UNITED STATES DISTRICT COURT
DISTRICT OF COLUMBIA
DIGITAL FORENSIC EXAMINATION REPORT

I. CASE DESCRIPTORS

Case Identifier:	USDC-DC-2017-0847-FE
Case Investigator:	Special Agent Jordan M. Reeves, Digital Forensics Unit
Submitting Agency:	Federal Bureau of Investigation, Cyber Division
Identity of Submitter:	SA Jordan M. Reeves, Badge #74821
Date of Receipt:	December 10, 2017
Date of Examination:	December 10–12, 2017
Date of Report:	December 14, 2017
Classification:	SENSITIVE – LAW ENFORCEMENT USE ONLY

II. ITEMS SUBMITTED FOR EXAMINATION

The following items were received and examined. All items were received with intact chain-of-custody documentation and tamper-evident packaging.

Item 1 – Cellular Device

Make / Model:	Apple iPhone 8 Plus
Serial Number:	F2LXQ7HJHG7T
IMEI:	356938035643809
Color:	Space Gray
Storage Capacity:	256 GB
Condition:	Powered on, locked with 6-digit PIN, screen intact
SIM Card Present:	Yes – AT&T USIM, ICCID: 8901410064027841492

Item 2 – Personal Laptop Computer

Make / Model:	Dell XPS 15 (9570)
Serial Number:	8XKPLQ2

Service Tag:	8XKPLQ2-7E3F
Operating System:	Windows 10 Pro (Build 17134)
RAM:	16 GB
Internal Drive:	Samsung 970 EVO 512 GB NVMe SSD, S/N: S3EVNX0K987654
Condition:	Powered off, no physical damage observed

III. FORENSIC EXAMINATION STEPS

A. Pre-Examination Procedures

Prior to beginning the examination of the digital devices located in the possession of D.M., the following steps were taken to ensure the integrity of the digital devices and the admissibility of the data that is extracted from the devices:

- Obtained search warrant (Case No. 17-MJ-4821) through the U.S. District Court for the District of Columbia on December 10, 2017 to examine the cellular device and the laptop computer located in the possession of D.M.
- Photographed the cellular device and the laptop computer in their received state and assigned each digital device a unique evidence tag in accordance with FBI Digital Evidence Policy 12.4.
- Performed the digital forensic examination of the cellular and laptop computer within an isolated laboratory that was shielded from the surrounding environment to prevent any remote wiping or data removal from the cellular device.

All tools utilized in the forensic examination were determined to be forensically sound and are of the current version numbers and license types listed below:

B. Cellular Device Examination

The following steps were taken to preserve and examine the data derived from Item 1 (Apple iPhone 8 Plus):

Airplane Mode / Network Isolation

Because the device was already powered on and locked, it was immediately placed in a Faraday bag upon its receipt. The device was then transported to the isolated examination lab, where it was removed from the Faraday bag only after confirming that all wireless communication protocols within the lab were disabled.

SIM Card Extraction

Using a forensic SIM card reader (UFED SIM Cloner), the SIM card was extracted from the device. The SIM card was analyzed using Oxygen Forensics Forensics Detective v.11.2 to recover the contacts, SMS and MMS messages, and call logs stored on the SIM card.

Device Logical Acquisition

Using Oxygen Forensics Detective v.11.2 connected to the device via a forensic USB cable and the Apple Mobile Device support software, a logical acquisition of the device was performed. During the investigation, the applications data, iMessages, call logs, contacts, pictures, and location data was acquired from the device. The acquired data was hashed with an MD5 hash value of: b3d4e7f1a2c9820d4f5e6b7c8d9e0f1a.

Contact and SMS Messages

Using the software previously utilized to extract the SIM card data (Oxygen Forensics Detective), the contacts and SMS messages from the device were indexed and reviewed. The messages were exported in PDF and CSV file formats. One of the contacts saved to the device by the user was under the name “Red Ralph” and had a saved Russian phone number. The text message to this individual stated that the two were to meet for lunch on February 15, 20XX.

