Case Identifier: 1267060

Case Investigator: Angelica Grace Castro

Identity of the Submitter: Angelica Grace Castro

Date of Receipt: 12/05/2025

Items for Examination:

- Cellular Device:
  - Model: Iphone 11
  - Model Number: A2172
  - Serial Number: F2LZQ9N9N70Y
- Personal Laptop Computer:
  - Model: Dell Latitude 5520
  - Model Number: LAT5520-CTO-P123
  - Serial Number: HF3L29X7C0B1

Findings and Report (Forensic Analysis):

- Cellular Device:
  - On today's date, I retrieved a search warrant through the U.S. District Courts in Washington D.C.
  - Acquire tools for examination of mobile device:
    - SIM card reader
    - Oxygen Forensics Detective (Digital Mobile Forensic Software)
  - Once the tools were acquired and the search warrant was retrieved, the examination began.
    - Because the device was still on and locked, the first step I took is to plug in the charger to maintain power and placed the device on airplane mode to ensure data is not modified due to cloud synchronization. The next

Case Identifier: 1267060

Case Investigator: Angelica Grace Castro

Identity of the Submitter: Angelica Grace Castro

Date of Receipt: 12/05/2025

step was to take note of any visible notifications on the phone's lock screen. Only the notification sender was visible which was Gmail.

- The next step is to place the SIM card into the SIM card reader which was connected to the forensic workstation via USB. Afterwards, the Oxygen Forensics Detective software is launched and UICC acquisition option is chosen. Finally, the card reader and the location for the extracted data is selected and then, the data is extracted.
- Next, with the case home screen opened, I clicked on the search tool under the Analytics tab, typed the keyword "Russia", and selected all text data in the advanced settings which yielded no results. Afterwards, I used the keyword "+7" and selected phone numbers on the advanced setting which yielded one result, a text message from a contact with the name "Red Ralph".
- Documented message:
    - Phone Number: +7 (922) 555-1543
    - Contact Name: Red Ralph
    - Message:
        - "Lunch at the Big Bear Café on 1st St. will still be at 11:30 AM on 2/15/2025. Table will be at the usual spot."

- Personal Laptop Computer:
    - On today's date, I began the forensic acquisition/imaging process of the personal laptop computer Dell Latitude 5520. The first step to conduct a static acquisition by creating a disk-to-image file is the removal of the SSD. Next, the device's SSD was attached to a write-blocker connected to the forensic workstation.
    - Once the drive was connected to the workstation, FTK Imager was launched and create a disk image was selected. After the source drive, destination, image details and hash verification were configured the image was created.
    - Next, the created image was loaded into AccessData FTK by creating a new case and selecting the image file. The next step is to verify the image by checking the hash value created by FTK Imager and the hash value in AccessData FTK.

Case Identifier: 1267060

Case Investigator: Angelica Grace Castro

Identity of the Submitter: Angelica Grace Castro

Date of Receipt: 12/05/2025

- Afterwards, the search tab was used with the keywords “Red Ralph” and “RedRalph”. Once the search is done, the resulting email messages are read under the email tab. The following email messages from Red Ralph and Senator Smith was discovered regarding meetings and payment for consulting services:

```
----------Original Message----------
To: Senator Smith
From: Red Ralph
Date: December 10, 2024 11:35 (- 05:00 EST)
Subject: Consultation Services

Are you interested in a first meeting for my consultation services?

_____

----------Original Message----------
To: Red Ralph
From: Senator Smith
Date: December 10, 2024 12:30 (- 05:00 EST)
Subject: Consultation Services

I could use some advice. Big Bear Cafe @ 11:30 AM on 01/10/2025.
Far right table next to bathrooms.

_____

----------Original Message----------
To: Senator Smith
From: Red Ralph
Date: January 11, 2024 06:44 (- 05:00 EST)
Subject: Consultation Services

It was a pleasure meeting you. Fees must be paid by January 15 no
later than 05:00 PM. Future meetings can be set up through the phone
number previously discussed.
```

- The next step is to use the evidence tree in conducting an analysis of all the file folders with the recycle bin and unallocated space folders as a priority. Upon analysis of the recycle bin, several zip files were discovered all marked with a red x indicating the file can be recovered and opened. The following files were found:

Case Identifier: 1267060

Case Investigator: Angelica Grace Castro

Identity of the Submitter: Angelica Grace Castro

Date of Receipt: 12/05/2025

- File named “Operation Bear”

Confidential

Operation Bear commences at 0600 hours location 47.07920 N, -122.58080 W on 21 April 2025.
Alpha team will approach from the North and Bravo team will approach from the West.
Extraction will commence 23 April 2025 1 hour after low tide and must be completed 1 hour prior to next low tide.

