

Digital Forensics Analysis

Research, Analyze and Investigate Cybersecurity incidents
and perform digital forensic assessment

Task 2 – By Mehdi BIZET

Summary:

1. Case background

2. Evidence Inventory

3. Methodology

4. Findings

5. Suspect Profiles

6. Conclusions

7. Recommendations

1. Case Background

Quantum Tech's IT security team detected unauthorized access to their proprietary patent database, specifically the AI chip design patent (ID: QT-AI-2025). Initial findings point to Emma, a senior engineer, joined recently at Quantum Tech's as the primary suspect. The company suspects Emma attempted to steal and sell these patents to a competitor, NexGen Circuits, through an intermediary, Joe.

2. Evidence Inventory

Owner	Device Info	
Emma Johnson	Name	Huawei POT-LX1 P Smart
	Image Size	15.0 GB
	Extraction Method	File System [Android ADB]
	Extraction Time	28/10/2025; 16:12:56 - 16:53:34
	Cable Used	Cable No.100
	Acquisition Computer	UOW3609
	Unit ID	1136568878
	UFED Version	7.73.0.162
	SHA-256 Hash	D5193DBF8246C09FDDE73BE855834398 5AB24A2E1C142E4D64E16E2B6507E31F
	Name	General UDisk
	Image Size	16 GB
	Acquisition Tool	FTK Imager
	Extraction Time	12/03/2026; 15:41:12 - 15:58:32
	Format	E01 (10 segments: E01 - E10)
	MD5 Hash	41a6d1cdaf265bbf4e531698e89b0e44
Norman Smith	Name	Nokia C2 2nd Edition
	Image Size	94 MB
	Extraction Method	File System [Android Backup]
	Extraction Time	28/10/2025; 16:01:06 - 16:03:26
	Cable Used	Cable No. 100 or 170
	Acquisition Computer	UOW3609
	Unit ID	1136568878
	UFED Version	7.73.0.162
	SHA-256 Hash	A693656C260E339069756BE8005346E97 033D0CCF2F79ADD56CD69C9EADE13AB

Joe Marsh	Name	Samsung SM-A137F Galaxy A13
	Extraction Method	File System [Android Backup]
	Extraction Time	28/10/2025; 11:57:02 - 12:36:47
	Cable Used	Cable No. 170 or Original Cable
	Acquisition Computer	UOW3609
	Unit ID	1136568878
	UFED Version	7.73.0.162
	SHA-256 Hash	0E585C4FE8160254253BE515A16FF94B 7FDF88B248B67D45CFDEF8753A9A3195
Vanessa	Name	Detected Model (Note 14)
	Extraction Method	File System [Android Backup]
	Extraction Time	28/10/2025; 11:25:18 - 11:27:40
	Cable Used	Cable No. 100 or 170
	Acquisition Computer	UOW3609
	Unit ID	1136568878
	UFED Version	7.73.0.162
	SHA-256 Hash	630724E2F8863ADB9C4F7DF1AB645E56 C19A832D546FE7AB55B0CEBF8EA7BEFD

3. Methodology

Here are the tools used for acquisition and analysis:

Operating System

- Windows 10 (Version 22H2)

