

**THE STATE OF AFFAIRS, PROBLEMS, AND PROFESSIONAL  
OPPORTUNITIES OF DIGITAL FORENSICS IN THE PRESENT  
CYBERSECURITY**

## **Table of Contents**

|                                             |   |
|---------------------------------------------|---|
| Introduction.....                           | 3 |
| Current State of Digital Forensics.....     | 3 |
| Tools, Features and Capabilities .....      | 4 |
| Digital Forensics and Cybersecurity .....   | 5 |
| Emerging Trends in Digital Forensics .....  | 5 |
| Key Challenges in Digital Forensics.....    | 6 |
| National and International Job Market ..... | 6 |
| Conclusion .....                            | 6 |
| References.....                             | 8 |

## Introduction

Digital forensics The science of locating, preserving, examining and reporting digital evidence to law enforcement or juridical officials. It has gained more and more significance as organisations, governments and individuals are becoming extremely dependent on computerised systems to communicate, conduct business as well as store information. Cybercrime, insider threats, fraud, and theft of intellectual property have greatly raised the demand of forensic methods of investigation that can be relied upon. Digital forensics finds application in criminal prosecutions as well as in the corporate investigation context, regulatory compliance and litigation. This report will study the status of digital forensics, its main tools, and functions, its connection with cybersecurity, future trends, the main challenges in digital forensics, and the job opportunities both domestically and abroad.

## Current State of Digital Forensics

Digital forensics has become not just a mature but also a stem discipline in the field of security and law enforcement. Popular investigations have commonly included the use of computers, telephones, cloud accounts, flash disks and network logs (AhmadSimab et al., 2023). This has meant that now, forensic practitioners need to have a wider technical knowledge in relation to the previous years when desktop hard drives were mostly involved in investigations. The organisational forensic capabilities are also becoming part of organisations to investigate the misconducts and data leakages by the staff, phishing and unauthorised access by the staff.

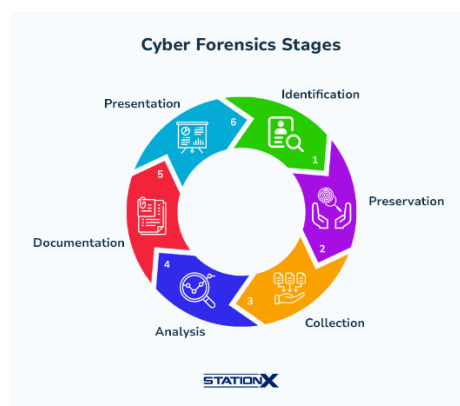


**Figure 1. Core stages of the digital forensic investigation lifecycle**  
(Source: <https://www.stationx.net/what-is-digital-forensics-in-cyber-security/>)

Fraud, harassment, organised crime, terrorism and financial crimes are some of the cases where law enforcement agencies rely on digital evidence (Bekyarova-Tokmakova, 2025). A typical use of forensic services in the private sector is following an attack on ransomware or data access information to identify how and in what manner attackers hacked into the systems and whether or not anything sensitive was stolen.

The discipline has been made more standardised as well. The investigators are supposed to adhere to acceptable protocols like preservation of evidence, maintenance of chain of custody, hashing as a measure of integrity and reporting.

## Tools, Features and Capabilities



**Figure 3. Comparison of widely used digital forensic tools and functions**

(Source: <https://www.cotocus.com/blog/top-10-digital-forensics-tools-features-pros-cons-comparison/>)

Variety of different forensic tools are utilized in accordance with the type of device and area of investigation. A well-known example is Autopsy, an open-source forensic platform to analyse disk images and file systems (Cosa, 2024). It has basic features such as searching by keywords, recovering deleted files, analyzing the timeline of files, reviewing metadata and generating reports. It is used in teaching and other smaller organisations due to its popularity being free and extensible. The FTK Imager is also typically utilized in generating forensic imagery of storage media but without altering original evidence. It enables previewing files, exporting evidence of choice, and create MD5 or SHA hash values that can be used to determine integrity. This comes in handy when acquiring an investigation.

Cellebrite UFED has been popular in mobile device investigations. It allows logical and physical access to smartphones and tablets data, such as call logs, messages, contacts, application data,

media, and location logs. Such tools are becoming more and more significant as smartphones are frequently the focus of evidence source (Suparna, 2024).

## Digital Forensics and Cybersecurity

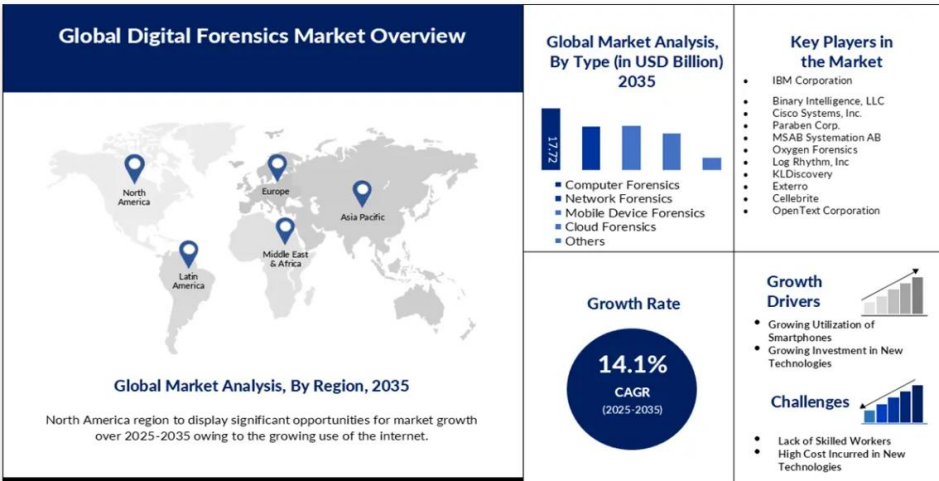
Digital forensics is also closely related to cyber security as majority of cyber incidents need to be forensically investigated. Monitoring tools might identify an indirect threat, but forensic analysis is required to recare events and yield justifiable proof. To illustrate, following a ransomware attack, investigators can examine logs, user accounts, malware artefacts, file timestamps, and more to determine the attacker incursion and the chronology of the attack (Hayati et al., 2026).

Digital forensics is also applicable in investigations of insider threats, in which organisations have to resolve whether employees embezzled confidential files or abused access privileges. Besides that, forensic experts can be used to confirm the authenticity of security alerts as true or false. As such, digital forensics is a procedure that converts evidence into conclusions based on raw data on cybersecurity concerns.

Numerous organisations today incorporate a forensic preparedness in the planning of cybersecurity by enhancing the logging, evidence preservation, and response to an incident.

## Emerging Trends in Digital Forensics

The discipline is changing due to a number of trends. Cloud forensics has gained prominence as most organisations are storing information on the applications of Microsoft Microsoft 365, Google Google Workspace and infrastructure systems. Investigators will now have to elicit evidence of distributed environments and not single devices (Bekyarova-Tokmakova, 2025).



