

# **CYSE407/Final Paper**

**John Wilson**

14 Dec 2022

—

CYSE 407 Digital Forensics

—

Professor Bryan Bechard

---

<b>Case Scenario</b>
----------------------

---

You were hired as a forensic expert to investigate alleged contact between US and Russian officials. You performed a forensic analysis on the laptop and cell phone of a high-ranking US government official. During the investigation you found the following:

On the phone - a text confirming a lunch meeting on 2/15/20xx and the phone number was labeled "Red Ralph" in the contact list.

On the laptop - several email communications about meetings and payment for "consulting services" between the official and [RedRalph@gmail.com](mailto:RedRalph@gmail.com)

On the laptop - several deleted zip files of classified material that web logs show were uploaded to a file sharing site. It is not clear if they were downloaded by anyone. The owner of the laptop and phone has "lawyered up" and is not saying anything about what they were doing on either device or any meetings that may have happened.

You are now preparing your official report to the special prosecutor as evidence that may go to court in the future.

---

Case Identifier: 2022-98765  
Date of Receipt: 10/15/2022

**Case Investigator: John Wilson**  
**Identity of Submitter: John Wilson**  
**Name of Forensics Lab: Digital Forensics Laboratories, LLC.**  
**Location of Forensics lab: 1234 Forensics Lab Way**  
**Virginia Beach, VA 23456**

---

### **Items for Examination:**

- ❖ Number of items for examination: 2
- ❖ Item Number 1: Cellular Phone
  - Model Name: Apple iPhone 12
  - Model Number: A2172
  - Serial Name: 79049XXXPRV
  - Model Color: Purple
  - Condition: Water Damaged
- ❖ Item Number 2: Laptop Computer
  - Model Name: Lenovo ThinkPad X1 Carbon
  - Model Number: 20XW00FPUS
  - Serial Name: LTP0000X1C2020
  - Model Color: Black
  - Condition: Excellent

---

### **Findings and Report (Forensics Analysis):**


- ❖ **Item Number One: Cellular Phone**
  - On 15 October 2022, Forensics Technician John Wilson received a cellular phone (known as Item One) in a sealed evidence bag, properly tagged, from Officer Pete Townsend.
  - Warrant for case number 2022-98765 allowing for digital forensics analysis on Item One looking for deleted or undeleted text messages on or about 15 February 2022.
  - Forensics tools used to conduct analysis:
    - Forensics Programs:
      - iMyFone D-Back for iOS (Apple iPhone recovery software)
    - Administrative Programs:
      - Microsoft Word
      - Microsoft Excel
    - Hardware:
      - Dry Rice
      - Plastic Container

- iPhone charging/data cable
  - Blank Solid-State Drive (SSD) (to place image of Item One and analyze so original image on is unmolested)
  - Forensics analysis conducted on Workstation #3 which is a standalone workstation with no internet connectivity. All updates, appropriate calibrations, and safeguards have been set into place.
- Item One was removed from evidence bag and placed in a container of dry rice to attempt to dry the phone for forensics analysis. Because this process takes time, the container was placed into an additional evidence bag, resealed, tagged and was placed in the secured evidence storage safe located at Digital Forensics Laboratories, LLC. Virginia Beach.
  - On 16 October 2022, Item One was removed from evidence bag and checked for operational ability. Powered up Item One and it is fully operational.
  - Item One was powered off and placed into an additional evidence bag, resealed, tagged and placed in the secured evidence storage safe located at Digital Forensics Laboratories, LLC. Virginia Beach.
  - On 19 October 2022, Item One was removed from evidence bag to begin forensics analysis.
  - Item One was plugged in by iPhone charger/data cable to begin the imaging copy process to a blank SSD. Perpetrators provided the passcode (court ordered) so there was no requirement to use password/code techniques.
  - After transferring the clean image onto the SSD. Item One was bagged, sealed, tagged, and placed into secured evidence storage safe located at Digital Forensics Laboratories, LLC. Virginia Beach.
  - With the image from Item One, located on the SSD, I was able to obtain deleted messages sent and received 15 February 2022 to a "Red Ralph"
    - Message#1:
      - 15 February 2022 @0845
      - From: Red Ralph
      - Phone Number: 202-509-6995
      - To: Keyser Soze
      - Phone Number: 757-564-8973

