



MODULE TITLE:

Digital Forensics Analysis

STUDENT NAME: MIZANUR RAHMAN

STUDENT ID: 2433477

COURSE: MSc Cybersecurity and Digital Forensics

LECTURER: Dr. Mohamed Ghanem

DATE OF SUBMISSION:

12th December 2025

Task 1: Research Report on Digital Forensics

Title: "Current Trends, Challenges, and Future Directions in Digital Forensics"

1.Current State of the Field — Tools, Features and Capabilities

The field of digital forensics has grown substantially in both scope and sophistication. As devices proliferate and digital crime becomes more widespread, forensic practitioners rely on a range of specialized tools — both open-source and commercial — to extract, preserve, and analyse digital data. For example:

- i. Open-source forensic platforms like Autopsy remain widely used for disk/volume analysis, metadata extraction, file indexing, and artefact recovery, and through the underlying The Sleuth Kit they benefit from active community support and cross-platform compatibility [1].
- ii. Commercial suites such as FTK Imager and other commercial forensic toolkits continue to support imaging (E01, DD, etc.), hash-based integrity checking (MD5/SHA1 or more modern hashes), deleted data recovery, and encrypted volume handling, allowing forensic investigators to deal with legacy file systems and storage media. This remains essential for classic file-system level investigations [2].

However, beyond legacy disk and file forensics, today's field must handle far more complex data types: cloud storage, volatile memory (RAM), mobile devices, network logs, application metadata, and data from IoT or distributed systems. A recent comprehensive survey of digital-forensics trends identifies six major subdomains — including cloud, network, IoT, mobile, database, and multimedia forensics — each with distinct challenges (heterogeneity, encryption, data volatility, jurisdiction and multi-tenancy) that demand specialized methods [3].

In short, the field is mature in its foundational tools and workflows, but also under constant pressure to evolve to handle new technologies and data types — requiring continuous development, evaluation, and standardization.

2 .Intersection of Digital Forensics and Cybersecurity

Digital forensics and cybersecurity are deeply intertwined. On one hand, forensic analysis is critical after a breach or cyber-incident: investigators reconstruct what happened, identify attackers, determine scope of compromise, and produce evidence for prosecution or remediation. On the other hand, forensic readiness — preparing systems and logging to support future investigations — is increasingly seen as part of a broader cybersecurity strategy: ensuring systems are designed with evidence collection, log integrity, and compliance in mind from the outset. This integration of forensics into incident response

operations is often referred to under the umbrella of DFIR (Digital Forensics and Incident Response) [4].

Furthermore, the security-compliance environment (e.g. data privacy laws, cross-border regulations, cloud-jurisdiction complexity) forces organizations to maintain detailed logs, enforce audit trails, and ensure evidence preservation — demands that lie at the convergence of cybersecurity hygiene and forensic readiness [5].

Thus, modern digital forensics cannot be treated in isolation: it is a core component of a holistic cybersecurity posture, especially given today's threat landscape (cloud breaches, ransomware, insider threats, etc.).

3..Emerging Trends in Digital Forensics

The digital forensics domain continues to evolve, with some of the most significant emerging trends being:

I. Cloud & Multi-Cloud Forensics: As organizations increasingly adopt cloud infrastructure (across multiple cloud providers), forensic investigations must adapt. Recent studies highlight the need for frameworks capable of handling evidence in cloud environments — factoring in audit logs, multi-tenancy, data volatility, and compliance across jurisdictions [6][7].

ii. AI / Machine Learning / Automation: The use of AI and ML in forensics is gaining traction — for tasks such as log analysis, anomaly detection, pattern recognition, metadata correlation, and automation of evidence triage. A 2025 study demonstrates an AI-enhanced privacy-preserving forensics framework for cloud settings using zero-knowledge proofs, showing how AI can support both forensic integrity and privacy compliance [8].

lii. AI-Driven Cloud Forensics Frameworks: New frameworks aim to combine traditional forensic process models (identification, collection, preservation, analysis, presentation) with automated and ontology-driven log analysis, especially for cloud environments. For example, the proposed **Cloud Investigation Automation Framework (CIAF)** leverages AI / ML to reduce manual workload, improve accuracy and speed up investigations in multi-cloud contexts [8].

iv. Scalability & Data Volume Handling: Given the explosion in data volumes — from cloud storage, IoT devices, network logs, and multimedia — forensic practices increasingly require scalable, automated, high-throughput workflows. Surveys and industry reports highlight that the shifting landscape demands forensic readiness at scale, not just point-in-time investigations [7].

These trends illustrate a shift: from manual, disk-by-disk analysis toward scalable, automated, intelligence-driven forensic methodologies — combining cybersecurity, big data analytics, and AI/ML

4. Key Challenges

Despite progress, digital forensics faces significant challenges, particularly in modern cloud-based contexts.

Difficulties specific to the cloud Cloud computing hampers evidence collection, preservation, and chain-of-custody due to data instability, multi-tenancy, lack of physical storage access, distributed logs, and jurisdictional/legal complexity [5].

Resource and competence shortages, as well as a case backlog, are straining forensic labs and practitioners. According to a 2024 practitioner poll, many investigators face limited resources and greater pressure to manage difficult investigations [3].

Reliability and Trust in AI-Assisted Forensics: While AI/ML-powered frameworks (such as CIAF) promise efficiency, issues regarding algorithmic bias, interpretability, and legal admissibility remain, especially when evidence must stand up in court. Some authors argue that explainable AI (XAI) in forensics is necessary to maintain transparency and confidence [5].

Standardization, legal, and compliance issues: Because cloud environments can span many jurisdictions, guaranteeing compliance (e.g., data protection regulations, privacy legislation) and maintaining a verifiable chain of custody are still difficult. There is presently no global standard for multi-cloud forensic readiness, complicating cross-border or multi-tenant investigations [7].

5. National and International Job Market (Industry Outlook)

The global digital forensics market size is projected to grow significantly: from an estimated USD 15.67 billion in 2025 to approximately USD 46.14 billion by 2035, at a compound annual growth rate (CAGR) of around 11.4% [8].

This growth is driven by increasing cybersecurity breaches, demand for compliance, cloud adoption, regulatory pressures, and the need for advanced forensic tools and services, especially in regulated sectors [6].

As digital evidence becomes more complex and voluminous (cloud, IoT, mobile, network logs), there is rising demand for practitioners skilled in both traditional forensics and modern, cloud-/AI-based forensic techniques [3].

The employment outlook in digital forensics appears strong — but entering the field increasingly requires technical competence (cloud, memory forensics, log analysis), familiarity with AI/ML-based tools, and understanding of compliance and legal frameworks.

6. Conclusion & Recommendations

Digital forensics today sits at the convergence of law enforcement, cybersecurity, cloud computing, and data science. As digital crime evolves — spanning cloud platforms, mobile devices, encrypted communications, IoT, and more — forensic practices must adapt. The integration of automation, AI/ML, scalable frameworks, and cloud-aware forensic readiness is becoming essential.

However, technological advances alone won't solve all problems: challenges around legal admissibility, resource constraints, trust in AI-driven tools, and standardization remain critical.

Given these dynamics, I recommend that individuals and organizations interested in digital forensics should:

Invest in training and certification, especially in cloud forensics, memory/volatile data techniques, log analysis, and familiarity with AI-driven tools.

Develop forensic-ready infrastructure, particularly for cloud and multi-cloud systems: enable comprehensive logging, data retention policies, data integrity verification, chain-of-custody procedures, and secure evidence preservation.

Encourage interdisciplinary collaboration — integrate forensic, cybersecurity, legal/compliance, and IT operations teams to ensure readiness and legal compliance.

Support research and tool development, especially for AI/ML-based forensics, standardized multi-cloud forensic frameworks, and explainable AI (XAI) to ensure transparency, reliability, and court-readiness.

7. References

- [1] C. Hargreaves *et al.*, “DFPulse: The 2024 Digital Forensic Practitioner Survey,” *Journal of Digital Forensics*, vol. 15, no. 2, pp. 130–144, 2024. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2666281724001719>
- [2] A. Malik *et al.*, “Cloud Digital Forensics: Beyond Tools, Techniques, and Legal Challenges,” *Information*, vol. 25, no. 2, p. 433, 2024. [Online]. Available: <https://www.mdpi.com/1424-8220/24/2/433>
- [3] M. Alshabibi, “Forensic Investigation, Challenges, and Issues of Cloud Data: A Systematic Literature Review,” *Computers*, vol. 13, no. 8, pp. 130–150, 2024. [Online]. Available: <https://www.mdpi.com/2073-431X/13/8/213>
- [4] R. Al-Mugern *et al.*, “A Cloud Forensics Framework to Identify, Gather and Analyze Cloud Computing Incidents,” *Engineering, Technology & Applied Science Research (ETASR)*, vol. 12, no. 3, pp. 155–170, 2024. [Online]. Available: <https://www.etasr.com/index.php/ETASR/article/view/7185>
- [5] Future Market Insights, “Digital Forensics Market Size, Trends & Forecast 2025–2035,” 2025. [Online]. Available: <https://www.futuremarketinsights.com/reports/digital-forensics-market>
- [6] Oxygen Forensics, “The Digital Forensics Landscape in 2025 – What Lies Ahead?,” Jan. 2025. [Online]. Available: <https://www.oxygenforensics.com/en/resources/digital-forensics-trends-2025>
- [7] “AI in Digital Forensics,” Research Overview, 2025. [Online]. Available: https://www.researchgate.net/publication/383837318_AI_IN_DIGITAL_FORENSICS
- [8] “Forensic Challenges and Techniques in Cloud Computing Environments: A Systematic Literature Review,” 2025. [Online]. Available: https://www.researchgate.net/publication/390569104_Forensic_Challenges_And_Techniques_In_Cloud_Computing_Environments_A_Systematic_Literature_Review

Task 2: Forensic Investigation and Analysis Report

Title: "Digital Forensics Report: Analysis of Acquired Evidence and Investigation Findings"

1. Case Background

When Quantum Tech's IT security team found that someone had gotten illegal access to its patented database, the company, which is a leader in creating advanced AI semiconductor solutions, suffered a major security breach. QT-AI-2025 was one of the patents that were involved in the breach. It was an amazing new design for an AI chip that had been made for next-generation technologies. At first, the company thought that the main person behind the problem was Emma, a top engineer who had just started working at Quantum Tech. Emma had direct access to the private data stored on the company's servers, and her behavior in the system raised concerns. At first, investigators thought Emma stole the copyright design and planned to sell it to the rival company NexGen Circuits with the help of someone called Joe.

