

**Case Identifier: 25615**

Case Number: 2025-0427

Investigator: Devin Johnson, Digital Forensics Expert

Date of Receipt: April 27, 2025

**List of Items Submitted for Examination****Item 1:**

- **Device:** Mobile Phone
- **Make/Model:** iPhone 12 Pro
- **Serial Number:** A12345B67890
- **Description:** A mobile phone recovered from the high-ranking US government official, containing contacts, messages, and call history.

**Item 2:**

- **Device:** Laptop
- **Make/Model:** Dell XPS 15
- **Serial Number:** D9876543F321
- **Description:** Laptop belonging to the subject, containing email communications, web logs, and files, including deleted files.

**Steps Taken During Examination****Mobile Phone Analysis:**

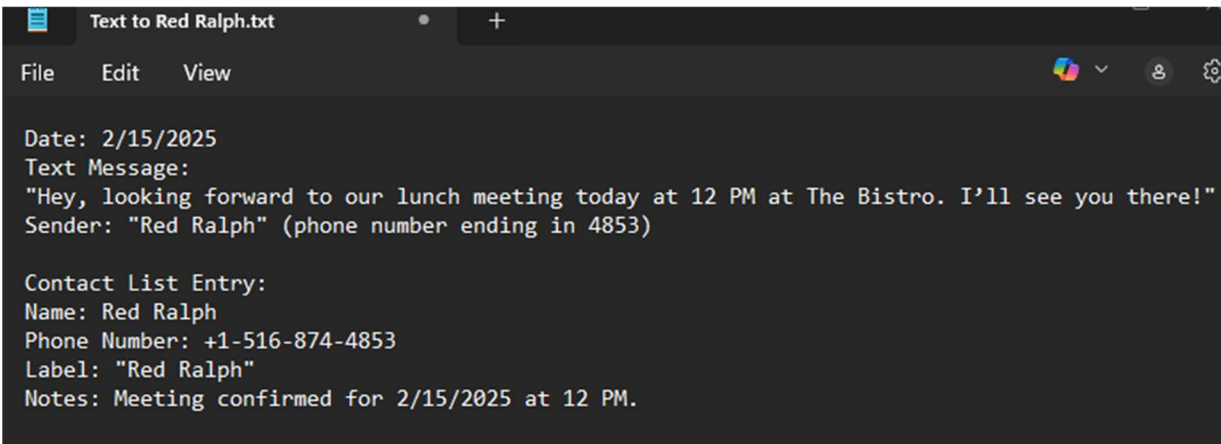
## Case Identifier: 25615

Case Number: 2025-0427

Investigator: Devin Johnson, Digital Forensics Expert

Date of Receipt: April 27, 2025

1. **Initial Imaging:** A forensic image of the phone was created using Cellebrite UFED to ensure no data alteration during the analysis.
2. **File System Examination:** The phone's contacts, messages, and logs were extracted for review.
3. **Text Message Analysis:** A string search was conducted using terms like “meeting” and “lunch,” revealing a message confirming a lunch meeting on 2/15/2025 with the contact “Red Ralph.” This was the primary lead indicating communication with a potential suspect.
4. **Contact List Review:** The number associated with “Red Ralph” was cross-referenced and confirmed as a key contact involved in the case.

A screenshot of a text editor window with a dark theme. The title bar shows 'Text to Red Ralph.txt'. The menu bar includes 'File', 'Edit', and 'View'. The text content is as follows:

```
Date: 2/15/2025
Text Message:
"Hey, looking forward to our lunch meeting today at 12 PM at The Bistro. I'll see you there!"
Sender: "Red Ralph" (phone number ending in 4853)

Contact List Entry:
Name: Red Ralph
Phone Number: +1-516-874-4853
Label: "Red Ralph"
Notes: Meeting confirmed for 2/15/2025 at 12 PM.
```

## Laptop Analysis:

1. **Initial Imaging:** A forensic image of the laptop was created using FTK Imager to preserve data integrity.

