# CYSE 407 Final Case Scenario

**Antonio Shields**

**School of Cybersecurity, Old Dominion University**

**CYSE 407: Digital Forensics**

**Prof. Bryan Bechard**

**December 8, 2023**

Case Identifier: 120723

Case Investigator: Antonio Shields

Identity of Submitter: Antonio Shields

Date of Receipt: 11/28/2023

## Items for Examination:

- Cellular Device
    - Model Name: Samsung S23
    - Model Number: SM-S911U
    - Serial Number: TMNT804S19A
    - Model Color: Graphite

- Personal Laptop Computer
    - Model Name: HP Envy Laptop 17T
    - Model Number: HP 17T-CW000
    - Serial Number: CND7613245890
    - Model Color: Silver

## 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.
    - Acquire tools for the examination of the mobile device and laptop:
        - SIM Card Reader
        - USB-C Data Cable
        - MOBILedit Forensics Pro (Mobile Phone Extraction Software/SIM Card Extraction)
        - Tableau Standalone Forensic Imager
        - Autopsy Digital Forensic Software
    - Once the tools were acquired and the search warrant was retrieved, the examination began.
        - When the cell phone was acquired, it was still on, but locked, so the first step is to get into the locked phone. This can be achieved by bypassing the cell phone's SIM pin. Using a SIM Card Reader and being very careful with the card to maintain integrity, the MOBILedit Forensic Pro Software is used. MOBILedit uses an integrated SIM cloning tool feature that can remove the requirement of a PIN for the original SIM card. It can also clone the SIM card to minimize actively working on original evidence. MOBILedit is also capable of connecting directly to most phones and using

advanced technology to bypass security measures. Both the SIM card pin bypass method and the direct connection were attempted. Once the pin was bypassed successfully and access to the phone was attained, the data was retrieved, making sure to gather information such as contact lists, text messages, incoming and outgoing calls, emails, application download history, and internet search history. This included all current items found and any deletion information as well, because there may have been an attempt to erase evidence before confiscation.

- Using the MOBILedit SIM card pin bypass and direct phone connection methods to unlock the cell phone, a text message from a contact named “Red Ralph” was extracted from the phone confirming a lunch meeting on February 15, 2016. MOBILedit allowed me to further investigate and analyze other message exchanges stored on the phone, SIM card, and retrieved deleted messages. MOBILedit Pro’s cloud forensics capabilities were used to access the phone’s cloud storage to retrieve any data stored there as well. From the compiled data retrieved and analyzed, the text messages’ header information was revealed.

- MOBILedit Pro can perform both physical extractions and logical extractions. Since logical extractions take the least amount of time and the least invasive, logical extraction was performed on the cell phone.

- After all of the data was retrieved from the cell phone, using MOBILedit Pro, with the capability of extracting the retrieved data, the data was placed on an external hard drive to complete the extraction process from the official’s actual cell phone device and to complete further analysis on the extracted data. In analyzing the text messages, another message was discovered:

- Documented Message:
    - Date: February 14, 2016
    - Phone Number +7 (922) 555-1543
    - Contact Name: Red Ralph
    - Message: “Let’s meet at Chili’s on Main Street for lunch tomorrow at 12:00pm.” This message was sent by Senator Smith to the contact listed above.

