

DIGITAL FORENSIC ANALYSIS (ACCA7031)

Name: Jyothi Avulareddygari

Student ID: 2436065

Introduction

According to a report issued by quantum technologies, it was the subject of a critical security incident in the form of unauthorized access and attempted theft of its proprietary AI chip design patent (ID: QT-AI-2025). There are even early indications of insider threat by people constituting part of its own IT security team.

Key Allegations

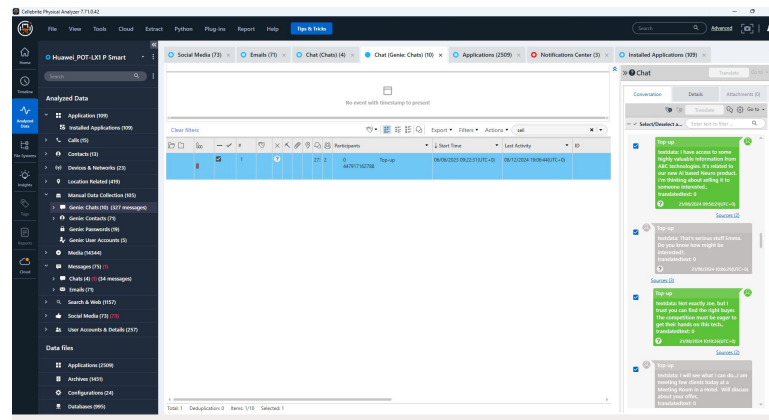
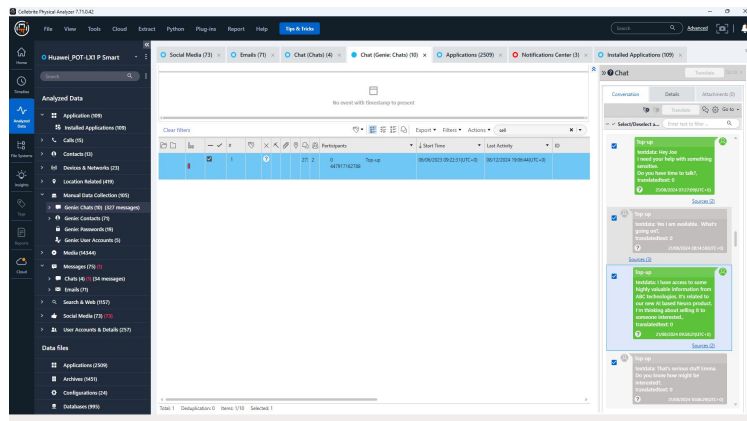
The Intellectual Property: QT-AI-2025, a high-price patent core to the competitive edge of Quantum Tech.

The Suspected Plot: There was an insider conspiracy to steal and sell intellectual property to a rival, NexGen Circuits.

The Reported Actors:

- Emma: a senior engineer who is likely to be the main culprit who had accessed the database.
- Joe: Proclaimed middleman who brings the sale.
- Norman: A third person associated with the conspiracy network; part that is being investigated.

Huawei Device



The investigation defines Joe as the facilitator and an active organizer of meetings with the buyers of the stolen trade secrets to sell them. This role is directly proved in the message to Emma, where he is sure that he will meet clients to talk about the proposal of information of high value provided by ABC technologies.

Cont..

The screenshot displays the Cellebrite Physical Analyzer interface. The left sidebar shows a tree view of analyzed data, including 'Application (100)', 'Calls (1)', 'Device & Networks (23)', 'Device Events (2)', 'Wireless Networks (1)', 'Location Related (183)', 'Device Locations (183)', 'Manual Data Collection (767)', 'Generic Contacts (10) (127 messages)', 'Generic Passwords (1)', 'Generic User Accounts (5)', 'Media (14344)', 'Audio (8)', 'Images (1610) (155 known files)', 'Videos (123)', 'Messages (73) (1) (14 messages)', 'Chats (4) (1) (14 messages)', 'Emails (7)', 'Search & Web (1157)', 'Cookies (102)', 'Search Items (100)', and 'User Data/History (100)'. The main pane shows a table of installed applications with columns for Participants, Start Time, Last Activity, and ID. A chat window is open on the right, showing a conversation with a contact named 'Joe'.

