



Student name:	Riddhi Mendpara	Student ID number:	2518862
Module Code:	ACCA7031		
Module:	Digital Forensics Analysis		
Assignment Title:	Research, Analyse and Investigate Cybersecurity incidents and perform digital forensic assessment		
Submission deadline:	7 th July 2026		

Abstract

Digital forensics plays a vital role in investigating cybercrime and preserving digital evidence for legal proceedings. The current status of digital forensics, its connection to cybersecurity, new developments, major obstacles, and job prospects in the area are all examined in this research. Additionally, it offers a useful analysis of the Quantum Tech corporate espionage case concerning the AI chip design patent theft (QT-AI-2025). To determine the suspects' activity, the investigation examined files, digital artefacts, and communication records using forensic tools like FTK Imager and Cellebrite UFED. The results highlight the value of digital forensics in assisting with cybersecurity investigations and safeguarding confidential company data.

Table of Contents

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

TASK - 1

1. Introduction

Digital forensics has become an essential field central to current criminal investigations and corporate security. As society becomes more dependent on digital technology, the amount and complexity of digital evidence have increased significantly. This field deals with the systematic Collection, Preservation, Analysis and Presentation of Digital Evidence in a manner that is acceptable in court [1]. The current state of digital forensic, its relationship to cybersecurity, emerging trends, major challenges and the employment market for specialists both domestically and abroad are all examined in this research.

2. Current State of the Field and Key Tools

FTK Imager:

One of the most used forensic imaging tools in digital investigations is FTK Imager, which was created by Access Data (now Exterro). Without changing any original data, it is mostly used to produce forensic bit-for-bit photographs of storage media such as memory cards, USB flash drives, and hard drives [2]. FTK Imager can recover deleted files, preview file contents, and generate MD5 and SHA-1 hash values to confirm the integrity of obtained evidence. It is compatible with all major operating systems and file systems [3]. It is a crucial tool for preserving the admissibility of evidence in court since it can replicate storage medium exactly while maintaining their original condition [1].

FTK (Forensic Toolkit) Analyzer:

Exterro has created FTK (Forensic Toolkit), a complete digital forensics analysis tool that is frequently utilised in corporate and law enforcement investigations. Unlike FTK Imager which focuses exclusively on acquisition, FTK Analyser includes a full range of analysis capabilities including file system investigation, keyword searching, email analysis, metadata extraction and registry analysis [2]. FTK is particularly successful in examining encrypted or password-protected files, recovering deleted content and building a clear timeline of file activity. Its integrated case management system helps investigators to efficiently process and organise enormous volumes of digital evidence, making it one of the leading tools in the field [1].

Cellebrite UFED & Physical Analyzer:

Law enforcement agencies, corporate investigators, and governmental institutions all across the world have embraced Cellebrite, the industry-leading mobile device forensics solution [2]. There are two main parts of the Cellebrite toolkit:

Cellebrite UFED (Universal Forensic Extraction Device) is utilised for the acquisition phase. It does full physical, logical and file system extractions from a wide range of smartphones, tablets and GPS devices, including both Android and iOS platforms [1]. UFED is capable of breaking some device locks and extracting data from encrypted devices, making it important in modern investigations where suspects regularly adopt security measures to safeguard their devices. Like FTK Imager, UFED generates MD5 and SHA-1 hash values upon acquisition to confirm evidence integrity.

The analysis stage makes use of the Cellebrite Physical Analyser. Physical Analyser processes and displays the retrieved data in an organised, investigator-friendly style after UFED has obtained the device picture [2]. Call logs, SMS and MMS messages, WhatsApp, Instagram direct messages, emails, media files, GPS location data, and application data may all be analysed with it. Additionally, Physical Analyser offers timeline visualisation tools that enable investigators to piece together a chronological sequence of events across many devices, which is crucial in situations where there are several suspects [1].

3. Intersection of Digital Forensics and Cybersecurity

Cybersecurity and digital forensics are closely related fields that assist businesses in safeguarding and examining digital systems. While digital forensics focuses on gathering, storing, and analysing digital evidence following a security incident, cybersecurity primarily focuses on avoiding, detecting, and responding to cyber threats such as malware assaults, phishing, and data breaches. Digital forensics is essential to cybersecurity because increasingly complex cyberattacks require complex methods for gathering and analysing evidence [4]. Additionally, the demand for forensic investigations and qualified experts who can handle digital evidence has greatly expanded due to the quick development of digital devices and internet services.

During incident response operations, the connection between cybersecurity and digital forensics becomes more crucial. When a cyberattack happens, forensic investigators examine system logs, emails, network traffic, and storage devices to identify the attacker's techniques and pinpoint the incident's origin, while cybersecurity teams struggle to contain the danger and recover impacted systems. Although security and forensics are considered independent disciplines, both professions have common aims and complement each other in enhancing organisational resilience and helping legal investigations. In order to enhance incident response, protect digital evidence and reinforce upcoming security measures, businesses are increasingly incorporating digital forensics skills into their cybersecurity strategy.

4. Emerging Trends in Digital Forensics

The application of artificial intelligence (AI) and machine learning (ML) is one of the most important new developments in digital forensics. By automatically recognising suspicious patterns, classifying data, and identifying abnormalities, these technologies help investigators in processing massive amounts of digital evidence more effectively. AI-powered forensic technologies are becoming more and more useful in contemporary cybercrime investigations since they can speed up investigations and increase the precision of evidence processing [4].

The development of cloud and Internet of Things (IoT) forensics is another significant trend. As organisations and individuals increasingly depend on cloud services and smart devices, investigators must deal with evidence kept across many locations and platforms. Smartwatches, smart home systems, and linked cars are examples of IoT devices that produce useful digital evidence, but their various architectures and data formats pose serious difficulties for forensic investigations.

Furthermore, blockchain forensics and forensic automation are attracting great attention. The increasing use of cryptocurrencies has generated a demand for blockchain research techniques to investigate financial crimes, fraud, and money laundering. At the same time, automated forensic tools

and Digital Forensics-as-a-Service solutions are being created to improve evidence collecting, processing, and reporting processes. These new tools are revolutionising digital forensics and making it possible for investigators to better address increasingly complex cyberthreats [4].

5. Key Challenges

Digital forensics has various obstacles due to the rapid evolution of technology and the increasing complexity of cybercrime. Since many devices and applications use robust security measures that make it difficult for investigators to access evidence, encryption is one of the main issues. Another key difficulty is the large number of digital data generated every day, which increases the time and resources required to locate meaningful evidence. In order to thwart investigations and evade detection, cybercriminals frequently employ anti-forensic strategies include erasing files, concealing data, and encrypting communications [4].

Cloud computing and Internet of Things (IoT) ecosystems present another major difficulty. Digital evidence may be maintained across numerous nations and service providers, posing legal and legal complications during investigations. Furthermore, the huge variety of IoT devices and non-standard data formats makes evidence collecting and processing more challenging. In order to ensure that evidence is gathered and stored in a way that complies with the law, investigators must also strike a balance between forensic investigations and privacy restrictions and data protection legislation.

6. National and International Job Market

The fast growth of digital technology and cybercrime has direct to a considerable increase in demand for digital forensics professionals on a national and international scale. Digital forensic analysts, incident responders, and cybercrime investigators are in high demand in the UK's government, law enforcement, banking, and commercial sectors. The majority of contemporary criminal investigations include electronic evidence, which is why nations like the United States, Canada, Australia, and those in the Middle East and Europe are facing a scarcity of qualified digital forensics specialists [4]. Digital forensics is one of the cybersecurity fields that is expanding the fastest due to the development of specialist education and certification programs brought about by the increased complexity of cyberattacks and the widespread usage of digital devices [4].

7. Conclusion

Because of the growing dependence on digital technology and the increasing sophistication of cyber threats, digital forensics has appeared as a critical discipline in contemporary cybersecurity and criminal investigations. The field has grown greatly with modern tools such as FTK Imager, FTK Analyser, and Cellebrite enabling investigators to capture, evaluate, and preserve digital evidence effectively. The strong relationship between digital forensics and cybersecurity underscores the need of combining preventive security measures with forensic investigative capabilities to improve incident response and support legal processes. Investigations are made more difficult by obstacles like encryption, anti-forensic methods, enormous data volumes, and legal concerns. Despite these challenges, the increasing need for qualified workers as well as the growth of specialist training and certification programs suggest that digital forensics will continue to be a crucial and quickly evolving industry with plenty of job possibilities across the globe.

