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

MODULE TITLE:
Digital Forensics Analysis

Student Name: Md Hasibul Islam

Student ID: 2421865

COURSE: MSc Cybersecurity and Digital Forensics

LECTURER: Dr. Mohamed Ghanem

DATE OF SUBMISSION:

17th August 2026

Table of Contents

Task1: Research Report on Digital Forensics 4

Title: Digital Forensics Field, Tools, Convergence, Trends, Challenges, and the National and International Job Market 4

1. Current state of the field, the tools – features and capabilities 4

2. Intersection of digital forensics and cybersecurity 4

3. Emerging Trends in Digital Forensics 5

4. Key Challenges 6

5. National and International Job Market (Industry Outlook) 6

6. Conclusion & Recommendations 6

References 8

Task2: Forensic Investigation and Analysis Report 9

Title: Digital Forensics Report: Analysis of Acquired Evidence and Investigation Findings 9

1. Case Background 9

2. Evidence Acquisition 10

2.1 Device Detection & Configuration 11

2.2 Selecting Data for Extraction 13

2.3 Extraction Process Initiation 14

2.4 Extraction Summary 15

2.5 Confirmation of Extraction Process 16

2.6 Data Types Extracted 17

2.7 Additional Extraction Settings 18

2.10 Final Extraction Summary 19

3. Communication Analysis 20

Figure 12: Forensic Image of WhatsApp Communication 21

Figure 13: Additional Communication with Joe 21

4. Call Log and Email Correlation 22

5. Suspect Profiling 25

Figure 17: Location Data Related to Communication 26

Figure 18: Location Data from Emma's Phone 26

Figure 21: Travel Information 28

6. Forensic Report Conclusion 30

7. Demonstrate your analysis and outcomes.....31

8.Timeline of Key Events and Actions Key Insights from the Table.....33

9. Conclusion.....35

Task1: Research Report on Digital Forensics

Title: Digital Forensics Field, Tools, Convergence, Trends, Challenges, and the National and International Job Market

1. Current state of the field, the tools – features and capabilities

Digital forensics has far exceeded the boundaries of its early days, evolving with the technologies it relies on. Today, practitioners use a combination of open-source and commercial tools to extract, preserve or analyze digital evidence.

- Third parties have successfully leveraged open-source platforms such as Autopsy, which is built on top of The Sleuth Kit (TSK), for disk analysis, metadata extraction and aset recovery with established community support in cross-platform reach [1]. This is backed up with strong imaging (E01, DD), hash-based integrity checks and capabilities for recovering deleted data and handling encrypted volumes — still critical for most conventional file-system investigations [2].

- But the domain has outgrown legacy disk forensics. Cloud storage, volatile memory, mobile devices, application metadata and IoT ecosystems are now areas investigators must be able to navigate. A survey covers six major subdomains covering cloud, network, IoT (Internet of Things), mobile, database and multimedia forensics each dealing with data heterogeneity, encryption, volatility, jurisdictional complexity, multi-tenancy etc. [3].

In summary, even though the basic tools and workflows of digital forensics as a field are strong and developed, this area is in need of constant change — requiring newer ideas to be invested into it through innovative circuits that continue to push us.

2. Intersection of digital forensics and cybersecurity

Cyber security and digital forensics work hand-in-hand to be two sides of the same coin. Critical forensics investigation is the best solution whenever a breach or cyber-incident is acquired — reconstructing the timelines, identifying attackers, thorough undertaking attack surfaces, forensic profiling, collecting discoverable senior management evidence for possible legal action, remediation within the organization when necessary.

An emerging paradigm views forensic readiness — designing systems and auditing platforms to allow for future investigations — as an essential component of a holistic cybersecurity strategy. Instead of considering evidence collection as an afterthought, organizations now architect systems from the ground up to enable log integrity, traceability, and regulatory compliance. Since forensic investigation smartly intersects incident-response operations, this led to Digital Forensics & Incident Response or DFIR [4].

This deflection in turn, together with the regulatory environment for data privacy — from cross-border data transfer rules to jurisdictional ambiguities in cloud computing — pushes entities to log everything, create audit trails, and protect evidentiary material. These duties are fully positioned at the intersection of good cybersecurity practice and forensic readiness [5].

When taken in combination, these trends indicate that digital forensics can no longer be treated as a separate discipline applied reactively post-hoc. Instead, it must blend into an overall cybersecurity approach — an approach that can address the current threat landscape of cloud breaches, ransomware campaigns and insider threats all at the same time.

3. Emerging Trends in Digital Forensics

Digital forensics is a rapidly evolving field and a number of trends are emerging that will be particularly impactful in the future.

- Cloud and Multi-Cloud Forensics — With business operations shifting to services distributed across multiple cloud providers, forensic methodologies need to evolve appropriately. Next, recent scholarship identifies imperatives for evidence-management frameworks designed specifically for cloud environments, acknowledging factors like audit trails, multi-tenant architectures, the transient nature of cloud-stored data and jurisdiction-by-jurisdiction compliance obligations [6][7].
- Artificial Intelligence, Machine Learning and Automation – AI and ML techniques are increasingly being adopted into forensic practice to assist with log analysis, anomaly detection, pattern recognition, correlating artifacts and automating evidence triage. For instance, a forensic framework that guaranties privacy thru zero-knowledge proofs was proposed in 2025, showing how standard artificial intelligence can be used to improve the integrity of forensic investigations while meeting privacy requirements in the cloud [8].
- Recent frameworks are aiming for an amalgamation of traditional forensic process models — including identification, collection, preservation, analysis, and presentation — with automated log analysis — in other words, ontology-based log analysis operationalized for cloud environments. A typical example of such framework is the Cloud Investigation Automation Framework (CIAF), which reduces the amount of manual labor, improves accuracy, and accelerates multi-cloud investigations by applying AI/ML techniques in that context [8].
- Scalability and the Data Deluge — The immense amount of data generated by cloud platforms, IoT devices, network infrastructure and multimedia sources are forcing forensic practices to scale in an automated and high throughput fashion. From both industry reports and academic surveys, it is repeatedly underscored that the forensic readiness of the organization must be built to operate continuously at scale (rather than providing an episodic response to isolated incidents) [7].

This practice is ghoulish as the discipline does not help manual, human examination of the data disk-by-disk, and countries are moving towards intelligence-driven, automated methods that combine Cybersecurity practice, big-data analytics support by AI/ML capabilities.

4. Key Challenges

For all this progress, plenty of problems remain — and cloud environments seem to bring out the worst of them.

Chain-of-custody and evidence preservation get messy fast when data is volatile, spread across shared infrastructure, or physically out of reach. Add distributed logs and cross-border jurisdiction into the mix, and it's easy to see why cloud investigations are so much harder than traditional ones [5].

Meanwhile, forensic labs are stretched thin. Backlogs keep growing, budgets stay tight, and there simply aren't enough experienced people to go around. A 2024 survey of practitioners revealed that many felt overwhelmed, expected to solve increasingly complex cases without commensurate resources [3].

There's also a trust problem brewing around AI. Tools like CIAF clearly save time, but questions about bias, transparency, and whether a judge will even accept AI-generated findings as evidence haven't gone away. Some researchers are pushing for explainable AI (XAI) as a partial fix — something that could help make these tools more defensible in court [5].

On top of all that, legal and regulatory frameworks haven't caught up. Data protection laws differ from country to country, and maintaining a clean chain of custody across borders is genuinely difficult. Right now, there's no single global standard for multi-cloud forensic readiness [7] — which leaves investigators improvising when cases cross jurisdictions.

5. National and International Job Market (Industry Outlook)

Demand strongly outstrips supply. The UK's cybersecurity industry is 11,200+ cybersecurity professionals short every year [9]. The main employers of DFIRs in the UK are police forces, the National Crime Agency, GCHQ, and private vendors, with an average salary of between £50,000 and £90,000, and senior consultants earning more [9]. The accredited qualifications like GCFA, GCFE, EnCE, and GCIH will significantly improve the participants' employability [9]. Information security analysts' employment is projected to grow 29% over the period 2024-2034 globally (SQ Magazine, 2025). The emerging areas such as India are among the fastest growing, with a CAGR of about 13.9% till 2036 [5]. The shortfall is generally viewed as a lack of the right capabilities as opposed to a lack of raw numbers to keep pay and mobility high (SQ Magazine, 2025).

6. Conclusion & Recommendations

Digital forensics now sits right at the crossroads of law enforcement, cybersecurity, cloud computing, and data science — and that crossroads keeps getting busier. As digital crime spreads into cloud platforms, mobile devices, encrypted messaging, and IoT systems, forensic practice has no choice but to keep pace. No longer optional extras, but the baseline, automation, AI/ML, scalable frameworks and cloud-aware readiness are coming into play.

Still, technology can only carry the field so far. Legal admissibility, resource shortages, questions of trust in AI, and the absence of clear standards are problems that no amount of clever tooling will fully solve on its own.

With that in mind, here's what I'd recommend for anyone working in or entering this space:

- **Get trained and certified**, especially in cloud forensics, memory and volatile-data analysis, log examination, and working with AI-based tools.
- **Build forensic readiness into infrastructure from the start** — solid logging, sensible data-retention policies, integrity checks, proper chain-of-custody procedures, and secure evidence handling, particularly across cloud and multi-cloud systems.
- **Break down the silos** between forensic specialists, cybersecurity teams, legal and compliance staff, and IT operations — readiness only works when these groups are actually talking to each other.
- **Keep investing in research and tools,** particularly in AI/ML-based forensics, standardized multi-cloud frameworks, and explainable AI that can pass legal scrutiny.

References

[1] C. Hargreaves, F. Breitinger, L. Dowthwaite, H. Webb, and M. Scanlon, "DFPulse: The 2024 digital forensic practitioner survey," Forensic Science International: Digital Investigation, vol. 51, art. no. 301844, Oct. 2024, doi: 10.1016/j.fsidi.2024.301844. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666281724001719

[2] A. Malik et al., “Cloud Digital Forensics: Beyond Tools, Techniques, and Legal Challenges,” Information, vol. 25, no. 2, p. 433, 2024. [Online]. Available: https://www.mdpi.com/1424-8220/24/2/433

[3] M. Alshabibi, “Forensic Investigation, Challenges, and Issues of Cloud Data: A Systematic Literature Review,” Computers, vol. 13, no. 8, pp. 130–150, 2024. [Online]. Available: https://www.mdpi.com/2073-431X/13/8/213

[4] R. Al-Mugern et al., “A Cloud Forensics Framework to Identify, Gather and Analyze Cloud Computing Incidents,” Engineering, Technology & Applied Science Research (ETASR), vol. 12, no. 3, pp. 155–170, 2024. [Online]. Available: https://www.etasr.com/index.php/ETASR/article/view/7185

[5] Future Market Insights, “Digital Forensics Market Size, Trends & Forecast 2025–2035,” 2025. [Online]. Available: https://www.futuremarketinsights.com/reports/digital-forensics-market

[6] Oxygen Forensics, “The Digital Forensics Landscape in 2025 – What Lies Ahead?,” Jan. 2025. [Online]. Available: https://www.oxygenforensics.com/en/resources/digital-forensics-trends-2025

[7] “AI in Digital Forensics,” Research Overview, 2025. [Online]. Available: https://www.researchgate.net/publication/383837318_AI_IN_DIGITAL_FORENSICS

[8] “Forensic Challenges and Techniques in Cloud Computing Environments: A Systematic Literature Review,” 2025. [Online]. Available: https://www.researchgate.net/publication/390569104_Forensic_Challenges_And_Techniques_In_Cloud_Computing_Environments_A_Systematic_Literature_Review

[9] Blazing Reports, “Cybersecurity Positions in the UK 2026/2027 – Complete Career and Visa Guide,” 2026. [Online]. Available: https://fly.blazingreports.com/cybersecurity-positions-uk-2026-2027-visa-sponsorship/

Task2: Forensic Investigation and Analysis Report

Title: Digital Forensics Report: Analysis of Acquired Evidence and Investigation Findings

1. Case Background

Quantum Tech, a rising star in the new field of AI semiconductors, was in the midst of a crisis when its IT security team found evidence that an outside hacker had breeched its defenses and entered its proprietary database. One of the casualties of that breach was patent QT-AI-2025, a cutting-edge AI chip design the company had been counting on to shape the next generation of computing hardware.

