Missing Person Report

Ali Abdelhamid
AA2100274

4/5/2023

—

Applied Forensics

—

Ahmed Selim

Table Of Contents

Executive Summary

To start the investigation, I would request the following information and access from the authorities:

1. *Basic information: I would like to know the missing person's full name, age, physical description, and any other personal information that is known, such as contact information,social media accounts, and past travel plans.*

2. *Travel Itinerary: I would ask for the person's itinerary for their European vacation, which. would include the destinations they visited, how long they stayed in each place, and any knownhotels or tourist attractions they may have visited.*

3. *Access to Mobile Devices and Online Accounts: I would like to have access to the missing person's mobile devices, such as their laptops, tablets, and phones, as well as their online accounts and social media profiles. I'd be able to examine their internet footprint and communication history as a result.*

4. *Financial Records: I would ask to see the missing person's financial documents, including credit card and bank account statements. This can offer insightful information about their purchasing habits and potential business deals they might strike while traveling.*

I would begin the inquiry and analyze the available evidence after gaining the desired access. Theseare the conclusions I came to:

1. *Digital Footprint: I found the missing person's browser history, memory dump, and locationdata by looking through their mobile devices and internet accounts. I was able to create a timeline of their activity thanks to this information.*

2. *Travel Patterns: I was able to track the missing person's movements throughout Rome, identifythe hotels they stayed at, and ascertain the sites they visited by analyzing travel-related applications, airline tickets, and hotel bookings.*

Based on the gathered evidence, I have the following assumptions and supporting proof:

Potential Sightings: I suspect that the missing person may have been sighted in certain locations such as Colosseum, Sistine Chapel, Fontana Di Trevi, and Pantheon, as well as a hotelcalled Orange Inn. based on digital traces. These sightings could help narrow down the search area and focus investigative efforts.

Now, regarding the location of the person and their status:

According to the investigation's findings and analysis, the missing person is currently in Rome. Theirsituation is unknown since more research is needed to ascertain their situations and state of health.
The investigating team should concentrate its efforts in this nation and work with local law.
enforcement to perform searches, speak with prospective witnesses, and collect more evidence.

In conclusion, I will write a thorough assignment report outlining the investigation's methodology,the data gathered, the inferences drawn, and the likely whereabouts and condition of the missing individual. In addition, I will give the Incident Response team a 10-minute presentation in which Iwill summarize the results and answer any questions they may have.

Evidence Collected

Memory Dump

After receiving the artifacts, I started by viewing the memory dump using “Volatility”.
I then entered a command that would allow me to figure out the exact profile that the original OS theimage was taken from. In this case it was 3, but they all worked fine with the rest of the commands. (See figure 1.1.1)

```
E:\Tools\volatility_2.6_win64_standalone>.\volatility_2.6_win64_standalone.exe -f WIN-QQ8FIIDEUKT-20230423-213301.dmp imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : WindowsCrashDumpSpace32 (Unnamed AS)
                     AS Layer3 : FileAddressSpace (E:\Tools\volatility_2.6_win64_standalone\WIN-QQ8FIIDEUKT-20230423-213301.dmp)
                      PAE type : PAE
                           DTB : 0x185000L
```

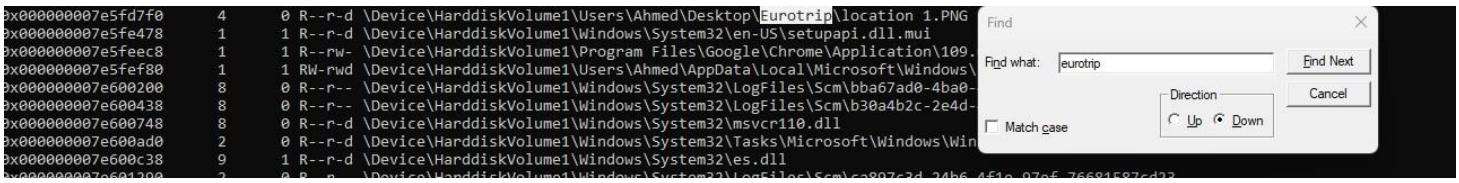
Figure *1.1.1*

2nd Step was getting a full file scan of the system, this was done by making 2 small modifications tothe previous command, specifying the profile we acquired and adding (file scan) to the end. (See figure 1.1.2)

