DIGITAL FORENSIC ANALYSIS (ACCA7031)

Final Combined Report

Submitted By,

Student Name: Md Al Amin Sarkar Reday
Student ID: 2406207

Table of content

Introduction....2
Digital Forensics Service Delivery Across Sectors....2
Professional Certification Pathways and Credential Requirements....3
National Job Market Dynamics....3
International Career Mobility and Global Opportunities....4
Emerging Skill Requirements and Career Development....4
Conclusion....5
Narrative Investigation: Corporate Espionage Through Digital Forensics and Behavioral Analysis....6
Investigation Genesis and Contextual Framework....6
Device Examination Methodology and Initial Discoveries....7
Analysis....10
Nokia forensics....11
Evidence tagging from the physical analyser....12
Forensic investigation on Huawei....15
Analysis....21
The Ulefone Device: Network Node and Conspiracy Archive....24
Artifacts....24
Analysis....27
Technical and Forensic Profile of the Samsung Galaxy A13....28
Artifacts captured form samsung....29
Conclusion....36

Introduction

The global industry of digital forensics has seen a great deal of growth in the past decade, but this has been driven by the increasing prevalence of cybercrime, as well as the stringent compliance requirements and organisational recognition of forensic capabilities as key infrastructure for security [1]. This report explores the contemporary field using an industry and career development framework to analyze employment opportunities, professional credential pathways, geographical market dynamics and emerging skill requirements [2]. The analysis includes forensic services delivery in law enforcement, corporate and consultancy sectors, professional certification frameworks and international job market dynamics. This examination shows that digital forensics is a strong career area with stable demand, several specialisation routes and possibilities for mobility abroad. Professionals setting up forensic expertise position themselves to work in an expanding field with significant talent shortages as well as offering competitive compensation commensurate with specialised knowledge [3]. Strategic professional development with a combination of technical credentials along with complementary certifications and soft skills for advancement to senior positions. The need to evolve with technological shifts and investigate complexities means that the field continually seeks to adapt to technology changes and challenges that will make it relevant for those who work in it and provide continuous skills development to meet the market needs in different sectors and geographical locations for long-term relevance.

Digital Forensics Service Delivery Across Sectors

Law Enforcement and Governmental Agencies

Digital forensics services are employed in three main areas: law enforcement, corporate organisations and professional consulting companies, and each has different operational requirements. Law enforcement agencies at federal, state and local levels employ the professional in specialised units focussed on the area of criminal and cyber crime investigation [4]. In developed nations such as the United States and United Kingdom there has been a significant increase in government-funding of forensic capability, with agencies developing dedicated laboratories and hiring specialised personnel. These governmental agencies offer stable jobs and structured careers, although pay is often lower than in the equivalent private sector jobs [5].

Corporate and Consulting Environments

Corporate sector forensic operations have seen dramatic growth as organisations have realised the need for in-house capabilities for incident response, regulatory compliance and risk management [6]. Financial institutions, healthcare organisations, and technology companies have in-house teams to support the system with fraud investigation, breach response, and regulatory investigations. The corporate industry, with higher pay, more flexibility in work arrangements, and more pay, usually pays more than law enforcement. Professional consulting companies offer

services on a contract basis, offering professionals exposure to diverse situations and technologies, but often requiring intense work schedules and client interactions [7].

Professional Certification Pathways and Credential Requirements

Core Forensic Certifications

Professional certifications have become important qualifications since employers have been demanding certified people to fill the role of investigator [8]. The certification of Certified Forensic Computer Examiner, administered by International Society of Forensic Computer Examiners, is the longest-established certification, where the candidates must demonstrate practical competency by examining actual forensic cases [9]. The GIAC Certified Forensic Examiner credential is focused on practical forensic analysis and evidence preservation methodologies and the candidate is required to complete authorised training via SANS Institute or equivalent programmes [10].

Vendor-Specific and Maintenance Requirements

There are vendor-specific certifications by Cellebrite, AccessData, and Encase that are tool-specific credentials for competency with widely-deployed forensic platforms [11]. These certifications usually mandates the completion of manufacturer provided training programmes and a successful completion of practical examinations. Professional certifications have continuing education requirements, which keeps credential holders abreast of the changes in forensic practices and technologies [12]. The certification landscape engenders career credentialing pathways for professionals who are able to systematically move through career progression from entry-level positions with advanced specialisations.

National Job Market Dynamics

Developed Markets: United States and United Kingdom

The United States is the biggest digital forensics job market with consistent demand across federal law enforcement and corporate fields [13]. The U.S. Bureau of Labor Statistics estimates 13% growth through 2032 which is considerably higher than the average occupation growth. In major technology centres organisations are competing hotly for forensic talent with senior positions fetching between $120,000 to $180,000 USD [14]. The United Kingdom market is no different, and the National Crime Agency and corporate organisations have substantial forensic operations [15].

Emerging Markets: India and Middle East

Within the Indian market, digital forensics employment has grown significantly during the past five years due to an increase in governmental regulations [16]. Multinational corporations that have technology centres in India are increasingly developing forensic capabilities, and this creates huge employment opportunities. However, there are huge skill gaps in the Indian forensic market with the demand being much higher than the number of trained professionals [17]. The

Middle Eastern market has become of growing importance, due to government investment in cybersecurity capabilities while digital infrastructure is rapidly expanding [18].

International Career Mobility and Global Opportunities

Digital forensics has become more internationalised with professional credentials and expertise being recognised internationally and allowing career mobility for qualified professionals [19]. The CFCE and GFCE credentials retain international recognition that will ease professional transitions from one country to another. Many professionals build their career in sequences of more than one country, having gained experience in various legal systems and technological environments. English-language skills and recognised professional qualifications are an important boost to international careers.

Remote work arrangements have increased the range of forensic opportunities across the globe, some consulting firms and corporate organisations employ forensic professionals and these are spread across multiple countries [20]. This development allows professionals from lower compensation countries to access higher compensation opportunities. International forensic investigation in which cross border criminal activity is involved leads to a demand for professionals with knowledge of various legal systems and international cooperation mechanisms [21]. These positions generally require a lot of experience although there are opportunities to contribute to important transnational investigations.

Emerging Skill Requirements and Career Development

Soft Skills and Career Progression Pathways
Soft skills development is increasingly crucial in career progression and the ability to communicate, interact with clients and write reports are just a few skills distinguishing professionals moving to senior careers [24]. Forensic professionals will often act as expert witnesses and will need presentation skills and the ability to communicate technical concepts to non-technical individuals. Career progression occurs through several routes such as technical career progression, management career progression, specialisation in particular fields, or through consulting practice [25].

Conclusion

Digital forensics is a solid and expanding field of professional practice with career opportunities in law enforcement and corporate and consultant sectors in developed and emerging economies. Professional certifications create credentialing pathways for validating evidence of expertise and career progression. National and international job markets show a continued demand for forensic professionals with differences in their compensation depending on geographic location and specialisation. Emerging skill requirements are focusing more on complementary skills that combine both forensics and cybersecurity with broader technical programming skills. Multiple

career progression pathways allow professionals to design a career to personal preferences of technical depth, management responsibility, or practicing consultation.

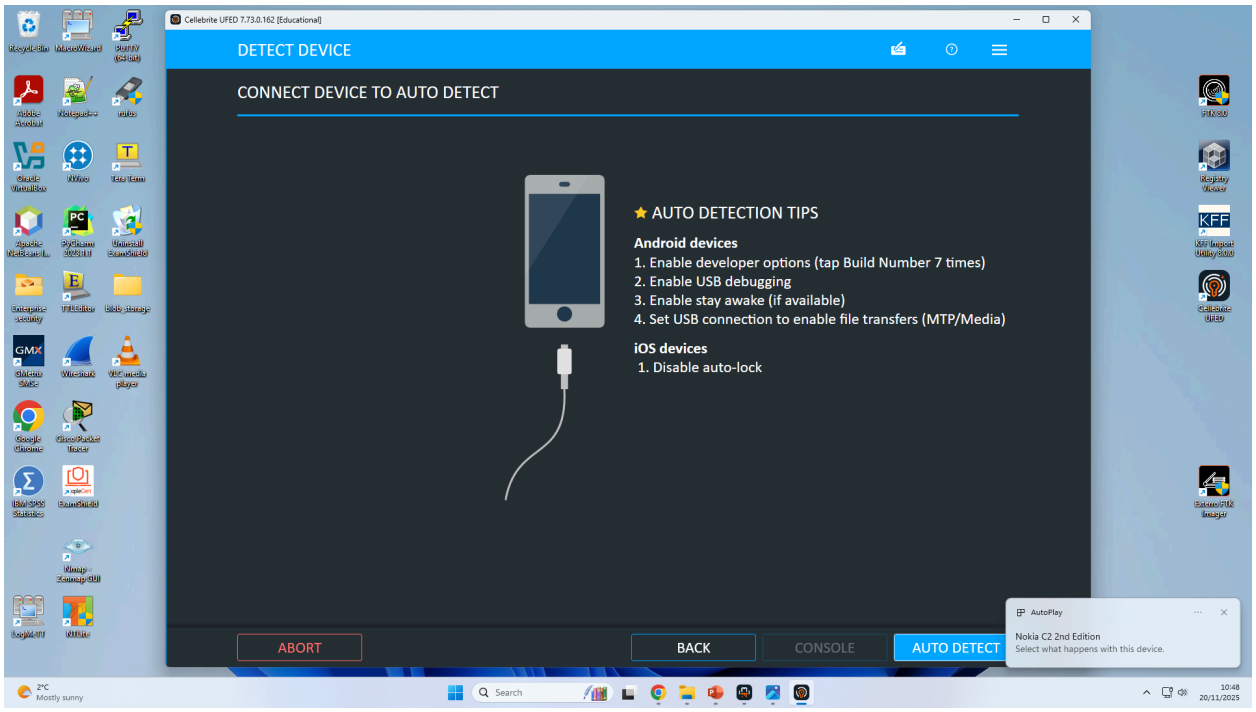
Narrative Investigation: Corporate Espionage Through Digital Forensics and Behavioral Analysis

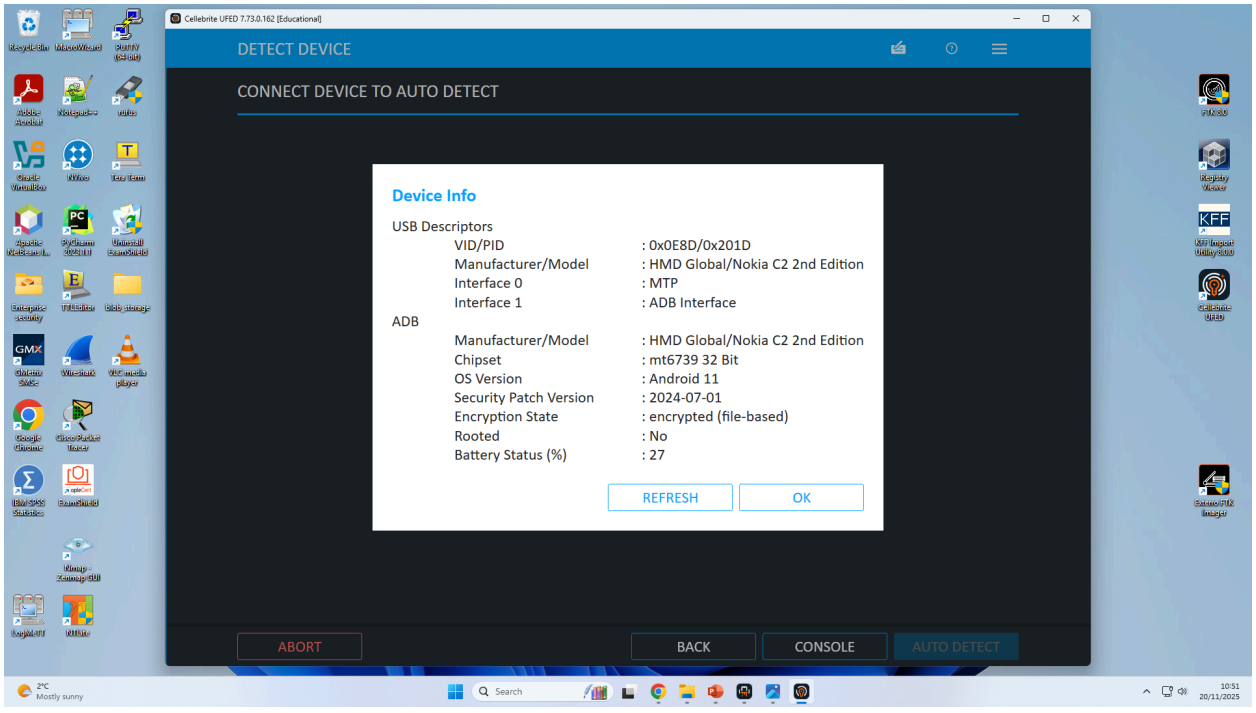
Investigation Genesis and Contextual Framework

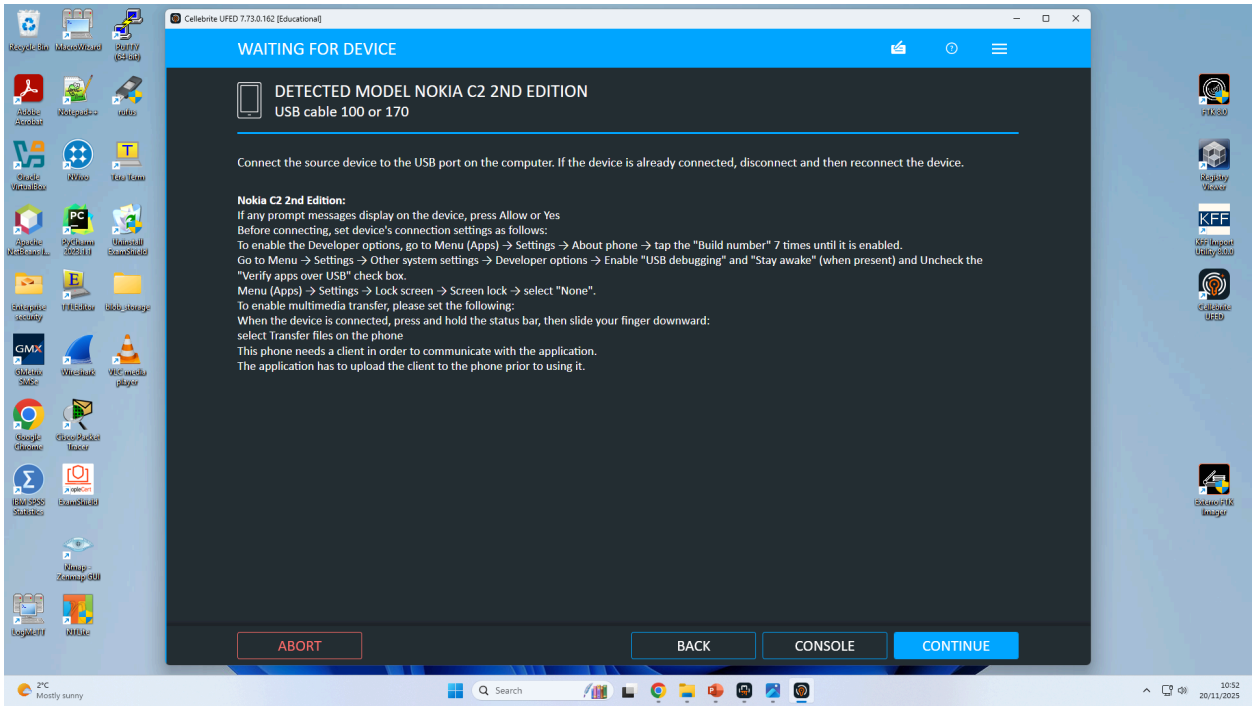
The investigation was initiated as the result of formal notification from Quantum Technologies, a technology-intensive research corporation, specializing on technologies in the area of advanced computational systems, about a suspected unauthorized access to proprietary research databases that contained sensitive intellectual property. The notification concerned in particular issues about the QT-AI-2025 patent database, which is a secure repository of detailed technical specifications, design parameters and implementation methodologies for an artificial intelligence-based neural processing system that represents several years of research investment and considerable commercial value.

Initial intelligence gathering determined that a somewhat disgruntled employee with higher system access privileges who was identified as Emma had been flagged by internal security monitoring systems for unusual system access patterns to the sensitive database during non-standard hours. Quantum Technologies internal investigation team had noticed that Emma's database queries went beyond her normal work obligations and included systematic extraction of entire design documentation, source code repositories and technical specifications unrelated to her defined projects. These preliminary findings provided probable cause for law enforcement intervention and warrant procuring search warrants for seizure and forensic examination of electronic devices that may contain evidence of IP theft.

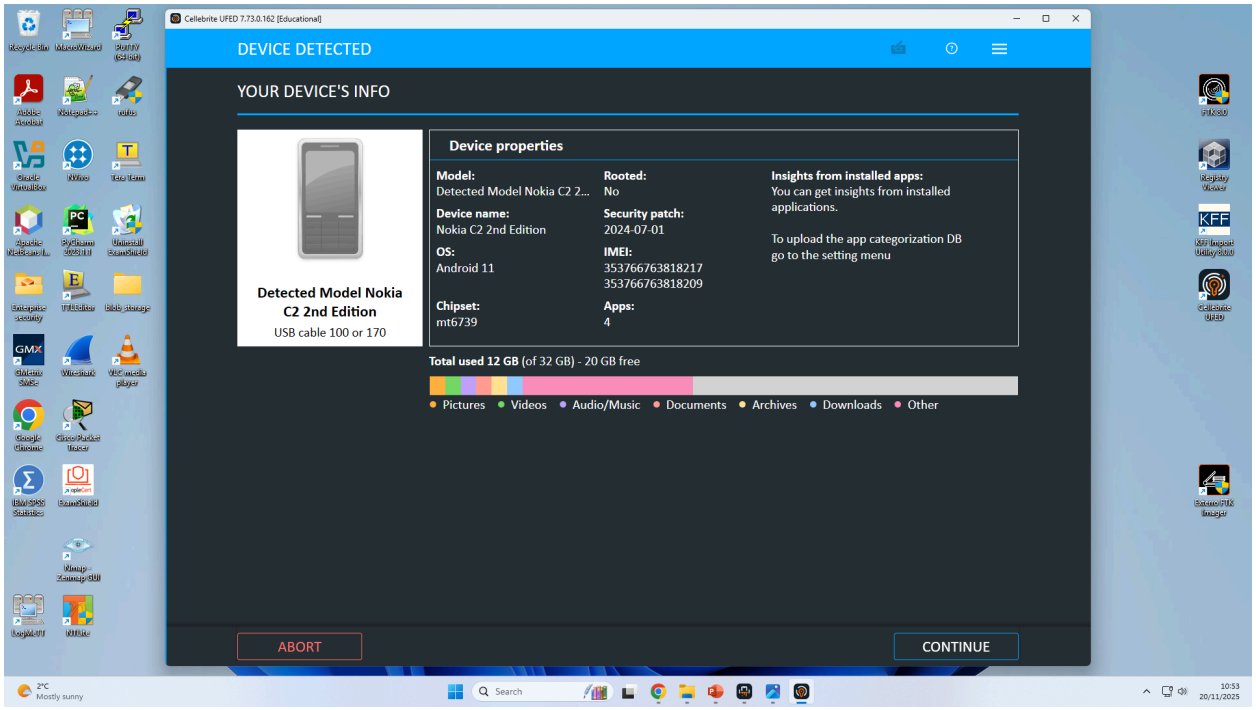
Device Examination Methodology and Initial Discoveries

