigations, incident response, and threat intelligence.

Conclusion

Digital forensics is now a mature but rapidly evolving discipline that sits at the intersection of technology, investigation, and cybersecurity operations. Its core purpose remains the same: to produce trustworthy explanations of digital events. However, the environment in which it operates has become far more complex. Investigators now work across mobile, cloud, IoT, and AI-influenced ecosystems where evidence is distributed, encrypted, fast-changing, and often legally complicated. The future of the field will depend not only on better tools, but also on better validation, clearer standards, stronger practitioner-researcher alignment, and professionals who can combine technical skill with evidential discipline. In that sense, digital forensics is not just about recovering data; it is about producing reliable knowledge from increasingly complex digital environments.

References

- [1] F. Breiting, J.-N. Hilgert, C. Hargreaves, J. Sheppard, R. Overdorf and M. Scanlon, "DFRWS EU 10-year review and future directions in digital forensic research," *Forensic Science International: Digital Investigation*, vol. 48, 2024. DOI: 10.1016/j.fsidi.2023.301685. [\[Link\]](#)
- [2] National Institute of Standards and Technology, "Mobile Device Forensic Tool Test Specification v3.3," Jan. 2025. [\[Link\]](#)
- [3] National Institute of Standards and Technology, "Computer Forensics Tool Testing Program (CFTT)," NIST. [\[Link\]](#)
- [4] M. N. Rouf and M. J. Hossain, "Mobile Forensics: Investigation and Tools," *International Journal of Computer Trends and Technology*, vol. 73, no. 6, 2025. [\[Link\]](#)
- [5] C. Hargreaves et al., "DFPulse: The 2024 digital forensic practitioner survey," *Forensic Science International: Digital Investigation*, 2024. [\[Link\]](#)

- [6] A. W. Malik, D. S. Bhatti, T. Park, H. U. Ishtiaq, J. Ryou and K.-I. Kim, “Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges,” *Sensors*, vol. 24, no. 2, 2024. [\[Link\]](#)
- [7] A. A. Ahmed et al., “IoT Forensics: Current Perspectives and Future Directions,” *Sensors*, vol. 24, no. 16, 2024. [\[Link\]](#)
- [8] M. Chernyshev et al., “Large language models in digital forensics: capabilities, opportunities, and risks,” *Forensic Science International: Digital Investigation*, 2026. [\[Link\]](#)
- [9] UK Department for Science, Innovation and Technology, “Cyber security skills in the UK labour market 2025,” 2026. [\[Link\]](#)
- [10] Prospects, “Forensic computer analyst,” 2026. [\[Link\]](#)
- [11] U.S. Bureau of Labor Statistics, “Information Security Analysts,” *Occupational Outlook Handbook*, 2025. [\[Link\]](#)
- [12] ISC2, “2024 Cybersecurity Workforce Study,” 2024. [\[Link\]](#)

Task – 2

2.1 Device Collection



Figure 1. Device connected to the computer using Cellebrite adapter

The figure above shows that Honor 400 pro connected to the computer via Cellebrite adapter. The adapter has two cables, one is power and another one is data.

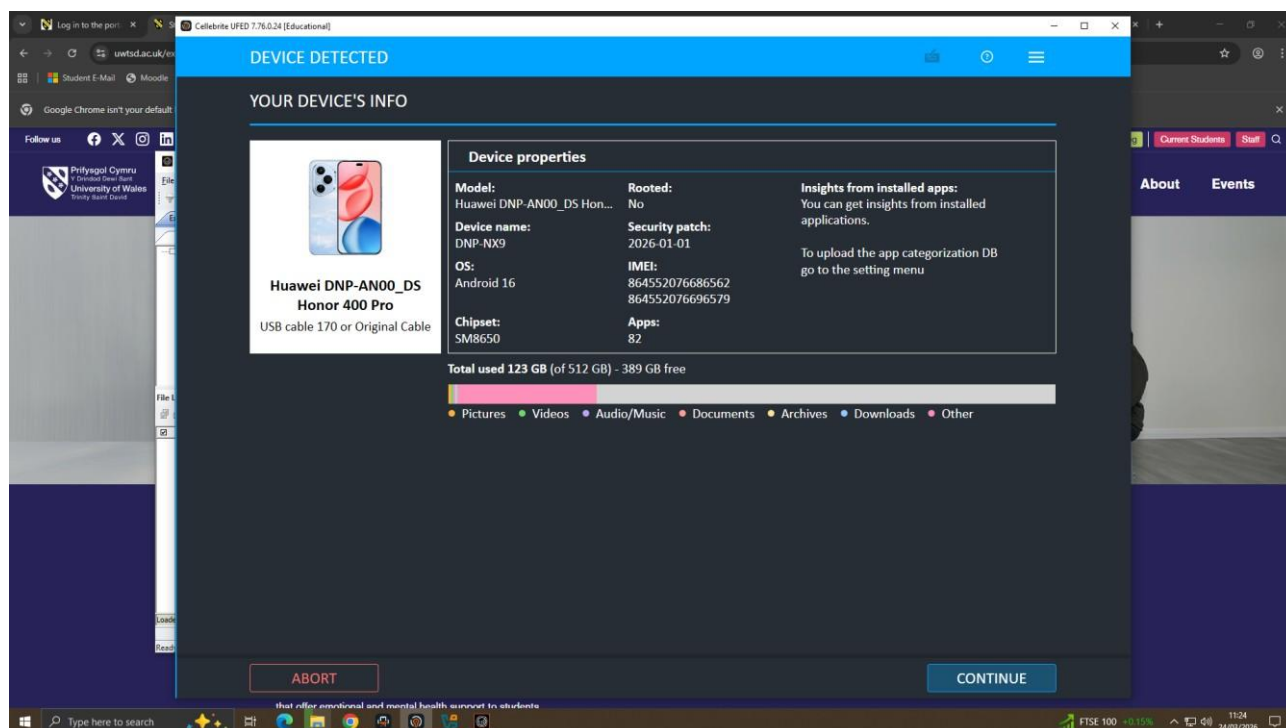


Figure 2. Device detection and identification in Cellebrite UFED

This figure shows the examined mobile device being detected within Cellebrite UFED. It demonstrates that the acquisition process was conducted using an industry-standard forensic tool and that the device was successfully recognized before data extraction commenced.

Figure 3 supports the methodology section by showing that the acquisition was structured and category-based rather than ad hoc.

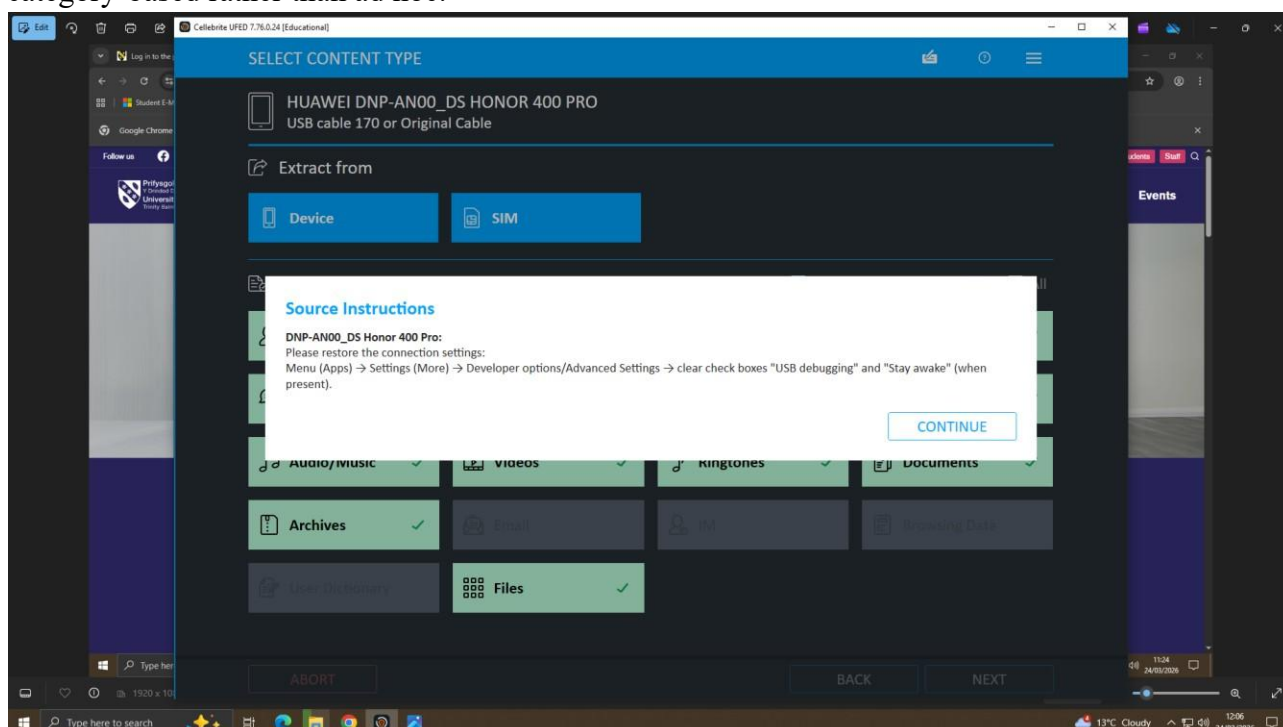


Figure 3. UFED extraction workflow and content selection

This figure shows the extraction workflow used to configure forensic acquisition. It demonstrates the categories of artefacts available for acquisition and supports the methodological reliability of the evidence collection process.

