

Mobile Forensic Investigation using Cellebrite Physical Analyzer

Digital Forensics Analysis

Practical examination of Huawei, Nokia and Samsung Android devices

Evidence acquisition • examination • artefact analysis • timeline correlation

Name: Patel Vinay Bhikhabhai

Student ID: 2519364

Course: MSc Cyber Security and Digital Forensic

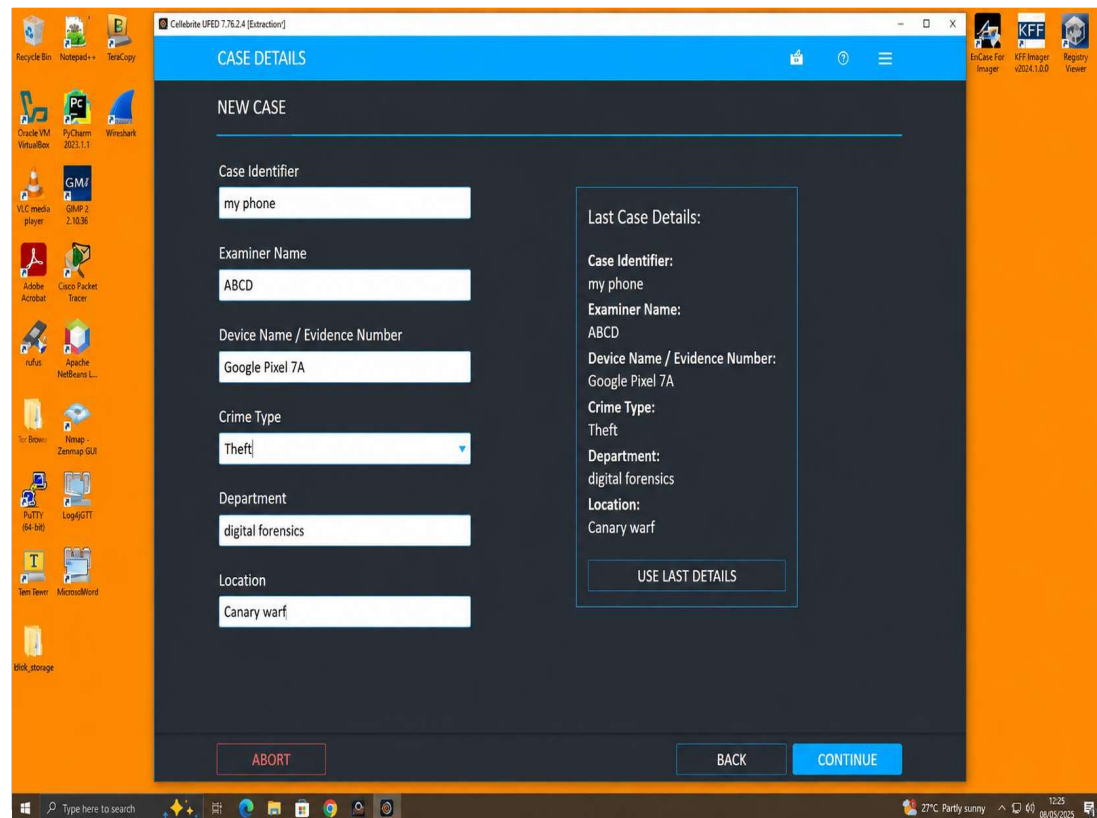
Module: Digital Forensic

MSc Digital Forensics • Mobile Artefact Analysis

Introduction to Mobile Forensics

Mobile Forensic Investigation using Cellebrite Physical Analyzer

- Digital forensics is defined as the process of identifying, preserving, analyzing, and presenting electronic evidence in a systematic and defensible manner.
- Mobile phones may have communication logs, application artifacts, media files, location data, documents, and operating system data.
- This investigation revolves around extraction and analysis of mobile evidence.

