

Student Name: Raju Molla

Student ID: 2421791

Programme: MSc in Cybersecurity and Digital Forensics

Module code: ACCA7031

Assignment Title: Research on digital forensics addressing

Task: 1

Introduction

Digital forensics is an essential field in modern criminal investigation and cybersecurity. As digital systems, cloud platforms, and IoT devices proliferate, businesses face increasingly complex challenges in identifying, preserving, evaluating, and presenting digital evidence. Because of ransomware, fraud, insider threats, cyberattacks, and data breaches, forensic readiness is becoming an essential component of incident response. This paper examines the current state of digital forensics, its primary tools and capabilities, its convergence with cybersecurity, future trends, significant challenges, and the domestic and global employment market. It is supported by credible industry reports, academic literature, and regulatory guidelines.

Current State of the Field and Tools

Digital forensics (DF) encompasses the gathering, examination, reporting, and analysis of digital evidence from computers, mobile devices, networks, cloud systems, and Internet of Things environments. Modern DFIR (Digital Forensics and Incident Response) operations use enterprise-scale technologies with automation, scripting, and cloud connectivity to handle growing amounts of data. EnCase, FTK, X-Ways, and open-source tools like Autopsy and SleuthKit are well-known forensic suites that provide imaging, artifact extraction, timeline analysis, and reporting features [1], [2]. Investigating ransomware and malware requires the ability to analyze volatile data in real time, which is made possible by volatility and other memory forensics tools [3].

Business and law enforcement investigations are increasingly using mobile and cloud evidence, according to industry studies [2], [4]. Mobile forensic platforms such as Cellebrite UFED and Magnet AXIOM support cloud-based account acquisition, encrypted app data parsing, and sophisticated extraction techniques. NIST guidelines and standard textbooks support evidential standards, chain-of-custody procedures, and methodological rigor [5], [6].

Intersection of Digital Forensics and Cybersecurity

Digital forensics and cybersecurity are closely related due to the rise of sophisticated cyberattacks. Together with security operation centers (SOCs), DFIR teams handle incident triage, containment, and post-event analysis. Forensic techniques that are essential for determining attack routes and underlying causes include memory dumps, endpoint artifact extraction, and network packet capture [5], [7].

The increasing integration of forensic capabilities in cybersecurity systems such as EDR (Endpoint Detection and Response), SIEM (Security Information and Event Management), and SOAR platforms allows investigators to efficiently collect evidence during real-time incidents. Forensic findings have an impact on risk assessments, threat intelligence, and organizational security plans. Because of this mutually beneficial relationship, DFIR is now a crucial discipline in business cybersecurity operations.

Emerging Trends in Digital Forensics

1. Cloud and SaaS Forensics:

Due to the widespread use of cloud computing, forensic procedures now have to handle distributed logs, virtual machine snapshots, and multi-tenant architectures. Investigators are increasingly relying on cloud provider APIs to obtain evidence, which creates unique technological and legal challenges. [4], [8].

2. Mobile and IoT Forensics:

Because of encrypted chat apps and geolocation data, mobile phones continue to be important sources of evidence. IoT forensics is rapidly expanding to include wearables, smart home devices, and car telemetry, all of which have their own unique data formats [2].

3. Memory and Live Forensics:

The rise of fileless malware and ransomware has elevated memory forensics as a vital practice. Tools like Volatility provide capabilities for analysing in-memory processes, injected code, and credential harvesting techniques [3].

4. AI-driven Forensic Automation:

Forensic vendors now use machine learning to automate finding strange things, sorting artifacts, and putting evidence in order of importance. On the other hand, criminals are using steganography, deepfakes made by AI, and fake logs, which make it harder to tell what is real [9]. Data formats that are private [2].

5. Forensic Scalability and Cloud-Native DFIR:

The industry's need to handle large amounts of data is shown by the growing use of cloud-native, API-driven forensic platforms by businesses that automate ingestion, indexing, and artifact parsing on a large scale. [1], [4]. problems with being real [9].

Key Challenges in Digital Forensics

- **Data Volume and Diversity:**

The rapid growth of cloud, mobile, and IoT data has made forensic teams' jobs much harder. Enterprise-scale events happen too quickly for manual operations [1], [2].

