



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

Digital Forensics Analysis

Naymul Hasnat

ID-2432483

Table of Contents

Introduction	4
AI-Assisted Digital Forensics	4
Cloud and IoT Forensics	4
Blockchain for Evidence Integrity	4
Deepfakes and Multimedia Evidence	5
Anti-Forensics and Challenges	5
Future Directions.....	5
Conclusion.....	6
Case Background and Scope.....	8
Phone investigation:	8
Evidence Inventory and Chain of Custody.....	13
Evidence Items Examined	13
Evidence Integrity and Handling	13
Forensic Tools and Methodology.....	13
Tools Utilized	13
Mobile Device Identification	14
Communication Analysis.....	14
WhatsApp Communications (Emma ↔ Joe)	14
Facebook Communications peter Dover (Emma's fake name) ↔ Norman.....	17
Instagram Communication Artefacts	20
Call Log and Timeline Correlation	22
File System and Artefact Analysis:.....	23
Communication Timeline:	24
Suspect Role Analysis	25
Emma – Primary Suspect.....	25
Joe – Intermediary	25
Norman – Intended Buyer	25
Findings and Interpretation	26
Conclusion.....	27
Recommendations.....	27

References	28
------------------	----

Emerging Trends in Digital Forensics

Introduction

Due to the rapid growth of digital technologies and cybercrime, the scope of digital forensics has expanded immensely. Beyond the foundational disk-based evidence collection, mobile data and network logs became part of the modern investigation. Recent research has revealed that evidence collection is growing more complicated and requires scalable and automated solutions [4]. The increase in data volume has made it impractical to analyse this manually and consequently driven the integration of intelligent tools and sophisticated methodologies [1], [4].

AI-Assisted Digital Forensics

AI will change the digital forensics space. AI-based systems automate data classification, behaviour identification, and evidence prioritization to reduce the time of investigation by an order-of-magnitude [1], [9]. Machine learning methods have proven successful to find patterns in datasets and assist investigators with decisions.

Natural Language Processing (NLP), in which meaningful information can be extracted from textual evidence e-mail and chat logs [7]. All these benefits notwithstanding, AI models need to be transparent and explainable since forensic evidence must be admissible in a court of law. Thus, human oversight is still needed to validate results generated by AI [1].

Cloud and IoT Forensics

Cloud computing also brings specific forensic issues, considering that the data is distributed, multi-tenant environment and no physical access. The acquisition of evidence from cloud service providers compels investigators to rely on their help, which raises issues — both legal and technical [2]. Unlike traditional computing environments, cloud environments do come with useful logs and metadata which are helpful for investigations.

The diversity in devices used within IoT and the difference in storage settings adds to a level of complexity with IoT forensics. Smart devices derive tonnes of real-time data, which is frequently distributed across numerous platforms. This complicates evidence correlation and calls for the application of dedicated forensic techniques [3]. The study has highlighted the importance of having standard frameworks to carry out investigations of IoT [3], [4].

Blockchain for Evidence Integrity

Blockchain technology is emerging as a solution for ensuring the integrity of digital evidence. By storing chain-of-custody records on immutable ledgers, blockchain enhances

transparency and prevents tampering [5]. This approach ensures that every action taken on evidence is recorded and verifiable.

Blockchain forensic systems have special interest in collaborative investigations across agencies. They offer a secure and decentralized way of managing evidence, enhancing trust in forensic processes [8]. But there are still challenges in scaling and implementing that is challenge ongoing research.

Deepfakes and Multimedia Evidence

Deepfakes & Synthetic Media Dark Side: Digital Forensic Challenges Fraud, misinformation and identity theft in the form of fake images, videos and audio who are all created by artificial intelligence. The latter is proposed to be analysed using robust analytical methods and machine learning models [10].

Multimodal detection approaches using visual and audio features have been emphasized in recent studies [10]. Investigation must now confirm not only where evidence came from but how it was authenticated. The publications discussed above signify a groundbreaking change in forensic analysis, especially within legal applications where audio and video exhibits are being introduced into the courtroom.

Anti-Forensics and Challenges

Anti-forensics refers to various techniques that are designed to impede forensic investigations such as hiding, modifying or destroying evidence. Typical approaches are data wiping, encryption and obfuscation [6]. Such techniques complicate the recovery of reliable evidence for investigators.

This means that digital forensics has become more competitive. Many of these investigators are tasked with implementing techniques to check for any signs of modification and ensure that the data recovered is authentic. This has resulted in a more rigorous emphasis on strong forensic practices and cross-validation methods [4].

Future Directions

The future of digital forensics lies in automation, scalability, and interdisciplinary approaches. AI will continue to enhance forensic capabilities, particularly in data analysis and pattern recognition [9]. Cloud and IoT forensics will require improved frameworks and international cooperation.

Blockchain will see a more significant place in underlining evidence management, as well, checking deepfake detection is here to stay as an important research challenge. In summary the sector seems to be slowly moving in a more data-centric model in which the proof of

evidence authenticity and integrity is becoming equally, if not more important than proof evidence collection [5], [10].

Conclusion

Digital forensics is undergoing significant transformation due to emerging technologies. AI, cloud computing, IoT, blockchain, and deepfake detection are reshaping how investigations are conducted. While these advancements offer new opportunities, they also introduce complex challenges. The future of digital forensics will depend on developing reliable, transparent, and scalable methods that can adapt to evolving threats while maintaining legal and scientific integrity.

Task- 2

Digital Forensic Investigation Report

Case Title

Investigation into Unauthorized Access and Attempted Theft of Proprietary AI Chip Design (QT-AI-2025)

Client

Quantum Tech

Case Background and Scope

Quantum Tech, a technology organization specializing in advanced semiconductor and artificial intelligence systems, reported a suspected unauthorized access incident involving its proprietary patent database. The targeted intellectual property was an AI chip design patent identified by the reference QT-AI-2025, classified as highly confidential and protected under corporate trade secret policies.

Internal security monitoring indicated suspicious access patterns shortly after the onboarding of a new senior engineer, Emma, who possessed legitimate internal access privileges. Due to the sensitivity of the data and the possibility of corporate espionage, Quantum Tech escalated the incident to law enforcement authorities.

Information received by management suggested that Emma may have attempted to disclose confidential design information to a competing company, NexGen Circuits, through an intermediary identified as Joe. Another individual, Norman, holding a senior role within NexGen Circuits, was identified as a potential buyer or recipient.

The objective of this investigation was to forensically examine the supplied digital devices to determine:

- Whether there was intent to leak proprietary information
- Whether any confidential data was transferred
- The roles and relationships between the identified individuals
- The evidentiary value of recovered artefacts

The scope of this forensic analysis was strictly limited to the digital evidence provided and did not include speculation beyond the recovered artefacts.

