

Digital Forensics Investigation Report

Part A - UFED Extraction Demo | Part B - Case Investigation

Quantum Tech Corporate Espionage | Case Ref: QT-CE-2025-001 | Patent: QT-AI-2025

Vaishnavi RiteshKumar Patel

Enrollment: 2503493 | Level 7 | MSc Cyber Security and Digital Forensics

University of Wales Trinity Saint David - London Campus

Presented: April 2026

A personal OnePlus smartphone was acquired using Cellebrite UFED 7.76.0.24 to demonstrate a correct forensic acquisition workflow per ACPO guidance [1].

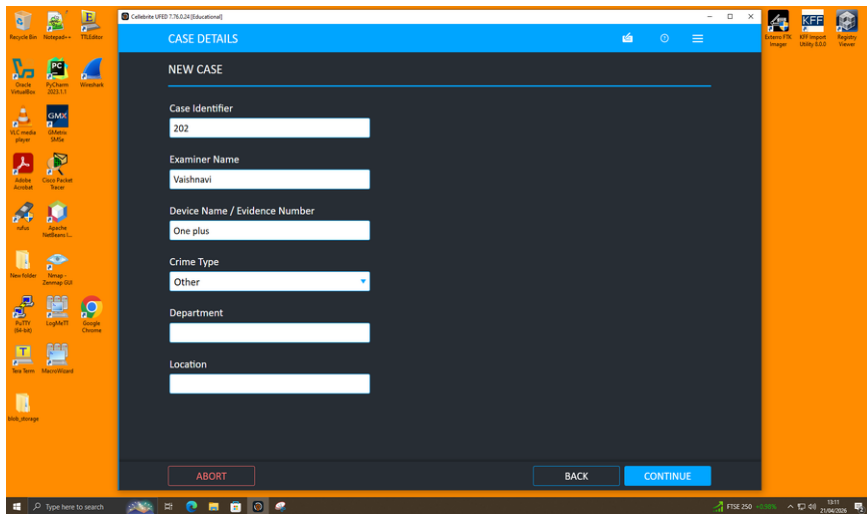


Fig. 1 — New Case created in Cellebrite UFED: Case ID 202, Examiner: Vaishnavi, Device: OnePlus DN2101 (21/04/2026)

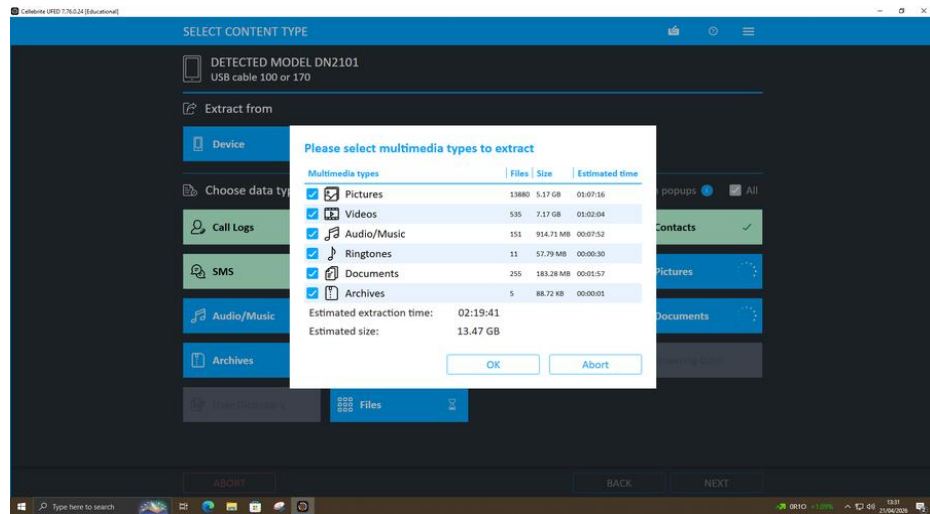


Fig. 2 — Multimedia extraction summary: 13,880 pictures, 535 videos, 255 documents. Total: 13.47 GB. Est. time: 2h 20m.