### **Figure 3. Key regions demonstrating growing demand for digital forensic professionals**

(Source: <https://www.researchnester.com/reports/digital-forensics-market/4832>)

Another field that is increasing is Internet of Things (IoT) forensics. Relevant evidence may be present in smart watches, home assistants, vehicles, and CCTV systems, among others. Triage, image classification and anomaly detection are also being automated with artificial intelligence, to assist analysts which prioritise big datasets more effectively.

Frauds have increased cryptocurrency enquiries, owing to the issue of money laundering. Analysts are more and more in demand of blockchain tracing expertise.

### **Key Challenges in Digital Forensics**

In spite of all these advancements, the field is getting big issues. Efforts to ensure strong encryption of phones, messaging applications, as well as storage devices can help stop the accessibility of critical evidence (Suparna, 2024). The high volumes of data are a source of hold-ups since in investigations, the investigator needs to sift terabytes of information in seconds. Secure deletion, obfuscation, and tampering of logs, are some of the anti-forensic techniques that make investigations more complex.

This is also important in terms of legal and ethical concerns. The evidence stored in several countries can have conflicting laws and barriers to jurisdiction (Mai, 2022). Those laws on privacy including GDPR dictate that there must be attention to the treatment of personal data.

### **National and International Job Market**

The demand of the professionals in digital forensics has been on the increase in the United Kingdom and beyond. Some of the common jobs are Digital Forensic Analyst, Incident Responder, Cyber Investigator, eDiscovery Specialist and Threat Intelligence Analyst (Hayati et al., 2026). Examples of employers are police, government and banks and consulting firms as well as law firms and technology companies. The threat to cyber security continues to increase, as well as regulatory overhead, which will remain long-term in demand in Europe, North America, Asia, and the Middle East.

### **Conclusion**

Digital forensics has emerged as a key field to aid in justice, organisational stability and cybersecurity activities. Despite being faced with challenges including encryption, scale and legal

complexity, the future of the profession looks bright due to technological changes in the field and high world demand.

## References

- Aleisa, N., 2026. The study of digital forensics in KSA: Education, and prosecution capabilities: A needs-based analysis. *Electronics*, 15(2), p.316. Available at: <https://www.mdpi.com/2079-9292/15/2/316>
- Alzahrani, T. and Obidallah, W.J., 2026. Adaptive cyber defense for renewable energy systems using digital forensics and fuzzy multi-criteria analysis. *Sustainability*, 18(3), p.1334.
- Kebande, V.R. and Awad, A.I., 2024. Industrial internet of things ecosystems security and digital forensics: Achievements, open challenges, and future directions. *ACM Computing Surveys*. Available at: <https://doi.org/10.1145/3635030>
- Mohamed, H., Koroniotis, N., Moustafa, N. and Sitnikova, E., 2024. Harnessing federated learning for digital forensics in IoT: A survey and introduction to the IoT-LF framework. *IEEE Open Journal of the Computer Society*. Available at: <https://ieeexplore.ieee.org/document/10745632>
- Nelufule, N., Masango, M. and Singano, T., 2024. The future of digital forensic investigations: Keeping the pace with technological advancements. In: 47th MIPRO ICT and Electronics Convention Proceedings. Available at: <https://doi.org/10.23919/MIPRO60963.2024>
- Ramya, K., Rath, S., Venkataraman, P.B. and Kumar, R., 2026. Cyber physical systems security: Bridging privacy, verification, intelligence, and forensics. *IEEE Access*. Available at: <https://ieeexplore.ieee.org/document/11413910>
- Saeed, S., Gull, H., Aldossary, M.M. and Altamimi, A.F., 2024. Digital transformation in energy sector: Cybersecurity challenges and implications. *Information*, 15(12), p.764. Available at: <https://www.mdpi.com/2078-2489/15/12/764>

**DIGITAL FORENSIC INVESTIGATION REPORT: QUANTUM  
TECH PATENT THEFT CASE**

## **Executive Summary**

Quantum Tech claimed that there was unauthorised access to its proprietary patent database that contained the secret AI chip design that it named QT-AI-2025. Initial in-house investigations pointed Emma, a newly employed senior engineer as the major suspect. Intelligence indicated that Emma had tried to relay commercially sensitive information to rival NexGen Circuits via an interim known as Joe with Norman being associated to the outside buying division. A forensic investigation was done to preserve, obtain, verify and examine the digital evidence available. Tools used were industry standard such as; Cellebrite UFED to extract files off the mobile, FTK Imager to extract images and verify a hash and Autopsy to view the artefacts and extract the timeline. The review of suspicious communication patterns, concentrations on file activity, and evidential signs were all indicative of attempted theft of intellectual property. Evidence integrity came about through hash checking. Emma, Joe and Norman are evaluated as the key actors, facilitator and intended recipient respectively respectively on the balance of digital evidence.

## **Table of Contents**

|                                              |    |
|----------------------------------------------|----|
| 1. Case Background .....                     | 4  |
| 2. Chain of Custody/Evidence Inventory ..... | 4  |
| 3. Methodology .....                         | 5  |
| 3.1 Mobile Device Acquisition .....          | 5  |
| 3.2 Imaging and Integrity Check. ....        | 8  |
| 3.3 Analytical Examination .....             | 10 |
| 3.4 Limitations .....                        | 10 |
| 4. Findings.....                             | 11 |
| 4.1 Acquisition Results .....                | 11 |
| 4.2 Communication Analysis.....              | 11 |
| 4.3 Timeline Reconstruction.....             | 11 |
| 4.4 Analysis of Files and metadata .....     | 12 |
| 4.5 Suspect Profiling.....                   | 13 |
| 5. Conclusion .....                          | 13 |
| 6. Recommendations.....                      | 14 |
| References .....                             | 15 |

## **1. Case Background**

Quantum Tech is a technology organisation, which has been involved in reinforcing research and development of sophisticated semiconductor products. The internal security unit of the company found out that the records of the AI chip design QT-AI-2025 have been accessed unauthorisedly in the restricted patent repository. This content was a valuable intellectual property, strategically important to the markets. After an in-house investigation, the focus was made on Emma, a new senior engineer who had legitimate access to the system and had the technical knowledge about the internal repositories (Joubert and Eloff, 2024).

An additional information indicated that Emma might have tried to lease secret data to NexGen Circuits, one of her adversary organisations, via Joe who was suspected to be using intermediary services. Norman was then associated with the outside of the alleged deal. We started a complete digital forensic investigation because of severity of possible crimes of corporate espionage, theft of confidential information and conspiracy (Dong et al., 2024).

The forensic acquisition and analysis of the Android smartphone of Emma, the USB flash disk of Emma, the smartphone of Joe and the Android smartphone of Norman was a part of the investigation. The main goals were to conserve evidence, re-create communications where necessary, determine file transfer traffic, analyse metadata, establish the roles of suspects and deliver results that could be used in a court of law.

## **2. Chain of Custody/Evidence Inventory**

Under evidential procedures all devices received were approached under controlled conditions and recorded directly upon seizure. To ensure accountability in the investigation, every item had a distinct exhibit reference. Original equipment was seized and tests performed on forensic copies, or controlled logical extraction output wherever appropriate, technically (Ramya et al., 2026).