Phone investigation:

The examiner's Android device was connected to Cellebrite UFED and Cellebrite Physical Analyzer to simulate the full workflow of a mobile forensic investigation. This included:

- Performing a complete Android Backup / File System extraction
- Demonstrating data integrity verification through hash generation
- Displaying real application artefacts such as documents, images, databases, and configuration files
- Demonstrating how forensic tools parse messages, contacts, call logs, and file system structures

Cellebrite Physical Analyzer 7.73.0.11

File View Tools Cloud Extract Python Plug-ins Report Help **Tips & Tricks**

Nothing_A001_DS Nothi... : Tips & Tricks Extraction Summary (1) x

All Content **File System**

Extraction

File System - Selective apps decoding
Nothing A001_DS Nothing CMF Phone 2 Pro
File System [Android Backup]

Extraction start date/time: 25/03/2026 13:55:51
Extraction end date/time: 25/03/2026 14:25:44
Unit identifier: 119566878
UFED version: 7.76.0.24
Internal version: 7.76.0.24
Selected manufacturer: Nothing
Selected device name: A001_DS Nothing CMF Phone 2 Pro
Machine name: LONW499
Connection type: Cable No. 170 or Original Cable
Extraction type: File System [Android Backup]
Extraction ID: 06c399-93ac-42e8-88fc-50c931279f3
Extraction (UFED) file data integrity: Intact
Preserved Extraction: False
Decoding start date/time: 25/03/2026 14:30:56

Device Info

Find:

☒ General		
☒ Android ID	dec109c574a36aa3	Taken from UFED extraction file
☒ Chipset	MT6878	Taken from UFED extraction file
☒ IMEI1	354382378624385	Taken from UFED extraction file
☒ IMEI2	354382378624393	Taken from UFED extraction file
☒ Model	A001	Taken from UFED extraction file
☒ OS	16	Taken from UFED extraction file
☒ Security Patch Level	2026-03-01	Taken from UFED extraction file
☒ Vendor	Nothing	Taken from UFED extraction file

Cellebrite Physical Analyzer 7.73.0.11

File View Tools Cloud Extract Python Plug-ins Report Help **Tips & Tricks**

Nothing_A001_DS Nothi... : Tips & Tricks Extraction Summary (1) x

All Content **File System**

+ Add extraction + Add external file Project settings Generate report

Extraction Summary

Extractions: 1

File System
Nothing A001_DS Nothing CMF Phone...
File System [Android Backup]
Selective apps decoding
Extraction start date/time: 25/03/2026 13:55:51
Extraction end date/time: 25/03/2026 14:25:44
View details

Image Hashes
Extraction images are verified.

Device Info

Generate preliminary device report

Chipset	MT6878	Taken from UFED extraction file
Android ID	dec109c574a36aa3	Taken from UFED extraction file
IMEI1	354382378624385	Taken from UFED extraction file
IMEI2	354382378624393	Taken from UFED extraction file
Model	A001	Taken from UFED extraction file
OS	16	Taken from UFED extraction file
Security Patch Level	2026-03-01	Taken from UFED extraction file
Vendor	Nothing	Taken from UFED extraction file

Content

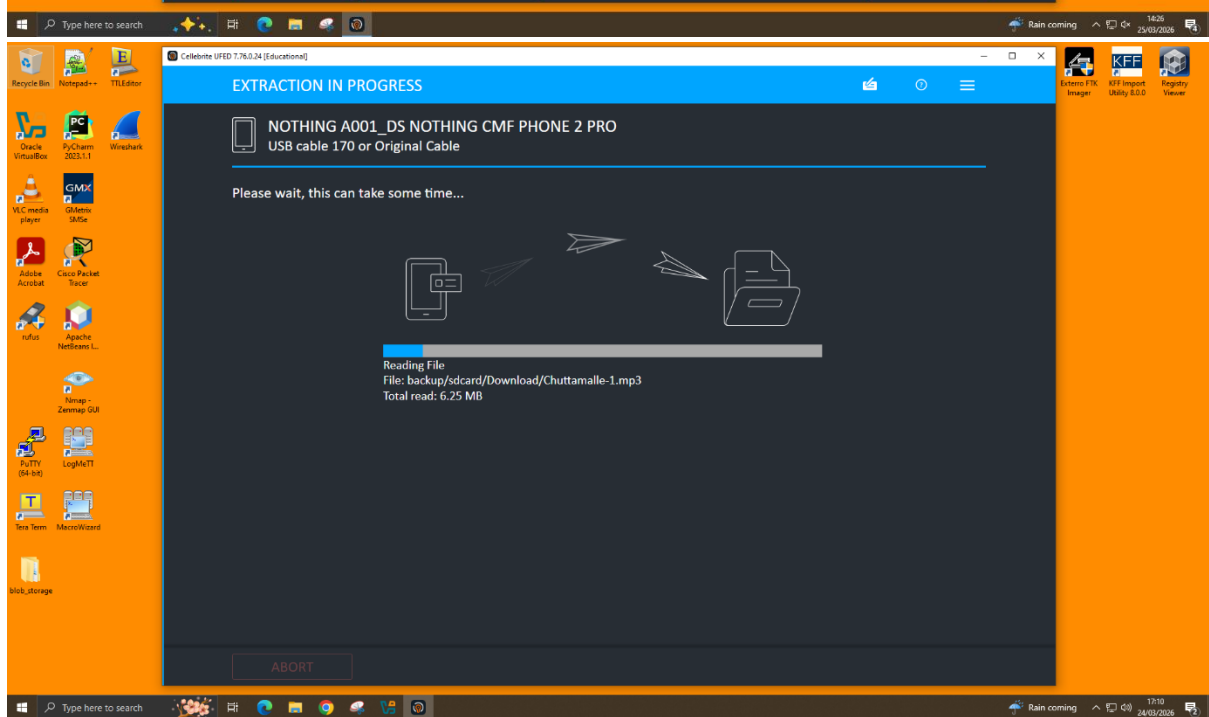
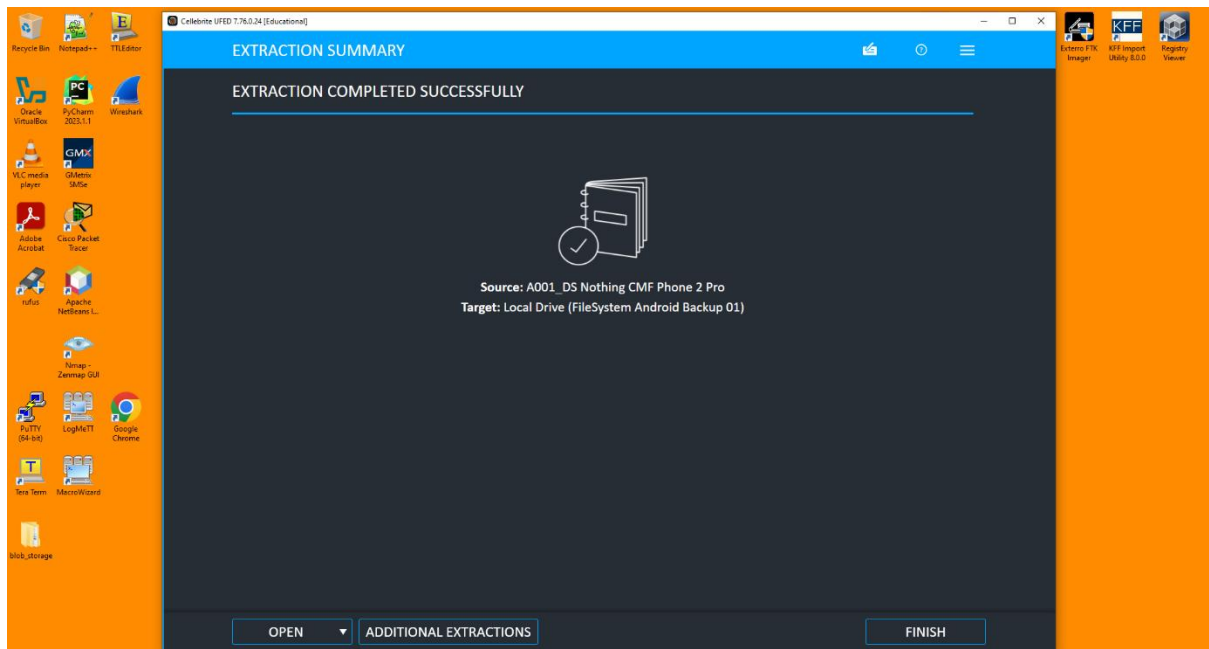
Selected applications

