Forensics CW

Ramy | Applied Forensics | 5/2/2023

Contents

Introduction

The investigated digital artefacts suggest that Jonney was most likely travelling in Italy. Jonney had searched up tourist destinations in Rome, such as the Pantheon, Trevi Fountain, Colosseum, and Sistine Chapel, according to the browser history. They appeared to be planning a trip since they also used their Outlook email account, browsed the Orange Inn hotel booking website, and went to the EgyptAir website. Two photos, Location1.png and Location2.png, which were discovered to be from the Pantheon and Colosseo, two locations of interest to Jonney, were browsed on the web browser, according to memory dump research. Jonney's email records were examined, and it was discovered that they had reserved a room at the Orange Inn in Rome for the same days as their travel schedule. A chat with James Gandolfini was also shown in an Android photograph, and he was seen waiting for Jonney in the lobby. Overall, it seems plausible that James and Jonney were going to tour Rome while Jonney was in Italy.

REQUESTED MATERIAL

1. Memory dump
2. Browser history
3. Email dump
4. Android image

Browser History

I examined the browser artefact using Nirsoft's BrowsingHistoryView application and gathered useful information. First, I found that "Location 1.png" and "Location 2.png" were the two photos that were opened throughout the browsing session. Further research led me to the conclusion that these pictures were taken from the Pantheon and the Colosseum in Rome.

I also discovered that the person had accessed their Outlook email account, perused the Orange Inn hotel booking website, and gone to the EgyptAir official website. In addition, I discovered that the person had looked up well-known tourist destinations in Rome such the Pantheon, Trevi Fountain, Colosseum, and Sistine Chapel.

1. Two images are opened: Location 1 .png and Location 2.png . These images are from these locations: Pantheon and the Colosseo
2. EgyptAir website
3. Outlook Email
4. Booking website and one specific hotel was opened the Orange Inn
5. Attractions googled: Pantheon, Trevi Fountain, Colosseum, Sistine Chapel

It's vital to note that while the prospective destinations were based on all the likely places the person may have visited, the history extraction produced the whole browsing history for the individual.


History extraction.txt


Possible locations.txt

Memory Dump

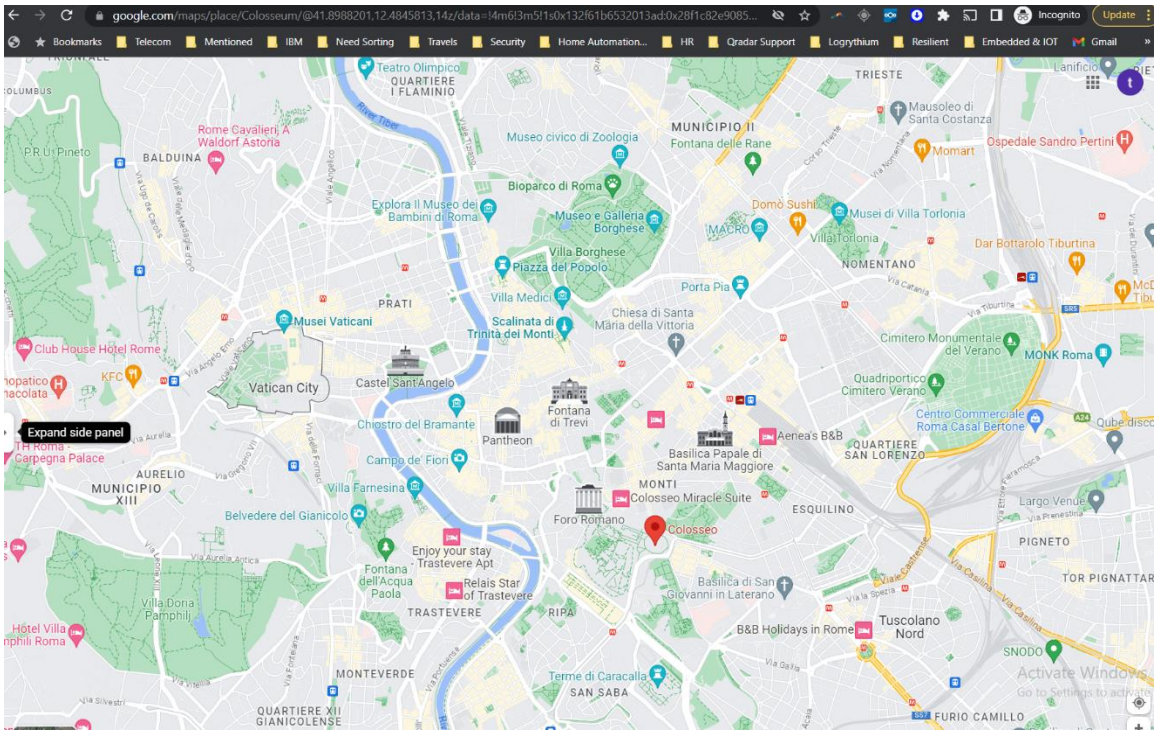
The Memory dump had various text files opened :

