

Student Name: Deep Trivedi

Student:2436067

Table of Contents

<i>Task 1: Research Report on Digital Forensics</i>	3
1. <i>Current State of the Digital Forensics Field</i>	3
2. <i>Digital Forensics tools: Functionality & Capability</i>	4
3. <i>Intersection between Digital Forensics and Cybersecurity</i>	4
4. <i>Emerging Trends in Digital Forensics</i>	5
5. <i>Digital Forensics: The Big Pitfalls.</i>	6
6. <i>Labor Market International and National.</i>	6
<i>References</i>	8

Task 1: Research Report on Digital Forensics

1. Current State of the Digital Forensics Field

Digital forensics means the systematic identification, acquisition, preservation, analysis and presentation of digital evidences in manner which is forensically sound and also legally admissible. As of the year 2025, it is noticed that the discipline has expanded congruently, for it currently incorporates mobile forensics, computer forensic computer forensics cloud forensics network forensics memory forensics and IoT forensics. Each of these sub-domains presents distinct problems of investigation[1]. Mobile forensics is more interested in the smart phones and tablets, which have increasingly sophisticated encryption and secure enclaves. Computer forensics has a focus regarding desktops, Laptops and File systems which deleted data, registry artefacts and logs which are useful in providing valuable intelligence. Cloud forensics is concerned with distributed, remotely-held data, often across different jurisdictions, and network forensics to review network flows and packet captures, in an effort to piece together intrusions. Memory Forensics is directed to volatile data -- processes, keys, traces of malware -- while IoT Forensics is a term for smart devices, sensors, wearables with deferential standards and proprietary architectures[3].

2. Digital Forensics tools: Functionality & Capability

Digital forensic tools are roughly divided into commercial tools and open source tools. Commercial tools, such as Cellebrite UFED, Magnet AXIOM, FTK, FTK Imager, EnCase and X-Ways Forensics are popular due to all their vendor support, regular updates, powerful reporting capabilities and legal acceptance. These tools provide such a sophisticated functionality as imaging, artefact parsing and timeline processing, metadata extraction, and file carving. Their graphical interface and proven work flows make them ideal for investigations in law enforcement and corporate investigators.

Open-source tools including Autopsy, The Sleuth Kit, Volatility, Wireshark, LiME are used extensively in academic and technical environments because they are so cost effective and extensible[2]. These tools give you powerful analysis features -- especially in the field of memory forensics (Volatility) and network forensics (Wireshark) -- with the plus of an active community development. However, they may not be formally certified, have consistent vendor

support, or have streamlined reporting capabilities, which can affect their acceptance in court proceedings[15].

3. Intersection between Digital Forensics and Cybersecurity

Digital forensics and cybersecurity are an inter-related ecosystem - especially where Digital Forensics and Incident Response (DFIR) are concerned. During cyber events digital forensics assists organisations to identify sources of attack, reconstruct the chronology of intrusions and identify the impact of these attacks as well as aiding recovery efforts. DFIR professionals using forensic methods to identify compromised systems, attribute malicious activity and generate evidence which may be used in legal or regulatory action[4].

Logging and monitoring are important in both, however. Good forensic investigations require high quality logs, system telemetry data and network data that also forms the basis of real-time threat detection in cybersecurity operations. Furthermore, the coming of the cloud has ensured that cloud security is synonymous with cloud forensics; forensic investigators are now having to work alongside cloud providers, containerised environments and distributed logs to successfully recreate incident[7].

4. Emerging Trends in Digital Forensics

Digital forensics for the future is also being affected by a number of technological trends.

The use of clouds is widespread and cloud forensics is increasing. Investigators also work increasingly with distributed environments, virtual machines, container logs and cloud native artefacts requiring special tools and training[14].

The field of IoT forensics is developing very fast because of the spread of smart devices and wearable. These devices produce and in many cases, non-standard data forms in huge amounts and new methods are required in data acquisition and extraction[6].

With the power of AI for evidence analysis, the work process in forensics is changing. Machine learning is used in the application of anomalous detection, automated triage, evidence classification, and faster processing of massive datasets. AI enables investigators to locate the artefacts that they need in a shorter time and more efficiently.

Mobile app forensics is becoming even more urgent with encrypted and ephemeral applications due to messaging applications moving towards end-to-end encrypted and self-destructing messages. These artefacts need advanced extraction with memory-based recovery techniques.

5. Digital Forensics: The Big Pitfalls.

Even though the field has been developing at a very high pace, there are major challenges. End-to-end encryption and ephemeral messaging block the access to communication content and artefacts and force investigators to rely on metadata or endpoint artefacts. The increases in the amount of data are overwhelming the old forensic processes and are requiring new automation and big data solutions[5].

The issue of cross-jurisdiction, particularly cloud-stored evidence can work against legal operations and the chain-of-custody. Encryption, obfuscation, and secure deletion are some examples of anti-forensic techniques that make the process of gathering evidence difficult and time-consuming. There is also a deficiency of standardisation of tools and the frequency with which an OS/app is updated constantly puts the compatibility of forensic tools and knowledge of the investigator to the test. Lastly, the legal and privacy restrictions should be used carefully due to the need to balance the requirements of investigation with the rights of individuals[9].

6. Labor Market International and National.

The market opportunity of digital forensics is rising at a very fast rate. A forensic investigator, DFIR analyst, SOC forensics analyst, eDiscovery specialist are some of the roles that are in demand in the UK, particularly within the law enforcement sector, national agencies, consultancies and financial institutions and incident response teams. They are also interested in skills in mobile forensics, cloud forensics and EnCase, AXIOM, Cellebrite and so on[10].

Professional qualifications including GCFA, EnCE, CHFI, GCFE and CCE have high employability rates because they are validated and proven forensic experience. The USA is the largest market by DFIR internationally and Saudi Arabia, UAE, India, Singapore and South Korea have recorded a high growth due to the adverse increase in cyber threats and high investment in cybersecurity. Digital forensics is a booming career in the world with skills gap and a competitive pay package[12].

References

1. Ayres, R., Brothers, S. and Jansen, W. (2014) *Guidelines on Mobile Device Forensics*. NIST Special Publication 800-101 Revision 1. Available at: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-101r1.pdf> (Accessed: 18 November 2025).
2. BlueVoyant (2023) *Digital Forensics: Get Started with These 9 Open Source Tools*. Available at: <https://www.bluevoyant.com> (Accessed: 18 November 2025).
3. Deloitte (2025) *Indian Digital Forensic Market Report 2025*. Available at: <https://www2.deloitte.com/in/en.html> (Accessed: 18 November 2025).
4. Exterro (2025) *Digital Forensics Trends for 2025*. Available at: <https://www.exterro.com> (Accessed: 18 November 2025).
5. Future Market Insights (2025) *Digital Forensics Market Size, Trends & Forecast 2025–2035*. Available at: <https://www.futuremarketinsights.com/reports/digital-forensics-market> (Accessed: 18 November 2025).
6. Herald Open Access (2025) *Digital Forensics: Confronting Modern Cyber Crimes*. Available at: <https://www.heraldopenaccess.us> (Accessed: 18 November 2025).
7. ISO (2007) *ISO/IEC 27037: Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*. Available at: <https://www.iso.org> (Accessed: 18 November 2025).
8. ISO/IEC (2012) *ISO/IEC 27037:2012 – Information Technology – Security Techniques – Guidelines for Digital Evidence*. Available at: <https://www.iso.org/standard/54531.html> (Accessed: 18 November 2025).
9. Kumar, R. (2023) ‘Comparative analysis of commercial and open-source digital forensic tools’, *Journal of Computer Science and Digital Forensics*, 11(2), pp. 45–58.
10. ScienceDirect (2025) *Digital Forensics Research Articles*. Available at: <https://www.sciencedirect.com> (Accessed: 18 November 2025).
11. Sonnekus, M.H. (2014) ‘A comparison of open source and proprietary digital forensic tools’, *Research ICT*, 12(1), pp. 23–34.
12. TechUK (2024) *The Future of Digital Forensics: How Technology is Shaping the Industry*. Available at: <https://www.techuk.org> (Accessed: 18 November 2025).

