

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:

Rishabh Choudhary

Student ID:

[2434332]

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

This report considers the issue of digital forensics through a thorough examination and discussion of theoretical approaches and practical investigation results. First of all, the review of current trends in digital forensics provides insight into the issues of existing tools, their application, future trends, and even labour market needs. Then, a practical investigation related to corporate espionage carried out against company Quantum Tech has been conducted. Digital data on several devices have been gathered and examined with the help of such tools as Cellebrite UFED and Cellebrite Physical Analyzer.

Contents

Introduction	4
1. Digital Forensics: State of the Field and Analysis	5
1.1 Current state of digital forensics	5
1.2 Forensic process and tools	5
1.3 Intersection of Digital Forensics and Cybersecurity	7
1.4 Emerging Trends in Digital Forensics	8
1.4.1 Artificial Intelligence and Machine Learning	8
1.4.2 Cloud Forensics and Digital Forensics as a Service (DFaaS)	8
1.4.3 Mobile, IoT, and Vehicle Forensics	9
1.4.4 Automation and Real-time Collaboration	9
1.4.5 Anti-forensics and Encryption	9
1.4.6 Blockchain Forensics and Deepfake Detection	10
1.4.7 Professional Training and Conferences	10
1.5 Key Challenges	10
1.6 National and International Job Market	11
1.6.1 United Kingdom	11
1.6.2 United States and Global Perspective	11
1.7 Conclusion	13
2. DIGITAL FORENSIC INVESTIGATION REPORT	14
2.1 Case Background	14
2.2 Evidence Inventory and Chain of Custody	14
2.3 Methodology	15
2.4 Evidence Acquisition	15
2.4.1 Verification of Evidence	17
2.4.2 Evidence Analysis	17
2.5 Evidence Inventory	17
2.5.1 Analysis of Communication Logs	18
2.5.2 Contact Analysis	19
2.5.3 Real-World Coordination	20
2.5.4 Timeline Reconstruction	21
2.5.5 File Analysis	22
2.5.6 Call Log and Email Analysis	22
2.5.7 Location Data Analysis	22
2.6 Evidence Correlation	23
2.7 Conclusion	25

Introduction

Digital forensics has become an essential branch of modern cybersecurity due to the increasing complexity and size of cyber threats. This process comprises a set of activities aimed at identifying, collecting, analysing, and presenting digital evidence in order to recreate what happened and make informed decisions based on this data [1]. Due to the ongoing expansion of the digital realm into the cloud, mobile phones, and other interconnected environments, digital forensics has become an integral part of cyber incident response and analysis procedures [2].

The present report encompasses both theoretical and practical aspects of digital forensics. On the one hand, the report analyses the existing state of digital forensics with a focus on the available tools, techniques, emerging trends, challenges, and employment prospects. On the other hand, the report illustrates the application of theoretical knowledge about digital forensics through a practical exercise concerning a potential case of corporate espionage in Quantum Tech. During the analysis of this scenario, this investigation uses industry-leading tools, such as Cellebrite UFED and Cellebrite Physical Analyzer.

1. Digital Forensics: State of the Field and Analysis

Digital forensics often referred to as cyber forensics involves systematic acquisition, collection, examination and presentation of electronic evidence collected from different digital sources (computers, mobile devices, networks, internet of things devices, cloud computing services, surveillance systems, and so forth). Unlike traditional cybersecurity which emphasizes the role of preventive risk management, digital forensics is a reactive field which seeks to reconstruct what happened, how and by whom [2].

1.1 Current state of digital forensics

Historical background

The history of digital forensics goes back to the period of the late 1970s when personal computers began to gain popularity among users. The criminalization of any unauthorized manipulation of computer data with the adoption of Florida's Computer Crimes Act in 1978 marked the emergence of early digital forensics [1]. Specialized police departments (such as the creation of the FBI's Computer Analysis and Response Team in 1984 and of the Fraud Squad computer crimes unit in the UK in 1985) also contributed greatly to early digital forensics [1]. The 1990s saw a move towards standardization (such as the establishment of the International Organization on Computer Evidence in 1995) which broadened the area beyond computers [1]. In the 2000s, specialized computer forensics laboratories and the Scientific Working Group on Digital Evidence (SWGDE) provided detailed guidelines [1]. Meanwhile, with the rise of cloud computing and mobile devices, the term "digital forensics" gained popularity over the past decade as the field has been expanded considerably [1].

It is evident that despite a great deal of development in the process of digital forensics, due to the high level of complexity of digital systems and environments, efficiency can be a challenge. Therefore, it seems necessary to introduce new solutions to ensure efficiency.

1.2 Forensic process and tools

The process of digital forensics includes several repetitive phases: identification of evidence; acquisition of information using such devices as write blockers and forensic duplicators; further preservation via the use of cryptographic hash functions; and finally – data analysis using special software applications [3]. These are classified into two major groups: hardware and software tools. The most common software used in digital forensics include:

Tool	Features and capabilities	Evidence sources
Cellebrite	Industry-leading mobile forensics suite; supports diverse devices; provides Universal Forensic Extraction Device, Physical Analyzer and Inspector modules; includes AI-based enhancements and a cloud version that improves collaboration [4].	Mobile devices and cloud data
Magnet Axiom	Comprehensive suite for computer, mobile, cloud and vehicle forensics; automation and simple UI; community “Artifact Exchange” for user-created artifacts; expanded support for Teams chats and ChatGPT logs [4].	Desktops, mobiles, cloud services, vehicles
Velociraptor	Open-source endpoint forensics utility; collects and stores event logs; uses its own query language; latest version adds Sigma rule editor and live-event sources; integrated into Rapid7’s managed detection and response platform [4].	Windows and Linux endpoints
Wireshark	Long-standing network analysis tool; captures and inspects packets on wired and wireless networks to identify traffic types, sources and destinations [4].	Network traffic
X-Ways Forensics	Advanced disk analysis tool for manual investigations; details drive contents, slack and inter-partition space; suits resource-constrained hardware; requires specialist training [4].	Hard drives

Autopsy / Sleuth Kit	Free, open-source suite built on Sleuth Kit; provides GUI for case management and analysis of hard drives, mobiles and cloud data; modular with extensions (e.g., email parsing or malware) [4].	Disks, mobiles, cloud
Oxygen Forensic Detective	Focused on mobile acquisition; extracts and analyses data from iOS/Android devices, cloud services, messaging platforms, drones and IoT devices [4].	Mobile and IoT devices
EnCase Forensic (OpenText)	Long-standing digital forensics suite widely accepted by courts; acquires and analyzes data from desktops, servers, mobiles and cloud; emphasises evidential integrity [4].	Multiple platforms
Forensic Explorer (FEX)	Lower-cost alternative; supports file system analysis, deleted file recovery and keyword search; automates repetitive tasks and integrates with imaging tools [4].	Windows systems

Other tools in use include data carving and timeline analysis tools such as FTK and Plaso. Digital forensic techniques include: file recovery, data carving, timeline analysis, live data forensics, steganography detection, cryptanalysis, network and database forensics. It is important to maintain a verifiable chain of custody through hashing and documentation. Beneficence, non-maleficence, integrity, and respect are the four principles of ethics in digital forensics [3].