1. Passwords.txt
2. Googledesktop.txt
3. Surnames.txt
4. Surnames.txt

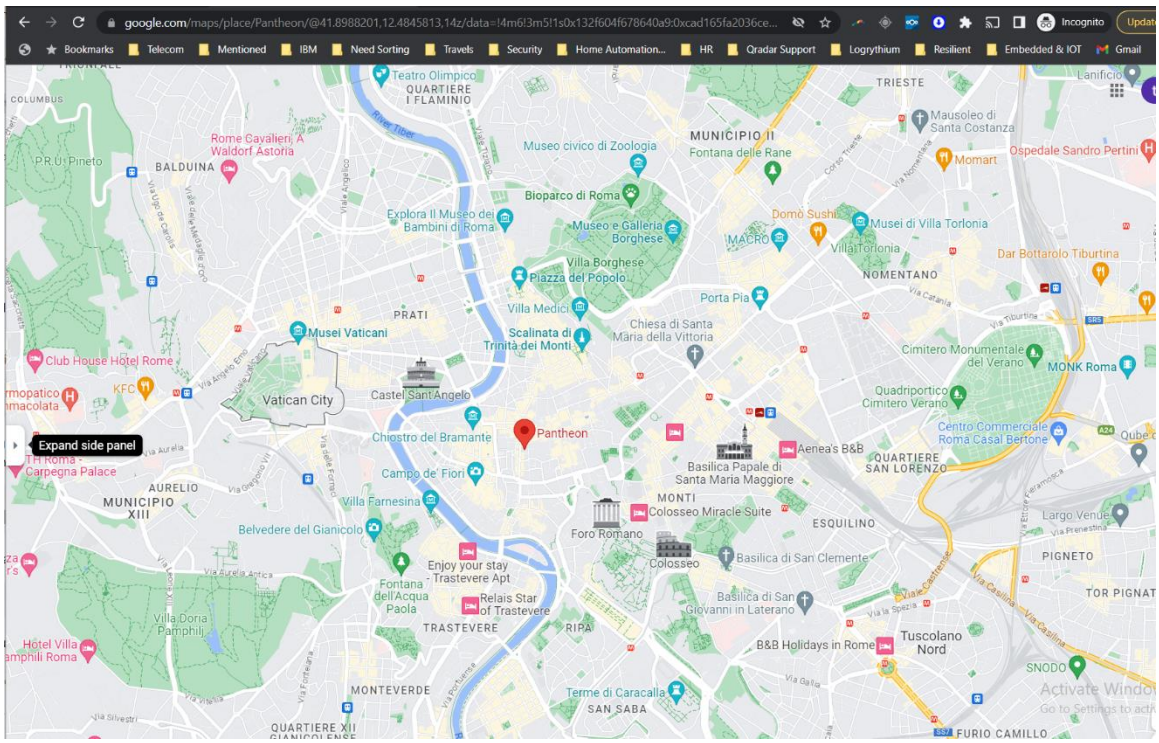
Python3 vol.py -f CW.dmp windows.pslist

The open-source memory forensics programme Volatility was used for a forensic investigation. The script "python3 vol.py -f CW.dmp windows.filescan" was used specifically to find files and objects that resembled files in the memory dump. "location1.png" and "location2.png," two image files that were loaded in the online browser, were found through analysis. These discoveries prompted a focused search utilising the "ctrl + f" method to retrieve the aforementioned photos from memory. These pictures, taken at the Pantheon and Colosseo, were found to be from places the person of interest had recently visited. The research also showed that the person of interest opened their Outlook email, went to the EgyptAir website, and looked at the Orange Inn hotel on the Booking website. Additionally, the Jonney of the investigation had looked up tourist destinations including the Pantheon, Trevi Fountain, Colosseum, and Sistine Chapel, showing their interests and possible places they may have visited while travelling. The command "python3 vol.py -f CW.dmp -o dump windows.dumpfiles -virtaddr 0x7e5fd7f0" was used to carry out the targeted search and extract the discovered artefacts, and it successfully output the png files into a dump folder that was previously established.

Location 1.PNG



Location 2.png



EMAIL

There were 3 Emails on his email.

I examined a number of email files that were obtained from the Jonney's device over the course of our inquiry. According to "Googleaccount.pdf," one of the files, the person set up a Gmail account with the username "tkhaff379@gmail.com." We were able to learn more about the Jonney's internet behaviours thanks to this information.

