Krypton Digital Forensics Firm

Digital Forensics Investigation Report

Case Investigator: Dennis Hargro Jr

Lead Forensics Lab Manager: Jeremy Noce

Case Number: JS0029324897

Date: April 22, 20xx

Investigation Summary:

On March 23rd 20xx, authorities reached out to our digital forensics team to examine electronic devices belonging to US official Joe Swanson. The focus of the investigation was to uncover any alleged evidence of communication between US official Swanson and Russian officials. Mr. Swanson had invoked his right to remain silent and refused to elaborate on the allegations. However, our analysis of his recovered laptop and personal cell phone presented numerous findings of an unidentified contact with Mr. Swanson.

Evidence Seized:

Laptop:

Figure 1: Seized ASUS Laptop

Make: ASUS

Model: E410M

Serial Number: N9M5ZV 10H789453

OS Version: Windows 11 Home

Cell Phone:

Figure 2: Seized Samsung Galaxy A32 5G

Make: Samsung

Model: Galaxy A32 5G/ SM-A326U

Serial Number: ABCR506WKKU

OS Version: Android 13

Investigation Details:

Preservation:

Before the examination, both devices were imaged to a separate 1 TB drive through a Media Writeblocker device for further analysis to avoid contamination of the original data. The drives carrying the copies of the original storage devices were then analyzed through our laboratory equipment.

Findings:

The laboratory was able to recover email logs and deleted files from the laptop through the OS Forensics software. Further examination revealed several email exchanges originating from Mr. Swanson to a "RedRalph@gmail.com". The following visual shows the results received when searching the index with the prompts "Ralph" and "Official". Other searches were conducted with prompts "Russian", "Meeting", "Secret", and "Red Star".

The results indicated a chain of emails relating to a "Meeting" and "Consultation services" between Mr. Swanson and this "Red Ralph".

