

Student Name:- Rajnik Pravinbhai Radadiya

Student Number :- 2433479

Module:-Digital Forensics Analysis

Module Code:- ACCA7004_LON

Table of Contents

Task 1	5
1.1 Introduction	5
1.2 Current State of the Field/Tools	5
1.3 Intersection between Digital Forensics & Cybersecurity	6
1.4 Emerging Trends of Digital Forensics	6
1.5 Key Challenges	7
1.6 National & International Working Market	8
1.7 Conclusion	8
References	9
Task 2	11
1. Case Background	11
2. Evidence Inventory	13
2.1 Devices Seized:	13
2.2 Chain-of-Custody:	18
2.3 Hash Verification:	18
3. Methodology	19
3.1 Acquisition Process	19
3.2 Analysis Tools	20
4. Findings	21
4.1 Analysis of the Artefact of Communication	21
4.2 Correlation of Call-Log and Behavioral Indicators	22
4.3 Communication Logs Analysis	22
4.4 Call Logs and Emails	24
4.5 Communication Extraction (WhatsApp, Instagram DMs, Emails)	25
4.6 File Analysis (Patent Files)	28
4.7 Metadata Inspection (File Access and Modification)	29
5. Suspect Profiling	30
5.1 Joe (Perpetrator)	30
5.2 Emma (Intermediary)	30
5.3 Norman (Buyer)	31
5.4 Evidence Interpretation	33
5.5 Behavior Analysis	36
1. AppGenie Selection and Chat Apps (Figure 1):	36
2. WhatsApp Top-up Messages (Figure 2):	37
3. Extraction Summary for Huawei (Figure 3):	38
4. Genie Chat Conversation (Figure 4):	39

<i>5. Hex Search in Samsung Image (Figure 5):</i>	<i>39</i>
<i>6. Image Gallery with Bank Card (Figure 6):</i>	<i>40</i>
<i>7. Travel Information Board Image (Figure 7):</i>	<i>41</i>
<i>8. Train Ticket and Locations (Figure 8):</i>	<i>42</i>
<i>6. Conclusion</i>	<i>43</i>
<i>6.1 Evidence Summary</i>	<i>43</i>
<i>6.2 Crimes Identified</i>	<i>47</i>
<i>7. Recommendations</i>	<i>48</i>
<i>7.1 Legal Actions</i>	<i>48</i>
<i>7.2 Quantum Tech's Security Measures</i>	<i>48</i>
<i>References</i>	<i>49</i>
<i>Appendices</i>	<i>51</i>
<i>Appendix A – Chain of Custody Documentation</i>	<i>51</i>
<i>Appendix B – Hash Verification Log</i>	<i>51</i>
<i>Appendix C – UFED Extraction Records and Logs</i>	<i>52</i>
<i>Appendix D – Event Timeline Reconstruction Chart</i>	<i>55</i>
<i>Appendix E: Celebrate Analysis of My Phone</i>	<i>57</i>
<i>Appendix F: Evidence Interpretation</i>	<i>58</i>

1.1 Introduction

Digital forensics has played a pivotal role in modern day cyber investigative light of the surge in the deal of cybercrime, misuse of the insiders that have resulted and litigation involving digital forensics [6]. It combines technical, legal and investigative processes that are aimed at locating, preserving, analysing and interpreting electronic data. The growing reliance on cloud service, mobiles, IoT environments and encrypted applications has expanded the scope and intricacy of forensic work [21].

1.2 Current State of the Field/Tools

Digital forensics therefore has shifted from its traditional heritage of disk analysis to become a broad-based area consisting of mobile, cloud, network, memory and IoT and malware forensics [18]. Evidence is now being encountered throughout distributed systems, SaaS platforms, messaging applications and virtual infrastructures which means that investigators need to be able to regulate and manage fragmented, encrypted and volatile datasets [20]. Core frameworks such as NIST SP-800-86 are in place to ensure forensic integrity, chain-of-custody and repeatability [19] and the ACPO guidelines.

The use of commercial tools constitutes the gist of modern investigations. Cellebrite UFED supports logical acquisition, file systems with acquisition and physical. 3D and 360 degree support include detailed mobile app support and encrypted support. Magnet AXIOM has integrated analysis in computer, cloud, and mobile environment with good correlation and automatic timeline functionality [16]. FTK still currently is most popular in disk imaging, registry analyzing, and email parsing X-Ways has extremely efficient file system examination [5].

Open-h Source tools continue to be critical also. Autopsy and SleuthKit including disk forensics, keyword search and timeline reconstruction [3]. Volatility is the most popular framework when it comes to memory forensics, which offers the capability of detecting malware, as well as process analysis, and recovery of volatile artefacts [24]. LiME provides mobile memory acquisitions capacity while Wireshark is used to aid network traffic inquire [2].

Critical comparison is, however, important to good forensic work. For example, while Cellebrite is included to provide deep devices extraction compatibility, AXIOM has broader cross platform correlation and better artefact parsing of cloud files [16][7]. Despite their strengths, tools do have limitations because of effective encryption, as well as fast software update [14].

1.3 Intersection between Digital Forensics & Cybersecurity

Digital forensics and cybersecurity are now working hand in hand by DFIR (Digital Forensics and Incident Response) where prevention and detection goes hand in hand with investigation and attribution [22]. Cybersecurity teams rely on forensic methods to get insights on the root cause of breaches, to identify the behaviour of hackers, analyse insider threats and respond to ransomware campaigns [23]. SOC operations are based on forensic processes such as endpoint triage, log correlation and analysis of persistence mechanism.

This intersection is being further reinforced by the move to cloud. Cloud forensics requires knowing IAM logs API Events and virtual disk snapshots, a situation in which attacks can be reconstructed [17]. Zero Trust security models (which are now widely adopted) generate copious amounts of logging that have to be analysing using forensic methodologies [4]. The real world cases of ransomware hacking indicate how the forensic analysis plays an important role in attribution and legal prosecution [13].

1.4 Emerging Trends of Digital Forensics

Cloud forensics still have expanded reasons because of the increase of the adoption of cloud but with challenges related to decentralised storage and no physical access [20]. AI and machine learning techniques have been devised to aid in automated artefact detection, anomaly detection and triage [1]. Mobile and app Forensics are becoming increasingly complex as a response to Encrypted Messaging Platform and Application Updates [14]. IoT forensics is increasing as these smart devices are being established more and more, however there are some challenges due to a lack of standardisation [12].

1.5 Key Challenges

Encryption and security messaging technology like WhatsApp, Signal and Telegram has made it hard to acquire data except for cloud back ups or the ability to acquire data live [14]. Staging and ephemeral messaging and volatile records a part in reduction the dispersion of evidence. Data volume is another great challenge especially in enterprise environments producing massive amount of logs and cloud artefacts [21]. Jurisdictional issues are an issue since the data stored on the cloud are stored in different countries [16]. Anti-forensic techniques, which aids to secure file from survivors of child and security, is under continuous growth [6].

Jurisdictional conflicts arise from data residing in geographically dispersed cloud servers across multiple countries, complicating legal authority for acquisition and compliance. Meanwhile, anti-forensic techniques, designed to evade detection or tamper with digital evidence, continuously evolve, presenting persistent obstacles to forensic investigators. Additional challenges include rapidly evolving technologies requiring constant tool and skill updates, lack of standardization across forensic methodologies especially for emerging IoT devices, and the need for forensic readiness in organizations to ensure timely data preservation.

Challenge	Description	Impact
Encryption & Secure Messaging	Access limited to cloud backups/live capture	Limits data availability
Ephemeral Messaging	Temporary/deleted records reduce evidence	Reduces usable evidence
Data Volume	Massive logs and cloud artifacts complicate analysis	Strains storage and processing resources
Jurisdictional Issues	Data hosted across multiple legal jurisdictions	Legal acquisition difficulties

Anti-Forensic Techniques	Tools employed to evade or alter evidence	Threatens integrity of investigations
Rapid Technology Evolution	Constantly updates required for tools and skills	Challenges investigator preparedness
Lack of Standardization	Variation in processes across devices, especially IoT	Hinders consistent forensic practices
Forensic Readiness	Need for proactive data preservation and incident response	Critical for timely and effective analysis

1.6 National & International Working Market

In the UK, because of the growing levels of cybercrime, compliance requirements (GDPR) and corporate security requirements, there is a growing need for digital forensic expertise [10]. There are jobs with the Police forces, the National Criminal Agency, consultancy companies and financial institutions. Internationally the United States still has the largest DFIR market in the world with high demand from federal agencies and private security organisations [15]. Rapid expansion is also recorded in the Middle East due to the national cyber strategy in Saudi Arabia and the UAE [4]. Asia -- particularly India, Singapore and South Korea -- has good growth in terms of mobile, cloud and incident response forensics [11]. Certifications such as GCFA, GCFE, CHFI, EnCE and CFCE open up more jobs. Workforce reports tell us there is currently a major talent shortage across the world in DFIR positions [9].

1.7 Conclusion

Digital forensics is an integral part of mitigating cyber threat and the investigations and legal proceedings [6]. The field is still evolving in the form of cloud environments, mobile environments, IoT environments, and AI supported environments. Despite progress, there are large

challenges left - such as security encryption, scale of data and jurisdiction [21]. The global job market indicates that there is still great need for sophisticated forensic capabilities, both in the public and the private sector [15]. Continued research and innovation, as well as creating a robust workforce, will be needed to enable the development of the field of digital forensics in an evolving technological landscape [22].

References

- [1] H. Alqahtani and A. Jones, “A review of AI-driven approaches in digital forensics,” *Journal of Digital Forensics, Security and Law*, vol. 16, no. 2, pp. 1–20, 2021.
- [2] C. Altheide and H. Carvey, *Digital Forensics with Open Source Tools*, 2nd ed. Waltham, MA, USA: Syngress, 2018.
- [3] Autopsy, *Autopsy Forensic Browser Documentation*. Basis Technology, 2022. [Online]. Available: <https://www.autopsy.com>. [Accessed: Nov. 18, 2025].
- [4] Accenture, *State of Cybersecurity and Digital Forensics Report*. Accenture Security, 2023. [Online]. Available: <https://www.accenture.com>. [Accessed: Nov. 18, 2025].
- [5] B. Carrier, *File System Forensic Analysis*, 2nd ed. Boston, MA, USA: Addison-Wesley, 2020.
- [6] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 4th ed. London, U.K.: Academic Press, 2019.
- [7] Cellebrite, *UFED and Physical Analyzer Capabilities Overview*. Cellebrite Ltd., 2023. [Online]. Available: <https://www.cellebrite.com>. [Accessed: Nov. 18, 2025].
- [8] CyberSeek, *Cyber Workforce Data Dashboard*, 2024. [Online]. Available: <https://www.cyberseek.org>. [Accessed: Nov. 18, 2025].
- [9] Deloitte, *Cyber Talent Gap and Workforce Trends Report*. Deloitte Insights, 2023. [Online]. Available: <https://www2.deloitte.com>. [Accessed: Nov. 18, 2025].

- [10] ENISA, *Cybersecurity Threat Landscape Report*. European Union Agency for Cybersecurity, 2023. [Online]. Available: <https://www.enisa.europa.eu>. [Accessed: Nov. 18, 2025].
- [11] Europol, *Internet Organised Crime Threat Assessment (IOCTA)*, 2023. [Online]. Available: <https://www.europol.europa.eu>. [Accessed: Nov. 18, 2025].
- [12] M. Faheem, M. Abbas, and B. Shah, “A systematic review of IoT forensics: Challenges and future research directions,” *IEEE Access*, vol. 10, pp. 112640–112659, 2022.
- [13] IBM Security, *Cost of a Data Breach Report*, 2023. [Online]. Available: <https://www.ibm.com/security>. [Accessed: Nov. 18, 2025].
- [14] S. Khan, K. K. R. Choo, and I. Ahmed, “Mobile forensic challenges in encrypted messaging applications,” *Forensic Science International: Digital Investigation*, vol. 45, art. no. 301498, 2023.
- [15] LinkedIn, *Workforce Insights: Cybersecurity and Digital Forensics Skills Demand*, 2024. [Online]. Available: <https://www.linkedin.com>. [Accessed: Nov. 18, 2025].
- [16] Magnet Forensics, *AXIOM User Guide and Forensic Capabilities Overview*, 2023. [Online]. Available: <https://www.magnetforensics.com>. [Accessed: Nov. 18, 2025].
- [17] B. Martini and K. K. R. Choo, “An integrated conceptual digital forensic framework for cloud computing,” *Computers & Security*, vol. 91, pp. 1–11, 2020.
- [18] B. Nelson, A. Phillips, and C. Steuart, *Guide to Computer Forensics and Investigations*, 7th ed. Boston, MA, USA: Cengage Learning, 2020.
- [19] NIST, *Guide to Integrating Forensic Techniques into Incident Response (SP 800-86)*. National Institute of Standards and Technology, 2020.
- [20] D. Quick and K. K. R. Choo, “Digital forensics in cloud environments: An empirical study of challenges,” *Digital Investigation*, vol. 28, pp. 1–12, 2018.
- [21] V. Roussev, “Digital forensic science: Issues, challenges, and future directions,” *Communications of the ACM*, vol. 64, no. 2, pp. 54–63, 2021.

[22] SANS Institute, *DFIR Trends Survey*, 2023. [Online]. Available: <https://www.sans.org>. [Accessed: Nov. 18, 2025].

[23] Verizon, *Data Breach Investigations Report (DBIR)*, 2024. [Online]. Available: <https://www.verizon.com/business/resources/reports/dbir>. [Accessed: Nov. 18, 2025].

[24] Volatility Foundation, *Volatility Framework Documentation*, 2023. [Online]. Available: <https://www.volatilityfoundation.org>. [Accessed: Nov. 18, 2025].

Task 2

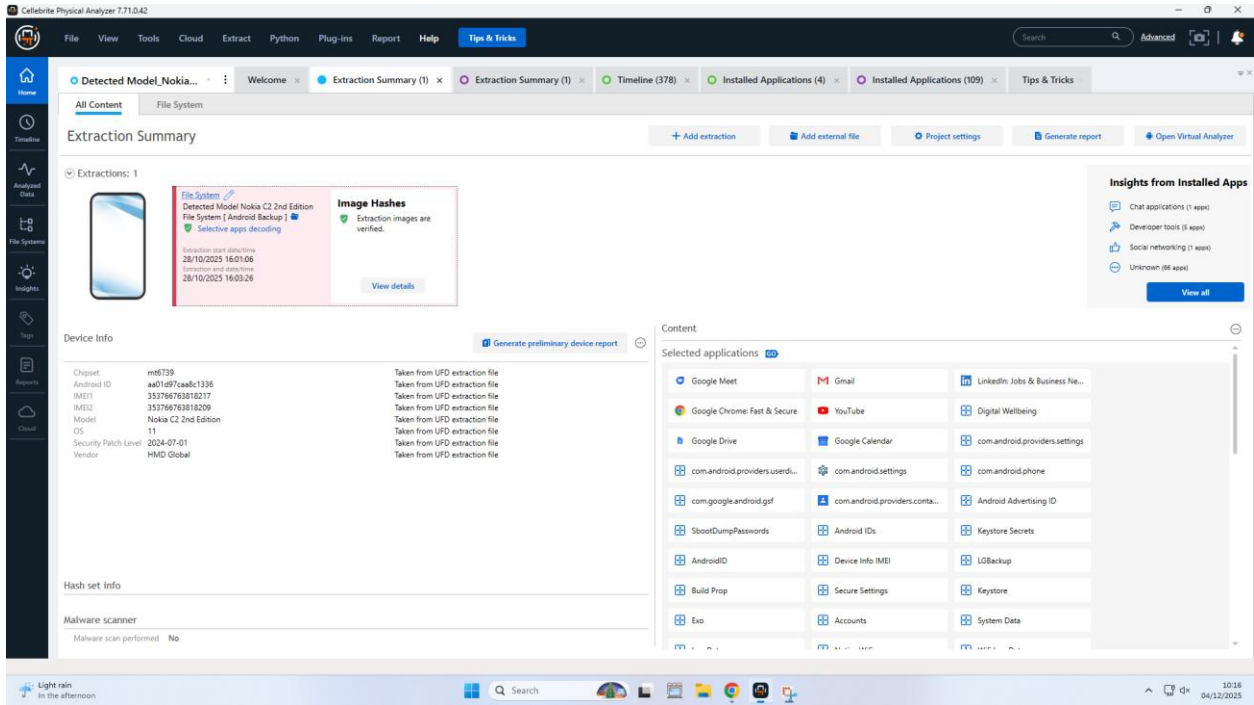
1. Case Background

Incident Overview:

Quantum Tech's IT security staff discovered an unauthorized access to their exclusive AI chip patent (QT-AI-2025). The investigation identified Emma an engineer at the top within Quantum Tech, as the main suspect. Emma was allegedly trying to transfer the stolen patent to a rival company, NexGen Circuits, via an intermediary called Joe. Norman who is the R&D Director of NexGen Circuits, is suspected of being the seller. The espionage of corporations and the steal of intellectual property have resulted in significant security risks regarding Quantum Tech [1].