Extraction type: File System | Device: Android 13, IMEI: 866448051376998 | Destination: E:\New folder (2) | Post-extraction MD5 + SHA-256 hashes recorded for chain of custody

Case Summary

Organisation:	Quantum Tech (AI chip manufacturer)
Incident:	Unauthorised access to patent QT-AI-2025
Breach Detected:	21 August 2024
Primary Suspect:	Emma — Senior Engineer (alias: 'Peter Dover')
Intermediary:	Joe — international broker
Buyer:	Norman Smith (NexGen Circuits)
Deal Value:	\$5 Million USD — offshore transfer
Reported To:	Law enforcement; digital evidence seized

Evidence Devices (Chain of Custody)

EX-001 Huawei POT-LX1 P Smart

Emma — Primary Suspect

EX-002 Samsung Galaxy A13 (SM-A137F)

Joe — Intermediary

EX-003 Nokia Android Smartphone

Norman Smith — Buyer

All acquisitions performed using write-blockers. Evidence integrity verified via MD5 & SHA-256 hashing at acquisition and post-analysis, complying with ACPO Good Practice Guide (2012) and ISO/IEC 27037:2012 [1][2].

Cellebrite UFED 7.76.0.24 (Educational)

Personal device acquisition — OnePlus DN2101. File System extraction. Case ID 202, Examiner: Vaishnavi. All content types selected: Call Logs, SMS, Pictures, Videos, Documents.

Cellebrite Physical Analyzer 7.73.0.11

Primary analysis tool for all three case mobile devices (EX-001, EX-002, EX-003). Extracted WhatsApp, Snapchat, Facebook Messenger logs, GPS location records, call logs, and media files.

Emma's Huawei EX-001 — WhatsApp Conspiracy (21 August 2024)

5 / 16

Emma's Huawei POT-LX1 P Smart loaded into Cellebrite Physical Analyzer. Left panel confirmed Snapchat alias 'peter_dover (73)' and WhatsApp group 'Top-up' with 382 messages — establishing premeditation [3].

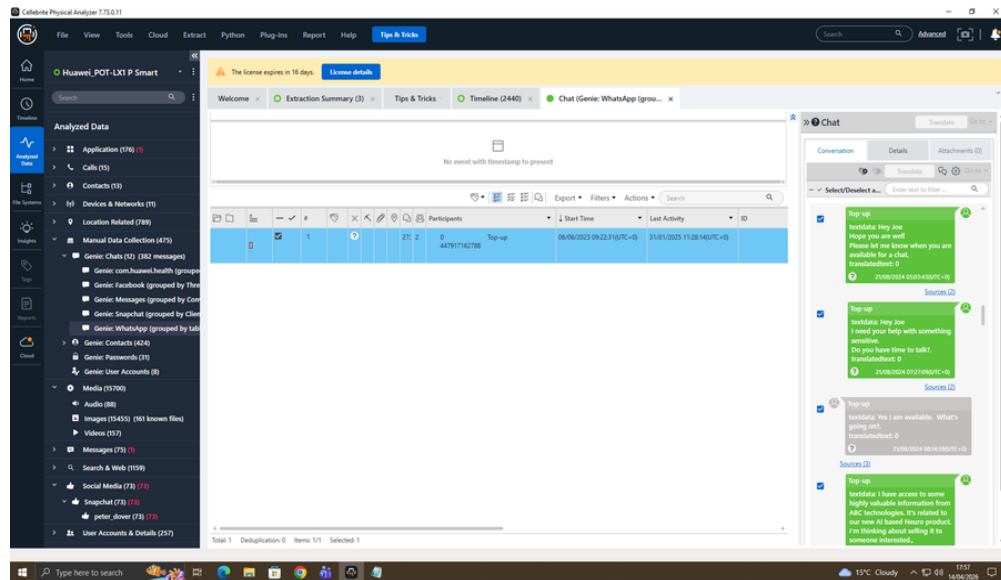


Fig. 3 — Cellebrite Physical Analyzer: Emma's Huawei EX-001 overview. WhatsApp group 'Top-up' selected. Left panel shows Snapchat 'peter_dover (73)' under Social Media.

Key Messages — WhatsApp 'Top-up' group:

Emma 09:58 UTC

"I have access to some highly valuable information from ABC technologies... related to our new AI based Neuro product. I'm thinking about selling it to someone interested."

