



Student Name: Md Abu Sayeed

Student ID: 2528454

Programme: MSc in Cyber security and digital forensic
programme.

Module: Digital Forensics Analysis

Module Code: ACCA7031

Lecturer: Dr. Mohamed Ghanem

Internal Verifier: Mr. Munyaradzi Murira

Submission Date: 17th August 2026

Contents

Task 1: Digital Forensics-Current State, Cybersecurity Intersection, Emerging Trends, Challenges and the Global Job Market

1. Introduction
2. Current State of Digital Forensics: Tools, Features and Capabilities
3. Interaction Between Digital Forensics and Cybersecurity
4. New Developments in Digital Forensics
5. Critical Challenges
6. National and International Job Market
7. Conclusion and Recommendations
8. References

Task 2

1. Personal Mobile Phone Acquisition via Cellebrite UFED

- 1.1. Creation of Case
- 1.2. Device identification and extraction method
- 1.3. Extraction Location
- 1.4. Content Selection
- 1.5. Extraction Results
- 1.6. Evaluation of the Acquisition

2. Digital Forensics Investigation Assessment: Case QT-AI-2025

- 2.1. Case background
- 2.2. Collection and Preservation of Digital Evidence
- 2.3. Communication Between Emma and Joe
- 2.4. Joe's Intermediary Position
- 2.5. Direct Communication Between Emma and Norman
- 2.6. Conclusion of the Deal
- 2.7. Hotel Communication
- 2.8. Manchester Trip of Joe
- 2.9. Joe's Travel Ticket to Glasgow
- 2.10. Location of Joe's Mobile Phone at the Hotel
- 2.11. Geospatial and Location Evidence (Norman)
- 2.12. Profiling the Suspects and Behavioral Analysis
- 2.13. Timeline Reconstruction
- 2.14. Conclusion and Recommendations

Task 1: Digital Forensics-Current State, Cybersecurity Intersection, Emerging Trends, Challenges and the Global Job Market

1. Introduction

Digital forensics has evolved from a specialized field in computer crime investigation to an essential part of modern cybersecurity and incident response/criminal investigation. Due to the widespread use of smartphones, cloud computing, Internet of Things (IoT), artificial intelligence (AI), and distributed computing environments, the number of digital evidence has increased drastically [1], [2]. Modern digital forensics consists of identifying, preserving, acquiring, analyzing, and presenting digital evidence, maintaining its integrity and evidentiary value [1]. Digital forensics is becoming more and more related to cybersecurity since forensic evidence is needed not only in conventional crimes but also during cyber attack investigations and response actions.

2. Current State of Digital Forensics: Tools, Features and Capabilities

There exist commercial, open-source, and specialist tools in the current digital-forensics arena that are used for computer, mobile, memory, network, cloud, and multimedia forensics investigations. Modern books explain that the need for knowledge about forensic methods as well as the underlying artefacts created by operating systems and applications is required when conducting forensic investigations [1].

Examples of computer and disk forensics tools include Magnet AXIOM, FTK, EnCase and Autopsy/The Sleuth Kit. They allow creating/analyzing forensic images, retrieving deleted files, file system analysis, analyzing

browser history, extracting metadata, tracking user activities and producing reports. Commercial tools offer workflow capabilities, extensive artefacts parsing. Autopsy, on the other hand, offers an inexpensive and transparent open source alternative to commercial tools. Recent studies suggest that commercial tools could be superior in terms of workflow capabilities while open source ones could work effectively in specific forensic scenarios [3][4].

3. Interaction Between Digital Forensics and Cybersecurity

Cybersecurity focuses mainly on prevention, detection and response to attacks, whereas digital forensics offers proof to establish what happened, how it happened, which systems were targeted and potentially the identity of those responsible for it [5], [6]. For instance, in a ransomware case, it is cybersecurity measures that help in identifying malicious processes, IP addresses, unusual authentication activities, and so forth. However, through forensic investigation, these data can be correlated to understand the sequence of events during the attack.

In this regard, digital forensics has become useful not only after incidents but also at all stages of the incident response process.

The relationship between digital forensics and cybersecurity is crucial because of increasing complexity of cybersecurity operations with the involvement of various cloud services, mobiles, IoT devices and other components. Recent literature describes digital forensics as developing from traditional computers to other areas like device forensics, artefacts forensics, memory forensics, network forensics and multimedia forensics [2].

4. New Developments in Digital Forensics

Several new technologies are changing the field of digital forensics. First, artificial intelligence and machine learning have become increasingly relevant to evidence categorization, detecting anomalies, pattern identification and automation. Data mining can support the analysis of

extensive amounts of textual and digital artefacts which cannot be examined manually [7]. However, the conclusions reached using AI should always be intelligible and verifiable because forensic conclusions need to be justified.

The second new technology is generative AI and large language models. The 2026 research demonstrates opportunities for LLMs to aid various forensic stages but at the same time notes the contradiction between probabilistic AI conclusions and deterministic nature of forensic evidence [8]. That is why AI is better considered as an investigative assistant rather than an independent forensic expert.

Second, IoT and multimedia forensics are advancing. The smart devices can provide evidence associated with physical activities and environmental factors. Moreover, the use of AI to manipulate multimedia creates additional forensic challenges.

5. Critical Challenges

Firstly, the huge amount of data and its complexity represent the first critical challenge for investigators. They may have to analyze huge amounts of endpoint, mobile, cloud and network data. The manual analysis is therefore getting increasingly difficult.

Secondly, the volatile nature of the data and the necessity to preserve evidence represent the next challenge. Cloud resources, memory, network traffic and application data may quickly disappear. It is especially problematic when it comes to cloud environment investigations since investigators do not have any control over the underlying infrastructure [6].

6. National and International Job Market

The job market is evidence that digital forensics is no longer confined to the old police forensic laboratories. Current UK vacancies include positions such as Digital Forensics Practitioners, Digital Forensic Specialists, Digital Investigators, DFIR Analysts, Incident Responders, eDiscovery

Consultants, Cyber Incident Response Analysts, and forensic technology graduates. The current LinkedIn job search in the UK also includes vacancies with HM Revenue & Customs, the police, S-RM, VodafoneThree, Tesco, Accenture, FTI Consulting and many others. London stands out with vacancies in the fields of financial services, consultancy, government, cybersecurity, and forensic specialists firms.

The wider UK cybersecurity labor market continues to face shortages of skilled people. According to the Government's UK labor market study for 2025, the number of required individuals in the field of cybersecurity amounts to approximately 12,900 annually against 9,100 new recruits. The difference comes to approximately 3,800 people annually. This suggests a favorable environment for graduates with a combination of forensic knowledge and cybersecurity skills.

7. Conclusion and Recommendations

Modern digital forensics goes far beyond traditional computer investigation and represents a multi-disciplinary capability for cybersecurity, incident response, cloud, mobile and IoT investigation and criminal justice. Current tools offer advanced capabilities for acquisition and analysis of evidence, but the difference in toolkits shows the necessity of tool validation and examiner's skill [4].

From the perspective of the career of students entering the field, the best course of action would be development of skills of DFIR, not only traditional digital forensics. The combination of skills related to networking and systems administration of both Linux and Windows systems should be accompanied by practice in such tools as Autopsy, Wireshark, KAPE and other platforms for mobile forensics, followed by specialized skills related to cloud and memory forensics.

In general, the future of digital forensics lies in its capability to unite forensic methodologies with cybersecurity, cloud technologies, AI and automation.

8. References

[1] J. Kävrestad, M. Birath, and N. Clarke, *Fundamentals of Digital Forensics: A Guide to Theory, Research and Applications*. Cham, Switzerland: Springer, 2024.

<https://scholar.google.com/scholar?q=%22Fundamentals+of+Digital+Forensics%22+K%C3%A4vrestad+Birath+Clarke>

[2] A. W. Malik, D. S. Bhatti, T.-J. Park, H. U. Ishtiaq, J.-C. Ryou, and K.-I. Kim, "Cloud digital forensics: Beyond tools, techniques, and challenges," *Sensors*, vol. 24, no. 2, p. 433, 2024.

<https://scholar.google.com/scholar?q=%22Cloud+digital+forensics%3A+Beyond+tools%2C+techniques%2C+and+challenges%22>

[3] "TLS key material identification and extraction in memory: Current state and future challenges," *Forensic Science International: Digital Investigation*, vol. 49, 301766, 2024.

<https://scholar.google.com/scholar?q=%22TLS+key+material+identification+and+extraction+in+memory%22>

[4] "What you say in the lab, stays in the lab": A reflexive thematic analysis of current challenges and future directions of digital forensic investigations in the UK," *Forensic Science International: Digital Investigation*, vol. 51, 301839, 2024.

