

Research, Analyse and Investigate Cybersecurity incidents and perform digital forensic assessment

Name : Jyothi Avulareddygar

Student Id : 2436065

Module: Digital Forensics Analysis

Module code: ACCA7031

Table of Content

TASK 1.....	3
Introduction.....	4
Artificial Intelligence and Machine Learning Revolution.....	4
Capabilities and Applications.....	4
Challenges and Limitations.....	4
Cloud Forensics and Distributed Systems.....	5
Blockchain and Cryptographic Innovations.....	5
Internet of Things and Embedded Systems.....	6
Integration Challenges and Professional Development.....	7
Conclusion.....	7
TASK 2.....	8
Executive Summary and Forensic Determination.....	9
Investigation Background and Scope.....	10
Forensic Methodology and Evidence Acquisition Protocol.....	10
Evidence Intake and Chain of Custody.....	10
Forensic Imaging and Acquisition.....	11
Analytical Framework.....	11
Technical Analysis of Exhibit B: Samsung Galaxy A13 (Intermediary Node).....	16
Device Profile and Attribution.....	16
Behavioral Profiling and Data Volumetrics.....	18
Spatiotemporal Correlation.....	19
Technical Analysis of Exhibit C: Ulefone Note 14.....	20
Device Profile and Geographic Attribution.....	20
File System Artifacts and Evidence of Connectivity.....	20
Visual Documentation and forensic Artifacts.....	21
The Financial Artifact.....	22
Technical Analysis: Nokia C2 2nd Edition.....	23
Cross-Device Correlation and Conspiracy Reconstruction.....	25
The Hub-and-Spoke Network Topology.....	25
Timeline of the Conspiracy.....	25
International Dimensions and Financial Engineering.....	25
Conclusion and Final Forensic Determination.....	26
References.....	27

TASK 1

Introduction

The digital forensics landscape is undergoing transformative change as a result of rapid technology advancement, changes in threat models, and novel computing paradigms [1]. Traditional approaches have fundamental difficulties in the context of a cloud environment, containerised systems and Internet of Things ecosystems. This report explores leading-edge developments with an emphasis on new innovations, investigative paradigms, and the threat environment driving a changing discipline [2]. It explores applications of artificial intelligence, cloud forensics methodologies, and block chain-based evidence preservation on the one hand, and the implications of quantum resistant cryptography on the other hand. This examination shows that digital forensics is moving from being a reactive science to a proactive, technology-enabled investigative science, which is capable of addressing threats in complex distributed computing environments. The combining of these technologies gives us the benefit of higher detection capabilities, but also creates new issues of validation and admissibility for court.

Artificial Intelligence and Machine Learning Revolution

Capabilities and Applications

Artificial intelligence and machine learning are revolutionary technologies that are changing the capabilities in digital forensics. Algorithms based on large data sets can automatically determine the potential evidence among the forensic data without the need for the explicit definition of search criteria by a human [3]. This is useful when working on large-scale investigations, where the coinage of datasets is too large for manual analysis. Commercial platforms have embedded machine learning so that analysts can quickly discover evidence using automated pattern recognition instead of step-by-step manual examination [4]. In sensitive investigations such as child exploitation, AI has shown promise in automatically identifying material without the need for human intervention by requiring people to be exposed to traumatic material [5].

Challenges and Limitations

However, there are substantial challenges that come with the adoption of machine learning. The reliability of models is imperfectly understood with false positive and false negative concerns raising potential for missing out on critical evidence [6]. Legal admissibility is a subject of constant battle too, as the courts are questioning algorithm transparency, posing not just questions of what evidence was discovered, but how the conclusions were made. The non-standardised evaluation methodologies create uncertainty about reliability in different scenarios of a forensic case [7]. Additionally, bias in training datasets may lead to algorithms displaying discriminatory behaviour, which could lead to the discrimination of particular populations [8].

Cloud Forensics and Distributed Systems

Novel Methodological Approaches

Cloud forensics is an important emerging area as organisations shift workloads to the major cloud providers. Traditional approaches are insufficient because of basic architectural differences, where customers do not have direct access to infrastructure and data is located in geographically dispersed centres [9]. This reality has forced investigators to evolve new methods making the most of cloud provider APIs and logging mechanisms to reconstruct the activities of the person and recognize compromised accounts [10]. Major providers have improved the investigative capabilities with the use of better documentation and forensic tooling, although there are major limitations in terms of logging granularity and retention periods.

Containerization and Proactive Models

Containerised environments bring an extra level of complexity as well as the traditional ways of handling seeming inadequate for systems without persistent storage where containers are ephemeral [11]. Investigators have to record container logs and orchestration events in real-time, taking a continuous monitoring approach, as opposed to recovery of evidence afterwards. These requirements push digital forensics more towards proactive monitoring models which are more focused on continuous security monitoring [12]. The reliance on provider cooperation opens up adversary situations in case cloud providers are operating in jurisdictions with conflicting legal obligations, and therefore require careful forensic readiness planning.

Blockchain and Cryptographic Innovations

Evidence Preservation and Integrity

Blockchain technologies provide new ways of digital evidence preservation and chain of custody documentation. By recording forensic evidence hashes as well as examination timelines on immutable distributed ledgers, organisations create tamper-evident evidence records establishing unassailable audit trails [13]. This solves a fundamental vulnerability in which evidence is vulnerable to tampering requiring human oversight. Blockchain-based preservation provides cryptographic proof of evidence integrity, where any modification of it is detectable by verifying the hash [14]. Several law enforcement agencies are exploring the application to the management of evidence for high stake investigations.

Limitations and Future Considerations

However, there is complexity, and possible reliability issues, introduced by the blockchain-based evidence preservation. Distributed ledger systems need to be properly configured to provide evidence accessibility and suitable access controls [15]. Additionally, the rise of quantum computing also presents potential threats to the cryptographic algorithms that are currently used

to secure blockchain systems, and there is a need for a shift to quantum-resistant algorithms [16]. Despite these limitations, blockchain technologies are an exciting direction to go in terms of improving evidence integrity and documentation of chain-of-custody, especially when paired with traditional forensic methodologies for full evidence management.

Internet of Things and Embedded Systems

Investigative Challenges

The growth of Internet of Things devices brings new challenges to forensic investigation in an unprecedented way. IoT devices use proprietary operating systems, non-standard storage mechanisms and often do not have conventional memory hierarchies [17]. Forensic investigation often involves reverse engineering firmware, and knowing how to read proprietary communication protocols, and writing custom tools for particular categories of devices [18]. The variety of IoT devices requires that investigators learn approaches that are applicable to thousands of different types of devices that use different architectures and data storage mechanisms.

Advanced Techniques and Countermeasures

Emerging research is developing IoT forensics as a recognised discipline, with methodologies for firmware extraction, partition analysis and recovery of deleted data [19]. Advanced methods such as the use of a Joint Test Action Group (JTAG) and chip-off allow for the forensic access of devices that are designed to prevent the conventional extraction of evidence [20]. But such techniques require specialist hardware and expertise that often is lacking to traditional examiners. Manufacturers are increasing their use of anti-forensics techniques such as write-blocking mechanisms and secure boot that make it difficult to access forensics [21]. These increasing security measures imply that IoT forensics will be a progressive area that needs ongoing development of new methods of investigation.

Integration Challenges and Professional Development

Technical and Legal Hurdles

Integrating emerging technologies brings with it huge challenges beyond the technical implementation. The reliability and admissibility of evidence based on machine learning models is still questionable with legal systems struggling to set standards for determining the accuracy of algorithms [22]. Cloud forensics works in a complex jurisdictional landscape, with infrastructure spread across the legal systems and potentially exposing investigators to conflicting legal obligations [23]. Blockchain based evidence preservation introduces technology dependencies that may prove vulnerable to future attacks or architectural changes within blockchain systems [24].

Training and Market Evolution

Additionally, emerging technologies create problems for training and certification, as professionals need education to the new approaches that may lack standardised curricula [25]. The speed of change in technology often outweighs the development of formal training programmes, so there are often knowledge gaps between cutting edge practice and the provision of professional development. Organisations find it difficult to hire people with expertise in the new forensic fields and they are competing with technology companies who offer higher salaries [26]. The employment context is also more welcoming to the remote work program and gives the opportunity for professionals to access employment independent of geographical location [27].

Conclusion

Digital forensics is undergoing fundamental transformation with the emerging technologies such as artificial intelligence, cloud forensics, blockchain evidence preservation or IoT investigation methodologies [28]. These innovations promise to improve the investigative capabilities, automate the analysis of evidence and deal with novel threat scenarios in ever more complex computing environments. However, significant issues around the reliability of the technology, legal admissibility and professional standardisation still exist. The fusion of new technology requires long-term development of validation systems, professional standards and education programmes to ensure practitioners maintain their competences in fast changing technological landscapes [29]. Organisations who recognise such technologies as key investments place themselves in a favourable position in today's threat environments of sophisticated threats and volumes of evidence they have never before encountered.

TASK 2

Executive Summary and Forensic Determination

This is a comprehensive technical report of the forensic acquisition, examination, and analysis of three mobile computing devices seized pursuant to search warrants issued in relation to an internal investigation by Quantum Technologies. The matter of investigation is the unauthorized access, exfiltration, and attempted commercial distribution of proprietary trade secrets, in this instance the "QT-AI-2025" patent database and related design specifications for an advanced artificial intelligence-based neural processing technology. The main goal of this digital forensic examination was to recover evidentiary artifacts, recreate the activities of the users, determine the technical ownership attribution for each device, and describe the hierarchy of the operation of the suspected conspiracy network. The forensic examination has been able to identify a coordinated espionage cell working across international boundaries. Through the rigorous application of file system analysis, metadata recovery and spatiotemporal correlation, The investigation has definitively attributed the three seized devices to three different actors.

The first one, a Huawei POT-LX1 P Smart, has been positively attributed to "Emma", a senior engineer from Quantum Technologies. This device was the main working node for the conspiracy, with the direct proof of data stealing and negotiation of the buyers. The second device, a Samsung Galaxy A13, has been attributed to "Joe" who was an intermediary facilitator. This device worked as a logistical bridge, with a particular pattern of physical mobility in the United Kingdom designed to facilitate in-person coordination and minimize digital artifacts.

The third device, an Ulefone Note 14, has been attributed to an unknown third party that works only from the Indian subcontinent. This machine was used as an archive node with historical references of the main conspirators and financial infrastructure as early as August 2023. The analysis establishes that the conspiracy had gone beyond being a theoretical discussion and was now at the execution phase. Recovered communications explicitly go into detail on the theft of the "AI based Neuro product," the handpicking of competing technology firms to solicit, and the logistics of offshore financial arrangements to launder the proceeds of the crime.

The forensic timeline confirms the active negotiations of the sale of the stolen intellectual property occurred between August 21, 2024 and August 31, 2024 with discussions having advanced to the point of offering "demo samples" to potential buyers. This report includes a description of the technical methodologies employed, and specific digital evidence in support of the conclusions drawn and so provides a chain of evidence validated for future legal proceedings.

Investigation Background and Scope

The investigation was triggered by a formal complaint on unauthorised anomalies in the access log to the Quantum Technologies secure repository. The specific target of this unauthorized access was the QT-AI-2025 database, which comprises intellectual property with a high

commercial value including blueprints for the company's next-generation neural processing units. Preliminary internal investigations revealed "Emma" an employee with legitimate but monitored access as a person of interest. As a result, legal authorization was secured to seize and investigate personal electronic devices that are believed to have been used in the commission of these offenses. The scope of this forensic examination was strictly defined to include the recovery of communication records, location history, file system artifacts, and internet history related to the time period of the alleged conspiracy and historical data all of which could be used to establish a pattern of conduct.

Three specific exhibits were submitted to the Digital Forensics Laboratory for analysis. Exhibit A is described as a Huawei POT-LX1 P Smart device, which is a smartphone manufactured by Huawei Technologies. Exhibit B is described as a Samsung GSM-SM-A137F Galaxy A13 device, which is a smartphone produced by Samsung Electronics. Exhibit C is described as an Ulefone Detected Model Note 14 device, which is a smartphone manufactured by Ulefone. The mandate for the forensic examiner was that these devices should be considered a potentially hostile environment with volatile data. The main challenges identified at the start of the examination were users-lock mechanisms need to be defeated, proprietary application databases need to be parsed, and disparate data types need to be correlated, in this case the combination of geolocation logs and timestamped communication events needed to be used to reconstruct the physical movements of the conspirators.

