

DIGITAL FORENSIC ANALYSIS (ACCA7031)

Name: Jyothi Avulareddygari

Student ID: 2436065

Introduction & Background

Quantum Technologies has reported a critical security incident involving the unauthorized access and attempted theft of its proprietary AI chip design patent (ID: QT-AI-2025). Initial internal alerts point to an insider threat involving members of its own IT security team.

Key Allegations

- The Target: QT-AI-2025, a high-value patent central to Quantum Tech's competitive advantage.
- The Suspected Plot: An internal conspiracy to steal and sell intellectual property to a competitor, NexGen Circuits.
- The Reported Actors:
 - Emma: A senior engineer, suspected as the primary perpetrator who accessed the database.
 - Joe: Alleged intermediary tasked with facilitating the sale.
 - Norman: A third individual linked to the conspiracy network; role under investigation.

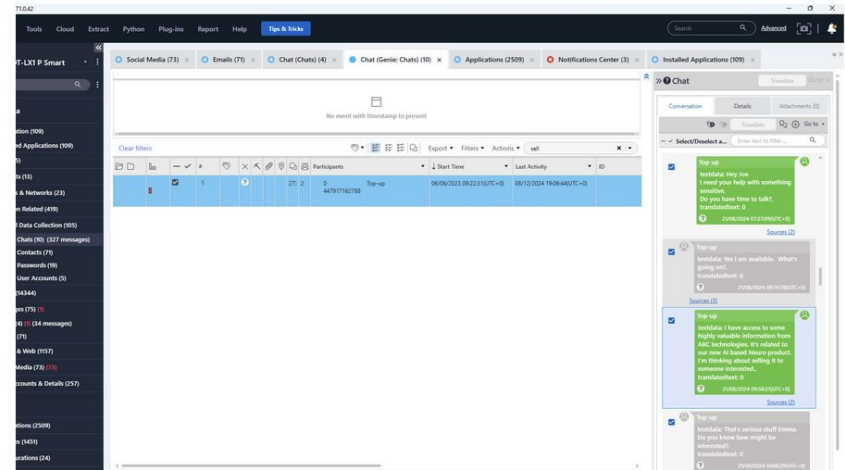
Core Objective

To determine, through digital evidence, the validity of the allegations and provide a conclusive account of the conspiracy to support legal proceedings.

Huawei Device

The timeline is showed in a form of messages exchanged on August 21st, 2024 with a critical conversation where the sender explicitly reaches out to the receiver by saying "Hey Joe" which validates the identity of the recipient directly in the text.

This conversation escalates to talk about the potential sale of "highly valuable information from ABC technologies" which is related to a "new AI based Neuro product", thus creating a direct link between "Joe" and the alleged corporate espionage activities.

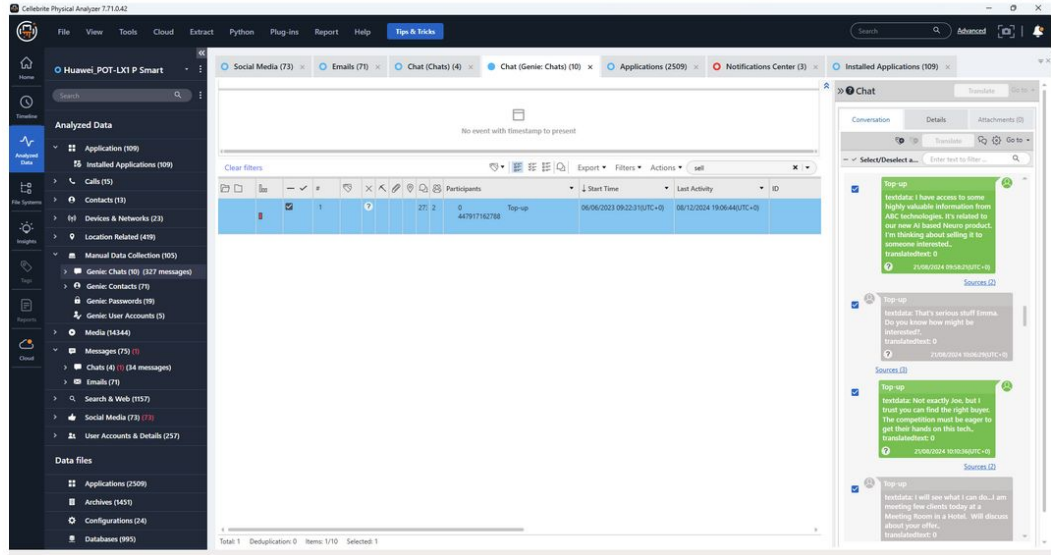


Cont..

