



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

**Research, Analyse and Investigate Corporate
Cybersecurity Incidents through Digital Forensic
Assessment**

Student Name & ID: Patel Vinay Bhikhabhai (2519364)

Module Code: ACFA7031

Module Name: Digital Forensics Analysis

Course: MSc Cyber Security and Digital Forensics

LECTURER: Dr. Mohamed Ghanem

Task 1

TABLE OF CONTENTS (Task 1)

Table of Contents

- 1. Introduction
- 2. The Evolution and Current Landscape of Digital Forensics
- 3. Analysis of Digital Forensic Tools and Technologies
- 4. Integration of Digital Forensics with Cybersecurity
- 5. Future Trends in Digital Forensic Investigations
- 6. Current Issues in Digital Forensics
- 7. Employment Trends in Digital Forensics
- 8. Conclusion
- 9. References

List of Figures

Figure No.	Figure Title
Figure 1	Stages of a Digital Forensic Investigation
Figure 2	Overview of Digital Forensic Software Tools
Figure 3	The Role of Digital Forensics in Cybersecurity Operations
Figure 4	Recent Innovations in Digital Forensic Technologies
Figure 5	Current Issues Affecting Digital Forensic Investigations

1.Introduction

Digital forensics is a highly important field that helps in investigating the cybercrimes through identifying, collecting, analysing, and presenting the digital evidence in a legally acceptable way. Due to the increased cybercrimes like data breach, ransomware, and insider threat, organizations make use of digital forensics for investigating incidents and taking legal action against them.



Figure 1: Stages of a Digital Forensic Investigation

Digital forensics is also highly important in the context of increasing the level of cybersecurity by understanding the security threats and preventing them in the future. The current report discusses the status quo of digital forensics, digital forensics tools, digital forensics and cybersecurity, upcoming trends, major challenges, and career opportunities.

2. The Evolution and Current Landscape of Digital Forensics

In recent years, digital forensics has become an important part of contemporary cybersecurity owing to an upsurge in cybercrimes and increased adoption of digital technology. Digital forensics is the practice of scientifically examining digital devices in order to identify, protect, gather, analyse and submit electronic evidence in a way that is acceptable in a court of law. In today's world, there are different kinds of digital forensic investigations performed depending on the type of crime committed, including computer forensics, mobile device forensics, network forensics, cloud forensics, and memory forensics.

The development of new technologies, including cloud computing, smartphones, and Internet of Things (IoT), has greatly impacted digital forensics and resulted in many new sources of digital evidence, thereby making the investigation process more complicated. However, forensic practitioners employ proven digital forensic methodologies that guarantee evidence integrity and involve acquisition, hash verification, analysis, and reporting among other procedures. The use of digital forensics is popular in investigating cybercrimes, cyberattacks, cyber fraud, insider threat, and intellectual property theft in both public and private sectors.

3. Analysis of Digital Forensic Tools and Technologies

There is some specialized software solutions used in digital forensic investigation process to collect, preserve, analyse, and report digital evidence. Digital forensic software solutions allow to recover the deleted files, analyse the file systems, communication history, and produce reports for further legal actions. Choice of the digital forensic software tool depends on the type of a device and operating system.

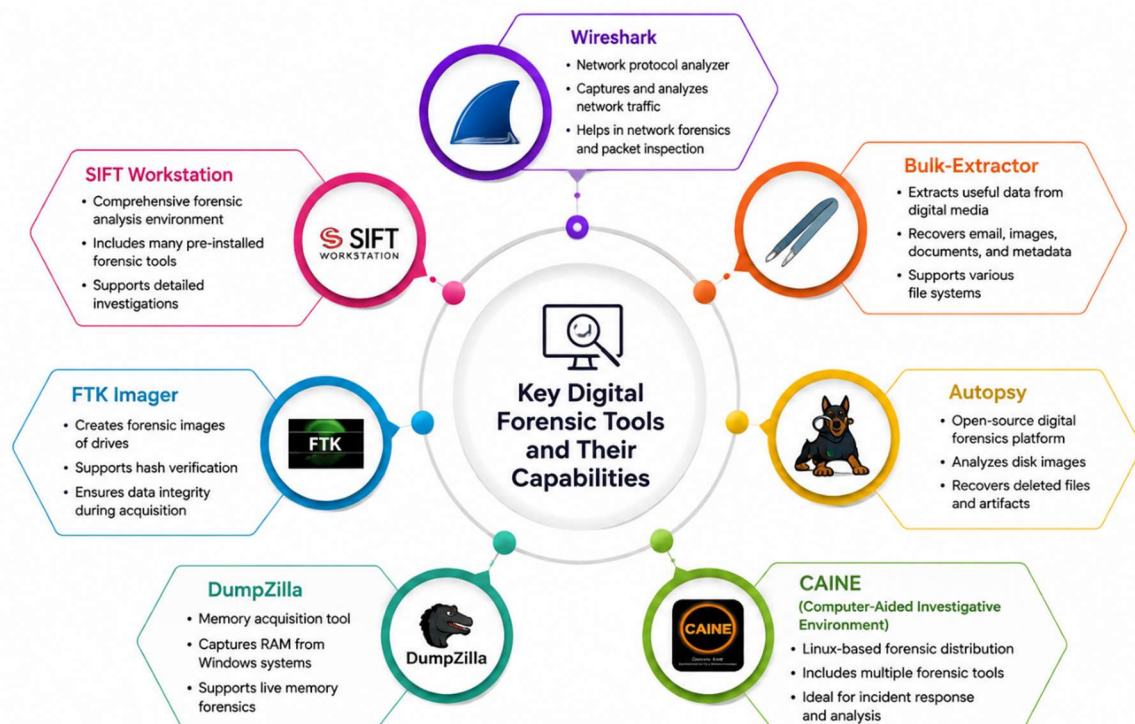


Figure 2: Overview of Digital Forensic Software Tools

Autopsy is one of the popular open-source digital forensics platforms, which allows to analyze digital forensics data by recovering the files, searching for keywords, producing timelines, and generating the hash values. FTK Imager is a common digital forensics software tool that helps to make forensic images of storage devices without any modification of the original data. EnCase is a commercial digital forensics product that allows to analyse the evidence, to generate reports, and work with a variety of file systems.

These forensic tools make the process of the investigations more efficient and accurate by automating evidence collection and analysis.

4. Integration of Digital Forensics with Cybersecurity

Cybersecurity and digital forensics are highly related to each other since both of these areas are concerned about the protection of the digital environment and information. Cybersecurity deals with the prevention of cyber-attacks through security controls implementation, whereas digital forensics deals with the investigation of cyber-attacks after their occurrence. During the investigation of a cybersecurity attack, digital forensics experts investigate such types of data as logs, network traffic, email messages, and other types of storage media. The results of digital forensics allow organizations to develop stronger security measures in order to prevent similar attacks in the future.

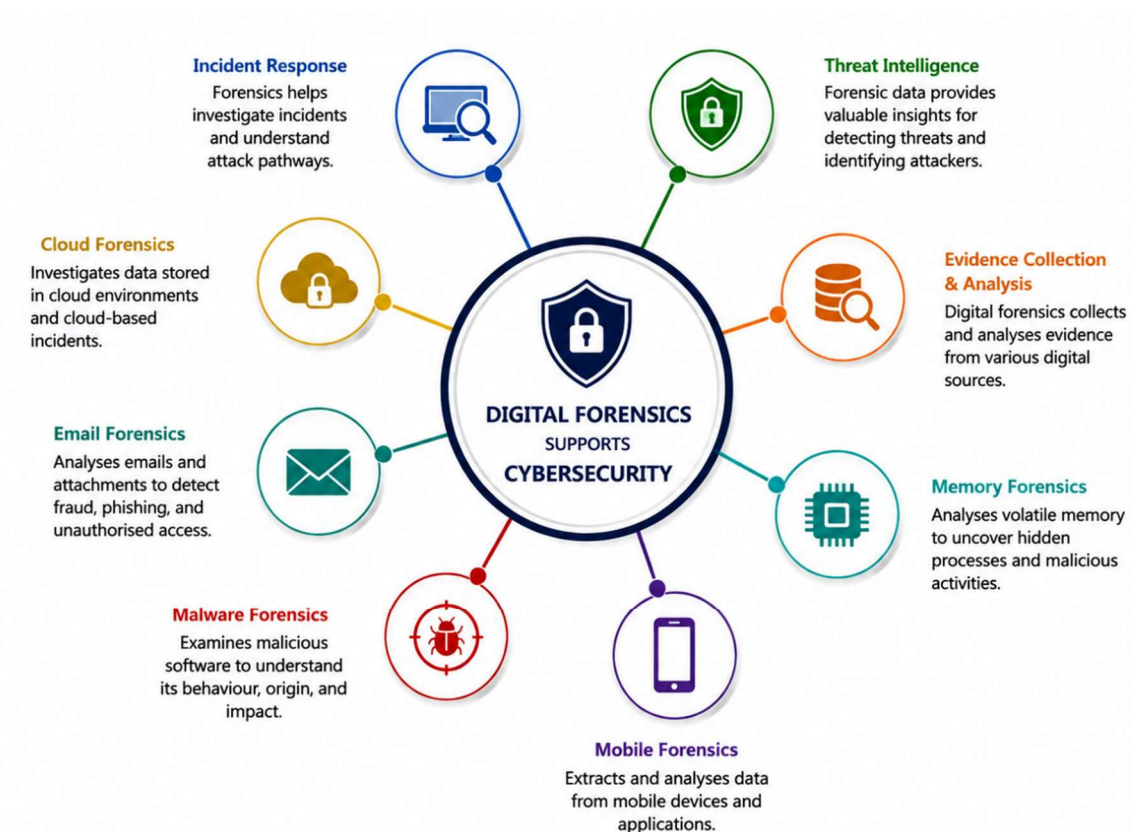


Figure 3: The Role of Digital Forensics in Cybersecurity Operations

Besides, digital forensics is a source of information that may be used in criminal cases or lawsuits. Thus, the combination of cybersecurity and digital forensics allows responding to cyber incidents effectively.

5. Future Trends in Digital Forensic Investigations

The digital forensics industry is continuously changing because of constant developments in technology and growing complexities of the cybercrime itself. The trend that is becoming very popular among investigators nowadays is the utilization of artificial intelligence and machine learning to analyse the evidence, detect the suspicious activity and speed up the whole process of investigation. It also became a very important area to study the topic of cloud forensics, since many companies now use cloud computing to save their big amounts of data and have problems with collecting evidence and jurisdiction. Internet of Things (IoT) forensics also became a relevant topic as the investigators started working with the evidence from smart devices and wearables.

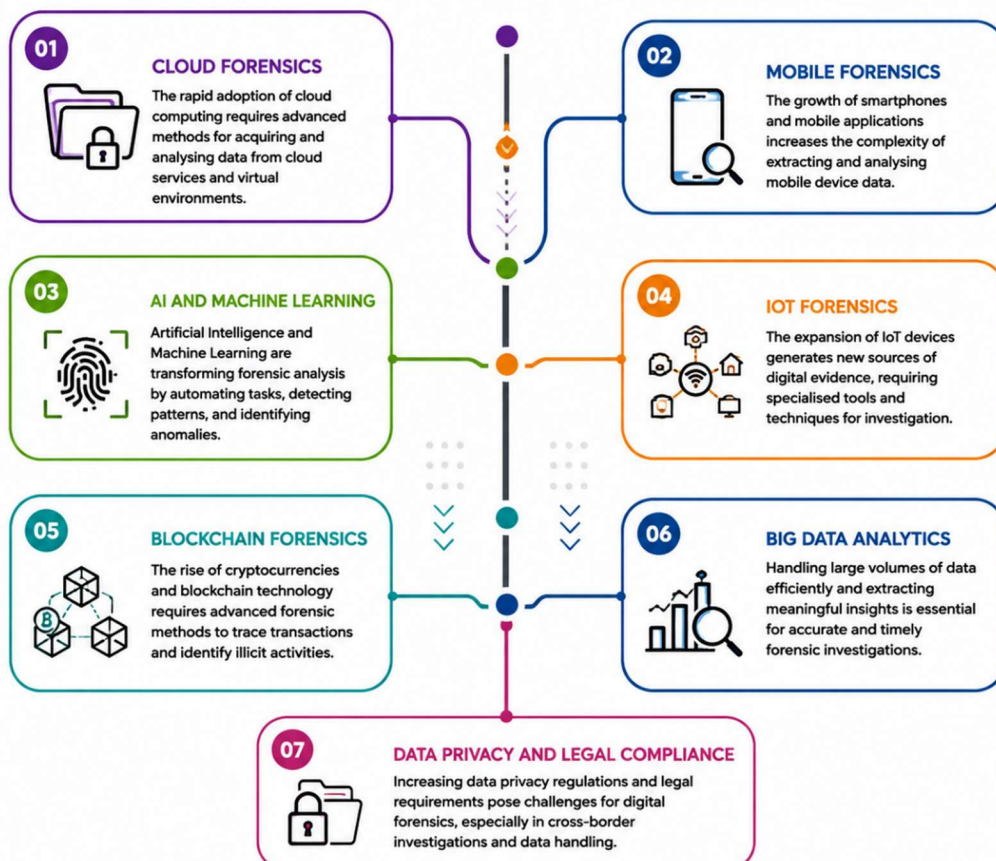


Figure 4: Recent Innovations in Digital Forensic Technologies

finally, blockchain and cryptocurrency investigations also turned out to be one of the important directions of digital forensics.