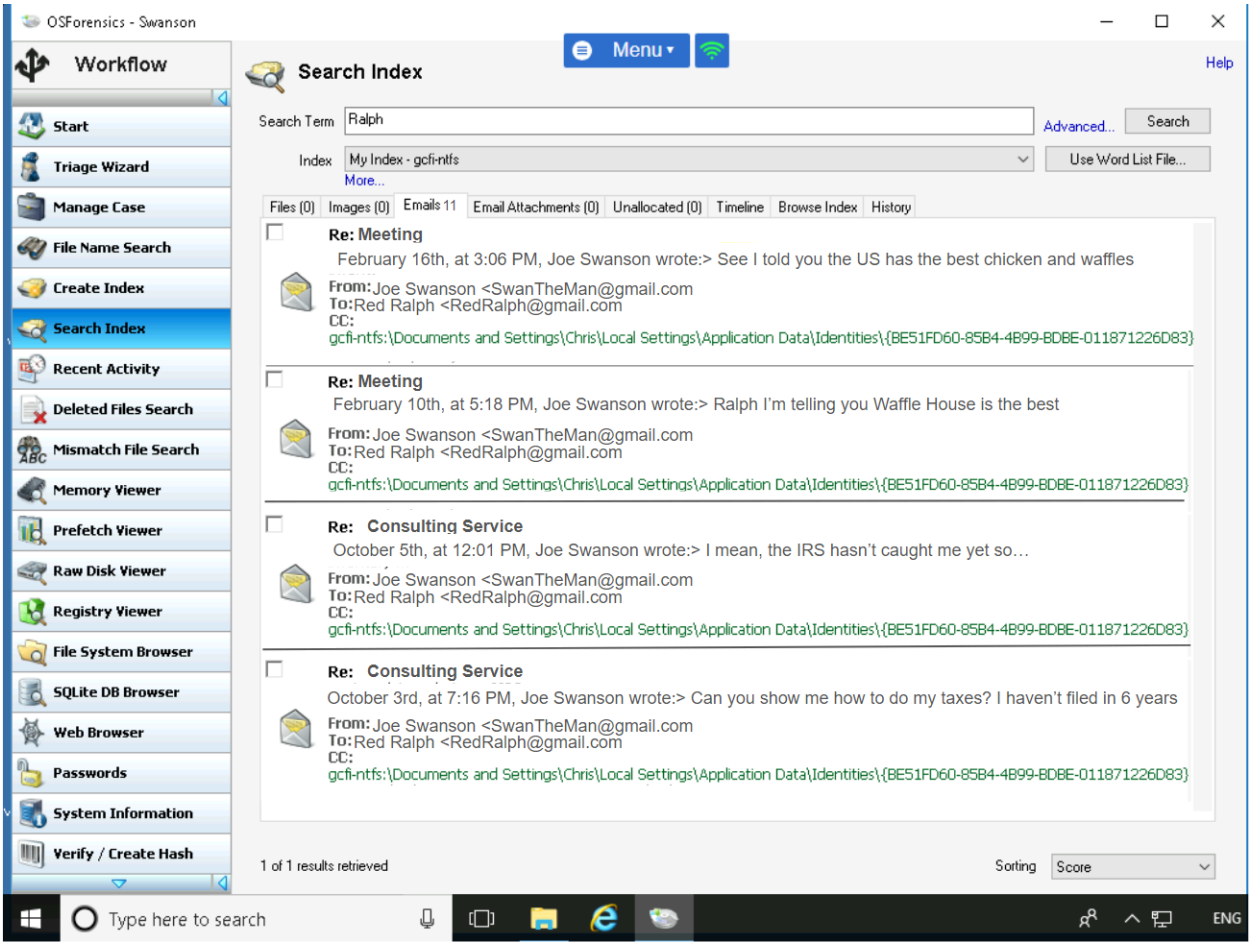

Figure 3: ASUS Email Analysis

Below is another index that was created in the same fashion for hidden files on the laptop; indicating Mr. Swanson's questionable handling of government information.