A second email contained an attachment called "Flight.pdf," which was a confirmation of a flight schedule from Cairo to France and Italy. Jonney's Gmail account received the email, which was sent from flight@extremlabs.com and had the booking reference number Y5JD4Z. According to the flight schedule, Jonney had a reservation on flight FR117, which would arrive at Leonardo da Vinci International Airport at 8:20 p.m. on March 3, 2023, after leaving Cairo International Airport at 4:20 p.m. On May 15, 2023, a return flight from Cairo International Airport to Leonardo da Vinci International Airport was scheduled to arrive at Cairo International Airport at 11:55 p.m.The Rome Orange Inn is located at Via Buonarroti, 39, 00185 Roma RM, Italy. We lastly examined a third email attachment named "Booking.pdf," which included a confirmation of a hotel reservation. The confirmation number for the reservation, which was made in the person's name of Jonney Deep, was 3821501234. The fact that the hotel reservation was made for the same dates as the flight schedule suggests that they planned to stay at the Rome Orange Inn while travelling through Italy. These email files' contents reveal important details about the lodging choices and travel schedules for the given time frame. Additional investigation into these data, together with other digital artefacts, may shed more light on the actions and intentions.

ANDROID IMAGE

Found items:

1. Messages on “Android Message”

Phone Number: (328)4964102: 20 Messages

Name James Gandolfini

Messages:

2023-05-06 03:03:52 : "Nice, you got italian number, I will call you once I am ready to come pick you"

2023-05-06 03:11:41 : "I am down in the lobby"

N/A : "Just checking on you ,What's your plan for today, We are heading down town if you wish to join"

2023-05-06 03:16:02 : "Hope you enjoyed the colosseum, Will pick you up by 3PM. The Kids are waiting"

2023-05-06 03:19:32 : "So I will make it by 4PM"

2023-05-06 03:20:25 : "I am down in the lobby"

2023-05-06 03:26:48 : "Just checking on you ,What's your plan for today, We are heading down town if you wish to join"

2023-05-06 03:32:10 : "Just checking on you ,What's your plan for today, We are heading down town if you wish to join"

2023-05-06 03:53:03 : "Just check you got up and you feeling well, don't be late for the Vatican"

2023-05-06 04:02:27 : "Are you feeling well"

