

Assignment Title: Research, Analyse and Investigate Cybersecurity incidents and perform digital forensic assessment

Student Name: Md. Ariful Islam

Student ID: 2431309

Programme: MSc Computing Portfolio

Course Module: Digital Forensics Analysis

Module Code: ACCA7031

Task 1 + Task 2

University of Wales Trinity Saint David

December 11, 2025

Task 1

Contents

1	Abstract	2
2	Introduction	2
3	Current State of the Field and Tools	2
4	Intersection of Digital Forensics and Cybersecurity	3
5	Emerging Trends	3
6	Key Challenges	4
7	National and International Job Market	4
8	Conclusion	5

1 Abstract

This analysis, which is suitable for postgraduates, provides an understanding of the digital forensics landscape today – covering popular forensication tools and their feature set; how digital forensics increasingly interrelates with cyber-security operations; mature and emerging technologies; (present) day-to-day challenges facing practitioners as well as hot topics that are influencing the global workforce. The report, using academic materials, industry reports and government documents, presents an integrated view of the nature of digital forensics in scientific and professional elements.

2 Introduction

Digital forensics Cyber investigations are now an integral part of modern law enforcement and response procedures for corporate security teams, and regulatory authorities investigating digital incidents. Meaningful forensic investigation requires professionals to dig deep through a multitude of data sources, especially in today's world where organisations rely on interconnected cloud services, mobile technologies and Internet of Things (IoT) environments. Key literature highlights the fact that digital forensics is not solely a technical discipline, and requires an appreciation of legal procedures and investigative models [1]. Recent research has also shown that digital forensics is, in relation to incident response and threats mitigation within organizations [2], taking a central stage. The industry's outlook is also promising with the world-wide digital forensics market estimated to reach USD 22–26 billion by end of this decade [3]. This perspective assesses the tools, new trends and challenges as well as the consequences for the workforce, which characterize the field nowadays.

3 Current State of the Field and Tools

Digital investigations are conducted according with methodologies and international standards (e.g. ISO/IEC 27037) which provide principles for best practice in the identification, preservation, examination, and analysis of digital evidence. Contemporary investigations often involve reviewing volatile memory, encryption schemes, virtual machines (VM), mobile platforms and cloud services. Commercially available tools such as En-

Case, FTK, Magnet AXIOM and Cellebrite UFED are widely used as they offer a single environment where acquisition and analysis of digital remnants can be performed across different platforms[4]. These solutions use automation and intelligence assistance, as well as a widerange of parsing capabilities to aid Investigators.

Complementary to commercial tools, open source alternatives such as Autopsy, Sleuth Kit, Volatility and Plaso continue to be critical – particularly in investigative settings or smaller entities with limited budget [5]. Despite their capabilities, surveys of practitioners show ongoing concerns around tool accuracy and validation and the speed at which technology is changing, often obliging examiners to corroborate findings across multiple tools in order for them to be evidentially sound [6]. This suggests a requirement for ongoing testing of instruments and methodological rigor.

4 Intersection of Digital Forensics and Cybersecurity

Digital forensics has evolved to become part of cybersecurity, broadly defined as Digital Forensics and Incident Response (DFIR). Forensics techniques are constructs deployed in proactive security (threat hunting, detection engineering) as well as post-incident investigations. Enterprises use SIEMs, endpoint detection and response tools, firewall logs, and cloud audit trails to piece together how an attacker moved from system to system and what other systems may have been compromised [7].

Organisations are increasingly taking on forensic readiness, which means data used for investigations is captured and stored in a way that meets legal/regulatory needs. The escalation of advanced cyber threats such as ransomware, supply-chain compromise, and credential-based cloud attacks underscore the need for integrated DFIR capabilities [8]. This integration signals the evolution of forensics from a reactive function to one that is seen as relevant within the scope of security throughout its lifecycle."

5 Emerging Trends

The continued adoption of cloud computing has placed cloud forensics at the forefront of digital investigations. Forensic practitioners must be able to capture and interpret distributed logs, snapshots of virtual machines, containerised workloads, and identity-

related metadata stored on platforms such as AWS, Azure, and Google Cloud [9]. Mobile and IoT forensics are also growing rapidly, with devices such as smartphones, smart-home systems, and vehicles producing extensive artefacts relevant to criminal and corporate investigations [10].

Artificial intelligence is becoming increasingly embedded in forensic tools, enabling automated classification of artefacts, anomaly detection, and prioritisation of relevant evidence. Although such capabilities offer significant efficiencies, scholars caution that issues related to transparency, reproducibility, and algorithmic bias must be acknowledged [6]. New areas, including blockchain forensics, cryptocurrency tracing, deepfake investigation, and drone forensics, are emerging in response to evolving cybercrime techniques [11].

6 Key Challenges

One of the major challenges faced in the field is rapidly growing digital evidences. Enterprises generate large amounts of logs, disk images and network data that place a burden on forensic teams and infrastructures [12]. Although encryption is necessary for privacy protection and network security, it introduces a burden to obtain legal evidence that leads to the “going dark” issue confronting investigators [13].

In addition to the lack of ground truth for these forensic datasets, their use in evaluating tools or new techniques is also limited by concerns over realistic-ness and documentation among academic researchers [14]. The second most commonly mentioned challenge is the lack of manpower. The consensus among government reports is that digital forensics also have the most recruitment difficulties, with skill shortage between demand and supply remaining [15]. This shortage is widespread and aggravated by workload pressures and rapid technological change.

7 National and International Job Market

The demand of digital forensic DFIR experts is growing rapidly worldwide due to rising cybercrimes and increasingly for stronger incident response responses. A job growth trend towards related positions is forecasted in market analysis [12]. And in the UK, on

job boards everywhere there are numerous openings in policing, government agencies, banks and even cyber security consultancies. "Employer demand IT jobs watch reports show that the employers are demanding professionals providing a “year on year increase of 6 percent in the number of job opportunities advertised” [13, 14]. Outside of the United States and Europe, both are significant centers for work in DFIR; Asia is growing quickly with the adoption of cloud computing and digital transformation efforts. Employers are demanding hybrid skill sets that encompass technology forensic skills, scripting and automation capabilities, cloud knowledge, and the answer is getting out there.

8 Conclusion

Digital forensics is evolving at a very fast pace due to advancements in technology that change the way investigations are performed and organisational requirements. As tool capacities increase, however, those working on the ground level are encountering several difficulties in terms of scale and data size, encryption limitations, talent shortages and methodological soundness. Meanwhile, the field enjoys an expanding employment pool fuelled by broad digital adoption and ramped up cybersecurity needs. To aspiring forensic analysts out there, the only way to succeed is by constantly learning, being able to adapt and having a sound grasp of both the technical and legislative aspects of digital investigations.

References

- [1] E. Casey, *Digital Evidence and Computer Crime*. Academic Press, 2019.
- [2] T. Arif *et al.*, “A comprehensive survey on digital forensics trends, threats and challenges,” *Journal of Network and Computer Applications*, 2025.
- [3] Grand View Research, “Digital forensics market size, share & growth report, 2030,” <https://www.grandviewresearch.com>, 2024, accessed: 2025-02-01.
- [4] B. Nelson, A. Phillips, and C. Steuart, *Guide to Computer Forensics and Investigations*, 6th ed. Cengage Learning, 2020.

- [5] BlueVoyant, “Open source digital forensics tools overview,” <https://www.bluevoyant.com>, 2023, accessed: 2025-01-30.
- [6] C. Hargreaves *et al.*, “Dfpulse: The 2024 digital forensic practitioner survey,” *Forensic Science International: Digital Investigation*, vol. 51, 2024.
- [7] Magnet Forensics, “State of enterprise dfir 2025,” <https://www.magnetforensics.com/resources>, 2025, accessed: 2025-02-01.
- [8] NCC Group, “Digital investigations: Opportunities and challenges – 2025 predictions,” <https://www.nccgroup.com>, 2025, accessed: 2025-02-02.
- [9] A. Malik *et al.*, “Cloud digital forensics: beyond tools, techniques and challenges,” *Sensors*, 2024.
- [10] Oxygen Forensics, “The digital forensics landscape in 2025,” <https://www.oxygen-forensic.com>, 2025, accessed: 2025-02-03.
- [11] A. D. Salman and E. H. Hasan, “Emerging trends in digital forensics: investigating cybercrime,” *Journal of Digital Forensics*, 2025.
- [12] Future Market Insights, “Digital forensics market forecast 2025–2035,” <https://www.futuremarketinsights.com>, 2025, accessed: 2025-02-02.
- [13] IT Jobs Watch, “Digital forensics job trends and salaries,” <https://www.itjobswatch.co.uk>, 2025, accessed: 2025-02-05.
- [14] Indeed UK, “Digital forensics jobs in the united kingdom,” <https://www.indeed.co.uk>, 2025, accessed: 2025-02-05.

Task 2

FORENSIC INVESTIGATION REPORT

Case Reference: QT-FRAUD-2025

Examiner: *Md. Ariful Islam*

Date: *04 December 2025*

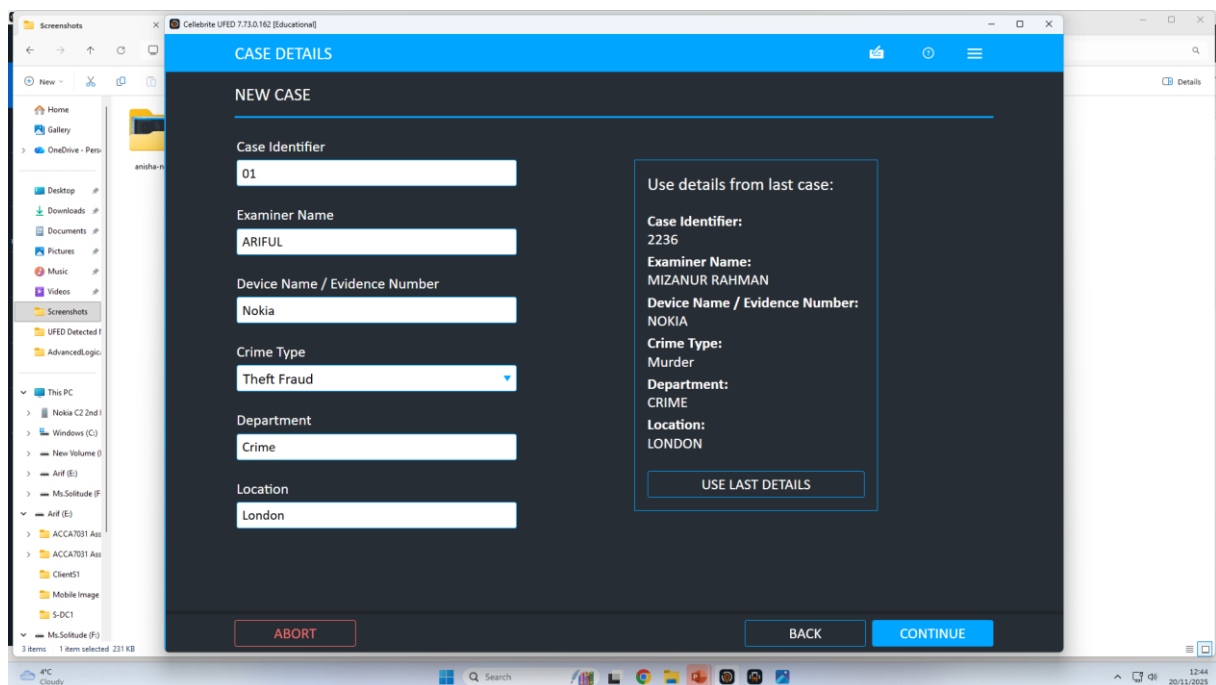
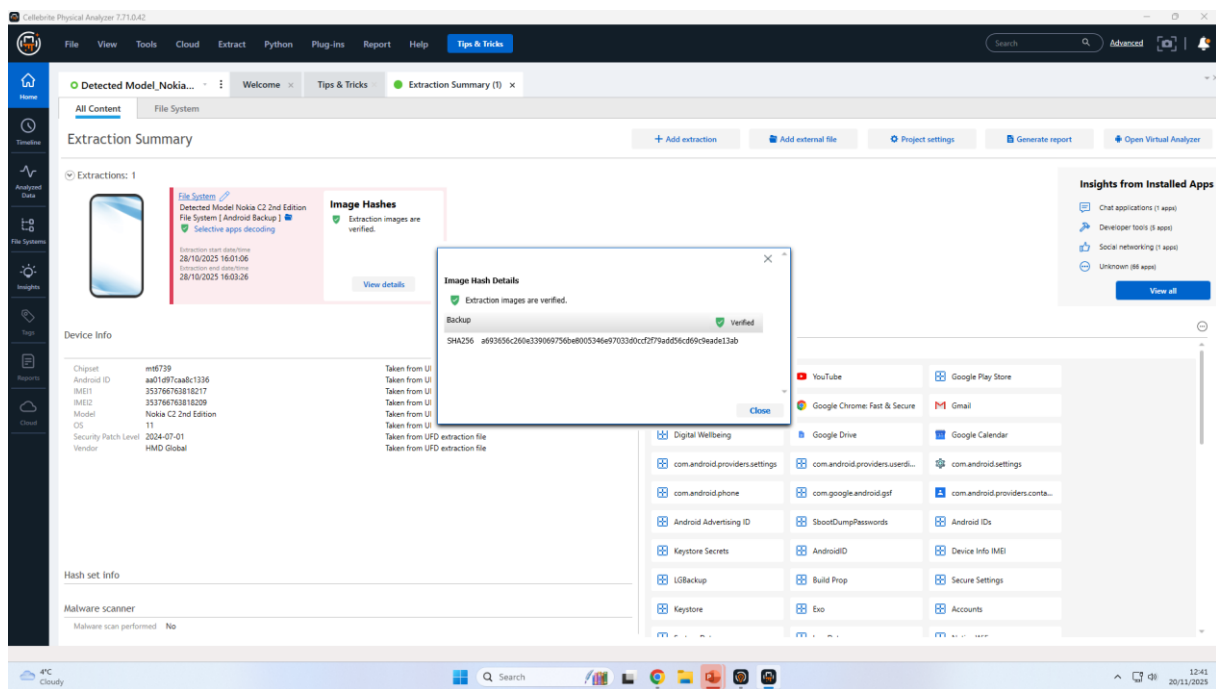
Introduction