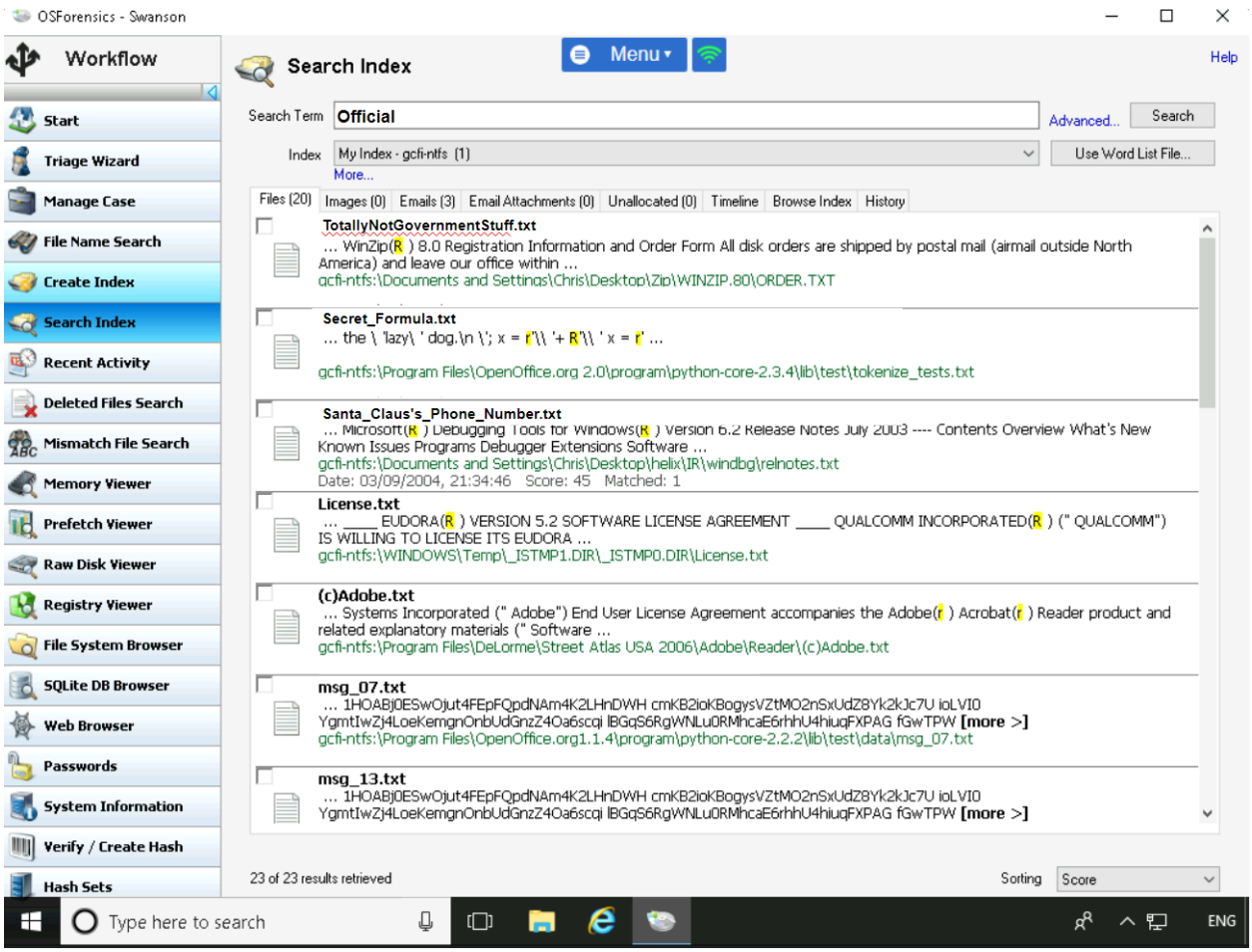

Figure 4: ASUS File Analysis

It was also apparent that Mr. Swanson would frequent a file-sharing site. What he has uploaded and what was downloaded has not been confirmed.

