Case Identifier: DF-2025-1225
Case Investigator: Emma Humphreys
Identity of the Submitter: Office of the Prosecutor
Date of Receipt: 12/01/2025

Case Overview

Items for Examination

Exhibit A- Smartphone

- Make/ Model: Apple iPhone 14 Pro
- Operating System: iOS 17.1
- Notes: Device was powered on and locked at the time of seizure

Exhibit B- Laptop

- Make/Model: Lenovo Thinkpad T14s (Gen 3)
- Operating System: Windows 10 Enterprise
- Notes: Primary workstation used by the suspect.

Forensic Examination

Upon receipt, all the items were photographed, documented and secured. Forensic images were created for applicable items using industry-standard software. All images were hashed with SHA-256 and compared to ensure exact duplication of source media.

A lawful search warrant was obtained to complete a forensic acquisition of the iPhone, SIM card and Lenovo Thinkpad device, the following steps were then taken:

Smartphone

- The device was received powered on, but locked.
- Immediately placed into a Faraday isolation enclosure to prevent any network connectivity or potential remote wipe.
- Lock screen, notifications, and visible indicators were photographed.
- The SIM card was extracted from the device using a sterile tool and imaged with a SIM card reader (SIQuest SIM Examiner).
- A raw binary SIM image was created.
- The raw image was hashed and imported to Oxygen Forensic Detective for analysis of subscriber data, SMS remnants and carrier metadata.
- Since the iPhone was powered on, a trusted extraction method was attempted.

Case Identifier: DF-2025-1225
Case Investigator: Emma Humphreys
Identity of the Submitter: Office of the Prosecutor
Date of Receipt: 12/01/2025

    - The laptop was examined for lockdown pairing records.
    - A valid pairing certificate was located, permitting a trusted advanced extraction without the device passcode.
    - The iPhone was connected to a forensic workstation running Oxygen Forensic Detective and Cellebrite UFED 4PC.
- Using Oxygen Forensics Detective:
    - There was an advanced logical extraction performed which obtained:
        - Messages (SMS/iMessage)
        - Contacts
        - Call logs
        - App data
        - Browser and location history
        - Wi-Fi and network artifacts
    - Extracted artifacts were saved into an OFD container and hashed.
- Using Oxygen's file-system access tool
    - Extracted SQLite databases, WAL files, application directories, analytics logs, and message database remnants.
    - Messages chat.db and chat.db-wal files were manually reviewed with DB Browser for SQLite to verify integrity and recover deleted fragments.
- All data containers were hashed using SHA-256 and logged in the chain-of-custody documentation.

Keyword Searches

Keyword searches were conducted for:

- "Red Ralph"
- "Ralph"
- "2/15/20xx"
- "consulting"
- "classified"
- Phone number +1-202-555-0198

Oxygen's timeline tool was used to correlate messages, calls, browser activity, and location data around the date of the alleged meeting.

Laptop

All standard forensic procedures were followed:

- Laptop drive was imaged with FTK Imager and verified via SHA-256 hashing.

Case Identifier: DF-2025-1225
Case Investigator: Emma Humphreys
Identity of the Submitter: Office of the Prosecutor
Date of Receipt: 12/01/2025

- Keyword searches were conducted for “Red Ralph”, “consulting”, “payment”, “zip”, and “classified”.
- Deleted files were recovered using EnCase and Autopsy.
- Outlook PST files were extracted and analyzed for emails and metadata.
- Browser history, network logs, and upload timestamps were reviewed.

Findings

Smartphone

- A text message thread dated February 10, 20xx shows *Red Ralph* confirming a lunch meeting schedule for February 15, 20xx.
- The contact entry for “*Red Ralph”* was stored under phone number +1-202-555-0198
- Timeline reconstruction confirmed messaging activity consistent with meeting coordination.

Laptop

- Numerous emails between the suspect and RedRalph@gmail.com referenced meetings, “consulting services”, and corresponding payments discussions.
- Browser logs show the subject accessed an anonymizing service shortly before uploading the files.
- Recovered ZIP achieves contained files suggestive of classified materials:
    - *ProjectAlpha_Restricted.docx*
    - *IntelBrief_Q1.xlsx*
    - Metadata indicates these files were deleted and then uploaded on February 16, 20xx at 11:23 AM to a third-party file-sharing site.

Conclusions

1. The suspect maintained ongoing communication with an individual identified as “Red Ralph” through both SMS and email
2. Forensic analysis revealed planning of a meeting on February 15, 20xx and discussion of “consulting services” potentially masking illicit coordination
3. Deleted files containing potentially classified materials were recovered, and evidence shows the suspect uploaded these files to an eternal file-sharing site shortly thereafter.

Case Identifier: DF-2025-1225
Case Investigator: Emma Humphreys
Identity of the Submitter: Office of the Prosecutor
Date of Receipt: 12/01/2025

4. While the upload is confirmed, there is no definitive evidence that the files were accessed by external parties.

Final Statement:
The examination uncovered substantial evidence showing communication, coordination, and handling of sensitive files inconsistent with standard government security protocols. The findings presented above were derived using valid forensic tools and procedures, and the integrity of all recovered evidence was maintained throughout the investigation.