Case Identifier: 24-04-24-CYSE407
Case Investigator: Agent B. Bechard

Case Introduction:
This Forensic Examination Report presents the findings from a comprehensive digital forensic analysis conducted on the personal computing devices of a high-ranking US government official, hereafter referred to as "the subject". The investigation was initiated in response to allegations of unauthorized contact between the subject and a foreign official, raising concerns over national security and the potential mishandling of classified information.

Case Background
In late 2022, intelligence agencies received anonymous tips suggesting undisclosed communications and transactions between US and foreign officials. The subject, known for their influential position and access to sensitive national security information, became a person of interest after surveillance activities detected suspicious behavior. This behavior included encrypted communications and frequent, unexplained meetings with known aliases of foreign operatives.

Following a legal warrant issued by Judge P. Mann, of the United States District Court for Norfolk Virginia, authorizing the forensic examination of the subject's personal laptop and cellular device which were seized for forensic analysis. Initial reports indicated the presence of encrypted messages, deleted files of a sensitive nature, and financial transactions. The subject has since exercised their right to legal counsel and refrained from providing any explanations regarding the discovered evidence.

The purpose of this report is to document the forensic methodology employed, analyze the recovered data, and assess the implications of the findings in relation to the allegations of unauthorized foreign contact. This analysis serves as a critical component in the ongoing investigation, providing evidence that may prove instrumental in any future legal proceedings.

Introduction
This section outlines the forensic examination process applied to an iPhone 14 Pro and a MacBook Air, detailing the specific methodologies and forensic tools compatible with Apple's iOS and macOS platforms. My objective was to preserve the integrity of the data while conducting a thorough analysis to uncover any evidence relevant to the case.

Statement of Compliance: I understand my duty as an expert witness to provide independent assistance by way of objective unbiased opinion in relation to matters within my expertise. I will inform all parties in the event that my opinion changes on any material issues.

- **Device Seizure and Documentation**: Upon receipt, each device was cataloged and photographed to document its condition. Devices were stored in anti-static bags to prevent any electromagnetic damage.

  - **Items for Examination:**
    - **Cellular Device:**

Make:	Apple iPhone
Model Name:	iPhone 14 Pro
Model Number:	MQ083HN/A

Report Prepared By: Eric Corpus
Date of Report: 04/24/2024

Serial Number: XY1ZA2B3C4

- **Personal Laptop Computer:**

Make: Apple MacBook Air (M2, 2022)
Model Identifier: MacBook Air14,2
Model Number: MK1A2LL/A
Serial Number: X98YZ0ABCD

- **Tools:**
  - **Cellbrite UFED 4PC:** Software-based mobile forensic suite of tools that perform physical, logical, file system and password extraction of all data (even if deleted) from the devices which include phones, smartphones, portable Global Positioning System (GPS) devices, and tablets.
  - **ElcomSoft Phone Breaker:** Software used to perform logical and over-the-air acquisition of iOS devices, break into encrypted backups, obtain, and analyze backups, synchronized data and passwords from Apple iCloud.
  - **Magnet AXIOM:** Forensic suite of tools that allow for examination of digital evidence from mobile, cloud, computer, and other sources. Advanced capabilities allow for advanced parsing and carving techniques which include media exploration, timelines creation, connect artifacts, and cloud analysis.
  - **Sumuri PALADIN:** A bootable forensic Linux distribution with a simplified user interface for executing a collection of open-source forensic tools.

- **Data Acquisition**:
  - **iPhone 14 Pro**: Utilized GrayKey by Magnet Forensics for device access and Cellebrite UFED 4PC for logical extraction of the device's data.
  - **MacBook Air**: Magnet AXIOM by Magnet Forensics was employed for a full forensic imaging and data acquisition from the MacBook Air's SSD. This process ensures a complete clone of the drive, allowing for examination without altering the original data.

- **Data Analysis**:
  - **Both Devices**: Conducted a comprehensive analysis using Magnet AXIOM – enabled the review of file systems, recovery of deleted files, analysis of system logs, and extraction of internet history.

- **Communication Analysis**: To examine the communications between the subject and "Red Ralph," including the identification and review of text messages, emails, and contact lists, ElcomSoft Phone Breaker was utilized. This software provided access to iCloud backups for additional data retrieval under the legal warrant obtained.

