

DIGITAL FORENSICS REPORT

Report Title

Digital Forensics in 2026: State of the Field, Cybersecurity Integration,
Emerging Trends, Challenges, and Forensic Investigation of a Corporate
Espionage Case

Student Name:

Keval Mahendra Motivaras

Student ID:

[2515743]

Module Name:

Digital Forensics Analysis (ACCA7031)

Programme:

MSc Cybersecurity and Digital Forensics

Module Leader:

Dr. Mohamed Ghanem

University

University of Wales Trinity Saint David (UWTSD) – London Campus

Submission Date

27 April 2026

Abstract

In recent years, digital forensics has become an essential component of cybersecurity, as a process of identifying, preserving and analysing digital evidence with regard to cybercrime and investigations at organisations. With the rise of digital technologies, cloud computing and mobile phones, the area of digital forensics becomes increasingly complex and extensive. The present report represents a thorough analysis of digital forensics combining theory and practice.

Firstly, the paper describes current practices and challenges in digital forensics such as key tools and capabilities, the relationship between forensic investigation and cybersecurity operations, the most prominent emerging technologies, as well as challenges like data volume, encryption and the shortage of skilled personnel. Moreover, the current labour market situation regarding employment in digital forensics is assessed with special emphasis on demand [1][2][3].

Secondly, a practical example of forensic investigation is given in which Cellebrite UFED and Cellebrite Physical Analyzer were used to conduct digital analysis of multiple devices, including acquisition, hash verification, cross-device correlation of data and their analysis. The main conclusions from the analysis include communication coordination, obfuscation of identities and meeting places based on geographical location.

Contents

Task 1 – Research Report	5
Current state of digital forensics and its tools	5
Intersection of digital forensics and cybersecurity	6
Emerging trends in digital forensics	6
Key challenges	7
National and international job market	9
Task 2 – Digital Forensics Investigation Report	10
2.1 Introduction	10
2.2 Evidence Acquisition and Integrity Verification	10
2.3 Multi-Device Data Integration and Analysis	12
2.4 Communication Analysis and Suspicious Conversations	13
2.5 Contact Analysis and Identity Obfuscation	14
2.6 Location-Based Evidence and Physical Meeting Correlation	16
2.7 Timeline Reconstruction and Event Correlation	17
2.8 Evidence Correlation and Findings	17
2.9 Conclusion	18

Introduction

Digital forensics is a distinct aspect of cybersecurity that entails the process of identifying, acquiring, preserving, and analysing digital evidence. The use of digital technologies and connected systems has necessitated the application of this field for cybercrime investigations and other related cases.

The contemporary form of digital forensics includes not only the computers but also mobile phones, cloud computing and networks, which makes the task more challenging [1]. This area is associated with cybersecurity in the sense that digital forensics provides organizations with the opportunity to analyse attacks, threats and implement appropriate security solutions [2].

The current report comprises two tasks – theoretical and practical. Task 1 highlights the current issues in the realm of digital forensics, tools, challenges, job opportunities and other related issues. Task 2 describes the practical side of digital forensics through an analysis of Cellebrite UFED and Cellebrite Physical Analyzer.

Task 1 – Research Report

Current state of digital forensics and its tools

Introduction Digital forensic is defined as the science of finding, gathering, maintaining and analysing electronic evidence in a legal and valid way. This area, which started in the 1970s as computer forensics focusing mostly on mainframes and PCs, developed into a multidisciplinary field including cloud, mobile, Internet of things (IoT), drone and car forensics. Cyber-crime nowadays consists of phishing, ransomware, investment scams, supply chain attacks and IoT threats [1]; thus, investigations tend to cover complicated distributed networks involving multiple devices and different legal jurisdictions. In order for digital evidence to be accepted in court, it must be gathered and maintained within a valid chain of custody [4]; all steps from seizure to examination must be recorded meticulously.

