DIGITAL FORENSIC INVESTIGATION REPORT

Case: QT-AI-2025 | Quantum Tech | Confidential

Field	Details
Organisation	Quantum Tech
Case	Unauthorised access to patent database (QT-AI-2025)
Report Date	May 2026
Classification	CONFIDENTIAL
Prepared By	Orneda Kamberi
Tools Used	Cellebrite UFED, FTK Imager, Autopsy
Devices Examined	4 Smartphones + 1 USB Flash Drive

1. Case Background

Quantum Tech's IT security team noticed that someone had accessed their patent database without permission. The patent that was accessed is called QT-AI-2025, which is an AI chip design and is very important to the company.

The investigation focused on three suspects. Emma (who used the name Peter Dover on her devices) is a senior engineer at Quantum Tech who had access to the patent database. Joe Marsh helped Emma find a buyer for the stolen patent, acting as a middleman. Norman Smith is suspected to be the buyer, working on behalf of NexGen Circuits, as stated in the case briefing. This was not independently confirmed through the digital evidence alone.

Quantum Tech reported the case to the police. The goal of this investigation was to collect and examine digital evidence from all devices that were taken from the suspects, and to produce findings that can be used in court.

2. Evidence Inventory and Chain of Custody

The five devices below were taken from the suspects following the correct evidence handling procedures. Each device was given a reference number and examined using professional forensic tools. All devices were unlocked, as confirmed by Quantum Tech.

Ref.	Device	Suspect	Digital ID	Tool	Format	Hash
E-001	Huawei POT-LX1 P Smart	Emma	Peter Dover / dovp59@gmail.com	Cellebrite UFED	Physical	MD5 + SHA-1
E-002	USB Flash Drive	Emma	N/A	FTK Imager	E01	MD5 + SHA-1
E-003	Samsung SM-A137F Galaxy A13	Joe Marsh	+447476538686	Cellebrite UFED	Physical	MD5 + SHA-1
E-004	Nokia C2 2nd Edition	Norman Smith	FB: 61564326251951	Cellebrite UFED	Logical	MD5 + SHA-1
E-005	Ulephone / Note 14	Joe (secondary)	N/A	Cellebrite UFED	Logical	MD5 + SHA-1

MD5 and SHA-1 hash values were recorded for each forensic image straight after acquisition. The hashes were checked again before analysis. There were no differences, which means none of the evidence was changed or tampered with.

3. Methodology

3.1 Acquisition

- Smartphones (E-001, E-003, E-004, E-005): Forensic images of the four devices were created by four separate groups during laboratory work at UWTSD (University of Wales

Trinity Saint David). Each group used Cellebrite UFED to perform a full physical extraction of their assigned device, capturing all data including deleted files and app data. Each phone was put into Airplane Mode before extraction to prevent remote wiping. The images were transmitted to the investigator one week later on 19/03/2026 for analysis.

- USB Flash Drive (E-002): The drive was connected using a hardware write-blocker to make sure nothing could be changed on it. FTK Imager was used to create a forensic image in E01 format. Hash verification (MD5 and SHA-1) was done before and after acquisition. This image was also transmitted on 19/03/2026 together with the smartphone images.

3.2 Analysis

- Three main tools were used in this investigation. Cellebrite UFED was used to acquire the smartphone images and generate extraction reports. FTK Imager was used to create the forensic image of the USB drive. Autopsy 4 was used to analyse all five images, it was used for keyword searches, communication analysis, file carving, and metadata extraction.
- Keywords used in the search included: QT-AI-2025, NexGen, patent, blueprint, offshore, deal, buyer, sell, transfer.
- Messages from WhatsApp, Facebook Messenger, Instagram DMs, and Gmail were extracted and compared across all devices.
- GPS data from photos and apps was used to track where each suspect was during the investigation period.

4. Findings

4.1 Emma's Android Smartphone : E-001 (Huawei POT-LX1 P Smart)

4.1.1 Device Details

Field	Detail
Device	Huawei POT-LX1 P Smart
Owner	Peter Dover (Emma's alias)
Email	dovp59@gmail.com
WhatsApp	+447917162788
Facebook ID	61565261156720
Instagram	peterdover2 (ID: 68515482744)
Extraction	Full Physical Cellebrite UFED
Total Artefacts	2,286

4.1.2 WhatsApp Messages : Emma and Joe Marsh

A series of important WhatsApp messages were found between Emma and Joe Marsh starting on 21 August 2024. These messages clearly show that Emma wanted to sell Quantum Tech's patent.