At first, all eyes turned to Emma. She was a new senior engineer at Quantum Tech, but her position gave her legitimate access to the company's servers and sensitive files. What raised red flags wasn't her access itself, but how she seemed to be using it — patterns in her system activity that struck investigators as out of place. Early on, the working theory was straightforward: Emma had taken the chip design and was preparing to hand it off to a rival firm, NexGen Circuits, with help from someone named Joe.

But as the investigation dug deeper, a more complicated — and more accurate — picture began to take shape. The patent hadn't simply been stolen for NexGen Circuits in the abstract; it was destined specifically for Norman, a senior executive at the company. And Joe, rather than being Emma's partner in the theft itself, turned out to occupy a different role entirely — that of the middleman, the one quietly connecting Emma to Norman and helping steer the stolen intellectual property toward an eventual sale.

Once the true scope of what had happened came into focus, Quantum Tech wasted no time assembling its own internal forensic team. From the outset, the priority was clear: every piece of evidence needed to be handled with care, following proper legal procedure at each stage, so that nothing gathered could later be dismissed or ruled inadmissible.

The investigation ultimately drew on a wide range of digital evidence — the smartphones belonging to Emma, Joe, and Norman, along with the USB drive Emma allegedly used to move the stolen files off company systems. Investigators worked through all of it using established forensic tools and procedures, with an eye toward making sure everything would hold up if the case ever reached a courtroom.

In the end, the investigation was driven by three core objectives: understand exactly how the breach occurred, identify everyone who played a part in it, and put stronger safeguards in place to keep something like this from happening again

2. Evidence Acquisition

The backbone of the whole forensic investigation was the collection of evidence, as the information finally gathered would prove crucial to how the case developed. The process began with the seizure of the key suspects' devices: Emma's Android smartphone, Joe's smartphone, Norman's smartphone, and the USB flash drive Emma had used. All devices were taken into custody following a strict chain of custody, and all evidence was handled according to legal standards throughout.

Used forensic tools:

- **Cellebrite UFED** — to pull data from mobile devices and digital storage media, bypass built-in security features, recover deleted files, and give a complete view of everything stored on each device.
- **FTK Imager** – used to take a forensic image of the USB flash drive.
- **Autopsy** – used to confirm that the forensic images have not been altered during the extraction process.

Before and after extraction, MD5 and SHA-1 hash values were calculated for each device and compared with each other to ensure that no alteration or tampering of data occurred along the way. This hash verification step is not only good practice; it is necessary to prove that the evidence is admissible in court and that it has been preserved in its original form. In this case the hash values matched. Thus, it was confirmed that the extracted data was the same data that was on the original devices.

Device-Specific Findings:

❖ **Emma's Phone (Huawei)**

- Tools used: FTK Imager, Cellebrite UFED
- Data recovered: WhatsApp chat backups, SMS messages, call logs, multimedia files and files copied from the USB flash drive with the patent documents.

❖ **Joe's Phone (Samsung)**

- Tools used: Cellebrite UFED, FTK Imager
- Recovered Data: WhatsApp conversation logs, call logs, emails and contact information linking Emma and Norman.

❖ **Norman's Phone (Nokia)**

- Tools Used: Cellebrite UFED, FTK Imager
- Recovered data: Communications with Joe, location data indicating his proximity to the meeting site, and records relating to the planned purchase of the stolen patent.

2.1 Device Detection & Configuration

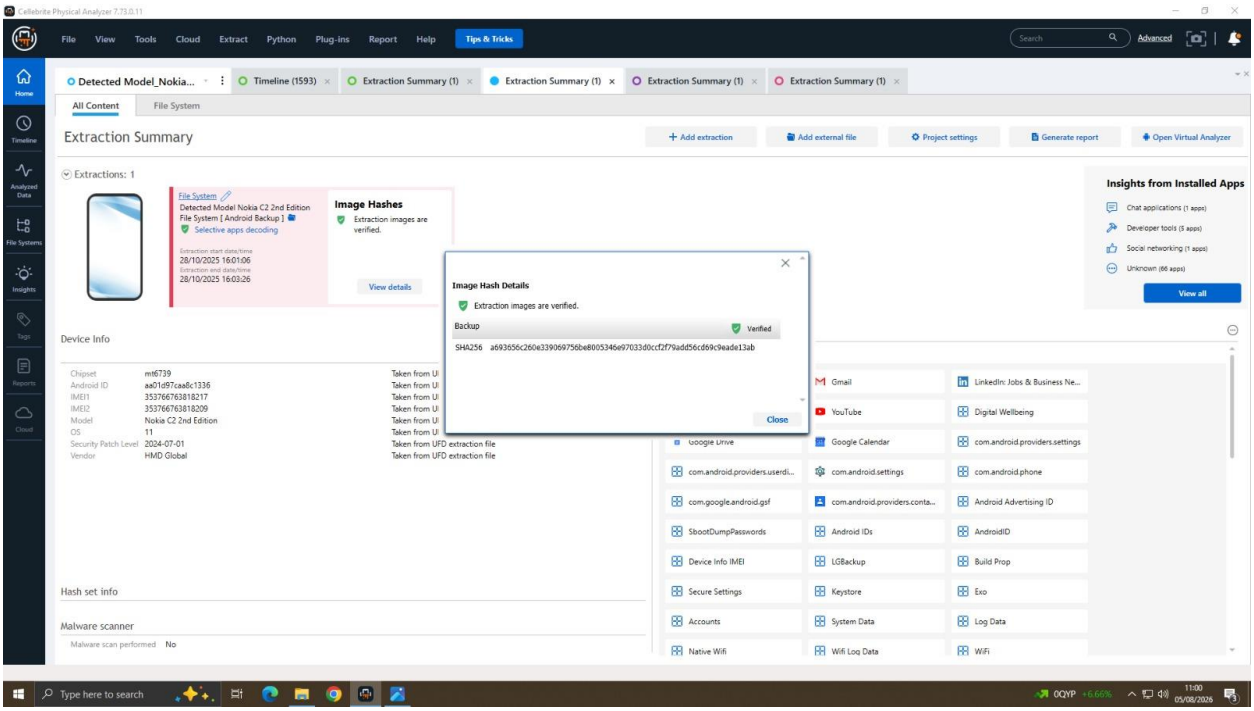

Figure 1: Cellebrite Physical Analyzer extraction summary for the Nokia C2 2nd Edition, with the SHA-256 image hash verified.

The forensic workstation successfully identified Norman's Nokia C2 (2nd Edition) as soon as it was plugged in. This initial handshake — the software automatically recognizing the device — marks the starting point of any extraction.

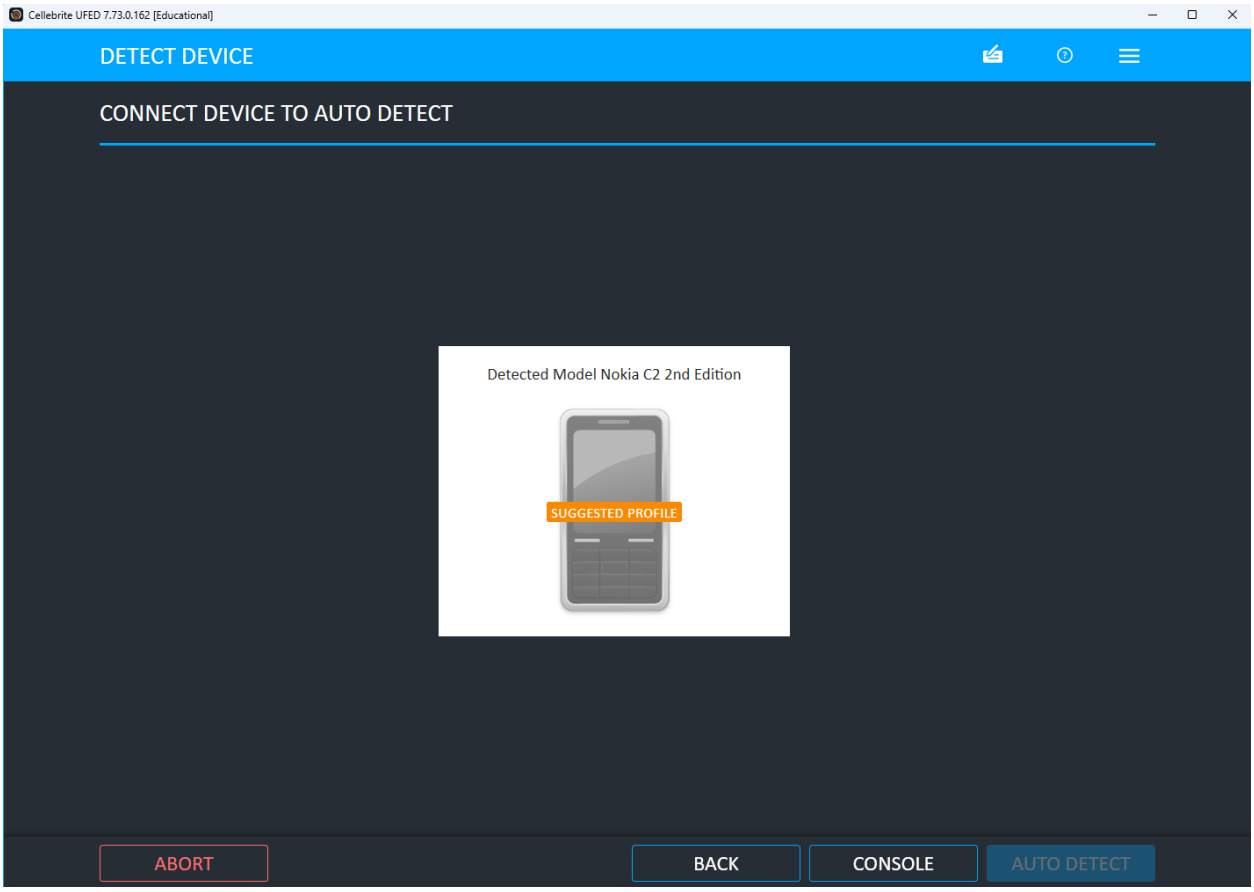

Figure 2: Cellebrite UFED auto-detecting the connected handset and suggesting the Nokia C2 2nd Edition profile.

