Case Identifier: DF-2025-0417
Case Investigator: Akela Villegas, Certified Digital Forensic Examiner
Submitter: Office of the Special Prosecutor, Washington D.C.
Date of Receipt: June 22, 2025

Items Submitted for Examination

Item #1: Apple iPhone 13 Pro

• Serial Number: C39ZG01FML6M

• IMEI: 353928107345632

• OS Version: iOS 17.3

• Owner: [REDACTED – High Ranking U.S. Official]

Item #2: Dell Latitude 7430 Laptop

• Serial Number: DLT7430-87432

• Operating System: Windows 11 Pro (Build 22631)

• Processor: Intel i7-1265U, 16GB RAM

• Storage: 1TB NVMe SSD

• Owner: [REDACTED – High Ranking U.S. Official]

Examination Procedures

The following procedures were used during the forensic examination of both devices:

- Physical and logical acquisition using Cellebrite UFED and FTK Imager.
- Hashing of all data (MD5/SHA256) to verify integrity before and after analysis.
- File carving and recovery of deleted files using Autopsy and EnCase.
- Keyword searches using strings: “Red Ralph,” “consulting,” “payment,” “classified,” “Russia,” and “upload.”
- Timeline reconstruction of system activity using Windows Event Logs and browser history analysis.
- Email analysis using Outlook PST export and parsing with X1 Social Discovery.
- Text message parsing via UFED’s reporting tools.
- Web history and cache analysis including file transfer records to Dropbox, Google Drive, and Mega.nz.
- Metadata extraction from all zip files, emails, and contact entries.
- Log correlation across devices to validate timestamps and cross-reference events.

Case Identifier: DF-2025-0417
Case Investigator: Akela Villegas, Certified Digital Forensic Examiner
Submitter: Office of the Special Prosecutor, Washington D.C.
Date of Receipt: June 22, 2025

Results and Conclusions

a. Phone Findings:

- A text message dated 02/13/20XX was found in the native SMS database (sms.db) indicating a lunch meeting confirmation on 02/15/20XX.
- The text read: “Lunch still good for 2/15? Usual spot. –RR”
- The number was labeled “Red Ralph”, associated with the phone number +7 912 345 6789, a country code linked to Russia.
- Call log analysis confirmed two additional brief phone calls between the parties in the two weeks prior to the text.

b. Laptop Findings:

- Multiple emails between the official and RedRalph@gmail.com discussing payments for “consulting services.”
  - Subject lines included: “Invoice for Services,” “Strategy Session Notes,” and “Feb Consultation.”
  - Attachments included PDFs and encrypted zip files (some password protected).
- At least six deleted .zip files were recovered from unallocated space, which contained classified-looking filenames (e.g., "SCIF_notes.zip", "DefenseReview2025.zip").
  - Contents included PDFs, DOCXs, and one XLSX file with header rows referencing defense budget allocations.
- Browser history shows uploads to Mega.nz and WeTransfer within a 30-minute period on 02/14/20XX.
  - IP logs match the official's home network.
- Deleted browser history showed searches like “how to securely share large files anonymously” and “Mega.nz upload encryption explained.”

c. General Observations:

- The user account on the laptop had administrative privileges, and Windows BitLocker was enabled, though forensic tools accessed the decrypted volume via live acquisition.
- Several antiforensic behaviors were identified:
  - Use of CCleaner on 02/14/20XX to wipe temp folders and browser logs.
  - Email client’s “Sent” folder was manually deleted but recovered via PST reconstruction.
- Timeline analysis places most of the sensitive activity between 02/12/20XX and 02/15/20XX, aligning with text messages and email threads.

Case Identifier: DF-2025-0417
Case Investigator: Akela Villegas, Certified Digital Forensic Examiner
Submitter: Office of the Special Prosecutor, Washington D.C.
Date of Receipt: June 22, 2025

Conclusions

- Corroborated Contact: The official had repeated digital communication with an individual labeled “Red Ralph,” whose phone number is Russian-based, and whose email address was involved in discussions of payment.
- Suspicious Data Transfers: Classified material (confirmed by filename and metadata, full validation pending classification authority review) was compressed, deleted, and uploaded to external sites.
- Intentional Obfuscation: The use of CCleaner, encrypted zip files, and the timing of deleted browser history strongly suggest intentional data concealment.
- Chain of Custody Maintained: All digital images were hashed, verified, and preserved. All actions were logged with timestamps in accordance with forensic standards.

Based on the evidence, there is strong indication of unauthorized communication and possible dissemination of sensitive or classified information to a foreign contact. Further legal and counterintelligence review is recommended.

Submitted By:

Akela Villegas
Certified Digital Forensic Examiner

Date: June 22, 2025