

DIGITAL FORENSIC ANALYSIS (ACCA7031)

Student Name: Md Al Amin Sarkar Reday
Student ID: 2406207

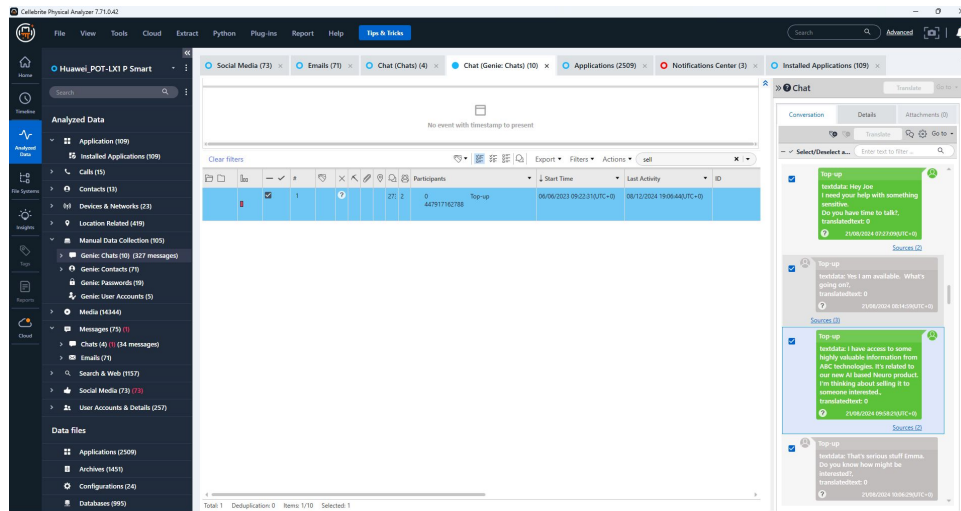
Introduction

The case under investigation is an advanced insider threat in the Quantum Technologies, where the theft of the QT-AI-2025 chip design patent has led to a well-planned conspiracy between the internal and external sources. Digital device forensics is to be conducted to track the flows and communications of the suspected individuals, Emma, Joe, and Norman, to be in a position to establish a clear chain of evidence of their actions leading to theft and attempted sale of the intellectual property that was of critical value. Investigating the dates, phone logs, and financial records will help transform accusations into evidence admissible in court, thus proving the claims of corporate spying and holding those responsible to face justice over the intrusion.

Huawei Device

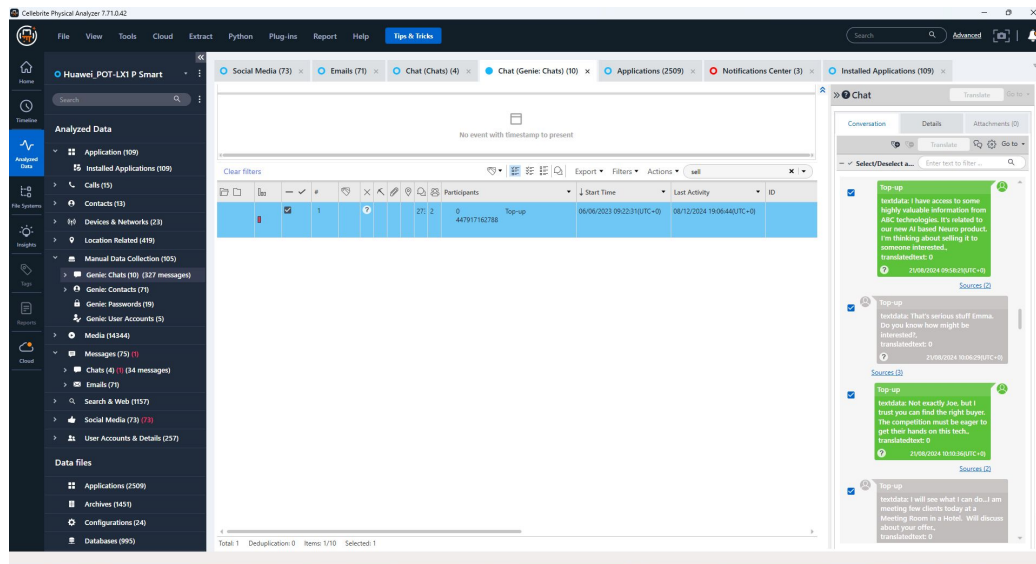
The chronology is presented as messages shared on the 21st of August 2024 with a conversation that is critical wherein the sender makes a direct contact with the receiver by calling him Hey Joe which confirms the identity of the receiver directly on the text.

