



Student Name: Md Ahasanul Kobir Opy

Student ID: 2522648

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

Table of Contents

Task 1: Digital Forensics as a Strategic Cybersecurity Capability

- 1.1 Introduction
- 1.2 The Field Now and the Tools Used
- 1.3 Cybersecurity Convergence
- 1.4 Emerging Technologies
- 1.5 Challenges
- 1.6 Career Outlook
- 1.7 Recommendation
- 1.8 Conclusion
- 1.9 References

TASK -2

Personal Mobile Phone Acquisition Using Cellebrite UFED

- 2.1 Introduction
- 2.2 Case Information and Evidence Identification
- 2.3 Identification of the Mobile Device
- 2.4 Choosing the Location of the Extraction
- 2.5 Selecting the Content to Extract
- 2.6 Analysis of the Extraction Process
- 2.7 Evaluation of the Mobile Phone Forensic Acquisition
- 3. Mobile Forensic Evidence Analysis and Event Reconstruction
 - 3.1 Introduction
 - 3.2 Device Identification and Hashing
 - 3.3. First Communication Between Emma and Joe
 - 3.4. Joe's Plan for Manchester
 - 3.5 Manchester Travel Ticket
 - 3.6 Location of the Hotel
 - 3.7. Glasgow Travel Document
 - 3.8 Direct Contact Between Emma and Norman
 - 3.9 Closure of the Agreement
 - 3.10 Location of Norman's Mobile Phone

3.11 Timeline Reconstruction

3.12 Conclusion

Task 1: Digital Forensics as a Strategic Cybersecurity Capability

1.1. Introduction

Digital forensics is becoming more of a strategy than just an investigation technique after the crime has been committed. Since organisations use computers to communicate, transact, and do other business activities, it means that any cyber attack can have serious repercussions for the organisation. The use of digital forensic methods gives organisations the capability to understand what happened and to preserve the evidence [1].

The evolution of digital forensics has been largely caused by the development of cloud computing, mobile technology, IoT, and artificial intelligence. Thus, current digital forensics should take into account both the technical aspect and the organisational environment in which the evidence has been collected.

1.2. The Field Now and the Tools Used

Conventional computer forensics continues to be crucial. Tools such as Autopsy, FTK, EnCase and Magnet AXIOM enable an examination of the storage media and identification of artifacts linked to user activity. These include file-system analysis, metadata analysis, deleted file extraction and timeline generation.

There has been a need for specialized capabilities, however. Cellebrite UFED and XRY provide capabilities for mobile investigations while Wireshark facilitates network traffic analysis. Memory forensics tools provide the capability to analyze volatile data that can be lost once the system is switched off.

The critical development is the shift toward integration in forensic tools. Instead of analyzing individual pieces of evidence in isolation, analysts increasingly correlate evidence from multiple sources – from endpoints, through networks, mobile devices and cloud services.

This trend is crucial because a single artifact often does not reveal anything about the cyber attack in question. A suspicious login becomes even more interesting when correlated with execution records on the endpoint and network connections.

1.3. Cybersecurity Convergence

In regard to incident response, the connection between digital forensics and cybersecurity is particularly high. Cybersecurity practitioners will find and isolate the compromised devices and begin containing the situation. Digital forensics practitioners will be collecting and analyzing the evidence to build a timeline of the attack.

For instance, in case of an attacker gaining administrative access, the cybersecurity measures will detect strange authentication activities. Digital forensics will reveal whether the attacker was running commands, creating persistence methods and accessing any files.

It means that digital forensics will help in detection, reaction, recovery and learning lessons. Additionally, it might provide some information for the threat intelligence, revealing methods used by attackers and their infrastructure.

1.4. Emerging Technologies

The first important trend is AI-assisted forensic analysis. Artificial intelligence can assist in classifying, analysing and identifying patterns within large datasets for investigations. The studies of mobile forensics reveal that image classification is one of the areas in which artificial intelligence techniques are being studied [3].

The second important trend is the use of language models to assist investigations. Language models might assist in summarising large amounts of texts, identifying relationships in communications and preparing investigative documentation. Nevertheless, the work of Wickramasekara et al. mentions the issues of explainability, bias and legal issues which need to be considered before LLMs can be used for autonomous forensic decision-making [4].

The third important trend is IoT forensic readiness. Forensic evidence in the IoT environment is produced by sensors, applications and network communication. Friedl and Pernul argue that forensic readiness requires legal, technical, organizational and human factors [5]. Therefore, organizations should consider the forensic requirements at the stage of IoT environment design instead of waiting for incidents.

Another emerging trend is the edge-based forensic acquisition. Ruiz-Villafranca et al. show how an edge node can monitor the IoT environment and assist in evidence identification and acquisition [6].

1.5. Challenges

One of the major challenges is that of evidence scale. Increasing amounts of digital data make full manual processing impossible. Automation becomes an essential part of the process then.

The second issue is the fragmentation of the data. Evidence can be spread across multiple devices and cloud service providers. Thus it is hard to correlate and jurisdiction issues arise.

The third challenge is the issue of privacy. Smartphones and cloud services can have huge amounts of personal, but irrelevant data. That means the investigators have to use proportional methods of acquisition and processing.

Also, the practitioner research indicates the existence of organisational and professional challenges for digital forensic investigators. The UK investigators had some issues related to workload, relations with investigating officers, lawyers and forensic technology validation [7].

1.6. Career Outlook

The field is evolving in parallel to the technologies used. The traditional occupations like Digital Forensic Examiner and Digital Investigator are still relevant, but career options are increasingly combined with those of DFIR Analyst, Cyber Incident Responder, Cybersecurity Analyst, Threat Intelligence Analyst and Security Operations Specialist.

The labour market for cybersecurity in the UK included approximately 143,000 employees in 2024, whilst the annual shortage of personnel was expected to amount to about 3,800 individuals. The deficiency of digital forensic expertise was one of the fields of technical skills shortages in cyber-sector companies.

Similar recruitment takes place internationally in both cybersecurity and forensic areas.

1.7 Recommendation

A contemporary digital forensics student must develop a multi-level skillset. The first level should involve knowledge of operating systems and cybersecurity concepts. The second should cover forensic acquisition, analysis, and reporting skills. The third level should consist of specialized skills like memory forensics, mobile forensics, cloud forensics, and IoT forensics. Lastly, a knowledge of Python and AI should be acquired.

1.8. Conclusion

Digital forensics has proven to be very strategic in cybersecurity since the organizations require evidence for understanding and responding to any attacks. Future investigations will require distributed and automated environments for evidence. Experts who have forensic skills in addition to their knowledge of cybersecurity and new technology will be well placed to deal with this change in cybercrime.

1.9. References

1. Dunsin et al., "A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response"
<https://scholar.google.com/scholar?q=%22A+comprehensive+analysis+of+the+role+of+artificial+intelligence+and+machine+learn+ing+in+modern+digital+forensics+and+incident+response%22>

[ng%22](#)

2. Vasilaras et al., "Artificial intelligence in mobile forensics," 2024.
<https://scholar.google.com/scholar?q=%22Artificial+intelligence+i+n+mobile+forensics%22+Vasilaras>
3. Wickramasekara, Breitinger and Scanlon, LLMs and digital forensic investigation
<https://scholar.google.com/scholar?q=Wickramasekara+Breitinge+r+Scanlon+large+language+models+digital+forensics>
4. Deep-learning solutions for malware detection and forensic analysis in IoT, 2024.
<https://scholar.google.com/scholar?q=%22Systematic+review+of+deep+learning+solutions+for+malware+detection+and+forensic+analysis+in+IoT%22>
5. AI and machine learning for cybercrime investigation
<https://scholar.google.com/scholar?q=artificial+intelligence+mac+hine+learning+digital+forensics+cybercrime+investigation>
6. Machine learning for digital forensic investigation
<https://scholar.google.com/scholar?q=machine+learning+digital+f+orensic+investigation>
7. AI-assisted digital evidence analysis
<https://scholar.google.com/scholar?q=AI-assisted+digital+eviden+ce+analysis>

Task 2: Personal Mobile Phone Acquisition Using Cellebrite UFED

2.1. Introduction

This practical demonstration was intended to illustrate how digital evidence could be obtained from a personal mobile phone by using Cellebrite UFED. There are various types of information that may be found on a mobile device that could assist the investigator to know more about the activities carried out by the user of the device and their digital behavior. Nevertheless, prior to any analysis of the information, the collection of the same needs to take place.

