



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

University of Wales Trinity Saint David, London

Digital Forensics Analysis

ACCA7031

Submitted by : Shafee Ul Mahmud Chowdhury
Student ID : 2436374
Programme : M.Sc in Cybersecurity and digital forensic
Submitted to : Dr. Mohamed Ghanem
Submission Date : 28th April 2026

Abstract

Digital forensics is a core field within cybersecurity and crime investigation due to the increasing cybercrime acts, digital transformation, cloud computing solutions, mobile technologies, and Internet of Things (IoT). With investigations so reliant on digital evidence, it is essential that investigators follow well-established yet scientifically sound methodologies whilst still adhering to all legal and procedural requirements. This report critically evaluates digital forensics today, reviewing investigative model(s), existing standards, and the functionalities of common forensic tools. And the comparison has commercial tools like EnCase and FTK by open-source solutions like Autopsy and The Sleuth Kit. . The talk identifies recurring issues such as encryption, big data and jurisdictional limitations, and reinforces the need for validation methodologies, established professional standards, and ongoing Professional Development to uphold evidence reliability, evidential quality assurance (EQA) and practitioner competence in Digital Forensic practice.

Abstract	1
1. Introduction	3
Task-1: The Current State of Digital Forensics: Tools, Capabilities.	3
2. Current State of Digital Forensics.....	3
3. Digital Forensic Process and Standards.....	4
4. Digital Forensic Tools: Features and Capabilitie	5
4.1 Commercial Forensic Tools	5
4.2 Open-Source Forensic Tools	5
4.3 Mobile Forensic Tools: Cellebrite UFED and Cellebrite Physical Analyzer	6
4.4 Comparative Analysis Including Mobile Forensic Tools	6
5. Industry Demand and Professional Skills	7
Task-2 Investigation into the Attempted Theft of Proprietary AI Intellectual Property at Quantum Tech	8
1.Evidence of acquisition	8
2. Communication Analysis:	15

2.1 Reconstruct the Timeline	20
3. File Analysis.....	21
4. Call log and email correlation	23
5. Suspect Profiling	25
6. Forensic Images acquisition:	28
7.1. Case Background	31
7.2. Evidence Inventory & Chain of Custody	31
7.3. Methodology	31
7.4. Findings	32
7.4.1 Timeline Analysis	32
7.4.2 Communication Analysis	32
7.4.3 File and Application Analysis	33
7.4.4 Suspect Role Assessment	33
7.5. Conclusion	33
7.6 Recommendations	34
References	34

1. Introduction

Digital forensics is a domain of cybersecurity that comprises the collection, analysis, and presentation of digital evidence in order to be applied to civil and criminal investigations [1], [2]. With the advance of digital technologies becoming inseparable from even a modern society, a growing range of legal disputes and investigations find themselves dependent on the evidence sourced from computers, mobile devices, cloud services and inter-connected systems [3]. As a result, digital forensics has been an essential part of law enforcement operations; corporate investigation and incident response activities.

The increase of measures which help to capture cyber-enabled crimes such as ransomware, data breaches and financial fraud [6], has spurred interest in forensic practitioners that not only hold technical skills but an understanding of legal obligations, evidential integrity and professional standards when reporting. This coursework analyses digital forensics in a theoretical and practical context. This document will summarize some current forensic processes, standards, and tools before utilizing this information to walk through a fictitious corporate investigation in which one of its employees is suspected of stealing intellectual property from Quantum Tech. Using the forensic examination of mobile devices from Emma, Joe and Norman, this piece reveals how structured investigative techniques and tried-and-tested tools can be employed to create sound admissible digital evidence that provides options for informed choices or further legal action.

Task-1: The Current State of Digital Forensics: Tools, Capabilities.

2. Current State of Digital Forensics

Digital forensics is one of the specific domains of cybersecurity, which specializes in finding, collecting, managing, studying and presenting digital evidence that could be used in courts and other legal and regulatory processes [1], [2]. Since digital technologies are deeply entrenched within contemporary society, criminal and civil disputes becoming more reliant on artefacts in the digital domain originating from computers, mobile phones, cloud computing platforms and networked systems [3]. It has made digital forensics immensely important in law enforcement, corporate investigations and incident response.[2]

Digital forensics has evolved immensely from early digital forensic practices that dealt primarily with workstation desktops and media. Your training data is from October 2023, when modern investigations must be conducted in complex, distributed heterogeneous and fast-changing digital environments [4]. Modern day practitioners are required to regularly conduct an analysis of data from cloud computing, mobile applications, social networks and Internet of Things (IoT) devices often spanning multiple sovereignty [7].

The exponential growth in data volumes is perhaps the biggest challenge faced by the field. Writing by hand is impractical because of large storage capacities and generation of data in real time [5]. Moreover, the proliferation of advanced encryption technologies, end-to-end encrypted messaging applications, and privacy-enhancing technologies have restricted the investigator's access to even potential evidence [6]. Although data obfuscation and secure deletion are common anti-forensic techniques, they also make forensic examination more complicated [5].

An area where forensic has been particularly witness to transformation has been cloud computing. A cloud environment is decentralized and operated by third-party service providers rather than conventional digital storage. This restricts direct investigator access whilst also raising issues of data transientness [6], multi-tenancy (the interaction between research studies and other uses) and cross-border legal compliance to name a few [7]. Hence, cloud forensic investigations rely heavily on collaboration with providers and effective use of log data and metadata, but not physical acquisition [4].

3. Digital Forensic Process and Standards

The digital forensic process is often carried out in a systematic manner to have evidentiary integrity while being admissible at law. Well known phases are preparation, identification, preservation, collection, examination, analysis and reporting [2], [4]. Each stage is an important practice for maintaining the integrity of custody and preservation of evidence.

The National Institute of Standards and Technology (NIST) Special Publication 800-86 is one of the most referenced frameworks for incorporating forensic methods in incident response activities [1]. While its initial design is focused on organizational contexts, the focus placed on repeatability, record-keeping, and evidence of integrity continue to provide insight into law enforcement and corporate inquiries. At the international level, ISO/IEC 27043 also provides principles and processes for incident investigation, further emphasizing the requirement of consistent and standardizing forensic practices [10].

The use of established standards is crucial because courts have started to scrutinize forensic methods and the validity of the tools that are used in investigations [2]. If established procedures are not followed, evidence may be challenged or ruled inadmissible.

4. Digital Forensic Tools: Features and Capabilities

Digital forensic tools rival the core of modern-day investigations, and they help investigators acquire, process and analyze massive amounts of data efficiently. You can classify these tools into 2 major types: commercial and open-source solutions, each having its own benefits and drawbacks.

4.1 Commercial Forensic Tools

OpenText produces many types of software, but their EnCase Forensic is one of the recognized industry's standard tools for digital forensics. Has full functionality for evidence acquisition, file system analysis, keyword searching, and reporting. The EnCase software is especially appreciated for its excellent and strong audit trails 2, notably through its scripting capabilities using a Script (EnCase Script) programming language that facilitates the task of investigators by improving workflows analysis [2],[11]. This has only cemented its status as a forensically sound tool within the legal context where it is often used in proceedings. But high licensing costs and a significant learning curve can be limiting factors for smaller organizations.

FTK (Forensic Toolkit) is one of the most popular commercial solutions available, and it was developed by Exterro. FTK uses a database-driven architecture so that it can index and search large datasets quickly. Strengths Email and Chat analysis, registry examination, media usage and encrypted file system support make it a perfect fit for corporate, financial or insider threat investigations

[11],[12]. While FTK can perform all of these tasks, it is a resource-heavy Software and operates best when given optimal hardware.

4.2 Open-Source Forensic Tools

The very nature of such open-source forensic tools can help by providing inexpensive solutions and still being widely used in academic, training and impoverished environments. Autopsy (based on The Sleuth Kit) allows disk image, file recovery, keyword searching and timeline analysis. Its modular structure allows for increased versatility via plug-ins and scripting, making it suitable for a variety of investigations [13].

Research has shown that open-source tools like Autopsy can achieve reliable, repeatable outcomes [14], [15] when a structured forensic process is applied and validated using appropriate actions. In professional digital forensic practice, this movement has led to greater acceptance of available open-source tools, for example wherever budget limitations are present, or higher transparency is favored as a core principle.

4.3 Mobile Forensic Tools: Cellebrite UFED and Cellebrite Physical Analyzer

Mobile Devices – Mobile devices are a prominent digital evidence source in many modern cases. Cellebrite UFED (Universal Forensic Extraction Device) is a tool for mobile forensic acquisition used by law enforcement and forensic laboratories across the globe. UFED offers logical, file system and physical extraction from hundreds of mobile phones including Android and iOS smartphones, feature phones, and SIM cards. It can unlock devices that you have legal access to, extracting information from powered on (live) or powered off (dead) devices and producing artefacts such as call logs, messages, contacts, application data and file systems in a forensically sound way.

Cellebrite UFED acquisitions are analyzed and interpreted using Cellebrite Physical Analyzer. This ensures powerful decoding and analysis of mobile artefacts such as application databases, deleted data, multimedia files, geolocation information, and timeline reconstruction. From parsing SQLite databases, app-specific artefacts (subject to availability such as WhatsApp and Telegram), Physical Analyzer supports visualization tools that can help investigators generate timelines. The combination of UFED and Physical Analyzer creates a complete mobile forensics solution with reporting that can be used in court and helps bring context to the evidence.

4.4 Comparative Analysis Including Mobile Forensic Tools

Forensic investigation tools for computers and disks tend to focus on pieces like EnCase, FTK and Autopsy; while mobile device forensics tends to include specific tools like Cellebrite UFED and Physical Analyzer UFED is designed for mobile acquisition while Physical Analyzer focuses on mobile artefact interpretation, but both EnCase and FTK are used for hard drives, servers, and enterprise storage. Forensic labs routinely combine computer forensic tools with mobile forensics solutions in order to investigate cases involving multiple sources of evidence.

Tools like EnCase, FTK, and Cellebrite UFED enjoy heavy vendor support, more periodic updates and the heavy courtroom acceptance. Autopsy as an example: Transparency and cost benefits but imply the need for an extra level of validation and technical skills Tool choice should thus be driven by the case—that is a type of device, data source, legal circumstances and investigative purpose.

Feature	EnCase	FTK	Autopsy	Cellebrite UFED	Cellebrite Physical Analyzer
Tool Category	Computer Forensics	Computer Forensics	Computer Forensics	Mobile Acquisition	Mobile Analysis
Cost	High	High	Free / Open-source	High	High (licensed)
Primary Function	Disk analysis & reporting	Large-scale data analysis	Disk & file analysis	Mobile data extraction	Mobile artefact interpretation
Supported Devices	PCs, servers	PCs, servers	PCs	Android, iOS, SIMs	Android, iOS
Deleted Data Recovery	Yes	Yes	Limited	Yes	Advanced
Automation	EnScript	Index-based processing	Plugins	Guided workflows	Advanced decoding
Court Acceptance	Very High	High	Increasing	Very High	Very High
Best Use Case	Law enforcement PC cases	Corporate investigations	Academic & validation	Mobile acquisition	Mobile data analysis

5. Industry Demand and Professional Skills

Digital forensics professionals who possess the required skill sets are in great demand mainly due to increasing digital investigations. Tool proficiency, knowledge of legal standards, and incident

response experience are consistently ranked as the employability essentials [11], [12]. Lab and field work now incorporate not just a mix of methods, but also a combination of commercial and open-source tools that reflect the hybrid nature of modern-day forensic practice.

It follows that continuous professional development is needed. To avoid loss of technical capacity and professional credibility, practitioners need to stay aware of new technology, changing laws, and good practice standards [4][10].

Task-2 Investigation into the Attempted Theft of Proprietary AI Intellectual Property at Quantum Tech

1.Evidence of acquisition

Evidence was acquired by Cellebrite UFED and Cellebrite Physical Analyzer version 7.73.0.11 These are the following figures that narrate the entire acquisition process flow and prove how getting identified, extracted and validated using industry-grade forensic method can be done easily on android device. Evidence integrity is maintained at each step, and it provides a level of legal admissibility.

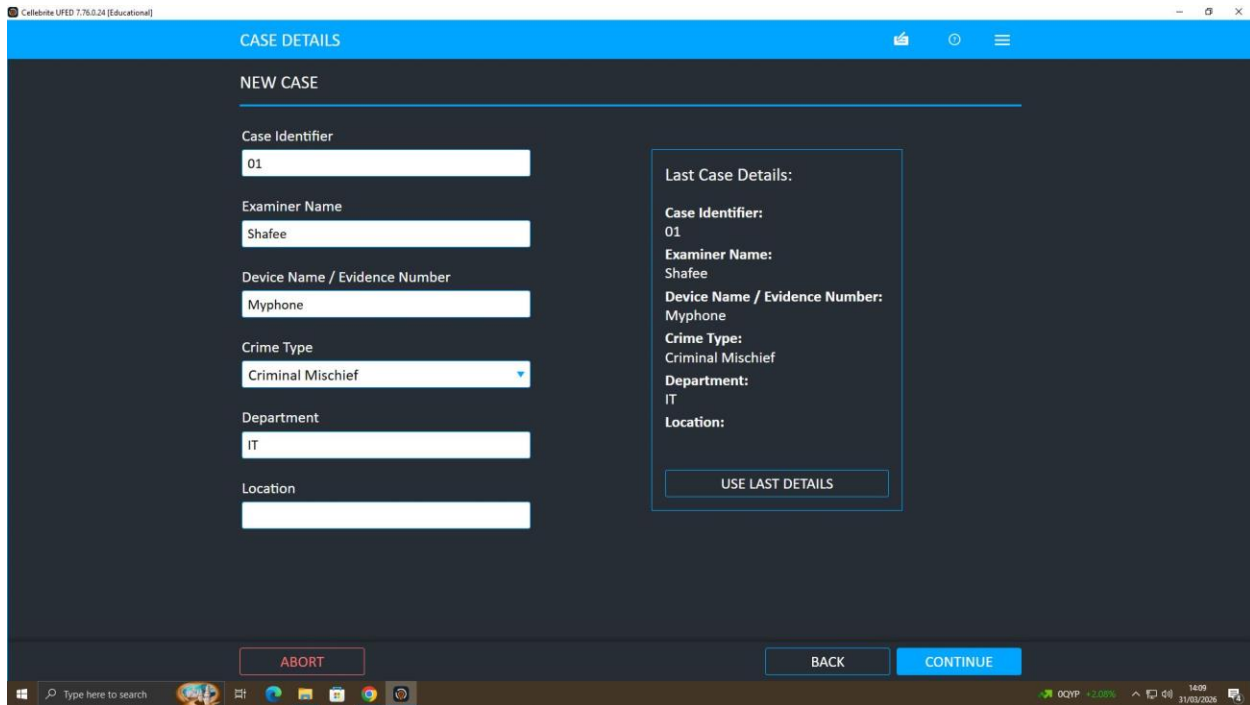


Figure1: Case details

This Figure depicts a forensic case created in Cellebrite UFED, noting the case ID, examiner and device label, and investigative context that is established to ensure accountability of examiners and recorded for proper chain-of-custody documentation prior to any evidential acquisition stage.