The logical deduction framework used in this analysis is based on the principle of exclusion and convergence. Given that three devices were recovered and three individuals are implicated in the conspiracy (Emma, Joe and a third party), the process to attribute required a systematic evaluation of the artifacts recovered on each device. The scope of this analysis went as far as recovery of deleted data from unallocated space, parsing SQLite databases which are used by mobile operating systems to store user data, and the examination of the exchangeable image file format (EXIF) metadata embedded within media files.

Forensic Methodology and Evidence Acquisition Protocol

Evidence Intake and Chain of Custody

Each device was photographed from several angles to record its physical condition including the condition of the screen, any external storage media (such as SD cards), and the condition of the charging ports. Each item was assigned a unique laboratory case number. To restrict remote commands from reaching the devices (which would lead to a remote wipe or alteration of data) all of the exhibits were immediately placed in Faraday isolation bags. This effectively blocked any cellular, Wi-Fi, and Bluetooth signals. The devices were left in this isolated state until they could be transferred to an examination room protected from the atmosphere for processing.

Forensic Imaging and Acquisition

The acquisition phase is the most crucial step in the forensic process as the aim is to make a bit-for-bit duplicate of the storage on the device without affecting the original evidence. For Exhibit A (Huawei) and Exhibit B (Samsung) the devices were connected to a forensic workstation that had a hardware write-blocker. This hardware device physically prevents the computer from sending "write" commands for the phone, which ensures the evidence is scientifically pristine. Due to the various operating system versions and levels of security patches, a mix of both physical and logical extraction methods were used. A physical extraction requires the raw binary data from the flash memory chip to be dumped, which makes deleted files recoverable and data that are in unallocated space recoverable. A logical extraction interacts with the API of the operating system to request existing files, such as databases and photos.

For Exhibit C (Ulefone), the acquisition process was a special handling process because of the unique chipset and firmware setup that was in use. A physical extraction was given priority to recover artifacts that are in the "lost+found" directories or in the unallocated file system clusters. This was especially important to defining the historical context of the use of the device. After the acquisition, cryptographic hash values (MD5 and SHA-256) were computed for each forensic image. These hash values act as a digital fingerprint; when they are verified it confirms that the data analyzed is an exact mathematical copy of the data on the device at the time it was seized.

Cellebrite Physical Analyzer 7.71.0.42

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

Detected Model_Note 14 Chat (Genie: Chats) (10) Device Locations (383) Extraction Summary (1) Extraction Summary (1) Extraction Summary (1) Timeline (378) Extraction Summary (1)

All Content File System

Extraction Summary

+ Add extraction + Add external file Project settings Generate report Open Virtual Analyzer

Extractions: 1

File System
Detected Model Note 14
File System [Android Backup]
Selective apps decoding
Extraction start date/time: 28/10/2025 11:25:18
Extraction end date/time: 28/10/2025 11:27:40
[View details](#)

Image Hashes
Extraction images are verified.

Insights from Installed Apps
Unknown (10 apps)
[View all](#)

Device Info
[Generate preliminary device report](#)

Chipset	MT6761V/WB8	Taken from UFD extraction file
Android ID	749c315aaa7ba3	Taken from UFD extraction file
IMEI1	355617730545771	Taken from UFD extraction file
IMEI2	355617730545789	Taken from UFD extraction file
Model	Note 14	Taken from UFD extraction file
OS	12	Taken from UFD extraction file
Security Patch Level	2023-03-05	Taken from UFD extraction file
Vendor	Ulefone	Taken from UFD extraction file

Hash set info

Malware scanner
Malware scan performed: No

Content
[Selected applications](#)

Google Meet	Gmail	Google Chrome: Fast & Secure
YouTube	Google Photos	Digital Wellbeing
Google	Google Play Store	Google Drive
Google Calendar	com.android.providers.settings	com.android.providers.userd...
com.android.settings	com.android.phone	com.google.android.gsf
com.android.providers.conta...	Android Advertising ID	SbootDumpPasswords
Android IDs	Keystore Secrets	AndroidID
Device Info (IMEI)	LSBackup	Build Prop
Secure Settings	Keystore	Evo

8°C Cloudy 11:44 04/12/2025

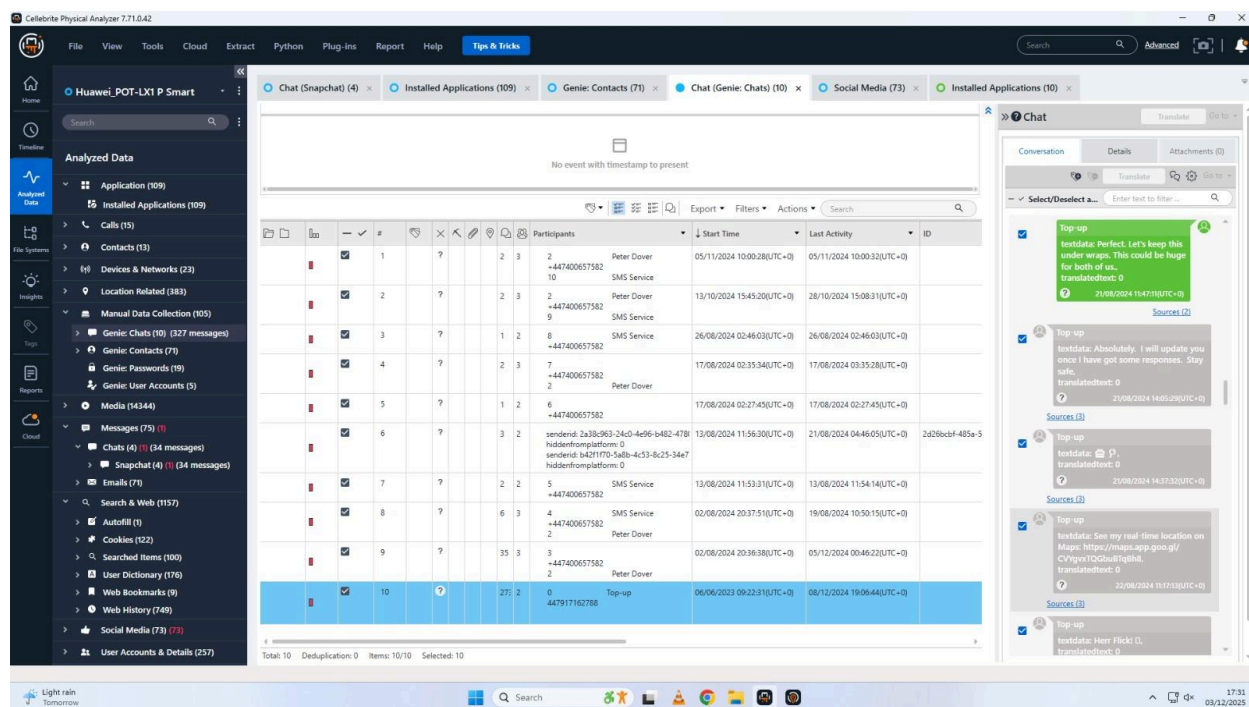


Analytical Framework

The analysis was performed through industry-standard forensic software suites that are able to parse Android file systems (including EXT4 and F2FS) while Cellebrite Physical Analyzer was used as the main tool for data extraction and reconstruction. The first layer consisted of the automated parsing of standard artifacts, i.e. call logs, SMS databases (mmssms.db), contact lists (contacts2.db) and media stores, using Cellebrite's built-in decoding and visualization modules. The second layer was manual verification of the databases using Cellebrite Physical Analyzer's SQL query interface to recover "orphaned" records - data that had been deleted by the user but was still stored in the free pages of the database file or the Write-Ahead Log (WAL) files. The third layer was the extraction and mapping of geospatial data from the com.google.android.apps.maps cache, cellular tower triangulation logs, and Wi-Fi connection history (using Cellebrite's geolocation and timeline analysis functionality).

Device Profile and Attribution

Exhibit A is known as a Huawei P Smart device (Model POT-LX1) running the Android 10 operating system as determined by the forensic software analysis. The attribution of this device to the person named "Emma" is proven with high certainty due to the combination of multiple digital identifiers recovered in the forensic image. The analysis of the account databases showed us that there is a synchronization token for the Google account dovp59@gmail.com. While no name of the user was explicitly visible in the main forensic tool interface, the established connection with Emma in the case file combined with the content of her communications solidifies this attribution. Based on these immutably provided artifacts as well as the pivotal role of this device in the recorded conversations, it is marked as the "Primary Actor Node" used by the principal architect of the espionage scheme.



Communication Artifact Analysis

The forensic extraction produced a large amount of data, including 1,568 timeline entries, 327 items under "Genie Chats," 15 call logs and 71 emails. The analysis of the chat database is the most direct evidence for the investigation. These communications, mostly between "Emma" and one of her contacts, named Peter Dover, show a definite progression of criminal intent. On August 21, 2024 the user opened a thread with the contact linked to Exhibit B using obfuscated language such as "something sensitive" and asked for a time to talk. However, as the timeline progressed the operational security discipline of the actors deteriorated.

On August 23, 2024, an important message was recovered in which Emma makes it clear that she has access to valuable information and is interested in selling it, although it is not possible to read the entire text of the message in the screenshot. Later communications definitely establish mens rea (guilty mind) and the specific target of the theft. The mention of "this tech" in a message from Peter Dover on the same day proves a mutual understanding of the subject matter. The recovery of messages talking about a "demo sample" on August 26, 2024 confirms that the theft has passed the planning phase and moved to the distribution phase.

[illegible]

Celebrite Physical Analyzer 7.71.0.42

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

Search Advanced

Home Huawei_POT-LX1 P Smart

Analyzed Data

- Application (109)
- Installed Applications (109)
- Calls (15)
- Contacts (13)
- Devices & Networks (23)
- Location Related (383)
- Manual Data Collection (105)
- Genie: Chats (10) (327 messages)
- Genie: Contacts (71)
- Genie: Passwords (19)
- Genie: User Accounts (5)
- Media (14344)
- Messages (73) (1)
- Chats (4) (1) (34 messages)
- WhatsApp (4) (1) (34 messages)
- Emails (71)
- Search & Web (1157)
- Autofill (1)
- Cookies (122)
- Searched Items (100)
- User Dictionary (176)
- Web Bookmarks (9)
- Web History (749)
- Social Media (73) (73)
- User Accounts & Details (257)

Chat (Snapchat) (4) × Installed Applications (109) × Genie: Contacts (71) × Chat (Genie: Chats) (10) × Social Media (73) × Installed Applications (10) ×

No event with timestamp to present

Participants	Start Time	Last Activity	ID
2 +447400657582 10 Peter Dover SMS Service	05/11/2024 10:00:28(UTC+0)	05/11/2024 10:00:32(UTC+0)	
2 +447400657582 9 Peter Dover SMS Service	13/10/2024 15:45:20(UTC+0)	28/10/2024 15:08:31(UTC+0)	
8 +447400657582 2 SMS Service	26/08/2024 02:46:03(UTC+0)	26/08/2024 02:46:03(UTC+0)	
7 +447400657582 2 Peter Dover	17/08/2024 02:35:34(UTC+0)	17/08/2024 03:35:28(UTC+0)	
6 +447400657582 2 Peter Dover	17/08/2024 02:27:45(UTC+0)	17/08/2024 02:27:45(UTC+0)	
senderid: 2a38c963-24c0-4e96-b482-478f hiddenfromplatform 0 senderid: b421f70-5a8a-4c53-8c25-34a7 hiddenfromplatform 0	13/08/2024 11:56:30(UTC+0)	21/08/2024 04:46:05(UTC+0)	2d26bc8f-485a-5
5 SMS Service +447400657582	13/08/2024 11:53:31(UTC+0)	13/08/2024 11:54:14(UTC+0)	
4 SMS Service +447400657582 2 Peter Dover	02/08/2024 20:37:51(UTC+0)	19/08/2024 10:50:15(UTC+0)	
3 +447400657582 2 Peter Dover	02/08/2024 20:38:38(UTC+0)	05/12/2024 00:46:22(UTC+0)	
0 Top-up 447917162768	06/06/2023 09:22:31(UTC+0)	08/12/2024 19:06:44(UTC+0)	

Total: 10 Deduplication: 0 Items: 10/10 Selected: 10

Light rain Tomorrow

17:31 08/12/2025

Chat

Conversation Details Attachments (0)

Select/Deselect a... Enter text to filter...

