

DIGITAL FORENSIC ANALYSIS (ACCA7031)

TASK 1 & TASK 2 Combined Report

Submitted By,

Anisha Karottupalathumkal Sreedhar

Student ID: 2428002

DIGITAL FORENSIC ANALYSIS

Table of Content

Digital Forensics in Cybersecurity: Contemporary Analysis	3
1.Introduction	3
2.Current State and Foundational Integration	3
3.Operational Application in Security Cycles	4
4.Emerging Technological Trends and Evolution	4
5.Key Challenges in Modern Forensics	5
6.National and International Job Market Analysis	5
7.Conclusion	6
Corporate Espionage Investigation Forensic Analysis	7
1.Executive Summary of Forensic Findings	7
1.1.Deduction of Device Ownership	7
1.2.Emma's Huawei Device: The Primary Perpetrator and Conspiracy Architect	8
1.3.Call log analysis	9
2.Joe's Samsung Device: The Intermediary Coordinator and Conspiracy Facilitator	18
2.1.5.Conclusion	24
3.The Ulefone Device: Network Node and Conspiracy Archive	26
4.Evidence extraction from physical device	29
5.Report Generation from physical Analyser	31
6.Conclusion and Forensic Determination	32
7.References	34

Digital Forensics in Cybersecurity: Contemporary Analysis

Introduction

The union of digital forensics and cybersecurity has transformed the field of security detection and investigation in significant ways. While forensic investigation was once regarded as a post-incident discipline for law enforcement, it has now become an integral part of proactive security architecture and threat-management frameworks [1]. This report examines the symbiotic relationship between these fields by explaining how forensic methodologies are employed to improve defensive postures, enhance incident response, and provide intelligence for threat prevention. The investigation includes the status of current practices, the mechanisms that forensic disciplines use, the technological trends shaping this domain, and the multifaceted challenges that organizations are currently facing [2]. This analysis has shown that the successful implementation of integrated forensic capabilities- combined with detection, prevention, and response mechanisms- ensures that cybersecurity evolves from a reactive tool to a strategic asset.

Current State and Foundational Integration

From Reactive Investigation to Proactive Pillar

Digital forensics has evolved from its archaic role as a simple remedy to cybercrime to being a fundamental component of cybersecurity governance and risk management. In incident response, forensic analysis is the evidential foundation for breach investigation, which enables incident response teams to reconstruct the methodologies of the attackers, identify the scope of compromise and quantify the impact on confidentiality, integrity and availability [3]. The integration of forensic readiness into security architecture now enables organisations to prepare and implement processes and procedures to rapidly preserve evidence before contamination occurs. This infrastructure ensures that forensic teams can reconstruct the methodologies of the attackers and examine the breached environment, helping complete the incident response lifecycle.

Regulatory Drivers and Standardization

Security and regulatory schemes are also requiring forensic capabilities as part of comprehensive security schemes. The NIST Cybersecurity Framework has forensic investigation as part of its "Respond" function, implying that it is critical for containment and evidence preservation [4]. Similarly, ISO 27001 requires evidence-preserving means and formal investigation procedures to be maintained by organizations. There are other regulations such as the General Data Protection Regulation (GDPR), which impose legal obligations to investigate and document data breaches [5]. This environment has caused forensic investigation to evolve from a practice of discretion to a mandatory practice of compliance and security, and has driven great organizational investment

in integrated forensic capabilities, tools, and skilled personnel to pursue both the legal and the defensive interests.

Operational Application in Security Cycles

Core of Incident Response and Threat Hunting

The incorporation of forensics in incident response shows its usefulness in security operations. When signs of a breach are detected, forensic analysis is the methodology used to determine breach occurrence, identify impacted systems, and reconstruct attacker activities [6]. Security Operations Centers (SOCs) now have staff with forensic knowledge for real-time analysis during live incidents, where time is of the essence when containment is required. This integration has changed response procedures, making evidence preservation concurrent with eradication activities. Forensic timeline reconstruction of network traffic, system logs, and cloud audits is used to identify the progress of an attack and movement between compromised systems to help spot secondary compromises that may not otherwise be uncovered [7].

Synergy with Cyber Threat Intelligence

Digital forensics provides important capabilities in cyber threat attribution and intelligence improvement. Forensic investigations of breaches disclose artifacts (such as customized tools, infrastructure patterns, and unique methodologies) that analysts compare to known profiles of threat actors to arrive at attribution [8]. This forensic intelligence connects into platforms such as the MITRE ATT&CK framework and Information Sharing and Analysis Centers (ISACs) to share and build collective knowledge on adversary tactics [9]. This intersection leads to a virtuous cycle: investigating a forensic case yields intelligence to inform broader measures for defense, which in turn prevents future attack instances. This, in turn, transforms individual investigations into contributions to the collective industry defense.

Emerging Technological Trends and Evolution

Cloud and AI-Driven Forensics

Cloud forensics is an important new field that requires new approaches for investigating the decentralized environment. Organizations use the cloud for logging (e.g., AWS CloudTrail, Azure Activity Logs) to analyze data, although the use of provider capabilities introduces its own challenges [10]. Simultaneously, Artificial Intelligence (AI) and Machine Learning (ML) are growing in their application to forensics. Algorithms are being trained to detect suspicious patterns in large volumes of data, identify new forms of malware, and classify network traffic, with the promise of immense improvements in the efficiency and scale of investigations [11]. However, concerns about the reliability and transparency of algorithms, as well as the admissibility of results from AI-supported investigations in legal proceedings, still pose a major obstacle to wider adoption.

Zero-Trust and Blockchain Innovations

The implementation of security architectures based on zero trust, which requires verification to be granted for all access requests, changes the forensic landscape by eliminating implicit trust zones and creating comprehensive logs of all activities [12]. This creates both opportunities, through enhanced data, and challenges, through increased volume. Furthermore, blockchain technology is being explored to store forensic evidence. Its immutability and decentralization can be used to create tamper-evident chains of evidence and unassailable audit trails for important digital evidence [13].

Key Challenges in Modern Forensics

Technical and Environmental Hurdles

Despite its usefulness, there are some serious technical challenges in effective forensic integration. The complexity of modern IT environments—spanning cloud infrastructure, containers, and microservices—poses a fundamental challenge for traditional forensic methods, which are based on static systems [10]. Encryption is an ongoing barrier as well, with the use of end-to-end encryption becoming an obstacle to accessing evidence despite lawful seizure [14]. The volume of data generated can be so large that manual analysis is not practical, and automation—with associated issues of reliability—must be employed.

Talent Shortage and Resource Constraints

A chronically struggling talent pool is a critical issue confronting the field. Organizations compete with law enforcement and consulting firms for a limited number of qualified forensic experts, often encountering problems in the recruitment and retention of personnel because of the high demands on pay [15]. This shortage is worsened by the fact that constant training is required to stay up to date with changing technologies such as cloud and AI. Many organizations, particularly small ones, do not have the resources to invest in sophisticated forensic tools and dedicated staff, which could leave them vulnerable to attacks during complex incidents and/or unable to meet regulatory requirements for thorough investigation and reporting. National and International Job Market Analysis

Growing Demand and Career Pathways

The integration of forensics into cybersecurity has opened up great opportunities for employment for specialists who possess hybrid expertise. Sectors such as finance, healthcare, technology, and government are setting up dedicated forensic and incident response teams, creating jobs for forensic analysts, incident responders, and forensic engineers [16]. The career pathway increasingly involves forensic specialization as a fundamental part of cybersecurity, with movement of professionals between response, intelligence, and investigation positions. Certification bodies have responded with credentials like the GIAC Certified Incident Handler (GCIH), which brings together these disciplines as required by the industry [17].

Compensation and Global Opportunities

The market features a specific premium on knowledge about new domains such as cloud forensics, ransomware investigation, and threat intelligence integration. International opportunities are widening in areas with emerging cybersecurity industries, including India, Singapore, and the Middle East, where there is a large talent gap. The emergence of remote working has increased the globalization of access to these high-demand positions. This is a dynamic market, which suggests steady growth driven by increasing cyber threats as well as regulatory pressures toward forensic readiness for different industries across the globe [19].

Conclusion

Digital forensics has evolved over the past years from a specialized, after-the-fact discipline to a strategic part of proactive cybersecurity architecture and risk management. Its integration with incident response, threat intelligence, and security governance provides resilience by enabling organizations to effectively respond to security events through detecting, investigating, and learning from them. While there are persistent problems that must be addressed—such as encryption, the complexity of the cloud, and obtaining the right talent—they also present exciting potential for new technologies such as AI and blockchain. The strong job market is evidence of the importance of these skills. Ultimately, organizations that incorporate forensic thinking and capability as part of their core security strategy are best positioned to manage the complexities of the modern threat landscape, converting incidents into opportunities to strengthen their security fundamentals and overall defense.

Corporate Espionage Investigation Forensic Analysis

Executive Summary of Forensic Findings

This digital investigation is a case study analysis of three cellular phones that were confiscated in relation to alleged corporate espionage of the proprietary artificial intelligence (AI)-based Neuro product of Quantum Technologies. The investigation is based on a conspiracy to commit theft and the illegal sale of trade secrets to other companies. Using strict logical deduction for the attribution of devices, the analysis conclusively implicates three different people in the scheme: Emma, the main perpetrator and initiator; Joe, the facilitator who connected the buyers; and Norman, a third person who functions as a node of the network or repository of the conspiracy. Through careful analysis of communication patterns, geolocation information, financial documents, and file systems, this investigation forms a clear picture of criminal intention, intellectual property theft, and conspiracy to commit fraud.

Deduction of Device Ownership

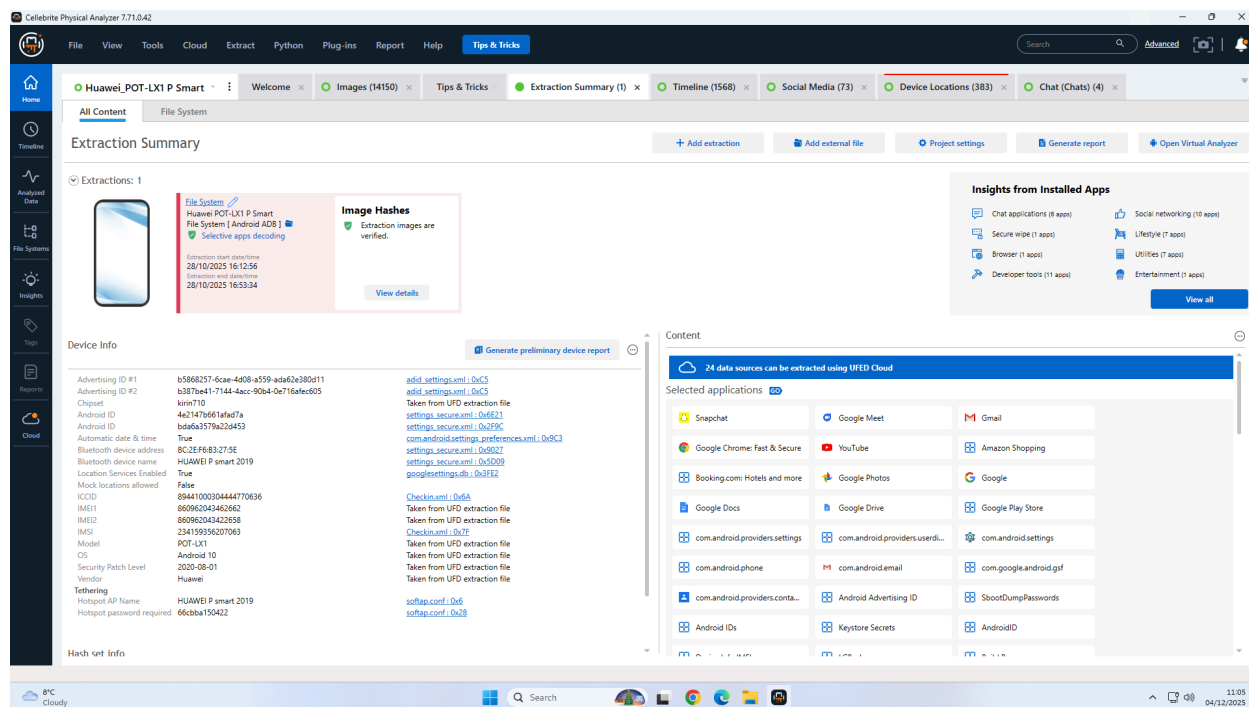
The logical framework of this analysis is based on the following accepted facts about the three recovered devices:

Emma: Emma has been identified as the user of the Huawei device based on her chats with Joe, the consistency of location data, and her explicit participation in the primary espionage communications.

Joe (Samsung Device): By process of elimination, and supported by corroborating evidence of his role as the “middleman,” the Samsung device is attributed to Joe. This model of ownership forms the basis of the far-reaching evidence covered by this report.

