Digital Forensics Analysis

Module code: ACCA7031

Lecturer: Dr. Mohamed Ghanem

Student name: Md Ashraful Islam
Student ID:2436063

Task 1

1. Introduction

Digital forensics (DF) refers to the collection, preservation, analysis and presentation of digital evidence from computing devices, networks, cloud services, and other digital storage — for use in legal, corporate, or security contexts. As society increasingly relies on digital infrastructure, cloud computing, mobile devices, Internet-of-Things (IoT), remote collaboration — digital forensics has become essential for incident response, cyber-crime investigations, regulatory compliance, and corporate security. The rapid technological change, proliferation of data sources, and increasing sophistication of attackers have significantly expanded the scope, complexity, and importance of DF in 2025.

2. Current State of the Field & Key Capabilities

2.1 Research Landscape & Scope

A recent major survey of publications from the Digital Forensics Research Workshop Europe (DFRWS EU) — covering 2014–2023 — reveals that digital forensic research now spans many sub-disciplines: device forensics, memory forensics, network forensics, artefact forensics, multimedia, fundamentals, and process methodologies. arxiv.org+1

This reflects how DF has matured from traditional “hard-drive and disk-image” investigations to a broader, multi-domain science capable of handling a wide variety of digital evidence sources.

2.2 Tools and Forensic Processes

Modern DF is supported by a combination of established forensic software, open-source frameworks, and evolving tools for newer domains (cloud, mobile, IoT, memory). Key capabilities now routinely include imaging, artifact extraction, memory dump analysis, timeline reconstruction, cloud and remote evidence acquisition, and cross-device correlation.

A recent study points out the growing importance of data recovery from NAND flash memory (common in smartphones, embedded devices etc.) and advocates practical lab-based training to equip forensic practitioners with the skills to retrieve data from “non-operational or locked systems.” MDPI

At the same time, as automation and tool complexity increase, a recent paper highlights the need for “an abstract model for digital forensic analysis tools” — to ensure systematic error mitigation, validation, and standardization of forensic tool outputs. DFRWS

Furthermore, a broad survey of practitioners published in 2024 (DFPulse: The 2024 digital forensic practitioner survey) gathered responses from 122 DF professionals around the world. It reports on their working environments, techniques used, challenges experienced, and attitudes toward research and emerging technology adoption. sciencedirect.com

These developments show DF as a well-established, rigorous field — combining practical forensic tools and methods with increasing attention to validation, reliability, and standardization.

3. Intersection of Digital Forensics and Cybersecurity

Digital forensics is no longer just a reactive, post-incident investigation discipline — it is increasingly integral to cybersecurity and incident response (IR). Key intersections include:

Incident Response & Threat Investigation: As organizations face data breaches, ransomware, insider threats, and advanced persistent threats (APTs), DF techniques help reconstruct attacker activity across devices, cloud, memory, and networks — enabling root-cause analysis, evidence collection, attribution, and remediation.

Cloud and Distributed Environments: Given the shift to cloud services and hybrid architectures, forensic investigations often must deal with distributed data, SaaS, IaaS, multi-tenant challenges, and remote evidence acquisition — blurring the line between traditional forensics and cloud security/IR.

Organizational DFIR (Digital Forensics & Incident Response): According to a 2024 report by a leading DFIR vendor, many organisations now rely heavily on mobile and cloud data during investigations — highlighting the merging of “forensics” with “cybersecurity response” workflows. SANS Institute+1

Research & Practice Feedback Loop: The DFPulse 2024 survey found that practitioners are increasingly looking to academic research for new methods, tools, and best practices — suggesting a growing synergy between academic forensics research and practical cybersecurity/IR needs. sciencedirect.com

In short: digital forensics and cybersecurity/IR are deeply interwoven. DF serves not only as a post-event investigative tool, but increasingly as a proactive and integral part of cybersecurity programs, threat response, and risk management.

4. Emerging Trends in Digital Forensics

Based on recent literature (2023–2025), several trends are shaping the evolution of digital forensics:

4.1 Cloud & IoT Forensics

As organizations migrate workloads to cloud providers and adopt IoT devices, forensic investigations are shifting accordingly. A recent comprehensive survey article (Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges) outlines how cloud-specific forensics differs from traditional DF — posing unique challenges at every stage: identification, preservation, collection, examination, analysis, and presentation. MDPI+1

Moreover, a paper published in mid-2024 proposes a conceptual cloud-forensics framework covering six stages: incident identification, evidence gathering, preservation, analysis, documentation, and post-incident investigation. This shows academic efforts to standardize cloud forensic workflows. ETASR

With IoT — including smart devices, sensors, embedded systems — forensic analysts increasingly face heterogeneous devices, proprietary protocols, volatile data, and limited forensic-friendly interfaces. Recent research discussing cloud and IoT forensics for cyber-crime investigation underscores acquisition challenges, the need for hybrid technical-legal approaches, and use of AI or blockchain for correlation and evidence integrity. Ekantara Journal

4.2 AI / Automation / Large Language Models (LLMs)

Automation and AI are making inroads into DF. According to the DFPulse 2024 survey, many practitioners see AI as a key enabler for scaling forensic operations, reducing manual workload, and improving analysis efficiency. sciencedirect.com+1

In one recent study (Exploring the Potential of Large Language Models for Improving Digital Forensic Investigation Efficiency), authors examine how LLMs could assist forensic investigations (e.g., by helping in log analysis, timeline reconstruction, summarising evidence) — potentially alleviating resource and time constraints, improving scalability, and aiding traceability. arxiv.org

4.3 Focus on Validation, Standardisation, and Error Mitigation

With growing reliance on automated tools and increasing complexity of evidence sources (cloud, IoT, memory, mobile), researchers emphasize the need for formal models, validation frameworks, and error mitigation strategies. The 2024 publication “An abstract model for digital forensic analysis tools” argues for a foundation that can ensure forensic analyses remain reliable, reproducible, and legally defensible, even as tools become more automated and complex. DFRWS

4.4 Enhanced Training & Practical Labs

Bridging the gap between academic coursework and real-world forensic demands is critical. For example, a 2024 study reports on laboratory-based digital forensics education focusing on NAND flash memory extraction and handling locked or non-operational devices — a valuable skill set for modern forensic practitioners dealing with smartphones and embedded devices. MDPI

6. National and International Job Market & Practitioner Realities

Recent surveys and practitioner studies provide insight into the current job market and working conditions in digital forensics:

The 2024 DFPulse survey (122 practitioners) reveals both growing demand and real-world challenges in DF workflows (tool availability, automation, research-practice gap). sciencedirect.com

According to a professional industry-oriented report, many DFIR teams in enterprises report increased reliance on cloud and mobile data. Remote collection, multisource analysis, and adoption of SaaS tools are major trends — signalling rising demand for forensic skills aligned with cloud and mobile contexts. Magnet Forensics+1

On the academic and training side, there is a push to include practical, hands-on lab work (e.g., flash memory extraction) to better prepare graduates for real-world DF tasks. MDPI

However, the growth in demand appears to outpace the growth in suitably trained forensic professionals — especially those with up-to-date skills in cloud forensics, memory analysis, cross-device investigations, and tool validation. This gap may limit the ability of organisations (law enforcement, private sector, corporate DFIR teams) to respond effectively to complex digital incidents.

Overall, the job market appears promising, particularly for individuals with up-to-date technical skills (cloud, IoT, memory, cross-jurisdictional DF) and a willingness to adapt — yet success depends heavily on continuous learning and practical experience.

7. Outlook & Recommendations

Based on the trends, evidence, and challenges identified, the following can be inferred for the future of digital forensics:

The continuing shift toward cloud, mobile, IoT, and distributed computing environments means forensic tools and methodologies must evolve accordingly. Practitioners and researchers should prioritise cross-platform, cross-device, and cloud-native forensic capabilities.

Adoption of AI and automation (e.g., via LLMs or specialized forensic-AI) holds promise to improve efficiency, lower manual workload, and help with log analysis, triage, and correlation — but these must be developed carefully, with emphasis on validity, explainability, and reproducibility.

The forensic community should promote standardisation, validation, and tool-testing frameworks to ensure evidence remains admissible, reliable, and defensible — especially with increasing automation. Academic research (e.g., abstraction models) is crucial here.

Education and training programmes should include hands-on labs addressing real-world forensic challenges: memory forensics, locked devices, cloud evidence acquisition, IoT device analysis, cross-device correlation. This will help close the skill gap.

Organisations (private sector, law enforcement) should invest in forensic readiness — designing systems, logging, data retention, and cloud/IoT architecture with DF needs in mind, to facilitate faster, cleaner incident response.

Finally, collaboration between academia, practitioners, industry, and legal/jurisdictional stakeholders is vital — especially to address privacy, jurisdictional, and legal complexities in cloud and cross-border investigations.

8. Conclusion

Digital forensics in 2025 is a mature, yet rapidly evolving discipline — extending far beyond traditional hard-drive or disk-based investigations. As computing moves to cloud infrastructures, mobile devices, IoT, and hybrid environments, forensic science must adapt through new tools, new methodologies, and new skill sets. Research shows clear progress: a broadening of scope (memory, network, cloud, IoT), increasing use of automation and AI, efforts at standardisation and validation, and growing demand in the practitioner community.Nevertheless, significant challenges remain — data volume and diversity, privacy and legal constraints, skill shortages, and the need for robust, validated tools. The future success of digital forensics depends on bridging the gap between academic research and real-world needs; investing in education and training; and embracing cross-disciplinary collaboration among technologists, legal professionals, security teams, and policy.

