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

ACCA7031 – Digital Forensics Analysis

Student Name:
SMIT BRIJESHKUMAR PATEL

Student ID:
2506590

Programme:
MSc Cybersecurity and Digital Forensics

Submission Date:
Friday, 29th April 2026

Table of Contents

TASK 1 3
- **1. Introduction** 3
- **2. Current State of the Field and Key Tools** 3
- **3. Intersection of Digital Forensics and Cybersecurity** 4
- **4. Emerging Trends** 4
- **5. Key Challenges** 4
- **6. National and International Job Market** 5
- **7. Conclusion** 5

TASK 2 6
- **Part A: Forensic Acquisition - Cellebrite UFED Demonstration** 6
  - **1. Overview** 6
  - **2. Cellebrite UFED - Tool Overview** 6
  - **3. Device Connection and Detection** 7
  - **4. Extraction and Results** 8
- **Part B: Quantum Tech Corporate Espionage Investigation** 9
  - **1. Case Background** 9
  - **2. Evidence Inventory** 9
  - **3. Analysis Methodology** 10
  - **4. Findings** 12
  - **5. Reconstructed Timeline** 22
  - **6. Suspect Profiling** 23
  - **7. Challenges and Limitations** 24
  - **8. Conclusion** 24
  - **9. Recommendations** 25
- **References** 25

TASK 1

Digital Forensics: Current State, Emerging Trends, and Career Landscape

1. Introduction

Ten years ago, digital forensics meant a specialist recovering files from a seized hard drive. That version of the field barely exists anymore. Today, almost every serious cyber incident needs forensic work somewhere - pulling deleted files out of a ransomware mess, figuring out how an attacker moved through a network, or piecing together messages that someone tried to destroy. The discipline expanded because the volume of digital evidence people generates through phones, cloud accounts, wearables, and connected cars left no other option [5]. This report covers five things: the tools practitioners rely on, how forensics connects to cybersecurity, where the field is heading, what makes the work hard, and what the job market looks like.

2. Current State of the Field and Key Tools

Two platforms dominate commercial forensics. Cellebrite UFED is what most examiners reach for on mobile - it covers physical, file system, logical, and backup extraction across thousands of Android and iOS models, generating a SHA-256 hash at acquisition [3]. Magnet AXIOM handles both mobile and computer forensics and is widely used in law enforcement for artefact recovery and timeline reconstruction.

On the open-source side, Autopsy and Sleuth Kit are what most universities teach. Autopsy handles multi-source ingestion, keyword search, hash filtering, and has a plugin system covering most evidence types [4][13]. FTK from Exterro is the go-to for disk forensics in corporate settings, mainly for its indexed search speed. No single tool covers everything, and most investigations pull from several.

Cloud has changed the game. When most of a person's data sits in Google Drive or iCloud rather than on their phone, imaging a device only gives you half the picture. Investigators now need API access to cloud platforms, subpoenas to providers, and artefacts like authentication tokens that did not exist in traditional forensics [10].

3. Intersection of Digital Forensics and Cybersecurity

In practice, the line between digital forensics and cybersecurity incident response has mostly disappeared. When ransomware hits an organisation, the IR team and the forensic examiners end up working the same problem from opposite ends - one side trying to contain it and get systems back, the other trying to work out exactly what happened and how the attacker got in. The NIST Cybersecurity Framework bakes forensic analysis directly into its response and recovery phases [9]. Without it, incident responders are patching blind.

Threat intelligence is the other obvious overlap. Malware analysis is a forensics discipline at its core, feeding indicators of compromise into the threat intel platforms that defenders rely on. Attribution relies on forensic artefacts - code reuse patterns, infrastructure fingerprints, TTPs pulled from captured samples [7][14]. The two fields need each other, which is probably why most MSc programmes now teach them together.

4. Emerging Trends

Three things are changing the field right now. First, AI-assisted analysis. Some tools have started using machine learning to flag unusual behaviour and classify artefacts on their own. It genuinely helps when you are sitting in front of terabytes of data and cannot review it all manually. But it also raises questions about explainability and admissibility that the courts have not sorted out yet [7].

Second, encrypted and ephemeral messaging. Signal, Snapchat, and WhatsApp with disappearing messages turned on are now the default in the cases that matter most. Snapchat wipes conversations from its servers before anyone gets near the phone [2]. Signal's encryption means backup extractions come back empty. The only realistic options are physical-level extraction on a rooted device, a legal order to the platform, or finding something on a linked device. None of those are easy [11].

Third, IoT and wearable evidence. Smartwatches record location and heart rate, smart speakers log audio, and cars generate route telematics. A fitness tracker placing someone at a location they denied visiting is real evidence now. But forensic tooling for these devices is still scattered compared to what exists for phones and computers [3][15] .

5. Key Challenges

Scale is the problem that never goes away. One phone can hold hundreds of thousands of files. A corporate investigation might involve dozens of devices and years of logs at once. Automated

triage helps, but it only works if the filtering criteria are right - get them wrong and you miss evidence [4].

Jurisdiction is almost as bad, especially once cloud is involved. Data sitting on servers in three different countries, each with its own legal framework for access requests, means getting lawful access can be slow, inconsistent, or flat-out impossible within the time a case actually needs [10]. Then there is anti-forensics. Suspects increasingly use encryption, secure deletion tools, and anonymisation deliberately to make the investigator's job harder. The counter-techniques have to keep evolving just to stay level [8].

6. National and International Job Market

In the UK, the job market for forensics examiners is solid. The NCA, the Met's Cyber Crime Unit, regional police forces, and HMRC all hire them. On the private side, the demand sits in incident response and cyber advisory teams at places like KPMG, Deloitte, PwC, NCC Group, and BAE Systems Applied Intelligence. Starting salaries for analysts tend to fall between £28,000 and £40,000, and experienced examiners or senior consultants can reach £55,000 to £80,000 or more, particularly in London [12].

Outside the UK, the US is where most demand sits - FBI, Secret Service, DoD cyber units, and a massive private sector all recruit continuously. The UAE and Saudi Arabia have also invested heavily in forensics capacity. Certifications that travel well include CCME (Cellebrite), EnCE (EnCase), and GCFE (GIAC) [12].

7. Conclusion

The field is not slowing down. The tools are better than five years ago, but the fundamental problem - recovering evidence, preserving it properly, and presenting it in a way that holds up in court - is as hard as it has ever been. The job market reflects that. Salaries are decent, demand is consistent, and the skills carry across law enforcement, corporate security, and consulting.

TASK 2

DIGITAL FORENSIC INVESTIGATION REPORT

Part A: Forensic Acquisition - Cellebrite UFED Demonstration

1. Overview

I used my own Samsung Galaxy S25 Ultra for this section. The idea was to run through the full UFED acquisition process - connecting a device, detecting it, extracting data, and generating a hash - so I could show I know how to use the tool before applying the same approach to the case images in Part B. Everything recovered here is from my personal phone and has nothing to do with the Quantum Tech investigation.

2. Cellebrite UFED - Tool Overview

I used Cellebrite UFED version 7.76.0.24 on an educational licence. UFED is the most widely used mobile acquisition tool in law enforcement and courts in the UK and internationally accept it as reliable [5]. It handles physical, file system, logical, and backup extraction across a wide range of Android and iOS devices, and it generates a SHA-256 hash automatically every time it creates an image [3]. Once you have the image, you load it into Physical Analyzer for the actual examination.

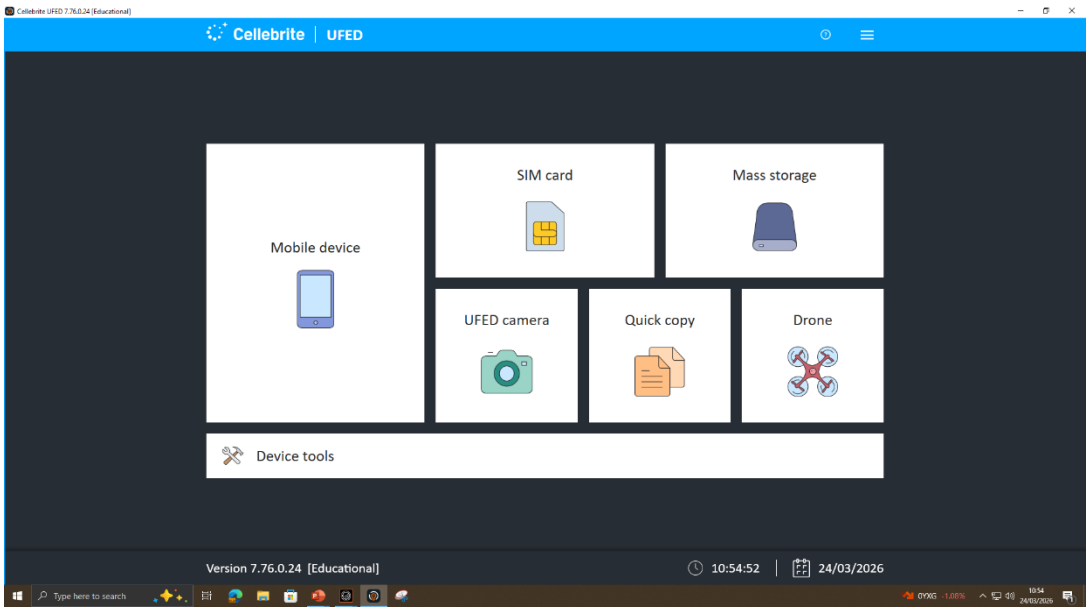

Figure 1: Cellebrite UFED 7.76 home screen - Mobile Device, SIM Card, Mass Storage, and UFED Camera options

3. Device Connection and Detection

I plugged the S25 Ultra into the UFED workstation through the Device Adapter using Cable No. 170, with the phone already in USB mode. I selected Mobile Device on the home screen and hit Auto Detect. UFED picked it up immediately as a Samsung GSM SM-S938B_DS Galaxy S25 Ultra. The properties screen confirmed everything: SM-S938B, Android 16, Snapdragon SM8750 chipset, IMEI1 357853619175517, IMEI2 356597459175514, 183 GB used out of 512 GB, 146 apps, not rooted.