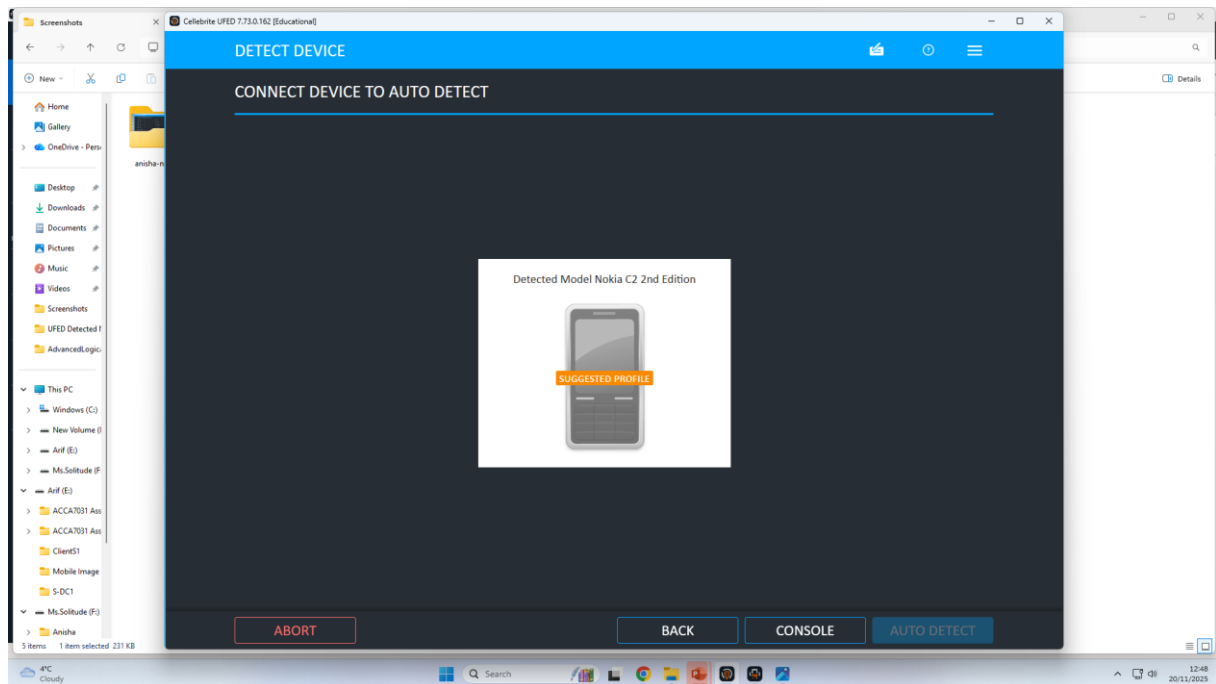
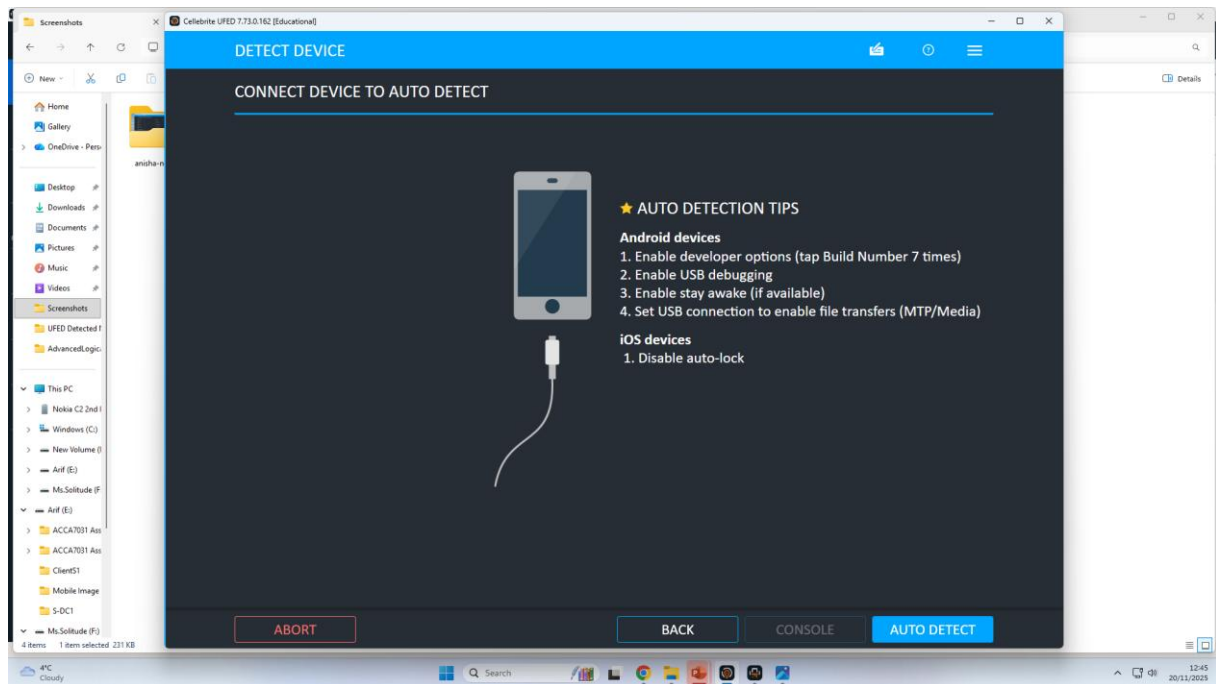
With the level of competition among technology companies today, securing your intellectual property is more important than ever. It is common to use digital means, such as devices and communication systems, for the purpose of corporate espionage, data stealing, and non-authorized information propagation. Consequently, such evidence requires that the tools and methodology used to acquire and submit it will not only withstand legal scrutiny, but also technical evaluation for evidence credibility.

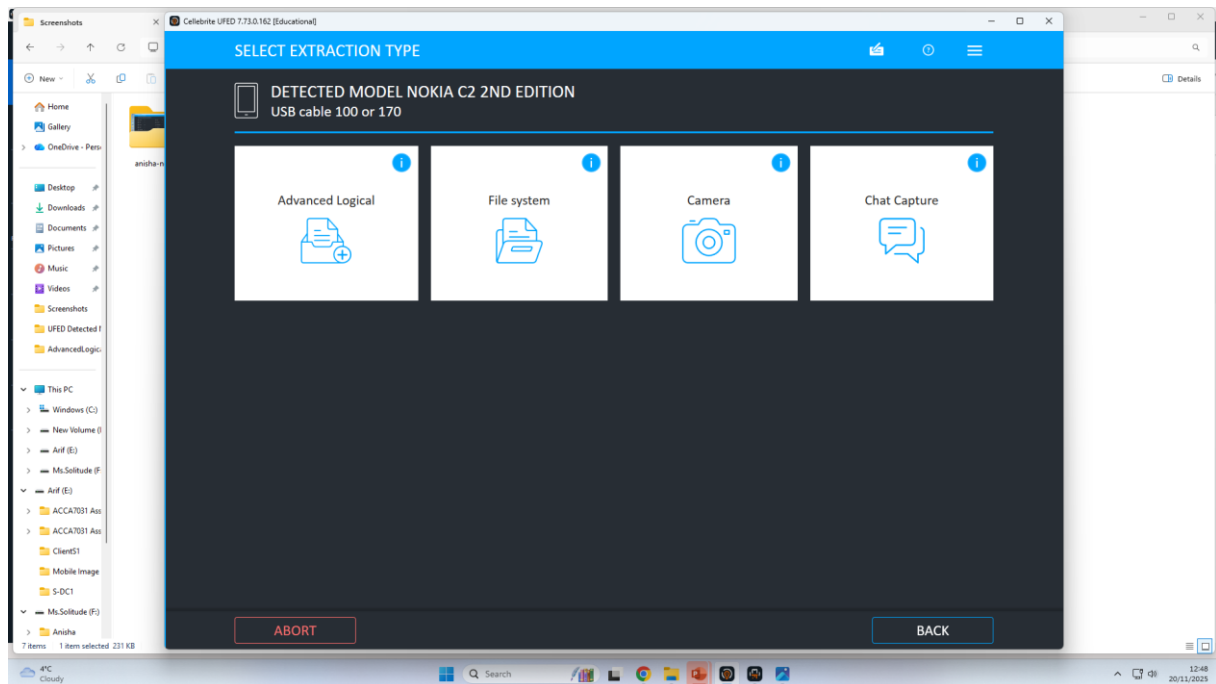
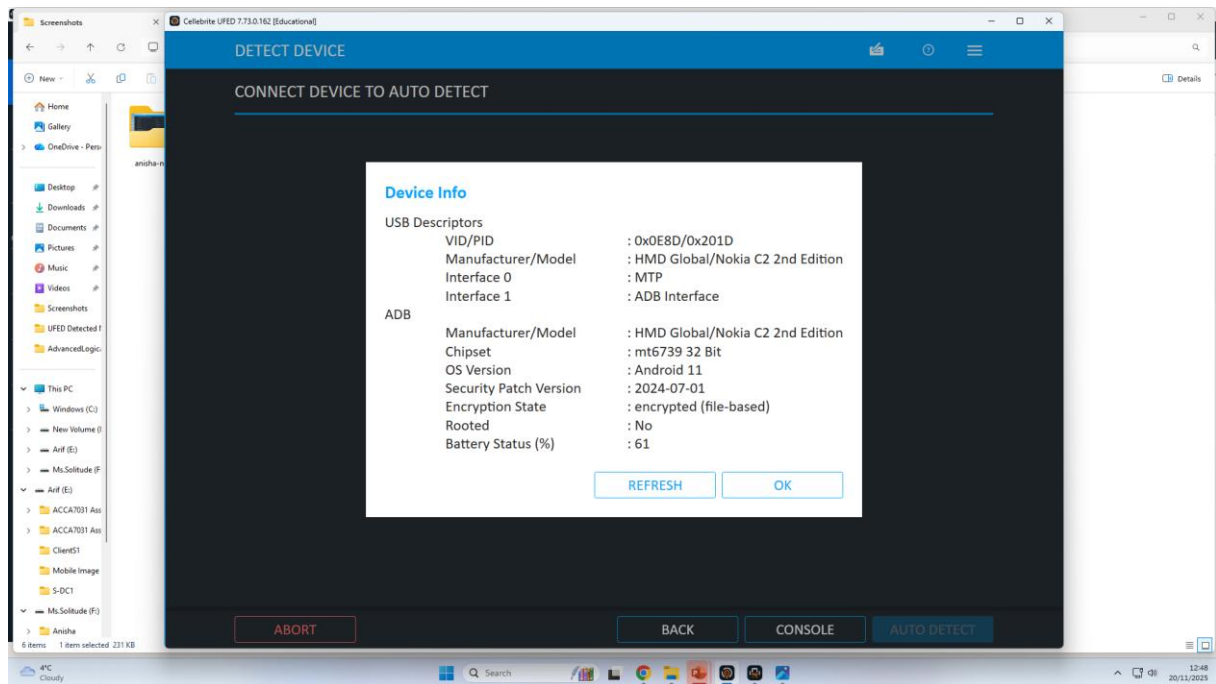
In the first role-playing reporter assignment will cover the fictional, simulated corporate espionage investigation at Quantum Tech as unauthorized access was identified in the company's own proprietary research patent database, hijacking of AI chip design patent QT-AI-2025. Three major suspects are identified in the investigation: Emma, a senior engineer at Quantum Tech; Joe, who has become a middle man to help them make contact; and Norman, believed to be associated with another company looking to make the purchase. Several digital devices (smartphones and one USB stick) were seized and forensically analyzed under strict rules of continuity of evidence.