Figure 4 confirms that the extraction was completed successfully and that relevant data classes were available for analysis.

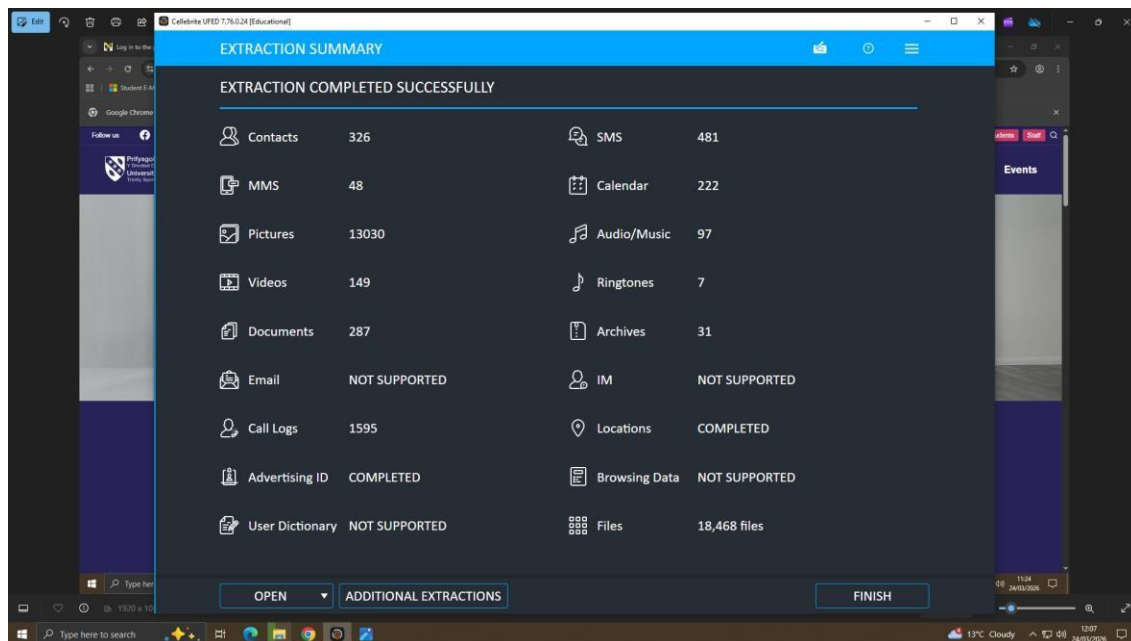


Figure 4. Successful extraction summary in Cellebrite UFED

This figure confirms that the extraction process was completed successfully and that multiple categories of evidence were acquired, including contacts, messages, media, documents, call logs, and locations. This provides the evidential foundation for the later analysis performed in Physical Analyzer.

2.2 Case Background

Quantum Tech reported unauthorized access to its proprietary patent database, specifically the AI chip design patent identified as QT-AI-2025. Initial internal findings identified Emma, a recently appointed senior engineer, as the primary suspect. The allegation was that Emma attempted to steal and sell confidential technical information to a competitor through Joe, who acted as an intermediary, with Norman identified as the intended buyer.

The purpose of this examination was to assess the available digital artefacts and determine whether they support the allegation of attempted corporate espionage. The analysis focused on acquisition evidence, communication artefacts, supporting travel and location traces, and file-related artefacts capable of showing intent, coordination, and role allocation. In keeping with forensic reporting principles, the conclusions in this report are confined to the artefacts reviewed and do not go beyond what can reasonably be supported by the evidence.

2.3 Evidence Inventory

The material consisted primarily of four images of different devices including Huawei POT – LX1, Nokia C2, Samsung Galaxy A13 and Note 14. The comprised screenshots from Cellebrite Physical Analyzer showing contacts, message threads, social-media chat content, location artefacts, image metadata, and a document archive artefact.

The screenshots are important because they demonstrate that the examined data was obtained through an industry-standard forensic workflow rather than through informal manual browsing. The full chain-of-custody forms and visible hash values were shown in the screenshot set, continuity-of-evidence principles remain central. The proper forensic position is that original devices should be preserved, extraction outputs should be verified through cryptographic hashes where available, and analysis should be performed on acquired forensic data rather than on the live original device.

2.4 Methodology

The investigation followed a structured forensic process. First, forensic acquisition was performed using Cellebrite Physical Analyzer (PA). A physical extraction (the provided images) was loaded into the tool to reconstruct the file system.

Second, to ensure chain of custody and evidentiary integrity, a **hash verification** (MD5/SHA-256) was conducted immediately after the data was ingested. It was to confirm that the digital evidence remained bit-for-bit identical to the original extraction and had not been modified during the analysis phase.

Lastly, the **Cellebrite App Genie** was executed to enhance the discovery of artifacts. This tool utilized heuristic analysis to identify and decode data from third-party applications that were not covered by standard decoding scripts. This ensured a more comprehensive view of user activity, specifically targeting communication logs and application-specific databases that often contain the most relevant forensic artifacts.

Figure 5-8 is included to document the acquisition stage and to demonstrate that the devices were first identified within Cellebrite Physical Analyzer (PA).