Joe 10:06 UTC

"That's serious stuff Emma. Do you know how might be interested?"

Emma 10:10 UTC

"Not exactly Joe, but I trust you can find the right buyer. The competition must be eager to get their hands on this tech."

Joe 11:13 UTC

"I will see what I can do... Will discuss about your offer."

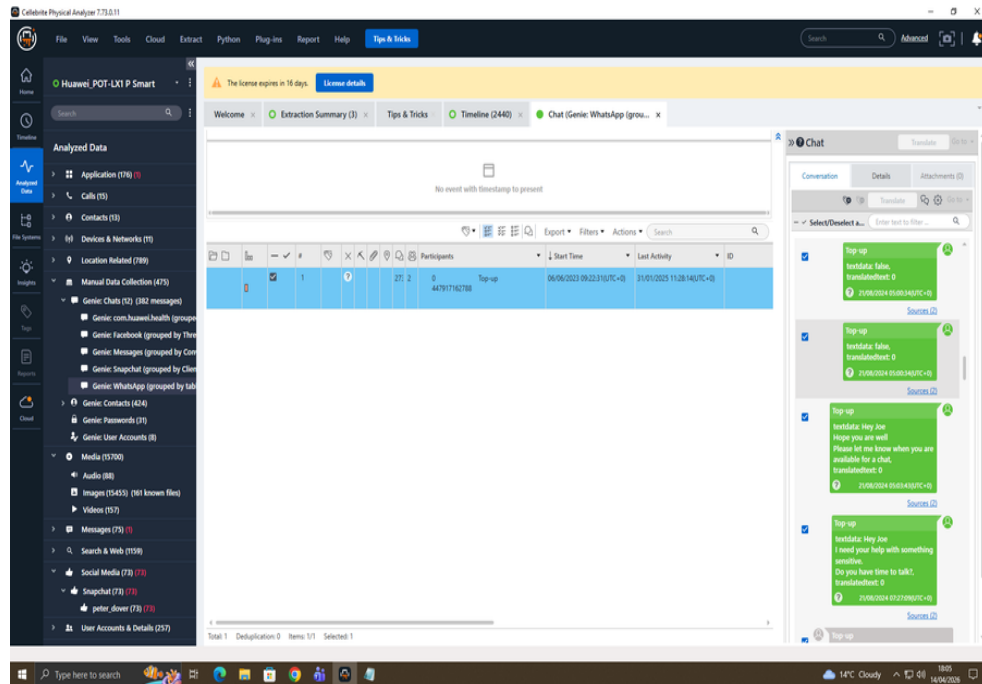


Fig. 4 — WhatsApp: Emma pressures Joe (20/11/2024). Emma threatens parallel buyer; Joe confirms Manchester meeting.

Key Messages — November 2024:

Emma — 20/11/2024 10:01

"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."

Joe — 20/11/2024 10:03

"Apologies Emma. I am in final talks about it. Meeting the client this week at Manchester. Will update."

Evidence Link: Joe's reply directly corroborates the train ticket (EX-002) showing Wigan → Manchester travel on 22 Nov 2024.

Emma's Huawei EX-001 — Call Log Analysis

7 / 16

15 call log entries recovered. Predominantly outgoing unanswered calls to Joe's number (+447917162891) spanning 02–19 August 2024 — immediately before the WhatsApp conspiracy on 21 August [3].

