

Module: Digital Forensics Analysis

Name: MD. Alif Khan

ID: 2434999

Table of Contents:

Task-1 Research 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 -----	5
Conclusion -----	6
References-----	6
Task-2 -----	7
2.1 Device Collection -----	7
2.2 Case Background -----	9
2.3 Evidence Inventory -----	9
2.4 Methodology -----	9
2.5 Findings -----	12
2.5.1 Communication Evidence -----	12
2.5.2 Buyer side Communication -----	16
2.6 Suspect Role Assessment -----	19
2.7 Conclusion -----	19
2.8 Recommendations -----	19

List of Figures:

- Figure-1: Device Samsung A22 Detected in Cellebrite UFED
- Figure-2: Files with lot of categories extracted from device
- Figure-3: Extraction completed successfully for Samsung A22
- 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 stating to Joe saying something sensitive
- Figure-9: Joe was instructed to find buyer for the patent
- Figure-10: Joe Managing Meeting with clients and acting as a middleman
- Figure-11: Joe went to Glasgow to meet client
- Figure-12: Joe and Emma both deal settled with client
- Figure-13: Emma initiated chat with Norman
- Figure-14: Emma and Norman agreed to release in chunks rather than full release
- Figure-15: Manchester ticket showing proof that Joe went there
- Figure-16: Glasgow Train Ticket proof joe went there
- Figure-17: Hotel picture with the location

Task-1

Introduction

Examining digital systems to find and analyse evidence connected to cyber incidents is the subject of the cybersecurity profession known as "digital forensics." It adheres to a methodical procedure in which information is gathered, stored, examined, and presented in a manner that guarantees dependability and trustworthiness. Reconstructing events and giving a clear picture of what happened in a digital context is the primary goal.

In the past, standalone computers were the primary focus of research. However, because to the quick development of technology, digital evidence is now produced on a variety of platforms, including networks, mobile devices, cloud services, and smart systems. Because data is frequently dispersed and fractured across various sources, modern investigations are therefore more complicated. Consequently, digital forensics has become an essential field.

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

The capabilities of digital forensics have been greatly impacted by the advancement of cutting edge technologies. These days, investigators gather and examine evidence from digital devices using a range of specialized technologies, like Magnet AXIOM, X-Ways Forensics, Cellebrite, and Autopsy.

These programs are made to do things like find hidden artifacts, analyse system logs, recover deleted files, and extract communication records. The ability to generate timelines, which assist investigators in understanding user behaviours in chronological sequence, is one of the most useful

capabilities. In addition, modern tools incorporate automation to process large volumes of data efficiently. This allows investigators to focus on relevant findings rather than manually reviewing every piece of information. However, automation should not be fully relied upon, as it may overlook subtle details that require human interpretation.

Intersection of Digital Forensics and Cybersecurity

Within the larger topic of cybersecurity, digital forensics is essential. Digital forensics is in charge of looking into incidents and determining their consequences, whereas cybersecurity seeks to stop and fight against attacks.

Both disciplines collaborate in real-world settings such as Security Operations Centers (SOC). Forensic techniques are used to analyze logs, track attacker behavior, and ascertain how the system was infiltrated when a possible threat is identified. Organizations can enhance their defensive tactics and respond more successfully thanks to this approach.

For instance, analysing network logs can reveal patterns of unauthorised access or data transfer. This information is essential for identifying vulnerabilities and preventing future attacks. Without forensic analysis, organisations would lack the insight needed to fully understand cyber incidents and their consequences [3].

Emerging Trends in Digital Forensics

As technology continues to advance, digital forensics is also evolving. One major trend is the increasing reliance on cloud-based investigations. Since many organisations store their data in cloud environments, investigators must depend on cloud service providers for access to logs and system information. This introduces challenges related to data control and legal jurisdiction [4].

Another important development is the focus on mobile and application forensics. Smartphones contain a large amount of personal and professional data, making them a key source of evidence. Investigators now analyse application data such as messaging apps, emails, and social media platforms. The use of data analytics and machine learning is also growing. These technologies help investigators process large datasets more efficiently and identify patterns that may not be immediately visible. However, human validation remains essential to ensure accuracy and avoid misinterpretation [5]. These trends indicate that digital forensics is becoming more advanced and requires continuous adaptation to new technologies.

Key Challenges in Digital Forensics

The use of encryption and security technologies. While these features protect user privacy, they can also restrict access to important data needed for investigations.

There are also concerns regarding tool accuracy and consistency. Since different tools may produce different results, investigators must carefully verify their findings to ensure reliability. This is especially important in legal contexts where evidence must be accurate and defensible.

Legal complexities also play a role, particularly when data is stored across multiple regions. Differences in laws and regulations can make it difficult to access and analyse evidence.

National and International Job Market

Globally, there is an increasing need for experts in cybersecurity and digital forensics. As organisations face increasing cyber threats, there is a strong need for individuals who can investigate and respond to incidents effectively.

Cybersecurity-related jobs are steadily increasing in the UK, and many of them call for familiarity with digital investigations. Jobs like SOC analyst, incident responder, and forensic analyst are becoming increasingly prevalent.

On a global scale, the demand is even higher. Reports indicate a significant shortage of skilled cybersecurity professionals worldwide. In the United States, employment opportunities in information security are expected to grow steadily over the next decade [7]. This growing demand makes digital forensics an attractive career option. It not only provides opportunities in specialised roles but also serves as a gateway into broader areas of cybersecurity.

Conclusion

Digital forensics has become a crucial part of contemporary cybersecurity procedures. It makes it possible for organizations to look into situations, comprehend digital activity, and make evidence-based decisions. Despite tremendous advancements, the area still faces obstacles such as data complexity, encryption, and legal concerns. Concurrently, new technologies such as data analytics and cloud computing are influencing how research is carried out.

To sum up, digital forensics involves more than just data analysis; it also involves turning digital evidence into insightful knowledge. The significance of digital forensics will only grow in the future as cyber threats continue to change.

References

- [1] G. Palmer, “A roadmap for digital forensic research,” *Digital Forensic Research Workshop (DFRWS)*, 2020.
- [2] B. Nelson, A. Phillips and C. Steuart, *Guide to Computer Forensics and Investigations*, 6th ed., Cengage Learning, 2021.

- [3] S. L. Pfleeger and S. Furnell, “Cybersecurity and cyberwar: What everyone needs to know,” Oxford University Press, 2022.
- [4] K. Ruan, J. Carthy, T. Kechadi and M. Crosbie, “Cloud forensics definitions and critical criteria,” *Digital Investigation*, vol. 10, no. 1, pp. 34–43, 2020.
- [5] Y. Liao and V. Vemuri, “Use of machine learning in intrusion detection,” *Computers & Security*, vol. 30, pp. 128–145, 2021.
- [6] J. Sammons, *Digital Forensics: Threatscape and Best Practices*, Syngress, 2020.
- [7] U.S. Bureau of Labor Statistics, “Information Security Analysts Occupational Outlook,” 2024.

Task-2

2.1 Device Collection

The initial phase of the investigation focused on acquiring data from the provided mobile devices using a structured forensic approach. Industry-standard software was used to ensure that the data collection process remained reliable and did not alter the original evidence.

Figure 1 demonstrates that the mobile device was successfully detected within the forensic acquisition tool. This confirms that the system recognised the device correctly before starting the extraction process.