Phases of the investigation the procedure follows a series of phases, starting with identifying potential evidence; the second phase involves acquiring digital evidence through bit stream imaging; followed by the third phase where file systems, artefacts and memory are examined. Analysis is conducted with the objective of understanding what has occurred and identifying the party responsible for it; finally, results are presented in reports [4]. Documentation of steps taken and cryptographic hash validation are vital for each of the steps [4]. Maintaining volatile memory and preventing contamination of the original media are crucial steps in the process. According to the NIST mobile device forensics guidelines, it is important to keep the device isolated in Faraday bags or another form of isolation, make a note of its status, gather its identifiers and validate integrity through hash calculations [4].

Variety of devices to be investigated the number of devices to be investigated has diversified. Traditional computers, including desktop, laptops and server, are supplemented by smartphones, tablets, wearables, smart home appliances, autonomous vehicle and drones. In addition, data may need to be retrieved not only from physical devices but also from cloud services and social media platforms. As per Belkasoft's 2025 DFIR trends report, digital investigations usually involve data from drones, cars and mobile devices. It is also noted that the vast amount of data stored on smartphones ranging from call logs and calendar entries to encrypted messaging applications makes them indispensable in almost any investigation [2]. On the other hand, Belkasoft report underlines that the security measures employed by modern phones make it more challenging to extract information from them [2].

Tools The digital forensics tools available for investigators cover imaging, acquisition, analysis, memory capture, network analysis and link analysis. Both commercial and open-source software products provide these features, and some solutions integrate imaging, memory capture and remote acquisition in order to gather evidence not only from physical devices but also from virtual machines, cloud services, vehicles and drones. Nowadays, the analysis platform is expected to use artificial intelligence to work with the vast amounts of data performing various pattern recognitions, media categorisation and natural language processing, identifying anomalies and extracting key terms from chat conversations [2]. Remote acquisition became an important part of modern investigations since it is quite common that evidence is located in the cloud services; for this purpose, there are specialized cloud forensics solutions that mimic client applications and download users' information from cloud-based platforms like social media services.

Intersection of digital forensics and cybersecurity

Forensic investigation is closely linked with cybersecurity. When cybersecurity personnel work towards detecting and preventing attacks, forensic experts analyse breaches in order to discover how they took place and which information was stolen during the attack. The logs of intrusion detection systems, endpoint detection and response and SIEM solutions provide the basis for the forensic process, and its outcomes are used to improve the detection algorithms. For evidence to be considered valid and presented in court, there needs to be an unbroken chain of custody [4]. The forensic process helps in identifying iOS based on analysis of artifacts left by previous attacks, which can be used to detect anomalies in real-time. Moreover, such information can be integrated into DFaaS platforms. Cooperation between authorities and private companies will depend upon having the same data format and secure means of communication.

Emerging trends in digital forensics

The digital forensics environment is changing quickly due to numerous technology trends. Below are some examples of trends that transform the process of evidence collection and analysis:

1. **Artificial intelligence and machine learning:** AI and machine learning revolutionise digital forensics due to the possibility to automate the analysis of repetitive and labour-intensive processes along with discovering patterns in logs, media and natural language [2]. Large language models (like an offline BelkaGPT used in Belkasoft X) use case-specific data to answer questions, detect tone of emotionality and analyse metadata [2]. However, despite significant improvements, AI-based digital forensics require human involvement.
2. **Cloud forensics and remote investigation:** The growing number of cloud services creates numerous challenges, including jurisdiction issues, fragmented data stored on several servers, complex data formats and strong encryption [2]. It is important to mention that data stored in a foreign data center can be protected by the legislation of this country, thus making it inaccessible. Fortunately, there are cloud forensics tools that simulate application clients and allow users to collect and decrypt data by sending proper credentials [2].
3. **Forensic investigations of drones, cars, mobile devices and other IoT equipment:** Nowadays, modern forensics should not ignore information obtained from drones, automobiles and mobile devices such as smartphones or smart watches [2]. Drones register the route, geolocation data and videos. Cars can contain infotainment systems and GPS information, and the list of possible data in mobile phones includes call logs, SMS messages, applications' databases and geolocation history [2]. Advanced encryption and secure architecture of modern phones add extra complexity to investigations of these devices requiring additional techniques of logical, file system, physical and even cloud extractions and sometimes brute force unlocking [2].
4. **Anti forensics measures:** Modern cyber criminals apply various ways to erase, obfuscate and fake evidence. The most widespread techniques of hiding evidence include encryption, steganography and data erasure [2]. Therefore, the process of investigation involves special measures such as analysing metadata, using powerful recovery tools and applying counter steganography tools. Special tools such as Belkasoft X support tamper detection and deep analysis of databases, including SQLite databases [2].

