

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

ACCA7031 LON ASSESSMENT

Digital Forensics Analysis

Habibur Rahman | 2428138

To

Dr. Mohamed Ghanem

Submission Date: 28/04/2026

Table of Contents

Table of Figures	4
1 Abstract	6
2 Introduction	6
3 Literature Review	6
4 Task 1	6
4.1 Topic Selection	6
4.1.1 What the Field Actually Covers	6
4.1.2 The Main Subfields	7
4.1.3 The Tools	7
4.1.4 Typical Forensic Workflow	8
4.1.5 How the Evidence Landscape Has Shifted	8
5 Task 2	8
5.1 Evidence Acquisition	8
5.1.1 Acquisition Process	8
5.1.2 Hash Verification	24
5.1.3 Chain of Custody Documentation	26
5.1.4 Scope and Limitation of Available Evidence	35
5.2 Communication Analysis	36
5.2.1 WhatsApp Analysis (Emma ↔ Joe)	36
5.2.2 Facebook Analysis (Norman Smith ↔ Peter Dover)	42
5.2.3 User Directory Conversation Analysis	44
5.2.4 Instagram DM Analysis	45
5.2.5 Possible Alias Analysis (Peter Dover)	47
5.2.6 Timeline Reconstruction	48
5.2.7 Key Discussions	50
5.3 File Analysis	51
5.3.1 Emma's USB Flash Drive Examination	52
5.3.2 QT-AI-2025 Patent Files (PDFs, CAD designs)	52
5.3.3 File Metadata Analysis	52
5.3.4 Additional Evidence Files	52
5.3.5 Smartphone File Artefacts	52

5.4	Call Log and Email Correlation	53
5.4.1	Call Log Cross-Reference	53
5.4.2	Email Exchange Analysis	54
5.5	Suspect Profiling	54
5.5.1	Emma (Perpetrator)	54
5.5.2	Joe (Intermediary)	54
5.5.3	Norman (Buyer)	55
5.5.4	Vanessa (Suspected Buyer)	55
5.5.5	Additional Supporting/Refuting Evidence	55
5.6	Forensic Report	55
5.6.1	Case Background	55
5.6.2	Evidence Inventory	56
5.6.3	Methodology	56
5.6.4	Findings	56
5.6.5	Conclusion	57
5.6.6	Recommendations	57
6	Overall Conclusion	57
7	References	58

Table of Figures

Table 1: Chain of Custody log	35
Table 2: Timeline Reconstruction	48
Table 3: Evidence Inventory Table	56
Figure 1: Digital Forensic Model Comprising	8
Figure 2: Phone Extraction	9
Figure 3: Cellebrite UFED User Interface	10
Figure 4: Cellebrite UFED Case Details	11
Figure 5: Cellebrite UFED Choose Action Interface	11
Figure 6: Cellebrite UFED Detect Device Interface	12
Figure 7: Cellebrite UFED Connect Device Interface	13
Figure 8: Cellebrite UFED Extraction Type Interface	13
Figure 9: Cellebrite UFED Select Mode Interface	14
Figure 10: Cellebrite UFED Extraction Progress Interface	15
Figure 11: Cellebrite Physical Analyzer Interface	16
Figure 12: Cellebrite Physical Analyzer Interface	16
Figure 13: Cellebrite Physical Analyzer Interface	17
Figure 14: Cellebrite Physical Analyzer Interface	18
Figure 15: Cellebrite Physical Analyzer Interface	19
Figure 16: Cellebrite Physical Analyzer Interface	19
Figure 17: Cellebrite Physical Analyzer Interface	20
Figure 18: Four Images Interface	21
Figure 19: Selecting View All for more Data	21
Figure 20: AppGenie Interface	22
Figure 21: Selected Apps Shown in AppGenie	23
Figure 22: AppGenie Running Process	23
Figure 23: Hash Verification of Huawei Phone	24
Figure 24: Hash Verification of Nokia Phone	25
Figure 25: Hash Verification of Samsung Phone	25
Figure 26: Hash Verification of Note Phone	26
Figure 27: Ulefone Note 14 Extraction Details	27
Figure 28: Cellebrite Collection Summary of Ulefone Note 14	28
Figure 29: Samsung Extraction Details	29
Figure 30: Cellebrite Collection Summary of Samsung	30
Figure 31: Nokia Extraction Details	31
Figure 32: Cellebrite Collection Summary of Nokia	32
Figure 33: Huawei Extraction Details	33
Figure 34: Cellebrite Collection Summary of Huawei	33
Figure 35: Cellebrite Collection Summary of Huawei 2	34
Figure 36: WhatsApp Conversation Between Emma and Joe 1	36
Figure 37: WhatsApp Conversation Between Emma and Joe 2	37
Figure 38: WhatsApp Conversation Between Emma and Joe 3	37
Figure 39: WhatsApp Conversation Between Emma and Joe 4	38

Figure 40: WhatsApp Conversation Between Emma and Joe 5	38
Figure 41: WhatsApp Conversation Between Emma and Joe 6	39
Figure 42: WhatsApp Conversation Between Emma and Joe 7	39
Figure 43: WhatsApp Conversation Between Emma and Joe 8	40
Figure 44: WhatsApp Conversation Between Emma and Joe 9	40
Figure 45: WhatsApp Conversation Between Emma and Joe 10	41
Figure 46: Facebook Conversation between Norman and Peter 1	42
Figure 47: Facebook Conversation between Norman and Peter 2	43
Figure 48: User Directory Analysis	44
Figure 49: Instagram Analysis 1	45
Figure 50: Instagram Analysis 2	45
Figure 51: Instagram Analysis Hex Viewer	46
Figure 52: Recovered “Peter Dover” user account artefact	47
Figure 53: Sensitive Chats	47
Figure 54: Timeline Conversation Overview 1	49
Figure 55: Timeline Conversation Overview 2	49
Figure 56: Timeline Conversation Overview 3	50
Figure 57: Patent Search	51
Figure 58: Patent Search 2	51
Figure 59: Call Logs	53
Figure 60: E-mail Analysis	54

1 Abstract

This report discusses digital forensics by combining theoretical knowledge with practical investigation. It reviews current forensic tools and methods and then applies them to a simulated corporate espionage case involving stolen patent data. The analysis shows how digital evidence can be used to reconstruct events, identify suspects, and support cybersecurity and legal actions.

2 Introduction

Digital forensics has existed since the 1980s, but the field has changed considerably since then. What once focused mainly on recovering deleted files from early storage devices in police laboratories has now developed into a broad professional discipline involving mobile devices, cloud environments, corporate networks, and digital evidence presented in courts across different countries [1]. The field continues to expand, both in its scope and in the level of technical skill required by investigators.

This examines the current state of digital forensics by looking at how discipline is organized, the tools commonly used by investigators, and the ways digital evidence has evolved in recent years. Understanding this is important for anyone entering the field, conducting investigations, or shaping policies related to digital evidence, because the work of digital forensics today is far more complex than it was in the past [2].

3 Literature Review

This paper focuses on two tasks. The first task explores a chosen area of digital forensics by reviewing key ideas, professional practices, and challenges discussed in existing literature. The second task builds on this knowledge by putting it into practice through a digital forensic investigation, in which seized devices are analyzed to reconstruct events and uncover evidence related to a simulated corporate espionage incident.

4 Task 1

Research on a digital forensic topic will be conducted here, addressing several important areas of the field from both academic and professional perspectives.

4.1 Topic Selection

In this section, the topic reviewed is the current state of digital forensics and the tools that are used in the field, including their features and capabilities

4.1.1 What the Field Actually Covers

Digital forensics, by its simplest definition, is the preservation, collection, and analysis of digital evidence in a manner that is legally competitive [3]. While these are simple steps, in practice, each of these can prove to be quite challenging. It traditionally meant identifying evidence, all of which may simultaneously be riding on a collection of sources (smartphones, cloud accounts, corporate servers, and even vehicle systems). To preserve that evidence, it needs to be done in a forensically sound way, suggesting processes that would survive legal challenge. The analysis stage is the one where most of the detective work happens, whilst the presentation stage deals with the step of clarifying a technical finding in such a way that it can be comprehended and relied upon by non-technical audiences.

Research trends in digital forensics indicate that the domains have extended to five significant subfields, such as Disk forensics, Mobile forensics, Memory forensics, and Cloud forensics [4]. Each of these areas has its own techniques, instruments, and increasing academic literature; Authors were primarily limited to disk and mobile forensics in the past, but all five forensic areas are combined into one area of interest within modern investigation.

4.1.2 The Main Subfields

One of the oldest and most common types of digital forensics is disk and computer forensics. The process primarily involves generating a virtual copy of the storage device (forensic imaging) to ensure that the original evidence remains intact. From there, investigators can analyze that snapshot for timestamps of deleted files, browsing history on the way up to the incident in question, system logs, and other digital remnants that might elucidate what broke down [5]. For many years, this application has been a fundamental part of forensic investigations and is currently the basis for many of the more specialised aspects of the field.

With the prevalence of smartphones that are used for communicating and storing files for personal activities, mobile forensics is an entirely new paradigm that has rapidly gained importance. Utilizing iOS and Android devices, encrypted information, app-based records, as well as cloud-related information that might not even be preserved on the phone itself [6]. investigators function in this domain. Mobile devices often contain messages, photographs, location tracking information, and financial details [6]. Making them one of the most important sources of digital evidence but will also require being dealt with carefully due to privacy and legal implications.

Network forensics is centred on monitoring and analysing network traffic to identify suspicious or unauthorised activity. Notably, evidence related to malicious activity can often be buried in multiple packet captures and network logs across a network, but not residing on any one single device, which is essential when dealing with malware, data exfiltration, or unlawful access-based investigations [7]. On the other hand, memory forensics is the process of analyzing data that was contained in a system's RAM when an incident took place. Active processes, encryption keys, open connections, and some malware types may also disappear when the system is powered off [8]. Despite being technically complex, this type of analysis frequently uncovers critical evidence that cannot be obtained from persistent storage [8].

Cloud forensics is a relatively new domain in the field and probably one of the most difficult as well. As organisations have turned to platforms like AWS, Azure, and Google Cloud, this means that a great deal of their digital evidence now sits in environments that investigators cannot physically access [9]. It also poses new technical and legal challenges, but has made cloud-based investigations more critical than ever. This growth in the market for cloud forensic skills and services is also reflected by recent research [9].

4.1.3 The Tools

The tools utilized in digital forensics can now typically be divided into two types: business options created for expert investigations and open-source options used for a great deal more general jobs, training, or mission teams with limited funds.

Of the commercial tools, Cellebrite UFED is well known for mobile device extraction. It works with numerous types of devices and performs deleted data, application content, and cloud-related evidence recovery [10]. Magnet AXIOM is more extensive, being able to acquire and critically analyze data from a computer, mobile devices, cloud account, and even vehicles in a single case [11]. Partial information or a framework for merging among multiple data sources is very important because it helps identify element links between them and consolidate evidence from unrelated sources [11]. As a common forensic tool, EnCase is one of the oldest computer forensics tools available. The tool is best known for disk imaging, keyword searching, and being useful in corporate investigations and legal discovery work [12].

Open-source tools also have a significant role in forensic investigations! Autopsy is one of the open-source digital forensic tools that has gained popularity and can be widely utilized in disk image analysis, timeline creation, and file scanning [13]. Volatility is a well-known memory forensics tool that assists digital forensic investigators with analyzing processes, code injection, network connections, and rootkits from memory dumps. [8]. Wireshark is primarily a network

analysis tool and has remained a reliable software for analyzing in law and forcy with the packet traffic (in both cybersecurity investigations) [7].

Another important thing is that no tool can independently address all the evidence. In practice, however, investigators use a mix of tools tailored to each case. For instance, you may use one tool to capture disk or memory images, another to investigate mobile devices, and yet another to analyze network traffic or correlate evidence from different sources. Therefore, Digital forensic work often relies on a toolkit of methods and software rather than just one tool [13].

4.1.4 Typical Forensic Workflow

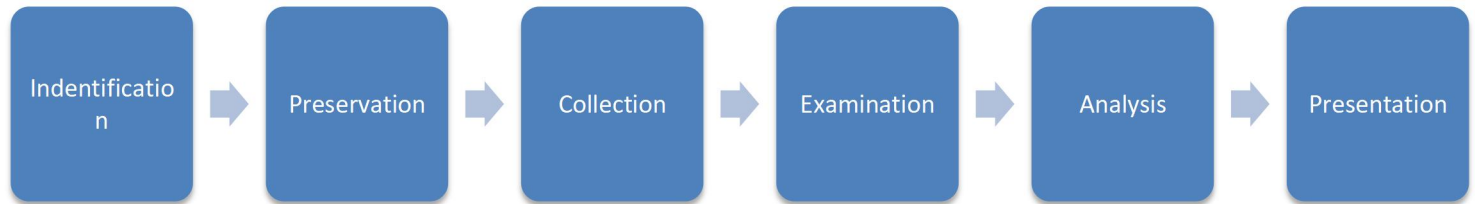


Figure 1: Digital Forensic Model Comprising

According to prior studies [1] In 2001, the Digital Forensic Research Workshop (DFRWS) proposed a seven- phase digital forensic process consisting of identification, preservation, collection, examination, analysis, presentation, and decision- making. Unlike earlier models, it formally incorporated activities conducted both before evidence acquisition and after analysis, particularly those related to legal proceedings. These phases are logically interconnected, with each stage building upon and influencing the outcomes of the others to ensure a reliable forensic investigation, as shown in Figure 1

4.1.5 How the Evidence Landscape Has Shifted

Digital forensic investigations have traditionally revolved around physical devices that could be seized, imaged, and analysed directly by investigators. While this is still done, it is no longer the only digital evidence source. An increasing proportion of evidence is now kept in cloud environments, which are not physically accessible to investigators and where data may be spread over servers in a number of different nations. In many cases, access to this information is bottlenecked by cloud service provider type, which has an impact on what data can be acquired and at what speed [14].

With the emergence of Internet of Things (IoT) devices, this matter has become more convoluted. IoT devices include gadgets like smartwatches, home assistants, connected automobiles, and industrial sensors, which generally hold forensic evidence; however, the varied hardware and software involved frequently make it significantly more challenging for investigators to analyze this evidence [2]. Studies demonstrate that the growth of Internet of Things (IoT) devices is set to accelerate, which is developing both the possible uses and technical challenges [2] . Moreover, legislative efforts like GDPR in Europe and the California Consumer Privacy Act impose further constraints on how digital evidence can be collected, stored, and utilized [1].

5 Task 2

Here, the focus is on investigating a simulated corporate espionage case involving the suspected theft and attempted sale of Quantum Tech’s confidential patent data using evidence collected from several digital devices.

5.1 Evidence Acquisition

5.1.1 Acquisition Process

Here, the forensic images of four phones were acquired, starting with the extraction process from each device and followed by analysis in Cellebrite Analyzer.



Figure 2: Phone Extraction

The following Figure 2 shows the process of extracting data from the phone for forensic acquisition.

After that, Cellebrite UFED was opened to perform mobile data extraction. As no screenshots of the original extraction process were available, a personal mobile device was used only to demonstrate the steps involved in the acquisition process.

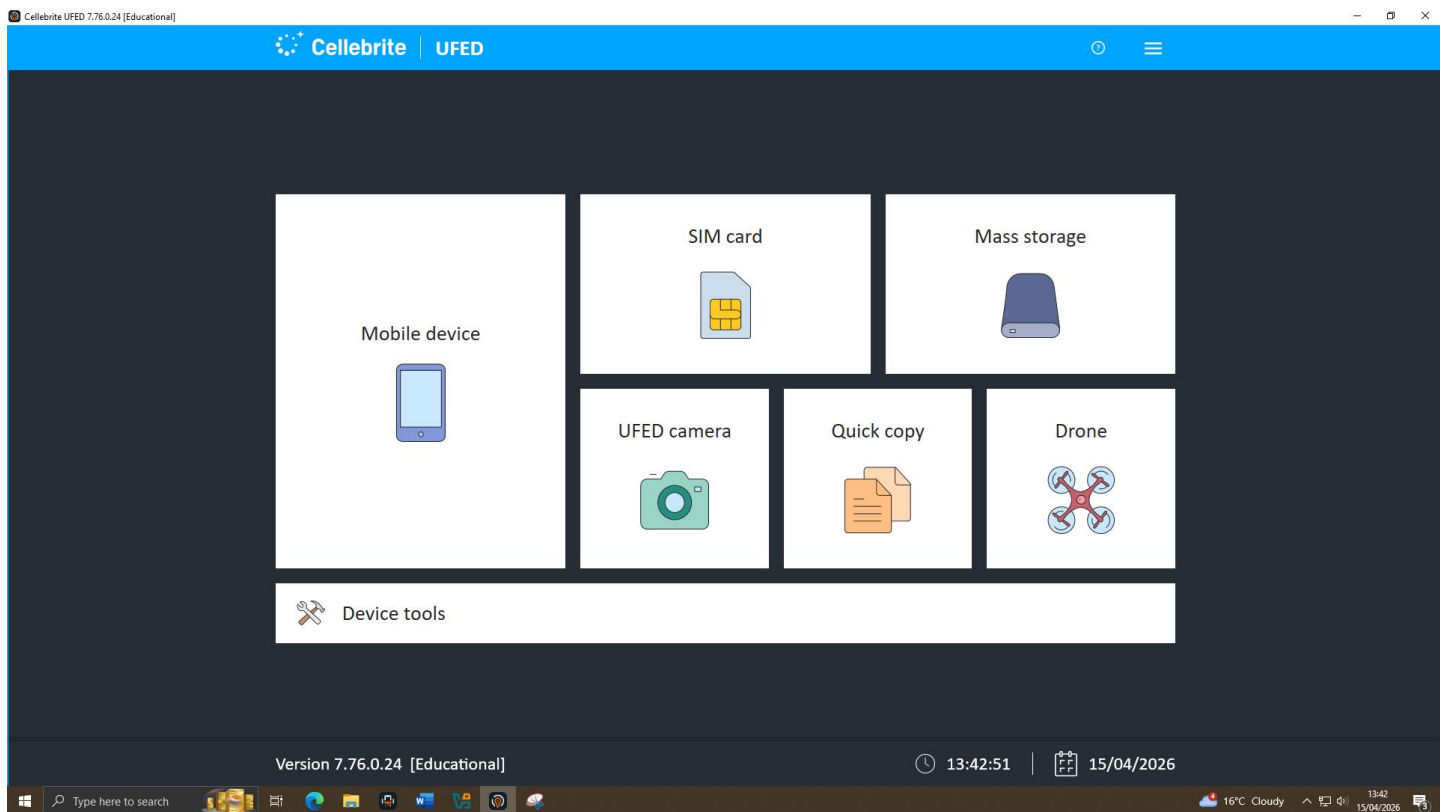


Figure 3: Cellebrite UFED User Interface

After opening Cellebrite UFED, the Mobile Device option was selected to begin the extraction process, as shown in Figure 3

Cellebrite UFED 7.76.0.24 [Educational]

CASE DETAILS

NEW CASE

Case Identifier
2428138

Examiner Name
Habibur Rahman

Device Name / Evidence Number
Samsung A22 5G

Crime Type
▼

Department
▼

Location
UWTSD London

ABORT BACK CONTINUE

Type here to search Masters of the Univer... 13:44 15/04/2026

Figure 4: Cellebrite UFED Case Details

The case details were documented for future investigation, as shown in Figure 4

Cellebrite UFED 7.76.0.24 [Educational]

CHOOSE ACTION

Smart Flow Details ▼

Auto Detect Details ▼

Search Devices Details ▼

Device Wizard Details ▼

ABORT BACK

Type here to search 16°C Cloudy 13:45 15/04/2026

Figure 5: Cellebrite UFED Choose Action Interface

The Auto Detect option was selected to identify the type of phone, its model, and version information automatically, as shown in Figure 5

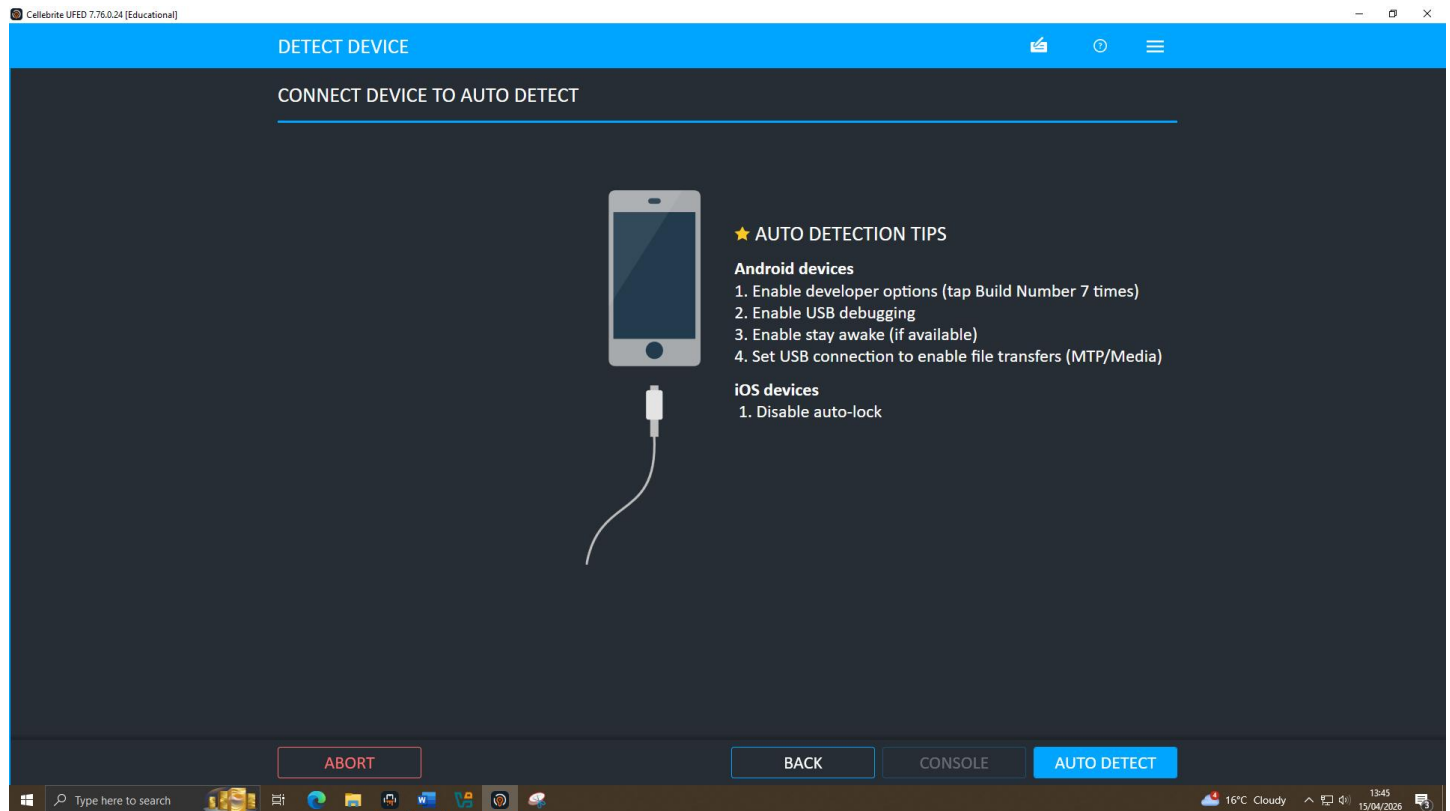


Figure 6: Cellebrite UFED Detect Device Interface

The Auto Detect function automatically identified the phone version and provided guidance for completing the extraction correctly, as shown in Figure 6.

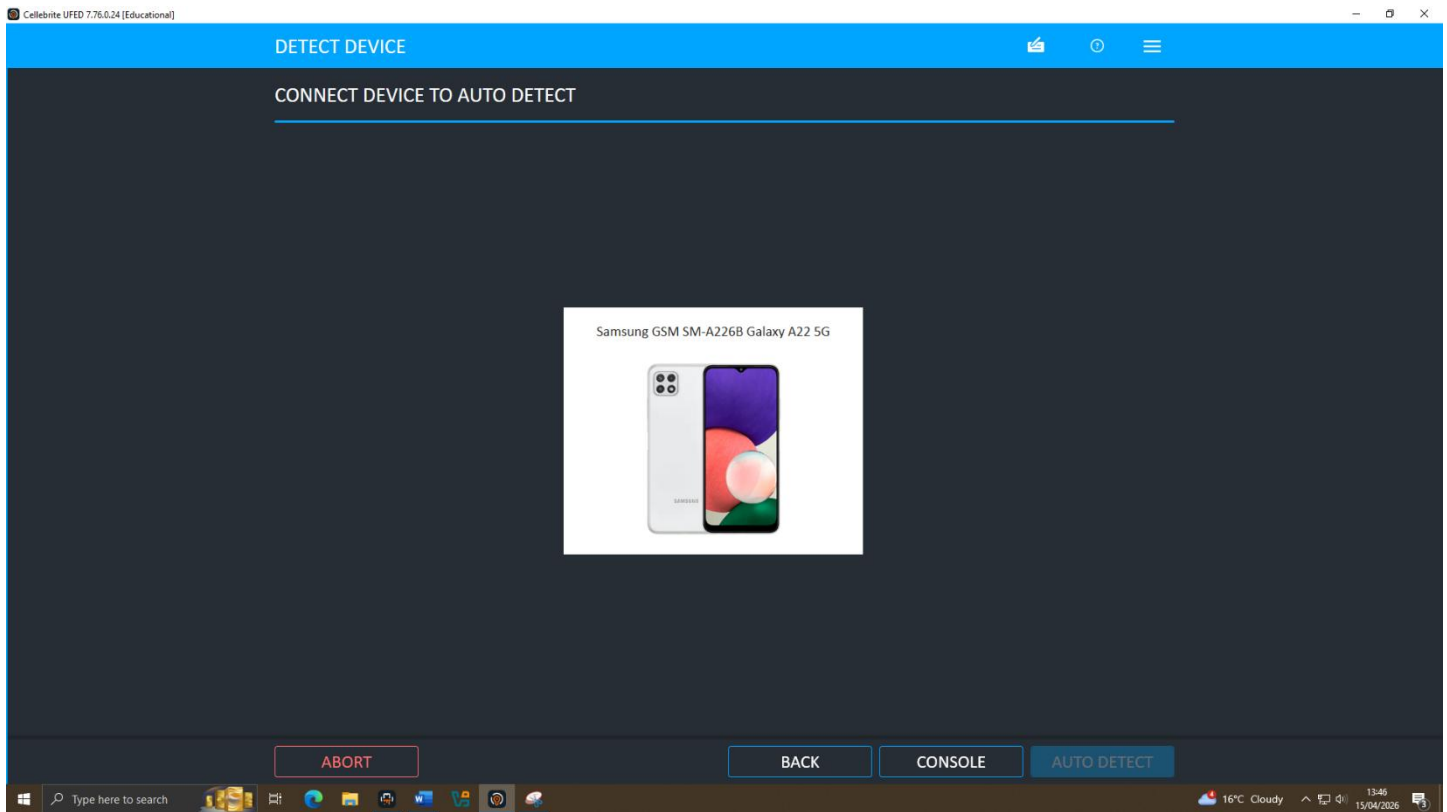


Figure 7: Cellebrite UFED Connect Device Interface

As a result, the device was automatically identified, and the detected phone was then selected for extraction, as shown in Figure 7