Joe clearly explains his operational process to Emma.

In response to Emma's sense of urgency to sell the "highly valuable information from ABC technologies", Joe assures his active involvement, stating: "I will see what I can do." I am meeting few clients today at a Meeting Room in a Hotel. Will discuss about your offer".

This message directly implicates Joe as the facilitator who is setting up physical meetings with potential buyers



Cont..

on August 21, 2024, which is a clear demonstration of the conspiratorial intention

This exchanging is explicit messages showing mutual understanding of the illegality of their doing and mutual agreement to camouflage their operations.

The conversation ends with a Google Maps sharing location of their location 11:17:13 on August 22 and further operationalizes their coordination.

The screenshot displays the Cellebrite Physical Analyzer 7.7.10.42 interface. The left sidebar shows a tree view of analyzed data for a device named 'Huwel_POT-LX1 P Smart'. The main pane shows a table of analyzed data items, including a chat conversation with a contact named 'Peter Dover'.

Item	Start Time	Last Activity	ID
Participants	05/11/2024 10:00:28(UTC+0)	05/11/2024 10:00:32(UTC+0)	
1	13/10/2024 15:45:20(UTC+0)	28/10/2024 15:08:31(UTC+0)	
2	26/08/2024 02:46:03(UTC+0)	26/08/2024 02:46:03(UTC+0)	
3	17/08/2024 02:35:34(UTC+0)	17/08/2024 03:35:28(UTC+0)	
4	17/08/2024 02:27:45(UTC+0)	17/08/2024 02:27:45(UTC+0)	
5	13/08/2024 11:56:20(UTC+0)	21/08/2024 04:46:05(UTC+0)	2d2bcbf485a-5
6	13/08/2024 11:53:31(UTC+0)	13/08/2024 11:54:14(UTC+0)	
7	02/08/2024 20:37:51(UTC+0)	19/08/2024 10:50:15(UTC+0)	
8	02/08/2024 20:36:38(UTC+0)	05/12/2024 00:46:22(UTC+0)	
9	06/06/2023 09:22:31(UTC+0)	06/12/2024 19:06:44(UTC+0)	
10			

The chat conversation shows a message from 'Peter Dover' with the text: 'Perfect. Let's keep this under wraps. This could be huge for both of us.' The message is timestamped 25/08/2024 11:47:11(UTC+0).

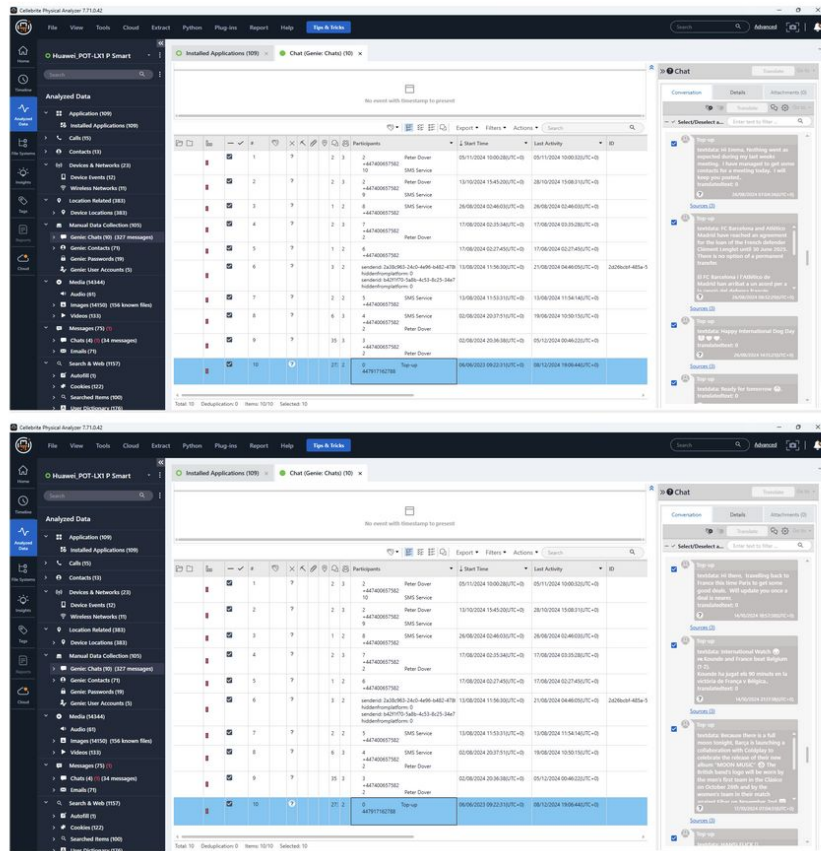
Cont..

