



**Prifysgol Cymru**  
Y Drindod Dewi Sant  
**University of Wales**  
Trinity Saint David

## **MSc Cybersecurity and Digital Forensics**

### **Module: Digital Forensics Analysis**

**Module Code: ACCA7031**

### **Assessment Components 1 and 2 – Digital Forensics Research and Investigation Reports**

**Submission Deadline:** 17th August 2025, 14:00 (2PM)

**Lecturer:** Dr. Mohamed Ghanem

Title of Assessment: Research and Analysis of Digital Forensics, and Investigation of the Suspected Theft and Sale of Quantum Tech's Proprietary AI Chip Design Patent

Student Name: Md. Asaddoz Jaman

Student Number: 2526322

## Table of Contents

|                                                                      |    |
|----------------------------------------------------------------------|----|
| 1. Introduction.....                                                 | 2  |
| 2. Present Status of Digital Forensics and Its Tools.....            | 2  |
| 3. Intersection of Digital Forensics and Cybersecurity.....          | 3  |
| 4. Latest Developments in Digital Forensics.....                     | 3  |
| 5. Key Challenges.....                                               | 4  |
| 6. UK and International Employment Market for Forensic Analysts..... | 4  |
| 7. Conclusion.....                                                   | 5  |
| References.....                                                      | 5  |
| 1. Executive Summary.....                                            | 6  |
| 2. Case Background and Context.....                                  | 6  |
| 3. Evidence Inventory.....                                           | 7  |
| 4. Acquisition, Integrity and Continuity.....                        | 7  |
| 4.1 Acquisition Procedure.....                                       | 7  |
| 4.2 Hash Verification.....                                           | 10 |
| 5. Forensic Methodology.....                                         | 11 |
| 6. Findings and Evidence Analysis.....                               | 13 |
| 6.1 Emma's Initial Approach to Joe.....                              | 13 |
| 6.2 Joe's Search for a Buyer.....                                    | 13 |
| 6.3 Proposed Payment.....                                            | 15 |
| 6.4 Peter Dover Alias and Norman.....                                | 15 |
| 6.5 Norman's Nokia Location Evidence.....                            | 17 |
| 6.6 Joe's Samsung Evidence.....                                      | 18 |
| 7. Reconstructed Timeline.....                                       | 20 |
| 8. Suspect Profiling.....                                            | 20 |
| 9. Limitations of Evidence.....                                      | 21 |
| 10. Conclusion.....                                                  | 21 |
| 11. Recommendations.....                                             | 21 |

## Index of Tables

|                                      |    |
|--------------------------------------|----|
| Table 1: Evidence Inventory.....     | 7  |
| Table 2: Reconstructed Timeline..... | 20 |

## Table of Figures

|                                                                          |    |
|--------------------------------------------------------------------------|----|
| Figure 1: Creation of the UFED forensic case.....                        | 9  |
| Figure 2: Selection of the Advanced Logical extraction method.....       | 9  |
| Figure 3: Detection and identification of the demonstration handset..... | 10 |

|                                                                                                                                                     |    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Figure 4: UFED extraction summary.....                                                                                                              | 10 |
| Figure 5: Emma’s Huawei:<br>d5193dbf8246c09fdde73be8558343985ab24a2e1c142e4d64e16e2b6507e31f.....                                                   | 11 |
| Figure 6: Norman’s Nokia:<br>a693656c260e339069756be8005346e97033d0ccf2f79add56cd69c9eade13ab.....                                                  | 11 |
| Figure 7: Joe’s Samsung:<br>0e585c4fe8160254253be515a16ff94b7fdf88b248b67d45cfdef8753a9a3195.....                                                   | 12 |
| Figure 8: Unknown Ulefone:<br>630724e2f8863adb9c4f7df1ab645e56c19a832d546fe7ab55b0cebf8ea7befd.....                                                 | 12 |
| Figure 9: Communication applications decoded from Emma’s Huawei.....                                                                                | 13 |
| Figure 10: Emma disclosing access to valuable AI-related information.....                                                                           | 14 |
| Figure 11: Joe reporting contacts and a further meeting.....                                                                                        | 15 |
| Figure 12: Negotiation update and proposed Manchester meeting.....                                                                                  | 15 |
| Figure 13: Communication concerning “5M” and the remaining arrangement.....                                                                         | 16 |
| Figure 14: Peter Dover and Norman negotiating blueprint delivery.....                                                                               | 17 |
| Figure 15: Offshore payment and proposal for inbox transfer. ....                                                                                   | 18 |
| Figure 16: Swansea-area location artefact from Norman’s Nokia.....                                                                                  | 19 |
| Figure 17: A picture about travels that can be obtained from the Samsung of Joe. ....                                                               | 19 |
| Figure 18: File and camera metadata for image 20241122_112158.jpg, captured using Joe’s<br>Samsung SM-A137F on 22 November 2024 at 11:21:58.....    | 20 |
| Figure 19: Cellebrite timeline correlating image 20241122_112158.jpg with the Wigan-<br>associated location event recorded on 22 November 2024..... | 20 |
| Figure 20: Cellebrite map view showing the Wigan-associated coordinates 53.543655, -2.627383<br>embedded in image 20241122_112158.jpg.....          | 20 |

# Task 01

## 1. Introduction

Digital forensics is defined as the scientific methodology of identifying, securing, acquiring, analysing, examining and presenting data from digital devices to be able to use the information either internally or in a court of law. In the initial stages, the field was concentrated on standalone computers and physical media storage. In the modern age, however, the investigation includes the use of smartphones, cloud computing, social media accounts, computer networks, Internet of Things (IoT) gadgets, cars and drones. According to the NIST, digital forensics investigators have to obtain data from various sources without changing the information [1].

Digital forensics is widely employed by law-enforcement organizations, governmental institutions, financial institutions, consultancy firms and corporate cybersecurity teams. Digital forensics aids in investigating cyber attacks, fraud, intellectual property theft, insider threat and other types of computer-related crimes. Consequently, digital forensics has become an essential field in the modern cybersecurity.

## 2. Present Status of Digital Forensics and Its Tools

Digital forensics investigation usually involves a structured lifecycle which includes identification, acquisition, preservation, analysis, examination and reporting. Investigators typically perform a forensic imaging process instead of analyzing the original storage medium. The process of creating a forensic image involves making a perfect bit-to-bit copy including the deleted files and unallocated space. Cryptographic hash functions such as SHA-256 are generated to prove the integrity of the evidence obtained. The chain of custody of the evidence obtained is also recorded to indicate who was involved in its collection, transfer, storage and analysis.

There are various specialized tools used for performing digital forensics investigation. Autopsy is one of the open-source platforms that is used for conducting digital-forensics investigation. The tool has features for file-system examination, timeline analysis, keyword search, hash filtering, artifact analysis, and deleted-file recovery [2]. The tool is capable of recovering information from unallocated space using the data carving technique.

FTK Forensic Toolkit is an expensive commercial forensic tool that allows processing and analyzing huge amounts of evidence. Features provided by FTK Forensic Toolkit are evidence indexing, search and distributed processing. These features will help to identify relevant files, e-mails and artifacts in huge data sets [3]. FTK Imager is able to create forensic images and check their integrity by computing their hash values.

Cellebrite UFED is a tool specialized in conducting mobile-device forensic investigations. Cellebrite UFED is capable of acquiring digital evidence from smartphones, feature phones, SIM cards, memory cards, GPS units and some types of drones [4]. Depending on the type of the device and jurisdiction, both logical and physical methods of acquisition can be applied. Other widely used forensic tools are EnCase for computer and enterprise forensics, Volatility for volatile memory forensics, Wireshark for network traffic analysis and Magnet AXIOM for

correlating mobile, computer and cloud artifacts. The results obtained with the use of forensic tools should be double-checked since different forensic tools may interpret the same artifact differently.

### **3. Intersection of Digital Forensics and Cybersecurity**

Despite their closeness, digital forensics and cybersecurity have different purposes. Cybersecurity focuses on prevention, detection, and mitigation of cyberattacks. Digital forensics, in turn, is a practice of finding out what has happened, how, what information was compromised and potentially who did it. Their combination is referred to as DFIR – Digital Forensics and Incident Response.

In the course of cybersecurity breach, such technologies as firewalls, intrusion-detection systems, endpoint detection and response technologies and Security Information and Event Management systems create alerts and logs. The investigators then save this data and correlate it with other evidence coming from storage media, computer memory, network traffic, cloud services, and mobile devices. In this way, an investigator might find out where the attacker got access, how he or she moved across the network, what malware did, and how did the data exfiltration happen.

The findings in the process of digital forensics could be used not only as evidence in the investigation but also as the information for the development of new cybersecurity controls. It could help to improve patch management if the attack involved exploitation of an unpatched service, and introduce multi-factor authentication if the breach included the use of credentials of an employee.

### **4. Latest Developments in Digital Forensics**

The application of artificial intelligence and machine learning to classify images and detect patterns, as well as find suspicious files and sort through evidence, is becoming more prevalent. These technologies help decrease the time needed for evidence evaluation. Nevertheless, it should be validated by humans since errors made by algorithms, bias or lack of explanation might make the evidence unreliable and inadmissible.

Another fast-growing field of digital forensics is cloud forensics. Companies store vast amounts of data using cloud services, such as Microsoft Azure and Amazon Web Services. Therefore, the investigation will be carried out with the help of audit logs, API, and cooperation of cloud providers. Cloud forensics is a complex process that involves many technical and legal challenges [5].