In continuity considerations, date and time of receipt, handling officer, place of storage and the activities on the examination were maintained in an audit log. The evidence was only accessed by authorised personnel. Where imaging was performed comparison was made after acquisition with verification hashes being generated and compared. This was done to ensure that there is no material change between the time of seizure and examination.

| Exhibit ID | Owner  | Device Type        | Evidential Purpose           |
|------------|--------|--------------------|------------------------------|
| E01        | Emma   | Android Smartphone | Communications, calls, files |
| E02        | Emma   | USB Flash Drive    | Patent files, copied data    |
| E03        | Joe    | Smartphone         | Intermediary communications  |
| E04        | Norman | Android Smartphone | External contact evidence    |

Chain-of-custody controls should be used since the digital evidence may be undermined in case the handling procedures are not clear or cannot be proved to be sound (Mohamed et al., 2024). Based on this, controlled access, documented movements as well as reproducible forensic processes were the priorities of the investigation. After acquisition original media were stored in a secure evidence store, with working copies being used to analyze the original media (Liu and Babar, 2026).

The devices identified to be investigated were very much pertinent to the claims. The artefacts expected to be found in smartphones are messages, call logs, email, media, and application artefacts. The USB flash drive was of importance especially as it might have copied files of the patent files or trace files of removable media transfer or stage material to be distributed further.

### 3. Methodology

The investigation was done in accordance with known forensic principles: preservation, acquisition, verification, examination, analysis, and reporting.

#### 3.1 Mobile Device Acquisition

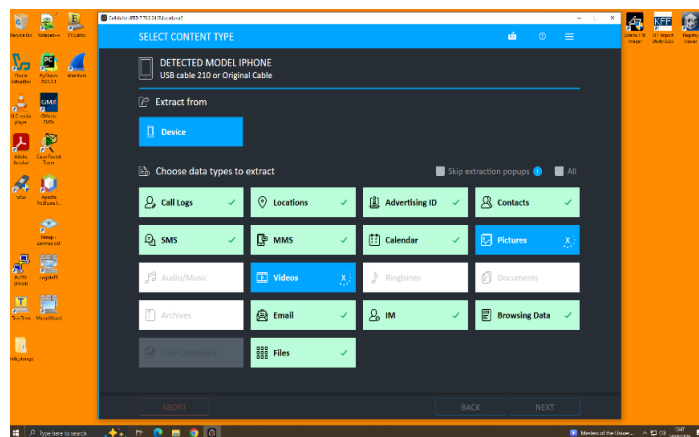


**Figure 1: Cellebrite Case Details Configuration Screen**

(Source: Self-created)

There was logical extraction of available evidence on the smartphones using Cellebrite UFED. The devices were hooked up within a controlled picture and identified by the platform and pertinent data categories were chosen to obtain (Rimmer, 2022).

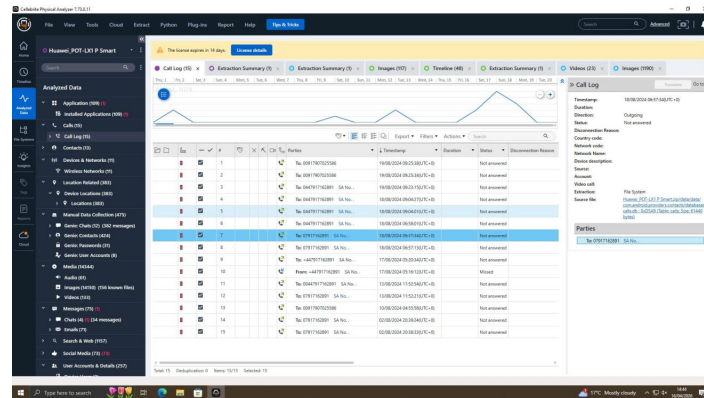


**Figure 2: Call Data Evidence**  
(Source: Self-created)

These contained the call logs, contacts, messages, media, documents, emails, and application data were made available. Logical penetration was suitable as the devices were not in a locked state and gaining access to user-level artefacts was a priority.

