University of Victoria

University of Victoria

ECE 570
Project III: Network Forensics Investigation

Somayeh Roshandel V00942553

Behnaz Saropourian V00857804

August 2020

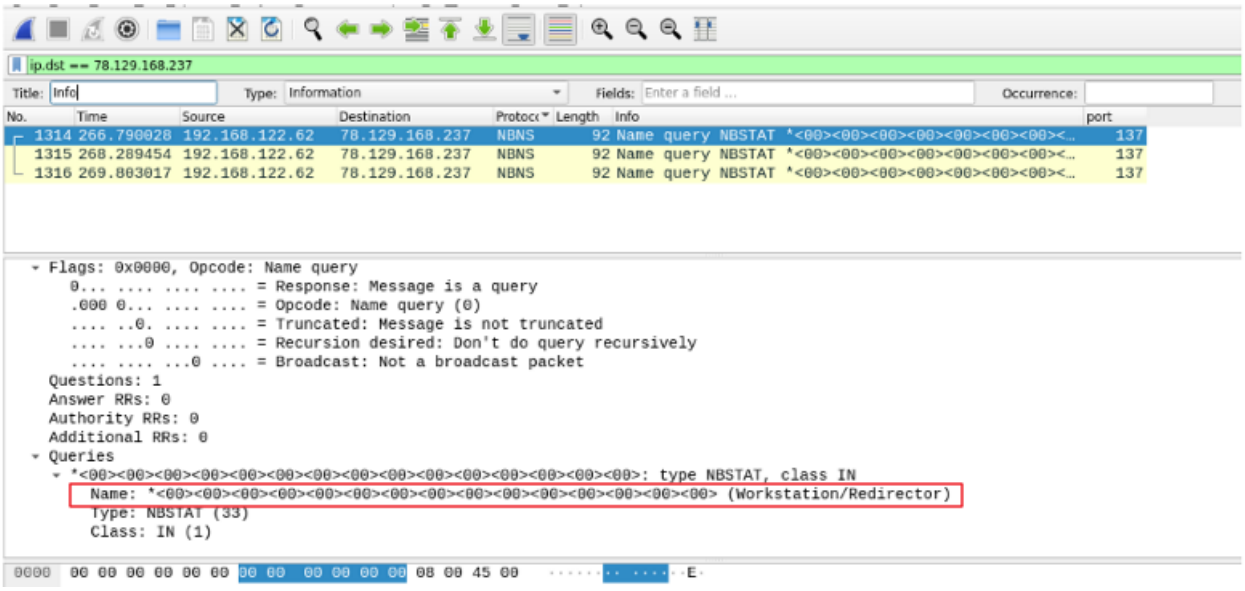
University of Victoria

University of Victoria

1. Identify the following characteristics for the infected host :

a. IP address of computer
b. Hostname of computer
c. MAC address of computer
d. Operating System (OS)

In this scenario we did not have any DHCP packets. Fortunately, we can use NBNS traffic to identify hostnames for computers running Microsoft Windows or Apple hosts running MacOS.
This pcap is from a Windows host using an IP address at 192.168.122.62. Open the pcap in Wireshark and filter on ***nbns***. This should reveal the NBNS traffic. Select the first frame, as shown

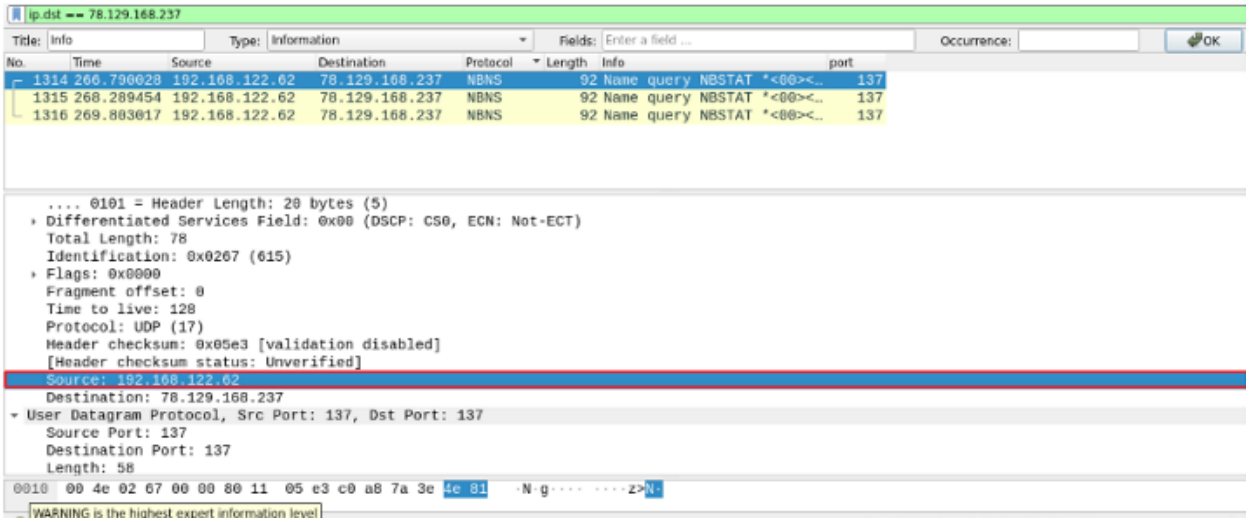


The host name is found here:

University of Victoria

```
▾ Flags: 0x0000, Opcode: Name query
    0... .... .... .... = Response: Message is a query
    .000 0... .... .... = Opcode: Name query (0)
    .... ..0. .... .... = Truncated: Message is not truncated
    .... ...0 .... .... = Recursion desired: Don't do query recursively
    .... .... ...0 .... = Broadcast: Not a broadcast packet
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
▾ Queries
  ▾ *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>: type NBSTAT, class IN
      Name: *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00> (Workstation/Redirector)
      Type: NBSTAT (33)
      Class: IN (1)
```

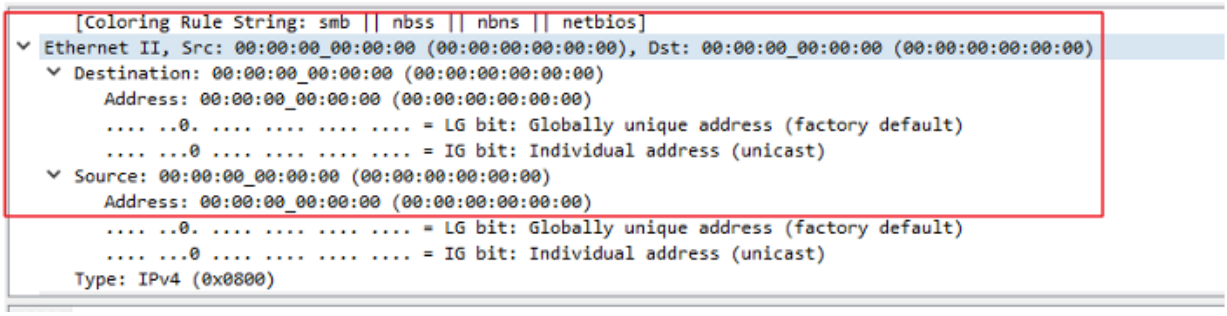
IP address is 192.168.122.62 for host machine found here:



As can be seen that Mac-address is not valid and all octet detected by 0.
This is Mac spoofing or DNS hijacking.

A MAC spoofing attack is where the intruder sniffs the network for valid MAC addresses and attempts to act as one of the valid MAC addresses. The intruder then presents itself as the default gateway and copies all of the data forwarded to the default gateway without being detected. This provides the intruder valuable details about applications in use and destination host IP addresses.

In layer II, we can find MAC addresses. But here all data are changed to zero.



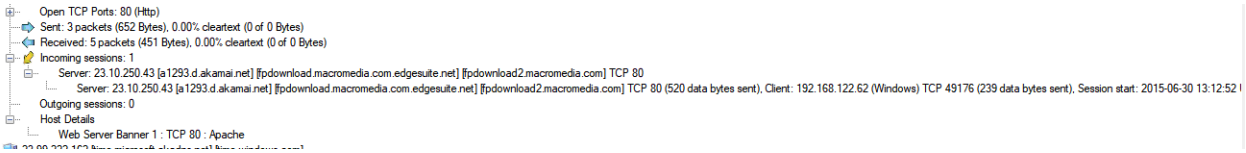
Based on Networkminer report on details of 216.58.210.68, on Host details, we found two Web Server Banner.

A **server banner** is a particular greeting message sent by a **server** running on a host. It is very important to hide this information as it may contain important strings that can

help an attacker to find breaks on your system. This tool shows you the banners sent by popular services over the **internet**. **Server banner** check.

And also we can found that in Network miner Web server banner use here, in screen shot is shown:

The attacker uses 23.10.250.43 and the server IP address is 23.10.250.18. The name is a.1293.d.akamai.net on TCP port 80 use Web Server Banner 1 to DNS hijacking and Mac spoofing.



In wireshark if right click on the IP address that is hosted and go to Follow/TCP stream . In this page we found Operating System information. The screenshot of operating system of host found based on wireshark capture is as follows:

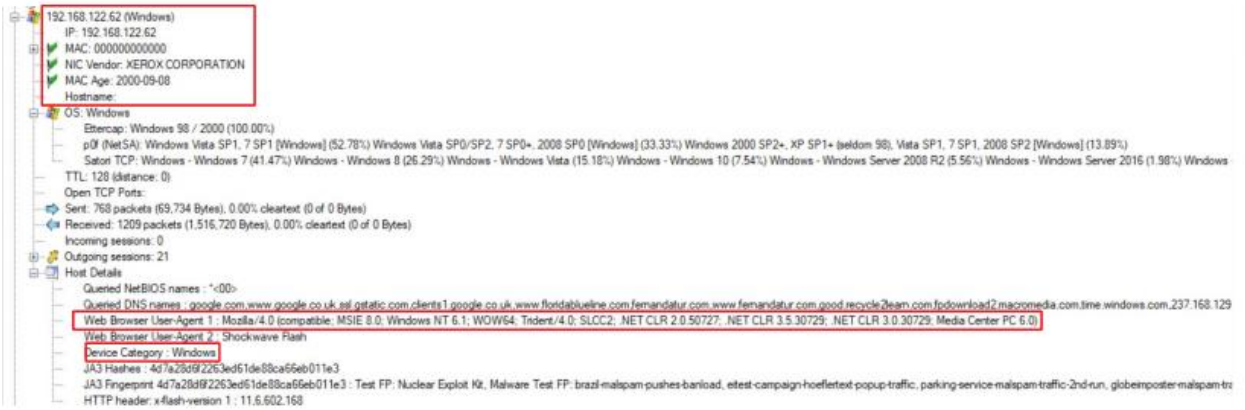
University of Victoria

Wireshark · Follow TCP Stream (tcp.stream eq 0) · ECE570-2020-project3.pcap

```
GET / HTTP/1.1
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap,
application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR
3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
Accept-Encoding: gzip, deflate
Host: google.com
Connection: Keep-Alive
```

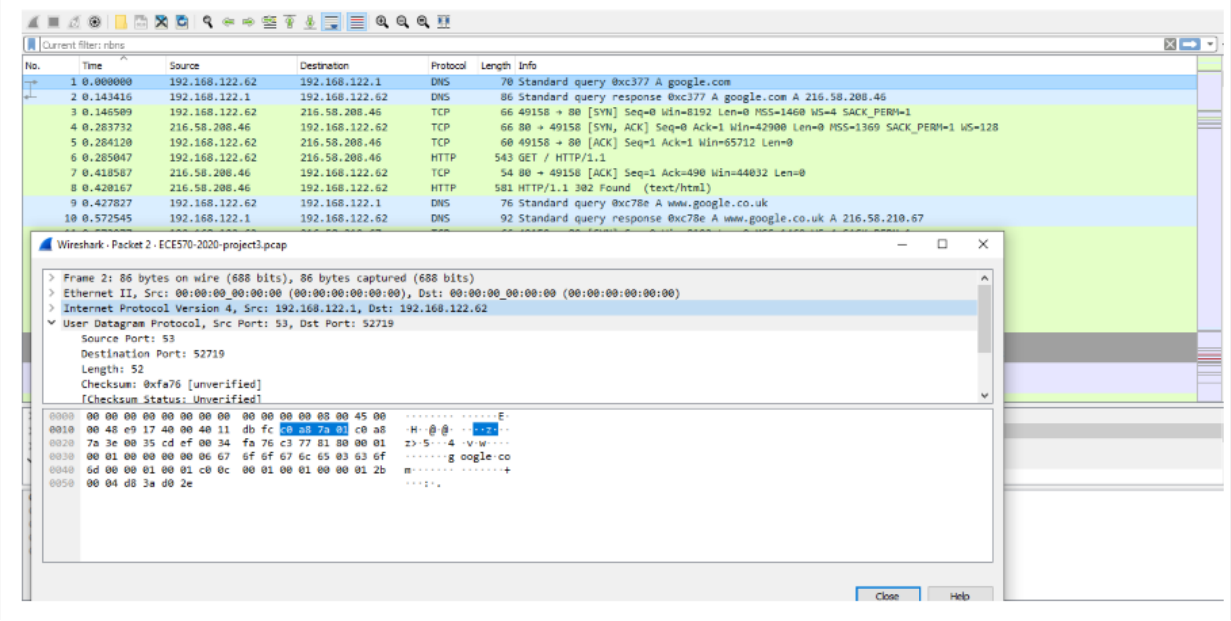
Windows NT 6.1 represents windows 7. So, the operating system of host with ip address 192.168.122.62 is Windows 7.

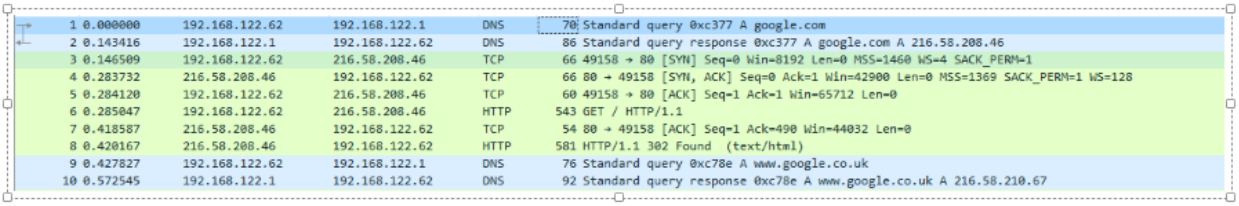
Also according to network miner report, we found information about the infected host such as operating system, IP address, web browser as following picture:



2. What is the IP address and URL of the compromised website the user looked at that triggered the malware traffic (i.e. before the malware traffic happened)?

The scenario starts from first frame in wireshark capture





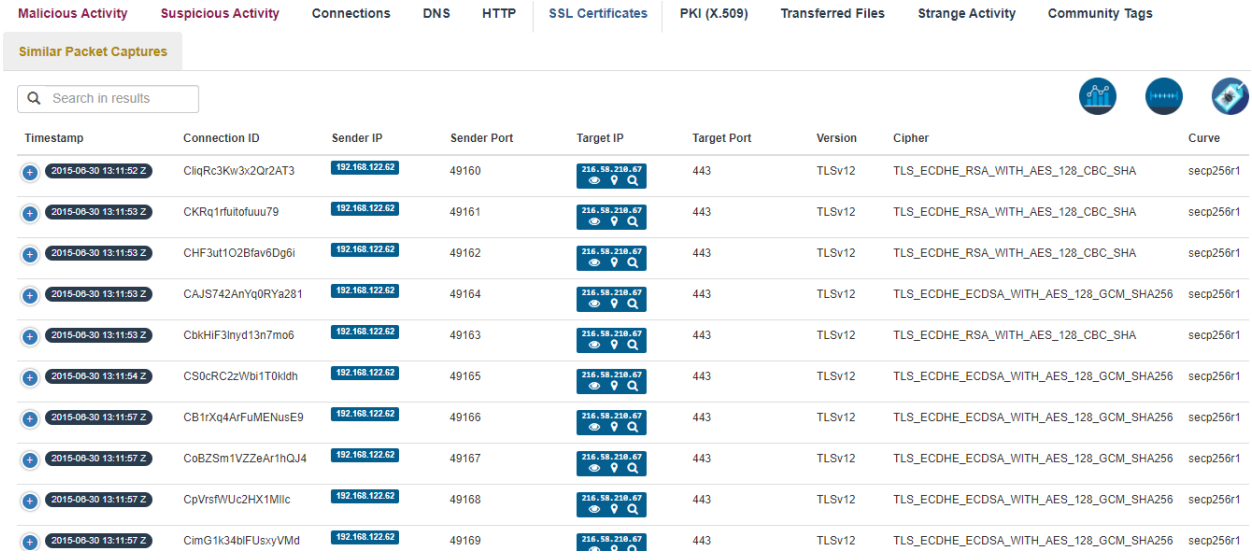
Here 192.168.122.62 target of suspected malware attack sent an packet to 192.168.122.1 as a DNS server for open google.com
A milli seconds later 192.168.122.1 replay to host request. And three TCP handshaking between host and google website done. Then in frame 6 the GET is a Hypertext Transfer Protocol command to ask for data from an HTTP Server.
In frame 8, the response of frame 6 indicates the HyperText Transfer Protocol (HTTP) **302 Found.** It means that redirect status response code indicates that the resource requested has been temporarily moved to the URL given by the Location header.

University of Victoria

So another google website ip address for google.co.uk sent to the host.
Here prove that the host is from the UK.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.122.62	192.168.122.1	DNS	70	Standard query 0xc377 A google.com
2	0.143416	192.168.122.1	192.168.122.62	DNS	86	Standard query response 0xc377 A google.com A 216.58.208.46
3	0.146509	192.168.122.62	216.58.208.46	TCP	66	49158 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
4	0.283732	216.58.208.46	192.168.122.62	TCP	66	80 → 49158 [SYN, ACK] Seq=0 Ack=1 Win=42900 Len=0 MSS=1369 SACK_PERM=1 WS=128
5	0.284120	192.168.122.62	216.58.208.46	TCP	60	49158 → 80 [ACK] Seq=1 Ack=1 Win=65712 Len=0
6	0.285047	192.168.122.62	216.58.208.46	HTTP	543	GET / HTTP/1.1
7	0.418587	216.58.208.46	192.168.122.62	TCP	54	80 → 49158 [ACK] Seq=1 Ack=490 Win=44032 Len=0
8	0.420167	216.58.208.46	192.168.122.62	HTTP	581	HTTP/1.1 302 Found (text/html)
9	0.427827	192.168.122.62	192.168.122.1	DNS	76	Standard query 0xc78e A www.google.co.uk
10	0.572545	192.168.122.1	192.168.122.62	DNS	92	Standard query response 0xc78e A www.google.co.uk A 216.58.210.67
11	0.573977	192.168.122.62	216.58.210.67	TCP	66	49159 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
12	0.620749	192.168.122.62	216.58.208.46	TCP	60	49158 → 80 [ACK] Seq=490 Ack=528 Win=65184 Len=0
13	0.703413	216.58.210.67	192.168.122.62	TCP	66	80 → 49159 [SYN, ACK] Seq=0 Ack=1 Win=42900 Len=0 MSS=1369 SACK_PERM=1 WS=128
14	0.703768	192.168.122.62	216.58.210.67	TCP	60	49159 → 80 [ACK] Seq=1 Ack=1 Win=65712 Len=0
15	0.704222	192.168.122.62	216.58.210.67	HTTP	585	GET /?gfe_rd=cr&ei=l5WSVaXXFrPj8wfRnYHACw HTTP/1.1
16	0.834170	216.58.210.67	192.168.122.62	TCP	54	80 → 49159 [ACK] Seq=1 Ack=532 Win=44032 Len=0
17	0.849802	216.58.210.67	192.168.122.62	HTTP	1187	HTTP/1.1 302 Found (text/html)

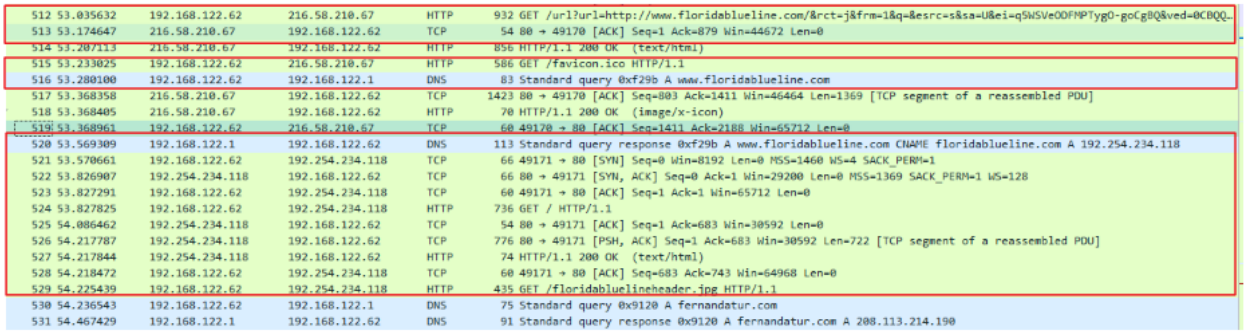
According to information from NetworkMiner and packet total and also wireshark capture report, all communication via TCP, TLSv1.2 are normal till frame 512 that host request for floridablueline.com
In this screenshot information about SSL Certificates are indicates the time between 13:11:52 to 13:11:57 is during access to google.co.uk



Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Version	Cipher	Curve
2015-06-30 13:11:52 Z	CliqRc3Kw3x2Qr2AT3	192.168.122.62	49160	216.58.210.67	443	TLSv12	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	secp256r1
2015-06-30 13:11:53 Z	CKRq1rfuitofuuu79	192.168.122.62	49161	216.58.210.67	443	TLSv12	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	secp256r1
2015-06-30 13:11:53 Z	CHF3ut1O2Bfav6Dg6i	192.168.122.62	49162	216.58.210.67	443	TLSv12	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	secp256r1
2015-06-30 13:11:53 Z	CAJS742AnYq0RYa281	192.168.122.62	49164	216.58.210.67	443	TLSv12	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	secp256r1
2015-06-30 13:11:53 Z	CbkHiF3Inyd13n7mo6	192.168.122.62	49163	216.58.210.67	443	TLSv12	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	secp256r1
2015-06-30 13:11:54 Z	CS0cRC2zWbi1T0kldh	192.168.122.62	49165	216.58.210.67	443	TLSv12	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	secp256r1
2015-06-30 13:11:57 Z	CB1rXq4ArFuMENusE9	192.168.122.62	49166	216.58.210.67	443	TLSv12	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	secp256r1
2015-06-30 13:11:57 Z	CoBZSm1VZZeAr1hQJ4	192.168.122.62	49167	216.58.210.67	443	TLSv12	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	secp256r1
2015-06-30 13:11:57 Z	CpVrsfWUc2HX1MIlc	192.168.122.62	49168	216.58.210.67	443	TLSv12	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	secp256r1
2015-06-30 13:11:57 Z	CimG1k34bIFUsxyVMd	192.168.122.62	49169	216.58.210.67	443	TLSv12	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	secp256r1

And in search engine of this site (www.google.co.uk) host write down and was going to open (access) to floridablueline.com

University of Victoria



512	53.035632	192.168.122.62	216.58.210.67	HTTP	932 GET /url?url=http://www.floridablueline.com/&rct=j&frm=1&q=&esrc=s&sa=U&ei=q5WSVeODFMPTygO-goCgBQ&ved=0CBQQ…
513	53.174647	216.58.210.67	192.168.122.62	TCP	54 80 → 49170 [ACK] Seq=1 Ack=879 Win=44672 Len=0
514	53.207113	216.58.210.67	192.168.122.62	HTTP	856 HTTP/1.1 200 OK (text/html)
515	53.233025	192.168.122.62	216.58.210.67	HTTP	586 GET /favicon.ico HTTP/1.1
516	53.280100	192.168.122.62	192.168.122.1	DNS	83 Standard query 0xf29b A www.floridablueline.com
517	53.368358	216.58.210.67	192.168.122.62	TCP	1423 80 → 49170 [ACK] Seq=803 Ack=1411 Win=46464 Len=1369 [TCP segment of a reassembled PDU]
518	53.368405	216.58.210.67	192.168.122.62	HTTP	70 HTTP/1.1 200 OK (image/x-icon)
519	53.368961	192.168.122.62	216.58.210.67	TCP	60 49170 → 80 [ACK] Seq=1411 Ack=2188 Win=65712 Len=0
520	53.569309	192.168.122.1	192.168.122.62	DNS	113 Standard query response 0xf29b A www.floridablueline.com CNAME floridablueline.com A 192.254.234.118
521	53.570661	192.168.122.62	192.254.234.118	TCP	66 49171 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
522	53.826907	192.254.234.118	192.168.122.62	TCP	66 80 → 49171 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1369 SACK_PERM=1 WS=128
523	53.827291	192.168.122.62	192.254.234.118	TCP	60 49171 → 80 [ACK] Seq=1 Ack=1 Win=65712 Len=0
524	53.827825	192.168.122.62	192.254.234.118	HTTP	736 GET / HTTP/1.1
525	54.086462	192.254.234.118	192.168.122.62	TCP	54 80 → 49171 [ACK] Seq=1 Ack=683 Win=30592 Len=0
526	54.217787	192.254.234.118	192.168.122.62	TCP	776 80 → 49171 [PSH, ACK] Seq=1 Ack=683 Win=30592 Len=722 [TCP segment of a reassembled PDU]
527	54.217844	192.254.234.118	192.168.122.62	HTTP	74 HTTP/1.1 200 OK (text/html)
528	54.218472	192.168.122.62	192.254.234.118	TCP	60 49171 → 80 [ACK] Seq=683 Ack=743 Win=64968 Len=0
529	54.225439	192.168.122.62	192.254.234.118	HTTP	435 GET /floridablueline header.jpg HTTP/1.1
530	54.236543	192.168.122.62	192.168.122.1	DNS	75 Standard query 0x9120 A fernandatur.com
531	54.467429	192.168.122.1	192.168.122.62	DNS	91 Standard query response 0x9120 A fernandatur.com A 208.113.214.190

According to the wireshark and network miner report, after clicking or accessing an image via floridablueline.com.
In frame number 512 in Wireshark, the host machine asks for data from HTTP server.
In frame 515, host request for favicon,ico from HTTP server with GET HTTP1.1 .

Note **HTTP1.1**:

The HyperText Transport Protocol is a text-based request-response client-server protocol. A HTTP client (e.g. a web browser such as Mozilla) performs a HTTP request to a HTTP server (e.g. the Apache HTTP server), which in return will issue a HTTP response. The HTTP protocol header is text-based, where headers are written in text lines.

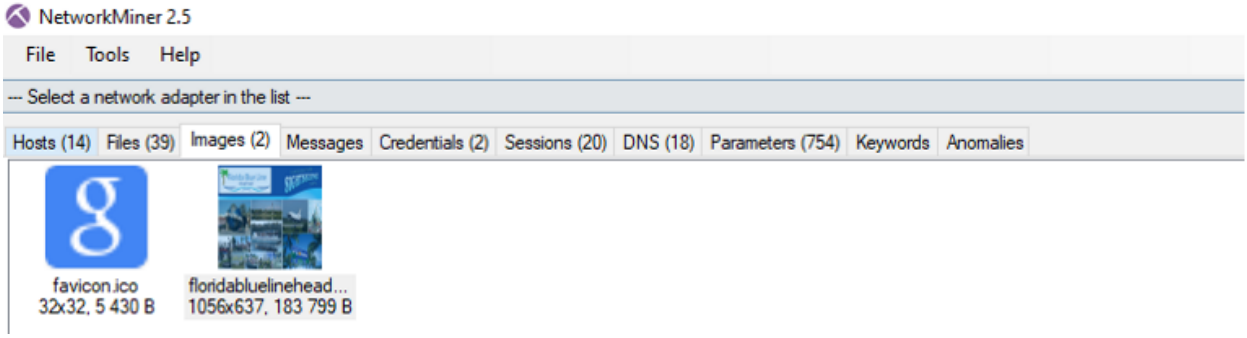
HTTP/1.1 allows for client-server connections to be pipelined, whereby multiple requests can be sent (often in the same packet), without waiting for a response from the server. The only restriction is the server MUST return the responses in the same order as they were received. This enables greater efficiency, especially on revalidation.

The below screenshots indicate that the floridablueline.com host machine requested two pictures, one of them icon (favicon.co) and the other one is header of site (floridabluelineheader.jpg).

University of Victoria

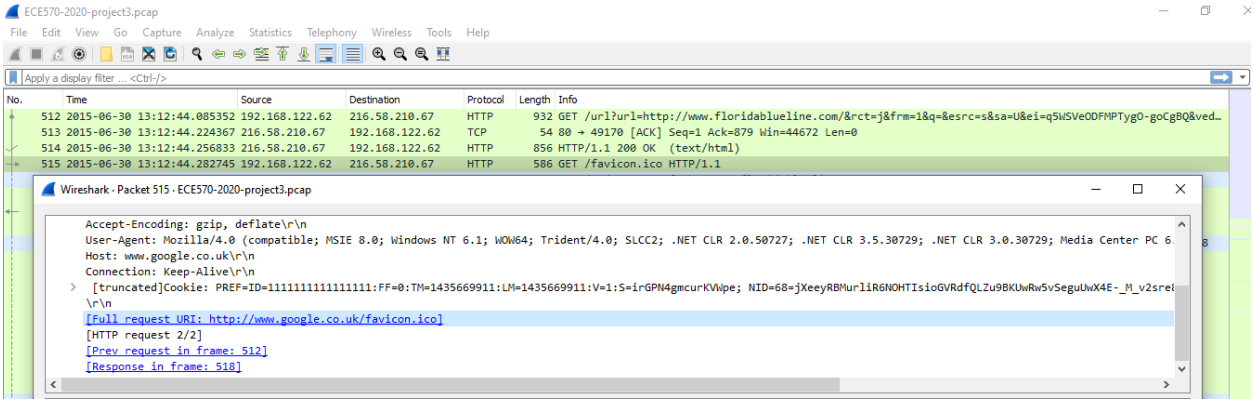
512	2015-06-30 13:12:44.085352	192.168.122.62	216.58.210.67	HTTP	932	GET /url?url=http://www.floridablueline.com/&rct=j&frm=1&q=&esrc=s&sa=U&ei=q5WSVeODFMPTygO-goCgBQ&ved…
513	2015-06-30 13:12:44.224367	216.58.210.67	192.168.122.62	TCP	54	80 → 49170 [ACK] Seq=1 Ack=879 Win=44672 Len=0
514	2015-06-30 13:12:44.256833	216.58.210.67	192.168.122.62	HTTP	856	HTTP/1.1 200 OK (text/html)
515	2015-06-30 13:12:44.282745	192.168.122.62	216.58.210.67	HTTP	586	GET /favicon.ico HTTP/1.1
516	2015-06-30 13:12:44.329820	192.168.122.62	192.168.122.1	DNS	83	Standard query 0xf29b A www.floridablueline.com
517	2015-06-30 13:12:44.418078	216.58.210.67	192.168.122.62	TCP	1423	80 → 49170 [ACK] Seq=803 Ack=1411 Win=46464 Len=1369 [TCP segment of a reassembled PDU]
518	2015-06-30 13:12:44.418125	216.58.210.67	192.168.122.62	HTTP	70	HTTP/1.1 200 OK (image/x-icon)
519	2015-06-30 13:12:44.418681	192.168.122.62	216.58.210.67	TCP	60	49170 → 80 [ACK] Seq=1411 Ack=2188 Win=65712 Len=0
520	2015-06-30 13:12:44.619029	192.168.122.1	192.168.122.62	DNS	113	Standard query response 0xf29b A www.floridablueline.com CNAME floridablueline.com A 192.254.234.118
521	2015-06-30 13:12:44.620381	192.168.122.62	192.254.234.118	TCP	66	49171 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
522	2015-06-30 13:12:44.876627	192.254.234.118	192.168.122.62	TCP	66	80 → 49171 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1369 SACK_PERM=1 WS=128
523	2015-06-30 13:12:44.877011	192.168.122.62	192.254.234.118	TCP	60	49171 → 80 [ACK] Seq=1 Ack=1 Win=65712 Len=0
524	2015-06-30 13:12:44.877545	192.168.122.62	192.254.234.118	HTTP	736	GET / HTTP/1.1
525	2015-06-30 13:12:45.136182	192.254.234.118	192.168.122.62	TCP	54	80 → 49171 [ACK] Seq=1 Ack=683 Win=30592 Len=0
526	2015-06-30 13:12:45.267507	192.254.234.118	192.168.122.62	TCP	776	80 → 49171 [PSH, ACK] Seq=1 Ack=683 Win=30592 Len=722 [TCP segment of a reassembled PDU]
527	2015-06-30 13:12:45.267564	192.254.234.118	192.168.122.62	HTTP	74	HTTP/1.1 200 OK (text/html)
528	2015-06-30 13:12:45.268192	192.168.122.62	192.254.234.118	TCP	60	49171 → 80 [ACK] Seq=683 Ack=743 Win=64968 Len=0

Both pictures are shown in Networkminer report.

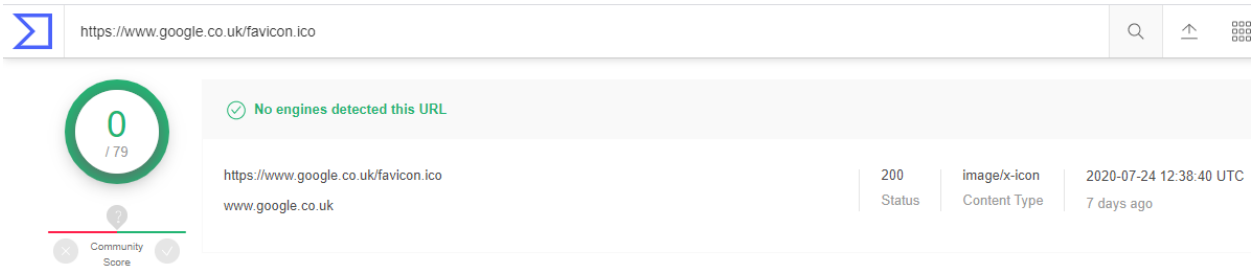


And also, we check both pictures linked on virusttotal.com which are clean. Screen shots of virustotal and wireshark about those pictures as a following pictures:

This site is clean and safe http://www.google.co.uk/favicon.ico

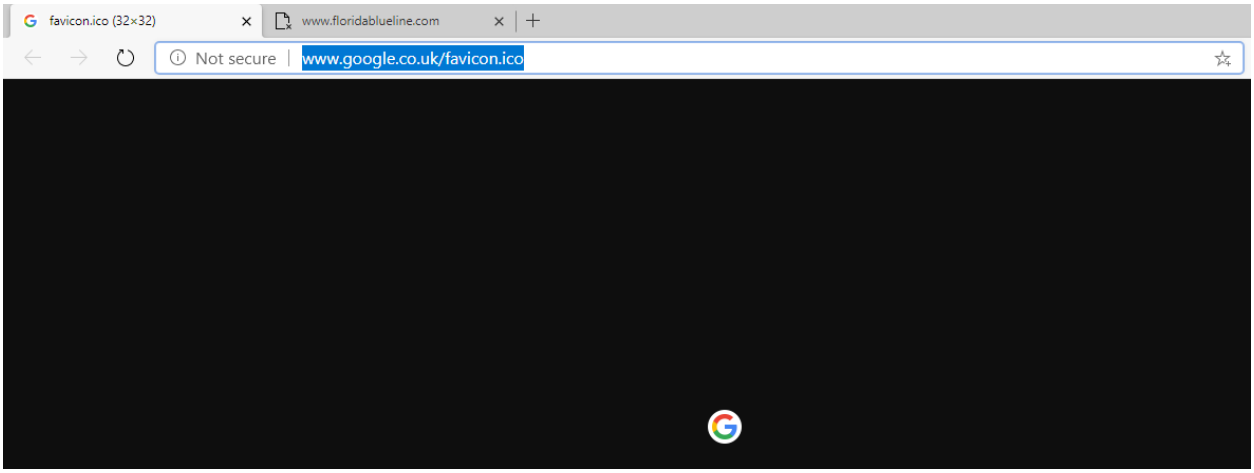


University of Victoria



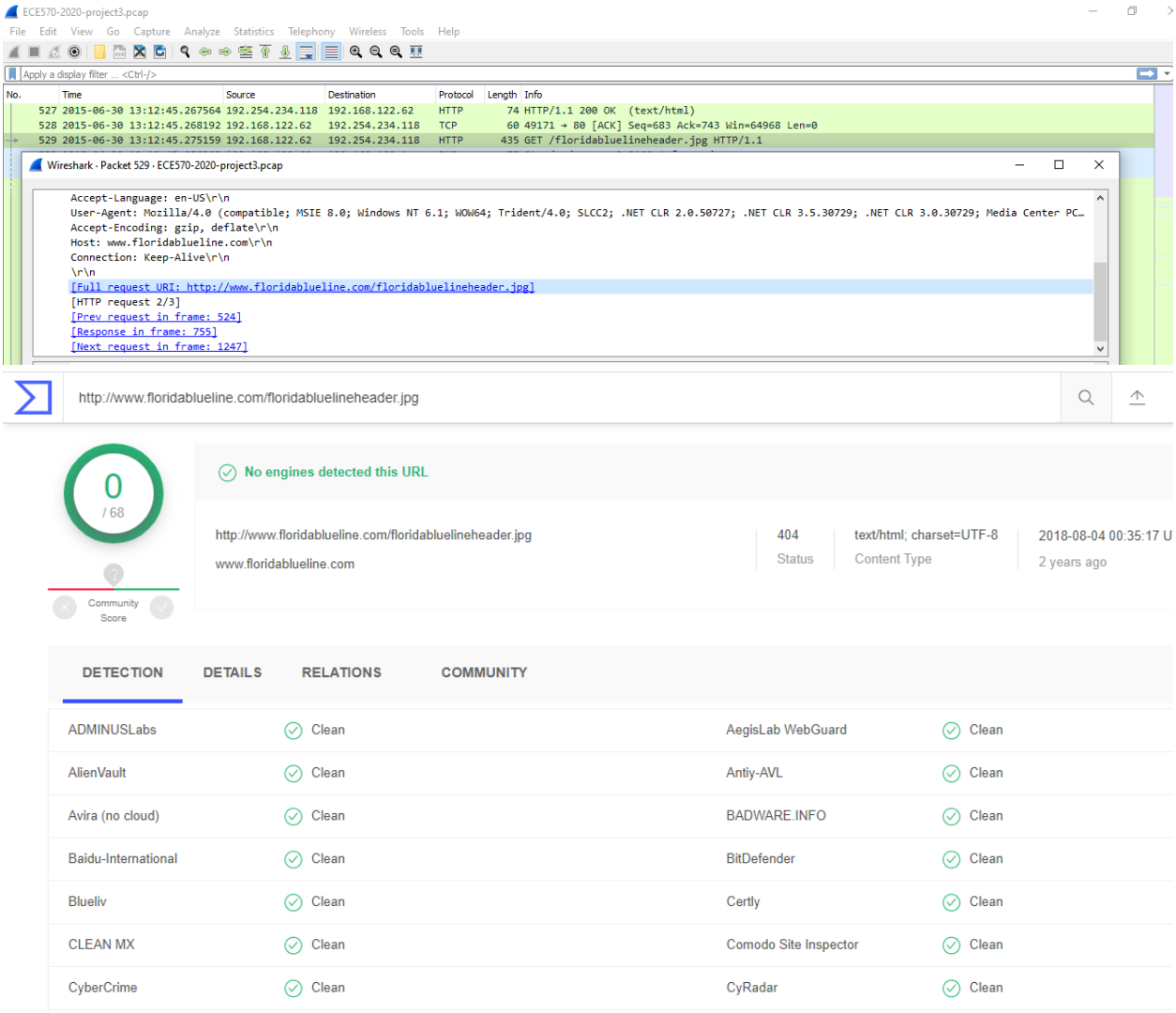
DETECTION | DETAILS | COMMUNITY

ADMINUSLabs	Clean	AegisLab WebGuard	Clean
AlienVault	Clean	Antiy-AVL	Clean
Artists Against 419	Clean	Avira (no cloud)	Clean
BADWARE.INFO	Clean	Baidu-International	Clean
BitDefender	Clean	BlockList	Clean
Blueliv	Clean	Botvrij.eu	Clean
Certego	Clean	CINS Army	Clean



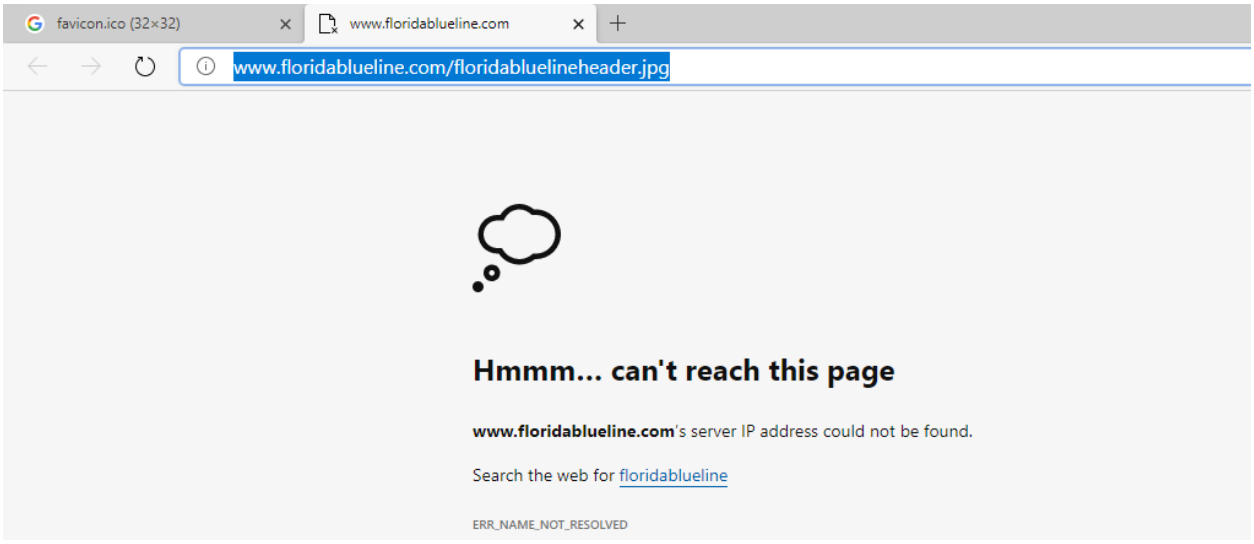
The header picture is safe http://www.floridablueline.com/floridablulineheader.jpg

University of Victoria

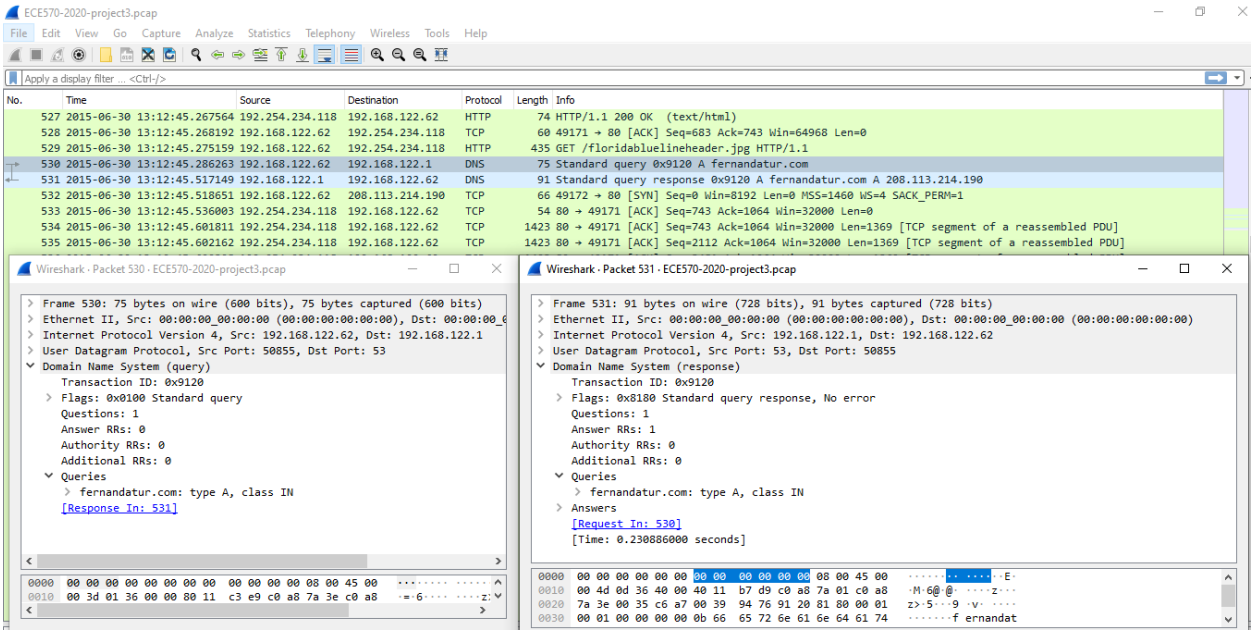


But this site has a **404 error** that indicates the server itself was found, but that the server was not able to retrieve the requested page.