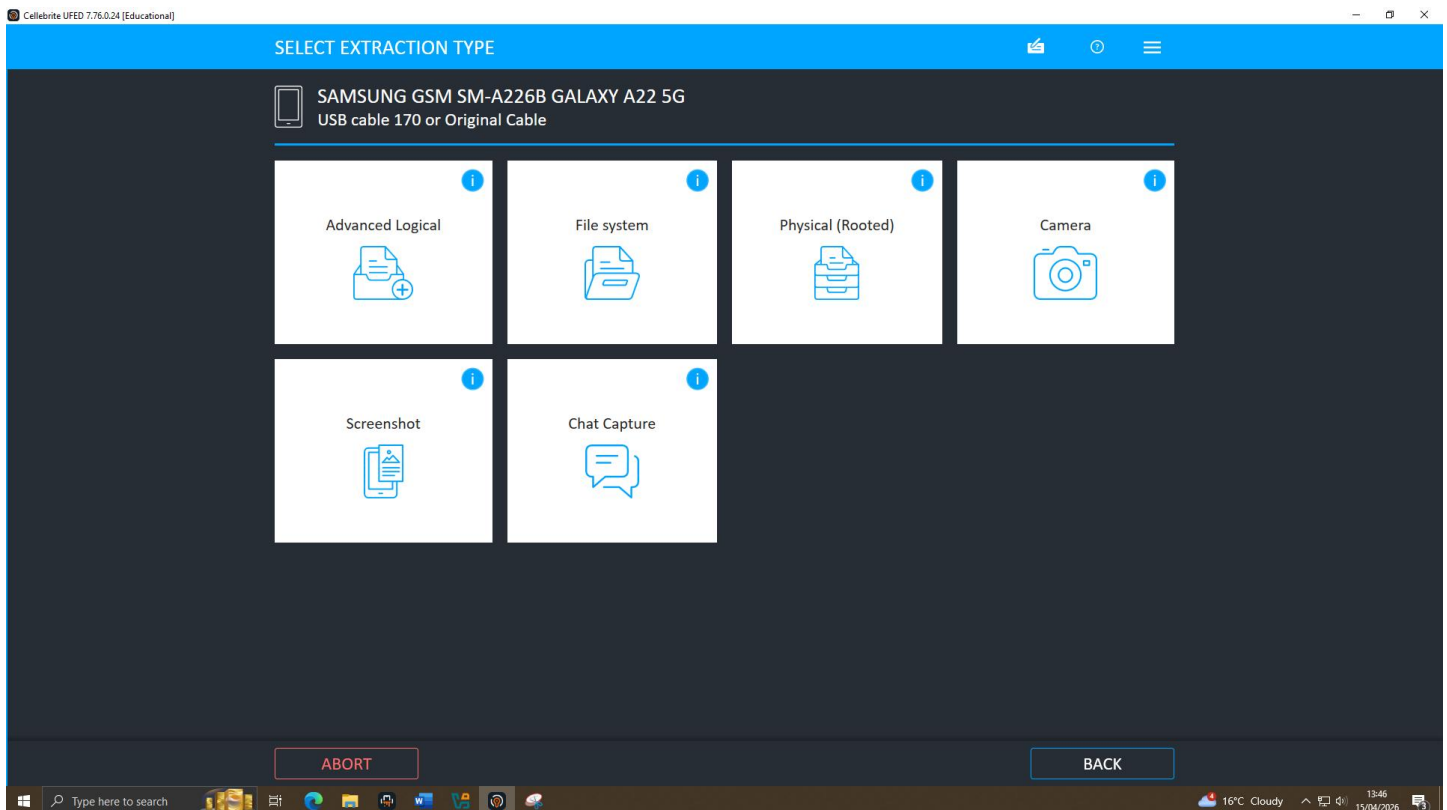


Figure 8: Cellebrite UFED Extraction Type Interface

Several extraction options were available, and for this process, the File System option was selected, as shown in Figure 8

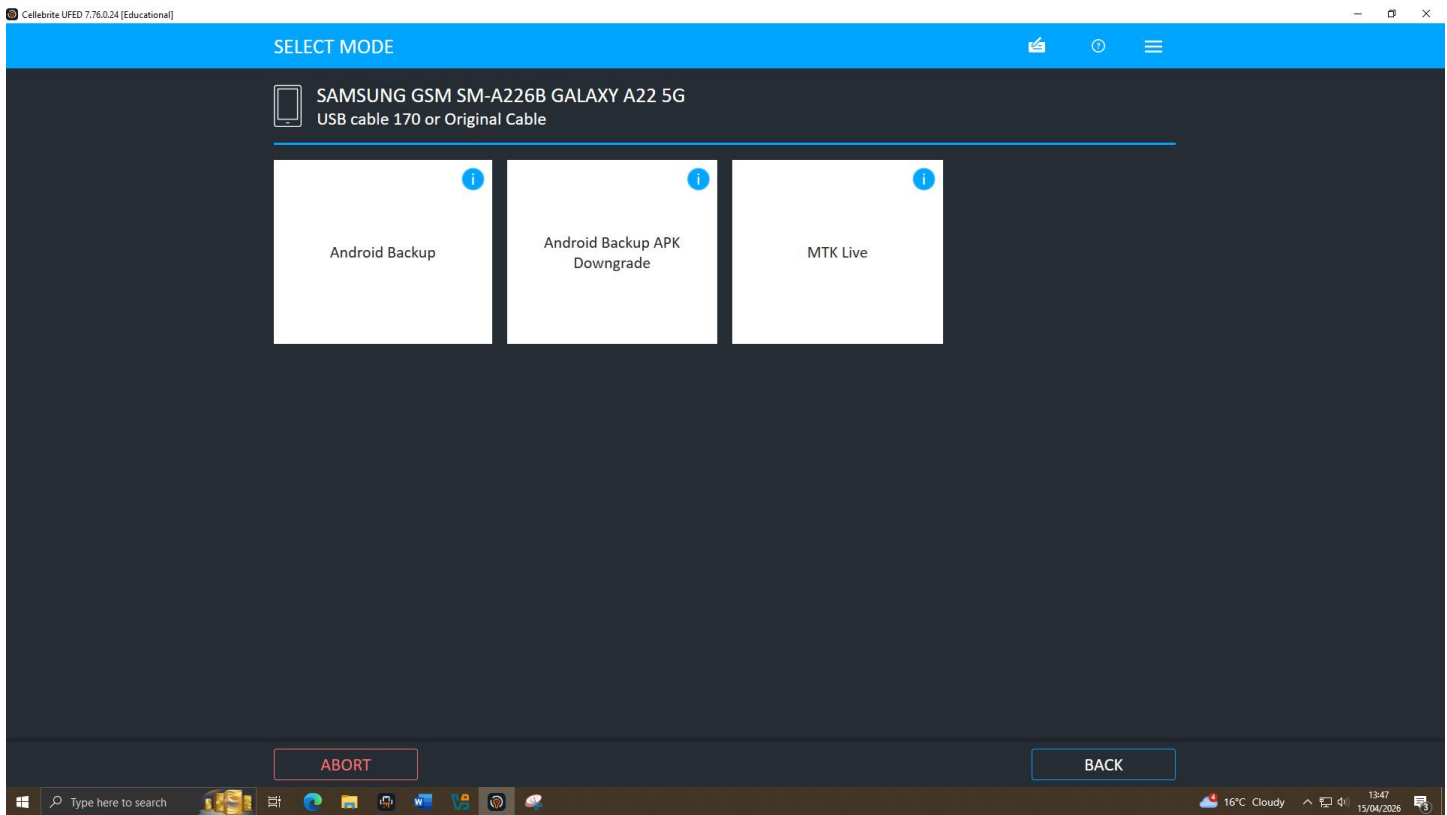


Figure 9: Cellebrite UFED Select Mode Interface

Several extraction modes were available, and the Android Backup mode was selected for this process, as shown in Figure 9

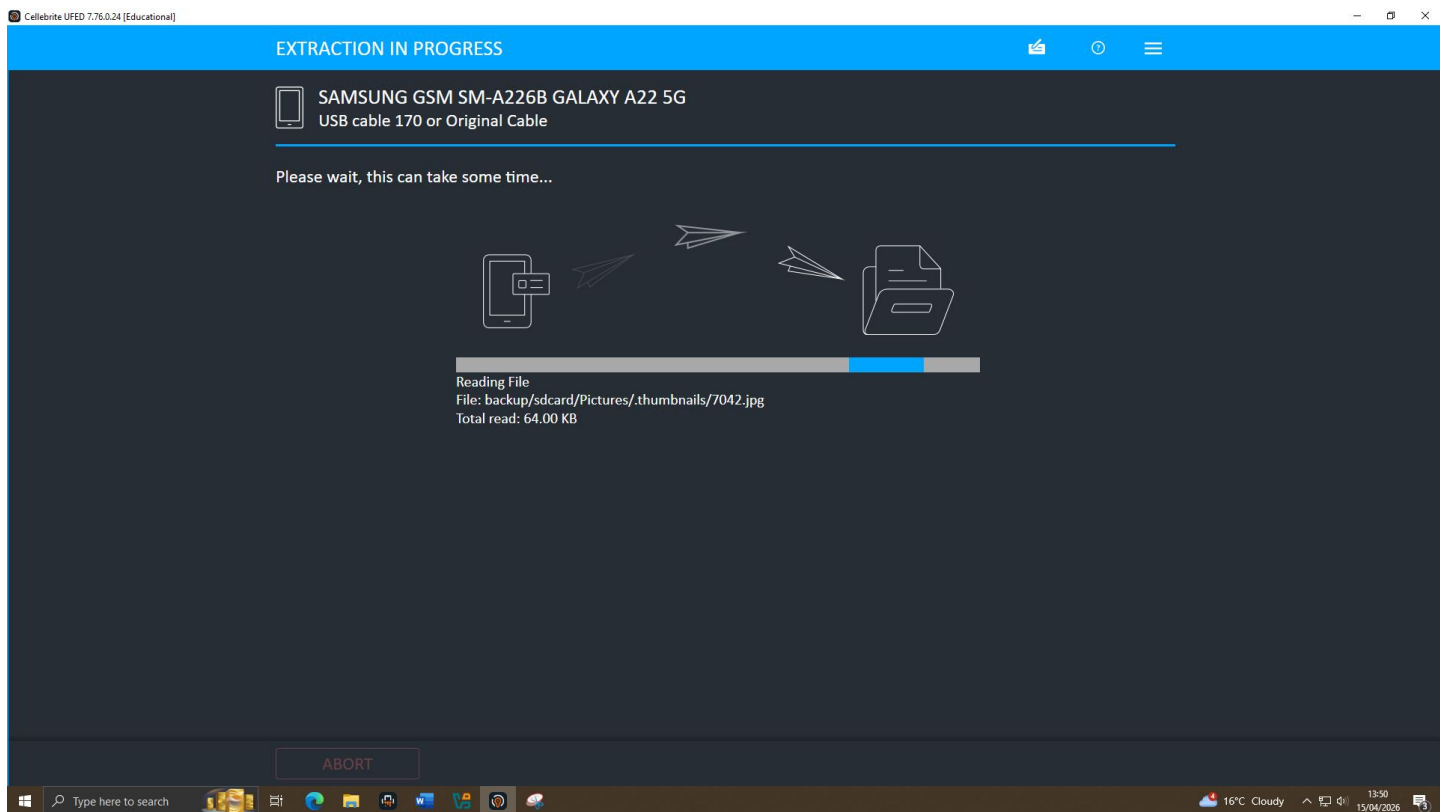


Figure 10: Cellebrite UFED Extraction Progress Interface

Finally, the extraction process was started, and the extracted data was obtained for further investigation, as shown in Figure 10

After the extraction was successfully completed, the acquired data was analyzed to support the investigation. For this purpose, the Cellebrite UFED Analyzer was opened to examine the extracted data.

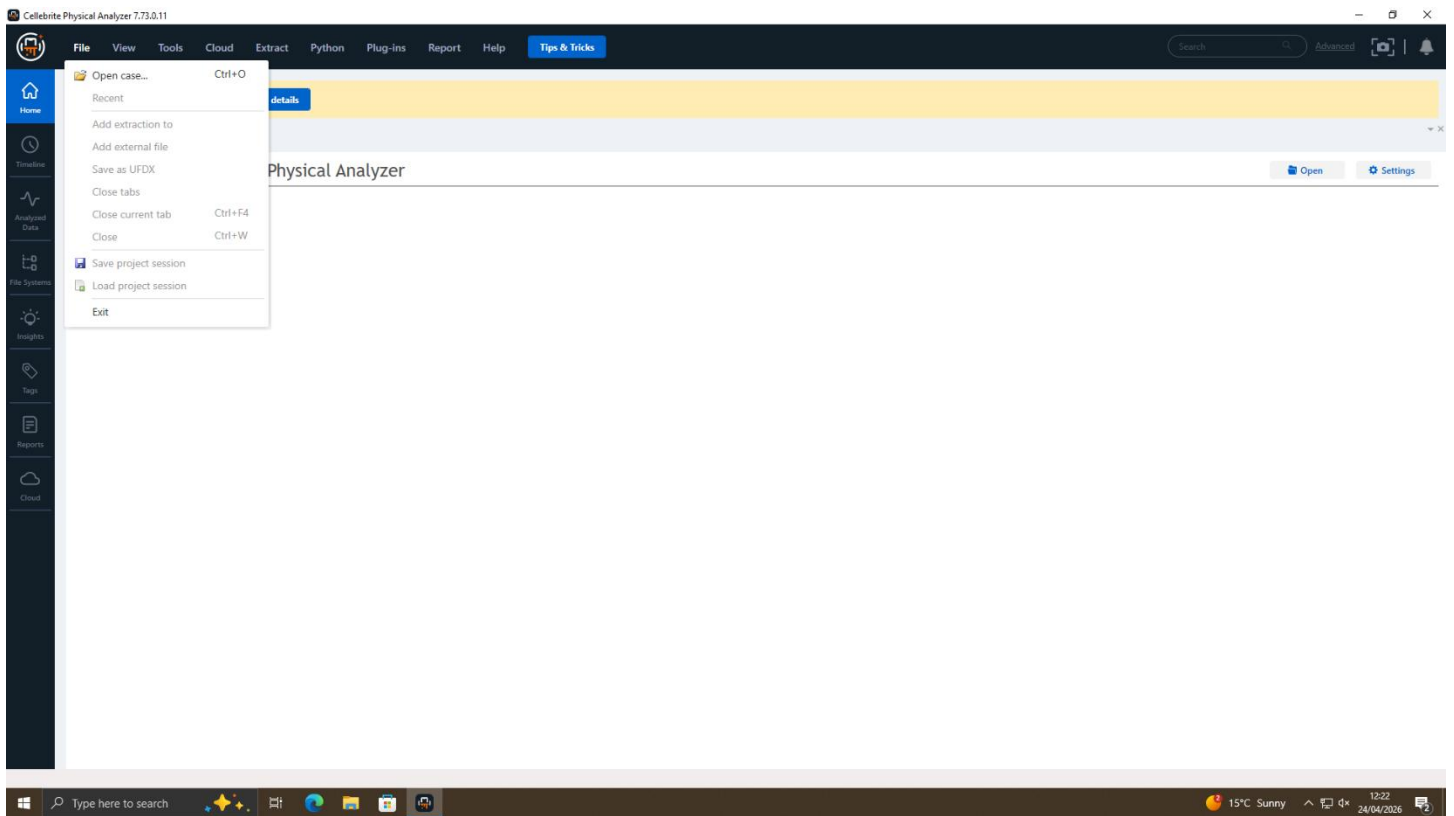


Figure 11: Cellebrite Physical Analyzer Interface

After opening Cellebrite Physical Analyzer, the Open Case option was selected to load the four extracted images into a single case for easier comparison and more effective investigation, as shown in Figure 11

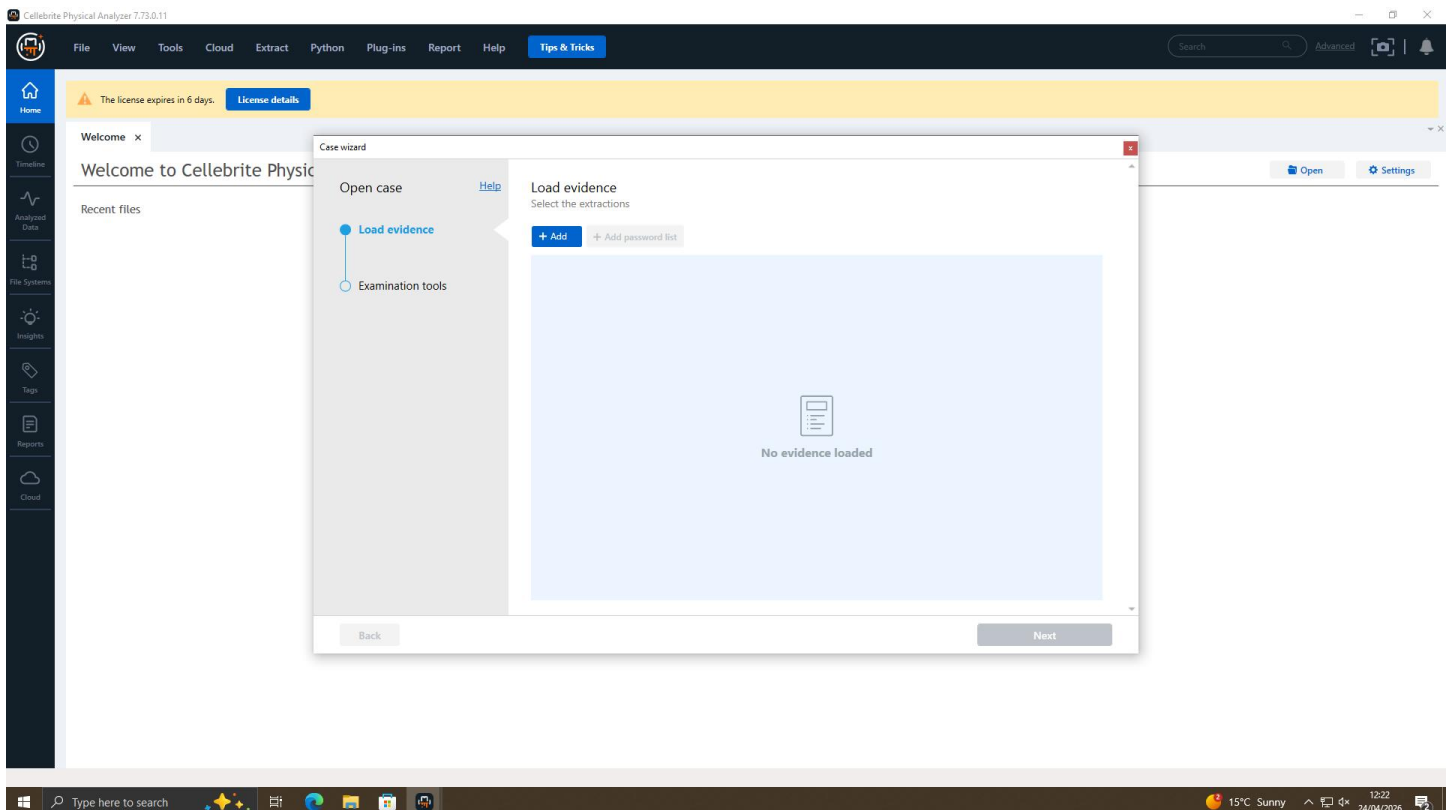


Figure 12: Cellebrite Physical Analyzer Interface

At this stage, the Load Evidence option was selected to add the extracted evidence files from the computer, as shown in Figure 12

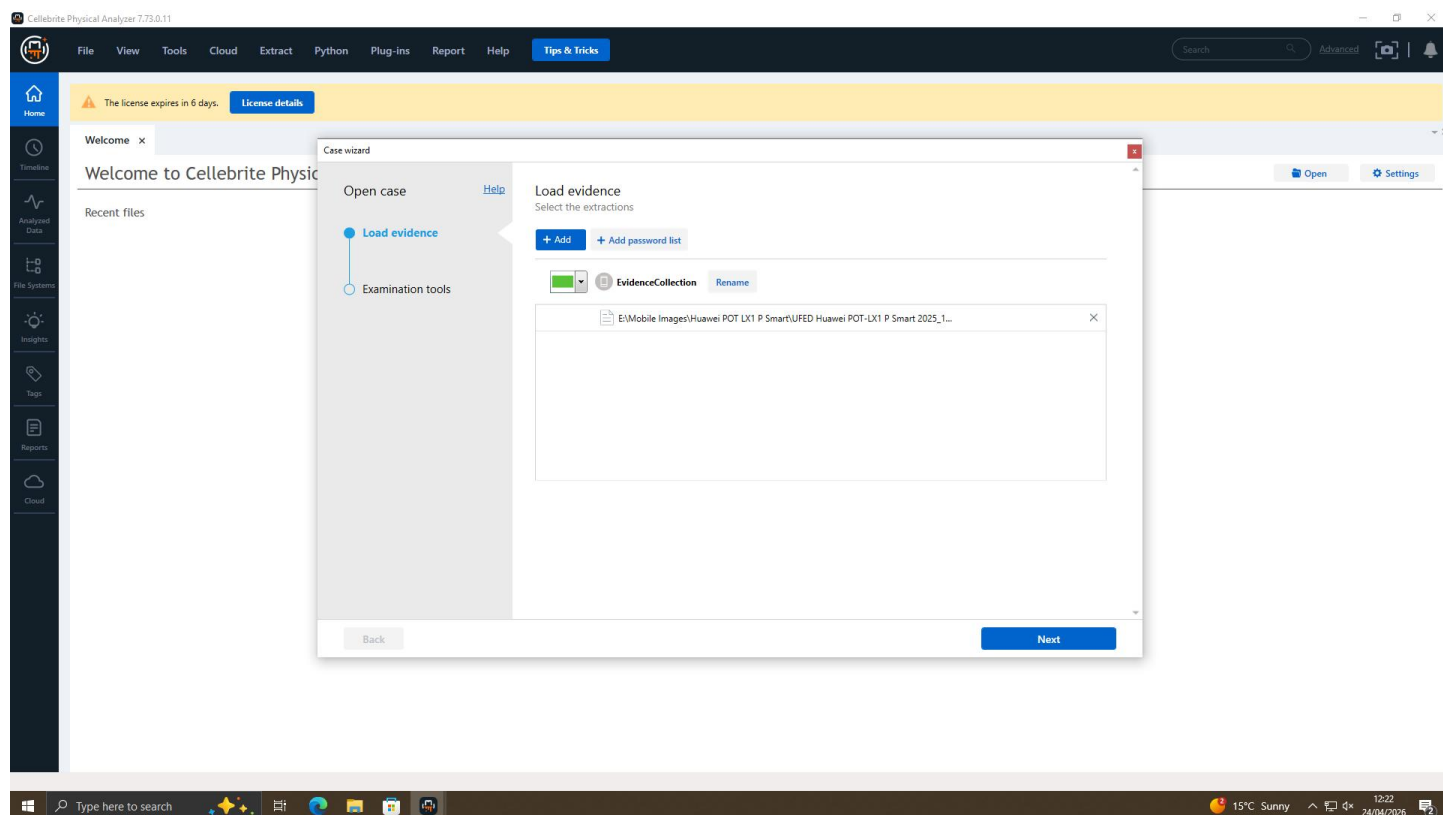


Figure 13: Cellebrite Physical Analyzer Interface

After the evidence was successfully loaded, the Next button was selected to continue the process, as shown in Figure 13

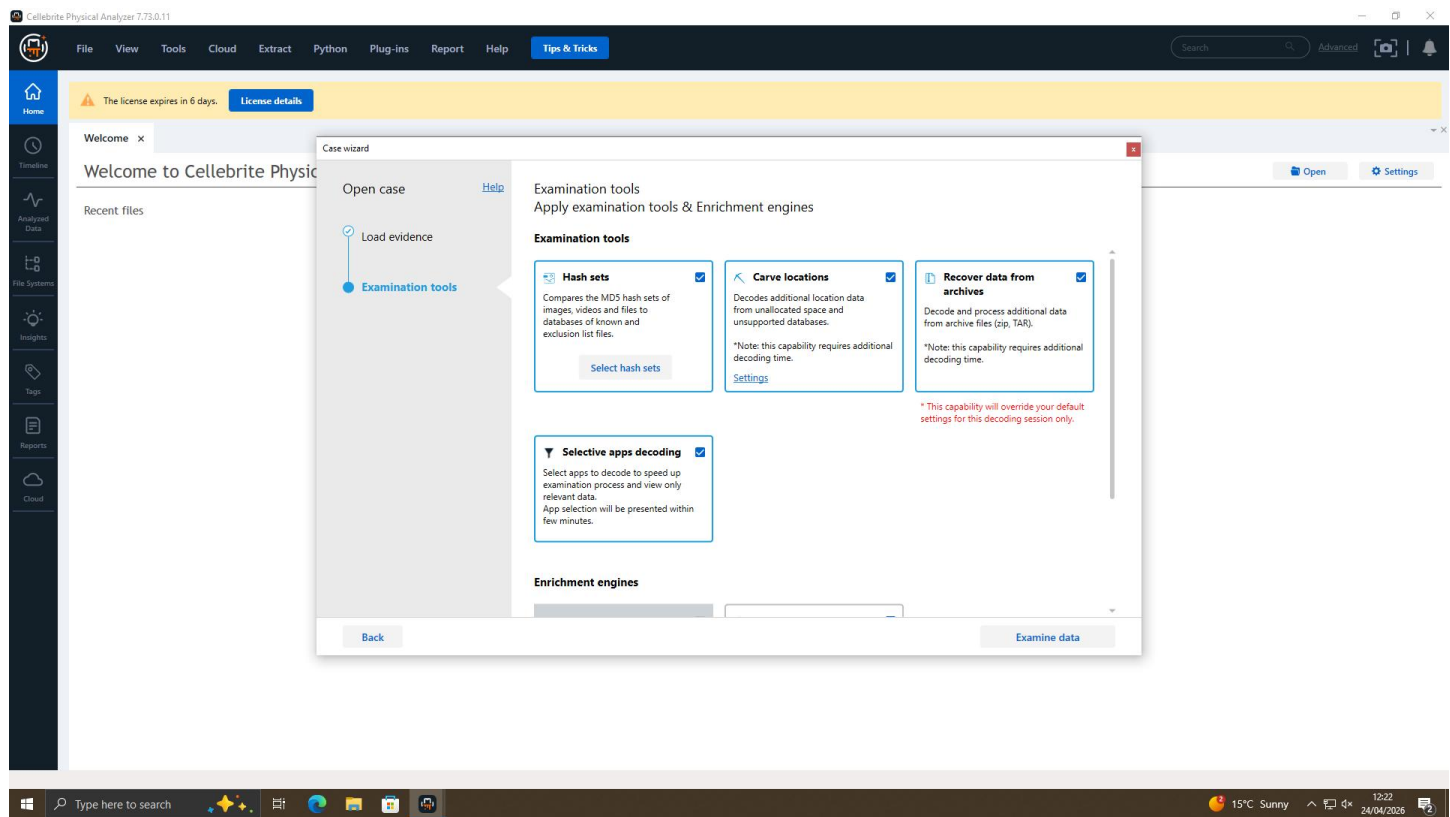


Figure 14: Cellebrite Physical Analyzer Interface

At this stage, only four options were selected: Hash Sets, Carve Locations, Recover Data from Archives, and Selective Apps Decoding, as shown in Figure 14

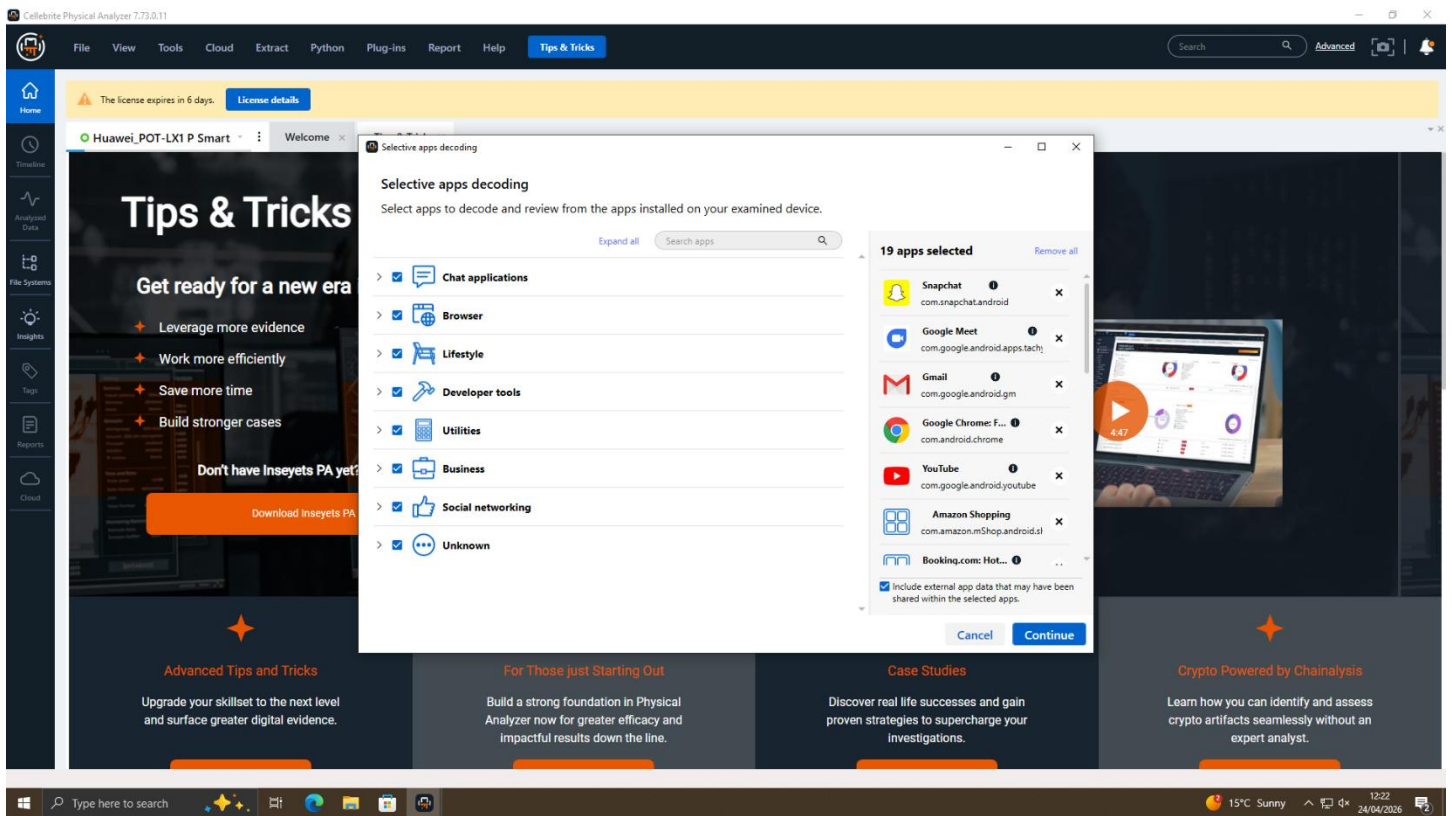


Figure 15: Cellebrite Physical Analyzer Interface

At this stage, all Selective Apps Decoding options were selected, and the process was continued by pressing Next, as shown in Figure 15