TASK-2

Table of Contents

1. Case Background	10
2. Chain of custody.....	10
3. Methodology.....	11
3.1 Evidence Acquisition.....	11
3.2 Evidence Preservation and Imaging.....	11
3.3 Hash Verification.....	11
3.4 Examination and analysis.....	11
3.5 Chain of Custody Maintenance.....	11
4. Findings.....	12
4.1 Communication Analysis.....	12
4.2 File Analysis.....	20
4.3 Image Analysis.....	24
4.4 Call log analysis.....	25
5. Suspect role and analysis.....	26
6. Conclusion	27
7.Recommendations.....	28

1. Case Background

Technology company Quantum Tech discovered a significant security compromise involving illegal access to their library of unique AI chip design patents, including the patent known as QT-AI-2025. Sensitive intellectual property may have been accessed and possibly extract without authorisation, according to suspicious activity found by the company's internal IT security team. Emma, a senior engineer who recently started working at Quantum Tech, is the main suspect in the event, according to preliminary forensic evidence.

Emma is suspect of using her privileged access to get private patent information with the goal of selling it to NexGen Circuits a rival company via a middleman named Joe. According to additional research, Norman who is connected to NexGen Circuits, would be a possible buyer of the stolen intellectual property. Several digital communication channels such as emails and call logs from different devices and mobile messaging are involved in the suspected actions.

Digital evidence has been legally obtained in accordance with appropriate chain-of-custody protocols to assist the inquiry. This includes Joe's smartphone, which might have coordination communications and Emma's Android smartphone which might have communication logs and application data. Emma's USB flash drive which might have stolen patent files and Norman's Android smartphone which might have proof of purchase or negotiation pertaining to the stolen data. The inquiry is being carried out in collaboration with law enforcement organisations and the results are meant to support future legal actions for associated cybercrimes business reconnaissance and intellectual property theft.

2. Chain of Custody

Item No.	Device	Owner	Tool Used
E01	Huawei	Emma	Cellebrite UFED
E02	USB Flash Drive	Emma	FTK Imager
E03	Samsung	Joe	Cellebrite UFED
E04	Nokia	Norman	Cellebrite UFED

Device	Hash Values SHA256
Huawei	D5193dbf8246c09fdde73be8558343985ab24a2e1c142e4d4e16e2b6507e31f
Samsung	0e585c4fe8160254253be515a16ff94b7fdf88b248b67d45cfdef8753a9a3195
Nokia	A693656c260e339069756be8005346e97033d0ccf2f79add56cad69c9eade13ab

3. Methodology

The methodology used for this investigation depends on standard digital forensic principles to make sure that all evidence is gathered, collected and analysed in a forensically sound manner. To preserve evidence integrity, support legal admissibility, and guarantee appropriate management of digital evidence throughout the investigative lifespan, a methodical forensic procedure is necessary [2]. Additionally, in order to prove the legitimacy and dependability of digital evidence in court, a documented chain of custody must be maintained.

3.1 Evidence Acquisition

To make sure that no original data was altered during extraction, industry-standard forensic techniques were used during the collecting procedure. Cellebrite UFED, which facilitates physical, logical, and file-system extraction from Android devices, was used to obtain Emma, Joe, and Norman's mobile devices. FTK Imager was used to produce a bit-by-bit forensic duplicate of Emma's USB flash drive. To guarantee the accuracy and admissibility of digital evidence, it is advised to employ forensic imaging techniques and organised acquisition procedures [2].

3.2 Evidence Preservation and Imaging

To stop any changes to the source data, write-blocking and read-only access techniques were used. To guarantee accurate monitoring and identification during the course of the inquiry, each gadget was given a distinct evidence ID (E01-E04). Any modification to the original data could compromise the legality of the investigation and the admissibility of evidence in court, hence proper evidence preservation procedures are crucial [1].

3.3 Hash Verification

By verifying that the evidence has not been tampered with during gathering, storage, or analysis, these hash values guarantee data integrity. To ensure the consistency and dependability of the evidence, the hash values were noted and compared at several points throughout the inquiry. The chain of custody procedure heavily relies on the use of cryptographic hashing and integrity verification techniques, which are regarded as essential requirements in digital forensic investigations.

3.4 Examination and analysis

WhatsApp messages, emails, call logs, and multimedia files were among the communication records found in mobile device data that was recovered using UFED. Metadata, file activity, and papers regarding to patents were examined in the USB evidence. The analysis procedure concentrated on finding evidence of intellectual property theft, reconstructing timeframes, and discovering relationships between suspects. In order To process massive amounts of digital information and assist

with incident reconstruction, modern digital forensic investigations increasingly rely on systematic investigative models and sophisticated analytical tools [4].

3.5 Chain of Custody Maintenance

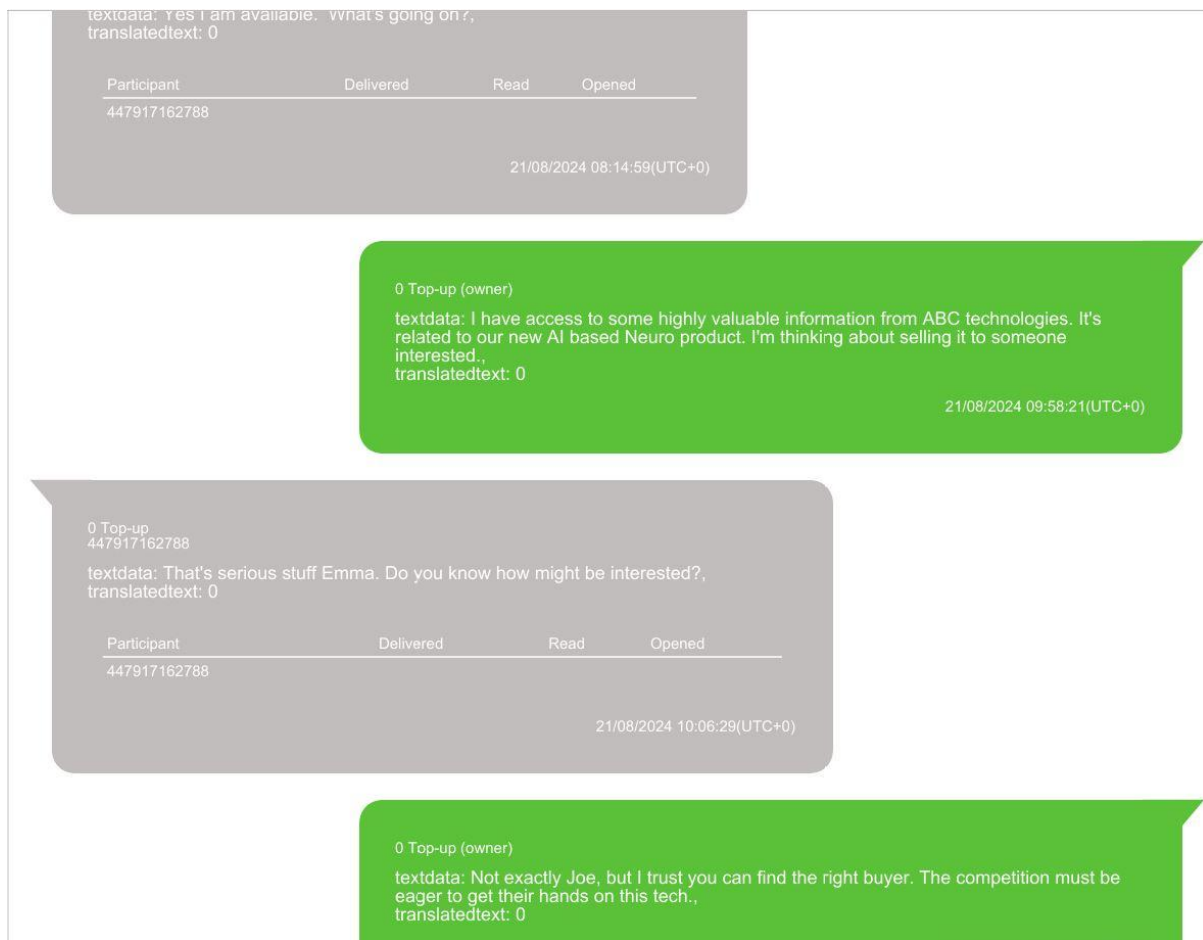
Details such the type of device, owner, tool used, and hash values were recorded for each piece of evidence. To avoid tampering, access to evidence was limited and recorded during the whole inquiry. To prove that digital evidence has remained genuine, trustworthy, and unaltered throughout the inquiry and ensuing legal actions, a full chain of custody must be maintained.

