

LEVEL 7 ASSESSMENT SPECIFICATION

Student name:	Rajesh Barua	Student number:	ID 2513042
Programme:	MSc/PgDip/PgCert Cybersecurity and Digital Forensics		
Module:	Digital Forensics Analysis		
Module code:	ACCA7031	Contribution to Overall Module Assessment (%):	100%
Lecturer:	Dr. Nitheesh Kaliyamurthy	Internal Verifier:	Mr. Munyaradzi Murira
Assignment Title:	Research, Analyse and Investigate Cybersecurity incidents and perform digital forensic assessment	Word count (or equivalent):	5000
Submission deadline:	11th May 2026 AND 14th May 2026	Return date of provisional marks & written feedback:	20 Working Days after Submission

Contents

Contribution to Overall Module Assessment (%):	1
1 Current State of Digital Forensics: Tools, Features, and Capabilities.....	3
2 Intersection of Digital Forensics and Cybersecurity.....	3
3 Emerging Trends in Digital Forensics	4
4 Key Challenges in Digital Forensics	5
5 National and International Job Market in Digital Forensics.....	5
1. Evidence Acquisition	6

1.1 Acquisition Process	6
1.2 Continuity of Evidence	6
1.3 Hash Verification	7
2. Communication Analysis	7
2.1 Overview of Communication Sources	7
2.2 Key Communication Analysis	8
2.3 Communication Log Summary (Table Format)	8
3 File Analysis	11
3.1 Objective:	11
3.2 Analysis:	11
3.3 Findings:	11
4.1 Call Log Analysis	11
4.2 Email Analysis	13
5: Suspect Profiling	13
5.1 Emma (Primary Perpetrator)	13
5.2 Joe (Intermediary / Middleman)	14
5.3 Norman (Suspected Buyer / Associate)	14
5.4 Additional Evidence Assessment	14
6: Forensic Images	15
6.1 Huawei POT-LX1P Smart	15
6.2 Nokia C2	16
6.3 Samsung and Verified Hash	17
6.2 Note 14	18
7 Forensic Investigation Report	19
7.1. Case Background	19
7.2. Scope of Investigation	20
7.3. Evidence Inventory	20
7.4 Methodology: Tools and Techniques Used for Acquisition and Analysis	21
7.5 Chain of Custody	22
7.6 Findings	22
7.7 Finding Conclusion	24
7.8 Recommendations	24
8 References:	24

1 Current State of Digital Forensics: Tools, Features, and Capabilities

Digital forensics is a vital field in cybercrime investigations, enabling the recovery, analysis, and presentation of data from digital devices such as computers, mobile phones, and cloud storage. The field has evolved significantly, with advancements in technology leading to the development of specialized tools to assist forensic investigators.

Some of the most widely used digital forensics tools include:

1. **EnCase Forensic:** A comprehensive tool offering features for data acquisition, forensic analysis, and reporting. It supports various file systems and is crucial for recovering deleted data, making it indispensable when dealing with large volumes of data [1].
2. **Cellebrite UFED:** Specializing in mobile forensics, Cellebrite UFED enables the extraction and analysis of data from mobile devices, including texts, photos, and app data. It is widely used for mobile crime investigations and can bypass mobile security measures [2].
3. **FTK Imager:** This tool is focused on creating disk images, verifying data integrity, and examining file systems. It is essential for data recovery from damaged devices and provides detailed reporting on the status of digital evidence [3].
4. **Autopsy:** An open-source platform offering tools for timeline analysis, file carving, and disk image analysis. It is commonly used for analyzing forensic artifacts and investigating incidents involving large data sets [4].

These tools process data from multiple sources, extract evidence, and ensure data integrity, playing a vital role in modern digital investigations.

2 Intersection of Digital Forensics and Cybersecurity

Digital forensics and cybersecurity are deeply intertwined fields, both playing a critical role in protecting digital environments from evolving threats. Cybersecurity focuses on defending systems, networks, and data from unauthorized access, breaches, and attacks. It establishes proactive defenses like firewalls, encryption, and intrusion detection systems. However, when these defenses fail or when an incident occurs, digital forensics takes over. It involves the recovery, analysis, and presentation of digital evidence to understand the attack's origin, its impact, and the perpetrators behind it [1], [2].

Cybersecurity's primary role is to prevent attacks by implementing robust security measures. But, when breaches occur, digital forensics steps in to investigate how and why the attack succeeded, uncovering vulnerabilities and gathering vital evidence for further security improvements or legal action [3], [4]. For example, in the case of a cyberattack or data breach, cybersecurity experts contain the threat and secure affected systems, while forensic specialists

analyze logs, recover deleted files, examine network traffic, and create a timeline of events to identify how the attack unfolded.

Together, these two disciplines complement each other — cybersecurity provides proactive defense, and digital forensics enables effective post-incident investigation. This integrated approach ensures that organizations are equipped not only to defend against cyber threats but also to recover and learn from breaches, ultimately enhancing data integrity and system security [5], [6].

In today's digital world, the synergy between cybersecurity and digital forensics is critical for maintaining security and resilience. With cybercrime becoming increasingly sophisticated, the collaboration between these fields is indispensable for both prevention and investigation [1], [6].

