

Digital Forensic 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

Smit Brijeshkumar Patel

Enrollment: 2506590 | Level 7 | MSc Cyber Security and Digital Forensics

University of Wales Trinity Saint David - London Campus

Presented: April 2026

Part A: UFED Extraction - Device Connection

I plugged my own Samsung Galaxy S25 Ultra into the UFED workstation to show I can run the acquisition process end to end. UFED v7.76.0.24 (Educational licence) picked it up straight away - SM-S938B, Android 16, IMEI1 357853619175517, 183 GB used, 146 apps, not rooted [3].

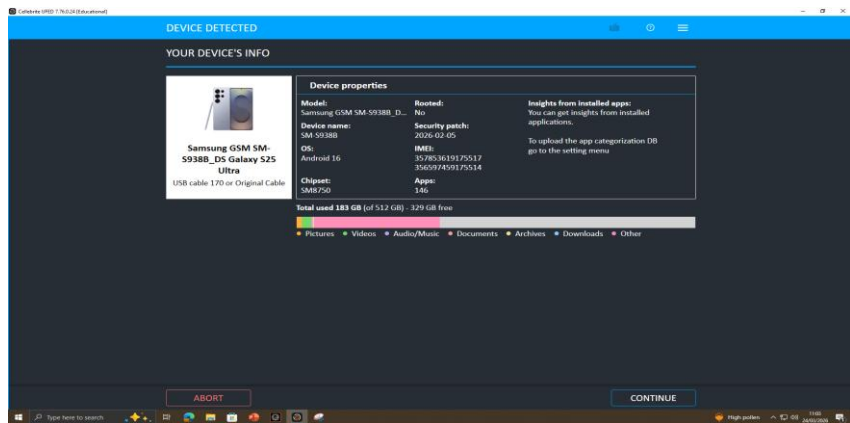


Figure 2: Device properties confirmed by UFED

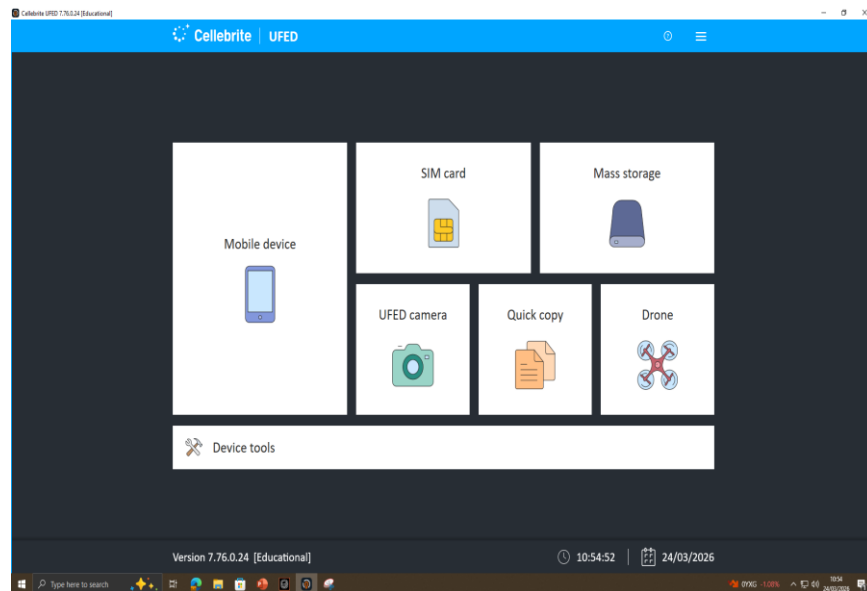
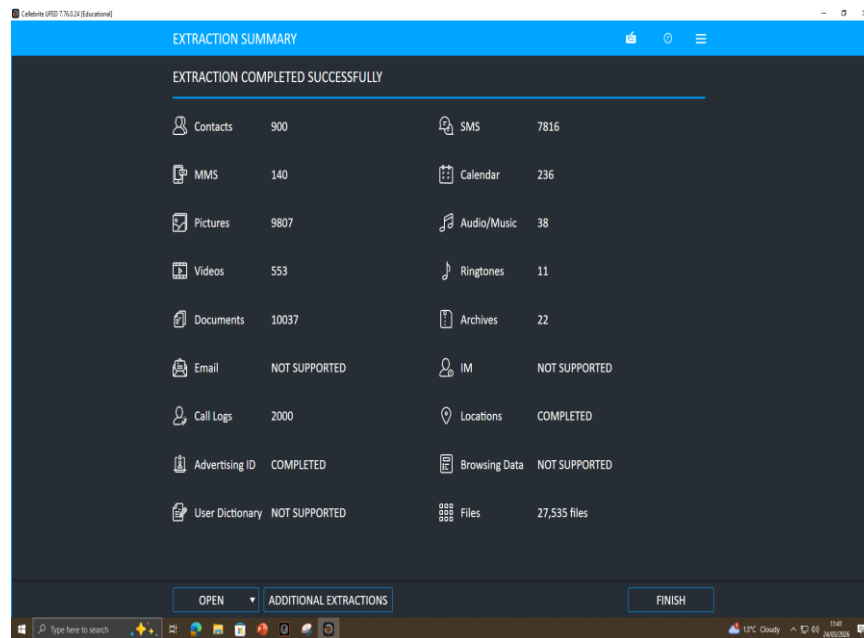


