

A large red circular graphic on the left side of the slide, partially cut off by the edge.

Digital
Forensic
Investigation
Report

Case: Investigation of
Attempted Corporate
Espionage – QT-AI-2025 Case

Presented By: Shahriar
Badhan

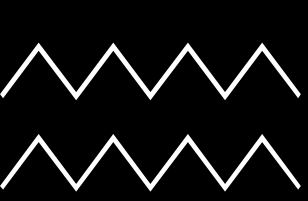
Id: 2505521



Case Background

Case Background – Unauthorized Access

- This case started when Unauthorized access detected in Quantum Tech's patent database
- Targeted file: **QT-AI-2025 confidential AI chip design**
- Activity suggested attempted data extraction
- Suspicious activity began after onboarding Emma, who showed abnormal access patterns.



Investigation Objectives



Determine whether Emma intended to leak confidential data



Identify any attempted or successful data transfer



Analyse communication between Emma → Joe → Norman



Evaluate forensic artefacts from mobile extraction

Key Investigation Timeline

**24/03/2026 —
Motorola device
connected** (*Motorola
Edge 50 Neo detected
in UFED*)

**15/04/2026 —
Motorola extraction
completed** (*Android
Backup method + hash
verification*)

**17/06/2024 — Huawei
device call logs
analysed** (*Repeated
calls between Emma &
Joe*)

**18–19/08/2024 —
Huawei outgoing calls
found** (*External
numbers contacted
multiple times*)

**Instagram evidence
from Huawei device**
(*Norman found in
contact list*)

**WhatsApp chats from
Huawei device** (*Emma
→ Joe communication*)

**Samsung-related
artefacts (if any)** (*If
Samsung device was
part of group
chat/media — optional*)

**14/04/2026 —
Motorola location
metadata recorded**
(*Movement timeline
reconstructed*)

**File system deletion
traces found** (*Possible
attempt to hide
QT-AI-2025 activity*)

Phone Investigation

UFED Case Initialization – Motorola Edge 50 Neo

Case Identifier: Phone

Examiner Name: Shahrior

Device Name / Evidence Number: Shahrior-01

Crime Type: Criminal Mischief

Department:

Location:

Last Case Details:

Case Identifier: Phone

Examiner Name: Shahrior

Device Name / Evidence Number: Shahrior-01

Crime Type: Criminal Mischief

Department:

Location:

USE LAST DETAILS

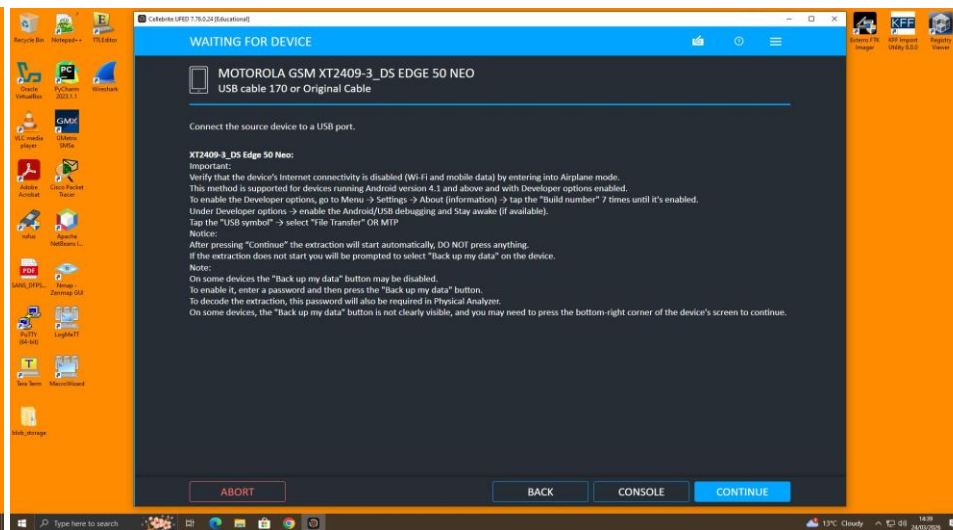
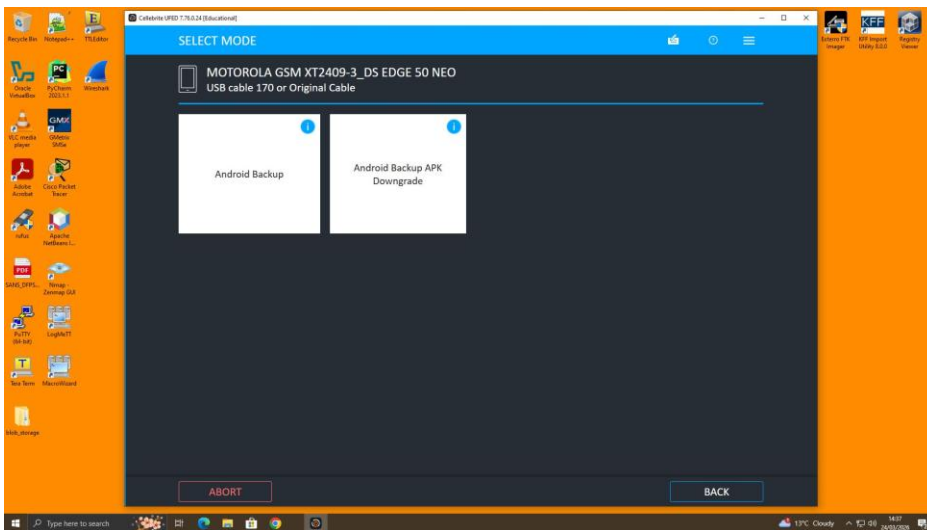
ABORT BACK CONTINUE

- ☐ New forensic case created in UFED
- ☐ Case ID, Examiner Name, Device ID documented
- ☐ Ensures chain-of-custody and forensic integrity
- ☐ Starting point of mobile investigation

Phone investigation

Device Detection & Identification

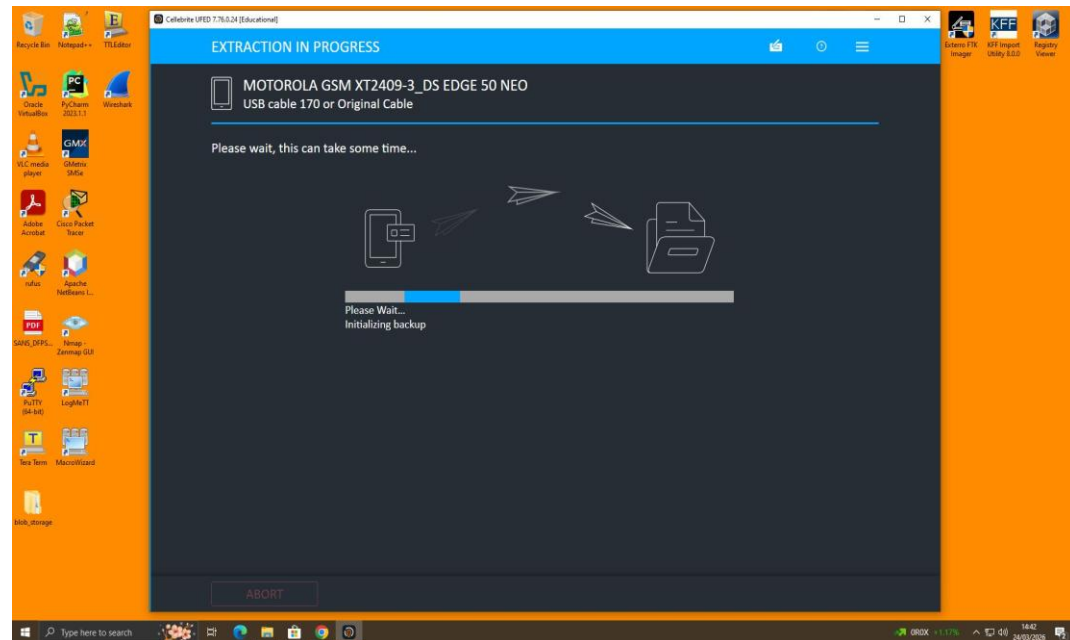
- UFED Auto Detect identifies **Motorola Edge 50 Neo**
- Device info: chipset, Android version, security patch
- Debugging & Airplane Mode required
- Confirms device readiness for extraction



