



Student Name: Zannatul Mawya Priya

Student ID: 2527766

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

Future Directions, Challenges and Career Opportunities in Digital Forensics

1. Introduction
2. Current Situation of the Discipline
3. Forensics and Cybersecurity
4. Emerging Trends
5. Major Problems
6. National and International Labor Market
7. Recommendations for Future Professionals
8. Conclusion
- 9 References

Task 2

Personal Mobile Phone Acquisition Using Cellebrite UFED

- 1 Introduction
2. Choosing the Extraction Technique
3. Choosing Evidence Categories
4. Mobile Phone Identification
5. Outcome of the Extraction Process
6. General Evaluation

Mobile Phone Forensic Examination and Digital Activities Reconstruction

- 1 Introduction
2. The First Set of Forensic Evidence
3. Joe as the Intermediary
4. Direct Communication Between Emma and Norman
5. Completion of the Transaction
6. Communication Related to Glasgow Meeting
7. Evidence of Glasgow Trip
8. Travel to Manchester

9. Norman's Phone Location
10. Correlation of Evidence on Communication, Travel and Location
11. Timeline Reconstruction
12. Reconstructing the Full Sequence
13. Conclusion

Task 1

Future Directions, Challenges and Career Opportunities in Digital Forensics

1. Introduction

There is considerable transformation in the area of digital forensics. Forensic investigations in the past were centered around computers and other physical mediums of storage. The modern investigations have started to cover more aspects like smartphones, cloud storage, IoT, encrypted communications, network-based and AI-generated information. Though the increase in scope has greatly increased the relevance of the digital evidence, there is considerable complexity involved in doing so.

Digital forensics is thus a discipline which is still evolving and has to keep up to date with the changes.

2. Current Situation of the Discipline

Forensic investigations now have a lot of phases which include Identification, Preservation, Acquisition, Examination, Analysis, and Reporting. Modern tools have automated many phases of forensic investigation.

Tools like Magnet AXIOM, FTK, and EnCase give you integrated solutions for examination of computer and mobile evidence. Autopsy gives you the open-source solution for education and research. Specialized mobile tools like Cellebrite UFED and XRY.

With greater diversity of evidence, it becomes impossible to use just one technique to collect evidence. Different tools can be used for different sources of evidence. For instance, Wireshark is used to collect network data, while endpoint tools are used to collect disk evidence.

Research in the area of IoT forensic frameworks illustrates the need for such an approach to collecting evidence [1].

3. Forensics and Cybersecurity

There has been a close relationship between digital forensics and cybersecurity since cyber incidents involve not only response but also investigation.

Such security systems as cybersecurity can detect malware, authentication attempts, data transfers and abnormal network connections. Such alerts serve as points of departure for the forensic investigation.

The task of the forensic investigator is to determine what happened and provide evidence to prove it. Thus, forensics play a crucial role in such cyberattacks as ransomware attacks, insider attacks, data breach, account compromise and advanced persistent threats.

Forensic readiness must therefore be incorporated into the cybersecurity plan for an organization as it matures. According to research carried out by Friedl and Pernul, forensic readiness in IoT environments relies on technology, standardization, management, legal issues, and human factors [2].

4. Emerging Trends

One of the most significant impacts that artificial intelligence will have on digital forensics is expected to be seen in the future. With the help of AI, analysis can be automated, and investigators can prioritize evidence. According to Dunsin et al., AI has applications in data recovery, pattern recognition, and incident response [3].

Nevertheless, AI is not supposed to replace human investigators by default. According to Vasilaras et al., forensic AI requires robustness, transparency, and interpretability [4].

Large language models provide yet another innovation. As per the research conducted by Wickramasekara et al., LLMs can help during various stages of the digital forensics process [5]. Recent research from law enforcement agencies found that several LLMs are able to help analyze mobile messaging evidence and provide contextual interpretations but also require analysis for hallucinations [6].

IoT and edge forensics are gaining significance as well. The IoT forensics research area points out the problem of accessing distributed devices and collecting ephemeral evidence [7]. Edge-based collection could make it possible to detect evidence close to its origin.

Lastly, forensic preparedness is gaining importance. Rather than waiting for an incident to happen, one can create a system that will provide investigators with logs, timestamps, and other useful information.

5. Major Problems

The first problem to be discussed here is a fast technological lifecycle. Operating systems and applications change all the time, which means

that forensic tools should be upgraded constantly. Therefore, digital forensics investigators should be aware of the latest technologies.

The second problem is the volume of the evidence. In the DFPulse practitioner survey (122 participants), it is pointed out that there is a need to bring academic research and operational forensics closer together [8]. It is critical since an interesting technological research technique might not resolve any practical issues.

There are also issues of a human and legal nature. Research conducted with participation of forensic investigators in England and Wales pointed at problems related to the relations with investigating officers and legal professionals, workload and introduction of automation and AI.

The reliability of evidence is yet another important problem. When forensic instruments deliver inconsistent results, investigators have to be ready to justify this and prove that their findings can be trusted.

6. National and International Labor Market

The labor market of digital forensics is directly associated with the broader cybersecurity market. Employers in the UK work in policing, government, financial services, consulting, technology and corporate security sectors.

According to the 2025 UK Government's research, there are approximately 143,000 people employed in cybersecurity-related jobs and there is a gap of about 3,800 professionals in the labor market. Moreover, 22% of cyber-sector companies experiencing skills shortages in technical areas noted the shortage of digital forensics specialists.

However, entry-level applicants find it increasingly competitive in the market. The same report showed that only 17% of core cybersecurity postings in 2024 required job applicants to have less than a year of experience, while 63% required two to six years of experience.

It implies that having a degree is not enough. They should showcase their skills via laboratories, projects, internships, competitions, and portfolio. Globally, career options are digital forensics examiner, cyber investigator, DFIR analyst, incident responder, forensic consultant, and cybercrime investigator.

7. Recommendations for Future Professionals

The best career approach is to remain technologically broad but forensically specialised. Students must acquire skills in:

Windows and Linux administration.

Networking and TCP/IP.

Forensic acquisition and analysis.

Wireshark and network forensics.

KAPE and endpoint artefacts analysis.

Memory forensics.

Mobile and cloud forensics.

Python and automation.

SIEM and incident response.

Evidence documentation and report writing.

These skills enable graduates to switch from forensic investigations to cybersecurity/DFIR positions.