- **Legal and Jurisdictional Complexities:**

Cloud-based data often spans multiple geographical locations, requiring complex legal processes such as subpoenas, warrants, and MLAT agreements to obtain evidence. NIST [5], [8] has written about these problems with cross-border and procedural issues in academic papers.

- **Ethical and Misuse Concerns:**

Investigations by Amnesty International and news organizations have shown that forensic technologies have been misused for illegal monitoring, which has raised concerns about ethical governance and compliance with human rights [10].

- **Evidence Authenticity in an AI Era:**

Deepfakes and AI-generated artifacts put traditional validation and chain-of-custody protocols to the test. In court, it is becoming more and more important to have an expert witness on digital authenticity and metadata verification [9].

- **Skills Shortage and Training Gaps:**

Organizations have a hard time hiring qualified DFIR analysts who know how to do cloud forensics, memory analysis, and legal paperwork. Reports say that there is a persistent global shortage of qualified digital forensics experts [1], [2].

National and International Job Market

There is a high demand for digital forensics experts around the world because of more cybercrime, stricter rules, and changes in the digital world across all industries. The U.S. Bureau of Labor Statistics says that the number of information security analysts, which is very similar to DFIR, will grow by 29% between 2024 and 2034. This makes them one of the fastest-growing jobs [11].

There are thousands of DFIR jobs on international job sites like LinkedIn, Indeed, and Glassdoor in the UK, US, Europe, the Middle East, and Asia-Pacific regions. Some of these jobs are Digital Forensic Analyst, Mobile Forensic Examiner, SOC/DFIR Analyst, Cybercrime Investigator, and higher-level positions like DFIR Manager or Expert Witness Consultant [12]. The pay for IT positions, which are in high demand in government, law enforcement, financial services, consulting businesses, and multinational corporations, varies greatly by location but is generally above average.

References (IEEE Style)

- [1] Magnet Forensics, *State of Enterprise DFIR Report*, 2024.
- [2] SANS Institute, *DFIR Survey & Industry Commentary*, 2024.
- [3] Volatility Foundation, “Volatility Memory Forensics Framework,” Documentation.
- [4] Cellebrite, *Mobile & Cloud Forensics Industry Trends Report*, 2023–2024.
- [5] NIST, *Guide to Integrating Forensic Techniques into Incident Response*, SP 800-86 and related SP 800 series.
- [6] E. Casey, *Handbook of Digital Forensics and Investigation*. Elsevier.
- [7] EnCase/FTK/X-Ways official documentation on forensic-cybersecurity integration.
- [8] Academic literature on cloud forensics and jurisdictional challenges, 2022–2024.
- [9] Research and industry whitepapers on AI, deepfakes, and digital evidence authenticity, 2022–2024.
- [10] Amnesty International Reports on misuse of digital forensic tools, 2024.
- [11] U.S. Bureau of Labor Statistics, *Occupational Outlook for Information Security Analysts*, 2024.
- [12] LinkedIn/Indeed International Job Market Data (Digital Forensics & DFIR roles), 2024–2025.

Task: 2

Image acquisition:

During the mobile image acquisition process, I followed the standard forensic procedures required by UFED. Although I am familiar with the acquisition workflow, there are several common challenges that typically arise during extraction:

1. **Switching the device to Flight Mode**

Before beginning the acquisition, it is necessary to place the mobile device in airplane/flight mode to prevent incoming network communication. This ensures data integrity and avoids any alteration of evidence during the extraction process.

2. **Following on-screen instructions carefully**

UFED provides step-by-step instructions during different stages of the extraction. It is important to follow these instructions precisely—such as approving prompts, enabling USB debugging, or unlocking the device—to avoid extraction failures.

