

Case Identifier: 23-0014

Case Investigator: Clarence V. Kimbrell Jr.

Identity of the Submitter: Clarence V. Kimbrell Jr.

Date of Receipt: 4/27/2023

Items for Examination:

- Cellular Device
 - Serial Number: F18W5L21JG7C
 - Apple
 - iPhone 13
- Personal Laptop Computer
 - Serial Number: 45KHJ346KV9D
 - Dell
 - Inspiron 15 3000 Series

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 mobile device:

- SIM card reader
- Oxygen Forensics Detective (Digital Mobile Forensic Software)

Once the tools were acquired and the search warrant was obtained, the examination began. Because the device was still on and locked, the first step I took was to document the phone's current state, as there may be changes to the phone later on. The second step is to take this phone to a forensic workstation, which will allow us to extract information from it. The third step is to bypass the lock screen, which can be done with multiple methods. Lastly, we need to create a copy of the phone's storage, including things such as deleted files and hidden data.

- Using the SIM card reader, I found Senator Smith's phone numbers, contacts, call history, and text messages. We can track the users active on this memory card that stores this information. By discovering the above-listed data, we can pinpoint which cellular device this belongs to.
- Each phone number and text message can be found in the extraction of data from the phone storage or the SIM card within the phone. This is important because it can provide us with leads.

Case Identifier: 23-0014

Case Investigator: Clarence V. Kimbrell Jr.

Identity of the Submitter: Clarence V. Kimbrell Jr.

Date of Receipt: 4/27/2023

- I took action by using Oxygen Forensics and EnCase to connect the iPhone to the computer to start the process of taking an exact copy of the storage. This will allow us to search for information without altering the physical device in question. During the examination, I performed various string searches and graphics image searches using Oxygen Forensics to uncover any relevant information. In addition, I used EnCase to recover erased files and examine their contents. Once that is achieved, we can use Oxygen Forensics to bypass the lock screen by exploiting vulnerabilities in the operating system. Finally, we can search through the iPhone storage to look at calls, text messages, emails, and social media activity. If there is any information of value, it will be extensively documented.
- Documented Message
Phone Number: +7 (922) 555-1543
Contact Name: Red Ralph
Message: "I have scheduled a lunch meeting on 2/15/16 at Pete's Diner. Meet me there to discuss this information further."
- Personal Computer

On today's date, I initiated the forensic acquisition/imaging process of the laptop's storage to search for email communications regarding meetings and possible payments for "consulting services" between the official and RedRalph@gmail.com. I identified several applications and files that appeared relevant to the investigation and extracted them for analysis using specialized forensic software tools such as Oxygen Forensics.

After connecting the original media in the laptop to the hardware write-blocker via USB 3.0 on my examination machine, I commenced the imaging process. The write blocker was utilized to ensure that the original media was not modified during the imaging process. Upon completion of the imaging process, a verification process was conducted to ensure the acquired data's integrity. This was to ascertain that they were identical and that no data had been lost or modified during the imaging process. The imaging process was thoroughly documented to guarantee that all steps taken were recorded for future reference.

CYSE 407 Final

Case Identifier: 23-0014

Case Investigator: Clarence V. Kimbrell Jr.

Identity of the Submitter: Clarence V. Kimbrell Jr.

Date of Receipt: 4/27/2023

- Once the imaging was completed and documented, I used Internet Evidence to search for any evidence of Internet activity on the imaged device. This can be used to recover internet-related information such as browsing history, cookies, and cached web content. With this information, we can create a possible timeline for the alleged conversations between Senator Smith and Red Ralph. Additionally, we found cookies stored on discussion forum websites discussing the popularity of Senator Smith and his potential revival.

-----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.]

Finally, during the analysis and documentation of the email, I was able to view previously deleted files, including information on future meeting dates, locations, payments, and conversation details. This can provide crucial insights into the relationship between the two individuals. While we cannot jump to conclusions at this point, the evidence suggests that it may be related to the upcoming Senator election in New York, based on the locations of Pete's Diner and the timeframe. Thus far, the evidence indicates a possible case of election fraud, given the surge in the popularity of Senator Smith.

CYSE 407 Final

Case Identifier: 23-0014

Case Investigator: Clarence V. Kimbrell Jr.

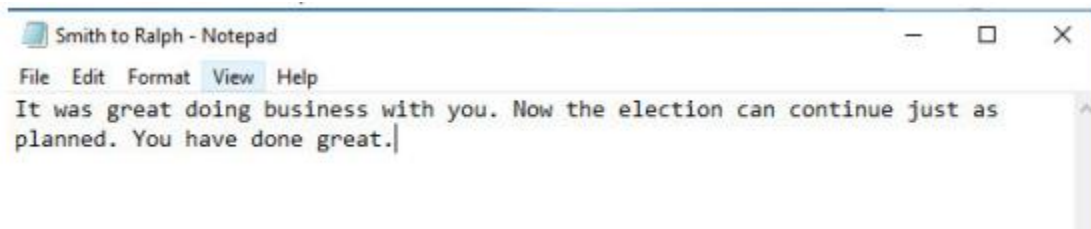
Identity of the Submitter: Clarence V. Kimbrell Jr.

Date of Receipt: 4/27/2023

- A file named “Objective Complete” was recovered that was previously deleted using Oxygen Forensics. Presumably, Red Ralph sent an email saying the objective was complete. Stating that their campaign to change public opinion has been successfully launched.



- File named “Smith to Ralph” Implying that the fake bot accounts and propaganda worked in destroying the reputation of his opponent. Now Senator Smith can win his reelection.



Case Identifier: 23-0014

Case Investigator: Clarence V. Kimbrell Jr.

Identity of the Submitter: Clarence V. Kimbrell Jr.

Date of Receipt: 4/27/2023

Conclusion:

In conclusion, no original media was damaged, manipulated, or changed in any way. Please refer to the detailed documentation of the imaging and analysis processes. All actions were conducted according to forensic standards for handling digital assets and recovery to ensure the integrity and authenticity of the acquired data. During the examination, we were able to find evidence of contact between the suspect and "Red Ralph" for criminal purposes. We used forensic tools such as Oxygen Forensics and EnCase to analyze the iPhone storage and laptop to recover deleted data. The evidence was documented diligently to support our finding on election fraud.

- Hardware that was used to recover the files:
 - Write-blocker
 - Forensic Duplicators (Imaging)
 - USB 3.0
 - Hard Drive Adapters
 - Data recovery devices

- Software that was used to recover files
 - Oxygen Forensics
 - EnCase

- Evidence includes
 - SIM card from Senator Smith's iPhone
 - An email conversation between Senator Smith and a contact named Red Ralph
 - Web browser cookies
 - Text messages