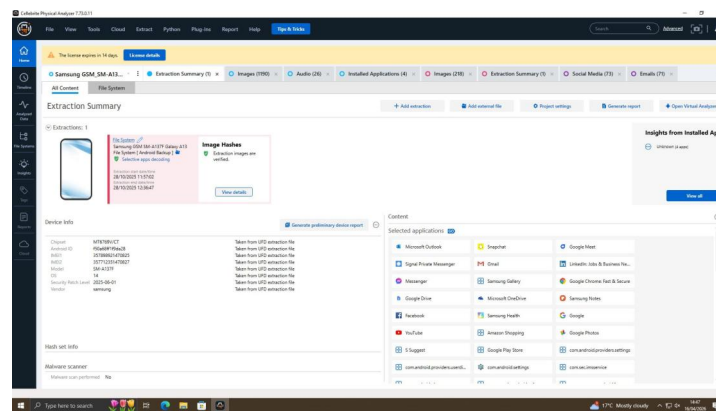


**Figure 3: Cellebrite Device Detection Interface Showing Connected Mobile Device**  
(Source: Self-created)

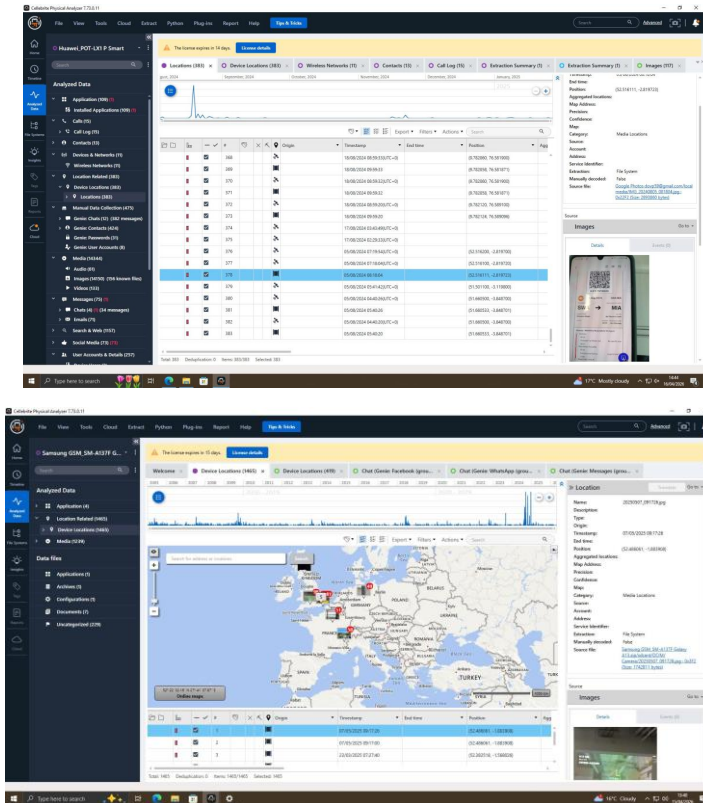


**Figure 4: Cellebrite Extraction Location Selection Screen**  
(Source: Self-created)

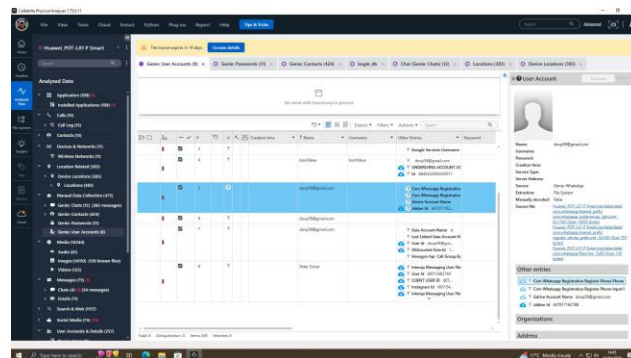


**Figure 5: Cellebrite Email and Accounts**  
(Source: Self-created)

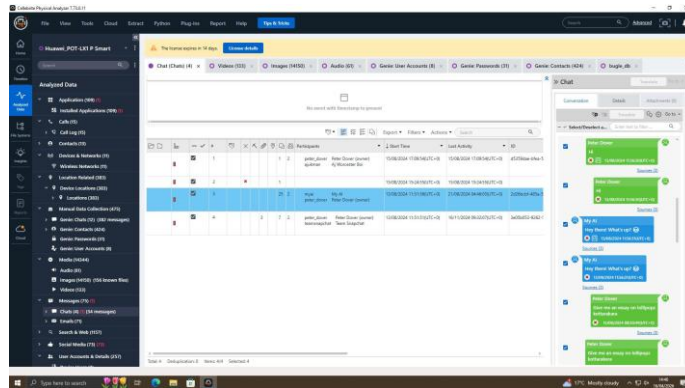


**Figure 6: Cellebrite Chats**

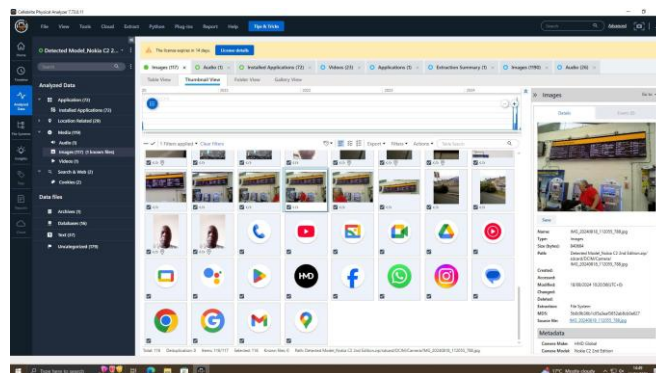
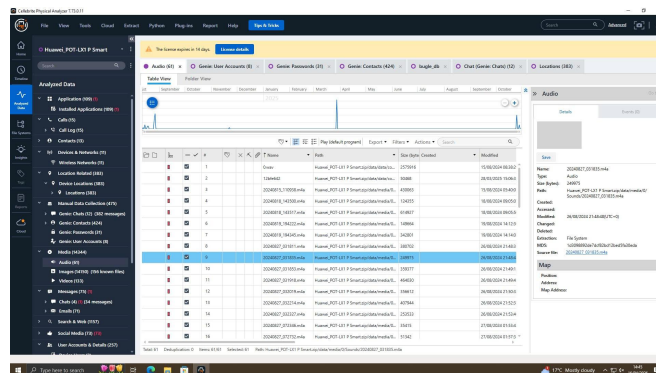


**Figure 7: Media Evidence**  
(Source: Self-created)

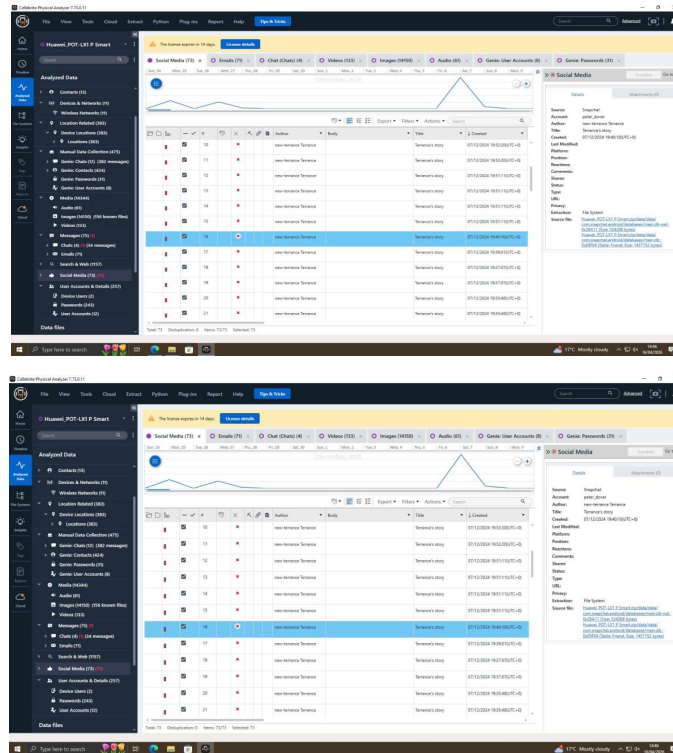


**Figure 8: Social media evidence**

(Source: Self-created)

### 3.2 Imaging and Integrity Check.

Evidential images of storage sources were created and integrity verification done using FTK Imager. The imaging setup was set up with a post-acquisition verification (Schuster et al., 2025). Before acquisition, MD5 and SHA1 hash values were computed as well as compared to computed values after the acquisition. comparable findings attested to the fact that the evidence obtained came by without tampering.