Figure 1: UFED 7.76 home screen

Part A: Extraction Results and Hash Generation

I ran a File System extraction and got back 27,535 files in total - 900 contacts, 7,816 SMS, 9,807 pictures, 553 videos, 10,037 documents. Email and IM came back as NOT SUPPORTED, which is a licence limitation. UFED generated a SHA-256 hash automatically once it finished [3].



EXTRACTION SUMMARY			
EXTRACTION COMPLETED SUCCESSFULLY			
Contacts	900	SMS	7816
MMS	140	Calendar	236
Pictures	9807	Audio/Music	38
Videos	553	Ringtones	11
Documents	10037	Archives	22
Email	NOT SUPPORTED	IM	NOT SUPPORTED
Call Logs	2000	Locations	COMPLETED
Advertising ID	COMPLETED	Browsing Data	NOT SUPPORTED
User Dictionary	NOT SUPPORTED	Files	27,535 files

Figure 3: Extraction summary - all categories recovered

Part B: Case Background and Evidence Inventory

Quantum Tech found someone accessing their AI chip patent QT-AI-2025 without authorisation. Three suspects: Emma (senior engineer with database access), Joe (intermediary), Norman (buyer). I was given four pre-acquired device images. Handled per ACPO [1] and ISO 27037 [4].

Device	Model	Suspect	OS	IMEI 1
Device 1	Huawei POT-LX1 P Smart	Emma	Android 10	860962043462662
Device 2	Samsung SM-A137F Galaxy A13	Joe	Android 14	357898921470825
Device 3	Nokia C2 2nd Edition	Norman	Android 11	353766763818217
Device 4	Ulefone Note 14	Unknown	Android 12	355617730545771

Analysis Methodology - Two-Stage Approach

Stage 1: Individual Projects

- Each device opened as standalone project
- Hash verified per device separately
- Device-specific apps, GPS, summaries
- Extraction Summary (1) in screenshots
- All counts = that device only

Stage 2: Combined Project

- All 4 images in EvidenceCollection project
- Cross-device communication analysis
- Genie decoded WhatsApp, Messenger, Snapchat
- Extraction Summary (4) in screenshots
- Sidebar counts = all 4 devices combined

