

Case Identifier: DF-7239

Case Investigator: John Peck

Identity of the Submitter: Mary Johnson, HR Manager at XYZ Corporation

Date of Receipt: February 14, 2023

Items for Examination:

- Cellular Device
 - Make and Model: iPhone 12
 - Storage Capacity: 128 GB
 - Model Number: A2403
 - Operating System: iOS 15.1.1
- Personal Laptop Computer
 - Make and Model: Dell XPS 13
 - Processor: Intel Core i7-1165G7 (11th Gen)
 - RAM: 16 GB LPDDR4x
 - Storage: 512 GB SSD
 - Operating System: Windows 10 Pro
 - Display: 13.4-inch FHD+ (1920 x 1200) InfinityEdge Non-Touch Anti-Glare 500-Nit Display

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. to authorize the forensic examination of the cellular device in question.
 - The following tools were acquired for the examination of the mobile device:
 - SIM card reader
 - Oxygen Forensics Detective (Digital Mobile Forensic Software)
 - Once the tools were acquired and the search warrant was retrieved, the forensic examination of the cellular device was conducted.
 - The first step taken was to use the SIM card reader to extract the data from the SIM card. The extracted data included phone numbers, call logs, text messages, and other information related to the use of the cellular device.

The data extracted from the SIM card was then analyzed using the Oxygen Forensics Detective software, which revealed the following findings:

- A text message was found on the device confirming a lunch meeting on 2/15/20xx, and the phone number was labeled "Red Ralph" in the contact list.

In addition to the data extracted from the SIM card, a logical extraction of the device data was also performed, which allowed for the recovery of data from the device's operating system and applications.

Case Identifier: DF-7239

Case Investigator: John Peck

Identity of the Submitter: Mary Johnson, HR Manager at XYZ Corporation

Date of Receipt: February 14, 2023

The data extracted from the device was also analyzed using the Oxygen Forensics Detective software, which revealed the following findings:

- Several email communications were found on the device that contained details about meetings and payment for "consulting services" between the high ranking US government official and RedRalph@gmail.com.
- Several deleted zip files of classified material were found on the device, which were uploaded to a file sharing site. It is unclear if these files were downloaded by anyone.

In this case, Oxygen Forensics Detective was used to analyze the data extracted from the SIM card of the cellular device, as well as the data extracted from the device's operating system and applications.

Once the SIM card was extracted using the SIM card reader, the data from the SIM card was imported into Oxygen Forensics Detective. The software then automatically decoded the data, allowing for the analysis of phone numbers, call logs, text messages, and other information related to the use of the cellular device. This analysis revealed the text message confirming the lunch meeting and the phone number labeled "Red Ralph" in the contact list.

Next, a logical extraction of the device data was performed, which allowed for the recovery of data from the device's operating system and applications. The data extracted from the device was then imported into Oxygen Forensics Detective, which automatically decoded the data and allowed for the analysis of emails, deleted files, and other data related to the use of the device. This analysis revealed the emails containing details about meetings and payments for "consulting services" between the high ranking US government official and RedRalph@gmail.com, as well as the deleted zip files of classified material uploaded to a file sharing site.

Using the Oxygen Forensics Detective was an essential tool for the forensic examination of the cellular device, allowing for the extraction, decoding, and analysis of critical data that was used to support the investigation.

Documented Message:

- Phone Number: +7 (922) 555-1543
- Contact Name: Red Ralph
- Message: Hey Red Ralph, just wanted to confirm our lunch meeting for 2/15 at 12:00 PM. Looking forward to catching up. –US Government Official

Personal Computer:

Case Identifier: DF-7239

Case Investigator: John Peck

Identity of the Submitter: Mary Johnson, HR Manager at XYZ Corporation

Date of Receipt: February 14, 2023

- On 14FEB2023, I began the forensic acquisition/imaging process of the personal laptop computer, which is suspected to contain evidence of contact between a high-ranking US government official and Red Ralph. I ensured the laptop was secured and removed from any network connectivity to prevent data tampering.
- 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. I used Forensic ToolKit (FTK) Imager to make a forensic image of the entire hard drive. The FTK Imager tool also generated a hash value to verify the integrity of the data.

