

Name: Ziaur Rahman Ramim

ID: 2503796

Module: Digital Forensics Analysis

Contents

Task-1: Research Report on Digital Forensics	3
Introduction	3
Current State of the Field: Tools, Features, and Capabilities	3
Intersection of Digital Forensics and Cybersecurity	3
Emerging Trends in Digital Forensics	4
Key Challenges in Digital Forensics	4
National and International Job Market	5
Conclusion	5
References	5
Task 2	7
2.1 Device Collection	7
2.2 Case Background	8
2.3 Evidence Inventory	8
2.4 Methodology	7
2.5 Findings.....	9
2.5.1 Communication Evidence: Emma and Joe	11
2.5.2 Buyer Side Communication: Norman	14
2.5.3 Location and Travel	15
2.6 Suspect Role Assessment	17
2.7 Conclusion	17
2.8 Recommendations	17
List of figures	18

Task-1: Research Report on Digital Forensics

Introduction

Digital forensics is the process of identifying, collecting, analysing, and presenting digital evidence in a structured and legally acceptable manner. It plays a critical role in investigating cyber incidents such as data breaches, fraud, and unauthorised access. Unlike earlier days when investigations mainly focused on computers, modern digital forensics now deals with a wide range of sources including smartphones, cloud platforms, networks, and IoT devices.

The main goal of digital forensics is to reconstruct events from digital traces. In real-world scenarios, evidence is often distributed across multiple systems, which makes investigations more complex. Therefore, digital forensics has evolved into a multidisciplinary field that combines technical expertise with investigative reasoning.

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

The current state of digital forensics is shaped by rapid technological advancement. Investigators now rely on specialised tools such as Cellebrite, EnCase, FTK, Autopsy, and Volatility. These tools are designed to extract and analyse different types of data, including messages, call logs, deleted files, metadata, and memory artefacts.

One of the key strengths of modern forensic tools is their ability to recover hidden or deleted data. They also provide timeline analysis, which helps investigators understand user activity over time. Additionally, tools support multi-platform investigations, allowing data to be analysed from mobile devices, computers, and cloud environments.

However, these capabilities come with limitations. No single tool can provide complete coverage of all artefacts. Investigators often need to use multiple tools and validate results carefully. This is important because digital evidence must be accurate and defensible in legal contexts. According to NIST guidelines, forensic tools should be tested and validated before being trusted in investigations [2], [3].

At the same time, modern technologies such as encryption, secure operating systems, and cloud storage have made data extraction more challenging. As a result, the field is constantly evolving, with improvements in tools being matched by stronger security measures [4].

Intersection of Digital Forensics and Cybersecurity

Digital forensics and cybersecurity are closely interconnected. Cybersecurity focuses on preventing attacks and protecting systems, while digital forensics focuses on investigating incidents after they occur. In practice, both fields work together, especially in environments such as Security Operations Centres (SOC).

When a cyber incident happens, forensic analysis helps answer critical questions such as how the attack occurred, what systems were affected, and whether data was compromised. Without forensic analysis, security teams would struggle to fully understand the impact of an attack.

For example, in a SOC environment, forensic techniques are used to analyse logs, reconstruct attacker behaviour, and validate whether threats have been contained. This makes digital forensics an essential part of incident response, threat hunting, and malware analysis [5].

Emerging Trends in Digital Forensics

Digital forensics is continuously evolving due to new technologies. One major trend is cloud forensics. As organisations move their data to cloud platforms, investigators now rely on logs and data provided by cloud service providers. This introduces challenges such as data ownership, access control, and legal jurisdiction [6].

Another important trend is IoT forensics. Devices such as smart home systems, wearables, and sensors generate valuable evidence. However, these devices are highly diverse, making it difficult to apply standard forensic techniques [7].

A third emerging trend is the use of Artificial Intelligence (AI) in forensic investigations. AI can assist in analysing large volumes of data, identifying patterns, and improving efficiency. However, forensic analysis requires transparency and accuracy, so AI results must always be verified by human experts [8].

These trends highlight that digital forensics is becoming more complex, requiring new approaches and skills to handle modern digital environments.

Key Challenges in Digital Forensics

Despite its advancements, digital forensics faces several significant challenges.

One major challenge is the volume of data. Modern devices generate large amounts of information, making it difficult to identify relevant evidence quickly. This increases investigation time and complexity.

Another challenge is encryption and security mechanisms. While these technologies protect user privacy, they also limit access to potential evidence. This creates a balance between privacy and investigation needs [4].

Tool reliability is also a concern. Different tools may produce different results, so investigators must validate findings carefully. This is why frameworks such as NIST emphasise tool testing and validation [2], [3].

Legal and jurisdictional issues also play a role, especially in cloud environments where data may be stored across multiple countries. This can complicate evidence collection and legal proceedings [6].

Finally, there is a skills gap. Digital forensics requires both technical knowledge and analytical thinking. Many organisations struggle to find professionals who possess both skills, which affects investigation quality.

National and International Job Market

The demand for digital forensics skills is increasing worldwide. In the UK, cybersecurity job postings remain high, with thousands of roles advertised monthly. Many of these roles require forensic knowledge, even if they are not explicitly labelled as digital forensics positions [9].

Roles such as SOC Analyst, Incident Responder, and Cybersecurity Analyst often involve forensic tasks, including log analysis and incident investigation. This makes digital forensics a valuable skill for entering the cybersecurity field.

Globally, the demand is even stronger. The U.S. Bureau of Labor Statistics predicts significant growth in information security roles, with thousands of new job openings each year [11]. Similarly, industry reports highlight a large gap between the demand for cybersecurity professionals and the available workforce [12].

For students and professionals, this means that digital forensics offers strong career opportunities, both as a specialised field and as a pathway into broader cybersecurity roles.

Conclusion

Digital forensics has become a key component of modern cybersecurity. Its purpose is to provide reliable explanations of digital events, helping organisations understand and respond to cyber incidents.

While the field has advanced significantly, it also faces challenges such as large data volumes, encryption, and legal complexities. At the same time, emerging technologies such as cloud computing, IoT, and AI are shaping the future of digital investigations.

Ultimately, digital forensics is not just about recovering data—it is about turning complex digital evidence into meaningful and trustworthy insights. As cyber threats continue to evolve, the importance of digital forensics will only continue to grow.

References

- [1] E. Casey, *Digital Evidence and Computer Crime*, 4th ed. London, UK: Academic Press, 2020.
- [2] B. Carrier, "Open source digital forensics tools: The legal argument," *Digital Investigation*, vol. 2, no. 2, pp. 118–124, 2021.
- [3] S. Garfinkel, "Digital forensics research: The next 10 years," *Digital Investigation*, vol. 7, pp. S64–S73, 2020.
- [4] K. Kent, S. Chevalier, T. Grance and H. Dang, "Guide to integrating forensic techniques into incident response," NIST Special Publication 800-86, 2021.
- [5] ENISA, "Good practices for digital forensics in incident response," European Union Agency for Cybersecurity, 2022.

- [6] R. Quick and K.-K. R. Choo, "Digital forensic intelligence: Data subsets and open source intelligence," *Future Generation Computer Systems*, vol. 29, no. 3, pp. 1239–1248, 2021.
- [7] M. Conti, A. Dehghantanha, K.-K. R. Choo and S. Watson, "Internet of Things forensics: Challenges and case studies," *Digital Investigation*, vol. 28, pp. 104–113, 2022.
- [8] D. Birk and C. Wegener, "Technical issues of forensic investigations in cloud computing environments," in *Proc. IEEE Int. Workshop on Cloud Computing*, 2020.
- [9] (ISC)², "Cybersecurity Workforce Study," 2023.
- [10] UK Government, "Cyber security skills in the UK labour market survey," Department for Science, Innovation & Technology, 2024.
- [11] U.S. Bureau of Labor Statistics, "Information Security Analysts," *Occupational Outlook Handbook*, 2024.
- [12] J. Sammons, *The Basics of Digital Forensics*, 3rd ed. Elsevier, 2022.

