

|  |
| --- |
| **Sports Competition Corruption Case Study**  *Investigating three provided .pcap files using modern digital forensics techniques, looking for specified evidence of corruption and recovering it in a forensically sound manner.*  **Mikołaj Mróz (2003114)**  CMP408: Advanced Digital Forensics  2022/23 |

Contents

[Introduction 5](#_Toc122269183)

[Methodology 5](#_Toc122269184)

[Preparation 5](#_Toc122269185)

[Extraction 6](#_Toc122269186)

[Analysis 6](#_Toc122269187)

[Ownership and Possession 6](#_Toc122269188)

[Conclusion 6](#_Toc122269189)

[Tools 7](#_Toc122269190)

[Establishing Context 7](#_Toc122269191)

[Correlation 7](#_Toc122269192)

[Timeline of Events 7](#_Toc122269193)

[Corroboration 8](#_Toc122269194)

[Suspects 8](#_Toc122269195)

[Interpretation 9](#_Toc122269196)

[Evaluation 9](#_Toc122269197)

[Reflection 9](#_Toc122269198)

[Appendix 1 - Investigative Working 10](#_Toc122269199)

[Capture 1.pcap 10](#_Toc122269200)

[Packet Analysis 10](#_Toc122269201)

[Server Message Block (SMB) Objects 11](#_Toc122269202)

[Hypertext Transfer Protocol (HTTP) Objects 13](#_Toc122269203)

[Capture 2.pcap 15](#_Toc122269204)

[FTP Traffic 15](#_Toc122269205)

[HTTP Traffic 16](#_Toc122269206)

[Capture 3.pcap 17](#_Toc122269207)

[Appendix 2 – Extra Screenshots 19](#_Toc122269208)

[Appendix 3 – Relevant Output 20](#_Toc122269209)

[Appendix 3A – SMB Folder Contents + Decoded 20](#_Toc122269210)

[Appendix 3B – Docs.pcap contents 22](#_Toc122269211)

[Appendix 3C – Text Coordinates 33](#_Toc122269212)

[Appendix 3D – Jigsaw Images Output 36](#_Toc122269213)

[Appendix 3E – Wireshark Output 37](#_Toc122269214)

[Edward Snowden to Julian Assange (Docs.pcap) [11-Jul-2014 16:03:55] 37](#_Toc122269215)

[Edward Snowden to Julian Assange (Hello Friend…) [11-Jul-2014 14:03] 37](#_Toc122269216)

[Julian Assange to Edward Snowden (I will look at that pcap…) [11-Jul-2014 16:07:20] 38](#_Toc122269217)

[The Gza to Kim Ill-Song (Bold Claim…) [Date Unknown] 39](#_Toc122269218)

[Kim Ill-Song to The Gza (Ask and you shall receive… 34jdsioj.zip, breaking\_bad\_season\_6.zip) [03-Jul-2014 16:19:42] 39](#_Toc122269219)

[Kim Ill-Song to The Gza (canc3l.zip transfer) [03-Jul-2014 16:22:05] 40](#_Toc122269220)

[Appendix 3F – Capture 3.pcap Text Messages 41](#_Toc122269221)

[Appendix 4 – Commands and Code 43](#_Toc122269222)

[Appendix 4A – Foremost 43](#_Toc122269223)

[Appendix 4B - Cat 43](#_Toc122269224)

[References 44](#_Toc122269225)

# Introduction

This case study was produced by request of a national security agency to investigate an international sporting corruption case. Three network capture files were provided by the agency for the investigation, named “Capture 1.pcap, Capture 2.pcap, and Capture 3.pcap” respectively, each with a distinct set of data and aims defined by the client.

Capture 1.pcap

The client requested an investigation into a potential case of bribery present within this packet capture; it was said to contain an undefined number of suspect details including names, aliases, and usernames, some of which may be obscured through the use of anti-forensic obfuscation techniques. The aim of the investigation into this packet is to recover said actor details and to describe the obfuscation techniques used and process of recovery.

Capture 2.pcap

This file contains communications between a competition official and a foreign national agent and is described as containing File Transfer Protocol (FTP) traffic as well as other network packet types, indicating the exchange of confidential virtual files or folders. More forensic obfuscation techniques have been utilized in this exchange, with the client providing the clue that an Edward Snowden quote can aid in the deciphering process. The client asks for evidence of the files that were sent over, including a documented process of how this was deciphered and extracted.

Capture 3.pcap

The third Capture file details communications between the actors Ill-Song and Ann Dercover, which the client suspects are attempting to schedule a discreet meeting. Details of the conversation (particularly the date and time of their meeting) are requested to be recovered for investigation purposes.

# Methodology

The use of a traditional forensic acquisition and analysis methodology such as OSCAR (Obtain Information, Strategize, Collect Evidence, Analyse, Report) would be ineffective throughout this investigation as the acquisition process has already been completed by the client and only the analysis and reporting stages need to be performed. In this instance, a more dynamic methodology focused on the analysis of network traffic needs to be utilized such as the Evidence Examination framework described in the US Department of Justice report: ‘Forensic Examination of Digital Evidence: A Guide for Law Enforcement’ (Ashcroft, et al., 2004). This was done following the steps mentioned in this guide – Preparation, Extraction, Analysis, Ownership and Possession, and finally Conclusion.

## Preparation

The preparation phase relates to getting the working directories ready to place extracted and recovered files into. The report recommends using separate media to store these files, however a simple desktop folder covered these requirements in this case. This is because the files do not need to be passed between investigators; this is an individual investigation with the results being passed on immediately to the client.

## Extraction

As this is an entirely network packet-based investigation, typical operating system forensic methods mentioned in the standard methodology do not apply; the procedure instead focuses entirely on recovering requested data from the provided packet files.

This includes the following:

* Sent files and messages identified by Wireshark
* Names and aliases
* IP addresses
* Suspicious port activity
* Compressed data
* Obfuscated data
* Encrypted data

**(The gathered data and working can be viewed in Appendix 1 of the Investigative Output file.)**

## Analysis

Analysis is the act of recovering and understanding evidence from gathered data; it typically begins at the initial leads that triggers the investigation to be called such as noticeable network anomalies, compromised systems, or Intrusion Detection System alerts. Ashcroft et al’s Guide For Law Enforcement only covers the analysis of disk image contents, though in this case, the trigger was suspicious network packets. Data Analysis (and inherently, network packet analysis) requires the use of the following methods to develop a working conclusion, as noted by the European Union Agency for Cybersecurity (ENISA, 2016):

1. Correlation – Gathering data from multiple sources to draw conclusions.
2. Timeline – Creating a timeline from the gathered evidence.

## Ownership and Possession

To cover the requirements for establishing ‘Ownership and Possession,’ the following topics were investigated within the given files, building off the previous two steps of analysis.

1. Events of Interest – Noting particular events that stand out or relate to the aims of the investigation.
2. Corroboration – Verifying potential false positives using other sources.

## Conclusion

Finally, a conclusion was reached through the use of interpretation based on all the evidence gathered.

1. Interpretation – Developing a working theory on the events that transpired.

# Tools

|  |  |
| --- | --- |
| Wireshark | Used to investigate internet packet capture files and export their contents where appropriate. |
| Foremost | A tool build to export hidden files and folders. |
| Autopsy | An all-rounder GUI forensics tool used to uncover file metadata and other hidden information. |
| Notepad | Enables the viewing of text files and raw file content, regardless of its extension or corrupted status. |
| HxD | Outputs raw file content and hexadecimal information of files, used to locate magic numbers. |
| Binwalk | Finds and outputs hidden files. |
| MyGeoData.com | Produces pins on a Google map from a CSV file, used to piece together clues from Capture 3. (MyGeodata, 2022) |
| Microsoft Excel | Opens CSV files, particularly used for WireShark packet exports and coordinate data. |
| Base64decode.com | Decodes Base64 into readable text. (base64decode, 2022) |

# Establishing Context

## Correlation

To provide the best basis for an analysis of the results, all three packet capture files were investigated and had all found relevant data extracted into the Investigative Output folder before the case study was performed. The packets were investigated using the strategy defined in the Extraction part of the methodology, first gathering and investigating transferred SMB and HTTP files before studying the contents of individual packet transfers to narrow down potential activity.

## Timeline of Events

|  |  |  |
| --- | --- | --- |
| Date | Event of Interest | Appendix |
| 20th June 2014  [21:21 – 21:25] | Edward Snowden captures the contents of Docs.pcap, later sent to Julian Assange. This includes numerous searches from 172.29.1.17 for websites and blogs relating to surviving Russian winters, hotel bookings, and studying Julian Assange on Wikipedia. | 3B |
| 2nd July 2014  [22:38 – 22:50] | Ann Dercover and Kim Ill-Song (Castling) exchange coordinates for their meetup at 5PM on the 17th of September at their old meetup spot. | 3F |
| 3rd July 2014  [16:19 – 16:22] | Kim Ill-Song sends The Gza canc3l.zip, 34jdsioj.zip, breaking\_bad\_season\_6.zip and other files containing broken JPGs that could be put together to form pictures of a Gundam robot, Kim Jong Un, and a chessboard. | 3E – Kim Ill-Song to The Gza |
| 11th July 2014  [14:03 – 16:07] | Edward Snowden and Julian Assange exchange DocsPcap.zip and Documents.zip, containing a pcap capture file of Russian Google searches and a list of potential suspects in a Wu Tang Clan lyrics file track6.docx respectively. | 3E – Edward Snowden to Julian Assange |
| 17th September 2014  [17:00 - ??:??] | Ann Dercover and Kim Ill-Song are expected to meet at their usual meetup spot. Kim Ill-Song uses the alias “Castling” in this exchange, tying back to the 3rd of July where a picture of a chessboard was sent (Castling is a chess term) (Chessbase, 2022). | 3F |

## Corroboration

Any extracted data that does not relate to the client’s requests or potential suspects was discarded, which greatly helped in narrowing the searching aspect of the investigation. This includes irrelevant WireShark packet transfers, Google searches, and image downloads. Throughout the investigation, a large number of files were found to be downloaded most likely without the subject’s knowledge, including default website images, thumbnails, profile pictures and website adverts, and were not included in the appendices due to their irrelevant nature.

## Suspects

|  |  |  |
| --- | --- | --- |
| Suspect Name | Alias | Links |
| Kim Ill-Song | kim.illsong@aol.com / Castling | * Communicated with The Gza, sending images hidden behind an Edward Snowden quote. * Spoke with Ann Dercover, saying they are behind the bribes. * Uses the alias “Castling”, a chess term, tying them to the documents that were sent to The Gza. * Mentioned in track6.docx |
| Mr. Method |  | * Mentioned only in track6.docx |
| Mr. Razor |  |
| Mr. G. Killah |  |
| Matt Cassel |  |
| Mr. I. Deck |  |
| Mr. M Killa |  |
| Mr. O.D.B. |  |
| Mr. Raekwon |  |
| Mr. U-God |  |
| Mr. Cappadonna |  |
| John Woo? |  |
| Mr. Nas |  |
| Ann Dercover |  | * Communicated with Kim Ill-Song/Castling and planned a meetup on the 17th of September. |
| Edward Snowden | snowedinedward@aol.com | * Captured and sent Docs.pcap * Communicated with Julian Assange via email * Sent Documents.zip containing the list of possible subjects in track6.docx. |
| Julian Assange | [wikiofleaks@aol.com](mailto:wikiofleaks@aol.com) | * Called “friend” by Edward Snowden * Received files from Snowden * Searched up on Wikipedia in Docs.pcap |
| Mr. Genius | The Gza / [da.genius36@aol.com](mailto:da.genius36@aol.com) | * Communicated with Kim Ill-Song * Named after the Wu Tang Clan member GZA, communicated with Kim who hid messages in Wu Tang Clan lyrics. |
| Bryan Schmidt |  | * Editor of all the files sent to Julian Assange in Documents.zip |
| Eric |  | * Owner of track6.docx and track10.docx |

## Interpretation

From the results of the investigation, one main theory can be created. Kim Ill-Song (Castling) is the one who is behind the bribes at the competition, as stated by themselves in text messages with Ann Dercover who also likely has ties to the bribes. While investigating this suspect, items related to North Korea were discovered - NK.jpg, NorthKorea.jpeg, and fullImage3 (Kim Jong Un Jigsaw) -possibly showing their activity is tied to the North Korean government. The suspect also shares a similar name with a previous leader of North Korea, “Kim Il-Sung”. The remaining images that were concatenated all have something to do with this suspect – fullImage (Chessboard – alias “Castling”), fullImage2 (Gundam – Season 1 features a character called Kim), and fullImage3 (Kim Jong Un’s portrait).

It can be assumed that Kim, The Gza, and Ann Dercover work together due to the texts and emails that were exchanged among them. Firstly, Ann said that the meeting planned over text with Kim would take place at the “usual spot”, suggesting they have met at least once before possibly to create plans. Secondly, Kim was found to be sending The Gza documents over email, meaning The Gza is either a higher-up member of the group or a co-conspirator.

# Evaluation

There were a number of points throughout the investigation that were found to be quite challenging. Firstly, reassembling the images sent by Kim Ill-Song to The Gza. Attempting to piece the images from the first found folder alone resulted in failure and prompted further investigation into the missing words. However, the client’s hint that an Edward Snowden quote was the key to unlocking this greatly helped in this case, as it suggested there were other files to be found.

This challenge extends to piecing together the pictures of the Gundam and Kim Jong Un as no hints were found for those two pictures and they had to be put together through many failed attempts until the pictures were complete and were ultimately necessary to hint that Kim Ill-Song was behind the bribe. Figuring out how to convert the MapQuest coordinates into a working CSV file and researching the possible ways of placing this data on a map also required outside research which added to the challenge. Furthermore, a large number of possible suspects were found, and all had to be investigated thoroughly through all the found files. This, of course, resulted in no further information being found about the members listed in track6.docx that were not already known to be acting maliciously and required a lot of time to investigate for no outcome at all.

# Reflection

Anti-forensic obfuscation and confusion techniques continue to become more advanced with each passing year as technology grows. Hackers are getting increasingly creative with these methods, hiding protocols under different port numbers, encrypting and compressing data, and using steganography to hide data within other files. Modern forensic investigations must account for all of these techniques as shown in “Extraction”, greatly increasing the amount of time an investigator spends looking for relevant data.

One of the most prominent Digital Forensic agents of recent times – Simson Garfinkel – writes that the use of anti-forensic techniques ultimately means that attackers are more likely to get away with malicious activity than those who choose not to employ the techniques mentioned throughout the paper, and that the tools that can confound forensics investigations may end up becoming banned outright due to how effective they really are (Garfinkel, 2007).

# Appendix 1 - Investigative Working

## Capture 1.pcap

### Packet Analysis

Viewing the data send using the SMB protocol in Wireshark (Figure 1) revealed a number of files sent across the network, displaying the workstation these files came from as DOG-WS.