While tools such as Cellebrite, Magnet Axiom, and Autopsy possess capabilities to perform comprehensive analysis, they are increasingly being challenged by encryption algorithms and anti-forensic techniques. This shows the need to continue developing tools and techniques such as artificial intelligence.

1.3 Intersection of Digital Forensics and Cybersecurity

As previously mentioned, cybersecurity and digital forensics share a common objective of protecting information and responding to security incidents, although

with different focuses. Whereas cybersecurity is preventive in nature, digital forensics is reactive as it involves reconstructing events after an incident has taken place [2]. Digital forensic investigators collect digital evidence from messaging logs, emails, social media and network traffic as part of criminal, civil, military and administrative investigations, while cybersecurity experts develop security architectures and manage operation centres [2].

As previously discussed, although the two disciplines differ in terms of focus, digital forensics plays an indispensable role in cybersecurity operations. During incident response, digital forensics helps investigators understand the root cause of the breach, assess its extent and pinpoint attackers through host artifacts, logs, and memory forensics [4]. Tools like Magnet Axiom and Cellebrite are commonly used together with intrusion detection systems to correlate digital evidence across multiple devices and networks [4]. Wireshark enables investigators to perform network forensics, which help pinpoint paths of data exfiltration [4]. Some of the cases that show the relevance of digital forensics in cyber investigations include the use of digital forensics to recover information from a floppy disk containing data that led to the apprehension of BTK serial killer, the investigation of surveillance footage, cell phone data, and social media records to identify perpetrators of the 2013 Boston Marathon bombing [3]. A major drug trafficking network was brought down in 2023 with the aid of mobile data analysis software provided by Cellebrite [3].

This illustrates the relationship between the two domains as digital forensics is now an essential aspect of cyber operations, without which it is impossible to conduct an effective response.

1.4 Emerging Trends in Digital Forensics

1.4.1 Artificial Intelligence and Machine Learning

The integration of AI in digital forensics has changed the game. Tools using machine learning are helping investigators automatically process massive volumes of digital evidence and extract valuable patterns from them in an efficient manner [5]. Industry experts note that AI allows forensic examiners to analyse digital evidence faster, spot relationships unnoticed by humans, and find indicators of compromise in digital evidence [5]. Belkasoft introduces its BelkaGPT assistant that processes massive volumes of text-heavy evidence such as SMS and emails offline while preserving privacy; it recognizes the context of discussion, emotions expressed, and metadata. Image and media files can be analysed with AI-based solutions to categorize explicit contents and weapons [6]. While the integration of AI brings benefits, the risk of bias and lack of transparency remains.

1.4.2 Cloud Forensics and Digital Forensics as a Service (DFaaS)

Cloud forensics requires tools that allow downloading digital evidence from cloud applications in a systematic manner. Specialized tools can emulate client applications that interact with cloud services via Application Program Interface (API) and help download digital evidence [6]. There are several tools offering cloud capabilities, including Magnet Axiom and Cellebrite. DFaaS offers investigations carried out in the cloud environment [1]. Belkasoft notes the issue of jurisdictional restrictions, evidence fragmentation and encryption as major obstacles in carrying out cloud forensics [6]. Current efforts aim at introducing legal framework harmonizing the management of digital evidence collected across borders [7].

1.4.3 Mobile, IoT, and Vehicle Forensics

The increasing number of connected devices is projected to reach 29 billion in 2030 [1]. Today digital forensic investigators should account for smartphones, smart watches, vehicles, drones and other connected devices [6]. Flight logs, infotainment system records, and navigation logs provide investigators with valuable evidence to establish timelines and travel patterns. However, connected devices feature strong encryption and advanced security features which make extraction more difficult [6]. Software packages like Cellebrite, Oxygen Forensic Detective, and Belkasoft X provide logical, file system, physical, and cloud extraction, as well as brute-force unlocking capabilities [6]. Free and open-source mobile forensic tools (ALEAPP, iLEAPP) are becoming popular [5].

1.4.4 Automation and Real-time Collaboration

Automating the process of digital forensics is crucial for processing massive amounts of data. Customizable analysis presets, unattended tasks execution, standardization of workflows, scalability of processes able to process images in terabytes overnight are some examples of innovations. This trend not only allows accelerating the process of investigation but reduces human errors. For example, automated detection of explicit images helped to accelerate the search of victims of child exploitation [6]. As per ArcPoint, there is a move towards collaboration, readiness, and real-time integration of threat intelligence feeds into incident response workflows [5].

1.4.5 Anti-forensics and Encryption

One of the trends seen in cybercrime is the use of anti-forensic techniques like encryption, steganography, and wiping to avoid detection by forensic tools. Metadata analysis, recovery of deleted and fragmented files, and anti-steganography capabilities help overcome this problem [6]. Cellebrite's suite has a number of features, including brute force unlocking of encrypted devices, recovery of SQLite

files etc. One of the emerging trends is quantum-resistant encryption, which may be overcome with quantum technologies in the future [7].

1.4.6 Blockchain Forensics and Deepfake Detection

The advent of cryptocurrency gave rise to blockchain forensics, which involves analysis of transaction graphs in order to trace money flows in illicit activities. Herald Open Access article mentions blockchain forensics and quantum computing as emerging frontiers in digital forensics [1]. Detecting deepfakes and preserving the authenticity of evidence is becoming a critical trend, with many of the forensic tools implementing artificial intelligence-based detection of manipulated evidence. One of the predicted trends is the emergence of AI-based attacks and deepfakes requiring creative solutions [1].

1.4.7 Professional Training and Conferences

There is a shortage of professionals specializing in digital forensics. Belkasoft points out the lack of professionals as one of the major obstacles and even provides educational courses addressing this challenge [6]. ArcPoint mentions several conferences, including National Cyber Crime Conference, IACIS Annual Training, and Techno Security & Digital Forensics Conference [5].

1.5 Key Challenges

Some of the main challenges that digital forensic investigators face include:

Data Volume and Variety: In today's investigations digital forensics specialists are dealing with enormous amounts of data stored across various devices and platforms. Connected devices and cloud-based applications produce vast volumes of heterogeneous data that needs to be investigated [1]. This problem can be addressed by automation and use of AI-based solutions, which come at the cost of investments [6].

Cloud Evidence and Jurisdiction: Digital forensics specialists are dealing with evidences spread across several jurisdictions, complicating the process of collection because of cross-jurisdiction restrictions, legal cooperation, and the need to comply with regulations such as GDPR [6], [7].