University of Victoria

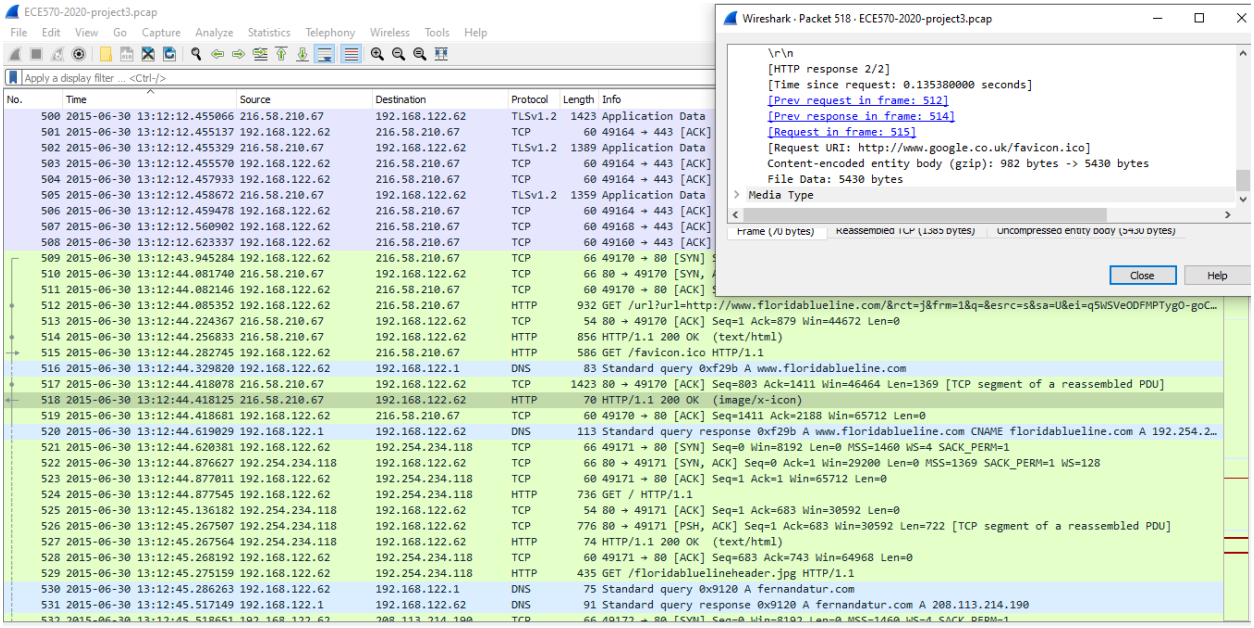


In frame 530, the host requested another website. The name of the website is **fernandatur.com** screen shots of request/response frames (530/531 in wireshark) are shows as a follows:

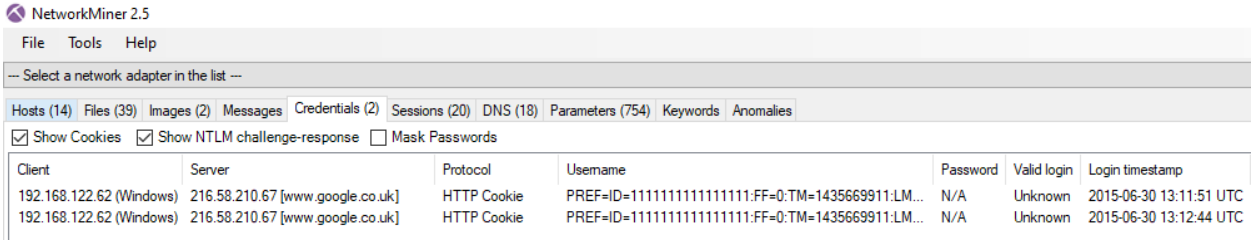


Note: when host access to floridablueline.com cookies created in 13:12:44

And later than in 13.11.51 another cookies created for google.co.uk
Both sites server is google.co.uk



based on network miner/credentials report, at the same time 13:12:44 HTTP (same time based on wireshark screenshots in above) cookies are created.



Based on the packet total report, in Transferred Files. We have two files transferred in that transfer between google.co.uk website (216.58.218.67) and host machine(192.168.122.67) in the time 13:12:44 and date 2015-06-30, text/plain and image/x-icon . Both of them are virustotal safe. Screenshots are as follows:

University of Victoria

2015-06-30 13:12:44 Z	CIFU4P2TqMGvSgfc62	FVBL1H1FVSERASI...	1332bd535c01fd41228b3e6c6f5e1723	da9515044bb6322029418f62870ccdede3c35aef7	216.58.210.67		192.168.122.62	HTTP	0

Mime Type	text/plain
File Name	null
Total Bytes	null

2015-06-30 13:12:44 Z	CIFU4P2TqMGvSgfc62	FB9ZMI3KOMATOYM...	a300693728f5caa531a6886d9b8f38c2	e2020bf4f2b65f62434c62ea967973140b3300df	216.58.210.67		192.168.122.62	HTTP	0

Mime Type	image/x-icon
File Name	null
Total Bytes	null

Two screenshots that prove no detection based on virustotal.com report:

165e12d13971f01b4c668d177d9bec4336856a1cf9ac946eb5953b93bef37cfb

0 / 58

Community Score

No engines detected this file

165e12d13971f01b4c668d177d9bec4336856a1cf9ac946eb5953b93bef37cfb

&rct=j&frm=1&q=&esrc=s&sa=U&ei=q5WSVeODFMPTygO-goCgBQ&ved=0CBQQFjAA&usg=AFQjCNEUrnlRimmDVTKWno90XOpmcDu8zA

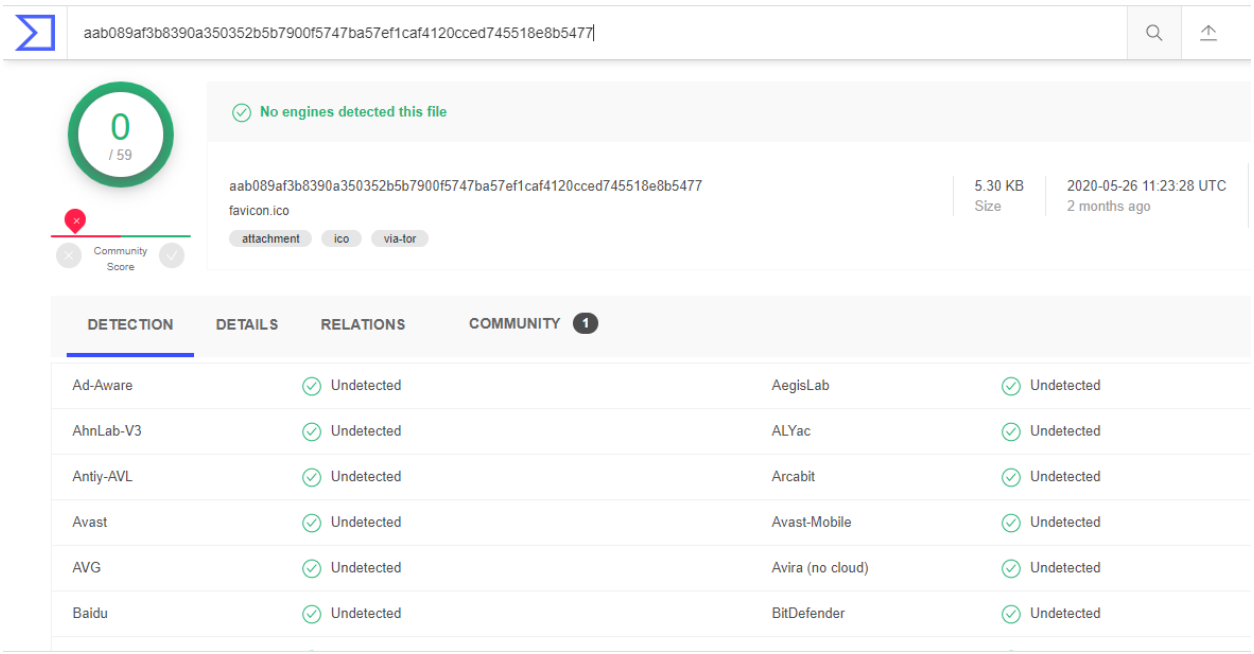
text

1.04 KB Size

2018-08-04 04:16:15 UTC 2 years ago

DETECTION DETAILS COMMUNITY

Ad-Aware	Undetected	AegisLab	Undetected
AhnLab-V3	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	Avast-Mobile	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
AVware	Undetected	Babable	Undetected



According to investigation all transferred Files in packet total From 13:11:51 that the capture started, to 13:12:44. We found that in these periods of time files, text, images, packets transferred were safe.

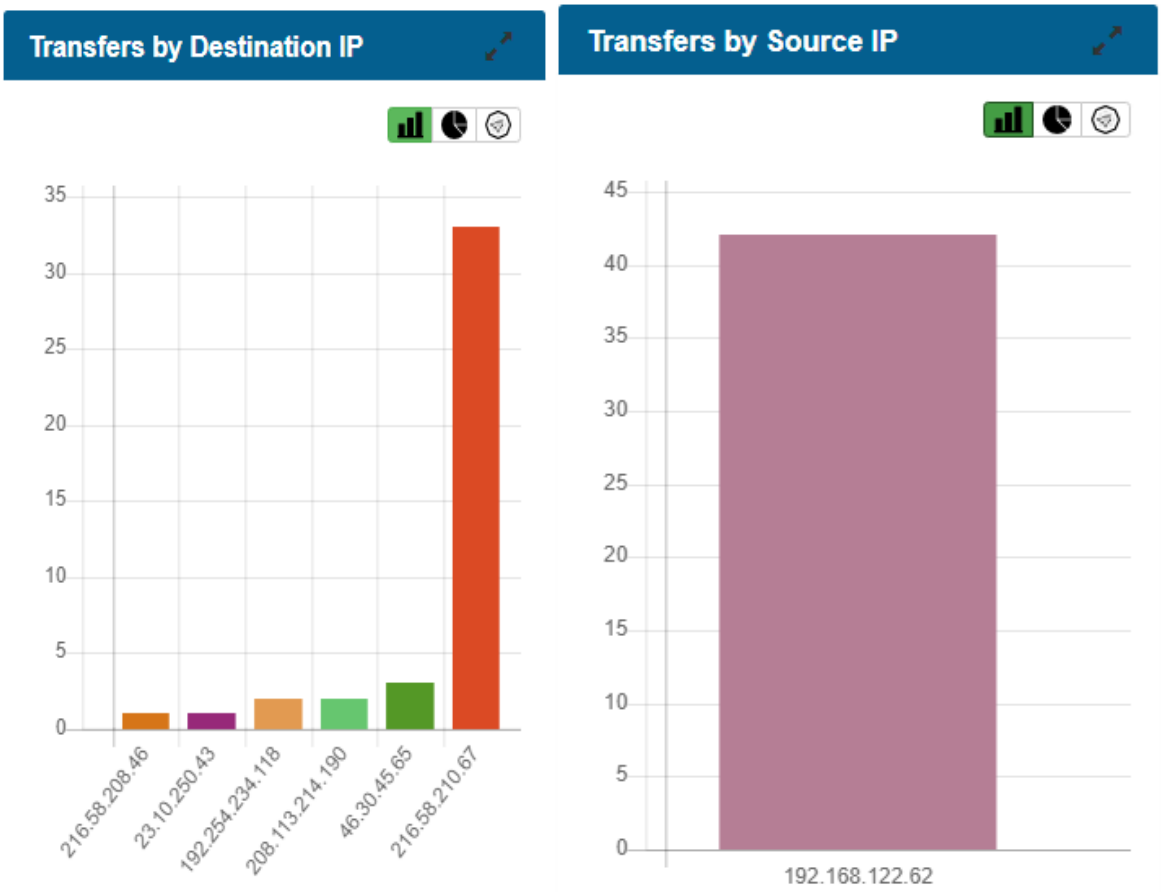
The graph shows in the following pictures:

University of Victoria

In this picture transfer data starts from the time 13:11:51 in the first frame of wireshark capture. After 14:00:41 duration transferred data received to time 13:12:44.
So the time that our diagram is zero is between 13:11:57 and 13:12:44.

And also transferred files by source ip and destination ip during this time shown as following pictures in Bar chart:

University of Victoria



34 files transferred between host and three different destination to those destination and host including: google.com, google.co.uk, and floridablueline.com that all of them checked on virustotal.com from Transferred Files Tab in packet total and they are clean and no detected report.

But at 13:12:45 the malicious traffic started.
According to the packettotal report, three Malicious activity from source IP address 192.265.234.118 related to floridablueline.com website to host machine (192.168.122.62) on TCP protocol done.

University of Victoria

Malicious Activity | Suspicious Activity | Connections | DNS | HTTP | SSL Certificates | PKI (X.509) | Transferred Files | Strange Activity | Community Tags

Similar Packet Captures

Search in results

Timestamp	Alert Description	Alert Signature	Severity	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	HTTP Hostname
2015-06-30 13:12:45 Z	A Network Trojan was detected	ET CURRENT_EVENTS Malicious Redirect 8x8 script tag	1	192.254.234.118	80	192.168.122.62	49171	TCP	www.floridablueline.com
2015-06-30 13:12:45 Z	A Network Trojan was detected	ET CURRENT_EVENTS Evil Redirector Leading to EK Dec 09	1	192.254.234.118	80	192.168.122.62	49171	TCP	www.floridablueline.com
2015-06-30 13:12:45 Z	A Network Trojan was detected	ET CURRENT_EVENTS Evil Redirector Leading to EK Jul 08	1	192.254.234.118	80	192.168.122.62	49171	TCP	www.floridablueline.com

Attention to alerts signature of those three malicious activities and description show that **A Network Trojan was detected.**

We check all three alerts one by one and screenshots are in the following pictures. All three alerts contain one HTTP referred that checked on virus total. And also, all alerts description.

First alert alert signature mentions the ET CURRENT_EVENTS Malicious Redirect 8x8 script tag. The picture show that a malicious script appended from the infected website:

Timestamp	Alert Description	Alert Signature	Severity	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	HTTP Hostname
2015-06-30 13:12:45 Z	A Network Trojan was detected	ET CURRENT_EVENTS Malicious Redirect 8x8 script tag	1	192.254.234.118	80	192.168.122.62	49171	TCP	www.floridablueline.com

HTTP URI /

HTTP Content-Type text/html

HTTP Method GET

HTTP User Agent ....NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)

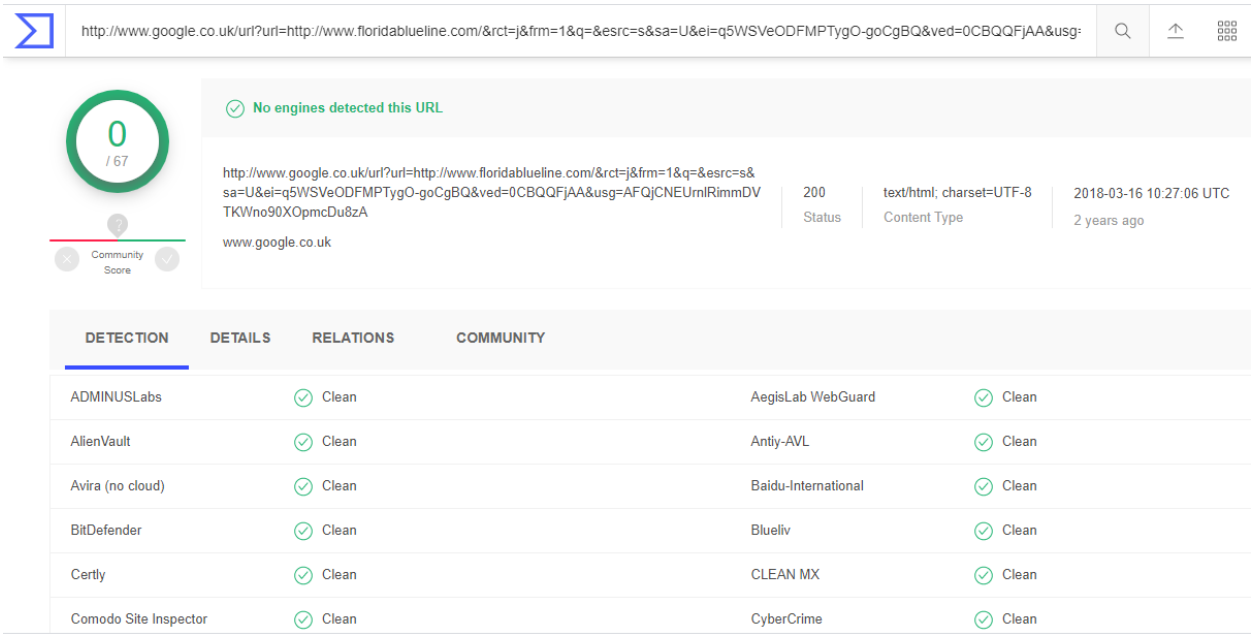
HTTP Referrer http://www.google.co.uk/url?url=http://www.floridablueline.com/&rct=j&frm=1&q=&esrc=s&sa=U&ei=q5WSVeODFMPTygO-goCgBQ&ved=0CBQQFjAA&usg=AFQjCNEUrnlRimmDVTKWno90XOpmcDu8zA

HTTP Protocol HTTP/1.1

HTTP Length 516

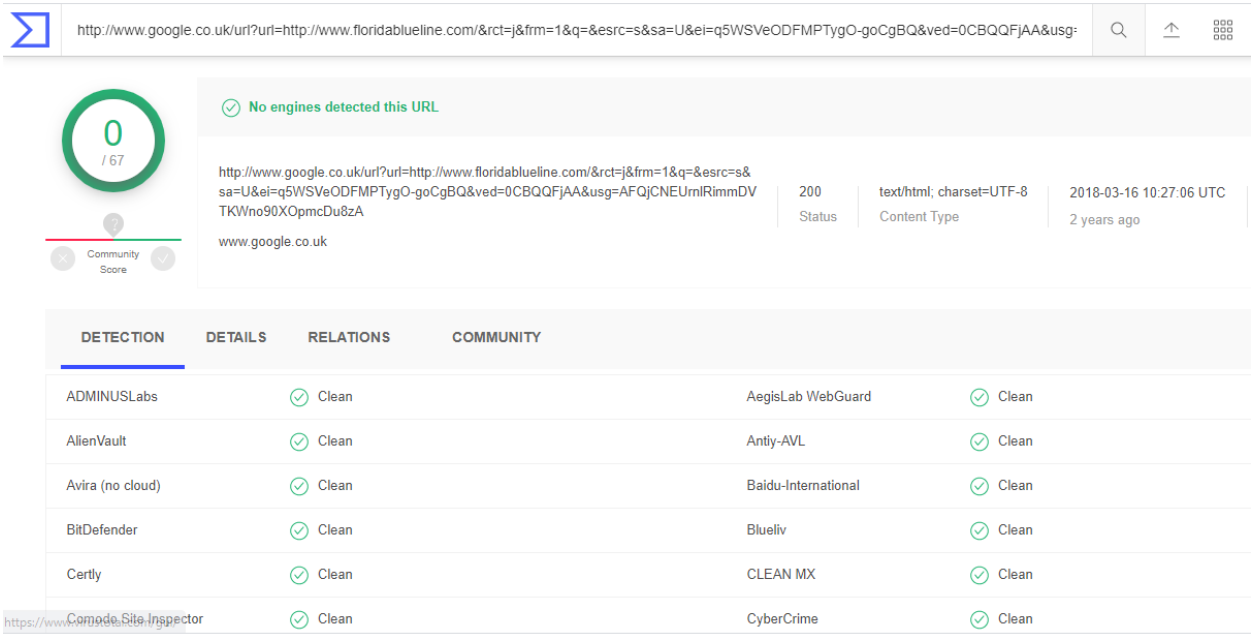
HTTP Status Code 200

When checked HTTP referred on virustotal.com we found this URL is clean:



The second alert signature is ET CURRENT_EVENTS Evil Redirector Leading to EK Dec 09. This alert is show:

When checked HTTP referred on virustotal.com we found this URL is clean:



The third alert is ET CURRENT_EVENTS Evil Redirector:

When checked HTTP referred on virustotal.com we found this URL is clean:

http://www.google.co.uk/url?url=http://www.floridablueline.com/&rct=j&frm=1&q=&esrc=s&sa=U&ei=q5WSVeODFMPTygO-goCgBQ&ved=0CBQQFjAA&usg=

0 / 67

Community Score

No engines detected this URL

http://www.google.co.uk/url?url=http://www.floridablueline.com/&rct=j&frm=1&q=&esrc=s&sa=U&ei=q5WSVeODFMPTygO-goCgBQ&ved=0CBQQFjAA&usg=AFQjCNEUrnlRimmDVTKWno90XOpmcDu8zA

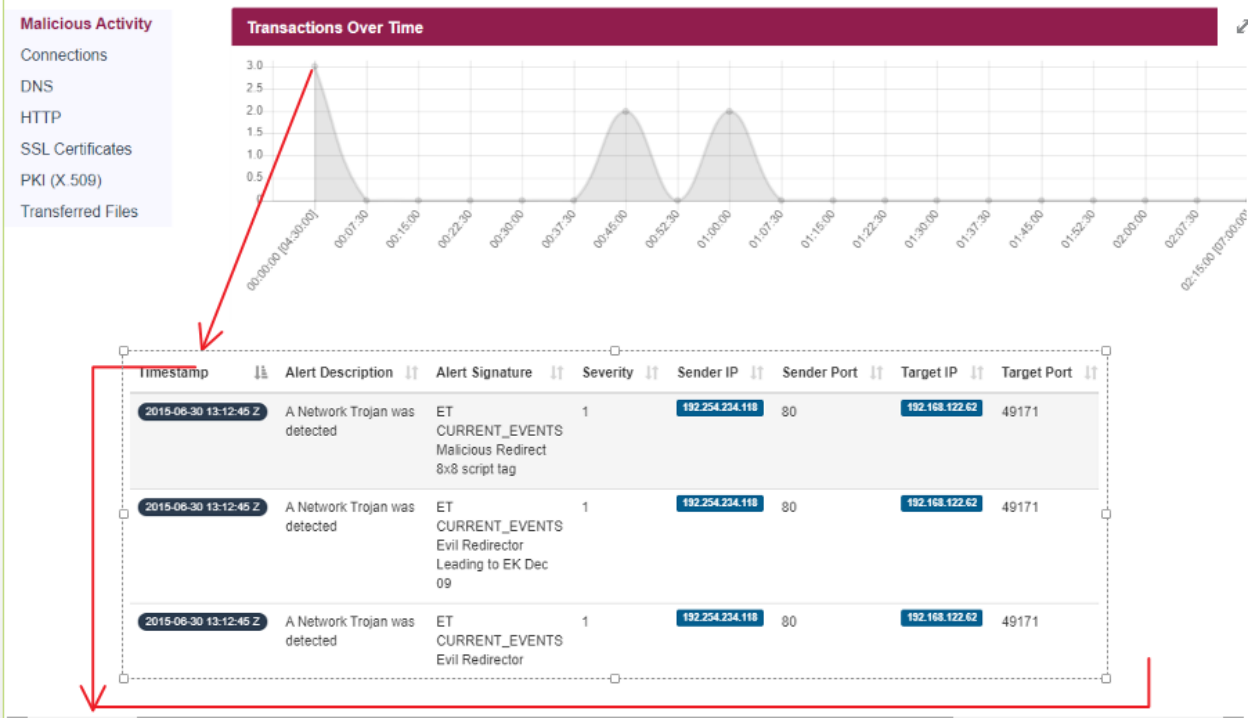
www.google.co.uk

200	text/html; charset=UTF-8	2018-03-16 10:27:06 UTC
Status	Content Type	2 years ago

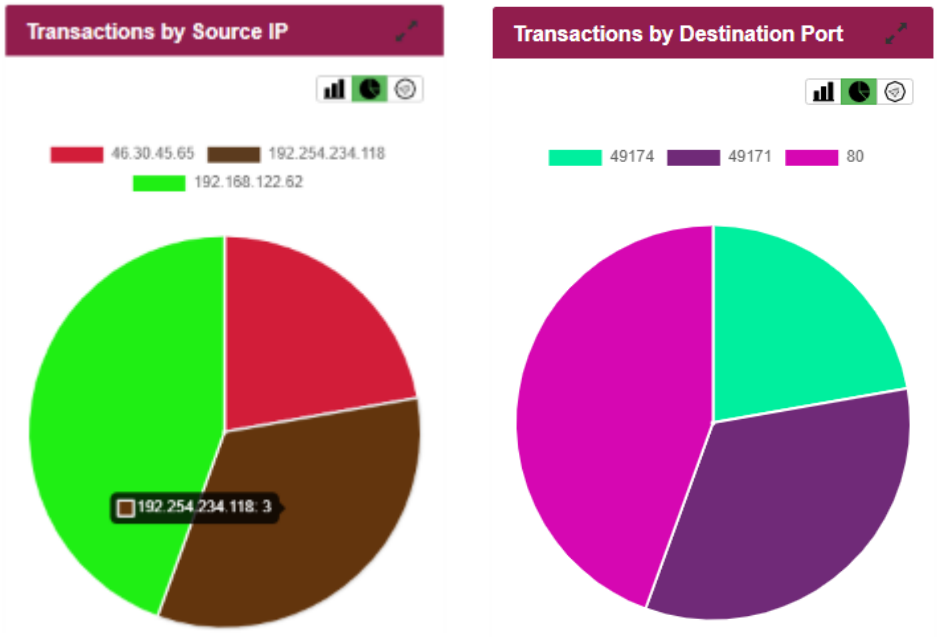
DETECTION | DETAILS | RELATIONS | COMMUNITY

ADMINUSLabs	Clean	AegisLab WebGuard	Clean
AlienVault	Clean	Antiy-AVL	Clean
Avira (no cloud)	Clean	Baidu-International	Clean
BitDefender	Clean	Blueliv	Clean
Certly	Clean	CLEAN MX	Clean
Comodo Site Inspector	Clean	CyberCrime	Clean

The graph of show as follows, those three transactions are highlights by red line on the graph.



The pie chart illustrates three transaction occurs by source ip (192.254.234.118) And also three transaction Destination ports are 49171 on TCP protocol.



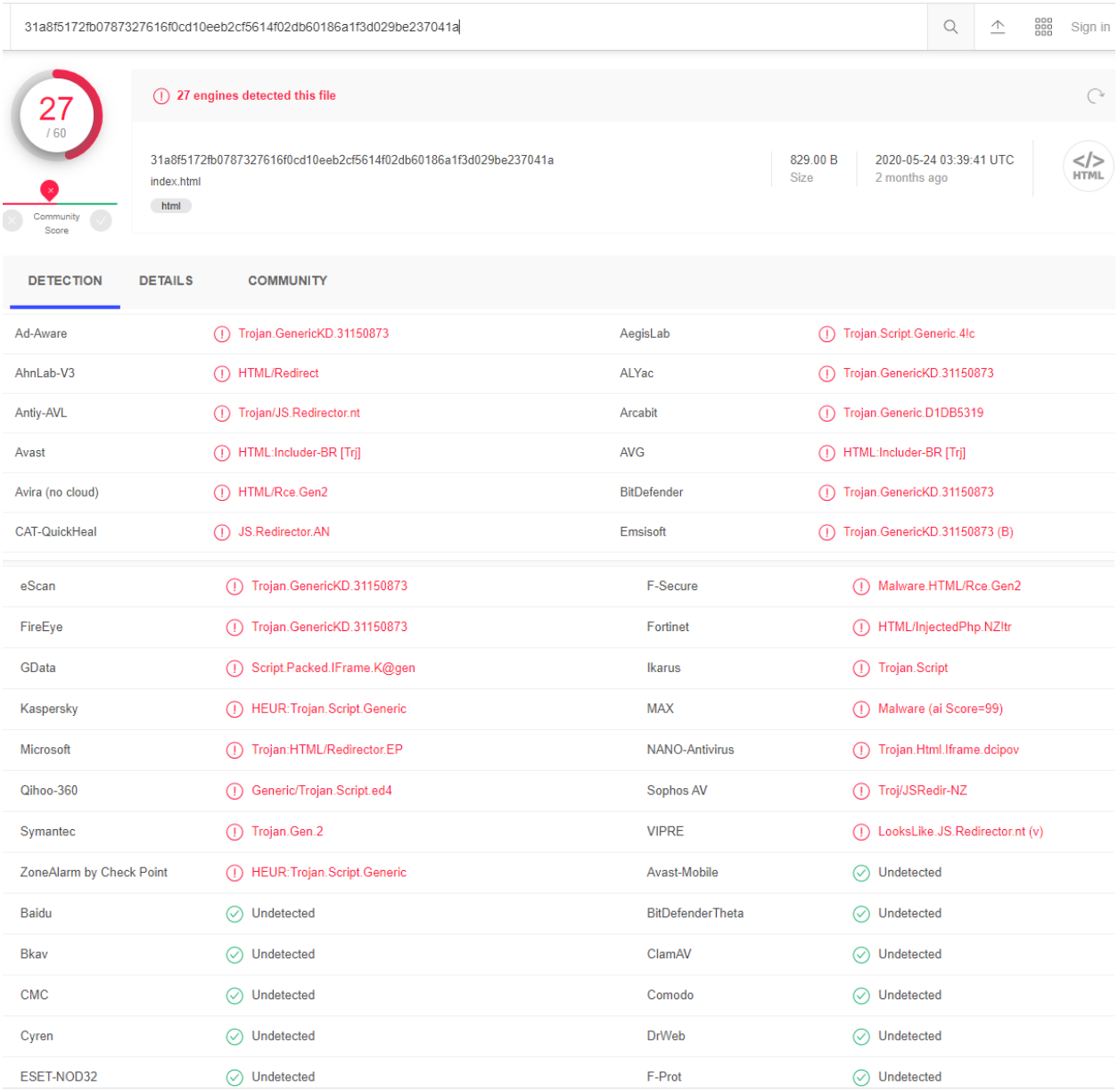
And also in this time 13.12.45 we checked Transferred Files in packet total and we found that three files transferred in that time, the screenshots are shown as following picture:

University of Victoria

Timestamp	Connection IDs	Artifact	MD5 Hash	SHA1 Hash	Originated From Host/s	Sent To Host/s	Source	Depth
2015-06-30 13:12:45 Z	CALygR1JnJXOgNnETj	FIA30B1ZBQB6MYX...	6535a237a2652f5d03b034fe52ff9fea	462fdab7eaf516bd8197aa7e9307f8473ff34570	192.254.234.118	192.168.122.62	HTTP	0
Mime Type	text/html							
File Name	null							
Total Bytes	null							
2015-06-30 13:12:45 Z	CALygR1JnJXOgNnETj	FIC2ID2ENIQ6Z2U...	cb5d1061b1ef3b2204f3c8efd666d4918	8fbec3e6569cefaacd30de45c80cab2b95cdbe35	192.254.234.118	192.168.122.62	HTTP	0
Mime Type	image/jpeg							
File Name	null							
Total Bytes	183799							
2015-06-30 13:12:45 Z	CMvAQV2OwfXQnWdhX2	FIPQVF2Z3IGGRO7...	1675befb11864f12ed74b68dfae7c21c	f162bf38954f6a9d8e8f8359b77b624b829a8580	208.113.214.190	192.168.122.62	HTTP	0
Mime Type	text/html							
File Name	null							
Total Bytes	null							

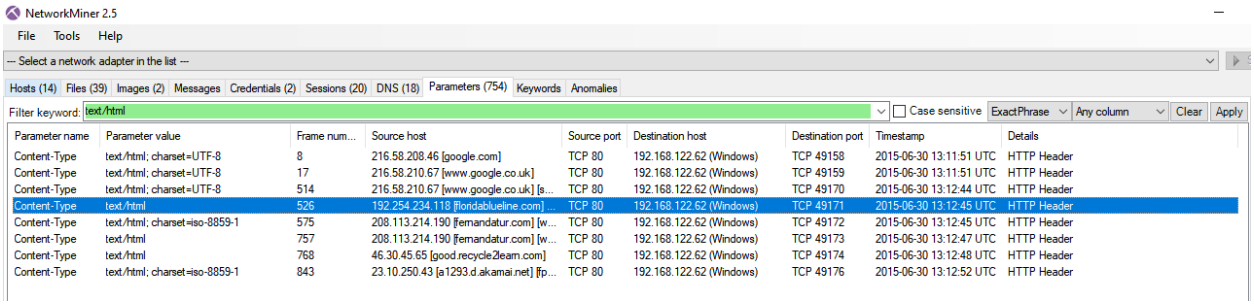
The check of all those three files on virustotal shows that the first files include text/html detected by 27 engines in virustotal.com and Trojan this is trojan scripts.
The other two files are checked in virus total and clean.
This file transferred from 192.254.234.118 that we know is the ip address of floridablueline.com to our host machine with the IP address of 192.168.122.62 on HTTP protocol. The virustotal report is shows as follows:

University of Victoria

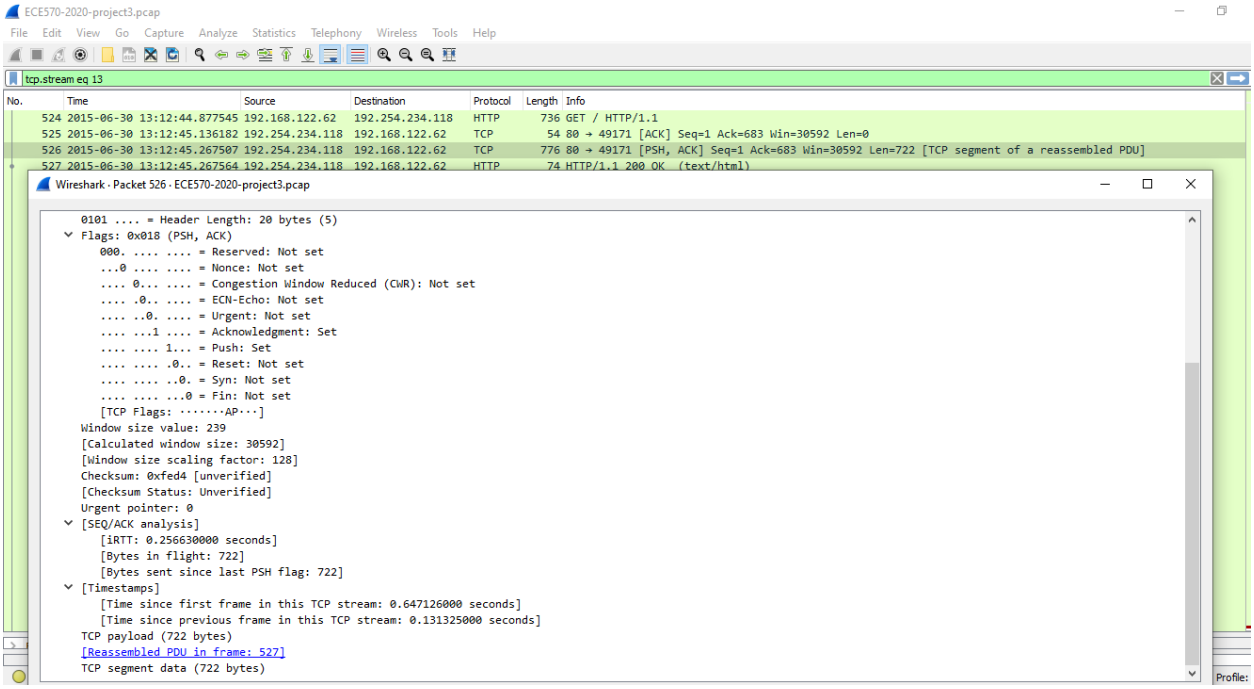


The Network Miner report in parameters shows that this file is on frame 526.