The examination shows an important communication of Joe on August 26, 2024. In this message Joe reports a setback in his operations saying, "Hi Emma, Nothing went as expected during my last weeks meeting."

I have been able to secure some contacts to meet today. I will keep you posted." . This text is important in that it vindicates Joe's dogged efforts to broker a deal in the face of initial failure and is a direct example of the ongoing and iterative nature of the conspiracy.

Another forensic extraction takes a critical communication from Joe by October 14, 2024.

In this message, Joe informs Emma on his operational movements to say, "Hi there, travelling back to France this time Paris to get some good deals. Will update you when deal is closer." .



The forensic analysis shows another important communication from Joe on August 29 2024.

For example, "I am flying to Glasgow to meet someone I have in contact with over there for a meeting." Will keep you posted." . This text is irrefutable corroboration for the physical evidence found on Joe's own device - namely the Glasgow train tickets and collection receipts for the same date (August 29) .

The screenshot displays the Cisco Prime Assurance interface. On the left is a navigation sidebar with icons for various functions. The main content area is divided into two panes. The left pane, titled 'Installed Applications (10)', contains a table with columns for Application, Status, Version, and a 'Participate' button. The right pane, titled 'Chat (Cisco Chat)', shows a chat window with a 'Conversation' tab and a 'Details' tab. The chat window displays a list of messages, including a welcome message and a message about the chat service.