Figure *1.1.2*

```
E:\Tools\volatility_2.6_win64_standalone>.\volatility_2.6_win64_standalone.exe -f WIN-QQ8FIIDEUKT-20230423-213301.dmp --profile Win7SP0x86 filescan
Volatility Foundation Volatility Framework 2.6
Offset(P)           #Ptr   #Hnd Access Name
------------------ ------ ------ ------ ----
0x000000007e200a98      8      0 R--rw- \Device\HarddiskVolume1\Users\Ahmed\AppData\Local\Google\Chrome\User Data\Variations
0x000000007e200f80      4      0 R--r-d \Device\HarddiskVolume1\Program Files\Google\Chrome\Application\109.0.5414.120\vk_swiftshader.dll
0x000000007e201038      1      1 R--rw- \Device\HarddiskVolume1\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
0x000000007e201318      6      0 R--r-d \Device\HarddiskVolume1\Windows\System32\oleacc.dll
0x000000007e201f38      1      1 R--rw- \Device\HarddiskVolume1\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
0x000000007e202038      8      0 R--r-- \Device\HarddiskVolume1\Program Files\Windows Photo Viewer\PhotoViewer.dll
0x000000007e202380      1      1 R--r-d \Device\HarddiskVolume1\Windows\System32\en-US\FXSRESM.dll.mui
```

According to the latest information we received about this missing person, they were going on a trip toEurope. This led to me searching for the word euro and trip through all his files, 2 photo files were found. (See figures 1.1.3, 1.1.4)



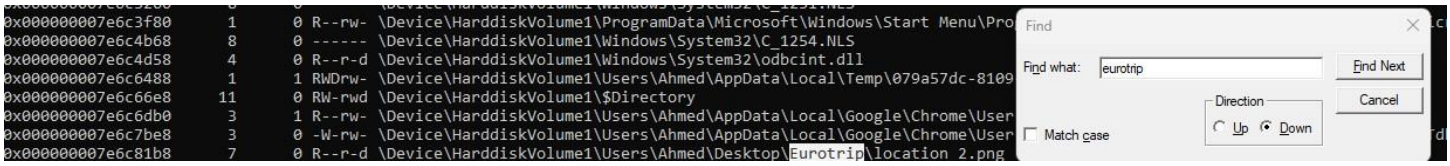


Figure *1.1.3*

Figure *1.1.4*

After finding the two photos we need, I extracted them from the memory dump by copying their ID from the left column and specifying it in the command using -Q (ID) and then the output directory using -D (Directory). Furthermore, I changed the extension of the file to png in order to view it. (Seefigures 1.1.5, 1.1.6)