The field of IoT forensic investigation has become even more important. Smartwatches, home assistants, closed circuit television (CCTV) systems, cars and sensors in industries, as well as other types of devices that are connected to IoT networks, might capture evidence related to locations, communications and activity of users. However, since IoT devices have different hardware and software components, operating systems, communication protocols and data formats, collecting and analyzing digital evidence becomes very challenging [6].

## 5. Key Challenges

The amount and types of digital evidence represent one of the key challenges for investigators. An individual case could entail huge volumes of data gathered from different devices and online accounts. According to NIST, finding valuable evidence in very large data volumes and extracting data from broken devices are some of the current problems [1].

Encryption, security features of mobile operating systems, anti-forensics, deleted files, and frequently updated applications limit access to evidence. Cloud and social media evidence are often stored on servers in other jurisdictions. In addition, it is essential to consider privacy and human rights issues during the process of gathering evidence and not collect unrelated personal data.

Some other challenges are the validation of forensic tools, lack of standardized processes in the international context, restricted access to realistic forensics datasets, and constant need for professional development of the specialist's skills. The growing sophistication of cyber-attacks and the evidence gathering process requires using several forensic technologies at a time [7].

## 6. UK and International Employment Market for Forensic Analysts

In the United Kingdom, digital forensics jobs are needed in the police service, the National Crime Agency, governmental departments, cybersecurity firms, banks and corporations. Possible career positions in this field include digital forensics investigator, mobile device examiner, cyber incident responder, e-discovery analyst, malware analyst and forensic consultant.

Even though there has been a decrease in the number of job postings in the UK cybersecurity industry amid the digital industry downturn recently, the employment in the UK cybersecurity industry rose from about 46,683 people in 2020 to 69,589 people in 2025 [8]. These statistics concern the entire industry in question, not digital forensics employment specifically.

Forensic science provides career possibilities in areas like law enforcement agencies, defense sectors, banks, tech companies, multinational companies, and forensic consulting firms. The typical requirements include understanding of forensic tools, Windows and Linux operating systems, mobile and cloud computing, networking, scripting and handling of evidences.

Credentials like the ones mentioned below can prove beneficial in career development in the profession.

Credentials for Forensic Science:

- EnCase Certified Examiner
- GIAC Certified Forensic Examiner
- GIAC Certified Forensic Analyst
- Cellebrite credentials

Technical skills need to be coupled with analytical skills, ethics, and the ability to communicate effectively.

## 7. Conclusion

From computer-based investigations, digital forensics has evolved into a multi-disciplinary branch dealing with data from mobile devices, the cloud, networks, IoT, and even artificial intelligence. Digital forensics has become a key part of cybersecurity incidents and legal investigation processes. Even though the issues with evidence quantity, encryption, privacy, jurisdiction, and reliability of the tools remain a challenge, the constant technological evolution and reliance on digital technologies will continue the need for digital-forensics experts.

## References

- [1] National Institute of Standards and Technology, Digital Evidence, NIST.
- [2] The Sleuth Kit, Autopsy: Digital Forensics Platform.
- [3] Exterro, FTK Forensic Toolkit.
- [4] Cellebrite, Cellebrite UFED: Mobile Forensic Data Extraction Tool.
- [5] 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, Art. no. 433, Jan. 2024, doi: 10.3390/s24020433.
- [6] A. A. Ahmed, K. Farhan, W. A. Jabbar, A. Al-Othmani and A. G. Abdulrahman, “IoT Forensics: Current Perspectives and Future Directions,” *Sensors*, vol. 24, no. 16, Art. no. 5210, Aug. 2024, doi: 10.3390/s24165210.
- [7] F. Casino, T. K. Dasaklis, G. P. Spathoulas, M. Anagnostopoulos, A. Ghosal, I. Borocz, A. Solanas, M. Conti and C. Patsakis, “Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews,” *IEEE Access*, vol. 10, pp. 25464–25493, 2022, doi: 10.1109/ACCESS.2022.3154059.
- [8] UK Government, Department for Science, Innovation and Technology, Cyber Security Sectoral Analysis 2026, May 2026.

# Task-02

## 1. Executive Summary

A case of unauthorised access to confidential data on Quantum Tech artificial-intelligence technology was raised. Emma, a newly hired senior engineer, was identified as the main culprit. Joe was suspected of acting as an intermediary, while Norman was suspected of acting as a buyer.

Extraction analysis of four Android phones was conducted using Cellebrite Physical Analyzer version 7.73.0.11. They were Emma's Huawei POT-LX1 P Smart, Joe's Samsung Galaxy A13, Norman's Nokia C2 2nd Edition, and another Ulefone Note 14 of undetermined ownership. All four extractions passed the integrity check through SHA-256 hash algorithm by Cellebrite. The most compelling piece of evidence found was on Emma's Huawei phone. On 21 August 2024, Emma told Joe that she had access to confidential information on AI technology and that she would consider selling it. In the subsequent conversations, Joe was shown searching for potential buyers, making arrangements and negotiating with a client in Manchester. "5M secured" was mentioned later on.

Conversely, another conversation between the account Peter Dover and Norman focused on Joe's preparedness, a "Blueprint," an "offshore 5M" payment and inbox transaction within 48 hours. Several accounts by Peter Dover were found on Emma's Huawei device. This shows that Emma could have been using Peter Dover as an alias; however, it is necessary to use the external accounts to prove the same conclusively.

The location and image meta-data obtained from Joe's Samsung and Norman's Nokia phones provided contextual information on their movement. No relevant evidence was found for the email or call-log category under review. Therefore, while the collected evidence strongly suggests that there was a concerted effort to leak and sell sensitive technical data, there is no proof of successful transfer of the information and/or payment.

## 2. Case Background and Context

Quantum Tech had suspicions of unauthorised access of confidential technical data. Emma was thought to be involved in acquiring this data to sell it to a rival company or an outsider. Joe had been involved in introducing Emma to Norman, who was considered to be the buyer.

It was intended to:

- Establish whether the device extraction provided was legitimate.
- Recover and analyse the relevant communication.
- Identify discussions about confidential data, buyers, meeting, payments, and transfers.
- Create a timeline of relevant activities.
- Analyze supporting imagery, metadata, and location data.
- Establish what were the possible roles of the suspects and their motivations.

### 3. Evidence Inventory

| ID  | Owner   | Device                      | Operating System | Principal evidence                                 |
|-----|---------|-----------------------------|------------------|----------------------------------------------------|
| E01 | Emma    | Huawei POT-LX1 P Smart      | Android 10       | Chats, user accounts and suspected alias           |
| E02 | Norman  | Nokia C2 2nd Edition        | Android 11       | Location and media artefacts                       |
| E03 | Joe     | Samsung Galaxy A13 SM-A137F | Android 14       | Images, timelines and location artefacts           |
| E04 | unknown | Ulefone Note 14             | Android 12       | Verified extraction; no relevant finding displayed |

*Table 1: Evidence Inventory*

The Google account that was used on Emma's Huawei included dovp59@gmail.com; the Snapchat username included peter\_dover; the several Peter Dover accounts, as well as telephone number +447917162788, which became significant when Peter Dover communicated directly with Norman.

### 4. Acquisition, Integrity and Continuity

#### 4.1 Acquisition Procedure

The software Cellebrite UFED 7.76.0.24 Educational Edition was used to show the procedure of Android acquisition. A controlled Samsung Galaxy J7 Prime 2 was used in the procedure and not an evidentiary device.

The procedure involved:

- Creation of the forensic case and noting of the examiner, department and place.
- assignment of an evidence device identifier.
- connection of the device by a data cable that is supported.
- selection of the device using Auto Detect.
- selection of an extraction process that is supported.
- selection of categories of content needed.
- saving the extraction into a controlled case directory.
- checking the acquisition summary for unsupported or failed content categories.
- opening of the extraction using Physical Analyzer and checking the hash value.

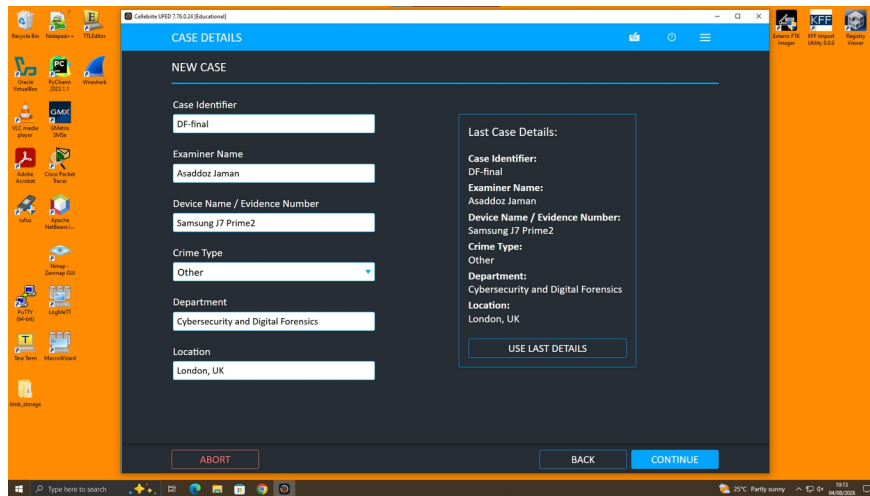


*Figure 1: Creation of the UFED forensic case.*

Figure 1 identifies the case ID as DF-final, the examiner and the location where the acquisition took place. This is done to set up the necessary administrative environment needed for a valid acquisition.