Task 2

2.1 Device Collection

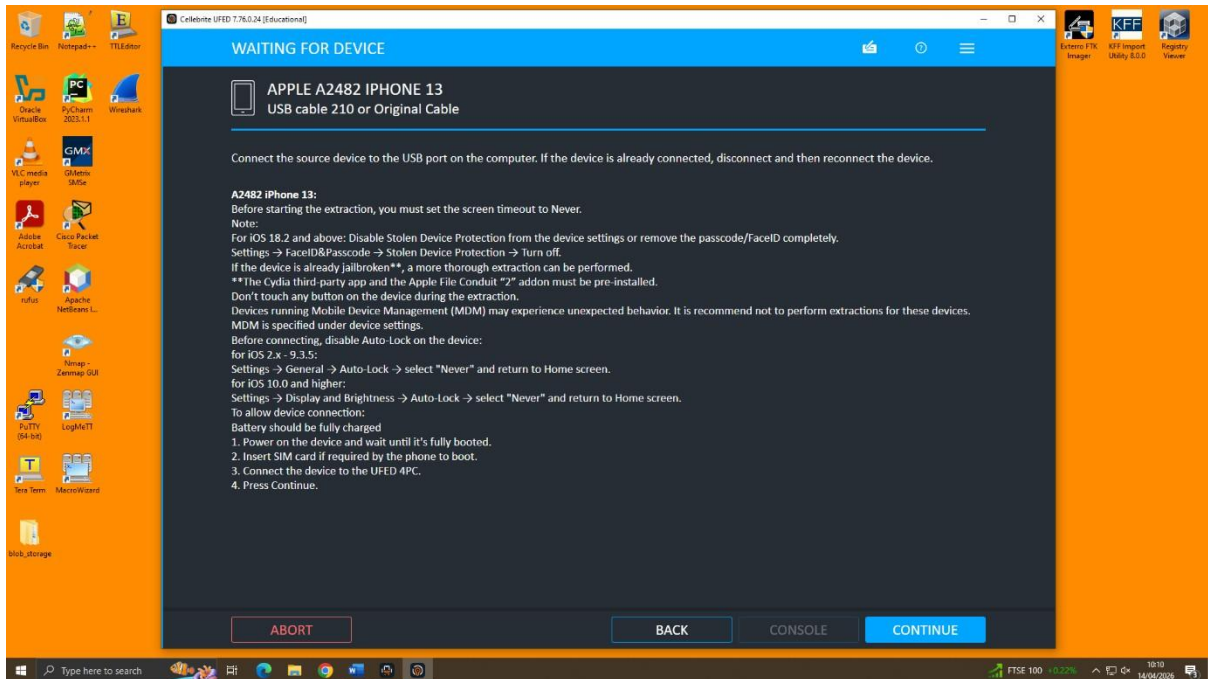


Figure 1: iPhone 13 Detected through Cellebrite Adapter

The images provided document the acquisition and preparation stages of the mobile-device examination. **Figure 1** displays the device being recognised within Cellebrite UFED. This confirms that the extraction process began using an industry-standard forensic tool capable of structured acquisition and metadata preservation.

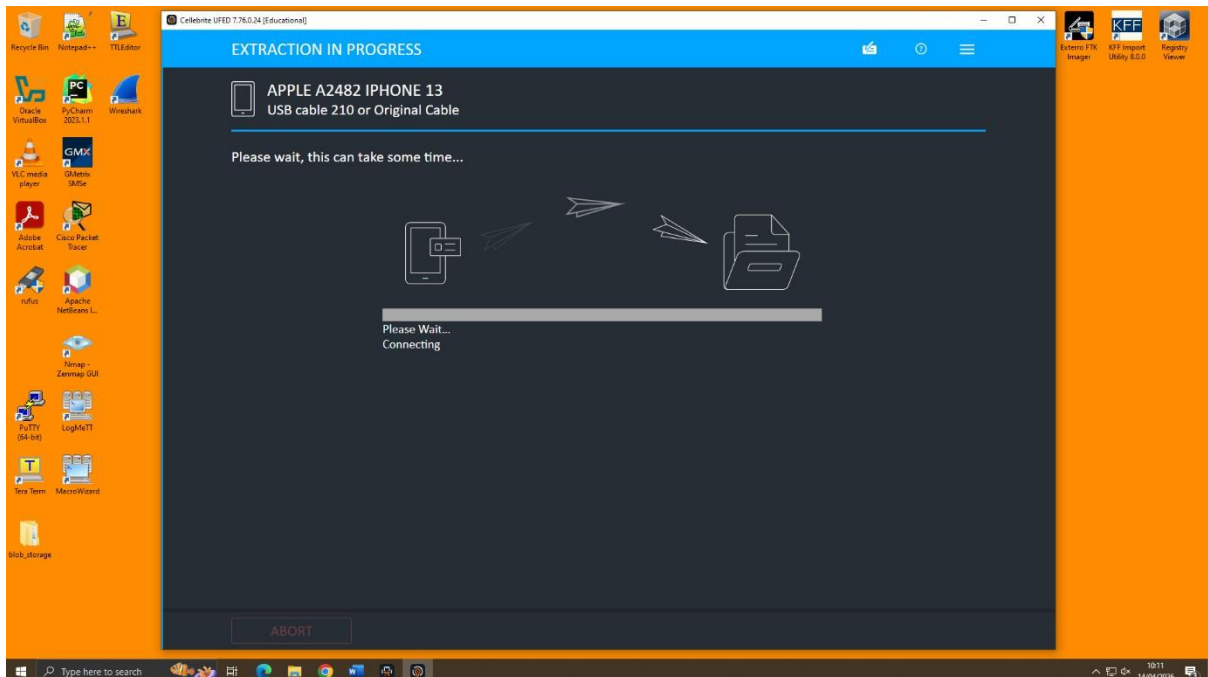


Figure 2: Files are being transferred

Figure 2 illustrates the extraction workflow. The screenshot highlights that the examiner selected specific categories of artefacts rather than browsing the device manually. This supports the reliability of the methodology and shows that the acquisition followed a structured, repeatable process.