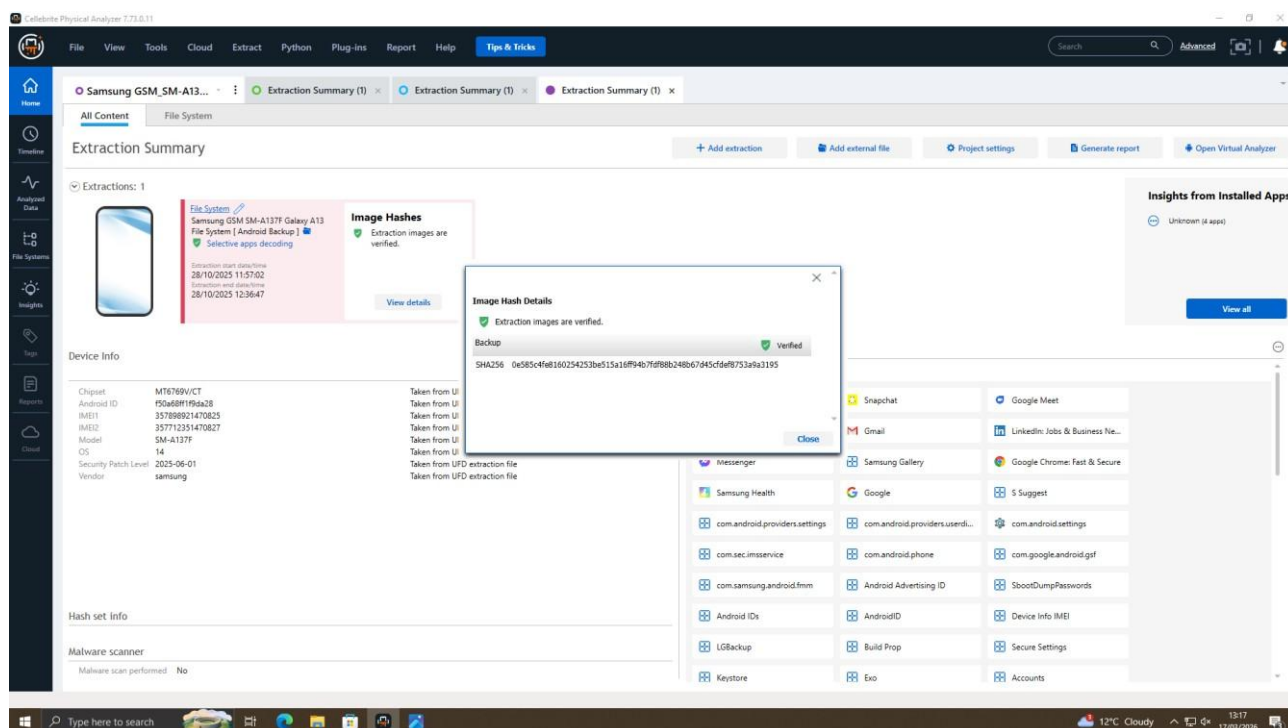


Figure 7. Samsung Galaxy A13 Device Hash Verification

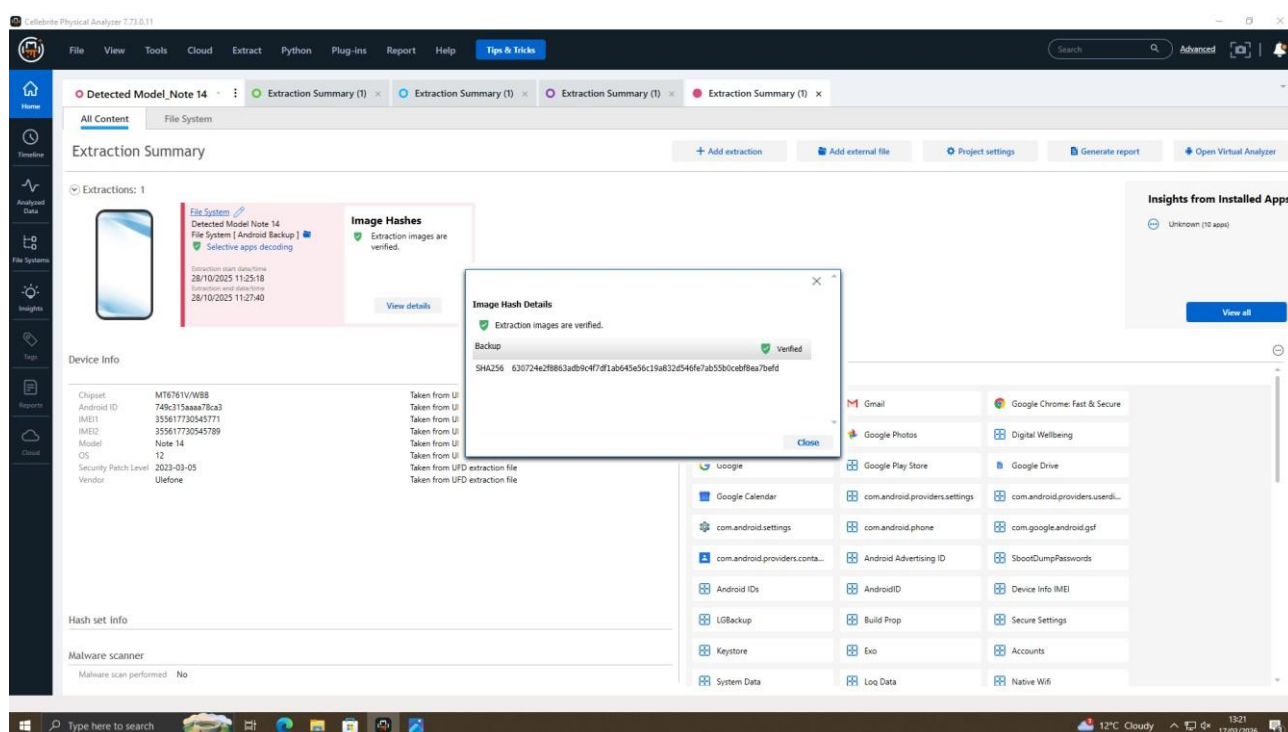


Figure 8. Note 14 Device Hash Verification

2.5 Findings

2.5.1 Communication evidence involving Emma and Joe

The earliest relevant communication appeared on 21 August 2024, when Emma contacted Joe and asked for help with “something sensitive.” This opening message is important because it shows that Emma initiated the contact and framed the matter as confidential from the outset.

Before interpreting the message content, it is helpful to establish attribution. Figure 9 identifies the Joe Marsh contact record associated with the communication thread.

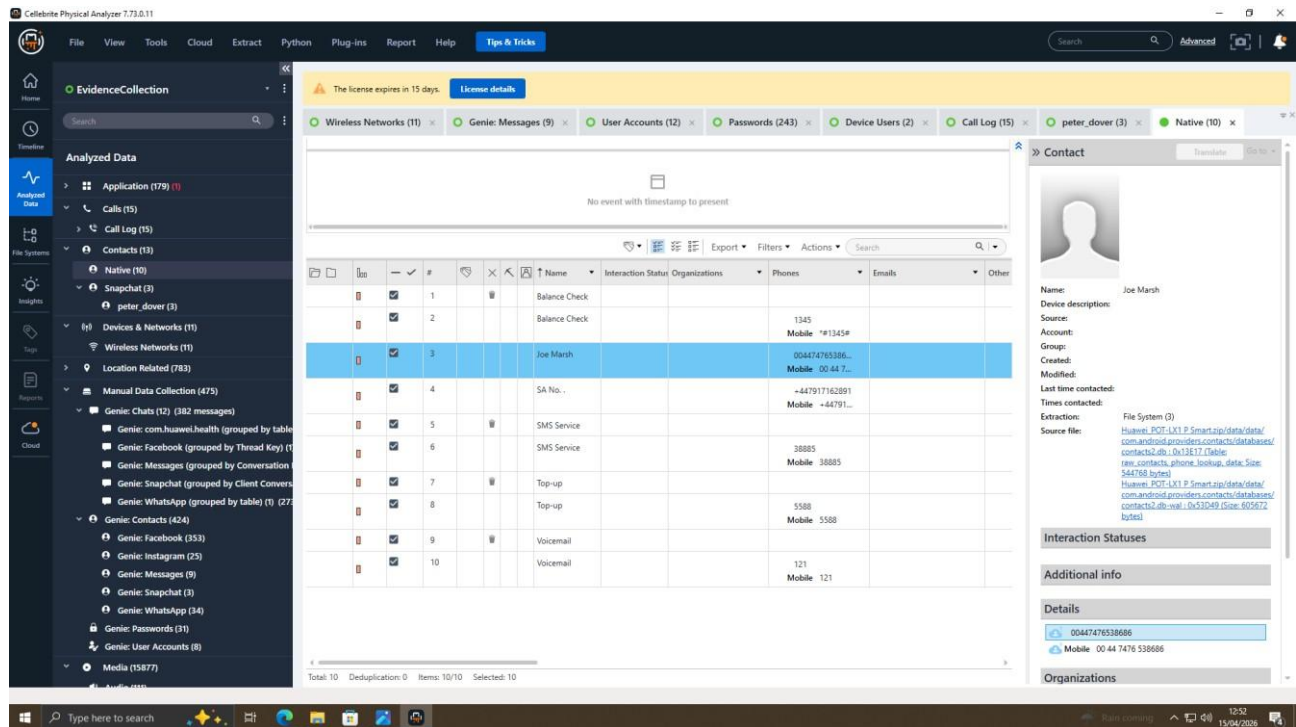


Figure 9. Contact artefact identifying Joe Marsh within Cellebrite Physical Analyzer

This figure shows the stored contact record for Joe Marsh within the recovered application data. It supports attribution of the subsequent message thread to a named intermediary and reduces ambiguity regarding the identity of the contact.

As shown in Figure 10, Emma made the initial approach and explicitly framed the matter as sensitive, supporting the inference that the conversation was deliberate rather than incidental.