Phone Investigation

Data Extraction – Android Backup Method

- Logical extraction started using Android Backup
- UFED reads data in real-time
- No user interaction allowed during extraction
- Ensures complete and untampered data capture



Cellebrite Physical Analyzer 7.73.0.11

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

Search Advanced

The license expires in 15 days. [License details](#)

Motorola GSM_XT2409-... Tips & Tricks Extraction Summary (1) x

All Content File System

Extraction Summary

+ Add extraction + Add external file Project settings Generate report Open Virtual Analyzer

Extractions: 1



File System
Motorola GSM_XT2409-3_DS Edge 50...
File System [Android Backup]
▲ Selective apps decoding

Extraction start date/time
15/04/2026 13:31:19(UTC+1)
Extraction end date/time
15/04/2026 14:09:42(UTC+1)

Image Hashes

Calculating hash...

Device Info

[Generate preliminary device report](#)

Chipset	MT6878	Taken from UFD extraction file
Android ID	2d5a9a7651de5963	Taken from UFD extraction file
IMEI1	352166632557917	Taken from UFD extraction file
IMEI2	352166632557925	Taken from UFD extraction file
Model	motorola edge 50 neo	Taken from UFD extraction file
OS	15	Taken from UFD extraction file
Security Patch Level	2026-03-01	Taken from UFD extraction file
Vendor	motorola	Taken from UFD extraction file

Content

Selected applications [GO](#)

Google Meet	imo-International Calls & Chat	Gmail
Messenger	Google Chrome: Fast & Secure	Digital Wellbeing
Google	YouTube	Amazon Shopping
Google Photos	Google Docs	Google Drive
Google Keep - Notes and Lists	Google Calendar	Google Wallet

Insights from Installed Apps

- Hide files or pictures (1 apps)
- Developer tools (1 apps)
- Unknown (5 apps)

[View all](#)

Extraction Completed – Integrity Verified

- ❑ Extraction finished successfully
- ❑ MD5 & SHA-1 hash values generated
- ❑ Confirms data integrity and no tampering
- ❑ This device was Ready for analysis in Physical Analyzer

Communication Analysis (WhatsApp & Instagram)

- WhatsApp messages show confidential discussions Emma and Joe.
- ~~Joe~~ negotiating with external contacts
- Instagram contact list includes Norman ,a senior member of the competitor.
- This confirms multi-platform communication

The image displays four screenshots of the Huawei_POT-LX1 P Smart analysis interface, showing various data extraction and communication analysis results.