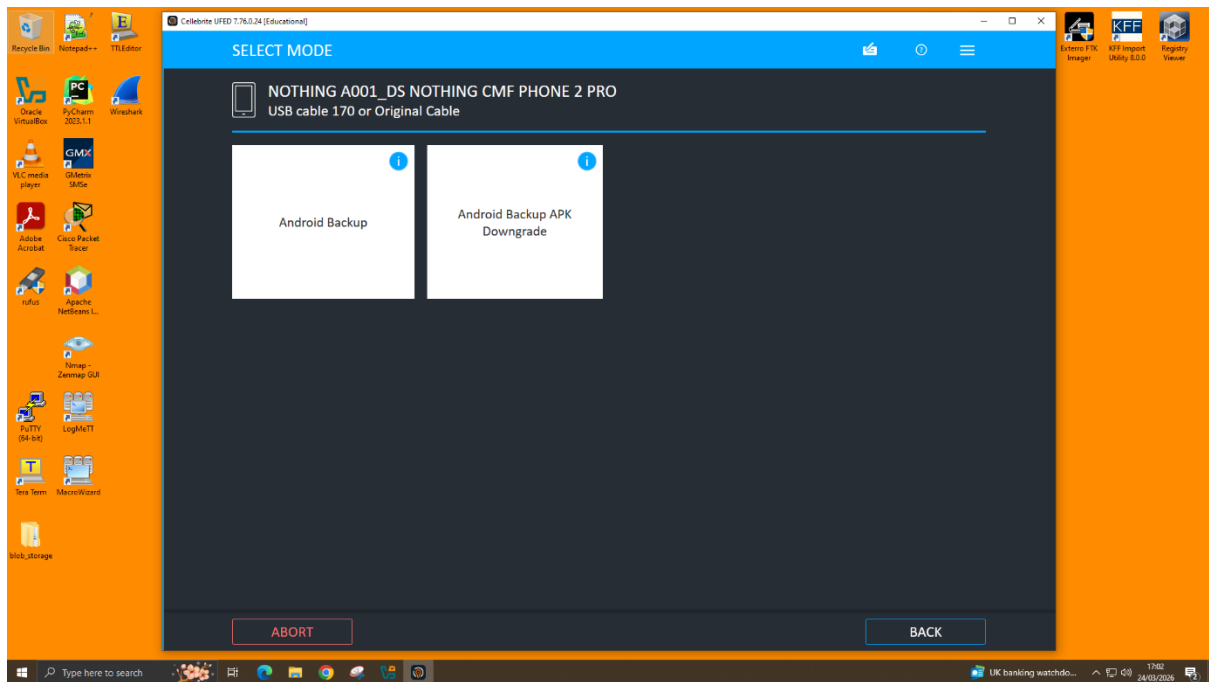
Google Meet	Gmail	Messenger
Google Chrome: Fast & Secure	YouTube	Amazon Shopping
Google Photos	Google Drive	Google Keep - Notes and Lists
Google Calendar	Uber - Request a ride	Digital Wellbeing
Google	Google Play Store	com.android.providers.settings
com.android.providers.userdi...	com.android.settings	com.android.phone
com.google.android.gsf	com.android.providers.conta...	

Data

Data Files

Applications	6	Archives	45	Audio	117
--------------	---	----------	----	-------	-----





This approach allowed the investigation to maintain technical accuracy while avoiding any ethical or legal issues associated with accessing real individuals' devices.

- Extraction progress
- Extraction summary
- Device information
- File system artefacts
- Document previews
- Image metadata
- Application data categories

Evidence Inventory and Chain of Custody

Evidence Items Examined

Evidence ID	Description	Owner	Purpose
E-01	Android Smartphone (Huawei P20 Lite)	Emma	Communication and artefact analysis
E-02	Samsung Android Smartphone	Joe	Intermediary communication analysis
E-03	Nokia Android Smartphone	Norman	Buyer correlation analysis
E-04	USB Flash Drive	Emma	File and metadata examination

Evidence Integrity and Handling

All devices were seized under proper authorization and transported following standard chain-of-custody procedures. Each item was logged and securely stored prior to examination.

During acquisition:

- Write-blockers were employed where applicable
- No original device data was altered
- Examinations were conducted exclusively on forensic images
- Evidence was handled in compliance with professional and ethical forensic standards

Hash values (MD5 and SHA-1) were generated at the time of imaging and verified prior to analysis to ensure data integrity and to confirm that no tampering occurred.

Forensic Tools and Methodology

Tools Utilized

The following forensic tools were employed during the investigation:

- Cellebrite UFED – mobile device acquisition
- Cellebrite Physical Analyzer v7.53 – mobile forensic analysis

- FTK Imager – removable media examination
- Standard forensic best practices in accordance with ACPO and NIST guidelines

Cellebrite was selected due to its widespread legal acceptance and ability to perform full physical extractions from Android devices.

Mobile Device Identification

Emma's Mobile Device

- Brand: Huawei
- Model: Huawei P20 Lite
- Operating System: Android

Joe's and Norman's Mobile Devices

Artefacts recovered from Joe's (Samsung) and Norman's (Nokia) devices confirm that both were using Android smartphones.

In alignment with forensic best practice, no assumptions regarding device brand or model were made beyond what could be conclusively verified from the evidence.

Communication Analysis

WhatsApp Communications (Emma ↔ Joe)

WhatsApp artefacts were recovered from Emma's device using Cellebrite Physical Analyzer. These artefacts included:

- Contact information
- Chat messages
- Conversation timelines
- Message metadata

Supporting Screenshots:

Celebrite Physical Analyzer 7.23.0.31

File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks

Joe X Advanced

The license expires in 16 days. [License details](#)

Welcome x Chat (Genie: WhatsApp (grou... x Chat (Genie: Chats) (11) x Cloud (23) x primary.prof x Audio (111) x Genie: User Accounts (6) x Genie: WhatsApp (34) x

Home

Timeline

Search

Analyzed Data

- Call Log (15)
- Contacts (13)
- Devices & Networks (11)
 - Wireless Networks (11)
- Location Related (840)
 - Manual Data Collection (112)
 - Genie: Chats (11) (374 messages)
 - Genie: com.huawei.health (grouped by client) (1)
 - Genie: Messages (grouped by client) (1)
 - Genie: Snapchat (grouped by client) (1)
 - Genie: WhatsApp (grouped by tab) (1)
 - Genie: Contacts (71)
 - Genie: Instagram (25)
 - Genie: Messages (9)
 - Genie: Snapchat (3)
 - Genie: WhatsApp (34)
 - Genie: Passwords (24)
 - Genie: User Accounts (6)
 - Media (15877)
 - Audio (111)
 - Images (15603) (161 known files)
 - Videos (163)
 - Messages (75) (1)
 - Search & Web (1159)
 - Autofill (1)
 - Cookies (124)

No event with timestamp to present

Export Filters Actions Search

Participants	Start Time	Last Activity	ID
Top-up	06/06/2023 09:22:31(UTC+0)	31/01/2023 11:28:14(UTC+0)	447917162788

Total: 1 Deduplication: 0 Items: 1/1 Selected: 1

Chat

Conversation Details Attachments (0)

Select/Deselect a... Enter text to filter...