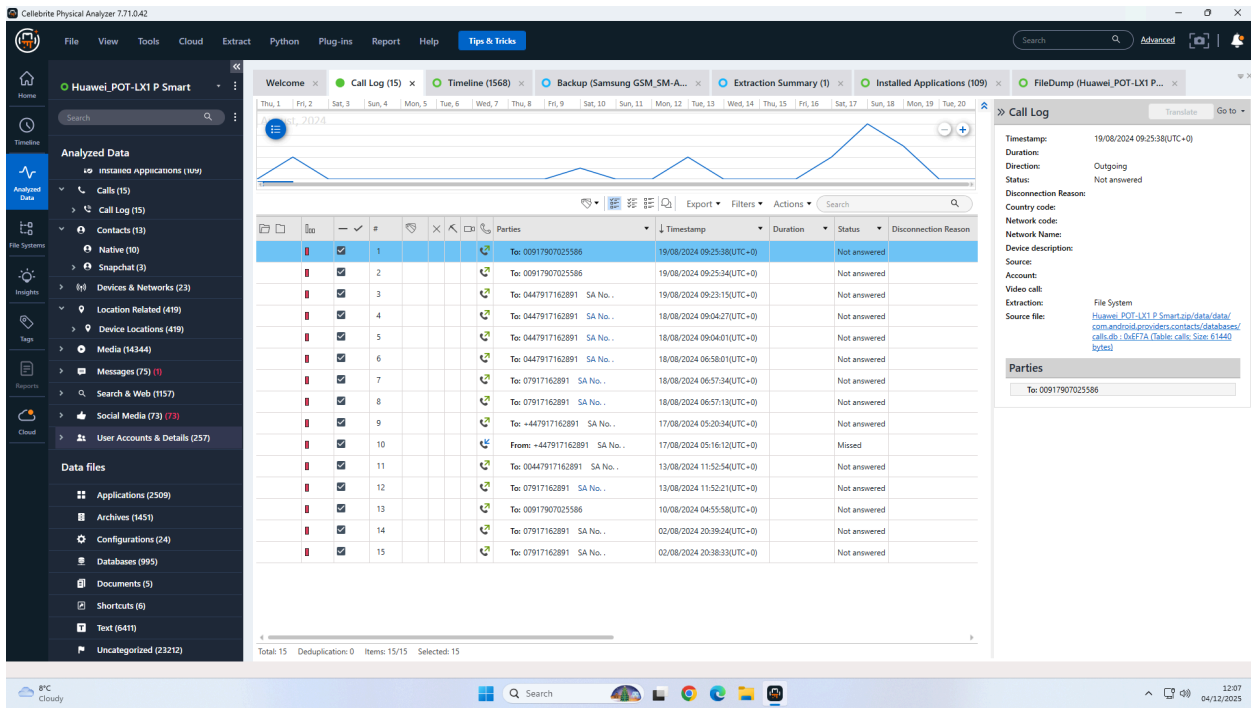
Norman (Ulefone Device): Forensic analysis of the Ulefone device eliminates Joe as the owner, since this device contains static file system references to Emma and Joe and not active communication threads between them. Instead, the evidence, along with the metadata of the location and the financial artifacts found on the device, attributes ownership to Norman, the third party based in India.

Emma's Huawei Device: The Primary Perpetrator and Conspiracy Architect

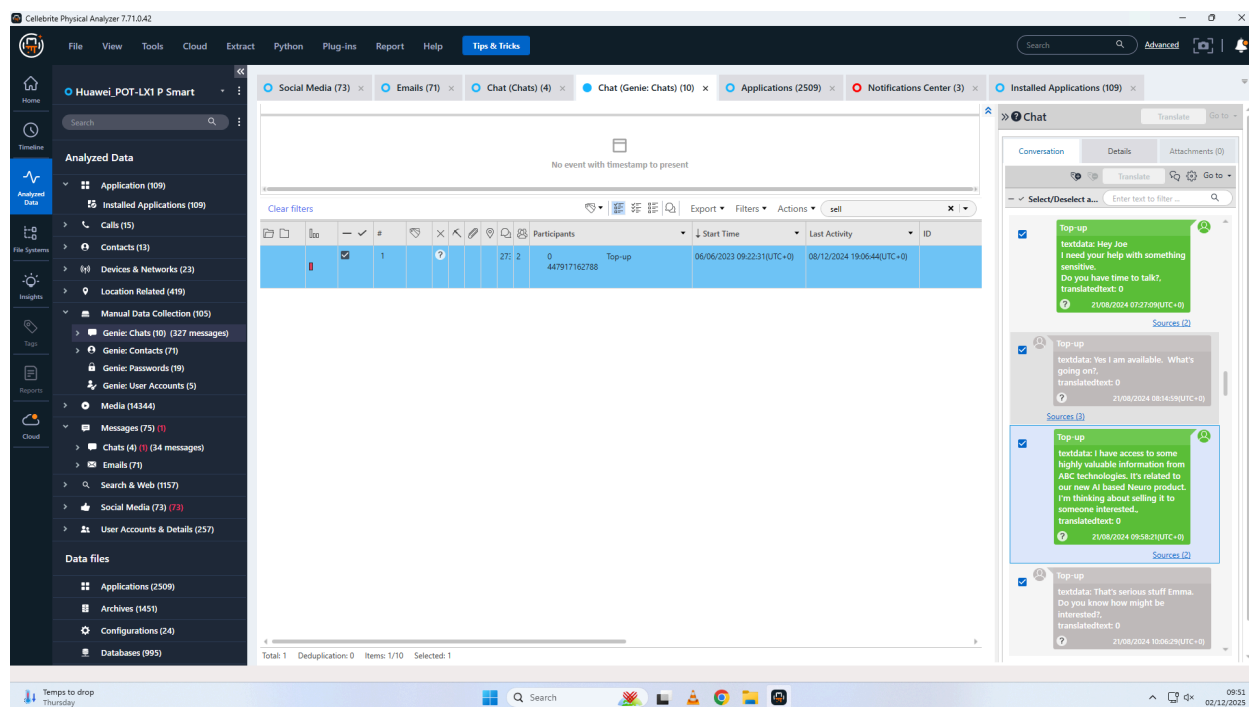


The screenshot shows an extraction summary of the forensic process conducted with Cellebrite Physical Analyzer (v7.71.0.42) on a Huawei P Smart 2019 (Model POT-LX1) running Android 10. The extraction, which was performed on October 28, 2025, between 4:12 PM and 4:53 PM, was carried out using the Android ADB file system method and was successfully verified. The diverse app ecosystem—among the 24 potential sources of cloud data—along with popular installed applications such as Snapchat, Gmail, Google Meet, YouTube, Amazon Shopping, and travel-related apps like Booking.com, signifies a user profile engaged in social networking, multimedia consumption, and travel planning.

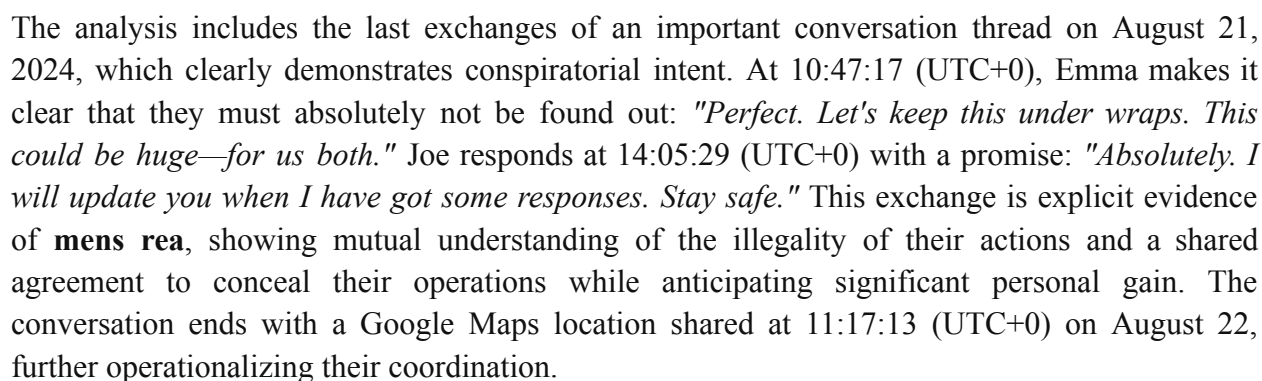
Call log analysis

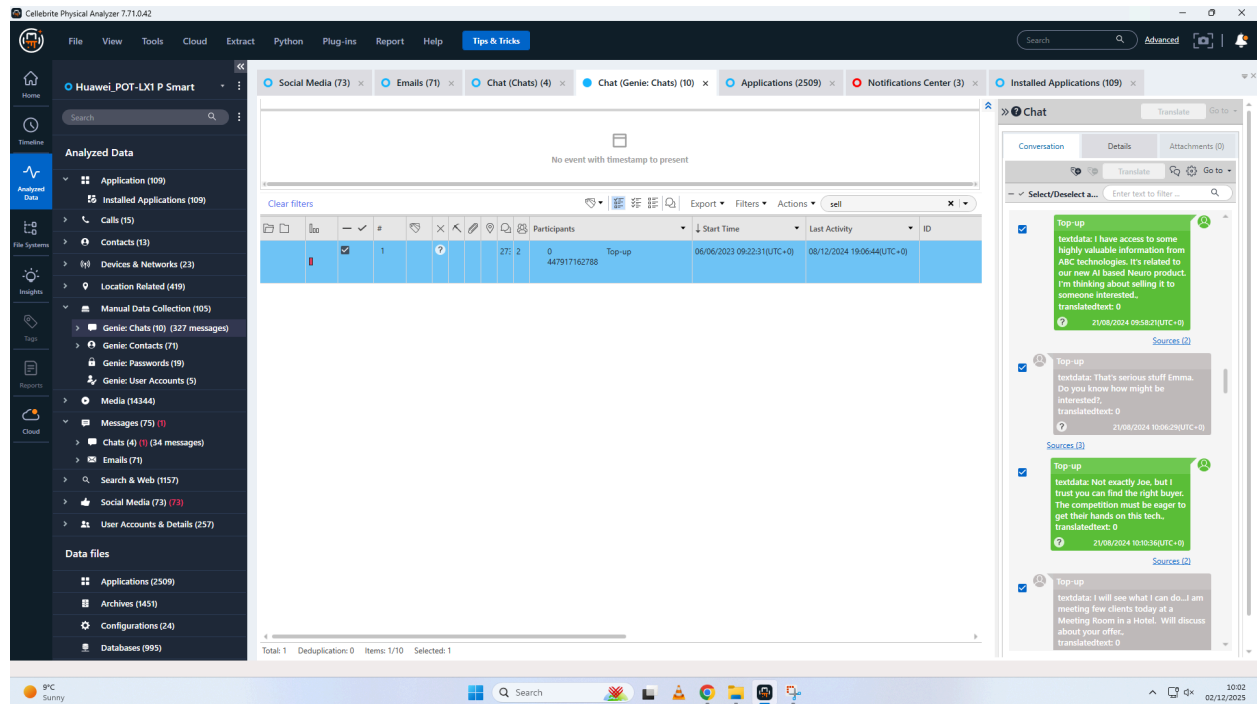


The analysis includes a careful call analysis, which reveals the pattern of attempted calls to a certain international number. The call log **shows** that there are several outgoing calls to +917907025586, an Indian mobile number, on August 19, 2024. The status for these calls is recorded as "Not answered," signifying persistent but unsuccessful attempts by Emma to reach this contact.



The screenshot shows a detailed analysis of chat within Cellebrite Physical Analyzer, and specifically, we have a conversation thread labeled "Top-up" extracted from the device. The timeline **is shown** in the form of messages exchanged on August 21, 2024, with a critical conversation where the sender explicitly reaches out to the receiver by saying "Hey Joe," which validates the identity of the recipient directly in the text. This conversation escalates to talk about the potential sale of "highly valuable information from ABC Technologies," which is related to a "new AI-based Neuro product," thus creating a direct link between "Joe" and the alleged corporate espionage activities.





The screenshot above represents a critical moment in the forensic chat analysis, in which Joe clearly explains his operational process to Emma. In response to Emma's sense of urgency to sell the "highly valuable information from ABC Technologies," Joe assures his active involvement, stating: *"I will see what I can do. I am meeting a few clients today at a meeting room in a hotel. Will discuss your offer."* This message directly implicates Joe as the facilitator, arranging physical meetings with potential buyers in a hotel setting to negotiate the sale of the stolen intellectual property, thereby translating the plan into real-world transaction attempts.