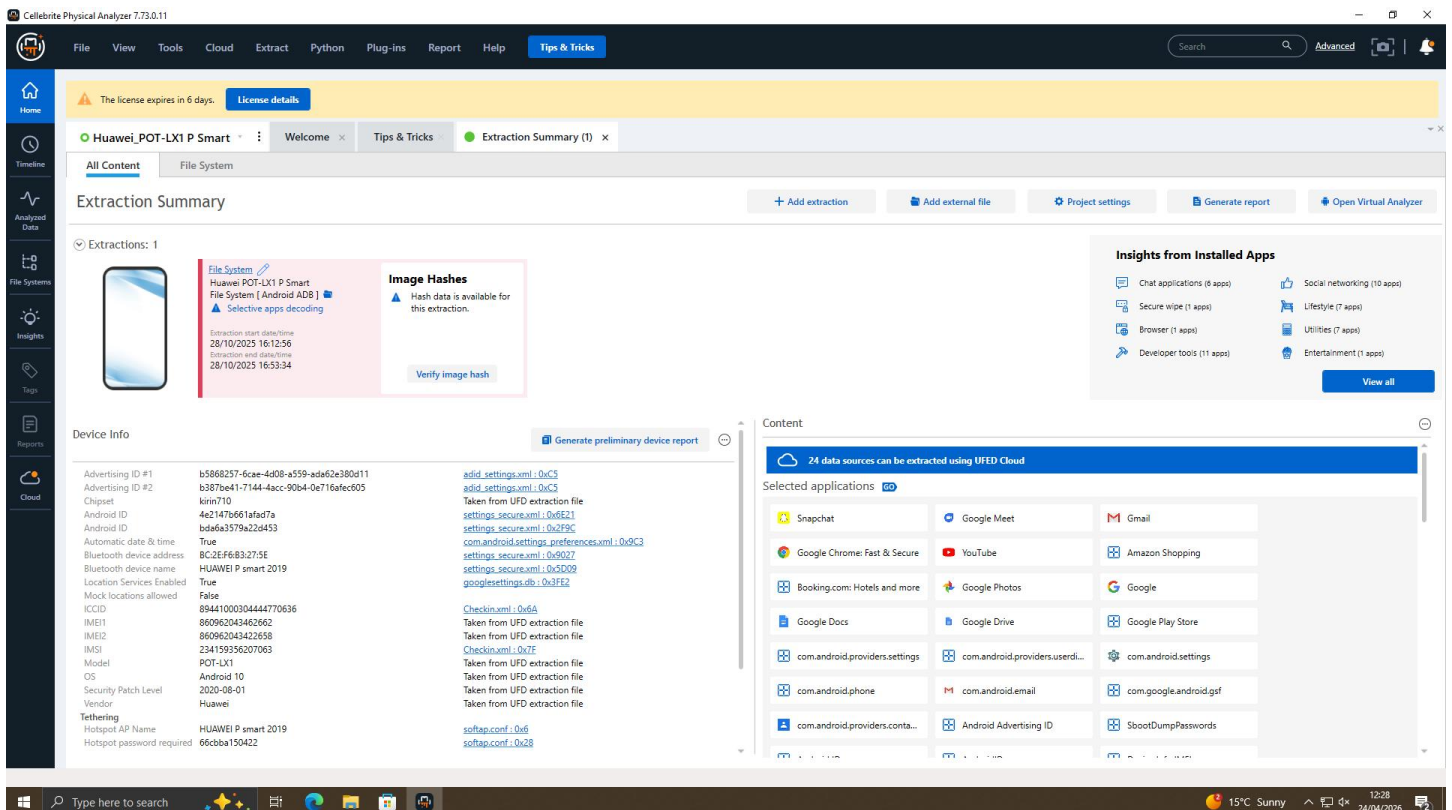


Figure 16: Cellebrite Physical Analyzer Interface

After all the required steps were completed successfully, the phone data output was displayed for analysis, as shown in Figure 16.

This process was completed for one phone image.

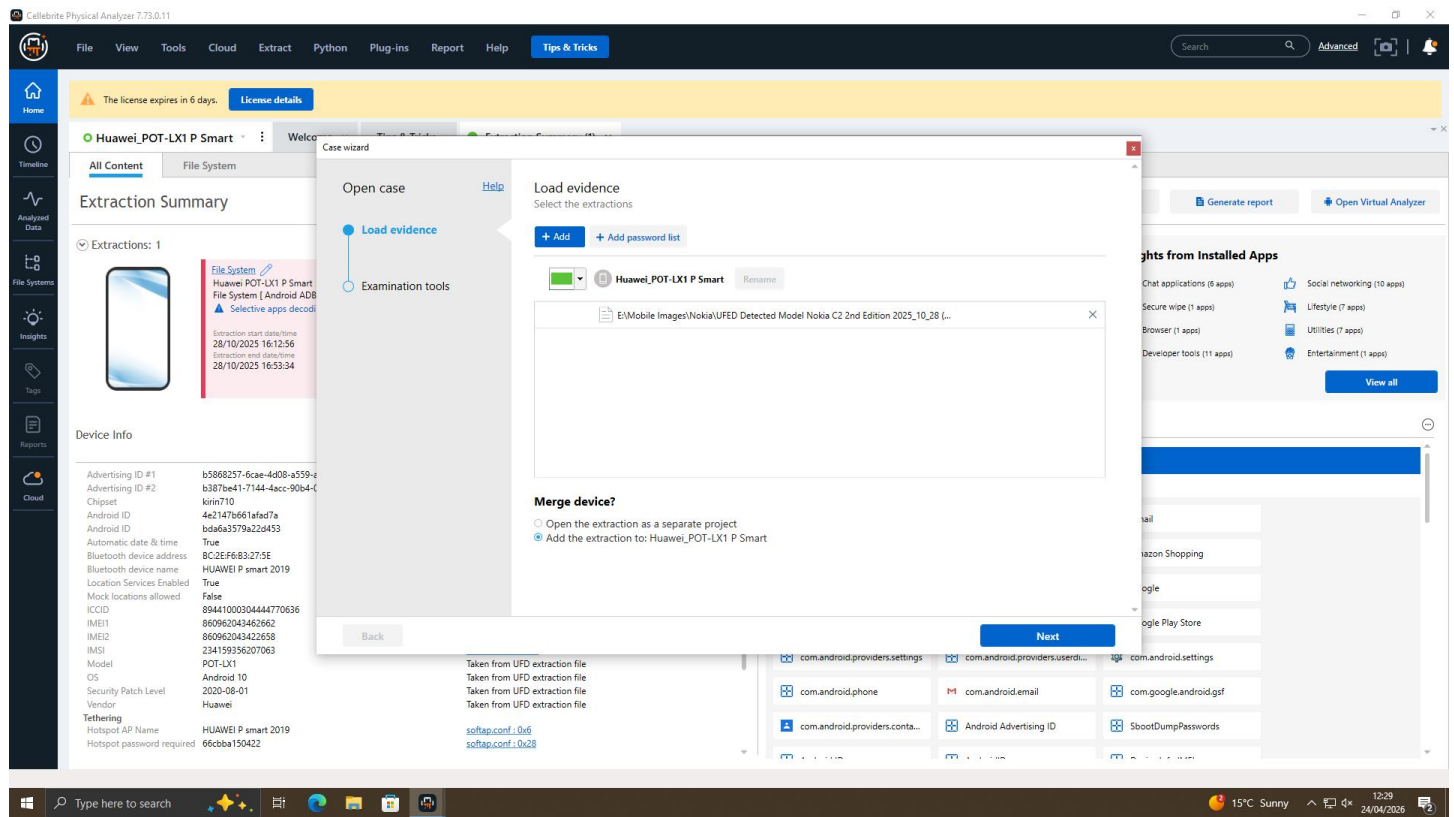


Figure 17: Cellebrite Physical Analyzer Interface

From the Files section, the Open Case and Load Evidence options were selected, and the same process as the previous step was followed. At the final stage, all four images were merged into a single case using the Merge option, as shown in Figure 17

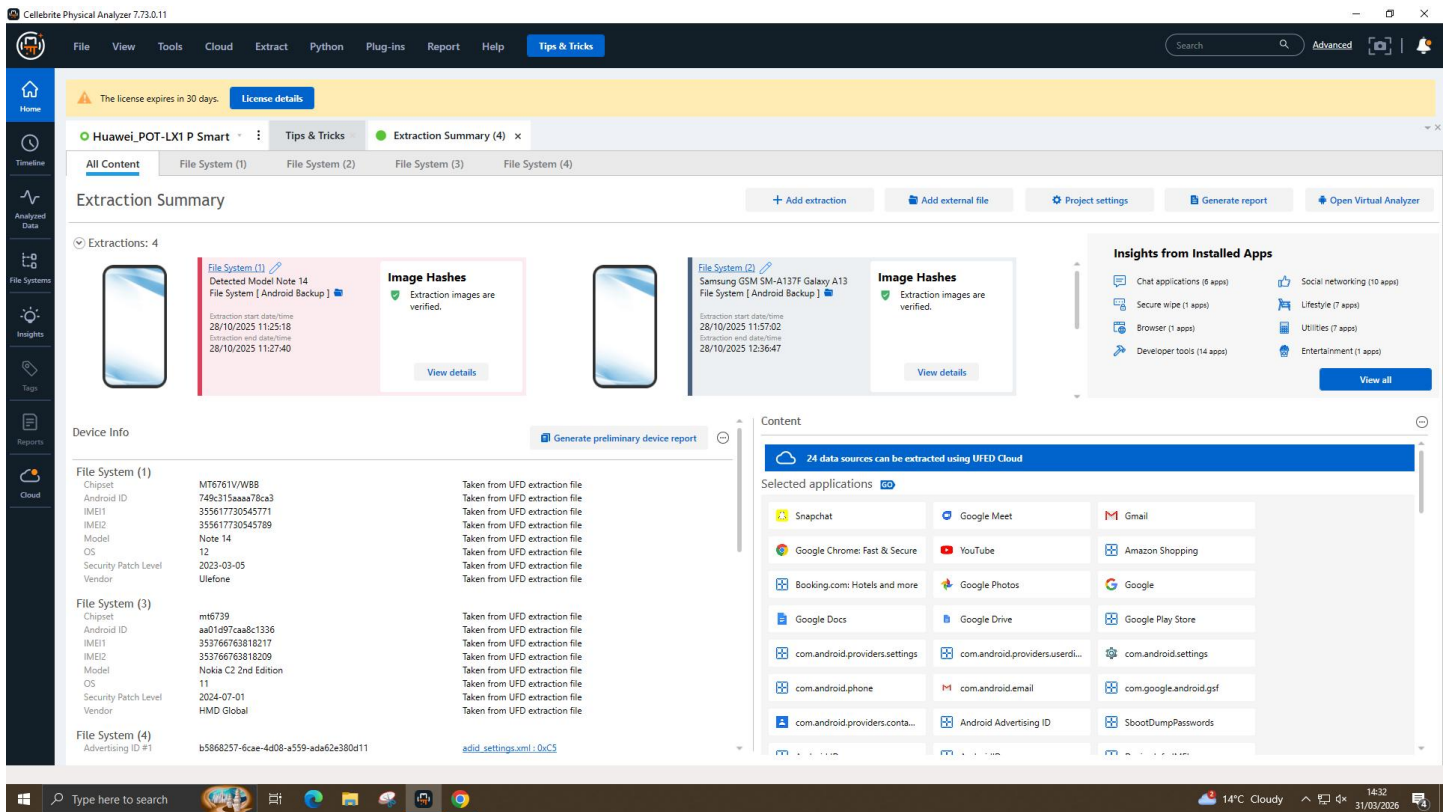


Figure 18: Four Images Interface

After the merging process was completed, the combined output was displayed in Cellebrite Physical Analyzer, as shown in Figure 18

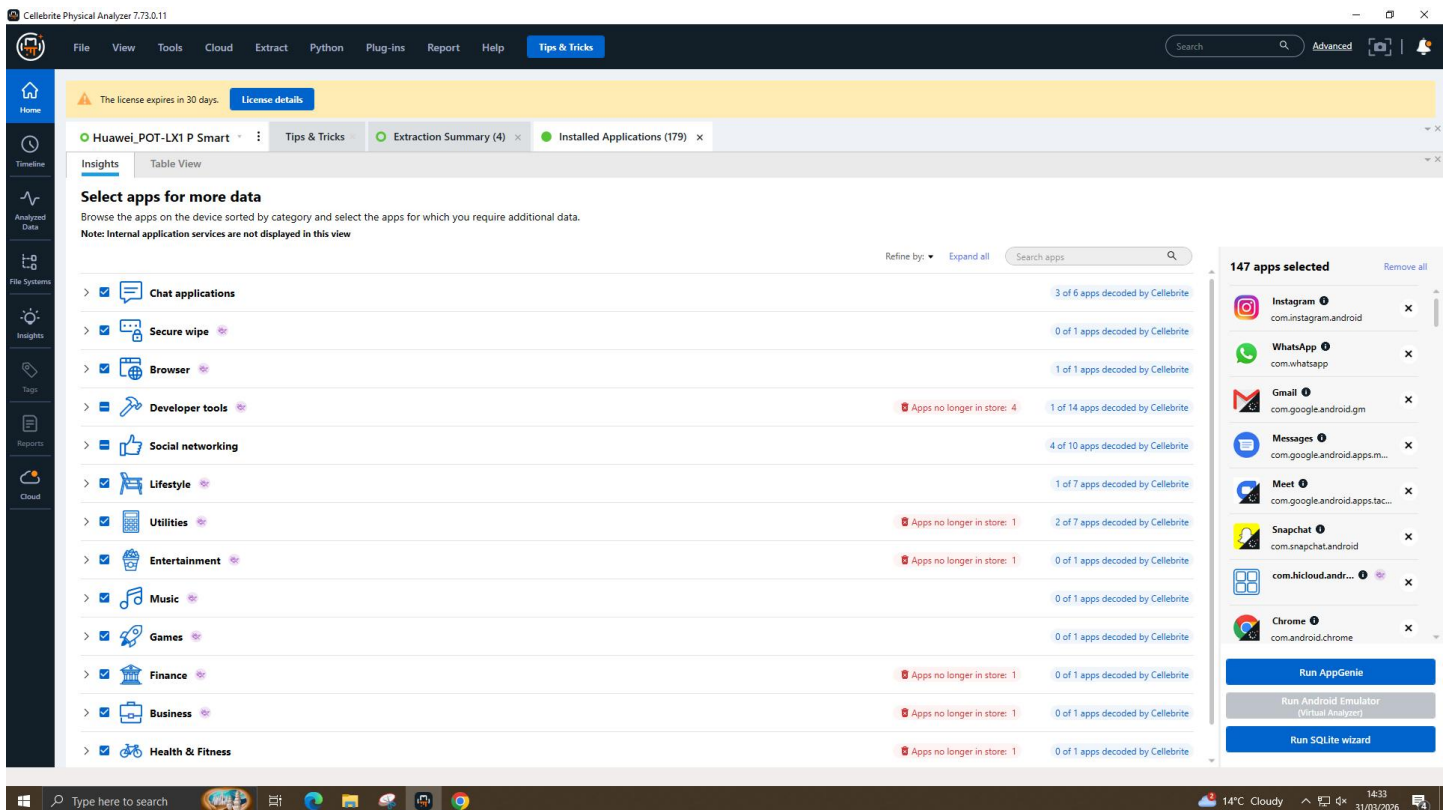


Figure 19: Selecting View All for more Data

The View All option was then selected, and all available applications were chosen to obtain more data before running App Genie, as shown in Figure 19

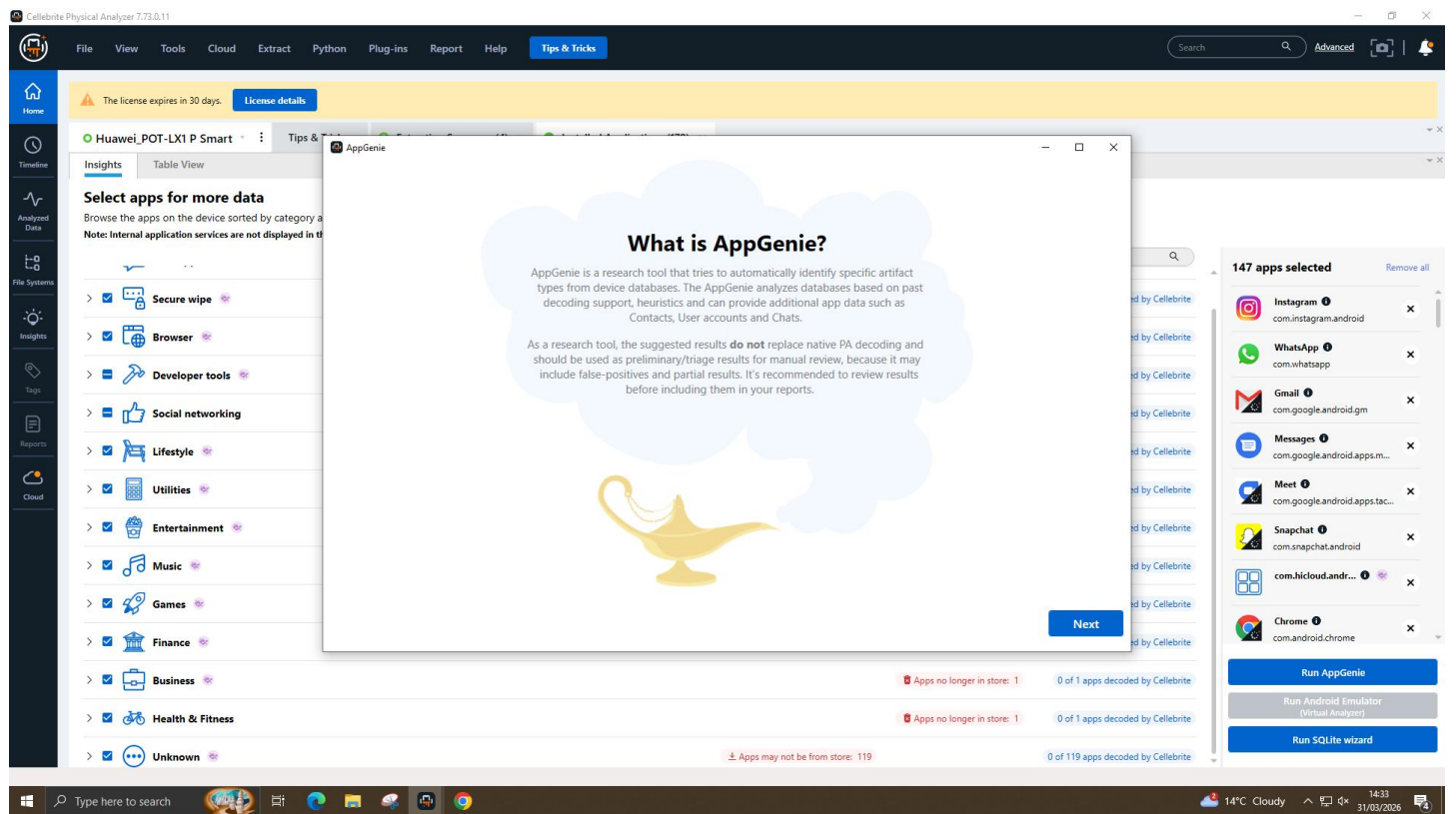


Figure 20: AppGenie Interface

After selecting all the available applications, App Genie was run to identify the supported apps and highlight the benefits of the analysis process, as shown in Figure 20

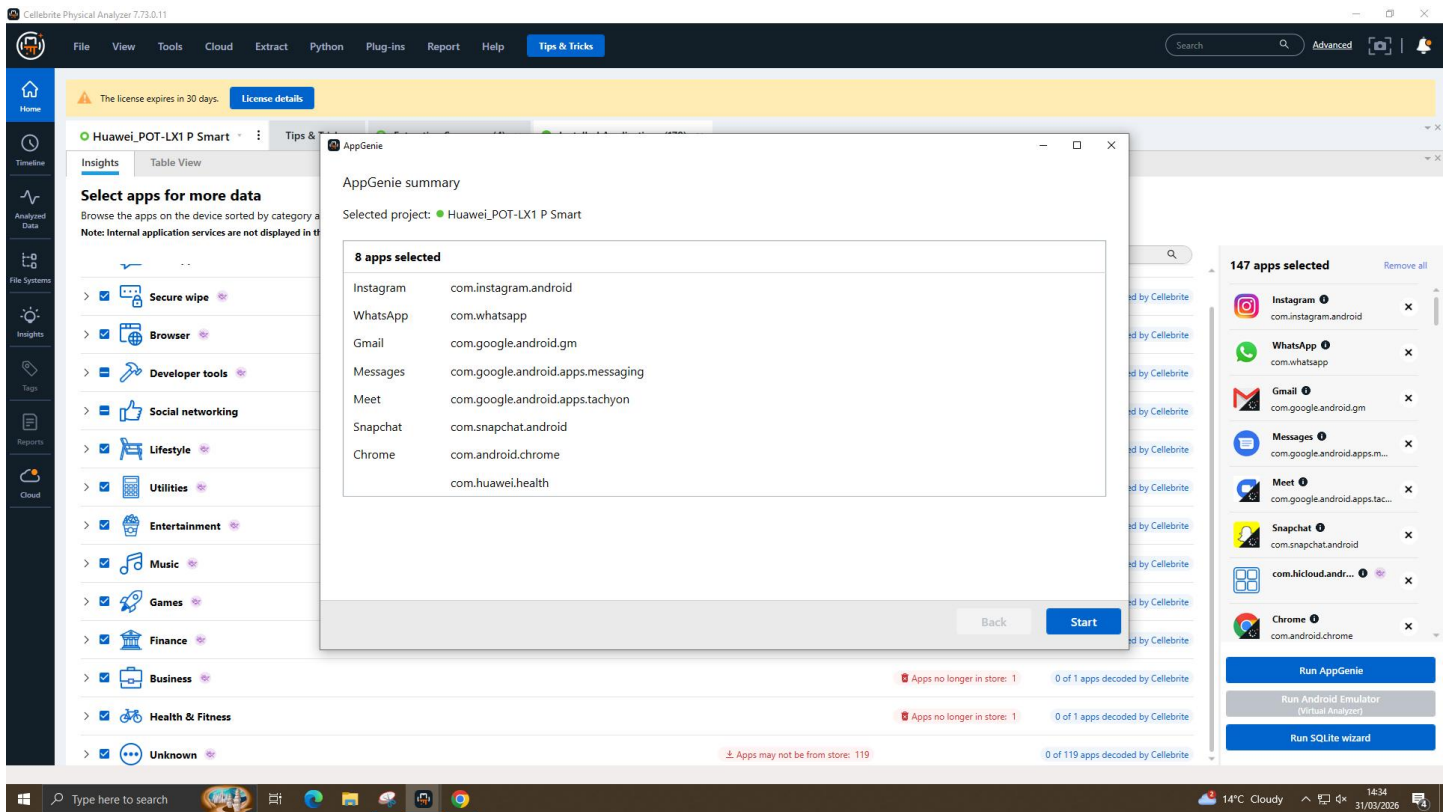


Figure 21: Selected Apps Shown in AppGenie

The App Genie summary was then displayed, and the Start button was selected to proceed with the analysis, as shown in Figure 21

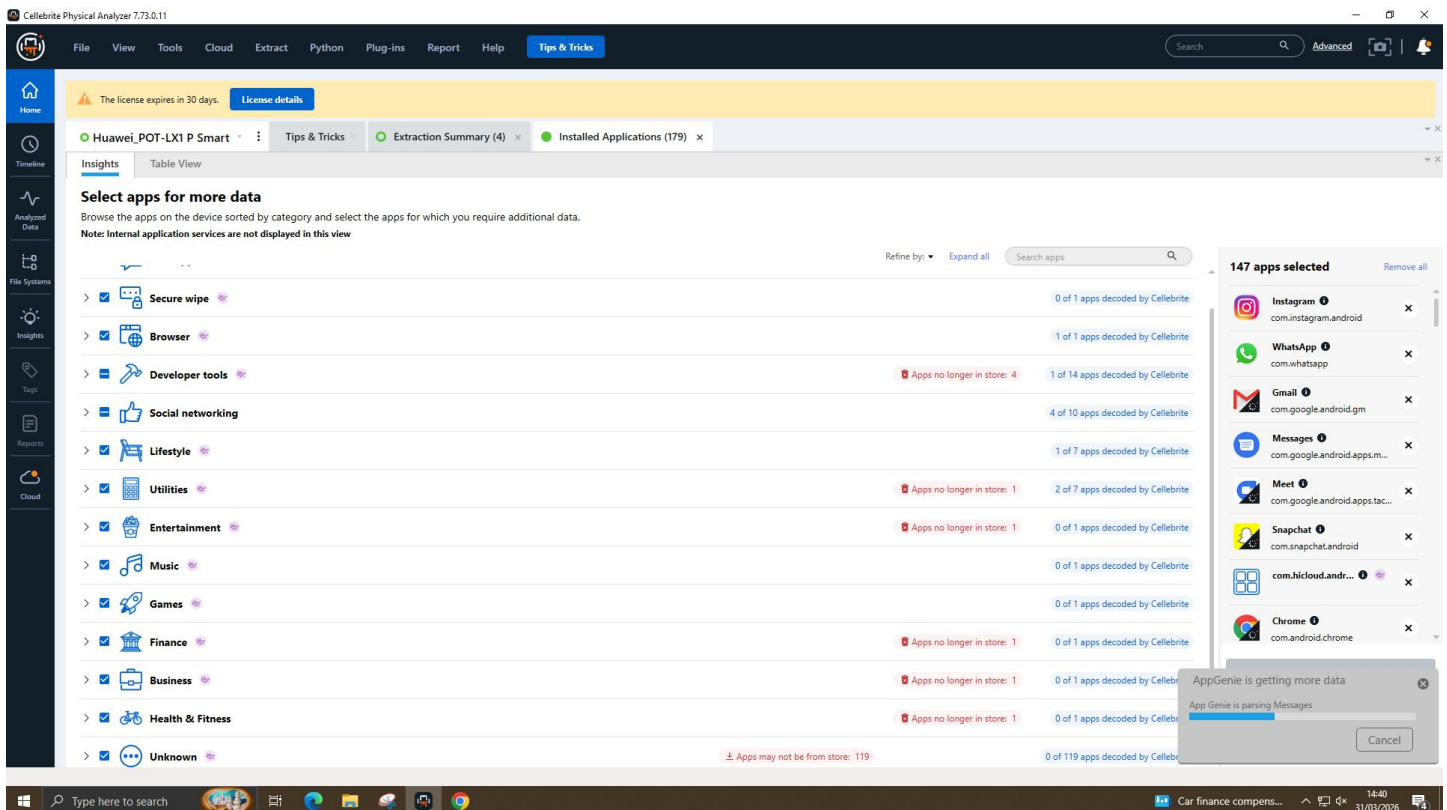


Figure 22: AppGenie Running Process

App Genie was then started, and once the process was completed, it displayed the relevant information needed to support the investigation, as shown in Figure 22

5.1.2 Hash Verification

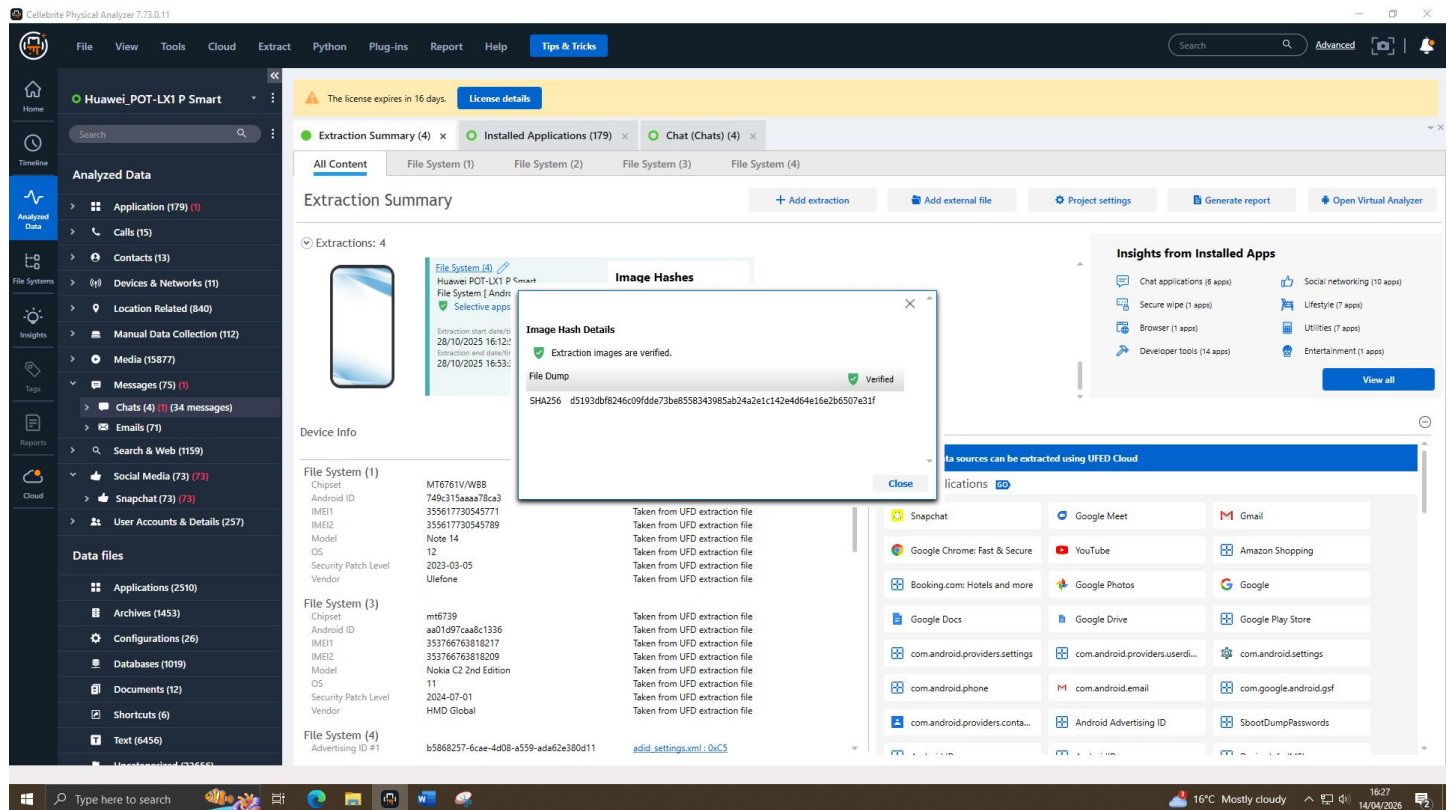


Figure 23: Hash Verification of Huawei Phone

Here, the SHA-256 hash value of the Huawei mobile phone was verified, as shown in Figure 23.