Figure 2: Samsung S25 Ultra connected to UFED Device Adapter via Cable No. 170

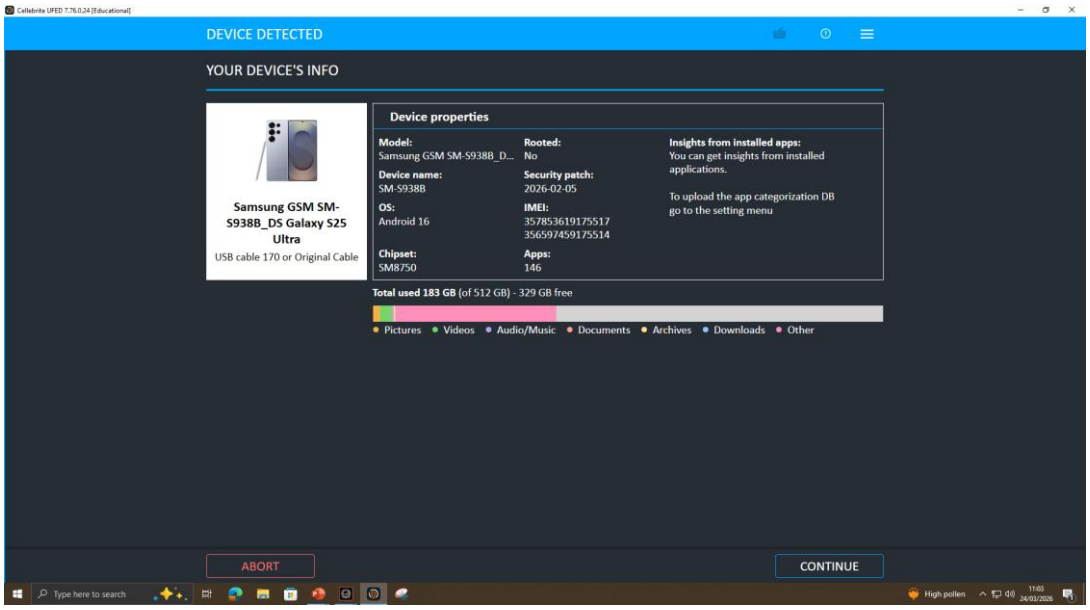

Figure 3: Device properties - model, OS, IMEI, storage, and app count confirmed by UFED

4. Extraction and Results

I ran a File System extraction. The Extraction Summary came back with 900 contacts, 7,816 SMS, 140 MMS, 9,807 pictures, 553 videos, 10,037 documents, 2,000 call log entries, 22 archives, and 27,535 total files. Email and Instant Messaging both showed as NOT SUPPORTED - that is a known limitation of the educational licence, not a device issue. The same restriction applies to the case images in Part B, where I used the Genie plugin inside Physical Analyzer to get at the chat data instead.

Once the extraction finished, UFED generated a SHA-256 hash automatically. That hash is basically a fingerprint of the image at the exact moment it was created. Later, when Physical Analyzer recalculates it and gets the same result, you know the data has not been touched between acquisition and analysis [5]. I followed the same process for all four case device images in Part B.

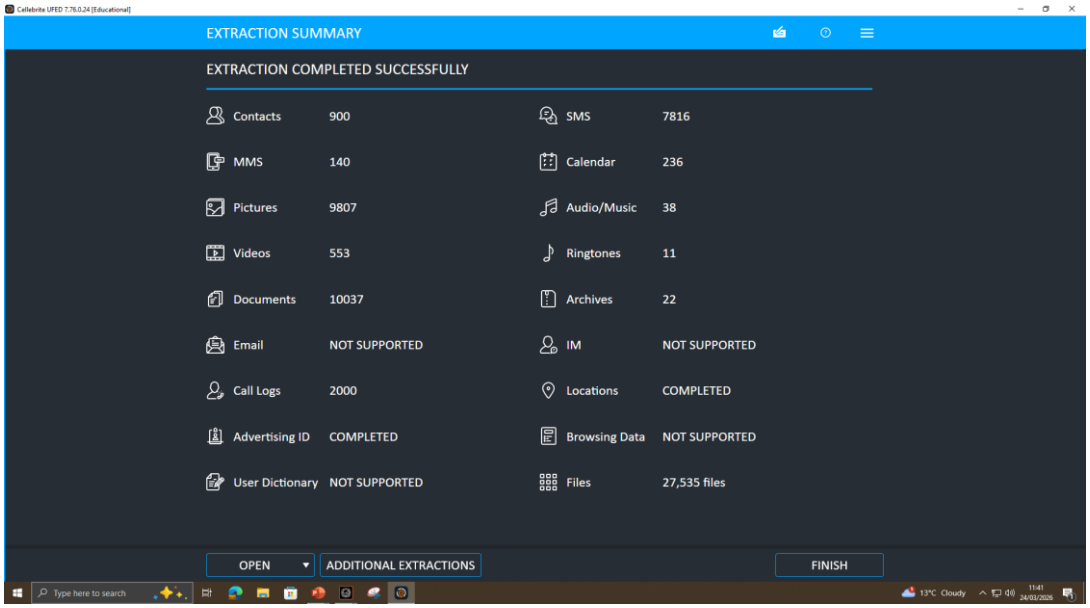

Figure 4: Extraction summary from my Samsung S25 Ultra - all supported categories recovered successfully

Part B: Quantum Tech Corporate Espionage Investigation

1. Case Background

Quantum Tech's IT security team picked up unauthorised access to their patent database. The target was QT-AI-2025, a proprietary AI chip design that sits at the centre of the company's commercial position. Losing that to a competitor would not just be a legal issue - it could genuinely threaten the business. Internal investigation, including access log analysis and HR review, pointed to Emma. She had joined recently as a senior engineer and had legitimate access to the database in question. Quantum Tech suspected she had been trying to sell the patent data through an intermediary called Joe, with someone called Norman acting as the buyer.

I was given four forensic images of suspect devices as part of the brief. I did not acquire them myself - they arrived pre-imaged and pre-hashed. My job was to load them into Physical Analyzer, pull out the communications data, and report what the evidence shows. I have not guessed at anything beyond what the devices actually contain. Everything in this report comes from the recovered data, and I have handled it in line with the ACPO Good Practice Guide [1] and ISO/IEC 27037:2012 [6].

2. Evidence Inventory

Four device images were provided. Device details below were confirmed from the Physical Analyzer extraction summaries.

Device	Model	Suspect	OS	IMEI 1
Device 1	Huawei POT-LX1 P Smart 2019	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	-	Android 12	355617730545771

3. Analysis Methodology

3.1 Loading into Physical Analyzer

I worked through the analysis in two stages. First, I opened each device image on its own as a separate Physical Analyzer 7.73.0.11 project. This is where I verified hashes and looked at device-specific data - app insights, GPS-tagged images, extraction summaries - in isolation. You can tell which screenshots come from this stage because the project name in the top-left shows the individual device: Huawei_POT-LX1 P Smart, Samsung GSM_SM-A13, Detected Model_Nokia, and Detected Model_Note 14. Each one shows Extraction Summary (1), meaning only that one device is loaded. Any data counts you see in those screenshots belong to that device alone. In the second stage, I loaded all four images together into one project called EvidenceCollection. This is where I did the cross-device communication analysis. Having them all in one project meant the Genie plugin could decode WhatsApp, Facebook Messenger, Snapchat, and other apps across all four devices at once, so I could see how conversations on one phone connected to activity on another. Screenshots from this stage show Extraction Summary (4) in the tab bar. One thing to be aware of: the Analysed Data sidebar in EvidenceCollection shows combined totals from all four devices. Those numbers cannot be pinned to any single phone. confirms all four devices are present. One important note: the Analysed Data sidebar in this combined project shows totals from all four devices together - those counts cannot be attributed to any single device.

3.2 Hash Verification

Before putting anything into the combined project, I opened each image individually and checked its SHA-256 hash. This is not just a box-ticking exercise. If a hash does not verify, anything you pull from that image can be challenged in court as potentially tampered evidence. All four came back Verified - the hashes matched exactly, so the data had not been altered at any point between acquisition and my analysis [6] . The verified hash values are listed below and are also visible in the screenshots showing the Physical Analyzer hash verification dialogs (Figures 5–8).