Encryption and Privacy: Encryption is critical in securing users' data, although making digital forensics harder. Finding balance between lawful access to information and privacy is difficult. The emergence of quantum computing may make breaking encryption possible, raising future ethical dilemmas [7].

Anti-forensics: Attackers employ wiping, steganography, metadata alteration and other techniques to conceal evidence [6].

Legal and Ethical Considerations: Ensuring the chain of custody and preserving privacy is the core of digital forensics [3]. In addition to maintaining ethical principles

of integrity, objectivity and respect to privacy, digital forensics specialists should adhere to emerging global guidelines [7]. Misinterpretation of the term "deleted" may jeopardize the case [3].

Skills shortage and training gaps: Fast-paced innovation makes the demand for highly-trained specialists ever-growing. Recruiters struggle with finding qualified employees, and it takes additional effort to retain talented specialists. According to the 2025 ISC² Cybersecurity Workforce Study, while the labour market situation has stabilized, there are still critical skills gaps in areas of incident response and security engineering [8].

These challenges are not only technical; legal and ethical considerations are increasingly becoming an integral part of digital forensics operations.

1.6 National and International Job Market

1.6.1 United Kingdom

The 2025 Cyber Security Skills in the UK Labour Market Report published by the UK Government analyses monthly job listings on popular sites and finds that while facing economic hardships, cyber security skills are in demand in the UK labour market. In 2024, there were 2,698 monthly job listings for core cyber jobs, and 2,399 listings for cyber-enabled positions [9]. The median salary for a core cyber position was £55,000 or 12% higher compared to the rest of the IT labour market [9]. The top five cities offering core cyber jobs were London, Manchester, Bristol, Birmingham and Leeds [9]. The remote work became more prevalent accounting for 26% of all job listings [9]. However, compared to previous years, the number of job postings decreased by 33% in 2024 due to decline in the digital industry [9]. Moreover, the wage premium fell from 25% to 12% [9]. Recruiting agents note that high-quality candidates are readily available [9].

For pursuing a career in digital forensics, graduates usually have degrees in computer science or cybersecurity, and specialized certifications [2]. According to Marshall University, career options include digital forensic examiner, incident responder, malware analyst, and network forensic specialist. Cyberese estimates the number of cyber security job openings in the US as exceeding 400,000 [2].

Certification options include: Certified Forensic Computer Examiner (CFCE), Certified Computer Examiner (CCE), and GIAC Certified Forensic Analyst (GCFA). Despite the decline in postings in 2024, the overall trend shows sustained demand for digital forensics professionals.

1.6.2 United States and Global Perspective

The Bureau of Labor Statistics includes computer forensics examiners among information security analysts. The Bureau expects a 29% increase in employment of computer forensics examiners between 2024 and 2034, or creation of about 52,100

new positions – far beyond the national average for all occupations [10]. Computer forensics examiners work alongside law enforcement agencies and private companies investigating digital data breaches. They help recover lost or deleted information and investigate malware; they also assist with preparing evidence in court cases [10]. According to BLS estimates, in 2024, the mean annual salary for information security analysts was \$127,730 (\$124,910 at the 50th percentile and \$186,000 at the 90th percentile [10]). Global job outlook is expected to be equally bright, judging by the projections of the digital forensics market size.

According to the findings of the 2025 ISC² Cybersecurity Workforce Study surveying over 16,000 people worldwide, economic uncertainty has led to slower hiring rates, yet skills shortage is the main concern among employers. AI-based technologies are disrupting the profession; however, the majority of employees are optimistic about career prospects [8]. Employers are trying to increase the skill set of existing employees and are less focused on recruitment [8].

1.7 Conclusion

Modern digital forensics has come a long way from the early practices in the 1970s. Currently, investigators use specialized software packages like Cellebrite, Magnet Axiom, EnCase and free alternatives to analyse diverse types of digital evidence produced by modern devices and cloud applications [4]. Innovations like AI, automation, and cloud computing are driving progress in digital forensics by helping process massive amounts of data, detect patterns and collaborate in real time [5][6]. New directions like blockchain forensics, deepfake detection, and quantum computing promise to provide new opportunities but also pose ethical and legal challenges [1], [7]. Challenges faced by investigators include data volumes, encryption and jurisdictional barriers, anti-forensics, privacy, and skill shortages [6]. Nonetheless, digital forensics is a cornerstone of modern cyber security operations, and it is essential for law enforcement investigations. With proper standards and training, and investment in innovative technologies, digital forensics will continue being relevant in the digital era.

Building on the theoretical understanding of digital forensics, the following section applies these principles in a practical investigation scenario involving suspected corporate espionage.

2. DIGITAL FORENSIC INVESTIGATION REPORT

2.1 Case Background

The Quantum Tech Organisation is a premier entity involved in semiconductor development. The company reported an apparent instance of corporate espionage, in which there was an illegal access to the firm's exclusive patent database. The affected intellectual property, QT-AI-2025, is an essential AI chip design necessary for the competitiveness of the company.

According to preliminary investigations, Emma, a senior engineer recently employed at Quantum Tech, was named as the first suspect. Emma reportedly tried to obtain and share confidential information illegally with another competitor, NexGen Circuits, via an intermediary called Joe. There were also allegations that Norman, likely acting on behalf of the buying party, was also involved.

In response, law enforcement officers confiscated different digital devices from the suspects under forensic supervision. Specifically, the confiscated devices include Emma's Android phone and USB drive, Joe's phone, and Norman's Android phone. The aim of this forensic investigation is to establish whether there was any illegal access to the confidential information and intent to distribute it among others.

2.2 Evidence Inventory and Chain of Custody

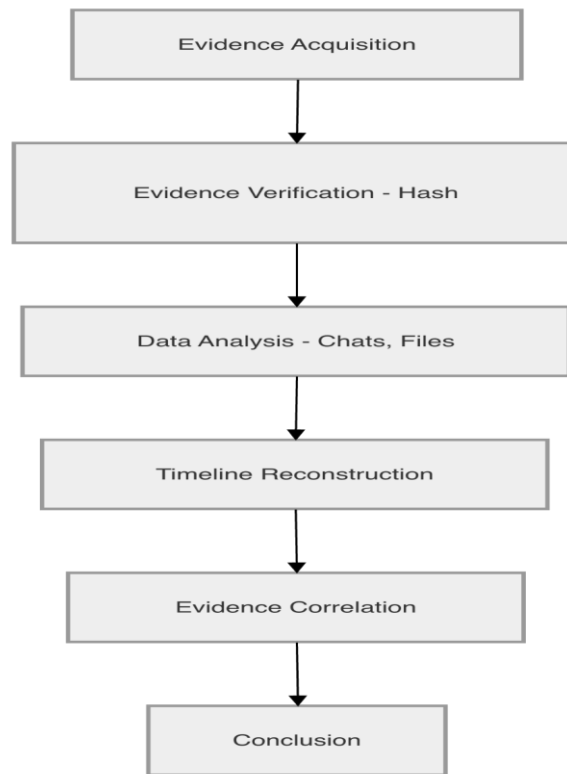
These sources of digital evidence were included in the investigation:

- Emma's Android Smartphone
- Emma's USB Flash Drive
- Joe's Smartphone
- Norman's Android Smartphone

Procedures in digital forensics were adhered to when collecting these sources. After their seizures, all of them were labelled, identified and accounted for. Documentation of the chain of custody was kept through the process from collection to analysis.