8. Conclusion

In the coming years, the field of digital forensics will be impacted by artificial intelligence, cloud computing, Internet of Things (IoT), automation and increasing complexity of digital evidence. Such changes will help to increase investigation efficiency but will lead to challenges in terms of reliability, privacy protection, preserving evidence and professional competencies. Consequently, the profession is not going to disappear due to automation but will change and focus on evidence evaluation and interpretation.

As for graduates, their best chance is to become specialists in cybersecurity and digital forensics.

9. References

1. DFPulse 2024 Digital Forensic Practitioner Survey
<https://scholar.google.com/scholar?q=%22DFPulse%3A+The+2024+digital+forensic+practitioner+survey%22>
2. “What you say in the lab, stays in the lab” — UK digital-forensic challenges
<https://scholar.google.com/scholar?q=%22What+you+say+in+the+lab%2C+stays+in+the+lab%22>
3. “The invisible evidence: Digital forensics as key to solving crimes in the digital age,” *Forensic Science International*, 2024.
<https://scholar.google.com/scholar?q=%22The+invisible+e>

[vidence%3A+Digital+forensics+as+key+to+solving+crimes+in+the+digital+age%22](#)

4. IoT forensic readiness research

[https://scholar.google.com/scholar?q=IoT+forensic+readiness+digital+forensics](#)

5. Digital forensic practitioner challenges

[https://scholar.google.com/scholar?q=digital+forensic+practitioner+challenges](#)

6. Digital forensic tool validation

[https://scholar.google.com/scholar?q=digital+forensic+tool+validation](#)

7. Digital evidence admissibility

[https://scholar.google.com/scholar?q=digital+evidence+admissibility+digital+forensics](#)

8. Anti-forensics and digital investigations

[https://scholar.google.com/scholar?q=anti-forensics+digital+forensics+investigation](#)

Task 2

Personal Mobile Phone Acquisition Using Cellebrite UFED

1. Introduction

The acquisition of a mobile phone is very crucial in digital forensics since smartphones have the ability to hold varied forms of information which might be useful at some point in the investigation process. Before analyzing any information, the first step should be to identify the kind of device that is being investigated along with the kind of acquisition process and evidence categories.

In this practical session, Cellebrite UFED was applied in investigating a mobile phone and the kind of information that could be retrieved. The screenshots provided below depict various stages of this investigation such as the choice of the extraction method, choice of evidence categories, identification of the device and the actual result of the extraction process.

2. Choosing the Extraction Technique

Figure 2 shows the "Select Extraction Type" window in Cellebrite UFED. The phone seen at the top of the picture is called an OPPO CPH2729, 5G, and it is connected via USB cable or original cable. There are a few ways to acquire data from the phone, such as Advanced Logical, File System, Physical (Rooted), Camera, Screenshot and Chat Capture.

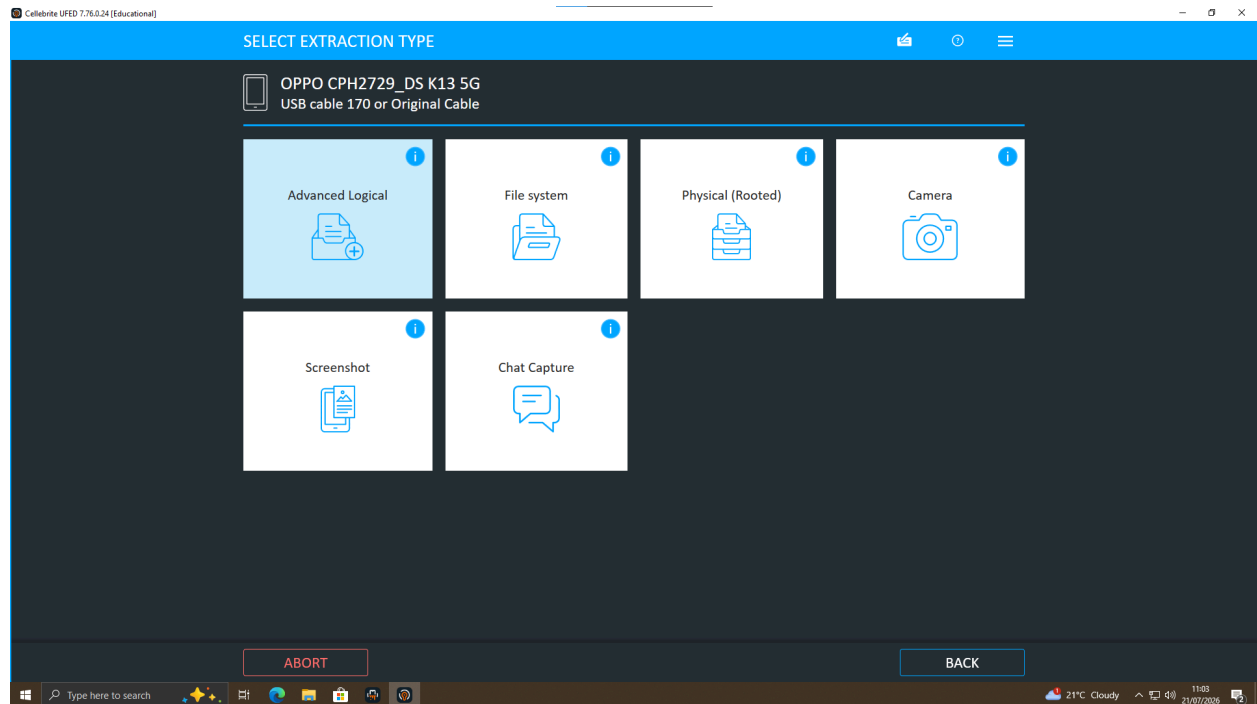


Figure 1: Data extraction techniques available for the connected mobile device in Cellebrite UFED.

Availability of a few ways of extraction means that data acquisition from mobile devices is not performed with only one technique. It depends on the device itself and the information needed by the examiner. For instance, advanced logical extraction will help to extract accessible information while other ways of data extraction will be used. It is possible to notice that one of the available ways (physical) is described as rooted.

It means that some data acquisition ways depend on the technical status of the device.

3. Choosing Evidence Categories

This phase includes choosing which type of evidence to gather. The Cellebrite software offers a Select Content Type screen where the selection can be done.