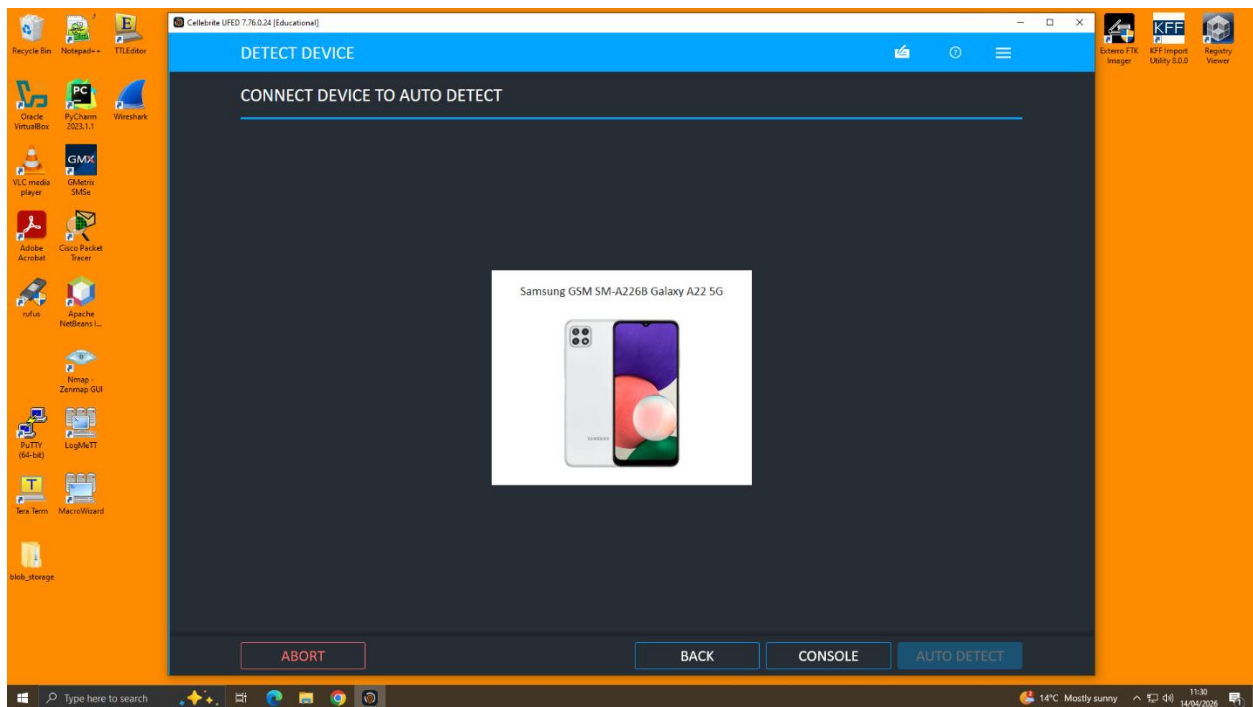


Figure-1: Device Samsung A22 Detected in Cellebrite UFED

The next stage involved selecting the types of artefacts to be extracted. Instead of manually browsing through the device, specific categories such as messages, contacts, and media files were chosen. This ensures consistency and reduces the risk of missing important data.

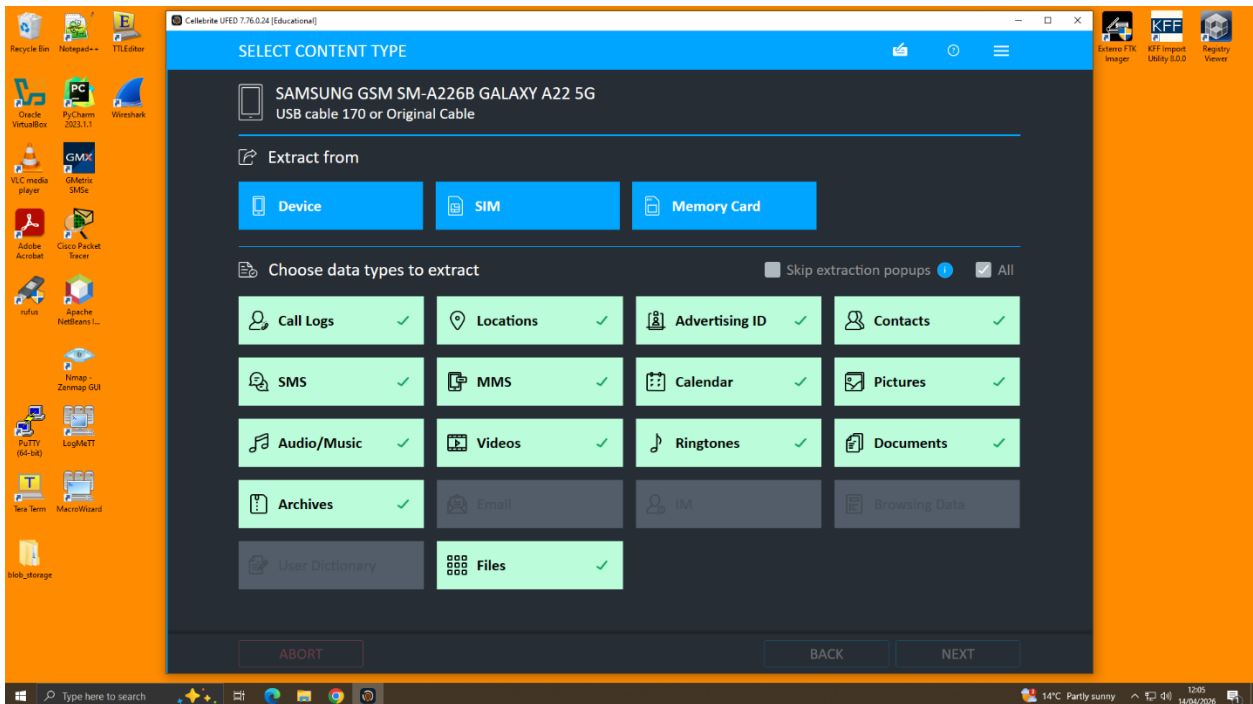


Figure-2: Files with lot of categories extracted from device

The tool produced a summary of the collected data once the extraction procedure was finished. This comprised many categories, including media files, system information, and communication logs, which served as the basis for additional research.

