Case Identifier: 89- 6753

Case Investigator: Ruth Abeselom

Identity of the Submitter: Anonymous

Date of Receipt: 12/08/23

FORENSIC EVIDENCE REPORT

Case: Alleged Contact between US and Russian Officials

To: Ryan Madden

[Prosecutor's Office]

I am writing to provide you with the findings of my forensic analysis conducted on the laptop and cell phone belonging to the high-ranking US government official in question. The following evidence has been discovered during the investigation:

1. Phone Evidence: A text message was found on the phone, dated 2/15/2023, confirming a lunch meeting. The contact associated with the phone number was labeled as "Red Ralph" in the contact list.

Evidence inquiries include a cellular iphone 13 pro max which runs on IOS software and has an IOS operating system. Serial number: 587697243-FNQ.

2. Laptop Evidence: Several email communications were recovered from the laptop, indicating meetings and discussions between the official and an individual associated with the email address RedRalph@gmail.com. The content of these emails suggests the existence of ongoing interactions and the involvement of the official in these discussions. Additionally, the laptop contained several deleted zip files of classified material. These files were discovered in the unallocated space of the hard drive, and web logs indicate that they were uploaded to a file sharing site. It remains uncertain if these files were downloaded by any other parties.

Evidence inquiries includes a Silver 13 inch MacBook Air 2020. The MacBook has a Linux Operating system and runs IOS software. Serial number: 789563261-BRN.

During the examination of the laptop and cell phone in question, several steps were taken to gather evidence and uncover relevant information. The following steps were undertaken:

1. String Searches: This involves scanning the devices for specific keywords or phrases that may be relevant to the investigation. In this case, string searches were conducted on both the laptop and phone to identify any references to individuals, meetings, or other significant terms. This helped in locating the text confirming the lunch meeting and the email communications related to the alleged contact.
2. Graphics Image Searches: Graphics image searches were performed on the laptop to identify any visual evidence or images that could shed light on the nature of the contact or provide additional information.
3. Recovering Erased Files: To uncover deleted or hidden evidence, specialized software and techniques were employed to recover erased files from the laptop's hard drive. By examining the unallocated space, where deleted files reside until overwritten, several deleted zip files containing classified material were discovered.

As a result, the evaluation concludes that no original media was altered, tampered with, or damaged in any way. Several deleted zip files containing classified material were found in the unallocated space of the laptop's hard drive. These files were identified as having been uploaded to a file sharing site, although it remains unclear if anyone downloaded them. The text message, email communications, and deleted classified files all indicate a level of engagement and potential compromise that requires further investigations.

Sincerely,

Ruth Abeselom
Forensic Expert