

**Module: Digital Forensics Analysis**

**Name: MD. Mehedi Hasan Mixon**

**ID: 2436061**

## Table of Contents:

|                                                                 |    |
|-----------------------------------------------------------------|----|
| Task-1 Report -----                                             | 4  |
| Introduction -----                                              | 4  |
| Current state of the field: Tools, Feature & 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 -----                     | 6  |
| Conclusion -----                                                | 6  |
| References-----                                                 | 6  |
| Task-2 -----                                                    |    |
| 2.1 Device Collection -----                                     | 8  |
| 2.2 Case Background -----                                       | 8  |
| 2.3 Evidence Inventory -----                                    | 10 |
| 2.4 Methodology -----                                           | 10 |
| 2.5 Findings -----                                              | 12 |
| 2.5.1 Communication Evidence: Joe and Emma -----                | 12 |
| 2.5.2 Buyer side Communication: Norman -----                    | 16 |
| 2.5.3 Joe Meeting clients in different places -----             | 17 |
| 2.6 Suspect Role Assessment -----                               | 19 |
| 2.7 Conclusion -----                                            | 19 |

## List of Figures:

Figure-1: Device CPH2585 Detected in Cellebrite UFED

Figure-2: Files of different categories extracted from device

Figure-3: Extraction completed successfully of device

Figure-4: Huawei Device in Physical Analyzer

Figure-5: Samsung Device in Physical Analyzer

Figure-6: Note 14 Device in Physical Analyzer

Figure-7: Nokia C2 Device in Physical Analyzer

Figure-8: Emma started chat with Joe saying something sensitive

Figure-10: Joe was asked to find potential buyer

Figure-11: Joe going to Glasgow to meet clients

Figure-12: Deal settles with client

Figure-13: Emma initiated chat with the client

Figure-14: Agreed to release in small part rather than full release

Figure-15: Hotel location Identification

Figure-16: Joe Travelling Ticket

Figure-17: Glasgow train ticket

## Task-1: Report

### Introduction

Digital forensics is a specialised field that focuses on examining digital systems to uncover evidence related to cyber incidents. It involves a careful process of collecting, preserving, analysing, and presenting data so that it can be trusted in investigations or legal proceedings. In simple terms, it helps investigators answer key questions such as what happened, how it happened, and who was involved.

Over time, the scope of digital forensics has expanded significantly. It is no longer limited to traditional computers but now includes mobile devices, cloud services, networks, and even smart devices. Because modern systems are interconnected, digital evidence is often distributed across multiple platforms. This makes the investigation process more complex and requires a structured and disciplined approach.

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

The digital forensics field has evolved alongside advancements in technology. Today, investigators rely on a wide range of forensic tools designed to extract and analyse data from various sources. Examples include X-Ways Forensics, Oxygen Forensic Detective, Sleuth Kit, and Belkasoft Evidence Center.

These tools provide several useful capabilities. They can recover deleted data, analyse communication records, examine file metadata, and reconstruct timelines of user activity. This allows investigators to understand how a system was used and identify suspicious behaviour.

Another important feature is automation. Many modern tools can quickly scan large volumes of data and highlight relevant artefacts. This reduces manual effort and improves efficiency. However, automation must be used carefully, as it can sometimes overlook important context.

Despite these improvements, forensic tools still face limitations. Different tools may interpret data differently, which means results must be verified. Additionally, newer technologies such as encrypted storage and secure operating systems can restrict access to evidence. As highlighted in recent studies, the field is continuously adapting to overcome these technical barriers [1], [2].

## Intersection of Digital Forensics and Cybersecurity

Digital forensics and cybersecurity are closely related disciplines that often work together. Cybersecurity focuses on protecting systems and preventing attacks, while digital forensics focuses on analysing incidents after they occur.

In practical environments such as Security Operations Centers (SOC), forensic techniques are essential for understanding security alerts. When suspicious activity is detected, forensic analysis helps determine whether it is a real threat, how the attacker gained access, and what actions were performed.

For example, forensic analysis of system logs can reveal patterns of unauthorised access or data exfiltration. This information is crucial for responding to incidents and preventing further damage. Without digital forensics, organisations would struggle to fully understand cyber incidents and improve their security strategies [3].

## Emerging Trends in Digital Forensics

Digital forensics is constantly evolving as new technologies emerge. One of the most significant trends is the increasing importance of cloud forensics. As organisations store more data in cloud environments, investigators must rely on provider-generated logs and remote data sources. This introduces challenges such as limited control over data and dependency on third-party systems [4].

Another key trend is mobile and application forensics. Smartphones contain a large amount of personal and organisational data, making them a valuable source of evidence. Investigators now focus on extracting data from apps such as messaging platforms and social media.

The rise of big data and analytics is also influencing digital forensics. Investigators are dealing with massive datasets, which require advanced techniques to analyse efficiently. Machine learning is being explored to identify patterns and anomalies within large datasets [5].

These trends show that digital forensics is becoming more data-driven and requires continuous learning to keep up with technological changes.

## Key Challenges in Digital Forensics

Although digital forensics has advanced significantly, it still faces several challenges.

One major issue is the increasing volume of data. Modern devices generate large amounts of information, making it difficult to identify relevant evidence within a reasonable time frame.

Another challenge is data encryption and security controls. While these features protect user privacy, they can prevent investigators from accessing critical evidence. This creates a balance between privacy rights and investigative needs.

There is also the challenge of tool reliability and validation. Since forensic tools can produce different results, investigators must verify findings carefully to ensure accuracy. This is especially important when evidence is used in legal cases.

Legal and jurisdictional issues further complicate investigations. Data stored in cloud environments may be in different countries, making it difficult to obtain access due to varying laws and regulations.

Finally, the field faces a shortage of skilled professionals. Digital forensics requires both technical expertise and analytical thinking, which can be difficult to develop and maintain [6].

## National and International Job Market

The demand for digital forensics and cybersecurity professionals is growing rapidly across the world. Organisations are increasingly facing cyber threats, which creates a strong need for experts who can investigate and respond to incidents.

In the UK, the cybersecurity job market continues to expand, with many roles requiring knowledge of digital investigations. Positions such as SOC Analyst, Digital Forensic Investigator, and Incident Responder are becoming more common.

Internationally, the demand is even higher. Reports indicate that there is a significant shortage of cybersecurity professionals globally. In the United States, job growth in information security roles is projected to remain strong for the coming years [7].

This demand makes digital forensics a valuable career path. It not only offers opportunities in specialised roles but also serves as a foundation for broader cybersecurity careers.

## Conclusion

Digital forensics has become an essential discipline in today's digital world. It provides the ability to investigate cyber incidents and uncover the truth behind digital activities.

While the field benefits from advanced tools and techniques, it also faces challenges such as large data volumes, encryption, and legal complexities. At the same time, emerging technologies like cloud computing and data analytics are shaping the future of investigations.

Overall, digital forensics plays a critical role in maintaining security and accountability in digital environments. As technology continues to evolve, the importance of this field will only increase.

## References

- [1] I. Baggili, A. Marrington and C. Valli, *Digital Forensics and Cyber Crime*, Springer, 2020.
- [2] N. Behl and K. Behl, "Cybersecurity and cyberwar: What everyone needs to know," Oxford University Press, 2021.
- [3] J. R. Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 3rd ed., Laxmi Publications, 2020.
- [4] M. Kohn, M. Eloff and J. Eloff, "Integrated digital forensic process model," *Computers & Security*, vol. 38, pp. 103–115, 2020.
- [5] S. Alqahtani, "Big data analytics in digital forensics: Opportunities and challenges," *Journal of Digital Investigation*, 2022.
- [6] A. Pichan, M. Lazarescu and S. Soh, "Cloud forensics: Technical challenges and solutions," *IEEE Access*, vol. 8, pp. 190–210, 2020.
- [7] U.S. Bureau of Labor Statistics, "Information Security Analysts Occupational Outlook," 2024.