The following evidence categories can be seen: Call Logs, Locations, Advertising ID, Contacts, SMS, MMS, Calendar, Pictures, Audio/Music, Videos, Ringtones, Documents, Archives and Files. Different sources, such as device or SIM, are also shown in the screen.

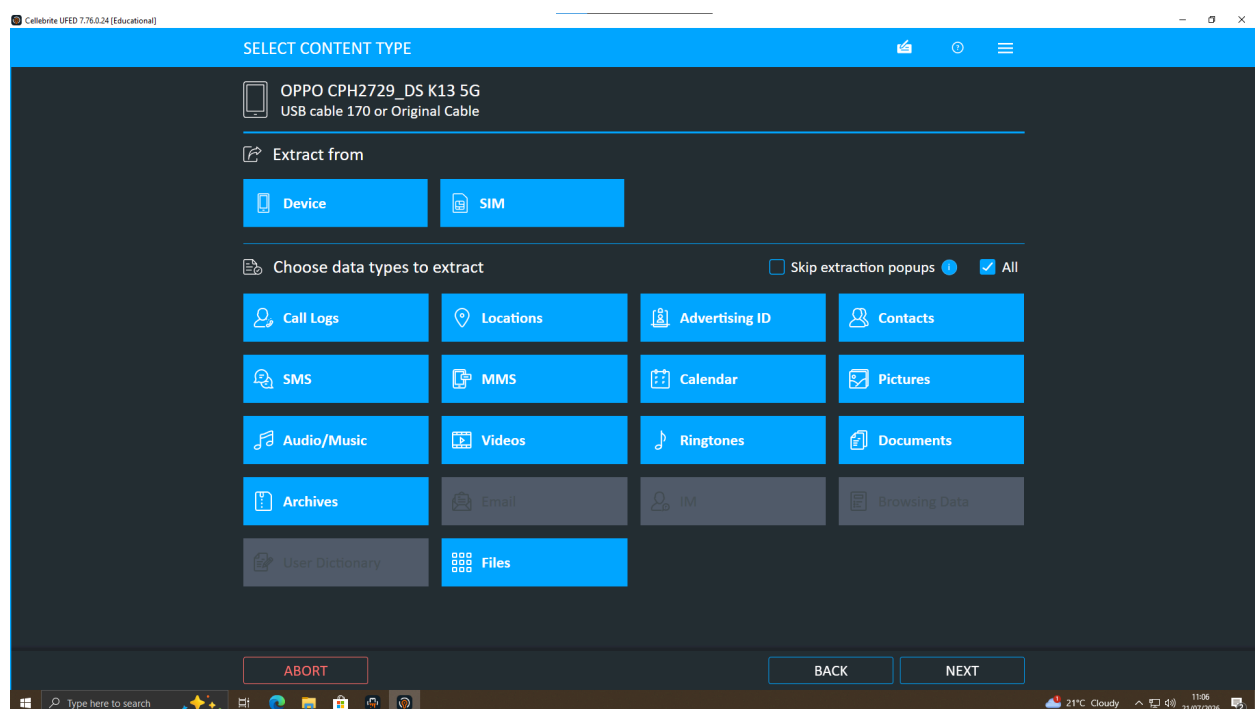


Figure 3: Available evidence categories for acquisition.

This step is important since the smartphone carries various types of digital information. For example, call logs and contacts could carry information related to communication, while images and videos could carry visual evidence. Documents and files could also carry information useful for the investigation.

Consequently, the investigator can set up the acquisition according to the evidence requirements. Choosing the content prior to starting the

process would help determine the type of information that Cellebrite was supposed to acquire.

4. Mobile Phone Identification

A new screenshot gives further information about the mobile phone. According to Cellebrite, the mobile phone under analysis is a Samsung GSM SM-G998B Galaxy S21 Ultra 5G. Additionally, it is worth mentioning that the operating system is Android 13.

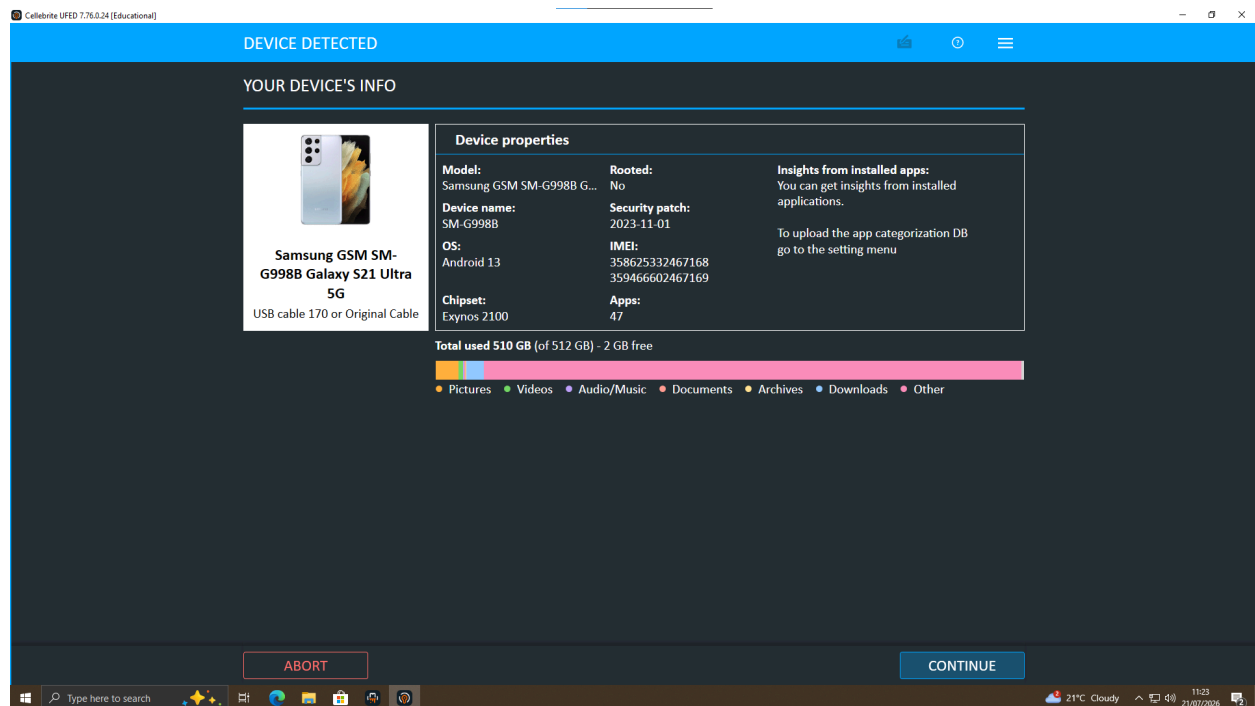


Figure 4: Information about the device provided by Cellebrite UFED for the Samsung Galaxy S21 Ultra 5G.