<https://scholar.google.com/scholar?q=%22What+you+say+in+the+lab%2C+stays+in+the+lab%22+digital+forensic>

[5] S. J. Sinaga, M. A. Asykar, H. Manurung, W. C. Wibowo, S. Yazid, and T. O. Edwardo, "Comparative evaluation of artifact extraction performance and usability in digital forensic tools: A study of Cellebrite UFED, MSAB XRY, and Magnet AXIOM," *Journal of Forensic Sciences*, vol. 71, no. 4, pp. 1652–1661, 2026.

<https://scholar.google.com/scholar?q=%22Comparative+evaluation+of+artifact+extraction+performance+and+usability%22>

[6] “A survey of data mining techniques for digital forensic analysis,” *Procedia Computer Science*, vol. 257, pp. 731–736, 2025.

<https://scholar.google.com/scholar?q=%22A+survey+of+data+mining+techniques+for+digital+forensic+analysis%22>

[7] “Large language models in digital forensics: Capabilities, challenges and future directions,” *Forensic Science International: Digital Investigation*, vol. 56, 302043, 2026.

<https://scholar.google.com/scholar?q=%22Large+language+models+in+digital+forensics%22>

[8] Department for Science, Innovation and Technology, *Cyber Security Skills in the UK Labour Market 2025*, UK Government, 2025.

<https://scholar.google.com/scholar?q=%22Cyber+Security+Skills+in+the+UK+Labour+Market+2025%22>

Task 2

1. Personal Mobile Phone Acquisition via Cellebrite UFED

Acquisition of the personal mobile phone was done via Cellebrite UFED software to gather digital evidence from a BlackBerry mobile phone. The process was carried out through a well-defined forensic process that started with creation of a case and ended with an extraction summary. These screenshots capture every step during the acquisition process and depict the data that was successfully extracted or those that could not be extracted during the process. The device used was a BlackBerry GSM 9720 SAMOA with a cable and BlackBerry tip T-100.

1.1. Creation of Case

The first step was to create a new case file on the Cellebrite UFED software. Information regarding the case was captured by the examiner such as case identifier, name of examiner, device/evidence number, crime type, department, and location. In the screenshot, the crime type is noted to be theft, the department was cyber while the location was London.

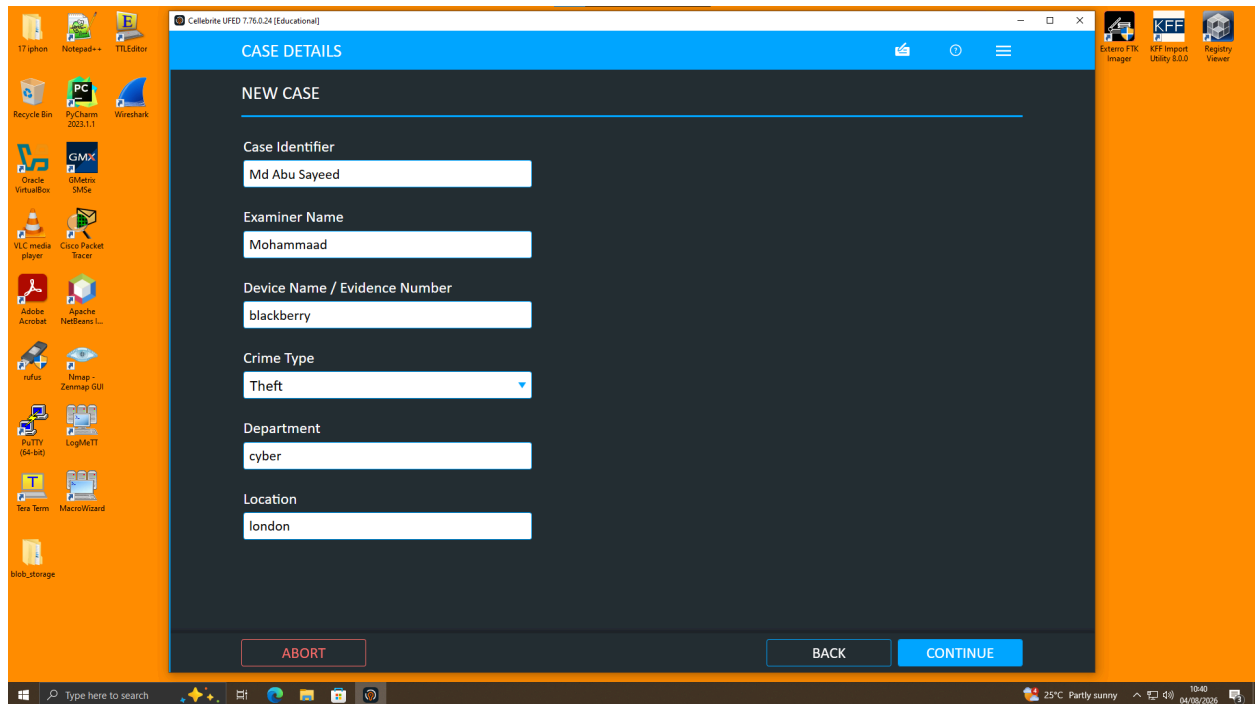


Figure 1: Creation of the case and documentation of the investigation process using Cellebrite UFED.

Having created the case, the examiner continued with the next step which was the device acquisition. Cellebrite gave several choices among which include Smart Flow, Auto Detect, Search Devices and Device Wizard. The examiner needs these options to identify the device connected and choose the appropriate workflow for the acquisition process. It is necessary to identify the right device and method of acquisition since different mobile devices will require different extraction methods.

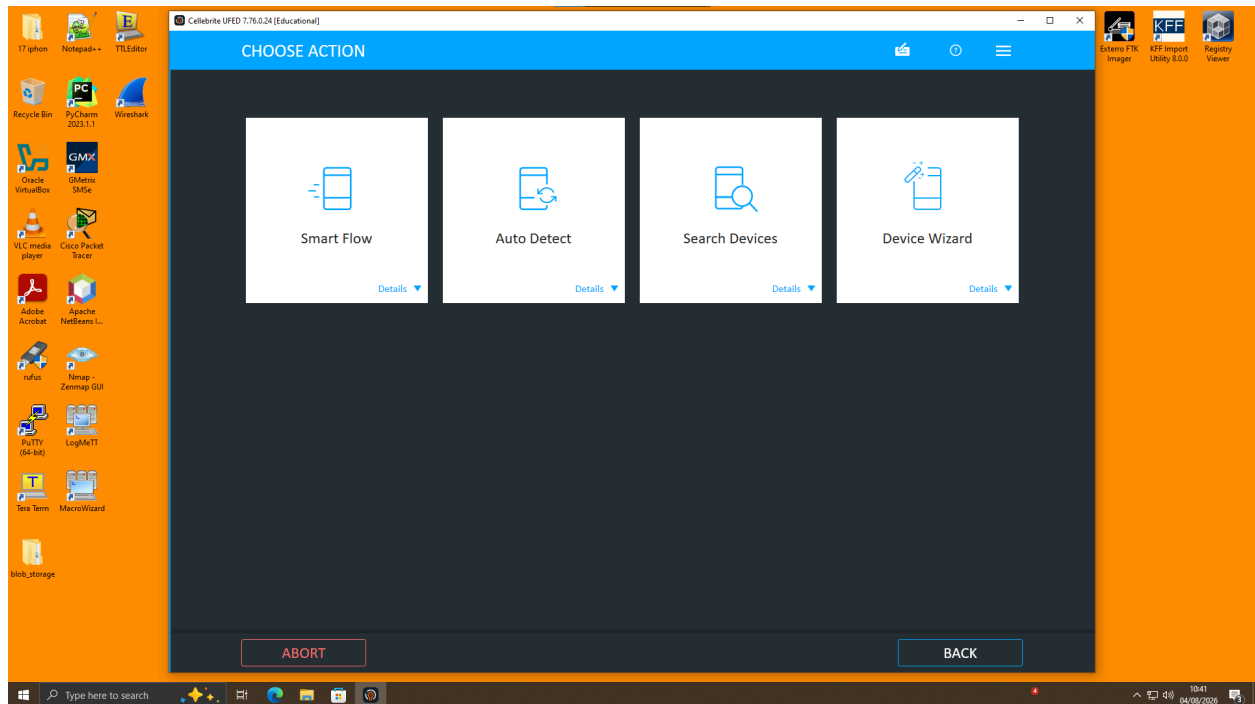


Figure 2: Options for identifying and acquiring the connected mobile device using Cellebrite UFED.

1.2. Device identification and extraction method

Identification of the connected device and the extraction method was the next step. According to Cellebrite, the phone was a BlackBerry GSM 9720 SAMOA. There were four extraction methods provided by Cellebrite: Logical, File System, Camera and Screenshot. In this case, logical extraction was chosen.

Logical extraction is done with the aim of gathering the available information from the device without necessarily making a complete image of the internal storage of the device.