Graphical user interface, text, application

Description automatically generated

Figure 1 - A list of reconstructed files from the Wireshark Export SMB list

Investigating the SMB packet transfer requests under the name “DOG-WS” shows that workstation these files came from has the IP address 172.29.1.23 and the destination is a device with the IP address 172.29.1.20 (Figure 2).

Graphical user interface, text, application, Word

Description automatically generated

Figure 2 - A WireShark packet info screenshot showing the IP addresses and Ports used within the exchange

A quick word search for ‘DOG-WS’ also revealed a connection to another workstation named FOX-WS in packet 23844 (Figure 3). This is the PC with the IP address of 172.29.1.20.

Graphical user interface, text, application

Description automatically generated

Figure 3 - Viewing packet 23844 shows DOG-WS and FOX-WS to be directly interacting over the network

### Server Message Block (SMB) Objects

Exporting all the SMB objects found within the packet capture (Figure 1) into a folder on the desktop revealed five .ini files with no relevant information and a srvscd file, which is used by Windows to pipe files across a network (Microsoft, 2020).

Documents.zip contained four folders – ‘More Documents,’ ‘Enter the WuTang,’ ‘Chess Boxing,’ ‘Actual Documents’, and another ZIP folder called ‘untitled folder.zip’. Opening ‘More Documents’ revealed NorthKorea.jpg (a picture of the North Korean flag) and BillofRights.txt, a file containing the American Bill of Rights.

The remainder of the files within these folders had their contents encrypted in base64 and had to be decoded using base64decode.org (2022). This revealed the following content, of which only track6.docx is relevant to the scandal. The complete file details are available at Appendix 2A.

|  |  |  |
| --- | --- | --- |
| Actual Documents | | |
| FILENAME | **CONTENT** | **RELEVANT** |
| GoT Spoilers.docx | Contains spoilers for Game of Thrones | No |
| NorthKorea.docx | Russian text theorizing that North Korea have developed a time travel device | No |
| PiD.docx | Shows an Email exchange between a man named William Campbell and a mailer trying to prove that he is not Paul McCartney. (PiD = Paul is Dead) | No |

Table 1 – Actual Documents contents

|  |  |  |
| --- | --- | --- |
| Chess Boxing | | |
| FILENAME | **CONTENT** | **RELEVANT** |
| NK.jpg | A picture of the North Korean flag | No |
| Rules1..docx – Rules7.docx | Rules for Chess Boxing | No |

Table 2 – Chess Boxing contents

|  |  |  |
| --- | --- | --- |
| Enter the Wu Tang | | |
| FILENAME | **CONTENT** | **RELEVANT** |
| track6.docx | **Shows a list of usernames associated with “The Mystery of Chess Boxing,” which are possible conspirators in this case.**  **“**Mr. Method  Kim Ill-Song  Mr. Razor  Mr. Genius  Mr. G. Killah  Matt Cassel  Mr. I. Deck  Mr. M Killa  Mr. O.D.B.  Mr. Raekwon  Mr. U-God  Mr. Cappadonna (possibly)  John Woo?  Mr. Nas” | **Yes** |
| track10.docx | Song Lyrics | No |

Table 3 – Enter the Wu Tang contents

Within untitled folder.zip was an empty folder called ‘SilentEye’ nested within an additional four folders named with variations of ‘untitled folder.’ This suggests the subject used the ‘SilentEye’ tool to hide data within files.

Analysing the metadata of the files in Documents.zip using Autopsy (Figure 4) displays two names – Bryan Schmidt, Owner of track6.docx and track 10.docx, and ‘Eric’, Owner of the rest of the files listed above. It also shows that NorthKorea.jpeg has hidden files in it, shown by analyzing the text output of the file (Figure 5).

Graphical user interface, text, application

Description automatically generated

Figure 4 - Metadata analysis of the files sent over in Documents.zip

Text, timeline

Description automatically generated

Figure 5 - Hidden folder and python file within NorthKorea.jpeg

Scanning the jpeg with Foremost, a file carving program, outputs a folder called untitled.zip that contains a python file called broken.py. It appeared to be a broken version of the encoding algorithm used by the suspect (the full broken.py file can be viewed in Appendix 3A).

### Hypertext Transfer Protocol (HTTP) Objects

Viewing the HTTP objects in Wireshark for Capture 1 showed a large octet stream file received from mail.aol.com, an email client.

Graphical user interface, text, application, chat or text message

Description automatically generated

Figure 6 - HTTP Object list

Investigating the packets that display when setting the http.referer filter to "http://mail.aol.com/38629-111/aol-6/en-us/Suite.aspx" revealed two suspect names, Edward Snowden (and his email snowedinedward@aol.com) and Julian Assange (wikiofleaks@aol.com), as well as the email messages they exchanged.



Figure 7 - wikiofleaks and snowedinedward exchanging emails

Opening the HTTP stream displays the emails that were sent, discussing the sending of a .pcap (packet capture) file related to the recent scandal and some documents. Snowden also calls Assange “Friend”, suggesting they are close with each other and are working together. (The full wireshark output of the conversation is available in Appendix 3E).

Text

Description automatically generated

Figure 8 - HTTP Stream contents from the email exchange

|  |  |
| --- | --- |
| Edward Snowden | Hello friend, I have a pcap I would like you to look through. Could be useful. |
| Julian Assange | I will look at that pcap as soon as I can. Can you also send me the documents you have collected during research of that recent scandal. |
| Edward Snowden | I will do so as soon as I can. |

Table 4 – A Conversation between Snowden and Assange related to a pcap file

Exporting the file from Figure 5 creates an unopenable file in the export location. However, opening it in a Hex editor such as HxD displayed the magic number of the file and its filename, showing it was called “DocsPcap.zip”, containing a file called ‘Docs.pcap’, and it has the appropriate magic number (50 4B 03 04) to be a zipped archive (Wikipedia, 2022).

Text

Description automatically generated

Figure 9 - Hexadecimal analysis of the extracted file

This file was extracted from the stream using the appropriate Foremost command (shown in Appendix 4A), and a zip was found containing the mentioned pcap file.

A screenshot of a computer

Description automatically generated

Figure 10 - Foremost audit.txt file for the stream

The Docs.pcap file did not have much information directly related to the scandal, but the user who captured the packets also captured data regarding google searches made by a subject (FOX-WS, 172.29.1.17) through DNS and it contains a number of Russian websites and searches implying the subject was planning a vacation to Russia in the winter. There are also searches on Wikipedia for Julian Assange, a conspirator in the case.

(The full list of browser searches can be found in Appendix 3B)

## Capture 2.pcap

### FTP Traffic

Viewing the File Transfer Protocol (FTP) traffic in Capture 2.pcap as the client requested shows login attempts from Ill-Song (172.29.1.23) and the returning of two .zip files (ojd34.zip and sandofwhich.zip) from the destination IP address as shown in Figure 11.

Graphical user interface, text

Description automatically generated

Figure 11 - Wireshark FTP traffic from Ill-Song

These attachments come from a series of messages between Kim Ill-Song (kim.illsong@aol.com) and “The Gza” (da.genius36@aol.com). Viewing the data from packets 2665 and 2666 shows these messages as follows (Table 5):

|  |  |
| --- | --- |
| Sender | Content |
| The Gza | You have made a bold claim but I’d like to see some proof. |
| Kim Ill-Song | Ask and you shall receive. You know where to look. |

Table 5 – Communications between The Gza and Kim Ill-Song

After exporting these folders from the “Export Objects > FTP-DATA” menu in WireShark, the contents were determined to be a series of broken JPG files, with only I.jpg showing any sort of corrupted display (Figure 12). The names of these files relate to an Edward Snowden quote, a hint which the client provided. The quote is as follows: “I can't in good conscience allow the U.S. government to destroy privacy, internet freedom and basic liberties for people around the world with this massive surveillance machine they're secretly building.”

A screenshot of a computer

Description automatically generated with medium confidence

Figure 12 - The combined contents of ojd34.zip and sandofwhich.zip

### HTTP Traffic

A number of files relating to the quote were missing, so the RPC.aspx files found in Capture 3 were exported from its HTTP object list (Figure 13) and ran through Foremost as was done with DocsPcap.zip previously. Foremost successfully uncovered the remaining files which were stored in folders ‘34jdsioj,’ ‘breaking\_bad\_season\_6,’ and ‘canc3l’.



Figure 13 - RPC.aspx multipart files containing the remaining zip files

The missing files were then compiled into one folder, and linux’ ‘cat’ command was used to concatenate the files into one (Appendix 4A) in the appropriate order. This resulted in the image of a chessboard being created (Figure 14).

A picture containing wall, indoor

Description automatically generated

Figure 14 - A picture of a chessboard made from multiple jpg files

The files “there.jpg” and “condone.jpg” also had a visible file start section as visible in Figure 12. It was possible to put these files together in a similar manner, the image beginning with ‘there.jpg’ produced a photo of Kim Jong Un, the leader of North Korea, and the image beginning with ‘condone.jpg’ produced a picture of a Gundam mech.

A screenshot of a video game

Description automatically generated with medium confidence

Figure 15 - cat commands and output for the jigsaw files

Binwalk and Foremost were then used to see if the perpetrator had hidden any files in these images but nothing was found.

## Capture 3.pcap

The client requested that communications between Ann Dercover and Ill-Song be recovered from this capture file. As with the other two files, the HTTP objects list was investigated for evidence of any sent files. The object list contained a number of ‘communications’ files, which, when viewed in notepad, showed the following information.

|  |  |  |
| --- | --- | --- |
| Time YYYY:MM:DD HH:MM:SS | Contact | Contents |
| 2014-07-02 22:38:55 | Kim Ill-Song | Good afternoon, Ann. |
| 2014-07-02 22:39:15 | Ann Dercover | Who is this? |
| 2014-07-02 22:39:31 | Kim Ill-Song | Castling. |
| 2014-07-02 22:39:46 | Ann Dercover | Where are you? |
| 2014-07-02 22:40:05 | Kim Ill-Song | I know I can’t tell you that. |
| 2014-07-02 22:41:31 | Ann Dercover | Do you know there are people investigating Kim Ill-Song? |
| 2014-07-02 22:41:47 | Kim Ill-Song | Of course. However, they will never know it is me behind the bribes. |
| 2014-07-02 22:42:54 | Ann Dercover | still we should be careful. Pay attention. I want to meet in September at 5PM. |
| 2014-07-02 22:43:06 | Kim Ill-Song | At our old meetup spot? |
| 2014-07-02 22:43:28 | Ann Dercover | Yes. |
| 2014-07-02 22:43:44 | Kim Ill-Song | What day? |
| 2014-07-02 22:50:32 | Ann Dercover | I told you to pay attention. |

Table 6 – The full text conversation between Kim Ill-Song and Ann Dercover.

Taking a close look at the other packets exchanged in this conversation shows a number of POST and GET requests for MapQuest, a mapping software. Setting the display filter to json.key == “latlng” and adding a Number Value column to WireShark’s display shows the exchanged longitude and latitude coordinates from Ann Dercover sent to Kim Ill-Song.

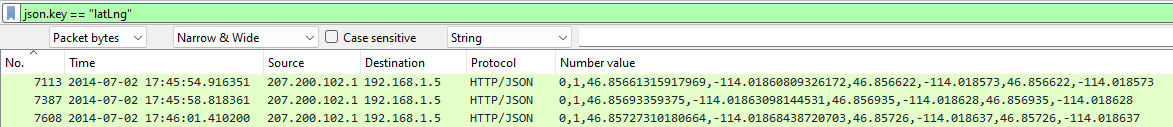


Figure 16 – Coordinates as they appear in Wireshark

The packets that make use of “latLng” notation were then exported as a CSV and cut down to just the first two columns. This is because the rest were duplicates and were rounded up, meaning the results would be less accurate.

Delimiting them again with Excel’s “Data > Text To Columns” feature to divide these values into two columns and uploading the file to MyGeoData showed multiple points on a map of Missoula, Montana in the shape of a 17 suggesting that the two subjects were planning to meet on the 17th of September at 5pm.

Graphical user interface

Description automatically generated with medium confidence

Figure 17 - MyGeoData map pin output

# Appendix 2 – Extra Screenshots

Appendix 2A – An overview of the contents of the three retrieved ZIP files for Capture 1. Note the missing data in the unopenable ZIP and duplication of data.

Graphical user interface, application

Description automatically generated

# Appendix 3 – Relevant Output

## Appendix 3A – SMB Folder Contents + Decoded

NorthKorea.docx

Для кого это может касаться:

Я был свидетелем, что Ким Чен Ун и правительство Северной Кореи разработали программу, которая позволяет им путешествовать во времени. С использованием этой технологии, я считаю, что они намерены двигаться вперед и изменить результаты войны в Корее.

Пожалуйста, Оби-Ван, ты моя единственная надежда.



NK.jpg

Logo

Description automatically generated

track6.docx

VGhlIE15c3Rlcnkgb2YgQ2hlc3MgQm94aW5nOg0KKHVzZXJuYW1lcykNCg0KTXIuIE1ldGhvZA0KDQpLaW0gSWxsLVNvbmcNCg0KTXIuIFJhem9yDQoNCk1yLiBHZW5pdXMNCg0KTXIuIEcuIEtpbGxhaA0KDQpNYXR0IENhc3NlbA0KDQpNci4gSS4gRGVjaw0KDQpNci4gTSBLaWxsYQ0KDQpNci4gTy5ELkIuDQoNCk1yLiBSYWVrd29uDQoNCk1yLiBVLUdvZA0KDQpNci4gQ2FwcGFkb25uYSAocG9zc2libHkpDQoNCkpvaG4gV29vPw0KDQpNci4gTmFzDQo=

----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The Mystery of Chess Boxing:

(usernames)

Mr. Method

Kim Ill-Song

Mr. Razor

Mr. Genius

Mr. G. Killah

Matt Cassel

Mr. I. Deck

Mr. M Killa

Mr. O.D.B.

Mr. Raekwon

Mr. U-God

Mr. Cappadonna (possibly)

John Woo?