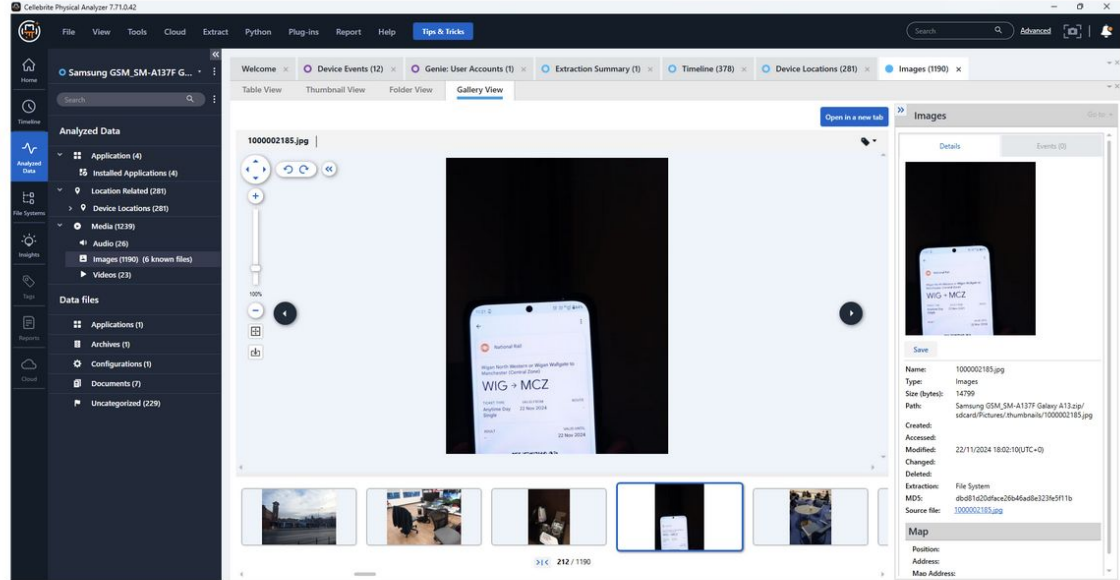
Application	Status	Version	Participate
101 Device & Networks (21)	1	1	2
102 Device Events (1)	1	1	2
103 Wireless Networks (7)	1	1	2
104 Location Related (36)	1	1	2
105 Device Locations (36)	1	1	2
106 Manual Data Collection (26)	1	1	2
107 Cisco Chat (1)	1	1	2
108 Cisco Chat (1)	1	1	2
109 Cisco Chat (1)	1	1	2
110 Cisco Chat (1)	1	1	2
111 Cisco Chat (1)	1	1	2
112 Cisco Chat (1)	1	1	2
113 Cisco Chat (1)	1	1	2
114 Cisco Chat (1)	1	1	2
115 Cisco Chat (1)	1	1	2
116 Cisco Chat (1)	1	1	2
117 Cisco Chat (1)	1	1	2
118 Cisco Chat (1)	1	1	2
119 Cisco Chat (1)	1	1	2
120 Cisco Chat (1)	1	1	2
121 Cisco Chat (1)	1	1	2
122 Cisco Chat (1)	1	1	2
123 Cisco Chat (1)	1	1	2
124 Cisco Chat (1)	1	1	2
125 Cisco Chat (1)	1	1	2
126 Cisco Chat (1)	1	1	2
127 Cisco Chat (1)	1	1	2
128 Cisco Chat (1)	1	1	2
129 Cisco Chat (1)	1	1	2
130 Cisco Chat (1)	1	1	2
131 Cisco Chat (1)	1	1	2
132 Cisco Chat (1)	1	1	2
133 Cisco Chat (1)	1	1	2
134 Cisco Chat (1)	1	1	2
135 Cisco Chat (1)	1	1	2
136 Cisco Chat (1)	1	1	2
137 Cisco Chat (1)	1	1	2
138 Cisco Chat (1)	1	1	2
139 Cisco Chat (1)	1	1	2
140 Cisco Chat (1)	1	1	2
141 Cisco Chat (1)	1	1	2
142 Cisco Chat (1)	1	1	2
143 Cisco Chat (1)	1	1	2
144 Cisco Chat (1)	1	1	2
145 Cisco Chat (1)	1	1	2
146 Cisco Chat (1)	1	1	2
147 Cisco Chat (1)	1	1	2
148 Cisco Chat (1)	1	1	2
149 Cisco Chat (1)	1	1	2
150 Cisco Chat (1)	1	1	2
151 Cisco Chat (1)	1	1	2
152 Cisco Chat (1)	1	1	2
153 Cisco Chat (1)	1	1	2
154 Cisco Chat (1)	1	1	2
155 Cisco Chat (1)	1	1	2
156 Cisco Chat (1)	1	1	2
157 Cisco Chat (1)	1	1	2
158 Cisco Chat (1)	1	1	2
159 Cisco Chat (1)	1	1	2
160 Cisco Chat (1)	1	1	2
161 Cisco Chat (1)	1	1	2
162 Cisco Chat (1)	1	1	2
163 Cisco Chat (1)	1	1	2
164 Cisco Chat (1)	1	1	2
165 Cisco Chat (1)	1	1	2
166 Cisco Chat (1)	1	1	2
167 Cisco Chat (1)	1	1	2
168 Cisco Chat (1)	1	1	2
169 Cisco Chat (1)	1	1	2
170 Cisco Chat (1)	1	1	2
171 Cisco Chat (1)	1	1	2
172 Cisco Chat (1)	1	1	2
173 Cisco Chat (1)	1	1	2
174 Cisco Chat (1)	1	1	2
175 Cisco Chat (1)	1	1	2
176 Cisco Chat (1)	1	1	2
177 Cisco Chat (1)	1	1	2
178 Cisco Chat (1)	1	1	2
179 Cisco Chat (1)	1	1	2
180 Cisco Chat (1)	1	1	2
181 Cisco Chat (1)	1	1	2
182 Cisco Chat (1)	1	1	2
183 Cisco Chat (1)	1	1	2
184 Cisco Chat (1)	1	1	2
185 Cisco Chat (1)	1	1	2
186 Cisco Chat (1)	1	1	2
187 Cisco Chat (1)	1	1	2
188 Cisco Chat (1)	1	1	2
189 Cisco Chat (1)	1	1	2
190 Cisco Chat (1)	1	1	2
191 Cisco Chat (1)	1	1	2
192 Cisco Chat (1)	1	1	2
193 Cisco Chat (1)	1	1	2
194 Cisco Chat (1)	1	1	2
195 Cisco Chat (1)	1	1	2