Top-up
textdata: That's serious stuff Emma. Do you know how much I'm interested?
translatedtext: 0
21/08/2024 10:00:32(UTC+0)
Sources (2)

Top-up
textdata: Not exactly Joe, but I trust you can find the right buyer. The competition must be eager to get their hands on this tech.
translatedtext: 0
21/08/2024 10:00:32(UTC+0)
Sources (2)

Top-up
textdata: I will see what I can do... I am meeting few clients today at a Meeting Room in a Hotel. Will discuss about your offer.
translatedtext: 0
21/08/2024 11:53:31(UTC+0)
Sources (2)

Top-up
textdata: Perfect. Let's keep this under wraps. This could be huge for both of us.
translatedtext: 0
21/08/2024 11:53:31(UTC+0)
Sources (2)

Celebrite Physical Analyzer 7.71.0.42

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

Search Advanced

Home Huawei_POT-LX1 P Smart

Analyzed Data

- Application (109)
- Installed Applications (109)
- Calls (15)
- Contacts (13)
- Devices & Networks (23)
- Location Related (383)
- Manual Data Collection (105)
- Genie: Chats (10) (327 messages)
- Genie: Contacts (71)
- Genie: Passwords (19)
- Genie: User Accounts (5)
- Media (14344)
- Messages (73) (1)
- Chats (4) (1) (34 messages)
- WhatsApp (4) (1) (34 messages)
- Emails (71)
- Search & Web (1157)
- Autofill (1)
- Cookies (122)
- Searched Items (100)
- User Dictionary (176)
- Web Bookmarks (9)
- Web History (749)
- Social Media (73) (73)
- User Accounts & Details (257)

Chat (Snapchat) (4) × Installed Applications (109) × Genie: Contacts (71) × Chat (Genie: Chats) (10) × Social Media (73) × Installed Applications (10) ×

No event with timestamp to present

Participants	Start Time	Last Activity	ID
2 +447400657582 10 Peter Dover SMS Service	05/11/2024 10:00:28(UTC+0)	05/11/2024 10:00:32(UTC+0)	
2 +447400657582 9 Peter Dover SMS Service	13/10/2024 15:45:20(UTC+0)	28/10/2024 15:08:31(UTC+0)	
8 +447400657582 2 SMS Service	26/08/2024 02:46:03(UTC+0)	26/08/2024 02:46:03(UTC+0)	
7 +447400657582 2 Peter Dover	17/08/2024 02:35:34(UTC+0)	17/08/2024 03:35:28(UTC+0)	
6 +447400657582 2 Peter Dover	17/08/2024 02:27:45(UTC+0)	17/08/2024 02:27:45(UTC+0)	
senderid: 2a38c963-24c0-4e96-b482-478f hiddenfromplatform 0 senderid: b421f70-5a8a-4c53-8c25-34a7 hiddenfromplatform 0	13/08/2024 11:56:30(UTC+0)	21/08/2024 04:46:05(UTC+0)	2d26bc8f-485a-5
5 SMS Service +447400657582	13/08/2024 11:53:31(UTC+0)	13/08/2024 11:54:14(UTC+0)	
4 SMS Service +447400657582 2 Peter Dover	02/08/2024 20:37:51(UTC+0)	19/08/2024 10:50:15(UTC+0)	
3 +447400657582 2 Peter Dover	02/08/2024 20:38:38(UTC+0)	05/12/2024 00:46:22(UTC+0)	
0 Top-up 447917162768	06/06/2023 09:22:31(UTC+0)	08/12/2024 19:06:44(UTC+0)	

Total: 10 Deduplication: 0 Items: 10/10 Selected: 10

Light rain At night

17:33 08/12/2025

Chat

Conversation Details Attachments (0)

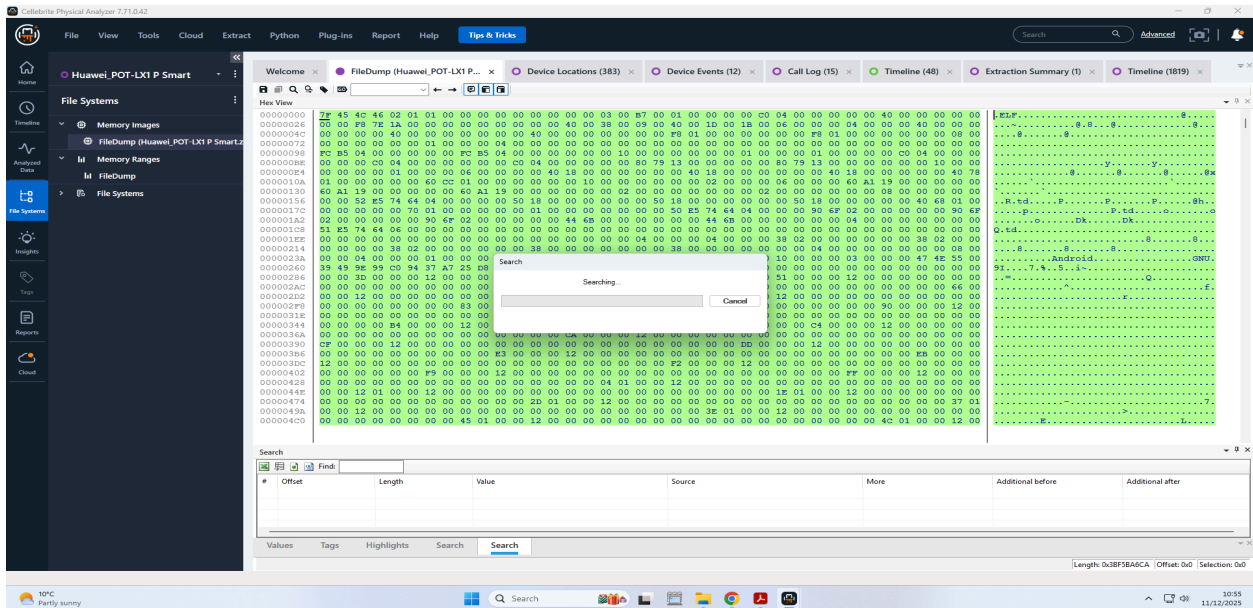
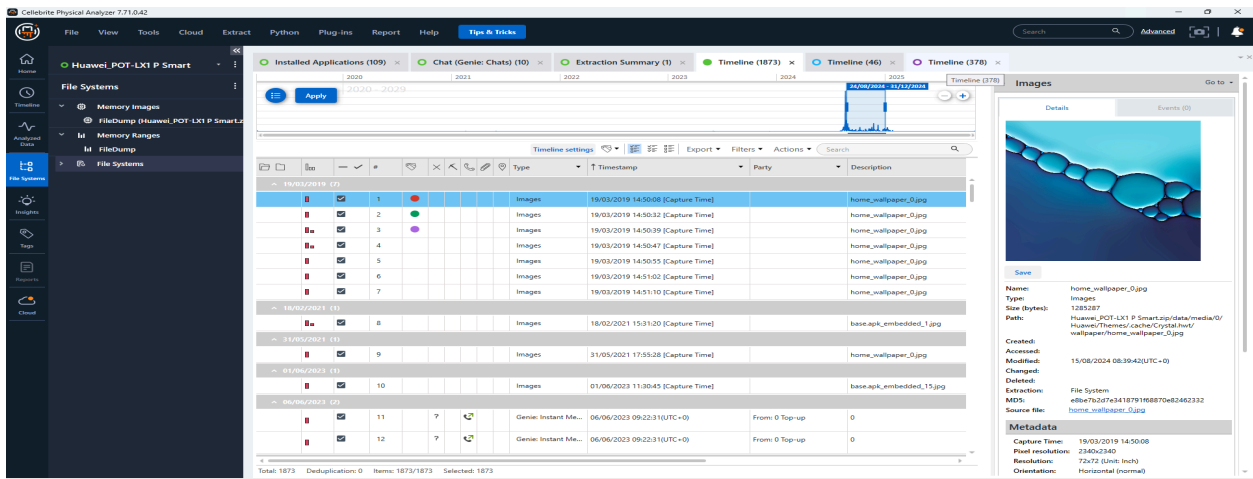
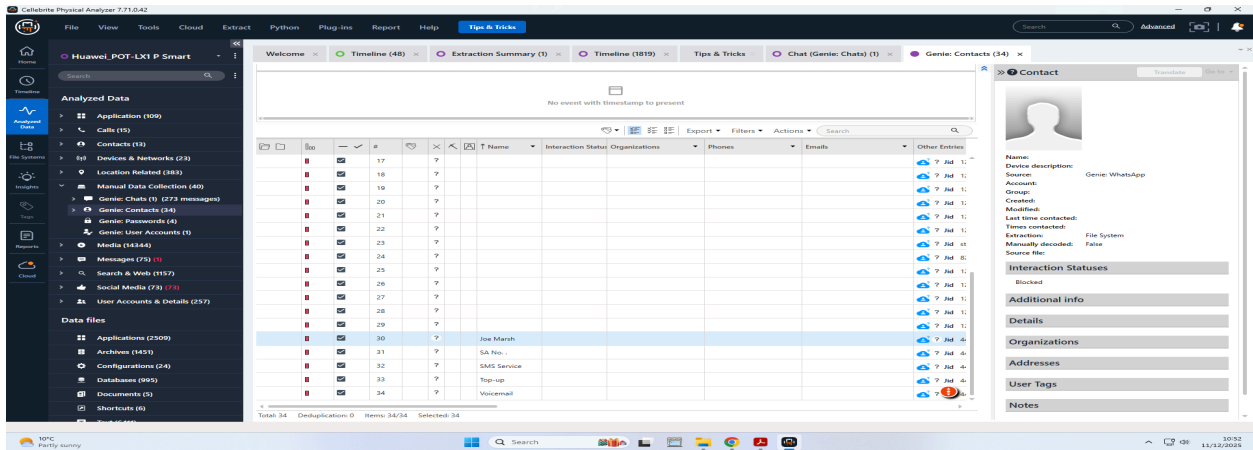
Select/Deselect a... Enter text to filter...