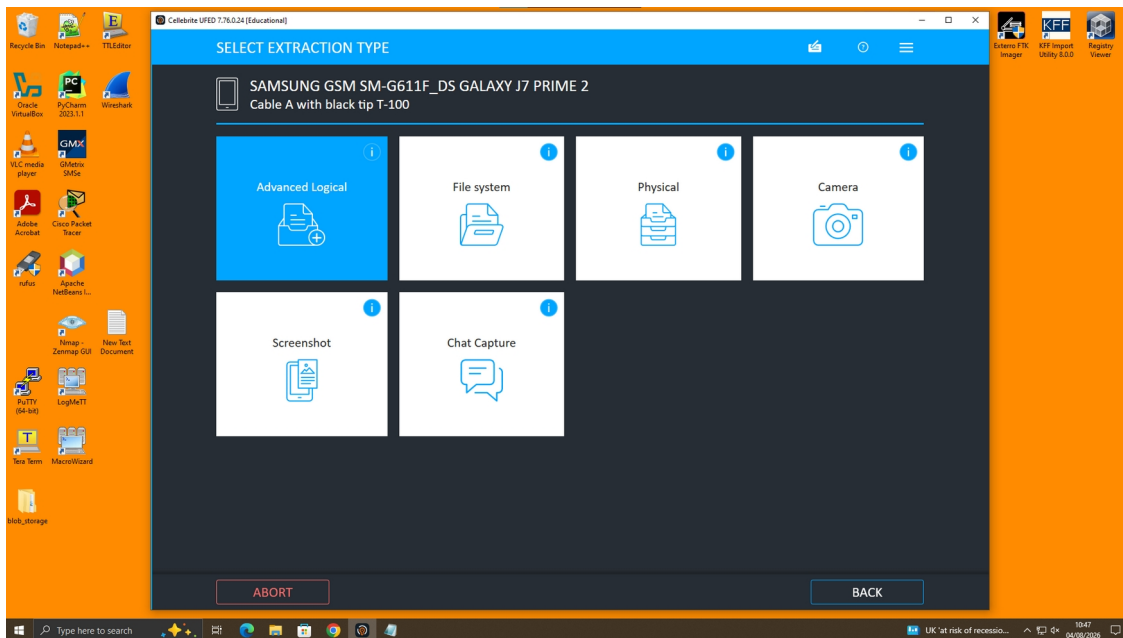


*Figure 2: Selection of the Advanced Logical extraction method.*

Figure 2 depicts the available extraction procedures for the demonstration phone. Advanced Logical was chosen as the procedure for this demonstration. The case phones have been acquired using their respective file system or android back-up procedure.

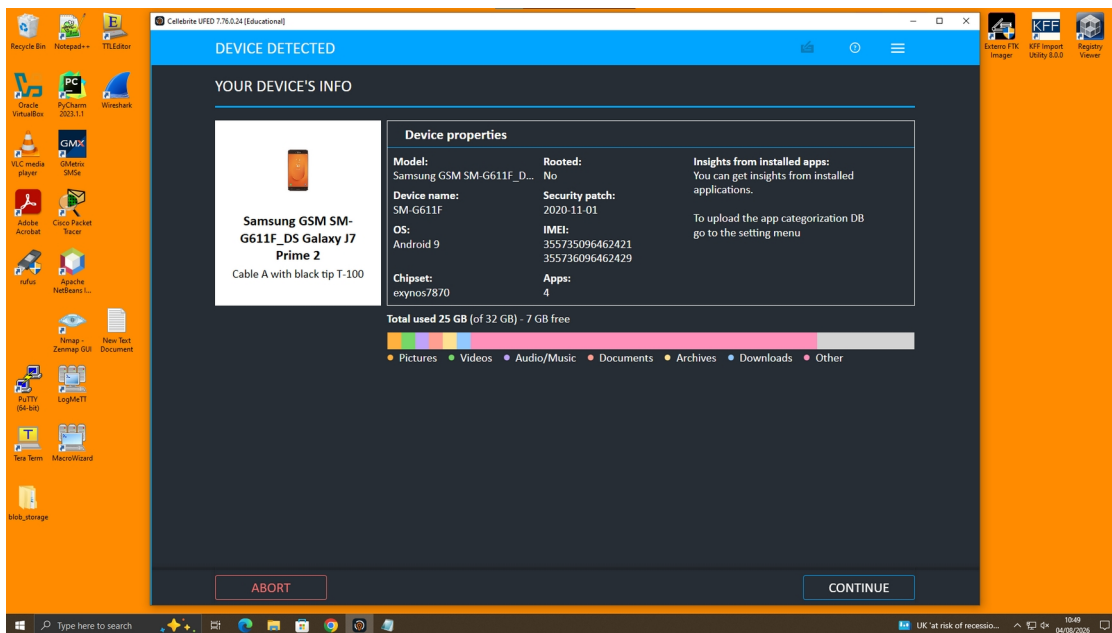


*Figure 3: Detection and identification of the demonstration handset.*

The information about the model, Android version, security update, and storage & IMEI IDs is shown in Figure 3. This clearly indicates the significance of verifying device identity prior to acquisition.

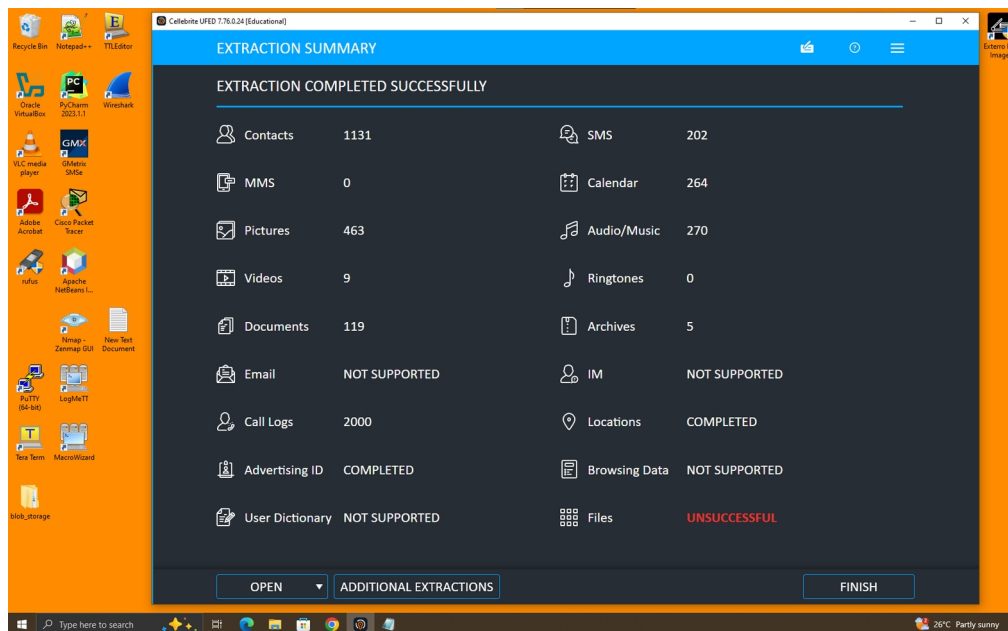


*Figure 4: UFED extraction summary.*

Figure 4 shows categories that were successfully recovered along with their limitations. The demonstration was able to recover contacts, messages, calls history, location, pictures, documents, and multimedia but not email and instant messaging categories. The general file category was also unsuccessful.

## 4.2 Hash Verification

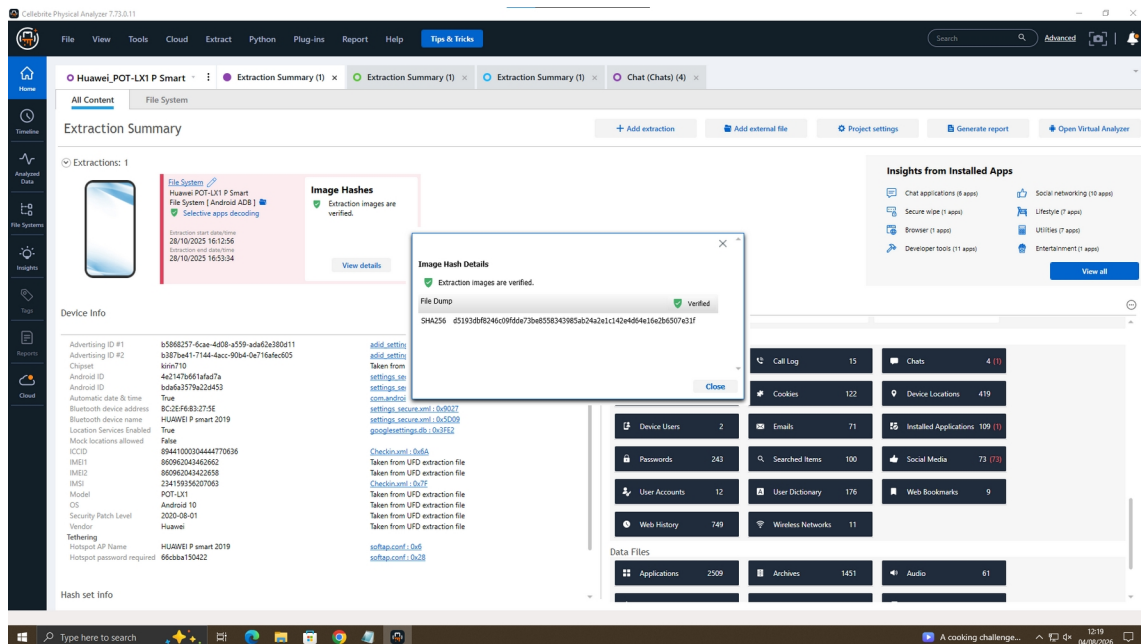


Figure 5: Emma's Huawei:  
*d5193dbf8246c09fdde73be8558343985ab24a2e1c142e4d64e16e2b6507e31f*

