Tristan Woodard

Old Dominion University

CYSE 407

Final

Cyber Forensics Lab Overview

Case Identifier: Case CYSE407
Case Investigator: John Doe
Identity of the Submitter: Dave Green
Date of Receipt: 12/10/17

Items For examination

Cellular Phone

- Model - Samsung Galaxy S7
- Black color
- Plain black plastic impact case attached
- Serial Number s8987488474

Personal Laptop Computer

- Model - HP Envy x360
- Silver color
- Serial Number hl39428924

Findings and Report (Forensic Analysis):

Cellular Phone

- Upon receiving items, a search warrant was obtained the same day. Investigation began promptly.
- Tools used to begin investigation include
    - SIM card reader
    - Oxygen Forensics
    - AccessData FTK Imager
- Because the device was unlocked the first step was to isolate the device and ensure it stays on. The device was placed on charge and isolated from the network.
- To crack the password, the hash file was taken from an Image of available files.
- The hash was cracked with a rainbow table.
- After the phone was unlocked, the SIM card reader and imager were used to have all the data isolated, including available deleted data.
- The data was mounted onto a drive and examined via Oxygen Forensics.
- Using the string search “Ralph”, texts and contact data were quickly found relating to contact “Red Ralph”
- Contact Red Ralph used the phone number #555-555-5555
- On 2/15/2017 Red Ralph texted Official A at 9:35am EST “Are there no changes in the scheduled lunch meeting?”
- On 2/15/2017 Official A texted back Red Ralph at 9:42 am EST “We will need to meet at 12:30 instead, but other than that no changes.”
- There was so record of other correspondence between the two via text message and no call data.
- The texts were added to the report in Oxygen Forensics.

Case Identifier: Case CYSE407
Case Investigator: John Doe
Identity of the Submitter: Dave Green
Date of Receipt: 12/10/17

Personal Laptop Computer

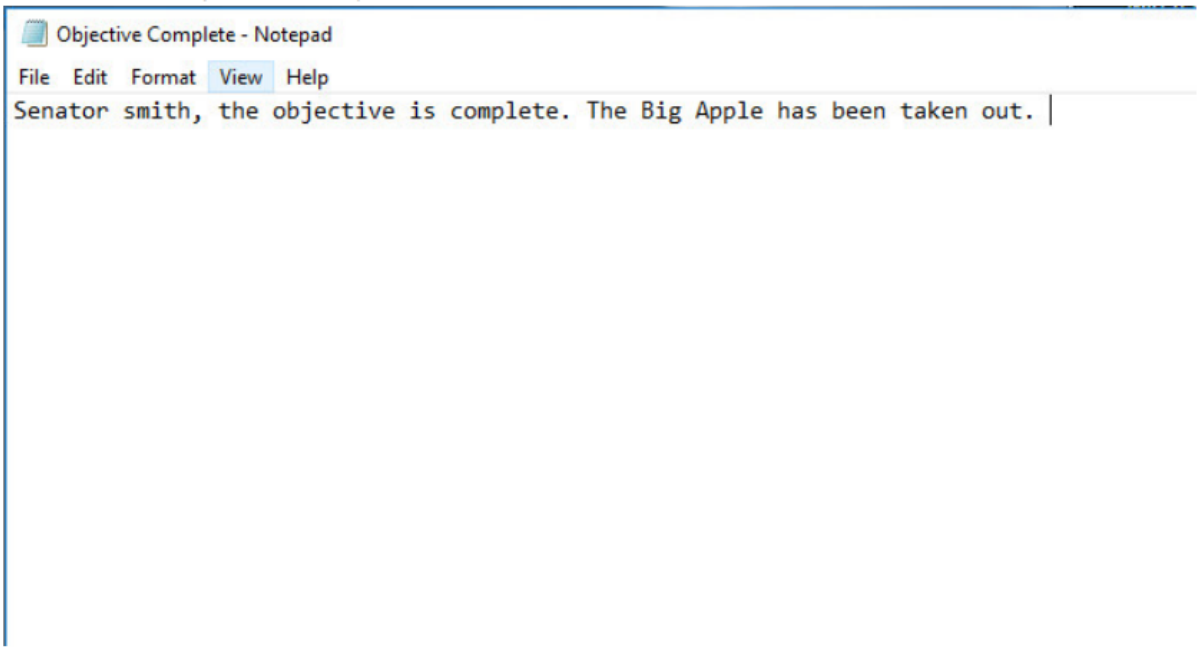
- After examining the Cellular phone, the Personal laptop computer was analyzed.
- The Personal Laptop Computer was isolated and powered on and connected to a non-internet connected device
- Hardware write blockers via USB 3.0 were introduced to ensure original data integrity
- AccessData FTK Imager was used to attain an image copy of the data.
- The data was mounted onto a virtual disk in Oxygen Forensics and analyzed.'
- Information was narrowed down using string search "Ralph"
- Using the Oxygen Forensics email viewer, correspondence was found between Official A, referred to as Senator Smith within the email system, and RedRalph@gmail.com. The emails view as the following:

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

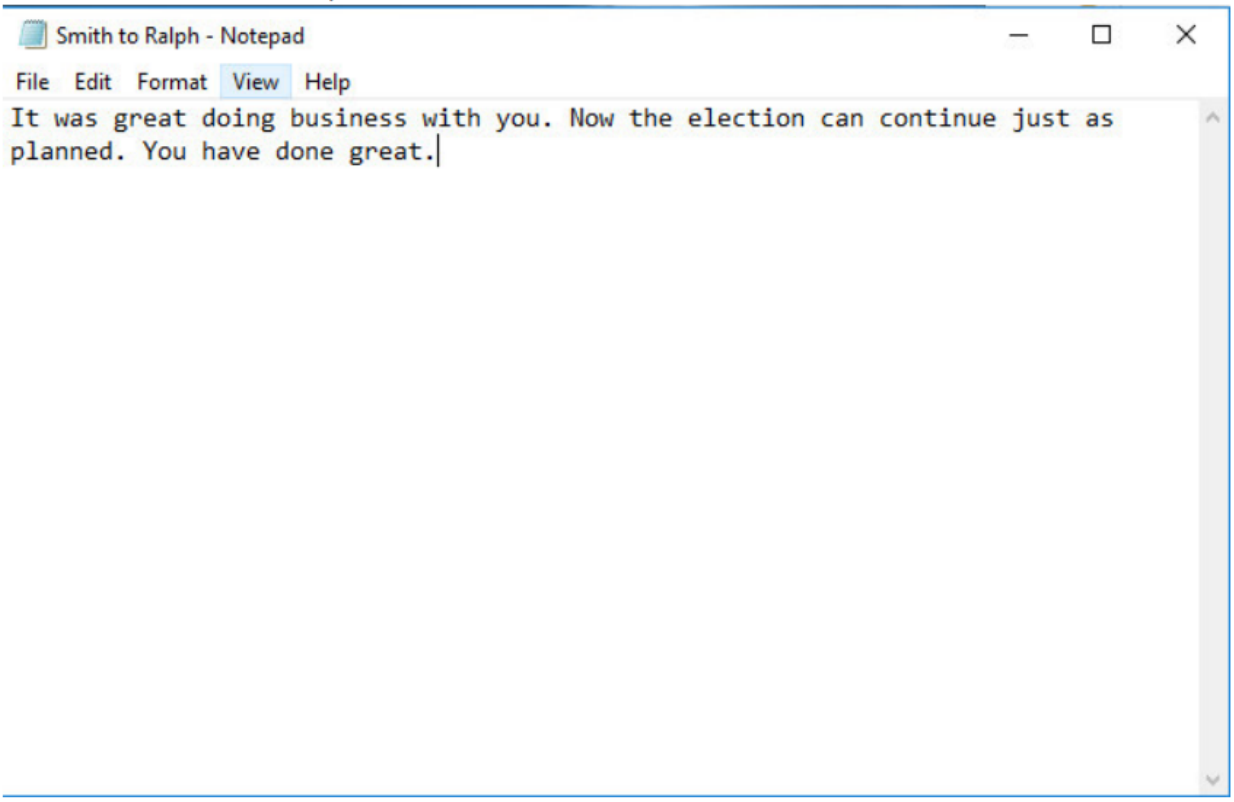
- Once the emails were discovered, further investigation occurred, including on deleted files.
- Two text files were recovered that had been deleted.

Case Identifier: Case CYSE407
Case Investigator: John Doe
Identity of the Submitter: Dave Green
Date of Receipt: 12/10/17

- Text file 1 was referred to as “Objective Complete.txt” and contained the following:



- Text file 2 was referred to as Smith to Ralph and contained the following:



- No further files related to Red Ralph were found.

Case Identifier: Case CYSE407
Case Investigator: John Doe
Identity of the Submitter: Dave Green
Date of Receipt: 12/10/17

Conclusion

- Upon conclusion of the report no original media was damaged, manipulated, or changed in any way and returned to its original state. Please refer to the attached chain of custody as needed.
- Hardware used:
    - Desktop Workstation
    - SIM Card Reader
    - USB 3.0 Write Blocker
    - USB to USB connector
- Software used:
    - Windows Notepad
    - AccessData FTK Imager
    - Oxygen Forensics
    - Windows Command Line
- Evidence Includes:
    - Text conversation between Red Ralph and Official A
    - Contact data for Red Ralph on Official A's phone
    - Email conversation between Red Ralph and Official A
    - Two text files deleted by Official A containing related information pertaining to Red Ralph