Alpha team: 20 PAX
Bravo team: 15 PAX
Equipment Needed: See equipment inventory list EIL-2025-OBB.

Review Base Plan prior to deployment of teams.
Verify Deployment Schedule matches.

Confidential

- File named “Base Security Plans”

Confidential

Base Security:

North Gate:
- Unarmed Guards: 2 8-hour shifts
- Spike Strips
- CCTV

South Gate:
- Armed Guards: 2 8-hour shifts
- Spike Strips
- CCTV

West Gate:
- No Guards
- Electronic Gate with 6 character code
- Spike Strips
- CCTV

East Gate:
- Armed Guards: 2 8-hour shifts
- Spike Strips
- CCTV

Confidential

Case Identifier: 1267060

Case Investigator: Angelica Grace Castro

Identity of the Submitter: Angelica Grace Castro

Date of Receipt: 12/05/2025

- File named “Deployment Schedule”

Confidential

Deployment Schedule 2025 (Subject to change as needed)

January 13-15: Helsinki Port
January 24-25: Port of Stockholm
February 25-28: Narvik Port
March 16-19: Copenhagen Port
April 01-03: Riga Port
April 21-23: Gdansk Port
May 05-09: Kiel Port
June 13-16: Gydnia Naval Shipyard
July 06-09: Narvik Port

Confidential

- Next, an analysis of the browser history revealed Google Drive was accessed multiple times and the URL ending in /Upload-resumable was visited always one minute prior to the deletion of the Zip files. Google Chrome Cache metadata also matches the deleted files indicating the files were uploaded to a sharing site. There is no indication that the files were downloaded by anyone.

Conclusion:

- In conclusion to the report, no original media was damaged, manipulated, or changed in anyway. A forensic analysis was completed on a mobile device and personal laptop computer to find evidence of contact between U.S. and Russian officials. Forensic analysis of the mobile device’s SIM card contents using a SIM card reader and digital mobile forensic software revealed a text message to a contact with a Russian country code listed as “Red Ralph”. The forensic analysis of the personal laptop computer’s contents through the creation of a disk-to-image file and use of a digital forensics software revealed email exchanges between Senator Smith and “Red Ralph” as well as the dissemination of classified documents. Through the investigation’s findings, it can be concluded that contact between U.S. and Russian officials have been made.
- Hardware used to recover files:
    - Samsung – T7 1 TB External USB 3.2 Gen 2 Portable SSD

Case Identifier: 1267060

Case Investigator: Angelica Grace Castro

Identity of the Submitter: Angelica Grace Castro

Date of Receipt: 12/05/2025

    - SCM Card Reader Professional Dual SIM (SIM card reader)
    - Dell Precision 7865 Tower Workstation
        - CPU: AMD Ryzen Threadripper PRO 3955 WX
        - RAM: 64 GB DDR4 ECC
        - Storage: 1 TB NVMe SSD
        - Operating System: Windows 11
    - Tableau TK8U Forensic USB 3.0 Bridge (Write-blocker)
- Software used to recover files:
    - Oxygen Forensics Detective
    - FTK Imager
    - AccessData FTK
- Evidence includes:
    - Text message from “Red Ralph” confirming a lunch meeting on 02/15/2025 with Senator Smith
    - Emails between Senator Smith and “Red Ralph” (RedRalph@gmail.com) discussing meetings and payment for consulting services
    - Deleted zip files with classified material with the filenames: “Operation Bear”, “Base Security Plans”, and “Deployment Schedule”
    - Browser history showing Google Drive visitation and uploads matching zip files metadata