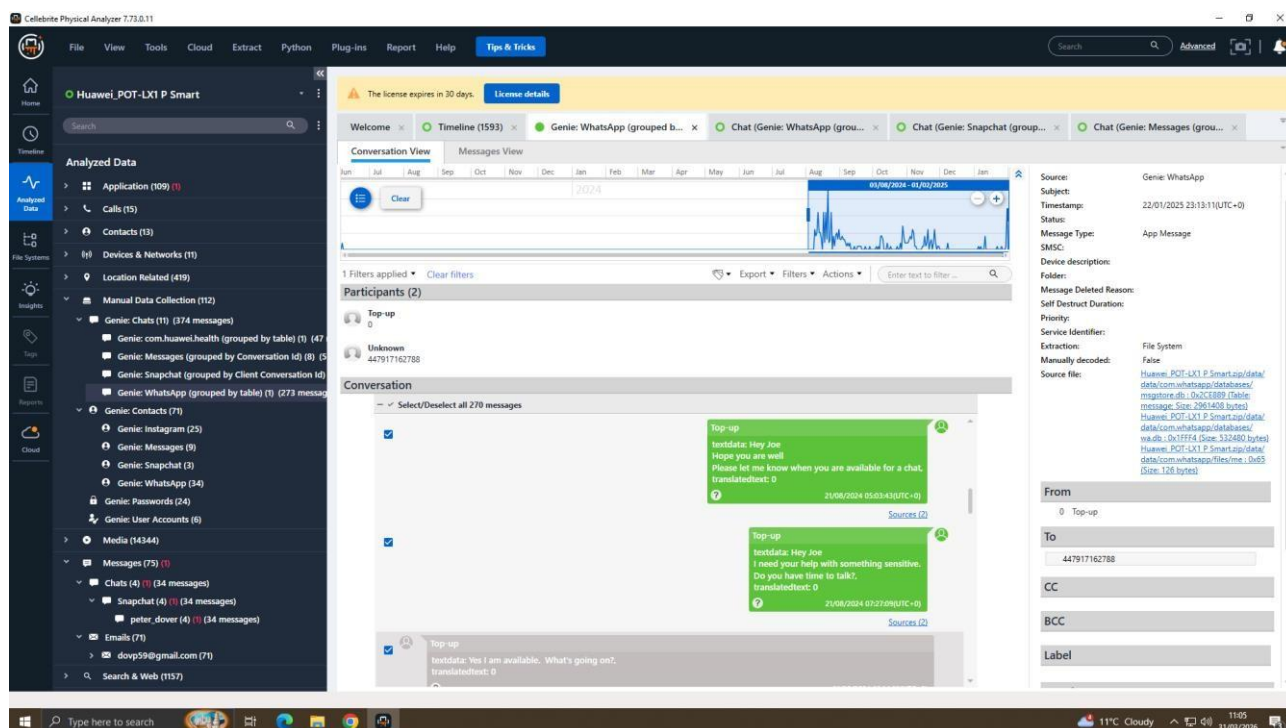


Figure 10. Initial WhatsApp communication in which Emma initiates a sensitive discussion

This figure shows Emma contacting Joe and requesting help with “something sensitive.” The message is significant because it marks the start of the communication sequence and supports the view that Emma initiated the exchange in a confidential manner.

Figure 11 is particularly significant because Emma explicitly frames the internal information as commercially valuable and suitable for sale.

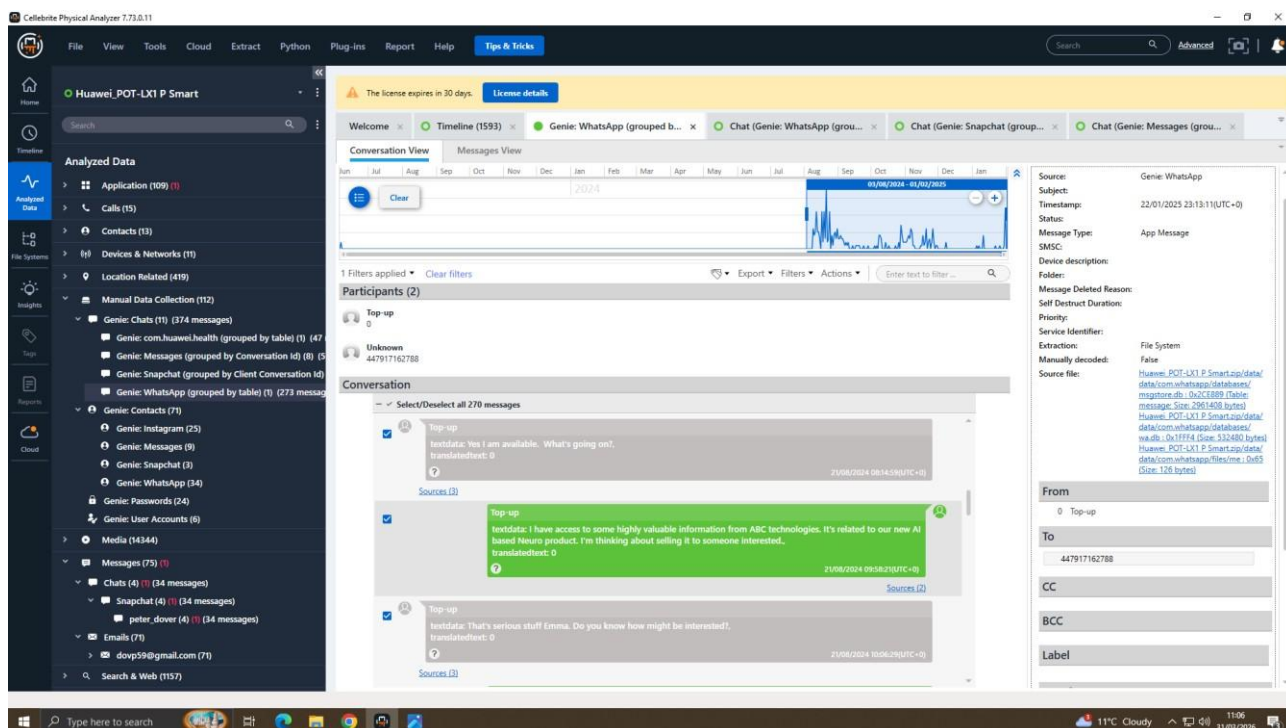


Figure 11: Emma’s disclosure of access to highly valuable AI-related information

This figure shows Emma informing Joe that she has access to highly valuable information linked to a new AI-based product and indicating that it could be sold. This is one of the clearest early indicators of criminal intent within the examined communication record.

The conversation then progressed from initial disclosure to operational planning. Emma told Joe that she trusted him to find the right buyer, thereby assigning him an active role in the scheme rather than leaving him as a passive listener. Joe's responses reinforce that interpretation, as he indicated that he was already meeting clients and would discuss the offer with them.

Figure 12 marks the point at which Joe becomes the functional intermediary in the attempted transaction.

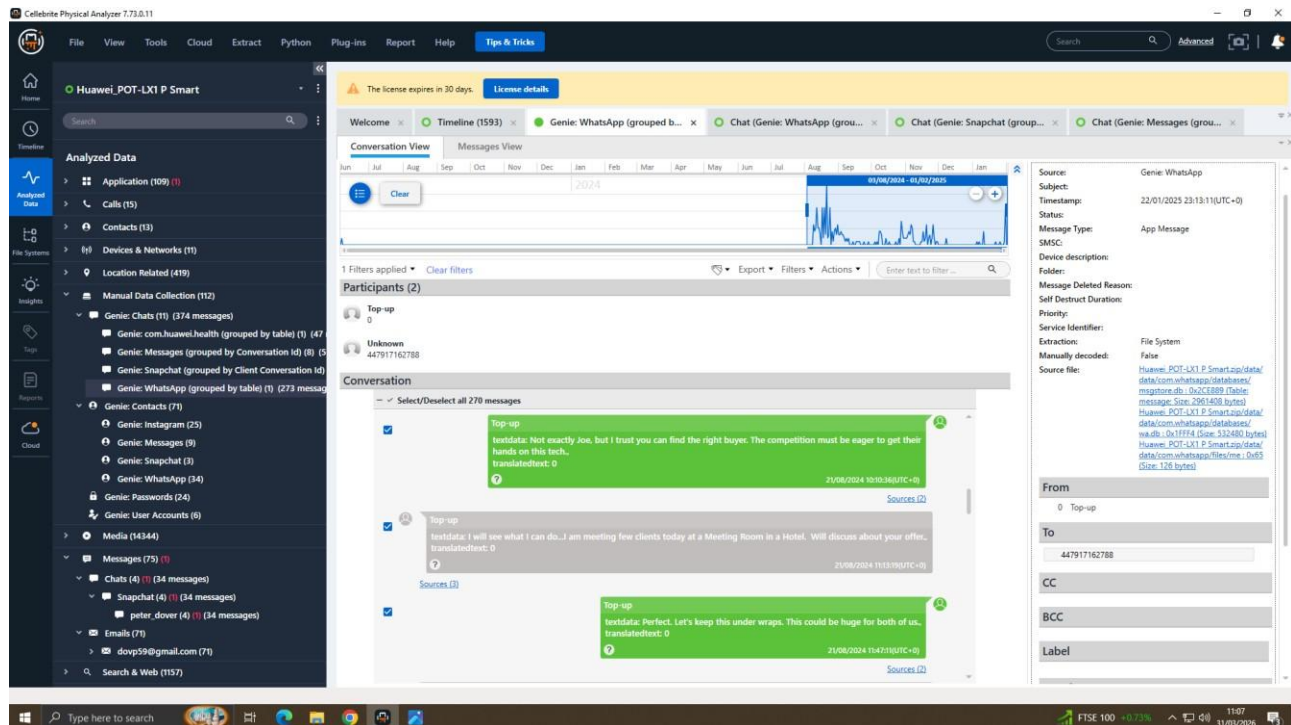


Figure 12: Emma instructs Joe to locate a suitable buyer

This figure shows Emma expressing trust in Joe to find the right buyer and Joe indicating that he is already meeting clients. The exchange is important because it establishes Joe's operational role as an intermediary rather than a passive recipient of information.