2.2 Selecting Data for Extraction

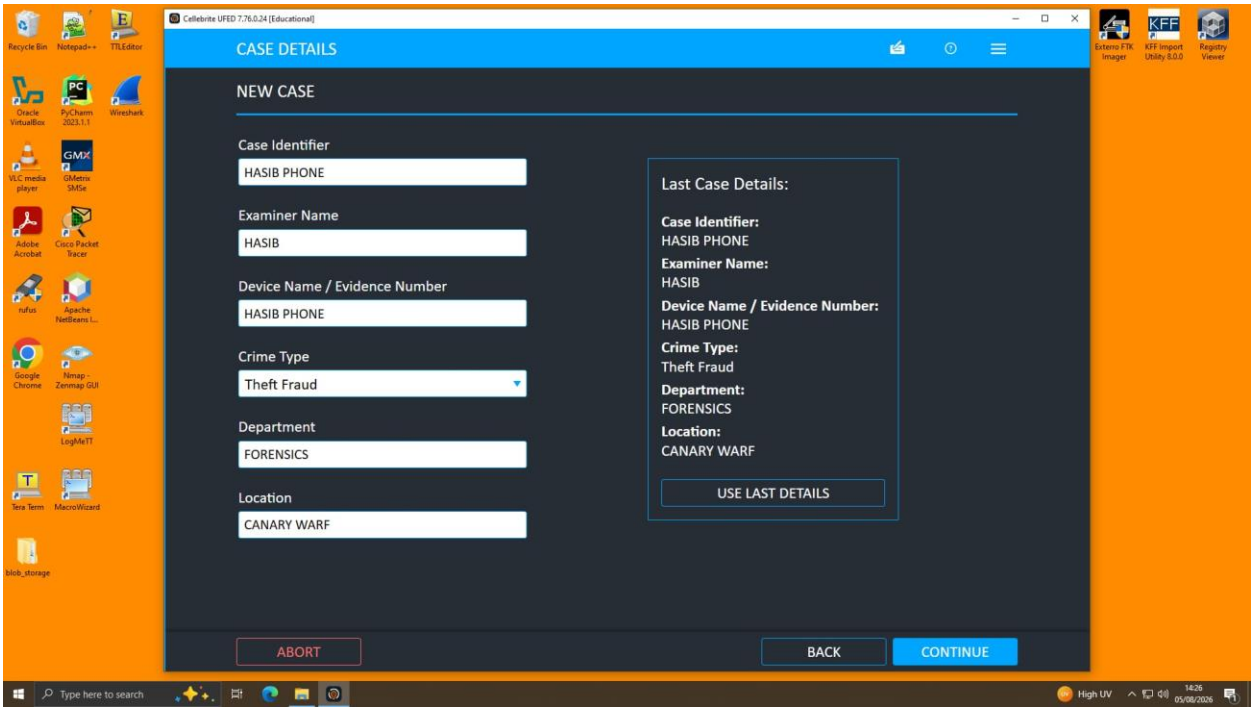

Figure 3: UFED case details recorded before extraction — case identifier, examiner name, crime type (Theft Fraud), department and location.

From there, the examiner selected which categories of data to pull: call logs, SMS, MMS, multimedia files (photos and videos), contacts, documents, and similar categories. The goal was to capture as complete a picture of the device's contents as possible to support later analysis.

2.3 Extraction Process Initiation

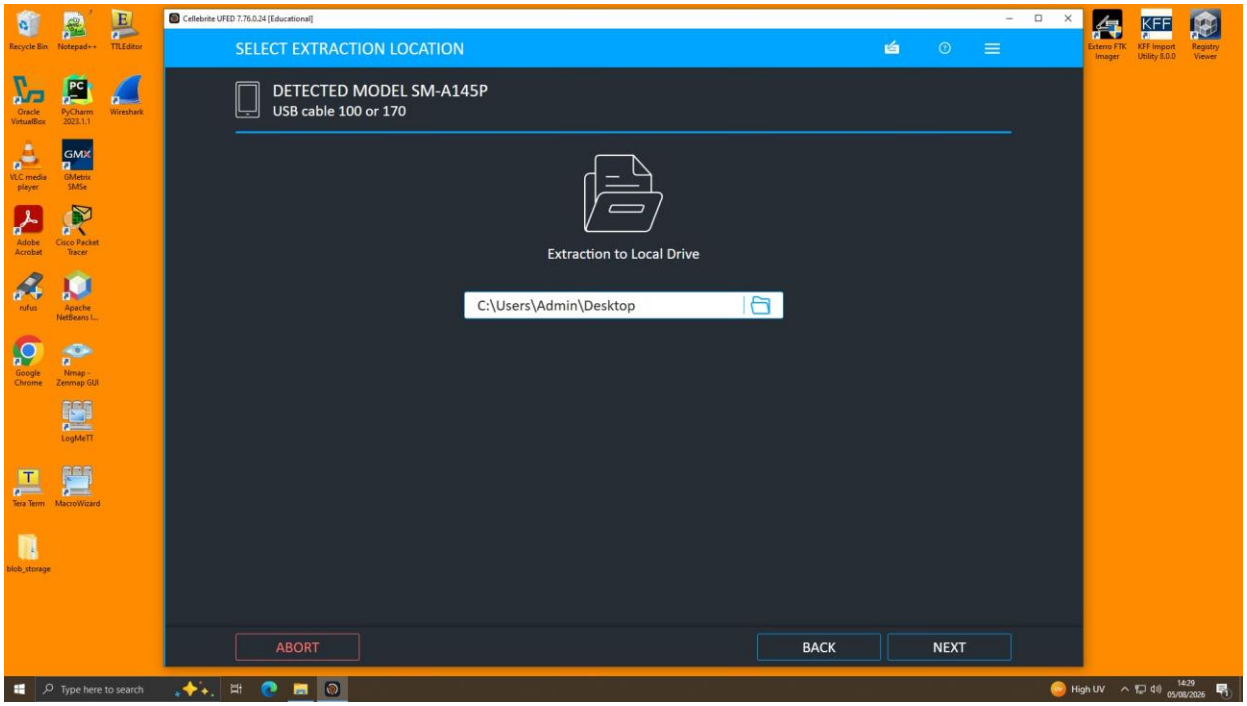

Figure 4: Selecting the extraction destination (local drive) for the detected Samsung SM-A145P.

Once these settings were locked in, the extraction itself began, with the software working through each selected category in turn.

2.4 Extraction Summary

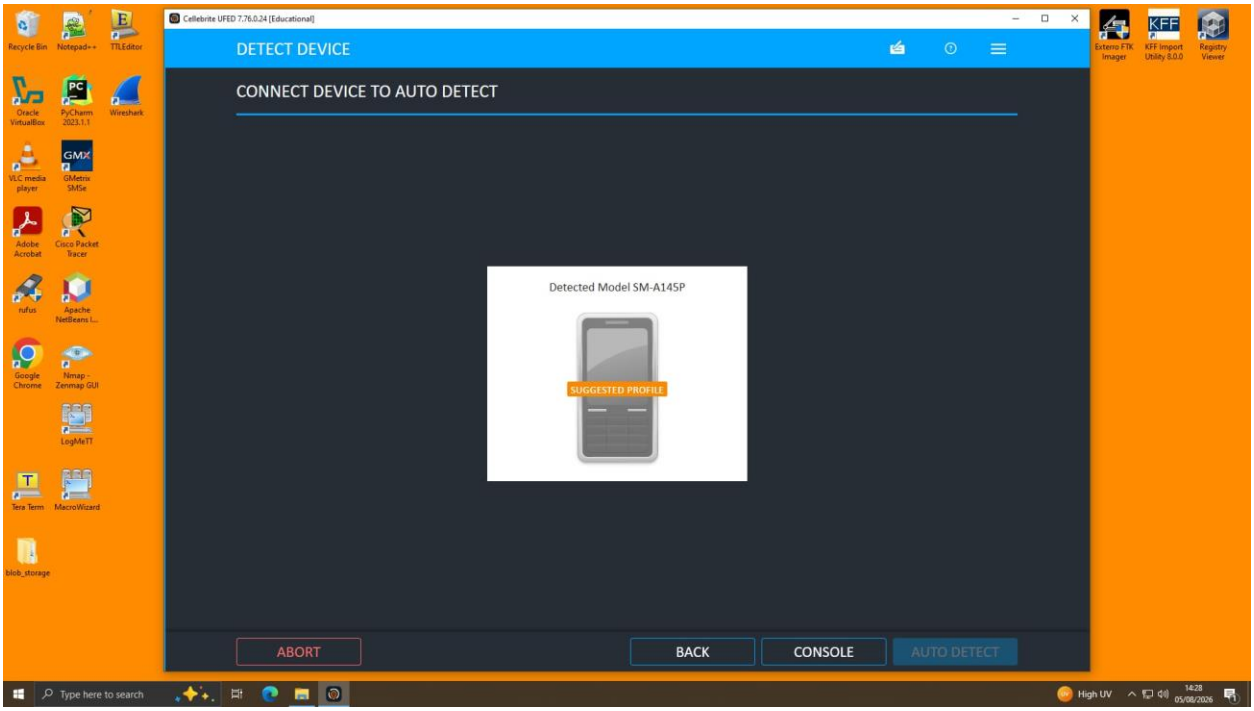

Figure 5: UFED device detection screen confirming the suggested profile for the Samsung SM-A145P.

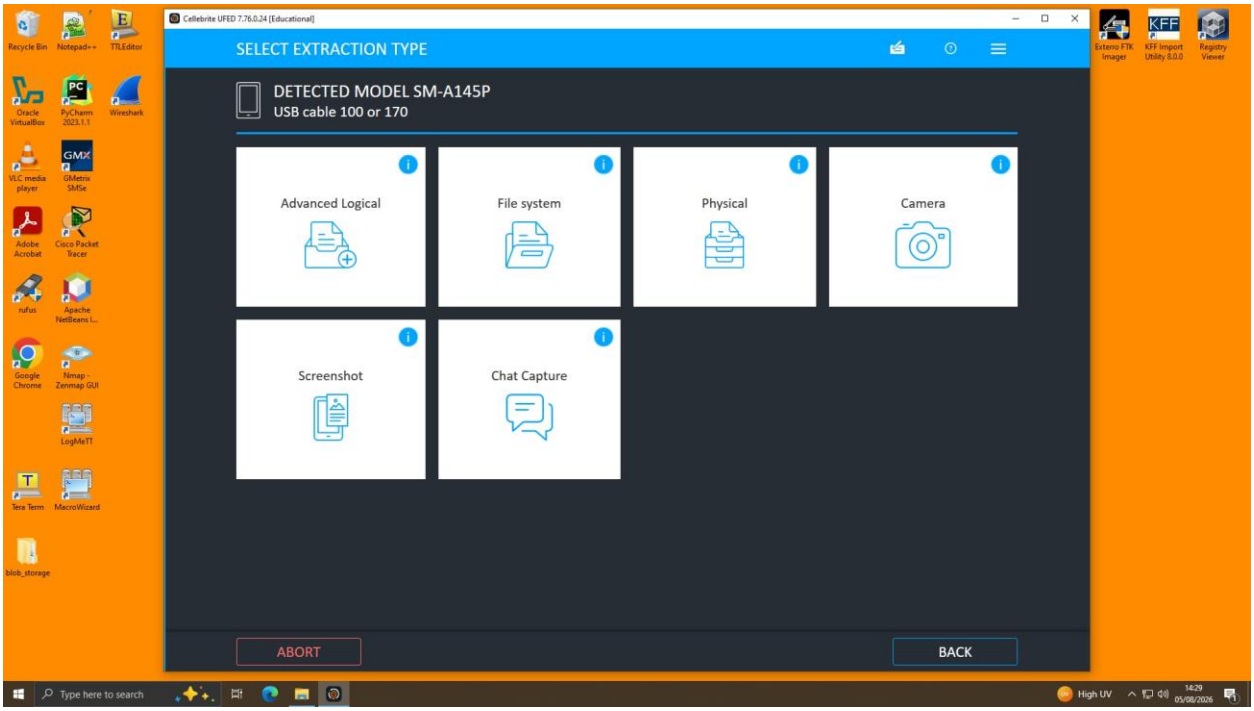

Figure 6: Extraction types offered by UFED for the SM-A145P — Advanced Logical, File System, Physical, Camera, Screenshot and Chat Capture.