In the present acquisition process, the mobile phone being analyzed was an Apple A2482 iPhone 13. Cellebrite UFED was used in order to profile the mobile phone, configure the extraction, choose the evidence categories and carry out the acquisition. The extraction window showed the result of the data collected. Thus, the screenshots serve as the documentation of the practical process.

2.2. Case Information and Evidence Identification

The acquisition started with the creation of a new case within the software Cellebrite UFED. The details about the case contained “identifier Md Ahsanul Kobir Opy,” examiner “Mohammad,” and “device/evidence iPhone13.” The type of crime is noted as “Theft,” while the department is noted as “Cyber Security” and location as “London.”

Such information is helpful as in the course of forensic analysis it needs to know what evidence is under investigation and who is the examiner. By entering such information before acquisition we create a

base for the information to be used later while creating a forensic report.

Cellebrite UFED 7.76.0.24 [Educational]

CASE DETAILS

NEW CASE

Case Identifier
Md Ahasanul Kobir Opy

Examiner Name
Mohammad

Device Name / Evidence Number
iPhone13

Crime Type
Theft

Department
Cyber Security

Location
London

Last Case Details:

Case Identifier:
Md Ahasa nul

Examiner Name:

Device Name / Evidence Number:

Crime Type:

Department:

Location:

USE LAST DETAILS

ABORT BACK CONTINUE

Figure 2.1: Forensic case creation and recording of the case and investigation details using Cellebrite UFED.

2.3. Identification of the Mobile Device

After the case had been created, the phone was attached to the forensic computer and the system detected it as an Apple A2482 iPhone 13 through the Detect Device screen of Cellebrite.

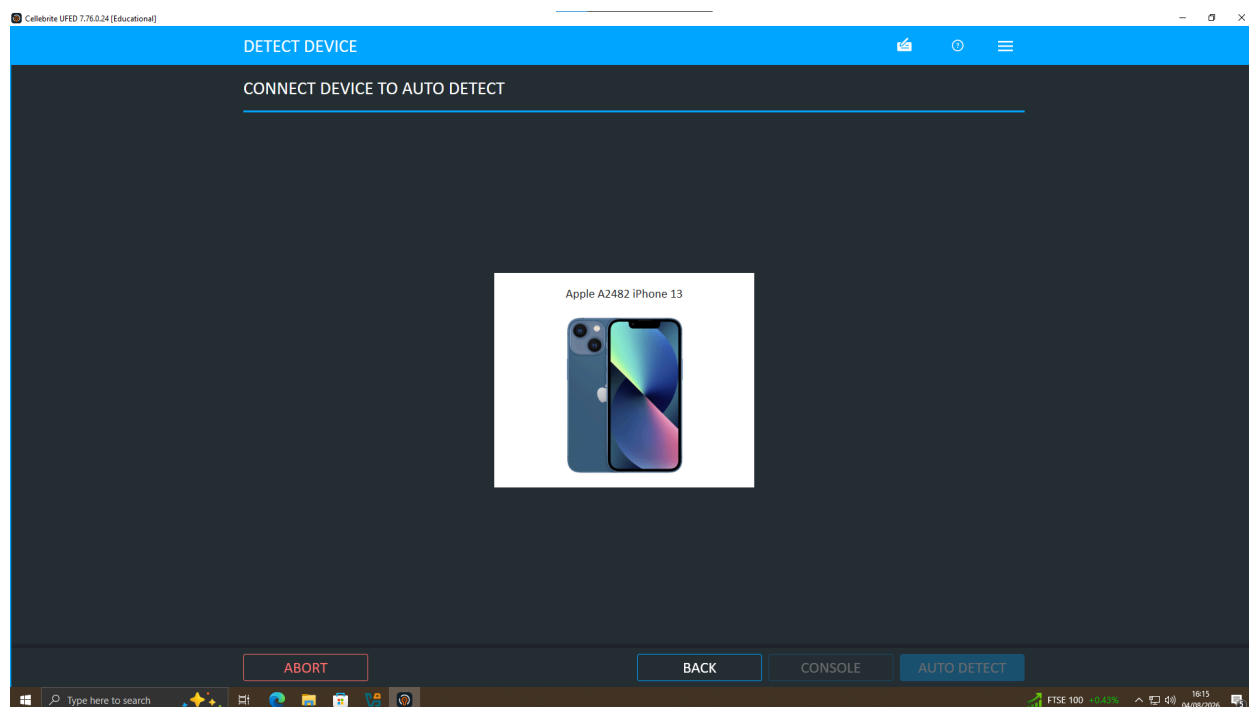


Figure 2.2: Automatic detection of the Apple A2482 iPhone 13 by Cellebrite UFED.

This is one of the key steps in the procedure. Prior to data extraction, the examiner needs to be absolutely sure that he or she is dealing with the right device. In this case, Cellebrite recognised the phone correctly, providing the appropriate device information.

It should also be noted that automatic recognition of the supported devices by the acquisition tool is one of its benefits as it allows for more options in terms of identification of the phone.

2.4. Choosing the Location of the Extraction

Having identified the device, the acquisition needed a destination where the extracted data would be saved. The device appeared on the screen as Apple A2482 iPhone 13 and was connected via USB cable.

For the current extraction, the local drive was chosen as a destination with the path as follows:

E:\Md Ahsanul Kobir Opy

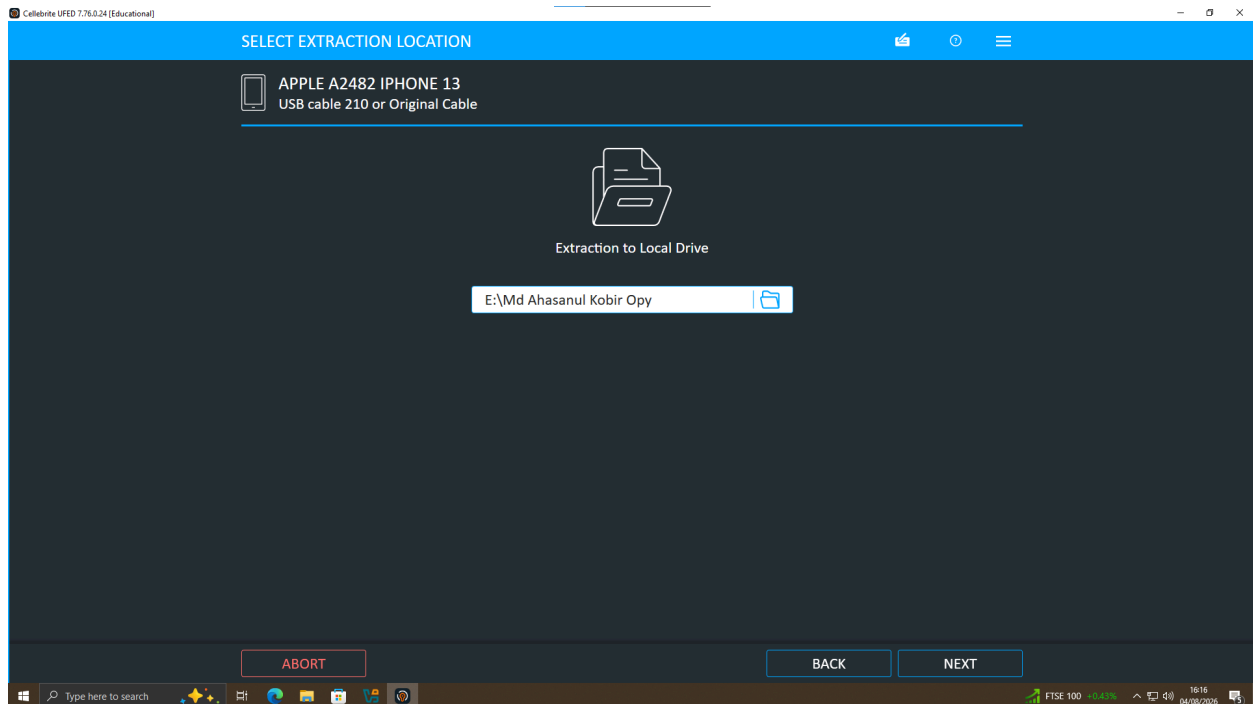


Figure 2.3: Selection of the local drive and destination folder for the extracted evidence.

