Case Identifier: 34W7L

Case Investigator: Ashley Barasebwa

Identity of the Submitter: Ashley Barasebwa

Date of Receipt: 11/24/2023

---

## Items for Examination:

- Cellular Device:
    - Serial Number: X0XX234XYXYX
    - Make: Apple
    - Model iPhone 14 Pro Max
    - A cellular device is used for the examination of the contents listed in the cell phone of a United States government official. By looking at the contents of the cell phone, I will be able to get access to the call log, messages, deleted files, and their digital footprint.

Personal Laptop Computer

- Serial Number: X0XX234XYXYX
- Make: Hewlett-Packard (HP)
- Model: HP Pavilion Laptop 15t-eg300, 15.6”
- A laptop computer device is used for the examination of the contents listed in the laptop of a United States government official. By looking at the contents inside of the laptop, I will be able to gain access to the digital trace, email communications and payment history.

---

## 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 the examination of mobile device:
        - SIM card reader
        - Oxygen Forensics Detective (Digital Mobile Forensic Software)
        - WinHex (Data Recovery Software)
    - Once the tools were acquired and the search warrant was retrieved, the examination began.

Case Identifier: 34W7L

Case Investigator: Ashley Barasebwa

Identity of the Submitter: Ashley Barasebwa

Date of Receipt: 11/24/2023

- Because the device was still on and locked, the first step I took was to inform the lead investigator that I was going to open the device. I then removed the device's back panel, and then I removed the battery. Once I removed the battery, I removed the SIM card from its holder. After removing the SIM card from its holder, I inserted the SIM card into the card reader. By doing that I was able to insert the card reader into my forensic workstation's USB port.
- Using the SIM card reader, I was able to see deleted messages, read and unread messages and even messages that were sent to the U.S. government official that they have not even read yet. I started viewing messages that were not read by the government official and I found some disturbing information. I found that the Russian official who was in contact with the U.S. official was asking the official feedback on their plans for an attack on U.S. soil. The contact's name of the Russian official in their phone was labeled as "Red Ralph". As I was looking through more messages between the Russian official, the conversation started off by the U.S. official offering money to do an attack on the United States of America. I found a text message confirming a lunch meeting with the Russian official on 2/15/2023.
- Each phone number and text message:
    - +7 (922)-555-1543 ("Is it okay if we hijack a plane and have it crash into the Washington Monument?"
    - +7 (922)-555-1543 ("Let us talk about this during lunch, does 2/15/2023 work for you?")
    - +1 (202-978-2879) ("Hi sweetie, please come home for dinner")
    - +1 (318-789-3456) ("Hey dude, are you coming over for work today?")
    - +1 (202- 334-2456) ("Hey dad, could you please take me and Natalie shopping today?')
- I took action by using Oxygen Forensics (Digital Mobile Forensic Software) which helped me obtain more information about the U.S. Government official. They were able to extract data from their mobile device. Oxygen Forensics found encrypted files in their iCloud. They were able to decrypt the files and found numerous hidden images and voice audio recordings. I found pictures of the high-ranking U.S. official with a group of other Russian officials playing golf. They also found pictures of the Washington Monument, the World Trade Center, and The White House. The pictures I found were blurry, so I decided to use another software to extract clear pictures.
- I was able to also use WinHex, which is a data recovery software where I can extract raw files. These are the steps I took in WinHex to recover the pictures.

Case Identifier: 34W7L

Case Investigator: Ashley Barasebwa

Identity of the Submitter: Ashley Barasebwa

Date of Receipt: 11/24/2023

- I started WinHex, and clicked on File, then clicked Open from the menu.
- Navigated to my work folder, and then double-clicked on Recover1.jpg. Then click OK.
- At the top of the WinHex window, I noticed that the hexadecimal values starting at the first-byte position (offset 0) are 7A 7A 7A 7A, and the sixth position (offset 6) is also 7A.
- Clicked to the left of the first 7A hexadecimal value.
- Then typed FF D8 FF E0, which are the hexadecimal values for the first 4 bytes of a JPEG file.
- In the right pane at offset 6, I clicked the letter Z, and then typed in the letter J.
- I clicked File, Save As from the menu. In the Save File As dialog box, I went back to my work folder, typed Fixed1.jpg as the filename, and then click Save.
- I opened an image viewer where I was able to view a clearer picture.