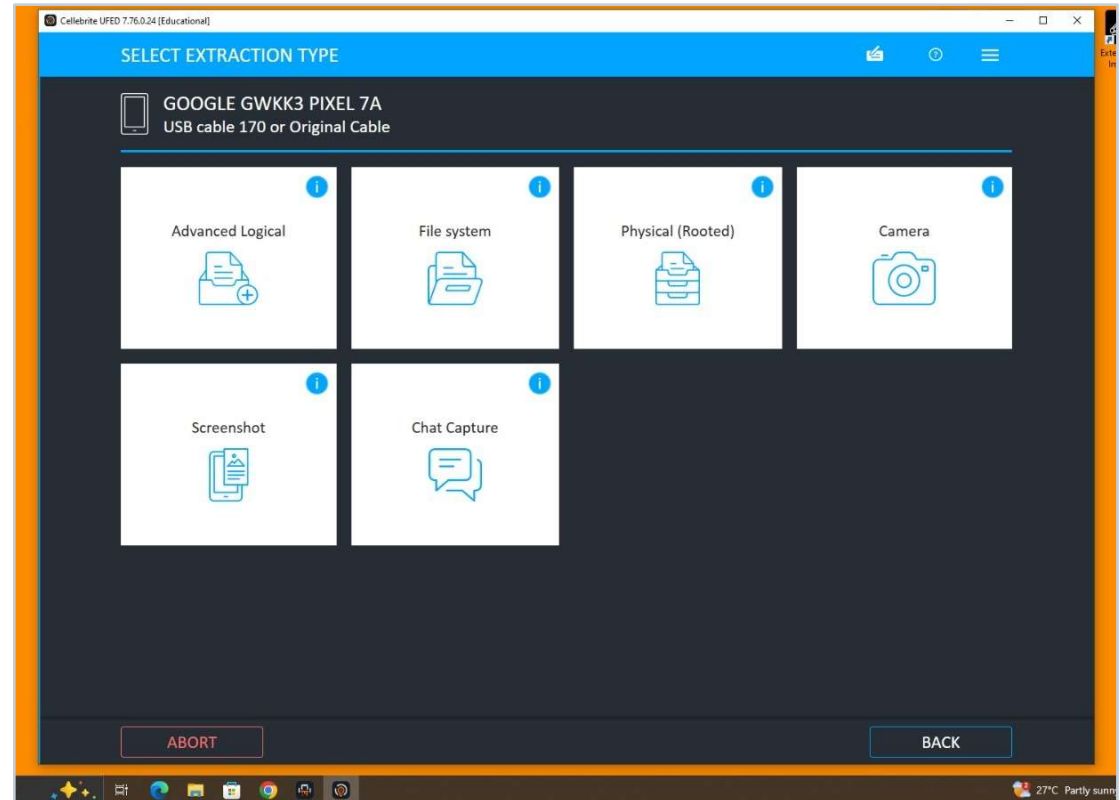


Practical Cellebrite evidence screenshot

Investigation Aim & Scope

Mobile Forensic Investigation using Cellebrite Physical Analyzer

- Investigate a range of Android phones by means of Cellebrite UFED and Physical Analyzer.
- Extract all pertinent communications, applications, contacts, media files, documents, locations and system artefacts.
- Compare different artefacts from different phones and establish connections based on timestamps.
- Document unsupported or unavailable artefact categories as part of the forensic limitations.

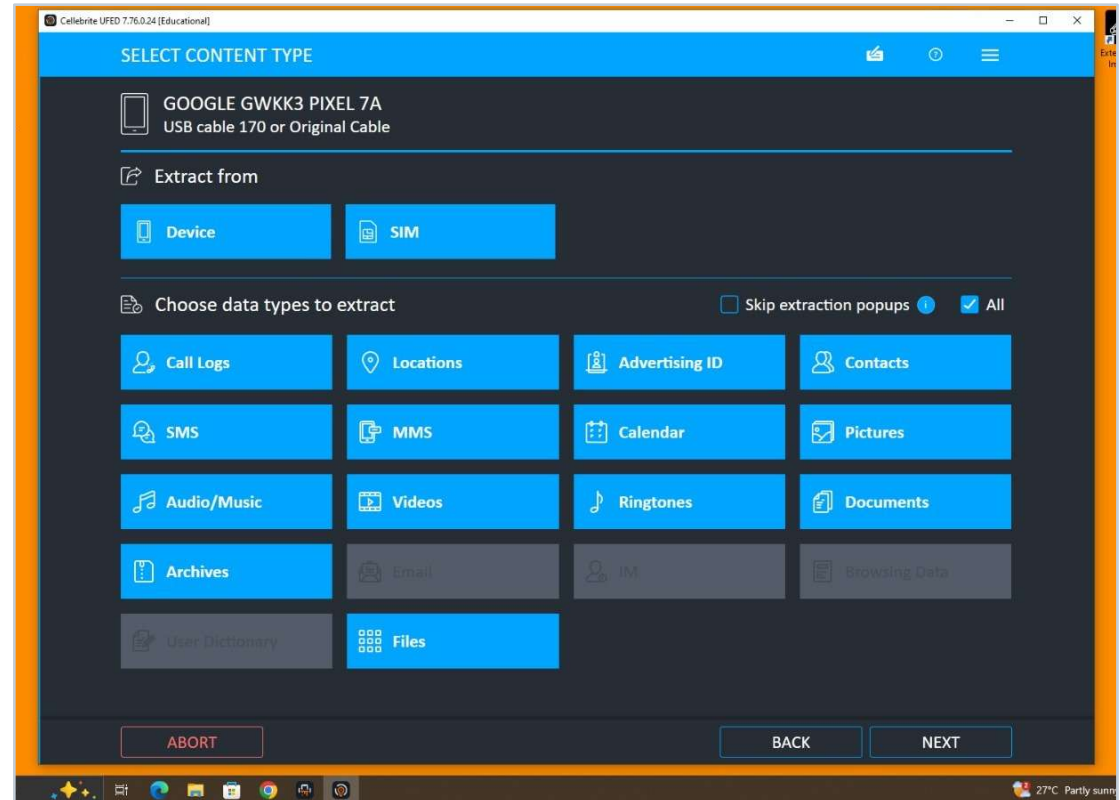


Practical Cellebrite evidence screenshot

Tools & Forensic Environment

Mobile Forensic Investigation using Cellebrite Physical Analyzer

- Cellebrite UFED 7.7.60.24 (Educational) – Mobile Forensics Acquisition & Selective Extraction
- Cellebrite Physical Analyzer – Decoding, Categorisation, Application Analysis, and Timeline Analysis
- Supplementary tools are FTK Imager for hashing and Autopsy/Sleuth Kit for file system analysis
- Controlled forensic lab, write protection, and chain of custody procedures ensure evidentiary soundness.