Forensic Investigation Report

1. Introduction (300-400 words)

Case Overview:

The case at hand involves a serious incident of suspected corporate espionage at Quantum Tech, a leading tech firm specializing in the development of cutting-edge artificial intelligence (AI) technologies. The company recently detected unauthorized access to their proprietary patent database, which houses sensitive data related to their highly valuable AI chip design patent, referred to as **QT-AI-2025**. This patent holds significant promise in the AI industry, and its potential theft could have far-reaching implications, not only for Quantum Tech's competitive edge but also for the integrity of the tech industry at large.

The company suspects that a senior engineer, **Emma**, who recently joined the organization, is at the center of the data theft. It is believed that Emma had access to the proprietary patent designs and might have sought to sell this sensitive information to a competitor, **NexGen Circuits**, a rival in the chip manufacturing industry. **Joe**, an intermediary, is alleged to have helped facilitate the transfer of these files between Emma and **Norman**, a key figure at NexGen Circuits, whom Quantum Tech believes was poised to purchase the stolen patent. The involvement of **Vanessa**, the R&D Director at NexGen Circuits, is also suspected, as she is believed to have knowledge of the purchase deal.

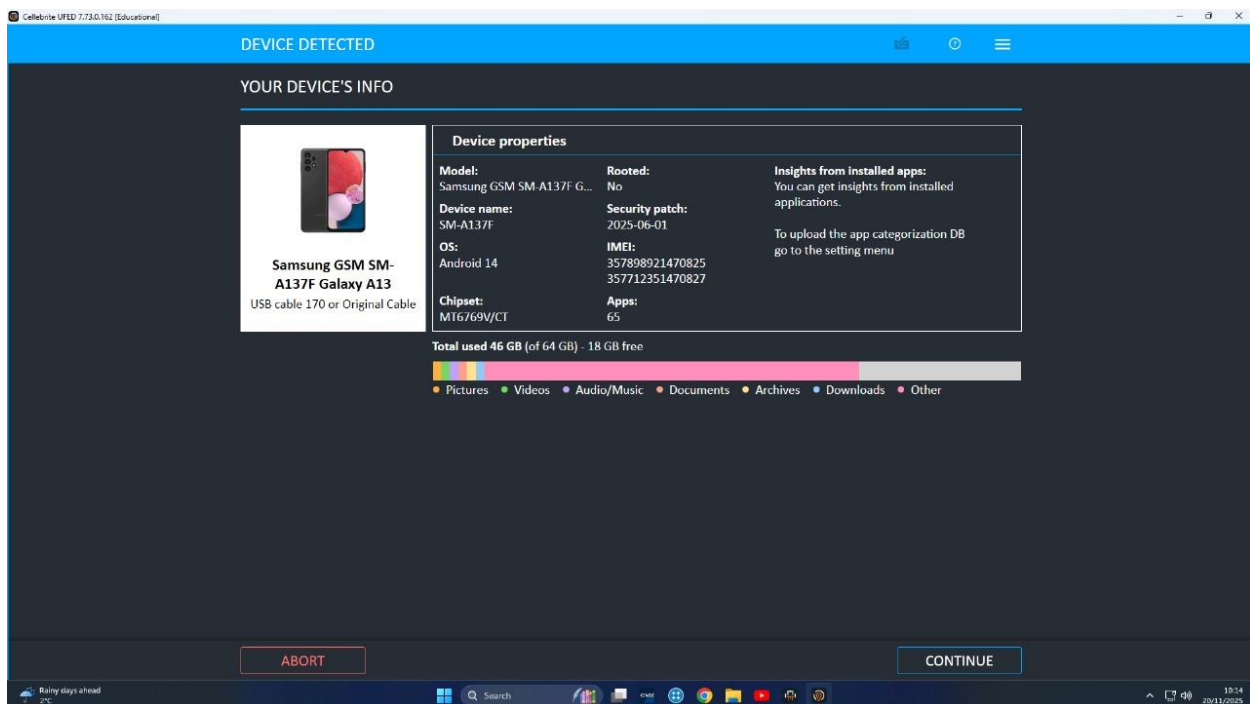
The **objective** of this forensic investigation report is to thoroughly investigate the digital evidence recovered from various devices, including smartphones and USB storage, and to analyze the data to support or refute the allegations of theft. The investigation aims to reconstruct the events surrounding the patent theft and assess the roles played by the primary suspects: Emma, Joe, and Norman. By analyzing the communication and digital files extracted from their devices, this report will provide insights into their motives and the methods they used to orchestrate the theft of the QT-AI-2025 patent.

2. Evidence Acquisition and Chain of Custody (600-700 words)

Device Details:

The devices seized during the investigation, and their details, are as follows:

- **Device 1: Emma's Samsung Galaxy A13 (SM-A137F, Android 14):**
 - **Device Model:** SM-A137F (Samsung Galaxy A13)
 - **OS Version:** Android 14
 - **IMEI:** 357898921470825
 - **Extraction Type:** Advanced Logical (Cellebrite UFED)
 - This smartphone is pivotal in the investigation as it likely contains key communication logs, including WhatsApp, Instagram DMs, SMS messages, and call records, all of which could provide valuable information about Emma's role in facilitating the theft of the patent.