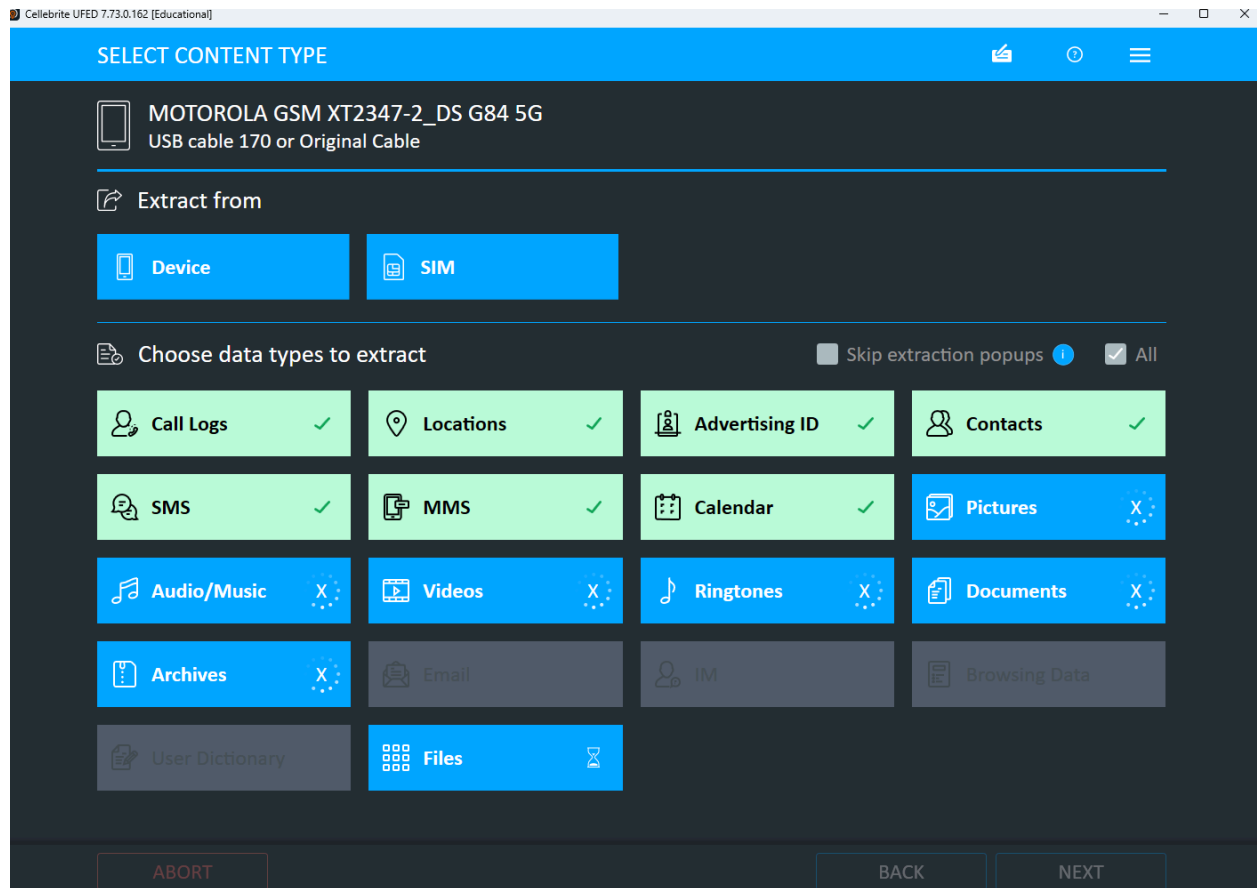
3. **Handling different acquisition types**

Depending on the device model and security level, various extraction methods may be available, such as

- **File System Acquisition**

- **Advanced Logical Acquisition**
- **Advanced Physical Acquisition**
Each method has its own limitations and requirements, and selecting the appropriate one is crucial for maximizing the amount of recoverable data.

Overall, ensuring proper device preparation and following UFED guidelines are essential for a successful and comprehensive mobile forensic image acquisition.



Cellebrite Collection Summary

Collection Summary Report

Case Identifier	001
Examiner Name	Raju Molla
Device Name / Evidence Number	Moto g84
Crime Type	Murder
Department	Molla_Dev
Location	UK
UFED 4PC ID	1136568878
UFED 4PC version	7.73.0.162
Extraction start time	2025-12-04 10:59:28
Extraction end time	2025-12-04 12:52:38
Selected vendor	Motorola GSM
Selected model	XT2347-2_DS g84 5G
Extraction type	Advanced Logical
Device Model	moto g84 5G
OS Version	14
Chipset	SM6375
Security Patch Level	2025-06-01
IMEI	358144796577728
IMEI2	358144796577710
Vendor	motorola
Is Device Rooted	No
Number Of Installed Applications	0
Live encryption state	file

DIGITAL FORENSIC INVESTIGATION REPORT

Case: Corporate Espionage—Quantum Tech AI Patent Leak

Investigator: Raju Molla

Date: 12/12/2024

1. Case Background:

Quantum Tech reported suspicious activity involving unauthorized access to their proprietary AI patent database, specifically AI Chip Design Patent QT-AI-2025.

