CYSE 407 Final

Hans Peterson

School of Cybersecurity, Old Dominion University

CYSE 407: Digital Forensics

Professor Bryan Bechard

December 5, 2025

Case Identifier: CI 20-0345

Case Investigator: Hans Peterson

Identity of Submitter: Hans Petereson

Date of Receipt: 11/25/2025

Devices Under Examination:

Cellular Device (Smart Phone), belonging to Senator Smith

- Make: Samsung
- Model: Galaxy S22
- Serial Number: BAF3245899

Laptop, belonging to Senator Smith

- Make: Acer
- Model: Aspire Intel
- Serial Number: TOL3345879

Findings & Report for Cellular Device:

Cellular Device (Samsung Galaxy S22, SN: BAF3245899)

1. On 11/20/2025, I received a search warrant through the US District Courts of Washington D.C.
2. Tools acquired for examining the Samsung Galaxy S22 cellular device:
    a. Sirchie SIM Card Reader
    b. Cellebrite UFED 4PC
    c. Autopsy

Case Identifier: CI 20-0345
Case Investigator: Hans Peterson
Identity of Submitter: Hans Petereson
Date of Receipt: 11/25/2025

3. Once I retrieved the cellular device, I wore gloves and took pictures of the device, noted the time and date in which I received the device and the case it belonged to. I then prepared a mobile forensics workstation for data extraction.
4. Considering the cellular device was powered but locked, I removed the device's SIM card and inserted the card into the Sirchie SIM Card Reader, which was connected to a workstation laptop.
5. I powered on Cellebrite UFED 4PC and created a new case and inputted the following information for case information: case identifier (CI 20-0345), case investigator (my name), and device information (make and model).
6. I clicked the SIM card extraction option, clicked another option for extracting a standard SIM card, and cloned the SIM card to minimize damage to the original data. Afterwards, I restarted the process and chose to make a logical extraction (Full File System Extraction) of the cellular device to get a forensic image for examination on Autopsy.
7. I closed Cellebrite UFED 4PC, started Autopsy, created a new case, and entered case information (case identifier of "RedRalph 20-0345", base directory, examiner information). As a data source, I selected the cellular device's cloned forensic image for examination. Under configure ingest, I chose the "Select All" option to gather as much data as possible. Under the "Keyword Search" option, I checked "Phone Numbers" and "Email Addresses."
8. After confirming the configured ingest screen, the image was added to the database for examination. I used Autopsy's keyword (string) search tool to identify information

Case Identifier: CI 20-0345
Case Investigator: Hans Peterson
Identity of Submitter: Hans Petereson
Date of Receipt: 11/25/2025

pertaining to the alleged Russian Official known as “Red Ralph.” My keyword search input included the following strings: Red Ralph, RedRalph, Red, Ralph, RR.

Results

9. After hitting the “search” tab and highlighting the data source as the target, several relevant results within the “listing” tab appeared.
    a. A contact labeled as “Red Ralph” with the phone number of (495) 823-12-15.
    b. An email address of RedRalph@gmail.com
    c. Several text messages. One in particular, from Senator Smith to “Red Ralph” was sent on 2/15/2025 with the following message:
        i. Meet at the Tysons CC near D.C. for a lunch meeting. Informal wear. About time we talk in person.

Case Identifier: CI 20-0345
Case Investigator: Hans Peterson
Identity of Submitter: Hans Petereson
Date of Receipt: 11/25/2025

Findings & Report for Laptop:

Laptop (Acer Aspire Intel, SN: TOL3345879)

1. Tools acquired for examining the Acer Aspire Intel laptop:
    a. Tableau Forensic Write Blocker
    b. FTK Imager
    c. Autopsy
2. After safely examining the data from the cellular device, I packed the cellular device into an evidence bag and stored it into an evidence locker. Afterwards, I prepared my workstation to receive the laptop.
3. I plugged the Tableau Forensic Write Blocker to prevent data overwriting. I then replaced my gloves and took photos of Senator Smith's laptop in the same manner I photographed his cellular device. I labeled it appropriately to the case it was assigned to.
4. With a screwdriver, I unscrewed the bottom panel of the laptop, extracted the internal hard drive, and connected it to the Tableau Forensic Write Blocker, then created an image of the hard drive using FTK Imager to prevent alterations to the original hard drive.
5. With Autopsy and the current case ("RedRalph 20-0345") opened, I added another data source for examining the hard drive image. After successfully mounting the image and configuring the same ingest as the one for the cellular device, I examined the results.

