Digital Forensic Report Case #1270-53

1. Introduction

The purpose of this report is to investigate the alleged contact between a US government official and a Russian government official. The facts presented in this report have been prepared within the investigator's own expertise and knowledge and do not extend outside of their knowledge and area of expertise.

1.1 Summary of case and tasking

Between the dates February 22nd, 2013 and August 5th, 2016 communication was enacted between John Doe, United States Secretary of State, and Red Ralph, a high ranking general for the Russian government. Communication consisted of emails and text messages.

During this time of communication, classified information was uploaded by 'John Doe' to a public file sharing site. It was unknown as to if any user or persons had downloaded said information uploaded to the site.

Due to this communication with a Russian government official, a forensic expert was engaged to reconstruct the deleted zip files of classified material. The forensic expert is to provide evidence of any collusion with foreign officials and treason committed by John Doe.

1.2 Statement of compliance

I understand that my duty as forensic investigator and expert witness to provide evidence that is unbiased and done independently to my area of knowledge and expertise. I will inform the courts and all parties if bias or opinions of case form to prevent impediment in this case.

2. Items Submitted for investigation

2.1 Laptop

Make: ACER
Model: Aspire S7-393 5th Generation
Serial Number: AC937-8364017-73027

2.2 Phone

Make: Samsung
Model: N900 Galaxy Note 3 32GB
Serial Number: SGN501-4657284-462981

3. Examination

The contents of communication executed through email communications and text communications between John Doe and Red Ralph were completed with the mobile forensics tool Cellebrite UFED. The contents of the deleted zip files uploaded to the file sharing web service were completed with WinRAR forensics recovery tool.

3.1 Tools Used:

Web Analysis:

Screaming Frog SEO Log File Analyser

Mobile Forensics:

Cellebrite UFED

3.2 String Searches with Cellebrite:

- classified
- text "Red Ralph" | meeting | confirmation | lunch
- email "RedRalph@gmail.com" | consulting

3.3 Web Log Anaylsis Searches:

- .zip | upload
- .zip | RedRalph@gmail.com | download
- .zip | download
- .zip | download | classified

4. Conclusion

4.1 Communications found through investigation are as follows:

Phone Communications:

a. Text message sent from John Doe to contact number: +7911 7429187"
b. The phone number above is labeled as 'Red Ralph'
c. Contents of the message pertained to confirming a lunch meeting for the date February 15th, 2014.

Email Communications:

a. Email communications pertaining to consulting services provided to 'Red Ralph' by John Doe
b. Payments received by John Doe for consulting services. Emails received from 'RedRalph@gmail.com"

Web Log Analysis:

a. Zip files that contain classified information were uploaded to file sharing site and downloaded 1,732 times.
b. The site is maintained through user accounts. The uploader can view who downloads their file on the site. The email 'RedRalph@gmail.com' has been identified as one of the downloaders of the classified files.

4.2 Summary

The contents of this investigation have concluded that communication has occurred between John Doe and Red Ralph for 'Consulting Services'. The sharing of classified information has taken place through a file sharing site which led to being downloaded by Red Ralph and numerous other site users. In conclusion, services have been provided by John Doe to Red Ralph for monetary gain. In the process of consulting services, classified information has been found to be shared.