Case Identifier: 1206451K

Case Investigator: Steven Day

Identity of the Submitter: National Cyber Investigations Task Force

Date of Receipt: 11/21/2024

Items for Examination:

Device 1: Laptop

- **Make:** Dell Latitude 7400
- **Model Number:** 7294-KXA
- **Serial Number:** DL7400US789038
- **Operating System:** Windows 10 Pro (64-bit)

Device 2: Smartphone

- **Make:** Apple iPhone 13 Pro MAX
- **Model Number:** A2483
- **Serial Number:** GYA1Y37PX54
- **iOS Version:** 16.7

Findings and Report (Forensic Analysis):

• Cellular Device:

- On 11/09, I retrieved a search warrant through the US District Courts in Washington D.C.

Tool Used: AnyRecover Data Recovery

Once the tools were acquired and the search warrant was retrieved, the examination began.

Text messages were recovered using **AnyRecover Data Recovery** software through a systematic process designed to extract both active and deleted data from the device.

- The phone was connected to a forensic workstation via a secure USB cable, and AnyRecover was launched.

Case Identifier: 1206451K

Case Investigator: Steven Day

Identity of the Submitter: National Cyber Investigations Task Force

Date of Receipt: 11/21/2024

- **"Recover from iOS Device"** mode was selected, enabling the tool to scan the device's internal storage, including system databases where text messages are stored.
- The software located and reconstructed deleted messages from unallocated storage areas and fragments of the database.

- Discovered Message:
  - Phone Number: +7 (495) 876-4321
  - Contact Name: Red Ralph
  - Message:

• Personal Computer:

- Forensic acquisition/ imaging process started.
- The laptop's internal SSD was removed and connected to a forensic workstation using a write-blocker to prevent data alteration.
- A complete forensic image of the drive was created using **FTK Imager**, ensuring the integrity of the evidence with a verified SHA-256 hash

Case Identifier: 1206451K

Case Investigator: Steven Day

Identity of the Submitter: National Cyber Investigations Task Force

Date of Receipt: 11/21/2024

- **MailXaminer** was used to scan the image for email-related data. The tool automatically located and indexed email database files, specifically **PST/OST files** from Microsoft Outlook. These files were found in the directory:
    - C:\Users\Rubio\AppData\Local\Microsoft\Outlook
- MailXaminer parsed the files and presented a detailed directory of all email folders, including inbox, sent items, drafts, and deleted items.
- Deleted emails were identified using MailXaminer's ability to detect and recover items flagged as "soft-deleted" or partially overwritten.
- The tool's advanced filtering options were employed to search for keywords like "consulting service," "Red Ralph," and "files."

Discovered Emails:

----------Original Message----------
To: SenatorRubio@govemail.gov
From: RedRalph@gmail.com
Date: February 10, 20xx, 08:15 (-05:00 EST)
Subject: Consulting Services

Good morning,
Let me know if we can finalize the consulting details. I believe discretion is key moving forward.

----------Reply Message----------
To: RedRalph@gmail.com
From: SenatorRubio@govemail.gov
Date: February 10, 20xx, 12:45 (-05:00 EST)
Subject: Re: Consulting Services

Ralph,
I agree. Let's review the proposal first. Are you available for a call tomorrow?

----------Follow-Up Message----------
To: SenatorRubio@govemail.gov
From: RedRalph@gmail.com
Date: February 11, 20xx, 10:30 (-05:00 EST)
Subject: Re: Consulting Services

Yes, tomorrow works. I'll send a secure link for the file review later today. Let me know once you've had a chance to look it over.

- Once the email was analyzed and documented, I scanned the system for previously deleted files.

