Eric Tran

CYSE 407

Professor Bryan Bechard

6/30/19

Digital Forensics Investigation (Final Paper)

Case Identifier: DI-2152016-1

Case Investigator: Eric Tran

Case Submitter: John Johnson, Department of Justice

Date of Receipt: 07/01/2017

Description of Evidence

Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)
PH-1	**1**	**Samsung Galaxy S10 (Serial: SM-G970W)** **Fairly new with minor scratches on the screen and a small chip on the upper right edge of the phone. Passcode is 1154, all applications and bookmarks remain the same since recovery. OS: Pie, 9.0.**
LT-1	**1**	**Asus ZenBook Pro UX533 (Serial:UX544FD-NS76)** **Pristine condition with minor wear on the keyboard. Passcode is Supreme223. Applications, bookmarks, and contents remain the same since recovery. A password Excel page titled "MyPass" was found on the desktop. OS: Windows 10.**
HD-1	**1**	**Hard drive containing captured data from both the S10 and Asus laptop. Given by John Johnson and the data was recovered at the scene in order of volatility. Best practice is to copy the contents to our own drive and perform analysis with our copies. Hashes have lined up with the original, checked on 07/01/19 at 8:45AM by Eric Tran.**

Investigation Process

After completing the initial preparation phase and physical forensics phase, we began the digital forensics phase – mostly focusing on performing search strings, graphic image searches, and recovering erased files on the phone and laptop.

Having a copied image of the laptop and phone, the files were fed into OSForensics to begin string searches. Inside the application, we mounted the drive image and created an index looking for emails, attachments, office + PDF documents, and web files + xml. With these categories, we casted a wide net at first to see what shows up and then we will begin narrowing down as the evidence comes in. Since the high-level U.S. official was dealing with the new railgun project, we began to search for terms relating to the classified project. The search terms that were used:

Railgun

Classified

Project Freedom Rain

Navy

Naval Research

Experimental Weapon

Project

Secret

Weapon

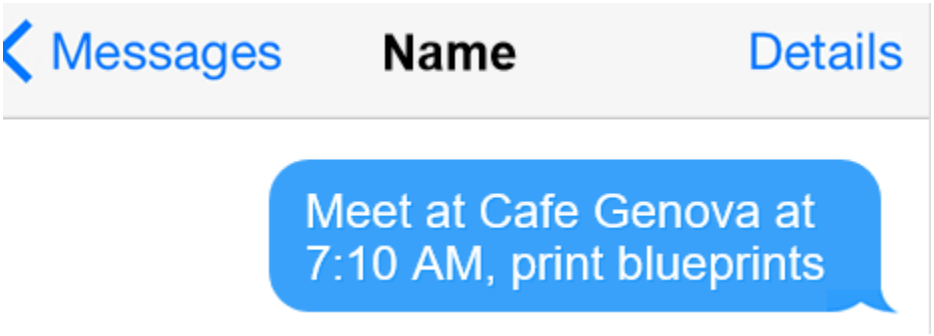
--Gmail Message--
From: RedRalph@gmail.com
To:Sgt01@gmail.com

Sgt01,
Thank you for the projects, meet you soon at Cafe Delmont 7:10 AM.
Remember technique I show you, alter headings of pics and change extension.

Red

Email from Red instructing the official to cover up crime.

After analyzing each result, there were several emails containing images which contained blueprints and specifications. The emails also detailed plans of the official's defection and payments to his offshore account. Along with the images and plans, the official promised more information and was told to rename the extensions of the pictures. Red Ralph instructed the official to change the first four bytes and the sixth byte. The phone on the other hand only contained text messages with Red Ralph regarding their meetings to discuss the project. Nothing of note was transmitted through text upon analysis with string search.



Text from Red instructing the official to bring blueprints of the railgun to their café meet.

After analysis and breakdown of the emails between Red Ralph and the official, we deducted that several images have been altered via extension to have different first four bytes and sixth byte. Using ProDiscover, we began to cluster search for type FIF since it is a label name of the JFIF JPEG format, which was mentioned in previous emails between Red Ralph and the official. Searching through the clusters, we found that several JPEG files have been overwritten with "yyyy." With this finding, we located the file and recovered several more JPEG images that contained a material manifest and electromagnetic specifications.

The official was stated to have used Dropbox to upload zipped files to their storage location which was then accessed by Red Ralph. The team then began to look for C:\Users\Sgt01\Dropbox and C:\Users\Sgt01\AppData\Roaming\Dropbox. Using the Internet Evidence Finder (IEF) Triage, we read and interpreted the filecache.dbx file and extracted the zipped files that were sent to Dropbox. These files contained classified information pertaining to the railgun.

The next step in our investigation consisted of recovering deleted files from the phone and laptop. Whenever a file is deleted in Windows, the file is renamed by the OS and moved to the recycle bin with a unique identifier. Windows then stores the original path and name in the info2 file. By looking at the ASCII data, Unicode data, and date and time of deletion, we recovered the files that were deleted. These files contained images of ship specifications sent to Red Ralph and several Word Documents containing meeting time and locations with Red Ralph.

Conclusion

Having gone through the examination process, the team concluded that we had enough evidence to present to John Johnson at the Department of Justice and handed over our documentation and evidence. We were tasked to answer the question, “Did the US official commit treason by transmitting classified projects to a Russian official by the name of Red Ralph” Basing off of evidence gathered from email, text message, Word documents, images, and text files, the collusion is present. Along with documents that contained blueprints and specifications, the official obeyed suggestions to hide the crime being committed and actively and knowingly deleted and modified files to throw off investigators. Through recovering of several classified documents that were deleted, the official sent more than railgun documents, but also ship specifications to the Russian official. It is the conclusion that, through evidence and action, the US official has knowingly and purposefully transmitted classified material to Red Ralph, a Russian official.

Works Cited

"Computer Forensics Investigation – A Case Study." *Infosec Resources*, 4 Mar. 2019, resources.infosecinstitute.com/computer-forensics-investigation-case-study/#gref.

"Forensic Analysis and Examination Planning." *Infosec Resources*, resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/forensic-science/forensic-analysis-and-examination-planning/#gref.