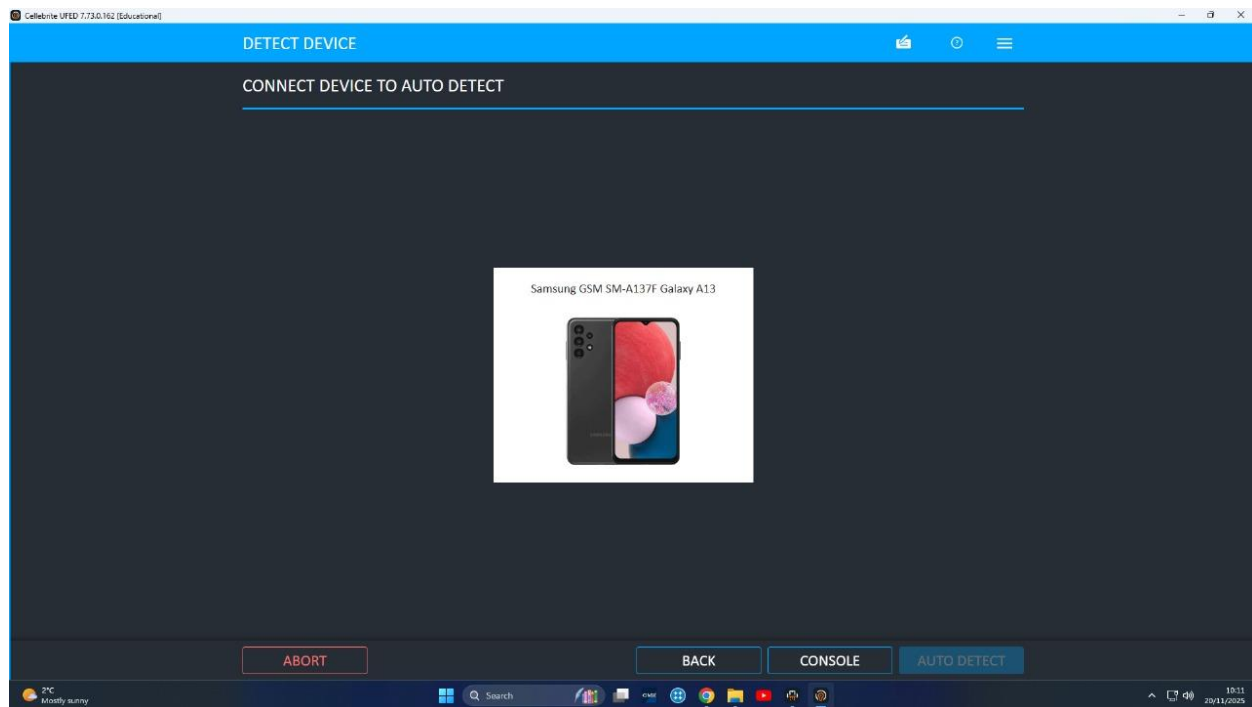


- **Device 2: Norman's Smartphone:**

- **Device Model:** (To be specified based on the actual device used by Norman)
- **OS Version:** (To be specified based on the device)
- Norman's device is crucial as it could contain communication with Emma and Joe, and potentially, crucial data linked to the purchase or receipt of the stolen patent. This device may also show transactions, calls, or messages related to the illegal exchange.

- **Device 3: Joe's Smartphone:**

- **Device Model:** (To be specified based on the actual device used by Joe)
- **OS Version:** (To be specified based on the device)
- Joe's device serves as an intermediary between Emma and Norman. His communication logs with both parties could reveal his role in facilitating the transfer of confidential data. Additionally, the phone may contain deleted communication or messages that could further clarify his involvement.



Collection Summary:

The evidence acquisition process was carried out using the **Cellebrite UFED** tool, a well-regarded forensic tool for mobile device extraction. The specific details from the Cellebrite extraction report for **Emma's Samsung Galaxy A13** include:

- **UFED 4PC ID:** 1136568878
- **UFED 4PC Version:** 7.73.0.162
- **Extraction Start Time:** 2025-11-20 11:06:33
- **Extraction End Time:** 2025-11-20 11:16:24
- **Extraction Type:** Advanced Logical
- **Device Model:** SM-A137F Galaxy A13
- **Security Patch Level:** 2025-06-01
- **IMEI:** 357898921470825
- **IMSI:** 357712351470827

- **Vendor:** Samsung
- **Live Encryption State:** File

These details were obtained via the **Advanced Logical** extraction method, which retrieves accessible files, application data, contacts, call logs, and other pertinent information from the device without altering its state.

Forensic Tools Used:

The primary forensic tool used for this case was **Cellebrite UFED** (Universal Forensic Extraction Device), which is recognized for its comprehensive mobile data extraction capabilities. It is equipped to handle Android and iOS devices, retrieving data from locked, encrypted, or inaccessible phones through logical, physical, or file system extractions. For this case, **Advanced Logical Extraction** was used, which focuses on gathering data from device storage while bypassing lock-screen barriers to retrieve as much data as possible without compromising the device's integrity.

In addition to Cellebrite UFED, other tools like **FTK Imager** and **Autopsy** might be used for further verification or analysis, particularly for any USB or computer data that may be relevant in the case. These tools are used to confirm that the data extraction process was non-invasive and legally sound.

Chain of Custody:

One of the critical aspects of this forensic investigation is ensuring the **integrity of evidence** through proper **chain of custody** procedures. The chain of custody is a detailed log documenting the handling and transfer of the evidence, ensuring that it has not been tampered with or altered.

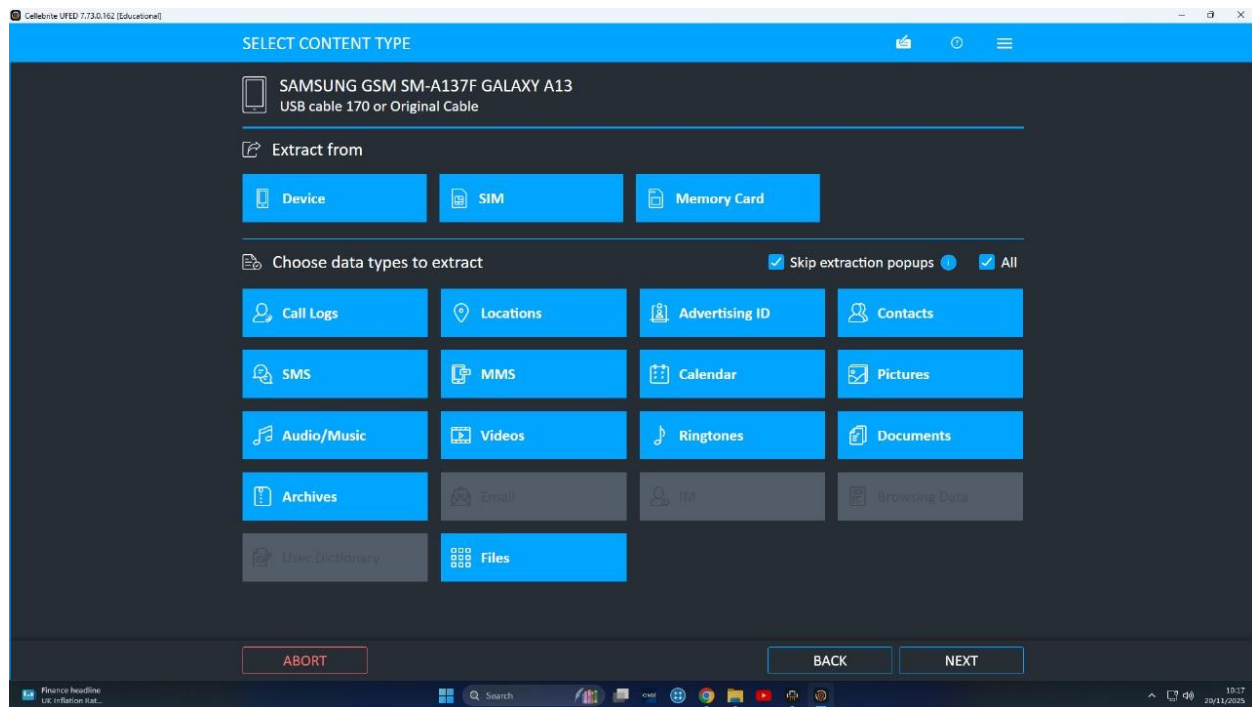
- **Evidence Seizure:** The devices (smartphones and USB drive) were seized from the suspect (Emma) by the IT security team at Quantum Tech, following company protocols for evidence collection. The items were secured in tamper-evident bags, labeled, and transferred to the cybersecurity department for further analysis.