Smartphone Analysis

- Cellebrite Physical Analyser 7.72.0.10

USB Key Analysis

- Autopsy 4.22.1

Archive Tool

- 7-Zip

Document

- Microsoft Word

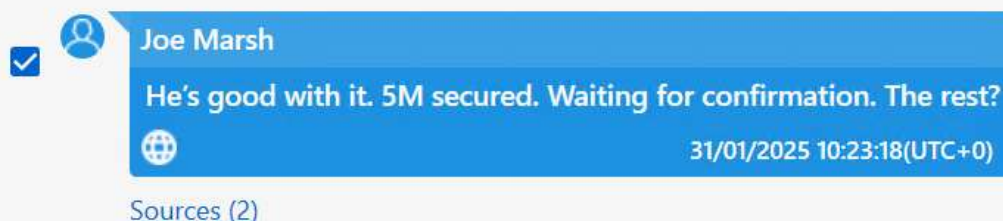
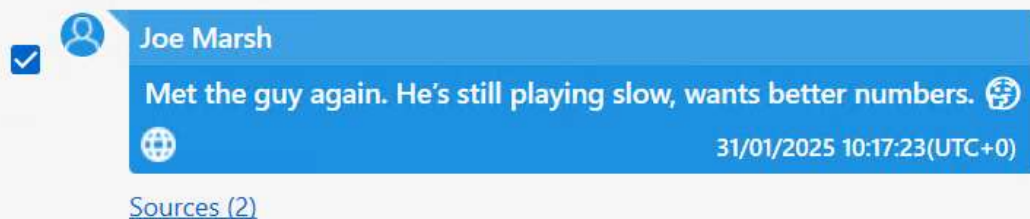
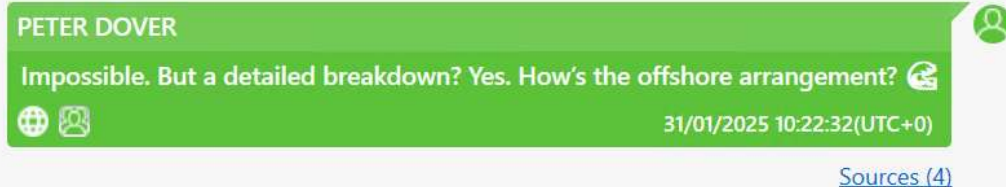
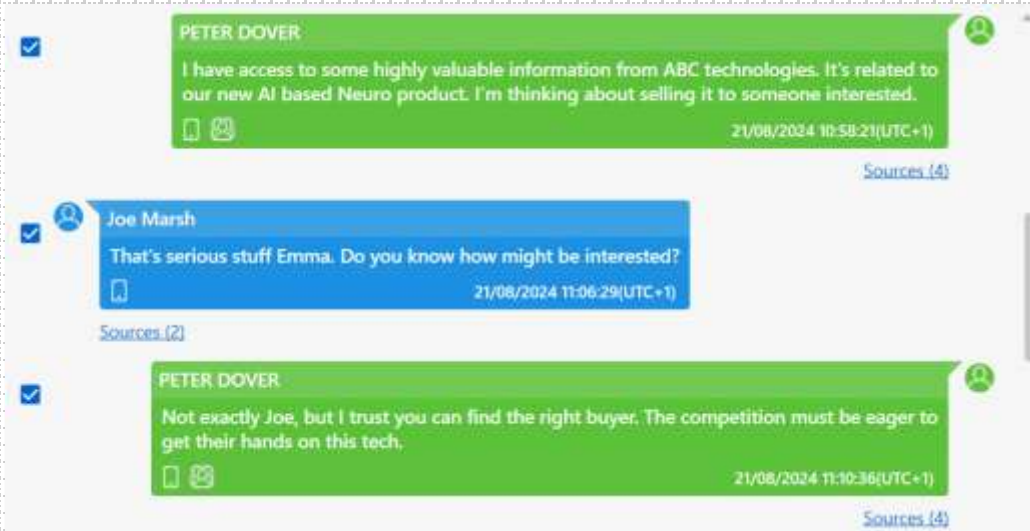
Password Cracking