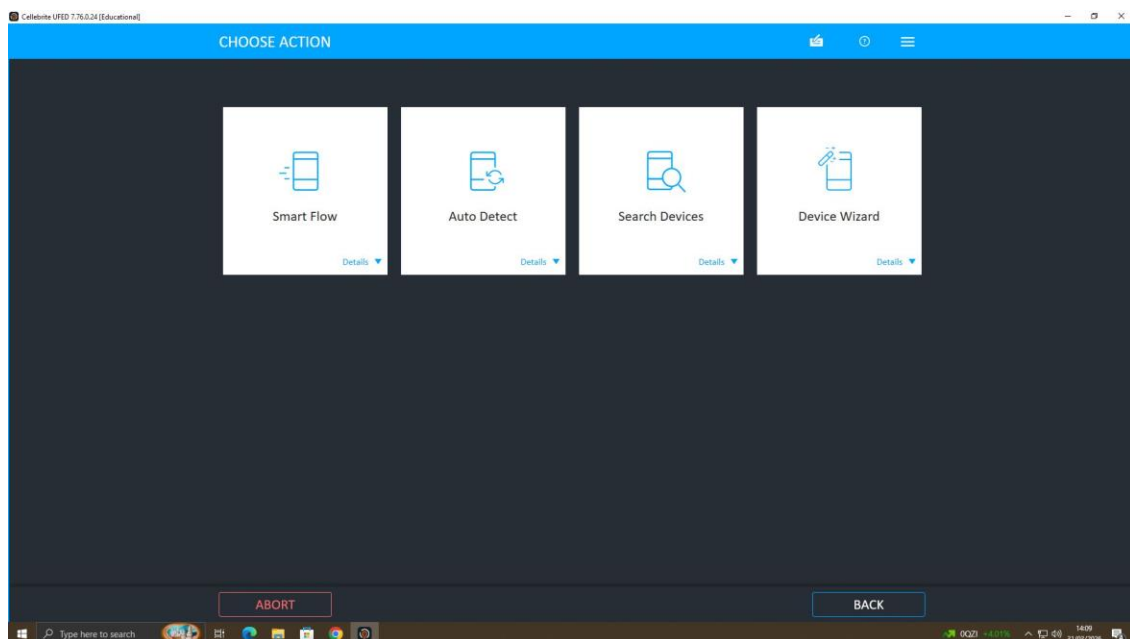


Figure-2: Action choose

This screen displays the action selection interface in Cellebrite UFED, where the examiner chooses the device detection method, including Auto Detect, ensuring a systematic and supported approach to identifying the connected mobile device. I have chosen auto detect to detect my phone.

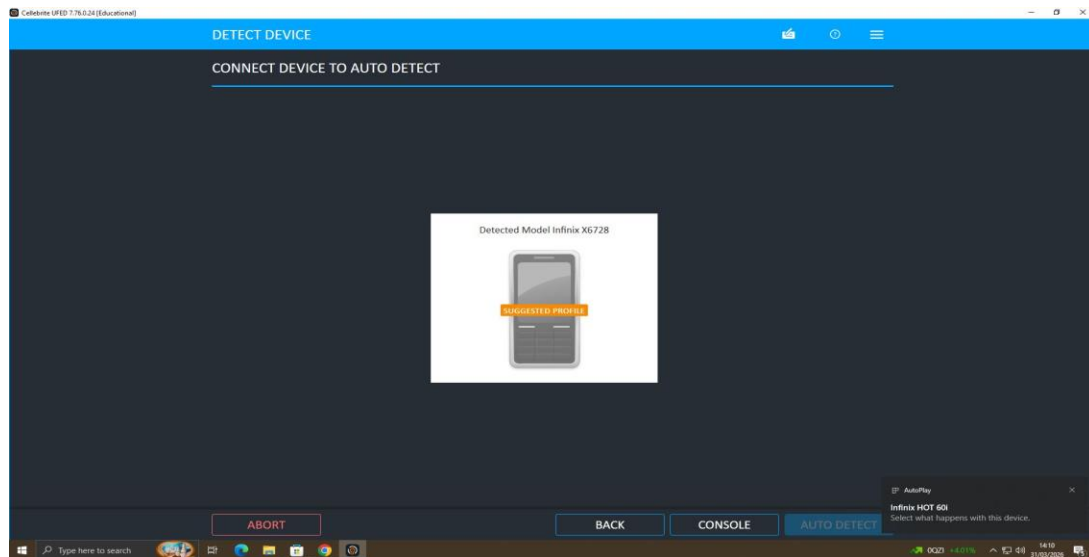


Figure3 :- Detect phone

This screen confirms successful automatic detection of the connected my device by Cellebrite UFED, identifying the model as Infinix X6728 and presenting the recommended forensic profile for subsequent evidence acquisition

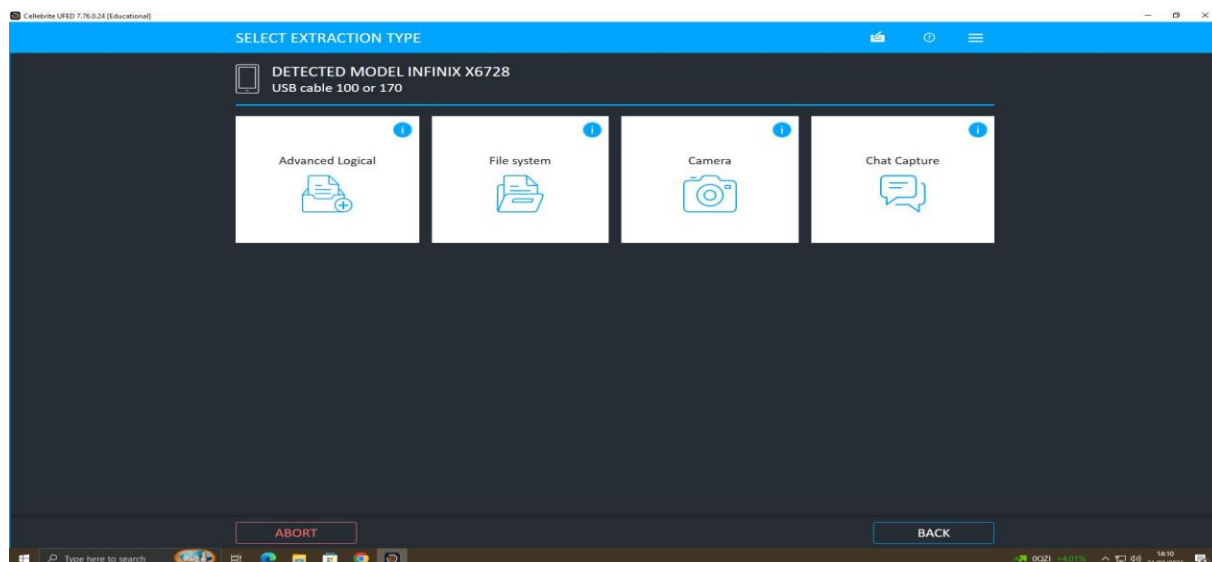


Figure-4:- Extraction type

This figure presents the available forensic extraction methods for the detected Android device, allowing the examiner to select an appropriate acquisition type based on data scope, device compatibility, and investigative requirements. I am going with the file system.

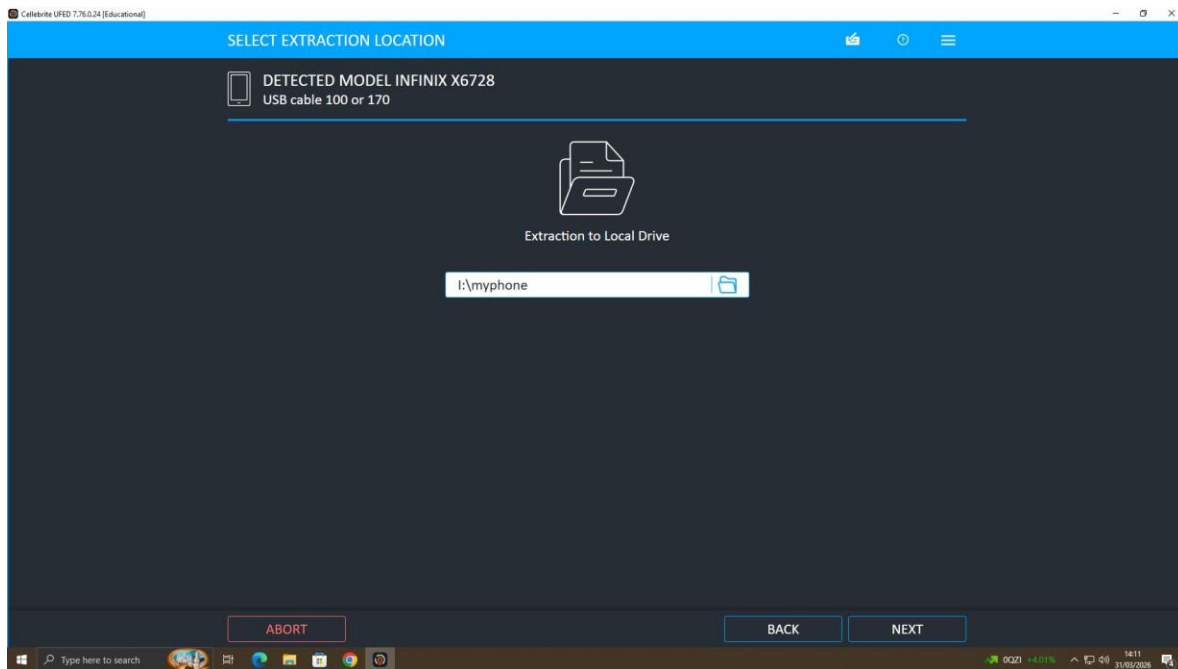


Figure-5: Select folder

This screen shows selection of the forensic extraction destination, specifying a controlled local drive path for storing acquired data, ensuring secure evidence of handling, organized case management, and prevention of cross-contamination.

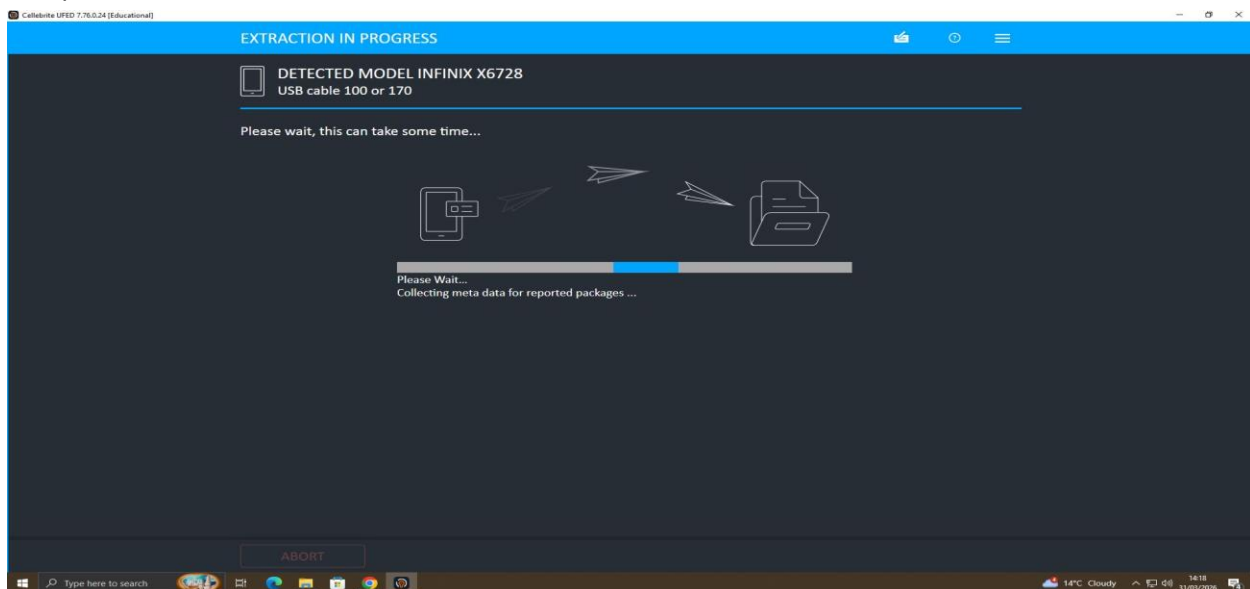


Figure-6: Backup data

This figure shows the Android forensic extraction process actively in progress, where Cellebrite UFED is collecting metadata and transferring data from the device to secure local storage without user interaction.