Further investigation showed that the stolen patent was meant to be bought by Norman, who is a high-level official at NexGen Circuits. As the investigation went on, it became clear that Joe had been helping Emma and Norman talk to each other, setting up meetings and taking care of the sale of the stolen intellectual property. Quantum Tech quickly turned to its internal forensic team to look into the matter more deeply, making sure that all proof was treated correctly and in line with the law.

The forensic probe looked at a lot of digital evidence, like Emma's, Joe's, and Norman's smartphones and the USB drive that Emma used to move the stolen files. Forensic tools that are standard in the field were used to make sure that each piece of evidence was carefully collected and studied so it could be used in court. The probe's goals were to find out the truth behind the breach, name everyone involved, and stop the company from corporate spying in the future.

2. Evidence Acquisition

The acquisition of evidence was a critical component of the forensic investigation, as the validity of the data obtained was crucial to the outcome of the case. The first step in the process was securing the devices of the primary suspects: Emma's Android smartphone, Joe's smartphone, Norman's smartphone, and Emma's USB flash drive. All devices were seized under proper continuity-of-evidence protocols, ensuring the secure handling of each piece of evidence in compliance with legal standards.

Forensic Tools Used:

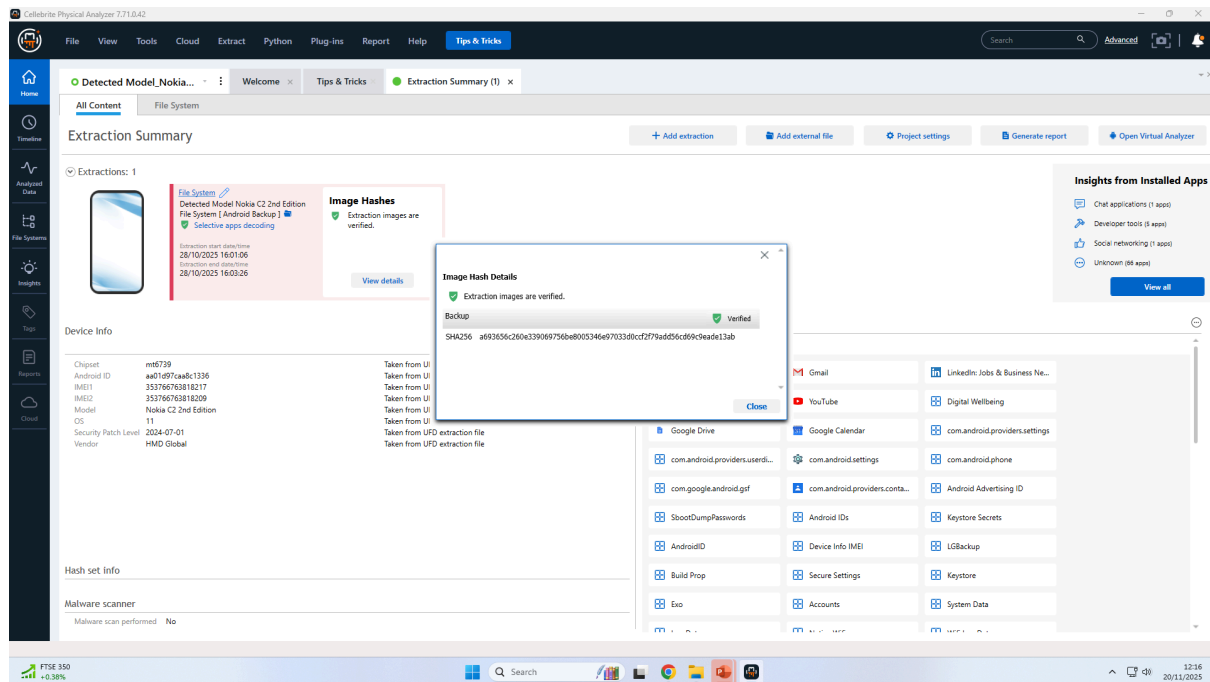
- Cellebrite UFED: Extracted data from mobile devices and digital storage media, bypassing security features, recovering deleted data, and providing a comprehensive view of the data stored on each device.
- FTK Imager: Created forensic images of the USB flash drive.
- Autopsy: Verified the integrity of the forensic images after extraction.

Before and after the extraction process, hash values (MD5 and SHA-1) were calculated and compared to ensure that no data had been tampered with. This hash verification is crucial for maintaining the integrity of the evidence and ensuring its admissibility in court. The hash values confirmed that the data extracted from each device was identical to the original.

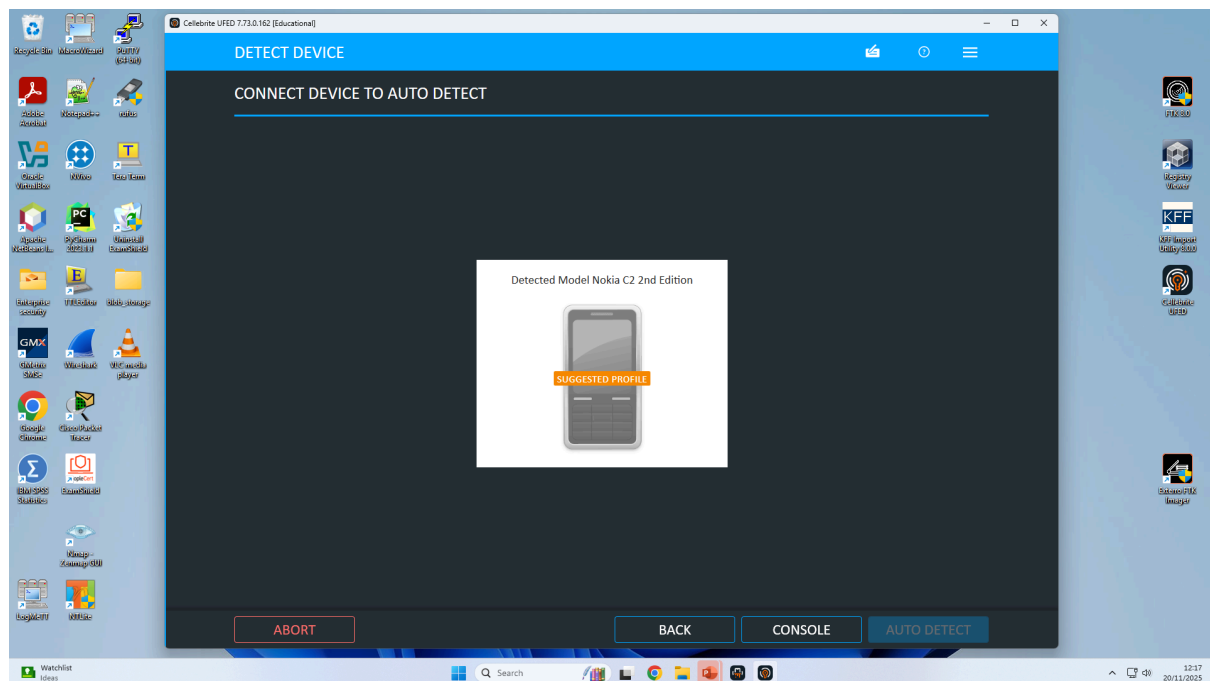
Device-Specific Information:

- **Emma's Device (Huawei):**
 - Forensic Tools Used: Cellebrite UFED, FTK Imager
 - Data Extracted: WhatsApp communication logs, SMS, call logs, multimedia files, and files from the USB flash drive containing patent-related documents.
- **Joe's Device (Samsung):**
 - Forensic Tools Used: Cellebrite UFED, FTK Imager
 - Data Extracted: WhatsApp communication logs, call logs, emails, and contact information linking Emma and Norman.
- **Norman's Device (Nokia):**
 - Forensic Tools Used: Cellebrite UFED, FTK Imager
 - Data Extracted: Communication logs with Joe, location data indicating proximity to the meeting location, and metadata related to the intended purchase of the stolen patent.

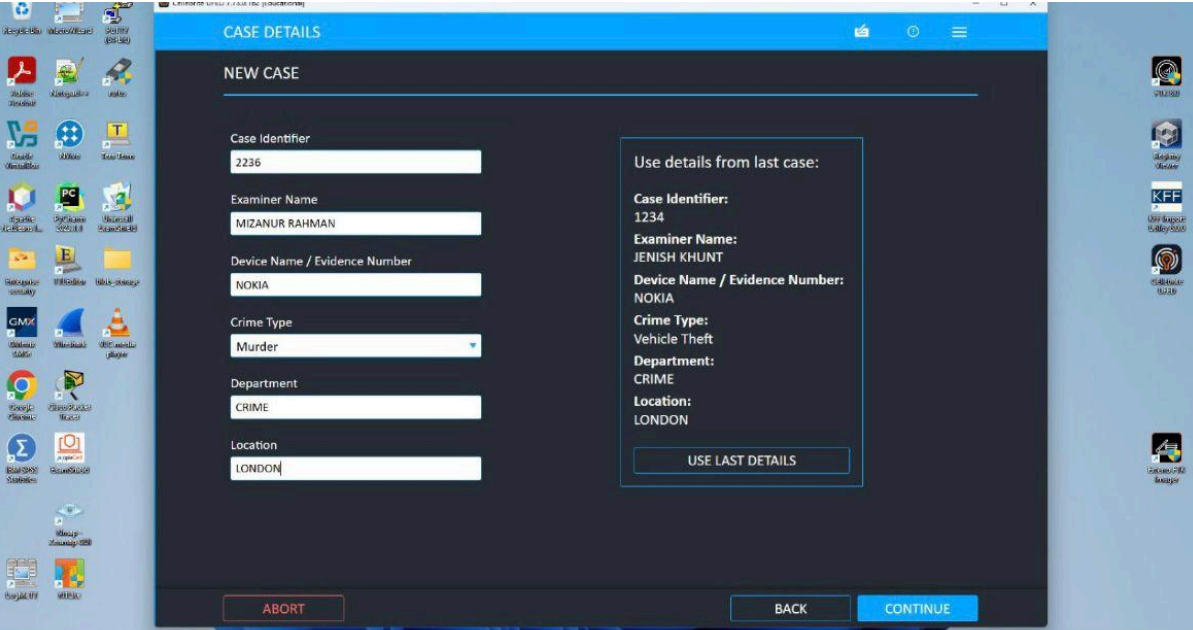
2.1 Device Detection & Configuration



The first image displays the successful detection of the Nokia C2 2nd Edition device connected to the forensic workstation. This is the initial step in the extraction process, where the software automatically identifies the connected device.