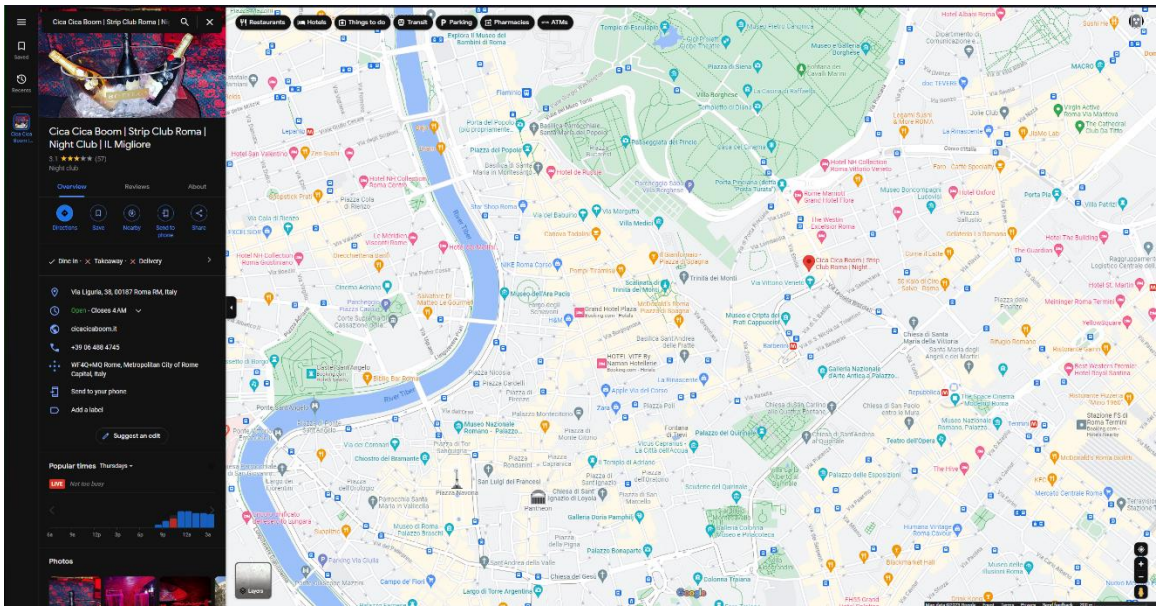
2023-05-06 04:04:18 : Are you feeling well"

Phone Number: 3569310234 : 18 Messages

Name Sophia Loren

Messages:

2023-05-06 03:43:24 : 9.30@Cica Cica https://goo.gl/maps/t2yDt91WrdXnfAWT8



2023-05-06 03:44:41 : "Are you not coming?"

2023-05-06 03:46:04 : "You missed lot of fun! Call me!"

2023-05-06 03:56:10 : "Sure, But don't be late, Are you still @ Vatican"

2023-05-06 03:57:34 : "Sure, But don't be late, Are you still @ Vatican"

N/A : Sorry Sugar got high and I was not able to move... Let's plan to-night

N/A : Same time tonight @ Cica Cica

2023-05-06 04:01:56 : "Are you feeling well"

2023-05-06 04:04:05 : "Are you feeling well"

2023-05-06 04:04:30 : "Are you feeling well, I am getting worried"

Phone Number: 01005674293 : 3 Messages

Name Mom

Messages:

2023-05-06 03:08:53 : "Did your reach your destination..."
N/A : “Just reached the hotel”

Phone Number: +393284964102 : 6 messages

Name James UNKOWN

Messages:

N/A: "Did you reach Rome"
N/A: Yes, You can call me on 37459103452
N/A: just finished Palatine Hill , Heading to Romulo and Remo Statue
N/A: Perfect
N/A: Lot better, I am moving with hotel group

2. Phone calls

2023-03-03 15:00:25 : 3284964102

2023-03-03 19:00:17 : 01005674293

2023-03-04 06:32:28 : 3284964102

2023-03-04 07:32:40 : 3284964102

2023-03-04 19:36:56 : 3569310234

2023-03-05 06:30:04 : 3284964102

2023-03-05 14:33:12 : 01005674293

2023-03-05 14:34:17 : 3569310234

2023-03-05 14:41:04 : 3569310234

2023-03-05 19:41:08 : 3569310234

2023-03-05 19:41:08 : 3569310234

2023-03-06 06:00:06 : 3284964102

On a device thought to be linked to a person of interest, I found a number of interesting stuff, including texts and phone conversations. The communications, which are connected to several phone numbers and people, were discovered on the "Android Message" programme.