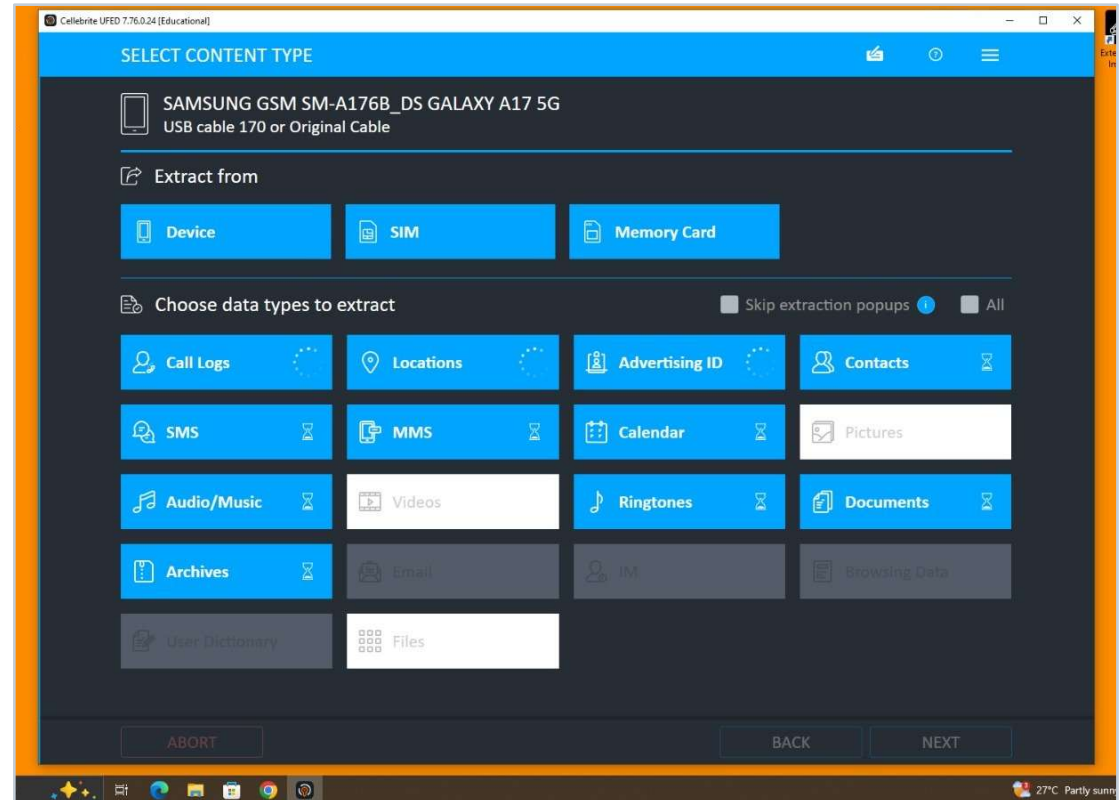


Practical Cellebrite evidence screenshot

Evidence Acquisition Workflow

Mobile Forensic Investigation using Cellebrite Physical Analyzer

- Establish a connection to the mobile device.
- Select the correct extraction profile and content type to extract.
- Extract the data without affecting the source evidence.
- Import the extracted data to Physical Analyzer.
- Record every step and save extraction metadata.

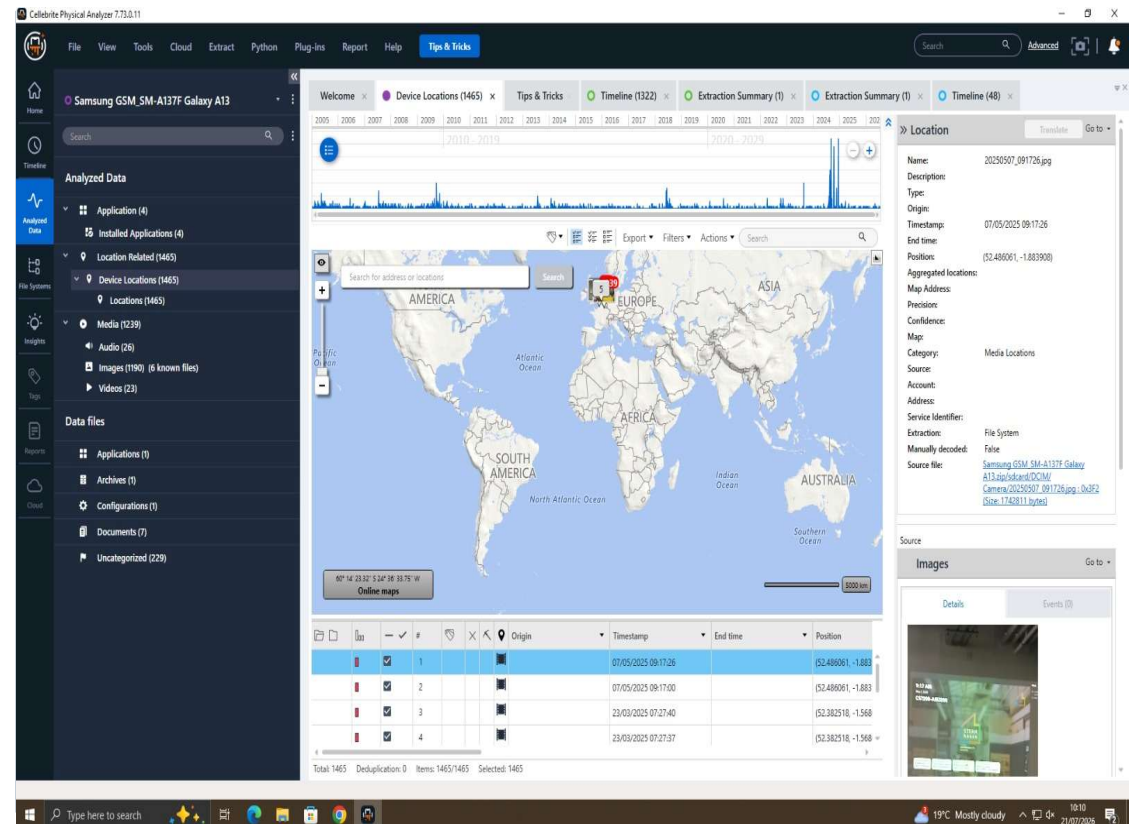


Practical Cellebrite evidence screenshot

Device Identification & Extraction Summary

Mobile Forensic Investigation using Cellebrite Physical Analyzer

- Device information and extraction data form the provenance of the evidence.
- Fields that can be recorded include device model, Android OS version, security patch level, and extraction process.
- The extract log lists the data types extracted and those that were not supported.
- This documentation clarifies the range and limitations of the examination.