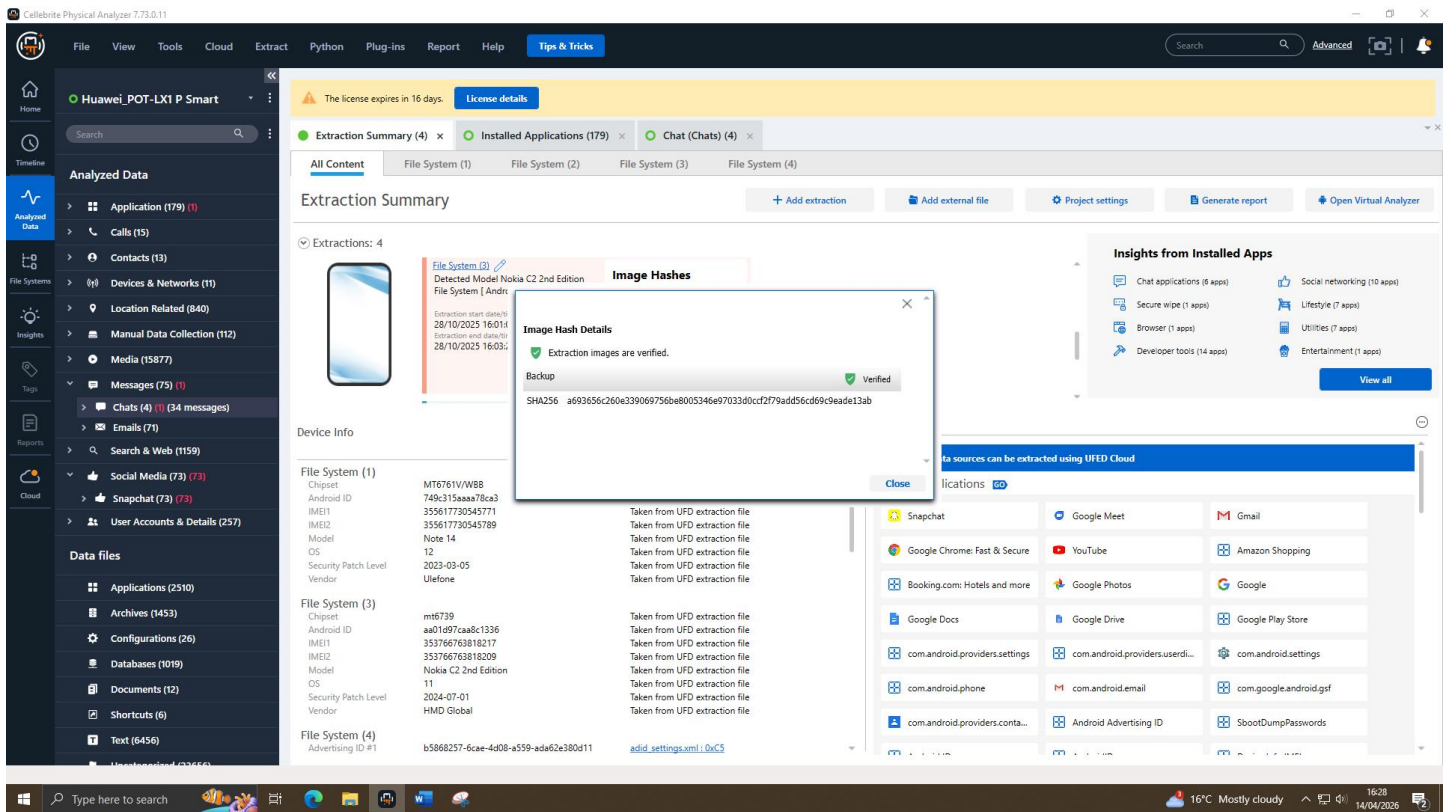


Figure 24: Hash Verification of Nokia Phone

Here, the SHA-256 hash value of the Nokia mobile phone was verified, as shown in Figure 24.

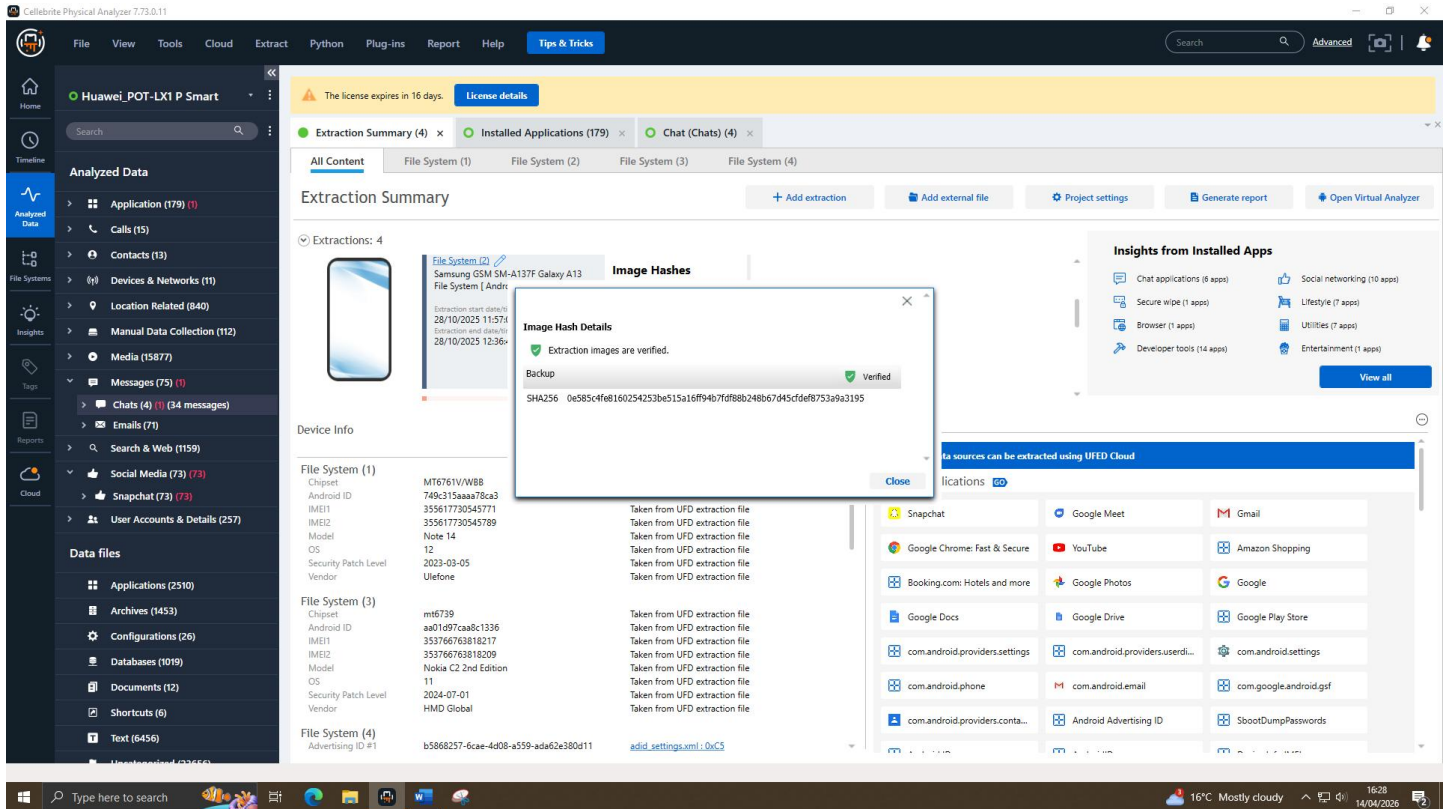


Figure 25: Hash Verification of Samsung Phone

Here, the SHA-256 hash value of the Samsung mobile phone was verified, as shown in Figure 25.

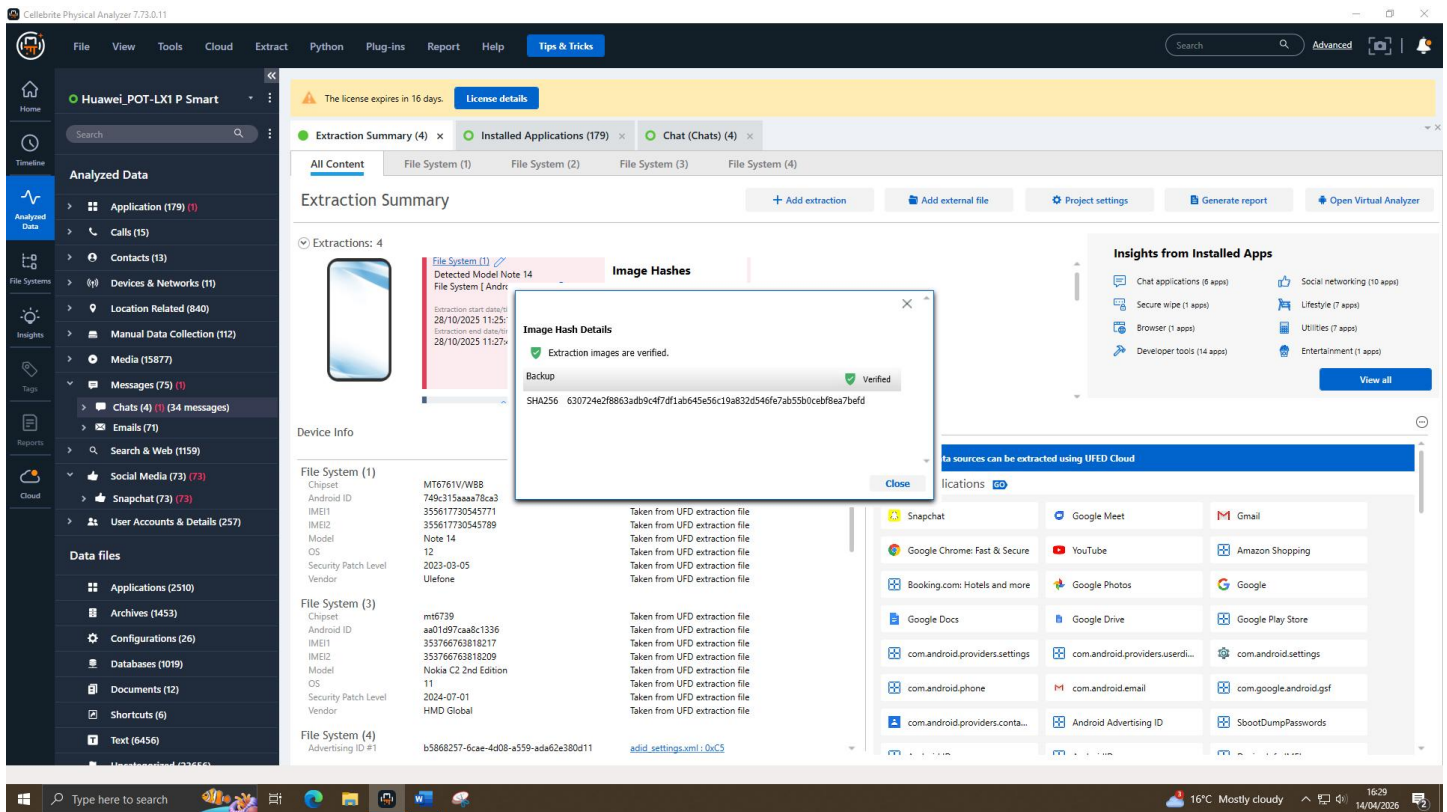


Figure 26: Hash Verification of Note Phone

Here, the SHA-256 hash value of the Note mobile phone was verified, as shown in Figure 26.

5.1.3 Chain of Custody Documentation

5.1.3.1 Evidence Inventory

- **MOB-01 – Ulefone Note 14 Smartphone**

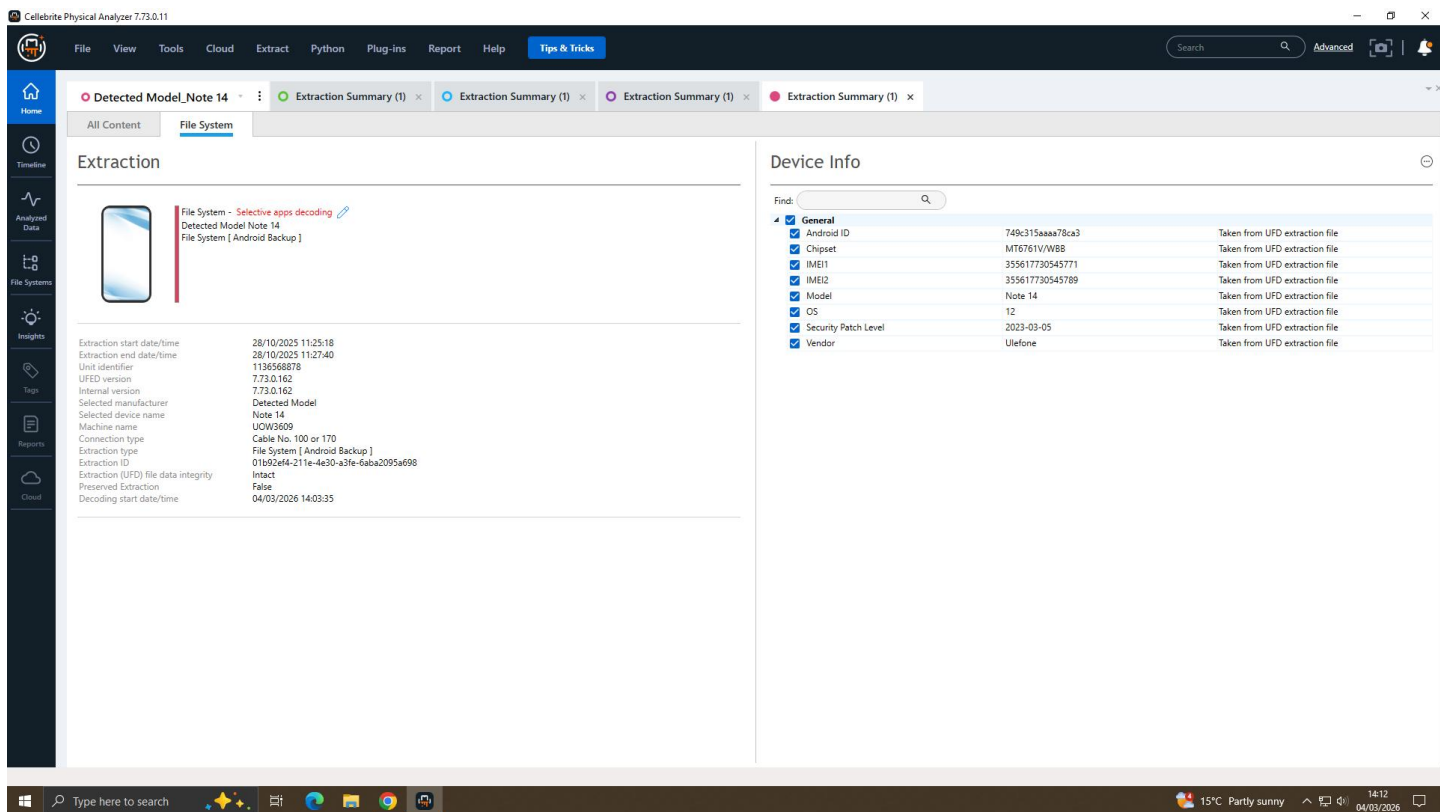


Figure 27: Ulefone Note 14 Extraction Details

Following data extraction using Cellebrite UFED Analyzer, the device was identified as a Ulefone Note 14, and its key device information was successfully recovered, as shown in Figure 27

Cellebrite Collection Summary

Collection Summary Report	
UFED 4PC ID	1136568878
UFED 4PC version	7.73.0.162
Extraction start time	2025-10-28 11:25:18
Extraction end time	2025-10-28 11:27:40
Selected vendor	Detected Model
Selected model	Note 14
Extraction type	File system
Extraction method	Android Backup
Device Model	Note 14
OS Version	12
Chipset	MT6761V/WBB
Security Patch Level	2023-03-05
IMEI	355617730545771
IMEI2	355617730545789
Vendor	Ulefone
Is Device Rooted	No
Number Of Installed Applications	0
Live encryption state	file

Figure 28: Cellebrite Collection Summary of Ulefone Note 14

The Cellebrite UFED Analyzer collection summary identified the extracted device as a Ulefone Note 14, with relevant device details successfully recovered, as illustrated in Figure 28

- **MOB-02 – Samsung Galaxy A13 (SM-A137F)**

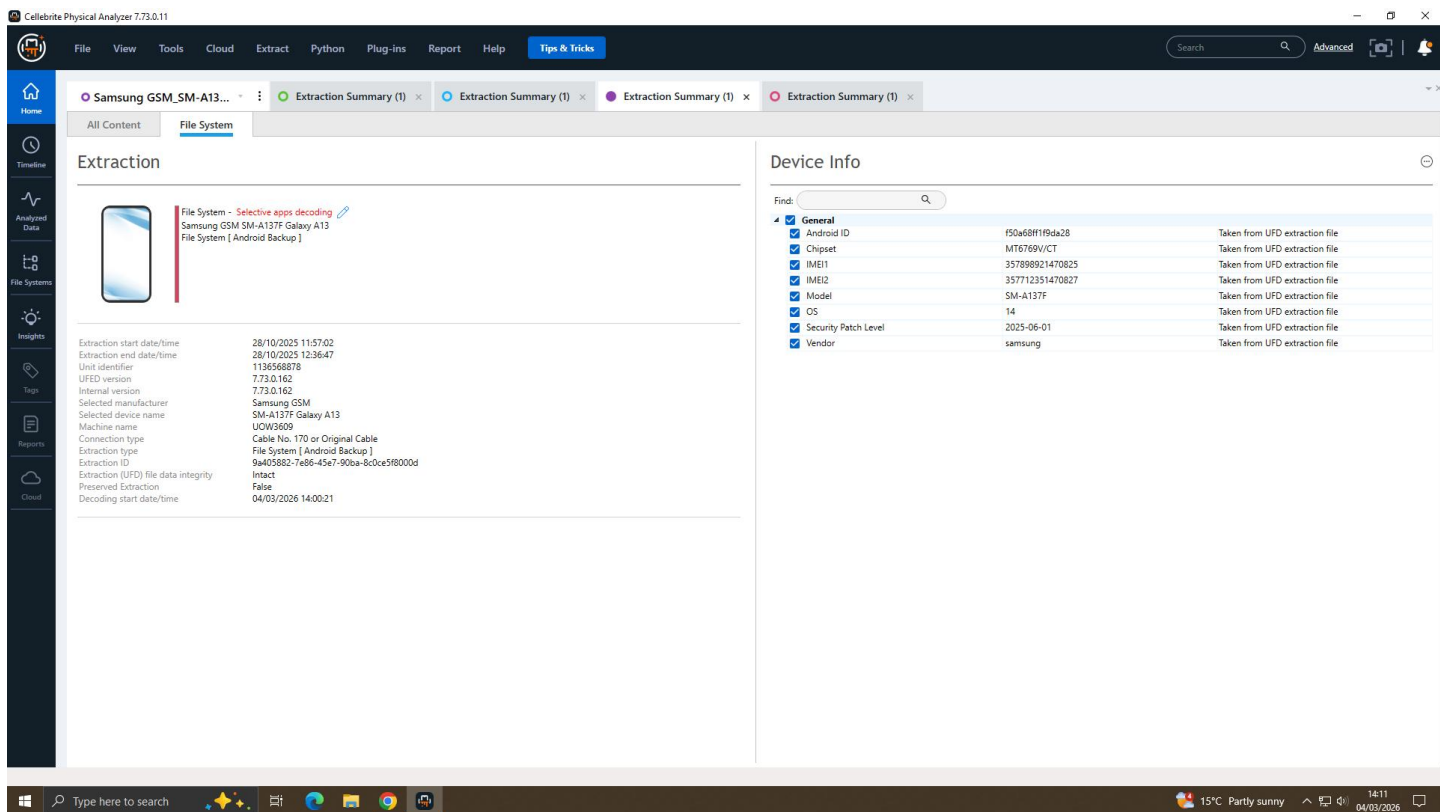


Figure 29: Samsung Extraction Details

Following data extraction using Cellebrite UFED Analyzer, the device was identified as a Samsung Galaxy A13 (SM-A137F), and its key device information was successfully recovered, as shown in Figure 29

Cellebrite Collection Summary

Collection Summary Report	
UFED 4PC ID	1136568878
UFED 4PC version	7.73.0.162
Extraction start time	2025-10-28 11:57:02
Extraction end time	2025-10-28 12:36:47
Selected vendor	Samsung GSM
Selected model	SM-A137F Galaxy A13
Extraction type	File system
Extraction method	Android Backup
Device Model	SM-A137F
OS Version	14
Chipset	MT6769V/CT
Security Patch Level	2025-06-01
IMEI	357898921470825
IMEI2	357712351470827
Vendor	samsung
Is Device Rooted	No
Number Of Installed Applications	0
Live encryption state	file

Figure 30: Cellebrite Collection Summary of Samsung

The Cellebrite UFED Analyzer collection summary identified the extracted device as a Samsung Galaxy A13 (SM-A137F), with relevant device details successfully recovered, as illustrated in Figure 30

- **MOB-03 – Nokia C2 2nd Edition Smartphone**

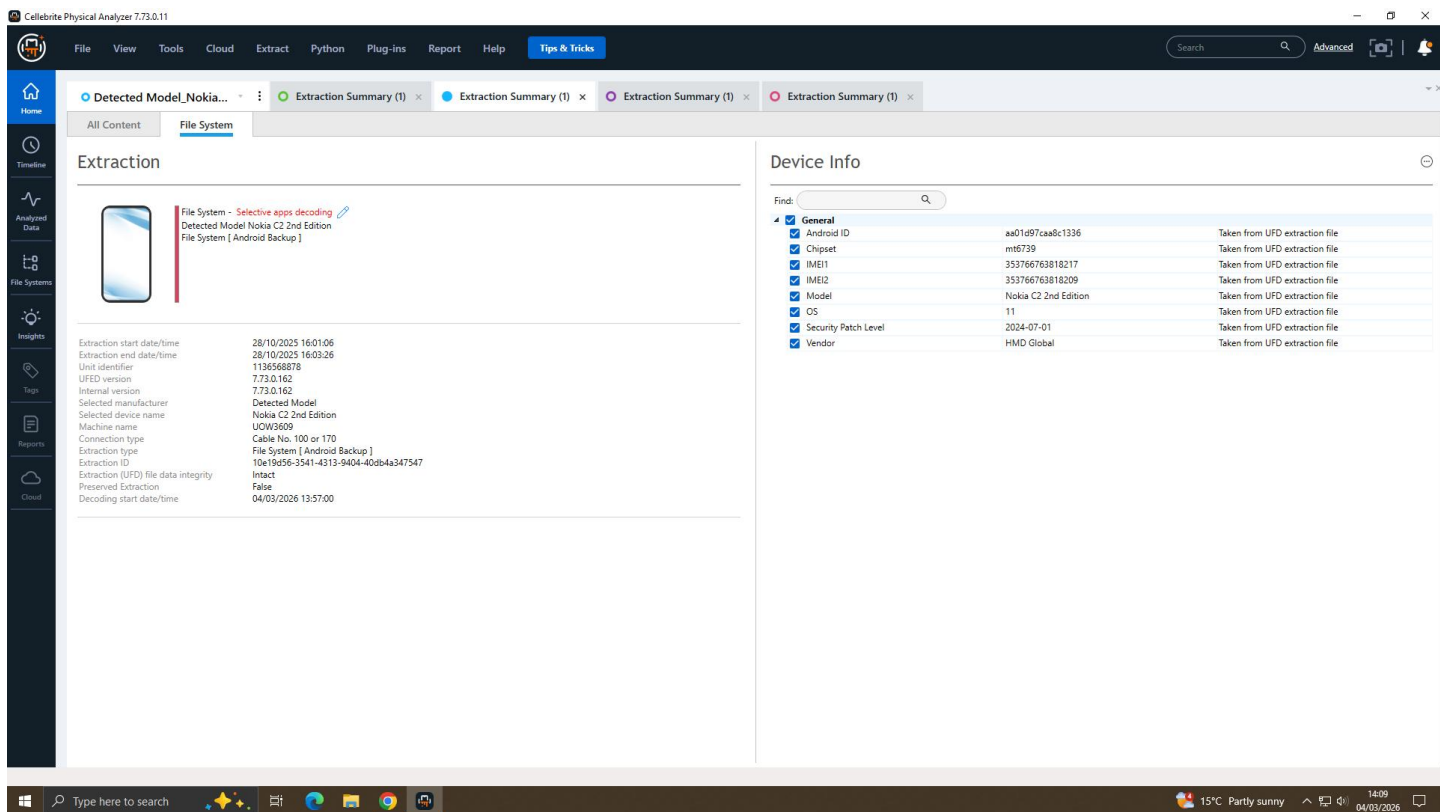


Figure 31: Nokia Extraction Details

Following data extraction using Cellebrite UFED Analyzer, the device was identified as a Nokia C2 2nd Edition, and its key device information was successfully recovered, as shown in Figure 31

Cellebrite Collection Summary

Collection Summary Report	
UFED 4PC ID	1136568878
UFED 4PC version	7.73.0.162
Extraction start time	2025-10-28 16:01:06
Extraction end time	2025-10-28 16:03:26
Selected vendor	Detected Model
Selected model	Nokia C2 2nd Edition
Extraction type	File system
Extraction method	Android Backup
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

Figure 32: Cellebrite Collection Summary of Nokia

The Cellebrite UFED Analyzer collection summary identified the extracted device as a Nokia C2 2nd Edition, with relevant device details successfully recovered, as illustrated in Figure 32