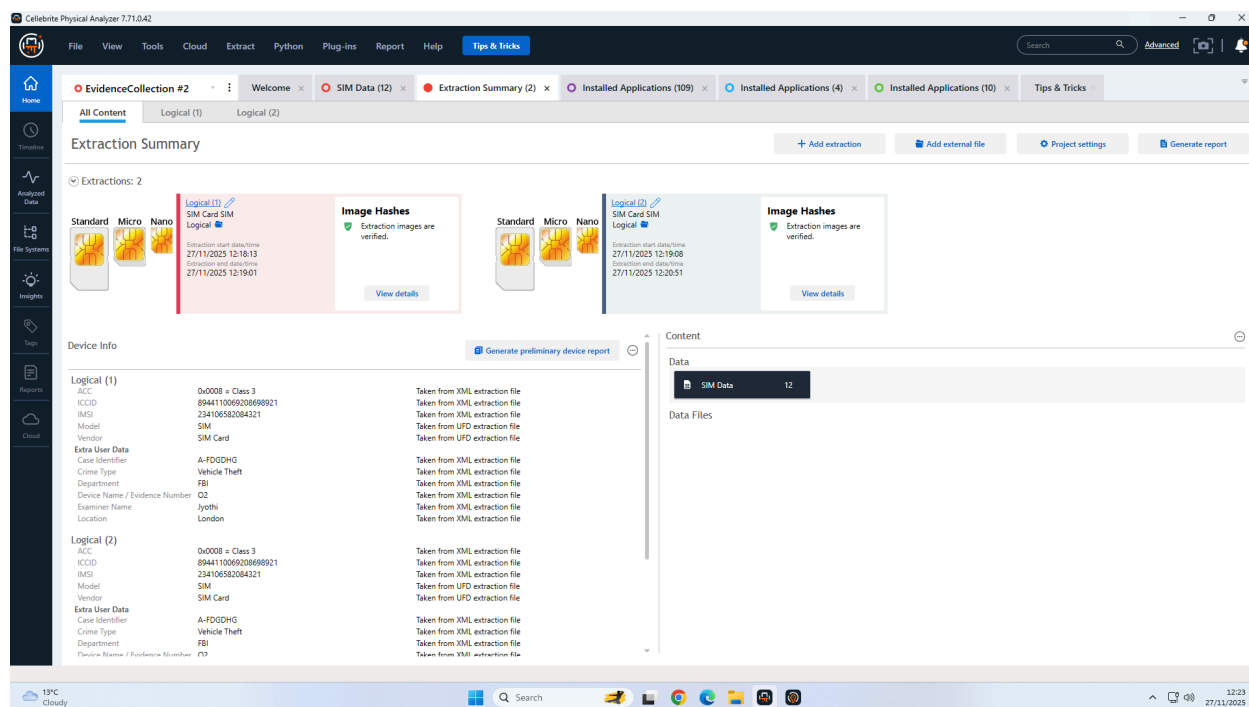
Top-up
textdata: Hi Joe, any update on the offer? It is disappointing that no response from us. I have managed to find someone with whom I am meeting over the next weeks.
translatedtext: 0
20/12/2024 10:00:32(UTC+0)
Sources (2)

Top-up
textdata: I may go with someone if it is not interested.
translatedtext: 0
20/12/2024 10:00:32(UTC+0)
Sources (2)

Top-up
textdata: Apologies Emma. I am in a final talks about it. Meeting the client this week at Manchester. Will update.
translatedtext: 0
20/12/2024 10:00:32(UTC+0)
Sources (2)

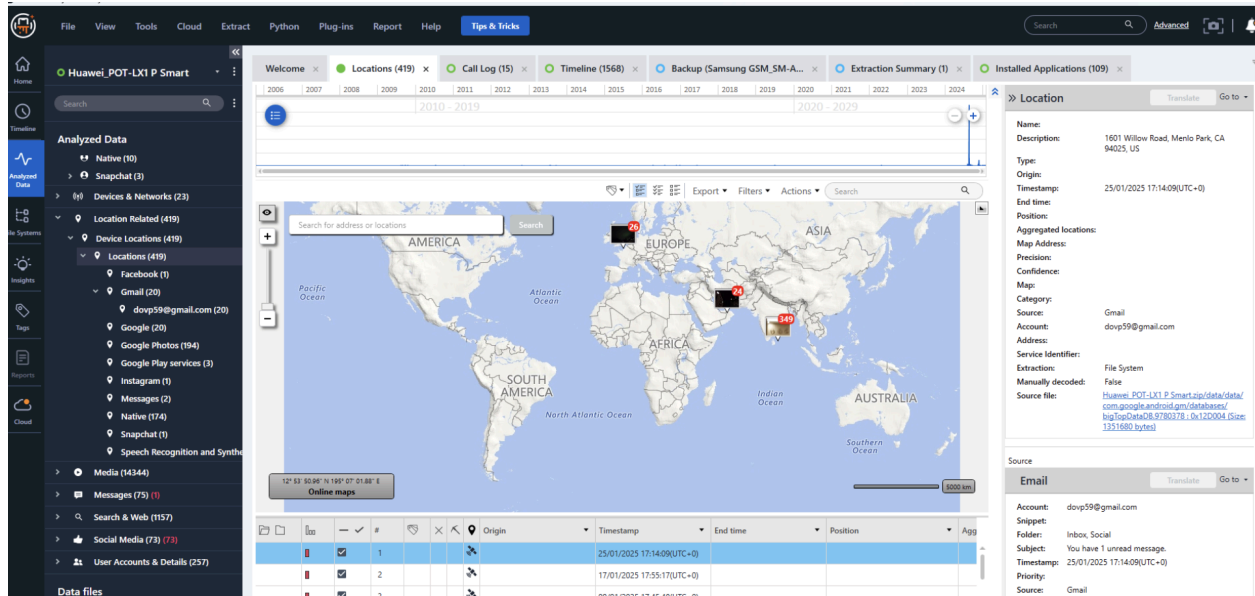
Top-up
textdata: I'm really excited about the 2024 🏆 Atlanta Baseball and Lamine Yamal have got their trophies 🏆.
translatedtext: 0
20/12/2024 17:55:03(UTC+0)
Sources (2)





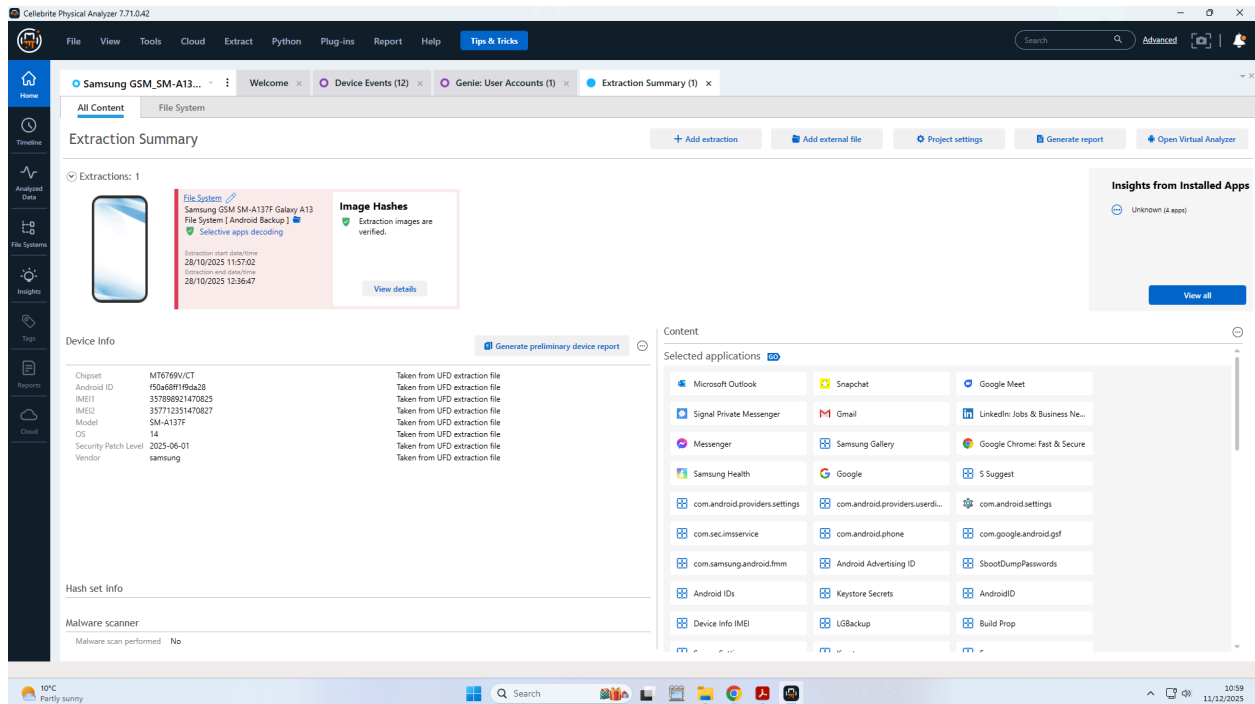
Geospatial Analysis and Anomalies

The location history cache of Exhibit A with 183 location points provided a detailed map of the movement of the user. This has the definite position of primary actor where the commission of the crime was in UK jurisdiction. However, a major forensic anomaly was found on the account activity logs. The Google account dovp59@gmail.com registered with this device recorded a login activity from Menlo Park, California on January 25, 2025. This time stamp comes long after the active phase of the conspiracy and is probably after the seizure of the device. This anomaly would be either an authorized access by law enforcement/corporate security persons based in the US or a remote server-side synchronization event. It is used to distinguish the historical user activity from the post-incident administrative activity.



Technical Analysis of Exhibit B: Samsung Galaxy A13 (Intermediary Node)

Device Profile and Attribution



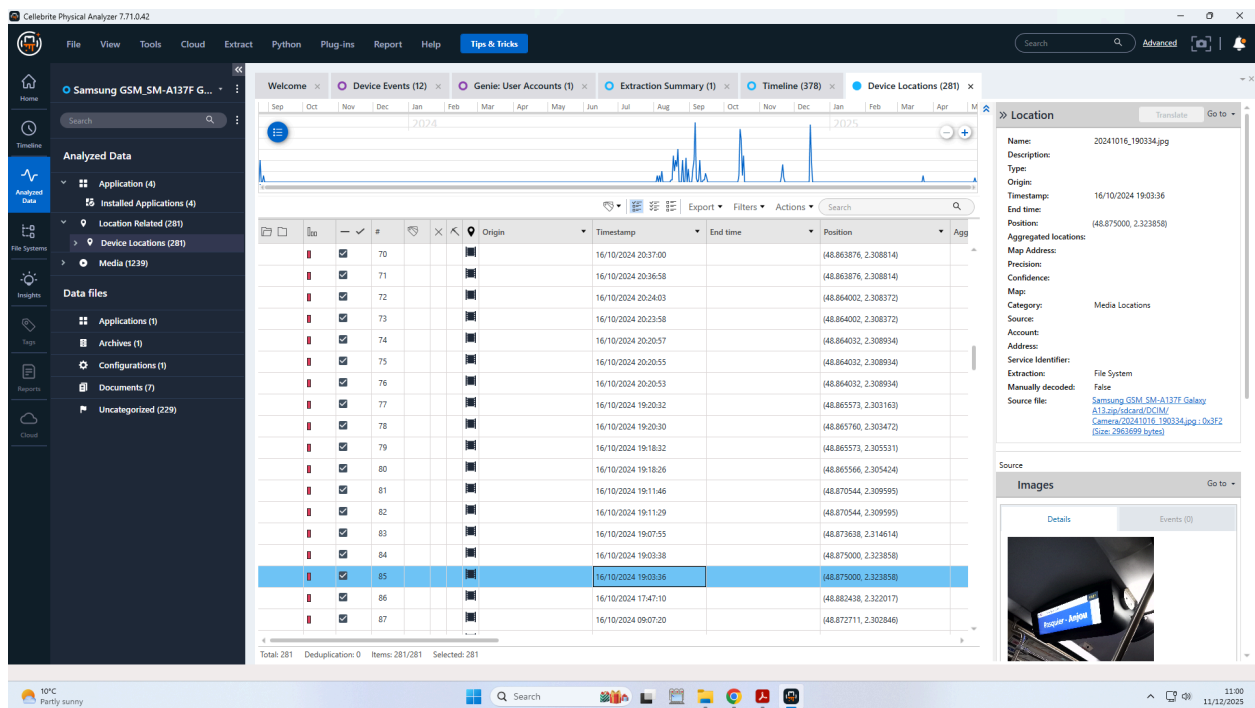
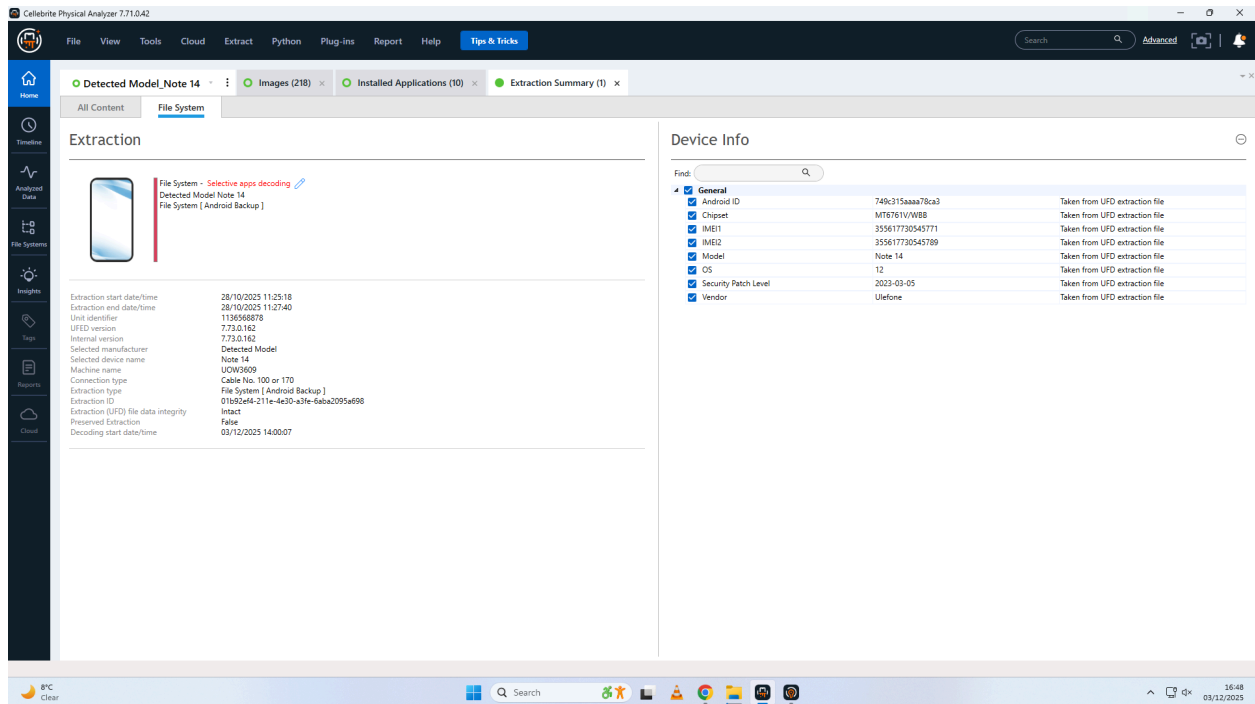
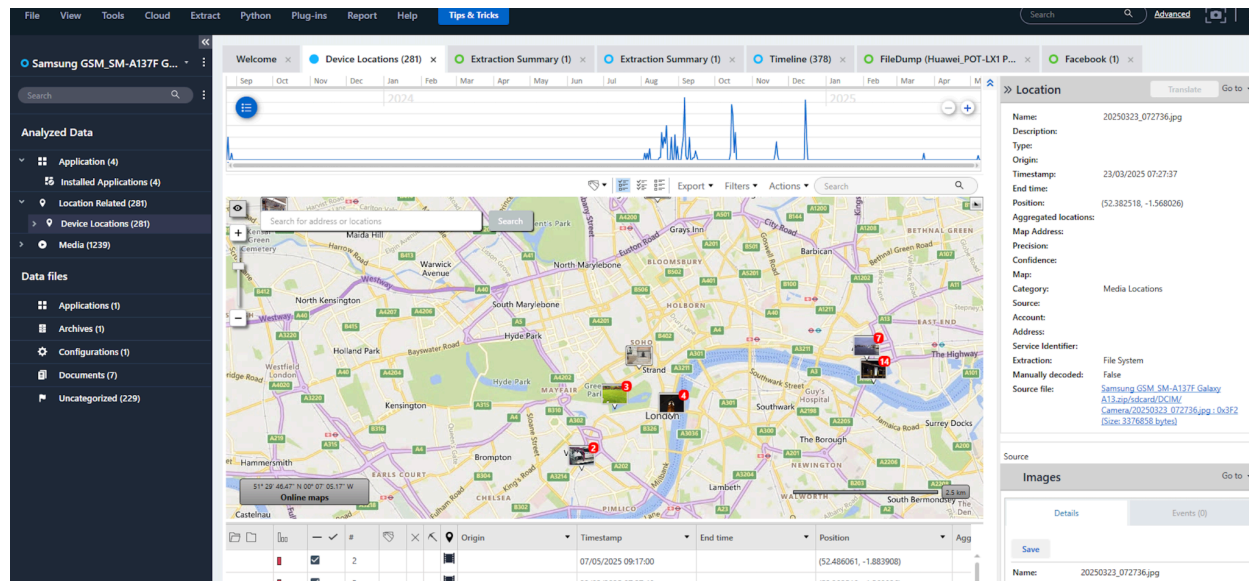