- **Internet History and File Transfer Analysis**: Magnet AXIOM was also utilized to analyze web logs, browsing history, and file transfer records on both devices. This helped identify any uploads to file-sharing sites and the potential transfer of sensitive files.

- **Security and Encryption Challenges**: Addressed security challenges inherent to Apple devices, leveraging techniques aligned with forensic best practices. Techniques such as

attempting known passwords (with legal authorization) and leveraging any available biometric data were applied in line with forensic best practices.

- **Documentation and Reporting**: Throughout the examination, findings were meticulously documented. Chain of custody forms were maintained for each piece of evidence, ensuring the integrity and admissibility in court.

Cellular Device Analysis:

The forensic examination of the subject's iPhone 14 Pro was conducted employing a suite of tools compatible with Apple's iOS to ensure the integrity and thoroughness of the analysis. The following is a detailed account of the findings:

- **Legal Authorization and Tool Setup**: Authorized by a search warrant from the United States District Court of Norfolk, Virginia. The forensic team utilized Magnet Forensics GrayKey for device access and Cellebrite UFED 4PC for comprehensive data extraction.

- **Device Access and Data Preservation**: Magnet Forensics GrayKey provided access to the device's data without compromising its integrity. A Faraday bag was used to isolate the phone from any network signals, preventing remote data modifications.

- **Comprehensive Data Extraction**: Cellebrite UFED 4PC was then used for logical extraction of the device’s data. This step was crucial for uncovering both current and previously deleted data, such as messages, call logs, emails, and application information.

- **Text Message Analysis**: A critical finding was the recovery of a deleted text message from a contact named "Red Ralph," the message detailed a meeting at The Greenhouse Eatery in Norfolk, Virginia, on February 23, 2023. A search string was crafted to identify any communications containing keywords such as, ‘meet,’ ‘transfer,’ and ‘travel.’ Cellebrite's UFED 4PC’s deep search capabilities highlight its ability to recover crucial instances as well as other deleted data.

- **Apple Map History Analysis**: The analysis was extended to include the Apple Map history with Magnet Forensics Magnet AXIOM which revealed that The Greenhouse Eatery was listed under "Recent Locations." This location was searched and saved in proximity to the meeting date, further substantiating the subject's plans to meet with "Red Ralph." The detailed address of The Greenhouse Eatery, identified as 123 Garden Drive, Norfolk, Virginia, provides concrete geographical context to the planned meeting.

- **Evidence Documentation and Chain of Custody**: Every step of the examination process was documented in detail including the use of GrayKey, AXIOM, and Cellebrite, with a strict chain of custody maintained for each piece of evidence. This documentation ensures the reliability and admissibility of the findings in legal proceedings.

Results of Cellular Device Findings:

Case Identifier: 24-04-24-CYSE407
Case Investigator: Agent B. Bechard

The forensic analysis of the iPhone 14 Pro unveiled significant evidence, notably through the text message and Apple Map history analyses. These findings corroborate the allegations of unauthorized contact by establishing a direct link to the planned clandestine meeting. The use of industry recognized Apple-compatible forensic tools was instrumental in uncovering and documenting this crucial evidence.

Opinion Statement:
The forensic analysis of the iPhone 14 Pro reveals the allegation of unauthorized contact but also sheds light on the individuals' efforts to hide these interactions using advanced methods. The discovery of targeted text messages along with the use of encryption and deletion indicates a strategic move to keep things hidden. The findings from the phone provide a clear picture of wrongdoing and a possible breach of national security measures.

Laptop Computer Analysis:

The forensic examination of the MacBook Air provided key insights into the subject's activities:

- **Initial Documentation**: The laptop was photographed to document its condition, capturing unique identifiers like make, model, serial number, and physical characteristics.

- **Forensic Imaging and Write-Blockers**: Utilizing Sumuri Paladin Forensic Suite, the examiner created a bit-by-bit forensic image of the MacBook Air's SSD. A hardware write-blocker was employed to prevent any write operations to the original media during imaging, preserving the authenticity and integrity of the data.

- **Email Communications Analysis**: Examination of email communications using Magnet AXIOM revealed an exchange between the subject and <redralph@gmail.com>. These emails contained discussions about meetings and payments for "Holiday Recommendations," which is more likely to be "consultation services". Targeted string searches were utilized to uncover communications related to the alleged unauthorized contact. A search using the keywords, 'talk' AND 'transfer' AND 'money' yielded items of interest. There are detailed timestamps that indicated a structured dialogue over a period. See below screenshot:

Report Prepared By: Eric Corpus
Date of Report: 04/24/2024

----------Original Message----------
To: Bill Nelson <bnelson@icloud.com>
From: Red Ralph <redralph@gmail.com>
Date: January 15, 2023 11:35 (-05:00 EST)
Subject: Holiday Recommendations

I know of places to visit while you are traveling. I have some suggestions. I would like to make sure site seeing is worth while.