Device	SHA-256 Hash (Verified)
Huawei P Smart – Emma	d5193dbf8246c09fdde73be8558343985ab24a2e1c142e4d64e16e2b6507e31f
Samsung A13 – Joe	0e585c4fe8160254253be515a16ff94b7fdf88b248b67d45cfdef8753a9a3195
Nokia C2 – Norman	a693656c260e339069756be8005346e97033d0ccf2f79add56cd69c9eade13ab
Ulefone Note 14	630724e2f8863adb9c4f7df1ab645e56c19a832d546fe7ab55b0cebf8ea7befd

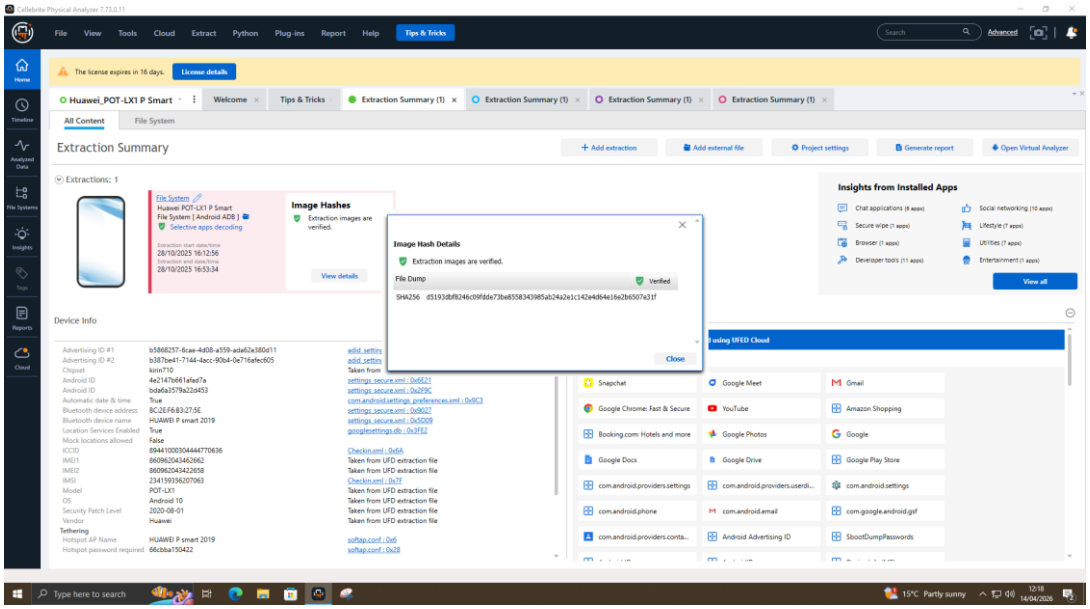

Figure 5: SHA-256 hash verified - Huawei P Smart (Emma) - individual standalone project

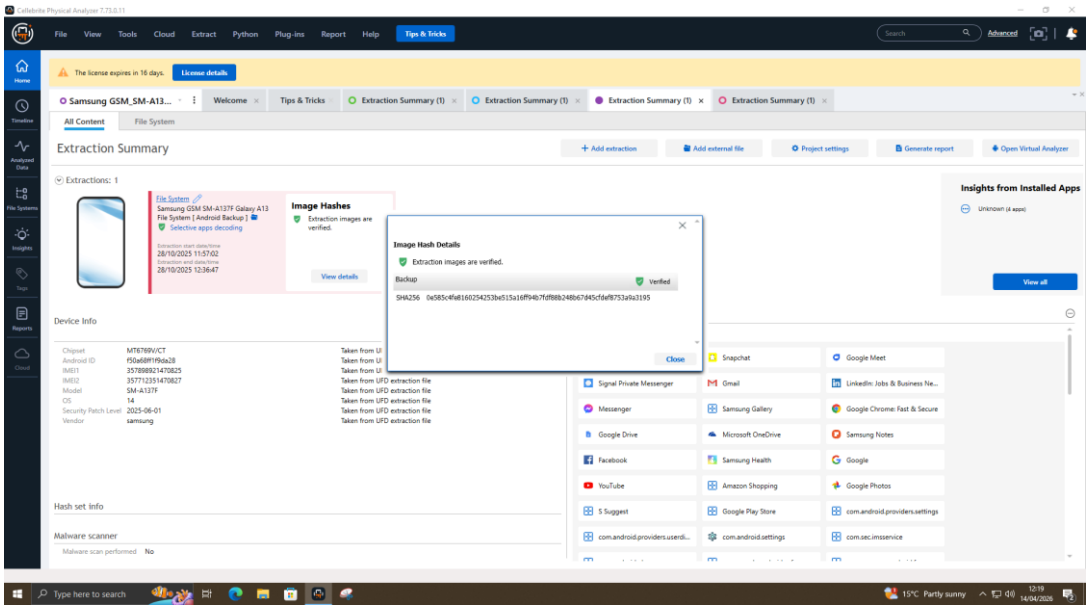

Figure 6: SHA-256 hash verified - Samsung Galaxy A13 (Joe) - individual standalone project

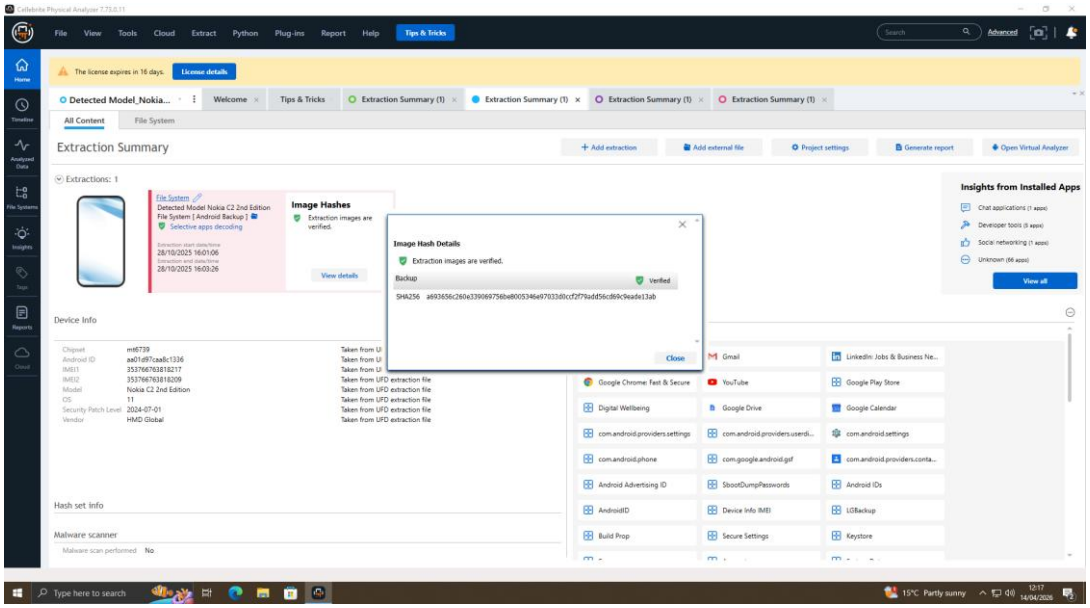

Figure 7: SHA-256 hash verified - Nokia C2 (Norman) - individual standalone project

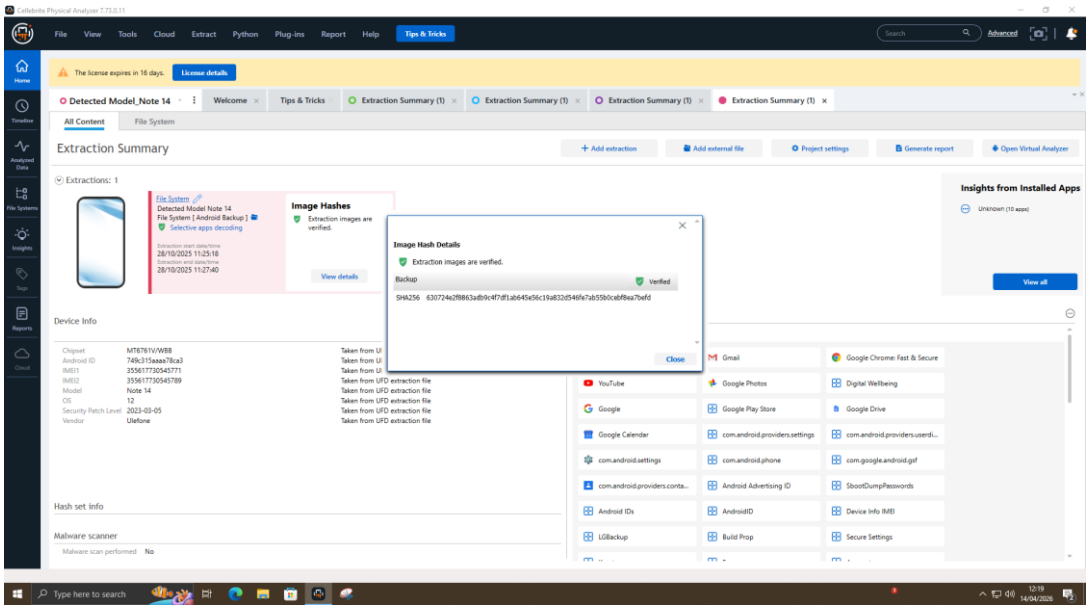

Figure 8: SHA-256 hash verified - Ulefone Note 14 - individual standalone project

4. Findings

4.1 WhatsApp - Emma and Joe

All the WhatsApp analysis was done in the combined EvidenceCollection project. One thread stood out immediately: a conversation between phone number 447917162788 and Joe. I traced 447917162788 back to Emma through the email account dovp59@gmail.com on the same Huawei device - that account is registered to Peter Dover. Facebook Messenger on the same phone was also under Peter Dover. So Emma was using a completely fake identity the entire

time. The email records show the Peter Dover account was created on 17 August 2024. Her first WhatsApp message to Joe came on 21 August - four days later. The alias, the burner Huawei, and the separate Lebara SIM were all ready before she made contact. That kind of advance setup is a textbook indicator of planned concealment [14].