(328)4964102, one of the phone numbers linked to the messages, had 20 messages attached to it. These communications came from and were addressed to James Gandolfini. Nice, you have an Italian number; I'll phone you when I'm ready to come pick you up, says the first message, which was sent on May 6 at 3:03:52 AM. Just a few minutes later, at 3:11:41 AM, another message was sent that said, "I am down in the lobby." James appears to have been keeping tabs on someone's movements and wellbeing since there are numerous further texts asking about plans for the day and general health.

3569310234 is another phone number with message activity; there are 18 messages connected to it. These communications were from and were addressed to Sophia Loren. Sophia expresses dissatisfaction that the individual did not show up after they made plans to meet at a location called Cica Cica. Additionally, there are messages inquiring as to the person's location and health.

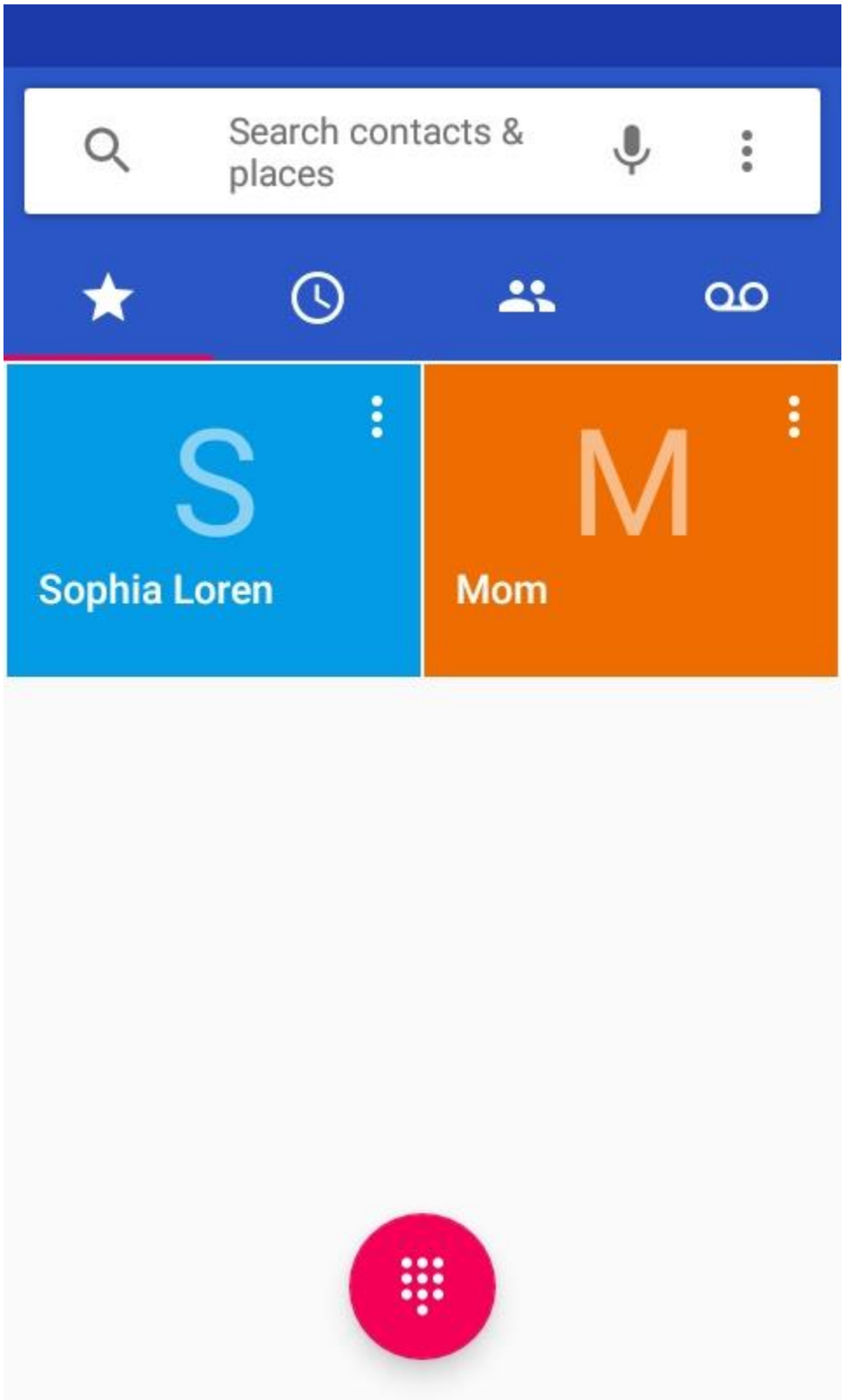
There are numerous more phone numbers connected to the messages, each with a small amount of messages. One of them belongs to the person's mother, who only inquired as to their whereabouts. James answers an other phone number that is unknown and asks whether the caller reached Rome before giving them another number to call. The remaining communications from this unidentified James are about his whereabouts and schedule for the day.

