

Case Identifier: 4511

Case Investigator: Bob Dylan (US government official)

Identity of the Submitter: Niko Florido

Date of Receipt: 04/28/25

Items for Examination:

- Cellular Device
 - Name: Bob's iPhone 15
 - iOS Version: 18.4.1
 - Model Name: iPhone15
 - Model Number: CUW73CGD0
 - Serial Number: JE85CYW0JC8N
 - Personal Laptop Computer
 - Name: MacBook Pro
 - macOS Version: Sequoia 15.4.1
 - Chip: Apple M4
 - Memory: 16 GB
 - Model Number: JCU53HW90
 - Serial number: HBT49MYR5V
-

Findings and Report (Forensic Analysis):

- Cellular Device:
 - On April 28, 2025, I obtained a search warrant from the US District Courts in Eastern Virginia.
 - Acquired Tools for Examination
 - SIM card reader
 - Forensic Imaging using FTK Imager Hash values (MD5/SHA-256)
 - Preservation:
 - Device was sealed in an evidence bag at the scene on 22 April 2025, timestamp 17:45
 - The first step I took was to analyze the condition of the device for any marks, ticks, scratches, fingerprints, etc. This is important to gather any information about the case

- The iPhone 15 had a battery status of 30%

Case Identifier: 4511

Case Investigator: Bob Dylan (US government official)

Identity of the Submitter: Niko Florido

Date of Receipt: 04/28/25

- The Internet Service Provider (ISP) is T-Mobile. This is usually a visual indicator of which carrier they are connected to, whether through cellular data or Wi-Fi. This display identifies which network the phone is using
- The phone was initially locked. It requires either a passcode or biometric authentication (facial recognition)
- I was notified once a warrant was approved by the Eastern District Court of Virginia on 23 April 2025.
- Device was retrieved from evidence storage on 24 April 2025 for examination.
- Acquisition:
 - I removed the SIM card from the iPhone 15
 - I made a replica image of the SIM card. This is standard procedure when examining digital forensics. The original SIM card was retained in storage.
 - SIM image analysis recovered contact data, stored messages, and session logs.
 - I placed the image into a SIM card reader to gather the user's information such as contact list, and stored text messages.
- Documented Message:
 - Contact Name: Red Ralph
 - Phone Number: +7 (239) 123-7484
 - Date: April 15, 2025
 - To: Bob Dylan, from: Red Ralph
 - Message: "There will be a meeting at the location. Wear the grey coat. Leave the envelope at the bus terminal locker 12 by 19:00"

Case Identifier: 4511

Case Investigator: Bob Dylan (US government official)

Identity of the Submitter: Niko Florido

Date of Receipt: 04/28/25

- Personal Computer:
 - Device Status:
 - Powered off and plugged into a charger at 100% battery
 - Single user account (Bob).
 - Required passcode to access.
 - Preservation:
 - On April 13, 2025, at the home of Bob Dylan, I disabled the laptop device from Wi-Fi and transported it to Norfolk Police Department
 - I stored the evidence in the proper locked locker.
 - On April 20, 2025, I obtained the search warrant to begin the digital forensics process
 - On April 28, 2025, I began the forensic imaging process of the MacBook Pro
 - Acquisition:
 - I removed the drive from the laptop
 - Connected the suspect's drive to the hardware write-blocker via USB 3.0
 - Used Forensic Toolkit (FTK) to capture the state of the device
 - Made two copied images of the drive with write blockers
 - Then created a storage folder on the target drive and placed it under C:\Work\Cases\Case4511
 - The image type selected was Raw (dd)
 - I used FTK to calculate an SHA-1 hash for the original drive to provide integrity for the investigation. This creates a digital fingerprint for the image file.
 - Once a copy of the image file had been completed, I used OSForensics to start a new case
 - I mounted the image file from C:\Work\Cases\Case4511 onto the software program
 - Indexed data targeting email, document, and text files

- Searched index for terms: "consulting", "payment", "Red Ralph".

Case Identifier: 4511

Case Investigator: Bob Dylan (US government official)

Identity of the Submitter: Niko Florido

Date of Receipt: 04/28/25

- Sample Email:
 - From: RedRalph@gmail.com
 - To: Bob Dylan
 - Date: 10 April 2025, 16:43
 - Subject: Consulting Services
 - "Final payment pending. Deliver contents as instructed. Clean your tracks."
- Recover Deleted Files:
 - Using OSForensics' deleted file scan, two documents were recovered.
- Document 1:
 - "The attached file contains the requested access keys."
- Document 2:
 - "Payment processed. Destroy this message chain."

Case Identifier: 4511

Case Investigator: Bob Dylan (US government official)

Identity of the Submitter: Niko Florido

Date of Receipt: 04/28/25

Conclusion:

The forensic investigation verified communications between Bob Dylan and a foreign contact known as Red Ralph. Evidence confirms:

- Documenting chain-of-custody
- Created images of original data
- Provided a validated hash for the image file
- SIM card reader with a USB plug.

- Software used in the investigation:
 - AccessData Forensic Toolkit (FTK)
 - OSForensics
 - Microsoft Office
 - Linux

- Evidence includes:
 - A message from red Ralph to Bob Dylan about a meeting in a location. He must wear a gray coat.
 - Emails that were sent from Bob Dylan from red Ralph.
 - Bob's computer shows a software program and receiving a form of payment while requesting that all correspondence be deleted.
 - Bob Dylan must undergo investigation regarding the hidden transactions from this Russian Official