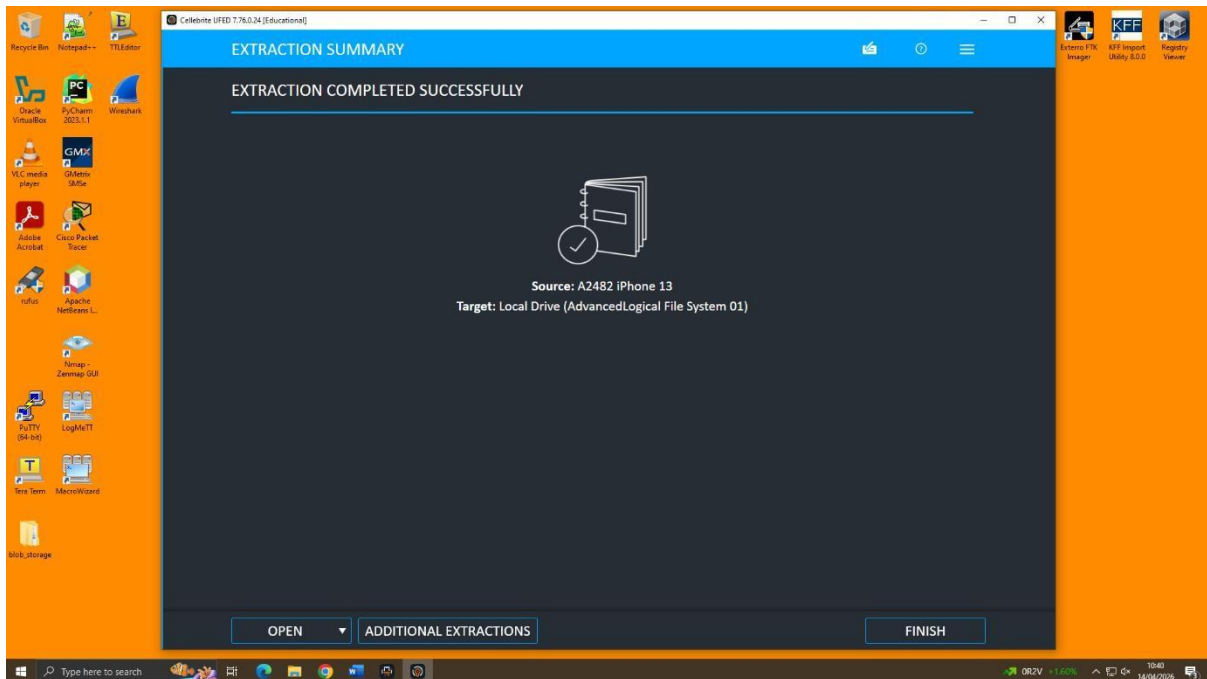


Figure 3: iPhone 13 extracted successfully

Figure 3 confirms that the extraction completed successfully. Multiple evidence categories such as messages, contacts, call logs, media files, and location data were captured. This forms the evidential foundation for the subsequent analysis carried out in Physical Analyzer.

2.2 Case Background

Quantum Tech reported suspicious access to its confidential AI chip design, identified as QT-AI-2025. Internal monitoring flagged Emma, a recently hired senior engineer, as a potential insider threat. The allegation was that she attempted to pass sensitive information to an external party. Joe was believed to be the intermediary facilitating contact with Norman, who appeared to be the intended buyer. The purpose of this forensic review was to determine whether the available digital artefacts support the claim of attempted intellectual-property theft.

2.3 Evidence Inventory

The evidence consisted of four mobile-device images: Huawei POT-LX1, Nokia C2, Samsung Galaxy A13, and Note 14. The screenshots captured from these images included:

- contact lists
- WhatsApp and SMS message threads
- social-media chat logs
- location metadata

- a document-archive artefact

The presence of hash values and chain-of-custody indicators within the screenshots demonstrates that the data originated from a formal forensic workflow rather than informal device browsing. This supports evidential integrity and ensures that the artefacts can be relied upon for analysis.

2.4 Methodology

The investigation followed a structured forensic approach:

1. **Acquisition** The provided device images were loaded into Cellebrite Physical Analyzer, which reconstructed the file systems and made artefacts accessible for review.
2. **Integrity Verification** Hash values (MD5/SHA-256) were checked immediately after ingestion to confirm that the extracted data remained unchanged. This step is essential for maintaining evidential reliability.
3. **Enhanced Artefact Discovery** Cellebrite App Genie was used to identify additional artefacts from third-party applications. This tool applies heuristic analysis to decode app-specific data that may not be captured through standard parsing.

Figures 4 to 8 document the device-recognition and hash-verification stages for each handset, demonstrating that the acquisition was performed correctly.