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**

Search

Analyzed Data

- Application (109)
 - Installed Applications (109)
- Calls (15)
- Contacts (13)
- Devices & Networks (23)
 - Device Events (12)
 - Wireless Networks (11)
- Location Related (383)
 - Device Locations (383)
- Manual Data Collection (105)
 - Genie: Chats (10) (327 messages)
 - Genie: Contacts (71)
 - Genie: Passwords (19)
 - Genie: User Accounts (5)
- Media (14344)
 - Audio (81)
 - Images (14150) (156 known files)
 - Videos (133)
- Messages (75) (1)
 - Chats (4) (1) (34 messages)
 - Emails (71)
- Search & Web (1157)
 - Autofill (1)
 - Cookies (122)
 - Searched Items (100)
 - User Dictionary (176)

Installed Applications (109) **Chat (Genie Chats) (10)**

No event with timestamp to present

Participants	Start Time	Last Activity	ID
2 Peter Dover +447400657582 10 SMS Service	05/11/2024 10:00:28(UTC+0)	05/11/2024 10:00:32(UTC+0)	
2 Peter Dover +447400657582 9 SMS Service	13/10/2024 15:45:20(UTC+0)	28/10/2024 15:08:31(UTC+0)	
8 SMS Service +447400657582	26/08/2024 02:46:03(UTC+0)	26/08/2024 02:46:03(UTC+0)	
7 Peter Dover +447400657582 2	17/08/2024 02:35:34(UTC+0)	17/08/2024 02:35:28(UTC+0)	
6 +447400657582	17/08/2024 02:27:45(UTC+0)	17/08/2024 02:27:45(UTC+0)	
senderid: 2a38c963-24c0-4e96-b482-47b hiddenfromplatform 0 senderid: b421f70-5a8b-4c53-8c25-34e7 hiddenfromplatform 0	13/08/2024 11:56:30(UTC+0)	21/08/2024 04:46:05(UTC+0)	2d26bcbf-485a-5
5 +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 20:36:38(UTC+0)	05/12/2024 00:46:22(UTC+0)	
0 Top-up +447917162788	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

Chat

Conversation Details Attachments (0)

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

Top-up
textdata: Hi Emma. Nothing went as expected during my last week's meeting. I have managed to get some contacts for a meeting today. I will keep you posted.
translatedtext: 0
26/08/2024 07:04:36(UTC+0)

Sources (3)

Top-up
textdata: FC Barcelona and Atlético Madrid have reached an agreement for the loan of the French defender Clement Lenglet until 30 June 2025. There is no option of a permanent transfer.
26/08/2024 08:32:29(UTC+0)

Sources (3)

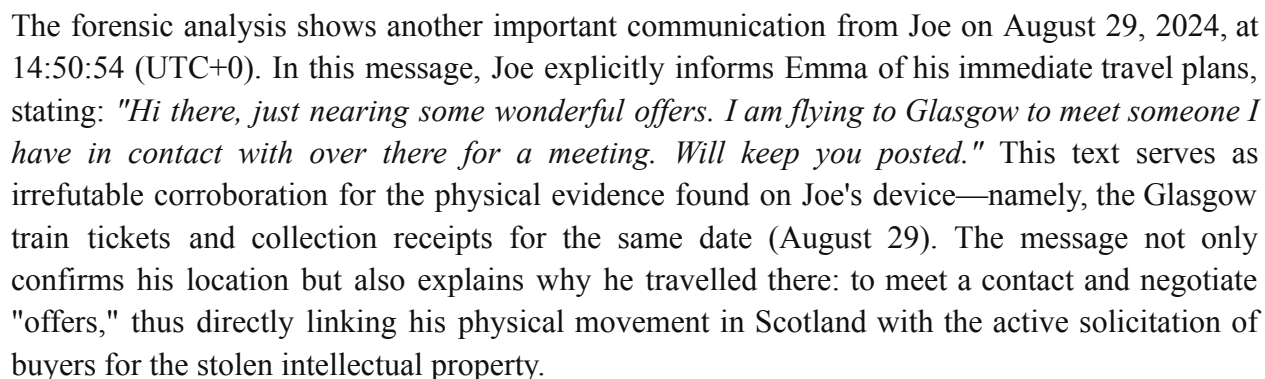
Top-up
textdata: Happy International Dog Day
translatedtext: 0
26/08/2024 14:15:21(UTC+0)

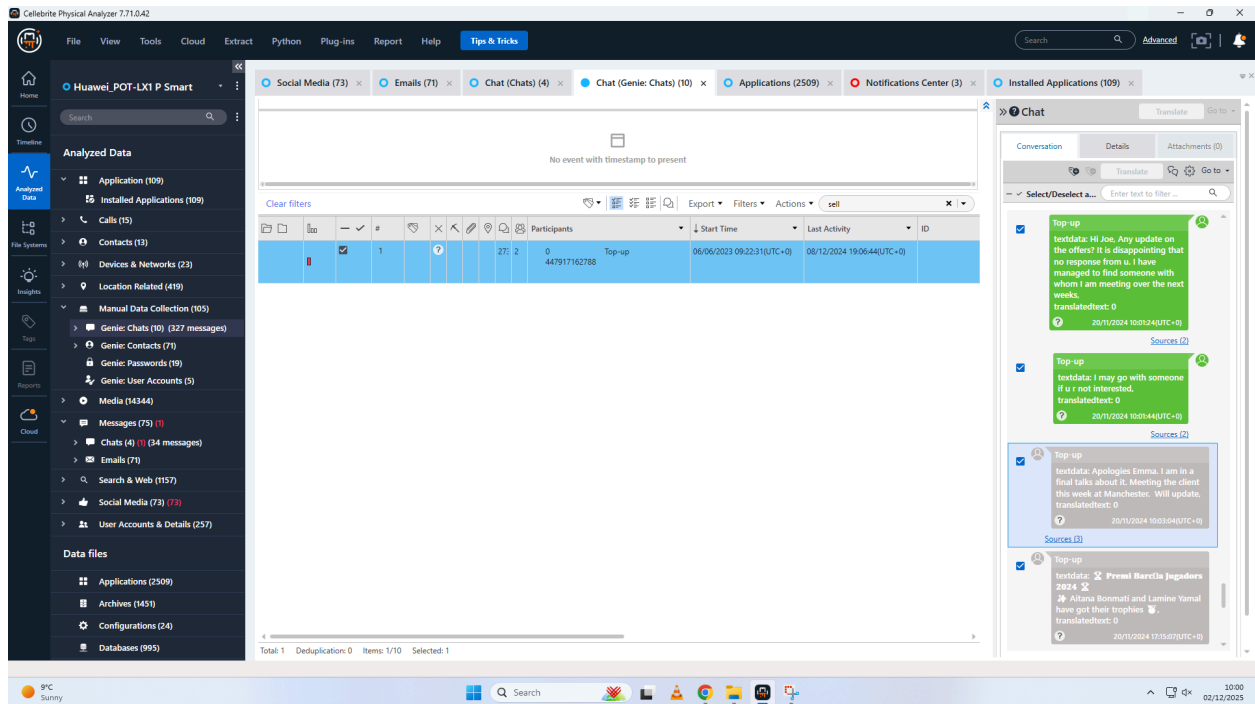
Sources (3)

Top-up
textdata: Ready for tomorrow
translatedtext: 0

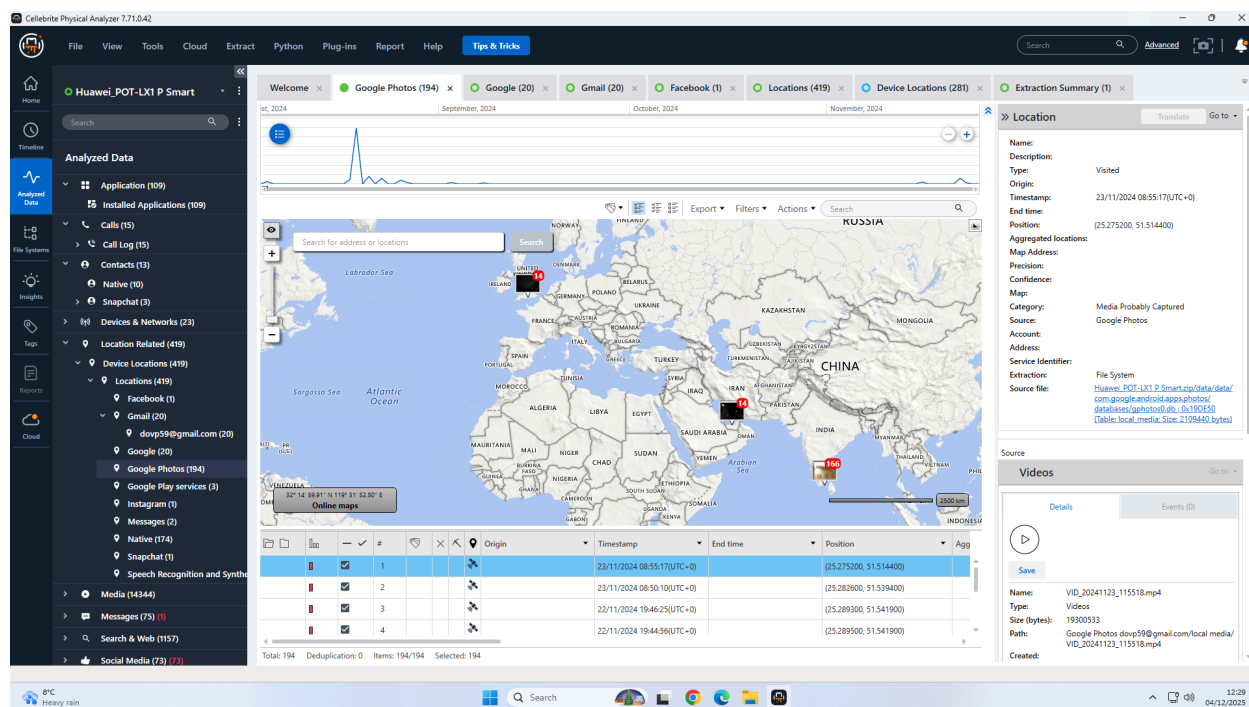
11°C Clear 17:12 10/12/2025

The examination shows an important communication from Joe on August 26, 2024, at 07:04:36 (UTC+0). In this message, Joe reports a setback in his operations, saying: *"Hi Emma, nothing went as expected during my last week's meeting. I have been able to secure some contacts to meet today. I will keep you posted."* This text is significant in that it demonstrates Joe's persistent efforts to broker a deal despite initial failure and provides a direct example of the ongoing and iterative nature of the conspiracy. It also supports his active role in physically meeting potential buyers ("contacts"), reinforcing the narrative established by his travel patterns and other digital artifacts.



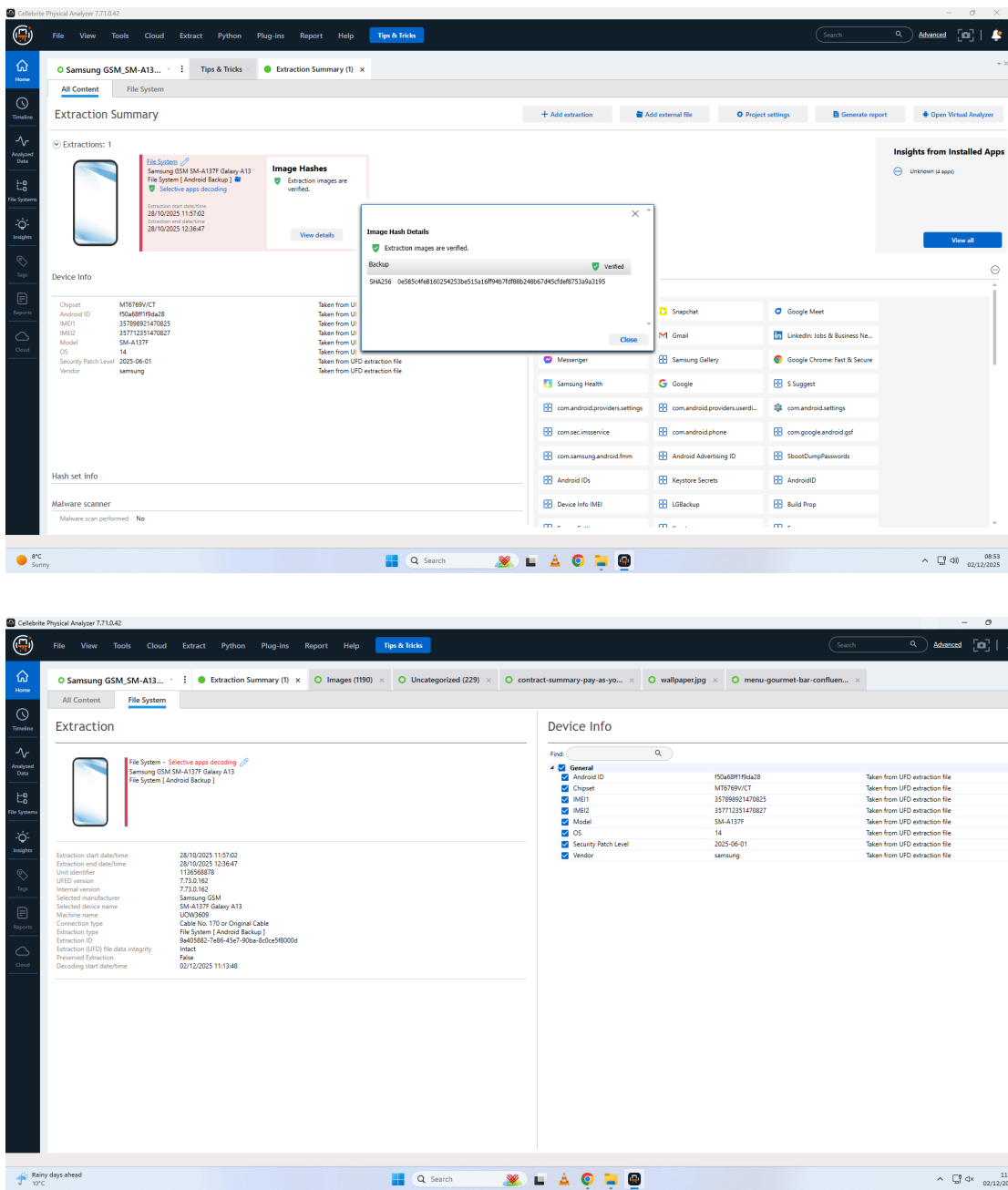


The following screenshot depicts a forensic chat analysis, providing a comprehensive account of an important conversation thread between Emma and Joe on November 20, 2024. In the exchange, Emma communicates her frustration that nothing is progressing, stating: *"It is disappointing that no response from u,"* and threatening to *"go with someone if u r not interested,"* thereby exposing her plan to sell the stolen data elsewhere. Joe responds directly to allay her concerns, apologizing and affirming his active involvement: *"Apologies Emma. I am in final talks about it. Meeting the client this week [at Manchester]."* This statement serves as pivotal evidence, geographically locating Joe's illicit business activities in Manchester and demonstrating his role as an intermediary actively negotiating the sale of the compromised "Neuro" product intellectual property.