The conversation ran from 21 August 2024 to 31 January 2025 - 27 messages across five months.

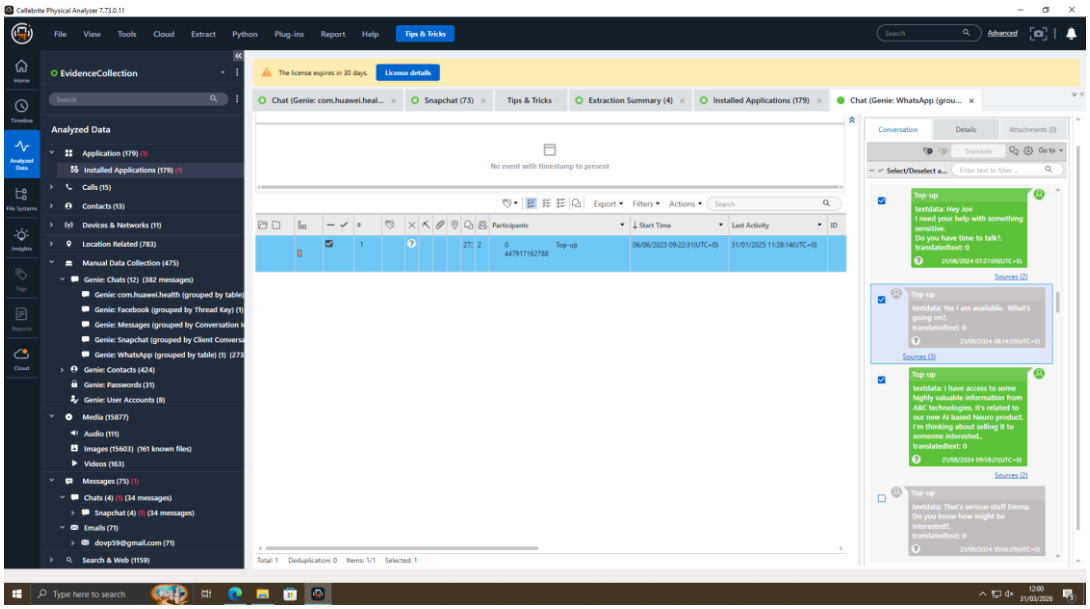

Figure 9: Opening WhatsApp messages - Emma approaches Joe on 21 August 2024

On 21 August Emma opened with: "Hey Joe I need your help with something sensitive." After Joe confirmed he was free, she said: "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." Joe replied: "That's serious stuff Emma." He confirmed he would help and said he was meeting clients at a hotel that same day.

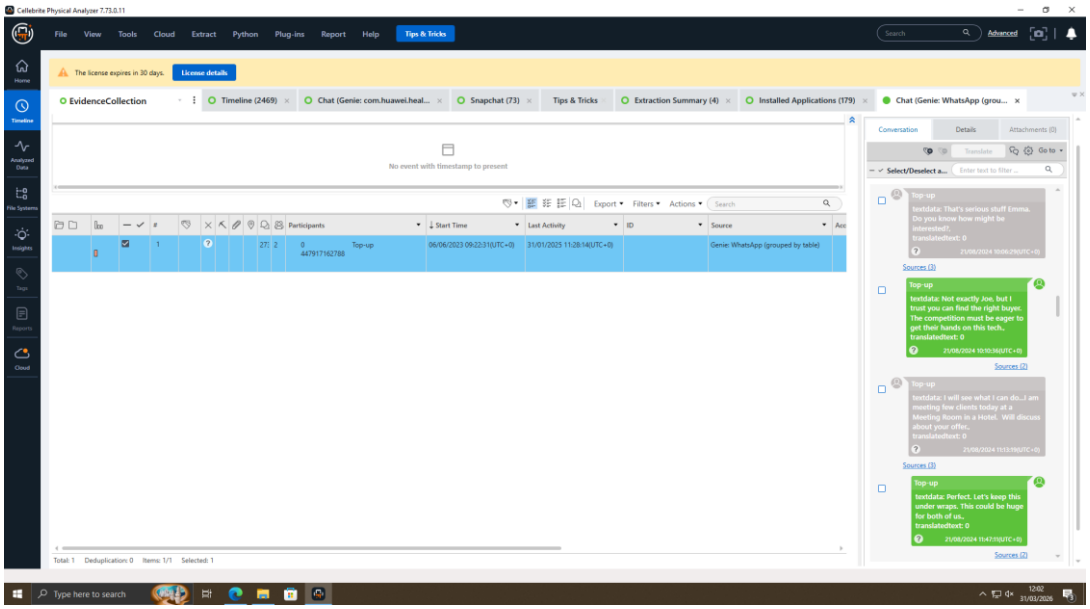

Figure 10: Joe agreeing to find a buyer and mentioning hotel meetings the same day

Emma replied: "Perfect. Let's keep this under wraps. This could be huge for both of us." By 26 August Joe updated her that the first meeting had not gone to plan but he had new contacts lined up and would keep her posted. Between August and November, the messages show a familiar pattern - Joe attending meetings, reporting back with partial progress, Emma growing progressively more impatient. By 20 November she was no longer hiding her frustration: "It is disappointing that no response from u. I have managed to find someone with whom I am meeting over the next weeks." The threat to look elsewhere was enough to get a response. Joe apologised and told her he was in final talks, meeting the client in Manchester that week.

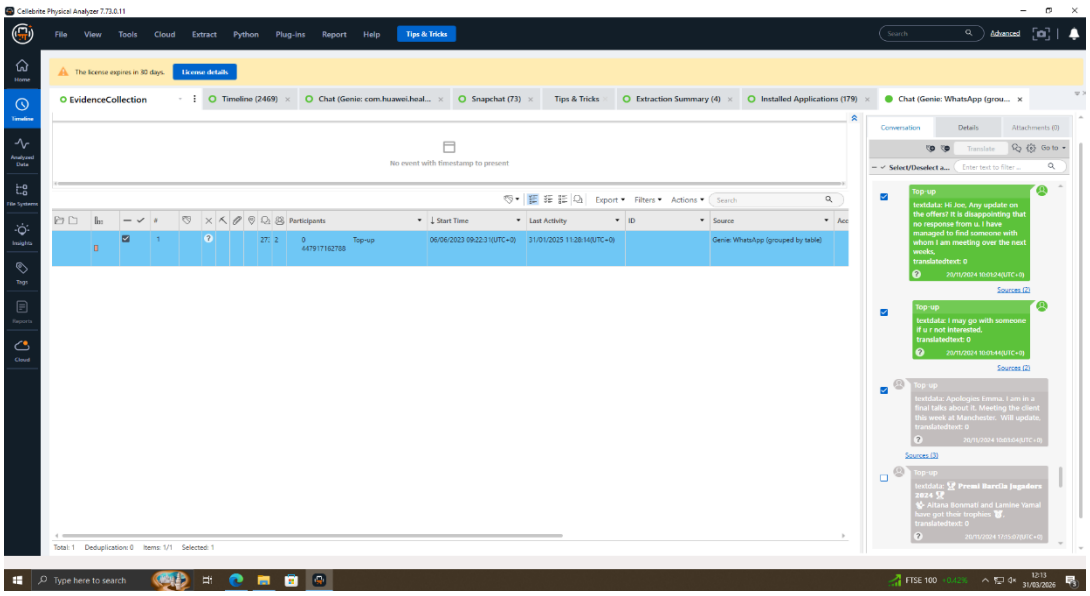

Figure 11: Emma pressing for progress in November 2024; Joe reports Manchester client meeting

The 31 January 2025 exchange is where the deal gets specific. Emma: "Any updates? Need to move fast." Joe: "Met the guy again. He's still playing slow, wants better numbers." Emma: "Waste of time. Should I reach others?" Joe: "No, he's serious. Wants a demo sample." Emma: "Impossible. But a detailed breakdown? Yes. How's the offshore arrangement?" Joe: "He's good with it. 5M secured."