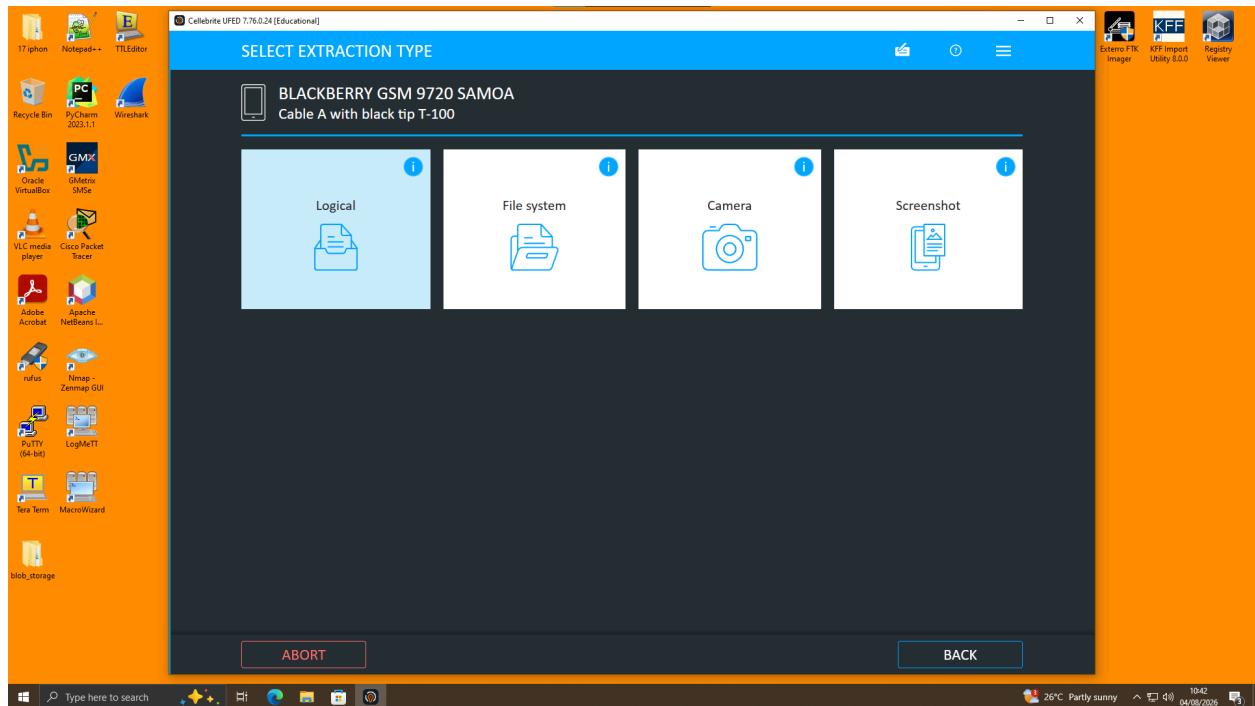


Figure 3: Identification of the BlackBerry device and selection of the logical extraction method.

1.3. Extraction Location

Once the extraction method was identified, the examiner needed to select the location where the extracted data will be saved. In Cellebrite, there was an option to save the extraction on the forensic workstation's local drive. The choice of an appropriate extraction location is vital as the extracted data has to be preserved for further analysis.

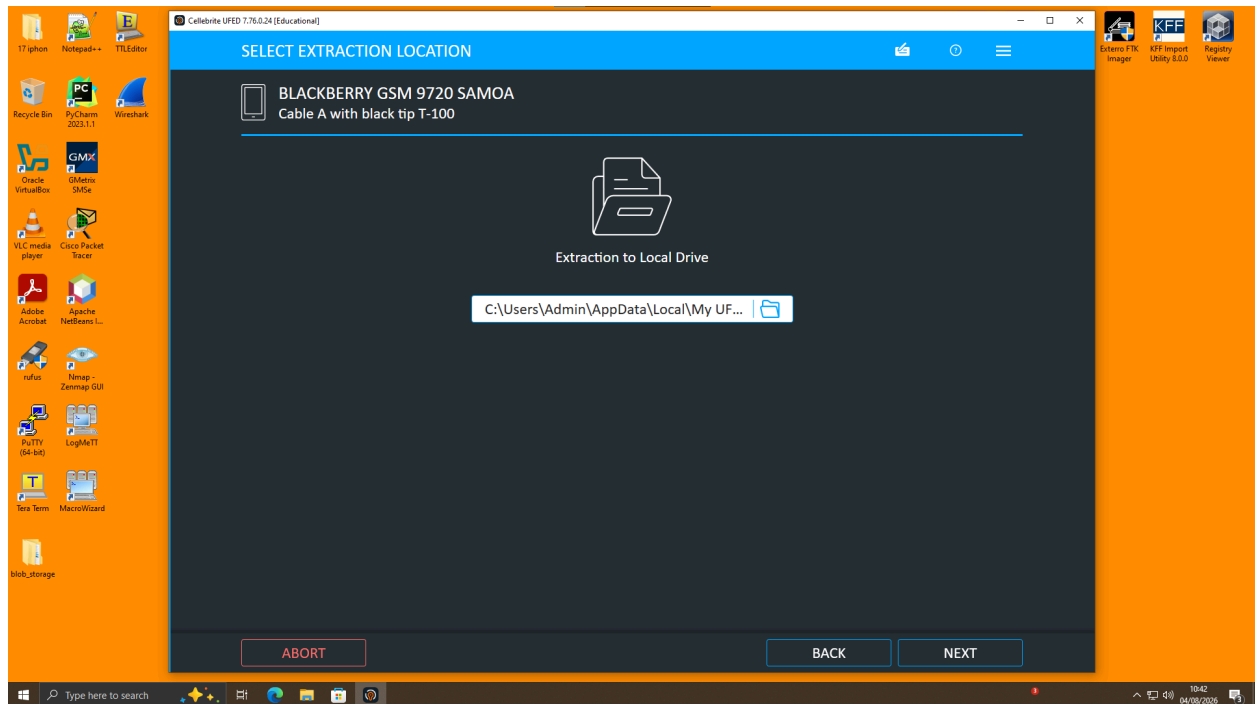


Figure 4: Choice of the local drive as the extraction location for forensic data.

1.4. Content Selection

The next step was to choose the information categories that Cellebrite should extract. These categories included call logs, contacts, SMS, MMS, pictures, audio/Music, videos, ringtones, documents, archives and email. However, not all categories were available at the time of extraction while some could be chosen.

The investigator chose the appropriate content categories before proceeding with the extraction. The selection of appropriate content categories is useful in concentrating on relevant evidence.

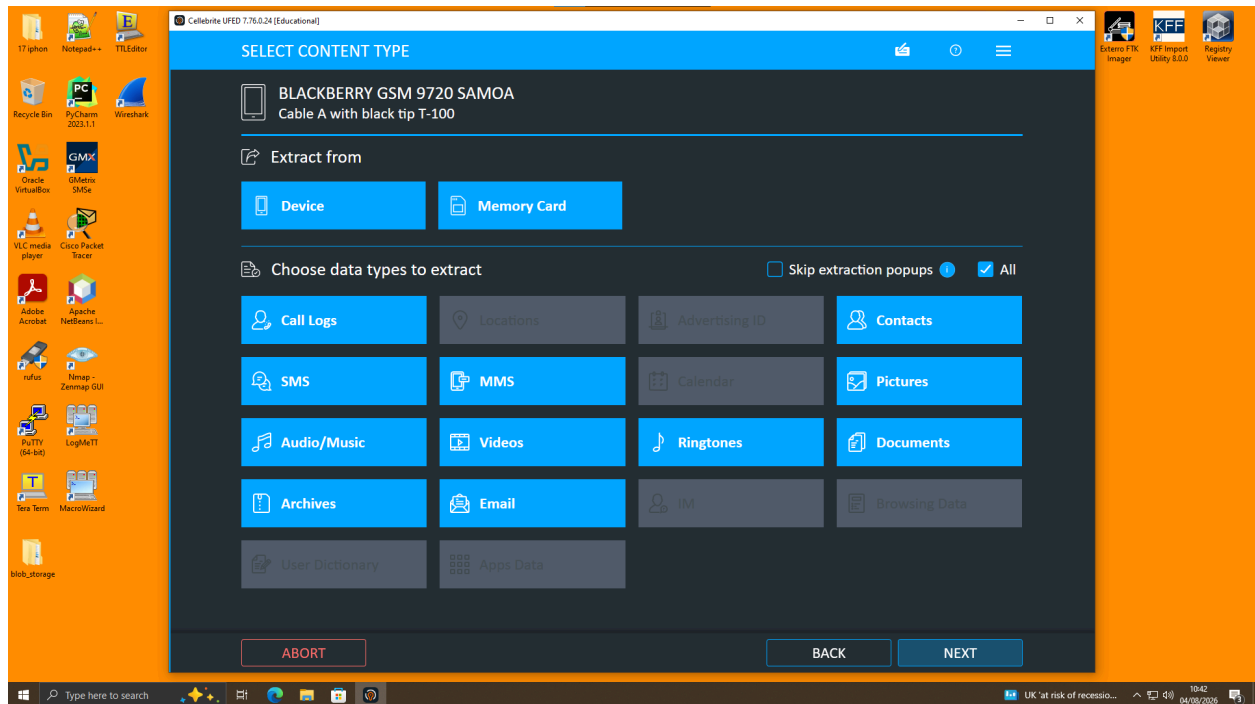


Figure 5: Selection of data categories to be extracted from the BlackBerry device.