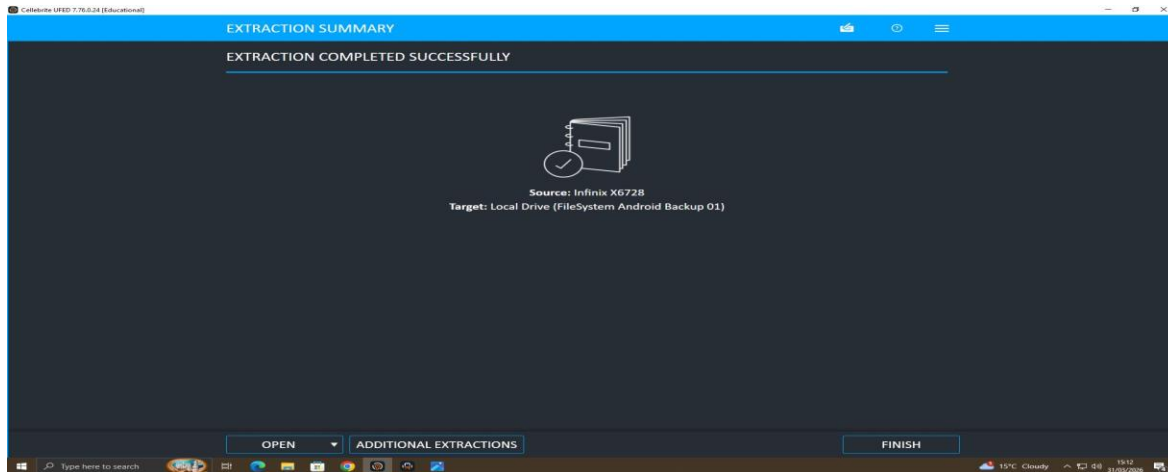


Figure-7: Extraction complete

This screen confirms successful completion of my phone forensic acquisition, identifying the source device and target storage location, and indicating that the file-system extraction was completed without errors or interruptions

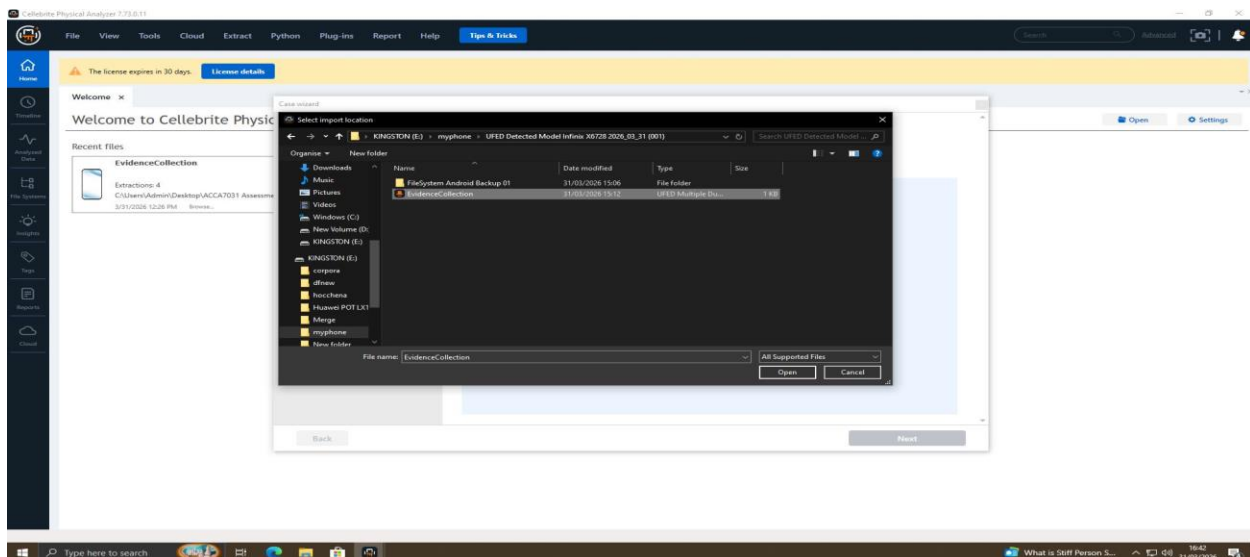


Figure- 8: import to analyzer

This screen shows the import of the UFED extraction output into Cellebrite Physical Analyzer, selecting the Evidence Collection file to load the acquired forensic image for read-only examination and further analysis.

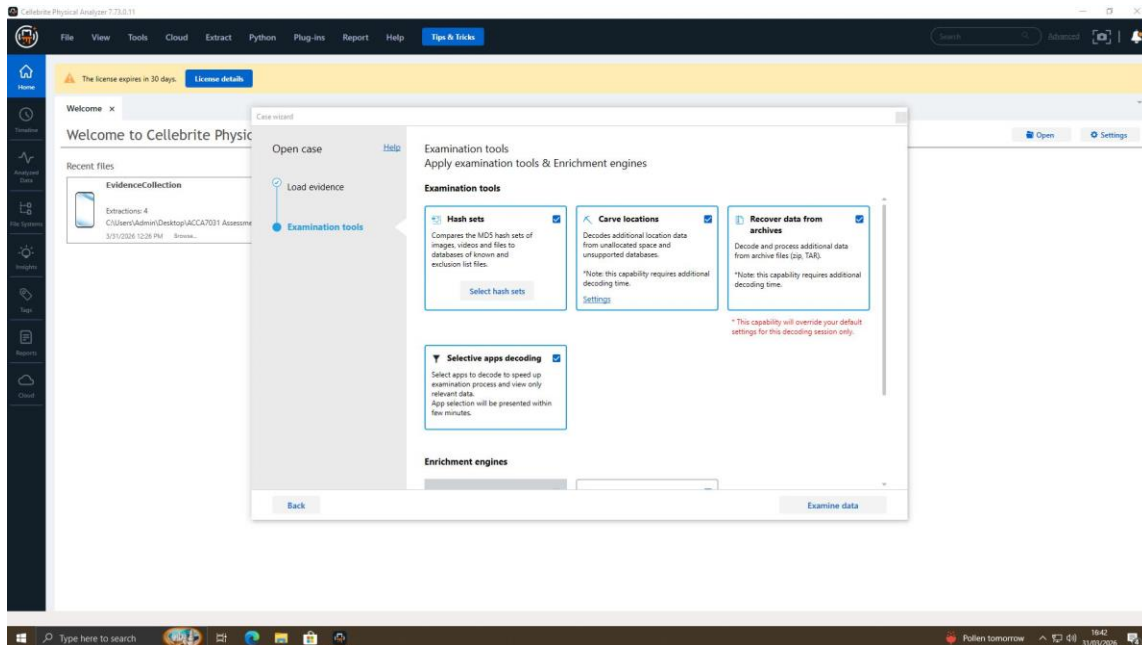


Figure 9:- Examining the data

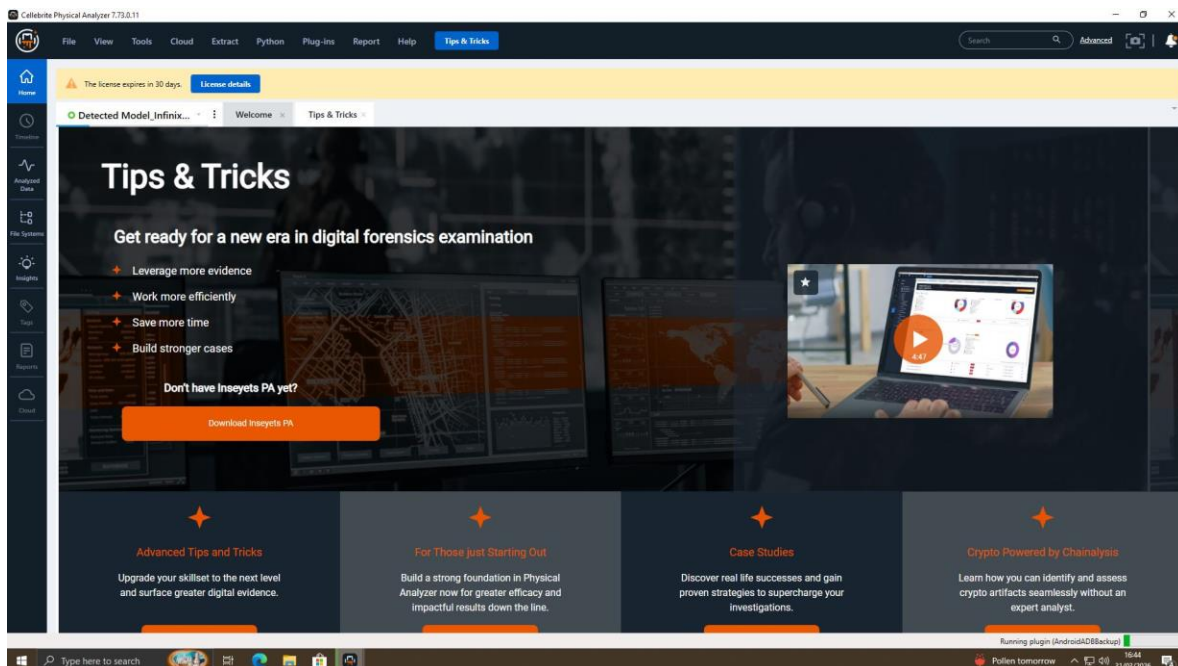


Figure- 10: decoding the apps

Figure 9 and 10 shows the selective application decoding interface in Cellebrite Physical Analyzer, allowing the examiner to control which application categories are decoded, ensuring relevant, proportionate, and efficient post-acquisition forensic analysis.

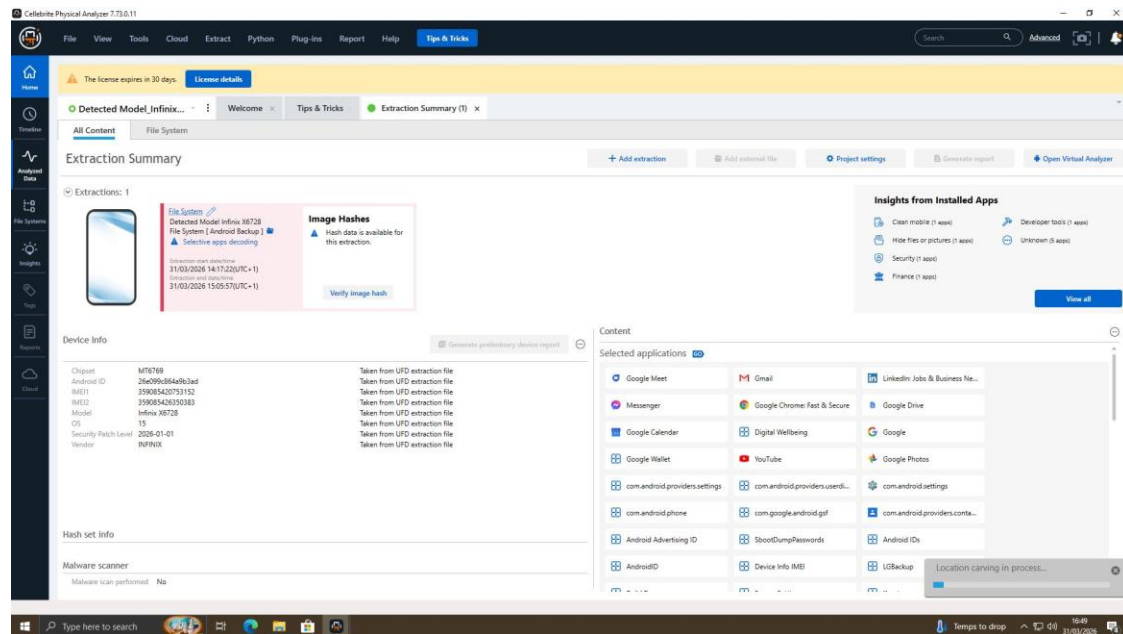


Figure 11- Verify hash

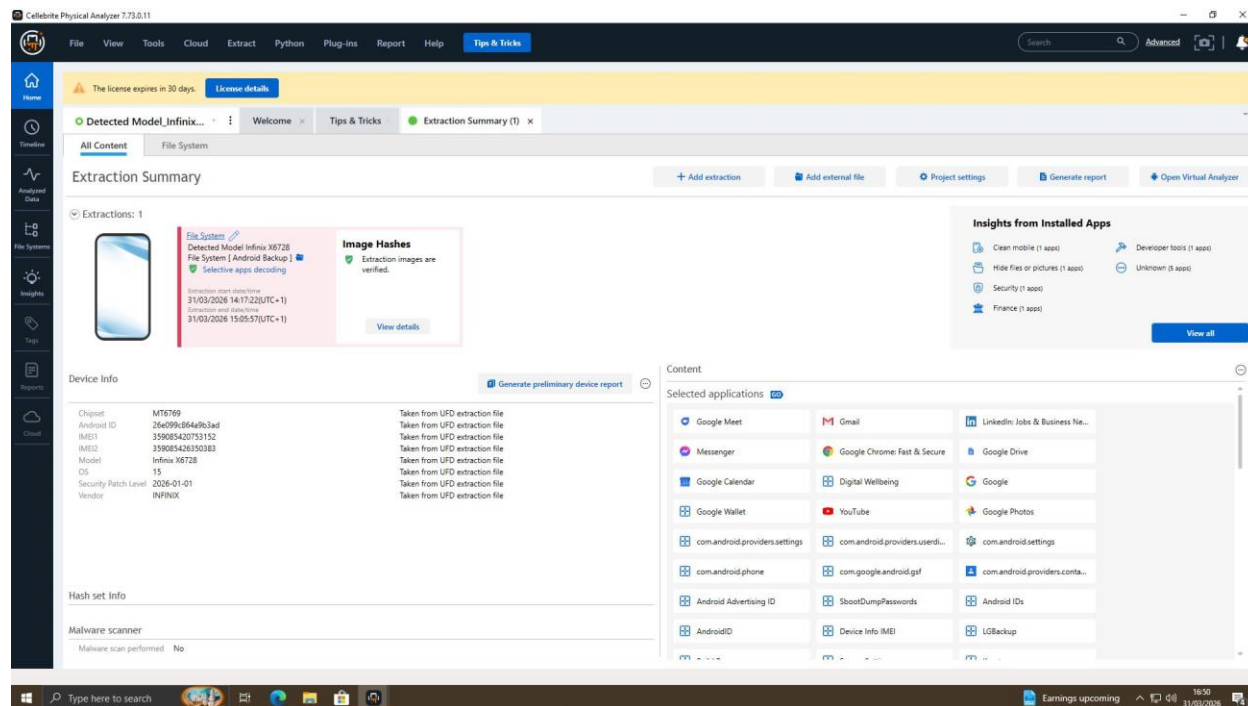


Figure- 12: verify image

This extraction summary confirms verified image hashes, demonstrating data integrity, and ensuring the forensic evidence remains authentic and admissible for analysis.