## Task-2

### 2.1 Device Collection

The mobile-device examination's acquisition and preparation phases are captured in the photographs. The device that Cellebrite UFED is recognizing is shown in Figure 1. This demonstrates that an industry-standard forensic instrument with structured capture and information retention capabilities was used to start the extraction process.

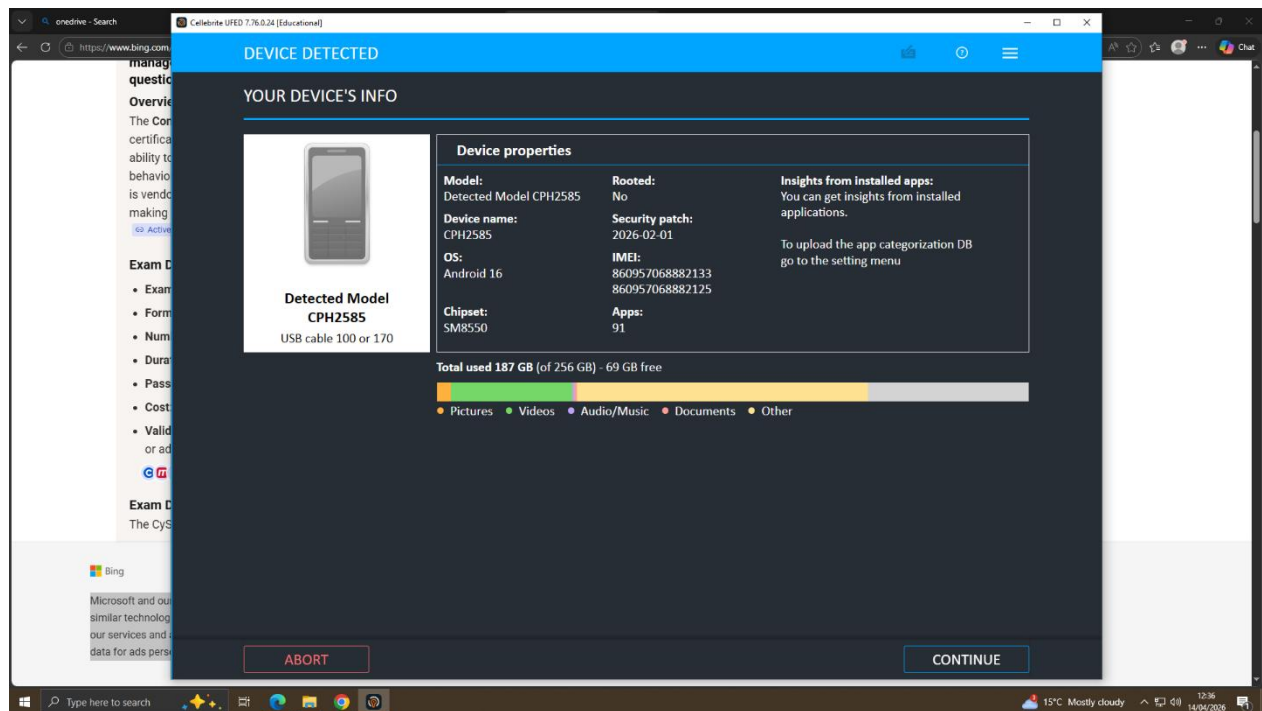


Figure -1: Device CPH2585 Detected in Cellebrite UFED

The extraction process is shown in Figure 2. The screenshot shows that instead of manually searching the device, the examiner chose kinds of artifacts. This demonstrates that the acquisition followed a methodical, repeatable procedure and bolsters the methodology's dependability.

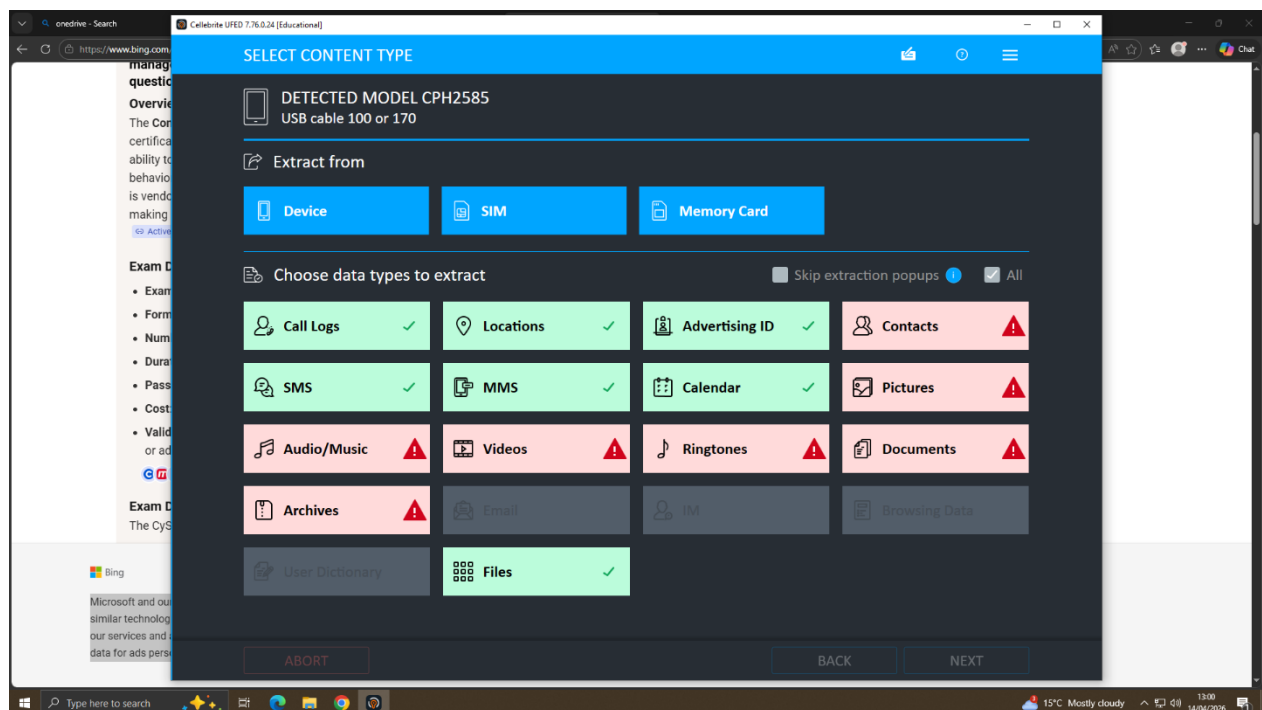


Figure-2: Files of different categories extracted from device

The satisfactory completion of the extraction is confirmed in Figure 3. Messages, contacts, call logs, media files, and location data were among the several types of evidence that were recorded. This serves as the supporting evidence for the analysis that follows in Physical Analyzer.