- **MOB-04 – Huawei P Smart (POT- LX1)**

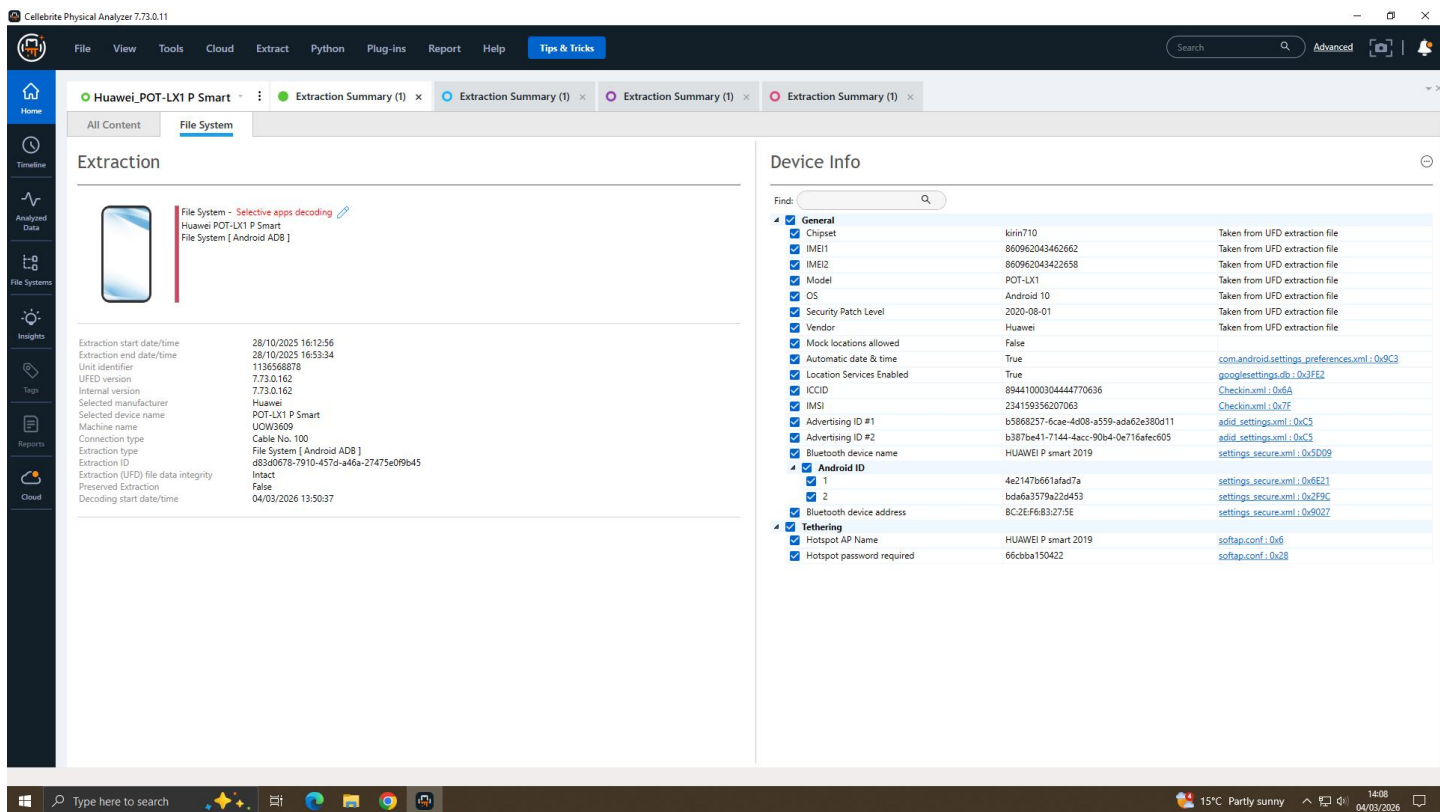


Figure 33: Huawei Extraction Details

Following data extraction using Cellebrite UFED Analyzer, the device was identified as a Huawei P Smart (POT-LX1), and its key device information was successfully recovered, as shown in Figure 33

Cellebrite Collection Summary	
Collection Summary Report	
UFED 4PC ID	1136568878
UFED 4PC version	7.73.0.162
Extraction start time	2025-10-28 16:12:56
Extraction end time	2025-10-28 16:53:34
Selected vendor	Huawei
Selected model	POT-LX1 P Smart
Extraction type	File system
Extraction method	Kirin Live
Device Model	POT-LX1
OS Version	Android 10
Chipset	kirin710
Security Patch Level	2020-08-01
IMEI	860962043462662
IMEI2	860962043422658
Is Device Rooted	No
Number Of Installed Applications	263

Figure 34: Cellebrite Collection Summary of Huawei

The Cellebrite UFED Analyzer collection summary with Kirin Live identified the extracted device as a Huawei P Smart (POT- LX1), with relevant device details successfully recovered, as illustrated in Figure 34

Collection Summary Report	
UFED 4PC ID	1136568878
UFED 4PC version	7.73.0.162
Extraction start time	2025-10-28 16:08:57
Extraction end time	2025-10-28 16:12:27
Selected vendor	Huawei
Selected model	POT-LX1 P Smart
Extraction type	File system
Extraction method	Android Backup APK Downgrade
Device Model	POT-LX1
OS Version	Android 10
Chipset	kirin710
Security Patch Level	2020-08-01
Vendor	HUAWEI
Is Device Rooted	No
Number Of Installed Applications	0
Live encryption state	File

Figure 35: Cellebrite Collection Summary of Huawei 2

The Cellebrite UFED Analyzer collection summary with Android Backup APK Downgrade identified the extracted device as a Huawei P Smart (POT- LX1), with relevant device details successfully recovered, as illustrated in Figure 35

5.1.3.2 Chain of Custody Log

Date & Time	Evidence ID	Mobile Name	IMEI Number	Action	Examiner	Notes
2025-10-28 11:25:18	MOB-01	Ulefone Note 14 Smartphone	355617730545771 / 355617730545789	Extraction Started	University Provided Dataset (UWTSD)	Android Backup
2025-10-28 11:27:40	MOB-01	Ulefone Note 14 Smartphone	355617730545771 / 355617730545789	Extraction Completed	University Provided Dataset (UWTSD)	Unrooted
2025-10-28 11:57:02	MOB-02	Samsung Galaxy A13 (SM-A137F)	357898921470825 / 357712351470827	Extraction Started	University Provided Dataset (UWTSD)	Android Backup
2025-10-28	MOB-02	Samsung	357898921470825 /	Extraction	University	Unrooted

12:36:47		Galaxy A13 (SM-A137F)	357712351470827	Completed	Provided Dataset (UWTSD)	
2025-10-28 16:01:06	MOB-03	Nokia C2 2nd Edition Smartphone	353766763818217 / 353766763818209	Extraction Started	University Provided Dataset (UWTSD)	Android Backup
2025-10-28 16:03:26	MOB-03	Nokia C2 2nd Edition Smartphone	353766763818217 / 353766763818209	Extraction Completed	University Provided Dataset (UWTSD)	Unrooted
2025-10-28 16:12:56	MOB-04	Huawei P Smart (POT- LX1)	860962043462662 / 860962043422658	Extraction Started	University Provided Dataset (UWTSD)	Kirin Live
2025-10-28 16:53:34	MOB-04	Huawei P Smart (POT- LX1)	860962043462662 / 860962043422658	Extraction Completed	University Provided Dataset (UWTSD)	263 Apps Recovered

Table 1: Chain of Custody log

5.1.3.3 Integrity Measures

- Cellebrite UFED 4PC v7.73.0.11 was used as an industry- standard forensic tool for all acquisitions.
- Extraction methods and timestamps were recorded to provide a complete audit trail of examiner actions.
- All devices were documented as not rooted, reducing the likelihood of data alteration during acquisition.
- SHA- 256 hash values were used to verify the integrity of the extracted data and confirm that no changes occurred after acquisition.
- Evidence handling followed recognized digital forensic best practices, supporting reliability and legal admissibility.

5.1.4 Scope and Limitation of Available Evidence

This investigation used only the four mobile forensic images provided. Although a USB flash drive linked to Emma was mentioned, no image or records for it were available. Therefore, the examination focused only on the smartphone data, and all findings are based solely on the evidence provided.

5.2 Communication Analysis

5.2.1 WhatsApp Analysis (Emma ↔ Joe)

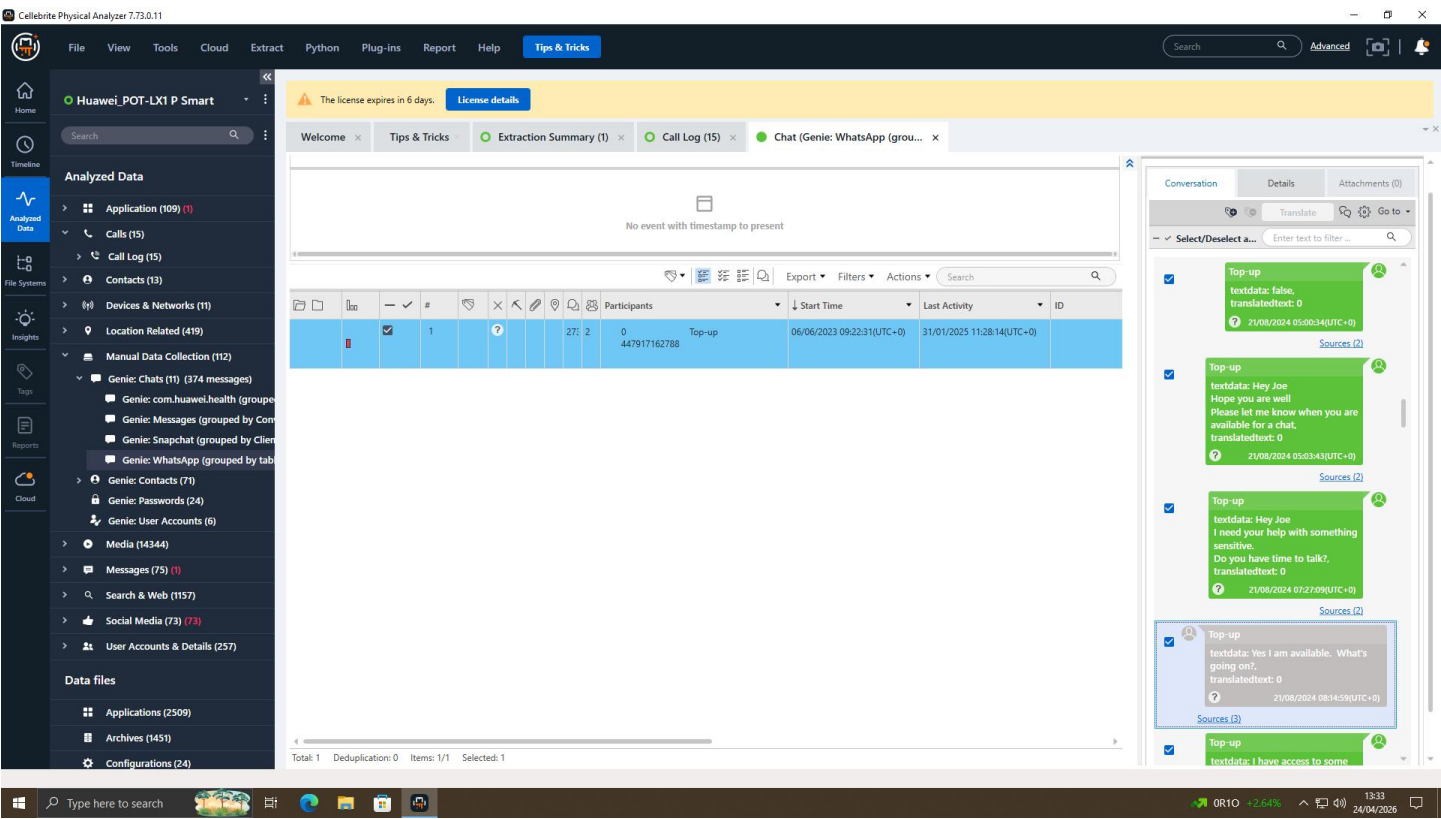


Figure 36: WhatsApp Conversation Between Emma and Joe 1

The extracted messages indicate that the individuals were discussing sensitive matters, as shown in Figure 36

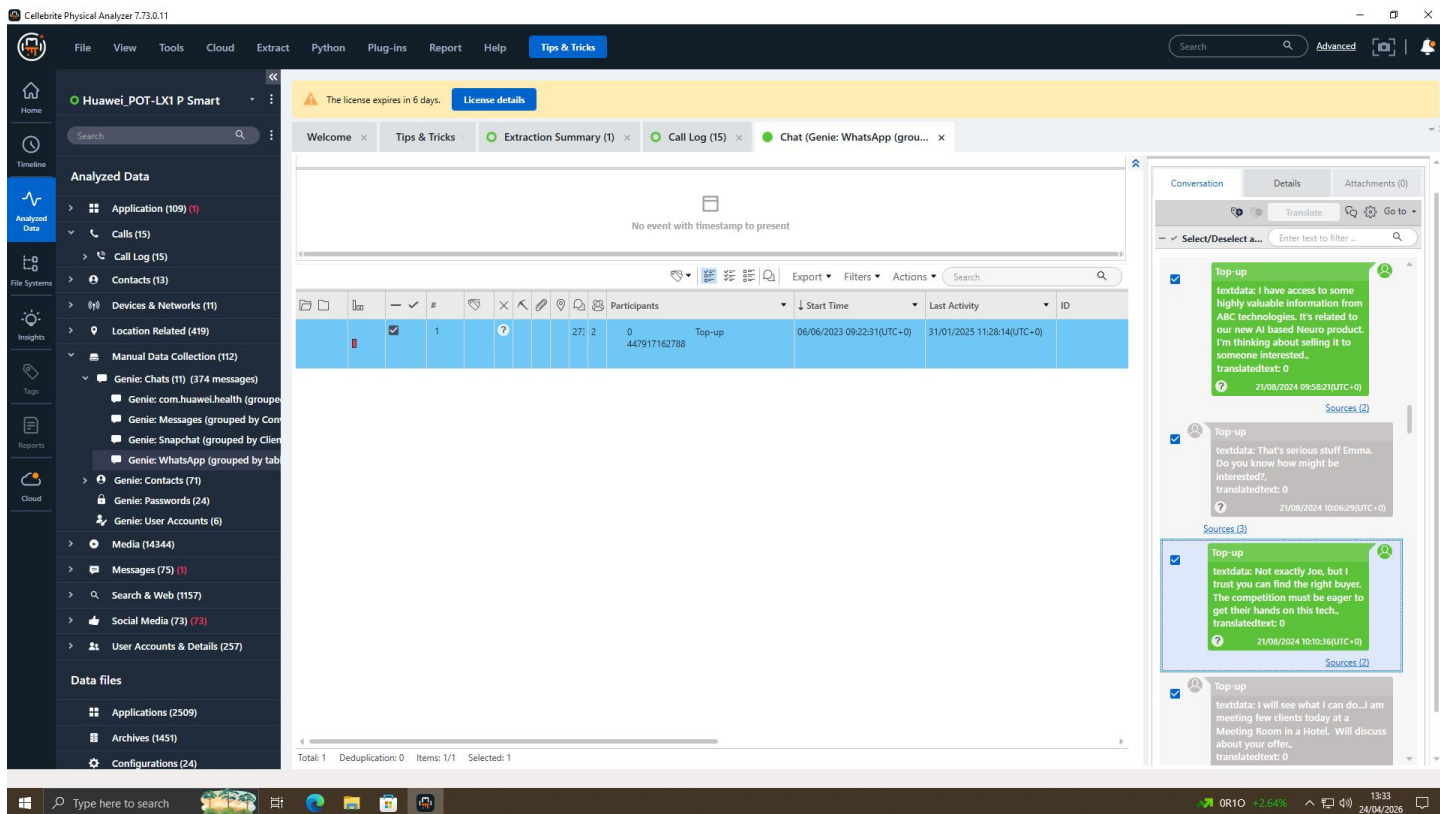


Figure 37: WhatsApp Conversation Between Emma and Joe 2

The communication indicates that Emma had company material and expressed a willingness to sell it, which she discussed with Joe, as shown in Figure 37

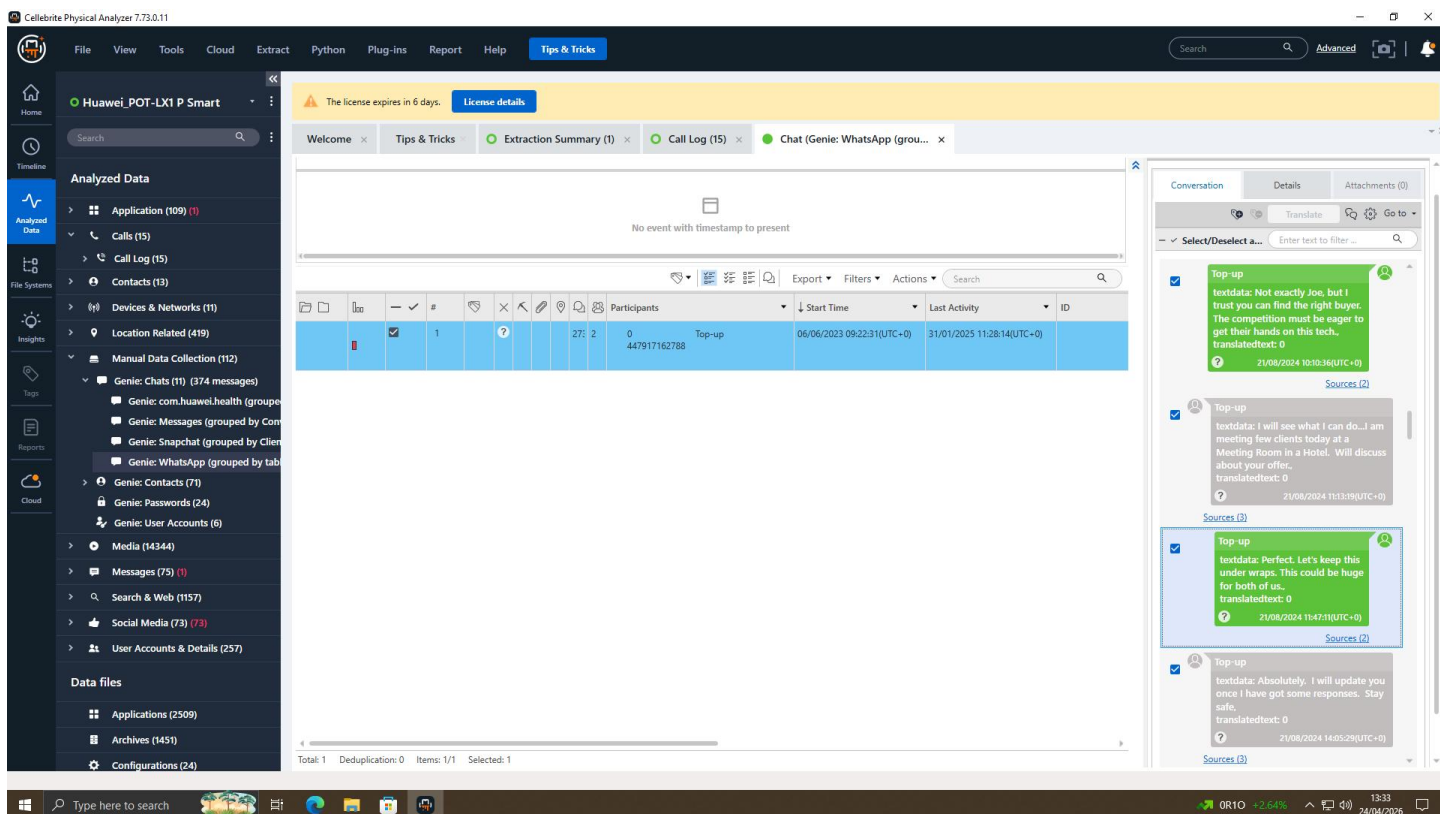


Figure 38: WhatsApp Conversation Between Emma and Joe 3

The messages indicate that arrangements were being made to meet with potential buyers, as shown in Figure 38

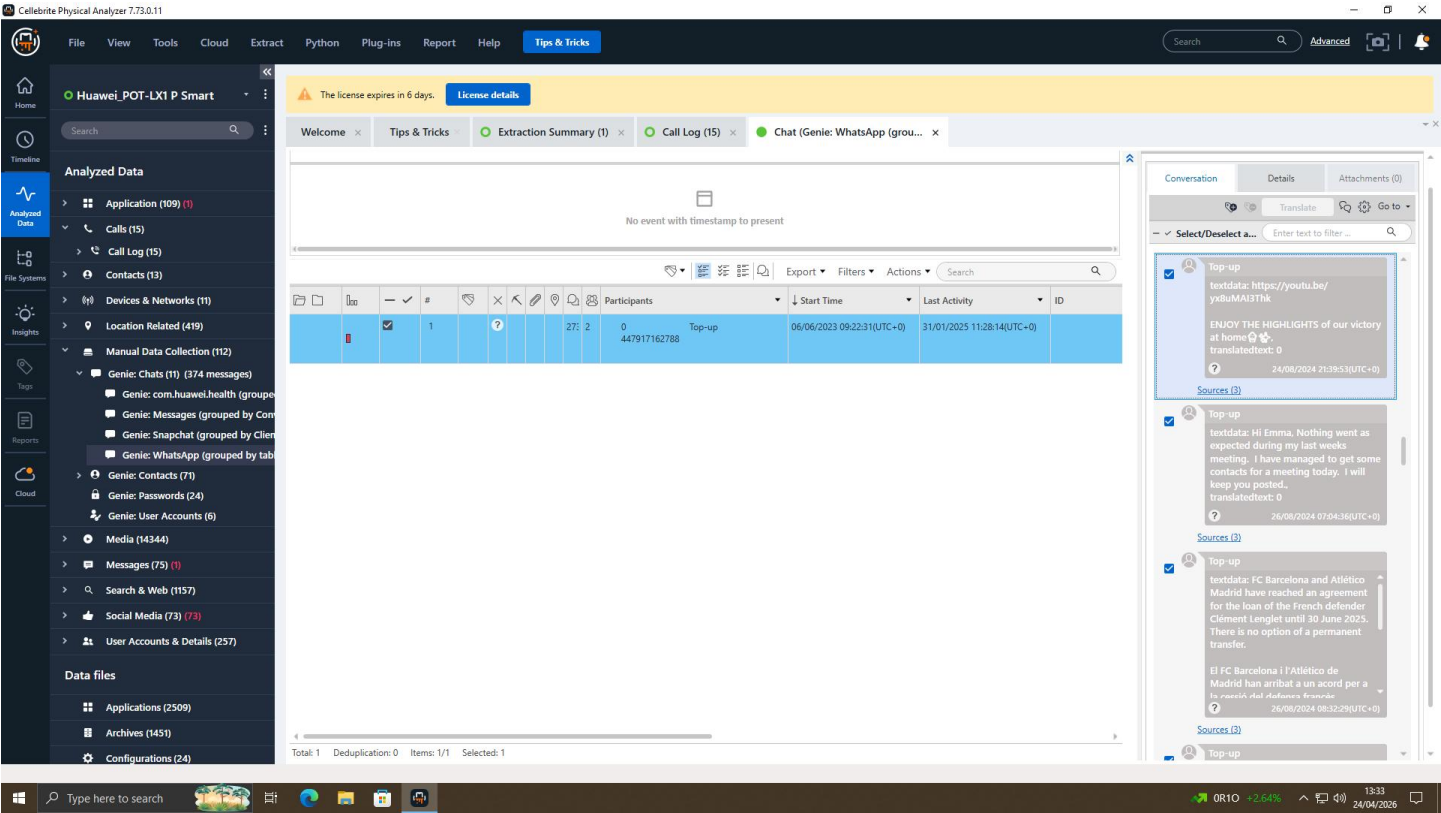


Figure 39: WhatsApp Conversation Between Emma and Joe 4

As the discussion with the buyer did not progress as expected, further meetings were requested, as shown in Figure 39

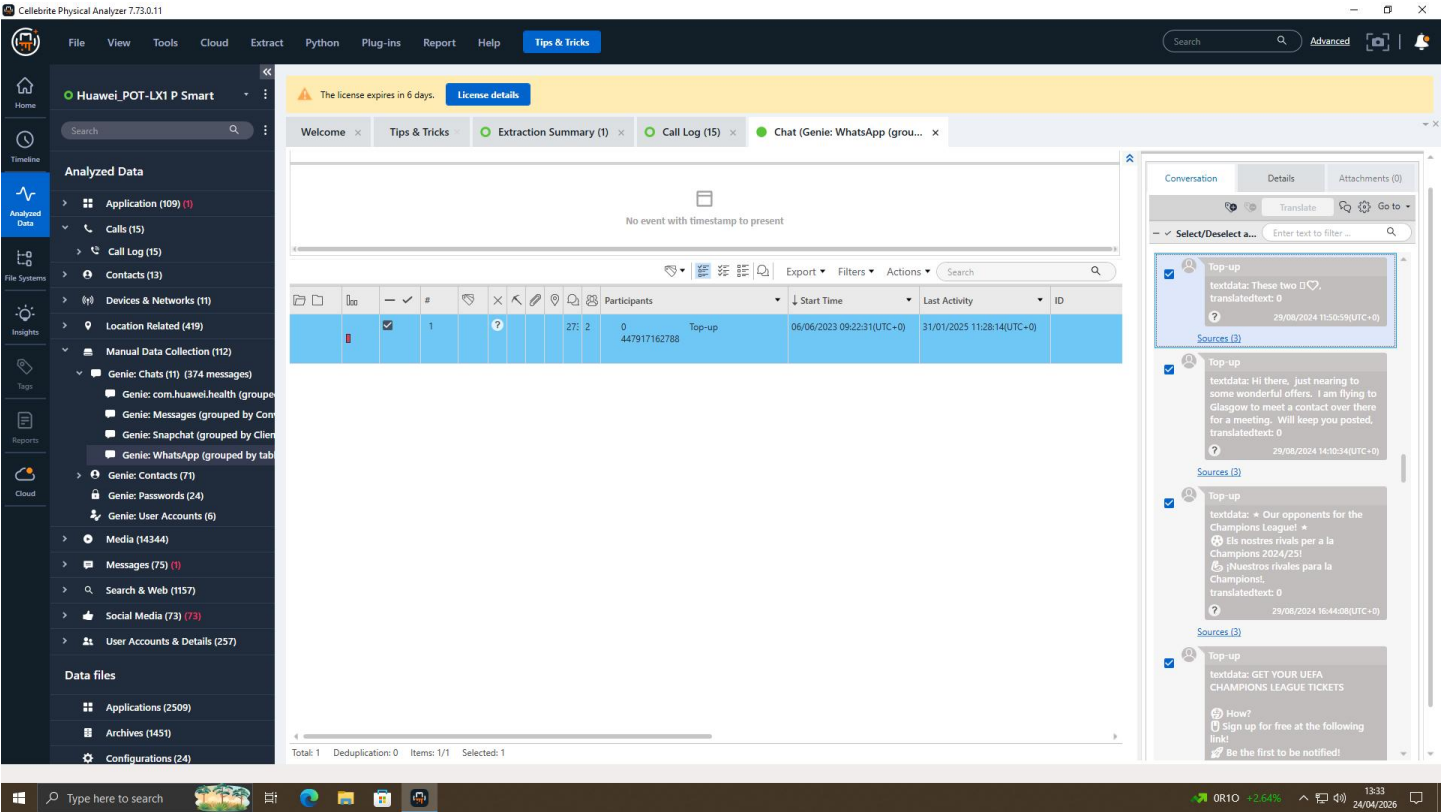


Figure 40: WhatsApp Conversation Between Emma and Joe 5

A more attractive offer was identified, and a meeting was arranged to discuss it, as shown in Figure 40