Mr. Nas

NorthKorea.jpeg

Logo

Description automatically generated with low confidence

untitled/PK? ìcÓDñˆeÐ\u €¤' untitled/broken.pyPK w ³

broken.py

def fileToString(pathToFile):

f = open(pathToFile, "r")

strs = ""

#adds each line of the file to the strs string

for line in f.readlines():

strs+=line

return strs

def ASCII():

#number of ASCII characters

NumOfASCII == 0

#returns list of all ASCII characters

return "".join([chr(i) for i in range(NumOfASCII)])

def sumName(name):

sums=0

#sums the indices in ASCII of all the characters in name

for x in name:

sums+=ord(x

return sums

def indexInFile(password):

indices = []

ASCIIArray = ASCII()

#populates an array of indices to be used by the encoder

for chrs in password:

indices.append(ASCIIArray.index(chrs)+sumName(name)\*2

return indices

def indexInASCII(name):

indices = []

ASCIIArray = ASCII()

#split on all non-numeric characters

#remove first index because it is blank

indexList = re.split("[^\d]",encoded)[1:]

#converts encoded characters to ASCII

for index in indexList:

indices.append(ASCIIArray[int(index) - (sumName(name)\*2)])

#returns decoded message

return "".join(indices)

def encode(name):

#returns a list of indices to be used for encoding

indices = indexInFile(password,name)

#convert file associated with name to a string

bill = fileToString("./%s.txt"%name)

encoded = ""

#add letter in file plus index of the letter in the file to the encoded string

for index in indices:

encoded+=bill[index]+str(index)

