Case Identifier: 2025-0620-DFR

Case Investigator: Danielle Caplinger

Submitter: Digital Forensics Office, FBI

Date of Receipt: June 20, 2025

Items for Examination:

- Cell Phone
  - iPhone 14 Pro
  - IMEI: 358721600611088
- Laptop
  - Lenovo ThinkPad, Carbon Gen 11
  - SN: PF48546T

Forensic Examination & Analysis

All chain-of-custody procedures and documentation were followed in accordance with state and federal guidelines. Devices were sealed in evidence bags and transported to my digital forensics laboratory after being removed from the official's office, as allowed by a search warrant issued on June 20,2025.

Cell Phone

Tools for cell phone digital forensics include a SIM card reader (Cellebrite Toolkit) and Oxygen Forensics Detective Software.

Examination Notes:

- The phone was locked with a numerical pin, so a forensic photograph was made of the lock screen for documentation purposes, showing a recent message notification.
- Using open-source intelligence, the birthday of the device owner's only child was used to successfully unlock the phone. Pin: 05272013
- The SIM card was removed and analyzed using a SIM card reader and Cellebrite Toolkit to recover relevant data including:
  - IMSI and ICCID identifying the carrier and region as Verizon Wireless in Washington DC, USA.
  - Call logs showing multiple text messages dating back three months with a contact name of "Red Ralph" and a phone number of +7 495-213-6897.
- Oxygen Forensic Detective was used to extract relevant artifacts including:
  - IMessage database
    - "Everything is set for next week. Same spot, 12:30pm. Back room is reserved. No watchers or no show"
  - Contact List

        - +7 495-213-6897 mapped to contact: Red Ralph
    - Calendar Events
        - "Lunch Out of Office" event on February 15, 2025
- Communications were mapped using Visual Timeline and Social Graph, found in the Oxygen toolsuite.

Laptop

Tools for laptop forensics included FTK Imaging software, a hardware write-blocker, Autopsy, Magnet AXIOM, and EnCase software suites.

Examination Notes:

- A forensic image was made of the internal SSD using FTK imager and the write-blocker.
- Hashes were calculated to ensure integrity of the device:
    - MD5: b2a1f3d0c1e89a56f8f9a2d8423f569e
    - SHA-256: 847c60c2cf6f88e43ae6de4d9b67c149a73e80e41d3a59b4acbce7f4a23a1131
- Autopsy and Magnet AXIOM were used for file system analysis to parse system logs, emails, and recover deleted accounts.
- The main email client used was Microsoft Outlook 365, signed in for the subject's official government email as well as a personal Gmail account titled govxxconsulting@gmail.com.
    - A PST archive file was extracted for forensic integrity and analysis.
- Four email threads were recovered between govxxconsulting and RedRalph@gmail.com from January 8th to February 14th, 2025.
- Subject lines:
    - Consulting Services Proposal
        - Recommendations on "geopolitical insight briefings" and "strategic guidance memos"
        - Deliverables named as documents titled: "EastEuropeSecBrief.pdf" and "SecReviewMemo.pdf"
    - Invoice Approval – February
        - Reference to a $50,000 payment
    - Cafe Reservation Confirmation
        - Reservation confirmed for Cafe Dulce in Arlington, VA for February 15th at 12:30pm.

    - Follow-Up to February, Termination
        - Requests for no further contact until another email is sent and receipt of payment for "February consulting"
- Deleted .zip files were found and recovered from unallocated space using EnCase, including:
    - NatSecurity2025.zip
    - EastEuropeBriefings.zip
- All zip files contained pdf and docx documents with headers of "Top Secret" and "Confidential" with information relating to military strategies in the Eastern European geo-zone.
- Magnet AXIOM's Web Artifacts module was used to analyze Microsoft Edge browser history.
- Web logs were analyzed showing:
    - Multiple logins to the file sharing site: Mega under the email of govxxconsulting@gmail.com
    - Uploads made within the same time frame as email threads of the deleted zip files found on the laptop.
- It is unclear whether downloads were made of the uploaded information since Mega uses end-to-end encryption, but metadata confirms the upload schedule to be consistent with email references.

Results & Conclusion

The examination of the subject's iPhone 14 Pro and Lenovo ThinkPad revealed compelling digital evidence of communication, coordination, and potential unauthorized handling of classified information between the subject and "Red Ralph," a suspected foreign contact.

Analysis of the cell phone showed the device was registered with Verizon Wireless in Washington DC, consistent with the subject's home and work geography. The phone number listed under "Red Ralph" can be mapped to Moscow, Russia based on the area code and international extension. Text messages and calendar invites, as well as Oxygen's Visual Timeline, validate the high number of communications surrounding a mid-February meeting.

Analysis of the laptop was done to reveal and recover deleted zip files as well as email threads surrounding government consulting and potentially classified information. Significant email threads tied to a personal Gmail account of govxxconsulting@gmail.com show references to

consulting services deliverables, security briefings, confirmation of the meeting mentioned on the phone, and a large sum used as payment for such services. Logins to Mega from the laptop's Microsoft Edge browser show multiple uploads of zip files before being deleted from the physical device. The information located in the deleted zip files that were uploaded to Mega contained sensitive documents related to military and security strategies in Eastern Europe.

As a whole, this digital forensics investigation provides substantial evidence regarding the unauthorized intelligence leak and communication to a foreign contact, likely tied to Russia. Calendar appointments, message records, and email threads confirm a physical meeting on February 15, 2025 at Cafe Dulce, coinciding with the upload of classified information to a third-party file sharing website.