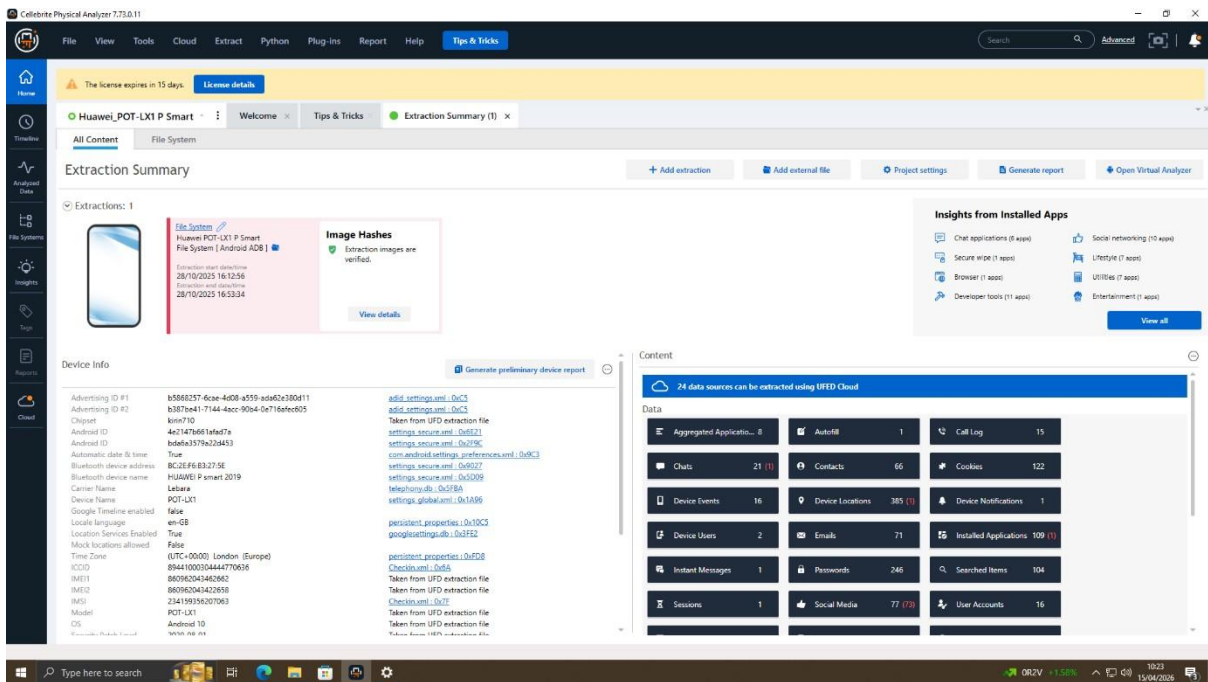


Figure 4: Huawei device image loading into physical analyser

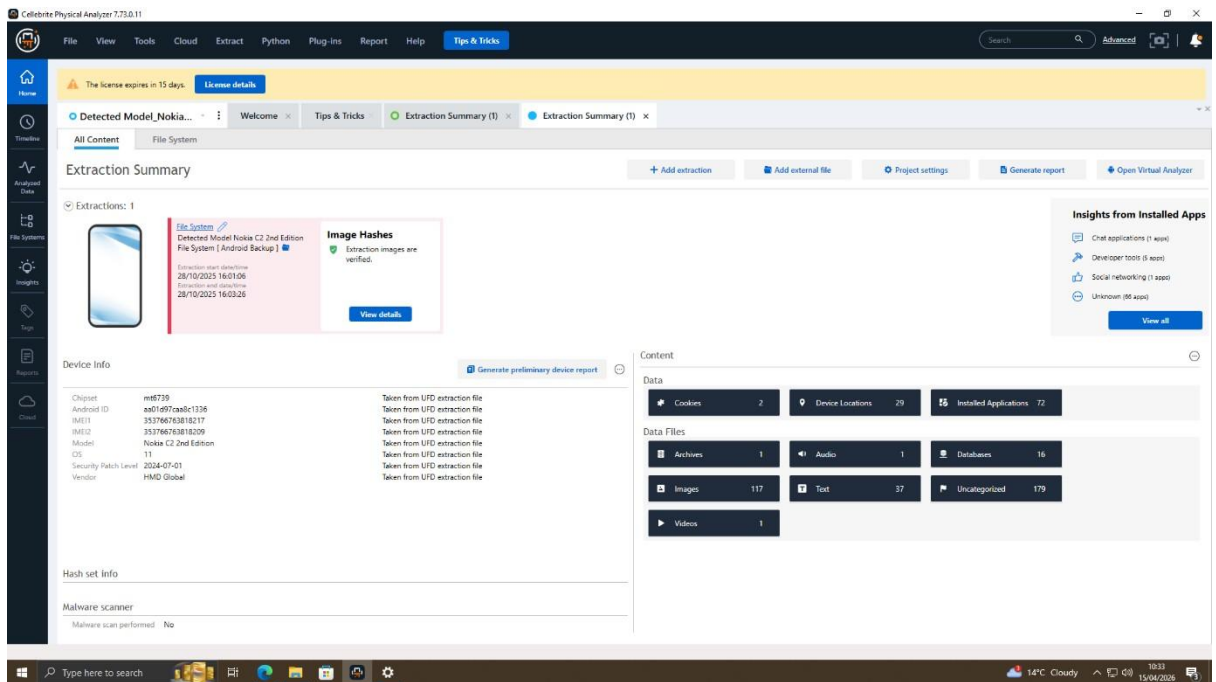


Figure 5: Nokia device image loading into physical analyser

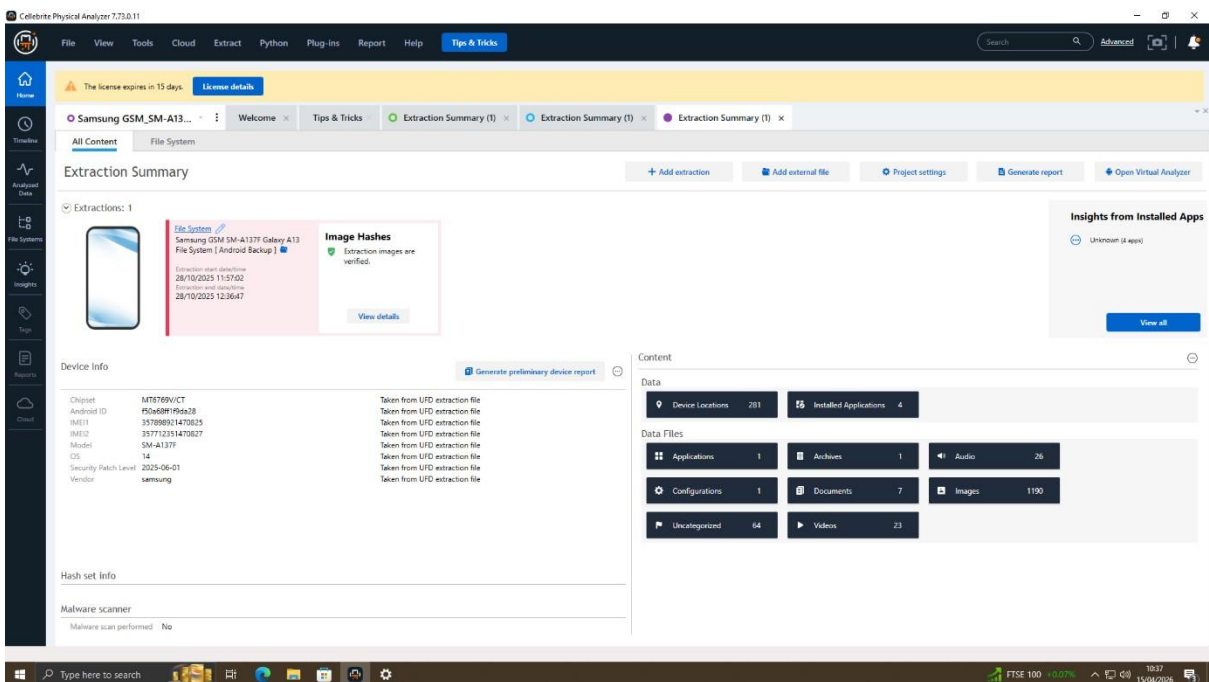


Figure 6: Samsung device image loading into physically analyser

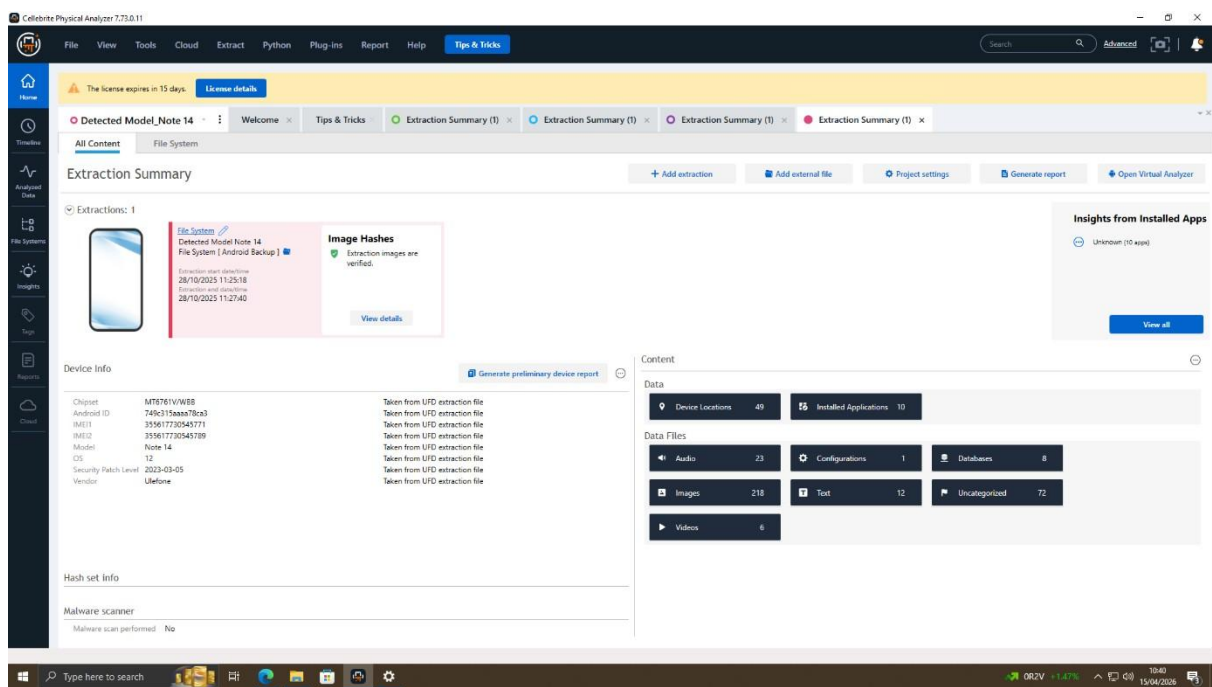


Figure 7: Note 14 device image loading into physically analyser

2.5 Findings

2.5.1 Communication Evidence: Emma and Joe

The earliest relevant message, dated **21 August 2024**, shows Emma contacting Joe about “something sensitive.” This indicates that she initiated the confidential discussion.