2.5 Confirmation of Extraction Process

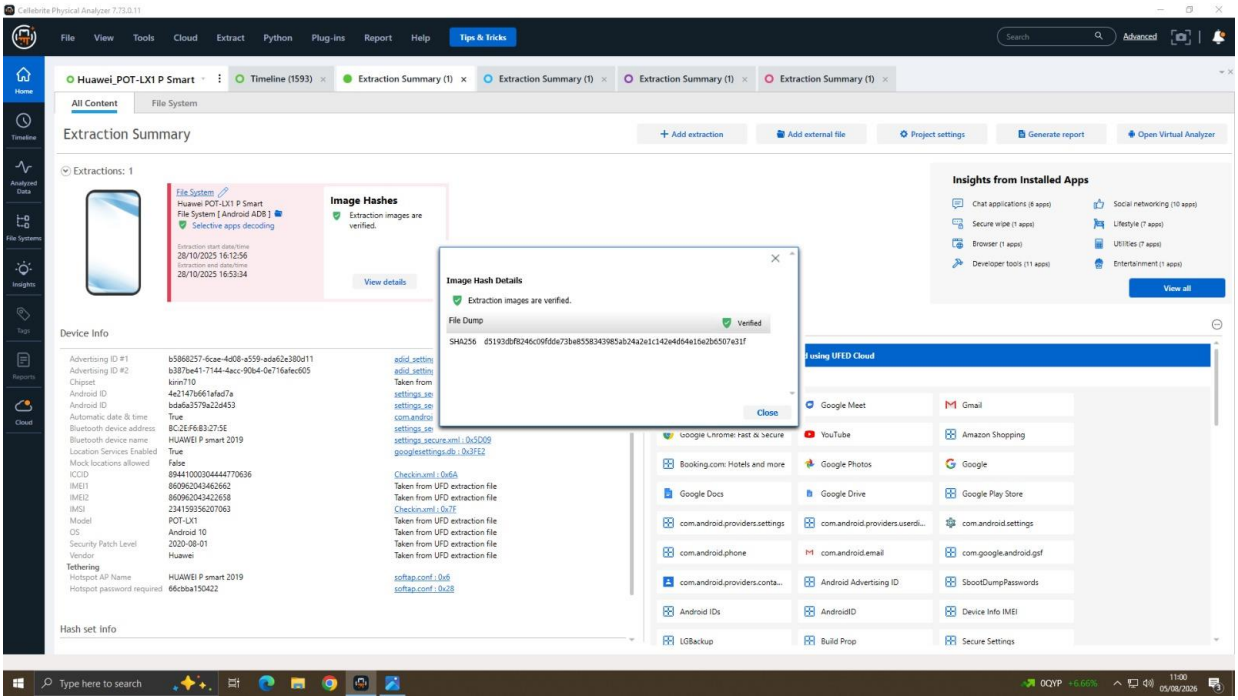

Figure 7: Physical Analyzer extraction summary for the Huawei POT-LX1 P Smart, file-dump hash verified.

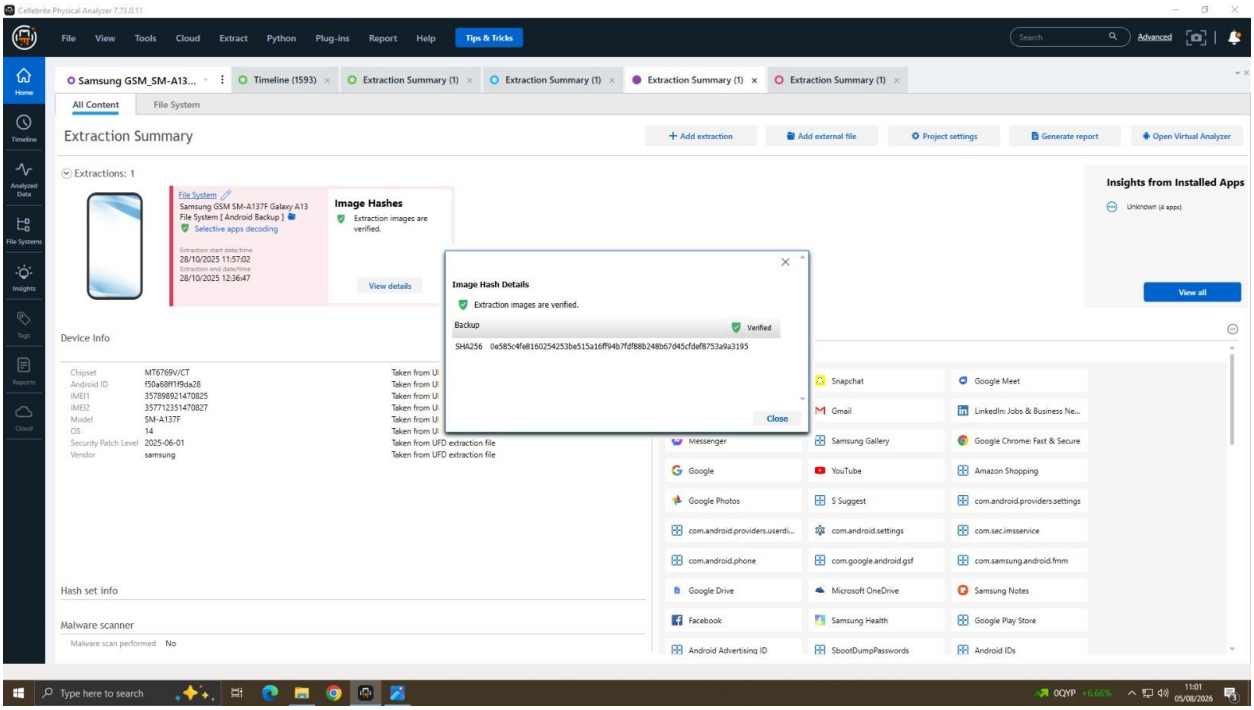

Figure 8: Physical Analyzer extraction summary for the Samsung SM-A137F Galaxy A13, backup hash verified.

This is a confirmation that the data extraction is completed successfully and what types of files were pulled from the device. This final step is to make sure you have successfully transferred all the data you selected for analysis.

2.6 Data Types Extracted

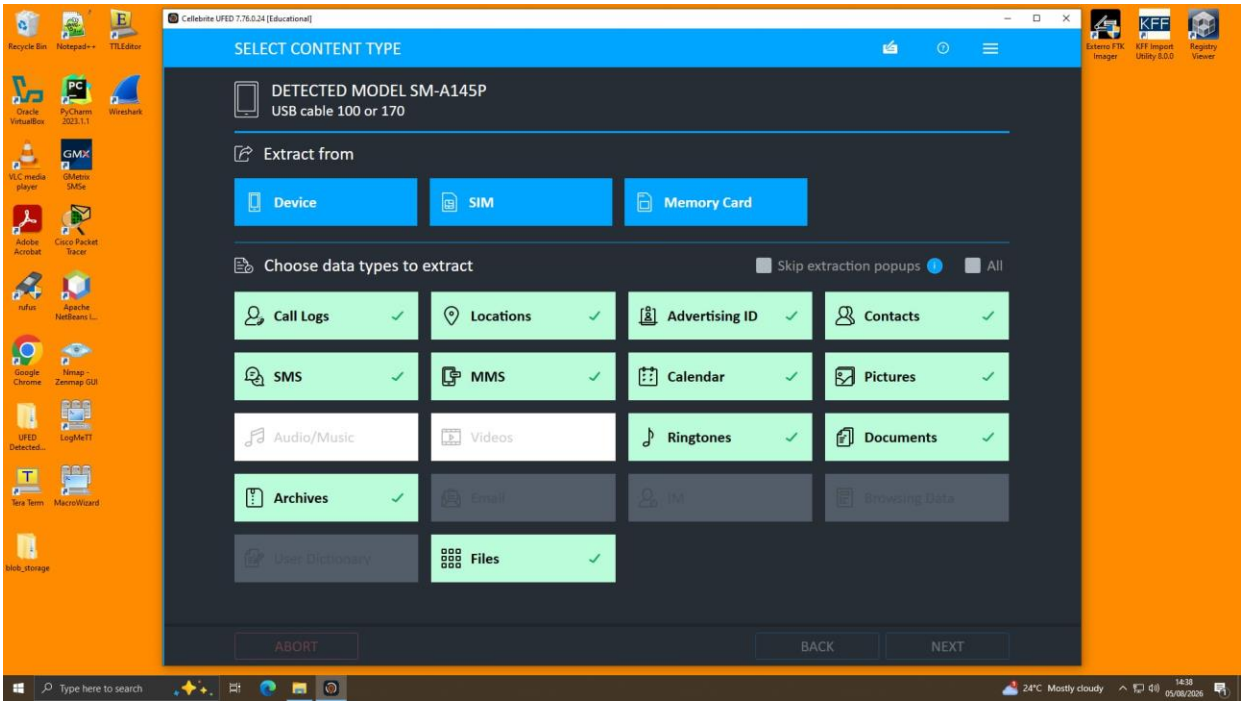

Figure 9: Content types selected for extraction — call logs, locations, contacts, SMS, MMS, calendar, pictures, ringtones, documents, archives and files.

The screenshot shows the particular data types the examiner decided to take from the device: SMS messages, call logs, location information, and multimedia files. Rather than extracting everything indiscriminately, these selections were made deliberately, ensuring the extraction would surface exactly the kind of detail needed to support a thorough investigation of the device's contents.

2.7 Additional Extraction Settings

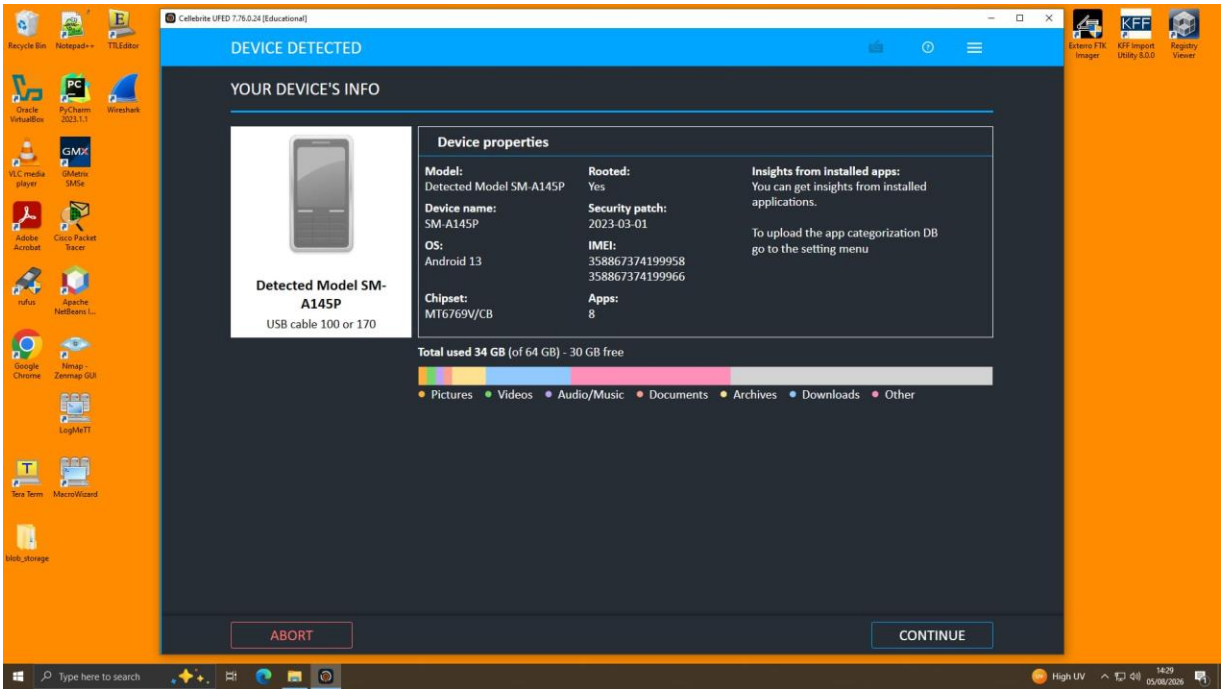

Figure 10: Device properties reported for the Samsung SM-A145P — Android 13, dual IMEI, rooted status and storage usage (34 GB of 64 GB).