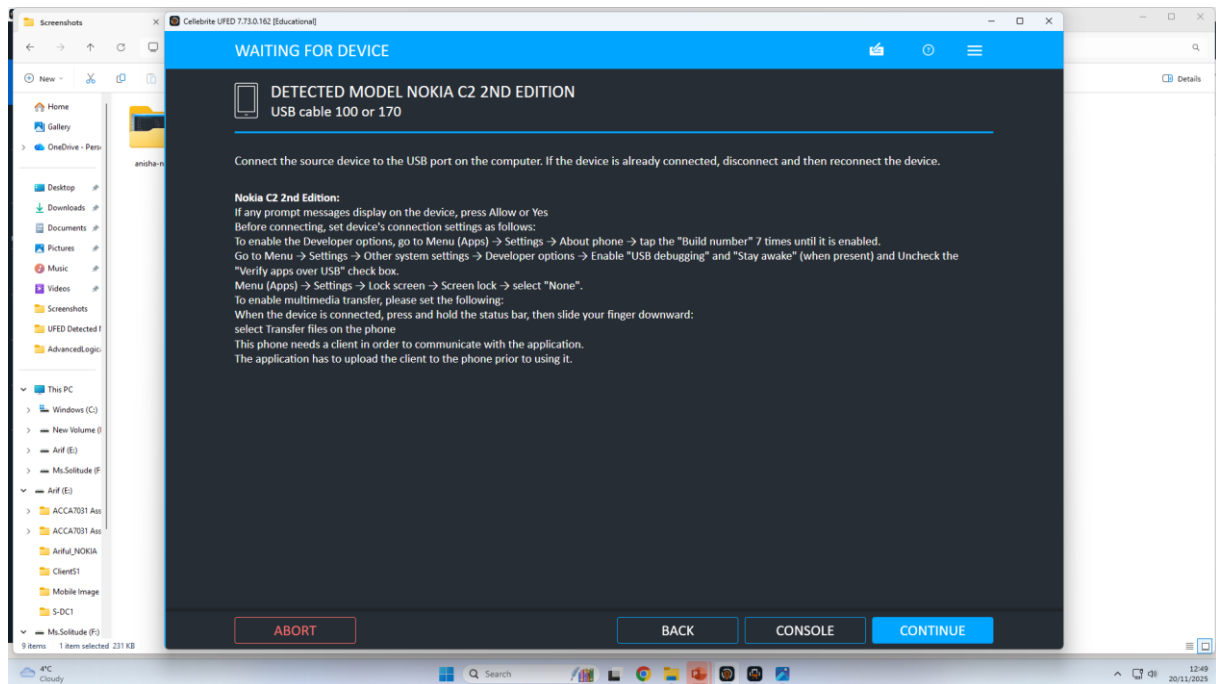
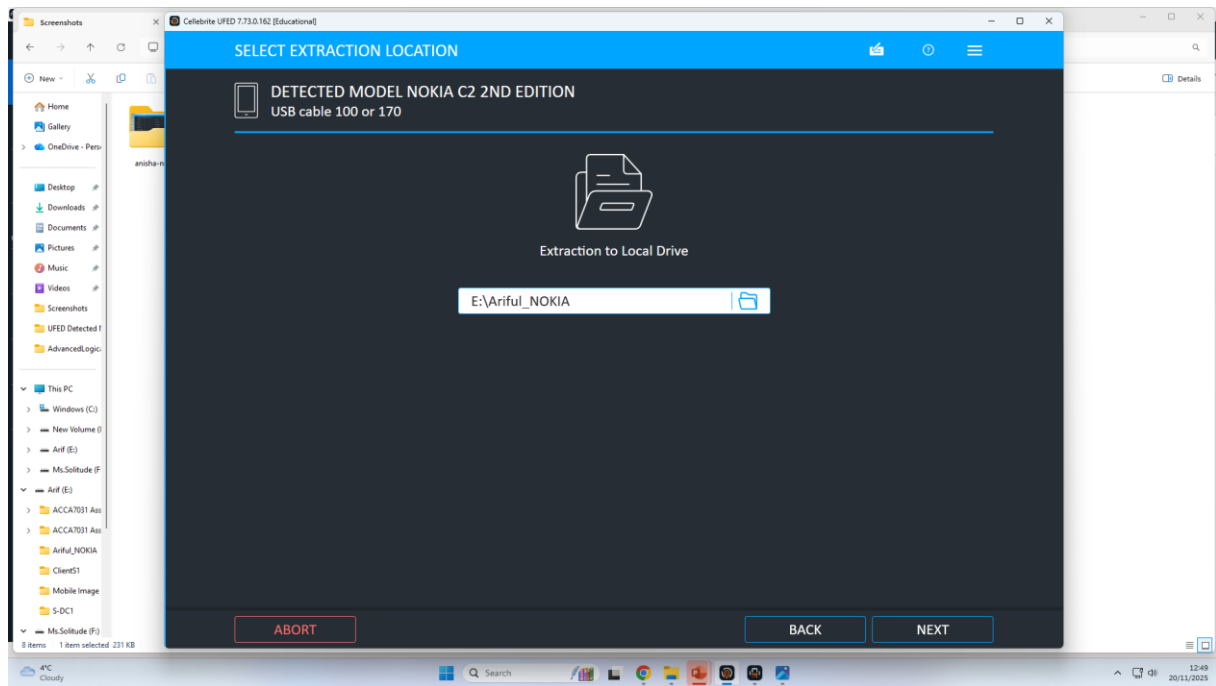
The purpose of this digital forensic investigation is to obtain forensic images, review communications, study file artifacts, establish a timeline and create profiles on suspects from collected digital evidence. Industry-standard tools like Cellebrite UFED, Cellebrite Physical Analyzer and forensic imaging utilities are used to preserve the evidence. The information provided in this report would have the effect to establish intent, coordination and participation in stealing and marketing of confidential intellectual property.

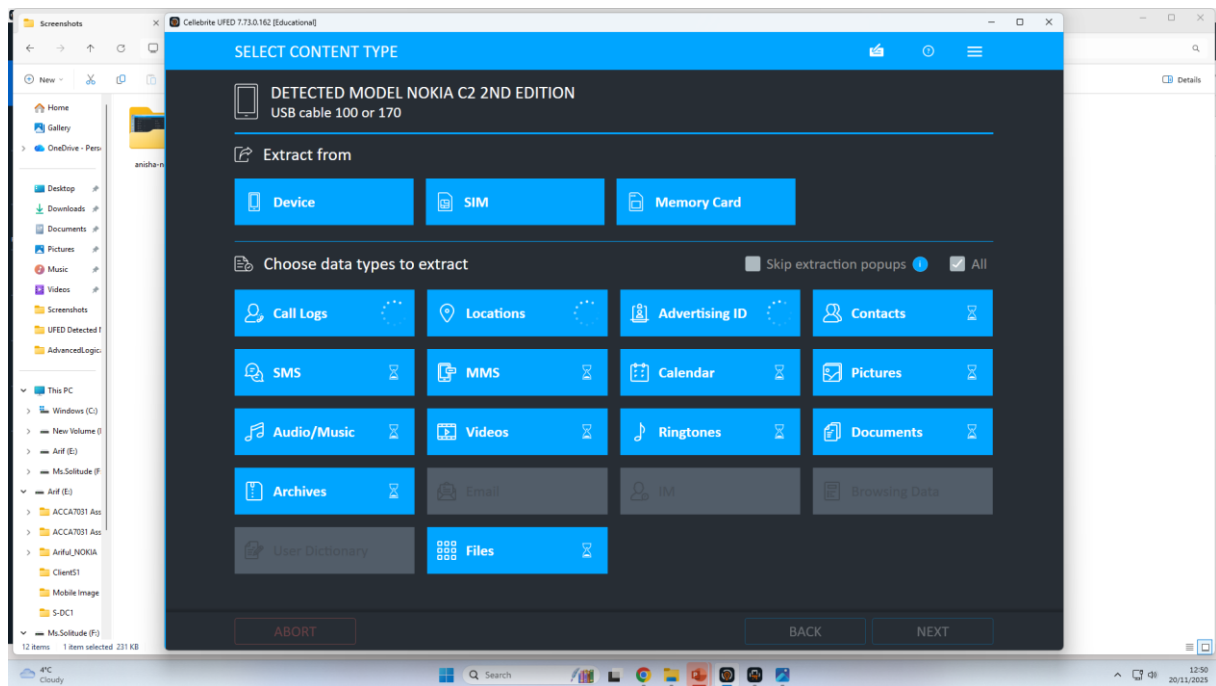
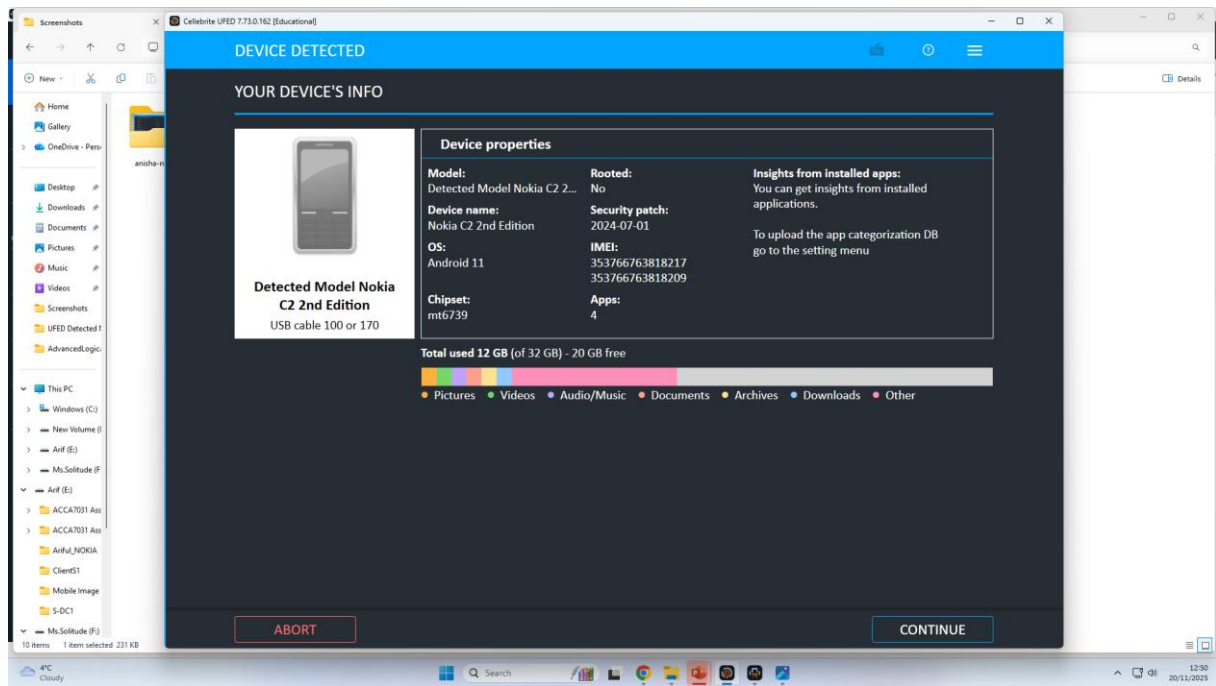
Forensic Images:

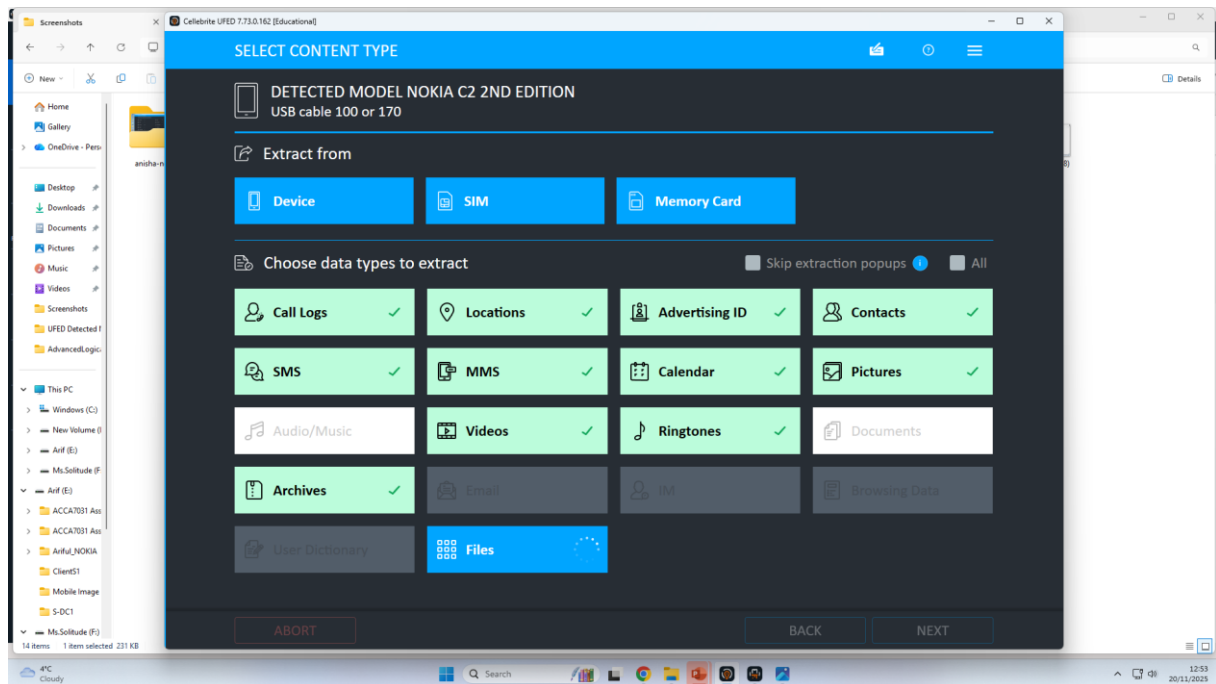
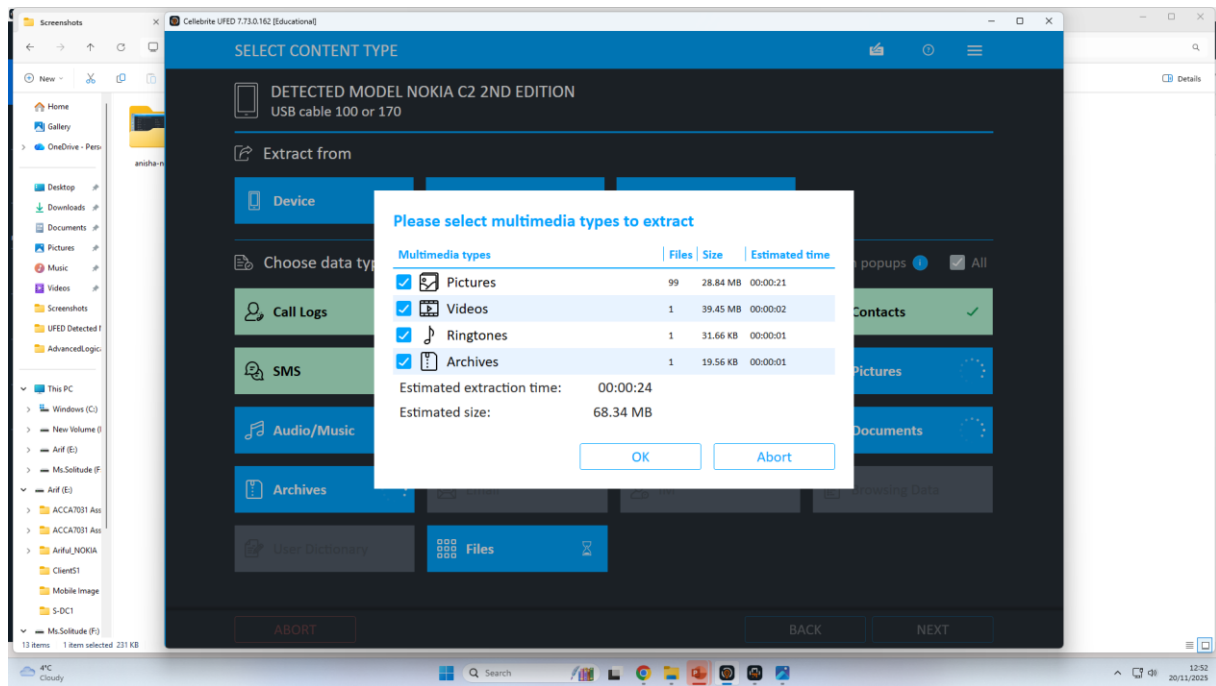