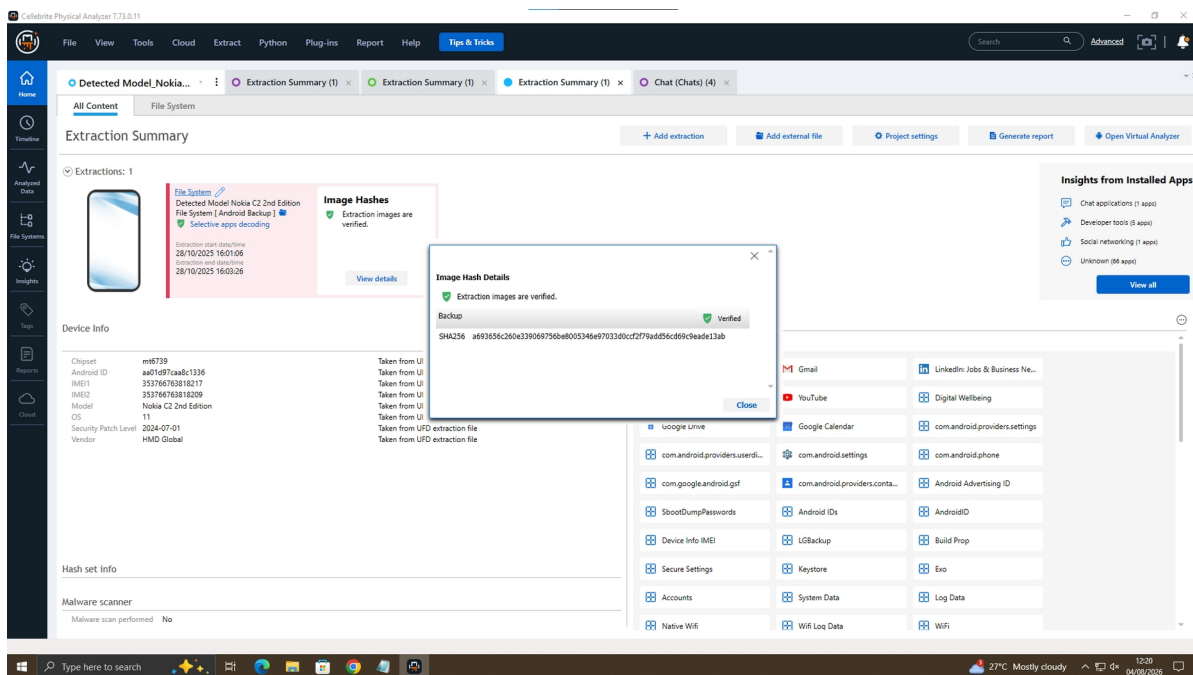


Figure 6: Norman's Nokia:  
*a693656c260e339069756be8005346e97033d0ccf2f79add56cd69c9eade13ab*

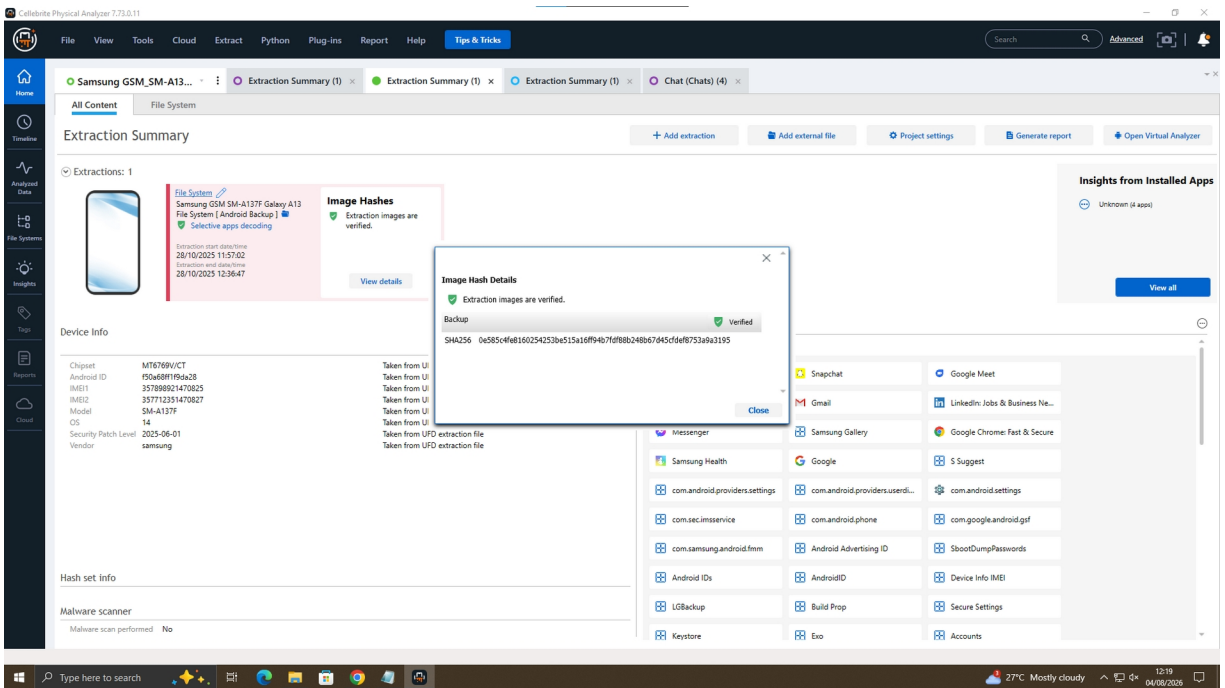


Figure 7: Joe's Samsung:

0e585c4fe8160254253be515a16ff94b7fd8b248b67d45cfdef8753a9a3195

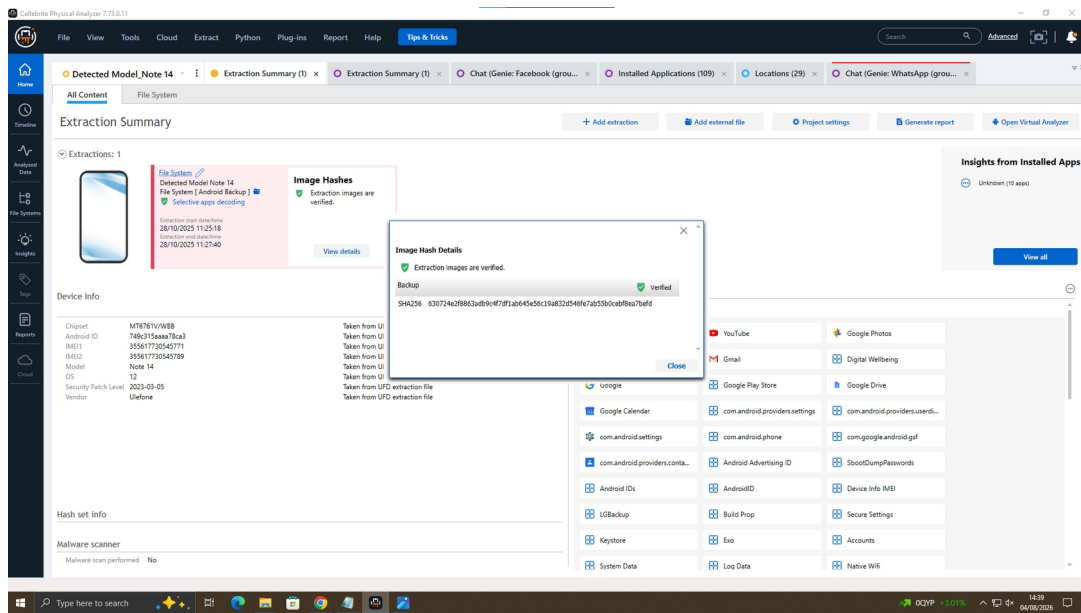


Figure 8: Unknown Ulefone:

630724e2f8863adb9c4f7df1ab645e56c19a832d546fe7ab55b0cebfb8ea7befd

The images shown in Figures 5, 6, 7, 8 prove that Cellebrite classified each image from an extraction as verified. Original files were saved, and the analysis was performed on the verified working copies. Access to the device, movement, and storage must be recorded.

## 5. Forensic Methodology

The Cellebrite Physical Analyzer was employed for decoding application databases, examining participant details, searching chats, analyzing media metadata and creating timelines. Among the relevant keywords, Emma, Joe, Norman, Peter, AI, information, client, meeting, blueprint, offshore, and 5M should be mentioned.