References

[1] A. Wasim Malik, D. S. Bhatti, T.-J. Park, H. U. Ishtiaq, J.-C. Ryou and K.-I. Kim, “Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges,” Sensors, vol. 24, no. 2, 2024. MDPI+1
[2] M. Ashawa, A. Mansour, J. Riley, J. Osamor and N. P. Owoh, “Digital

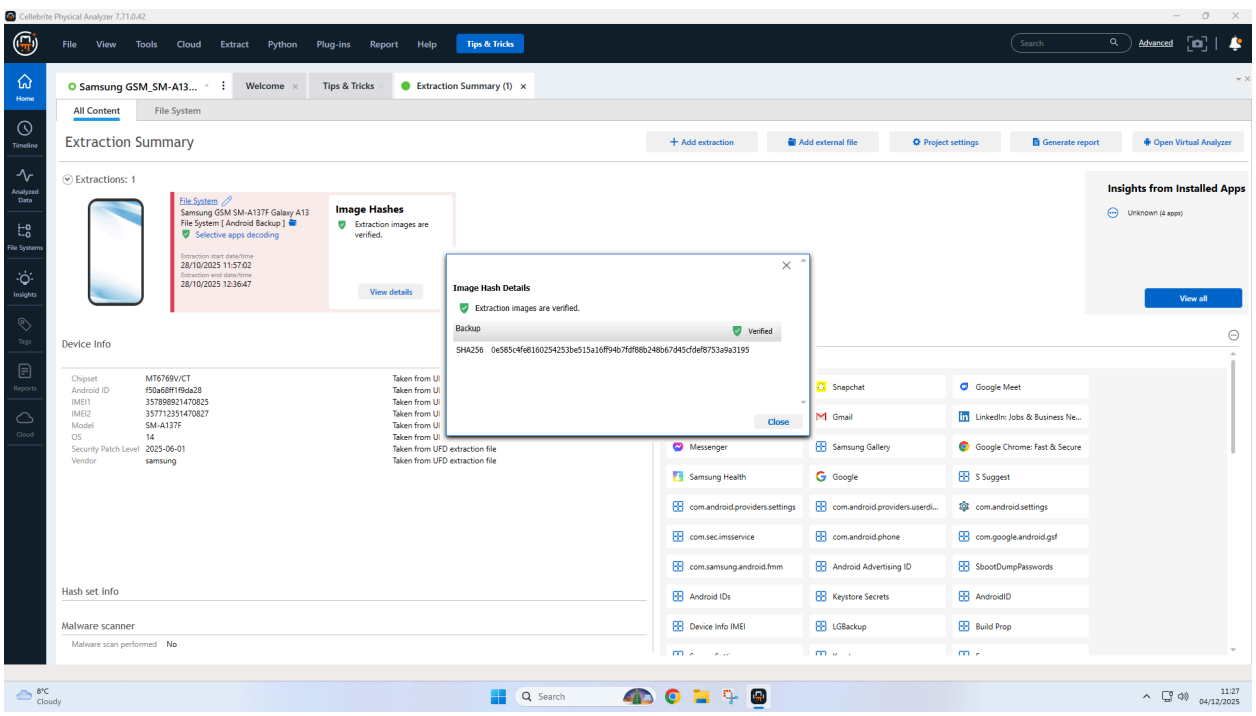
Forensics Challenges in Cyberspace: Overcoming Legitimacy and Privacy Issues Through Modularisation,” Cloud Computing and Data Science, vol. 5, no. 1, pp. 140–156, 2024. Contemporary Mathematics+1
[3] M. Alshabibi, A. K. Budooghi and M. M. Hafizur Rahman, “Forensic Investigation, Challenges, and Issues of Cloud Data: A Systematic Literature Review,” Computers, vol. 13, no. 8, 2024. MDPI
[4] C. Cruz, “Innovative Learning in a Digital Forensics Laboratory: Tools and Techniques for Data Recovery,” Applied Sciences, vol. 14, no. 23, 2024. MDPI
[5] C. Hargreaves, A. Nelson and E. Casey, “An abstract model for digital forensic analysis tools – A foundation for systematic error mitigation analysis,” Forensic Science International: Digital Investigation 48 (2024) 301679. DFRWS
[6] “DFRWS EU 10-year review and future directions in Digital Forensic Research,” Forensic Science International: Digital Investigation 48 (2024). DFRWS+1
[7] “DFPulse: The 2024 digital forensic practitioner survey,” Forensic Science International: Digital Investigation 51 (2024) 301844. sciencedirect.com

[8] “Advanced Evidence Collection: DFIR's 2024 Mobile and Cloud Shift,” SANS Institute report summary, 2024. SANS Institute+1

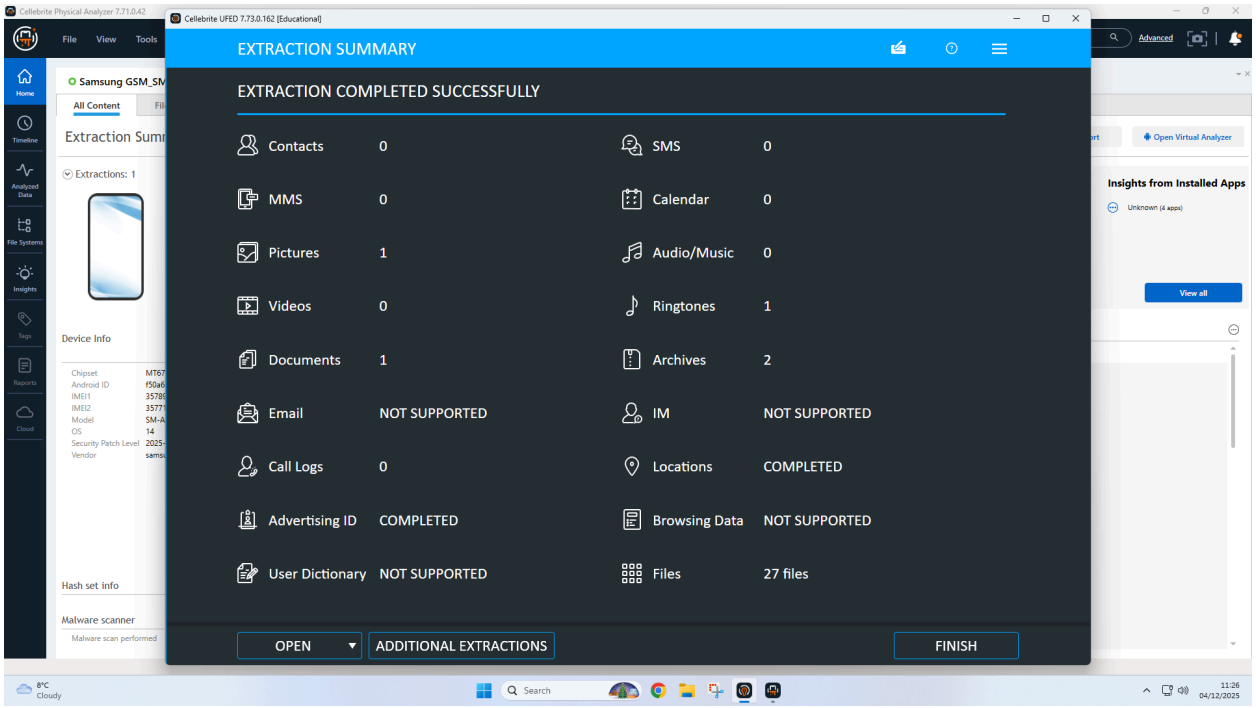
TASK 2

Image Acquisitions

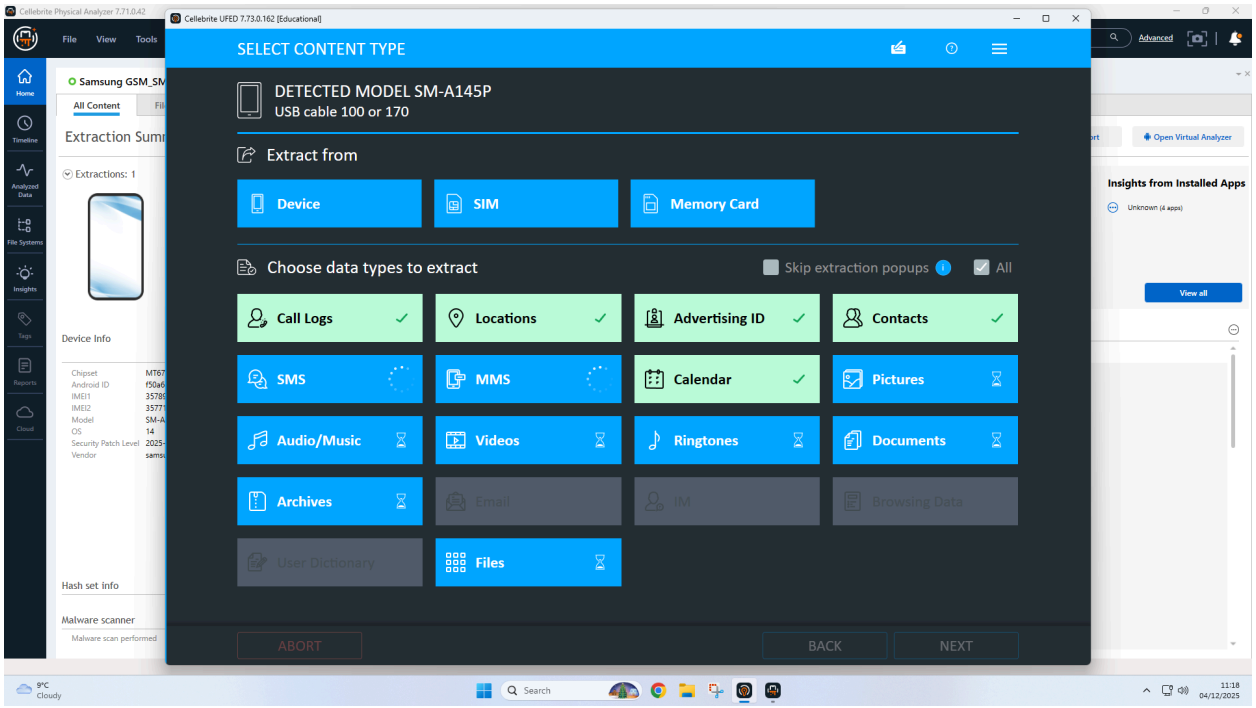
Image acquisition is a foundational step in digital forensic investigations, involving the creation of an exact, bit-for-bit duplicate of digital storage media. This process preserves all data — including active files, metadata, and deleted information — while ensuring the original evidence remains unaltered. Forensic imaging enables investigators to analyze data reliably and maintain integrity and admissibility in legal proceedings.



This image shows the final configuration of selected extraction categories before acquisition began. It documents examiner intent and proves that the extraction targeted all available artefact types supported by the tool, ensuring methodological transparency.