6. Current Issues in Digital Forensics

There are various issues in digital forensics as a result of technological and cyber threats advancements. One of the major issues is the encryption of user information which ensures protection of user data but at the same time it makes it hard for investigators to obtain digital evidence. The advancement of cloud computing causes even more issues since the data can be found in different places and therefore, obtaining the evidence can take time. Anti-forensic methods including the deletion of files, encryption, data wiping and others are used by cyber criminals as ways to cover the evidence and delay the investigation process. Moreover, a huge amount of data is collected and therefore, the time and the effort required to analyze it are considerable. Another issue is maintaining the integrity of the evidence during the whole process of investigation.

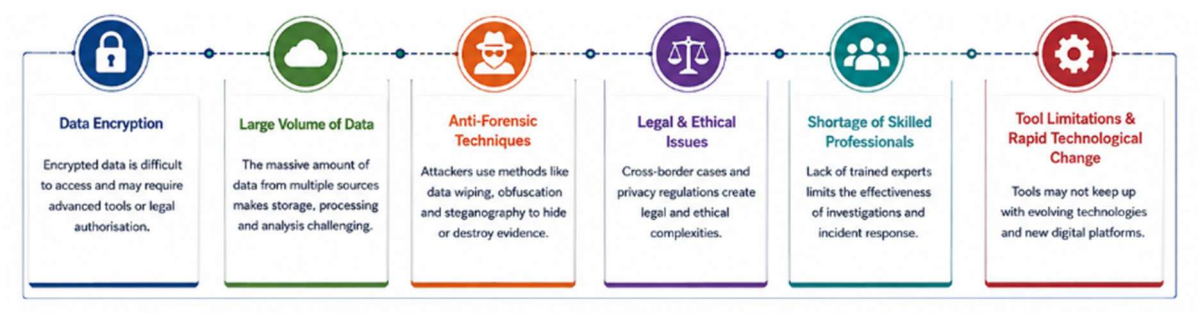


Figure 5: Current Issues Affecting Digital Forensic Investigations

7. Employment Trends in Digital Forensics

The need for digital forensics experts keeps increasing because cybercrimes keep on becoming increasingly frequent and complex. In the UK, as well as in many other nations, there are many organizations, including those that belong to law enforcement agencies, government departments, financial institutions, technology firms, and cybersecurity businesses that employ digital forensic experts and incident response experts. Some of the typical jobs in digital forensics include Digital Forensic Analyst, Cybercrime Investigator, Incident Response Analyst, Malware Analyst, and Security Consultant. It is common practice for employers to look out for individuals with good technical expertise and certification, such as EnCE, CHFI, GCFA, or Cellebrite certifications.

8. Conclusion

Digital forensics is an increasingly dynamic field, and it is very important for conducting investigations into cybercrimes and managing the security of computers. The development of technology in the field of forensics has positively impacted investigations, although challenges like encryption, cloud computing, and anti-forensics are still difficult problems to deal with. With the increasing cyber-crimes, the need for professionals in digital forensics is anticipated to rise.

IEEE References

- [1] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 3rd ed. Burlington, MA, USA: Academic Press, 2011.
- [2] B. Nelson, A. Phillips, F. Enfinger, and C. Steuart, *Guide to Computer Forensics and Investigations*, 6th ed. Boston, MA, USA: Cengage Learning, 2019.
- [3] National Institute of Standards and Technology, *Computer Security Incident Handling Guide (SP 800-61 Rev. 2)*. Gaithersburg, MD, USA: NIST, 2012.
- [4] NIST, *Cybersecurity Framework (CSF) 2.0*. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2024.
- [5] IBM Security, *Cost of a Data Breach Report 2024*. IBM Corporation, 2024.

Task 2 – Mobile Device Forensic Examination and Analysis Report

TABLE OF CONTENTS (TASK 2)

Section	Topic
1	Introduction
2	Tools and Environment
2.1	Forensic Tools Used
2.2	Laboratory Environment

Section	Topic
2.3	Devices Analysed
2.4	Examination Features
2.5	Evidence Inventory and Chain of Custody
3	Evidence Acquisition
3.1	Acquisition Process
3.2	Extraction Methods
3.3	Device Extraction Summary
3.4	Data Integrity and Verification
3.5	Practical Device Extraction and Validation
4	Examination Process
4.1	Overview of Examination
4.2	Contacts Analysis
4.3	Email Analysis
4.4	Application Analysis
4.5	Social Media Analysis
4.6	File System Analysis
4.7	Device Information Analysis
5	Analysis and Findings
5.1	Overview of Findings
5.2	Contact-Based Evidence
5.3	Email Communication Findings
5.4	Application Usage Insights

Section	Topic
5.5	Social Media Evidence
5.6	File System Findings
5.7	Device Correlation
5.8	Timeline Reconstruction
6	Conclusion
7	References

INDEX 2 — LIST OF FIGURES (TASK 2)

Figure	Figure Title
Figure 1	Cellebrite/forensic tool environment and overall examination setup
Figure 2	Practical Windows/Cellebrite forensic working environment
Figure 3	Device identification/information showing the examined handset
Figure 4	Case Wizard examination tools such as hash sets, carving, archive recovery and selective decoding
Figure 5	Extraction/evidence information suitable for documenting the evidence item
Figure 6	UFED device-detection/acquisition stage
Figure 7	UFED extraction/content selection demonstrating the extraction method
Figure 8	Extraction summary containing acquisition and device information
Figure 9	Hash/integrity verification evidence
Figure 10	Loading the acquired evidence into Physical Analyzer
Figure 11	Selective application decoding/examination configuration

Figure	Figure Title
Figure 12	Recovered native and application/Snapchat contacts
Figure 13	Email-related artefact/category evidence
Figure 14	Installed Applications view and application categorisation
Figure 15	Snapchat/social-media artefacts and recovered communications
Figure 16	Data-file/file-system/database-related forensic artefacts
Figure 17	Detailed handset/device information and identifiers
Figure 18	Additional contact evidence supporting relationships/identification
Figure 19	Detailed email-related findings
Figure 20	Installed-app/AppGenie evidence supporting application examination
Figure 21	Recovered social-media/chat evidence
Figure 22	Additional database/file-system findings
Figure 23	Location/device artefacts useful for cross-device or activity correlation
Figure 24	Timeline evidence showing chronological artefacts

1.Introduction

Mobile devices are now an increasingly important source of digital evidence as they hold a lot of data about communication, activity on the device, applications, browsing, multimedia files, geographical locations, and configurations of the device itself. Thus, forensic examination of mobile devices can help recover evidence that will assist in understanding how the device was used over the time period under consideration.

The aim of this task was to perform a forensic examination of evidence from mobile devices using Cellebrite forensic tools. The procedure included acquisition and importation of mobile device evidence, analysis of processed evidence using Cellebrite Physical Analyzer software, analysis of different types of artefacts, and evaluation of the evidential value of recovered data. Special emphasis was made on contacts, communications, applications, social media artefacts, file system information, geographical locations, and timeline information.

More than one Android device dataset was used for the practical part of the work. The screenshots below contain examinations carried out for the datasets of the Samsung and Huawei devices, whereas another analysed dataset can be seen on the Physical Analyzer screenshot below in the form of a detected Nokia C2 series device. One of the Samsung device extractions is identified in Physical Analyzer as Samsung GSM SM-A137F Galaxy A13, running Android 14. On the other hand, a separate UFED acquisition screen contains an identification of a Samsung GSM SM-A176B_DS Galaxy A17 5G as the extracted device. There are also screenshots of examination of a Huawei POT-LX1 P Smart dataset.

2. Tools and Environment

2.1 Forensic Tools Used

The two main software programs utilized for the practical exam included Cellebrite UFED and Cellebrite Physical Analyzer.

The Cellebrite UFED was employed for the extraction of the mobile device. The Cellebrite UFED offered various sources where one could extract data, ranging from the device itself to the SIM card and memory card. The extraction process offered various data categories that could be selected; these included:

- Call logs
- Locations
- Advertising ID
- Contacts

- SMS
- MMS
- Calendar
- Pictures
- Audio/music
- Videos
- Ringtones
- Documents
- Archives
- Email
- Instant messaging
- Browsing data
- User dictionary
- Files

However, all the categories were not present in the shown acquisition. Some were greyed out, reflecting one of the important characteristics of mobile forensics where the information available for acquisition depends on the device, OS, security status, and extraction procedure.

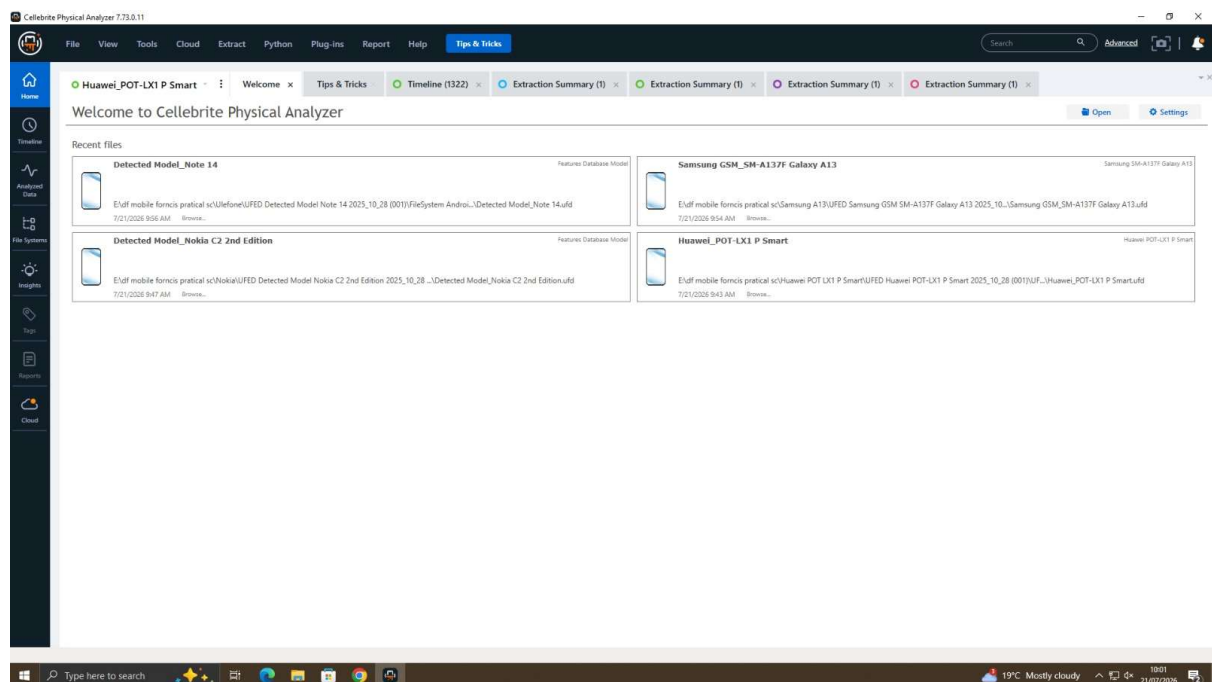


Figure 1: Cellebrite/forensic tool environment and overall examination setup

The main examination tool used in this investigation was Cellebrite Physical Analyzer 7.73.0.11 as shown in the attached screenshots. Physical Analyzer was employed to decipher the extracted mobile data and organize it into categories for further evaluation by the investigator.

The tool offered categories like applications, calls, contacts, devices and networks, location data, media, messages, search/web artefacts, social networking sites, user accounts, passwords, and underlying raw data files.

Physical Analyzer thus became the primary environment for analysis and examination of mobile artefacts derived from extracted mobile data.

2.2 Laboratory Environment

This test was done in the forensic lab using Windows operating system. The screen captures show applications such as Cellebrite working on a Windows machine alongside other software.

On the desktop screen is an array of software such as FTK Imager, Registry Viewer, Wireshark, Nmap/Zenmap, PuTTY, Oracle VirtualBox, Notepad++ and others. However, the presence of these software on the computer does not mean that they were used in this particular investigation to obtain the results presented here. In fact, the evidence presented here is mainly based on the Cellebrite process as depicted by the screen captures.

A controlled lab environment is very necessary since forensics tests do not change evidence and have a reproducible process. Evidences need to be acquired first before doing any analysis on them.