Participants	Start Time	Last Activity	ID
2 44742065782 10	05/11/2024 10:00:26(UTC+0)	05/11/2024 10:00:32(UTC+0)	
2 44742065782 9	13/10/2024 15:49:20(UTC+0)	26/10/2024 15:08:33(UTC+0)	
3 44742065782 3	26/08/2024 02:46:03(UTC+0)	26/08/2024 02:46:03(UTC+0)	
2 44742065782 2	17/08/2024 02:35:34(UTC+0)	17/08/2024 02:35:36(UTC+0)	
6 44742065782 1 2	17/08/2024 02:27:45(UTC+0)	17/08/2024 02:27:45(UTC+0)	
3 44742065782 2	13/08/2024 11:56:31(UTC+0)	21/08/2024 06:48:03(UTC+0)	2028634 4454-5
3 44742065782 2	13/08/2024 11:56:31(UTC+0)	13/08/2024 11:56:31(UTC+0)	
4 44742065782 2	02/08/2024 20:37:51(UTC+0)	16/08/2024 10:58:10(UTC+0)	
3 44742065782 3	02/08/2024 20:36:18(UTC+0)	05/12/2024 09:46:32(UTC+0)	
6 44742065782 1 2	05/08/2024 09:42:31(UTC+0)	05/12/2024 09:46:32(UTC+0)	

The screenshot displays the Cellebrite Physical Analyzer interface. The left sidebar shows a tree view of analyzed data, including 'Application (100)', 'Calls (1)', 'Device & Networks (23)', 'Device Events (2)', 'Wireless Networks (1)', 'Location Related (183)', 'Device Locations (183)', 'Manual Data Collection (767)', 'Generic Contacts (10) (127 messages)', 'Generic Passwords (1)', 'Generic User Accounts (5)', 'Media (14344)', 'Audio (8)', 'Images (1610) (155 known files)', 'Videos (123)', 'Messages (73) (1) (14 messages)', 'Chats (4) (1) (14 messages)', 'Emails (7)', 'Search & Web (1157)', 'Cookies (102)', 'Search Items (100)', and 'User Data/History (100)'. The main pane shows a table of installed applications with columns for Participants, Start Time, Last Activity, and ID. A chat window is open on the right, showing a conversation with a contact named 'Joe'.

Participants	Start Time	Last Activity	ID
2 44742065782 10	05/11/2024 10:00:26(UTC+0)	05/11/2024 10:00:32(UTC+0)	
2 44742065782 9	13/10/2024 15:49:20(UTC+0)	26/10/2024 15:08:33(UTC+0)	
3 44742065782 3	26/08/2024 02:46:03(UTC+0)	26/08/2024 02:46:03(UTC+0)	
2 44742065782 2	17/08/2024 02:35:34(UTC+0)	17/08/2024 02:35:36(UTC+0)	
6 44742065782 1 2	17/08/2024 02:27:45(UTC+0)	17/08/2024 02:27:45(UTC+0)	
3 44742065782 2	13/08/2024 11:56:31(UTC+0)	21/08/2024 06:48:03(UTC+0)	2028634 4454-5
3 44742065782 2	13/08/2024 11:56:31(UTC+0)	13/08/2024 11:56:31(UTC+0)	
4 44742065782 2	02/08/2024 20:37:51(UTC+0)	16/08/2024 10:58:10(UTC+0)	
3 44742065782 3	02/08/2024 20:36:18(UTC+0)	05/12/2024 09:46:32(UTC+0)	
6 44742065782 1 2	05/08/2024 09:42:31(UTC+0)	05/12/2024 09:46:32(UTC+0)	

The messages show how Joe was constantly taking the role of a facilitator, actively seeking to find buyers to the stolen information even when faced with failure and even went to other countries in search of business. Moreover, the fact that the communication between the conspirators and the location were very explicit shows that their operation was well coordinated, clearly thought out, and consciously illegal.

Cont..

The screenshot shows the Colossus Project Analyzer 7.10.042 interface. The 'Installed Applications' table is displayed with columns for Application, Start Time, and Last Activity. The table contains 10 rows of data, including applications like 'Huawei_POT-LXI P Smart', 'Huawei_POT-LXI P Smart', 'Huawei_POT-LXI P Smart', 'Huawei_POT-LXI P Smart', 'Huawei_POT-LXI P Smart', 'Huawei_POT-LXI P Smart', 'Huawei_POT-LXI P Smart', 'Huawei_POT-LXI P Smart', 'Huawei_POT-LXI P Smart', and 'Huawei_POT-LXI P Smart'. The chat window on the right shows a conversation between 'Joe' and 'Peter' discussing the project.