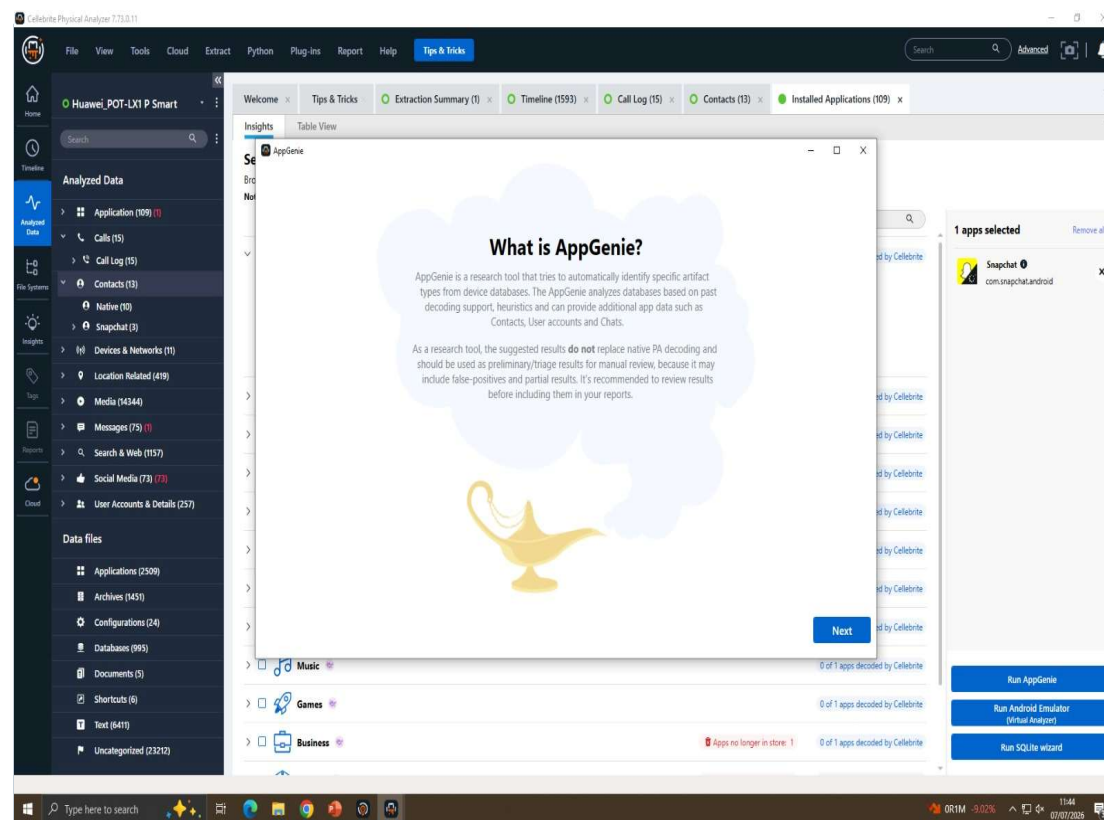


Practical Cellebrite evidence screenshot

Examination Tools Configuration

Mobile Forensic Investigation using Cellebrite Physical Analyzer

- Hashing sets can help decrease noise through the use of recognized files.
- Carving can be used to look for artifacts in unallocated space.
- Recovering archives allows for decompression of the data and its analysis.
- Selective application decoding allows for filtering of applications used for the investigation.

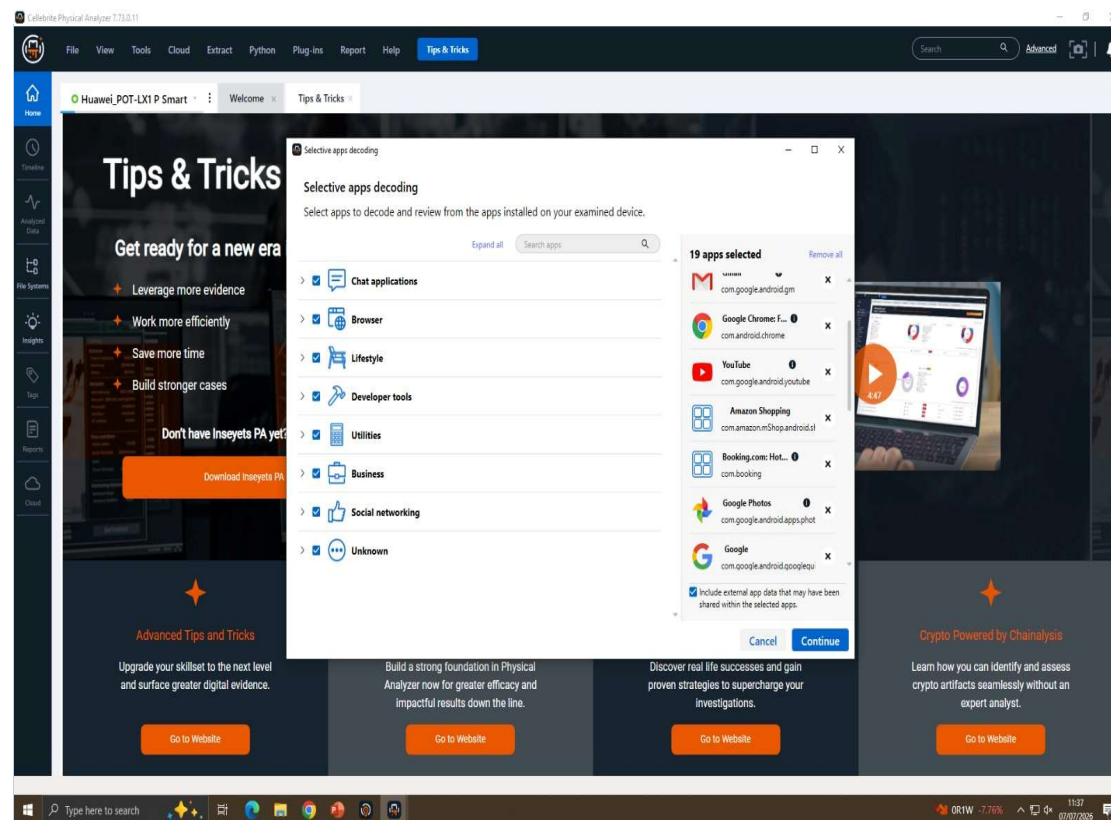


Practical Cellebrite evidence screenshot

Selective Application Decoding

Mobile Forensic Investigation using Cellebrite Physical Analyzer

- The installed applications are examined to locate potential sources of evidence.
- It is possible to select messaging, browser, social networking, and utilities categories.
- Decoding selectively is more efficient but still maintains an investigative direction.
- Unsupportable or un-decoded applications must be listed as constraints.