5. **Automation in digital forensics:** There is too much evidence for a digital investigator to examine manually, so automation tools are vital for efficient forensics work. Using automation, it is possible to create templates and run lengthy tasks in background mode, apply standards and even distribute tasks among different devices [2]. The description of how Belkasoft X implements automation shows that the process involves calculating hashes, carving files and detecting specific strings or images using YARA/Sigma rules and artificial intelligence [2].
6. **Professional development and education:** DFIR industry suffers from the lack of professional investigators. Belkasoft states that there are not enough training programs allowing companies to train specialists [2]. To solve this problem, some providers and educational institutions develop specialized training programs focusing on acquisition, investigation and documentation of results [2]. This approach is important since it allows staying abreast of new legal regulations and changes in technologies. Moreover, there are official statistics stating that 8% of cyber sector enterprises have digital forensics specialists and 22% see the skills gap in this field [3].

Key challenges

As digital forensics involves a range of devices and services, there are some significant issues which may jeopardize its effectiveness. Firstly, mobile device forensics poses special challenges due to the complex nature of the devices' structure and operation. Belkasoft mentions that smartphones possess substantial amounts of evidence, including call logs, messages, application content, and location history, but have highly developed security features, namely, encryption and secure enclave technology [2]. Hence, the forensic specialist will have to combine logical, file system, physical, and cloud acquisitions in order to access encrypted devices using brute force unlocking. Moreover, the investigator will have to learn about various hardware updates and changes in software regularly. Other issues which can be identified as pressing include:

Data volume and heterogeneity:

Modern investigations may involve terabytes of data which come from emails, messages, cloud storages, network logs, social media accounts, and other Internet of Things (IoT) devices. With the proliferation of IoT devices, the amount of evidence collected during each examination becomes larger and more diverse. According to Soni, by 2030 there might be up to 29 billion IoT devices [1]. The processing of large datasets requires DFaaS solutions as well as validation of AI based instruments to eliminate false positives. The huge amount of data on one's smartphone also makes it difficult for an investigator to prioritize relevant artefacts and apply automation techniques.

Strong encryption and secure devices:

Strong encryption and sophisticated security procedures are used to ensure the user's privacy but hamper digital forensics efforts. Belkasoft states that increased security on mobile devices which includes full disk encryption, secure enclaves, and biometric locking complicates extraction of evidence[2]. An investigator will have to know different encryption standards in different operating systems, select an adequate acquisition method, and even try to unlock the device using brute force methods in a safe environment. It may lead to legal issues related to the right for compulsory decryption.

Anti forensic actions and tampering:

Criminals actively hide their traces by encrypting information, wiping it off the storage, changing timestamps or hiding it in other documents. Belkasoft's annual report shows that cybercriminals encrypt, perform steganographic transformations, and erase data from hard drives, which requires additional measures, including metadata analysis, deep recovery technologies, and counter steganography techniques [2]. Therefore, any forensic software must feature tools aimed at detection of altered or erased evidence.

Cloud and IoT complications:

Evidence is distributed across various remote storages and IoT devices, which makes it complicated to extract it for investigation. Laws regarding cross border data make delays possible, and data may be fragmented across numerous servers [2]. Cloud forensic technologies require simulating applications and using valid usernames and passwords [2]. As Soni notices, IoT devices present great opportunities as well as great risks for digital forensics specialists, thus requiring standardization of the procedure and protection of users' privacy [1].