Application	Start Time	Last Activity
Huawei_POT-LXI P Smart	05/11/2024 10:00:28(UTC+0)	05/11/2024 10:00:28(UTC+0)
Huawei_POT-LXI P Smart	13/10/2024 15:45:28(UTC+0)	26/10/2024 13:08:13(UTC+0)
Huawei_POT-LXI P Smart	26/08/2024 03:46:03(UTC+0)	26/08/2024 03:46:03(UTC+0)
Huawei_POT-LXI P Smart	17/08/2024 03:53:34(UTC+0)	17/08/2024 03:53:34(UTC+0)
Huawei_POT-LXI P Smart	17/08/2024 03:53:34(UTC+0)	17/08/2024 03:53:34(UTC+0)
Huawei_POT-LXI P Smart	17/08/2024 03:53:34(UTC+0)	17/08/2024 03:53:34(UTC+0)
Huawei_POT-LXI P Smart	17/08/2024 03:53:34(UTC+0)	17/08/2024 03:53:34(UTC+0)
Huawei_POT-LXI P Smart	17/08/2024 03:53:34(UTC+0)	17/08/2024 03:53:34(UTC+0)
Huawei_POT-LXI P Smart	17/08/2024 03:53:34(UTC+0)	17/08/2024 03:53:34(UTC+0)
Huawei_POT-LXI P Smart	17/08/2024 03:53:34(UTC+0)	17/08/2024 03:53:34(UTC+0)

The screenshot shows the Colossus Project Analyzer 7.10.042 interface. The 'Installed Applications' table is displayed with columns for Application, Start Time, and Last Activity. The table contains 10 rows of data, including applications like 'Huawei_POT-LXI P Smart', 'Huawei_POT-LXI P Smart', 'Huawei_POT-LXI P Smart', 'Huawei_POT-LXI P Smart', 'Huawei_POT-LXI P Smart', 'Huawei_POT-LXI P Smart', 'Huawei_POT-LXI P Smart', 'Huawei_POT-LXI P Smart', 'Huawei_POT-LXI P Smart', and 'Huawei_POT-LXI P Smart'. The chat window on the right shows a conversation between 'Joe' and 'Peter' discussing the project.

Application	Start Time	Last Activity
Huawei_POT-LXI P Smart	05/11/2024 10:00:28(UTC+0)	05/11/2024 10:00:28(UTC+0)
Huawei_POT-LXI P Smart	13/10/2024 15:45:28(UTC+0)	26/10/2024 13:08:13(UTC+0)
Huawei_POT-LXI P Smart	26/08/2024 03:46:03(UTC+0)	26/08/2024 03:46:03(UTC+0)
Huawei_POT-LXI P Smart	17/08/2024 03:53:34(UTC+0)	17/08/2024 03:53:34(UTC+0)
Huawei_POT-LXI P Smart	17/08/2024 03:53:34(UTC+0)	17/08/2024 03:53:34(UTC+0)
Huawei_POT-LXI P Smart	17/08/2024 03:53:34(UTC+0)	17/08/2024 03:53:34(UTC+0)
Huawei_POT-LXI P Smart	17/08/2024 03:53:34(UTC+0)	17/08/2024 03:53:34(UTC+0)
Huawei_POT-LXI P Smart	17/08/2024 03:53:34(UTC+0)	17/08/2024 03:53:34(UTC+0)
Huawei_POT-LXI P Smart	17/08/2024 03:53:34(UTC+0)	17/08/2024 03:53:34(UTC+0)
Huawei_POT-LXI P Smart	17/08/2024 03:53:34(UTC+0)	17/08/2024 03:53:34(UTC+0)

The messages of Joe show that he is trying all his best to be a facilitator and after a setback in late August, Joe obtains new contacts and eventually travels to Paris in October to make deals. This trend affirms the repetitive and cyclical character of the conspiracy to sell the stolen information.