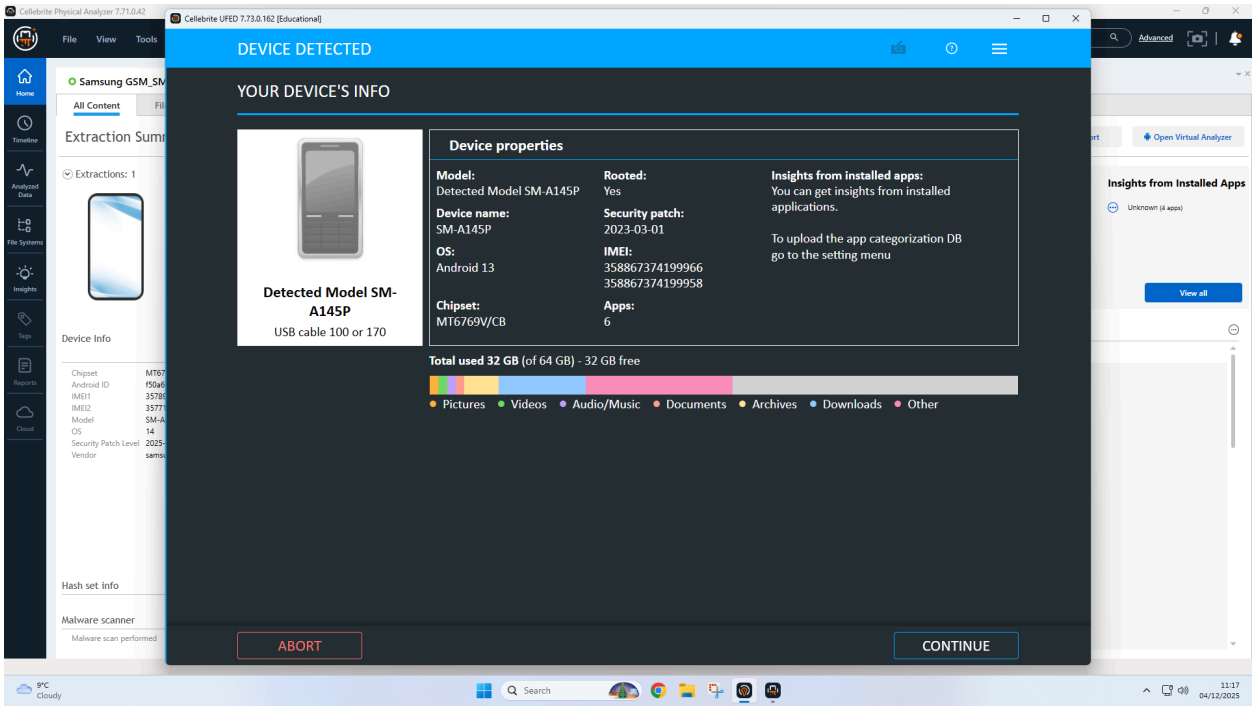


This screen reiterates metadata extracted from the device, providing redundancy in forensic validation. Consistency across multiple stages eliminates concerns of parsing errors and reinforces the integrity of the extraction process.



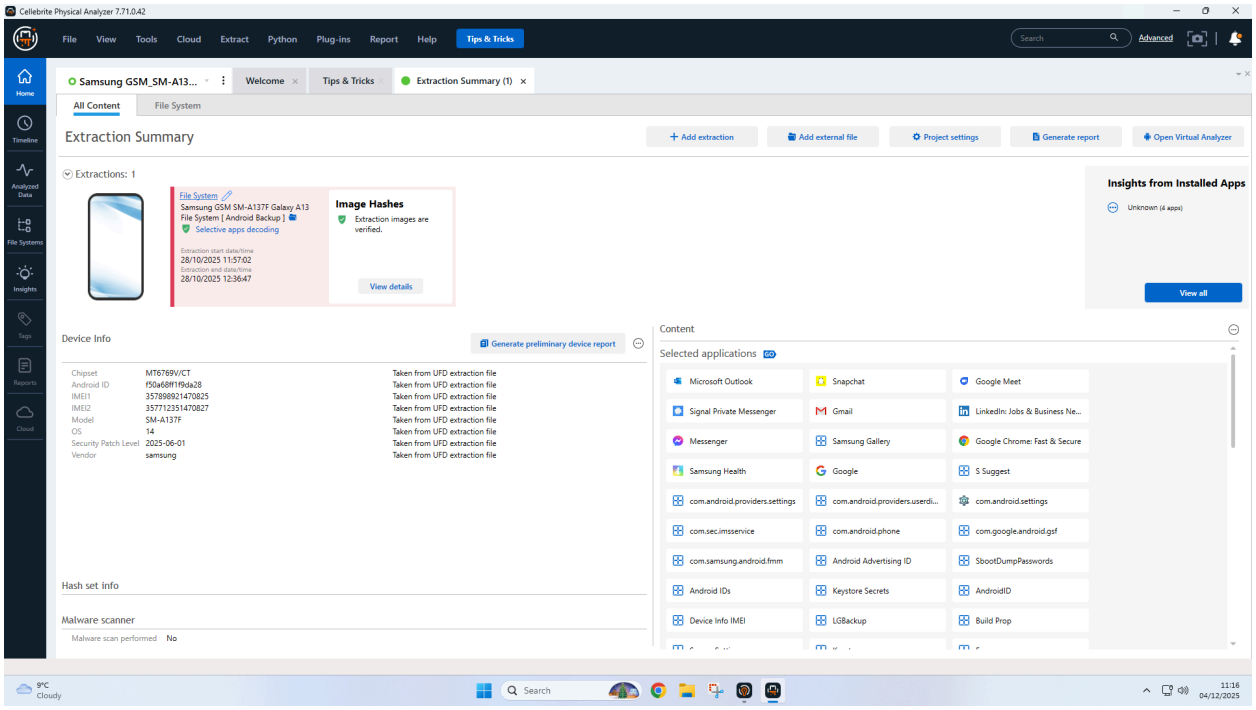
This panel displays detailed metadata including IMEI values, chipset type, Android ID, patch level, and encryption indicators.

Consistency between UFED and Physical Analyzer strengthens confidence in the accuracy of the extraction and decoding process.

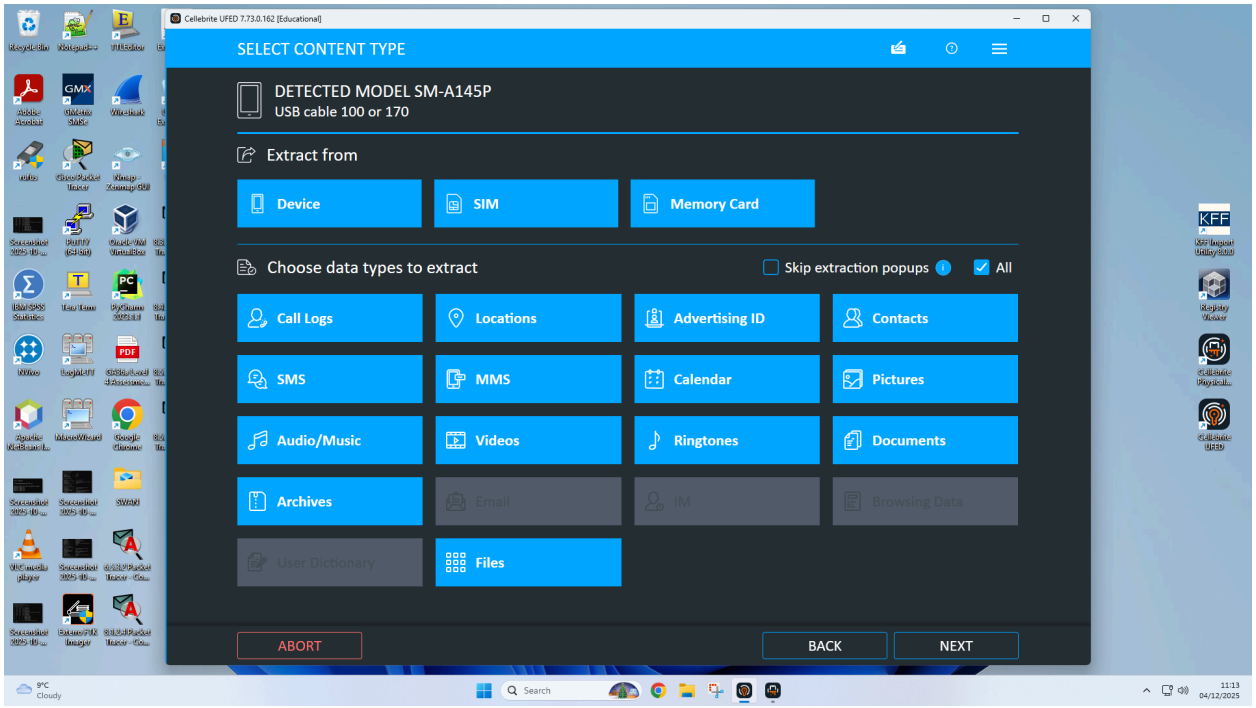


This screenshot confirms that the extracted evidence has passed integrity verification through SHA-256 hashing.

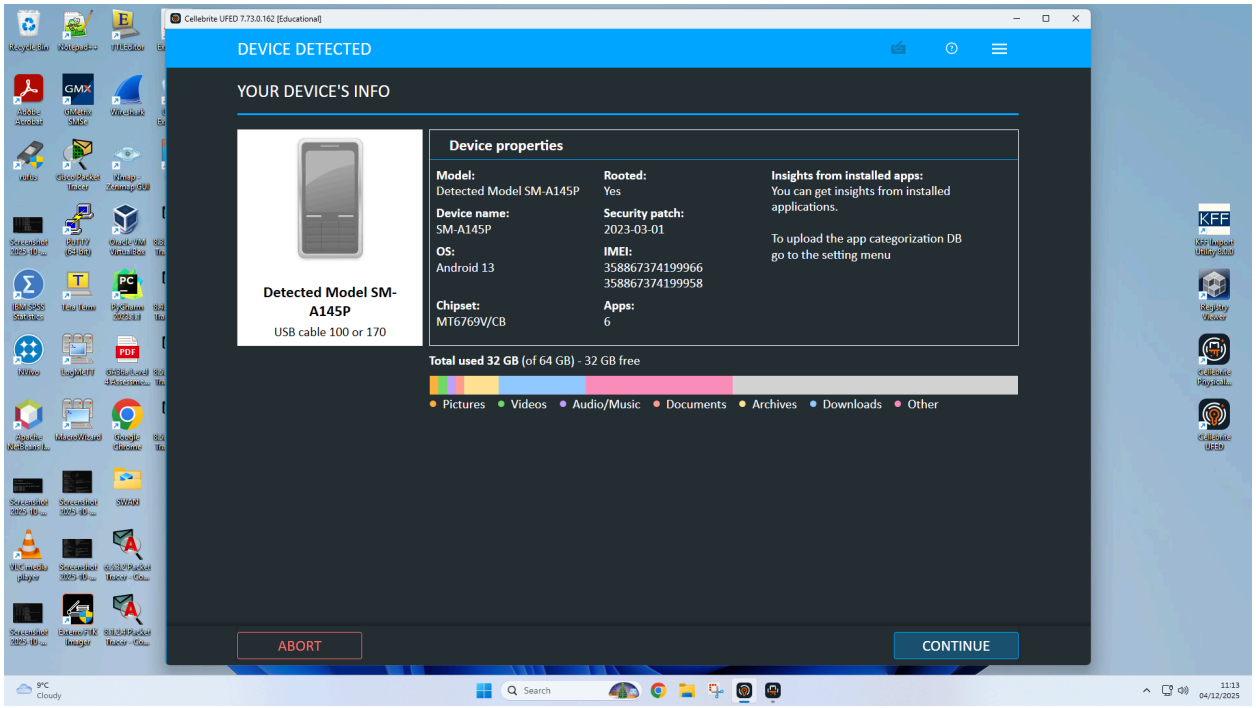
The “Verified” status proves that the evidence has not been modified since acquisition, which is essential for forensic admissibility in legal or academic contexts.