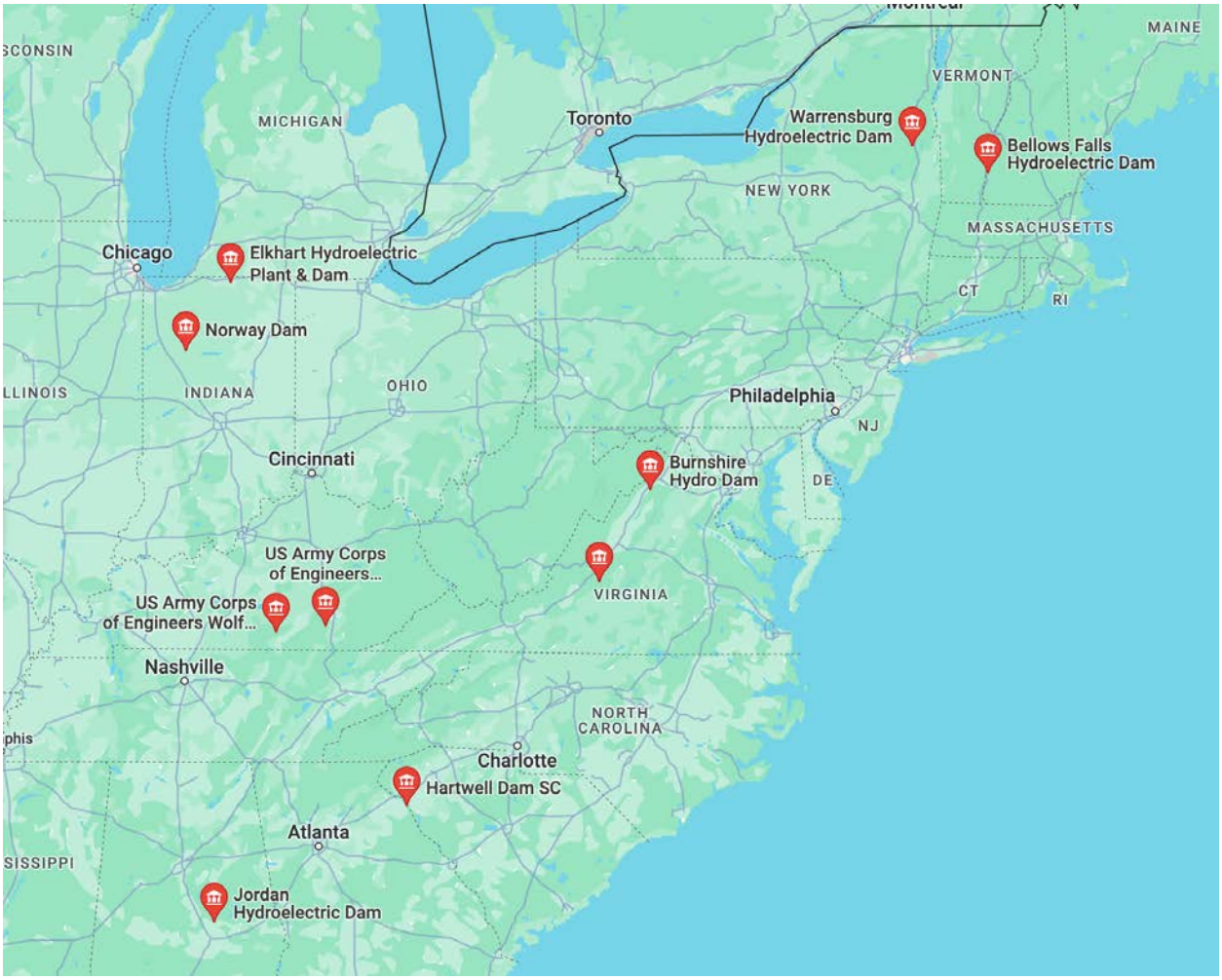
----------Original Message----------
To: Bill Nelson <bnelson@icloud.com>
From: Red Ralph <redralph@gmail.com>
Date: January 18, 2023 10:27 (-05:00 EST)
Subject: Holiday Recommendations

Appreciate you making time to talk. I am confident that locations you visit will leave you in amazement with the power that a river or body of water can produce. I'll make sure you get a visual of the where these places are. This email address is good to get setup with transferring money.