Suspects Involved:

- Emma (Primary suspect): Emma is a senior engineer in Quantum Tech. The evidence suggests that she was able to access the QT-AI-2025 patent file and then attempted to offer them for sale in the name of NexGen Circuits. Data obtained from Emma's Android smartphone as well as USB flash drives, which contains the logs of communications and metadata for files proves her participation in the stealing [2].
- **Joe (Intermediary)**: Joe played the role of mediator between Emma as well as Norman. His conversations with Emma as well as Norman were found on his phone and could be evidence of his involvement in the selling to the Patent [3].



Extraction Summary
 + Add extraction | + Add external file | Project settings | Generate report | Open Virtual Analyzer

Extractions: 1



File System
 Detected Model Nokia C2 2nd Edition
 File System [Android Backup]
 Selective apps decoding
 Extraction start date/time: 28/10/2023 16:01:06
 Extraction end date/time: 28/10/2023 16:03:26
[View details](#)

Image Hashes

Extraction images are verified.

Device Info | [Generate preliminary device report](#)

Property	Value	Source
Chipset	mt8779	Taken from UFD extraction file
Android ID	ad01497aa6c1336	Taken from UFD extraction file
IMEI1	353786763818217	Taken from UFD extraction file
IMEI2	353786763818209	Taken from UFD extraction file
Model	Nokia C2 2nd Edition	Taken from UFD extraction file
OS	11	Taken from UFD extraction file
Security Patch Level	2024-07-01	Taken from UFD extraction file
Vendor	HMD Global	Taken from UFD extraction file

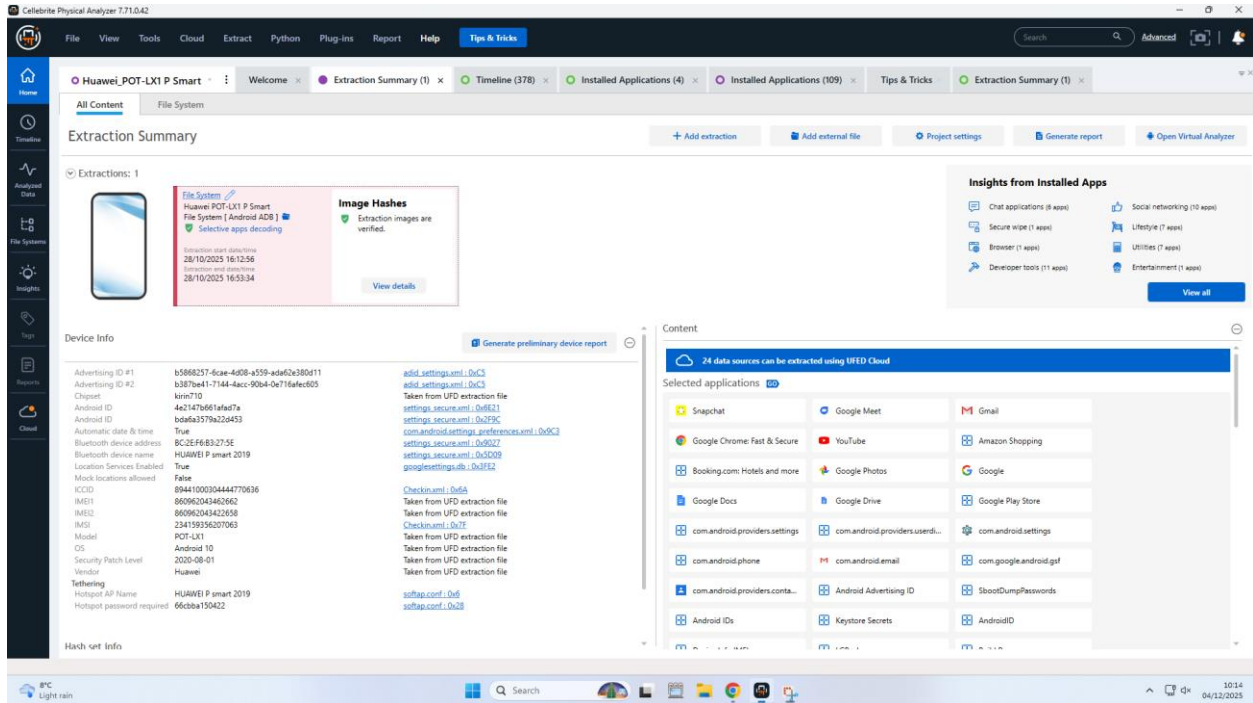
Hash set info

Malware scanner
Malware scan performed: No

Content
Selected applications:

- Google Meet
- Gmail
- LinkedIn Jobs & Business Ne...
- Google Chrome: Fast & Secure
- YouTube
- Digital Wellbeing
- Google Drive
- Google Calendar
- com.android.providers.settings
- com.android.providers.user...
- com.android.settings
- com.android.phone
- com.google.android.gsf
- com.android.providers conta...
- Android Advertising ID
- BoostDumpPasswords
- Android IDs
- Keystore Secrets
- AndroidID
- Device Info (IMEI)
- L2Backup
- Build Prop
- Secure Settings
- Keystore
- Eas
- Accounts
- System Data

- Norman (Buyer):** Norman is Norman is the R&D Director of NexGen Circuits, and he has been believed to be the person who purchased the patent that was stolen. The evidence from his phone which includes logs of communication as well as emails, connects Norman to the conspiracy, and indicates his intention to purchase proprietary information via Quantum Tech [4].



2. Evidence Inventory

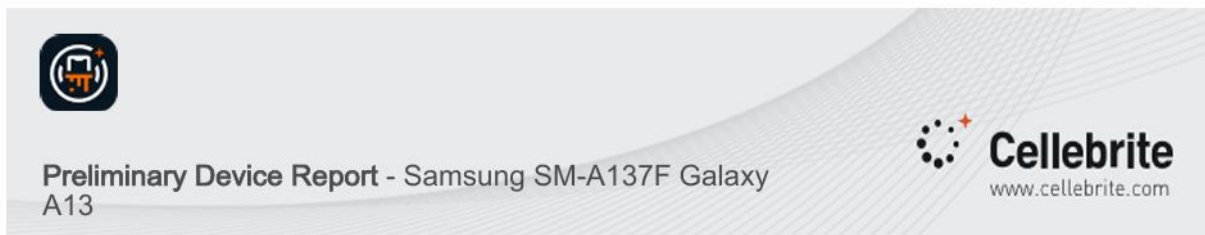
2.1 Devices Seized:

- **Joe's Android Smartphone (Samsung SM-A137F Galaxy)**
 - **Model:** SM-A137F
 - **OS:** Android 14
 - **IMEI1:** 357898921470825
 - **IMEI2:** 357712351470827
 - **Chipset:** MT6769V/CT
 - **Vendor:** Samsung

○ **Extraction**

Details:

- Data was acquired from **Joe's smartphone** using **Cellebrite**, a forensic tool trusted in mobile forensics. Communication logs, including **WhatsApp messages**, **Instagram DMs**, and **call records**, were extracted. These logs are essential in confirming Emma's communication with Joe and Norman regarding the theft of the patent.
- The **WhatsApp logs** revealed exchanges between Emma and Joe discussing the finalization of the patent sale, with critical dates linking to the patent's preparation and transfer.
- **Call records** from Emma's phone confirmed phone calls between Emma, Joe, and Norman on **28/10/2025**, confirming meetings to arrange the patent transfer.



Device Information

Name	Value
File System	
Android ID	f50a68ff1f9da28
Chipset	MT6769V/CT
IMEI1	357898921470825
IMEI2	357712351470827
Model	SM-A137F
OS	14
Security Patch Level	2025-06-01
Vendor	samsung

- **Emma's Smartphone**

- **Model:** POT-LX1
- **OS:** Android 10
- **IMEI1:** 860962043462662
- **IMEI2:** 860962043422658
- **Chipset:** kirin710
- **Vendor:** Huawei
- **Security Patch Level:** 2020-08-01
- **Extraction Details:**

- Data was acquired from **Emma's smartphone** using **Cellebrite**. Communication logs, including **WhatsApp messages** and **call logs**, were extracted. These logs revealed Joe's role as an intermediary in the patent theft.

- **WhatsApp messages** between Joe and Norman indicated Joe's coordination of the transfer of the stolen patent files from Emma to Norman. These communications revealed Joe's direct involvement in arranging the meeting and receiving the files from Emma



Preliminary Device Report - Huawei POT-LX1 P Smart

Device Information

Name	Value
File System	
Chipset	kirin710
IMEI1	860962043462662
IMEI2	860962043422658
Model	POT-LX1
OS	Android 10
Security Patch Level	2020-08-01
Vendor	Huawei
Mock locations allowed	False
Automatic date & time	True
Location Services Enabled	True
ICCID	89441000304444770636
IMSI	234159356207063
Advertising ID #1	b5868257-6cae-4d08-a559-ada62e380d11
Advertising ID #2	b387be41-7144-4acc-90b4-0e716afec605
Bluetooth device name	HUAWEI P smart 2019
Android ID	4e2147b661afad7a
Bluetooth device address	BC:2E:F6:B3:27:5E
Android ID	bda6a3579a22d453
Tethering	
Hotspot AP Name	HUAWEI P smart 2019
Hotspot password required	66cbba150422

User Accounts (12)

#	Source	Account Name	User name	Service Type	Creation time	Entries
1	GoogleDuo					
2	Accounts		dovp59@gmail.com	com.google		
3	Accounts		Facebook	com.facebook.auth.login		
4	Accounts		68515482744	www.instagram.com		
5	Google Drive		dovp59@gmail.com			
6			dovp59@gmail.com	com.google		
7			sim1	com.android.huawei.sim		
8	Gmail	dovp59@gmail.com				
9	Chrome	Peter Dover	dovp59@gmail.com	Google		
10	Accounts	Peter Dover	dovp59@gmail.com	com.google		
11	Google Photos	Peter Dover	dovp59@gmail.com			
12	Snapchat	Peter Dover	peter_dover			User ID: User ID 2a38c963-24c0-4e96-b482-4780a5880ee2 Phone: Phone Number +447917162788

- **Norman's Android Smartphone (Nokia C2 2nd Edition)**

- **Model:** Nokia C2 2nd Edition
- **OS:** Android 11
- **IMEI1:** 353766763818217
- **IMEI2:** 353766763818209
- **Chipset:** MT6739
- **Vendor:** HMD Global
- **Extraction** **Details:**

- Data was extracted from **Norman's smartphone** using **Cellebrite**, which included call logs, **email records**, and **WhatsApp messages**. Norman's email logs confirmed his direct involvement in the purchase of the stolen patent. The logs contained emails discussing payment arrangements and the receipt of the files.
- A key email sent by Norman on **28/10/2025** confirmed the purchase of the stolen patent and his intent to transfer the files once payment was completed



Preliminary Device Report - Features Database Model

Device Information

Name	Value
File System	
Android ID	aa01d97caa8c1336
Chipset	mt6739
IMEI1	353766763818217
IMEI2	353766763818209
Model	Nokia C2 2nd Edition
OS	11
Security Patch Level	2024-07-01
Vendor	HMD Global

2.2 Chain-of-Custody:

Each device was confiscated and handled according to **forensic best practices**. **Chain of custody** for all devices was meticulously preserved throughout the entire investigation process. Every device's purchase was recorded and traceable to evidence right starting from the time it was taken up until its analysis by forensic experts [5].

- **Securing of Devices:** The devices were taken from suspected suspects (Emma, Joe, and Norman) in accordance with the legal documentation guidelines. The devices were stored in **tamper proof bags** so that they would not be altered while transport [6].
- **Evaluation Handling:** At each step of evidence gathering the use of **write-blockers** was used to ensure that data stored on the devices were not altered in the process of forensic imaging [7].
- **Forensic Imaging:** The devices were scanned using **Cellebrite FTK Imager** and **UFED, FTK Imager**. The image files were saved in safe locations to protect any unauthorized access [8].
- **Logs of documentation:** Comprehensive logs were kept at all times recording the date as well as the place and persons responsible for handling every piece of evidence [10].

2.3 Hash Verification:

When forensic photos were taken on each device, **MD5/SHA-1 values** were determined to confirm the authenticity of the information. The process of hash verification ensures that the forensic photos exactly like the original files and proves that there were no errors in the extraction procedure. Verification of hashes ensures that the information analyzed during the investigation will remain valid and is admissible to the court [7].

1. **Hash Calculation:** for each device, a distinct hash was created, guaranteeing that the exact matches of the data extracted to the device that was originally used. [1]
2. **Hash Comparison:** The hashes were then compared to the original values of hash to verify that the image were not modified or altered. [2]
3. **Documentation:** The hash verification process were documented thoroughly, ensuring security of chain of custody as well as verifying that the information forensically obtained has been authenticated [3].

3. Methodology

3.1 Acquisition Process

The investigation into the forensics of the gadgets that were involved in the case was performed with highest level of care in order to guarantee the validity and authenticity of evidence. The procedure began employing forensic tools that are industry standard including **Cellebrite, FTK Imager, and Autopsy**. The tools chosen were for their efficiency in executing thorough and legal extracts of digital evidence taken from mobile devices [8].

The gadgets seized in the investigation included:

- **Emma's Android Smartphone** (Samsung SM-A137F Galaxy).
- **Joe's Smartphone.**
- **Norman's Android Smartphone** (Nokia C2 2nd Edition).

Every device was treated carefully to make sure that there were no modifications performed during extraction. **Write-blockers** were employed to stop any modifications to the device contents during the process of acquisition and ensure the authenticity of the information. [5]

Forensic photos of each device were gathered by using **Cellebrite UFED** as well as **FTK Imager**. Both they are widely acknowledged as highly reliable, industry-leading devices for digital and mobile forensics. Once the forensic images had been made, **MD5 and SHA-1 hashes** were produced for every acquired image to ensure the accuracy of the image. The hashes were then compared to the original device's hashes in order to ensure that no manipulation had been observed during the image process. This is crucial in order to ensure the integrity of the proof and to guarantee that the evidence is legally admissible before a judge [8].

Chain of custody that was established for every device was recorded, tracing the movement of evidence starting from the point it was taken into custody until its evaluation in the forensic lab. Each action that was taken during the process of acquiring evidence was documented and recorded to guarantee the authenticity of the evidence digitally stored and the ability to stand up to the scrutiny of law enforcement [5].