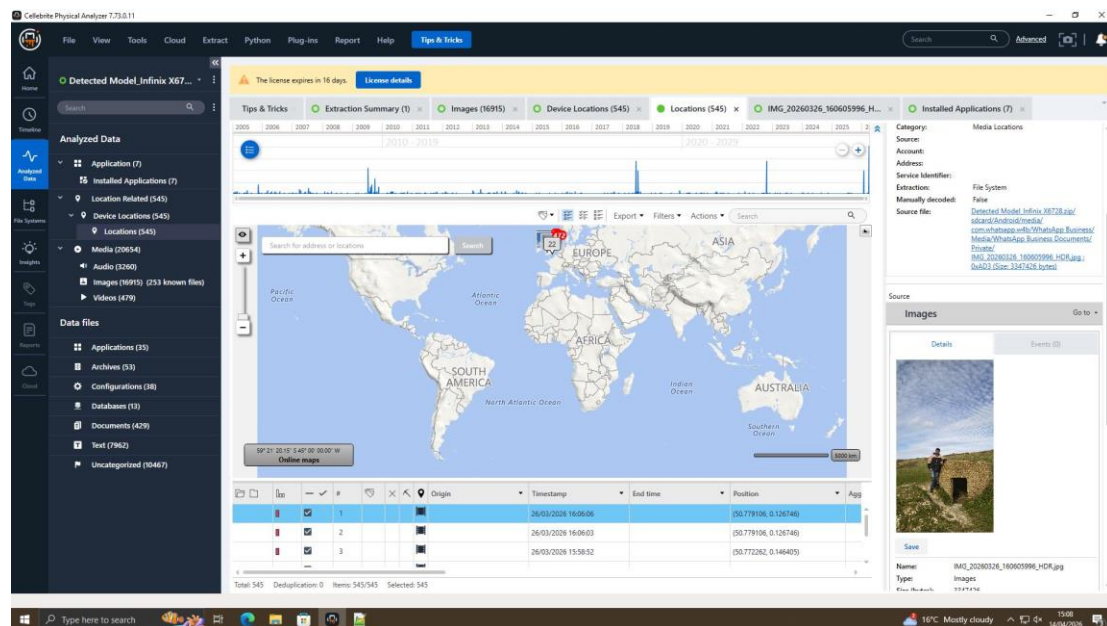


Figure 13: image evidence of mine

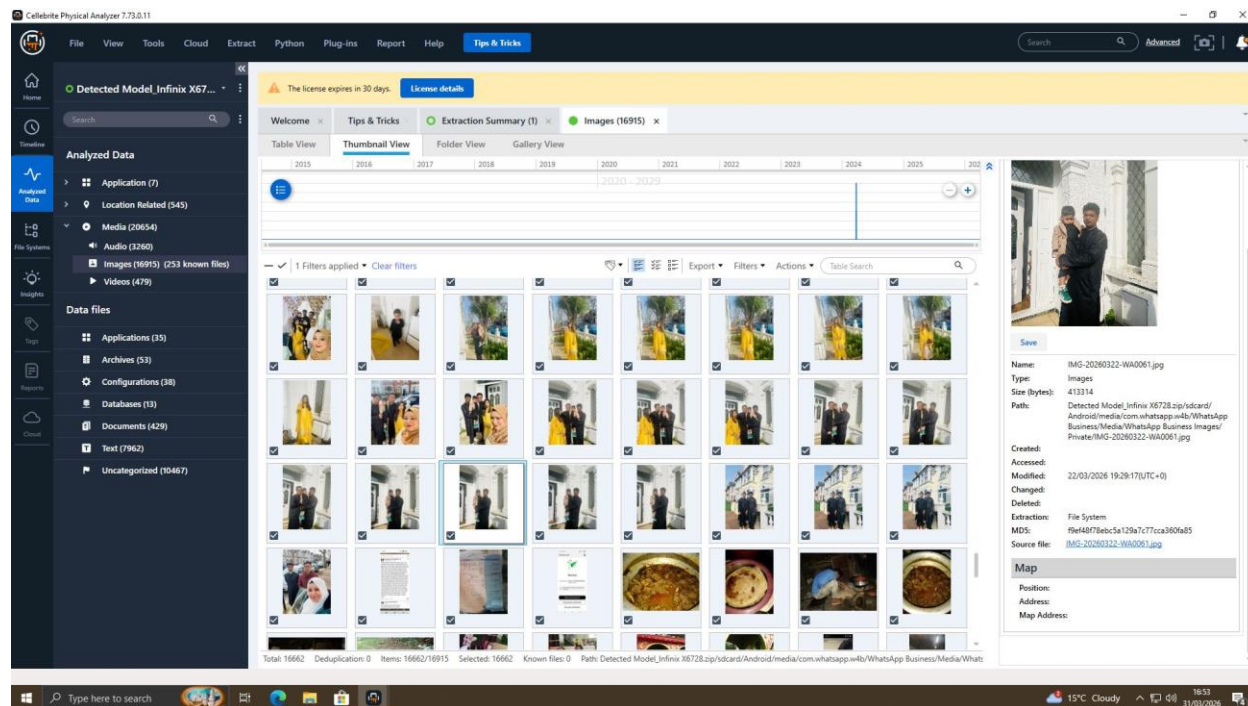


Figure 14 : Image of mine

This interface displays extracted image artefacts and associated metadata, alongside mapped geolocation information, demonstrating preservation of media files, timestamps, hashes, and location data within Cellebrite Physical Analyzer after verified acquisition

2. Communication Analysis:

WhatsApp, Snapchat, Genie and Gmail were all sampled over each smartphone to retrieve the communication artefacts. By breaking down how Emma began these conversations, they proved that she was clearly trying to let someone know far in advance of this development — long before October 2023 for their analysis — that there would access given to the data and intent to sell. Joe was a middleman who helped with negotiations and served as a liaison with a buyer connected to NexGen Circuits.

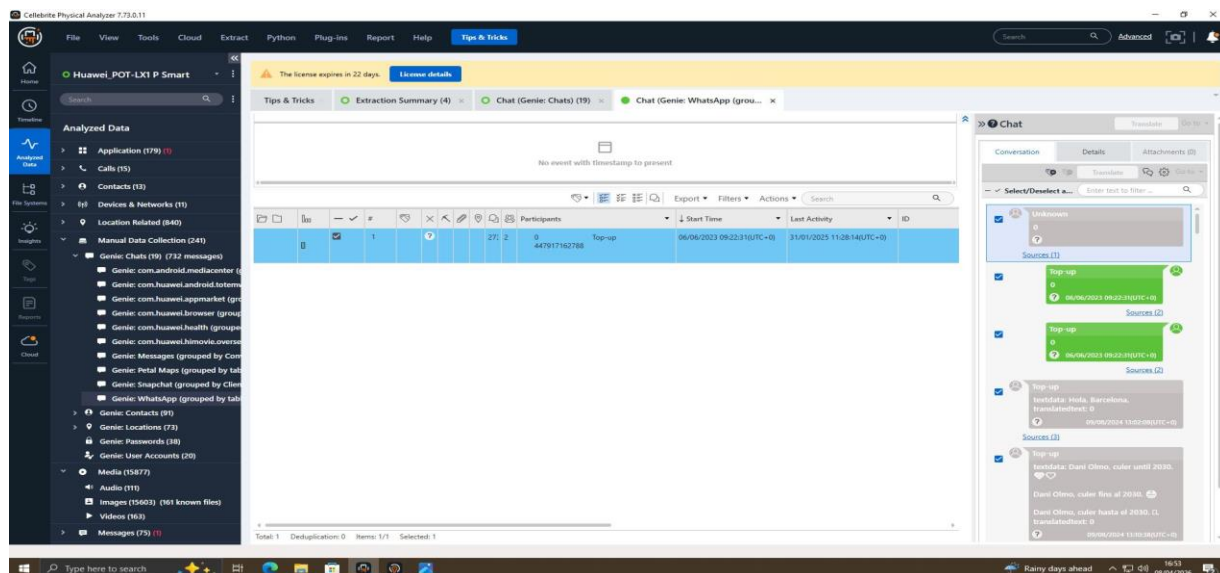


Figure 15: Extracting the WhatsApp conversation

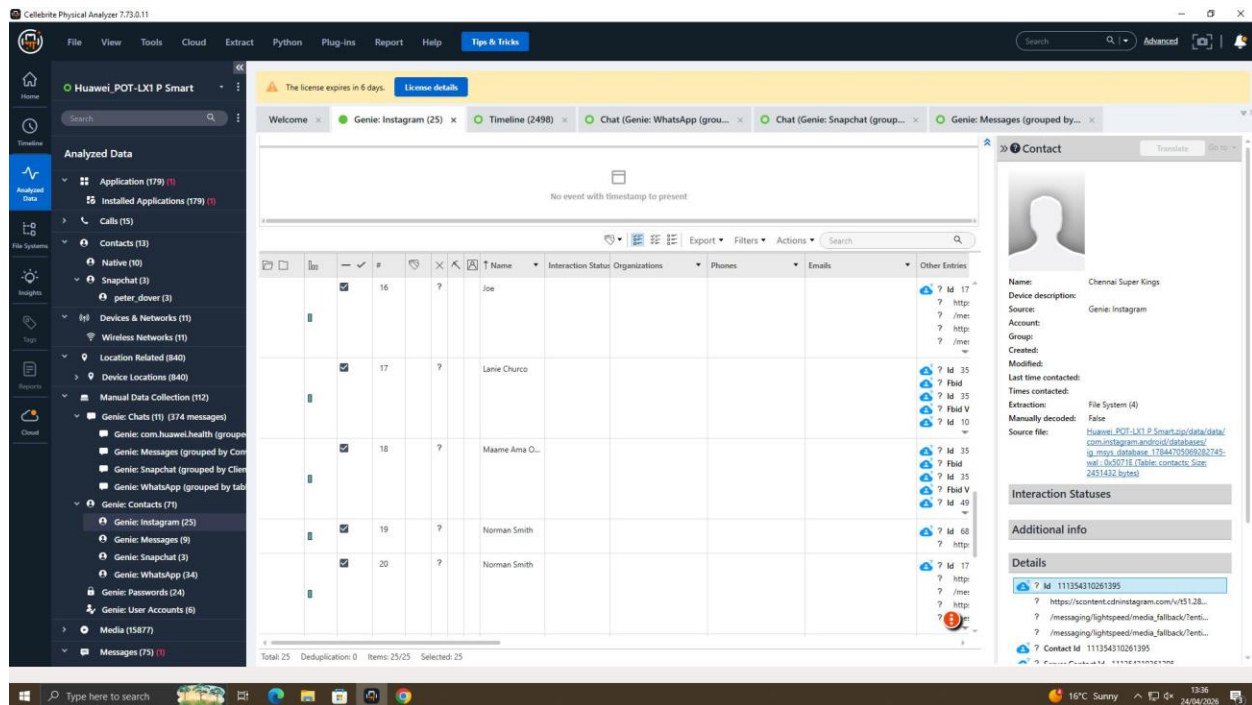


Figure 16 :- Instagram DM

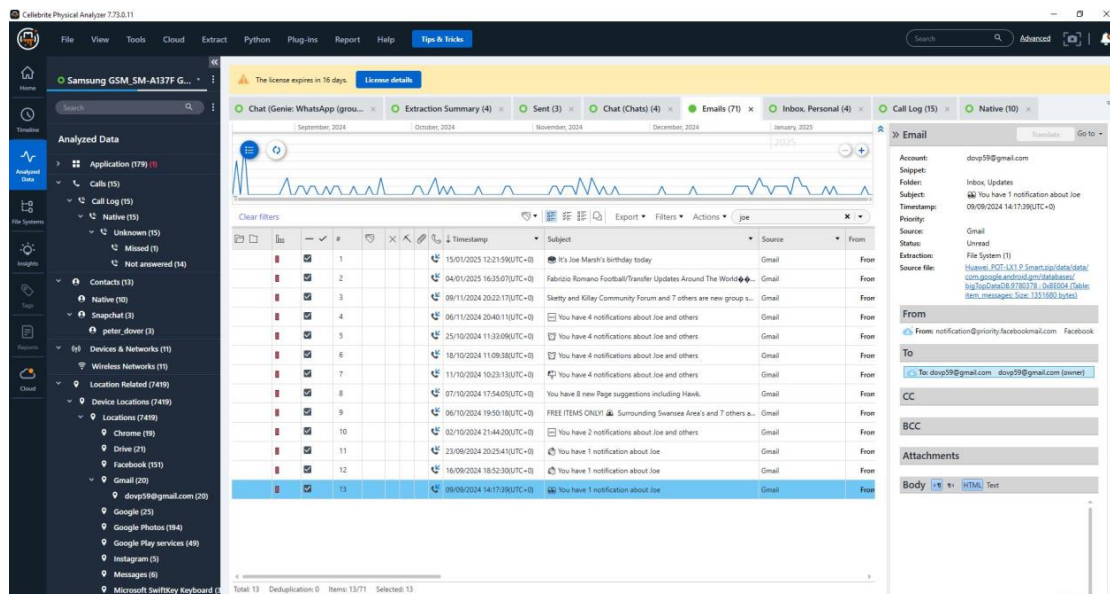


Figure 16: Email extraction

This view presents extracted email messages and WhatsApp conversation within Cellebrite Physical Analyzer, enabling correlation of timestamps, contacts, and communication frequency to corroborate interactions between suspects across devices.

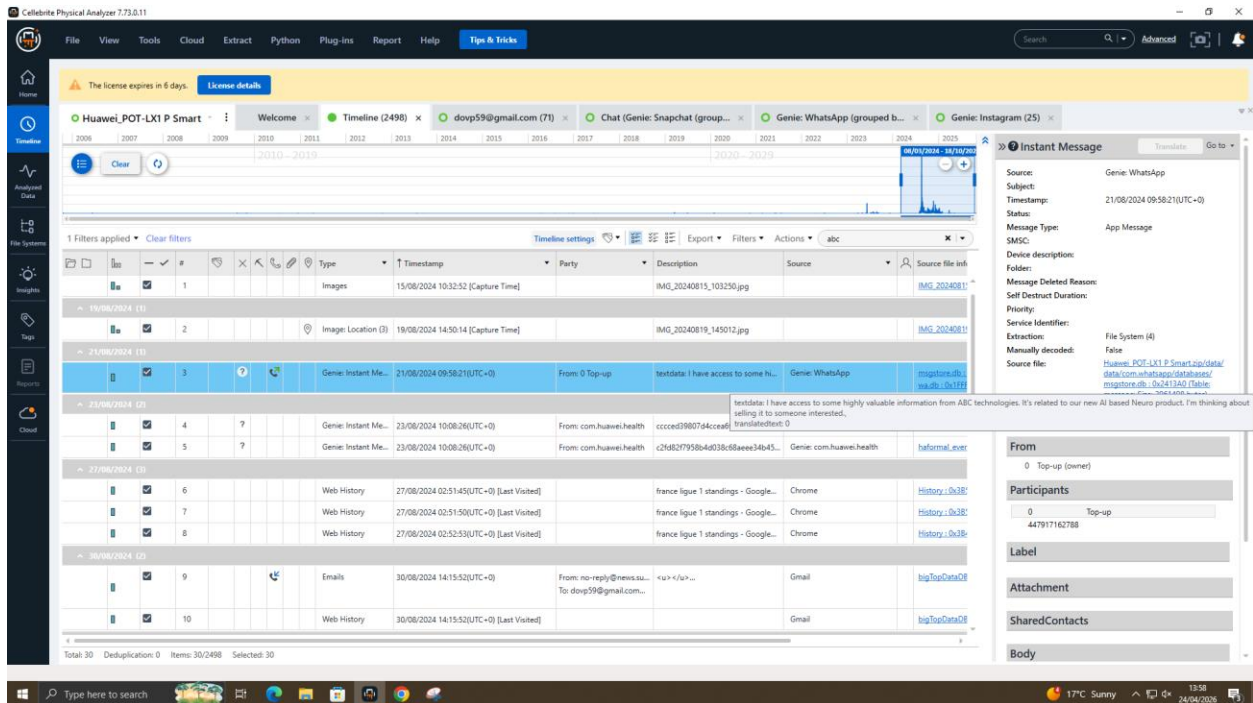


Figure 17: Timeline

Screenshot of Cellebrite Physical Analyzer showing mobile forensic timeline, WhatsApp messages, images, web history, timestamps of participants Joe, Emma, Norman.