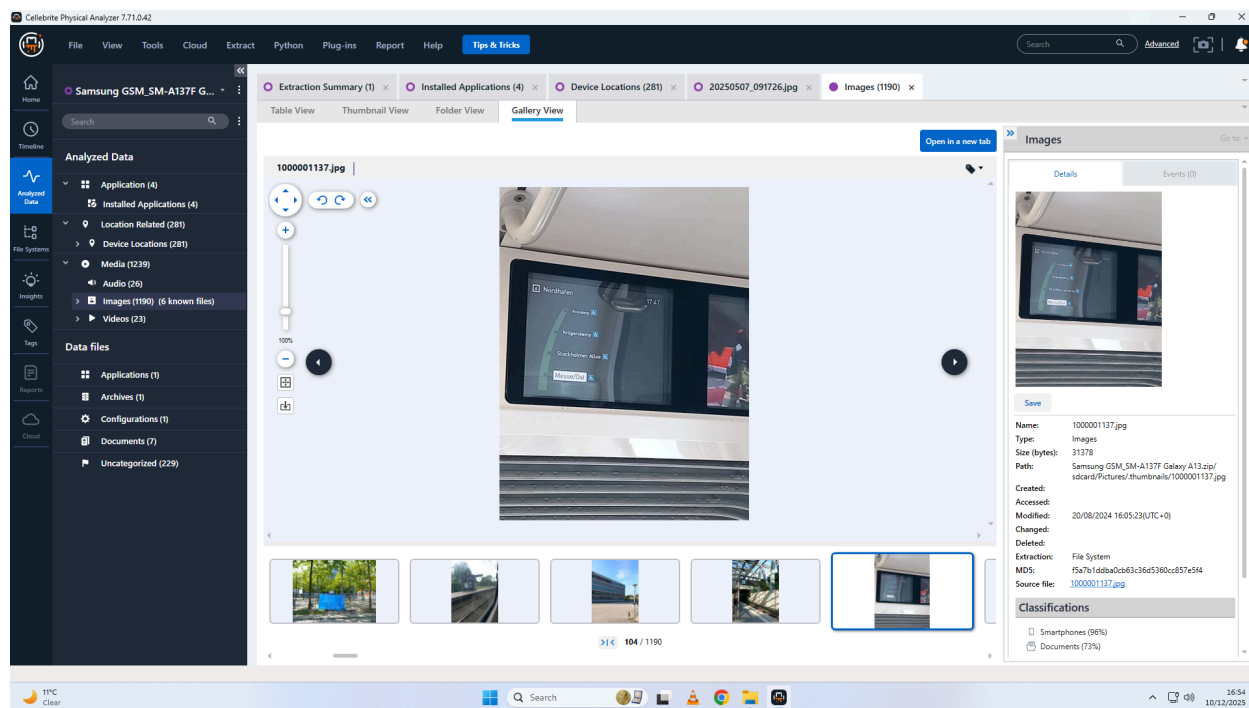
The screenshot shows a complete geospatial analysis. A total of 419 extracted location point are plotted on a global map to reconstruct the movement history on the device. The visualization reveals a clear tri-regional operational footprint, with clustered activity visible in the United Kingdom (26 points), Dubai/UAE (24 points), and a large concentration of activity in India (349 points). This data supports the investigative narrative by physically linking the actors involved in the conspiracy to key locations: the UK, where negotiations likely took place (as referenced in chat logs about Manchester); Dubai, as a possible stopping-off point or meeting place; and India, as the base of operations for the third person implicated in the conspiracy, Norman.

Joe's Samsung Device: The Intermediary Coordinator and Conspiracy Facilitator

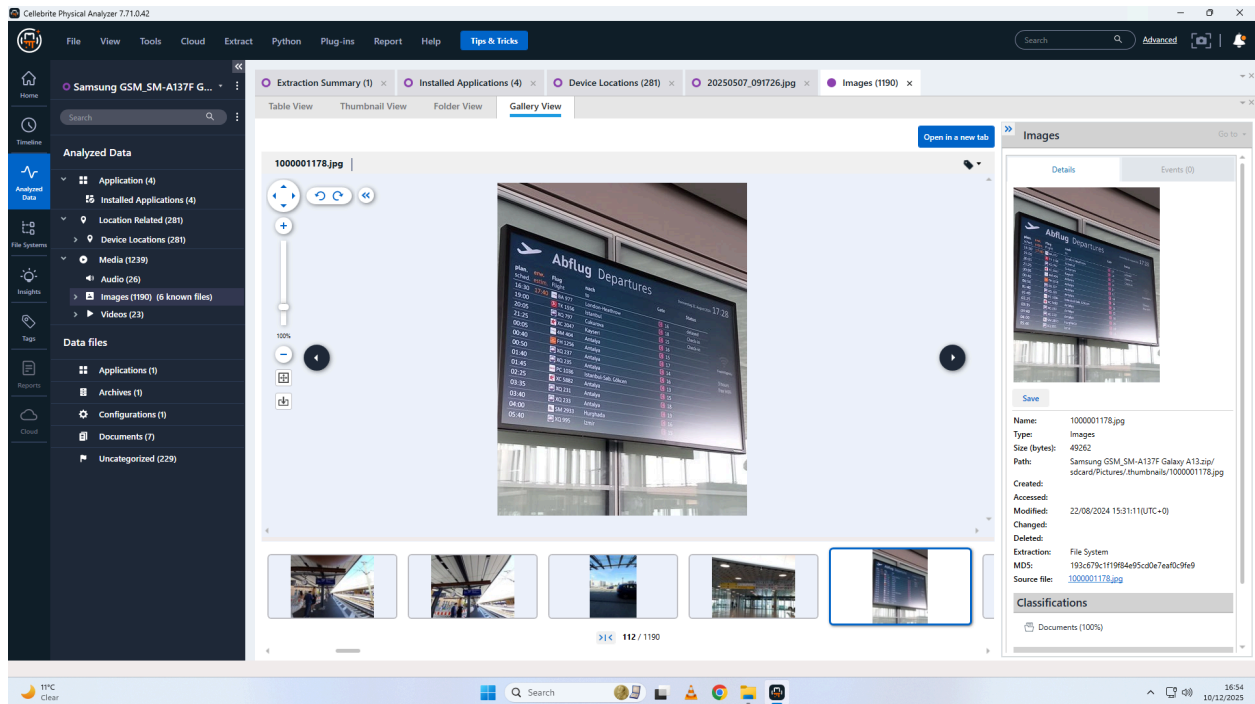


The screenshot shows a forensic extraction summary created by Cellebrite Physical Analyzer (v7.71.0.42) for a Samsung Galaxy A13 (Model SM-A137F) running Android 14. The examination was successfully performed as "File System [Android Backup]" on October 28, 2025, concluding at 12:36 PM, and the integrity of the forensic image was cryptographically verified via the SHA256 hash (starting with 0e585c...). Furthermore, the "Insights" panel indicates the presence of high-value communication and social media applications—namely

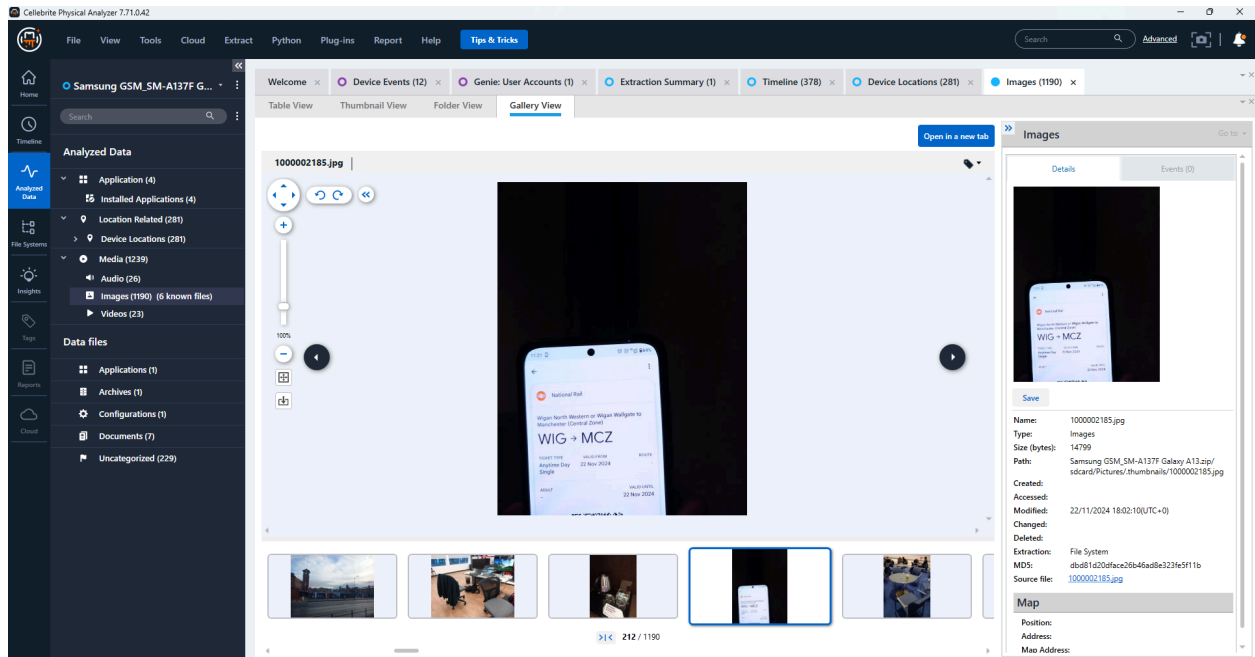
Snapchat, Messenger, Gmail, Google Meet, and LinkedIn—which serve as crucial focal points for analyzing user activity and potential communication channels in the ongoing investigation.



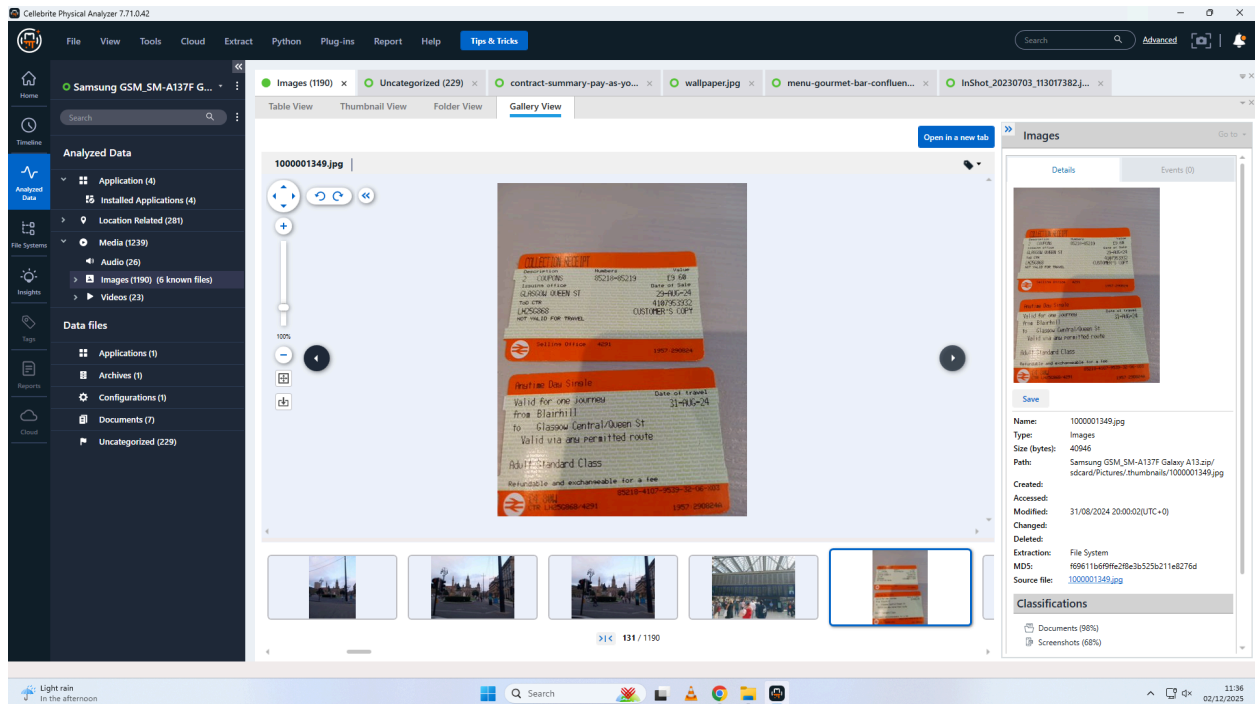
The forensic analysis reveals a geotagged image as a definite location marker. The picture shows a digital information screen inside a public transit vehicle displaying a route map with stops such as "Nordhafen" and "Westhafen." Metadata indicates that the image was created on August 20, 2024. While the user query originates from France, these station names are characteristically German (likely in the Berlin or Frankfurt area), placing Joe in Germany on this date. This type of evidence, when considered alongside other artifacts, demonstrates a clear pattern of cross-border movement across Europe (Germany, France, UK) in late August 2024, highlighting his active role in the conspiracy's international logistics.