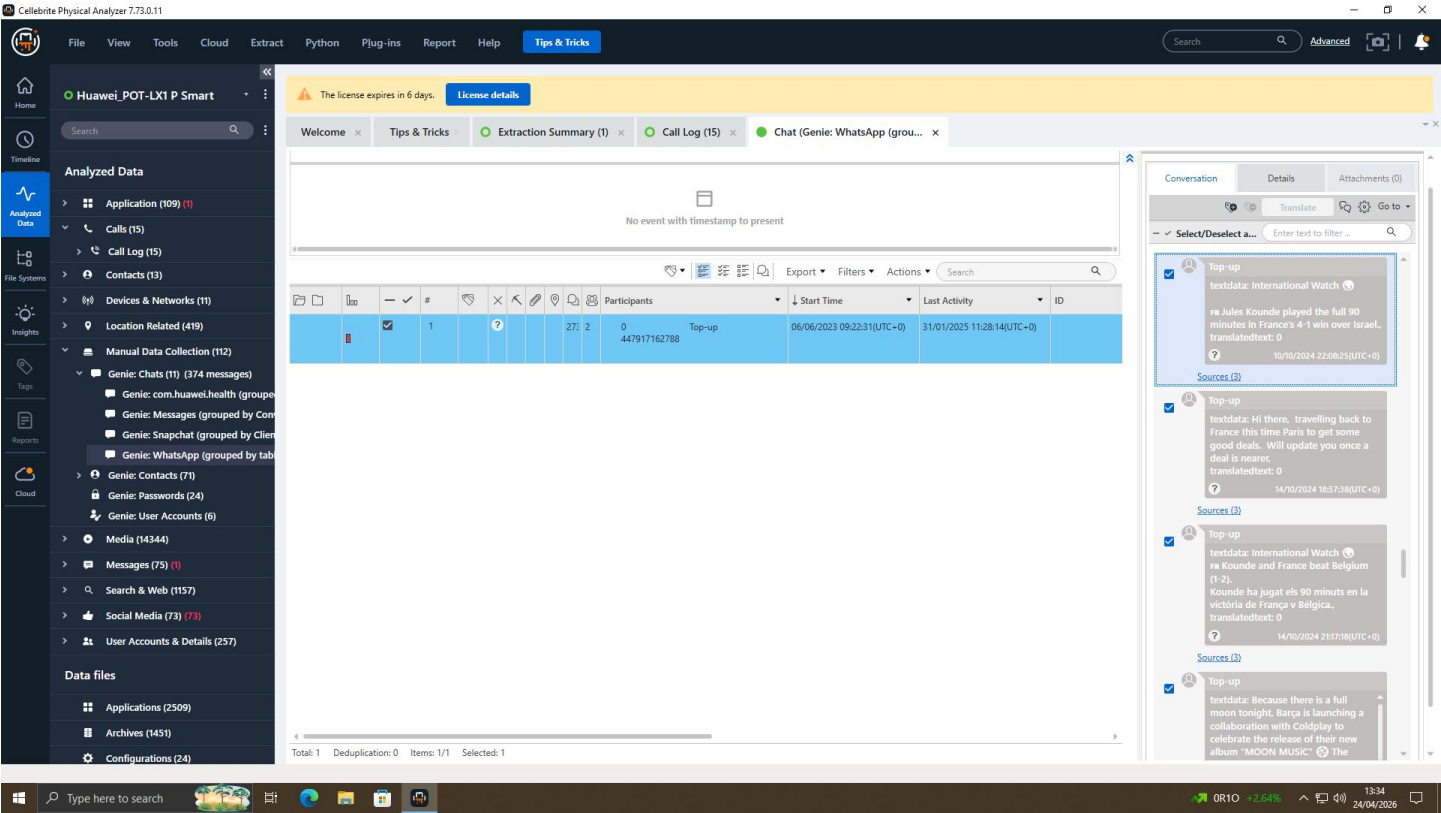


Figure 41: WhatsApp Conversation Between Emma and Joe 6

A further trip was made in pursuit of a better offer, as shown in Figure 41

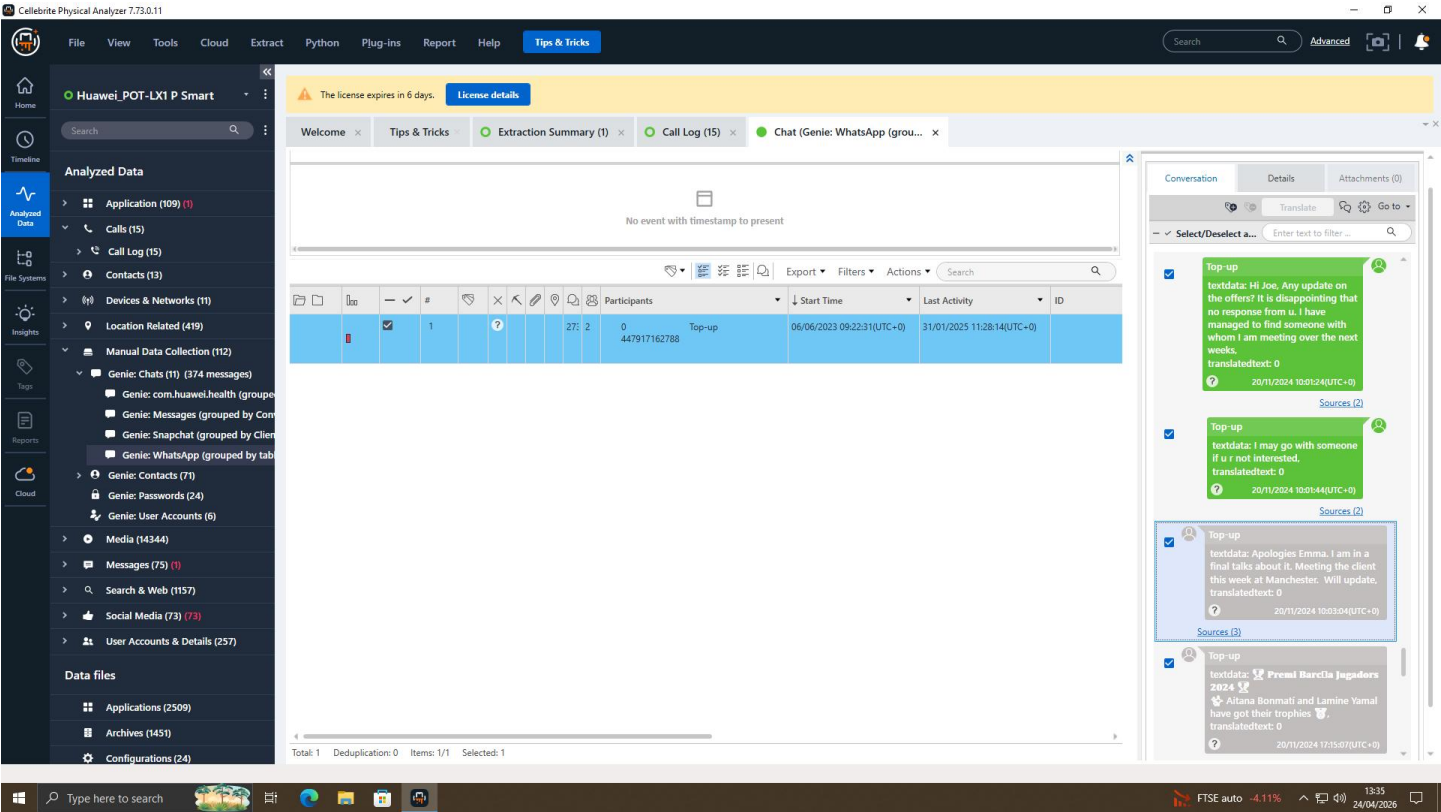


Figure 42: WhatsApp Conversation Between Emma and Joe 7

As negotiations took longer than expected, Emma showed signs of frustration, as shown in Figure 42

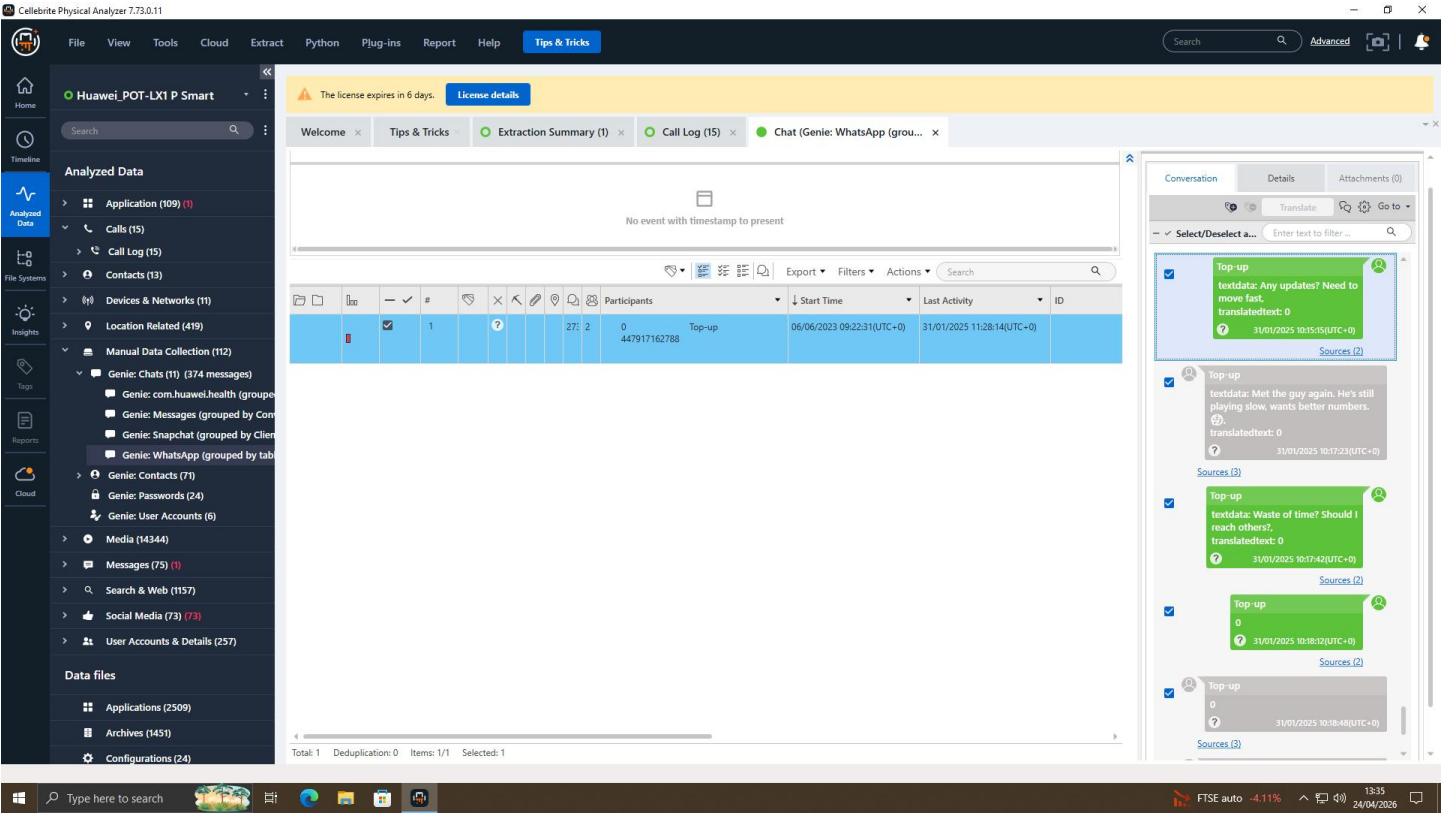


Figure 43: WhatsApp Conversation Between Emma and Joe 8

As the deal was not progressing well, Emma decided to look for a new buyer, as shown in Figure 43

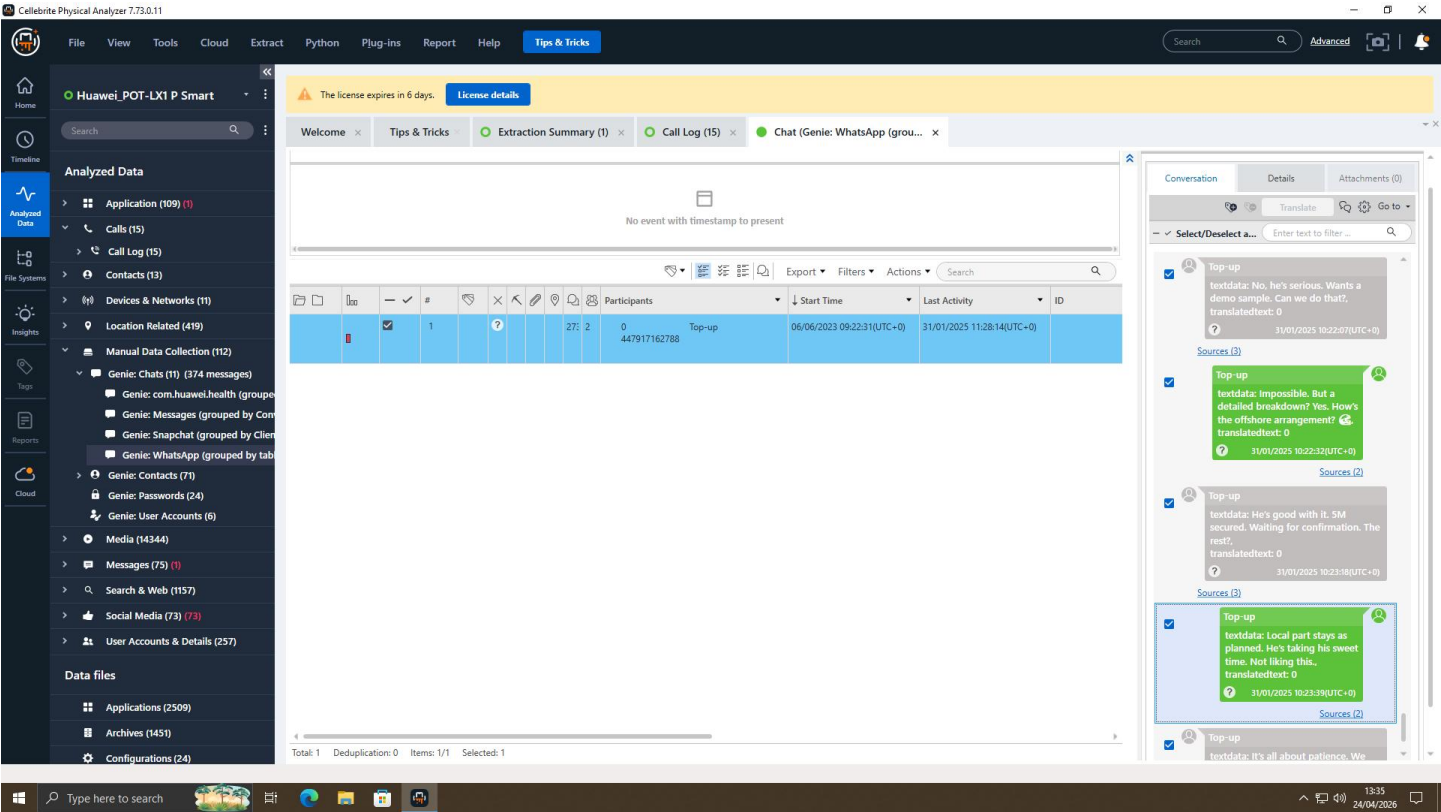


Figure 44: WhatsApp Conversation Between Emma and Joe 9

Further discussions took place regarding the payment of 5 million to secure the deal, as shown in Figure 44

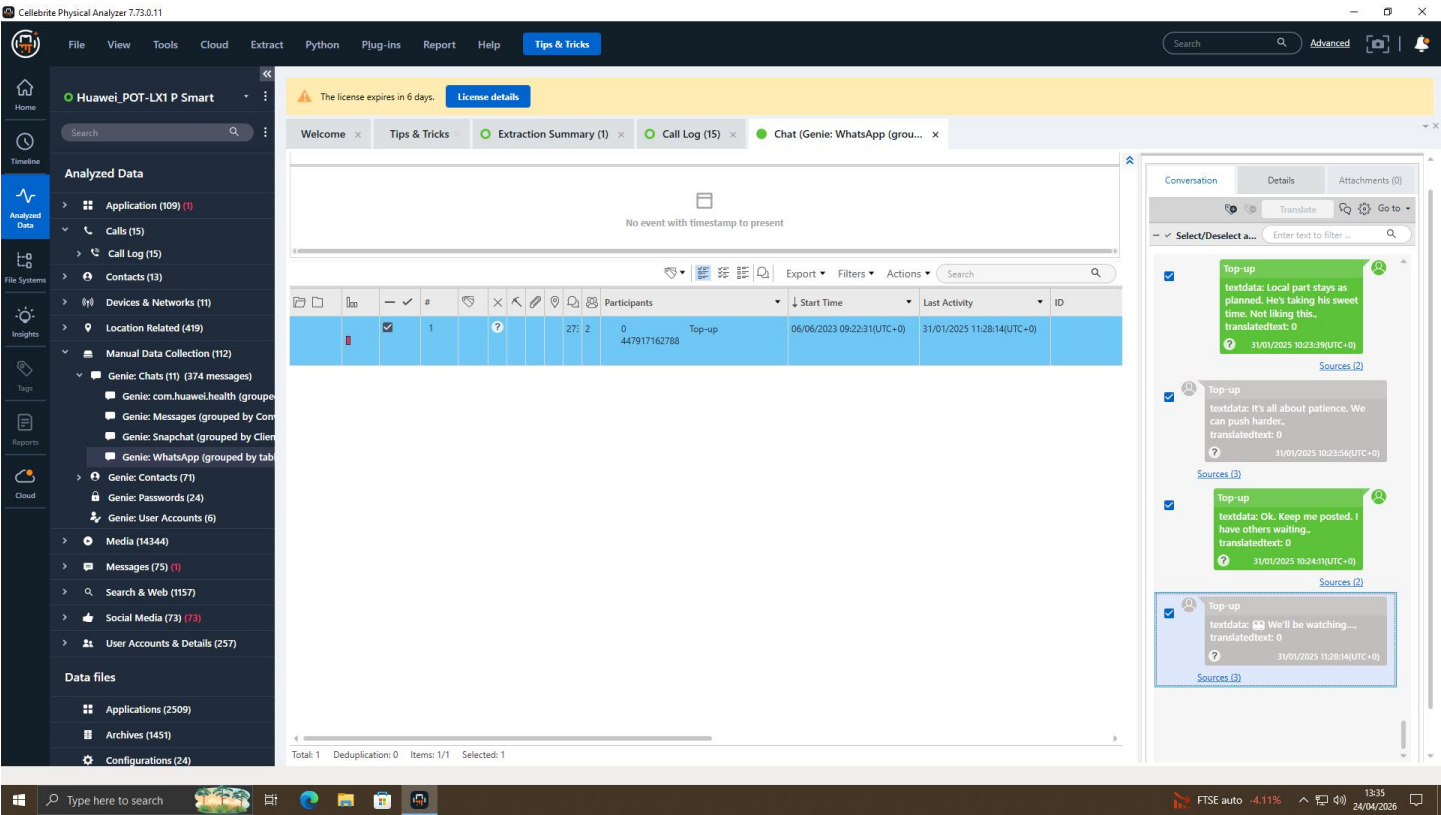


Figure 45: WhatsApp Conversation Between Emma and Joe 10

Further details of the conversation between Emma and Joe will be provided at a later stage, as shown in Figure 45

5.2.2 Facebook Analysis (Norman Smith ↔ Peter Dover)

The screenshot displays the Cellebrite Physical Analyzer 7.73.0.11 interface. The top menu bar includes File, View, Tools, Cloud, Extract, Python, Plug-ins, Report, Help, and Tips & Tricks. A license expiration notice is visible at the top. The sidebar on the left shows the 'Analyzed Data' section with a search bar and a list of analyzed items, including 'peter_dover (3)', 'Devices & Networks (11)', 'Wireless Networks (11)', 'Location Related (468)', 'Device Locations (468)', 'Locations (468)', 'Gmail (20)', 'Google Photos (194)', 'Native (254)', 'Manual Data Collection (724)', 'Genie: Chats (33) (1110 messages)', 'Genie: com.android.mediacenter (grouped)', 'Genie: com.huawei.android.totemweather', 'Genie: com.huawei.appmarket (grouped by t)', 'Genie: com.huawei.browser (grouped by t)', 'Genie: com.huawei.health (grouped by tab)', 'Genie: com.huawei.himovie.overseas (grou', 'Genie: Facebook (grouped by Thread Key)', 'Genie: Messages (grouped by Conversation)', 'Genie: Petal Maps (grouped by table) (2)', 'Genie: Snapchat (grouped by Client Conve', 'Genie: WhatsApp (grouped by table) (2)', 'Genie: Contacts (515)', 'Genie: com.huawei.browser (20)', 'Genie: Facebook (353)', 'Genie: Instagram (50)', 'Genie: Messages (18)', and 'Genie: Snapchat (6)'. The main window shows a 'Welcome' tab and a 'Genie: Facebook (353)' tab. A table of participants is displayed, showing two entries: 'Peter Dover (owner)' and 'Norman Smith'. The right-hand pane shows a conversation between Peter Dover and Norman Smith. The conversation includes messages such as 'Norman, Joe told me u r ready to proceed. Lets keep this clean and quick', 'You can now call each other and see information such as Active Status and when you've read messages.', 'Almost. We need the. Blueprint in chunks. Too risky in one go.', 'That wasn't the deal. Everything at once or no deal.', and 'Security reasons. Let's start with just the "head". You know what I mean.'.

Participants	Start Time	Last Activity	ID
61565261156720	31/01/2025 12:47:10(UTC+0)	31/01/2025 12:53:09(UTC+0)	61564326251951
61564326251951			

Figure 46: Facebook Conversation between Norman and Peter 1

This conversation shows negotiation over staged release terms and a proposed payment of 5 million, as shown in Figure 46

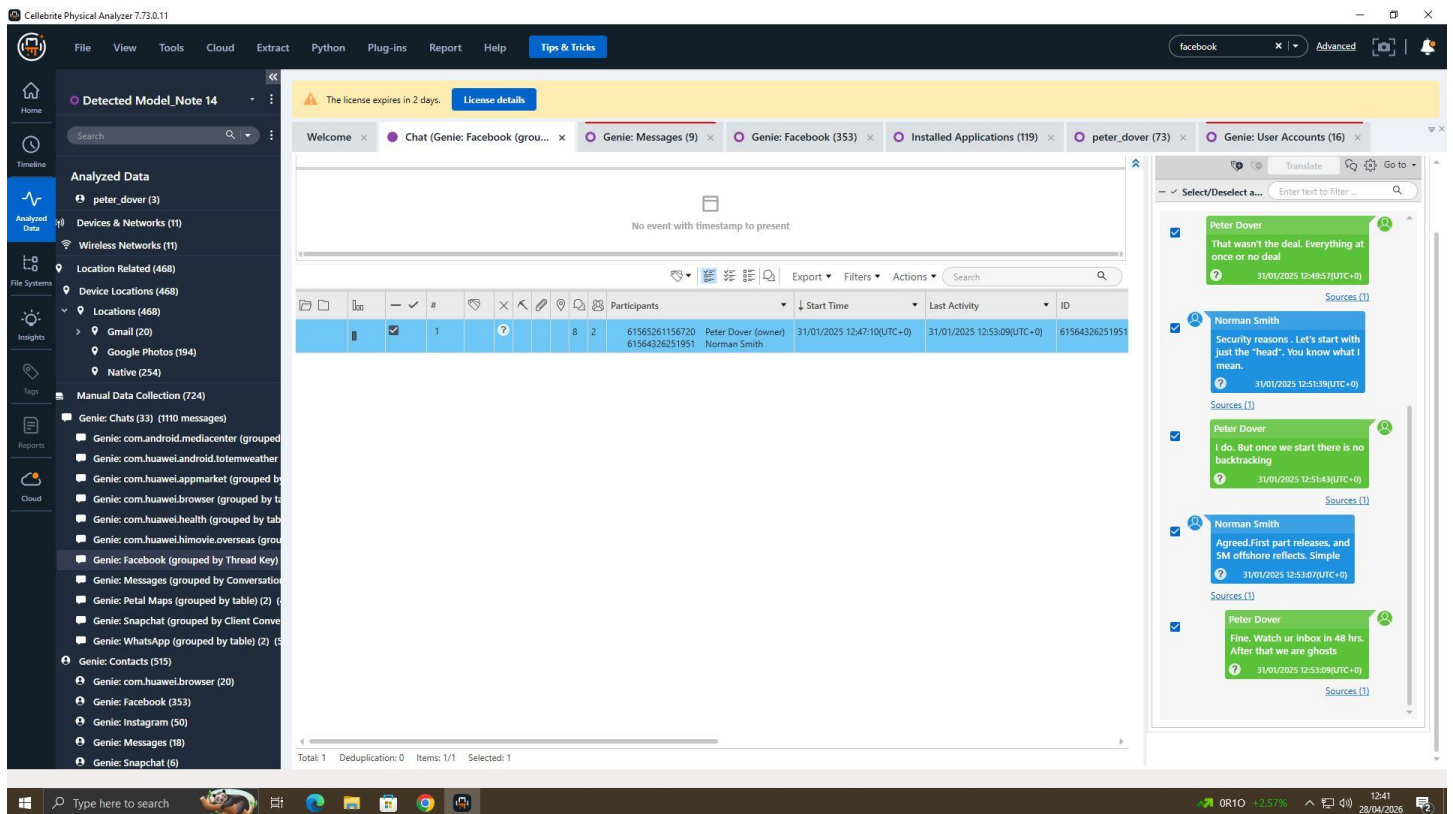


Figure 47: Facebook Conversation between Norman and Peter 2

These messages show disagreement over the deal, followed by a possible 48-hour delivery arrangement, as shown in Figure 47

5.2.3 User Directory Conversation Analysis

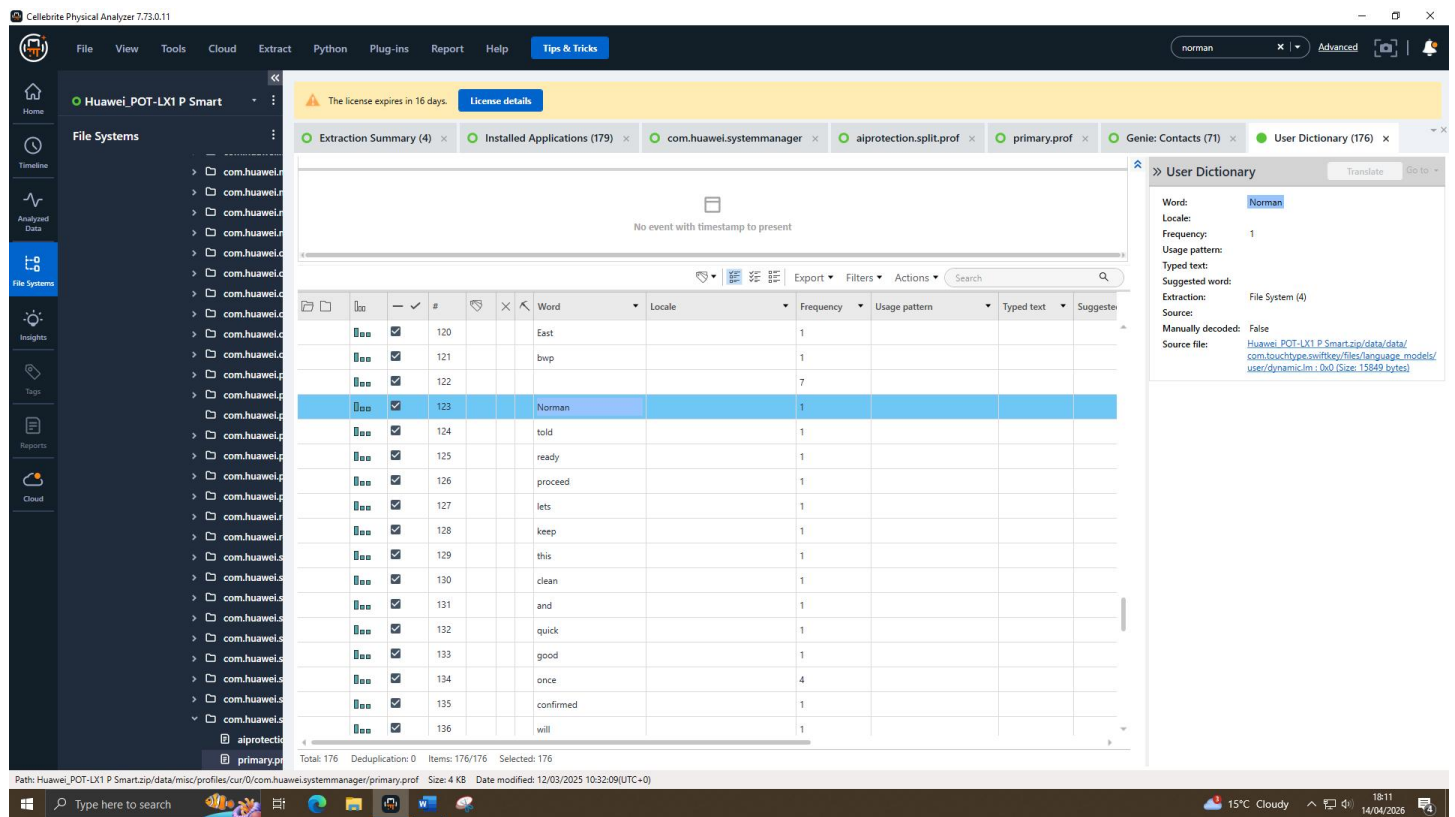


Figure 48: User Directory Analysis

According to Figure 46 The conversation suggests that the material would be shared in stages or chunks, as shown in Figure 48

