Case Identifier: 2024-98-001

Case Investigator: Hayden Vermeulen

Submitter: Bryan Bechard

Date of Receipt: 4/24/2024

Items Submitted for Examination:

Phone:

- *Serial Number: XYZ123456789*
- *Make and Model: Samsung Galaxy S20*
- *Description: The phone belonging to the high-ranking US government official is a Samsung Galaxy S20, a commonly used device known for its advanced features and capabilities. It was confiscated as part of the investigation into alleged contact with Russian officials.*

Laptop:

- *Serial Number: ABC987654321*
- *Make and Model: Dell XPS 13*
- *Description: The laptop belonging to the high-ranking US government official is a Dell XPS 13, a popular choice among professionals for its performance and portability. It was seized for forensic examination to uncover potential evidence related to unauthorized activities and communications.*

Forensic Analysis:

- ***Phone***

- *Receiving the Phone:*

  In a bag for evidence that was sealed and closed to avoid any meddling or pollution, the forensic examiner got the phone. They noted down detailed documentation which covered its physical state and signs of harm on it plus if it had power or not. Also, they registered any other things like chargers or earphones that came with the phone for making sure everything is included in this record keeping process.

- *Obtaining a Warrant:*

Case Identifier: 2024-98-001

Case Investigator: Hayden Vermeulen

Submitter: Bryan Bechard

Date of Receipt: 4/24/2024

Before starting the process of forensic analysis, it was confirmed by the forensic examiner that a warrant with legal validity has been acquired from related judicial authority. This legal document described what could be searched and seized, giving details about contacts supposedly made with Russian officials to maintain alignment with law and constitution prerequisites.

- *Chain of Custody Documentation:*

  A very specific chain of custody log was made to keep a record of where and how the phone moved and was handled from when it got received up until after forensic analysis finished. Every time ownership changed hands, we noted down names of people involved, times it happened with their details as well as any related notes or observations - this done in order for the evidence to be maintained correctly and accepted.

- *Forensic Imaging:*

  By using forensic imaging tools Cellebrite UFED or Magnet AXIOM, I made a copy of the phone's storage media bit by bit. This way guarantees that original data is preserved and can be studied in detail without changing anything on the device itself or putting its safety at risk.

- *Data Extraction:*

  The forensic imaging finished and the examiner started to take out all possible data from the phone, this included both things that are active and deleted. This involved various kinds of information like call logs, text messages, emails, social media use details such as where they were located at different times as well as data from applications among other types of information.

- *Data Analysis:*

  The data that was taken out went through detailed analysis using special forensic analysis software Oxygen Forensic Detective. This process included looking for keywords, filtering data, examining metadata and correlating data to find evidence linked with the claimed contact involving Russian officials.

- *Unlocking the Phone:*

Case Identifier: 2024-98-001

Case Investigator: Hayden Vermeulen

Submitter: Bryan Bechard

Date of Receipt: 4/24/2024

The phone had a lock through passcode, biometric check or encryption. This might include using already identified weak points, forceful attempts known as brute-force attacks, or making use of possible legal paths like getting permission or an order from court for accessing what's inside the device.

- *Timeline Reconstruction:*

  A sorted timeline of events was made using the data found, showing the order of communications, gatherings and contacts between an important person in United States government with people who are linked to claimed contact with Russians officials. This gave helpful understanding about kind and situation of communication for investigation as whole.

- *Reporting:*

  After the analysis, a full forensic report was made that wrote down all discoveries, ways of study and examination results. It was accompanied with important things like artifacts, pictures of screens, records and metadata. This report also had explanations and interpretations made from looking into these evidences to give a complete summary about forensic process done as well as what it means for this case.

- *Secure Storage:*

  The original and duplicate proofs, also forensic pictures and data extraction, all were kept safely following the rules to hold chain of custody intact. The stored evidence was controlled for access strictly and proper measures were taken to avoid any unauthorized tampering or alteration.

- ***Laptop***

- *Receiving the Laptop:*

  After getting the laptop, the forensic investigator carefully recorded its physical state. They noted any signs of outside harm or interference on it. The laptop and all accessories

Case Identifier: 2024-98-001

Case Investigator: Hayden Vermeulen

Submitter: Bryan Bechard

Date of Receipt: 4/24/2024

like power adapter were kept in evidence bag for safety to maintain their integrity during forensic examination.

- *Obtaining a Warrant:*

  I first made sure we have a warrant that is legally correct, which was given by the suitable judicial authority. This warrant allows us to search and take the laptop for any proof linked with supposed meetings and talks about payment with Russian officials.