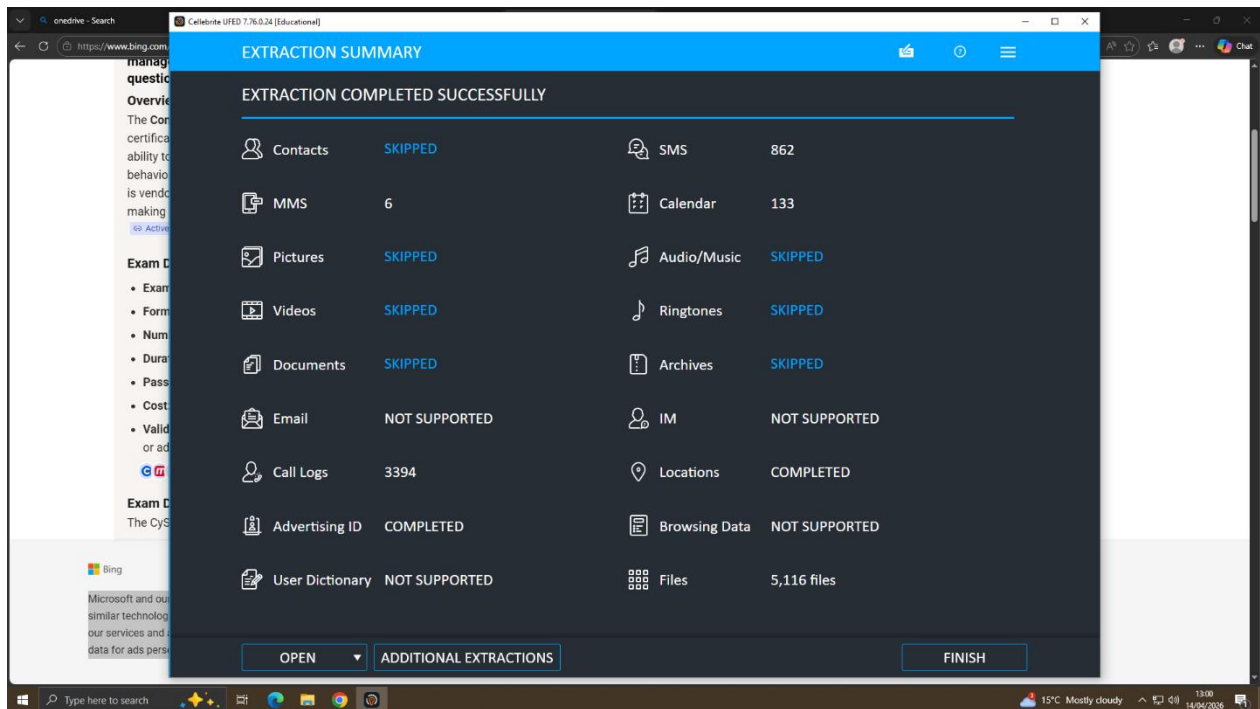


Figure-3: Extraction completed successfully of device

## 2.2 Case Background

Suspicious access to Quantum Tech's proprietary AI chip design, known as QT-AI-2025, was reported. Emma, a freshly hired senior engineer, was identified as a possible insider threat by internal surveillance. She was accused of trying to give private information to a third party. Norman seemed to be the intended buyer, and Joe was thought to be the middleman enabling contact with him. This forensic review's goal was to ascertain whether the allegation of attempted intellectual property theft is supported by the digital artifacts that are currently available.

## 2.3 Evidence Inventory

Four photos of mobile devices the Huawei POT-LX1, Nokia C2, Samsung Galaxy A13, and Note 14 made up the proof. The following screenshots were taken from these pictures:

- listings of contacts
- SMS and WhatsApp message threads
- logs on social media
- location-specific information
- A document-archive artifact

The screenshots chain-of-custody indicators and hash values show that the data came from a professional forensic methodology rather than casual device surfing. This guarantees that the artifacts may be trusted for analysis and protects evidentiary integrity.

## 2.4 Methodology

An organized forensic method was used in the investigation:

- Acquisition Cellebrite Physical Analyzer rebuilt the file systems and made artifacts available for examination by loading the supplied device pictures.
- Integrity Verification Hash values (MD5/SHA-256) were tested right away after intake to make sure the extracted data didn't change. Maintaining the trustworthiness of the evidence depends on this stage.
- Additional artifacts from third-party programs were found using Enhanced Artefact Discovery Cellebrite App Genie. Heuristic analysis is used by this tool to decode app specific data that conventional parsing might miss.

The device-recognition and hash-verification phases for every handset are shown in Figures 4 through 8, proving that the acquisition was carried out correctly.