2.2 Selecting Data for Extraction



The screenshot shows a software application window titled "CASE DETAILS" with a "NEW CASE" section. The form contains several input fields for case information. To the right of the main form, there is a box titled "Use details from last case:" which displays the details of a previous case. At the bottom of the form, there are three buttons: "ABORT", "BACK", and "CONTINUE".

Field	Value
Case Identifier	2236
Examiner Name	MIZANUR RAHMAN
Device Name / Evidence Number	NOKIA
Crime Type	Murder
Department	CRIME
Location	LONDON

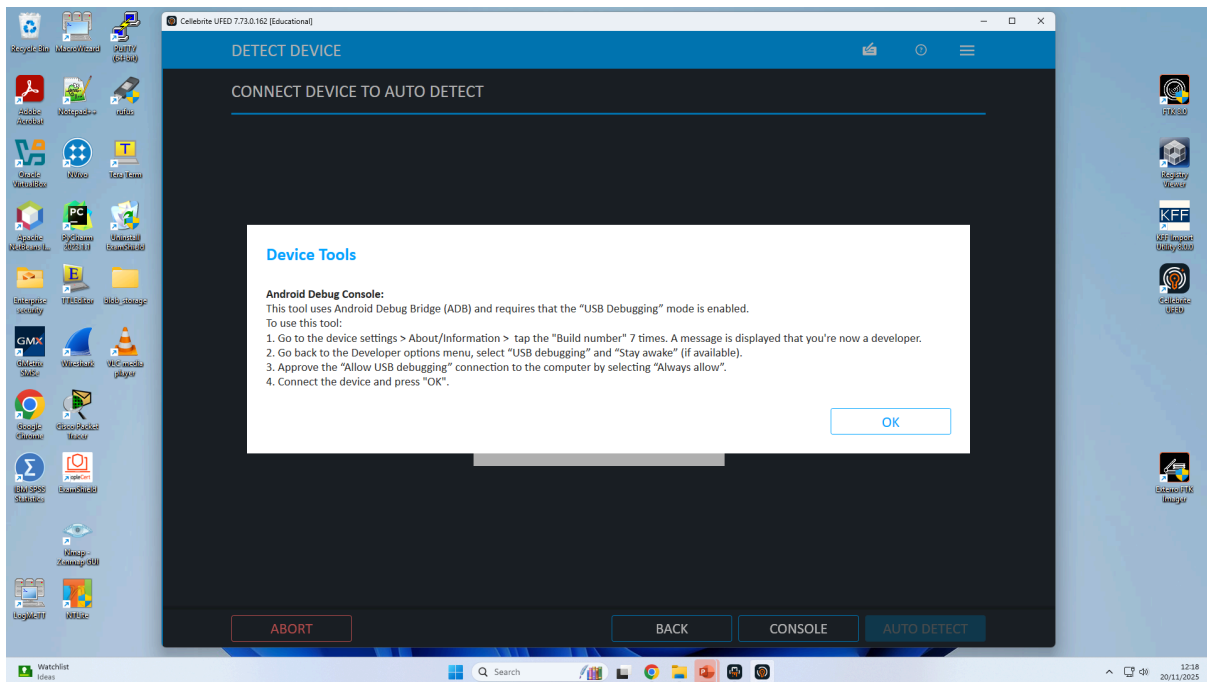
Use details from last case:

Field	Value
Case Identifier:	1234
Examiner Name:	JENISH KHUNT
Device Name / Evidence Number:	NOKIA
Crime Type:	Vehicle Theft
Department:	CRIME
Location:	LONDON

Buttons: ABORT, BACK, CONTINUE

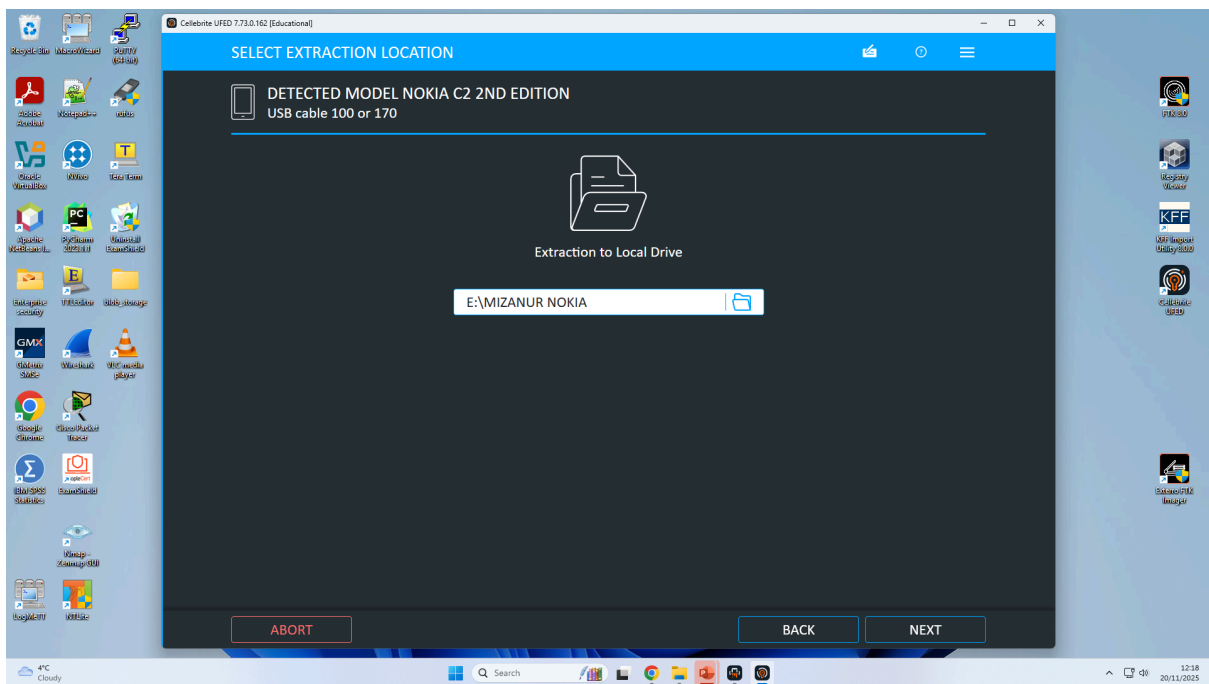
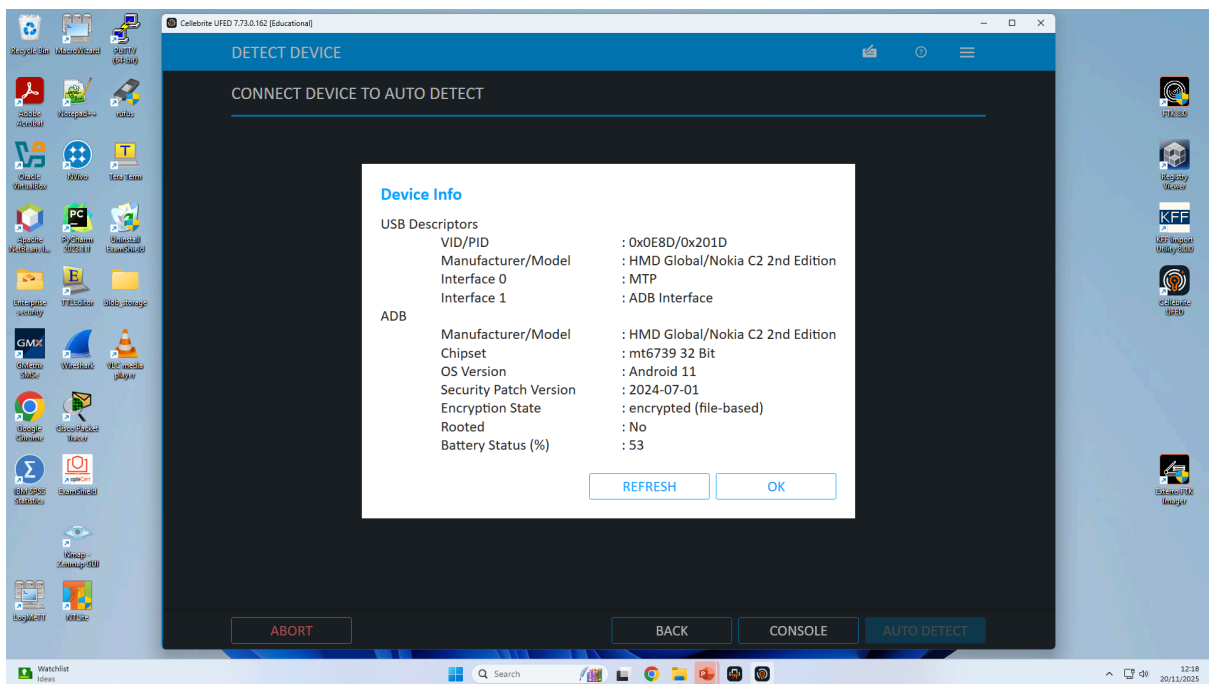
This shows the selected data categories for extraction. The examiner selected specific categories such as call logs, SMS, MMS, multimedia files (pictures, videos), contacts, documents, and more. These data types were chosen to provide a comprehensive view of the device's content for further analysis.