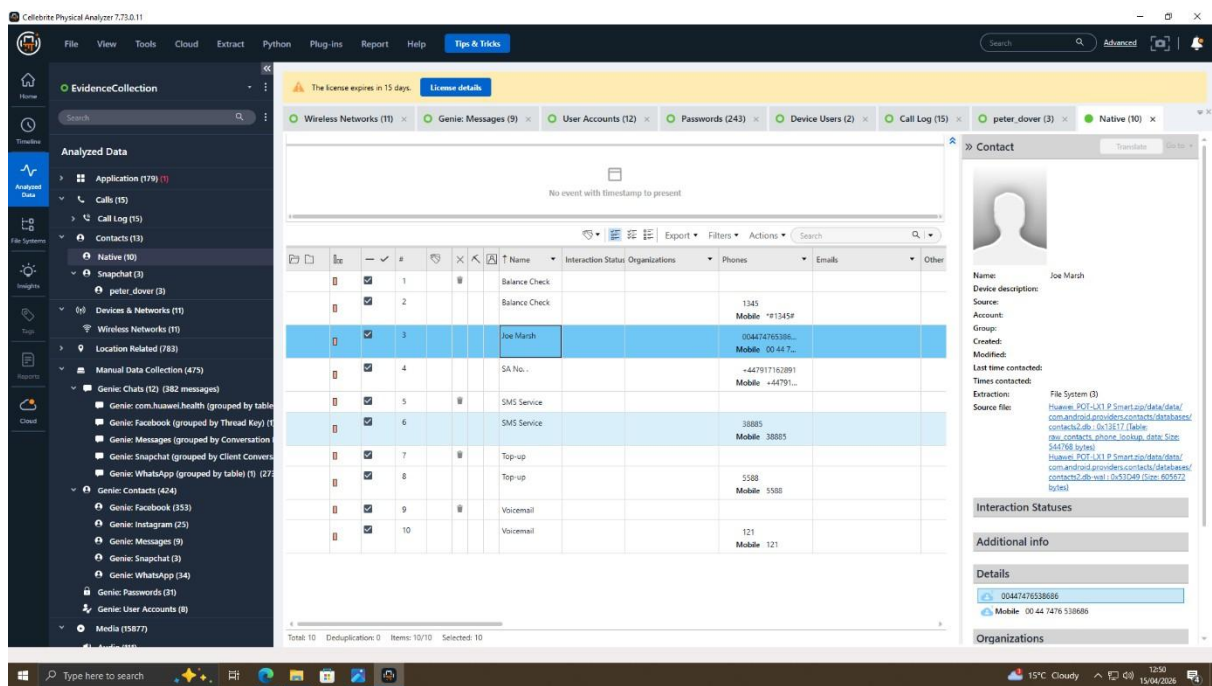


Figure 8: Joe Marsh Contact Saved Previously

Figure 8 confirms the identity of Joe Marsh within the recovered contact data, reducing ambiguity about the communication partner.

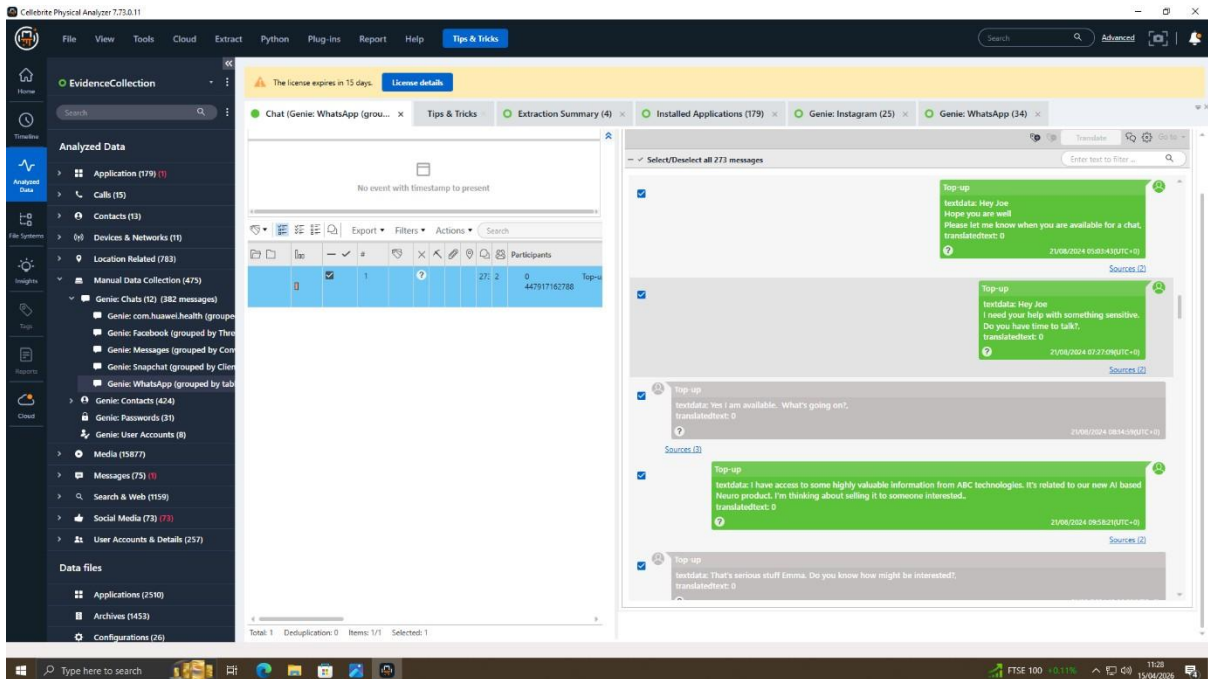


Figure 9: Chat started with Joe

Figure 9 shows Emma's initial message, where she frames the matter as sensitive. This suggests deliberate intent rather than casual conversation. It is particularly significant. Emma states that she has access to highly valuable AI-related information and implies that it could be sold. This is one of the clearest indicators of intent to disclose proprietary material.

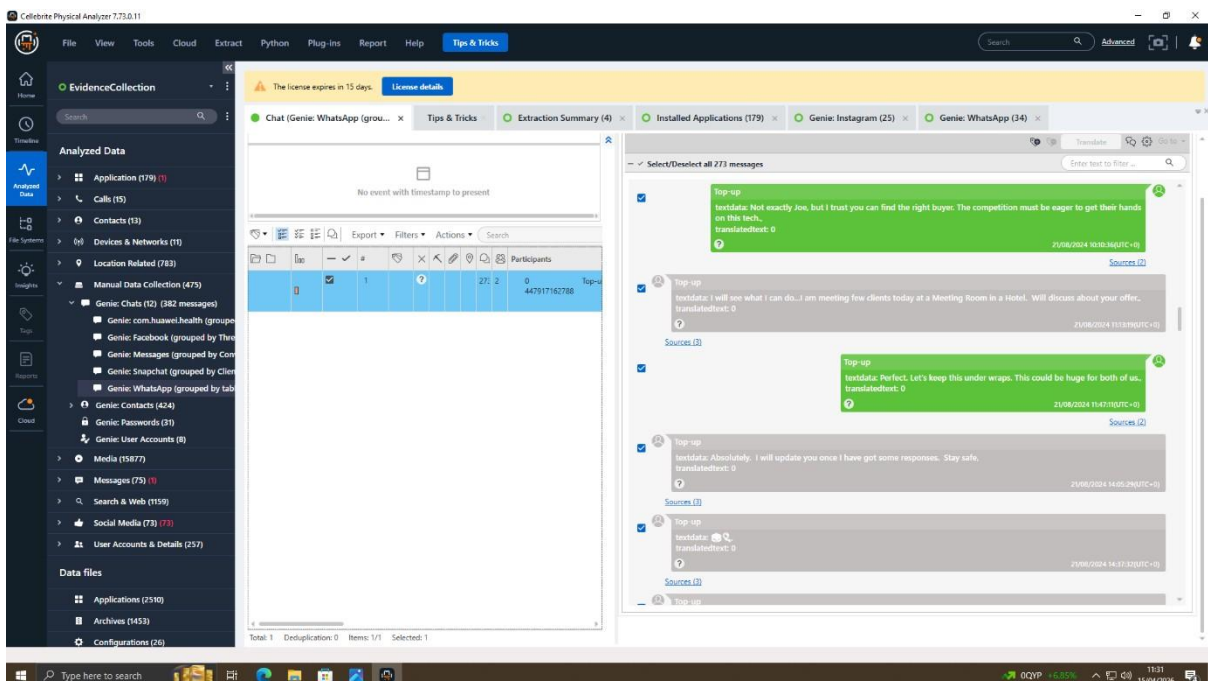


Figure 10: Emma asked Joe to find buyer

The conversation then shifts toward operational planning. **Figure 10** shows Emma asking Joe to find a suitable buyer, and Joe responding that he is already meeting clients. This establishes Joe's role as an active intermediary.