- Hashcat

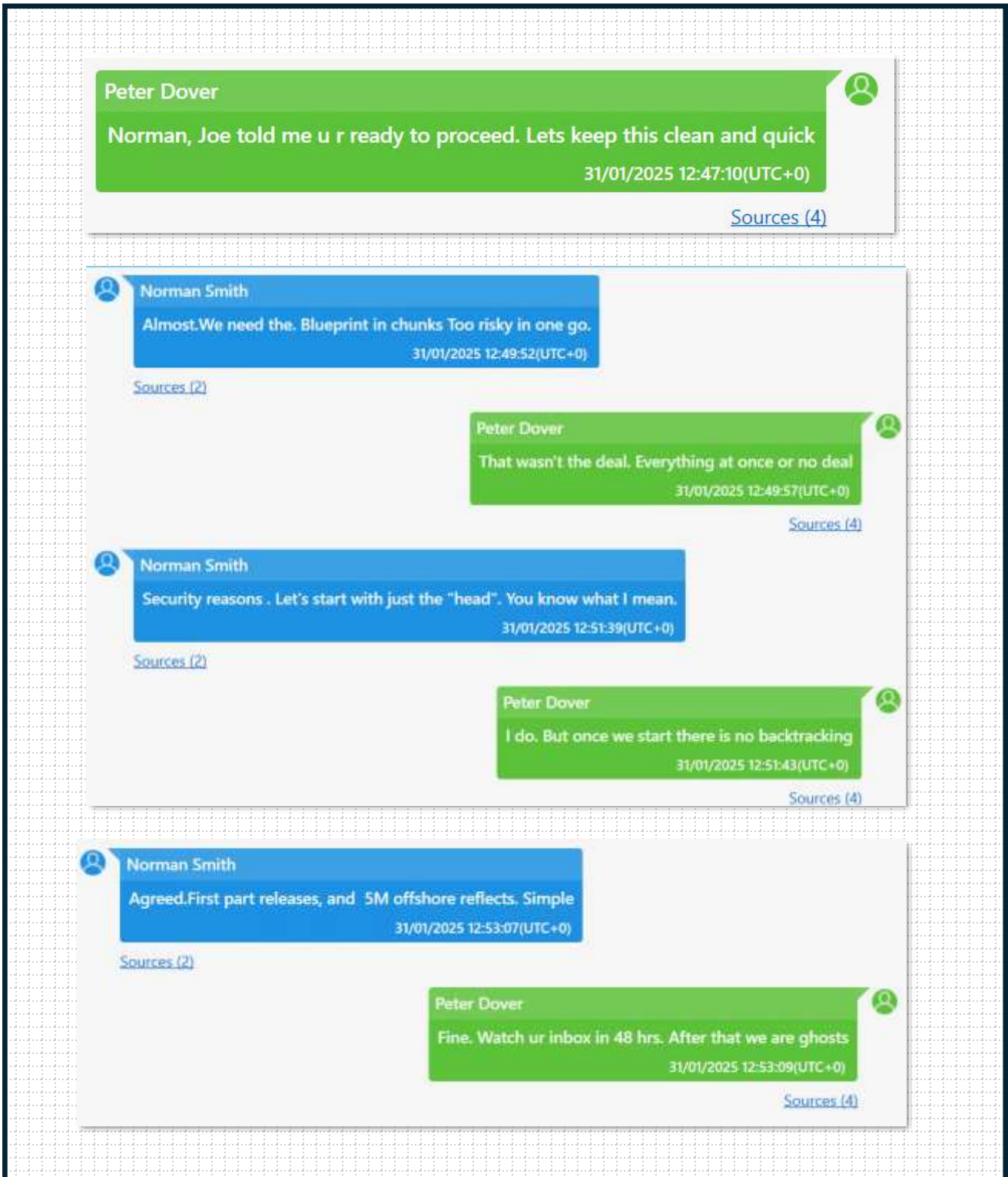
4. Finding

Huawei POT-LX1 P Smart

Between January 31st, 2024, and August 21st, 2024, Emma Johnson (alias Peter Dover) initiate the discussion to Joe Marsh about the detention of “highly valuable information”, and want that Joe search someone interested in this information:



On January 31st, 2025, Emma Johnson (alias Peter Dover) contacted Norman Smith through Facebook to proceed to the transaction:

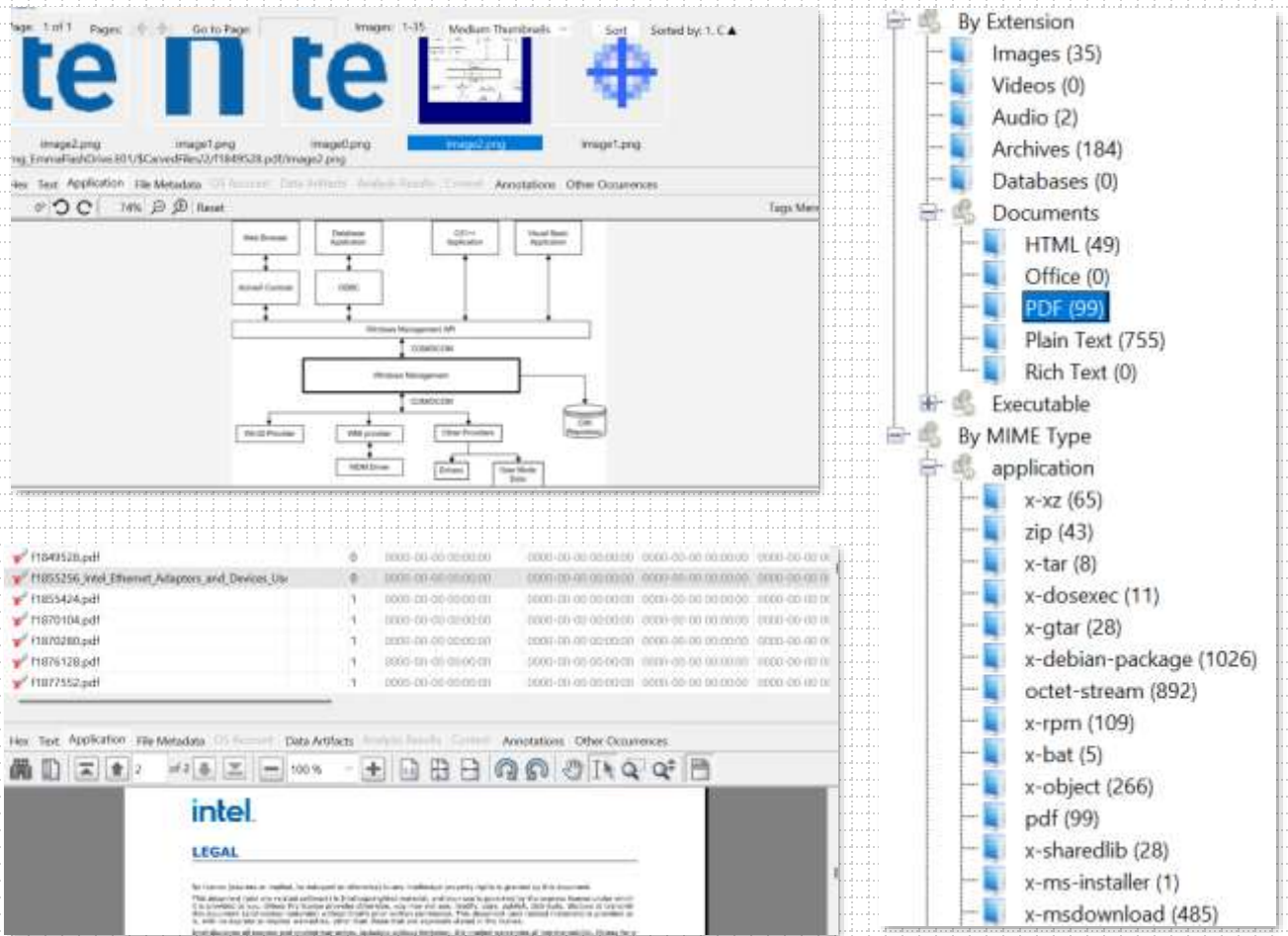


The screenshot shows a Facebook chat interface with a light gray background. The chat is between Peter Dover (green bubbles) and Norman Smith (blue bubbles). The messages are as follows:

- 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)
[Sources \(4\)](#)
- Norman Smith:** Almost.We need the. Blueprint in chunks Too risky in one go.
31/01/2025 12:49:52(UTC+0)
[Sources \(2\)](#)
- Peter Dover:** That wasn't the deal. Everything at once or no deal
31/01/2025 12:49:57(UTC+0)
[Sources \(4\)](#)
- Norman Smith:** Security reasons . Let's start with just the "head" . You know what I mean.
31/01/2025 12:51:39(UTC+0)
[Sources \(2\)](#)
- Peter Dover:** I do. But once we start there is no backtracking
31/01/2025 12:51:43(UTC+0)
[Sources \(4\)](#)
- 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 \(4\)](#)

Emma USB Drive

The carved files analysis from Autopsy Identified 4109 files across 3 allocation units and 969 Orphan Files. Even if there is no direct mention of QT-AI patent document, there are still Intel network card drivers, technical documentation, and diverse stored in the USB Key.



The screenshot displays the Autopsy digital forensics interface. The main window shows a file list with columns for file name, size, and date. The file list includes:

File Name	Size	Date
image2.png	1049528	2000-01-01 00:00:00
image1.png	1049528	2000-01-01 00:00:00
image0.png	1049528	2000-01-01 00:00:00
image3.png	1049528	2000-01-01 00:00:00
image4.png	1049528	2000-01-01 00:00:00

The right sidebar shows a summary of files by extension and MIME type:

- By Extension**
 - Images (35)
 - Videos (0)
 - Audio (2)
 - Archives (184)
 - Databases (0)
 - Documents
 - HTML (49)
 - Office (0)
 - PDF (99)
 - Plain Text (755)
 - Rich Text (0)
 - Executable
- By MIME Type**
 - application
 - x-xz (65)
 - zip (43)
 - x-tar (8)
 - x-dosexec (11)
 - x-gtar (28)
 - x-debian-package (1026)
 - octet-stream (892)
 - x-rpm (109)
 - x-bat (5)
 - x-object (266)
 - pdf (99)
 - x-sharedlib (28)
 - x-ms-installer (1)
 - x-msdownload (485)

The bottom window shows the Intel logo and the word "LEGAL" in a document viewer.