5.2.4 Instagram DM Analysis

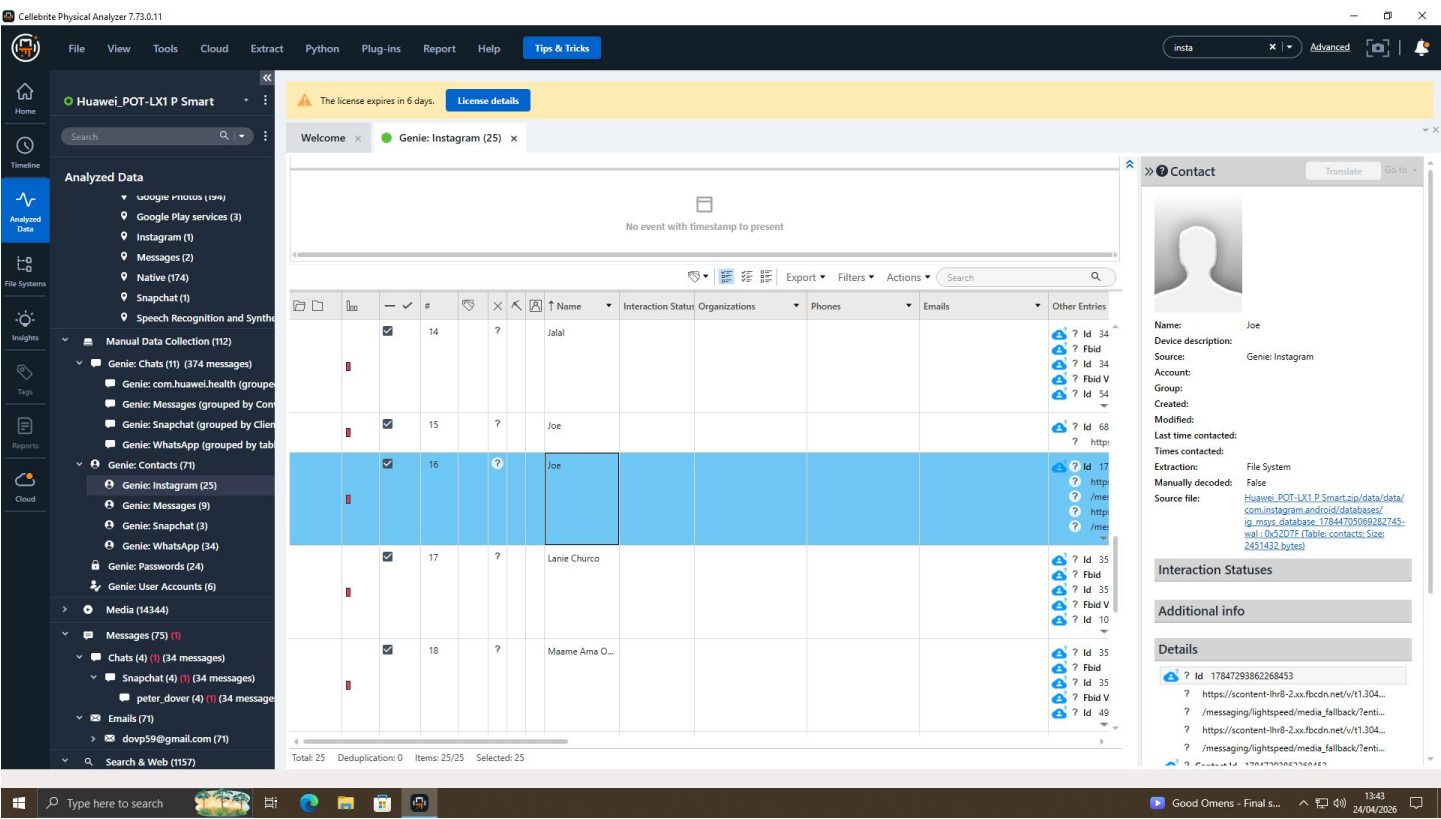


Figure 49: Instagram Analysis 1

On Instagram, Joe appears among the listed contacts, as shown in Figure 49

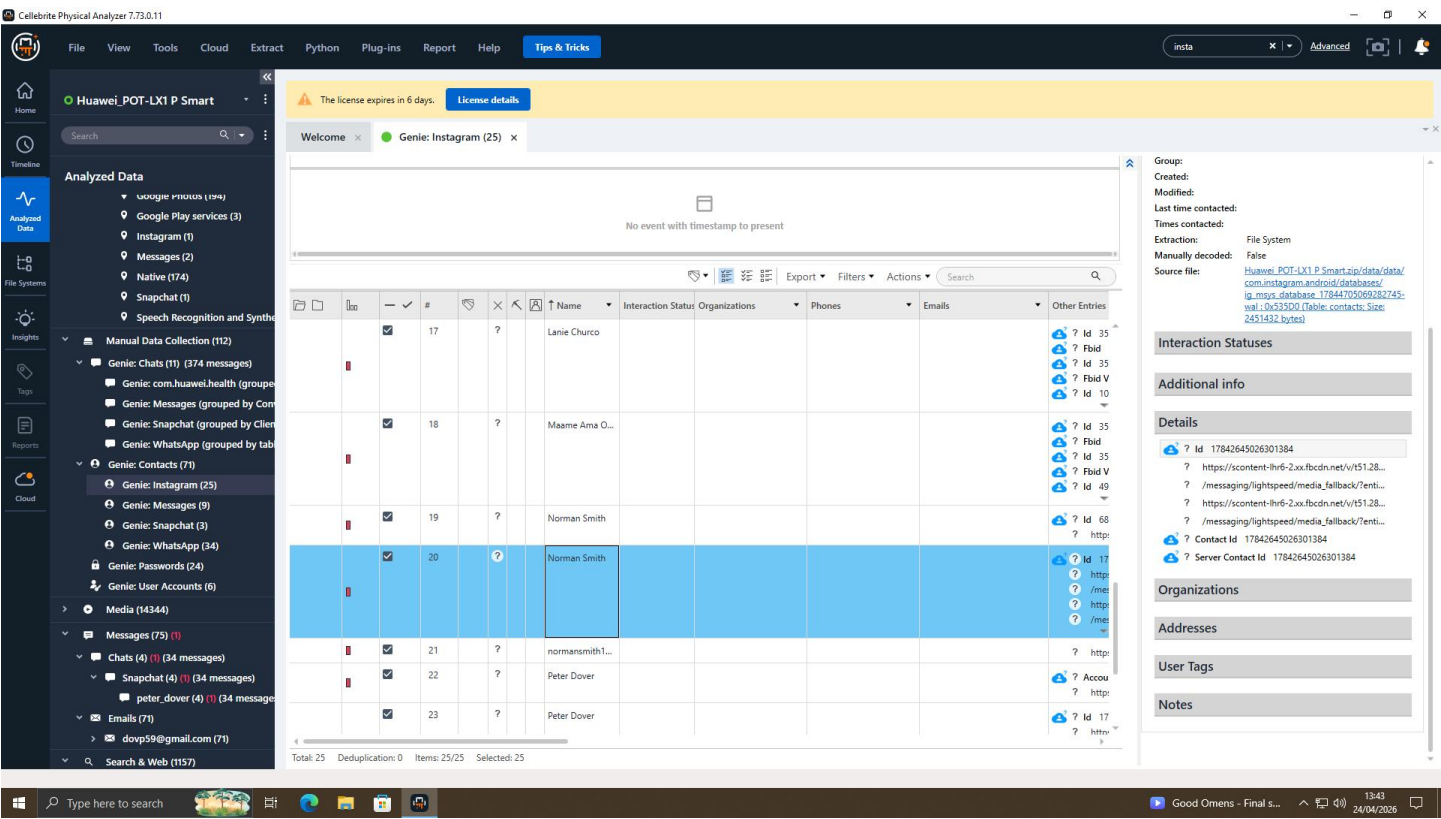


Figure 50: Instagram Analysis 2

On Instagram, Norman appears among the listed contacts, as shown in Figure 50

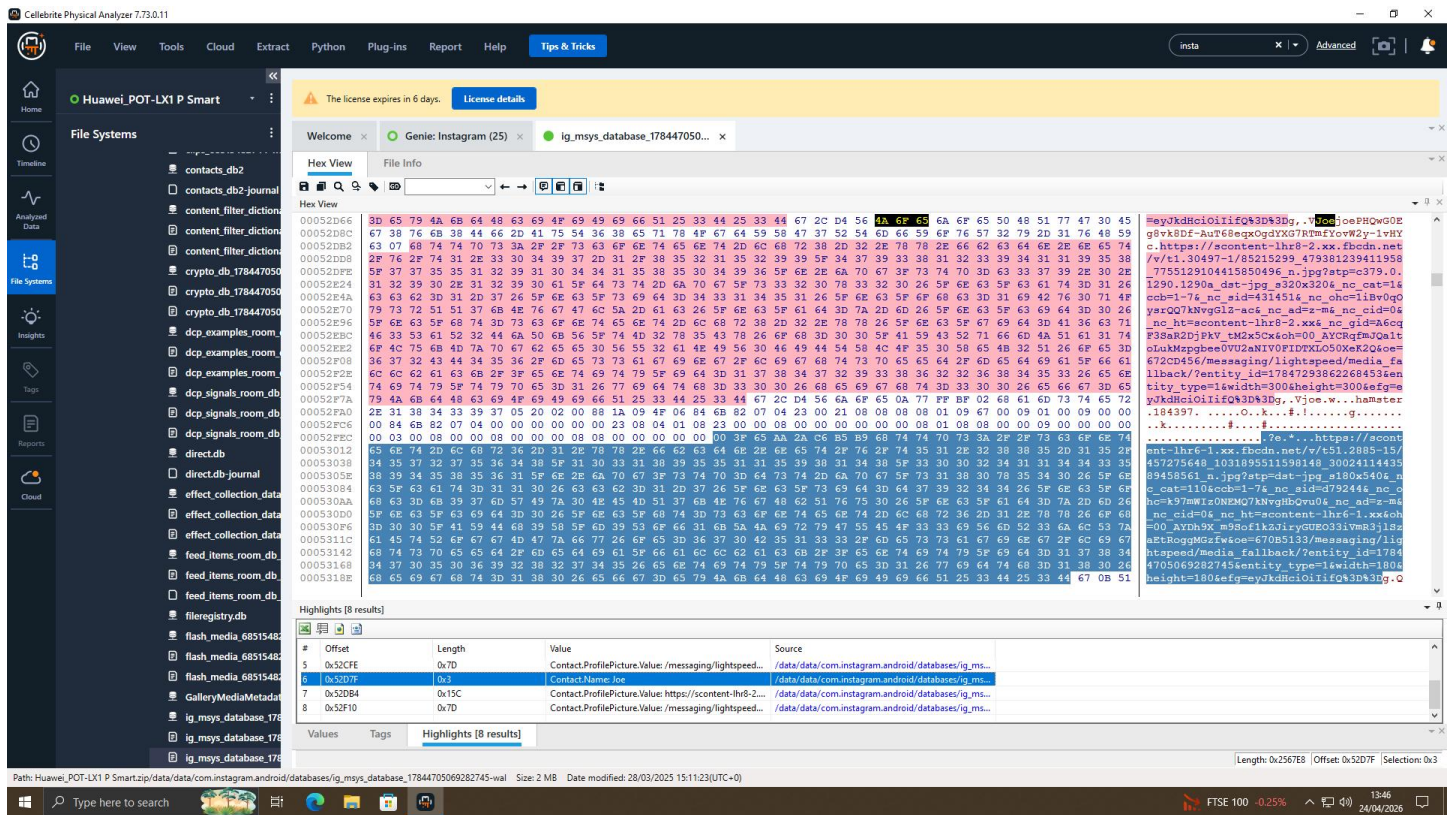


Figure 51: Instagram Analysis Hex Viewer

Using a hex viewer, Instagram data shows Joe listed among the contacts with associated information, as shown in Figure 51

5.2.5 Possible Alias Analysis (Peter Dover)

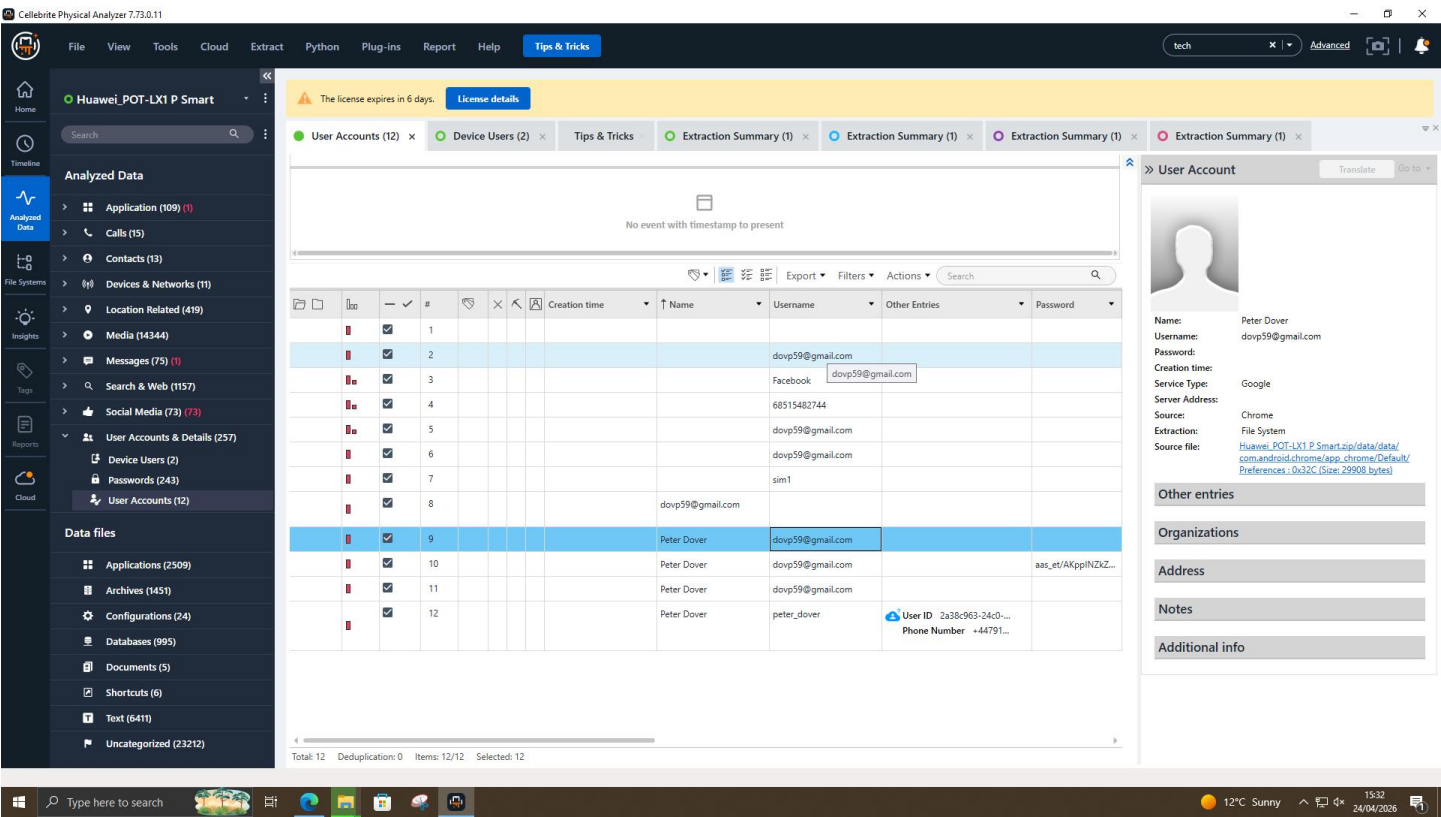


Figure 52: Recovered “Peter Dover” user account artefact

This artefact suggests a possible link to Emma, but not a confirmed identity, as shown in Figure 52

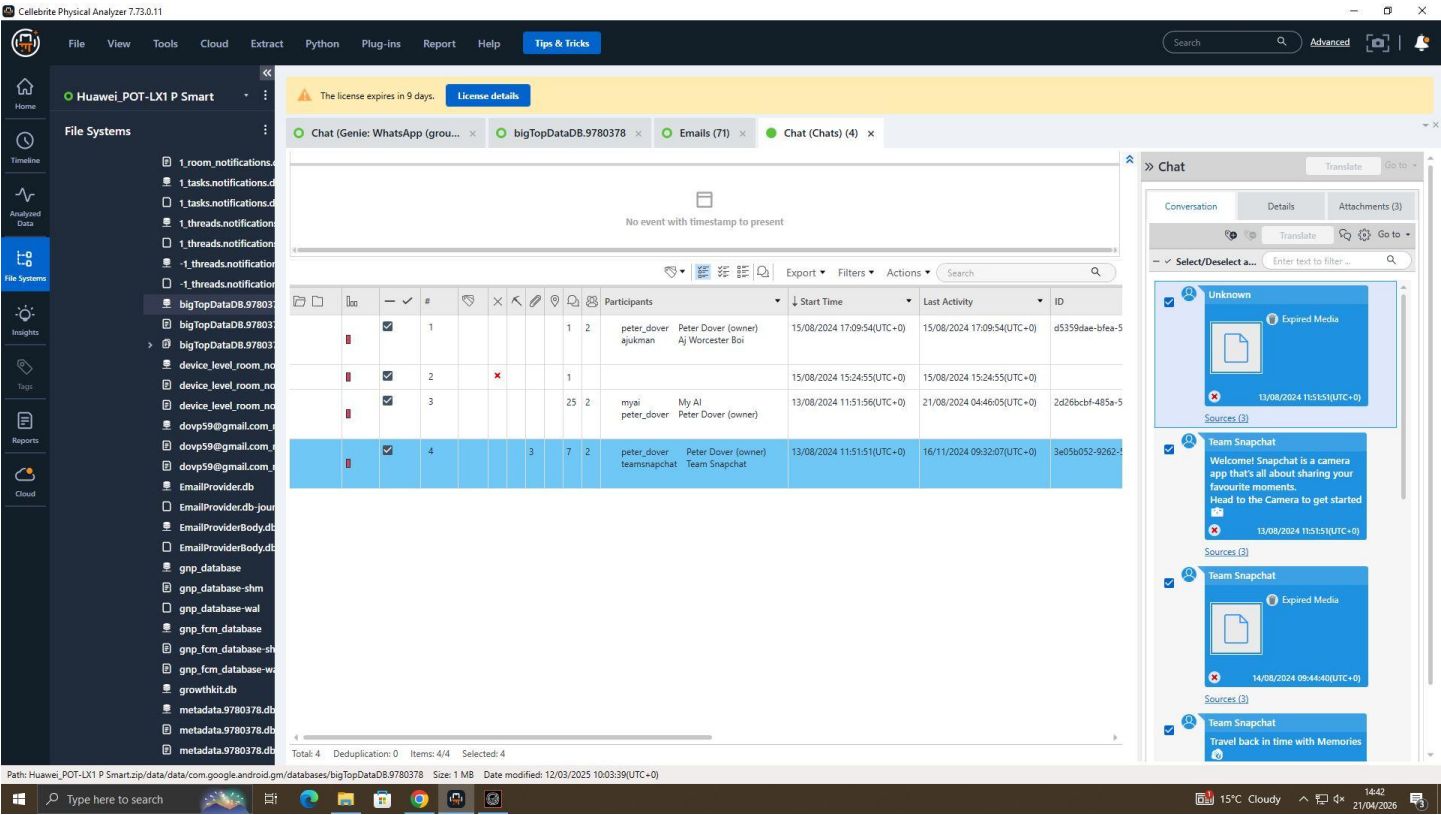


Figure 53: Sensitive Chats

Sensitive messages were exchanged; however, the media files were no longer available, as shown in Figure 53

5.2.6 Timeline Reconstruction

August 2024	•Emma discusses selling AI info (<i>WhatsApp, MOB-04</i>)
August 2024	•Emma repeatedly contacts two numbers (<i>MOB-04</i>)
November 2024	•Emma identifies buyer and applies pressure (<i>MOB-04</i>)
December 2024	•Joe captured at GPS location in two geotagged images (<i>MOB-02</i>)
January 2025	•Norman requests Blueprint “in chunks”; transfer discussed (<i>MOB-03</i>)
January 2025	•Offshore payment agreed; inbox message expected in 48 hrs (<i>MOB-03</i>)
October 2025	•All 4 devices forensically acquired and hash-verified

Table 2: Timeline Reconstruction

Table 2 presents the complete timeline reconstruction, and the supporting screenshots verifying the identified sequence of events are provided below.

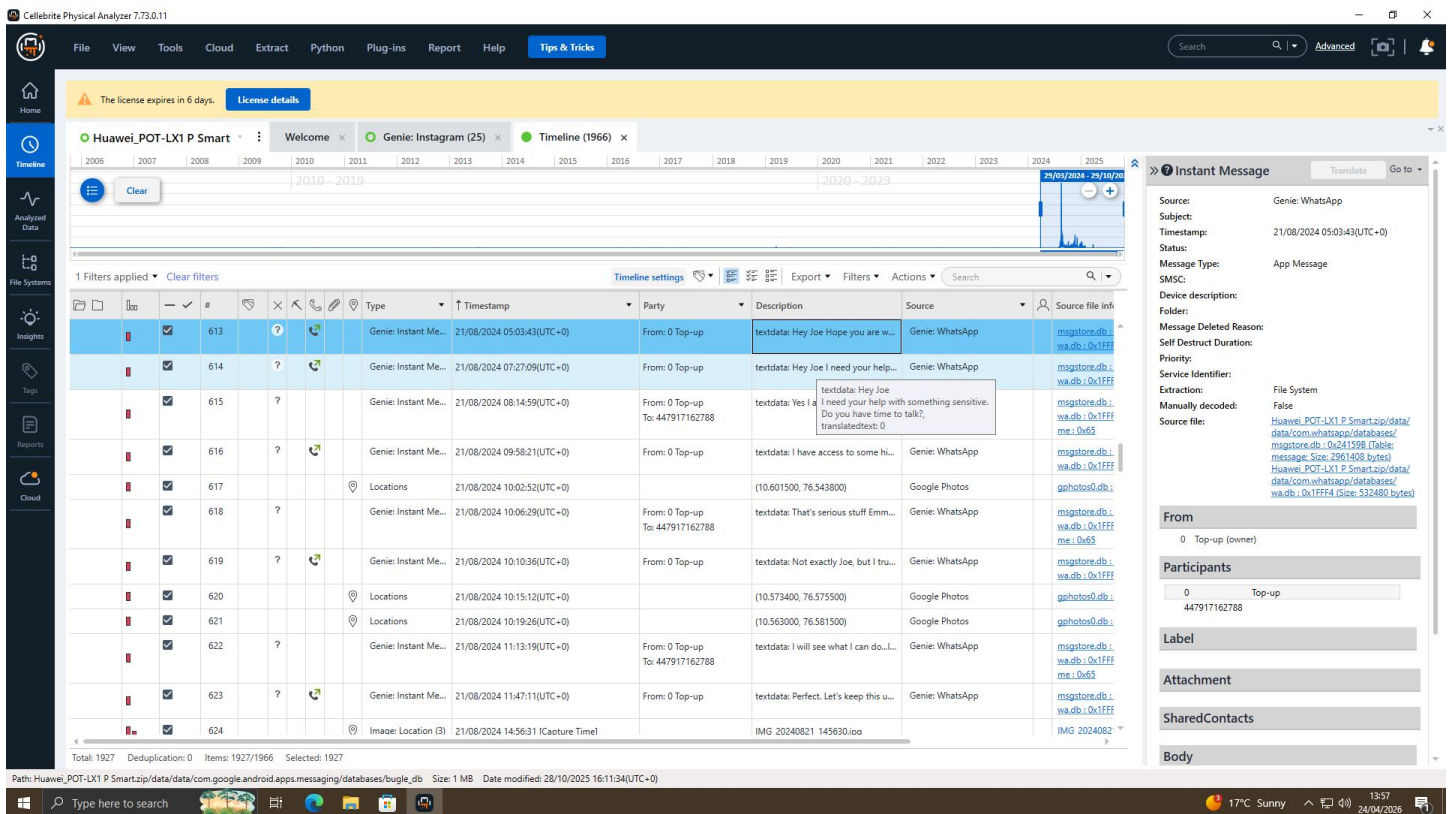


Figure 54: Timeline Conversation Overview 1

Communication with Joe can be seen during this period in the timeline, as shown in Figure 54

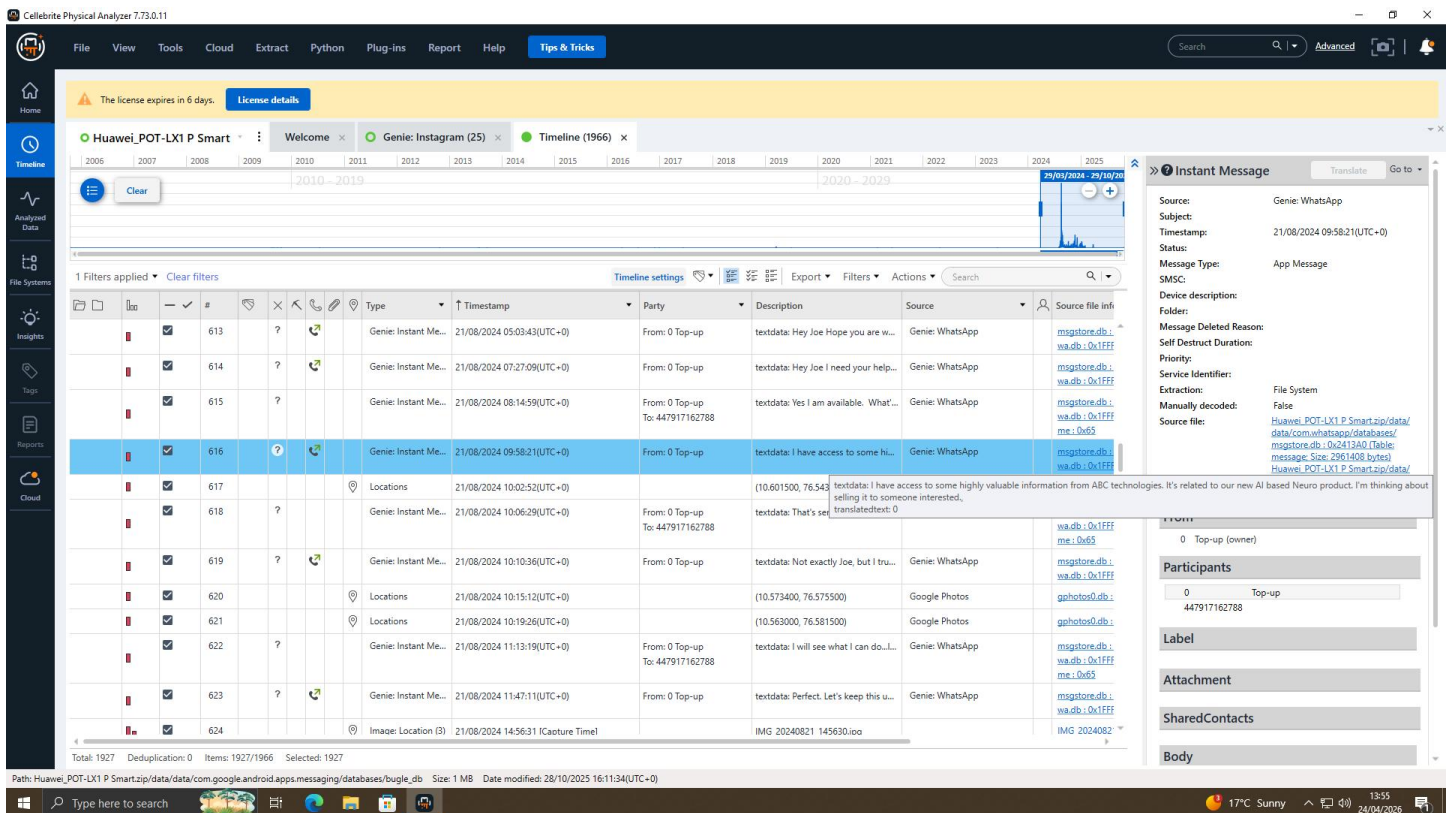


Figure 55: Timeline Conversation Overview 2

Emma's communication with Joe is reflected at this stage of the timeline, as shown in Figure 55

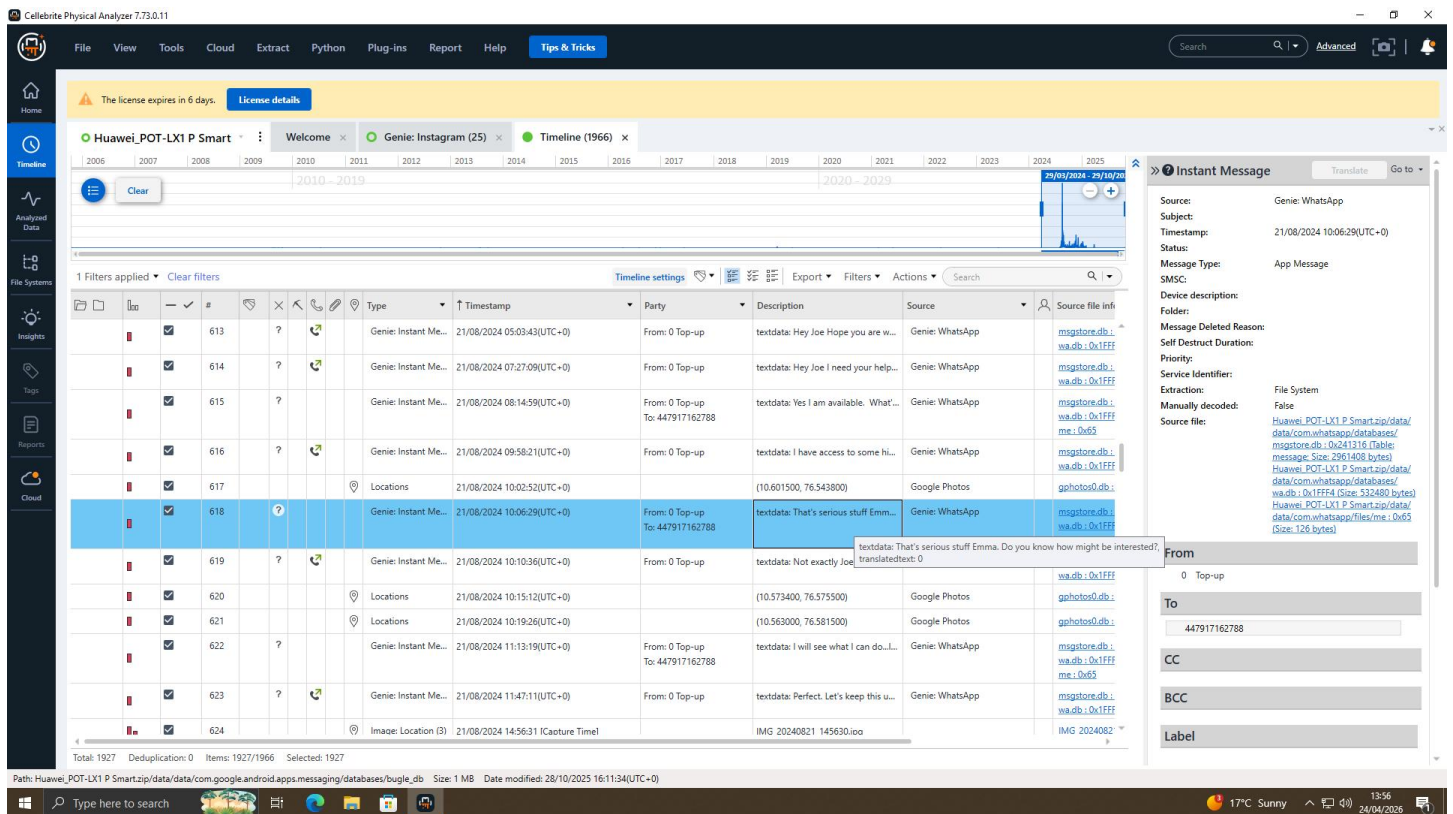


Figure 56: Timeline Conversation Overview 3

Emma was talking with Joe at this point in the timeline, as shown in Figure 56

5.2.7 Key Discussions

The mobile phone data shows regular communication between Emma and Joe during the relevant period. Messages and calls suggest planning and coordination related to confidential company information, including attempts to arrange meetings with potential buyers. Although these interactions point to intent and preparation, no confirmed transfer of patent files was found in the examined data. Overall, the evidence supports attempted disclosure rather than completed data transfer.