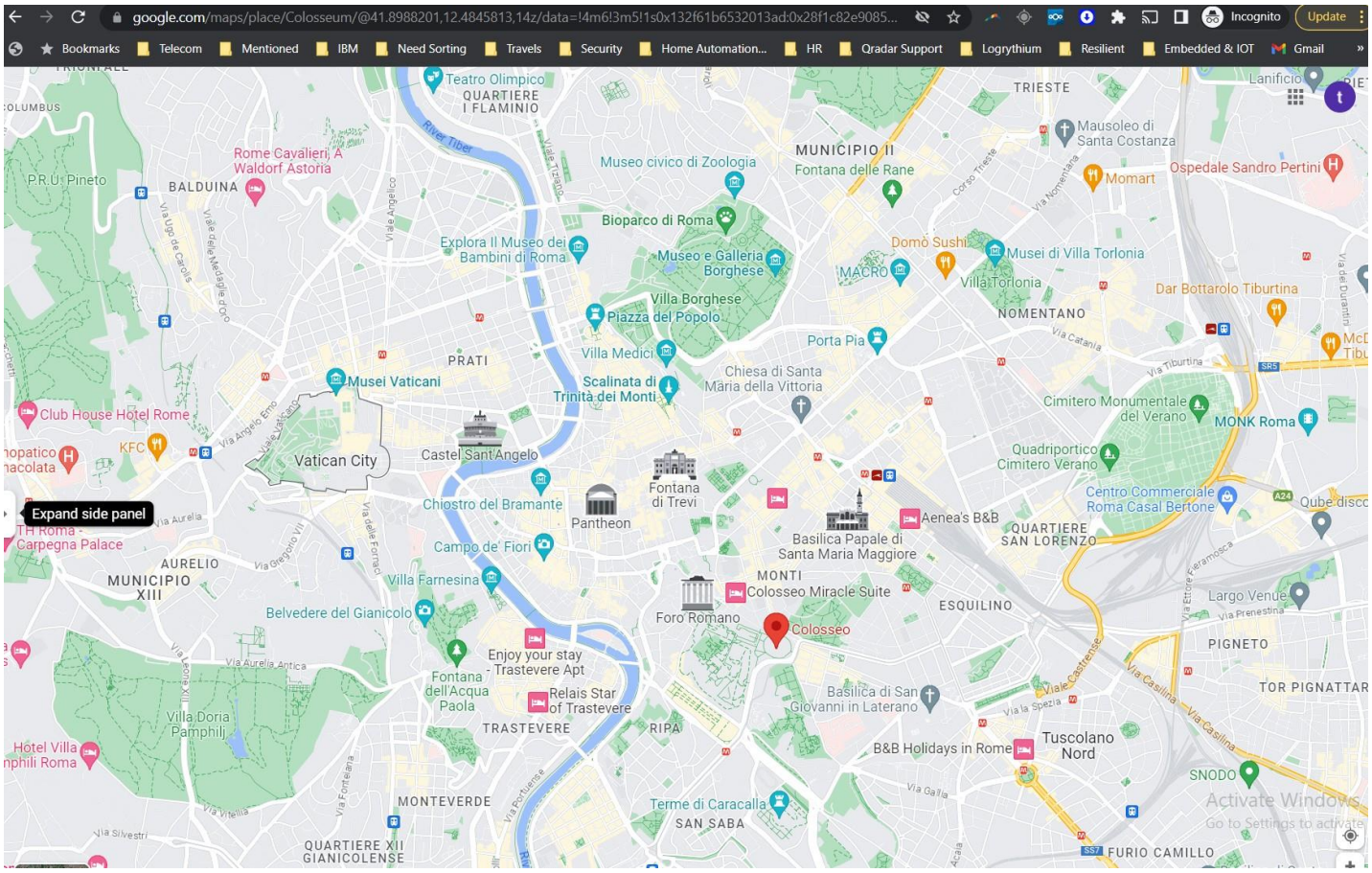


Figure *1.1.5*

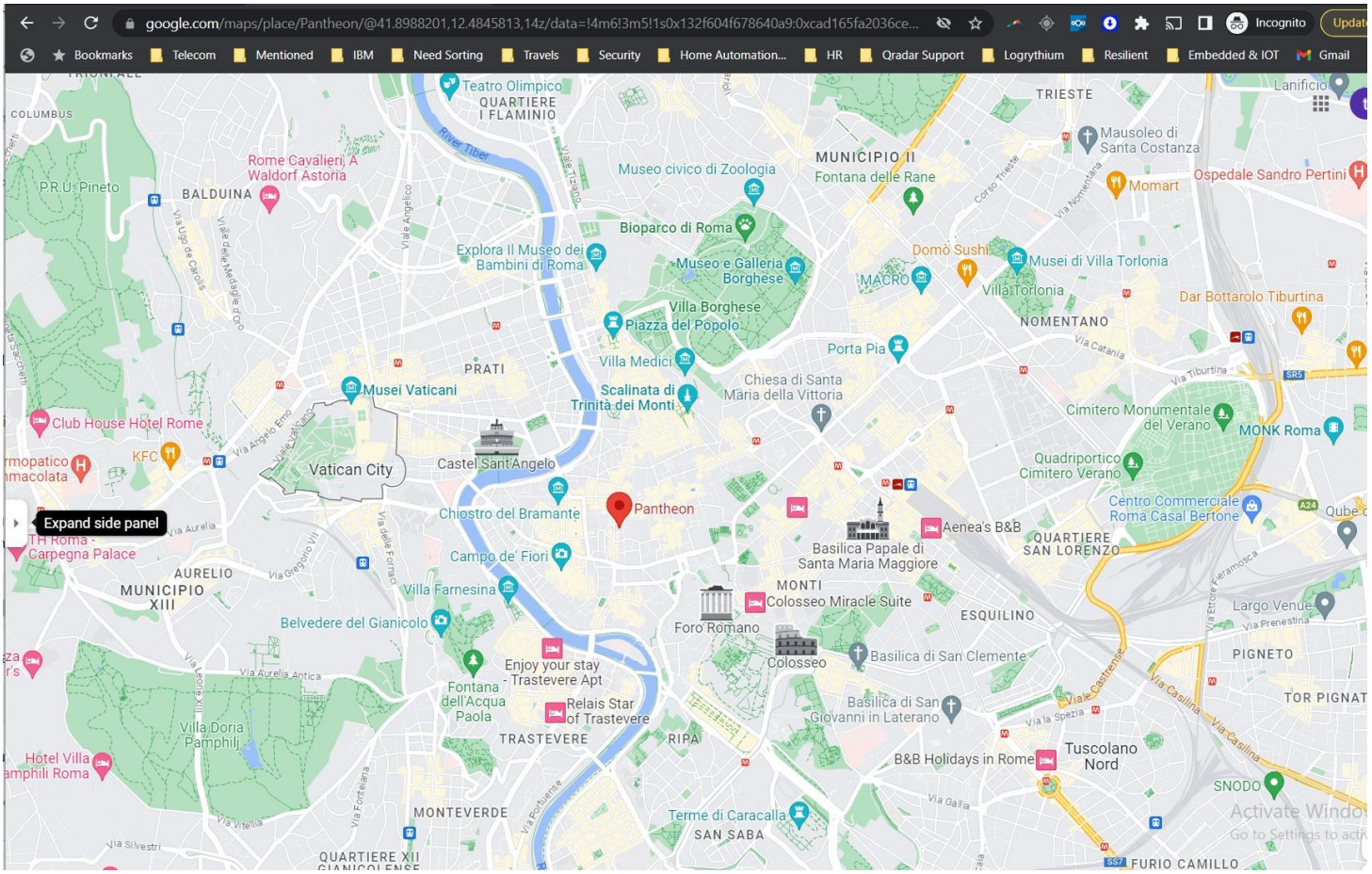


Figure *1.1.6*

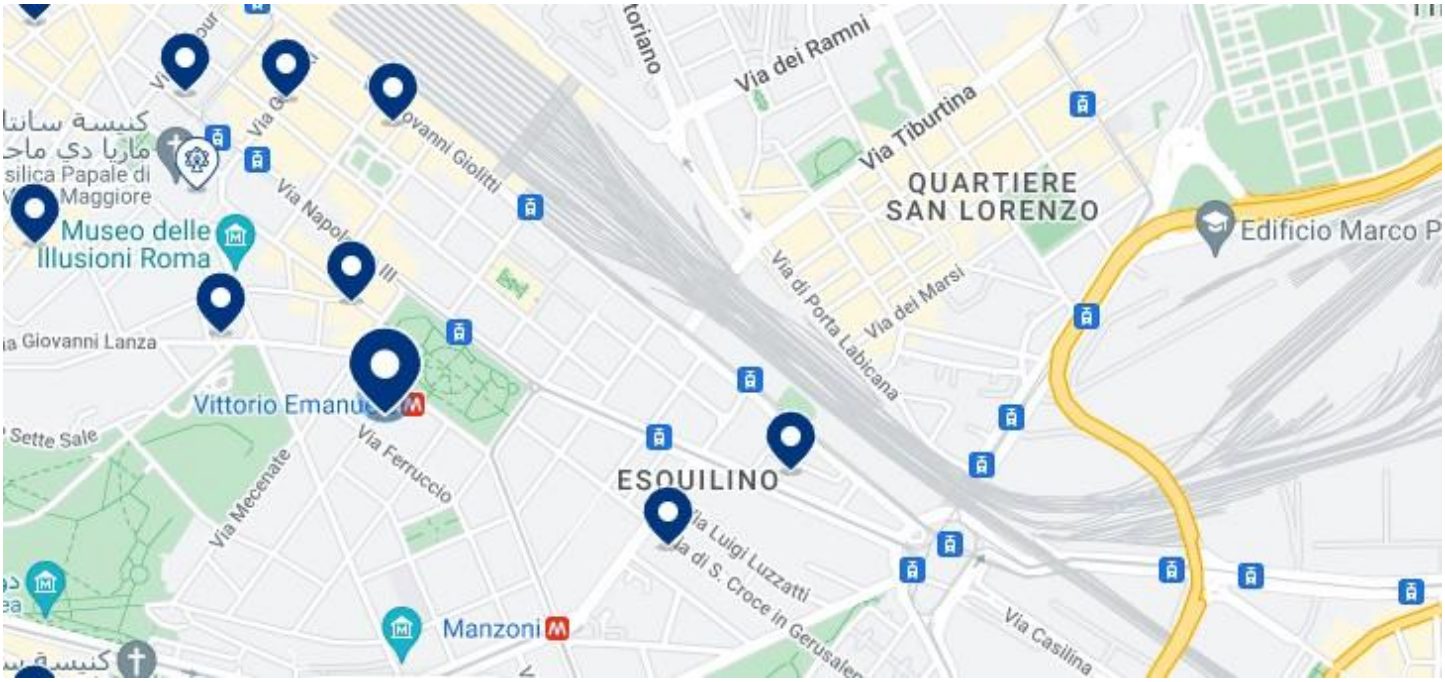
Browser History

After collecting all the information, we could from the memory dump, we started to search through the other evidence provided, Artifact 2, since it was a browser history file, BrowserHistoryViewer wasused. We found some interesting website visits and google searches that might help guide us to his
exact location, the following screenshots dictate all the interesting searches we found which are: “thecolosseum”, “Fontana Di Trevi”, “Pantheon”, “Sistine Chapel” and a hotel called “Rome Orange Inn”.(See figures 1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5)

https://www.google.c...	كولوسيوم - بحث Google	4/23/2023 11:55:00 PM	2	https://www.google.co...	Link	00:00:01.507	Chrome
https://www.google.c...	كولوسيوم - بحث Google	4/23/2023 11:55:01 PM	2	https://www.google.co...	Link	00:01:19.114	Chrome
https://www.google.c...	fontana di trevi - بحث Google	4/23/2023 11:55:31 PM	2		Generated	00:00:00.920	Chrome
https://www.google.c...	fontana di trevi - بحث Google	4/23/2023 11:55:32 PM	2	https://www.google.co...	Link	00:00:03.307	Chrome
https://www.google.c...	البانتيون - بحث Google	4/23/2023 11:54:42 PM	2	https://www.google.co...	Link	00:00:01.223	Chrome
https://www.google.c...	البانتيون - بحث Google	4/23/2023 11:54:44 PM	2	https://www.google.co...	Link	00:00:06.212	Chrome