C. Laptop Computer Examination

To examine the data contained within Item 2 (laptop), the following steps were performed:

Hardware Write-Blocker Connection

The internal SSD drive of the laptop was connected to the examination machine via a Tableau TX1 hardware write-blocker. This hardware write-blocker ensures that no writes are performed to the original media.

Forensic Imaging

A forensic image of the internal SSD drive of the laptop was created using FTK Imager v4.5. The image was successfully created. Hash values of the image are as follows:

MD5: f3c4d5e6a7b8c9d0e1f2a3b4c5d6e7f8

SHA-256: a1b2c3d4e5f67890abcdef1234567890abcdef1234567890abcdef1234567890

String and Keyword Searches

The forensic image of the SSD drive was mounted into Autopsy v4.19. The image was indexed for keyword searching. Keywords searched for included: Red Ralph, Big Apple, consulting, payment, classified, transfer, and upload.

Email and Internet Evidence Review

The Internet Evidence Finder (IEF) v6.8 software was used to review browser history and cached e-mails of the laptop. Cached e-mails were located at the following location on the drive: C:\Users[Subject]\AppData\Local\Microsoft\Outlook\ The software revealed an e-mail thread between the laptop owner and RedRalph@gmail.com with the following content:

Email 1 - From: RedRalph@gmail.com | To: Senator Smith | Date: February 21, 2016, 11:35 AM EST | Subject: The Big Apple

Let me know when you are ready for me to discuss about taking out the Big Apple.

Email 2 - From: RedRalph@gmail.com | To: Senator Smith | Date: February 22, 2016, 10:27 AM EST | Subject: The Big Apple

Thank you for meeting. Transfer the money by 06:00 by Friday.

Email 3 - From: RedRalph@gmail.com | To: Senator Smith | Date: February 26, 2016, 11:35 AM EST | Subject: The Big Apple

Thank you for the cooperation. Meet me at the outpost on Saint Patrick's Day at 0700 hours EST. The objective will be complete 30 minutes before.

Deleted File Recovery

Files that were previously deleted from the laptop were recovered from unallocated space using Autopsy v4.19 and the PhotoRec file recovery application. Files recovered include three ZIP archives, which contained government classified information, a text file named "Objective Complete," and a text file named "Smith to Ralph."

Cryptographic Hash Verification of All Evidence

An MD5 hash value was generated for each of the files that were recovered from the SSD drive. These values will allow for any future examinations of these same files to ensure that they have not been altered from their original state.

IV. HARDWARE AND SOFTWARE USED

Hardware

Tableau TX1 Forensic Imager / Write-Blocker

The Tableau TX1 write-blocker was used to safely connect the Samsung 970 EVO drive to the examination machine without making any writes to the original media. The product information can be located at the following link: https://www.guidancesoftware.com/tableau

UFED SIM Cloner (Cellebrite)

The UFED SIM cloner was used to extract the SIM card from the submitted cellular device.

Faraday Isolation Bag

A Faraday isolation bag was utilized to prevent any wireless communications from the cellular device.

Examination Workstation

The examination workstation has the following specifications: Dell Precision 7920 Tower, 64 GB RAM, Windows 10 Pro

Software

Oxygen Forensics Detective v11.2

The Oxygen Forensics Detective software was used to acquire an image of the iPhone and the SIM card data.

FTK Imager v4.5 (AccessData)

FTK Imager was used to create a forensic image of the SSD drive of the laptop, and to calculate its MD5 and SHA-256 hash values.

Autopsy v4.19 (Basis Technology)

Autopsy was used to mount the forensic image of the SSD drive and to search for keywords on the drive. Additionally, Autopsy was used to recover deleted files from the SSD drive.

Internet Evidence Finder (IEF) v6.8 (Magnet Forensics)

The Internet Evidence Finder was used to review the browser history and cached e-mails of the laptop.

PhotoRec

The PhotoRec application was used in conjunction with Autopsy to recover the previously deleted ZIP files from unallocated space on the SSD drive.