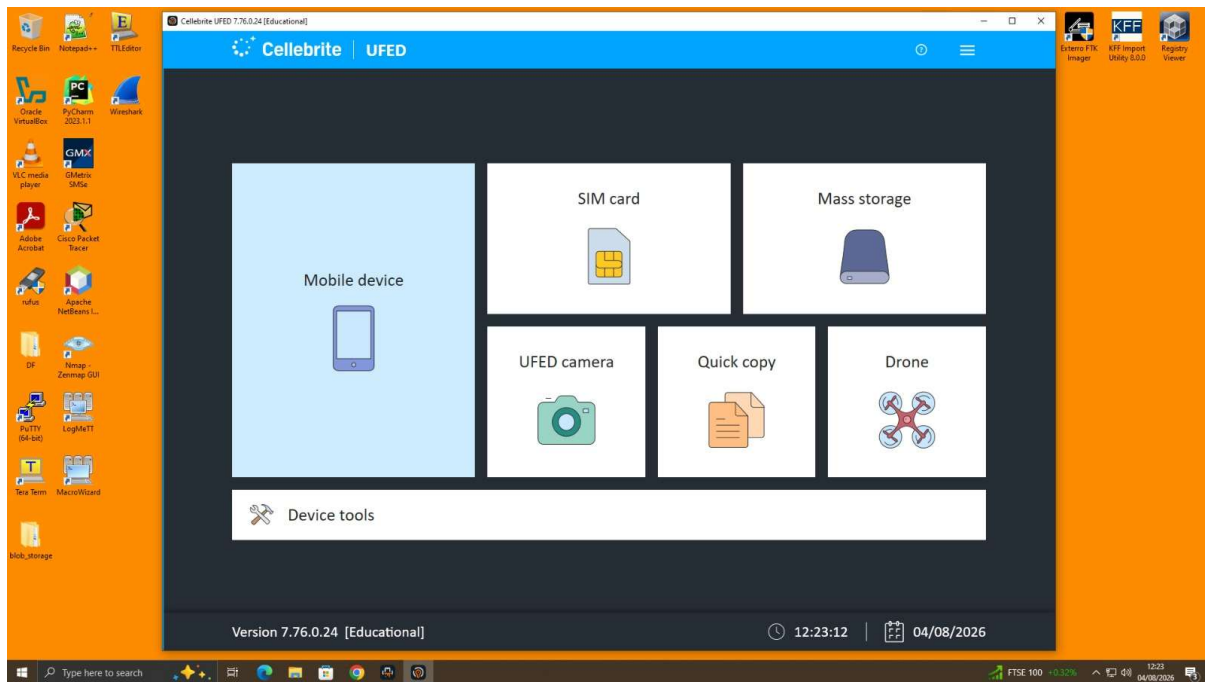


Figure 2: Practical Windows/Cellebrite forensic working environment

The examination environment also provided functionality for loading previously acquired evidence. Physical Analyzer's **Case Wizard** contains a "Load evidence" stage in which an extraction can be added to the examination. One screenshot demonstrates selection of an EvidenceCollection item associated with a UFED extraction directory.

2.3 Devices Analysed

Several device-related datasets are visible during the practical work.

A Samsung extraction displayed in Physical Analyzer identifies the selected device as **Samsung GSM SM-A137F Galaxy A13**. The Device Info section reports:

- Model: SM-A137F
- Operating System: Android 14
- Security Patch Level: 2025-06-01
- Vendor: Samsung
- Chipset: MT6769V/CT

The same extraction summary indicates the extraction to be File System [Android Backup] with the connection type indicated as Cable No. 170 or Original Cable.

In another screenshot from UFED acquisition, there is a Samsung GSM SM-A176B_DS Galaxy A17 5G showing content type selection before extraction.

Another dataset analyzed using Physical Analyzer is identified as Huawei_POT-LX1 P Smart. The analysis of this dataset yielded various kinds of information recovered including calls, contacts, messages, web artefacts, media, social media information, and application data.

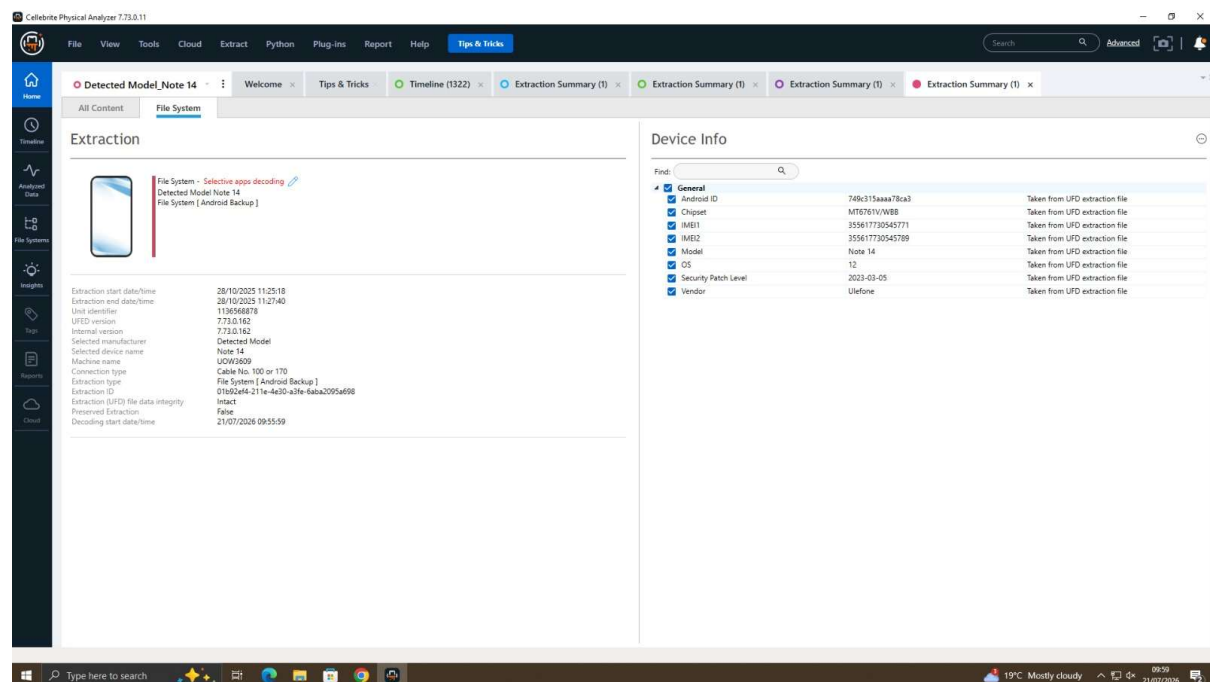


Figure 3: Device identification/information showing the examined handset

Another Physical Analyzer screenshot is labeled as the identification of a Nokia C2 series with recovered artefacts that include call logs, contacts, Snapchat information, device locations, web history, and user dictionary.

These are some datasets that have been used for recovering information.

2.4 Examination Features

Several features that were found within the Physical Analyzer tool were utilized or analyzed in the practical exercise.

Case Wizard featured an Examination Tools step where there were:

- Hash sets – which enable files that have been recovered to be checked against various hash sets.
- Carve locations – which is meant to allow for the discovery of additional location details from unallocated space and databases.
- Recover data from archives – which allows for extra data to be extracted from archive files such as ZIP and TAR files.

Selective applications decoding – where the examiner can choose some applications to decode and not all the applications installed.

Selective decoding comes in handy when there are many applications in a forensic extraction. The analyst can use processing power on applications that are related to the examination.

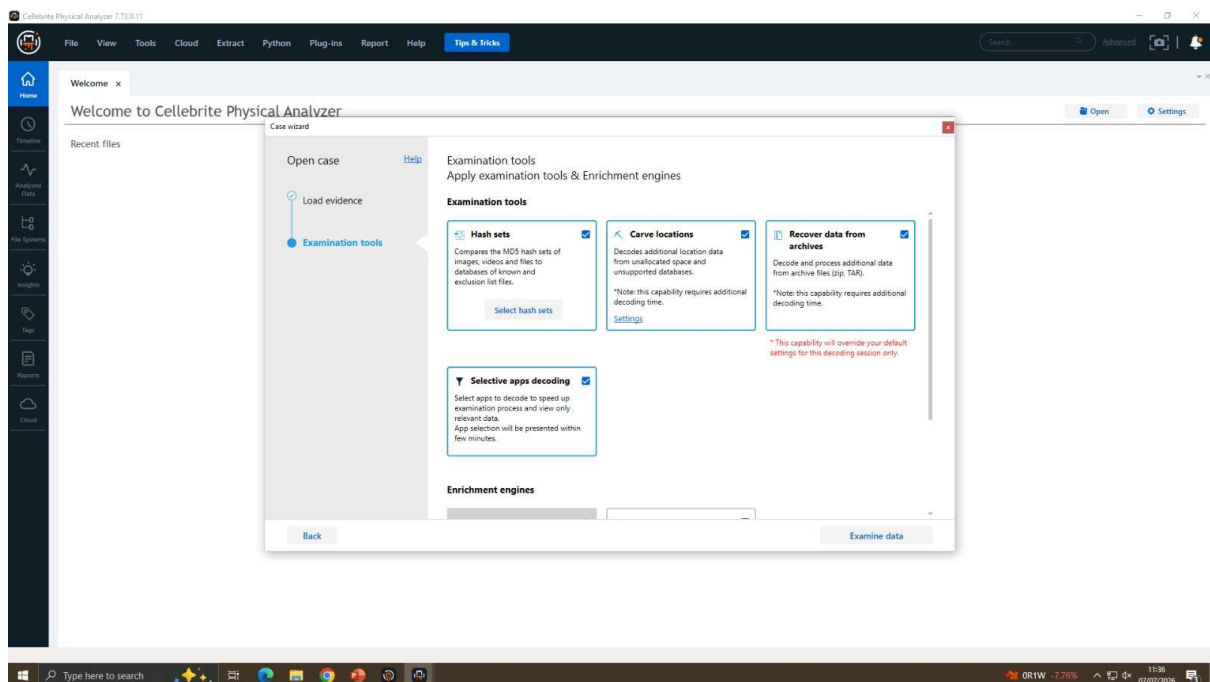


Figure 4: Case Wizard examination tools such as hash sets, carving, archive recovery and selective decoding

The practical exercise involved the use of AppGenie, Android Emulator (Virtual Analyzer) and the SQLite Wizard that are accessible through the installed applications interface.

2.5 Evidence Inventory and Chain of Custody

It is important to have an evidence inventory and chain-of-custody log throughout the process of acquisition and examination in a proper mobile forensics investigation.

In an evidence inventory, each physical device or forensic extraction needs to be identified accordingly. Information in the evidence inventory could include the evidence identifier, manufacturer, model, serial number or device identifier as necessary, date and time of acquisition, the examiner, extraction method, location of storage and integrity values.

Through the Samsung extraction summary, it can be seen that Cellebrite collects useful metadata regarding acquisition. In the extraction of the Note 14 as shown, the Physical Analyzer shows the extraction start date/time as 28/10/2025 11:25:18 and extraction end date/time as 28/10/2025 11:27:40. The type of extraction and device details are also identified.

Another point noted in the extraction summary is the Extraction (UFD) file data integrity which is noted to be Intact. This is vital since it provides an indication that the extraction being examined had passed integrity verification.

All these details obtained automatically need to be supplemented by manually recording the chain-of-custody in a forensic case scenario.

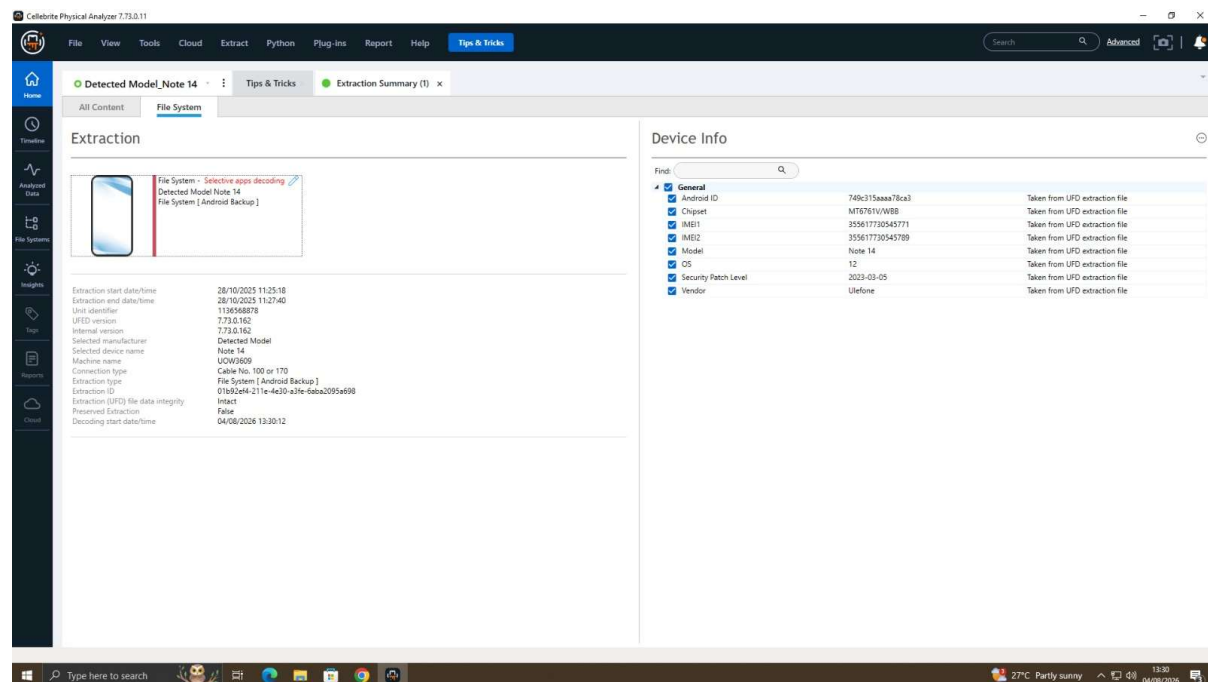


Figure 5: Extraction/evidence information suitable for documenting the evidence item

3. Evidence Acquisition

3.1 Acquisition Process

Collection of evidence is an essential step in the mobile device forensics process as the validity of the analysis performed later would depend on the quality of the collected evidence.