#	Date & Time (UTC)	From	Message
625	21/08/2024 07:27	Emma → Joe	Hey Joe. I need your help with something sensitive. Do you have time to talk?
626	21/08/2024 08:14	Joe → Emma	Yes I am available. What's going on?
627	**21/08/2024 09:58**	**Emma → Joe**	**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.**
630	**21/08/2024 10:10**	**Emma → Joe**	**Not exactly Joe, but I trust you can find the right buyer. The competition must be eager to get their hands on this tech.**
633	21/08/2024 11:13	Joe → Emma	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.
634	**21/08/2024 11:47**	**Emma → Joe**	**Perfect. Let's keep this under wraps. This could be huge for both of us.**
1088	**14/10/2024 18:57**	**Joe → Emma**	**Hi there, travelling back to France this time Paris to get some good deals. Will update you once a deal is nearer.**

4.1.3 Instagram Direct Messages

Instagram DMs were also recovered from Emma's device (direct.db database). Three accounts were identified: peterdover2 (Emma), hamster.184397 (Joe Marsh), and normansmith1987 (Norman Smith). On 09 September 2024, Joe sent Emma the following message:

Joe Marsh (09/09/2024 15:57 UTC): "I found someone in NSI compa. He is interested. He needs to know the level of information you would be willing to share."

This message shows that Joe found a buyer (Norman/NexGen) after his trip to Lyon, France. A separate Instagram thread (threads:29) also exists between Emma and Norman, showing they communicated directly on Instagram as well as Facebook.

4.1.4 Facebook Messenger: Emma and Norman Smith

On 31 January 2025, a conversation between Emma and Norman Smith was found on Facebook Messenger. This is the most important evidence in the case because it shows the final agreement, including the price and how the payment would be made.

#	Date & Time (UTC)	From	Message
1898	31/01/2025 12:47	Emma → Norman	Lets keep this clean and quick
1900	31/01/2025 12:49	Norman → Emma	Almost. We need the Blueprint in chunks. Too risky in one go.
1901	**31/01/2025 12:49**	**Emma → Norman**	**That wasn't the deal. Everything at once or no deal**

#	Date & Time (UTC)	From	Message
1902	31/01/2025 12:51	Norman → Emma	Security reasons. Let's start with just the 'head'. You know what I mean.
1904	**31/01/2025 12:53**	**Norman → Emma**	**Agreed. First part releases, and 5M offshore reflects. Simple**
1905	**31/01/2025 12:53**	**Emma → Norman**	**Fine. Watch ur inbox in 48 hrs. After that we are ghosts**

KEY FINDING: Emma and Norman agreed to sell the patent for $5,000,000, to be sent to an offshore bank account. Emma said she would deliver the files within 48 hours, and both agreed to disappear after.

4.1.5 Call Logs

Emma's call logs show multiple calls to Joe Marsh's number (+447917162891) between August and September 2024. These calls match the timeline of the WhatsApp messages and confirm that Emma and Joe were in regular contact.

4.1.6 Location Data

GPS data from Emma's photos shows she was in Kerala, India (coordinates 10.60, 76.54) from 18 to 21 August 2024. This is exactly when she sent the first WhatsApp messages to Joe about the patent sale.

4.1.7 Browser Search Cache

A Chrome browser cache file (10.jpeg) was found on Emma's phone. It shows a Google search for 'How to unblock a contact on WhatsApp', done at 04:59 UTC on 21 August 2024, exactly 2 hours and 28 minutes before Emma first messaged Joe. This strongly suggests Emma unblocked Joe's number just before starting the plan.

KEY FINDING: Emma searched how to unblock Joe on WhatsApp at 04:59 UTC, then messaged him 2 hours and 28 minutes later at 07:27 UTC. This shows the contact was planned in advance.

4.2 Emma's USB Flash Drive : E-002

FTK Imager was used to create a forensic image (img_EmmaFlashDrive.E01) of Emma's USB drive. All files were found in unallocated space, which means Emma deleted them before the drive was taken. However, Autopsy was able to recover them through file carving.

The recovered files are mostly Linux software packages created on 09 April 2025. Together, they show the USB drive was set up as a Kali Linux bootable drive, a tool used for hacking and security testing. The key packages found include:

File	Type	Purpose
cryptsetup (x4 packages)	.deb	LUKS disk encryption - hides stolen files
isc-dhcp-client	.udeb	Gets a network IP - needed for iSCSI connection

File	Type	Purpose
libgcrypt20	.udeb	Cryptography library
mdadm	.deb	Disk management
partman-auto +kali1	.udeb	Kali Linux disk partitioning - confirms Kali OS
NTFS_X64.EFI / NTFS_ARM.EFI	.EFI	Lets Kali read Windows hard drives
EXFAT_~3.EFI	.EFI	Reads ExFAT drives
APT_29~1.DEB (note: the name resembles a known advanced threat group, but the file contents were not analysed - no direct link has been established)	.deb	Suspicious - name matches known hacking group APT-29
H^^H^^tj.h^t	unknown	Obfuscated file - name hidden using control characters

KEY FINDING: Emma's USB was a Kali Linux bootable drive, which may have been used for data exfiltration. The isc-dhcp-client package suggests network connectivity was planned, possibly to support iSCSI remote storage access, however, no iSCSI configuration or server IP was recovered to confirm this. The cryptsetup packages suggest files may have been encrypted during transfer. All files were deleted before seizure, suggesting Emma tried to hide the contents of the drive.