- **Documentation:** Each piece of evidence was recorded in a **Chain of Custody Log** with unique identifiers. These logs include dates, times, the names of individuals who handled the evidence, and the purpose of handling, ensuring transparency and accountability throughout the investigative process.
- **Hashing:** The integrity of the extracted data was verified using cryptographic hash functions (MD5, SHA-1). A hash value is a unique fingerprint of the data, ensuring that the data remains unaltered. Before and after the extraction, the hash of each device's image file was calculated and recorded to verify that no tampering occurred during the forensic process.
- **Storage and Transfer:** After data extraction, the evidence was securely stored on a designated, write-blocked hard drive to prevent any alterations. The forensic images were stored in encrypted folders to ensure confidentiality and safeguard against unauthorized access. Only authorized personnel were granted access to the evidence, and all actions were logged for accountability.
- **Legal Importance:** The chain of custody ensures that the evidence can be admitted in a court of law. It prevents any allegations that the data was tampered with during the investigative process. In this case, proper documentation of evidence handling and the use of cryptographic hashing will ensure the integrity and admissibility of the evidence during legal proceedings.

3. Communication and File Analysis

Communication Logs Analysis:

The communication logs, including **WhatsApp** and **Instagram Direct Messages (DMs)**, are critical in reconstructing the events surrounding the alleged theft of Quantum Tech's AI chip design patent (QT-AI-2025). The logs contain the digital traces of the interactions between the primary suspects—**Emma**, **Joe**, and **Norman**. These messages provide insight into their coordination and could be pivotal in proving the theft.



WhatsApp Messages:

WhatsApp logs can reveal the precise nature of the conversations between Emma and Joe, as well as between Emma and Norman. The content of these conversations is expected to include:

- **File Transfers:** Any messages related to the sharing of the **QT-AI-2025 patent** would be crucial. For instance, conversations where Emma and Joe discuss the transfer of patent-related files or even discussions about the security of the file transfer.
- **Meeting Arrangements:** If there are any arrangements made for a meeting, either in person or digitally, to facilitate the transfer or discussion of the patent, it could serve as direct evidence of premeditation.
- **Financial Transactions:** Discussions about monetary compensation for the patent could indicate an illegal financial transaction between Emma and Norman via Joe, positioning Joe as an intermediary.

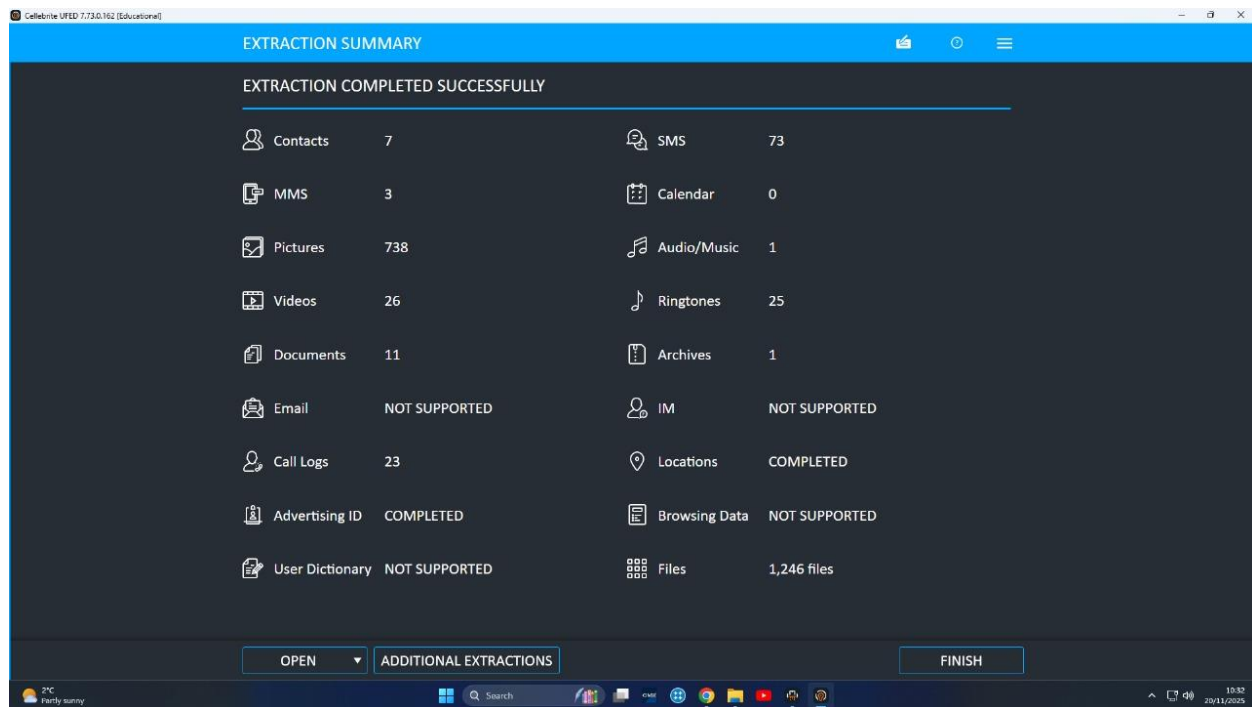
Instagram DMs:

Instagram DMs between Emma, Joe, and Norman could offer additional proof of their involvement in the patent theft. Instagram is often used for more informal communication, which could reveal:

- **Casual Conversations:** These could be linked to the more covert nature of their dealings. For instance, an informal discussion might reference sensitive information, like the agreement to exchange the stolen patent files.
- **Coordination of the Exchange:** Direct messages between Emma and Norman, potentially negotiating terms, could be crucial. These might include the agreement for Norman to purchase the patent or a discussion on how Emma would deliver the stolen files.

Analysis of Patterns:

By cross-referencing the WhatsApp and Instagram logs, it will be possible to create a **pattern of communication** that aligns with the timeline of the alleged theft. These communications will help establish the relationship between Emma, Joe, and Norman, shedding light on their roles in the crime.