Hash Verification -All Four Images Intact

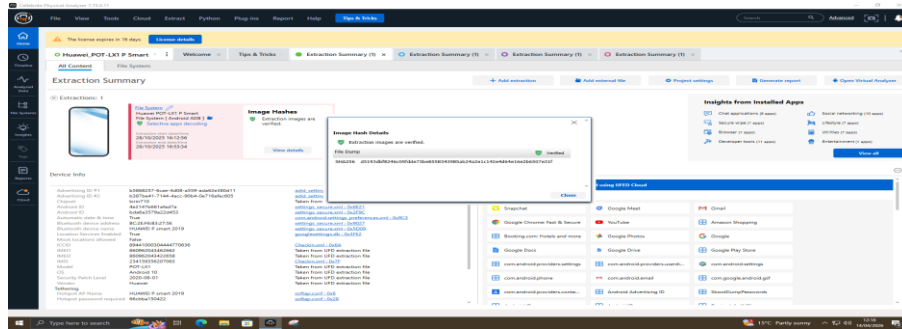


Figure 4: Huawei P Smart (Emma) - Verified

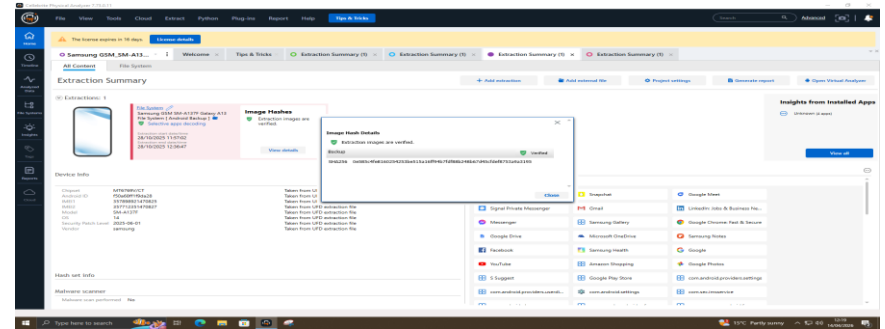


Figure 5: Samsung A13 (Joe) - Verified

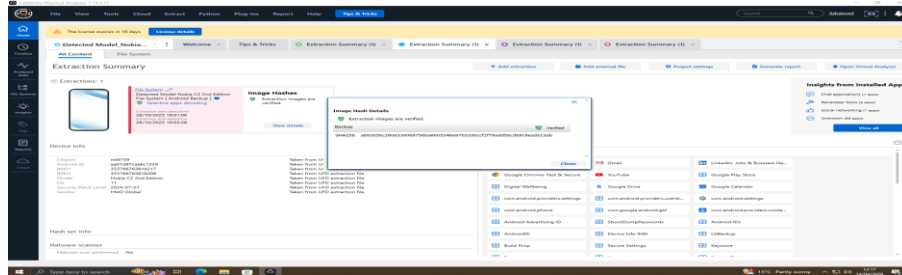


Figure 6: Nokia C2 - Verified

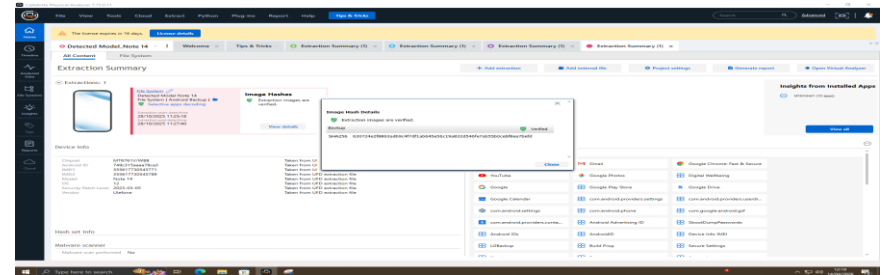


Figure 7: Ulefone Note 14 - Verified

WhatsApp Evidence -The Peter Dover Alias

Emma ran a completely fake identity the whole time. She set up the Peter Dover alias on 17 Aug 2024 - a dedicated Huawei with a Lebara SIM and dovvp59@gmail.com - four days before she first messaged Joe [7]. 27 messages over 5 months (21 Aug 2024 to 31 Jan 2025).