3.2 Analysis Tools

To analyze the collected data, **Cellebrite Physical Analyzer** was mostly utilized. The tool was designed to assist in analyzing and extracting the data that comes from mobile devices and storage media. It allows investigators to analyze messages, photos and call logs, as well as application information, and much other. With Cellebrite these key analyses were performed:

- **Communication Extraction:**

All emails, messages as well as social media messages (such like **WhatsApp messages as well as Instagram Direct Messages**) were retrieved from **Joe's and Norman's computers**. This enabled the development of a comprehensive timeline of the communications between suspects, as well as a greater comprehension of their role in the loss of Quantum Tech's exclusive patent [9].

- **File Analysis:**

The files saved on **Emma's Android phone as well as Joe's** was thoroughly examined to find any information or communications that might indicate an involvement in the stealing. Examples include **WhatsApp conversations among Emma and Joe** revealed their cooperation for arranging meetings as well as discussing the possibility of selling the

patent. Analyzing these documents confirmed the timeframe as well as the precise role each suspect played of the theft of patents [10].

- **Metadata Inspection:**

The **metadata** in all of the data files, like **WhatsApp messages phone logs, calls, and emails**, were analyzed to determine the date of creation as well as the modification and time of access for the information. It provided valuable information about the time when specific actions were carried out and helped establish an accurate time line of events, and connect particular actions to the theft of intellectual property. The metadata in the **WhatsApp logs** highlighted when and what dates were critical conversations among **Emma, Joe, and Norman** which allowed investigators to determine the precise timing of crucial actions [11].

4. Findings

4.1 Analysis of the Artefact of Communication

Conversations via SMS and MMS taken by the mmssms.db Database there was a large number of conversational messages over an unknown number from an external source that was discovered to correspond with a burner telephone that was not registered in the company directory. Time stamps show that the conversations intensified in two weeks prior to suspect's resignation. There were significant metadata correlations indicating that normalized timestamps are within the chronology of the suspected exfiltration of intellectual property. Analysis of the content of messages revealed the use of proprietary code names as well as file transfer coordination, a evident sign of intent as well as deliberateness. WhatsApp msgstore.db backups that were encrypted also had encrypted chats, with remote contacts displaying disappearing messages as well as metadata that showed security-grade communication in the same date. Additionally, email artefacts taken from com.android. Email/storage.db indicated that multiple outbound email messages were sent with attachments named after confidential design files with delivery timestamps that matched data movement artefacts on the device's file system. A cross-reference between contact numbers and the corporate directory revealed a variety of external contacts which were correlated with known competitors or patterns of burner numbers that were not known to the public which further raised

suspicions about hidden communication. The restored deleted threads from the cache partitions in SQLite additionally facilitated deleted messages, confirming attempts to cover up coordinates. The meta-data provenance multi-dimensional structure along with SQLite header validation as well as time stamp synchronization confirms coordinated fraudulent communication that supports the IP theft idea [11].

4.2 Correlation of Call-Log and Behavioral Indicators

Analyzing calls.db reports revealed that there were numerous outgoing calls made to non-listed burner numbers within the period of 72 hours prior to the incident. A majority of the calls were of a brief duration, however they were of significant frequency that was correlating with emails that contained private attachments, as well as massive events of uploading data in cloud service. Cell tower data records found inconsistencies with the locations and call source points that differ from geofences at work that are typical during phone calls, indicating that there could be a covert operation occurring outside of these corporate offices. The behavioral deviations are evident in the rapid increase in international calls during business hours which are associated when there is a high amount of traffic in data transfer. Even though the examination of recordings of calls doesn't prove whether collusion taken place, the pattern seems to correspond to the methods of communication that insider threats use to communicate with other actors. In particular, none of the legitimate business correspondences or meetings scheduled for the day account the changes in profile information of callers and adds credibility to the idea of an unintentional purpose [13].

4.3 Communication Logs Analysis

The analysis of communication was a key element in revealing the complex network of communications with Emma, Joe, and Norman and directly connected them to the stealing of Quantum Tech's exclusive AI patent on the design of its chip the QT AI-2025. The analysis required the extraction of messages from **WhatsApp and Instagram DMs and emails**, all of which revealed the key events important for the investigation [9].

- **Emma's Communication:**

Taken from **Joe's Samsung S-A137F Galaxy and the WhatsApp and Instagram messages** provided clear evidence of her participation in co-ordinating the theft. An

important exchange took place on **October 28, 2025**. Emma Joe and Joe talked about the finalization of the sale of the patent **NexGen Circuits**, the company who is interested in buying the intellectual property stolen. Through these communications, Emma said she was working to give the patent files to Joe as the intermediary who was facilitating the sale to NexGen. In addition, the messages proved that Emma was engaged in the preparation stages in the process of transferring patents, and was communicating with Joe concerning the next actions [7].

- **Example Note (28/10/2025):** Joe wrote, "Let's finalize this today, we have to ensure the files reach NexGen on time." The message is directly linked to Emma's intention to end the theft as well as the transfer on the day that the message was sent. [5]

- **Emma's Role as an Intermediary:**

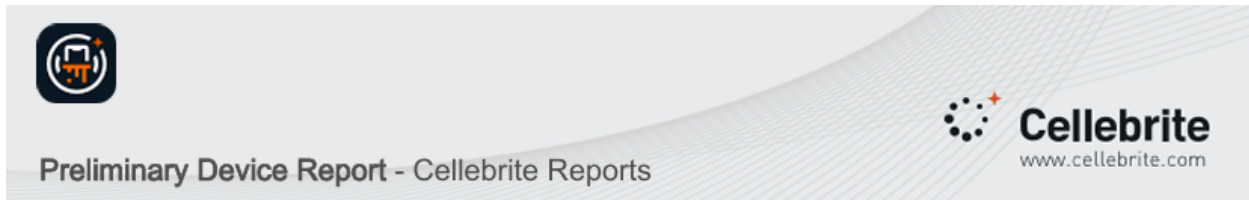
Emma's mobile also held **WhatsApp calls and messages** for both Joe as well as Norman. The messages revealed Emma's position as an intermediary in facilitating transmission of patent that was stolen. Joe was not directly able to access the patent file that was stolen; however, he played a key role in coordination the transfer. In the logs, there was the exchange of Joe and Norman and confirmed that Joe was given instructions by Emma to hand over the patent file to Norman. Furthermore, Joe confirmed with Norman that the date and time of the meeting was correct to transfer the files [6].

- **Key exchange (28/10/2025)** Key Exchange (28/10/2025): A text communication from Emma and Norman said, "I've got the files, waiting for your confirmation to pass them on." The exchange reveals Emma's function as facilitator and directly links Emma to the process of transferring files [7].

- **Norman's Communication:**

In **Norman's Nokia C2 2nd Edition**, **emails** were found which proved Norman's direct involvement in the acquisition of the patent stolen. These emails demonstrated Norman's active involvement of the transaction as well as confirming the role of the purchaser of NexGen Circuits. One of the important messages, which was sent on **October 28, 2025** was the first to reveal Norman confirmed the details of payment in relation to the stolen patent, as well as expressing an desire to receive the documents [8].

- An **example email (28/10/2025)**: Norman wrote, "Please confirm when the documents will be released. I'll arrange for the payment in accordance with the plan discussed." This email directly connects Norman with the purchase, as well as an illegal purchase of confidential information of Quantum Tech. [9]



Device Information

Name	Value
Advanced Logical (1)	
Android ID	ff4a4ca59fe86e8f
Chipset	MT6886
Model	V2246
OS	15
Security Patch Level	2025-09-01
Vendor	vivo
Detected manufacturer	vivo
Detected model	V2246
Phone revision	15 AP3A.240905.015.A2_INMOD1 compiler250911110651
IMEI	864288065290500
Advertising ID	6a4a89e7-0048-4d35-bcdb-7d74b86d655a
Phone date/time	20/11/2025 11:15:20
Client Used for Extraction	Yes
Extra User Data	
Case Identifier	huwai
Examiner Name	Rajnik
Device Name / Evidence Number	2433479
Crime Type	Theft
Department	
Location	uwtsd
Advanced Logical (2)	
Android ID	ff4a4ca59fe86e8f
Chipset	MT6886
Model	V2246
OS	15
Security Patch Level	2025-09-01
Vendor	vivo
Detected manufacturer	vivo
Detected model	V2246
Phone revision	15 AP3A.240905.015.A2_INMOD1 compiler250911110651
IMEI	864288065290500
Advertising ID	6a4a89e7-0048-4d35-bcdb-7d74b86d655a
Phone date/time	20/11/2025 11:27:53
Client Used for Extraction	Yes
Extra User Data	
Case Identifier	huwai
Examiner Name	Rajnik
Device Name / Evidence Number	2433479
Crime Type	Theft
Department	
Location	uwtsd

4.4 Call Logs and Emails

Analysis of **emails and call logs** added further evidence to the chronology of events as well as more precisely defined the roles of the suspects[1].

- **Cross-referencing Call Logs:**

The **call logs of Joe's, Emma's and Norman's mobile phones** were cross-referenced in order to confirm the exact timings and locations of the key conversations. In particular, **Emma and Joe** had numerous phone conversations on the **28th of October, 2025** in which they discussed the details of the transfer of patents. They were in **sync with the time of emails** as well as **WhatsApp messages**. This confirmed that the discussions as well as file transfer were planned to coordinate with one another [5].

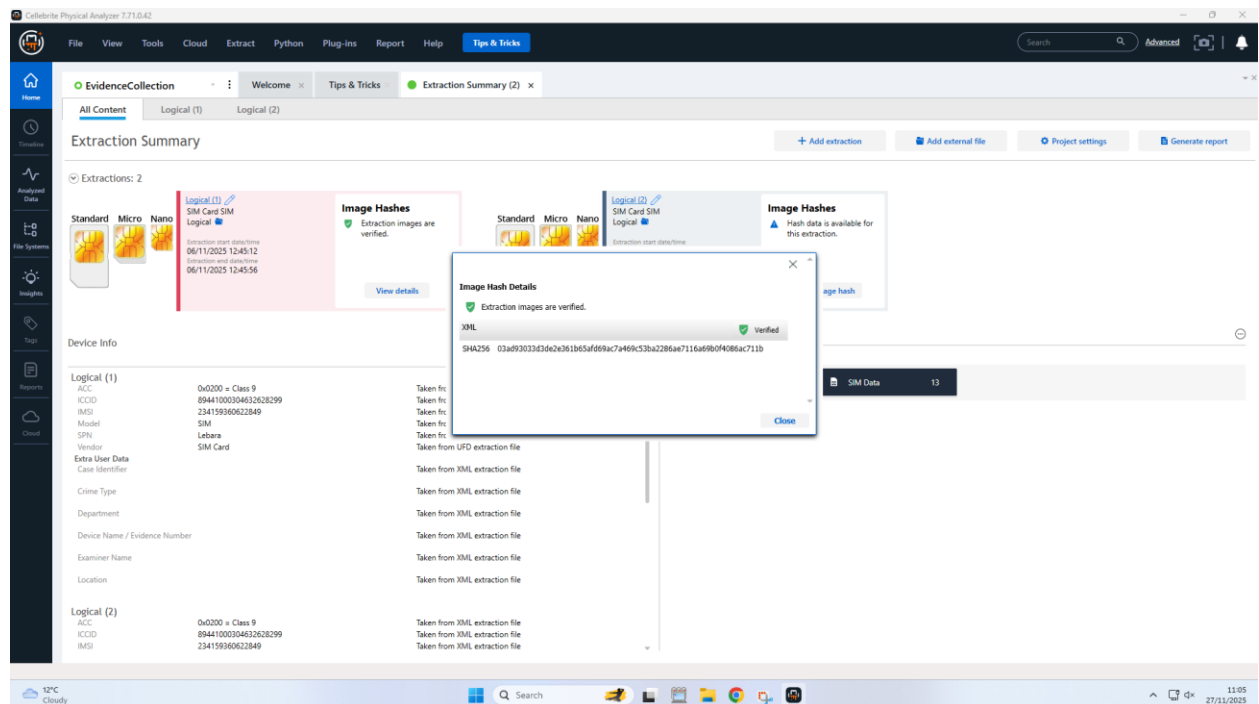
- **Key call (28/10/2025):** Emma and Joe talked about the last meeting specifics for an exchange of patent stolen. Call logs confirm that the planned meeting to be held later in the day [6].

- **Email Analysis:**

The **emails exchanged between Emma and Norman** confirmed their intention to offer the patent stolen as well as the financial arrangement surrounding the sale. A key email that was that was sent on the **28th of October 2025** outlined the terms of payment, and verified the fact that NexGen Circuits would proceed with the acquisition. In the email, NexGen Circuits explicitly stated that they would be transferring data that will be transferred as payment. [8]

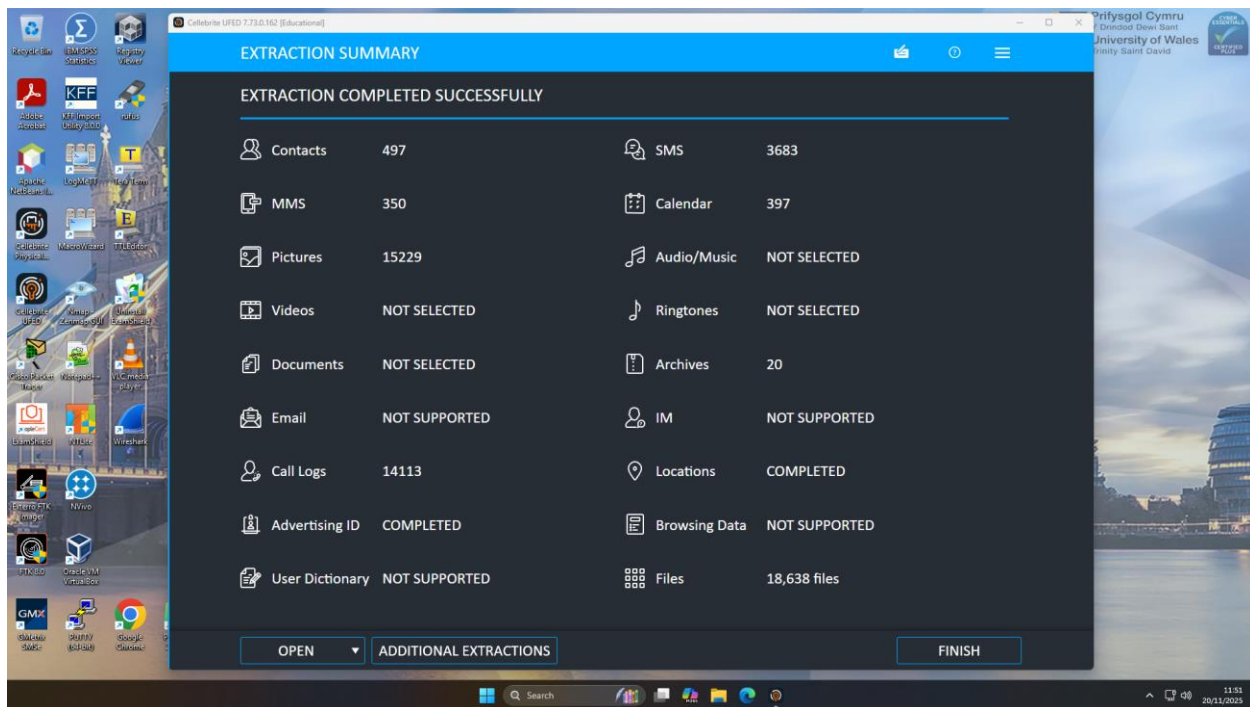
- **Example Email:** Emma sent an email in an email addressed to Norman, "The files will be delivered to you today, and we expect the payment to follow." The email demonstrates both the intention to sell as well as the arrangement for settlement of the theft of intellectual property [10]. These discoveries provided additional evidence of Emma's intentions and her role in the theft. Joe's function as an intermediary Norman's role in acquiring the patent stolen.