Samsung Device

The following screenshot from the forensic analysis performed on Joe's Samsung device shows an important digital artifact found in the thumbnail cache on the device.

This image is of a digital ticket from the National Rail app which shows the journey from Wigan North Western (WIG) or Wigan Wallgate to Manchester (Central Zone) (MCZ).

The ticket is valid from November 22, 2024, which conveniently coincides with the timeline of Joe's communications of "meeting the client this week at Manchester".

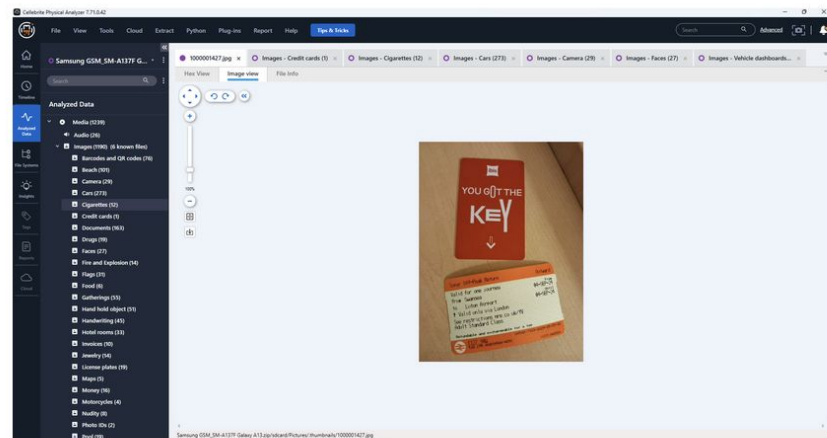
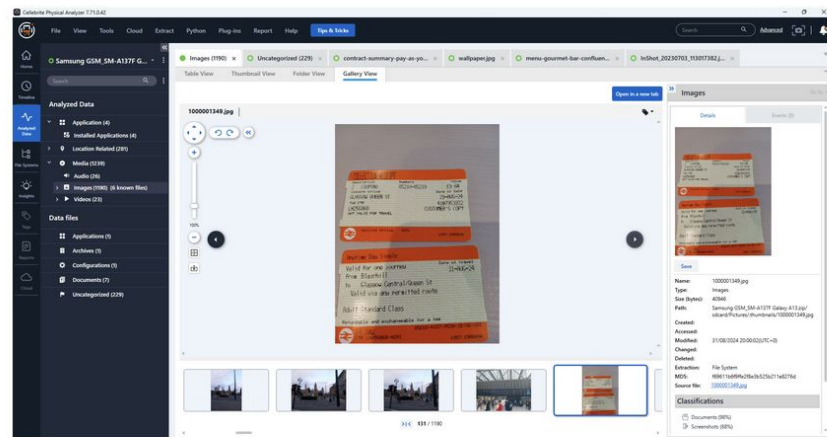


Cont..

The screenshot shows a forensic examination of Joe's Samsung device which captures physical train tickets and a collection receipt.

The upper part of the picture is the "Collection receipt" from Glasgow Queen St station, from August 29 2024. Below is an "Anytime Day Single" ticket which will be valid for travel on the August 31st 2024 from Blairhill to Glasgow Central/Queen St.