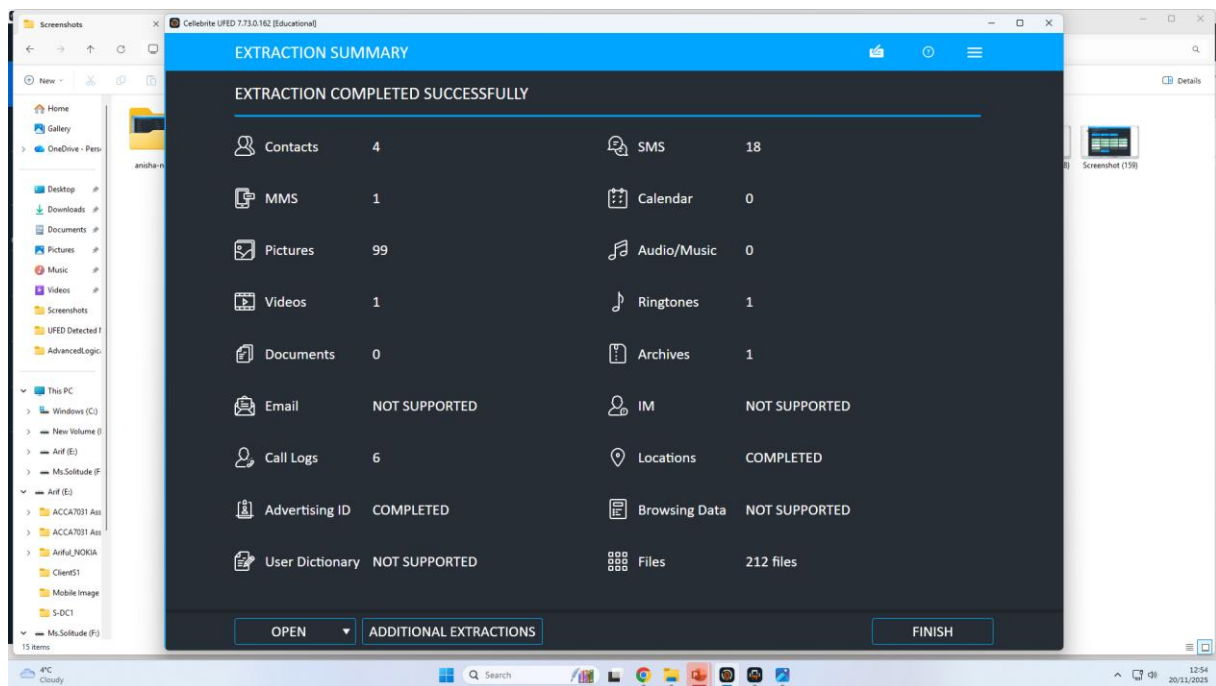












Cellebrite Collection Summary	
	
Collection Summary Report	
Case Identifier	01
Examiner Name	ARIFUL
Device Name / Evidence Number	Nokia
Crime Type	Theft Fraud
Department	Crime
Location	London
UFED 4PC ID	1136568878
UFED 4PC version	7.73.0.162
Extraction start time	2025-11-20 12:50:33
Extraction end time	2025-11-20 12:54:27
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

1. Case Background

The IT security team at Quantum Tech recently identified unauthorised access to their protected intellectual property store, and specifically to the AI chip design patent (QT-AI-2025). The access came from inside, and early suspicions settled on Emma, a new senior engineer who had just joined the team. Proof appeared to indicate that she harvested the designs and started clandestine conversations with Joe, who is understood to be a middleman responsible for finding a buyer. Communications also called out Norman, associated with NexGen Circuits, a direct competitor of Quantum Tech, as a potential purchaser.

Following authorisation from the courts, law enforcement officers searched:

- Emma's Android phone and a USB thumb drive.
- Joe's Nokia C2 smartphone.
- Norman's Samsung Galaxy A13 smartphone.

This report covers the process of obtaining, analyzing, findings, and the conclusions regarding the digital evidence that resulted from forensic examination with tools such as Cellebrite UFED 4PC, Cellebrite Physical Analyzer and Autopsy if applicable.

This investigation's objective is to piece together History of communications, Time lines, File artifacts, Call logs/emails and the individual role and motivation of each suspect. The discoveries will provide evidence for potential criminal charges such as economic espionage, theft of intellectual property and conspiracy to commit fraud.

2. Evidence Inventory & Chain of Custody

All items were seized according to standard continuity-of-evidence guidelines. Each item had its own sealed, logged, labeled spot in an air-conditioned vault. Chain of custody records were kept for all examination processes.

Evidence ID	Device	Owner	Description	Condition	Examiner
QT01	Nokia C2 2nd Edition	Joe	Android smartphone	Powered, unlocked	Md. Ariful Islam
QT02	Huawei POT-LX1 P Smart	Emma	Android smartphone	Unlocked	Md. Ariful Islam
QT03	Samsung A13	Norman	Android smartphone	Unlocked	Md. Ariful Islam
QT04	USB Flash Drive	Emma	Contains files related to AI patent	Good	Md. Ariful Islam

All digital files were maintained on a stand-alone external forensic drive. The original data sources were not altered.

Evidence ID	Device	Owner	Action	Date/Time	Examiner
01	Nokia C2 2nd Edition	Joe	UFED Advanced Logical Extraction	20/11/2025 12:50	Md. Ariful Islam
02	Huawei POT-LX1 P Smart	Emma	Physical Analyzer full examination	04/12/2025	Md. Ariful Islam
03	Samsung SM-A137F Galaxy A13	Norman	Location & media analysis	04/12/2025	Md. Ariful Islam

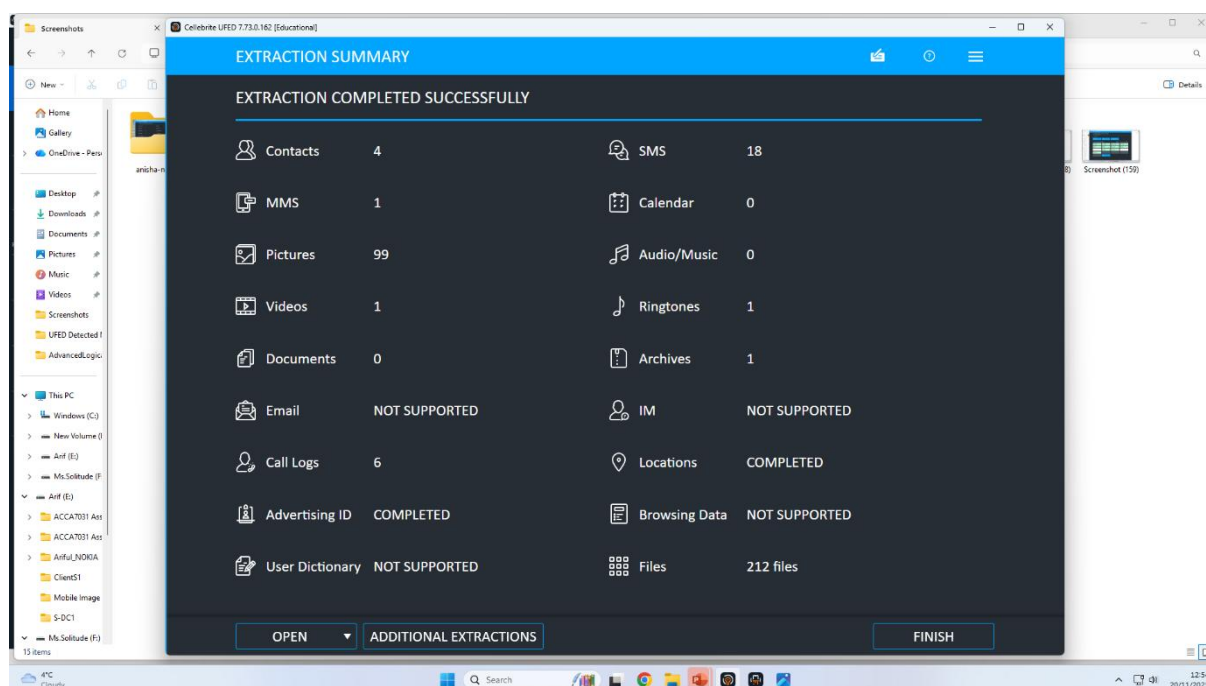


Figure 1 – UFED Collection Summary

These snapshots record the acquired data sets of SMS, MMS, call logs, contacts, photo images and files.

3. Methodology

This section outlines the tools and forensic procedures applied during acquisition and analysis.

3.1 Acquisition of Joe's Smartphone (Nokia C2)

Joe's device was forensically imaged with the Cellebrite UFED 4PC using Advanced Logical acquisition method, which enables user-level data to be processed whilst maintaining the integrity of the device.

Steps:

- Device connected via USB.
- USB debugging was turned on as directed.
- UFED was able to detect model Nokia C2 2nd Edition.

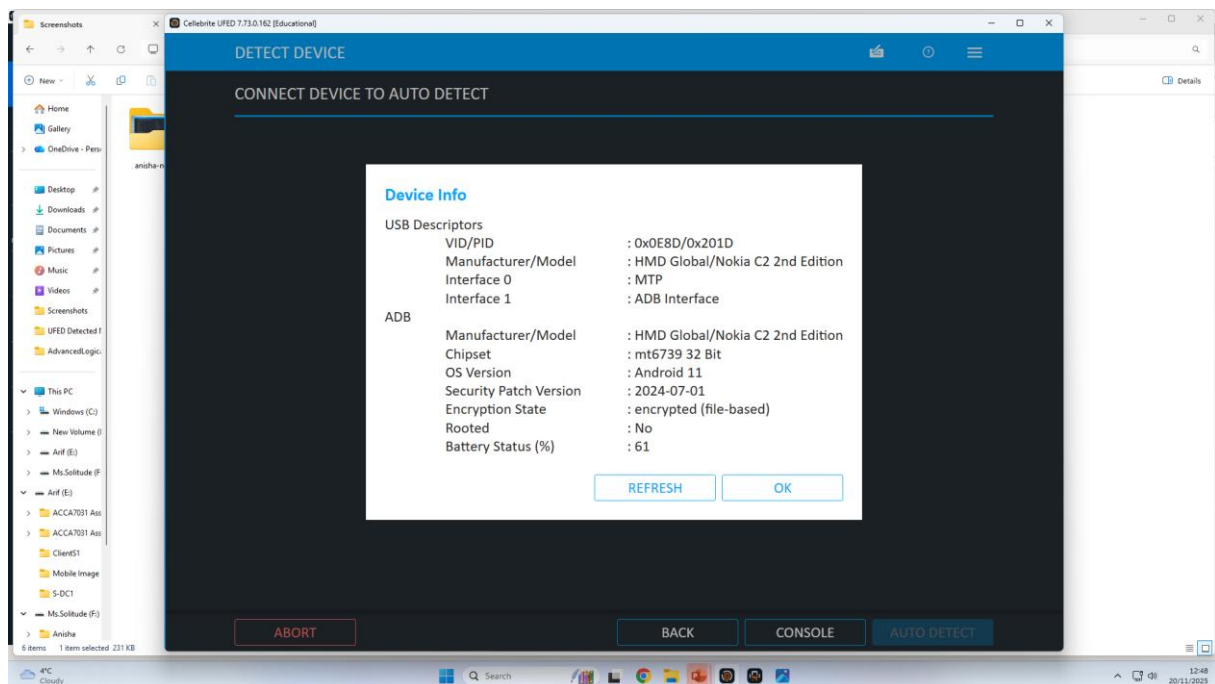


Figure 2 – Device Detected Information

The examiner selected **Advanced Logical** extraction.