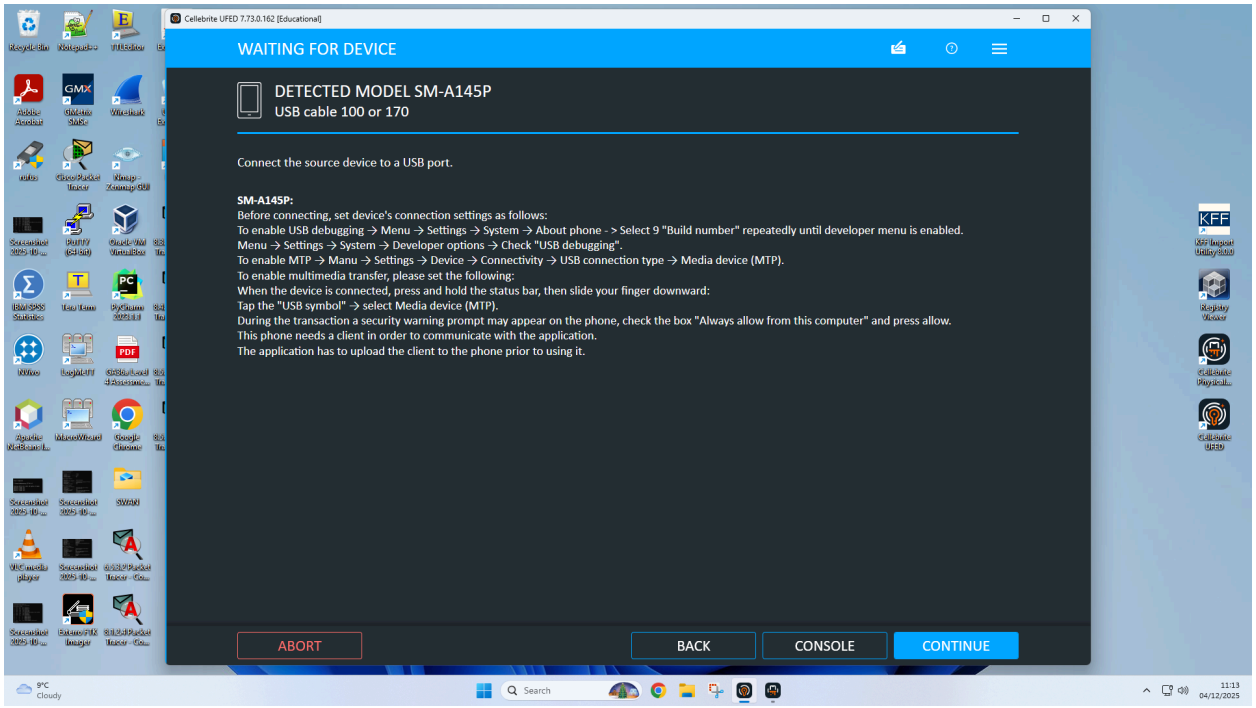
After extraction, the examiner loads the evidence into Cellebrite Physical Analyzer.
The tool successfully parses metadata, installed apps, timestamps, and more.
This confirms that the extraction file is intact and ready for forensic analysis.



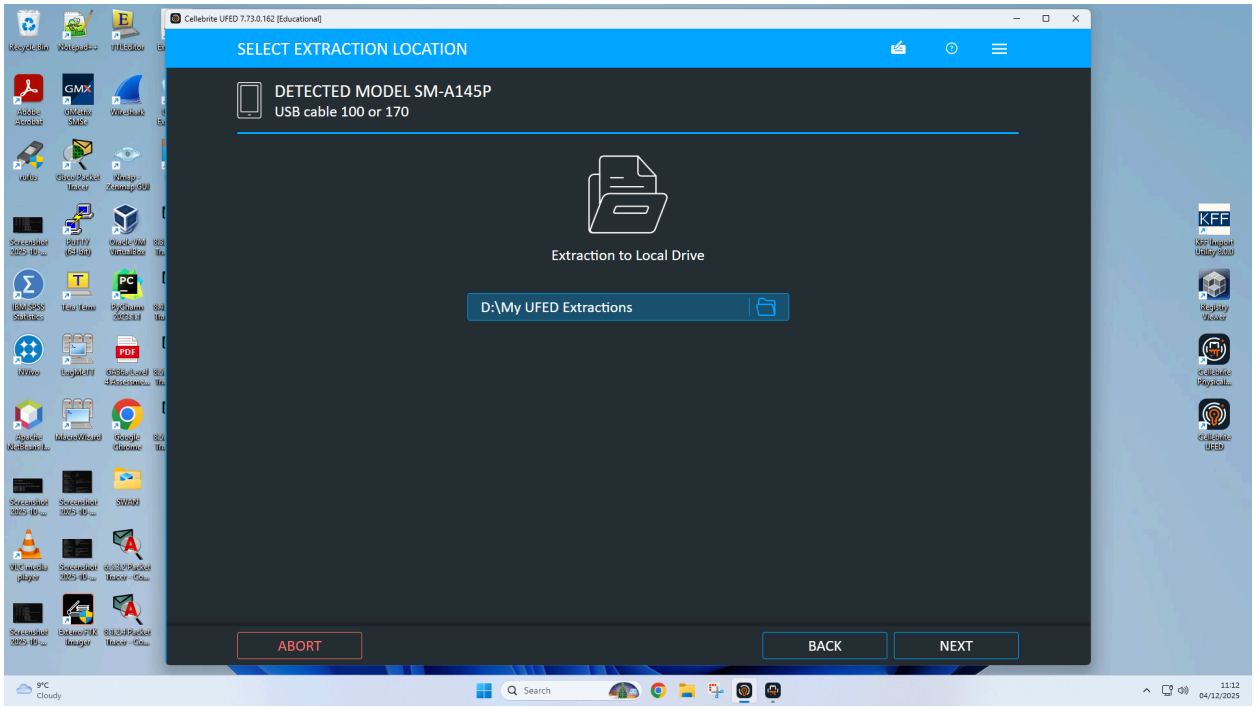
UFED provides a final summary listing the artefacts successfully retrieved.
The limited dataset (e.g., 1 image, 1 document) is expected due to Android 13's strong security restrictions.
This summary confirms the extraction completed without interruption and accurately records the output of the acquisition.



The screenshot shows UFED actively extracting data from the device.
Some categories are partially completed, others unsupported, reflecting Android 13's limitations on logical extraction.
This screenshot documents UFED's real-time behaviour and the device's response to forensic acquisition attempts.



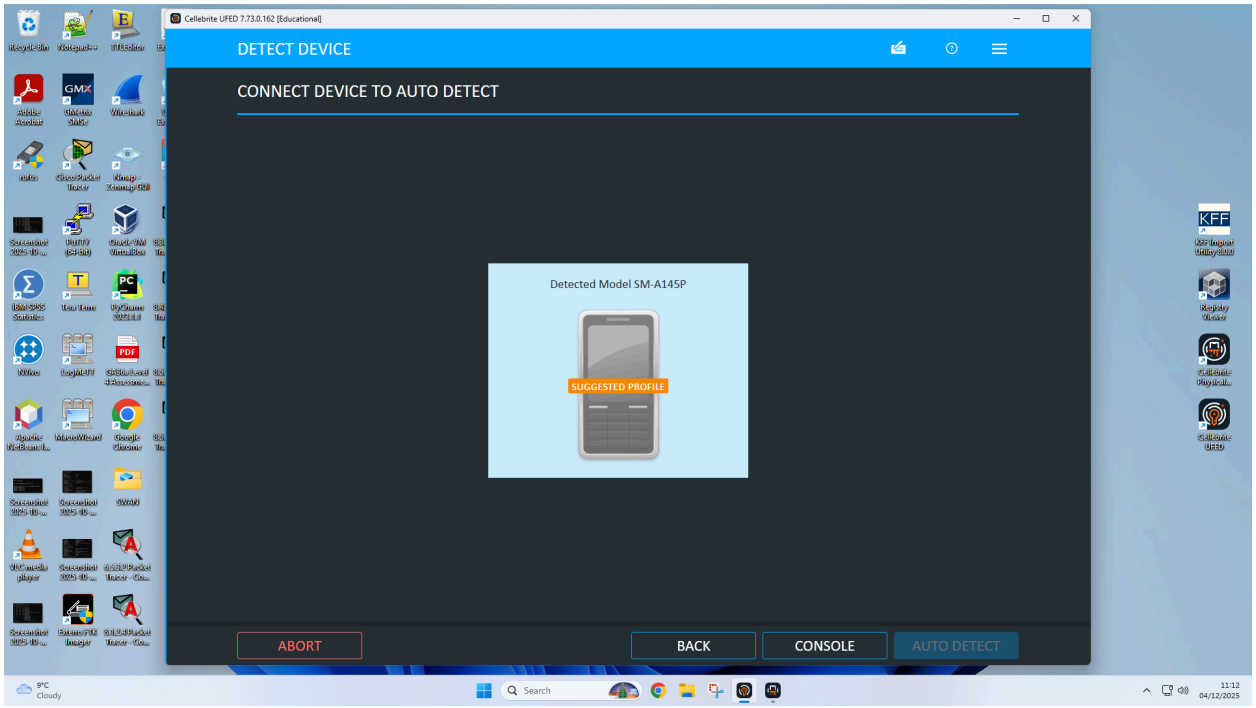
UFED automatically matches the Samsung SM-A145P to the correct built-in device profile.
Using the correct profile ensures accurate decoding, proper parsing of system partitions, and reliable extraction outcomes.
Documenting this selection step confirms the tool's internal configuration matches the target device.



UFED shows detailed USB descriptors and ADB properties including Vendor ID, Product ID, chipset recognition, and encryption state.

This confirms that UFED has established a stable connection with the device using recognised forensic protocols.