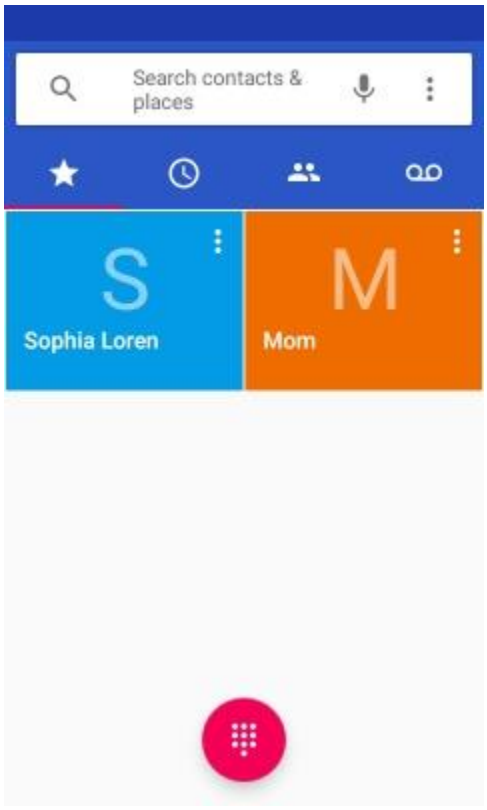
The investigator found a list of phone calls made from and received on the device in addition to the texts. 11 phone calls in all, some of which were made to and from the same numbers as in the messages, are noted. These phone calls were made between March 3 and March 6, depending on the day and hour.