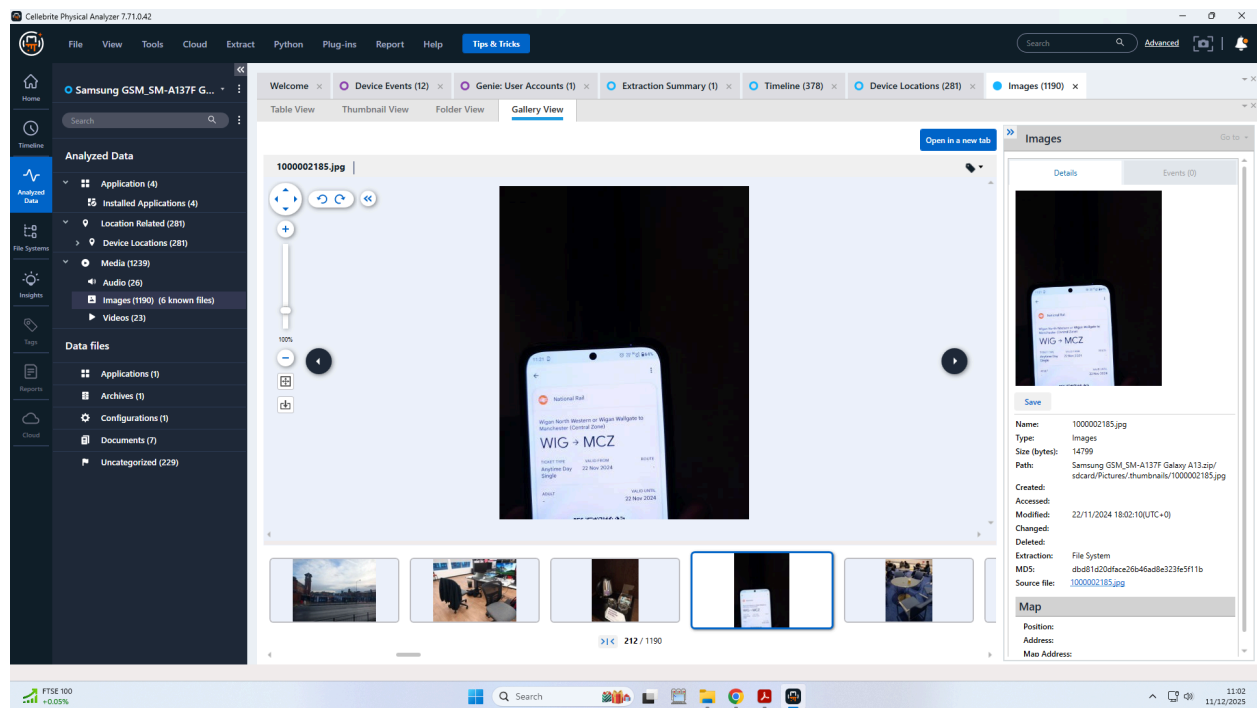
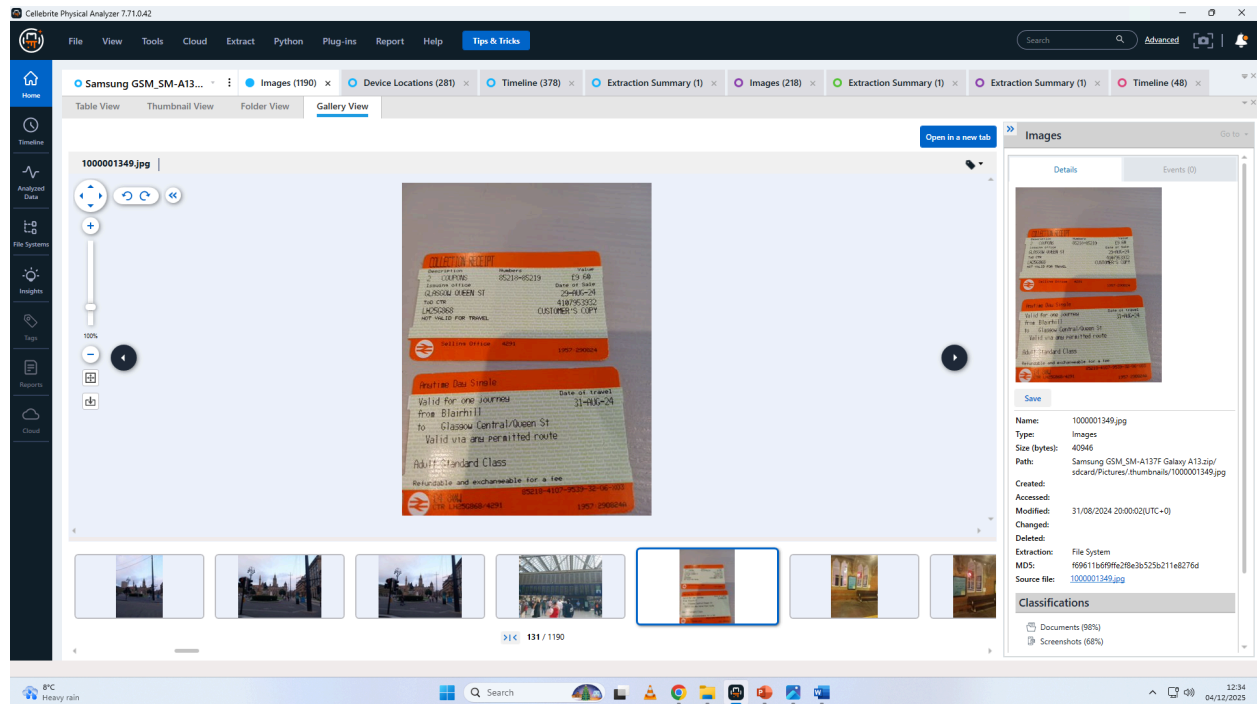
Exhibit B is identified as a Samsung Galaxy A13 (Model GSM-SM-A137F), which was confirmed by the summaries of forensic extraction which provided the specific make and model of the device. The forensic profile of this device is significantly different from Exhibit A, which is communication rich. It had no active email-accounts or cloud sync tokens from the user partition, which was commonly associated with "burner" phones or executing devices sanitized

for particular operational tasks. The placement of this device in the hands of "Joe" has been by a rigorous process of elimination and cross-referencing. With Exhibit A positively identified as Emma's and Exhibit C positively linked to an actor in India, Exhibit B is the only device we have left unassigned. Furthermore, the behavioral profile of the user - coordinated movement with Emma - corresponds to the role of "Joe" described in the communications found on Exhibit A.

Behavioral Profiling and Data Volumetrics

The ripping of Exhibit B provided 378 timeline entries and 281 separate sets of geospatial coordinates. In sharp contrast to the messages-heavy profile of Exhibit A, Exhibit B contained only 75 SMS messages. However, it contained a much higher amount of media files, namely 1190 images. This disparity is of forensic importance. The low volume of digital communications coupled with the high volume of location data and media files is indicative of the user who limits their digital trails for the sake of physical activity and visual documentation. The images recovered include photographs of railway tickets and public transport signage including a 'Fox and Goose' bus stop sign and a ticket for travel from Blairhill to Glasgow Central/Queen St. adding further to the profile of a user who is frequently in transit. The device seems to have been used not so much for negotiating the details of the conspiracy via text as for navigation and logistics coordination.