The communication pattern continued over several months. Figure 13 shows that by late August 2024 the scheme had already moved into travel and contact meetings.

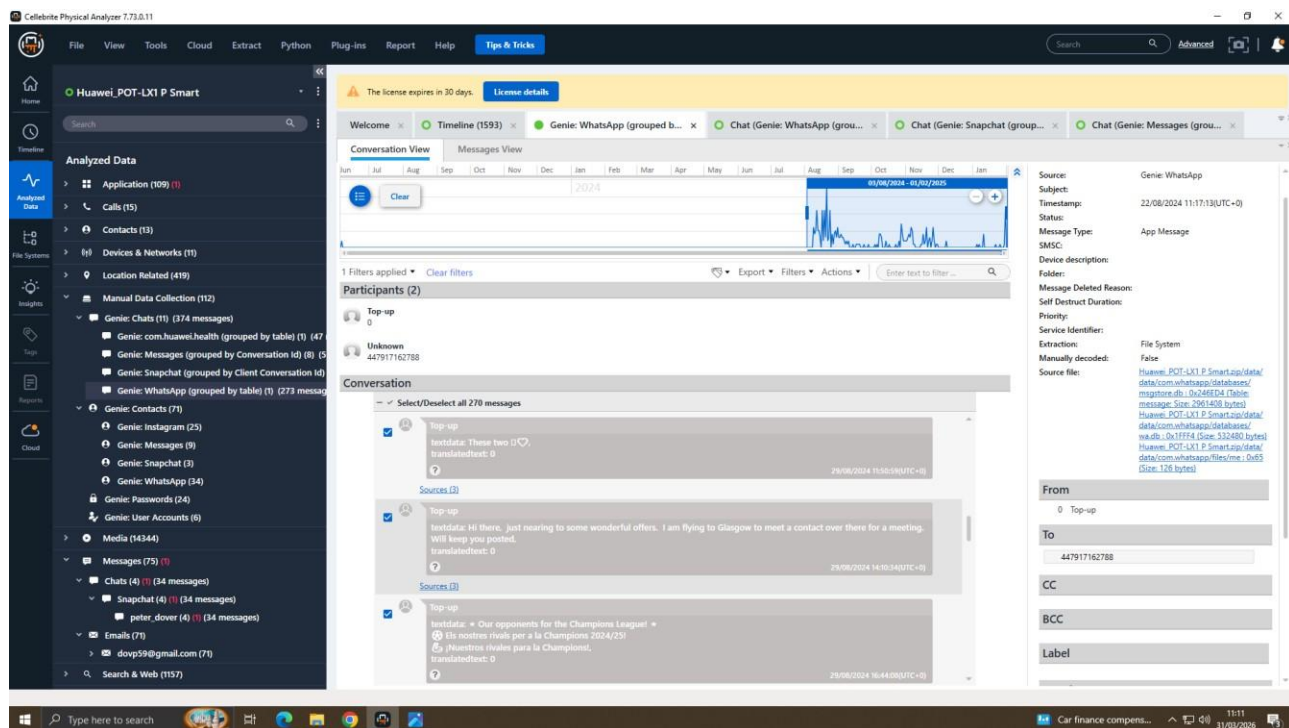


Figure 13: Message indicating travel to Glasgow for a meeting with contact

This figure shows Joe informing Emma that he is flying to Glasgow to meet a contact. It is significant because it indicates that the communications had developed into physical meeting arrangements linked to the attempted sale.

The most incriminating exchange appears on 31 January 2025. Figure 14 shows Emma limiting the disclosure to a detailed breakdown rather than a full sample, which is consistent with staged release of sensitive material.

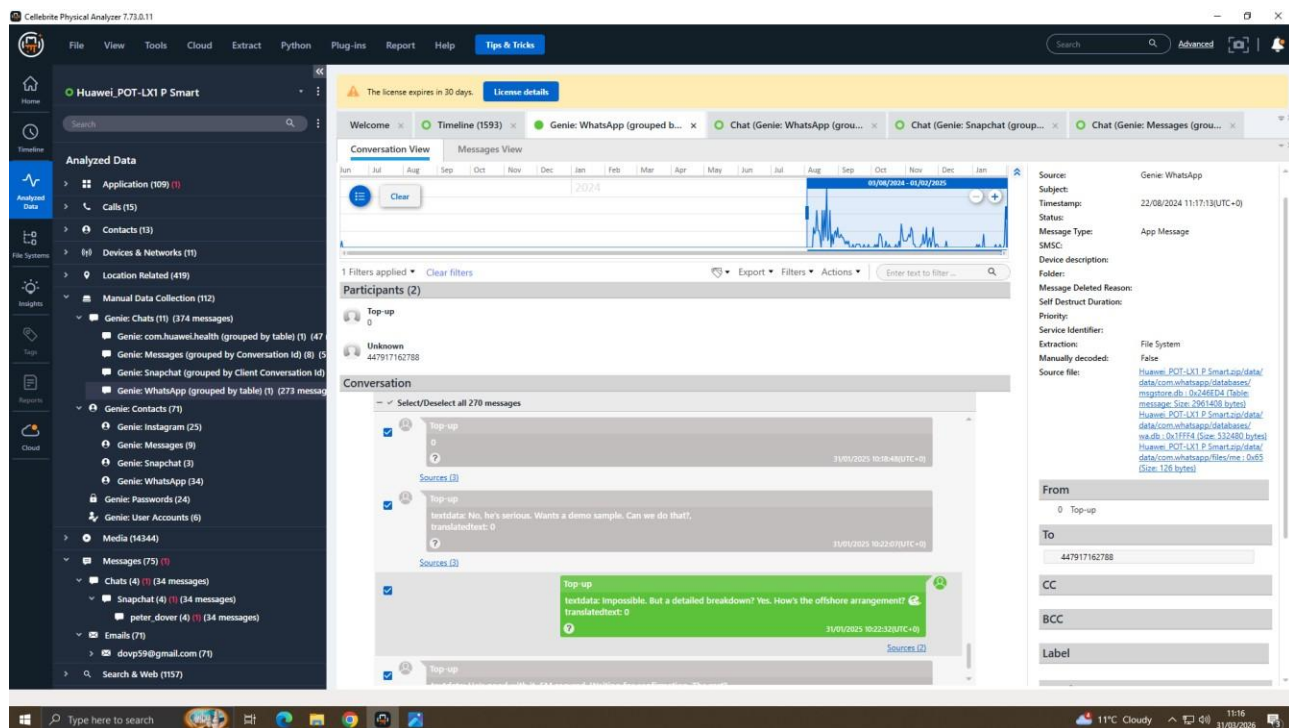


Figure 14: Discussion of controlled disclosure and offshore payment structure

This figure shows Emma refusing to release a full sample while agreeing to provide a detailed breakdown, alongside discussion of offshore arrangements. This is among the strongest artefacts in the case because it suggests deliberate control over staged disclosure and an effort to conceal payment flows.

Figure 15 further strengthens the evidential picture by linking the proposed release of information to an apparent financial arrangement.