University of Victoria



The wireshark information on frame 526 show that this frame reassembled PDU in frame 527.The screen shot is shown in following picture:

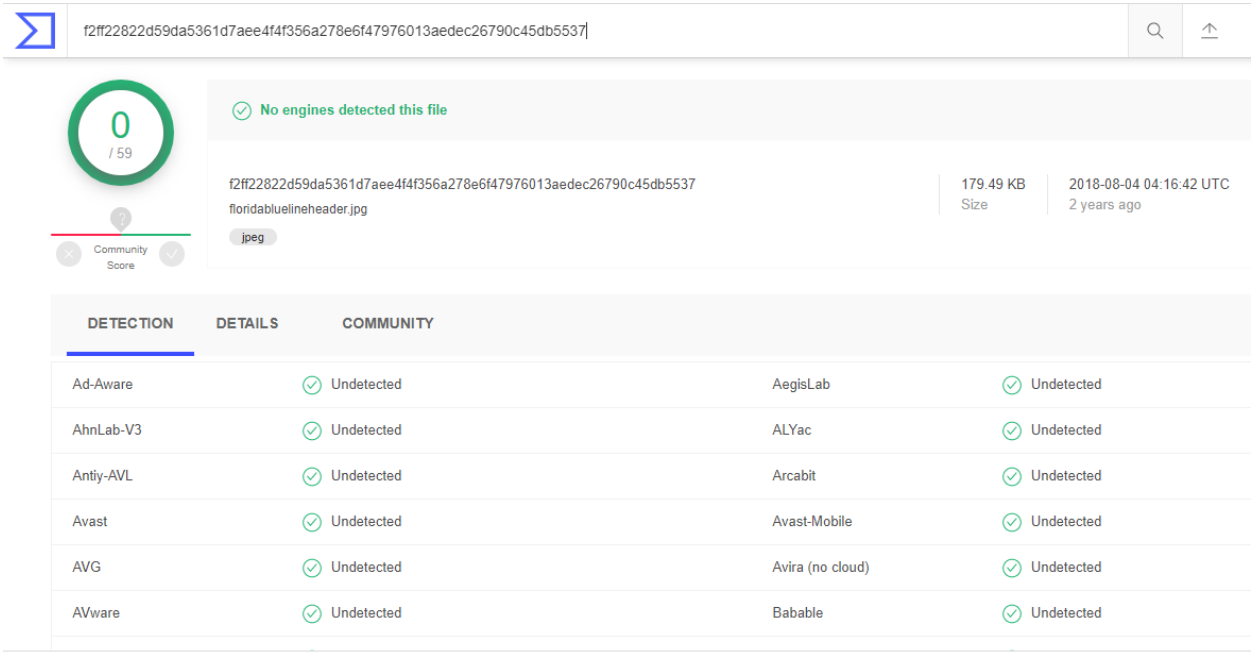


In this frame, frame 526, we have PSH,ACK.

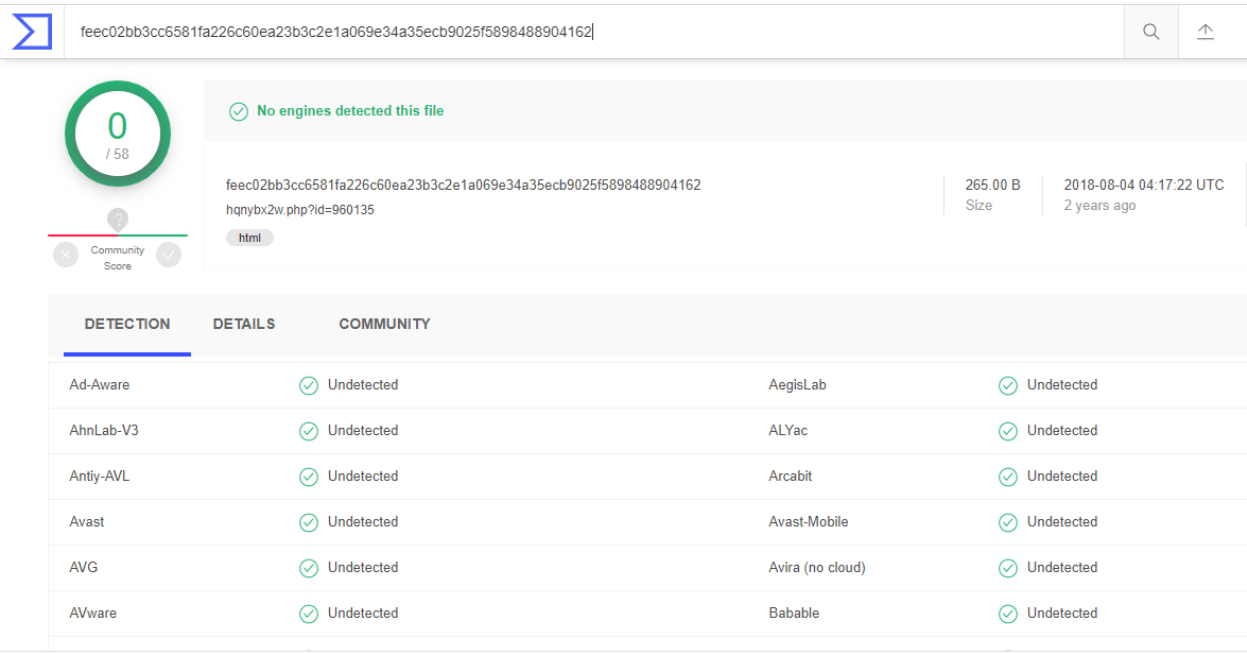
The **ACK** indicates that a host is acknowledging having received some data, and the **PSH**,**ACK** indicates the host is acknowledging receipt of some previous data and also transmitting some more data.

So, here based on all information above **floridablueline.com** with the ip address of 192.254.234.118 is the compromised website.

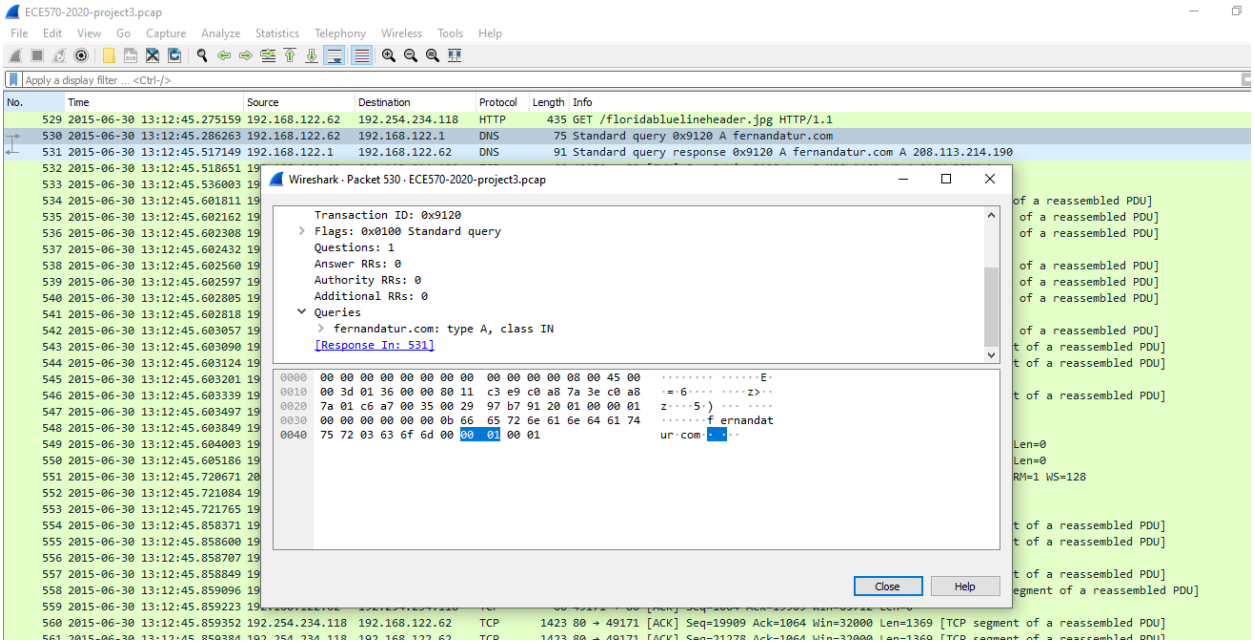
The two other two screen shots for virustotal.com of two timestamps of File transferred are shown in following pictures:
Tow files are clean in virustotal scan.



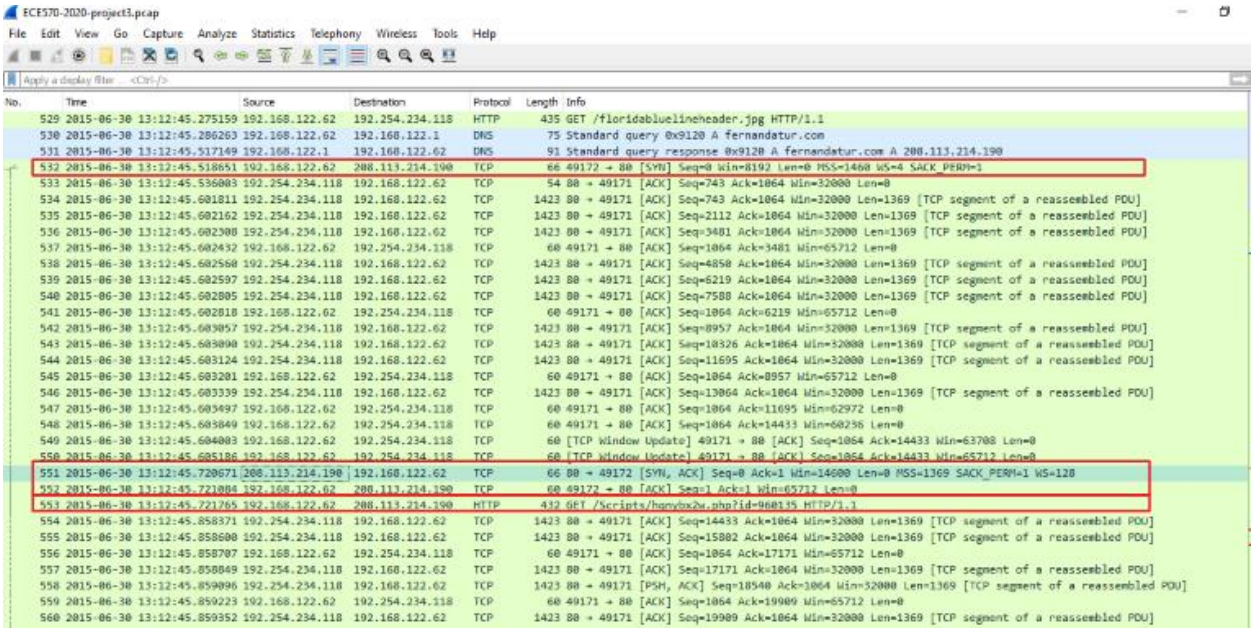
University of Victoria



And also in frame 530, host request to DNS for fernandature.com The website ip address is sent to host by DNS, 208.113.214.190 . The screenshot shows as a follows:



Host sent an SYN to this site from frame 532. In frame 551 ferandature.com sent an SYN.ACK to the host. Host sent back the ACK to this site in frame number 662. The picture as a following show this handshaking:



And also in the above picture that is highlighted by a red pen. The time of frame 553 is 13:12:45.

We found two GET HTTP protocols in packettotal/HTTP . According to packet total report, we checked two files are HTTP on time 13:12:45 on virustotal com

University of Victoria

Malicious Activity | Suspicious Activity | Connections | DNS | HTTP | SSL Certificates | PKI (X.509) | Transferred Files | Strange Activity | Community Tags

Similar Packet Captures

Search in results

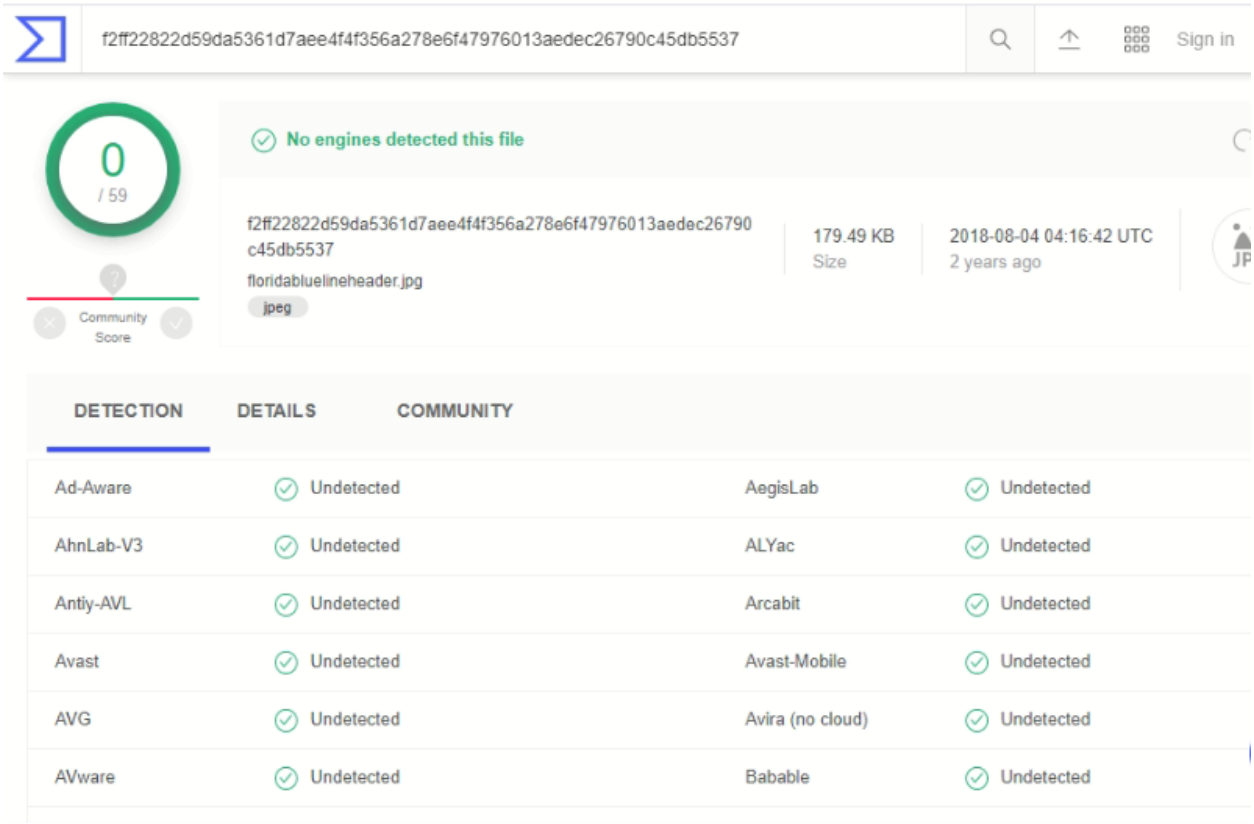
Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transaction Depth	Method	Host
2015-06-30 13:11:51 Z	Cs8Y2Q2yukRvrbFS6	192.168.122.62	49158	216.58.208.46	80	1	GET	google.com
2015-06-30 13:11:51 Z	CMuHRQ3Jfj0FRkK1Qc	192.168.122.62	49159	216.58.218.67	80	1	GET	www.google.co.uk
2015-06-30 13:12:44 Z	CIFU4P2TqMGvSgfc62	192.168.122.62	49170	216.58.218.67	80	1	GET	www.google.co.uk
2015-06-30 13:12:44 Z	CIFU4P2TqMGvSgfc62	192.168.122.62	49170	216.58.218.67	80	2	GET	www.google.co.uk
2015-06-30 13:12:44 Z	CALygR1JnJXOgNnETj	192.168.122.62	49171	192.254.234.118	80	1	GET	www.floridablueline.com
2015-06-30 13:12:45 Z	CALygR1JnJXOgNnETj	192.168.122.62	49171	192.254.234.118	80	2	GET	www.floridablueline.com
2015-06-30 13:12:45 Z	CMvAQV2OwfXQnWdhX2	192.168.122.62	49172	208.113.214.190	80	1	GET	fernandatur.com
2015-06-30 13:12:46 Z	CMHhzK1MVihV1X1U2j	192.168.122.62	49173	208.113.214.190	80	1	GET	www.fernandatur.com
2015-06-30 13:12:47 Z	CocBdE3VP4U7EE8PX5	192.168.122.62	49174	46.30.45.65	80	1	GET	good.recycle2learn.com
2015-06-30 13:12:48 Z	CtGI8I22yrRPVILob	192.168.122.62	49175	46.30.45.65	80	1	GET	good.recycle2learn.com

The first is related to www.floridablueline.com that source IP is Host (192.168.122.62) to the IP address of this site as a destination. We checked this file on virustotal and result is shown as a follows:

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transaction Depth	Method	Host
2015-06-30 13:12:45 Z	CALygR1JnJXOgNnETj	192.168.122.62	49171	192.254.234.118	80	2	GET	www.floridablueline.com

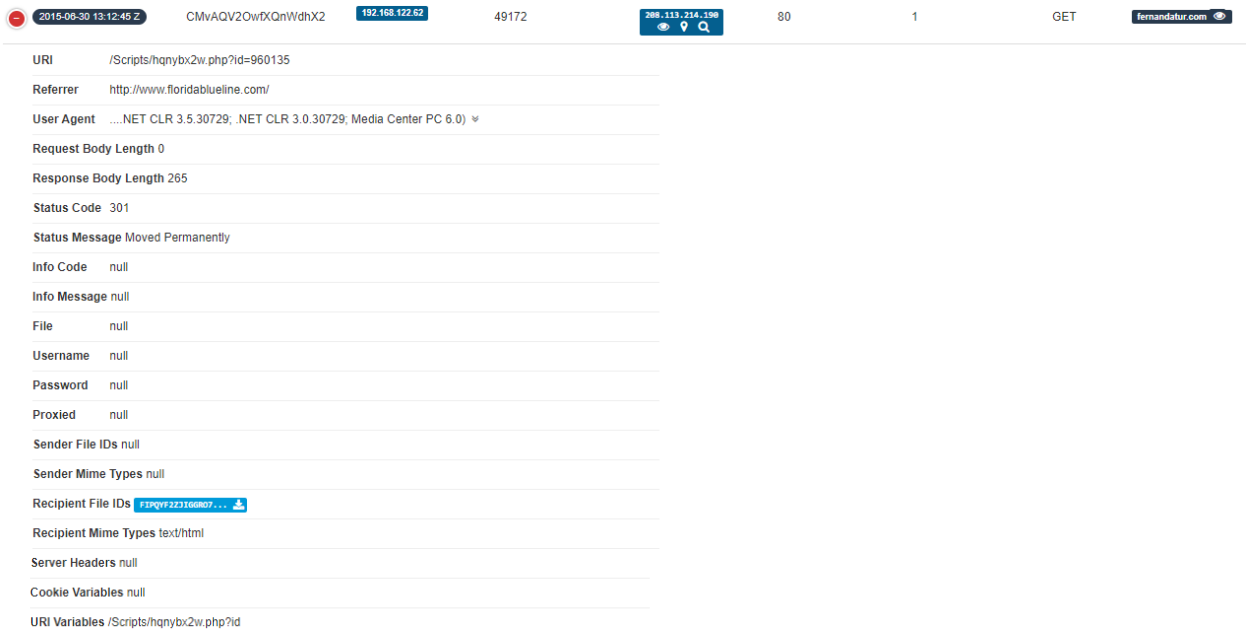
URI /floridablueline header.jpg
Referrer http://www.floridablueline.com/
User Agent ....NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
Request Body Length 0
Response Body Length 183799
Status Code 200
Status Message OK
Info Code null
Info Message null
File null
Username null
Password null
Proxied null
Sender File IDs null
Sender Mime Types null
Recipient File IDs FIC2ID2ENIQ6ZZU...
Recipient Mime Types image/jpeg
Client Headers ACCEPT,REFERER,ACCEPT-LANGUAGE,USER-AGENT,ACCEPT-ENCODING,HOST,CONNECTION
Server Headers null
Cookie Variables null
URI Variables /floridablueline header.jpg

Virustotal scan result is this file that transfer visa HTTP protocol is clean.



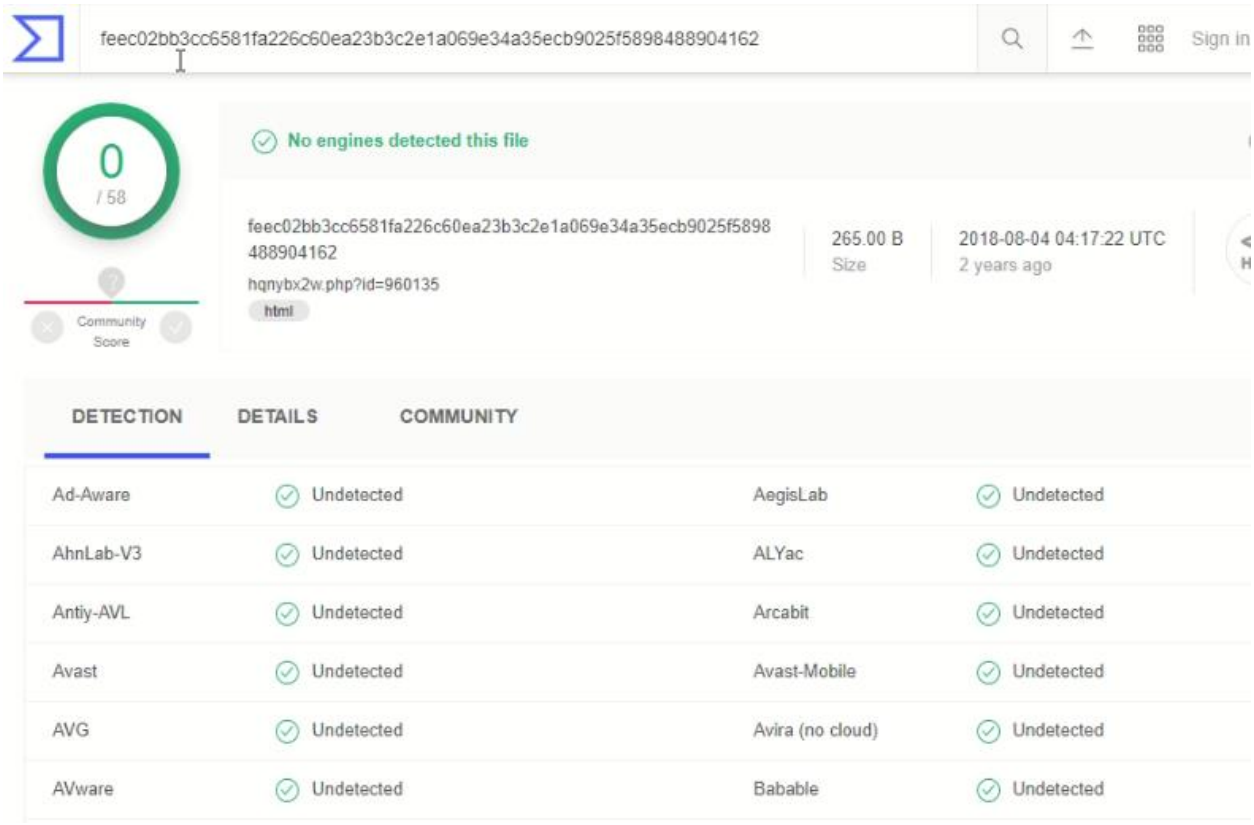
The second is related to fernandature.com that source IP is Host (192.168.122.62) to this site as a destination.We checked this file on virustotal and result is shown as a follows:

University of Victoria

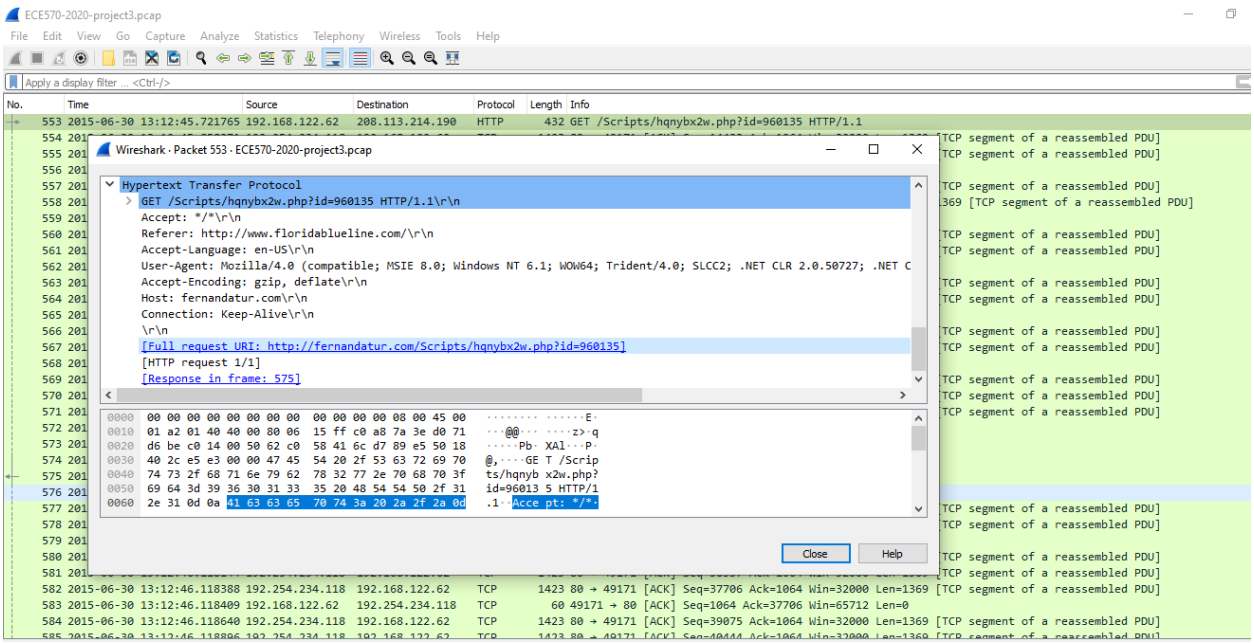


Virustotal scan result is this file that transfer visa HTTP protocol is clean.

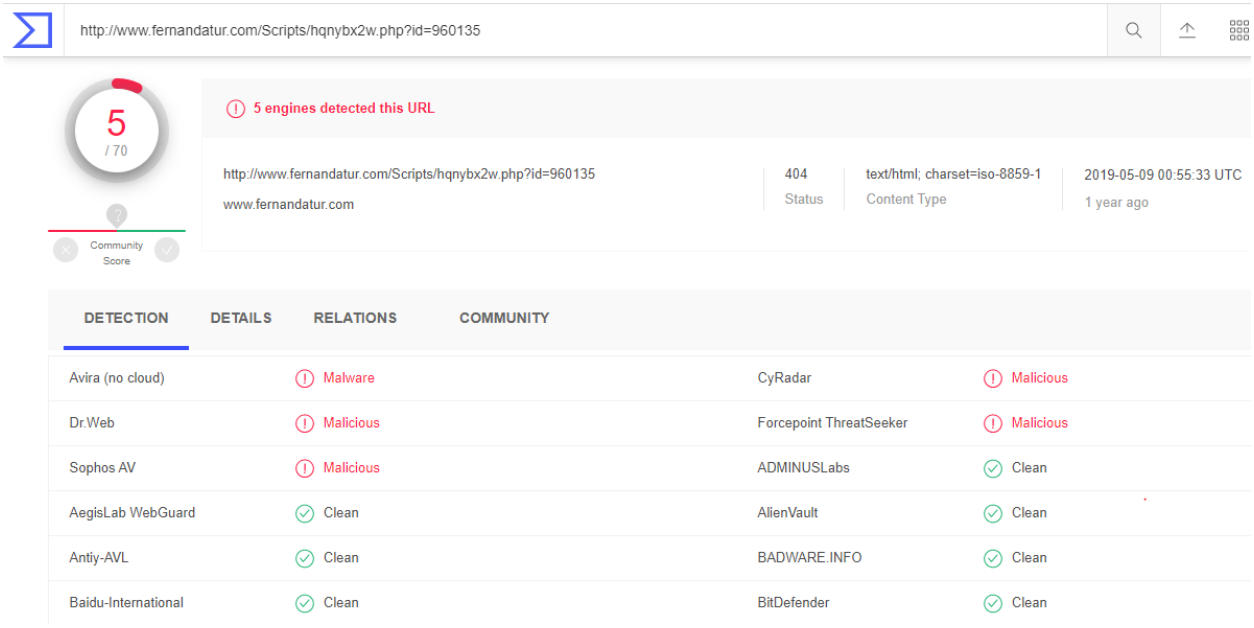
University of Victoria



In wireshark capture data, in frame 553 that we highlighted in above last wireshark screenshot. We found GET scripts via fernandature.com

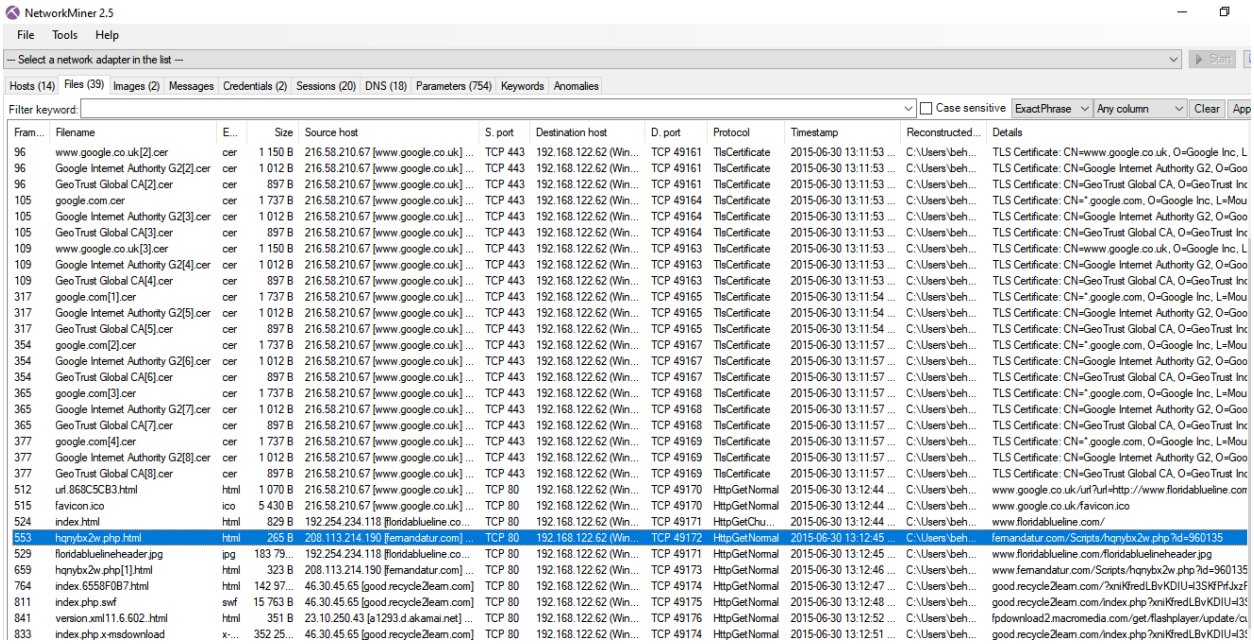


When we checked this URL that shows with blue color on virustotal.com, we found that this URL is malicious and Malware. The screenshots are as following picture:



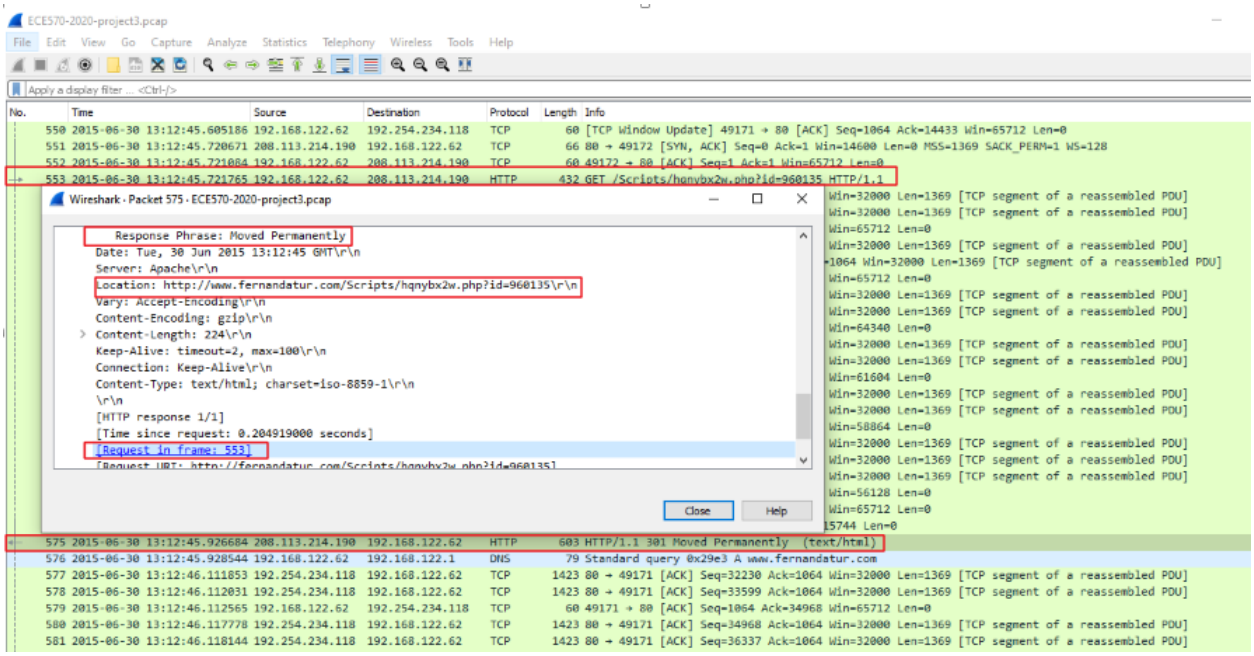
According to Networkminer report, frame 553 is a file that name is hqnybx2w.php.html

University of Victoria



Fram...	Filename	E...	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp	Reconstructed...	Details
96	www.google.co.uk[2].cer	cer	1 150 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49161	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=www.google.co.uk, O=Google Inc, L
96	Google Internet Authority G2[2].cer	cer	1 012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49161	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Goo
96	GeoTrust Global CA[2].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49161	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
105	google.com.cer	cer	1 737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49164	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=*.google.com, O=Google Inc, L=Mou
105	Google Internet Authority G2[3].cer	cer	1 012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49164	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Goo
105	GeoTrust Global CA[3].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49164	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
109	www.google.co.uk[3].cer	cer	1 150 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49163	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=www.google.co.uk, O=Google Inc, L
109	Google Internet Authority G2[4].cer	cer	1 012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49163	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Goo
109	GeoTrust Global CA[4].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49163	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
317	google.com[1].cer	cer	1 737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49165	TlsCertificate	2015-06-30 13:11:54 ...	C:\Users\beh...	TLS Certificate: CN=*.google.com, O=Google Inc, L=Mou
317	Google Internet Authority G2[5].cer	cer	1 012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49165	TlsCertificate	2015-06-30 13:11:54 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Goo
317	GeoTrust Global CA[5].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49165	TlsCertificate	2015-06-30 13:11:54 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
354	google.com[2].cer	cer	1 737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49167	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=*.google.com, O=Google Inc, L=Mou
354	Google Internet Authority G2[6].cer	cer	1 012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49167	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Goo
354	GeoTrust Global CA[6].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49167	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
365	google.com[3].cer	cer	1 737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49168	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=*.google.com, O=Google Inc, L=Mou
365	Google Internet Authority G2[7].cer	cer	1 012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49168	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Goo
365	GeoTrust Global CA[7].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49168	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
377	google.com[4].cer	cer	1 737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49169	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=*.google.com, O=Google Inc, L=Mou
377	Google Internet Authority G2[8].cer	cer	1 012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49169	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Goo
377	GeoTrust Global CA[8].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49169	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
512	url.868C5CB3.html	html	1 070 B	216.58.210.67 [www.google.co.uk] ...	TCP 80	192.168.122.62 (Win...	TCP 49170	HttpGetNormal	2015-06-30 13:12:44 ...	C:\Users\beh...	www.google.co.uk/url?url=http://www.floridablueline.com
515	favicon.ico	ico	5 430 B	216.58.210.67 [www.google.co.uk] ...	TCP 80	192.168.122.62 (Win...	TCP 49170	HttpGetNormal	2015-06-30 13:12:44 ...	C:\Users\beh...	www.google.co.uk/favicon.ico
524	index.html	html	829 B	192.254.234.118 [floridablueline.co...	TCP 80	192.168.122.62 (Win...	TCP 49171	HttpGetChu...	2015-06-30 13:12:44 ...	C:\Users\beh...	www.floridablueline.com/
553	hqnybx2w.php.html	html	265 B	208.113.214.190 [fernandatur.com] ...	TCP 80	192.168.122.62 (Win...	TCP 49172	HttpGetNormal	2015-06-30 13:12:45 ...	C:\Users\beh...	fernandatur.com/Scripts/hqnybx2w.php?id=960135
529	floridablueline header.jpg	jpg	183 79...	192.254.234.118 [floridablueline.co...	TCP 80	192.168.122.62 (Win...	TCP 49171	HttpGetNormal	2015-06-30 13:12:45 ...	C:\Users\beh...	www.floridablueline.com/floridablueline header.jpg
659	hqnybx2w.php[1].html	html	323 B	208.113.214.190 [fernandatur.com] ...	TCP 80	192.168.122.62 (Win...	TCP 49173	HttpGetNormal	2015-06-30 13:12:46 ...	C:\Users\beh...	www.fernandatur.com/Scripts/hqnybx2w.php?id=960135
764	index.6558F0B7.html	html	142 97...	46.30.45.65 [good.recycle2learn.com]	TCP 80	192.168.122.62 (Win...	TCP 49174	HttpGetNormal	2015-06-30 13:12:47 ...	C:\Users\beh...	good.recycle2learn.com/?xniKfredLBvKDIU=I3SKfPrfJxzF
811	index.php.swf	swf	15 763 B	46.30.45.65 [good.recycle2learn.com]	TCP 80	192.168.122.62 (Win...	TCP 49175	HttpGetNormal	2015-06-30 13:12:48 ...	C:\Users\beh...	good.recycle2learn.com/index.php?xniKfredLBvKDIU=I3S
841	version.xml11.6.602..html	html	351 B	23.10.250.43 [a1293.d.akamai.net] ...	TCP 80	192.168.122.62 (Win...	TCP 49176	HttpGetNormal	2015-06-30 13:12:52 ...	C:\Users\beh...	fpdownload2.macromedia.com/get/flashplayer/update/cu
833	index.php.x-msdownload	x-...	352 25...	46.30.45.65 [good.recycle2learn.com]	TCP 80	192.168.122.62 (Win...	TCP 49174	HttpGetNormal	2015-06-30 13:12:51 ...	C:\Users\beh...	good.recycle2learn.com/index.php?xniKfredLBvKDIU=I3S

In frame 575, in wireshark capture, we found that fernandature.com with IP address 208.113.214.190 sent HTTP1.1 moved permanently to the host machine(192.168.122.62) . Moreover, this frame is the response frame of 553. The wireshark screenshot is shown as a following picture:



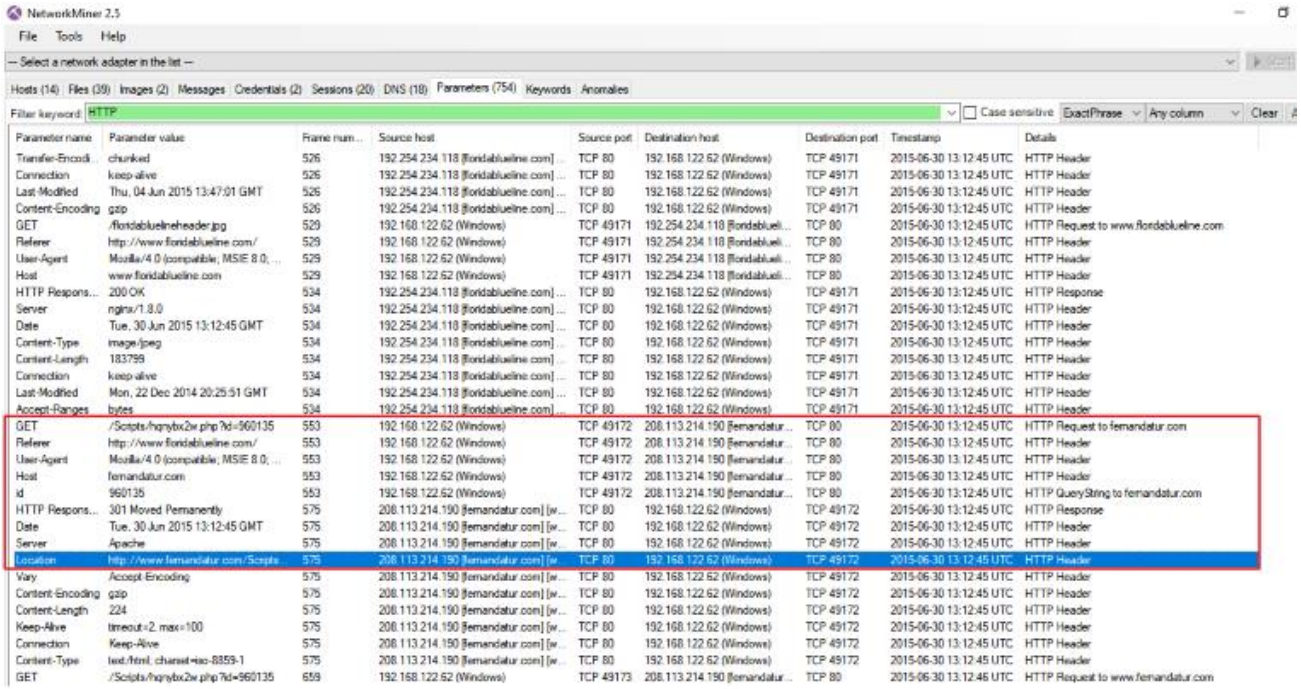
Here, we found that A TCP handshake does not contain any redirect information. So TCP handshaking is fine. However, we check the application layer, we found that:
< HTTP/1.1 301 Moved Permanently …

< Location: http://www.fernandatur.com/Scripts/hqnybx2w.php?id=960135

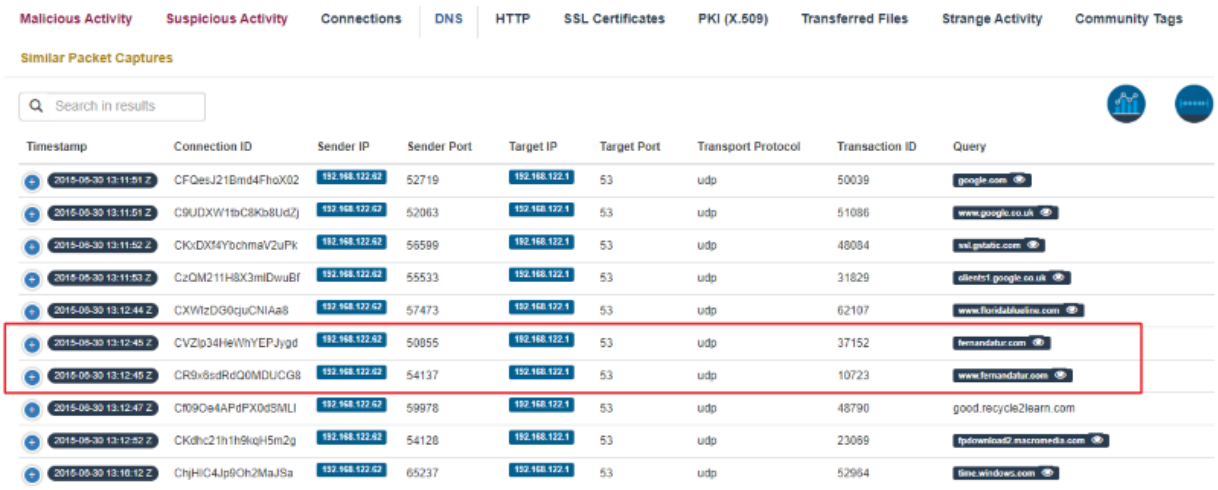
Since this is a 301 **permanent** redirect the client does not even need to visit the original site again but will instead use the new location on repeated tries. Only on the first try it will visit the original site to receive the redirect.