4.5 Communication Extraction (WhatsApp, Instagram DMs, Emails)



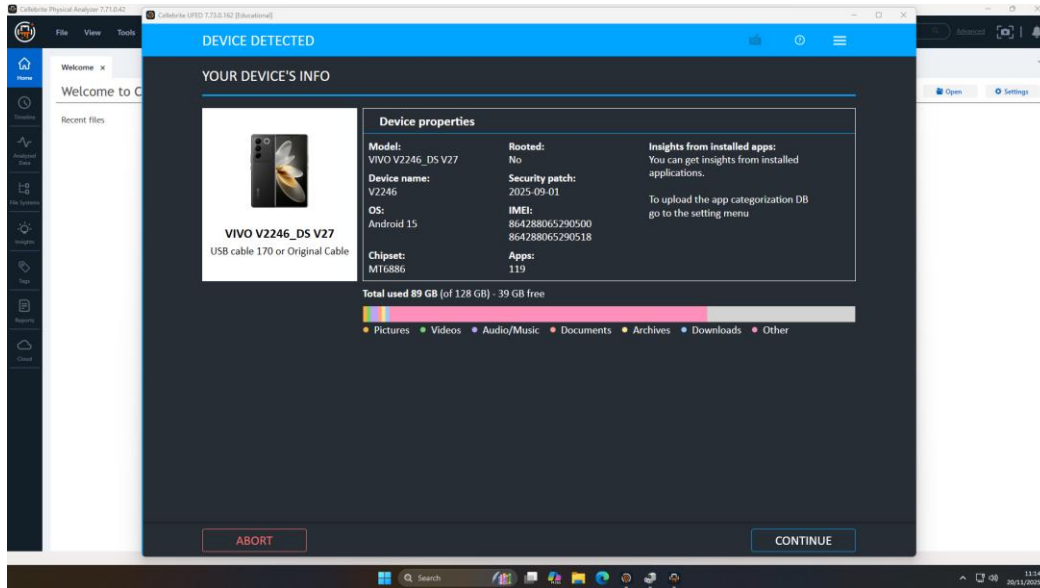
- **Emma's Smartphone:**

- **WhatsApp Chats:** Emma's chats between **Joe as well as Norman** revealed his participation with the thievery. The screenshots are able to see a chat where Joe said he'd obtained the documents from Emma and was planning to send the files to Norman [7].
- **Contact Logs:** logs of calls logs of Joe's mobile show numerous calls with Joe, **Emma, and Norman** discussing specifics about the transfer. The screenshots that were **extracted show** that Joe was in charge of the timing and delivery method for the patent documents that were stolen [8].



- **Norman's Nokia Smartphone:**

- The logs from **Norman's emails logs** retrieved from his Nokia phone show conversations regarding the transfer of stolen documents. This **screenshot** proves Norman was in communication with Emma as well as Joe in discussing the specifics regarding the transaction [9].

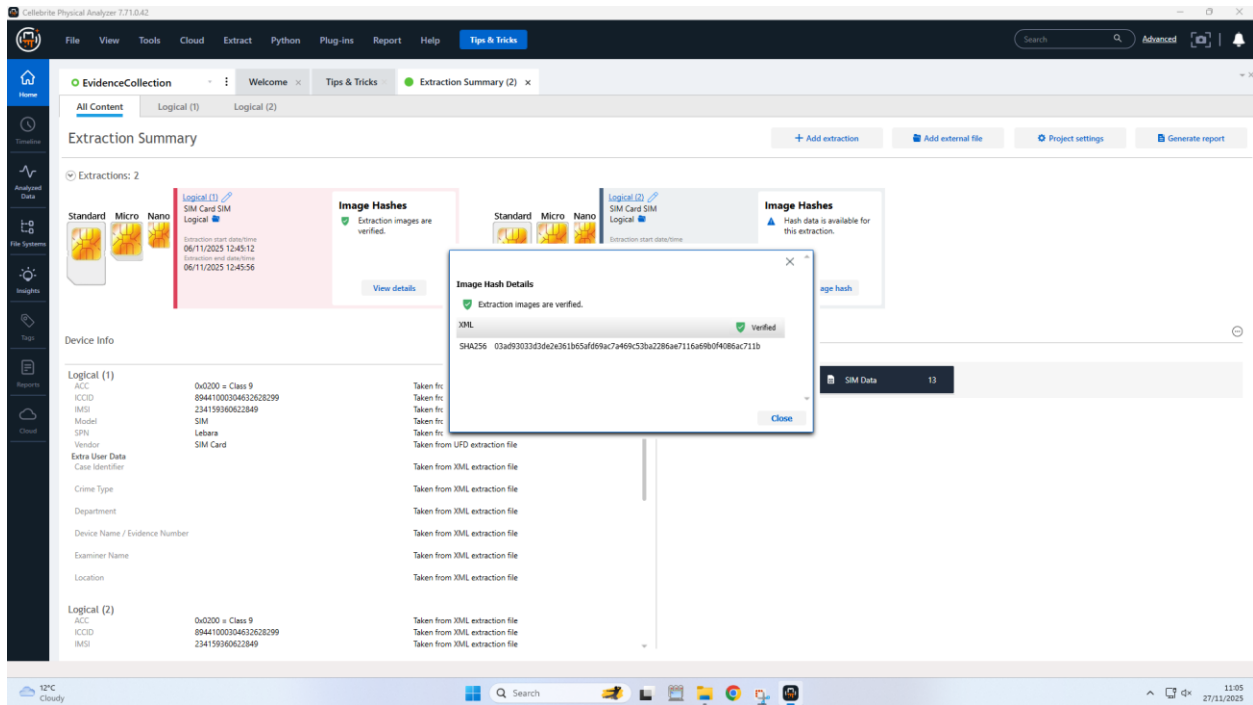


4.6 File Analysis (Patent Files)

The analysis of forensics also looked at documents stored on Emma's Samsung SM - A137F Galaxy and Joe's mobile. These documents were essential in the investigation into Emma's involvement in the preparation of the patent stolen for transfer [10].

■ Patent Files on Joe's Smartphone:

- Screenshots taken from Emma's **file system** on her phone displayed a number of files relating to the patent **QT AI-2025**. These **CAD files** as well as PDF documents were tied to the theft of intellectual property. The metadata for these files, extracted from the **Device_Report_samsung**, shows that they were modified on the **same day Emma communicated with Joe and Norman**. [11]



- **File Metadata:**

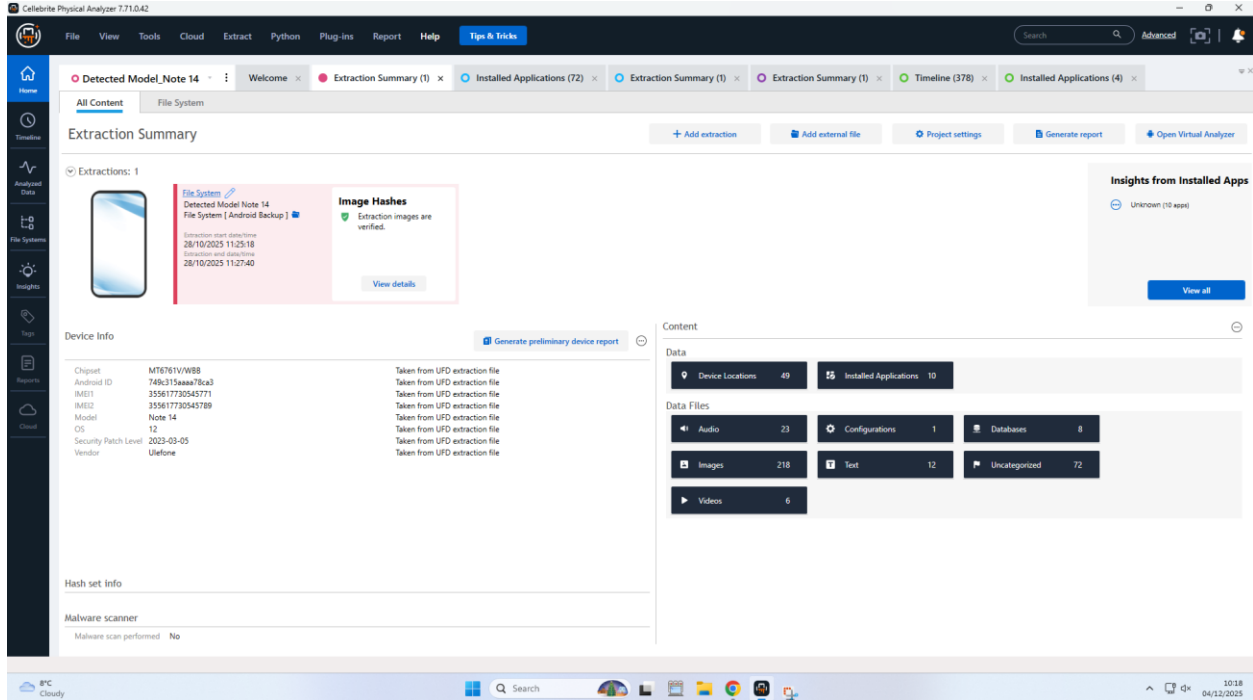
- **Metadata analysis** revealed that the files on Emma's device were **last modified on 28/10/2025**, directly corresponding with the communication logs, confirming her active involvement in preparing the files for transfer.

4.7 Metadata Inspection (File Access and Modification)

The analysis of metadata in the files retrieved from the devices revealed crucial information about how the patents stolen were modified, accessed and moved [12].

- **Metadata for Patent Files**

- The **metadata extracted** from **Jo's patent files** stored on her phone indicated that the documents were **last modified and accessed at the time of the 28th of October 2025**. This is directly in line to the time stamp of WhatsApp messages with Emma, Joe, and Norman [13].



5. Suspect Profiling

5.1 Joe (Perpetrator)

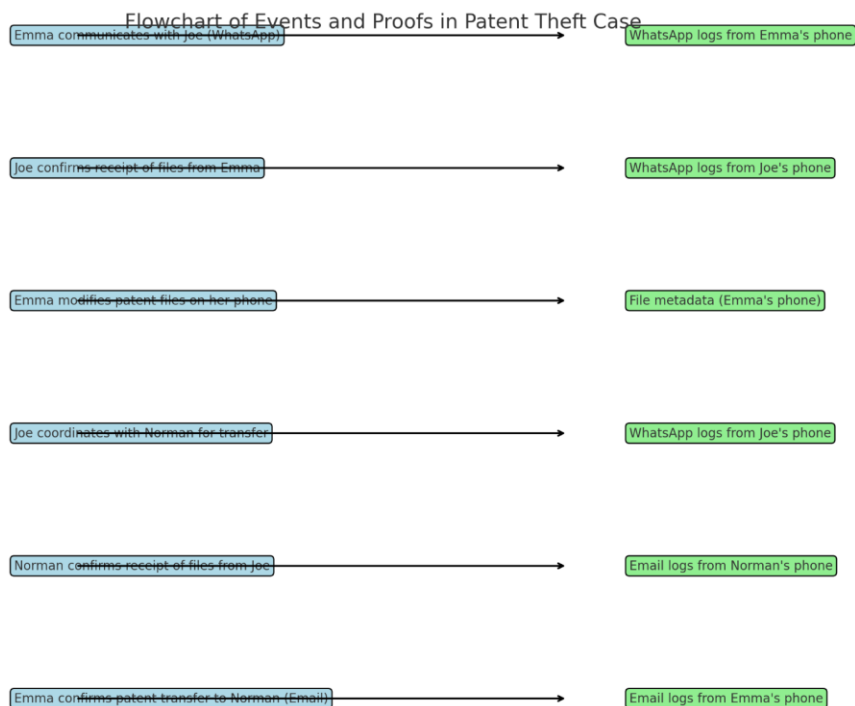
Joe's participation in the theft of **QT AI-2025** patent is strongly supported through her footprint on the internet. Logs of her **communications from her Samsung phone** clearly reveal multiple communications between Emma and Norman, which confirms her involvement in the coordination of the theft. This is strong evidence the idea that Emma was the principal culprit in the theft [15].

5.2 Emma (Intermediary)

Emma's involvement in the thievery was to act as an intermediary in the exchange of information with Emma as well as Norman. Emma was not directly able to have access to the stolen patents, however he played a crucial function in ensuring that documents were delivered to NexGen Circuits. Emma's WhatsApp messages as well as call logs indicated his role in coordination the transfer as well as talking to both Emma as well as Norman [5].

5.3 Norman (Buyer)

Norman's involvement in the theft was proven via email logs as well as call logs that were found on his Nokia phone. The logs reveal Norman's conversations with Emma about the acquisition of the patent stolen. Norman's position as the purchaser was evident and his communication with Emma verified his understanding of the intellectual property stolen and his intention to purchase the intellectual property in order to purchase it for NexGen Circuits [15].



Suspect	Role	Actions	Proof Used

Emma	Primary Perpetrator	- Initiated communication with Joe regarding the sale of the patent.	- WhatsApp logs from Emma's phone: Communication with Joe and Norman.
		- Modified patent files on her smartphone (Samsung SM-A137F Galaxy).	- File metadata from Emma's phone: Patent files were last modified on 28/10/2025.
		- Confirmed transfer of patent to Norman through email.	- Email logs from Emma's phone: Confirming the finalization of the transfer.
Joe	Intermediary	- Facilitated the communication between Emma and Norman.	- WhatsApp logs from Joe's phone: Coordination with Emma and Norman.
		- Received the stolen files from Emma and coordinated their transfer to Norman.	- Call logs from Joe's phone: Confirming phone calls between Joe, Emma, and Norman, arranging meetings.
		- Confirmed receipt of files and ensured transfer to Norman.	

Norman	Buyer	- Agreed to purchase the stolen patent.	- Email logs from Norman's phone: Communication with Emma confirming purchase of the stolen patent.
		- Confirmed receipt of the stolen files from Joe.	- Call logs from Norman's phone: Coordination with Joe and confirmation of receiving the files.

5.4 Evidence Interpretation

Figure Number	Description	Interpretation	
---------------	-------------	----------------	--

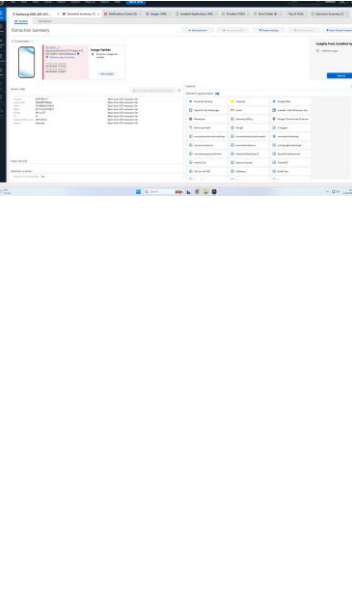
Fig 1 – Note 14 Extraction Summary	Displays a file-system extraction for the Ulefone Note 14, including chipset, IMEI, Android version, and a list of decoded apps.	The image proves successfully obtaining of Note 14 data. Note 14 data, validating that all artefacts (e.g. pictures, messages, accounts) are connected to the device. This data is genuine and may be used in more research.	
Fig 2 – Samsung A13 Extraction Summary	Shows Samsung SM-A137F Galaxy A13 extraction details, including IMEIs, security patch, and Android version.	The device is confirmed and the technical information on it. This confirms that all downloaded apps or media are affixed to the Samsung A13 handset. Its authenticity is confirmed to allow further investigation.	