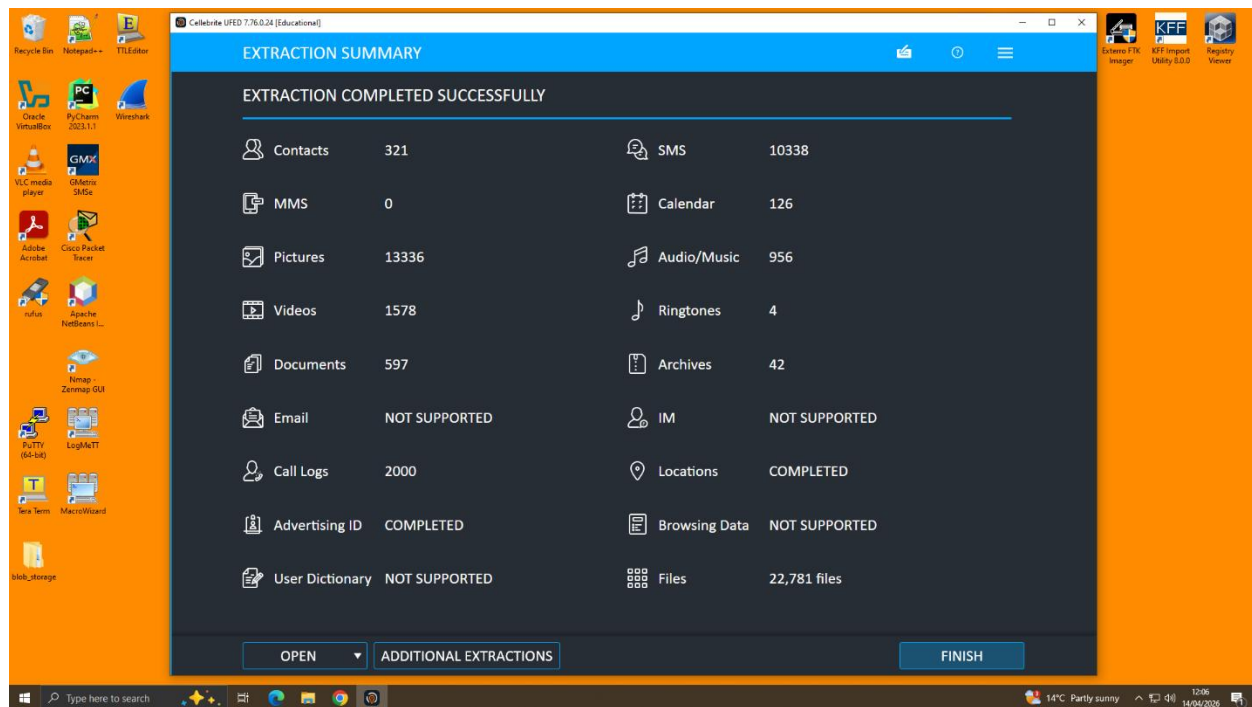


Figure-3: Extraction completed successfully for Samsung A22

2.2 Case Background

Unusual access to Quantum Tech's private patent database was discovered, particularly in relation to an AI chip design known as QT-AI-2025. Emma, a newly hired senior engineer, was identified by internal monitoring systems as a possible insider threat.

Emma may have tried to send private information to a third party, the organization suspected. Norman seemed to be the intended recipient of the information, while Joe was thought to serve as a middleman.

2.3 Evidence Inventory

The investigation was based on forensic images obtained from four mobile devices:

- Huawei POT-LX1
- Nokia C2
- Samsung Galaxy A13
- Note 14

The extracted data included:

- Contact records
- Messaging conversations (WhatsApp and SMS)
- Social media communication logs
- Location-related artefacts
- Document-related data

The presence of hash values and structured extraction outputs indicates that the data was collected through a proper forensic process. This ensures that the evidence remains reliable and has not been altered during analysis.

2.4 Methodology

- A systematic approach was followed during the investigation to ensure accuracy and integrity.
- **Step 1: Data Acquisition**
The forensic images were loaded into Cellebrite Physical Analyzer, which reconstructed the file system and allowed access to relevant artefacts.
- **Step 2: Integrity Verification**
Hash values (MD5/SHA-256) were checked to confirm that the data remained unchanged. This step is essential to maintain the credibility of the evidence.
- **Step 3: Advanced Analysis**
Additional artefacts were identified using built-in analytical tools such as App Genie. This helped uncover application-level data that may not be visible through basic extraction.

Figures below demonstrate the loading and verification process for each device:

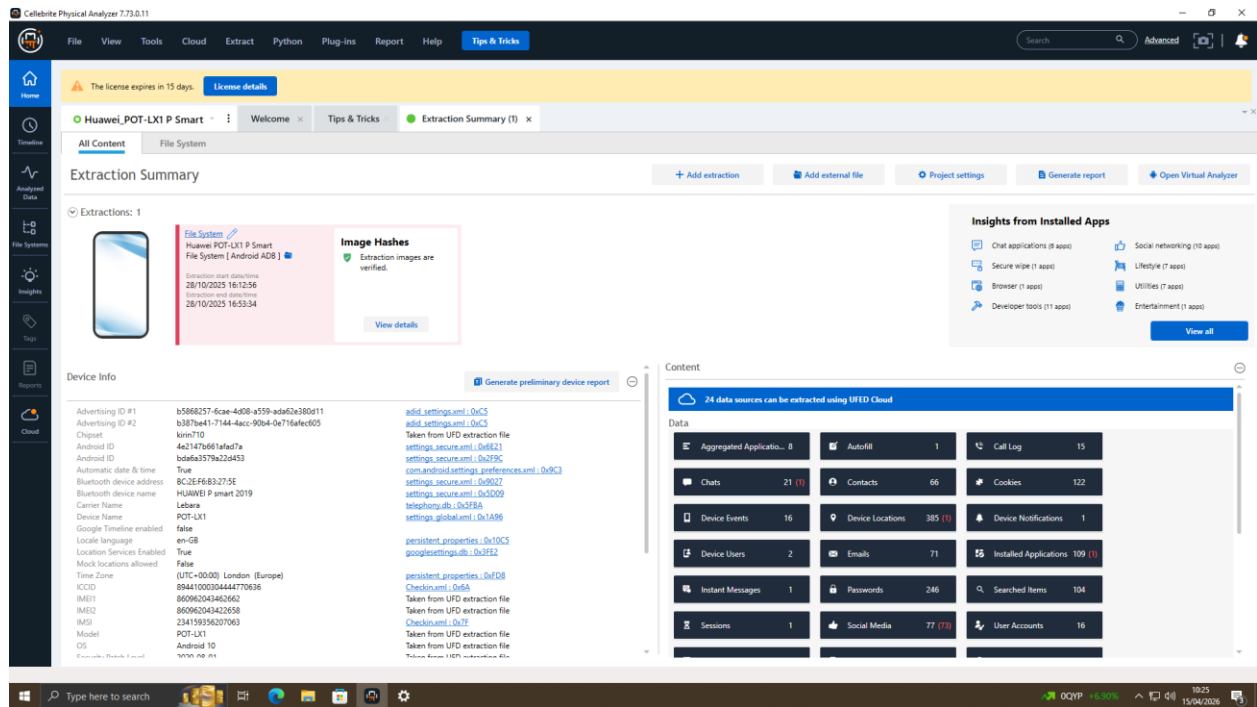


Figure-4: Huawei Device in Physical Analyzer

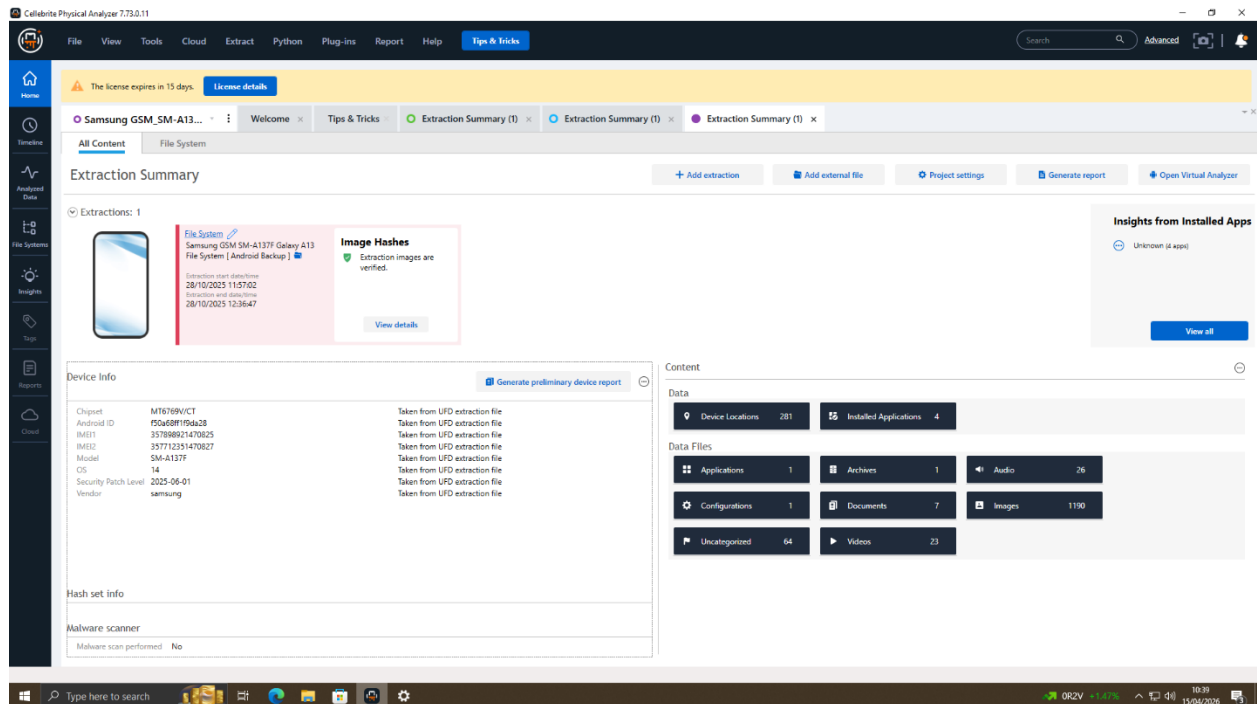


Figure-5: Samsung Device in Physical Analyzer

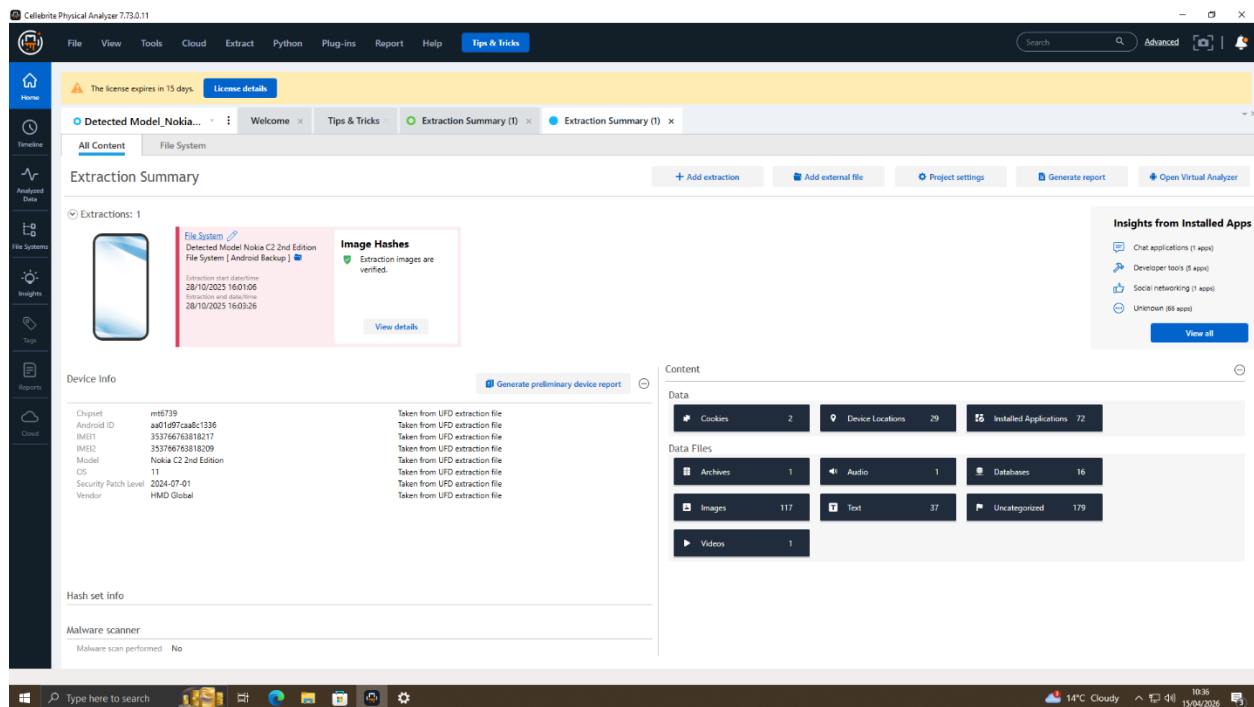


Figure-7: Nokia C2 Device in Physical Analyzer

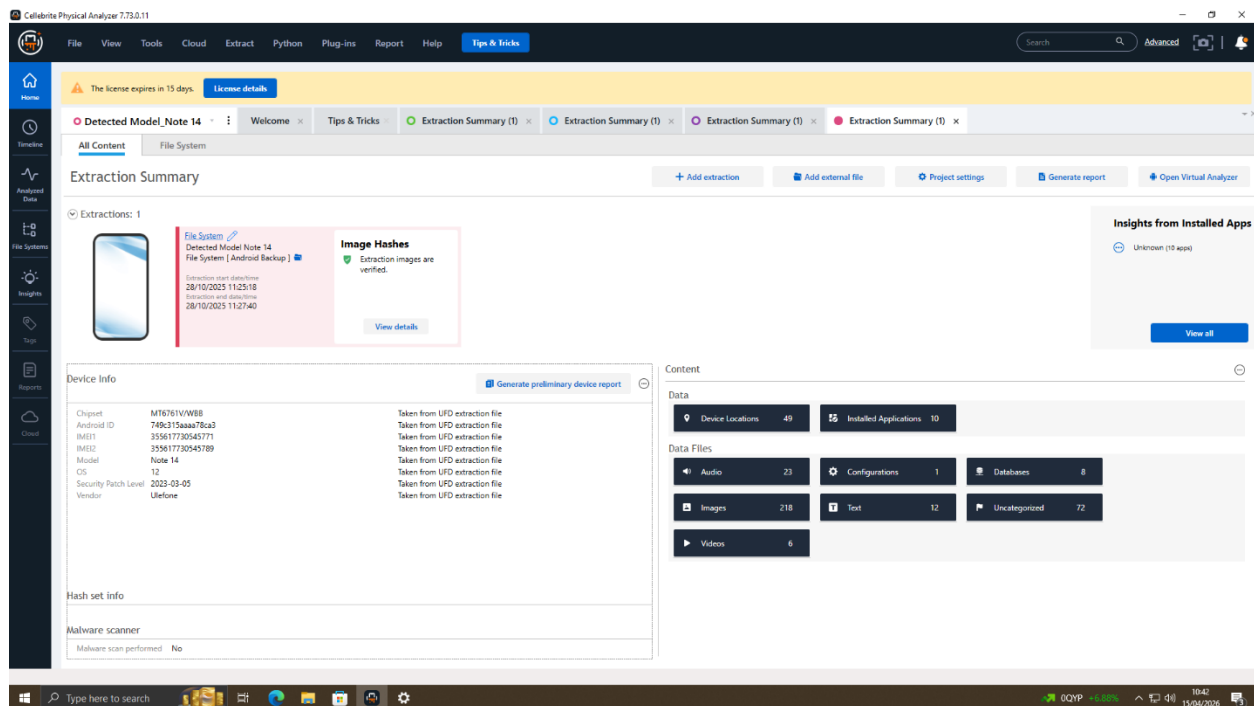


Figure-7: Note 14 Device in Physical Analyzer

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.