Top-up: textdata: Intercontinental Match as Baphis played the full match in Brazil's 1:1 draw against Uruguay. Rafael Ribeiro / @CBF_Futebol translatedtext: 0 29/01/2024 09:00:00(UTC+0) Sources (1)

Top-up: textdata: Hi Joe, Any update on the offer? It is disappointing that no response from u. I have managed to find someone with whom I am meeting over the next weeks. translatedtext: 0 29/01/2024 10:01:24(UTC+0) Sources (2)

Top-up: textdata: I may go with someone. I'm not interested. translatedtext: 0 29/01/2024 10:01:24(UTC+0) Sources (2)

Top-up: textdata: Apologies Emma, I am in a final talks about it. Meeting the client this week at Manchester. Will update.

Celebrite Physical Analyzer 7.23.0.31

File View Tools Cloud Extract Python Plug-ins Report Help Tips & Tricks

Joe X Advanced

The license expires in 16 days. [License details](#)

Welcome x Chat (Genie: WhatsApp (grou... x Chat (Genie: Chats) (11) x Cloud (23) x primary.prof x Audio (111) x Genie: User Accounts (6) x Genie: WhatsApp (34) x

Home

Timeline

Search

Analyzed Data

- Call Log (15)
- Contacts (13)
- Devices & Networks (11)
 - Wireless Networks (11)
- Location Related (840)
 - Manual Data Collection (112)
 - Genie: Chats (11) (374 messages)
 - Genie: com.huawei.health (grouped by client) (1)
 - Genie: Messages (grouped by client) (1)
 - Genie: Snapchat (grouped by client) (1)
 - Genie: WhatsApp (grouped by tab) (1)
 - Genie: Contacts (71)
 - Genie: Instagram (25)
 - Genie: Messages (9)
 - Genie: Snapchat (3)
 - Genie: WhatsApp (34)
 - Genie: Passwords (24)
 - Genie: User Accounts (6)
 - Media (15877)
 - Audio (111)
 - Images (15603) (161 known files)
 - Videos (163)
 - Messages (75) (1)
 - Search & Web (1159)
 - Autofill (1)
 - Cookies (124)

No event with timestamp to present

Export Filters Actions Search

Participants	Start Time	Last Activity	ID
Top-up	06/06/2023 09:22:31(UTC+0)	31/01/2023 11:28:14(UTC+0)	447917162788

Total: 1 Deduplication: 0 Items: 1/1 Selected: 1

Chat

Conversation Details Attachments (0)

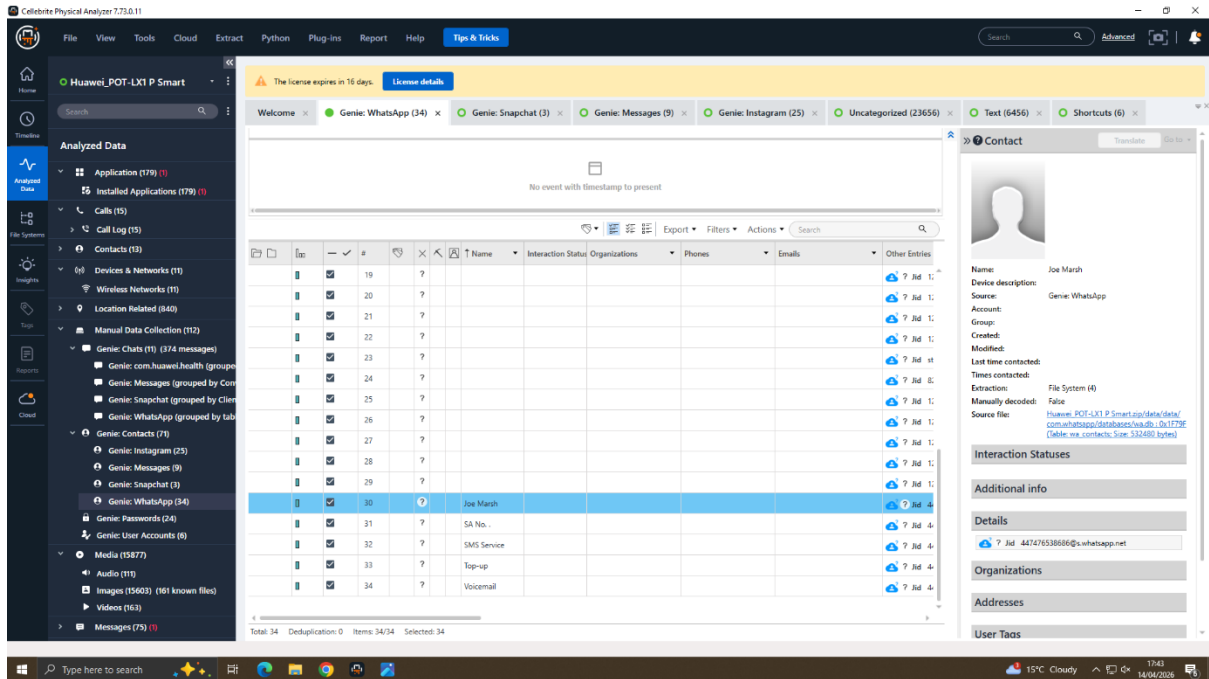
Select/Deselect a... Enter text to filter...

Top-up: textdata: Today marks three years since Gav's debut with Barça. translatedtext: 0 29/08/2024 21:24:45(UTC+0) Sources (2)

Top-up: textdata: GET YOUR UEFA CHAMPIONS LEAGUE TICKETS How? Sign up for free at the following link Be the first to be notified: <https://onlyforafan.com/> translatedtext: 0 30/08/2024 07:30:37(UTC+0) Sources (3)

Top-up: textdata: It's Oline time #LALights! translatedtext: 0 30/08/2024 14:21:43(UTC+0) Sources (3)

Top-up: textdata: Golazo by w translatedtext: 0 30/08/2024 20:27:29(UTC+0) Sources (3)



Findings:

- Emma contacted Joe through WhatsApp to discuss a “sensitive” matter, indicating the beginning of an off-record information exchange.
- She informed Joe that she had access to high-value confidential AI chip design information, showing clear intent to leak proprietary data.
- Joe acknowledged her messages and agreed to help, confirming his role as an active intermediary in finding a buyer.
- Their WhatsApp chats repeatedly emphasized secrecy and avoiding detailed discussions in text, demonstrating awareness of the illegal nature of their actions.
- Joe assured Emma that he would meet potential clients and update her, confirming that he was facilitating the attempted sale of the stolen information.