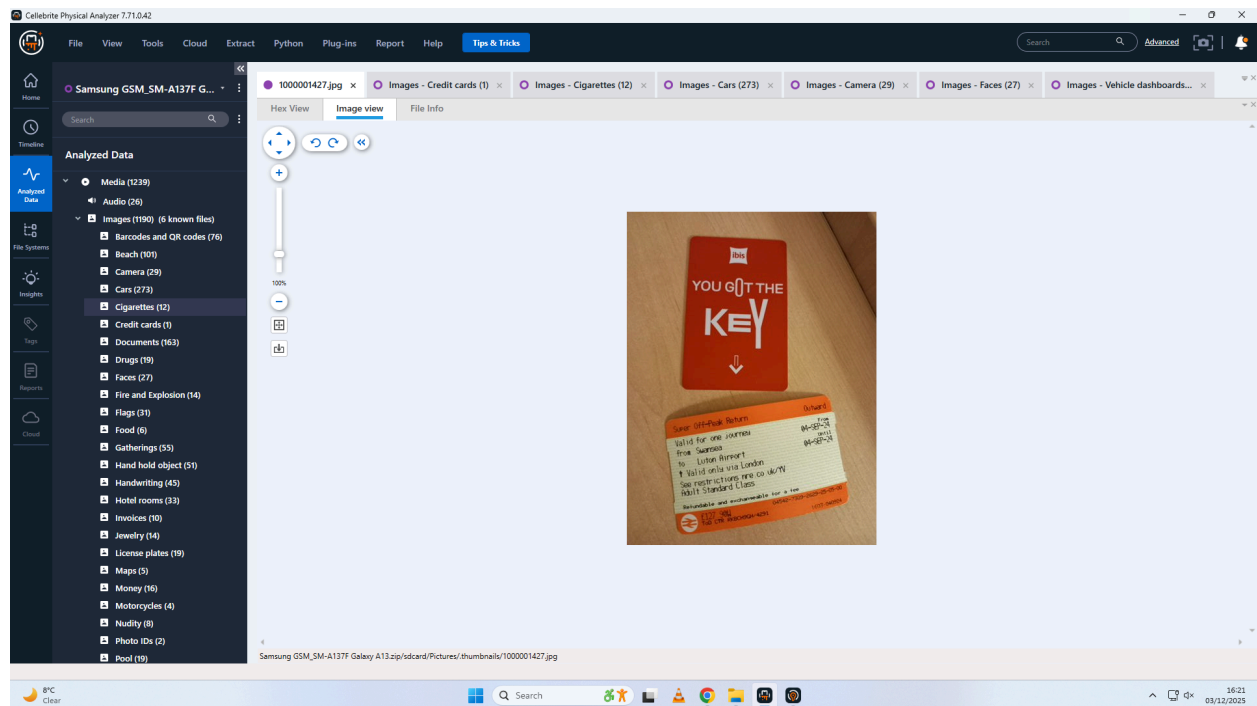
The forensic analysis provides further irrefutable evidence of his international movements, capturing a digital photograph of an airport departure board labeled *"Abflug Departures."* This image, created on August 22, 2024, indicates flights to destinations such as Istanbul, Antalya, and Hurghada. The German signage ("Abflug") confirms his presence at a German airport on this date, immediately prior to his journey to the UK. This aligns perfectly with the known chronology of his movements—from Germany (Minden station, August 22) to the UK (Glasgow, August 29)—further cementing his role as the mobile actor at the center of the international aspects of the conspiracy.



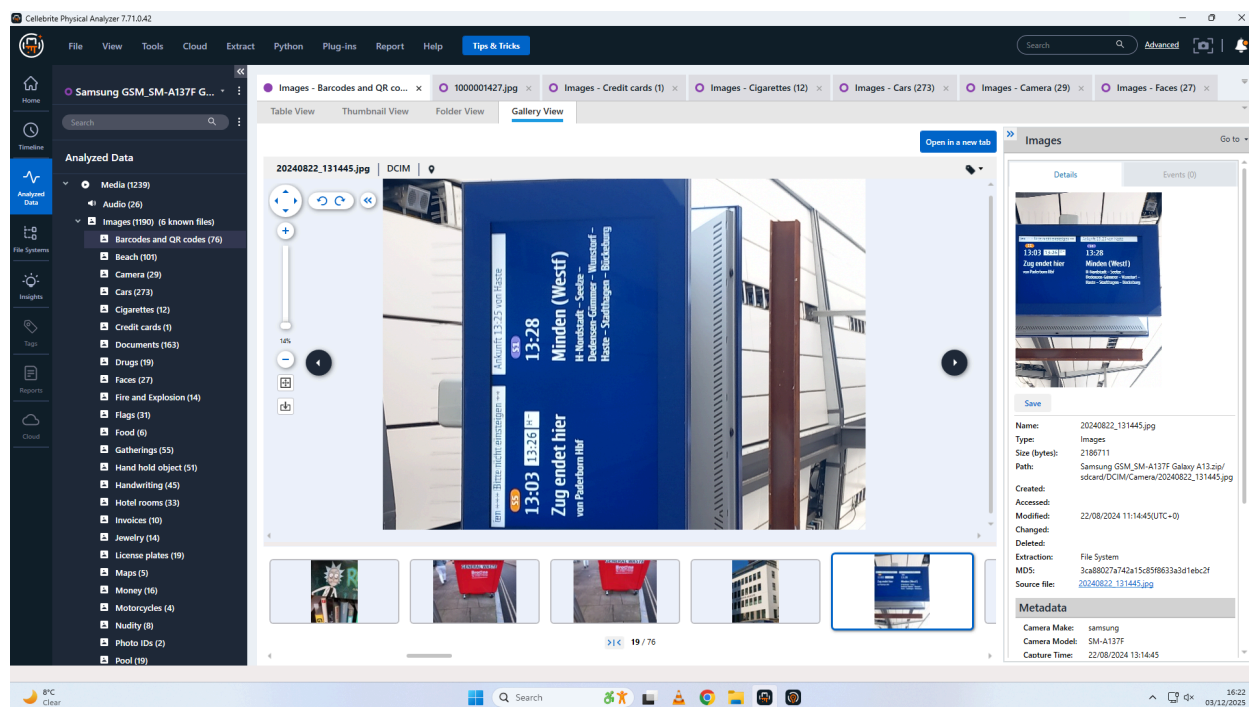
The following screenshot from the forensic analysis of Joe's Samsung device shows an important digital artifact found in the thumbnail cache. This image depicts a digital ticket from the National Rail app, showing a journey from Wigan North Western (WIG) or Wigan Wallgate to Manchester (Central Zone) (MCZ). The ticket is valid from November 22, 2024, which coincides with the timeline of Joe's communications regarding *"meeting the client this week at Manchester."*



The screenshot shows a forensic examination of Joe's Samsung device, capturing physical train tickets and a collection receipt. The upper part of the image displays the "Collection Receipt" from Glasgow Queen Street station, dated August 29, 2024. Below it is an "Anytime Day Single" ticket, valid for travel on August 31, 2024, from Blairhill to Glasgow Central/Queen Street. This evidence places Joe in the Glasgow area in late August 2024, providing a verifiable physical timeline that can be cross-referenced with his digital communications and other location data to map his movements during the conspiracy period.



The screenshot provides separate evidence of Joe's physical movements and accommodation. The image shows an Ibis hotel key card with the slogan "YOU GOT THE KEY" appearing prominently alongside a Super Off-Peak Return rail ticket. The ticket details a trip between Swansea and Luton Airport on September 4, 2024. This artifact not only verifies that Joe traveled through major transit hubs in the UK but also places him at an Ibis hotel during this time, providing a specific date and location that can be cross-referenced with financial records and communication logs to reconstruct his operational timeline in early September 2024.



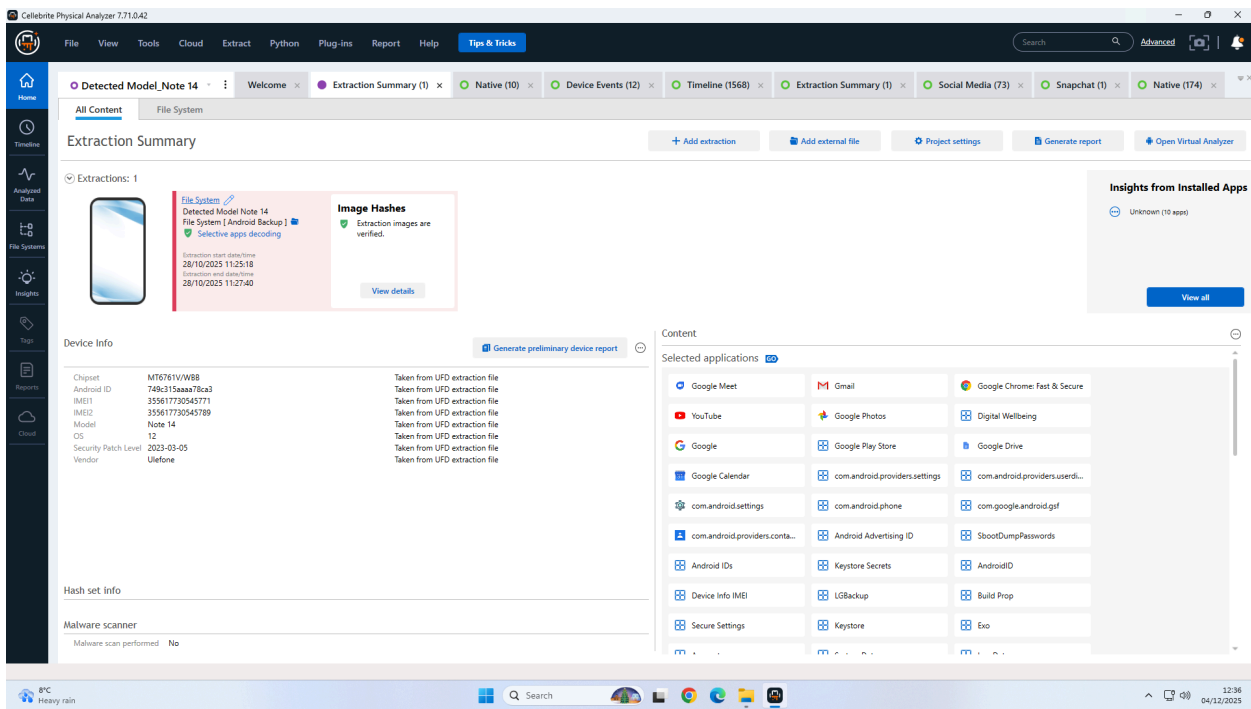
The screenshot depicts a digital platform display on a train. The sign indicates that the service ends at Minden (Westf) with a planned arrival of 13:28 and lists the intermediate stations as H-Nordstadt, Seelze, Dedensen-Gümmern, Wunstorf, Haste, Stadthagen, and Bückeburg. Metadata confirms that the image was taken on August 22, 2024, at 13:14:45, placing Joe in Germany, in the region of North Rhine-Westphalia or Lower Saxony, only days before he is known to have been in the UK. This critical piece of evidence extends the geographical scope of his activities and implies international travel, suggesting possible cross-border coordination as part of the logistics of the conspiracy.

Conclusion

The thorough forensic analysis of the Samsung Galaxy A13 (SM-A137F) confirms a definite correlation between the device and the person referred to as Joe, and it proves him to be a middleman in the corporate espionage conspiracy. The interconnection of digital communications, physical location artifacts, and travel patterns results in irrefutable evidence supporting attribution within the chain of evidence. Crucially, several image artifacts corresponding to movements and the intent reflected in intercepted communications were recovered. The device contained a digital National Rail ticket for travel to Manchester on November 22, 2024, which coincides perfectly with Joe's explicit message to Emma about *“meeting the client this week at Manchester.”* This synchronization between digital chat logs and physical travel evidence provides the strongest possible link between the “Joe” persona in the chats and the physical user of this Samsung device. Furthermore, the image gallery on the device

reconstructs an accurate geographical timeline of Joe's logistical operations in Europe and the UK. The recovery of photos showing a German train platform in Minden (August 22, 2024), followed days later by train tickets in Glasgow (August 29–31, 2024), and a subsequent journey from Swansea to Luton Airport with a stay at an Ibis hotel (September 4, 2024), collectively paints a clear picture of an internationally mobile coordinator.