This discussion is then progressed to discussing the possible sale of highly valuable information of ABC technologies which is connected to a new AI based Neuro product, hence a direct connection between "Joe" and the alleged corporate espionage acts is created



Cont..

To Emma, who is desperate to sell the highly valuable information of ABC Technologies, Joe confirms that he is in the process of doing so, declaring that he will seek alternatives and is planning to have face-to-face meetings with the prospective clients in a meeting room in a hotel to make the offer. This message proves that Joe was the facilitator who arranged the illicit sale by physical face-to-face dealings.



Cont..

The communication of the 21 st August 2024 clearly portrays the conspiracy nature of both sides of the communication. This is demonstrated in their communications where they recognize that their activities are illegal and have a consensus to hide their operations. This coordination process was also operationalized on the 22 nd of August when they posted their exact position on Google Maps.

Caliber Physical Analyzer 7.7.15.42

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

Home Timeline

Analysed Data

- Application (100)
- Installed Applications (109)
- Calls (15)
- Contacts (13)
- Devices & Networks (23)
- Device Events (12)
- Wireless Networks (10)
- Location Related (383)
- Device Locations (383)
- Manual Data Collection (105)
- Genie: Chats (16) (327 messages)
- Genie: Contacts (7)
- Genie: Passwords (16)
- Genie: User Accounts (5)
- Media (14344)
- Audio (81)
- Images (14150) (156 known files)
- Videos (133)
- Messages (75) (1)
- Chats (4) (1) (34 messages)
- Emails (7)
- Search & Web (1157)
- Autofill (1)
- Cookies (122)
- Searched Items (100)
- User Dictionary (13)

Installed Applications (109) Chat (Genie: Chats) (16)

No event with timestamp to present

Participants	Start Time	Last Activity	ID
Peter Dover	05/11/2024 10:00:28(UTC+0)	05/11/2024 10:00:32(UTC+0)	
SMS Service	13/10/2024 15:45:20(UTC+0)	28/10/2024 15:08:31(UTC+0)	
Peter Dover	26/08/2024 02:46:03(UTC+0)	26/08/2024 02:46:03(UTC+0)	
SMS Service	17/08/2024 02:35:34(UTC+0)	17/08/2024 02:35:28(UTC+0)	
Peter Dover	17/08/2024 02:27:45(UTC+0)	17/08/2024 02:27:45(UTC+0)	
SMS Service	13/08/2024 11:56:30(UTC+0)	21/08/2024 04:46:05(UTC+0)	2026c8f-485e-5
Peter Dover	02/08/2024 20:37:51(UTC+0)	19/08/2024 10:50:15(UTC+0)	
SMS Service	02/08/2024 20:36:38(UTC+0)	05/12/2024 00:46:22(UTC+0)	
Top-up	06/06/2023 09:22:31(UTC+0)	06/12/2024 18:06:44(UTC+0)	

Total: 10 Deduplication: 0 Items: 10/10 Selected: 10

Chat

Conversation Details Attachments (3)

Select/DeSelect all Enter text to filter

Top-up

Textdata: Perfect. Let's keep this under wraps. This could be huge for both of us.

21/08/2024 14:47:19(UTC+0)

Sources (2)

Top-up

Textdata: Absolutely. I will update you once I have got some responses. Stay safe.

21/08/2024 14:45:29(UTC+0)

Sources (3)

Top-up

Textdata: P?

21/08/2024 14:37:33(UTC+0)

Sources (3)

Top-up

Textdata: See my real-time location on Maps: <https://maps.app.goo.gl/CV9vgt1QGbua1gthn8>.