4. Findings

4.1 Communication Analysis

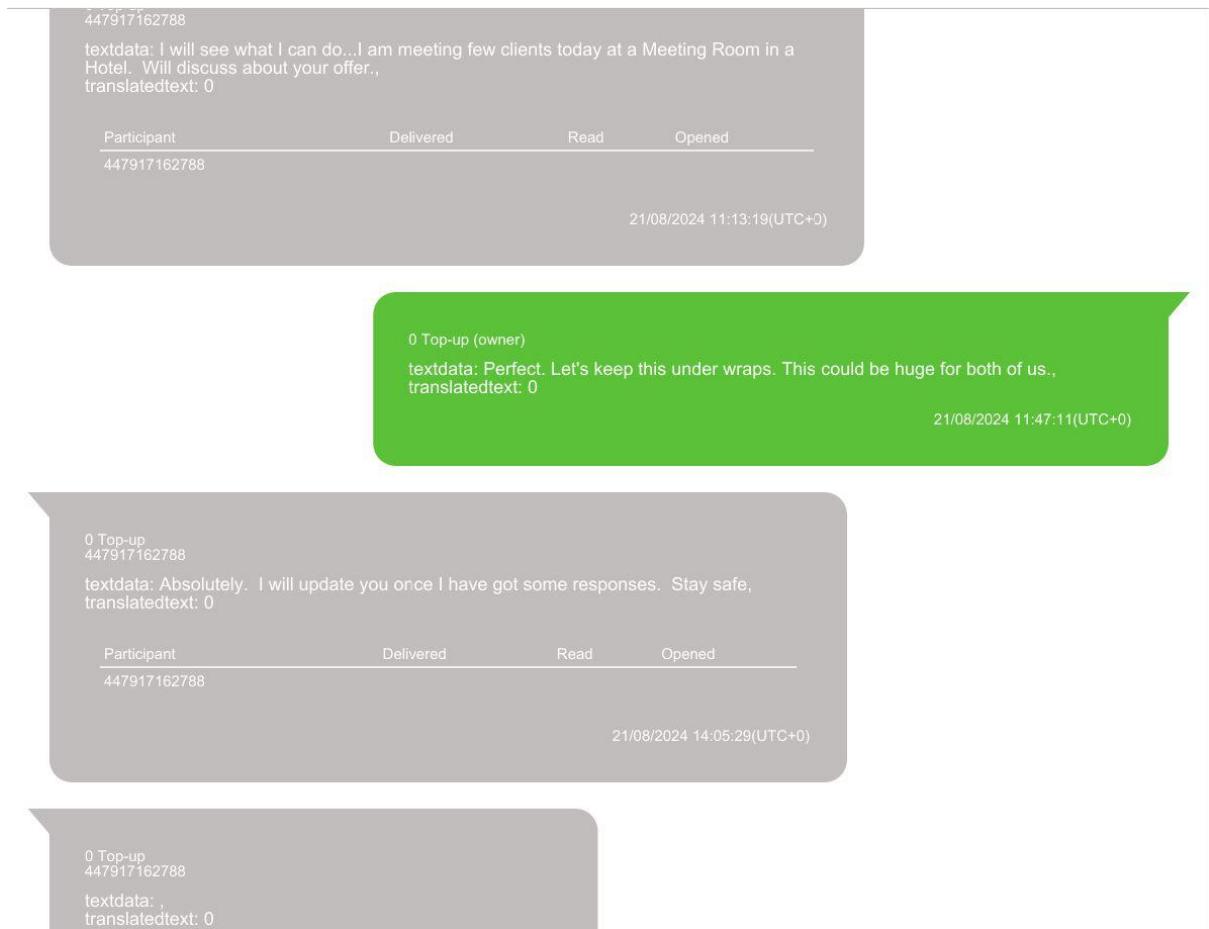
A. Emma's Smartphone (Huawei):

The examination of Emma's smartphone The messages between Emma and one unknown number that was found and that number was not saved number in the contact list.



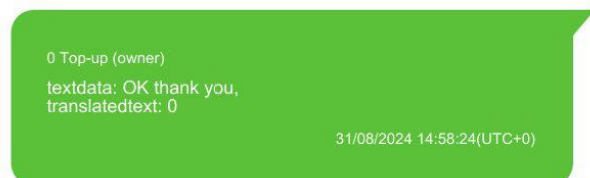
a. Message Information – 1

In this Image, Emma sent that she has some “Highly information from ABC tech.” and that is related to their new AI based Neuro product And that unknown sent that stuff message and looking for one person for selling.



b. Message Information – 2

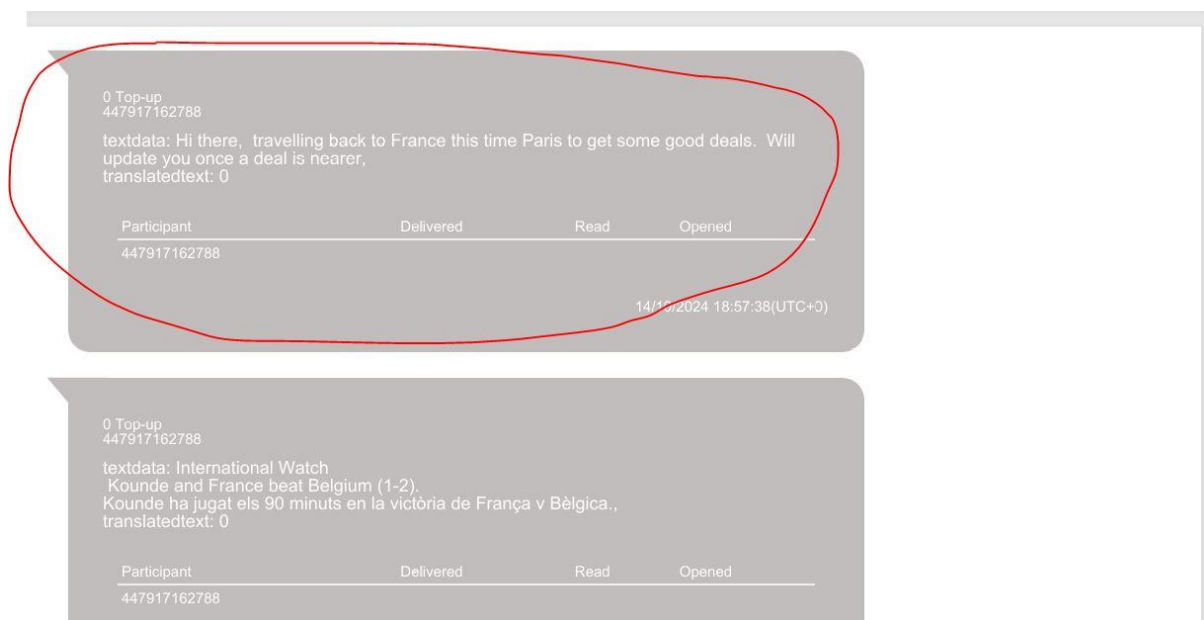
In this message, that unknown guy was going in a meeting and searching about the right buyer. Emma said that they have to keep this conversation secret between us.