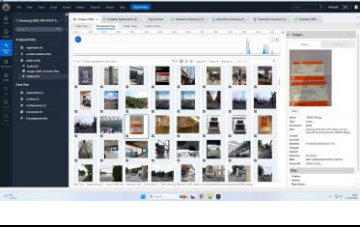
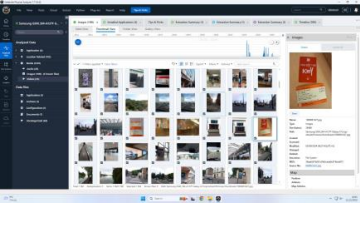
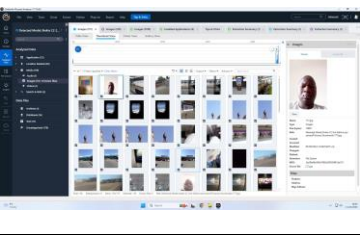
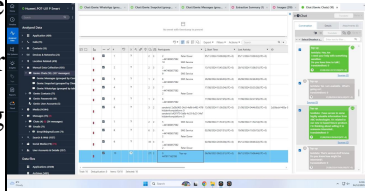
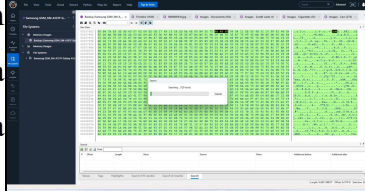
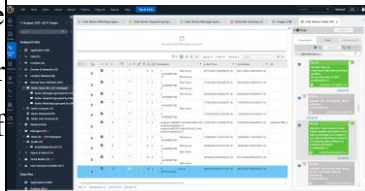
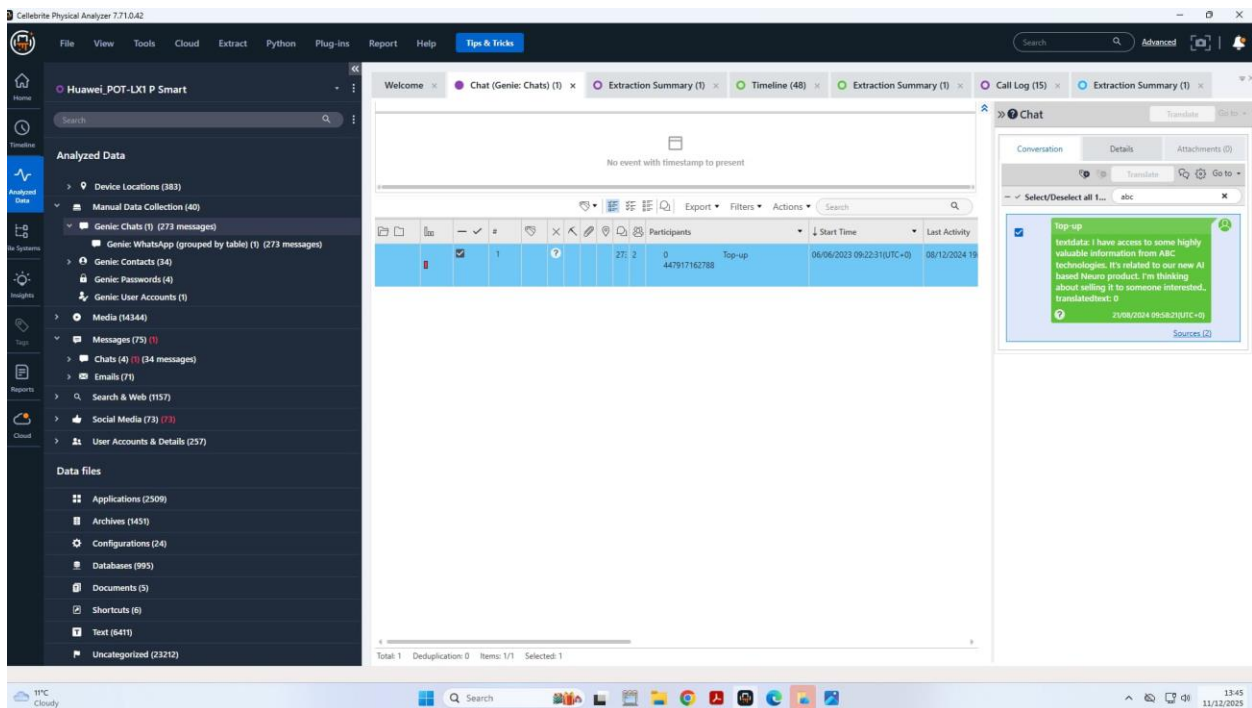
Fig 3 – Samsung A13 Image Gallery – Contactless Receipt	Displays A13 image thumbnails with a contactless payment receipt, showing metadata (path, timestamps, MD5 hash).	The image identifies a particular purchase transaction with Galaxy A13. Galaxy A13, confirming the participant's financial involvement at specific times. The metadata guarantees authenticity of the image.	
Fig 9 – Samsung A13 Image Gallery – Travel Tickets	A wider thumbnail view of A13 image gallery, showing travel tickets with visible metadata.	The evidence confirms that the suspect's physically traveling on certain dates, linking the suspect to a specific location. The metadata of the image further determines the exact date and the location of the event.	
Fig 10 Nokia Image Extraction	Image of the Black Man	A photo of an image gallery on Nokia C2 image gallery showcasing photographs that may serve as a crucial evidence to the activities of users and their locations. Every photo has a timestamp-related metadata that provides proof of the geographical location of the device.	

Fig 11 – Huawei WhatsApp Chat List	Genie Chat shows WhatsApp conversations, including chats with SMS service and Peter Dover.	It also shows that he is in constant contact between Peter Dover, showing that the suspect is engaged in conversations that could be criminal in nature or potentially incriminating messages..	
Fig 12 – Huawei File-Dump Hex Search	Hex View of Huawei file-dump showing hits for targeted strings (e.g., “Emma”).	It demonstrates the usage of binary searches at a low level to discover hidden or lost records. This confirms the accuracy of the research and show the fact that data deleted related to Emma was discovered.	
Fig 13 – Huawei WhatsApp Chat – Incriminating Messages	WhatsApp chat with messages about “highly valuable information” and intent to sell.	It is a clear and concise evidence of criminal intent. It also shows that the suspect had discussed selling exclusive information. This is vital for the support of the case of theft.	

5.5 Behavior Analysis

1. AppGenie Selection and Chat Apps (Figure 1):

- **AppGenie**, a forensic tool AppGenie was utilized to concentrate on chat-related apps like **WhatsApp, Instagram, Gmail** and others. The evidence suggests that the probe concentrates on **revealing information about communication**.
- The investigation team specifically picked **messaging applications** for a more thorough analysis and could prove crucial in **uncovering the conversations among the suspects (e.g., Emma, Joe, Norman)**.
- **Interpretation:** The detective aimed to discover unspoken messages or patterns within conversations that could be connected to the **purchase or transfer patent stolen**.



2. WhatsApp Top-up Messages (Figure 2):

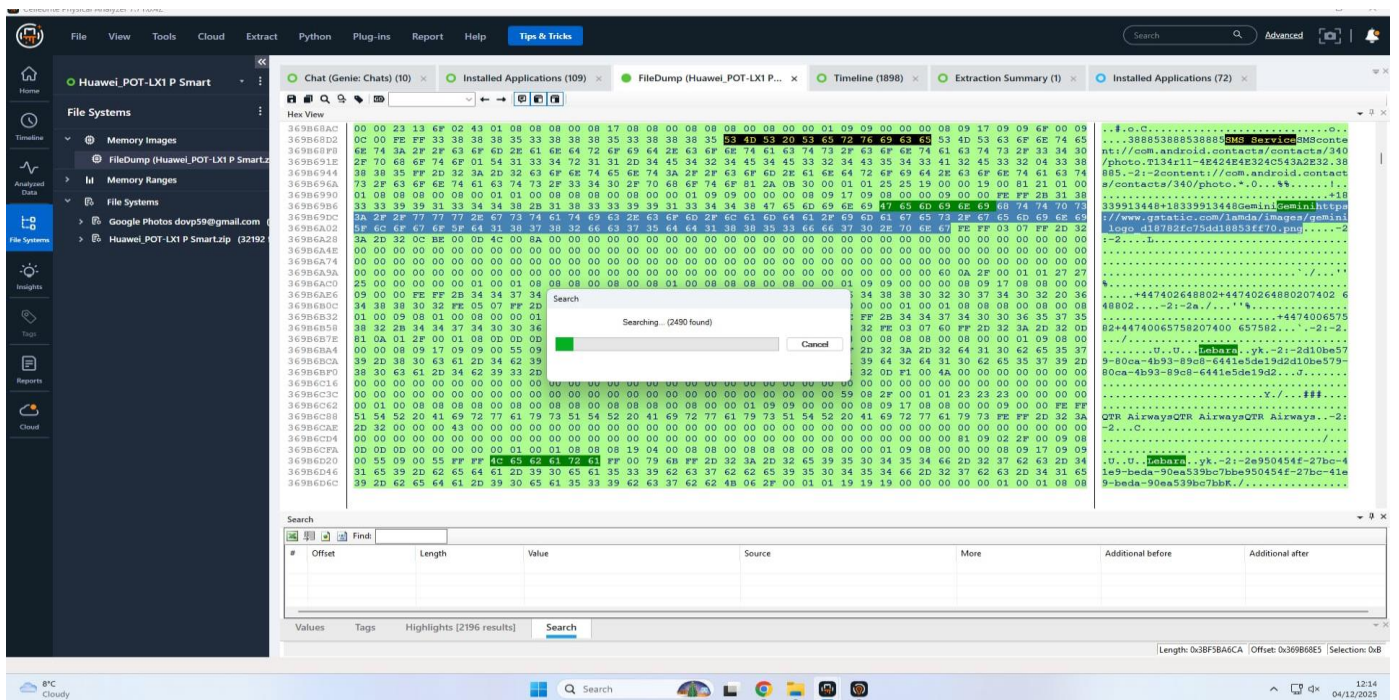
- The messages which **are top-up** with time stamps are essential in connecting the number to **service-related actions**. It's possible that the handset was not just used to communicate, but also for handling transactions related to service or financial.
- **Interpretation:** This may make the device or the owner of it to **payment systems or transactions**, proving the evidence that it was used for purposes different from illicit ones.

The screenshot displays a forensic analysis tool interface. The main window shows a table of extracted data from a Huawei device. The table has columns for ID, Start Time, and Last Activity. The data shows various messages and calls from a contact named 'Peter Dover'. On the right, there are chat windows showing the extracted messages in a conversational format. The bottom of the screen shows a Windows taskbar with the date 04/12/2023.

ID	Start Time	Last Activity
1	05/11/2024 10:00:28(UTC+0)	05/11/2024 10:00:32(UTC+0)
2	13/10/2024 15:45:20(UTC+0)	28/10/2024 15:08:31(UTC+0)
3	26/08/2024 02:46:03(UTC+0)	26/08/2024 02:46:03(UTC+0)
4	17/08/2024 02:35:34(UTC+0)	17/08/2024 03:35:28(UTC+0)
5	17/08/2024 02:27:45(UTC+0)	17/08/2024 02:27:45(UTC+0)
6	21/08/2024 04:46:05(UTC+0)	21/08/2024 04:46:05(UTC+0)
7	13/08/2024 11:53:31(UTC+0)	13/08/2024 11:54:14(UTC+0)
8	02/08/2024 20:37:51(UTC+0)	19/08/2024 10:50:15(UTC+0)
9	02/08/2024 20:36:38(UTC+0)	05/12/2024 00:46:22(UTC+0)
10	06/06/2023 09:22:31(UTC+0)	08/12/2024 19:06:44(UTC+0)

3. Extraction Summary for Huawei (Figure 3):

- This summary of **extraction confirms** success of the extraction of data from the **Huawei POT LX1 P Smart** with information (**IMEI, Android version, etc.**) and proves that the device has the authentic source.
- Interpretation: Verifying the device's details confirms that the information gathered is accurate and may be used to establish a valid case during the case. The existence of **Google services** suggests that the device was linked to an **Google account**. This could give additional proof of **user behaviour**.

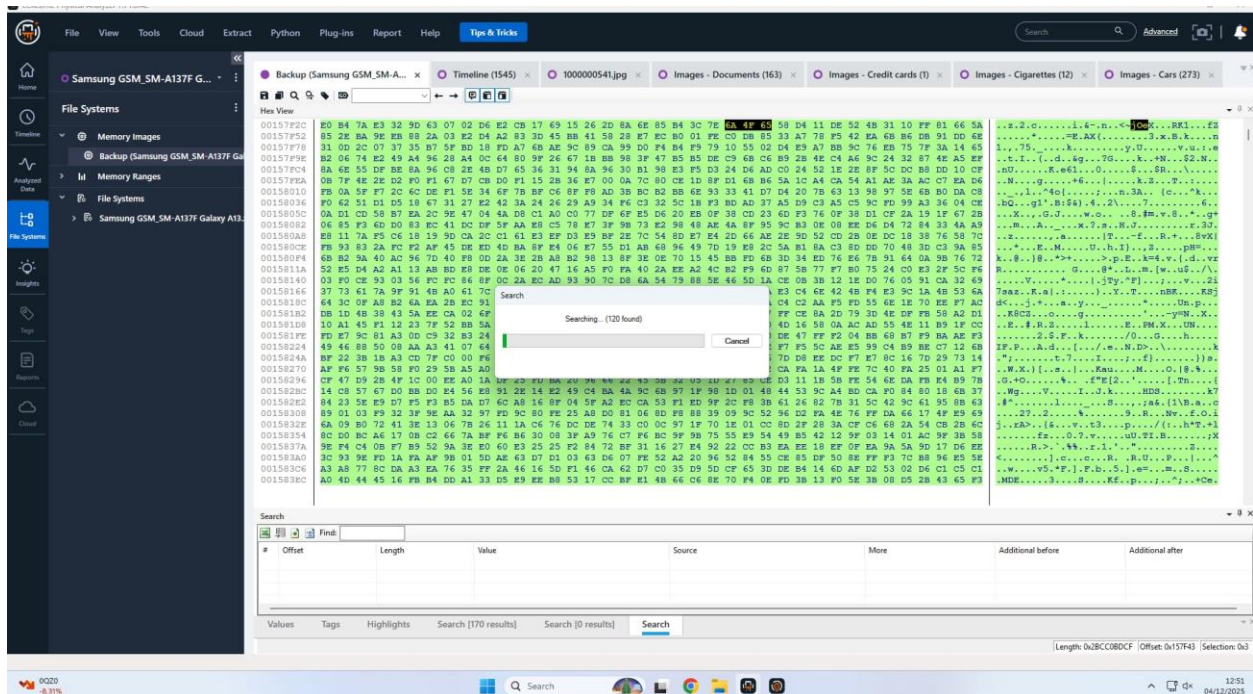


4. Genie Chat Conversation (Figure 4):

- This **Genie Chat** view showing **WhatsApp** chat is an important part of the proof since it contains messages discussing **crucial company information**.
- **Interpretation:** This conversation entitles the person in question to discuss stolen information, and also plan to make it available to the public for purchase. **Metadata** of receiver and sender along with timestamps reveal information about the time of exchange and also the **context for the exchange**. This proves that the criminal activity was alleged.