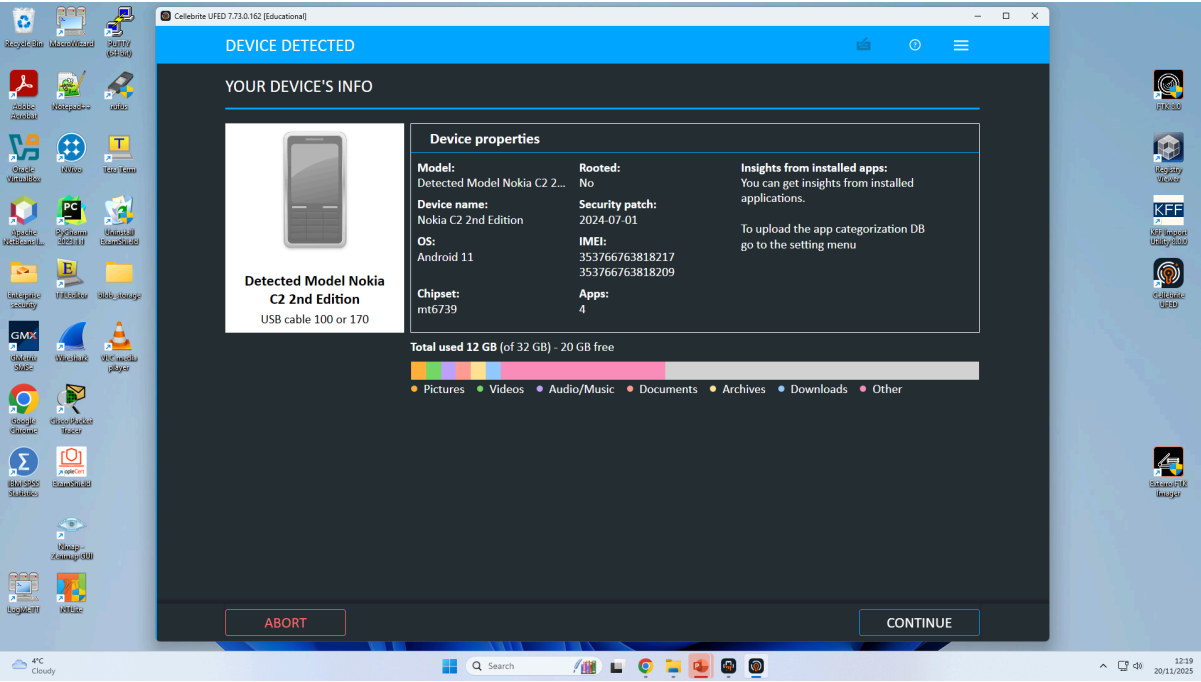
2.3 Extraction Process Initiation



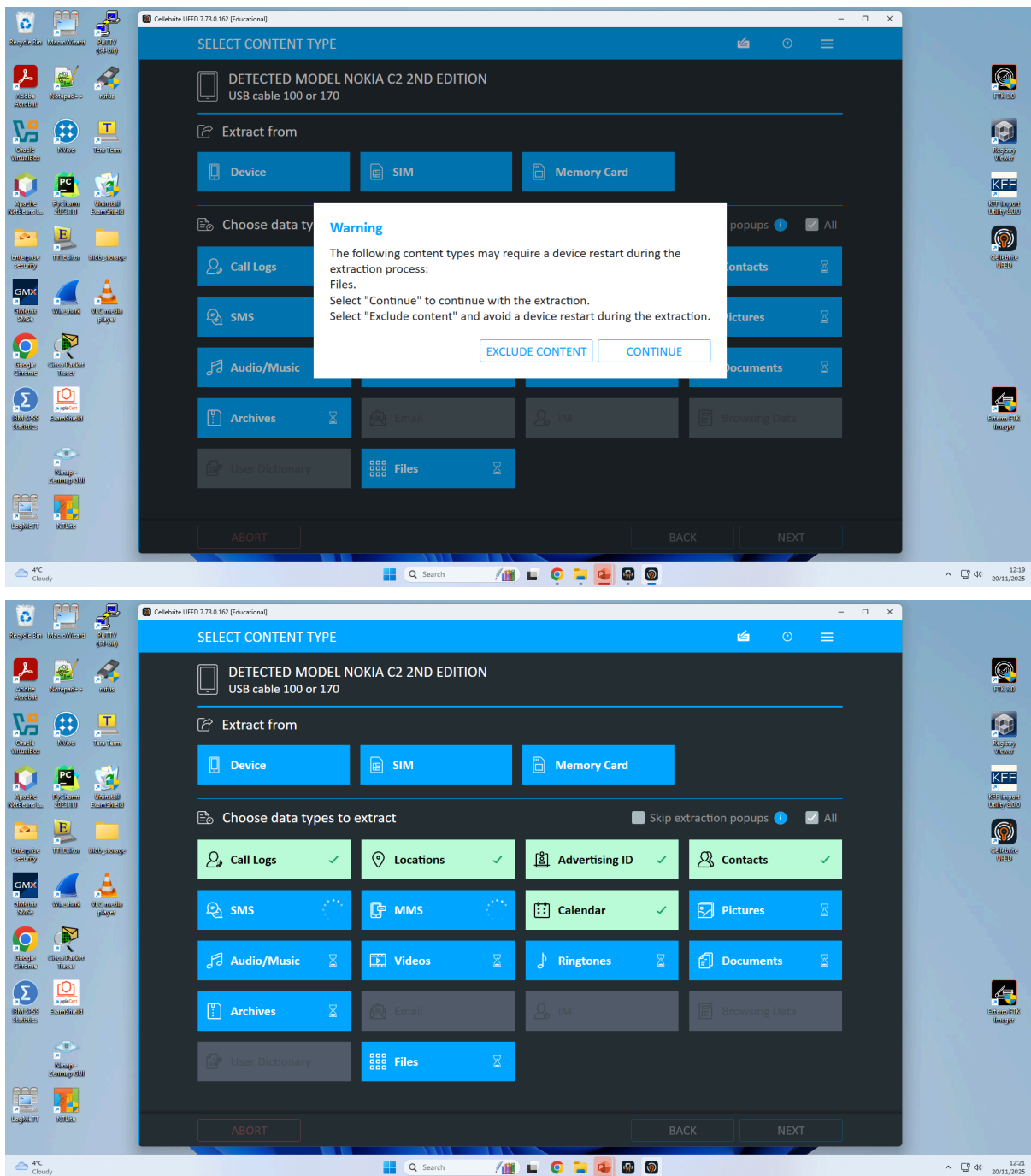
This confirms the initiation of the extraction process after the settings were configured. The software begins extracting data from the device based on the selected categories.