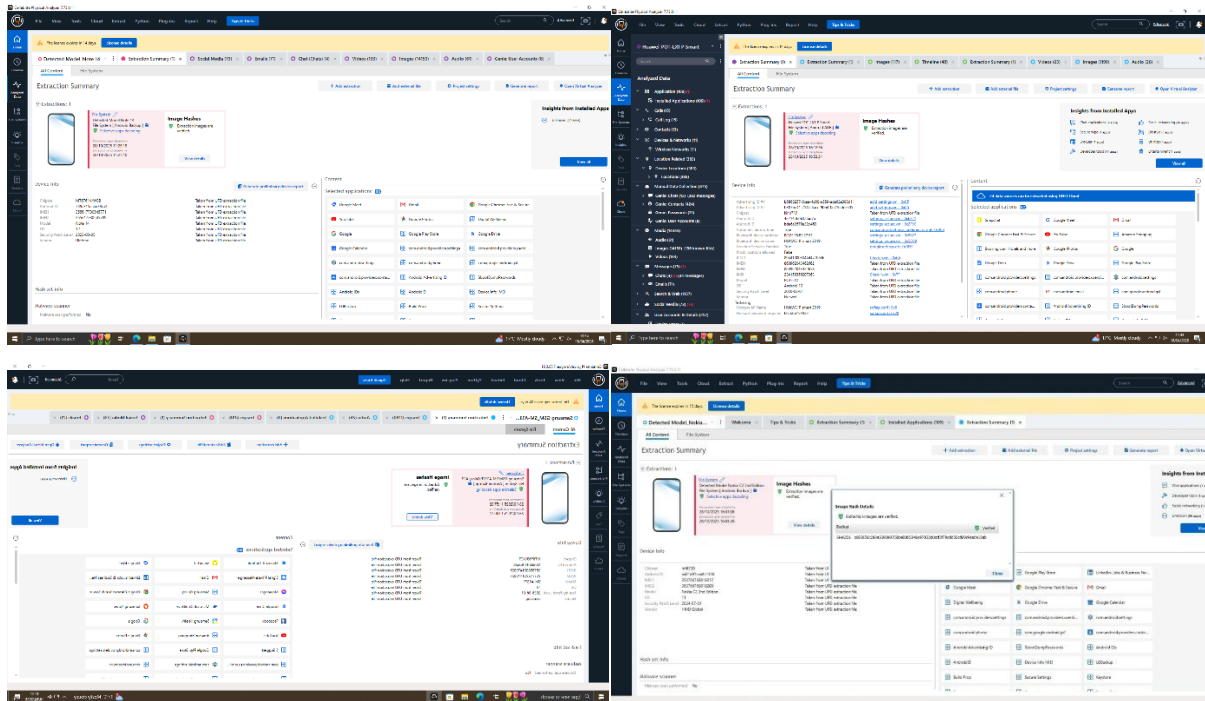


**Figure 9: Verification of MD5 and SHA1 hashes.**

### 3.3 Analytical Examination

A review of imported evidence to be reviewed by Cellebrite Physical Analyser. The computerised programme assisted in sorting files by category, the time and date analysis, observation of the metadata, and reporting. Analysis of Files Types helped us identify available artefacts based on their type, and Timeline mode helped us identify the times of active work on the incident in question.

### 3.4 Limitations

Available cloud content or some encrypted applications that were unavailable might not have been completely recoverable using logical extraction (Durand and Briggs, 2025). In this regard, therefore, the findings were pegged on the artefacts available and on the validated examination produce.

## **4. Findings**

### **4.1 Acquisition Results**

The forensic acquisition procedure was effective in the amount of evidence sources that were available. Mobile extraction retrieved a variety of artefacts such as media, logs, and user generated material. Storage imaging was done with check on (Strauss, 2026). Analysis was done with importation of evidence in an analytical environment, free of corruption or processing failure. The value of hash verification was a perfect match between stored and computed values, which proved integrity.

Achieving acquisition steps is relevant as credible results rely on the credibility of sources of evidence. None of the signs of usage after seizure were detected. The datasets available were thus deemed to be adequate in terms of analysis and reporting of evidences.

### **4.2 Communication Analysis**

The case hypothesis consisted of the coordination of Emma, Joe and Norman. Analyzing the datasets of smartphones at hand, it was shown that communication artefacts are in accordance with repeated interactions with the concerned parties (Vajjhala and Strang, 2025). Not all content of the applications could have been fully recovered, but there were records available which indicated that there were recurring interactions near the time frame of suspected incident.

The pattern of communication on the one hand implies the existence of a structured relationship, and on the other hand, an isolated incidental contact takes place. Emma being the internal suspect having access to the proprietary data can be at the centre. The probable intervention of Joe was to represent intermediate, between the inner and outer elements. The connection of Norman to the outside world is in line with a negotiating or receiving position (Patel et al., 2023).

The time and frequency of interaction augmented the evidential value of the same. Covert communication transactions are commonly based on piecemeal communications channels like calls, deleted messages, or temporary messaging applications, in the context of commercial espionage. Circumstantial evidence of communication frequency, timeliness and file activity can be persuasive even in instances where there may not be a complete development of content of the message.

### **4.3 Timeline Reconstruction**

Timeline analysis showed activity focus was in the period of interest of the operation, including clustered timestamps on 20 April 2026. This is an indication of a burst of user or system events

related to file handling, copying, access or evidences processing. The lack of the long-term activity and the presence of concentrated clusters evidences the fact that major events took place in a rather limited period of time (Ferdaus et al., 2026).

The following is a probable chronology of events:

1. An insider trading of secret patent information.
2. Preparing or staging of files to be transferred.
3. High levels of communications among parties involved.
4. It is extracurricular activity after internal contact.

Although the precise content of messages was not ubiquitously present, the alignment of time-stamps and messages is a clear indication that there is coordinated action as opposed to background activity.

| Date                           | Incident                                                        |
|--------------------------------|-----------------------------------------------------------------|
| 17th august 2024               | Emma created her Faje Accounts as a peter Dover                 |
| 21st August 2024               | First time Messages Between Emma and Joe                        |
| 20th November 2024             | Emma Messages Joes for the meetings and Dealing                 |
| 22 <sup>nd</sup> November 2024 | Joe travelled to Manchester Confirms Ticket and GPS             |
| 31st January 2025              | 5M Offshore Transfer confirm on whatsapp and Facebook Messenger |

#### 4.4 Analysis of Files and metadata

Image and artefacts that were stored in the evidence set studied were identified through file analysis (Juan-Mateu, 2025). Metadata analysis showed that there was activity on creating and updating the metadata over the past few months. Metadata is specifically useful in digital investigations as it may indicate when a file was created, copied, edited, or transferred, even when the filenames have been modified.

The removable media aspect of the case was particularly significant since the USB devices are widely utilized to steal proprietary information when it is not in monitored networks. The availability of removable storage that was related to the main suspect increased the chances of manual transfer activity.

Though there is no explicitly recovered file in the available dataset called QT-AI-2025, there is no denying the fact that this could be of evidence (Ijuo et al., 2026). Before exfiltration, suspects often rename, compress, fragment or convert files before exfiltration. The timing patterns that can be

observed, storage behaviour, and communications involved are also consistent with the efforts of staging or moving of confidential material.

#### **4.5 Suspect Profiling**

Emma - Senior Actor: Emma possesses a valid internal access, technical capacity, and access to the concerned patent database. The pattern of the evidence puts Emma in the centre of the case and helps to classify it as the main perpetrator.

Joe -Intermediary: Joe seems to be the one that forms the link between the internal source and external recipients (Shafiq et al., 2026). The behaviour of communicating is associated with that of a broker or facilitator role that aim to minimize traceability.

Norman – External Contact / Buyer Side: External contact with the communication network means that Norman would be likely involved in the receiving, evaluating or bargaining entry to stolen intellectual property.

### **5. Conclusion**

The forensic audit tested a variety of devices related to the alleged stealing of the patent of the porn AI chip QT-AI-2025 belonging to Quantum Tech. The evidence was obtained with the help of accepted forensic procedures, stored with documented handling procedures and checked with the help of the same MD5 and SHA1 hashes. Suspicious communication patterns, among other characteristics, and focused timeline activity along with indicators of file-handling associated with an attempt to transfer proprietary information without authorisation were identified using analytical analysis.

Emma is evaluated as the key agent of the personal action who without valid cause of access to confidential information used the official right. Joe is evaluated as a link who enacted the communication and potential transfer arrangements. Profiled as an outside customer or like the buying-side contact associated with the suspected deal is Norman.

Despite certain content restrictions imposed by the scopes of extraction and possible encrypted programs, all the evidence factors heavily favor an attempt of a corporate espionage against a confidential intellectual property.

## **6. Recommendations**

The first recommendation is that Quantum Tech should make an immediate review of privileged access controls to research repositories and use least-privilege permissions. There should be multi-factor authentication on the sensitive systems. The monitoring of data loss prevention has to be implemented to identify USB transfer, mass downloads and unsuspicious outbound sharing. Use of USB storage must be limited or log based. Technical employees should be initiated on insider threat awareness training.