A laboratory was used as the location for image acquisition using industry standard software. Hashes MD5 and SHA-1 were generated at the time of acquisition and then again during the analysis to verify data integrity. Identical hashes indicate that there was no alteration or change made to the evidence.

2.3 Methodology



2.4 Evidence Acquisition

Digital evidence acquisition was done with the use of Cellebrite UFED, which is one of the industry standards for mobile forensics. Logical acquisition methods were employed on all the phones to extract structured data such as phone logs, application data, and metadata.

The USB stick used by Emma was imaged using the bit-by-bit method, which creates an exact copy of the source data storage device. The acquisition process followed proper forensics protocols such as secure storage areas.

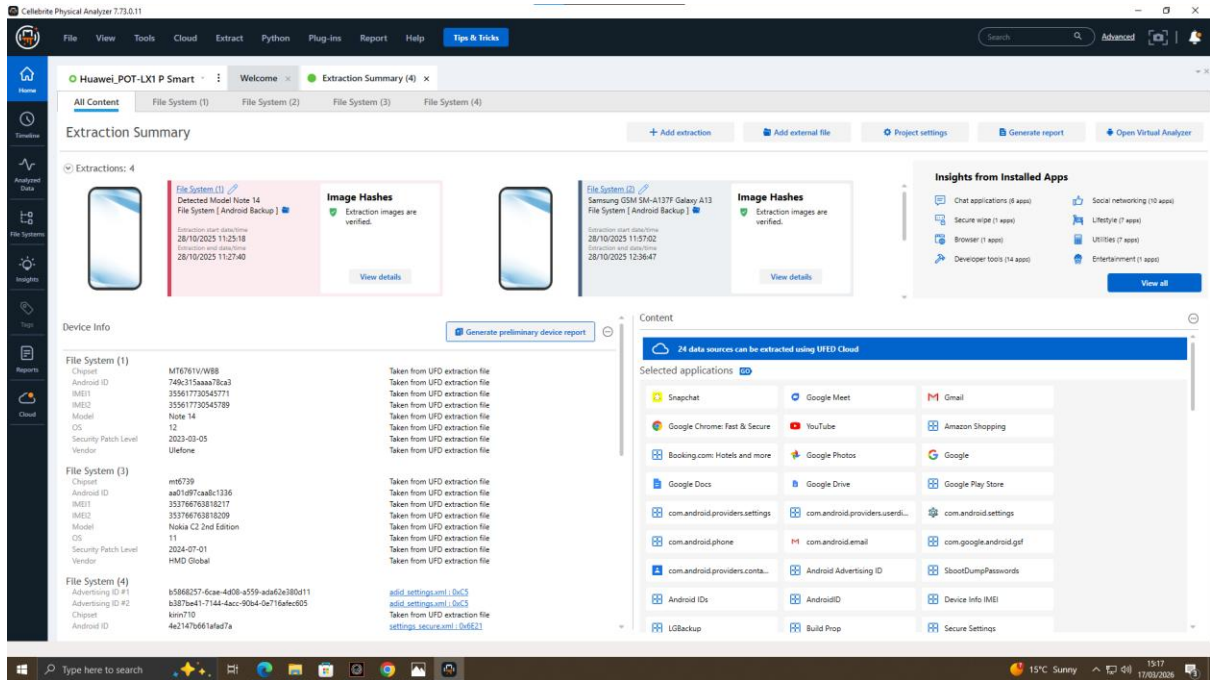


Figure 1: Forensic extraction summary

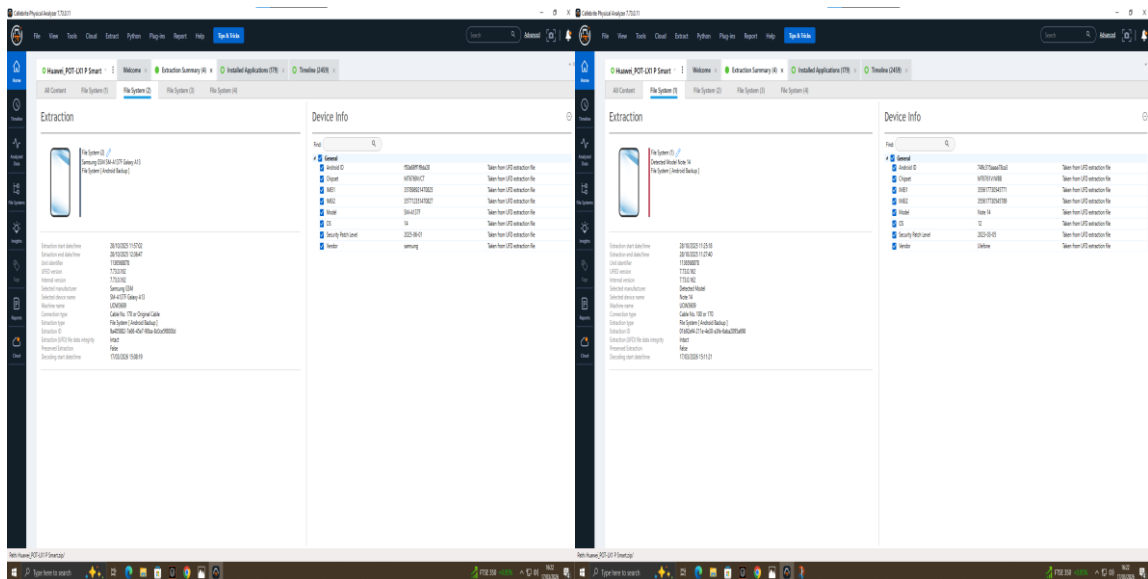


Figure 2: Forensic extraction summary of different devices

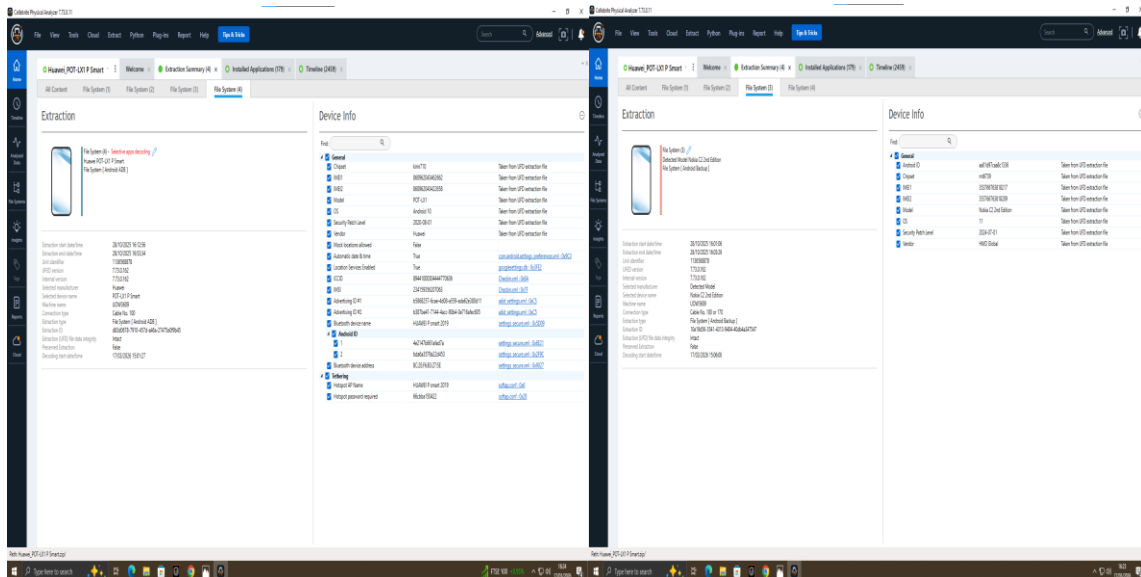


Figure 3: Forensic extraction summary showing multiple devices analysed and hash verification.

2.4.1 Verification of Evidence

After the acquisition phase, cryptographic hash codes (MD5 and SHA-1) were computed and matched with those of the original images. Consistency of the hash values ensures the integrity of the evidence and provides a basis for its admissibility in court.

2.4.2 Evidence Analysis

Evidence analysis was performed using Cellebrite Physical Analyzer, allowing all devices to be analyzed together within a common forensic investigation. This allowed for correlations to be drawn between devices, and helped in establishing relations within the collected evidence.

Key elements included:

- Communication logs (WhatsApp, instant messenger applications, emails)
- Contact information and identities
- File systems
- Time line analysis
- Location evidence

2.5 Evidence Inventory

2.5.1 Analysis of Communication Logs

The review of the communication log showed organized and periodic communications among the involved parties indicating concerted efforts. As shown in figure 4 & 5, there are several conversations showing negotiations of financial transactions.

Key messages found during communication analysis include:

- "5M secured. Still waiting for confirmation."
- "Keep me updated. I have others interested."
- "The local bit will stay as planned."

These communications indicate that there is a clear motive for money from a negotiated transaction of a trade. From the inclusion of financial aspects in the communication, it can be seen that the data under discussion had some commercial value.

Analysis further shows negotiation patterns:

- "Any update on offers?"
- "I have been able to find someone..."
- "I may go with someone else..."

