Case Identifier: RR2-15
Case Investigator: India Henry
Identity of the Submitter: India Henry - Forensic Expert
Date of Receipt: 12/5/2025

Abstract:

The phone of a high ranking US government official, Senator Grant, was seized and a forensics investigation on the phone found messages confirming a lunch meeting on February 15, 2025. The other individual in the text-chain went by the screen name “Red Ralph;” this name coincides with another investigation done on the lawmaker’s personal laptop, where several email chains about meetings and payment for “consulting services” occurred between the official and “Red Ralph”. The phone number recovered from the investigation into Senator Grant’s cell phone was traced back to a Russian phone. The investigation into the computer also uncovered several zip files of classified material that were uploaded to a file sharing site; although, it is unclear if the files were downloaded by anyone. The objective of this report is to provide an overview of the findings found from the actions and communications of the government official.

Items for Examination:

- Cellular Device: (iPhone 16 Pro Max; Serial Number: 9083-264-751-9032)
    - Text messages
    - Contact list
    - Call logs
    - Calendar information
- Personal Laptop: (HP Flagship 17; Serial Number: 5674-182-093-7561)
    - E-mail messages
    - Payment information
    - E-mail contacts
    - Files (stored, deleted, zipped, unzipped)

Findings and Report (Forensic Analysis):

On November 28, 2025, I retrieved a search warrant through the US District Courts in Washington D.C. The investigation began by arranging to interview the IT manager and picking up the media. During the interview with the IT manager, I filled out an evidence form which includes the information above: the case and evidence numbers, information related to evidence collection, evidence details, and image details. The media was stored in an evidence bag and transported back to the forensics facility. Before beginning the examination, I completed an evidence custody form. (Nelson et al., 2018, 41)

Before beginning to analyze the digital evidence, I acquired the following tools to perform the examination (Forensics Insider, 2025):

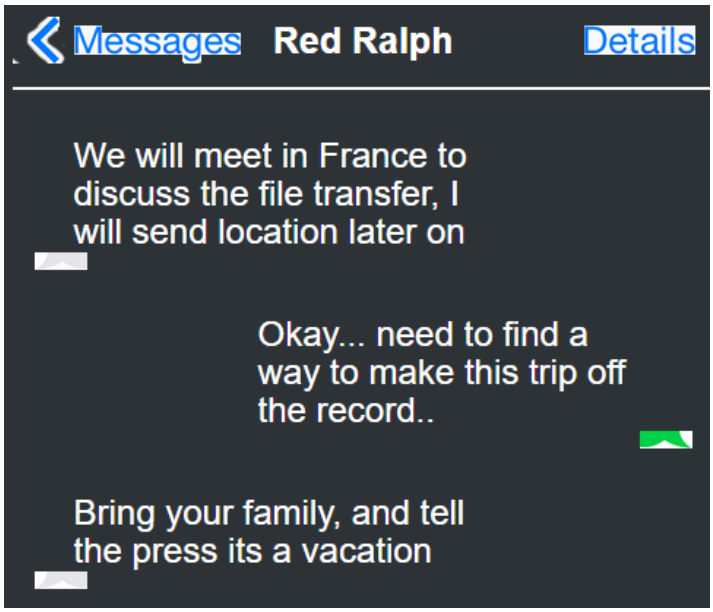
- Cellebrite UFED - used for logical and physical extractions, for recovering deleted data, decrypting passwords, and analyze acquired data
- Oxygen Forensics - excels in data carving, password recovery, cloud extraction, and timeline analysis
- MSAB XRY - decryption capabilities for gaining access to password-protected data

Case Identifier: RR2-15
Case Investigator: India Henry
Identity of the Submitter: India Henry - Forensic Expert
Date of Receipt: 12/5/2025

- SIM Card reader

After acquiring the tools, I began the examination of the cellular device. The phone was powered on, but locked. The original PIN is usually assigned to the SIM card, and the service provider can be called to get the PIN unlock key; Cellebrite UFED and MSAB XRY can both aid in password decryption. Before continuing, it is important to disable the device's password and isolate the device from the network to prevent it from gathering any information and receiving any further communication. After isolating the device, I imaged the phone's data to preserve the original evidence. Once the device has been imaged, the next step is to find the incriminating text messages via "WhatsApp," and add them to the investigation file. The number provided within WhatsApp was traced to a Russian IP address using Cellebrite UFED. The metadata from the messages provides the details, the date, and times of the message exchange. This is all potentially relevant information, so it will also be included in the results section. The text messages also revealed a plan for a lunch meeting between the official and "Red Ralph" on February 15th of this year. From there, any calendar information related to the meetings were also examined and added to the case file. While looking through the contact list, a foreign phone number was recovered attached to the name "Red Ralph", but no calls were made to the phone number. After the data acquisition, the phone was powered off and placed into a faraday bag before being secured in the evidence room of the lab.