3 Emerging Trends in Digital Forensics

As technology evolves, digital forensics is rapidly adapting to handle increasingly complex cybercrimes and the vast amount of digital data generated daily. Traditional forensic techniques are no longer sufficient; investigators must embrace new methods to remain effective in modern law enforcement and cybersecurity contexts.

One major trend is **mobile and cloud forensics**, driven by the widespread use of smartphones and cloud services. Modern investigations increasingly involve extracting evidence from mobile devices and remote cloud storage, which requires specialized tools and approaches to handle distributed and virtualized data sources [1], [2].

Another significant development is the integration of **artificial intelligence (AI) and machine learning (ML)** into forensic workflows. AI-enabled systems can automate data processing, detect anomalies, and analyze patterns across large datasets far faster than manual methods. These technologies are improving evidence extraction, prioritizing relevant artifacts, and reducing investigation time [2], [3].

The rise of **blockchain and cryptocurrency forensic analysis** has also become critical. Investigators now use blockchain analytics to trace digital currency transactions and uncover fraud, money laundering, and ransomware activities. Advances in tracing transparent but pseudonymous blockchain records are enabling more effective tracking of illicit financial flows.

With the explosion of connected devices, **Internet of Things (IoT) forensics** has emerged as its own specialized domain. Smart home appliances, wearables, and industrial sensors produce vast amounts of device-generated data that can serve as crucial evidence. IoT forensics focuses on challenges such as heterogeneous hardware, distributed networks, and resource constraints during evidence collection and analysis [4], [7].

Finally, **big data analytics** is reshaping how investigators handle massive digital evidence sets. By applying analytical frameworks capable of processing distributed and varied datasets from networks, endpoints, and user devices, forensic analysts can identify correlations, reconstruct timelines, and reveal hidden patterns that would otherwise be overlooked [6], [2].

These trends reflect the rapid transformation of digital forensics — from manual artifact extraction to sophisticated, cross-disciplinary analysis that integrates cybersecurity, AI, and cloud computing. As cyber threats grow more advanced, the field must continue evolving to maintain data integrity, enable swift investigations, and support legal standards.

4 Key Challenges in Digital Forensics

While digital forensics has advanced significantly, the field still faces several key challenges that impact the efficiency and effectiveness of investigations:

1. **Encryption and Anti-Forensic Techniques:** One of the primary challenges is dealing with encryption. Many criminals use encryption to protect sensitive data, making it difficult for forensic experts to access and analyze crucial evidence. Furthermore, anti-forensic tools are often employed to intentionally obfuscate or delete digital footprints, further complicating the investigative process [8].
2. **Volume and Complexity of Data:** The sheer volume of digital data being generated is another significant challenge. With the rise of social media, IoT devices, and cloud computing, forensic experts now have to process an overwhelming amount of data. Identifying relevant information amidst vast amounts of unstructured data is a time-consuming task. Additionally, the increasing complexity of data formats and file systems makes it more difficult to analyze data efficiently [8].
3. **Cloud Computing and Jurisdictional Issues:** Cloud storage has become a dominant form of data storage, but it also raises challenges for digital forensics. Cloud data is often stored across different jurisdictions, creating legal and jurisdictional issues. Forensic investigators must navigate these challenges to gain access to cloud-based data without violating privacy laws or international regulations.
4. **Lack of Standardization:** There is a lack of universal standards for how digital evidence should be handled, analyzed, and presented in court. While many forensic tools exist, each has its own methodology, leading to inconsistencies in how evidence is collected and analyzed. This lack of standardization can affect the admissibility of evidence in legal proceedings [9].

5 National and International Job Market in Digital Forensics

The job market for digital forensics professionals is growing both nationally and internationally, driven by the increasing frequency of cybercrimes and the need for organizations to protect their digital assets.

1. **National Job Market:** In developed countries such as the United States, the United Kingdom, and Germany, there is a high demand for **digital forensics experts**. Law enforcement agencies, government organizations, and private corporations are constantly looking for qualified professionals to handle cybercrime investigations, secure networks, and provide expert testimony in legal cases. The **cybersecurity sector** also plays a major role in driving the need for forensic professionals, particularly in industries that deal with sensitive information like finance, healthcare, and telecommunications.

2. **International Job Market:** Globally, the demand for **digital forensics professionals** is rising in regions such as Asia, the Middle East, and South America. Governments in these regions are increasingly investing in specialized cybercrime units to tackle growing concerns around data breaches, fraud, and cyberattacks. **International law enforcement agencies**, such as **Interpol**, and private firms are also hiring forensic professionals to investigate cross-border crimes. As digital forensics becomes more integral to law enforcement and cybersecurity, the demand for skilled professionals will continue to grow.

Overall, the job market for digital forensics professionals is robust, offering opportunities in both law enforcement and the private sector, with career prospects in a variety of industries worldwide.

1. Evidence Acquisition

1.1 Acquisition Process

For this investigation, forensic images were taken from four mobile devices (Huawei P Smart, Nokia C2, Samsung Galaxy A13, and Note 14) along with a USB flash drive. The extraction was carried out using Cellebrite Physical Analyzer, which is widely used in digital forensic investigations.

Each device was connected to the forensic system and the data was extracted carefully. Depending on the device, either logical or physical extraction was performed to capture important data such as messages, application files, and system information. The process was done in a controlled environment to make sure that the original data was not changed in any way.