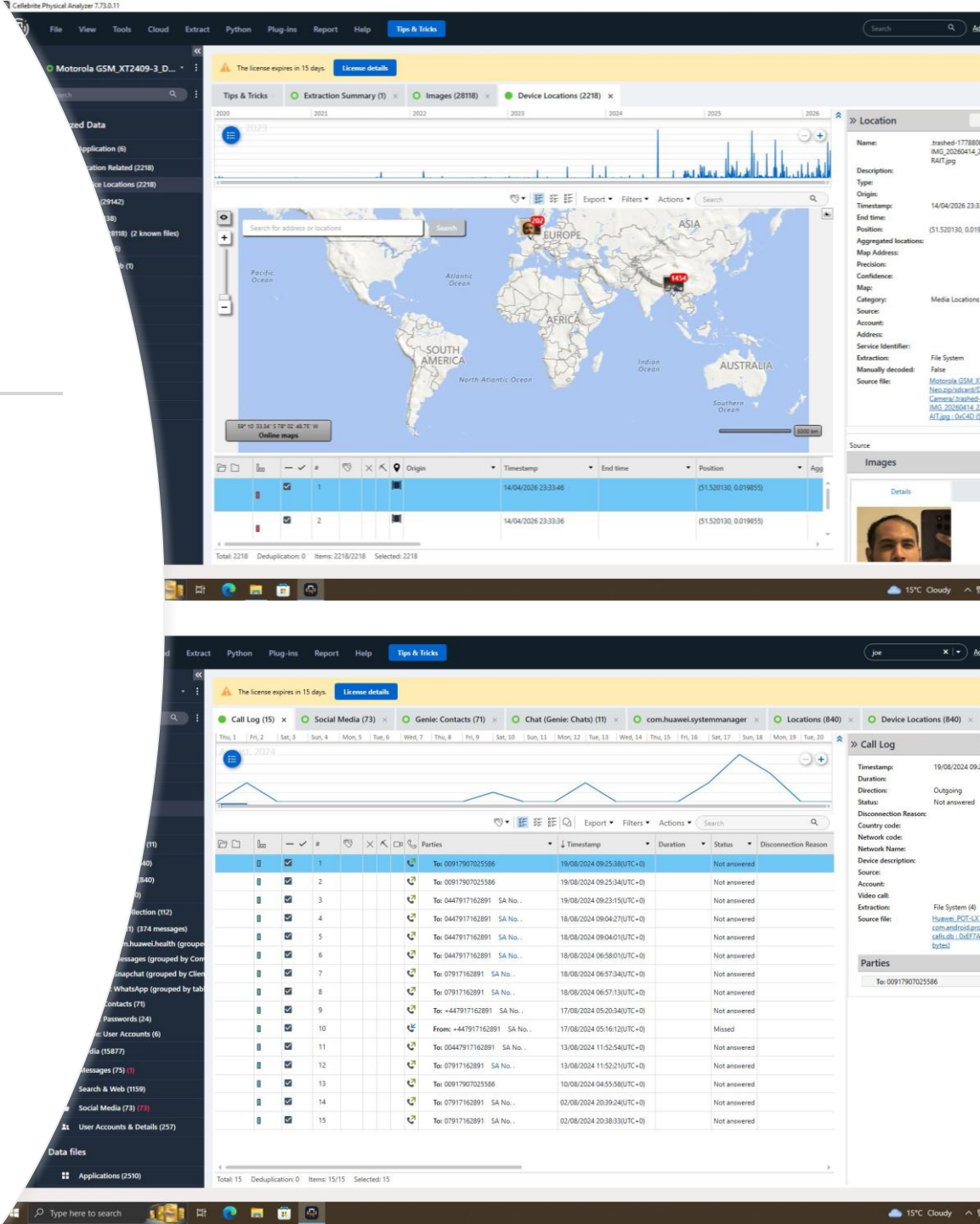
Top Left Screenshot: Shows the 'Analyzed Data' section with a list of extracted data items, including 'Messages (15)', 'Locations (15)', 'Device Locations (15)', 'Manual Data Collection (15)', 'Generic Chats (15)', 'Generic Contacts (15)', 'Generic Messages (15)', 'Generic User Accounts (15)', 'Media (15)', 'Audio (15)', 'Images (15)', 'Videos (15)', and 'Messages (15)'. The 'Messages (15)' item is selected.