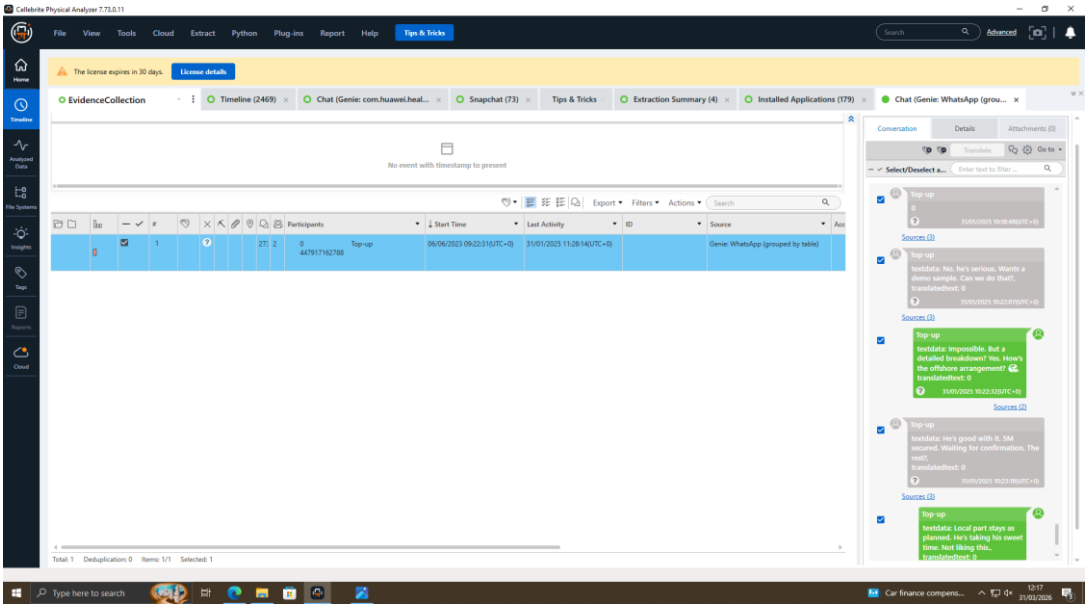

Figure 12: 31 January 2025 - 5M secured, offshore arrangement confirmed

Both figures are in the messages explicitly. Emma's use of the phrase "offshore arrangement" indicates the parties were discussing routing the payment to avoid straightforward detection [7]. Emma then said: "Local part stays as planned. He's taking his sweet time." Joe: "We can push harder." Emma: "I have others waiting." Joe's final message at 11:28:14: "We'll be watching...."

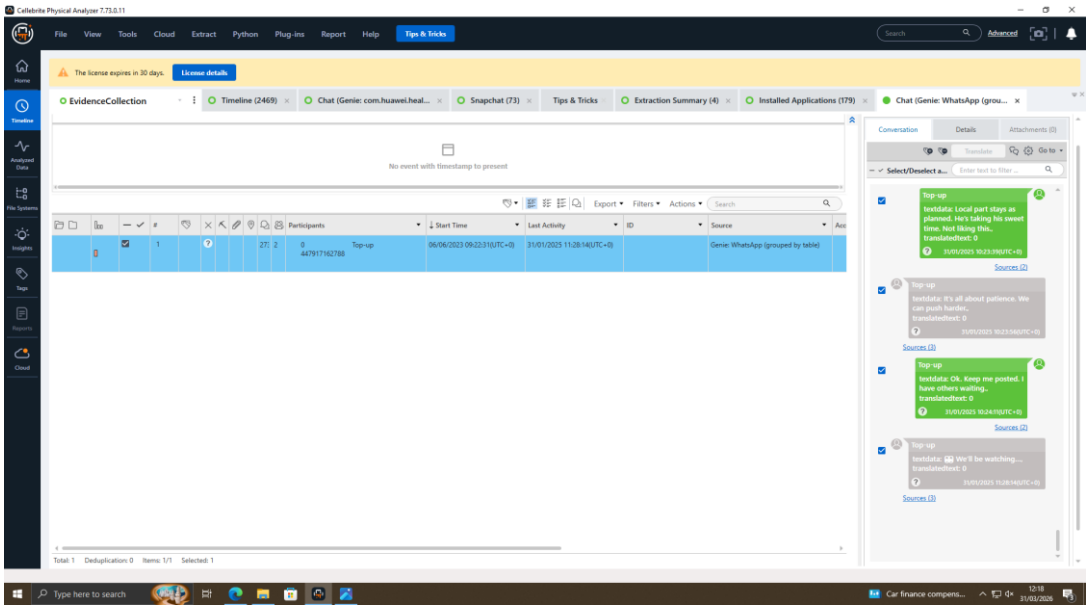

Figure 13: Final messages in the WhatsApp thread - 31 January 2025 at 11:28

4.2 Joe's Manchester Trip - Physical Corroboration

Joe told Emma on 20 November that he was meeting the client in Manchester that week. Two independent pieces of evidence from his Samsung Galaxy A13 confirm the trip actually happened.

First, a photograph in the camera roll - file 20241122_112158.jpg, dated 22/11/2024 at 11:21:58 - shows a National Rail train ticket reading WIG → MCZ: Wigan to Manchester, on 22 November 2024. That is exactly the week Joe said he was travelling.

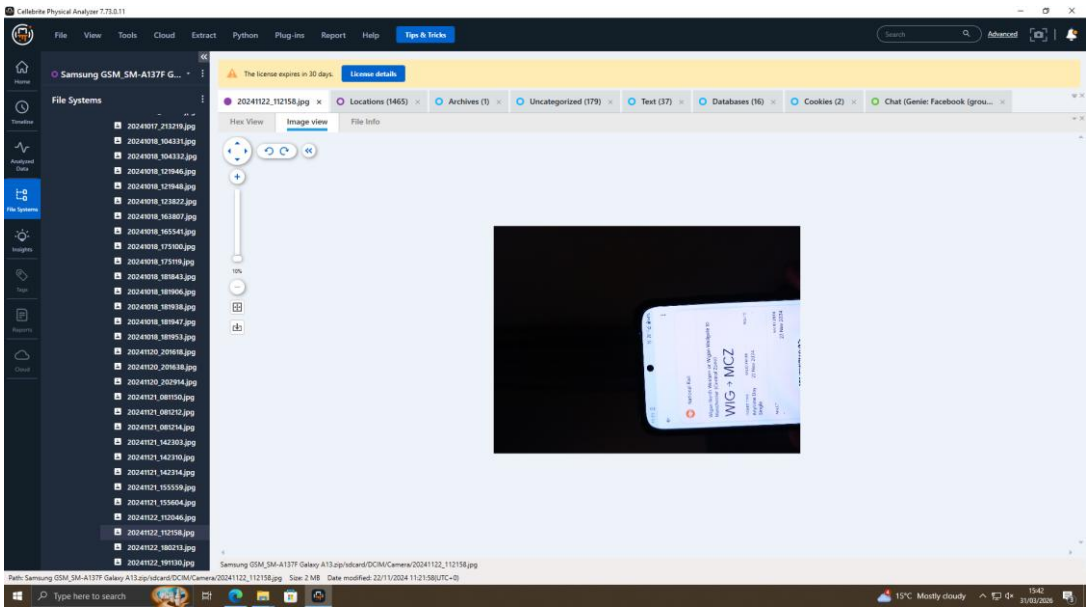

Figure 14: Train ticket photo from Joe's Samsung A13 - WIG to MCZ (Wigan to Manchester), 22 November 2024

Second, the Device Locations data from the Samsung shows 1,465 location records. Filtering for Manchester and sorting by date, two GPS fixes place Joe in Manchester city centre on 22 November: coordinates 53.543655, -2.627383 at 11:21:58 and 53.543624, -2.627375 at 11:20:48. That is not just Joe saying he went to Manchester. His phone was physically there.

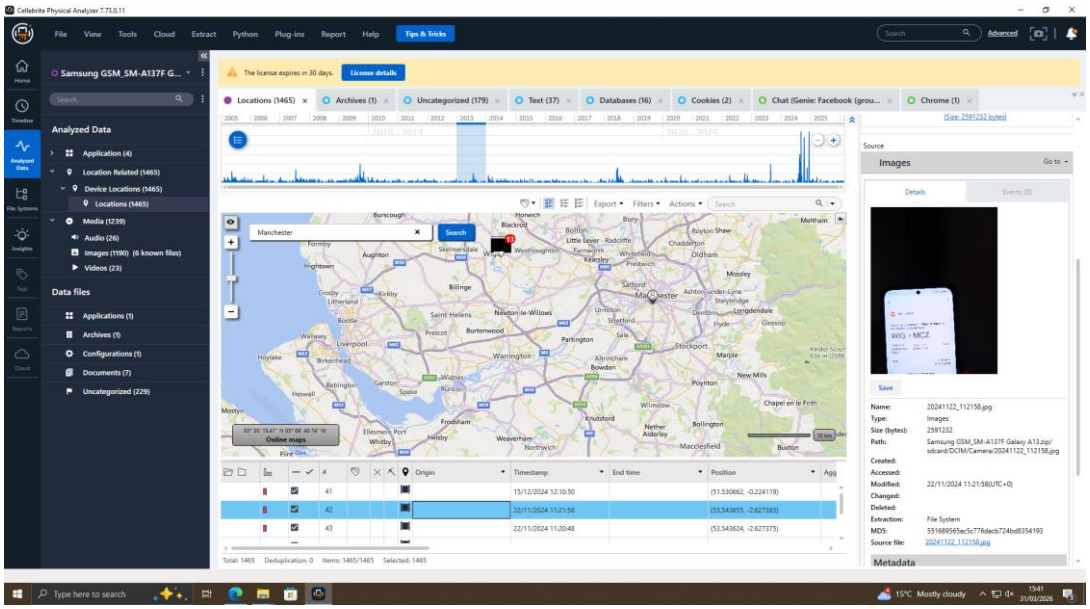

Figure 15: GPS data from Joe's Samsung A13 - device confirmed in Manchester city centre, 22 November 2024

4.3 Facebook Messenger - Peter Dover and Norman Smith

On the same day as the final WhatsApp exchange with Joe, a Messenger thread appeared between Peter Dover (Facebook ID 61565261156720) and Norman Smith (Facebook ID 61564326251951). Eight messages from 12:47 onwards - about an hour after the WhatsApp thread with Joe had closed at 11:28. Emma had just wrapped up with the intermediary and immediately opened a direct channel to the buyer.