In Networkminer is again this redirection shows:

University of Victoria

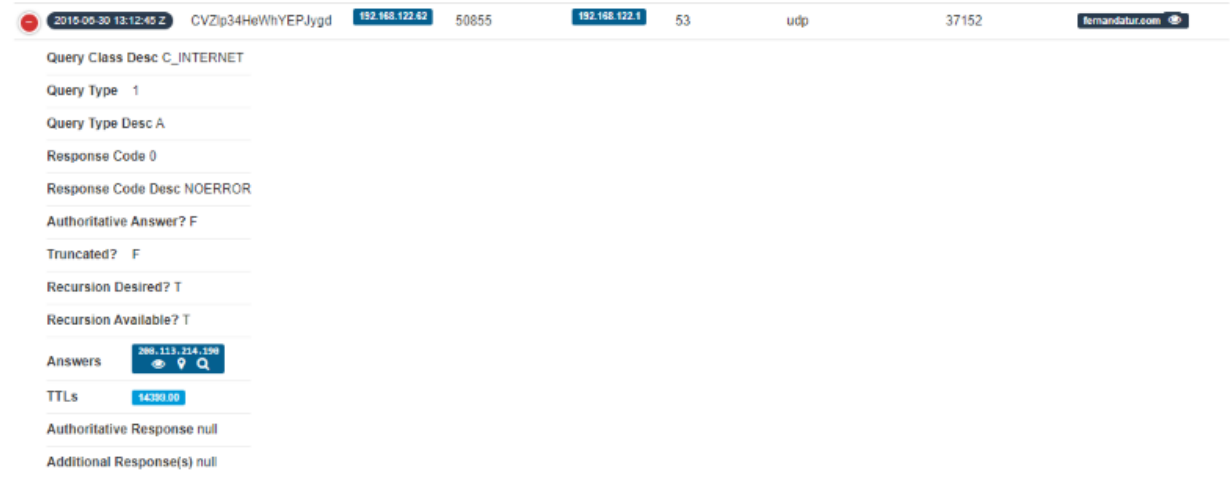


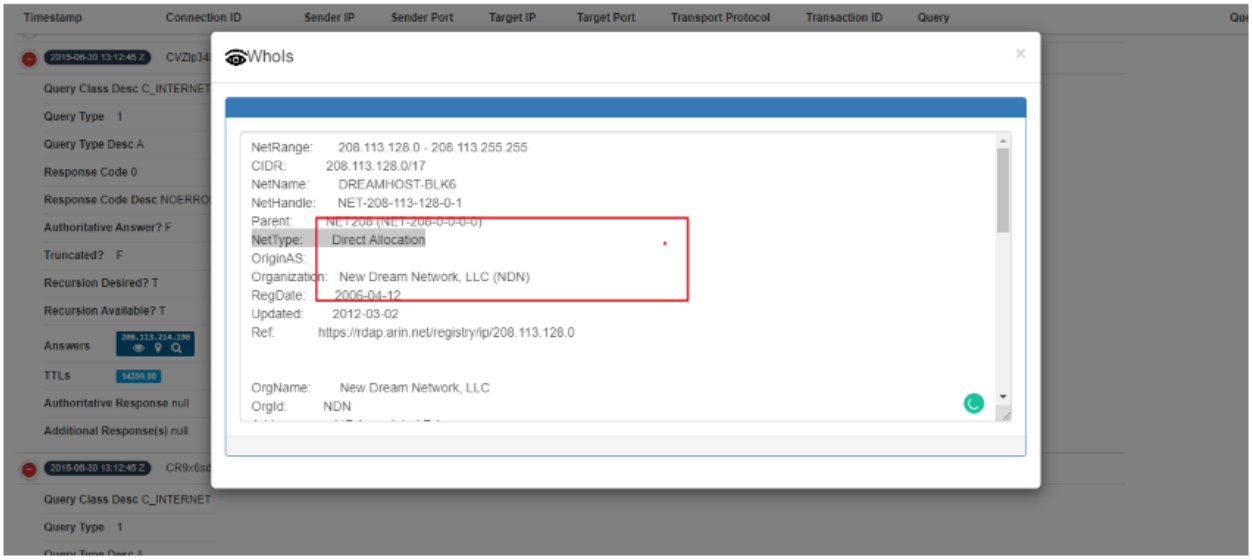
Finally, as a report of packettotal in DNS Tab we can see that this site is redirected.

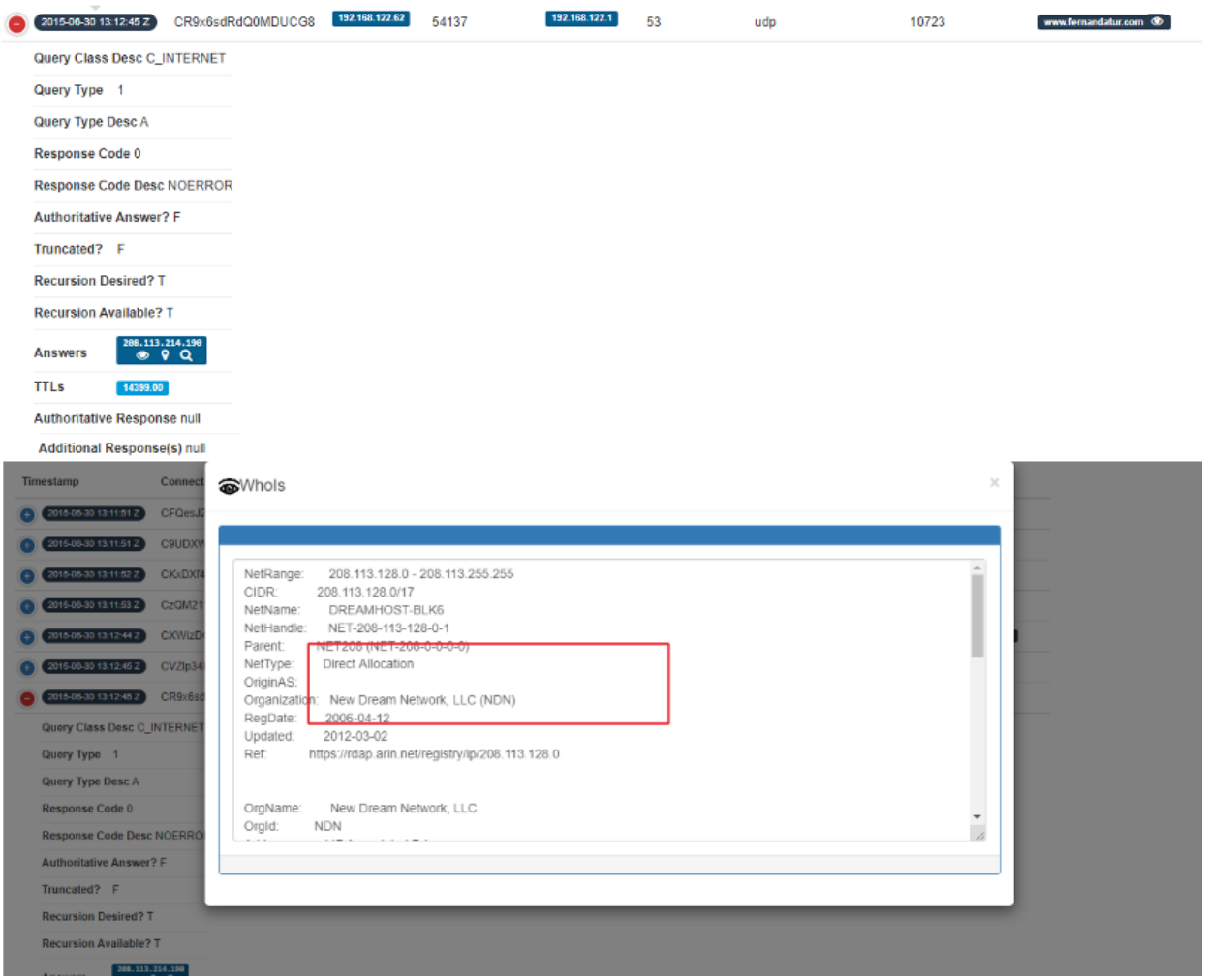


When we click on whoIs Lookup we can see that those sites (fernandatur.com and www.fernandatur.com) are Direct Allocation.All screenshots are shown as a following pictures:

University of Victoria

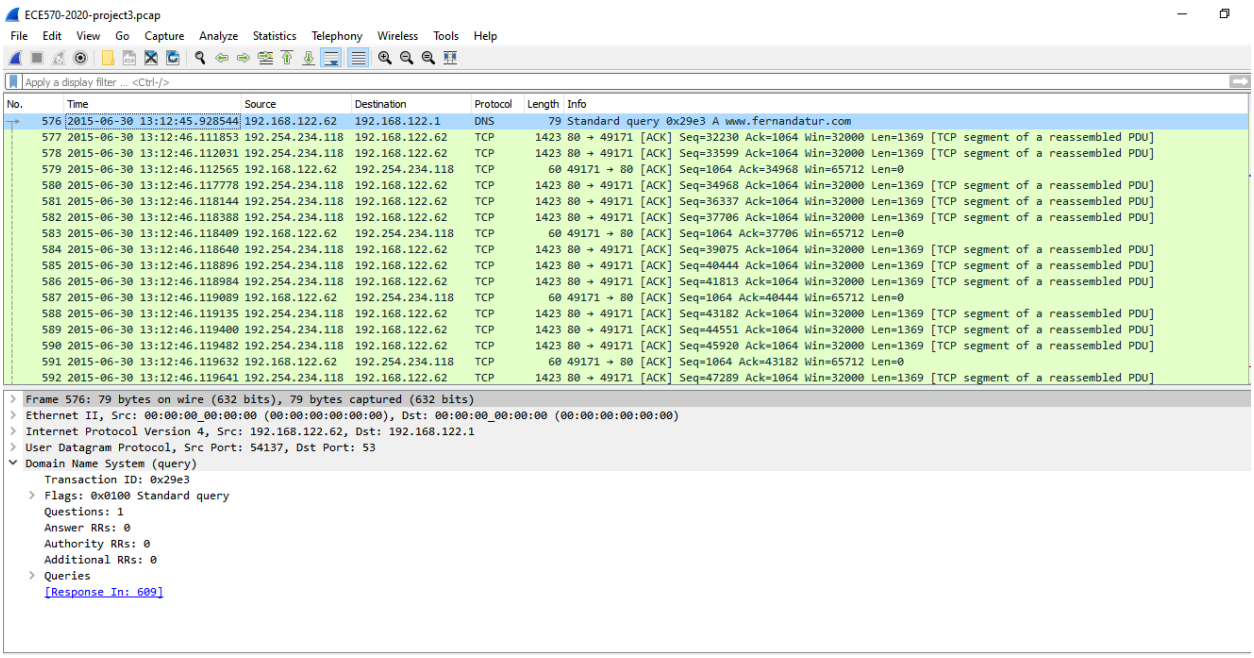






Note: We have a lot of TCP ACK between floridablueline.com and host from frame 533 after host open fernandature.com

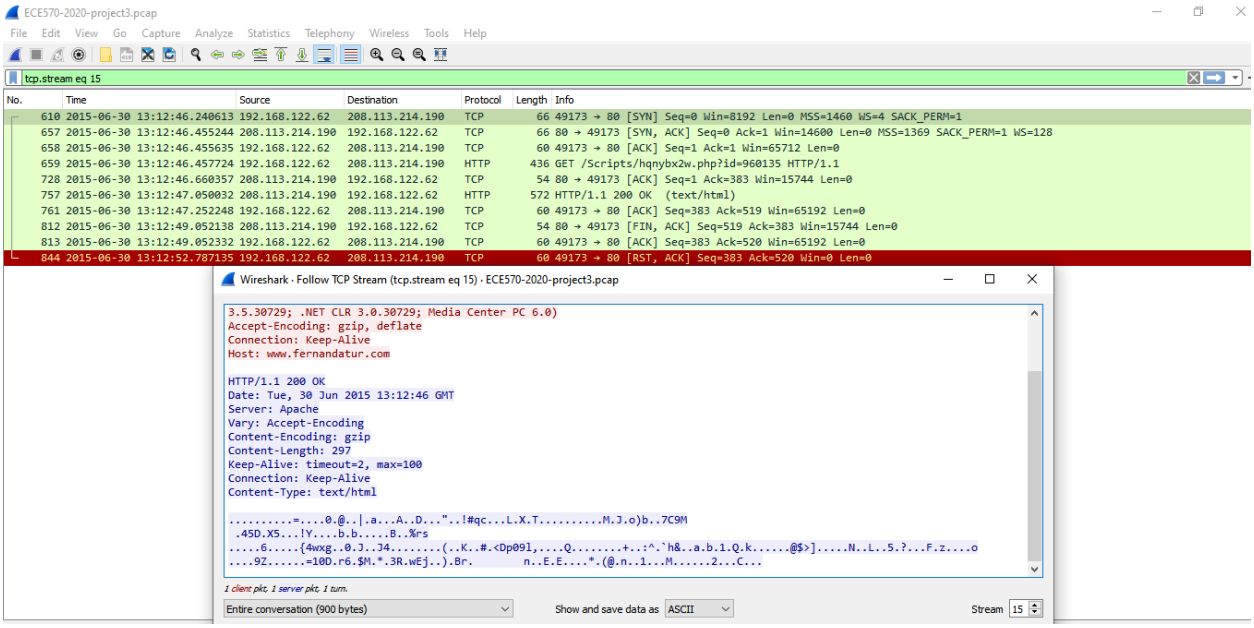
At the end of seconds of 13:12:45, in frame 576 the host sent a request to DNS for open www.fernandature.com. In frame 609, DNS responded to the host and sent the IP address of this site. The IP address is 208.113.214.190.



In frame 610 host request to start TCP handshaking to IP address is 208.113.214.190. In frame 610 send SYN, IP address 208.113.214.190 response SYN,ACK on frame 657. And immediately on frame 658 the host sent ACK to this IP address that is the website: www.fernandature.com.

In frame 659, the host machine sent one HTTP request to 208.113.214.190. This request was sent via HTTP protocol at 13:12:46. The wireshark screenshot is as follows:

University of Victoria



The host machine was infected by a file transferred on frame 526 from floridablueline.com and after that the host led to infection of other sites.

During that time again floridablueline.com sent an ACK to the host and after some ACK from this site the host sent a response.

According to packet total information, in HTTP Tab we found one data related to 13:12:46. After, download that file and check on virustotal. We found that this script is trojan. Infact, this script is the same as the script of frame 553. This file transferred to host in frame 526 from flordblueline.com .

University of Victoria

Malicious Activity | Suspicious Activity | Connections | DNS | HTTP | SSL Certificates | PKI (X.509) | Transferred Files | Strange Activity | Community Tags

Similar Packet Captures

Search in results

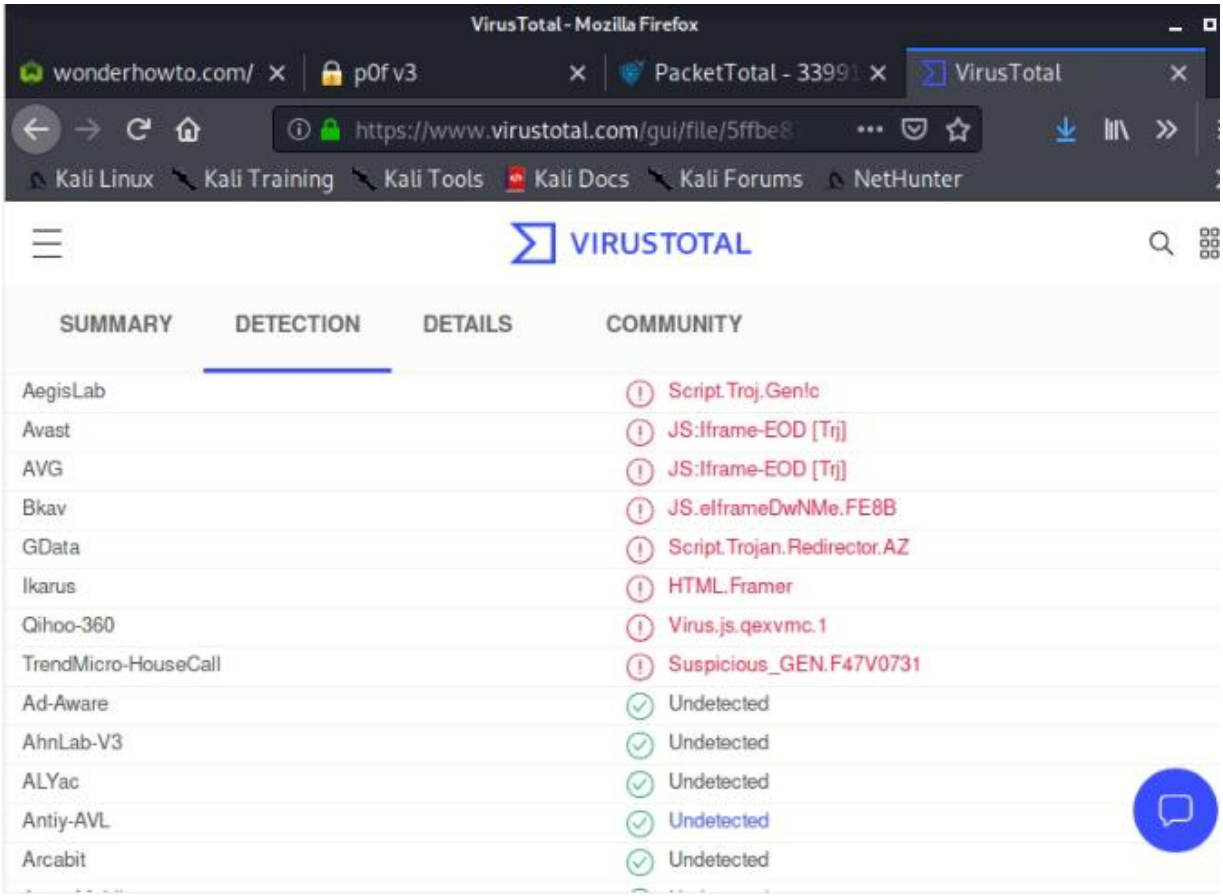
Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transaction Depth	Method	Host
2015-06-30 13:11:51 Z	Cs8Y2Q2yukRvrbFS6	192.168.122.62	49158	216.58.208.46	80	1	GET	google.com
2015-06-30 13:11:51 Z	CMuHRQ3Jfj0FRkK1Qc	192.168.122.62	49159	216.58.210.67	80	1	GET	www.google.co.uk
2015-06-30 13:12:44 Z	CIFU4P2TqMGvSgfc62	192.168.122.62	49170	216.58.210.67	80	1	GET	www.google.co.uk
2015-06-30 13:12:44 Z	CIFU4P2TqMGvSgfc62	192.168.122.62	49170	216.58.210.67	80	2	GET	www.google.co.uk
2015-06-30 13:12:44 Z	CALygR1JnJXOgNnETj	192.168.122.62	49171	192.254.234.118	80	1	GET	www.floridablueline.com
2015-06-30 13:12:45 Z	CALygR1JnJXOgNnETj	192.168.122.62	49171	192.254.234.118	80	2	GET	www.floridablueline.com
2015-06-30 13:12:45 Z	CMvAQV2OwfXQnWdhX2	192.168.122.62	49172	208.113.214.190	80	1	GET	fernandatur.com
2015-06-30 13:12:46 Z	CMHhzK1MVihV1X1U2j	192.168.122.62	49173	208.113.214.190	80	1	GET	www.fernandatur.com
2015-06-30 13:12:47 Z	CocBdE3VP4U7EE8PX5	192.168.122.62	49174	46.30.45.65	80	1	GET	good.recycle2learn.com
2015-06-30 13:12:48 Z	CtGI8l22yrRPVILob	192.168.122.62	49175	46.30.45.65	80	1	GET	good.recycle2learn.com

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transaction Depth	Method	Host
2015-06-30 13:12:46 Z	CMHhzK1MVihV1X1U2j	192.168.122.62	49173	208.113.214.190	80	1	GET	www.fernandatur.com

URI /Scripts/hqnybx2w.php?id=960135
Referrer http://www.floridablueline.com/
User Agent ....NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
Request Body Length 0
Response Body Length 323
Status Code 200
Status Message OK
Info Code null
Info Message null
File null
Username null
Password null
Proxied null
Sender File IDs null
Sender Mime Types null
Recipient File IDs F43AYX1VSTBLTTS...
Recipient Mime Types application/javascript

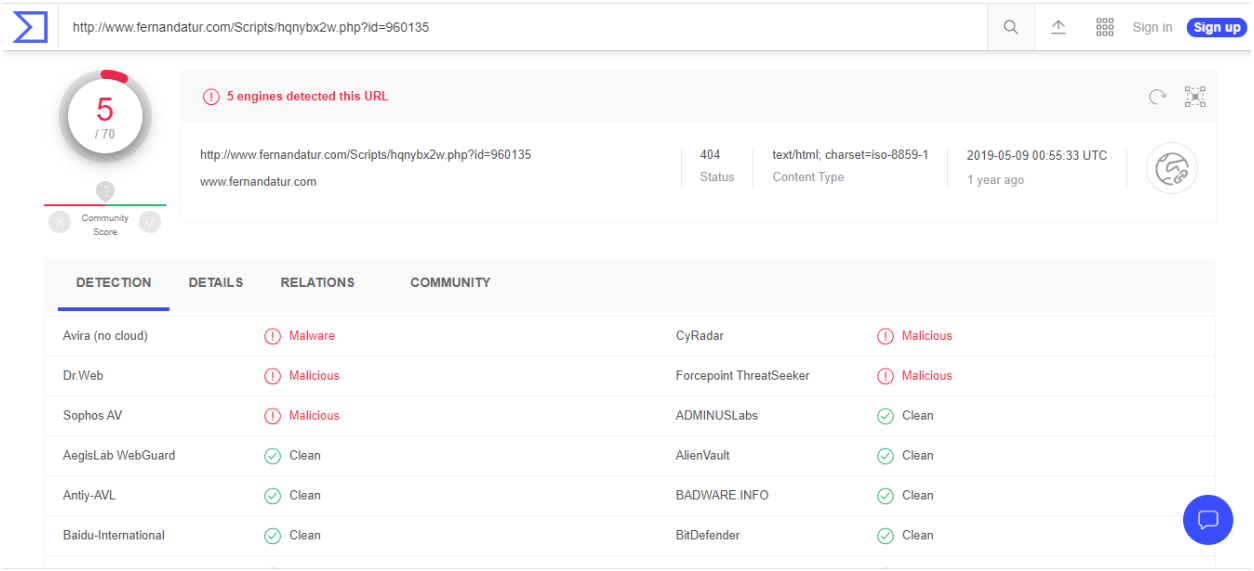
Client Headers ACCEPT,REFERER,ACCEPT-LANGUAGE,USER-AGENT,ACCEPT-ENCODING,CONNECTION,HOST
Server Headers null
Cookie Variables null
URI Variables /Scripts/hqnybx2w.php?id

University of Victoria

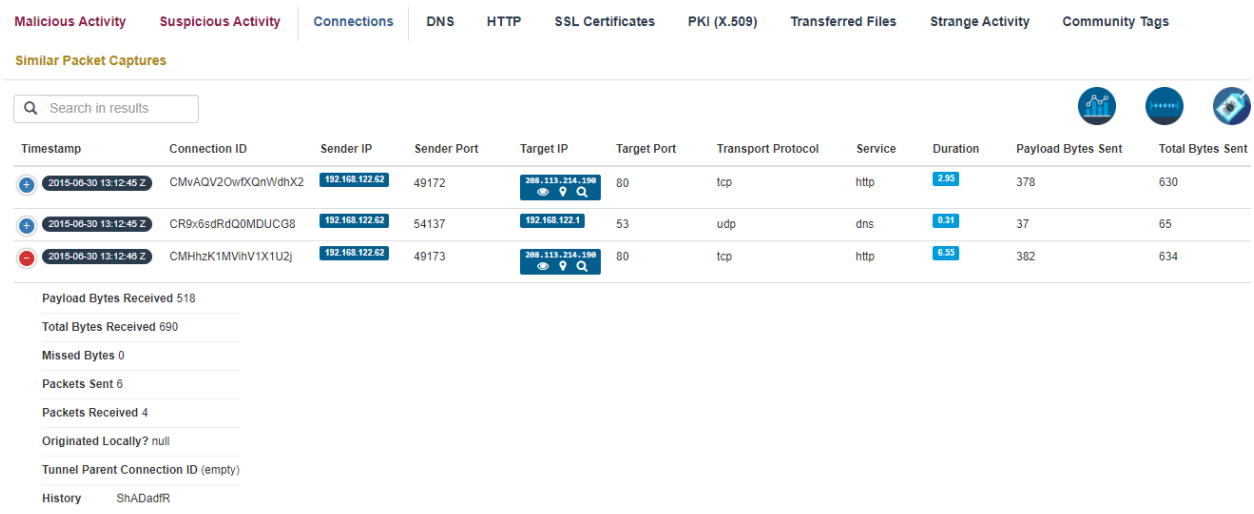


Again the URL of this site is in virus total indicates trojan. Same as frame 553.

University of Victoria

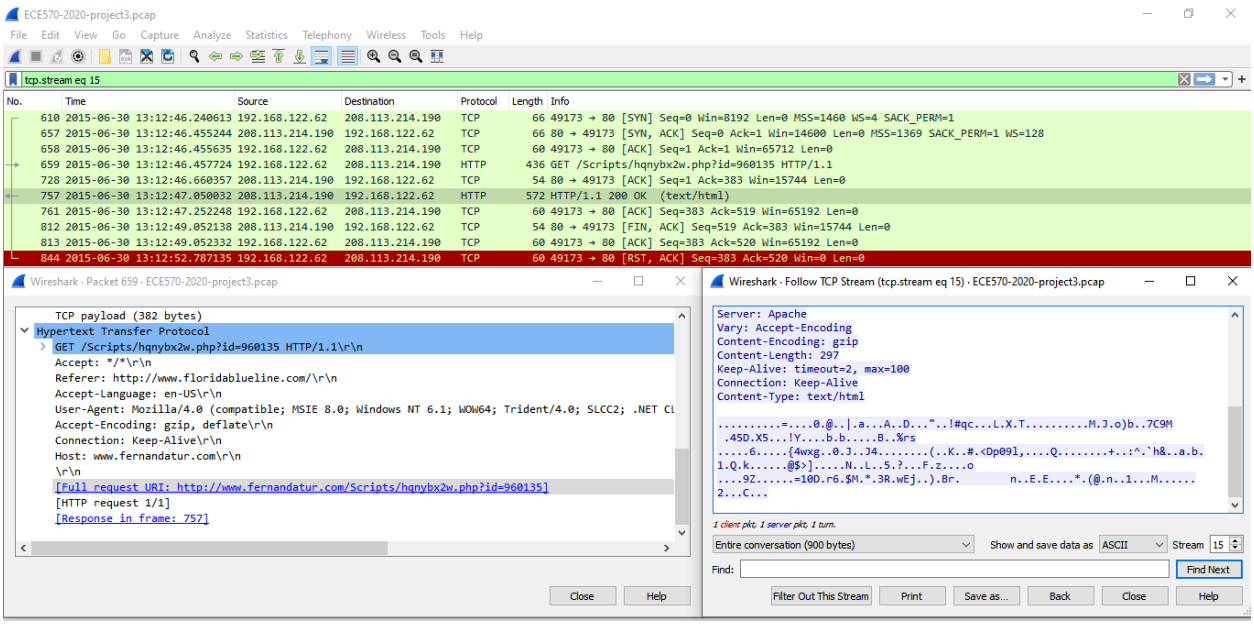


In the connection Tab of the packet total we found that in time 13:12:46 the connection duration between host and 208.113.214.190 is 6:55 seconds.



After HTTP request of host to 208.113.214.190 in frame 659 to GET malicious scripts. In frame 757, the target with 208.113.214.190 as an IP address sent HTTP 1.1 200 OK

to the host. The host IP address is 192.168.122.62. The wireshark screenshot and TCP stream is as a follows:

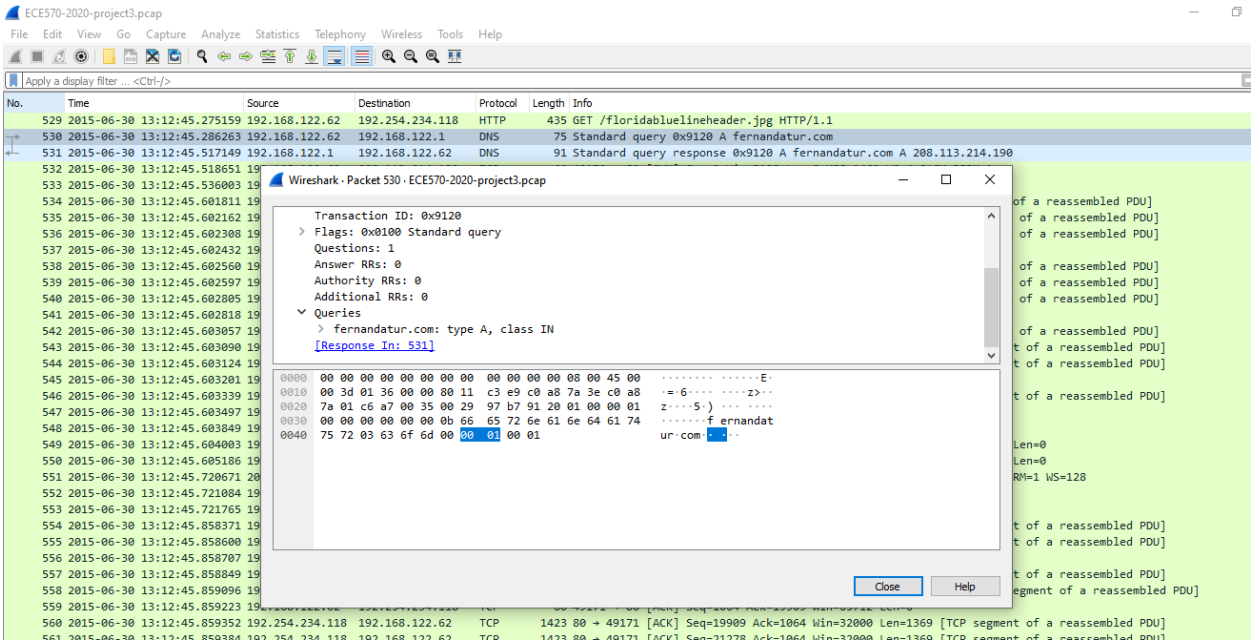


Note: The **HTTP 200** OK success **status response code** indicates that the request has succeeded.

University of Victoria

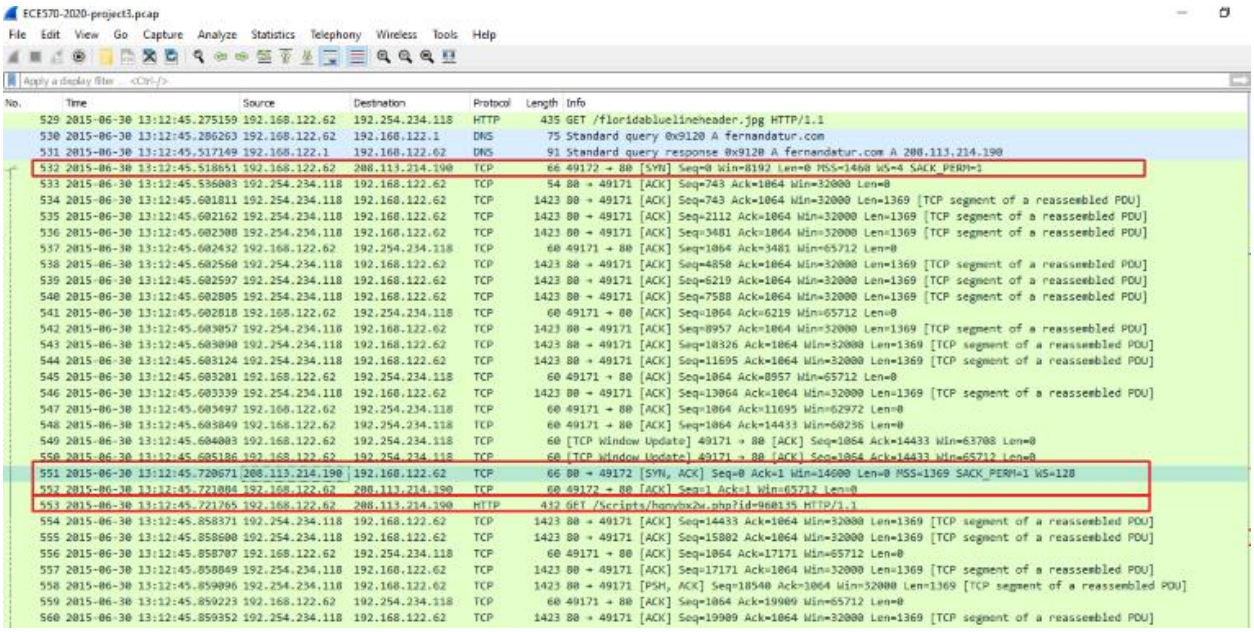
3. What is the IP address and domain name that delivered the malware?

This scenario that host machine infected some websites or IP address is start from frame 530 that host request to access to site fernandature.com
So,
in frame 530, host request to DNS for fernandature.com The website ip address is sent to host by DNS, 208.113.214.190 . The screenshot shows as a follows:



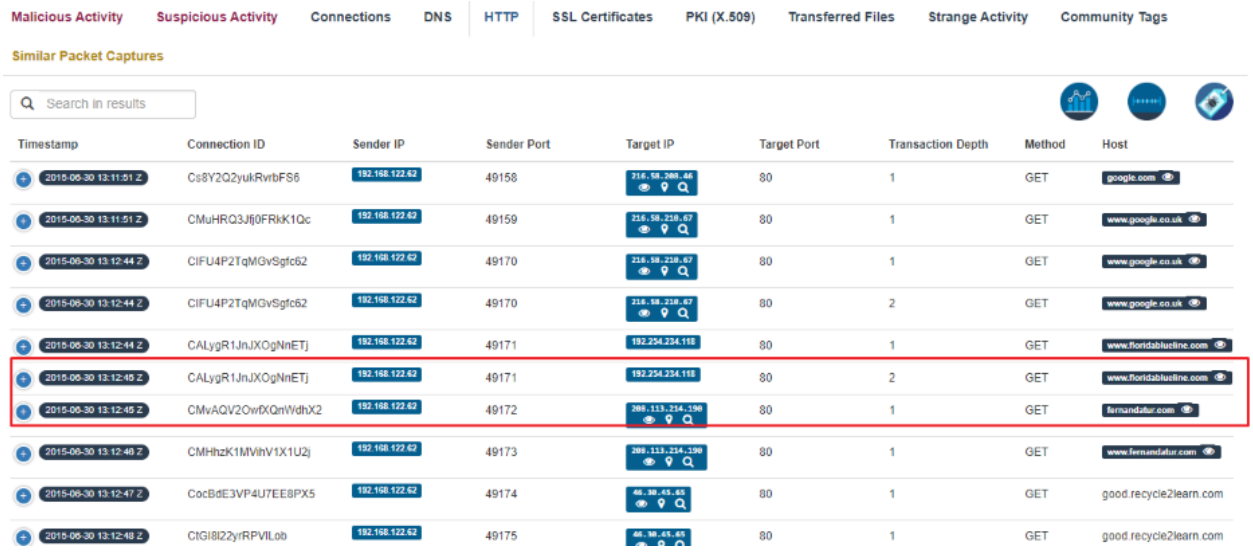
Host sent an SYN to this site from frame 532. In frame 551 ferandature.com sent an SYN.ACK to the host. Host sent back the ACK to this site in frame number 662. The picture as a following show this handshaking:

University of Victoria

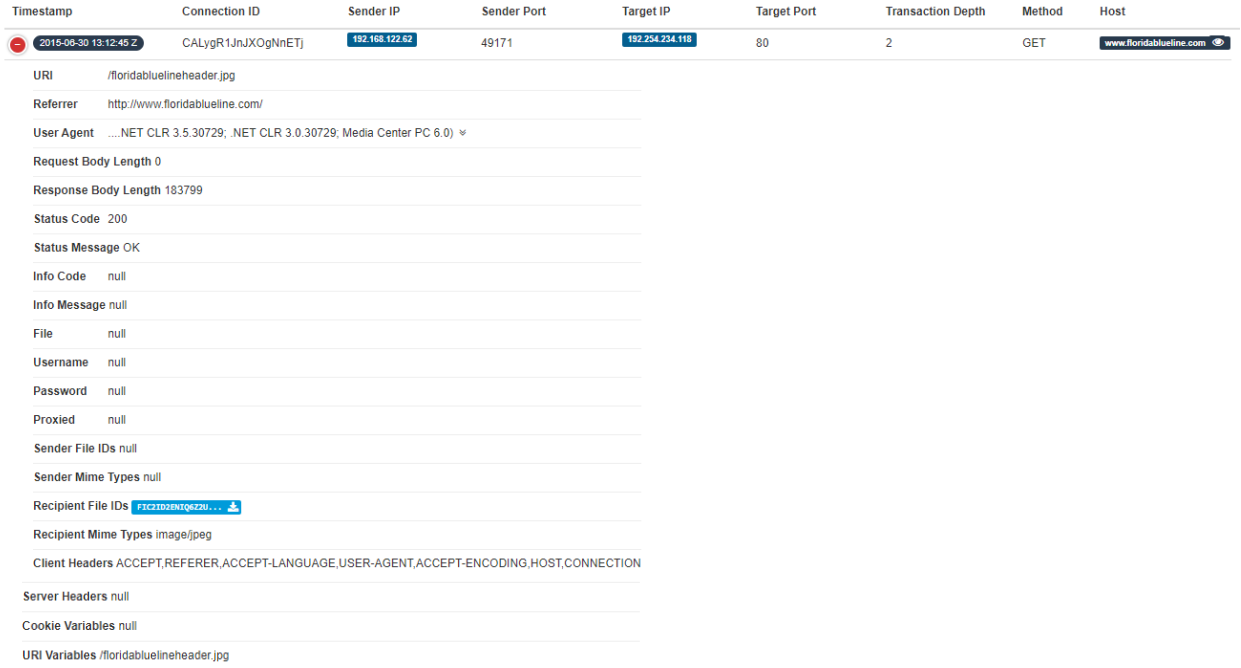


And also in the above picture that is highlighted by a red pen. The time of frame 553 is 13:12:45.