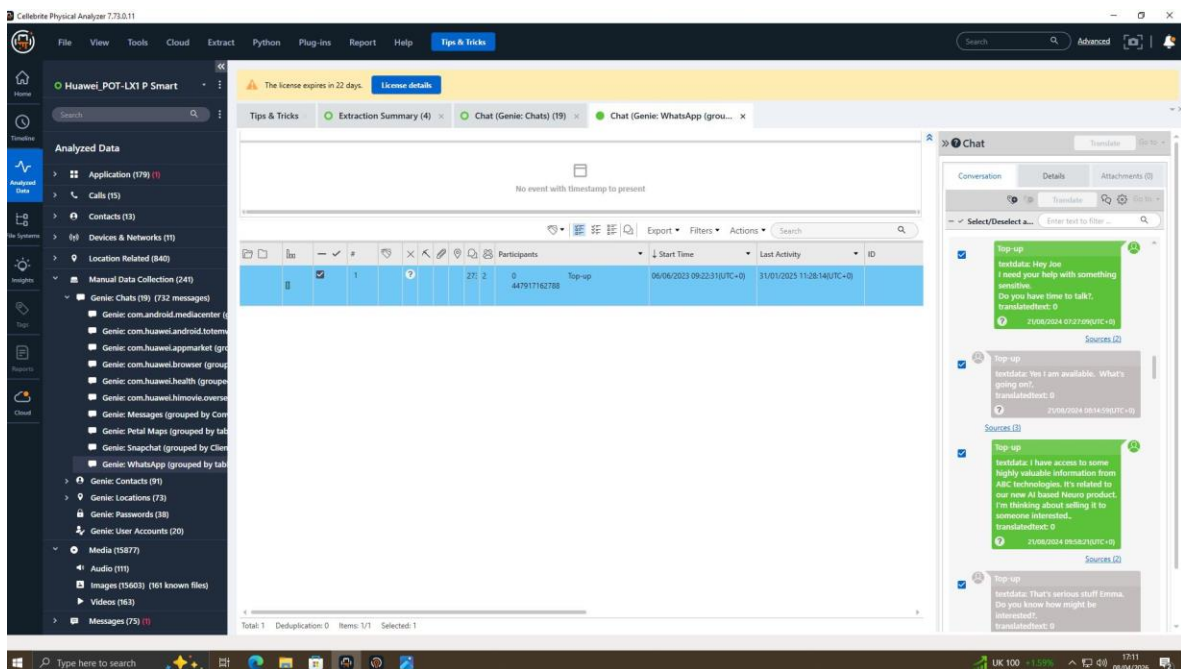


Figure 18: Whatsapp conversation between Emma and Joe

This screenshot displays a time-stamped WhatsApp chat where a Emma raises a request for assistance and discloses intent to sell valuable AI-related information, indicating initial escalation of coordinated communication activity.

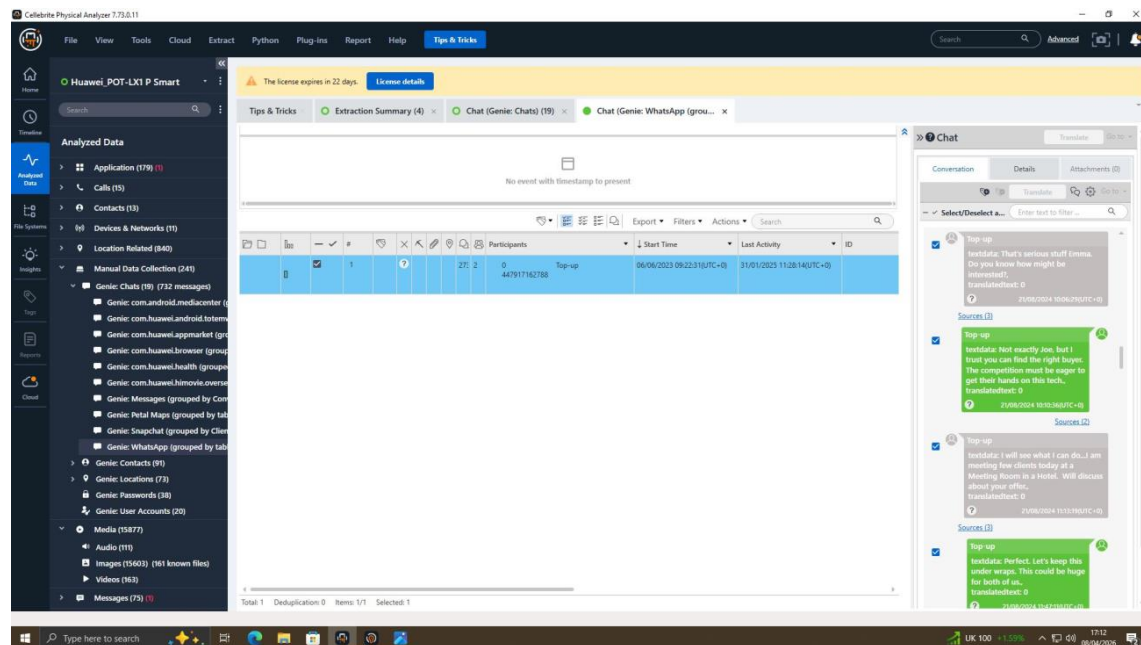


Figure 19:

From the above conversation we understand that Emma is looking for buyer and joe is taking responsibility to manage a client.

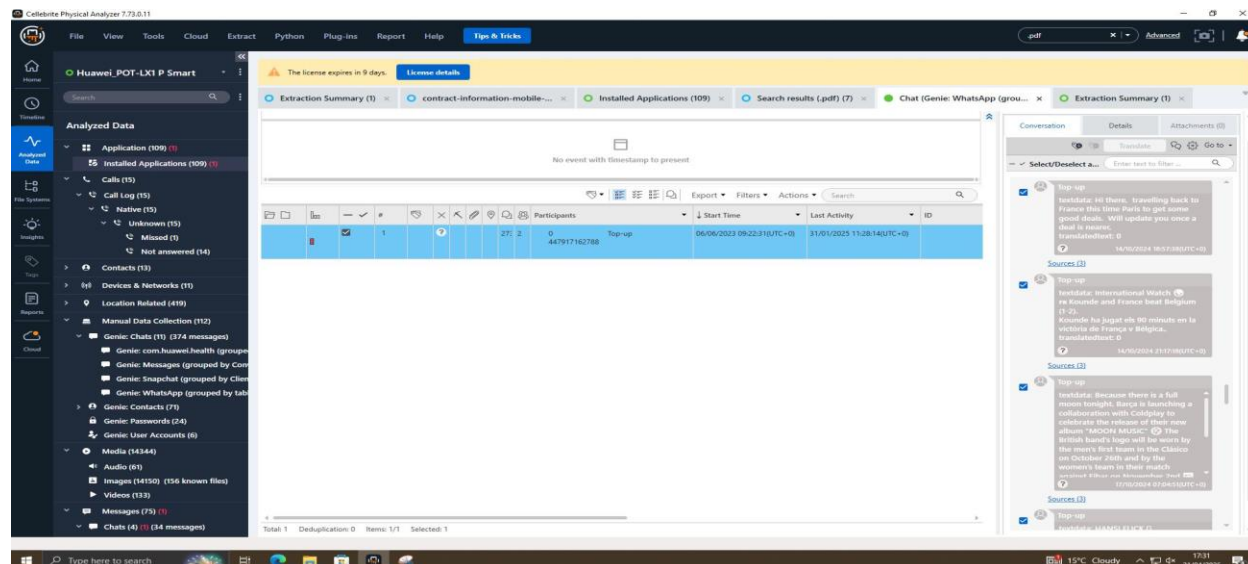
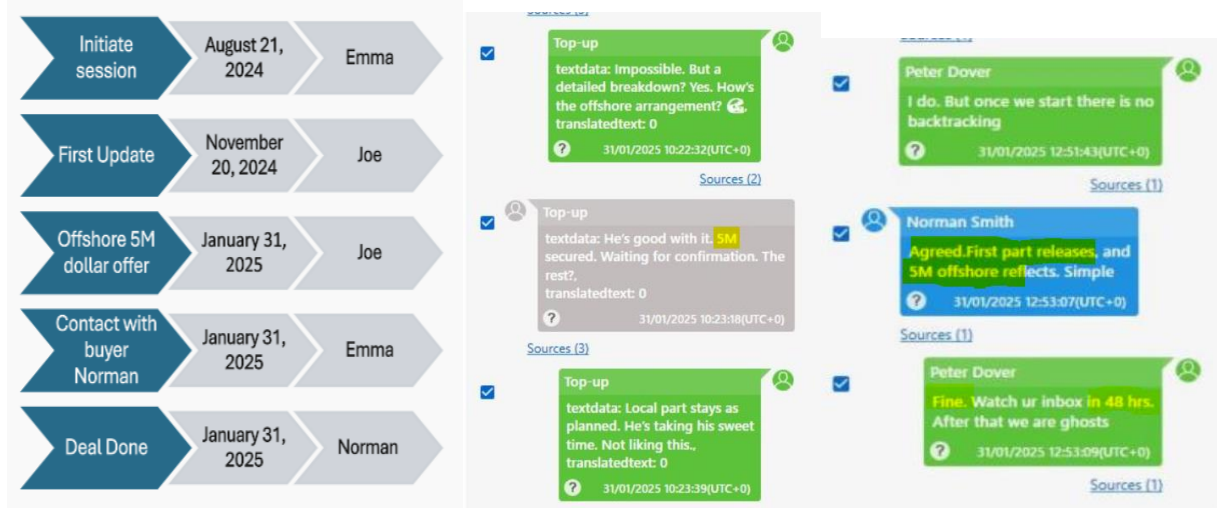


Figure 20

In this conversation Joe updates Emma that he did a meeting at Paris in France and very near to deal. This is the update of 14th of October 2024.

2.1 Reconstruct the Timeline



According to the analysis of WhatsApp messages, emails, Instagram, and Facebook DMs, the timeline is as follows. On August 21, Emma initiated the session with Joe and shared with him what she had. Joe took responsibility for managing a client. On November 20, 2024, Emma asked for an update in response to Joe's messages, in which he shared that he had met with the client, and she continued messaging him about it. On January 31, 2025, Emma asked about the progress, and Joe told her that he had managed to find a buyer, but they required a demo or sample copy and offered a financial deal of \$5 million. On the same date, Emma directly contacted Norman Smith, who offered the same financial deal after the release of the first part, and Emma agreed to this.

3.File Analysis

The image displays a file analysis tool interface, likely for mobile device forensics. The top section shows a list of analyzed data categories and their counts. Below this, a table lists individual files with columns for file name, path, size, and creation date. A sidebar on the right provides detailed information about the selected file, including its type, size, path, and creation date. The bottom section shows a file explorer view of the analyzed data, with a list of files and folders displayed in a grid format.

Analyzed Data:

- search & web (1194)
- Autofill (1)
- Calendar (184)
- Search History (190)
- User Dictionary (176)
- Native (173)
- Swiftkey (3)
- Web Bookmarks (9)
- Web History (749)
- Snapchat (73)
- petar_dover (73)
- User Accounts & Details (237)
- Device Users (2)
- Passwords (243)
- User Accounts (12)

Data Files:

- Applications (2510)
- Archives (1453)
- Configurations (26)
- Databases (1019)
- Documents (12)
- Shortcuts (6)
- Text (1456)
- Uncategorized (28656)

File Details:

- Name: Open.7z
- Type: Archives
- Size (bytes): 20033
- Path: Detected Model_Nokia C2 2nd Edition.zip/Android/WhatsApp/Documents/Open.7z
- Created: 31/01/2023 10:33:34(UTC+0)
- Modified: 31/01/2023 10:33:34(UTC+0)
- Changed: 31/01/2023 10:33:34(UTC+0)
- Deleted: 31/01/2023 10:33:34(UTC+0)
- Extraction: File System (3)
- MDS: d0322a604b701132db0512419737051a
- Source file: Open.7z

File Explorer View:

- 22 items | 1 item selected | 19.3 KB
- Files: 01, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20

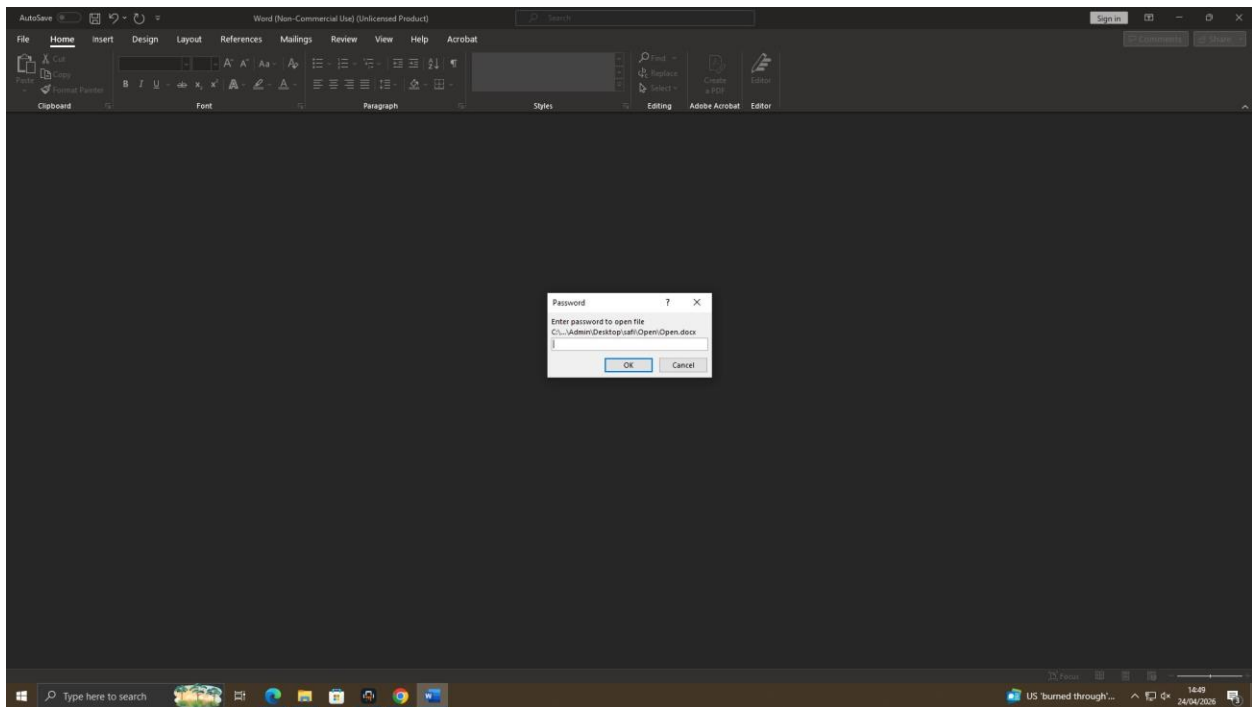


Figure –22: Other file

This figure shows the files marked as possibly related to the investigation but could not be analyzed further due to password protection.