return encoded

## Appendix 3B – Docs.pcap contents

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Time | Source | Destination IP | Content |
| 20 June 2014 | 21:21:52 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x60c6 A www.google.com A 74.125.129.104 A 74.125.129.103 A 74.125.129.106 A 74.125.129.105 A 74.125.129.147 A 74.125.129.99 |
| 20 June 2014 | 21:21:53 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xfc07 A ssl.gstatic.com A 74.125.224.239 A 74.125.224.248 A 74.125.224.247 |
| 20 June 2014 | 21:21:54 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x937f A www.gstatic.com A 74.125.239.111 A 74.125.239.127 A 74.125.239.120 A 74.125.239.119 |
| 20 June 2014 | 21:21:54 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xc6a6 A apis.google.com CNAME plus.l.google.com A 74.125.239.40 A 74.125.239.38 A 74.125.239.34 A 74.125.239.46 A 74.125.239.39 A 74.125.239.32 A 74.125.239.37 A 74.125.239.35 A 74.125.239.33 A 74.125.239.36 A 74.125.239.41 |
| 20 June 2014 | 21:22:11 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xea5e A download.cdn.mozilla.net CNAME 2-01-2967-0010.cdx.cedexis.net CNAME wpc.1237.edgecastcdn.net CNAME gsb1.wpc.v2cdn.net A 93.184.215.248 |
| 20 June 2014 | 21:22:11 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x7d7e A www.gadling.com CNAME win.blogsmith.aol.com CNAME win.blogsmith.aol.com.aol.akadns.net A 207.200.74.18 |
| 20 June 2014 | 21:22:12 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xad88 A www.blogsmithmedia.com CNAME www.blogsmithmedia-ds.com.edgesuite.net CNAME a1983.dscg.akamai.net A 96.17.148.51 A 96.17.148.41 |
| 20 June 2014 | 21:22:12 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x2875 A o.aolcdn.com CNAME o.aolcdn-ds.com.edgesuite.net CNAME a1123.dscg.akamai.net A 184.28.16.65 A 184.28.16.64 |
| 20 June 2014 | 21:22:12 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xe601 A www.aolcdn.com CNAME www.aolcdn-ds.com.edgesuite.net CNAME a1621.dscg.akamai.net A 184.28.16.48 A 184.28.16.19 |
| 20 June 2014 | 21:22:12 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xe707 A switcher.dmn.aol.com CNAME switcher.dmn.aol.com.aol.akadns.net A 207.200.111.147 |
| 20 June 2014 | 21:22:13 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x523e A platform.tumblr.com CNAME dy0k9wscos2ll.cloudfront.net A 54.230.68.132 A 54.240.188.254 A 54.240.188.148 A 54.230.69.245 A 54.230.70.122 |
| 20 June 2014 | 21:22:13 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x1e68 A pshared.5min.com CNAME ashared.5min.com CNAME ashared.5min.com.edgesuite.net CNAME a756.g.akamai.net A 184.28.16.59 A 184.28.16.35 |
| 20 June 2014 | 21:22:13 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x1815 A www.blogcdn.com CNAME www.blogsmithcdn-ds.com.edgesuite.net CNAME a1949.dscg2.akamai.net A 96.17.148.10 A 96.17.148.32 |
| 20 June 2014 | 21:22:13 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x8bf1 A cfiles.5min.com CNAME afiles.5min.com CNAME afiles.5min.com.edgesuite.net CNAME a1670.g.akamai.net A 184.28.16.10 A 184.28.16.17 |
| 20 June 2014 | 21:22:13 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x7381 A syn.5min.com CNAME fivemin-cs.egslb.aol.com A 64.12.245.3 |
| 20 June 2014 | 21:22:13 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x0943 A travel.aol.com CNAME travel.aol.com.aol.akadns.net A 207.200.74.102 |
| 20 June 2014 | 21:22:14 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x8353 A www.facebook.com CNAME star.c10r.facebook.com A 31.13.70.65 |
| 20 June 2014 | 21:22:14 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x869c A at.atwola.com CNAME glb-ads.atwola.adtechus.com CNAME atwola-sb-wc.adtechus.com A 152.163.13.68 |
| 20 June 2014 | 21:22:14 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x22ae A connect.facebook.net CNAME connect.facebook.net.edgekey.net CNAME e3821.dspe1.akamaiedge.net A 69.192.240.74 |
| 20 June 2014 | 21:22:14 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xb212 A b.scorecardresearch.com CNAME b.scorecardresearch.com.edgesuite.net CNAME a1294.w20.akamai.net A 184.28.16.72 A 184.28.16.67 |
| 20 June 2014 | 21:22:14 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x0e29 A ct.buzzfeed.com CNAME wac.09fc.edgecastcdn.net CNAME gsb1.wac.v3cdn.net A 93.184.216.229 |
| 20 June 2014 | 21:22:15 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x5a85 A c.aol.com CNAME c.aol.com.aol.akadns.net A 205.188.87.158 A 205.188.95.158 |
| 20 June 2014 | 21:22:15 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xbec1 A o.sa.aol.com CNAME sa.aol.com.122.2o7.net A 66.235.141.145 A 66.235.141.146 A 66.235.141.16 A 66.235.141.17 A 66.235.141.144 A 63.140.35.161 A 63.140.35.162 A 63.140.35.160 A 66.235.142.20 A 66.235.142.24 |
| 20 June 2014 | 21:22:15 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xf0f4 A l.5min.com CNAME loggers.5min.aol.com CNAME fivemin-cs.egslb.aol.com A 64.12.245.3 |
| 20 June 2014 | 21:22:15 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xadd7 A b.gadling.com CNAME b.aol.com CNAME b.egslb.aol.com A 149.174.144.1 |
| 20 June 2014 | 21:22:15 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xa5aa A static.ak.facebook.com CNAME static.ak.facebook.com.edgesuite.net CNAME a749.dsw4.akamai.net A 96.17.148.10 A 96.17.148.24 |
| 20 June 2014 | 21:22:16 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x44fe A s-static.ak.facebook.com CNAME s-static.ak.facebook.com.edgekey.net CNAME e566.dspe1.akamaiedge.net A 69.192.241.154 |
| 20 June 2014 | 21:22:16 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x753d A view.atdmt.com CNAME view.atdmt.com.nsatc.net A 157.56.67.168 |
| 20 June 2014 | 21:22:16 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xc84a A aka-cdn-ns.adtechus.com CNAME aka-cdn-ns.adtechus.com.edgesuite.net CNAME a627.g.akamai.net A 184.28.16.50 A 184.28.16.43 |
| 20 June 2014 | 21:22:16 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xc67a A pthumbnails.5min.com CNAME athumbnails.5min.com CNAME athumbnails.5min.com.edgesuite.net CNAME a1165.g.akamai.net A 184.28.16.58 A 184.28.16.40 |
| 20 June 2014 | 21:22:16 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x9f8b A pixel.quantserve.com CNAME map-pb.quantserve.com.akadns.net CNAME ac-na.quantserve.com.akadns.net A 64.94.107.55 A 64.94.107.30 A 64.94.107.35 A 64.94.107.23 A 64.94.107.26 A 64.94.107.57 A 64.94.107.58 A 64.94.107.22 |
| 20 June 2014 | 21:22:16 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xd44c A pglb.buzzfed.com CNAME s.buzzfeed.com.edgesuite.net CNAME a1186.g.akamai.net A 184.28.16.33 A 184.28.16.65 |
| 20 June 2014 | 21:22:16 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x62b4 A apx.moatads.com A 54.83.84.206 A 54.197.208.165 A 54.89.139.152 A 75.101.248.37 |
| 20 June 2014 | 21:22:16 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x18b2 A www.blogcdn.com CNAME www.blogsmithcdn-ds.com.edgesuite.net CNAME a1949.dscg2.akamai.net A 184.28.16.43 A 184.28.16.42 |
| 20 June 2014 | 21:22:18 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xf197 A b.aol.com CNAME b.egslb.aol.com A 149.174.97.86 |
| 20 June 2014 | 21:22:18 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x74b7 A ads-us.pictela.net CNAME glb-ads.pictela.adtechus.com CNAME pictela-sb-wc.adtechus.com A 152.163.13.76 |
| 20 June 2014 | 21:22:18 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x2bef A ohlone.vizu.com CNAME vizu.x.miisolutions.net CNAME w31.b.cap-mii.net A 216.38.162.159 |
| 20 June 2014 | 21:22:18 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xa068 A accounts.google.com CNAME accounts.l.google.com A 74.125.129.84 |
| 20 June 2014 | 21:22:18 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x87c0 A a248.e.akamai.net A 184.28.16.179 A 184.28.16.161 |
| 20 June 2014 | 21:22:18 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xe742 A fbcdn-profile-a.akamaihd.net CNAME fbcdn-profile-a.akamaihd.net.edgesuite.net CNAME fbcdn-profile-a.ak.fbcdn.akamaihd.net.akadns.net CNAME a2047.dspl.akamai.net CNAME a2047.dspl.akamai.net.0.1.cn.akamaitech.net A 23.67.247.18 A 23.67.247.209 A 23.67.247.59 A 23.67.247.33 A 23.67.247.42 A 23.67.247.50 A 23.67.247.73 A 23.67.247.217 A 23.67.247.58 |
| 20 June 2014 | 21:22:18 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x2a46 A fbstatic-a.akamaihd.net CNAME fbstatic-a.akamaihd.net.edgesuite.net CNAME a1168.dsw4.akamai.net A 96.17.148.50 A 96.17.148.51 |
| 20 June 2014 | 21:22:19 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x9aa5 A clients1.google.com CNAME clients.l.google.com A 74.125.224.196 A 74.125.224.195 A 74.125.224.200 A 74.125.224.206 A 74.125.224.194 A 74.125.224.199 A 74.125.224.198 A 74.125.224.193 A 74.125.224.201 A 74.125.224.192 A 74.125.224.197 |
| 20 June 2014 | 21:22:19 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x31cc A uac.advertising.com CNAME uac.advertising.com.edgesuite.net CNAME a957.g.akamai.net A 184.28.16.48 A 184.28.16.8 |
| 20 June 2014 | 21:22:19 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xc732 A a248.e.akamai.net A 184.28.16.179 A 184.28.16.161 |
| 20 June 2014 | 21:22:20 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x2d29 A aka-cdn.adtech.de CNAME aka-cdn.adtech.de.edgekey.net CNAME e1611.c.akamaiedge.net A 23.210.248.17 |
| 20 June 2014 | 21:22:20 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x7772 A imp.bid.ace.advertising.com CNAME adservingbase.ace.advertising.com CNAME nw-ads.gslb.ace.advertising.com.adcom.akadns.net A 149.174.67.65 A 149.174.67.71 |
| 20 June 2014 | 21:22:20 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x229b A oauth.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 74.125.239.106 A 74.125.239.108 A 74.125.239.107 |
| 20 June 2014 | 21:22:21 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x97c8 A ads.pictela.net CNAME ads.pictela.net.edgesuite.net CNAME a1694.g2.akamai.net A 96.17.148.17 A 96.17.148.56 |
| 20 June 2014 | 21:22:21 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x4379 A bs.serving-sys.com CNAME bs.eyeblaster.akadns.net A 12.129.210.71 |
| 20 June 2014 | 21:22:21 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xfdef A ad.doubleclick.net CNAME dart.l.doubleclick.net A 74.125.239.59 A 74.125.239.60 |
| 20 June 2014 | 21:22:22 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x6681 A s0.2mdn.net CNAME s0-2mdn-net.l.google.com A 74.125.224.188 A 74.125.224.187 |
| 20 June 2014 | 21:22:22 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x25f9 A pagead2.googlesyndication.com CNAME pagead46.l.doubleclick.net A 74.125.239.121 A 74.125.239.122 A 74.125.239.109 |
| 20 June 2014 | 21:22:22 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x192c A leadback.advertising.com CNAME ns.leadback.ace.advertising.com.adcom.akadns.net A 152.163.13.6 |
| 20 June 2014 | 21:22:22 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xf54b A cdn.at.atwola.com CNAME cdn.atwola.com CNAME cdn.atwola.com.edgesuite.net CNAME a1655.g.akamai.net A 184.28.16.34 A 184.28.16.59 |
| 20 June 2014 | 21:22:22 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x406c A radar.cedexis.com CNAME 2-01-2a40-0017.cdx.cedexis.net CNAME radar.cedexis.com.c.footprint.net A 4.27.22.252 A 8.26.194.251 |
| 20 June 2014 | 21:22:23 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xa775 A an.tacoda.net CNAME an.tacoda.net.edgesuite.net CNAME a1406.g.akamai.net A 184.28.16.32 A 184.28.16.26 |
| 20 June 2014 | 21:22:23 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x4ff1 A tacoda.at.atwola.com CNAME rtx-at.tacoda.akadns.net A 149.174.67.69 |
| 20 June 2014 | 21:22:24 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xf0dd A i1-js-14-3-01-11844-216973042-i.init.cedexis-radar.net A 50.97.227.68 |
| 20 June 2014 | 21:22:24 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xcd0a A probes.cedexis.com CNAME 2-01-2a40-0009.cdx.cedexis.net A 50.97.227.70 |
| 20 June 2014 | 21:22:24 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xd56f A d.p-td.com CNAME d.p-td.com.turn.com.akadns.net A 69.194.244.14 |
| 20 June 2014 | 21:22:24 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x2ba6 A probes.cedexis.com CNAME 2-01-2a40-0009.cdx.cedexis.net A 173.192.228.131 |
| 20 June 2014 | 21:22:24 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xc77e A www.aol.com CNAME portal.aol.akadns.net CNAME portal-standard.aol.akadns.net CNAME v6v4.portal-standard.aol.akadns.net A 207.200.111.13 |
| 20 June 2014 | 21:22:24 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xbaa2 A webmail.aol.com CNAME hostheader.web.aol.com CNAME hostheader.web.aol.com.websys.akadns.net A 207.200.74.38 |
| 20 June 2014 | 21:22:24 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x4693 A en.wikipedia.org CNAME wikipedia-lb.wikimedia.org CNAME text-lb.eqiad.wikimedia.org A 208.80.154.224 |
| 20 June 2014 | 21:22:24 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x852d A rt.com A 62.213.85.4 |
| 20 June 2014 | 21:22:24 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x4276 A feeds.feedburner.com CNAME www4.l.google.com A 74.125.239.102 A 74.125.239.100 A 74.125.239.110 A 74.125.239.97 A 74.125.239.103 A 74.125.239.99 A 74.125.239.105 A 74.125.239.101 A 74.125.239.104 A 74.125.239.98 A 74.125.239.96 |
| 20 June 2014 | 21:22:25 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xeab7 A www.coffeehouse.ru A 195.239.244.163 |
| 20 June 2014 | 21:22:25 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xa675 A teremok.ru A 90.156.201.31 A 90.156.201.22 A 90.156.201.48 A 90.156.201.12 |
| 20 June 2014 | 21:22:25 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x5b1c A www.tumblr.com A 66.6.43.20 A 66.6.44.20 |
| 20 June 2014 | 21:22:25 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xb46b A www.mamaison.com A 80.188.162.253 |
| 20 June 2014 | 21:22:25 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x5986 A www.twitter.com CNAME twitter.com A 199.59.148.82 A 199.59.150.7 A 199.59.150.39 A 199.59.149.198 |
| 20 June 2014 | 21:22:25 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xce05 A gadling.tumblr.com A 66.6.42.21 A 66.6.41.21 |
| 20 June 2014 | 21:22:25 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x1c08 A www.mapquest.com CNAME winston.mapquest.akadns.net CNAME winston-west.mapquest.akadns.net CNAME v6v4.winston-west.mapquest.akadns.net A 207.200.102.32 |
| 20 June 2014 | 21:22:25 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x4a58 A news.travel.aol.com CNAME misc.blogsmith.aol.com CNAME misc.blogsmith.aol.com.aol.akadns.net A 207.200.74.27 |
| 20 June 2014 | 21:22:25 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x7eb5 A www.huffingtonpost.com CNAME www.huffingtonpost.com.edgesuite.net CNAME a495.g.akamai.net A 96.17.148.8 A 96.17.148.10 |
| 20 June 2014 | 21:22:25 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x0444 A www.dailyfinance.com CNAME www.dailyfinance.com.aol.akadns.net A 207.200.74.113 |
| 20 June 2014 | 21:22:25 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x2b01 A on.aol.com CNAME fivemin-cs.egslb.aol.com A 64.12.245.3 |
| 20 June 2014 | 21:22:25 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x9705 A gasprices.mapquest.com CNAME mq-gasweb.egslb.aol.com A 207.200.102.2 |
| 20 June 2014 | 21:22:25 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x820c A www.foxnews.com CNAME www.foxnews.com.edgesuite.net CNAME a20.g.akamai.net A 96.17.148.40 A 96.17.148.58 |
| 20 June 2014 | 21:22:25 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xa77e A local.aol.com CNAME yellowpages.aol.com CNAME yp-cs.egslb.aol.com A 207.200.74.126 |
| 20 June 2014 | 21:22:25 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x67b8 A www.engadget.com CNAME v4.engadget.com.aol.akadns.net A 207.200.74.123 |
| 20 June 2014 | 21:22:25 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x4a02 A search.aol.com CNAME search.aol.com.aol.akadns.net CNAME search-west.aol.com.aol.akadns.net A 207.200.66.100 |
| 20 June 2014 | 21:22:25 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xa072 A www.shermanstravel.com A 54.243.71.138 |
| 20 June 2014 | 21:22:25 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x1b13 A feeds.foxnews.com CNAME foxnews.feedproxy.ghs.google.com CNAME ghs.l.google.com A 74.125.129.121 |
| 20 June 2014 | 21:22:25 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xac4d A www.lonelyplanet.com CNAME b.global-ssl.fastly.net A 199.27.77.143 |
| 20 June 2014 | 21:22:25 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xf0bb A blog.shermanstravel.com A 107.21.223.137 |
| 20 June 2014 | 21:22:25 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x342b A www.nytimes.com A 170.149.168.130 |
| 20 June 2014 | 21:22:25 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x0fa8 A inside-digital.blog.lonelyplanet.com CNAME lpmodules.com A 203.43.23.92 |
| 20 June 2014 | 21:22:25 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xfa0e A reports.cedexis.com CNAME 2-01-2a40-0015.cdx.cedexis.net A 23.21.88.16 |
| 20 June 2014 | 21:22:26 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xfdf4 A sjc.sl.bench.cedexis.com A 50.97.220.18 |
| 20 June 2014 | 21:22:26 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x3c70 A reports.cedexis.com CNAME 2-01-2a40-0015.cdx.cedexis.net A 23.21.88.16 |
| 20 June 2014 | 21:22:33 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x2f50 A www.blogsmithcdn.com CNAME www.blogsmithcdn-ds.com.edgesuite.net CNAME a1949.dscg2.akamai.net A 184.28.16.43 A 184.28.16.42 |
| 20 June 2014 | 21:22:39 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xdcc5 A sfr.cedexis.com CNAME cedexis.pfd.sfr.net A 93.20.64.20 |
| 20 June 2014 | 21:22:41 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xbe60 A ovh-canada.bench.cedexis.com A 142.4.202.26 |
| 20 June 2014 | 21:23:04 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x3569 A www.sovietcity.com CNAME sovietcity.com A 50.87.147.145 |
| 20 June 2014 | 21:23:05 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xa937 A 0.gravatar.com CNAME cs91.wac.edgecastcdn.net A 72.21.91.121 |
| 20 June 2014 | 21:23:05 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x999d A 1.gravatar.com CNAME cs91.wac.edgecastcdn.net A 72.21.91.121 |
| 20 June 2014 | 21:23:05 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xae2b A translate.google.com CNAME www3.l.google.com A 74.125.224.161 A 74.125.224.160 A 74.125.224.162 A 74.125.224.166 A 74.125.224.169 A 74.125.224.167 A 74.125.224.168 A 74.125.224.165 A 74.125.224.163 A 74.125.224.164 A 74.125.224.174 |
| 20 June 2014 | 21:23:05 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x1db1 A fonts.googleapis.com CNAME googleapis.l.google.com A 74.125.25.95 |
| 20 June 2014 | 21:23:06 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x2eea A fonts.googleapis.com CNAME googleapis.l.google.com A 74.125.28.95 |
| 20 June 2014 | 21:23:06 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x1c54 A www.google-analytics.com CNAME www-google-analytics.l.google.com A 74.125.224.230 A 74.125.224.227 A 74.125.224.224 A 74.125.224.238 A 74.125.224.226 A 74.125.224.233 A 74.125.224.229 A 74.125.224.232 A 74.125.224.228 A 74.125.224.225 A 74.125.224.231 |
| 20 June 2014 | 21:23:06 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x11a0 A themes.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 74.125.224.171 A 74.125.224.172 A 74.125.224.170 |
| 20 June 2014 | 21:23:06 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xcf2b A googleads.g.doubleclick.net CNAME pagead46.l.doubleclick.net A 74.125.239.121 A 74.125.239.122 A 74.125.239.109 |
| 20 June 2014 | 21:23:07 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xd695 A themes.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 74.125.239.106 A 74.125.239.108 A 74.125.239.107 |
| 20 June 2014 | 21:23:07 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xf03c A js.nrcdn.com CNAME js.nrcdn.com.edgesuite.net CNAME a1682.g2.akamai.net A 184.28.16.58 A 184.28.16.17 |
| 20 June 2014 | 21:23:09 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x2e57 A translate.googleapis.com CNAME googleapis.l.google.com A 74.125.25.95 |
| 20 June 2014 | 21:23:10 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xe874 A t1.gstatic.com A 74.125.239.113 A 74.125.239.114 A 74.125.239.116 A 74.125.239.115 A 74.125.239.112 |
| 20 June 2014 | 21:23:11 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xf24e A t3.gstatic.com A 74.125.239.49 A 74.125.239.51 A 74.125.239.52 A 74.125.239.50 A 74.125.239.48 |
| 20 June 2014 | 21:23:11 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xbf4b A api.nrelate.com A 71.19.242.237 |
| 20 June 2014 | 21:23:12 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xcfd4 A css.nrcdn.com CNAME css.nrcdn.com.edgesuite.net CNAME a1051.g2.akamai.net A 96.17.148.35 A 96.17.148.16 |
| 20 June 2014 | 21:23:12 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x45cd A imgcdn.nrelate.com CNAME nrelate.anycastcdn.net A 96.127.141.83 A 64.120.19.11 A 64.120.19.11 A 23.81.7.107 A 94.100.23.179 A 94.100.23.179 |
| 20 June 2014 | 21:23:13 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xa390 A s1.2mdn.net CNAME s0-2mdn-net.l.google.com A 74.125.224.188 A 74.125.224.187 |
| 20 June 2014 | 21:23:16 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x41aa A lz0.gstatic.com A 224.1.1.1 |
| 20 June 2014 | 21:23:17 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x29ab A topsy.com A 74.112.131.41 |
| 20 June 2014 | 21:23:17 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xd705 A www.deanobrien.co.uk A 82.165.115.39 |
| 20 June 2014 | 21:23:17 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x332b A goo.gl A 74.125.224.161 A 74.125.224.160 A 74.125.224.162 A 74.125.224.166 A 74.125.224.169 A 74.125.224.167 A 74.125.224.168 A 74.125.224.165 A 74.125.224.163 A 74.125.224.164 A 74.125.224.174 |
| 20 June 2014 | 21:23:17 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x537e A twitter.com A 199.59.148.10 A 199.59.149.198 A 199.59.149.230 A 199.59.148.82 |
| 20 June 2014 | 21:23:17 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xef57 A www.youtube.com CNAME youtube-ui.l.google.com A 74.125.239.101 A 74.125.239.97 A 74.125.239.102 A 74.125.239.99 A 74.125.239.104 A 74.125.239.110 A 74.125.239.100 A 74.125.239.103 A 74.125.239.98 A 74.125.239.96 A 74.125.239.105 |
| 20 June 2014 | 21:23:17 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x8ac0 A www.pinterest.com CNAME pinterest.com A 54.235.185.83 |
| 20 June 2014 | 21:23:17 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xffae A nothingbutperfection.blogspot.com CNAME blogspot.l.googleusercontent.com A 74.125.239.107 A 74.125.239.108 A 74.125.239.106 |
| 20 June 2014 | 21:23:17 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x0d78 A amrusob.blogspot.com CNAME blogspot.l.googleusercontent.com A 74.125.239.108 A 74.125.239.106 A 74.125.239.107 |
| 20 June 2014 | 21:23:17 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xdd15 A www.visahq.com CNAME visahq.com A 209.9.163.250 |
| 20 June 2014 | 21:23:17 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x9868 A diaryinvisible.wordpress.com CNAME lb.wordpress.com A 192.0.81.250 A 76.74.254.120 A 66.155.11.238 A 66.155.9.238 A 76.74.254.123 A 192.0.80.250 |
| 20 June 2014 | 21:23:18 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x8160 A englishteacherx.blogspot.co.uk CNAME blogspot.l.googleusercontent.com A 74.125.239.107 A 74.125.239.108 A 74.125.239.106 |
| 20 June 2014 | 21:23:18 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x5859 A windowstorussia.com A 93.95.225.253 |
| 20 June 2014 | 21:23:18 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x1f31 A www.learnrussianweb.com CNAME ghs.google.com CNAME ghs.l.google.com A 74.125.20.121 |
| 20 June 2014 | 21:23:18 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x72bc A video.sovietcity.com A 50.87.147.145 |