- Documented Message:
- Phone Number: +7 (922)-555-1543
- Contact Name: Red Ralph
- Messages: (“Is it okay if we hijack a plane and have it crash into the Washington Monument?’)
- (“Let us talk about this during lunch, does 2/15/2023 work for you?”)

- Personal Computer:
- On today’s date, I retrieved a search warrant through the US District Courts in Washington D.C. To retrieve data from the U.S. officials' laptop
- I began the forensic acquisition/imaging process of the personal computer of a U.S. government official.
- Acquire tools for the examination of personal computer:
  - UFED
  - Autopsy (Digital Forensics Software)
- Once the tools were acquired and the search warrant was retrieved, the examination began.
  - These are the steps I took for using the Universal Forensic Extraction Device (UFED).
  - Downloaded the UFED Reader 3.2.exe file.

Case Identifier: 34W7L

Case Investigator: Ashley Barasebwa

Identity of the Submitter: Ashley Barasebwa

- In the table on the first page, I found the entry with Nokia in the first column and Logical Acquisition in the second column. In the third column, I clicked the **ufdr** link, and download the Nokia-logical.ufdr.
- I started the UFED Reader. Click File, Open from the menu, and click Nokia-logical.ufdr
- Next, I opened the Nokia-physical.ufdr file, and then I examined the information acquired from the computer. I found emails from "Red Ralph".
- The emails I found are listed below.

```
----------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.
```

- These emails were sent from an email named RedRalph@gmail.com. These emails also entail the payments and consulting services between the U.S. and Russian officials.
- I reached out to Autopsy, a digital forensic software tool that used data carving to recover deleted files. These are the steps that took place to retrieve the data.
- I used an FTK imager tool, then I went to File, then I clicked Add evidence file, and then the image file.
- Once I opened the image file, I selected the partition item in the evidence tree. Then I choose the Export Disk Image option in the context menu.
- Next, I added an image destination (Raw (dd)) into an image destination folder. I made sure to Set the image fragment size equal to zero since we want a single file, and then I clicked finish.
- Then using the Photorec in Autopsy, to recover the data from the unallocated space from the file.
- I then ranqphotorec_win.exe and selected the raw disk image as the data to recover from.
-