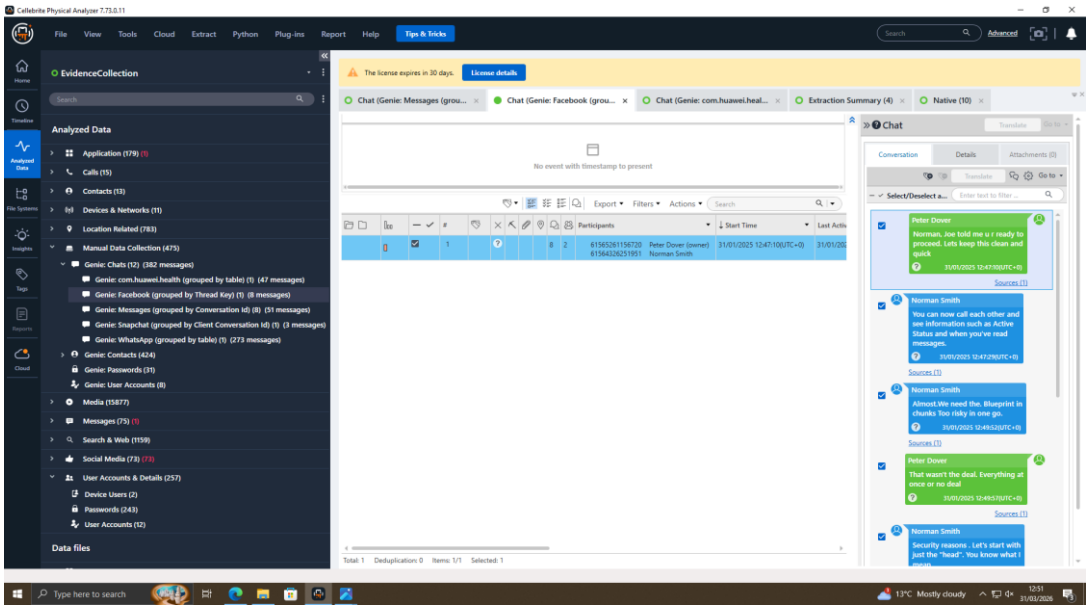

Figure 16: Facebook Messenger - Peter Dover and Norman Smith, 31 January 2025 from 12:47

Emma: "Norman, Joe told me u r ready to proceed. Lets keep this clean and quick." Norman: "Almost. We need the Blueprint in chunks. Too risky in one go." Emma: "That wasn't the deal. Everything at once or no deal." Norman: "Security reasons. Let's start with just the 'head'. You know what I mean."

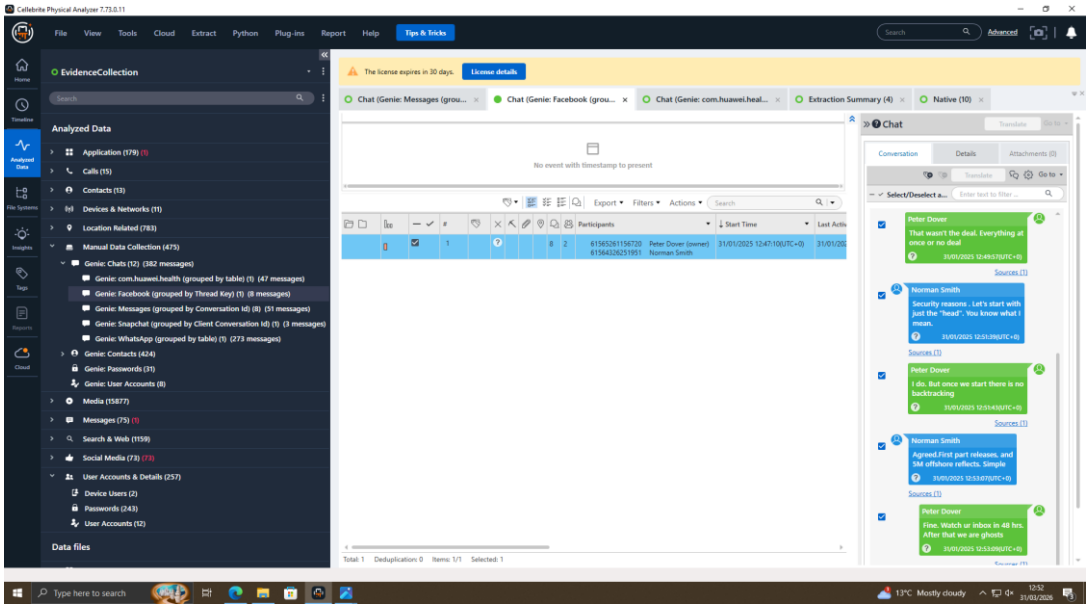

Figure 17: Norman requesting blueprint in chunks; 5M offshore agreed

Emma: "I do. But once we start there is no backtracking." Norman: "Agreed. First part releases, and 5M offshore reflects. Simple." Emma: "Fine. Watch ur inbox in 48 hrs. After that we are ghosts."

4.4 Snapchat

Three Snapchat messages were recovered from the Huawei device. Snapchat deletes messages server-side shortly after they are read, so most historical content is gone long before any device gets to a forensics lab [2]. The three fragments recovered did not relate to the patent transfer, but the app was in active use on the device.

4.5 Call Logs

The Huawei P Smart showed 15 recorded calls in total - mostly outgoing to two numbers: 00917907025586 (an international number) and 0447917162891 / 07917162891 (a UK number). The vast majority were marked Not Answered. One incoming call from +447917162891 on 17 August 2024 was recorded as Missed. What makes this interesting is the timing - the call activity concentrated in August 2024, the same narrow window as the opening WhatsApp exchanges between Emma and Joe. Voice contact was clearly being attempted alongside the written negotiation, though apparently without success. The number 07917162891 also appears in some of the email notifications recovered from the device, linking it further to the Peter Dover identity and the communication network surrounding this case.

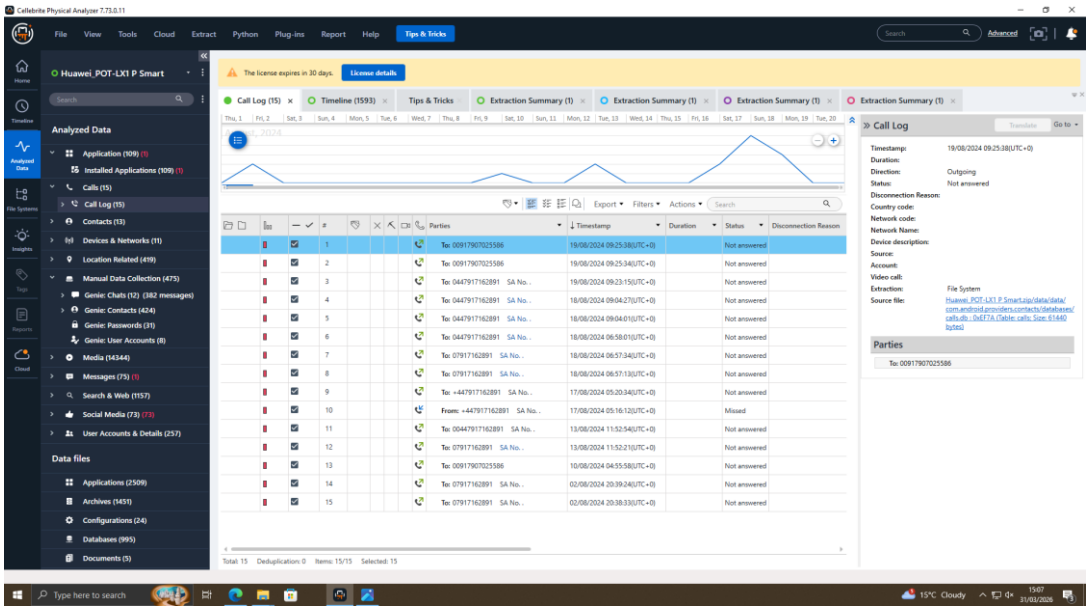

Figure 18: Call log from Huawei P Smart - 15 records, mostly unanswered, August 2024

4.6 Email Analysis

71 emails were recovered from dovp59@gmail.com on the Huawei device. The earliest, dated 17 August 2024, was addressed to "Peter" and concerned setting up the Google Account on the Huawei - pinning the Peter Dover alias creation to exactly four days before Emma first messaged Joe on 21 August. That gap is significant. It shows Emma did not reach out to Joe on impulse and then set up the alias afterwards; she had the infrastructure in place before she made

first contact. Several subsequent emails in the inbox referenced the mobile number 07917162788 - the same number linked to the WhatsApp conversations throughout this investigation - confirming the number was actively registered under the Peter Dover identity. Facebook notification emails in the inbox also mentioned Joe by name, which is a further thread connecting the email account to the wider network of activity documented elsewhere in the evidence.