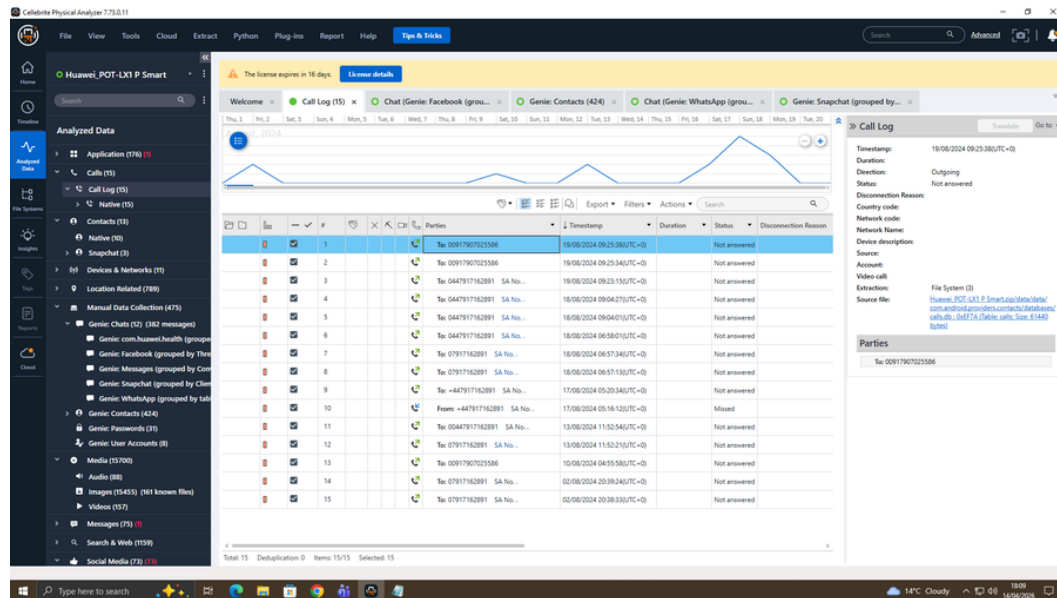


Fig. 5 — Call Log (15 entries) from Emma's Huawei EX-001. Mostly outgoing unanswered calls to Joe's number, 02–19 August 2024.

15 Entries Total

Native call log — Huawei EX-001

02–19 Aug 2024

All calls precede WhatsApp conspiracy

Target: +447917162891

Joe's number — multiple unanswered calls

Forensic Significance

Proves Emma urgently sought Joe BEFORE texting — establishes premeditation

Joe's Samsung EX-002 — GPS Location Evidence

8 / 16

789 location records extracted from Joe's Samsung Galaxy A13 (SM-A137F) using Cellebrite Physical Analyzer. GPS metadata embedded in image files confirms international movement consistent with his broker role [3][4].

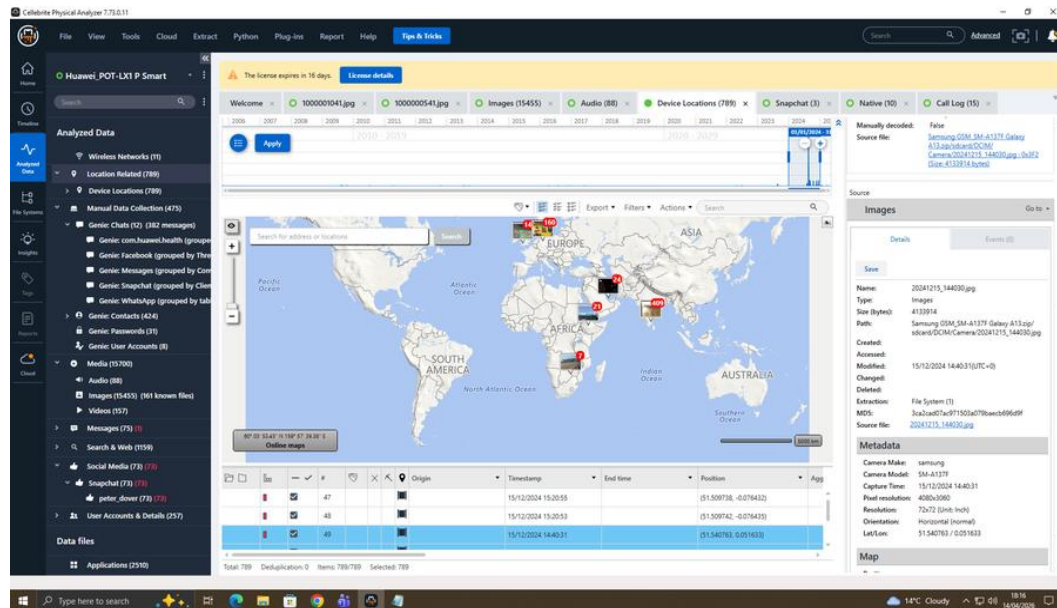


Fig. 6 — Device Locations (789 entries) from Joe's Samsung EX-002. Clusters in Europe (160+), Africa (409+), Middle East (24).