Nokia C2 2nd Edition

Norman Smith has the offshore bank account details via an encrypted Microsoft office document, proving Emma's real identity, and shows the offshore payment mechanism from the patent sale.

The Encrypted Microsoft office password has been found by extracting the hash of the encryption and has been cracked with Hashcat through a dictionary attack.

The result of the dictionary attack is "Neuro2023".

Offshore Bank Details
Bank Name: Global Offshore Bank & Trust
Account Holder Name: Emma Johnson
Account Number: 9876543210
IBAN (International Bank Account Number): GB29NWBK60161331926819
SWIFT/BIC Code: NWBKGB2L
Bank Address: Global Offshore Bank & Trust 15 Ocean View Drive George Town, Grand Cayman Cayman Islands
Currency: USD (US Dollars)
Account Type: Private Offshore Savings Account
Beneficiary Contact Information: Email: emma.johnson@securemail.com Phone: +1-345-123-4567
Additional Notes: - The account is linked to a trust named "NeuroTech Trust 2023". - A minimum balance of \$500,000 must be maintained to avoid fees. - Wire transfers are processed within 1-2 business days.

Galaxy A13 and Huawei:

There is a correlation between the GPS Extracted Data of the Huawei smartphone belonging to Emma and the Galaxy A13 belonging to Joe that they were both in Wales.

- Joe being at Cardiff (51.479°N, -3.174°W) on Aug 26, 2024, 11:20-15:00
- Emma being at Cardiff (51.479°N, -3.174°W) on Nov 16, 2024, 17:34

Timeline of Events:

Date	Event
August 21 st 2024	Emma initiates the conversation with Joe about selling information.
August 22 nd 2024	Joe shares location and begins contacting buyers
August 26 th 2024	Joe stating he is “meeting contacts for a meeting today”
	Joe GPS Location in Cardiff, Wales
August 29 th 2024	Joe flying to Glasgow to meet contact
October 14 th 2024	Joe traveling to Paris for “good deals”
November 16 th 2024	Emma’s GPS Location in Cardiff, Wales to meet Norman
November 20 th 2024	Emma writing “I have managed to find someone with whom I am meeting over the next weeks”
	Joe saying he’s “Meeting the client this week at Manchester”
January 31 st 2025	Day of the final negotiations with \$5M offshore, confirmed on Facebook with Norman and Emma stating “After that we are ghosts”

5. Suspect roles:

Name	Info	
Emma Johnson	Device	Huawei
	Email	emma.johnson@securemail.com
	Offshore Account	Global Offshore Bank & Trust (Cayman Islands)
	Trust	NeuroTech Trust 2023
	Role	Senior engineer at Quantum Tech
	Evidence	WhatsApp messages by initiating the plot and negotiating terms
	Motivation	Financial gain (\$5M offshore)
Norman Smith	Device	Nokia C2
	Role	Buyer
	Evidence	Encrypted document
	Motivation	Obtain competitive AI technology

Joe Marsh	Device	Galaxy A13
	Role	Intermediary
	Evidence	Payment agreement on facebook
	Motivation	Financial gain (Commission from sale)
Vanessa	Device	Note 14
	Role	R&D Director of NexGen Circuits and suspected buyer

6. Conclusion:

Emma Johnson (alias Peter Dover) initiated the theft of Quantum Tech's proprietary AI chip patent QT-AI-2025. To sell the patent, Emma contacted Joe Marsh as an intermediary to arrange meetings with buyers. Then, Norman Smith agreed to purchase the stolen patent for \$5M offshore arrangement.

7. Recommendations:

First, Quantum Tech can process Emma's employment termination with possible civil recovery damage caused by Emma. Quantum Tech should reinforce anti-espionage measures to avoid the reproduction of the problem.

From these events, probable charges would be Corporate Espionage from the UK Computer Misuse Act, Theft of Trade Secrets, Conspiracy to Commit Fraud, Breach of Confidence, and Money Laundering.