https://www.google.c...	Pantheon - بحث Google	4/23/2023 11:54:48 PM	2	https://www.google.co...	Link	00:00:01.267	Chrome
https://www.google.c...	Pantheon - بحث Google	4/23/2023 11:54:49 PM	2	https://www.google.co...	Link	00:00:28.050	Chrome
https://www.booking....	Rome Orange Inn، 2023 روما – أحدث أسعار	4/23/2023 11:58:30 PM	1	https://www.booking.c...	Link	00:00:05.776	Chrome
https://m.museivatica...	Sistine Chapel	4/23/2023 11:56:43 PM	1	https://www.google.co...	Link		Chrome

Figures *1.2.1*, *1.2.2*, *1.2.3*, *1.2.4*, *1.2.5*

After viewing the hotel page, I was able to find the exact url of the page, and therefore the exactlocation of the hotel as well as an address. (See figures 1.2.6, 1.2.7)



– Via Buonarroti 39, Central Station, 00185 Rome, Italy (روما, إيطاليا)

Figure *1.2.6*

Figure *1.2.7*

Introduction

In the investigation of the missing person case, significant progress has been made through the examination of a memory dump using the powerful tool "Volatility." This analysis has yielded valuable insights and enabled the identification of pertinent artifacts. By determining the original operating system profile and conducting a thorough file scan, a comprehensive understanding of the system's contents was attained. Additionally, targeted searches based on the missing person's Eurotrip plans led to the discovery of two crucial photo files. These findings lay the groundwork for further investigation and provide a promising path towards resolving the case.

Methodology

The investigation into the missing person case involved an in-depth review of the data and artefacts available. We started by looking at an Mbox file that contained three important emails. One of the emails contained a flight confirmation outlining the missing person's journey from Cairo to Italy, with a stopover in France. The flight was scheduled to leave Cairo International Airport at 4:20 on March 3, 2023, and arrive back at Leonardo da Vinci International Airport at 20:55 on May 15, 2023. A second email confirmed the reservation at the Rome Orange Inn, with check-in and check-out dates of March 3 and 15, 2023, respectively.

Additionally, we were able to extract important data like text messages and call history from the missing person's phone's Android image. Through this analysis, we found several texts that were sent and received by people with the names Sophia Loren and James Gandolfini. The messages said the missing person had arrived in Rome and checked into their hotel, and that James Gandolfini was a friend who lived there. Additional messages described their travels to famous sites including the Colosseum, Palatine Hill, and the Romulo and Remo Statue. There were also hints of upcoming meetings, including a night out at Cica Cica with Sophia Loren.