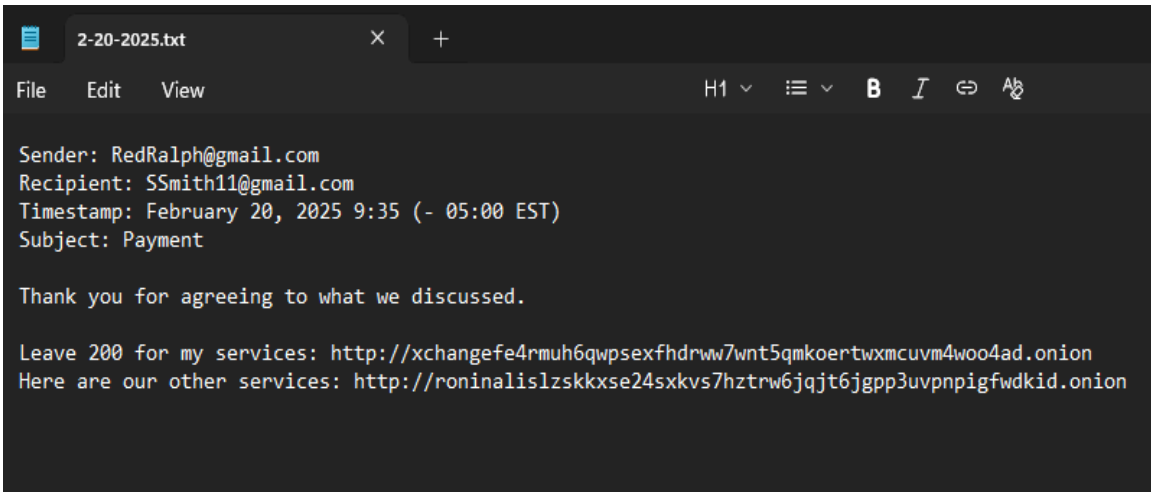
Results

Case Identifier: CI 20-0345

Case Investigator: Hans Peterson

Identity of Submitter: Hans Petereson

Date of Receipt: 11/25/2025

6. I performed another search with the following keywords: Red Ralph, RedRalph, Red, Ralph, RR. Several results appear in the “listing” tab on Autopsy.
    a. An email address of RedRalph@gmail.com.
    b. An email address of RRa34ph@mail.ru.
    c. Text file containing the number (495) 823-12-15 and “Red Ralph num.”
    d. Several notable email exchanges between Senator Smith and RedRalph@gmail.com recovered from Outlook:
        i. 