21/08/2024 14:37:33(UTC+0)

Sources (3)

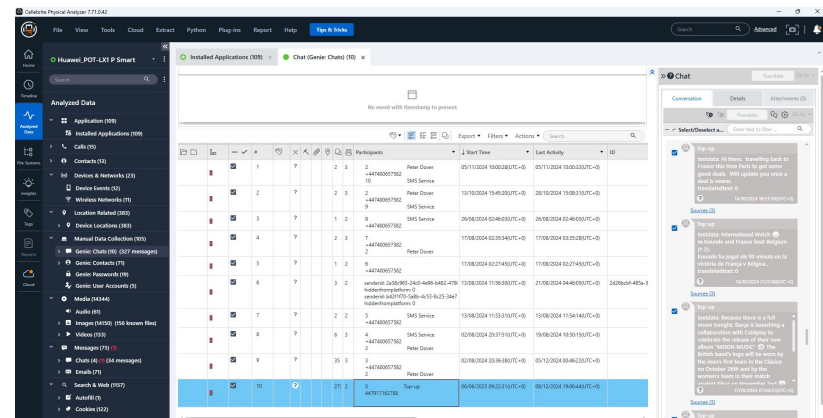
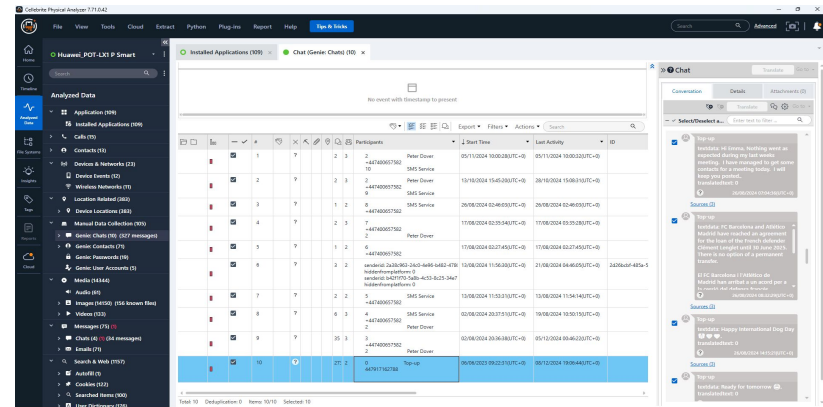
Top-up

Textdata: Here Erick! I.

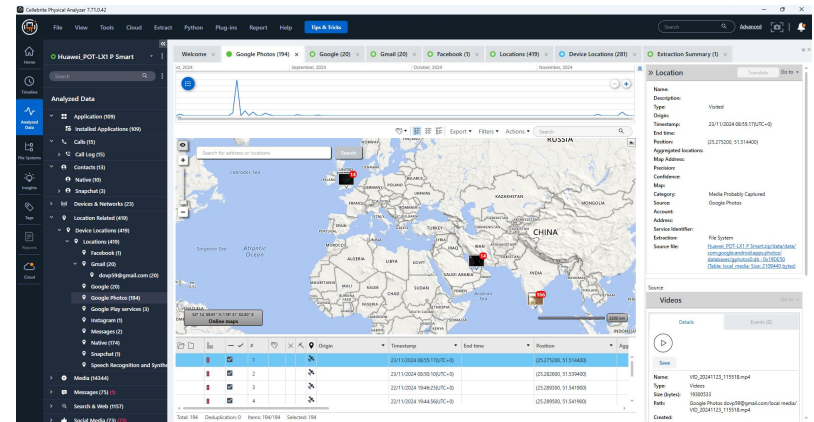
21/08/2024 14:37:33(UTC+0)

Cont..

The forensic examination shows that Joe is the consistent actor as the organizer of the conspiracy as he sends a message on August 26, 2024, where he admits to a failed meeting but immediately gains new contacts, which shows that the operation is planned repeatedly. This continued role is further affirmed by another communication dated October 14, 2024, where he tells Emma that he is going to Paris to work out the deal.

