Case identifier: 012345

Case investigator: Ethan Heeter

Identity of the submitter: Ethan Heeter

Date of receipt: 4/24/2024

Examined items:

- Cellular device
    - Apple iphone 14: Serial Number R79DR8C47N
    - Personal device of the defendant
    - IOS 17.4.1 Operating System
- Laptop computer
    - Dell Inspiron 15: Serial Number DPVWZ94
    - Personal device of the defendant
    - Windows 10 operating system

Findings and report:

- Apple Iphone 14
    - I received a search warrant from the Washington D.C court system on 4/1/2024 to search through and analyze the data on the mobile device
    - The following forensics tools were used to search the mobile device:
        - SIM card reader
        - Oxygen Forensics Detective
    - The passcode to the Iphone needed to be bypassed in order to better analyze its contents. This was done using Oxygen Forensics Detective, which can break the passcode in order to find the correct one. This is done through the Oxygen

Case identifier: 012345

Case investigator: Ethan Heeter

Identity of the submitter: Ethan Heeter

Date of receipt: 4/24/2024

Forensic Device Extractor tool. This tool also extracts the contents of the phone to the PC for further analysis.

- The SIM card is taken out of the Iphone so that the SIM card reader can be hooked up to it. The SIM card houses critical information such as contact lists and any stored messages, which lend vital evidence to the case.
- The SIM card revealed suspicious contacts on the defendants contact list, namely contact named “Red Ralph”. The messages between the defendant and the contact were deleted.
- In order to view the deleted messages, the manually extracted data from the previous use of the Oxygen Forensic Device Extractor tool was examined on PC, which allows for the use of more advanced Oxygen Forensic tools. The tool that was used to access the deleted messages is Oxygen Forensics SQLite Viewer
- Recovered message between the defendant and Red Ralph is as follows:
  - Phone Number: (922) 555-1543
  - Contact Name: Red Ralph
  - Message Sent: 2/14/2024 at 3:42 PM
  - Message:

    “The meeting is confirmed for 2:00 PM tomorrow. We will discuss matters pertaining to our agreement then.”

Case identifier: 012345

Case investigator: Ethan Heeter

Identity of the submitter: Ethan Heeter

Date of receipt: 4/24/2024

- Personal Computer
    - The search warrant to search the personal computer was obtained from the Washington DC court system on 4/1/2024 to search through and analyze the data on the personal computer
    - The following forensic tools were used to search the personal computer:
        - EnCase
        - Hardware Write Blocker
    - First, a hardware write blocker was connected to the computer. This prevents any changes to the device by blocking any attempt to write data, leaving the device in a read-only state. This ensures that the contents of the device are not altered, maintaining the integrity of any data found in the device.
    - A forensic image of the computer's hard drive was made. This was in order to maintain the integrity of the data itself, making sure that none of the tools or processes that are used would compromise the integrity of the findings as an original, unaltered version still exists. This was done through EnCase. Now that an image has been made, forensic tools can be used on the system without fear of contaminating evidence, as there is always a copy of the unaltered original to return to.
    - EnCase is used to check the system's records, notably the emails. This is done through a string search using the previous contact name, "Red Ralph" alongside

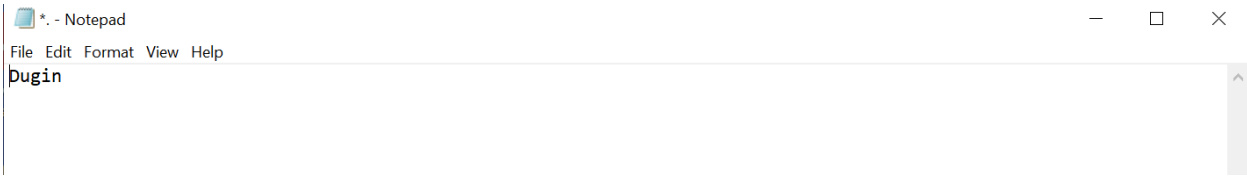
Case identifier: 012345

Case investigator: Ethan Heeter

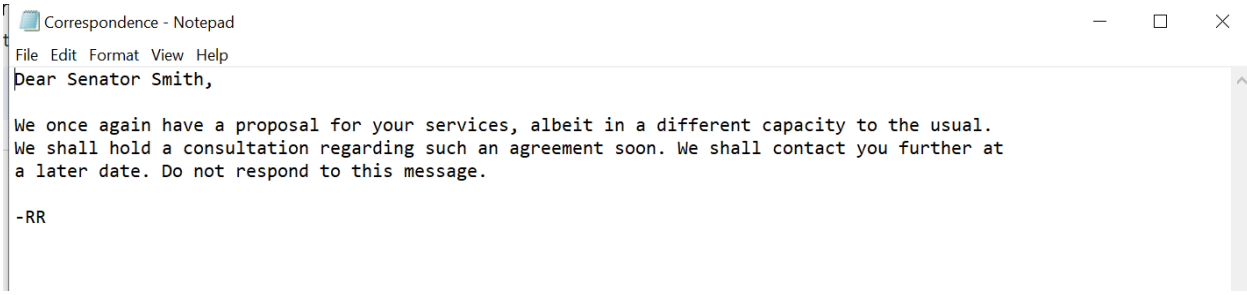
Identity of the submitter: Ethan Heeter

Date of receipt: 4/24/2024

various permutations like “RedRalph” and “RR”. Three deleted emails are found addressed to the defendant from “RedRalph@gmail.com”, the first of which is a single word and the other two containing one image each. The first email sent from Red Ralph is a single word, that word being “Dugin”, the last name of the author of the influential russian book, “The Foundations of Geopolitics: The Geopolitical Future of Russia”, a book which describes strategies and goals of destabilizing and reducing the influence of the United States. This was sent on 12/12/2023 at 1:03 PM.



