Case Identifier: 2024-DOJ-0847

Case Investigator: Christian A. Coleman

Identity of the Submitter: Department of Justice, Criminal Division

Date of Receipt: February 28, 2024

Items for Examination:

Cellular Device

- Samsung Galaxy S22 Ultra
- Serial Number: RF8M419KTXD
- IMEI: 354808110123456
- Model: SM-G998U

Personal Laptop Computer

- Dell XPS 15 9520
- Serial Number: 7NQXK63
- Model: P109F
- Service Tag: 7NQXK63

Findings and Report (Forensic Analysis):

Cellular Device Analysis:

On February 28, 2024, I obtained a federal search warrant through the US District Court for the District of Columbia authorizing examination of the subject's mobile device. The Samsung Galaxy S22 Ultra was received in powered-on but locked state.

Acquisition Process:

- Secured device in airplane mode to prevent remote wiping
- Used Cellebrite UFED Touch2 for physical extraction

Case Identifier: 2024-DOJ-0847

Case Investigator: Christian A. Coleman

Identity of the Submitter: Department of Justice, Criminal Division

Date of Receipt: February 28, 2024

- Created bit-by-bit forensic image using write-blocking procedures
- Verified image integrity using SHA-256 hashing

Key Findings:

The examination revealed significant communications between the subject and an individual identified as "Red Ralph" in the contact database.

Critical Text Message Evidence:

Phone Number: +7 (495) 555-0147 (Russian Federation country code)

Contact Name: Red Ralph

Date/Time: February 15, 2024, 14:32 EST

Message Content: "Meeting confirmed for tomorrow 3PM at usual spot. Bring the materials we discussed. Payment ready as agreed - $250,000 transferred to account ending 4789."

Additional Communication Patterns:

Analysis of call logs revealed 47 incoming and outgoing calls with the Russian number between January 10, 2024 and February 25, 2024. Call duration analysis shows conversations averaging 12-15 minutes, suggesting substantive discussions rather than brief coordination calls.

Personal Computer Analysis:

Case Identifier: 2024-DOJ-0847

Case Investigator: Christian A. Coleman

Identity of the Submitter: Department of Justice, Criminal Division

Date of Receipt: February 28, 2024

Acquisition Process:

- Connected suspect laptop to forensic workstation via Tableau T35u write blocker
- Created forensic image using FTK Imager 4.7.1
- Performed comprehensive analysis using EnCase Forensic 21.4

Email Communications Analysis:

Using Internet Evidence Finder, I recovered extensive email communications between the subject and RedRalph@gmail.com. Key findings include:

Email Thread #1 - "Consulting Services"

Date Range: January 8, 2024 - February 20, 2024

Subject Line: "Payment for consulting services - Project Blackbird"

Key Content: Discussion of $500,000 payment structure for "access to strategic intelligence reports" and "policy position papers"

Email Thread #2 - "Meeting Logistics"

Date: February 14, 2024

Subject: "Tomorrow's discussion"

Content: "The submarine patrol schedules you requested are ready for review. NATO positioning data included as bonus. Swiss account transfer confirmed."

Case Identifier: 2024-DOJ-0847

Case Investigator: Christian A. Coleman

Identity of the Submitter: Department of Justice, Criminal Division

Date of Receipt: February 28, 2024

Deleted File Recovery:

Through forensic analysis of unallocated disk space, I successfully recovered multiple ZIP files that had been deleted using secure deletion software. File system analysis indicates deletion occurred on February 26, 2024, approximately 6 hours after news reports surfaced about the ongoing investigation.

Recovered Files Include:

- "NATO_Baltic_Operations_2024_CLASSIFIED.zip" (2.4 MB)
- "Submarine_Patrol_Routes_Q1_2024.zip" (1.8 MB)
- "Nuclear_Readiness_Assessment_SECRET.zip" (3.2 MB)

Web Activity Analysis:

Browser forensics revealed uploads to encrypted file-sharing service "SecureDrop.onion" on February 22, 2024. Server logs (obtained through separate warrant) confirm these files were accessed from IP addresses registered in Moscow, Russia on February 23, 2024.

Financial Evidence:

Banking application stored credentials revealed automated transfers totaling $750,000 to Swiss bank account CH93 0076 2011 6238 5295 7. Account holder listed as "R. Petrov Consulting Services."

Case Identifier: 2024-DOJ-0847

Case Investigator: Christian A. Coleman

Identity of the Submitter: Department of Justice, Criminal Division

Date of Receipt: February 28, 2024

Conclusion:

Forensic analysis provides substantial digital evidence supporting charges of espionage and conspiracy. The subject maintained regular contact with Russian intelligence operative "Red Ralph," received significant financial compensation, and provided classified US military intelligence in exchange for payment. All evidence was acquired following proper chain of custody procedures and forensic best practices.

Evidence Inventory:

- Complete forensic images of both devices
- 47 call records with Russian contact
- 23 email communications discussing classified material exchange
- 3 recovered ZIP files containing classified documents
- Banking records showing $750,000 in suspicious transfers
- Web logs confirming hostile intelligence service access to uploaded materials

Hardware/Software Used:

- Cellebrite UFED Touch2 Mobile Forensics Platform
- Tableau T35u Hardware Write Blocker
- FTK Imager 4.7.1
- EnCase Forensic 21.4
- Internet Evidence Finder v6.9

Case Identifier: 2024-DOJ-0847

Case Investigator: Christian A. Coleman

Identity of the Submitter: Department of Justice, Criminal Division

Date of Receipt: February 28, 2024

All forensic procedures followed Department of Justice Computer Crime and Intellectual Property Section guidelines. Original media integrity maintained throughout the examination process.

Case Status: Investigation Complete - Evidence Ready for Prosecution