Legal and ethical issues:

Digital forensics specialists must balance the collection of evidence with the protection of users' privacy which is guaranteed by such laws as the GDPR. Also, access to data stored in cloud servers cannot be guaranteed, but there are mutual legal assistance treaties between countries [5]. In addition, the Digital Evidence Chain of Custody framework emphasizes the importance of authenticity and documentation during the procedure [5].

Chain of custody integrity:

Digital evidence is extremely fragile because its originality should always be verified. According to NIST recommendations, cryptographic hashes of the acquired media must be calculated, and then they must be recalculated repeatedly through the analysis process [4]. Each time media was transferred, this fact had to be recorded, and proper storing should prevent any tampering. Keeping an uninterrupted chain of custody is crucial for making sure that evidence will pass judicial evaluation [5]. Automated acquisitions should also involve procedures of maintaining an adequate chain of custody and recalculating cryptographic hashes.

Skills shortage and continuous training:

Digital Forensics and Incident Response specialists need to possess a range of skills, including legal knowledge, computer science, network management, and cryptography. The shortage of skilled employees is recognized by Belkasoft, and inadequate training options create difficulties for organizations in tracking the development of technology and anti-forensic tactics. This problem can be overcome by specialized vendor and university courses [2]. The UK government's Cyber Security Skills in the UK Labour Market 2025 report confirms a deficiency in DFIR specialists, showing that only 8 % of cyber sector businesses have people in this position, and 22 % find a lack of technical skills in digital forensics [3].

AI's imperfections and supervision:

Despite the advantages, AI technologies and large language models are not completely flawless. As Belkasoft states, accuracy depends on the quality of data on which the model is built [2]. Therefore, it should be checked against original artifacts to avoid mistakes. Oversight of AI algorithms is also required since any automated decision made without proper supervision can negatively affect the rights of a suspect under examination.

National and international job market

There is a very high need for digital forensics experts. As revealed in the United Kingdom Government's "Cyber Security Skills in the UK Labour Market 2025," only 8 % of companies in the cyber sector employ experts who have experience in digital forensics. However, about 22 % of the same companies identify digital forensics as a skills gap [3]. The above statistics indicate that the number of digital forensics experts available in the labour market is insufficient to meet the needs of employers. Globally, the digital forensics market is expected to grow at a double-digit rate owing to the rise in the prevalence of cybercrimes, regulations, and the growing use of digital devices.

Task 2 – Digital Forensics Investigation Report

2.1 Introduction

Below is described a well-organised digital forensic examination carried out on a number of mobile devices via industry standard forensic software. The purpose of this forensic examination is to collect and analyse the digital evidence to determine communication patterns and any sort of coordination among the involved people.

1. Emma's Android smartphone - including WhatsApp, Instagram direct messages, emails and call history.
2. Emma's USB flash drive - comprising all the documents about the patent and possibly other files.
3. Joe's mobile device – including messaging logs between Joe, Emma and other people.
4. Norman's mobile phone - being a mobile device of the Research and Development Director from NexGen Circuits Company, and it includes communications between Norman and Joe.

The digital forensic investigation was carried out systematically with an approach comprising data acquisition, hashing, data correlation and artefacts analysis. Cellebrite UFED software was used for the data acquisition and Cellebrite Physical Analyzer for further examination.

2.2 Evidence Acquisition and Integrity Verification

The initial phase of the investigation involved the forensic acquisition of four digital devices. Each device was extracted individually to ensure adherence to forensic best practices and to maintain the integrity of the original data.

The extraction process was performed using Cellebrite UFED, which supports both logical and physical acquisition methods. Following extraction, cryptographic hash values (e.g., MD5 and SHA-1) were generated for each dataset. These hash values act as digital fingerprints, ensuring that the acquired data remains identical to the original source.

Hash verification was conducted immediately after extraction and again prior to analysis. The consistency of hash values confirmed that no modification or tampering occurred during the acquisition process. This step is critical in maintaining the chain of custody and ensuring that the evidence is admissible in legal proceedings.

2.3 Multi-Device Data Integration and Analysis

Post acquisition, each and every dataset was then imported into the Cellebrite Physical Analyzer for further analysis together. This process ensured that data from various devices could be analysed in one single place.