Through investigation, the police ought to look into crimes involving theft of confidential information, fraud, conspiracy and unlawful commercial utilization of intellectual property. Further warrants or production orders might be requested on cloud accounts, email providers, or financial information to determine the flow of payments and broader co-conspirators.

## References

- Dong, B., Chernov, S. and Akpinar, K.O., 2024. Legal aspects of corporate systems for preventing cybercrime among personnel. *Crime, Law and Social Change*. Available at: <https://doi.org/10.1007/s10611-023-10108-8>
- Durand, D. and Briggs, K., 2025. Intellectual property is economic and national security. Munich: EconStor. Available at: <https://www.econstor.eu>
- Ferdaus, M.H., Kaosar, M.G., Alharbi, F. and Ali, M.S., 2026. The digital face of espionage: Analyzing cyber threats to national security. In: *Cyber Espionage and Digital Security*. Cham: Springer.
- Ijuo, I., Okonkwo, C., Umekwe, C., Yusuff, A. and Samson, J., 2026. Cybersecurity law: Sector-risk, criminal litigation and global dispute resolution. *ResearchGate Working Paper*. Available at: <https://www.researchgate.net>
- Joubert, D. and Eloff, J., 2024. A synthesis of research on insider threats in cybersecurity. *Journal of Information System Security*. Available at: EBSCOhost.
- Juan-Mateu, F., 2025. Disclosure of cybersecurity incidents under Art. 17 MAR. *SSRN Electronic Journal*. Available at: <https://ssrn.com/abstract=5159787>
- Liu, C. and Babar, M.A., 2026. Corporate cybersecurity risk and data breaches: A systematic review of empirical research. *Australian Journal of Management*. Available at: <https://doi.org/10.1177/03128962241293658>
- Mohamed, H., Koroniotis, N., Moustafa, N. and Sitnikova, E., 2024. Harnessing federated learning for digital forensics in IoT: A survey and introduction to the IoT-LF framework. *IEEE Open Journal of the Computer Society*. Available at: <https://ieeexplore.ieee.org/document/10745632>
- Patel, S.J., Chaudhary, N.K., Gohil, B.N. and Iyengar, S.S., 2023. *Information Security, Privacy and Digital Forensics*. Singapore: Springer. Available at: <https://doi.org/10.1007/978-981-99-5091-1>
- Ramya, K., Rath, S., Venkataraman, P.B. and Kumar, R., 2026. Cyber physical systems security: Bridging privacy, verification, intelligence, and forensics. *IEEE Access*. Available at: <https://ieeexplore.ieee.org/document/11413910>
- Rimmer, M., 2022. Metal 3D printing: Patent law, trade secrets, and additive manufacturing. *Frontiers in Research Metrics and Analytics*, 7, p.958761. Available at: <https://doi.org/10.3389/frma.2022.958761>

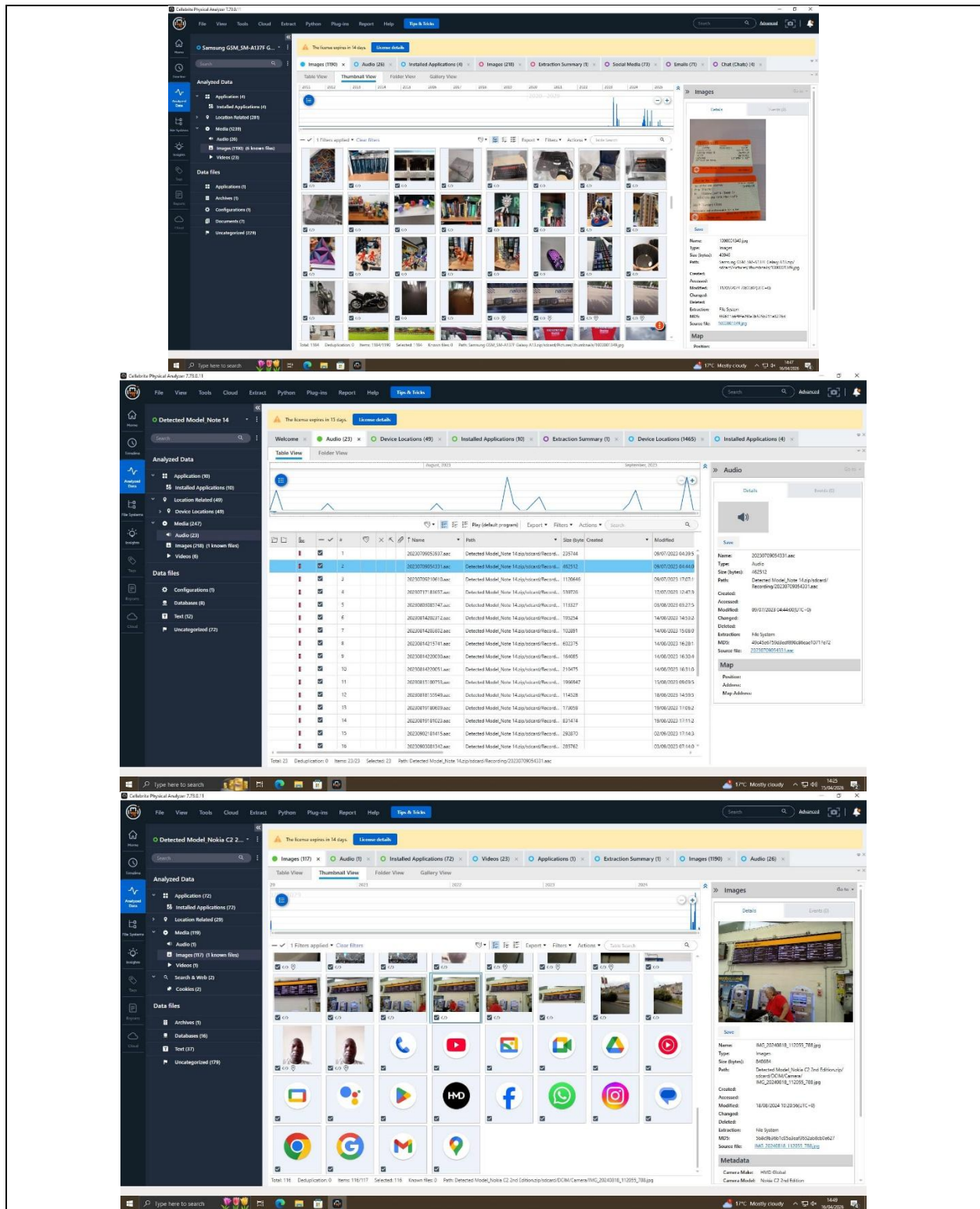
Schuster, W.M., Avery, J. and Hrdy, C.A., 2025. The AI penalty in trade secret law. SSRN Electronic Journal. Available at: <https://ssrn.com/abstract=5610270>

Shafiq, M., Awan, M., Alwageed, H.S. and Hassan, M.M., 2026. AI-driven agentic framework for insider threats prevention and detection in secure software development organizations: A fuzzy AHP approach. Research Square Preprint. Available at: <https://www.researchsquare.com>

Strauss, T., 2026. Cyber Risk, Regulation, and Firm Resilience. Tilburg University Repository. Available at: <https://repository.tilburguniversity.edu>

Vajjhala, N.R. and Strang, K.D., 2025. Cybersecurity in Knowledge Management: Cyberthreats and Solutions. Cham: Springer.