This stage is important in the sense that the evidence gathered during the acquisition process needs to be saved somewhere. A dedicated location is very important for organising the extracted evidence.

The importance of using a particular folder becomes critical especially if there are several forensic cases being worked on by one examiner.

2.5. Selecting the Content to Extract

Afterward, Cellebrite presented the user with the Select Content Type screen. Numerous data categories were available for extraction from

the device. Such as Call Logs, Locations, Advertising ID, Contacts, SMS, MMS, Calendar, Pictures, Audio/Music, Videos, Ringtones, Documents, Archives, Email, IM, Browsing Data, and Files.

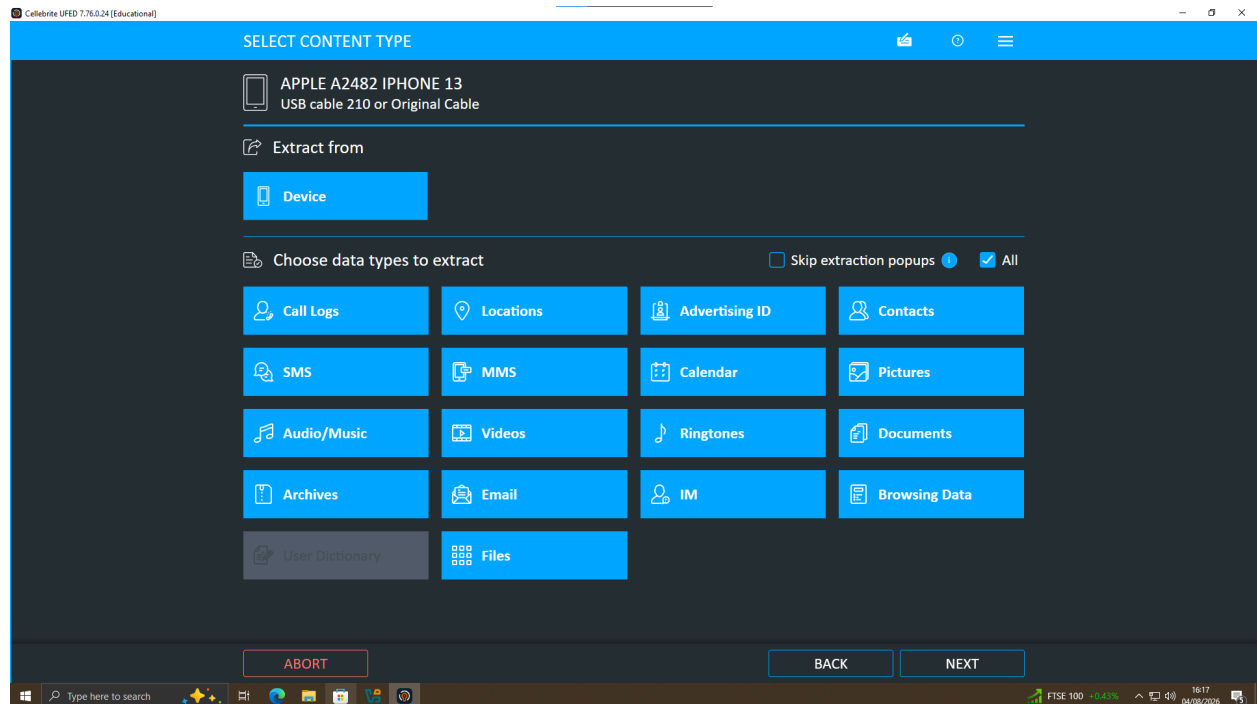


Figure 2.4: Selection of the different content categories for extraction from the iPhone 13.

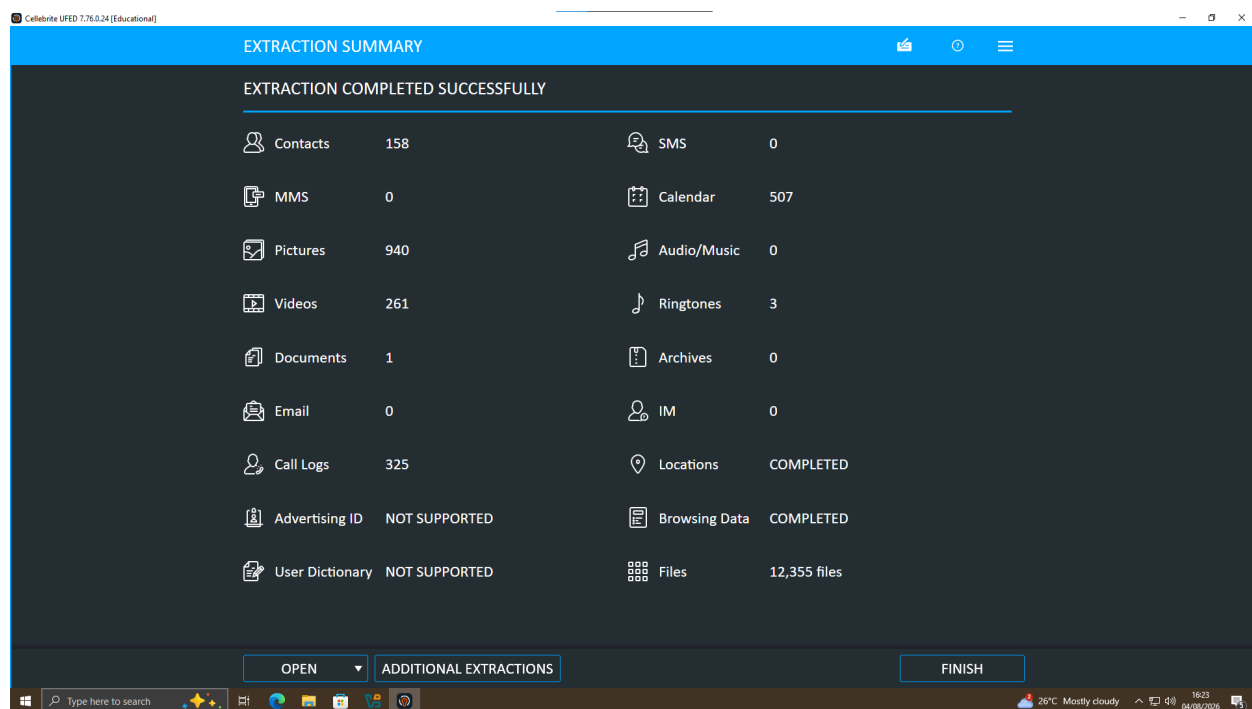
This screen indicates that numerous kinds of digital evidence can be contained in a smartphone. For instance, contact data can reveal the identity of people who have some connection to the device; calendar entries can be useful for scheduling activities; images and videos may hold information about events or locations.

Therefore, the investigator should decide on the categories of evidence relevant to the case at hand. The selection process is also an opportunity to set up the acquisition prior to processing. Additionally, the investigator is made aware of what kind of evidence will be extracted using the forensic software.

2.6. Analysis of the Extraction Process

Once the extraction process has been finished, the Cellebrite presents the Extraction Summary. The software indicated that the extraction process has been successfully completed and provided information on what kind of information has been acquired from the phone.