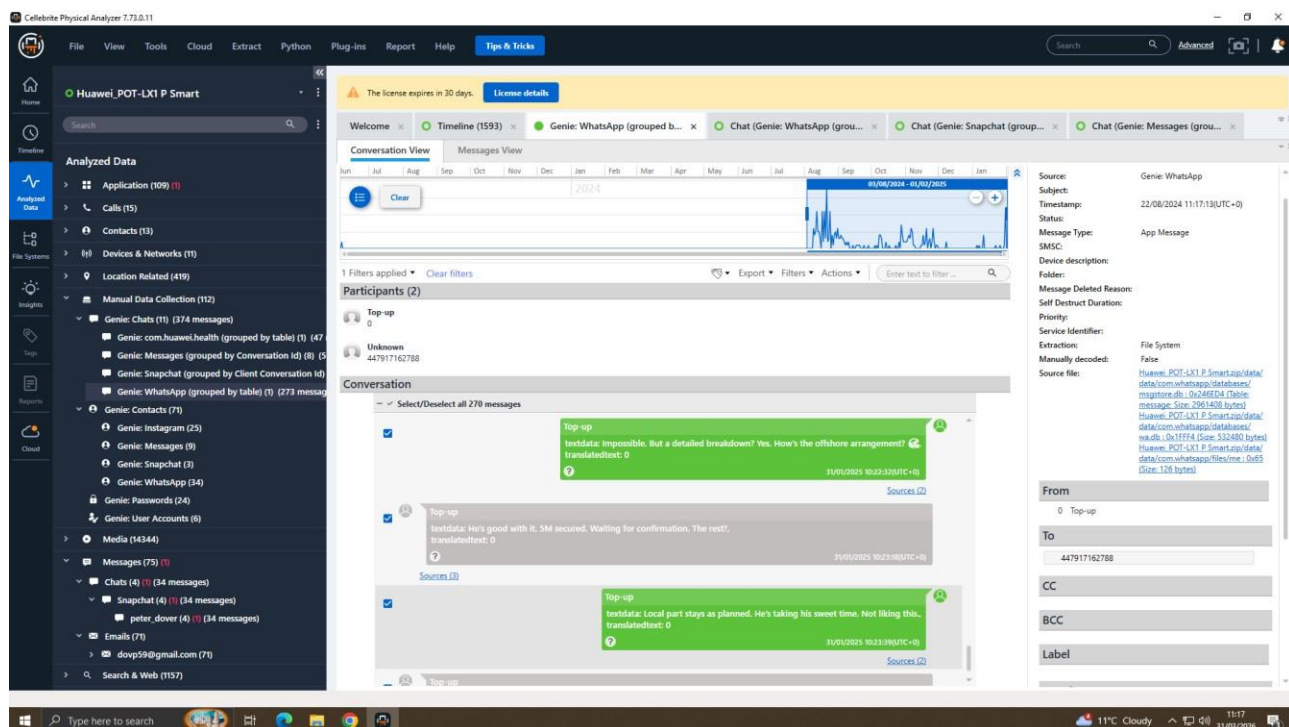


Figure 15: Message reflecting structured financial negotiation

This figure shows Joe stating that “5M” has been secured and Emma responding that the local part will stay as planned. The exchange strongly supports the existence of a structured payment arrangement linked to the sale of confidential information.

2.5.2 Buyer-side communication involving Norman

A separate communication stream places Norman on the recipient side of the transaction.

Figure 16 shows that Norman was not incidental to the communication chain but was positioned as a ready participant in the deal.

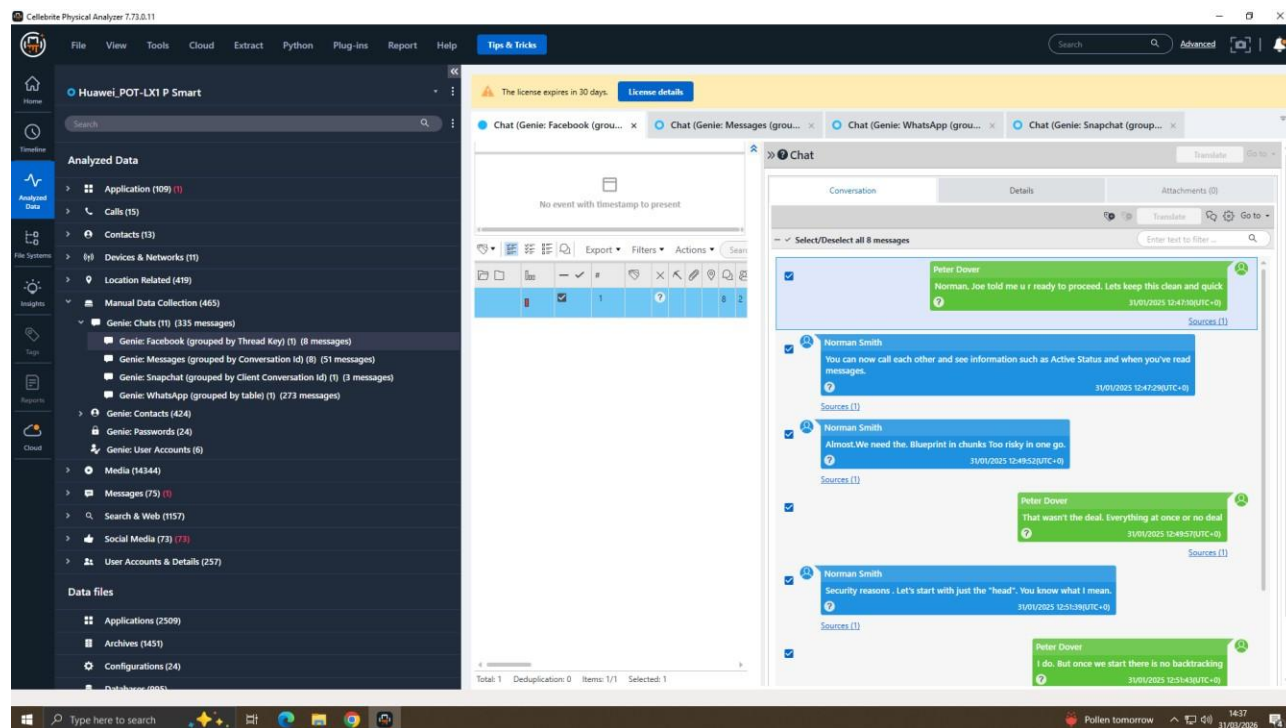


Figure 16: Buyer-side communication linking Norman to the planned transaction

This figure shows a communication in which Norman is described as ready to proceed. It connects Norman directly to the transaction and supports his identification as the buyer.

As shown in Figure 17, Norman’s reference to chunked release and offshore payment strongly supports the conclusion that he was an active buyer rather than an incidental contact.

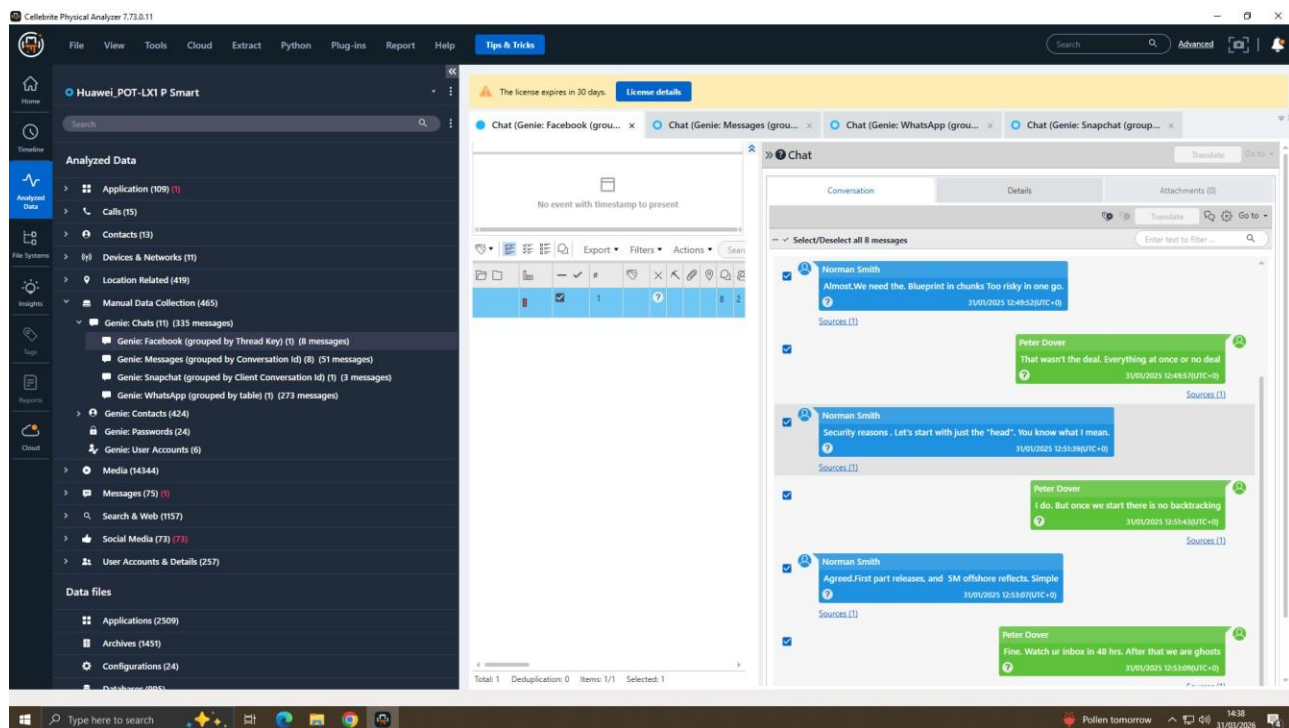


Figure 17: Buyer-side discussion of staged blueprint release and offshore payment

This figure shows Norman discussing receipt of the blueprint in chunks and referring to a 5M offshore arrangement. This is one of the strongest buyer-side artefacts because it indicates both knowledge of the material and conscious efforts to reduce detection risk.