We found two GET HTTP protocols in packettotal/HTTP . According to packet total report, we checked two files are HTTP on time 13:12:45 on virustotal com



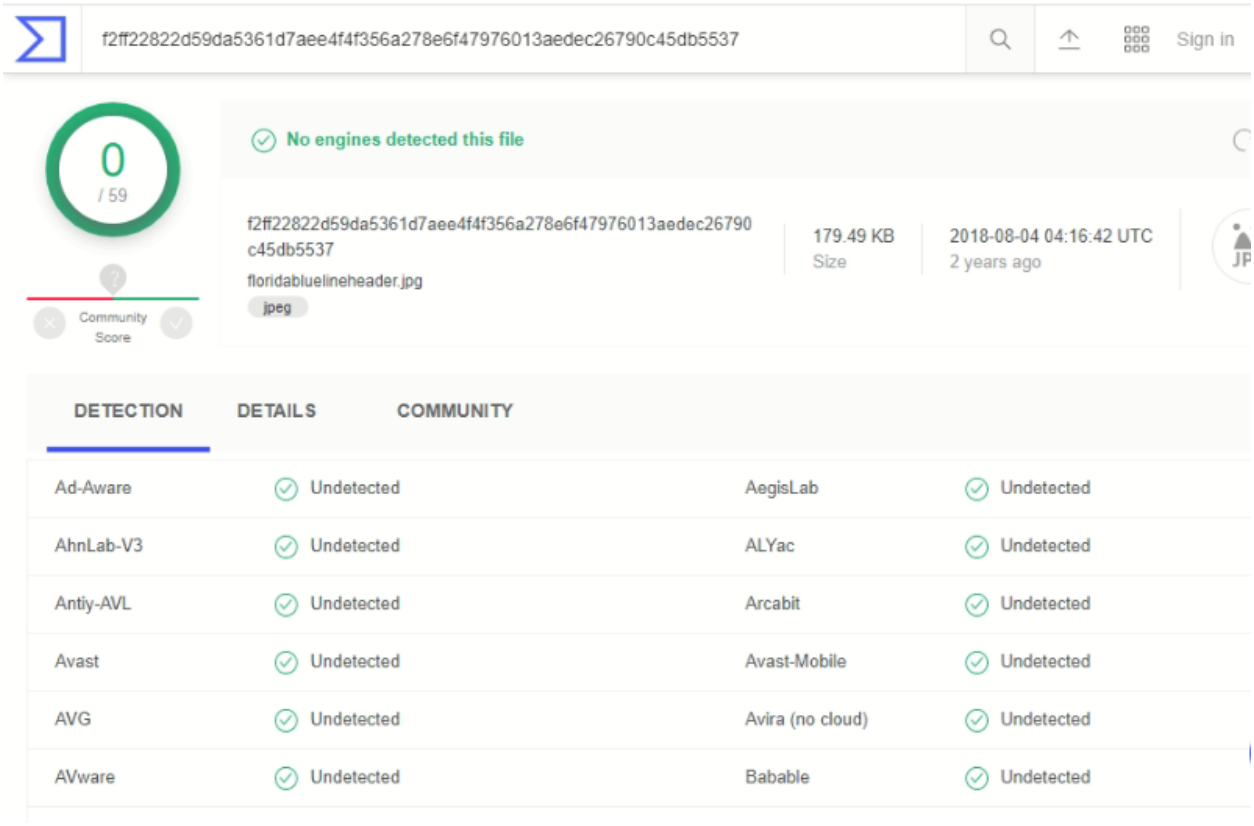
The first is related to www.floridablueline.com that source IP is Host (192.168.122.62) to the IP address of this site as a destination. We checked this file on virustotal and result is shown as a follows:



Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transaction Depth	Method	Host
2015-06-30 13:12:45.2	CALygR1JnJXOgNnETj	192.168.122.62	49171	192.254.234.118	80	2	GET	www.floridablueline.com

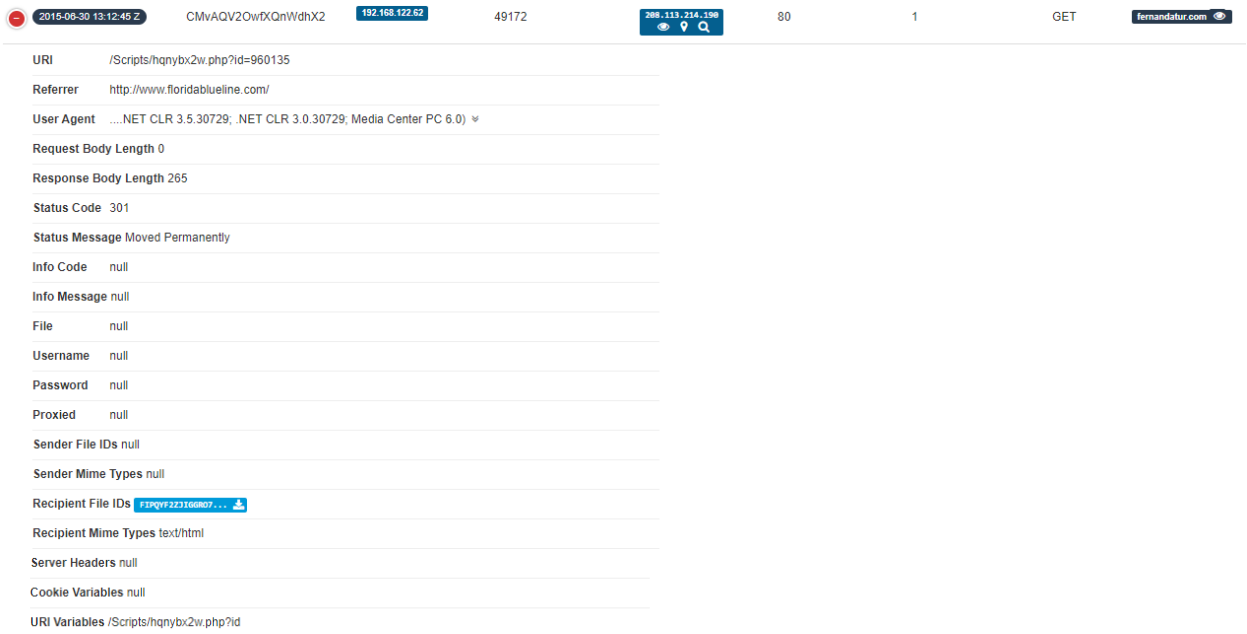
URI /floridablueline header.jpg
Referrer http://www.floridablueline.com/
User Agent ....NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
Request Body Length 0
Response Body Length 183799
Status Code 200
Status Message OK
Info Code null
Info Message null
File null
Username null
Password null
Proxied null
Sender File IDs null
Sender Mime Types null
Recipient File IDs F1C2TD2ENTQ6Z2U...
Recipient Mime Types image/jpeg
Client Headers ACCEPT,REFERER,ACCEPT-LANGUAGE,USER-AGENT,ACCEPT-ENCODING,HOST,CONNECTION
Server Headers null
Cookie Variables null
URI Variables /floridablueline header.jpg

Virustotal scan result is this file that transfer visa HTTP protocol is clean.



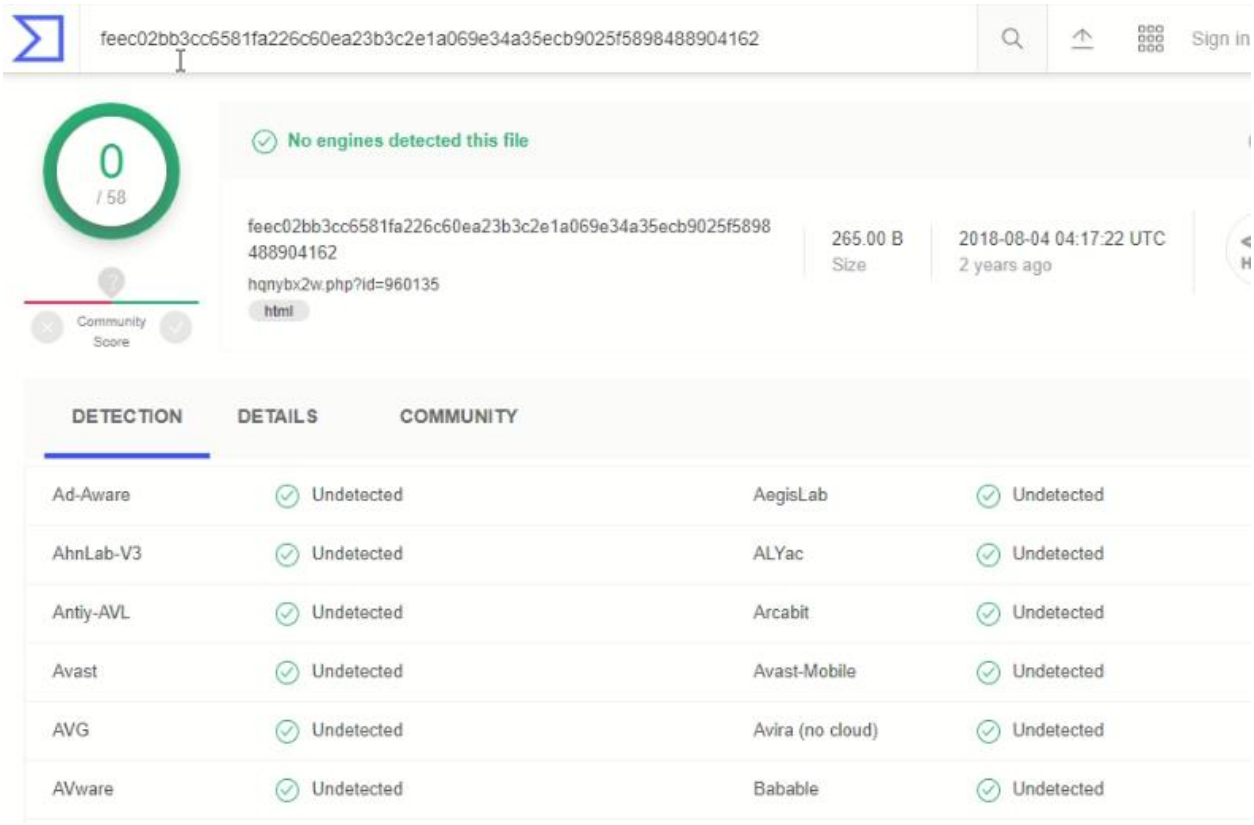
The second is related to fernandature.com that source IP is Host (192.168.122.62) to this site as a destination.We checked this file on virustotal and result is shown as a follows:

University of Victoria

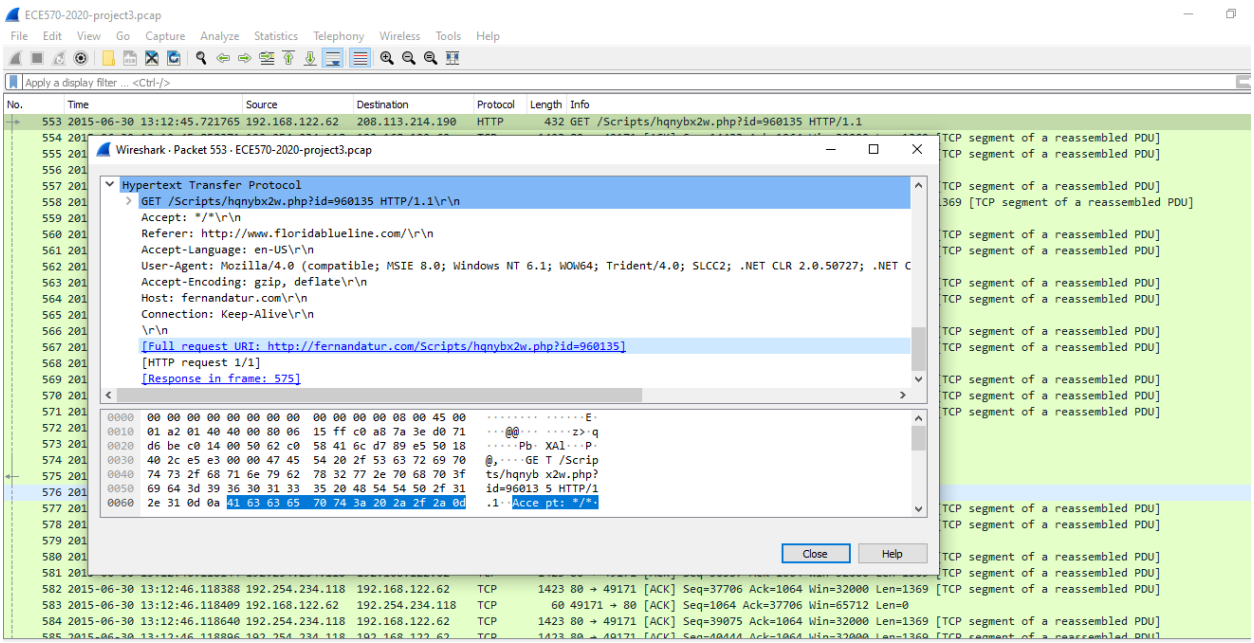


Virustotal scan result is this file that transfer visa HTTP protocol is clean.

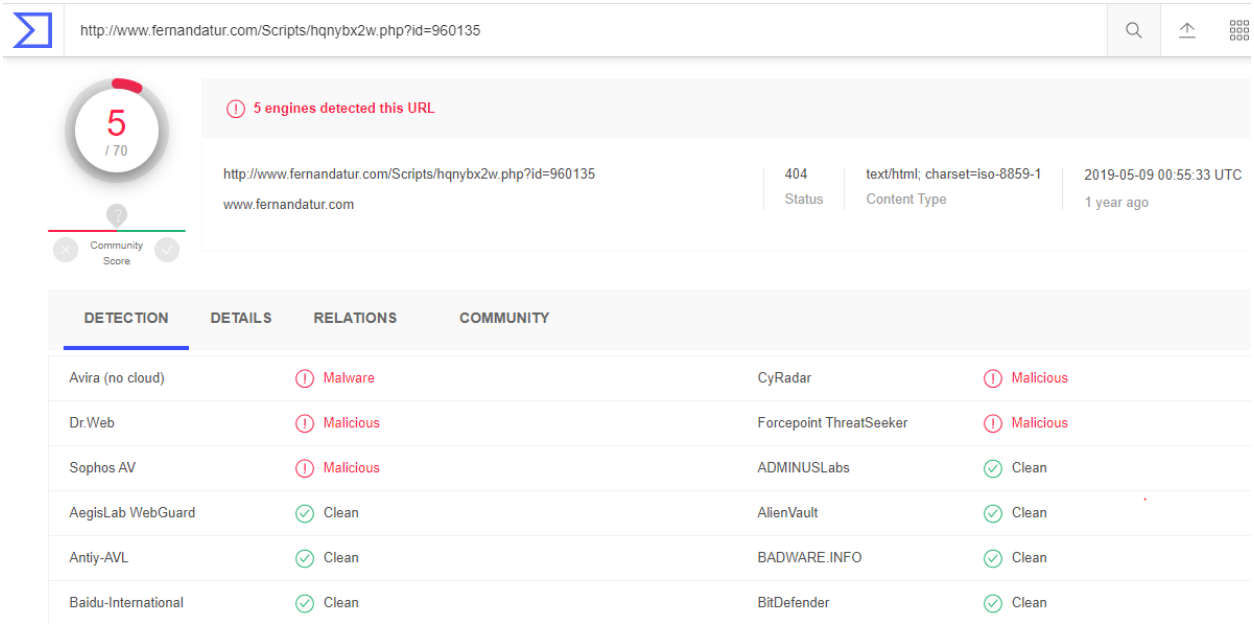
University of Victoria



In wireshark capture data, in frame 553 that we highlighted in above last wireshark screenshot. We found GET scripts via fernandature.com

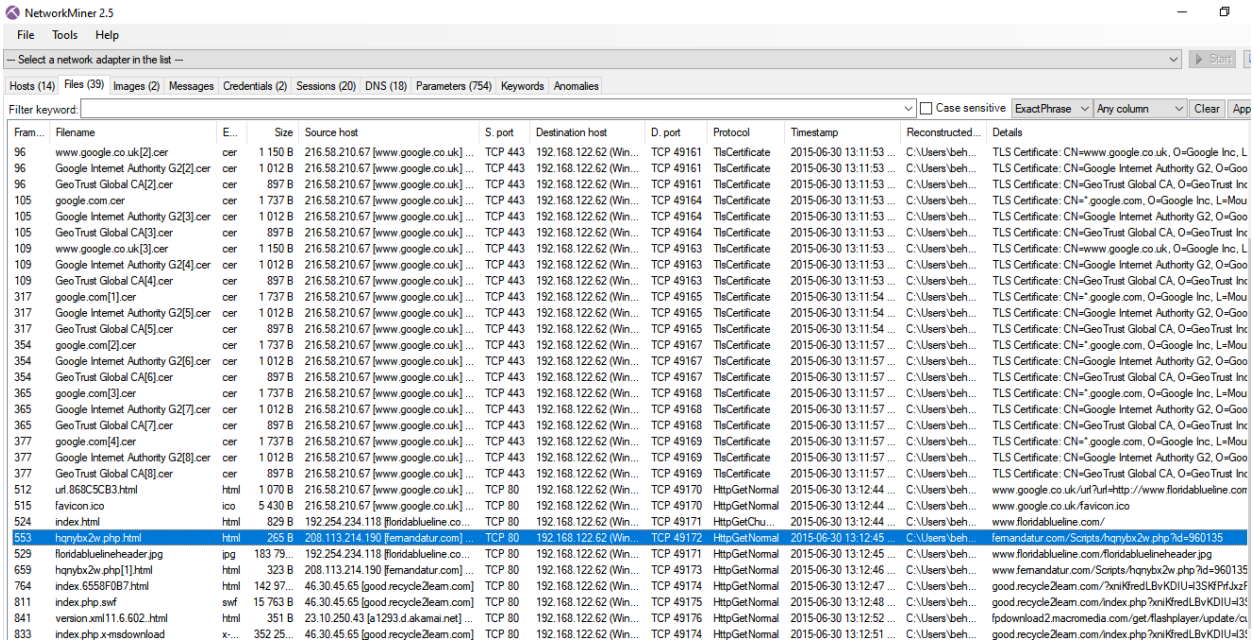


When we checked this URL that shows with blue color on virustotal.com, we found that this URL is malicious and Malware. The screenshots are as following picture:



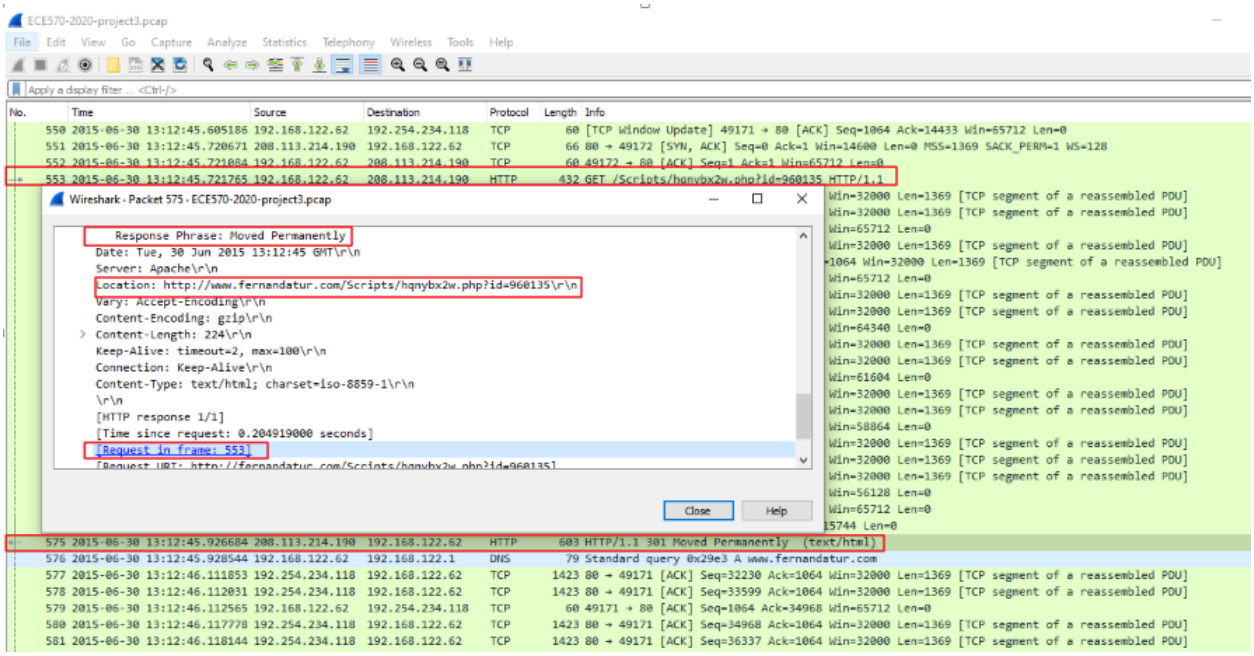
According to Networkminer report, frame 553 is a file that name is hqnybx2w.php.html

University of Victoria



Fram...	Filename	E...	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp	Reconstructed...	Details
96	www.google.co.uk[2].cer	cer	1 150 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49161	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=www.google.co.uk, O=Google Inc, L
96	Google Internet Authority G2[2].cer	cer	1 012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49161	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Goo
96	GeoTrust Global CA[2].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49161	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
105	google.com.cer	cer	1 737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49164	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=*.google.com, O=Google Inc, L=Mou
105	Google Internet Authority G2[3].cer	cer	1 012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49164	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Goo
105	GeoTrust Global CA[3].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49164	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
109	www.google.co.uk[3].cer	cer	1 150 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49163	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=www.google.co.uk, O=Google Inc, L
109	Google Internet Authority G2[4].cer	cer	1 012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49163	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Goo
109	GeoTrust Global CA[4].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49163	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
317	google.com[1].cer	cer	1 737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49165	TlsCertificate	2015-06-30 13:11:54 ...	C:\Users\beh...	TLS Certificate: CN=*.google.com, O=Google Inc, L=Mou
317	Google Internet Authority G2[5].cer	cer	1 012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49165	TlsCertificate	2015-06-30 13:11:54 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Goo
317	GeoTrust Global CA[5].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49165	TlsCertificate	2015-06-30 13:11:54 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
354	google.com[2].cer	cer	1 737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49167	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=*.google.com, O=Google Inc, L=Mou
354	Google Internet Authority G2[6].cer	cer	1 012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49167	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Goo
354	GeoTrust Global CA[6].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49167	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
365	google.com[3].cer	cer	1 737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49168	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=*.google.com, O=Google Inc, L=Mou
365	Google Internet Authority G2[7].cer	cer	1 012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49168	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Goo
365	GeoTrust Global CA[7].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49168	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
377	google.com[4].cer	cer	1 737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49169	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=*.google.com, O=Google Inc, L=Mou
377	Google Internet Authority G2[8].cer	cer	1 012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49169	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Goo
377	GeoTrust Global CA[8].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...	TCP 49169	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
512	url.868C5CB3.html	html	1 070 B	216.58.210.67 [www.google.co.uk] ...	TCP 80	192.168.122.62 (Win...	TCP 49170	HttpGetNormal	2015-06-30 13:12:44 ...	C:\Users\beh...	www.google.co.uk/url?url=http://www.floridablueline.com
515	favicon.ico	ico	5 430 B	216.58.210.67 [www.google.co.uk] ...	TCP 80	192.168.122.62 (Win...	TCP 49170	HttpGetNormal	2015-06-30 13:12:44 ...	C:\Users\beh...	www.google.co.uk/favicon.ico
524	index.html	html	829 B	192.254.234.118 [floridablueline.co...	TCP 80	192.168.122.62 (Win...	TCP 49171	HttpGetChu...	2015-06-30 13:12:44 ...	C:\Users\beh...	www.floridablueline.com/
553	hqnybx2w.php.html	html	265 B	208.113.214.190 [fernandatur.com] ...	TCP 80	192.168.122.62 (Win...	TCP 49172	HttpGetNormal	2015-06-30 13:12:45 ...	C:\Users\beh...	fernandatur.com/Scripts/hqnybx2w.php?id=960135
529	floridablueline header.jpg	jpg	183 79...	192.254.234.118 [floridablueline.co...	TCP 80	192.168.122.62 (Win...	TCP 49171	HttpGetNormal	2015-06-30 13:12:45 ...	C:\Users\beh...	www.floridablueline.com/floridablueline header.jpg
659	hqnybx2w.php[1].html	html	323 B	208.113.214.190 [fernandatur.com] ...	TCP 80	192.168.122.62 (Win...	TCP 49173	HttpGetNormal	2015-06-30 13:12:46 ...	C:\Users\beh...	www.fernandatur.com/Scripts/hqnybx2w.php?id=960135
764	index.6558F0B7.html	html	142 97...	46.30.45.65 [good.recycle2learn.com]	TCP 80	192.168.122.62 (Win...	TCP 49174	HttpGetNormal	2015-06-30 13:12:47 ...	C:\Users\beh...	good.recycle2learn.com/?xniKfredLBvKDIU=I3SKfPf.JxzF
811	index.php.swf	swf	15 763 B	46.30.45.65 [good.recycle2learn.com]	TCP 80	192.168.122.62 (Win...	TCP 49175	HttpGetNormal	2015-06-30 13:12:48 ...	C:\Users\beh...	good.recycle2learn.com/index.php?xniKfredLBvKDIU=I3S
841	version.xml11.6.602..html	html	351 B	23.10.250.43 [a1293.d.akamai.net] ...	TCP 80	192.168.122.62 (Win...	TCP 49176	HttpGetNormal	2015-06-30 13:12:52 ...	C:\Users\beh...	fpdownload2.macromedia.com/get/flashplayer/update/cu
833	index.php.x-msdownload	x-...	352 25...	46.30.45.65 [good.recycle2learn.com]	TCP 80	192.168.122.62 (Win...	TCP 49174	HttpGetNormal	2015-06-30 13:12:51 ...	C:\Users\beh...	good.recycle2learn.com/index.php?xniKfredLBvKDIU=I3S

In frame 575, in wireshark capture, we found that fernandature.com with IP address 208.113.214.190 sent HTTP1.1 moved permanently to the host machine(192.168.122.62) . Moreover, this frame is the response frame of 553. The wireshark screenshot is shown as a following picture:



Here, we found that A TCP handshake does not contain any redirect information. So TCP handshaking is fine. However, we check the application layer, we found that:

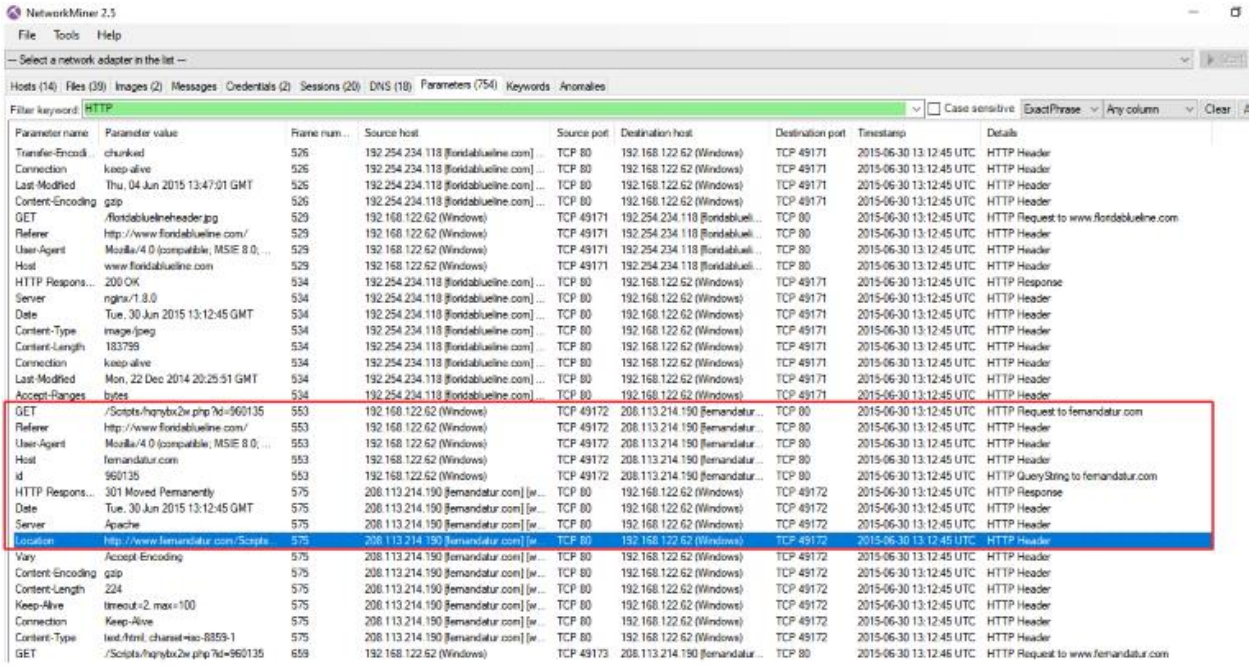
< HTTP/1.1 301 Moved Permanently …

< Location: http://www.fernandatur.com/Scripts/hqnybx2w.php?id=960135

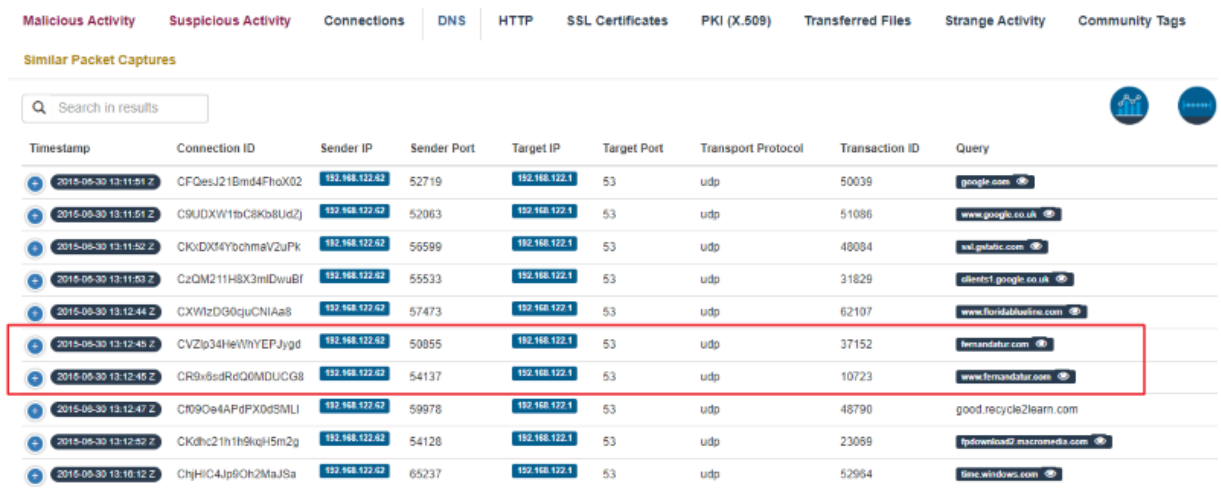
Since this is a 301 **permanent** redirect the client does not even need to visit the original site again but will instead use the new location on repeated tries. Only on the first try it will visit the original site to receive the redirect.

In Networkminer is again this redirection shows:

University of Victoria

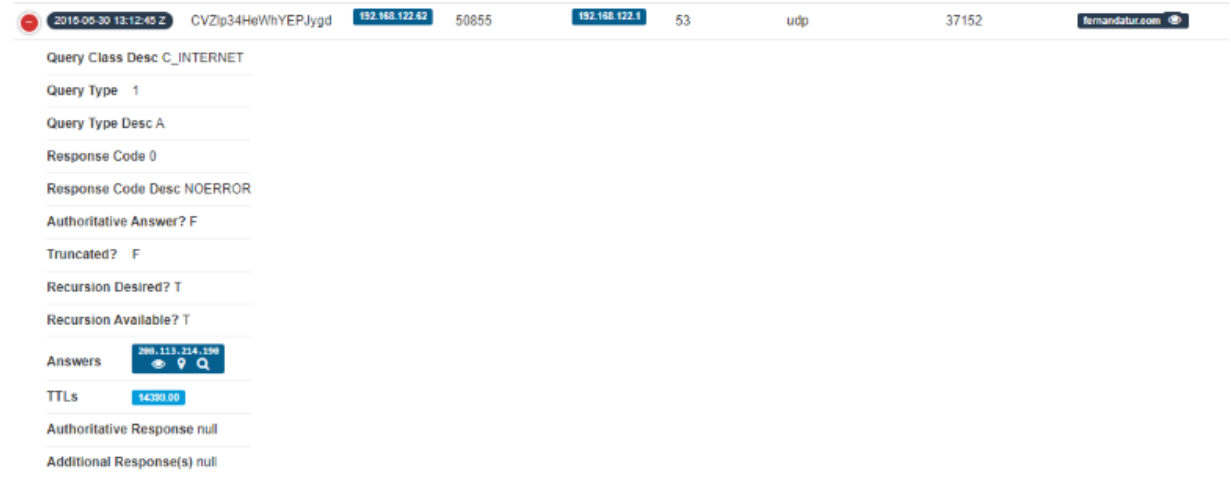


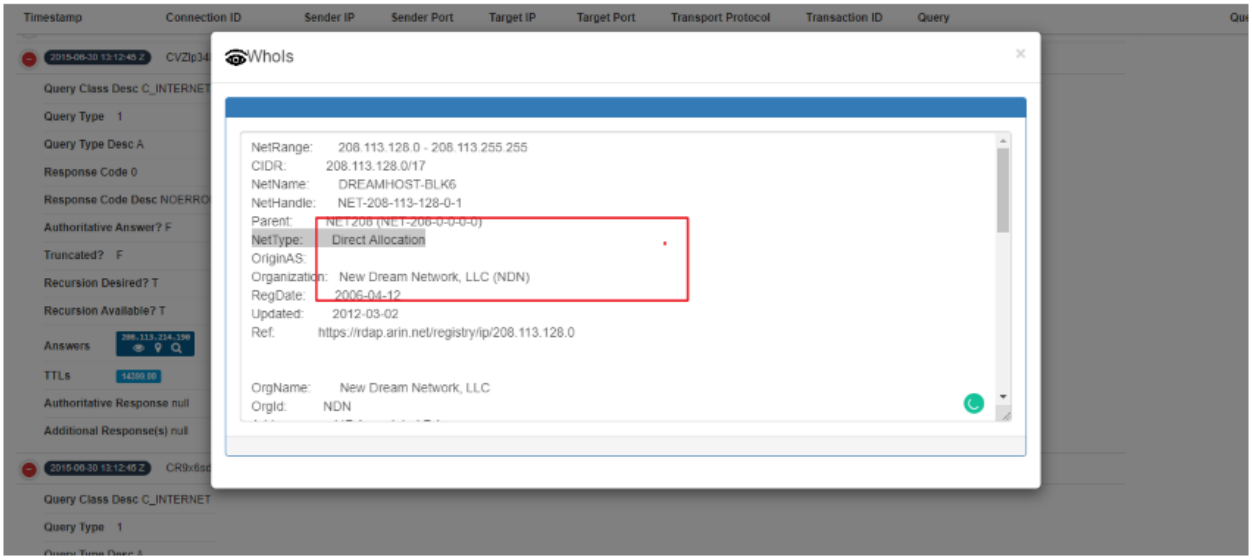
Finally, as a report of packettotal in DNS Tab we can see that this site is redirected.

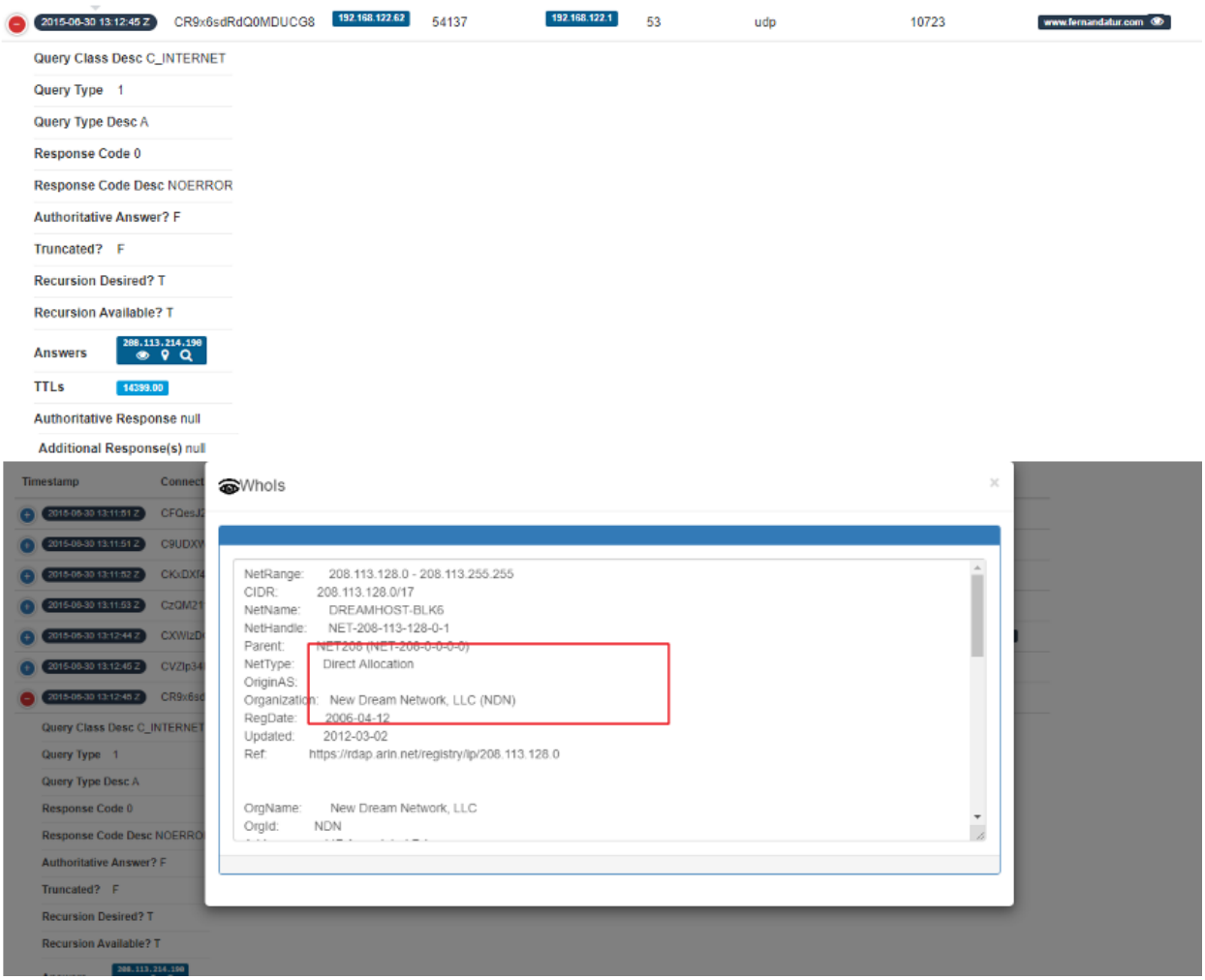


When we click on whoIs Lookup we can see that those sites (fernandatur.com and www.fernandatur.com) are Direct Allocation.All screenshots are shown as a following pictures:

University of Victoria

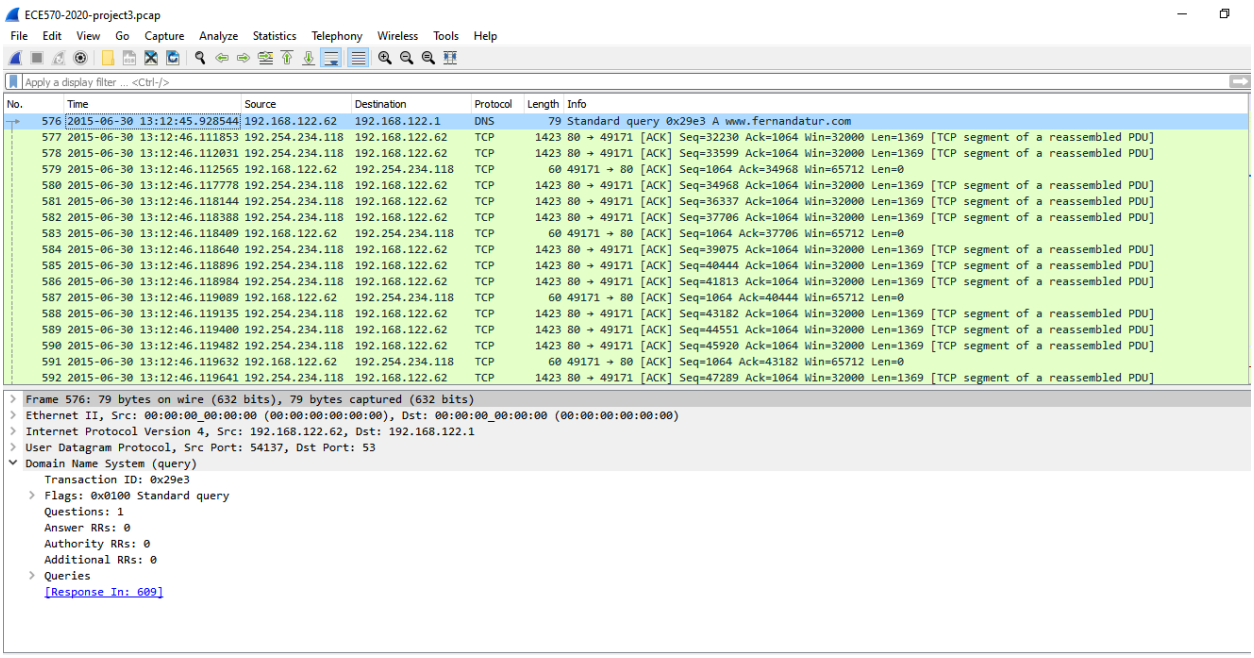






Note: We have a lot of TCP ACK between floridablueline.com and host from frame 533 after host open fernandature.com

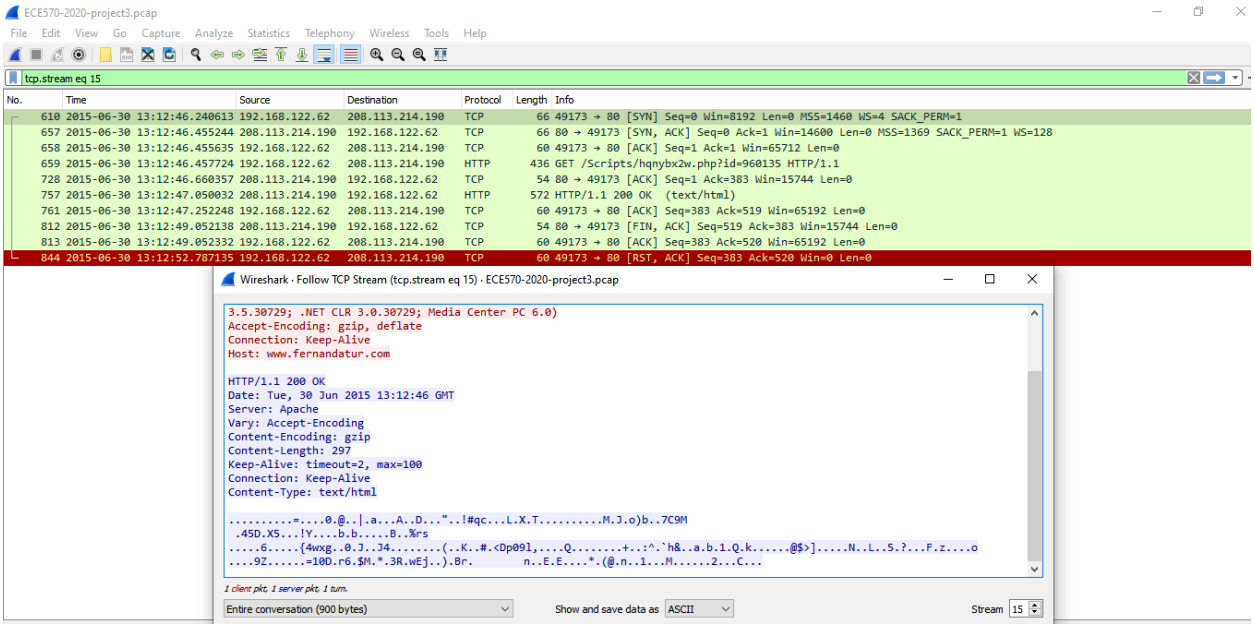
At the end of seconds of 13:12:45, in frame 576 the host sent a request to DNS for open www.fernandature.com. In frame 609, DNS responded to the host and sent the IP address of this site. The IP address is 208.113.214.190.