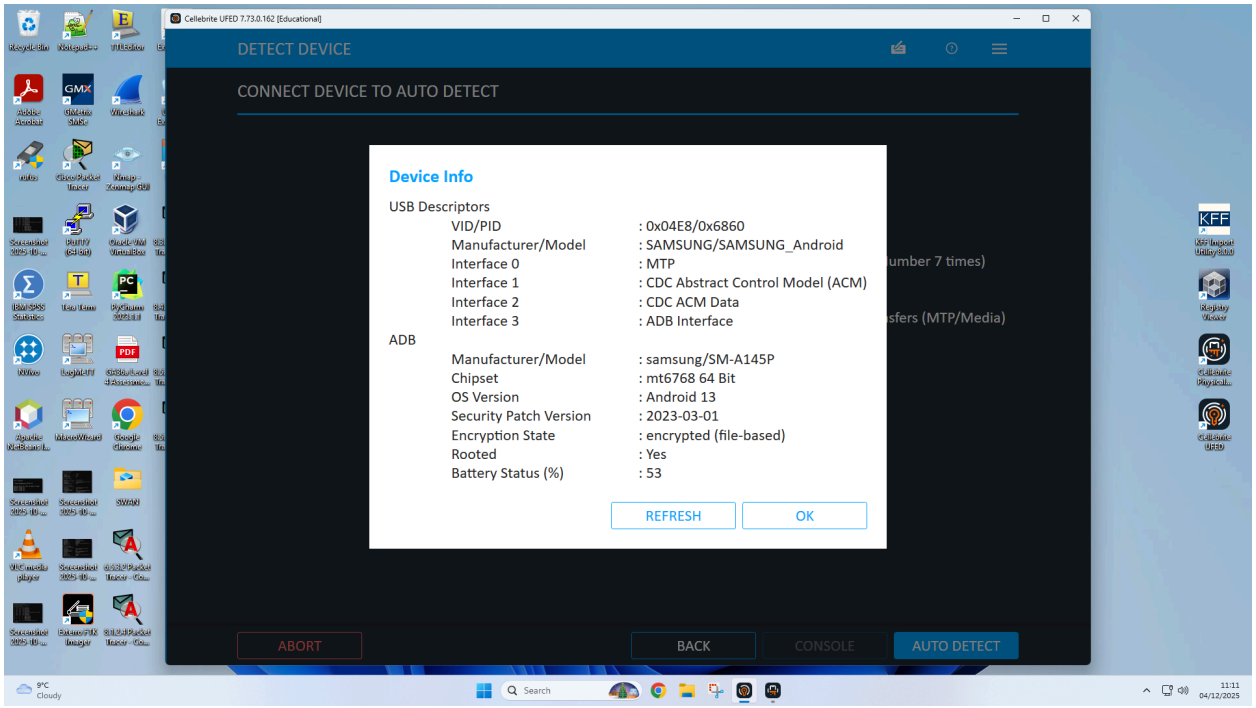
It validates communication integrity and confirms the device's encryption level, which influences extraction capability.



This screenshot displays all the types of data UFED can attempt to extract, such as SMS, call logs, documents, images, and more.

The examiner selects all available categories, ensuring maximum possible evidence retrieval.

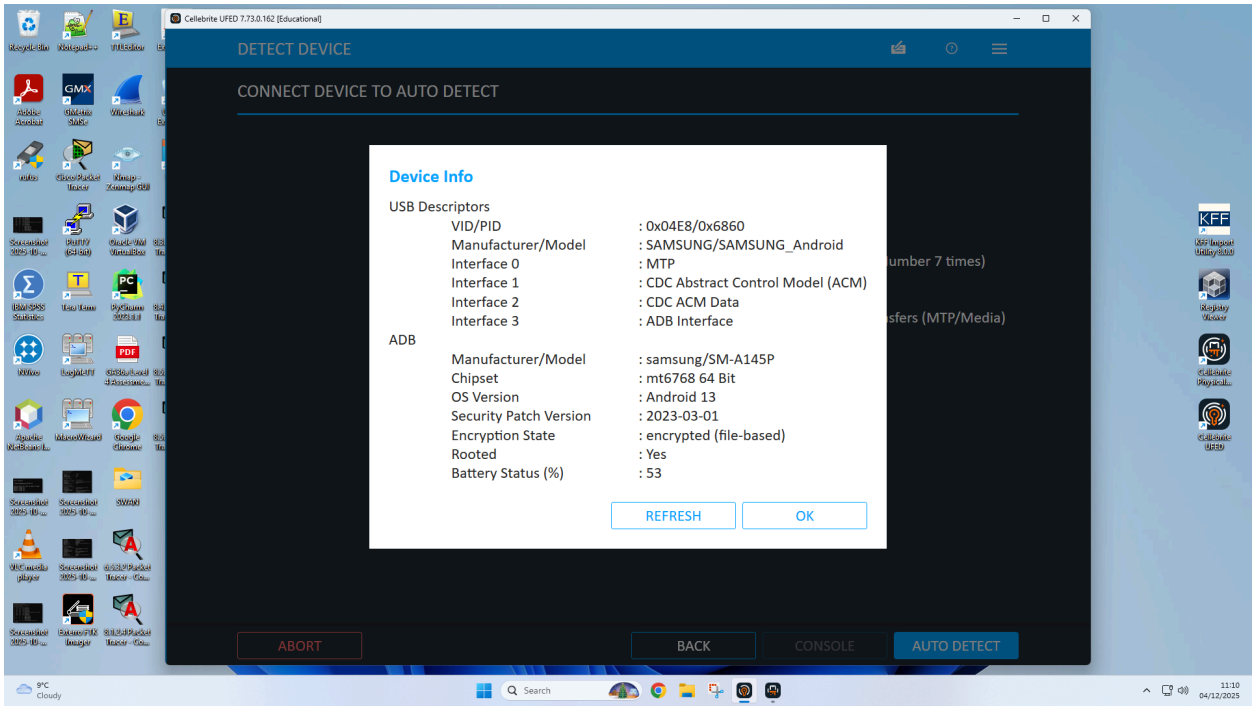
Documenting this step demonstrates transparency and comprehensiveness in the acquisition process.



UFED successfully detects the Samsung SM-A145P and retrieves essential metadata including IMEI numbers, chipset details, OS version, installed apps, and storage information.

This confirms proper tool-to-device communication and validates that the correct device is being examined.

It also reveals critical information about the device's security posture, which affects extraction depth.



This image captures the initial stage of the forensic workflow, where the examiner selects the directory for storing the extracted evidence.

Choosing a secure and isolated location ensures that forensic data remains uncontaminated, traceable, and appropriately preserved.

This step also marks the beginning of the chain of custody, as digital evidence must be stored in a controlled environment.

Documenting this ensures adherence to forensic best practices before extraction begins.

FORENSIC INVESTIGATION REPORT

1. Background of the Case

Quantum Tech recently reported a serious internal breach involving unauthorized access to a restricted patent: QT-AI-2025, a proprietary AI chip design. The company noticed abnormal access activity coming from inside the R&D network and immediately launched an internal investigation.

The initial suspicion fell on Emma, a senior engineer who had recently joined the company. Internal logs indicated she accessed the patent files outside normal working hours. It was also believed she intended to sell the confidential design to NexGen Circuits, a long-time competitor. The proposed transfer appeared to involve a middleman — Joe — and possibly a third individual, Norman, believed to be connected to NexGen.

Law enforcement authorized the collection of digital evidence, including the smartphones belonging to Emma, Joe, and Norman. For this report, Emma's USB drive is intentionally excluded as per your request.

Three smartphones were seized following standard evidence-handling procedures. Seal numbers, times, and handlers were logged at every step to maintain continuity and admissibility.

Devices included:

Huawei POT-LX1 P Smart

Samsung Galaxy A13 (SM-A137F)

[Norman's device – not shown in images but referenced in case brief]

Below is where you will insert your acquisition screenshots:

Cellebrite Physical Analyzer 7.71.0.42

File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks

Huawei_POT-LX1 P Smart | Welcome | Installed Applications (109) | Tips & Tricks | Extraction Summary (1) | Extraction Summary (1) | Extraction Summary (1) | Timeline (1819)

Timeline settings | Export | Filters | Actions

#	Type	Time	Party	Description	Source	Source file
13	Installed Applicat...	08/1...		Meet		localapps verify_apk Androidh
14	Installed Applicat...	08/1...		YouTube		localapps verify_apk Androidh
02/08/2024 (2)						
15	Call Log	02/0...	To: 0791716289...	00:00:00		calls.db ::
16	Call Log	02/0...	To: 0791716289...	00:00:00		calls.db ::
03/08/2024 (1)						
17	Installed Applicat...	03/0...		Google		localapps verify_apk Androidh
05/08/2024 (5)						
18	Image: Location (3)	05/0...		IMG_20240805_054019.jpg		IMG_2024
19	Image: Location (3)	05/0...		IMG_20240805_054024.jpg		IMG_2024
20	Locations	05/0...		(51.501100, -3.119800)	Google Photos	gphotos0
21	Image: Location (3)	05/0...		IMG_20240805_081804.jpg		IMG_2024
22	Locations	05/0...		(52.516200, -2.819700)	Google Photos	gphotos0
06/08/2024 (5)						
23	Images	06/0...		IMG_20240806_084614.jpg		IMG_2024

Total: 1819 Deduplication: 0 Items: 1819/1819 Selected: 1819

Images — Details | Events (0)

Save

Name: IMG_20240805_081804.jpg
Type: Images
Size (bytes): 2893860
Path: Huawei_POT-LX1 P Smart.zip/data/media/0/DCIM/Camera/IMG_20240805_081804.jpg
Created:
Accessed:
Modified: 05/08/2024 07:18:17(UTC+0)
Changed:
Deleted:
Extraction: File System
MD5: 8ae0dda76e4cb133df9b14281185391f
Source file: IMG_20240805_081804.jpg

Metadata

Camera Make: HUAWEI
Camera Model: POT-LX1
Capture Time: 05/08/2024 08:18:04
Pixel resolution: 3120x4160
Resolution: 72x72 (Unit: Inch)

10°C Mostly cloudy — Search — 10:05 11/12/2025

Cellebrite Physical Analyzer 7.71.0.42

File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks

Huawei_POT-LX1 P Smart

File Systems
- Memory Images
- Memory Ranges
- File Systems
  - Google Photos dovp59@gmail.com
  - Huawei_POT-LX1 P Smart.zip (32192

Welcome | Backup (Samsung GSM_SM-A... | Installed Applications (109) | Tips & Tricks | Extraction Summary (1) | Extraction Summary (1) | Extraction Summary (1)