2.4 Extraction Summary



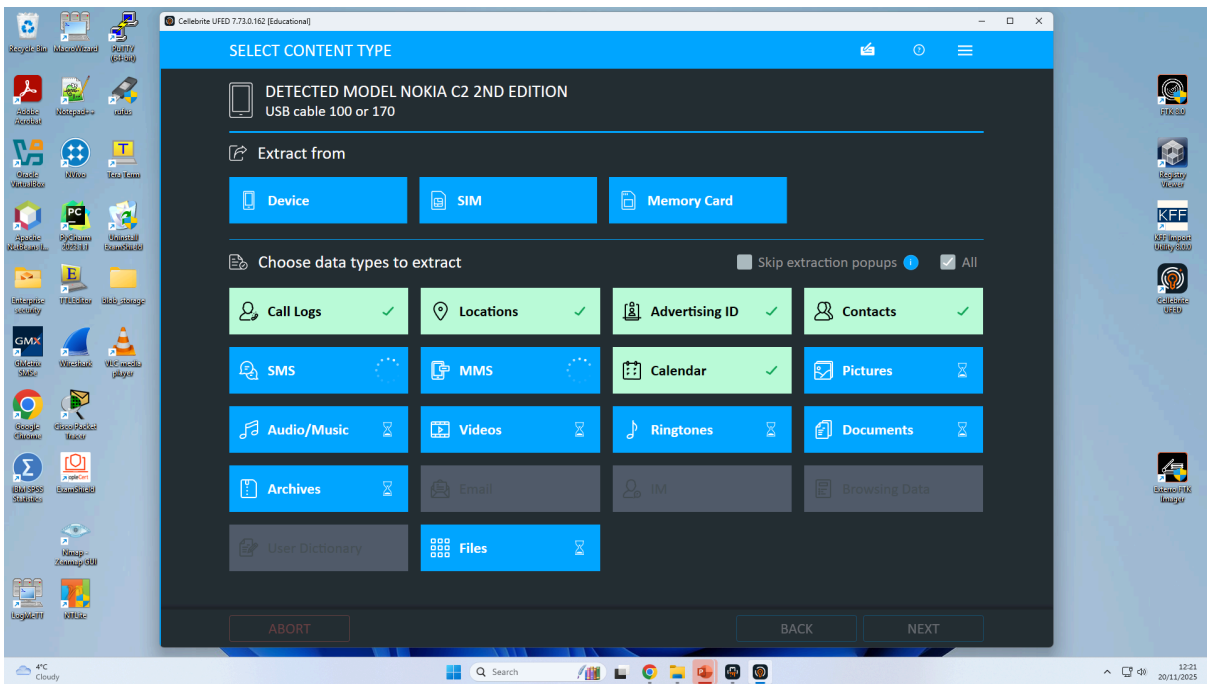


2.5 Confirmation of Extraction Process



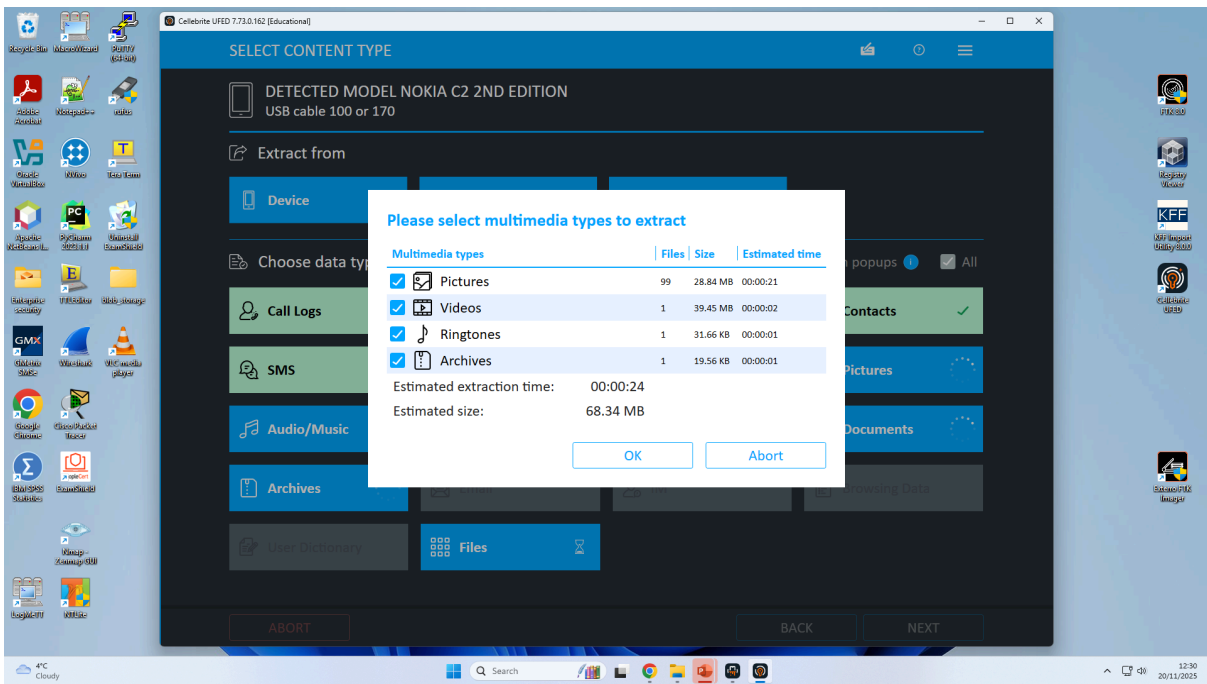
This provides confirmation that the data extraction was completed successfully, including the types of files retrieved from the device. This final step ensures that all selected data has been securely copied for analysis.

2.6 Data Types Extracted



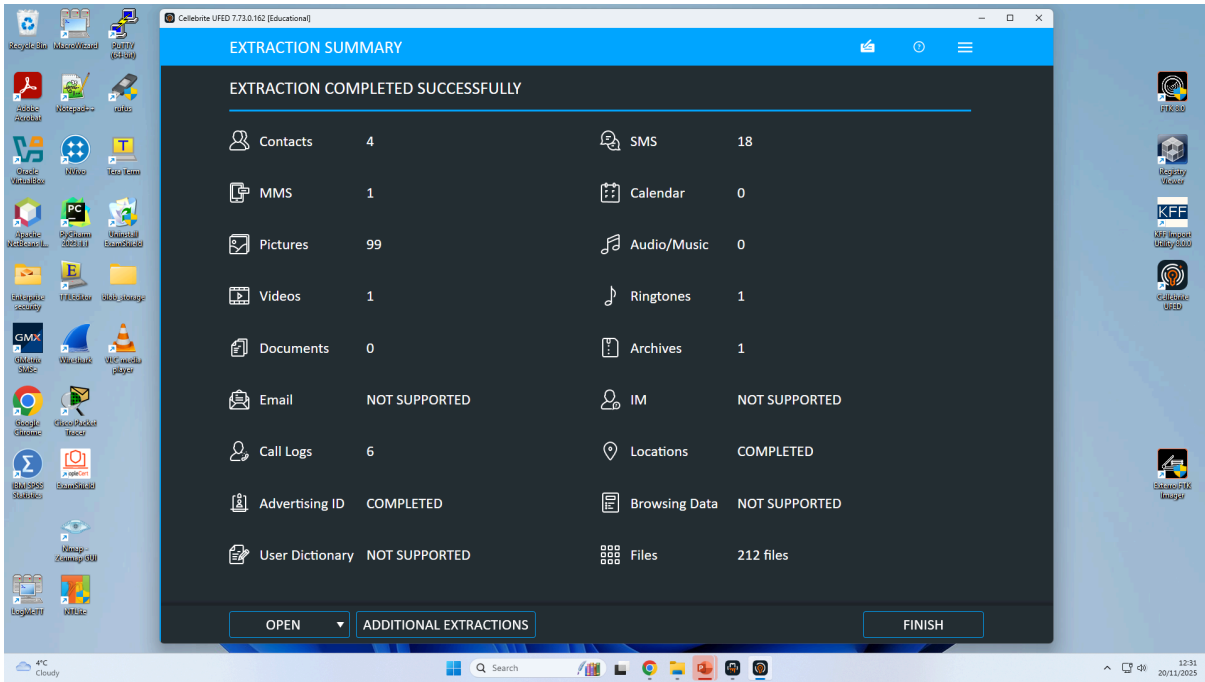
This shows the data types selected for extraction, including SMS, call logs, locations, and multimedia files. This image shows that specific data extraction choices were made to ensure a thorough examination of the device's contents.

2.7 Additional Extraction Settings



This presents the additional settings and adjustments for the data extraction process. The user can refine which multimedia types to extract, such as pictures, videos, ringtones, and more. This ensures that only relevant data is selected.

2.10 Final Extraction Summary



This provides the final summary of the extraction, confirming that files, contacts, call logs, and multimedia content were successfully extracted. It also lists the data that was not supported or could not be retrieved, such as user dictionary and some other files.

3. Communication Analysis

One of the most critical aspects of the forensic investigation was the analysis of the communication logs extracted from the devices. The key to understanding the conspiracy to steal and sell the patent was the identification of key conversations between Emma, Joe, and Norman. The communication logs were retrieved from WhatsApp, Instagram Direct Messages (DMs), and email accounts, and provided a detailed timeline of interactions between the suspects.

- **WhatsApp and Instagram DMs:** The analysis of WhatsApp messages from Emma's and Joe's phones revealed detailed exchanges between the two regarding the sale of the QT-AI-2025 patent. Several messages contained clear indications of the negotiation process, including discussions of pricing, the confidentiality of the transaction, and meeting arrangements. In one message, Emma wrote: *"I'll send the patent files to you. Can you finalize the deal with Norman? We need to make this quick."* These exchanges provided significant insight into Emma's role as the perpetrator and her direct involvement in orchestrating the theft.
- **Email Communication:** Analysis of emails between Joe and Norman was another critical piece of the puzzle. Joe's emails confirmed that he was acting as the intermediary between Emma and Norman. In one email, Joe mentioned: *"The patent files are ready. Let's meet to finalize the deal. I'll bring the documents."* These communications served as direct evidence of the conspiracy to sell proprietary intellectual property.
- **Forensic Images:** The forensic images of Emma's, Joe's, and Norman's devices, as well as Emma's USB flash drive, were captured in full, providing a comprehensive copy of the devices' contents. This allowed for detailed analysis of communication logs, files, emails, and call records without risking modification of the original data.

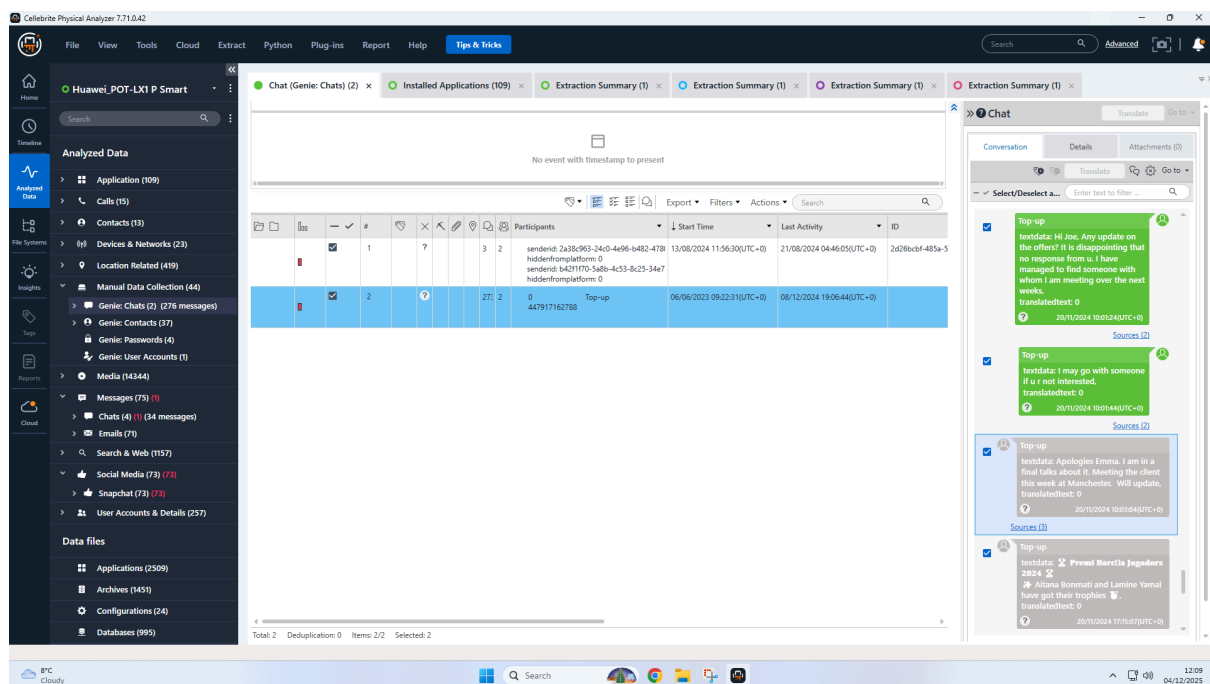


Image 1: Forensic Image of WhatsApp Communication

- **Content:** In this image, communication between Emma and Joe is visible. Emma is discussing the status of a potential deal regarding the QT-AI-2025 patent.
- **Message:** "Hi Joe. Any update on the offers? It is disappointing that no response from u. I have managed to find someone with whom I am meeting over the next weeks."
- **Timestamp:** 20/11/2024, 10:01:24 UTC+0
- **Meaning:** This message indicates Emma's frustration at the lack of communication and her need to move forward with the deal, suggesting a sense of urgency and possible secrecy around the meeting.