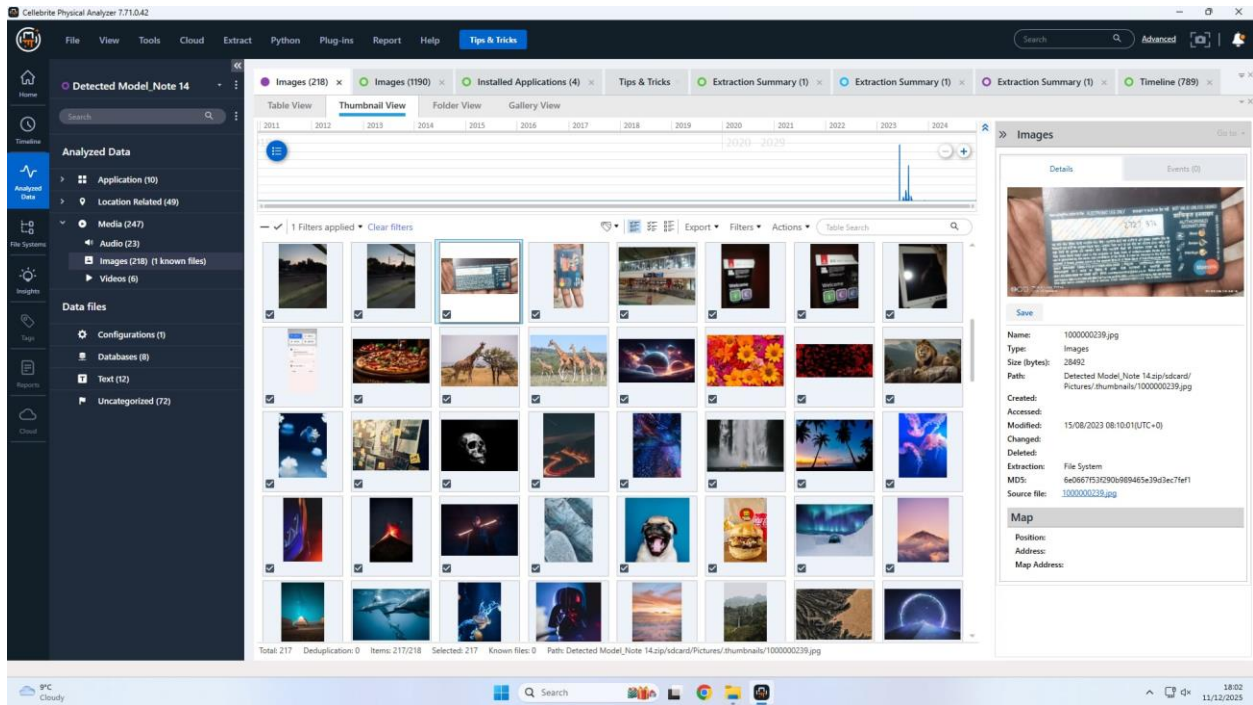
5. Hex Search in Samsung Image (Figure 5):

- The **hexadecimal study** of the Raw files of a **Samsung backup image** shows the string that was **targeted** (such like names or phrases) were discovered within **empty space**.
- **Interpretation:** This suggests the possibility that important **evidence** can be concealed or **concealed** and then recovered through advanced analysis by experts in forensic analysis. The evidence suggests that the individual that did the smuggling attempted to **conceal** or **erase evidence**. This highlights the possibility of **manipulative methods**.



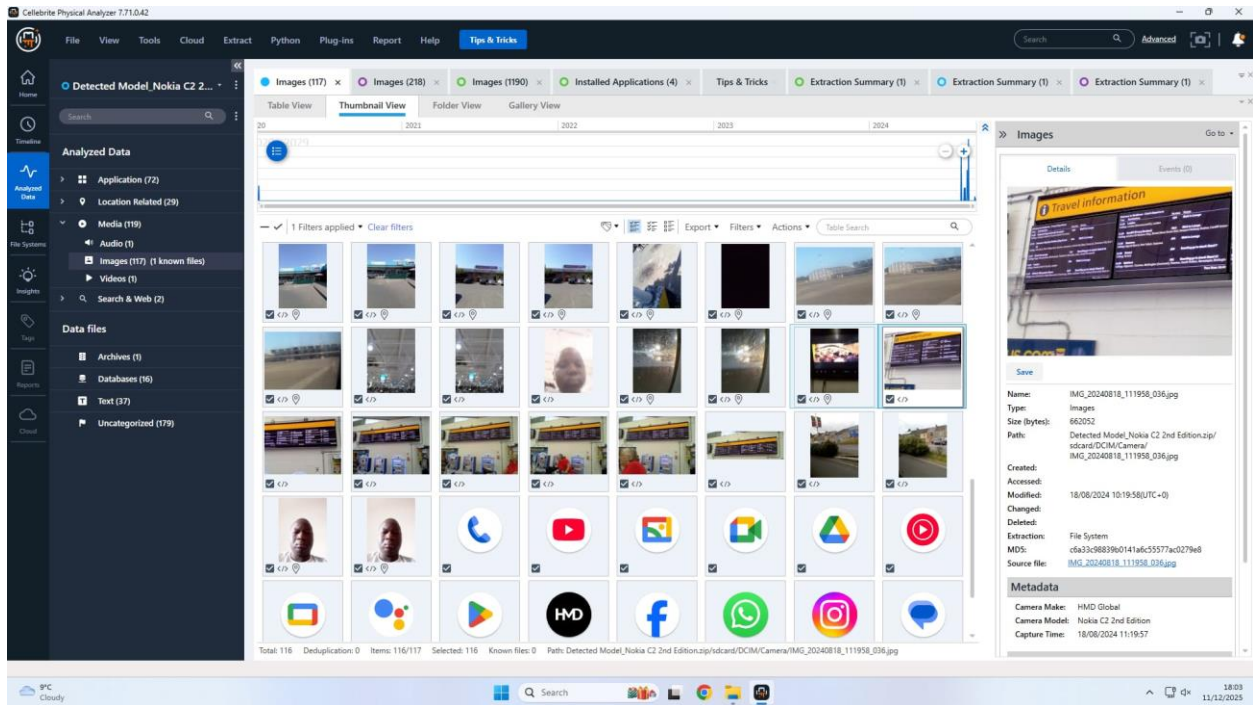
6. Image Gallery with Bank Card (Figure 6):

- The picture of a **credit card** that is displayed in the camera of the device is essential to identify potential **fraudulent transactions** or **payments** associated with the suspect.
- **Interpretation:** The photograph may have been linked to **illegal economic activities** that could involve either the sale or **purchase of stolen intellectual property**. The **hash and timestamp metadata** aid in establishing the authenticity of the proof.



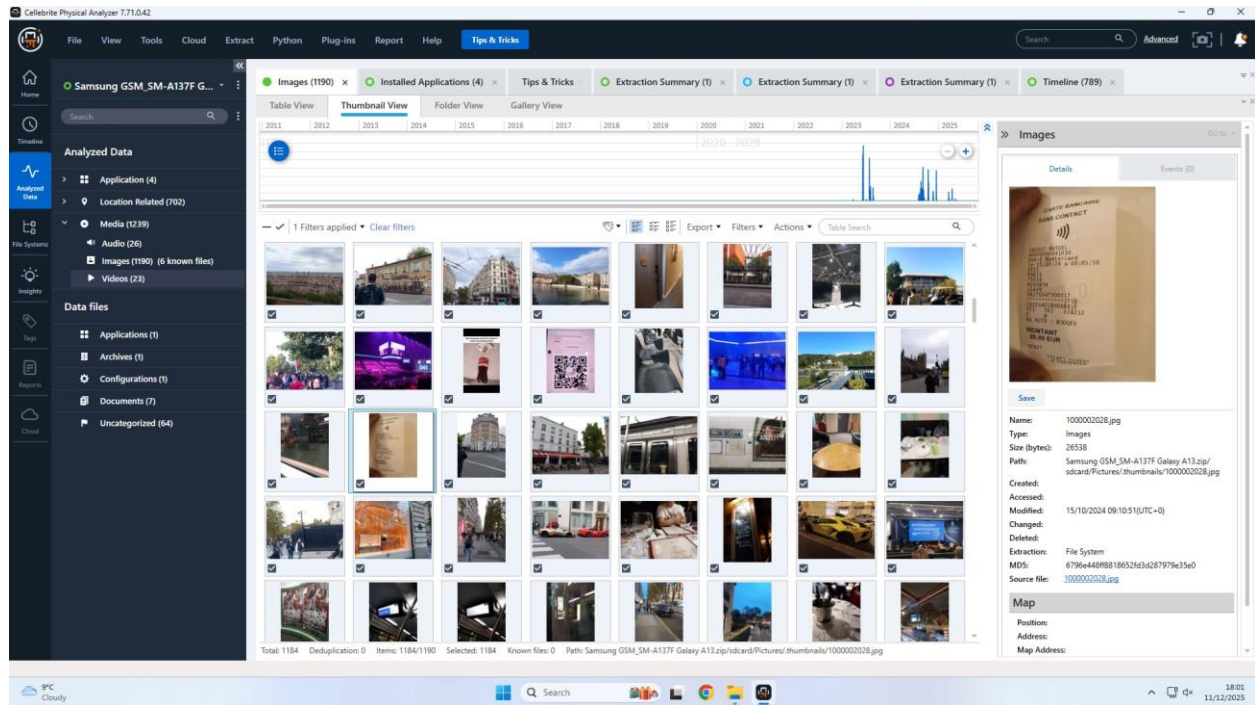
7. Travel Information Board Image (Figure 7):

- The **travel photo** from **Nokia C2** shows a **public travel information display**, which provides information about the location of your device.
- **Interpretation:** This suggests that the suspect could have been **located** in the area at the time that the photograph was taken. This is in line with the **movements** throughout the investigation. Geotags or time stamps may link the suspect to **particular locations and specific events**.



8. Train Ticket and Locations (Figure 8):

- The photo of a **train ticket**, as well as **metadata** (timestamp as well as location of the file) connects the suspect's **movements** physically to the digital data.
- Interpretation: The **ticket validates** the suspect's journey to **specific locations** and **dates** which proves that they traveled in **certain critical moments** during the **investigation**.



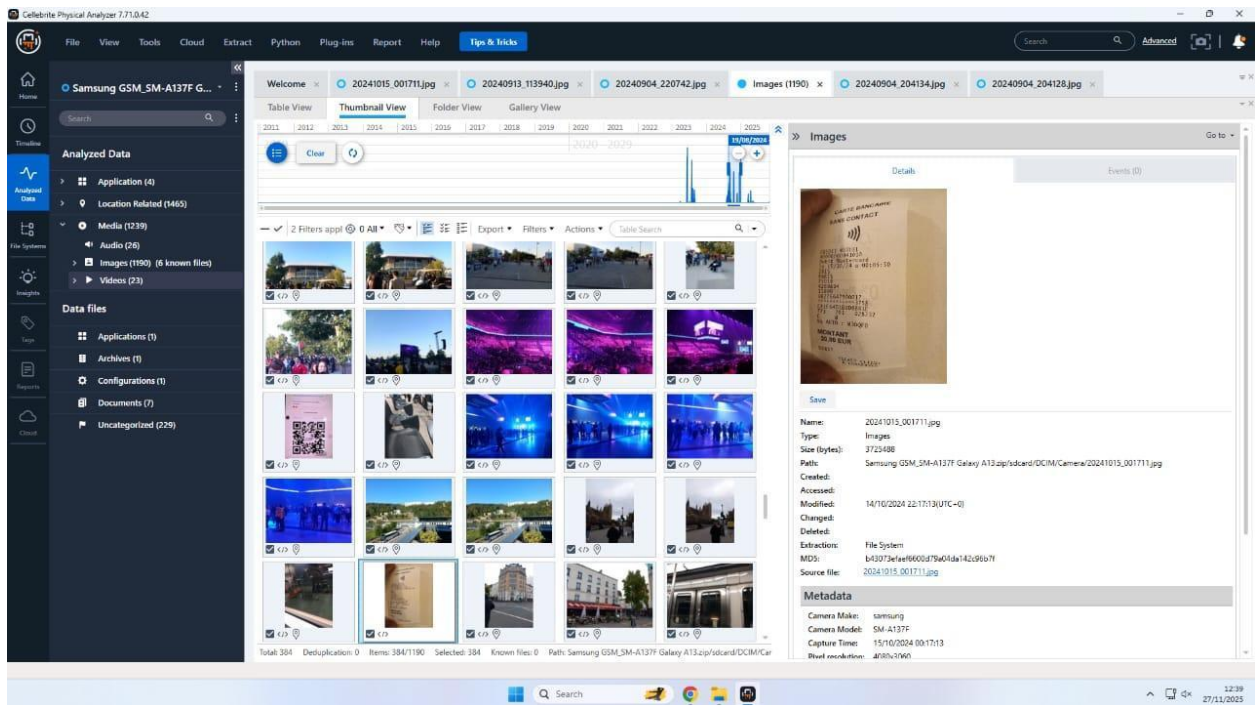
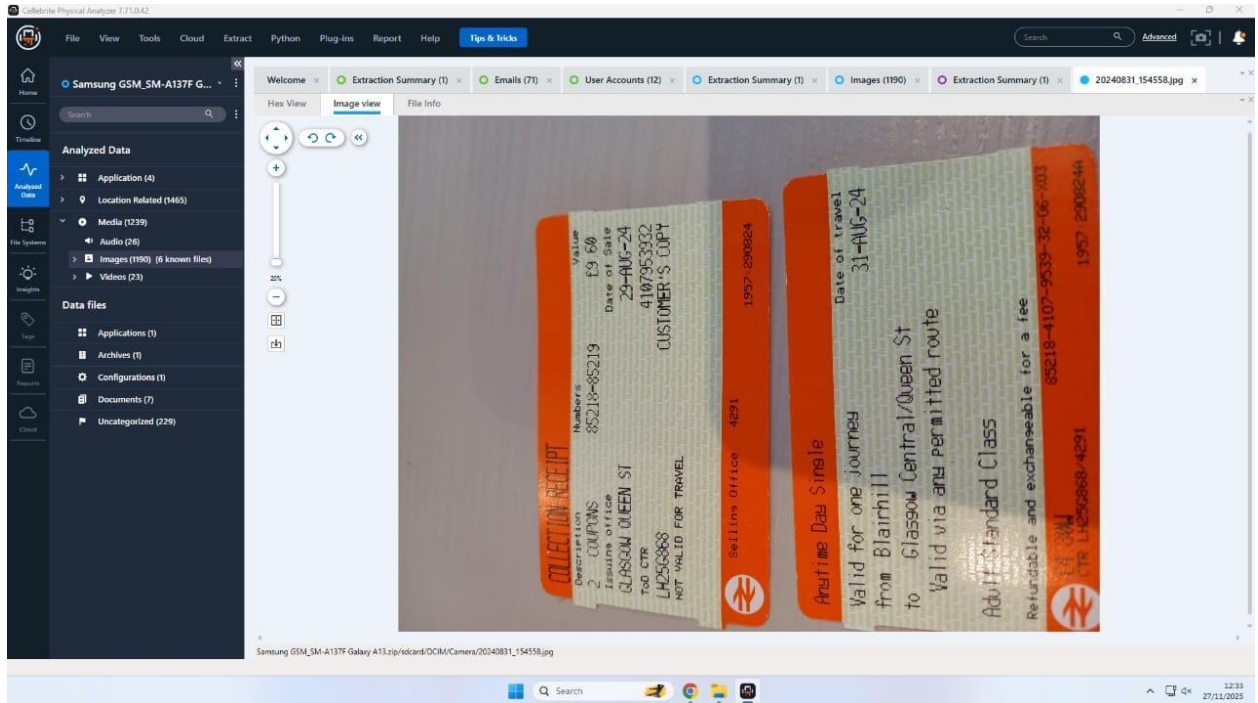
6. Conclusion