| 20 June 2014 | 21:23:18 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x12ec A astore.amazon.com A 176.32.98.40 |
| 20 June 2014 | 21:23:18 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x4928 A russianreport.wordpress.com CNAME lb.wordpress.com A 192.0.81.250 A 66.155.9.238 A 66.155.11.238 A 76.74.254.120 A 192.0.80.250 A 76.74.254.123 |
| 20 June 2014 | 21:23:18 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x46de A thingsevewoulddo.blogspot.com CNAME blogspot.l.googleusercontent.com A 74.125.239.12 A 74.125.239.11 A 74.125.239.10 |
| 20 June 2014 | 21:23:18 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xd8ca A www.studiopress.com CNAME studiopress.com A 72.10.35.80 |
| 20 June 2014 | 21:23:18 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xf010 A wordpress.org A 66.155.40.249 A 66.155.40.250 |
| 20 June 2014 | 21:23:18 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xa676 A www.googleadservices.com CNAME pagead.l.doubleclick.net A 74.125.239.57 A 74.125.239.58 A 74.125.239.45 |
| 20 June 2014 | 21:23:21 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xc30d A vt-1.nrelate.com CNAME vt.nrelate.com A 71.19.244.184 |
| 20 June 2014 | 21:23:38 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xb5b1 A s.huffpost.com CNAME s.huffpost.com.edgesuite.net CNAME a1428.g.akamai.net A 96.17.148.24 A 96.17.148.18 |
| 20 June 2014 | 21:23:38 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x6f36 A i.huffpost.com CNAME i.huffpost.com.edgesuite.net CNAME a1280.g.akamai.net A 23.212.52.41 A 23.212.52.48 |
| 20 June 2014 | 21:23:38 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xe09e A s0.huffpost.com CNAME s.huffpost.com.edgesuite.net CNAME a1428.g.akamai.net A 96.17.148.18 A 96.17.148.24 |
| 20 June 2014 | 21:23:38 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x4dc6 A ar.voicefive.com CNAME ar.comscore.akadns.net A 205.218.48.171 |
| 20 June 2014 | 21:23:38 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xc339 A ar.voicefive.com CNAME ar.comscore.akadns.net A 4.26.66.43 |
| 20 June 2014 | 21:23:40 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x57e7 A cdn.taboola.com CNAME taboola.com.edgekey.net CNAME e3091.g.akamaiedge.net A 23.192.252.168 |
| 20 June 2014 | 21:23:40 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x78f0 A cdn.tt.omtrdc.net A 66.117.23.103 A 66.117.23.104 A 66.117.23.105 A 66.117.23.106 A 66.117.23.107 A 66.117.23.100 A 66.117.23.101 A 66.117.23.102 |
| 20 June 2014 | 21:23:40 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x3a50 A aol.tt.omtrdc.net A 66.117.23.107 A 66.117.23.100 A 66.117.23.101 A 66.117.23.102 A 66.117.23.103 A 66.117.23.104 A 66.117.23.105 A 66.117.23.106 |
| 20 June 2014 | 21:23:40 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x1e36 A netstorage.taboola.com CNAME taboola.com.edgekey.net CNAME e3091.g.akamaiedge.net A 172.231.4.212 |
| 20 June 2014 | 21:23:41 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x954e A d8rk54i4mohrb.cloudfront.net A 54.239.132.105 A 54.230.116.53 A 54.230.117.66 A 54.230.116.109 A 54.230.119.11 A 54.230.116.145 A 54.230.118.208 A 54.230.119.40 |
| 20 June 2014 | 21:23:41 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x70fa A platform.twitter.com CNAME cs107.wac.edgecastcdn.net A 93.184.216.146 |
| 20 June 2014 | 21:23:42 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xd8cc A entry-stats.huffpost.com CNAME entry-stats-nova.egslb.aol.com A 205.188.95.181 |
| 20 June 2014 | 21:23:44 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xdbe5 A d8rk54i4mohrb.cloudfront.net A 54.230.143.147 A 205.251.215.10 A 54.230.140.112 A 54.230.142.35 A 205.251.215.107 A 54.230.142.227 A 54.230.143.234 A 205.251.215.224 |
| 20 June 2014 | 21:23:44 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x0c21 A plugin.mediavoice.com CNAME plugin.mediavoice.com.edgesuite.net CNAME a1670.g.akamai.net A 23.212.52.48 A 23.212.52.43 |
| 20 June 2014 | 21:23:46 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xea1b A b.huffingtonpost.com CNAME b.aol.com CNAME b.egslb.aol.com A 149.174.97.86 |
| 20 June 2014 | 21:23:46 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x5b3e A plus.google.com A 74.125.239.34 A 74.125.239.32 A 74.125.239.40 A 74.125.239.33 A 74.125.239.46 A 74.125.239.41 A 74.125.239.37 A 74.125.239.36 A 74.125.239.35 A 74.125.239.38 A 74.125.239.39 |
| 20 June 2014 | 21:23:46 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x1e45 A ajax.googleapis.com CNAME googleapis.l.google.com A 74.125.25.95 |
| 20 June 2014 | 21:23:46 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x0425 A mail.aol.com CNAME mail.aol.com.aol.akadns.net A 64.12.132.55 A 64.12.132.103 A 64.12.132.39 |
| 20 June 2014 | 21:23:47 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x115a A ak.sail-horizon.com CNAME ak.sail-horizon.com.edgekey.net CNAME e5508.g.akamaiedge.net A 172.231.24.208 |
| 20 June 2014 | 21:23:49 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x145b A mono.vizu.com CNAME vizu.x.miisolutions.net CNAME w31.b.cap-mii.net A 216.38.160.159 |
| 20 June 2014 | 21:23:49 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xc471 A edge.quantserve.com CNAME map-js.quantserve.com.akadns.net CNAME anycast-americas.quantserve.com.akadns.net A 64.94.107.23 A 64.94.107.46 A 64.94.107.48 A 64.94.107.54 A 64.94.107.18 A 64.94.107.59 A 64.94.107.24 A 64.94.107.15 |
| 20 June 2014 | 21:23:49 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xb97b A b.grvcdn.com CNAME b.grvcdn.com.edgesuite.net CNAME a1711.g.akamai.net A 96.17.148.32 A 96.17.148.16 |
| 20 June 2014 | 21:23:50 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x8dff A secure-us.imrworldwide.com A 65.171.135.52 |
| 20 June 2014 | 21:23:50 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x52d9 A cdn.pubexchange.com CNAME d1pjxw0noc2yxg.cloudfront.net A 54.230.118.239 A 54.230.117.50 A 54.230.117.53 A 54.230.116.145 A 54.230.116.21 A 54.230.117.225 A 54.230.119.37 A 54.239.132.105 |
| 20 June 2014 | 21:23:53 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x8da0 A rma-api.gravity.com CNAME rma-api.gravity.com.edgesuite.net CNAME a1015.g.akamai.net A 96.17.148.42 A 96.17.148.24 |
| 20 June 2014 | 21:23:56 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xc9d3 A fiji-production-ws.use1.huffpo.net CNAME fiji-wslb-production.use1.huffpo.net A 54.85.19.152 |
| 20 June 2014 | 21:23:57 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x6e99 A edge.simplereach.com CNAME dualstack.edge-1835309090.us-east-1.elb.amazonaws.com A 54.243.120.1 A 107.20.189.168 A 174.129.232.163 A 184.73.234.225 A 174.129.194.97 A 107.22.186.214 A 107.22.189.124 A 107.20.214.165 |
| 20 June 2014 | 21:23:57 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x335f A pixel.quantserve.com CNAME map-pb.quantserve.com.akadns.net CNAME ac-na.quantserve.com.akadns.net A 64.94.107.55 A 64.94.107.30 A 64.94.107.35 A 64.94.107.23 A 64.94.107.26 A 64.94.107.57 A 64.94.107.58 A 64.94.107.22 |
| 20 June 2014 | 21:23:58 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x4646 A mono.vizu.com CNAME vizu.x.miisolutions.net CNAME w31.b.cap-mii.net A 216.38.162.159 |
| 20 June 2014 | 21:23:58 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x4793 A graph.facebook.com CNAME api.facebook.com CNAME star.c10r.facebook.com A 31.13.70.81 |
| 20 June 2014 | 21:24:00 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x797a A cc.simplereach.com CNAME cc-774214060.us-east-1.elb.amazonaws.com A 54.243.64.188 A 50.16.206.45 A 50.16.219.149 A 54.243.213.28 A 50.19.231.203 A 75.101.152.157 |
| 20 June 2014 | 21:24:01 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x6d29 A evsecure-ocsp.verisign.com CNAME ocsp.ws.symantec.com.edgekey.net CNAME e8218.ce.akamaiedge.net A 23.5.251.27 |
| 20 June 2014 | 21:24:02 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x53f3 A itunes.apple.com CNAME itunes-cdn.apple.com.akadns.net CNAME itunes.apple.com.edgekey.net CNAME e673.e9.akamaiedge.net A 184.85.98.217 |
| 20 June 2014 | 21:24:02 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x7883 A play.google.com CNAME www3.l.google.com A 74.125.224.161 A 74.125.224.160 A 74.125.224.162 A 74.125.224.166 A 74.125.224.169 A 74.125.224.167 A 74.125.224.168 A 74.125.224.165 A 74.125.224.163 A 74.125.224.164 A 74.125.224.174 |
| 20 June 2014 | 21:24:02 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x42cc A elections.huffingtonpost.com CNAME www.huffingtonpost.com.edgesuite.net CNAME a495.g.akamai.net A 23.212.52.41 A 23.212.52.49 |
| 20 June 2014 | 21:24:02 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x698a A moviefone.com A 207.200.74.38 A 64.12.79.57 A 64.12.89.186 A 205.188.100.58 A 205.188.101.58 |
| 20 June 2014 | 21:24:02 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x4067 A live.huffingtonpost.com CNAME live.huffingtonpost.com.edgesuite.net CNAME a1784.g1.akamai.net A 63.146.70.8 A 63.146.70.11 |
| 20 June 2014 | 21:24:02 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x208c A voces.huffingtonpost.com CNAME www.huffingtonpost.com.edgesuite.net CNAME a495.g.akamai.net A 96.17.148.10 A 96.17.148.8 |
| 20 June 2014 | 21:24:02 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xe6c1 A www.moviefone.com CNAME moviefone.com.aol.akadns.net A 207.200.74.87 |
| 20 June 2014 | 21:24:02 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x61ce A www.stumbleupon.com A 199.30.80.32 |
| 20 June 2014 | 21:24:02 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x800a A www.offthebus.org CNAME hostheader.web.aol.com CNAME hostheader.web.aol.com.websys.akadns.net A 207.200.74.38 |
| 20 June 2014 | 21:24:02 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x494d A reddit.com A 88.221.87.175 A 88.221.87.177 |
| 20 June 2014 | 21:24:02 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x3ac4 A www.inyourpocket.com A 82.208.14.244 |
| 20 June 2014 | 21:24:02 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x4816 A feeds.huffingtonpost.com CNAME 1mtlf7e.feedproxy.ghs.google.com CNAME ghs.l.google.com A 74.125.28.121 |
| 20 June 2014 | 21:24:02 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x28c6 A appworld.blackberry.com CNAME appworld.blackberry.com.edgekey.net CNAME e2508.e5.akamaiedge.net A 96.16.186.82 |
| 20 June 2014 | 21:24:02 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x7908 A advertising.aol.com CNAME newfront.egslb.aol.com A 149.174.144.164 |
| 20 June 2014 | 21:24:02 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x3430 A adinfo.aol.com CNAME misc.blogsmith.aol.com CNAME misc.blogsmith.aol.com.aol.akadns.net A 207.200.74.27 |
| 20 June 2014 | 21:24:03 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x0c3f A www.sanduny.ru CNAME sanduny.ru A 81.177.33.16 |
| 20 June 2014 | 21:24:18 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xb9bc A www.google.com A 173.194.79.147 A 173.194.79.105 A 173.194.79.99 A 173.194.79.106 A 173.194.79.103 A 173.194.79.104 |
| 20 June 2014 | 21:24:24 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x6363 A bits.wikimedia.org CNAME bits-lb.eqiad.wikimedia.org A 208.80.154.234 |
| 20 June 2014 | 21:24:24 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x6fdf A upload.wikimedia.org CNAME upload-lb.eqiad.wikimedia.org A 208.80.154.240 |
| 20 June 2014 | 21:24:26 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x2b64 A login.wikimedia.org CNAME wikimedia-lb.wikimedia.org CNAME text-lb.ulsfo.wikimedia.org A 198.35.26.96 |
| 20 June 2014 | 21:24:26 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x18c2 A meta.wikimedia.org CNAME wikimedia-lb.wikimedia.org CNAME text-lb.eqiad.wikimedia.org A 208.80.154.224 |
| 20 June 2014 | 21:25:10 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x96ad A www.cnbc.com A 207.223.6.19 A 207.223.6.20 |
| 20 June 2014 | 21:25:11 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xba96 A fm.cnbc.com A 207.223.6.19 A 207.223.6.20 |
| 20 June 2014 | 21:25:11 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x093e A www.nbcudigitaladops.com CNAME www.nbcudigitaladops.com.edgekey.net CNAME e5099.b.akamaiedge.net A 23.203.58.170 |
| 20 June 2014 | 21:25:11 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x1a7a A code.jquery.com CNAME code.jquery.netdna-cdn.com A 108.161.188.209 A 108.161.187.43 |
| 20 June 2014 | 21:25:11 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xb755 A cdn.gigya.com CNAME cdn.gigya.com.edgesuite.net CNAME a221.g.akamai.net A 96.17.148.19 A 96.17.148.50 |
| 20 June 2014 | 21:25:11 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x7259 A pdk.theplatform.com CNAME pdk.theplatform.com.edgekey.net CNAME e5015.g.akamaiedge.net A 172.230.172.39 |
| 20 June 2014 | 21:25:11 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x0ac5 A b.scorecardresearch.com CNAME b.scorecardresearch.com.edgesuite.net CNAME a1294.w20.akamai.net A 96.17.148.41 A 96.17.148.51 A 96.17.148.49 A 96.17.148.10 |
| 20 June 2014 | 21:25:11 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x6093 A widget.perfectmarket.com CNAME widget.perfectmarket.com.cdngc.net A 174.35.7.186 A 174.35.6.76 |
| 20 June 2014 | 21:25:11 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xb86e A www.google-analytics.com CNAME www-google-analytics.l.google.com A 74.125.239.35 A 74.125.239.32 A 74.125.239.38 A 74.125.239.46 A 74.125.239.36 A 74.125.239.39 A 74.125.239.40 A 74.125.239.34 A 74.125.239.37 A 74.125.239.41 A 74.125.239.33 |
| 20 June 2014 | 21:25:11 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x2379 A async-lb-2129785755.us-east-1.elb.amazonaws.com A 174.129.203.72 A 54.235.219.0 |
| 20 June 2014 | 21:25:12 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x79a8 A ad.doubleclick.net CNAME dart.l.doubleclick.net A 74.125.239.155 A 74.125.239.156 |
| 20 June 2014 | 21:25:12 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x23d4 A s0.2mdn.net CNAME s0-2mdn-net.l.google.com A 74.125.224.188 A 74.125.224.187 |
| 20 June 2014 | 21:25:12 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x292d A b.voicefive.com CNAME b.voicefive.com.edgesuite.net CNAME a1294.w20.akamai.net A 23.212.52.51 A 23.212.52.56 |
| 20 June 2014 | 21:25:12 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x06c5 A pagead2.googlesyndication.com CNAME pagead46.l.doubleclick.net A 74.125.239.122 A 74.125.239.109 A 74.125.239.121 |
| 20 June 2014 | 21:25:13 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x0dce A pubads.g.doubleclick.net CNAME partnerad.l.doubleclick.net A 74.125.239.122 A 74.125.239.109 A 74.125.239.121 |
| 20 June 2014 | 21:25:13 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xd830 A ads.pubmatic.com CNAME pubmatic.edgekey.net CNAME e6603.g.akamaiedge.net A 172.230.179.250 |
| 20 June 2014 | 21:25:13 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xce45 A showads.pubmatic.com CNAME showads33000c.pubmatic.com CNAME showads33000.pubmatic.com A 162.248.16.37 |
| 20 June 2014 | 21:25:13 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xabdb A icompass.insightexpressai.com CNAME icompass.insightexpressai.com.edgesuite.net CNAME a84.g.akamai.net A 23.212.52.49 A 23.212.52.42 |
| 20 June 2014 | 21:25:13 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xef3b A image3.pubmatic.com A 162.248.16.26 |
| 20 June 2014 | 21:25:13 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x0b23 A www.gstatic.com A 74.125.239.159 A 74.125.239.143 A 74.125.239.152 A 74.125.239.151 |
| 20 June 2014 | 21:25:13 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x681b A googleads.g.doubleclick.net CNAME pagead46.l.doubleclick.net A 74.125.239.58 A 74.125.239.57 A 74.125.239.45 |
| 20 June 2014 | 21:25:13 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x2ea7 A aktrack.pubmatic.com CNAME aktrack.pubmatic.edgekey.net CNAME e6603.b.akamaiedge.net A 23.7.196.174 |
| 20 June 2014 | 21:25:15 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xffd2 A cm.g.doubleclick.net CNAME pagead.l.doubleclick.net A 74.125.239.57 A 74.125.239.58 A 74.125.239.45 |
| 20 June 2014 | 21:25:15 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x56e9 A themes.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 74.125.239.139 A 74.125.239.138 A 74.125.239.140 |
| 20 June 2014 | 21:25:15 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x4692 A widgets.outbrain.com CNAME san.outbrain.com.edgekey.net CNAME e6565.b.akamaiedge.net A 23.211.4.136 |
| 20 June 2014 | 21:25:15 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x26b4 A www.wtp101.com A 54.86.5.94 A 54.86.29.88 A 54.86.24.86 A 54.86.24.47 A 54.84.26.142 A 54.85.67.81 |
| 20 June 2014 | 21:25:15 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x43de A odb.outbrain.com CNAME alldcs.outbrain.com A 4.71.33.181 |
| 20 June 2014 | 21:25:17 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x9e20 A images.outbrain.com CNAME san.outbrain.com.edgekey.net CNAME e6565.b.akamaiedge.net A 23.211.4.136 |
| 20 June 2014 | 21:25:18 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x09c4 A magnetic.t.domdex.com CNAME tracking-2094563516.us-west-1.elb.amazonaws.com A 50.18.114.249 A 184.169.156.215 A 184.169.173.125 A 50.18.181.92 |
| 20 June 2014 | 21:25:18 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xe0b3 A register.cnbc.com A 207.223.6.24 A 207.223.6.23 |
| 20 June 2014 | 21:25:18 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x4a5f A cnbc.disqus.com CNAME disqus.map.fastly.net A 199.27.79.134 |
| 20 June 2014 | 21:25:19 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x888f A oimg.nbcuni.com CNAME nbcuni.com.122.2o7.net A 66.235.141.146 A 66.235.141.16 A 66.235.141.17 A 66.235.141.144 A 63.140.35.161 A 63.140.35.162 A 63.140.35.160 A 66.235.142.20 A 66.235.142.24 A 66.235.141.145 |
| 20 June 2014 | 21:25:19 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x495e A cnbc.disqus.com CNAME disqus.map.fastly.net A 199.27.79.134 |
| 20 June 2014 | 21:25:19 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x88f1 A cdn.krxd.net CNAME cdn-traffic-director.krxd.net CNAME cdn-fastly.krxd.net CNAME cdn-fastly.krxd.net.c.global-ssl.fastly.net CNAME c.global-ssl.fastly.net A 199.27.79.175 |
| 20 June 2014 | 21:25:19 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xe64a A ocsp.csctrustedsecure.com CNAME ocsp.comodoca.com A 178.255.83.1 |
| 20 June 2014 | 21:25:20 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x7929 A go.disqus.com CNAME disqus.map.fastly.net A 199.27.77.134 |
| 20 June 2014 | 21:25:20 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xd098 A cdn.api.twitter.com CNAME platform.twitter.com.tw.map.fastly.net A 199.96.57.6 |
| 20 June 2014 | 21:25:20 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xe8d5 A api.pinterest.com CNAME api-origin.pinterest.com A 107.21.102.114 |
| 20 June 2014 | 21:25:20 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xa0f2 A feeds.delicious.com CNAME api-688261400.us-west-1.elb.amazonaws.com A 50.18.155.13 A 184.72.40.0 A 184.72.62.200 A 50.18.153.29 A 184.169.134.158 A 50.18.253.198 A 50.18.171.56 A 50.18.58.68 |
| 20 June 2014 | 21:25:20 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x3507 A www.linkedin.com CNAME glb-naw.www.linkedin.com CNAME pop-ela4.www.linkedin.com A 216.52.242.80 |
| 20 June 2014 | 21:25:20 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xe9fb A ocsp.usertrust.com A 178.255.83.1 |
| 20 June 2014 | 21:25:21 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xe865 A disqus.com A 173.192.42.188 A 108.168.209.242 A 173.192.42.190 A 108.168.209.244 |
| 20 June 2014 | 21:25:21 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x3b72 A commentsapi.cnbc.com A 207.223.6.19 A 207.223.6.20 |
| 20 June 2014 | 21:25:22 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xf68a A adclick.g.doubleclick.net CNAME pagead.l.doubleclick.net A 74.125.224.250 A 74.125.224.249 A 74.125.224.237 |
| 20 June 2014 | 21:25:22 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xbbb2 A portfolio.cnbc.com A 64.210.194.213 |
| 20 June 2014 | 21:25:22 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x47e7 A watchlist.cnbc.com A 207.223.6.24 A 207.223.6.23 |
| 20 June 2014 | 21:25:22 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x5015 A recode.net A 76.74.254.123 A 192.0.80.250 A 192.0.81.250 A 66.155.9.238 A 76.74.254.120 A 66.155.11.238 |
| 20 June 2014 | 21:25:22 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x91c5 A pro.cnbc.com A 64.210.199.153 A 64.210.199.158 |
| 20 June 2014 | 21:25:22 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x3a7a A www.twitter.com CNAME twitter.com A 199.59.148.10 A 199.59.150.7 A 199.59.150.39 A 199.59.148.82 |
| 20 June 2014 | 21:25:22 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x949f A static.chartbeat.com CNAME global.ssl.fastly.net CNAME global-ssl.fastly.net CNAME fallback.global-ssl.fastly.net A 199.27.79.184 A 199.27.79.185 |
| 20 June 2014 | 21:25:22 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x4185 A video.cnbc.com A 64.210.194.213 A 64.210.194.214 |
| 20 June 2014 | 21:25:22 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x34b8 A videoreprints.cnbc.com A 216.218.210.168 |
| 20 June 2014 | 21:25:22 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xccc8 A newsletters.cnbc.com CNAME cnbc.com A 207.223.6.19 A 207.223.6.20 |
| 20 June 2014 | 21:25:22 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x0202 A cnbcmediasales.com A 54.208.98.245 |
| 20 June 2014 | 21:25:22 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xbada A cnbcllca.custhelp.com A 74.117.206.64 |
| 20 June 2014 | 21:25:22 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x5da5 A nbcuni.com A 216.178.96.229 |
| 20 June 2014 | 21:25:22 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x900f A corporate.comcast.com CNAME corporate.comcast.com.edgesuite.net CNAME a978.dscg.akamai.net A 23.212.52.51 A 23.212.52.42 |
| 20 June 2014 | 21:25:22 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x5d37 A www.yahoo.com CNAME fd-fp3.wg1.b.yahoo.com CNAME ds-fp3.wg1.b.yahoo.com CNAME ds-any-fp3-lfb.wa1.b.yahoo.com CNAME ds-any-fp3-real.wa1.b.yahoo.com A 206.190.36.45 A 98.138.252.30 A 98.138.253.109 A 206.190.36.105 |
| 20 June 2014 | 21:25:22 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xcdc5 A gscounters.us1.gigya.com CNAME farm2.us1.gigya.com A 74.120.148.12 |
| 20 June 2014 | 21:25:22 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x8694 A sjobs.brassring.com A 66.77.22.60 |
| 20 June 2014 | 21:25:23 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x8717 A connect.facebook.net CNAME connect.facebook.net.edgekey.net CNAME e3821.dspe1.akamaiedge.net A 23.9.38.149 |
| 20 June 2014 | 21:25:23 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xa9ec A www.petmd.com CNAME cs39.adn.edgecastcdn.net A 72.21.92.59 |
| 20 June 2014 | 21:25:23 | 4.2.2.1 | 172.29.1.17 | Standard query response 0xa4be A www.mlssoccer.com CNAME wac.3b01.edgecastcdn.net CNAME gs1.wac.edgecastcdn.net A 72.21.91.19 |
| 20 June 2014 | 21:25:23 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x18e6 A wallstcheatsheet.com A 199.83.131.100 A 199.83.128.100 |
| 20 June 2014 | 21:25:23 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x008f A www.greencarreports.com A 198.101.191.210 |
| 20 June 2014 | 21:25:23 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x5d88 A www.eonline.com CNAME www.eonline.com.edgesuite.net CNAME a825.g.akamai.net A 96.17.148.42 A 96.17.148.18 |
| 20 June 2014 | 21:25:23 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x2688 A www.frontdoor.com A 54.213.174.154 |
| 20 June 2014 | 21:25:23 | 4.2.2.1 | 172.29.1.17 | Standard query response 0x84fe A www.nbcuni.com CNAME www.nbcuni.com.edgesuite.net CNAME a1778.dscb.akamai.net A 216.156.211.25 A 216.156.211.42 |