The actual evidence collection process was performed using Cellebrite UFED. First of all, the tool identified the proper device profile, presenting the investigator with the potential sources of extraction.

For Samsung Galaxy A17 5G example, the following three main options were shown:

Device, SIM, and Memory Card.

To perform the demonstration of evidence collection from the device, the device option was chosen. Then, the tool showed the categories of potentially recoverable evidence. The user interface provided the option to select certain classes of data or everything that could be potentially recovered by the software.

The fact that the particular category of evidence is accessible does not mean that there is any evidence within that category; rather, it means that it is possible to attempt to acquire that type of data.

After collection, the evidence could be imported to Physical Analyzer.

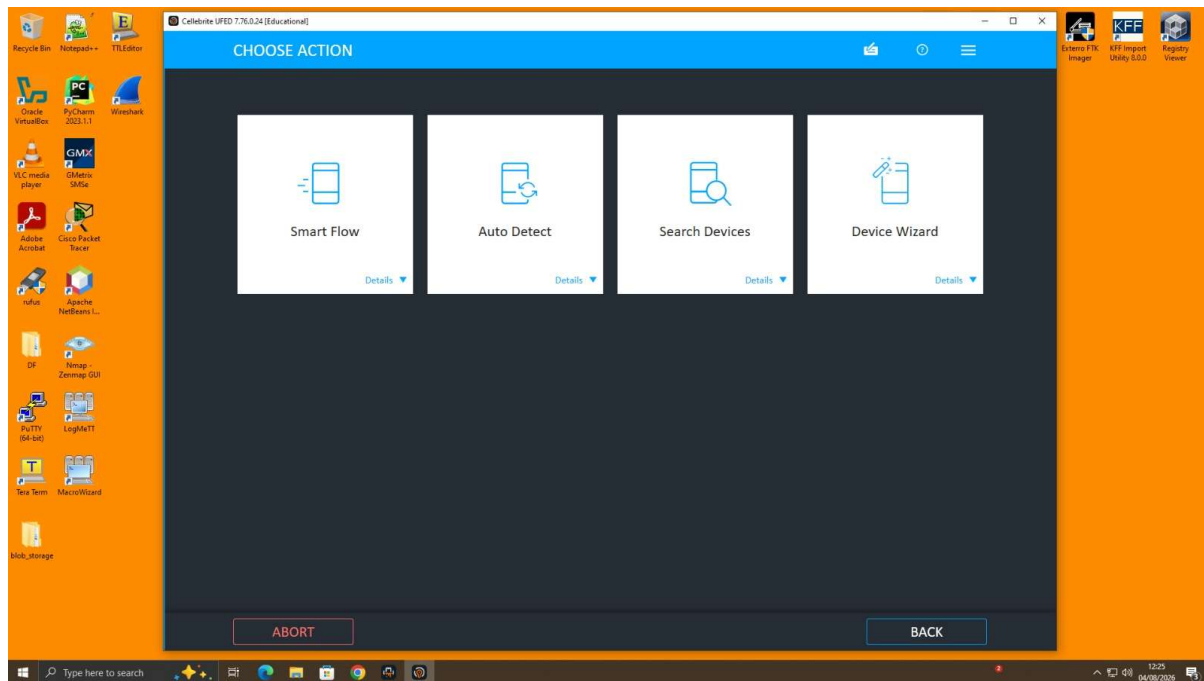


Figure :6 UFED device-detection/acquisition stage

3.2 Extraction Methods

The screenshots show a File System [Android Backup] extraction of the Samsung Galaxy A13 dataset.

A file-system extraction allows the files and databases to be accessed, from which the forensic applications analyze the higher-level artifacts. The exact quantity of data retrieved will depend on several factors, such as the version of Android, device security, the extraction method, and the permissions available during acquisition.

The extraction summary shows the connection as "Cable No. 170 / Original Cable," which means that the acquisition method used included the physical cable connection.

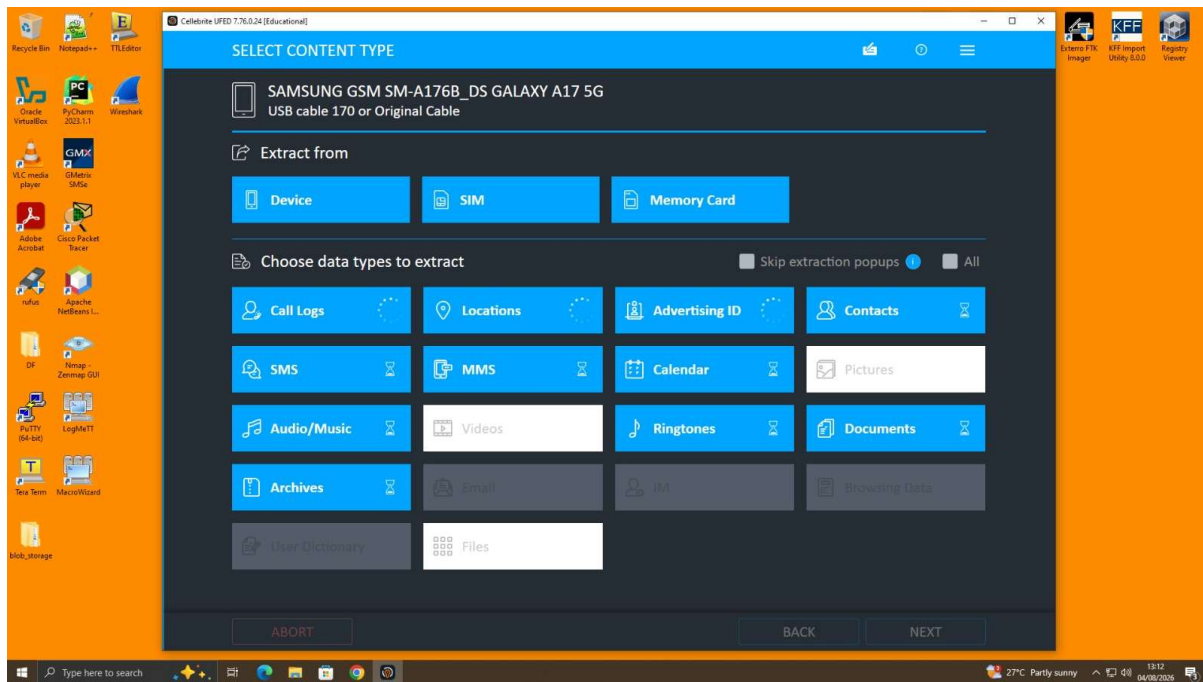


Figure 7: UFED extraction/content selection demonstrating the extraction method

It should be noted that the term "physical extraction" should not be applied to this particular dataset simply because the examination software is known as "Physical Analyzer." Physical Analyzer is the analysis software; the actual extraction method shown in the evidence summary is File System [Android Backup].

3.3 Device Extraction Summary

Information provided through the extraction summary is contextual and can serve as documentation of the evidence.

In regard to Samsung Galaxy A13, Physical Analyzer shows:

- Manufacturer selected: Samsung GSM
- Device name selected: SM-A137F Galaxy A13
- Extraction type: File System [Android Backup]
- Data integrity of extraction file: Intact
- Preservation of extraction: False

The Device Info panel provides additional identification information in terms of Android ID, chipset, IMEI field, model, OS version, and security patch level/vendor.

Such information is helpful since it identifies the device environment that has created the extraction and enables differentiating between different mobile devices in the context of a large case.

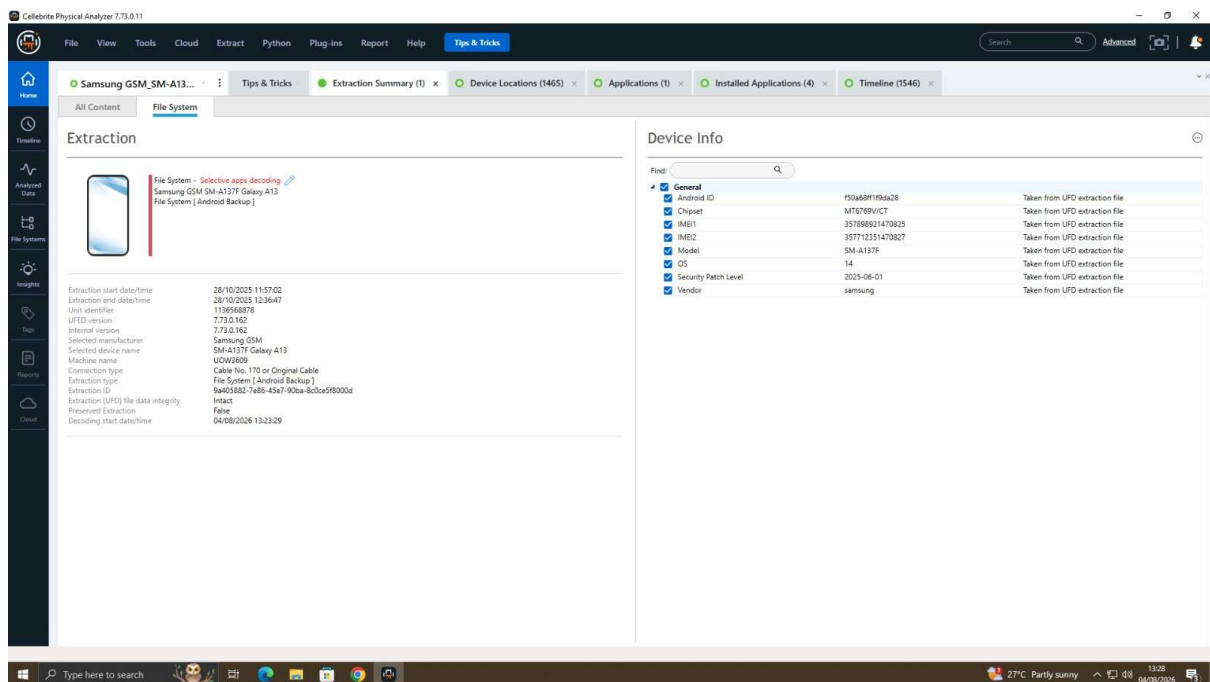


Figure 8: Extraction summary containing acquisition and device information

3.4 Data Integrity and Verification

Integrity verification is important to show that the forensic evidence was not inadvertently changed after being acquired until examination.

The Physical Analyzer extraction summary shows the data integrity of the UFD file as Intact. It confirms the assertion that the extraction container has undergone integrity check conducted by the Cellebrite environment during the time of the captured screenshots.

The Case Wizard also provides for hash sets. Hashing is an important cryptographic process in forensics that helps identify files and check the data integrity. But the screenshots have not shown any MD5, SHA-1 or SHA-256 hash value of the complete evidence image. So, no specific hash value can be made in this report based on the presented evidence alone.

That is a critical distinction. The provided evidence only justifies that Cellebrite reported the integrity of the UFD extraction as intact, but not creating any hash for the evidence.

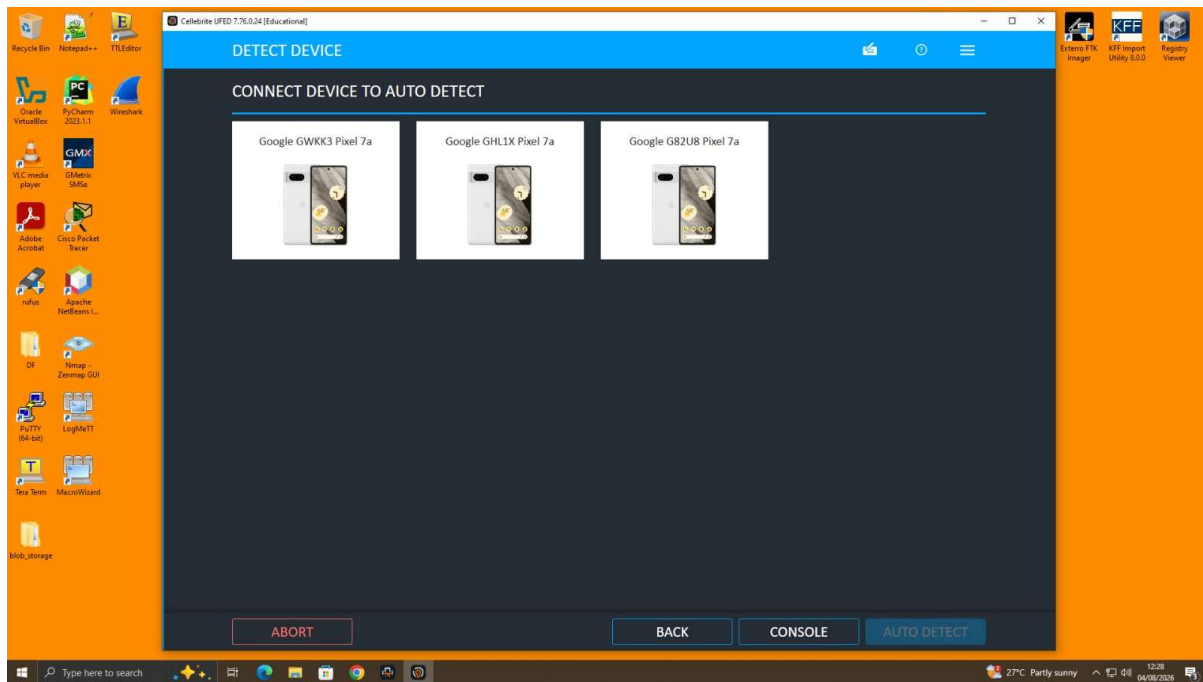


Figure 9: Hash/integrity verification evidence

3.5 Practical Device Extraction and Validation

After extraction, the evidence was imported into Physical Analyzer via the Case Wizard. The analyst chose the appropriate evidence collection and moved on to the examination tools phase.

