CYSE 407 Digital Forensics Final

By

Ritz Carr

April 25th, 2023

Submitted in partial completion for CYSE 407

Department of Cybersecurity

Old Dominion University

A note: all characters after mentioned are those belonging to the show The Blacklist. President Diaz (referred to as the "Number 15" Blacklister), in the show, had received $300 million from Constantinian Rostov (referred to as the "Number 14" Blacklister), a Russian oligarch and political power, to supply his presidential campaign. The following are the substituted emails/aliases:

Red Ralph > Alexander Kirk

RedRalph@gmail.com> Ak1rk@gmail.com

I. ABSTRACT

This report details the review of the following evidence to support the case: text evidence from President Diaz's phone confirming a lunch meet with "~~Red Ralph~~ Alexander Kirk (alias use in the show)" on February 15th, 2016. On Diaz's laptop, there were multiple email correspondences between himself and Ak1rk@gmail.com regarding meetings and payments for said meetings labelled as "consulting services". Lastly, also found on the laptop were several deleted zip files that were previously classified web logs uploaded to a file sharing site. Unfortunately, it is unclear if anyone had viewed or downloaded the files.

I.II CASE DETAILS

- CASE IDENTIFIER: *Number 14 and Number 15*
- CASE INVESTIGATOR: ARC
- SUBMITTER: RAYMOND REDDINGTON
- DATE OF RECIEPT: May 15th, 2019

II. DETAILED ANALYSIS

II.I ITEMS FOR EXAMINATION

A. **PHONE:** Black Nokia 2760 4G Flip (Diaz is often seen making discreet communications with a flip in the show). Serial Number: 286182047827381
B. **LAPTOP:** A silver 2017 HP Pavilion 360 (Windows) with an AMD 5 core. Serial Number: MYL12345678

II.II DIAZ'S PHONE

A. **TOOLS USED:** SIM Card reader and OpenOffice.
B. **EXAMINATION:**
As a complying witness, President Diaz's secretary provided the password to both the phone and laptop, so I was able to surpass those difficulties and get straight to using the SIM Card Reader. Of course, this was after I acquired a search warrant for the phone.

Using the SIM Card Reader, I then gathered all available text message content and info to examine in an OpenOffice Spreadsheet on my workstation. From here, I was able to confirm that Rostov, alias Alexander Kirk, had sent a text to Diaz to confirm their lunch meeting on February 15th, 2016 at the Blue Pete's Coffee shop. Diaz had read the message, as shown by the spreadsheet in Appendix A. No other correspondence between the parties via text was recorded.

SENDER PHONE NUMBER: +7(992)832-3381
CONTACT NAME: ALEXANDER KIRK
MESSAGE: "Blue Pete's, today, at 0800. -A Kirk"

II.III DIAZ'S LAPTOP

II.III.I EMAILS

A. **TOOLS USED:** EnCase and OSForensics.
B. **EXAMINATION:**
In addition to the search warrant for the phone, I also received a search warrant for the laptop. I proceeded to acquire a forensic copy of the drive with EnCase to examine on my workstation with OSForensics. The password for the laptop was also provided by President Diaz's secretary.

After connecting the laptop to my hardware write-blocker, I completed a sparse acquisition imaging of the drive for email contents and any deleted files specifying to the classified zip files Diaz has uploaded to the file-sharing site.

In OSForensics, I then proceed to mount the image and create an index looking for only emails and their attachments on the entire drive. Once the index was created, I would then string search the index for all instances of "consulting services".

Upon this index, I found an email chain of 5 messages, detailed in Appendix B.

II.III.II DELETED FILES

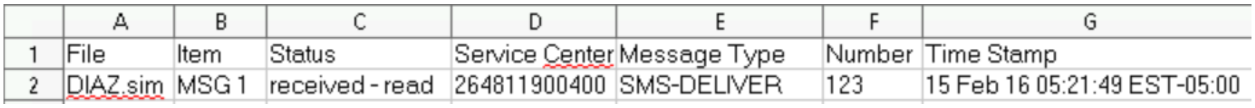
In addition to the emails, I was also able to recover the deleted files of classified information regarding the following: the amount of money transferred from Kirk to Diaz and the bank routing and account numbers, as detailed in Appendix C. I created a new index to include unknown files and string searched for instances of "invest" in the "deleted files" tab of OSForensics. The logs detailed that they were uploaded shortly after their meeting at Blue Pete's.

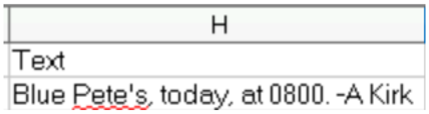
III. CONCLUSION

Overall, the investigation was brief and successful- no files retrieved were found to be altered or corrupted upon creation. The entirety of this investigation was conducted on May 17th, 2019.