The device identification step is especially important for the examiner since he/she should understand the exact nature of the device he/she is going to analyze. The model of the device, its operating system and other technical aspects can influence the extraction process.

Additionally, the screenshot provides an insight into the storage of the device. There are roughly 510 GB on the storage partitioned into such categories as pictures, videos, audio/music, documents, archives, downloads and others. Such information helps the examiner to understand how much information is contained in the device in general before he/she attempts to extract it.

5. Outcome of the Extraction Process

The extraction results provide the most significant indication of the extraction outcome. According to Cellebrite, there are several categories of files that were skipped, unsuccessful and not supported.

Contacts, SMS, MMS, Calendar – skipped. Pictures, Audio/Music, Videos, Ringtones, Documents, Archives, Call Logs, Locations, Advertising ID, Files – unsuccessful. E-mail, Instant Messaging, Browsing Data, User Dictionary – not supported.

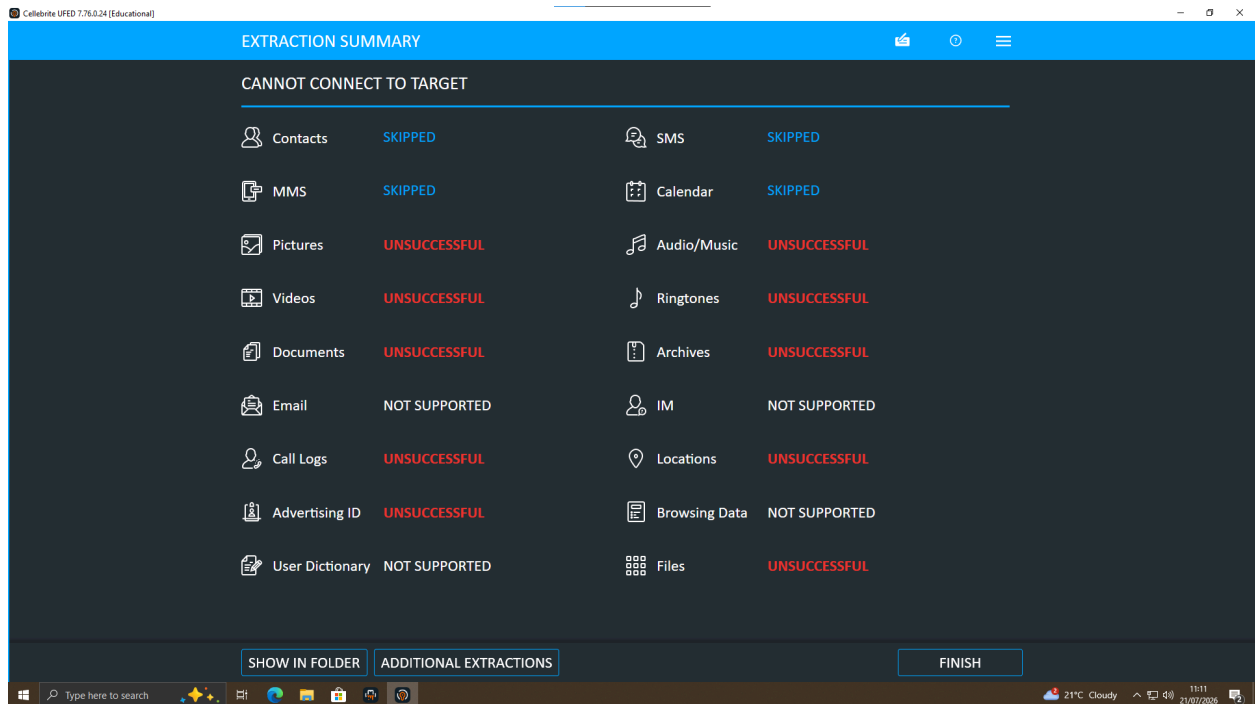


Figure 5: The extraction report summarizing skipped, failed, and unextractable evidence categories.

This finding is significant since it indicates that forensic acquisition is not always successful in obtaining evidence. Even if the examiner had picked a number of categories for acquisition, it may still be difficult for the extraction application to extract them effectively due to technical difficulties like device security, restrictions in the operating system, connection issues, or even limitations of the acquisition method.

Therefore, the examiner should never assume that there was no relevant evidence on the device just because of failed extraction. The correct way to describe the finding is that the acquisition process could not successfully extract the evidence categories chosen.

6. General Evaluation

Some crucial elements of mobile phone forensics have been shown through the practical exercise. Firstly, the examiner has to select the right method of acquisition according to the device. Secondly, the examiner should know various sources of evidence such as the mobile phone, SIM card, and memory card. Thirdly, the results of the extraction process need to be analyzed in order to know what has been extracted.

A failed extraction can prove to be very informative in terms of forensic learning. It will provide the information that forensic tools cannot provide access to any type of information in any mobile phone. In case of failed extraction, the examiner needs to think about some other method of acquisition that has been supported by the forensic tool or the configuration of the mobile phone that has been restricting the access.

The screenshots also tell about the necessity of distinction between skipped, unsuccessful and unsupported categories in the forensic reports.

Mobile Phone Forensic Examination and Digital Activities Reconstruction

1. Introduction

Forensic examination of mobile phones will allow the investigator to get the necessary information that may help in reconstructing a chain of events. Communication via digital channels will help establish connections between different people, while documentation of travel will help reconstruct their movements and meetings.

The evidence examined here are related to three mobile phones and many other digital artifacts. Initial evidence includes hash information from Huawei, Nokia, and Samsung phones. Further evidence are related to communications of Emma and Joe, where Joe is acting as an intermediary, and direct communications between Emma and Norman.

Unlike an investigation which relies on only one source, this piece of evidence has several types which can be combined to make it more complete. The communication gives details about the interaction, travel evidence gives details about movements, while location evidence is geographical in nature.

This analysis is therefore going to look at the recreation of this activity using the provided evidence.

2. The First Set of Forensic Evidence

Moving on to the communications before analyzing them, the first set of evidence is that of identifying three phones through their hashes.