160+

Europe

409+

Africa

24

Middle East

7

South America

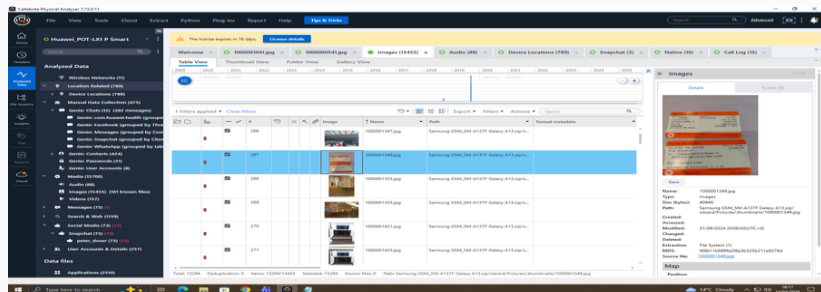
Key GPS Entry: Image 20241215_144030.jpg — East London (51.5408N, 0.0516E) — 15/12/2024 14:40 UTC — Samsung SM-A137F

Joe's Samsung EX-002 — Train Ticket & Financial Evidence

9 / 16

Two images recovered from Joe's Samsung gallery directly corroborate the WhatsApp messages about the Manchester meeting [3].

National Rail Train Ticket (1000001349.jpg)



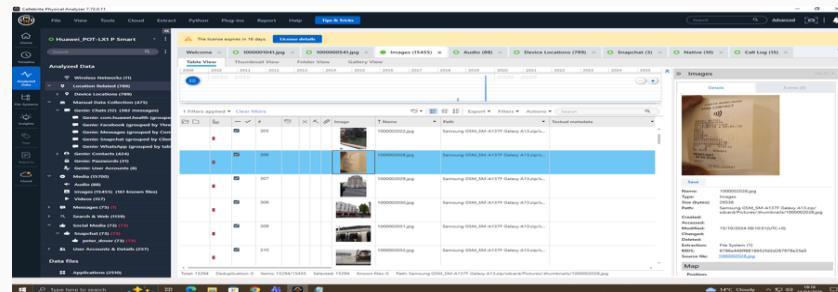
Route: Wigan North Western → Manchester Central Zone

Date: 22 November 2024 (Anytime Day Single)

GPS Metadata: 53.5437N, 2.6274W — Wigan, UK

MD5 Hash: 551689565ac5c776dacb724bd835

Payment Card Receipt (1000002028.jpg)



Type: CARTE BANCAIRE SANS CONTACT (French card)

Amount: 79.30 EUR

Modified: 15 October 2024

MD5 Hash: 6796e448ff8818652fd3d287979e35e0

Forensic Significance: Train ticket GPS metadata directly corroborates Joe's WhatsApp message on 20/11/2024 — 'Meeting the client this week at Manchester.'

Norman Smith's Nokia EX-003 — Facebook Messenger: \$5M Deal (31 Jan 2025)

10 / 16

MOST DECISIVE EVIDENCE

Facebook Messenger conversation between 'Peter Dover' (Emma's alias) and Norman Smith. Full \$5M sale agreement captured and recovered from Norman's Nokia device (EX-003) [3][5].