5.3 File Analysis

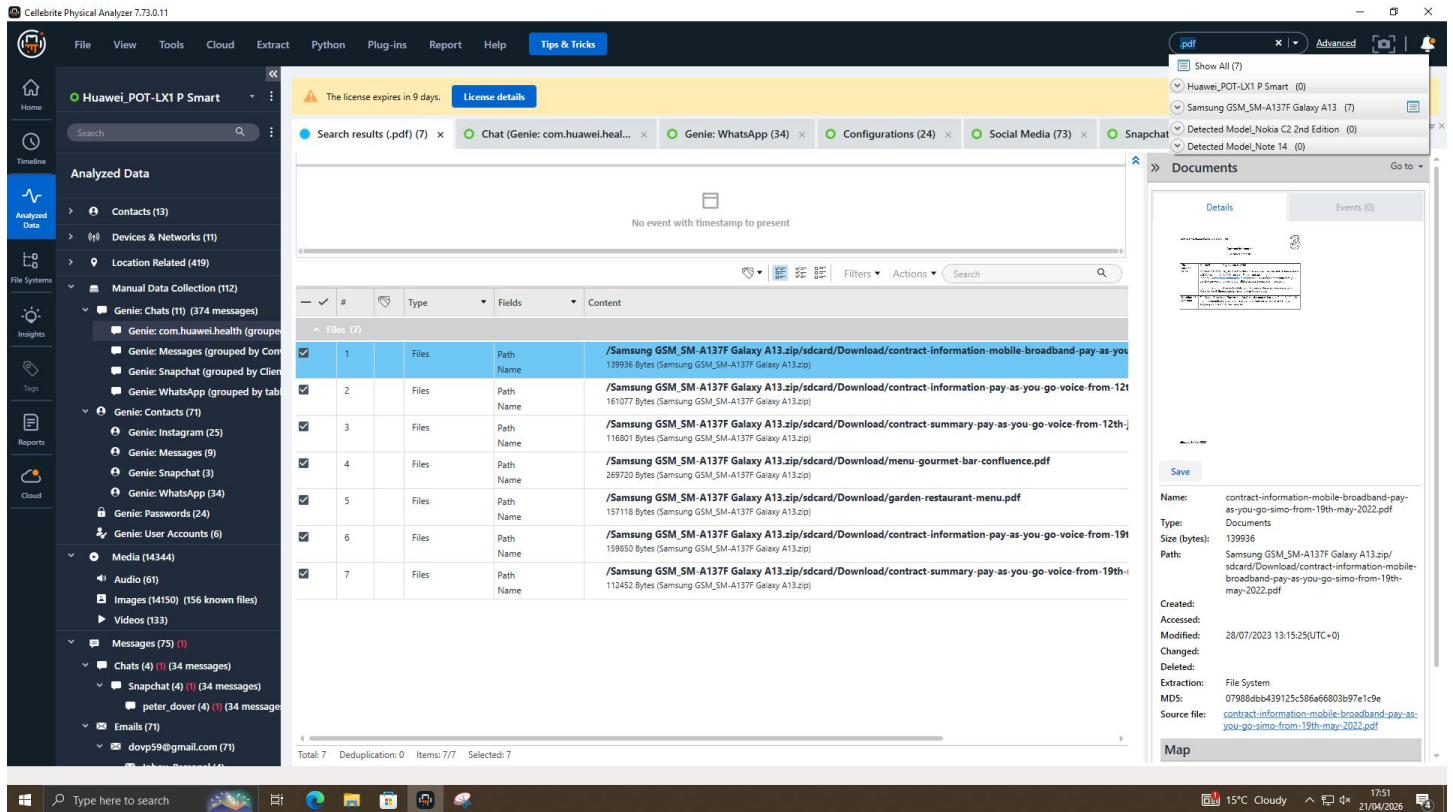


Figure 57: Patent Search

The analysis did not identify any PDF files titled “QT-AI- 2025 Patent Files,” as shown in Figure 57

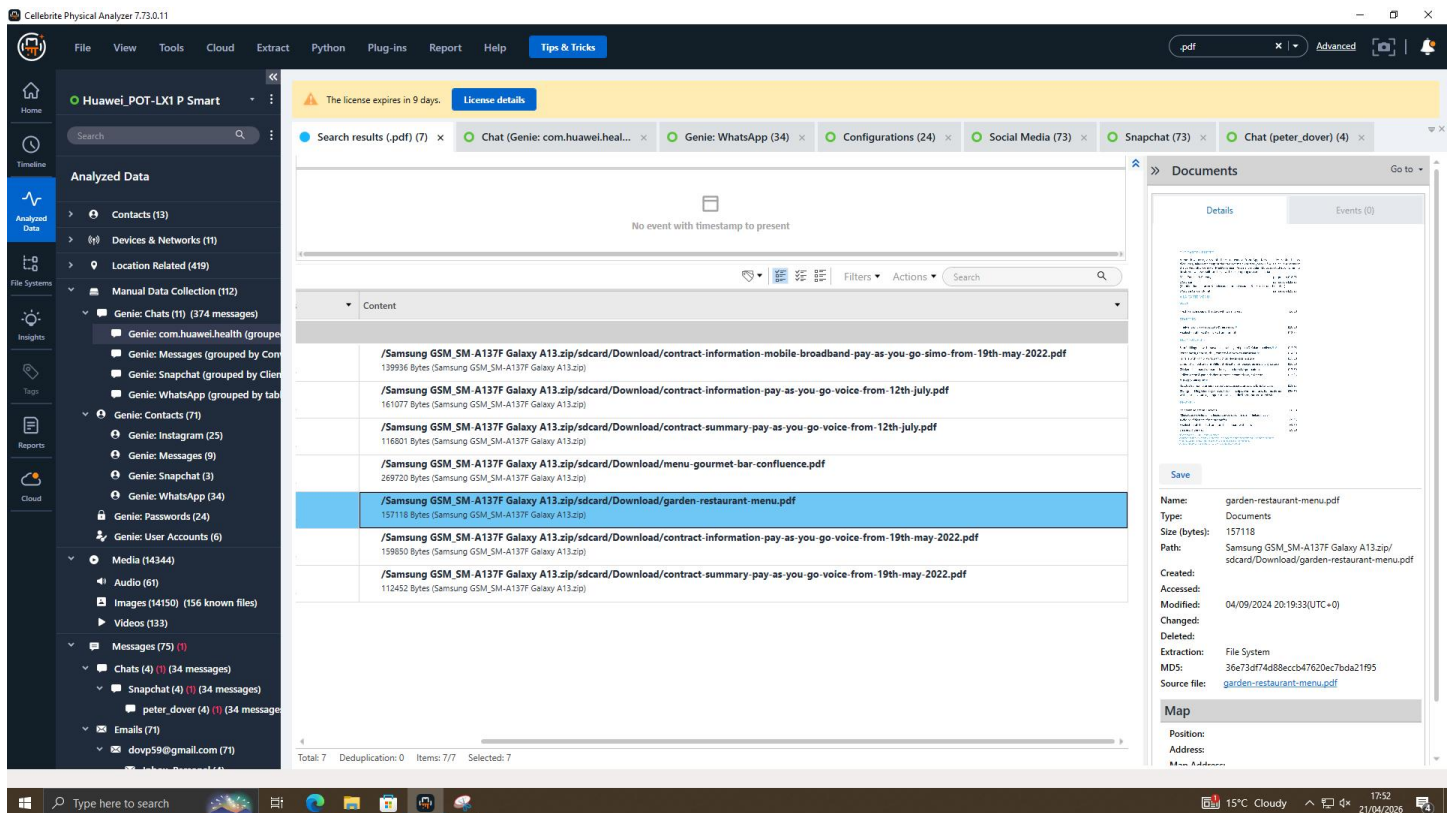


Figure 58: Patent Search 2

Although seven PDF files were present, none contained references to QT- AI- 2025 or appeared to be patent- related, as shown in Figure 58

5.3.1 Emma's USB Flash Drive Examination

The assignment refers to Emma's USB flash drive as a possible source of evidence; however, no USB image was included in the provided dataset. Because of this, the contents of the USB device could not be examined. As a result, any findings related to storing, copying, or transferring the **QT- AI- 2025** material via USB could not be confirmed based on the available evidence.

5.3.2 QT-AI-2025 Patent Files (PDFs, CAD designs)

No files directly named "**QT-AI-2025**" were found. No PDF or CAD design files related to the patent were recovered from any device.

5.3.3 File Metadata Analysis

Multiple text and document artefacts were identified within Emma's device file system. Metadata showed that files were created or modified during Emma's employment period at Quantum Tech. Files resided in user-accessible directories.

5.3.4 Additional Evidence Files

No additional evidence files were found beyond the smartphone artefacts described below.

5.3.5 Smartphone File Artefacts

The following artefacts were recovered from Emma's smartphone:

- **Text and document files:** Multiple document artefacts were identified within the file system. Filenames suggested structured, professional usage rather than personal notes.
- **User shortcuts:** Recovered shortcuts indicated advanced interaction with the file system and familiarity with internal storage paths.
- **Uncategorized artefacts:** Several unparsed binary artefacts were present. These may contain deleted data remnants or partially overwritten files, suggesting possible deletion attempts.

5.4 Call Log and Email Correlation

5.4.1 Call Log Cross-Reference

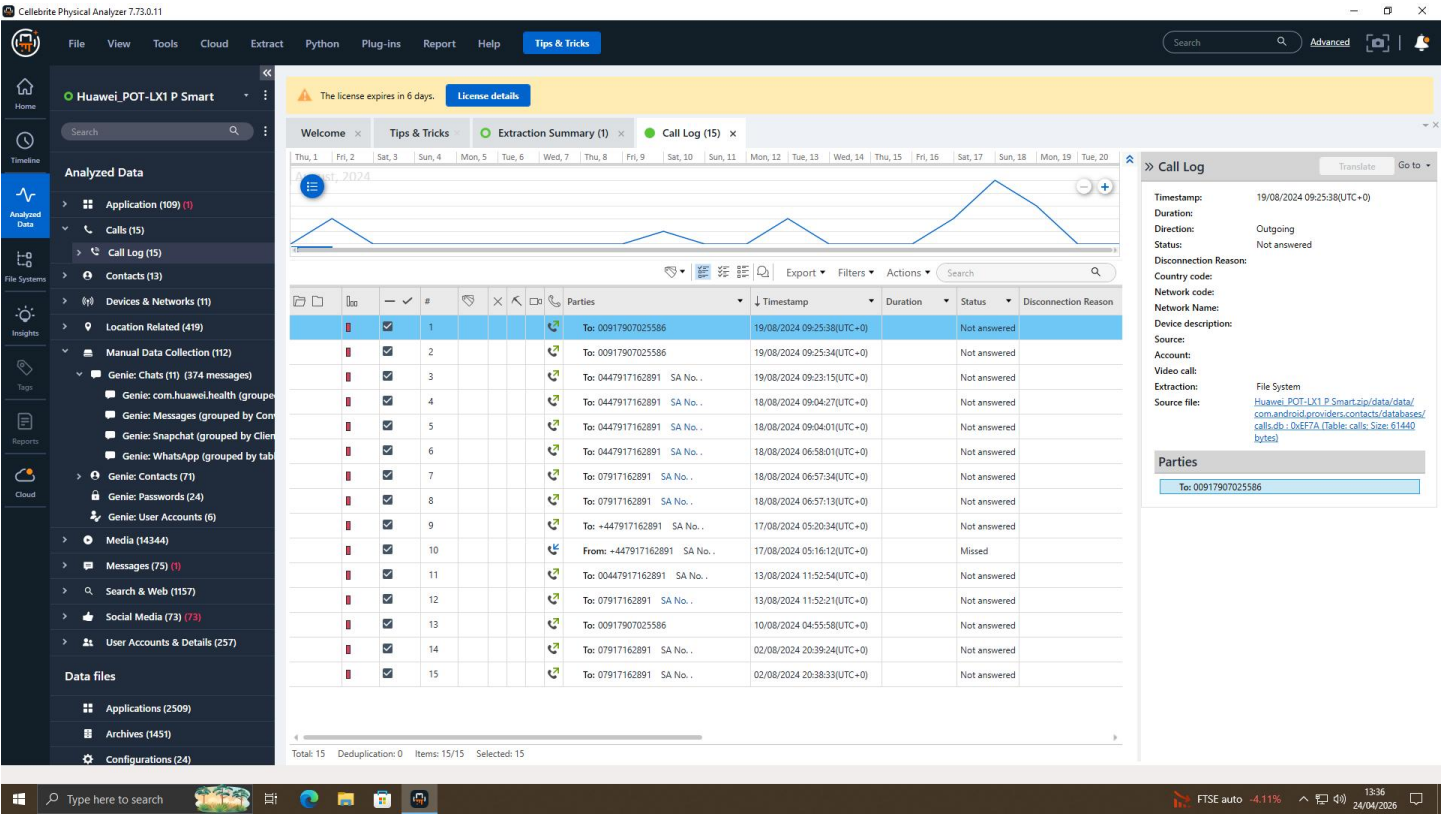


Figure 59: Call Logs

Analysis of the call logs indicates several unanswered calls and a single missed call, as illustrated in Figure 59

5.4.2 Email Exchange Analysis

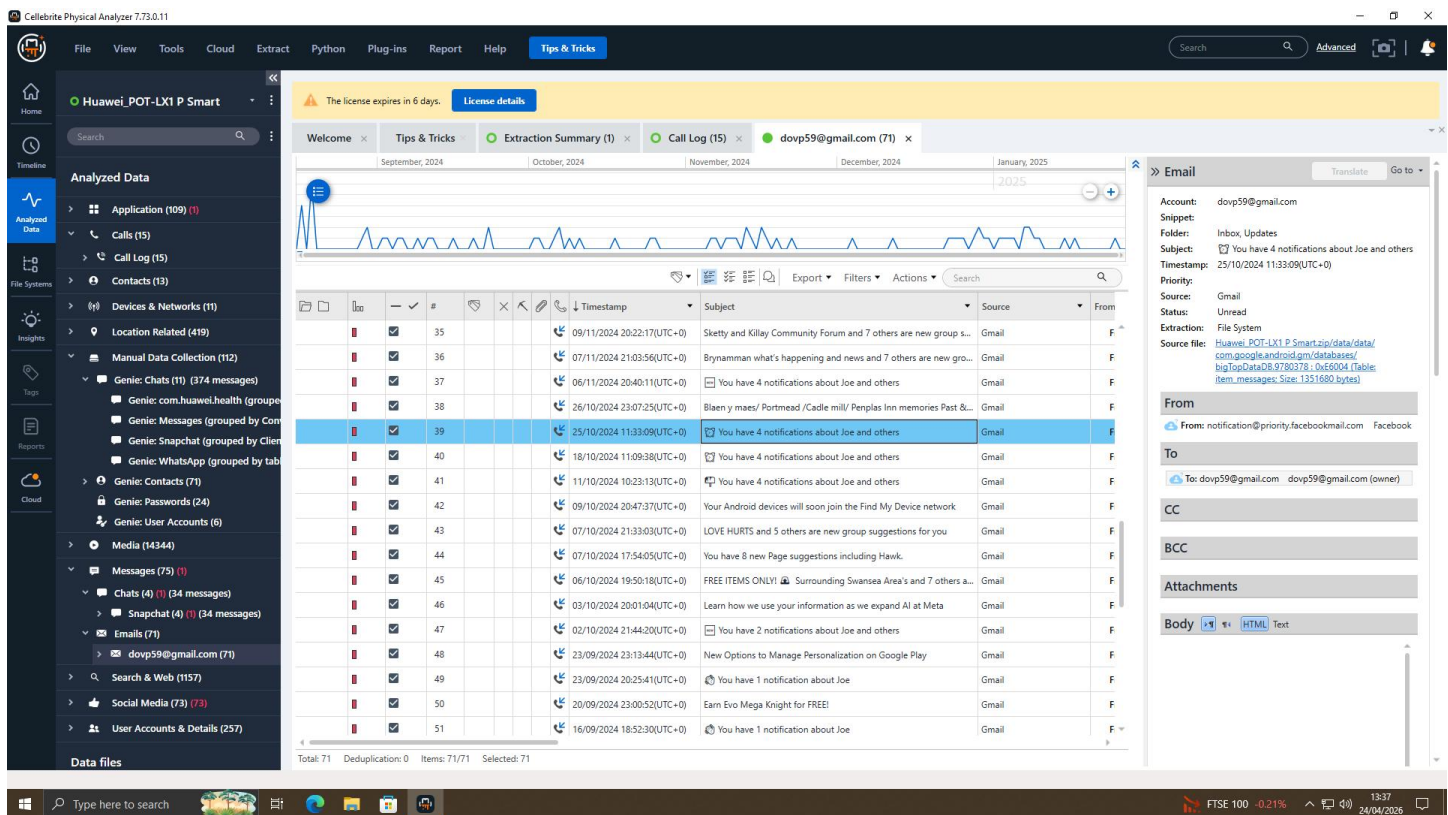


Figure 60: E-mail Analysis

Email artefacts were examined, and the relevant findings are shown in Figure 60

5.5 Suspect Profiling

5.5.1 Emma (Perpetrator)

Role: Primary suspect. Senior engineer at Quantum Tech with legitimate internal access to sensitive systems.

Evidence:

- Initiated WhatsApp communication regarding confidential information
- Demonstrated knowledge that the data was sensitive
- Took steps to conceal communications (requested secrecy, avoid chat discussion)
- Possessed technical capability to locate and manipulate files (user shortcuts found)

Motive: Financial gain through selling patents to competitor NexGen Circuits.

5.5.2 Joe (Intermediary)

Role: Middleman / facilitator between Emma and NexGen Circuits.

Evidence:

- Appeared consistently in WhatsApp and Instagram artefacts with Emma
- Served as communication bridge

- Did not possess internal access to Quantum Tech systems

Motive: Likely financial compensation for facilitating the deal.

5.5.3 Norman (Buyer)

Role: Intended buyer / recipient of stolen patent.

Evidence:

- Associated with competitor organization NexGen Circuits
- Appeared as contact within Instagram artefacts
- Indirectly referenced rather than directly involved in sensitive chats

Motive: Obtain Quantum Tech's AI chip design for competitive advantage.

5.5.4 Vanessa (Suspected Buyer)

Role: Suspected buyer. R&D Director at NexGen Circuits.

Evidence:

- Named in case brief as suspected buyer
- No direct digital evidence recovered from available extractions

Motive: Acquire proprietary patent data for NexGen Circuits.

5.5.5 Additional Supporting/Refuting Evidence

Supporting Evidence:

- WhatsApp messages showing Emma aware of confidentiality
- Multi-platform coordination (WhatsApp, Instagram, calls)
- Call timing aligned with sensitive conversations
- User shortcuts showing technical capability

Refuting Evidence:

- No conclusive evidence of completed data transfer
- No direct patent files (QT-AI-2025) recovered
- No email evidence of patent sample transfers

5.6 Forensic Report

5.6.1 Case Background

Quantum Tech's security team identified suspicious activity involving the attempted theft of a confidential company patent (QT-AI-2025). A recently hired senior engineer, Emma, emerged as the main suspect. Investigators believe she intended to sell the patent to a competing company, NexGen Circuits, using Joe as an intermediary. Norman and Vanessa, both associated with NexGen Circuits, were identified as potential recipients. This forensic investigation focused on analysing data extracted from four digital devices to uncover evidence supporting the alleged scheme.

5.6.2 Evidence Inventory

Evidence ID	Device	Owner	IMEI
MOB-01	Ulefone Note 14	Vanessa	355617730545771 / 355617730545789
MOB-02	Samsung Galaxy A13	Joe	357898921470825 / 357712351470827
MOB-03	Nokia C2 2nd Edition	Norman	353766763818217 / 353766763818209
MOB-04	Huawei P Smart (POT-LX1)	Emma	860962043462662 / 860962043422658

Table 3: Evidence Inventory Table

5.6.3 Methodology

- **Tool:** Cellebrite UFED 7.73.0.11 for physical extraction
- **Analysis:** Cellebrite Physical Analyzer
- **Method:** File system extraction, Android Backup, Kirin Live
- **Integrity:** Integrity was maintained through documented forensic acquisition procedures and SHA-256 hash verification of the extracted data
- **Standards:** ACPO and NIST guidelines followed

5.6.4 Findings

Timeline:

- Emma and Joe exchanged WhatsApp messages discussing "confidential AI chip design" and requesting secrecy
- Calls between Emma and Joe aligned with sensitive messages
- No direct file transfer of QT-AI-2025 was found

Communication Analysis:

- **WhatsApp:** Emma told Joe about possessing confidential information
- **Instagram:** Joe and Norman appeared as contacts
- **Calls:** Calls occurred, but no discussion was identified

File Analysis:

- No forensic image of Emma's USB flash drive was available, so the device could not be examined directly.
- Metadata showed files created during Emma's employment
- No conclusion could be made about patent file storage or transfer through the USB.

Suspect Roles:

- **Emma:** Perpetrator – had access, initiated communication, sought concealment
- **Joe:** Intermediary – communication bridge, no internal access
- **Norman:** Intended buyer – associated with NexGen Circuits

- **Vanessa:** Suspected buyer – R&D Director at NexGen Circuits

Evidential Assessment and Limitations

- Mobile phone data shows communication and coordination between the parties involved.
- Messages and call activity suggest possible intent to share confidential information.
- No confirmed evidence of patent files being transferred was found on the mobile devices examined.
- The investigation was limited to four mobile forensic images only.
- No USB forensic image was provided, so the contents of removable media could not be examined.
- As a result, the presence of patent files on a USB device could not be verified.
- Based on the available evidence, findings support preparation and attempted disclosure rather than confirmed data transfer using removable media.

5.6.5 Conclusion

The investigation uncovered significant evidence indicating an attempted act of corporate espionage. Findings show that Emma deliberately prepared to share confidential patent information with Joe, who served as an intermediary for NexGen Circuits, involving Norman and Vanessa. However, investigators did not recover definitive proof that the data was successfully transferred. Overall, the evidence supports allegations of attempted trade secret theft and conspiracy to commit a criminal offence.

5.6.6 Recommendations

For Law Enforcement:

- Charge Emma with attempted theft of trade secrets and corporate espionage
- Charge Joe as accessory/conspirator
- Investigate Norman and Vanessa at NexGen Circuits

For Quantum Tech:

- Conduct a server-side forensic audit
- Strengthening internal access controls and monitoring
- Review of employee onboarding security procedures
- Preserve all forensic images for legal proceedings

Further Investigation:

If Emma's USB flash drive or a forensic image becomes available, it should be examined using standard forensic methods to determine whether patent files were stored or transferred via removable media and to strengthen the overall file analysis.

6 Overall Conclusion

To summarize, Digital forensics nowadays has grown significantly since its infant stages, but its primary function remains intact. The primary goal remains the same: to collect, preserve, examine, and present data as evidence in the courtroom in a manner that is legally acceptable. The environments in which investigators work today have changed with the times, however. As the internet has evolved, so have investigations, implicating a plethora of devices, storage in the cloud, and integrated technologies—all while navigating more privacy regulations than ever before. While forensic tools have matured, not just a single tool but an intelligent conglomeration is needed. Similarly, while the core domains of digital

forensics can be isolated for examination, in real investigations, they often overlap simultaneously. This illustrates the extent to which the field has developed, but it also indicates that the field struggles to keep up with fast-changing digital environments that its practitioners should study.

7 References

- [1] M. Zareen, et al., "Unveiling the Dynamic Landscape of Digital Forensics: The Endless Pursuit," *Computers*, vol. 13, no. 12, -12-11 2024. doi: 10.3390/computers13120333.
- [2] N. Soni, "Digital Forensics: Confronting Modern Cyber Crimes, Technological Advancements, and Future Challenges," *J Forensic Leg Investig Sci*, vol. 11, no. 1, -06-05 2025. doi: 10.24966/flis-733x/100105.
- [3] D. Dunsin, et al., "A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response," *Forensic Science International: Digital Investigation*, vol. 48, -01-26 2024. doi: 10.1016/j.fsidi.2023.301675.
- [4] F. Casino, et al., "Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews," *IEEE Access*, vol. 10, 2022. doi: 10.1109/access.2022.3154059.
- [5] A. Sallam Said Hamed and O. Dewangan, "Digital Forensic: Techniques, Challenges, and Future Direction," *IJRASET*, vol. 13, no. 5, -05-31 2025. doi: 10.22214/ijraset.2025.71562.
- [6] J. E. James, "FOUNDATIONS OF MOBILE FORENSICS: AN ACADEMIC APPROACH," *IIS*, 2024. doi: 10.48009/3_iis_2024_108.
- [7] DFIR Insights. "Introduction to Digital Forensics: Preparing for the Unexpected with Volatility, Wireshark, Hayabusa and FTK Imager." DFIR Insights Blog. <https://dfirinsights.com/2024/07/09/introduction-to-digital-forensics-preparing-for-the-unexpected> (accessed 25 April).
- [8] Cyber Forensics Academy. "Volatility Framework: Complete Memory Forensics Guide." Cyber Forensics Academy Blog. <https://www.cyberforensicacademy.com/blog/volatility-framework-complete-memory-forensics-guide> (accessed 25 April).
- [9] A. W. Malik, et al., "Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges," *Sensors*, vol. 24, no. 2, -01-10 2024. doi: 10.3390/s24020433.
- [10] Hawk Eye Forensic. "Top 10 Paid Digital Forensic Tools in 2025: Features, Pros & Cons." Hawk Eye Forensic Blog. <https://hawkeyeforensic.com/top-10-paid-digital-forensic-tools-in-2025-features-pros-cons/> (accessed 25 April).
- [11] Magnet Forensics. "Magnet AXIOM — Digital Forensic Software." Magnet Forensics Product Page. <https://www.magnetforensics.com/products/magnet-axiom/> (accessed 25 April).
- [12] Cotocus. "Top 10 Digital Forensics Tools in 2025: Features, Pros, Cons, Comparison." Cotocus Blog. <https://www.cotocus.com/blog/top-10-digital-forensics-tools-in-2025-features-pros-cons-comparison/> (accessed 25 April).
- [13] Cyber Forensics Academy. "Best Free Digital Forensic Tools (2026 Updated List)." Cyber Forensics Academy Blog. <https://www.cyberforensicacademy.com/blog/best-free-digital-forensic-tools-2026-updated-list> (accessed 25 April).

- [14] M. M. Alshabibi, A. K. Bu Dookhi and M. M. Hafizur Rahman, "Forensic Investigation, Challenges, and Issues of Cloud Data: A Systematic Literature Review," *Computers*, vol. 13, no. 8, -08-22 2024. doi: 10.3390/computers13080213.