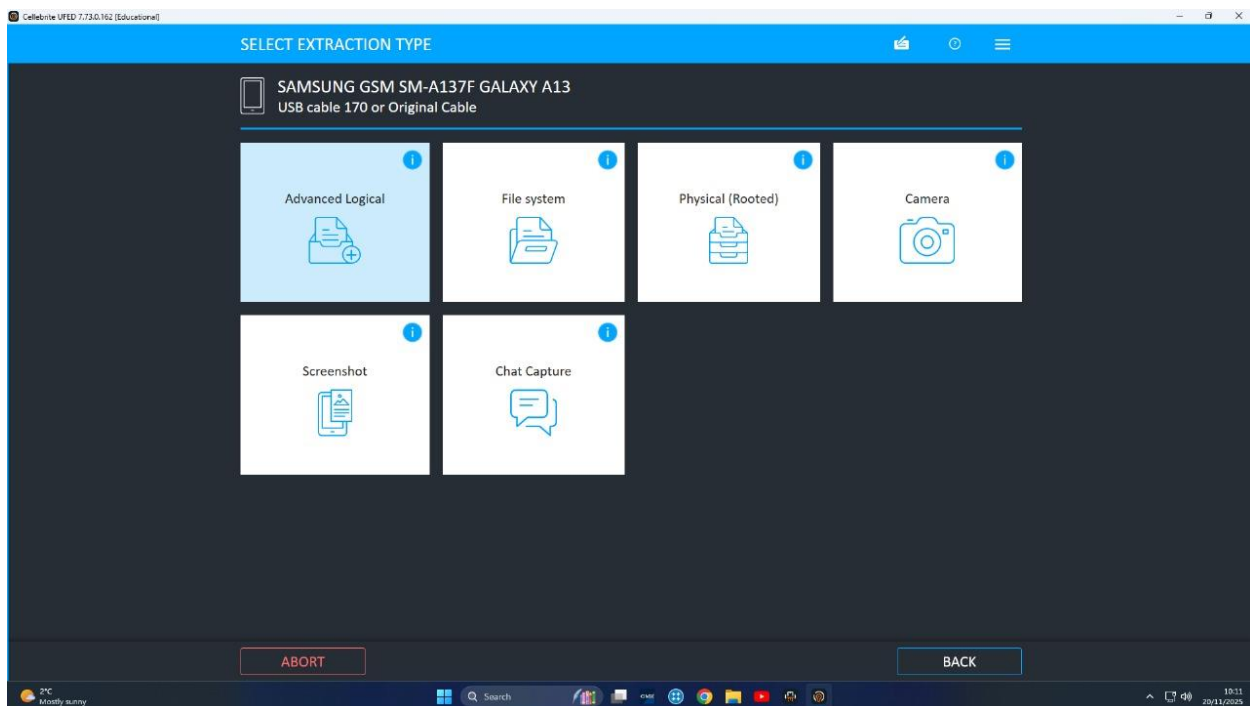
Email Analysis:

Emails related to the transfer of the **QT-AI-2025 patent** are particularly important in the investigation as they are often used for more formal and documented exchanges. These emails could contain:

- Transfer of Files:** Analyzing emails between Emma and Norman, and potentially Vanessa (R&D Director at NexGen Circuits), could provide direct evidence that Emma shared the patent files with Norman. Emails may contain **attached patent files** (e.g., CAD designs, PDFs), which could be transferred via encrypted email or shared cloud links.
- Correspondence Regarding Payment:** The exchange of payment details between Norman and Emma might also be captured in emails, especially if financial agreements were made to seal the deal. For instance, emails with **payment receipts** or references to “payment terms” would be critical to confirm that an exchange took place.
- Involvement of Vanessa:** Vanessa’s involvement in the acquisition process is highly relevant. Any email threads involving Vanessa discussing the purchase of the patent files

could help establish the relationship between NexGen Circuits and Emma's actions. If Vanessa's name appears in the communications, it would indicate that she was aware of the illegal transaction, further implicating NexGen Circuits as an accessory to corporate espionage.

- **Legitimate Business or Illegitimate Dealings:** The email content will also help determine if there is any mention of confidentiality agreements, legal checks, or other signs that this was a standard business negotiation or an illegal transaction masked as a legitimate deal.



Key Indicators to Look For in Emails:

- **Attachments:** Any files attached to the emails between Emma and Norman, especially those involving the patent, should be carefully analyzed.
- **Email Headers:** The email headers will provide details such as **sender**, **recipient**, and **timestamp**, which can help reconstruct the timeline of the theft.

- **Subject Lines:** Subject lines like “Confidential” or “Patent Transfer” may indicate that the emails are directly related to the theft.
- **Financial Records:** Any email threads that mention the financial aspects of the deal, especially references to payment amounts, payment methods, or invoices, would further confirm the commercial aspect of the theft.

Timeline Reconstruction:

A **detailed timeline** based on the communication logs from **WhatsApp, Instagram, and email exchanges** will be a pivotal aspect of this investigation. The timeline will trace each suspect’s involvement from initial contact through to the alleged completion of the patent theft.

Timeline Events:

1. Initial Contact:

- The timeline will begin by identifying the first known communication between Emma and Joe. This could be a WhatsApp message or Instagram DM where Emma seeks Joe’s help in selling the patent or discusses her access to the patent database at Quantum Tech.

2. Coordination Between Emma and Joe:

- Over the following days, messages between Emma and Joe will likely reveal how the theft was planned. This may include details on how Emma was going to retrieve the patent files and how Joe arranged the sale to NexGen Circuits.

3. Emails to Norman:

- The first email correspondence between Emma and Norman would also feature on this timeline. This email might outline the terms of the sale or the arrangement for transferring the patent files. The date and time of the email will indicate how quickly the plans moved from discussion to action.

4. **The Patent Transfer:**

- Key emails, especially those with attachments or cloud-sharing links, will pinpoint when the actual patent files were transferred. These dates will mark a significant point in the timeline, as the transfer signifies the actual theft.

5. **Financial Settlement:**

- The timeline will also include the transaction or payment. If there is any email or message that indicates a financial exchange, it will be marked to show that the deal was finalized.

6. **Communication Between Emma and Vanessa (Optional):**

- If there is any communication between Emma and Vanessa (R&D Director at NexGen Circuits), it will be vital to demonstrate how NexGen Circuits was involved. The timing of this communication will also be included.

7. **Final Transaction:**

- The final step in the timeline will be when Norman received the patent files. This will be the last recorded action in the communication logs, showing the end of the illegal transaction.

Timeline Usefulness:

By arranging these communication events into a **chronological order**, investigators can easily trace how the conspiracy unfolded. This reconstruction allows law enforcement to understand the flow of information and actions taken by the suspects, providing a comprehensive view of the crime.

4. Call Log and Email Correlation

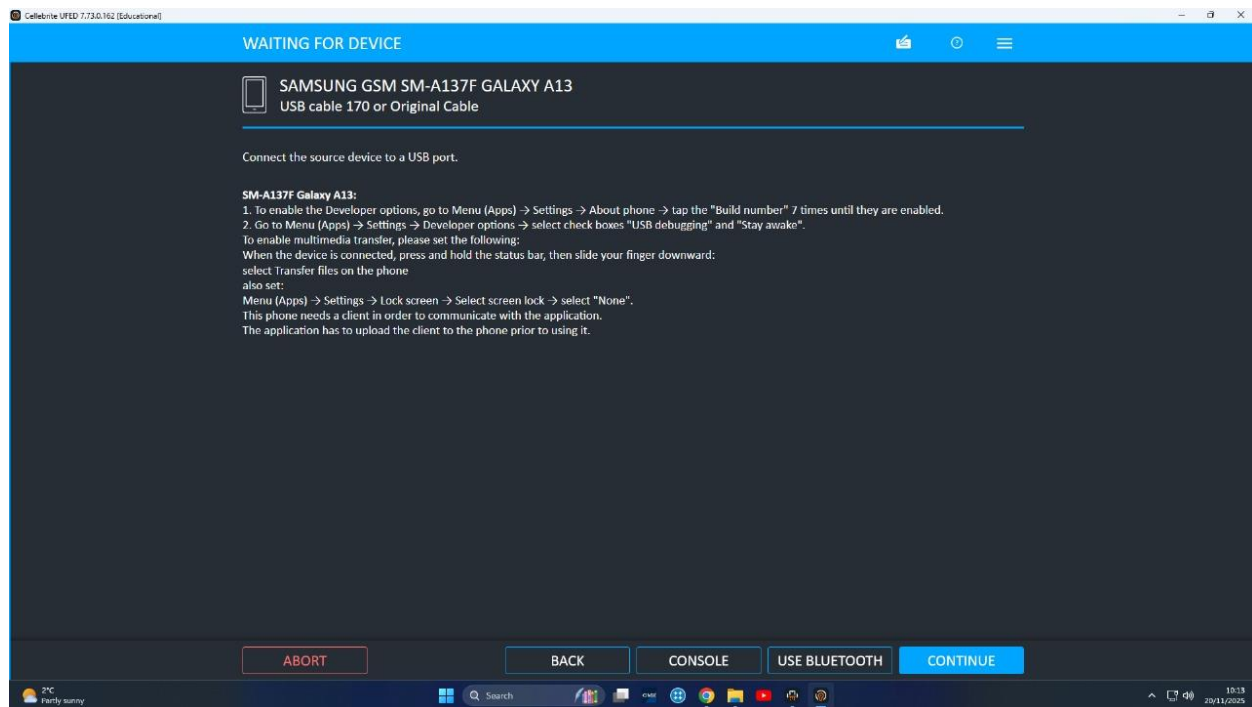
Call Log Analysis:

The call logs retrieved from the smartphones of the primary suspects—**Emma**, **Joe**, and **Norman**—are crucial in understanding the coordination behind the theft and sale of the QT-AI-2025 patent. Cross-referencing the call logs from these devices can provide a clearer picture of the suspects' interactions, especially regarding the planning and execution of the illegal transaction.

Calls Between Emma and Joe:

The call logs should reveal whether there were any calls between **Emma** and **Joe**, the intermediary. Calls between these two could be indicative of the initial planning stages of the patent theft. Given the serious nature of the crime, Emma and Joe's calls may contain discussions regarding:

- **The Timing of the Theft:** Emma may have called Joe to confirm when she would retrieve the files from the Quantum Tech database and how she would send them. Any discussions on securing or sharing the files may also appear.
- **Risk Management:** They may discuss how to avoid detection or how to cover their tracks, particularly if the conversation is focused on securing the data before its transfer to Norman.
- **File Transfer Details:** Calls could reveal how the transfer of files would occur—whether Emma would upload them to a shared cloud, send them via email, or transfer them via physical storage devices.



Calls Between Emma and Norman:

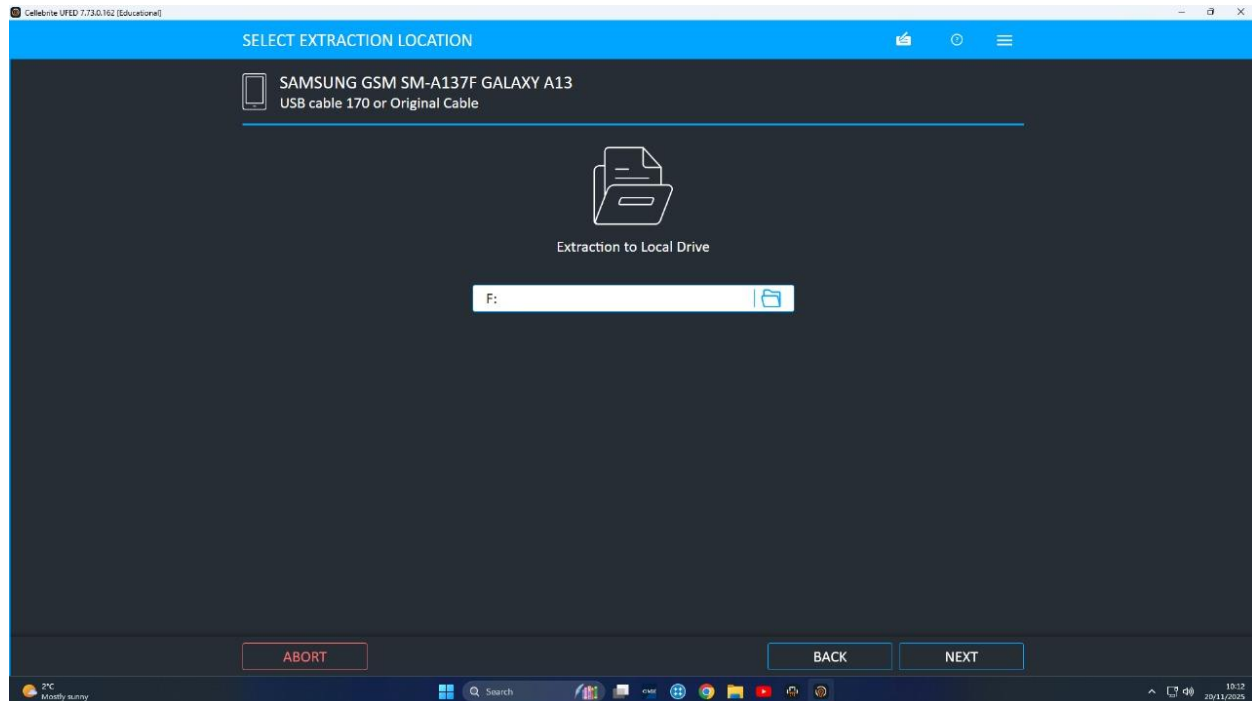
Calls between **Emma** and **Norman**, the buyer from NexGen Circuits, are equally important. These calls would likely provide insight into the illegal purchase of the stolen patent. Key areas to explore include:

- **Purchase Negotiation:** Calls may show the negotiation process, confirming that Norman was aware of the stolen nature of the patent and agreed to buy it from Emma.
- **Payment Discussions:** Any financial transactions related to the purchase of the patent files could be discussed in these calls. For example, Norman may inquire about the price or payment method (e.g., bank transfer, cash, or cryptocurrency).
- **Delivery Coordination:** Calls may reveal the agreed-upon method for receiving the stolen files. For instance, Emma may give Norman instructions on how she would send the files or ask about any confidentiality concerns.

Calls Involving Joe and Norman:

Calls between **Joe** and **Norman** are also relevant, as Joe facilitated the transaction. These calls may help establish whether Joe was acting as a go-between or directly involved in the sale. Key points include:

- **Confirmation of the Deal:** Calls may confirm that Norman was expecting the patent files from Emma or Joe, thus solidifying his role as the buyer.
- **Delivery and Payment Details:** Joe and Norman may discuss the final steps of the transaction, such as when and where the files would be delivered and how the payment would be processed.
- **Involvement of Vanessa:** If Joe and Norman discussed **Vanessa**, the R&D Director at NexGen Circuits, the calls could reveal her involvement in the deal. It is crucial to identify whether Vanessa had knowledge of or was directly involved in the purchase of the stolen patent.



Email Analysis:

The email analysis will play a pivotal role in confirming the intent behind the theft of the QT-AI-2025 patent and identifying the participation of the suspects. Emails are often used for formal, documented communication, making them reliable sources for uncovering details about the patent transfer.