- *Chain of Custody Documentation:*

  The most important was to keep the evidence's integrity intact. I carefully noted every step made in the process of custody chain. Beginning from when I received laptop, then to its final storage place - each shift of responsibility was precisely documented for accountability assurance and admissibility of evidence within courtroom.

- *Forensic Imaging:*

  I have made a copy of the storage media in the laptop using forensic imaging tools that are commonly used in this field, like EnCase Forensic. This method of bit-by-bit imaging ensures that all data from original is kept identical and undamaged for investigation purposes while protecting against any changes or alterations on source device itself.

- *Data Extraction:*

  Having the forensic image ready, I started to get all available data from the laptop. This included files, folders, system logs and registry entries - both active and deleted. The aim was for a thorough look at possible proof related to our inquiry.

- *Data Analysis:*

Case Identifier: 2024-98-001

Case Investigator: Hayden Vermeulen

Submitter: Bryan Bechard

Date of Receipt: 4/24/2024

The retrieved data was carefully examined and analyzed using specialized forensic analysis tools, such as Autopsy or Sleuth Kit. To find and retrieve relevant evidence about meetings, payment talks, and file uploads connected to Russian authorities, keyword searches, file signatures, metadata analysis, and file carving techniques were applied.

- *Decryption and Recovery:*

  Forensic investigators used sophisticated decryption and data recovery methods to recover and rebuild the contents of files that had been encrypted or erased. This can include recovering erased or hidden data that is relevant to the investigation using forensic tools, file carving, or cryptographic keys.

- *Timeline Reconstruction:*

  Using the collected data, a chronological chronology of events was created to determine the order of conversations, gatherings, and file transfers involving the senior US government official and people who were allegedly in contact with Russian officials. This timeline made it easier to comprehend the background and importance of the forensic findings.

- *Reporting:*

  A thorough forensic report outlining the procedures, results, and conclusions of the investigation was created after the analysis. In order to present a cogent account of the forensic procedure and its consequences for the case, the report includes pertinent artifacts, screenshots, logs, and interpretations of the evidence.

- *Secure Storage:*

  Forensic photos and extracted data, as well as all original and duplicate evidence, were safely kept in compliance with established processes to uphold the evidence's integrity and chain of custody. Severe access controls were in place, and suitable measures were put in place to stop unwanted interference or manipulation of the evidence that was stored.

Case Identifier: 2024-98-001

Case Investigator: Hayden Vermeulen

Submitter: Bryan Bechard

Date of Receipt: 4/24/2024

Conclusion:

- *Phone Analysis:*

The phone, a Samsung Galaxy S20, was inspected with the help of forensic tools like Cellebrite UFED and Oxygen Forensic Detective. There was some small physical harm seen on the phone's casing, like scratches and scuffs. However, we did not observe any significant damage to its functionality. The official had communication with someone titled "Red Ralph," which was discovered using forensic imaging and data extraction. This includes a text message that confirms their lunch meeting on 2/15/20xx. Further investigation exposed a string of email communications involving meetings and payment discussions for "consulting services," utilizing an email address linked to "RedRalph@gmail.com."

- *Laptop Analysis:*

The laptop, which we recognized to be a Dell XPS 13, was subjected to forensic study by utilizing EnCase Forensic and Autopsy tools.The laptop did not show any serious physical harm, confirming that it remains intact for forensic examination. Through forensic imaging and data extraction, they discovered deleted zip files. These files were found on a file-sharing site and contained classified material. The timestamps of these files matched with the official's activity log. Additional study of the data showed email exchanges about meetings and payment talks with "Red Ralph" for consultancy work.

- *Overall Findings:*

The examination of both devices by forensics showed some interesting findings. They point to serious communication and cooperation happening between the important US government person and people linked with "Red Ralph." This could suggest unauthorized contact with Russian officials.Although there were some small physical damages on the casing of phone, both devices could work completely and provide for thorough forensic examination. Forensic software, like Cellebrite UFED, Oxygen Forensic Detective, EnCase Forensic, and Autopsy helped to find deleted files or review data on different devices. It also aided in recreating events' schedules. The laptop having deleted zip files that hold classified stuff is a serious worry about

Case Identifier: 2024-98-001

Case Investigator: Hayden Vermeulen

Submitter: Bryan Bechard

Date of Receipt: 4/24/2024

possibly breaking national safety rules and revealing important details without permission. The results of both devices are strong proof that needs more study and possible legal steps to handle the effects of claimed misbehavior on national safety interests. In summary, the study of the phone and laptop in forensics has given important understanding about what the high-level US government official was doing. This underlines the requirement for careful investigation and action to handle any breaking of confidence or safety rules.