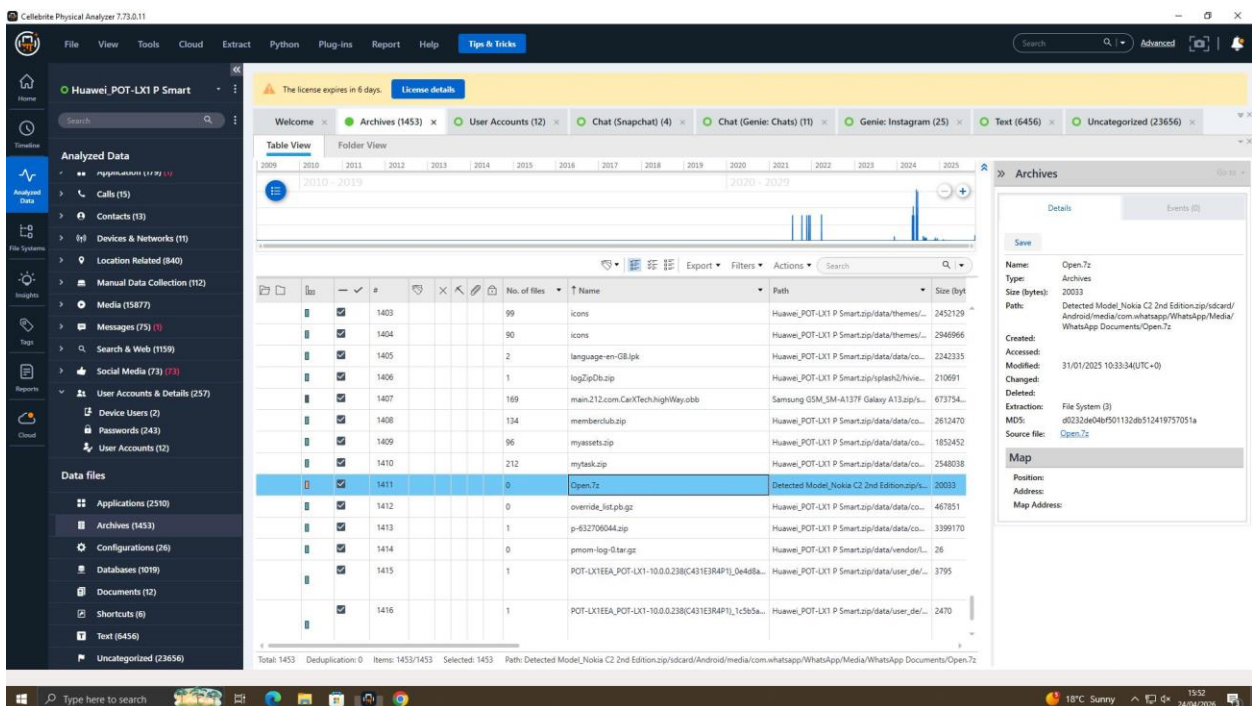


Figure : Metadata Analyze.

This snapshot indicates that this file is Updated on 31st January,2025

4. Call log and email correlation

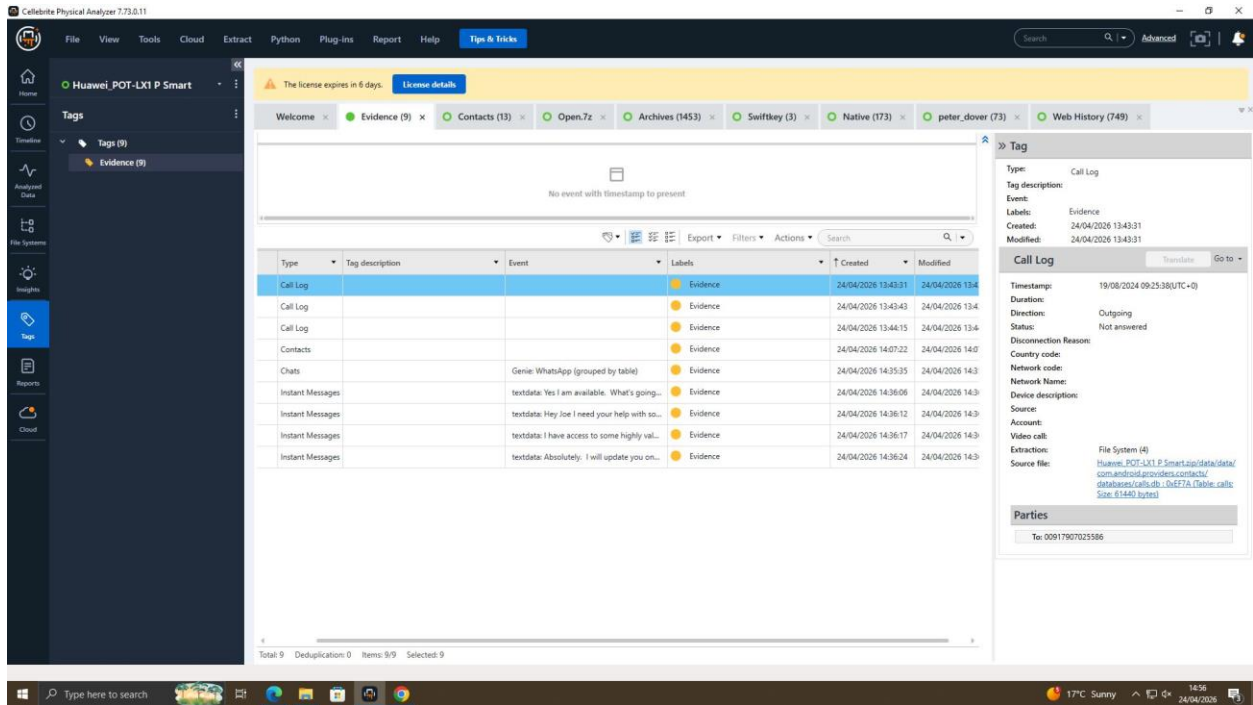


Figure-23: Correlation

Instagram DM and evidence call log correspond with one another

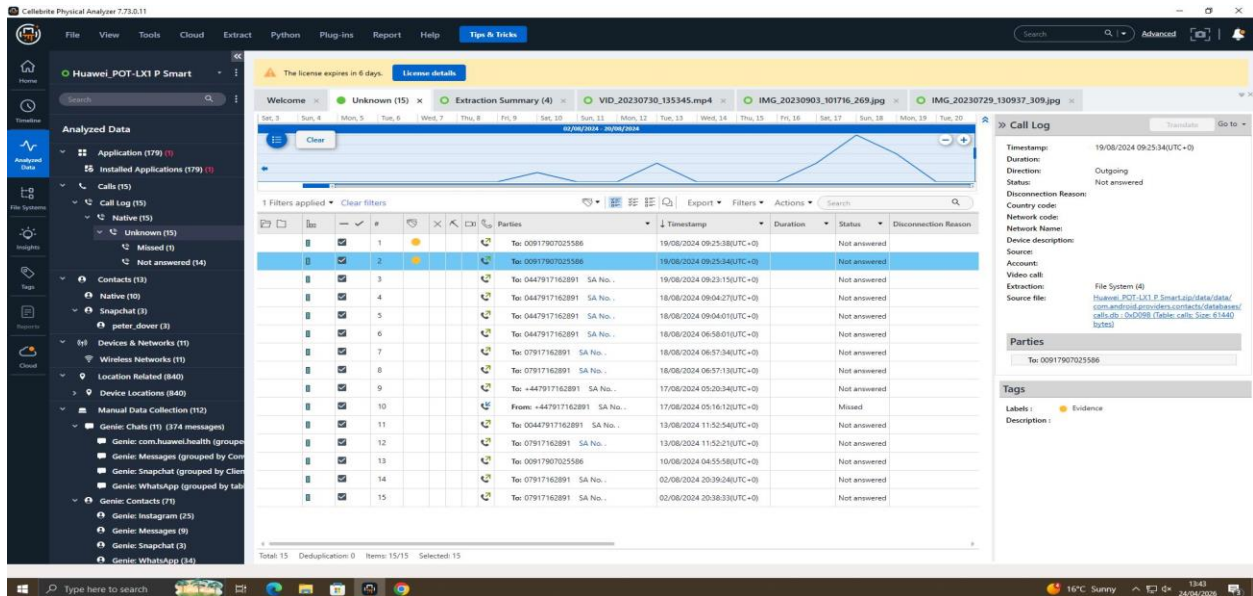


Figure 24:- Call log

In figure-24 call log is extracted and tagged the Joe's number it is called by Emma on 19th of August 2024

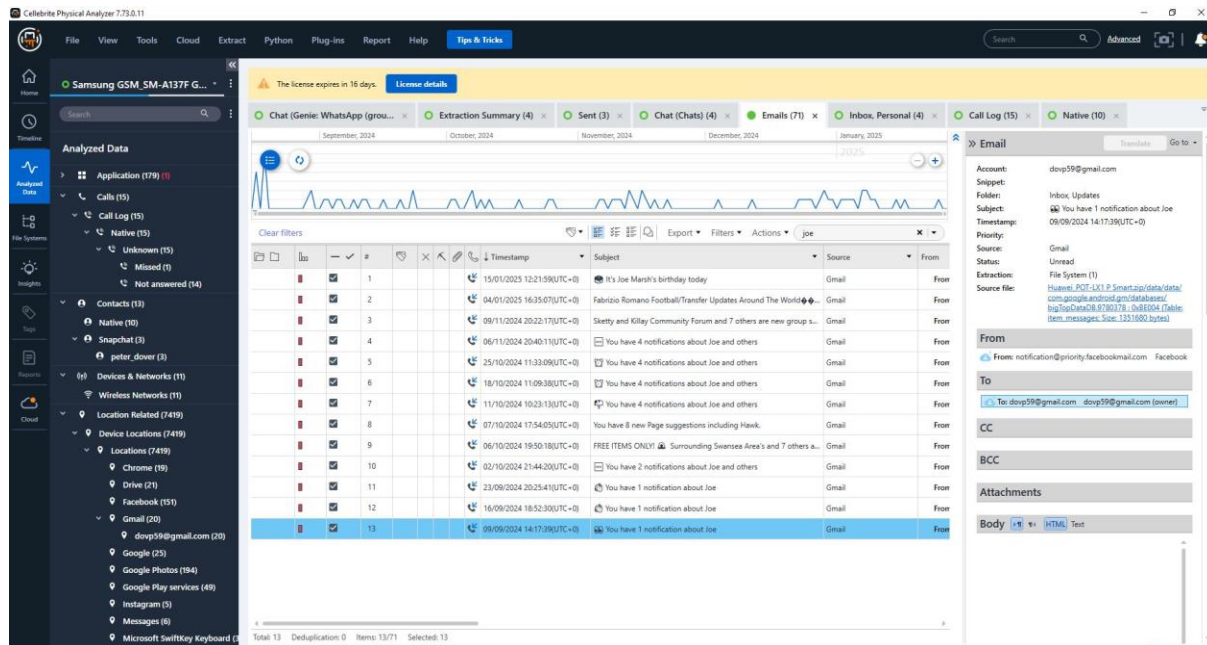


Figure-25: Email log

Here is the email exchange log, but nothing found relevant to patent or named Emma.

5. Suspect Profiling

The suspect outline follows the WhatsApp discussion log, call log and it's obvious pattern. I give some solid digital evidence to put this profile together.

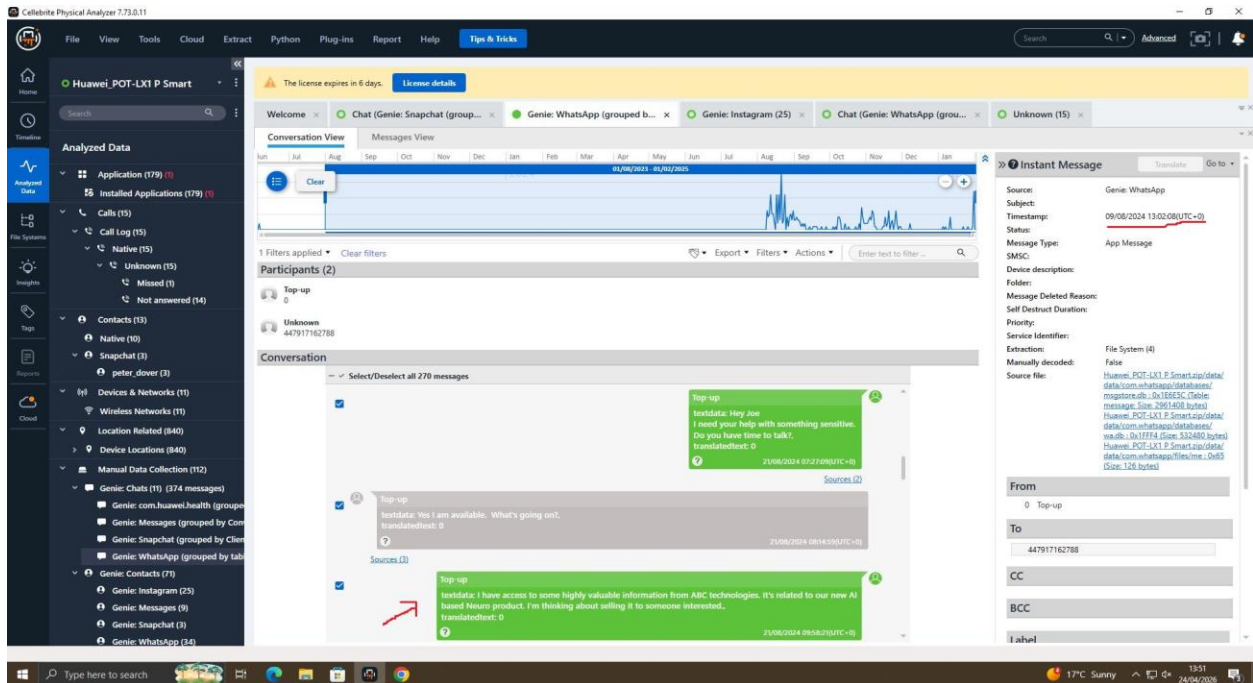


Figure-26: Conversation

Looking at this figure, Emma Clearly states that she had illegally accessed high-value assets. She goes on to reveal that she needed help finding a buyer and mentioned that she told Joe so he could look after a potential client.