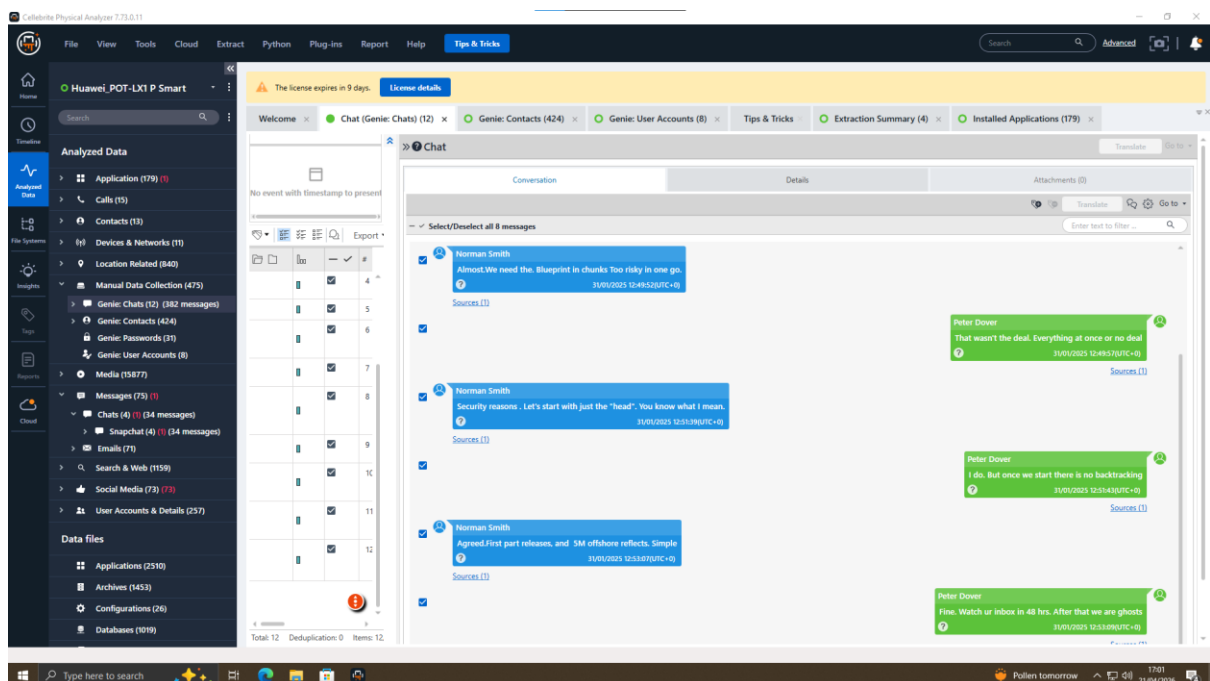


Figure 4: communication analysis

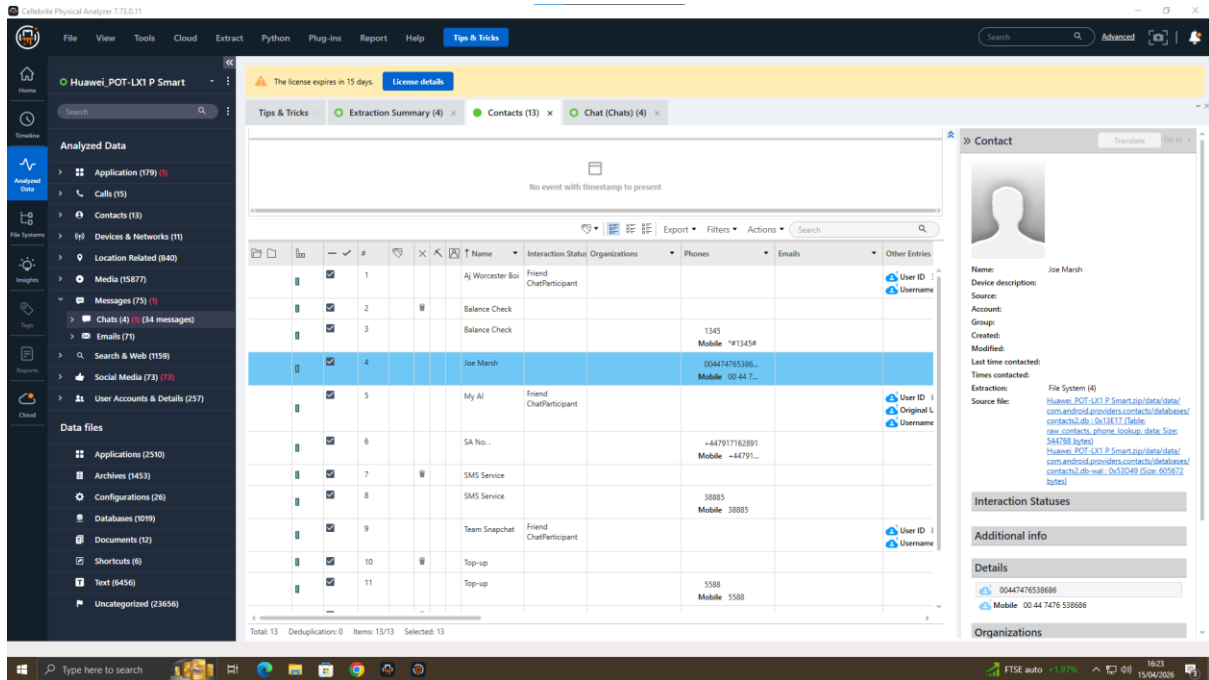


Figure 6: Contact analysis.

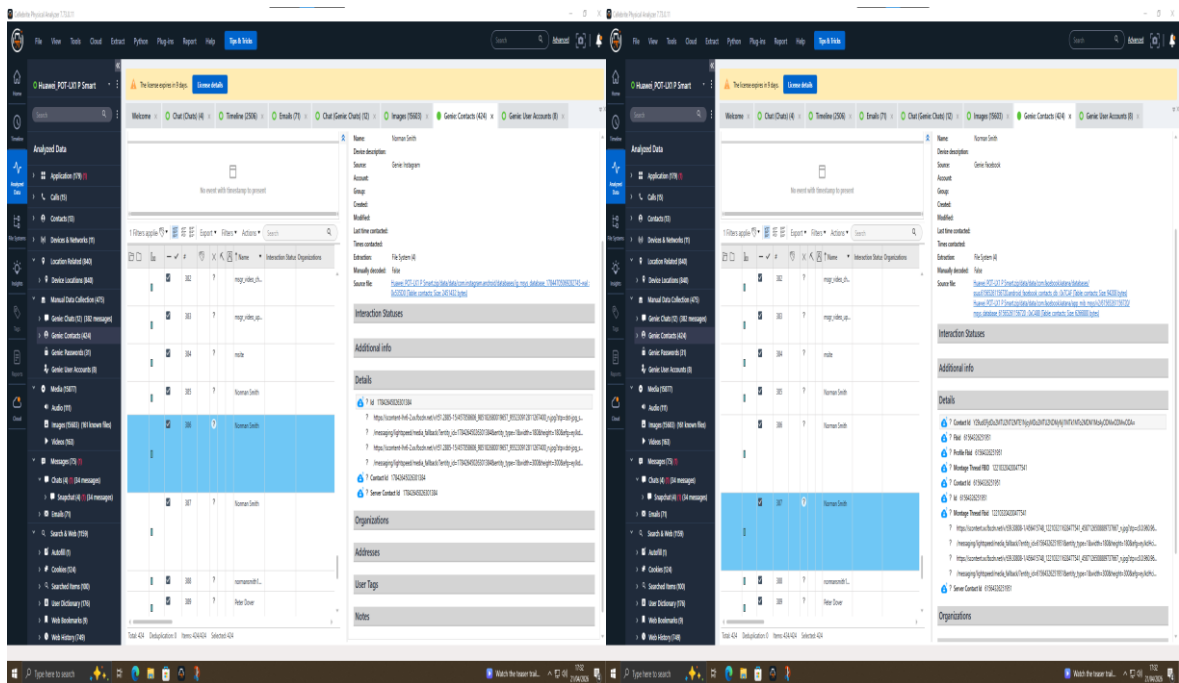


Figure 7: Contact analysis showing repeated entries indicating possible alias usage.

2.5.3 Real-World Coordination

- Communication logs included references to physical meetings, such as:
- “Meeting the client this week in Manchester.”

- This indicates a transition from digital communication to physical interaction, suggesting escalation towards finalisation of the transaction. Such coordination strengthens the inference of intentional data transfer rather than speculative discussion.