1.5. Extraction Results

The last step yielded the Extraction Summary, demonstrating the outcome of the acquisition. According to Cellebrite, the extraction was performed successfully. Nevertheless, as can be seen from the results, not all categories of information were successfully extracted. In total, there were 372 pictures, 89 videos, and 6,596 files. Audio/music, ringtones, documents, and archives were zero.

There were several data categories marked as skipped: contacts, SMS, MMS, calendar, e-mail, and instant messaging. There were also some data categories marked as unsuccessful: call logs, locations, advertising ID, and browsing data. As far as the user dictionary is concerned, it was marked as not supported by Cellebrite.

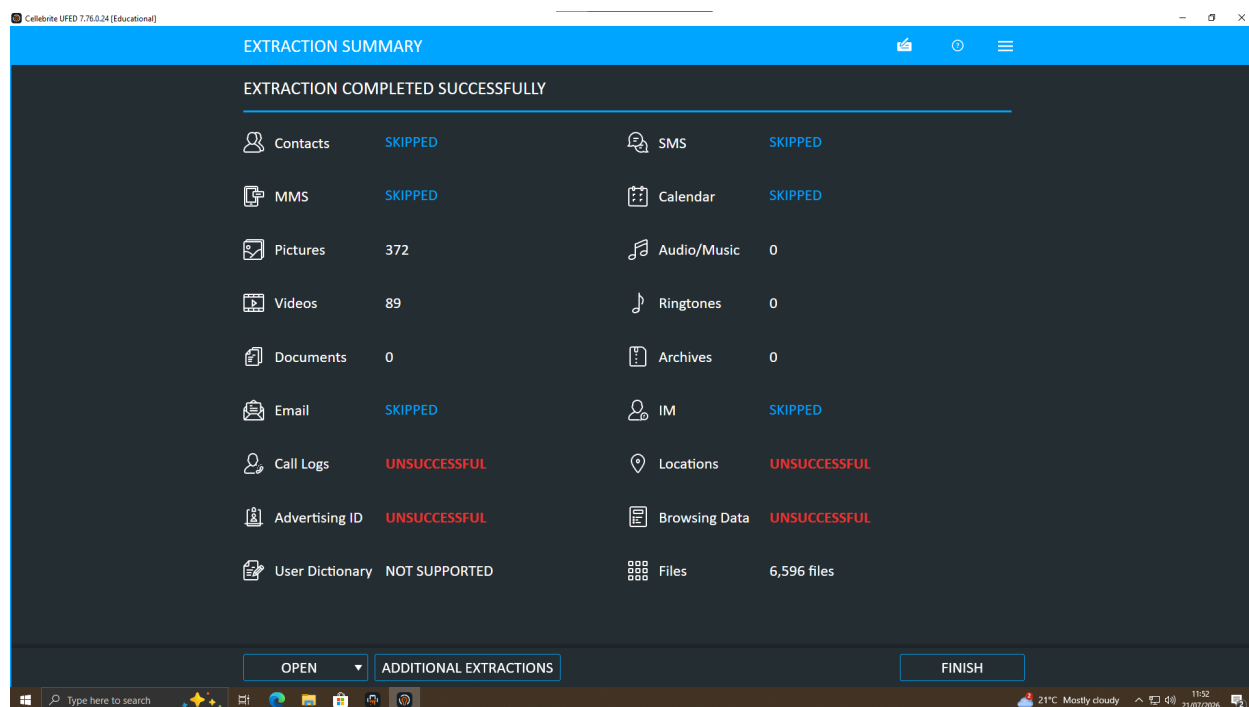


Figure 6: Extraction summary of Cellebrite UFED containing data categories which have been successfully extracted, skipped and unsuccessful.

It is crucially important to note that the extraction summary gives an idea about the limitations of the acquisition. In spite of the fact that Cellebrite claims that the extraction process has been completed successfully, it does not necessarily mean that every item has been retrieved from the phone. Thus, it is vital to distinguish between data categories which have been extracted successfully, skipped, unavailable and could not be acquired.

1.6. Evaluation of the Acquisition

In general, the acquisition process took place in a particular sequence, namely, case creation, device identification, selection of the extraction technique, selection of the storage location, selection and review of extraction results.

The results obtained in this case show an important characteristic of digital forensics – the success of the extraction process does not guarantee full access to the information stored on the device. Thus, it is necessary to

describe in detail the way of extraction and its limitations. If the investigator encounters some problems with the information that is essential for the case, then alternative ways of extracting it must be explored.

Detailed documentation is also extremely important in the extraction process. All details about the device, technique of extraction, selected data types and the results of extraction must be documented. This way, another investigator will have a possibility to know how the evidence has been extracted.

Overall, the process of acquiring information using the Cellebrite UFED tool from the BlackBerry device resulted in obtaining substantial data including pictures, videos, and files. However, the extraction process made it possible to identify the categories of information that failed to be recovered. Six screenshots attached to the paper are provided to visually show the entire acquisition process.

2. Digital Forensics Investigation Assessment: Case QT-AI-2025

2.1. Case background

It is necessary to mention that digital forensics is an integral part of any investigation that involves electronic devices as sources of possible evidence related to communication, planning, movements and criminal activity. In this particular case, the investigation is focused on the unauthorized disclosure and attempted selling of some information about the QT-AI-2025 patent. The investigation involved three mobile devices, namely QT-01 Nokia C2, QT-02 Huawei P Smart and QT-03 Samsung Galaxy A13. It is stated that the device were collected as a part of evidence and that SHA-256 verification was applied for the sake of integrity of the evidence

The collection of evidence related to the phone acquisition serves as a practical addition to the investigation process. The presentation describes the methodology of the forensic investigation, communication analysis, geospatial analysis, profiling of the suspects and reconstruction of the time frame of the crime. The screenshots of the phones' acquisition present practical examples of the digital artefacts that were used in the investigation, such as communication and geolocation information.

2.2. Collection and Preservation of Digital Evidence

The first significant phase of the examination was the identification and preservation of the digital evidence. In total, there were three items used as evidence, which included QT-01 Nokia C2, QT-02 Huawei P Smart and QT-03 Samsung Galaxy A13. As highlighted in the presentation, SHA-256 hashing was employed for the evidence.

Preserving digital evidence is important since the information that exists on the mobile device can easily be changed, deleted or replaced. Therefore, a forensic expert should be able to analyze the collected evidence instead of tampering with the original one. The process followed as highlighted in the presentation includes identification and seizure, transportation and isolation, acquisition and hashing, and lastly analysis and correlation.

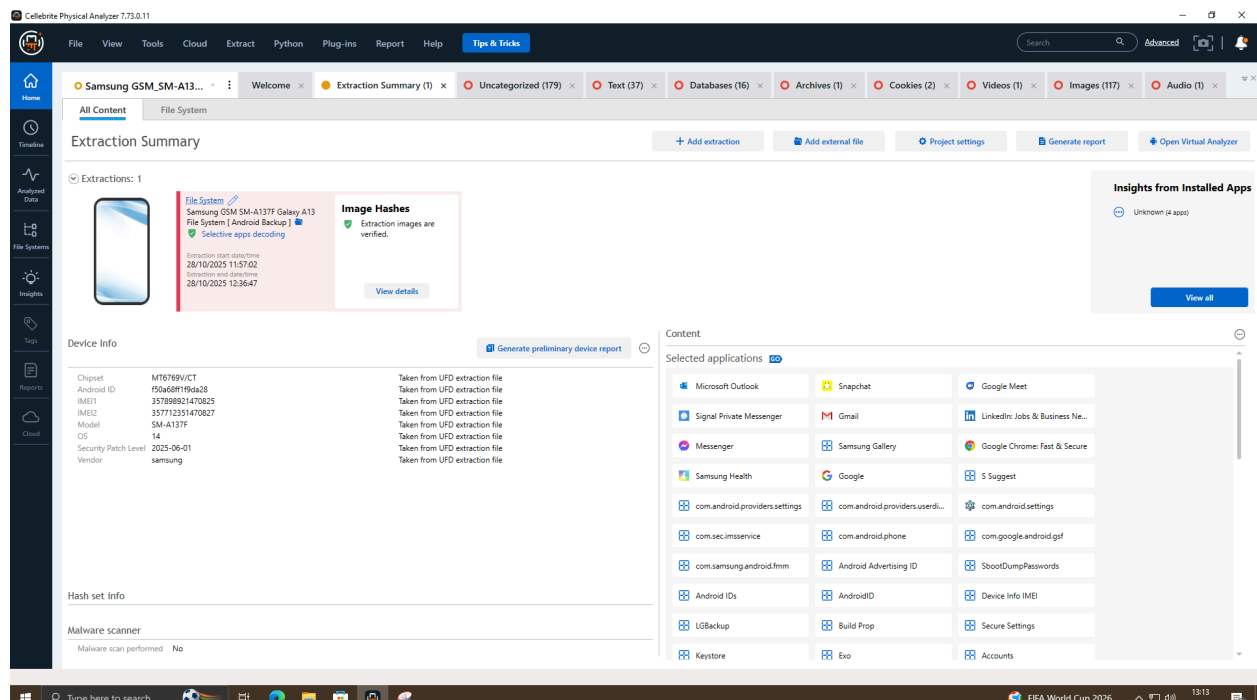


Figure 9: The Forensic Extraction and Hash Comparison of the samsung Phone Evidence (Joe’s phone)

