Case Identifier: 605897

Case Investigator: Logan Powell

Identity of the Submitter: Logan Powell

Date of Receipt: 12/10/21

Items for Examination:

- Cellular Device
    - Model: iPhone 11 Pro
    - Serial Number: H0583HT8GE
    - Model Number: NESPFOE/S
    - Color: White
- Personal Laptop Computer
    - Dell Inspiron 3000
    - Model Number: GIO4804
    - Serial Number: GSKSF0FG4T
    - Color: Steel Grey

Findings and Report (Forensic Analysis):

- Cellular Device:
    - On today's date, I retrieved a search warrant through the US District Courts in Washington D.C.
    - Acquire tools for examination of mobile device:
        - SIM card reader
        - Oxygen Forensics Detective (Digital Mobile Forensic Software)

    - Once the tools were acquired and the search warrant was retrieved, the examination began.
        - Because the device was still on and locked, the first step I took the device and used the SIM card reader to get around the Face ID/PIN lock. From there I made sure to note any files that had been tampered with or deleted such as downloads, search history, text messages, emails, and more.
        - Using the SIM card reader, I extracted a text that was sent from a contact labeled "Red Ralph", that was confirming a lunch meeting on 2/14/2021. From this I was able to use iCloud operation which gave me access to all the suspects information.
        - Each phone number and text message
            - +1 202 872 4863 – Red Ralph
        - I took action by using the Oxygen Forensics tool. I connected the device to the software extractor where I selected UICC acquisition and chose the corresponding reader. Next, I established an output location with the extracted data so it can be accessed.
        - Documented Message:
            - Message Recovered: "Lets meet at the café downtown at noon"

    - On today's date, I began the forensic acquisition/imaging process of the suspect's SSD on their personal laptop to begin extracting the emails and accounts that were used. To acquire the data from the suspects drive, an MD5 hash was created to validate the original image securely through WinHex. Before exposing myself to being susceptible to any type

Case Identifier: 605897

Case Investigator: Logan Powell

Identity of the Submitter: Logan Powell

Date of Receipt: 12/10/21

of viruses and malware I used X-ways security to clean all the data from the suspects media.

- After connecting the original media in the laptop to the hardware write-blocker via USB 3.0 to my examination machine, I began the imaging process. During the imaging process, Autopsy was used to organize and list all the suspects' files and folders for viewing. While conducting my investigation I came across some files that were protected by password and encryption. OSForensics was used to acquire the password and WinHex bitshifting to decrypt data found.
- To ensure that I acquired all the information from the suspects computer I use WinHex to view all connected disks. I also double check the disk space to make sure there are no hidden partitions by examining any areas containing space that I never accounted for and is checked for any remaining evidence.

Case Identifier: 605897

Case Investigator: Logan Powell

Identity of the Submitter: Logan Powell

Date of Receipt: 12/10/21

- Once the imaging had been completed and was then documented, I used Internet Evidence to further my investigation on the suspect's machine. When conducting my search, I found email receipts of the Suspect and 'Red Ralph' of casual exchanges of messages relating to money being exchanged and the idea of 'Taking out the Big apple'.

----------Original Message----------
To: Senator Smith
From: Red Ralph
Date: February 21, 2016 11:35 (- 05:00 EST)
Subject: The Big Apple

Let me know when you are ready for me to discuss about taking out the Big Apple.

----------Original Message----------
To: Senator Smith
From: Red Ralph
Date: February 22, 2016 10:27 (- 05:00 EST)
Subject: The Big Apple

Thank you for meeting. Transfer the money by 06:00 by Friday.

----------Original Message----------
To: Senator Smith
From: Red Ralph
Date: February 26, 2016 11:35 (- 05:00 EST)
Subject: The Big Apple

Thank you for the cooperation. Meet me at the outpost on Saint Patrick's Day at 0700 hours EST. The objective will be complete 30 minutes before.