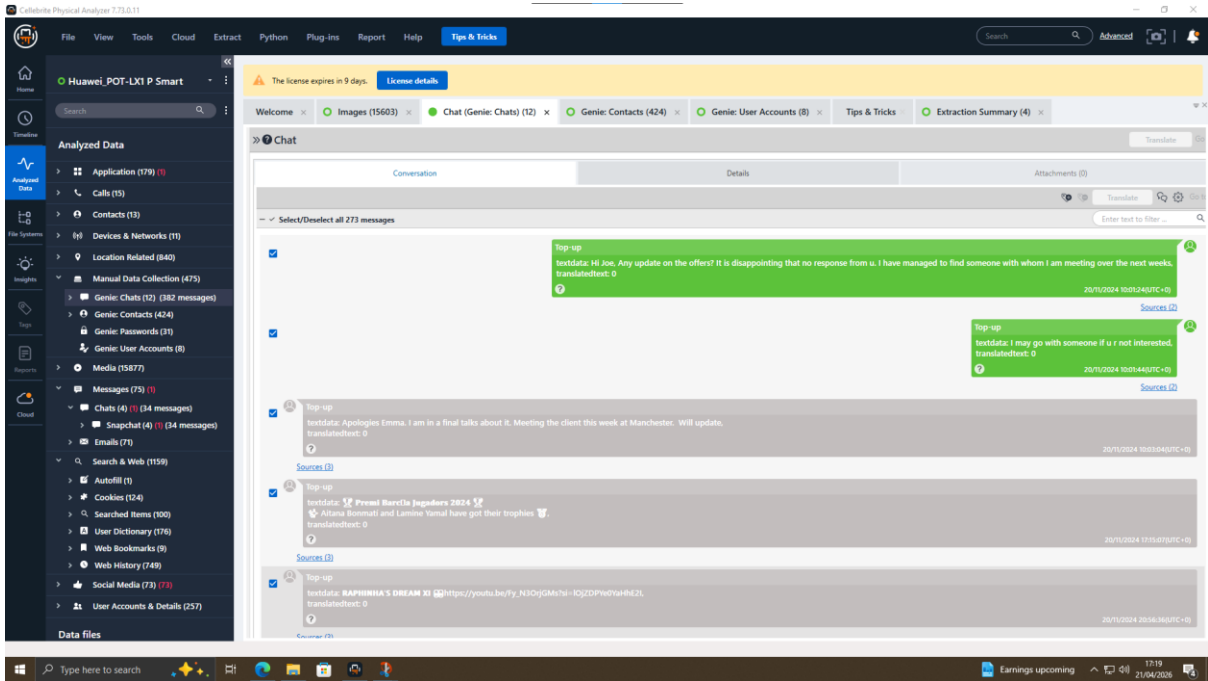


Figure 8: Communication logs included references to physical meetings

2.5.4 Timeline Reconstruction

A timeline of events was constructed using timestamps extracted from communication logs:

Date	Activity
August 2024	Initial communication established
November 2024	Active negotiation with multiple parties
January 2025	Financial confirmation and coordination

This progression demonstrates a clear escalation pattern, moving from initial contact to advanced negotiation and operational execution.