The use of Cellebrite UFED and Cellebrite Physical Analyzer V7 was the basic forensic toolset. UFED was utilized in the process of the acquisition, whereas Physical Analyzer was a medium for examining and analyzing the acquired data.

The screenshot of the phone data acquisition process is especially important since it illustrates the fact that the investigation was not based on some kind of theoretical process. The phone data contained communication and geolocation artifacts, which could be further analyzed and compared to other evidence.

2.3. Communication Between Emma and Joe

The second piece of evidence revolves around communication between Emma and Joe.

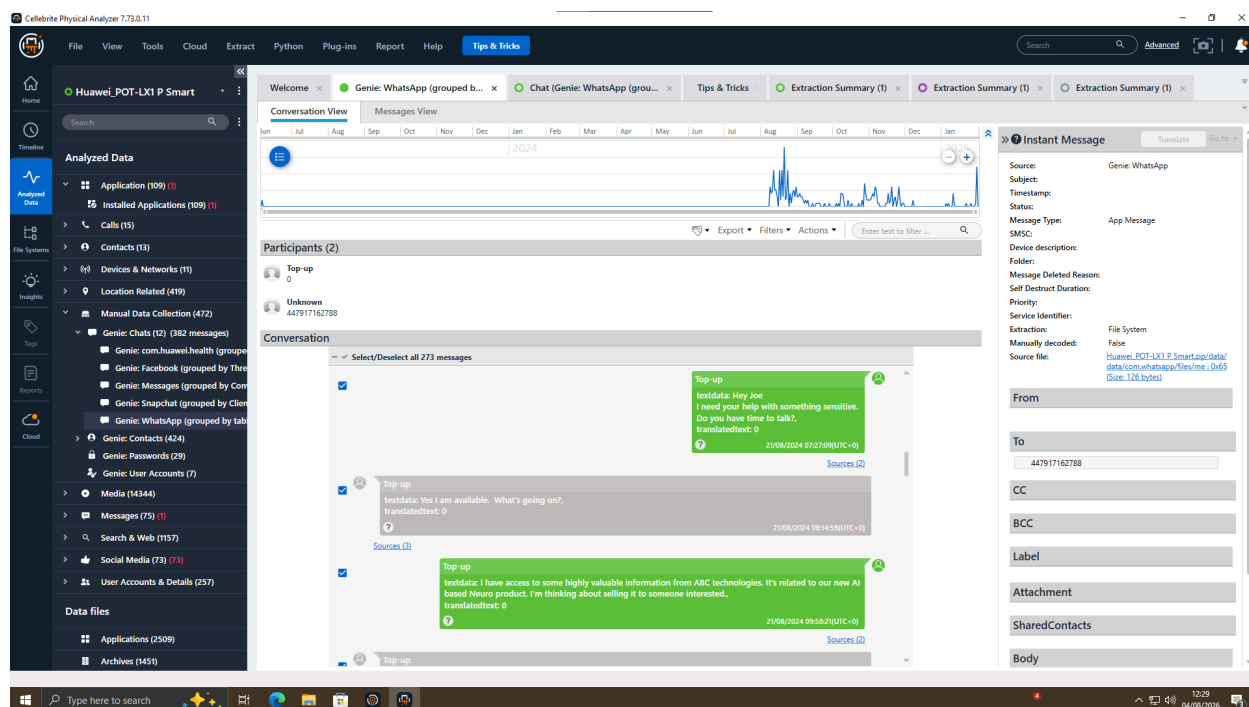


Figure 10: Communication Between Emma and Joe Regarding the Search for a Buyer

From figure 10, it is evident that Emma communicated with Joe on how to find a buyer. The communication is relevant in the sense that it shows how there was an initial communication between the two people involved, and they were discussing how a potential buyer would be found.

Communication gives a clue regarding the nature of interaction. The communication can also be taken into consideration together with the subsequent evidence regarding Norman. From the information at hand, there is evidence regarding communication between Emma and Joe, while there will be subsequent evidence regarding communication between Emma and Norman.

The forensic report also shows that there was communication between Emma and Joe on how to sell the AI-based Neuro product.

2.4. Joe's Intermediary Position

The following section of the evidence shows the position that Joe plays in the process of communication.

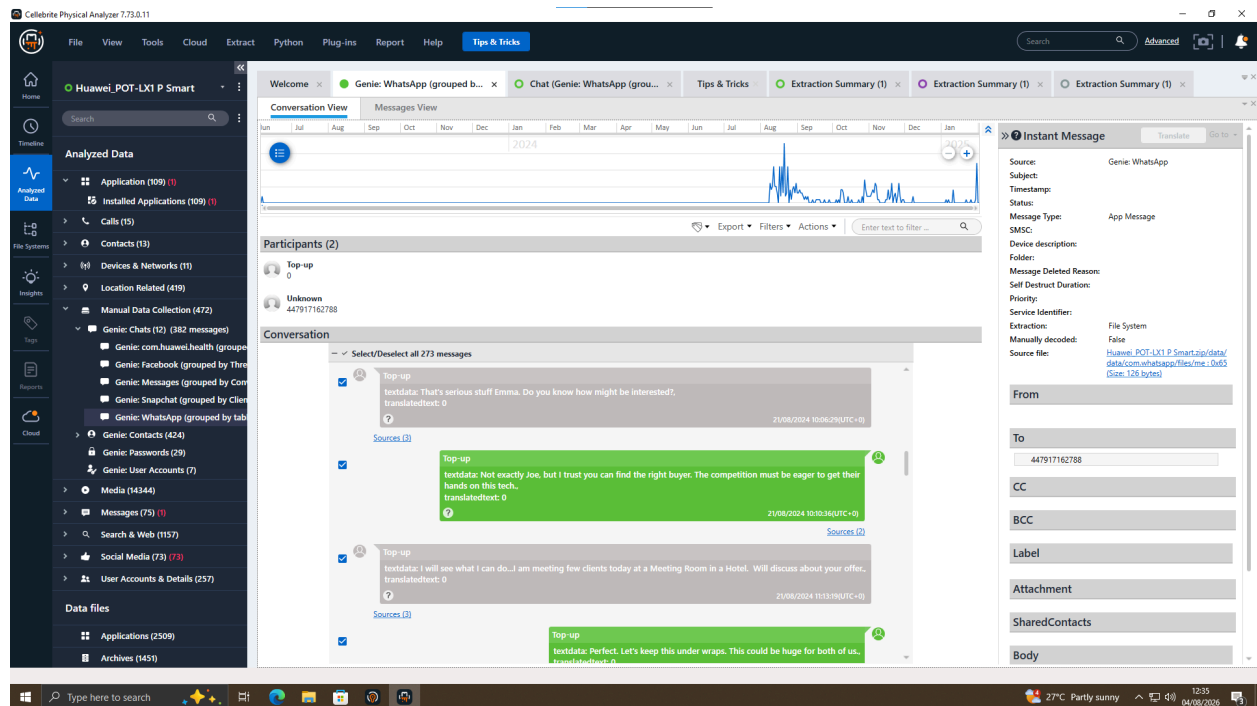


Figure 11: Evidence Concerning Joe's Intermediary Position

Joe appears to play the role of an intermediary in this case. This is significant as it provides an explanation for the connection between the first contact with Emma and the later communication between Emma and Norman.

Instead of communicating immediately with the potential buyer, Emma's interaction started with Joe. This means that Joe's position acts as a connecting link between the various people who were involved in the interaction.

According to the forensics report, Joe plays the role of an intermediary in this case, acting as a logistical buffer between Emma and Norman.

This piece of evidence can therefore be placed between the first communication between Emma and Joe and the latter one between Emma and Norman.