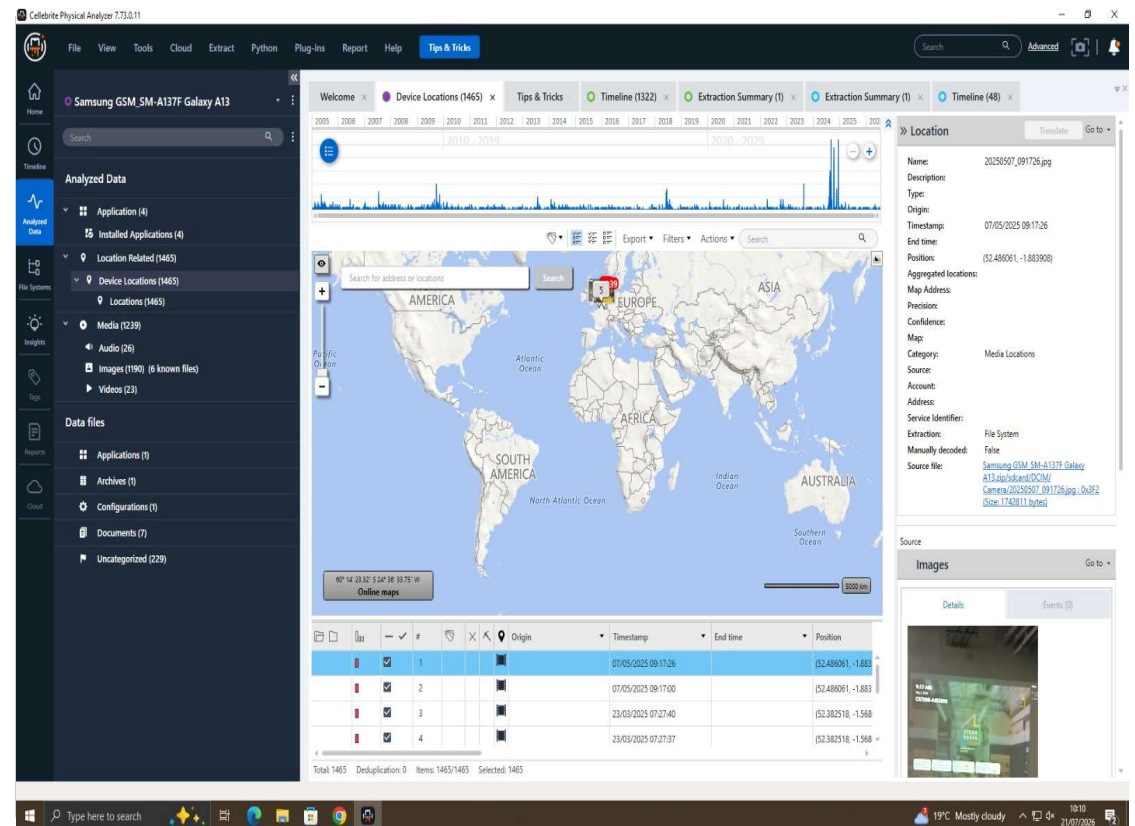


Practical Cellebrite evidence screenshot

Application & Social Media Analysis

Mobile Forensic Investigation using Cellebrite Physical Analyzer

- Artefacts of application use help explain the use made of the device and where any communication or file sharing could take place.
- Snapchat contacts and chat artefacts were found in one of the devices under analysis.
- Additionally, there were AI/chat artefacts present in the decoded artefacts that could help interpret the context of the user activities.
- Interpretation should be focused on the artefacts collected and not on user intentions.