As for the data, the result indicates 158 contacts, 507 calendar items, 940 photos, 261 videos, 3 ringtones, 1 document and 325 call logs. Moreover, there have been 12,355 files extracted. SMS, MMS, audio/music, archives, email and IM are equal to zero. Locations and Browsing history have been completed. Advertising ID and User dictionary are listed as not supported.



EXTRACTION SUMMARY	
EXTRACTION COMPLETED SUCCESSFULLY	
Contacts	158
MMS	0
Pictures	940
Videos	261
Documents	1
Email	0
Call Logs	325
Advertising ID	NOT SUPPORTED
User Dictionary	NOT SUPPORTED
SMS	0
Calendar	507
Audio/Music	0
Ringtones	3
Archives	0
IM	0
Locations	COMPLETED
Browsing Data	COMPLETED
Files	12,355 files

Figure 2.5: Cellebrite UFED extraction results summary with information about the volume of extracted data.

This summary is helpful as it gives insight into the results of the data acquisition process. It was successful since a great amount of data was gathered. Especially worth mentioning is the high number of

images and general files acquired. There were 940 images and 261 videos which might be very helpful for the investigation, depending on the situation.

It is also necessary to carefully analyze the results obtained. If there was zero data found in one of the categories, it does not prove the fact that the phone had never had such data at all. This fact just means that this category has been retrieved as a result of this particular extraction.

Mobile Forensic Evidence Analysis and Event Reconstruction

3.1. Introduction

Mobile phones are capable of storing different types of data that could turn out to be useful during forensics. Messages can help in understanding the connections between people and their conversation, whereas travel information and location data can prove valuable when it comes to establishing movements and connections. Thus, the process of forensics is not only about the extraction of files, but also about building the relations between them.

In this particular case, the evidence set includes three records of hash of mobile phones, communication with Emma and Joe, travel data from Manchester and Glasgow concerning Joe, direct communication between Emma and Norman and location data for Joe and Norman. The evidence set can be organized in the following sequence: the identification and hashing of the mobile phones, communication concerning buyers and client meetings, travel data and direct

communication concerning the deal and the locations of the people involved.

3.2. Device Identification and Hashing

The first three pieces of evidence are linked to the mobile phones that were used during the examination. Information about the hashes of the Huawei, Samsung and Nokia mobiles was collected.

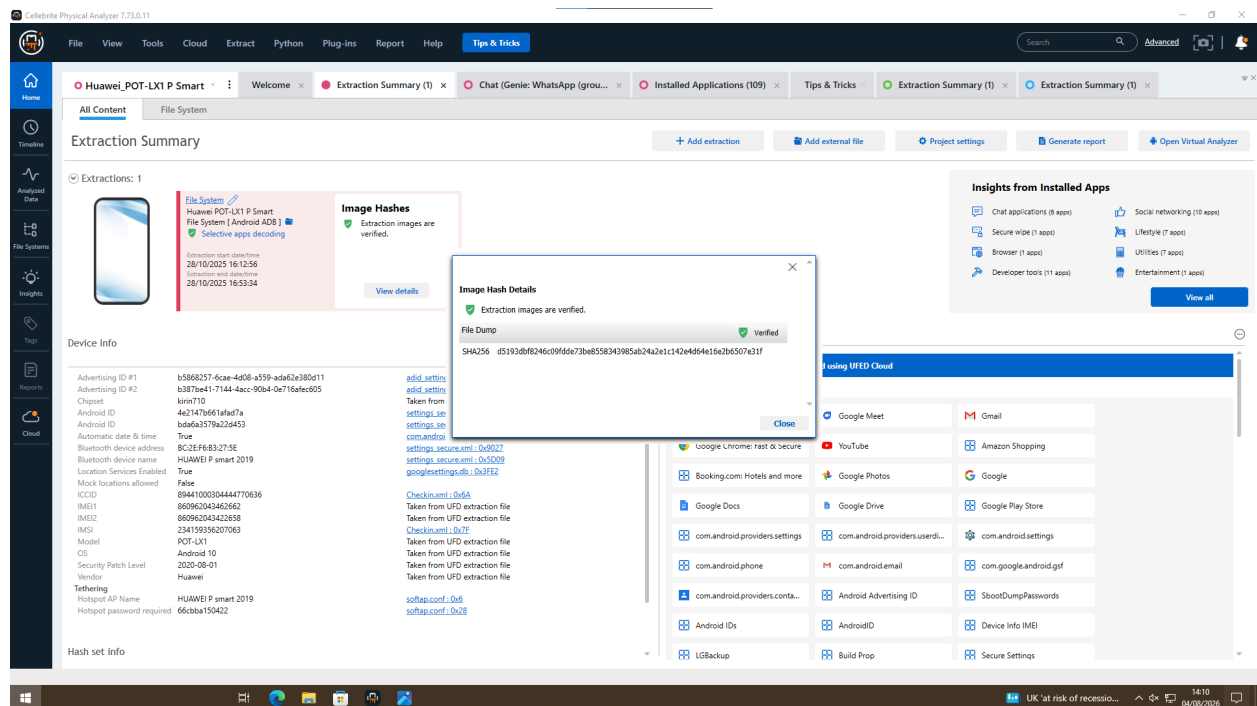


Figure 3.1: Hash Record of Huawei Mobile

The hash of the Huawei mobile is evidence of identification of the first device. Registration of the hash will allow the examiner to create evidence identification with respect to the acquired evidence.

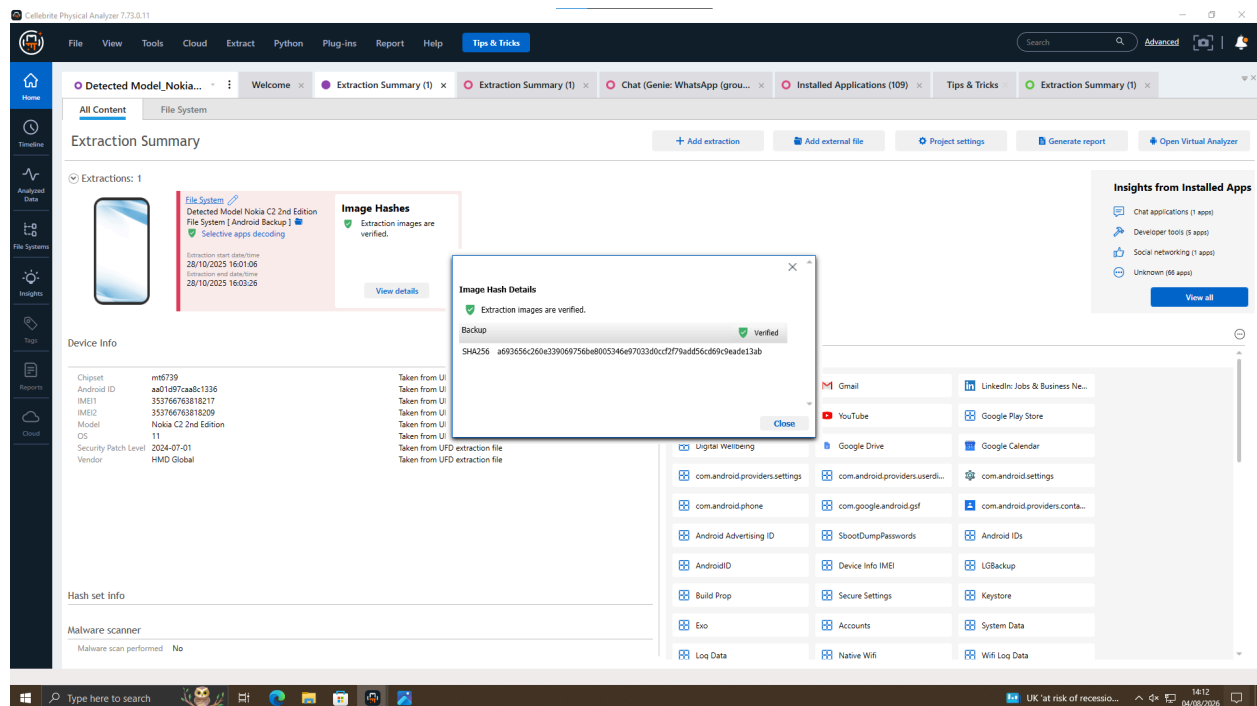


Figure 3.2: Hash Record of Samsung Mobile

The second device is identified by means of the hash of the Samsung mobile. Given the multiple devices being used, it becomes necessary to keep the evidence records separate in order to associate each device with its corresponding evidence.