80

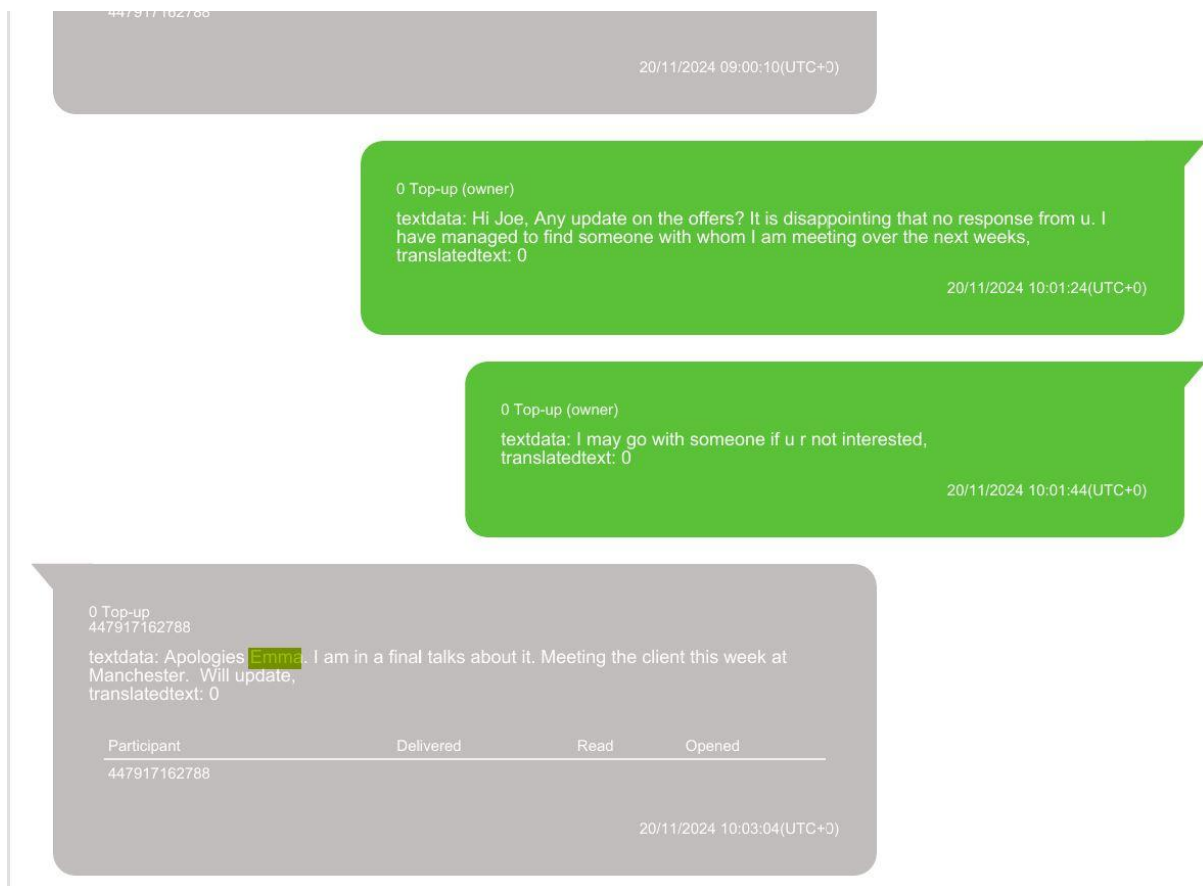
c. Message Information - 3

In this conversation, the unknown person sent message in Spanish, according to our research. The Spanish meaning of BARCA XI is Barcelona's Starting eleven may be it related to meeting.



d. Message Information – 4

See the round one message, The unknown person was travelling France for some good deals which is related to search e buyer or may be make some deals for Product.



e. Message Information – 5

Additionally, after 24 days Emma sent message that She was looking for someone else if they not interested in it and after just 2 minute that guy responded that they already have one person and going to deal finalize in that week in Manchester.



f. Message Information – 6

After long time, Emma sent message about updates.

0 Top-up
447917162788

textdata: No, he's serious. Wants a demo sample. Can we do that?,
translatedtext: 0

Participant	Delivered	Read	Opened
447917162788			

31/01/2025 10:22:07(UTC+0)

0 Top-up (owner)

textdata: Impossible. But a detailed breakdown? Yes. How's the offshore arrangement? ,
translatedtext: 0

31/01/2025 10:22:32(UTC+0)

0 Top-up
447917162788

textdata: He's good with it. 5M secured. Waiting for confirmation. The rest?,
translatedtext: 0

Participant	Delivered	Read	Opened
447917162788			

31/01/2025 10:23:18(UTC+0)

g. Message Information – 7

On that same day, the unknown person said that the buyer wants some sample and Emma clearly said no because of detailed breakdown. And in the Last they both waiting for the buyer Confirmation.

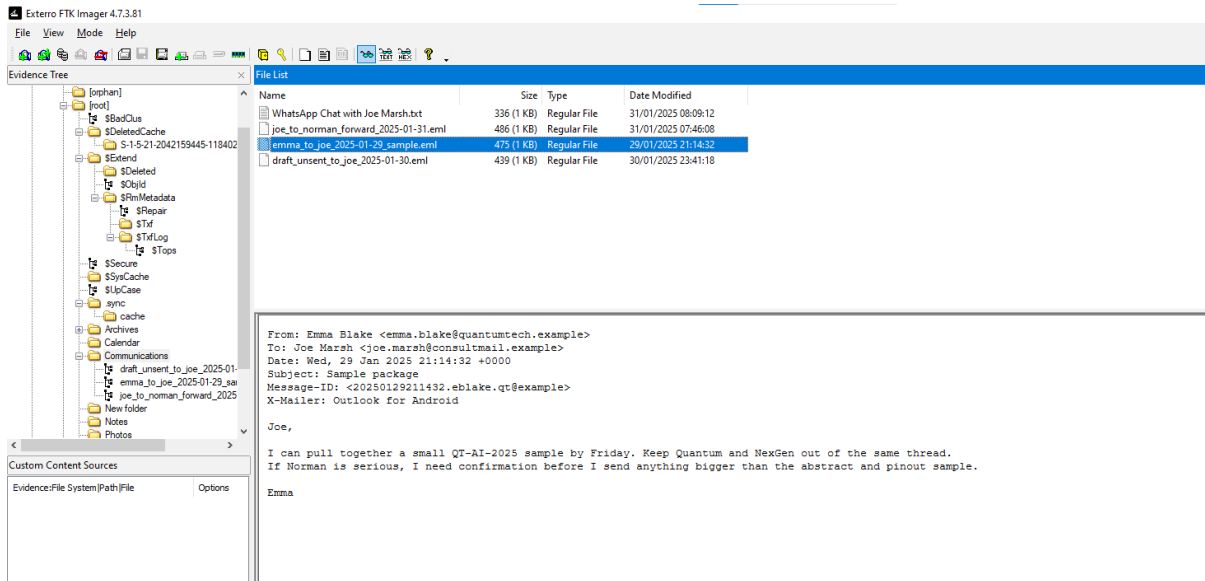
According to this all Communication, I get some hint or I think that Joe is a middleman between Emma and the buyer. Here is the table of on which date and time the messages was sent.

