Forensics Evidence Report
Final Exam

Technician: Nathaly Flores

Date of Receipt: March 30, 2022

Case Identifier number:
A37889G88TE-00

Skeletal Assessment:

Investigating the alleged contact of the United States and the Russian officials. The investigation purpose is to provide the evidence that can be used to determine if there was any collusion present amongst the United States and Russian officials.

Evidence:

The evidence in question is a Google Pixel, with serial number: G25BC2R1SDG442 black color. The phone is in 2016 that google introduced. The phone specifications are 5-inch display, 4 GB of RAM, 128 GB of internal storage, with rear cameras with 12.3 megapixel and 8-megapixel front-facing cameras. Running Android 7.1 Nougat. Weight of 143 g.

In addition, a Mac Book Silver was used with one USB-C on the side of the laptop. Running macOS Sierra, the serial number of the computer is G22TG5RDX7DG

Size and Weight

- **Height:** 0.14–0.52 inch (0.35–1.31 cm)
- **Width:** 11.04 inches (28.05 cm)
- **Depth:** 7.74 inches (19.65 cm)
- **Weight:** 2.03 pounds (0.92 kg)2

Analysis:

Steps taken during the investigation included storing the original material by taking photos of the physical evidence. Moreover, taking screenshots and copying computer and phone logs, documenting the dates and times on the case, and re-creating a timeline of the series of events that prompted this investigation. The type of data acquisition was copied from the laptop's hard drive using the method of hard drive-to-file to another external hard drive. This method copies a sector-by-sector by copying the hard drive under study using a hardware WiebeTECH Forensic UltraDock V5 write blocker, which automatically detects and unlocks complex drive areas such as 'Device Configuration Overlay' (DC0) and 'Host Protected Area' (HPA). The Belka soft Acquisition Tool allowed me to create forensic images of hard drives, mobile devices' exact data from cloud storage. The created hash of the image file copied the image files, generated a hash for each image file, and mounted the image files using Prodiscover to search for any emails or data related to the investigation.

A text confirming a meeting on the date 12/15/2016 from the phone number labeled Red Ralph in the contact list was found on the phone. In the laptop, emails with photo attachments were found upon further investigation, and the photos were altered using the technique of Steganography. The suspect used the steganography method the least significant bit in the

images found. The last bits of information in the carrier image were substituted with their secret message. The hidden message was the "consulting services."
Furthermore, "payments" in the attachments in the email RedRalph@gmail.com handle. Deleted files that were deleted were rebuilt using a hex editor for Mac. Those files had UNC paths of a directory of a server. Analyzing the entire hard drive and partitions initially was not visible. A hidden partition was discovered. Since Apple uses Solid State Drive with TRIM on the Mac Book, there were zip files of classified material in the hidden partition within the hard drive volume. The fstab file can specify how to partition is handled in Os'—removing the fstab file line that defines the partition. Will make the hidden partition visible in MacOS Sierra it will get mounted.
However, I uploaded several zip files from the hidden partition on the file-sharing site, which explained that the deleted files equally important confidential files were found in the hidden partition. On the file-sharing website, we contacted the ISP and the company that hosts the website's service on which the files were uploaded to provide logs and find who is the owner of the file data server. The ISP confirmed that the IP Address location of a computer connecting to their file server was near Moscow, Russia. The suspect used Red Ralph as an alias name when he signed up for the service. This file uploading serves as solid evidence against the Official that he might have disclosed the confidential information to the other person named Red Ralph.

Summary

The evidence suggests the reason for leaking sensitive information was for monetary gain. Based on the solid evidence, there is reason to believe there was contact between the high-ranking United States government official and the Russian Official. There is also enough evidence that potentially shows that the United States official worked in collaboration with a Russian official.