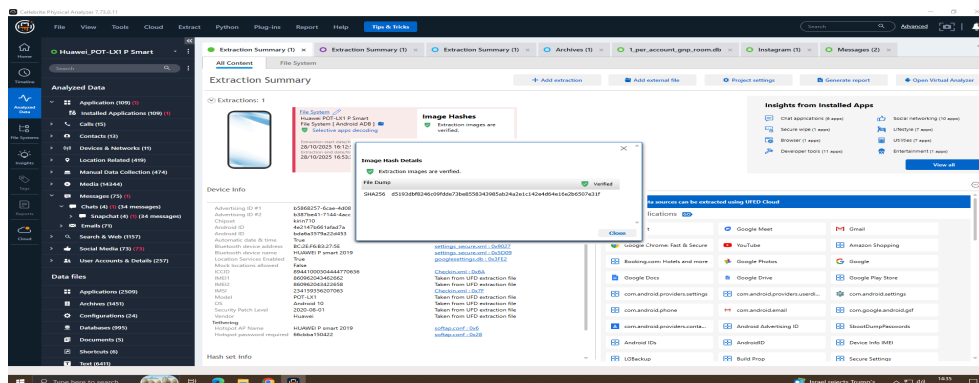


Figure 1: Evidence Hashes of Huawei Phone

The evidence hash of the Huawei phone constitutes one of the evidence records.

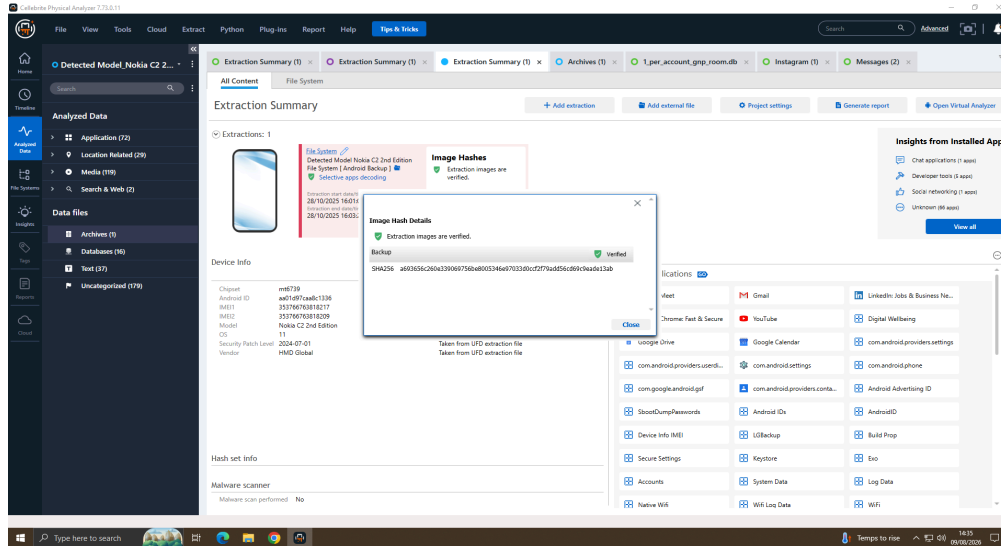


Figure 2: Evidence Hashes of Nokia Phone

The evidence hash of the Nokia phone constitutes the second evidence record.

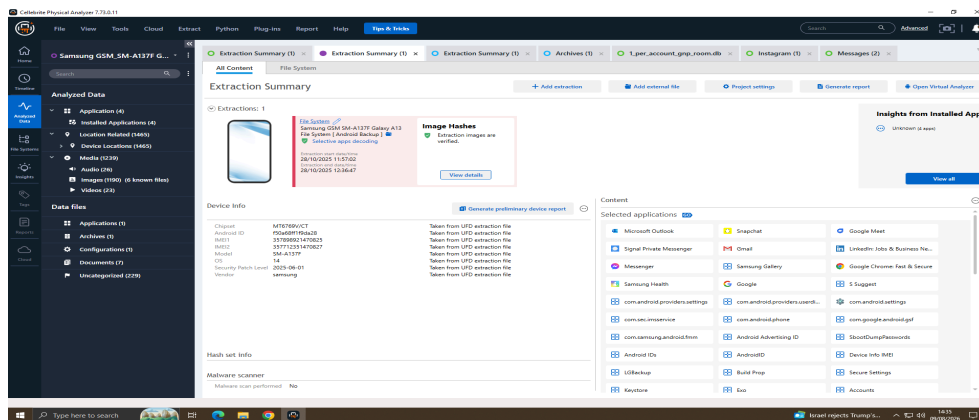


Figure 3: Evidence Hashes of Samsung Phone

The evidence hash of the Samsung phone is the third evidence record. It is significant to separate the records by device because of the different individuals and devices in the latter evidence.

These constitute the first set of evidence records.

3. Joe as the Intermediary

Identification of Joe's role in the activity is another vital piece of evidence in this case.

It turns out that Joe served as the intermediary in the activity according to the evidence provided. It will become clear when the communication between Emma and Joe is analyzed.

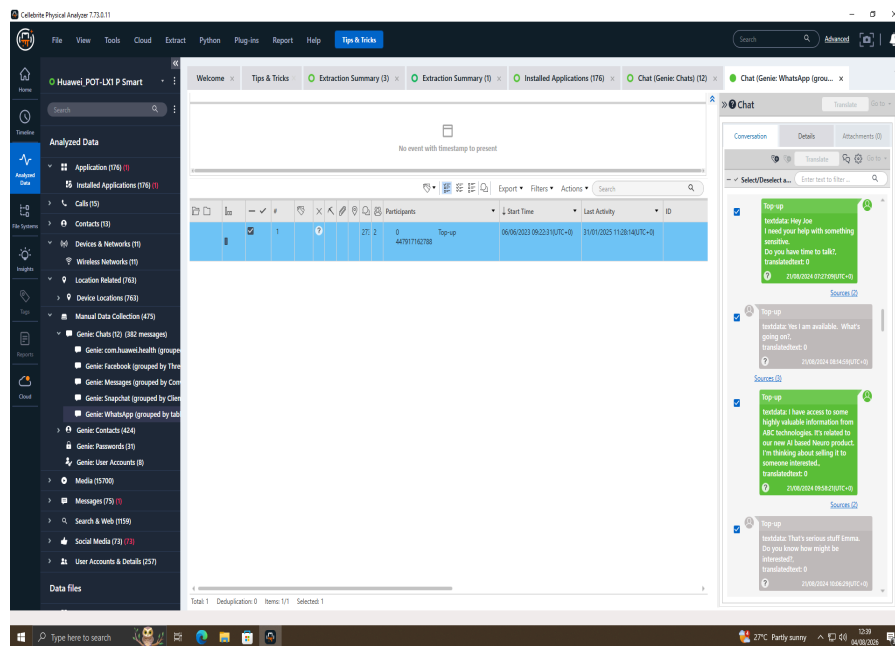


Figure 4: Communication Between Emma and Joe on the Search for a Buyer

This communication proves that Emma was talking to Joe about the search for a buyer, which constitutes the communication between Emma and Joe and serves as the first stage of the activity.