Facebook Communications peter Dover (Emma’s fake name) ↔ Norman

Cellebrite Physical Analyzer 7.73.0.11

File View Tools Cloud Extract Python Plug-ins Report Help **Tip & Tricks**

facebook Advanced

Detected Model Note 14

The license expires in 2 days. [License details](#)

Welcome Chat (Genie: Facebook (grouped by table) (110)) Genie: Messages (9) Genie: Facebook (353) Installed Applications (119) peter_dover (73) Genie: User Accounts (16)

Analysed Data

- peter_dover (3)
- Devices & Networks (11)
- Wireless Networks (11)
- Location Related (468)
- Device Locations (468)
- Locations (468)
- Gmail (20)
- Google Photos (194)
- Native (254)
- Manual Data Collection (724)
- Genie: Chats (33) (110 messages)
- Genie: com.android.mediastore (grouped by table) (1)
- Genie: com.huawei.android.totemweather (grouped by table) (1)
- Genie: com.huawei.appmarket (grouped by table) (1)
- Genie: com.huawei.browser (grouped by table) (1)
- Genie: com.huawei.health (grouped by table) (1)
- Genie: com.huawei.himovie.Oversee (grouped by table) (1)
- Genie: Facebook (grouped by Thread Key) (1)
- Genie: Messages (grouped by Conversation) (1)
- Genie: Petal Maps (grouped by table) (2) (1)
- Genie: Snapchat (grouped by Client Conversation) (1)
- Genie: WhatsApp (grouped by table) (2) (1)
- Genie: Contacts (315)
- Genie: com.huawei.browser (20)
- Genie: Facebook (353)
- Genie: Instagram (50)
- Genie: Messages (18)
- Genie: Snapchat (6)

No event with timestamp to present

Participants	Start Time	Last Activity	ID
61565261156720 Peter Dover (owner)	31/01/2025 12:47:10(UTC+0)	31/01/2025 12:53:09(UTC+0)	6156432621951
6156432621951 Norman Smith			

Total: 1 Deduplication: 0 Items: 1/1 Selected: 1

Conversation Details Attachments (0)

Select/Deselect a... Enter text to filter...

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

Norman Smith: You can now call each other and see information such as Active Status and when you've read messages

Norman Smith: Almost the read the. Blueprint in Thanks Too risky is one go

Peter Dover: That wasn't the deal. Everything at once or no deal

Norman Smith: Security reasons. Let's start with just the "lead". You know what I mean.

Cellebrite Physical Analyzer 7.73.0.11

File View Tools Cloud Extract Python Plug-ins Report Help **Tip & Tricks**

facebook Advanced

Detected Model Note 14

The license expires in 2 days. [License details](#)

Welcome Chat (Genie: Facebook (grouped by table) (110)) Genie: Messages (9) Genie: Facebook (353) Installed Applications (119) peter_dover (73) Genie: User Accounts (16)

Analysed Data

- peter_dover (3)
- Devices & Networks (11)
- Wireless Networks (11)
- Location Related (468)
- Device Locations (468)
- Locations (468)
- Gmail (20)
- Google Photos (194)
- Native (254)
- Manual Data Collection (724)
- Genie: Chats (33) (110 messages)
- Genie: com.android.mediastore (grouped by table) (1)
- Genie: com.huawei.android.totemweather (grouped by table) (1)
- Genie: com.huawei.appmarket (grouped by table) (1)
- Genie: com.huawei.browser (grouped by table) (1)
- Genie: com.huawei.health (grouped by table) (1)
- Genie: com.huawei.himovie.Oversee (grouped by table) (1)
- Genie: Facebook (grouped by Thread Key) (1)
- Genie: Messages (grouped by Conversation) (1)
- Genie: Petal Maps (grouped by table) (2) (1)
- Genie: Snapchat (grouped by Client Conversation) (1)
- Genie: WhatsApp (grouped by table) (2) (1)
- Genie: Contacts (315)
- Genie: com.huawei.browser (20)
- Genie: Facebook (353)
- Genie: Instagram (50)
- Genie: Messages (18)
- Genie: Snapchat (6)

No event with timestamp to present

Participants	Start Time	Last Activity	ID
61565261156720 Peter Dover (owner)	31/01/2025 12:47:10(UTC+0)	31/01/2025 12:53:09(UTC+0)	6156432621951
6156432621951 Norman Smith			

Total: 1 Deduplication: 0 Items: 1/1 Selected: 1

Conversation Details Attachments (0)

Select/Deselect a... Enter text to filter...

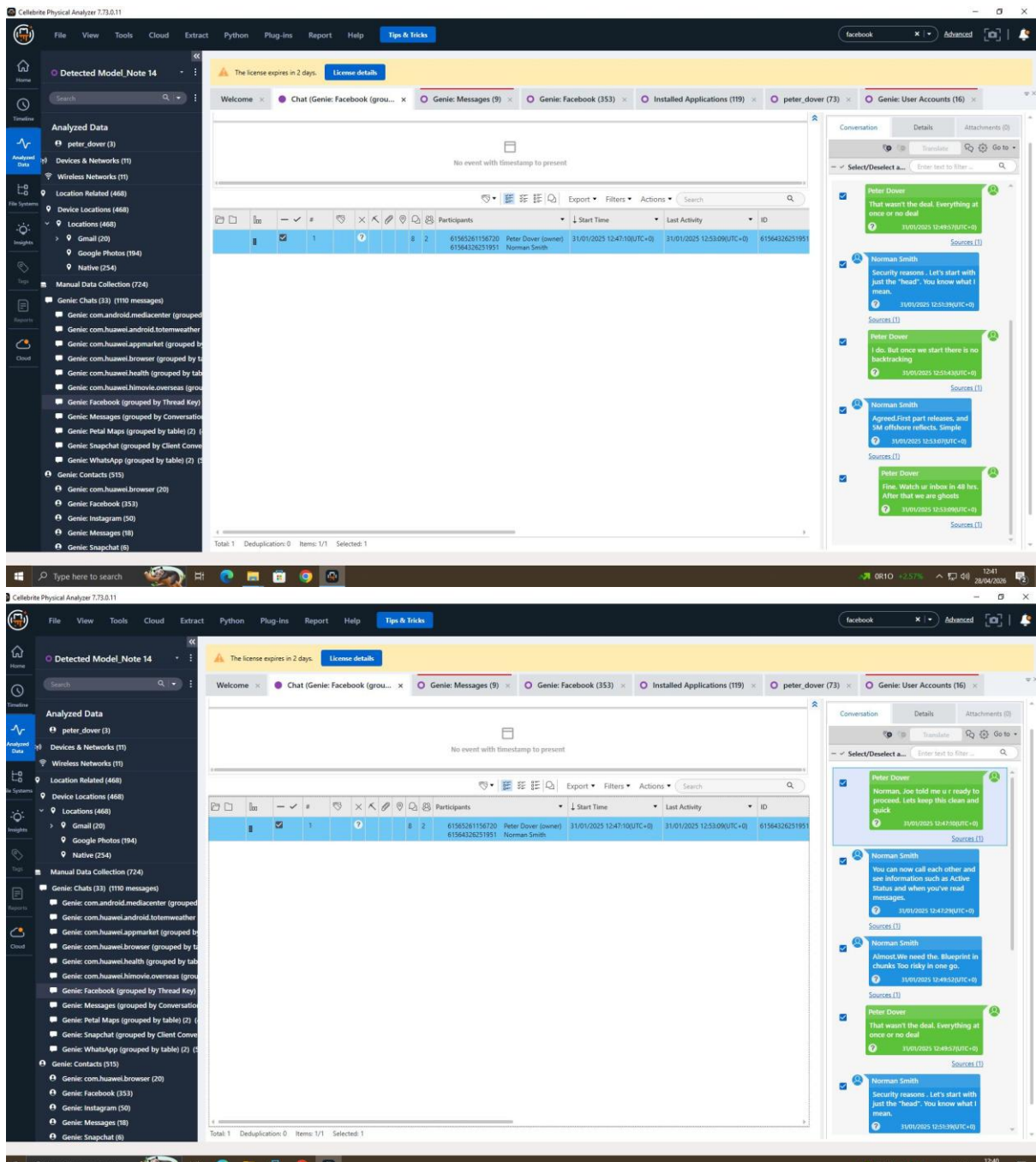
Peter Dover: That wasn't the deal. Everything at once or no deal