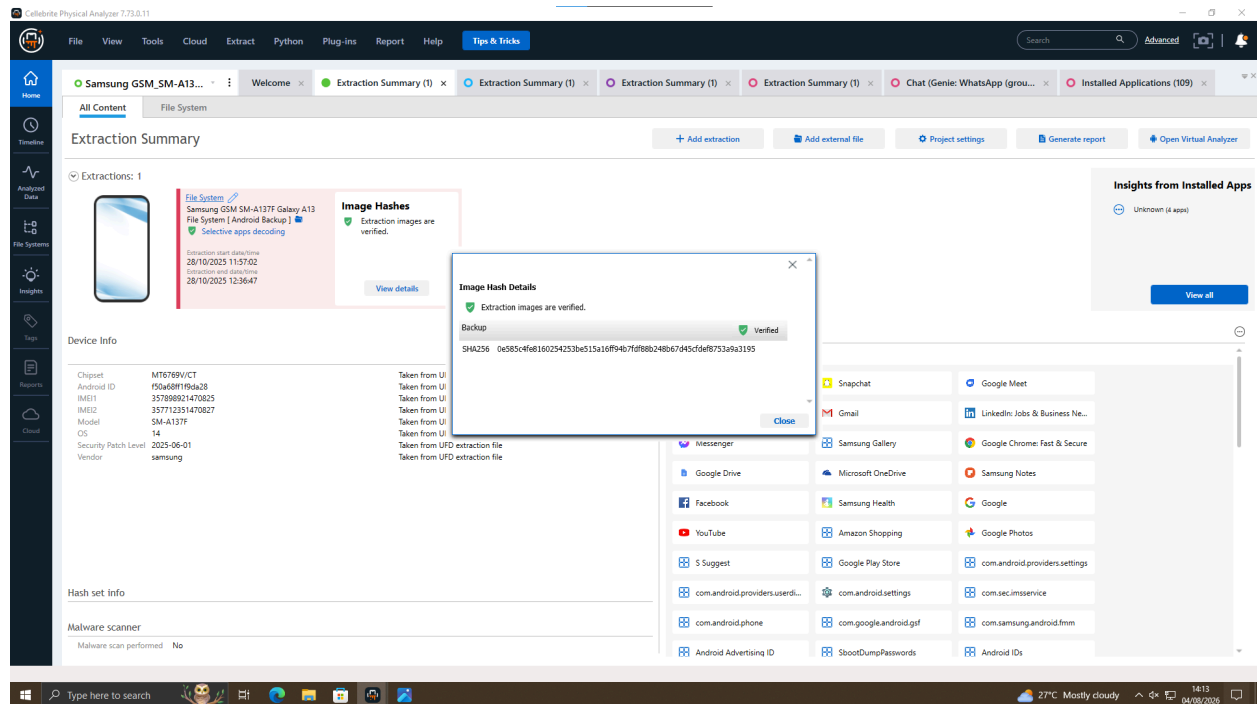


Figure 3.3: Hash Record of Nokia Mobile

The Nokia mobile closes the list of hashes records.

3.3. First Communication Between Emma and Joe

The communication evidence starts with the communication between Emma and Joe.

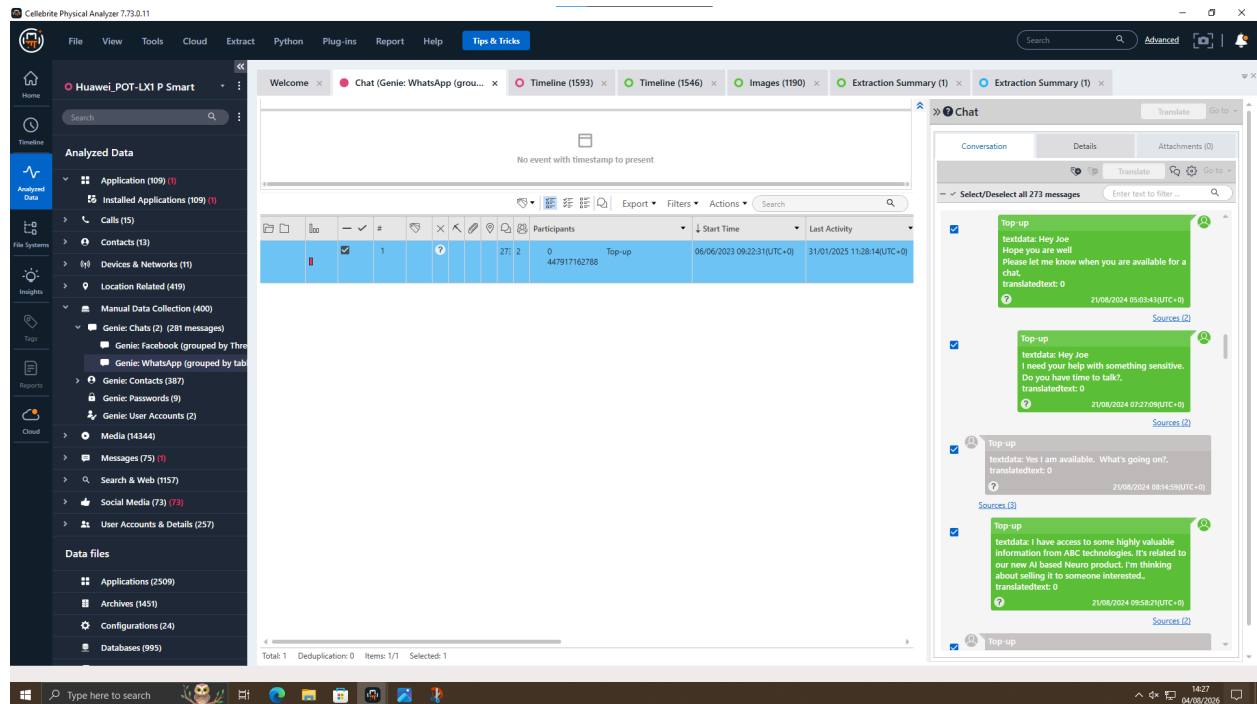


Figure 3.4: Communication of Emma and Joe on Search for a Buyer

It is evident that Emma communicated with Joe to look for a buyer. It is a key evidence since it helps to establish a relationship between the two people as well as to identify the search for a buyer as one of the first events.

A timestamp from this communication will help the examiner to place the communication in the general timeline. Further evidence related to Norman can then be compared with this first evidence.

3.4. Joe's Plan for Manchester

The second communication has to do with Joe's travels.