- Message: Need to meet at the regular spot today at 1200. Reservation under "Griswold".
  - Message#2:
    - 15 February 2022 @0849
    - From: Keyser Soze
    - Phone Number: 757-564-8973
    - Phone Number:
    - To: Red Ralph
    - Phone Number: 202-509-6995
    - Message: Got it, can't do the regular place because of GI issues. How about the backup place, Omelets are good there?
  - Message#3:
    - 15 February 2022 @0901
    - From: Red Ralph
    - Phone Number: 202-509-6995
    - To: Keyser Soze
    - Phone Number: 757-564-8973
    - Message: NP. Reservation will still be under "Griswold". Don't forget SDR.
  - Message#4:
    - 15 February 2022 @0849
    - From: Keyser Soze
    - Phone Number: 757-564-8973
    - Phone Number:
    - To: Red Ralph
    - Phone Number: 202-509-6995
    - Message: I don't forget and stop hounding me about this stuff it makes me anxious.
  - On 19 October 2022, Digital Forensics was completed on Item One that satisfies the warrant obligation.
  - Investigator has been notified the forensics on Item One is complete and waiting for Investigator to pick up evidence.
  - ❖ **Item Number Two: Laptop Computer**
    - On 15 October 2022, Forensics Technician John Wilson received a laptop computer (known as Item Two) in a sealed evidence bag properly tagged, from Officer Pete Townsend.
    - Warrant for case number 2022-98765 allowing for digital forensics analysis on Item Two looking for deleted or undeleted email communications about meetings and payment for "consulting services" between the Kayser Soze and [RedRalph@gmail.com](mailto:RedRalph@gmail.com). Additionally, the warrant allows
-

searching for deleted zip files of classified material that web logs show were uploaded to a file sharing site.

- Forensics tools used to conduct analysis:
    - Forensics Programs:
      - Autopsy
      - OSForensics
      - OpenText EnCase
    - Administrative Programs:
      - Microsoft Word
      - Microsoft Excel
    - Hardware:
      - Tool Bench
      - Laptop taking part tools (to disconnect the hard drive so that you can image it.)
      - disk imaging station (with Sata data cable)
      - Blank Solid-State Drive (SSD) (to place image of Item Two and analyze so original image on is unmolested)
      - Forensics analysis conducted on Workstation #3 which is a standalone workstation with no internet connectivity. All updates, appropriate calibrations, and safeguards have been set into place.
  - On 15 October 2022, Item Two was placed in the secured evidence storage safe located at Digital Forensics Laboratories, LLC. Virginia Beach.
  - On 20 October 2022, Item Two was removed from evidence bag to begin forensics analysis.
  - Item Two was taken apart at the work bench and the Hard Disk Drive (HDD) was removed. The HDD was placed into a disk cloning station that will transfer a complete clone of the disk image onto a clean SSD that will be used for analysis.
  - After transferring the clean image onto the SSD. Item Two was bagged, sealed, tagged, and placed into secured evidence storage safe located at Digital Forensics Laboratories, LLC. Virginia Beach.
  - Upon, analysis of the Item Two image four emails was discovered between the assailant and Red Ralph on 01 February 2022.
-

<  \*Untitled - Notepad

File Edit Format View Help

---Original Message-----

MIME-Version: 1.0  
Date: Wed, 01 Feb 2022 09:03:20 -0400  
From: Red Ralph <RedRalph@gmail.com>  
Subject: We need to meet about Ukraine  
Thread-Topic: We need to meet about Ukraine  
Message-ID: <PH0PR06MB9025460817EEED5724C24371A42B9@HUGRWS6MB9025.namprd03.prod.outlook.com>  
To: Kayser Soze <ghostKS@msn.com>

Need to discuss US assistance to Ukraine. ASAP.

-----

---Original Message-----

MIME-Version: 1.0  
Date: Wed, 01 Feb 2022 09:23:43 -0400  
From: Kayser Soze <ghostKS@msn.com>  
Subject: Re: We need to meet about Ukraine  
Thread-Topic: We need to meet about Ukraine  
Message-ID: <PH0PR06MB9025460817EEED5724C24371A42B9@HUGRWS6MB9025.namprd03.prod.outlook.com>  
To: Red Ralph <RedRalph@gmail.com>

Dude, can you be anymore vocal? I thought we were using Green for Ukraine so people dont get suspicious? When do you want to meet? I am busy this week.

-----

---Original Message-----

MIME-Version: 1.0  
Date: Wed, 01 Feb 2022 10:54:22 -0400  
From: Red Ralph <RedRalph@gmail.com>  
Subject: Re: We need to meet about Ukraine  
Thread-Topic: We need to meet about Ukraine  
Message-ID: <PH0PR06MB9025460817EEED5724C24371A42B9@HUGRWS6MB9025.namprd03.prod.outlook.com>  
To: Kayser Soze <ghostKS@msn.com>

03 Feb 2022 at the regular spot.  
And I am the handler here not you so do as your told or I cut your funding.  
and make sure to bleach bit your workspace.

-----

---Original Message-----

MIME-Version: 1.0  
Date: Wed, 01 Feb 2022 11:41:43 -0400  
From: Kayser Soze <ghostKS@msn.com>  
Subject: Re: We need to meet about Ukraine  
Thread-Topic: We need to meet about Ukraine  
Message-ID: <PH0PR06MB9025460817EEED5724C24371A42B9@HUGRWS6MB9025.namprd03.prod.outlook.com>  
To: Red Ralph <RedRalph@gmail.com>

Alright man. You dont have to be such a drag. I will meet you at the regular spot, time, and bone fides.