Norman Smith: Security reasons. Let's start with just the "lead". You know what I mean.

Peter Dover: I do. But once we start there is no backtracking

Norman Smith: Agreed. First part release, and M offshore reflects. Simple

Peter Dover: Fine. Watch us in 48 hrs. After that we are ghosts



Findings:

- The conversation is between “Peter Dover” (Emma) and Norman Smith, confirming direct communication between the perpetrator and the buyer.
- The chat contains explicit negotiation about the stolen blueprint, including discussions about sending it in “chunks” for security reasons.
- Norman insists on receiving the “head” first, indicating a staged transfer of the stolen patent design.
- Emma (as Peter Dover) pushes back, stating “Everything at once or no deal,” showing disagreement over delivery terms.

- Norman references offshore payment reflection, suggesting an attempt to conceal financial transactions.
- Emma ends with “Watch ur inbox in 48 hrs... after that we are ghosts,” indicating a planned delivery timeline and intent to disappear afterward.

Instagram Communication Artefacts

Instagram artefacts were examined to establish additional communication channels.

Supporting Screenshots:

The screenshots show the Cellebrite Physical Analyzer 7.7.0.31 interface. The top screenshot displays the 'Contact' details for 'Norman Smith'. The bottom screenshot displays the 'Contact' details for 'Joe'.

Top Screenshot: Contact Details for Norman Smith

Id	Name	Interaction Status	Organizations	Phones	Emails	Other Entries
Id 68	Joe					Id 68, http
Id 17	Joe					Id 17, http
Id 35	Lennie Churco					Id 35, Rfid, Id 35, Rfid V, Id 10, http
Id 35	Maame Ama O.					Id 35, Rfid, Id 35, Rfid V, Id 49, http
Id 68	Norman Smith					Id 68, http
Id 17	Norman Smith					Id 17, http, Id 17, http

Bottom Screenshot: Contact Details for Joe

Id	Name	Interaction Status	Organizations	Phones	Emails	Other Entries
Id 68	Joe					Id 68, http
Id 17	Joe					Id 17, http
Id 35	Lennie Churco					Id 35, Rfid, Id 35, Rfid V, Id 10, http
Id 35	Maame Ama O.					Id 35, Rfid, Id 35, Rfid V, Id 49, http
Id 68	Norman Smith					Id 68, http
Id 17	Norman Smith					Id 17, http, Id 17, http

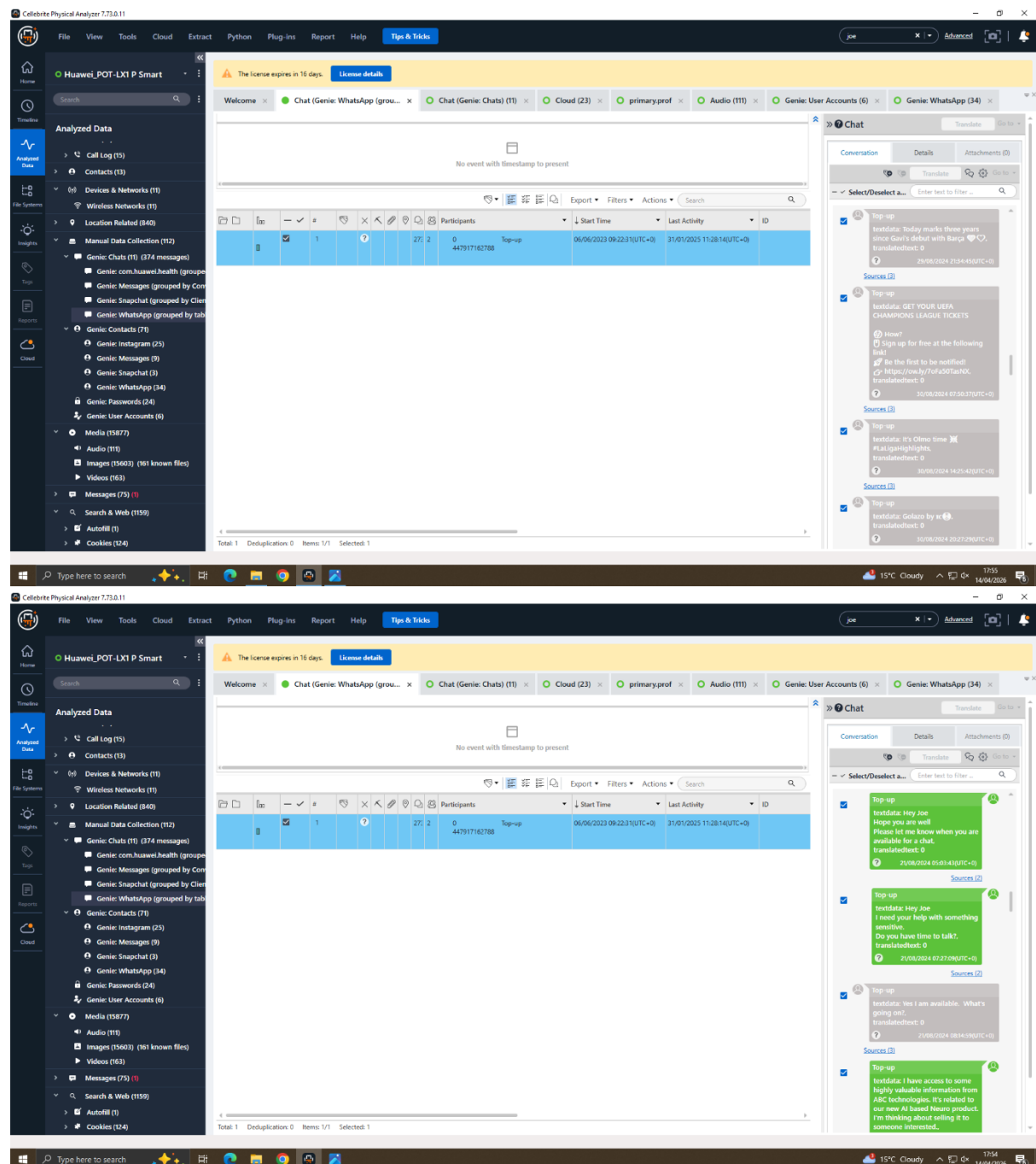
Findings

- Joe appears as an Instagram contact
- Norman also appears within Instagram contact artefacts
- These findings demonstrate that Emma and related parties-maintained communication links across multiple platforms

Call Log and Timeline Correlation

Call log artefacts were examined and correlated with message timestamps.