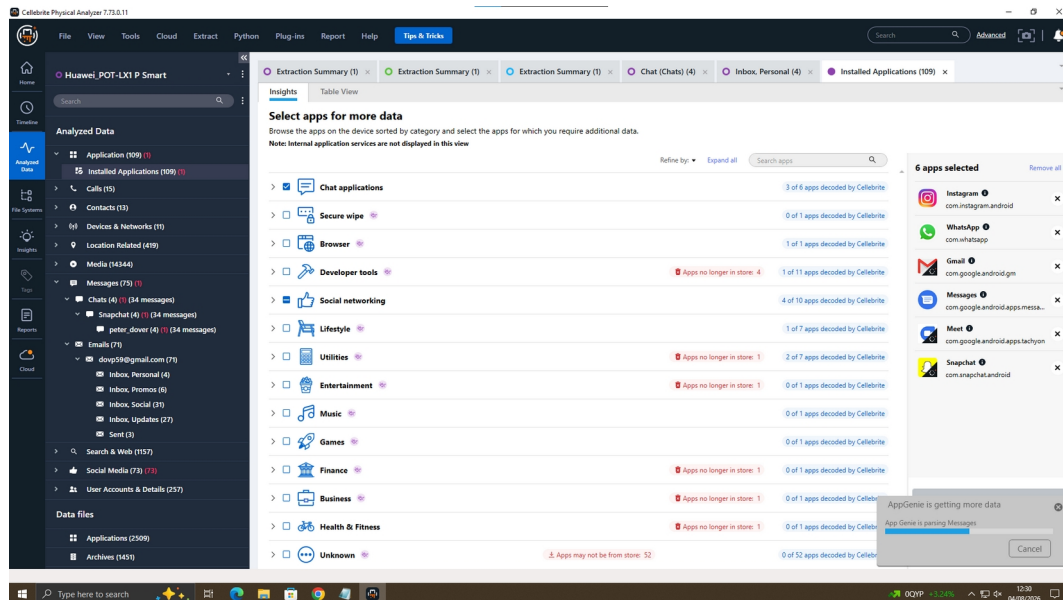


*Figure 9: Communication applications decoded from Emma's Huawei.*

Figure 9 depicts such applications as WhatsApp, Instagram, Gmail, Messages, Google Meet and Snapchat. With the use of the Cellebrite Genie, 327 chat messages were found. Email and call log artifacts were inspected; however, there was no relevant evidence found.

Notable artifacts were analyzed within the context of the conversation they occurred in. Timestamps were noted according to what was presented in Cellebrite and mainly represented in UTC+0. Image metadata, geographical coordinates and timeline data were linked when possible. No artifact was considered to be related to a suspect because it was located on his/her device only.

## 6. Findings and Evidence Analysis

### 6.1 Emma's Initial Approach to Joe

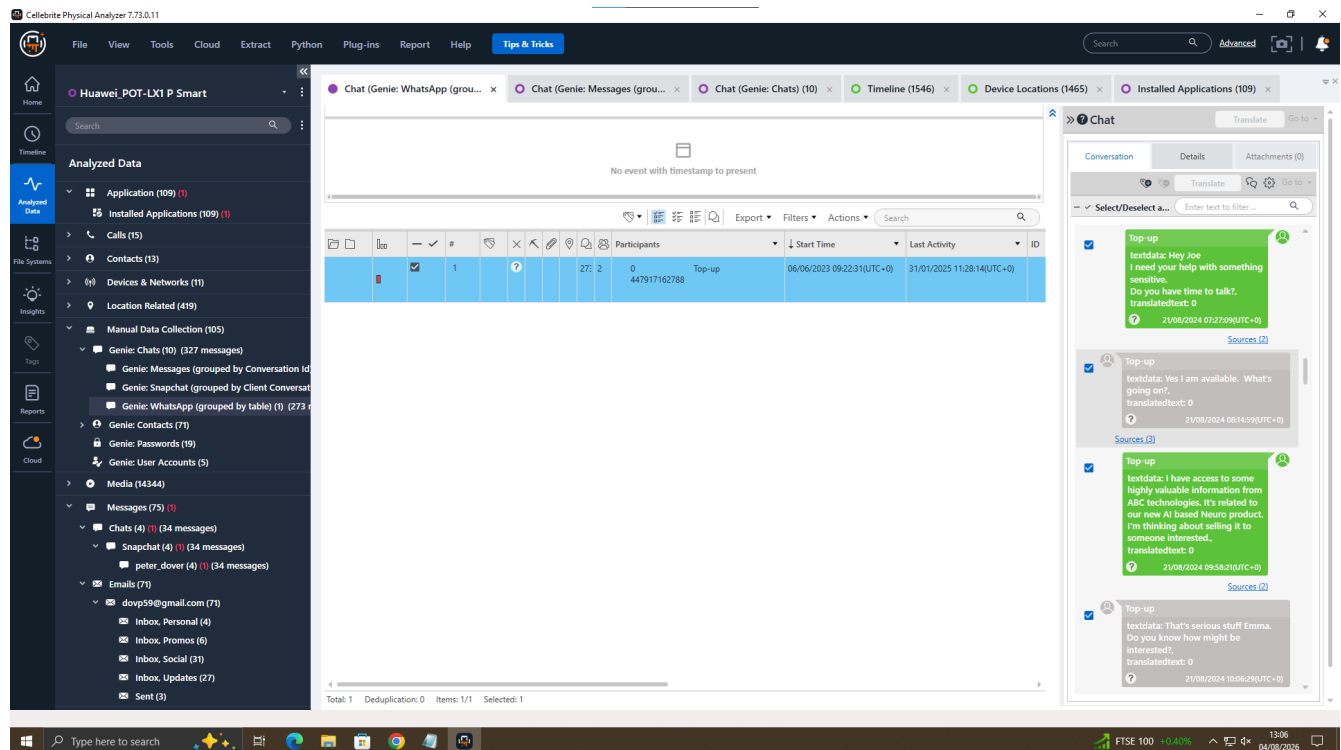


Figure 10: Emma disclosing access to valuable AI-related information.

Intention is set out in Figure 10 since Emma has confidential information and plans on selling the information. The response by Joe shows that he is aware of the intention behind this request.

The mention of “ABC technologies” is different from Quantum Tech in the scenario. Consequently, this chat depicts an attempt to sell confidential AI-related information, but the ownership of this information remains unknown.

### 6.2 Joe's Search for a Buyer

Joe told Emma on 26 August 2024 that although an earlier meeting did not go as planned, he managed to get contacts for a second meeting.

This is evidenced by Figure 11, which shows how Joe was reaching out to other people after Emma made her request.

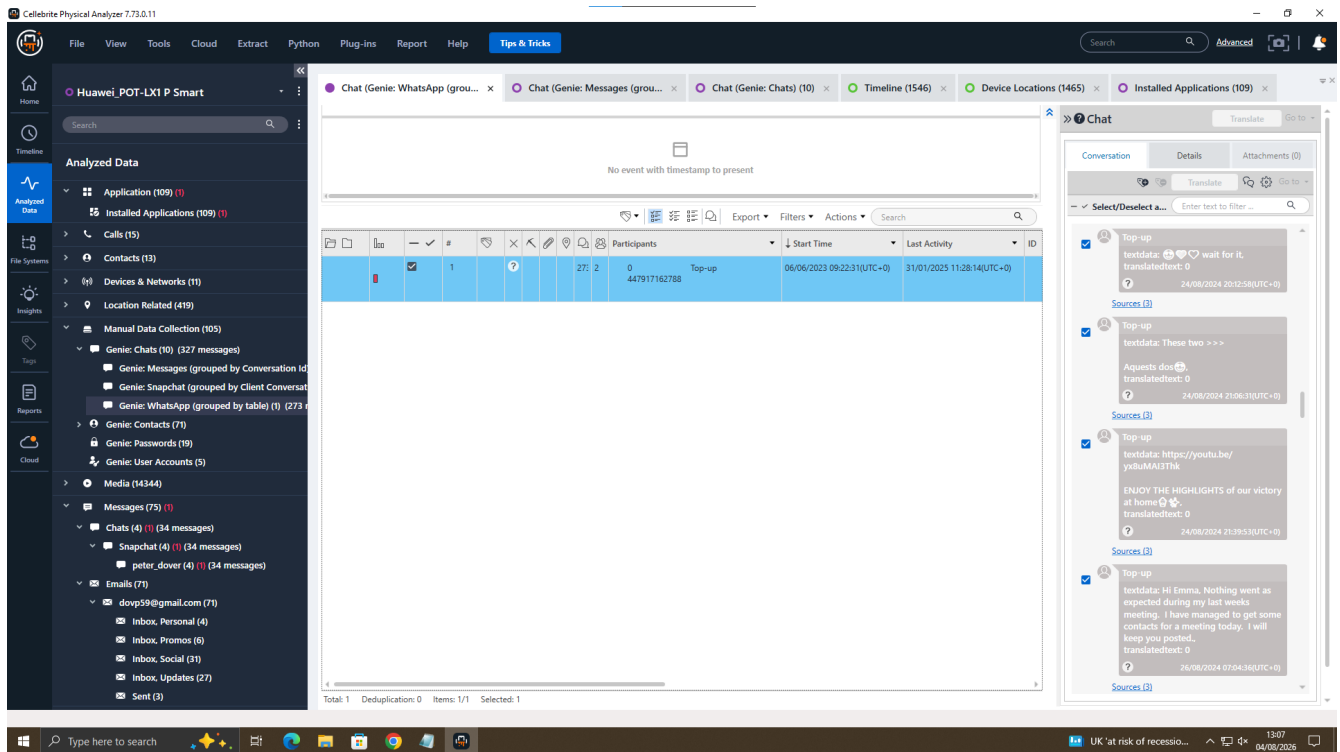


Figure 11: Joe reporting contacts and a further meeting.

20 November 2024, Emma asked for update and threatened that she will talk to other people who are interested. I am in final talks about it. Meeting the client this week at Manchester.