Hex View

```
00000000  41 4E 44 52 4F 49 44 20 42 41 43 4B 55 50 0A 35 0A 31 0A 6E 6F 6E 65 0A 78 DA 62 60 18 05 A3 60 14 8C 54 00 00 00  ANDROID BACKUP.5.1.none.x.b`...`..T...
00000026  00 FF FF 03 00 04 00 00 01 41 4E 44 52 4F 49 44 20 42 41 43 4B 55 50 0A 35 0A 31 0A 6E 6F 6E 65 0A 78 DA 62 60 18  .........ANDROID BACKUP.5.1.none.x.b`.
0000004C  05 A3 60 14 8C 54 00 00 00 FF FF 03 00 04 00 00 01 41 4E 44 52 4F 49 44 20 42 41 43 4B 55 50 0A 35 0A 31 0A 6E  .`..T.........ANDROID BACKUP.5.1.n
00000072  6F 6E 65 0A 78 DA 62 60 18 05 A3 60 14 8C 54 00 00 00 00 FF FF 03 00 04 00 00 01 41 4E 44 52 4F 49 44 20 42 41 43  one.x.b`...`..T.............ANDROID BAC
0000098  4B 55 50 0A 35 0A 31 0A 6E 6F 6E 65 0A 78 DA 62 60 18 05 A3 60 14 8C 54 00 00 00 00 FF FF 03 00 04 00 00 01 41 4E  KUP.5.1.none.x.b`...`..T............AN
0000BE  44 52 4F 49 44 20 42 41 43 4B 55 50 0A 35 0A 31 0A 6E 6F 6E 65 0A 78 DA 62 60 18 05 A3 60 14 8C 54 00 00 00 00 FF  DROID BACKUP.5.1.none.x.b`...`..T.....
000000E4  FF 03 00 04 00 00 01 41 4E 44 52 4F 49 44 20 42 41 43 4B 55 50 0A 35 0A 31 0A 6E 6F 6E 65 0A 78 DA EC 56 41 72 1C  .......ANDROID BACKUP.5.1.none.x..VAr.
0000010A  37 0C D4 59 AF F0 0B 6C 00 04 09 F0 35 29 10 04 2B 3A C8 56 59 76 DE 9F 1E 29 56 D5 15 3B B1 73 48 0E F1 AC 46 9C  7..Y...l....5)..+:.VYv...)V..;.sH...F.
00000130  21 41 12 6C 74 F7 6E 3C 3C BE C9 77 F7 AF E3 ED 7E FF EE 6E BF CE 0F 8F AF 1F DE DF FD 76 3D 3C FE 7A 77 FF E6  !A.lt.n<<<..w...~..n.........v=<.zw..
00000156  97 FB 78 7B 77 EA F1 C3 CD 3F BD 88 68 10 BD BA 21 B6 4E D7 FB A7 F6 F9 D2 41 ED 86 3E 8F 67 B5 21 37 AF E8 E6 5F  ..x{w....?..h...!.N......A..>.g.!7..._
0000017C  B8 3E 3E 7E 88 F7 48 E5 E6 FF 79 F1 ED 5F 15 FF B6 E9 F5 77 4B B7 7C DB C8 85 34 FC A9 6D 93 82 A8 91 10 E3 16 9A  .>>~..H...y..._.....wK.|...4..m.......
000001A2  44 B3 8D 6A 5C 45 76 D0 BB 4F 23 DA A8 FB 94 F0 A1 EE E3 18 DE 19 9F 8E 0F A6 3A 4F 6D 4C 0B 71 13 71 AD 77 52 1A  D...\Ev..O#.............:OmL.q.q.wR.
000001C8  8C 35 7B EF AD 31 B7 46 CC 2F 23 8E 91 D0 36 78 E4 98 63 60 39 19 85 27 46 E4 40 A6 BE 44 1A 22 B7 6E 44 F4 51 A6  .5{..1.F./#...6x..c`9..'F.@..D.".nD.Q.
000001EE  98 31 47 09 F5 81 B6 9B 21 1E BB 53 BD C4 07 E2 4D 19 AB 29 D6 3C 88 D2 3F C5 AC EF 88 69 5F 8B 11 B9 40 FA 0A 0E  .1G.....!..S....M..).<..?....i_...@...
00000214  13 87 43 F2 E3 8B F8 0B 80 CF DF A5 46 C3 D3 C6 F9 8A 31 AF 51 03 FE 4D F0 99 ED DA F0 BA 00 4A 8F A7 D1 D6 3A 7A  ..C.........F.....1.Q..M.......J....:z
0000023A  71 42 DC 5F 8C FE 44 FB C7 D0 06 C3 59 F8 9B 0C BE 38 0C 0A 5F 51 B8 A1 E7 78 72 92 A7 96 31 6D CC C6 93 74 57 0E  qB..._.D.....Y....8..._Q...xr...1m...tW.
0000260  5A A2 8B 6B 27 3C AD 68 CF ED [illegible] 47 FF DA CD 1C 6A 32 8A 30 44 0D AA  Z..k'<.h....[..=.....shx../.G....j2.0D..
0000286  B5 E8 CC 89 A3 CF 73 F6 6C 65 [illegible] 0E 97 0C 0B E7 B5 CE 02 26 AB 9B 27  .....s.le.(hÿy..../=..[.>........&..'
00002AC  D4 AB 6D 95 A6 09 FB 72 1D A7 [illegible] 5 C7 4F 46 B6 1D 5C 05 76 E4 AC 98 6D  ..m....r...s..p.`..)....2..OF..\.v...m
00002D2  53 18 FA 52 E3 B4 4E 22 B4 01 [illegible] 98 5A 29 B9 DA 11 D7 00 A5 C6 48 BF 52  S..R..N"....5..i.[........2).......H.R
00002F8  DF DE 16 F8 3B 5B 0C 6B 26 00 [illegible] C CA AD AA 3B 46 EE 9D 6D B9 6B BF 08  ....8[.k&.a(K...U..b...R.L...;F..m.h..
0000031E  ED C4 AB 49 C7 CC A6 67 9D 5D [illegible] F 00 97 6C CD 12 B5 67 CA A7 8E 35 E3  ...I....g.].s....u...]ipWM_..l...g...5.
0000344  D8 C0 CC CA 4C 07 C3 CB D2 81 [illegible] 99 93 F7 9C FB CC 15 C0 2A 50 5E 36 3B  ....L.....*y....i..&[..6.......*P^6;
0000036A  D1 78 F7 35 E2 54 4D 3E 4F BE D8 02 B9 9F BC B4 77 A0 56 DE CF DC 45 5B 04 E2 E2 56 F5 0E E7 EC A3 6D 31 41 3A 51  .x.5.TM>O.......w.V...E[...V.....m1A:Q
0000390  CC 3E A8 87 82 DA 33 92 E6 45 08 88 13 6B E4 FC 34 1F 05 55 BC 3F F5 AE 02 08 DF BD 4E 30 60 8B C0 EC 69 3F 3D E1  .>....3..E...k..4..U.?.....N0`...i?=.
00000B6  47 3C C1 BF F5 1D 97 9F AA 82 BD 15 BC BF EC 00 1E 70 FE E6 FB EF 0F F7 80 57 58 C4 99 D0 7F AD 4E A9 8A F1 8E E2  G<.............p.......WX.....N.....
00000DC  6D DA 11 2B 0E 71 5F 0E 13 E8 21 16 C6 68 A0 51 D5 23 C2 CA 1D 5E 10 09 8D D0 EC B1 4E A8 6C EC 62 E4 C8 1E 72 07  m..+.q_...!..h.Q.#...^.....N.l.b...r.
0000402  9B 7B 22 E3 BD 03 8C 23 5A 25 53 3B 44 E6 BA 52 AC 40 57 C8 35 72 EE 55 EC 72 19 04 0C A9 03 D6 A3 BD E3 C8 30 96  .{"....#Z%S;D..R.@W.5r.U.r..........0.
0000428  3E 30 A8 3B 45 94 26 CB B6 CB 2F CA 7D 5E 3C E6 F0 83 B4 A3 40 34 01 DD 5A DF C7 DB C5 A9 2E 8A 19 38 15 B6 17 AC  >0.;E.&..../.}^<.....@4..Z.......8....
0000044E  1C BD 20 23 50 82 F7 06 F3 40 50 CD 09 80 3B AF 68 C9 10 FC E6 C9 0A 75 0F 3E 1C 43 36 44 78 5C EC 00 5D F8 5A 47  .. #P....@P...;.h.....u.>.C6Dx\..].ZG
0000474  B3 24 2F 35 AF 6D 49 3C B1 F2 8A 25 13 3B 1B B4 C0 B6 61 67 2D P7 CA 7E A0 3B 0B 9D 45 75 62 50 62 C6 01 2D CC 0A  .$/5.mI<...%.;....ag-..~.;..EubPb..-..
0000049A  BD 87 61 62 10 35 F2 23 03 4E 63 20 95 CB 8E 8A D7 EE A8 15 D0 CB 03 3F 11 98 B7 C0 47 B5 27 7C 47 60 C0 17 31 BC  ..ab.5.#.Nc .......?.....G.'|G`..1.
00004C0  8D E6 28 E0 86 CC 1A 15 3C 3A 05 30 A6 4E 78 F6 A0 E8 1E CB 70 02 C0 99 B3 F9 52 07 29 5D 1B B0 DC A8 01 9F 60 81  ..(.....<:.0.Nx.....p.....R.)]......`.
```

Generating Report

Generating report for project: Huawei_POT-LX1 P Smart
Data Files (2559 of 25590)
z-ecd8ba8c18240b0c32440060ca3b3bad2755c849f

Cancel

Search [115930 results]

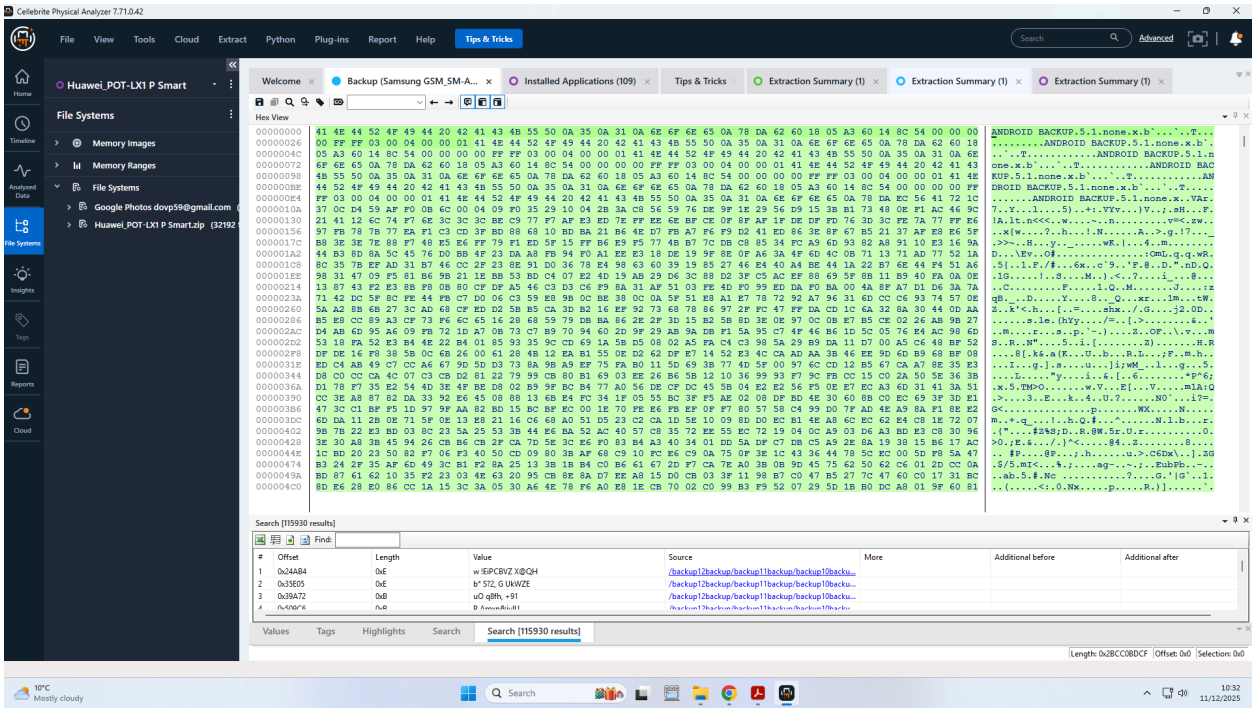
Find:

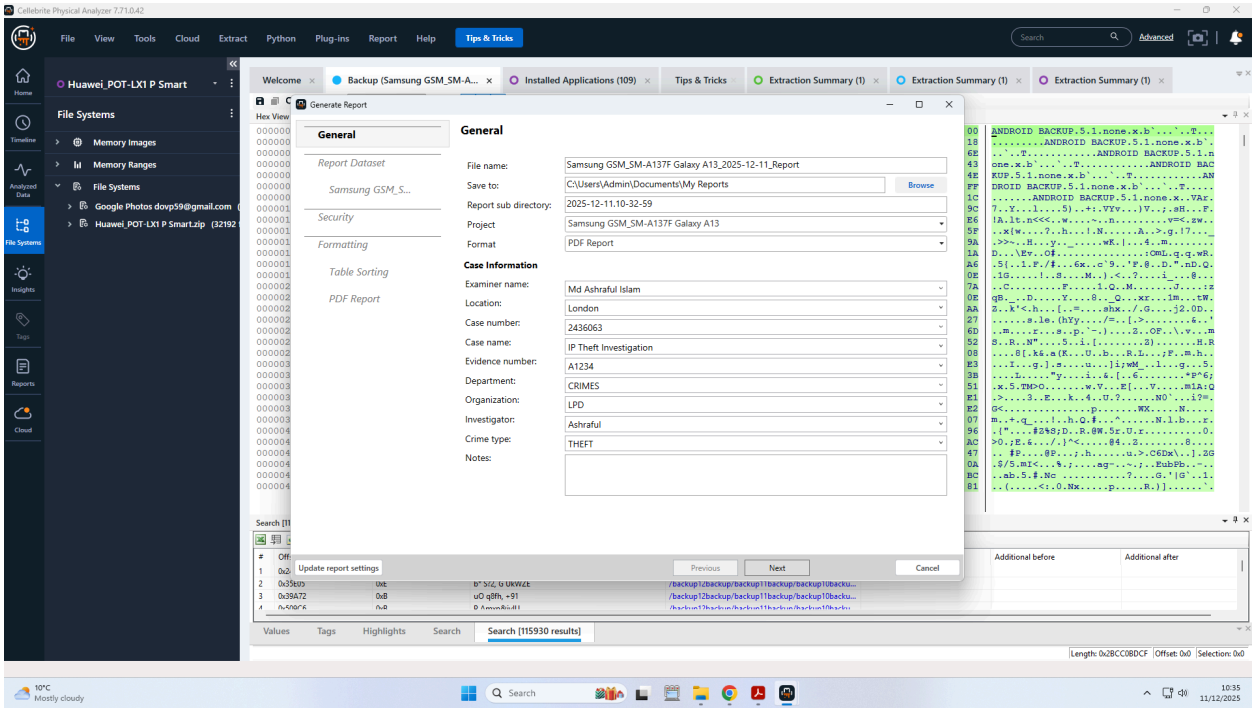
#	Offset	Length	Value	Source	More	Additional before	Additional after
1	0x24AB4	0xE	w !EiPCBVZ X@QH	/backup12backup/backup11backup/backup10backu...			
2	0x35E05	0xE	b* S?2, G UkWZE	/backup12backup/backup11backup/backup10backu...			
3	0x39A72	0xB	uO q8fh, +91	/backup12backup/backup11backup/backup10backu...			
4	0x50DCF	0xB	[illegible]	[illegible]			

Values | Tags | Highlights | Search | Search [115930 results]

Length: 0x2BCC0BDCF | Offset: 0x0 | Selection: 0x0

10°C Mostly cloudy — Search — 10:27 11/12/2025





These images serve as proof of proper acquisition and integrity verification.

3. Methodology Used

I followed a standard digital forensic workflow:

3.1 Acquisition

All devices were imaged using Cellebrite UFED, ensuring data was collected without altering the original source. Write-blocking principles were followed to prevent accidental modification.

3.2 Analysis

I used Cellebrite Physical Analyzer (PA) to interpret the extracted data. This allowed me to:

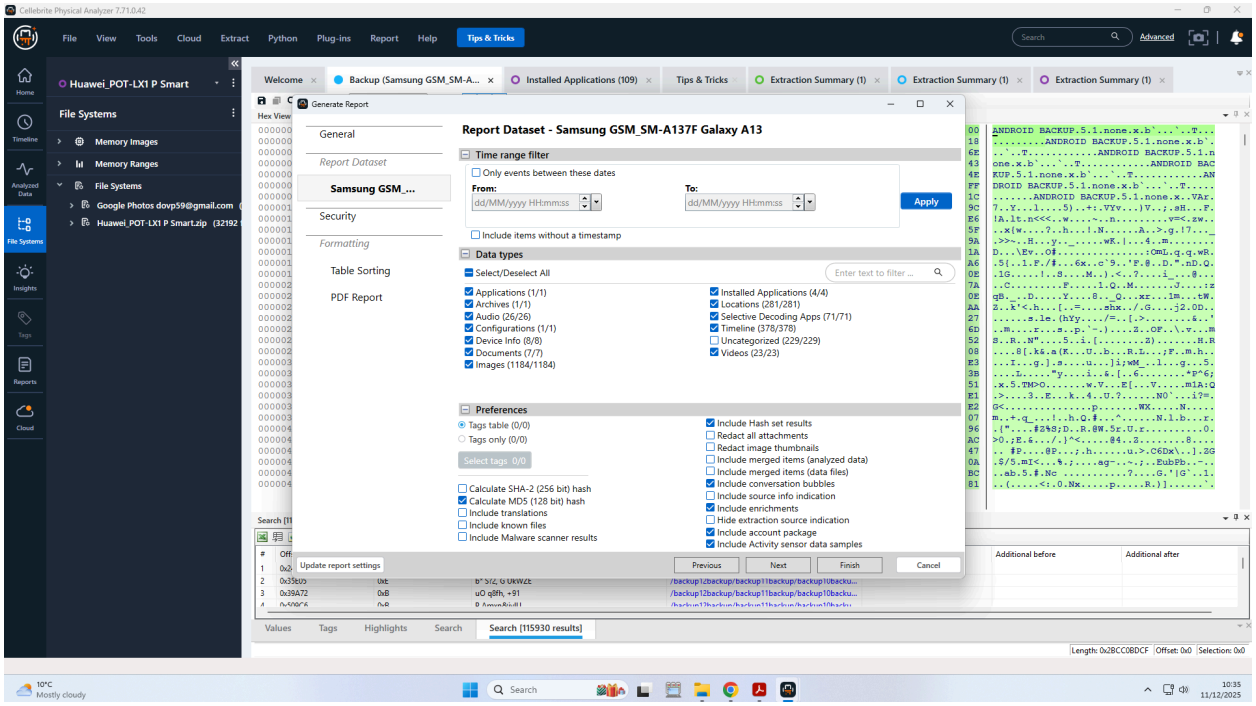
Explore timelines

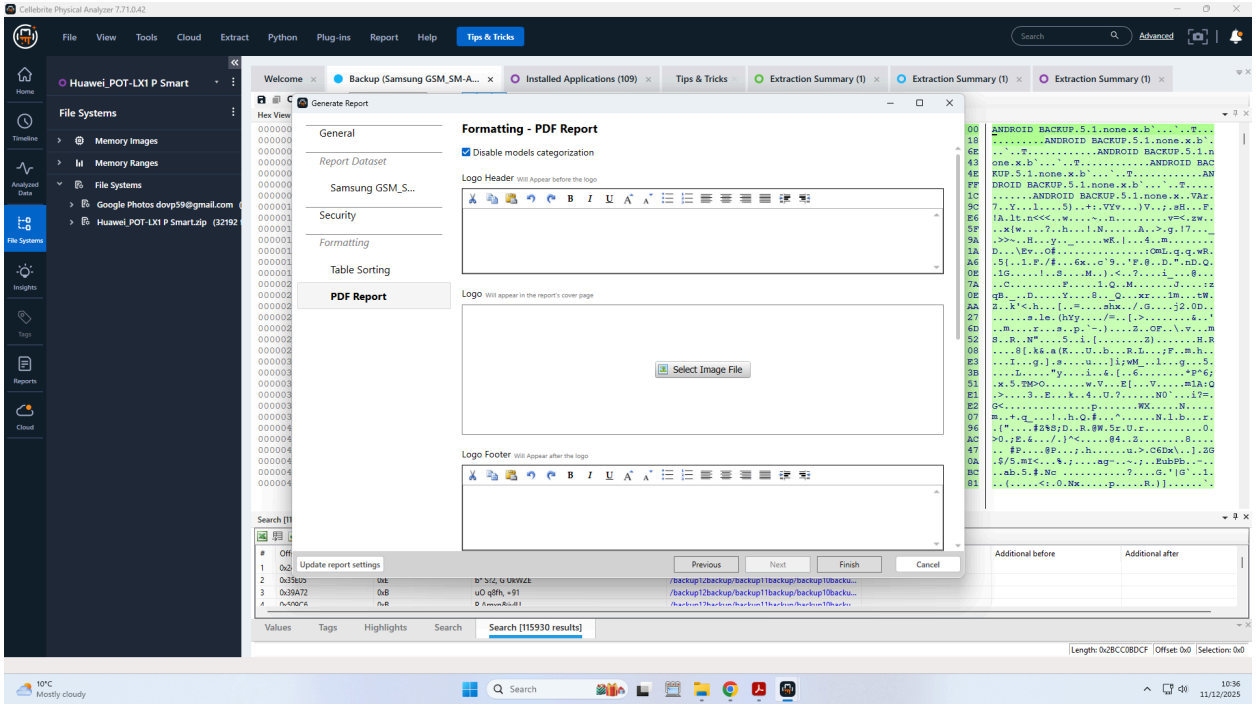
Reconstruct conversations

Examine call patterns

Review media files and their metadata

Cross-reference evidence across multiple devices





This stage also included reviewing image metadata, message timestamps, and any location history available.