In frame 610 host request to start TCP handshaking to IP address is 208.113.214.190. In frame 610 send SYN, IP address 208.113.214.190 response SYN,ACK on frame 657. And immediately on frame 658 the host sent ACK to this IP address that is the website: www.fernandature.com.

In frame 659, the host machine sent one HTTP request to 208.113.214.190. This request was sent via HTTP protocol at 13:12:46. The wireshark screenshot is as follows:

University of Victoria



The host machine was infected by a file transferred on frame 526 from floridablueline.com and after that the host led to infection of other sites.

During that time again floridablueline.com sent an ACK to the host and after some ACK from this site the host sent a response.

According to packet total information, in HTTP Tab we found one data related to 13:12:46. After, download that file and check on virustotal. We found that this script is trojan. Infact, this script is the same as the script of frame 553. This file transferred to host in frame 526 from flordblueline.com .

University of Victoria

Malicious Activity | Suspicious Activity | Connections | DNS | HTTP | SSL Certificates | PKI (X.509) | Transferred Files | Strange Activity | Community Tags

Similar Packet Captures

Search in results

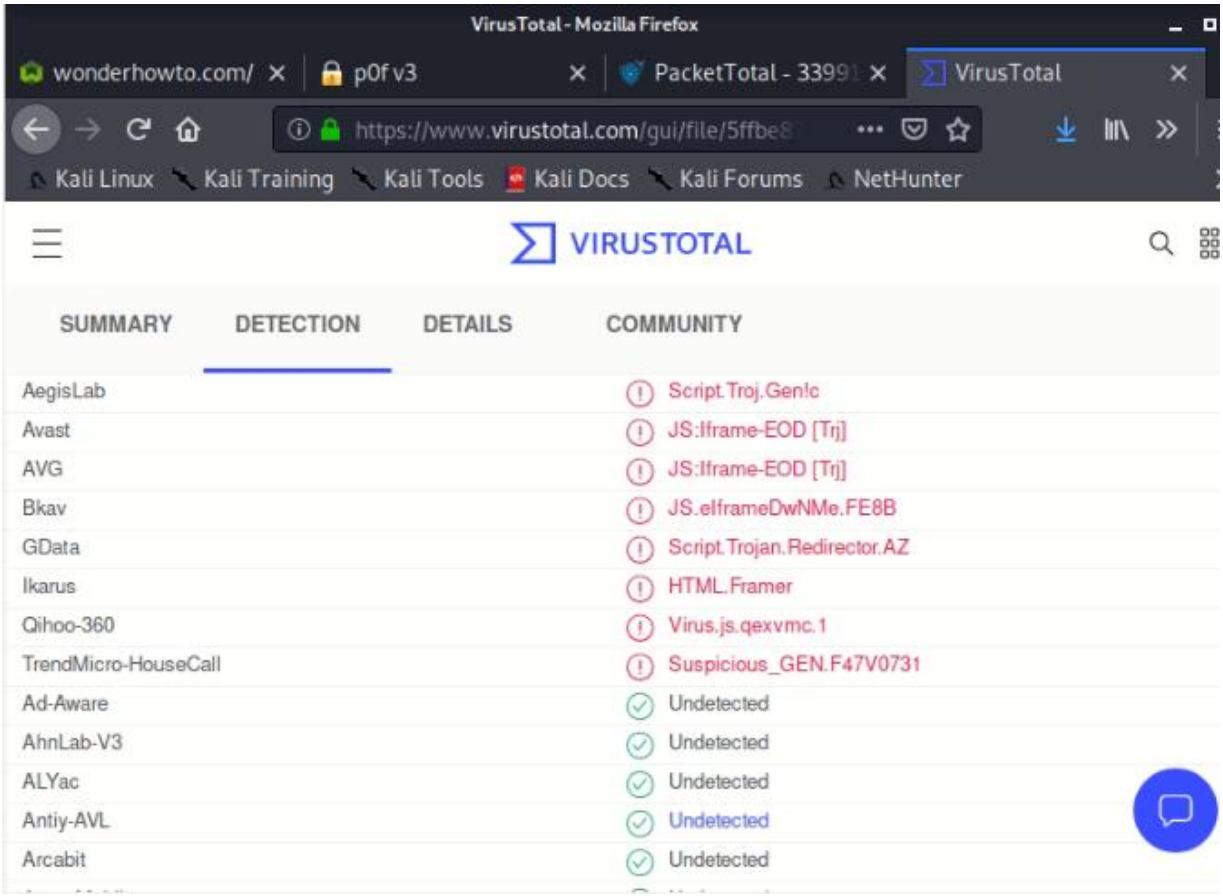
Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transaction Depth	Method	Host
2015-06-30 13:11:51 Z	Cs8Y2Q2yukRvrbFS6	192.168.122.62	49158	216.58.208.46	80	1	GET	google.com
2015-06-30 13:11:51 Z	CMuHRQ3Jfj0FRkK1Qc	192.168.122.62	49159	216.58.210.67	80	1	GET	www.google.co.uk
2015-06-30 13:12:44 Z	CIFU4P2TqMGvSgfc62	192.168.122.62	49170	216.58.210.67	80	1	GET	www.google.co.uk
2015-06-30 13:12:44 Z	CIFU4P2TqMGvSgfc62	192.168.122.62	49170	216.58.210.67	80	2	GET	www.google.co.uk
2015-06-30 13:12:44 Z	CALygR1JnJXOgNnETj	192.168.122.62	49171	192.254.234.118	80	1	GET	www.floridablueline.com
2015-06-30 13:12:45 Z	CALygR1JnJXOgNnETj	192.168.122.62	49171	192.254.234.118	80	2	GET	www.floridablueline.com
2015-06-30 13:12:45 Z	CMvAQV2OwfXQnWdhX2	192.168.122.62	49172	208.113.214.190	80	1	GET	fernandatur.com
2015-06-30 13:12:46 Z	CMHhzK1MVihV1X1U2j	192.168.122.62	49173	208.113.214.190	80	1	GET	www.fernandatur.com
2015-06-30 13:12:47 Z	CocBdE3VP4U7EE8PX5	192.168.122.62	49174	46.30.45.65	80	1	GET	good.recycle2learn.com
2015-06-30 13:12:48 Z	CtGI8l22yrRPVILob	192.168.122.62	49175	46.30.45.65	80	1	GET	good.recycle2learn.com

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transaction Depth	Method	Host
2015-06-30 13:12:46 Z	CMHhzK1MVihV1X1U2j	192.168.122.62	49173	208.113.214.190	80	1	GET	www.fernandatur.com

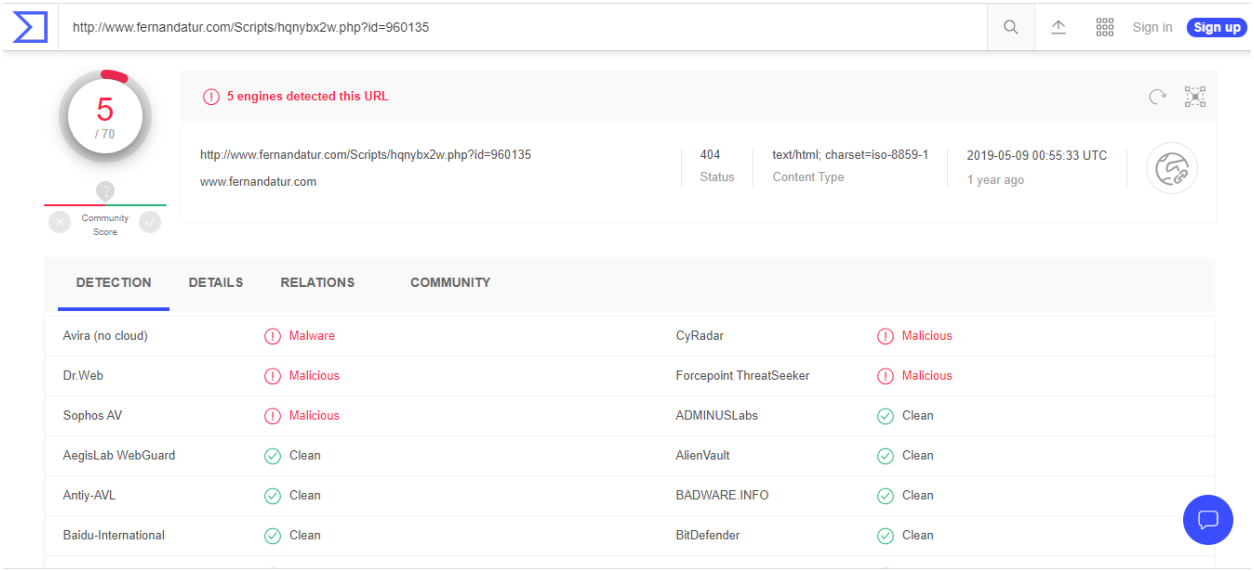
URI /Scripts/hqnybx2w.php?id=960135
Referrer http://www.floridablueline.com/
User Agent ....NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
Request Body Length 0
Response Body Length 323
Status Code 200
Status Message OK
Info Code null
Info Message null
File null
Username null
Password null
Proxied null
Sender File IDs null
Sender Mime Types null
Recipient File IDs F43AYX1VSTBLTTS...
Recipient Mime Types application/javascript

Client Headers ACCEPT,REFERER,ACCEPT-LANGUAGE,USER-AGENT,ACCEPT-ENCODING,CONNECTION,HOST
Server Headers null
Cookie Variables null
URI Variables /Scripts/hqnybx2w.php?id

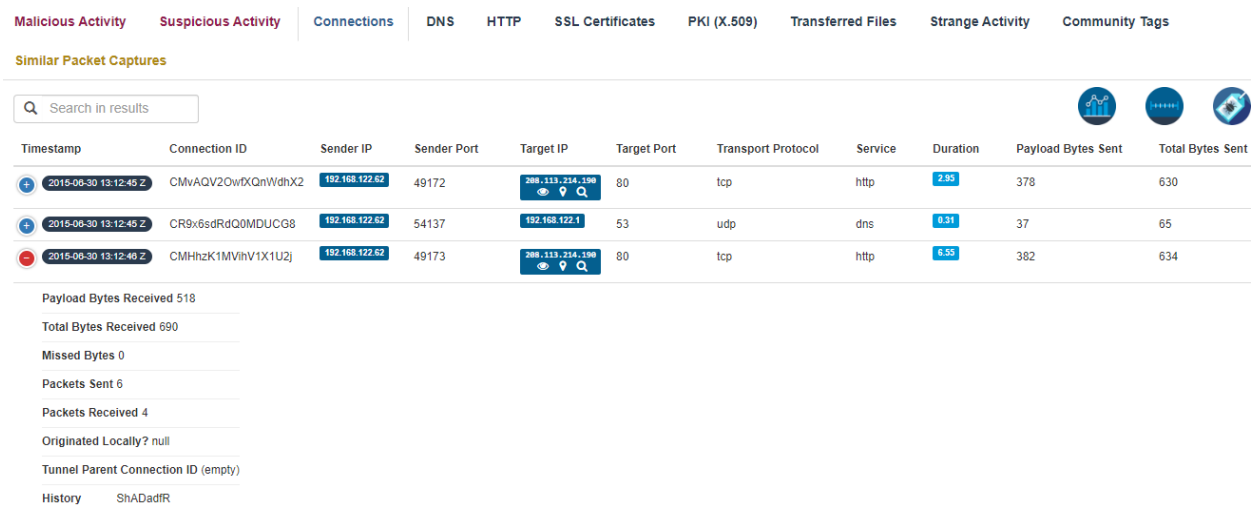
University of Victoria



Again the URL of this site is in virus total indicates trojan. Same as frame 553.

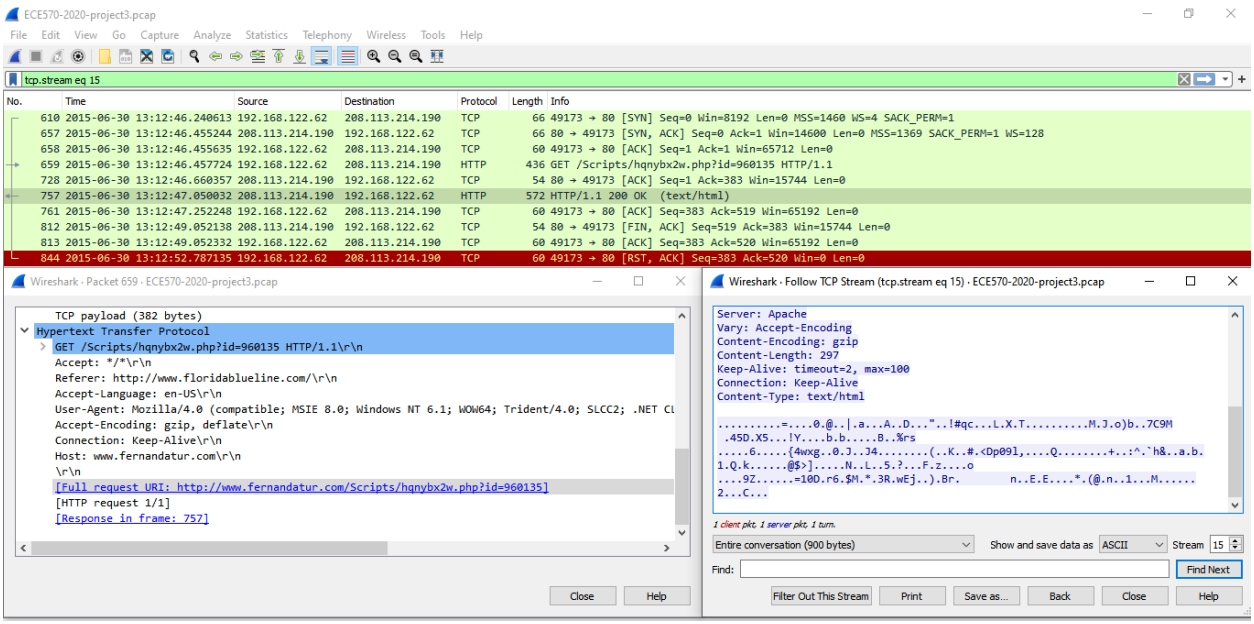


In the connection Tab of the packet total we found that in time 13:12:46 the connection duration between host and 208.113.214.190 is 6:55 seconds.



After HTTP request of host to 208.113.214.190 in frame 659 to GET malicious scripts. In frame 757, the target with 208.113.214.190 as an IP address sent HTTP 1.1 200 OK

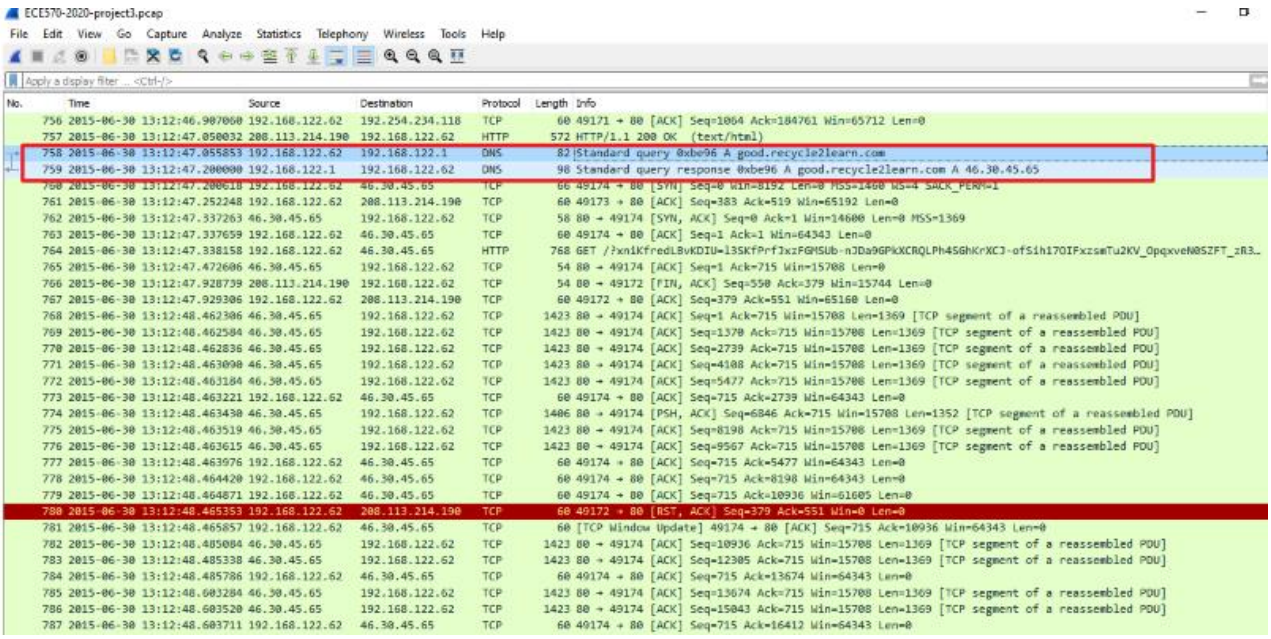
to the host. The host IP address is 192.168.122.62. The wireshark screenshot and TCP stream is as a follows:



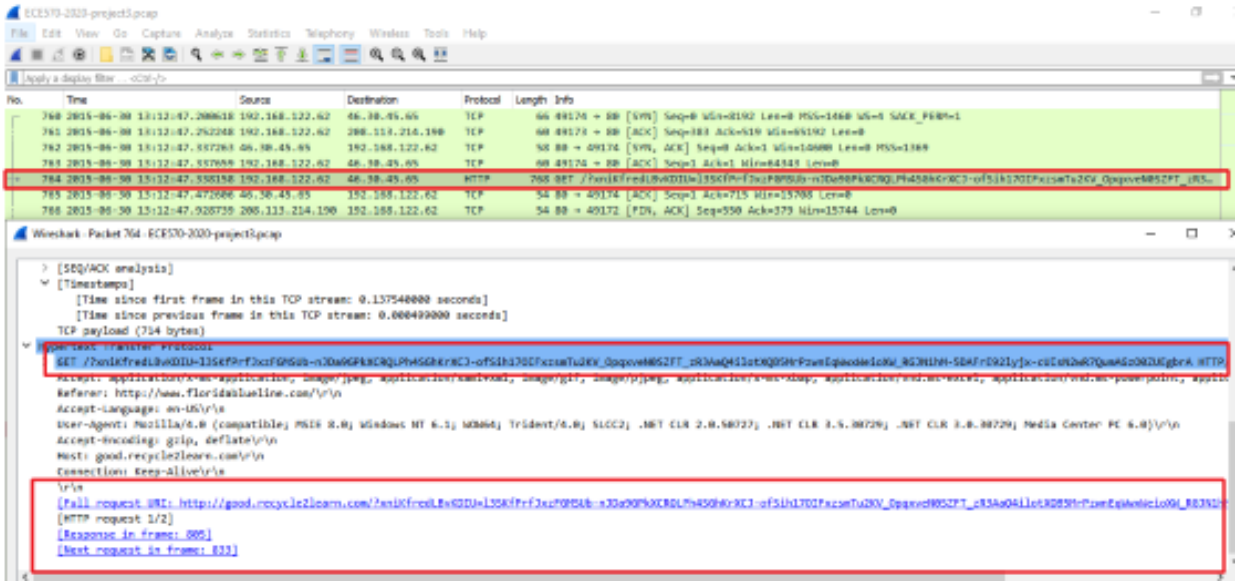
Note: The **HTTP 200** OK success **status response code** indicates that the request has succeeded.

In frame 758, new requests start. Host sent a request to the DNS server to access the site good.recycle2learn.com at 13:12:47. And in the next frame, DNS responded to the host and sent the IP address of this site. The ip address is 46.30.45.65. The wireshark screenshot is as a follow:

University of Victoria

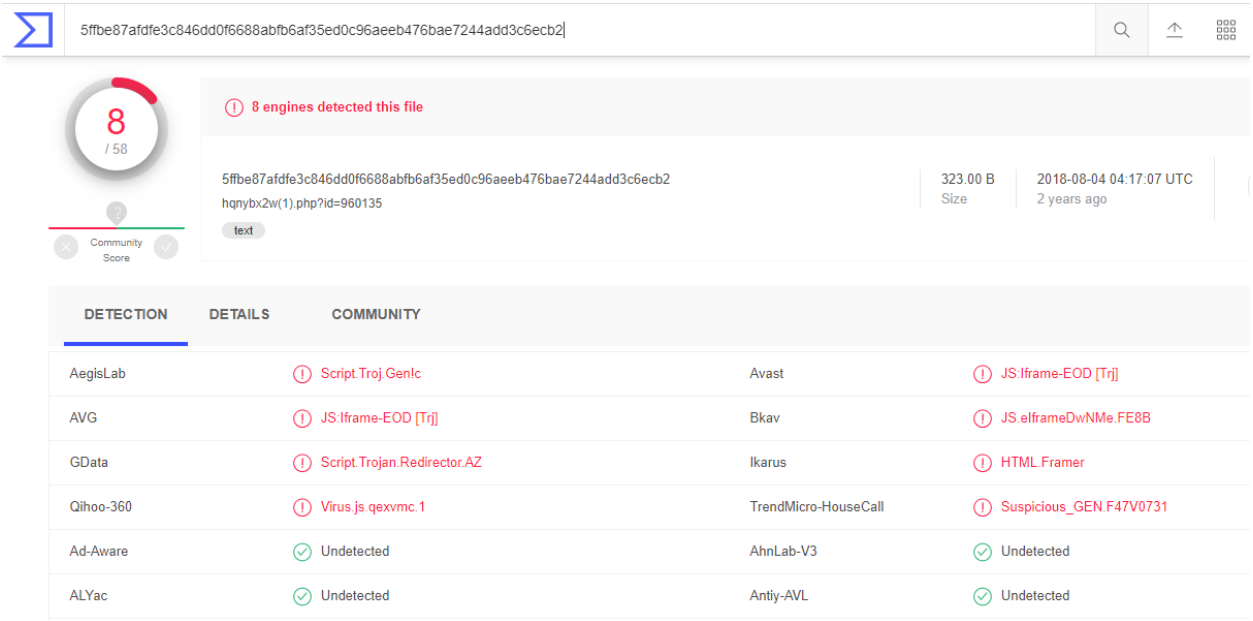


After TCP handshaking in packet 760-761-762, the host sent ACK to 46.30.45.65. In frame number 764, the host sent an HTTP GET request to 46.30.45.65 at 13:12:47.



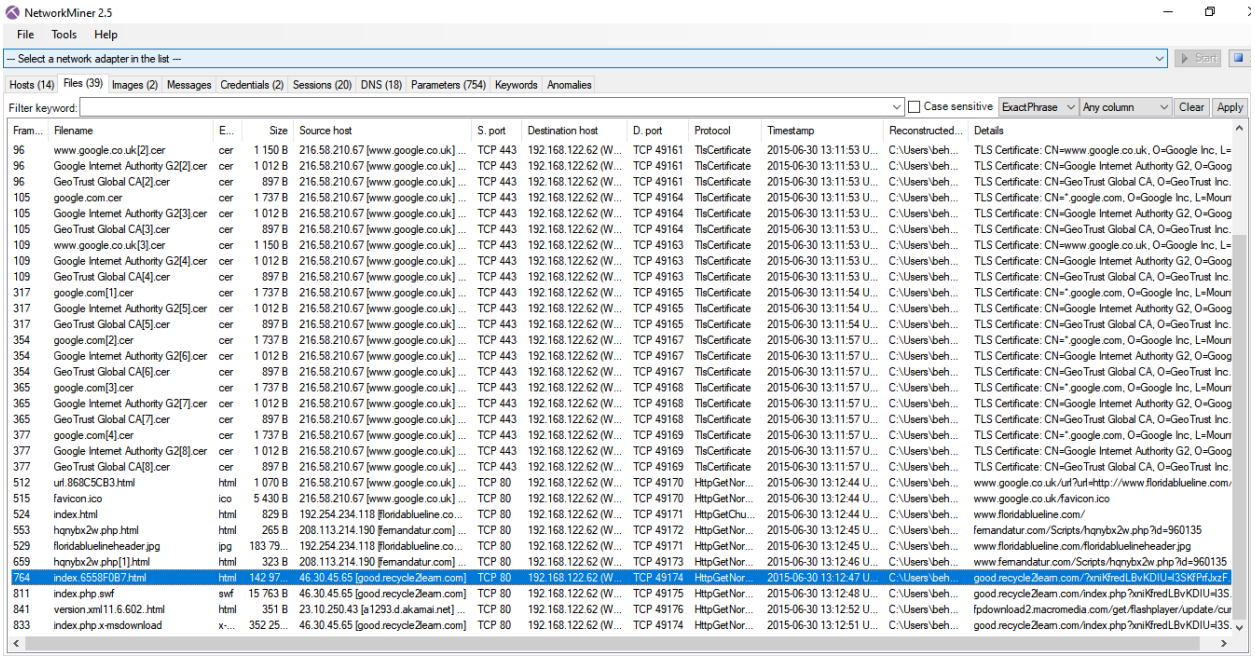
At 13:12:47 in File Transferred on packet total we found information that the host machine infected 46.30.45.65 with file as a script like the last two IP addresses which related to fernandature.com and www.fernandature.com . Screenshot is shown as a follows:

The virustotal check result of this scripts shown as a follows:



Network miner report on part Files prove that this scripts and file transferred to good.recycle2learn.com with IP address 46.30.45.65 from host (192.168.122.62).The screenshot shown as a follows:

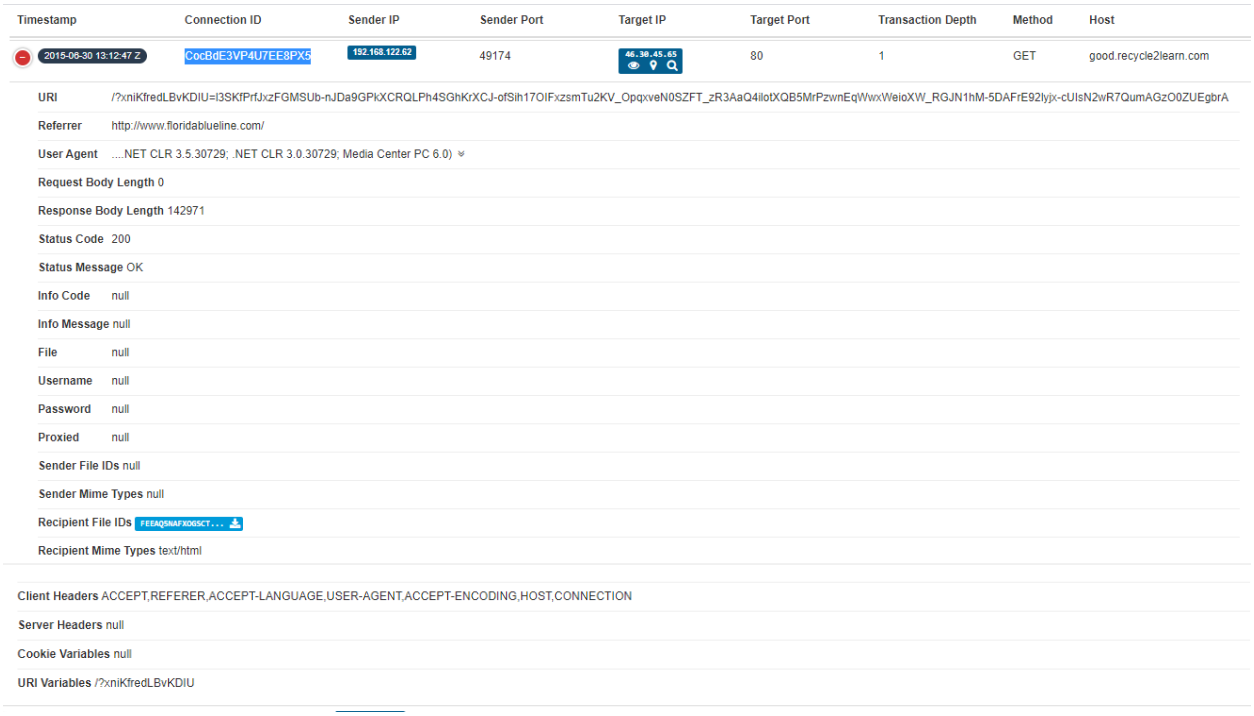
University of Victoria



529 floridablulineheader.jpg jpg 183 79... 192.254.234.118 [floridablueline.co... TCP 80 192.168.122.62 (W... TCP 49171 HttpGetNor... 2015-06-30 13:12:45 U... C:\Users\beh... www.floridablueline.com/floridablulineheader.jpg
659 hqnybx2w.php[1].html html 323 B 208.113.214.190 [fernandatur.com] ... TCP 80 192.168.122.62 (W... TCP 49173 HttpGetNor... 2015-06-30 13:12:46 U... C:\Users\beh... www.fernandatur.com/Scripts/hqnybx2w.php?id=960135
764 index.6558F0B7.html html 142 97... 46.30.45.65 [good.recycle2learn.com] TCP 80 192.168.122.62 (W... TCP 49174 HttpGetNor... 2015-06-30 13:12:47 U... C:\Users\beh... good.recycle2learn.com/?xniKfredLBvKDIU=l3SKfPrfJxzF
811 index.php.swf swf 15 763 B 46.30.45.65 [good.recycle2learn.com] TCP 80 192.168.122.62 (W... TCP 49175 HttpGetNor... 2015-06-30 13:12:48 U... C:\Users\beh... good.recycle2learn.com/index.php?xniKfredLBvKDIU=l3

In packettotal report, in HTTP Tab, we found one HTTP Transaction between Sender IP: 192.168.122.62 and target IP: 46.30.45.65 . The screenshot shown as a follows:

University of Victoria



Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transaction Depth	Method	Host
2015-08-30 13:12:47 Z	CocBdE3VP4U7EE8PX5	192.168.122.62	49174	46.30.45.65	80	1	GET	good.recycle2learn.com

URI /?xniKfredLBvKDIU=I3SKfPrfJxzFGMSUb-nJDa9GPkXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_OpqxveN0SZFT_zR3AaQ4ilotXQB5MrPzwnEqWwxWeioXW_RGJN1hM-5DAFrE92lyjx-cUIsN2wR7QumAGzO0ZUEgbrA

Referrer http://www.floridablueline.com/

User Agent ....NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)

Request Body Length 0

Response Body Length 142971

Status Code 200

Status Message OK

Info Code null

Info Message null

File null

Username null

Password null

Proxied null

Sender File IDs null

Sender Mime Types null

Recipient File IDs FEEAQSNAFXO0SCT...

Recipient Mime Types text/html

Client Headers ACCEPT,REFERER,ACCEPT-LANGUAGE,USER-AGENT,ACCEPT-ENCODING,HOST,CONNECTION

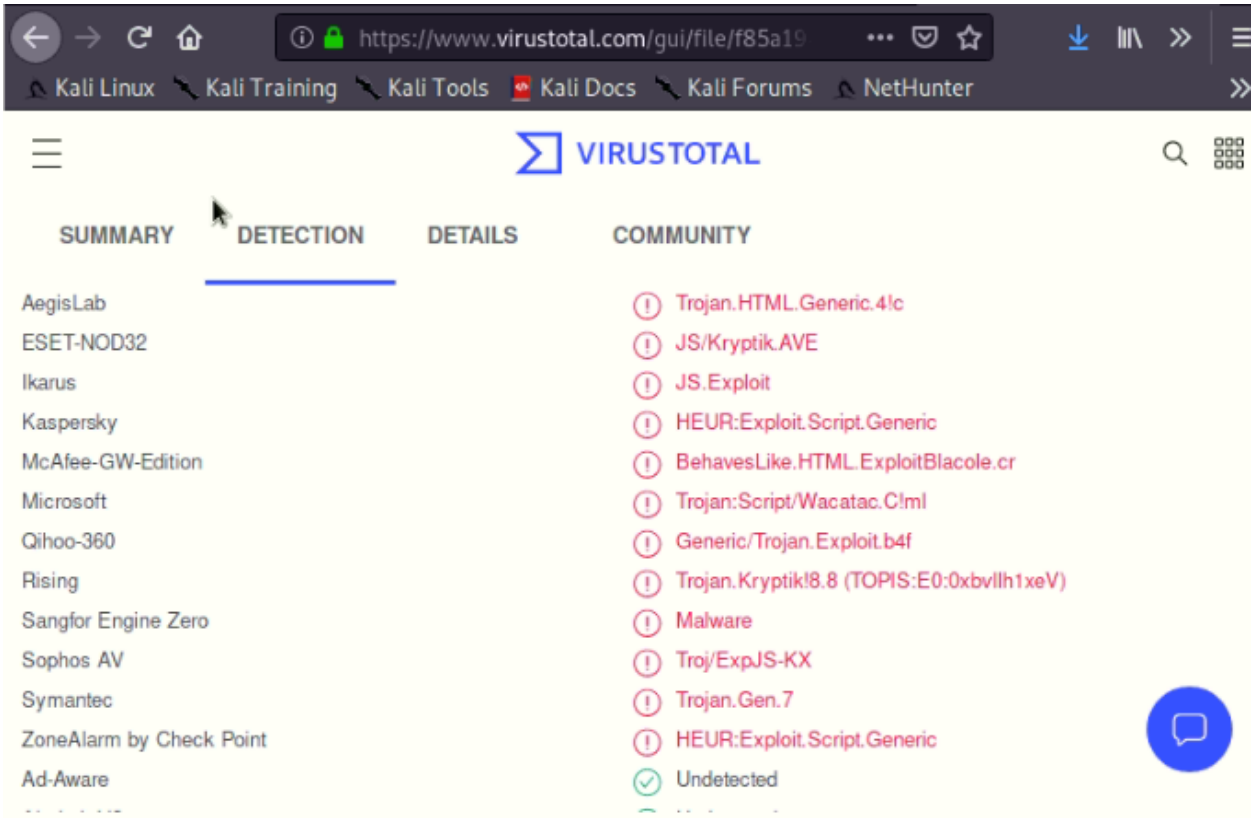
Server Headers null

Cookie Variables null

URI Variables /?xniKfredLBvKDIU

The virustotal check of the file in this part illustrates that this script is trojan scripts. Again like other URLs , fernandature.com, www.fernandature.com this site good.recycled2learn.com and this scriptis is Trojan scripts and Malware. The screen shot of virustotal report is as follows:

University of Victoria



The DNS Tab in the packet total gives information about sender IP is 192.168.122.62 and target IP is DNS server with IP address 192.168.122.1. Sender port is 59978 and target port is 53 on UDP transport protocol at 13:12:47. The screenshot is as a follows:
Note:

Port: 59978/TCP

59978/TCP - Known port assignments *(2 records found)*		
Service	Details	Source
	Dynamic and/or Private Ports	IANA
	Xsan. Xsan Filesystem Access	Apple

Port: 59978/UDP

59978/UDP - Known port assignments *(1 record found)*		
Service	Details	Source
	Dynamic and/or Private Ports	IANA

University of Victoria

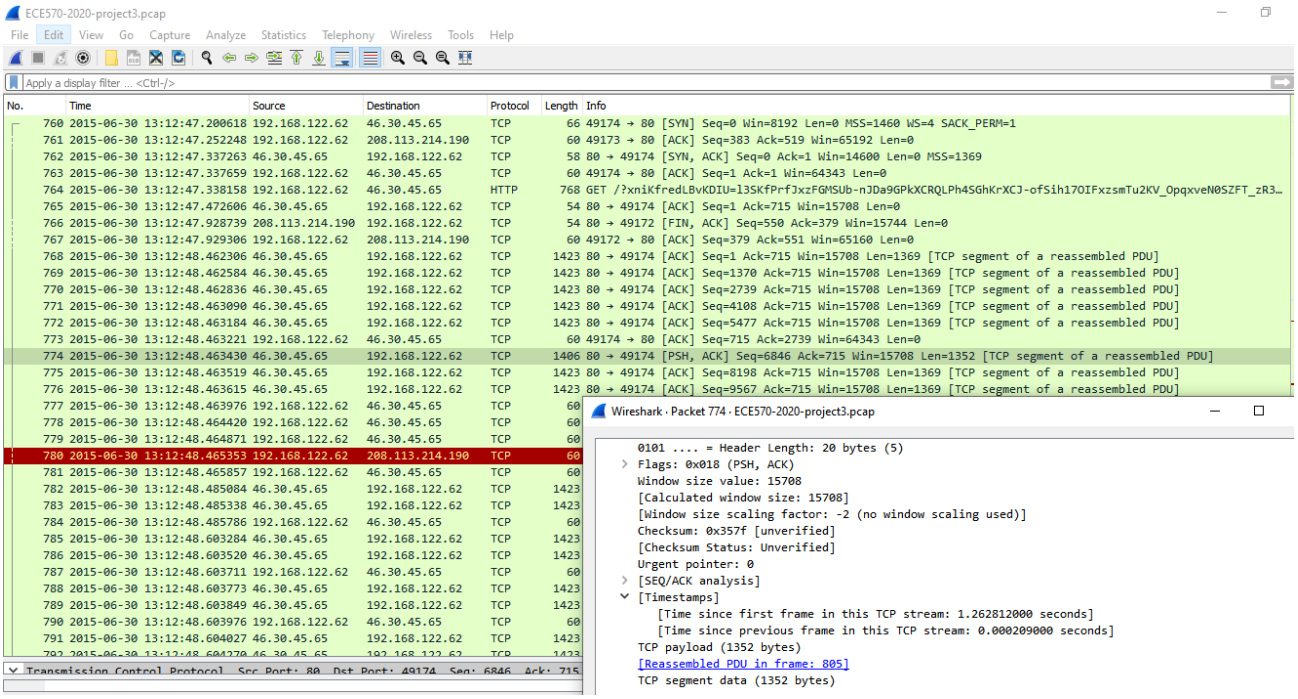
Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	Transaction ID	Query
2015-06-30 13:12:47 Z	Cf09Oe4APdPX0dSMLI	192.168.122.62	59978	192.168.122.1	53	udp	48790	good.recycle2learn.com

Query Class Desc C_INTERNET
Query Type 1
Query Type Desc A
Response Code 0
Response Code Desc NOERROR
Authoritative Answer? F
Truncated? F
Recursion Desired? T
Recursion Available? T
Answers 46.30.45.65
TTLs 3321.00
Authoritative Response null
Additional Response(s) null

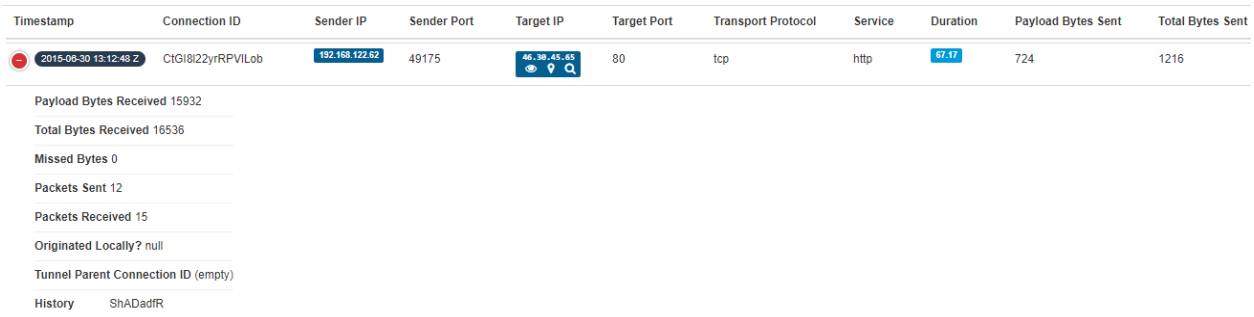
In frame 768, good.recycle2learn.com with IP address 46.30.45.65 sent some ACK to the host. After 5 frames, the host sent ACK to respond in time :13:12:48.