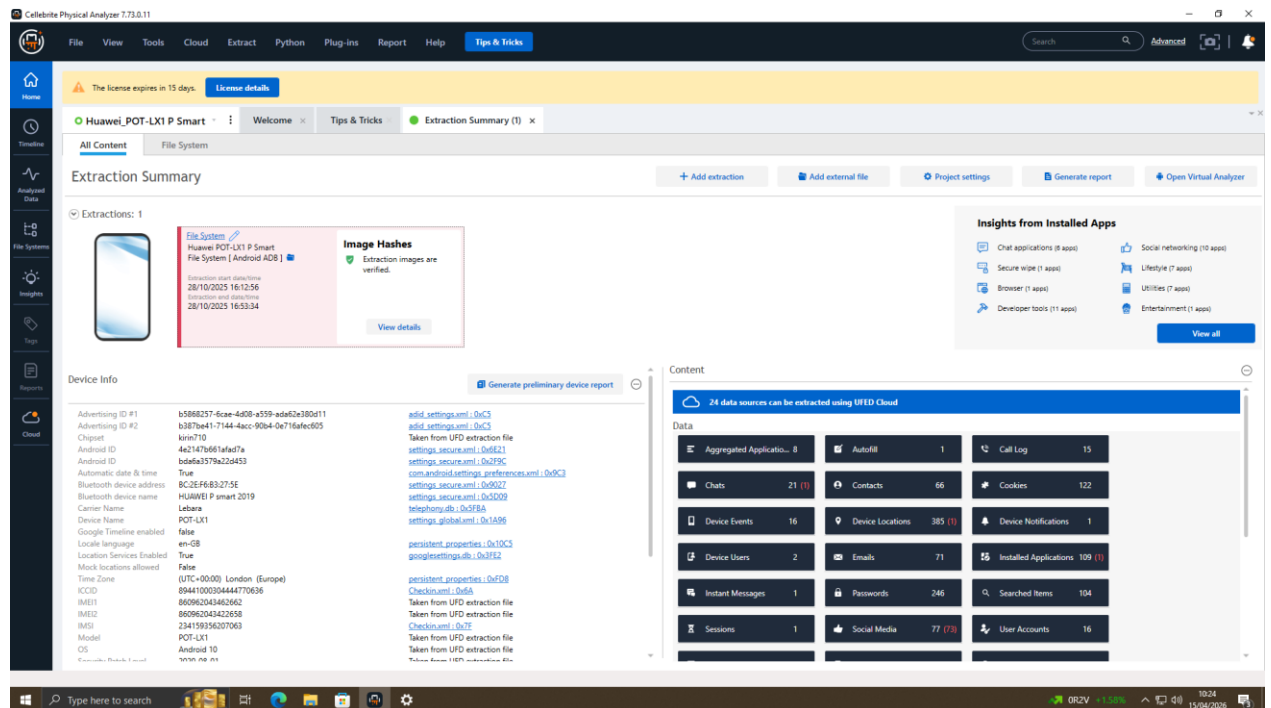


Figure-4: Huawei Device in Physical Analyzer

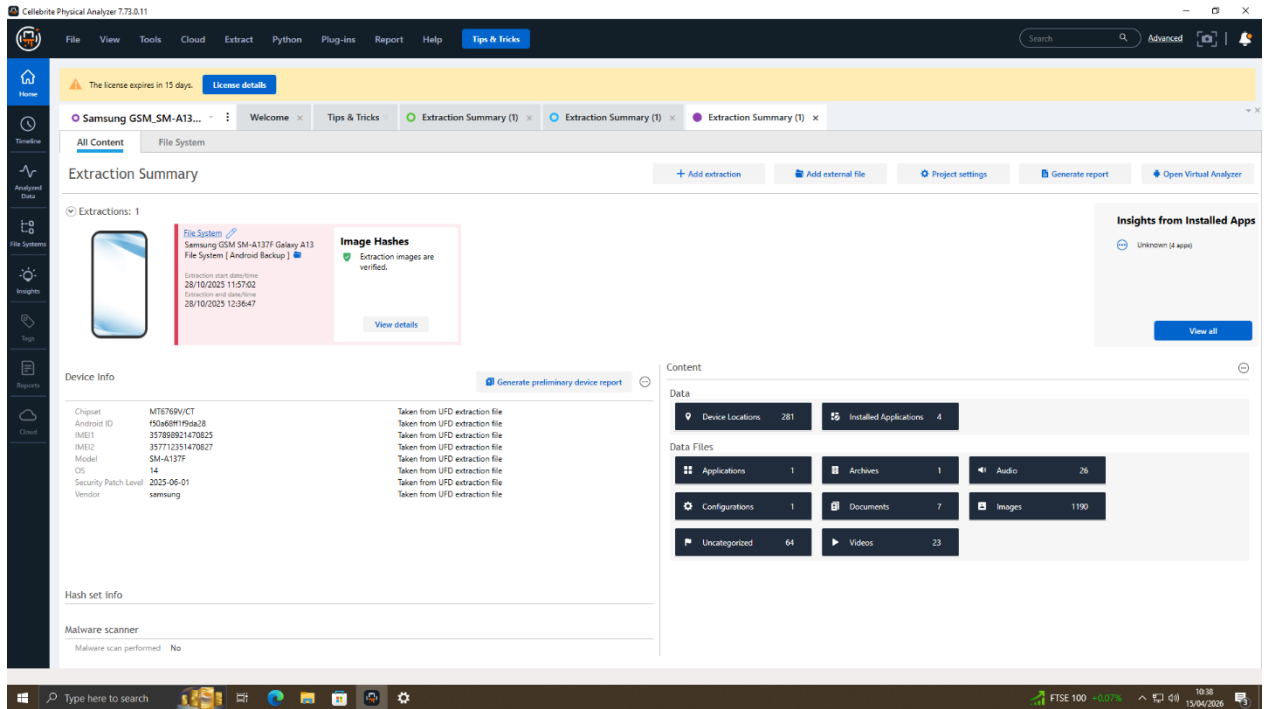


Figure-5: Samsung Device in Physical Analyzer

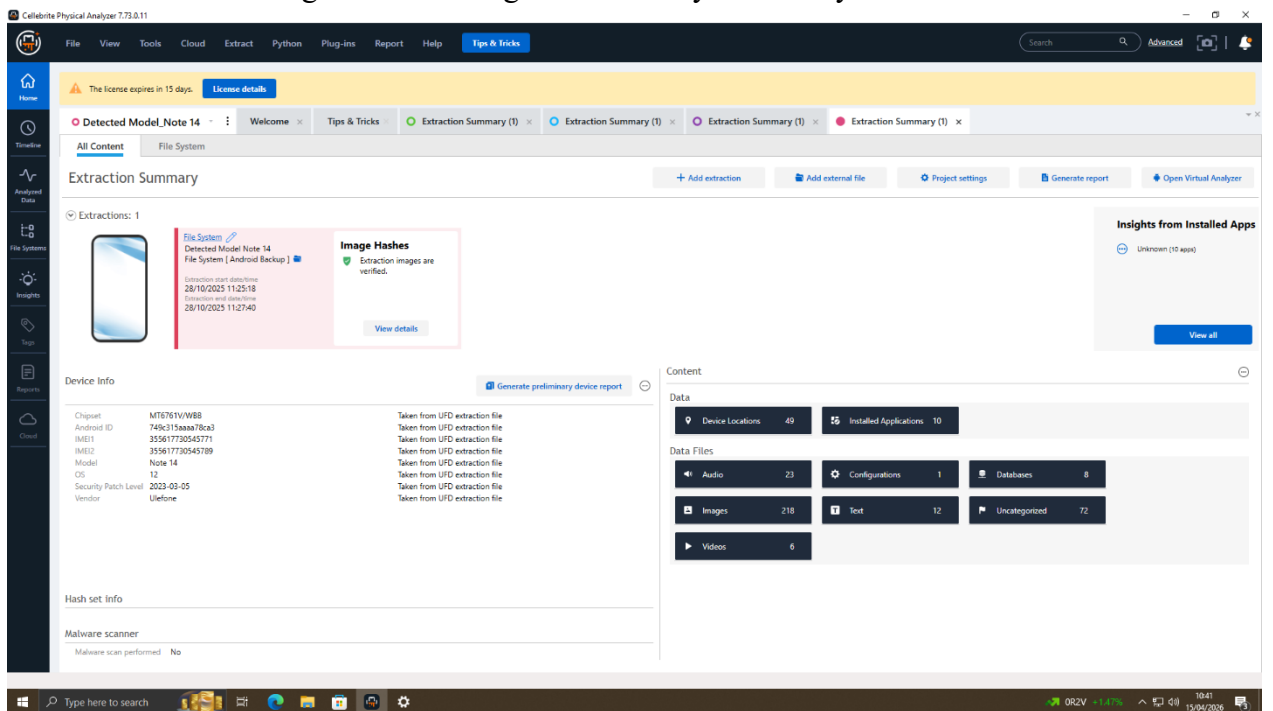


Figure-6: Note 14 Device in Physical Analyzer

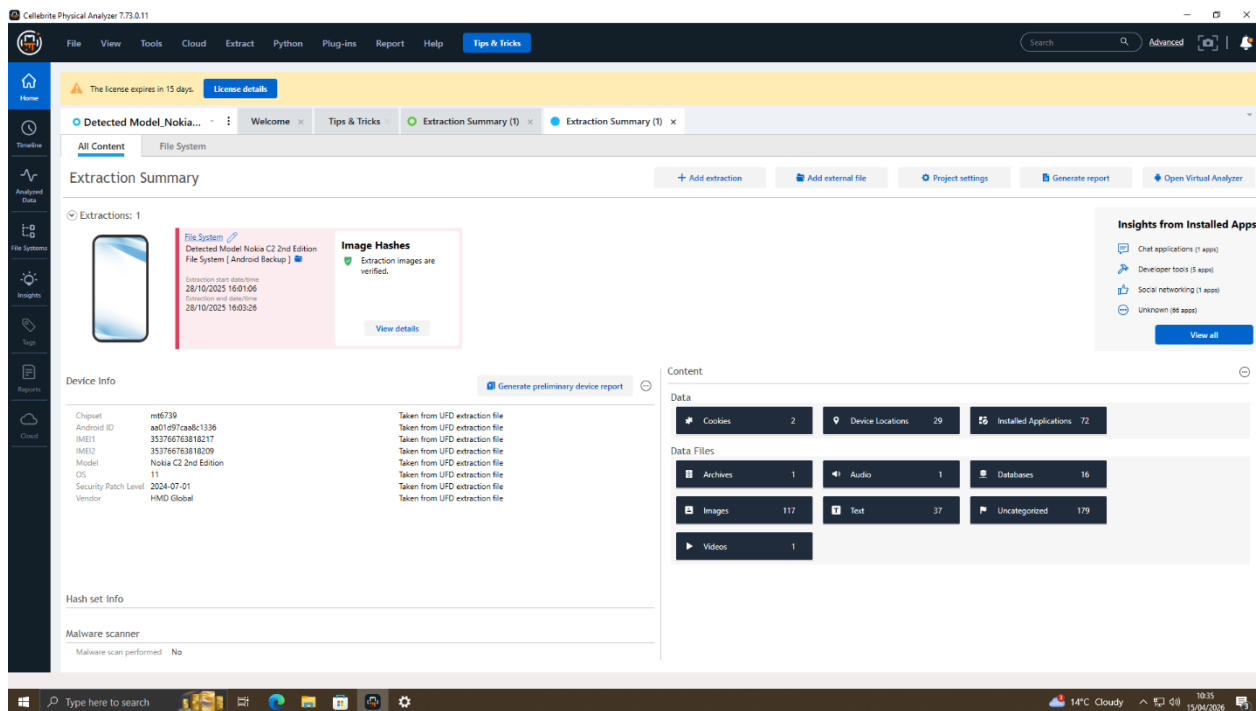


Figure-7: Nokia C2 Device in Physical Analyzer

## 2.5 Findings

### 2.5.1 Communication Evidence: Emma and Joe

Emma is seen approaching Joe about "something sensitive" in the earliest pertinent message, which is dated August 21, 2024. This suggests that she started the private conversation.