IV. EVIDENCE APPENDICES

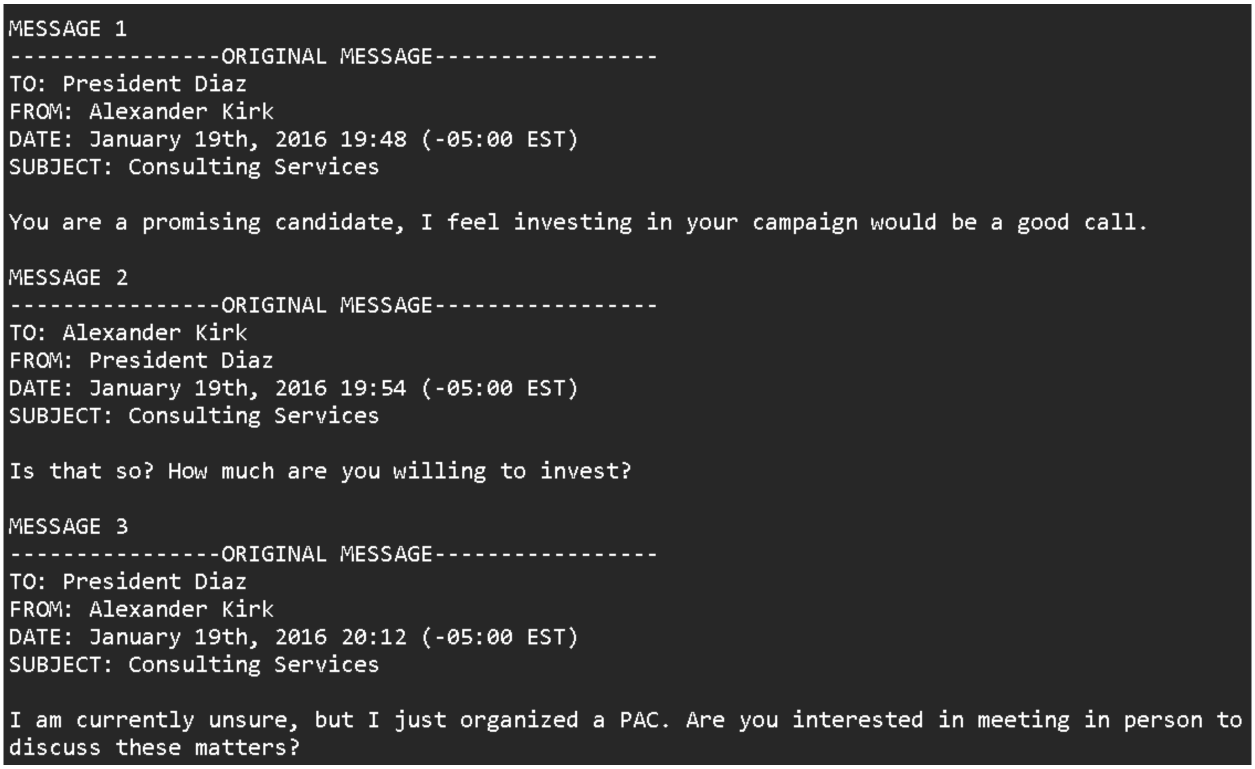
APPENDIX A – PHONE TEXT MESSAGES



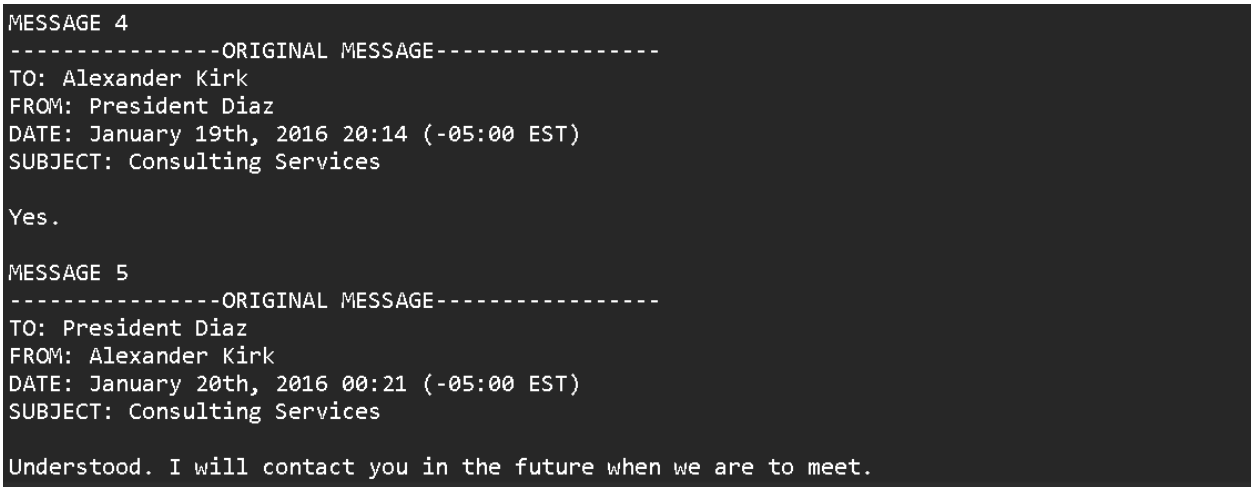


	A	B	C	D	E	F	G	H
1	File	Item	Status	Service Center	Message Type	Number	Time Stamp	Text
2	DIAZ.sim	MSG 1	received - read	264811900400	SMS-DELIVER	123	15 Feb 16 05:21:49 EST-05:00	Blue Pete's, today, at 0800. -A Kirk