Case Identifier: 120723

Case Investigator: Antonio Shields

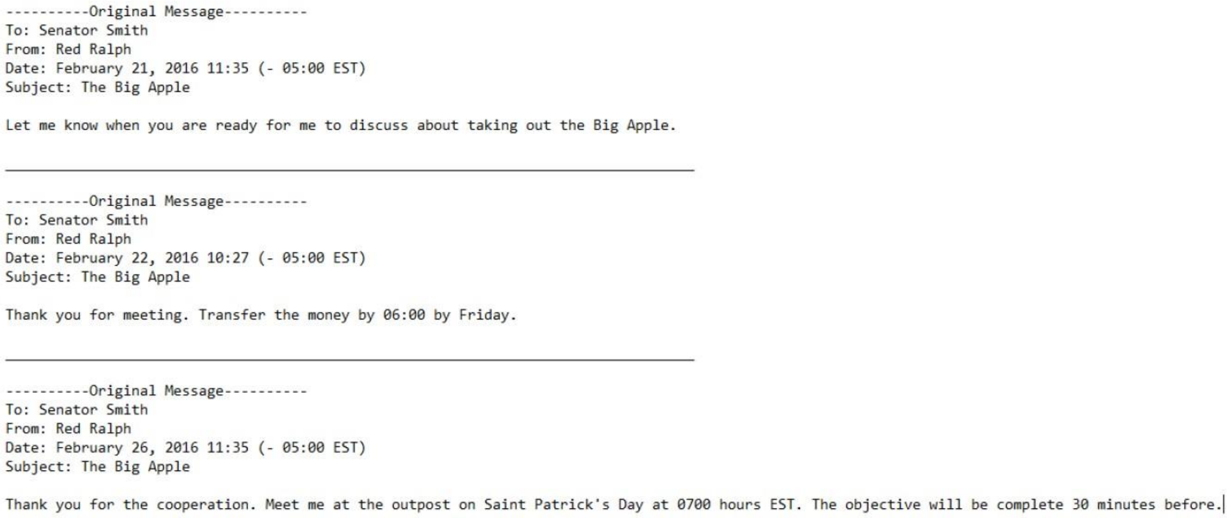
Identity of Submitter: Antonio Shields

Date of Receipt: 11/28/2023

- Personal Computer:
  - On today's date, I began the forensic acquisition/imaging process of the personal computer of Senator Smith, where there were several communications about meetings and payment for "consulting services" between Senator Smith and RedRalph@gmail.com. There were also several deleted zip files of classified material that web logs showed were uploaded to a file-sharing site.

    It is not clear, however, if those files were downloaded by anyone. The contents contained in the messages discussed meeting locations, dates, and times, in addition to monetary agreements and identity concealment.

  - After connecting the original media in the laptop to the hardware write-blocker via USB 3.0, which keeps the original hard drive protected from getting overwritten or modified, then to my examination machine, the imaging process began. The Tableau forensic imager was used to create a copy of the laptop's hard drive so that analysis is conducted on the copy and not the original. The Tableau Forensic Imager is a standalone image copier that copies evidence hard drives and does so without tying up computer resources, like RAM or space.
  - Once the imaging was copied, Autopsy forensic software was used to analyze the laptop's data and show proof of email information between Senator Smith and Red Ralph.
  - Once the image's analysis had been completed and documented, the emails, images, financial transaction history, and internet browsing history were logged and stored on the investigation laptop in the evidence case file. Below are the email exchanges between Senator Smith and Red Ralph:



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

Case Identifier: 120723

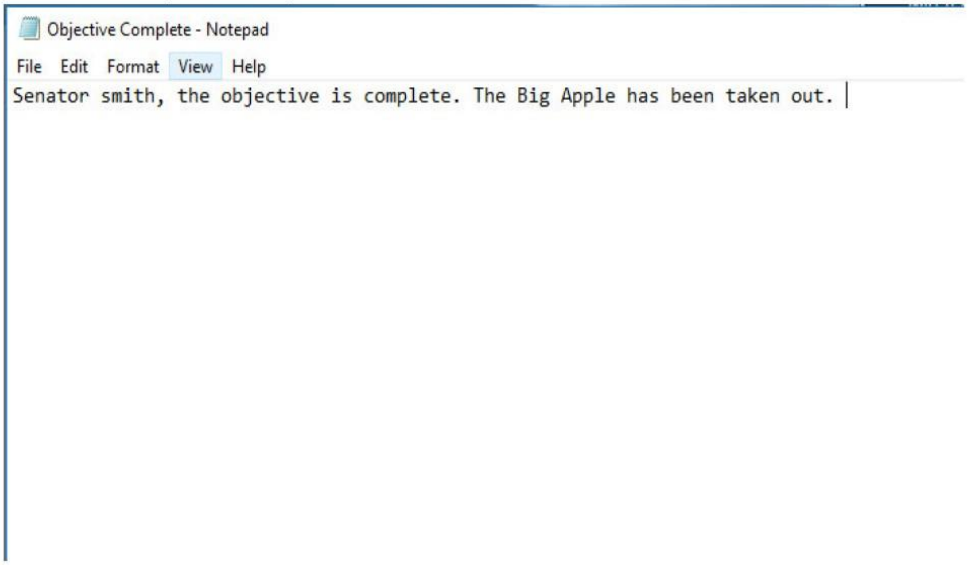
Case Investigator: Antonio Shields

Identity of Submitter: Antonio Shields

Date of Receipt: 11/28/2023

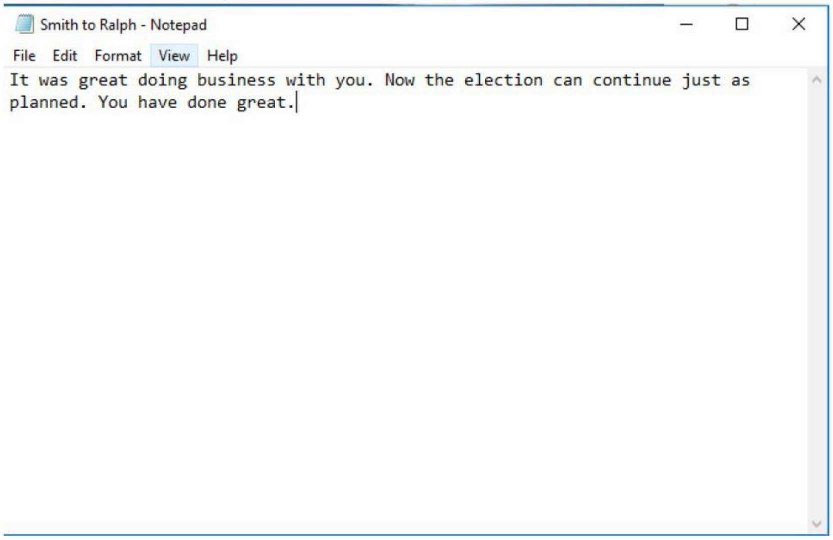
- Once the email was analyzed and documented, previously deleted files like emails, word documents, internet browser history, and any other files containing pertinent information throughout the laptop were also retrieved, analyzed, and documented. Below are retrieved messages that were marked for deletion, but were not overwritten that show two-way communication between Senator Smith and Red Ralph involving "The Big Apple" being taken out:

- File named "Objective Complete"



Senator smith, the objective is complete. The Big Apple has been taken out.

- File named "Smith to Ralph"



It was great doing business with you. Now the election can continue just as planned. You have done great.

Case Identifier: 120723

Case Investigator: Antonio Shields

Identity of Submitter: Antonio Shields

Date of Receipt: 11/28/2023

## Conclusion:

- In conclusion to the report, no original media of the evidential devices was damaged, manipulated, or changed in any way throughout the digital forensics investigation and analysis.
- Hardware that was used to recover files:
  - UltraKit v5 + TD4 Forensic Imager: https://digitalintelligence.com/store/products/w3834?taxon_id=22#contents
  - FRED L Forensic Laptop https://digitalintelligence.com/store/products/fred-l-forensic-laptop-f4140?taxon_id=18
  - Thermaltake BlacX Duet 2.5”/3.5” SATA I/II/III USB 3.0 External Hard Drive Enclosure Docking Station ST0014U-D,Black https://www.amazon.com/Thermaltake-External-Enclosure-Docking-ST0014U-D/dp/B01J4XNLN6/ref=pd_bxgy_d_sccl_2/133-5316145-0015210?pd_rd_w=QleoM&content-id=amzn1.sym.839d7715-b862-4989-8f65-c6f9502d15f9&pf_rd_p=839d7715-b862-4989-8f65-c6f9502d15f9&pf_rd_r=3N54GK5JR7YQ489N81QG&pd_rd_wg=rD7Sj&pd_rd_r=a740bd36-7325-4196-90b7-22d2d411aaed&pd_rd_i=B01J4XNLN6&th=1
  - USB CAC Smart Card Reader, CAC/DOD Military, SDHC/SDXC/SD & Micro SD Card Reader for SIM and MMC RS & 4.0, Compatible with Windows, Linux/Unix, MacOS X https://www.amazon.com/Reader-Military-Compatible-Windows-RT-SCR10/dp/B08QCH8JBM/ref=sr_1_6?crid=2PZ2IGKRRMLQK&keywords=sim%2Bcard%2Breader&qid=1702037834&sprefix=sim%2Bcard%2Breader%2Caps%2C84&sr=8-6&th=1
  - Western Digital 5TB My Passport Portable External Hard Drive with backup software and password protection, Black - WDBPKJ0050BBK-WESN https://www.amazon.com/gp/product/B07VP5X239/ref=ox_sc_act_title_1?smid=ATVPDKIKX0DER&tag=p00935-20&ascsubtag=06tUfVhDSH3mOS6wWv9JTK9&th=1

- Software that was used to recover files:
  - MOBILedit Forensics Pro https://www.mobiledit.com/online-store/forensic-mobiledit
  - Autopsy https://www.sleuthkit.org/autopsy/

- Evidence includes:
  - Text message conversations between Senator Smith and Red Ralph
  - Email correspondences between Senator Smith and Red Ralph
  - Internet Browser Search History

- Windows Registry and Log Files
- File Metadata Information
- Deleted, hidden, and encrypted files
- Bank statements from two separate banks and accounts showing all financial transactions that occurred