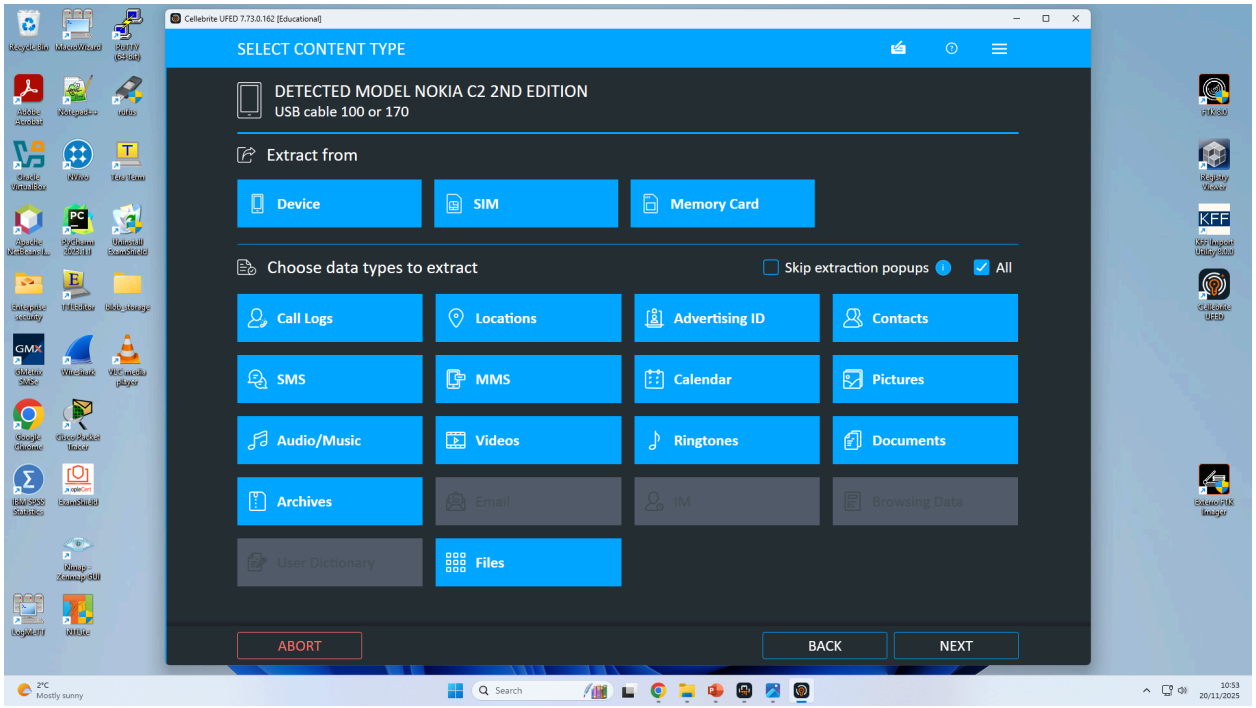


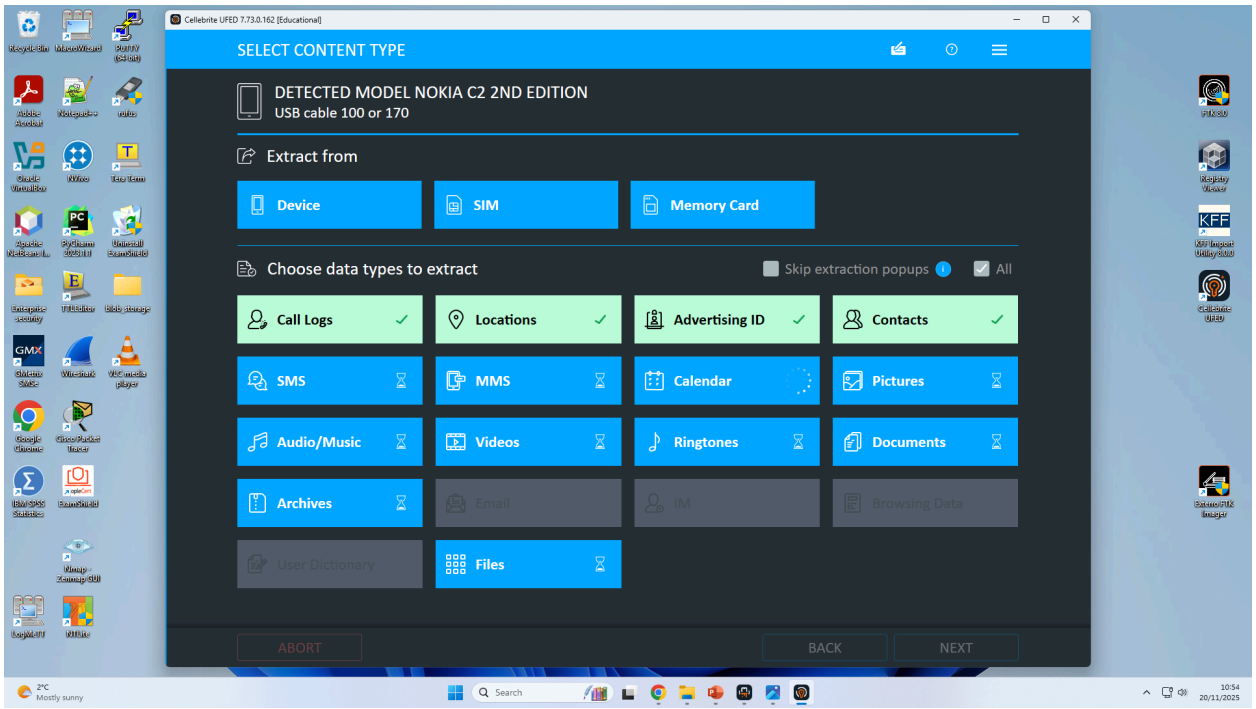


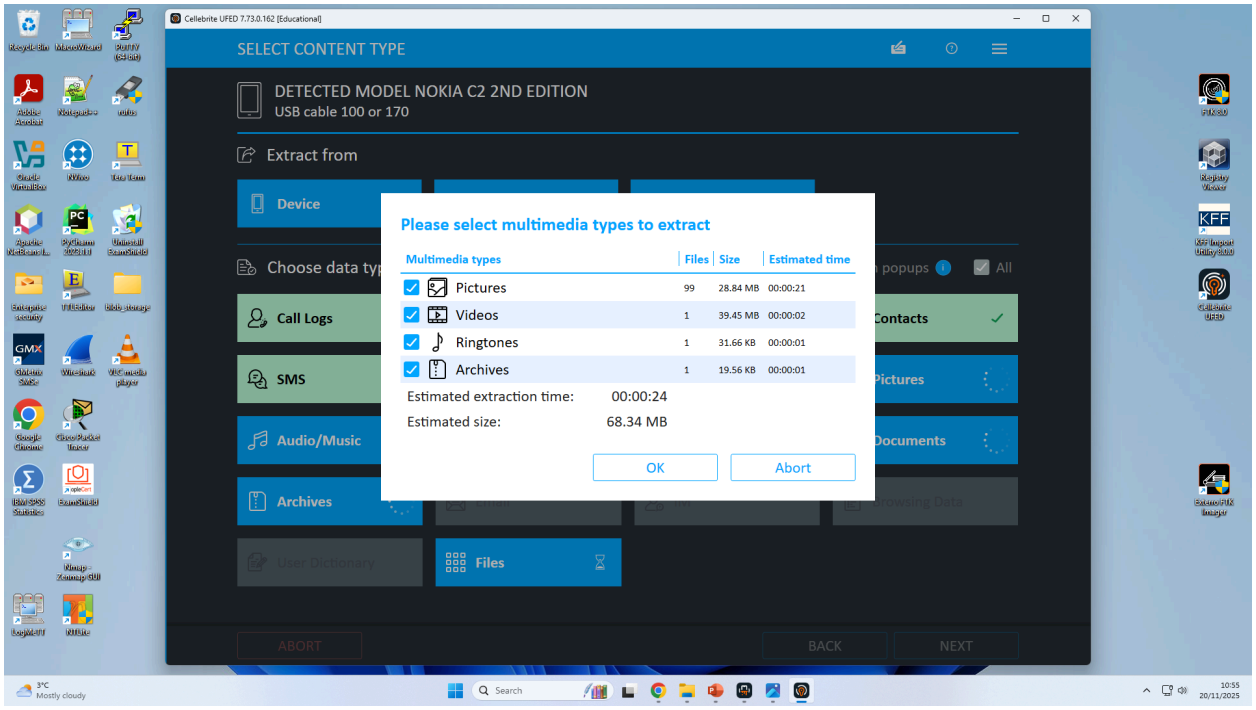

Cellebrite UFED 7.73.0.162 [Educational]
WAITING FOR DEVICE
DETECTED MODEL NOKIA C2 2ND EDITION
USB cable 100 or 170
Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.
Nokia C2 2nd Edition:
If any prompt messages display on the device, press Allow or Yes
Before connecting, set device's connection settings as follows:
To enable the Developer options, go to Menu (Apps) -> Settings -> About phone -> tap the "Build number" 7 times until it is enabled.
Go to Menu -> Settings -> Other system settings -> Developer options -> Enable "USB debugging" and "Stay awake" (when present) and Uncheck the "Verify apps over USB" check box.
Menu (Apps) -> Settings -> Lock screen -> Screen lock -> select "None".
To enable multimedia transfer, please set the following:
When the device is connected, press and hold the status bar, then slide your finger downward:
select Transfer files on the phone
This phone needs a client in order to communicate with the application.
The application has to upload the client to the phone prior to using it.
ABORT
BACK
CONSOLE
CONTINUE

\


Cellebrite UFED 7.73.0.162 [Educational]
DEVICE DETECTED
YOUR DEVICE'S INFO
Detected Model Nokia C2 2nd Edition
USB cable 100 or 170
Device properties
Model:
Detected Model Nokia C2 2...
Rooted:
No
Insights from installed apps:
You can get insights from installed applications.
Device name:
Nokia C2 2nd Edition
Security patch:
2024-07-01
To upload the app categorization DB go to the setting menu
OS:
Android 11
IMEI:
353766763818217
353766763818209
Chipset:
mt6739
Apps:
4
Total used 12 GB (of 32 GB) - 20 GB free
Pictures
Videos
Audio/Music
Documents
Archives
Downloads
Other
ABORT
CONTINUE


Cellebrite UFED 7.73.0.162 [Educational]
SELECT CONTENT TYPE
DETECTED MODEL NOKIA C2 2ND EDITION
USB cable 100 or 170
Extract from
Device
SIM
Memory Card
Choose data types to extract
Skip extraction popups
All
Call Logs
Locations
Advertising ID
Contacts
SMS
MMS
Calendar
Pictures
Audio/Music
Videos
Ringtones
Documents
Archives
Email
IM
Browsing Data
User Dictionary
Files
ABORT
BACK
NEXT


Cellebrite UFED 7.73.0.162 [Educational]
SELECT CONTENT TYPE
DETECTED MODEL NOKIA C2 2ND EDITION
USB cable 100 or 170
Extract from
Device
SIM
Memory Card
Choose data types to extract
Skip extraction popups
All
Call Logs
Locations
Advertising ID
Contacts
SMS
MMS
Calendar
Pictures
Audio/Music
Videos
Ringtones
Documents
Archives
Email
IM
Browsing Data
User Dictionary
Files
ABORT
BACK
NEXT

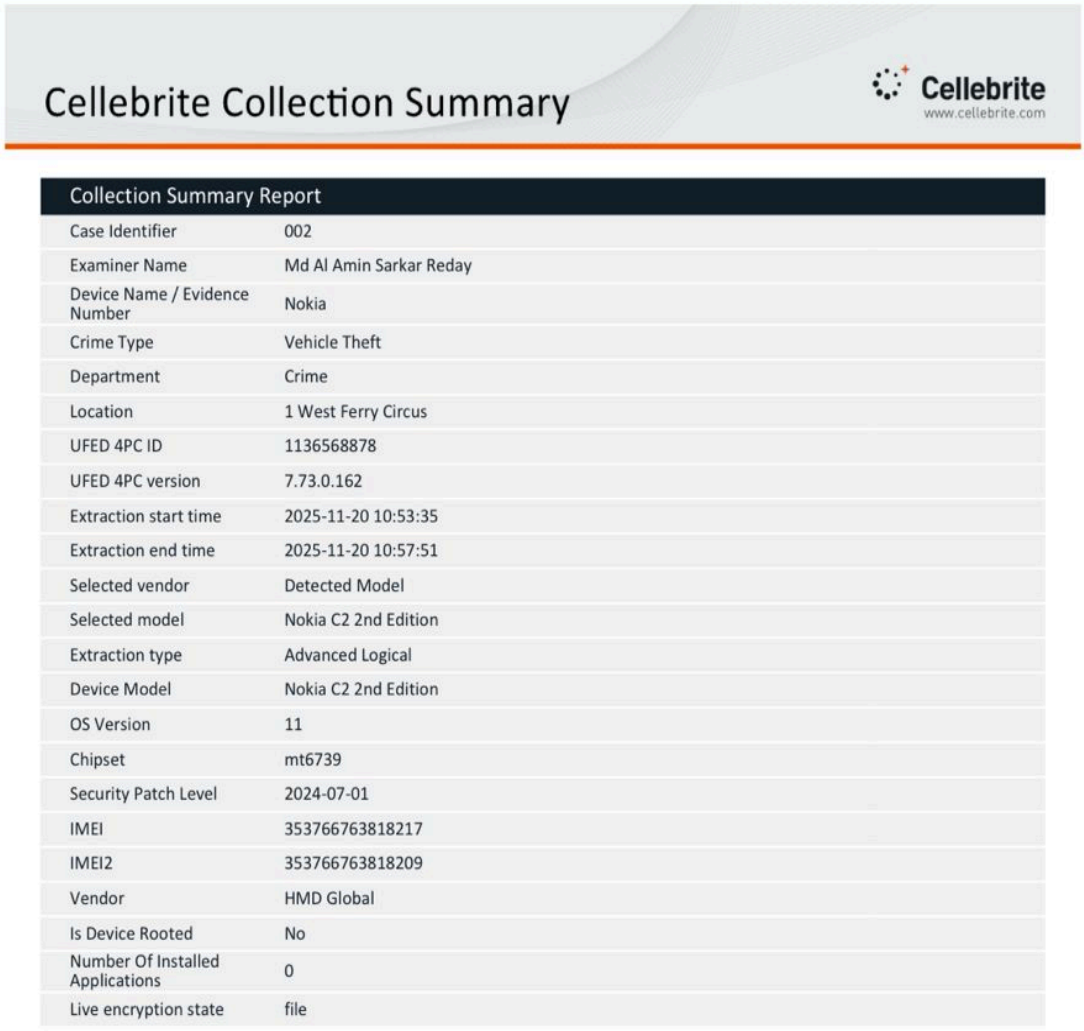


Analysis

The forensic workflow starts at the successfully detection and logical identification of the mobile device. The software requires the examiner to activate certain Android settings (such as "USB debugging" and "Stay awake"), so that the tool will be able to communicate with the device through the ADB interface. On connecting to the tool, the tool extracts key device information, including the target being a Nokia C2 2nd Edition running Android 11 with the MT6739 chipset. This stage is also where vital security metadata is captured which confirms the following facts: the device uses file-based encryption, the security patch level of the device is July 1, 2024, and the state of the device is unrooted.

Once the device is profiled, then the process proceeds to the content selection phase, where the extent of the extraction would be defined. The interface shows the various types of data that can be accessed such as Call Logs, SMS, and various multimedia, which again enables the examiner to use a targeted extraction rather than a complete physical dump. In the particular case, the configuration performs downloading multimedia artifacts like 99 pictures, a video file and ringtones. The system gives immediate feedback on the scale of the operation giving the total size of about 68MB and extraction time of less than 30 seconds on the selected items

Cellbrite collection Summary

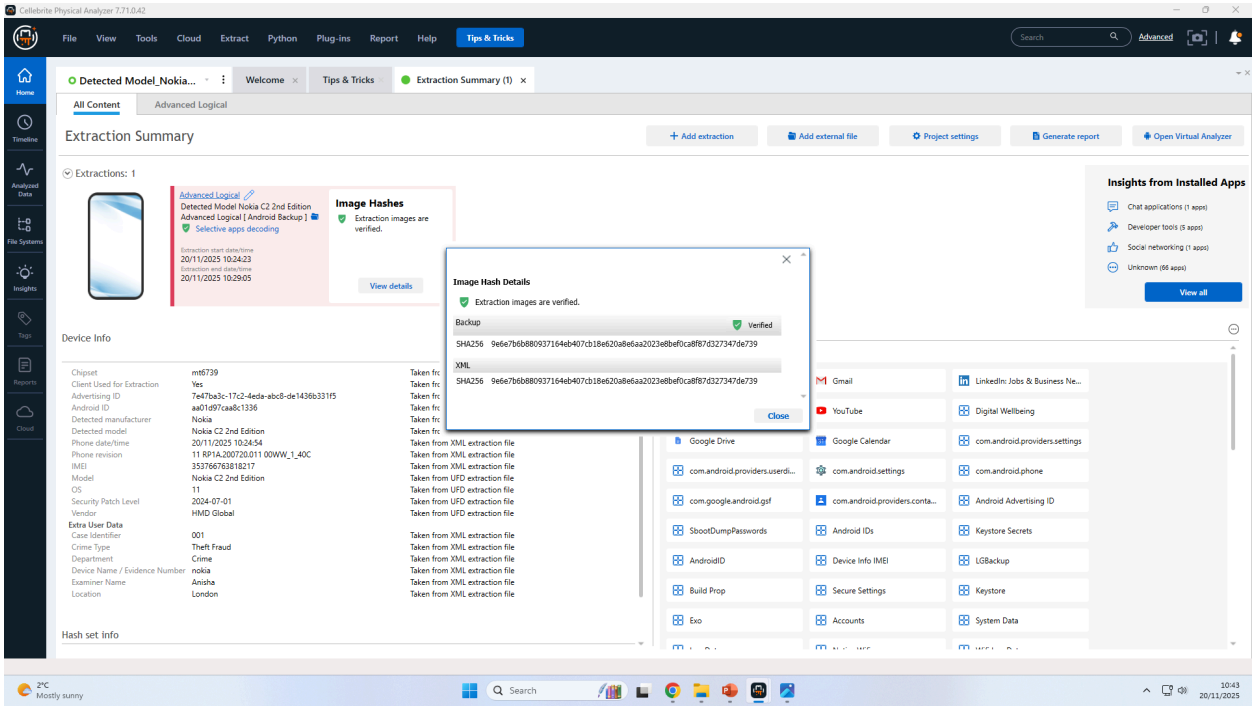


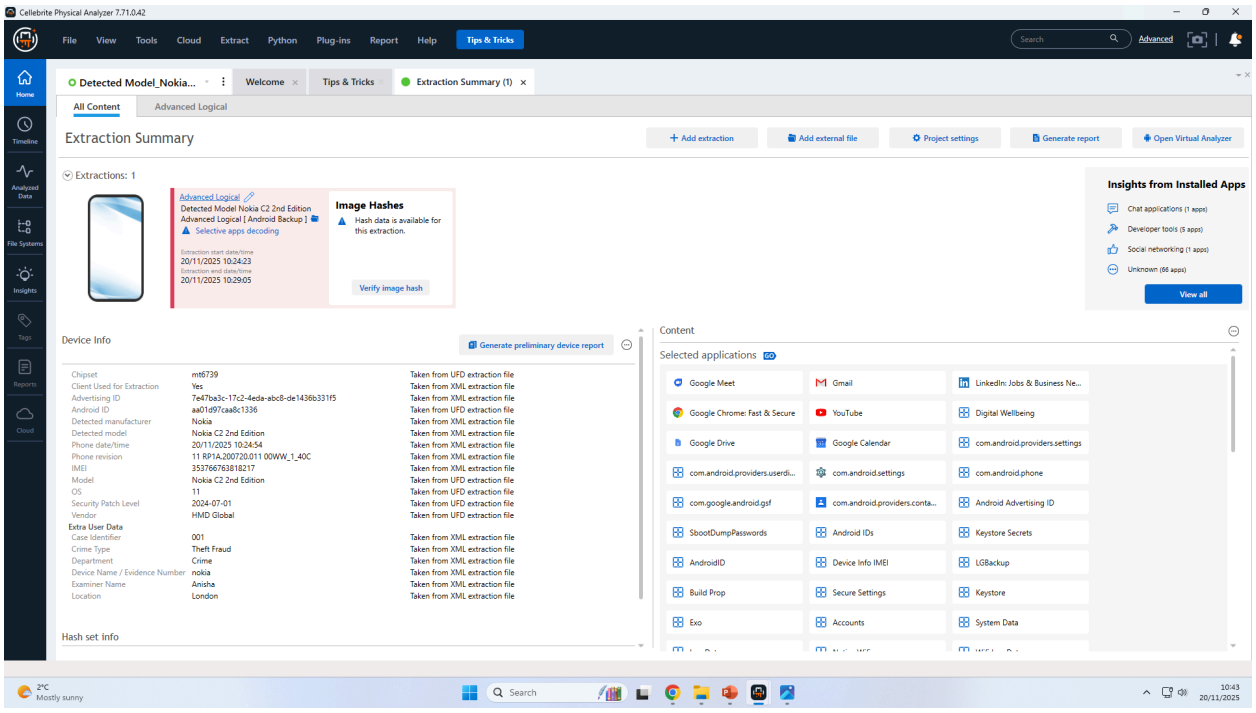
Cellebrite Collection Summary

Cellebrite
www.cellebrite.com

Collection Summary Report	
Case Identifier	002
Examiner Name	Md Al Amin Sarkar Reday
Device Name / Evidence Number	Nokia
Crime Type	Vehicle Theft
Department	Crime
Location	1 West Ferry Circus
UFED 4PC ID	1136568878
UFED 4PC version	7.73.0.162
Extraction start time	2025-11-20 10:53:35
Extraction end time	2025-11-20 10:57:51
Selected vendor	Detected Model
Selected model	Nokia C2 2nd Edition
Extraction type	Advanced Logical
Device Model	Nokia C2 2nd Edition
OS Version	11
Chipset	mt6739
Security Patch Level	2024-07-01
IMEI	353766763818217
IMEI2	353766763818209
Vendor	HMD Global
Is Device Rooted	No
Number Of Installed Applications	0
Live encryption state	file

Nokia forensics



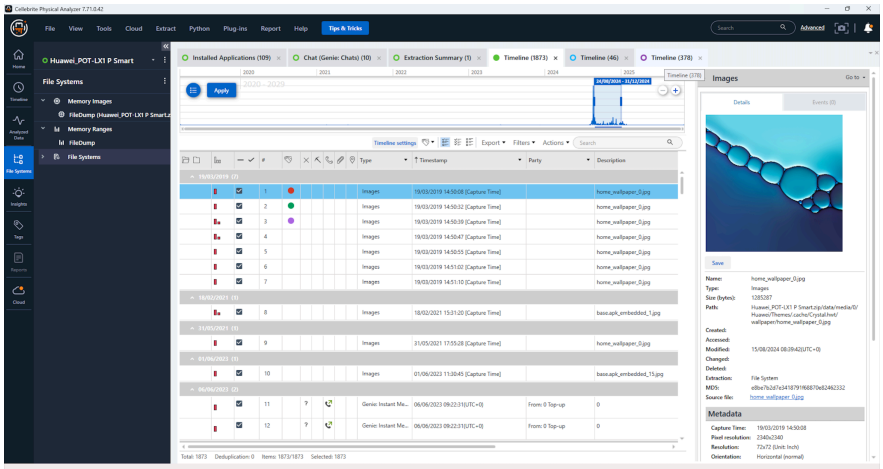


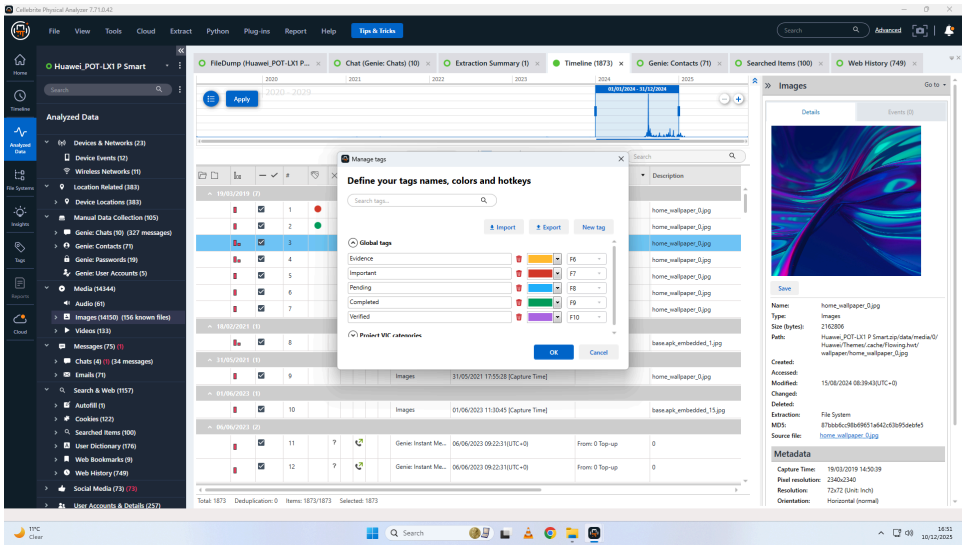
Analysis

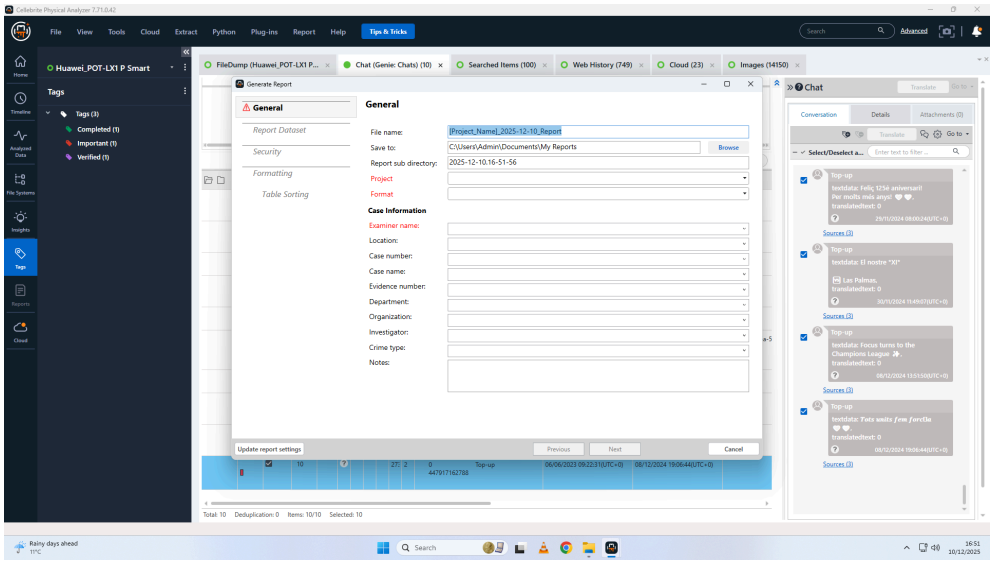
In the "Extraction Summary" view of Cellebrite Physical Analyzer, the acquired data is validated by the forensic integrity of the deducted data using cryptographic hashing and done

automatically by the software. The presented 'Image Hash Details' dialogue confirms successful verification for the Nokia C2 2nd Edition, which shows the same SHA256 hash values (starting with 9e6e7b) for the backup and XML file structure to ensure that the extracted evidence is not altered. This critical validation step, when combined with the detailed nature of the device metadata (the IMEI, Android 11 OS version, etc) creates a provable chain of custody that is essential to thereby admitting the digital evidence into a legal proceeding