The Case Wizard offered some processing options such as location carving, archive recovery, and selective decoding of applications. Then the analyst could move on to the examination process by choosing the option to Examine data.

After being processed, Physical Analyzer provided decoded artefacts and extracted artefacts summary. Successful interpretation of information of the device and the recovered artefacts proved that the extracted evidence could be analyzed by the software.

Validation at this stage consisted in the analysis of the device identified, extracted metadata and available categories against the anticipated evidence source. The integrity status reported by the software was also assessed.

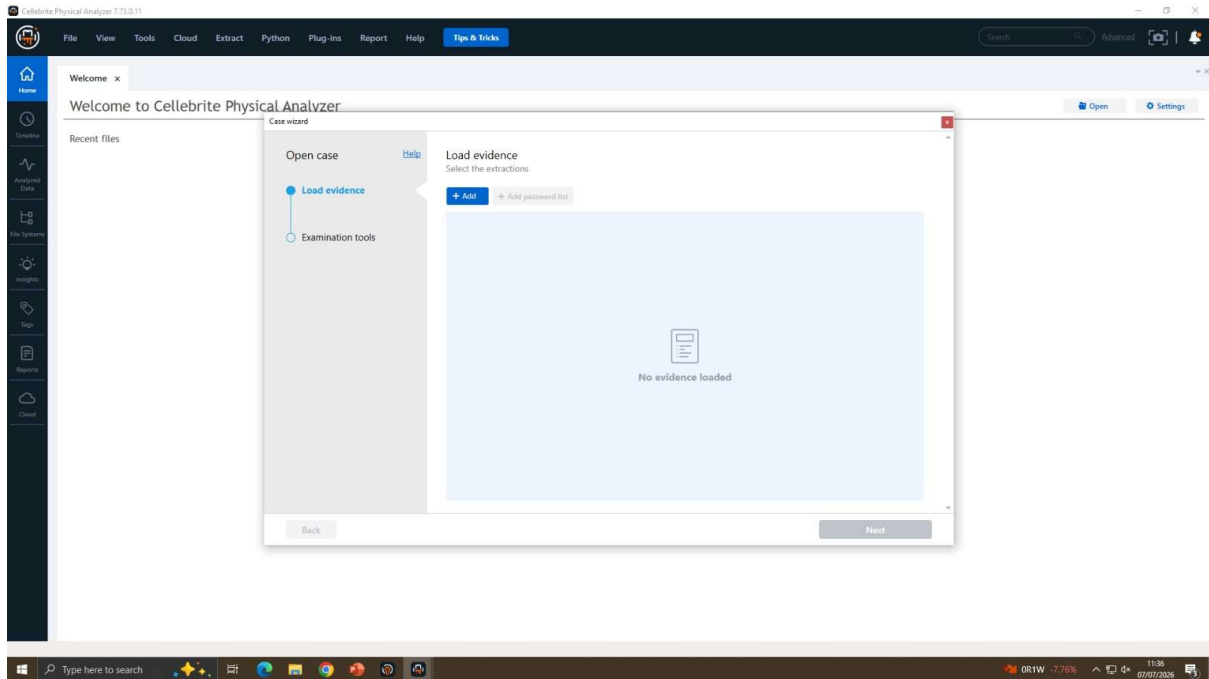


Figure 10: Loading the acquired evidence into Physical Analyzer

4. Examination Process

4.1 Overview of Examination

After acquiring and analyzing the evidence, there was systematic analysis done using categories generated by Physical Analyzer.

In this case, the analysis focused on artifacts that may help in understanding ownership of devices, communications, online activities, application usage, and movement.

In Physical Analyzer, there are Analyzed Data as well as Data files. This is quite helpful since Analyzed Data categories generate interpreted artifacts whereas data-file categories enable investigators to analyze actual files and databases for more verification.

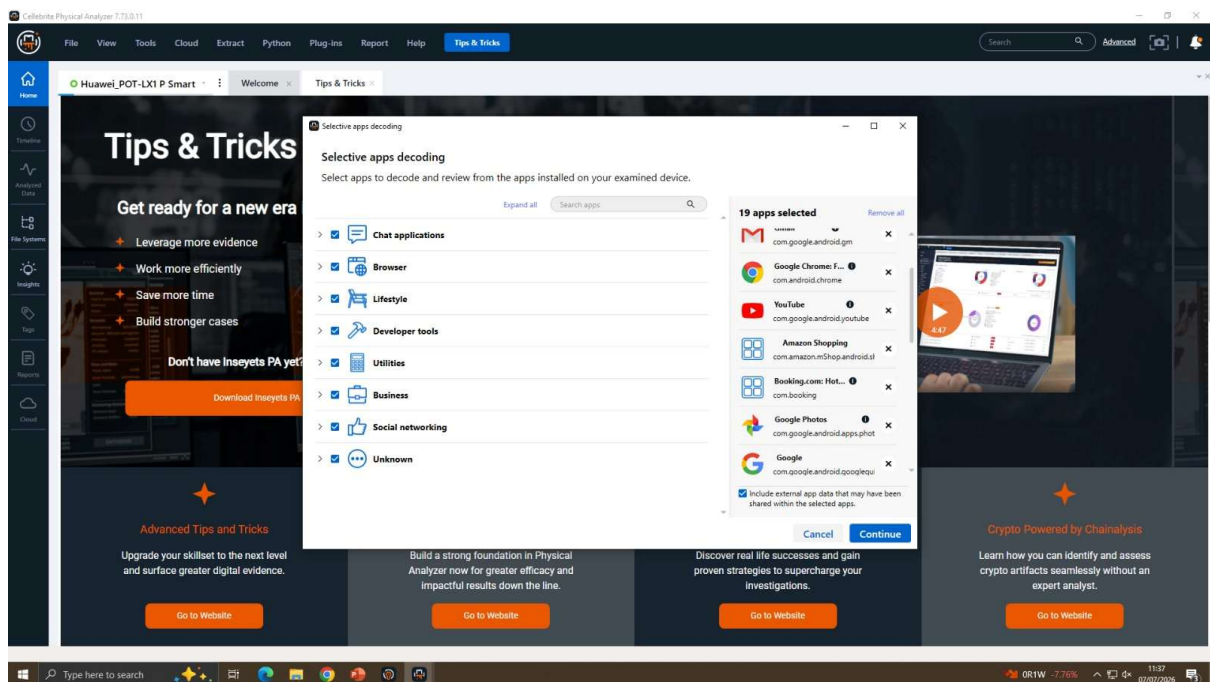


Figure 11: Selective application decoding/examination configuration

4.2 Contacts Analysis

Contacts category was used in order to find out individuals, services and application-based contacts which are connected with the device.

One of the datasets analyzed included 13 contacts which were divided into Native and Snapchat contacts. Contact entries which can be seen in the contact table are: "Joe Marsh", "My AI", "Team Snapchat", "SMS Service", "Top-up" and "Voicemail".

Both native and application-based contacts show us that contact evidence does not always need to appear in Android Address Book. Applications may have their own contacts and participants.

For example, when "My AI" is chosen, Snapchat appears as a source of information, along with some other identifiers in the details section. The same situation happens with "Team Snapchat", which appears as Snapchat contacts with application-based details.

These contacts do not always mean that they belong to actual persons in the real world. They might be services or platforms-related contacts. That is why forensic analyst must distinguish between native contacts, application contacts, automated services and communication partners.

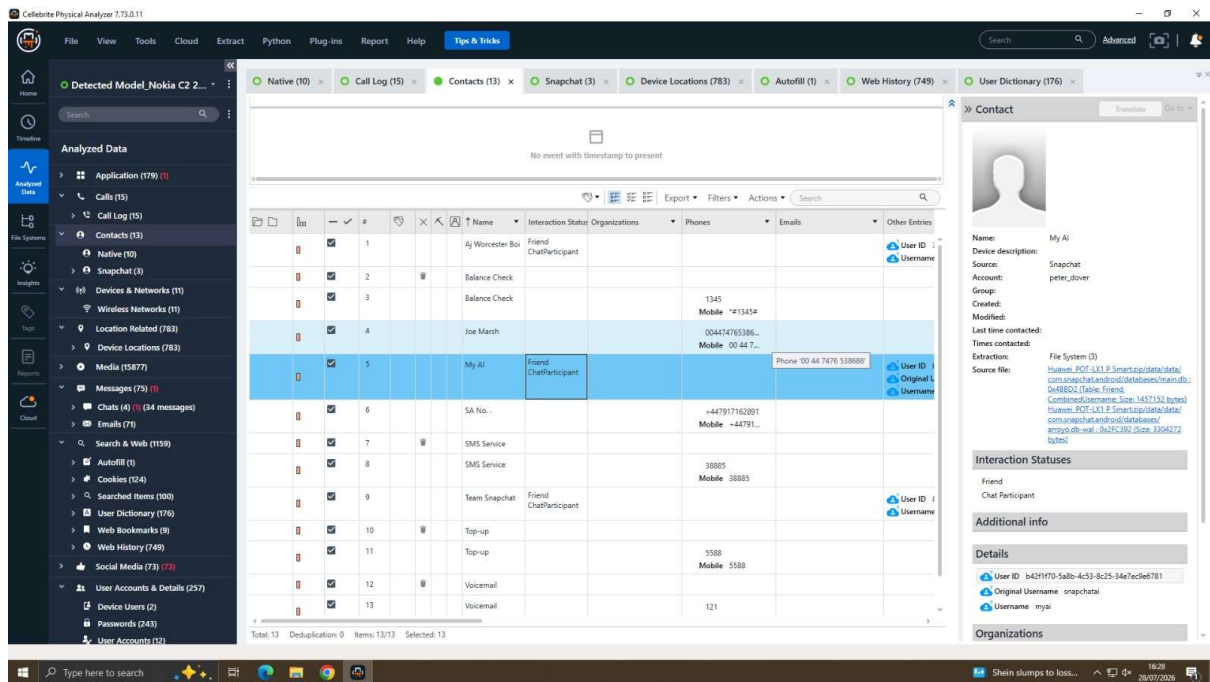


Figure 12: Recovered native and application/Snapchat contacts

4.3 Email Analysis

In the examined dataset, there is an Emails (71) category in the Messages section. It means that Physical Analyzer detected 71 artefacts which were classified as emails in that data extraction.

But the presented screenshots do not provide details on specific email entries, such as sender and receiver names, subjects and actual messages.

The only thing that can be concluded from the presented screenshots is that there is an email category containing 71 artefacts detected by the forensic tool.

Full examination would involve opening that category and analyzing sender and receiver names, timestamps, subjects and contents of the email messages and any attachments. The email timestamps can then be cross-referenced with browser, applications and location artefacts.

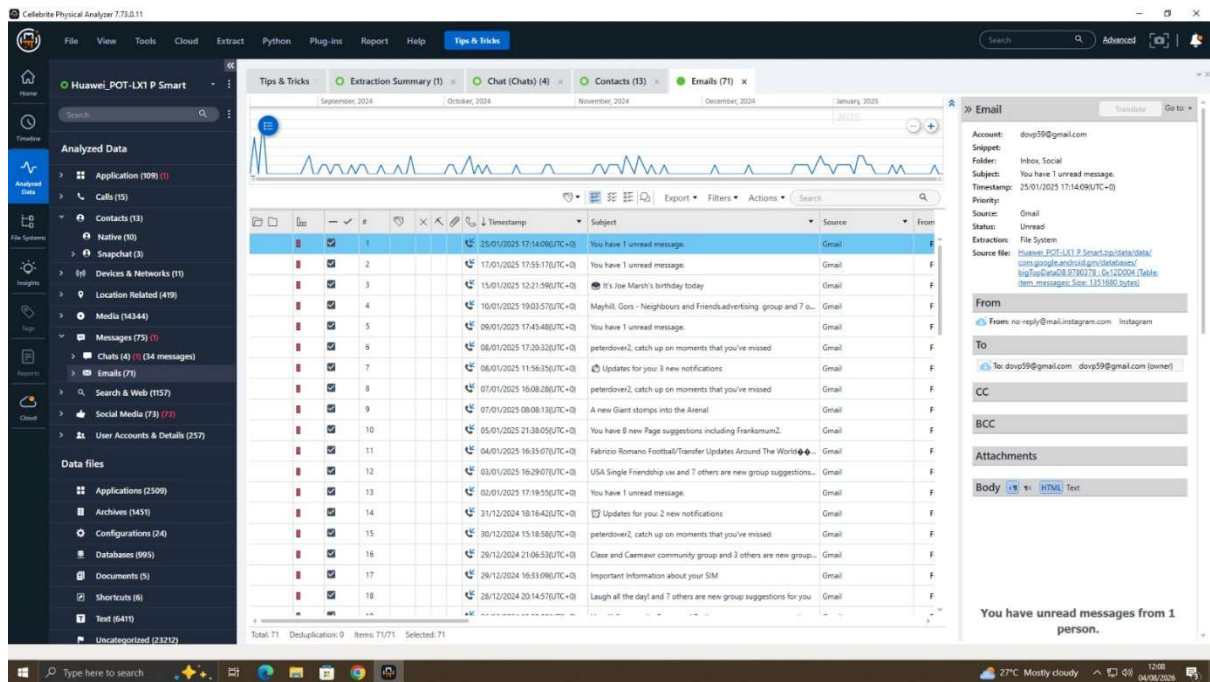


Figure 13: Email-related artefact/category evidence

4.4 Application Analysis

Application analysis was a vital element of the test.