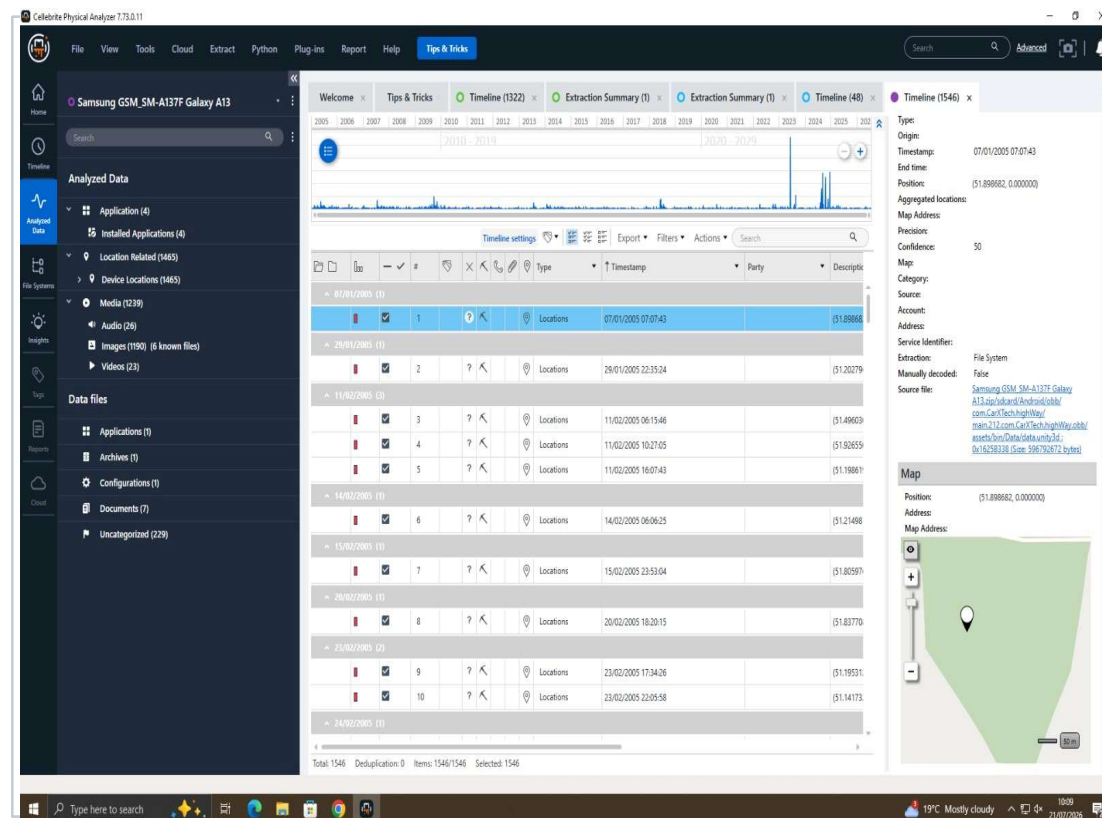


Practical Cellebrite evidence screenshot

Contacts & Communication Artefacts

Mobile Forensic Investigation using Cellebrite Physical Analyzer

- Recovered contacts can be related to the name, number, username, and identity of an application.
- Native and application contacts should be differentiated based on their origin.
- The communication artifacts can then be correlated with the identities of contacts and time stamps.
- In some cases, communication artifacts on some devices can be limited due to extraction and/or decoding limitations.

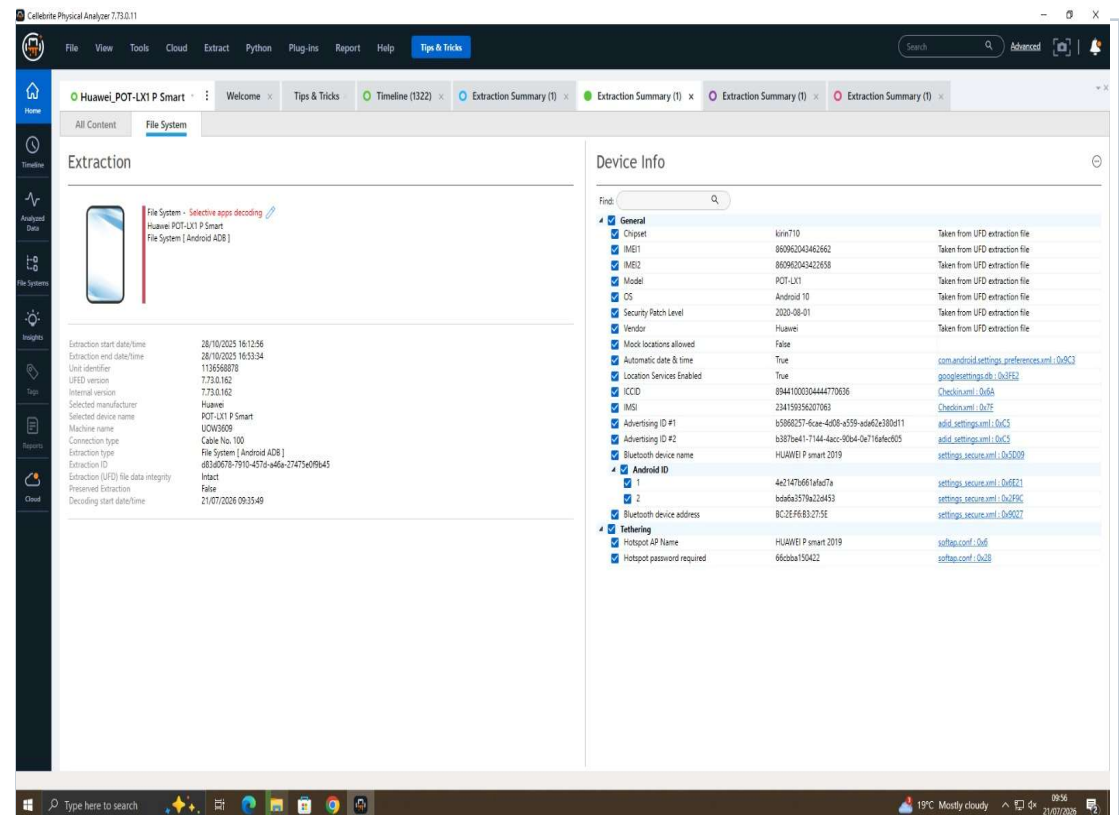


Practical Cellebrite evidence screenshot

File System & Device Artefacts

Mobile Forensic Investigation using Cellebrite Physical Analyzer

- File-system artefacts reveal application directories, databases, caches, documents, archives, and media.
- Source paths are critical because they indicate the source of the artefact.
- Device details aid in understanding extraction capabilities and limitations.
- File-system artefacts may support findings from high-level decoded artefacts.

