

Investigation Case QT-AI-2025

Digital forensics analysis



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Alexis Rochefort

Investigation Case QT-AI-2025	1
Executive summary :	1
Case background :	1
Evidence Inventory:	2
Methodology:.....	3
Acquisition:	3
Analysis:	3
Forensic Findings:	4
Conversation Timeline:.....	4
Usb key analysis:	5
geographic analysis:	6
.....	7
Suspect profiling:	9
Conclusion:	9
Context Analysis	10
Communication Extraction & Processing	10
Geolocation & Mobility Analysis	10
USB Drive Analysis	11
Encrypted Document Decryption (Open.docx)	11
Advanced USB Analysis	11
Vanessa Link Analysis	12
Extended Intelligence Correlation	12
Location Intelligence Interpretation	12

Executive summary :

This investigation confirms a coordinated operation of industrial data theft aiming for an industrial patent of a chip “QT-AI-2025” belonging to a company: “Quantum tech”. This investigation proves the sale of the stolen data by a person for personal interests.

responsibilities:

- The main suspect's name is **Emma Jonhson**, an engineer employee of Quantum tech, also identified as "Peter Dover". Her culpability is proven by the technical link between her personal email dovp59@gmail.com and her bank details.
- **Joe Marsh**, the intermediary, acted as a broker to identify buyers and organize logistics.
- The buyer: **Norman Smith**, work for NexGen Circuits (NSI), a Quantum tech's competitor's company.

Timeline:

- 1) Emma contact Joe about data she stole
- 2) Joe brings Emma to meet some potential buyers and meet Norman Smith: they eventually meet some in Qatar and India
- 3) A transactions is agreed of 5M to sell to nexgen and a delivery plan hashed is agreed
- 4) They lost contact and try to clean up evidences

Evidence:

the accusations are based on four things:

- Communications, extract from whatsapp/email/sms/facebook conversations give details on the transaction, the negotiations, the price and the delivery plan of the blueprints
- Financial evidence: a decrypted word containing the details of an offshore bank account registered at Caiman's Islands at Emma Johnson's name, supposed to receive a 5M USD payment.
- Technical support: an USB key containing something probably like an "extraction kit" (firmware and drivers). A deletion attempt have been tried on 9th April 2025.
- Geographic data: GPS coordinates extracted from Emma's phone confirm Emma conducted the mission across the world (Quatar and India).

To conclude, every evidence have been extracted following the digital forensics principles. Their Integrity have been preserved during the analysis.

Case background :

The target:

Quantum Tech's IT security team detected unauthorized access to their proprietary patent database, specifically, the AI chip design patent (QT-AI-2025). This forensic investigation was organized to analyze the digital devices of the primary suspect, Emma

Johnson, and her suspected associates.

The security team of Quantum tech detected unauthorized access to his patent's database. First internal investigation has designed Emma Johnson as the first suspect, a senior Engineer in the company who have all the rights necessary to access this patent.

Hypothesis :

Quantum tech suspect Emma for the theft of the QT-AI-2025 patent to sell it to a commercial competitor, NextGen circuit, with the help of an intermediary named Joe.

The investigation aims to confirm that a data theft and a transaction happened.

Investigation perimeter:

Five devices have been retrieved:

- The Emma's phone, a Huawei
- Her personal USB key
- Joe's Marsh smartphone
- Norman Smith's smartphone
- A fourth device, a Nokia C2 containing secondary evidence

Evidence Inventory:

Evidence ID	Owner	Device Model	Manufacturer	OS	Extraction Type	Hash Type	Hash Value	Integrity Status
Item A	Emma Johnson	Huawei POTS-LX1P Smart	Huawei	Android 10	File System (ADB)	SHA-256	d5193dbf8246c09fdde73be8558343985ab24a2e1c142e4d64e16e2b6507e31f	Verified
Item B	Emma Johnson	USB Flash Drive (16GB)	Generic (EmmaFlashDrive)	FAT32	Physical (E01)	MD5	41a6d1cdaf265bbf4e531698e89b0e44	Verified
Item C	Joe Marsh	Samsung SM-A137F Galaxy A13	Samsung	Android 14	File System (Backup)	SHA-256	0e585c4fe8160254253be515a16ff94b7fdf88b248b67d45cfdef8753a9a3195	Verified
Item D	Norman Smith	Note 14	Ulefone	Android 12	File System (Backup)	SHA-256	630724e2f8863adb9c4f7df1ab645e56c19a832d546fe7ab55b0cebf8ea7befd	Verified
Item E	Emma Johnson	Nokia C2 2nd Edition	HMD Global	Android 11	File System (Backup)	SHA-256	a693656c260e339069756be8005346e97033d0ccf2f79add56cd69c9eade13ab	Verified

Methodology:

Acquisition:

- Cellebrite for mobile device image acquisition and data extraction
- FTK imager for USB key image extraction

Analysis:

- Cursor ai agent have been used to create automated scripts to retrieve the data from the extracted reports
- Gemini CLI have been used to help performing the password bruteforcing, by creating a dictionary of keywords used in the project.