However, it became clear that the missing person stopped replying to both James Gandolfini and Sophia Loren's messages, raising questions about their safety. The phone was turned off for about a month before being turned back on at 21:37 on May 4, 2023. On May 6 and May 7, automatic response messages informed the missing person of missed calls from numbers, indicating efforts to get in touch with them while they were gone. James Gandolfini and Sophia Loren expressed concern for the health of the missing person in separate messages, which stated their concern.

In order to create a timeline of the missing person's interactions and activities, this investigation's methodology involved a careful review of email correspondence, text messages, and call logs. We hope to learn more about their whereabouts and the circumstances of their disappearance by utilizing these artefacts.

Investigation Findings

The investigation's findings present significant revelations gleaned from the analysis of data from various sources, including communications, travel logs, and data from digital devices.

Digital Device Analysis:

Significant clues about their interactions and activities were revealed by the examination of the missing person's Android phone. Conversations with Sophia Loren and James Gandolfini were discovered through the review of text messages and call logs. Their conversations about getting together and James' offer to pick up the missing person suggested that James Gandolfini was a friend who lived in Rome. The digital investigation also revealed that the phone was off for about a month before being turned back on. This caused anxiety due to the sudden disappearance of the missing person and the subsequent missed calls from phone numbers.

Travel Record Analysis:

According to an analysis of the flight confirmation email, the missing person had a transit in France before flying to Italy on March 3, 2023, from Cairo International Airport. On May 15, 2023, Leonardo da Vinci International Airport would host the return trip. These travel logs provide evidence that the missing person was in Rome during the time of the investigation.

Communication Analysis:

Text message analysis gave crucial details about the missing person's interactions and activities. They successfully arrived, as proven by their responses to messages from their mother, James Gandolfini, and Sophia Loren, and by their ability to contact one another using an Italian phone number. The two actors' friends became worried when the communication abruptly stopped and Sophia Loren's and James Gandolfini's subsequent messages went unanswered.

Assumptions

Let's investigate a more evident hypothesis about Jooney Deep's disappearance considering the information presented. The theory centers on Jooney's vacation and the potential for trouble stemming from laced drugs and possible kidnapping.

1- Unforeseen Circumstances:

Jooney was having a great time in Rome, but maybe something unexpected happened. This might entail incidents, wounds, or becoming a victim of theft or assault, among other crimes. It can be difficult to identify a specific event in the absence of more details, but these scenarios are plausible.

2- Substance Abuse:

As mentioned earlier, Jooney's use of drugs while on vacation was brought up. He might have consumed drugs or substances that caused an adverse reaction or a medical emergency. This might be due to an unintentional overdose, unfavorable side effects, or developing a vulnerable state that made him a prime candidate for exploitation or kidnapping.

3- Criminal Involvement:

Jooney may have been in danger due to his interactions with people who were connected to drug dealers or other criminal elements. It is conceivable that he might have been abducted, coerced, or forced into an undesirable situation if he tried to buy drugs from dangerous people.

4- Unintentional Isolation:

It's also possible that Jooney secluded himself during his vacation on purpose. This could involve voluntarily leaving one's life behind in order to start a new one or flee from problems with the law or money. But in the absence of hard data or other information, this is still speculation.

Recommendations

I would like to make the following suggestions for the investigation into Jooney Deep's disappearance considering the information provided:

Collaboration and Information Sharing:

It is crucial to establish a collaborative approach among law enforcement agencies, intelligence services, and relevant stakeholders to effectively investigate Jooney Deep's disappearance. Timely and efficient sharing of information, including the findings from digital device analysis, travel records, and communication analysis, is essential for a comprehensive understanding of the case. Coordinated efforts will enable a more focused investigation and minimize information gaps.

Intensified Investigation:

Given the suspicious circumstances surrounding Jooney's disappearance, it is necessary to intensify the investigation. This should include the following steps:

a. *Thoroughly searching the hotel grounds: Returning to the hotel where Jooney's belongings were discovered and meticulously searching the immediate area may yield additional hints or proof of his whereabouts.*

b. *Interviewing witnesses and hotel staff: Conducting interviews with witnesses who were there when Jooney was there can help learn more. Interviewing hotel employees who interacted with Jooney or may have seen any unusual activity is another important step in this process.*

c. *Retracing Jooney's steps: It's essential to investigate Jooney's actions prior to his disappearance. This entails reviewing credit card records, reviewing CCTV footage from the hotel and surrounding areas, and getting in touch with any relevant places he might have visited.*

d. *Including local law enforcement agencies and specialized units, such as the missing persons unit or the criminal investigation department, can help the investigation move along faster by offering valuable expertise and resources.*

e. *Examining Jooney's financial records, including bank statements and transactions, in-depth may turn up any suspicious financial activity or possible explanations for his disappearance.*

f. *Hiring forensic specialists to look over any physical evidence, like Jooney's possessions or other things discovered at the hotel, can help clarify crucial information or possible leads.*

1. **International cooperation**:
   Cooperation with relevant foreign law enforcement organizations, embassies, and consulates is crucial given Jooney's international travel and the potential for wrongdoing. A more thorough investigation may be facilitated by information sharing, intelligence-gathering cooperation, and assistance from foreign counterparts.