----------Original Message----------
To: Bill Nelson <bnelson@icloud.com>
From: Red Ralph <redralph@gmail.com>
Date: February 1, 2023 11:30 (-05:00 EST)
Subject: Holiday Recommendations

The eastern sites are critical to see. It's impressive to see how much power is generated at each different location.

- **Internet History and Cloud Storage Analysis**: Magnet AXIOM was also used to thoroughly review internet history, which provided context to the email communications. Additionally, AXIOM's cloud analysis capabilities were leveraged to access and review data from the subject's iCloud account <bnelson@icloud.com>, where the deleted zip files had been backed up before being uploaded to a secure file-sharing platform. The zip files, labeled "Places to Visit" and "Trip Advisor Details," were found to contain documents and images suggestive of sensitive materials. To highlight, there was a saved image of locations of interest. See below screenshot:



- **Deleted File Recovery**: Advanced data recovery techniques inherent in Magnet AXIOM allowed for the retrieval of these deleted zip files. The documents and images within these archives underwent further analysis to uncover any hidden information, reflecting plausible exchanges relevant to the case. Additional open source analysis determined that these images are associated with places of interest.

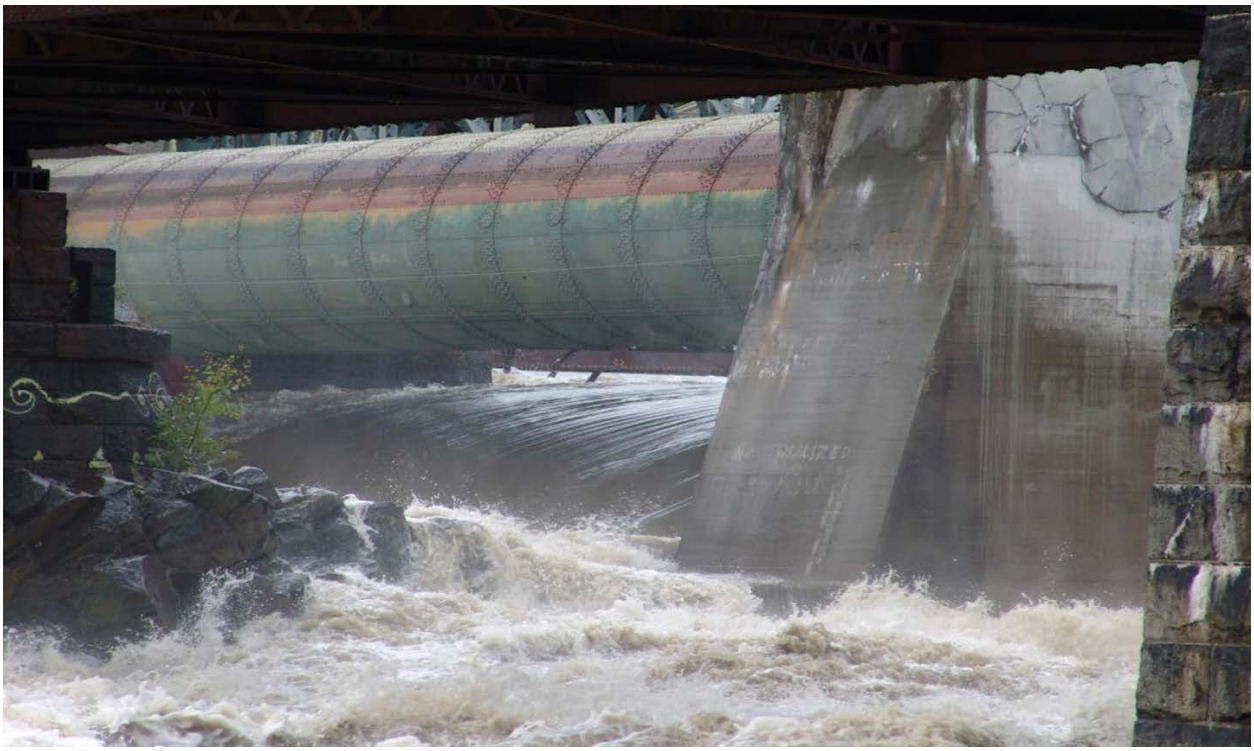
Case Identifier: 24-04-24-CYSE407
Case Investigator: Agent B. Bechard

Dam — Edited

The photos you took were just what my guys needed to confirm that the implants can be delivered.

