Case Identifier: INV-2025–US-01

Case Investigator: Raneem Alarian

Identity of the Submitter: Agent William Scott, Federal Marshal's Office

Date of Receipt: 06/25/2025

---

## Items for Examination:

- ☐ Cellular Phone
  - **Serial Number:** C89F-1890A-449X
  - **Make & Model:** Apple iPhone 13 Pro Max
  - **Condition Upon Receipt:** No visible damage; phone is powered on
  - **Chain of Custody:** Received from Federal Marshal's Office on 06/25/2025
- ☐ Personal Laptop Computer
  - **Serial Number:** X1Q4-L9M7-889F
  - **Make & Model:** Dell XPS 15 9500
  - **Condition Upon Receipt:** Powered off; accessible with warrant
  - **Chain of Custody:** Logged into digital evidence locker D-113

## Forensic Analysis Findings:

- ☐ Cellular Phone

  Date of Analysis: 06/25/2025
  - Tools Used for Examination:
    - **Cellebrite Physical Analyzer**
    - **Oxygen Forensic Detective**
    - **SIM Card Reader**
  - Once my tools were acquired, my analysis began:
    - Because the device was still powered on and locked, my first action was to place it in a Faraday bag to pre-empt any incoming and outgoing signals. This safeguards against potential tampering or remote wiping. I then confirmed the chain of custody and photographed the phone's condition before initiating forensic acquisition.
    - Next, with a SIM card reader,  I pulled identifying details like the phone number, ICCID, and IMSI, and confirmed the SIM was active on a foreign carrier network—indicating potential overseas communications.
    - I extracted all the text messages and the phone numbers using Cellebrite Physical Analyzer, which facilitated full file system acquisition. I checked the integrity of the acquisition through SHA256 hashing. I continued to look for SMS and contact databases.
    - I went a step further to utilize Oxygen Forensic Detective to examine communication logs such as deleted messages, contacts, and geolocation. I was also able to build a timeline of activities on the device on the day in question with the assistance of this tool.
    - Documented Message Evidence:

Case Identifier: INV-2025–US-01

Case Investigator: Raneem Alarian

Identity of the Submitter: Agent William Scott, Federal Marshal's Office

Date of Receipt: 06/25/2025

---

    - **Phone Number:** +7 (922) 858-1483
    - **Contact Name (as listed in phone):** Red Ralph
    - **Message Date & Time:** February 15, 2025 - 12:24 PM
    - **Message Content:** "Looking forward to our lunch shortly. Same place as last time."
    - **Location Data:** The phone was located near a known Russian diplomatic residence at the time of the message
    - **Additional Activity:** There were two hours of inactivity with the device after this message, which corroborates the likelihood of a face-to-face meeting.

☐ Personal Laptop Computer:
Date of Analysis: 06/25/2025

- Tools Used for Examination:
    - **EnCase Forensic**
    - **Autopsy**
- Once my tools were acquired, my analysis began:
    - The laptop was received in a powered-off state, and I recorded its physical condition through photographs. I established a chain of custody prior to continuing.
    - I made a forensic image of the internal drive with EnCase Forensic and checked the integrity of the image by generating SHA256 hash values. The forensic image was mounted on an air-gapped forensic workstation that was write-blocked via software and hardware to prevent the image from being modified during analysis. The workstation is not connected to any external network and is accessed only by authorized forensic staff in order to preserve the integrity and security of the evidence.
    - I used Autopsy to analyze the email files and extracted existing and deleted emails. I found some email exchanges between the subject and RedRalph@gmail.com that discussed making plans for meetings and compensation for "consulting services." Some of the emails contained allusions to cryptocurrency transactions and utilized evasive references to file transfers.
    - Additionally, I restored some deleted ZIP files from unallocated disk space. These ZIP files seemed to hold sensitive data, as evidenced by file names and metadata. Browser history analysis corroborated that these ZIP files were uploaded to a file-sharing site. Although I did not find any

---

direct hint if the files were downloaded by third parties or not, upload timestamps were very close to email exchanges with Red Ralph.

## Conclusion:

- As a conclusion to this report, no original media was changed, altered, or modified in any way. All forensic acquisitions were made in accordance with standard digital evidence handling procedures. Refer to the confirmed SHA256 hash values and recorded chain of custody for each device to ascertain the integrity of all data recovered.
- **Hardware** used to recover files:
    - **Faraday bag** for cellular isolation
    - **SIM card reader**
    - Write-blocked, air-gapped **forensic workstation**
- **Software** used to recover and analyze files:
    - **Cellebrite Physical Analyzer** (mobile data extraction)
    - **Oxygen Forensic Detective** (mobile data timeline & deleted message analysis)
    - **EnCase Forensic** (disk imaging and integrity verification)
    - **Autopsy** (email recovery, deleted file analysis, browser history review)
- **Evidence includes:**
    - A text message on February 15, 2025, from the subject's iPhone to "Red Ralph" arranging a lunch meeting at which time geolocation information put the phone in proximity to a known Russian diplomatic residence and two hours of inactivity after the message.
    - SIM card examination revealed a number associated with an international carrier, which further facilitated potential foreign communication.
    - A chain of emails between the subject and RedRalph@gmail.com, recovered from the laptop, which mentioned meetings and payments for "consulting services." The emails further mentioned cryptocurrency payments and associated file transfers.
    - Erased ZIP files that were recovered from the laptop had filenames and metadata indicating they consisted of sensitive or classified data. The files were found to have been uploaded to a file-sharing site and had upload dates that corresponded closely with Red Ralph communications
- Based on the communications, confirmations of meetings, and electronic trail of transfers of sensitive information and compensation negotiations, there exists a clear and documented trail of unauthorized contact and possible criminal association between the U.S. government official and the person known as "Red Ralph."

Case Identifier: INV-2025–US-01

Case Investigator: Raneem Alarian

Identity of the Submitter: Agent William Scott, Federal Marshal's Office

Date of Receipt: 06/25/2025

---

**References**


Canny Creative. (2024, May 22). Top 10 Analytic Features Available in Oxygen Forensic® Detective. Oxygen Forensics. https://www.oxygenforensics.com/en/resources/10-analytical-features-available-in-oxygen-forensic-detective/

Carrier, B. (2019). Autopsy. Sleuthkit.org. https://www.sleuthkit.org/autopsy/

Cellebrite. (2023). *Cellebrite - Digital Intelligence For A Safer World*. Cellebrite.com. https://cellebrite.com/en/home/

National Institute of Justice. (2023, August 22). Law 101: Legal Guide for the Forensic Expert | Chain of Custody | National Institute of Justice. Nij.ojp.gov. https://nij.ojp.gov/nij-hosted-online-training-courses/law-101-legal-guide-forensic-expert/pretrial/pretrial-motions/chain-custody

*Top features of Cellebrite Physical Analyzer.* (2023, April 21). Pelorus Technologies. https://www.pelorus.in/top-features-of-cellebrite-physical-analyzer/

*Walkthrough: Oxygen Forensic Detective Latest Features - Forensic Focus.* (2018, October 5). Forensic Focus. https://www.forensicfocus.com/articles/walkthrough-oxygen-forensic-detective-latest-features/

*Wisemonkeys*. (2024). Wisemonkeys.info. https://wisemonkeys.info/blogs/Exploring-the-Power-of-Encase-Forensic-Tools-Unraveling-Digital-Mysteries

*Write a Forensic Report Step by Step.* (2022, November 7). Salvation Data Technology. https://www.salvationdata.com/work-tips/write-a-forensic-report/