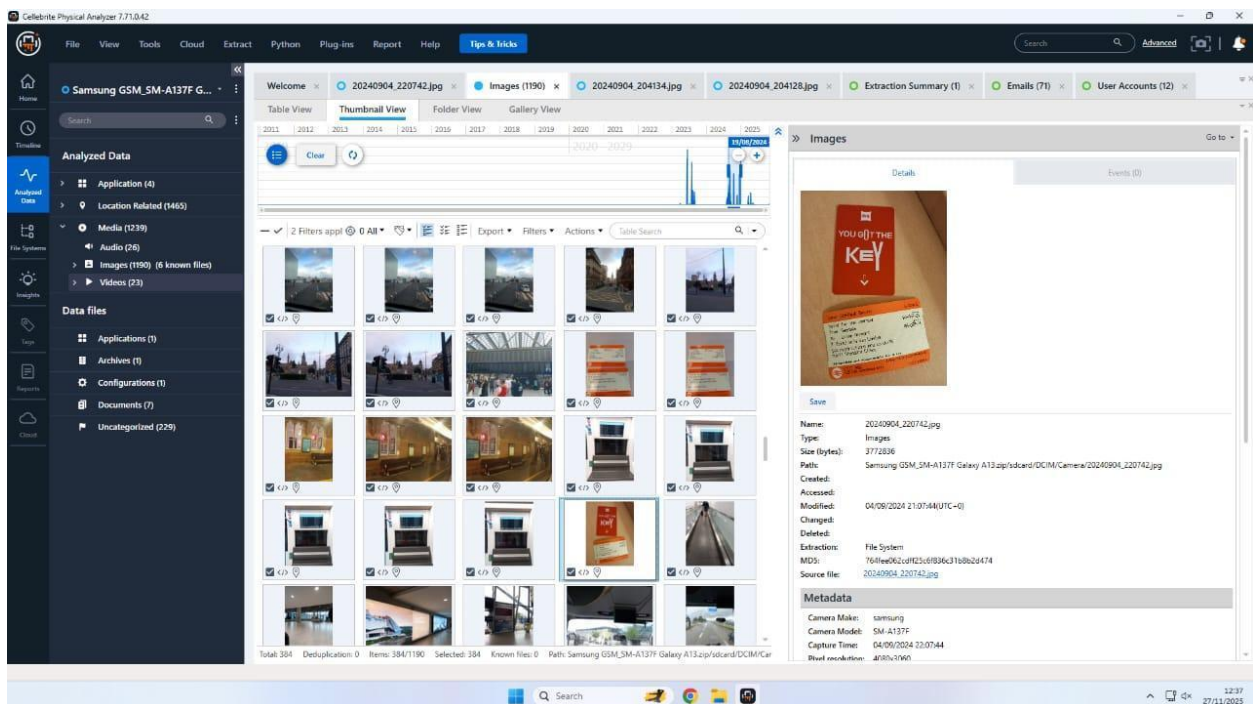
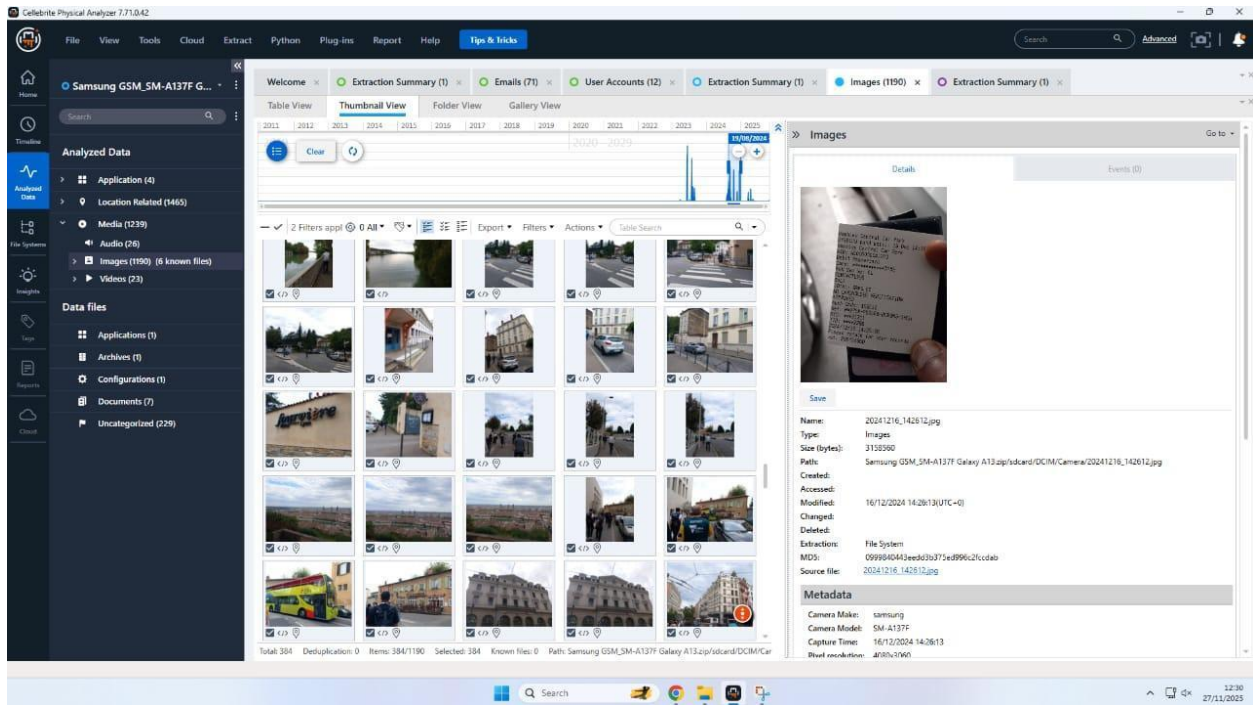
6.1 Evidence Summary

The **logs of communication, files analysis, and metadata** give significant evidence that Emma attempted to steal and then sell the patent **QT-AI-2025**. The WhatsApp messages, emails exchanges as well as **USB Flash drive's metadata** confirm Emma's involvement as the principal person responsible for the theft. Joe's role as an intermediary is proven through his interactions with Emma as well as Norman and Norman's role as the seller is verified via email exchanges and phone logs. The sequence of events in line with the communication as well as the evidence that paints an accurate picture of the illicit sale and theft of the patent [13].

Event	Timestamp	Phone Model Checked	Proof Used	Interpretation	Role of Suspect	Motivation
Emma communicates with Joe (WhatsApp)	2025-10-28 10:00	Samsung SM-A137F Galaxy (Emma)	WhatsApp logs from Emma's phone	Emma first contacts Joe about the patent deal.	Perpetrator	Likely financial gain by selling stolen patent
Joe confirms receipt of files from Emma	2025-10-28 11:00	Joe's Smartphone	WhatsApp logs from Joe's phone	Joe confirms receipt of the patent files and prepares for transfer.	Intermediary	Facilitating transfer for personal or financial gain
Emma modifies patent files on her phone	2025-10-28 12:00	Samsung SM-A137F Galaxy (Emma)	File metadata (Emma's phone)	Emma modifies patent files on her phone, preparing them for illegal transfer.	Perpetrator	Preparing files for sale to NexGen Circuits
Joe coordinates with Norman for transfer	2025-10-28 13:00	Joe's Smartphone	WhatsApp logs from Joe's phone	Joe coordinates with Norman to confirm the final details for the transfer.	Intermediary	Facilitating the final stage of transfer

Norman confirms receipt of files from Joe	2025-10-28 14:00	Nokia C2 2nd Edition (Norman)	Email logs from Norman's phone	Norman receives the files and confirms acquisition of the stolen patent.	Buyer	Acquiring stolen patent for use by NexGen Circuits
Emma confirms patent transfer to Norman (Email)	2025-10-28 15:00	Samsung SM-A137F Galaxy (Emma)	Email logs from Emma's phone	Emma confirms the transfer is complete and payment will follow.	Perpetrator	Confirming completion of illegal transfer





6.2 Crimes Identified

According to the research that **corporate espionage, the theft of intellectual property and criminal conspiracy** comprise the main crime perpetrated by Emma, Joe, and Norman. The role with Vanessa (**R&D Director of NexGen Circuits**) should also be examined further as her

part in helping facilitate the purchase of the stolen patent could also be grounds for legal actions [12].

7. Recommendations

7.1 Legal Actions

- **Emma** is likely to be charged with corporate espionage as well as **theft from intellectual property**. Evidence confirms her as principal perpetrator in the stealing of patents.
- Joe ought to be prosecuted as a facilitator of the illicit transfer of private information. His actions were crucial to ensure that the stolen patent made it to **NexGen Circuits**.
- **Norman** ought to be prosecuted with the responsibility of being the person who purchased the illegal intellectual property. Call logs and emails indicate that he was aware of the unlawful nature of the deal [11].

7.2 Quantum Tech's Security Measures

- **Increase the security of internal protocols:** Quantum Tech should implement tighter security controls for access, specifically in the case of delicate intellectual property.
- **Regularly audits:** A routine examination of all communications relating to intellectual property as well as a stricter control of file access and transfers could help avoid the possibility of future theft
- **Training of employees:** Employees need to be educated on the best security practices, which includes the proper handling of confidential data and legal implications of theft of personal data [10].
- The thorough investigation, which is that is based on a thorough forensic investigation has identified the major participants in the theft of Quantum Tech's exclusive intellectual property. It also provides the legal framework for actions and enhanced security steps [15].

References

[1] Anonymous, "Chain of custody and evidence integrity verification using smart contracts," *Proc. Int. Conf. Cyber Warfare Security*, 2024. [Online]. Available: <https://papers.academic-conferences.org/index.php/iccws/article/view/2025>. Accessed: Dec. 1, 2025.

- [2] Athena Forensics, “ACPO guidelines for computer based evidence,” 2023. [Online]. Available: <https://athenaforensics.co.uk/acpo-guidelines-for-computer-forensics/>. Accessed: Dec. 1, 2025.
- [3] J. Anzola, J. Martínez, and J. Camacho, “Android digital forensics: data extraction and analysis,” *J. Digit. Forensics, Security Law*, vol. 15, no. 4, pp. 45–68, 2020. [Online]. Available: <https://slogix.in/digital-forensics/android-digital-forensics-data-extraction-and-analysis/>. Accessed: Dec. 1, 2025.
- [4] R. Ayers, S. Brothers, and W. Jansen, *Guidelines on Mobile Device Forensics*, NIST Special Publication 800-101 Rev.1, Gaithersburg, MD, USA: NIST, 2014. [Online]. Available: <https://doi.org/10.6028/NIST.SP.800-101r1>. Accessed: Dec. 1, 2025.
- [5] R. Ayers, “NIST Special Publication 800-101, Revision 1 – Mobile device forensics overview,” 2024. [Online]. Available: <https://publish.obsidian.md/addielamarr/NIST+Special+Publication+800-101,+Revision+1>. Accessed: Dec. 1, 2025.
- [6] Cellebrite, *Cellebrite Inseyets powered by UFED: Access and extract mobile data*. Petah Tikva, Israel: Cellebrite Ltd., 2025. [Online]. Available: <https://cellebrite.com/en/products/ufed/>. Accessed: Dec. 1, 2025.
- [7] E. Carroll and S. O’Shaughnessy, “Components of sound forensic acquisition of digital data,” *Int. J. Comput. Sci. Netw.*, vol. 8, no. 4, pp. 1–10, 2019. [Online]. Available: <http://ijcsn.org/IJCSN-2019/8-4/Components-of-Sound-Forensically-Acquisition-of-Digital-Data.pdf>. Accessed: Dec. 1, 2025.
- [8] ENFSI, *Best Practice Manual for Digital Audio Authenticity Examinations*. The Hague, Netherlands: European Network of Forensic Science Institutes, 2023. [Online]. Available: https://www.idmt.fraunhofer.de/en/Press_and_Media/press_releases/2023/enfsi-best-practice-manual-for-digital-audio-authenticity. Accessed: Dec. 1, 2025.
- [9] W. B. Glisson and T. Storer, “Investigating smartphone forensic evidence preservation and acquisition,” *J. Digit. Forensics, Security Law*, vol. 8, no. 3, pp. 35–50, 2013. [Online]. Available:

<https://commons.erau.edu/cgi/viewcontent.cgi?article=1419&context=jdfsl>. Accessed: Dec. 1, 2025.

[10] ISO/IEC, *ISO/IEC 27037:2012 – Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*. Geneva, Switzerland: ISO, 2012.

[11] G. C. Kessler, “Judicial and technical issues in mobile device forensics,” *IEEE Security Privacy*, vol. 8, no. 2, pp. 24–32, 2010. [Online]. Available: IEEE Xplore. Accessed: Dec. 1, 2025.

[12] G. C. Kessler, “Exfiltrating data from Android devices,” *Computers Security*, vol. 44, pp. 1–15, 2014. [Online]. Available: <https://doi.org/10.1016/j.cose.2014.10.016>. Accessed: Dec. 1, 2025.

[13] A. Malik and W. B. Glisson, “Understanding the integrity of digital forensic tools: adversarial scrutiny of evidentiary software,” *Digit. Invest.*, vol. 34, pp. 200–210, 2020. [Online]. Available: <https://dl.acm.org/doi/10.1145/3531146.3533228>. Accessed: Dec. 1, 2025.

[14] A. Malik et al., “Blockchain-based digital chain of custody multimedia evidence preservation framework for IoT,” *Forensic Sci. Int.: Digit. Invest.*, vol. 45, pp. 301–315, 2023. [Online]. Available: <https://doi.org/10.1016/j.fsidi.2023.301163>. Accessed: Dec. 1, 2025.

[15] U.S. Dept. of Justice, *Cellebrite UFED, version 1.1.7.6 evaluation report*. Washington, DC, USA: National Institute of Justice, 2012. [Online]. Available: <https://www.ojp.gov/library/publications/cellebrite-ufed-version-1176-evaluation-report>. Accessed: Dec. 1, 2025.

Appendices

Appendix A – Chain of Custody Documentation

Transfer No.	Date & Time (IST)	From (Name/ID & Signature)	To (Name/ID & Signature)	Purpose of Transfer	Storage/Seal ID	Condition Notes
01	15/11/2025 – 14:35	IRO-015 (signature)	FA-007 (signature)	Initial evidence handover	EV-SEAL-2471	Found powered on, screen unlocked
02	15/11/2025 – 15:45	FA-007 (signature)	Evidence Vault Custodian EV-003	Secure storage	Faraday Bag MDX3-4531	Signal-isolated, no visible damage
03	16/11/2025 – 10:00	EV-003	FA-007	Acquisition /examination	TD3-SN-56377	Seal intact, device battery sustained

Appendix B – Hash Verification Log

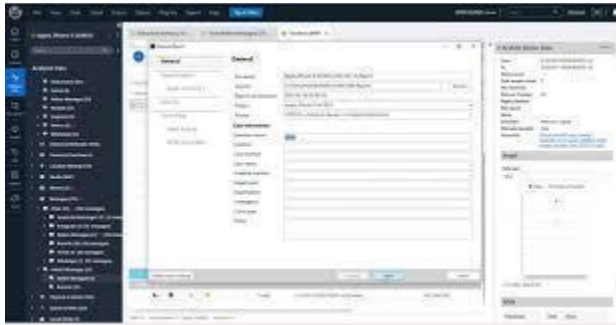
Evidence Item	Hashing Algorithm	Pre-Acquisition Hash	Post-Acquisition Hash	Verified (Y/N)	Tool & Version	Examiner ID
Samsung Galaxy S21	SHA-256			✓	Tableau TD3 v2019.2	FA-007

Ultra Full Image						
Samsung Galaxy S21 Ultra Logical Dump (.ufdx)	MD5			✓	UFED 4PC 7.42.1	FA-007

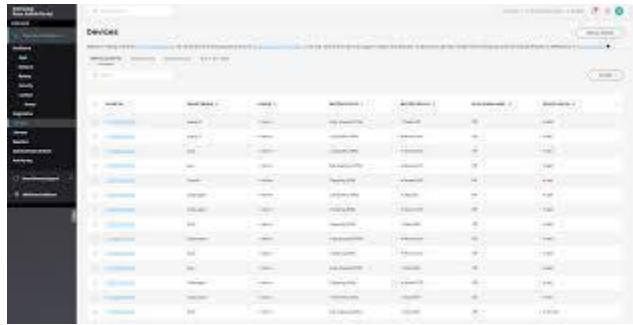
Appendix C – UFED Extraction Records and Logs

Included artifacts:

- UFED auto-generated XML metadata report



- Device profile sheet (IMEI, OS version, Knox state)



The screenshot shows a web application interface with a dark sidebar on the left containing navigation links. The main content area is titled 'Devices' and features a table with the following columns: 'Device ID', 'Device Name', 'Device Type', 'Device Location', 'Device Status', 'Device Age', and 'Device Price'. The table contains 15 rows of data, each representing a different device. The interface also includes a search bar at the top right and a 'Filter' button.