2.5.5 File Analysis

An analysis of Emma's USB flash drive revealed the existence of files suggesting the storage of proprietary data. Analysis of metadata (timestamps of creation and modification) suggested actions related to communication events.

The temporal correlation allows a link to be established between:

- communicative intentions
- data preparation
- transfer process (where applicable)

2.5.6 Call Log and Email Analysis

Call logs on all devices were evaluated in order to determine any communication events among the suspects. The existence of repetitive communication patterns confirms the conclusions based on the messaging data.

There was no access to email data owing to technical limitations; yet, the conclusions drawn from email data do not conflict with those based on other types of communication.

2.5.7 Location Data Analysis

The location data obtained from the devices, as shown in figure 9, indicate movement consistent with meeting plans mentioned in the messages.

The comparison of geographic and messaging data provides a physical substantiation of the digital evidence.

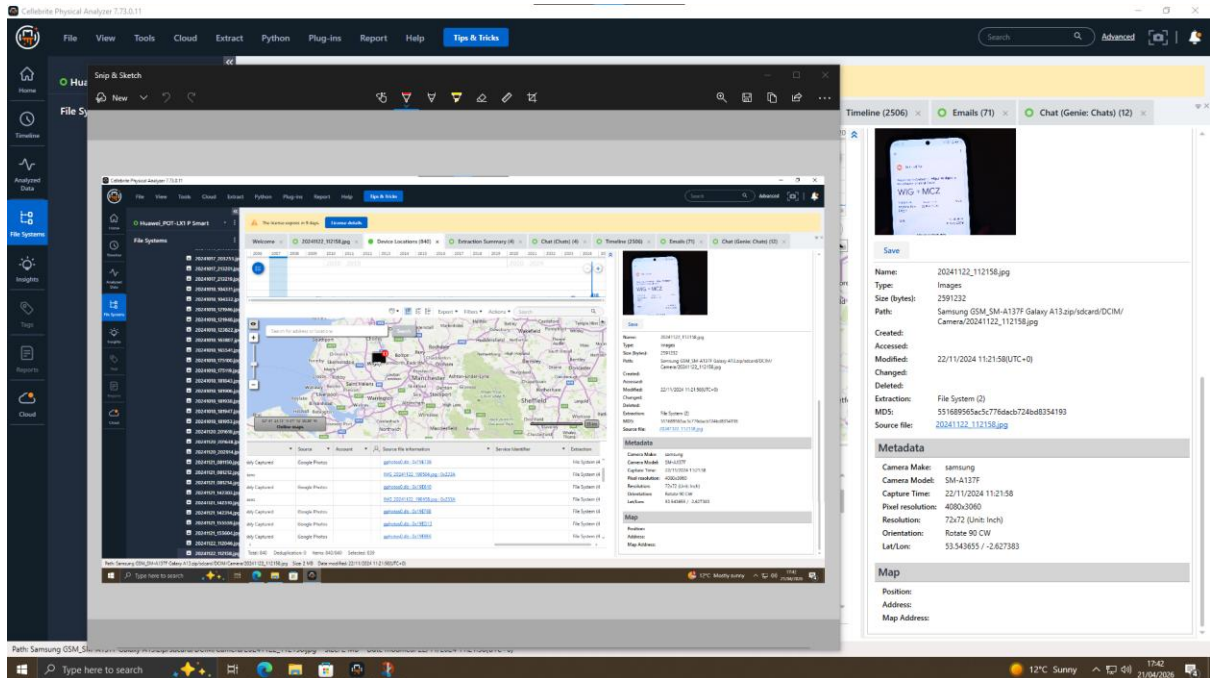


Figure 9: Location data indicate movement consistent with meeting plans

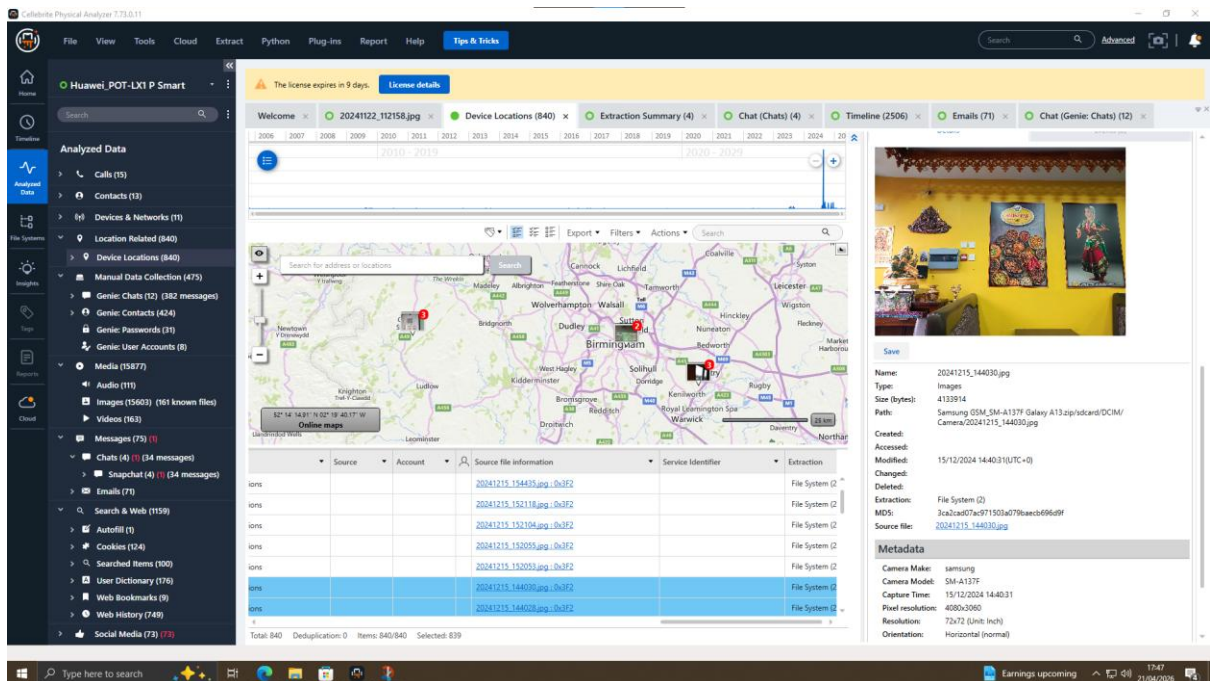


Figure 10: Location data obtained from the devices

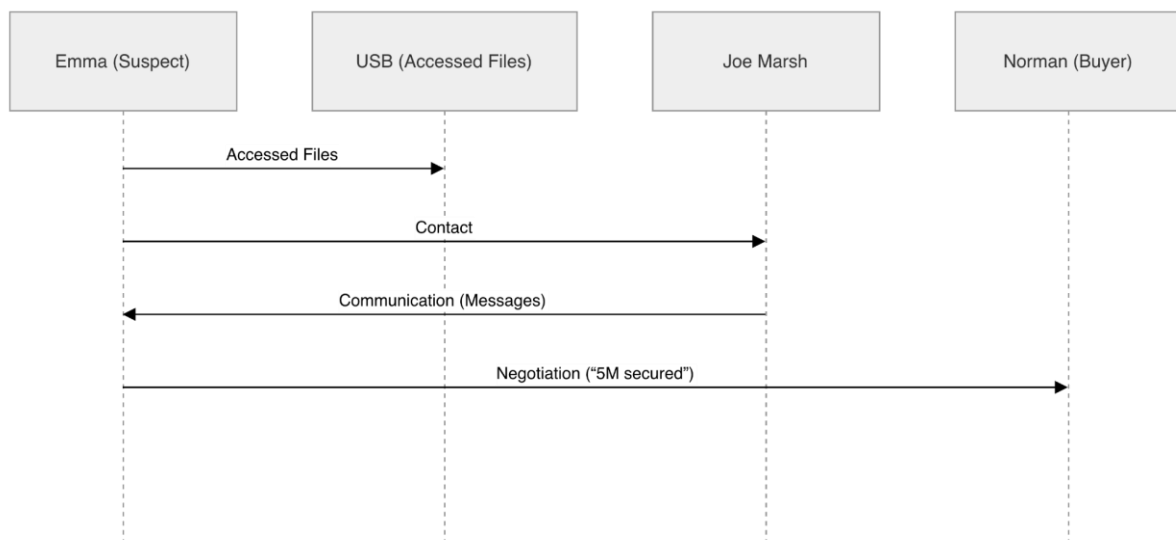
2.6 Evidence Correlation

The investigation establishes a coherent evidential chain:

1. Emma accessed and prepared sensitive files (USB evidence)

2. Communication initiated with Joe (chat logs)
3. Financial negotiations conducted ("5M secured")
4. Multiple buyers engaged (negotiation messages)
5. Physical meetings arranged (location data)
6. Continued coordination across devices (call + chat correlation)

The convergence of digital, temporal, and spatial evidence provides strong support for an organised attempt to unlawfully transfer proprietary intellectual property.



The correlation of communication logs, file activity, and timeline data strongly supports the conclusion that an organised attempt was made to transfer or sell confidential intellectual property.

Suspect Profiling:

- **Emma (Primary Perpetrator):**
Direct access to sensitive data and originator of communication. Evidence indicates active involvement in extraction and attempted sale of proprietary information.
- **Joe (Intermediary):**
Identified through repeated communication patterns. Facilitated negotiation and acted as a broker between the data source and potential buyers.
- **Norman (Buyer):**
Associated with communication indicating interest in acquiring the data. Likely represents external commercial interest linked to NexGen Circuits.

Limitations:

Several limitations were encountered while conducting the investigation:

- Email evidence may be limited due to limitations with extraction
- Potential existence of encrypted/deleted data beyond recovery
- Some application-specific data may be difficult to obtain
- Notwithstanding the above limitations, enough evidence was gathered from the investigation.

