

Case Identifier: #01218542

Case Investigator: Helena Trent

Identity of the Submitter: Helena Trent

Date of Receipt: 12/05/2023

Items for Examination

Cellular Device

- Galaxy A54 128GB (Black)
- Serial Number: 4CE0023F
- Evidence Item: ECG-14005
- Passcode: 112603

Personal Laptop Computer

- Samsung Galaxy Book3 1000GB
- Model Number: NP750QFG-KA1US
- Serial Number: 8GS55897
- Evidence Item: ECG-14055
- Passcode: Williams!78CG6

Forensic Analysis

On 12/5/2023 I received a search warrant through the US District Courts in Washington D.C. Information pertaining to the investigation was provided and I was instructed to pay close attention to communications as the suspect is believed to have had contact with Russian officials.

Cellular Device:

Tools Acquired

- SIM card reader
- Charger
- Oxygen Forensics Detective Software

After receiving the warrant and acquiring the needed tools I began the examination.

- The device was still on and locked
 - I turned on airplane mode from the lockscreen to stop the device from receiving signals.
- Reading SIM Card
 - I moved on to reading the SIM card. On this particular device the card is located at the top. I used a tray ejector to carefully remove the card and insert it into the SIM card reader attached to my workstation.

Case Identifier: #01218542

Case Investigator: Helena Trent

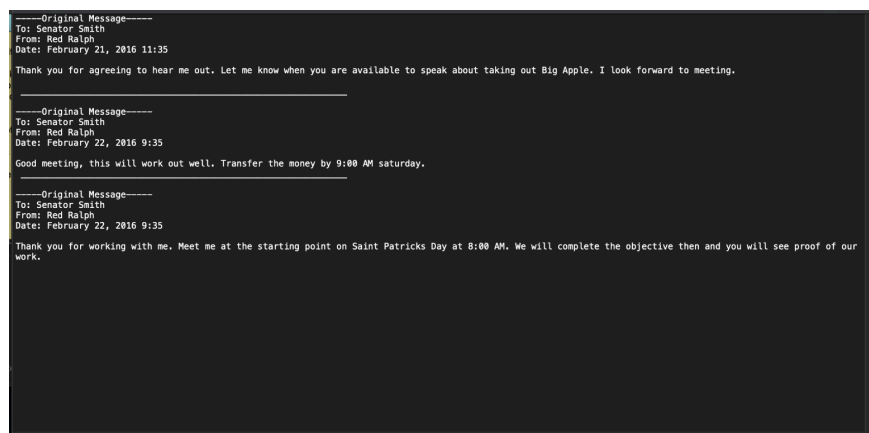
Identity of the Submitter: Helena Trent

Date of Receipt: 12/05/2023

- Phone Numbers & Text Messages
 - There were numerous phone numbers that were contacted within the time window covered by the search warrant. There was one number of interest with a Russian country code (+7 (922) 555-1543) under the contact Red Ralph.
- I took action by using Oxygen Forensics
 - Due to the operating system the file system was extracted from the device. In addition oxygen forensics also allowed me to extract the Samsung smart switch backups which contain contacts, notes, messages, and more. I also used oxygen forensics' cloud extractor to ensure that I was getting all the information possible from the device.
- Relevant Documented Messages
 - Phone Number: +7 (922) 555-1543
 - Contact Name: Red Ralph
 - Message:
 - It is imperative that we talk in person for this conversation. Lunch on Saturday 12/15 at our usual spot on 5th. Be there at 12pm, see you then.

Personal Computer:

- On today's date I began the forensic acquisition/imaging of evidence item ECG-14055. The device was shut off when I received it and it was noted that it was dead at the time it was collected. I charged the device before proceeding with the investigation.
- To begin the imaging process I connected the original media to the write blocker via USB to my examination machine. I then began the process.
 - This imaging was done to protect the original media. I can confirm that no damage was done to the original media or device. After making the duplicate I did not do anything else to the original media. Hashes were generated to ensure integrity.
- Once the imaging had been completed and was then documented, I used Internet Evidence.I primarily used OS forensics for this step. I used search and carving techniques to find relevant emails that could be useful to the investigation. I knew that the name was Red Ralph from the analysis of the mobile device so I started there. I was able to find the following string of emails.



```
-----Original Message-----
To: Senator Smith
From: Red Ralph
Date: February 21, 2016 11:35

Thank you for agreeing to hear me out. Let me know when you are available to speak about taking out Big Apple. I look forward to meeting.

-----Original Message-----
To: Senator Smith
From: Red Ralph
Date: February 22, 2016 9:35

Good meeting, this will work out well. Transfer the money by 9:00 AM saturday.

-----Original Message-----
To: Senator Smith
From: Red Ralph
Date: February 22, 2016 9:35

Thank you for working with me. Meet me at the starting point on Saint Patricks Day at 8:00 AM. We will complete the objective then and you will see proof of our work.
```

Case Identifier: #01218542

Case Investigator: Helena Trent

Identity of the Submitter: Helena Trent

Date of Receipt: 12/05/2023

- Once the emails were analyzed and documented, I was also able to view deleted files. I used OS forensics to find pieces of the deleted files to recover them. The relevant messages found are pictured below. The files were not overwritten so it was fairly easy to recover them.

It was wonderful doing buiness with you.The election should now go according to your plan. Great work.

-

Senator Smith, the objective is complete and everything went according to plan. The Big Apple has been taken down.

-

Case Identifier: #01218542

Case Investigator: Helena Trent

Identity of the Submitter: Helena Trent

Date of Receipt: 12/05/2023

Conclusion

In conclusion to the report, no original media was damaged, manipulated, or changed in any way. I analyzed the devices as they were brought to me and within the parameters of the search warrant. The devices and evidence yielded from them stayed in a secure location for the duration of the time it was at the lab. Logs were updated when it first entered our possession and when it was no longer in our possession. Chain of custody was maintained to the best of my knowledge.

- Hardware used to recover information
 - Lab workstation
 - SIM card reader
 - Write Blocker
- Software used to recover information
 - Oxygen Forensics
 - Cloud Extractor
 - OS Forensics
- Evidence Includes
 - Text message between suspect and Russian phone number.
 - Smith had contact with a Russian national involving a meetup for lunch.
 - Email Conversations with Red Ralph
 - The conversations recovered confirmed the meeting. In addition it is clear that both Red Ralph and Smith were using code names to avoid detection. "Big Apple" seems to be code for their target.
 - Several Deleted Zip Files
 - These files showed confirmation that whatever plan the two were working on was completed to Red Ralph's satisfaction.