Evidence tagging from the physical analyser







Analysis

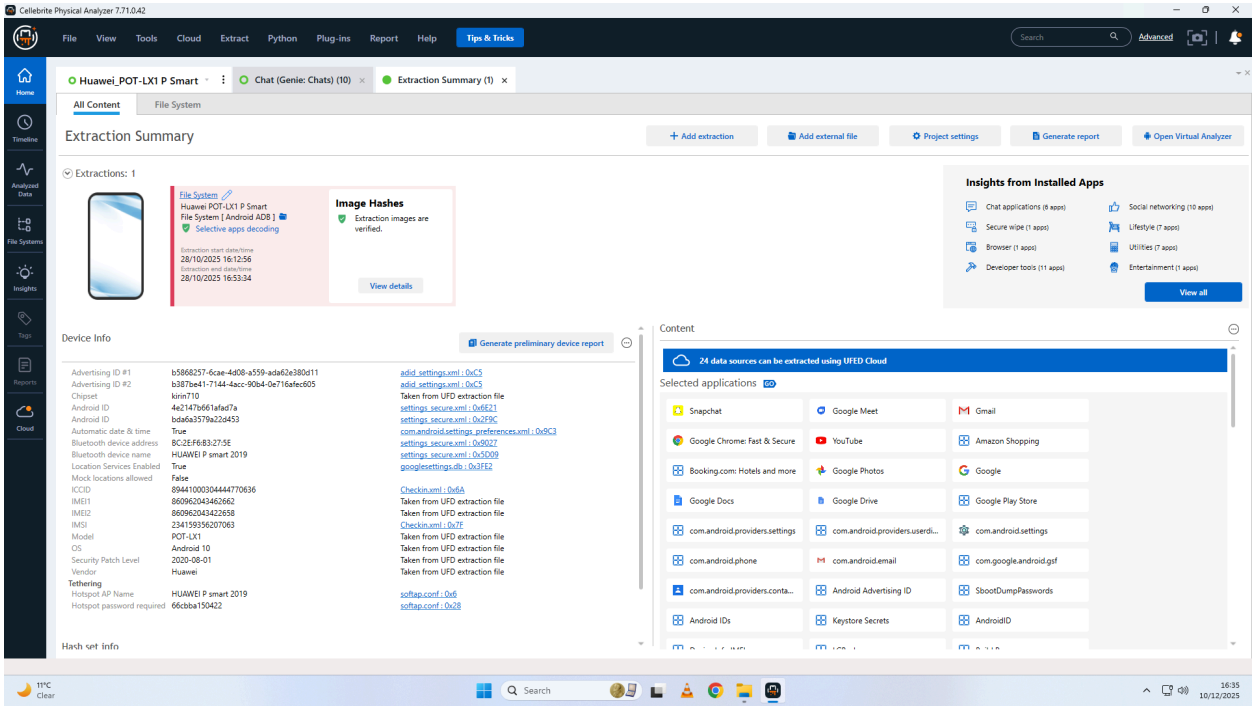
The Cellebrite Physical Analyzer workspace supports reaching deeper levels of analysis in the form of views such as "Timeline" and "Analyzed Data," which aggregate chronological events and artifacts which came out of the device. In the presented "Timeline" tab, the examiner is shown a mixed chronological list of data types, e.g. the system images ("homewalpaper0.jpg") & Instant Messages visible in the extraction. The interface offers a comprehensive dashboard on which detailed metadata, such as the time of capture, path to file, and MD5 hash, is displayed in the right-hand panel so that the properties of an artifact can be verified immediately before any classification is done.

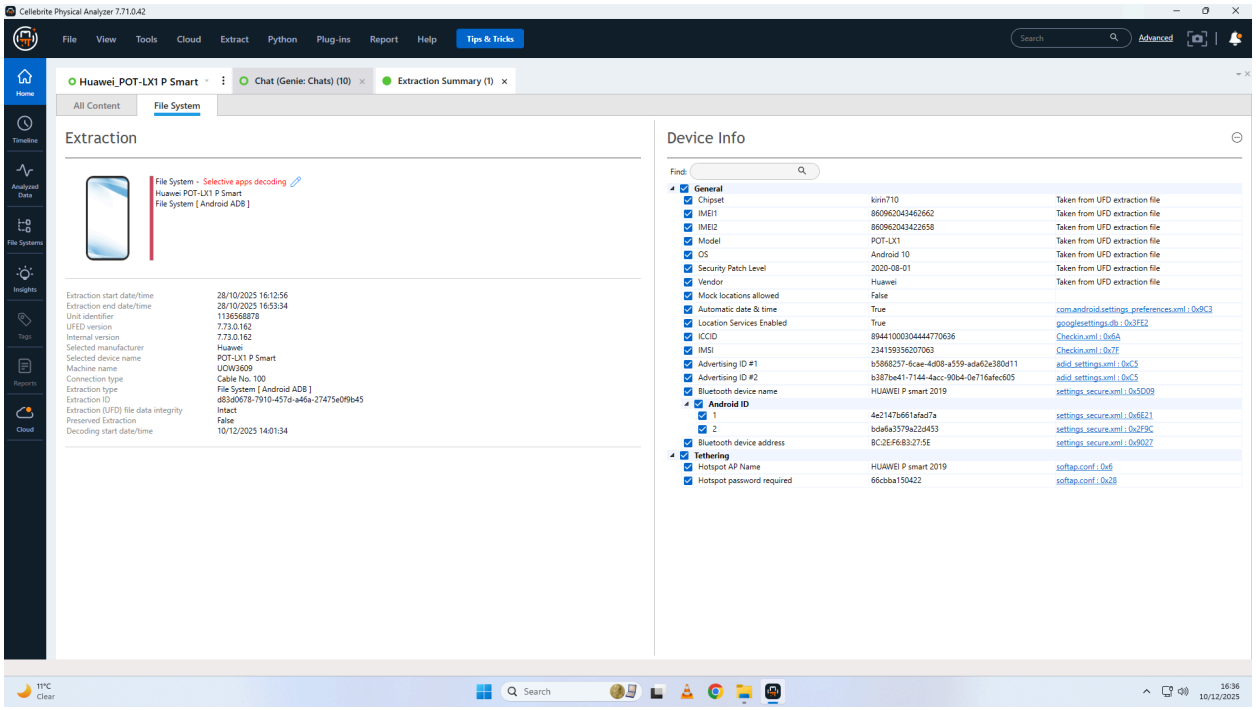
To structure this amount of data, the software supports efficient tagging of evidence directly within the interface for analysis to produce a structured report. As the main view shows, a user only has to select the relevant entry (be it a chat message, image, or location point, etc) by clicking the box adjacent to the relevant item row. Once chosen, the examiner can sort these items by specific "Tags" that are symbolically reflected in the customized value word problem as indicated by colored dots (red, green, purple) in the second column of the image in the screenshot. These indicators relate to classifications made with respect to relevance of, for example, "Pertinent", "Suspect" or custom case-specific labels such as "Project Neuro".

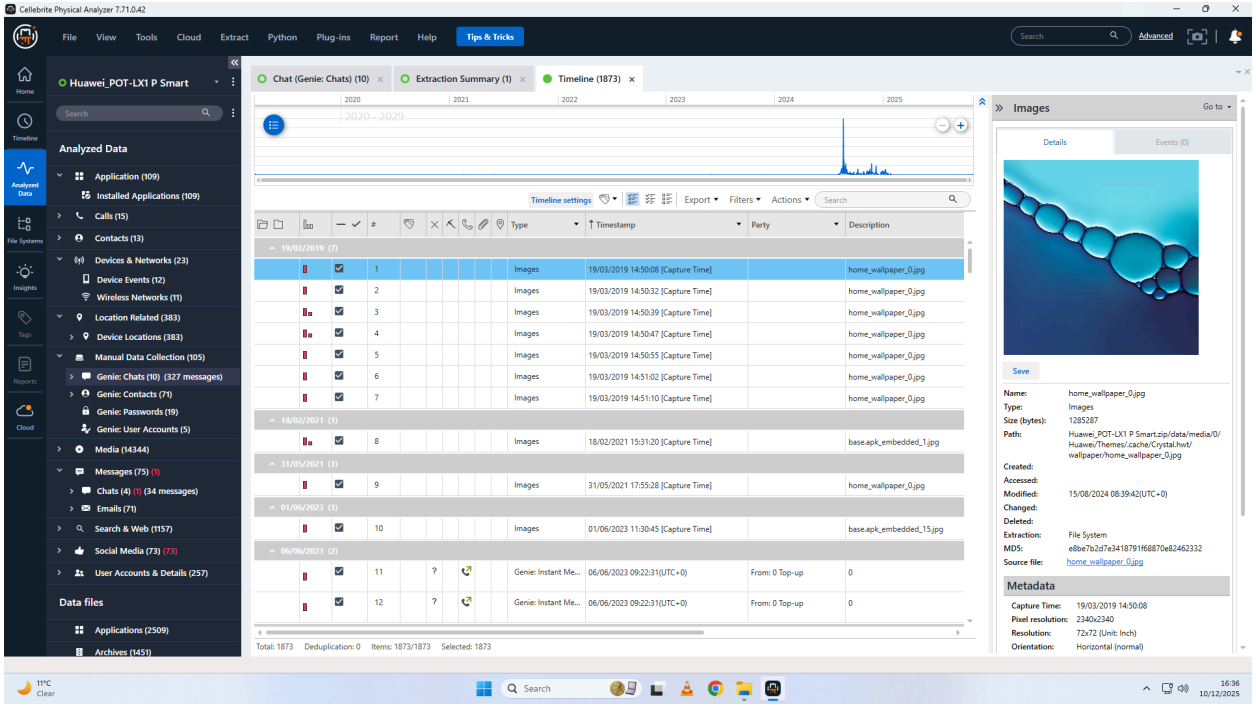
These tags are effectively critical bookmarks of the digital document that are able to group important evidence into sections that streamline the review process for the investigator. By segregating these artifacts, the examiner can easily filter through thousands of files to focus only on important findings as opposed to raw data. This classification system is essential for the last stage in reporting of the findings, as it will enable the user to finally export only the most important and tagged findings into the last phase of the forensic reporting process, ensuring the final deliverable report is concise and limited to the key objectives of the investigation