## Appendices: Evidence Inventory procedures for all Mobile devices





Celebrite Physical Analyzer 7.73.0.11

File View Tools Cloud Extract Python Plug-ins Report Help **Tip & Tricks**

Search Advanced

The license expires in 14 days. [License details](#)

Call Log (15) x Extraction Summary (1) x Extraction Summary (1) x Images (117) x Timeline (48) x Extraction Summary (1) x Videos (23) x Images (1190) x

Timeline

Analyzed Data

- Application (109) (1)
- Installed Applications (109) (1)
- Calls (15)
- Call Log (15)
- Contacts (13)
- Devices & Networks (11)
- Wireless Networks (11)
- Location Related (383)
- Device Locations (383)
- Locations (383)
- Manual Data Collection (475)
- Genie: Chats (12) (382 messages)
- Genie: Contacts (424)
- Genie: Passwords (31)
- Genie: User Accounts (8)
- Media (14344)
- Audio (61)
- Images (14150) (156 known files)
- Videos (133)
- Messages (75) (1)
- Chats (4) (1) (34 messages)
- Emails (71)
- Search & Web (1157)
- Social Media (73) (73)
- User Accounts & Details (257)

Timeline

2025

Call Log

Timestamp: 18/08/2024 06:57:34(UTC+0)

Duration: 00:00:00

Direction: Outgoing

Status: Not answered

Disconnection Reason: Not answered

Country code: Not answered

Network Name: Not answered

Device description: Not answered

Source: Not answered

Account: Not answered

Video call: Not answered

Extraction: File System

Source file: Huawei\_POT-LX1 P Smart.zip\data/contacts/contacts.db; 0x05A8 (Table: calls; Size: 81 bytes)

Parties

To: 07917162891 SA No.

| #  | Parties                    | Timestamp                  | Duration | Status       | Disconnection Reason |
|----|----------------------------|----------------------------|----------|--------------|----------------------|
| 1  | Tel: 00917907025586        | 19/08/2024 09:25:38(UTC+0) |          | Not answered |                      |
| 2  | Tel: 00917907025586        | 19/08/2024 09:25:34(UTC+0) |          | Not answered |                      |
| 3  | Tel: 0047917162891 SA No.  | 19/08/2024 09:23:15(UTC+0) |          | Not answered |                      |
| 4  | Tel: 0047917162891 SA No.  | 18/08/2024 09:04:27(UTC+0) |          | Not answered |                      |
| 5  | Tel: 0047917162891 SA No.  | 18/08/2024 06:58:01(UTC+0) |          | Not answered |                      |
| 6  | Tel: 0047917162891 SA No.  | 18/08/2024 06:57:34(UTC+0) |          | Not answered |                      |
| 7  | Tel: 07917162891 SA No.    | 18/08/2024 06:57:13(UTC+0) |          | Not answered |                      |
| 8  | Tel: +447917162891 SA No.  | 17/08/2024 05:20:34(UTC+0) |          | Not answered |                      |
| 9  | From: +447917162891 SA No. | 17/08/2024 05:16:12(UTC+0) |          | Missed       |                      |
| 10 | Tel: 00447917162891 SA No. | 13/08/2024 11:52:54(UTC+0) |          | Not answered |                      |
| 11 | Tel: 07917162891 SA No.    | 13/08/2024 11:52:21(UTC+0) |          | Not answered |                      |
| 12 | Tel: 00917907025586        | 10/08/2024 04:55:58(UTC+0) |          | Not answered |                      |
| 13 | Tel: 07917162891 SA No.    | 02/08/2024 20:39:24(UTC+0) |          | Not answered |                      |
| 14 | Tel: 07917162891 SA No.    | 02/08/2024 20:38:33(UTC+0) |          | Not answered |                      |

Total: 15 Deduplication: 0 Items: 15/15 Selected: 15

Table View Folder View

September October November December January February March April May June July August September October

2025

Audio

Details

Save

Name: 20240827\_03183

Type: Audio

Size (bytes): 249975

Path: Huawei\_POT-LX1 Sounds/20240827\_03183.m4a

Created: 26/08/2024 21:48:00

Accessed: 26/08/2024 21:48:00

Modified: 26/08/2024 21:48:00

Changed: 26/08/2024 21:48:00

Deleted: 26/08/2024 21:48:00

Extraction: File System

MD5: 1d3098924c7d

Source file: 20240827\_03183

| #  | Name                | Path                                       | Size (byte) | Created            | Modified |
|----|---------------------|--------------------------------------------|-------------|--------------------|----------|
| 1  | 0wav                | Huawei_POT-LX1 P Smart.zip\data/media/0... | 2575916     | 15/08/2024 08:38:2 |          |
| 2  | 12bfe642            | Huawei_POT-LX1 P Smart.zip\data/media/0... | 50468       | 28/03/2025 15:06:3 |          |
| 3  | 20240815_110938.m4a | Huawei_POT-LX1 P Smart.zip\data/media/0... | 430063      | 15/08/2024 05:40:0 |          |
| 4  | 20240818_143500.m4a | Huawei_POT-LX1 P Smart.zip\data/media/0... | 124355      | 18/08/2024 09:05:0 |          |
| 5  | 20240818_143517.m4a | Huawei_POT-LX1 P Smart.zip\data/media/0... | 614927      | 18/08/2024 09:05:5 |          |
| 6  | 20240819_194222.m4a | Huawei_POT-LX1 P Smart.zip\data/media/0... | 149664      | 19/08/2024 14:12:3 |          |
| 7  | 20240819_194345.m4a | Huawei_POT-LX1 P Smart.zip\data/media/0... | 342801      | 19/08/2024 14:14:0 |          |
| 8  | 20240827_031811.m4a | Huawei_POT-LX1 P Smart.zip\data/media/0... | 380702      | 26/08/2024 21:48:3 |          |
| 9  | 20240827_031835.m4a | Huawei_POT-LX1 P Smart.zip\data/media/0... | 249975      | 26/08/2024 21:48:4 |          |
| 10 | 20240827_031853.m4a | Huawei_POT-LX1 P Smart.zip\data/media/0... | 359377      | 26/08/2024 21:49:1 |          |
| 11 | 20240827_031918.m4a | Huawei_POT-LX1 P Smart.zip\data/media/0... | 464030      | 26/08/2024 21:49:4 |          |
| 12 | 20240827_032019.m4a | Huawei_POT-LX1 P Smart.zip\data/media/0... | 356612      | 26/08/2024 21:50:3 |          |
| 13 | 20240827_032214.m4a | Huawei_POT-LX1 P Smart.zip\data/media/0... | 407944      | 26/08/2024 21:52:3 |          |
| 14 | 20240827_032327.m4a | Huawei_POT-LX1 P Smart.zip\data/media/0... | 253533      | 26/08/2024 21:53:4 |          |
| 15 | 20240827_072346.m4a | Huawei_POT-LX1 P Smart.zip\data/media/0... | 35415       | 27/08/2024 01:53:4 |          |
| 16 | 20240827_072732.m4a | Huawei_POT-LX1 P Smart.zip\data/media/0... | 51342       | 27/08/2024 01:57:3 |          |