2.5.3 Corroborative location and travel artefacts

The communication evidence is reinforced by supporting location and travel artefacts. One screenshot showed Joe sharing a live location during the communication sequence, while other screenshots contained geo-tagged images and travel-related photographs that aligned with the negotiation timeline.

Figure 18 provides independent metadata support for the meeting claim made in the message.

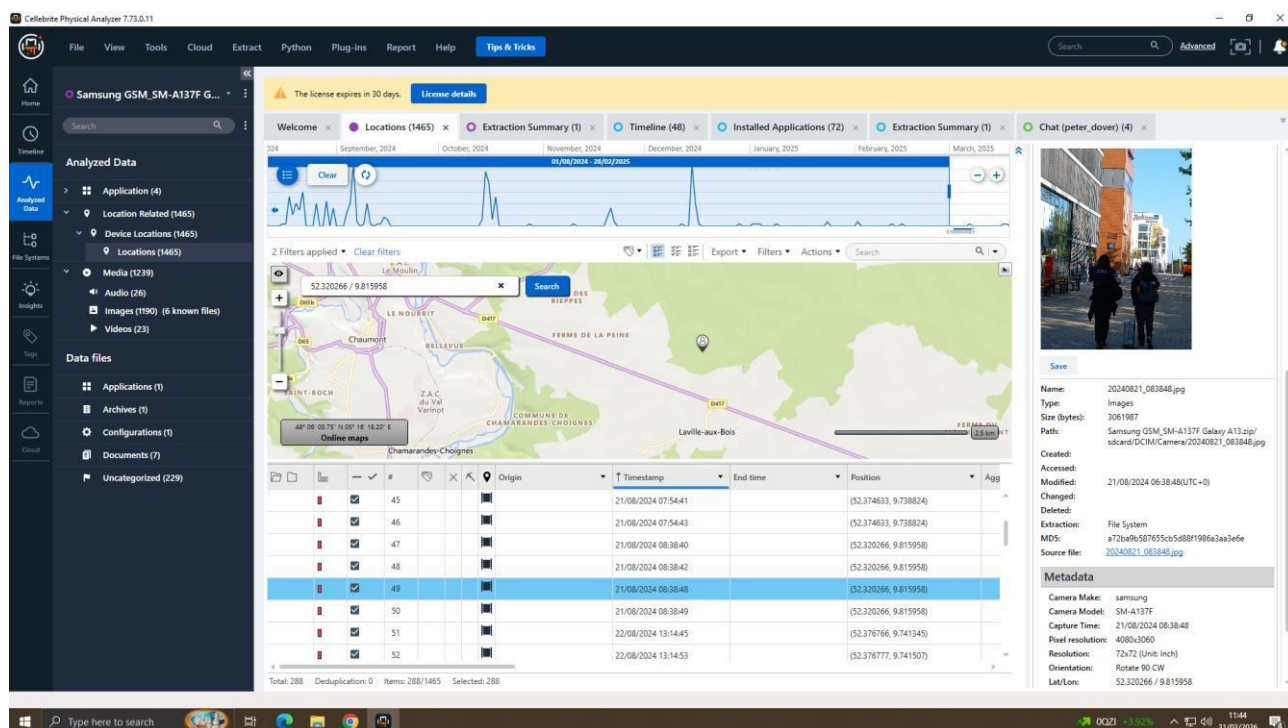


Figure 18: Geo-tagged image placing a device at a hotel during the relevant meeting period

This figure shows location metadata placing the device in a hotel at a time that aligns with Joe's message about going to a hotel to meet a client. It provides corroborative support for the communication timeline.

Figure 19 provides independent metadata support for the Glasgow travel claim made in the message thread.

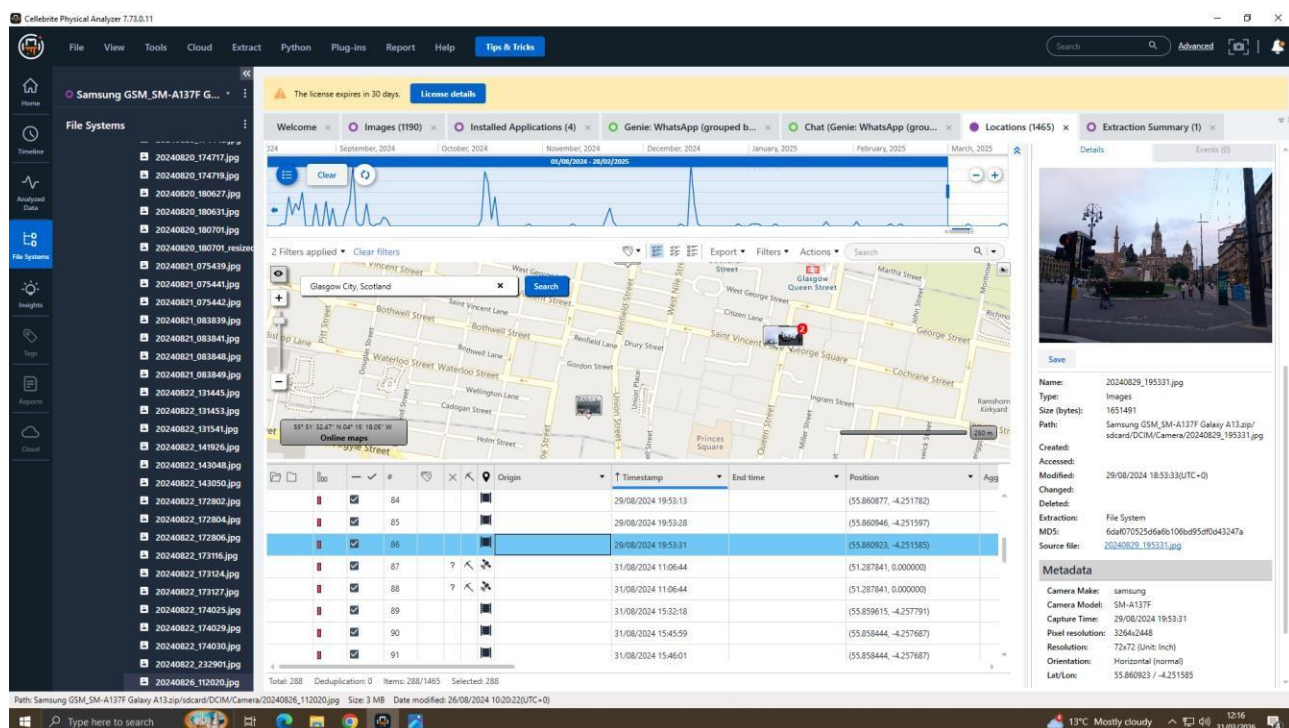


Figure 19: Geo-tagged image placing a device in Glasgow during the negotiation period

This figure shows location metadata placing the device in Glasgow at a time that aligns with Joe's message about travelling there to meet a contact. It provides corroborative support for the communication timeline.

Figure 20 further corroborates movement during the active negotiation phase by showing travel-related images rather than only message assertions.

