Case Identifier: CASE-2003-16732

Case Investigator: Christiane Joy Galang

Identity of the submitter: Richard Smith

Date of Receipt: 2/15/2025

Items for Examination:

iPhone 16 Pro

- 128 GB
- Model Number: MYMC3LL/A
- Serial Number: HQM56HX5XV
- iOS 26.1

MacBook Air M2

- 8GB
- Serial Number: GK1JYKGVQM
- macOS Sequoia Version 15.6.1

Procedures

- U.S. official Richard Smith has been raising suspicion in and out of the office. They suspect him of contacting Russian officials.
- Judge Evan Waters issued a search warrant that allows us to collect an iPhone and a MacBook from the suspect to gather evidence for our investigation.

Softwares Used for iPhone:

- Cellebrite UFED: used for file-system extractions and analyzing messages, contacts, and call logs. It can also generate reports for the courts.
- Magnet AXIOM: data acquisition
- Autopsy: keyword search for “Red Ralph.”

Steps:

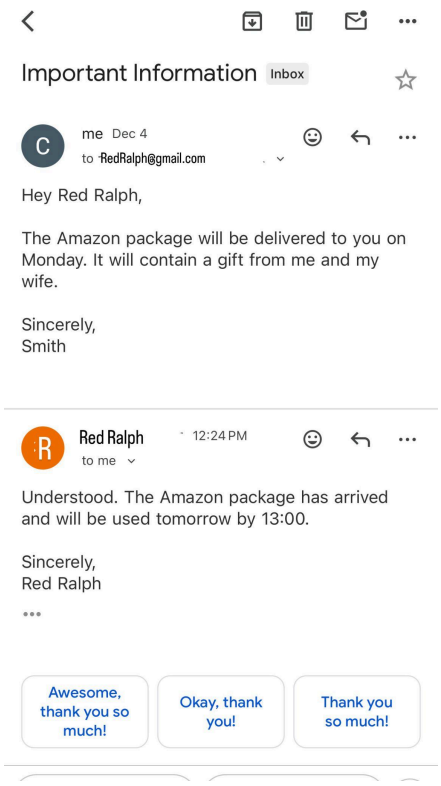
- Once the search warrant was granted, the phone and the laptop were taken to the digital forensics lab for examination.
- The phone was connected to Cellebrite UFED. We created a new case to run the extraction. We navigated to contacts to locate “Red Ralph” and noted the phone number associated with it. We then navigated to messages to find the text confirming the lunch meeting on 2/15/2025. We also checked call logs for calls to and from “Red Ralph.”
- Magnet AXIOM was used as a second tool to confirm the number and messages from “Red Ralph.”
- Autopsy is used for hash lookup and keyword search for “Red Ralph,” phone number variants, and keywords such as “lunch” and “meeting.”
- Documented evidence:
    - Phone number: +7 (997-376-4414)
    - Contact name: Red Ralph
    - Message: Meet me at the restaurant at 1900 on 2/15/2025 to further discuss this topic.

Softwares used for MacBook:

- FTK Imager

Using FTK Imager, we were able to search the MacBook's data files. We analyzed emails between Mr. Smith and Red Ralph. We also ensured that a forensic image was created to avoid altered data in the MacBook. We discovered emails between Mr. Smith and redralph@gmail.com.

Email showed:



Conclusion:

After conducting a deep investigation of these two devices, we found evidence that Richard Smith and a Russian official were in contact about serious government secrets. Using the iPhone 16 Pro and the MacBook Air 2, we were able to find a Russian phone number linked to "Red Ralph" revealing conversations about secrets. There were also Emails concerning packages

or letters sent between parties. The tools used for the investigation were Cellebrite UFED, Magnet AXIOM, Autopsy, and FTK Imager for the laptop. These tools helped confirm the interaction between Smith and “Red Ralph.”