In frame 774, good.recycle2learn.com with IP address 46.30.45.65 sent some PSH,ACK to the host. PSH,ACK indicates the host is acknowledging receipt of some previous data and also transmitting some more data.

University of Victoria

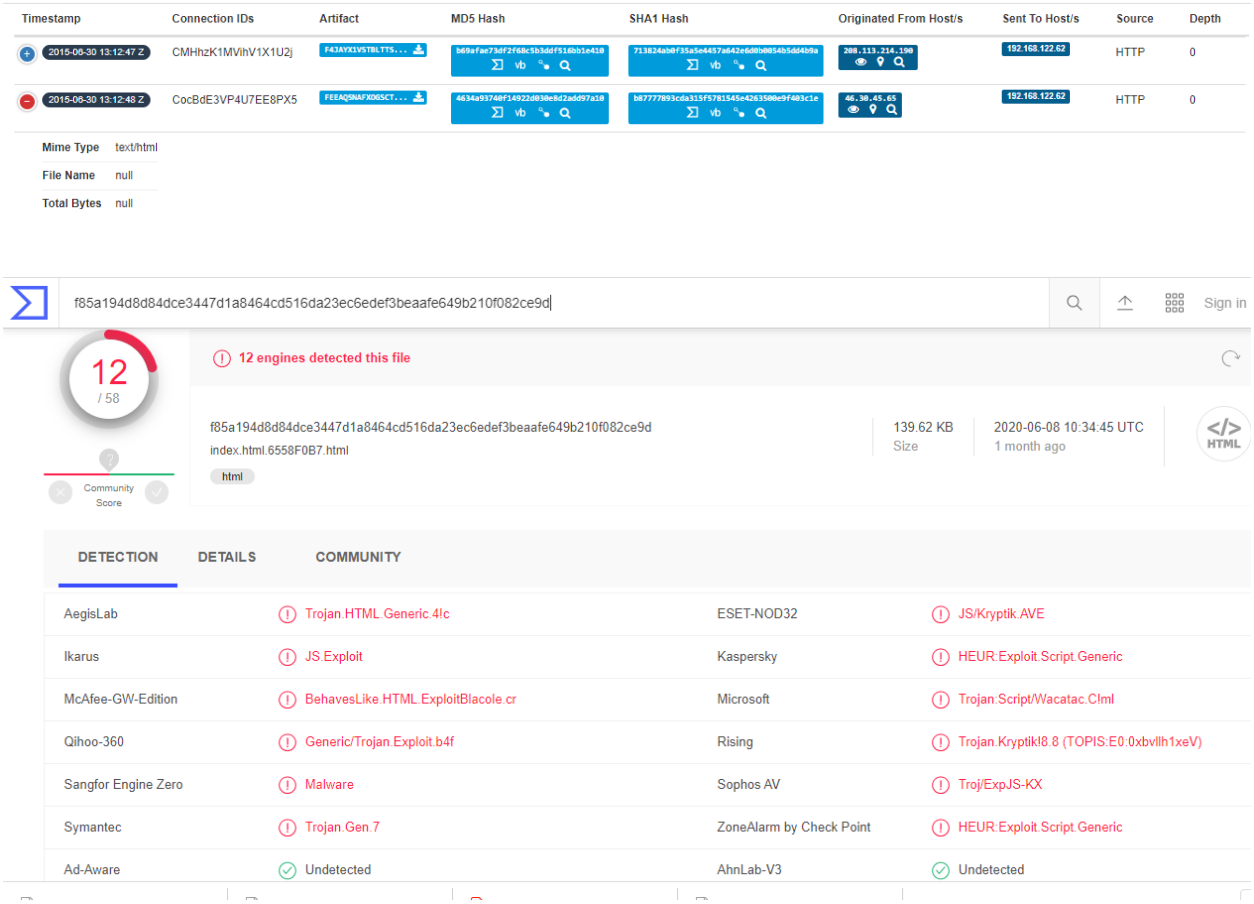


According to information on packettotal in the Connections part, we found a packet information between host and good,recycle2learn.com on TCP transport protocol and http services.



Data from Files Transferred in packet total illustrates that the data transferred between 46.30.45.65 and 192.168.122.62 are malware and virustotal indicates that this is a

Trojan script. 12 engines prove this, and text/html file is detected by 12 engines. The screenshots are as a follows:



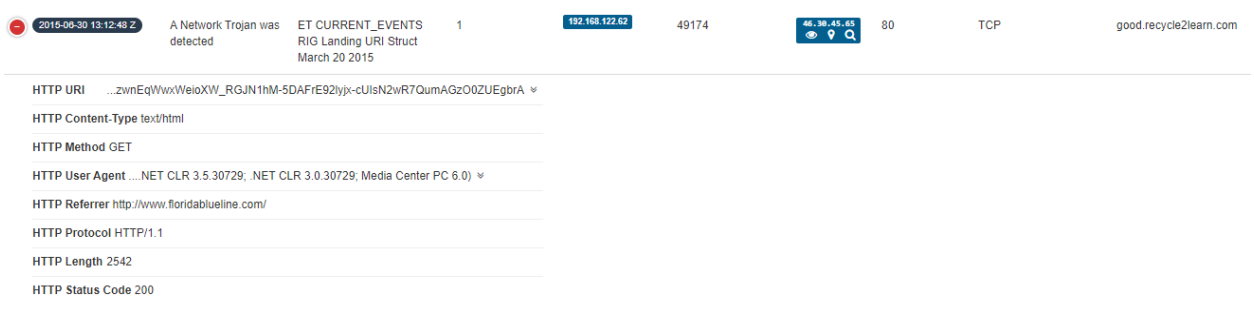
Packettotal malicious activity illustrates that at 13:12:48, we found two alert descriptions. The screenshot is shown as a follows:

University of Victoria

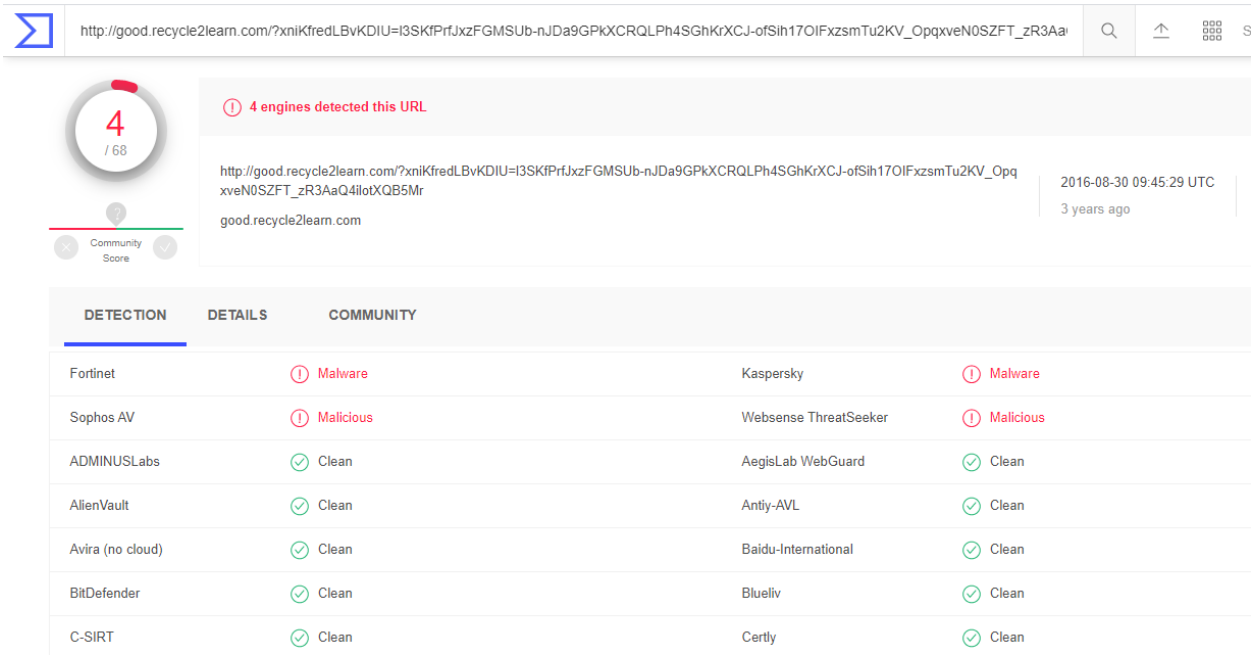
In this time, we check both alerts at time 13:12:48

At first open those alerts we can see that the first alert is ET CURRENT_EVENTS RIG Landing URI Struct March 20 2015.

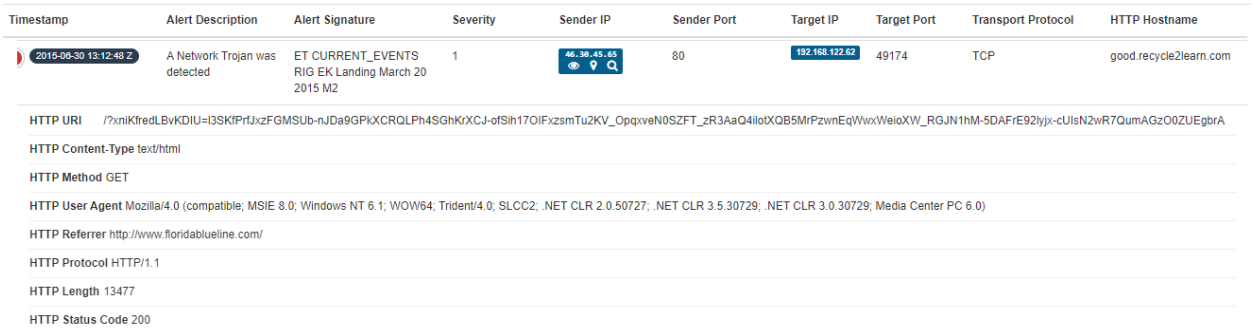
Note: One of the most well-known exploit kits in the crimeware underground marketplaces, clearly dominating the overall exploit kits category during the last several months, is no other but the RIG EK. Many words have been poured on RIG's close ties to Ransomware.



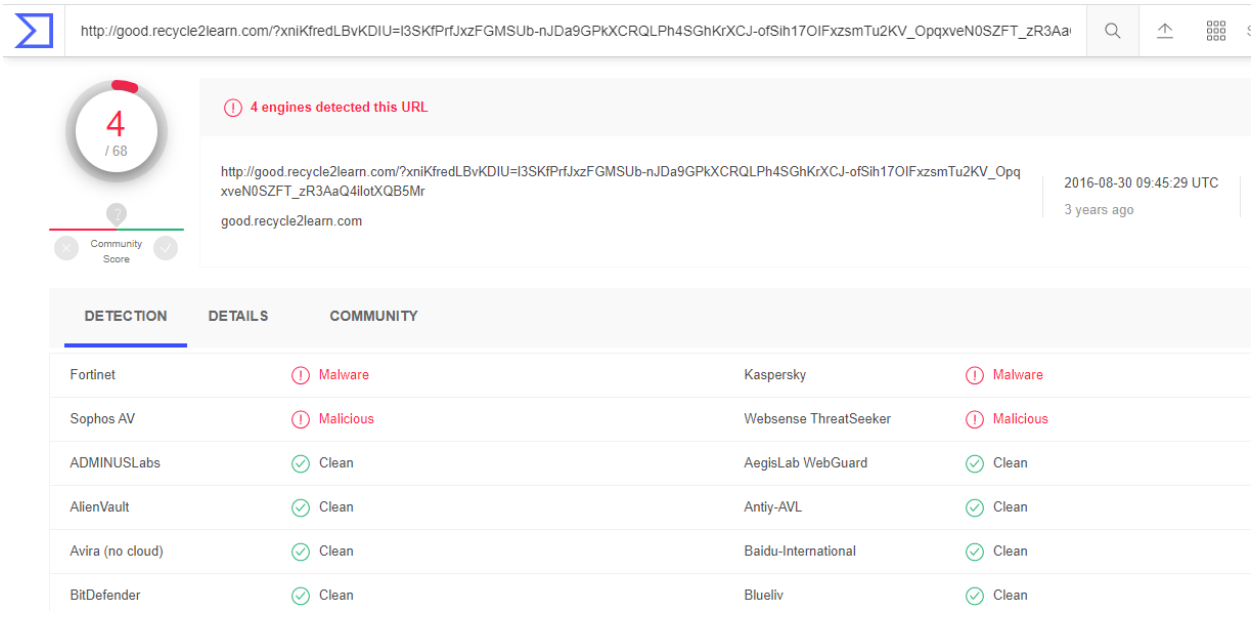
When we copy the Url to check on virustotal. We found that this is malware.



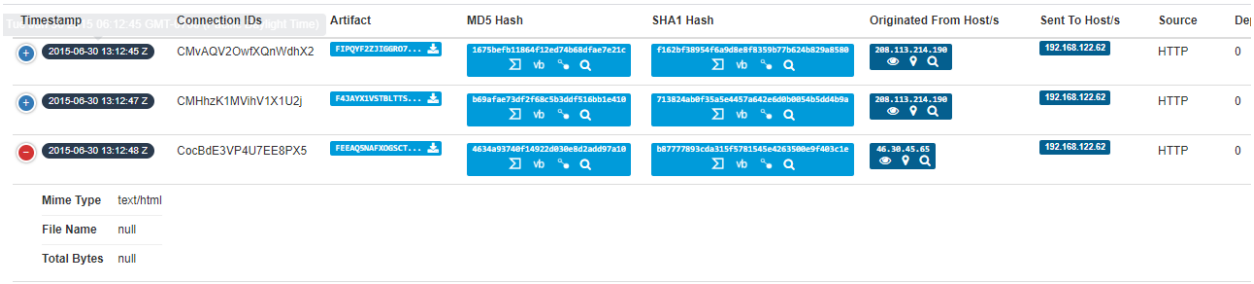
In the second alert ET CURRENT_EVENTS RIG EK Landing March 20 2015 M2, we found that this alert is between good.recycle2learn.com and host on TCP protocol.



When we copy this url to virustotal.com to check detected engines. Screenshot is as a follow:

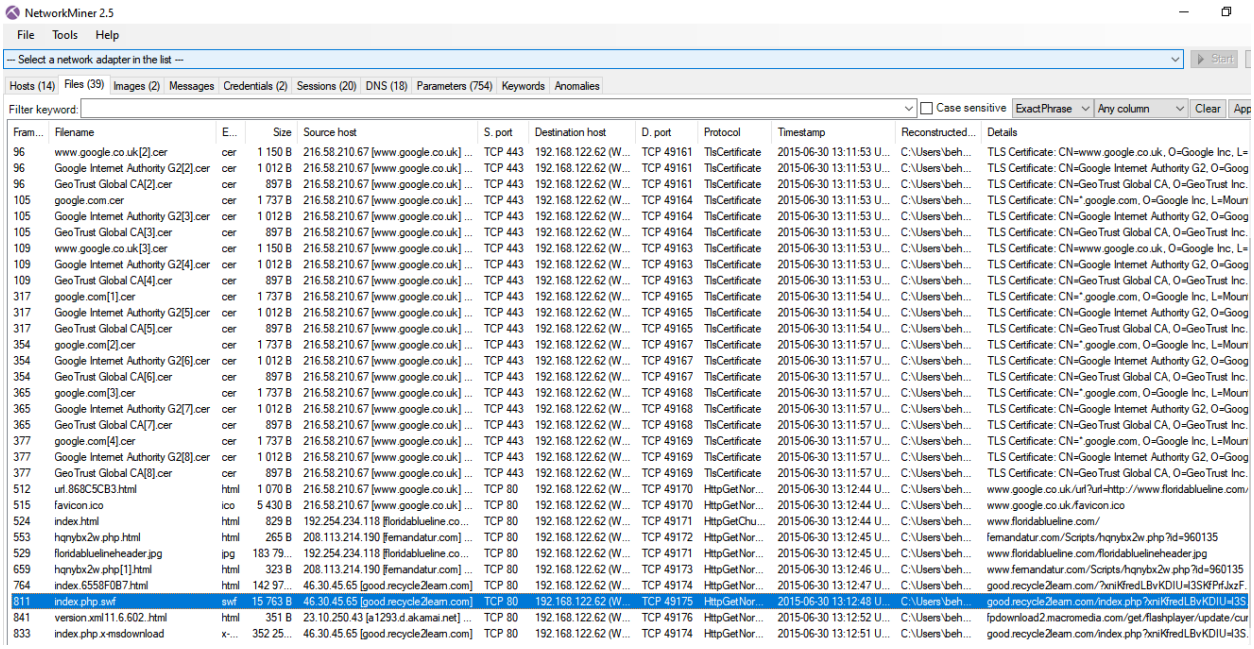


Only one item available in File Transferred related to time 13:12:48

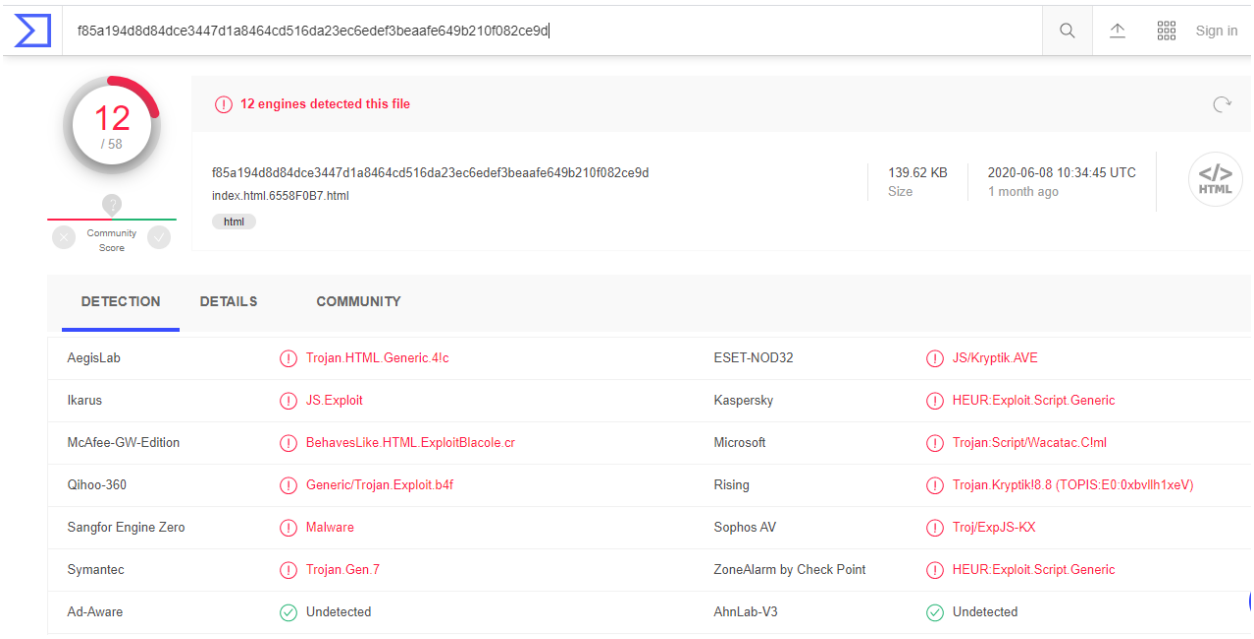


The file type is text.html. And also, in NetworkMiner we can find that this packet that sent the frame is 811. The file type is swf.

University of Victoria

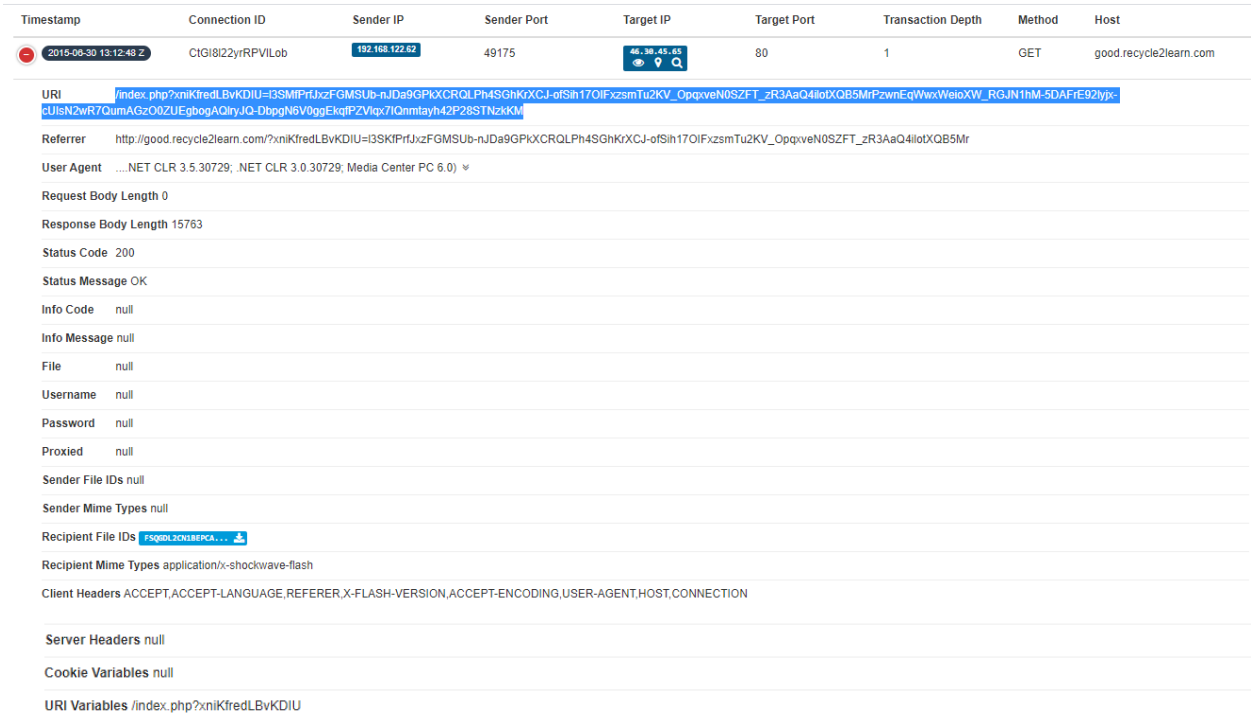


Based on the virustotal report, this file is malware when we click on virustotal lookup in File Transferred.



University of Victoria

According to HTTP report on packettotal, we found that in time 13:12:48



Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transaction Depth	Method	Host
2015-06-30 13:12:48 Z	CtGI8I22yrRPVILob	192.168.122.62	49175	46.30.45.65	80	1	GET	good.recycle2learn.com

URI /index.php?xniKfredLBvKDIU=I3SMfPrfJxzFGMSUb-nJDa9GPkXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_OpqxveN0SZFT_zR3AaQ4ilotXQB5MrPzwnEqWwxWeioXW_RGJN1hM-5DAFrE92Iyjx-cUIsN2wR7QumAGzO0ZUEgbogAQlryJQ-DbpgN6V0ggEkqfPZVlqx7lQnmtayh42P28STNzkKM

Referrer http://good.recycle2learn.com/?xniKfredLBvKDIU=I3SKfPrfJxzFGMSUb-nJDa9GPkXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_OpqxveN0SZFT_zR3AaQ4ilotXQB5Mr

User Agent ....NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)

Request Body Length 0

Response Body Length 15763

Status Code 200

Status Message OK

Info Code null

Info Message null

File null

Username null

Password null

Proxied null

Sender File IDs null

Sender Mime Types null

Recipient File IDs FSQ6DL2CN1BEPCA...

Recipient Mime Types application/x-shockwave-flash

Client Headers ACCEPT,ACCEPT-LANGUAGE,REFERER,X-FLASH-VERSION,ACCEPT-ENCODING,USER-AGENT,HOST,CONNECTION

Server Headers null

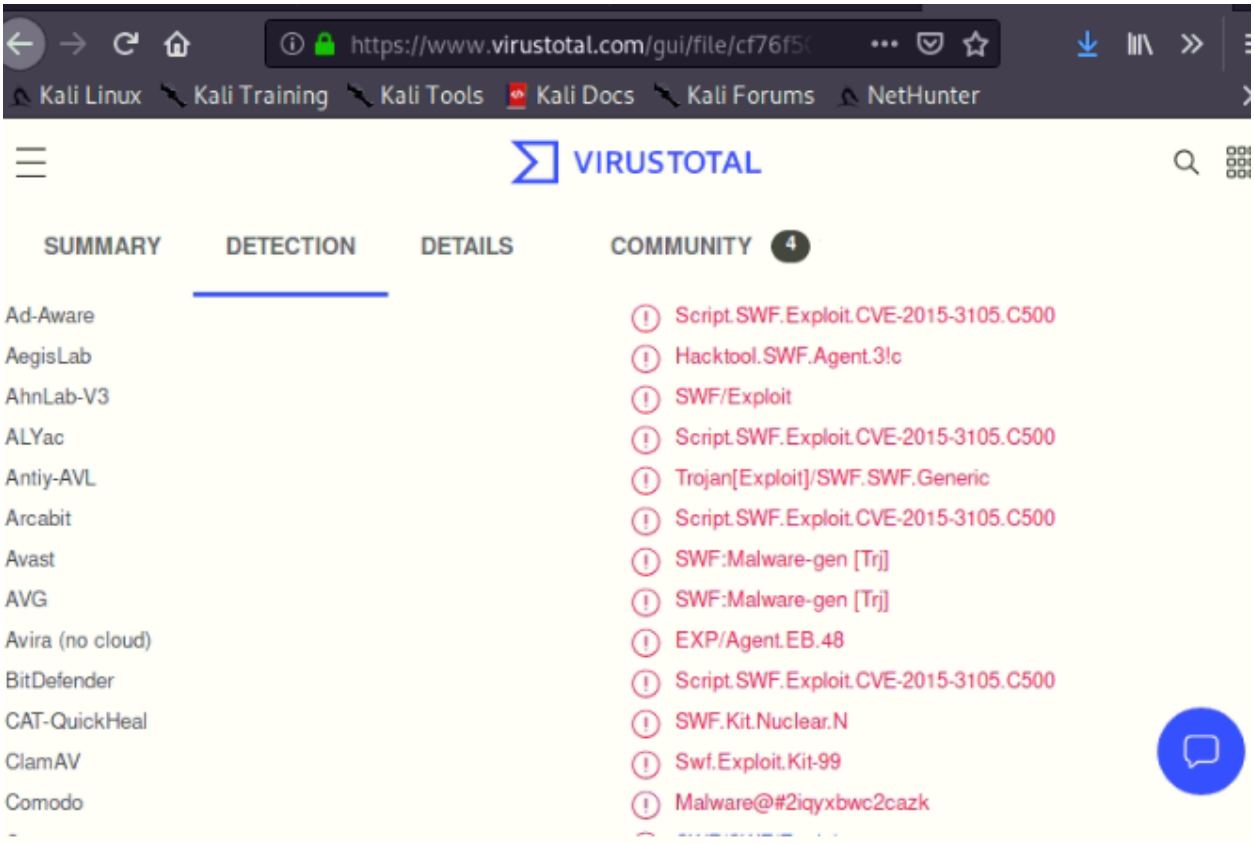
Cookie Variables null

URI Variables /index.php?xniKfredLBvKDIU

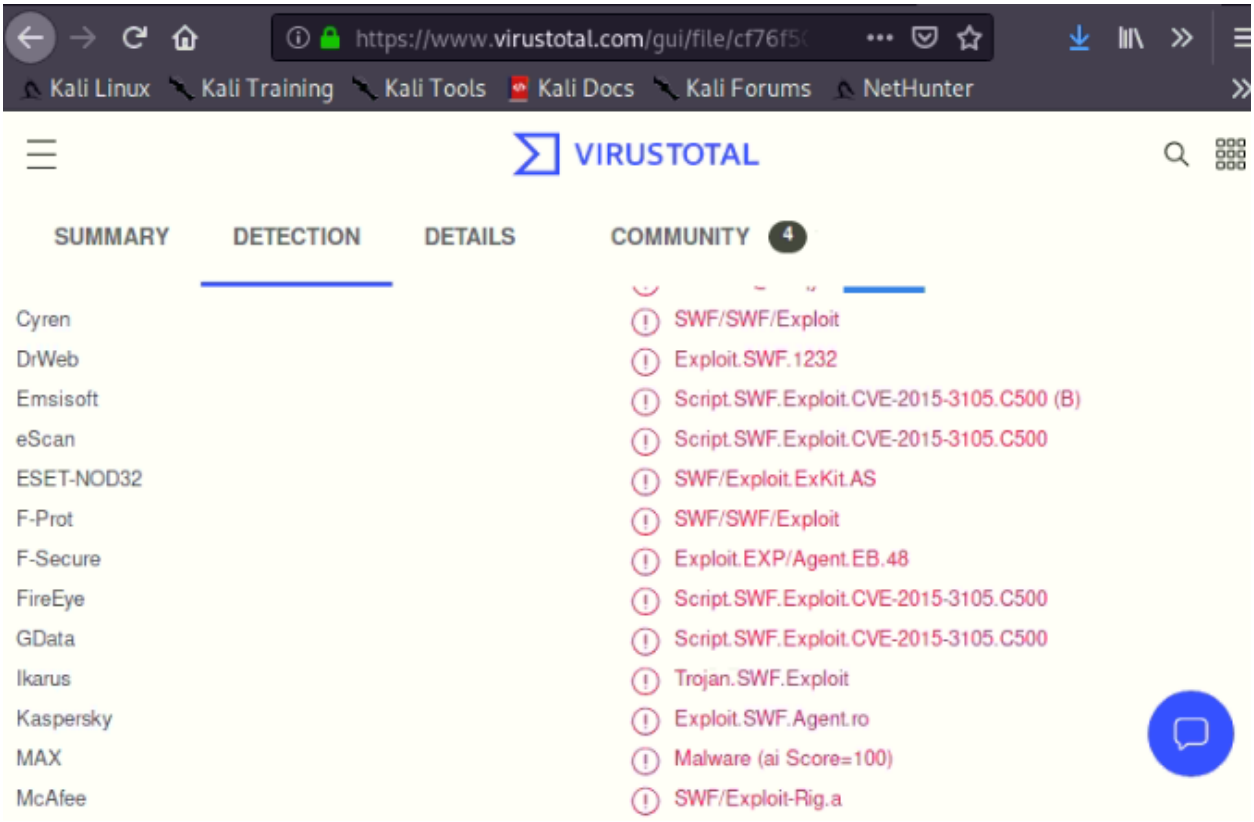
After, download the file and check it on virustotal, virustotal result check is shown as a follows:

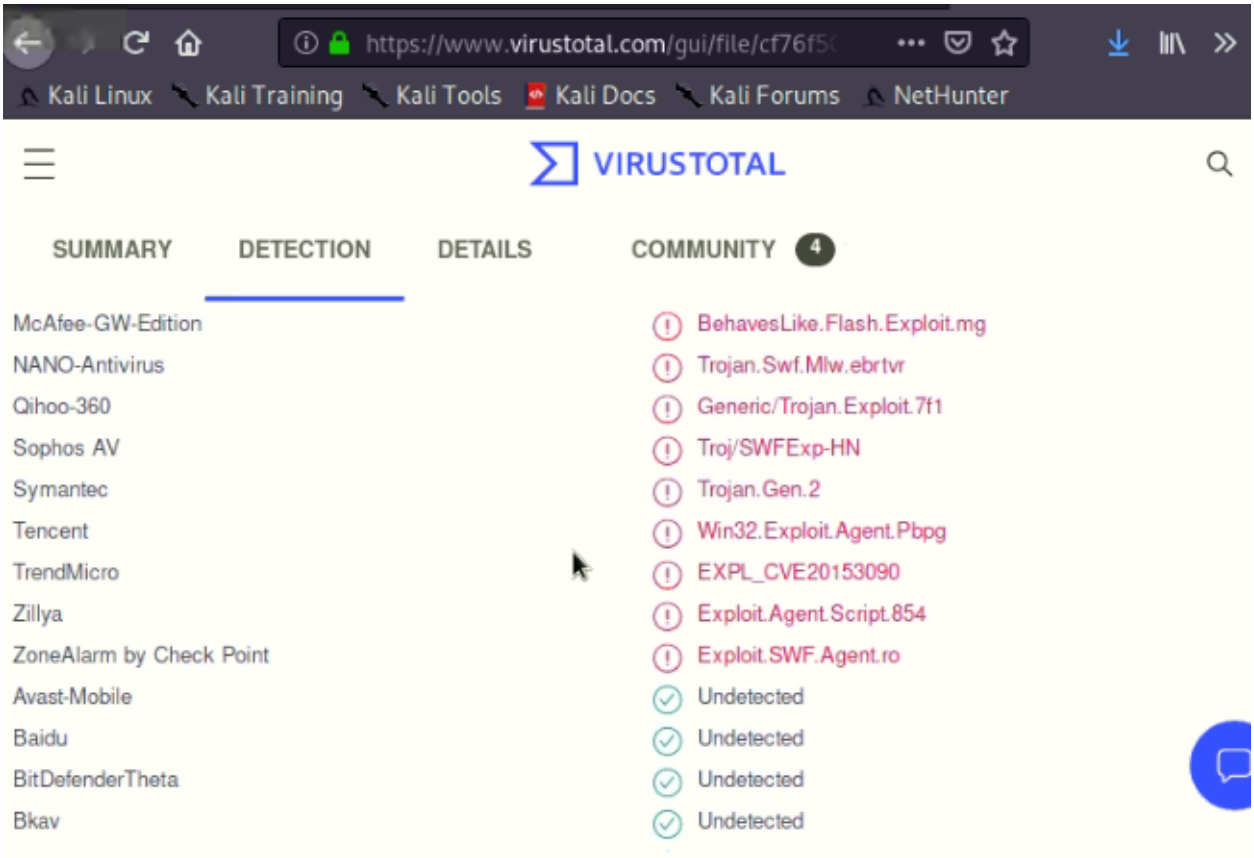
University of Victoria

University of Victoria

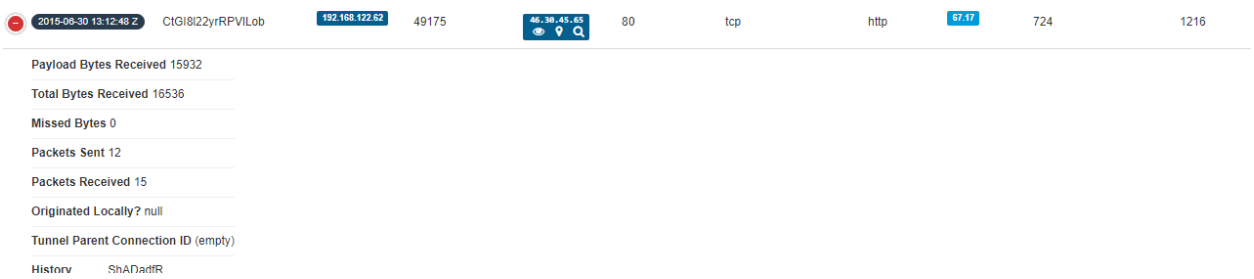


University of Victoria



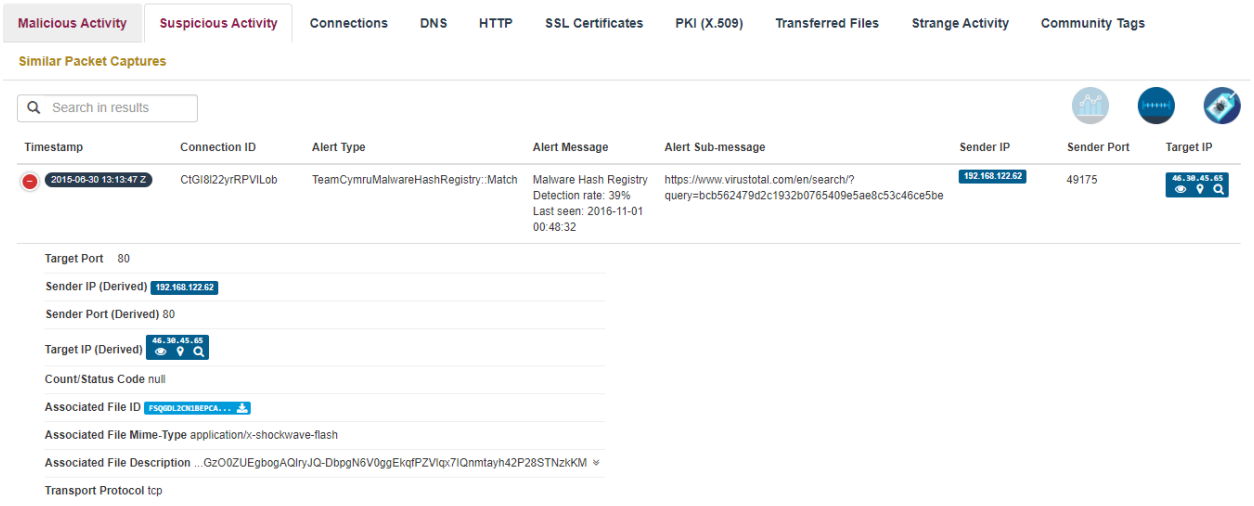


In the connections Tab of packet total, we can see that connection established between host and good.recycle2learn.com. The duration is 67:17 seconds on http. The screenshot as a follows:

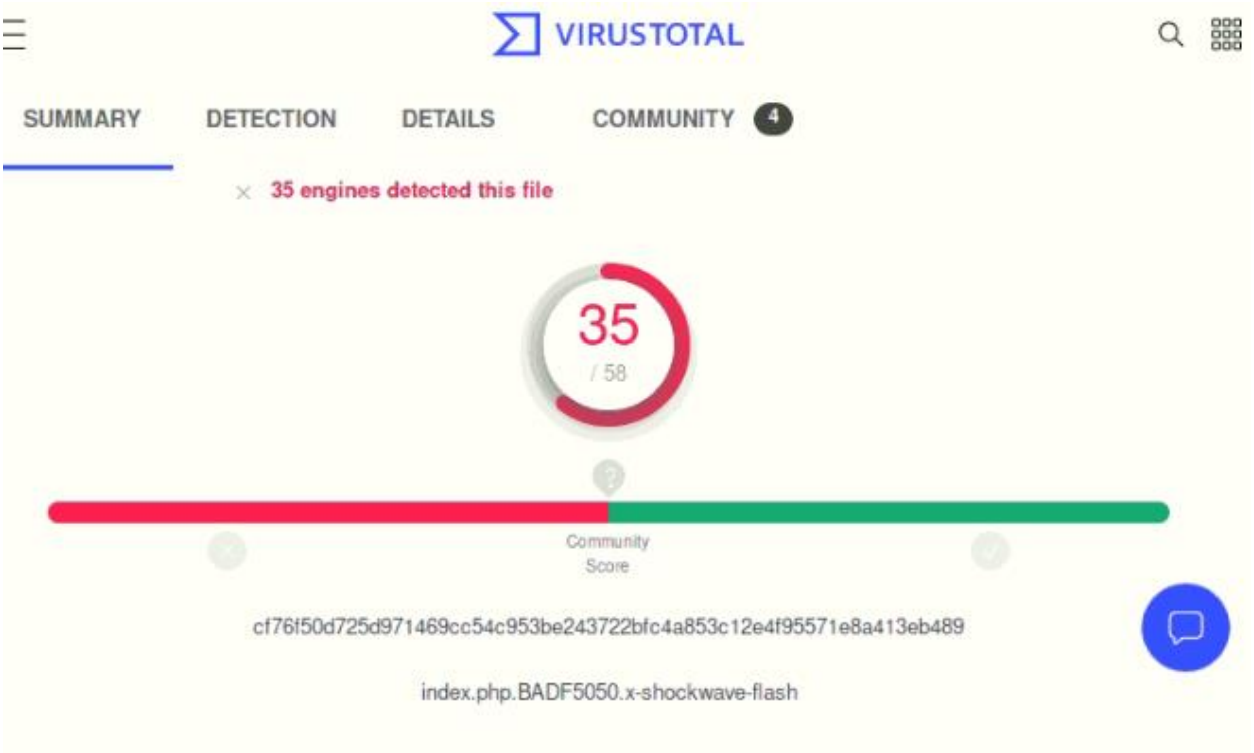


Finally, in packettotal, suspicious activity occurred at 13:12:47. Based on the report we found only one suspicious activity in this packet captured.