2.5. Direct Communication Between Emma and Norman

The evidence now goes to direct communication between Emma and Norman.

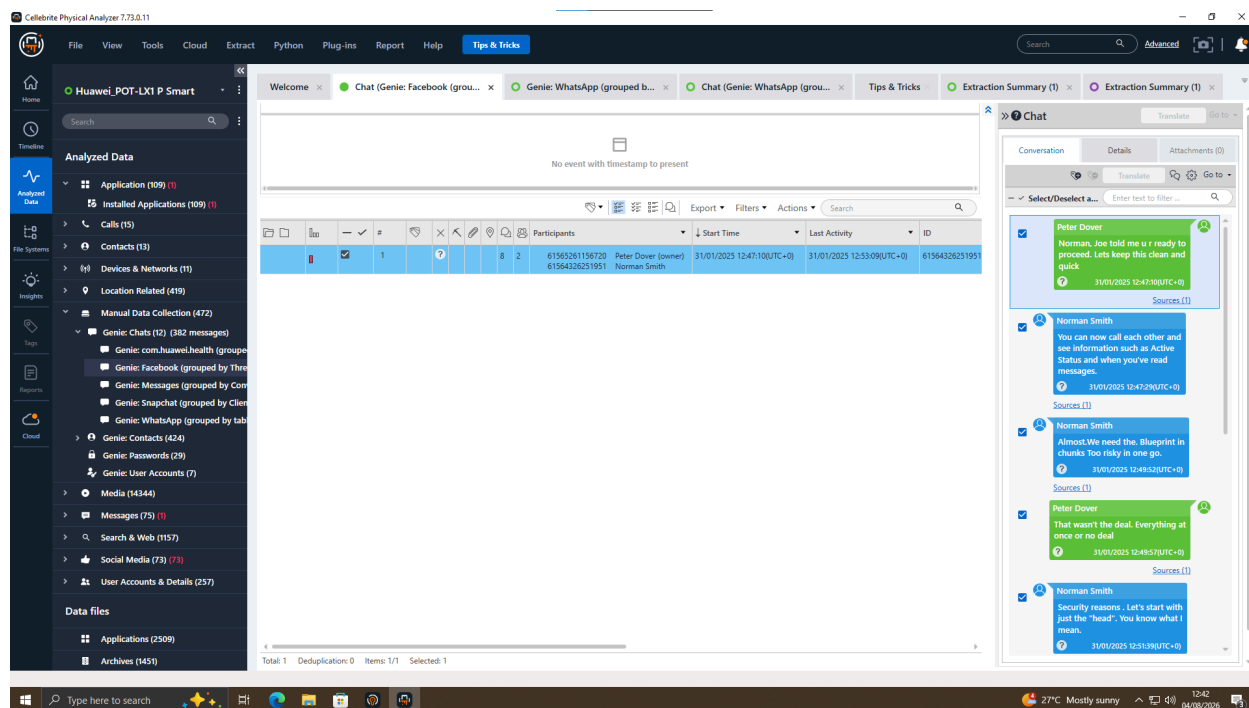


Figure 12: Direct Communication Between Emma and Norman Regarding the Deal

From figure 12, it can be observed that Emma communicated directly with Norman regarding the deal and there was an agreement between them.

It is significant because the previous evidence was based on Emma communicating with Joe. In the case, the direct communication shows that Emma later communicated directly with Norman about the deal.

According to the forensic report, there is another incident where Emma started direct communication with the corporate buyer through Facebook Chats.

The communication can thus be seen to be part of a developing pattern and not an isolated one. It can be compared with other artifacts retrieved using the timestamp to find its place in the overall chronology.

2.6. Conclusion of the Deal

The next piece of evidence relates to the conclusion of the deal.

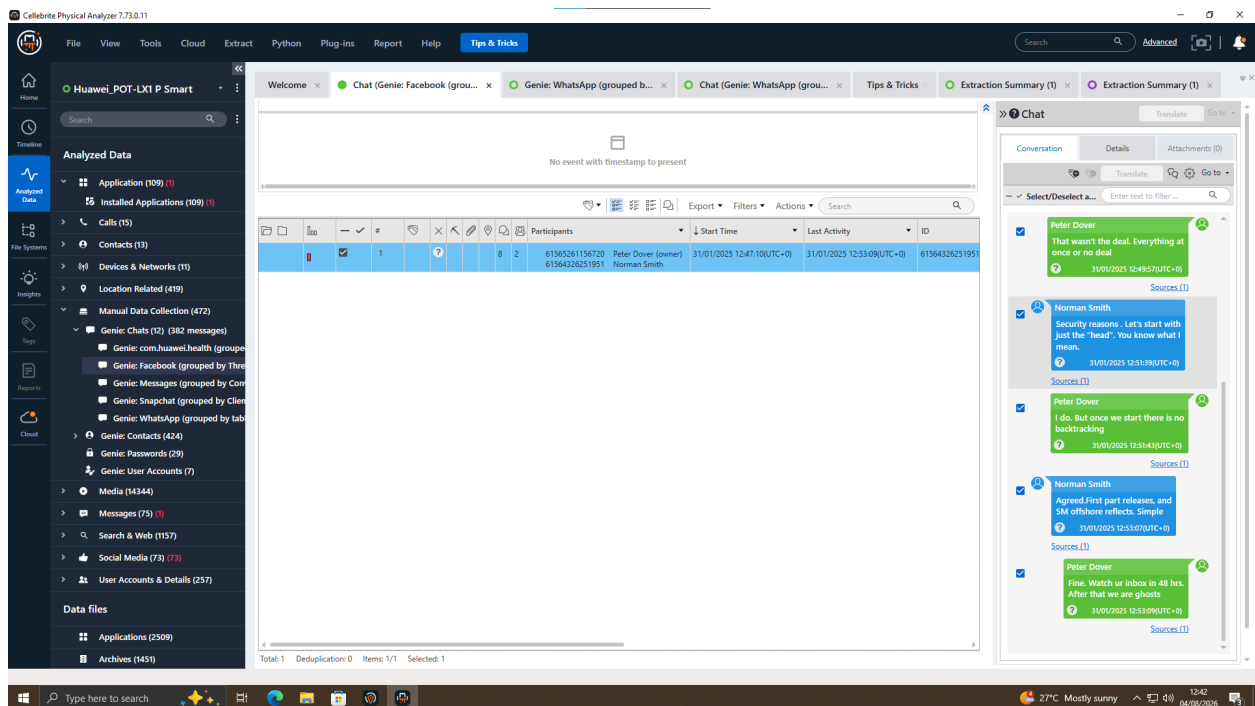


Figure 13: Communication Between Emma and Norman Where the Deal Is Concluded

It can be seen from figure 13 that Emma and Norman have concluded the deal.

This evidence comes later in the course of events. It starts from the first contact where the search for a buyer is initiated; then follows the mediator's intervention by Joe, after which direct communication with Norman is established and finally the deal concludes.

There is another piece of evidence recorded by the forensic report where Norman agrees on the deal.

In showing this piece of evidence, it is good to keep the whole conversation and not just the particular message containing the agreement.

2.7. Hotel Communication

The other interesting piece of evidence is related to a hotel.

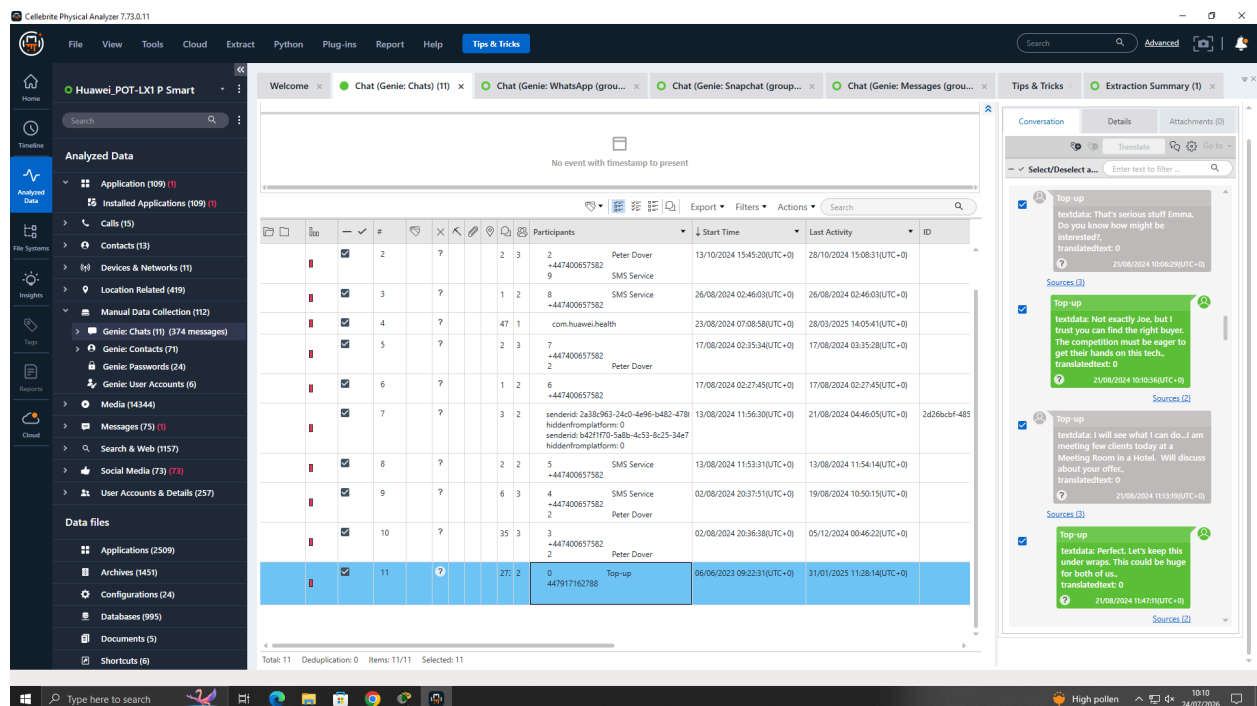


Figure 14: Communication about Emma's Stay at the Hotel

As can be seen from figure 14, Joe told Emma that she is staying at the hotel.