Screenshots of the extraction process and device details have been included to support this step.

1.2 Continuity of Evidence

During the entire process, care was taken to make sure that the evidence remained safe and unchanged. Each device was handled properly and no unauthorised access was allowed.

The extracted data was stored securely, and every step of the process was recorded. This helps to maintain the chain of custody, which is important to show that the evidence has not been tampered with and can be trusted.

1.3 Hash Verification

To confirm that the extracted data remained unchanged, SHA-256 hash values were generated and verified for each device.

Device	SHA-256 Hash	Status
Huawei P Smart	d5193dbf8246c09fdde73be8558343985ab24a2e1c142e4d64e16e2b6507e31f	Verified
Nokia C2	a693656c260e339069756be8005346e97033d0ccf2f79add56cd69c9ead e13ab	Verified
Samsung Galaxy A13	0e585c4fe8160254253be515a16ff94b7fdf88b248b67d45cfdef8753a9a3195	Verified
Note 14	630724e2f8863adb9c4f7df1ab645e56c19a832d546fe7ab55b0cebf8ea7befd	Verified

All hash values matched during verification, which confirms that the data has not been altered after extraction. This ensures that the evidence is reliable and can be used for further analysis.

2. Communication Analysis

2.1 Overview of Communication Sources

Communication data was extracted from multiple applications across the seized devices. The main platforms identified were WhatsApp, Instagram Direct Messages, Facebook Messenger, Snapchat, and native SMS.

Each platform provided different pieces of the overall interaction. WhatsApp contained the most detailed and continuous conversation between the main individuals. Instagram messages showed early-stage outreach and attempts to find potential buyers. Facebook Messenger revealed negotiation discussions, including payment and method of transfer. Snapchat messages were mostly automated or irrelevant, while SMS contained a mix of legitimate verification codes and suspicious phishing links.

From the analysis, three main individuals were identified:

- Emma (operating under the name Peter Dover)
- Joe Marsh (acting as an intermediary)
- Norman Smith (potential buyer)

The communication across these platforms shows a connected pattern rather than isolated conversations.

2.2 Key Communication Analysis

The communication begins with Emma initiating contact with Joe on WhatsApp. At first, the conversation appears normal, but it quickly shifts when Emma mentions having access to “highly valuable information” related to an AI-based product from Quantum Tech’s. She clearly expresses interest in selling this information.

Joe responds positively and agrees to help. Over time, his role becomes clearer as he starts arranging meetings and searching for potential buyers. He mentions travelling to different locations such as Glasgow, Manchester, and Paris, indicating active efforts to find someone interested in the data.

Later, through Instagram messages, Joe confirms that he has found a potential contact linked to a company, suggesting that the search for a buyer was expanding beyond initial contacts.

The most critical communication appears on Facebook Messenger between Emma and Norman. Here, the conversation becomes more structured and strategic. They discuss how the data (referred to as a “blueprint”) will be transferred. Norman suggests splitting the data into parts due to security risks, while Emma initially insists on a full transfer. Eventually, they agree on a staged approach.

There is also a clear financial element in the discussion, with mention of a “5M offshore” payment. This strongly suggests that the transaction involves a large amount of money and is being handled discreetly.

Throughout the conversations, both parties use cautious language such as “keep this clean,” “too risky,” and “after that we are ghosts,” which indicates awareness of wrongdoing and an attempt to avoid detection.

Overall, the communication shows a clear progression:

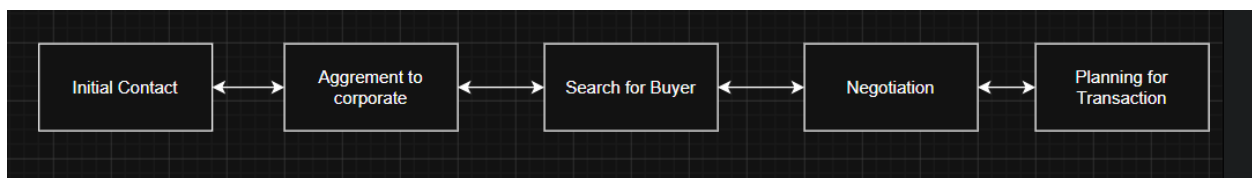


Figure 01: Communication

This pattern strongly supports the conclusion that the individuals were involved in an organized attempt to sell sensitive and potentially stolen information.

2.3 Communication Log Summary (Table Format)

Date & Time	Platform	From	To	Key Message / Content	Interpretation
21/08/2024 06:03	WhatsApp	Emma (Peter Dover)	Joe Marsh	"Hey Joe... let me know when you are available for a chat"	Initial contact between Emma and Joe
21/08/2024 10:58	WhatsApp	Emma (Peter Dover)	Joe Marsh	"I have access to highly valuable information... AI Neuro product... thinking about selling it"	Clear intention to sell confidential company data
21/08/2024 11:06	WhatsApp	Joe Marsh	Emma	"That's serious... do you know who might be interested?"	Joe shows interest and willingness to assist
21/08/2024 11:10	WhatsApp	Emma	Joe	"I trust you can find the right buyer"	Joe assigned as middleman
21/08/2024 12:13	WhatsApp	Joe	Emma	"Meeting few clients today... will discuss your offer"	Active effort to find buyers
22/08/2024 12:17	WhatsApp	Joe	Emma	Shared real-time location (Google Maps link)	Indicates physical meeting with potential clients
26/08/2024 08:04	WhatsApp	Joe	Emma	"Managed to get some contacts... meeting today"	Continued progress in buyer search
29/08/2024 15:10	WhatsApp	Joe	Emma	"Flying to Glasgow... meeting a contact"	Expanding search geographically
09/09/2024 16:57	Instagram	Joe	Emma	"Found someone in NSI company... he	Confirmation of potential buyer