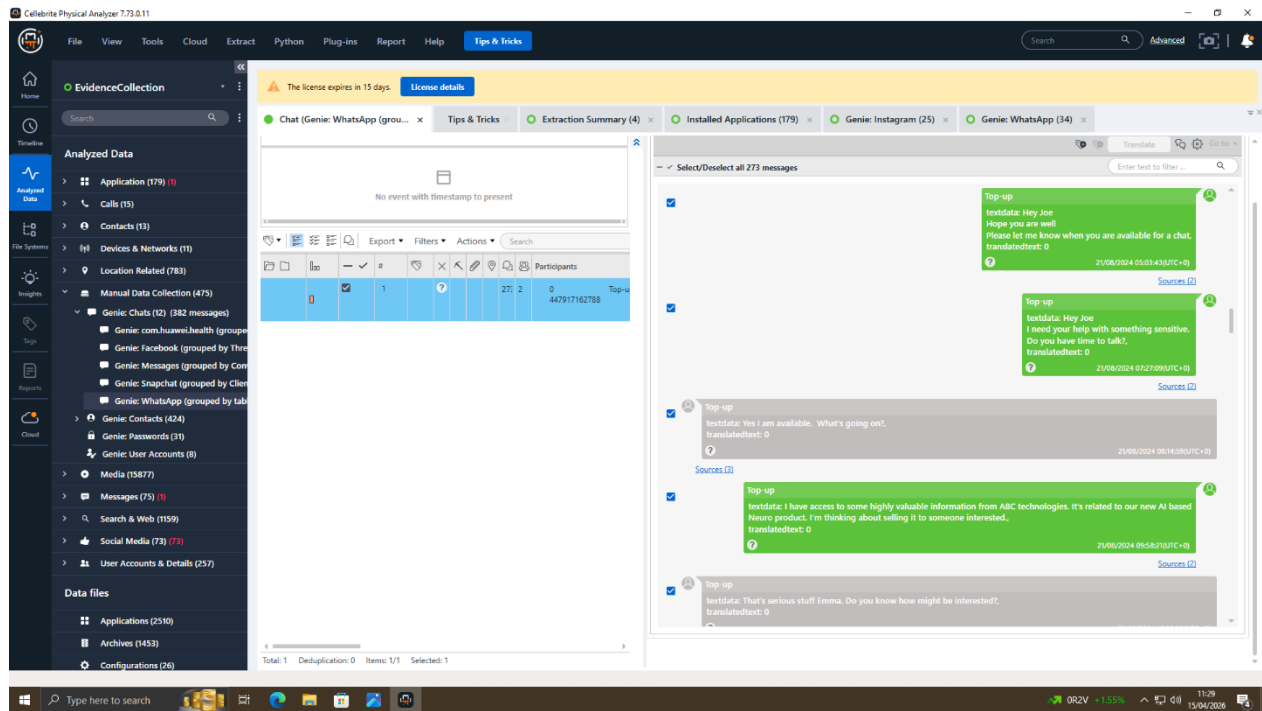


Figure-8: Emma started chat with Joe saying something sensitive

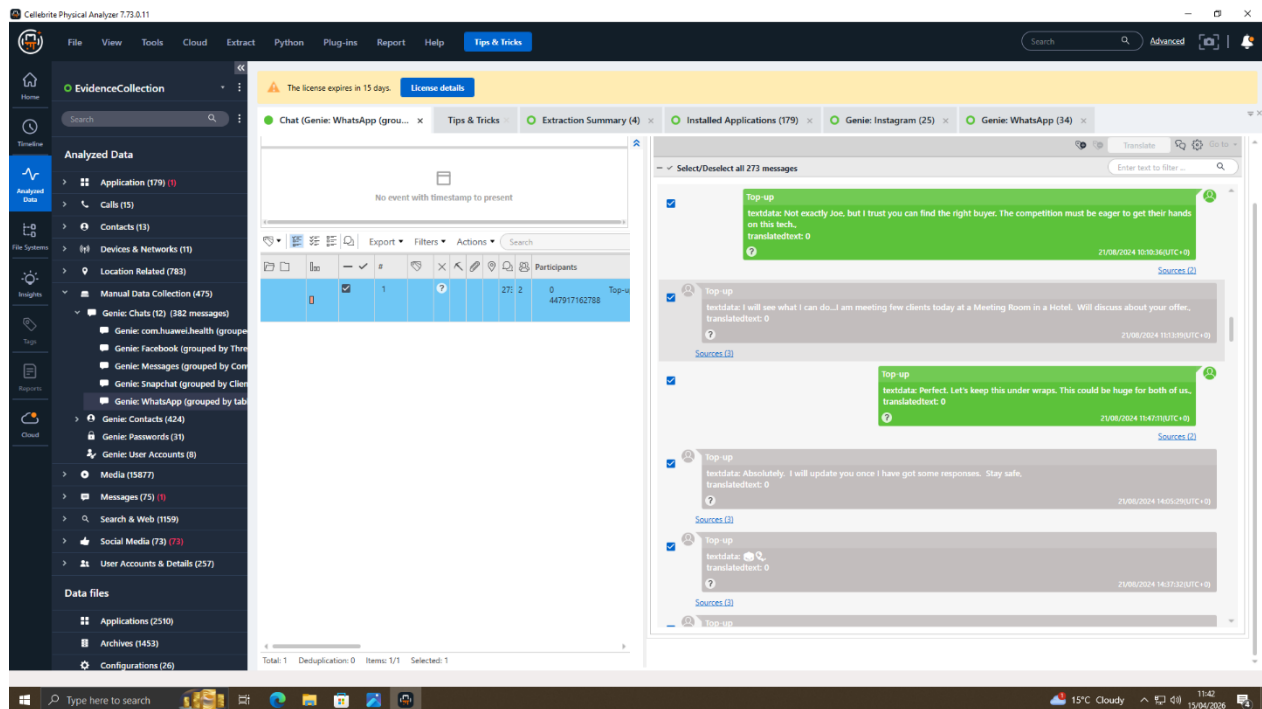


Figure-9: Joe was asked to find potential buyer

Emma presents the issue as delicate in her first message, which is depicted in Figure 9. This implies intentionality as opposed to informal discourse. It is especially important. Emma claims to have

access to extremely valuable information about AI and suggests that it might be sold. One of the most obvious signs of a desire to reveal confidential information is this.