The benefits of using a centralized forensic analysis platform include the ability to:

- Mine correlations in communication artifacts between various devices
- Discover common contacts and relations between them
- Rebuild timelines of events
- Recognize patterns among various sources

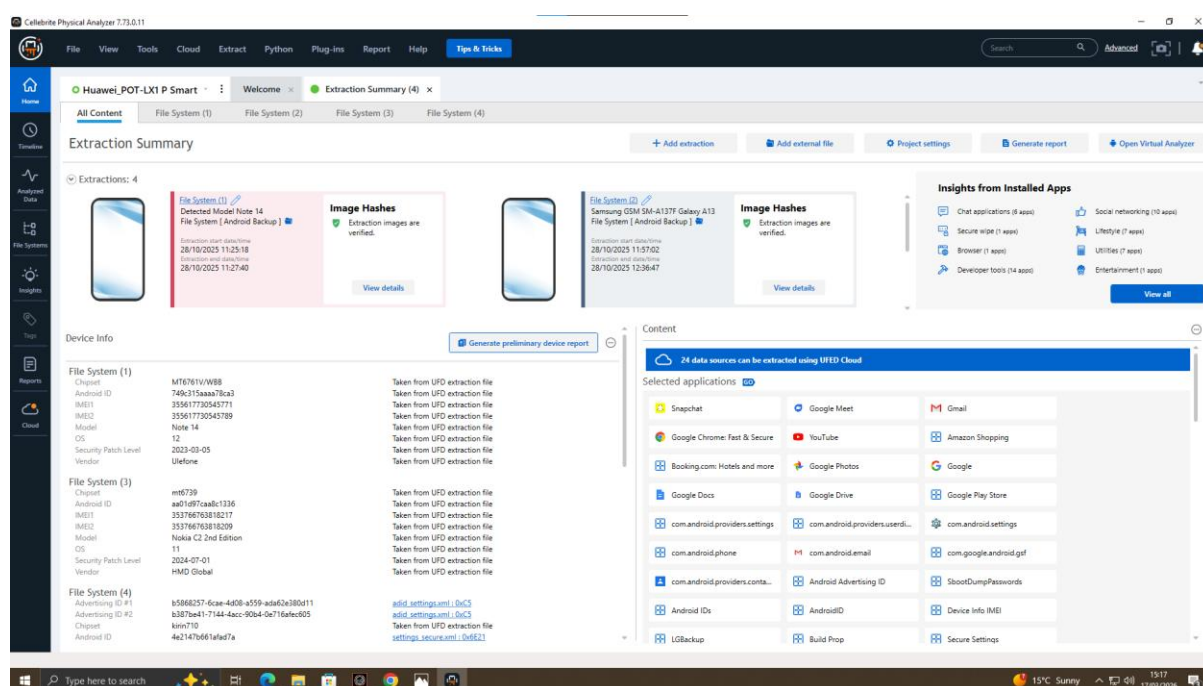


Figure 2: Multi-device data integration and analysis using Cellebrite Physical Analyzer

Evidence Figure 2 below shows that there are several datasets available on the Physical Analyzer, including chats, contacts, media and timeline. This helps in filtering, organizing, and conducting searches for evidences efficiently and effectively.

This is important in today's investigations since the suspects tend to utilize multiple devices and mediums to organize their plans.

2.4 Communication Analysis and Suspicious Conversations

The analysis of the information obtained from the chats showed multiple conversations between various people indicating coordination of actions. The chats consist of a pattern that implies that they are communicating something to each other.