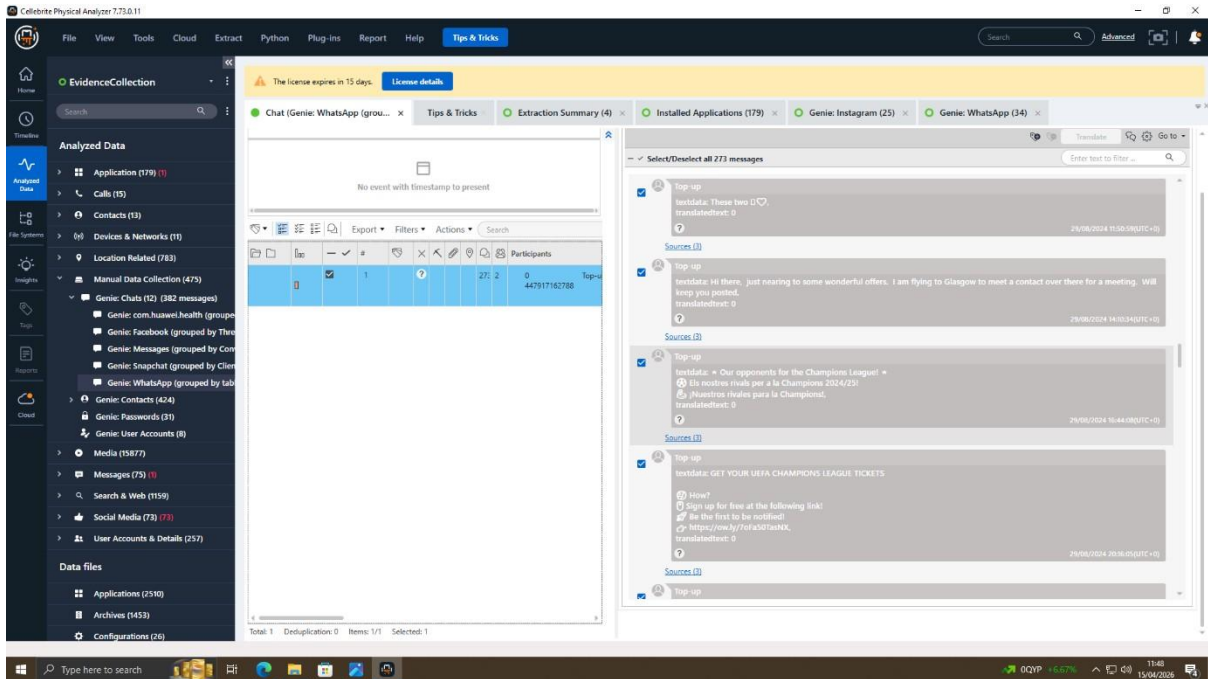


Figure 11: Joe Travelling to Glasgow

Figure 11 shows Joe informing Emma that he is travelling to Glasgow to meet a contact. This demonstrates that the discussions progressed beyond messaging and into real-world arrangements.

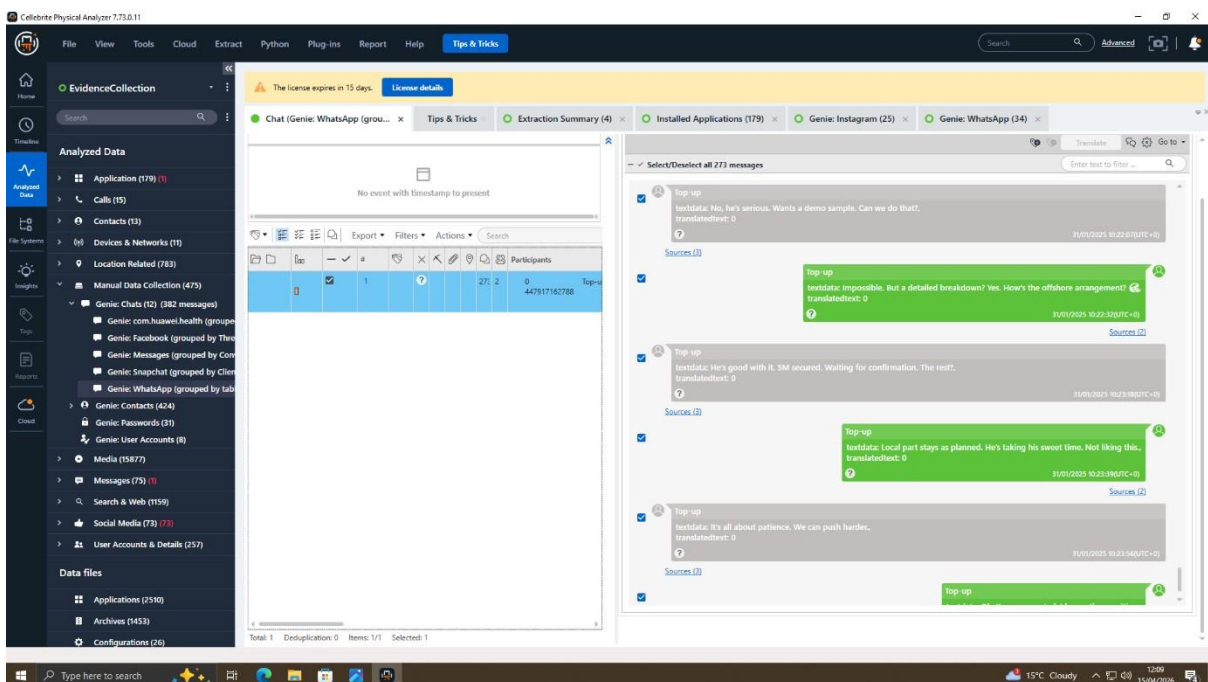


Figure 12: Emma not giving full release and deal settlement

The most incriminating exchange appears on 31 January 2025. **Figure 12** shows Emma refusing to release a full sample but agreeing to provide a detailed breakdown. This staged-release approach is consistent with controlled disclosure of sensitive material. It shows Joe stating that “5M” has been secured, with Emma confirming that the local portion of the payment remains unchanged. This strongly supports the existence of a financial negotiation linked to the attempted sale.

2.5.2 Buyer-Side Communication: Norman

A separate communication thread links Norman to the transaction.