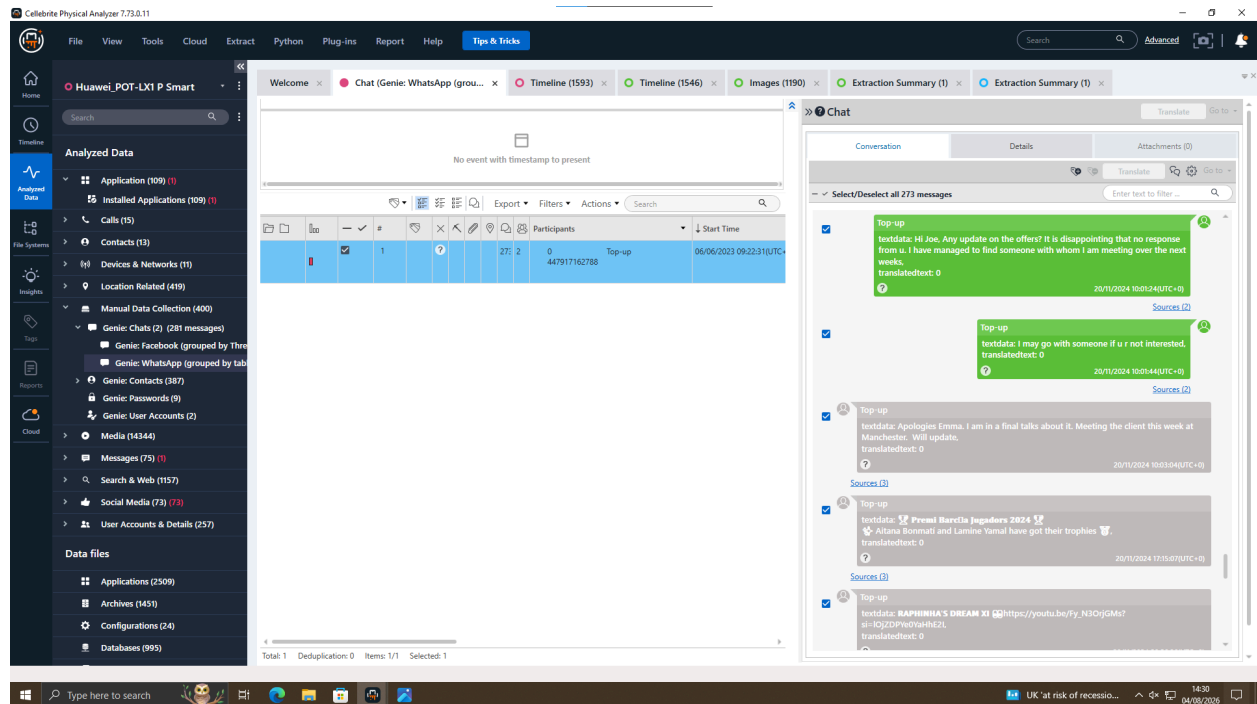


Figure. 3.5: Joe's Communication on Travelling to Manchester

From the analysis of the communication, it can be seen that Joe was traveling to Manchester to visit some clients. This gives a particular movement activity and brings Manchester into the reconstructed timeline.

This communication will be particularly useful when put together with the travel ticket to Manchester given later in the evidence.

3.5. Manchester Travel Ticket

The Manchester trip is facilitated through a travel object that is different from the rest.

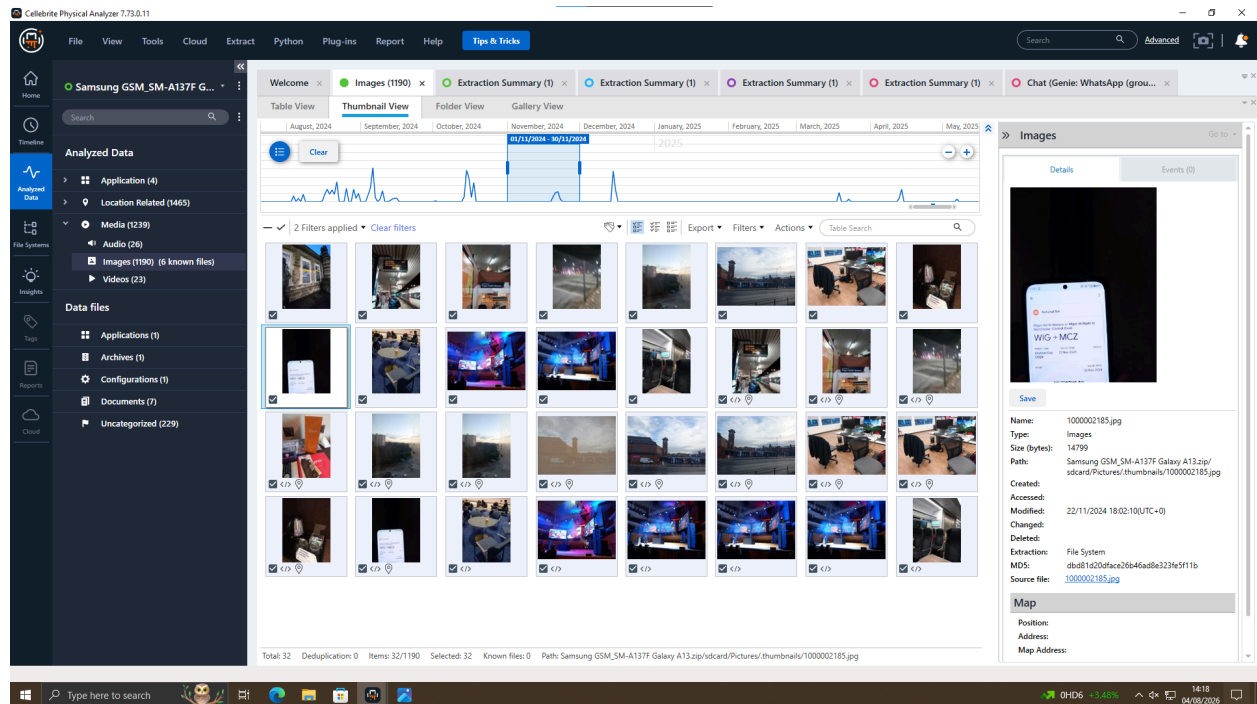


Figure 3.6: Joe's Manchester Travel Ticket

If the dates and other relevant details match, then the travel document becomes evidence for the travel movement recorded in the communication.

This shows the distinction between an evidence object and evidence correlation. Image 5 is the evidence of Joe's communication while Image 6 is a different travel object. The significance of their relationship arises during the examination.

3.6. Location of the Hotel

Another piece of evidence included in this analysis is the location information of Joe's phone.

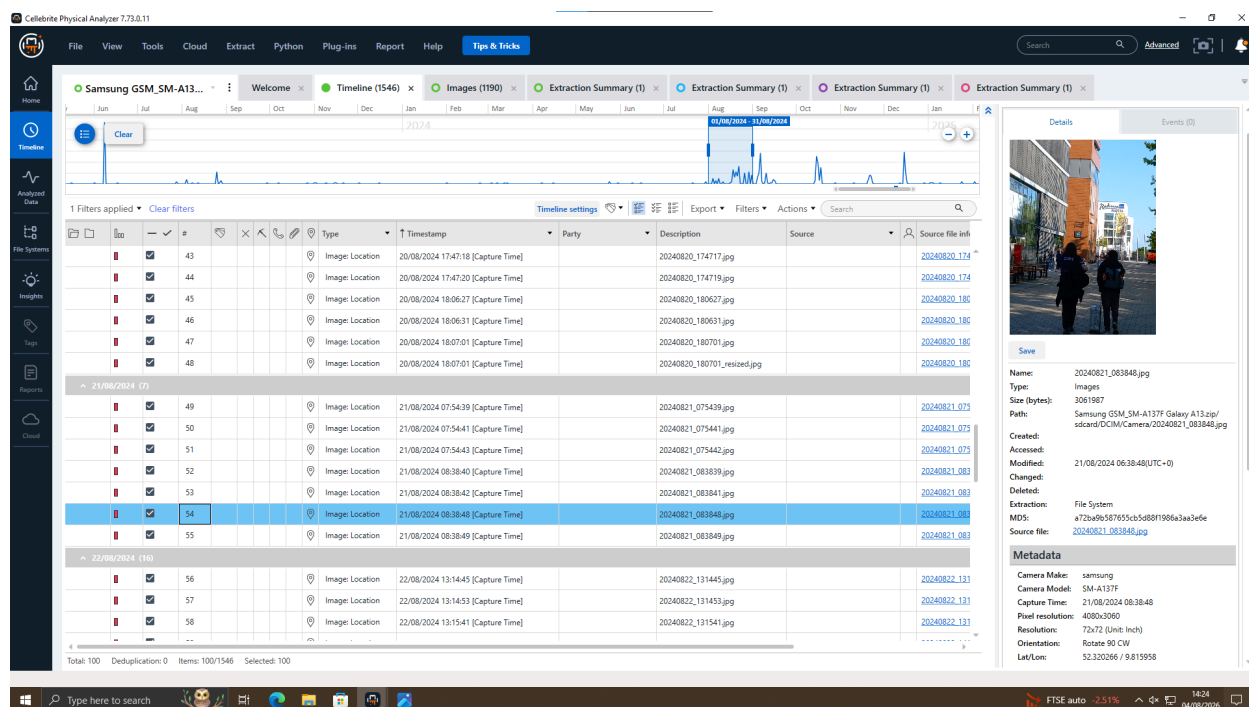


Figure 3.7: Joe's Phone Location at the Hotel

Evidence of location shows that the hotel is the relevant physical location. This can be correlated with other evidence about the meetings and communication.