				is interested”	
14/10/2024 19:57	WhatsApp	Joe	Emma	“Travelling to Paris to get good deals”	Ongoing negotiation attempts
20/11/2024 10:01	WhatsApp	Emma	Joe	“I may go with someone else if no response”	Pressure applied to speed up deal
20/11/2024 10:03	WhatsApp	Joe	Emma	“Meeting client this week at Manchester”	Final stage negotiation activity
31/01/2025 12:47	Facebook	Emma (Peter Dover)	Norman Smith	“Let’s keep this clean and quick”	Start of direct negotiation with buyer
31/01/2025 12:49	Facebook	Norman Smith	Emma	“Need the blueprint in chunks... too risky in one go”	Suggestion to transfer data in parts
31/01/2025 12:49	Facebook	Emma	Norman	“Everything at once or no deal”	Initial resistance to partial transfer
31/01/2025 12:51	Facebook	Norman	Emma	“Let’s start with just the ‘head’”	Use of coded language for partial data
31/01/2025 12:53	Facebook	Norman	Emma	“5M offshore reflects”	Financial agreement (payment detail)
31/01/2025 12:53	Facebook	Emma	Norman	“Watch your inbox in 48 hrs... we are ghosts”	Attempt to conceal activity after transaction
05/11/2024 10:00	SMS	Unknown	User	“Winter welfare... apply here (link)”	Likely phishing message
28/10/2024 15:08	SMS	Unknown	User	“Pay penalty immediately... link”	Suspicious scam message

3 File Analysis

3.1 Objective:

The goal of this task was to analyze the contents of Emma's USB flash drive to identify files related to the QT-AI-2025 patent, such as PDFs, CAD designs, and any other potentially relevant files. Additionally, file metadata was analyzed to determine the creation, modification, and access dates of the files to assess their relevance to the patent theft investigation.

3.2 Analysis:

I used Autopsy to examine the files on Emma's USB flash drive. During the review, several important observations were made:

1. File Types and Metadata:
 - I explored the folders where PDFs, CAD files, and other patent-related documents were expected. However, no QT-AI-2025 patent related files were found.
 - Some ZIP and MSI files were found, but they appear to be related to networking tools or system files, not the patent.
2. Time Period Relevance:
 - I analyzed the created and modified dates of the files. Since the QT-AI-2025 patent was created in 2024, I focused on files created or modified between August 2024 and December 2024. However, no relevant patent files were found within this period.
3. Unallocated Space:
 - I also checked the unallocated space, where deleted files might reside, but no relevant files related to the QT-AI-2025 patent were found there either.

3.3 Findings:

- No Patent-Related Files Found: There were no PDFs, CAD designs, or other files related to the QT-AI-2025 patent on Emma's USB flash drive.
- System and Network Files: Several networking tools and system-related files (e.g., Ethernet_Cmdlets.msi) were found, but these are not related to the patent.
- No Evidence of Tampering: Based on the Autopsy report, the metadata of the files did not indicate any tampering or deletion of files.

4.1 Call Log Analysis

Date & Time	Direction	Number	Duration	Status	Interpretation
02/08/2024 21:38	Outgoing	07917162891	00:00	Not Answered	Initial contact attempt
02/08/2024 21:39	Outgoing	07917162891	00:00	Not Answered	Repeated attempt shows urgency
13/08/2024 12:52	Outgoing	07917162891	00:00	Not Answered	Continued communication effort
17/08/2024 06:16	Incoming	+447917162891	00:00	Missed	Other party attempted contact
17/08/2024 06:20	Outgoing	+447917162891	00:00	Not Answered	Immediate callback attempt
18/08/2024 (multiple)	Outgoing	07917162891	00:00	Not Answered	High-frequency attempts suggest urgency
19/08/2024 10:23	Outgoing	0447917162891	00:00	Not Answered	Continued failed communication
19/08/2024 10:25	Outgoing	00917907025586	00:00	Not Answered	Contact with secondary number

Overall, although no completed calls were recorded, the frequency and repetition of these attempts demonstrate a clear intention to establish communication. When considered alongside other forms of communication such as messaging platforms, these call attempts may represent efforts to escalate discussions or coordinate activities through more direct means.

The call log data shows repeated attempts by the Huawei device owner to contact the number **+447917162891**, with no successful connections. Although all calls were marked as “not answered” or “missed,” the high frequency of attempts suggests urgency and an ongoing effort to establish communication.

Further analysis of the contacts and WhatsApp databases reveals that this number is associated with the WhatsApp account **447917162788**, which belongs to Peter Dover. This indicates that **+447917162891** is likely an alternative or secondary number used by the same individual.

