Marcus Sowers

Digital Forensics

Final

4/10/21

Case Scenario:

You were hired as a forensic expert to investigate alleged contact between US and Russian officials. You performed a forensic analysis on the laptop and cell phone of a high-ranking US government official. During the investigation you found the following:

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

On the laptop - several email communications about meetings and payment for "consulting services" between the official and RedRalph@gmail.com

On the laptop - several deleted zip files of classified material that web logs show were uploaded to a file sharing site. It is not clear if they were downloaded by anyone. The owner of the laptop and phone has "lawyered up" and is not saying anything about what they were doing on either device or any meetings that may have happened. You are now preparing your official report to the special prosecutor as evidence that may go to court in the future.

Items Submitted for Examination:

Cell Phone:

- Apple iPhone XR Device via T-Mobile
- Serial Number: X45F782AWGAK
- Registered to U.S Attorney General Merrick B. Garland

Laptop:

- Surface Pro 7 Platinum Intel Core i7
- Model Number: MYD8369/A
- Registered to U.S Attorney General Merrick B. Garland

Forensic Analysis Findings:

Today, April 10th, 2021 I successfully obtained a search warrant allowing me to go through the possessions of the United States Attorney General Merrick B Garland. We than used both a hex dump and a sim card reader allowing me to search for information from the cell phone obtained. The iPhone being extracted for information had almost full battery with a pass lock. A Joint Test Action Group process was preformed that allows us to bypass the password cleanly. The next step we took was to create a copy of the information obtained, so we can always have second copy and to be safe. This can be done with the sim card reader tool discussed earlier. We can digitally connect it to a software allowing us to easily create a copy of the information in question. Anyone the United States General Attorney has been contacting will be under further investigation. All contacts and recent messages will be further analyzed to determine potential connections. Following, we than completed a hex dump which allows us to obtain the iPhones raw image in a binary format. This process will obtain all information regarding the

investigation including deleted and hidden files. A message was flagged from (293) 687-9384, whose contact name was “Red Ralph”. This text message stated, “I can meet April 15th, 2021 for our lunch date to discuss the plan further and get things started.”

Today, April 10th, 2021 I successfully obtained a search warrant allowing me to go through the possessions of the United States Attorney General Merrick B Garland. After the iPhone was extracted for information, we than did the same to his Surface pro-7. When we began the procurement of the hard drive on his laptop, we noticed it was windows 10 compatible making it easier for us to extract information. The forensic imaging process was copied from drive to drive. We decided to this because it more cost efficient and still allows us to transfer the files and information obtained. A CRU WiebeTech USB WriteBlocker was than used as an adapter between the laptop of General Attorney Merrick B. Garland and our forensic machine. Once the imaging process starts, we had to be sure to use a hardware blocker and software that helps create a forensic image. There are plenty of programs that could be used to complete this specific function. We will be using Belkasoft Acquisition tool. The forensic images created will than be saved to the hard drive.

Once the forensic imaging is saved and documented, I analyzed the evidence gathered from the US General Attorney Merrick B. Garlands computer. A software called Clonezilla is than used for our data recovery software, helping find huge evidence that were red flags. There were several email communications about meetings and payment for "consulting services" between the official and RedRalph@gmail.com. Emails recovered from Merrick B. Garland computer proved the meeting went on and payment for "consulting services" was flagged. The emails recovered will be used as evidence, and my Clonezilla software is able to provide the

proper evidence to prove the emails were deleted. Several files and emails were deleted that involved the United States General Attorney Merrick B. Garland to “Red Ralph”.

Conclusion:

In conclusion, all legally obtained evidence and potential leads from the United States general Attorney Merrick B. Garland for this forensics case have not been damaged or tampered with. These include the items in our report labeled as our “items being examined”. Different hardware was used to recover files including both a Sim Card Reader for the iPhone and the CRU WiebeTech USB WriteBlocker for the laptop. There were different software’s used to recover the files including the Belkasoft Acquisition Tool, which was used along with the CRU WriteBlocker to help create a forensic image of United States General Attorney Merrick B. Garland laptop. The other software used was the Clonezilla program, which was also extremely useful for the investigation.

The Evidence includes a text message found in the US General Attorneys cell phone between himself and “Red Ralph” that proved a meeting was going to take place between the two 2/15/2021. The message stated, “I can meet April 15th, 2021 for our lunch date to discuss the plan further and get things started.” This confirms the belief that the General Attorney Merrick B. Garland went to the meeting and committed a payment for "consulting services". This was confirmed because of the deleted emails discovered from the General attorney’s laptop confirmed the payments sent. The evidence gathered on the General Attorney is too compelling and convincing to determine what exactly happened on that date.