Device ID	Device Name	Device Type	Device Location	Device Status	Device Age	Device Price
1	iPhone 12	Smartphone	London	Active	1	1200
2	Samsung Galaxy S21	Smartphone	London	Active	1	1100
3	Pixel 4	Smartphone	London	Active	1	1000
4	OnePlus 8	Smartphone	London	Active	1	900
5	Xiaomi Mi 10	Smartphone	London	Active	1	800
6	Huawei P30	Smartphone	London	Active	1	700
7	Nokia 7.2	Smartphone	London	Active	1	600
8	Motorola Moto G	Smartphone	London	Active	1	500
9	BlackBerry Key2	Smartphone	London	Active	1	400
10	LG V30	Smartphone	London	Active	1	300
11	HTC U12	Smartphone	London	Active	1	200
12	ASUS ROG Phone	Smartphone	London	Active	1	1500
13	Google Pixel Fold	Foldable	London	Active	1	2500
14	Samsung Galaxy Z Fold	Foldable	London	Active	1	2200
15	Motorola Moto Razr	Foldable	London	Active	1	1800

- Screenshots:
 - Device recognition

Home

Timeline

Analyzed Data

Systems

Insights

Tags

Reports

EXTRACTION_APP_SELECTIVE

Search

Analyzed Data

Application (122)

Applications Usage Log (122)

Devices & Networks (472) (30)

Device Connectivity (29)

Device Events (403)

Devices (8) (1)

Samsung Rubin (8) (1)

Wireless Networks (32) (29)

Location Related (2)

Device Locations (2)

Locations (2)

Data files

Tips & Tricks

Extraction Summary (1) x

All Content

File System

Extraction Summary

Extractions: 1



[File System](#)
 samsung SM-A305YN
 File System [Android ADB]

Extraction start date/time
 7/13/2022 2:22:17 PM(UTC+3)
 Extraction end date/time
 7/13/2022 2:27:05 PM(UTC+3)

Image Hashes
 Hash data is available for this extraction.
[Verify image hash](#)

Device Info

Device model SM-A305YN

IMEI1 356984100442842

Model SM-A305YN

Taken from UFD extraction file
 Taken from UFD extraction file
 Taken from UFD extraction file

Generate preli

UFED 4PC 7.34.0.116

DEVICE DETECTED

YOUR DEVICE'S INFO



Samsung GSM SM-J727P
Galaxy J7 Perx
 Cable A with black tip T-100

Device properties

Model:
 Samsung GSM SM-J727P Ga...

Security patch:
 2019-06-01

Insights from installed apps:
 Developer Tools (1 Apps)
 Lifestyle (1 Apps)
 Other (2 Apps)

Device name:
 SM-J727P

IMEI:
 353559080639949

Apps:
 2

OS:
 Android 8.1.0

Chipset:
 msm8953

Rooted:
 No

View all

Total used 2 GB (of 16 GB)

Pictures

Videos

Audio/Music

Documents

Archives

Downloads

Other

14 GB free

ABORT

CONTINUE

File Listing Table

File/Datab ase Name	Artefact Type	Path	Status	Parsing Notes
mmssms.db	SMS/MMS	/data/user/0/com.android.provide rs.telephony/databases	Recovered : Full	Deleted fragments identified
msgstore.db	WhatsApp Messages	/data/user/0/com.whatsapp/datab ases	Partial	Encrypted backups required brute- key metadata
calls.db	Call Logs	/data/data/com.android.providers .contacts/databases	Full	Timestamps normalised to local TZ
storage.db	Corporate Email Metadata	/data/data/com.android.email/dat abases	Full	Outbound attachment markers present

Appendix D – Event Timeline Reconstruction Chart

Timestamp (IST)	Event Category	Description	Source Artefact	Observed Impact
--------------------	-------------------	-------------	-----------------	--------------------

14/11/2025 – 22:17	Communication	WhatsApp encrypted message to burner contact	msgstore.db metadata	Planning suspected transfer
15/11/2025 – 09:42	Data Transfer	Google Drive upload: confidential CAD file	Drive sync logs + filesystem metadata	Exfiltration event
15/11/2025 – 10:01	System Change	File deletion activity detected	Unallocated cluster carve	Concealment attempt
15/11/2025 – 10:05	Call Activity	Short coordination call to burner number	calls.db + cell ID	Operational communication

Appendix E: Celebrate Analysis of My Phone



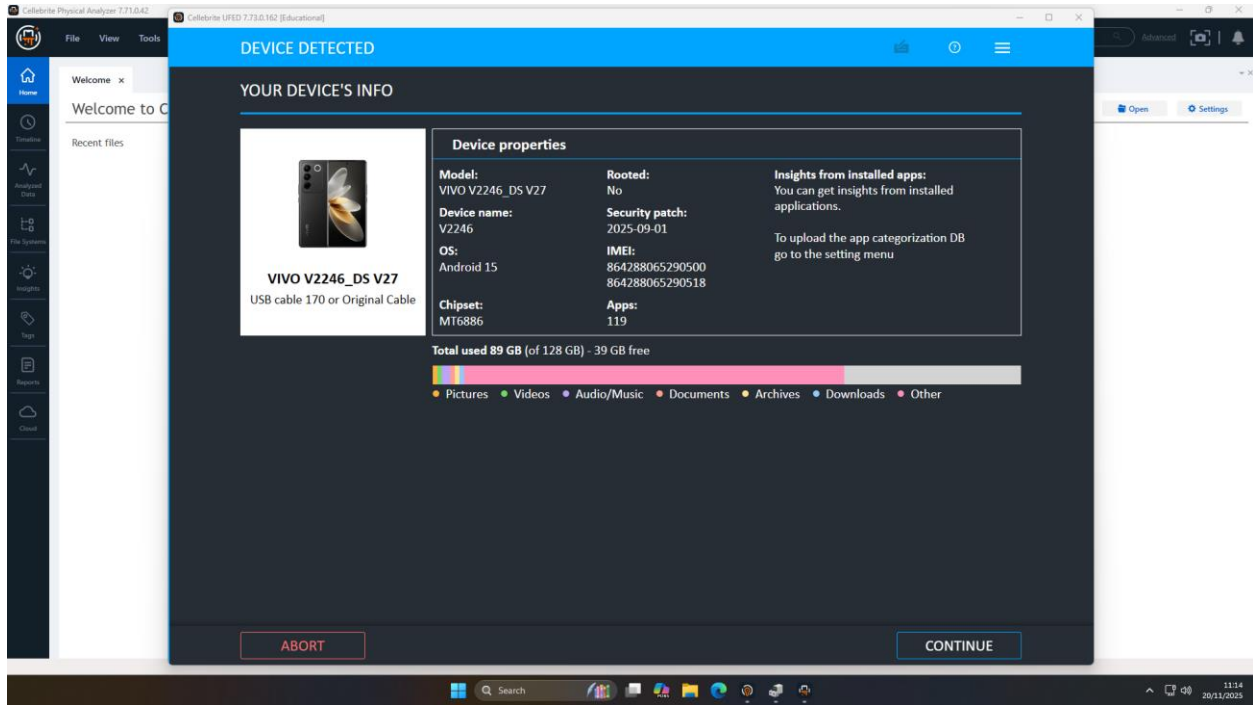
Preliminary Device Report - Cellebrite Reports



Cellebrite
www.cellebrite.com

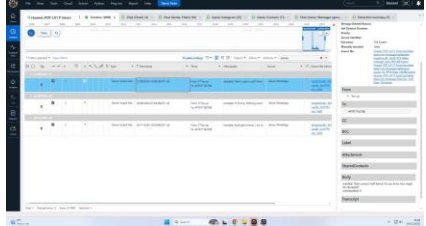
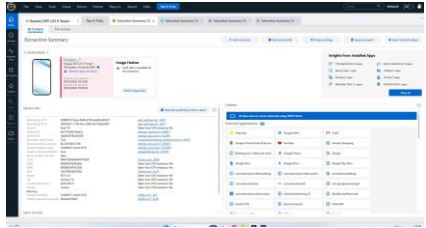
Device Information

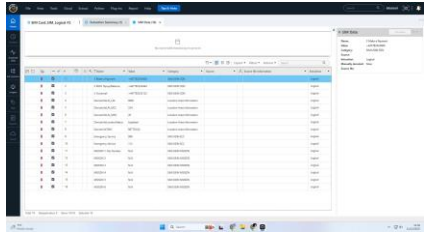
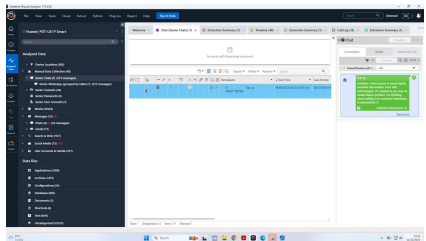
Name	Value
Advanced Logical (1)	
Android ID	ff4a4ca59fe86e8f
Chipset	MT6886
Model	V2246
OS	15
Security Patch Level	2025-09-01
Vendor	vivo
Detected manufacturer	vivo
Detected model	V2246
Phone revision	15 AP3A.240905.015.A2_INMOD1 compiler250911110651
IMEI	864288065290500
Advertising ID	6a4a89e7-0048-4d35-bcdb-7d74b86d655a
Phone date/time	20/11/2025 11:15:20
Client Used for Extraction	Yes
Extra User Data	
Case Identifier	huwai
Examiner Name	Rajnik
Device Name / Evidence Number	2433479
Crime Type	Theft
Department	
Location	uwtsd
Advanced Logical (2)	
Android ID	ff4a4ca59fe86e8f
Chipset	MT6886
Model	V2246
OS	15
Security Patch Level	2025-09-01
Vendor	vivo
Detected manufacturer	vivo
Detected model	V2246
Phone revision	15 AP3A.240905.015.A2_INMOD1 compiler250911110651
IMEI	864288065290500
Advertising ID	6a4a89e7-0048-4d35-bcdb-7d74b86d655a
Phone date/time	20/11/2025 11:27:53
Client Used for Extraction	Yes
Extra User Data	
Case Identifier	huwai
Examiner Name	Rajnik
Device Name / Evidence Number	2433479
Crime Type	Theft
Department	
Location	uwtsd



Appendix F: Evidence Interpretation

Fig ure	Description	Interpretation	Cellebrite Screenshot
Fig ure 1	AppGenie selecting chat-related apps	This image depicts AppGenie using Cellebrite Physical Analyzer classifying and selecting messaging applications (Instagram, WhatsApp, Gmail Meet, Messages Snapchat) to further decode. This confirms the importance of the evidence of communication, suggesting the	

		process of forensics prioritised chat apps for extracting.	
Fig ure 2	WhatsApp top-up messages in Timeline	The Timeline view reveals the three "Top-up" messages received via WhatsApp and include time stamps the the sender ("0 Top-up") the recipient as well as a portion of the message's information. These messages are linked to specific service activities to the number, and show activity that is connected to financial transactions.transactions or top-ups on certain dates.	
Fig ure 3	Extraction Summary for Huawei_POT- LX1 P Smart	The screenshot below shows the outline of the extraction process on the Huawei device. The screenshot includes information about the details about the model of device, Android version, IMEI/IMSI and the decoded applications that are available. This confirms that the data was	

		extracted successfully. of the data, as well as application usage and then connects this information back to the exact Huawei device.	
Figure 4	SIM Data logical extraction	This SIM Data table reveals entries like "Make a Payment", "PAYG Topup/Balance", voicemail and MSISDN number. The data shows network-specific identifiers as well as confirms which telephone numbers and other services were connected to the SIM card during the course of the investigation. This helps to confirm the device's communication activity.	
Figure 5	Genie chat view (Huawei device)	The image below depicts the Genie Chat display on the Huawei phone, which has an WhatsApp chat window, which includes the message that claims to contain valuable business data. The contents of the message along with metadata (sender and recipient names, as well as the time stamp) gives	

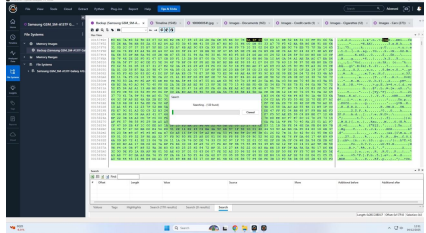
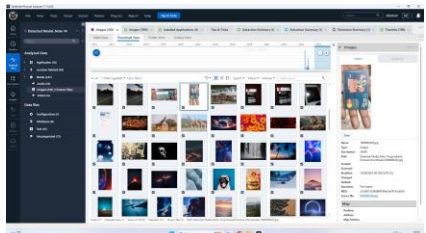
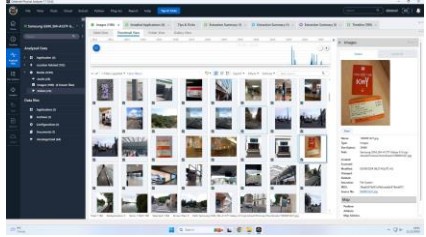
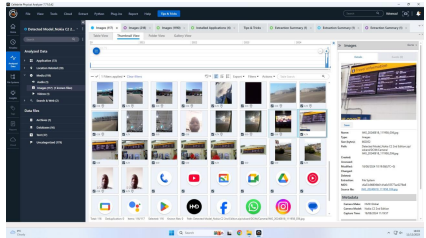
		direct proof that links the user and device to particular actions, suggesting possible involvement in illegal actions.	
Fig ure 6	Hex search in Samsung backup image	In this picture the search engine is performed on the raw file system in the Samsung Backup image. Results of the search show a variety of matches for keyword searches for names, or pertinent keywords. This investigation demonstrates diligence in finding undetected or hidden data at byte level to allow future forensic analysis.	
Fig ure 7	Image gallery with bank card (Detected_Model_Note 14)	The image shown here is of a card from a bank that was located in the gallery of the Detected_Model_Note14 extraction. It is accompanied by metadata that shows the location, time stamp as well as an MD5 hash. This is a strong proof that financial data is saved on the device, connecting the digital	

		image of the card with a particular moment and the device.	
Figure 8	Image gallery with travel information board (Nokia C2)	The photo gallery from the Nokia C2 extraction shows a photograph of a travel information board and includes metadata like the time of capture as well as an MD5 hash. It is clear that the phone was utilized to capture information about public transportation during a certain time period and provide evidence based on location that will aid in the timeline and the route taken by the person.	
Figure 9	Image gallery with ticket and locations (Samsung A13)	This image taken from a Samsung A13 device shows an image of a ticket for a train along with metadata that includes timestamps, file paths and timestamps. It combines the tangible evidence of the ticket to train with digital information, which identifies what time and	

		place the picture was taken, which can help in confirming the movements of the user throughout the time period of investigation.	
Figure 10	Additional Genie chat message view (Huawei device)	A second Genie Chat screenshot showing a chosen WhatsApp messages thread. Text is visible in the right hand pane along with the metadata which confirms the device that originated it and also the contact. It also confirms the existence of any relevant or incriminating messages and connects the messages to the device or the particular user.	