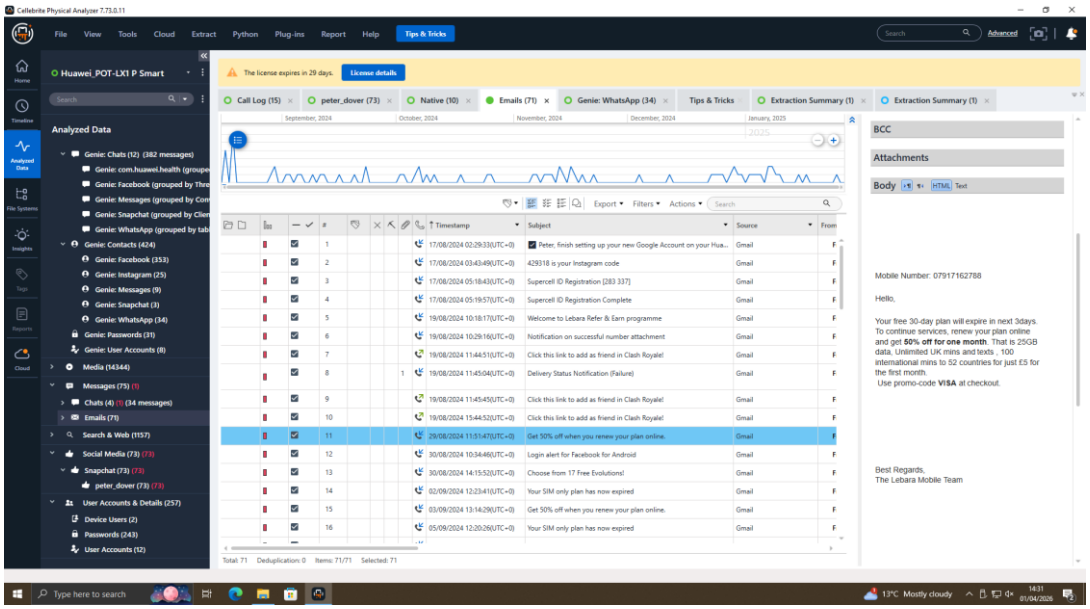

Figure 19: Email list from dovp59@gmail.com - earliest dated 17 August 2024

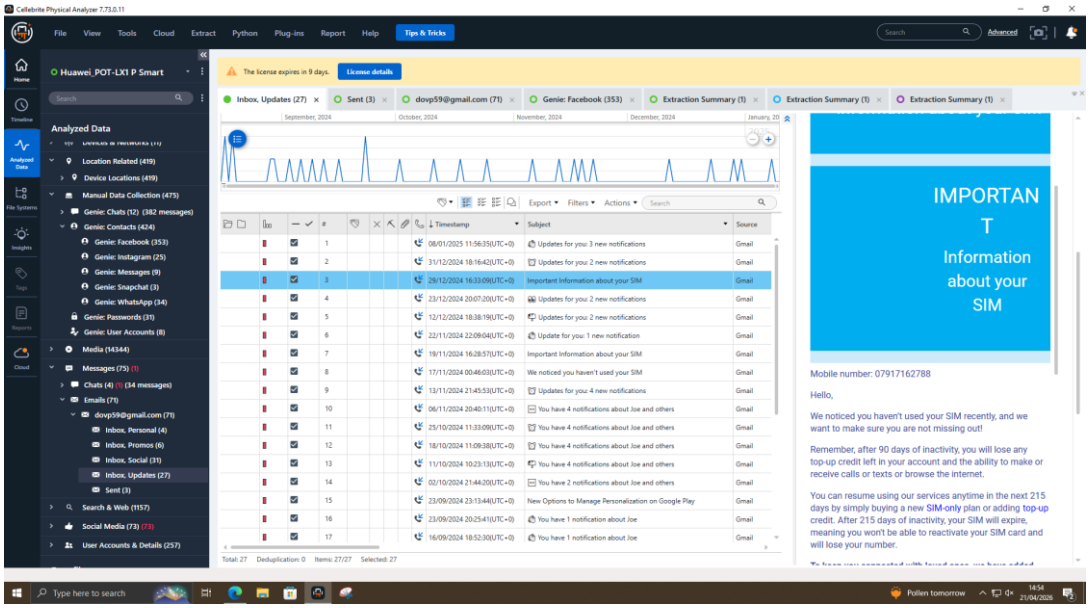

Figure 20: Email inbox - SIM notifications for 07917162788 and Facebook updates mentioning Joe

4.7 Device Extraction Details

The Nokia C2 image (Norman's device) was extracted on 28 October 2025, 16:01:06 to 16:03:26, via File System (Android Backup). Device info: chipset mt6739, Android 11, security patch 2024-07-01, HMD Global, IMEI1 353766763818217. UFD data integrity: Intact. The screenshot below was captured while the Nokia image was loaded within the combined EvidenceCollection project alongside all four devices - therefore the data counts visible in the Analysed Data sidebar belong to all four devices combined and cannot be assigned to Norman's Nokia alone.

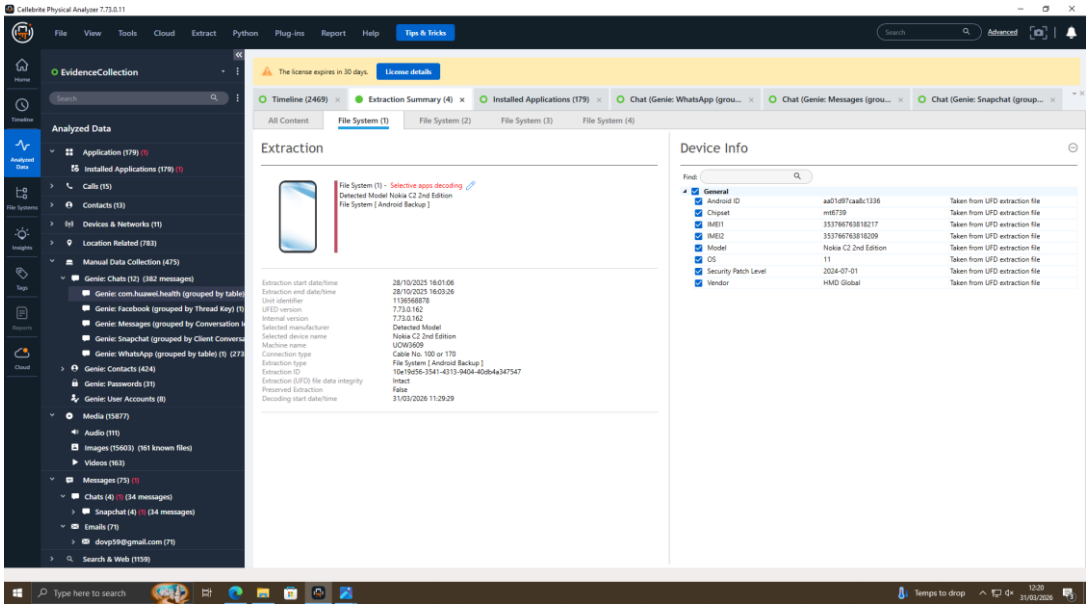

Figure 21: Nokia C2 extraction details - device info Nokia-specific; sidebar counts are from the combined project

Joe's Samsung Galaxy A13 was extracted on 28 October 2025, 11:57:02 to 12:36:47, also via Android Backup. Installed apps included Signal Private Messenger, Facebook Messenger, Snapchat, and WhatsApp. Hash verified as intact.

8.8 Media and Location Data - Norman's Nokia C2

Opening Norman's Nokia image in a standalone project showed 117 images with GPS EXIF data. One photo taken on 04/09/2024 at 12:38:04 recorded coordinates 51.625252, -3.996134 - Physical Analyzer placed this in the Swansea area. Camera metadata confirmed Nokia C2 2nd Edition by HMD Global. These counts and coordinates are Nokia-specific, confirmed by the standalone project view.

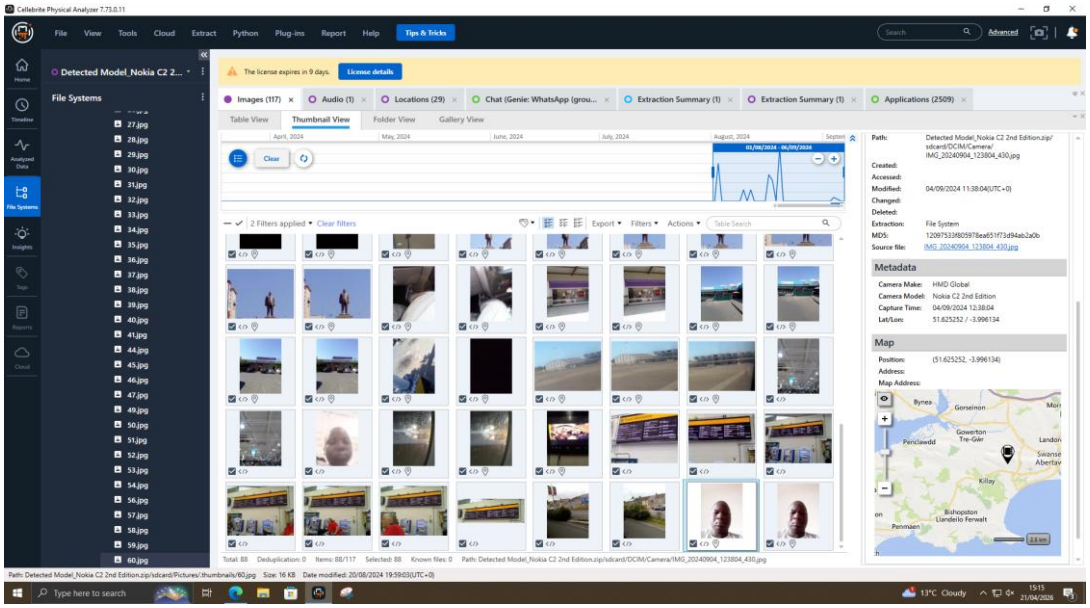

Figure 22: Nokia C2 standalone project - 117 images; EXIF GPS places one photo in Swansea, September 2024