APPENDIX B - EMAILS

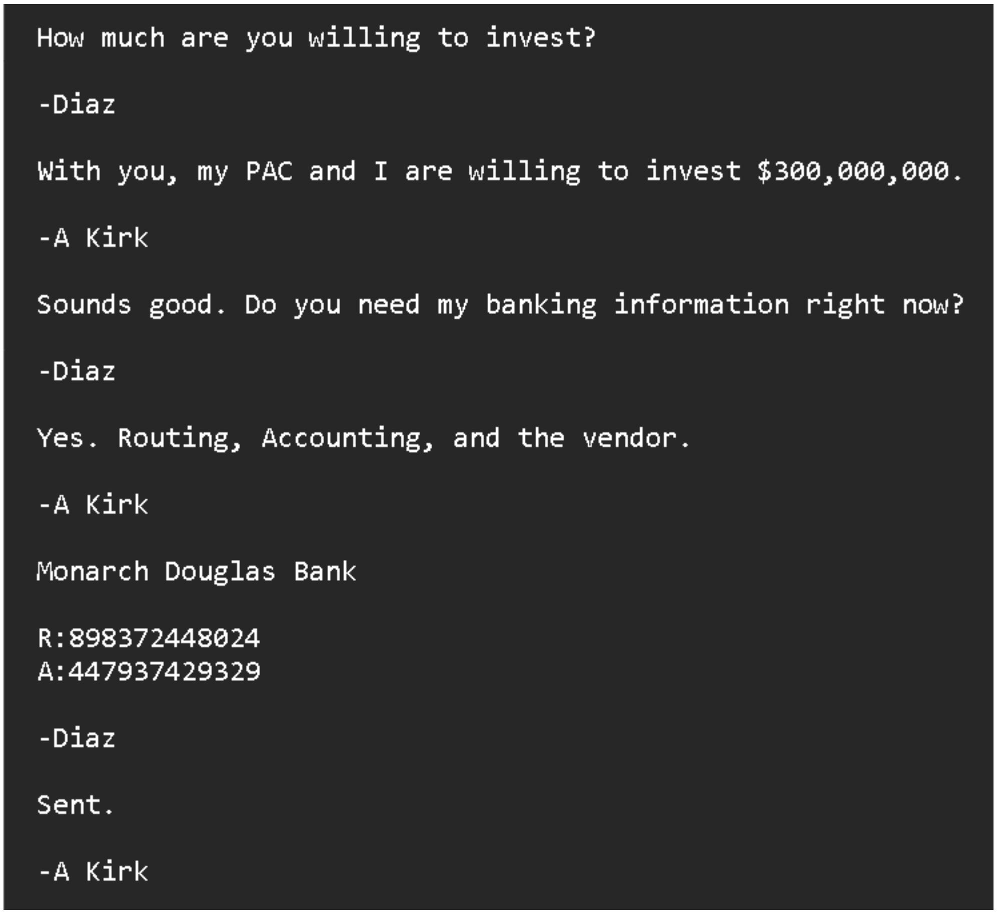


```
MESSAGE 1
----------------ORIGINAL MESSAGE-----------------
TO: President Diaz
FROM: Alexander Kirk
DATE: January 19th, 2016 19:48 (-05:00 EST)
SUBJECT: Consulting Services

You are a promising candidate, I feel investing in your campaign would be a good call.

MESSAGE 2
----------------ORIGINAL MESSAGE-----------------
TO: Alexander Kirk
FROM: President Diaz
DATE: January 19th, 2016 19:54 (-05:00 EST)
SUBJECT: Consulting Services

Is that so? How much are you willing to invest?

MESSAGE 3
----------------ORIGINAL MESSAGE-----------------
TO: President Diaz
FROM: Alexander Kirk
DATE: January 19th, 2016 20:12 (-05:00 EST)
SUBJECT: Consulting Services

I am currently unsure, but I just organized a PAC. Are you interested in meeting in person to
discuss these matters?
```



```
MESSAGE 4
----------------ORIGINAL MESSAGE-----------------
TO: Alexander Kirk
FROM: President Diaz
DATE: January 19th, 2016 20:14 (-05:00 EST)
SUBJECT: Consulting Services

Yes.

MESSAGE 5
----------------ORIGINAL MESSAGE-----------------
TO: President Diaz
FROM: Alexander Kirk
DATE: January 20th, 2016 00:21 (-05:00 EST)
SUBJECT: Consulting Services

Understood. I will contact you in the future when we are to meet.
```

APPENDIX C – DELETED FILES



```
How much are you willing to invest?

-Diaz

With you, my PAC and I are willing to invest $300,000,000.

-A Kirk

Sounds good. Do you need my banking information right now?

-Diaz

Yes. Routing, Accounting, and the vendor.

-A Kirk

Monarch Douglas Bank

R:898372448024
A:447937429329

-Diaz

Sent.

-A Kirk
```