Forensic Findings:

Emma Identity

Identity of Emma as Peter Dover has been proven through the conversations, even if the phone and her email address are registred under the name of “Peter Dover”, Peter has been called “Emma” in every conversation.

Conversation Timeline:

Date	Time	Platform	Sender	Receiver	Message Content	Forensic Interpretation
2024-08-21	10:58:21	WhatsApp	Emma (Peter Dover)	Joe Marsh	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.	EXPLICIT INTENT: Emma offers to sell stolen AI Neuro tech.
2024-08-21	11:06:29	WhatsApp	Joe Marsh	Emma (Peter Dover)	That s serious stuff Emma. Do you know who might be interested?	BROKER ENGAGEMENT: Joe acknowledges and asks for targets.
2024-08-21	11:10:36	WhatsApp	Emma (Peter Dover)	Joe Marsh	Find the right buyer; competition would be eager	INSTRUCTIONS: Emma tells Joe to source a buyer from competitors.
2024-08-29	15:10:34	WhatsApp	Joe Marsh	Emma (Peter Dover)	Hi there, just nearing to some wonderful offers. I am flying to Glasgow to meet a contact over there for a meeting.	LOGISTICS: Joe travels to Glasgow to pitch the stolen data.
2024-09-09	15:55:59	Instagram	Joe Marsh	Emma (Peter Dover)	Hi Emma	IDENTIFICATION: Joe confirms he knows Peter Dover is Emma.
2024-09-09	15:57:16	Instagram	Joe Marsh	Emma (Peter Dover)	Found someone in NSI company; asks what level of information can be shared	BUYER FOUND: NexGen Circuits (NSI) identified as the buyer.

2024-11-20	10:03:04	WhatsApp	Joe Marsh	Emma (Peter Dover)	Apologies Emma. I am in a final talks about it. Meeting the client this week at Manchester.	<i>LOGISTICS: Final negotiations in Manchester.</i>
2025-01-31	10:15:15	WhatsApp	Emma (Peter Dover)	Joe Marsh	Any updates? Need to move fast	<i>URGENCY: Emma pushes for finalization on deal day.</i>
2025-01-31	10:22:32	WhatsApp	Emma (Peter Dover)	Joe Marsh	Impossible. But a detailed breakdown? Yes. How's the offshore arrangement? 🌊	<i>PAYMENT SETUP: Emma refuses demo but asks about offshore account.</i>
2025-01-31	10:23:18	WhatsApp	Joe Marsh	Emma (Peter Dover)	He's good with it. 5M secured. Waiting for confirmation. The rest?	<i>PRICE AGREED: 5 Million USD confirmed and secured.</i>
2025-01-31	12:47:10	Facebook	Emma (Peter Dover)	Norman Smith	Norman, Joe told me u r ready to proceed. Lets keep this clean and quick	<i>HANDOVER INITIATION: Emma contacts the buyer Norman directly.</i>
2025-01-31	12:49:52	Facebook	Norman Smith	Emma (Peter Dover)	Almost. We need the. Blueprint in chunks Too risky in one go.	<i>SEGMENTED TRANSFER: Buyer requests data in parts for safety.</i>
2025-01-31	12:53:07	Facebook	Norman Smith	Emma (Peter Dover)	Agreed. First part releases, and 5M offshore reflects. Simple	<i>ESCROW/PAYMENT: Payment triggered by first data release.</i>
2025-01-31	12:53:09	Facebook	Emma (Peter Dover)	Norman Smith	Fine. Watch ur inbox in 48 hrs. After that we are ghosts	<i>CONCEALMENT: Emma sets delivery window and plan to disappear.</i>

Messages from Emma's phone has also been found on snapchat, we can see she tried to delete them to hide her trip to India, on those messages, she is talking to snapchat's ai bot about things not related to the investigation.