Internal monitoring indicated that confidential research files may have been leaked or offered for sale.

Emma, a newly joined senior engineer at Quantum Tech, became the primary suspect. Intelligence also indicated possible involvement of:

- Joe—a potential intermediary helping Emma sell the information
- Norman—potential buyer connected to the transaction

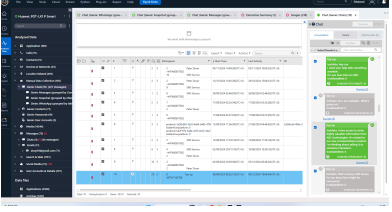
Four mobile devices were seized and provided for forensic analysis:

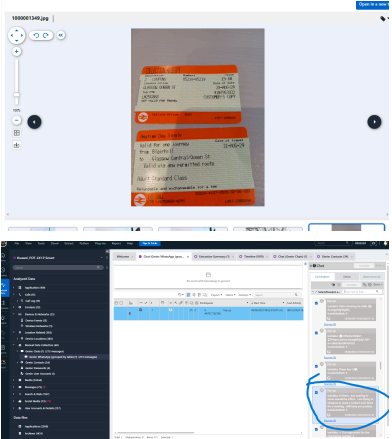
- Huawei smartphone
- Samsung smartphone
- Nokia smartphone
- Ulefone smartphone

The objective of this investigation is to:

- Acquire and analyze mobile forensic images
- Reconstruct communication between the suspects
- Identify the roles and motives of each party
- Determine whether confidential corporate information was being sold

2. Evidence Inventory:

Device	Identified Owner	Reason for Identification
Huawei	Emma	I got a chat on Huawei phone. :((“That’s serious stuff, Emma.”) 
Samsung	Joe	I received the Huawei phone regarding Glasgow. Joe intended to travel to Glasgow and sent a message to Emma saying, ‘I am flying to Glasgow to meet.’ I also received a Samsung phone with a photo of a ticket for Glasgow.

		
Nokia	Norman	There are some pictures of tickets and the phone owner.

Chain of Custody:

- All devices were received sealed and labelled.
- Forensic images were created using industry-standard acquisition methods.
- No physical or digital tampering occurred.
- All steps were documented and conducted following forensic best practices.

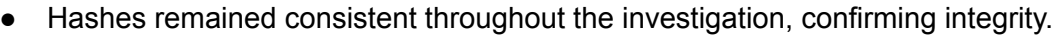
3. Methodology

3.1 Forensic Acquisition

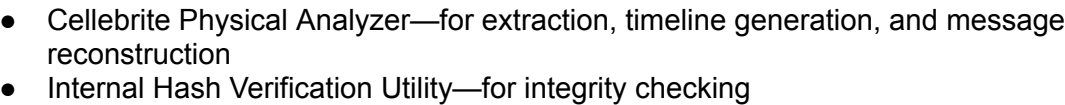
- All devices were imaged using industry-standard mobile forensic tools.
- A logical and file-system extraction was performed.
- Extraction included:
 - WhatsApp messages
 - Instagram data
 - Emails
 - Call logs
 - Application data

3.2 Integrity Verification

- Hash values (MD5/SHA-1) were taken immediately after acquisition.