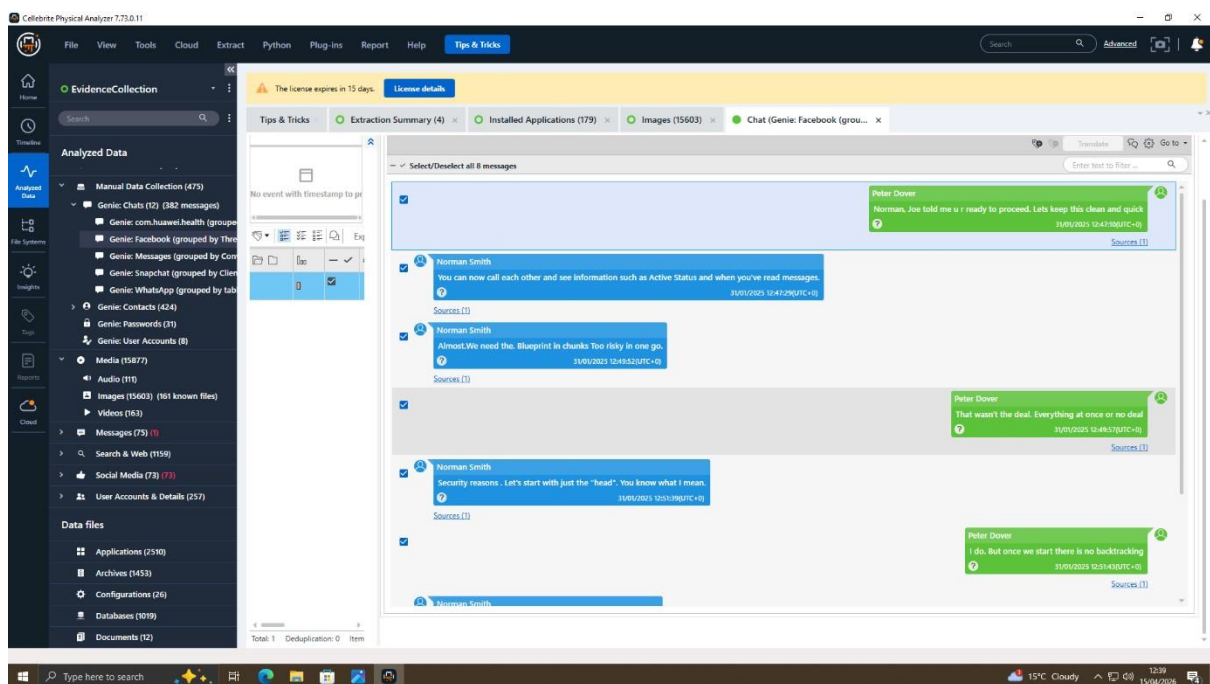


Figure 13: Emma chat with client

Figure 13 shows Norman being described as ready to proceed, indicating that he was not an incidental contact but an intended buyer.

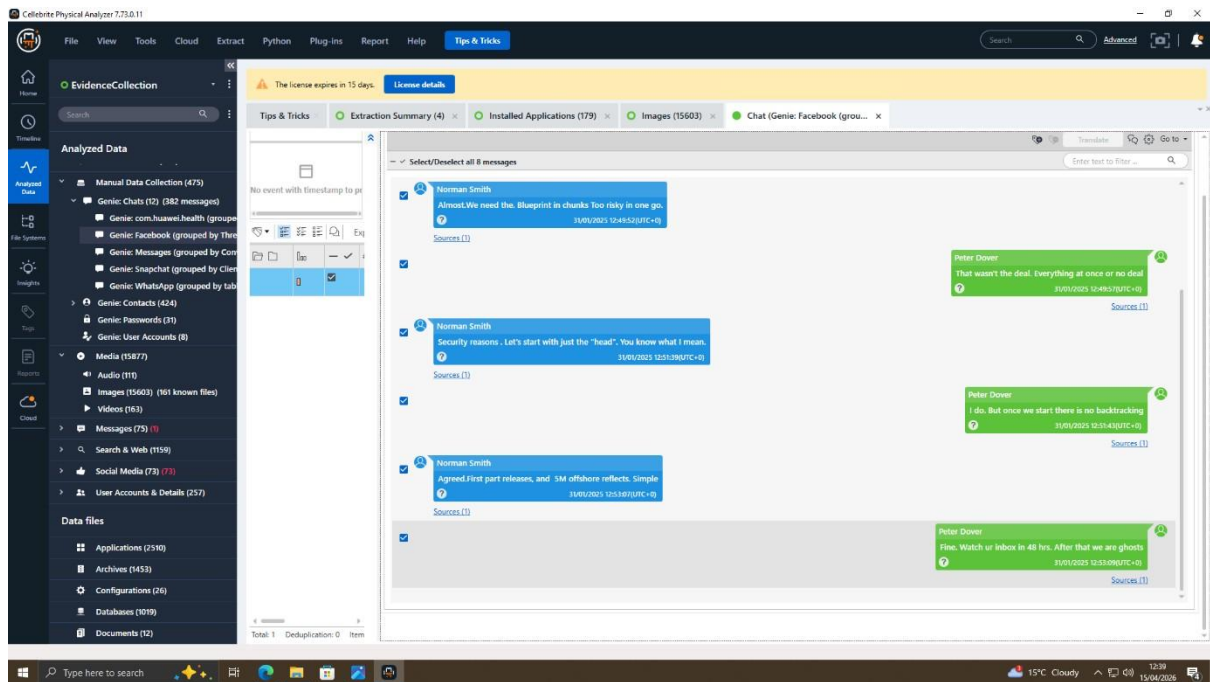


Figure 14: Emma final chat with client

Figure 14 shows Norman discussing receiving the blueprint in chunks and referencing offshore payment. This demonstrates awareness of both the material and the risks associated with transferring it.

2.5.3 Location and Travel

Location and travel artefacts support the communication timeline.

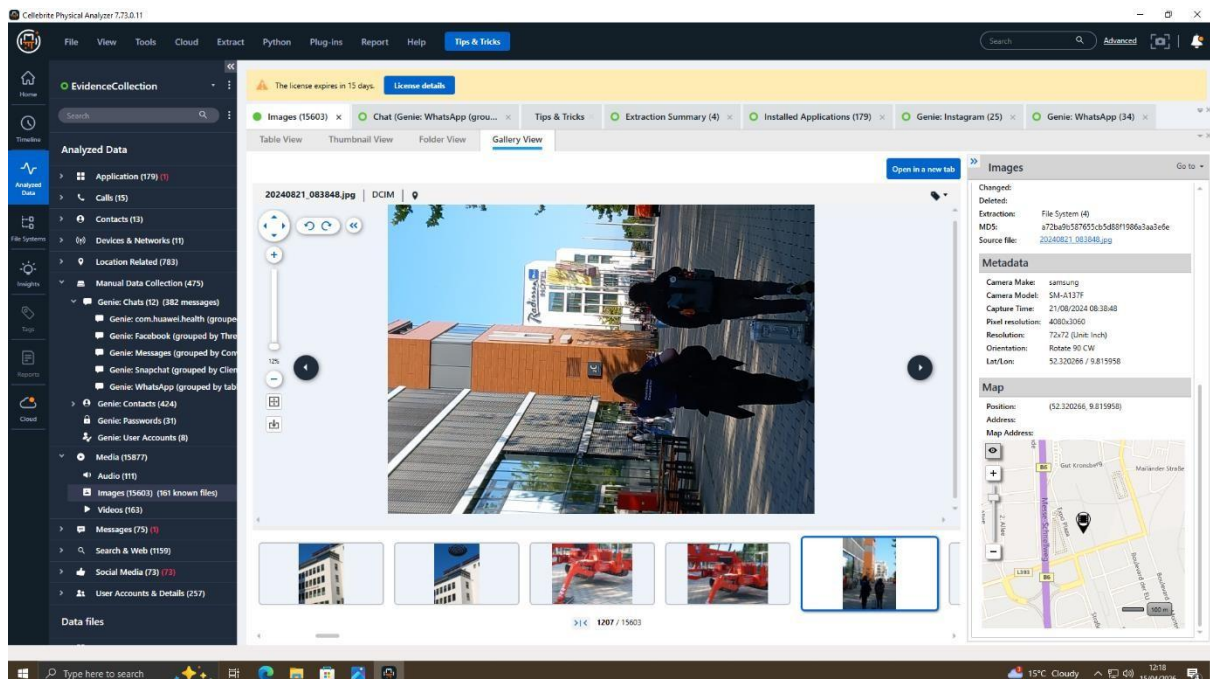


Figure 15: Joe meeting client in a hotel

Figure 15 shows a geo-tagged image placing a device at a hotel during the period Joe claimed to be meeting a client.