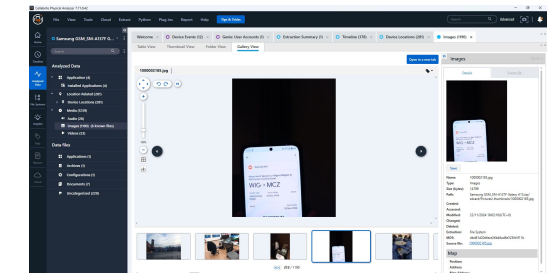
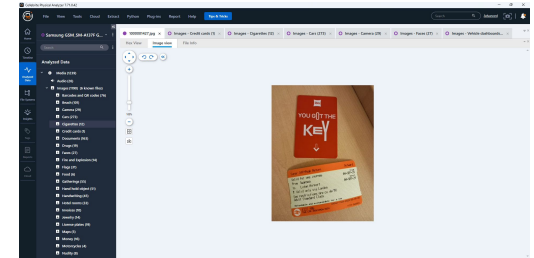
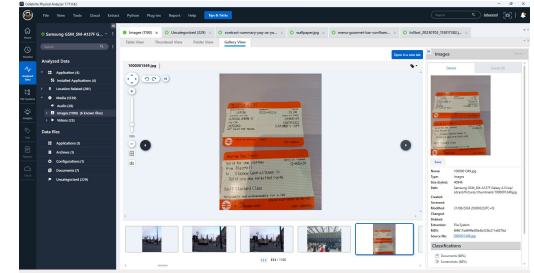


Physical evidence found on his device is directly verified by a forensic analysis of a communication sent by Joe on August 29, 2024. Joe mentions in the message that he is going to Glasgow on a meeting and it exactly correlates with digital train tickets and a station receipt on the same date that are on his phone. More so, a geospatial analysis of the information of the device traces the history of his whereabouts on the map, re-creating his movements in the course of the conspiracy.



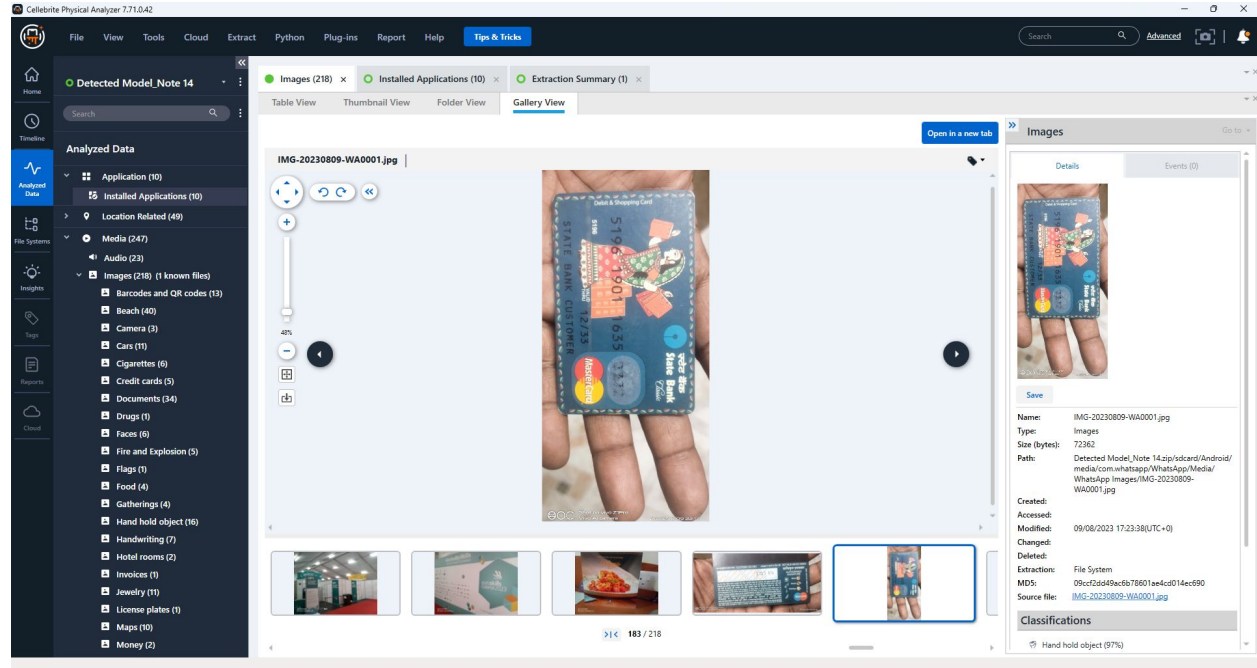
Cont..