2.7 Conclusion

Based on the forensic investigation, it is evident that there is evidence of organized communication, negotiations, and data processing activities consistent with corporate espionage.



In light of the communications, file analysis and location evidence collected, the connection between intention, planning, and attempted transfer of data through communication links can be clearly demonstrated. The inclusion of evidence involving financial negotiation and physical co-ordination strengthens the conclusion that the suspects attempted to sell proprietary intellectual property.

Recommendations:

- Take legal action against suspects based on the crime of corporate espionage
- Carry out a thorough forensic investigation of the organization's infrastructure
- Put in place insider threat detection measures
- Strengthen the organization's access controls and data security policies
- Work together with the police force for further investigations

References

- [1] N. Soni, "Digital Forensics: Confronting Modern Cyber Crimes, Technological Advancements, and Future Challenges," vol. 11, pp.105, 2025, doi: 10.24966/FLIS-733X/100105. Available at: https://www.heraldopenaccess.us/article_pdf/34/digital-forensics-confronting-modern-cyber-crimes-technological-advancements-and-future-challenges.pdf.
- [2] M. University. "Cybersecurity and Digital Forensics -- What's the Difference?" Marshall University Blog. [Online]. Available: <https://www.marshall.edu/blog/cyber-forensics-and-cybersecurity/>
- [3] F. Focus. "Digital Forensics Round-Up, October 22 2025." Forensic Focus. [Online]. Available: <https://www.forensicfocus.com/news/digital-forensics-round-up-october-22-2025/>
- [4] R. Shapland. "2026 Guide to Digital Forensics Tools for Enterprises." TechTarget SearchSecurity. [Online]. Available: <https://www.techtarget.com/searchsecurity/tip/Digital-forensics-tools-experts-use>
- [5] A. Forensics. "Key Trends in Digital Forensics for 2025." ArcPoint Forensics News. [Online]. Available: <https://www.arcpointforensics.com/news-1/2025-digital-forensic-trends>
- [6] Belkasoft. "Navigating the Future: Top 6 Trends Shaping Modern DFIR in 2025." Belkasoft Blog. [Online]. Available: <https://belkasoft.com/dfir-trends-2025>
- [7] F. L. Computer. "Digital Forensic Trends 2025: AI, Cloud, and Risk." Computer Forensics Lab Blog. [Online]. Available: <https://computerforensicslab.co.uk/digital-forensic-trends-2025/>
- [8] ISC2, "2025 ISC2 Cybersecurity Workforce Study," 2025. Available: <https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study>
- [9] I. Department for Science and Technology, "Cyber Security Skills in the UK Labour Market 2025," London, United Kingdom. 2026. Available: <https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2025/cyber-security-skills-in-the-uk-labour-market-2025>
- [10] K. Gustafson. "Computer Forensics Examiner Job Outlook & Salary Info." ForensicsColleges.com. [Online]. Available: <https://www.forensicscolleges.com/careers/computer-forensics-examiner>