It is important to mention a hotel in this case because one of the other pieces of evidence mentions Joe's phone at the hotel. It allows for combining the evidence about communication and location into a single analysis.

In this way, the connection between the location of the two people and their communication can be established. While the message is the communication evidence, the phone-location data is the geographical one. The forensic report contains information about hotel meetings as well as about correlation of GPS logs during communication and geospatial analysis.

2.8. Manchester Trip of Joe

There is also some information about Joe's trip to Manchester in the evidence.

The screenshot displays the Cellebrite Physical Analyzer 7.73.0.11 interface. The left sidebar shows the 'Analyzed Data' section with various categories like Application (109), Installed Applications (109), Calls (15), Contacts (13), Devices & Networks (11), Location Related (419), Manual Data Collection (112), Genie: Chats (11), Genie: Contacts (71), Genie: Passwords (24), Genie: User Accounts (6), Media (14344), Messages (73), Search & Web (1157), Social Media (73), User Accounts & Details (257), and Data files. The main window shows a list of analyzed data items with columns for Participants, Start Time, Last Activity, and ID. The right sidebar shows a chat conversation with a search bar and a list of messages.

Participants	Start Time	Last Activity	ID
2 +447400657582 9 SMS Service	13/10/2024 15:45:20(UTC+0)	28/10/2024 15:08:31(UTC+0)	
8 +447400657582 SMS Service	26/08/2024 02:46:03(UTC+0)	26/08/2024 02:46:03(UTC+0)	
com.huawei.health	23/08/2024 07:08:58(UTC+0)	28/03/2025 14:05:41(UTC+0)	
7 +447400657582 2 Peter Dover	17/08/2024 02:35:34(UTC+0)	17/08/2024 03:35:28(UTC+0)	
6 +447400657582	17/08/2024 02:27:45(UTC+0)	17/08/2024 02:27:45(UTC+0)	
senderid: 2a38a963-24c0-4e96-b482-478f hiddenfromplatform 0 senderid: b421f170-5a1b-4c53-8c25-34e7 hiddenfromplatform 0	13/08/2024 11:56:30(UTC+0)	21/08/2024 04:46:05(UTC+0)	2d26bcdf-485
5 SMS Service	13/08/2024 11:53:31(UTC+0)	13/08/2024 11:54:14(UTC+0)	
6 SMS Service	02/08/2024 20:37:51(UTC+0)	19/08/2024 10:50:15(UTC+0)	
2 +447400657582 2 Peter Dover	02/08/2024 20:36:38(UTC+0)	05/12/2024 00:46:22(UTC+0)	
3 +447400657582 2 Peter Dover	02/08/2024 20:36:38(UTC+0)	05/12/2024 00:46:22(UTC+0)	
0 Top-up 447917162788	06/06/2023 09:22:31(UTC+0)	31/01/2025 11:28:14(UTC+0)	

Chat conversation details:

- Top-up: textdata: Hi Joe, Any update on the offer? It is disappointing that no response from u. I have managed to find someone with whom I am meeting over the next weeks. translatedtext: 0
- Top-up: textdata: I may go with someone. If u r not interested, translatedtext: 0
- Top-up: textdata: Apologies Emma. I am in a final talks about it. Meeting the client this week at Manchester. Will update. translatedtext: 0
- Top-up: textdata: Premal Barcia Jegaders 2824 Altana Bonmati and Lamine Yamal have got their trophies. translatedtext: 0

Figure 15: Communication Regarding Joe's Meeting with Clients in Manchester

From figure 15, we can see that Joe was planning to go to Manchester in order to meet his clients there.

This is another piece of evidence showing movement on the part of Joe. This also introduces another important location in the case – Manchester.

2.9. Joe's Travel Ticket to Glasgow

This investigation further involves a travel ticket belonging to Joe's Glasgow travels.

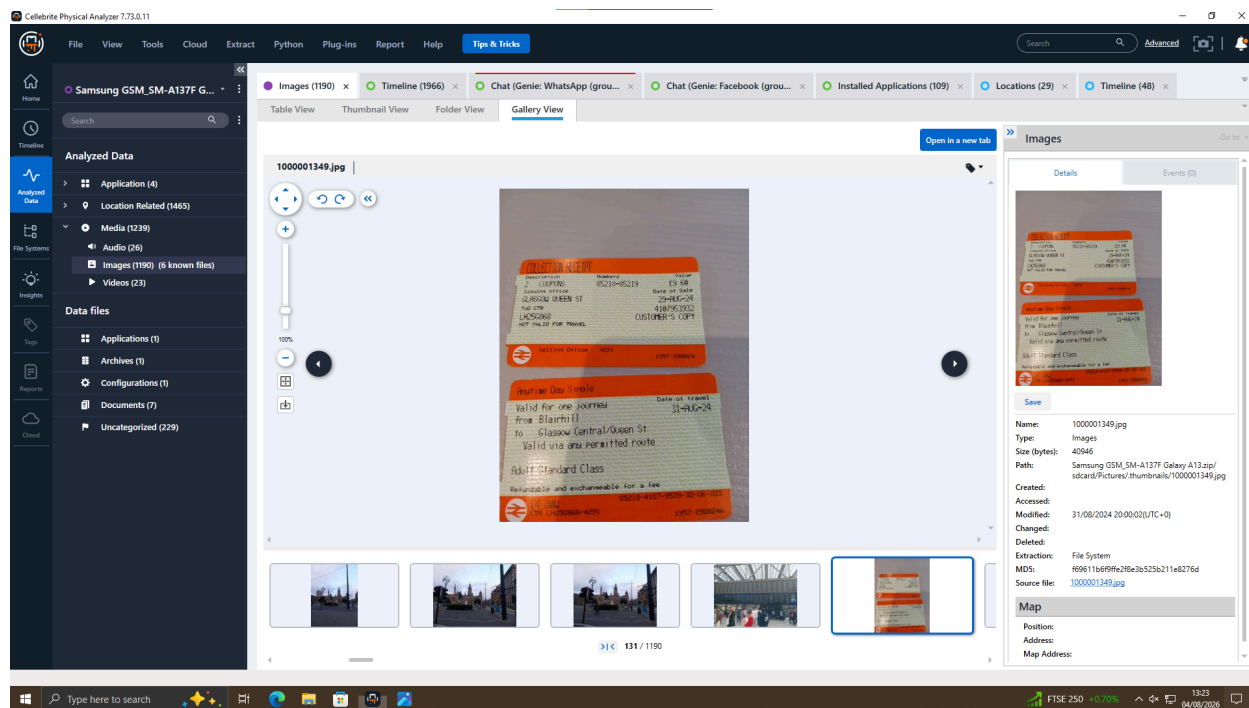


Figure 16: Joe's Travel Ticket to Glasgow

Figure 16 depicts the Glasgow travel ticket belonging to Joe. The ticket could be used in comparison with any communications relating to the Glasgow activities, if such communications are found in the entire evidential material available.

2.10. Location of Joe's Mobile Phone at the Hotel

Another point of evidence is the location of Joe's mobile phone.