One Physical Analyzer dataset showed 179 installed applications. The applications were categorized in groups such as:

- Chat apps
- Secure wipe
- Browser
- Developer apps
- Social media
- Lifestyle
- Utilities
- Entertainment
- Music
- Games
- Finance
- Business

- Health & Fitness
- Unknown

Some recognizable applications that could be seen in the interface were Gmail, Instagram, Google Meet, Messages, Snapchat, WhatsApp and Chrome.

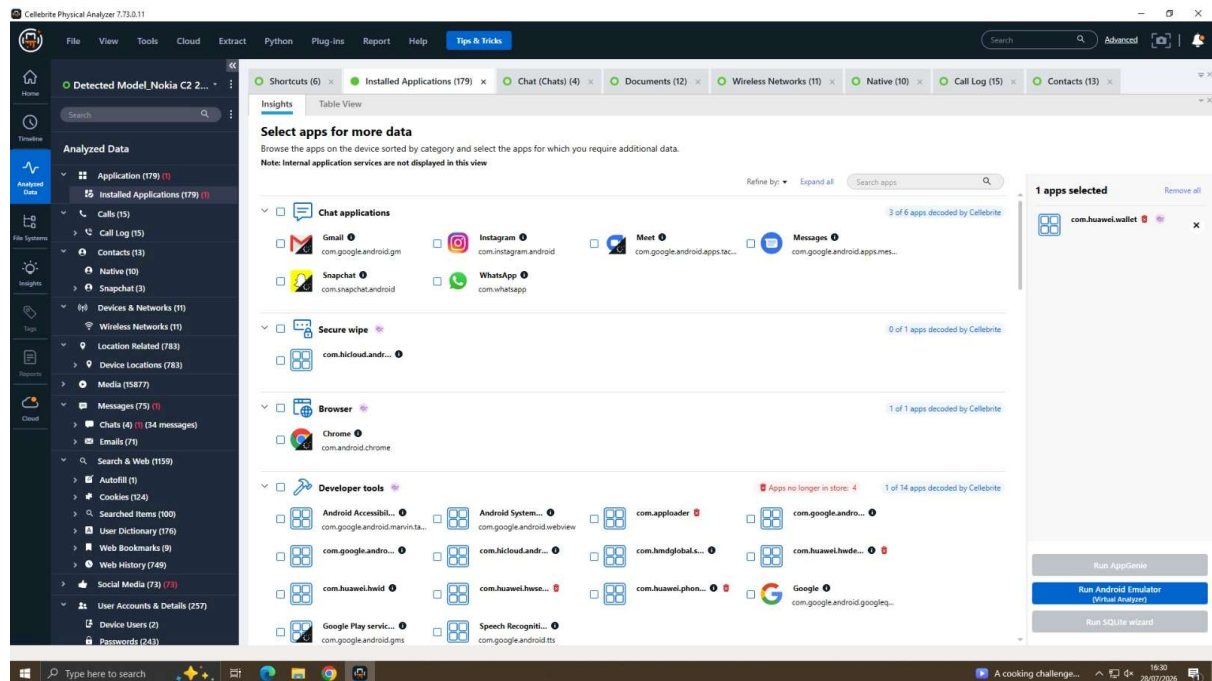


Figure 14: Installed Applications view and application categorisation

The application interface also provides information on the number of applications in each category that can be decoded through Cellebrite. That is because some applications may lack decoders. This is a vital point to consider since even the installation of a particular application does not necessarily mean that all of its data can be retrieved by Physical Analyzer.

Another tested Huawei dataset showed 109 installed applications.

4.5 Social Media Analysis

Snapchat has been analyzed as a source for social media and messaging.

Snapchat-related contacts and chats have been captured through these screen captures. Physical Analyzer shows that there is a Snapchat section with 3 entries in the contacts folder. Specific application contacts include My AI and Team Snapchat.

There are four chats in the Chats folder and 34 messages in the chat folder in total. One of these chats has participants including the device owner and My AI, while another one has participants including the device owner and Team Snapchat.

One of the My AI chats includes a text message discussing Palakkad, Kerala, India and talking about the area geographically and culturally. This can be considered a Snapchat chat artifact as

far as the fact that it exists. However, just by itself, this message does not prove that the device user has physically visited Palakkad.

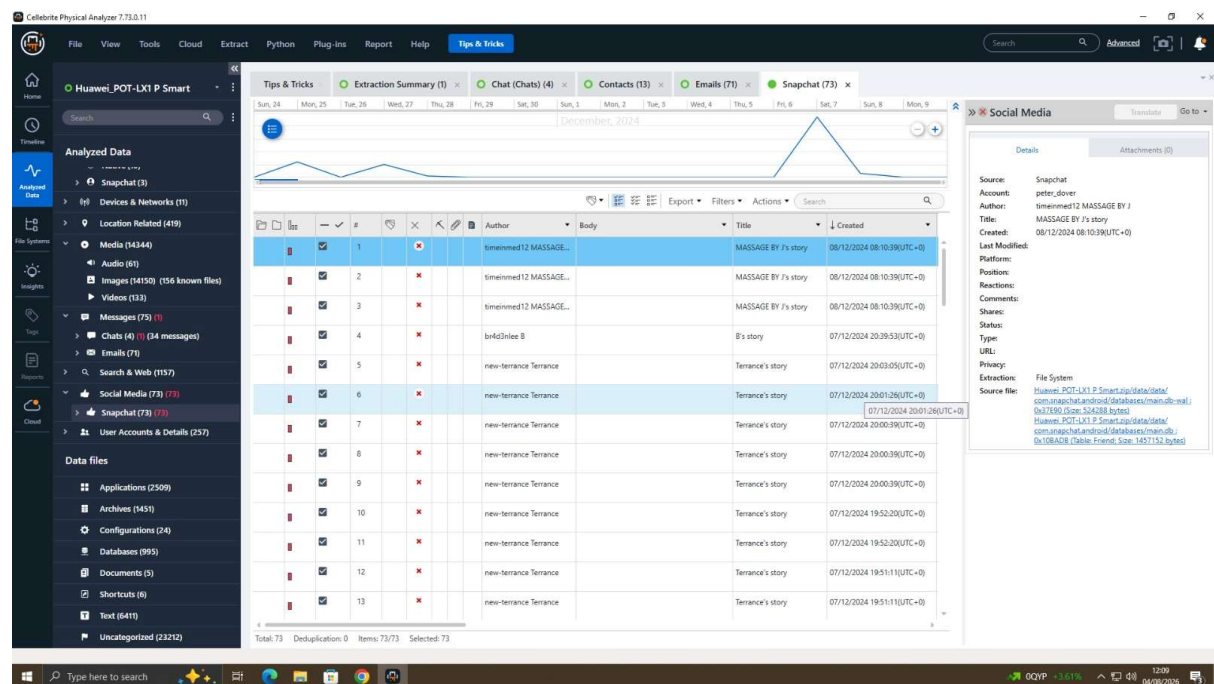


Figure 15: Snapchat/social-media artefacts and recovered communications

Conversations' timestamps can serve as valuable temporal data for comparison with other activities of the device.

4.6 File System Analysis

The categories for data files at a lower level within Physical Analyzer enable the examination of the raw evidence used for decoded artefacts.

The data-file categories in the Huawei dataset are as follows:

- Applications
- Archives
- Configurations
- Databases
- Documents
- Shortcuts
- Text
- Uncategorized

From the screenshot, there are large numbers of artefacts, such as thousands of artefacts under application and many under the category uncategorized.

Database evidence is essential in android examinations since applications use SQLite database files in storing structured data. Physical Analyzer has the capability to use a SQLite Wizard, which is helpful in examining application database files, which have not been decoded.

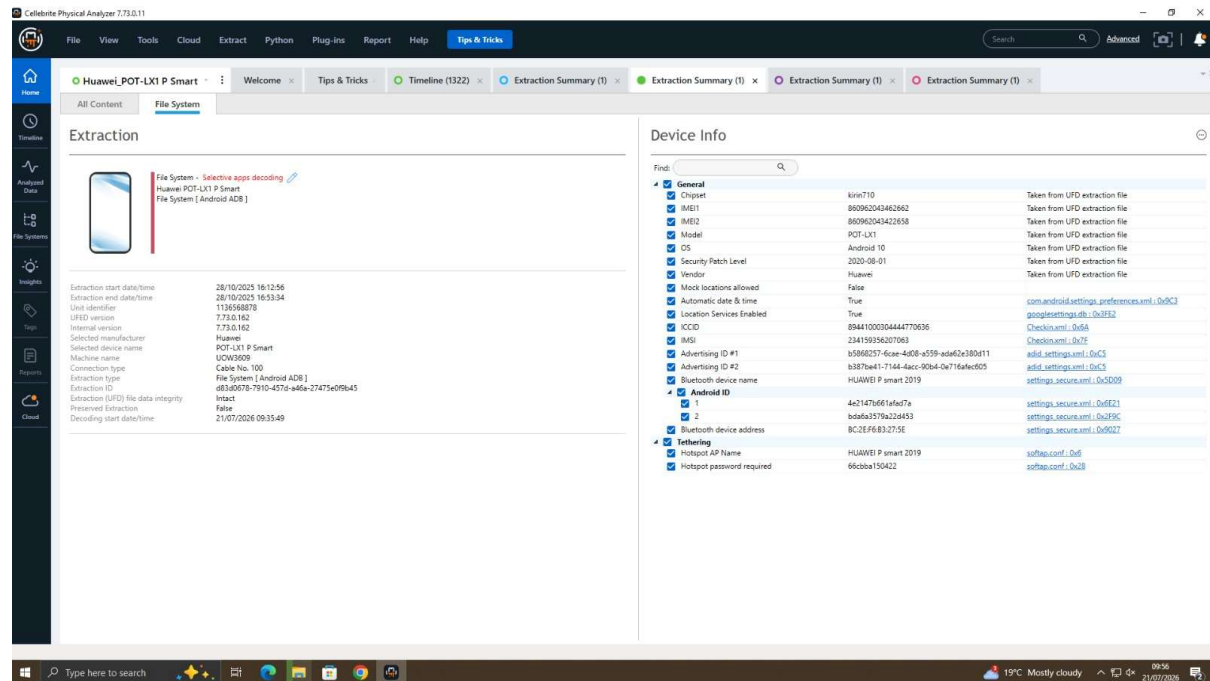


Figure 16: Data-file/file-system/database-related forensic artefacts

The information from the source file beside the decoded Snapchat contact files indicates the connection between high-level artefacts and database files.

4.7 Device Information Analysis

Information regarding the device was collected to create the technical context of the extraction.

The model of Samsung Galaxy A13 dataset was found to be SM-A137F, using Android version 14, with the security patch level of 2025-06-01. Information related to Android ID, Chipset, and IMEI was also available from Physical Analyzer.

Metadata about the device is important in the sense that it may assist in associating the extraction with a particular mobile phone and provide reasoning behind particular methods used for the extraction.

However, such metadata like IMEI number should be provided with caution in any report.

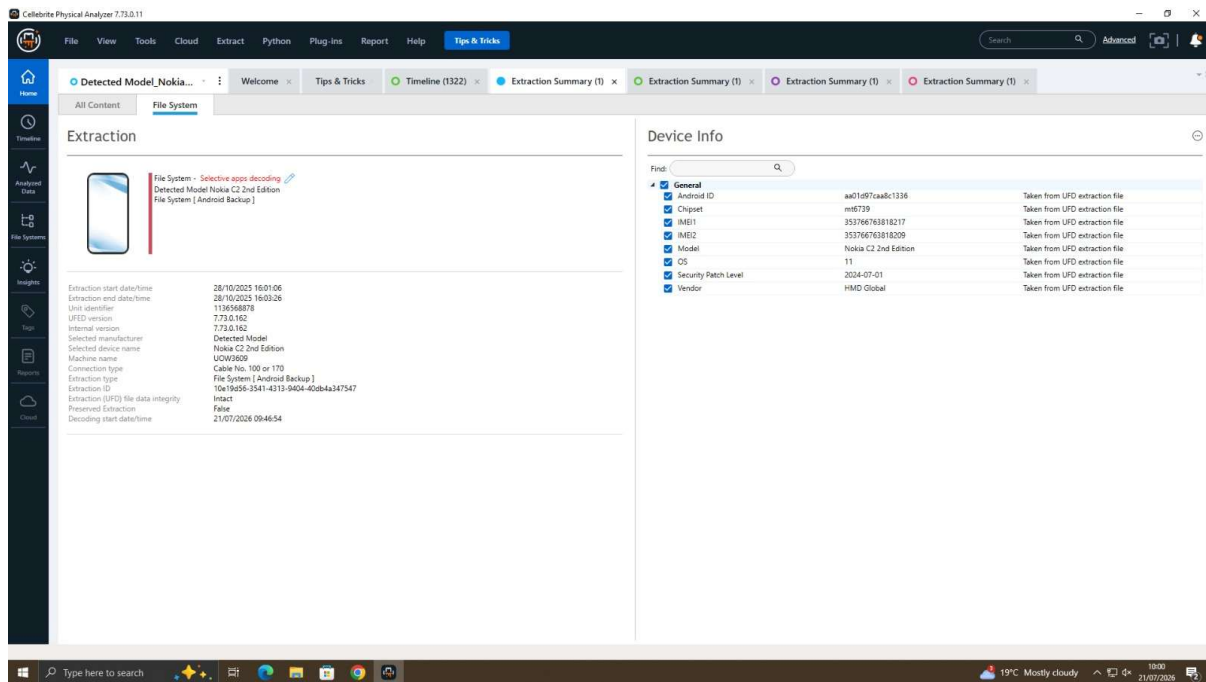


Figure 17: Detailed handset/device information and identifiers

5. Analysis and Findings

5.1 Overview of Findings

Forensic analysis revealed numerous types of evidence that were capable of adding to the reconstruction of device activities.