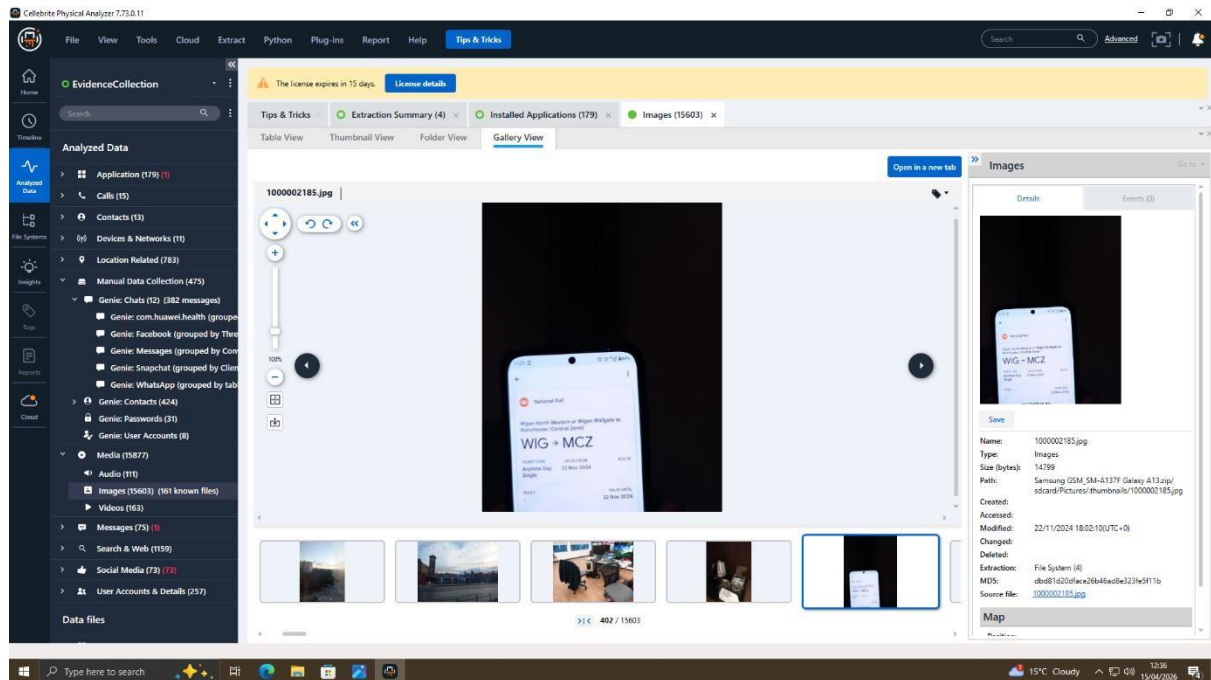


Figure 16: Joe meeting client in Glasgow

Figure 16 places a device in Glasgow, aligning with Joe's message about travelling there.

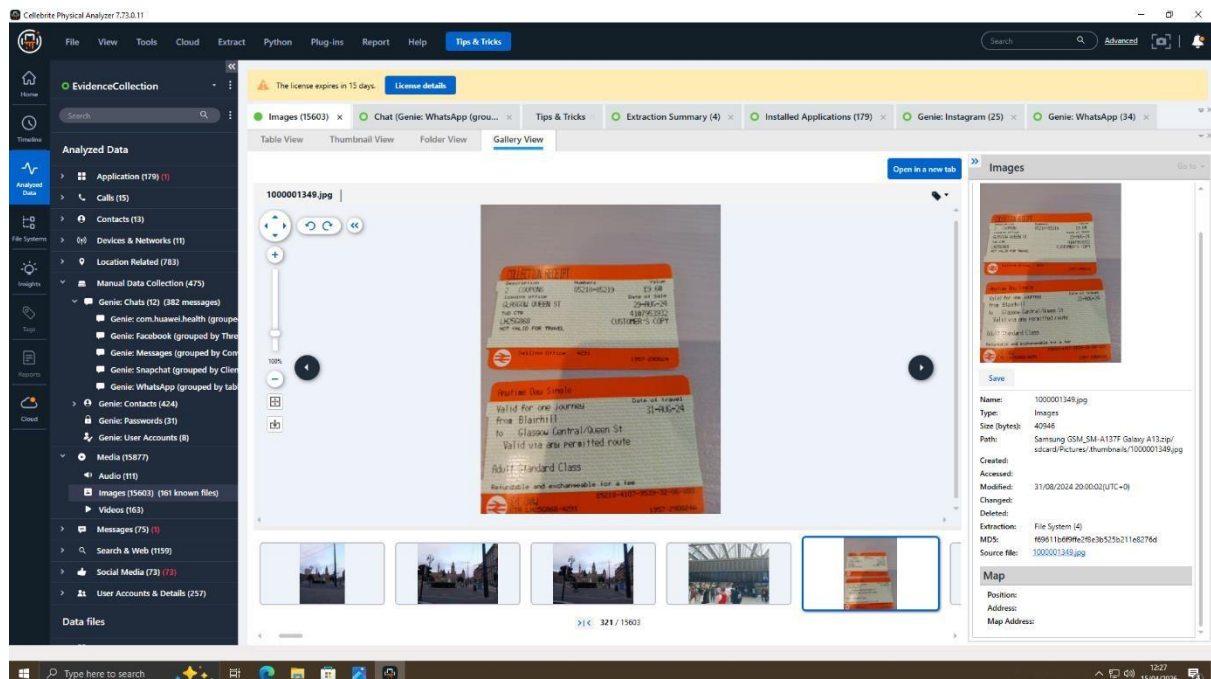


Figure 17: Joe meeting client in Manchester

Figure 17 shows photographs of train tickets, further supporting real-world movement during the negotiation period.

These artefacts corroborate the communication evidence and strengthen the overall narrative.

2.6 Suspect Role Assessment

Based on the artefacts:

- Emma appears to be the originator of the scheme. She initiated contact, identified the information as valuable, and controlled disclosure.
- Joe acted as the intermediary, contacting buyers, arranging meetings, and negotiating terms.
- Norman was positioned as the intended buyer, discussing staged transfer and offshore payment.

2.7 Conclusion

The evidence strongly supports the allegation that Emma, Joe, and Norman were involved in an attempted sale of Quantum Tech's confidential AI chip design. The communication pattern from initial disclosure to buyer sourcing, travel arrangements, and financial negotiation is consistent with attempted corporate espionage rather than innocent discussion.

2.8 Recommendations

- Preserve all devices, extraction outputs, and hash values to maintain evidential integrity.
- Conduct a deeper review for emails, deleted artefacts, and cloud-linked data.
- Verify the identities of all named contacts, including potential aliases.
- Strengthen internal controls around sensitive R&D assets, including access restrictions and monitoring.
- Consider referring the case to law-enforcement authorities for potential offences involving trade-secret theft and conspiracy.

List of figures

Figure 1: iPhone 13 Detected through Cellebrite Adapter

Figure 2: Files are being transferred

Figure 3: iPhone 13 extracted successfully

Figure 4: Huawei device image loading into physically analyser

Figure 5: Nokia device image loading into physically analyser

Figure 6: Samsung device image loading into physically analyser

Figure 7: Note 14 device image loading into physically analyser

Figure 8: Joe Marsh Contact Saved Previously

Figure 9: Chat started with Joe

Figure 10: Emma asked Joe to find buyer

Figure 11: Joe Travelling to Glasgow

Figure 12: Emma not giving full release and deal settlement

Figure 13: Emma chat with client

Figure 14: Emma final chat with client

Figure 15: Joe meeting client in a hotel

Figure 16: Joe meeting client in Glasgow

Figure 17: Joe meeting client in Manchester