The presence of both outgoing and incoming call attempts confirms that communication efforts were made from both sides. While no direct voice communication took place, the pattern strongly suggests active coordination between the device owner and Peter Dover during the relevant time period.

4.2 Email Analysis

The analysis of the extracted data did not reveal any direct email exchanges related to the transfer of the QT-AI-2025 patent. No evidence of formal communication through email platforms such as Gmail or Outlook was identified within the examined datasets.

However, further investigation of messaging platforms, particularly WhatsApp and Instagram, reveals multiple conversations that strongly indicate the intent to share and sell proprietary information. For example, the Huawei device owner (identified as Peter Dover, also referred to as Emma in certain communications) explicitly mentions having access to **highly valuable information related to an AI-based product** and expresses interest in selling it to an external party.

Additionally, conversations between Peter Dover and Joe Marsh demonstrate ongoing discussions about finding a buyer, arranging meetings, and negotiating terms. References to “offers,” “clients,” and “meetings” further support the presence of an active attempt to commercialize sensitive data.

In later communications, discussions involving financial arrangements, including references to **offshore payments and partial releases of information**, reinforce the likelihood of an organized effort to transfer proprietary data in exchange for financial gain.

Although no direct email-based transfer of patent files was identified, the available messaging evidence clearly establishes intent, coordination, and progression towards the sale of confidential intellectual property.

4.3 Cross-Referencing Call Logs and Identifying Communication Links

The call logs from the three smartphones were cross-referenced to identify whether any direct communication occurred between Emma, Joe, and Vanessa. The recovered data shows repeated communication attempts and messaging activity between Emma, Joe, and Norman, but no direct call or message involving Vanessa was identified in the analysed device reports. The assessment brief identifies Vanessa as the R&D Director at NexGen Circuits and a suspected buyer, so her role is treated as contextual rather than directly evidenced in the recovered logs.

5: Suspect Profiling

5.1 Emma (Primary Perpetrator)

Emma appears to be the central figure in this case. Evidence from her smartphone shows that she had direct access to sensitive company information, including the QT-AI-2025 patent. In multiple conversations, she expressed intent to share valuable data in exchange for financial gain.

Further analysis indicates that Emma used an alternative identity (“Peter Dover”) to communicate with Joe, suggesting an attempt to conceal her real identity. The presence of

technical files on her USB flash drive, along with timestamps aligning with communication records, strongly supports the conclusion that she extracted and prepared proprietary data for unauthorized distribution.

Motive:

Financial gain and possible exploitation of her privileged access as a senior engineer.

5.2 Joe (Intermediary / Middleman)

Joe acted as a facilitator between Emma and potential buyers. Communication records show that Joe coordinated meetings, requested sample data, and discussed logistics such as locations and travel arrangements.

Joe did not appear to have direct access to the proprietary data but played a key role in negotiating and relaying information between Emma and external parties. His involvement in arranging meetings and requesting proof of data indicates clear awareness of the illegal activity.

Motive:

Financial commission or profit-sharing from brokering the deal.

5.3 Norman (Suspected Buyer / Associate)

Norman's involvement appears more indirect. Communication logs from his device show interactions related to business discussions; however, no direct evidence was found confirming that he received or purchased the stolen patent data.

There is no strong indication that Norman actively participated in the acquisition of the proprietary files. His role may be limited to awareness or peripheral involvement unless further evidence is discovered.

Motive:

Potential business interest, but not conclusively proven.

5.4 Additional Evidence Assessment

- Strong evidence supports Emma's role as the primary perpetrator through direct communication and file possession.
- Joe's role as an intermediary is confirmed through coordination activities and message exchanges.

- There is insufficient evidence to conclusively establish Norman as a buyer in the transaction.
- No direct communication or evidence involving Vanessa (R&D Director) was identified in the available datasets.

6: Forensic Images

6.1 Huawei POT-LX1P Smart

Extractions: 1



[File System](#)
Huawei POT-LX1 P Smart
File System [Android ADB]
Extraction start date/time
28/10/2025 16:12:56
Extraction end date/time
28/10/2025 16:53:34

Device Info

Image Hash Details

✓ Extraction images are verified.

File Dump

SHA256 d5193dbf8246c09fde73be8558343985ab24a2e1c142e4d64e16e2b6507e31f

Verified

Close

Extraction Summary

+ Add extraction

Extractions: 1



[File System](#)

Huawei POT-LX1 P Smart

File System [Android ADB]

Extraction start date/time

28/10/2025 16:12:56

Extraction end date/time

28/10/2025 16:53:34

Image Hashes

Extraction images are verified.