## Appendix 3C – Text Coordinates

|  |  |
| --- | --- |
| Latitude | Longitude |
| 46.85661316 | -114.0186081 |
| 46.85693359 | -114.018631 |
| 46.8572731 | -114.0186844 |
| 46.85760117 | -114.0186691 |
| 46.85805511 | -114.0186615 |
| 46.85828781 | -114.0186462 |
| 46.85852432 | -114.0186386 |
| 46.85873413 | -114.0186462 |
| 46.85884476 | -114.0186462 |
| 46.85894394 | -114.0186462 |
| 46.85904694 | -114.0186462 |
| 46.85914993 | -114.0186462 |
| 46.85946655 | -114.0186462 |
| 46.85957718 | -114.0186462 |
| 46.85969162 | -114.0186462 |
| 46.85980988 | -114.0186462 |
| 46.85993195 | -114.0186462 |
| 46.86029053 | -114.018631 |
| 46.86052322 | -114.0186386 |
| 46.86075592 | -114.018631 |
| 46.86098862 | -114.018631 |
| 46.86122894 | -114.0186386 |
| 46.8614769 | -114.018631 |
| 46.86159897 | -114.018631 |
| 46.86183548 | -114.0186234 |
| 46.86206436 | -114.0186157 |
| 46.8622818 | -114.0186005 |
| 46.86248779 | -114.0186005 |
| 46.86260223 | -114.0185928 |
| 46.8628273 | -114.0185776 |
| 46.86306381 | -114.0185776 |
| 46.86330032 | -114.0185623 |
| 46.86342621 | -114.0185547 |
| 46.86355209 | -114.0185471 |
| 46.86367416 | -114.0185394 |
| 46.86378098 | -114.0185394 |
| 46.86387253 | -114.0185318 |
| 46.86370468 | -114.0116425 |
| 46.8637085 | -114.0116348 |
| 46.86401749 | -114.0110703 |
| 46.86404419 | -114.0107498 |
| 46.864048 | -114.0107117 |
| 46.86408997 | -114.0104218 |
| 46.86408997 | -114.0101242 |
| 46.86407852 | -114.0096283 |
| 46.86407089 | -114.0094223 |
| 46.86406708 | -114.0091019 |
| 46.86407471 | -114.0087585 |
| 46.86408234 | -114.0084229 |
| 46.86405182 | -114.0074692 |
| 46.86404419 | -114.007164 |
| 46.86404419 | -114.0069427 |
| 46.864048 | -114.0068054 |
| 46.86405563 | -114.0067062 |
| 46.86405182 | -114.0066223 |
| 46.86405182 | -114.0064621 |
| 46.86405182 | -114.006279 |
| 46.86405182 | -114.0060577 |
| 46.86405182 | -114.005928 |
| 46.86405945 | -114.0056305 |
| 46.86405945 | -114.0053406 |
| 46.86405563 | -114.0050659 |
| 46.86405182 | -114.004776 |
| 46.86405182 | -114.0045242 |
| 46.86404419 | -114.0042725 |
| 46.86404419 | -114.0041428 |
| 46.86404037 | -114.0039215 |
| 46.86398315 | -114.0035477 |
| 46.86393356 | -114.0035172 |
| 46.86381912 | -114.0035248 |
| 46.86364365 | -114.00354 |
| 46.86354446 | -114.0035477 |
| 46.86325455 | -114.0036011 |
| 46.86309052 | -114.0037689 |
| 46.86293411 | -114.0039673 |
| 46.86286163 | -114.0040817 |
| 46.86270142 | -114.0043259 |
| 46.86253357 | -114.0045776 |
| 46.86236191 | -114.0048141 |
| 46.86210632 | -114.0052032 |
| 46.86183548 | -114.0055923 |
| 46.86166 | -114.0058441 |
| 46.86148453 | -114.0060959 |
| 46.86122131 | -114.0064774 |
| 46.86103058 | -114.0067291 |
| 46.86084366 | -114.0069962 |
| 46.86065674 | -114.0072708 |
| 46.86037064 | -114.0076675 |
| 46.85998917 | -114.0082092 |
| 46.8597908 | -114.0084839 |
| 46.85969162 | -114.0086212 |
| 46.85950089 | -114.008873 |
| 46.85930252 | -114.00914 |
| 46.85910416 | -114.0094147 |
| 46.85900879 | -114.0095444 |
| 46.8588295 | -114.0097961 |
| 46.85864639 | -114.0100555 |
| 46.85837555 | -114.0104446 |
| 46.85812378 | -114.0107956 |
| 46.85795212 | -114.0110397 |
| 46.85778809 | -114.0112762 |
| 46.85765839 | -114.0114517 |
| 46.85751343 | -114.0116425 |
| 46.85749054 | -114.0116882 |
| 46.85747147 | -114.0117111 |
| 46.85741806 | -114.011795 |
| 46.85733414 | -114.0119095 |
| 46.85723495 | -114.0120468 |
| 46.85718155 | -114.0121231 |
| 46.85708237 | -114.0122528 |
| 46.85697937 | -114.0123749 |
| 46.85683441 | -114.0125656 |
| 46.85672379 | -114.0127106 |
| 46.8565979 | -114.0128708 |
| 46.85647202 | -114.0130234 |
| 46.85631943 | -114.0131302 |

## Appendix 3D – Jigsaw Images Output

A picture containing wall, indoor, old

Description automatically generated

fullImage

A close-up of a robot

Description automatically generated with low confidence

fullImage2

A picture containing person, outdoor, person

Description automatically generated

fullImage3

## Appendix 3E – Wireshark Output

### Edward Snowden to Julian Assange (Docs.pcap) [11-Jul-2014 16:03:55]

Date: Fri, 11 Jul 2014 20:04:24 GMT

Cache-Control: private

Content-Type: application/json; charset=utf-8

Content-Encoding: gzip

Vary: Accept-Encoding

P3P: CP="CURo TAIo IVAo IVDo ONL UNI COM NAV INT DEM STA OUR"

X-Powered-By: ASP.NET

Content-Length: 1222

Keep-Alive: timeout=120

Connection: Keep-Alive

[{"isCertifiedMail":false,"inlineImgIds":[],"isVirusRepaired":false,"replyAllCcAddrs":"","isSuccess":true,"baseSubject":"Urgent","spamReasonMsg":"","attachments":[{"size":11840428,"subType":"zip","url":"http://mail.aol.com/38629-111/aol-6/en-us/mail/get-attachment.aspx?uid=280&folder=Inbox&partId=3&saveAs=DocsPcap.zip","name":"DocsPcap.zip","baseType":"application","id":3}],"folderType":"Inbox","hasLinksAndImages":false,"displayTo":"wikiofleaks <wikiofleaks@aol.com>","sentTime":"11-Jul-2014 16:03:55 +0000","isLikelyForward":false,"spamReason":"none","displayBcc":"","receivedTime":1405109035000,"bcc":[],"hasImages":false,"isRead":true,"knownSender":true,"to":[{"shorterDisplayForm":"wikiofleaks","displayForm":"wikiofleaks <wikiofleaks@aol.com>","userInputForm":"wikiofleaks@aol.com"}],"isSeen":true,"isVoicemail":false,"isVirusScanned":true,"uid":"280","hasAttachments":true,"replyAllAddrs":"snowedinedward@aol.com","isSpam":false,"messageID":"<8D16B5A5A79286C-2514-4513@webmail-m285.sysops.aol.com>","hasFailedSpfCheck":false,"displayFrom":"Edward Snowden <snowedinedward@aol.com>","subject":"Urgent","isFlagged":false,"replyToAddrs":"snowedinedward@aol.com","cc":[],"isDraft":false,"body":"<html>\r\n<body class=\"AOLWebSuite\" style=\"background-color: white;font-family: Arial,sans-serif;font-size: 10pt;border: 0px;\">\r\n\r\n<div id=\"AOLMsgPart\_2\_49c99f9d-5d59-4248-ae5c-760340797f7a\">\r\n<font color=\"black\" size=\"2\" face=\"arial\">\n<div><font face=\"Arial, Helvetica, sans-serif\" style=\"background-color: transparent;\">Hello friend,</font></div>\n\n<div>&nbsp;</div>\n\n<div><font face=\"Arial, Helvetica, sans-serif\" style=\"background-color: transparent;\">&nbsp;I have a pcap I would like you to look through. Could be useful.</font></div>\n\n<div>&nbsp;</div>\n\n<div><font face=\"Arial, Helvetica, sans-serif\" style=\"background-color: transparent;\">&nbsp;Snowedinedward</font></div>\n</font>\r\n</div>\r\n\r\n</body>\r\n</html>\r\n","inputFrom":"snowedinedward@aol.com","canUnsubscribe":false,"from":[{"shorterDisplayForm":"Edward Snowden","displayForm":"Edward Snowden <snowedinedward@aol.com>","userInputForm":"snowedinedward@aol.com"}],"isOfficialMail":false,"displayCc":"","folder":"Inbox"}]