An electronic analysis of the Samsung phone owned by Joe found digital train tickets and a receipt of his collection, which puts him physically in the Glasgow area between August 29th and 31st, 2024. This can be directly cross-examined with his digital correspondence by this verifiable timeline that includes a receipt of Glasgow Queen Street station and a ticket of Blairhill to Glasgow. Further pieces of evidence like a digital ticket of travelling between Wigan and Manchester further tracks his movements during the conspiracy period.

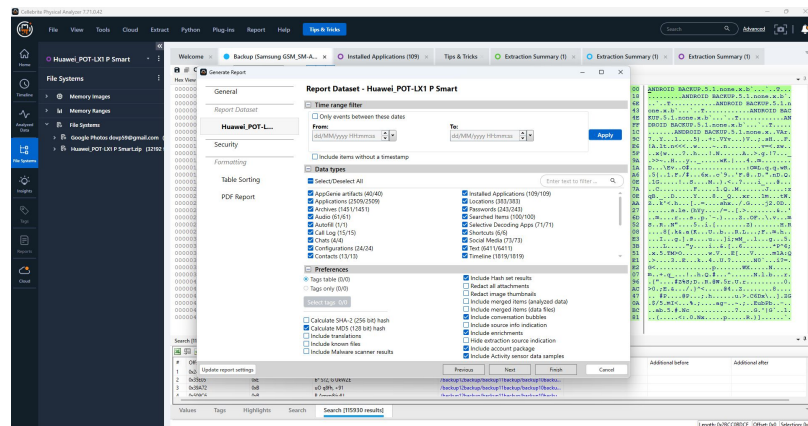
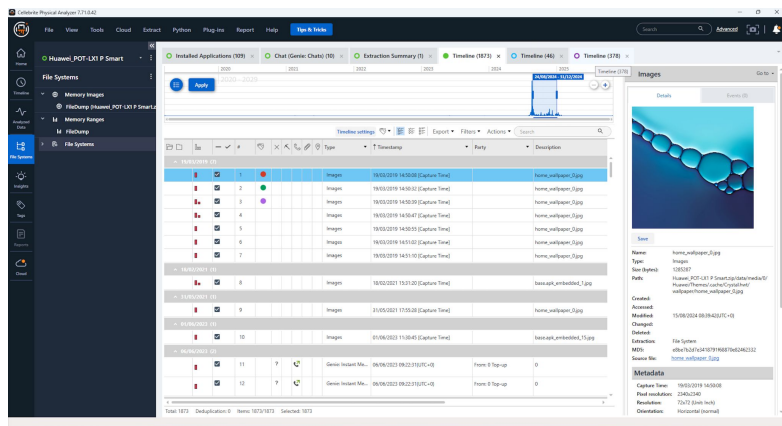


The Ulefone Device

A forensic examination of the Ulefone gadget showed an Indian Maestro debit card, produced on the 9th of August 2023, which is a year older than Emma started to engage in active espionage communications.



Evidence tagging & Report generation



Evidence tagging is a forensic procedure that is vital and requires an organized process of labeling and classifying digital artifacts to preserve chain of custody and contextual relevance. After this, a detailed report is created to bring together findings, methodologies, and conclusions of the tagged evidence into a logical story of investigation or legal action.

Conclusion

The evidence of the three devices has made the case and roles have been definitely allocated in the Quantum Tech plot. Emma in the UK was the mastermind of the case, as she accessed the core trade secrets on her Huawei phone and launched the plot. With Joe, her middleman, in the UK on a Samsung, the dirty business of locating buyers and transferring the stolen data to an offshore location was done. One more participant in the network, Norman in India on a Ulefone, is under investigation, but his role remains unclear, whether he was a former accomplice, world contact, or money mover.