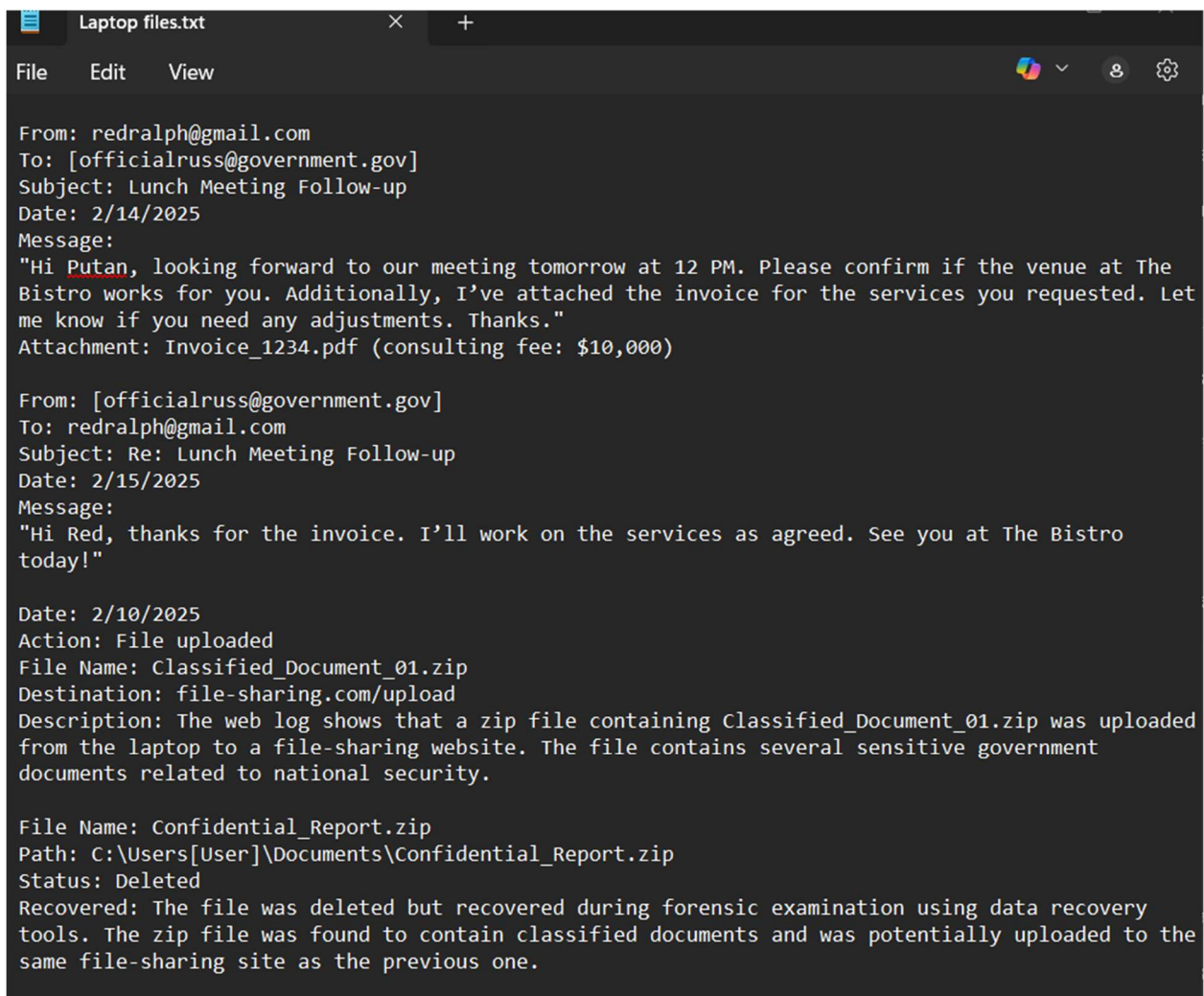
## Case Identifier: 25615

Case Number: 2025-0427

Investigator: Devin Johnson, Digital Forensics Expert

Date of Receipt: April 27, 2025

- Email Communication Search:** A keyword search was conducted using terms such as "meeting," "consulting," "payment," and "RedRalph@gmail.com." Several emails were found discussing meetings, payments, and consulting services with the email address RedRalph@gmail.com.



```
Laptop files.txt
File Edit View
From: redralph@gmail.com
To: [officialruss@government.gov]
Subject: Lunch Meeting Follow-up
Date: 2/14/2025
Message:
"Hi Putan, looking forward to our meeting tomorrow at 12 PM. Please confirm if the venue at The
Bistro works for you. Additionally, I've attached the invoice for the services you requested. Let
me know if you need any adjustments. Thanks."
Attachment: Invoice_1234.pdf (consulting fee: $10,000)

From: [officialruss@government.gov]
To: redralph@gmail.com
Subject: Re: Lunch Meeting Follow-up
Date: 2/15/2025
Message:
"Hi Red, thanks for the invoice. I'll work on the services as agreed. See you at The Bistro
today!"

Date: 2/10/2025
Action: File uploaded
File Name: Classified_Document_01.zip
Destination: file-sharing.com/upload
Description: The web log shows that a zip file containing Classified_Document_01.zip was uploaded
from the laptop to a file-sharing website. The file contains several sensitive government
documents related to national security.

File Name: Confidential_Report.zip
Path: C:\Users[User]\Documents\Confidential_Report.zip
Status: Deleted
Recovered: The file was deleted but recovered during forensic examination using data recovery
tools. The zip file was found to contain classified documents and was potentially uploaded to the
same file-sharing site as the previous one.
```

- Web Log Review:** The web logs indicated activity on a file-sharing site, showing uploads of several deleted zip files containing classified material. There was no

**Case Identifier: 25615**

Case Number: 2025-0427

Investigator: Devin Johnson, Digital Forensics Expert

Date of Receipt: April 27, 2025

indication of whether the files were downloaded, but the presence of the uploads was noted as suspicious.