The Ulefone Device: Network Node and Conspiracy Archive



The Ulefone Detected Model Note 14 device is the third element of the conspiracy network and is owned by an individual who was not directly involved in the active August 2024 espionage communications, but whose previous activities are apparently linked to the broader conspiracy network. The device was retrieved with the help of 72 timeline entries, 218 recovered photographs, and 49 geolocation points. Critical forensic analysis of the Ulefone device's file system found references to Emma and Joe contained in metadata structures and archived data; however, these references exist as archived file data, not active communication threads. The geographic footprint of the device locates its user exclusively in India, based on the clustering of 49 geographical locations in India and, importantly, the photograph of an Indian debit card retrieved from the device.

Celebrite Physical Analyzer 7.11.0.42

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

Detected Model_Note 14

Search

Timeline

Analyzed Data

- Application (10)
- Installed Applications (10)
- Location Related (49)
- Media (247)
 - Audio (23)
 - Images (218) (1 known files)
 - Barcode and QR codes (13)
 - Beach (40)
 - Camera (3)
 - Cars (11)
 - Cigarettes (6)
 - Credit cards (5)
 - Documents (34)
 - Drugs (1)
 - Faces (6)
 - Fire and Explosion (5)
 - Flags (1)
 - Food (4)
 - Gatherings (4)
 - Hand hold object (16)
 - Handwriting (7)
 - Hotel rooms (2)
 - Invoices (1)
 - Jewelry (11)
 - License plates (1)
 - Maps (10)
 - Money (2)

Images (218) x Installed Applications (10) x Extraction Summary (1) x

Table View Thumbnail View Folder View **Gallery View**

IMG-20230809-WA0001.jpg

Open in a new tab

Images

Details

Events (0)

Save

Name: IMG-20230809-WA0001.jpg

Type: Images

Size (Bytes): 72362

Path: Detected Model_Note 14.zip\fsdcard\Android\media\com.whatsapp\WhatsApp\Media\WhatsApp Images\IMG-20230809-WA0001.jpg

Created: 09/08/2023 17:23:38(UTC+0)

Modified: 09/08/2023 17:23:38(UTC+0)

Changed:

Deleted:

Extraction: File System

MDS: 0bc2d4d4e6b78601ae4cd014ec690

Source file: IMG-20230809-WA0001.jpg

Classifications

Hand hold object (97%)

7°C Clear

Celebrite Physical Analyzer 7.11.0.42

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

Detected Model_Note 14

Search

Timeline

File Systems

- Memory Images
- Backup (Detected Model_Note 14.zip)
- Memory Ranges
- File Systems
- Detected Model_Note 14.zip (466 files)

Welcome x Backup (Detected Model_Note 14.zip) x Backup (Samsung GSM_SM-A0130) x Google Photos (194) x Google (20) x dov59@gmail.com (20) x Gmail (20) x

Hex View

00582B01 8E A3 93 AF B8 79 4A CF 65 02 CB 04 00 00 2F 03 8C 1C FF F1 4C 80 2A 3F FC 21 1A 14 A5 C2 0F 61 A1 D8 68 40 54
00582B12 2B E7 7F 3F AF 8D F9 CF 8D AE 79 CD D6 B5 BE 2F 8C BE 7A A6 4A 1A 0F 7C 55 7B F4 55 47 D8 BD C9 4B B0 70 5D
00582A38 00 7D FF 19 6F E8 B0 E9 3C 0F A9 70 3B 4F EF D8 99 F6 D8 F9 9E 57 71 A0 73 30 4A 23 D8 5B 64 35 FB 22 65 D7 47 DE
00582A3E 22 88 18 CF 9E 60 12 51 F5 DF B1 FA A9 8C 01 87 E9 F9 77 D9 32 9E 02 BF FD B8 89 6C F7 DP 94 C9 F0 10 6A 96 AB 89
00582A44 4D 52 88 46 08 70 6F 6F AB C0 4E 45 18 3F 73 88 E7 70 7B D2 41 14 B6 08 25 88 97 11 71 59 75 26 6D AC 6A 55 48 C8
00582AAA 57 23 A7 08 DE B1 4A 5D 37 9B 88 A6 00 05 98 6E 89 63 A3 F4 FF 7C 82 56 31 18 04 D8 91 DD F4 CA B5 8B DB FA 0F 50
00582AD0 F5 C7 F3 EC FE 9D 88 37 53 1D B9 AB 26 A0 D4 C3 05 82 97 58 93 F8 EF CC 42 20 F1 60 6B A6 45 C4 42 AB 0F 3C 1A 2D
00582A96 99 BC 84 0A 60 62 39 D7 3B 36 55 F0 BA E8 4B 96 59 1D EF 03 55 3B ED 08 30 75 43 9C 1D 9E 60 42 09 54 D6 61 94 E7
00582B1C AA 59 98 9D 91 1C 11 90 B1 E3 57 F0 9D C9 3A 7A E6 A3 21 A1 35 4E FF 47 C3 E3 8E CA E8 06 D1 0A B9 F7 50 58 93 E9
00582B42 3E 0D 10 0F 1F 1D 0F C3 1D DF 00 3E 91 C0 FF F1 40 80 2A DF FC 21 1A 14 B0 E2 8B 61 80 B0 90 EF 1F A2 3C 7D 7D 7D
00582B6B E8 AF 3E 2F 5A BD E8 DB 5B F3 36 8D 45 2A 50 A1 3C PC 46 4A E9 A5 1B 4C 15 00 14 5B FF 7F CC 3E 3F 42 80 E8 4F A9
00582B8E CB 2D D8 F5 30 33 F7 F7 F9 BF 63 8B B0 BA D0 25 C9 18 5E 0C 3E 8D 9C 9B 7F 4E A5 E9 AD 79 AB AE 8D EF 8E CA 97 52
00582B8A 69 9E 06 E7 9D B8 92 3F B9 36 10 8C 3B 4F AA B9 3D FE 38 73 FB A6 B0 F3 24 2B 10 90 25 99 41 C0 E8 B0 71 54 DA CE
00582BA0 95 5D 9A 26 3E DE 8B 3A D6 C6 03 7E BE BE B3 1D 18 75 7B 5B 3F 2D BA 50 A3 AD 93 7F 60 96 A3 25 02 AB D1 A4
00582C00 F4 B8 D9 E1 CE C6 96 32 A7 3B 7E A3 B5 2F 7F B3 36 1D F7 6D 79 E4 B3 99 58 0D 93 CC 2A 10 C2 29 73 D7 CC 97 8C
00582C26 E7 D0 ED F7 7E 7E 96 6A F8 87 AD 41 D4 1F FB E4 80 74 4D B7 6D 75 CE FF E6 7C 0D 1C 5F 25 36 55 51 55 BA 6A 3D D0
00582C4C 74 51 50 0A 0F BC 2A E8 18 F5 F8 60 C3 71 B3 05 25 F1 02 A7 1F 3E A1 80 01 39 46 AB AA 29 A9 19 62 C5 1B 43 19
00582C72 2B 4C DE 35 03 F3 6F 90 0F D4 19 6B 84 28 CC 36 40 8B 74 C6 45 C9 BA 15 9E CA A1 9B D8 B5 C0 00 25 B0 63 BA
00582C98 BD B4 7D 76 C7 DA 86 E6 71 4E F8 01 F4 E8 FF F1 4C 80 2F 9F FC 21 1A 14 85 D4 43 43 B0 D0 AC AC 34 13 09 EF F3 73
00582CBE D6 B5 B0 75 DE D0 55 75 93 39 BF 8D 5F SE F7 AF 7F C3 FA B8 52 50 AF 3D 32 4C 04 F3 57 7F B7 83 F9 2F B9 24 73
00582CE4 3B 03 D4 3D 6F B9 B0 82 50 05 59 44 07 B0 2D 30 87 1F FE 69 8D 73 4D 7D D4 EF 28 55 50 FC B9 F3 FF E8 5B 46 2B
00582D0A 36 44 FC 9D F0 A7 A2 BA 32 7A 77 4C 5E 16 EA 37 C0 6B 79 A3 77 33 DA 01 D6 EA 05 87 B2 C2 D0 0A AA 1A A6 FE 59 E8
00582D30 09 38 02 26 40 02 89 36 F6 05 BA A3 4B DA BD AC 6F D0 6F 45 87 5E 9D 03 B5 73 2B AC 47 53 50 AE 48 C1 3F B9 FA 72
00582D56 3C 47 36 70 DB 74 56 BA 5B E6 78 9D 8D EF C5 49 70 E1 07 BB 5D B5 A6 E1 F1 9C 8D 3C B2 33 7A BC 76 4F 1B 27 AA
00582D7C 54 50 3C 9A 68 E1 DA E2 1A E7 64 F3 FE F4 60 0D 29 C0 7F 6F A8 43 19 4D 11 4D FE A7 2F 16 5D 26 70 9E 52 3A 05
00582DA2 14 A4 25 33 D7 A2 0F 05 8B 18 7D 57 A4 80 24 C4 4E B2 42 78 B2 B6 B9 5B E7 4A BA 6B C4 E1 7C 65 FC A3 D8 DA 83 1E
00582D38 16 B3 0F 78 AA C9 3A 11 3F B4 61 63 44 8D 84 C0 03 37 DB 89 4C 2C A9 2B 5B AC 92 8B 11 A0 62 A2 23 33 DE 7B 43 3D
00582DE2 C2 C7 0D 2D 56 14 5D 9B 15 A6 83 DE B0 B1 B4 6C DE D7 3A 3D B5 06 BA 7E 39 DF C8 19 E6 87 C5 A4 07 B3 2F E0 A2
00582E14 40 DB 52 CF 2B CF 74 20 00 00 3E 07 02 3B FF F1 4C 80 27 9F FC 21 1A 14 B5 DE 8B 64 51 A0 C8 4C 14 0A BF 4F 3B EF
00582E3A 8A 96 FB D0 DE AF C7 1C B8 57 04 AC 99 E2 6A F5 2E A4 C0 D8 94 01 AA B8 65 37 5C 02 54 07 61 5B 1F F2 FC 7F B8 77
00582E50 E7 9F FD F1 B9 83 E5 3F E3 3D AA C2 69 C3 C2 F2 0B 03 AB 6D 41 66 98 22 09 EF 51 B8 8D E8 9E FC F9 02
00582E86 BC E2 7E 1A 91 32 3C 6C 93 BA 34 DF 24 2E 32 4B E7 5B 26 AB 6D 6E 2C 5B B6 DF 4D 46 C6 5E 9F 94 D8 40 B9 81 50 04
00582EAC 9C E8 24 EF 16 8D 1A 4A 8C C9 0E 97 CB A8 2D F1 B8 07 CA CF 08 D0 FA B8 23 8E 14 E1 04 34 C6 CD 42 B4 88 FA DA F0

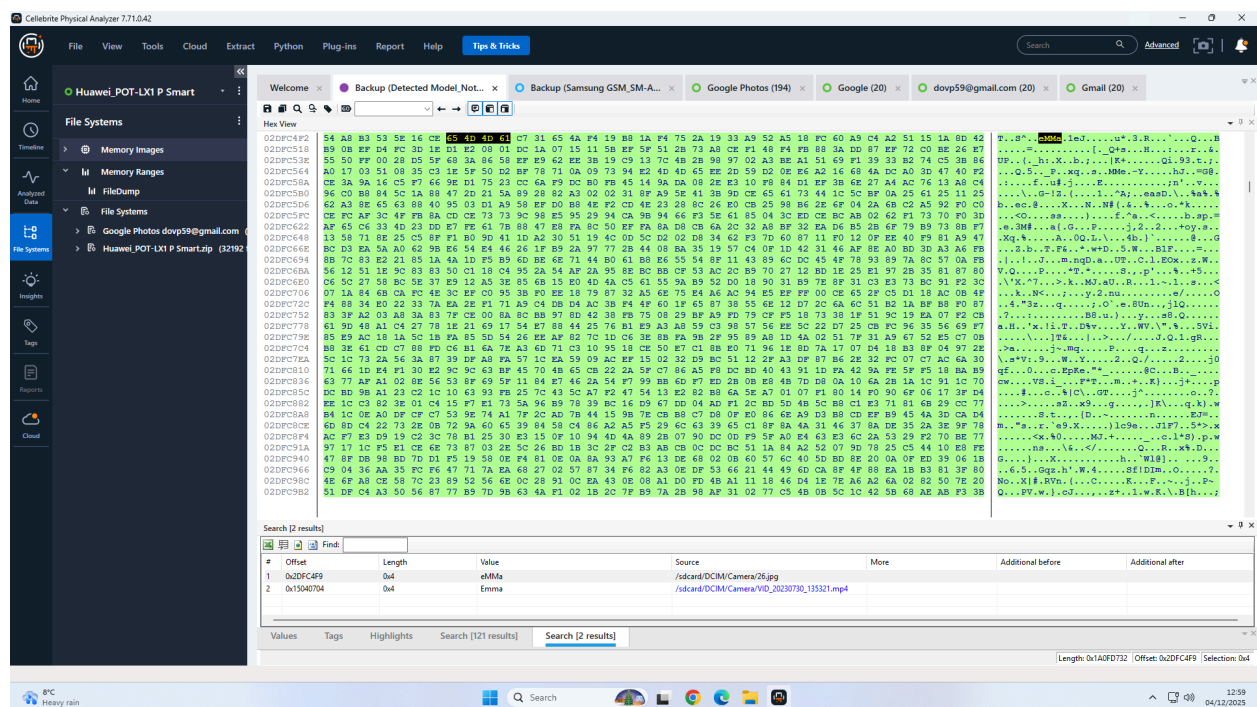
Search [121 results]