Usb key analysis:

The drive contained what can be described as a genuine "exfiltration kit," consisting of:

Firmware and Technical Blueprints: Presence of numerous NVM update packages (E810, I210, I225) and binary files (.bin) related to critical network infrastructure components (Intel).

Source Code: Extraction of header files (.h) and C source files (.c) linked to proprietary drivers (ixgbev, iavf).

Restricted Documentation: Multiple copies of documents named Intel_Proprietary_License.pdf found within carved ZIP archives.

Deployment Packages: A collection of .deb and .rpm files suggesting the theft of a complete development environment or ready-to-deploy firmware.

Modification Dates: Intense activity was detected in January 2025, coinciding exactly with the final negotiation phase between Emma (“Peter Dover”) and Norman Smith.

Mass Deletion: Nearly all technical archives (.tar.gz, .zip) were marked as deleted on April 9, 2025, likely after the transaction was confirmed or as part of an attempted “cleanup” by the suspect.

Recovery (Carving): Through forensic tools, these files were successfully restored, demonstrating that the USB drive was used as a storage medium for data stolen from ABC Technologies.

Financial evidence:

A word document password protected has been retrieved from the nokia phone and has been decrypted. It contains all the offshore bank account details. The document links directly Emma to the transaction.

geographic analysis:

[FIG 1]

Owner	Date/Timestamp	Latitude	Longitude	Device Model
Emma Johnson	2024-08-05 05/08/2024 06:41:42(UTC+1)	51,5011	-3,1198	Huawei POT-LX1
Emma Johnson	2024-08-05 05/08/2024 08:19:54(UTC+1)	52,5162	-2,8197	Huawei POT-LX1
Emma Johnson	2024-08-18 18/08/2024 08:01:40(UTC+1)	9,9378718	76,3257527	Huawei POT-LX1
Emma Johnson	2024-08-19 19/08/2024 02:18:27(UTC+1)	10,7378	76,6297	Huawei POT-LX1
Emma Johnson	2024-08-19 19/08/2024 04:12:30(UTC+1)	11,0148	77,1882	Huawei POT-LX1
Emma Johnson	2024-08-19 19/08/2024 04:12:35(UTC+1)	11,0148	77,1882	Huawei POT-LX1
Emma Johnson	2024-08-19 19/08/2024 04:22:32(UTC+1)	10,9959	77,2811	Huawei POT-LX1
Emma Johnson	2024-08-19 19/08/2024 04:33:49(UTC+1)	10,9798	77,3369	Huawei POT-LX1
Emma Johnson	2024-08-19 19/08/2024 07:17:58(UTC+1)	10,8705	78,6382	Huawei POT-LX1
Emma Johnson	2024-08-19 19/08/2024 07:25:38(UTC+1)	10,839	78,6856	Huawei POT-LX1
Emma Johnson	2024-08-19 19/08/2024 07:27:25(UTC+1)	10,8354	78,6897	Huawei POT-LX1

Emma Johnson	2024-08-19 19/08/2024 07:29:51(UTC+1)	10,836	78,6996	Huawei POT-LX1
Emma Johnson	2024-08-19 19/08/2024 07:30:50(UTC+1)	10,8361	78,7	Huawei POT-LX1
Emma Johnson	2024-08-19 19/08/2024 07:35:42(UTC+1)	10,8487	78,7132	Huawei POT-LX1
Emma Johnson	2024-08-21 21/08/2024 11:02:52(UTC+1)	10,6015	76,5438	Huawei POT-LX1
Emma Johnson	2024-08-21 21/08/2024 11:15:12(UTC+1)	10,5734	76,5755	Huawei POT-LX1
Emma Johnson	2024-08-21 21/08/2024 11:19:26(UTC+1)	10,563	76,5815	Huawei POT-LX1
Emma Johnson	2024-08-23 23/08/2024 01:41:15(UTC+1)	10,5727	76,3867	Huawei POT-LX1
Emma Johnson	2024-08-26 26/08/2024 02:56:02(UTC+1)	9,7942	76,5791	Huawei POT-LX1
Emma Johnson	2024-08-26 26/08/2024 02:57:32(UTC+1)	9,7942	76,5791	Huawei POT-LX1
Emma Johnson	2024-08-26 26/08/2024 02:58:01(UTC+1)	9,7942	76,5791	Huawei POT-LX1
Emma Johnson	2024-08-26 26/08/2024 03:00:07(UTC+1)	9,7942	76,5791	Huawei POT-LX1
Emma Johnson	2024-11-22 22/11/2024 16:31:48(UTC+0)	25,2706	51,5431	Huawei POT-LX1
Emma Johnson	2024-11-22 22/11/2024 16:33:53(UTC+0)	25,2724	51,5448	Huawei POT-LX1
Emma Johnson	2024-11-22 22/11/2024 16:35:02(UTC+0)	25,276	51,5398	Huawei POT-LX1
Emma Johnson	2024-11-23 23/11/2024 08:50:10(UTC+0)	25,2826	51,5394	Huawei POT-LX1
Emma Johnson	2024-11-23 23/11/2024 08:55:17(UTC+0)	25,2752	51,5144	Huawei POT-LX1