The tool also allowed for finer control over multimedia extraction specifically — letting the examiner choose between pictures, videos, ringtones, and other file types, so that only genuinely relevant material was pulled rather than everything indiscriminately.

2.10 Final Extraction Summary

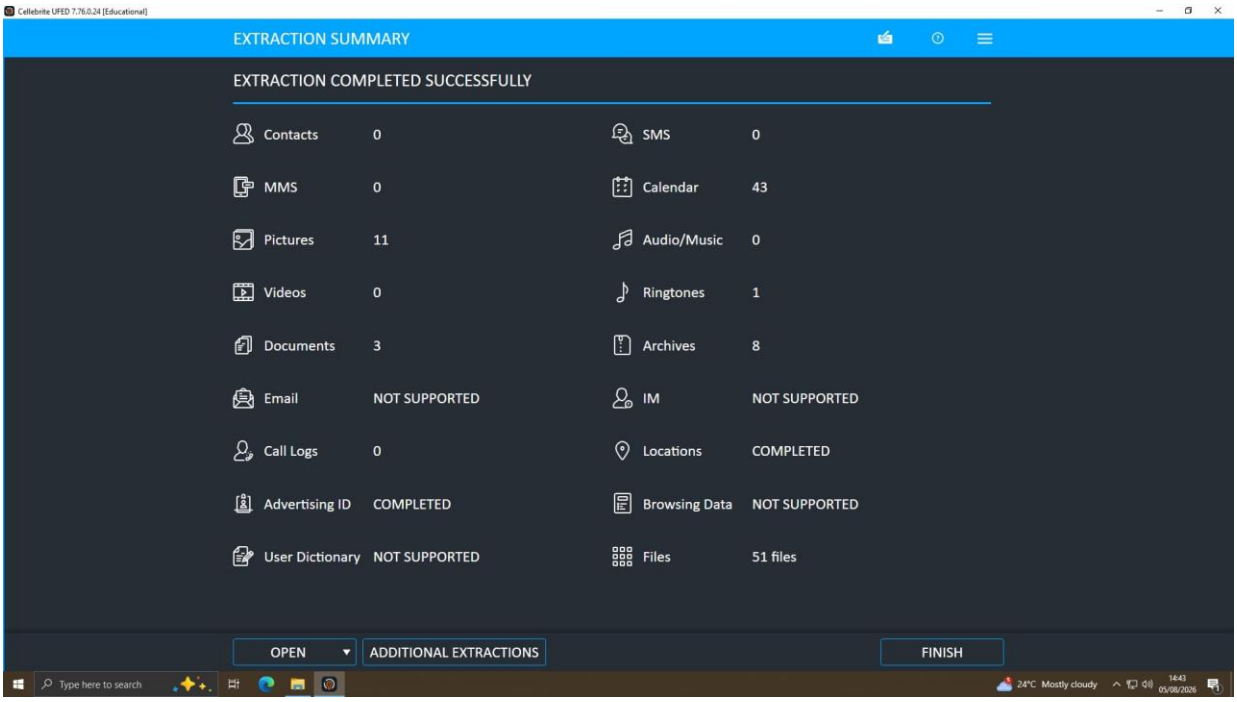

Figure 11: Final UFED extraction summary — 11 pictures, 43 calendar entries, 3 documents, 8 archives, 1 ringtone and 51 files recovered; email, IM, browsing data and user dictionary were not supported.

The final summary confirmed successful extraction of files, contacts, call logs, and multimedia content, while also flagging anything that couldn't be recovered — such as the user dictionary and a handful of other unsupported file types.

3. Communication Analysis

One of the most important parts of the investigation was the analysis of the communication logs. The plan to steal and resell the QT-AI-2025 patent relied exclusively on Emma, Joe and Norman remaining in close contact and they did so principally thru WhatsApp, Instagram direct messages and email, all of which were extracted and reviewed.

- **WhatsApp and Instagram:** Looking thru the messages between Emma and Joe, we could see detailed discussions about selling the patent – the price, keeping the deal quiet and arranging meetings. In one exchange Emma said she would send over the patent files and urged Joe to bring Norman up to speed fast. All these messages add up to point clearly to Emma as the one pushing the theft along.
- **Email:** The email conversations between Joe and Norman added another piece to the puzzle, revealing that it was Joe who originally had Emma brought to Norman. In these messages Joe told him that the files were ready and discussed closing the deal and Norman replied about dealing with the paper work on his side. The emails, when read together, provide a blueprint for selling stolen intellectual property.
- **Forensic Imaging:** Full forensic imaging was performed on all three suspects' phones and Emma's USB drive, allowing investigators to review messages, files, emails and call records in their entirety without altering underlying data.

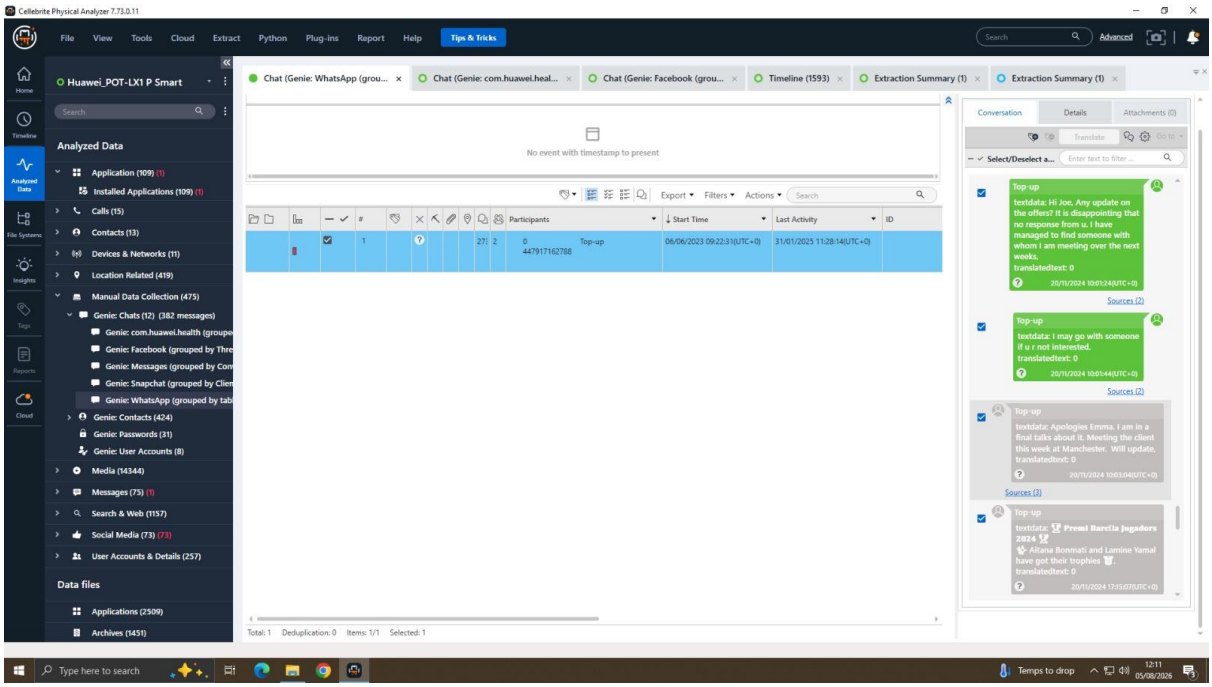

Figure 12: Forensic image of the WhatsApp conversation recovered from Emma's Huawei POT-LX1 P Smart in Cellebrite Physical Analyzer.

Figure 12: Forensic Image of WhatsApp Communication

- **Content:** In this image, communication between Emma and Joe is visible. Emma is discussing the status of a potential deal regarding the QT-AI-2025 patent.

- **Message:** "Hi Joe. Any update on the offers? It is disappointing that no response from u. I have managed to find someone with whom I am meeting over the next weeks."

- **Timestamp:** 20/11/2024, 10:01:24 UTC+0

- **Meaning:** The message's tone indicates Emma is getting impatient with Joe's silence and has started to look for another buyer to keep the wheels turning. The fact she says she'll meet with someone "over the next weeks" hints at some level of secrecy to the arrangement, and with her obvious frustration, the message implies that she's in a hurry to get the deal done.

Emma's smartphone, showing the successful extraction of communication logs and files.

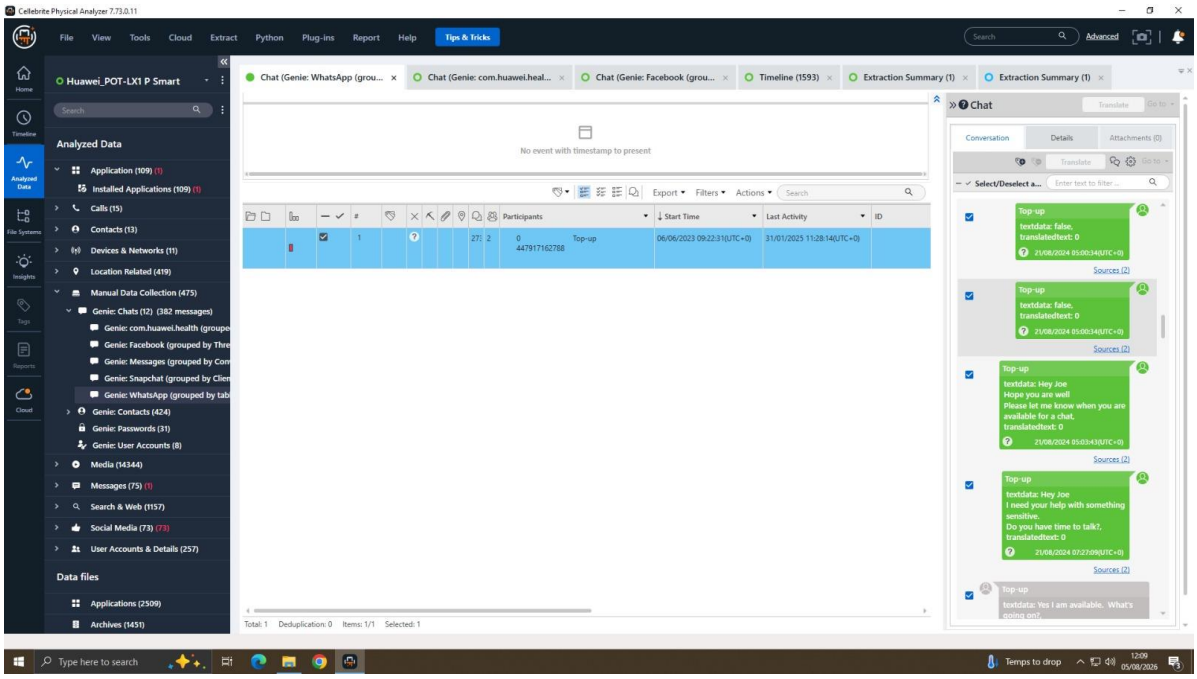

Figure 13: Continuation of the Emma–Joe WhatsApp thread in Cellebrite Physical Analyzer.

Figure 13: Additional Communication with Joe

- **Content:** Emma follows up with additional messages.
- **Message:** "Apologies Emma. I am in final talks about it. Meeting the client this week at Manchester. Will update."
- **Timestamp:** 20/11/2024, 10:03:04 UTC+0

4. Call Log and Email Correlation

Communication logs and call logs and email exchanges were also cross-referenced to further corroborate the timeline of events and the involvement of each suspect. Call logs from the phones of Emma, Joe and Norman were meticulously checked and the suspects were also traced on the phone at crucial points of the conspiracy.

- **Call logs:** One call in particular stands out, a conversation linking Emma, Joe and Vanessa – an R&D Director at NexGen Circuits – which records suggest was the final detail of the patent sale being negotiated. Joe's call history had a story to tell as well, a pattern of repeated contact with Norman that made his role unmistakable. He was not just a name that passed between Emma and Norman, he was the thread that was holding their communication together.