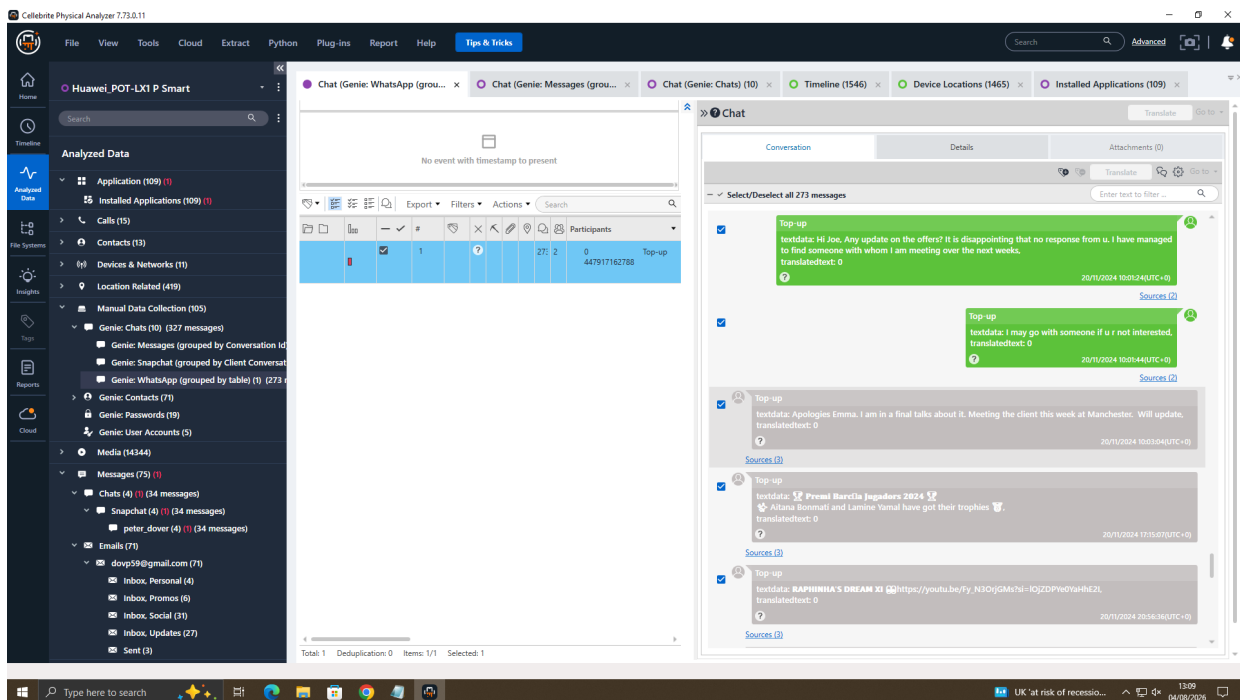


Figure 12: Negotiation update and proposed Manchester meeting.

Figure 12 shows that Joe's activities had evolved to include negotiating with a particular client. Emma's mention of other potential buyers clearly indicates that her objective remains selling the data.

### 6.3 Proposed Payment

A message dated 31 January 2025 read:

He's good with it. 5M secured. Confirming it. What about the rest?

The answers related to "local part," which exerted pressure and there were others waiting.

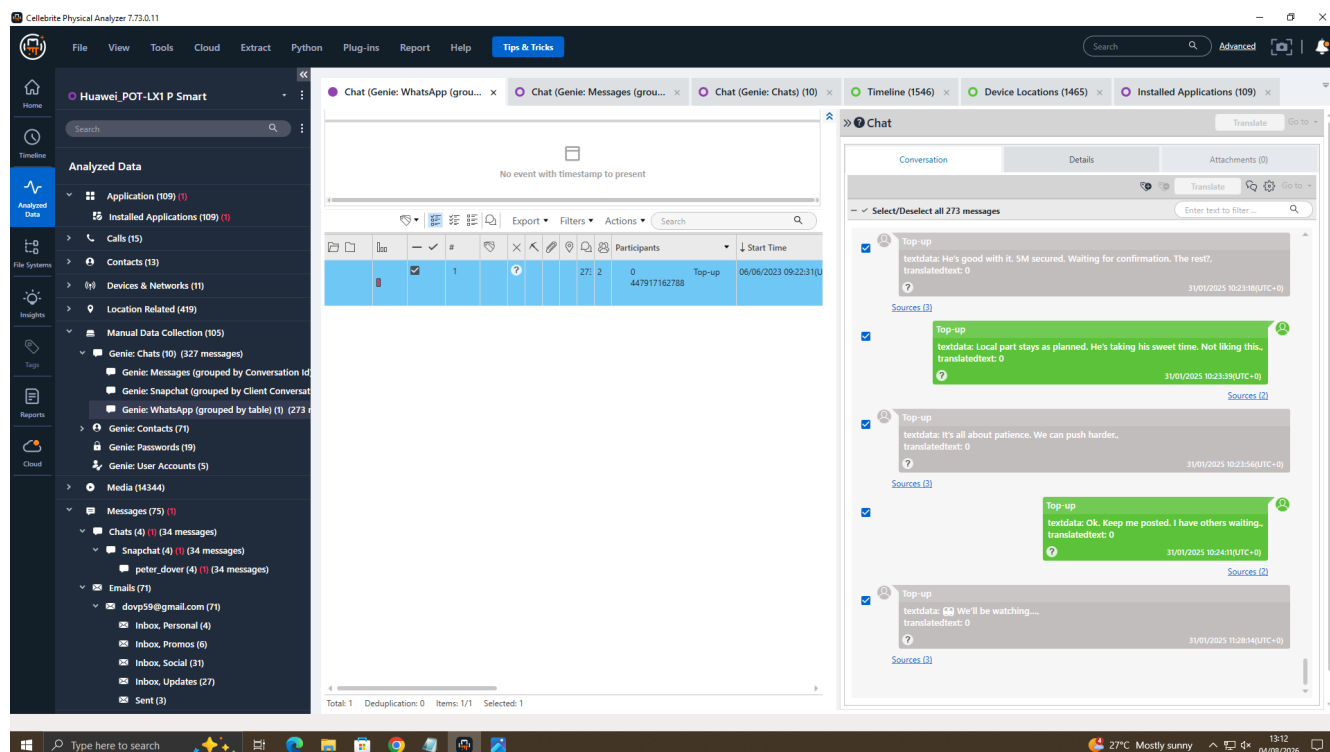


Figure 13: Communication concerning “5M” and the remaining arrangement.

As shown in Figure 13, the negotiation process involved a large proposed payment. Yet, the currency or the completion of the transaction is not known. Thus, “5M” is considered a proposed amount and not a confirmed one.

### 6.4 Peter Dover Alias and Norman

The Huawei preliminary report included multiple accounts belonging to Peter Dover. Since the phone is owned by Emma, it indicates that Peter Dover must have been an alias name used by Emma.

On 31 January 2025, Peter Dover contacted Norman: Norman, Joe told me u r ready to proceed. Let us keep this clean and quick.

Norman responded: Almost there. We will need the Blueprint in chunks. Risky to send all at once.

Peter insisted on getting the whole content, but Norman suggested starting with the “head” for security purposes.

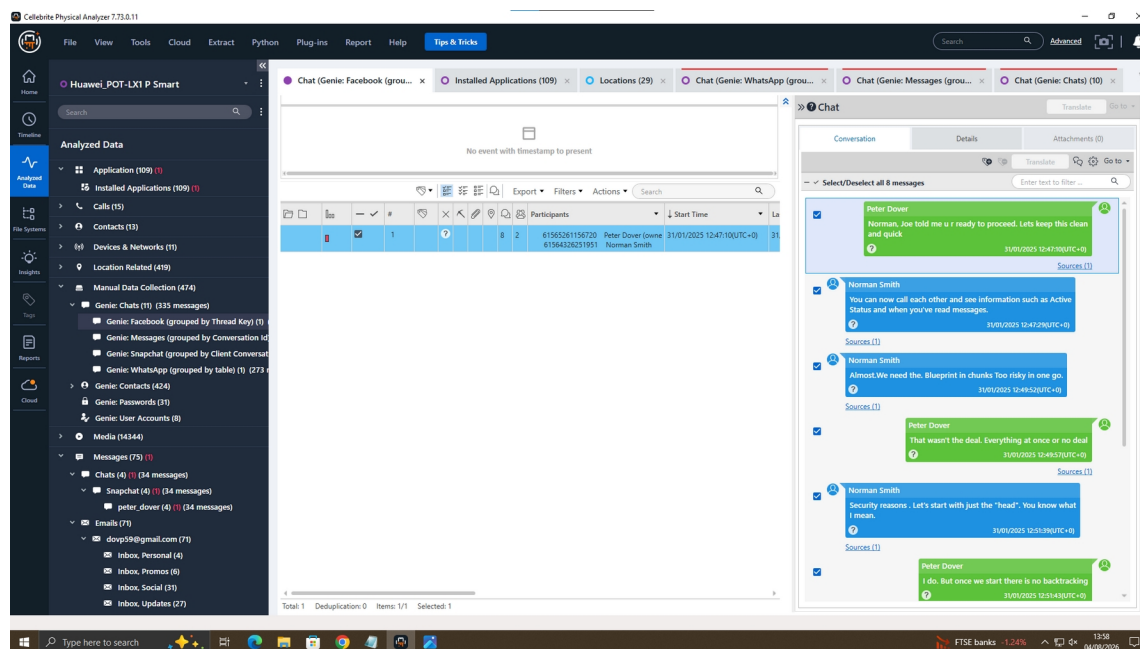


Figure 14: Peter Dover and Norman negotiating blueprint delivery.