Those information shows Emma's phone movement: She went from the UK to Qatar to India. The dates and destination are corelated to the date of the sale, showing she probably met the potential buyer.

Calls analysis:

Device	Type	Direction	Date	Time	Party	Duration	Correlation Note
Emma Johnson (Huawei)	Call Log	Outgoing	2024-08-02 21:38:33	02/08/2024 21:38:33(UTC+1)	To: 07917162891 SA No. .	00:00:00	SUSPICIOUS: Frequent private contact
Emma Johnson (Huawei)	Call Log	Outgoing	2024-08-02 21:39:24	02/08/2024 21:39:24(UTC+1)	To: 07917162891 SA No. .	00:00:00	SUSPICIOUS: Frequent private contact

Emma Johnson (Huawei)	Call Log	Outgoing	2024-08-10 05:55:58	10/08/2024 05:55:58(UTC+1)	To: 00917907025586	00:00:00	
Emma Johnson (Huawei)	Call Log	Outgoing	2024-08-13 12:52:21	13/08/2024 12:52:21(UTC+1)	To: 07917162891 SA No. .	00:00:00	SUSPICIOUS: Frequent private contact
Emma Johnson (Huawei)	Call Log	Outgoing	2024-08-13 12:52:54	13/08/2024 12:52:54(UTC+1)	To: 00447917162891 SA No. .	00:00:00	
Emma Johnson (Huawei)	Call Log	Incoming	2024-08-17 06:16:12	17/08/2024 06:16:12(UTC+1)	From: +447917162891 SA No. .	00:00:00	
Emma Johnson (Huawei)	Call Log	Outgoing	2024-08-17 06:20:34	17/08/2024 06:20:34(UTC+1)	To: +447917162891 SA No. .	00:00:00	
Emma Johnson (Huawei)	Call Log	Outgoing	2024-08-18 07:57:13	18/08/2024 07:57:13(UTC+1)	To: 07917162891 SA No. .	00:00:00	SUSPICIOUS: Frequent private contact
Emma Johnson (Huawei)	Call Log	Outgoing	2024-08-18 07:57:34	18/08/2024 07:57:34(UTC+1)	To: 07917162891 SA No. .	00:00:00	SUSPICIOUS: Frequent private contact
Emma Johnson (Huawei)	Call Log	Outgoing	2024-08-18 07:58:01	18/08/2024 07:58:01(UTC+1)	To: 0447917162891 SA No. .	00:00:00	
Emma Johnson (Huawei)	Call Log	Outgoing	2024-08-18 10:04:01	18/08/2024 10:04:01(UTC+1)	To: 0447917162891 SA No. .	00:00:00	
Emma Johnson (Huawei)	Call Log	Outgoing	2024-08-18 10:04:27	18/08/2024 10:04:27(UTC+1)	To: 0447917162891 SA No. .	00:00:00	
Emma Johnson (Huawei)	Call Log	Outgoing	2024-08-19 10:23:15	19/08/2024 10:23:15(UTC+1)	To: 0447917162891 SA No. .	00:00:00	
Emma Johnson (Huawei)	Call Log	Outgoing	2024-08-19 10:25:34	19/08/2024 10:25:34(UTC+1)	To: 00917907025586	00:00:00	
Emma Johnson (Huawei)	Call Log	Outgoing	2024-08-19 10:25:38	19/08/2024 10:25:38(UTC+1)	To: 00917907025586	00:00:00	

This table shows the phone calls from Emma's phone, I couldn't figure out who she did call, but regarding to the dates those phone calls have been emitted, those phone calls are corelated to the conversations exchanged between Emma, Joe and Norman but

also calls that could be related to a potential buyer in India, regarding the country code +91 of some phone calls.