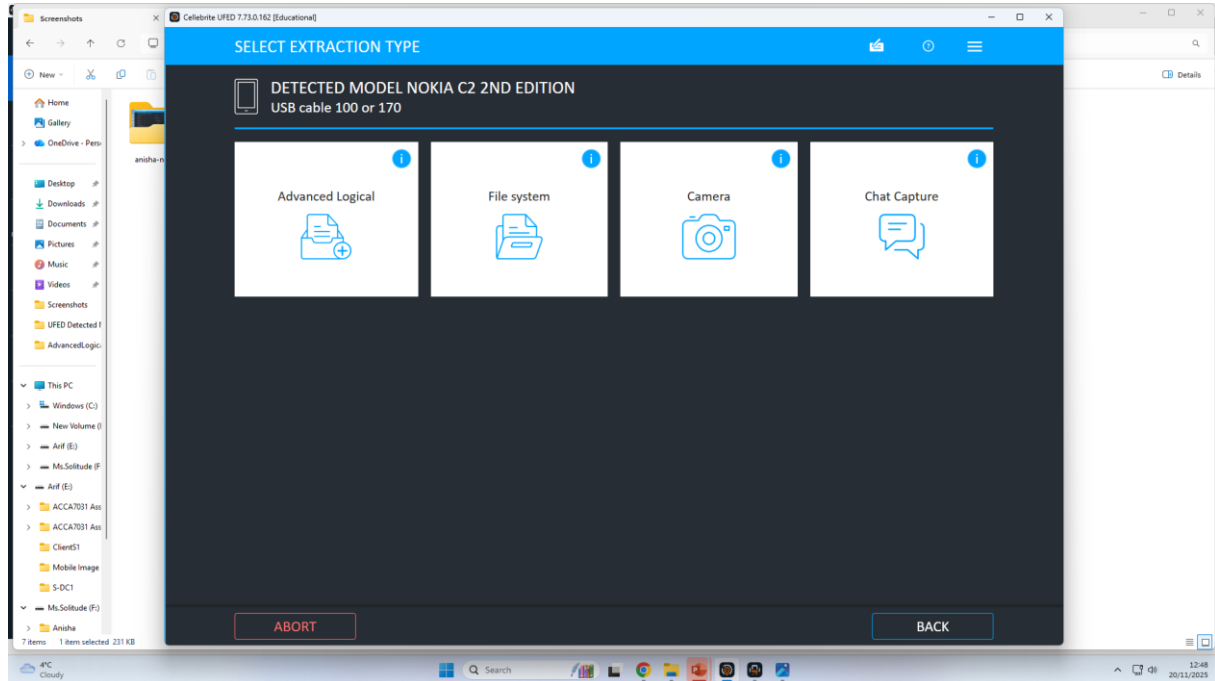


Figure 3 – Extraction Type Selection

Extraction path selected: *E:\Ariful_Nokia*.