- Suspecting the images to be cases of Steganography, the practice of imbedding files into images, Steghide was used with the keyword Dugin to check the images sent in the emails for hidden messages. This revealed a hidden text file, the contents of which are as follows.

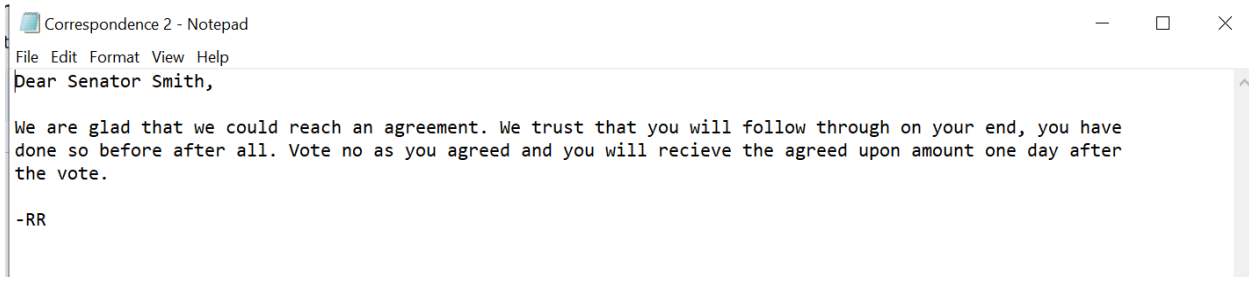


Case identifier: 012345

Case investigator: Ethan Heeter

Identity of the submitter: Ethan Heeter

Date of receipt: 4/24/2024



- The emails were sent on 2/12/2024 at 3:29 PM and 2/16/2024 at 4:42 PM respectively.
- After uncovering the emails, more searches were performed to find any other evidence. Using EnCases ability to see deleted files, we found 3 deleted zip folders that contained classified documents and information.
- Web logs files for internet explorer, made available by EnCase, were searched to attempt to find any signs of the defendant using file sharing websites. A string search using the names of such sites shows that the defendant visited popular file sharing website Dropbox, where he uploaded these three zip files. It is unclear as to if the zipped folders of classified documents were then downloaded by others. The three uploads are as follows:
  - Important1.zip uploaded to Dropbox on 12/15/2023
  - Important2.zip uploaded to Dropbox on 1/24/2024
  - Important3.zip uploaded to Dropbox on 3/3/2024

Case identifier: 012345

Case investigator: Ethan Heeter

Identity of the submitter: Ethan Heeter

Date of receipt: 4/24/2024

Conclusions:

- No damage was caused to the mobile phone or the personal computer, both still contain all of the relevant data as described in the report. Images of the two devices were taken and used to ensure that the originals remain unchanged.
- The use of software and hardware, notably a SIM card reader and Oxygen Forensics Detective for the mobile phone and a Hardware Write Blocker and EnCase for the personal computer allowed evidence to be retrieved from both devices.
- The deleted emails on the personal computer suggest that the defendant seems to have been in contact with someone setting up a later meeting, and in the follow up email mentioning swaying the defendants vote with a payout, a bribe he seems to have accepted according to the emails. The emails also allude to another, “usual” way that the defendant interacts with them, likely alluding to the possible sharing of classified information via a file sharing site the defendant has uploaded such documents to, as detailed in the report.
- The sending of the Dugin email suggests that the defendant had been in contact with Red Ralph since at least 12/12/2023, as that email contained a code word for communication via steganography that would be used in the emails. This also aligns with the uploads of classified documents to Dropbox, the first of which came 3 days later on 12/15/2023.
- Using this information, a timeline of events surrounding the meeting can be constructed. First, an email was sent on the 12th detailing Red Ralph’s intentions of holding a meeting with the defendant, who at this point has been in contact with Red Ralph and uploading

Case identifier: 012345

Case investigator: Ethan Heeter

Identity of the submitter: Ethan Heeter

Date of receipt: 4/24/2024

classified documents to Dropbox for five months. The message sent two days later on the 14th found on the mobile phone seems to be a confirmation of the meeting described in the first email. The second email was sent a day after such a meeting occurred according to the time suggested by the text message, thus why the email mentions that an agreement has been reached between the two parties. Using this evidence, it can be concluded that the first email alerted the defendant to a future meeting, then two days later on the 14th the text confirmed the meeting for the 15th. Then the final email on the 16th, which came one day after the supposed meeting, confirms that a deal was reached, with the deal seemingly being Red Ralph paying the defendant to vote no to an upcoming Senate vote.