Recovered Text Message:

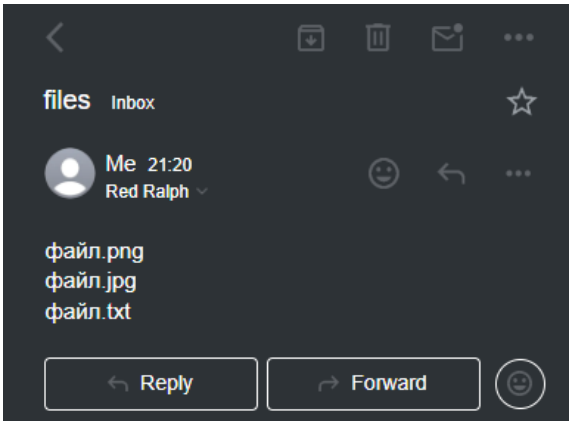


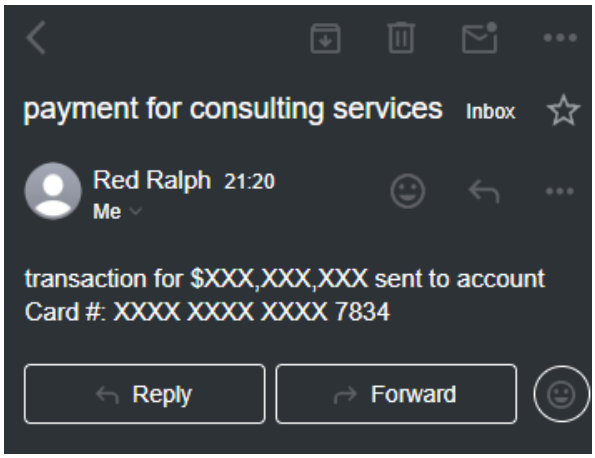
Senator Grant's personal laptop was also powered on, but had a password lock. The Senator used the same password for his laptop as he had for his phone. After gaining access to the laptop, I imaged the device to preserve the original for evidence. Once the imaging process was completed, I began to look through the emails and document any relevant information. During this process, I found there were certain emails that were seemingly deleted, so I used Oxygen Forensics data carving and time analysis tools to uncover deleted information and see

where it fits into the timeline. The deleted emails occurred between Senator Grant and “RedRalph@gmail.com”, whose name matches the contact name for the phone number recovered during the cellphone acquisition. The messages revealed communications about more meetings between the two and a receipt under the name “consulting services” was recovered. One email was a conversation where “Red Ralph” explained that the files that were talked about in their in person meetings would be shared to a website with a link under the message; the link went to a file sharing website. Another email sent from Senator Grant showed a series of files, which led to the file manager after moving that information into the case file. Similarly, there were several deleted zipped files found in the Senator’s file manager. Cellebrite UFED helped to analyze the zipped files which uncovered the information within the files, which showed US government documents. Due to jurisdiction issues, I was unable to see if anyone downloaded those files. After the examination, I put the device in a faraday bag and placed it with the phone in the evidence room.

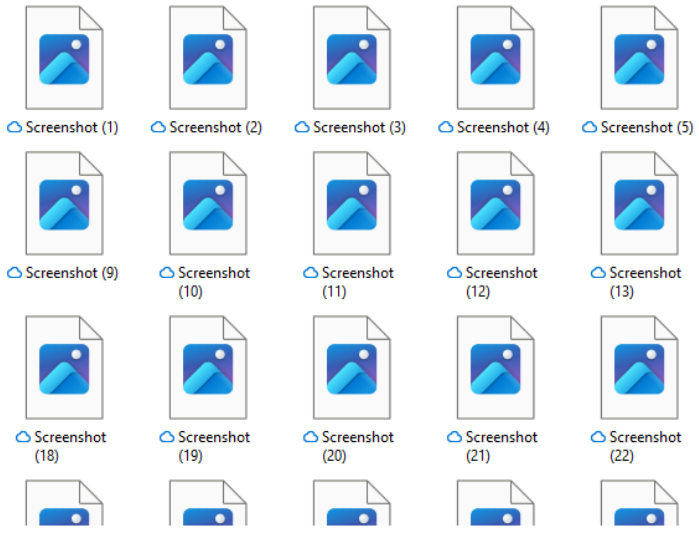
Recovered Emails:

Case Identifier: RR2-15
Case Investigator: India Henry
Identity of the Submitter: India Henry - Forensic Expert
Date of Receipt: 12/5/2025





Recovered Files:



Case Identifier: RR2-15
Case Investigator: India Henry
Identity of the Submitter: India Henry - Forensic Expert
Date of Receipt: 12/5/2025

Results:

The investigation uncovered that a sitting US Senator, Senator Grant, did have contact with an individual that went by the name of "Red Ralph". The investigation on Senator Grant's cellphone uncovered communication between the two to meet up in person. This investigation also gave access to phone numbers, contact information, and the metadata from the text exchange to help create a timeline for the investigation. The messages on the cellphone help to prove the "alleged contact" between the Senator and "Red Ralph," whose phone number is traced back to a Russian IP address, did occur.

The email messages uncovered a broad chain of events. The emails contained several communications about meetings between Senator Grant and "Red Ralph", most of these communication chains were similar to the text messages, they talked about in person meetings the two planned to have. One of the emails shows a series of files being sent from Senator Grant to the "Red Riot" email address. Another of the emails showed a receipt titled "consulting services" which shows a transaction between Senator Grant and "Red Ralph," given the prior email, it can be inferred that Senator Grant received money from the Russian officials for the documents that were later deleted from his personal laptop. While the email exchange revealed that Senator Grant was aware that those files were going to be uploaded onto a file sharing site, due to jurisdiction issues, it is unclear whether or not the files have been downloaded by anyone.

References

Forensics Insider. (2025, September 22). *The 5 Best Mobile Forensics Tools: Unveiling the Power of Digital Investigation*. Forensics Insider. https://www.forensicsinsider.com/digital-forensics/best-mobile-forensics-tools/

Nelson, B., Phillips, A., & Steuart, C. (2018). *Guide to Computer Forensics and Investigations*. Cengage Learning.