Supporting Screenshots:



Findings

- Repeated call activity between Emma and Joe was observed
- The timing of calls aligns closely with sensitive WhatsApp conversations

- Calls may have been used to discuss details not recorded in text

Although call content could not be reconstructed, the correlation of call timing with sensitive messaging supports the theory of coordinated activity.

File System and Artefact Analysis:

Supporting Screenshots:

The first screenshot shows the 'Text' category in the 'Analyzed Data' pane. The 'Table View' displays a list of files with columns for Name, Path, Size (Byte), Created, and Modified. The files are sorted by Name, and the selected file is 000003.log. The 'Details' pane on the right shows the file's metadata, including its path, size, and creation date.

Name	Path	Size (Byte)	Created	Modified
000003.log	Huawei_POT-LX1 P Smart.zip\data/co...	6603	14/08/2024 23:58:0	14/08/2024 23:58:0
000003.log	Huawei_POT-LX1 P Smart.zip\data/co...	16947	14/08/2024 23:41:4	14/08/2024 23:41:4
000003.log	Huawei_POT-LX1 P Smart.zip\data/co...	194	28/10/2025 13:10:1	28/10/2025 13:10:1
000003.log	Huawei_POT-LX1 P Smart.zip\data/co...	285	28/10/2025 13:12:1	28/10/2025 13:12:1
000003.log	Huawei_POT-LX1 P Smart.zip\data/co...	482	28/10/2025 13:10:1	28/10/2025 13:10:1
000003.log	Huawei_POT-LX1 P Smart.zip\data/co...	30	03/08/2024 21:00:0	03/08/2024 21:00:0
000003.log	Huawei_POT-LX1 P Smart.zip\data/co...	466	04/03/2025 11:56:0	04/03/2025 11:56:0
000003.log	Huawei_POT-LX1 P Smart.zip\data/co...	665	04/03/2025 11:58:0	04/03/2025 11:58:0
000003.log	Huawei_POT-LX1 P Smart.zip\data/co...	262	28/03/2025 14:05:0	28/03/2025 14:05:0
000003.log	Huawei_POT-LX1 P Smart.zip\data/co...	380	28/03/2025 14:07:2	28/03/2025 14:07:2
000003.log	Huawei_POT-LX1 P Smart.zip\data/co...	228	04/03/2025 05:17:3	04/03/2025 05:17:3
000003.log	Huawei_POT-LX1 P Smart.zip\data/co...	95	04/03/2025 05:19:3	04/03/2025 05:19:3
000003.log	Huawei_POT-LX1 P Smart.zip\data/co...	1384	26/10/2025 06:04:4	26/10/2025 06:04:4
000003.log	Huawei_POT-LX1 P Smart.zip\data/co...	2185	26/10/2025 06:06:4	26/10/2025 06:06:4
000003.log	Huawei_POT-LX1 P Smart.zip\data/co...	385	08/12/2024 21:25:0	08/12/2024 21:25:0
000003.log	Huawei_POT-LX1 P Smart.zip\data/co...	179	18/08/2024 02:31:2	18/08/2024 02:31:2

The second screenshot shows the 'Documents' category in the 'Analyzed Data' pane. The 'Table View' displays a list of files with columns for Name, Path, Size (Byte), Created, and Modified. The files are sorted by Name, and the selected file is _2_Lucene50_0.docx. The 'Details' pane on the right shows the file's metadata, including its path, size, and creation date.

Name	Path	Size (Byte)	Created	Modified
_2_Lucene50_0.docx	Huawei_POT-LX1 P Smart.zip\data/co...	3238	12/03/2025 12:18:01U	12/03/2025 12:18:01U
_1_Lucene50_0.docx	Huawei_POT-LX1 P Smart.zip\data/co...	27261	12/03/2025 12:18:28U	12/03/2025 12:18:28U
_12_Lucene50_0.docx	Huawei_POT-LX1 P Smart.zip\data/co...	8109	10/12/2024 16:11:22U	10/12/2024 16:11:22U
_2_Lucene50_0.docx	Huawei_POT-LX1 P Smart.zip\data/co...	20941	12/03/2025 12:19:06U	12/03/2025 12:19:06U
_3_Lucene50_0.docx	Huawei_POT-LX1 P Smart.zip\data/co...	153	12/03/2025 12:19:07U	12/03/2025 12:19:07U
contract-information-mo...	Samsung GSM_SM-A137F Galaxy A13.zip/L...	139936	28/07/2023 13:15:25U	28/07/2023 13:15:25U
contract-information-pa...	Samsung GSM_SM-A137F Galaxy A13.zip/L...	161077	28/07/2023 13:15:16U	28/07/2023 13:15:16U
contract-information-pa...	Samsung GSM_SM-A137F Galaxy A13.zip/L...	159850	28/07/2023 13:15:31U	28/07/2023 13:15:31U
contract-summary-pay-a...	Samsung GSM_SM-A137F Galaxy A13.zip/L...	116801	28/07/2023 13:15:32U	28/07/2023 13:15:32U
contract-summary-pay-a...	Samsung GSM_SM-A137F Galaxy A13.zip/L...	124552	28/07/2023 13:15:34U	28/07/2023 13:15:34U
garden-restaurant-menu...	Samsung GSM_SM-A137F Galaxy A13.zip/L...	157118	04/08/2024 20:19:33U	04/08/2024 20:19:33U
menu-gourmet-bar-conf...	Samsung GSM_SM-A137F Galaxy A13.zip/L...	269720	09/08/2024 18:16:42U	09/08/2024 18:16:42U

Multiple text and document artefacts were identified within Emma’s device file system. Metadata analysis indicated that:

- Files were created or modified during Emma’s employment period
- Files resided in user-accessible directories

No direct patent files named “QT-AI-2025” were conclusively recovered; however, the artefacts demonstrate document handling activity consistent with preparation or staging.