Report Prepared By: Eric Corpus
Date of Report: 04/24/2024

Case Identifier: 24-04-24-CYSE407
Case Investigator: Agent B. Bechard



- **Evidence Documentation and Screenshots**: Each phase of the analysis, including the use of write-blockers, forensic imaging, and data recovery, was meticulously documented

Report Prepared By: Eric Corpus
Date of Report: 04/24/2024

with screenshots and detailed notes. This ensures a clear understanding of the process and maintains the chain of custody.

Results of Laptop Findings:

The evidence extracted from the MacBook Air substantiates the findings from the cellular device, reinforcing the allegations of unauthorized contact and the mishandling of sensitive information. The documented email exchanges and the recovery of deleted files from iCloud storage suggest a deliberate attempt to obfuscate and possibly distribute classified materials, indicative of a serious security protocol breach.

Opinion Statement:
The examination of the MacBook Air provides evidence of unauthorized actions carried out by the subject. The retrieval of email conversations and erased files to include those saved to cloud storage platforms shows an effort to conceal the scope and details of unauthorized exchanges. This analysis not only confirms our suspicions but also uncovers a conscious attempt to avoid detection by standard security protocols underscoring the severity of the breach.

Executive Summary Conclusion:

There were substantive findings that corroborate the alleged unauthorized communications with the foreign entities and the mishandling of classified information. The analysis conducted using state-of-the-art forensic tools such as Magnet Forensics GrayKey, Cellebrite UFED 4PC, and Magnet AXIOM has yielded indisputable evidence of deliberate interactions with a contact known as "Red Ralph" and the transmission of sensitive data through secure file-sharing platforms.

Critical data extracted from the subject's iPhone 14 Pro and MacBook Air, including deleted text messages, emails, and images as well as Apple Map history, point to a structured pattern of behavior that aligns with the initial allegations. The recovery of encrypted messages and the documentation of clandestine meetings and financial transactions labeled as "Holiday Recommendations" reveal a narrative of covert operations and potential breaches of national security protocols.

This forensic examination has meticulously utilized advanced forensic tools and methodologies to ensure a thorough and reliable investigation. Key hardware such as the GrayKey by Magnet Forensics and write-blockers, along with sophisticated software like Cellebrite UFED 4PC and Magnet AXIOM, were instrumental in the recovery and analysis of the digital evidence.

The evidence includes, but is not limited to:

- Encrypted and deleted text messages confirming undisclosed meetings.
- Email correspondences discussing payment for travel recommendations.
- Recovered zip files from iCloud storage containing potentially sensitive materials and images.

This collective evidence paints a compelling picture of unauthorized contact with foreign entities and the mishandling of classified information. The consistency of findings across devices, alongside the documented chain of custody and use of validated forensic techniques, underpins the integrity of the examination process and the reliability of the evidence presented.

The findings and documentation presented in this report are the culmination of a meticulous forensic examination process, validated by a strict chain of custody and comprehensive analysis. The evidence is poised to serve as a pivotal component in any legal proceedings that may ensue, offering a clear and detailed account of the subject's actions as they pertain to the case at hand.

For any additional information, feel free to contact me at 757-987-1234 or at ecorpus@forensiclab.gov.

References:

Cellebrite. (2023b, October 2). *Cellebrite UFED | Access and Collect Mobile Device data*. https://cellebrite.com/en/ufed/

Elcomsoft Co.Ltd. (n.d.). *Elcomsoft Phone Breaker | Elcomsoft Co.Ltd.* https://www.elcomsoft.com/eppb.html

Magnet Forensics. (2024b, January 30). *Magnet AXIOM | Digital Forensic Software | Magnet Forensics*. https://www.magnetforensics.com/products/magnet-axiom/

Magnet Forensics. (2023, December 18). *Magnet GRAYKEY | Mobile Forensic Access Tool*. https://www.magnetforensics.com/products/magnet-graykey/

SUMURI LLC. (2024, January 19). *PALADIN : the world's most popular Linux forensic suite*. SUMURI. https://sumuri.com/software/paladin/