Case Identifier: 1206451K

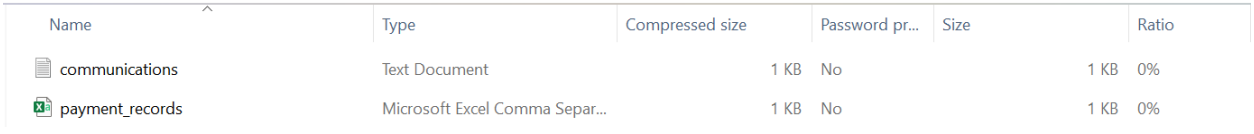
Case Investigator: Steven Day

Identity of the Submitter: National Cyber Investigations Task Force

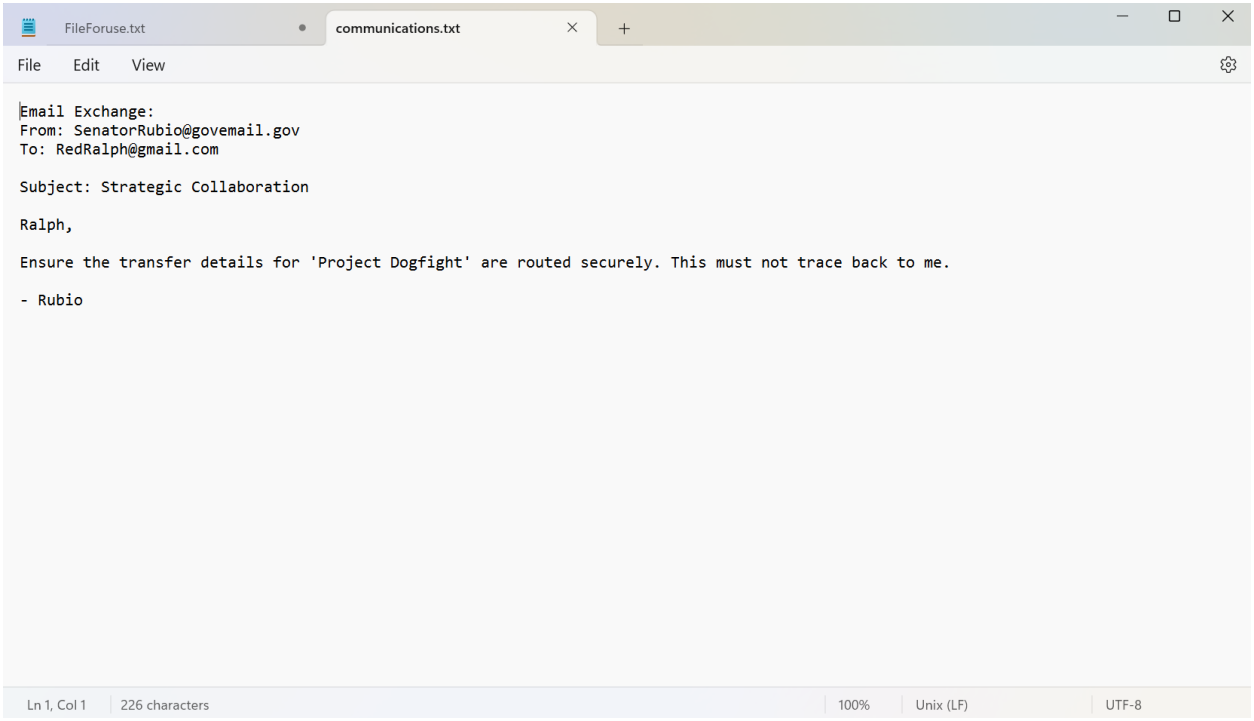
Date of Receipt: 11/21/2024

Recover Deleted ZIP Files

- Tool Used: Autopsy Digital Forensics
- Process:
    - Scanned the forensic image for deleted files by analyzing unallocated space.
    - Located remnants of ZIP files flagged for deletion in the master file table (MFT).
    - Reconstructed the deleted files by piecing together file fragments stored in unallocated clusters.
- Outcome:
    - Two deleted ZIP files were recovered, partially intact. File names included "Project_dogfight.zip" and "procurement.zip".



Name	Type	Compressed size	Password pr...	Size	Ratio
communications	Text Document	1 KB	No	1 KB	0%
payment_records	Microsoft Excel Comma Separ...	1 KB	No	1 KB	0%