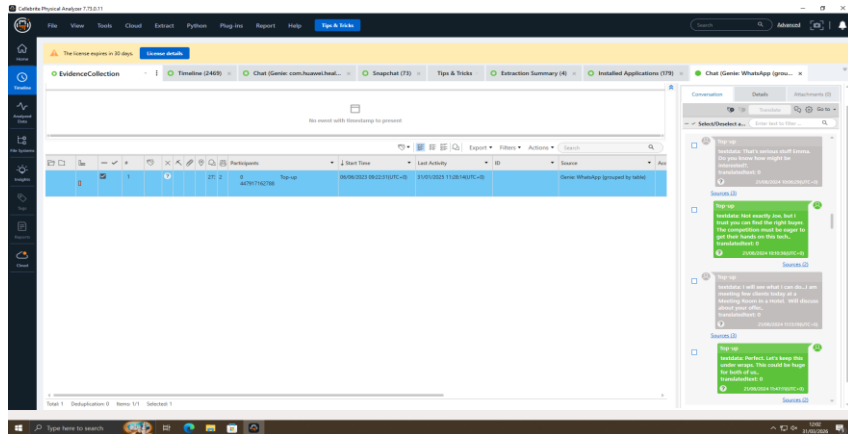


Figure 9: Joe agrees to help

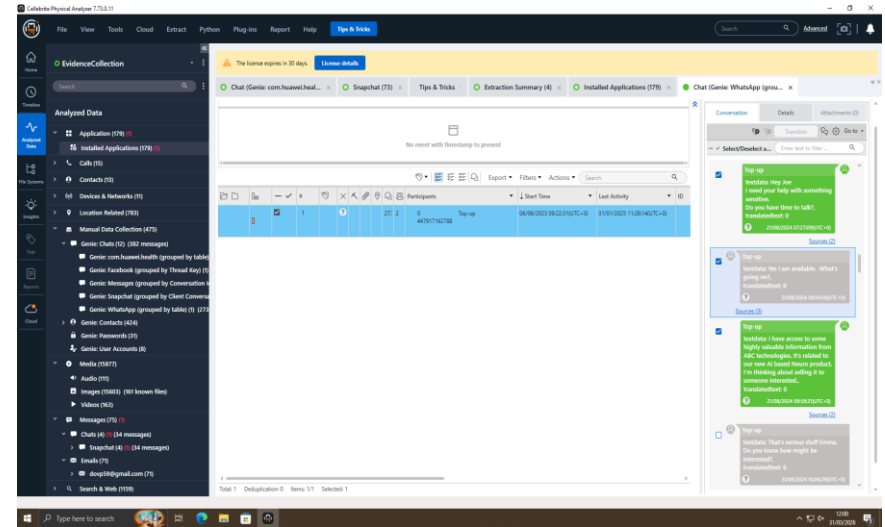


Figure 8: Emma approaches Joe - 21 August 2024

WhatsApp Evidence -Five Months of Negotiation

From August to November 2024, Joe went to meetings and reported back with partial progress. By 20 Nov Emma had lost patience: "It is disappointing that no response from u." That got Joe moving - he told her he was in final talks and meeting the client in Manchester that week.