Once the imaging had been completed and was then documented, I used Internet Evidence Finder (IEF) to analyze the data. During my analysis, several email communications were discovered between the high ranking US government official and the email address RedRalph@gmail.com. The emails discussed meetings and payment for "consulting services" provided by Red Ralph to the US government official.

Moreover, several deleted zip files were found during the investigation. The web logs show that these files were uploaded to a file sharing site, although it is not clear if they were downloaded by anyone. Further analysis of these files may be required to determine their content and whether they contain classified material.

The forensic analysis of the personal laptop computer provided evidence of communication and meetings between the high ranking US government official and Red Ralph, as well as possible violations of information security protocols. The findings of this analysis are documented in the accompanying report and will be provided to the prosecutor for use as evidence in any potential legal proceedings.

Email 1:

From: highrankingofficial@us.gov

To: RedRalph@gmail.com

Subject: Meeting Request

Dear Red Ralph,

Case Identifier: DF-7239

Case Investigator: John Peck

Identity of the Submitter: Mary Johnson, HR Manager at XYZ Corporation

Date of Receipt: February 14, 2023

I hope this email finds you well. I am interested in discussing your consulting services and setting up a meeting to discuss your rates and how we can work together. Can you please let me know your availability for a lunch meeting next week?

Looking forward to hearing back from you soon.

Best regards,

High Ranking Official

Email 2:

From: RedRalph@gmail.com

To: highrankingofficial@us.gov

Subject: Re: Meeting Request

Dear High Ranking Official,

Thank you for your email. I'm available for a lunch meeting next week on February 15th. How about we meet at the Capitol Hill Club at 12 PM?

Regarding my consulting services, I can provide a range of services such as market analysis, lobbying, and strategic planning. My rates vary depending on the scope of work, but I can send you a detailed proposal if you're interested.

I look forward to meeting with you and discussing this further.

Best regards,

Red Ralph

Case Identifier: DF-7239

Case Investigator: John Peck

Identity of the Submitter: Mary Johnson, HR Manager at XYZ Corporation

Date of Receipt: February 14, 2023

- After completing the forensic acquisition and imaging process of the personal computer, I proceeded with the analysis of the data. Using forensic software, I was able to recover deleted files and emails that were of interest to the investigation. In particular, I discovered several deleted zip files containing classified material that had been uploaded to a file-sharing site.
- Upon further analysis, I was able to determine that the files had been deleted approximately one week after the date of the lunch meeting between the high-ranking US government official and Red Ralph, as documented in the email communications found on the laptop. The web logs show that the files were uploaded but it is unclear if they were downloaded by anyone.
- Based on my analysis, it appears that the high-ranking official may have been engaging in illegal activity by sharing classified information with Red Ralph. I have documented all of my findings and will submit a detailed report to the prosecutor as evidence in any future court proceedings.


Case Identifier: DF-7239

Case Investigator: John Peck

Identity of the Submitter: Mary Johnson, HR Manager at XYZ Corporation

Date of Receipt: February 14, 2023

File named "meeting"

 meeting - Notepad

File Edit Format View Help

"Meeting Notes - 2/15/20xx

Attending: Red Ralph, [High-Ranking Official], [Other Official]

Discussion:

Discussed payment for consulting services
[High-Ranking Official] provided Red Ralph with classified information
Discussed future meetings and plans for continued cooperation


Action Items:

Red Ralph to provide payment via offshore account
[High-Ranking Official] to provide additional classified information at next meeting
[Other Official] to provide cover for future meetings

Next Meeting:

Date: 3/10/20xx
Location: [Undisclosed location]
Agenda: Further discussion of classified information and continued cooperation"

File named "report"

 report - Notepad

File Edit Format View Help

"Expense Report - Q1 20xx

Consulting Services Payment to Red Ralph

Invoice Number: RR-2001
Date: 1/15/20xx
Amount: \$50,000
Payment Method: Offshore account transfer
Travel Expenses for Meeting with Red Ralph

Date: 2/15/20xx
Location: [Undisclosed location]
Airfare: \$2,500
Lodging: \$1,500
Meals: \$500
Miscellaneous: \$1,000
Total Expenses for Q1 20xx: \$55,500

Notes:

All expenses related to consulting services and travel for meetings with Red Ralph were approved by [High-Ranking Official]
All expenses were paid via personal funds and not reimbursed by the US government"

Case Identifier: DF-7239

Case Investigator: John Peck

Identity of the Submitter: Mary Johnson, HR Manager at XYZ Corporation

Date of Receipt: February 14, 2023

Steps I conducted during this investigation, and what they are.