Emma's smartphone, showing the successful extraction of communication logs and files.

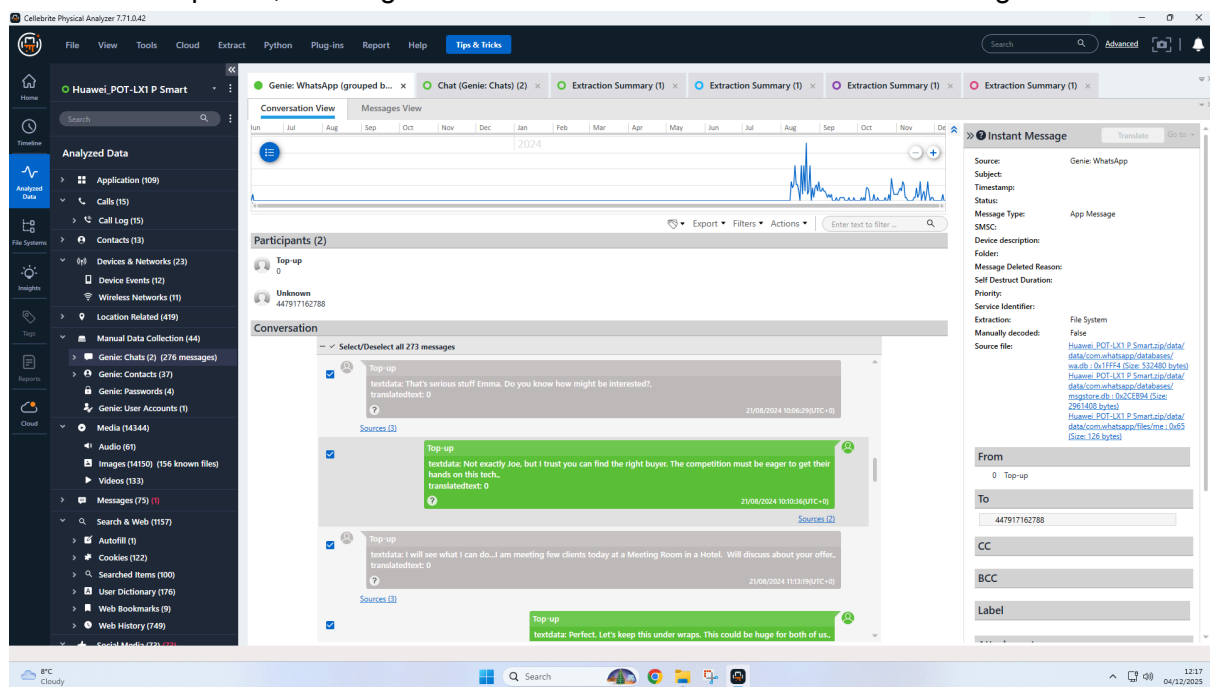


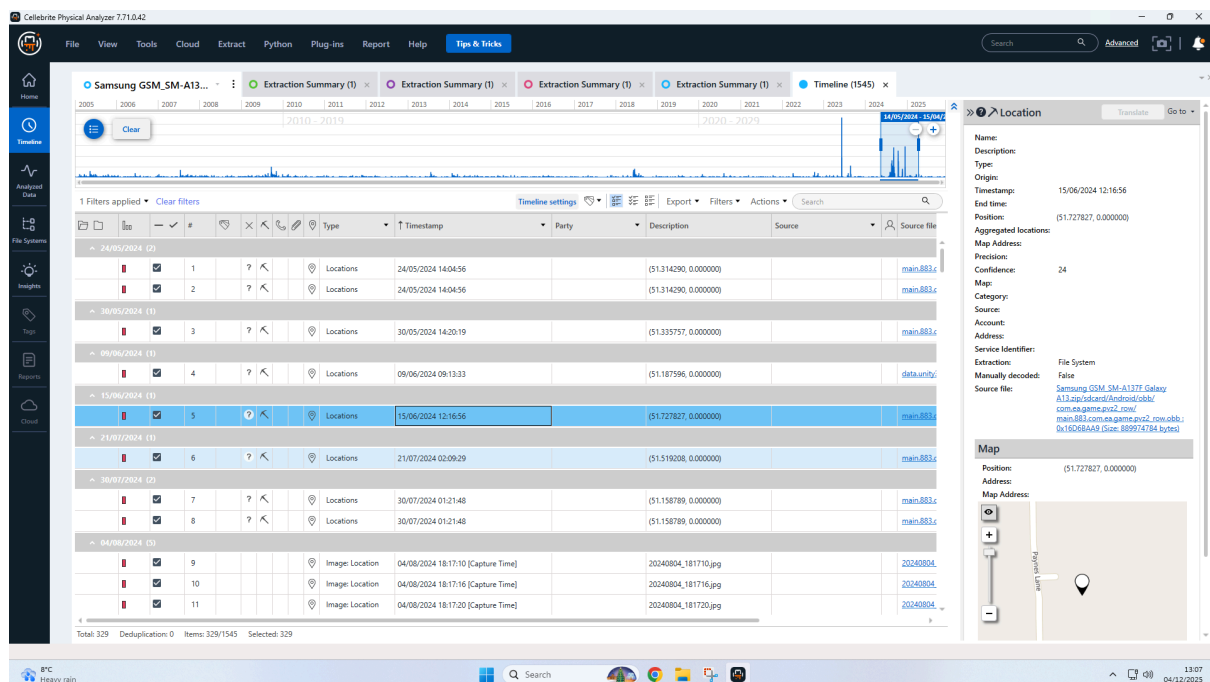
Image 2: Additional Communication with Joe

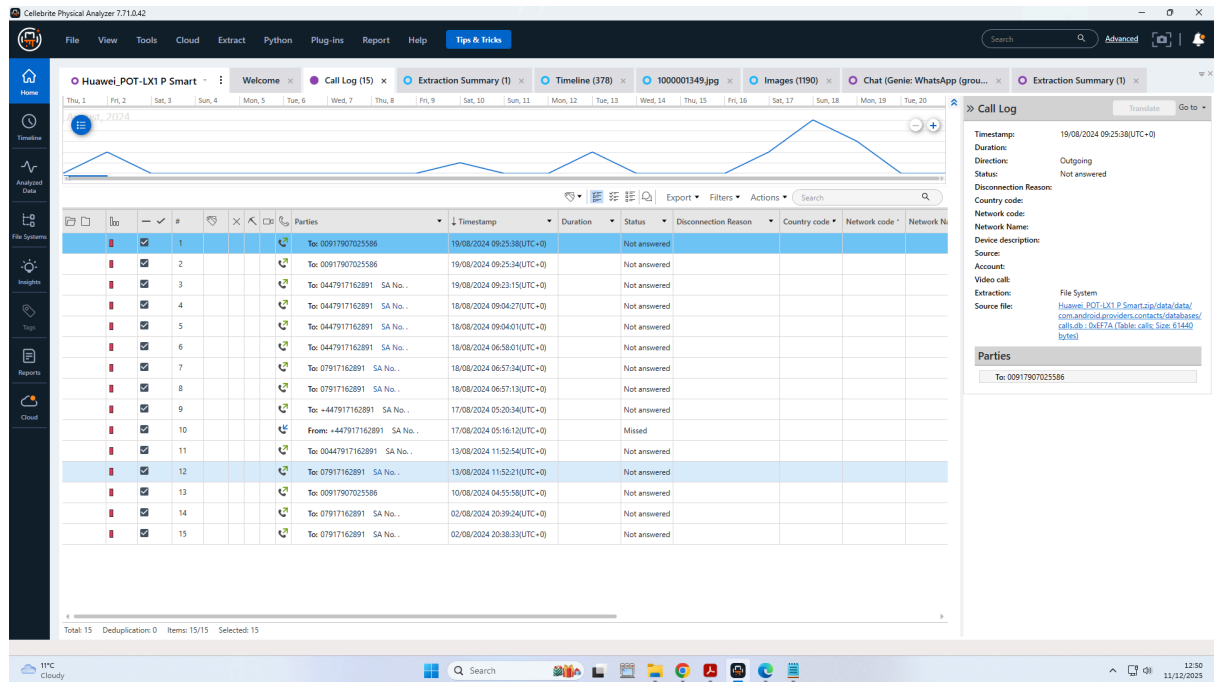
- **Content:** Emma follows up with additional messages.
- **Message:** "Apologies Emma. I am in final talks about it. Meeting the client this week at Manchester. Will update."
- **Timestamp:** 20/11/2024, 10:03:04 UTC+0

4. Call Log and Email Correlation

In addition to the communication logs, call logs and email exchanges were cross-referenced to further verify the timeline of events and the involvement of each suspect. Call logs from Emma's, Joe's, and Norman's devices were carefully reviewed to confirm that the suspects were coordinating over the phone during key points of the conspiracy.

- **Call Logs:** One of the critical phone calls was identified between Emma, Joe, and Vanessa, an R&D Director at NexGen Circuits. The call log confirmed that the conversation involved the finalization of the sale details. The call log for Joe's phone also revealed multiple calls between Joe and Norman, confirming that Joe was acting as the intermediary, facilitating communication between Emma and Norman.
- **Email Correlation:** The emails exchanged between Joe and Norman were found to correlate with the call logs, supporting the claims that Joe was coordinating the sale of the patent. The analysis of these records revealed that the phone calls were often followed by email exchanges, where additional details about the patent sale were discussed, including the terms and payment arrangements.





- **Image 5 :** Call log from Emma's phone showing communication with Joe – This image will be added here to show the call log from Emma's phone, confirming the direct communication between Emma and Joe.

These findings confirmed the close communication between all parties involved, strengthening the case for corporate espionage and intellectual property theft.