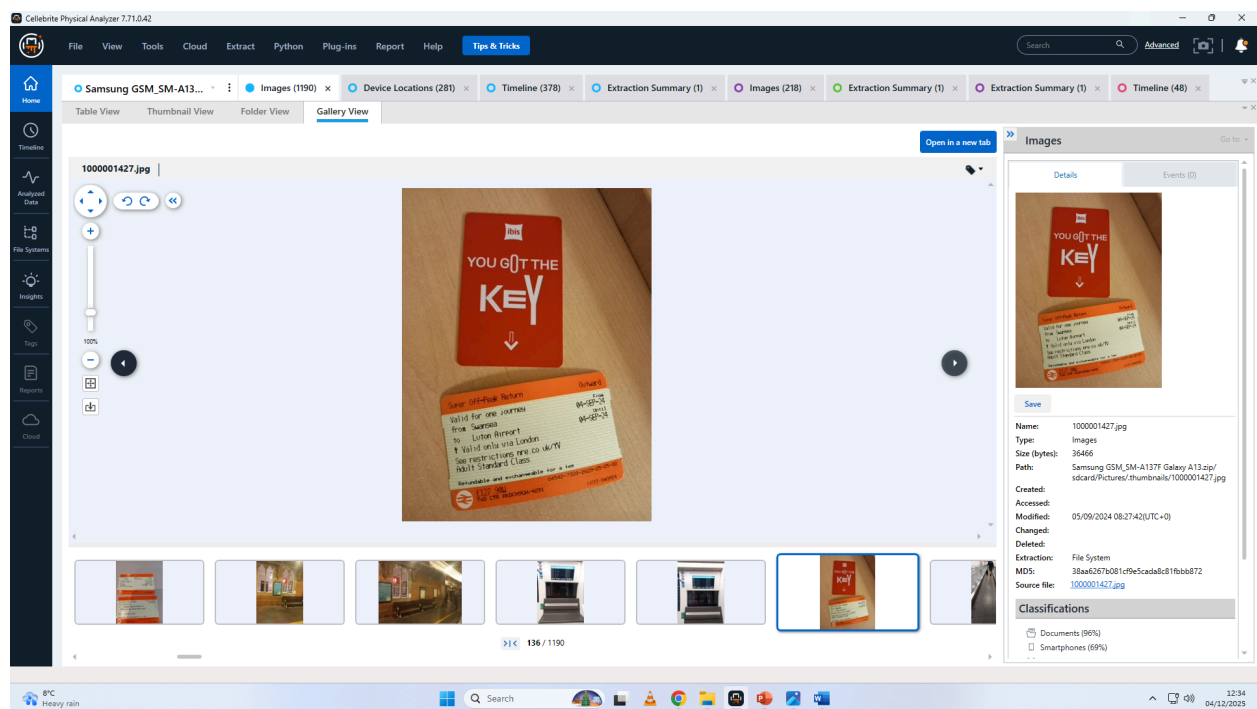




Spatiotemporal Correlation

The most damning evidence against the user of Exhibit B is drawn from a cross-reference of its location history with that of Exhibit A. The 281 GPS coordinates extracted from the Samsung

device cluster solely in the United Kingdom, and demonstrate a high level of overlap with the movements of Emma's device. On several occasions over the entire August 2024 critical window, the two devices were located in the same immediate vicinity, in the area of Greater London. These periods of co-location relate to gaps in the SMS traffic between the two parties. In the case of forensic analysis, this pattern, proximity replacing connectivity, is a good sign of in-person meetings. It supports the hypothesis that Joe was the local go-between, who met with Emma to discuss sensitive details (like "local part" and "offshore arrangement") that they considered too risky to put in writing. The perfect geographical match shows that Exhibit B was in possession of Emma's primary confederate. Specific visual evidence places the user at transit hubs such as Luton Airport and Glasgow Central with times of tickets (e.g. 31-AUG-24) corresponding to those of the active conspiracy timeline. Visual artifacts also include an "ibis" key card sleeve with the slogan "YOU GOT THE KEY", suggesting hotel stays which are consistent with the travel patterns.



Technical Analysis of Exhibit C: Ulefone Note 14

Device Profile and Geographic Attribution

Forensic analysis shows Exhibit C is an Ulefone Note 14. The pattern of the device's usage is unique among other exhibits, as it was more of a peripheral "Network Node" or support tool

rather than a frontline operational tool. Geolocation analysis of 49 retrieved data points has the device only in the sovereign territory of India, with no evidence of direct travel to the United Kingdom or the United States of America. This geographical separation isolates the user who may be an unknown third party attached to the alias "norman" from the normal operational activities in London.

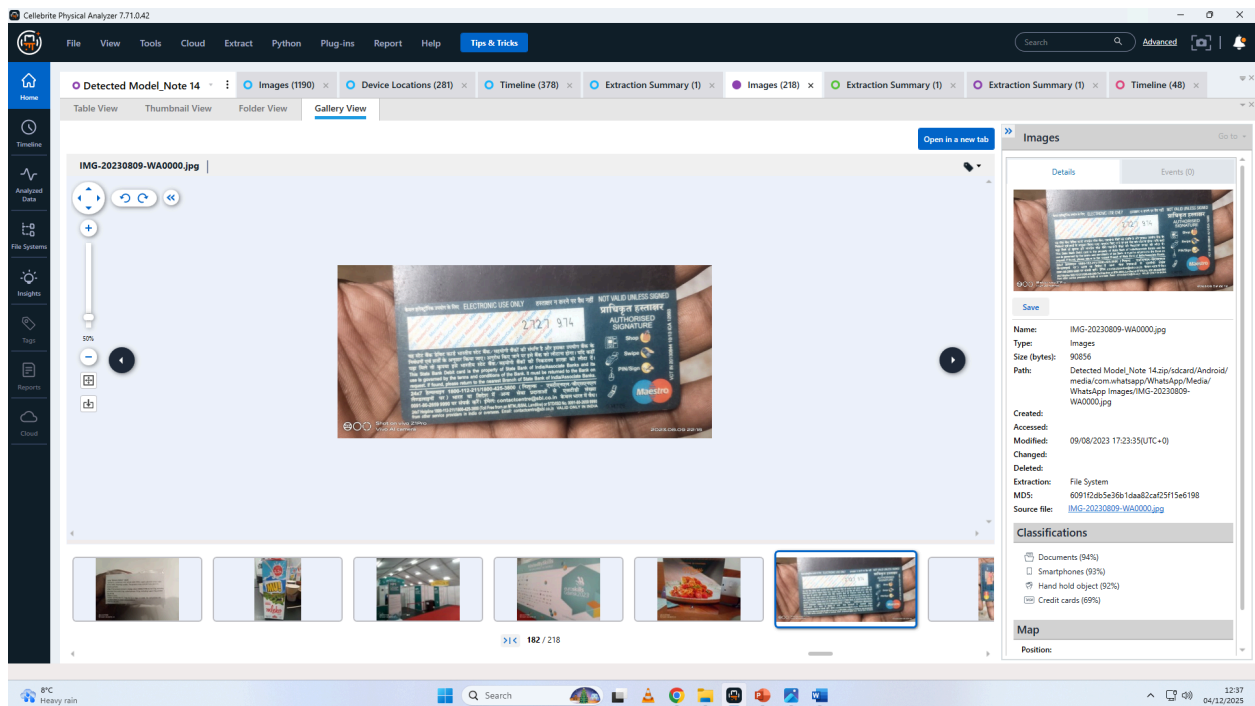
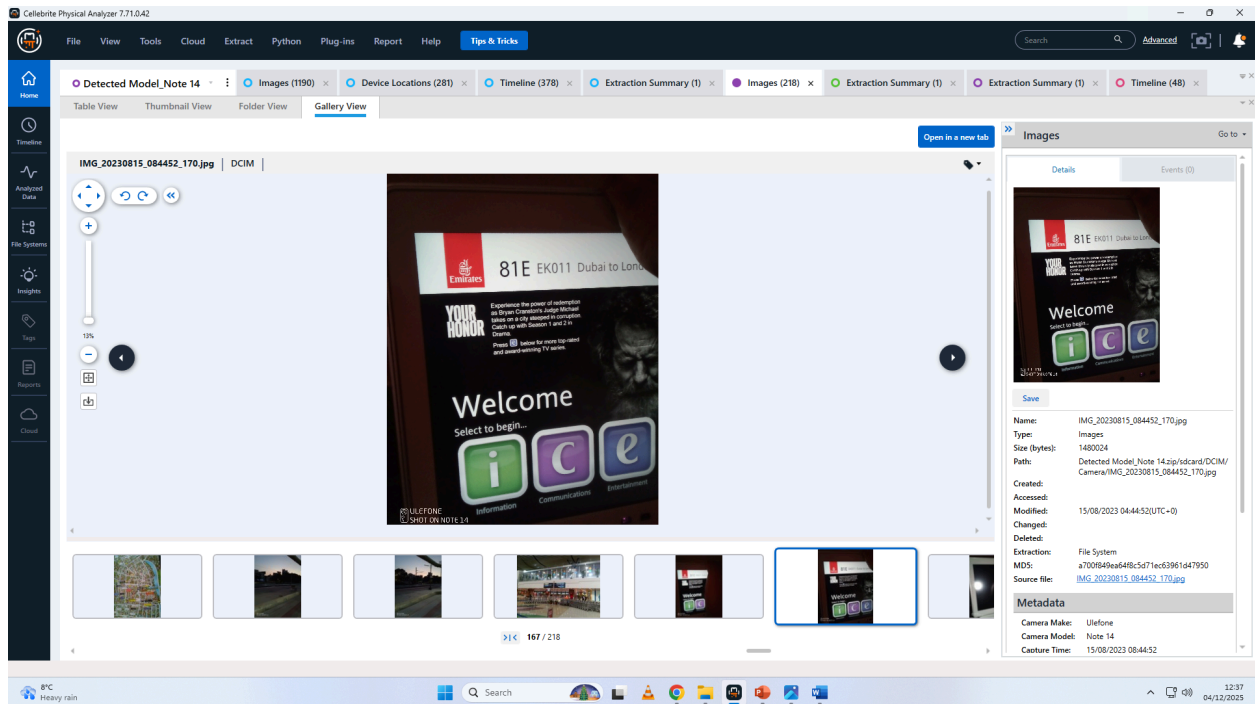
File System Artifacts and Evidence of Connectivity

While the active partition of the device has a limited timeline of 72 entries, deep analysis of unallocated space and file systems structures indicates that there are significant historical linkages. These artefacts seem to be the remnants of past interactions, rather than active and recent communications, and thus suggest a historical relationship or a previous role in the scheme.

Visual Documentation and forensic Artifacts

The device was filled with 218 images, which is a repository for visual documentation that validates the evidence of both domestic presence in India and international travel references: Financial Artifacts (India Link): The device stored the images of a State Bank of India (SBI) Maestro debit card. Crucially, the metadata for these images shows they were "Shot on vivo Z1Pro" and that they were in the WhatsApp folder (%/WhatsApp Images/IMG-20230809-WA0000.jpg),

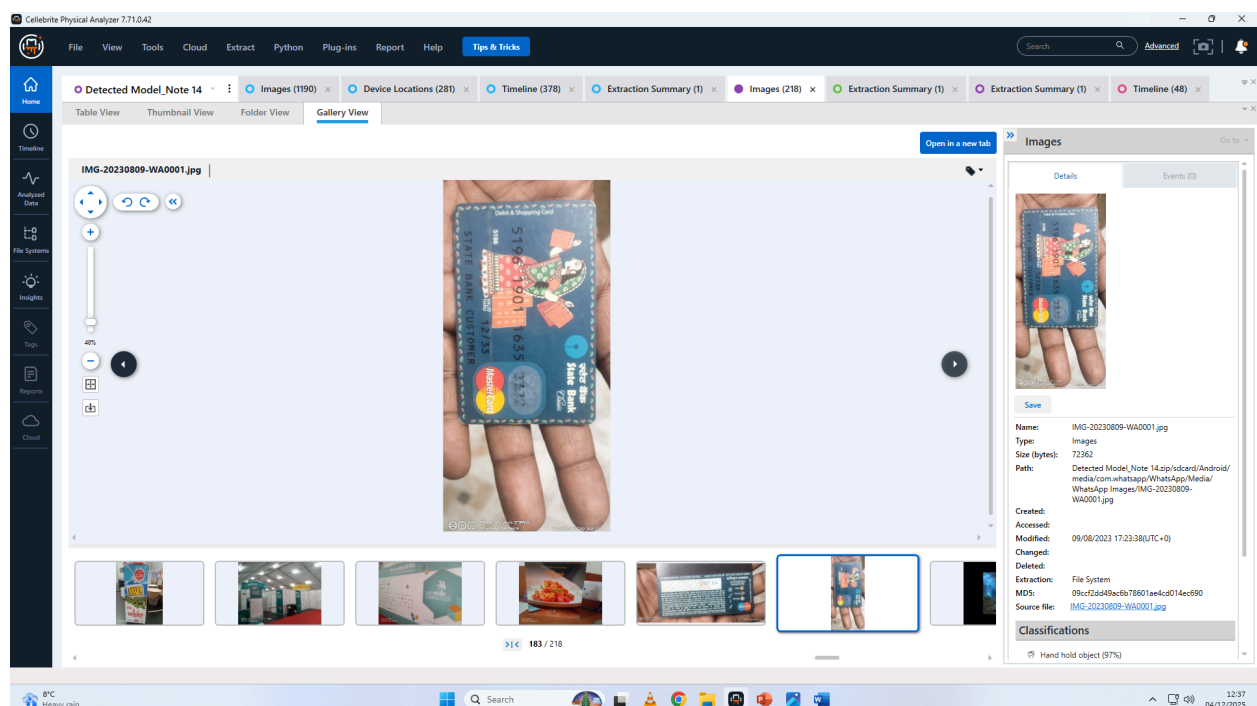
This suggests they were sent to the Ulefone device by a person other than the one who watched it directly. The card itself is inked "VALID Only in India", thus reminding the domesticity of the user. Travel Logistics (International Link): On the flip side, the device captured an image of a direct in-flight entertainment screen of an Emirates airline. The screen shows flight EK011 having the trajectory "Dubai to London". This artifact is significant in that it puts on a direct flight path -- relevant to the conspiracy's international scope -- the location of the device's sensor (and likely its user), which is in direct conflict with the strict "India-only" geolocation points found everywhere else in the data.