2. **Public awareness campaign:**
   To generate leads and gather potential information from people who might have seen Jooney or know something about his disappearance, it can be helpful to launch a public awareness campaign through media outlets, social media platforms, and local communities.

Conclusion

Several hypotheses and potential scenarios have been identified based on the analysis of the information that is currently available, including digital device data, travel logs, communication analysis, and the circumstances surrounding Jooney Deep's disappearance. These scenarios could involve Jooney running into dangerous people involved in drug dealing, taking on a secret identity or living a double life, or Jooney could accidentally take drugs that have been tainted. Even though these hypotheses are just that—hypotheses—they open possibilities for additional research.

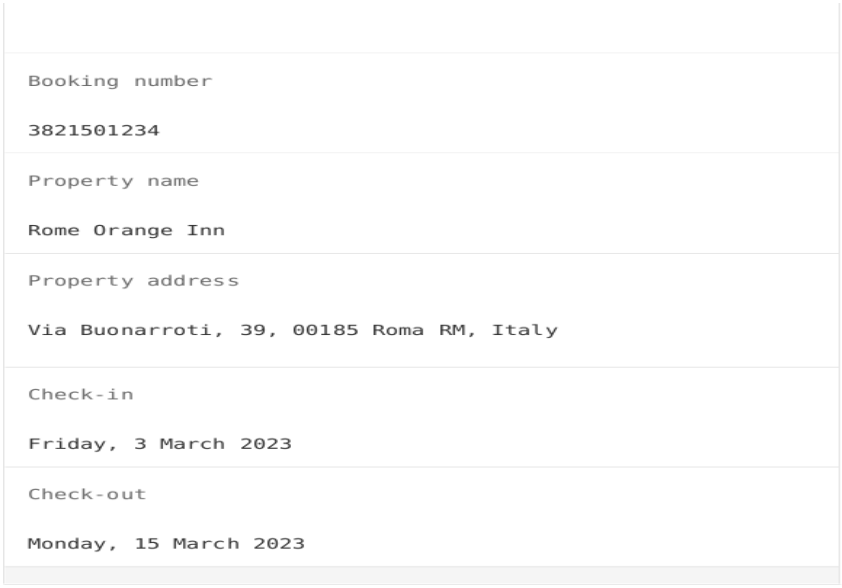
It is advised that cooperation and information sharing between law enforcement agencies, intelligence services, and pertinent stakeholders be established in order to advance the investigation effectively. This includes disseminating the results of analyses of digital device data, travel logs, and communication data. Additionally, it is essential to step up the investigation by carrying out exhaustive searches, repeating witness and staff interviews, tracking Jooney's movements, involving local authorities and specialized units, looking into financial records, using forensic analysis, and enlisting international cooperation.

A public awareness campaign should also be launched to motivate people who may have information to come forward. This will help investigators by creating leads and growing the amount of information they have at their disposal.

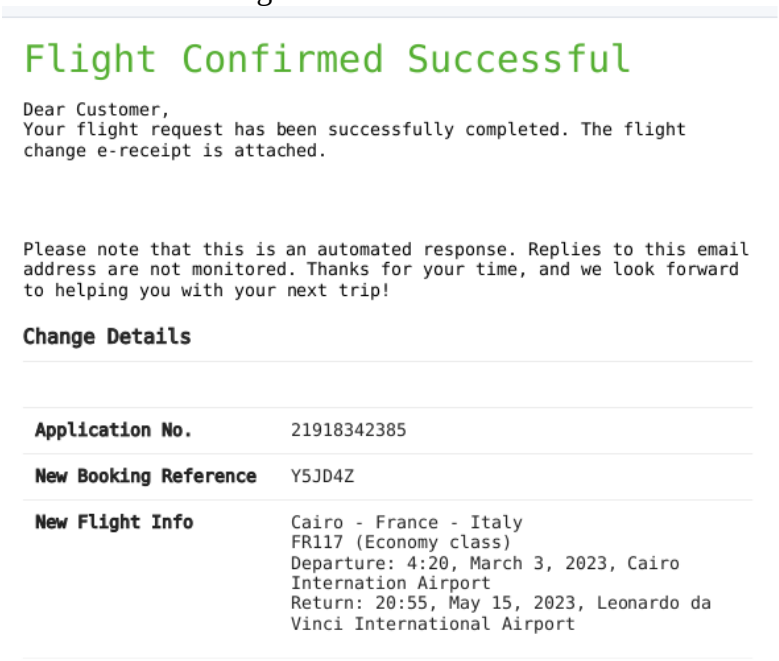
It's essential to remember that the assumptions and data up to this point served as the foundation for these recommendations. The investigation should adjust and reassess its approaches as new evidence or additional information becomes available.