- Acquisition and Imaging: The first step was to acquire and image both the cellular device and personal computer. This was done using specialized hardware and software to ensure that no data was altered or lost during the process.
- String Searches: With the cellular device, we used software like Oxygen Forensics Detective to search for specific keywords, phrases, or phone numbers within the text messages, call logs, and other data on the device. This allowed us to quickly find any relevant information that could be used as evidence.
- Graphics Image Searches: With the personal computer, we used FTK Imager to search for graphic images that may have been relevant to the case. For example, we might search for any images of a specific location or individual that could be connected to the investigation.
- Erased File Recovery: With both the cellular device and personal computer, we used specialized software to recover any files that had been deleted or erased from the device. This involved analyzing the device's storage to locate areas where data had been marked for deletion, but not yet overwritten by the operating system.

Conclusion:

In conclusion to the report, no original media was damaged, manipulated, or changed in anyway.

Based on the findings of the forensic analysis conducted on the cellular device and personal computer, it appears that the high-ranking US government official had engaged in communication and meetings with a person labeled as "Red Ralph" through his phone and laptop.

On the cellular device, a text message was found that confirmed a lunch meeting on a specific date, and the phone number was labeled as "Red Ralph" in the contact list. On the laptop, several email communications were found about meetings and payment for "consulting services" between the official and an email address belonging to Red Ralph.

Furthermore, several deleted zip files of classified material were found on the laptop, which were uploaded to a file-sharing site. Although it is not clear whether anyone downloaded these files, their existence raises concerns regarding the potential disclosure of classified information. During the forensic acquisition and imaging process of the personal computer, no original media was damaged, manipulated, or changed in any way

Case Identifier: DF-7239

Case Investigator: John Peck

Identity of the Submitter: Mary Johnson, HR Manager at XYZ Corporation

Date of Receipt: February 14, 2023

- The hardware used to recover files from the personal computer was a hardware write-blocker connected to an examination machine via USB 3.0. The write-blocker ensured that the original media was not damaged, manipulated, or changed in any way during the imaging process. The examination machine used was a standard forensic workstation with appropriate specifications to run the imaging and analysis software. Additionally, a SIM card reader was used to extract data from the cellular device, including call logs, messages, and other relevant data.
- The software tool used to recover files was Internet Evidence Finder (IEF), which helped recover the deleted zip files from the laptop. The evidence recovered includes the email conversation between the user named Red Ralph and the high-ranking US government official. The imaging process was completed using specialized software, Oxygen Forensics Detective, which allowed for the acquisition of digital evidence from the personal computer. We also used FTK Imager to search for any images on the computer relating to the case.

Evidence includes:

- Email conversation between a user named "Red Ralph" and the high-ranking US government official's email address, which suggests the occurrence of several meetings and payments for "consulting services."
- A text message found on the cellular device which confirms a lunch meeting between the official and Red Ralph, which raises questions about the purpose of their meeting and what information was exchanged.
- Two text files found on the personal computer, one named "meeting" and the other "report," that appear to contain sensitive information related to US government operations. The contents of these files could be potentially damaging if leaked, and raise concerns about the official's handling of classified information.

Based on the evidence gathered, it is highly likely that the US government official was engaging in discussions with a potentially unauthorized party, which could be seen as a breach of national security. It is recommended that further investigation is conducted to determine the extent of the damage caused by the potential disclosure of classified information and to identify any other parties involved in the matter.

In conclusion, the forensic analysis conducted on the cellular device and personal computer revealed potentially damaging evidence that warrants further investigation. The evidence recovered was obtained using non-invasive methods, and the original media was handled in a manner that ensured its integrity was preserved throughout the process.