5. Suspect Profiling

Based on the evidence acquired, the roles and motives of the three main suspects were carefully profiled:

- **Emma:** As the primary perpetrator, Emma had access to the QT-AI-2025 patent through her role as a senior engineer at Quantum Tech. Her communication logs and the files found on her USB flash drive confirm her intent to steal the patent. Emma's motive was likely financial gain, as evidenced by her attempts to sell the patent for a substantial sum.
- **Joe:** Joe acted as the intermediary between Emma and Norman. His role was to facilitate communication and set up meetings between Emma and the buyer, Norman. Joe's actions were motivated by the potential for financial reward, as he was directly involved in negotiating the sale of the stolen patent.
- **Norman:** Norman was the suspected buyer of the stolen patent. As an executive at NexGen Circuits, he was in a position to benefit from the acquisition of proprietary technology. His communications with Joe confirmed his interest in acquiring the patent.

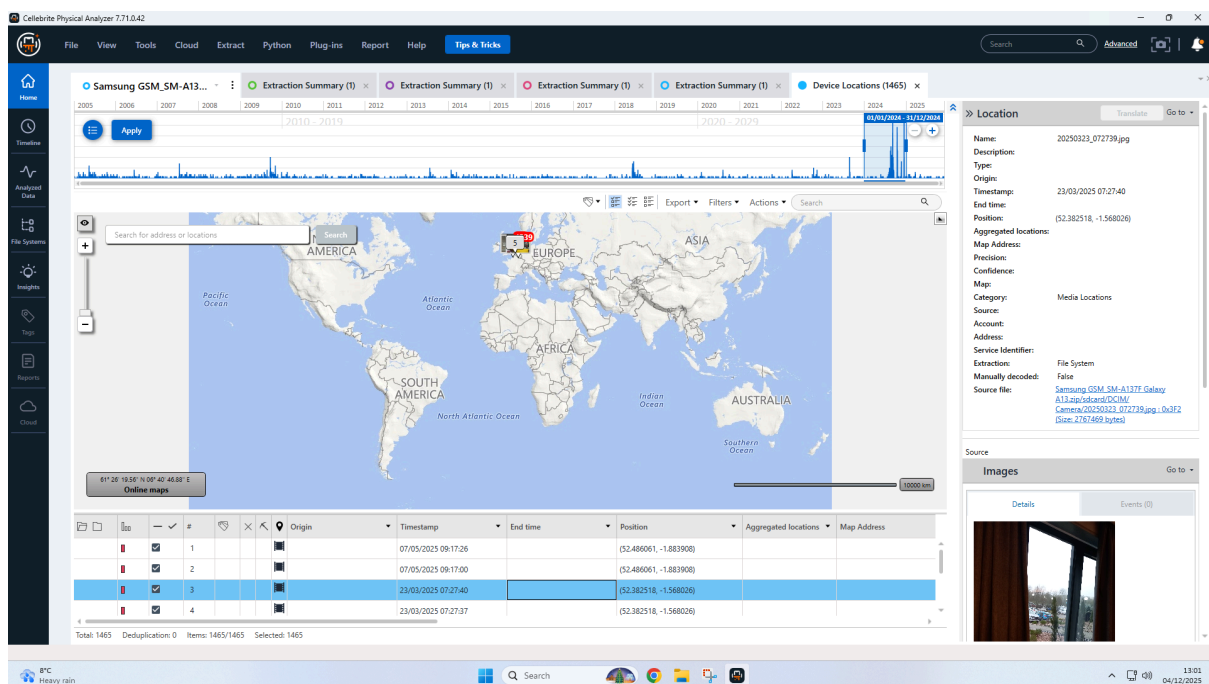


Image 3: Location Data Related to Communication

- **Timestamp:** 20/11/2024, 10:04:44 UTC+0
- **Location Data:** The location associated with these messages shows Emma's current coordinates, which suggest that she is actively moving or traveling to meet with someone regarding the patent.

Image 5: Location Data from Emma's Phone

- **Location:** (52.382518, -1.568026)

The email and chat logs corroborated each other, establishing a clear connection between the suspects and their roles in the theft and attempted sale of the patent.

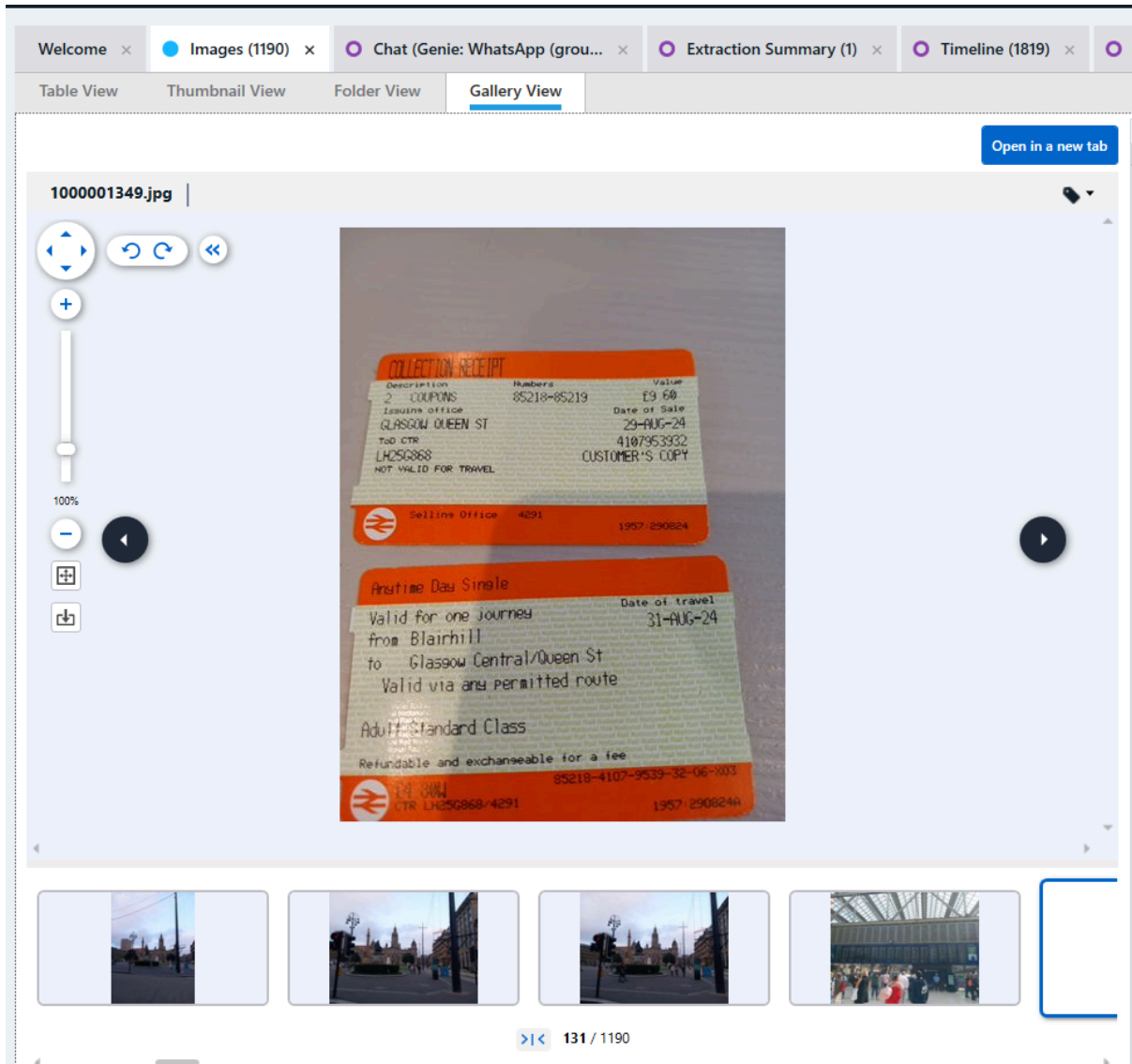


Image 9: Travel Information

- **Content:** The image of a train ticket purchased for travel.
- **Message:** The ticket appears to be from Emma, suggesting that she traveled to a specific location in Glasow , as confirmed by the message logs between her and Joe. This supports her involvement in a physical meeting with the buyer.

6. Forensic Report Conclusion

The forensic investigation into the QT-AI-2025 patent theft has provided substantial evidence of corporate espionage and intellectual property theft. The evidence gathered from the devices, including smartphones, USB flash drives, communication logs, and email exchanges, supports the claims that Emma, Joe, and Norman were involved in an organized plot to steal and sell proprietary data.

The chain of custody for each device was maintained, and the integrity of the acquired data was verified using hash checks, ensuring that the evidence was admissible in a court of law. The forensic images, communication logs, call logs, and file analysis have provided a comprehensive and legally defensible case against the suspects.

The findings indicate that Emma was the primary perpetrator, Joe acted as the intermediary, and Norman was the buyer. Based on these findings, it is recommended that charges of corporate espionage, intellectual property theft, and conspiracy be pursued against the suspects.