Main types of evidence identified during practical analysis included contacts, calls, email artifacts, applications, social media data, internet usage data, media, location-based data and timeline events.

The main advantage of mobile forensics lies in correlation of various artifacts. In other words, one artifact is not always enough to understand a situation, but several artifacts can help much.

5.2 Contact-Based Evidence

It was identified through contact analysis that the data in the tested device contained both native and application-based contacts.

Thirteen contacts were seen in one of the datasets where ten contacts were native and three belonged to Snapchat. Snapchat artifacts found were My AI and Team Snapchat.

This shows that the significance of analyzing application-based data instead of just the contacts in the device should be realized.

Contact information can help in an investigation as it can identify potential relationships within the context of communications. However, merely saving a contact does not necessarily mean there has been any communication.

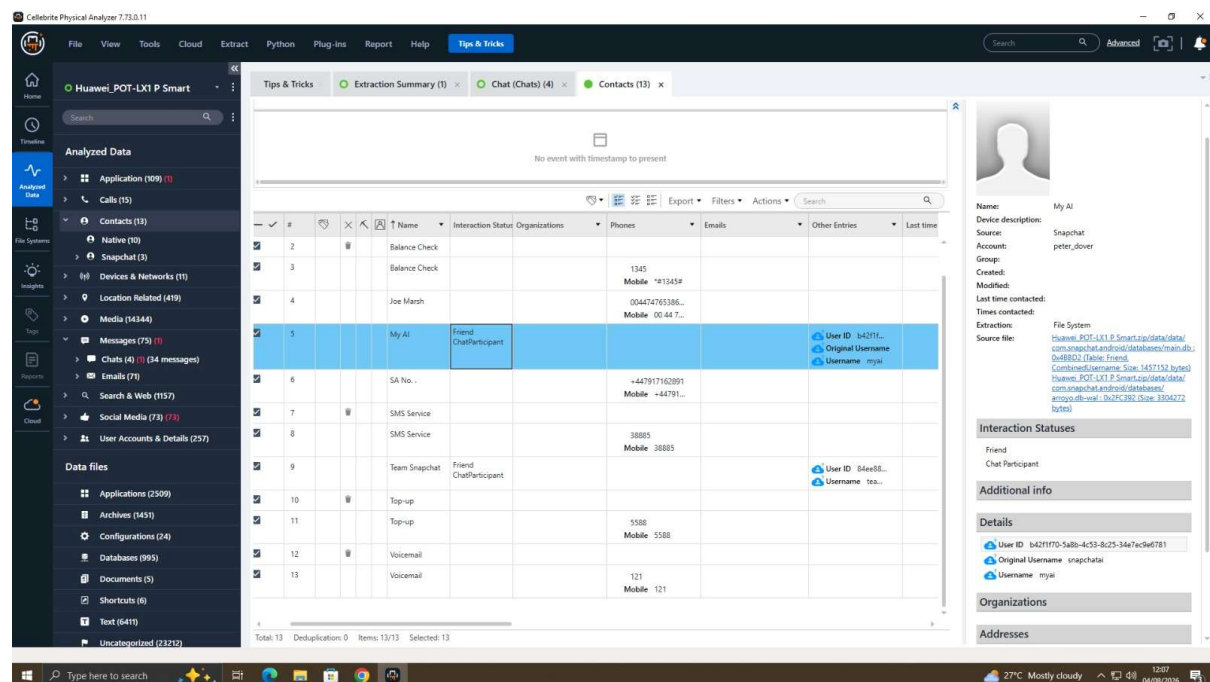


Figure 18: Additional contact evidence supporting relationships/identification

5.3 Email Communication Findings

Physical Analyzer detected 71 email artefacts from the data that was under scrutiny.

This could turn out to be an important source for communications. Nonetheless, because the individual emails were not shown in the screenshots provided, it is impossible to conclude anything regarding the email content and relevance based on the information provided.

The proper forensic conclusion from this scenario, therefore, is that there were email artefacts found and classified.

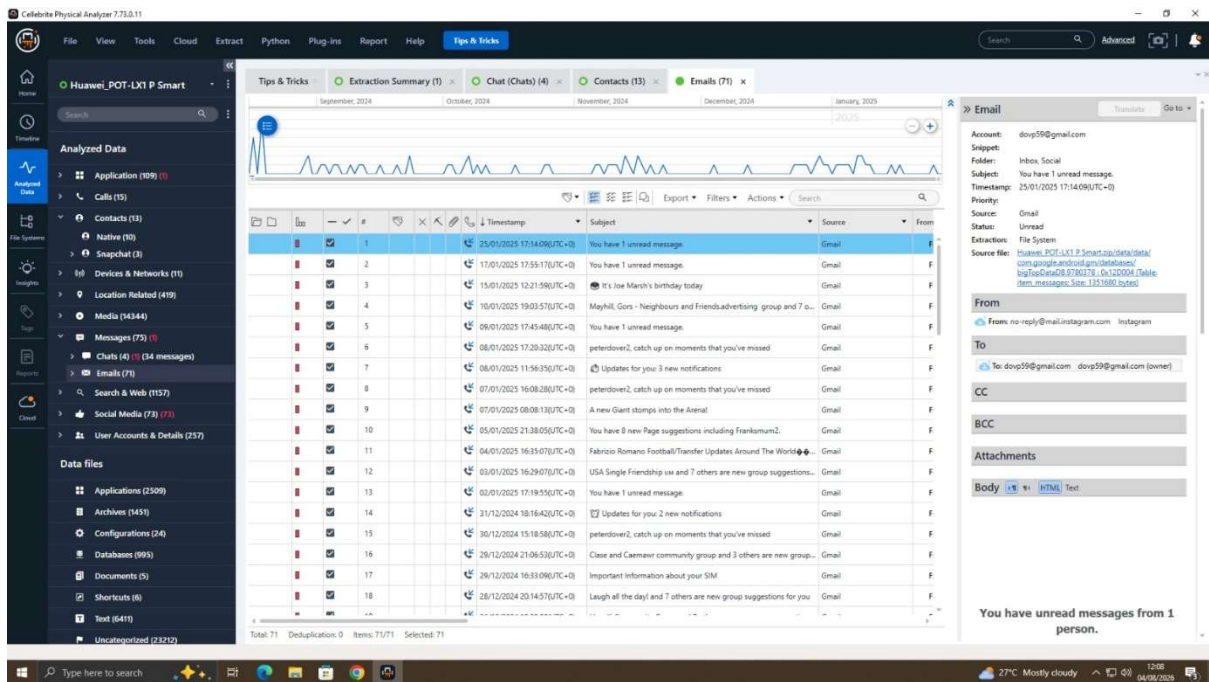


Figure 19: Detailed email-related findings if the visible contents support your discussion

5.4 Application Usage Insights

Software installed applications were found to cover a wide variety of software types.

Gmail, Instagram, Snapchat, WhatsApp, Chrome, Google Meet, and Messages show the variety of applications related to communication and the internet that can be found on the device.

It is essential to understand the difference between application installation and its usage. An installed applications list shows that an application existed in the extracted environment, but it is not evidence of its use during the period under consideration.

Usage of the application should be proven by other artefacts, such as database records, accounts, chats, browser links, cache records, time stamps, or application-specific files.

The recovered Snapchat chats are examples of other artefacts related to Snapchat application usage.

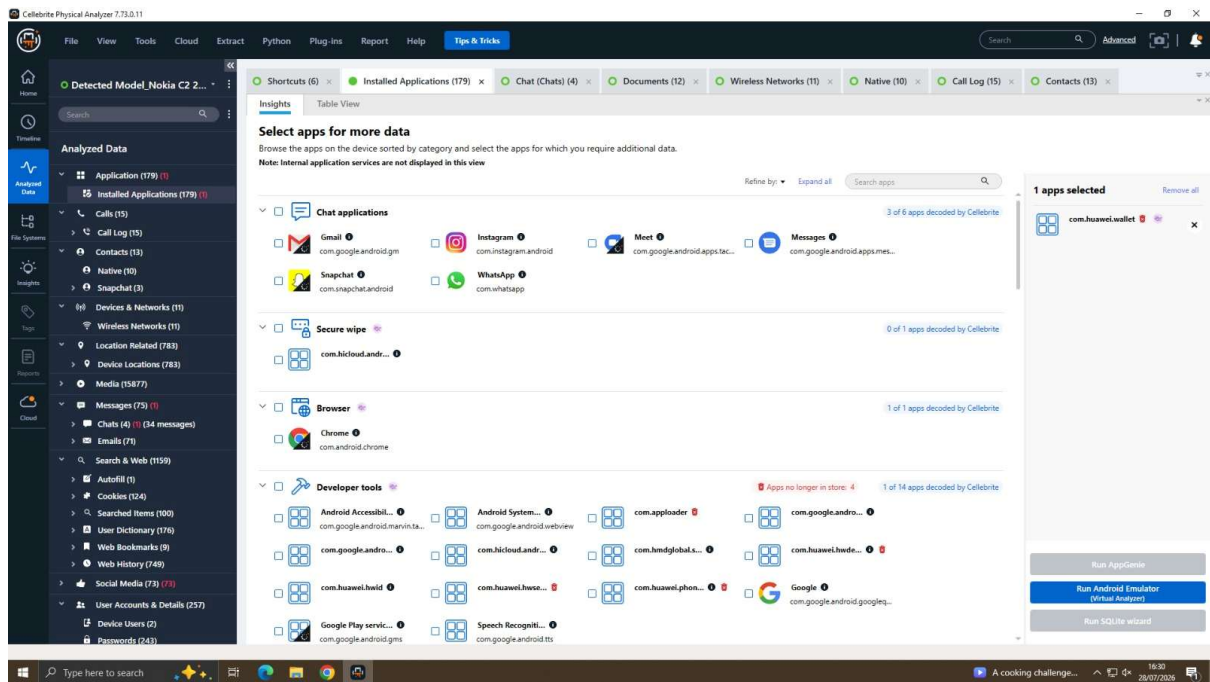


Figure 20: Installed-app/AppGenie evidence supporting application examination

5.5 Social Media Evidence

Some of the most explicit application-specific evidence that was available in the screenshots was that of Snapchat.

Evidence collected included Snapchat contacts and Snapchat chat messages. Some of the chosen chats contained interactions with My AI and Team Snapchat.

The chat with My AI had some details about Palakkad, Kerala, India. It shows that some relevant evidence was found from Snapchat data which might help in the investigation if the topic was Palakkad.

However, this should not be considered as location evidence. There is a fundamental difference between talking about a location and the evidence of the physical presence of the device at the location.

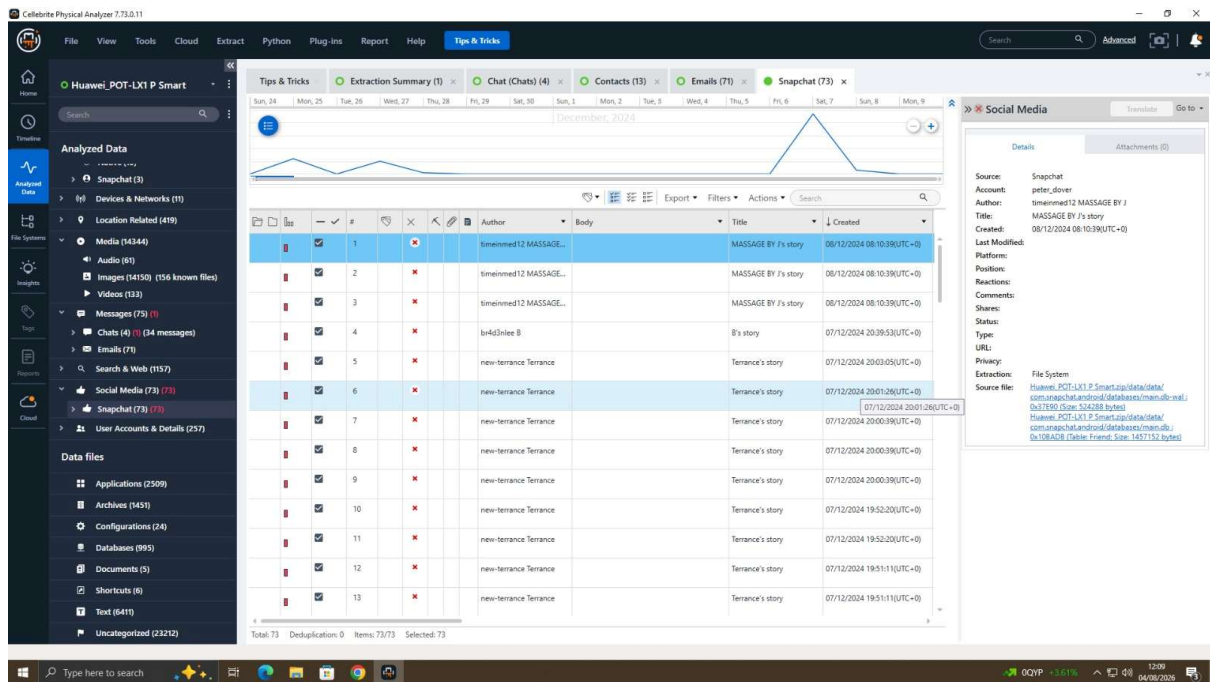


Figure 21: Recovered social-media/chat evidence

5.6 File System Findings

The investigation of the file system revealed that there was a significant amount of data, both raw and structured, lying under the categories provided by Physical Analyzer.