The geographical aspect of location evidence gives more context to the location of the device. However, communication information could give a reason for the location.

3.7. Glasgow Travel Document

The document collection also includes Joe's ticket for travel to Glasgow.

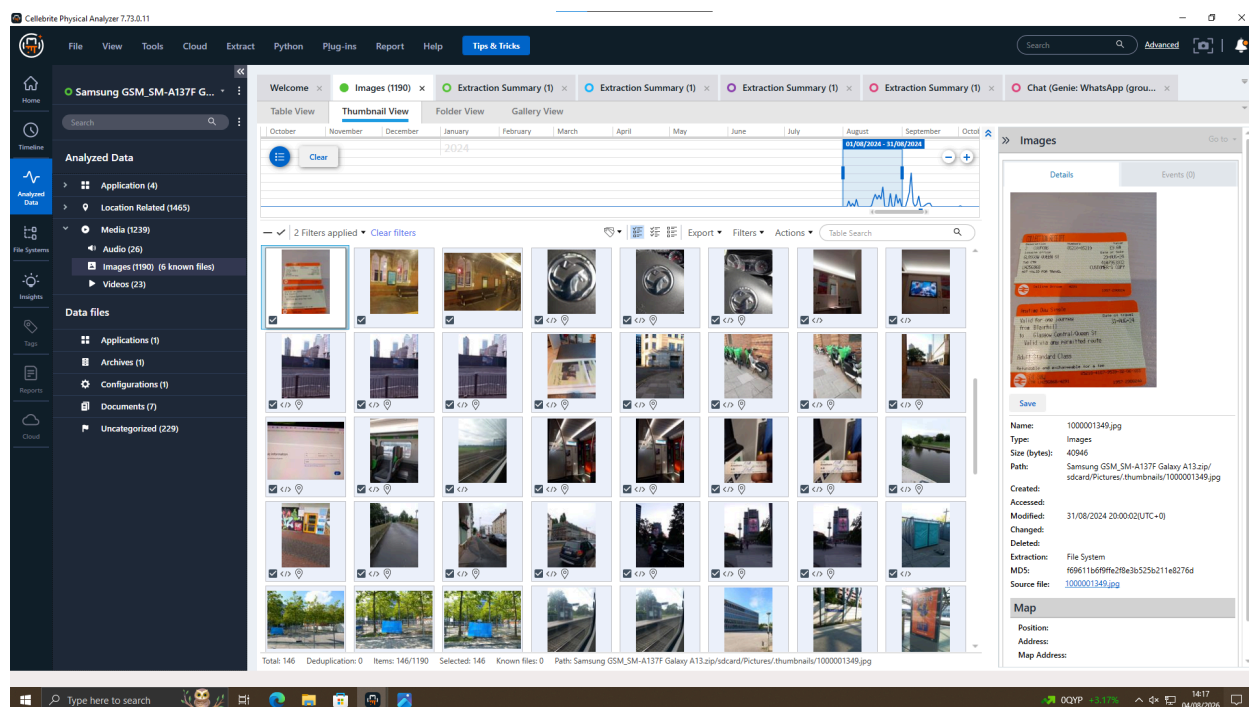


Figure 3.8: Joe's Ticket for Glasgow Travel

The Glasgow travel document is another artifact related to travel. The Glasgow travel document can be compared with the communication documents regarding the Glasgow meeting.

This document is useful in this case because it is an independent document related to travel.

3.8. Direct Contact Between Emma and Norman

Having established that indirect communication took place via Joe, this study now turns to examine direct communication between Emma and Norman.

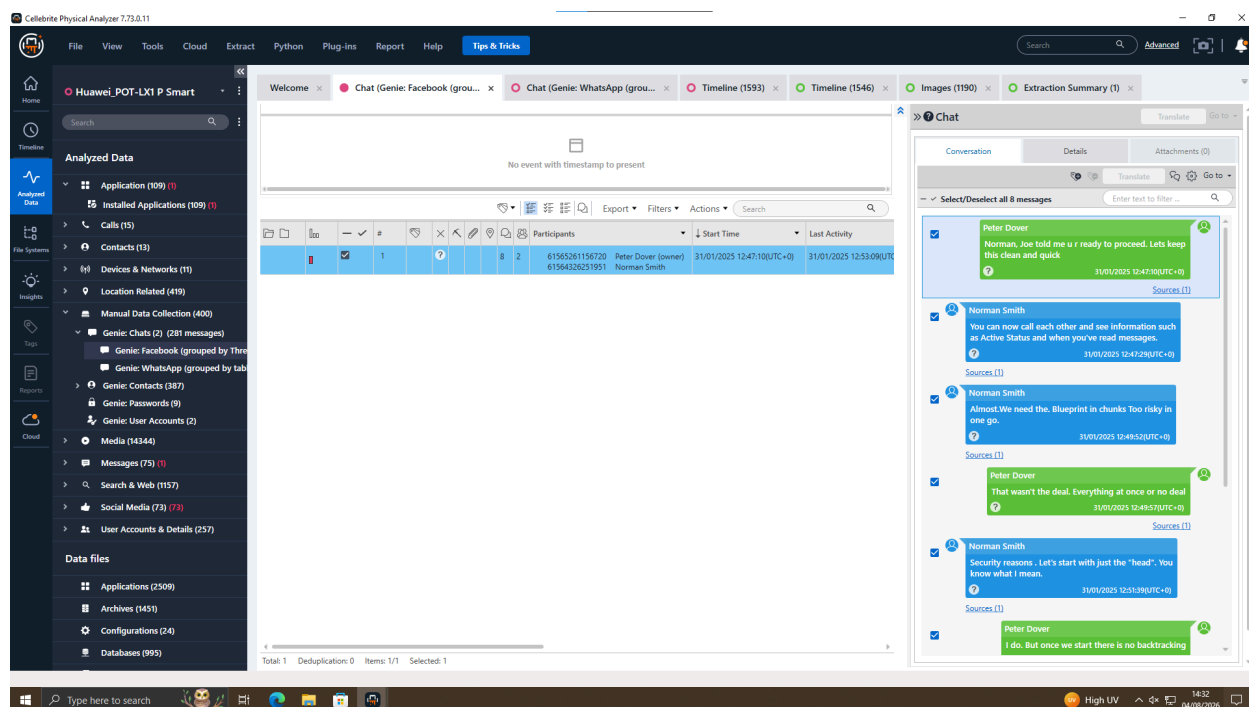


Figure 3.9: Direct Communication Between Emma and Norman on the Deal

The facts suggest that Emma directly communicated with Norman on the deal, and that both parties came to an agreement.

This fact is a very important aspect in the timeline since it establishes a direct link between Emma and Norman. The previous piece of information had to do with Emma's direct communication with Joe on the search for a buyer.

This communication can thus be analyzed along with the previous information.

3.9. Closure of the Agreement

The following is the evidence showing that the agreement reached its conclusion.