5. Reconstructed Timeline

Date / Time	Event
17 Aug 2024	Peter Dover Gmail and Lebara SIM created on Huawei P Smart
17–19 Aug 2024	Multiple outgoing calls from Huawei, mostly unanswered
21 Aug 2024	Emma messages Joe on WhatsApp; discloses patent data access and proposes a sale
21 Aug 2024	Joe agrees to find a buyer; attends hotel meetings the same day
26 Aug 2024	Joe updates Emma: first meeting failed but has new contacts
20 Nov 2024	Emma presses for updates; Joe says he is meeting client in Manchester that week
22 Nov 2024 11:20–11:22	Joe physically in Manchester: GPS confirms 53.543655, -2.627383; train ticket WIG→MCZ photographed same day
31 Jan 2025 ~10:15–11:28	WhatsApp: demo sample requested; 5M secured; offshore arrangement confirmed
31 Jan 2025 12:47	Facebook Messenger: Emma contacts Norman directly; blueprint in chunks discussed; 5M offshore agreed; 48-hour deadline set

6. Suspect Profiling

6.1 Emma - Primary Suspect

Emma set up the Peter Dover alias on a dedicated Huawei P Smart - Gmail account, UK Lebara SIM, all of it - four days before she messaged Joe for the first time. She was the person who started the scheme, identified the buyer channel, set the financial terms, kept pressure on Joe across five months of stop-start negotiation, and eventually cut him out entirely to contact Norman directly on the final day. Every stage of the operation traces back to her decision-making. Her messages reference secrecy from the very first exchange, a 5M payment figure, offshore routing of proceeds, a 48-hour transfer window, and plans to go ghosts once the deal concluded. The alias and its supporting infrastructure were fully operational before first contact - confirmed by the 17 August email timestamp - making this a premeditated operation rather than an opportunistic one [14].

6.2 Joe – Intermediary

Joe's number is 7476538686 per recovered contact data from the Samsung A13. The WhatsApp messages show him actively working the deal across several months attending hotel meetings, making the Manchester trip on 22 November 2024, chasing contacts, reporting back to Emma with updates, and eventually relaying both the demo sample request and the 5M offshore confirmation. He was not a passive message-passer; he was running the commercial side of the negotiation on Emma's behalf. His Manchester trip is now independently corroborated from two sources on the same device: GPS coordinates placing him physically in Manchester city centre at 11:20–11:22 on 22 November, and a train ticket photo in his camera roll showing WIG → MCZ on that exact date. Signal Private Messenger was also installed on the Samsung A13 alongside WhatsApp, Facebook Messenger, and Snapchat, though no Signal content was recovered under the backup extraction method.

6.3 Norman Smith - Buyer

Norman communicated with Emma through Facebook Messenger on 31 January 2025. His messages show he was already briefed on what the Blueprint was and had thought through the security risk of transferring it all at once before this conversation began. He proposed sending it in chunks, agreed to the 5M offshore payment, and specified starting with just the head of the patent data. His Nokia C2 image contains GPS coordinates placing him in the Swansea area in September 2024. The forensic evidence does not establish Norman's employer or organisational affiliation - determining that would require investigation beyond the four device images provided, including financial records and corporate background checks.

7. Challenges and Limitations

The Educational licence flagged Email and Instant Message extraction as NOT SUPPORTED on some devices. This is a licence limitation, not a device problem - a full commercial Cellebrite licence includes direct IM extraction that the educational version does not. Chat data in this investigation was recovered through the Genie plugin and selective app decoding within Physical Analyzer, which produced usable and detailed results. That said, a commercial licence would probably recover a wider range of message metadata and content than the Genie plugin managed [11].

Only three Snapchat messages survived on the Huawei device. Snapchat's server-side deletion of messages shortly after they are read is a well-documented challenge in mobile forensics - most of a conversation is gone long before a phone ever reaches a lab [2]. The three fragments recovered are not necessarily representative of all Snapchat communications that took place on that device. The absence of more messages should not be read as evidence that more did not exist. Signal Private Messenger was also installed on Joe's Samsung A13, but produced no recoverable content under the backup extraction method. A full file system or physical-level extraction on a rooted device might yield more from both applications.

8. Conclusion

The four device images tell one consistent story, and the pieces corroborate each other. In Joe's case, two completely independent sources on his own phone confirm what he told Emma in the messages. Emma spent four days building a fake identity before she even contacted Joe, then pushed the deal for five months. On 31 January 2025, both conversation threads landed on the same result: 5M offshore, blueprint sent in chunks, 48 hours to deliver, then both sides disappear. The same 5M figure showing up independently in two separate conversations - WhatsApp with Joe and Messenger with Norman - within sixty minutes of each other is not a coincidence. Emma was running both sides of this deal at the same time, on the same day. Joe's Manchester trip is not just something he claimed in a message anymore. His GPS puts him there on 22 November, and a photo of a Wigan-to-Manchester train ticket in his camera roll confirms it. All four image hashes verified as intact.

The device evidence backs up the allegation that Emma tried to sell proprietary patent data through Joe to Norman. What it does not tell us is who Norman actually works for, what his full identity is beyond the Facebook profile, or the complete financial picture. Answering those

questions would take financial records, corporate background checks, and network analysis - none of which are within the scope of four phone images.

9. Recommendations

Quantum Tech's legal team should review these recovered communications to assess whether the content supports formal complaints to law enforcement regarding Emma, Joe, and Norman Smith. The evidence shows explicit discussion of selling proprietary technical data, offshore payment arrangements, and deliberate plans to cut contact once the transfer was complete. Emma's access to the QT-AI-2025 patent database should be revoked immediately if it has not been already, and a full audit of the database access logs should be conducted to establish whether any files were actually downloaded or exfiltrated before the devices were seized [9].

Law enforcement should look at getting production orders for dovp59@gmail.com and the Facebook accounts tied to Peter Dover and Norman Smith. The offshore payment arrangement that both conversations reference is worth a financial investigation on its own - following the money might reveal who else is involved. Norman Smith's real identity and who he works for still need to be established. And any USB devices or cloud storage that Emma had access to should be examined. The 48-hour inbox delivery she mentioned in the Messenger conversation suggests the blueprint was going to be sent digitally, and there may still be traces of the transfer method in those locations.

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. doi:10.1016/j.diin.2017.09.002.

[3] Ayers, R., Brothers, S. and Jansen, W. (2014) Guidelines on Mobile Device Forensics, NIST Special Publication 800-101 Rev. 1. Gaithersburg, MD: NIST. doi:10.6028/NIST.SP.800-101r1.

[4] Carrier, B. (2005) File System Forensic Analysis. Upper Saddle River, NJ: Addison-Wesley.

[5] Casey, E. (2011) Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd edn. Amsterdam: Academic Press.

[6] ISO (2012) ISO/IEC 27037:2012 - Information Technology - Security Techniques - Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. Geneva: ISO.

[7] Jahankhani, H., Kendzierskyj, S. and Chelvachandran, N. (2021) Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity. Cham: Springer. doi:10.1007/978-3-030-35746-7.

[8] Gogolin, G. (2010) 'The digital crime tsunami', Digital Investigation, 7(1-2), pp. 3-8. doi:10.1016/j.diin.2010.07.001.

[9] NIST (2020) NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations. Gaithersburg, MD: NIST. doi:10.6028/NIST.SP.800-53r5.

[10] Quick, D. and Choo, K.K.R. (2014) 'Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata?', Digital Investigation, 11(3), pp. 220–233. doi:10.1016/j.diin.2014.05.011.

[11] Rathod, D. (2017) 'Mobile forensics: An overview, tools, future trends and challenges from law enforcement perspective', International Journal of Scientific and Engineering Research, 8(9), pp. 1462–1471.

[12] Sammons, J. (2015) The Basics of Digital Forensics. 2nd edn. Waltham, MA: Syngress.

[13] Garfinkel, S.L. (2010) 'Digital forensics research: The next 10 years', Digital Investigation, 7, pp. S64-S73. doi:10.1016/j.diin.2010.05.009.

[14] Nelson, B., Phillips, A. and Steuart, C. (2015) Guide to Computer Forensics and Investigations. 5th edn. Boston, MA: Cengage Learning.

[15] Zawoad, S. and Hasan, R. (2015) 'Digital forensics in the age of big data: Challenges, approaches, and opportunities', Proceedings of the IEEE 17th International Conference on High Performance Computing and Communications, pp. 1320-1325. doi:10.1109/HPCC-CSS-ICESS.2015.170.