It will be possible to recognize Joe's intermediary role in view of the following evidence related to Norman. Instead of analyzing Joe's role in the particular communication, the examiner can analyze the latter communication of Emma and Norman.

4. Direct Communication Between Emma and Norman

Further evidence reveals that Emma communicated with Norman directly.

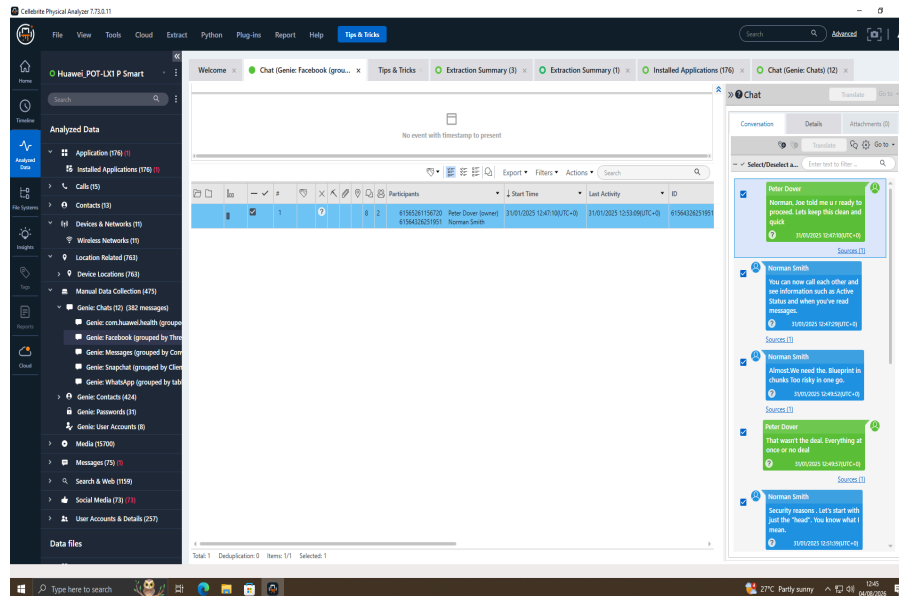


Figure 5: Direct Communication Between Emma and Norman Regarding the Deal

The evidence suggests that Emma and Norman made direct communication on the deal and that both had come to an agreement.

This clearly marks a big difference from the earlier communication as the intermediation through Joe will eventually lead to direct communication between Emma and Norman.

This process can thus be represented by:

Emma → Joe → potential buyer → Emma → Norman

There is no necessity for the evidence to show just one single conversation. Instead, the evidence about the communications can be put together in chronological order.

5. Completion of the Transaction

The next piece of evidence shows the completion of the transaction.

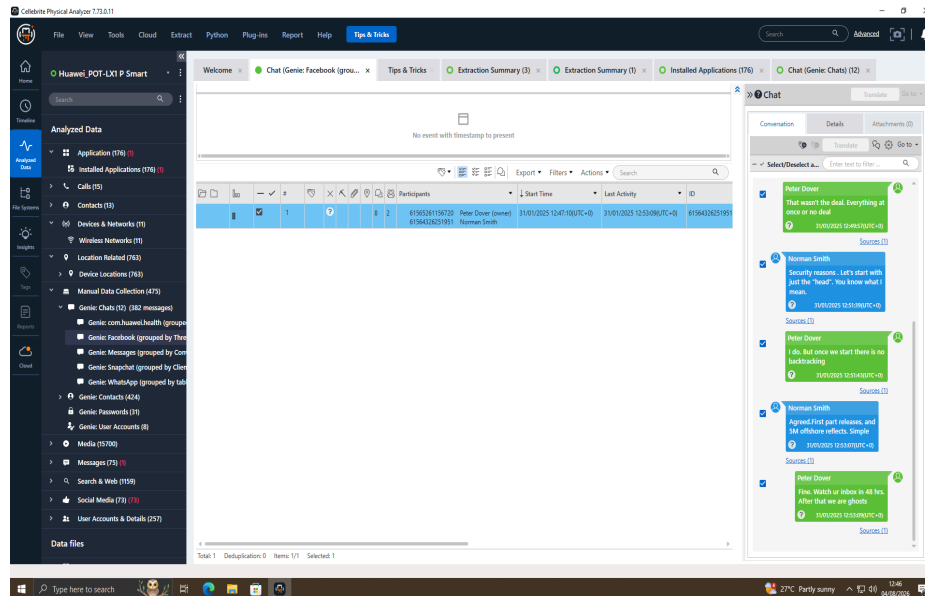


Figure 6: Communication between Emma and Norman showing the Completion of the Transaction

Evidence is present showing that Emma and Norman successfully completed the transaction.

It comes after the direct communication and represents another point in the reconstructed sequence. It would be wise to retain the surrounding communication since it may play an important role in determining the meaning of individual communications.

These two pieces of evidence show the progression from direct conversation to the completion of the transaction.

6. Communication Related to Glasgow Meeting

The report also includes communication related to Emma's Glasgow meeting.