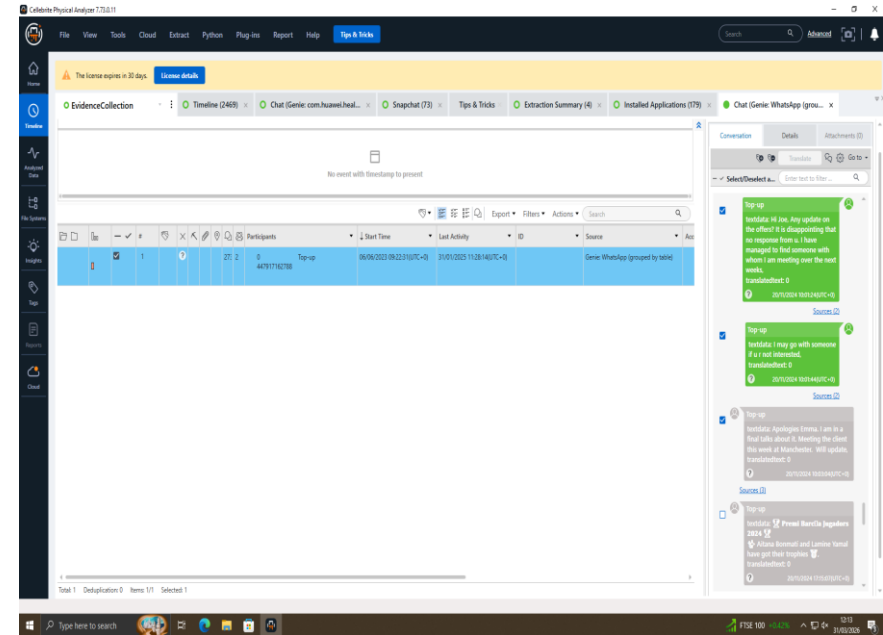


Figure 10: Nov 2024 - Emma pressing for progress

WhatsApp Evidence -5M Offshore Deal Confirmed

31 January 2025 - the deal gets specific:

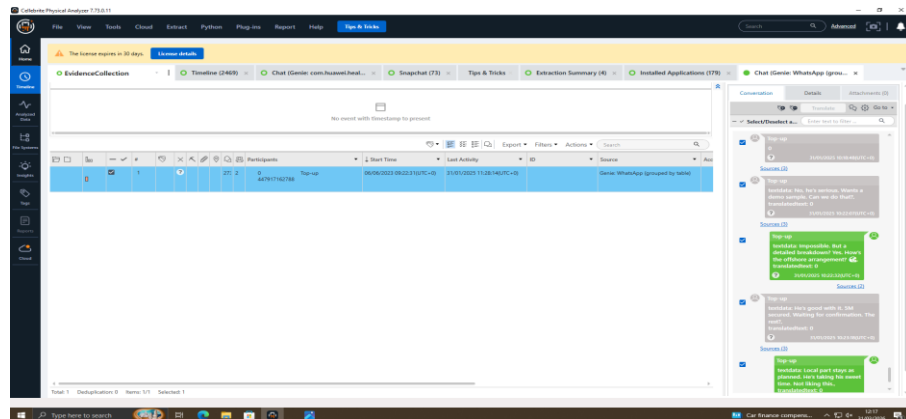


Figure 11: 5M secured, offshore arrangement

5M payment and offshore routing both stated explicitly [5]

Joe: "He's good with it. 5M secured." | Emma: "How's the offshore arrangement?"

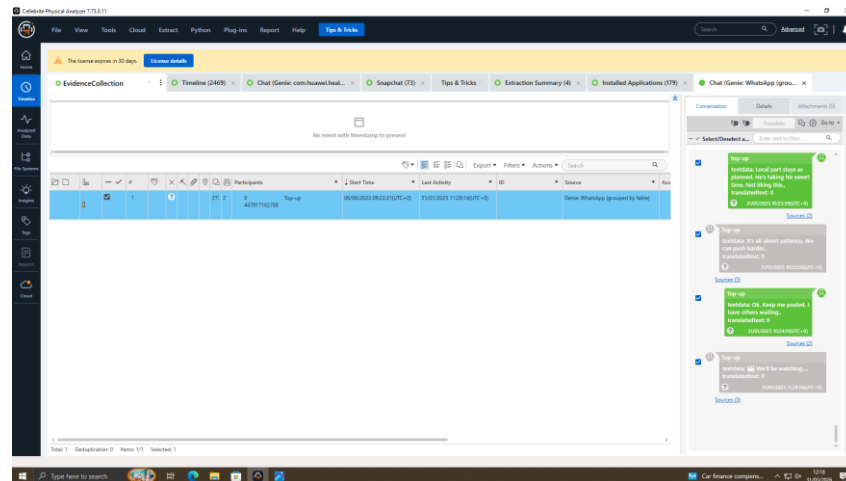


Figure 12: Final messages - 11:28:14

Joe's Manchester Trip - Physical Corroboration

Joe told Emma he was going to Manchester to meet the client. His phone proves he actually went - two independent pieces of evidence from his Samsung A13.