4.3 Joe Marsh's Smartphone : E-003 (Samsung SM-A137F Galaxy A13)

4.3.1 Location Evidence : Travel to France

GPS data from photos on Joe's Samsung phone confirm he travelled to several European cities. The GPS coordinates for 15-18 October 2024 place Joe in central Paris, which matches his WhatsApp message to Emma. It is likely that Joe met with a buyer contact during this trip, but no direct evidence was found confirming exactly who he met or whether Emma was also present.

Date	Location	Significance
06/08/2024	East London, UK	Joe's home base
18-22/08/2024	Hannover, Germany	International travel, possible buyer meetings
03-07/09/2024	Lyon, France	After this trip, Joe messaged Emma on Instagram about finding buyer
15-18/10/2024	Paris, France	Paris trip confirmed by GPS. Joe stated he was going to Paris for “good deals” (WhatsApp 14/10/2024). It is likely buyer meetings took place here, but no direct evidence confirms who Joe met.
18/10/2024	CDG Airport, Paris	Departure from Paris

4.3.2 Credit Card Photos : Ulephone (E-005)

Two WhatsApp images were found on the Ulephone device showing both sides of a State Bank of India MasterCard debit card. The card number (5196 1901 6355), expiry date (12/33), and CVV area are all visible. The images were sent via WhatsApp on 09/08/2023 (MD5:

6091f2db5e36b1daa82caf25f15e6198). This is a possible case of financial fraud or identity theft, separate from the patent case.

4.4 Norman Smith's Smartphone : E-004 (Nokia C2 2nd Edition)

4.4.1 Location Evidence

GPS data from Norman's Nokia phone shows he was in Addis Ababa, Ethiopia in early August 2024, and Botswana in mid-August 2024. On 04 September 2024, his phone was located in Wales, UK (51.625, -3.996), the same area as Joe Marsh on the same day. This suggests a possible face-to-face meeting between the two, though this is not directly confirmed by the digital evidence.

4.4.2 Encrypted Archive : Open.7z

A password-protected 7-Zip archive called Open.7z was found in Norman's WhatsApp Documents folder. It was last modified at 10:33:34 UTC on 31 January 2025, exactly 2 hours and 14 minutes before Emma and Norman agreed the $5M deal on Facebook Messenger.

The archive was cracked using Hashcat (Mode 9600, hybrid attack). The password was 'Neuro2023' the same word used by Emma to describe the AI product. Inside was a Word document with Emma's offshore bank account details:

Field	Detail
Bank	Global Offshore Bank & Trust, Grand Cayman, Cayman Islands
Account Holder	Emma Johnson
IBAN	GB29NWBK60161331926819
SWIFT	NWKBGB2L
Trust Name	NeuroTech Trust 2023, matches 'AI Neuro product' in WhatsApp
Currency	USD : Private Offshore Savings Account (min. $500,000)
File MD5	d0232de04bf501132db512419757051a

KEY FINDING: Emma prepared her offshore bank account details in advance and sent them to Norman 2 hours before they agreed the deal. The trust name 'NeuroTech Trust 2023' links directly to the patent. This shows the money laundering was planned from the start.

5. Timeline of Events

Date & Time	What Happened	Evidence
09/08/2023	Credit card images sent via WhatsApp (Ulephone)	E-005
02/08/2024	Emma gets new SIM card and calls Joe	E-001 call logs
21/08/2024 04:59	Emma Googles how to unblock WhatsApp contact	E-001 Chrome cache