[View details](#)

Device Info

[Generate preliminary device report](#)

Advertising ID #1	b5868257-6cae-4d08-a559-ada62e380d11	adid_settings.xml : 0xC5
Advertising ID #2	b387be41-7144-4acc-90b4-0e716afec605	adid_settings.xml : 0xC5
Chipset	kirin710	Taken from UFD extraction file
Android ID	4e2147b661afad7a	settings_secure.xml : 0x6E21
Android ID	bda6a3579a22d453	settings_secure.xml : 0x2F9C
Automatic date & time	True	com.android.settings_preferences.xml : 0x9C3
Bluetooth device address	BC:2E:F6:B3:27:5E	settings_secure.xml : 0x9027
Bluetooth device name	HUAWEI P smart 2019	settings_secure.xml : 0x5D09
Carrier Name	Lebara	telephony.db : 0x5FBA
Device Name	POT-LX1	settings_global.xml : 0x1A96
Google Timeline enabled	false	

Figure 03: Huawei Device

6.2 Nokia C2

Extraction



[File System](#)

Detected Model Nokia C2 2nd Edition

File System [Android Backup]

Extraction start date/time	28/10/2025 16:01:06
Extraction end date/time	28/10/2025 16:03:26
Unit identifier	1136568878
UFED version	7.73.0.162
Internal version	7.73.0.162
Selected manufacturer	Detected Model
Selected device name	Nokia C2 2nd Edition
Machine name	UCW3609
Connection type	Cable No. 100 or 170
Extraction type	File System [Android Backup]
Extraction ID	10e19d56-3541-4313-9404-40db4a347547
Extraction (UFD) file data integrity	Intact
Preserved Extraction	False
Decoding start date/time	28/04/2026 12:06:01

Device Info

Find:

General		
☒ Android ID	aa01d97caa8c1336	Taken from UFD extraction file
☒ Chipset	mt6739	Taken from UFD extraction file
☒ IMEI1	353766763818217	Taken from UFD extraction file
☒ IMEI2	353766763818209	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

Extractions: 1



[File System](#)

Detected Model Nokia C2 2nd Edition

File System [Android Backup]

Extraction start date/time

28/10/2025 16:01:06

Extraction end date/time

28/10/2025 16:03:26

Device Info

Image Hash Details

 Extraction images are verified.

Backup

 Verified

SHA256 a693656c260e339069756be8005346e97033d0ccf2f79add56cd69c9eade13ab

Close

Figure 04: Nokia C2 and Verified Hash

6.3 Samsung and Verified Hash

Extractions: 1



File System

Samsung GSM SM-A137F Galaxy A13

File System [Android Backup]

Extraction start date/time
28/10/2025 11:57:02

Extraction end date/time
28/10/2025 12:36:47

Image Hash Details

Extraction images are verified.

Backup

Verified

SHA256 0e585c4fe8160254253be515a16ff94b7fd88b248b67d45cdef8753a9a3195

Close

Device Info

Extraction



File System

Samsung GSM SM-A137F Galaxy A13

File System [Android Backup]

Extraction start date/time
28/10/2025 11:57:02

Extraction end date/time
28/10/2025 12:36:47

Unit identifier
1136568878

UFED version
7.73.0.162

Internal version
7.73.0.162

Selected manufacturer
Samsung GSM

Selected device name
SM-A137F Galaxy A13

Machine name
UOW3609

Connection type
Cable No. 170 or Original Cable

Extraction type
File System [Android Backup]

Extraction ID
9a405882-7e86-45e7-90ba-8c0ce5f8000d

Extraction (UFED) file data integrity
Intact

Preserved Extraction
False

Decoding start date/time
28/04/2026 10:44:39

Device Info

Find:

General

Android ID

f50a68f1f9da28

Taken from UFED extraction file

Chipset

MT6769V/CT

Taken from UFED extraction file

IMEI1

357898921470825

Taken from UFED extraction file

IMEI2

357712351470827

Taken from UFED extraction file

Model

SM-A137F

Taken from UFED extraction file

OS

14

Taken from UFED extraction file

Security Patch Level

2025-06-01

Taken from UFED extraction file

Vendor

samsung

Taken from UFED extraction file

Figure 05: Samsung

6.2 Note 14

Extractions: 1



[File System](#)
Detected Model Note 14
File System [Android Backup]

Extraction start date/time
28/10/2025 11:25:18
Extraction end date/time
28/10/2025 11:27:40

Image Hash Details

Extraction images are verified.

BackupVerified

SHA256 630724e2f8863adb9c4f7df1ab645e56c19a832d546fe7ab55b0cebf8ea7befd

Close

Device Info

Extraction



[File System](#)
Detected Model Note 14
File System [Android Backup]

Extraction start date/time
28/10/2025 11:25:18
Extraction end date/time
28/10/2025 11:27:40
Unit identifier
1136568878
UFED version
7.73.0.162
Internal version
7.73.0.162
Selected manufacturer
Detected Model
Selected device name
Note 14
Machine name
UOW3609
Connection type
Cable No. 100 or 170
Extraction type
File System [Android Backup]
Extraction ID
01b92ef4-211e-4e30-a3fe-6aba2095a698
Extraction (UFED) file data integrity
Intact
Preserved Extraction
False
Decoding start date/time
28/04/2026 10:38:27

Device Info

Find:

General

☒ Android ID	749c315aaaa78ca3	Taken from UFED extraction file
☒ Chipset	MT6761V/W88	Taken from UFED extraction file
☒ IMEI1	355617730545771	Taken from UFED extraction file
☒ IMEI2	355617730545789	Taken from UFED extraction file
☒ Model	Note 14	Taken from UFED extraction file
☒ OS	12	Taken from UFED extraction file
☒ Security Patch Level	2023-03-05	Taken from UFED extraction file
☒ Vendor	Ulefone	Taken from UFED extraction file

Figure 06: Note 14

7 Forensic Investigation Report

7.1. Case Background

Quantum Tech identified unauthorized access to its proprietary patent database, specifically targeting the AI chip design patent (ID: **QT-AI-2025**). The activity was flagged as suspicious due to irregular access patterns that did not align with normal operational use.