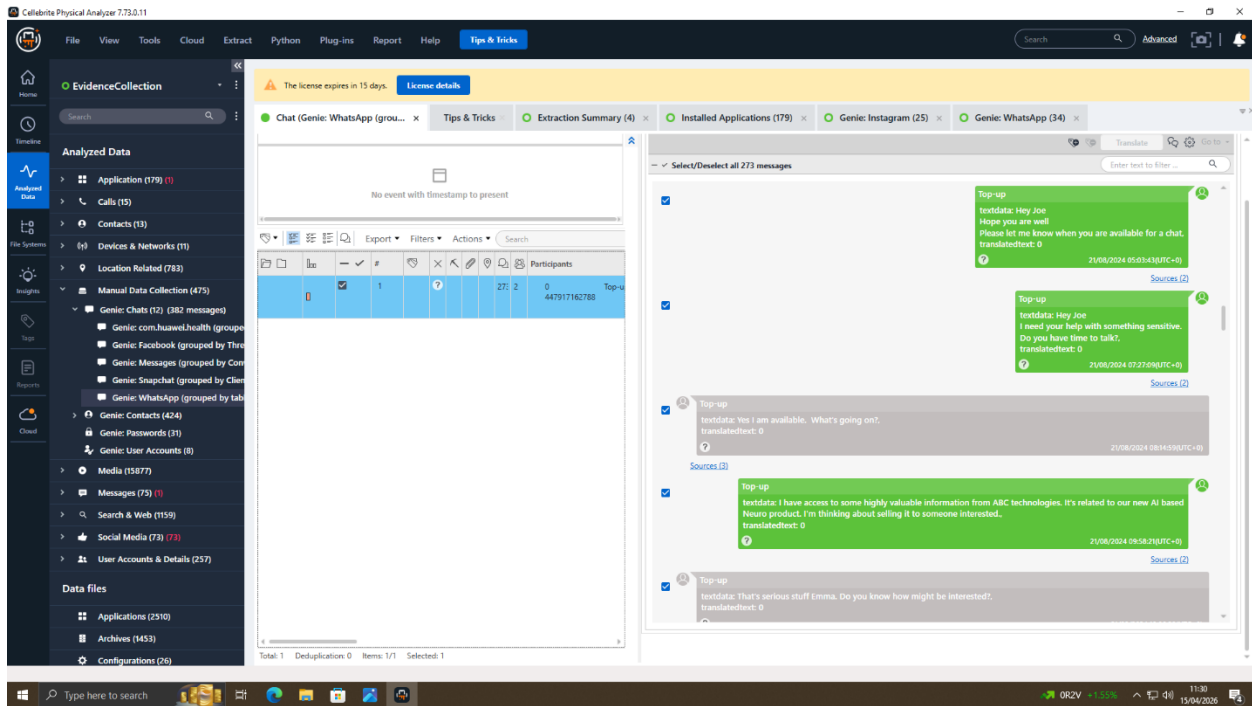


Figure-8: Emma stating to Joe saying something sensitive

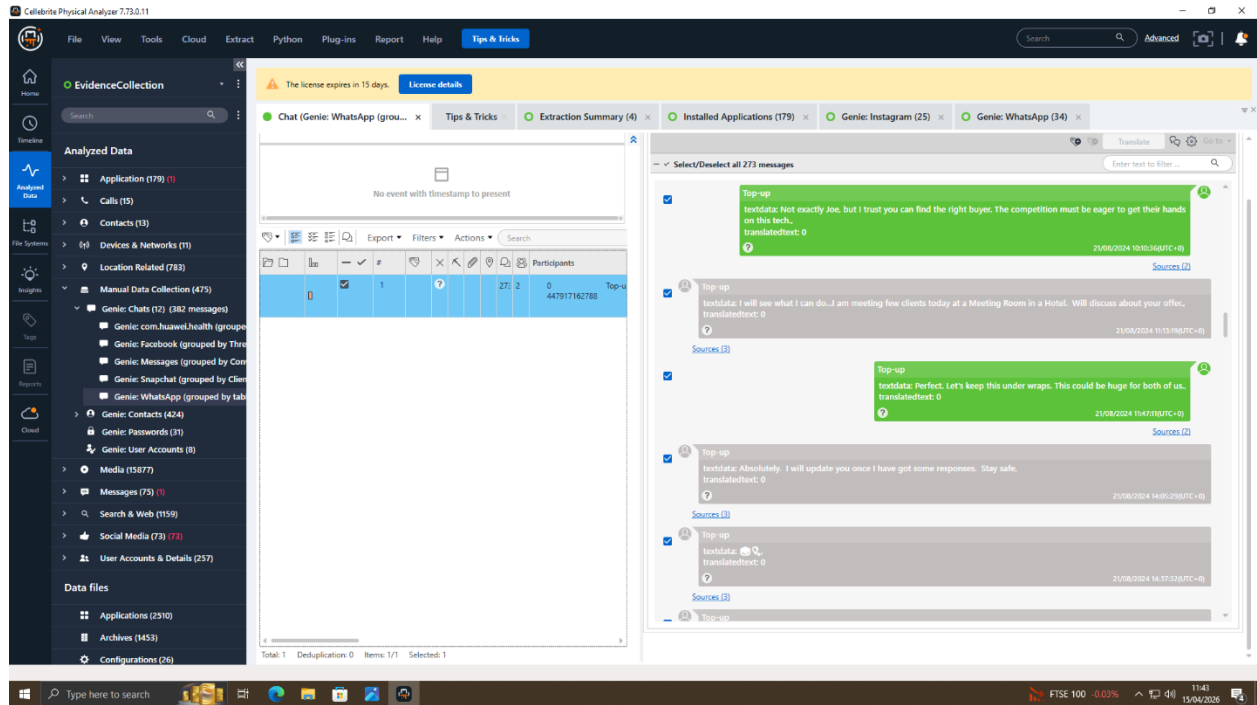


Figure-9: Joe was instructed to find buyer for the patent

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.

