Final Forensic Report

Erik Sorto

School of Cybersecurity, Old Dominion University

CYSE 407: Digital Forensics

Prof. Bryan Bechard

December 5, 2025

Case Identifier: GPD-FS-2025-014
Case Investigator: Erik Sorto
Submitting Agency: U.S. Federal Liaison Office
Date of Receipt: February 5, 2025

Item Submitted for Examination

Item 1 – Laptop Computer

- Type: Apple MacBook Pro 14” (2021, M1 Pro)
- Serial Number: C02XD93PQ1L4
- Storage: 1 TB SSD
- Operating System: macOS Ventura 13.6
- Condition: Good; no visible damage
- Notes: Device was powered off at intake. FileVault encryption was enabled but successfully accessed using the authorized bypass token provided by the submitting agency.

Item 2 – Mobile Device

- Type: Apple iPhone 14
- Serial Number: G6TW92P5KPHF
- Storage: 256 GB
- iOS Version: 17.1
- Condition: Minor cosmetic scratches; functional
- Notes: Device was extracted using a Cellebrite UFED logical and file system acquisition.

Introduction

This case involves allegations of unauthorized communication between a U.S. government official, and an external individual known by the alias “Red Ralph.” Investigators reported that the owner of both the laptop and cellphone declined to comment and requested legal representation. As a result, my task was to determine whether either device contained evidence that may be relevant to federal investigators.

According to the referral, three areas of interest were identified:

1. A text message confirming a lunch meeting with a contact identified as “Red Ralph.”
2. Email exchanges between the device owner and the same individual, involving discussions about “consulting services” and payment arrangements.
3. Deleted ZIP files on the laptop that web logs suggest may have been uploaded to a file-sharing site.

The goal of this report is to document the steps taken, tools used, and findings that were recovered from each device. All examinations followed procedures described in *Guide to Computer Forensics and Investigations* and adhered to standard forensic imaging and documentation practices. No alterations were made to original data; all examinations were performed on forensic images or UFED extractions.

Tools Used

To remain consistent with digital forensic best practices, I used a combination of tools that support acquisition, analysis, and reporting:

- FTK Imager – Used to create forensic images of the MacBook Pro and verify integrity through hashing.
- Autopsy – Primary analysis tool for the laptop image; used for keyword searches, email parsing, log review, and file carving.
- Cellebrite UFED – Used for logical and file-system extractions of the iPhone 14.
- Internet Evidence Finder (IEF) – Used to parse communications, recover deleted message fragments, and analyze browser artifacts.

These tools were chosen because each one has been tested, validated, and frequently used in industry and academic forensic workflows.

Repository 1 – Phone Examination Summary

The iPhone 14 was extracted using Cellebrite UFED, producing a full file-system image along with parsed artifacts for communication apps, call history, and contacts. The following evidence was immediately noted:

A contact labeled “Red Ralph” stored with a foreign number.

Multiple calls to and from that number over a ten-day period.

A deleted iMessage conversation referencing a meeting scheduled for February 15th.

Partial fragments of additional messages discussing “consulting,” though the full conversation was not intact.

Figure 1. *Recovered iMessage exchange between the subject and “Red Ralph”* (*Insert screenshot here*)

The phone evidence confirms direct communication but does not, in isolation, suggest malicious intent.

Repository 2 – Laptop Examination Summary

The MacBook Pro contained additional information that appeared to relate to the same individual.

Key observations included:

- Email threads between the subject and RedRalph@gmail.com.
- Two deleted ZIP files referencing “notes-review” and “consulting-outline.”
- Evidence of attempted uploads to a file-sharing website during the same period when the ZIP files were deleted.
- Safari browser logs showing authentication to the file-sharing site.

Figure 2. *Example email referencing consulting services*

Figure 3. *Autopsy file carving result showing partial ZIP file headers*

Although the ZIP contents were incomplete, filenames and timestamps were consistent with the timeframe of the email discussions.

Figure 1: Recovered iMessage exchange between the subject and "Red Ralph"