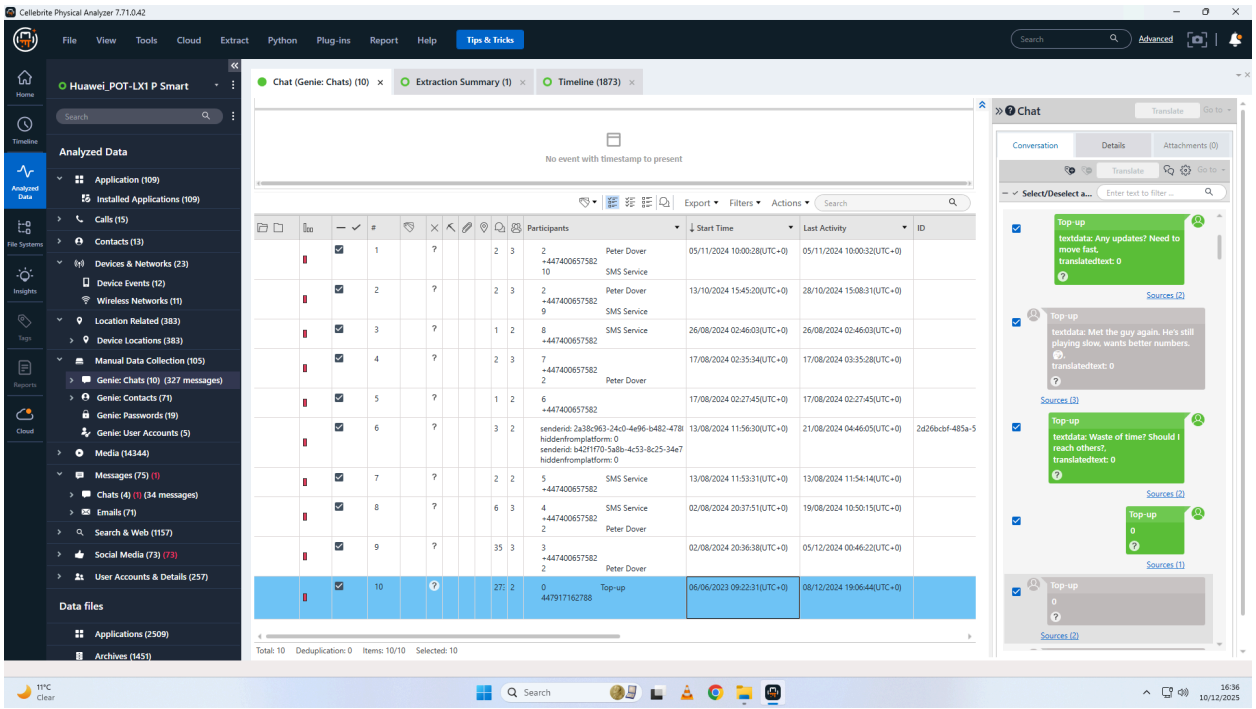
Forensic investigation on Huawei

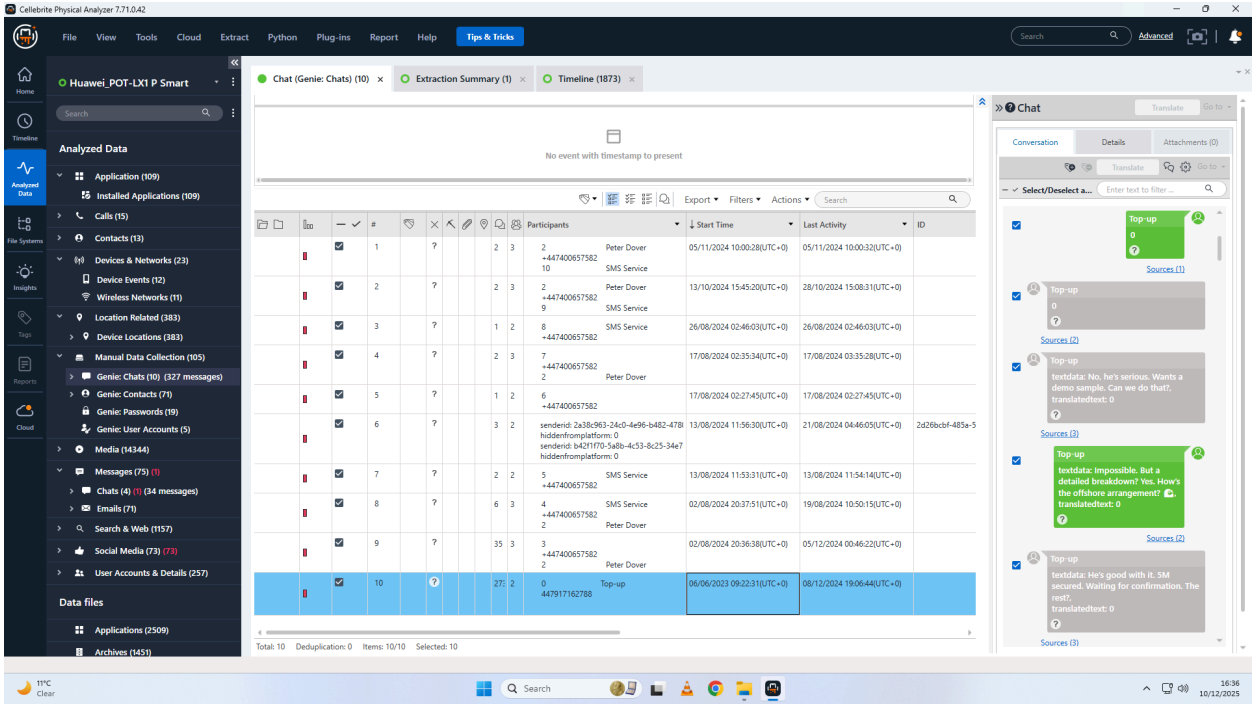
Artifacts

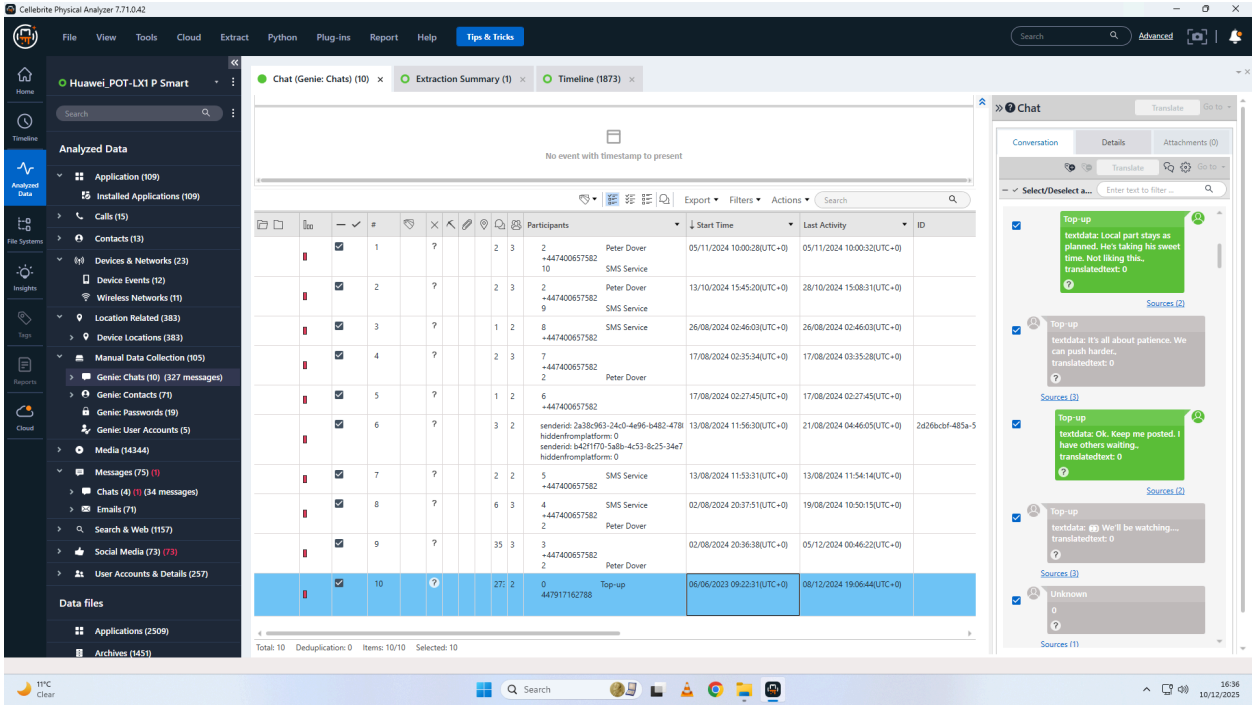


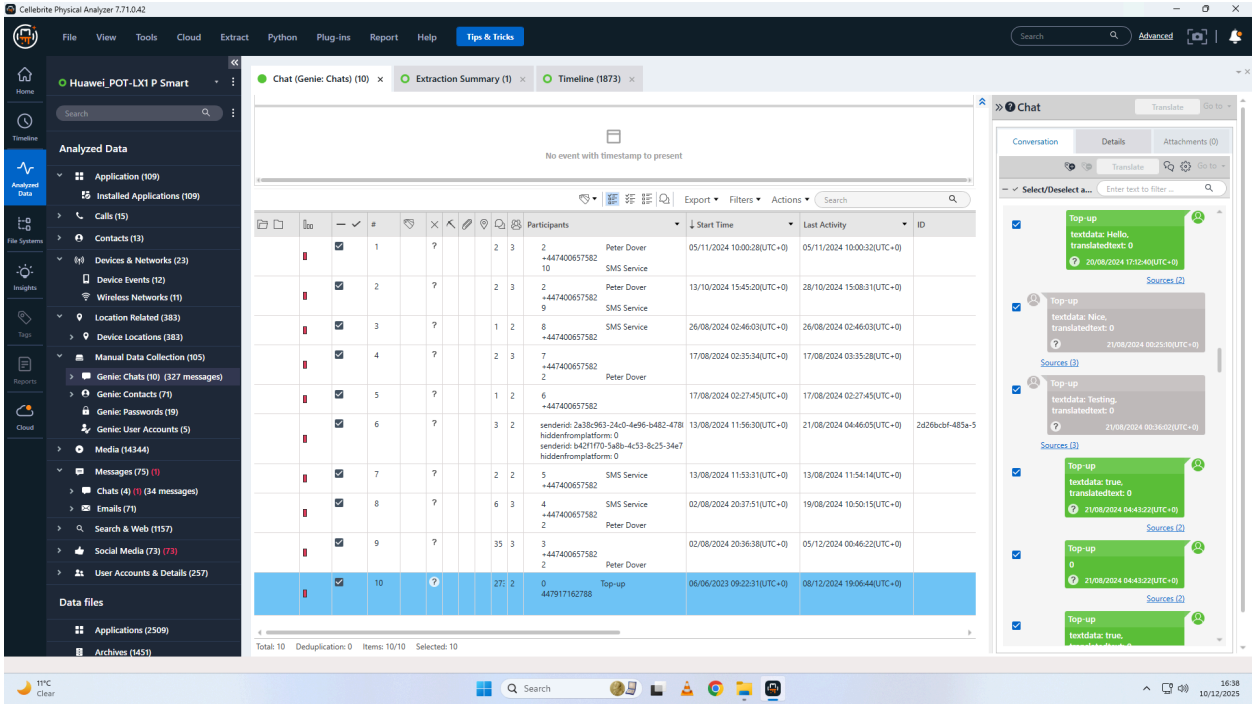


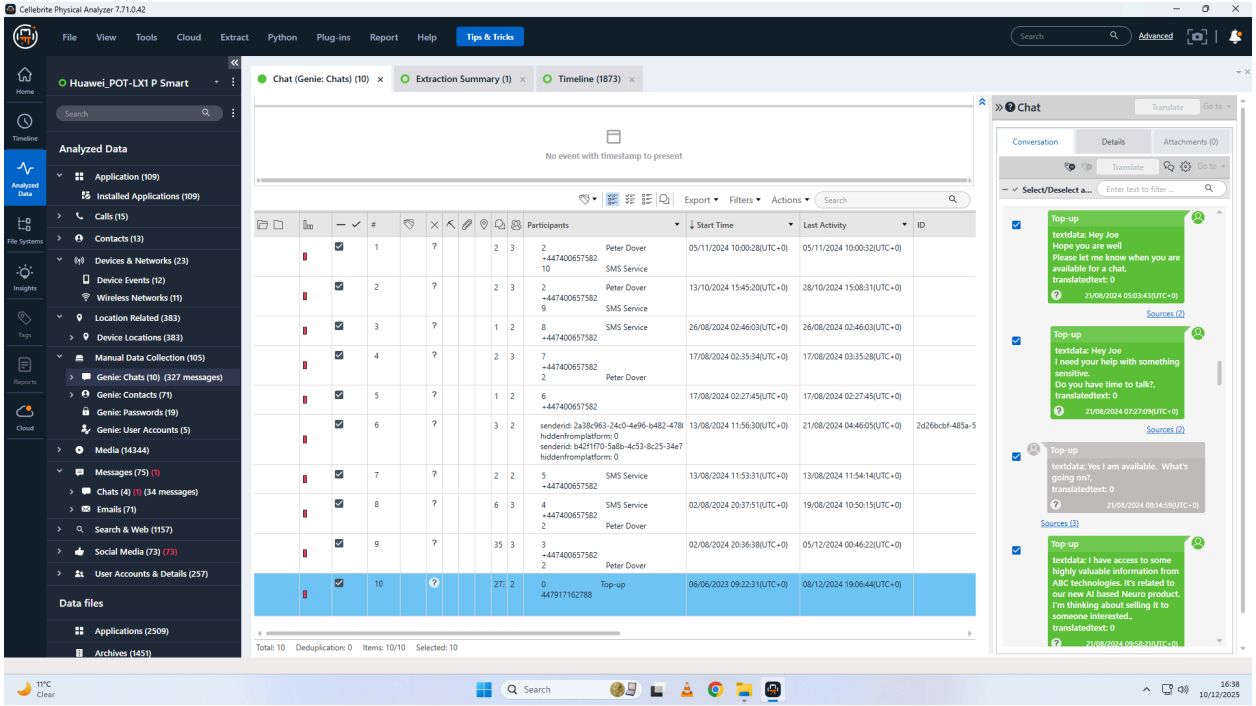

Cellebrite Physical Analyzer 7.71.0.42
File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks
Advanced
Huawei_POT-LX1 P Smart
Analyzed Data
Application (109)
Installed Applications (109)
Calls (15)
Contacts (13)
Devices & Networks (23)
Device Events (12)
Wireless Networks (11)
Location Related (383)
Device Locations (383)
Manual Data Collection (105)
Genie: Chats (10) (327 messages)
Genie: Contacts (71)
Genie: Passwords (19)
Genie: User Accounts (5)
Media (14344)
Messages (75) (1)
Chats (4) (1) (34 messages)
Emails (71)
Search & Web (1157)
Social Media (73) (73)
User Accounts & Details (257)
Data files
Applications (2509)
Archives (1451)
Chat (Genie: Chats) (10)
Extraction Summary (1)
Timeline (1873)
2020 2021 2022 2023 2024 2025
2020 - 2029
Timeline settings
Export
Filters
Actions
Type
Timestamp
Party
Description
19/03/2019 (7)
18/02/2021 (1)
31/05/2021 (1)
01/06/2023 (1)
06/06/2023 (2)
Images
Go to
Details
Events (0)
Save
Name: home_wallpaper_0.jpg
Type: Images
Size (bytes): 1285287
Path: Huawei_POT-LX1 P Smart.zip/data/media/0/Huawei/Themes/.cache/Crystal.hwt/wallpaper/home_wallpaper_0.jpg
Created:
Accessed:
Modified: 15/08/2024 08:39:42(UTC+0)
Changed:
Deleted:
Extraction: File System
MD5: e8be7b2d7e3418791f68870e82462332
Source file: home_wallpaper_0.jpg
Metadata
Capture Time: 19/03/2019 14:50:08
Pixel resolution: 2340x2340
Resolution: 72x72 (Unit: Inch)
Orientation: Horizontal (normal)
Total: 1873 Deduplication: 0 Items: 1873/1873 Selected: 1873
11°C Clear
Search
16:36 10/12/2025

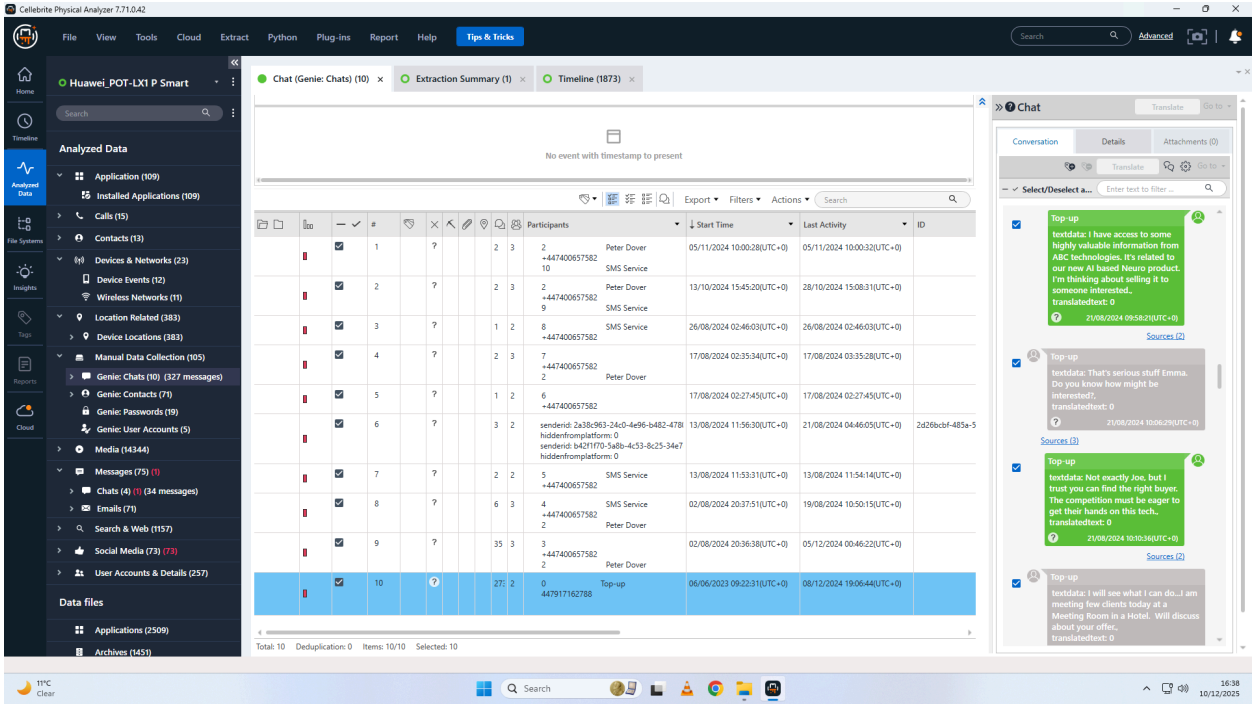

Cellebrite Physical Analyzer 7.71.0.42
File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks
Advanced
Huawei_POT-LX1 P Smart
Analyzed Data
Chat (Genie: Chats) (10)
Extraction Summary (1)
Timeline (1873)
No event with timestamp to present
Export
Filters
Actions
Participants
Start Time
Last Activity
ID
Chat
Translate
Conversation
Details
Attachments (0)
Select/Deselect a...
Enter text to filter ...
Top-up
textdata: Any updates? Need to move fast, translatedtext: 0
Sources (2)
textdata: Met the guy again. He's still playing slow, wants better numbers. translatedtext: 0
Sources (3)
textdata: Waste of time? Should I reach others?, translatedtext: 0
Sources (2)
Sources (1)
Sources (2)
Total: 10 Deduplication: 0 Items: 10/10 Selected: 10
11°C Clear
Search
16:36 10/12/2025

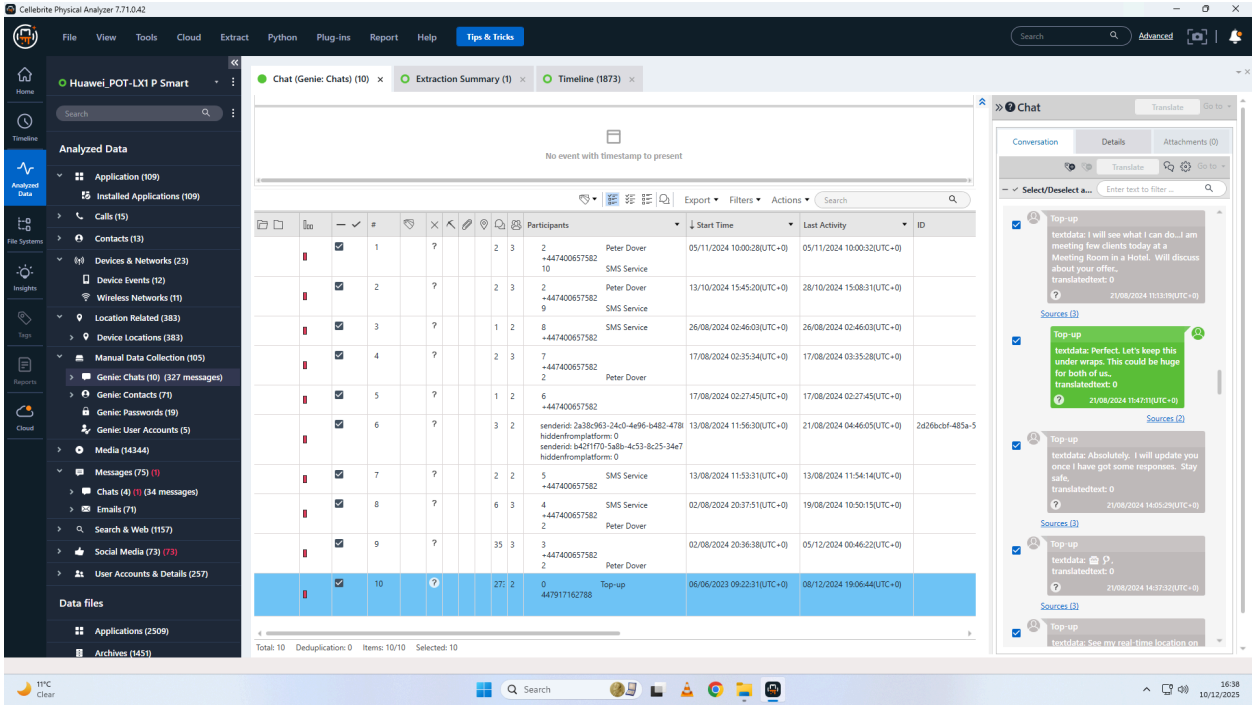

Cellebrite Physical Analyzer 7.71.0.42
File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks
Advanced
Huawei_POT-LX1 P Smart
Analyzed Data
Application (109)
Installed Applications (109)
Calls (15)
Contacts (13)
Devices & Networks (23)
Device Events (12)
Wireless Networks (11)
Location Related (383)
Device Locations (383)
Manual Data Collection (105)
Genie: Chats (10) (327 messages)
Genie: Contacts (71)
Genie: Passwords (19)
Genie: User Accounts (5)
Media (14344)
Messages (75) (1)
Chats (4) (1) (34 messages)
Emails (71)
Search & Web (1157)
Social Media (73) (73)
User Accounts & Details (257)
Data files
Applications (2509)
Archives (1451)
Chat (Genie: Chats) (10)
Extraction Summary (1)
Timeline (1873)
No event with timestamp to present
Export Filters Actions
Participants
Start Time
Last Activity
ID
Total: 10 Deduplication: 0 Items: 10/10 Selected: 10
Chat
Conversation
Details
Attachments (0)
Top-up
Sources (1)
Sources (2)
Sources (3)
Sources (2)
Sources (3)
11°C Clear
16:36 10/12/2025

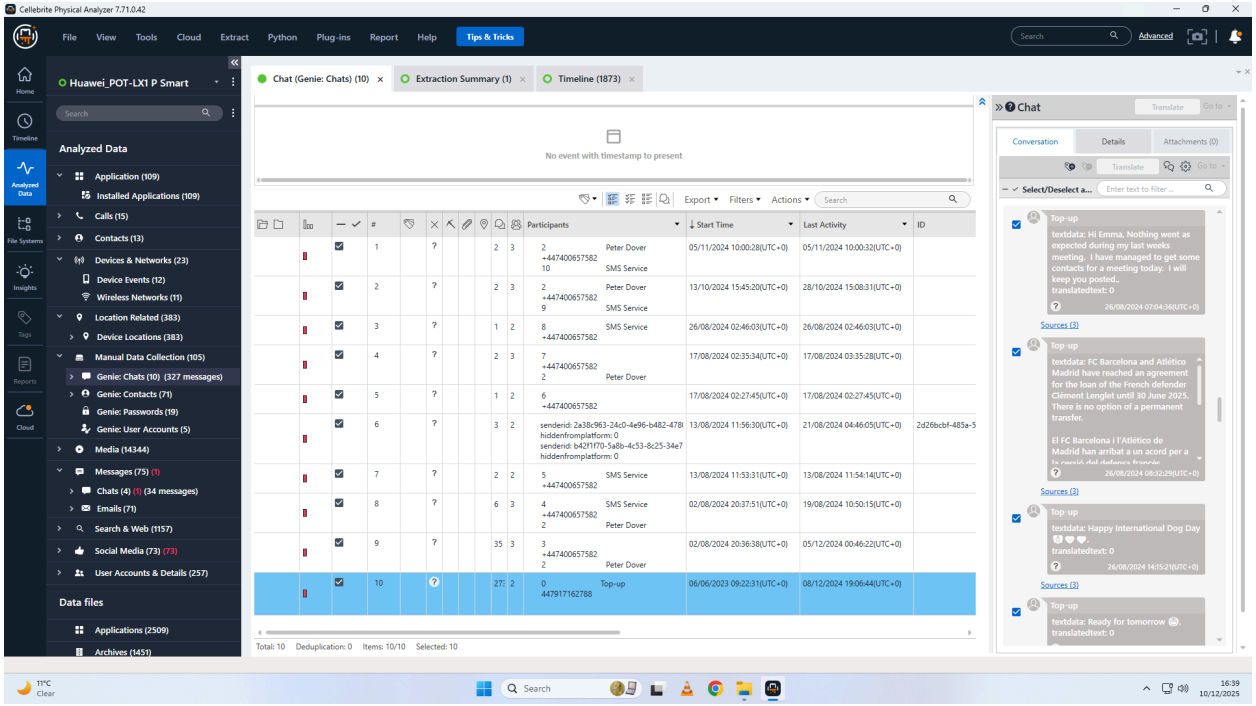

Cellebrite Physical Analyzer 7.71.0.42
File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks
Advanced
Huawei_POT-LX1 P Smart
Analyzed Data
Chat (Genie: Chats) (10)
Extraction Summary (1)
Timeline (1873)
No event with timestamp to present
Export Filters Actions
Participants
Start Time
Last Activity
ID
Total: 10 Deduplication: 0 Items: 10/10 Selected: 10
Chat
Conversation
Details
Attachments (0)
Top-up
Sources (2)
Sources (3)
Sources (2)
Sources (3)
Unknown
Sources (1)
11°C Clear
16:36 10/12/2025

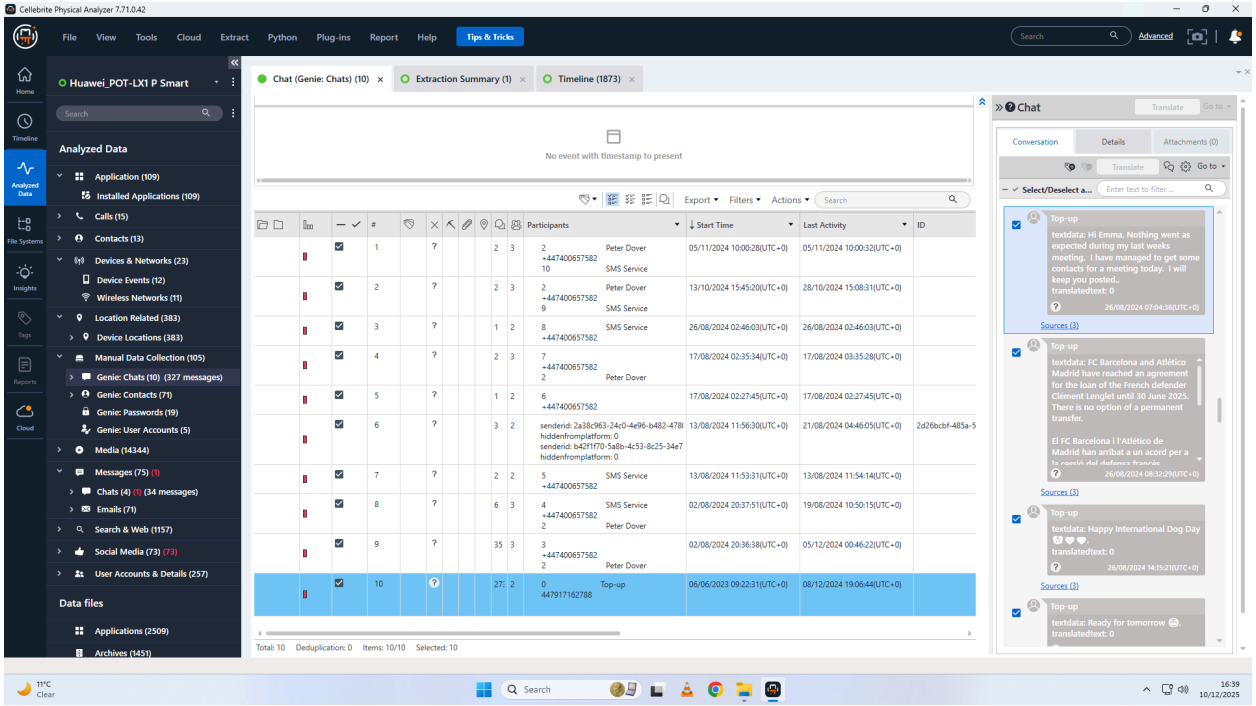

Cellebrite Physical Analyzer 7.71.0.42
File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks
Advanced
Huawei_POT-LX1 P Smart
Analyzed Data
Application (109)
Installed Applications (109)
Calls (15)
Contacts (13)
Devices & Networks (23)
Device Events (12)
Wireless Networks (11)
Location Related (383)
Device Locations (383)
Manual Data Collection (105)
Genie: Chats (10) (327 messages)
Genie: Contacts (71)
Genie: Passwords (19)
Genie: User Accounts (5)
Media (14344)
Messages (75) (1)
Chats (4) (1) (34 messages)
Emails (71)
Search & Web (1157)
Social Media (73) (73)
User Accounts & Details (257)
Data files
Applications (2509)
Archives (1451)
Chat (Genie: Chats) (10)
Extraction Summary (1)
Timeline (1873)
No event with timestamp to present
Export Filters Actions
Participants
Start Time
Last Activity
ID
Total: 10 Deduplication: 0 Items: 10/10 Selected: 10
Chat
Conversation
Details
Attachments (0)
Top-up
textdata: Hello,
translatedtext: 0
Sources (2)
Top-up
textdata: Nice,
translatedtext: 0
Sources (3)
Top-up
textdata: Testing,
translatedtext: 0
Sources (3)
Top-up
textdata: true,
translatedtext: 0
Sources (2)
Top-up
0
Sources (2)
Top-up
textdata: true,
11°C
Clear
16:38
10/12/2025

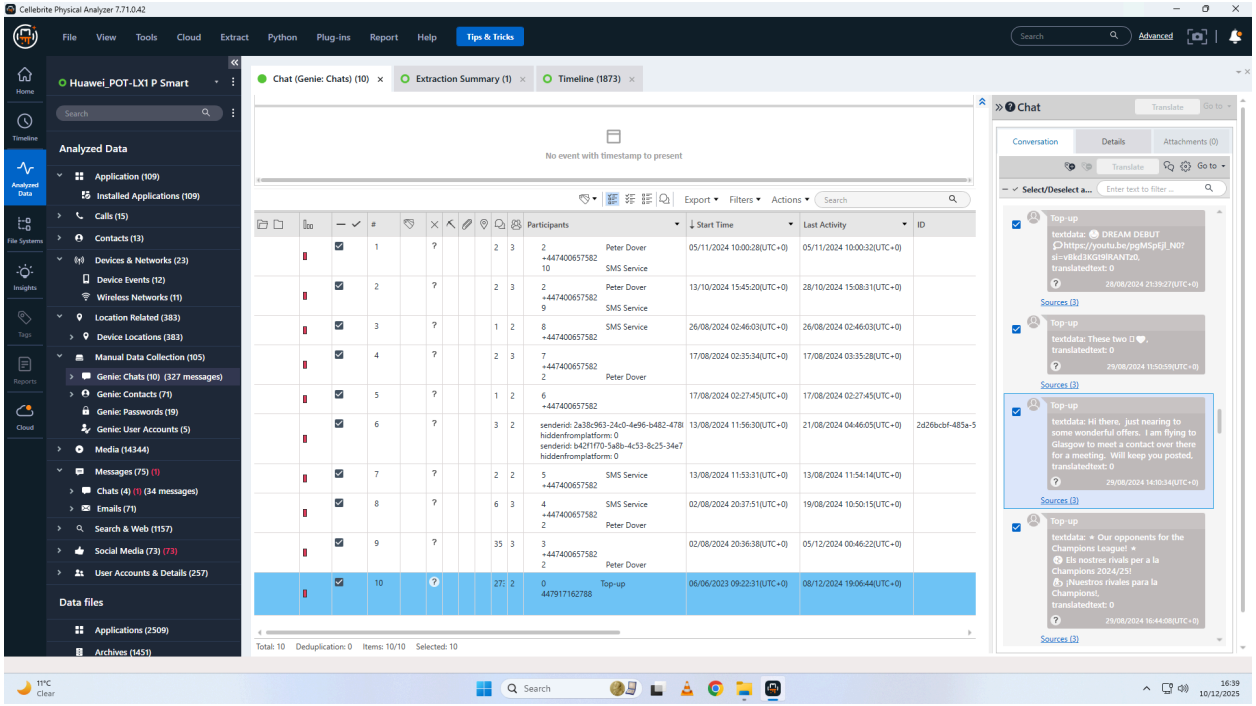

Cellebrite Physical Analyzer 7.71.0.42
File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks
Advanced
Huawei_POT-LX1 P Smart
Analyzed Data
Application (109)
Installed Applications (109)
Calls (15)
Contacts (13)
Devices & Networks (23)
Device Events (12)
Wireless Networks (11)
Location Related (383)
Device Locations (383)
Manual Data Collection (105)
Genie: Chats (10) (327 messages)
Genie: Contacts (71)
Genie: Passwords (19)
Genie: User Accounts (5)
Media (14344)
Messages (75) (1)
Chats (4) (1) (34 messages)
Emails (71)
Search & Web (1157)
Social Media (73) (73)
User Accounts & Details (257)
Data files
Applications (2509)
Archives (1451)
Chat (Genie: Chats) (10)
Extraction Summary (1)
Timeline (1873)
No event with timestamp to present
Export Filters Actions
Participants
Start Time
Last Activity
ID
Total: 10 Deduplication: 0 Items: 10/10 Selected: 10
Chat
Conversation
Details
Attachments (0)
Top-up
textdata: Hey Joe
Hope you are well
Please let me know when you are available for a chat,
translatedtext: 0
Sources (2)
Top-up
textdata: Hey Joe
I need your help with something sensitive.
Do you have time to talk?,
translatedtext: 0
Sources (2)
Top-up
textdata: Yes I am available. What's going on?,
translatedtext: 0
Sources (3)
Top-up
textdata: I have access to some highly valuable information from ABC technologies. It's related to our new AI based Neuro product. I'm thinking about selling it to someone interested.,
translatedtext: 0
11°C
Clear
16:38
10/12/2025