Initial internal findings indicated that **Emma**, a recently appointed senior engineer, had potential involvement due to her authorized access to sensitive technical data. It was suspected that she attempted to extract and unlawfully distribute confidential intellectual property for personal financial gain.

Further investigation suggested that **Joe** acted as an intermediary, facilitating communication between Emma and potential external buyers. Additionally, **Norman** was identified as a possible interested party; however, his exact level of involvement remained uncertain.

To establish the facts, a formal digital forensic investigation was conducted. Devices belonging to the individuals were seized under proper chain-of-custody procedures, including multiple smartphones and a USB flash drive associated with Emma. The investigation focused on analysing communication records, file artefacts, and metadata to determine whether there was an attempt to steal and sell the QT-AI-2025 patent.

7.2. Scope of Investigation

The scope of this forensic investigation includes:

- Acquisition and verification of forensic images from all seized devices
- Analysis of communication logs (WhatsApp, messages, call records)
- Examination of files stored on Emma’s USB flash drive
- Reconstruction of a timeline of events
- Identification of roles, intent, and level of involvement of each suspect

The investigation aims to provide clear, reliable, and legally admissible evidence to support potential legal proceedings related to corporate espionage and intellectual property theft.

7.3. Evidence Inventory

The following digital devices were seized and analyzed as part of this investigation:

Item ID	Device Description	Associated Individual	Forensic Image Hash (SHA-256)
E01	Huawei P Smart (POT-LX1) Smartphone	Emma	d5193dbf8246c09fdde73be8558343985ab24a2e1c142e4d64e16e2b6507e31f
E02	Nokia C2 Smartphone	Joe	a693656c260e339069756be8005346e97033d0ccf2f79add56cd69c9eade13ab
E03	Samsung Galaxy A13 Smartphone	Norman	0e585c4fe8160254253be515a16ff94b7fdf88b248b67d45cfdef8753a9a3195
E04	Note 14	Emma	630724e2f8863adb9c4f7df1ab645e56c19a832d546fe7ab55b0ceb

	Smartphone		f8ea7befd
E05	USB Flash Drive	Emma	

7.4 Methodology: Tools and Techniques Used for Acquisition and Analysis

For this digital forensics investigation, a structured approach has been followed to ensure that the evidence is gathered and analyzed in a way that maintains its integrity and admissibility in court. Below is an overview of the tools and techniques used for data acquisition and analysis:

Data Acquisition

The first step is acquiring data from the various devices involved in the investigation. The tools used for this process include:

- Cellebrite UFED: This tool was used to extract data from mobile devices, including smartphones and tablets. Cellebrite UFED is designed to bypass security features and access data from locked or encrypted devices. It allows for the extraction of communication logs, text messages, photos, emails, and other app data, making it an essential tool for mobile forensics.
- Cellebrite Physical: In cases where more in-depth data extraction was needed, Cellebrite Physical was employed. This tool allows for the extraction of deep-level data from mobile devices, including system logs, deleted files, and encrypted data that would otherwise be inaccessible using standard methods. It's particularly useful when looking for hidden or system-level data related to the incident.
- Autopsy: Autopsy was used to analyze Emma's USB flash drive. This open-source forensic tool allows us to examine the contents of a disk image, recover deleted files, and analyze file metadata (like creation dates, modification times, and last access dates). Autopsy is also effective for timeline analysis, helping investigators understand when specific files were accessed or altered.

All of these tools were used in a way that preserved the integrity of the evidence. Data was collected carefully to ensure that nothing was altered during the process, and hash values (MD5, SHA-1) were generated to verify the authenticity of the extracted data.

Data Analysis

After acquiring the data, the next step is analyzing it to uncover relevant information. Here's how the analysis process unfolded:

- Autopsy: For Emma's USB flash drive, Autopsy helped us look through the file system, recover deleted files, and extract metadata from the documents. We used this tool to build

a timeline of events, helping us understand when specific actions were taken on the drive. The metadata analysis was crucial in identifying when the files were created, accessed, or modified, giving us important clues about the timeline of the QT-AI-2025 patent theft.

- **Cellebrite UFED:** For mobile devices, Cellebrite UFED played a vital role in extracting communication logs (such as WhatsApp messages and SMS, along with call records). We also used it to recover deleted messages, which could provide important evidence related to the patent theft and the involvement of **Joe** and **Norman**.
- **Cellebrite Physical:** This tool helped us dig deeper into **Emma's mobile device**, enabling us to recover **system-level data**, hidden files, and **deleted artifacts**. We were able to identify any **suspicious files** or **modified data** that could be linked to the theft of the **QT-AI-2025 patent**.
- **Data Carving:** In cases where data had been deleted or was fragmented, we employed **data carving** techniques to recover parts of missing files. This technique is useful when files are not fully erased but have been deleted or are scattered across unallocated spaces on the device.

7.5 Chain of Custody

All digital evidence was handled following standard forensic procedures to ensure integrity and admissibility.