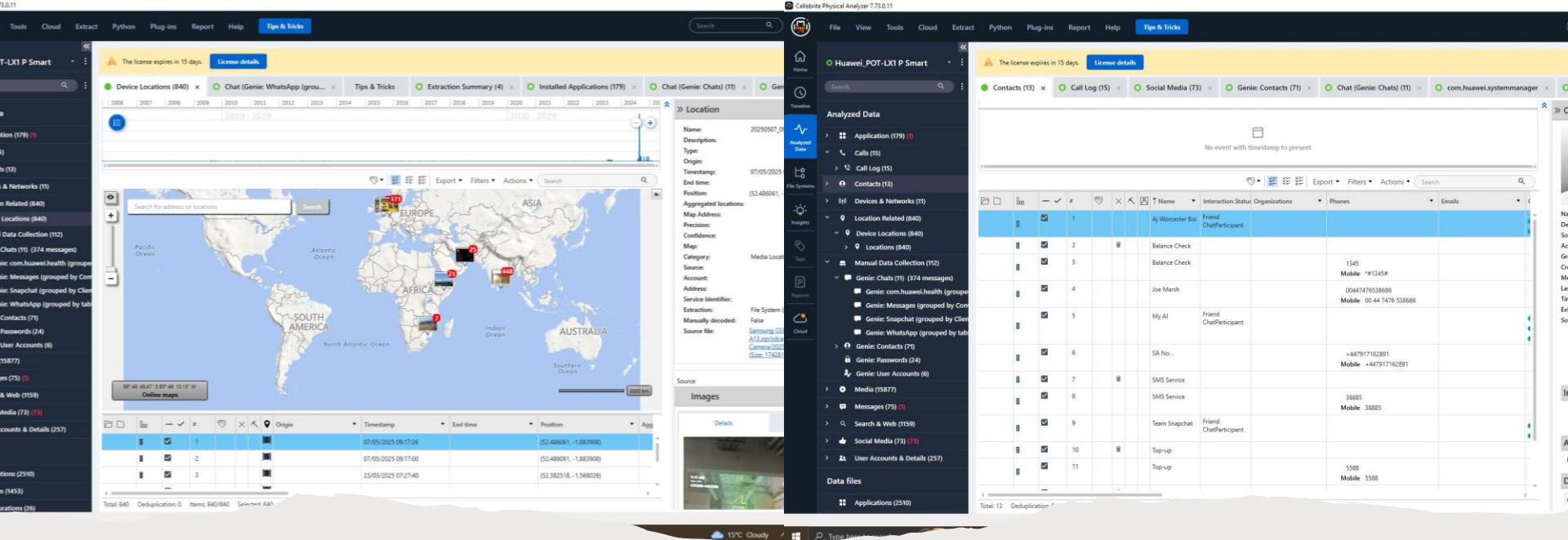
Top Right Screenshot: Shows the 'Chat (Generic WhatsApp (15))' section with a table of chat data. The table has columns for 'Name', 'Device description', 'Source', 'Account', 'Group', 'Contact', 'Modified', 'Last time contacted', 'Texts contacted', 'Extractions', 'Manually deleted', and 'Source file'. The table lists several contacts, including 'Norman Smith' and 'Peter Dover'.

Bottom Left Screenshot: Shows the 'Contact (Generic WhatsApp (15))' section with a table of contact data. The table has columns for 'Name', 'Device description', 'Source', 'Account', 'Group', 'Contact', 'Modified', 'Last time contacted', 'Texts contacted', 'Extractions', 'Manually deleted', and 'Source file'. The table lists several contacts, including 'Norman Smith' and 'Peter Dover'.

Bottom Right Screenshot: Shows the 'Chat (Generic WhatsApp (15))' section with a table of chat data. The table has columns for 'Name', 'Device description', 'Source', 'Account', 'Group', 'Contact', 'Modified', 'Last time contacted', 'Texts contacted', 'Extractions', 'Manually deleted', and 'Source file'. The table lists several contacts, including 'Norman Smith' and 'Peter Dover'.

- ❑ Found Repeated calls between Emma & Joe
- ❑ Call timings match WhatsApp conversations
- ❑ Location data extracted from Motorola media files
- ❑ Supports timeline reconstruction





File System Findings & Media Metadata

- UFED shows all Install apps. This helps identify apps used for communication or file transfer.
- Audio metadata confirms authenticity, that means file are original and not edited.
- Location + media artefacts support movement timeline that shows track where the device was at different times.
- No QT-AI-2025 file found, but deletion traces exist, that means someone tried to hide activity.



Conclusion & Recommendations

- ❑ In conclusion, the evidence shows attempted data leakage, not a completed transfer.
- ❑ The communication chain Emma → Joe → Norman is clearly established.
- ❑ I recommend legal action, stronger access controls, server-side audits, and improved employee security training.



**Thank you
Everyone**