The summary of chats between emma and joe

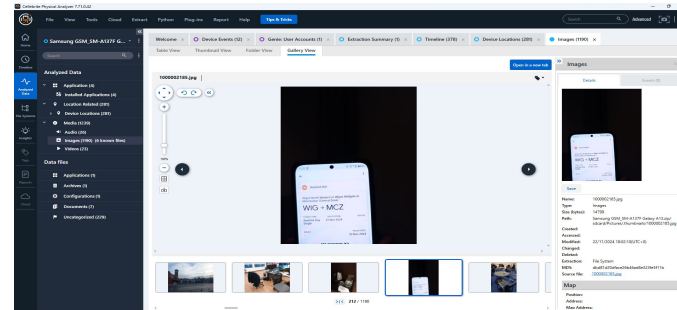
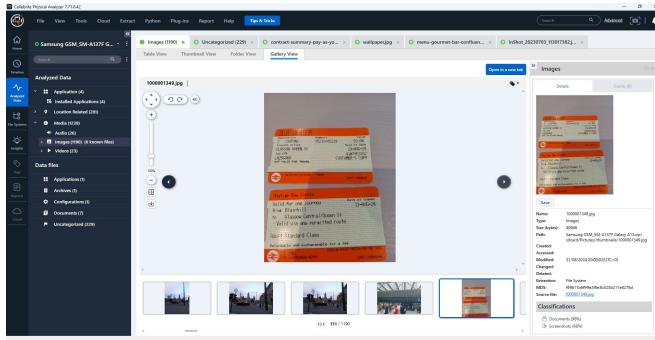
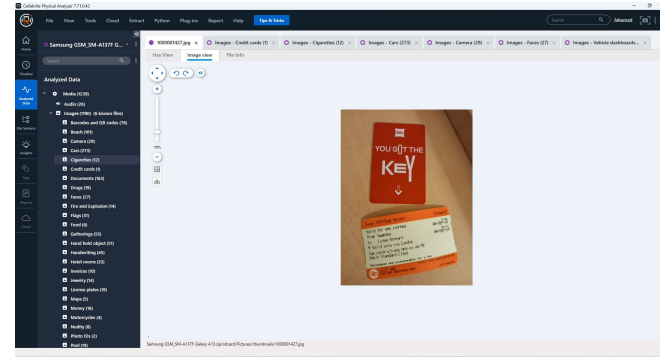
- ❑ The chat messages between Emma and Joe show that they organized the sale of confidential information of ABC Technologies. Their communication starts at the end of August 2024 with the open conversation on the illegality of their activity and the agreements to hide their actions, such as sharing the live locations. Joe, who is the facilitator, keeps Emma updated and reports on the first setbacks on August 26th before he finds new contacts. This conversation is especially incriminating as the messages that Joe sent regarding going to Glasgow to conduct meetings on August 29th are directly supported by digital train tickets and receipts located on his device, which establishes a verifiable connection between his intentions and actions.
- ❑ The dialogues also show a continued and cyclical conspiracy, full of a sense of urgency and operational specificity. Joe keeps on reassuring Emma that he was working hard, arranging meetings with clients in hotel meeting rooms and giving her definite travel schedules, such as going to Glasgow in August and Paris in October as he sought possible buyers. Not only does this paper trail of his bodily movements in the UK and into Europe create a clear timeline of intent and act, but it also demonstrates that both sides were fully aware that they were both involved in an illegal operation of making money off stolen information.

Summary of events

Date	Person(s)	Location	Event Description
August 21, 2024	Joe & Emma	Not specified	Explicit discussion of illegal activities; Google Maps location shared.
August 26, 2024	Joe	Not specified	Joe reports a setback in previous meetings but secures new contacts.
August 29, 2024	Joe	Glasgow, UK	Joe travels to Glasgow for meetings; train receipt and ticket evidence.
August 31, 2024	Joe	Blairhill → Glasgow, UK	"Anytime Day Single" ticket for travel from Blairhill to Glasgow Central/Queen St.
October 14, 2024	Joe	Paris, France	Joe informs Emma he is traveling to Paris to secure deals.
Various dates	Joe	Hotel meeting rooms	Joe meets potential buyers to discuss selling ABC technologies information.

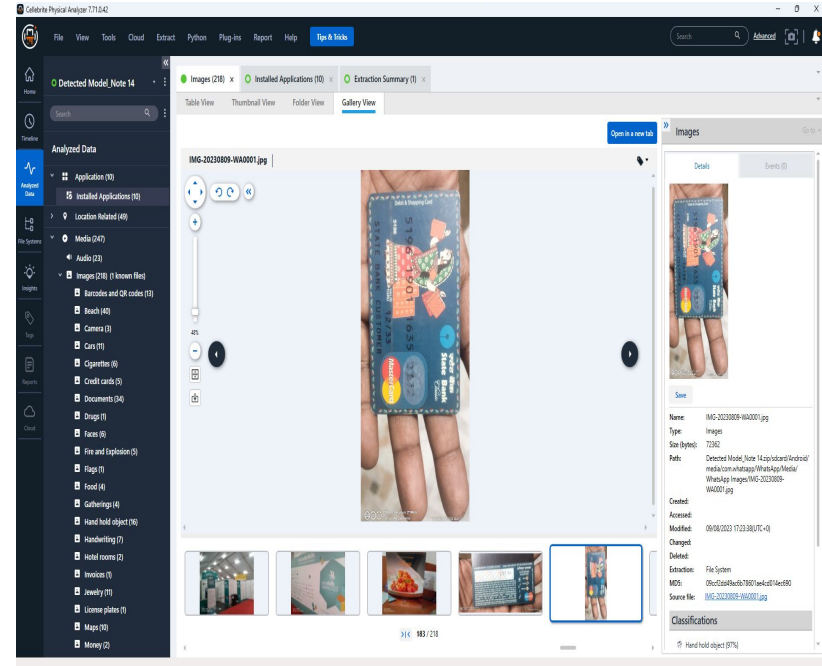
Cont..