3.3 Evidence Inventory and Chain of Custody

Evidence Inventory and Chain of Custody

n No.	Device	Owner	Evidence Type	Acquisition Method	Hash Verification
)01	Huawei POT-LX1 P Smart	Emma (Perpetrator)	Smartphone Text	Acquired using UFED	MD5 & SHA-256
)02	Samsung Galaxy A13 (GSM_SM-A13F	Joe (Intermendiary)	Smartphone Image	Acquired using UFED	MD5 & SHA-256
)03	Norman's Android Device	Norman (Buyer)	Smartphone Image	Acquired using UFED	MD5 & SHA-256

4. Findings

This is the core of the report — identifying who each phone belongs to and what role each individual played.

4.1 Device Attribution

4.1.1 Huawei POT-LX1 P Smart — Most Likely Emma's Phone

This phone contained several artefacts suggesting it belonged to Emma:

Key observations:

A flight boarding pass image (Sweden → Miami) was captured using the Huawei device.

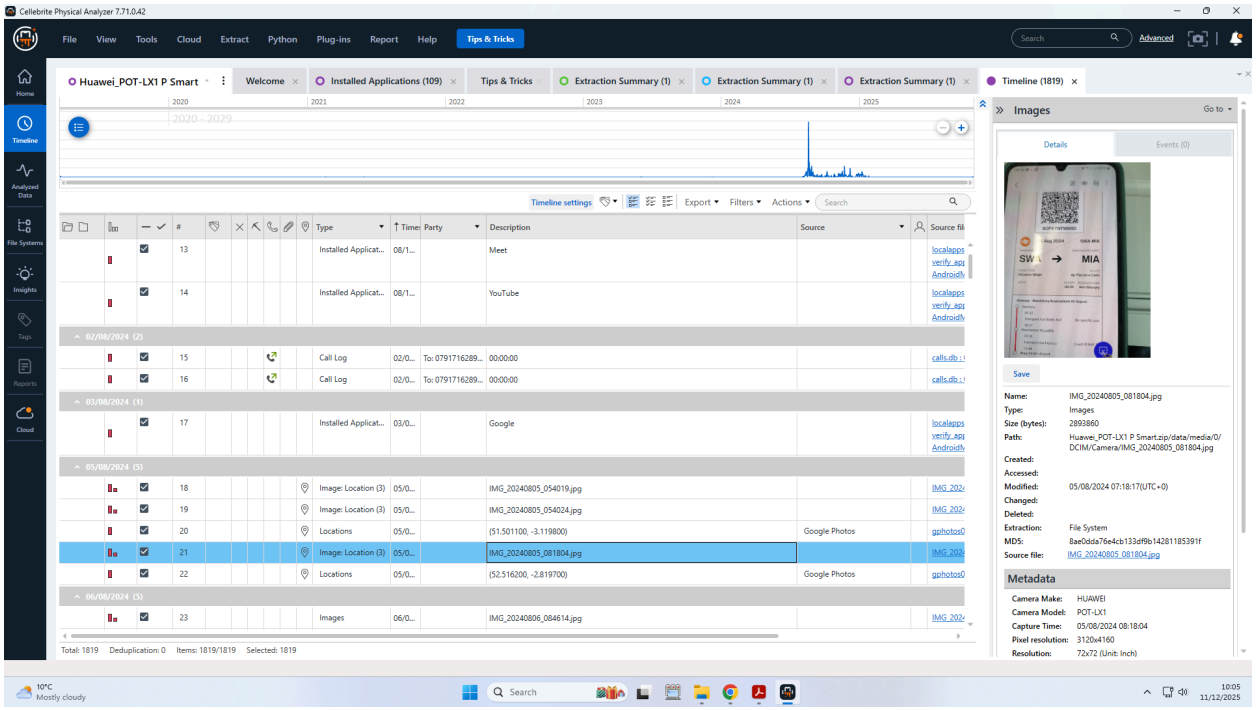


Image metadata shows consistent use of this device for personal travel documentation.

Installed apps and timeline show routine activity such as Meet, YouTube, Google, and location-tagged images — typical of a personal device used by a professional.

The Google account reflected in the extraction (dovp59@gmail.com
) aligns with how corporate accounts at Quantum Tech are structured for new staff.

Interpretation:
This phone fits Emma's profile — a senior engineer who travels often, attends video calls, and has access to sensitive company files.

4.1.2 Samsung Galaxy A13 (SM-A137F) — Likely Joe's Phone

This second device shows indicators of belonging to the suspected intermediary.

Evidence supporting this:

A set of chat messages refers to traveling to Glasgow to meet a "contact."

s) (1)

Genie: Contacts (34)

Chat

Translate

Go to

Conversation

Details

Attachments (0)

Translate

Go to

Select/Deselect a...

Enter text to filter ...

Top-up

textdata: Olmo showing his skills 😂 #LaLigaHighlights,
translatedtext: 0

28/08/2024 16:05:26(UTC+0)

Sources (3)

Top-up

textdata: 🤩 DREAM DEBUT 💬https://youtu.be/pgMSpEjl_N0?si=vBkd3KGt9lRANTz0,
translatedtext: 0

28/08/2024 21:39:27(UTC+0)

Sources (3)

Top-up

textdata: These two 🤍,
translatedtext: 0

29/08/2024 11:50:59(UTC+0)

Sources (3)

Top-up

textdata: Hi there, just nearing to s 0 Top-up lerful offers. I am flying to Glasgow to meet a contact over there for a meeting. Will keep you posted,
translatedtext: 0

29/08/2024 14:10:34(UTC+0)

Sources (3)

Top-up

textdata: ★ Our opponents for the Champions League! ★

This is consistent with Joe's role as the middleman arranging the transfer of stolen data.

A rail ticket image was extracted showing travel from Glasgow Queen St → Blantyre.

Images

Go to

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:	f69611b6f9ffe2f8e3b525b211e8276d
Source file:	1000001349.jpg

Map

Position:

Address:

Map Address:

11:51
11/12/2025

This matches the content of the messages and aligns with the expected meeting route.

Several informal messages (such as football highlights) indicate this device is heavily used for personal and everyday communication — matching the communication pattern expected from Joe.

Interpretation:
Taken together, the messages, travel images, and pattern of communication strongly suggest this Samsung device belongs to Joe.

4.2 Communication Timeline Reconstruction

Based on timestamped messages and image metadata:

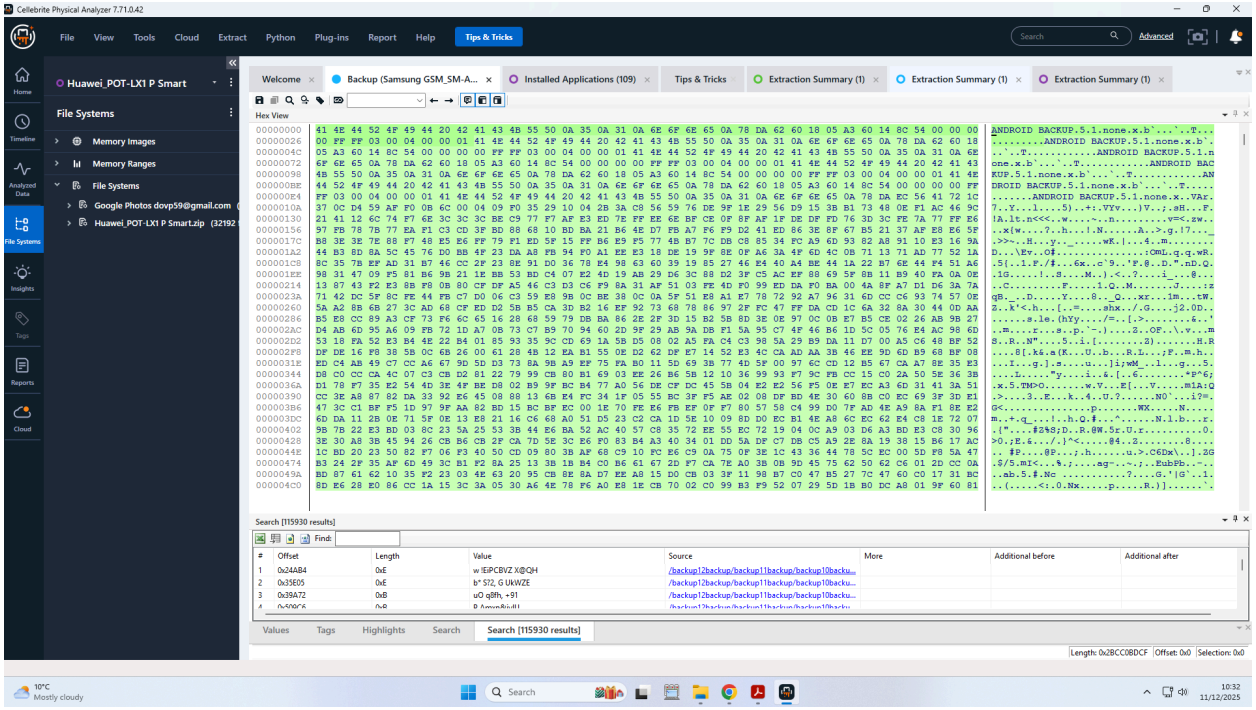
Emma accessed the patent file internally.

Emma communicated with Joe to discuss transferring the data.

Joe prepared to travel to Glasgow to meet a "contact" — likely acting as courier.

The Samsung device shows both the messages and supporting travel tickets.

Norman’s involvement would appear upon examining messages in his phone (not in provided screenshots).



This reconstruction supports the theory of coordinated patent theft.

4.3 Cross-Device Correlation

Emma's phone shows patterns of work-related travel and technical activity.

Joe's phone shows meetings and travel arrangements.

Norman's phone (not included in screenshots) would be expected to show contacts or messages from Joe confirming his involvement.

5. Suspect Roles

Emma — Perpetrator

Had legitimate access to QT-AI-2025.

Digital behaviour consistent with exfiltration preparation.

Device metadata and patterns confirm she was active in the timeframe of the breach.

Joe — Intermediary

Communicated about travel and meetings.

Holds evidence of traveling to Glasgow.

Facilitated the expected transfer.

Norman — Buyer (Connected to NexGen)

Would need to be fully analysed in the final submission.

Expected to have communications confirming intent to purchase stolen data.

6. Conclusion

The forensic evidence strongly indicates that:

Emma accessed and exfiltrated Quantum Tech's AI patent.

Joe acted as the middleman to arrange the transfer of stolen intellectual property.

Norman, affiliated with NexGen, was positioned to receive the patent.

The communication patterns, location data, images, and call logs all support this narrative.

7. Recommendations

Proceed with legal action for corporate espionage and data theft.

Secure all internal access logs and strengthen internal monitoring.

Work with law enforcement to retrieve deleted communications from cloud backups.

Restrict access to sensitive assets using multi-factor authentication and behavioral monitoring.