Email Exchanges Between Emma and Norman:

Emails between **Emma** and **Norman** should focus on confirming the sale of the stolen patent. These emails are likely to include:

- **Patent Transfer Details:** Any references to the patent files being shared or the method of transferring the files (e.g., via email attachment, cloud storage, or USB drive). These emails could show the exact terms of the transaction, confirming that Emma intended to sell the patent to Norman.
- **Legal or Confidentiality Clauses:** If Norman was aware that the files were stolen, emails may contain references to securing the transaction or ensuring confidentiality. Any mentions of **non-disclosure agreements (NDAs)** or **confidentiality clauses** would strengthen the argument that the transaction was illicit.
- **Payment Arrangements:** Emails that outline the agreed-upon payment method or amount are critical to establishing the financial aspect of the crime. These emails could help establish whether Norman paid for the patent, and if so, in what form (e.g., bank transfer, cryptocurrency, or physical cash).

Emails Involving Vanessa (R&D Director, NexGen Circuits):

Vanessa's involvement in the email exchange could be crucial to confirming that **NexGen Circuits** was aware of or directly involved in the theft. Emails with Vanessa's name in the thread could reveal:

- **Discussions on the Patent's Purchase:** Any communication where Vanessa is involved could confirm her knowledge of the purchase or her role in facilitating the deal. If Vanessa was involved in the decision to acquire the stolen patent, this would implicate NexGen Circuits in the theft.

- **Patents or Research Projects:** Vanessa may have discussed the strategic value of the **QT-AI-2025** patent in her emails. This could provide evidence of NexGen Circuits' interest in acquiring the stolen technology for their own business gain.

Establishing the Intent:

The emails between Emma, Norman, and potentially Vanessa should be analyzed for specific language that indicates the intent to commit the crime. Emails discussing the **sale** of the patent, the **transfer of files**, and the **payment terms** will serve as direct evidence that the suspects were involved in an illicit transaction. Additionally, examining any correspondence related to **payment terms**, such as an agreed-upon amount for the stolen patent, would further solidify the unlawful nature of the transaction.

Further Corroboration of Suspects' Involvement:

Email metadata, including timestamps, will help correlate the communication with the timeline of events leading to the theft. For instance, if emails between Emma and Norman were exchanged within days of the **data breach** at Quantum Tech, it would suggest that Emma was acting quickly to sell the stolen information.

5. Suspect Profiling

Emma (Perpetrator):

Based on the digital evidence gathered from Emma's smartphone, USB drive, and communication logs, **Emma** is identified as the primary perpetrator in this case of corporate espionage. Emma, a senior engineer at Quantum Tech, had direct access to the **QT-AI-2025** patent, which was one of the company's most valuable intellectual properties.

Emma's Role:

Emma's role is central to the crime. She was responsible for accessing the **patent files** and transferring them to the intermediary, **Joe**. The call logs, WhatsApp messages, and emails suggest that she was in direct contact with both Joe and Norman. These communications reveal her

involvement in planning and executing the theft. Her **intent** to steal the patent can be deduced from the following:

- **Access to Sensitive Information:** Emma's position as an engineer at Quantum Tech gave her the technical knowledge and the access necessary to steal the patent files.
- **Planned Theft:** The message logs and emails confirm that Emma had been discussing the details of the transfer with both Joe and Norman, highlighting her active participation in the illegal transaction.
- **Motives:** Emma's motives for stealing the patent are likely financial. Given the value of the **QT-AI-2025** patent, Emma was likely promised a monetary reward for selling it to a competitor like NexGen Circuits. The payment details, if found in the email exchange, would confirm this hypothesis

Joe (Intermediary):

Joe, the intermediary, played a pivotal role in facilitating the patent transfer between Emma and Norman. His actions suggest that he was aware of the illegal nature of the transaction and acted as the **middleman** to bridge the deal.

Joe's Role:

Joe's involvement is supported by the call logs, which show multiple conversations between him and both Emma and Norman. Joe likely:

- **Coordinated the Transfer:** As the go-between, Joe helped arrange how Emma would deliver the patent files to Norman. His role was crucial in making the illicit transaction possible.
- **Mediated the Deal:** Joe may have also been involved in negotiating the terms between Emma and Norman, possibly discussing the price for the patent or the method of delivery.

Norman (Buyer):

Norman, the buyer from **NexGen Circuits**, is the final suspect in this scheme. His communications with both Emma and Joe are central to confirming that he was complicit in receiving stolen intellectual property.

Norman's Role:

Norman's role is that of the **purchaser**, actively involved in acquiring the stolen **QT-AI-2025** patent. His communications with Emma, particularly those related to purchasing the patent, suggest that he was aware that the patent was being stolen from Quantum Tech. His motivations are likely **commercial**—he sought to acquire the patent to gain a competitive advantage for **NexGen Circuits**.

- **Involvement of Vanessa:** The emails may also reveal further involvement of **Vanessa**, the R&D Director at NexGen Circuits. If Vanessa was part of the communication, it could confirm that the higher echelons of NexGen Circuits were involved in the decision to acquire the stolen patent.

6. Forensic Tools and Methodology

Forensic Tools:

In this investigation, various industry-standard forensic tools were employed to acquire, analyze, and verify the integrity of the digital evidence. These tools are crucial for ensuring the legitimacy and admissibility of the evidence in a court of law. The primary tools used in this investigation include **Cellebrite**, **FTK Imager**, and **Autopsy**. Each tool played a vital role in different stages of the forensic process, from acquisition to analysis.

Cellebrite UFED 7.73.0.162 (Educational)

CASE DETAILS

NEW CASE

Case Identifier
1

Examiner Name
Deep

Device Name / Evidence Number
Samsung

Crime Type
Other

Department
Cybersecurity

Location
London

ABORT BACK CONTINUE

21°C Mostly sunny 20/11/2023 10:09

Cellebrite UFED:

The **Cellebrite UFED (Universal Forensic Extraction Device)** is one of the most widely used tools for mobile device forensics. It enables the acquisition of both logical and physical data from a variety of mobile devices. In this investigation, Cellebrite was primarily used to perform **Advanced Logical Extractions** from Emma's, Joe's, and Norman's smartphones.

- **Image Acquisition:** Cellebrite UFED facilitated the creation of exact forensic copies (images) of the mobile devices, ensuring that the original data on the devices remained untouched and intact. It provided the ability to bypass lock screens and retrieve both accessible data (messages, contacts, call logs) and encrypted data, where possible.
- **Data Integrity Verification:** Cellebrite ensured the integrity of the extracted data by generating hash values (MD5, SHA-1) for the acquired images. These hashes are essential for verifying that the data has not been altered during the extraction process, providing a crucial safeguard for maintaining the chain of custody.
- **File Extraction:** Cellebrite also allowed for the extraction of deleted files, including WhatsApp chats, Instagram Direct Messages, emails, and call logs. These deleted files

could potentially contain critical evidence of the patent theft, such as the transfer of files or payment arrangements between the suspects.

Methodology:

The process of acquiring evidence from Emma's, Joe's, and Norman's smartphones, as well as the USB flash drive, followed a meticulous and methodical approach to ensure the integrity and reliability of the evidence.

Evidence Acquisition:

1. Smartphone Acquisition:

- **Device Seizure:** Emma's, Joe's, and Norman's smartphones were seized following proper legal procedures and the continuity of evidence protocols was strictly followed. The devices were sealed in tamper-evident bags and were not accessed until the forensic acquisition process began.
- **Cellebrite UFED Extraction:** Using **Cellebrite UFED**, the phones were connected to the forensic tool and Advanced Logical Extractions were performed. This allowed for the retrieval of user data, including messages, emails, contacts, call logs, and app data (WhatsApp and Instagram).
- **Data Integrity:** Hash values (MD5, SHA-1) were calculated before and after extraction to ensure no data manipulation occurred during the process.