The digital tickets and receipts recovered by the forensic examinations of the device used by Joe put him in Glasgow and Manchester in the late August of 2024, which comes as verifiable physical evidence of his whereabouts. This physical timeline is an important part of the cross-referential tool that matches his physical communication with his online activity and movement in the period of conspiracy.

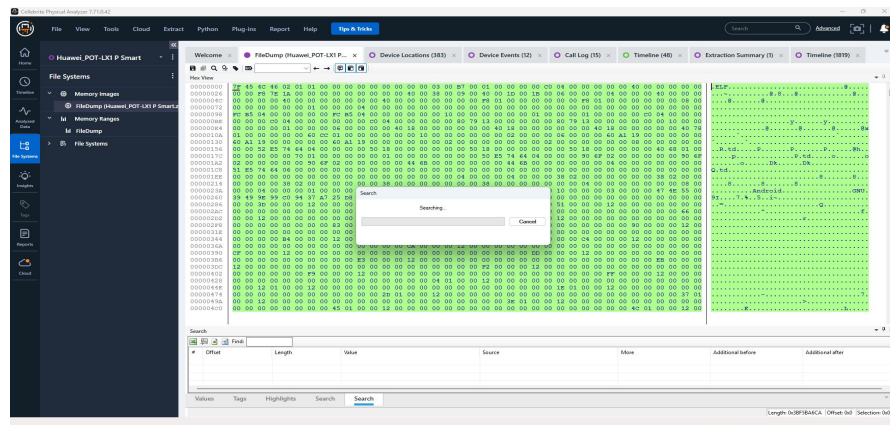
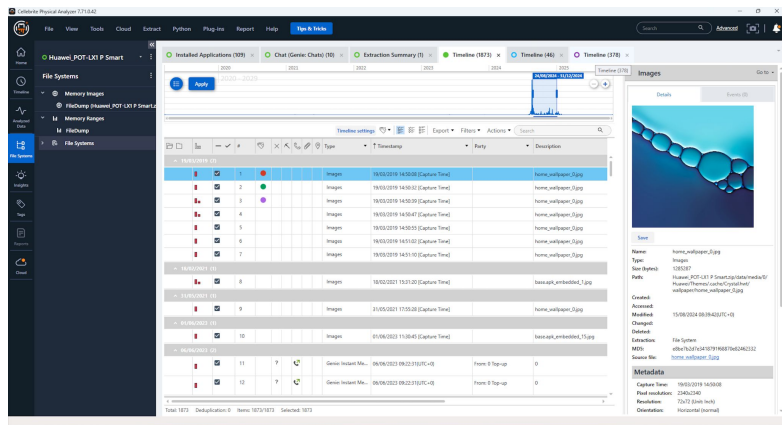


The Ulefone Device

This forensic evidence shows that there was an Indian Maestro debit card, which was issued on August 9, 2023, in the reviewed digital space. The fact is that the evidence can indicate that the card could be related to the device of a third party, which may broaden the conspiracy of the main participants, Joe and Emma. Although this brings in a new aspect, which is the indication of other monetary players or procedures, and it is essential to conduct further research to identify the role of this third party, its relationship, and its involvement in the overall scheme of brokering and selling confidential information.



Evidence tagging & Report generation



Conclusion

The main culprit is Emma who is working in the UK using a Huawei phone. Emma was the one who stole the trade secrets and was the initiator of the conspiracy. Joe, who is also situated in the UK and is also using a Samsung device was also playing the role of the facilitator. The work of Joe was to act as an intermediary, who would seek buyers and handle the offshore logistics and financial aspects to the plan. It is not clear the role of a third person, Norman in India with a Ulefone device. Although Norman was clearly a part of the network, it was not possible to establish precisely the role he played, whether as a former operative, a coordinator, or a financial contact.