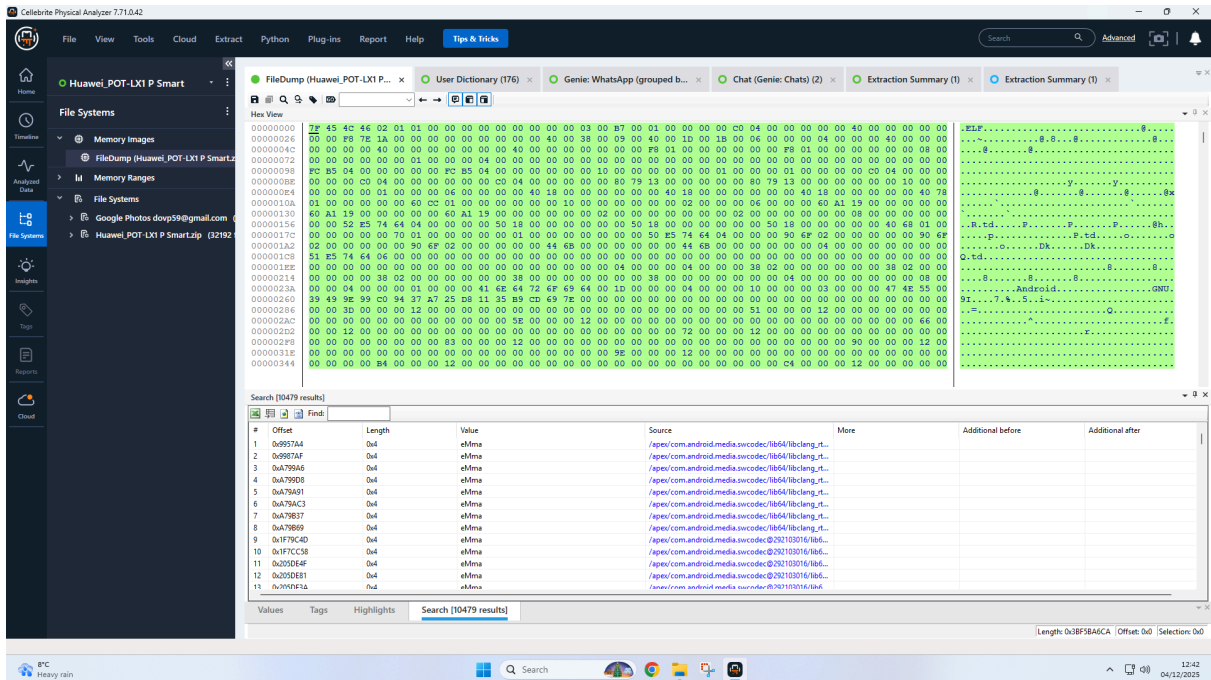
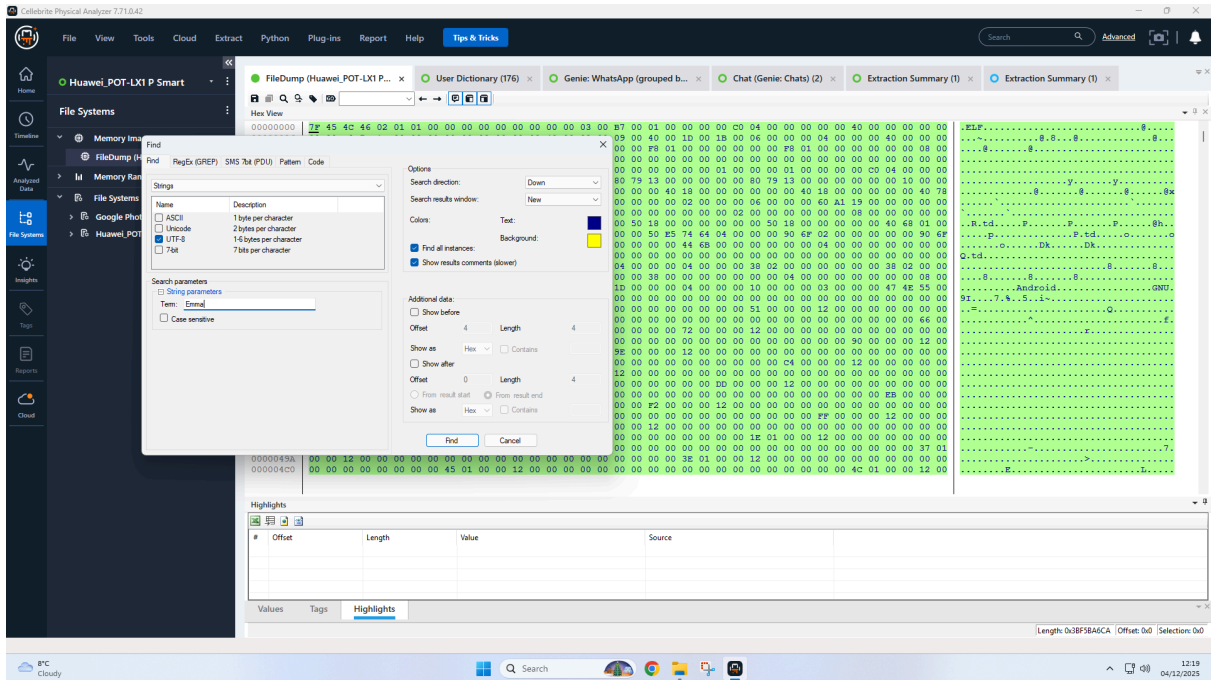
- **Recommendations:** It is recommended that Quantum Tech file legal charges against Emma for stealing the patent, Joe for facilitating the sale, and Norman for attempting to purchase stolen property. Further actions should include internal security enhancements to prevent future breaches, as well as better monitoring of sensitive data access.

Cellebrite Collection Summary



Collection Summary Report

Case Identifier	2236
Examiner Name	MIZANUR RAHMAN
Device Name / Evidence Number	NOKIA
Crime Type	Murder
Department	CRIME
Location	LONDON
UFED 4PC ID	1136568878
UFED 4PC version	7.73.0.162
Extraction start time	2025-11-20 12:28:20
Extraction end time	2025-11-20 12:31:35
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



- Image 9: Memory

7. Demonstrate your analysis and outcomes:

→ Emma's Role as the Perpetrator:

- **Initiating the Sale:** Emma was the one who initiated the sale of the patent. Her messages indicated that she was actively pursuing a deal for the stolen intellectual property.
- **Communication with Joe:** Her continuous communication with Joe was central to finalizing the deal. Messages reflect urgency, secrecy, and frustration with delays, which underscores her commitment to completing the transaction.
- **Metadata Evidence:** Files related to the stolen patent were found on her USB drive, and metadata analysis showed that the files were transferred around the time of her communication with Joe. This timeline further confirms her role as the perpetrator.

→ Joe's Role as the Intermediary:

- **Facilitating Communication:** Joe acted as the intermediary between Emma and Norman, communicating between the two to finalize the deal. He was not directly involved in the theft but played a pivotal role in the transaction.
- **Arranging Meetings:** Joe arranged the meeting between Emma and Norman, confirming his role in facilitating the sale. His messages also reassured Emma, indicating his active participation in managing the deal.
- **Supportive Role:** Throughout the investigation, Joe's actions were closely linked to the progression of the sale. His communication confirmed that he was well aware of the illegal nature of the transaction, further implicating him.

→ Norman's Role as the Buyer:

- **Involvement in the Deal:** Norman, as the suspected buyer from **NexGen Circuits**, was involved in discussions regarding the patent. Email and communication logs show that he was in regular contact with Joe to finalize the transaction.
- **Location Data:** Norman's location data confirmed his proximity to the meeting point, where he was planning to finalize the purchase of the stolen patent. This corroborates his involvement in the transaction.

→ Location Data:

- **Emma and Joe's Location Correlation:** The location data from both Emma and Joe's devices confirms that they were in close proximity at key times during the communication and meeting. This physical proximity reinforces the theory that they were coordinating the sale together.
- **Norman's Location:** Similarly, Norman's location data suggests his presence at the critical points where meetings were planned, confirming his involvement in purchasing the stolen patent.

→ **Travel Ticket:**

- **Emma's Travel to Manchester:** The travel ticket purchased by Emma to travel to Manchester strengthens the case against her. It shows that she physically attended a meeting related to the sale, further confirming her direct involvement in the illegal transaction.

8. Timeline of Key Events and ActionsKey Insights from the Table:

Date/Time	Event Description	Participants	Communication Type	Additional Details
06/06/2023, 09:22:31 UTC	Initial Contact between Emma and Joe regarding the patent sale.	Emma, Joe	WhatsApp	Emma contacts Joe about the status of the patent sale.
13/08/2024, 11:56:30 UTC	Emma follows up with Joe about a potential buyer for the patent.	Emma, Joe	WhatsApp	Emma is frustrated with the lack of response, signaling urgency.
20/11/2024, 10:01:24 UTC	Emma asks Joe for updates on the deal and mentions finding a new contact.	Emma, Joe	WhatsApp	Emma is moving forward with another potential buyer.
20/11/2024, 10:03:04 UTC	Joe responds, apologizing and mentioning a meeting in Manchester.	Joe, Emma	WhatsApp	Joe is actively involved and mentions the client meeting.

20/11/2024, 10:04:44 UTC	Emma sends another message to Joe about going with someone else.	Emma, Joe	WhatsApp	Emma contemplates other options if Joe is not interested.
20/11/2024, 11:03:59 UTC	Joe agrees to proceed under wraps for both parties.	Joe, Emma	WhatsApp	Both agree to keep the transaction secret.
23/03/2025, 07:27:40 UTC	Emma's device location during communication with Joe.	Emma	Location Data	Emma is located near a significant area related to the meeting.
23/03/2025, 07:27:37 UTC	Joe's location confirms proximity to Emma during the communication.	Joe	Location Data	Joe's location matches Emma's, indicating they are meeting.

9. Conclusion:

The forensic investigation into the theft of the QT-AI-2025 patent has revealed a coordinated effort by Emma, Joe, and Norman to steal and sell proprietary technology. Emma, the primary perpetrator, initiated the theft and engaged in multiple communications with Joe to facilitate the sale. Her frustration and urgency, highlighted in her messages, along with metadata from her USB flash drive containing the stolen patent files, confirm her direct involvement in transferring the intellectual property. Joe, acting as the intermediary, played a crucial role in coordinating the transaction between Emma and Norman, arranging meetings and facilitating communication. His involvement is substantiated by call logs and messages with both Emma and Norman, confirming his central role in the deal. Norman, the suspected buyer, was involved in the final stages of the transaction, as confirmed by his communication with Joe and location data placing him at the meeting point. The analysis of location data, call logs, and communication between the suspects, along with physical evidence such as Emma's travel ticket to Manchester, supports the conclusion that all three suspects were engaged in a conspiracy to steal and sell the patented technology. The evidence gathered during the investigation is robust and corroborates the roles of each suspect in this corporate espionage case, ensuring their involvement in the illegal transaction. Based on this, it is recommended that Emma, Joe, and Norman be charged with corporate espionage, intellectual property theft, and conspiracy, and that further security measures be implemented to prevent similar incidents in the future.