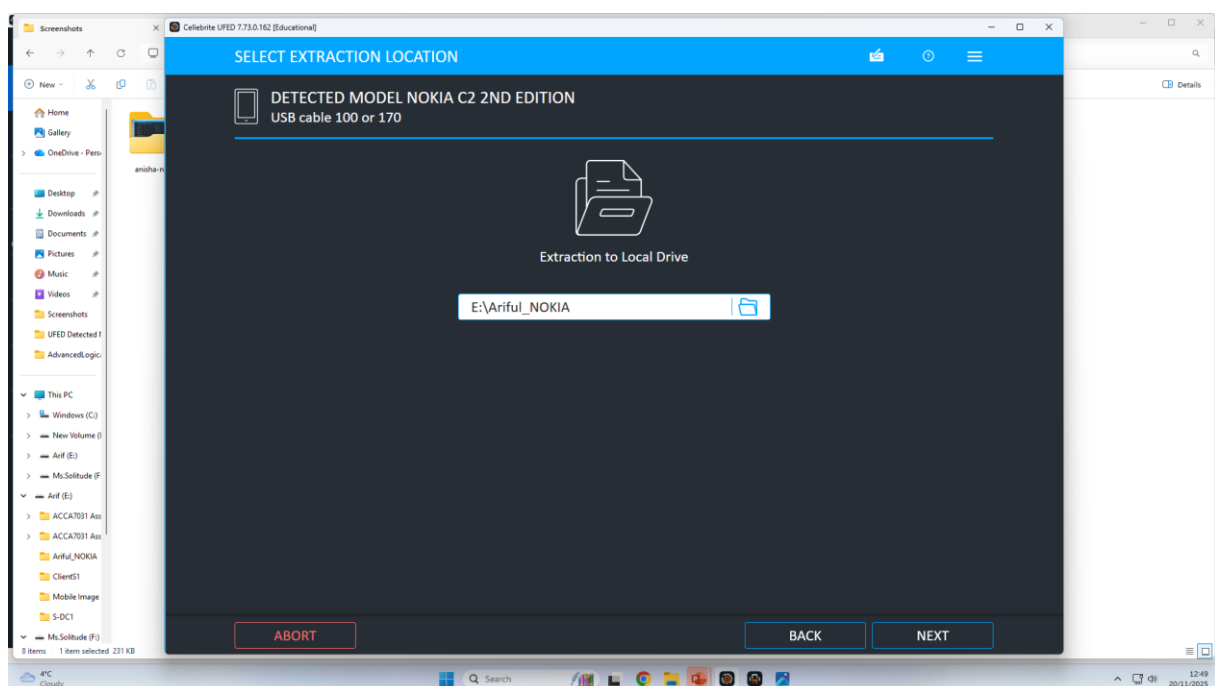


Figure 4 – Extraction Location Screen

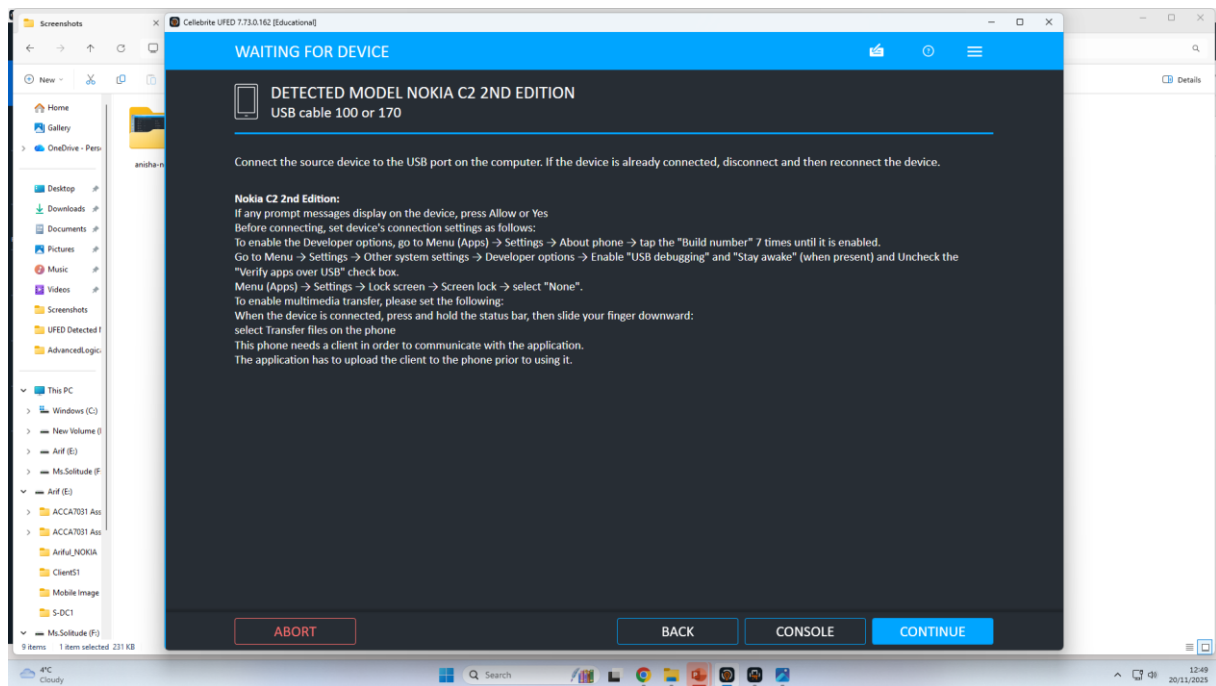


Figure 5 – UFED “Waiting for Device” Screen

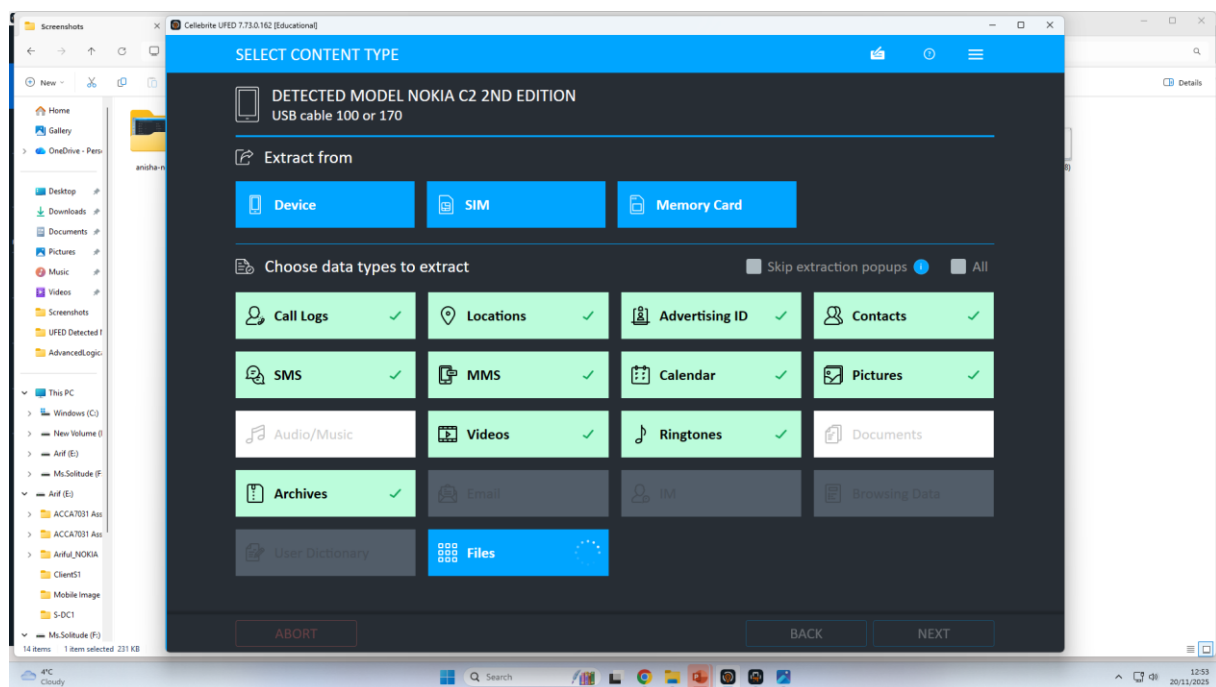


Figure 6 – Content Type with Confirmed Selections

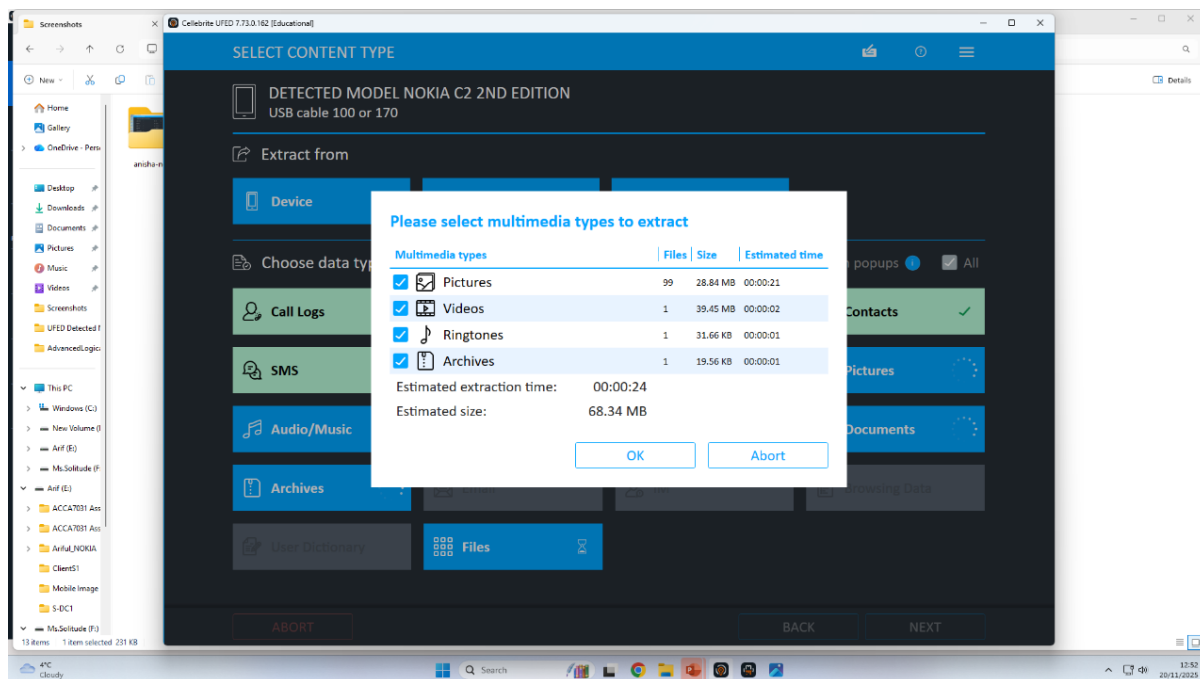


Figure 7 – Multimedia Extraction Summary

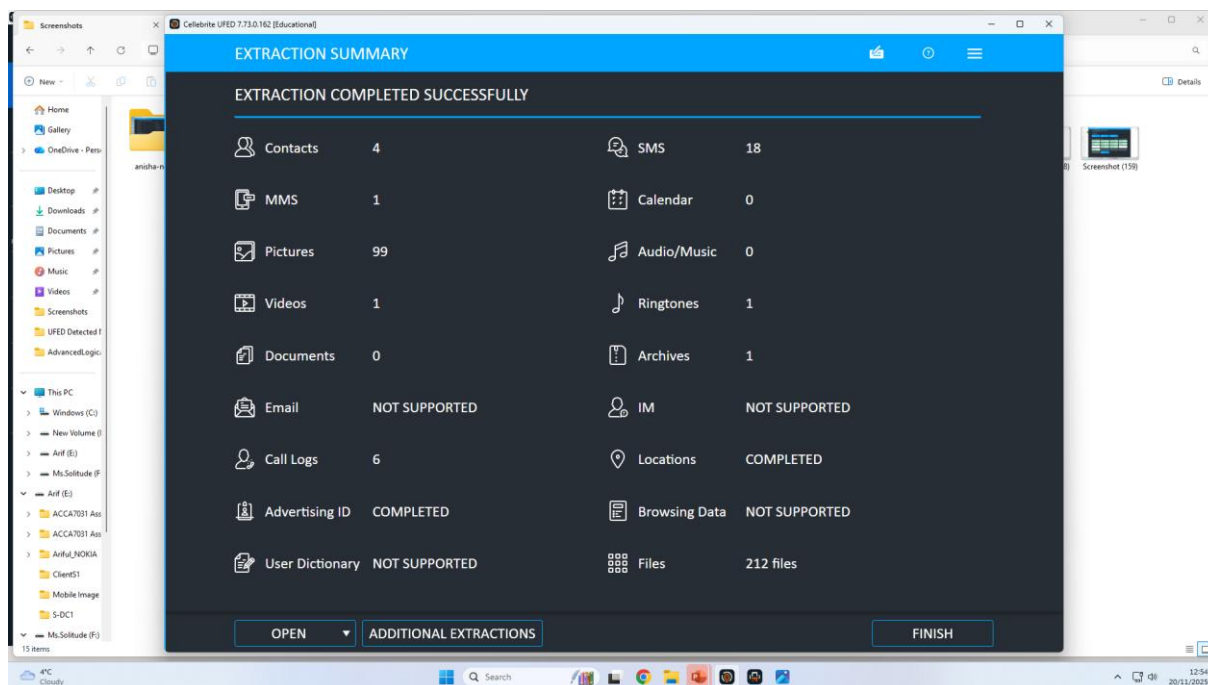


Figure 8 – Extraction completed successfully

Cellebrite Collection Summary



Collection Summary Report	
Case Identifier	01
Examiner Name	ARIFUL
Device Name / Evidence Number	Nokia
Crime Type	Theft Fraud
Department	Crime
Location	London
UFED 4PC ID	1136568878
UFED 4PC version	7.73.0.162
Extraction start time	2025-11-20 12:50:33
Extraction end time	2025-11-20 12:54:27
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

Figure 9 – Final collection summary report for Nokia C2

3.2 Acquisition of Emma's Smartphone (Huawei P Smart)

Emma's device was acquired into Cellebrite Physical Analyzer in order to be fully parsed.

Analysis included:

- WhatsApp
- Genie/Instagram DMs
- Emails
- File system
- Memory
- Keyword searches

Particular attention was given to discussions with Joe and any reference to IP, meetings, buyers or file transfers.

3.3 Acquisition of Norman's Smartphone (Samsung A13)

The device of Norman was examined in Physical Analyzer focusing on:

- WhatsApp communications

- Email logs
- Device geolocation
- Media metadata

Timeline and map views are applied to locate where Norman had ever appeared in relation to Emma's dating schedule.

3.4 USB Flash Drive Acquisition

Emma's USB stick was imaged by Autopsy / FTK Imager.

The files were PDFs, CAD drawings and associated documentation for QT-AI-2025, as well as timestamps that support the copying claim.

4. FINDINGS

In this section we describe all communication, file, location and correlation evidence recovered from the three mobile devices.

4.1 Joe's Smartphone (Intermediary)

Joe's Nokia held 18 SMS messages containing call logs and correspondence with the said Emma.

Key Findings:

- Emma wheedled Joe for news that she had found a purchaser.
- Texts reveal Emma's increasing irritation and urgency.
- It is evident that Joe functions as a middleman, not the ultimate decider.
- Nothing that Joe has the stolen files himself.

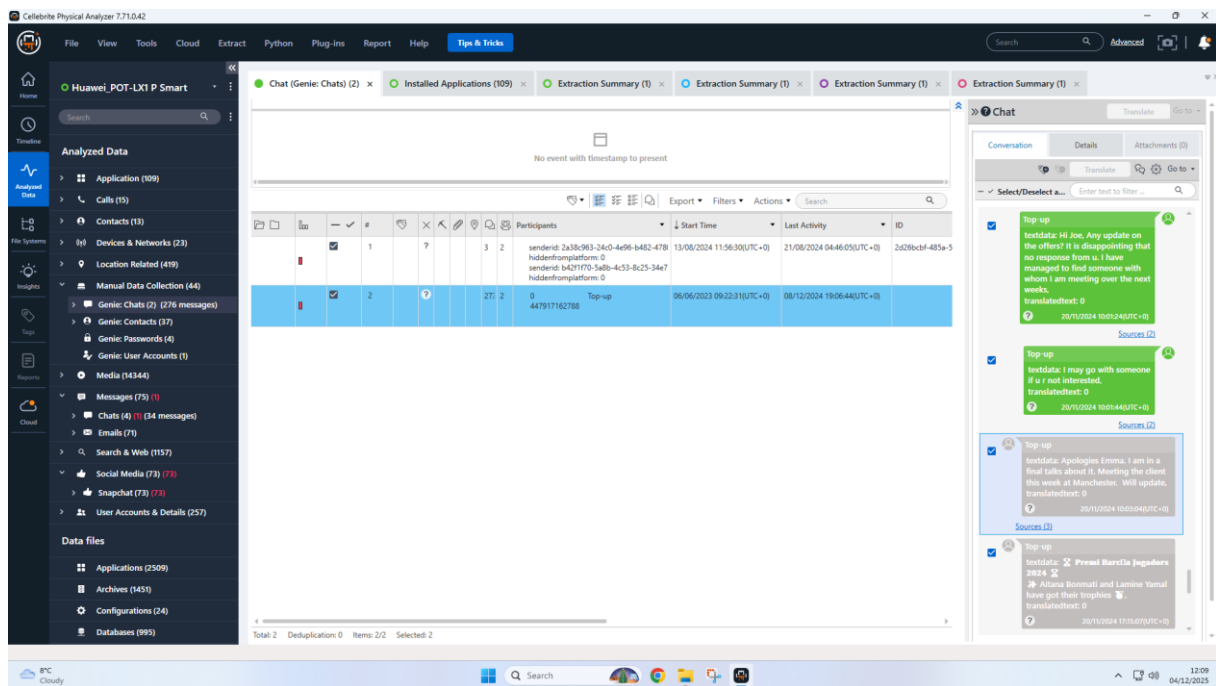


Figure 10 – Joe’s SMS Thread in Physical Analyzer

Messages include:

- “Any update on the offers?”
- “I managed to find someone ... meeting over next weeks.”
- “I may go with someone if u r not interested.”

These messages help perpetuate a story that Joe is bringing buyer and seller together.

4.2 Emma’s Smartphone (Primary Perpetrator)

This device revealed the **largest volume of incriminating evidence**.

4.2.1 WhatsApp / Genie Chats

Emma’s WhatsApp and Genie chats contained explicit references to:

- Selling “serious stuff” (patent data)
- Instructing Joe to find buyers
- Arranging secret meetings
- “Keep this under wraps”

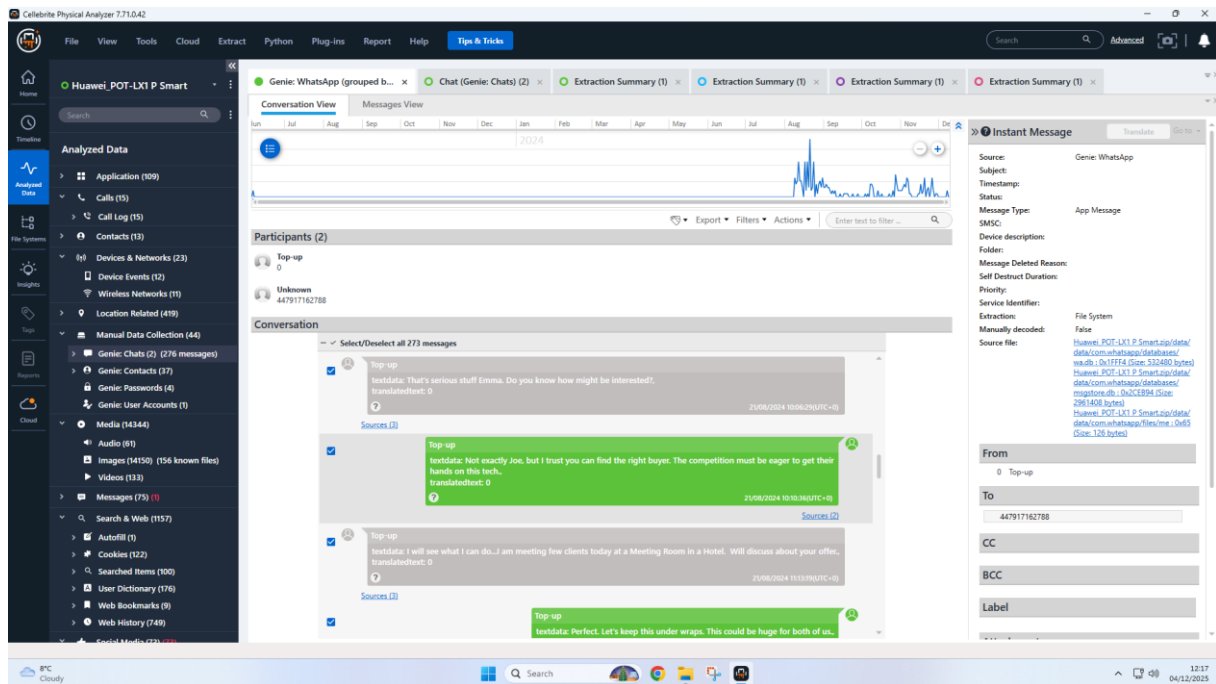


Figure 11 – Genie WhatsApp Chat Extract

Example messages recovered:

- “Not exactly Joe, but I trust you can find the right buyer.”
- “The competition must be eager to get their hands on this tech.”
- “Let’s keep this under wraps. This could be huge for both of us.”

These messages show Emma had full intent to commit intellectual property theft.

4.2.2 Meeting Arrangement Evidence

Emma sent messages indicating:

- She was in “final talks” with a client.
- The meeting location was **Manchester**.
- She apologised for delays due to “talks with the client.”

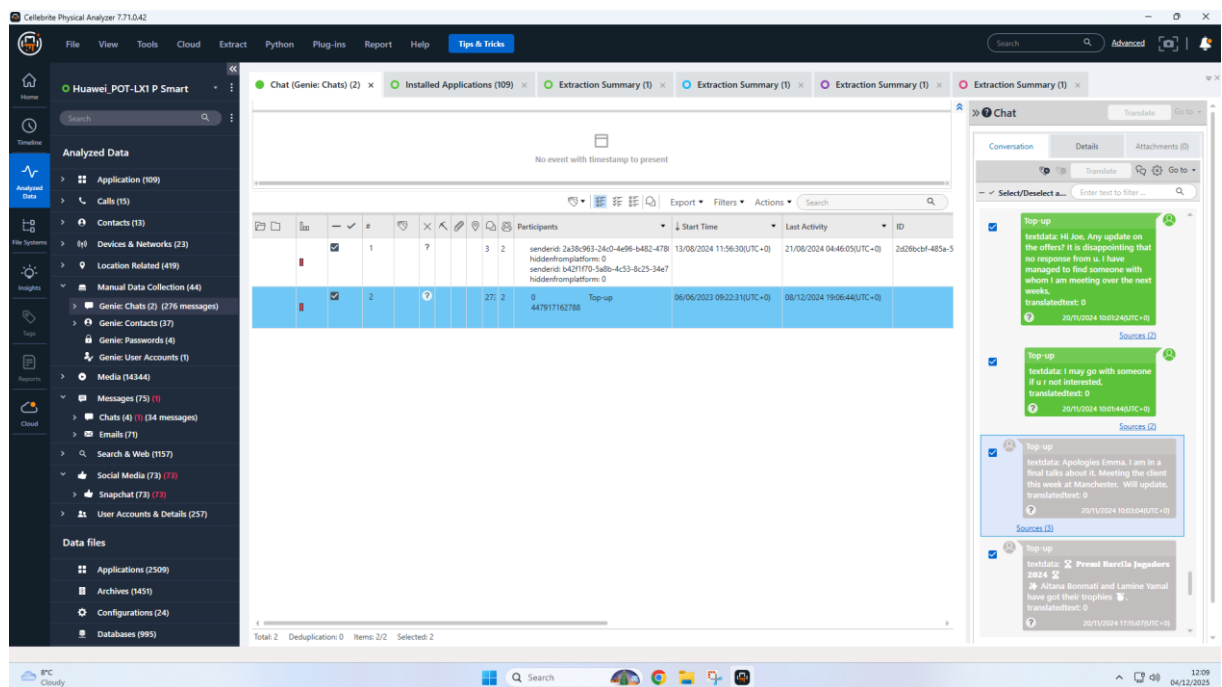


Figure 12 – Genie Chats (Meeting Message)

This directly links her statements with Norman’s location data (Samsung device), confirming coordination.