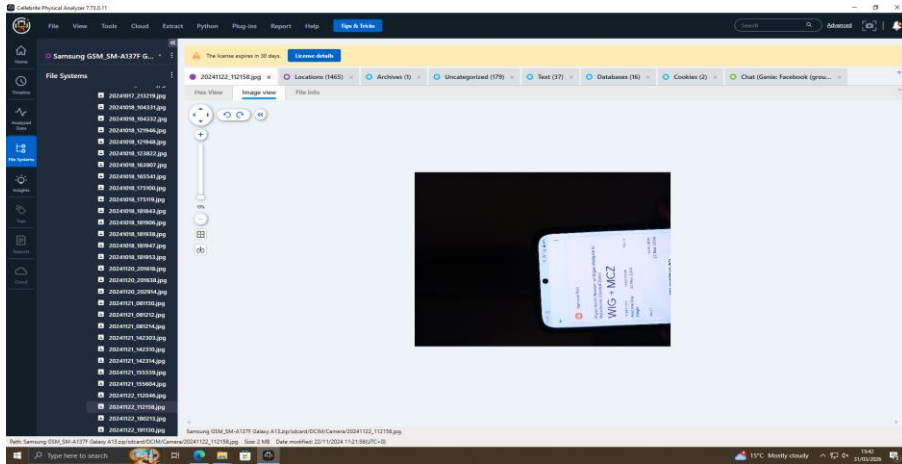


Figure 13: Train ticket WIG→MCZ, 22 Nov 2024

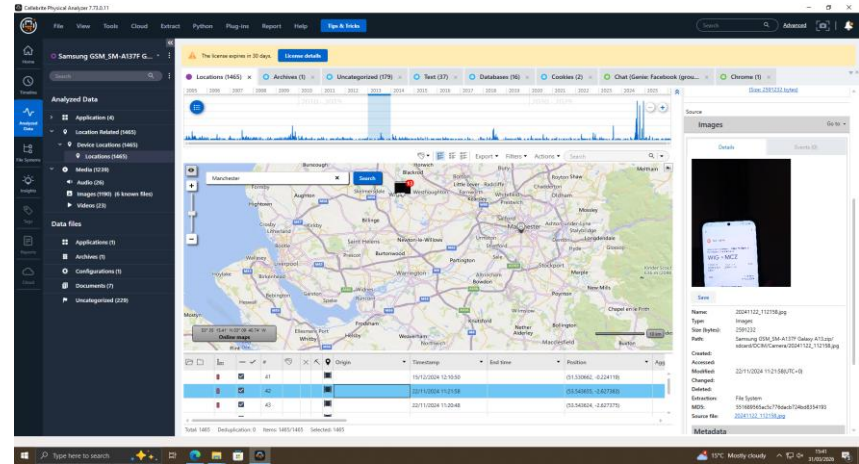


Figure 14: GPS 53.543655, -2.627383 - Manchester

That is not just Joe saying he went to Manchester. His phone was physically there on 22 November 2024 at 11:21:58