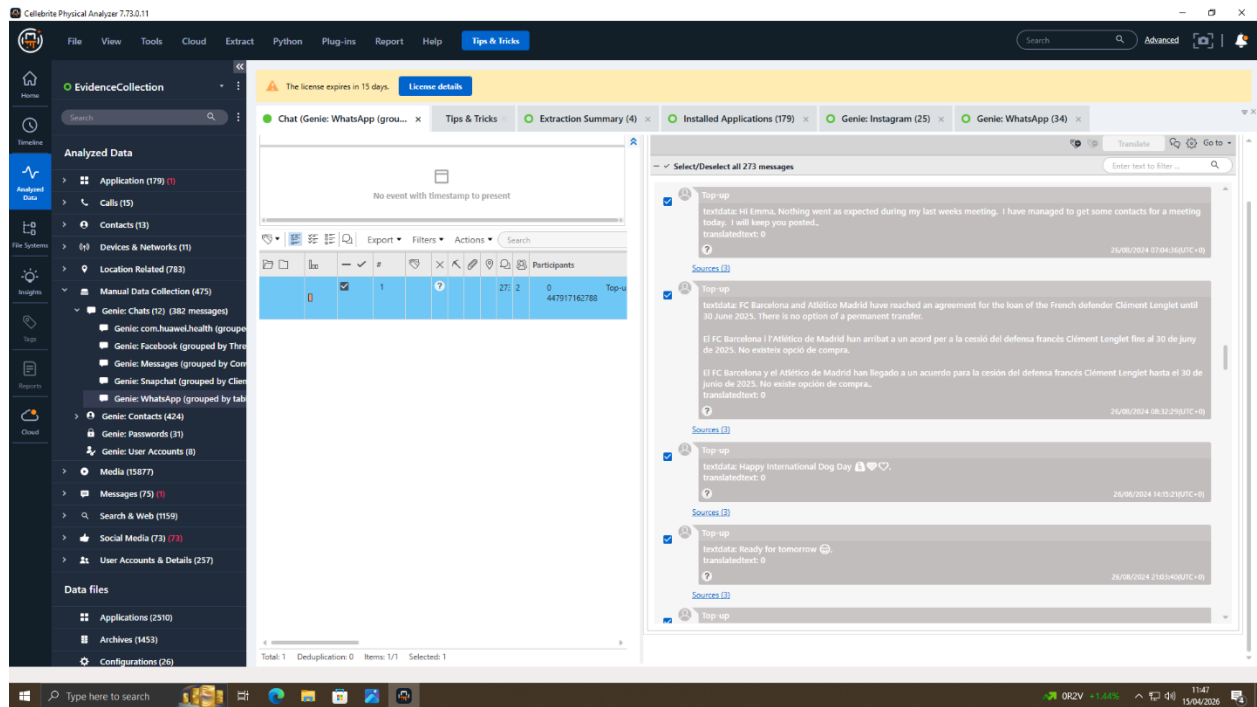


Figure-10: Joe Managing Meeting with clients and acting as a middleman

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.

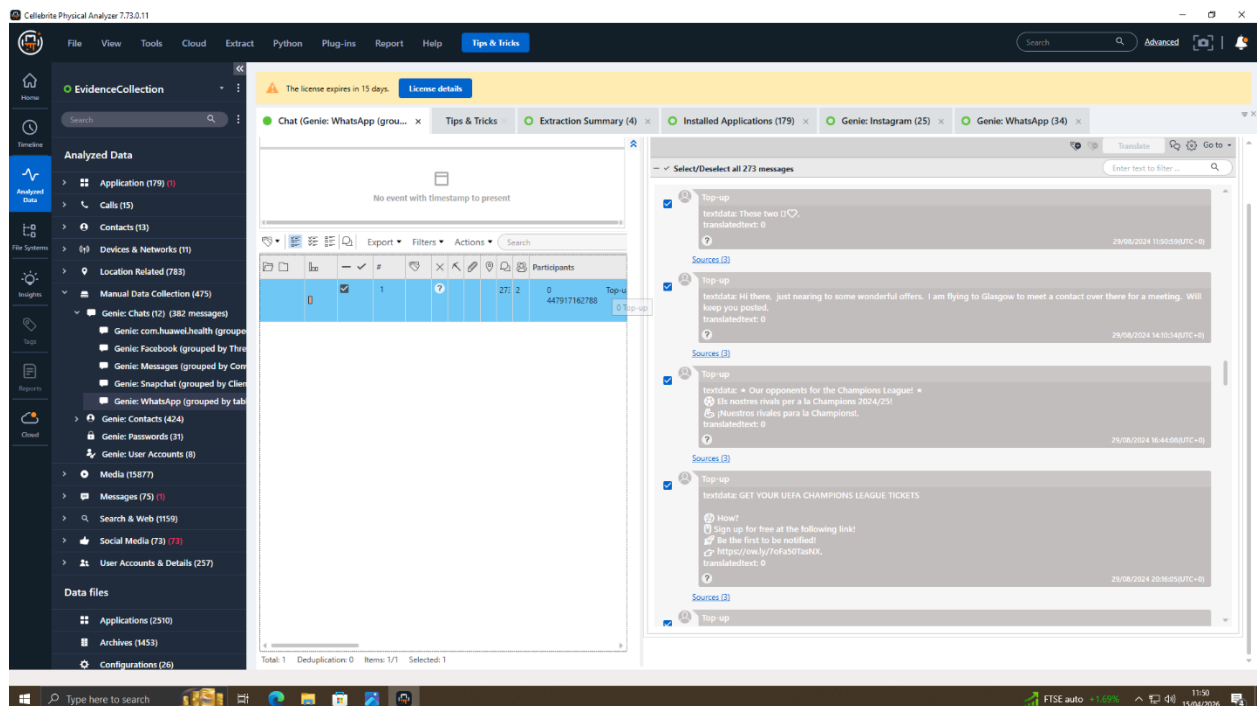


Figure-11: Joe went to Glasgow to meet client

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.