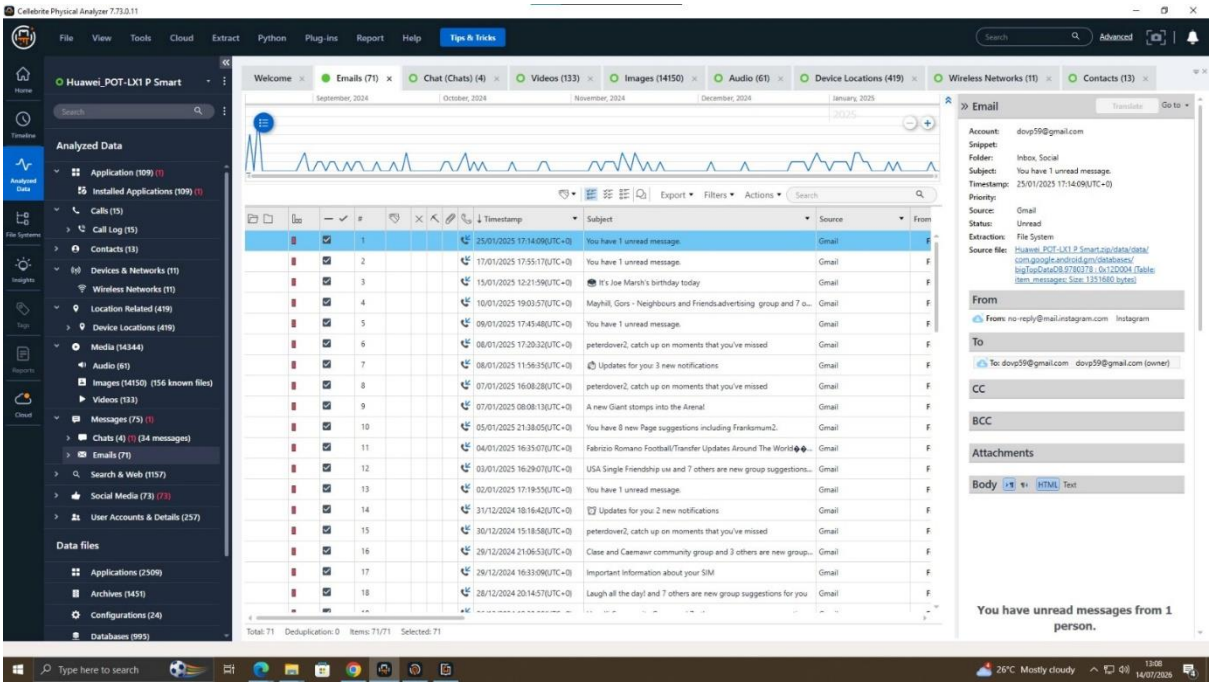

Figure 14: Email records recovered from the Huawei P Smart (71 items) as displayed in Physical Analyzer.

- **Email Correlation:** When investigators lined up the timestamps, a rhythm emerged: a phone call, then an email shortly after, often filling in the practical specifics — payment terms, logistics, the kind of detail people prefer to put in writing once the verbal agreement is settled. This back-and-forth between calls and emails strongly suggests Joe wasn't simply passing messages along passively; he was actively steering the deal.

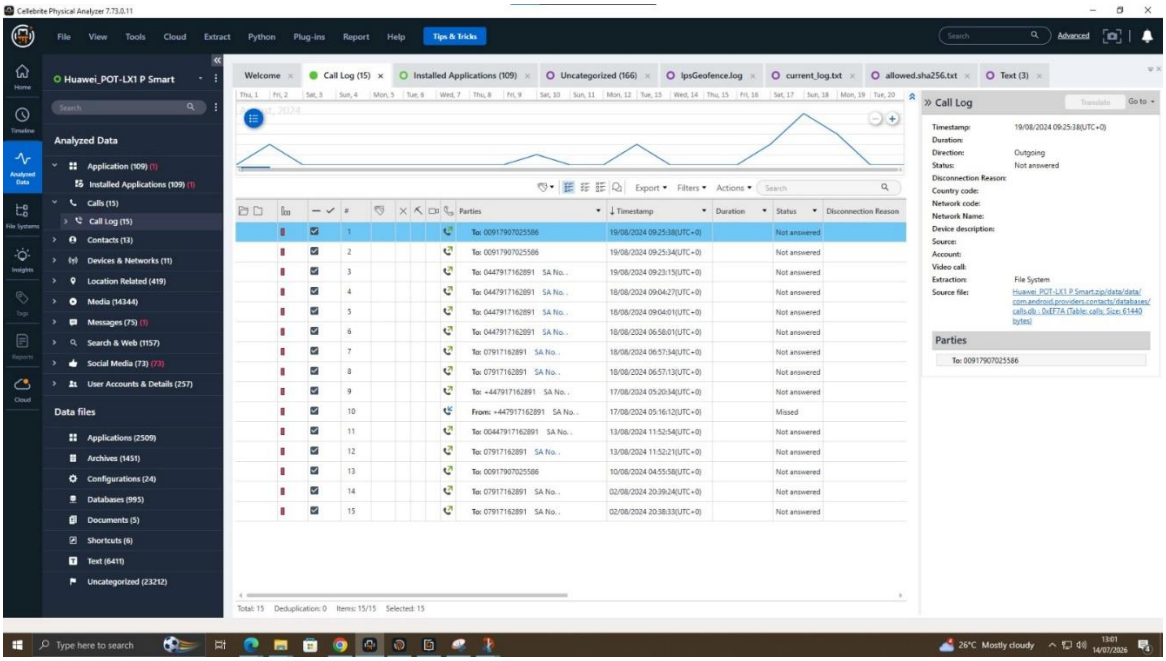

Figure 15: Call log recovered from Emma's Huawei P Smart — 15 entries, largely outgoing and unanswered calls to Joe's number during August 2024.

- **Image:** Call log from Emma's phone showing communication with Joe – This image will be added here to show the call log from Emma's phone, confirming the direct communication between Emma and Joe.

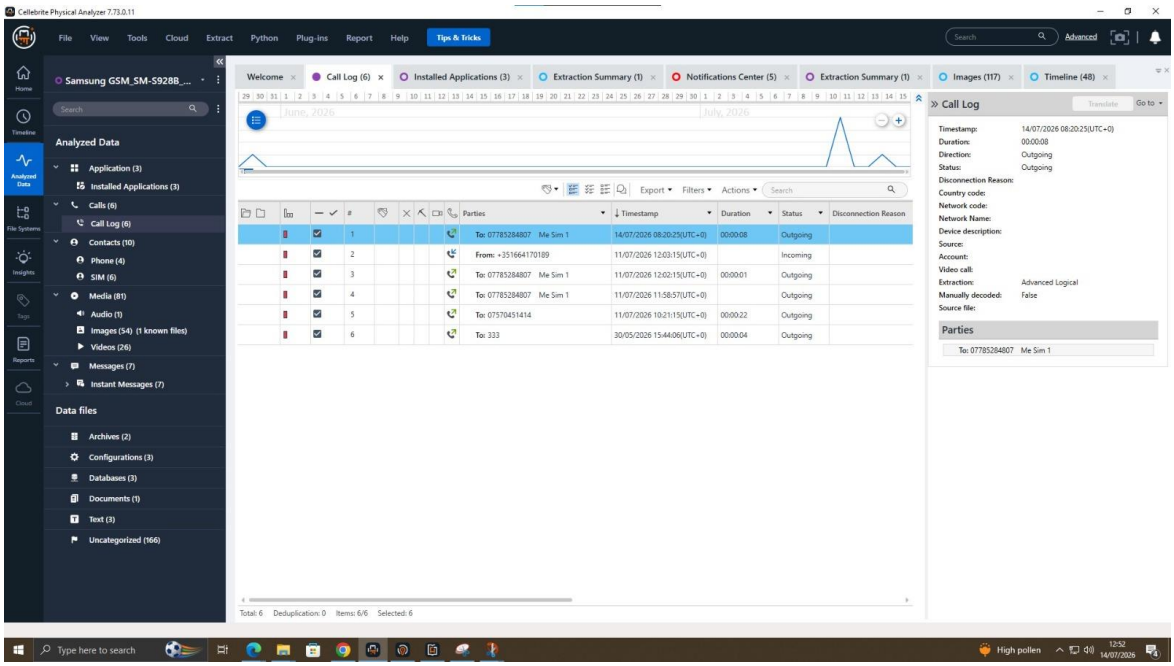

Figure 16: Call log recovered from the Samsung SM-S928B handset, showing six entries including repeated outgoing calls to a single number.

These findings confirmed the close communication between all parties involved, strengthening the case for corporate espionage and intellectual property theft

5. Suspect Profiling

The evidence gathered was painstakingly used to profile the roles and motivations of the three main suspects:

- **Emma:** She was a senior engineer at Quantum Tech so she had legit access to the QT-AI-2025 patent – which was the weak link the whole scheme hinged on in the end. The evidence, the message history, the patent files recovered from her USB drive, all pointed to her as the one who set the theft in motion. Money seems to have been the primary motivation, as she tried several times to sell the design to someone who would pay her for it.
- **Joe:** Joe, however, was a very different sort of man. He was not the thief, but the fixer. He was the guy behind the scenes, hooking Emma up with a buyer, getting them together, keeping the wheels turning. Nothing suggests he touched the stolen files himself, but his fingerprints were all over the negotiation that followed, and the promise of a cut appears to have kept him invested in seeing the deal through.
- **Norman:** Norman was the buyer, so he rounded out the trio. He had much to gain from a buy of proprietary AI chip technology as an exec at NexGen Circuits without the years of R&D investment that usually comes with it. His constant letters to Joe left no doubt of his interest in the patent.

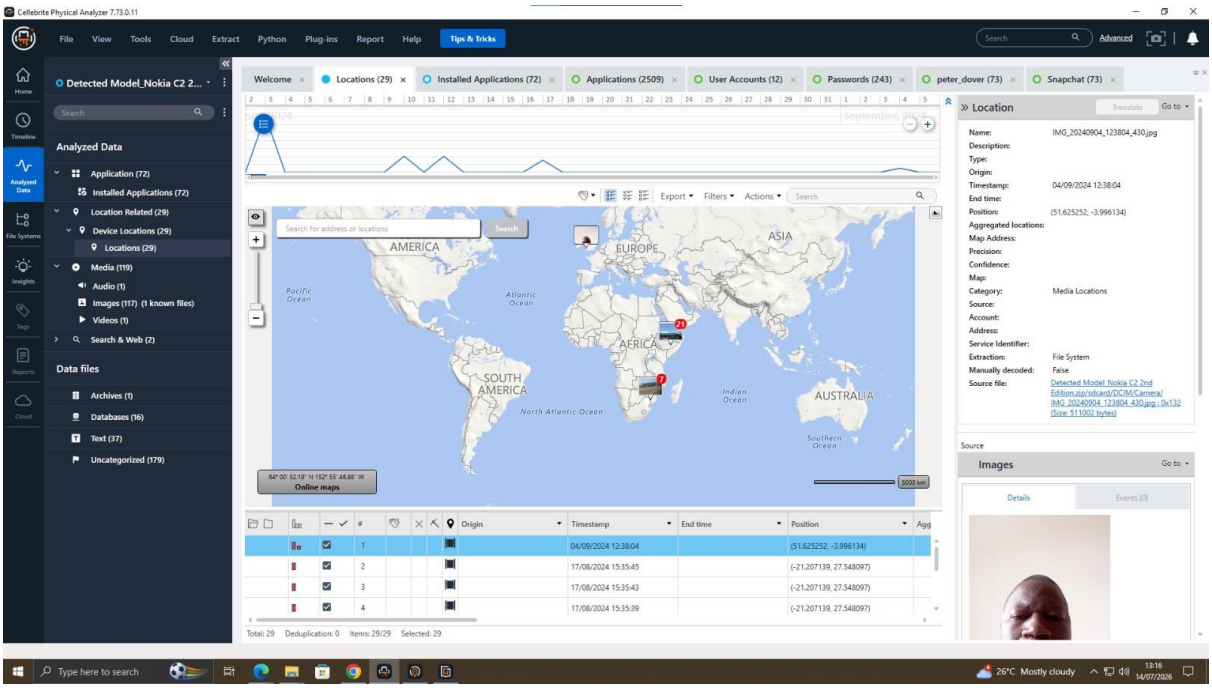

Figure 17: Location data related to the communication, shown in the Cellebrite Physical Analyzer Locations tab for the Nokia C2 2nd Edition