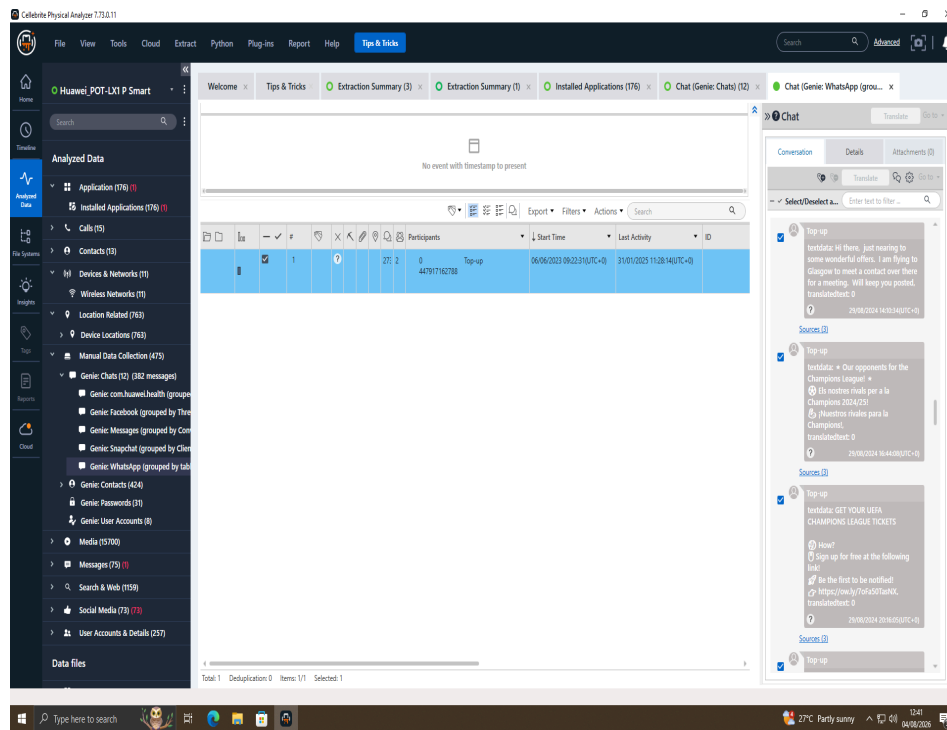


Figure 7: Communication Regarding Emma's Glasgow Client Meeting

It is clear from the findings that Joe informed Emma that she would be traveling to Glasgow for a meeting with her clients.

In this case, we have added a particular incident of traveling to the reconstructed timeline of events. It is then possible to compare it with the Glasgow travel ticket.

Travel communication and travel tickets are two types of evidence.

7. Evidence of Glasgow Trip

The Glasgow trip is evidenced through Joe's travel ticket.

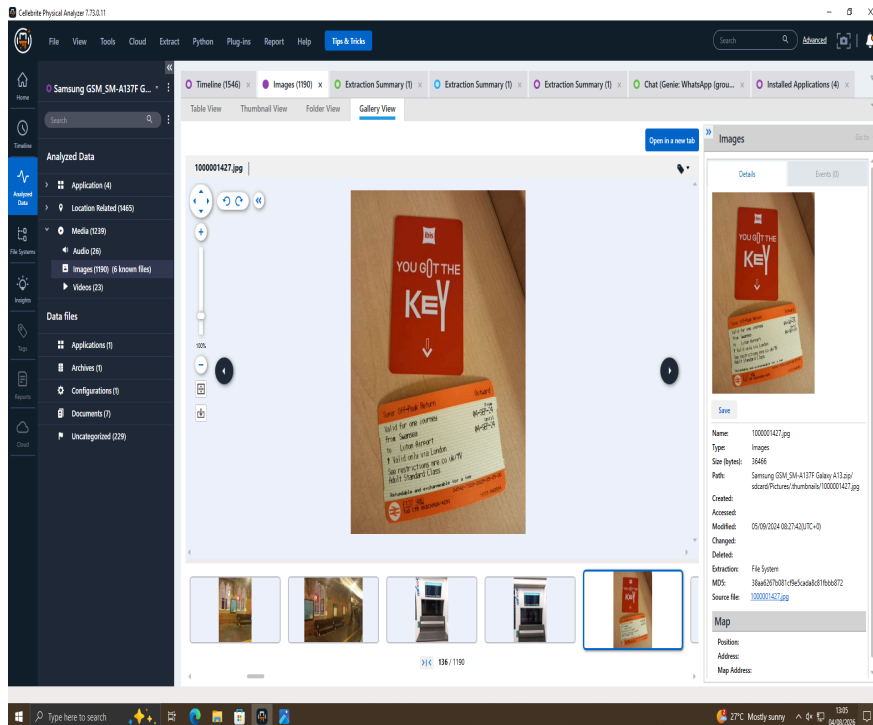


Figure 8: Glasgow Travel Ticket of Joe

The ticket can be compared to the communication as provided in figure 7. The examiner can analyze the corresponding date, time, and destination of the travel record to ascertain its consistency with the communication.

This is vital to the construction of timelines since both the evidence can be placed side by side.

8. Travel to Manchester

The documents also provide information about Joe's movements to Manchester.

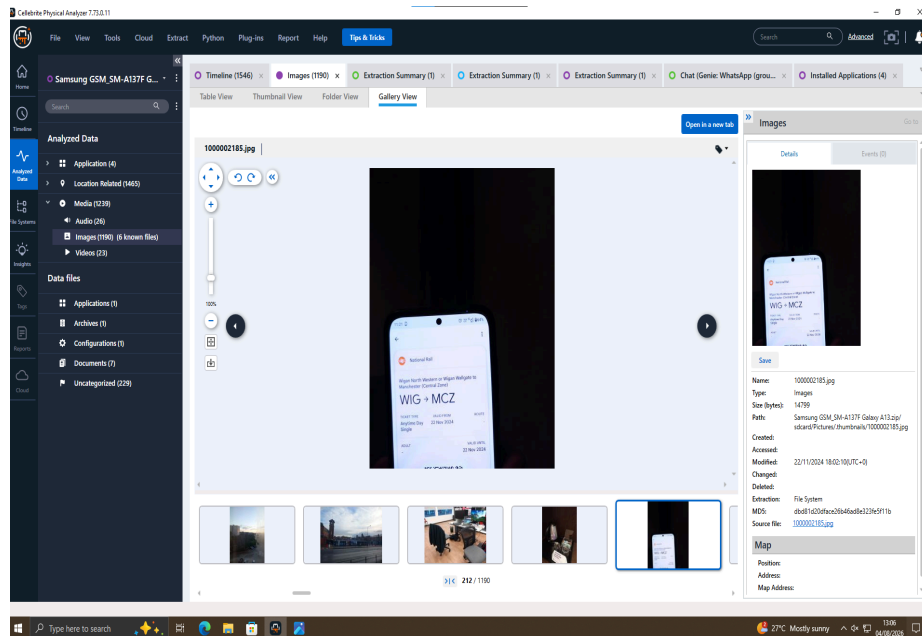


Figure 9: Joe's Manchester Travel Ticket

This ticket offers evidence relating to Joe's travels. This document can be placed on the timeline as a movement event.