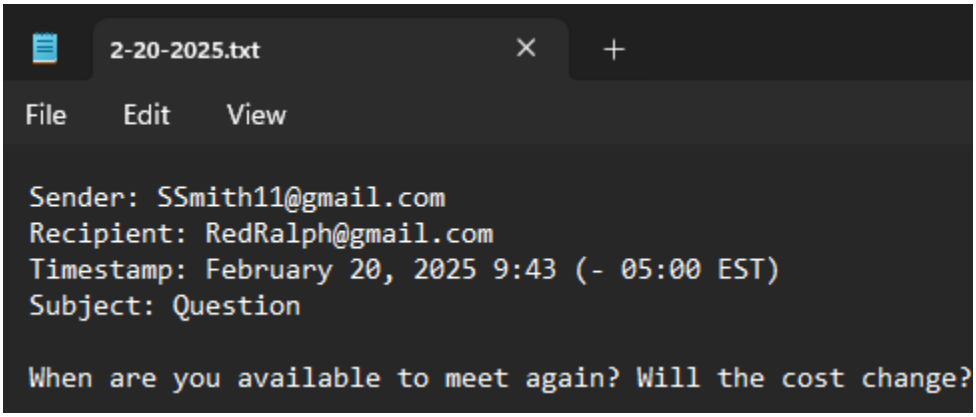
Case Identifier: CI 20-0345

Case Investigator: Hans Peterson

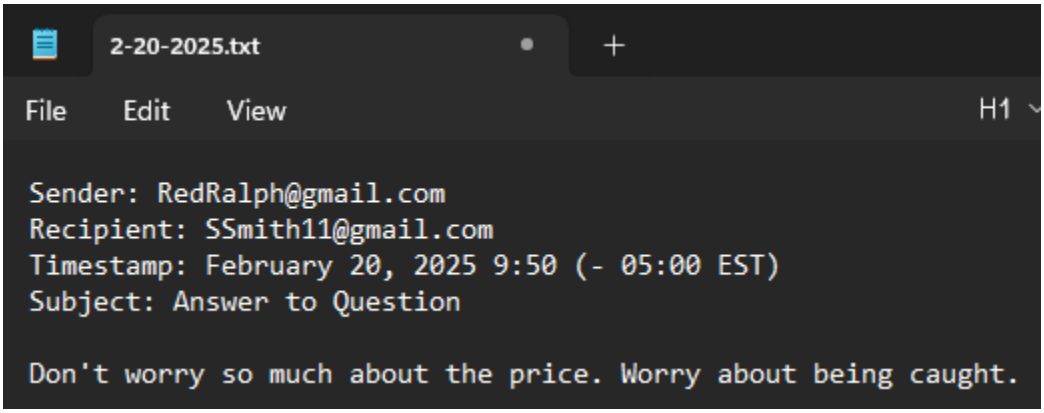
Identity of Submitter: Hans Petereson

Date of Receipt: 11/25/2025

ii.



iii.



7. Under the “Images/Videos” tab in Autopsy, there were several results linked to emails sent by “Red Ralph” to Senator Smith requesting verification on whether or not the meeting location was correct. These images consist of unique (original hashes) photographs of the Tysons Corner Center in Virginia.

Case Identifier: CI 20-0345

Case Investigator: Hans Peterson

Identity of Submitter: Hans Petereson

Date of Receipt: 11/25/2025

a. 

8. Within the “Deleted Files” section, there were several deleted but recoverable zip files. After downloading and examining them, I checked the contents of the zip files. They appear to be highly classified patents. The web history reveals that user uploading

websites, such as MEGA, were visited, and the files were uploaded. It is unclear if anyone had downloaded these classified zip files, however.

Conclusion:

1. In conclusion, there was no alteration, damage, or any form of modification to the original media in any way. All forensic examinations were conducted on copies of the original media.
2. Hardware used to recover files:
    a. Tableau Forensic Write Blocker
    b. Sirchie SIM Card Reader
3. Software used to recover files:
    a. FTK Imager
    b. Autopsy
    c. Cellebrite UFED 4PC
4. Evidence Includes:
    a. On the cellular device, email addresses and contact number of “Red Ralph”
    b. On the cellular device, sms/text messages between Senator Smith and “Red Ralph” requesting a meeting at the Tysons Corner Center in Virginia.
    c. On the laptop, a text file labeled as “Red Ralph num.”

d. On the laptop, email exchanges between Senator Smith and “Red Ralph” on the subject of a “payment.”
e. On the email exchanges, a Tor link to a Bitcoin payment processor and a Tor link to a weapons and narcotics online market.
f. On the laptop, there is a Tor browser.
g. On the laptop, images of the Tysons Corner Center (with unique hash values) attached to emails sent by “Red Ralph” to Senator Smith.
h. On the laptop, deleted zip files containing classified information pertaining to patents.
i. On the laptop, web logs that reveal that MEGA, a user uploading website, was visited, and the now deleted zip files were uploaded onto the website.

5. Summary:

The evidence suggests that Senator Smith and a “Red Ralph” have or had a partnership that involved “Red Ralph” offering “services” in exchange for Senator Smith offering financial payment. However, it is highly likely that “Red Ralph” is a Russian official, or of Russian descent, as their email address (mail.ru) is from a Russian email service. “Red Ralph’s” phone number of (495) 823-12-15 has an area code designated for Moscow, Russia, and the formatting is different from U.S. formatting.

The evidence also suggests that Senator Smith and “Red Ralph” met in person at the Tysons Corner Center, considering “Red Ralph” verified the location they were to

meet at. An email from Senator Smith to “Red Ralph” sent on February 20, 2025 also requests another date for a meeting.

The evidence also suggests that Senator Smith knowingly participated in illicit activities. In the email exchanges, “Red Ralph” revealed two Tor links to Senator Smith. The first Tor link, which requested “200” from Senator Smith, led to a Bitcoin exchange/processor website. Essentially, it is payment through cryptocurrency. The second Tor link, which was “Red Ralph’s” offer to Senator Smith for other services, led to a black market specializing in weapons and narcotics trading. It is unclear if Senator Smith visited these Tor links. However, the laptop has the Tor browser installed. Additionally, the classified zip files were uploaded onto a MEGA link; it is unclear if any user had downloaded these zip files. It is possible, though, that Senator Smith uploaded these classified zip files as an alternate method of payment for “Red Ralph’s” services.