-----

- In addition more emails were recovered between the assailant and Red Ralph on 7 February 2022.

\*Untitled - Notepad  
File Edit Format View Help  
---Original Message-----  
MIME-Version: 1.0  
Date: Wed, 17 Feb 2022 019:03:20 -0400  
From: Red Ralph <RedRalph@gmail.com>  
Subject: We need to meet about Ukraine  
Thread-Topic: We need to meet about Ukraine  
Message-ID: <PH0PR06MB9025460817EEED5724C24371A42B9@HUGRWS6MB9025.namprd03.prod.outlook.com>  
To: Kayser Soze <ghostKS@msn.com>  
  
Your payment has been made.  
  
-----  
---Original Message-----  
MIME-Version: 1.0  
Date: Wed, 17 Feb 2022 19:23:43 -0400  
From: Kayser Soze <ghostKS@msn.com>  
Subject: Re: We need to meet about Ukraine  
Thread-Topic: We need to meet about Ukraine  
Message-ID: <PH0PR06MB9025460817EEED5724C24371A42B9@HUGRWS6MB9025.namprd03.prod.outlook.com>  
To: Red Ralph <RedRalph@gmail.com>  
  
Dude, where is the rest of the money?  
  
-----  
---Original Message-----  
MIME-Version: 1.0  
Date: Wed, 17 Feb 2022 20:54:22 -0400  
From: Red Ralph <RedRalph@gmail.com>  
Subject: Re: We need to meet about Ukraine  
Thread-Topic: We need to meet about Ukraine  
Message-ID: <PH0PR06MB9025460817EEED5724C24371A42B9@HUGRWS6MB9025.namprd03.prod.outlook.com>  
To: Kayser Soze <ghostKS@msn.com>  
  
That is it, you get what you provided. You did not provide all the information I requested  
You provided half and some data was corrupted. Did you encrypt it?  
  
-----  
---Original Message-----  
MIME-Version: 1.0  
Date: Wed, 17 Feb 2022 21:41:43 -0400  
From: Kayser Soze <ghostKS@msn.com>  
Subject: Re: We need to meet about Ukraine  
Thread-Topic: We need to meet about Ukraine  
Message-ID: <PH0PR06MB9025460817EEED5724C24371A42B9@HUGRWS6MB9025.namprd03.prod.outlook.com>  
To: Red Ralph <RedRalph@gmail.com>  
  
I did encrypt and you will get the key once I get my money. No pay, no play.]  
  
-----

- No other evidence could be located on Item Two.
- On 20 October 2022, Digital Forensics was completed on Item Two that satisfies the warrant obligation.
- Item Two was placed into an evidence bag, resealed, tagged, and placed into secured evidence storage safe located at Digital Forensics Laboratories, LLC. Virginia Beach.
- Investigator has been notified the forensics on Item Two is complete and waiting for Investigator to pick up evidence.

---

## Conclusion:

The Forensic investigation found direct digital evidence of communication between the perpetrator (Kayser Soze) and the Russian Official (aka Red Ralph) through text messages and email messages.

The text messages were discovered from Item One dated 15 February 2022 and indicated a lunch meeting at an unknown location that serves omelets because the perp has GI (possibly Gastric Intestinal) issues. No other evidence was found on Item One

Deleted email messages were discovered on Item Two dated 01 February 2022 and 17 February 2022.

The email messages dated for 01 February was coordinating a meeting between the perpetrator (Kayser Soze) and the Russian Official (aka Red Ralph) coordinating a meeting at an unknown location to talk about the current US assistance of Ukraine. In addition, safety controls of bone fides are being applied prior to the meeting taking place which could further indicate perpetrator has been trained in the use of trade craft.

The email messages dated for 17 February were to confirm payment for services rendered. Additionally, a disagreement over payment total was also discussed between the perpetrator (Kayser Soze) and the Russian Official (aka Red Ralph). The perpetrator was not satisfied with the amount and was holding an unencrypting key to unknown documents as hostage for more money.

No other evidence was discovered.

- ❖ Number of items examined: 2
    - Item Number 1: Cellular Phone
    - Item Number 2: Laptop Computer
  - ❖ Evidence found:
    - Text messages from Item One
    - Emails from Item Two
    - Evidence legally discovered was placed on an external HDD identified as HDD-2022-98765 and placed with the original evidence waiting for pickup from investigator
  - ❖ Analysis Time total (start to finish) evidence (billing the requesting organization): 38 hours.
    - 24 hours: Item One
    - 8 hours: Item Two
    - 4 hours: Analysis write up
    - 2 hours: Brief Investigating officer and hand over evidence.
  - ❖ During forensics examination no information was altered or hindered throughout the investigative process.
-

- 
- ❖ In the case of loss of evidence, backup copies of this report and evidence are kept on a redundant local backup system and cloud storage device.
  - ❖ For subject matter expert testimony can be requested by the investigating officer or the commonwealth attorney's office. Please provide at least two-weeks advance notice for time to properly prepare.
-