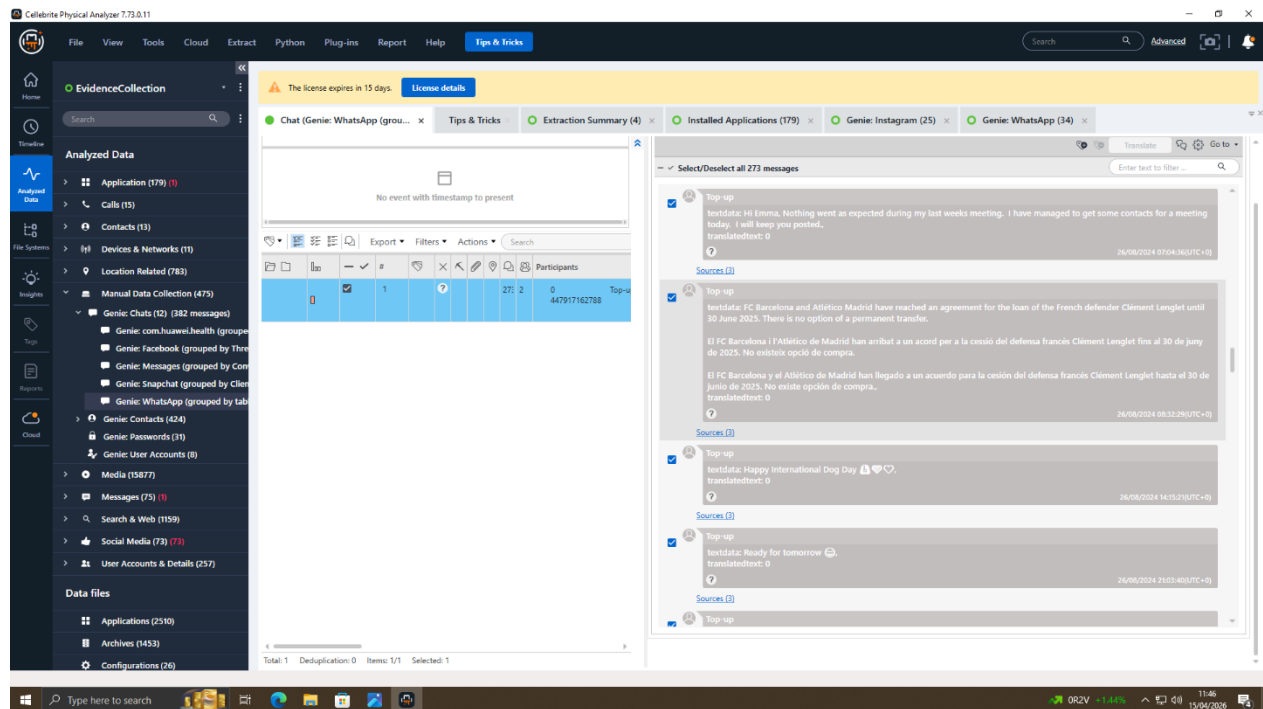


Figure-10: Joe updating that he is looking for buyer

After that, the topic of operational planning comes up. In Figure 10, Joe responds that he is already meeting clients when Emma asks him to find a suitable buyer. Joe's function as an active middleman is thus established.

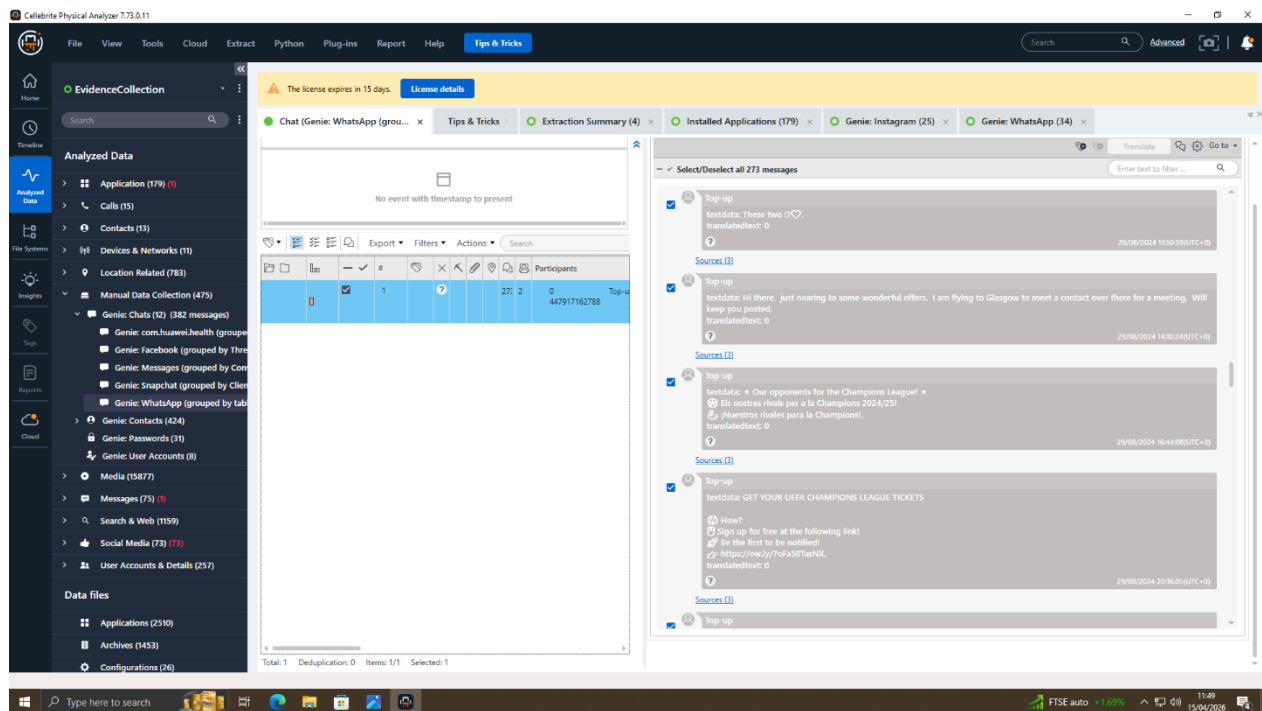


Figure-11: Joe going to Glasgow to meet clients

Joe tells Emma that he is going to Glasgow to meet a contact in Figure 11. This shows that the conversations moved beyond message to actual agreements.

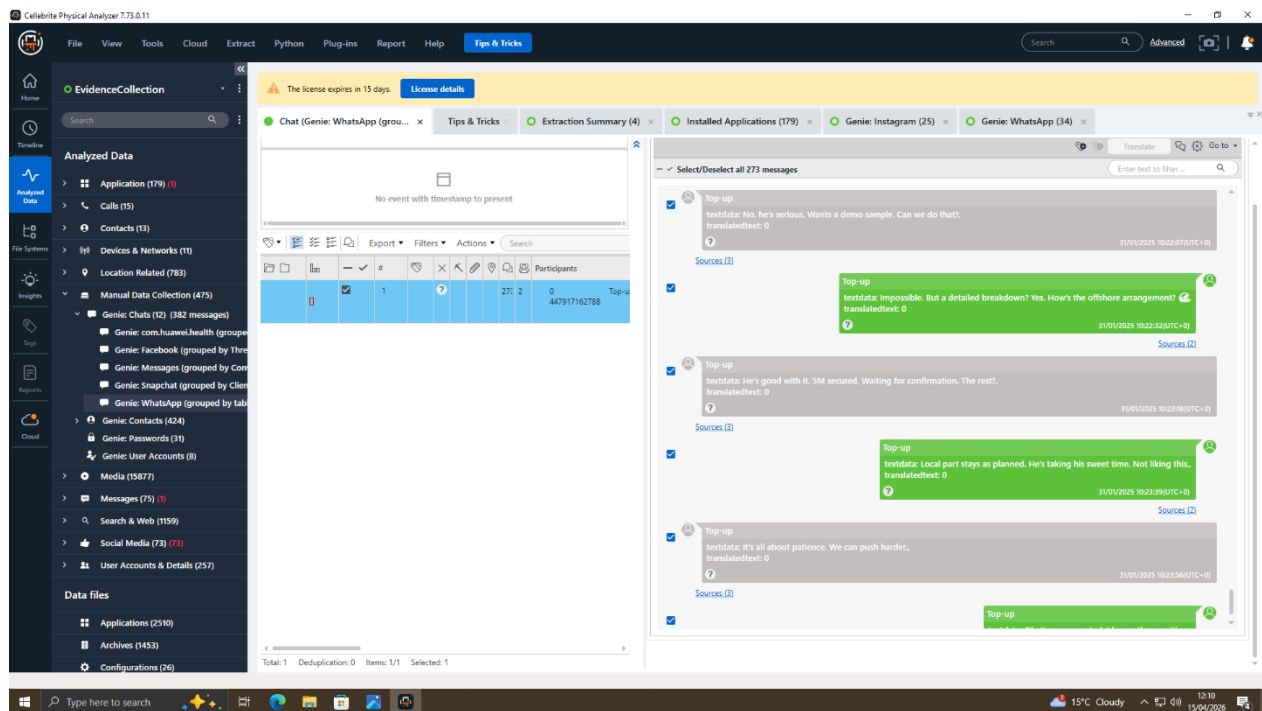


Figure-12: Deal settles with client

The most damning conversation takes place on January 31, 2025. Emma is seen in Figure 12 agreeing to give a thorough analysis but declining to release a whole sample. This method of staged release aligns with the controlled disclosure of sensitive information. Emma confirms that the local portion of the payment has not changed, while Joe declares that "5M" has been obtained. This provides compelling evidence that the proposed transaction was the subject of a financial negotiation.