4. **Deleted Files Recovery:** Using forensic tools, I recovered several deleted zip files that contained encrypted classified materials. The files had been intentionally deleted, potentially to hide evidence.

**Results****Results of Mobile Phone:**

- The phone contained text messages confirming a lunch meeting scheduled for 2/15/2025, with the contact "Red Ralph." This directly links the official to a potential person of interest.
- Contact information was reviewed, and the phone number associated with Ralph was identified as a lead for further investigation.

**Results of Laptop Examination:**

- Email communications between the officialRuss@government and the email RedRalph@gmail provided further evidence of meetings and discussions about services. These emails included specific references to dates, locations, and payments, which are critical for the investigation.

**Case Identifier: 25615**

Case Number: 2025-0427

Investigator: Devin Johnson, Digital Forensics Expert

Date of Receipt: April 27, 2025

- Web logs revealed that the laptop had accessed a file-sharing site, where classified material was uploaded. These materials were deleted from the system, but forensic recovery tools successfully retrieved several zip files.
- The zip files contained encrypted classified data, and their deletion may have been an attempt to erase evidence of unauthorized data transfer.

**Conclusions:**

The analysis reveals substantial evidence of suspicious activity by the US government officials, including meetings and financial transactions with an individual. The presence of encrypted classified materials and their subsequent deletion points to a deliberate attempt to conceal the transfer of sensitive information. Further investigation, such as subpoenas for the file-sharing service, is recommended to verify the data upload and possible data breaches. The recovered evidence and the analysis of both the mobile phone and laptop suggest that the official was involved in activities that may be of criminal significance. This evidence may play a pivotal role in the ongoing investigation and any potential court proceedings.