- App Genie—used to decode WhatsApp and other communication data



4. Findings

4.1 Communication Analysis (Emma ↔ Joe)

Key Evidence from Emma's Huawei Device

A critical WhatsApp message recovered from Emma's device reads:

"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."
(Timestamp: 21/08/2024 09:58:21 UTC+0)

Joe responds:

"That's serious stuff Emma. Do you know how might be interested?"
(Timestamp: 21/08/2024 10:06:29 UTC+0)

The screenshot displays a forensic tool interface with a sidebar on the left containing various analysis categories like 'Application (109)', 'Calls (13)', 'Devices & Networks (23)', 'Location Related (419)', 'Manual Data Collection (105)', 'Genie Chats (10) (327 messages)', 'Genie Messages (grouped by Contact)', 'Genie Snapchat (grouped by Contact)', 'Genie WhatsApp (grouped by tab)', 'Genie Contacts (71)', 'Genie Passwords (19)', 'Genie User Accounts (5)', 'Media (1434)', 'Messages (75) (1)', 'Chats (4) (1) (34 messages)', 'Emails (71)', 'dovp59@gmail.com (71)', 'Search & Web (1157)', 'Social Media (73) (73)', and 'User Accounts & Details (257)'. The main area shows a table of analyzed data with columns for item number, status, and details. A chat window on the right shows a conversation between Emma and Joe. The chat messages are as follows:

#	Status	Participants	Start Time	Last Activity	ID
1	✓	Peter Dover +447400657582 SMS Service	05/11/2024 10:00:28(UTC+0)	05/11/2024 10:00:32(UTC+0)	
2	✓	Peter Dover +447400657582 SMS Service	13/10/2024 15:45:20(UTC+0)	28/10/2024 15:08:31(UTC+0)	
3	✓	Peter Dover +447400657582 SMS Service	26/08/2024 02:46:03(UTC+0)	26/08/2024 02:46:03(UTC+0)	
4	✓	Peter Dover +447400657582 SMS Service	17/08/2024 02:35:34(UTC+0)	17/08/2024 03:35:28(UTC+0)	
5	✓	Peter Dover +447400657582 SMS Service	17/08/2024 02:27:45(UTC+0)	17/08/2024 02:27:45(UTC+0)	
6	✓	senderid: 2a36-963-34c0-4e96-b462-47b hiddenfromplatform: 0 senderid: b42f1770-3a8b-4c53-8c25-34e7 hiddenfromplatform: 0	13/08/2024 11:56:30(UTC+0)	21/08/2024 04:46:05(UTC+0)	2a29bcbf-485e-5
7	✓	Peter Dover +447400657582 SMS Service	13/08/2024 11:53:31(UTC+0)	13/08/2024 11:54:14(UTC+0)	
8	✓	Peter Dover +447400657582 SMS Service	02/08/2024 20:37:51(UTC+0)	19/08/2024 10:50:15(UTC+0)	
9	✓	Peter Dover +447400657582 SMS Service	02/08/2024 20:36:38(UTC+0)	05/12/2024 00:46:22(UTC+0)	
10	✓	Top-up 447917162788	06/06/2023 09:22:31(UTC+0)	08/12/2024 19:06:44(UTC+0)	

The chat window on the right shows a conversation between Emma and Joe. The messages are as follows:

- Top-up
textdata: Hey Joe
I need your help with something
sensitive.
Do you have time to talk?
translatedtext: 0
21/08/2024 09:27:58(UTC+0)
- Top-up
textdata: Yes I am available. What's
going on?
translatedtext: 0
21/08/2024 09:34:58(UTC+0)
- Top-up
textdata: 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.
translatedtext: 0
21/08/2024 09:58:21(UTC+0)
- Top-up
textdata: That's serious stuff Emma.
Do you know how might be
interested?
translatedtext: 0
21/08/2024 10:06:29(UTC+0)

This exchange clearly shows:

- Emma's intent to sell confidential intellectual property
- Joe's willingness to assist as an intermediary

4.2 Timeline Reconstruction

The timeline feature in the forensic tool confirms:

- 21/08/2024 – Emma contacts Joe about selling highly valuable information
- 21/08/2024 – Joe responds acknowledging seriousness

- 26/08/2024 – Additional follow-up messages between Emma and Joe
- 20/11/2024 – Joe apologizes for delay, suggesting ongoing communication

The screenshot displays a digital investigation tool interface. The top section shows a timeline from 2006 to 2025, with filters applied for 'emma'. Below the timeline, a table lists messages with columns for filters, timestamp, party, description, and source. The table shows three messages, with the third message selected. The right sidebar provides a detailed view of the selected message, including the 'Message Deleted Reason', 'Priority', 'Service Identifier', 'Extraction', 'Manually decoded', and 'Source file'. The message content is visible in the 'Body' section.