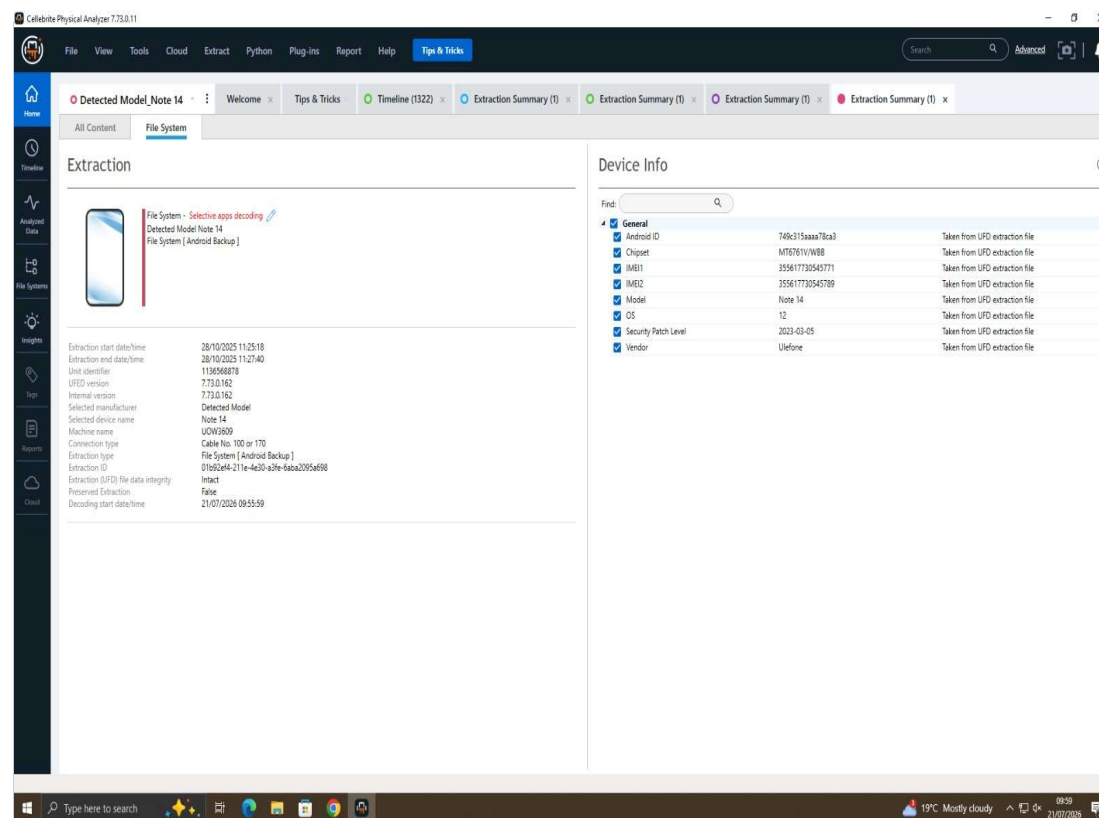


Practical Cellebrite evidence screenshot

Location Evidence

Mobile Forensic Investigation using Cellebrite Physical Analyzer

- Physical Analyzer categorized recovered location-based artifacts into device locations.
- Map visualization aids in understanding the meaning of the coordinates and related timestamp data.
- The location-based evidence can be cross-referenced with the media metadata and other device events.
- Coordinates that lack strong metadata must be carefully understood.

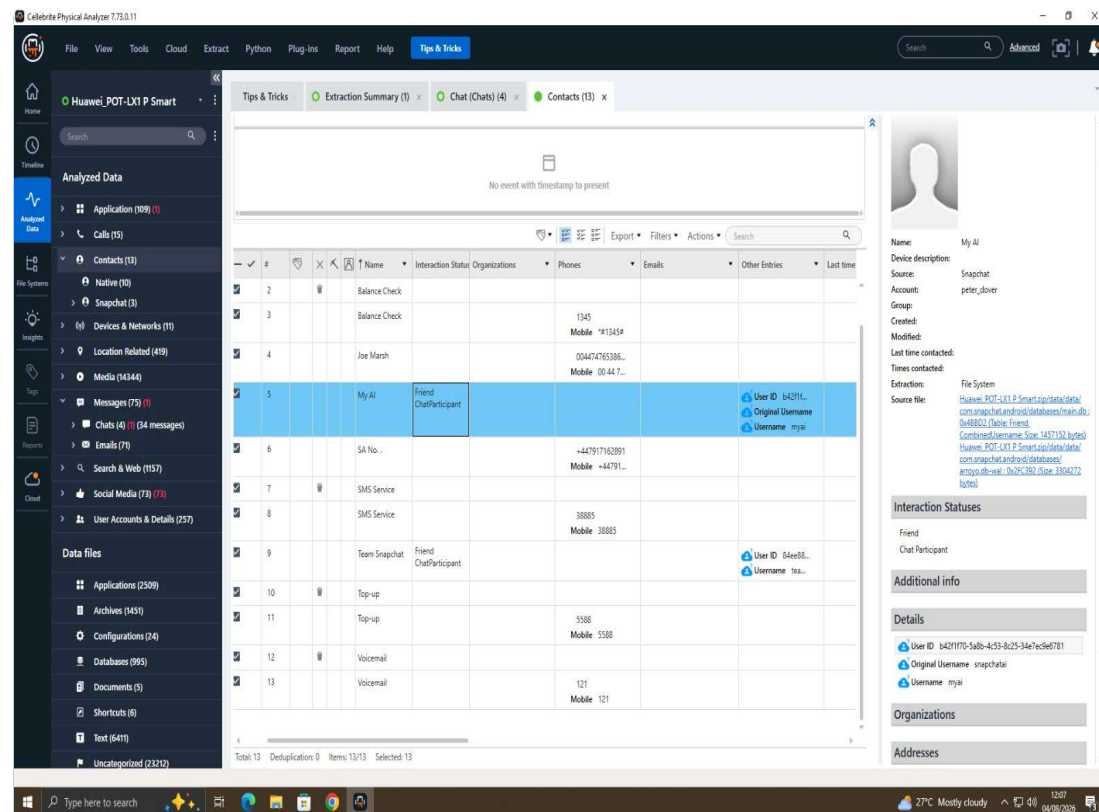


Practical Cellebrite evidence screenshot

Timeline Reconstruction

Mobile Forensic Investigation using Cellebrite Physical Analyzer

- Chronological organization allows for a timeline analysis of discovered events.
- Timestamps of various locations, media, applications and communications can be compared in order to understand device usage.
- The correlation becomes greater when a certain period is backed by more than one independent source of artefacts.
- Any unusual date or a default timestamp should be validated.

