

Case Identifier: 457984

Case Investigator: Quintin Sumpter

Identity of the submitter: Quintin Sumpter

Date of receipt: 03/27/2022

Items for Examination:

- Cellular Device
 - Model Name: iPhone 11
 - Model Number: MWKK2LL/A
 - Serial number: A7SRW9QXS09M
 - Model color: Red
 - Acquire tools for mobile examination:
 - Oxygen Forensic Detective
 - SIMCon (SIM card reader)
 - Once the tools were acquired and the search warrant was retrieved, the examination began.
 - Because the phone was still on and locked, the first step I took was to disconnect it from the network and disable all network connections, including Wi-Fi, hotspot, GPS, etc. I then activate airplane mode to protect the integrity of the evidence. I then put the phone in a faraday bag because a phone can be unknowingly connected to incendiary devices. They also can be attached to booby traps that can injure or murder someone at the crime scene.
 - Using SIMCon, I was able to trace the message sent to the contact “Red Ralph” on February 15th, 2022 confirming a lunch meeting. I was able to analyze the contents of sent, received, and deleted messages from the sim card in the cellphone. Gaining access to the cloud-based system allowed me access to all of the user’s information. The location and destination of these text messages were also traced by the use of this application.
 - A hashing technique was used to store and transfer all contacts and messages from the phone to an external hard drive on my laptop which I used to store much of the evidence from the devices.
 - I used Oxygen Forensic Detective because it is an all-in-one forensic software platform built to extract, decode, and analyze data from multiple digital sources. It can also find and extract a vast range of artifacts, system files as well as credentials from Windows, macOS, and Linux machines. It can also bypass screen locks, locate passwords to encrypted backups, extract and parse data from secure applications and uncover deleted data.

Case Identifier: 457984

Case Investigator: Quintin Sumpter

Identity of the submitter: Quintin Sumpter

Date of receipt: 03/27/2022

- Documented message:
 - ❖ Phone number: +8 (696) 420-6006
 - ❖ Contact name: Red Ralph
 - ❖ Message:

“Is the lunch meeting still on for noon on 02/15/2022?” This message was sent by the official to the contact listed above.
- Personal computer:
 - Model Name: HP Laptop 17Z-ca000
 - Model Number: 57C7865E-73F2-4314-BDA2-022A7926C78D
 - Serial number: 00325-81097-03801-AAOEM
 - Model color: Black
 - On 03/15/2022, I began the forensic acquisition /imaging process of the information stored on the laptop.
 - Image processing starts by acquiring an unprocessed picture, something that must be done before anything else. It does not matter what device was used because all we need is a camera. The image acquisition is where we establish the parameters of the input. The goal is to create a source of input that works within certain defined and measurable parameters that make it easier to replicate an experiment.
 - After connecting the original media in the laptop to the hardware write-blocker via USB 3.0 to my examination machine, I began the imaging process.
 - The write-block prevents Windows or other operating systems from making changes to the drive. If a drive is connected to a system without a write-blocker and changes were written to the drive, the drive is contaminated. Searches or investigations cannot be conducted on a suspect's original media. A forensic copy of the original evidence is analyzed so the original suspect's media is not contaminated.
 - Once the imaging had been completed and was then documented, I used internet evidence to find data posted on a Web site by the suspect and data posted on a Web site by others with the suspect's consent. Down below is evidence of Red Ralph and Senator John's communication:

-----Original Message-----

To: Senator John

From: Red Ralph

Date: February 01, 2022, 10:25 (- 05:00 EST)

Subject: Star Wars

Case Identifier: 457984

Case Investigator: Quintin Sumpter

Identity of the submitter: Quintin Sumpter

Date of receipt: 03/27/2022

Tell me when you are ready to watch Star Wars.

-----Original Message-----

To: Senator John

From: Red Ralph

Date: February 02, 2022, 12:45 (- 05:00 EST)

Subject: Star Wars

Thank you for meeting with me today. You should be receiving the money by 9:00 on Monday.

-----Original Message-----

To: Senator John

From: Red Ralph

Date: February 7, 2022, 3:00 (- 05:00 EST)

Subject: Star Wars

Thank you for your cooperation. Meet me at Towne Square on Valentine's Day at 1400 hours EST. The project will be completed an hour prior.

- Once the email was analyzed and documented, I was also able to view previously deleted files. Previous versions of files and folders on Windows are automatically saved as part of a restore point. Previous versions are sometimes referred to as shadow copies. A disk drill can also be downloaded and installed to help recover the deleted files.

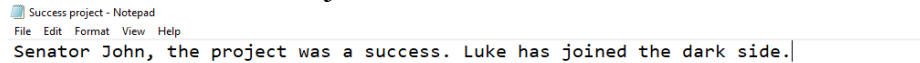
Case Identifier: 457984

Case Investigator: Quintin Sumpter

Identity of the submitter: Quintin Sumpter

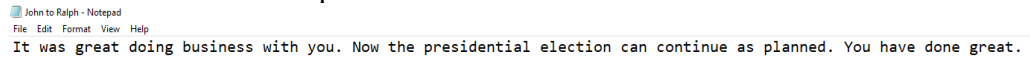
Date of receipt: 03/27/2022

○ File named “Success Project”



Success project - Notepad
File Edit Format View Help
Senator John, the project was a success. Luke has joined the dark side.

○ File named “John to Ralph”



John to Ralph - Notepad
File Edit Format View Help
It was great doing business with you. Now the presidential election can continue as planned. You have done great.

Conclusion:

- In conclusion to the report, no original media was damaged, manipulated, or changed in any way.
Refer to the:

Case Identifier: 457984

Case Investigator: Quintin Sumpter

Identity of the submitter: Quintin Sumpter

Date of receipt: 03/27/2022

Findings and report summary. I was able to safely extract and decode information found on both devices that senator John had kept. If you look under files, you will find images of certain emails and messages. This process took a couple of weeks, but everything was secured safely without any hiccups in the process.

- Hardware that was used to recover files:
 - Tableau Forensic T35u IDE/SATA Kit - <https://www.forensiccomputers.com/forensic-hardware/tableau-t35u-bridge-kit.html>
 - TX1 Ultimate Kit - <https://www.forensiccomputers.com/forensic-hardware/tx1-ultimate-kit.html>
 - Tableau T3iu Forensic SATA Imaging Bay - <https://www.forensiccomputers.com/forensic-hardware/t3iu-forensic-sata-imaging-bay.html>
- Software that was used to recover files:
 - E3:DS software
 - Oxygen Forensic Detective
 - Software Write-blocker
- Evidence includes:
 - Text messages between the two parties
 - An email conversation between a user named Red Ralph
 - Deleted, hidden, and encrypted files
 - Financial transactions