OLD DOMINION UNIVERSITY

CYSE 407 DIGITAL FORENSICS

Final Paper

Joy Diggs

00491693

Case Identifier: 245823

Case Investigator: Joy Diggs

Identity of Submitter: Joy Diggs

Date of Receipt: 06/22/2021

Items for Examination:

- Mobile Device
    - Model Name: Apple iPhone 11 Pro Max
    - Model Number: MXHVZLL/A
    - Serial Number: J9TK1X7ZB40D
    - Model Color: Space Grey
- Personal Laptop Computer
    - Model Name: Apple MacBook Pro 16-inch with Retinal Display
    - Model Number: A2251
    - Serial Number: R68R511MVN3Q
    - Model Color: Space Grey

Findings and Report (Forensic Analysis):

- Mobile Device
    - On today's date, I was granted a search warrant through the US District Courts in District of Columbia.
    - Acquire forensic tools to execute the investigation
        - SIMCon (SIM Card Reader)
        - ENCase Forensic Software
        - Oxygen Forensic Suite (Logical Extraction)
    - When the tools and warrant acquired, the forensic investigation can begin.
        - Although, the phone was powered on it was locked and needed a pin to gain access to the phone. By using SIMCon, I was able to gain entry by getting the phone's pin code to access the home screen. Once I was in the phone, I was able to take the steps to investigate the data, locate any deleted messages, emails, call log, downloaded applications, and pictures. I could also attain downloaded

materials, internet search history along with deleted history, and the phone contacts.

- With SIMCon I was able to trace a message that was sent to one of the contacts in the phone by the name of "Red Ralph" from February 15, 2021 confirming a lunch meeting. I was able to analyze the files of the sent, received, and deleted messages from the sim card that was in the phone. Because the mobile device was an Apple iPhone, once I gained entry into the device, I was also able to gain access to the account holders iCloud user information and all the devices previous locations that were recorded for the life of the device.
- I used hashing to store and transfer all data from the phone including but not limited to contact list, messages, GPS locations and more to an external hard drive connected to my workstation used only for this investigation. I was able to trace the location and destination of the messages with that application.
- Using Oxygen Forensics Suite to perform a logical extraction I was able to obtain the files from the official's device without altering or damaging the original evidence.
- Message obtained to "Red Ralph":
    - Phone Number: 202-952-8471
    - Contact Name: "Red Ralph"
    - Message: "Lets meet for lunch tomorrow at 12:30 pm." This message was sent by the suspect to the list contact above.

- Personal Computer
    - On today's date, I started a forensic acquisition of the suspects laptop where several email communications about meeting and payment for "consulting services" that occurred between the suspect's email address and RedRalph@gmail.com. The email messages contained meeting times, along with money agreements and confidentiality of identification.
    - Before I started to look for the evidence, I used ENCase imaging software with built in write blocker to make a disk-to-image copy to not alter the original media as I did my investigations. By doing this and validating the evidence with hashes I was able to prove that the communications between the two suspects occurred through email.

Case Identifier: 245823

Case Investigator: Joy Diggs

Identity of Submitter: Joy Diggs

Date of Receipt: 06/22/2021

- Once I acquired email, history of financial transactions, and documented the images that I needed for this case I secured the original hard and the copy I made in our secured evidence locker and tagged them with the case number.
- The messages recovered from the email exchanges that I recovered from the suspects laptop can be find below:

---- Original Message -----
To: Senator Smith
From: Red Ralph (RedRalph@gmail.com)
Date: February 19, 2021 9:14:23 AM
Subject: Consulting Services

Per our lunch meeting on Feb. 15, I am ready to talk about operation twilight and what it is that you need done.

----- Original Message -----
To: Red Ralph (RedRalph@gmail.com)
From: Senator Smith
Date: February 19, 2021 10:08:58 AM
Subject: Consulting Services

Yes, your help on this would be greatly appreciated and I can compensate you for your help. I need my opposition to disappear so I can put this election to bed.

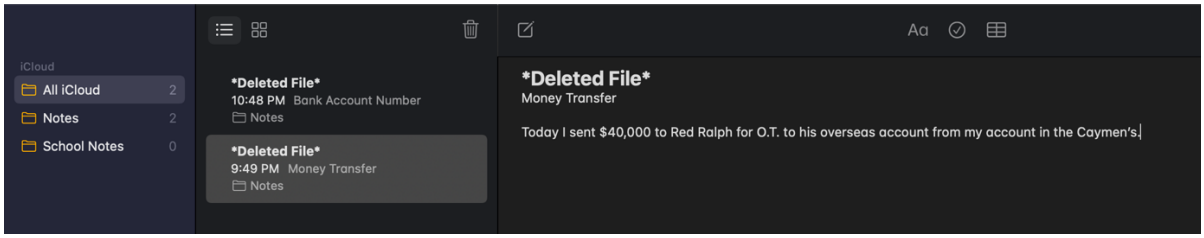
---- Original Message ------
To: Senator Smith
From: Red Ralph (RedRalph@gmail.com)
Date: February 21, 2021 12:00:00 PM
Subject: Consulting Services

I received the materials from the drop, Operation Twilight has commenced.

----- Original Message -----
To: Senator Smith
From: Red Ralph (RedRalph@gmail.com)
Date: February 24, 2021 11:20:35 AM
Subject: Consulting Services

Operation Twilight was a success, wire the money to the account by 3pm on Wednesday. Nice doing business with your Senator.

- After I was able to recover the emails, I find some deleted files that were uploaded to the user's iCloud. It contained two deleted files.
- Deleted File Name: Money Transfer



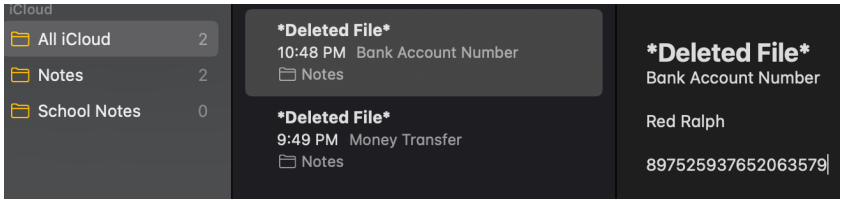
Case Identifier: 245823

Case Investigator: Joy Diggs

Identity of Submitter: Joy Diggs

Date of Receipt: 06/22/2021

- Deleted File Name: Bank Account Number



Conclusion:

- In conclusion to the report, no data, files, or images were altered as a result of my investigation of the suspects devices.
- It is in my opinion that I have found the evidence that I was task to found.
- Evidence includes:
  - Text messages between the two parties
  - Emails sent between the two parties
  - Internet search history
  - Deleted, hidden, and encrypted files
  - Financial transactions