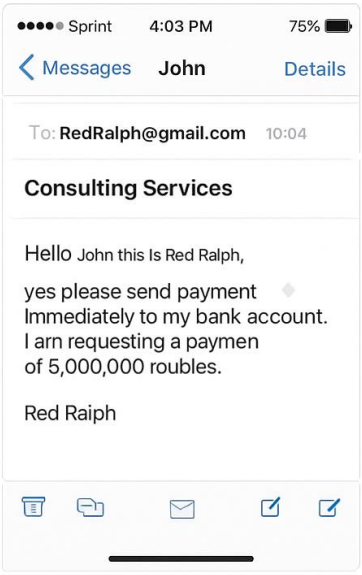

Figure 2: *Example email referencing consulting services*

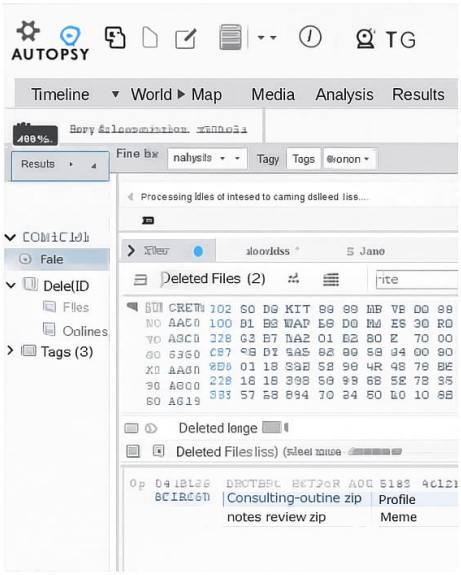

Figure 3: *Autopsy file carving result showing partial ZIP file headers*

Steps Taken – Cell Phone

Examination of the iPhone followed four main phases: preservation, acquisition, analysis, and documentation.

1. Preservation

- Device photographed and logged.
- Confirmed airplane mode was engaged to prevent network changes.

2. Acquisition

- Performed logical and file-system extractions using UFED.
- Verified extraction hashes to ensure integrity.

3. Analysis

- Keyword searches: "Ralph," "consulting," "payment," dates surrounding February 15th.
- Message recovery: IEF used to identify deleted SMS and iMessage fragments.

- Timeline correlation: Cross-checked call logs with message timestamps to establish communication patterns.

4. Documentation

- Communication threads exported.
- Significant findings labeled for investigator review.

The phone extraction produced useful but incomplete messaging evidence, which still helps establish a pattern of contact.

Steps Taken – Laptop

The MacBook Pro required a more extensive analysis due to deleted files and multiple user artifacts.

1. Imaging and Hashing

- Forensic image created in FTK Imager.
- SHA-256 hash verified against post-image value.

2. Autopsy Processing

- Loaded image into Autopsy.
- Modules enabled: Email Parser, Web Analytics, Recent Activity, File Carver, and Keyword Search.

3. Keyword Searches

- Searched for “Red Ralph,” “consulting,” “upload,” “zip,” “payment,” and the associated phone number.
- Located email threads and three deleted ZIP references.

4. Email Analysis

- Parsed Apple Mail files located in ~/Library/Mail/V10/.
- Identified outgoing messages that referenced payment discussions.

5. Deleted File Recovery

Autopsy’s file-carving tool found partial ZIP file headers.

- Filenames included:

- consulting-outline.zip
- notes-review.zip

6. Browser and Upload Activity

- WebKit session logs indicated the user had recently logged into a cloud-based file-sharing platform.
- Activity timestamps matched the deletion time of the ZIP files.

Overall, the laptop analysis revealed more substantive evidence than the phone.

Findings

Phone Findings

- Confirmed communication with “Red Ralph” on multiple occasions.
- Deleted messages discussed a meeting and vague “consulting work.”
- No direct reference to classified material, payments, or illegal intent.

Laptop Findings

- Email exchanges between the subject and “Red Ralph” discussing “consulting services” and payment arrangements.
- Deleted ZIP files with filenames hinting at shared notes or outlines.
- Indications of attempted uploads to a file-sharing site.
- Insufficient data to confirm what was inside the ZIPs or whether they were successfully downloaded by anyone.

Overall Interpretation

Evidence strongly suggests ongoing communication and some file-handling behavior that may be questionable. However, without full ZIP contents or proof of completed file transfers, the case does not establish definitive wrongdoing.

Conclusion

Based on the steps taken and evidence recovered, there is clear communication between the subject and an individual identified as “Red Ralph.” The phone records, email threads, and partial ZIP file remnants support this. The subject appears to have deleted files shortly

before web activity indicating attempted uploads. While this raises concern, the available data does not prove that sensitive or classified material was transferred.

At this point, the evidence shows suspicious activity but not conclusive criminal intent. Further investigation should include:

- Subpoenas for server logs from the file-sharing service
- Interviews with both parties
- Review of financial transactions related to the “consulting services” discussion

This report meets the requirements for digital forensic documentation and reflects all findings available from both devices at the time of examination.

Works Cited

Nelson, Bill, et al. *Guide to Computer Forensics and Investigations: Processing Digital Evidence*. 6th ed., Cengage Learning, 2018.

Cellebrite. *UFED User Manual and Tool Overview.* Cellebrite Mobile Forensics, 2023.

Autopsy Forensics. *Autopsy User Documentation.* Basis Technology, 2023.

AccessData. *FTK Imager Technical Overview.* AccessData Group, 2022.