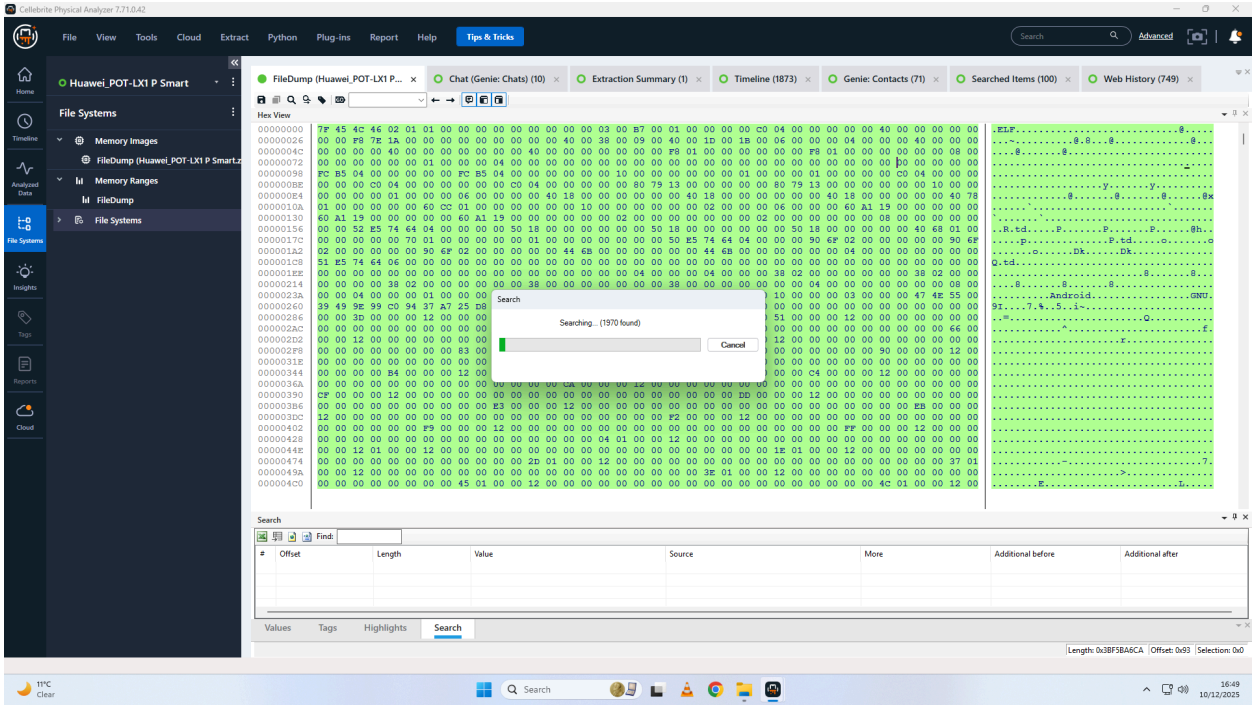

Cellebrite Physical Analyzer 7.71.0.42
File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks
Huawei_POT-LX1 P Smart
Analyzed Data
Application (109)
Installed Applications (109)
Calls (15)
Contacts (13)
Devices & Networks (23)
Device Events (12)
Wireless Networks (11)
Location Related (383)
Device Locations (383)
Manual Data Collection (105)
Genie: Chats (10) (327 messages)
Genie: Contacts (71)
Genie: Passwords (19)
Genie: User Accounts (5)
Media (14344)
Messages (75) (1)
Chats (4) (1) (34 messages)
Emails (71)
Search & Web (1157)
Social Media (73) (73)
User Accounts & Details (257)
Data files
Applications (2509)
Archives (1451)
Chat (Genie: Chats) (10)
Extraction Summary (1)
Timeline (1873)
No event with timestamp to present
Export Filters Actions
Participants
Start Time
Last Activity
ID
Total: 10 Deduplication: 0 Items: 10/10 Selected: 10
Chat
Conversation
Details
Attachments (0)
Top-up
Sources (2)
Sources (3)
11°C Clear
16:38 10/12/2025


Cellebrite Physical Analyzer 7.71.0.42
File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks
Huawei_POT-LX1 P Smart
Analyzed Data
Chat (Genie: Chats) (10)
Extraction Summary (1)
Timeline (1873)
No event with timestamp to present
Export Filters Actions
Participants
Start Time
Last Activity
ID
Total: 10 Deduplication: 0 Items: 10/10 Selected: 10
Chat
Conversation
Details
Attachments (0)
Top-up
Sources (2)
Sources (3)
11°C Clear
16:38 10/12/2025


Cellebrite Physical Analyzer 7.71.0.42
File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks
Huawei_POT-LX1 P Smart
Analyzed Data
Application (109)
Installed Applications (109)
Calls (15)
Contacts (13)
Devices & Networks (23)
Device Events (12)
Wireless Networks (11)
Location Related (383)
Device Locations (383)
Manual Data Collection (105)
Genie: Chats (10) (327 messages)
Genie: Contacts (71)
Genie: Passwords (19)
Genie: User Accounts (5)
Media (14344)
Messages (75) (1)
Chats (4) (1) (34 messages)
Emails (71)
Search & Web (1157)
Social Media (73) (73)
User Accounts & Details (257)
Data files
Applications (2509)
Archives (1451)
Chat (Genie: Chats) (10)
Extraction Summary (1)
Timeline (1873)
No event with timestamp to present
Export Filters Actions
Participants
Start Time
Last Activity
ID
Total: 10 Deduplication: 0 Items: 10/10 Selected: 10
Chat
Conversation
Details
Attachments (0)
Top-up
Sources (3)
11°C Clear
16:39 10/12/2025


Cellebrite Physical Analyzer 7.71.0.42
File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks
Huawei_POT-LX1 P Smart
Analyzed Data
Application (109)
Installed Applications (109)
Calls (15)
Contacts (13)
Devices & Networks (23)
Device Events (12)
Wireless Networks (11)
Location Related (383)
Device Locations (383)
Manual Data Collection (105)
Genie: Chats (10) (327 messages)
Genie: Contacts (71)
Genie: Passwords (19)
Genie: User Accounts (5)
Media (14344)
Messages (75) (1)
Chats (4) (1) (34 messages)
Emails (71)
Search & Web (1157)
Social Media (73) (73)
User Accounts & Details (257)
Data files
Applications (2509)
Archives (1451)
Chat (Genie: Chats) (10)
Extraction Summary (1)
Timeline (1873)
No event with timestamp to present
Export Filters Actions
Participants
Start Time
Last Activity
ID
Total: 10 Deduplication: 0 Items: 10/10 Selected: 10
Chat
Conversation
Details
Attachments (0)
Top-up
Sources (3)
11°C Clear
16:39 10/12/2025





Analysis

The device's application ecosystem makes it visible a highly active and digitalized user profile. Among the 24 cloud data sources identified, the user had a strong presence on social networking platforms such as Snapchat and Youtube, in addition to important productivity and

communication tools such as Gmail and Google Meet. Crucially, the presence of travel-focused applications also (i.e. Booking.com) suggest a user engaged in active logistical planning. This digital footprint is in line with the wider investigation which found a co-ordinated and mobile operation with travel to different destinations for illicit meetings.

On August 19, 2024, the logs showed several calls being made from the subject to an Indian mobile number (+917907025586). Forensic significance of disposition of these calls as "Not answered" It signifies a persistent, but unilateral, effort by the device owner, which is identified as Emma, to make the connection with an offshore node -- possibly the "Norman" feature identified in other parts of the investigation. This activity proposes a first, possibly unsuccessful, attempt at coordinating with external support then transferring attention to local intermediaries. The basic evidence of criminal conspiracy comes from a parsed chat thread titled "Top-up," which contains a continuation and incriminating conversation between Emma and a contact clearly referred to as "Joe." On August 21, 2024, the topic moves away from general pleasantries and gets right to the point, a solicitation of corporate espionage. With respect to this claim, Emma clearly states possessing "highly valuable information from ABC technologies" in relation to a "new AI-based Neuro product."

This admission becomes a nexus of the investigation, proving three key elements: what exactly the stolen intellectual property is, who took it (in this case Emma), and that the clear intention is to mint money from these trade secrets through illegal sales. The communications clearly prove mens rea (criminal intent) and a mutual understanding about the illegality of the operation.

Joe's yes at 14:05:29 (UTC+0)--"Absolutely -- well you may not use the word "lord" in his yes, but in some sense; Stay safe"--shows his willingness and acceptance of operational security measures This thread helps prove that both parties were well aware of the unauthorized nature of their activities, making an express agreement to try to cover their activities while anticipating substantial financial gain. The chat logs describe the operational tradecraft used to sell the stolen data with Joe's role clearly defined as the external facilitator or broker. In response to Emma's need for urgency, Joe confirms that he is actively observing by stating that, "I am meeting few clients today at a Meeting Room in a Hotel." This message is a crucial investigative turn point in that it turns the conspiracy from a digital negotiation to a reality. It secures Joe in a particular, physical location, to try and sell the stolen IP.

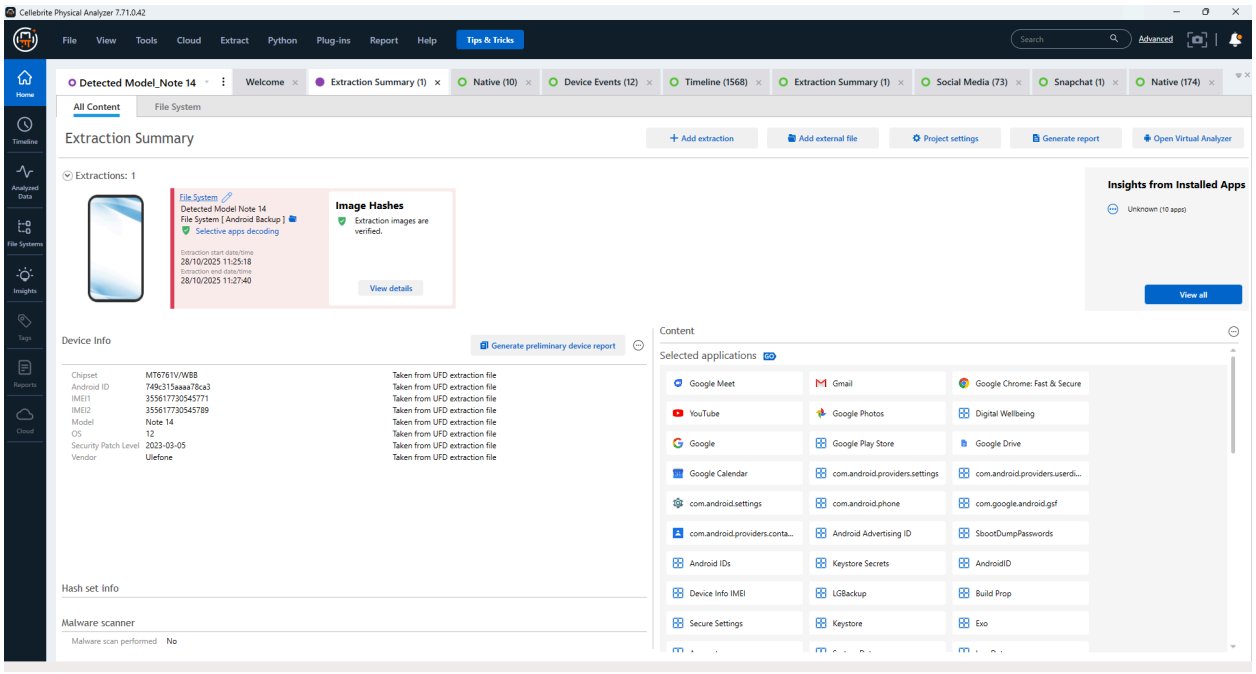
Despite early failures reported on August 26, 2024 ("Nothing went as expected"), Joe shows persistence and proves he had acquired new contacts in proving the iterative and ongoing nature of the criminal enterprise. The digital communications are irrefutable corroboration of physical evidence recovered elsewhere. On August 29, 2024, Joe tells Emma, "I am flying to Glasgow to meet someone . . . for a meeting," a statement which is directly consistent with physical artifacts that belong to Joe's flight (tickets and receipts) on his own device. This message does confirm his location and explicitly correlates his travel with the negotiation of "offers" for the stolen data.

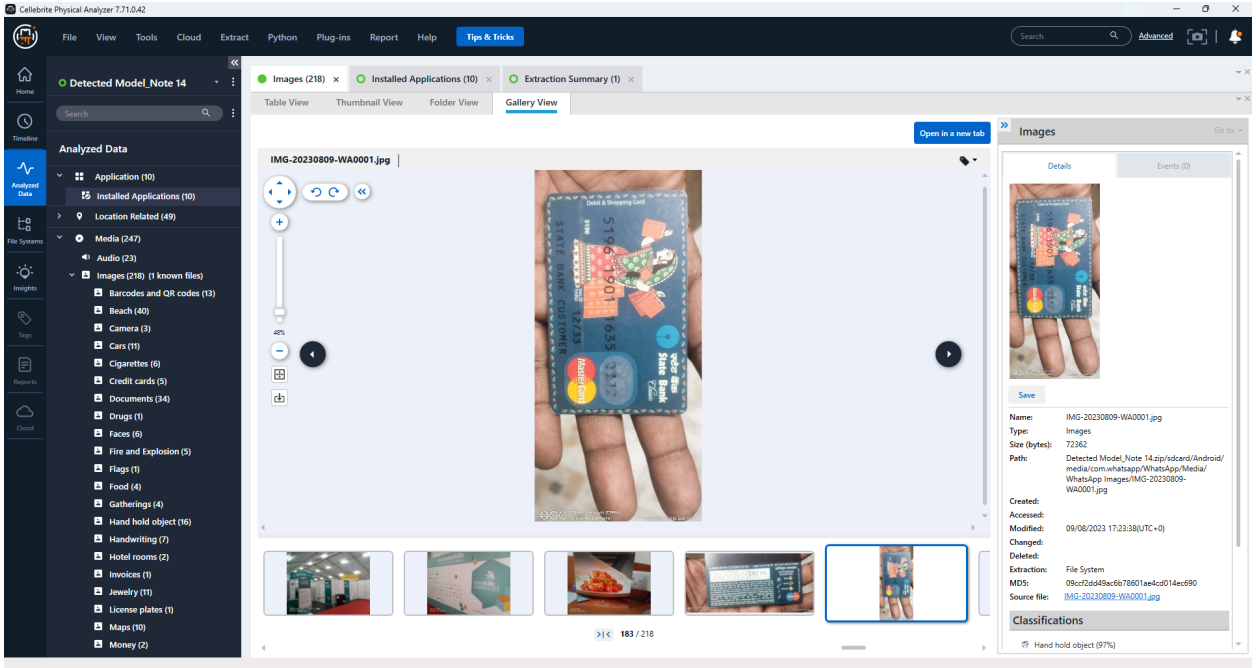
Furthermore in a later exchange on October 14, 2024, Joe's expansion into international markets is shown, when he mentions that he traveled to Paris to "get some good deals." This has established the fact that the conspiracy was not confined to the UK but involved active seeking out of buyers from major European commercial centres. Finally, the investigation indicates a tense exchange between Emma and on November 20, 2024, Emma threatens to "go with someone else" because of a lack of progress.

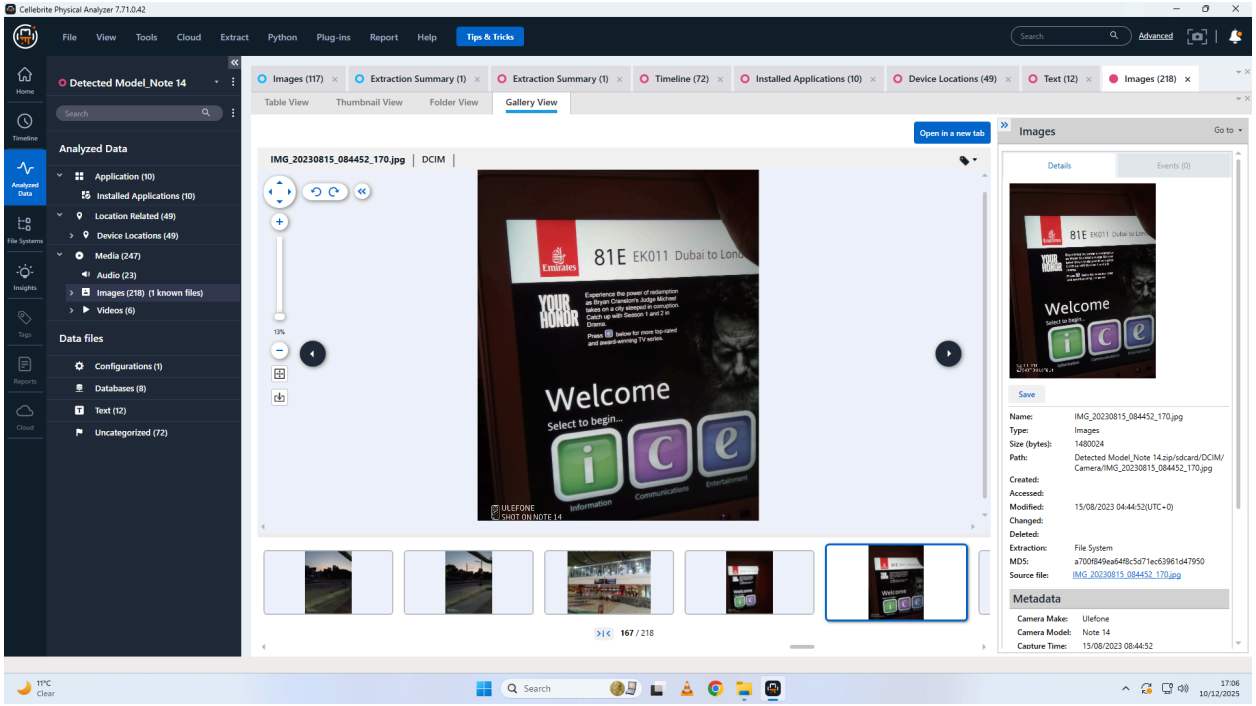
Joe's immediate response - "Apologies Emma." I am in a final talks about it. Meeting the client this week [at Manchester]"--is monumental. It places his criminal business ventures geographically in Manchester and reiterates his purpose as active intermediary negotiating the final sale of the defrauded "Neuro" product intellectual property. The location history of the device allows for a comprehensive, data-driven picture of movements by the user. A total of 419 extracted geospatial points were placed to reconstruct a comprehensible tri-Regional operational footprint. The data clusters show great activity in the United Kingdom (26 points), which was used as primary location to host the negotiations; Dubai/UAE (24 points), possibly a transit point or location for intermediate meetings; a substantial amount of activity is also seen in India (349 points). This geospatial distribution strengthens the theory of a transnational network investigated in the research - establishing a physical link between the main perpetrators in the UK and UAE and the support infrastructure identified in India.