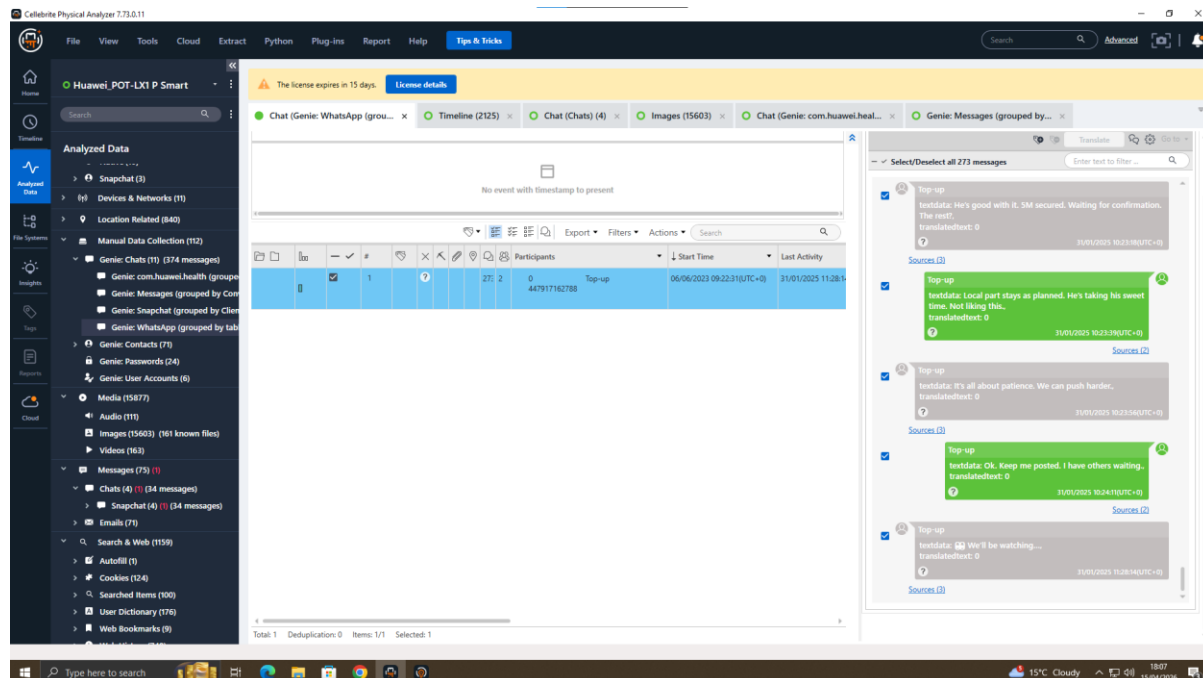


Figure 3: Extracted chat communication displaying interaction between users

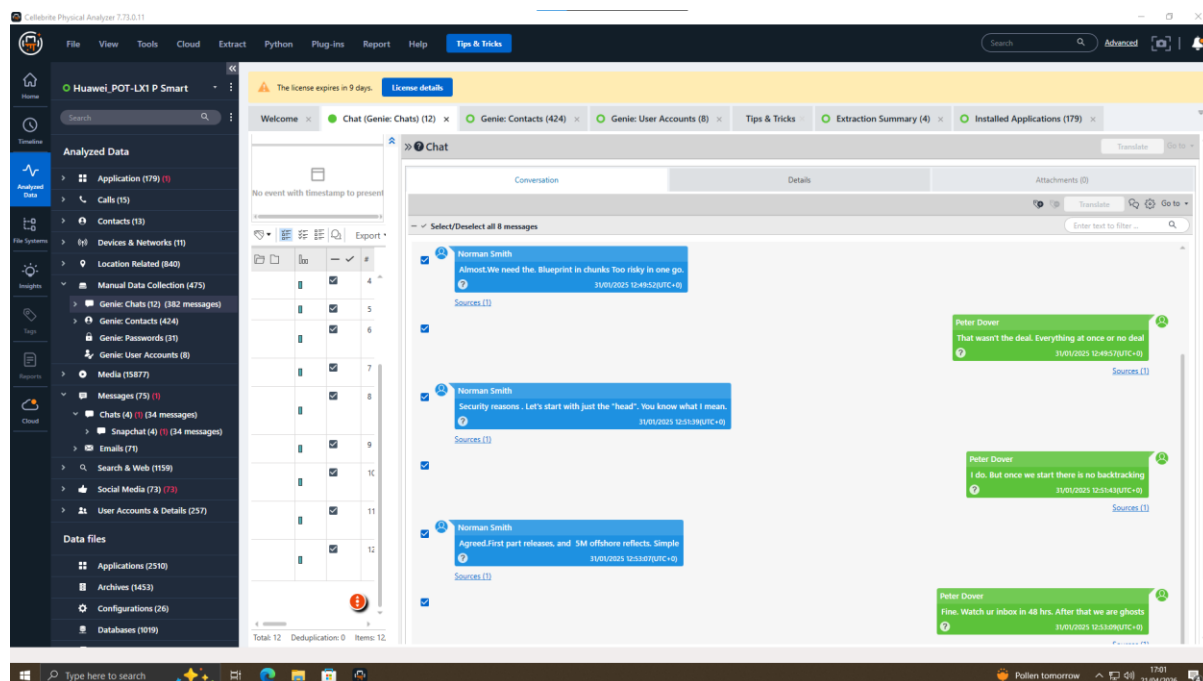


Figure 4: Chat messages indicating potential coordinated activity, including negotiation-related language

From the Evidence Figure 3 and 4, we can see that the following information was obtained:

1. Repeated communication between specific individuals
2. Use of informal yet contextually meaningful language
3. Sequential message patterns indicating active coordination
4. References to external actions and decision-making

One notable conversation includes statements such as:

- *"I may go with someone if u r not interested"*
- *"Any update on the offers?"*
- *"It's disappointing that no response from u"*

These messages suggest negotiation behaviour and indicate the presence of alternative options, which is often associated with transactional discussions.

Further messages such as:

- *"He's good with it. 5M secured. Waiting for confirmation."*
- *"Local part stays as planned."*
- *"We'll be watching..."*

provide stronger indicators of coordinated activity, possibly involving financial or operational arrangements.

These communication artefacts are significant as they demonstrate:

- Intent
- Coordination
- Ongoing interaction between parties

Such evidence is critical in digital forensic investigations as it establishes a behavioural link between individuals.

2.5 Contact Analysis and Identity Obfuscation

The forensic analysis of the contact information has found numerous contacts with identical or similar names but tied to various identifiers (such as phone numbers or usernames). Such a trend is characteristic of several electronic gadgets.

Such conduct indicates the employment of identity concealment practices, which involves the deliberate creation or use of multiple identities.

It became possible to cross-link the contacts due to the capabilities of the analysis environment.

2.6 Location-Based Evidence and Physical Meeting Correlation

Location-related artefacts extracted from the devices provided additional context to the investigation. The data includes references to meeting arrangements and geographical locations.