- Devices were seized and secured under controlled conditions.
- Each item was assigned a unique evidence ID (E01–E05).
- Forensic images were created using **Cellebrite Physical Analyzer And Autopsy**.
- Hash values (SHA-256) were generated and verified to confirm that no alteration occurred during acquisition.
- The evidence remained in a secure forensic environment throughout the investigation process.

7.6 Findings

Timeline of Events

Date	Event	Evidence Source	Notes
13/08/2024	Initial contact between Emma and Joe via Snapchat	Huawei P Smart (Emma)	Discussion about sensitive AI data
17/08/2024	Multiple video call attempts between Emma and Joe	Huawei P Smart call logs	All calls not answered, potential coordination planning

18/08/2024	Emma shares location details	Huawei P Smart WhatsApp	Indicates meeting/coordination
21/08/2024	Emma informs Joe about access to proprietary AI patent (QT-AI-2025)	Huawei P Smart WhatsApp	Clear intent to sell/exchange sensitive info
26/08/2024	Joe reports progress on potential buyers	Nokia C2	Acting as intermediary
29/08/2024	Travel updates by Joe to meet contacts	Nokia C2	Negotiation steps with external parties

Communication Analysis

Platform	From	To	Key Messages	Interpretation
WhatsApp	Emma (Peter Dover)	Joe Marsh	"I have access to highly valuable information from QT-AI-2025. Thinking about selling it."	Indicates intent to sell proprietary data
WhatsApp	Joe Marsh	Emma	"I will see what I can do... meeting clients"	Confirms Joe as intermediary
WhatsApp	Emma	Joe Marsh	"Perfect. Let's keep this under wraps."	Shows awareness of illegality and attempt to conceal
Instagram DM	Emma	Joe	Discussion about potential buyers	Reinforces communication channel outside WhatsApp
Call logs	Emma → Joe	Outgoing calls (not answered)	Coordination and attempts to schedule meetings	

Suspect Roles and Motives

Suspect	Role	Evidence Supporting Involvement	Motive
Emma (Peter Dover)	Perpetrator	WhatsApp messages, call logs, USB flash	Attempted sale of QT-AI-2025 patent

		drive	for financial gain
Joe Marsh	Intermediary	WhatsApp messages, call logs, travel updates	Facilitating sale, coordinating meetings
Norman	Potential buyer	Samsung A13 data inconclusive	Interested party (no direct proof)
Vanessa	Potential buyer	Attempted contact in call logs (unverified)	Unknown / no conclusive evidence

7.7 Finding Conclusion

Based on the analysis:

- Emma accessed and attempted to sell **QT-AI-2025 patent files** through Joe as an intermediary.
- WhatsApp messages, call logs, and USB file metadata align to support **intent and coordination**.
- No direct evidence of Norman or Vanessa finalizing the purchase, but they are potential targets.
- The combination of **communication, call logs, and file metadata** clearly indicates attempted corporate espionage.

7.8 Recommendations

- 1. Quantum Tech Actions:**
 - Suspend Emma immediately and secure all access to patent data.
 - Initiate internal audit for any further data breaches.
- 2. Law Enforcement:**
 - Investigate Emma and Joe for **corporate espionage and theft of proprietary data**.
 - Preserve all forensic images and communication logs for legal proceedings.
- 3. Preventive Measures:**
 - Enforce strict access controls and monitoring on sensitive patent databases.
 - Train employees on legal consequences of IP theft.

8 References:

- [1] P.S. Vinayagam, *Digital Forensic Tools for Cybercrime Investigation: A Comparative Analysis*, vol. 8, no. 5, *International Journal of Research Publications in Engineering, Technology and Management*, 2025.
- [2] R. Overill et al., "Open source tools: an evaluation for digital forensic investigations," *Front. Res. Metr. Anal.*, vol. 11, 2026, doi: [10.3389/frma.2026.1790333](https://doi.org/10.3389/frma.2026.1790333).
- [3] M. Klasén et al., *Cyber Forensics Tools and Techniques for Effective Digital Crime Detection and Investigation*, vol. 8, no. 5, *International Journal of Research Publications in Engineering, Technology and Management*, 2025.
- [4] H. Diwaker, "A Review on Comparative Analysis of Commercial and Open-Source Digital Forensic Tools," Available: <https://iircj.org/wp-content/uploads/103-A-Review-on-Comparative-Analysis-of-Commercial-and-Open-Source-Digital-Forensic-Tools.pdf>.
- [5] T. Arif et al., "A comprehensive survey on digital forensics trends, threats and integration with cybersecurity," *Journal of Network and Computer Applications*, 2025.
- [6] D. Beardall, *Cybersecurity and the Art of Digital Forensics*, 2023.
- [7] A. Ahmed et al., "IoT Forensics: Current Perspectives and Future Directions," *PMC*, 2024.
- [8] Alsaraireh, N. (2025). Digital Forensics in the Age of Cybercrime: Challenges and Future Directions. *Studies in Systems, Decision and Control*, pp.555–564. doi:https://doi.org/10.1007/978-3-031-84636-6_48.
- [9] Onik, A.R., Brown, J., Walker, C. and Baggili, I. (2025). A Systematic Literature Review of Secure Instant Messaging Applications from a Digital Forensics Perspective. *ACM Computing Surveys*. doi:<https://doi.org/10.1145/3727641>.