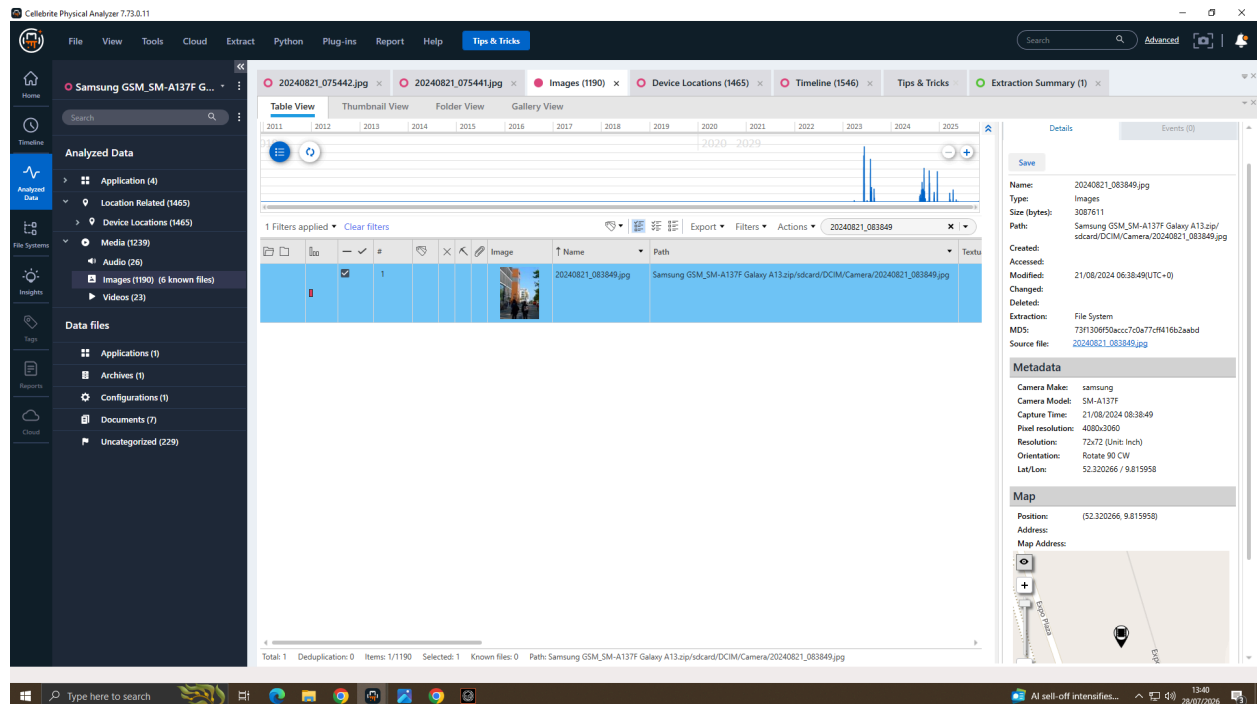


Figure 17: Location of Joe's Mobile Phone at the Hotel

Figure 17 above depicts the location of Joe's mobile phone at the hotel.

It is crucial since it may be compared with the previous evidence about the hotel shown in Image 8 below. Both of these pieces of evidence offer different kinds of information about the same location.

While figure 14 is related to communication evidence, figure 17 relates to location evidence. While communication suggests that the hotel was relevant to the individuals, the location shows that Joe's mobile phone was at that location.

According to the forensic report, geospatial analysis was part of the investigation process, and GPS logs were correlated with a hotel meeting.

2.11. Geospatial and Location Evidence (Norman)

This case does not involve only communication artefacts as described in the presentation. It also involves geospatial analysis which includes correlation of GPS logs and confirmed meetings at the hotel.

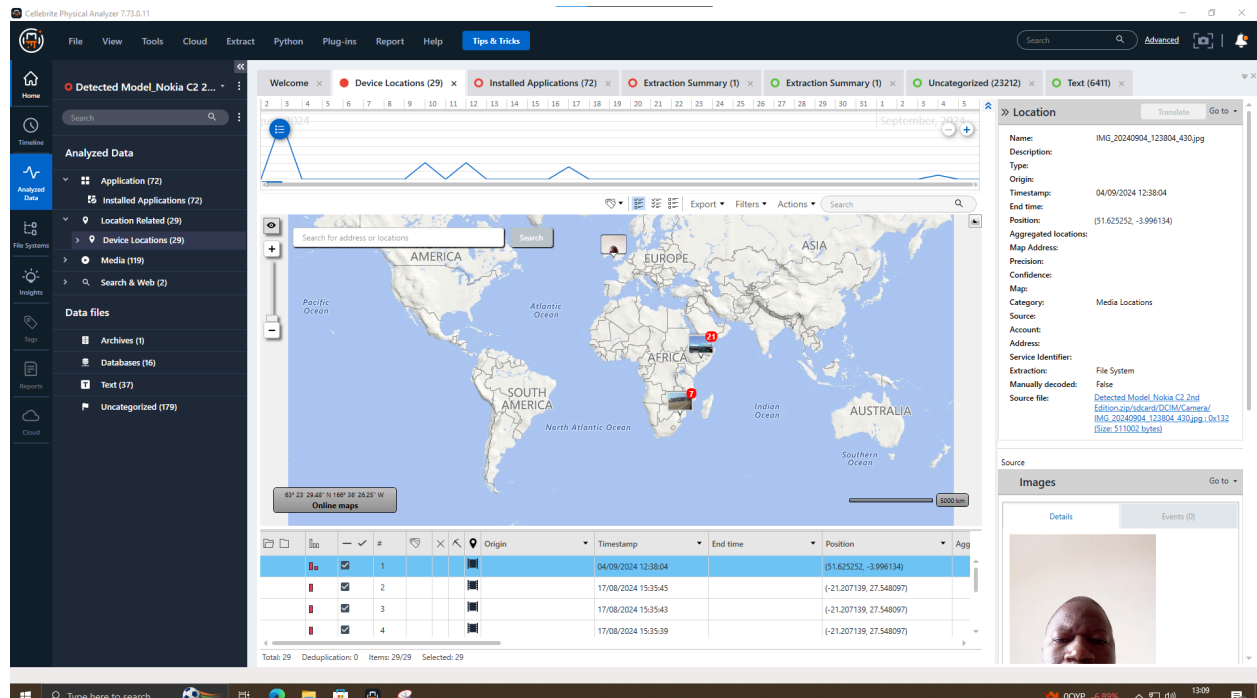


Figure 17: Norman travelled to the exact same region for meet with Joe.

The mobile acquisition evidence includes location artefacts whereas the investigation presentation identifies a location event involving Norman. The timeline identifies an event of 04/09/2024 12:08:04 whereby the evidence source is defined as the location of Nokia C2 device, geolocation mapping records were involved in establishing the artefact.

Location artefacts can be especially helpful when correlated with communication artefacts. For instance, when a communication is showing a scheduled meeting but the location of the person on the other device shows he/she is at the same place, the two artefacts can help in the reconstruction of the events.

However, location artefacts need to be treated carefully because of differences in precision of the GPS artefacts. The investigator needs to

establish the source, time and precision of the location evidence in order to draw any inference. This case does not involve location artefacts independently of the communication artefacts.

2.12. Profiling the Suspects and Behavioral Analysis

The suspects' roles are divided into three different individuals: Emma, Joe, and Norman. Emma is recognized as the alleged perpetrator, Joe as the intermediary, and Norman as the buyer.

Emma is characterized by authorized access and the use of access in committing the crime against the QT-AI-2025 patent for personal benefit and intellectual property betrayal. Joe acts as a logistical intermediary for minimizing the direct contact between Emma and Norman. Norman is recognized as the buyer and is characterized by anti-forensic behavior.

The above type of profiling is helpful because it tries to establish the relationship between the digital evidence and the roles played by the suspects. The examiner should be careful not to conclude any role of a person without tangible evidence.

It is best, therefore, to relate the alleged role of each suspect with digital evidence.

2.13. Timeline Reconstruction

Date	Suspect	Event
21/08/2024	Emma and Joe	Emma communicated with Joe in order to get the buyer.
21/08/2024	Emma and Joe	Joe was the intermediary in the communication process.
21/08/2024	Joe and Emma	Joe communicated to Emma about her presence in the hotel.

20/11/2024	Joe	Joe communicated to Emma that he is on his way to Manchester.
31/01/2025	Emma and Norman	Emma contacted Norman and came to an agreement with him
31/01/2025	Emma and Norman	Emma and Norman concluded the deal.
31/08/2024	Joe	The travel ticket for Glasgow was found.
21/08/2024	Joe	Joe's phone was found in the hotel.
04/09/2024	Norman	Norman's phone was found in the meeting place.

2.14. Conclusion and Recommendations

In conclusion, the above report has shown how mobile phones could be forensically analyzed to recreate a suspect digital espionage. The three mobiles used in the investigation were marked as exhibits while SHA-256 hashes were used in the process of proving evidence integrity. Cellebrite UFED and Physical Analyzer V7 were used as the main set of forensic tools.

In terms of the communications analysis, the communication between Emma, Joe and Norman, along with evidence related to the alleged sale of the AI-based information has been found out. Additionally, anti-forensic communication and SIM card removal were established. Next, geospatial evidence and GPS data were linked to communication evidence, which included the hotel meeting and Nokia C2 location.