It must be compared to the rest of the communication evidence in order to determine its position chronologically.

Since travel evidence is a different form of evidence from communication evidence, it can serve to corroborate movement events.

9. Norman's Phone Location

The last piece of evidence is Norman's phone location.

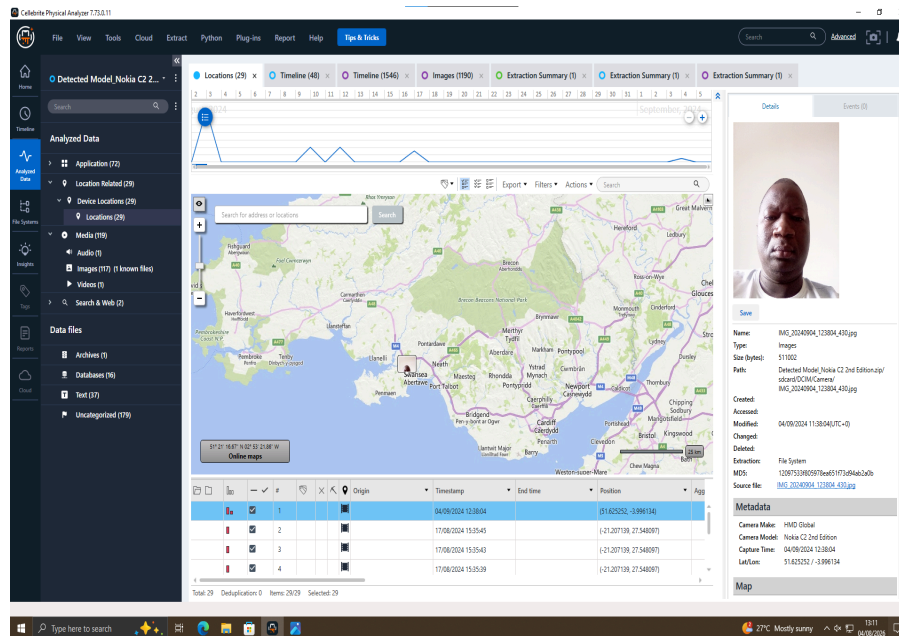


Figure 10: Norman's Phone Location During the Meeting Location

It shows the location of Norman's phone during the meeting location. This kind of evidence adds a geographic dimension that can be compared with the communication between Emma and Norman and the report about closing the deal.

It is especially valuable to have such evidence that can be linked to some event from another source. That way, the location timestamp can be compared with the timestamp of the corresponding communication.

10. Correlation of Evidence on Communication, Travel and Location

The evidence can be correlated using three main categories.

Communication

Figure 4 shows communication between Emma and Joe regarding the buyer. Then figure 5 shows direct communication between Emma and Norman regarding the deal followed by figure 6 which shows the closure of the deal.

Travel

Figure 7 shows communication about the Glasgow meeting of Emma while figure 8 shows the Glasgow ticket of Joe. figure 9 shows the Manchester ticket of Joe.

Location

Figure 10 shows the location of Norman's phone during the meeting.

The different categories can be correlated through their time stamp and description of the events. The correlation does not mean that each artifact will prove the whole incident but rather each artifact will be used to prove a certain aspect of the incident.

For instance, the Glasgow communication will prove the planning of the meeting whereas Glasgow ticket will provide travel evidence. Similarly, direct communication with Norman will prove the communication while Norman's location will provide geographical evidence of the meeting.

11. Timeline Reconstruction

Date	Suspect Involved	Activity
21/08/2024	Emma and Joe	Contact was made by Emma to Joe to get a buyer.

29/08/2024	Joe and Emma	A meeting in Glasgow for the clients by Emma was confirmed by Joe.
20/11/2024	Joe	Travel ticket to Manchester by Joe was determined.
31/01/2025	Emma and Norman	Emma contacted Norman directly about the deal and they sealed it.
31/01/2025	Emma and Norman	Emma and Norman concluded the deal formally.
31/08/2024	Joe	Joe's travel ticket to Glasgow by Joe was determined.
22/11/2024	Joe	Travel ticket of Joe to Manchester provides supplementary evidence to his travel to Manchester and it can be compared to the communication about his meeting in Manchester.
21/08/2024	Joe	The travel ticket of Joe for Manchester serves as supportive evidence for his travel to Manchester and this can be compared with the communication regarding his meeting in Manchester.
04/09/2024	Norman	The location of Norman's mobile phone mentioned the location of his device at the meeting place.

12. Reconstructing the Full Sequence

Looking at the full picture, the task can be logically sequenced.

First of all, there is the evidence in the form of the hashes on the three mobile devices. These hashes define the mobiles that are going to be investigated.

After that, there is the evidence about Emma and Joe. It becomes known that Emma talks to Joe to find the buyer, and Joe acts as an intermediary.

Then, it moves to the communication between Emma and Norman. Here, the evidence shows that the deal was discussed, and it became agreed upon. Afterward, the closing of the deal is mentioned.

Apart from that, there is also travel evidence, which includes the tickets to Glasgow and Manchester for Joe.

Finally, there is the location evidence in relation to the meeting place of Norman.

It can be seen from this sequence how the investigation can go from device evidence - communication - intermediary activity - direct communication - deal - travel - location.

13. Conclusion

The digital artifacts from the mobile devices reveal various separate sources which can be used to recreate the chronological order of events. The analysis starts with the hash of three phones, and continues with the communications between Emma and Joe regarding searching for a buyer.

The intermediary position of Joe is important in connecting the early communications with the further communications of Emma and

Norman directly. The next step is the direct communications between Emma and Norman, and the closure of the deal.

The communication from Glasgow and the travel ticket give information about the planned movement, and the travel ticket from Manchester is another travel artifact. In addition, the location of Norman's phone at the meeting gives the geographic information.

Therefore, the overall analysis proves that it is very important to combine different digital artifacts. Communications reveal interactions, travel tickets give the information about movements, and locations are the geographic information. When they are combined in chronological order and connected with each other, it gives the organized reconstruction of the activity reflected in the evidence.