V. RESULTS AND CONCLUSIONS

An examination of the SSD drive of the laptop revealed several important findings. The investigations of both Item 1 (laptop) and Item 2 (iPhone) led to the discovery of the individual named RedRalph, who is connected to the laptop's owner (a high-ranking government official). More specifically, the results of the investigation of Item 2 (laptop) lead to the following conclusions:

Finding 1 - Covert Communications with a Foreign National

An SMS text message on the iPhone indicates that there was to be a meeting between the owner of the device and RedRalph. Furthermore, the text message indicates to RedRalph that he is not to bring any written materials to the meeting (instead, he is to "keep it clean"), indicating that there was some knowledge of potential surveillance of the meeting.

Three different e-mails were recovered from the laptop that were sent from RedRalph to the laptop owner. The e-mails indicated that the two individuals were to meet in person, and that RedRalph was to transfer money to the laptop owner.

Finding 2 - Financial Transactions / Payment for Services

An indication of money transfer was made within Email 2 of the thread initiated by RedRalph to the laptop owner. The content of the e-mail stated that RedRalph was to “transfer the money by 06:00 by Friday.” Thus, money was to be transferred between the two parties; an act that indicates a transfer of services between the two individuals.

Moreover, additional files (discussed in Finding 4) help to explain the reason for this payment to RedRalph.

Finding 3 - Unauthorized Upload of Classified Material

Three ZIP archive files were recovered from the SSD drive of the laptop. Upon opening these files with a ZIP application, revealed that the files contained several classified government documents.

Additionally, browsing history of the laptop revealed that the owner visited the file-sharing website dropbox-xfer[.]ru. Furthermore, a web log inspection of that browser history revealed that files were uploaded to that website. While it is unknown whether any third parties accessed those uploaded files, the upload of classified government material to a third-party file sharing website indicates a potential violation of 18 U.S.C. § 1030.

Finding 4 - Deleted Files Confirming Completion of Objective

Two text files were deleted from the laptop but were recovered with the investigation. The files included “Objective Complete” and “Smith to Ralph.”

Objective Complete: Senator Smith, the objective is complete. The Big Apple has been taken out.

Smith to Ralph: It was great doing business with you. Now the election can continue just as planned. You have done great.

These two files help to explain the purpose of the entire communication between the laptop owner (a Senator) and RedRalph. Specifically, these files indicate that the objective (which related to the election of Senator Smith) was completed, and that RedRalph was to thank the Senator for his time and efforts.

Finding 5 - Integrity of Original Media

The original media was not damaged during this investigation. Write-blocking hardware was used during the acquisition of the SSD drive. Additionally, MD5 hash values were created prior to and after the acquisition of the SSD drive and its contents. Furthermore, photographs of the items before and after the investigation were taken and archived in the file of the investigation.

VI. EVIDENCE SUMMARY

Item #	Evidence Item	Significance
E-001	SMS Text Message - "Red Ralph" (+7 (922) 555-1543)	Confirmed that the two individuals were to meet; advised to "keep it clean" (no written materials).

E-002	Email Thread - "The Big Apple" (3 emails, RedRalph@gmail.com)	Emails indicated that there was to be an in-person meeting between the two individuals; money indicated to be transferred.
E-003	Deleted ZIP Archives (3 files) containing classified material	Files contained classified government material. Additionally, the owner visited a file sharing website indicating that the files were to be uploaded.
E-004	Deleted text file - "Objective Complete"	Confirmed that the objective (related to election of Senator Smith) has been completed.
E-005	Deleted text file - "Smith to Ralph"	Indicated to RedRalph that the Senator was grateful for the work that he completed, and that the election would continue as planned.
E-006	Browser History - Upload activity to dropbox-xfer[.]ru	Files were uploaded to a third-party website. Thus, the laptop owner may have potentially violated 18 U.S.C. § 1030.

VII. EXAMINER CERTIFICATION

I, Special Agent Jordan M. Reeves, certify that the contents of this report are true and accurate to the best of my knowledge and belief.

_____

Special Agent Jordan M. Reeves

Digital Forensics Unit, FBI Cyber Division

Badge #74821

Date: December 14, 2017