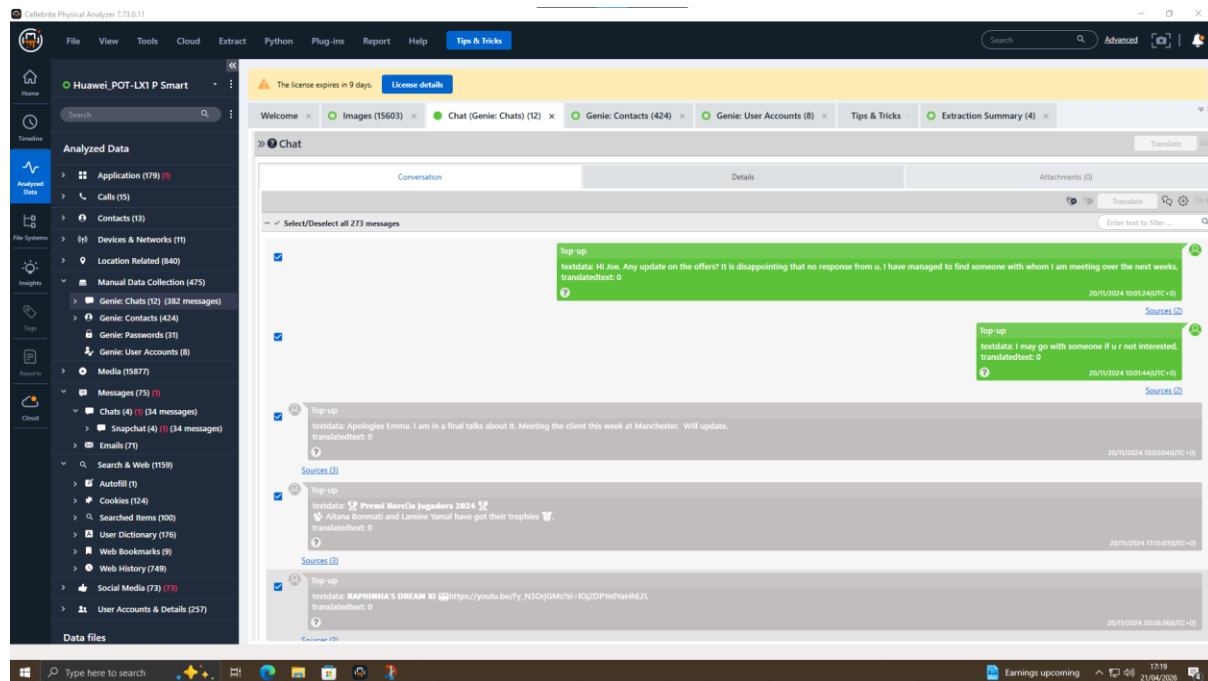


Figure 6: Extracted message content referencing a planned meeting in Manchester

According to Evidence Figure 6, one particular message shows:

"Meeting the client this week in Manchester."

Mentioning of Manchester shows the presence of planning of a physical meeting, which is linked with the digital conversation.

Timestamp, messages, and location analysis imply:

- Physical meetings were planned via digital communication
- Suitable locations were chosen to conduct the meetings
- Co-relation of conversations and actions were present

The location evidence is an essential aspect in forensic investigation because it helps validate the incidents at specific places.

2.7 Timeline Reconstruction and Event Correlation

It was possible to develop a timeline thanks to the availability of the information about communications, contacts and location. It was possible to reconstruct the timeline based on the examination of the time stamps related to the messages sent and actions performed.

The findings of the timeline analysis include:

- Persistent communication during a certain timeframe
- The development of conversations which resulted in decisions made
- Convening a meeting after virtual communication

Cellebrite Physical Analyzer can display a timeline of events for investigators to make it possible to link events from different data sources.

The timeline analysis demonstrates that there were some organized activities of the parties rather than separate actions.

2.8 Evidence Correlation and Findings

Consequently, a combination of analysis of the items serves as a holistic evidence base. The conclusions reached by this study can be outlined as follows:

Evidence Intact

- All the data sets have been collected and authenticated through hash values.

Collaborated Communication

- A pattern of coordinated messages has been established from the chat analysis.

Identity Concealment

- The duplicates of contacts show attempts at identity concealment.

Physical Connection to Communication

- The evidence gathered from location data proves a physical connection in Manchester.

Timeline Integrity

- The events' timeline remains intact throughout the process.

2.9 Conclusion

A thorough investigation into the matter using digital forensics was successful in showing how systematic and evidence-based techniques can be used for the examination of multi-device data sets.

Through the use of the Cellebrite system, a number of significant artifacts were revealed to show that there was indeed a level of coordination involved on the part of the people investigated.

In light of this, it can be said that these people were coordinating their efforts, as evidenced by both digital communication and arranged meetings.

References

- [1] N. Soni, "Digital Forensics: Confronting Modern Cyber Crimes, Technological Advancements, and Future Challenges," vol. 5, no. 3, 2025,
- [2] R. T. Belkasoft. "Navigating the Future: Top 6 Trends Shaping Modern DFIR in 2025." [Online]. Available: <https://belkasoft.com>
- [3] Department for Science, Innovation and Technology (DSIT), "Cyber Security Skills in the UK Labour Market 2025," London. 2026.
- [4] R. Ayers, S. Brothers and W. Jansen, "Guidelines on Mobile Device Forensics," NIST Special Publication 800-101 Rev.1, Gaithersburg, MD. 2014.
- [5] S. Nath, et al., "Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics", pp. 1–8.