Facebook Messenger - Peter Dover and Norman Smith

31 Jan 2025 from 12:47 - barely an hour after the WhatsApp thread closed. Emma went straight to Norman.

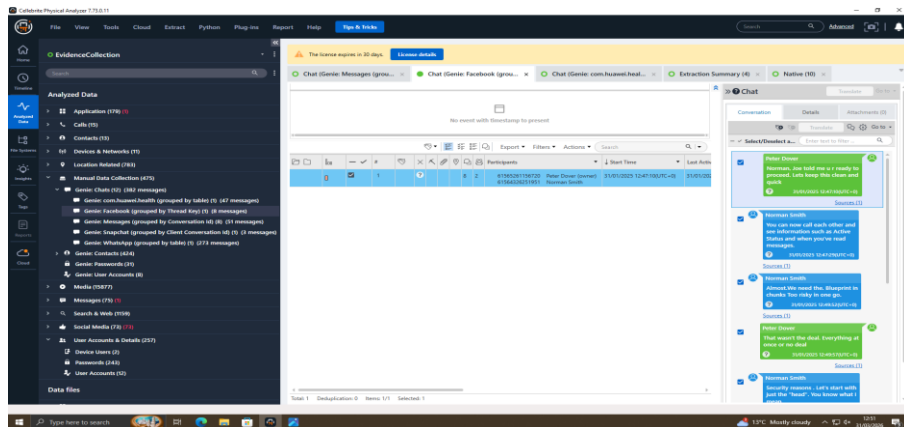


Figure 15: Messenger thread opens

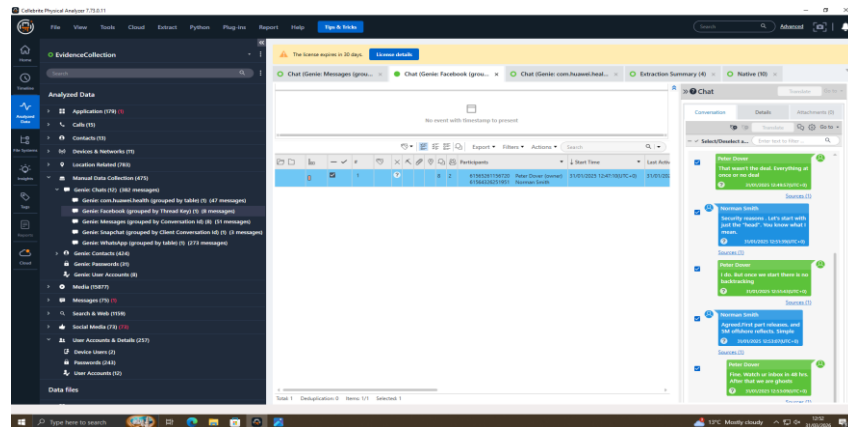


Figure 16: 5M offshore agreed, blueprint in chunks

The same 5M figure shows up in both WhatsApp and Messenger within 60 minutes - Emma was running both sides of the deal on the same day