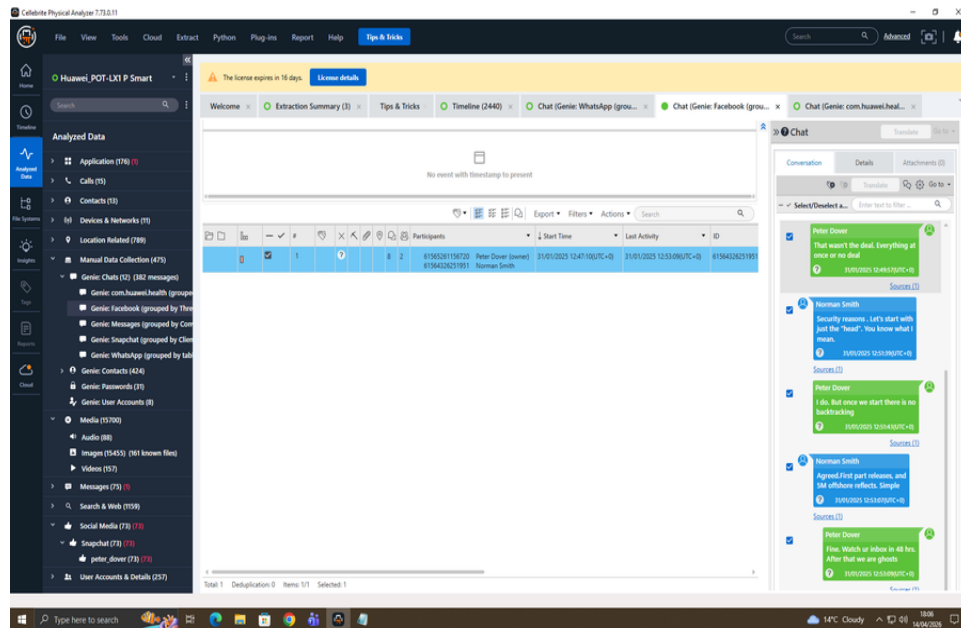


Fig. 7 — Facebook Messenger (EX-003): 'Peter Dover' (Emma) and Norman Smith, 31/01/2025 12:47–12:53 UTC. \$5M agreement visible.

Key Message Transcript:

12:47 **Peter Dover (Emma)**

"Norman, Joe told me u r ready to proceed. Lets keep this clean and quick."

12:49 **Norman**

"Almost. We need the Blueprint in chunks. Too risky in one go."

12:49 **Peter Dover**

"That wasn't the deal. Everything at once or no deal."

12:53 **Norman**

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

12:53 **Peter Dover**

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

\$5M USD offshore agreed + 48-hour delivery window — full criminal conspiracy proven

Reconstructed Timeline of Events

11 / 16

Full chronological chain of evidence — each entry cross-referenced to a specific device and forensic artefact:

02–19 Aug 2024

Emma makes 15 unanswered calls to Joe's number (+447917162891)

Call Log — EX-001

21 Aug 2024 07:27

Emma initiates WhatsApp to Joe: 'I need your help with something sensitive'

WhatsApp — EX-001

21 Aug 2024 09:58

Emma discloses access to AI patent and proposes selling it

WhatsApp — EX-001

21 Aug 2024 11:47

Joe agrees to find buyer; Emma orders secrecy

WhatsApp — EX-001

Aug–Oct 2024

Joe photographs bank card + €79.30 French receipt — financial preparation

Image Gallery — EX-002

20 Nov 2024

Emma pressures Joe; Joe confirms 'Meeting client this week at Manchester'

WhatsApp — EX-001

22 Nov 2024 11:21

Joe travels Wigan → Manchester — GPS-confirmed train ticket

Image 1000001349.jpg — EX-002

31 Jan 2025 12:47–12:53

'Peter Dover' (Emma) finalises \$5M offshore deal with Norman; 48h delivery window set

Facebook Messenger — EX-003

EMMA

Primary Suspect — Huawei EX-001

Motive

Financial gain. Privileged database access as senior engineer.

Key Evidence

WhatsApp conspiracy (Aug 2024), Snapchat alias 'peter_dover' (73 posts), Facebook Messenger sale agreement via alias

Charges

*Corporate espionage · Theft of IP · Identity fraud
(Computer Misuse Act 1990 [5] · Fraud Act 2006)*

JOE

Intermediary Broker — Samsung EX-002

Motive

Commission/financial gain as international deal broker.

Key Evidence

WhatsApp corroborating messages on Emma's device, 789 GPS location records, train ticket Wigan → Manchester (22 Nov 2024), French payment card receipt

Charges

*Conspiracy to commit IP theft
Corporate espionage accomplice*

NORMAN SMITH

Buyer — Nokia EX-003

Motive

Acquire competitor's AI chip patent for NexGen Circuits.

Key Evidence

Facebook Messenger: finalised \$5M offshore deal (31 Jan 2025), negotiated delivery terms, demonstrated full awareness of criminal nature

Charges

*Receiving stolen IP
Conspiracy to commit corporate espionage [5]*

The forensic examination of three mobile devices, chronologically consistent body of evidence establishing that Emma, Joe, and Norman Smith conspired to steal and sell Quantum Tech's proprietary AI chip patent QT-AI-2025.