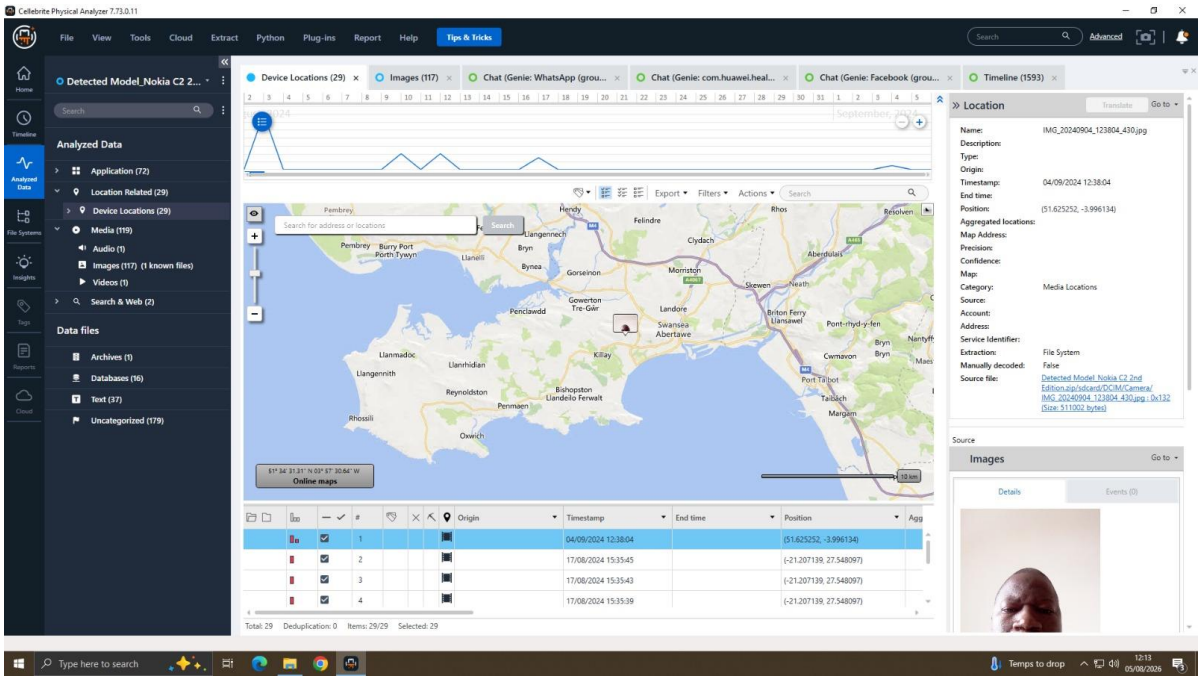

Figure 18: Location data from Emma's phone plotted at street level in Cellebrite Physical Analyzer.

Figure 17: Location Data Related to Communication

- **Timestamp:** 20/11/2024, 10:04:44 UTC+0

- **Location Data:** The coordinates recovered alongside this message thread capture Emma's position at the time — data that points to her being in motion rather than stationary, consistent with someone actively traveling toward a meeting connected to the patent deal.

Figure 18: Location Data from Emma's Phone

- **Location:** (51.625252, -3996134)

Taken alongside the message and email logs reviewed earlier, this location data adds another layer of confirmation, reinforcing the picture already forming from the digital communications — one that ties Emma, Joe, and Norman together through both what they said and where they were.

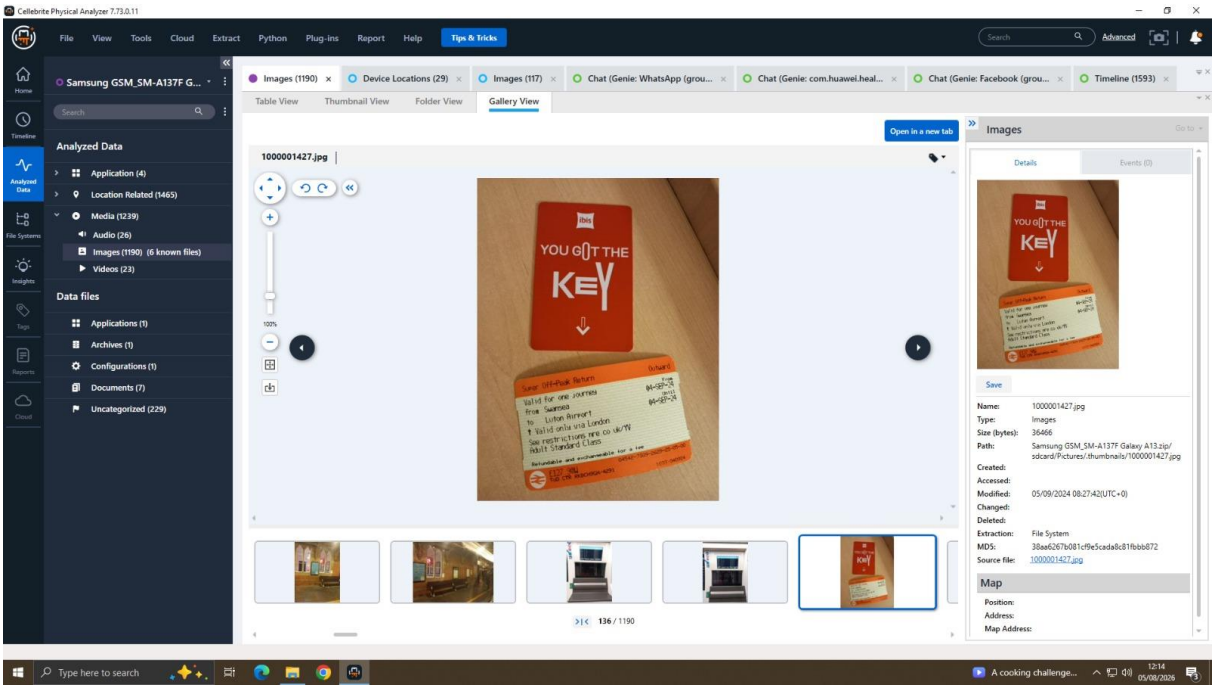

Figure 19: Recovered photograph from the Galaxy A13 — a hotel key-card wallet and an off-peak return rail ticket from Swansea to Luton Airport dated 04-SEP-24.

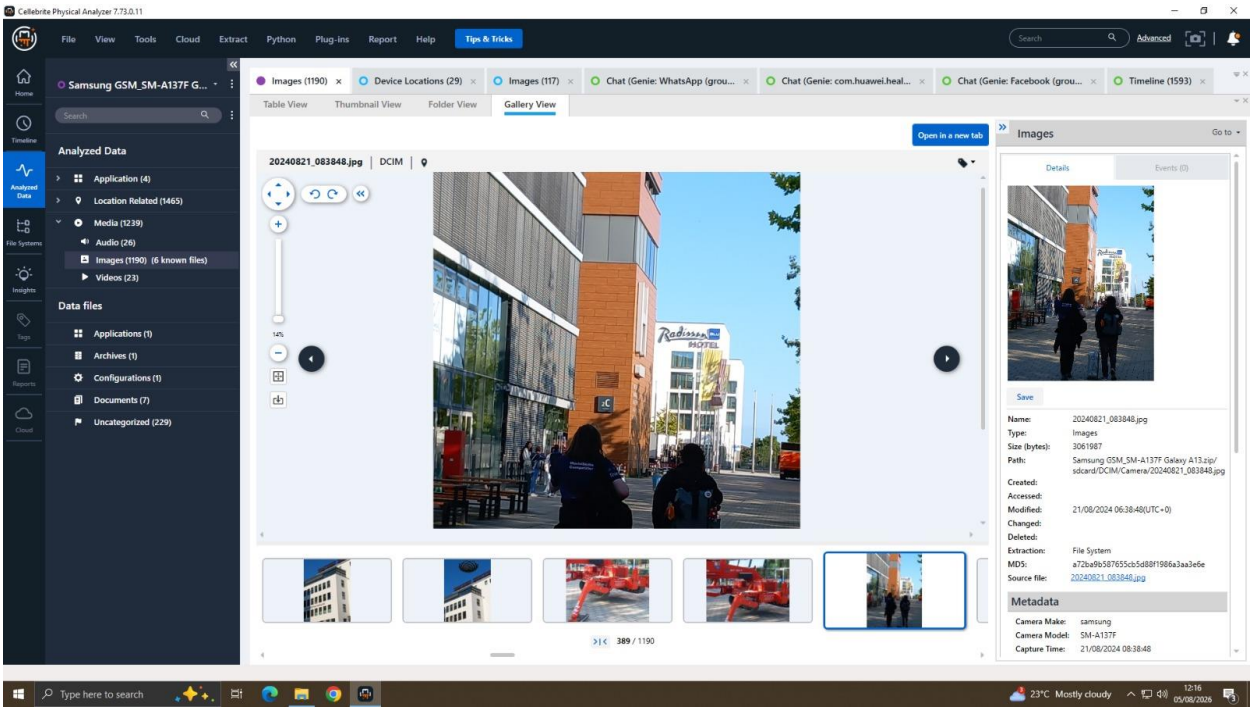

Figure 20: Street-level photograph recovered from the Samsung Galaxy A13 (SM-A137F).

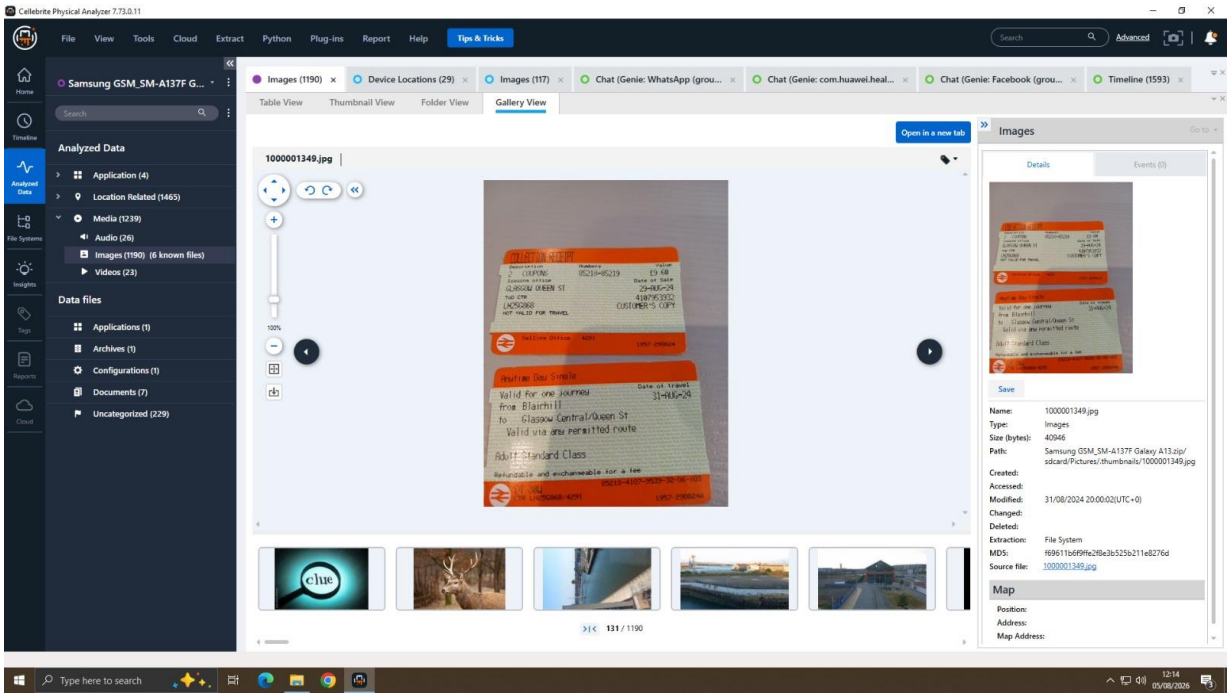

Figure 21: Travel information recovered from the Samsung Galaxy A13 (SM-A137F).