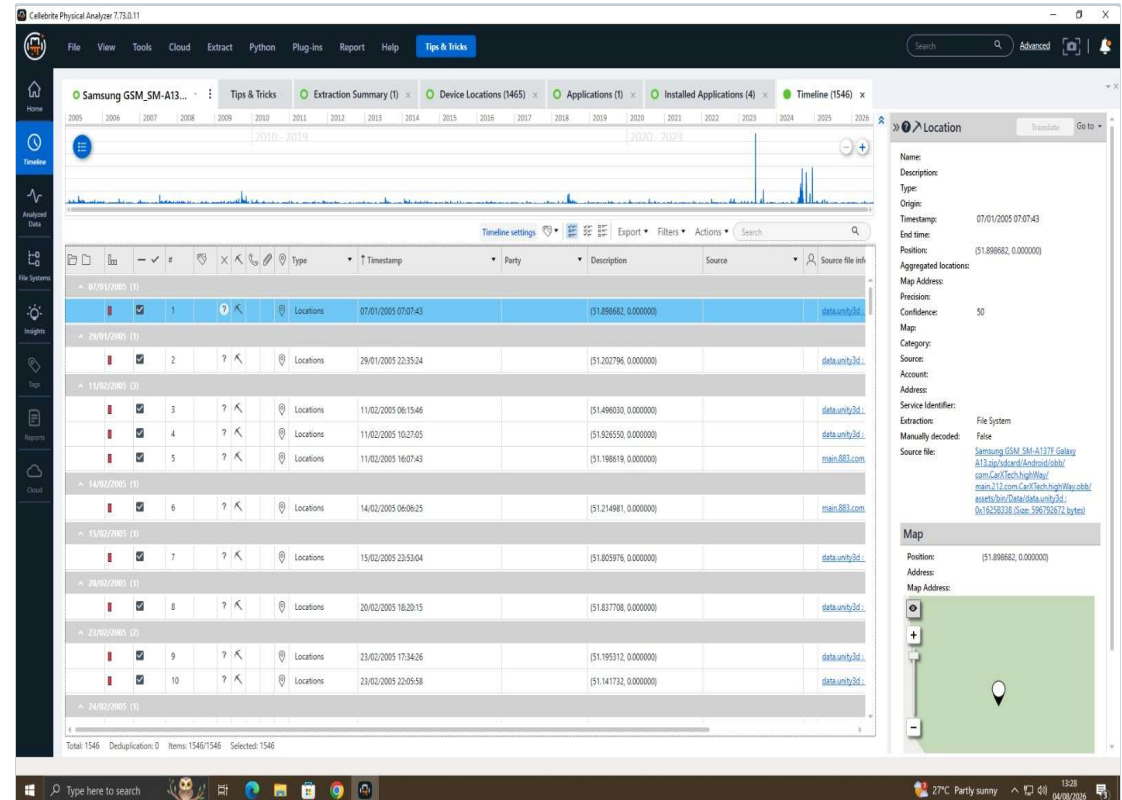


Practical Cellebrite evidence screenshot

Key Findings & Limitations

Mobile Forensic Investigation using Cellebrite Physical Analyzer

- The actual process proved the possibility of acquisition, decoding, and analysis on various types of Android devices.
- The data recovered included information from applications, contacts, media files, locations, documents, and many other system artefacts depending on the specific device.
- Communication types which cannot be examined should not be considered as non-existent – this is simply a forensic problem.
- Comparing different devices and artefacts yields the most reliable interpretation framework.

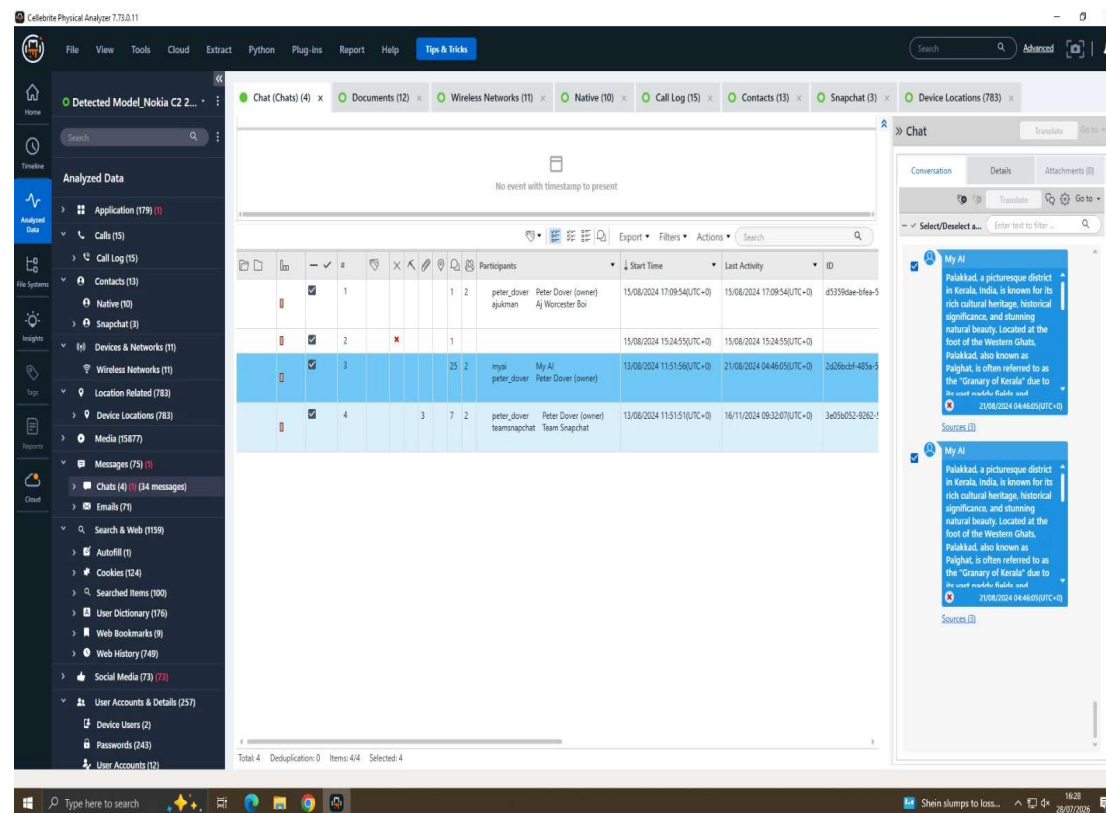


Practical Cellebrite evidence screenshot

Conclusion

Mobile Forensic Investigation using Cellebrite Physical Analyzer

- Structured process was applied through the use of tools such as Cellebrite UFED and Physical Analyzer.
- It is a good example of how device metadata, applications, contacts, file system artifacts, location and timeline information could be used in the mobile device forensics.
- The integrity of the evidence is ensured by documentation, acquisition, provenance, validation and careful interpretation of unproven information.
- The findings need to be presented distinguishing the recovered facts, the relations found and limitations of the examination.



Practical Cellebrite evidence screenshot