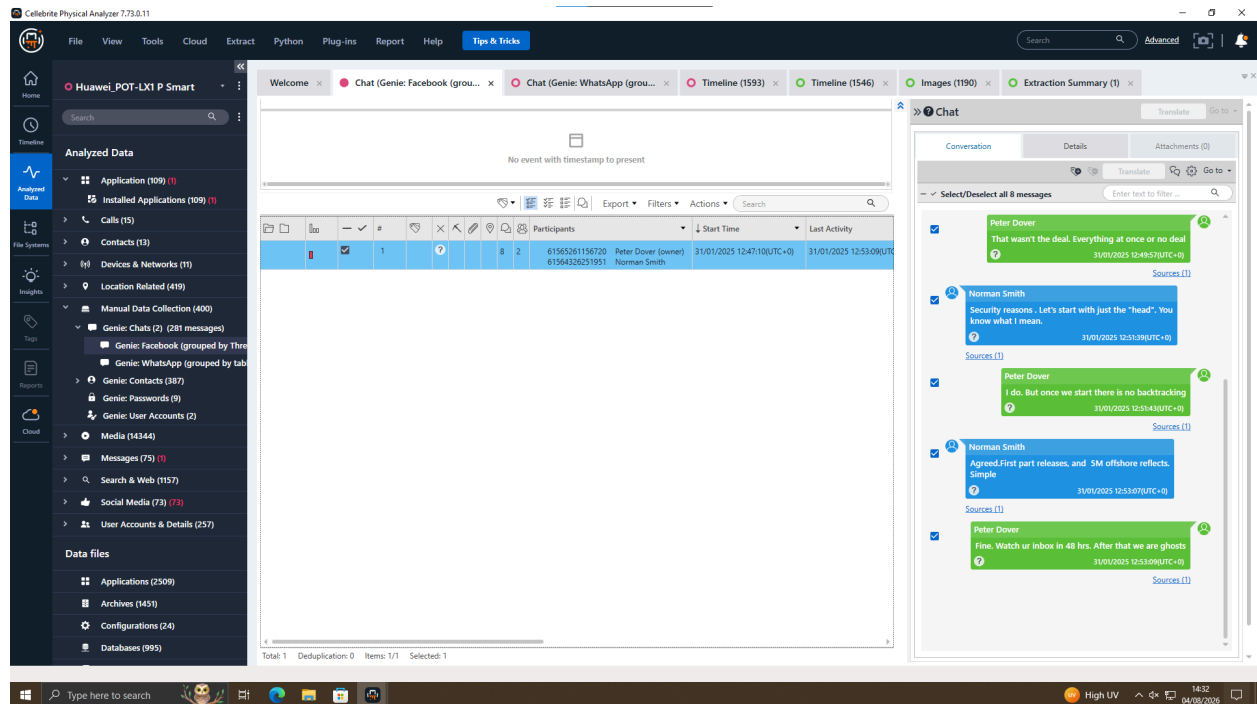


Fig. 3.10: Direct Communication Evidence of Emma and Norman Closing the Agreement

The evidence shows that Emma and Norman concluded the agreement. This marks a subsequent stage in the chain.

The examiner will be able to place this event in relation to the earlier direct communication event. Together, Image 11 and 12 show progression from the discussion about the agreement to its closure.

The times need to be noted properly so that the two events can be appropriately positioned in the final chronology.

3.10. Location of Norman's Mobile Phone

The last piece of evidence refers to the location of Norman's mobile phone.

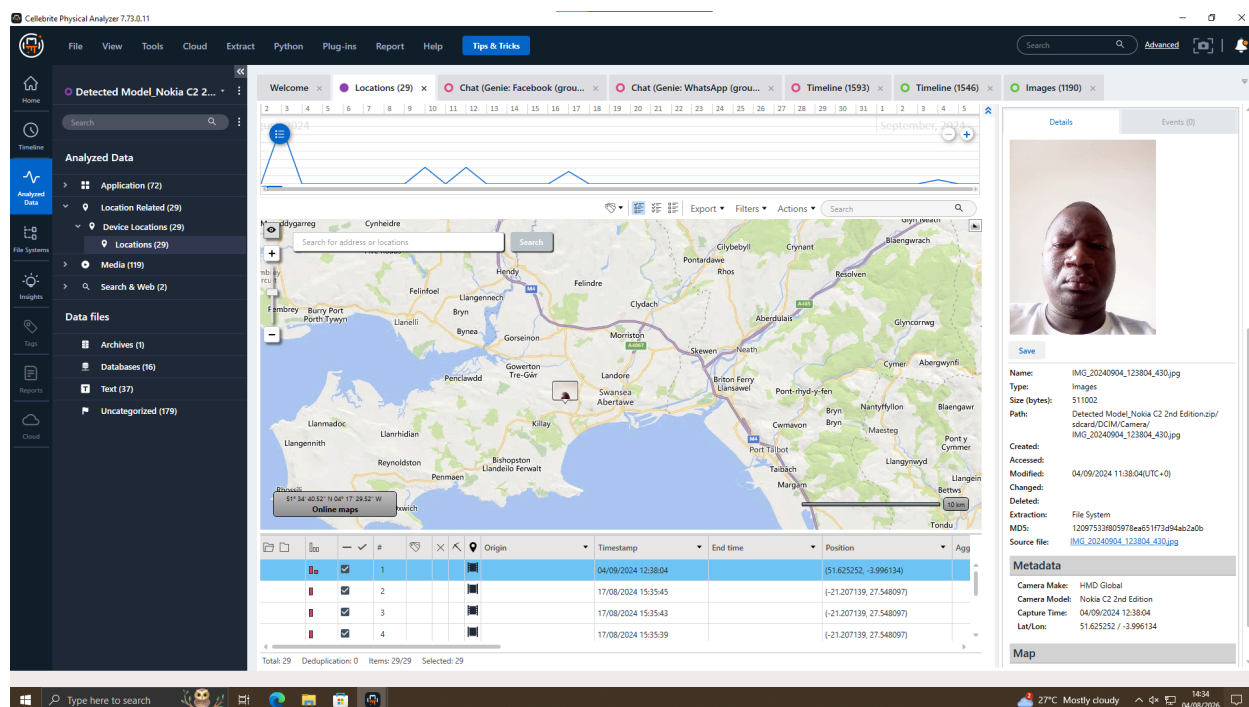


Figure 3.11: Norman's Phone Location at the Time of the Meeting

Location data helps to add the geographical dimension to the investigation. This data can be compared with the communication between Emma and Norman and with evidence of the conclusion of the transaction.

This data will become much more helpful when used together with other evidence. The investigator needs to decide whether the location matches the situation of the communication.

3.11. Timeline Reconstruction

Date	Suspect	Activity / Events
21/08/2024	Emma and Joe	Emma contacted Joe to find a buyer.

21/08/2024	Joe and Emma	Joe told Emma that she was at the hotel. This communication provided the evidence linking the persons to the hotel location.
20/11/2024	Joe	Joe communicated that he would be travelling to Manchester for meetings with the clients.
31/01/2025	Emma and Norman	Emma contacted Norman directly regarding the deal and they made an agreement. Emma and Norman closed the deal.
31/01/2025	Emma and Norman	Emma and Norman closed the deal.
31/08/2024	Joe	Joe's Glasgow travel ticket was confirmed.
22/11/2024	Joe	Joe's Manchester travel ticket was confirmed.
21/08/2024	Joe	Joe's phone location was logged while at the hotel.
04/09/2024	Norman	Norman's phone location was logged at the meeting place.

3.12. Conclusion

There is enough evidence available to make out the chain starting from the forensic identification of three mobile phones and moving on to the evidence related to communication, travel, and locations.

Emma's communication with Joe about a buyer can be considered the

first link in the chain with further links in the form of Joe's activities in Manchester and travel evidence.

The ticket for Glasgow represents another form of movement evidence whereas the location of Joe in his hotel represents the geographical evidence. Further, the communication between Emma and Norman marks the progress in the process and closure of the deal.

The geographical location of Norman's phone represents another piece of geographical evidence which can be compared with other evidence relating to the communication and deal.