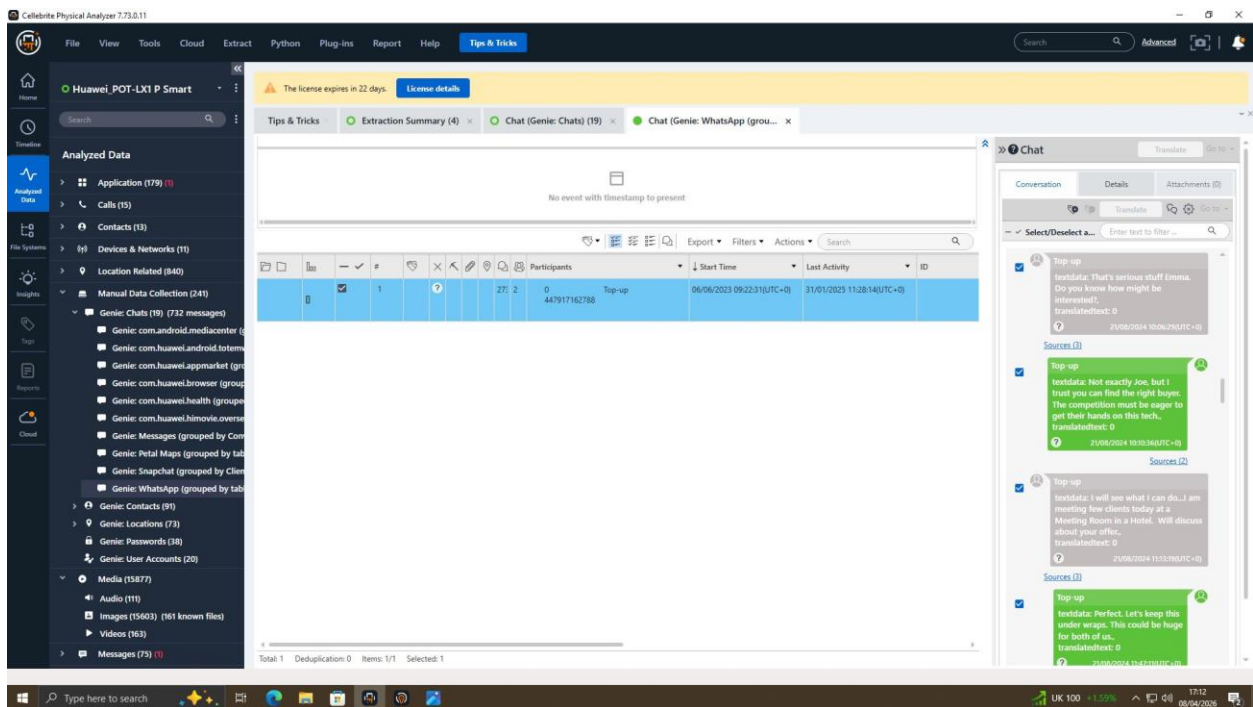


Figure 27: Conversation

Joe acted as an intermediary who directly met with the client. Following this engagement, he subsequently provided an update to Emma regarding the outcome of the interaction.

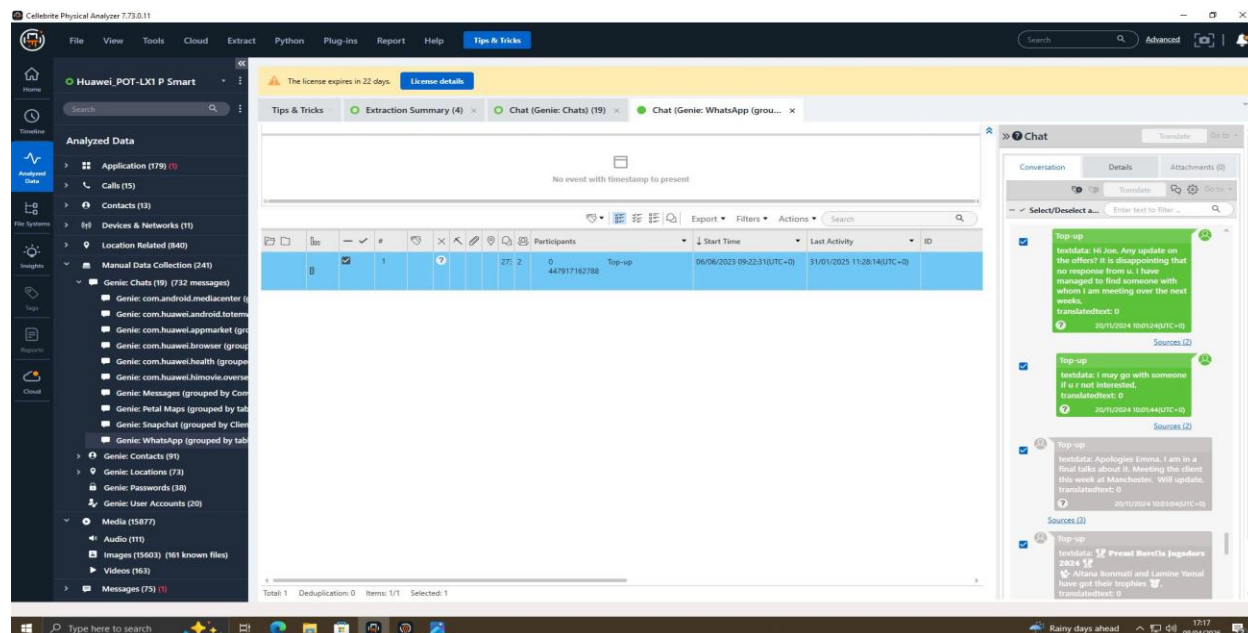


Figure-27: Conversation

Emma repeatedly requested status updates from Joe, to which Joe responded with a final communication within a very short time frame.

Suspected profile is based on forensic analysis of WhatsApp chat logs, call records & identified conversation behavior patterns. Digital evidence reflects an organized and interactive partnership between the parties that indicates premeditated planning and assignment of roles.

A review of the conversation logs suggests that Emma Clearly confirmed accessing high-value assets without authorization. The messages also detail how she inquired about selling these assets and finding a buyer for them. Emma's solution to this was to contact Joe and put him in charge of handling client interactions.

Later evidence shows that joe was used as a middleman where he got in touch and arranged meeting with the potential client. Joe then updated Emma on the progress of the engagement and what happened. Analysis of the timestamps and rate of messaging suggests Emma was the constantly asking for status updates, insinuating active participation

and monitoring. Joe is the only one responding to all, including a last message within milliseconds of time announcing the end of a transaction-relevant conversation.

The following analysis of the digital artefacts as a whole points to the conclusion that such details imply a more planned collaboration, in which Emma acts as initiator and coordinator, while Joe acts as intermediary. The information is based on digital evidence and behavioural patterns, and it seeks only to assist investigative evaluation rather than provide proof of legal responsibility

6. Forensic Images acquisition:

Forensic images are given by the Quantum-IT, after that just extract all the images for investigation by using cellebrite physical analyzer 7.7.2. Now, describing the extraction process and image verification.

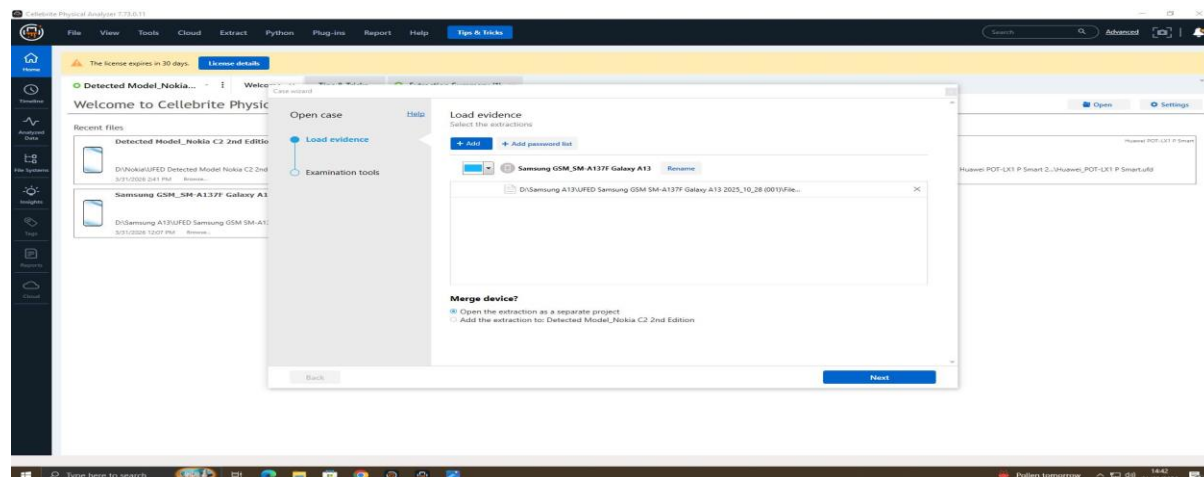


Figure-29: Loading image

First of all open the Cellebrite physical analyzer and from file open the image and four image all together.

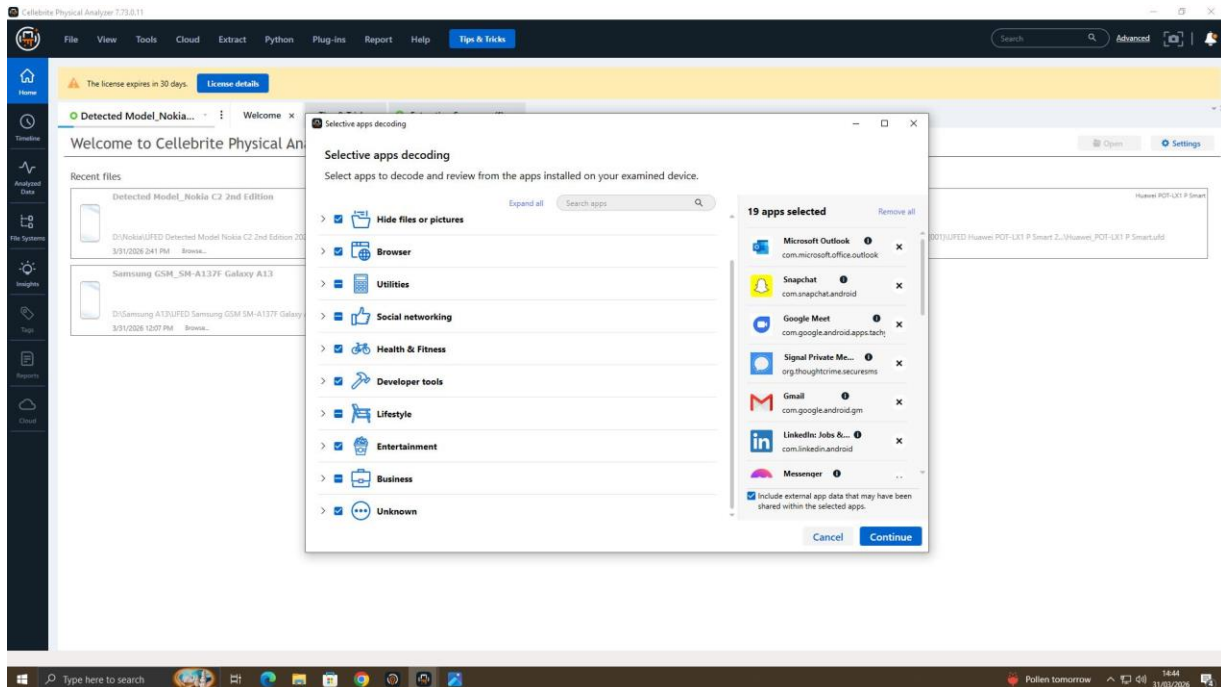


Figure-30: App decoding

After introducing the image pop-up, a window with loaded app and select for decoding.

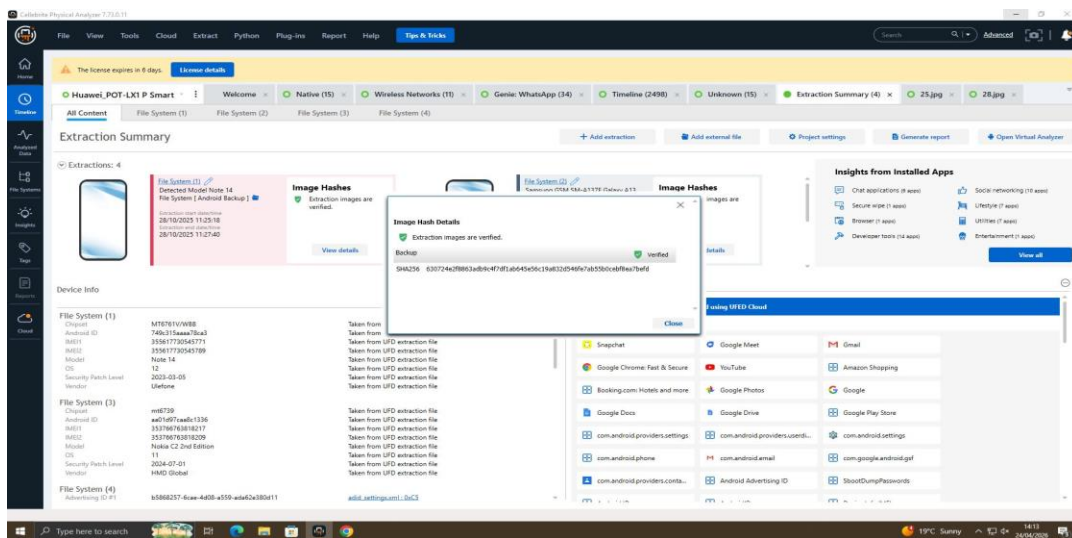
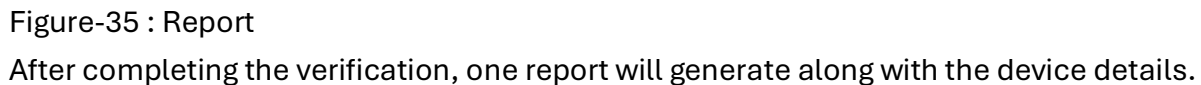
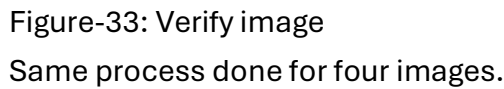


Figure-31: After decoding verify the hash for images. In here sha-256 is verified.