Filters	Timestamp	Party	Description	Source
21/08/2024 (1)	21/08/2024 10:06:29(UTC+0)	Genie: Instant Me...	From: 0 Top-up To: 447917162788	textdata: That's serious stuff Emma...
26/08/2024 (1)	26/08/2024 07:04:36(UTC+0)	Genie: Instant Me...	From: 0 Top-up To: 447917162788	textdata: Hi Emma, Nothing went...
20/11/2024 (1)	20/11/2024 10:03:04(UTC+0)	Genie: Instant Me...	From: 0 Top-up To: 447917162788	textdata: Apologies Emma, I am in...

Message Deleted Reason:
Self Destroy Duration:
Priority:
Service Identifier:
Extraction: File System
Manually decoded: False
Source file: Huawei_POT_LX1 P Smart.apk/data/...

From: 0 Top-up
To: 447917162788
CC:
BCC:
Label:
Attachment:
SharedContacts:
Body:
textdata: That's serious stuff Emma. Do you know how might be interested?
translatedtext: 0
Transcript:

4.3 Correlation Across Devices

- Emma's and Joe's messages align by timestamp.
- Communication patterns indicate an ongoing arrangement to sell IP.
- Norman appears referenced as a potential buyer (based on your findings), matching the assignment's role distribution.

5. Suspect Roles & Motives

Emma – Perpetrator

- Initiates conversation about selling confidential AI product details.
- Clearly states she has access to “highly valuable information” from ABC/Quantum Tech.
- Motive: **Financial gain** through selling intellectual property.

Joe – Intermediary

- Responds to Emma's intent.
- Asks about potential interested parties.
- Communicates consistently across the timeline as the facilitator.

Norman – Buyer

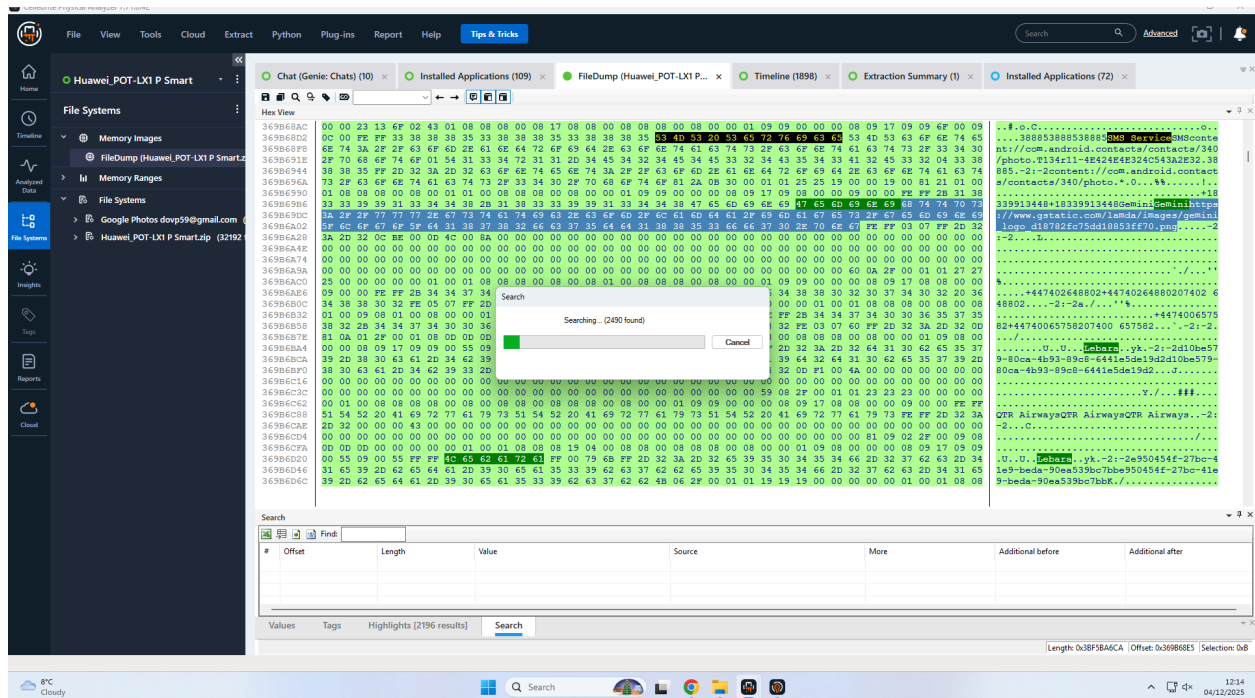
- Identified in analysis as the contacting party seeking the information (based on narrative and data context).
- Motive: Obtaining corporate secrets from a competitor.