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

Supporting Evidence - Emails, Calls, Nokia GPS

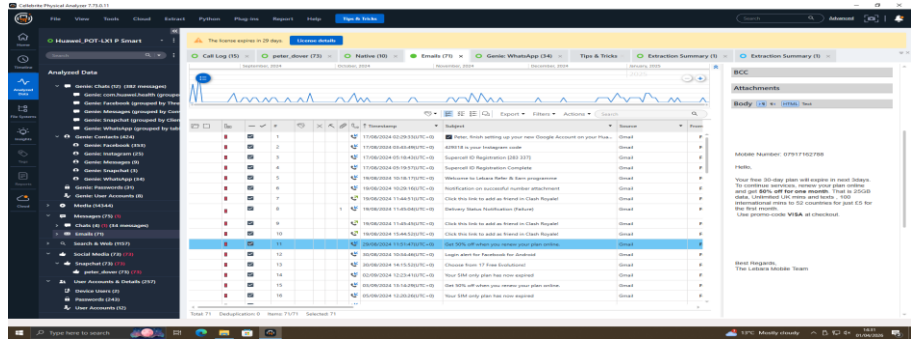


Figure 17: 71 emails - earliest 17 Aug 2024

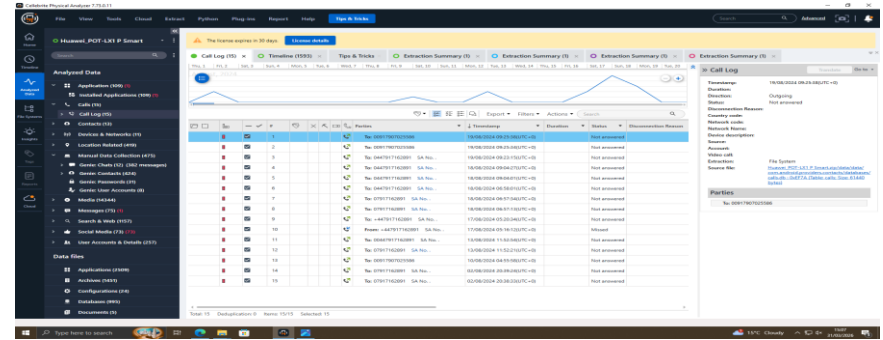


Figure 18: 15 calls, mostly unanswered, Aug 2024

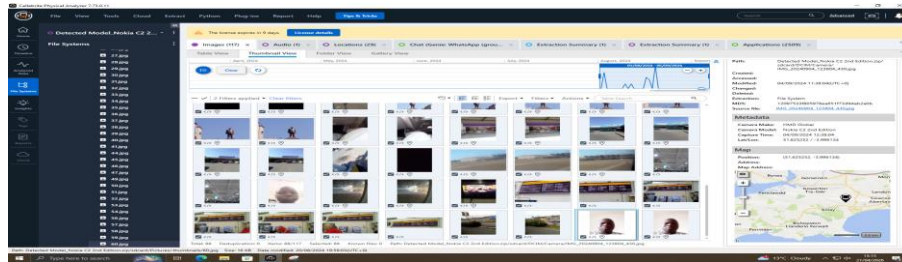


Figure 19: Nokia GPS - Swansea, Sep 2024

- 3 Snapchat msgs recovered [2]
- Signal on Samsung - no content
- Nokia C2: 117 GPS images
- Swansea: 51.625, -3.996

Reconstructed Timeline

Date	Event
17 Aug 2024	Peter Dover alias + Lebara SIM created on Huawei
21 Aug 2024	Emma messages Joe: proposes selling AI patent data
21 Aug 2024	Joe agrees; attending hotel meetings same day
26 Aug 2024	Joe: first meeting failed, has new contacts
20 Nov 2024	Emma presses; Joe confirms Manchester meeting
22 Nov 2024	Joe in Manchester: GPS + train ticket WIG→MCZ
31 Jan 10:15-11:28	WhatsApp: 5M secured, offshore confirmed
31 Jan 12:47	Messenger: Emma→Norman. Blueprint in chunks. 5M offshore. "Ghosts"

Suspect Profiling

Emma - Primary Suspect

Set up the Peter Dover alias 4 days before contacting Joe. She started the whole thing, set the terms, kept pushing for 5 months, then cut Joe out and went straight to Norman. The alias being ready before first contact points to premeditation [7].

Joe - Intermediary

Not just a message-passer - he actively worked the deal. Hotel meetings, the Manchester trip (GPS + ticket prove he was there), chased contacts, confirmed the 5M and offshore arrangement. Signal was on his phone but nothing recovered.

Norman Smith - Buyer

Contacted via Messenger on the final day. He already knew what the Blueprint was before the conversation started. Agreed to 5M offshore, wanted it sent in chunks. Nokia GPS puts him in Swansea area in Sep 2024. Who he works for is still unknown.

Conclusion and Recommendations

Key Findings

- Consistent, corroborated evidence across 4 devices
- Premeditated false identity (4-day lead time)
- 5M offshore in both WhatsApp and Messenger
- Joe's Manchester trip: GPS + ticket confirmed
- All 4 image hashes verified intact

Recommendations

- Revoke Emma's database access immediately
- Audit QT-AI-2025 patent access logs [6]
- Production orders for email + Facebook accounts
- Financial investigation: offshore arrangements
- Examine Emma's USB/cloud for blueprint transfer

Thank You

Smit Brijeshkumar Patel | 2506590 | ACCA7031 | April 2026

References

- [1] ACPO (2012) Good Practice Guide for Digital Evidence, Version 5. Association of Chief Police Officers.
- [2] Anglano, C., Canonico, M. and Guazzone, M. (2017) 'Forensic analysis of Telegram Messenger on Android smartphones', Digital Investigation, 23, pp. 31-49.
- [3] Casey, E. (2011) Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd edn. Amsterdam: Academic Press.
- [4] ISO (2012) ISO/IEC 27037:2012 - Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. Geneva: ISO.
- [5] Jahankhani, H., Kendzierskyj, S. and Chelvachandran, N. (2021) Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity. Cham: Springer.
- [6] NIST (2020) NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations. Gaithersburg, MD: NIST.
- [7] Nelson, B., Phillips, A. and Steuart, C. (2015) Guide to Computer Forensics and Investigations. 5th edn. Boston, MA: Cengage Learning.