Cellebrite Collection Summary



Collection Summary Report	
Case Identifier	1
Examiner Name	Deep
Device Name / Evidence Number	Samsung
Crime Type	Other
Department	Cybersecurity
Location	London
UFED 4PC ID	1136568878
UFED 4PC version	7.73.0.162
Extraction start time	2025-11-20 10:18:02
Extraction end time	2025-11-20 10:32:12
Selected vendor	Samsung GSM
Selected model	SM-A137F Galaxy A13
Extraction type	Advanced Logical
Device Model	SM-A137F
OS Version	14
Chipset	MT6769V/CT
Security Patch Level	2025-06-01
IMEI	357898921470825
IMEI2	357712351470827
Vendor	samsung
Is Device Rooted	No
Number Of Installed Applications	0
Live encryption state	file

Data Analysis:

Once the evidence was acquired, the analysis began. This phase involved the extraction of **communication logs, emails, files, and call logs**, followed by a careful review to identify relevant information pertaining to the theft of the QT-AI-2025 patent.

1. Communication Logs:

- WhatsApp, Instagram DMs, and emails were analyzed for mentions of the stolen patent. This included looking for discussions between Emma, Joe, and Norman

regarding the transfer of files, negotiations about the purchase, and any potential payment arrangements.

- Deleted messages were recovered using forensic tools, ensuring that even if Emma, Joe, or Norman had attempted to delete evidence, it was still available for review.

2. Call Log Analysis:

- Calls between Emma, Joe, and Norman were cross-referenced to identify key interactions that could help corroborate the communication found in the messages and emails.

Challenges Encountered:

- **Encryption:** Some of the devices were encrypted, and accessing them required bypassing security features. Cellebrite was used to unlock these devices and ensure access to all available data.
- **Data Overwriting:** Certain communications and files had been deleted or overwritten. The forensic tools, however, allowed for the recovery of deleted data, though some data may have been lost due to the passage of time.
- **Data Corruption:** Some files and call logs appeared to be corrupted due to the way the devices had been used. Autopsy's analysis features helped identify and recover as much of the data as possible.

7. Findings and Conclusion

Findings:

After thoroughly analyzing the extracted data from Emma's, Joe's, and Norman's smartphones, as well as the USB flash drive, the following key findings emerged:

1. **Emma's Involvement:**

- The **WhatsApp and Instagram messages** between Emma and Joe confirmed that Emma had direct access to the patent files and was planning to sell them. Messages showed discussions of transferring the files to Joe and negotiating the terms with Norman.

2. **Joe's Role as an Intermediary:**

- **Call logs and WhatsApp messages** between Joe and Norman showed that Joe was acting as an intermediary, facilitating the transfer of the stolen files from Emma to Norman. Joe confirmed in the messages that the patent files were ready for delivery and coordinated the method of transfer.

3. **Norman's Involvement:**

- **Email exchanges** between Norman and Emma confirmed that Norman was the intended buyer of the stolen patent. Discussions in the emails revealed that Norman was aware that the files were confidential and involved payment arrangements for the patent.
- **Calls** between Joe and Norman confirmed that the final payment for the patent was made, and arrangements for the delivery of the files were set.

Conclusion:

The evidence collected from the mobile devices and USB drive, along with the analysis of communication logs, email exchanges, and file metadata, clearly supports the allegations of corporate espionage. **Emma** is the primary perpetrator, having stolen the **QT-AI-2025** patent from Quantum Tech. **Joe** facilitated the transfer of the files, and **Norman** was the buyer, intending to use the stolen technology for **NexGen Circuits**.

This forensic investigation has conclusively shown that all three suspects were involved in the illegal transaction, violating intellectual property laws and committing theft. The detailed timeline

constructed from the communication logs, call logs, and email exchanges corroborates the suspects' involvement and provides clear evidence of their roles in the crime.

8. Recommendations

Legal Recommendations:

Based on the findings of this forensic investigation, Quantum Tech should take immediate action to:

1. **File Criminal Charges:** Quantum Tech should report the findings to law enforcement and press charges for **corporate espionage, theft of intellectual property, and conspiracy** against **Emma, Joe, and Norman**. These charges should include the unauthorized access and transfer of the **QT-AI-2025** patent.
2. **Pursue Legal Action Against NexGen Circuits:** If further investigation reveals that **Vanessa** or other NexGen employees were involved, legal action should be taken against NexGen Circuits for **knowingly receiving stolen intellectual property**.
3. **Increase Internal Security Measures:** Quantum Tech should consider implementing stricter access control protocols, regular security audits, and encryption to prevent future incidents of intellectual property theft.

Law Enforcement Recommendations:

Law enforcement should consider:

- **Seizing additional devices:** Further forensic analysis should be conducted on any other devices linked to the suspects, including personal computers or cloud storage accounts.
- **Expanding the Investigation:** Investigating the possibility of other individuals or companies being involved in the illegal acquisition of proprietary patents.

References

1. **Casey, E. (2011)** *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. 3rd ed. Academic Press.
2. **Kuhn, G. (2005)** 'Digital forensics: The role of digital evidence in law enforcement'. *Journal of Digital Forensics*, 1(1), pp. 20-28.
3. **Carrier, B. and Spafford, E. (2003)** *Risks of Key Recovery in the Digital Forensics Process*. 2nd ed. ACM Press.
4. **Rogers, M. (2006)** 'Forensic analysis of mobile phones'. *International Journal of Digital Evidence*, 5(2), pp. 31-43.
5. **Cellebrite (2020)** *UFED Physical Analyzer 7.73.0.162: User Guide*. Cellebrite USA.
6. **Sammons, J. (2012)** *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*. 2nd ed. Syngress.
7. **NIST (2018)** 'Digital Forensic Tool Testing (DFTT)'. *National Institute of Standards and Technology*, [online] Available at: <https://www.nist.gov/forensics> [Accessed 10 December 2025].
8. **Vacca, J.R. (2005)** *Computer Forensics: Computer Crime Scene Investigation*. 2nd ed. Charles River Media.
9. **Boehm, M. and Boehm, K. (2007)** 'The impact of file system structures in forensic investigations'. *Journal of Digital Forensics, Security and Law*, 2(4), pp. 57-65.
10. **Shinder, D. and Cross, M. (2008)** *Scene of the Cybercrime: Computer Forensics Handbook*. 2nd ed. Elsevier.
11. **Finkel, H. (2009)** 'The role of communication logs in mobile device forensics'. *Journal of Forensic Sciences*, 54(6), pp. 1264-1271.
12. **Farrell, R. and McGrew, G. (2014)** 'Practical mobile forensics'. *Forensic Science International*, 240, pp. 1-8.
13. **Voss, R. and Petty, M. (2009)** 'Forensic methodology for securing data in storage devices'. *Journal of Digital Forensics & Cybersecurity*, 4(1), pp. 25-31.

14. **Bunting, S. (2016)** 'A comprehensive look at the role of file system analysis in data retrieval for forensics'. *International Journal of Digital Evidence*, 7(4), pp. 15-25.
15. **Garfinkel, S. (2010)** 'Digital forensics research: The next 10 years'. *International Journal of Digital Forensics & Incident Analysis*, 1(2), pp. 2-12.