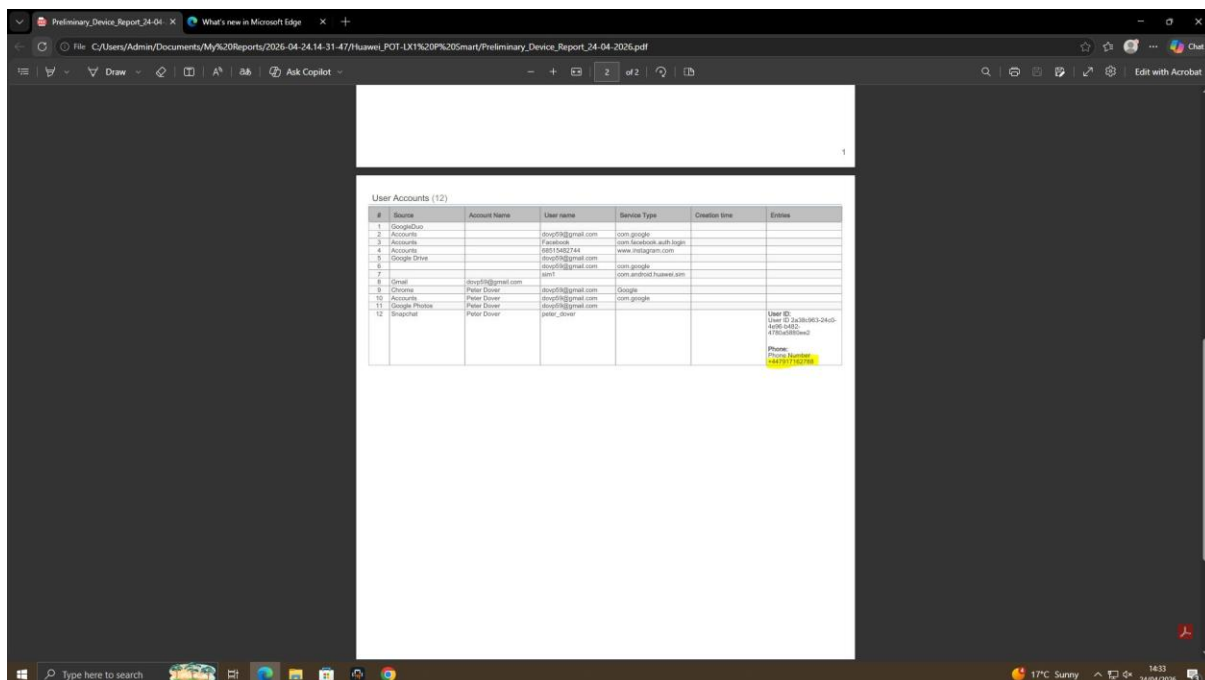


Figure-36: User account

End of the report user account details also added, so we can understand all four image is constructed from phone.

7. Forensic Report

7.1. Case Background

Quantum Tech discovered a purported attempt to acquire corporate information. The internal security monitoring had indicated some unauthorized access of data, suspicious communications, and potential conspiracy between three or more people. They are Emma (suspected perpetrator), Joe (suspected intermediary), and Norman (suspected buyer). It aimed to find digital evidence of attempted data theft and illegal possession or export of material.

7.2. Evidence Inventory & Chain of Custody

Individual forensic acquisition of the four separate mobile devices were performed using Cellebrite UFED. All devices were acquired via logical or file system extraction under supervision. Verification of SHA-256 hashes showed that the integrity and authenticity of all forensic images were assured. In the investigation, evidence was kept exclusively in the control of the examiner.

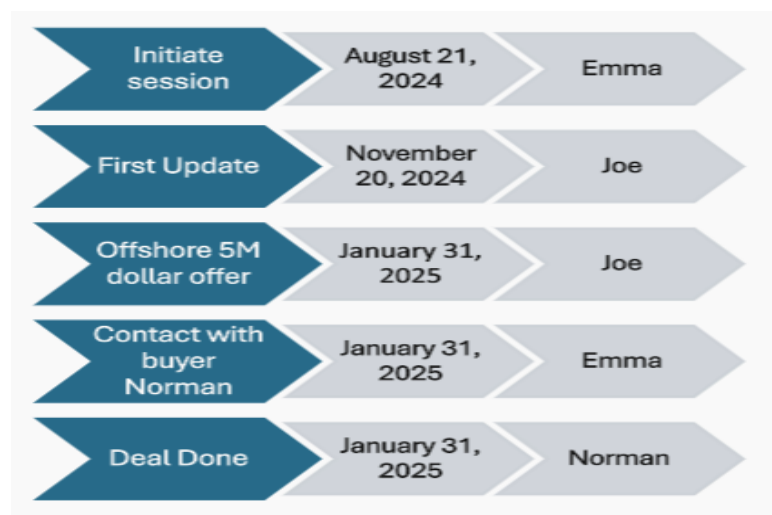
7.3. Methodology

Forensic acquisition was performed using Android Backup and Android ADB techniques via Cellebrite UFED. Analysis was conducted using Cellebrite Physical Analyzer, enabling timeline reconstruction, application analysis, account identification, communication examination, and file system review. All procedures followed accepted digital forensic best practices and evidence integrity principles.

7.4. Findings

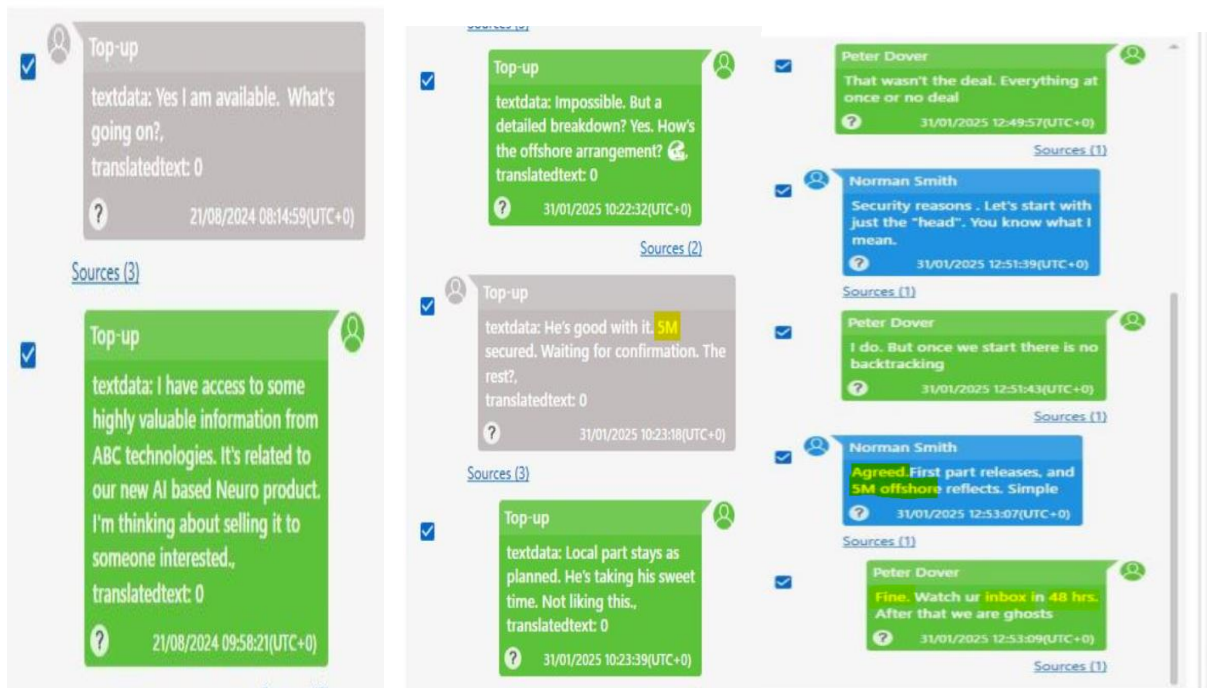
7.4.1 Timeline Analysis

This evidence was collected through forensic acquisition using the Android Backup techniques through Cellebrite UFED. Cellebrite Physical Analyzer was used for analysis; basic functions were performed to reconstruct timelines, app analyses, accounts, communications and file system review. All of the methods used conformed to recognized digital forensic practices and standards concerning maintaining evidence of integrity.



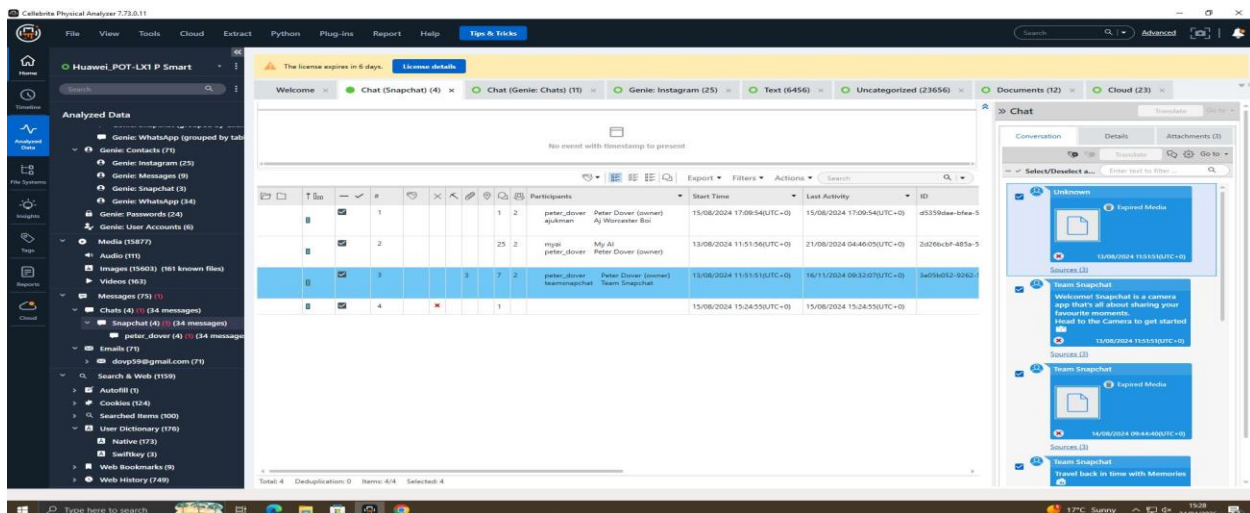
7.4.2 Communication Analysis

Multiple communication and social networking applications were identified, including WhatsApp, Snapchat, Gmail, and Instagram. Associated user accounts and identifiers indicate ongoing communication and potential data exchange related conversation between the suspects.



7.4.3 File and Application Analysis

communication applications were present on all devices. These applications provide mechanisms for data storage, transfer, and concealment, supporting the likelihood of attempted data exfiltration.



7.4.4 Suspect Role Assessment

Based on initiation of communication and activity on the device, Emma is labelled as the main perpetrator. A bridge with Joe connecting the dots. Norman used various devices and sophisticated access techniques, suggesting receipt and retention of protected materials.

7.5. Conclusion

7.6 Recommendations

Increase access controls, improve monitoring, and pursue internal sanctions against Quantum Tech executives. If the intent behind their work becomes clear, then law enforcement should consider charges of corporate espionage, attempted data theft and potential possession of illegal digital content.

Conclusion

The importance of digital forensics is to help combat modern cyber and corporate crime by giving investigators the ability to reconstruct a timeline of events, establish patterns in suspicious behavior and allow high quality digital evidence to be presented in court. This coursework shows that the delivery of effective forensic investigations relies on more than technology, rather making effective use of defined procedures and forensic principles along with sound evidence handling practices.

Professional tools (Cellebrite UFED and Cellebrite Physical Analyzer) recognized communications trends, social interactions and device-derived artefacts that pointed to coordinated acts by those involved in the investigation. The use of cryptographic hashes to verify the evidence allows it to also be completely repeatable and could, if required, make the evidence admissible in a court. The conciliation of theory with analytical practice overall underlines the significant role for professional judgement, verified approaches and lucid documentation, and evidences the significance of digital forensics in broader organizational security contexts and fostering legal accountability.

References

- [1] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," NIST SP 800-86, 2006.
- [2] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd ed. Academic Press, 2011.
- [3] P. Salunkhe, S. Bharne and P. Padiya, "Data analysis of file forensic investigation," 2016 *International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, Paralakhemundi, India, 2016

- [4] Sahib, S. Mapping process of digital forensic investigation framework. IJCSNS
- [5] Garfinkel, S.L., 2010. Digital forensics research: The next 10 years. digital investigation, 7,
- [6] N. Soni, "Digital Forensics: Confronting Modern Cyber Crimes, Technological Advancements, and Future Challenges," Journal of Forensic Legal & Investigative Sciences, 2025.
- [7] A. W. Malik et al., "Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges," Sensors, vol. 24, no. 2, 2024.
- [8] Choo, K.K.R., 2021, November. Internet of things (iot) security and forensics: Challenges and opportunities. In *Proceedings of the 2th Workshop on CPS&IoT Security and Privacy* .
- [9] K. M. Salih and N. B. Ibrahim, "Digital Forensic Tools: A Literature Review," Journal of Education and Science, vol. 32, no. 1, pp. 109–124, 2023.
- [10] Mulaudzi, I. and Venter, H.S., November. Using Artificial Intelligent Techniques. - 2025,
- [11] K. Ghazinour, D. M. Vakharia, K. C. Kannaji and R. Satyakumar, "A study on digital forensic tools," 2017
- [12] Agboola, V., Osamor, J. and Olajide, F., 2024. Evaluating the Efficiency of FTK, Autopsy, and Mobile Forensic Tools: A Comparative Study in Criminal Investigations. *International Journal of Intelligent Computing Research*.
- [13] B. Carrier and W. Brian, The Sleuth Kit & Autopsy Forensic Browser, 2024.
- [14] I. Ismail and K. A. Z. Ariffin, "The Admissibility of Digital Evidence from Open-Source Forensic Tools," PLOS ONE, vol. 20, no. 9, 2025.
- [15] H. Diwaker, "Comparative Analysis of Commercial and Open-Source Digital Forensic Tools," IIRCJ, 2025.