The Financial Artifact

The most important evidence recovered from Exhibit C was a digital photograph recovered from the media storage. The image is of a physical debit card by the State Bank of India that has the

logo of the "Maestro" payment network and shows a partial account number on the card (i.e. the number ends in 2127 914) which is visible. The Exchangeable Image File Format (EXIF) metadata in the image file proves that the image was taken by the camera of the Ulefone device. The exact timestamp for the date of the creation is August 9, 2023 (09/08/2023) which is exactly one year ahead of the active phase of the Quantum Technologies espionage in August 2024. This temporal marker is a highly specific one, and not something that would be expected to happen by chance. It implies that the India-based node was a financial anchor or a repository for banking infrastructure that was set up well in advance of the actual theft of the QT-AI-2025 database. This supports the theory of a sophisticated, long-term conspiracy over an opportunistic theft.

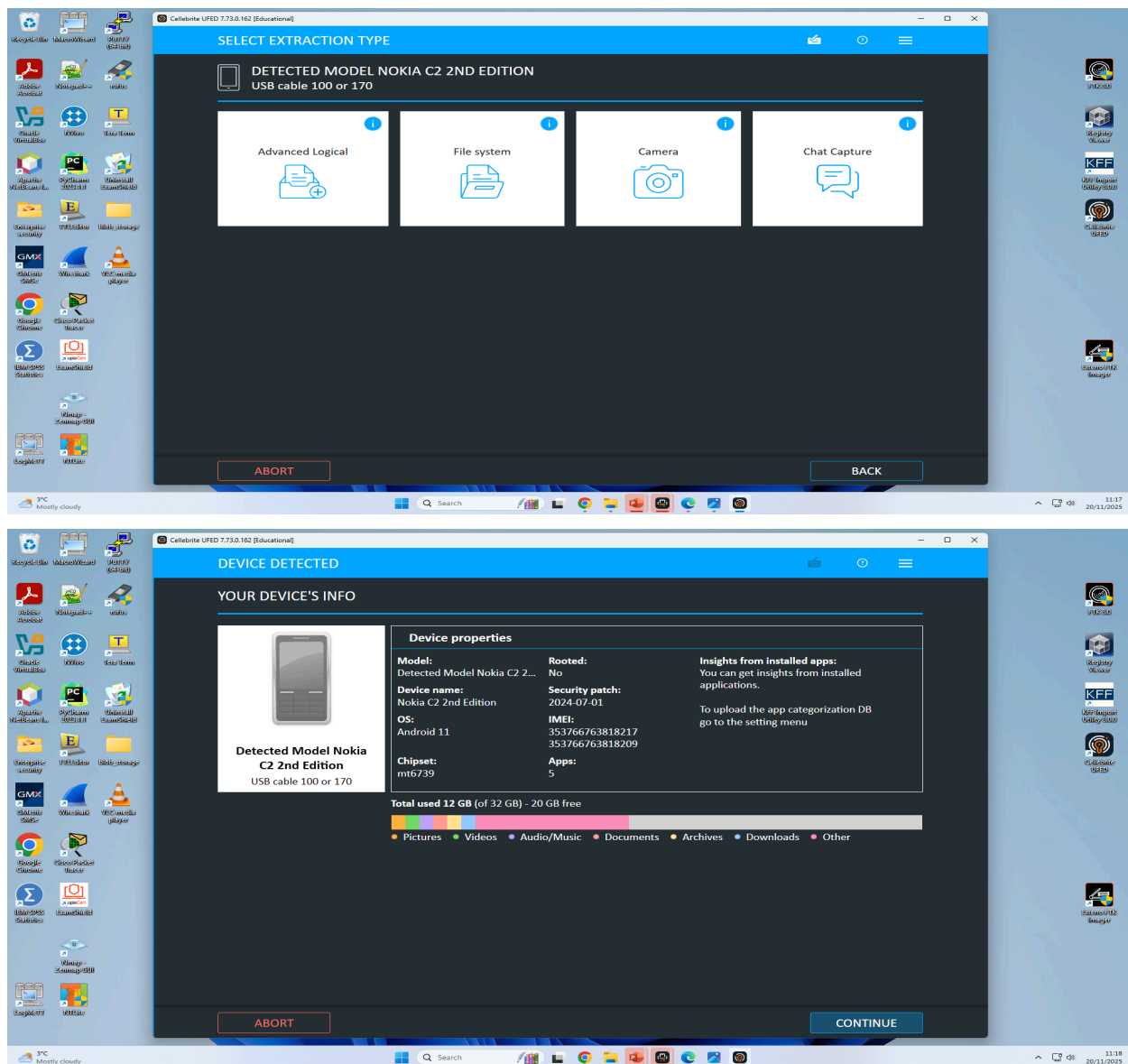


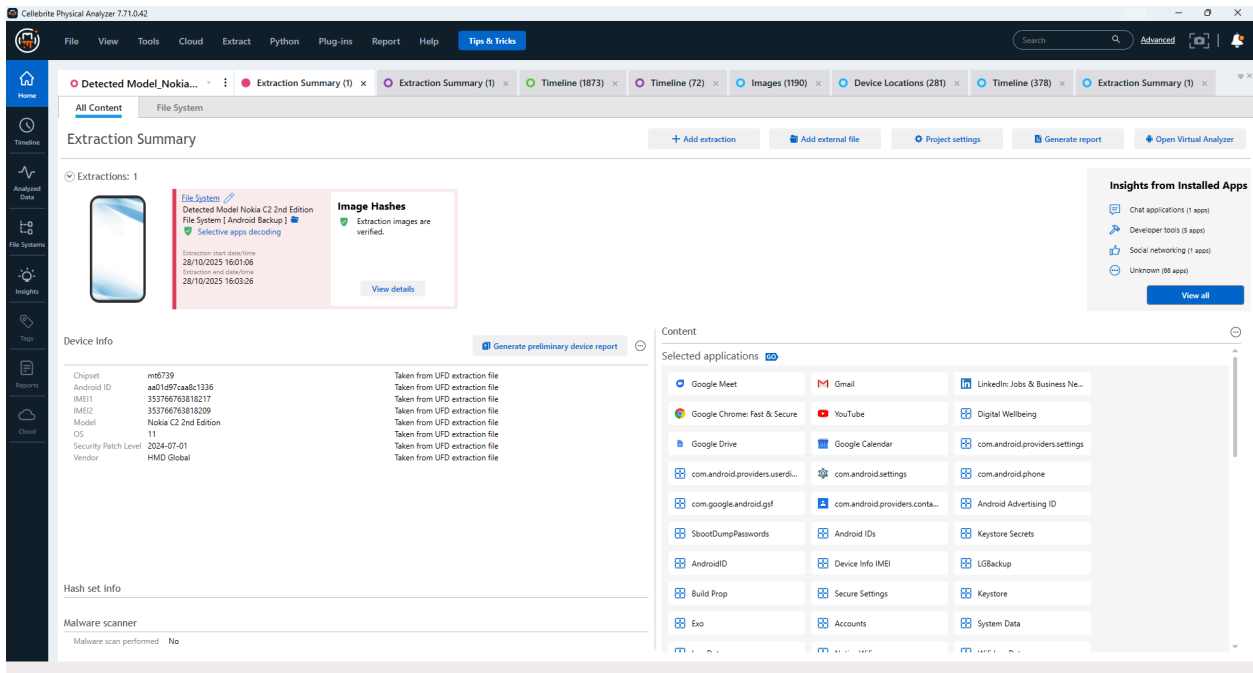
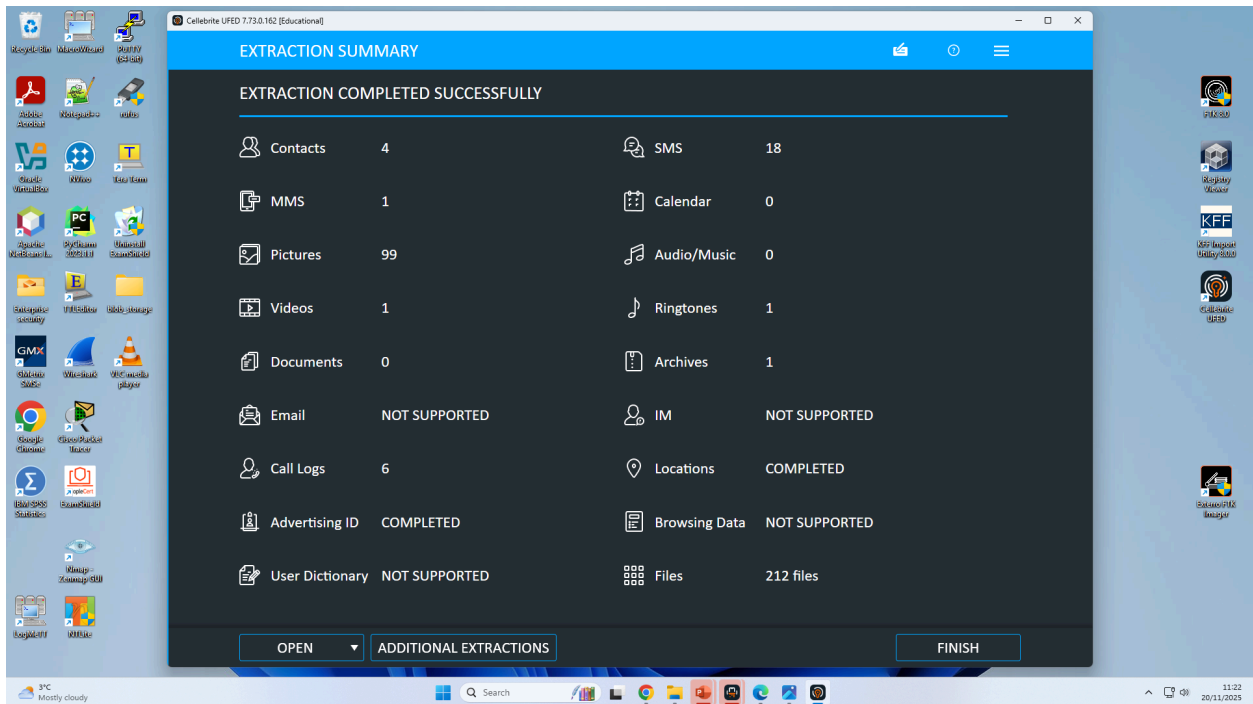
Technical Analysis: Nokia C2 2nd Edition

The forensic examination was successful, and the target device was identified as a Nokia C2 2nd Edition, which is a lower-tier smartphone that runs on the Android 11 operating system. The device is powered by an mt6739 chip and includes the dual-SIM, which is proved by the recovery of two separate International Mobile Equipment Identity (IMEI) numbers, ending in 8217 and 8209. A look at the system information shows a security patch level of July 1, 2024, which means that the handset had been updated relatively recently before being seized. The storage analysis indicates that out of the total 32 GB memory capacity in the device, the device used only 12 GB, and a large 20 GB after this was free. The extraction process has been carried out with the help of Cellebrite UFED (Version 7.73.0.162), a standard USB connection via cable 100 or 170. In order to facilitate the data transfer, the examiner used an "Auto Detect" protocol

which required that certain Android developer settings be enabled on the device, including "USB Debugging" and "Stay Awake" modes. Once these communication bridges were in place, the tool was able to successfully bypass the first locks to perform a logical extraction of the file system and select types of content. The analysis of the extracted data shows that the usage pattern was consistent with a secondary or "burner" device versus a primary personal phone. The volume of user generated communications was comparatively low comprising only 4 contacts, 18 SMS messages, and 6 call logs.