Suspect profiling:

- Emma Jonhson: The main suspect, engineer having the required access right to access and copy the data of the project and identified by her bank account for the transaction at Caiman's Islands.
- Joe Marsh: The broker, He found potentials buyers and organized the transfer of the stolen data.
- Norman Smith: The buyer, he represents NextGen circuit (NSI) identified by messenger.
- Another name appeared in the evidence: Vanessa, she is the director of the R and D at nexgen circuit

Conclusion:

This investigation has proven, mainly through the usb key, the messenger and WhatsApp conversations, and the protected word document, that a data theft has been committed, involving at least 3 people (based on the findings). The conversations prove that the data has been stolen, the research of a potential buyer by Emma and Joe. the usb key give a hint on how Emma probably stole the data of the project patent, and the protected word document give all the details required to identify and find the bank account that received the money.

Recommendations:

The next step would be suing Emma Jonhson, Joe Marsh and Norman Smith for patent protected data theft and illegal sale immediately. To recover and confiscate the money used within the transaction. The next step for Quantum tech would be to perform a complete risk management and security audit, in order to find solutions for securing the sensitive data, like quantum-based encryption, and quantum insensitive data encryption, using solutions like CRYSTALS-Kyber or CRYSTAL- Dilithium.

Technical support:

This section summarizes the technical support used to investigate. Massive use of ai agent has been used to perform script writing, faster analysis.

Context Analysis

- OCR extraction of assessment PDF
- Identification of targets:
 - Emma Johnson (Huawei POT-LX1, USB)
 - Joe Marsh (Samsung Galaxy A13)
 - Norman Smith (Note 14)
 - Vanessa (NexGen Circuits)

Communication Extraction & Processing

- Python environment:
 - python3
 - openpyxl (Excel parsing)
- Input files:
 - instant_messages_log.xlsx
 - email_log.xlsx
- Data normalization fields:
 - Source
 - Platform
 - Date
 - Sender
 - Receiver
 - Message
- Keyword filtering:

```
grep -iE
```

```
"5M|offshore|patent|blueprint|sample|Emma|Joe|Norman|Vanessa|ghost|Q  
T-AI" all_conversations.csv
```

- Output generation:
 - Forensic_Comms_Analysis.xlsx
- Alias mapping:
 - "Peter Dover" → Emma Johnson

Geolocation & Mobility Analysis

- Data extraction:
 - GPS coordinates (Latitude / Longitude)

- Timestamps
- Source files:
 - filesystem_X.xlsx
 - Sheets: Timeline, Image: Location
- Python processing
- Map generation:
 - JavaScript library: Leaflet.js
- Output:
 - Forensic_Locations_Map.html
- Visualization:
 - Color-coded per suspect

USB Drive Analysis

- Tool:
 - Autopsy
- Input artifacts:
 - Metadata.csv
 - Keyword Hits
- Indicators:
 - Deleted files
 - Unallocated space
 - File carving traces

Encrypted Document Decryption (Open.docx)

- Hash extraction:
 - Office 2013 format
- Tool:
 - Hashcat
- Mode:
 - -m 9600 (Office 2013)
- Attack strategy:
 - Custom wordlist (case intelligence)
 - Rule: best64
 - Mask: 4-digit numeric
- Password recovered:
 - Neuro2023
- Archive extraction:

7z x Open.7z

- Document decryption:

msoffcrypto-tool Open.docx decrypted.docx

Advanced USB Analysis

- File carving validation
- Recovery of deleted archives (.zip, .tar.gz)
- Technical asset identification:
 - Firmware
 - Source code
 - Deployment packages

Vanessa Link Analysis

- Cross-referencing communications
- Correlation with external entity:
 - NexGen Circuits

Extended Intelligence Correlation

- Roaming data analysis:
 - India (Aug 2024)
 - Gulf region (Qatar, Oman, UAE)
 - South Africa (Nov-Dec 2024)
- System artifact inspection:
 - eventinfo-hms.zip
- Timestamp correlation:
 - 31/01/2025 10:20 UTC
- Audio evidence inventory:
 - Formats: AAC / M4A
 - Devices: Joe Marsh, Norman Smith

Location Intelligence Interpretation

- Python geospatial processing
- Map correction:
 - Tile rendering fix (CartoDB)
- Output:
 - Analyse_Geographique.md
- Correlation points:
 - India → initial exfiltration offer
 - Qatar → final negotiation phase
 - UK (Manchester) → intermediary movements

Fig 1:
map of Emma's phone locations