Here, are the Emma's smartphone findings:

No.	Date	Time	From to
Message Information – 1	21/08/2024	09:58:21	Emma to unknown person
Message Information – 2	21/08/2024	11:13:19	Unknown person to Emma
Message Information – 3	31/08/2024	13:52:36	Unknown person to Emma
Message Information – 4	14/10/2024	18:57:38	Unknown person to Emma
Message Information – 5	20/11/2024	10:01:24	Emma to unknown person
Message Information – 6	31/01/2025	10:15:15	Emma to unknown person
Message Information – 7	31/01/2025	10:22:07	Unknown person to Emma

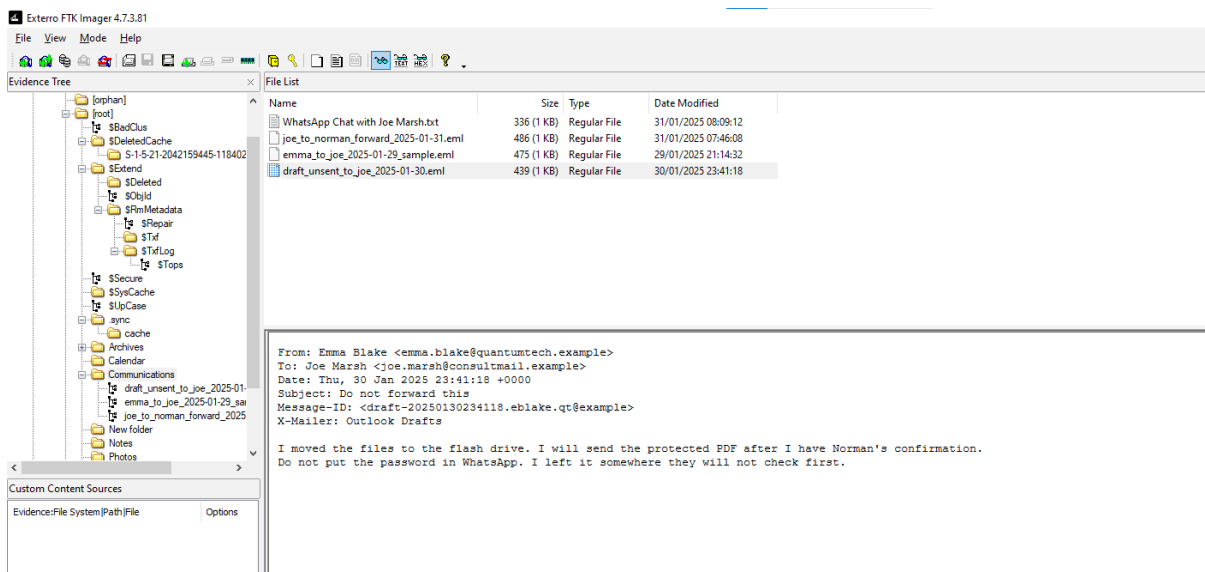
B. Emma's USB Drive

This Drive I analysed in the FTK Imager tool and found some messaged between Emma and Joe. The below Image show the outlook message from Emma to Joe.



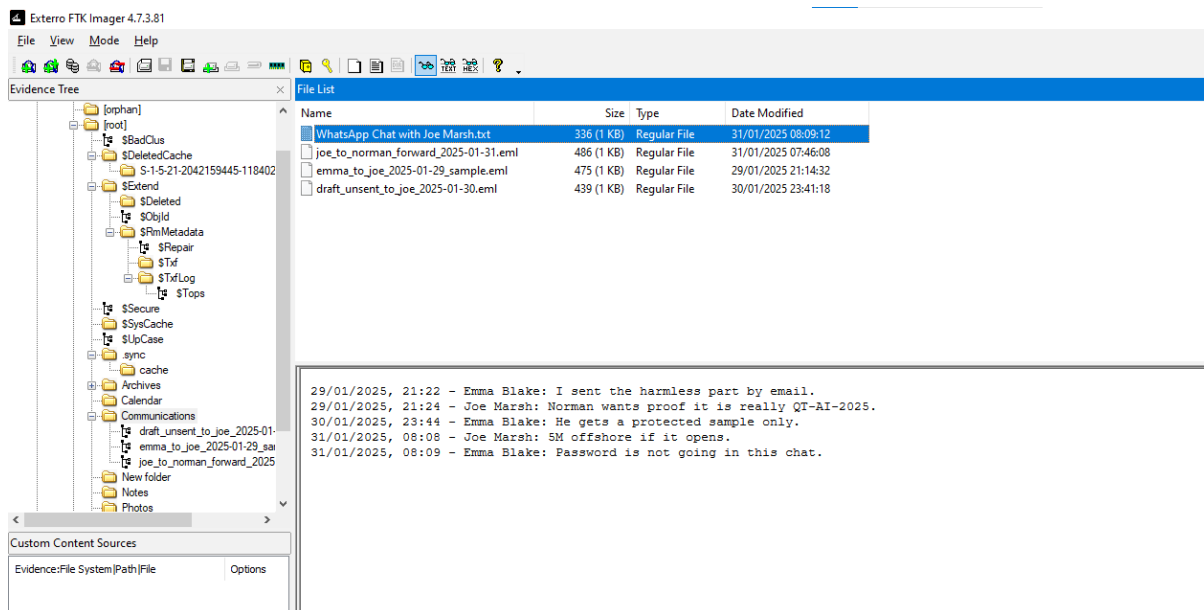
h. Message Information – 8

In this image, Emma was sending a small sample of QT-AI-2025 to Joe and Joe was sending that sample to Norman. This conversation prove that Norman is a Buyer who was responding immediately for this and that guy conversation between Emma and Joe in Emma's smartphone that was Norman.



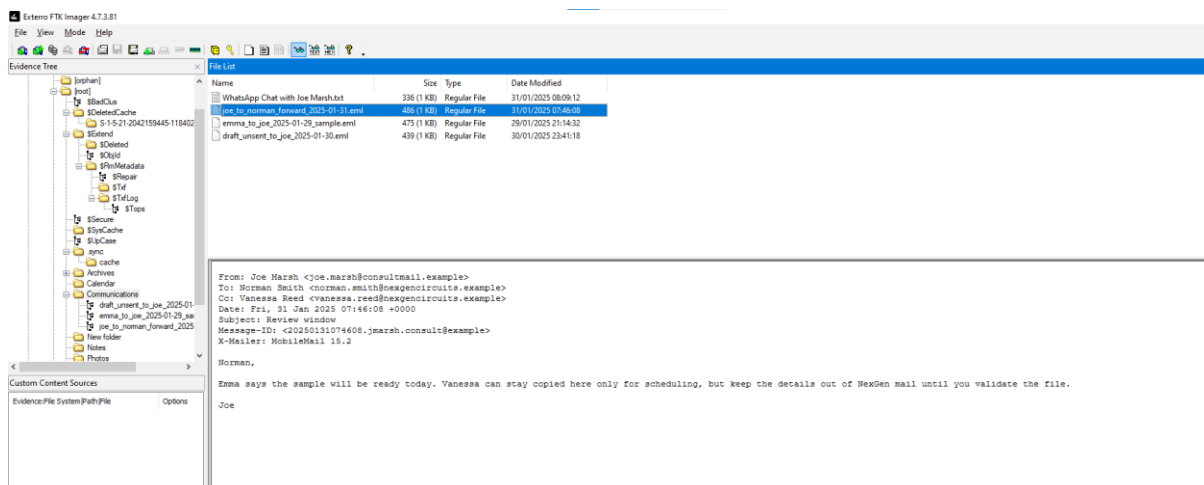
i. Message Information – 9

The upper picture is the biggest clue in my view. That was unsent message in outlook. Emma put that important file in this flash drive and that was password protected PDF. She sent this PDF after Norman's confirmation and the password clue was in somewhere else may be in smartphone.



J. Message Information – 10

This is the WhatsApp chat between Emma and Joe. Emma sent harmless part by email but I unable to find that part by email. And password was not in this chat but I mentioned in previous image that one password protected PDF file.



k. Message Information – 11

From this image, I found one more person Venessa Reed who is R&D Director at NexGen Circuits and may be suspected buyer. This message is forwarded Joe to Norman via Mobile Mail platform.

Emma's USB Flash Drive table which contains Date, Time and on which platform messages was sent.