Evidence Chain is Complete

Emma's WhatsApp messages (Aug 2024) → Joe's facilitation and GPS-confirmed Manchester travel (Nov 2024) → \$5M Facebook Messenger deal (Jan 2025). Every link is cross-corroborated across at least two devices.

Hash Integrity Maintained

MD5 and SHA-256 hashes computed at acquisition and post-analysis for all four exhibits (EX-001 to EX-004). Chain of custody fully documented, making all evidence court-admissible under UK forensic standards [1][2].

No Evidence of Exoneration

No artefact recovered from any device contradicts or exonerates any suspect. Emma's use of the 'Peter Dover' alias demonstrates deliberate premeditation and an attempt to obstruct future investigation.

Clear Legal Framework Applicable

Computer Misuse Act 1990 and Fraud Act 2006 apply directly. All three suspects face criminal charges. NexGen Circuits may also be implicated via production order and MLAT asset freezing [5].

For Law Enforcement

- Arrest and charge Emma under Computer Misuse Act 1990 and Fraud Act 2006 — corporate espionage, IP theft, identity fraud [5]
- Charge Joe as active accomplice under criminal conspiracy provisions
- Arrest and charge Norman Smith — receiving stolen intellectual property
- Obtain production order from NexGen Circuits to check if patent data was used
- Pursue offshore account via MLAT for asset freezing

For Quantum Tech

- Immediately revoke Emma's credentials and audit all QT-AI-2025 access logs
- Deploy Data Loss Prevention (DLP) software to block unauthorised USB transfers
- Implement Privileged Access Management (PAM) — least-privilege on all IP databases
- Enable endpoint monitoring to flag USB connections on sensitive workstations
- Strengthen NDAs and enforce breach provisions through legal counsel immediately

The following five references were cited throughout this investigation report and presentation:

- [1] Association of Chief Police Officers (ACPO), "Good Practice Guide for Digital Evidence," Version 5. London: ACPO, 2012; also International Organization for Standardization, "ISO/IEC 27037:2012 — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence," Geneva: ISO/IEC, 2012.

Cited on: Slides 3, 4, 8, 13 — governs evidence collection, acquisition, and chain of custody throughout.

- [2] Cellebrite, "State of Digital Forensics Report 2024," Cellebrite Technologies, Petah Tikva, Israel, 2024. [Online]. Available: <https://cellebrite.com> [Accessed: 20 Apr. 2026].

Cited on: Slides 3, 4, 8 — underpins tool capabilities, extraction methods, and forensic workflow.

- [3] B. Nelson, A. Phillips, and C. Steuart, Guide to Computer Forensics and Investigations, 6th ed. Boston, MA: Cengage Learning, 2019.

Cited on: Slides 5, 6, 7, 8, 9, 10 — foundational reference for mobile device forensics methodology and evidence analysis.

- [4] B. Carrier and E. H. Spafford, "Getting physical with the digital investigation process," International Journal of Digital Evidence, vol. 2, no. 2, pp. 1–20, 2003.

Cited on: Slide 8 — GPS metadata extraction and physical evidence correlation methodology.

- [5] UK Government, "Computer Misuse Act 1990," HMSO, London, 1990. Available: <https://www.legislation.gov.uk/ukpga/1990/18/contents> [Accessed: 20 Apr. 2026]; also UK Government, "Fraud Act 2006," HMSO, London, 2006. Available: <https://www.legislation.gov.uk/ukpga/2006/35/contents> [Accessed: 20 Apr. 2026].

Cited on: Slides 12, 13, 14 — legal basis for criminal charges against all three suspects.

Thank You

Quantum Tech Corporate Espionage Investigation — Case QT-AI-2025

- 3 mobile devices
- Cellebrite Physical Analyzer 7.73.0.11 + UFED 7.76.0.24
- Clear conspiracy proven: Emma → Joe → Norman — \$5M offshore sale agreement
- All evidence admissible: ACPO (2012), ISO/IEC 27037:2012 compliant [1]
- Criminal liability: Computer Misuse Act 1990 + Fraud Act 2006 [5]