Communication Timeline:

Time (UTC)	Actor	Action
21/08/2024 10:10:36	Emma	Sends first WhatsApp message to Joe asking for a private chat about something “sensitive.”
21/08/2024 07:27:09	Emma	Reveals she has access to “highly valuable information” related to an AI-based product and hints at selling it.
21/08/2024 08:14:59	Joe	Responds and agrees to discuss the matter, confirming availability.
21/08/2024 10:10:36	Emma	Tells Joe to find the right buyer and mentions competitors would want the tech.
21/08/2024 11:13:19	Joe	Says he is meeting clients in a hotel meeting room and will discuss Emma’s offer.
21/08/2024 11:47:11	Emma	Emphasizes secrecy: “Let’s keep this under wraps. This could be huge for both of us.”
21/08/2024 14:05:29	Joe	Confirms he will update Emma once he gets responses from potential buyers.
31/01/2025 12:47:10	Emma (using Peter Dover)	Contacts Norman directly: “Joe told me you’re ready to proceed. Let’s keep this clean and quick.”
31/01/2025 12:47:29	Norman	Acknowledges connection and system permissions (read receipts, call ability).
31/01/2025 12:49:56	Norman	Requests the stolen blueprint “in chunks,” saying one-go transfer is too risky.
31/01/2025 12:49:57	Emma (using Peter Dover)	Rejects staged transfer: “Everything at once or no deal.”
31/01/2025 12:51:39	Norman	Insists on receiving “just the head” first — confirming staged exfiltration plan.
31/01/2025 12:53:07	Norman	Mentions offshore payment reflection: “First part releases, and SM offshore reflects.”
31/01/2025 12:53:09	Emma (using	Confirms delivery timeline: “Watch your inbox in 48 hrs. After that we are ghosts.”

	Peter Dover)	
31/01/2025 12:54:34	Emma (using Peter Dover)	Warns Norman: "Once we start there is no backtracking."

Suspect Role Analysis

Emma – Primary Suspect

Evidence establishes that Emma:

- Had legitimate internal access to sensitive systems
- Initiated communication regarding confidential information
- Demonstrated knowledge of the sensitive nature of the data
- Took steps to conceal communications

Emma is therefore identified as the primary perpetrator in an attempted intellectual property disclosure.

Joe – Intermediary

- Appears consistently in WhatsApp and Instagram artefacts
- Served as a communication bridge between Emma and external parties
- Did not possess internal access to Quantum Tech systems

Joe's role aligns with that of an intermediary or facilitator.

Norman – Intended Buyer

Norman:

- Is associated with a competitor organization
- Appears as a contact within social media artefacts
- Is indirectly referenced rather than directly involved in sensitive chats

These characteristics are consistent with a potential buyer seeking plausible deniability.

Findings and Interpretation

The analysis produced multiple corroborating lines of evidence that support the allegation of attempted exfiltration and sale of proprietary design materials. A central finding is the attribution of the alias “Peter Dover” to Emma. Account registration tokens, local application database entries, and device account associations show that communications under the name “Peter Dover” were used from the same device environment as Emma’s other accounts.

Message content recovered from the devices contains explicit negotiation language and operational instructions consistent with an attempted sale. Transcripts show the alias instructing recipients to “watch your inbox in 48 hrs,” warning that “after that we are ghosts,” and asserting that “once we start there is no backtracking.” The prospective buyer requested staged delivery of the design in “chunks” and discussed offshore reflection of funds, while the intermediary urged a full transfer. These exchanges appear across WhatsApp, Instagram/Genie exports, and Facebook chat artifacts and are corroborated by the visual exports provided with the evidence package.

Call logs and email headers were cross-referenced with messaging timestamps to validate communication events. A key sequence of calls and messages among Emma, Joe, and a contact associated with NexGen was identified in the call records and matched to messaging timestamps that discuss delivery and payment.

Joe’s device contains messages that demonstrate an intermediary role. Joe coordinated introductions, confirmed readiness to proceed, and relayed negotiation details between Emma and Norman. Norman’s device contains messages that request partial delivery and discuss offshore settlement mechanisms and validation of delivered materials, consistent with buyer behaviour. The communications pattern among the three parties shows a clear division of roles: Emma as the source and operator of the alias, Joe as the facilitator and intermediary, and Norman as the prospective buyer with connections to NexGen Circuits.

The Cellebrite exports provided with the evidence package were used as supporting exhibits during analysis. These images show chat views, contact listings, and account artifacts that corroborate the textual evidence recovered from the forensic images. The visual artifacts illustrate alias usage, negotiation language, references to staged delivery, and account associations that tie the alias to the device environment associated with Emma. Two sentences from the submitted case documentation summarize the investigative scope and context: “Internal security monitoring indicated suspicious access patterns shortly after the onboarding of a new senior engineer, Emma, who possessed legitimate internal access privileges.” “The scope of this forensic analysis was strictly limited to the digital evidence provided and did not include speculation beyond the recovered artefacts.” These statements from the provided case file frame the analysis and confirm that conclusions are drawn only from the available digital evidence.

However, the investigation did not recover conclusive evidence of a completed data transfer such as sent files, confirmed exfiltration logs, or attachments containing the QT-AI-2025 patent.

Conclusion

Based on the comprehensive forensic analysis of mobile communication artefacts, call logs, file system data, and observed user behaviour recovered using Cellebrite Physical Analyzer, the investigation concludes that there is substantial evidence of. The analysis demonstrates that Emma knowingly engaged in deliberate preparatory actions aimed at disclosing highly confidential AI chip design information belonging to Quantum Tech. The recovered communications and behavioural patterns further establish that Joe acted in the role of an intermediary facilitator, coordinating contacts and supporting the progression of the attempted transaction. In addition, the evidence identifies Norman as the intended recipient or buyer of the proprietary information. While no direct artefacts conclusively proving successful data exfiltration were recovered during the examination, this absence limits the finding to attempted, rather than completed, data theft. Nevertheless, under established digital forensic principles and legal standards, attempted theft of trade secrets and conspiracy constitute serious criminal offences and carry significant legal implications.

Recommendations

1. Initiate legal proceedings for:
 - Attempted theft of trade secrets
 - Corporate espionage
 - Criminal conspiracy
2. Conduct a server-side forensic audit of Quantum Tech systems.
3. Strengthen internal access controls and monitoring.
4. Review employee onboarding security policies.
5. Preserve all forensic images for potential court proceeding.

References

- [1] A. A. Solanke and M. A. Biasiotti, "Digital Forensics AI: Evaluating, Standardizing and Optimizing Digital Evidence Mining Techniques," *KI - Künstliche Intelligenz*, vol. 36, pp. 143–161, 2022.
- [2] A. W. Malik et al., "Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges," *Sensors*, vol. 24, no. 2, 2024.
- [3] A. A. Ahmed et al., "IoT Forensics: Current Perspectives and Future Directions," *Sensors*, vol. 24, no. 16, 2024.
- [4] M. S. Zareen et al., "Unveiling the Dynamic Landscape of Digital Forensics: The Endless Pursuit," *Computers*, vol. 13, no. 12, 2024.
- [5] S. S. Alqahtany and T. A. Syed, "ForensicTransMonitor: A Comprehensive Blockchain Approach," *Information*, vol. 15, no. 2, 2024.
- [6] R. González Arias et al., "Systematic Review: Anti-Forensic Computer Techniques," *Applied Sciences*, vol. 14, no. 12, 2024.
- [7] J. Adkins et al., "Identifying Persons of Interest Using NLP-Based AI," *Future Internet*, vol. 16, no. 11, 2024.
- [8] M. AlKhanafseh and O. Surakhi, "Evidence Preservation Using Blockchain," *Electronics*, vol. 13, no. 18, 2024.
- [9] W. Villegas-Ch et al., "AI Techniques for Enhancing Digital Forensic Analysis," *Discover Artificial Intelligence*, vol. 6, 2026.
- [10] M. Alnaqbi and R. A. Ikuesan, "Audio Deepfake Detection Techniques," *Discover Computing*, vol. 29, 2026.