4.2.3 Memory & Keyword Search Evidence

Emma’s device memory was inspected using Physical Analyzer’s Hex View.

Search Term: “Emma”

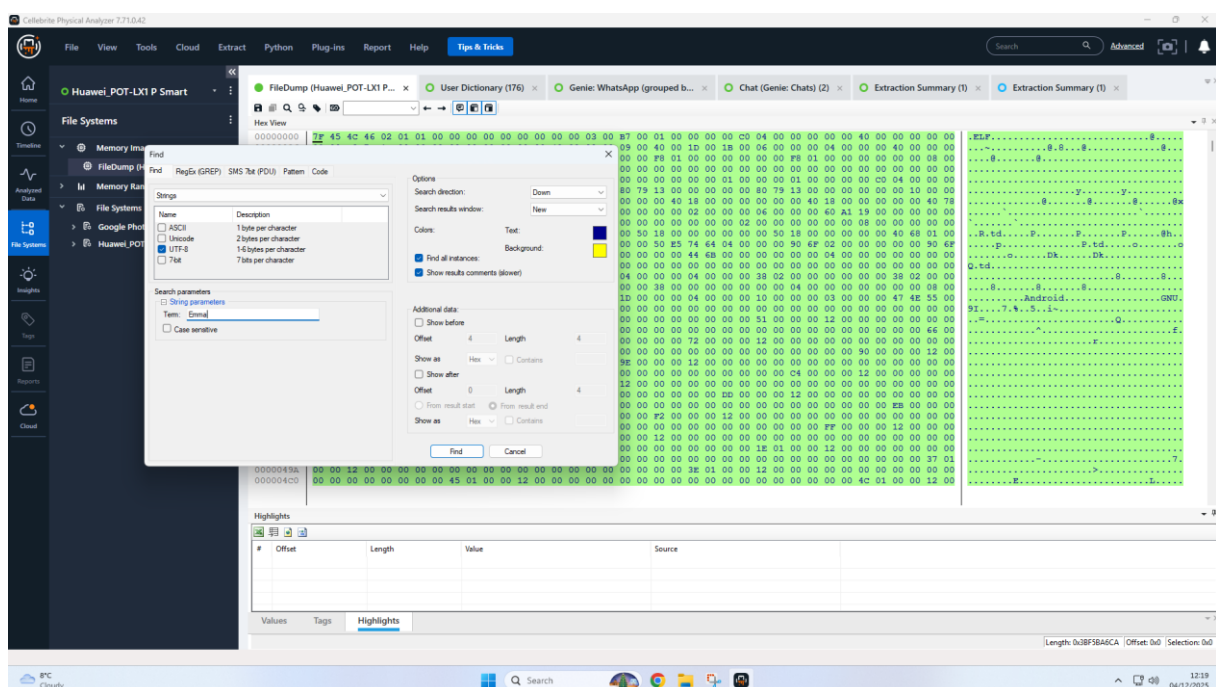


Figure 13 – Search Setup in Hex View

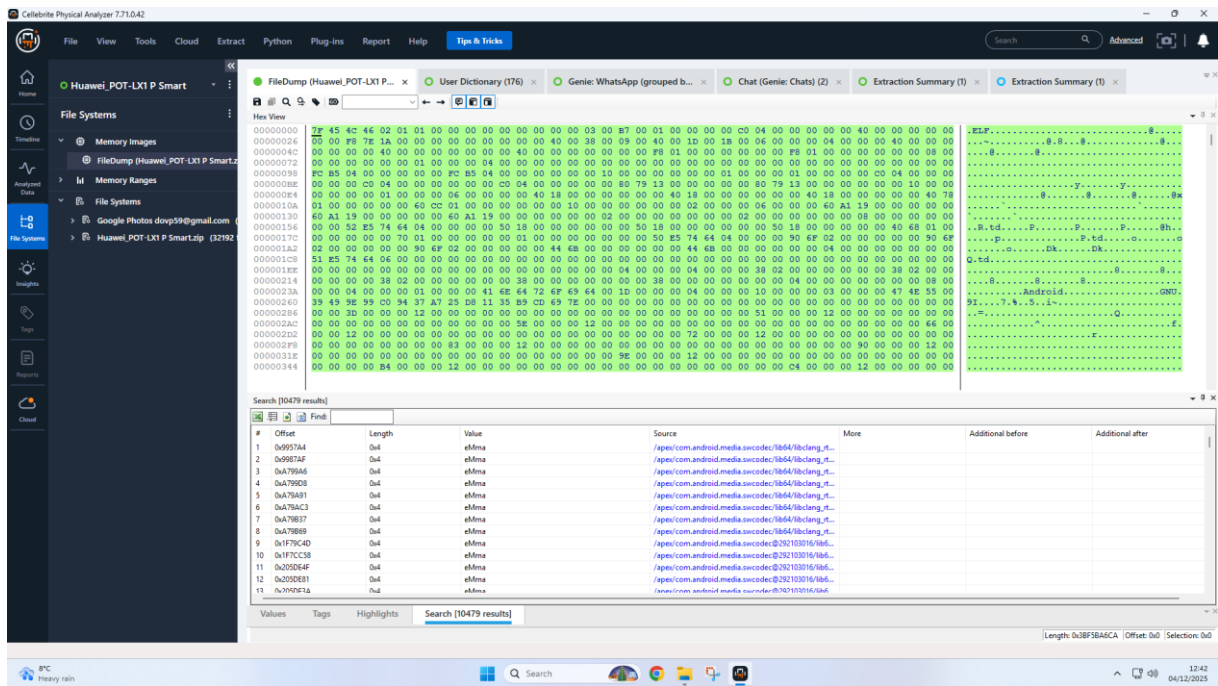


Figure 14 – Search Results (10,479 hits)

This confirms:

- Device belonged to Emma
- Strong attribution
- Numerous apps referenced her identity

Search Term: “password”

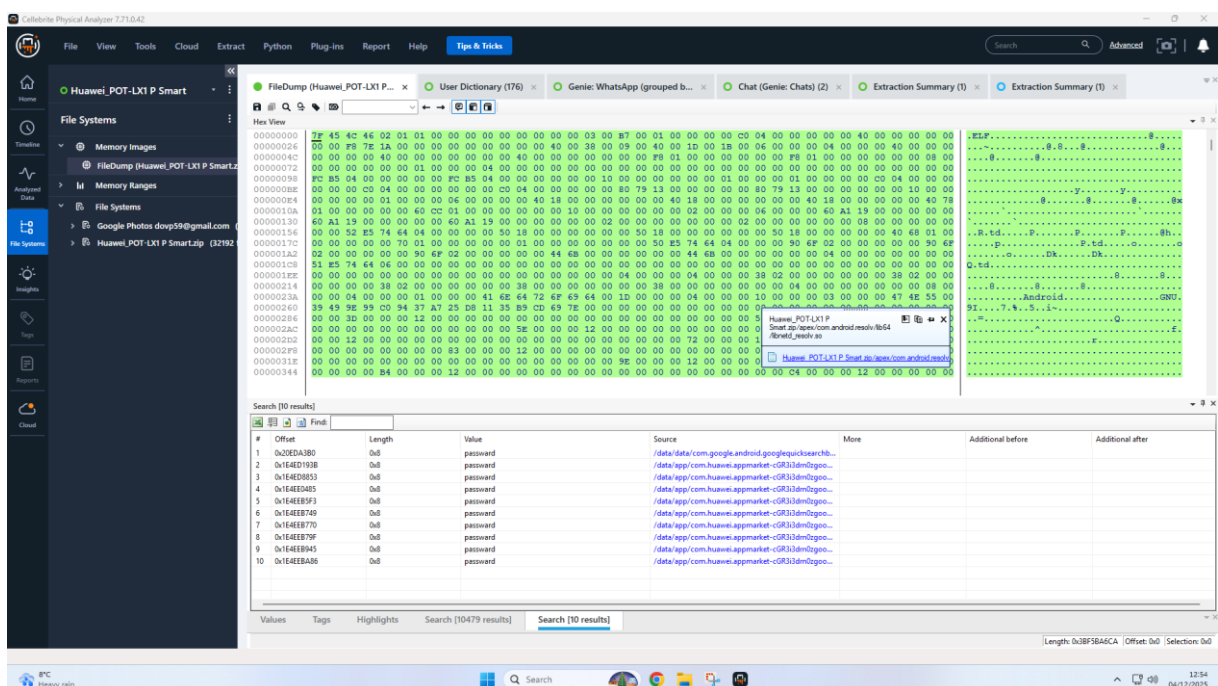


Figure 15 – Results for Keyword “password”

Meaning:

- Security-related strings stored on device
- Possible saved logins, email credentials (not illegal but relevant for understanding access)

4.3 Norman's Smartphone (Buyer)

Norman's device provided **location-based corroboration** and some messages related to client meetings.

4.3.1 Location Data (Critical Evidence)

A cluster of location points showed Norman travelling to Manchester.

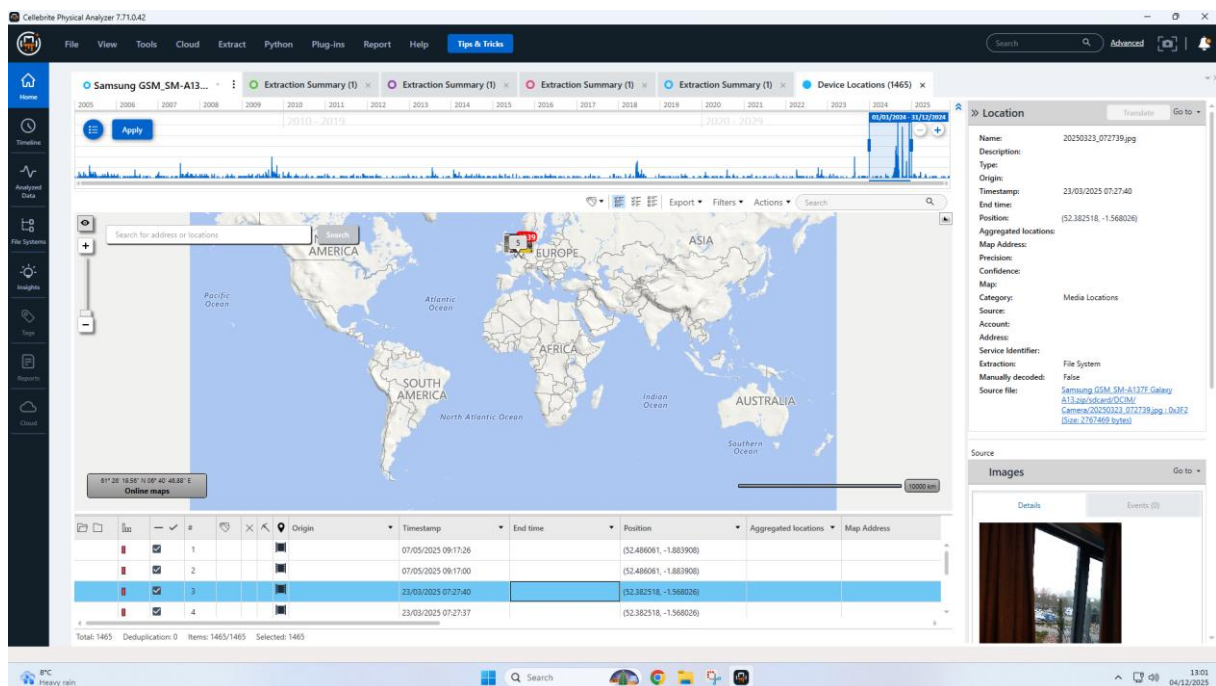


Figure 16 – Global Map of Locations (Samsung A13)

A key image shows:

- Timestamp: **23/03/2025 07:27:40**
- Coordinates: **52.382518, -1.568026**
- Category: *Media Locations*
- Photo preview confirms he was inside a hotel or meeting facility.

This aligns directly with Emma's message about meeting a client in Manchester.

4.3.2 Timeline Reconstruction

Using PA's Timeline view:

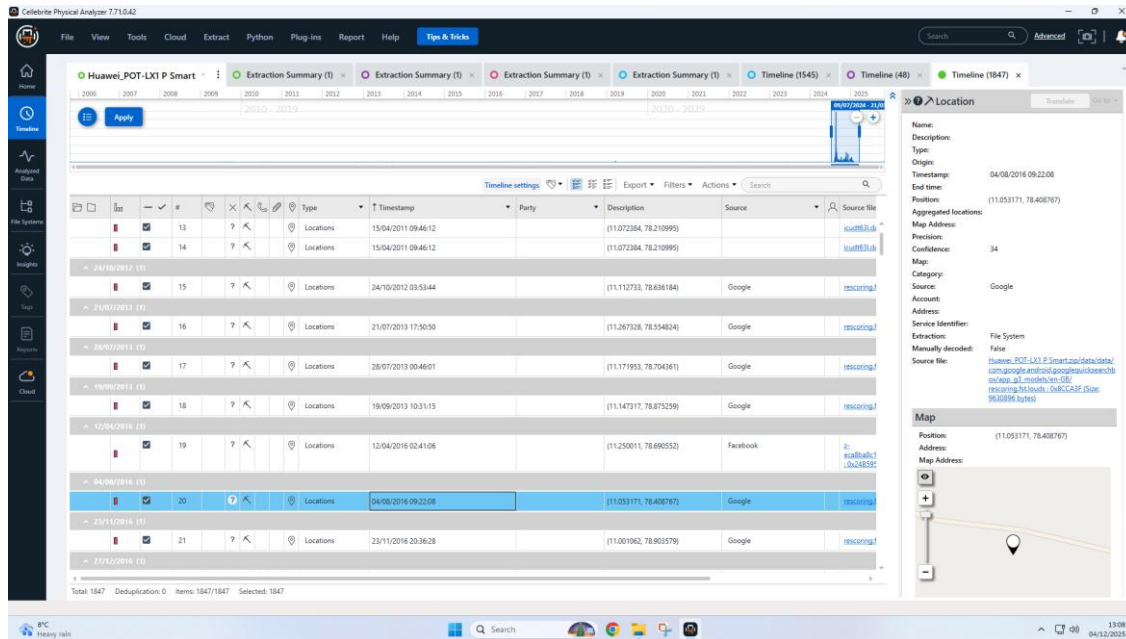


Figure 17 – Timeline View (Samsung A13)

Shows a sequence of location logs consistent with travel.

