Case Identifier: 23CR00006-950

Case Investigator: Luke Skywalker

Identity of the Submitter: James Hetfield

Date of Receipt: 4/11/23

Items for Examination:

Cellular Device: 5G Samsung S23 Ultra Cellular Device

- Dual SIM
- 256GB ROM
- 8GB RAM

Personal Laptop Computer: Lenovo ThinkPad P16 Intel (16”) Mobile Workstation

- 128 GB DDR5-4800MHz (SODIMM) - (4 x 32 GB)
- 1 TB SSD M.2 2280 PCIe Gen4 Performance TLC Opal

Findings and Report (Forensic Analysis):

• On April 11th, 2023, I was able to retrieve a search warrant through the US District Courts in Washington D.C. to examine two devices belonging to Mr. Jacob Sanderson.

Cellular Device:

In order to examine the mobile device, I acquired the listed tools below:

- SIM card reader
- Oxygen Forensics Detective (Digital Mobile Forensic Software)

I began the examination process once I was able to obtain the search warrant and gather the necessary tools needed for the process.

- Due to the device being locked as well as still being powered on, the first step I took was to unlock the phone.
- I was able to unlock the phone because the senator’s aide was able to provide me with the password to unlock the phone but otherwise could not provide me with any further information.

Case Identifier: 23CR00006-950

Case Investigator: Luke Skywalker

Identity of the Submitter: James Hetfield

Date of Receipt: 4/11/23

- Using the SIM card reader, I was able to extract data from the mobile device's SIM card and upload it to my workstation, which will allow me to examine the information and data that was/is present on the mobile device.
- Using Oxygen Forensics, I was able to identify text messages and import call data from the mobile device that pertained to a contact in the phone labeled with the alias "Red Ralph" in the mobile device.
- The next step I took was to document a message that included information about a meeting held between Mr. Sanderson and "Red Ralph".
- Documented Message:
  • Phone Number: +7 (922) 555-1543
  • Contact Name: Red Ralph
  • Message Details: "Mr. Sanderson, I believe our lunch meeting that occurred on March 3rd went a long way towards helping us both accomplish our goals. I will email you in the next two-to-three-days to discuss further the services we will provide to you and the payment you will provide to us. We will also meet again during this two-to-three-day time period. Stay vigilant to those who may be watching or suspecting anything."

Personal Computer

- On April 11th, 2023, I was able to retrieve a search warrant through the US District Courts in Washington D.C. to examine two devices belonging to Mr. Jacob Sanderson.

In order to examine the computer, I acquired the listed tools below:

- OSForensics

I began the examination process once I was able to obtain the search warrant and gather the necessary tools needed for the process.

- As with Mr. Sanderson's cell phone, his laptop was locked, but still powered on.
- The first step I took was to gain access to the laptop. This was completed by a live acquisition, due to the fact that Mr. Sanderson had the actual password of his device present when requesting a hint for the sign in password.
- I then began the process to examine the hard drive that was associated with Mr. Sanderson's laptop in order to find any information that would be helpful to my case.

Case Identifier: 23CR00006-950

Case Investigator: Luke Skywalker

Identity of the Submitter: James Hetfield

Date of Receipt: 4/11/23

- First, I used OSForensics to recover any E-mail messages that would be relevant to the case. Within OSForensics, I used the create index feature and selected E-mails and attachments. I then began the indexing process.
- After the indexing process was completed, I then used the search index feature within OSForensics, and proceeded to search for any instances of the term “Red Ralph” being used.
- Once the search was completed, I determined Mr. Sanderson did indeed exchange emails with the individual known as “Red Ralph”.
- I made proper documentation of the exchanging of such emails between the two, before beginning the process to search for any files that may have been deleted.

-----Original message-----
To: Jacob Sanderson
From: Red Ralph
Date: March 1, 2023 9:38
Subject: Campaign Finance Document

Good day Mr. Sanderson. I hope you are well. My consulting services have provided me the ability to provide you a way to see Mrs. Evelyn Doe's campaign finances. Please send me an email when you are available to meet again to discuss payment and completion of the task.

-----Original message-----
To: Jacob Sanderson
From: Red Ralph
Date: March 3, 2023 10:11
Subject: Campaign Finance Document

I think the meeting went as well as we all could have hoped Mr. Sanderson. Please transer me the amount of $10,000 on Monday, March 6th. The routing and account number are as follows.
Routing: 1122333444
Account number: 5556667788

-----Original message-----
To: Jacob Sanderson
From: Red Ralph
Date: March 6, 2023 7:33
Subject: Campaign Finance Document

Excellent, we are ready to move in. Please meet me at Footy's Diner at 0600 hours EST tomorrow. I will discuss how you can now access the document and what uses having this document can provide you.

Case Identifier: 23CR00006-950

Case Investigator: Luke Skywalker

Identity of the Submitter: James Hetfield

Date of Receipt: 4/11/23

- I began the process of searching for deleted files that had previously been present on the device by using OSForensics.
- While using OSForensics, I used the deleted index file feature that is provided and was able to make notice that there was a large number of deleted files that were zipped.
- The quality indicator within OSForensics also was able to show me that the files were largely intact.
- These zipped files contained classified information discussing the upcoming election.
- It was then determined that the individual listed as “Red Ralph” received the money from Mr. Sanderson.
- Furthermore, more zipped files were discovered, and they contained notes about a task being completed that involved a stolen document belonging to Mrs. Evelyn Doe, who is Mr. Jacob Sanderson’s opponent in the upcoming election.

Case Identifier: 23CR00006-950

Case Investigator: Luke Skywalker

Identity of the Submitter: James Hetfield

Date of Receipt: 4/11/23

Text file named “Access granted”

Senator Sanderson, now that you have access to those documents, I expect you to attack Mrs. Doe about her lack of finances. Once you are elected, we expect other forms of "compensation" or "assistance" for our country in exchange for helping you reach your position. If you are not elected or our communication line is compromised, be advised there will be no refunds, and you are to erase any and everything relating to me.

Text file named “Sanderson to Ralph”

Fantastic work, I have a huge lead on her already in the polls and this will only help solidify the election in my favor. Don't worry, I won't forget about the "assistance" that you are looking for. That will come in due time. I just need this election over with as soon as possible and we will all benefit. If I do need your services again, we can discuss that futher as well when that time comes.

Case Identifier: 23CR00006-950

Case Investigator: Luke Skywalker

Identity of the Submitter: James Hetfield

Date of Receipt: 4/11/23

Conclusion:

None of the original media has been damaged or changed in any way. Backups were created, and proper analyzation and documentation methods were followed. The devices are currently locked in a safe. I used a SIM card reader and Oxygen Forensics to help examine the mobile device belonging to Mr. Sanderson in order to gather the provided evidence, and I used OSForensics to help examine Mr. Sanderson's computer which helped me gather the provided evidence. The evidence provided includes documented emails and text messages which show communication, meetings, and payment between Mr. Jacob Sanderson and the individual with the alias "Red Ralph".