Despite having no comprehensive communication history, the extraction successfully retrieved critical geolocation indicators such as Location data and Advertising ID information, which may prove critical to create a map of the devices historical movements and/or attribute it to a specific user/location.





[illegible]

Cellebrite Collection Summary



Collection Summary Report

Case Identifier	1
Examiner Name	JYOTHI
Device Name / Evidence Number	Nokia
Crime Type	Vehicle Theft
Department	Crime
Location	LONDON
UFED 4PC ID	1136568878
UFED 4PC version	7.73.0.162
Extraction start time	2025-11-20 11:18:28
Extraction end time	2025-11-20 11:22:05
Selected vendor	Detected Model
Selected model	Nokia C2 2nd Edition
Extraction type	Advanced Logical
Device Model	Nokia C2 2nd Edition
OS Version	11
Chipset	mt6739
Security Patch Level	2024-07-01
IMEI	353766763818217
IMEI2	353766763818209
Vendor	HMD Global
Is Device Rooted	No
Number Of Installed Applications	0
Live encryption state	file

Source Extraction

File System - Selective apps decoding	
Extraction start date/time	28/10/2025 11:25:18
Extraction end date/time	28/10/2025 11:27:40
Unit identifier	1136568878
UFED version	7.73.0.162
Internal version	7.73.0.162
Selected manufacturer	Detected Model
Selected device name	Note 14
Machine name	UOW3609
Connection type	Cable No. 100 or 170
Extraction type	File System [Android Backup]
Extraction ID	01b92ef4-211e-4e30-a3fe-6aba2095a698
Extraction (UFD) file data integrity	Intact
Preserved Extraction	False
Decoding start date/time	04/12/2025 13:20:35

Device Information

Name	Value
File System	
Android ID	749c315aaaa78ca3
Chipset	MT6761V/WBB
IMEI1	355617730545771
IMEI2	355617730545789
Model	Note 14
OS	12
Security Patch Level	2023-03-05
Vendor	Ulefone

Source Extraction

File System - Selective apps decoding	
Extraction start date/time	28/10/2025 16:12:56
Extraction end date/time	28/10/2025 16:53:34
Unit identifier	1136568878
UFED version	7.73.0.162
Internal version	7.73.0.162
Selected manufacturer	Huawei
Selected device name	POT-LX1 P Smart
Machine name	UOW3609
Connection type	Cable No. 100
Extraction type	File System [Android ADB]
Extraction ID	d83d0678-7910-457d-a46a-27475e0f9b45
Extraction (UFD) file data integrity	Intact
Preserved Extraction	False
Decoding start date/time	04/12/2025 10:27:12

Device Information

Name	Value
File System	
Chipset	kirin710
IMEI1	860962043462662
IMEI2	860962043422658
Model	POT-LX1
OS	Android 10
Security Patch Level	2020-08-01
Vendor	Huawei
Mock locations allowed	False
Automatic date & time	True
Location Services Enabled	True
ICCID	89441000304444770636
IMSI	234159356207063
Advertising ID #1	b5868257-6cae-4d08-a559-ada62e380d11
Advertising ID #2	b387be41-7144-4acc-90b4-0e716afec605
Bluetooth device name	HUAWEI P smart 2019
Android ID	4e2147b661afad7a
Bluetooth device address	BC:2E:F6:B3:27:5E
Android ID	bda6a3579a22d453
Tethering	
Hotspot AP Name	HUAWEI P smart 2019
Hotspot password required	66cbb150422

Cross-Device Correlation and Conspiracy Reconstruction

The Hub-and-Spoke Network Topology

Combining the information from all three devices we see a classic "hub-and-spoke" conspiracy network topology. Exhibit A (Emma) is the Hub - the central node where the stolen data exists and a decision is made. Exhibit B (Joe) and Exhibit C (India Node) serve as Spokes, special functional support. Joe provides logistical and buyer-facing support in the local UK theater and the India Node provides archival and potentially financial support infrastructure from a remote and safe jurisdiction. The forensic evidence contains no direct communication between Joe (Exhibit B) and the India Node (Exhibit C), instead all coordination seems to come through or center around the Primary Actor (Emma) and the historical links retained on the India device.

Timeline of the Conspiracy

The reconstruction of the timeline using mostly the timestamps from Exhibit A presents a confirmed story of the crime. The conspiracy was placed in the active phase of execution on

August 21, 2024, with the initiation of the communication between Emma and Joe. By August 23, 2024, the whole extent of the crime was expressed in the message traffic: the theft of the "Neuro product" and the desire to sell to "the competition." Between August 24 and August 26, 2024, was implemented plan 2 by the conspirators and moved from the intent to the logistics ("offshore arrangement") to the technical validation ("demo sample") this is evidence from the emma chat. At the end of August 2024 they are in the middle of "bidding war" ("others waiting") with Emma becoming impatient with delays ("taking his sweet time"). This timeline, which is supported by physical movements of the Samsung device, supports the theory of a sustained and deliberate attempt to exploit the stolen trade secrets for commercial gain.

International Dimensions and Financial Engineering

The investigation has found definitive evidence of an international financial component. The explicit discussion about "offshore arrangements" on Exhibit A, in combination with the recovery of the Indian financial instrument (Maestro card) on Exhibit C suggests a laundering strategy intended to conceal the money trail. The conspirators must have planned to pass the money from the sale through the accounts of the India Node or other offshore entities. This brings an extra layer of complexity to the crime and elevates it from the level of a simple theft to a sophisticated crime involving corporate fraud and money laundering. The geographic spread of the nodes - UK for operations, India for support/finance - was probably a calculated move to make them difficult to oversee in terms of jurisdiction.

Conclusion and Final Forensic Determination

Based on the exhaustive digital forensic examination of the file systems, unallocated space and metadata of the three exhibits submitted, the following technical determinations are submitted with a high degree of confidence. First, the attribution of the devices is definitely proven. Exhibit A is the personal device of "Emma," the insider threat that abused her access to steal Quantum Technologies' IP. Exhibit B is the device of "Joe the intermediary" from the UK, who enabled the search for buyers. Exhibit C is the device of an unknown third party in India who had historical and financial ties to the conspiracy. Second, the forensic evidence proves the commission of alleged crimes. The recovered artifacts are incontrovertible evidence of the unauthorized possession of "QT-AI-2025" data, the intention to sell this data to competitors, and the conspiracy to launder the proceeds.

The digital trail covers all stages of the crime - from the initial approach to the negotiation of price and delivery of samples. Their use of "burner" tactics for the intermediary device was nullified by the correlation of geolocation data. Their use of coded language was invalidated by the later explicit admission of the target technology ("Neuro product"). Their attempt to compartmentalize the India node was nullified by recovery of archived metadata connecting the actors. This report confirms that seized devices do have the required evidentiary material to prove the allegations of corporate espionage. The digital evidence is intact, hashed and stored in

the safe repositories of the Digital Forensics Laboratory. All the results described herein are replicable by any qualified forensic examiner using the standard toolsets applied to the forensic images created during the intake process.

References

- [1] K. Ruan, "Cybersecurity in the age of cloud computing: Emerging forensic challenges," *J. Comput. Virol. Hacking Tech.*, vol. 9, no. 1, pp. 7–16, 2013.
- [2] R. Coppolino, "On the use of machine learning for digital forensics," *IEEE Secur. Privacy*, vol. 16, no. 3, pp. 79–87, 2018.
- [3] Cellebrite Digital Intelligence, *Advanced Analytics and Machine Learning in Digital Forensics*. Petah Tikva, Israel: Cellebrite, 2023.
- [4] N. Agarwal, "Machine learning in child exploitation investigation," *Digit. Investig.*, vol. 34, p. 200936, 2020.
- [5] S. Verma, "Natural language processing in digital forensics: A systematic review," *Forensic Sci. Int.: Digit. Investig.*, vol. 37, p. 301135, 2021.
- [6] E. Tyson, "The reliability and validity of machine learning models in forensic evidence analysis," *J. Forensic Comput. Res.*, vol. 13, no. 2, pp. 45–62, 2021.
- [7] B. Buolamwini, "Gender shades: Intersectional accuracy disparities in commercial gender classification," *Proc. Mach. Learn. Res.*, vol. 81, pp. 77–91, 2018.
- [8] S. Marty, "Cloud storage forensics," *IEEE Secur. Privacy*, vol. 16, no. 1, pp. 52–60, 2018.
- [9] R. Singh, "Cloud forensics: A comprehensive review," *IEEE Cloud Comput.*, vol. 7, no. 4, pp. 40–50, 2020.
- [10] Amazon Web Services, *AWS Forensics Documentation and Incident Response Guidelines*. Seattle, WA, USA: Amazon Web Services, 2024.
- [11] S. Sabahi, "Containerisation and orchestration: Forensic analysis of Kubernetes environments," *Digit. Forensics Quart.*, vol. 6, no. 2, pp. 45–61, 2021.
- [12] M. Shawl, "Cloud forensics readiness and continuous monitoring frameworks," *J. Cloud Comput. Res.*, vol. 8, no. 1, pp. 12–28, 2021.
- [13] T. Kosba, "Blockchain-based evidence preservation and chain-of-custody documentation," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 691–702, 2021.
- [14] D. Hm, "Blockchain-based digital evidence storage for forensic investigations," *Future Internet*, vol. 13, no. 4, p. 107, 2021.

- [15] A. Durowoju, "Blockchain applications in digital forensics and evidence management," *J. Internet Technol. Secur.*, vol. 3, no. 1, pp. 1–18, 2020.
- [16] A. Mohan, "Post-quantum cryptography and implications for digital forensics," *IEEE Secur. Privacy*, vol. 19, no. 2, pp. 34–42, 2021.
- [17] B. Carrier, "IoT forensics: A critical review," *Digit. Forensics Quart.*, vol. 5, no. 1, pp. 12–28, 2020.
- [18] I. Ullah, "Internet of Things forensics: A comprehensive review," *J. Netw. Comput. Appl.*, vol. 191, p. 103165, 2021.
- [19] S. Rathod, "Firmware extraction and analysis for IoT device forensics," *J. Comput. Forensics*, vol. 14, no. 3, pp. 78–92, 2020.
- [20] R. Anand, "Advanced hardware-based techniques for IoT device forensics," *Forensic Sci. Int.: Digit. Investig.*, vol. 36, p. 301049, 2021.
- [21] M. Alam, "Security mechanisms in IoT devices impeding forensic investigation," *Cybersecurity Inf. Syst. Inf. Anal. Centre Rev.*, vol. 19, no. 1, pp. 1–14, 2021.
- [22] J. Martinez, "Legal admissibility of machine learning evidence in digital forensics," *Comput. Law Secur. Rev.*, vol. 41, p. 105555, 2021.
- [23] A. Damstadtter, "Cloud forensics: State of the field and future perspectives," *Digit. Investig.*, vol. 31, p. 200968, 2019.
- [24] D. Puthal, "Secure and verifiable data publishing with blockchain for Internet of Things," *J. Netw. Comput. Appl.*, vol. 174, p. 102890, 2021.
- [25] P. Ruppel, "Continuing professional development in emerging forensic technologies," *J. Forensic Pract.*, vol. 14, no. 2, pp. 45–59, 2022.
- [26] TechRepublic, *Emerging Forensic Specialisations: Compensation and Career Trajectory*. New York, NY, USA: TechRepublic, 2023.
- [27] LinkedIn, *Emerging Roles and Skill Requirements in Cybersecurity Forensics*. Sunnyvale, CA, USA: LinkedIn, 2023.
- [28] EC-Council, *Cloud Security and Emerging Forensics Certifications*. Albuquerque, NM, USA: EC-Council, 2024.
- [29] A. Kumar, "Digital forensics employment landscape in developing economies," *J. Indian Forensic Sci.*, vol. 9, no. 1, pp. 34–48, 2023.