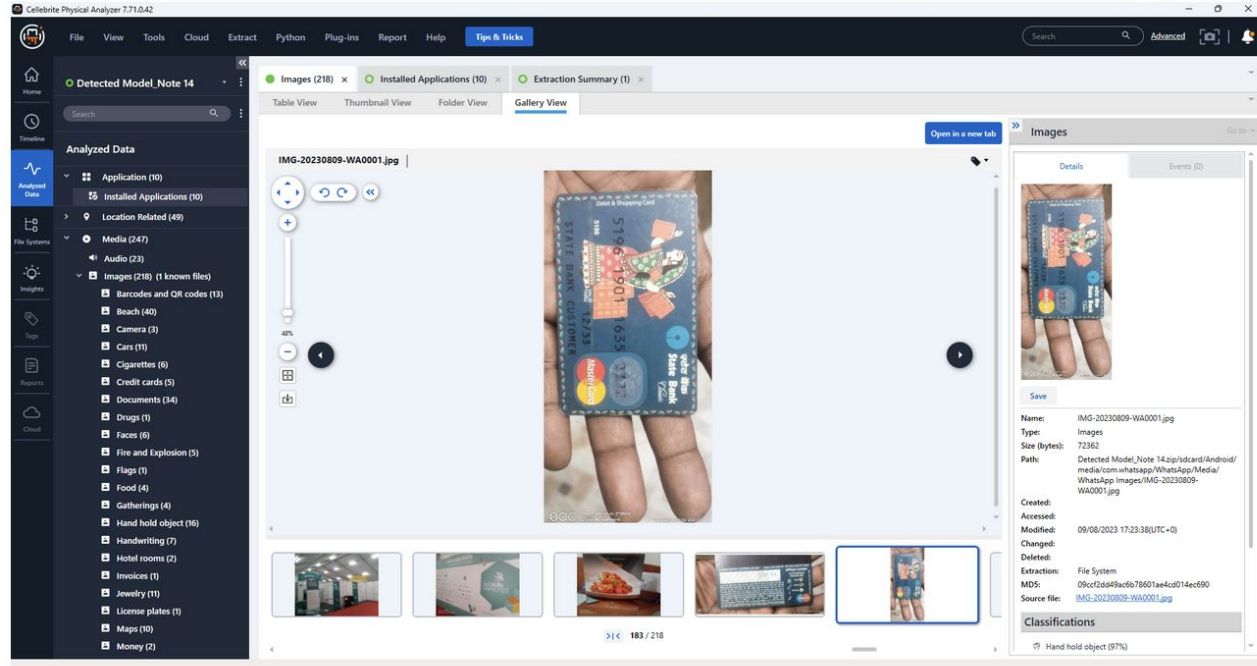
This evidence locates Joe in the Glasgow area in late August 2024, which is a verifiable physical timeline which can be cross-referenced with his digital communications and other location data to be further mapped out for his movements during the conspiracy period.

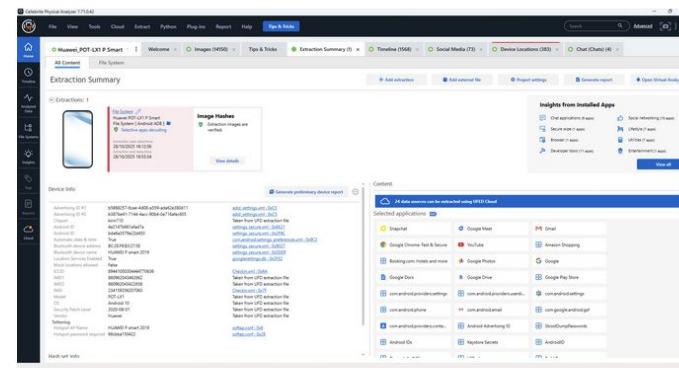
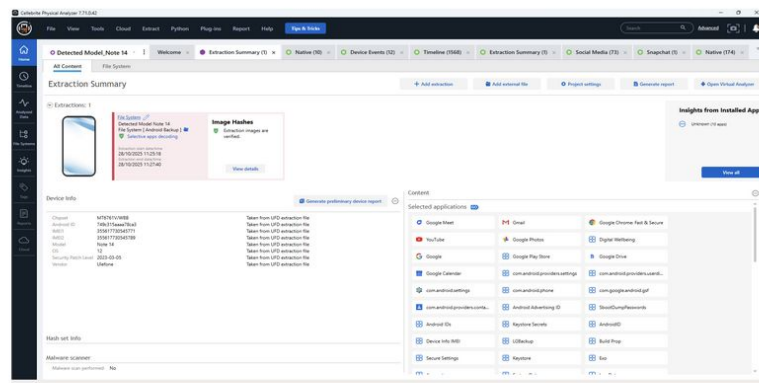
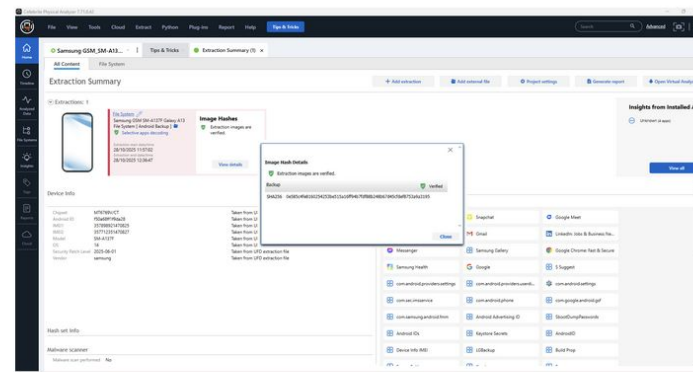