  - Once the email was analyzed and documented, I was also able to view previously deleted files where there I came across 2 txt. files one named "Objective complete" stating "Senator Smith, the objective is complete. The Big Apple has been taken out.", and another named "Smith to Ralph" stating "It was great doing business with you. Now the election can continue just as planned. You have done great."

Case Identifier: 605897

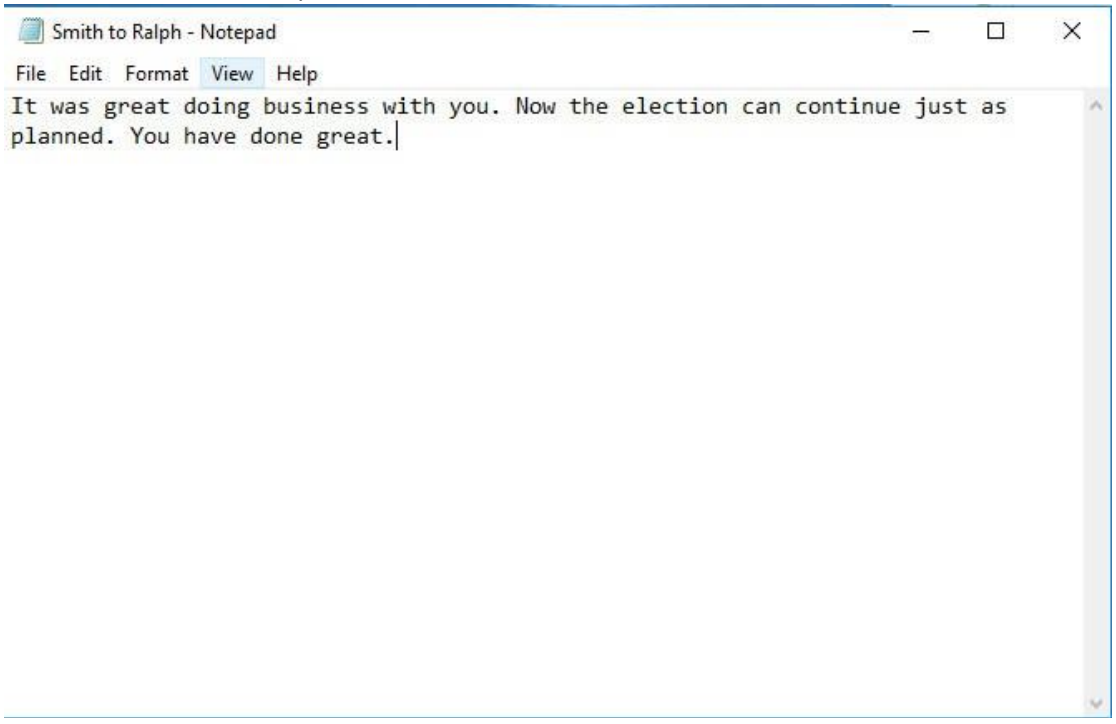
Case Investigator: Logan Powell

Identity of the Submitter: Logan Powell

Date of Receipt: 12/10/21

- File named “Objective Complete”

- File named “Smith to Ralph”



Case Identifier: 605897

Case Investigator: Logan Powell

Identity of the Submitter: Logan Powell

Date of Receipt: 12/10/21

Conclusion:

- In conclusion to the report, no original media was damaged, manipulated, or changed in anyway. After thorough investigation the findings were conclusive of the alleged interference and tampering in the election.
- Hardware that was used to recover files:
    - ACR38T-D1 Plug-in (SIM-Sized) Card Reader
    - AMD Athlon 5000+ processor
    - Adaptec FireWire card
    - One SPP/EPP/ECP parallel port
- Software that was used to recover files:
    - OSForensics
    - Winhex
    - Oxygen Forensics
- Evidence includes:
- Transcript of messages being exchanged back and forth
- Encrypted txt. And deleted Files
- Recovered text files with information on confirmation of objectives
- Emails

Case Identifier: 605897

Case Investigator: Logan Powell

Identity of the Submitter: Logan Powell

Date of Receipt: 12/10/21