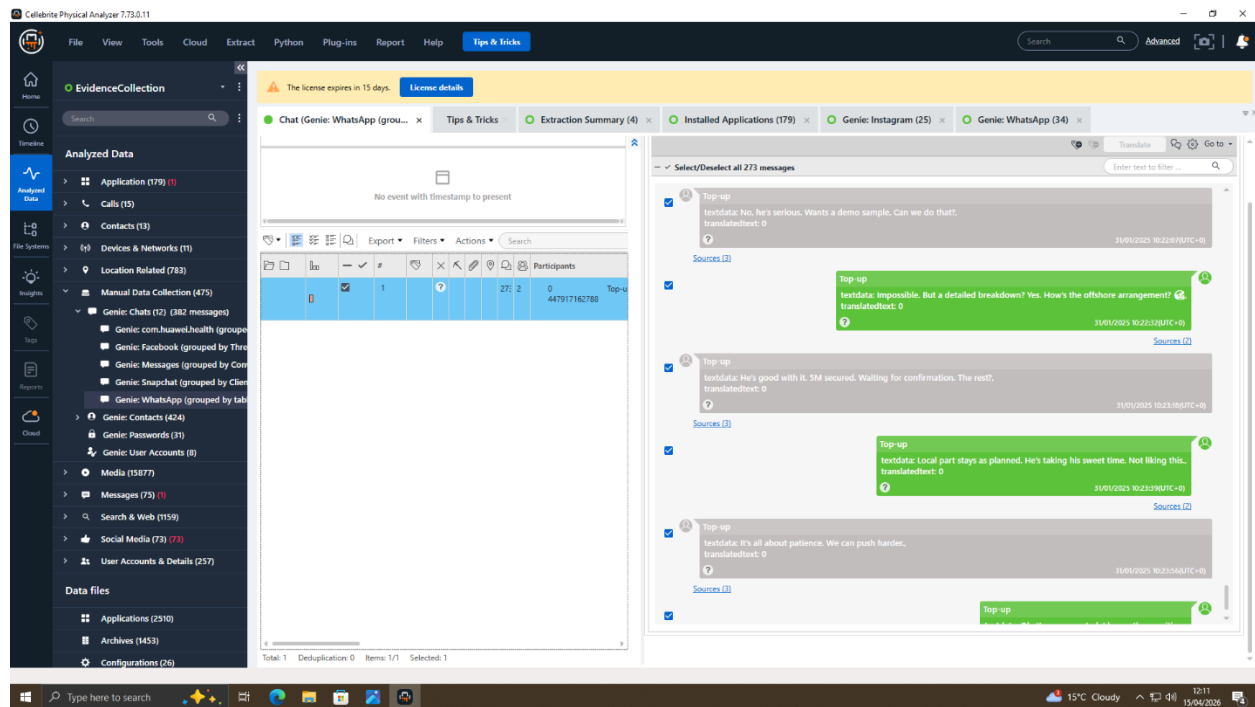


Figure-12: Joe and Emma both deal settled with client

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

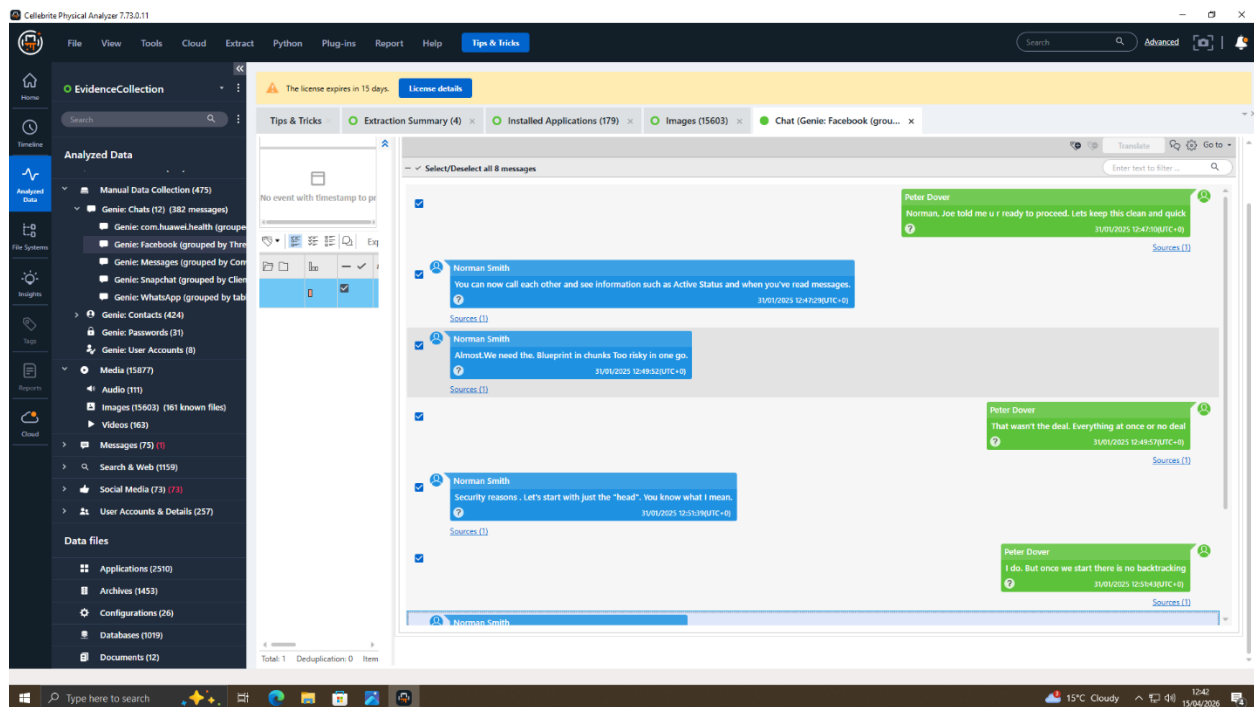


Figure-13: Emma initiated chat with Norman

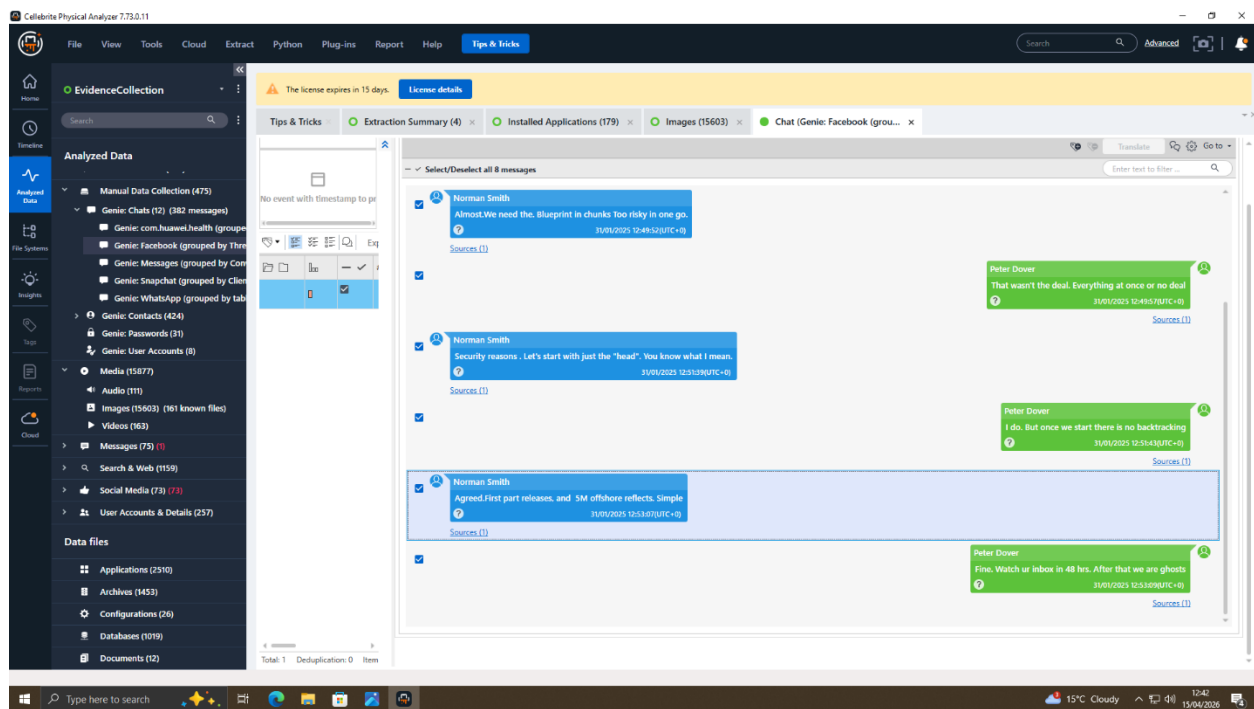


Figure-14: Emma and Norman agreed to release in chunks rather than full release

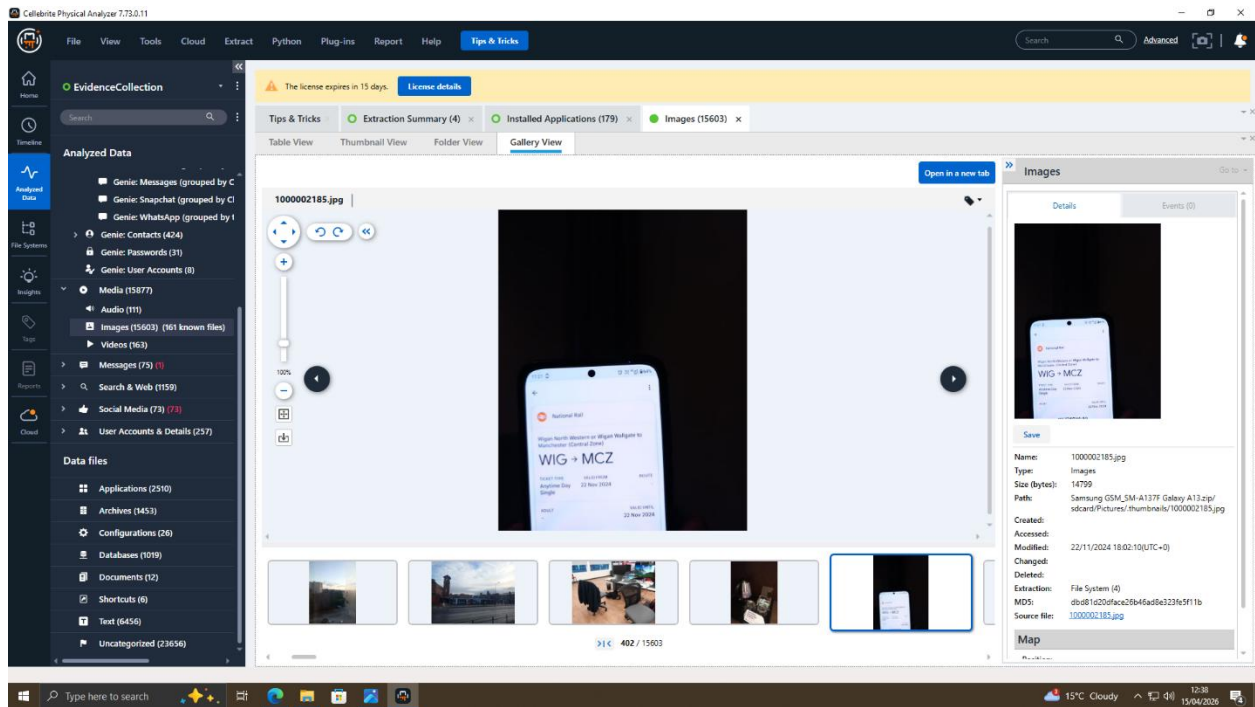


Figure-15: Manchester ticket showing proof that Joe went there

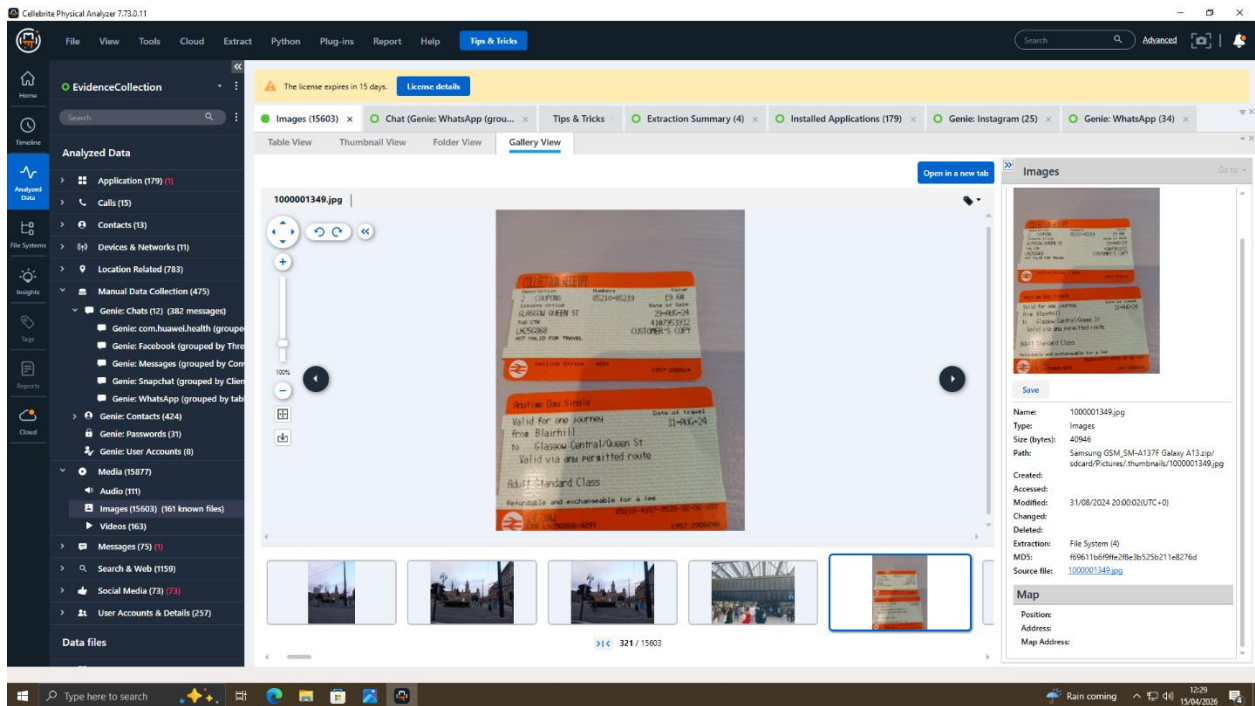


Figure-16: Glasgow Train Ticket proof joe went there

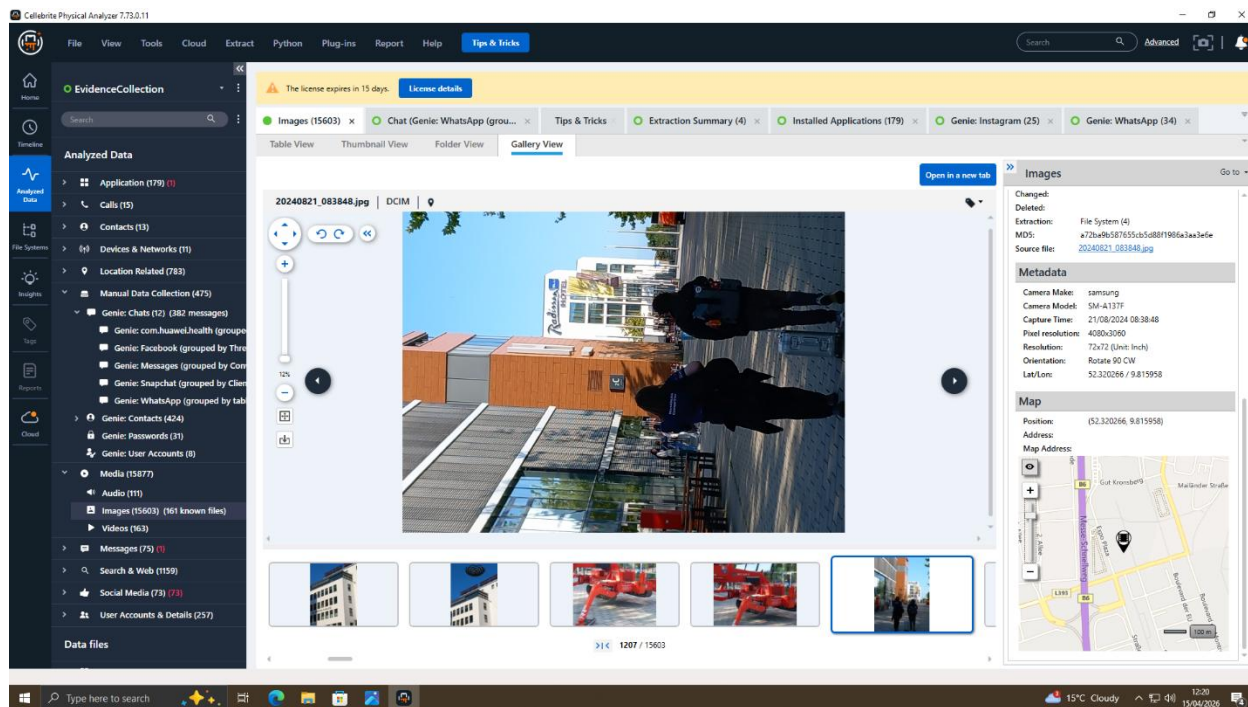


Figure-17: Hotel picture with the location

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 evidence gathered clearly points to a coordinated effort to transfer private data from Quantum Tech. From first contact to negotiation and travel, the communication process shows a clear path toward a planned transaction.

The results corroborate the assertion that the participants were not communicating in a typical professional manner but rather participated in actions associated with an attempt to steal corporate data.

2.8 Recommendation

- Preserve all forensic images and associated hash values for legal purposes
- Conduct deeper analysis on deleted or hidden data
- Investigate additional communication channels such as email or cloud storage

- Strengthen internal security controls to prevent similar incidents
- Consider legal action based on the evidence collected