Figure 14 shows that Norman has connections to Joe and the account using Emma’s Huawei. The communication clearly exhibits familiarity with the technical content and the negotiation of the transfer process.

Norman further commented: Agreed. First part releases, and 5M offshore reflects.

Peter responded: Check ur inbox in 48 hrs. After that we are ghosts.

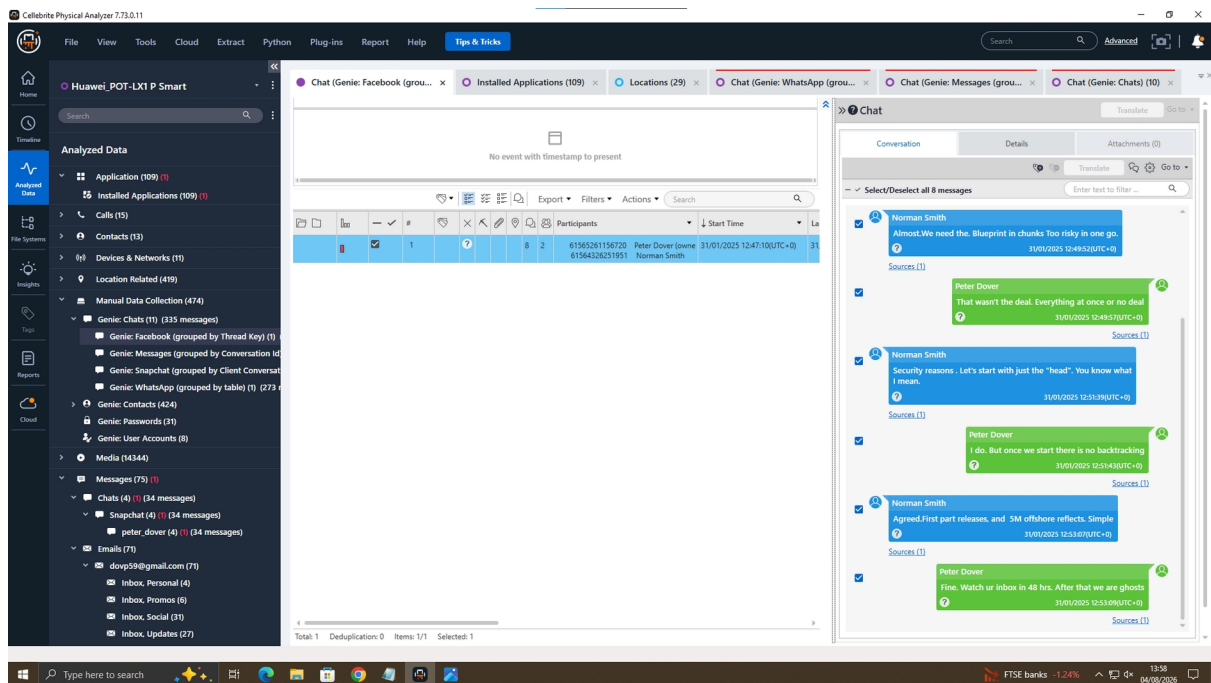


Figure 15: Offshore payment and proposal for inbox transfer

Figure 15 links the plan with an offshore “5M” deal and 48 hours for transfer. The expression “after that we are ghosts” suggests a possible attempt to remain undetected after the proposed transaction.

Alias association is only an assumption. Proof of external account registration/authenticity would be necessary to confirm that Emma had indeed written all Peter Dover communications.

## 6.5 Norman’s Nokia Location Evidence

The mobile phone belonging to Norman was found to have 29 location artefacts. The photograph named IMG\_20240904\_123804\_430.jpg, which had been taken on 4 September 2024 at 12:38:04, had the coordinates 51.625252, -3.996134

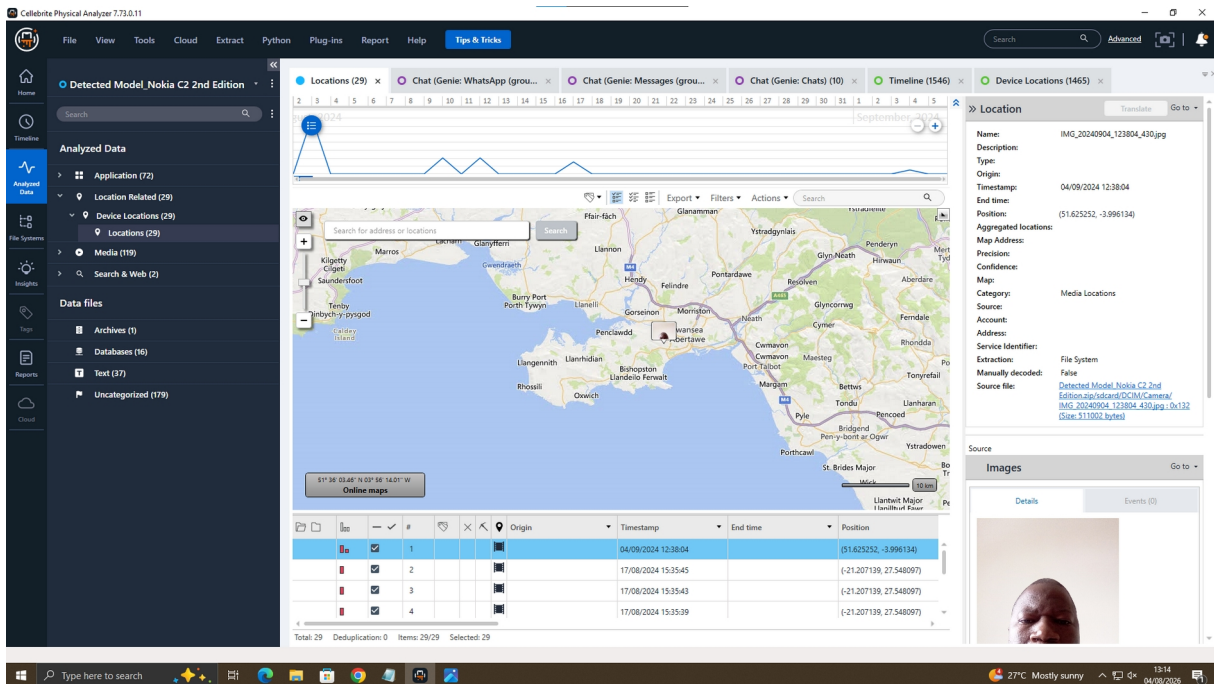


Figure 16: Swansea-area location artefact from Norman's Nokia.

Image association on Norman's Nokia with the Swansea region is indicated in Figure 16. This offers context for movement but does not necessarily prove Norman had contact with a second suspect.

### 6.6 Joe's Samsung Evidence

The number of images and location artefacts within the Samsung device of Joe included 1,190 images and 1,465 location artefacts. Image 1000001349.jpg showed Joe's travel tickets and it was edited on 31 August 2024.

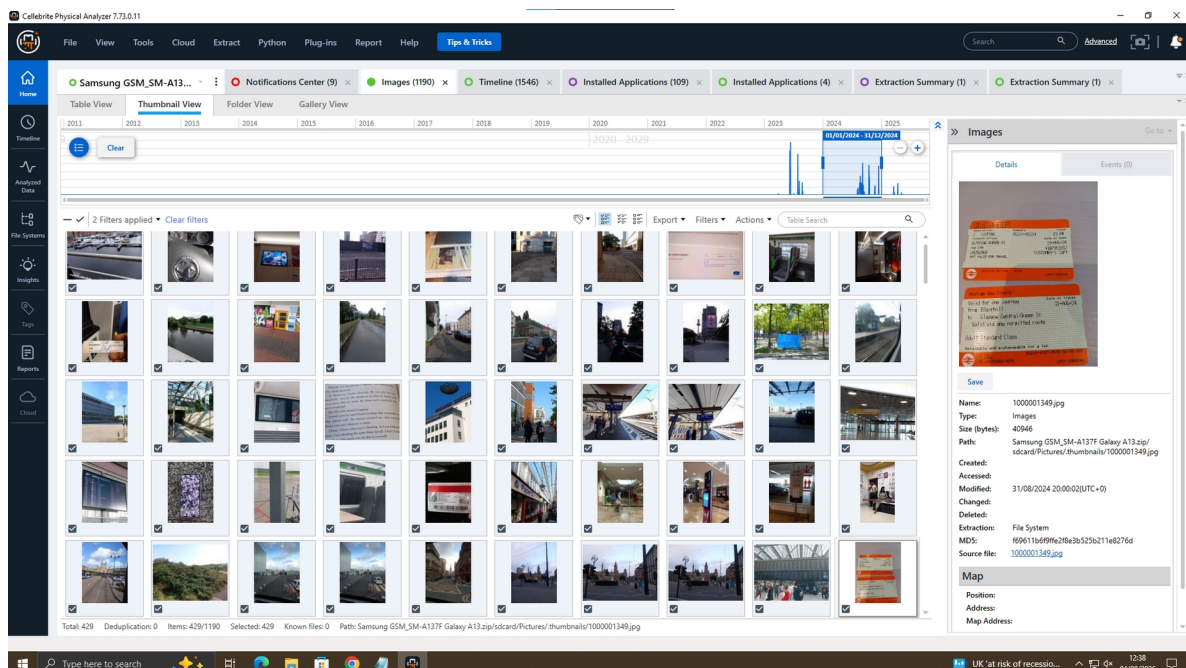


Figure 17: A picture about travels that can be obtained from the Samsung of Joe.