The availability of databases, archives, application files, configuration files, documents, text files, and other unclassified artifacts makes it possible to dig deeper into the system.

References to the source files provided for artifacts decoded from Snapchat can be of particular use in forensic analysis since they enable an analyst to trace down the database where the artifact came from.

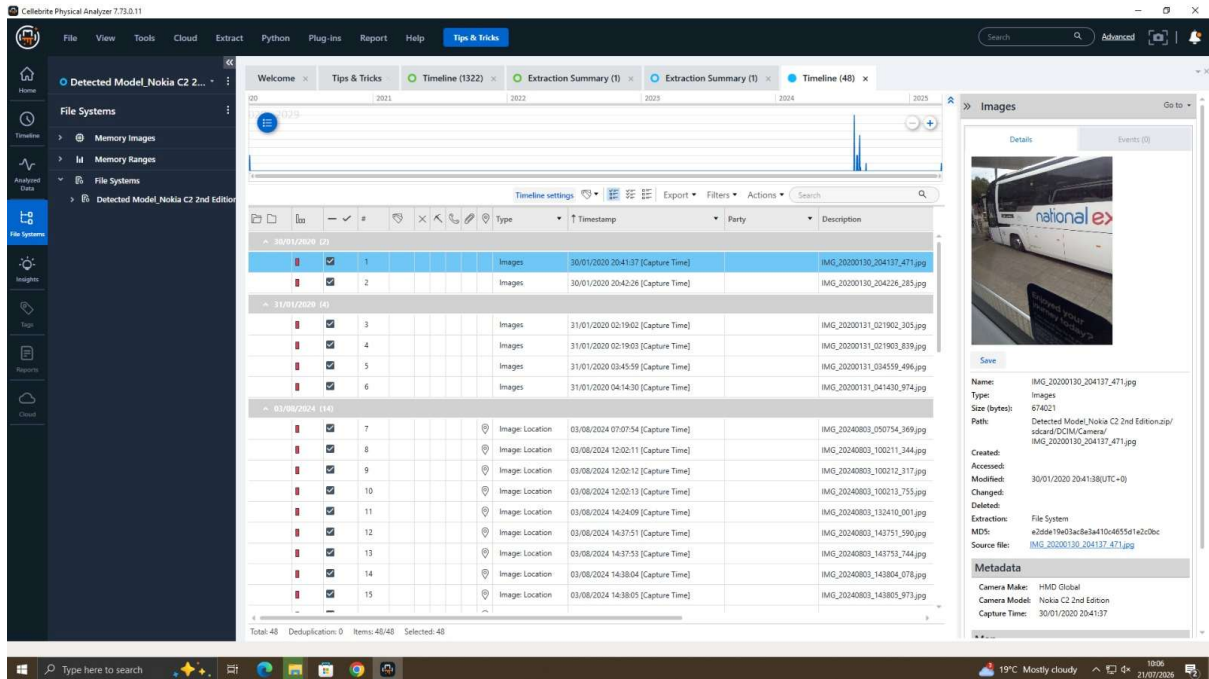


Figure 22: Additional database/file-system findings

5.7 Device Correlation

Correlation between devices and artefacts is vital when there are various evidence sources available.

In the case of the screen shots, these show various data sets that relate to different types of mobile devices, and therefore findings cannot be combined automatically. The extraction must first be regarded as an individual piece of evidence.

Once the device identity and owner have been determined, the investigation can involve comparisons between contacts, user names, accounts for applications, time stamps and any other identifiers within the data sets.

For instance, one can compare the Snapchat account information from one data set with the recovered chat participants and application.

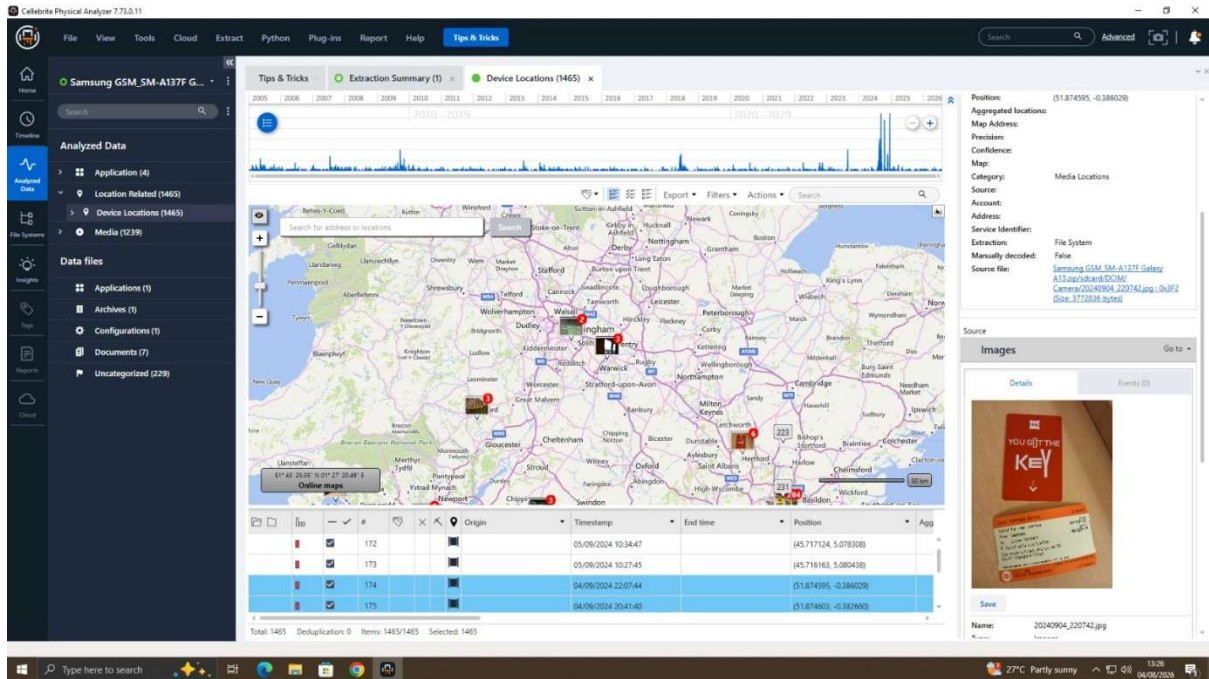


Figure 23: Location/device artefacts useful for cross-device or activity correlation

5.8 Timeline Reconstruction

The timeline capability of Physical Analyzer was applied when reviewing chronological artifacts.

There is a Samsung dataset containing a timeline with 1,546 items. This timeline shows fields such as type, date stamp, description, and source, among other things.

One problem seen in the provided screenshots is that there are some locations showing dates in 2005 while most of the analysis is performed with newer device data. The location artifacts contain the geographical coordinates with longitude being 0.000000.

This is something that needs to be handled carefully because an anomalous date stamp does not mean the presence of the device at that location and the same time. It can be the result of the source data interpretation or another artifact that needs to be validated.

Some other location artifacts are much more recent. There is a Device Locations view with 1,465 items related to location and some selected artifacts dated 07/01/2005 with geographical coordinates like 51.898682.

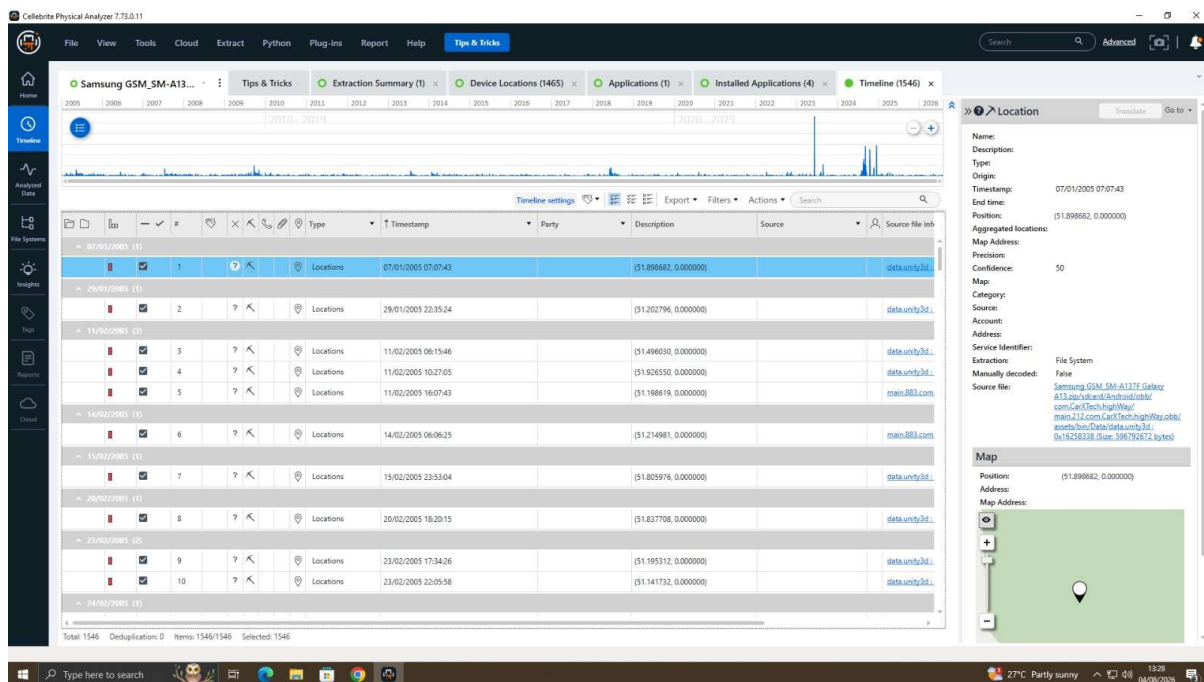


Figure 24: Timeline evidence showing chronological artefacts

Thus, the timeline and locations perspectives show not only the strengths, but also the weaknesses of an automated forensic investigation. The physical analyzer can correlate thousands of artefacts in chronological order, but the examiner is still the one who needs to assess their source, accuracy, reliability, and plausibility.

An accurate reconstruction of the timeline will, therefore, correlate location entries with pictures, applications usage, messaging activities, browsing histories, and other timestamped artifacts.

6. Conclusion

The hands-on exercise showed a comprehensive mobile forensics workflow, from acquisition through evidence loading, decoding, examination and analysis through Cellebrite UFED and Physical Analyzer.

The UFED was used to choose the type of mobile device, while Physical Analyzer was used to process the acquired evidence according to forensic categories.

The exercise yielded significant amounts of digital evidence, such as contacts, calls, emails, installed applications, Snapchat details, web artifacts, media, file system artifacts, device artifacts, and geographic locations.

The analysis of the applications showed that the mere presence of an application in the phone cannot be taken as evidence of its use. More accurate conclusions can be drawn by correlating information about the installation with databases, messages, contacts, or timestamps of the application. The example of Snapchat was given where contacts and chat information of the application were found.

Similarly, location analysis also showed the importance of careful interpretation of data. Physical Analyzer produced numerous artifacts of geographical data and mapped some of them on the map. Anomalous historical timestamps and coordinates with zero longitude are some examples that forensic investigators must validate the information decoded before using it as evidence.

7. References

- [1] “Mobile Device Forensics: Extracting and Analysing Data from an Android-Based Smartphone,” *IEEE Conference Publication*. Available: [IEEE Xplore – Document 7491574](#).
- [2] “On the Efficacy of Using Android Debugging Bridge for Android Device Forensics,” *IEEE Conference Publication*. Available: [IEEE Xplore – Document 8992948](#).
- [3] “Forensic Extraction and Analysis of Signal Application in Android Phones,” *IEEE Conference Publication*. Available: [IEEE Xplore – Document 9702702](#).
- [4] “Digital Forensics Analysis of YouTube, Instagram, and TikTok on Android Devices: A Comparative Study,” *IEEE Conference Publication*. Available: [IEEE Xplore – Document 10527244](#).
- [5] “Smartphone Forensics: A Comparative Study of Common Mobile Phone Models,” *IEEE Conference Publication*. Available: [IEEE Xplore – Document 10527262](#).
- [6] “A Survey of Digital Forensic Tools for Android and iOS Smart Phones,” *IEEE Conference Publication*. Available: [IEEE Xplore – Document 10679486](#).
- [7] “A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020, doi: 10.1109/COMST.2019.2962586. Available: [IEEE Xplore – Document 8950109](#).
- [8] “Shopping While Watching: An Updated Forensic Analysis of TikTok on Android and iOS,” *IEEE Conference Publication*. Available: [IEEE Xplore – Document 10759027](#)