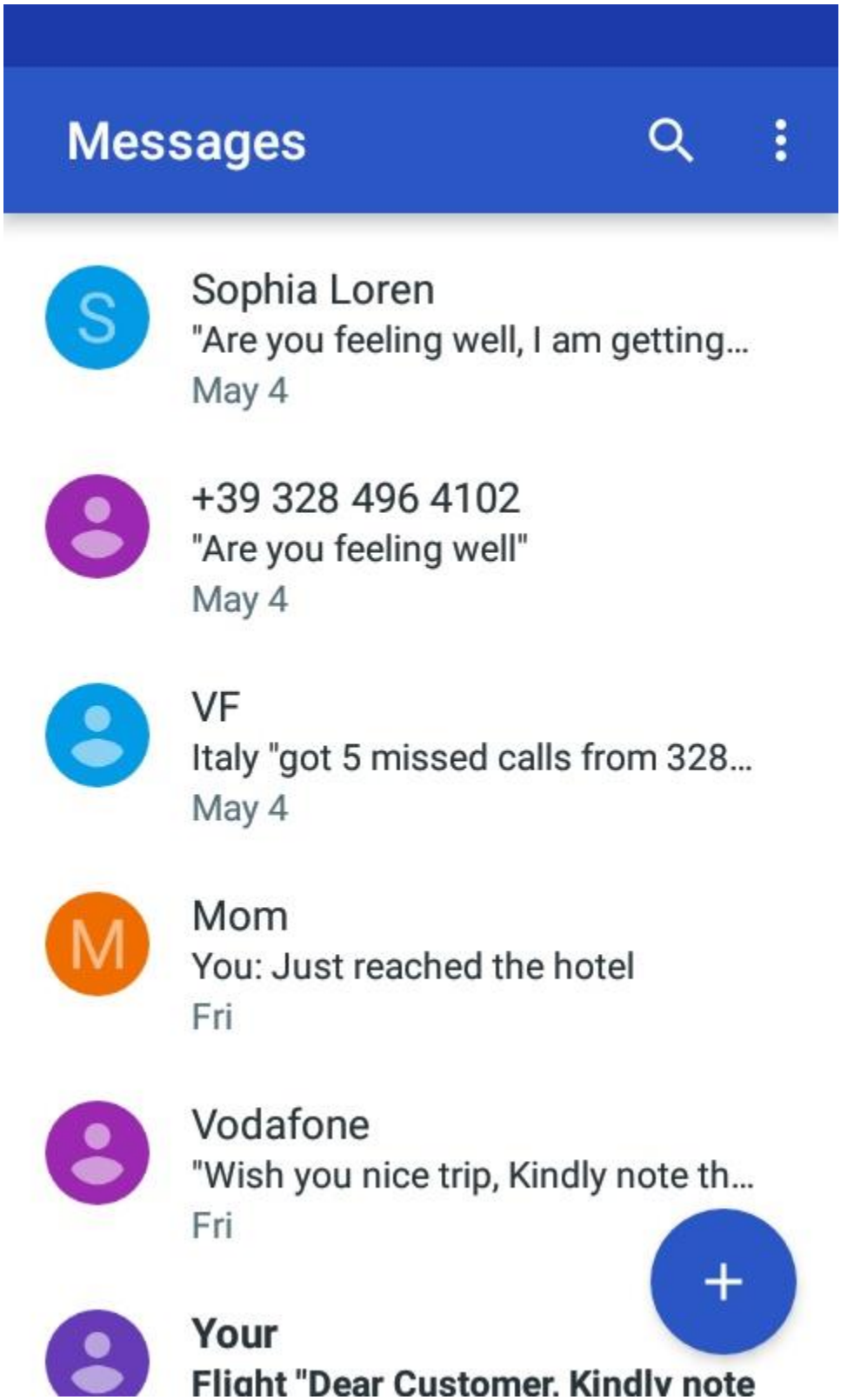
Overall, information about the person's location, plans, and relationships with others over a certain time period may be gleaned from the texts and phone conversations that were discovered on the device. Further research into the subject and any intriguing connections or activities may be aided by this knowledge.