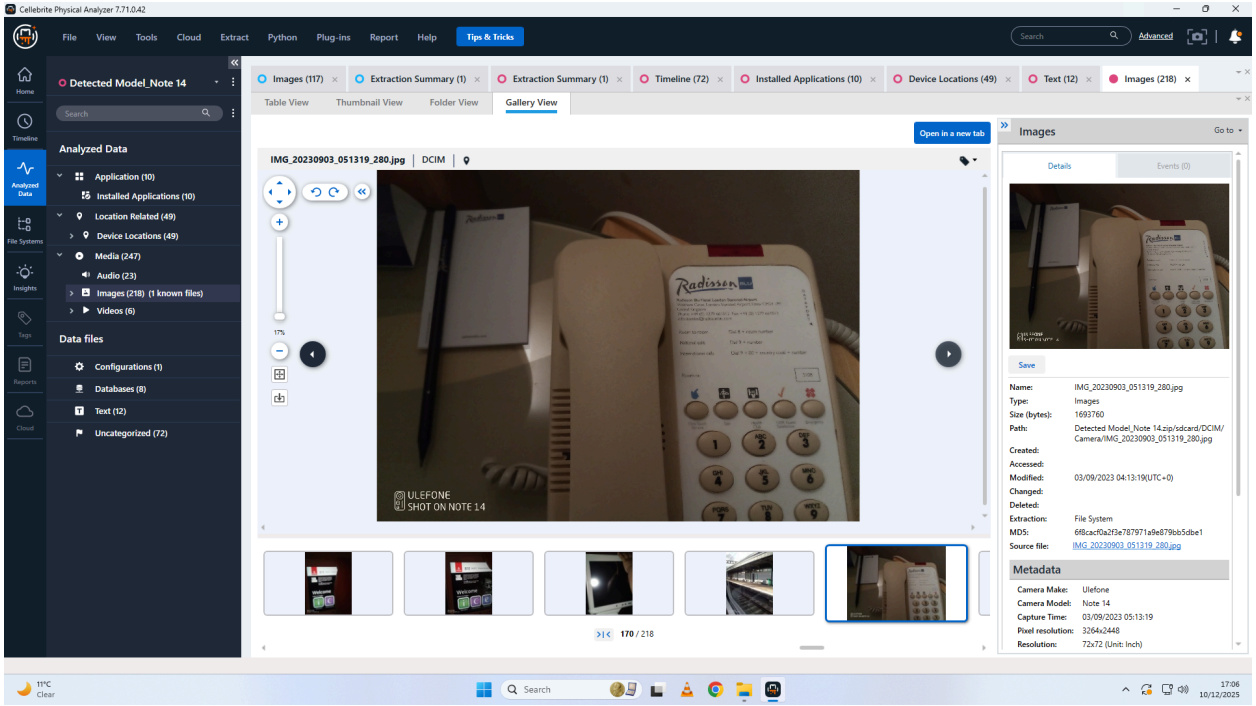
The Ulefone Device: Network Node and Conspiracy Archive

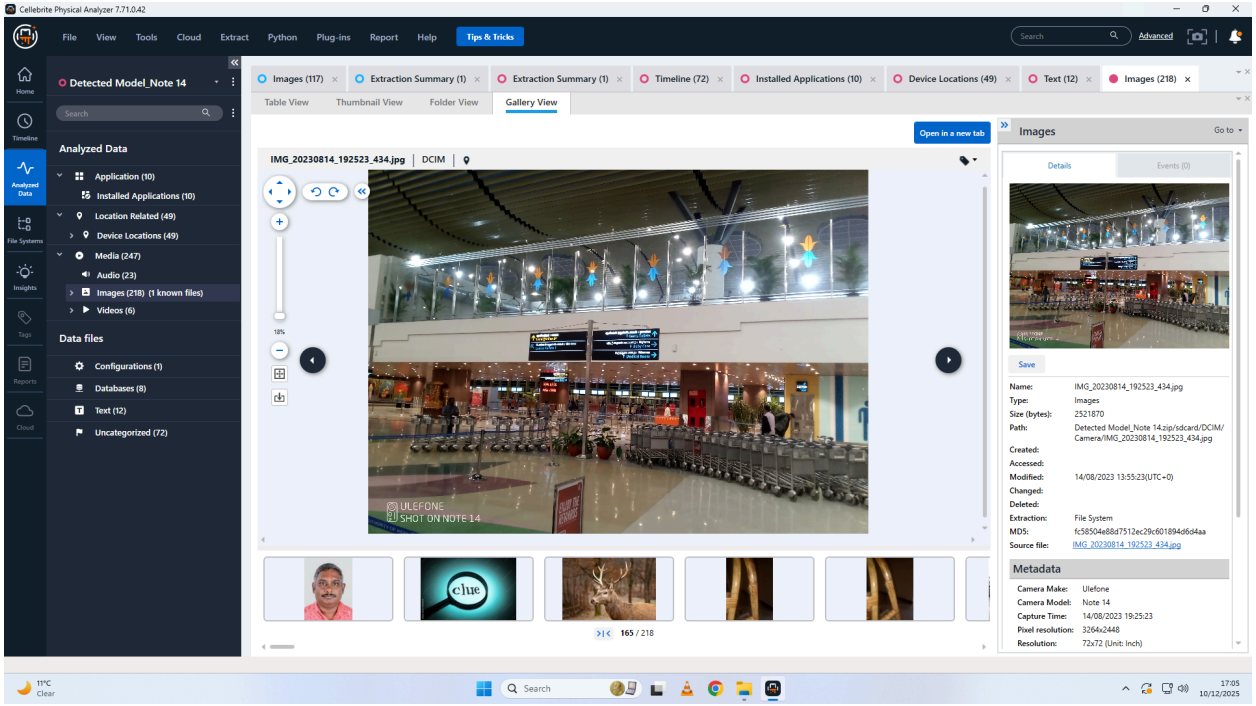
Artifacts

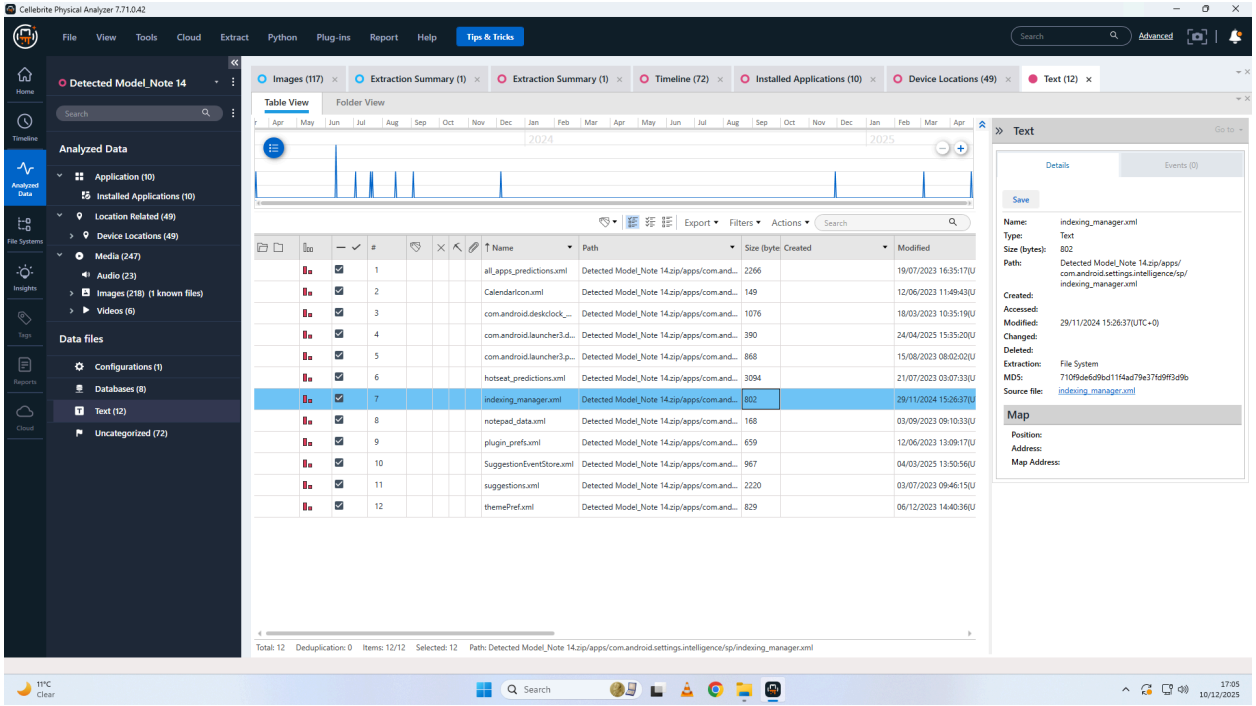





Cellebrite Physical Analyzer 7.71.0.42
Detected Model_Note 14
Analyzed Data
Application (10)
Installed Applications (10)
Location Related (49)
Device Locations (49)
Media (247)
Audio (23)
Images (218) (1 known files)
Videos (6)
Data files
Configurations (1)
Databases (8)
Text (12)
Uncategorized (72)
Images (117)
Extraction Summary (1)
Extraction Summary (1)
Timeline (72)
Installed Applications (10)
Device Locations (49)
Text (12)
Images (218)
Table View
Thumbnail View
Folder View
Gallery View
IMG_20230815_084452_170.jpg | DCIM
Open in a new tab
Images
Details
Events (0)
Save
Name: IMG_20230815_084452_170.jpg
Type: Images
Size (bytes): 1480024
Path: Detected Model_Note 14.zip/sdcard/DCIM/Camera/IMG_20230815_084452_170.jpg
Created:
Accessed:
Modified: 15/08/2023 04:44:52(UTC+0)
Changed:
Deleted:
Extraction: File System
MD5: a700f849ea648c5d71ec63961d47950
Source file: IMG_20230815_084452_170.jpg
Metadata
Camera Make: Ulefone
Camera Model: Note 14
Capture Time: 15/08/2023 08:44:52
167 / 218


Cellebrite Physical Analyzer 7.71.0.42
Detected Model_Note 14
Analyzed Data
Application (10)
Installed Applications (10)
Location Related (49)
Device Locations (49)
Media (247)
Audio (23)
Images (218) (1 known files)
Videos (6)
Data files
Configurations (1)
Databases (8)
Text (12)
Uncategorized (72)
Images (117)
Extraction Summary (1)
Extraction Summary (1)
Timeline (72)
Installed Applications (10)
Device Locations (49)
Text (12)
Images (218)
Table View
Thumbnail View
Folder View
Gallery View
IMG_20230903_051319_280.jpg | DCIM
Open in a new tab
Images
Details
Events (0)
Save
Name: IMG_20230903_051319_280.jpg
Type: Images
Size (bytes): 1693760
Path: Detected Model_Note 14.zip/sdcard/DCIM/Camera/IMG_20230903_051319_280.jpg
Created:
Accessed:
Modified: 03/09/2023 04:13:19(UTC+0)
Changed:
Deleted:
Extraction: File System
MD5: 6f8cacf0a2f3e787971a9e879bb5dbe1
Source file: IMG_20230903_051319_280.jpg
Metadata
Camera Make: Ulefone
Camera Model: Note 14
Capture Time: 03/09/2023 05:13:19
Pixel resolution: 3264x2448
Resolution: 72x72 (Unit: Inch)
170 / 218





Analysis

The Ulefone Note 14 is a crucial third node in the overall conspiracy structure as part of an individual who seems to be working on the periphery than at the centre of the espionage activities that flared up during August 2024. While this subject was not involved directly in the

primary communication exchanges recorded during that critical month, sounds forensic evidence clearly show their historical activities coming into contact with the operational network to be investigated. The device produced a lot of forensic data consisting of 72 discrete timeline events, 218 photographic files and 49 specific geolocation information, which all together paint a picture of sustained use over a period of time. A closer examination of the file system architecture of the device led to interesting findings of this being one of the user accounts linked by metadata structures and data repositories archived from Emma and Joe.

The geospatial analysis based on the location data of the device shows an unequivocal view of the user's territory of operation, the coordinates of which are 49 were recorded all exclusively within the geographical boundaries of India. This pattern indicates that the owner of the device had no international travel or international movements of any kind during the monitored period, thus effectively proclaiming India as the only operational area. This geographic attribution is also well supported with one important artifact of evidence recovered from the image gallery of the device: a photograph of an Indian-issued debit card carrying the Maestro branding and with a partially visible account number.

This exact interval of one year between the Indian debit card evidence and active UK-based conspiracy communications opens two reasonable investigative possibilities: either that the Ulefone device was used as an archived back-up system from an earlier stage of the conspiracy's operations, or that it was that of an international facilitator, who organized the logistics and support for Emma's UK-based activities from his remote point of residence in India, thus spreading the conspiracy's geographical reach across international boundaries.

Technical and Forensic Profile of the Samsung Galaxy A13

The second device used for this investigation is a Samsung Galaxy A13 found to be a GSM-SM-A137F by forensic tool reports. The forensics profile of this phone is very different from this primary communication device Emma is using. A deep dive into the user data partition showed a curious lack of any of the configured email clients, cloud service accounts or persistent synchronization tokens. The attribution of this device to the intermediary "Joe" is based on the convergence of evidence. With the devices in the network accounted for, this Samsung A13 is the last node and its movement patterns perfectly align with the actions described by and expected of this contact "Joe" in the chat logs from Emma's phone. The data that was retrieved from the Samsung A13 gives a clear picture of what the device is designed to do.

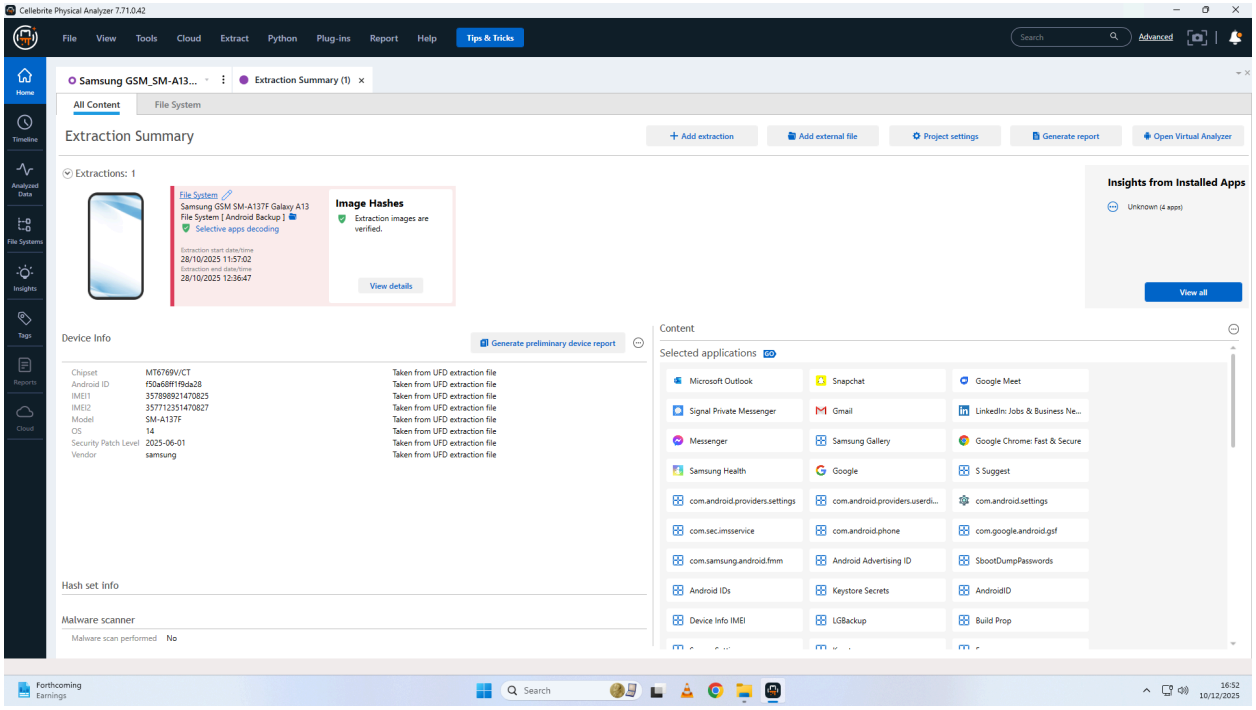
In stark contrast to this, the storage was enriched with a heavy volume of logistical and visual data where there were 1,190 images and 281 unique geospatial coordinates sets. This large difference suggests that the use case of the user was not to have lengthy textual interactions but to navigate, record physical movements, and take pictures. The day's use of the phone is consistent for someone who goes out into the field and becomes an operative or a logistical

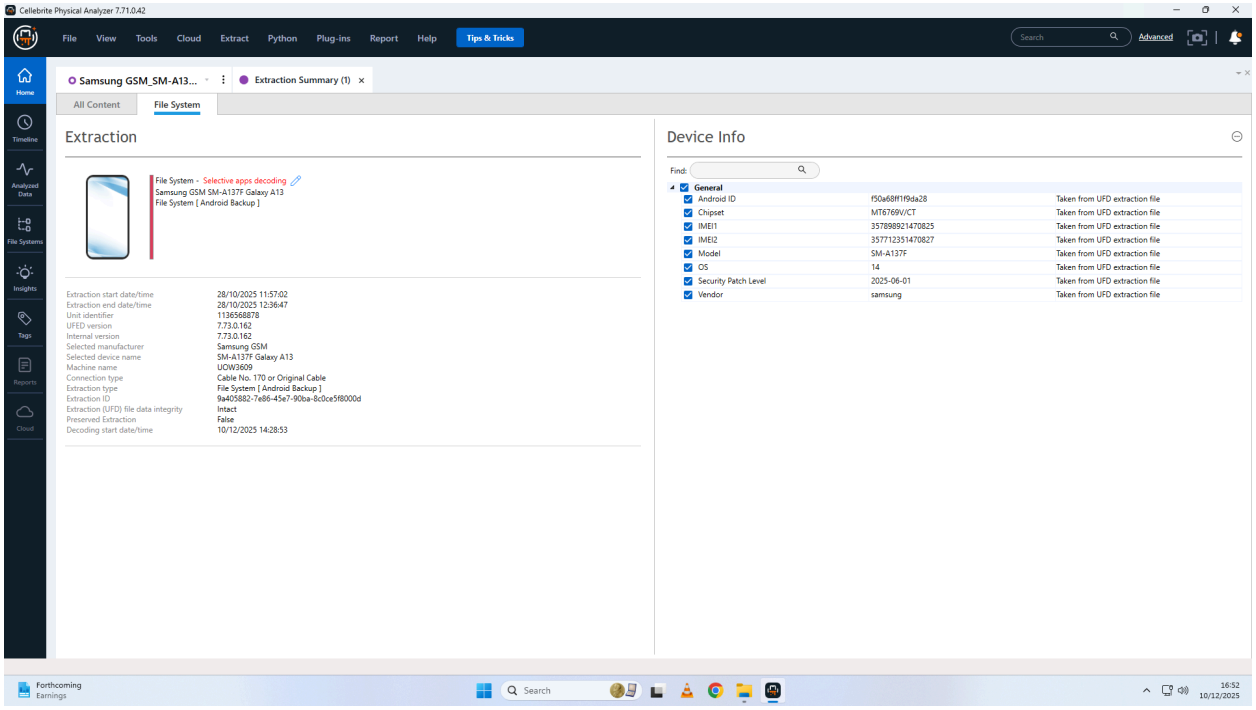
coordinator - someone who is concerned with managing physical transit issues, reconnaissance rather than negotiating the fine points of the conspiracy over digital text. The user's behavior as determined from the data on the device is that of constant movement and logistic planning. The huge collection of pictures was not for personal use but as a sort of documentation. Recovered artifacts include photographs of railway tickets, public transport timetables and location identifying signage. Specific examples include a good image of a "Fox and Goose" bus stop sign and a digital photograph of a train ticket to travel between Blairhill and Glasgow Central/Queen St.

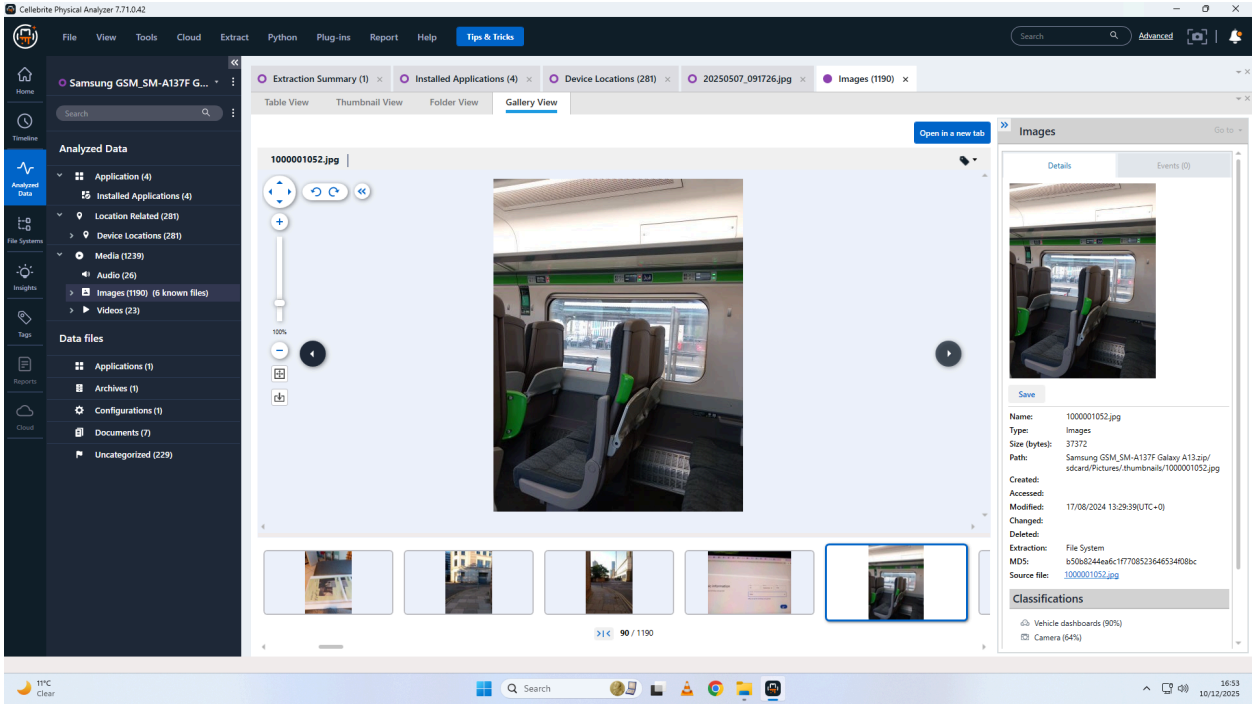
The strongest case for this device being involved in the conspiracy is the spatiotemporal analysis of correlating how the movements of this device correspond to that of Emma's device. The 281 retrieved GPS Coordinates for the Samsung A13 are clustered in the area of operation of the United Kingdom alone, proving the validity of the area the user has been operating in. Crucially, from the critical operational time frame of August 2024, the location data reveals multiple occurrences where Samsung A13 and Emma's Huawei device were geolocated in the same immediate vicinity location of the Greater London area. These times of close proximity of physical proximity have a direct correlation to noticeable voids in their SMS communications. This pattern, of physical proximity substituting for digital connectivity, is a very strong forensic indicator of in-person meetings. It supports the theory that Joe and Emma met face-to-face to workout intimate details, like the "local part" and "offshore arrangement" that they felt were too compromising to put on paper. Several important images with concrete evidence of the user's travel and activities are provided. A train ticket with a date of 31-AUG-24 places the user's travel into Glasgow squarely in the active date of the conspiracy. Another image puts the user in Luton Airport, another key transit hub. Furthermore, the recovery of a photograph of an ibis hotel key card filler, with the slogan of the chain "YOU GOT THE KEY", seems to indicate a temporary housing, in accordance with a transient operational lifestyle.