### Edward Snowden to Julian Assange (Hello Friend…) [11-Jul-2014 14:03]

">-----Original Message-----<br>\n\nFrom: Edward Snowden &lt;<a href='mailto:snowedinedward@aol.com'>snowedinedward@aol.com</a>&gt;<br>\n\nTo: wikiofleaks &lt;<a href='mailto:wikiofleaks@aol.com'>wikiofleaks@aol.com</a>&gt;<br>\n\nSent: Fri, Jul 11, 2014 2:03 pm<br>\n\nSubject: Urgent<br>\n\n<br>\n\n\n\n\n\n\n<div id=\"AOLMsgPart\_2\_49c99f9d-5d59-4248-ae5c-760340797f7a\">\n<font color=\"black\" face=\"arial\" size=\"2\">\n\n\n<div><font style=\"background-color: transparent;\" face=\"Arial, Helvetica, sans-serif\">Hello friend,</font></div>\n\n\n\n\n\n<div>&nbsp;</div>\n\n\n\n\n\n<div><font style=\"background-color: transparent;\" face=\"Arial, Helvetica, sans-serif\">&nbsp;I have a pcap I would like you to look through. Could be useful.</font></div>\n\n\n\n\n\n<div>&nbsp;</div>\n\n\n\n\n\n<div><font style=\"background-color: transparent;\" face=\"Arial, Helvetica, sans-serif\">&nbsp;Snowedinedward</font></div>\n\n\n</font>\n</div>\n\n\n\n\n\n</div>\n\n</font>\r\n</div>\r\n\r\n</body>\r\n</html>\r\n","inputFrom":"wikiofleaks@aol.com","canUnsubscribe":false,"references":"<8D16B5A5A79286C-2514-4513@webmail-m285.sysops.aol.com>","from":[{"shorterDisplayForm":"Julian Assange","displayForm":"Julian Assange <wikiofleaks@aol.com>","userInputForm":"wikiofleaks@aol.com"}],"isOfficialMail":false,"displayCc":"","folder":"Inbox"}]

### Julian Assange to Edward Snowden (I will look at that pcap…) [11-Jul-2014 16:07:20]

Date: Fri, 11 Jul 2014 20:07:50 GMT

Cache-Control: private

Content-Type: application/json; charset=utf-8

Content-Encoding: gzip

Vary: Accept-Encoding

P3P: CP="CURo TAIo IVAo IVDo ONL UNI COM NAV INT DEM STA OUR"

X-Powered-By: ASP.NET

Content-Length: 1634

Keep-Alive: timeout=120

Connection: Keep-Alive

[{"isCertifiedMail":false,"inlineImgIds":[],"isVirusRepaired":false,"replyAllCcAddrs":"","isSuccess":true,"baseSubject":"Urgent","spamReasonMsg":"","attachments":[],"folderType":"Inbox","hasLinksAndImages":false,"displayTo":"wikiofleaks <wikiofleaks@aol.com>","sentTime":"11-Jul-2014 16:07:20 +0000","isLikelyForward":false,"spamReason":"none","displayBcc":"","receivedTime":1405109240000,"bcc":[],"hasImages":false,"isRead":true,"knownSender":true,"to":[{"shorterDisplayForm":"wikiofleaks","displayForm":"wikiofleaks <wikiofleaks@aol.com>","userInputForm":"wikiofleaks@aol.com"}],"isSeen":true,"isVoicemail":false,"isVirusScanned":false,"uid":"283","hasAttachments":false,"replyAllAddrs":"snowedinedward@aol.com","isSpam":false,"messageID":"<8D16B5ADABC350E-2514-45E5@webmail-m285.sysops.aol.com>","hasFailedSpfCheck":false,"displayFrom":"Edward Snowden <snowedinedward@aol.com>","subject":"Re: Urgent","isFlagged":false,"replyToAddrs":"snowedinedward@aol.com","cc":[],"isDraft":false,"body":"<html>\r\n<body class=\"AOLWebSuite\" style=\"background-color: white;font-family: Arial,sans-serif;font-size: 10pt;border: 0px;\">\r\n\r\n<div id=\"AOLMsgPart\_1\_acf6c41b-1f63-4943-8bfe-405075847cef\">\r\n<font color=\"black\" size=\"2\" face=\"arial\">\n<div><font style=\"background-color: transparent;\"></font></div>\n\n<div>Julian,</div>\n\n<div>&nbsp;</div>\n\n<div>I will do so as soon as I can.</div>\n\n<div>&nbsp;</div>\n\n<div style=\"color: black; font-family: arial,helvetica; font-size: 10pt;\">-----Original Message-----<br>\nFrom: Julian Assange &lt;<a href='mailto:wikiofleaks@aol.com'>wikiofleaks@aol.com</a>&gt;<br>\nTo: snowedinedward &lt;<a href='mailto:snowedinedward@aol.com'>snowedinedward@aol.com</a>&gt;<br>\nSent: Fri, Jul 11, 2014 2:05 pm<br>\nSubject: Re: Urgent<br>\n<br>\n\n\n\n\n<div id=\"AOLMsgPart\_1\_e504e425-093f-43d8-a052-3e446db71831\">\n<font color=\"black\" face=\"arial\" size=\"2\">S<font size=\"2\">nowedinedward,<br>\n\n<br>\n\nI will look at that pcap as soon as I can. Can you also send me the documents you have collected during research of that recent scandal.<br>\n\n</font>\n\n\n<div> <br>\n\n\n</div>\n\n\n\n\n\n<div> <br>\n\n\n</div>\n\n\n\n\n\n<div> <br>\n\n\n</div>\n\n\n\n\n\n<div style=\"color: black; font-family: arial,helvetica; font-size: 10pt;\">-----Original Message-----<br>\n\n\nFrom: Edward Snowden &lt;<a href=\"mailto:snowedinedward@aol.com\">snowedinedward@aol.com</a>&gt;<br>\n\n\nTo: wikiofleaks &lt;<a href=\"mailto:wikiofleaks@aol.com\">wikiofleaks@aol.com</a>&gt;<br>\n\n\nSent: Fri, Jul 11, 2014 2:03 pm<br>\n\n\nSubject: Urgent<br>\n\n\n<br>\n\n\n\n\n\n\n\n\n<div id=\"AOLMsgPart\_2\_49c99f9d-5d59-4248-ae5c-760340797f7a\">\n<font color=\"black\" face=\"arial\" size=\"2\">\n\n\n\n<div><font face=\"Arial, Helvetica, sans-serif\" style=\"background-color: transparent;\">Hello friend,</font></div>\n\n\n\n\n\n\n\n<div>&nbsp;</div>\n\n\n\n\n\n\n\n<div><font face=\"Arial, Helvetica, sans-serif\" style=\"background-color: transparent;\">&nbsp;I have a pcap I would like you to look through. Could be useful.</font></div>\n\n\n\n\n\n\n\n<div>&nbsp;</div>\n\n\n\n\n\n\n\n<div><font face=\"Arial, Helvetica, sans-serif\" style=\"background-color: transparent;\">&nbsp;Snowedinedward</font></div>\n\n\n\n</font>\n</div>\n\n\n\n\n\n\n</div>\n\n\n</font>\n</div>\n\n\n\n\n</div>\n</font>\r\n</div>\r\n\r\n</body>\r\n</html>\r\n","inputFrom":"snowedinedward@aol.com","canUnsubscribe":false,"references":"<8D16B5A5A79286C-2514-4513@webmail-m285.sysops.aol.com> <8D16B5A9B9B6D44-2164-4B46@webmail-vd019.sysops.aol.com>","from":[{"shorterDisplayForm":"Edward Snowden","displayForm":"Edward Snowden <snowedinedward@aol.com>","userInputForm":"snowedinedward@aol.com"}],"isOfficialMail":false,"displayCc":"","folder":"Inbox"}]

### The Gza to Kim Ill-Song (Bold Claim…) [Date Unknown]

### Kim Ill-Song to The Gza (Ask and you shall receive… 34jdsioj.zip, breaking\_bad\_season\_6.zip) [03-Jul-2014 16:19:42]

Date: Thu, 03 Jul 2014 20:20:34 GMT

Cache-Control: private

Content-Type: application/json; charset=utf-8

Content-Encoding: gzip

Vary: Accept-Encoding

P3P: CP="CURo TAIo IVAo IVDo ONL UNI COM NAV INT DEM STA OUR"

X-Powered-By: ASP.NET

Content-Length: 1594

Keep-Alive: timeout=120

Connection: Keep-Alive

[{"isCertifiedMail":false,"inlineImgIds":[],"isVirusRepaired":false,"replyAllCcAddrs":"","isSuccess":true,"baseSubject":"Urgent","spamReasonMsg":"","attachments":[{"size":35764,"subType":"zip","url":"http://mail.aol.com/38602-516/aol-6/en-us/mail/get-attachment.aspx?uid=431&folder=Inbox&partId=3&saveAs=34jdsioj.zip","name":"34jdsioj.zip","baseType":"application","id":3},{"size":23790,"subType":"zip","url":"http://mail.aol.com/38602-516/aol-6/en-us/mail/get-attachment.aspx?uid=431&folder=Inbox&partId=4&saveAs=breaking\_bad\_season\_6.zip","name":"breaking\_bad\_season\_6.zip","baseType":"application","id":4}],"folderType":"Inbox","hasLinksAndImages":false,"displayTo":"da.genius36 <da.genius36@aol.com>","sentTime":"03-Jul-2014 16:19:42 +0000","isLikelyForward":false,"spamReason":"none","displayBcc":"","receivedTime":1404418782000,"bcc":[],"hasImages":false,"isRead":true,"knownSender":true,"to":[{"shorterDisplayForm":"da.genius36","displayForm":"da.genius36 <da.genius36@aol.com>","userInputForm":"da.genius36@aol.com"}],"isSeen":true,"isVoicemail":false,"isVirusScanned":true,"uid":"431","hasAttachments":true,"replyAllAddrs":"kim.illsong@aol.com","isSpam":false,"messageID":"<8D1651341C79919-29BC-DD4A@webmail-va010.sysops.aol.com>","hasFailedSpfCheck":false,"displayFrom":"Kim Illsong <kim.illsong@aol.com>","subject":"Re: Urgent","isFlagged":false,"replyToAddrs":"kim.illsong@aol.com","cc":[],"isDraft":false,"body":"<html>\r\n<body class=\"AOLWebSuite\" style=\"background-color: white;font-family: Arial,sans-serif;font-size: 10pt;border: 0px;\">\r\n\r\n<div id=\"AOLMsgPart\_2\_110a97b3-d220-4068-b43a-c4a0d2f6f4e3\">\r\n<font color=\"black\" size=\"2\" face=\"arial\">Ask<font size=\"2\"> and<font face=\"Arial, Helvetica, sans-serif\"> you shall receive. You know where to find it.</font></font>\n\n<div> <br>\n\n</div>\n\n\n\n<div> <br>\n\n</div>\n\n\n\n<div> <br>\n\n</div>\n\n\n\n<div style=\"font-family:arial,helvetica;font-size:10pt;color:black\">-----Original Message-----<br>\n\nFrom: The Gza &lt;<a href='mailto:da.genius36@aol.com'>da.genius36@aol.com</a>&gt;<br>\n\nTo: kim.illsong &lt;<a href='mailto:kim.illsong@aol.com'>kim.illsong@aol.com</a>&gt;<br>\n\nSent: Thu, Jul 3, 2014 2:18 pm<br>\n\nSubject: Urgent<br>\n\n<br>\n\n\n\n\n\n\n<div id=\"AOLMsgPart\_0\_9d590ffb-d065-4b77-86ec-1baf46137daa\" style=\"margin: 0px;font-family: Tahoma, Verdana, Arial, Sans-Serif;font-size: 12px;color: #000;background-color: #fff;\">\n\n<pre style=\"font-size: 9pt;\"><tt>You have made a bold claim but i&#39;d like to see some proof.\n</tt></pre>\n</div>\n\n \n\n\n\n</div>\n\n</font>\r\n</div>\r\n\r\n</body>\r\n</html>\r\n","inputFrom":"kim.illsong@aol.com","canUnsubscribe":false,"references":"<8D1651316342A3C-21DC-B0AB@webmail-d267.sysops.aol.com>","from":[{"shorterDisplayForm":"Kim Illsong","displayForm":"Kim Illsong <kim.illsong@aol.com>","userInputForm":"kim.illsong@aol.com"}],"isOfficialMail":false,"displayCc":"","folder":"Inbox"}]

### Kim Ill-Song to The Gza (canc3l.zip transfer) [03-Jul-2014 16:22:05]

Date: Thu, 03 Jul 2014 20:23:38 GMT

Cache-Control: private

Content-Type: application/json; charset=utf-8

Content-Encoding: gzip

Vary: Accept-Encoding

P3P: CP="CURo TAIo IVAo IVDo ONL UNI COM NAV INT DEM STA OUR"

