Digital Forensics Examination Report

Case Identifier: OP-RR-INTEL-2077

Case Investigator: Special Agent Michaela Myers – Office of the Special Prosecutor

Identity of the Submitter: Mathieu Crosby, Lead Digital Forensics Examiner

Date of Receipt: June 22, 2025

Items Submitted for Examination:

- Cellular Device
  - Device: Apple iPhone 13 Pro
  - Model No.: A2341
  - Serial No.: F2LZ35HGN72C
  - Condition: Screen-on, passcode-protected, with SIM and eSIM active
  - Submitted with original charging cable

- Personal Laptop Computer
  - Device: Apple MacBook Pro 15” (2019)
  - Model No.: A1990
  - Serial No.: C02ZV00KMD6T
  - Condition: Powered off, encrypted drive, minor exterior wear
  - Submitted with USB-C hub and charging brick

Forensic Methods and Examination Procedures:

The devices were examined forensically with the usage of credible, industry McNally-AXIOM, FTK Imager, and Cellebrite UFED. Usage of write-blockers ensured data integrity. Our team had three primary, main products to focused on: analysis of communication, recover deleted data, and recreate cloud activity.

- On the iPhone, we extracted message databases, analyzed call and text logs, contact lists, location metadata, and Bluetooth device pairing history.
- For the laptop, we conducted a full disk image scan, keyword string searches (“Ralph,” “payment,” “upload,” “classified”), and email client parsing. We carved deleted file fragments and mapped upload timestamps against system logs.

- Recovered artifacts were correlated using a cross-device timeline to reconstruct potential intent and concealment efforts.

Findings and Analysis:

1. Cellular Device (iPhone 13 Pro):

- A text message from 2/14/2025 reads: “Lunch still on tomorrow? I’ll bring the brief.”
  - Contact name: Red Ralph
  - Number: +7 922-555-1543, matching a Moscow-based VoIP service.
- Location history shows the phone in Georgetown diplomatic quarter on 2/15/2025 around 12:36 PM.
- Bluetooth logs indicate a pairing with an unknown device (MAC: 7C:1F:EE) at the same time.

2. Laptop Computer (MacBook Pro):

- Email threads between user and RedRalph@gmail.com were recovered.
  - An email on 2/12/2025 at 9:17 PM mentioned: “Materials zipped and uploaded to our usual drop. Honor system applies.”
  - A reply confirmed receipt with: “Got it. You’ll be taken care of.”
- Four deleted .zip files were recovered with filenames like “Q1StrategyNotes.zip.”
- Contents included documents labeled CONFIDENTIAL and one titled “Joint Energy Initiative Draft – Not for Distribution.”
- Files were uploaded to SendSharePro.com on 2/13/2025 at 10:43 PM.
- Access logs show a Russian VPN IP (185.88.233.91) accessed the upload link 35 minutes later.
- “CleanSweep 3.2” was installed and executed on 2/14/2025 to clear digital traces.
- Files were unencrypted and fully recovered.

Conclusion:

This investigation revealed a coordinated digital footprint leading from the government representative to "Red Ralph" and the records attest to everything discussed, evidence of meetings that were scheduled, file transfers, and attempts to cover up digital evidence. They were using a foreign VoIP phone number, there were file uploads that were deleted, as well as some cleaning software that all go to conceal the trail between red ralph and the government representative. This all suggests intent to transmit sensitive or confidential information. All the original media has been preserved, and digital forensic images are also being secured in line with federal evidence protocol. Supporting documents and logs are retained for legal proceedings.