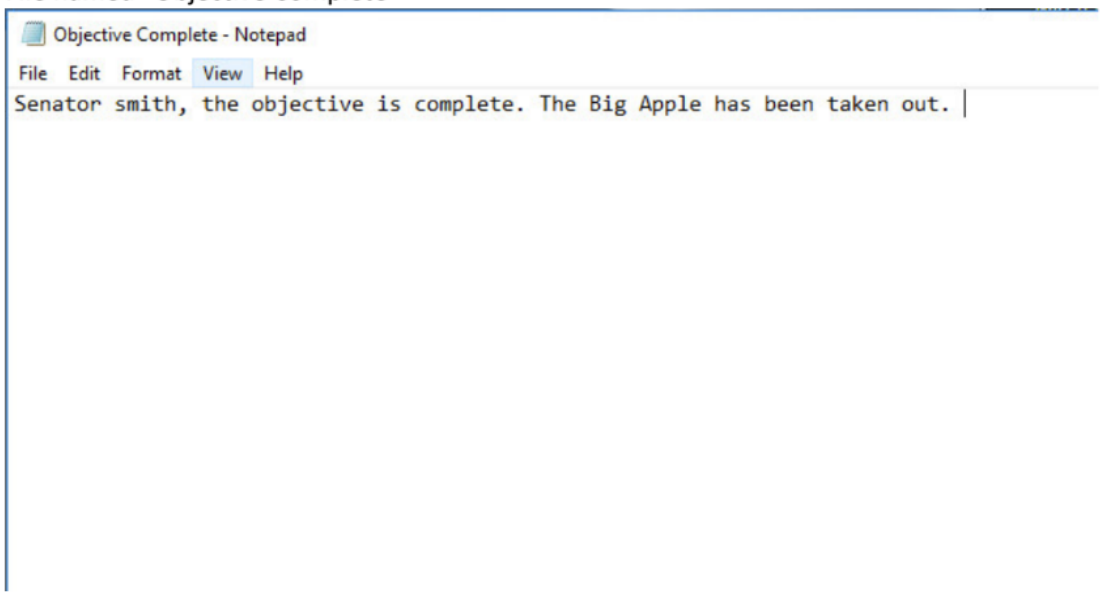
Case Identifier: 34W7L

Case Investigator: Ashley Barasebwa

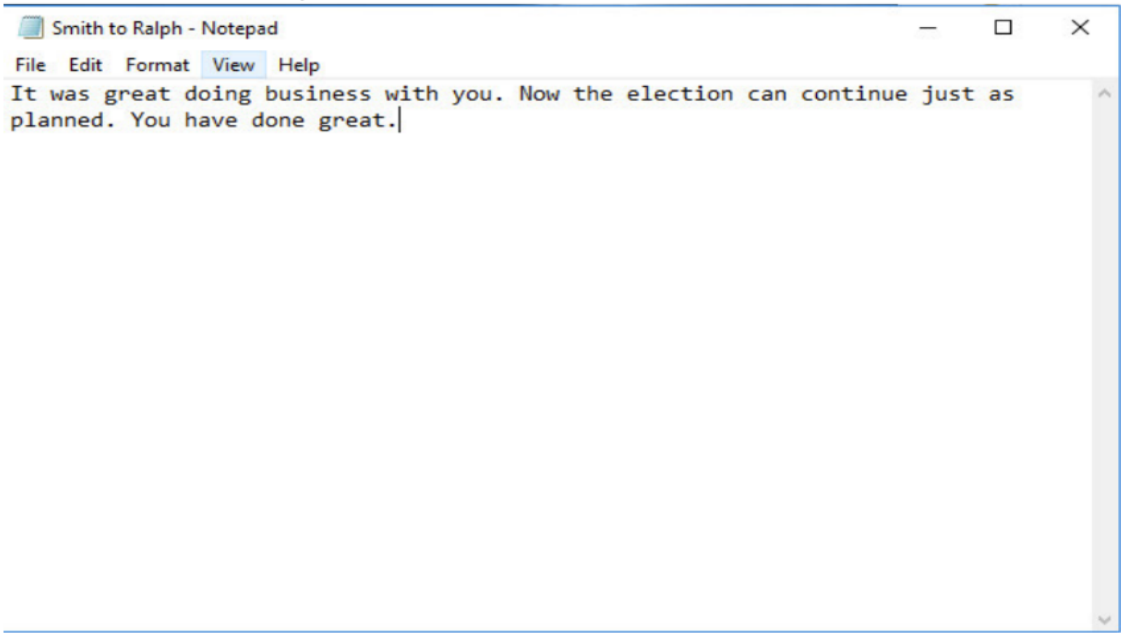
Identity of the Submitter: Ashley Barasebwa

- Then I set up the following options: file system type to FAT/NTFS/HFS+/ReiserFS/…
- Then set the search type to free: Scan for files from unallocated space only.
- Then I chose the folder to store the recovered files and pressed search.
- I was able to find deleted files the U.S. official deleted. The files are displayed below.
- These files and other zip consisting of classified material were on weblogs, they were uploaded to a file-sharing site. I was not able to see if these weblogs were viewed by anyone else.

File named “Objective Complete”




File named “Smith to Ralph”



Case Identifier: 34W7L

Case Investigator: Ashley Barasebwa

Identity of the Submitter: Ashley Barasebwa

## Conclusion:

- In conclusion to the report, no original media was damaged, manipulated, or changed in any way. Refer to the forensic analysis to the conclusion of how evidence was gathered. All steps taken to gather data were followed under the ISO/IEC 27037 and national law enforcement rules so the evidence could be presented in court. The forensic investigation included utilizing hardware and software systems to extract data from the phone device and personal computer. The U.S. official has incriminating evidence that could indict themselves in a trial with the United States. Their device entails messages with foreign nationals of Russia with plans to destruct and terrorize the United States of America.
- Hardware that was used to recover files: SIM card reader and Universal Forensic Extraction Device (UFED)
- Software that was used to recover files:
    - Oxygen Forensics Software https://oxygenforensics.com/en/
    - WinHex (Data Recovery Software) https://winhex.en.softonic.com/
    - Autopsy (Digital Forensics Software) https://www.autopsy.com/
- Evidence includes A text message confirming a lunch meeting on 2/15/2023 and the phone number was labeled "Red Ralph" in the contact list.
- Several email communications about meetings and payment for "consulting services" between the official and RedRalph@gmail.com
- Several deleted zip files of classified material that weblogs show were uploaded to a file-sharing site. It is not clear if they were downloaded by anyone.