No.	Date	Time	From to	Platform
Message Information – 8	29/01/2025	21:14:32	Emma to Joe	Android Outlook
Message Information – 9	30/01/2025	23:41:18	Unsent message to Joe	Android outlook
Message Information – 10	31/01/2025	08:09:36	Emma and Joe	WhatsApp
Message Information – 11	31/01/2025	07:46:08	Joe to Norman (forwarded)	Mobile Mail

C. Norman's smartphone (Nokia)

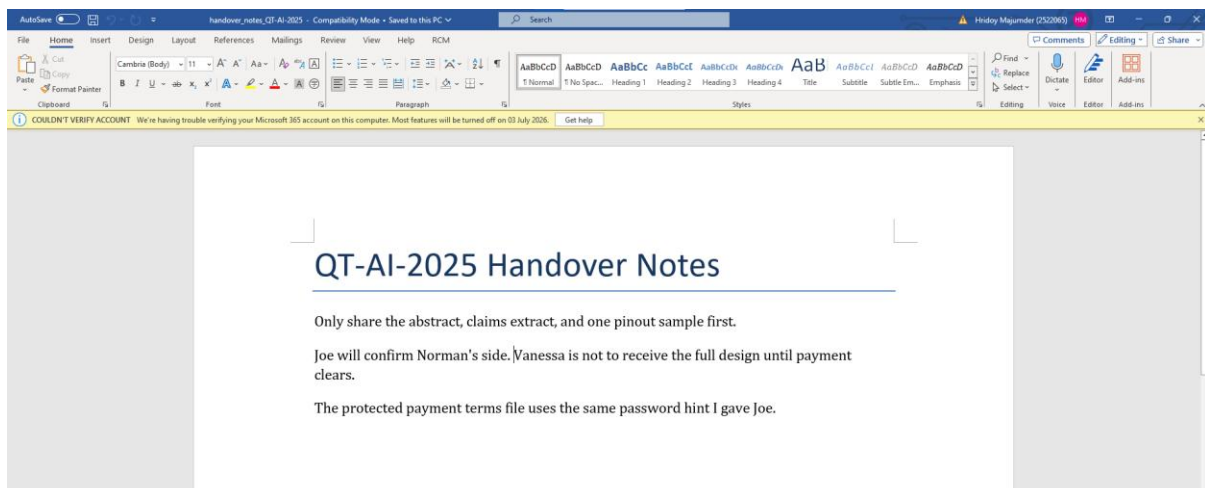
The examination of Norman's Nokia Smartphone unable to finding any evidence to the theft of Quantum Tech's confidential data. However, Norman's alleged participation in this case, it's possible to further investigation will turn up communication between Norman and Joe about the attempt to obtain company information. Additionally, there may be some call logs between Norman and Venessa, the R&D Director at NexGen Circuits.

D. Joe's smartphone (Samsung)

During investing Joe's Samsung Smartphone unable to identify any images related to the stolen patent information. However, the communication records between Joe and Emma might be on the device because Joe's suspected role as an intermediary. Additionally, detectives may be able to access protected information connections between the suspects with the use of password clues, authentication messages or other digital artefacts kept on the device.

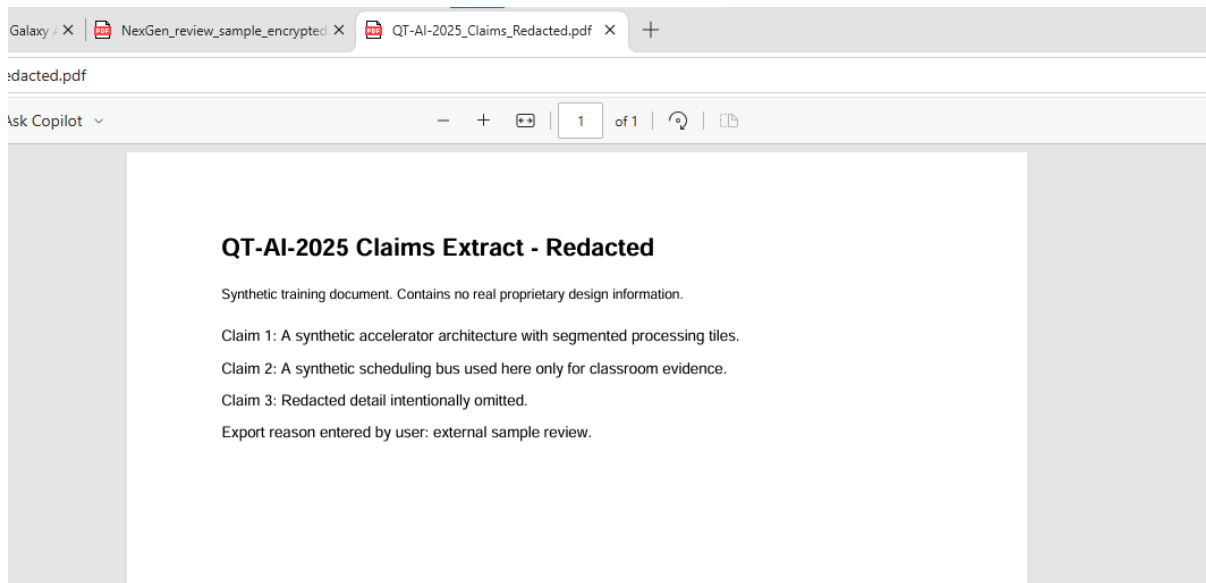
4.2 File Analysis

A. Emma's USB Drive:



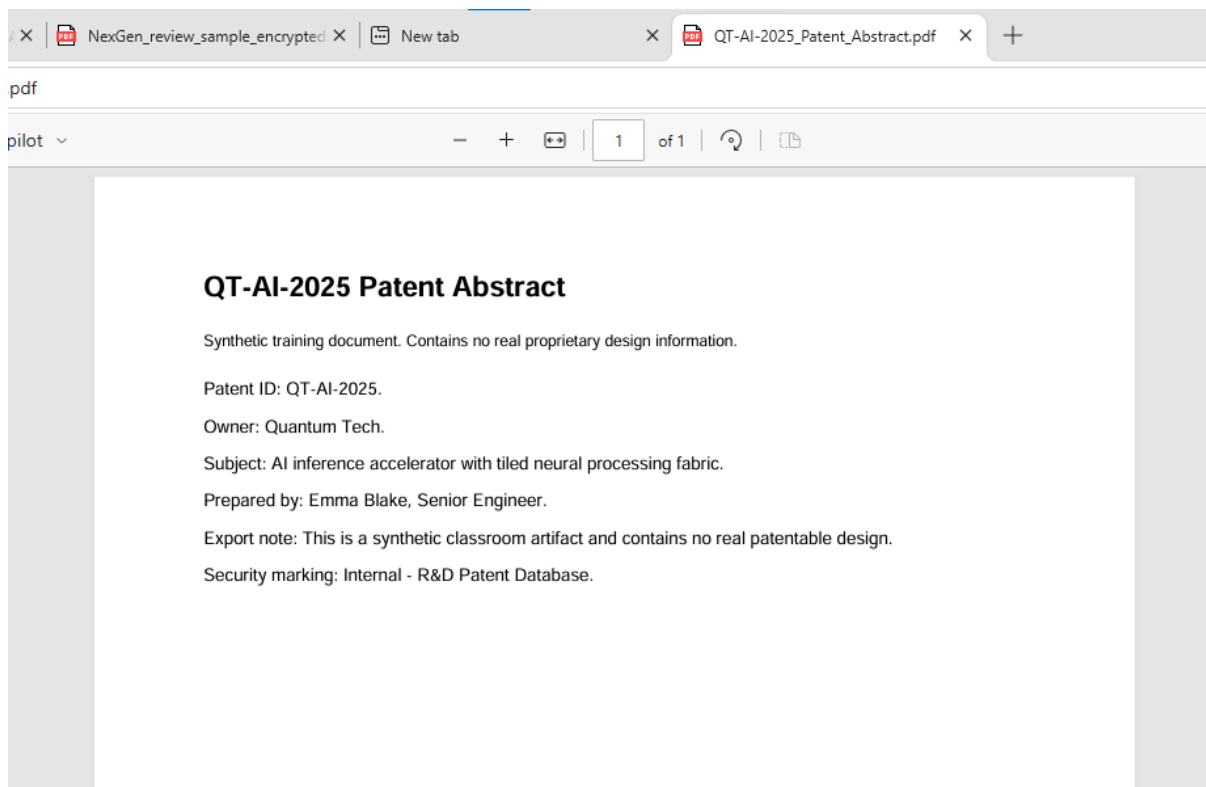
a. File Image – 1

Emma made one file Handover Note which was related to share the abstract and Emma sent the password protected file to Joe which hint was Emma gave Joe previously. And that protected file name is "NexGen_review_sample_encrypted.pdf" I found.