## 2.5.2 Buyer-Side Communication: Norman

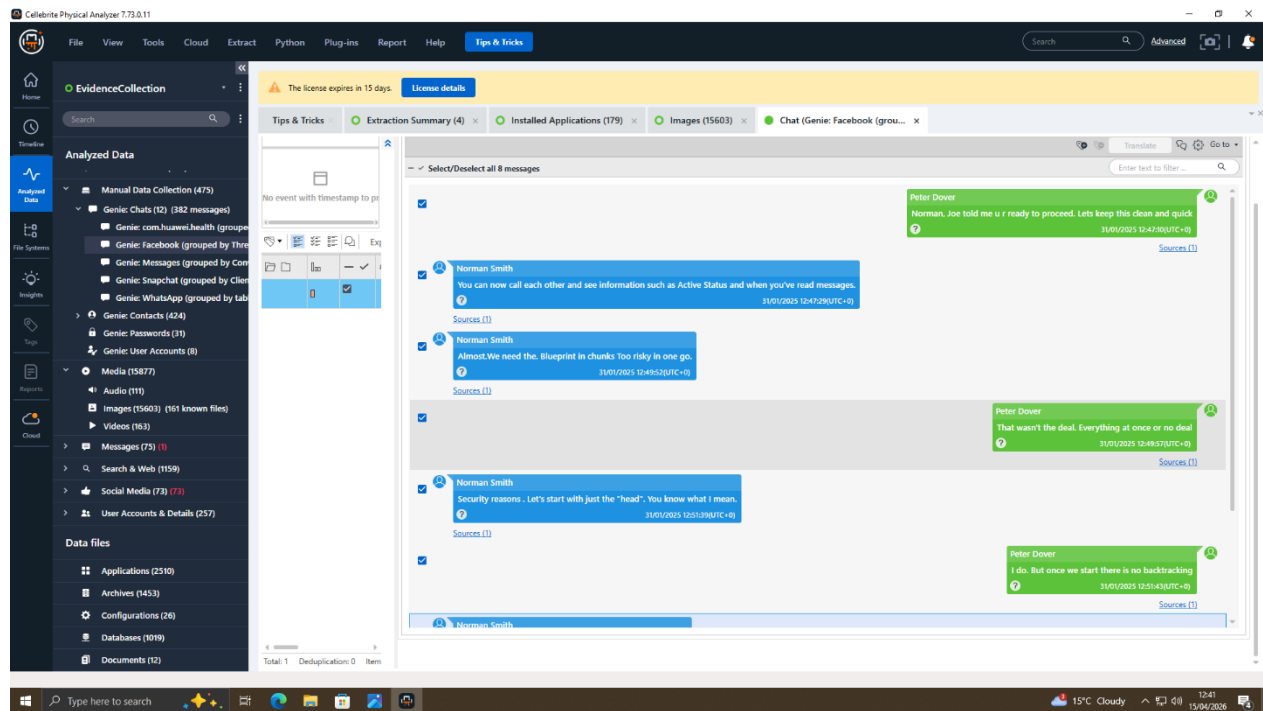


Figure-13: Emma initiated chat with the client

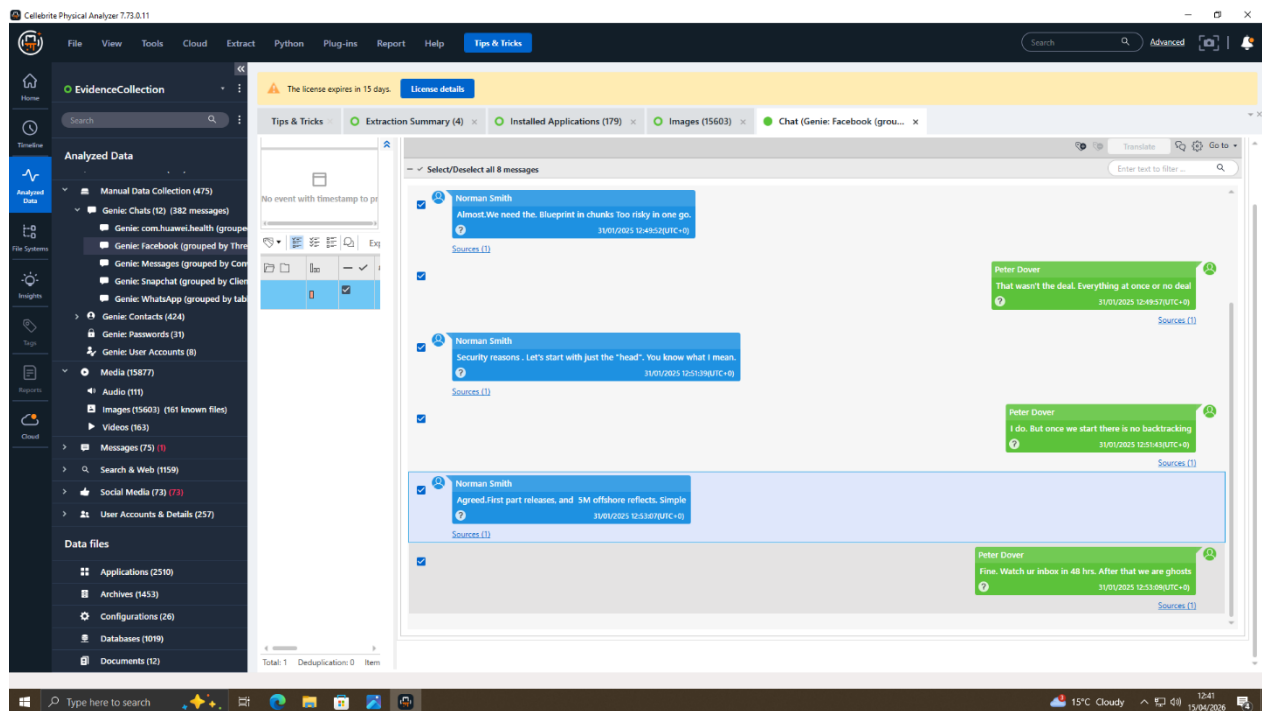


Figure-14: Agreed to release in small part rather than full release

### 2.5.3 Joe Metting Clients in Different Places

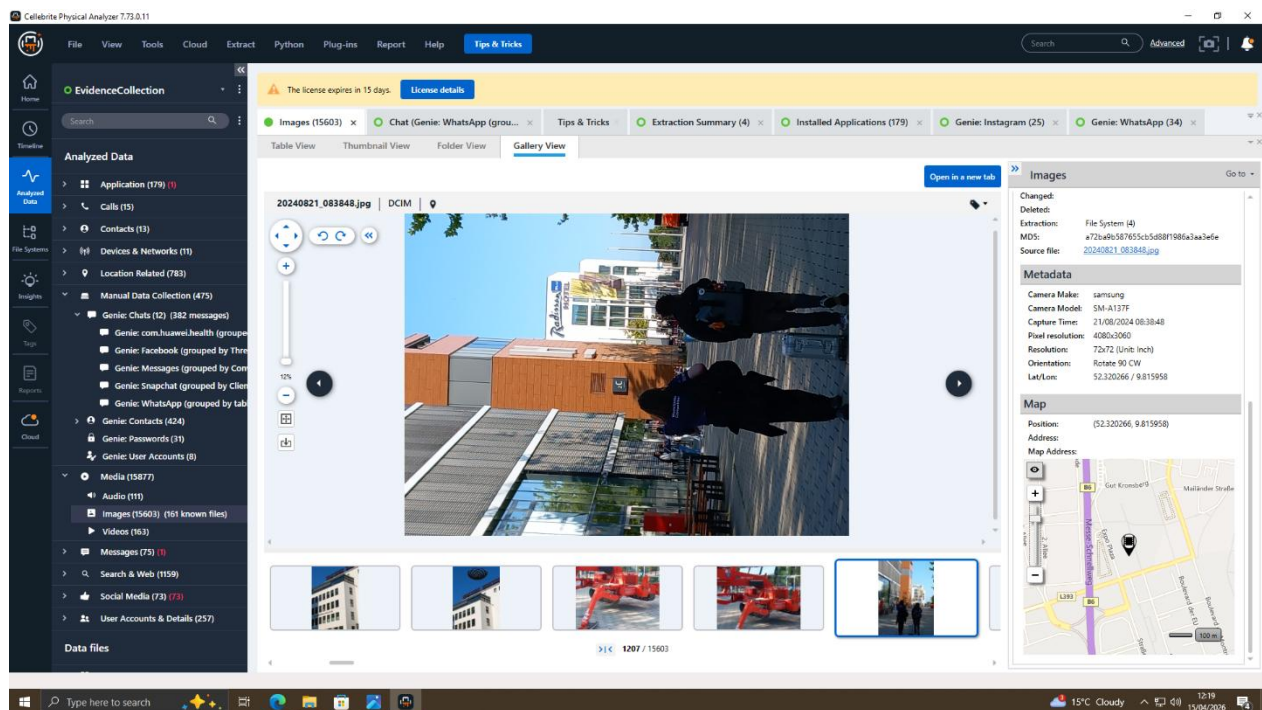


Figure-15: Hotel location Identification

Figure 15 stated when Joe was talking with Emma, he stated that he was meeting with client in a hotel.

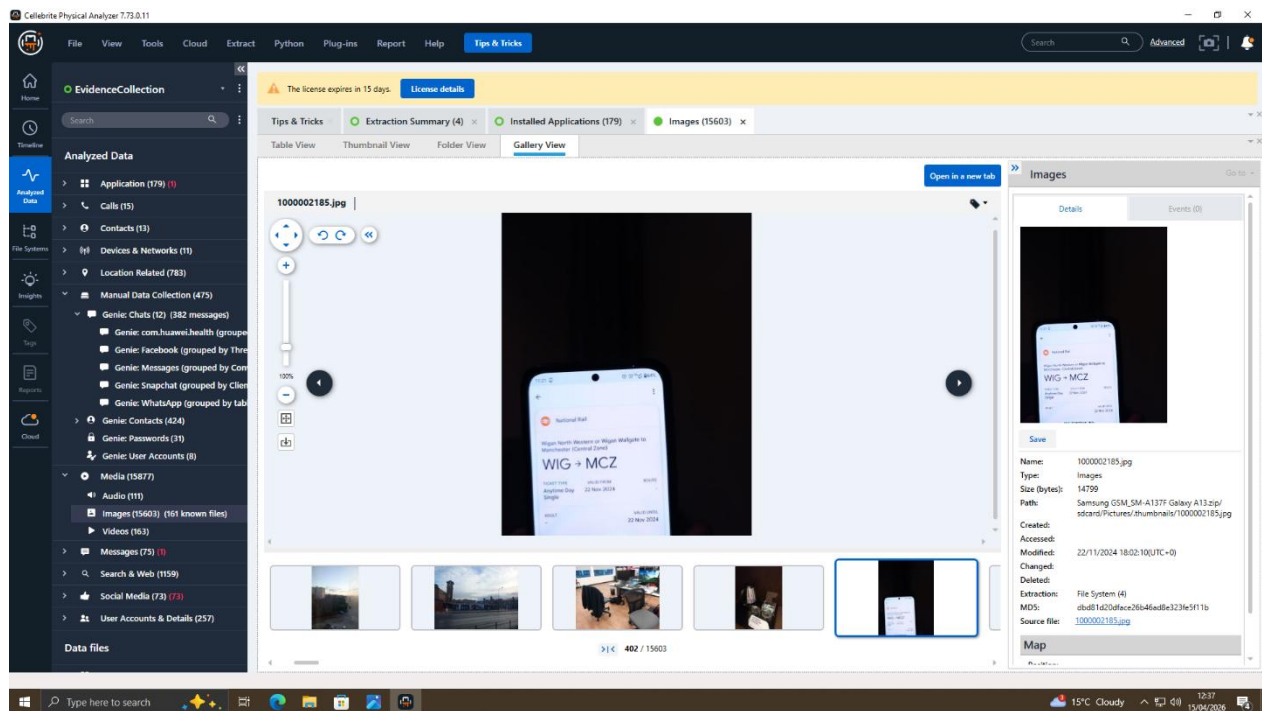


Figure-16: Joe Travelling Ticket

Figure 16 states that Joe was going to Manchester to meet clients and this is the picture of the ticket.

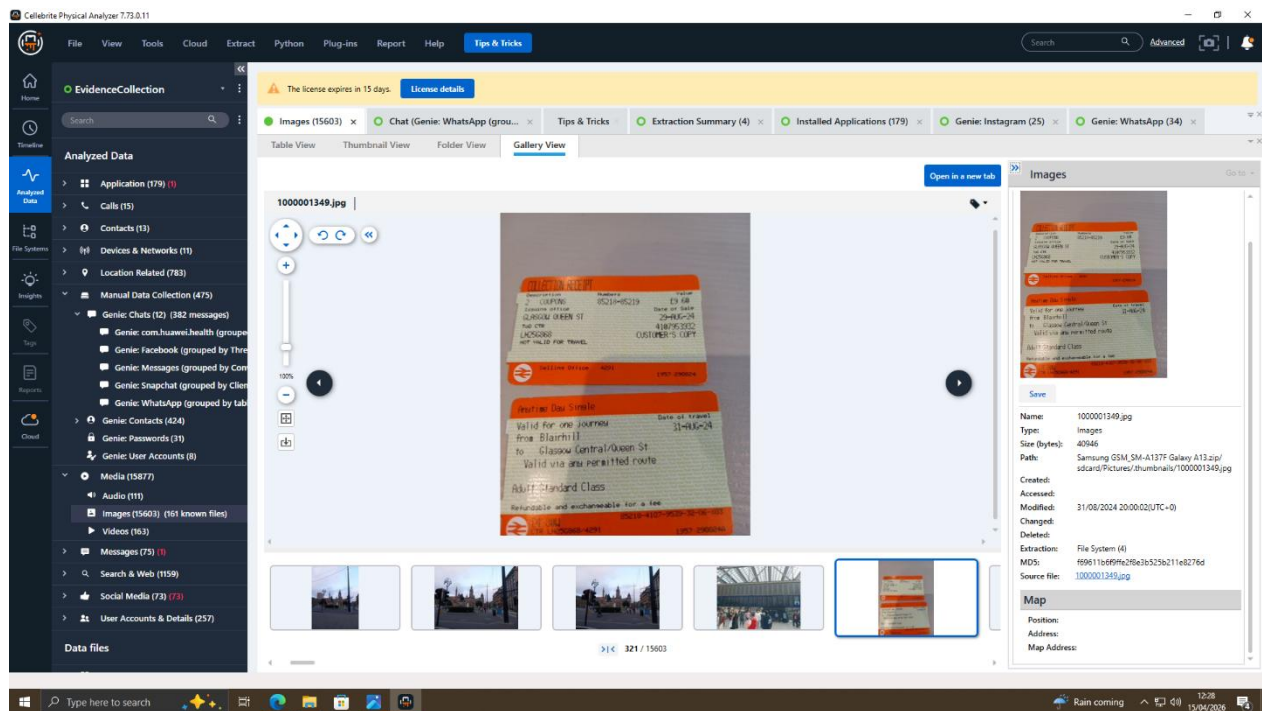


Figure-17: Glasgow train ticket

## 2.6 Suspect Role Assessment

- Emma seems to have come up with the plan. She made the first move, determined that the material was important, and managed disclosure.
- Joe served as the go-between, reaching out to purchasers, setting up meetings, and negotiating conditions.
- Staged transfer and offshore payment were discussed with Norman, who was positioned as the intended buyer.

## 2.7 Conclusion

The claim that Emma, Joe, and Norman participated in an attempt to sell Quantum Tech's proprietary AI chip design is amply supported by the evidence. From the first revelation to buyer sourcing, vacation plans, and financial negotiations, the communication pattern is more in line with attempted corporate espionage than with casual conversation.