The Ulefone Device

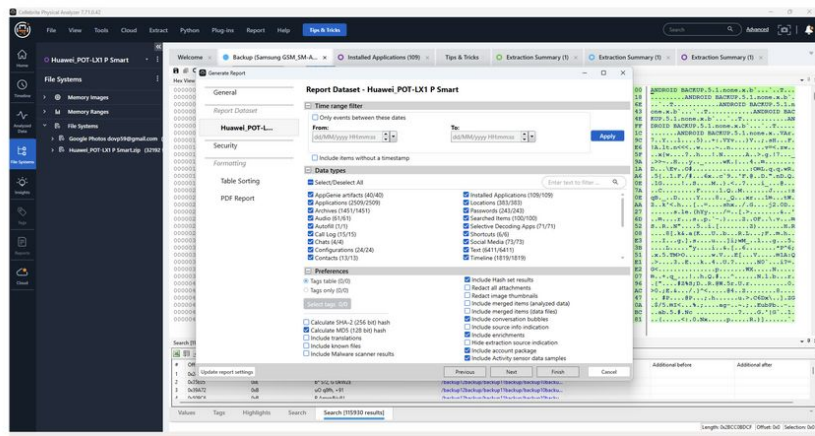
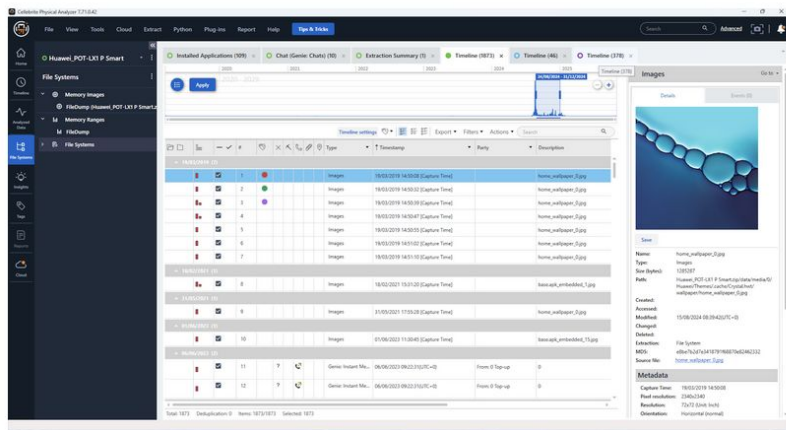
The Indian debit card found on the Ulefone device has the branding of Maestro and a partial account number.

The metadata of the card gives the date of its creation as August 9th, 2023, exactly a year before the actual date of Emma's active espionage communications in August 2024.





Evidence tagging & Report generation



Conclusion

The investigation (via three devices) conclusively identifies:

- Perpetrator: Emma (UK, Huawei device). Stole trade secrets and launched the conspiracy.
- Facilitator: Joe (UK, Samsung device). Middleman finding buyers and managing offshore logistics/finance.
- Unclear Role: Norman (India, Ulefone device). Involved in the network; role (past operative, coordinator, or financial link).