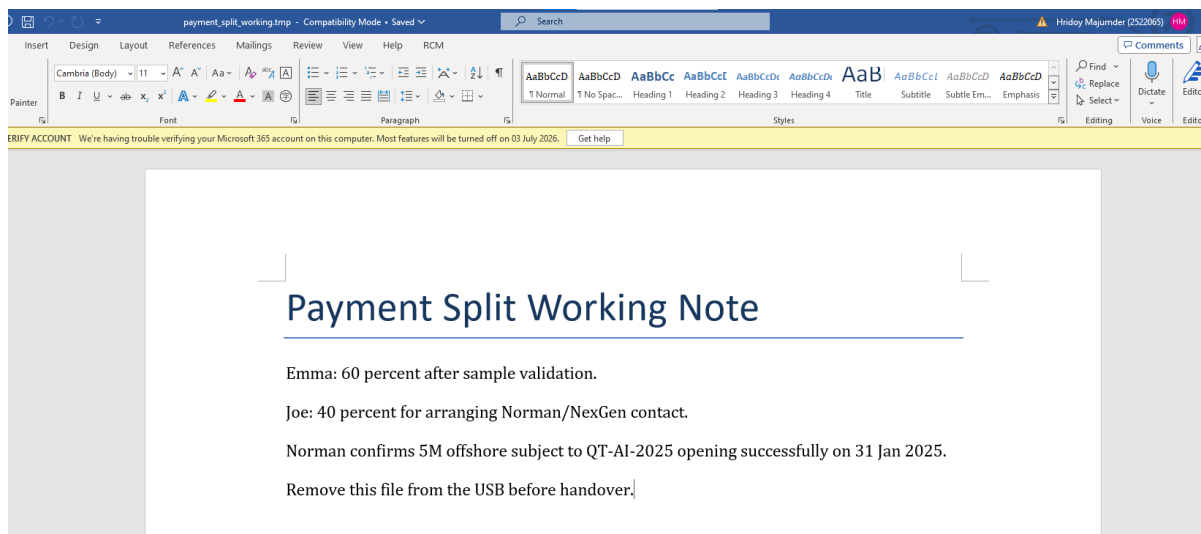
b. File Image – 2

After investigating this file, It may be training document not a real one which contain some information related to design.



c. File Image – 3

QT-AI-2025 Patent Abstract file describes the ID, owner name, subject that all information. But this was also not a real one document.

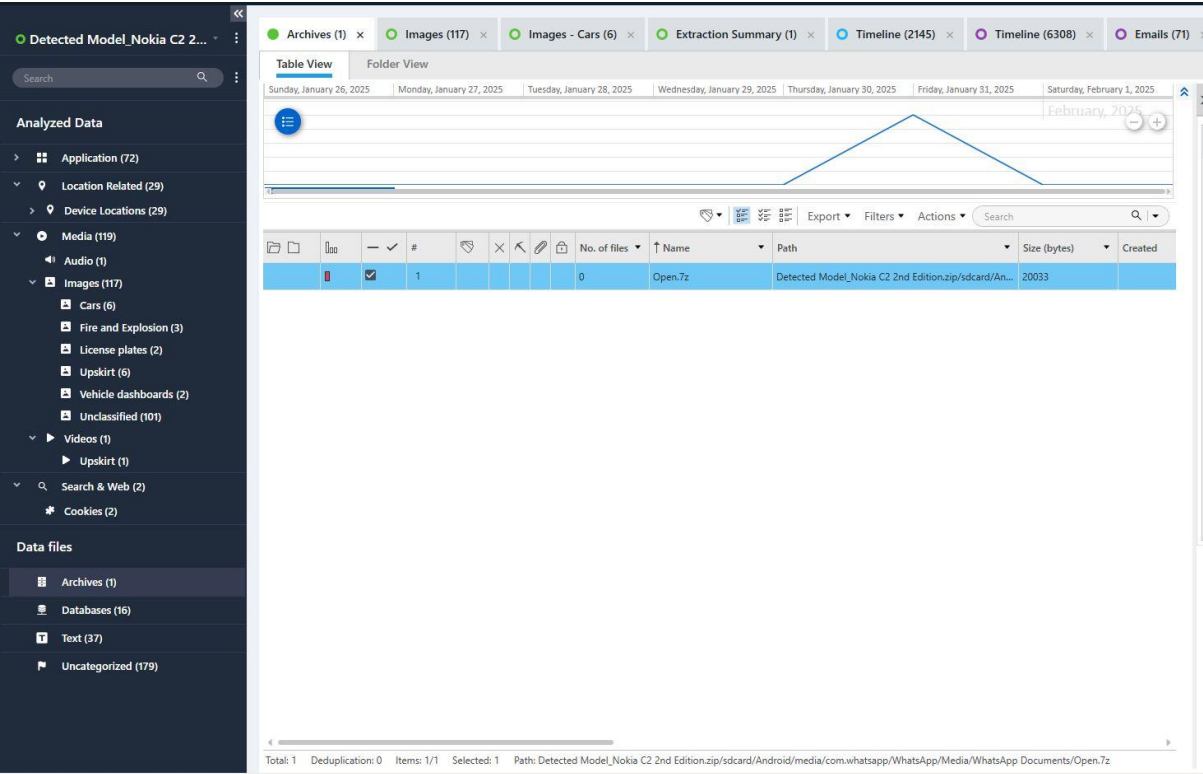


d. File Image – 4

This Payment split working note was the important file. it shows how payment was split after Norman’s Confirmation. After that Emma wants to remove this file before handover.

No.	Date	Time	File Name
File Image - 1	30/01/2025	22:09:33	handover_notes_QT-AI-2025.docx
File Image - 2	28/01/2025	20:13:04	QT-AI-2025_Claims_Redacted.pdf
File Image - 3	27/01/2025	18:22:11	QT-AI-2025_Patent_abstract.pdf
File Image - 4	31/01/2025	20:38:55	payment_split_working.tmp

B. Norman’s Smartphone (Nokia)

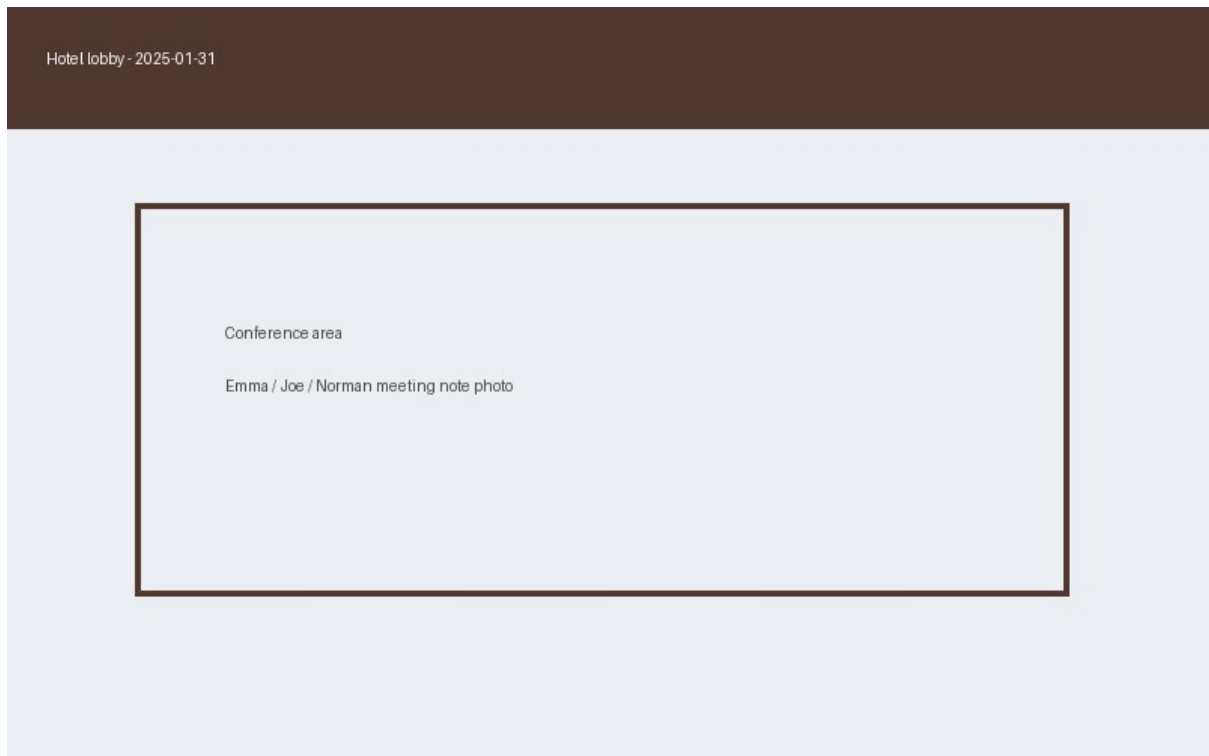


e. File Image – 5

During the Norman’s Smartphone investigation I found one zip file was founded in his archive and after save this zip in my PC it may be password protected.