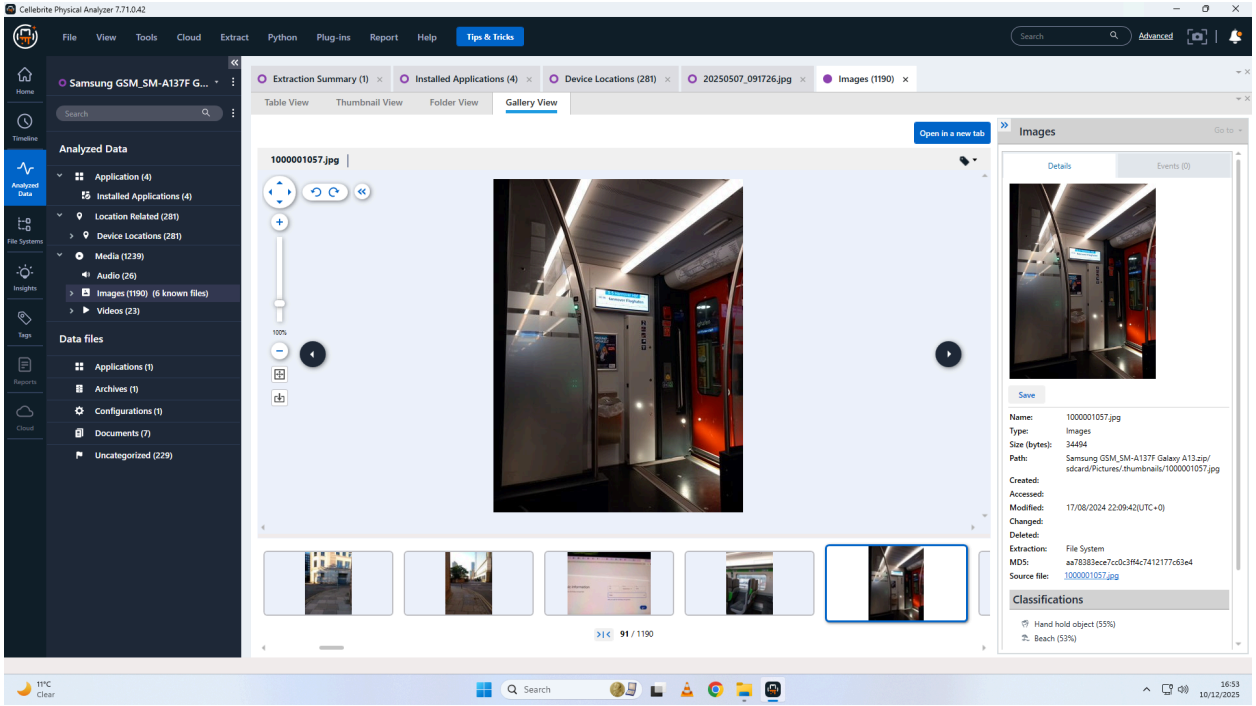
These visual artifacts are not unimportant; rather, they act as physical anchors that support the digital GPS information that demonstrates the user was not merely planning to travel, but actually moving between important locations such as London, Glasgow and Luton for the purposes of creating the conspiracy's goals.

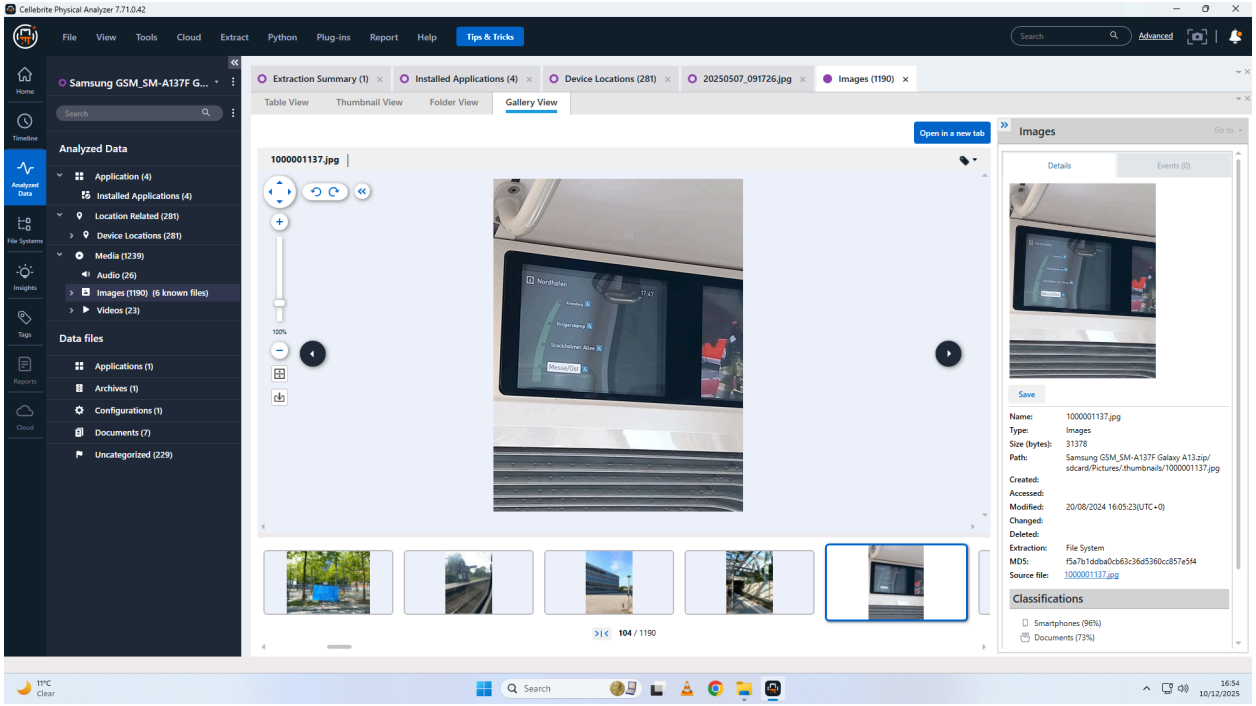
Artifacts captured form samsung

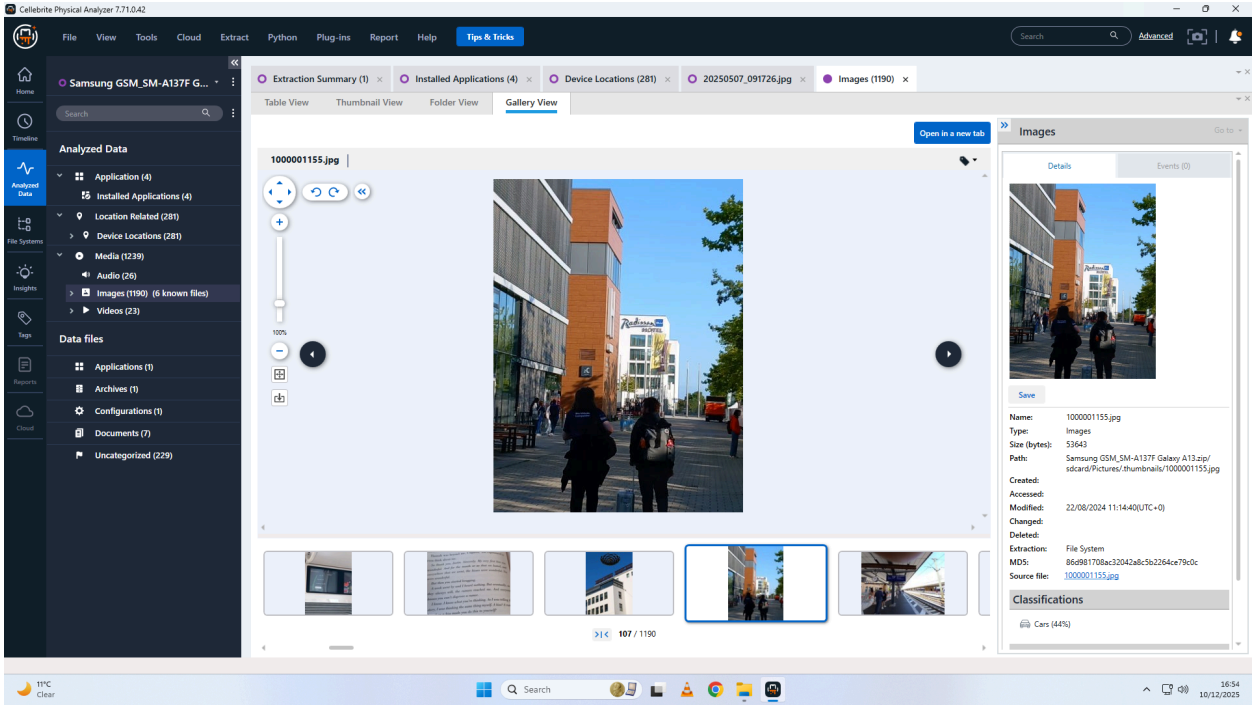


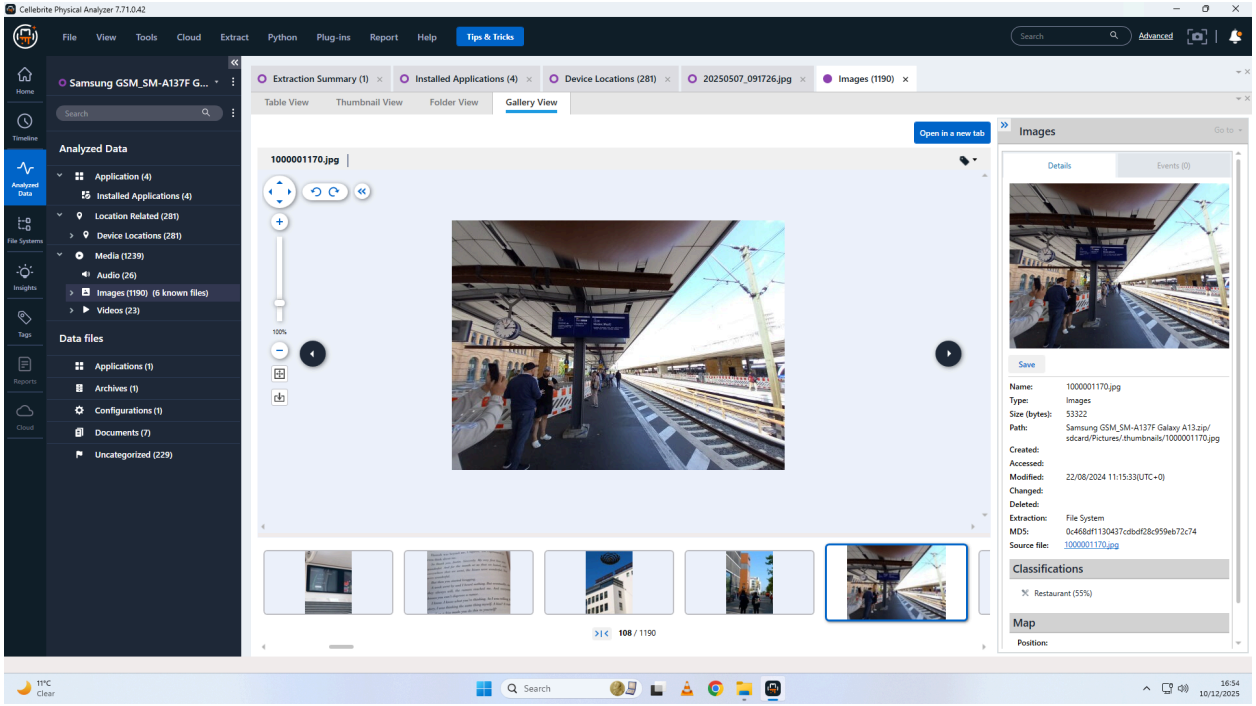


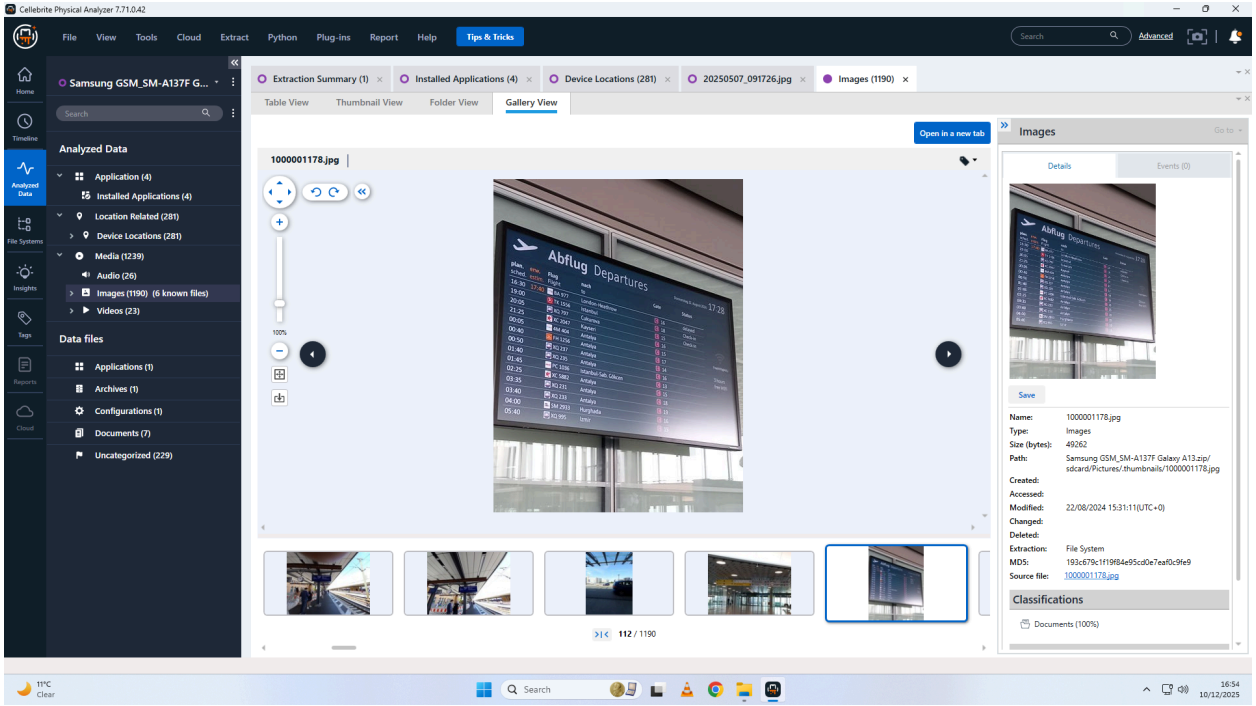

Cellebrite Physical Analyzer 7.71.0.42
File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks
Advanced
Samsung GSM_SM-A137F G...
Analyzed Data
Application (4)
Installed Applications (4)
Location Related (281)
Device Locations (281)
Media (1239)
Audio (26)
Images (1190) (6 known files)
Videos (23)
Data files
Applications (1)
Archives (1)
Configurations (1)
Documents (7)
Uncategorized (229)
Extraction Summary (1)
Installed Applications (4)
Device Locations (281)
20250507_091726.jpg
Images (1190)
Table View
Thumbnail View
Folder View
Gallery View
Open in a new tab
1000001052.jpg
90 / 1190
Images
Details
Events (0)
Save
Name: 1000001052.jpg
Type: Images
Size (bytes): 37372
Path: Samsung GSM_SM-A137F Galaxy A13.zip/ sdcard/Pictures/.thumbnails/1000001052.jpg
Created:
Accessed:
Modified: 17/08/2024 13:29:39(UTC+0)
Changed:
Deleted:
Extraction: File System
MD5: b50b8244ea6c1f770852364653408bc
Source file: 1000001052.jpg
Classifications
Vehicle dashboards (90%)
Camera (64%)

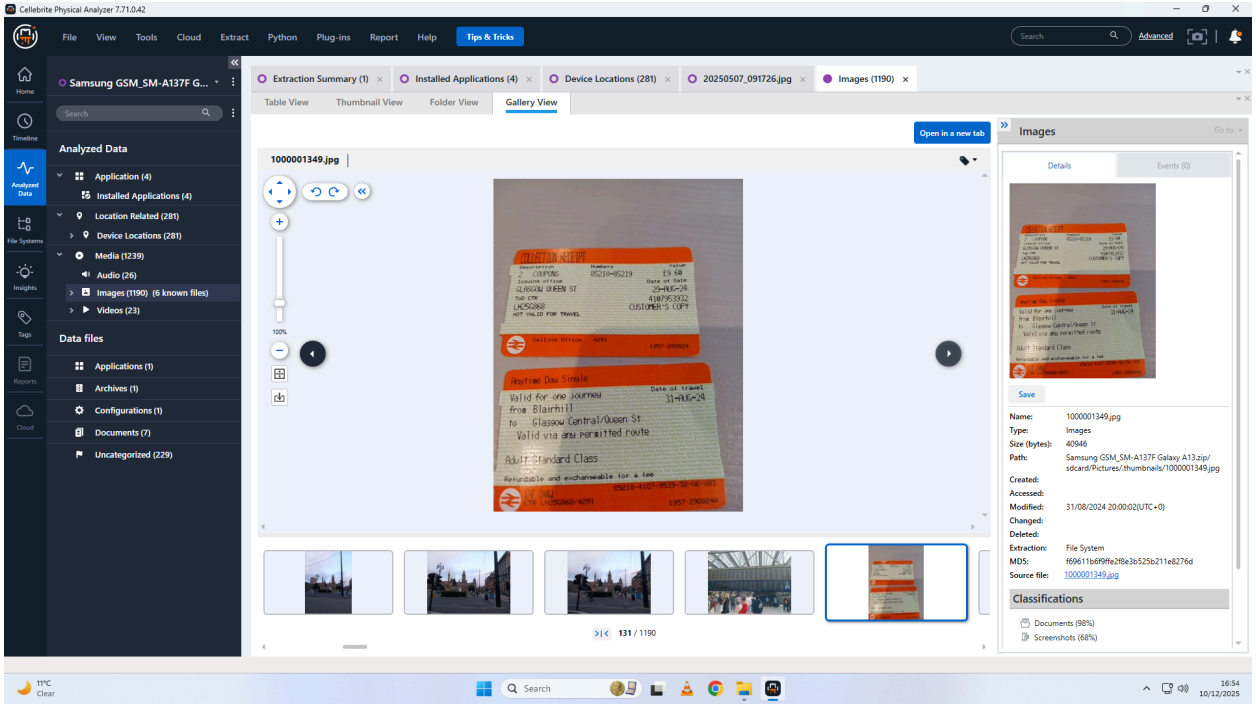

Cellebrite Physical Analyzer 7.71.0.42
File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks
Advanced
Samsung GSM_SM-A137F G...
Analyzed Data
Application (4)
Installed Applications (4)
Location Related (281)
Device Locations (281)
Media (1239)
Audio (26)
Images (1190) (6 known files)
Videos (23)
Data files
Applications (1)
Archives (1)
Configurations (1)
Documents (7)
Uncategorized (229)
Extraction Summary (1)
Installed Applications (4)
Device Locations (281)
20250507_091726.jpg
Images (1190)
Table View
Thumbnail View
Folder View
Gallery View
Open in a new tab
1000001057.jpg
91 / 1190
Images
Details
Events (0)
Save
Name: 1000001057.jpg
Type: Images
Size (bytes): 34494
Path: Samsung GSM_SM-A137F Galaxy A13.zip/ sdcard/Pictures/.thumbnails/1000001057.jpg
Created:
Accessed:
Modified: 17/08/2024 22:09:42(UTC+0)
Changed:
Deleted:
Extraction: File System
MD5: aa78383ece7cc0c3ff4c7412177c63e4
Source file: 1000001057.jpg
Classifications
Hand hold object (55%)
Beach (53%)

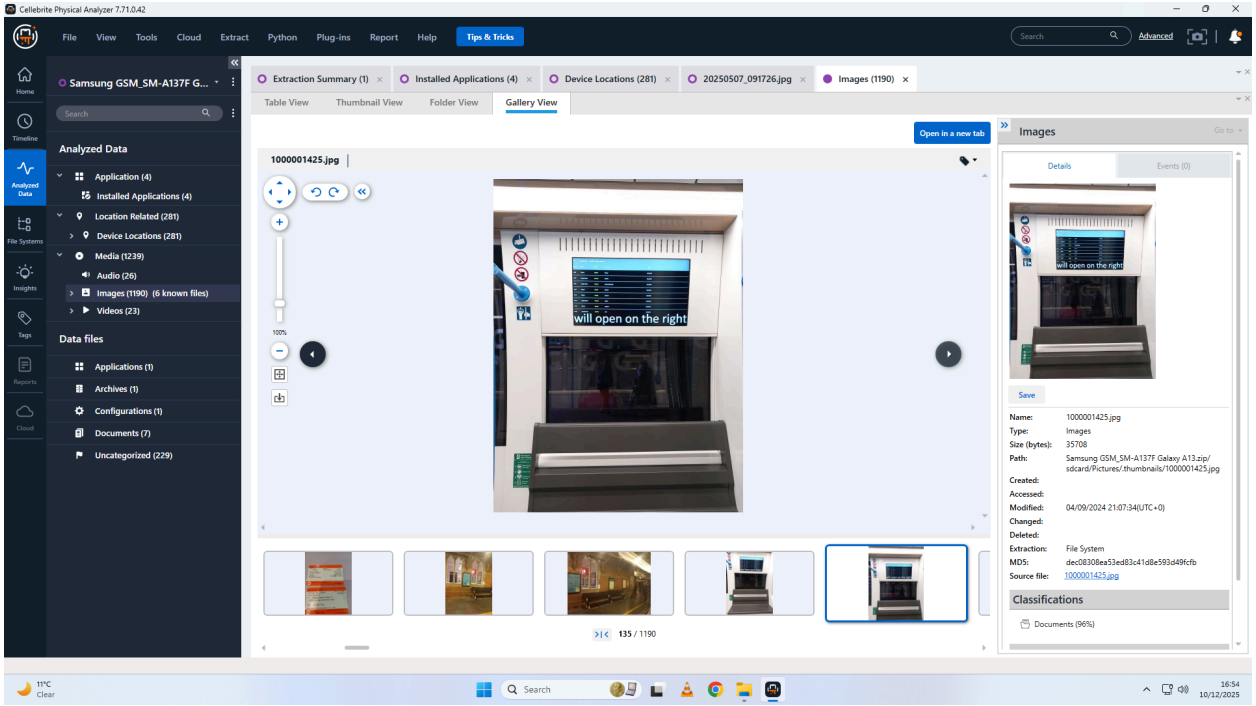

Cellebrite Physical Analyzer 7.71.0.42
File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks
Advanced
Samsung GSM_SM-A137F G...
Analyzed Data
Application (4)
Installed Applications (4)
Location Related (281)
Device Locations (281)
Media (1239)
Audio (26)
Images (1190) (6 known files)
Videos (23)
Data files
Applications (1)
Archives (1)
Configurations (1)
Documents (7)
Uncategorized (229)
Extraction Summary (1)
Installed Applications (4)
Device Locations (281)
20250507_091726.jpg
Images (1190)
Table View
Thumbnail View
Folder View
Gallery View
Open in a new tab
1000001137.jpg
104 / 1190
Images
Details
Events (0)
Save
Name: 1000001137.jpg
Type: Images
Size (bytes): 31378
Path: Samsung GSM_SM-A137F Galaxy A13.zip/ sdcard/Pictures/.thumbnails/1000001137.jpg
Created:
Accessed:
Modified: 20/08/2024 16:05:23(UTC+0)
Changed:
Deleted:
Extraction: File System
MD5: f5a7b1ddba0cb63c36d5360cc857e564
Source file: 1000001137.jpg
Classifications
Smartphones (96%)
Documents (73%)