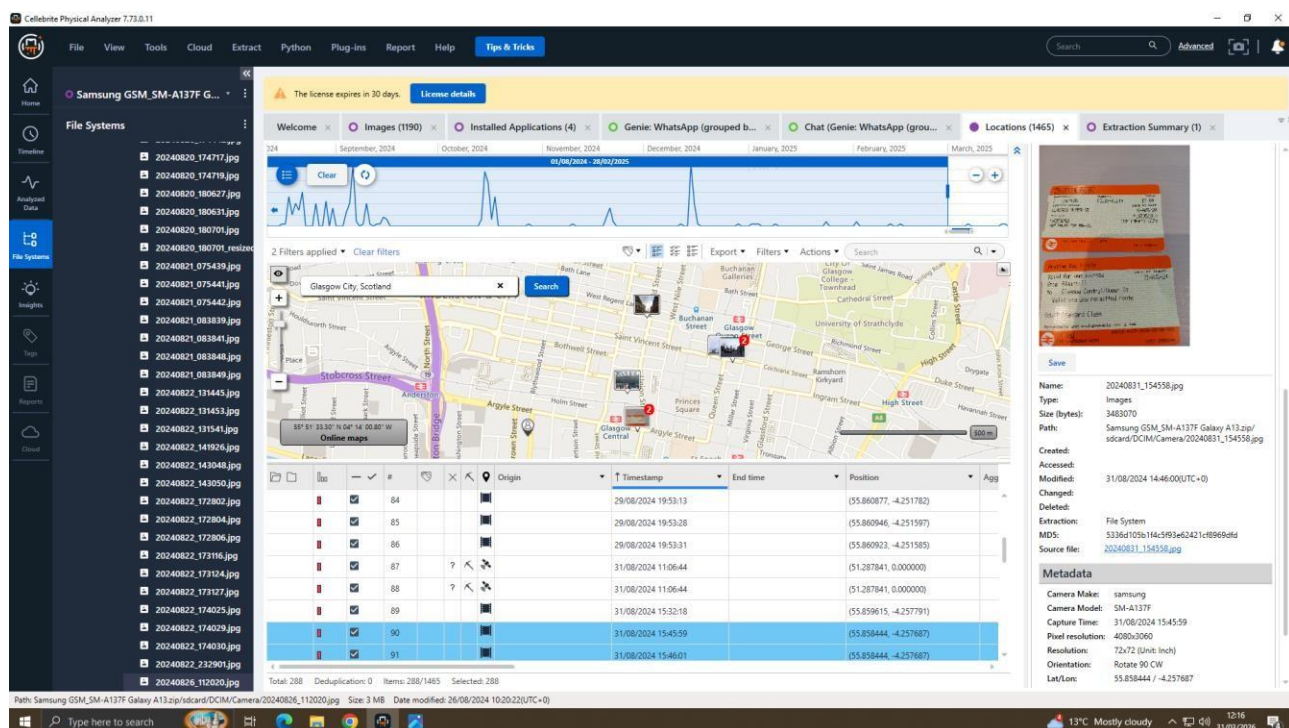


Figure 20: Travel-related image artefact showing train ticket photographs

This figure shows photographs of train tickets recovered from the extracted data. These artefacts support the interpretation that real-world travel took place during the period of active negotiation.

2.5.4 Call log Analysis

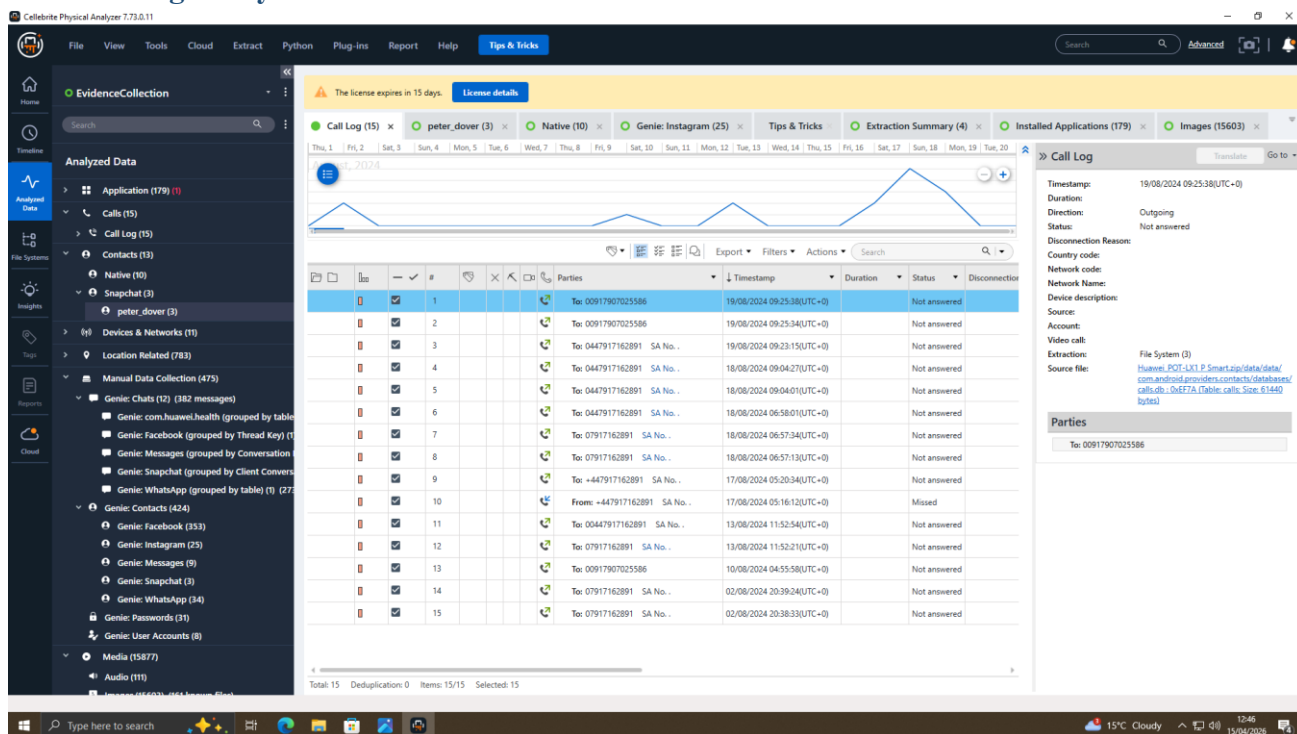


Figure 21: Call log of Emma's Phone

2.6 Suspect role assessment

Based on the examined artefacts, Emma is best assessed as the originating perpetrator. She initiated the sensitive contact, identified the information as highly valuable, indicated that it could be sold, sought buyer access through Joe, and controlled the extent of disclosure. Joe is best assessed as the intermediary because he accepted Emma's proposal, approached buyers, arranged meetings, travelled to pursue contacts, relayed buyer requests, and discussed financial progress. Norman is best assessed as the buyer because he discussed receiving the blueprint in parts, recognized the risks of full transfer, acknowledged offshore payment, and awaited delivery through his inbox.

2.7 Conclusion

The examined artefacts provide strong evidential support for a coordinated attempt to unlawfully disclose and monetize Quantum Tech's proprietary AI chip design information associated with patent QT-AI-2025. Communications show a clear development from confidential initiation to buyer sourcing, to sustained negotiation, and finally to staged disclosure and payment planning. This pattern is inconsistent with innocent or hypothetical conversation and is instead consistent with attempted corporate espionage.

Emma's role is most consistent with that of an insider source and originating perpetrator. Joe's conduct is most consistent with that of a facilitating intermediary. Norman's conduct is most consistent with that of the intended buyer. The strongest evidential features are the direct discussion of valuable proprietary information, the search for a buyer, repeated references to secrecy, the proposal of partial release, and the presence of offshore payment arrangements.

2.8 Recommendations

First, all original devices, extractions, and reporting artefacts should be securely preserved, and cryptographic hash verification should be recorded wherever the full extraction outputs permit. This is necessary to support integrity and admissibility.

Second, the complete extraction should be reviewed again for direct emails, call logs, deleted content, and cloud-linked communications, since these evidence classes are explicitly expected by the brief and may materially strengthen the case.

Third, all named accounts and contact identities, including Peter Dover, should be formally attributed to determine whether they represent a genuine individual, alias, or communication proxy.

Fourth, Quantum Tech should strengthen internal controls around sensitive R&D assets by improving least-privilege access, monitoring unusual file access, restricting removable media use, and deploying stronger data loss prevention controls.

Finally, the case should be considered for escalation to law enforcement and legal review in relation to suspected trade-secret theft, unlawful disclosure of confidential business information, conspiracy, and related offences supported by the wider evidence set.