4.3 Image analysis

A. Emma's USB drive



a. Image – 1

In Emma's USB drive I found this image. It shows that Emma, Joe and Norman meet up called Conference area.



b. Image – 2

After looking carefully this image, it hidden some data into it because shows “Review image for external discussion” means some is hidden inside the image but I unable to find.

B. Joe’s Smartphone (Samsung)

Evidence supporting the conversation between Emma and Joe was found when Joe's Samsung smartphone was examined. Based on their correspondence, Joe told Emma on 14/10/2024 18:57:38 that time he was going to Paris for a meeting. However, location information found on Joe's smartphone suggests that he was still in London at the time because a picture on the device had metadata indicating a location in London at the same time and date.

Afterward investigation showed that Joe bought a ticket to Paris on 14/10/2024 22:17:13 indicating that the trip might have been scheduled soon after the correspondence with Emma. Joe also planned to meet Norman in Manchester, according to messages found on the smartphone. The relevant communication was sent on 20/11/2024 10:03:04 and Joe's smartphone location data shows that he was in Manchester on 20/11/2024 20:16:20. These results suggests that Joe visited several places that might have been related to discussions and agreements on the alleged transfer of Quantum Tech's private data.

4.4 Call Log Analysis

A. Emma’s smartphone:

According to Emma’s smartphone findings. I found one contact on Emma’s phone which was Joe Marsh number which was ended with 8686 and that communication chat, the number was different that was ended with 2788.

4	Name: Joe Marsh Source file: Huawei_POT-LX1 P Smart.zip\data\data/com.android.provider.s.contacts/databases/contacts2.db : 0x13E17 (Table: raw_contacts, phone_lookup, data; Size: 544768 bytes) Huawei_POT-LX1 P Smart.zip\data\data/com.android.provider.s.contacts/databases/contacts2.db-wal : 0x53D49 (Size: 605672 bytes)		Phone: 00447476538686 Mobile 00 44 7476 538686				
---	---	--	--	--	--	--	--

a. Contact Information – 1

B. Joe’s Smartphone

Furthermore, an audio file dated Octo, was found on the device. It is thought that the recording was recorded inside an aeroplane based on the background noises and the accompanying visual and communication data.

5. Suspect Roles & Analysis

5.1 Emma – Primary Suspect

Emma is a Senior Engineer at Quantum Tech and she is identified as the primary suspect in the corporate espionage investigation. Evidence from her android Smartphone and USB flash drive suggests that the company's exclusive AI chip design patent (QT-AI-2025) may have been accessed without authorisation. Emma has discussed with Joe about private company information from her communication records which includes messages, emails and some document files. Furthermore, the existence of patent on her USB drive suggests that she may have duplicated and tried to take some critical intellectual property out of her company.

According to the evidence, Emma is evaluated as the primary perpetrator accountable for the theft and attempted sale of the company's confidential patent information.

5.2 Joe – Intermediary

Communication records connecting Joe to both Emma and Norman were found during the forensic analysis of his smartphone. According to the call logs and messages that was recovered Joe served as a middleman between the buyer (Norman) and the person who was allegedly stealing the information (Emma).

According to the evidence, Joe may have organised the transfer of the confidential information and helped with communication. Joe's involvement in the attempted sale of the stolen intellectual property is evaluated as an accomplice based on the evidence.

5.3 Norman – Potential buyer

Based on Emma's smartphone and USB drive data, Norman might have more proof of the theft of Quantum Tech's confidential data. Norman's smartphone may also contain communication records, such as emails and messages sent and received to Joe. Additionally, there can be some images and documents that include private sensitive data about company. Emma's USB drive was found to include a password-protected PDF file with private company information that may have been shared with Norman.

Furthermore, messages forwarded by Joe to Norman about payment discussion for the material that was taken. Therefore, Norman's smartphone and banking records may uncover transactions history about that sensitive data.

6. Conclusion

In conclusion, this report has analysed the digital forensics from both theoretical and practical standpoint. Digital forensics plays most important role in modern cybersecurity. It makes identification, Preservation, analysis and presentation of digital evidence in a manner way that is legally acceptable. The study of current forensic tool such as FTK imager, FTK analyser and Cellebrite UFED highlight the importance of advanced technologies in the collection and analysis of digital evidence while maintaining data integrity. Additionally, the connection between cybersecurity and digital forensic shows how both field collaborate to stop cyberattacks and look into security events when they happen.

The study also examined new developments that are changing the view of digital investigations including blockchain analysis, cloud forensics, IoT forensics and artificial intelligence. However, challenges like encryption, anti-forensic methods, massive data quantities and jurisdictional concerns still restrict the efficiency of forensics requiring the ongoing creation of new tools and procedures.

Forensic examination of several digital devices revealed evidence of illegal access to the AI chip design patent (QT-AI-2025) in the Quantum Tech case's practical investigation. The results suggested that Emma might be the main suspect with Joe serving as a middleman and Norman as a buyer of the stolen information. The investigation ensured the dependability and integrity of the evidence by adhering to appropriate forensic processes which include acquisition, preservation, hash verification, and analysis.

Overall, this study highlights the growing significance of digital forensics in today's technologically advanced society and shows that it is a crucial discipline in fighting cybercrime and assisting with legal investigations.

7. Recommendations

Act	Relevance of Case	Max Punishment
Computer misuse act 1990	Emma accessed Quantum Tech's Patent database without authorisation, directly violating Section 1 and section 3 this act.	Up to 10 years imprisonment
Theft act 1968	Emma stole the QT-AI-2025 patent, which constitutes theft of intellectual property and proprietary data under this act.	Up to 7 years imprisonment
Fraud act 2006	Joe and Norman are implicated in the attempted fraudulent sale of stolen patent data, constituting fraud by false representation.	Up to 10 years imprisonment
Intellectual Property Act 2014	The theft and attempted sale of Quantum Tech's AI chip design patent constitutes a direct violation of intellectual property rights protected under this Act.	Fine and imprisonment
Police and Criminal Evidence act (PACE) 1984	This investigation was conducted in accordance with PACE 1984 guidelines, ensuring all evidence was lawfully obtained, property documented and maintained under strict chain of custody protocols.	Governs investigators

Suspect	Role	Applicable Act(s)	Recommended Action
Emma	Perpetrator	Computer Misuse Act 1990, Theft Act 1968, intellectual Property Act 2014	Arrest and prosecution maximum 10 years imprisonment.
Joe	Intermediary	Fraud Act 2006, Theft Act 1968	Arrest and prosecution as co-conspirator maximum 10 years imprisonment
Norman	Buyer	Fraud Act 2006, intellectual Property Act 2014	Arrest and Prosecution as co-conspirator maximum 10 years imprisonment
Venessa	NexGen Contact	Intellectual Property Act 2014, Fraud Act 2006	Further investigation recommended possible charges as accessory

References

- [1] A. D. Salman and E. H. Hasan, "Survey Study of Digital Forensics: Challenges, Applications and Tools," *2023 16th International Conference on Developments in eSystems Engineering (DeSE)*, pp. 788, 2023. . DOI: 10.1109/dese60595.2023.10469020.
- [2] A. R. Javed *et al*, "A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions," *IEEE Access*, vol. 10, pp. 11065, 2022. . DOI: 10.1109/access.2022.3142508.
- [3] F. Casino *et al*, "Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews," *IEEE Access*, vol. 10, pp. 25464, 2022. . DOI: 10.1109/access.2022.3154059.