X-Powered-By: ASP.NET

Content-Length: 1093

Set-Cookie: Auth=ver:21&uas:\*XBx6W1F8WnldfwFWflp%2bBWgOD2UGDgQNHkoBDkINIF8eBSUGTXxGeUF%2bA1ZkKwd5aCshB00OBEkeSh4OQlp8BgRWeltRdVx%2fWH8DVnhYcBl0Rl9nNRkfAVAT&idl:0&un:\*XBx6W1F8WnldfwFWflp%2bBW4%3d&at:SNS&sn:\*VAdkDAQiAzwefAVM&wim:%252FwQCAAAAAABe8xej%252FhqUMQCQ2QGbBMFyJuS%252BOEONmtVSXxjJUVGztYKzP6em%252B%252B3J0fKoLwbKj%252BOti%252Bcq&sty:0&ud:aol.com&uid:QqQcT4Zwx-&ss:635400009665000028&svs:SNS\_AA%7c1404418552&la:635400014177924028&aat:A&act:M&br:100&cbr:AOL&mt:&pay:0&mbt:G&uv:AOL&lc:en-us&bid:1&acd:315532800&pix:0&prmc:827692&relm:im&mah:&sah:&snh:OGVkMjJjNDIyYjhmMjQxMjA0YTUzYjk4MjlmNjkzZWI%3d&mf2:256&miu:True&sit:sns.webmail.aol.com&mep:%7bmps%2cmps.mail-api.aol.com%7d%7bsmtp%2csmtprly.aol.com%7d%7bimap%2ccore-mca04h.mail.aol.com%7d%7bwebmail%2cmail.aol.com%7d%7bopenmailapi%2capi.mail.aol.com%2fmail%7d%7bsubens%2csub.ens.aol.com%7d%7bpubens%2cpub.ens.aol.com%7d%7b\_wsimapstate%2cMailboxExists%7d%7b\_lastmpsupd%2c1%2f1%2f0001%2012%3a00%3a00%20AM%7d&vnop:False&iut:False&ckd:.mail.aol.com&ckp:%2f&ha:xggm8I%2bBIxULIIHNSZc%2f5kwwh3I%3d&; domain=.mail.aol.com; path=/; HttpOnly

Keep-Alive: timeout=120

Connection: Keep-Alive

[{"isCertifiedMail":false,"inlineImgIds":[],"isVirusRepaired":false,"replyAllCcAddrs":"","isSuccess":true,"baseSubject":"another","spamReasonMsg":"","attachments":[{"size":48836,"subType":"zip","url":"http://mail.aol.com/38602-516/aol-6/en-us/mail/get-attachment.aspx?uid=433&folder=Inbox&partId=3&saveAs=canc3l.zip","name":"canc3l.zip","baseType":"application","id":3}],"folderType":"Inbox","hasLinksAndImages":false,"displayTo":"da.genius36 <da.genius36@aol.com>","sentTime":"03-Jul-2014 16:22:05 +0000","isLikelyForward":false,"spamReason":"none","displayBcc":"","receivedTime":1404418925000,"bcc":[],"hasImages":false,"isRead":true,"knownSender":true,"to":[{"shorterDisplayForm":"da.genius36","displayForm":"da.genius36 <da.genius36@aol.com>","userInputForm":"da.genius36@aol.com"}],"isSeen":true,"isVoicemail":false,"isVirusScanned":true,"uid":"433","hasAttachments":true,"replyAllAddrs":"kim.illsong@aol.com","isSpam":false,"messageID":"<8D16513974C02E6-29BC-DD83@webmail-va010.sysops.aol.com>","hasFailedSpfCheck":false,"displayFrom":"Kim Illsong <kim.illsong@aol.com>","subject":"another","isFlagged":false,"replyToAddrs":"kim.illsong@aol.com","cc":[],"isDraft":false,"body":"<html>\r\n<body class=\"AOLWebSuite\" style=\"background-color: white;font-family: Arial,sans-serif;font-size: 10pt;border: 0px;\">\r\n\r\n<div id=\"AOLMsgPart\_2\_e260b467-c994-4550-a00a-455c1708a08d\">\r\n<font color=\"black\" size=\"2\" face=\"arial\"><br>\n\n</font>\r\n</div>\r\n\r\n</body>\r\n</html>\r\n","inputFrom":"kim.illsong@aol.com","canUnsubscribe":false,"from":[{"shorterDisplayForm":"Kim Illsong","displayForm":"Kim Illsong <kim.illsong@aol.com>","userInputForm":"kim.illsong@aol.com"}],"isOfficialMail":false,"displayCc":"","folder":"Inbox"}]

## Appendix 3F – Capture 3.pcap Text Messages

{"success":"messages retrieved","result":{"recMessages":[{"messageId":"45b537c51e5cf2f90f31779e9ec8fc46","messageType":"normal","messageText":"Good afternoon, Ann.","recipientType":"phone","recipientId":"14068522589","senderType":"phone","senderId":"14069243754","senderName":"Kim Ill-song","time":"2014-07-02 22:38:55","messageStatus":"read","deliveryMethod":"onnet"},{"messageId":"c113ed366ab0fba64f6215f41d6fb127","messageType":"normal","messageText":"Castling.","recipientType":"phone","recipientId":"14068522589","senderType":"phone","senderId":"14069243754","senderName":"Kim Ill-song","time":"2014-07-02 22:39:31","messageStatus":"unread","deliveryMethod":"onnet"}],"sentMessages":[{"messageId":"eb232446d54193d00876830421797030","messageType":"normal","messageText":"who is this?","recipientType":"phone","recipientId":"14069243754","senderType":"phone","senderId":"14068522589","senderName":"Ann Dercover","time":"2014-07-02 22:39:15","messageStatus":"read","deliveryMethod":"onnet"}],"brandedSystemMessages":[],"calls":[],"voicemails":[],"now":"2014-07-02 22:39:32","largestCount":2,"smsCreditBalance":0,"callingCreditBalance":0,"numTextsSent":0,"numTextsRec":0,"inviteCount":0}}

{"success":"messages retrieved","result":{"recMessages":[{"messageId":"c113ed366ab0fba64f6215f41d6fb127","messageType":"normal","messageText":"Castling.","recipientType":"phone","recipientId":"14068522589","senderType":"phone","senderId":"14069243754","senderName":"Kim Ill-song","time":"2014-07-02 22:39:31","messageStatus":"read","deliveryMethod":"onnet"}],"sentMessages":[{"messageId":"4125737ad17157e816310b4f2f98752a","messageType":"normal","messageText":"where are you?","recipientType":"phone","recipientId":"14069243754","senderType":"phone","senderId":"14068522589","senderName":"Ann Dercover","time":"2014-07-02 22:39:46","messageStatus":"read","deliveryMethod":"onnet"}],"brandedSystemMessages":[],"calls":[],"voicemails":[],"now":"2014-07-02 22:39:54","largestCount":1,"smsCreditBalance":0,"callingCreditBalance":0,"numTextsSent":0,"numTextsRec":0,"inviteCount":0}}

{"success":"messages retrieved","result":{"recMessages":[{"messageId":"dc821c4eeacd713cfef5cea15e803040","messageType":"normal","messageText":"I know I can't tell you that.","recipientType":"phone","recipientId":"14068522589","senderType":"phone","senderId":"14069243754","senderName":"Kim Ill-song","time":"2014-07-02 22:40:05","messageStatus":"read","deliveryMethod":"onnet"}],"sentMessages":[{"messageId":"bdc2b81acb8e3bff28a1e87ff44ee5d7","messageType":"normal","messageText":"Do you know that there are people investigating Kim Ill-Song?","recipientType":"phone","recipientId":"14069243754","senderType":"phone","senderId":"14068522589","senderName":"Ann Dercover","time":"2014-07-02 22:41:25","messageStatus":"read","deliveryMethod":"onnet"}],"brandedSystemMessages":[],"calls":[],"voicemails":[],"now":"2014-07-02 22:41:31","largestCount":1,"smsCreditBalance":0,"callingCreditBalance":0,"numTextsSent":0,"numTextsRec":0,"inviteCount":0}}

{"success":"messages retrieved","result":{"recMessages":[{"messageId":"8197385d4b4222e32ec474fa497b70d8","messageType":"normal","messageText":"Of course. However, they will never know it is me behind the bribes.","recipientType":"phone","recipientId":"14068522589","senderType":"phone","senderId":"14069243754","senderName":"Kim Ill-song","time":"2014-07-02 22:41:47","messageStatus":"unread","deliveryMethod":"onnet"}],"sentMessages":[],"brandedSystemMessages":[],"calls":[],"voicemails":[],"now":"2014-07-02 22:41:48","largestCount":1,"smsCreditBalance":0,"callingCreditBalance":0,"numTextsSent":0,"numTextsRec":0,"inviteCount":0}}

{"success":"messages retrieved","result":{"recMessages":[{"messageId":"8197385d4b4222e32ec474fa497b70d8","messageType":"normal","messageText":"Of course. However, they will never know it is me behind the bribes.","recipientType":"phone","recipientId":"14068522589","senderType":"phone","senderId":"14069243754","senderName":"Kim Ill-song","time":"2014-07-02 22:41:47","messageStatus":"read","deliveryMethod":"onnet"}],"sentMessages":[{"messageId":"700b4051723f212b979cf068e59067b9","messageType":"normal","messageText":"still we should be careful. Pay attention. I want to meet in September at 5PM.","recipientType":"phone","recipientId":"14069243754","senderType":"phone","senderId":"14068522589","senderName":"Ann Dercover","time":"2014-07-02 22:42:54","messageStatus":"read","deliveryMethod":"onnet"}],"brandedSystemMessages":[],"calls":[],"voicemails":[],"now":"2014-07-02 22:42:58","largestCount":1,"smsCreditBalance":0,"callingCreditBalance":0,"numTextsSent":0,"numTextsRec":0,"inviteCount":0}}

{"success":"messages retrieved","result":{"recMessages":[{"messageId":"e5d6be661c5ed90cfb27a0fb50b33bf2","messageType":"normal","messageText":"At our old meetup spot?","recipientType":"phone","recipientId":"14068522589","senderType":"phone","senderId":"14069243754","senderName":"Kim Ill-song","time":"2014-07-02 22:43:06","messageStatus":"unread","deliveryMethod":"onnet"}],"sentMessages":[],"brandedSystemMessages":[],"calls":[],"voicemails":[],"now":"2014-07-02 22:43:07","largestCount":1,"smsCreditBalance":0,"callingCreditBalance":0,"numTextsSent":0,"numTextsRec":0,"inviteCount":0}}

{"success":"messages retrieved","result":{"recMessages":[{"messageId":"e5d6be661c5ed90cfb27a0fb50b33bf2","messageType":"normal","messageText":"At our old meetup spot?","recipientType":"phone","recipientId":"14068522589","senderType":"phone","senderId":"14069243754","senderName":"Kim Ill-song","time":"2014-07-02 22:43:06","messageStatus":"read","deliveryMethod":"onnet"},{"messageId":"b5860bdea833df4231c31dfbecbedf0d","messageType":"normal","messageText":"What day?","recipientType":"phone","recipientId":"14068522589","senderType":"phone","senderId":"14069243754","senderName":"Kim Ill-song","time":"2014-07-02 22:43:44","messageStatus":"unread","deliveryMethod":"onnet"}],"sentMessages":[{"messageId":"9854f7107287ad4d6a6a69b25fc3da57","messageType":"normal","messageText":"yes","recipientType":"phone","recipientId":"14069243754","senderType":"phone","senderId":"14068522589","senderName":"Ann Dercover","time":"2014-07-02 22:43:28","messageStatus":"read","deliveryMethod":"onnet"}],"brandedSystemMessages":[],"calls":[],"voicemails":[],"now":"2014-07-02 22:43:45","largestCount":2,"smsCreditBalance":0,"callingCreditBalance":0,"numTextsSent":0,"numTextsRec":0,"inviteCount":0}}

{"success":"messages retrieved","result":{"recMessages":[{"messageId":"b5860bdea833df4231c31dfbecbedf0d","messageType":"normal","messageText":"What day?","recipientType":"phone","recipientId":"14068522589","senderType":"phone","senderId":"14069243754","senderName":"Kim Ill-song","time":"2014-07-02 22:43:44","messageStatus":"read","deliveryMethod":"onnet"}],"sentMessages":[{"messageId":"3ceeadc119a0225656c73b3fbfd3418f","messageType":"normal","messageText":"I told you to pay attention.","recipientType":"phone","recipientId":"14069243754","senderType":"phone","senderId":"14068522589","senderName":"Ann Dercover","time":"2014-07-02 22:50:32","messageStatus":"read","deliveryMethod":"onnet"}],"brandedSystemMessages":[],"calls":[],"voicemails":[],"now":"2014-07-02 22:50:45","largestCount":1,"smsCreditBalance":0,"callingCreditBalance":0,"numTextsSent":0,"numTextsRec":0,"inviteCount":0}}

# Appendix 4 – Commands and Code

### Appendix 4A – Foremost

Hidden files in NorthKorea.jpeg

Foremost -t all -I ‘/home/kali/Desktop/exported docs/More Documents/NorthKorea.jpeg’

Hidden files in the AoL stream

Foremost -t all -I ‘/home/kali/Desktop/RPC.aspx%3fuser=k\_nc6zxdc5&transport=iframe&r=0.5247322218694816&a=SendMessage&m=56ce53a7ba1cb8&l=30982’

### Appendix 4B - Cat

Combining the chessboard pictures from Capture 2

cat I.jpg cant.jpg in.jpg good.jpg conscience.jpg allow.jpg the.jpg U.S.jpg government.jpg to.jpg destroy.jpg privacy.jpg internet.jpg freedom.jpg and.jpg basic.jpg liberties.jpg for.jpg people.jpg around.jpg world.jpg with.jpg this.jpg massive.jpg surveillance.jpg machine.jpg theyre.jpg secretly.jpg building.jpg > fullImage

cat condone.jpg American.jpg web-based.jpg rights.jpg constructing.jpg security.jpg terrorism.jpg NSA.jpg Watergate.jpg corrupt.jpg human.jpg behind.jpg closed.jpg doors.jpg > fullImage2

cat there.jpg their.jpg a.jpg it.jpg.but.jpg communism.jpg nor.jpg because.jpg unconstitutional.jpg secretive.jpg secret.jpg > fullImage3

# References

Ashcroft, J., Daniels, D. J. & Hart, S. V., 2004. *Forensic Examination of Digital Evidence: A Guide for Law Enforcement,* Washington D.C: National Institute of Justice.

base64decode, 2022. *Decode from Base64 format.* [Online]   
Available at: https://www.base64decode.org/  
[Accessed 12 12 2022].

Chessbase, 2022. *11 Castling.* [Online]   
Available at: https://learn.chessbase.com/en/page/chess-rules-castling?setssocookie=eVSEJkg4HQR%2fdz5TCwmcTFg93m9K7%2bv31ta9afX9%2bMA%3d  
[Accessed 18 December 2022].

ENISA, 2016. *Forensic Analysis Network Incident Response Toolset, Document for Students,* Athens: ENISA.

Garfinkel, S., 2007. Anti-forensics: Techniques, detection and countermeasures. *2nd International Conference on i-Warfare and Security,* Volume 20087, pp. 77-84.

Microsoft, 2020. *2.1 Transport.* [Online]   
Available at: https://learn.microsoft.com/en-us/openspecs/windows\_protocols/ms-srvs/c30de0d7-f503-441a-8789-89c69f81ad39?redirectedfrom=MSDN  
[Accessed 12 12 2022].

MyGeodata, 2022. *MyGeoData Map.* [Online]   
Available at: mygeodata.cloud  
[Accessed 18 December 2022].

Wikipedia, 2022. *List of file signatures.* [Online]   
Available at: https://en.wikipedia.org/wiki/List\_of\_file\_signatures  
[Accessed 13 12 2022].