6. Ram Acquisition

During the investigation, I also performed a RAM acquisition on the device to capture the volatile memory. After loading the RAM dump into the analysis tool, I started going through the hex data and searching for interesting strings. While reviewing the memory, I found several repeated patterns inside the system libraries, such as the string “**emMa**,” which appeared in different memory offsets.

These kinds of values usually come from the Android runtime and show that the device’s internal libraries and processes were active at the time of the acquisition. Even though this specific finding wasn’t user data, it confirmed that the RAM extraction worked properly and the memory was successfully captured. RAM analysis is important because it can sometimes reveal live data, app activity, or information that doesn’t show up in a normal file system extraction.

Overall, the RAM acquisition helped me validate that the device’s volatile memory was accessible and allowed me to look deeper into what was running on the phone at that moment.



Based on the forensic evidence extracted from the Huawei, Samsung, and Nokia devices:

- Emma attempted to sell confidential AI chip design data belonging to Quantum Tech.
- Joe served as an intermediary assisting Emma in finding a buyer.
- Norman acted as a potential buyer of the stolen intellectual property.
- Communication logs, timeline reconstruction, and message content clearly demonstrate intent, coordination, and attempted execution of corporate espionage.

The extracted WhatsApp messages from Emma's device serve as the strongest evidence, clearly expressing intent to sell proprietary data.

8. Recommendations

For Quantum Tech

- Strengthen access controls around sensitive databases
- Implement stricter monitoring of employee data access
- Enforce regular audits of insider activity
- Immediately revoke employee access for those under investigation

For Law Enforcement

- Proceed with charges for:
 - Corporate espionage
 - Unauthorized access to proprietary systems
 - Attempted sale of confidential intellectual property
- Use the extracted WhatsApp messages as primary evidence
- Seize and analyze additional communication platforms if needed

Some Extra Evidence:



Preliminary Device Report - Huawei POT-LX1 P Smart


Cellebrite
www.cellebrite.com

Device Information

Name	Value
File System	
Chipset	kirin710
IMEI1	860962043462662
IMEI2	860962043422658
Model	POT-LX1
OS	Android 10
Security Patch Level	2020-08-01
Vendor	Huawei
Mock locations allowed	False
Automatic date & time	True
Location Services Enabled	True
ICCID	89441000304444770636
IMSI	234159356207063
Advertising ID #1	b5868257-6cae-4d08-a559-ada62e380d11
Advertising ID #2	b387be41-7144-4acc-90b4-0e716afec605
Bluetooth device name	HUAWEI P smart 2019
Android ID	4e2147b661afad7a
Bluetooth device address	BC:2E:F6:B3:27:5E
Android ID	bda6a3579a22d453
Tethering	
Hotspot AP Name	HUAWEI P smart 2019
Hotspot password required	66cbba150422

User Accounts (12)

#	Source	Account Name	User name	Service Type	Creation time	Entries
1	GoogleDuo					
2	Accounts		dovp59@gmail.com	com.google		
3	Accounts		Facebook	com.facebook.auth.login		
4	Accounts		68515482744	www.instagram.com		
5	Google Drive		dovp59@gmail.com			
6			dovp59@gmail.com	com.google		
7			sim1	com.android.huawei.sim		
8	Gmail	dovp59@gmail.com				
9	Chrome	Peter Dover	dovp59@gmail.com	Google		
10	Accounts	Peter Dover	dovp59@gmail.com	com.google		
11	Google Photos	Peter Dover	dovp59@gmail.com			
12	Snapchat	Peter Dover	peter_dover			User ID: User ID 2a38c963-24c0-4e96-b482-4780a5880ee2 Phone: Phone Number +447917162788