Total: 61 Deduplication: 0 Items: 61/61 Selected: 61 Path: Huawei\_POT-LX1 P Smart.zip\data/media/0/Sounds/20240827\_031835.m4a

Celebrite Physical Analyzer 7.73.0.11

File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks

Search Advanced

The license expires in 14 days. [License details](#)

Locations (383) Device Locations (383) Wireless Networks (11) Contacts (13) Call Log (15) Extraction Summary (1) Images (107)

September 2024 October 2024 November 2024 December 2024 January 2025

Analysis Data

- Application (109) (1)
- Installed Applications (109)
- Calls (15)
- Call Log (15)
- Contacts (13)
- Devices & Networks (11)
- Wireless Networks (11)
- Location Related (383)
- Device Locations (383)
- Locations (383)
- Manual Data Collection (475)
- Genie: Chats (12) (382 messages)
- Genie: Contacts (424)
- Genie: Passwords (31)
- Genie: User Accounts (8)
- Media (14344)
- Audio (61)
- Images (14150) (156 known files)
- Videos (133)
- Messages (75) (1)
- Chats (4) (1) (34 messages)
- Emails (71)
- Search & Web (1157)
- Social Media (73) (73)
- User Accounts & Details (257)

Timeline

File Systems

Images

Reports

Cloud

Table with columns: #, Origin, Timestamp, End time, Position, App

| #   | Origin | Timestamp                  | End time | Position               | App |
|-----|--------|----------------------------|----------|------------------------|-----|
| 368 |        | 18/08/2024 08:59:33(UTC+0) |          | (8.782860, 76.581900)  |     |
| 369 |        | 18/08/2024 09:59:33        |          | (8.782856, 76.581871)  |     |
| 370 |        | 18/08/2024 08:59:32(UTC+0) |          | (8.782860, 76.581900)  |     |
| 371 |        | 18/08/2024 09:59:32        |          | (8.782858, 76.581871)  |     |
| 372 |        | 18/08/2024 08:59:20(UTC+0) |          | (8.782120, 76.589100)  |     |
| 373 |        | 18/08/2024 09:59:20        |          | (8.782124, 76.589096)  |     |
| 374 |        | 17/08/2024 03:43:49(UTC+0) |          |                        |     |
| 375 |        | 17/08/2024 02:29:33(UTC+0) |          |                        |     |
| 376 |        | 05/08/2024 07:19:54(UTC+0) |          | (52.516200, -2.819700) |     |
| 377 |        | 05/08/2024 07:18:04(UTC+0) |          | (52.516100, -2.819720) |     |
| 378 |        | 05/08/2024 06:18:04        |          | (52.516111, -2.819723) |     |
| 379 |        | 05/08/2024 05:41:42(UTC+0) |          | (51.501100, -3.111800) |     |
| 380 |        | 05/08/2024 04:40:26(UTC+0) |          | (51.660500, -3.848700) |     |
| 381 |        | 05/08/2024 05:40:26        |          | (51.660533, -3.848701) |     |
| 382 |        | 05/08/2024 04:40:26(UTC+0) |          | (51.660500, -3.848700) |     |
| 383 |        | 05/08/2024 05:40:20        |          | (51.660533, -3.848701) |     |

Extraction Summary (1)

End time: 05/08/2024 05:40:20

Position: (52.516111, -2.819723)

Aggregated locations:

Map Address: Map Address

Position: Position

Confidence: Confidence

Map: Map

Category: Media Locations

Source: Source

Account: Account

Address: Address

Service Identifier: Service Identifier

Extraction: Extraction

Manually decoded: Manually decoded

Source file: Source file

Source: Source

Images

Details

Events (0)

SW → MIA

17°C Mostly cloudy 14:46 16/04/2025

Celebrite Physical Analyzer 7.73.0.11

File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks

Search Advanced

The license expires in 14 days. [License details](#)

Social Media (73) Emails (71) Chat (Chats) (4) Videos (133) Images (14150) Audio (61) Genie: User Accounts (8) Genie: Passwords (31)

Sun, 24 Mon, 25 Tue, 26 Wed, 27 Thu, 28 Fri, 29 Sat, 30 Sun, 1 Mon, 2 Tue, 3 Wed, 4 Thu, 5 Fri, 6 Sat, 7 Sun, 8 Mon, 9

Analysis Data

- Contacts (13)
- Devices & Networks (11)
- Wireless Networks (11)
- Device Locations (383)
- Locations (383)
- Manual Data Collection (475)
- Genie: Chats (12) (382 messages)
- Genie: Contacts (424)
- Genie: Passwords (31)
- Genie: User Accounts (8)
- Media (14344)
- Audio (61)
- Images (14150) (156 known files)
- Videos (133)
- Messages (75) (1)
- Chats (4) (1) (34 messages)
- Emails (71)
- Search & Web (1157)
- Social Media (73) (73)
- User Accounts & Details (257)

Timeline

File Systems

Images

Reports

Cloud

Table with columns: #, Author, Body, Title, Created

| #  | Author                | Body | Title            | Created                    |
|----|-----------------------|------|------------------|----------------------------|
| 10 | new-terrance Terrence |      | Terrence's story | 07/12/2024 19:52:20(UTC+0) |
| 11 | new-terrance Terrence |      | Terrence's story | 07/12/2024 19:52:20(UTC+0) |
| 12 | new-terrance Terrence |      | Terrence's story | 07/12/2024 19:51:11(UTC+0) |
| 13 | new-terrance Terrence |      | Terrence's story | 07/12/2024 19:51:11(UTC+0) |
| 14 | new-terrance Terrence |      | Terrence's story | 07/12/2024 19:51:11(UTC+0) |
| 15 | new-terrance Terrence |      | Terrence's story | 07/12/2024 19:51:11(UTC+0) |
| 16 | new-terrance Terrence |      | Terrence's story | 07/12/2024 19:40:10(UTC+0) |
| 17 | new-terrance Terrence |      | Terrence's story | 07/12/2024 19:39:01(UTC+0) |
| 18 | new-terrance Terrence |      | Terrence's story | 07/12/2024 19:37:07(UTC+0) |
| 19 | new-terrance Terrence |      | Terrence's story | 07/12/2024 19:37:07(UTC+0) |
| 20 | new-terrance Terrence |      | Terrence's story | 07/12/2024 19:35:48(UTC+0) |
| 21 | new-terrance Terrence |      | Terrence's story | 07/12/2024 19:35:48(UTC+0) |

Extraction Summary (1)

Source: Snapchat

Account: pater\_dover

Author: new-terrance Terrence

Title: Terrence's story

Created: 07/12/2024 19:40:10(UTC+0)

Platform: Platform

Position: Position

Reactions: Reactions

Comments: Comments

Status: Status

Type: Type

URL: URL

Privacy: Privacy

Extraction: File System

Source file: Source file

Source: Source

Attachments (0)

17°C Mostly cloudy 14:46 16/04/2025