Figure 21: Travel Information

- **Content:** A photograph of a train ticket recovered during the extraction process.
- **Message:** The ticket appears to belong to Emma and indicates travel toward Manchester, aligning with references made in her exchanges with Joe. On its own, a ticket might seem like a minor detail — but placed alongside the surrounding messages, it becomes meaningful physical corroboration, suggesting Emma didn't merely discuss meeting the buyer but actually traveled to do so.

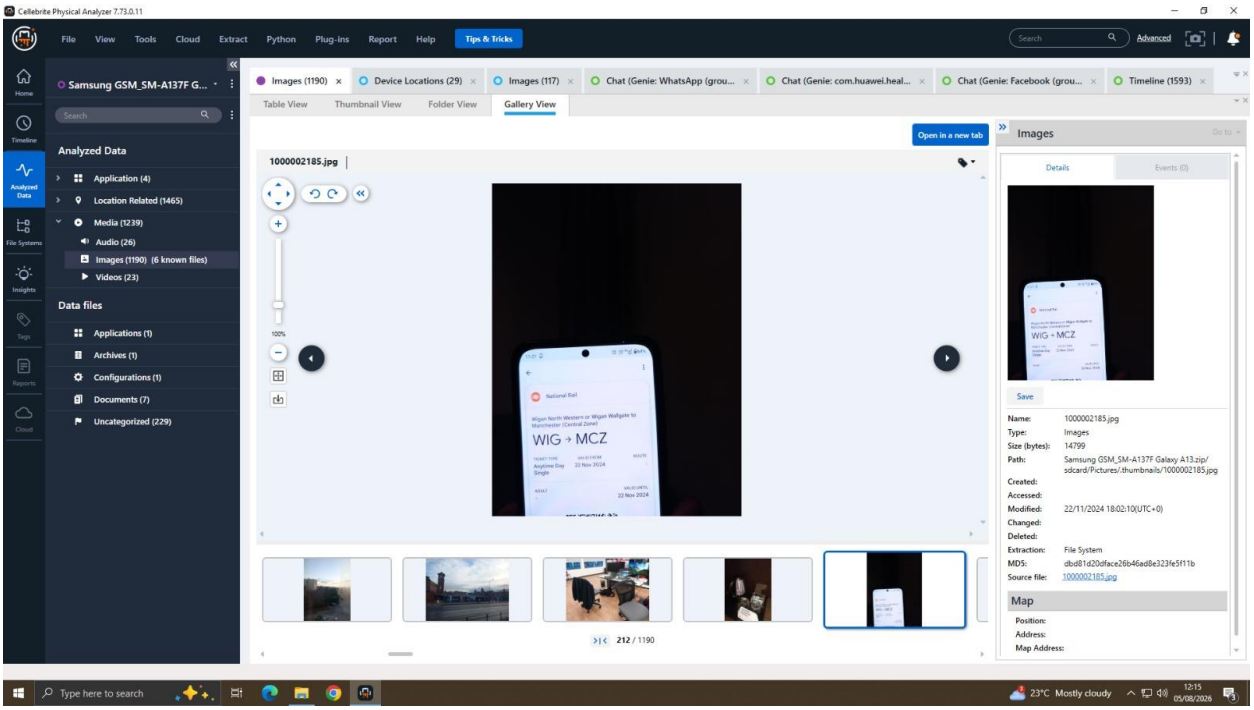

Figure 22: Second rail ticket recovered from the Samsung Galaxy A13 (SM-A137F)

6. Forensic Report Conclusion

All the evidence was gathered and cross-referenced and a clear, consistent story emerged. The devices, the USB drive, the messages, the calls, and the emails — none of it existed in isolation. Together, they built a case strong enough to describe not a lone actor, but three people working in concert to steal and sell proprietary technology.

Every step of the process was handled with care. Chain of custody was preserved throughout, and hash verification confirmed that nothing had been altered during extraction — a detail that matters enormously if this evidence is ever tested in a courtroom. This results in a complete body of evidence that is credible within a legal context.

What roles evolved were clear. Emma had instigated and driven the theft, Joe was the link between her and a buyer, and Norman was the buyer, positioned to benefit from the pilfered design. In light of this, it is recommended the three all face charges of corporate espionage, theft of intellectual property and conspiracy.

Recommendations: Quantum Tech should pursue legal action against Emma for the theft itself, against Joe for facilitating the sale, and against Norman for being the intended purchaser. More importantly, internally the company should use this as a wake-up call to tighten controls on access and beef up monitoring of sensitive data going forward, so a similar breach doesn't have the same chance to happen twice.

7. Demonstrate your analysis and outcomes

➔ Emma's Role as the Perpetrator:

- Putting the Wheels in Motion—It wasn't that Emma got caught up in someone else's scheme. Every message makes her sound like the one driving the deal. Looking for a buyer to take the stolen patent off her hands.
- An Urgent Relationship – Joe's back and forth with Emma wasn't just a casual check in, it felt like Joe was racing against time. The frustration when Joe went silent, the pressure to keep it secret, and all the follow-ups all point to a person with a profound interest in making this deal happen, not a bystander who got dragged into it.
- When the Metadata Tells the Same Story — maybe the most damning evidence of all isn't the words themselves, but the timing behind them. The patent files sitting on Emma's USB drive weren't transferred at some random, unconnected moment—the metadata places that transfer squarely within the same window as her most active conversations with Joe. There are two independent threads of evidence that point to the exact same conclusion.

➔ Joe's Role as the Intermediary:

- The Bridge Between Two Sides — Joe never touched the stolen files, but without him, Emma's plan probably wouldn't work. He was the glue that tied her to Norman, the one who turned an intention into a real transaction.
- Setting the Stage — Instead of just passing messages, Joe took the concrete step of setting up the meeting between Emma and Norman. His texts to Emma are reassuring, the sort of thing you'd expect from someone who's actively managing a deal, not someone who's vaguely aware of it from the sidelines.

- Joe's Own Words – Joe's own words make it clear he knew exactly what he was involved in, and it was difficult to deny. Nothing in his communication suggests confusion or innocence about what was being arranged—quite the opposite. He knew what the arrangement was, and he kept helping it along anyway.

➔ Norman's Role as the Buyer:

- A Buyer With Something to Gain — Norman, as a NexGen Circuits executive, had something to gain from the purchase. He would gain access to Quantum Tech's proprietary chip design. He was in constant contact with Joe during the process which shows he was not a passive party but someone who was actively trying to close the purchase.

- Right Place at the Wrong Time—Location data put Norman right where the deal should have been sealed, adding a physical aspect to what may otherwise have been a trail of messages and calls on paper.

➔ Where Digital Evidence Meets Physical Reality:

- Emma and Joe, Moving in Sync — The best evidence this was not a totally remote setup was how often Emma's and Joe's locations coincided at crucial moments. People coordinating a secret deal don't usually need to be in the same place—unless the deal has reached a stage where face-to-face contact matters.

- Norman, Right on Schedule—His location data tells a similar story, placing him at key points exactly when meetings were expected to happen—hardly the pattern of someone uninvolved.

➔ The Ticket That Told the Truth:

- From Words to Action — A train ticket on Emma's device, going to Manchester, might seem a small thing by itself. But set against everything else—the messages, the timing, the location pings—it becomes something far more significant: proof that Emma didn't just discuss meeting a buyer. She got on a train and went.

8.Timeline of Key Events and Actions Key Insights from the Table

Date/Time (UTC)	What Happened	Who Was Involved	Channel	Context
06/06/2023, 09:22:31 UTC	Emma reaches out to Joe for the first time regarding the patent sale	Emma, Joe	WhatsApp	The opening move — Emma checking in on where things stand
13/08/2024, 11:56:30 UTC	Emma follows up, pressing Joe about a potential buyer	Emma, Joe	WhatsApp	Her tone shifts here — frustration at the silence starts to show, along with a growing sense of urgency
20/11/2024, 10:01:24 UTC	Emma pushes again for an update, mentioning she's found a new contact	Emma, Joe	WhatsApp	A turning point — she's no longer waiting patiently and is actively exploring alternatives
20/11/2024, 10:03:04 UTC	Joe responds with an apology, referencing an upcoming meeting in Manchester	Joe, Emma	WhatsApp	Joe re-engages, and the Manchester meeting enters the picture for the first time
20/11/2024, 10:04:44 UTC	Emma raises the possibility of going with someone else instead	Emma, Joe	WhatsApp	She's clearly weighing her options, unwilling to wait indefinitely on Joe
20/11/2024, 11:03:59 UTC	Joe agrees to move forward quietly, on both sides	Joe, Emma	WhatsApp	The two settle on discretion — a mutual understanding to keep the deal under wraps
23/03/2025, 07:27:40 UTC	Emma's device pings a location during contact with Joe	Emma	Location Data	Places her physically near a location tied to the planned meeting

23/03/2025, 07:27:37 UTC	Joe's device shows a matching location at nearly the same moment	Joe	Location Data	Confirms the two were in the same place — moving the relationship from digital contact to a real-world meeting

9. Conclusion

The forensic investigation of the theft of the QT-AI-2025 patent leaves little doubt: Emma, Joe and Norman were not three isolated actors who happened to cross paths, but partners working toward a single, deliberate goal – stealing proprietary technology and turning a profit from it.

Emma is at the heart of the scheme. It was she who got the ball rolling, calling Joe over and over to find a buyer for what she'd taken. Her messages don't come across as idle curiosity—they're filled with real frustration and urgency, the tone of someone actively trying to push a deal over the finish line. And the metadata pulled from her USB drive removes any ambiguity about her role, tying the transfer of the stolen files directly to the periods when she was in closest contact with Joe.

Joe, for his part, was the connective thread holding the deal together. He wasn't the one who took the files, but without him, it's hard to see how Emma's plan would have gone anywhere. He brought Norman into the picture, kept communication flowing between both sides, and arranged the meetings that moved the transaction from conversation to reality. His call logs and messages with both Emma and Norman make his involvement — and his awareness of what he was facilitating — difficult to dispute.

Norman entered the picture as the deal neared its conclusion, positioned as the buyer waiting to close the purchase. His talk with Joe shows he was a player, not a watcher. And his location data being at the proposed meeting point is a physical piece of evidence that supports what the digital evidence already indicated.

Each piece of evidence taken separately tells part of the story. The whereabouts data, the call logs, the message threads, the physical evidence, like Emma's travel ticket to Manchester. Together they make a case that's hard to argue with. The three suspects appeared to have had different but connected roles in a coordinated effort to steal and sell patented technology.

Given the strength and consistency of this evidence, charges of corporate espionage, intellectual property theft and conspiracy are recommended against Emma, Joe and Norman. Equally important, this case should be a catalyst for Quantum Tech to shore up its internal security posture — tightening controls on access and improving oversight of sensitive data — to lower the likelihood of a similar breach happening again.