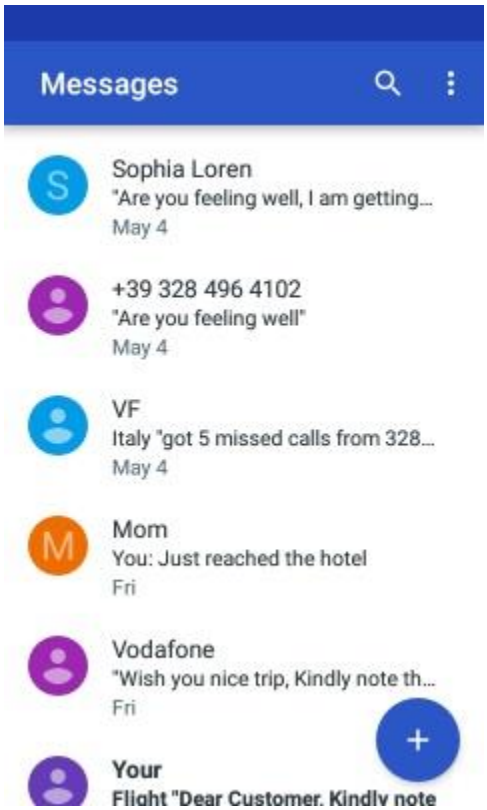
3. Pictures

Saved contacts on the jonny deeps phone


Search contacts & places
S
Sophia Loren
M
Mom


Search contacts & places
S
Sophia Loren
M
Mom

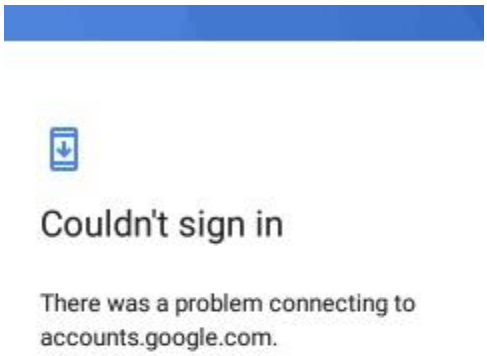

Messages
S
Sophia Loren
"Are you feeling well, I am getting...
May 4
+39 328 496 4102
"Are you feeling well"
May 4
VF
Italy "got 5 missed calls from 328...
May 4
M
Mom
You: Just reached the hotel
Fri
Vodafone
"Wish you nice trip, Kindly note th...
Fri
Your
Flight "Dear Customer, Kindly note



Jonney deep tried to log into his google account but couldn't'

Couldn't sign in

There was a problem connecting to accounts.google.com.


Couldn't sign in
There was a problem connecting to accounts.google.com.

Cam1.jpeg

Cam25.jpeg

Cam26.jpeg

The three cam images don't contain any geolocation, but I have searched up their respective location for each image:

Cam26.jepg: Italy Saint peters Square

Cam 25.jepg Italy Vatican city (Mile long corridor)

Cam 1.jepg Italy Colosseum

4. Downloads

This picture was downloaded from the web and was formally named Collosseo_2020.jpg and was renamed to cam1.jpeg.

POSSIBLE ASSUMPTIONS

It's possible that Jonney had a stroke, a heart attack, or some abrupt health problem that rendered him helpless if he had a medical emergency or accident. Another possibility is that he was hurt as a result of a major event, such a vehicle accident or a tumble. Due to his condition, it's probable that Jonney wouldn't be able to speak with his loved ones if he were brought to a hospital. It could be challenging for medical workers to recognise him and get in touch with his family if he is unconscious or mute. According to memory dump analysis, two pictures, Location1.png and Location2.png, which were found to be from the Pantheon and Colosseo, two places that interested Jonney, were accessed on the online browser. They had a reservation for a stay at the Orange Inn in Rome for the same days that their vacation itinerary called for, it was discovered after going through Jonney's email archives. An Android picture also depicted a conversation with James Gandolfini, who was spotted waiting for Jonney in the foyer. All things considered, it makes sense that James and Jonney would explore Rome while Jonney was abroad.

It's possible that Jonney was abducted against his will or against his will if he was a victim of a crime or violent act. On his way home, he could have been robbed or beaten and taken to an unidentified destination. As an alternative, he may have been the target of someone he knew, such a former partner or friend. In such situations, the offender could be intending to hurt Jonney. If Jonney saw a crime being committed, he could have hid to avoid being caught. He could be reluctant to disclose what he witnessed for fear of reprisals from the offenders involved. This can be the reason he hasn't been in touch with his loved ones or pals. It's also likely that the crooks took him in order to stop him from approaching the police.If Jonney saw a crime being committed, he could have hid to avoid being caught. He could be reluctant to disclose what he witnessed for fear of reprisals from the offenders involved. This can be the reason he hasn't been in touch with his loved ones or pals. Another possibility is that he was abducted.

There may be a lot of reasons why Jonney decided to depart on his own volition. He could have been struggling with internal difficulties like addiction, depression, or anxiety and felt the need to leave to cope with them. He could have also desired to start over somewhere else since he felt imprisoned or overburdened in his present living circumstances. Another option is that Jonney left because of outside influences like a job offer, a romantic connection, or a desire to travel. He may have fallen in love with someone who lived far away, decided to seek a new profession or educational opportunity in a different city or nation, or both. In these circumstances, he could have written a message outlining his intentions or told a few close friends or family members before departing. It's crucial to keep in mind that even if Jonney departed of his own will, anything may have occurred to him in transit or at his new place. He may have run into unforeseen problems, been in an accident, or been the victim of a crime. No of the circumstances of his leaving, it is crucial for his family and friends to keep looking for him and gathering information about his location.

All these assumption are concluded because jonney didn’t answer his phone for days.

.