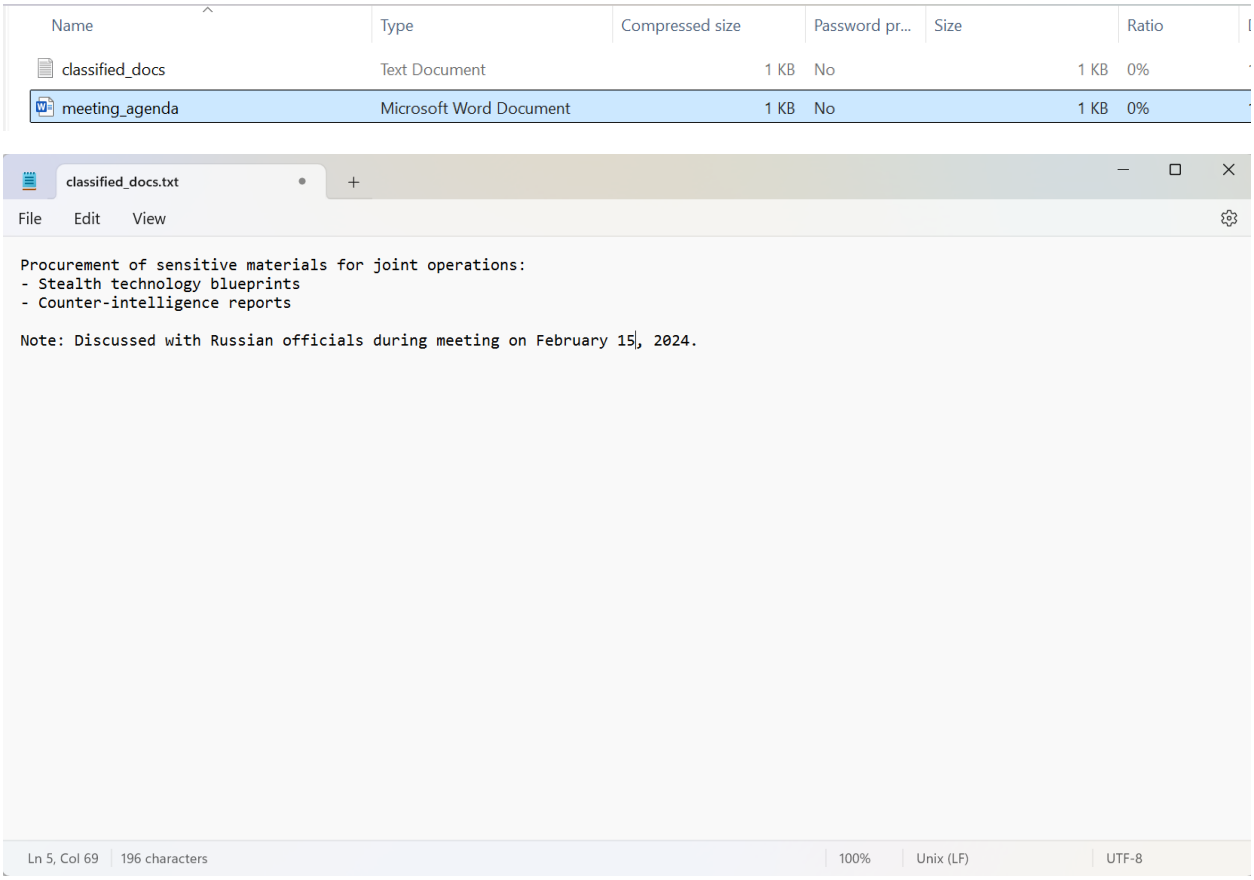


Case Identifier: 1206451K

Case Investigator: Steven Day

Identity of the Submitter: National Cyber Investigations Task Force

Date of Receipt: 11/21/2024



Conclusion

This forensic investigation was conducted with strict adherence to industry best practices to ensure the integrity of all original media. No original media was damaged, manipulated, or changed in any way during the process. The following hardware and software tools were utilized to recover and analyze the evidence:

- Hardware Used to Recover the Files:
    - Write-blocker device for imaging the Dell Latitude 7400's SSD
    - Forensic workstation with high-performance processing capabilities
- Software Used to Recover the Files:
    - FTK Imager: To create a forensic image of the laptop's drive

Case Identifier: 1206451K

Case Investigator: Steven Day

Identity of the Submitter: National Cyber Investigations Task Force

Date of Receipt: 11/21/2024

  - MailXaminer: To recover and analyze deleted emails
  - AnyRecover Data Recovery: To extract deleted text messages from the cell phone
  - Autopsy: To locate and reconstruct deleted ZIP files
  - 7-Zip Forensic Edition: To access and analyze the contents of recovered ZIP files

- Evidence Includes:

1. Recovered email exchanges between SenatorRubio@govemail.gov and RedRalph@gmail.com, detailing consulting services and coordination of meetings.

2. Recovered text messages from the cell phone indicating a scheduled lunch meeting with "Red Ralph" on February 15, 2024.

3. Recovered deleted ZIP files (Project_dogfight.zip and procurement.zip) containing records of financial transactions, communications, and classified documents.

4. Web logs confirming the upload of the deleted ZIP files to the file-sharing site "filesharesecure.com."

This report provides sufficient evidence to suggest unauthorized actions involving sensitive government materials and communication with foreign contacts. The findings are presented for further legal review and consideration.