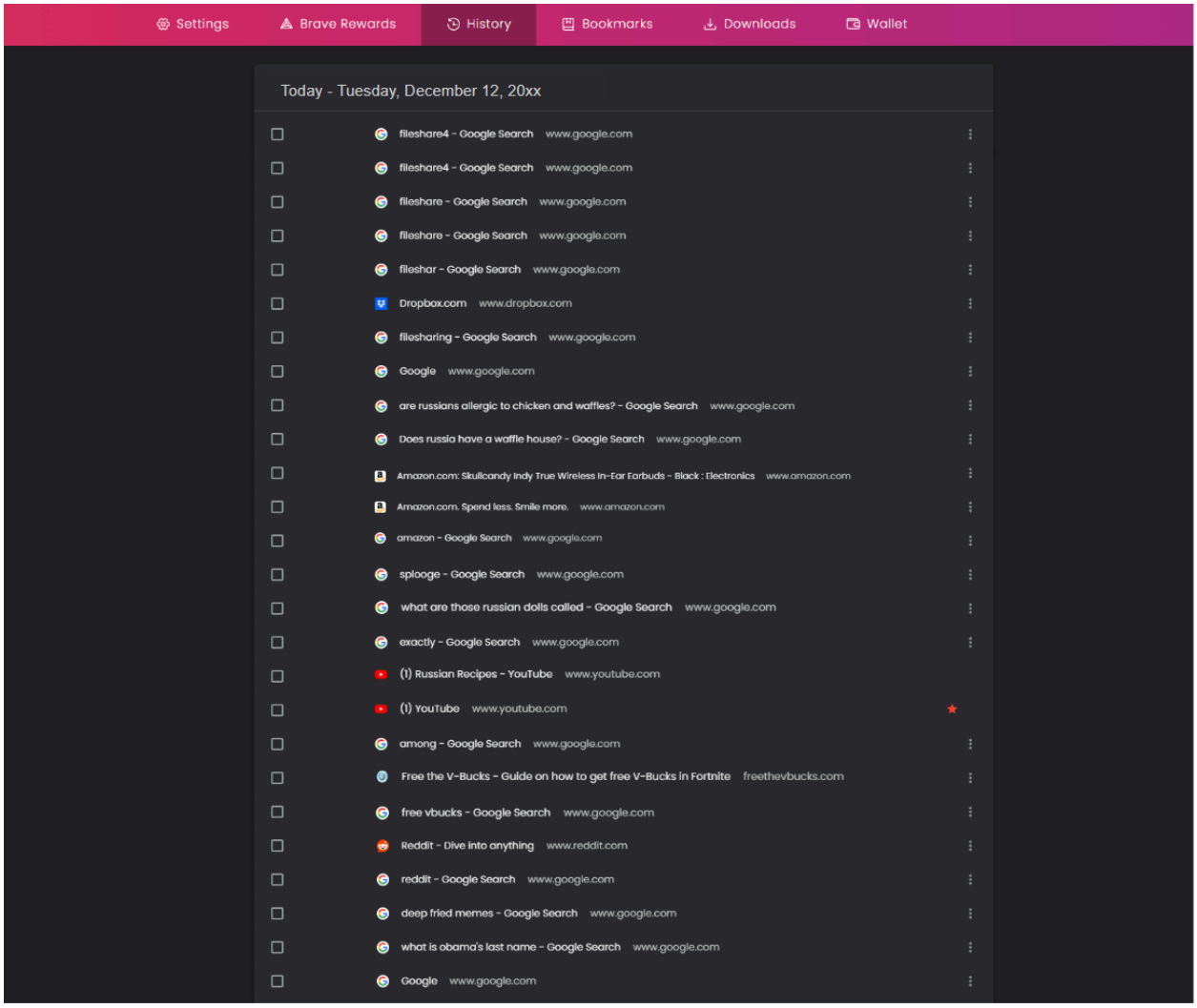

Figure 5: Laptop Browser History

On the phone, we discovered chat logs between the US official and “Red Ralph” from the system’s default SMS messaging application. The contact has no further information, but it seems to be the only contact in Mr. Swanson’s list that is an obvious alias. Further analysis is required to determine the identity of “Red Ralph”.

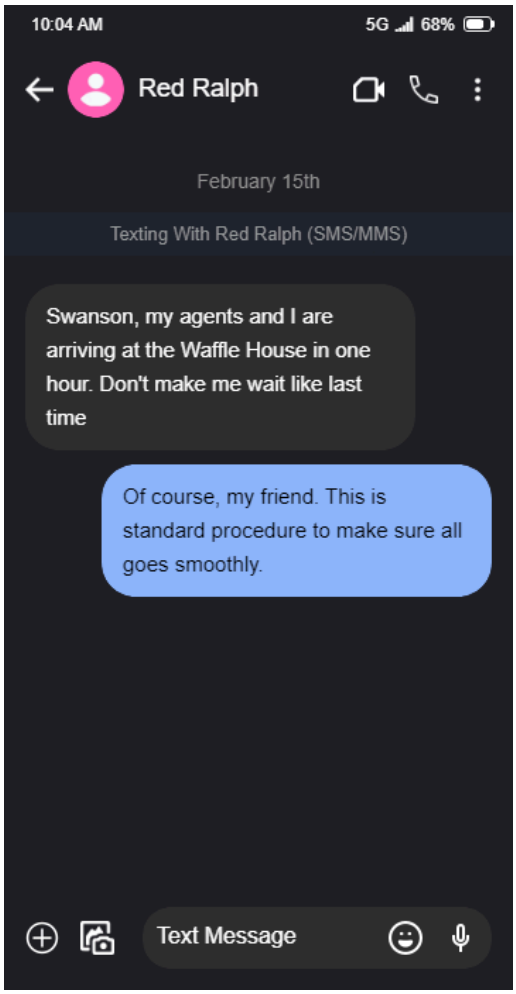

Figure 5: Samsung SMS Analysis

Results of the Investigation:

Based on the findings of our team, there exists a lead as to whether Mr. Swanson is in contact with a Russian official; however, the identity of this “Red Ralph” is unknown. The recovered data suggests Mr. Swanson is in contact with someone he would rather not have his colleagues know about. We recommend suggesting that Mr. Swanson clarify who “Red Ralph” is and provide context behind their meetings.

Do not hesitate to contact our laboratories for further information.

Forensics Investigator: Dennis Hargro Jr

Reviewed by Lead Digital Forensics Manager: Jeremy Noce

Krypton Digital Forensics Firm

Ph: 123-456-7890

Fx: 123-456-3456