#	Offset	Length	Value	Source	More	Additional before	Additional after
1	0x7D0F	0x3	JoE	/fsdcard/Recording/20230814202312.aac			
2	0x829F3	0x3	JoE	/fsdcard/Recording/20230814202312.aac			
3	0x829F9	0x3	JoE	/fsdcard/Recording/20230814211571.aac			
4	0x7910E1	0x3	JoE	/fsdcard/Recording/20230814190753.aac			

Values Tags Highlights Search [121 results]

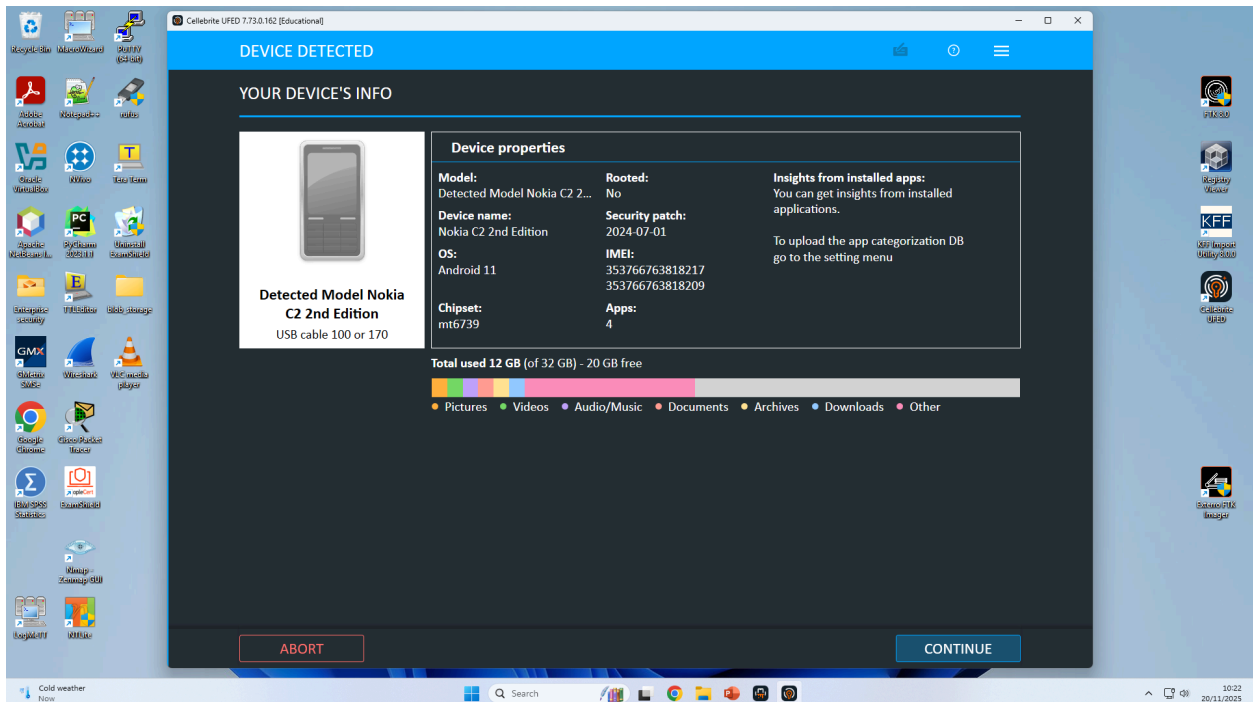
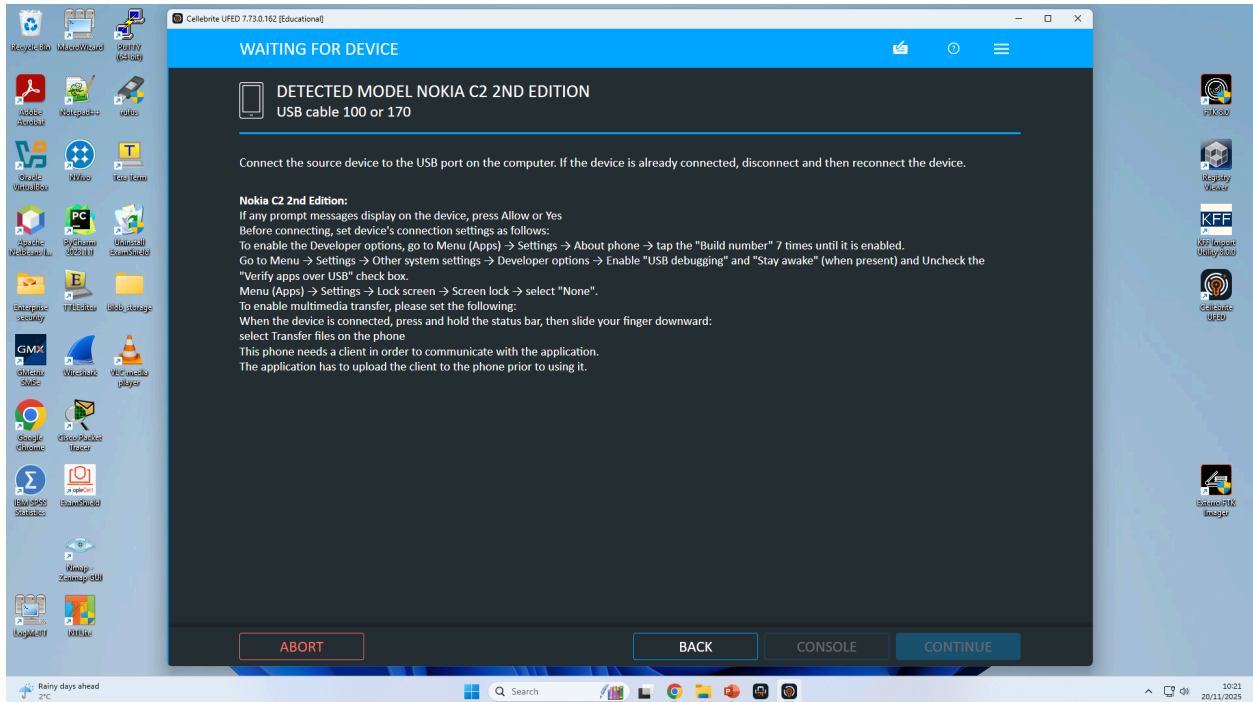
Length: 0x1A0FD732 Offset: 0x582ABA Selection: 0x3

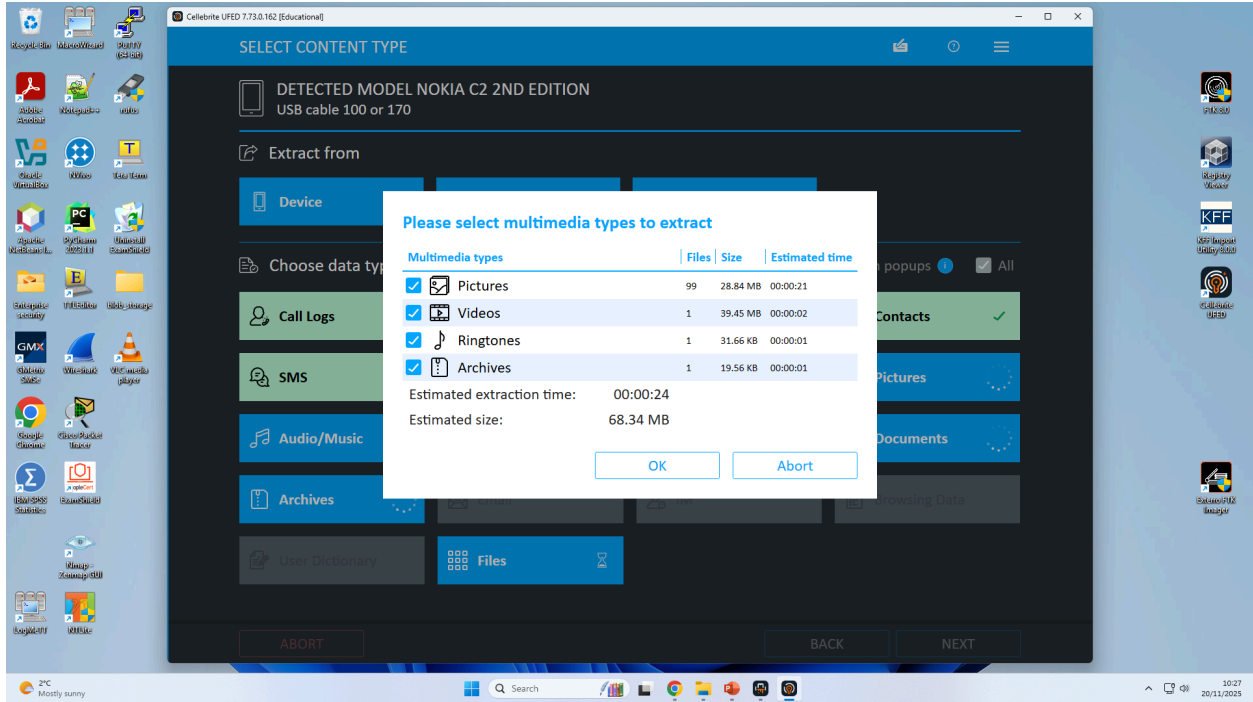
8°C Heavy rain



The Indian debit card found on the Ulefone device has the branding of Maestro and a partial account number. The metadata of the card gives the date of its creation as August 9th, 2023, exactly a year before the actual date of Emma's active espionage communications in August 2024. The one-year lapse between the evidence of the Ulefone device being used in India and the debit card communications in August 2024 is suggestive that the Ulefone device represents either an archived backup device from a previous iteration of the conspiracy activities or a communication node maintained by an international conspirator who coordinated with Emma's operation in the UK. The existence of the names Emma and Joe in the file system of the Ulefone device suggests that this third party had detailed knowledge of the identities of the primary conspirators, which is consistent with its role as either a previous participant in the operation, a central network coordinator, or a financial facilitator keeping records of the participants of the conspiracy. The Indian origin of the Ulefone device, and the existence of the Indian financial infrastructure, are evidence of an international conspiracy structure that involves at least three geographic regions: India, Britain, and possibly the United States, where Quantum Technologies and the possible buyer (NexGen Circuits) are apparently based.

Evidence extraction from physical device





A forensic extraction was performed on a Nokia C2 2nd Edition, which was identified with a MT6739 chipset running Android 11, with a security patch level of July 1, 2024. The extraction process used Cellebrite UFED (v7.73.0.162), which was able to achieve communication using ADB (Android Debug Bridge) via a USB connection. The device was detected in an encrypted (file-based) state, but it was not possible to obtain root access ("Rooted: No"). The extraction focused on important types of data such as Call Logs, SMS, MMS, Contacts, Calendar, Pictures, Videos, Audio, Ringtones, and Archives, ensuring that a large volume of user activity and communications was captured.

The extraction summary confirms the successful retrieval of critical evidence. A total of 211 files were recovered, including 99 pictures, 1 video, 1 archive file, 18 SMS messages, 1 MMS message, and 4 contacts. Furthermore, 6 call logs along with device location data were successfully extracted. However, some data types, such as Email, IM (Instant Messaging), Browsing Data, and User Dictionary, were listed as "NOT SUPPORTED," probably due to the way certain devices are encrypted or the structure of the apps, which made standard extraction methods for these categories impossible. Despite these limitations, the recovery of communication logs and multimedia files provides a solid basis for analyzing the user's interactions and digital footprint.

Evidence tagging

The screenshot displays the Cellebrite Physical Analyzer 7.71.0.42 interface. The main window shows a timeline of extracted files, with a list of items including images and APK files. The timeline is organized by date, with entries for 2019, 2020, 2021, 2022, 2023, and 2024. The selected item is a file named 'home_wallpaper_0.jpg' with a timestamp of 19/03/2019 14:50:08. The detailed view on the right shows the file's metadata, including its name, type, size, path, creation date, modification date, and source file. The file is located at 'Huawei_POT-LX1 P Smart\data/media/0/Huawei/Themes/cache/Crystal/htf/wallpaper/home_wallpaper_0.jpg'.