Figure 17 may help us to investigate further into the movements of Joe. It is necessary for us to review the original image in order to make any claims on the ticket or Joe's travel.

A Samsung SM-A137F was used to take image 20241122\_112158.jpg on November 22, 2024, at 11:21:58. It was located in the Wigan region at coordinates 53.543655, -2.627383.

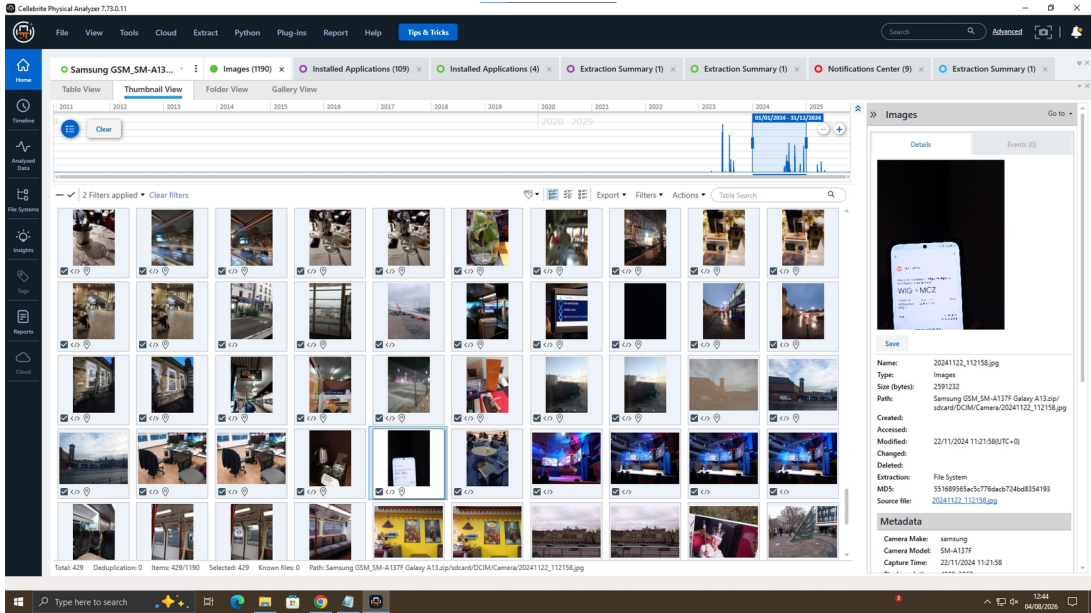


Figure 18: File and camera metadata for image 20241122\_112158.jpg, captured using Joe's Samsung SM-A137F on 22 November 2024 at

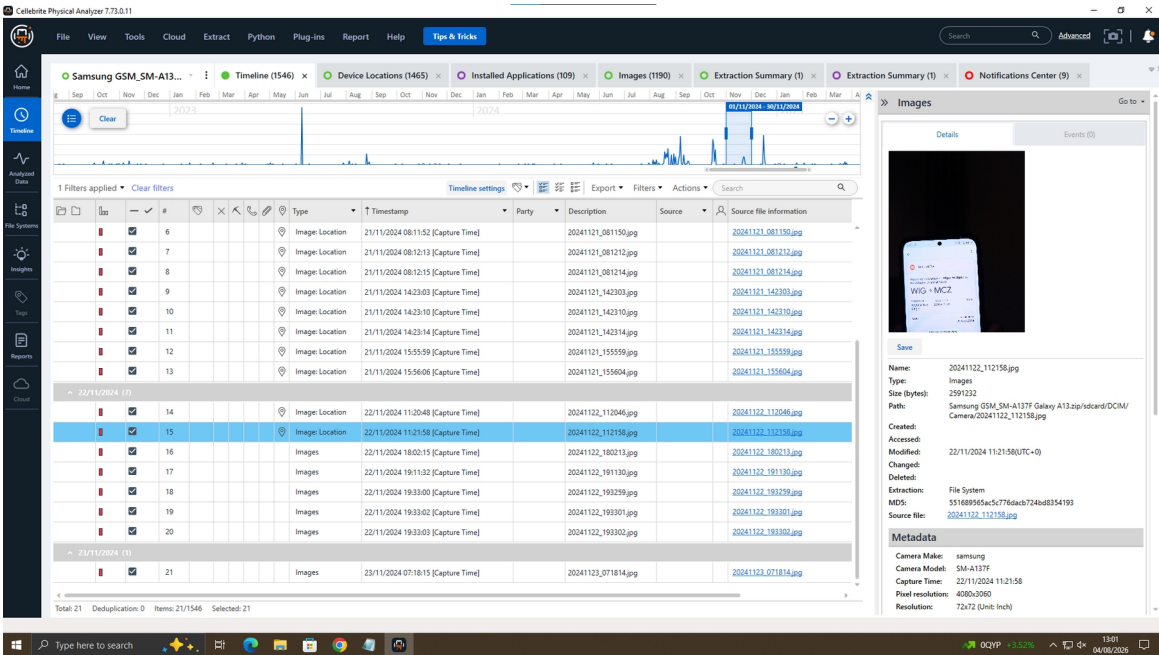


Figure 19: Cellebrite timeline correlating image 20241122\_112158.jpg with the Wigan-associated location event recorded on 22 November 2024.

Figures 18-19 confirm the filename, handset model, time of capture, MD5 value and coordinates. The incident came just after Joe reported a possible meeting with a Manchester

client. The geographical and temporal proximity is interesting, but does not prove the meeting occurred.

The extraction from the Ulefone did not yield any meaningful relevant finding in the evidence provided.

## 7. Reconstructed Timeline

| Date          | Significant Event                                                                             |
|---------------|-----------------------------------------------------------------------------------------------|
| 21 Aug. 2024  | Emma approaches Joe and proposes selling valuable AI information.                             |
| 26 Aug. 2024  | Joe reports obtaining contacts for a further meeting.                                         |
| 31 Aug. 2024  | Travel-related material appears on Joe’s Samsung.                                             |
| 04 Sept. 2024 | Norman’s Nokia contains a Swansea-area location artefact.                                     |
| 20 Nov. 2024  | Joe reports final discussions and a Manchester client meeting.                                |
| 22 Nov. 2024  | Joe’s Samsung records a Wigan-associated photograph.                                          |
| 31 Jan. 2025  | Messages refer to “5M secured.”                                                               |
| 31 Jan. 2025  | Peter Dover and Norman negotiate blueprint delivery, offshore payment and a 48-hour transfer. |

*Table 2: Reconstructed Timeline*

The sequence of significant events found from the evidence gathered from the mobile devices is illustrated in Table 2 below. This sequence starts with the first encounter of Emma with Joe on matters of AI and continues with the alleged effort by Joe to find people to have further meetings. The travel and location artifacts obtained from Joe’s Samsung and Norman’s Nokia offer more temporal and geographic context for this series of events. The latter communications involving the meeting at Manchester, the statement of securing “5M”, the delivery of blueprints, offshore payment and 48 hours transfer suggests a sequence of activities that range from planning to negotiation and completion. Despite this chronological reconstruction that backs up the suggested roles of Emma, Joe and Norman, these events should be taken within the bounds of the evidence.

## 8. Suspect Profiling

Emma – primary suspect: Emma boasted access to useful information, announced plans to sell it, and forced Joe into getting an offer. The Peter Dover transactions on Emma's Huawei reveal that an alias was likely used by her to obscure her true identity. Emma had a money-motive.

Joe – intermediary: Joe searched for contacts, fixed meetings, and reported on the process of negotiation with a client. Joe's function appeared to be helping Emma make contact with a buyer and organize the deal.

Norman – alleged buyer: Norman discussed the delivery methods of blueprints and made mention of an offshore "5M" deal. Norman's security considerations show his understanding of the risks and the value of the transaction.

## **9. Limitations of Evidence**

- Peter Dover attribution is probably true but unverified.
- No currency is known for "5M," nor any financial records of it.
- The conversation mentions "ABC technologies," not Quantum Tech.
- Location metadata proves only the identities of devices and photos, not users.
- Emails and call log evidence were unavailable.
- No evidence proves the transfer of blueprints or money.
- The Ulefone user identity was unknown.

The current evidence has a number of drawbacks that may have an impact on the accuracy of the conclusions. First, user attribution, financial significance and any blueprint or money transfers have not been confirmed. Also, the metadata for locations identifies the device, but not the person. In addition, there is no email or call-log evidence available.

## **10. Conclusion**

It is clear that there was a planned attempt to sell confidential information related to artificial intelligence. It seems that Emma started and managed the operation, while Joe worked as an intermediary and Norman negotiated on behalf of the purchaser. The planned transfer of the blueprint, the offshore "5M" plan and the effort to operate under an alias point towards planning, motive and avoidance of detection.

There is strong evidence for unauthorised disclosure and sale of confidential technical information. But the evidence confirms only planning and negotiation, not necessarily completion of the transfer or the payment.

## **11. Recommendations**

- Gather authentication records for the accounts belonging to Peter Dover.
- Search the entire extraction for identifiers and deleted data related to the projects.
- Export the relevant communications with path and timestamps.
- Look into lawful financial documents for the planned offshore payment.
- Correlate Joe's travelling evidence with the meeting in Manchester.
- Keep copies of all original extractions, their hash values and continuity evidence.
- Differentiate between an attempt and a completed transfer in a legal accusation