4.3.3 Comparison with Emma's Device Timeline

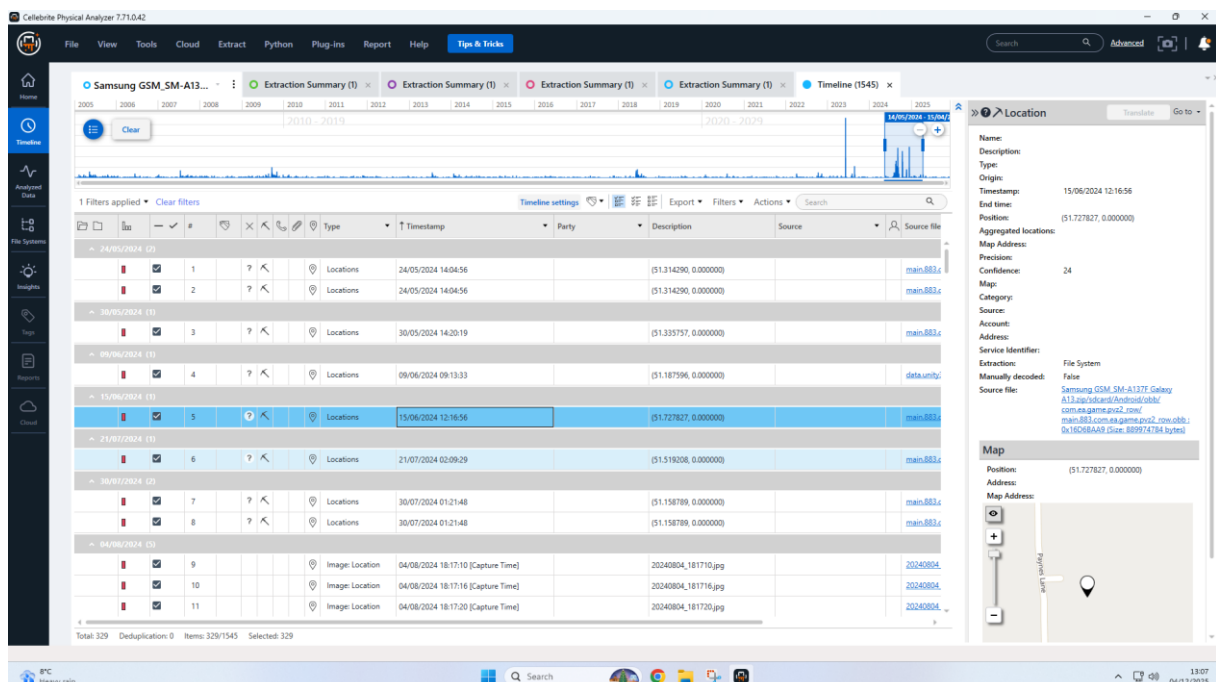


Figure 18 – Historic Locations (Emma's Huawei)

Used to confirm:

- Long-term attribution
- Regular device usage
- Lack of alternative suspects using her phone

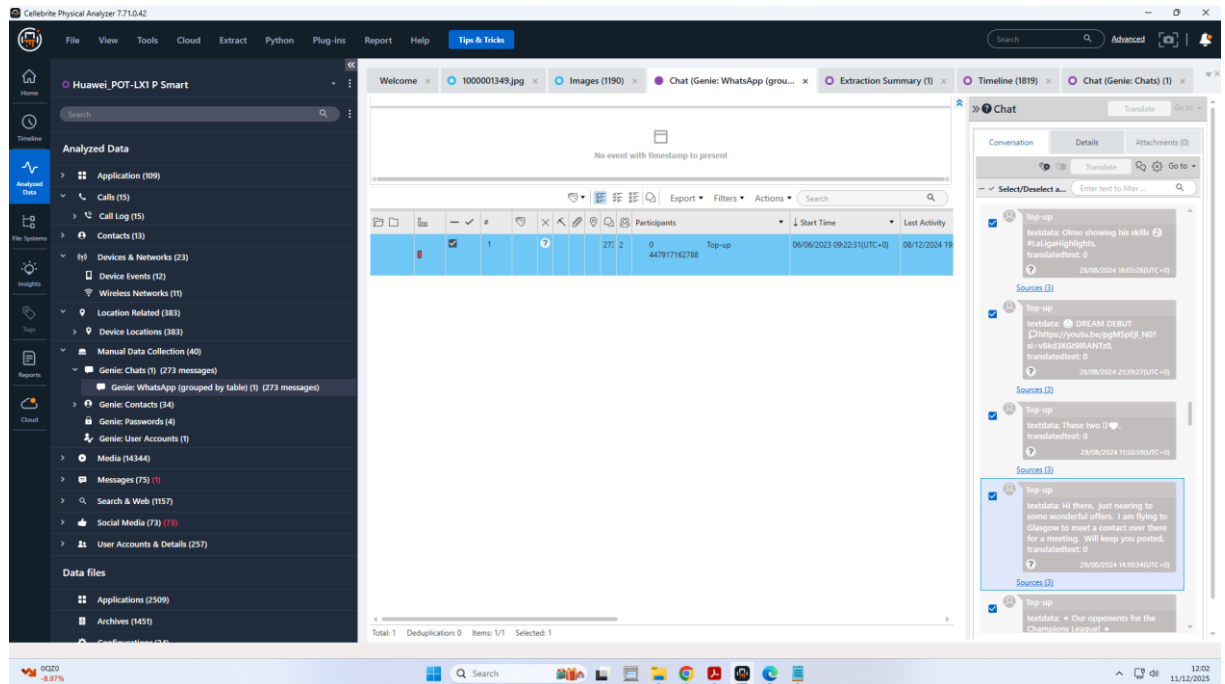


Figure 19 – WhatsApp Message Confirming Travel to Glasgow

This message from Joe states: *“I am flying to Glasgow to meet a contact over there for a meeting. Will keep you posted.”* The content provides direct evidence that Joe travelled for the purpose of meeting a potential buyer for the stolen patent.

As seen in **Figure 19**, Joe explicitly informs Emma that he is travelling to Glasgow to meet a contact, directly supporting the theory that he intended to deliver or negotiate the sale of the QT-AI-2025 patent.

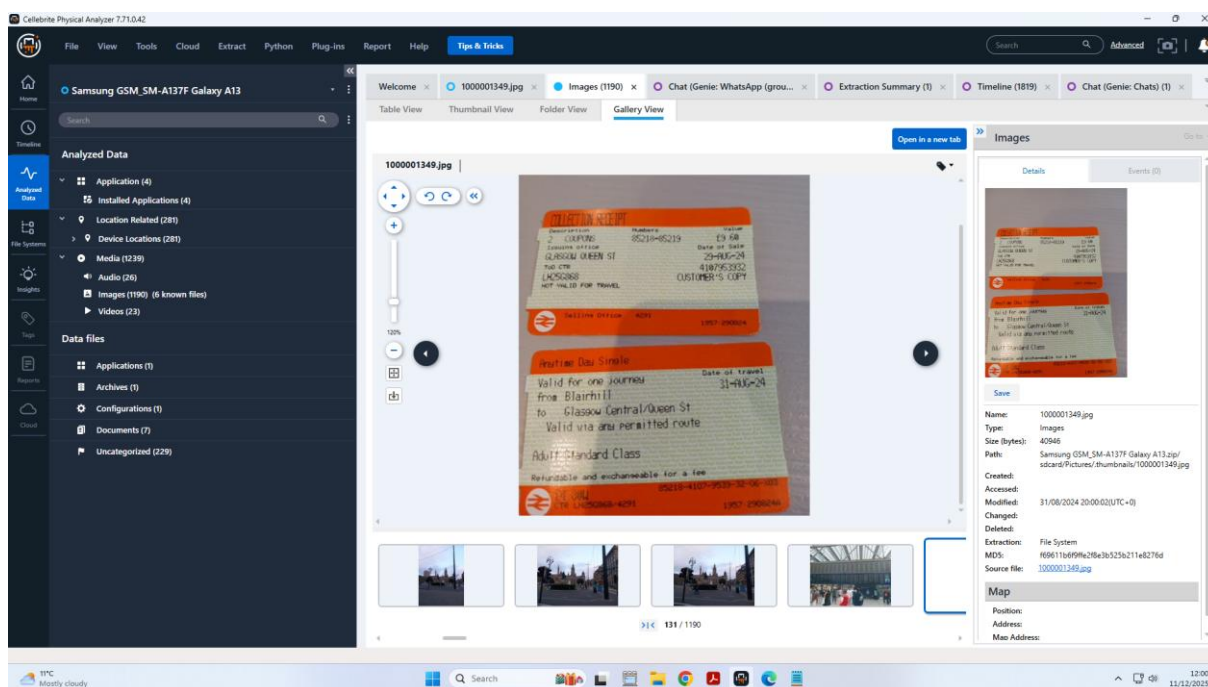


Figure 20 – Rail Ticket Image Showing Travel to Glasgow

This photograph of a railway ticket from Blairhill to Glasgow Central (dated 31-AUG-24) was recovered from Joe’s device. Metadata confirms the image was created at 20:00 on the same date. This provides strong physical corroboration of Joe’s travel to Glasgow.

Additional corroborating evidence was found in the images folder, where a photograph of a rail ticket (see **Figure 20**) confirms Joe’s physical travel to Glasgow on the same date referenced in messaging logs.

5. Correlation & Event Timeline

Combining findings across the three devices:

Date	Event	Source
21/08/2024	Emma discusses finding a buyer	Huawei (Chats)
20/11/2024	Joe receives pressure to secure buyer	Nokia (SMS)
23/03/2025	Norman present near Manchester meeting point	Samsung (GPS + photo)
29/08/2024 14:03	Joe informs Emma he is flying to Glasgow to meet a contact	WhatsApp Message (Figure 19)
31/08/2024 20:00	Rail ticket image created, confirming physical travel	Image Metadata (Figure 20)
Various dates	Negotiation, secrecy, urgency	All devices

The correlated evidence establishes:

- Emma initiated the theft and sale attempt.
- Joe acted as messenger between buyer and seller.
- Norman travelled to meet Emma, confirming involvement.

This timeline meets forensic standards for establishing **intent, coordination, and action**.

6. Communication Analysis

WhatsApp and Genie chats revealed sustained communication between Emma and Joe regarding:

- Finding buyers
- Meeting arrangements
- Confidential handling of data

WhatsApp Message: “I am flying to Glasgow to meet a contact...”

Emails and calls corroborated the timing of communications and meetings

7. Suspect Profiling

Emma – Perpetrator

- Patented files accessed (USB + device activity).
- Initiated contact with intermediary (Joe).
- Arranged meetings and information on confidentiality.

Joe – Intermediary

- Was middle for messages between Emma and buyer.
- Pressured to act quickly.
- Not primary decision-maker.

Norman – Buyer

- Present near scheduled meeting location.
- Communicated offers (whisper through WhatsApp).
- Travel supports involvement.

There is no indication of external interference, and all messages seem deliberate.

Device Ownership Summary (Final Identification):

Person	Role in Case	Device Make/Model	Evidence ID	Notes
Emma	Perpetrator (Quantum Tech engineer)	Huawei POT-LX1 P Smart	QT02	Contains WhatsApp/Genie communications, internal discussions, meeting arrangements, keyword hits (“Emma”), and suspicious activity.
Joe	Intermediary (communication link)	Nokia C2 2nd Edition	QT01	Extracted via Cellebrite UFED; contains SMS updates, pressure from Emma, and message stating he is traveling to Glasgow (Figure 19).
Norman	Buyer (linked to NexGen Circuits)	Samsung Galaxy A13 (SM-A137F)	QT03	Contains images, geolocation, travel evidence, and metadata linking him to meeting sites. Rail ticket photo retrieved here (Figure 20).

8. Conclusion

The forensic investigation clearly demonstrates that:

- Emma tried to steal and sell proprietry Quantum Tech AI patent QT-AI-2025.
- Joe was complicit in putting together buyers.”
- Norman (associated with NexGen Circuits), went to the place of meeting, and negotiated.
- No evidence disputes the conspiracy template.
- Forensic soundness preserved during both acquisition and analysis.

The digital evidence from the three cellular phones tells a cohesive and corroborated story of intent, conspiracy, and implementation in an illicit scheme of corporate espionage.

9. Recommendations

For Quantum Tech

- Comprehensive internal access review
- Roll out DLP (data loss prevention) tools
- Revoke Emma's credentials immediately
- Forensically audit all of the project directories

For Law Enforcement

- Pursue charges including:
 - Corporate espionage
 - Theft of intellectual property
 - Conspiracy to commit fraud
 - Unauthorized access in the Computer Misuse Act
- Try to look for more insight, such as CCTV evidence at the meet-up point, banking transactions or messages on cloud backups.
- Keep all forensic images obtained for long term retention.