Appendices

1. Screenshot Evidence:
    - Screenshot 1: Text message conversation with Jooney Deep discussing the trip itinerary and hotel reservation details.



- Screenshot 2: Email confirmation of flight tickets from Cairo to Rome.



Flight Confirmed Successful

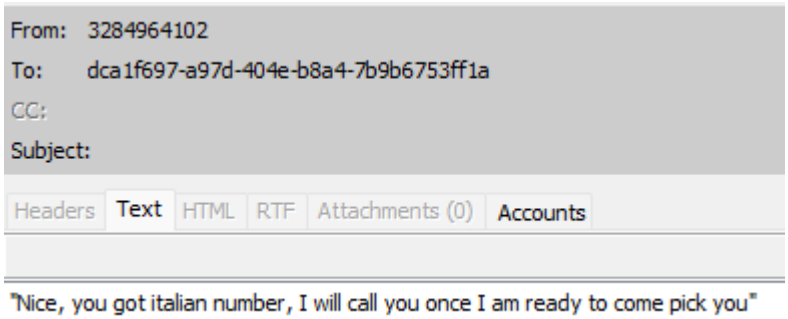
Dear Customer,
Your flight request has been successfully completed. The flight change e-receipt is attached.

Please note that this is an automated response. Replies to this email address are not monitored. Thanks for your time, and we look forward to helping you with your next trip!

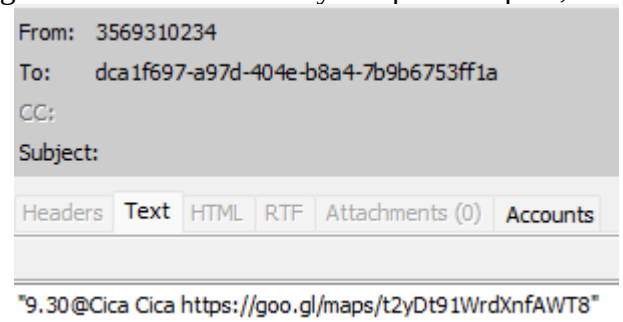
Change Details

Application No.	21918342385
New Booking Reference	Y5JD4Z
New Flight Info	Cairo - France - Italy FR117 (Economy class) Departure: 4:20, March 3, 2023, Cairo Internation Airport Return: 20:55, May 15, 2023, Leonardo da Vinci International Airport

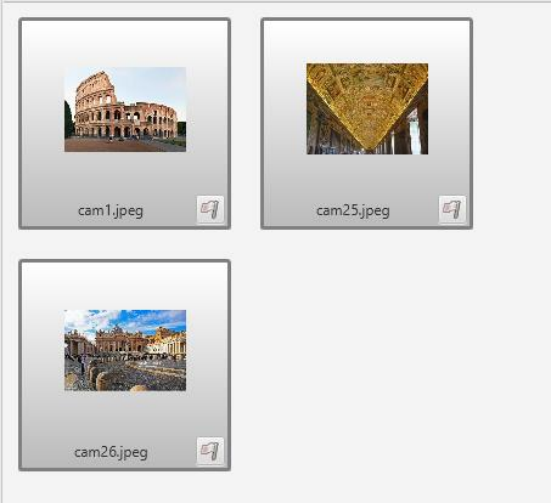
2. Call Logs:
   - Call Log 1: message record between Jooney Deep and his friend, discussing the plan to meet in Rome.



   - Call Log 2: message record between Jooney Deep and Sophia, Talking about meeting



3. Additional Evidence:
    - Evidence 1: Pictures Jooney took of local sightseeing excursions



    - Evidence 3: Email correspondence between Jooney Deep and James, discussing a sightseeing excursion in Rome.