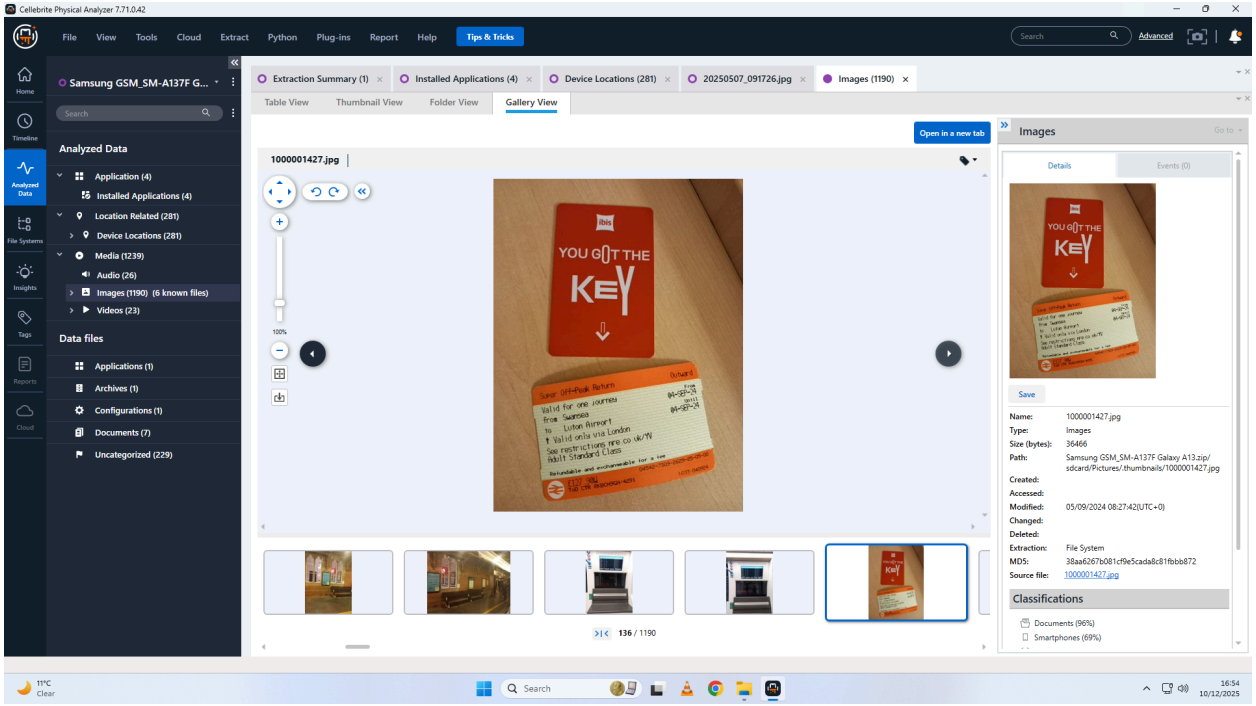

Cellebrite Physical Analyzer 7.71.0.42
File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks
Advanced
Samsung GSM_SM-A137F G...
Analyzed Data
Application (4)
Installed Applications (4)
Location Related (281)
Device Locations (281)
Media (1239)
Audio (26)
Images (1190) (6 known files)
Videos (23)
Data files
Applications (1)
Archives (1)
Configurations (1)
Documents (7)
Uncategorized (229)
Extraction Summary (1)
Installed Applications (4)
Device Locations (281)
20250507_091726.jpg
Images (1190)
Table View
Thumbnail View
Folder View
Gallery View
Open in a new tab
1000001155.jpg
107 / 1190
Images
Details
Events (0)
Save
Name: 1000001155.jpg
Type: Images
Size (bytes): 53643
Path: Samsung GSM_SM-A137F Galaxy A13.zip/ sdcard/Pictures/.thumbnails/1000001155.jpg
Created:
Accessed:
Modified: 22/08/2024 11:14:40(UTC+0)
Changed:
Deleted:
Extraction: File System
MD5: 86d981708ac32042a8c5b2264ce79c0c
Source file: 1000001155.jpg
Classifications
Cars (44%)

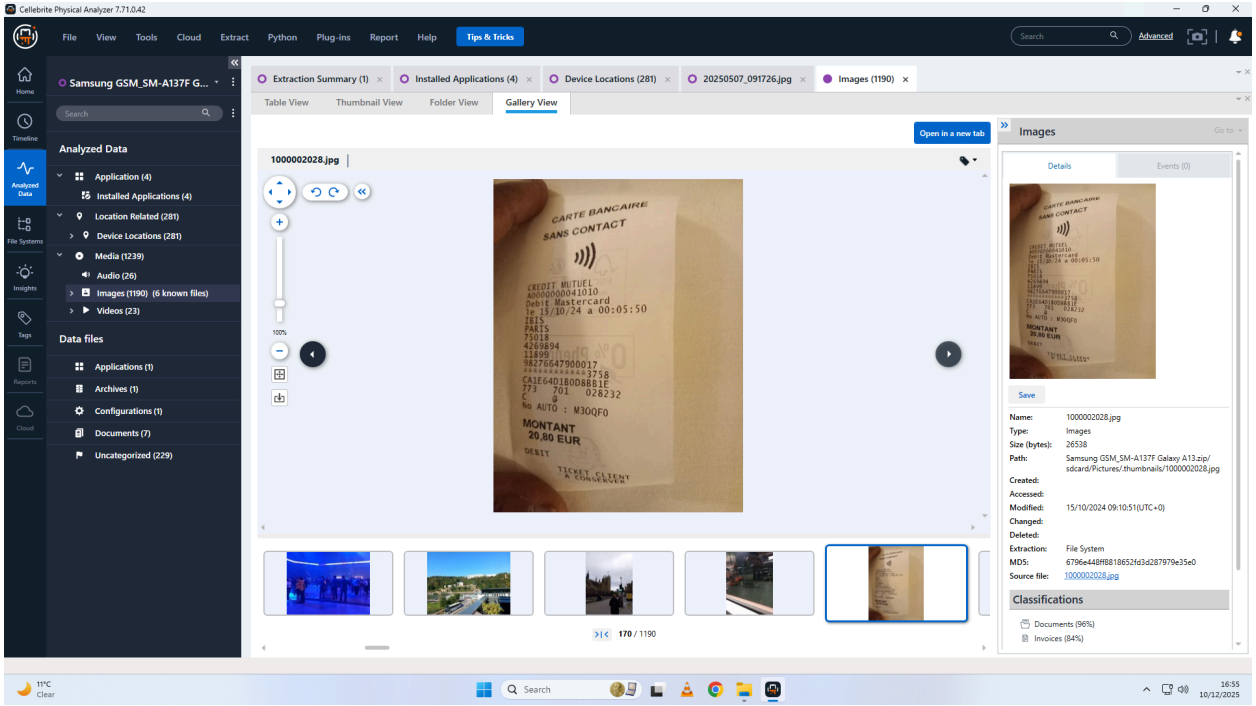

Cellebrite Physical Analyzer 7.71.0.42
File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks
Advanced
Samsung GSM_SM-A137F G...
Extraction Summary (1)
Installed Applications (4)
Device Locations (281)
20250507_091726.jpg
Images (1190)
Table View Thumbnail View Folder View Gallery View
Open in a new tab
1000001170.jpg
Analyzed Data
Application (4)
Installed Applications (4)
Location Related (281)
Device Locations (281)
Media (1239)
Audio (26)
Images (1190) (6 known files)
Videos (23)
Data files
Applications (1)
Archives (1)
Configurations (1)
Documents (7)
Uncategorized (229)
Images
Details
Events (0)
Save
Name: 1000001170.jpg
Type: Images
Size (bytes): 53322
Path: Samsung GSM_SM-A137F Galaxy A13.zip/ sdcard/Pictures/.thumbnails/1000001170.jpg
Created:
Accessed:
Modified: 22/08/2024 11:15:33(UTC+0)
Changed:
Deleted:
Extraction: File System
MD5: 0c468df1130437cdbdf28c959eb72c74
Source file: 1000001170.jpg
Classifications
Restaurant (55%)
Map
Position:
108 / 1190

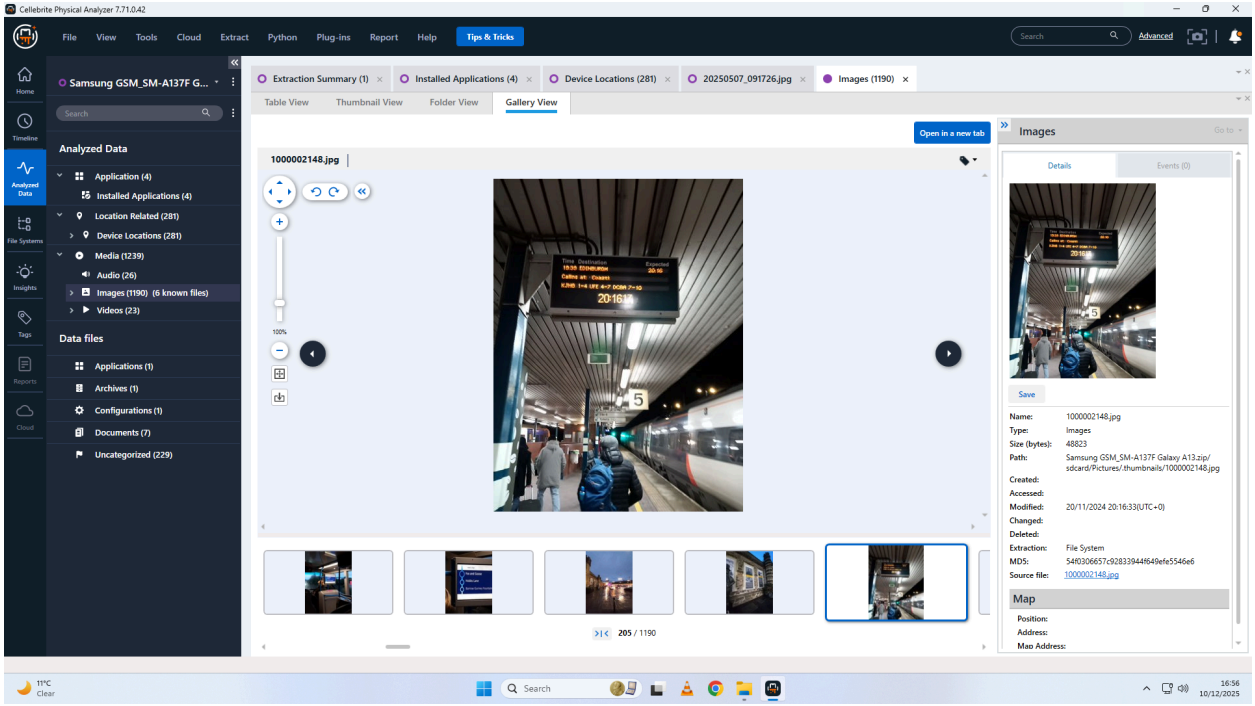

Cellebrite Physical Analyzer 7.71.0.42
File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks
Advanced
Samsung GSM_SM-A137F G...
Extraction Summary (1)
Installed Applications (4)
Device Locations (281)
20250507_091726.jpg
Images (1190)
Table View Thumbnail View Folder View Gallery View
Open in a new tab
1000001178.jpg
Abflug Departures
Analyzed Data
Application (4)
Installed Applications (4)
Location Related (281)
Device Locations (281)
Media (1239)
Audio (26)
Images (1190) (6 known files)
Videos (23)
Data files
Applications (1)
Archives (1)
Configurations (1)
Documents (7)
Uncategorized (229)
Images
Details
Events (0)
Save
Name: 1000001178.jpg
Type: Images
Size (bytes): 49262
Path: Samsung GSM_SM-A137F Galaxy A13.zip/ sdcard/Pictures/.thumbnails/1000001178.jpg
Created:
Accessed:
Modified: 22/08/2024 15:31:11(UTC+0)
Changed:
Deleted:
Extraction: File System
MD5: 193c679c1f19f84e95cd0e7ea40c9fe9
Source file: 1000001178.jpg
Classifications
Documents (100%)
112 / 1190


Cellebrite Physical Analyzer 7.71.0.42
File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks
Advanced
Samsung GSM_SM-A137F G...
Extraction Summary (1)
Installed Applications (4)
Device Locations (281)
20250507_091726.jpg
Images (1190)
Table View Thumbnail View Folder View Gallery View
Open in a new tab
1000001349.jpg
Analyzed Data
Application (4)
Installed Applications (4)
Location Related (281)
Device Locations (281)
Media (1239)
Audio (26)
Images (1190) (6 known files)
Videos (23)
Data files
Applications (1)
Archives (1)
Configurations (1)
Documents (7)
Uncategorized (229)
Images
Details
Events (0)
Save
Name: 1000001349.jpg
Type: Images
Size (bytes): 40946
Path: Samsung GSM_SM-A137F Galaxy A13.zip/sdcard/Pictures/.thumbnails/1000001349.jpg
Created:
Accessed:
Modified: 31/08/2024 20:00:02(UTC+0)
Changed:
Deleted:
Extraction: File System
MD5: f69611b6f9fe2f8e3b525b211e8276d
Source file: 1000001349.jpg
Classifications
Documents (98%)
Screenshots (68%)
131 / 1190


Cellebrite Physical Analyzer 7.71.0.42
File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks
Advanced
Samsung GSM_SM-A137F G...
Extraction Summary (1)
Installed Applications (4)
Device Locations (281)
20250507_091726.jpg
Images (1190)
Table View Thumbnail View Folder View Gallery View
Open in a new tab
1000001425.jpg
will open on the right
Analyzed Data
Application (4)
Installed Applications (4)
Location Related (281)
Device Locations (281)
Media (1239)
Audio (26)
Images (1190) (6 known files)
Videos (23)
Data files
Applications (1)
Archives (1)
Configurations (1)
Documents (7)
Uncategorized (229)
Images
Details
Events (0)
Save
Name: 1000001425.jpg
Type: Images
Size (bytes): 35708
Path: Samsung GSM_SM-A137F Galaxy A13.zip/sdcard/Pictures/.thumbnails/1000001425.jpg
Created:
Accessed:
Modified: 04/09/2024 21:07:34(UTC+0)
Changed:
Deleted:
Extraction: File System
MD5: dec08308ea53ed83c41d8e593d49fcfb
Source file: 1000001425.jpg
Classifications
Documents (96%)
135 / 1190


Cellebrite Physical Analyzer 7.71.0.42
File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks
Advanced
Samsung GSM_SM-A137F G...
Analyzed Data
Application (4)
Installed Applications (4)
Location Related (281)
Device Locations (281)
Media (1239)
Audio (26)
Images (1190) (6 known files)
Videos (23)
Data files
Applications (1)
Archives (1)
Configurations (1)
Documents (7)
Uncategorized (229)
Extraction Summary (1)
Installed Applications (4)
Device Locations (281)
20250507_091726.jpg
Images (1190)
Table View
Thumbnail View
Folder View
Gallery View
Open in a new tab
1000001427.jpg
136 / 1190
Images
Details
Events (0)
Save
Name: 1000001427.jpg
Type: Images
Size (bytes): 36466
Path: Samsung GSM_SM-A137F Galaxy A13.zip/ sdcard/Pictures/.thumbnails/1000001427.jpg
Created:
Accessed:
Modified: 05/09/2024 08:27:42(UTC+0)
Changed:
Deleted:
Extraction: File System
MD5: 38aa6267b081cf9e5cada8c81fbbb872
Source file: 1000001427.jpg
Classifications
Documents (96%)
Smartphones (69%)
11°C Clear
Search
16:54 10/12/2025


Cellebrite Physical Analyzer 7.71.0.42
File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks
Advanced
Samsung GSM_SM-A137F G...
Analyzed Data
Application (4)
Installed Applications (4)
Location Related (281)
Device Locations (281)
Media (1239)
Audio (26)
Images (1190) (6 known files)
Videos (23)
Data files
Applications (1)
Archives (1)
Configurations (1)
Documents (7)
Uncategorized (229)
Extraction Summary (1)
Installed Applications (4)
Device Locations (281)
20250507_091726.jpg
Images (1190)
Table View
Thumbnail View
Folder View
Gallery View
Open in a new tab
1000002028.jpg
CARTE BANCAIRE
SANS CONTACT
CREDIT MUTUEL
Debit Mastercard
Le 15/10/24 a 00:05:50
IBIS
PARIS
75018
MONTANT
20,80 EUR
DEBIT
170 / 1190
Images
Details
Events (0)
Save
Name: 1000002028.jpg
Type: Images
Size (bytes): 26538
Path: Samsung GSM_SM-A137F Galaxy A13.zip/ sdcard/Pictures/.thumbnails/1000002028.jpg
Created:
Accessed:
Modified: 15/10/2024 09:10:51(UTC+0)
Changed:
Deleted:
Extraction: File System
MD5: 6796e448ff8818652fd3d287979e35e0
Source file: 1000002028.jpg
Classifications
Documents (96%)
Invoices (84%)
11°C Clear
Search
16:55 10/12/2025


Cellebrite Physical Analyzer 7.71.0.42
File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks
Search Advanced
Samsung GSM_SM-A137F G...
Analyzed Data
Application (4)
Installed Applications (4)
Location Related (281)
Device Locations (281)
Media (1239)
Audio (26)
Images (1190) (6 known files)
Videos (23)
Data files
Applications (1)
Archives (1)
Configurations (1)
Documents (7)
Uncategorized (229)
Extraction Summary (1)
Installed Applications (4)
Device Locations (281)
20250507_091726.jpg
Images (1190)
Table View
Thumbnail View
Folder View
Gallery View
Open in a new tab
1000002148.jpg
205 / 1190
Images
Details
Events (0)
Save
Name: 1000002148.jpg
Type: Images
Size (bytes): 48823
Path: Samsung GSM_SM-A137F Galaxy A13.zip/ sdcard/Pictures/.thumbnails/1000002148.jpg
Created:
Accessed:
Modified: 20/11/2024 20:16:33(UTC+0)
Changed:
Deleted:
Extraction: File System
MD5: 54f0306657c92833944f649efe5546e6
Source file: 1000002148.jpg
Map
Position:
Address:
Map Address:
11°C Clear
Search
16:56 10/12/2025

Conclusion

Based on the thorough forensic analysis of the seized pieces of digital evidence, the investigation has been able to reconstruct a transnational network of corporate espionage targeted against the proprietary "Project Neuro" intellectual property belonging to Quantum Technologies. The inquiry had its origin in internal security warnings about unauthorized access by an employee of an organization known as Emma into some of its computer databases, whereat three font-end devices were hopeless three Huawei P Smart 2019, Samsung Galaxy A13 and Nokia C2 (Ulefone Note 14). Using forensic extraction with Cellebrite Physical Analyzer, verified with SHA 256 hashing, it was verified that Emma's Huawei device had been used as the central command node.

Analysis of this device yielded up a pattern of "Top-up" chat logs in which Emma clearly solicited a contact named "Joe" with the specific purpose of selling stolen trade secrets, with conversations demonstrating a clear mens rea as to the illegality of their conduct and that the value of the data was very high for commercial benefit. The investigation was able to further identify "Joe" as the user of the Samsung Galaxy A13, a device with "sterile" configuration with no personal accounts but replete with logistical data. This attribution is supported by a good level of spatiotemporal correlation between the two devices; the locations of the two phones, using the GPS data, are shown to be in the same part of Greater London during certain gaps in their digital communications, which provided evidence for in-person meetings to discuss sensitive operational details. While Emma was responsible for the data exfiltration, this time around, Joe was the external facilitator with chat logs and supporting visual artifacts (such as photographs of train tickets and hotel key cards) to record his movement between Glasgow, Manchester, and Paris to negotiate with potential buyers.

Finally the reach of the network is not solely UK based as demonstrated by the (Ulefone) device and geospatial data. Combined with call logs from Emma's device that showed incessant attempts to contact a mobile number in India, and geospatial clustering in India, this evidence is suggestive of a long-term support infrastructure, or an inactive historical node of the conspiracy.

References

[1] P. Manson, "Global digital forensics market analysis and projections," *Forensic Sci. Int.: Digit. Investig.*, vol. 35, p. 301149, 2020.

[2] (ISC)² & Cybersecurity Ventures, *2024 Official Cybersecurity Workforce Study*. Arlington, VA, USA: (ISC)², 2024.

[3] McKinsey & Company, *State of Cybersecurity and Digital Forensics in the Enterprise 2024*. New York, NY, USA: McKinsey Global, 2024.

[4] U.S. Federal Bureau of Investigation, *Digital Forensics Capabilities and Career Opportunities*. Washington, DC, USA: FBI, 2023.

[5] U.S. Bureau of Labor Statistics, *Information Security Analysts Occupational Handbook 2024*. Washington, DC, USA: U.S. Dept. Labor, 2024.

[6] Financial Industry Regulatory Authority, *Cybersecurity and Forensic Investigations in Financial Services*. New York, NY, USA: FINRA, 2023.

[7] Deloitte Touche Tohmatsu Limited, *Digital Forensics and Incident Response Market Analysis*. New York, NY, USA: Deloitte, 2023.

[8] P. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 4th ed. Waltham, MA, USA: Syngress, 2018.

[9] International Society of Forensic Computer Examiners, *CFCE Certification Requirements and Standards*. Washington, DC, USA: ISFCE, 2023.

[10] SANS Institute, *GIAC Certified Forensic Examiner Certification Program*. Bethesda, MD, USA: SANS, 2024.

[11] Cellebrite, *Cellebrite Certified Examiner Program and Credentials*. Petah Tikva, Israel: Cellebrite, 2023.

[12] GIAC, *Continuing Education Requirements for GIAC Forensic Certifications*. Arlington, VA, USA: GIAC, 2023.

[13] U.S. Bureau of Labor Statistics, "Information security analysts: Career outlook and employment projections," U.S. Dept. Labor, Washington, DC, USA, 2024.

[14] Glassdoor, *Digital Forensics Analyst Compensation Analysis 2024*. San Francisco, CA, USA: Glassdoor, Inc., 2024.

[15] National Crime Agency, *Digital Forensics and Cybercrime Units Recruitment*. London, UK: Nat. Crime Agency, 2023.

[16] National Association of Software and Service Companies, *India Digital Forensics and Cybersecurity Employment Survey*. New Delhi, India: NASSCOM, 2023.

[17] Indeed, *Digital Forensics Analyst Salaries in India*. Bangalore, India: Indeed, 2024.

[18] Gulf Cooperation Council, *Regional Cybersecurity and Digital Forensics Initiatives*. Riyadh, Saudi Arabia: GCC Secretariat, 2023.

[19] N. Yusoff, "International career mobility in cybersecurity and forensics professions," *Int. J. Prof. Stud.*, vol. 15, no. 2, pp. 123–141, 2022.

[20] FlexJobs, *Remote Digital Forensics and Incident Response Positions*. Arlington, VA, USA: FlexJobs, 2024.

[21] Interpol, *International Digital Forensics Cooperation and Training Programmes*. Lyon, France: Interpol, 2023.

[22] LinkedIn Workplace Intelligence, *Future of Work in Cybersecurity and Forensics*. Sunnyvale, CA, USA: LinkedIn, 2023.

[23] Cloud Security Alliance, *Cloud Forensics Specialist Compensation and Skill Requirements*. Seattle, WA, USA: Cloud Secur. Alliance, 2023.

[24] Harvard Business School, *Executive Presence and Communication Skills Development for Technical Professionals*. Boston, MA, USA: Harvard Business School, 2023.

[25] Robert Half, *2024 Technology Salary Guide: Forensic and Security Specialisation*. Menlo Park, CA, USA: Robert Half Int., 2024.