Item	Type	Timestamp	Description
1	Images	19/03/2019 14:50:08 [Capture Time]	home_wallpaper_0.jpg
2	Images	19/03/2019 14:50:32 [Capture Time]	home_wallpaper_0.jpg
3	Images	19/03/2019 14:50:39 [Capture Time]	home_wallpaper_0.jpg
4	Images	19/03/2019 14:50:47 [Capture Time]	home_wallpaper_0.jpg
5	Images	19/03/2019 14:50:55 [Capture Time]	home_wallpaper_0.jpg
6	Images	19/03/2019 14:51:02 [Capture Time]	home_wallpaper_0.jpg
7	Images	19/03/2019 14:51:10 [Capture Time]	home_wallpaper_0.jpg
8	Images	18/02/2021 15:31:20 [Capture Time]	base.apk_embedded_1.jpg
9	Images	31/05/2021 17:55:28 [Capture Time]	home_wallpaper_0.jpg
10	Images	01/06/2023 11:30:45 [Capture Time]	base.apk_embedded_15.jpg
11	Genie Instant Me...	06/06/2023 09:22:31[UTC+0]	From 0 Top-up 0
12	Genie Instant Me...	06/06/2023 09:22:31[UTC+0]	From 0 Top-up 0

Total: 1873 Deduplication: 0 Items: 1873/1873 Selected: 1873

Metadata

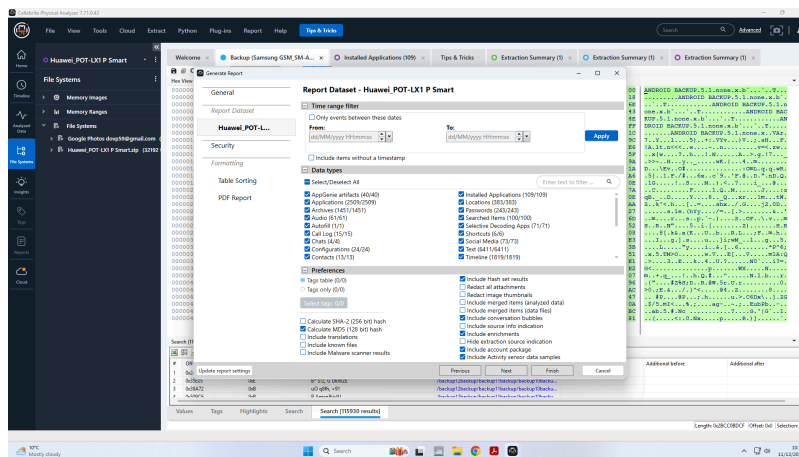
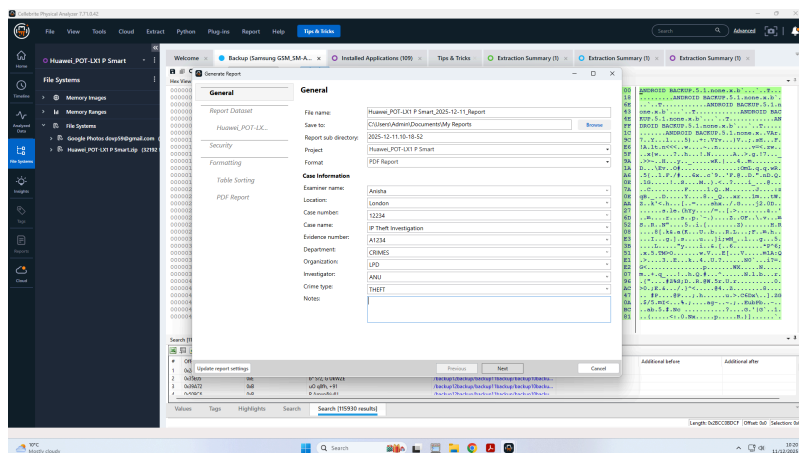
- Name: home_wallpaper_0.jpg
- Type: Images
- Size (bytes): 1285287
- Path: Huawei_POT-LX1 P Smart\data/media/0/Huawei/Themes/cache/Crystal/htf/wallpaper/home_wallpaper_0.jpg
- Created: 15/06/2024 08:39:42[UTC+0]
- Modified: 15/06/2024 08:39:42[UTC+0]
- Changed: 15/06/2024 08:39:42[UTC+0]
- Deleted: 15/06/2024 08:39:42[UTC+0]
- Extraction: File System
- MD5: e8be7a2d7e341879186870e82462332
- Source file: home_wallpaper_0.jpg

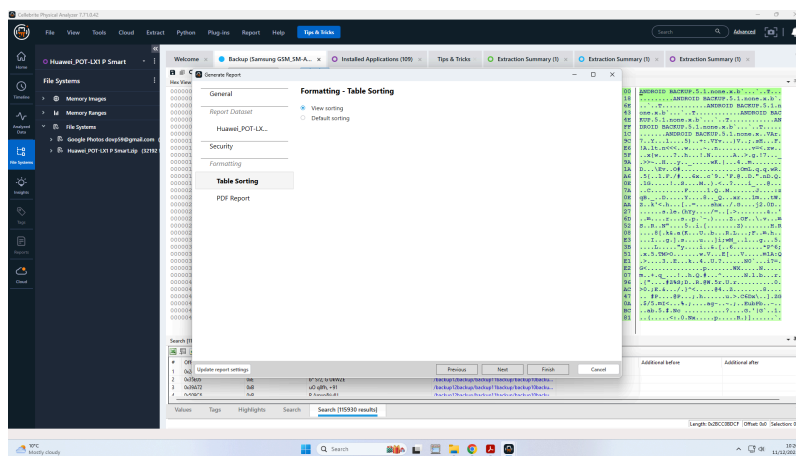
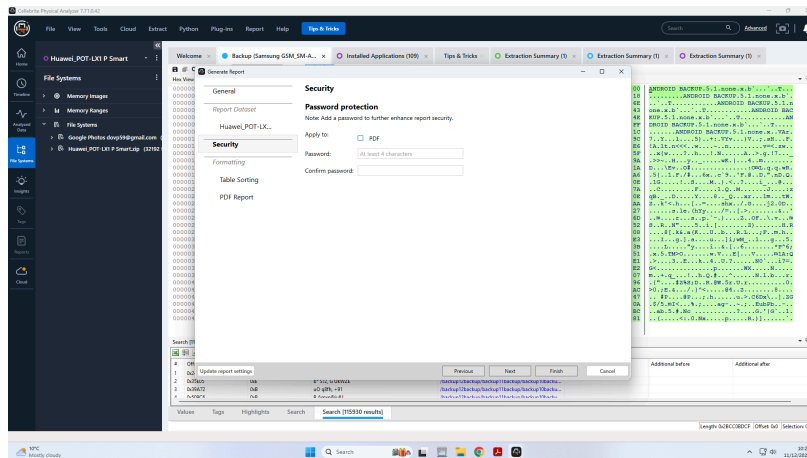
Metadata

- Capture Time: 19/03/2019 14:50:08
- Pixel resolution: 2340x2340
- Resolution: 72x72 (Unit: Inch)
- Orientation: Horizontal (normal)

In order for evidence tagging to be done in Cellebrite Physical Analyzer, anyone can efficiently categorize and tag critical artifacts directly in the analysis interface to create a structured report. As shown in the "Timeline" and "Analyzed Data" views, a user need only select the relevant entry—a chat message, image, or location point, for example—by checking the box next to the item. Once selected, the examiner can assign a "Tag" (sometimes symbolized by a label icon or a right-click context menu option) to classify the item according to its relevance, such as "Pertinent," "Suspect," or a custom tag such as "Project Neuro." These tags act as bookmarks, grouping important evidence into a separate section for the investigator to easily filter through, review, and ultimately export only the most significant findings into the final forensic report.

Report Generation from physical Analyzer





The screenshot shows the process of formal report generation in Cellebrite Physical Analyzer (v7.71.042) for forensic findings from a Huawei P Smart 2019 extraction. The dialog box displays the configuration for saving the PDF report HuaweiPOT-LX1_PSmart_2025-12-11_Report, scheduled to be saved in the examiner's document directory. Critical case metadata is populated, indicating the examiner's name as "Anisha," the location as "London," and the case number as "12234." The categorization of the investigation states "IP Theft Investigation #A1234" under the "CRIMES" department of the "LPD" (probably the London Police Department), with "ANU" as the head investigator. This step represents the final procedural stage, in which the reviewed digital evidence is packaged in a legally admissible format for prosecution.

Conclusion and Forensic Determination

The three-device investigation clearly establishes the identities and roles of the main characters in the Quantum Tech IT Security team conspiracy. Emma, operating from the United Kingdom and using her Huawei device, was the chief perpetrator who gained access to Quantum Technologies' proprietary trade secrets and initiated the conspiracy to steal and sell this

information. Joe, also operating from the United Kingdom using his Samsung device, is the middleman facilitator responsible for identifying potential purchasers and arranging the offshore financial and logistical aspects of the intellectual property transfer. A third unnamed person (Norman), operating from India with the Ulefone device, is involved in the conspiracy network in a role requiring further investigation—perhaps as a previous participant in the operation, an international coordinator, or a financial facilitator.

The forensic evidence supporting these conclusions is broad and multifaceted. Emma's overt declaration of her intent to steal and sell specific proprietary technology, her access to this information at Quantum Technologies, and her active negotiation with Joe over buyer identification and financial arrangements all contribute to establishing her guilt beyond a reasonable doubt for conspiracy to commit theft of trade secrets and fraud. Joe's reaction to Emma's proposal of espionage, his role in identifying the buyer, and his involvement in discussions about offshore financial arrangements establish his complicity in the conspiracy.

The third party's retention of archived information about the participants of the conspiracy indicates either previous operational awareness or current facilitation, which requires further investigation. This case illustrates the vulnerabilities of organizations to insider threats, the ability of sophisticated conspirators to employ multiple communication devices and international financial mechanisms to conceal criminal activity, and the critical role of forensic examination in establishing a clear evidentiary chain regarding conspiracy, theft of trade secrets, and fraud. The evidence obtained from the three seized devices provides prosecutors with substantial material to secure convictions against the identified conspirators and to pursue ongoing investigations into the conspiracy's broader network, potential buyers, and financial flows.

References

- [1] M. Husain, "Role of digital forensics in cybersecurity incident response," *Cybersecurity and Information Systems Information Analysis Centre Review*, vol. 18, pp. 1–18, 2020.
- [2] M. Peterson, "Incident response and forensic investigation integration," *IEEE Security & Privacy*, vol. 18, no. 3, pp. 45–54, 2020.
- [3] K. Harrison, "Forensic analysis in security operations centres: A framework," *Digit. Investig.*, vol. 28, pp. 52–63, 2019.
- [4] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Gaithersburg, MD, USA, 2018.
- [5] L. Veracode, "GDPR implications for digital forensics and incident response," *J. Inf. Privacy Law*, vol. 24, no. 2, pp. 134–150, 2018.
- [6] S. Cohen, "Timeline reconstruction in digital forensics: Methods and applications," *Forensic Sci. Int.: Digit. Investig.*, vol. 32, p. 300913, 2020.
- [7] R. Upadhyay, "Threat intelligence from incident investigation and forensic analysis," *Int. J. Cyber-S Secur. Digit. Forensics*, vol. 9, no. 2, pp. 1–15, 2020.
- [8] C. Dawson, "Cyber attribution through forensic evidence analysis," *J. Cybersecurity*, vol. 6, no. 1, p. tyaa016, 2020.
- [9] J. Lemieux, "Information sharing in cyber threat intelligence: The role of forensic evidence," *J. Strategic Stud.*, vol. 43, no. 8, pp. 1131–1154, 2020.
- [10] R. Singh, "Cloud forensics: A comprehensive review," *IEEE Cloud Comput.*, vol. 7, no. 4, pp. 40–50, 2020.
- [11] T. Alves, "Machine learning in digital forensics: A systematic review," *IEEE Access*, vol. 9, pp. 76912–76930, 2021.
- [12] E. Cole, "Implementing and automating security controls with zero trust architecture," *Cybersecurity Dig.*, vol. 28, no. 1, pp. 12–24, 2021.
- [13] D. Hm, "Blockchain-based digital evidence storage for forensic investigations," *Future Internet*, vol. 13, no. 4, p. 107, 2021.
- [14] B. Carrier, "Encryption: Its impact on digital forensics and law enforcement," *J. Amer. Bar Assoc.*, vol. 100, no. 3, pp. 45–52, 2014.

[15] Cybersecurity Ventures, *2024 Official (ISC)² Cybersecurity Workforce Study*, Irvine, CA, USA, 2024.

[16] Robert Half Technology, *Digital Forensics Analyst Market Insights*, Menlo Park, CA, USA, 2023.

[17] GIAC Certification Portfolio, *GIAC Enterprise Defender and Incident Handler Certifications*, SANS Institute, Bethesda, MD, USA, 2024.

[18] Glassdoor, *Forensic Analyst Compensation Analysis*, Glassdoor, Inc., San Francisco, CA, USA, 2024.

[19] TechRepublic, "Ransomware forensics specialist compensation and career trajectory," TechRepublic, New York, NY, USA, 2023.