Date & Time	What Happened	Evidence
21/08/2024 07:27	Emma messages Joe: 'I need your help with something sensitive'	E-001 WhatsApp
21/08/2024 09:58	Emma tells Joe about the patent and offers to sell it	E-001 WhatsApp
21/08/2024 11:47	Emma: 'Let's keep this under wraps'	E-001 WhatsApp
03-07/09/2024	Joe travels to Lyon, France	E-003 GPS
04/09/2024	Norman in Wales, UK, likely meets Joe in person	E-004 GPS
09/09/2024 15:57	Joe messages Emma on Instagram: 'I found someone in NSI compa'	E-001 Instagram
14/10/2024	Joe confirmed in Paris by GPS (48.86-48.88, 2.29-2.36) for 3 days. WhatsApp suggests deal negotiations likely took place. It is not confirmed who he met.	E-001 WhatsApp + E-003 GPS
31/01/2025 10:33	Open.7z (bank details) received by Norman via WhatsApp	E-004 Nokia
31/01/2025 12:53	Emma and Norman agree: $5M offshore, delivery in 48 hours	E-001 Facebook
31/01/2025 12:53	Emma: 'After that we are ghosts'	E-001 Facebook

6. Suspect Roles

Suspect	Role	Key Evidence
Emma (Peter Dover)	Main suspect stole the patent from inside Quantum Tech	WhatsApp msgs, Facebook deal, offshore bank account, Kali Linux USB
Joe Marsh	Middleman found the buyer and set up meetings in Europe	Instagram msg (found contact in NSI company), Paris GPS (Oct 2024 likely buyer meetings), Lyon GPS, WhatsApp msgs
Norman Smith	Buyer agreed to pay $5M and receive the patent	Open.7z, Facebook msgs, Wales GPS (met Joe)

7. Conclusion

The evidence from all five devices shows that Emma, Joe, and Norman planned and carried out the theft of Quantum Tech's AI chip patent QT-AI-2025. The scheme began in August 2024 and a final agreement was reached in January 2025.

Emma used her position as a senior engineer to access and take the patent. Evidence suggests she prepared a Kali Linux USB drive, likely to copy and remove the files without being detected. She also opened an offshore bank account in the Cayman Islands to receive payment. Joe travelled through Europe to find a buyer and acted as the connection between Emma and Norman. Norman agreed to pay $5,000,000 and requested the files to be sent in separate parts.

The evidence was gathered from multiple sources including WhatsApp, Facebook, Instagram, GPS data, browser history, and file analysis. All sources are consistent with each other, which strengthens the overall case and supports the use of this evidence in legal proceedings.

The $5,000,000 offshore payment also suggests money laundering, which should be reported to financial crime authorities separately.

8. Recommendations

8.1 For Law Enforcement

- Charge Emma with corporate espionage, intellectual property theft, and conspiracy.
- Charge Joe Marsh with conspiracy and acting as an accessory.
- Charge Norman Smith with conspiracy to receive stolen property.
- Report the offshore payment plan to financial crime authorities for money laundering investigation.
- Investigate the credit card images found on the Ulephone as a separate fraud case.
- Request a preservation order from Facebook/Meta for the full message history of both accounts.

8.2 For Quantum Tech

- Remove Emma's access to all systems immediately.
- Check the access logs for the patent database to see exactly what was accessed and when.
- Apply for an injunction to stop NexGen Circuits from using any information they may have already received.
- Improve access controls and add Data Loss Prevention tools for staff with access to sensitive patents.

8.3 Further Investigation

- Continue analysing Emma's USB drive to look for the actual patent files in unallocated space.
- Examine the obfuscated files (H^^H^^tj.h^t) and APT_29~1.DEB (note: the name resembles a known advanced threat group, but the file contents were not analysed, no direct link has been established) from the USB drive.
- Recover deleted messages from Norman's Nokia device.
- Analyse Instagram thread:29 between Emma and Norman for additional messages.

Appendix : Key Evidence Summary

ID	Type	Device	Date	What It Shows
WA-001	WhatsApp	E-001	21/08/2024	Emma tells Joe she wants to sell the patent
WA-002	WhatsApp	E-001	21/08/2024	Emma asks Joe to find a buyer

ID	Type	Device	Date	What It Shows
IG-001	Instagram DM	E-001	09/09/2024	Joe tells Emma he found someone at NSI company
FB-001	Facebook	E-001	31/01/2025	Norman asks for patent in parts
FB-002	Facebook	E-001	31/01/2025	$5M offshore payment agreed
FB-003	Facebook	E-001	31/01/2025	Emma confirms delivery and plans to disappear
GPS-001	Location	E-003	15-18/10/2024	Joe confirmed in Paris
GPS-002	Location	E-004	04/09/2024	Norman in Wales, same general area as Joe on the same date
ARCH-001	7z Archive	E-004	31/01/2025	Emma's offshore bank details sent to Norman
FIN-001	WhatsApp Image	E-005	09/08/2023	Full bank card details transmitted
BROWSER-001	Chrome Cache	E-001	21/08/2024	Emma searched how to unblock Joe 2hrs before messaging him

Report prepared by: Orneda Kamberi | Date: April 2026 | Classification: CONFIDENTIAL | Case: QT-AI-2025