After downloading the file on this part, we upload this file to virustotal.com. And we found that 35 engines were detected. The screenshots are shown as a follows:



University of Victoria



University of Victoria

VIRUSTOTAL

SUMMARY | DETECTION | DETAILS | COMMUNITY 4

Ad-Aware	Script.SWF.Exploit.CVE-2015-3105.C500
AegisLab	Hacktool.SWF.Agent.3!c
AhnLab-V3	SWF/Exploit
ALYac	Script.SWF.Exploit.CVE-2015-3105.C500
Antiy-AVL	Trojan[Exploit]/SWF.SWF.Generic
Arcabit	Script.SWF.Exploit.CVE-2015-3105.C500
Avast	SWF:Malware-gen [Trj]
AVG	SWF:Malware-gen [Trj]
Avira (no cloud)	EXP/Agent.EB.48
BitDefender	Script.SWF.Exploit.CVE-2015-3105.C500
CAT-QuickHeal	SWF.Kit.Nuclear.N
ClamAV	Swf.Exploit.Kit-99
Comodo	Malware@#2iqyxbwc2cazk

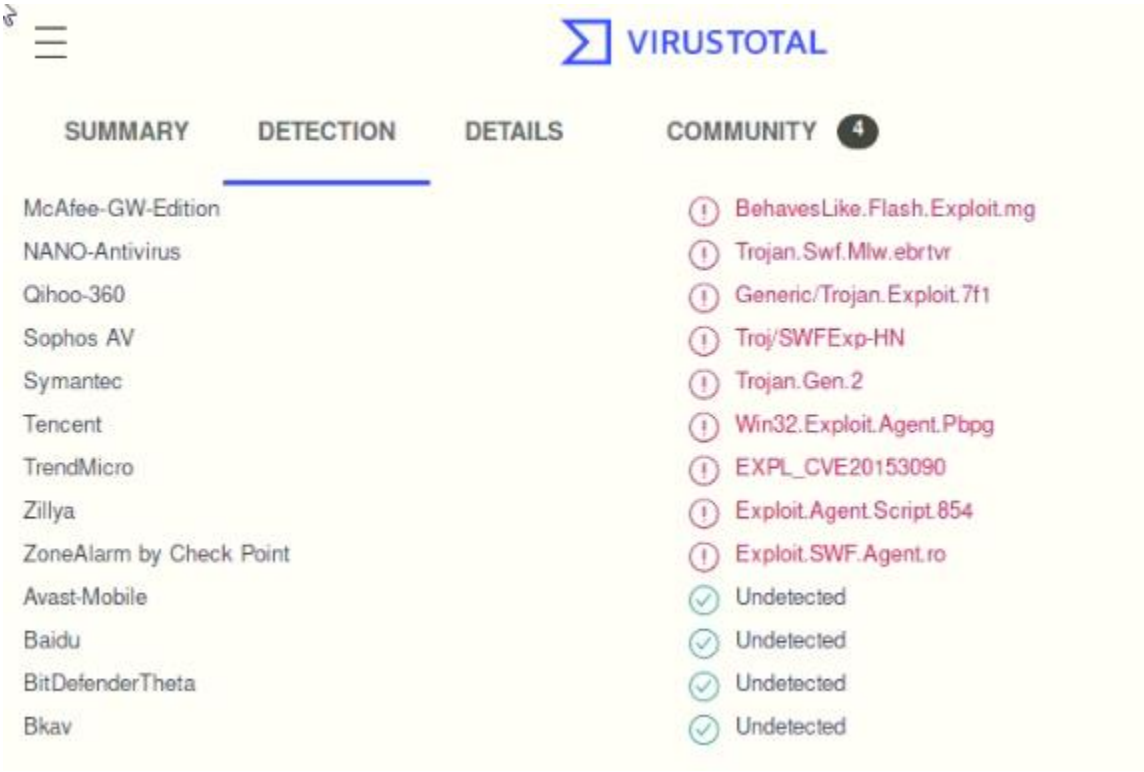
University of Victoria

VIRUSTOTAL

SUMMARY | DETECTION | DETAILS | COMMUNITY 4

Cyren	SWF/SWF/Exploit
DrWeb	Exploit.SWF.1232
Emsisoft	Script.SWF.Exploit.CVE-2015-3105.C500 (B)
eScan	Script.SWF.Exploit.CVE-2015-3105.C500
ESET-NOD32	SWF/Exploit.ExKit.AS
F-Prot	SWF/SWF/Exploit
F-Secure	Exploit.EXP/Agent.EB.48
FireEye	Script.SWF.Exploit.CVE-2015-3105.C500
GData	Script.SWF.Exploit.CVE-2015-3105.C500
Ikarus	Trojan.SWF.Exploit
Kaspersky	Exploit.SWF.Agent.ro
MAX	Malware (ai Score=100)
McAfee	SWF/Exploit-Rig.a

University of Victoria

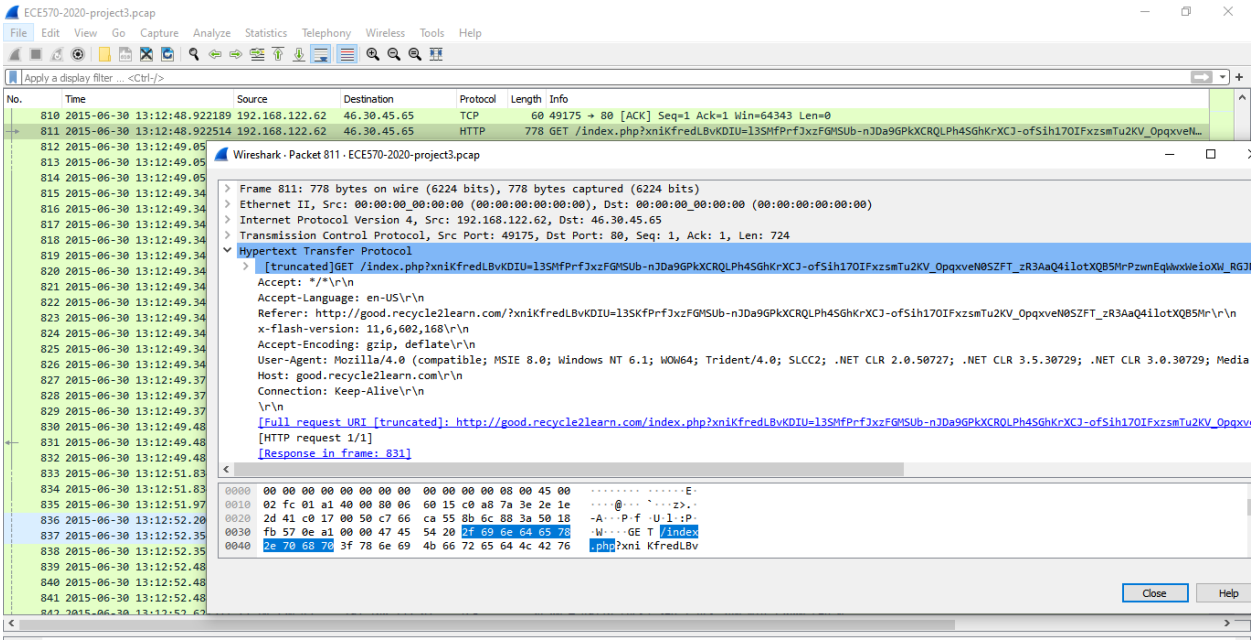


Note: all files transferred, packets are referred to www.floridablueline.com

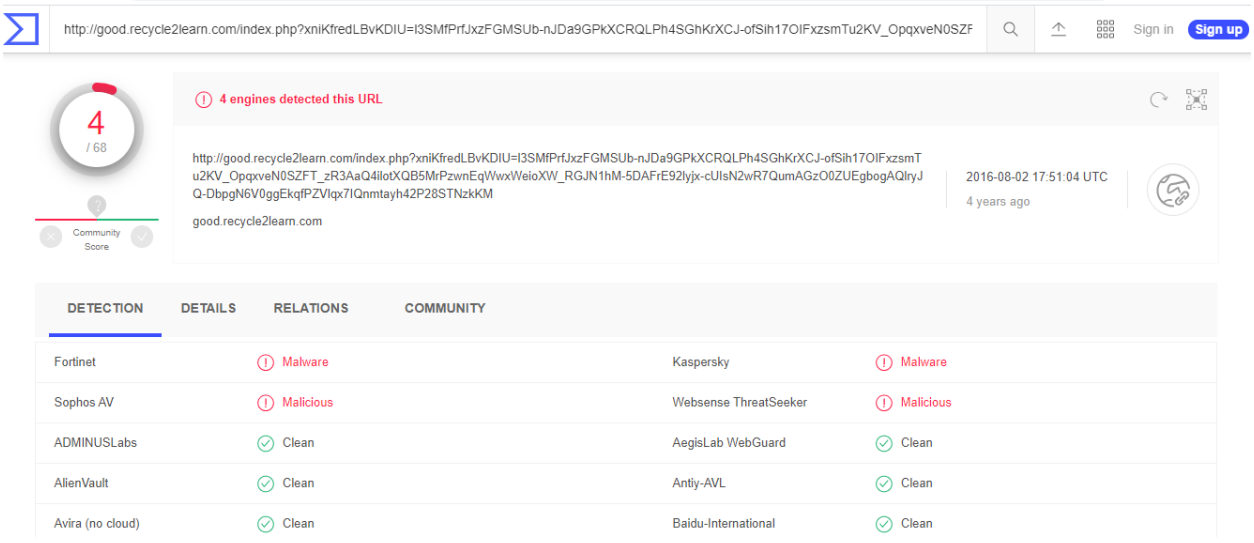
And also in this site, when the host infected www.good.recycled2learn.com then this site sent packet ACK to host 192.168.122.62.

According to wireshark capture file, when the host sent packet contains swf malware in frame 811, the website: www.good.recycle2learn.com responded 192.168.122.62 on packet 831. The weird difference is time. At 13:12:48 192.168.122.62 sent a request GET http to 46.30.45.65 after a seconds, in 13:12:49 the 46.30.45.65 sent HTTP1.1 to the host.

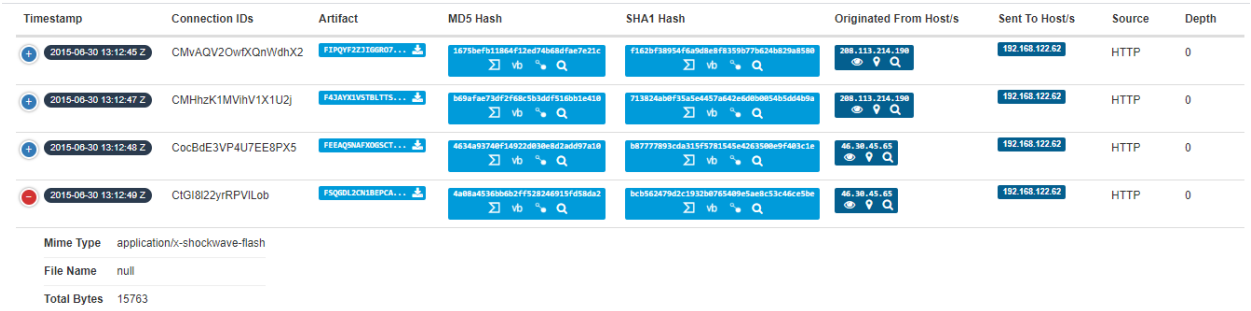
University of Victoria



Virustotal check of this URL that show in above picture indicates this URL is malware, shows as a follows:



In time 13:12:49 In Files Transferred of packettotal, the file shockwave-flash is shown as a following picture:



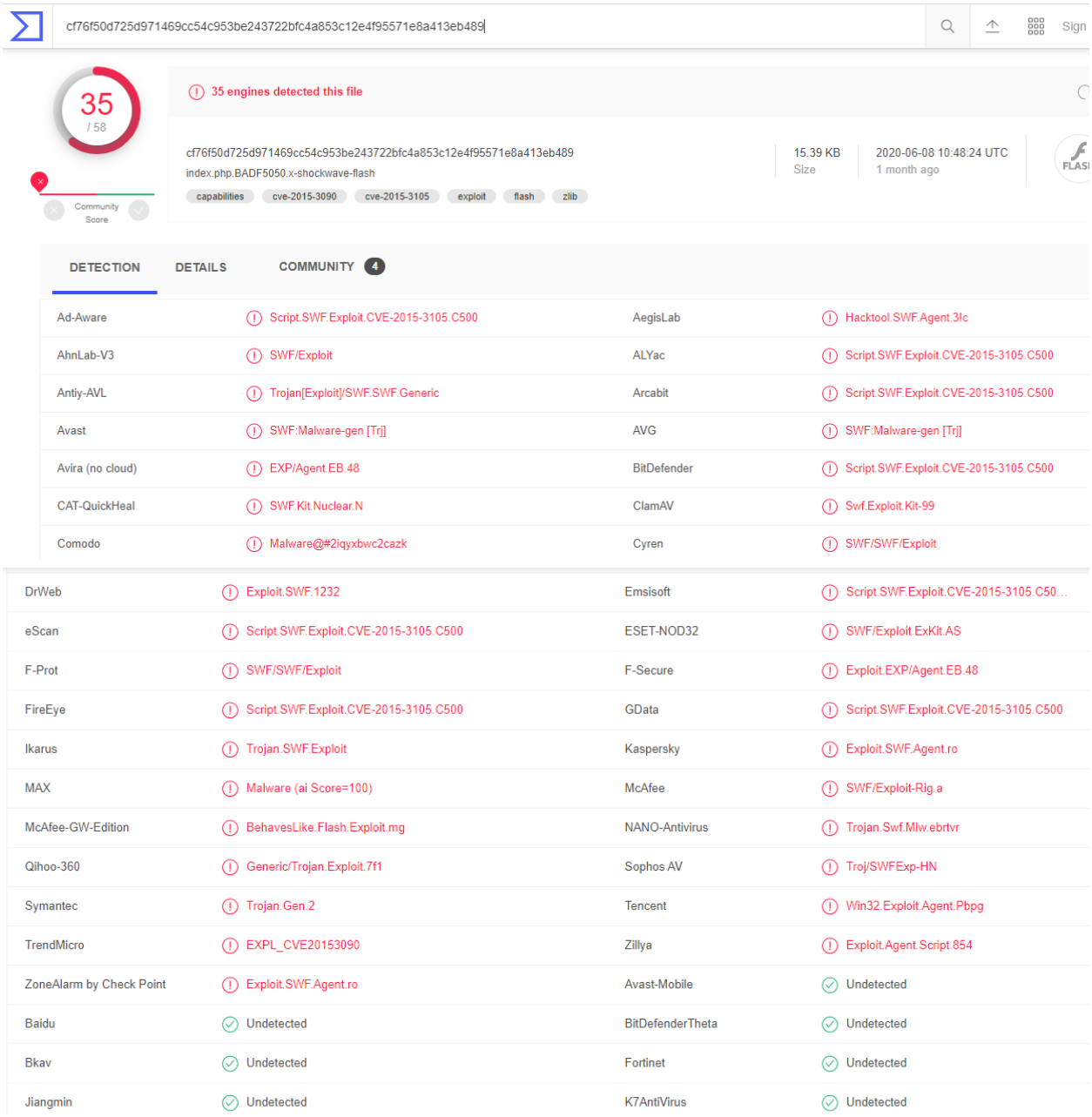
Timestamp	Connection IDs	Artifact	MD5 Hash	SHA1 Hash	Originated From Host/s	Sent To Host/s	Source	Depth
2015-06-30 13:12:45 Z	CMvAQV2OwfXQnWdhX2	FIPQYF2Z3I6GR07...	1675befb11864f12ed74b68dfae7e21c	f162bf38954f6a9d8e8f8359b77b624b829a8580	208.113.214.190	192.168.122.62	HTTP	0
2015-06-30 13:12:47 Z	CMHhzK1MVlhV1X1U2j	F4JAYX1V5TBLTT5...	b69afae73df2f68c5b3ddf516bb1e410	713824ab0f35a5e4457a642e6d0b0054b5dd4b9a	208.113.214.190	192.168.122.62	HTTP	0
2015-06-30 13:12:48 Z	CocBdE3VP4U7EE8PX5	FEEAQ5NAFXOGSCT...	4634a93748f14922d038e8d2add97a10	b87777893cda315f5781545e4263580e9f403c1e	46.30.45.65	192.168.122.62	HTTP	0
2015-06-30 13:12:49 Z	CtGI8I22yrRPVILob	F5Q6DL2CN1BEPCA...	4a88a4536bb6b2ff528246915fd58da2	bcb562479d2c1932b0765409e5ae8c53c46ce5be	46.30.45.65	192.168.122.62	HTTP	0

Mime Type	application/x-shockwave-flash
File Name	null
Total Bytes	15763

We know in frame 831 based on wireshark, between the website www.good.recycle2learn.com and 192.168.122.62 the HTTP connection established. And HTTP 1.1 200 OK.

After, click on virustotal.com lookup, the virustotal check shown as follows and 35 engines detected this file.

University of Victoria

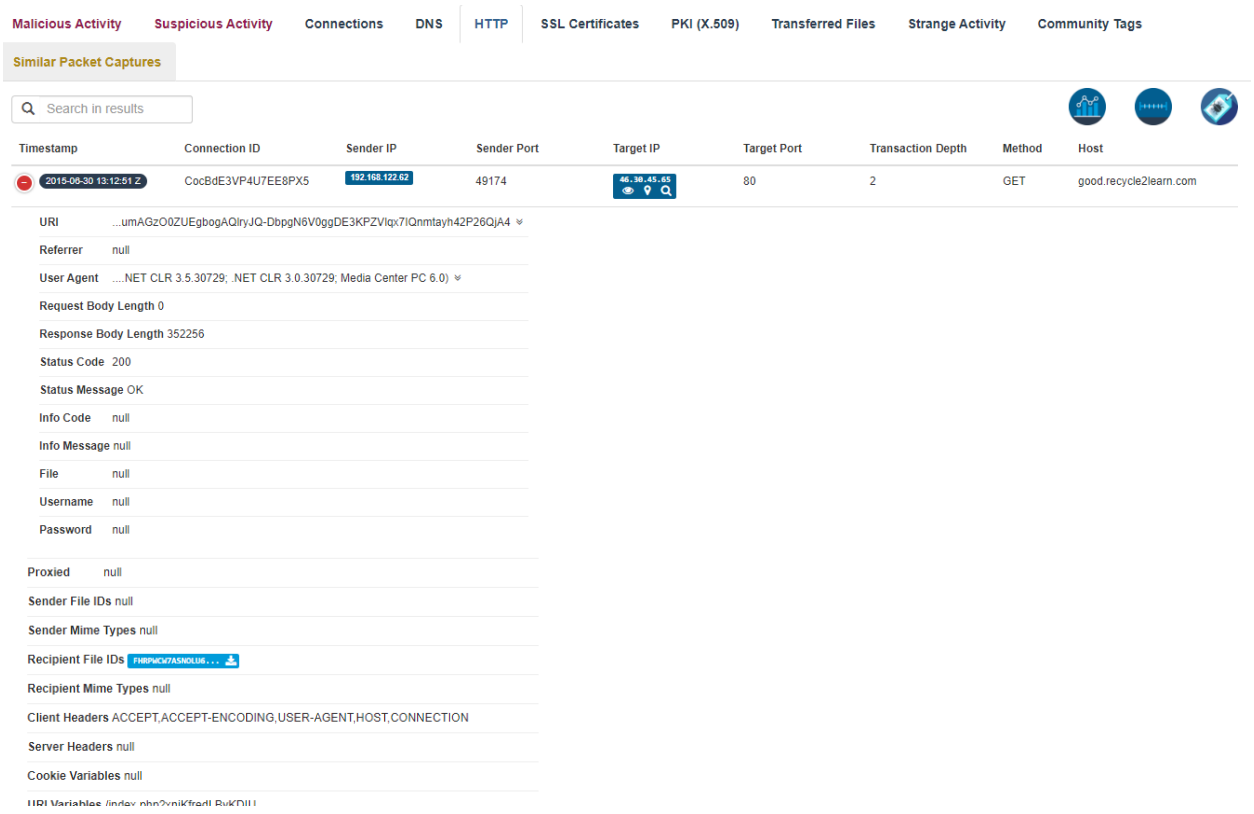


Compared with frame 811, at first the host sent HTTP requests to www.good.recycle2learn.com as a HTTP GET this file infected by 35 engines. And now

in frame 831 www.good.recycle2learn.com sent a file to the host. And this file is the same as before.Infected by 35 engines. We checked both files in Files Transfered of packet total.

After being infected www.good.recycle2learn.com by the host, two of them sent a lot of ACK together.

In time 13.12.51 based on packettotal report, HTTP Tab, we found an HTTP transaction between source IP which is host and target IP which is 46.30.45.65. The picture is as a follows:

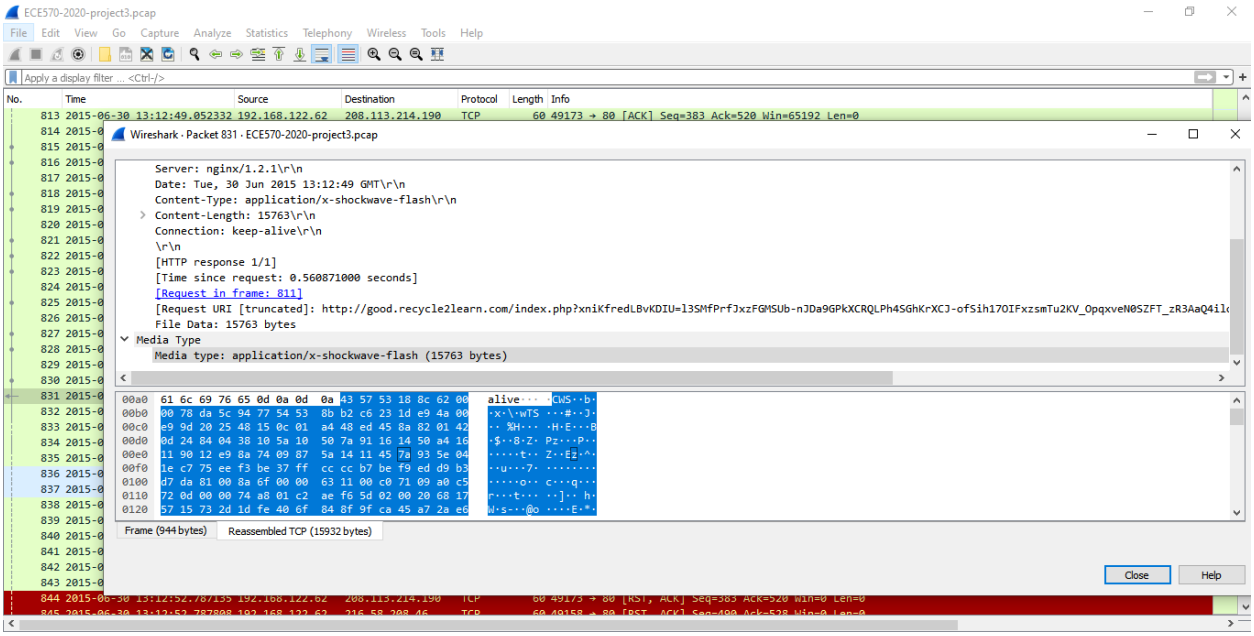


Base on virustotal report, this file contains four detected engines, the screen shot as a follows:

University of Victoria

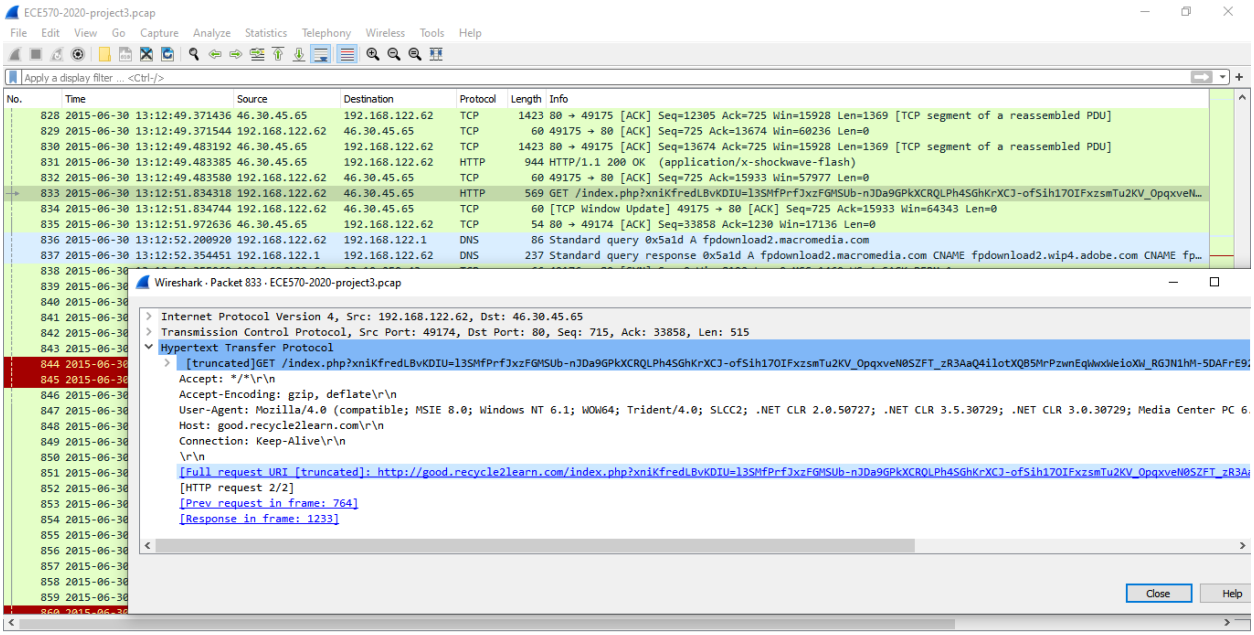
Based on the wireshark report, frame 831 indicates that include media type. Application/X-shockwave flash.

University of Victoria

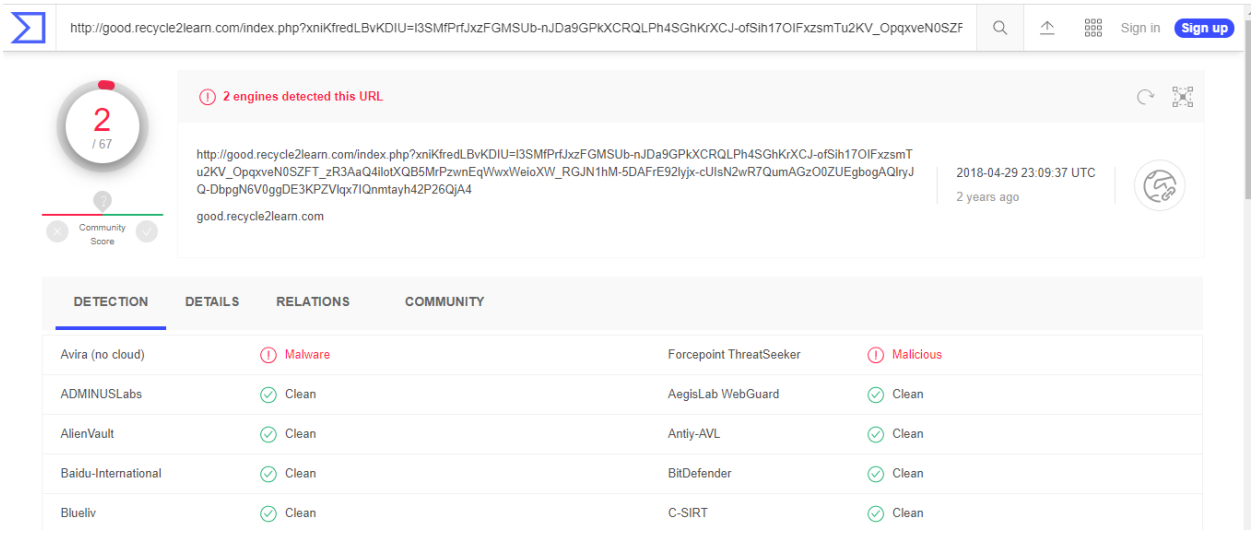


Based on wireshark in frame 833 the GET HTTP request between 192.168.122.62 and 46.30.45.65 start.

University of Victoria



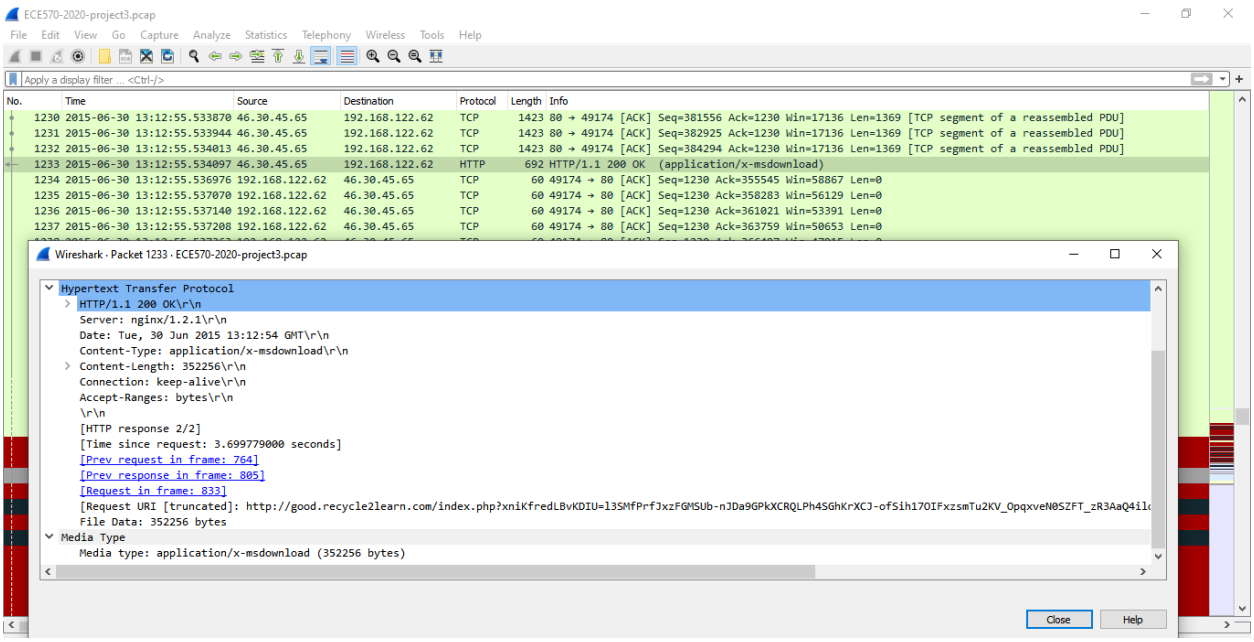
The URL of above screenshot related to scripts that GET on virustotal check indicates this script is malware. The screen shot as a follows:



And also, we recognized that this frame was requested in frame 764. Moreover, the response of this request (frame 833) will be in frame 1233.

So, we will check frame 1233.

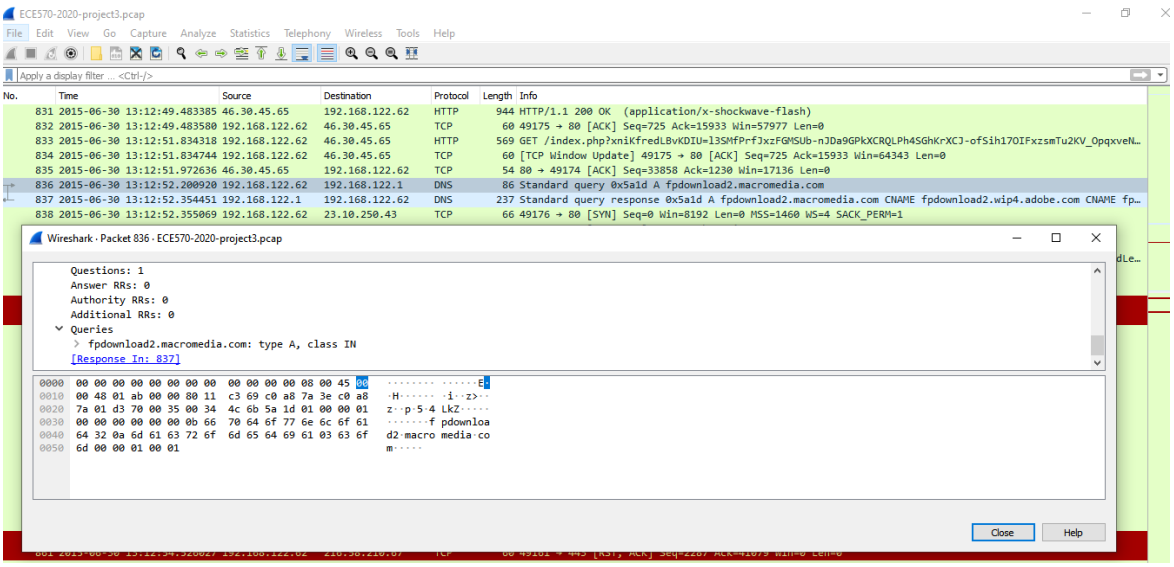
In frame 1233, application/x-msdownload is HTTP 200 OK. This frame response of frame 833 request.



In addition, this frame time at 13:12:55.

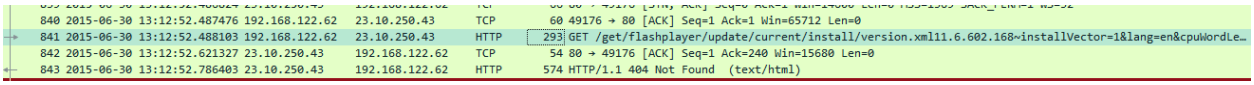
In frame 836, one request from the host windows machine to DNS sent for fpdownload.macromedia.com and response on frame 837.

University of Victoria



After TCP handshaking in frame 841 GET flash player from IP 23.10.250.43

But in frame 843 HTTP response 404 Not found



We check DNS in the packet total at the same time of this transfer.

University of Victoria

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	Transaction ID	Query
2015-06-30 13:12:52 Z	CKdhc21h1h9kqH5m2g	192.168.122.62	54128	192.168.122.1	53	udp	23069	fpdownload2.macromedia.com

Query Class Desc C_INTERNET
Query Type 1
Query Type Desc A
Response Code 0
Response Code Desc NOERROR
Authoritative Answer? F
Truncated? F
Recursion Desired? T
Recursion Available? T
Answers fpdownload2.wip4.adobe.com,fpdownload.macromedia.com.edgesuite.net,a1293.d.akamai.net,23.10.250.43,23.10.250.18
TTLs 21078.000000,119.000000,21232.000000,19.000000,19.000000
Authoritative Response null
Additional Response(s) null

HTTP in packet total checked. We found that at this time 13:12:51 and 13:12:52 we have tow information.

Malicious Activity | Suspicious Activity | Connections | DNS | HTTP | SSL Certificates | PKI (X.509) | Transferred Files | Strange Activity | Community Tags

Similar Packet Captures

Search in results

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transaction Depth	Method	Host
2015-06-30 13:12:51 Z	CocBdE3VP4U7EE8PX5	192.168.122.62	49174	46.30.45.65	80	2	GET	good.recycle2learn.com
2015-06-30 13:12:52 Z	CtOXLI293JVZ3Ot68h	192.168.122.62	49176	23.10.250.43	80	1	GET	fpdownload2.macromedia.com
2015-06-30 13:12:55 Z	CALygR1JnJXOgNnETj	192.168.122.62	49171	192.254.234.118	80	3	GET	www.floridablueline.com

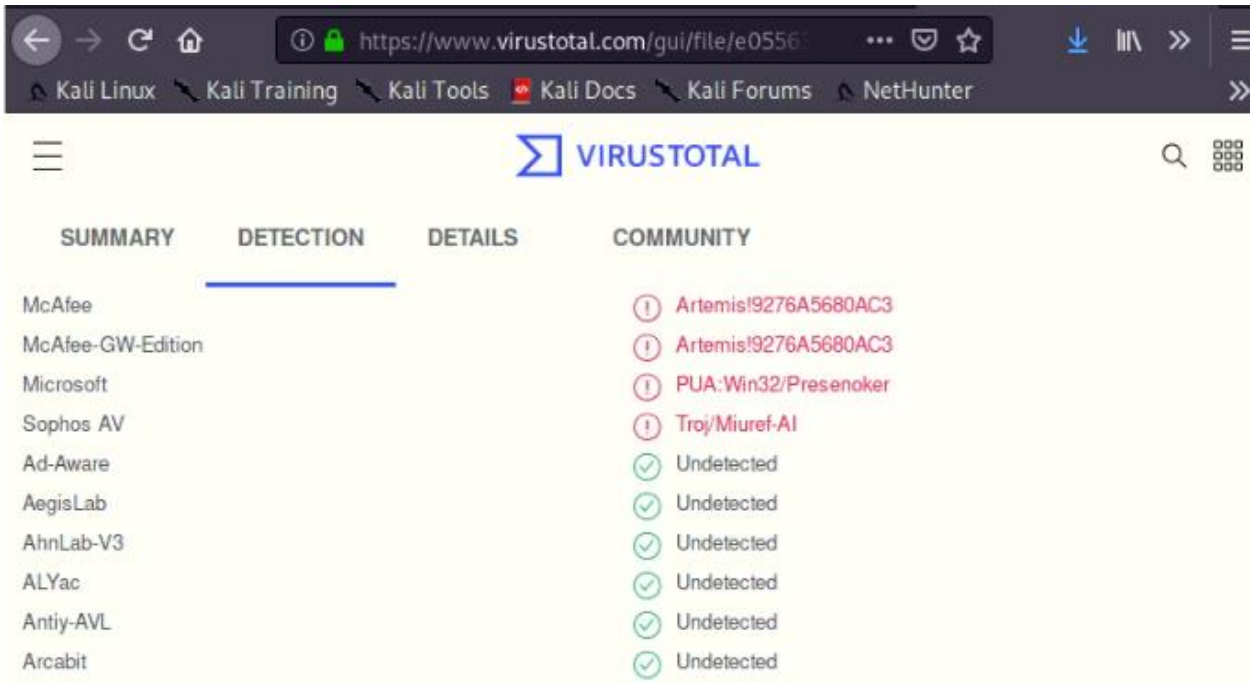
The first one occurs at 13:12:51 and contains one file. In this file 192.168.122.62 as a sender and 46.30.45.65 is as a target on host that is good.recycle2learn.com

University of Victoria

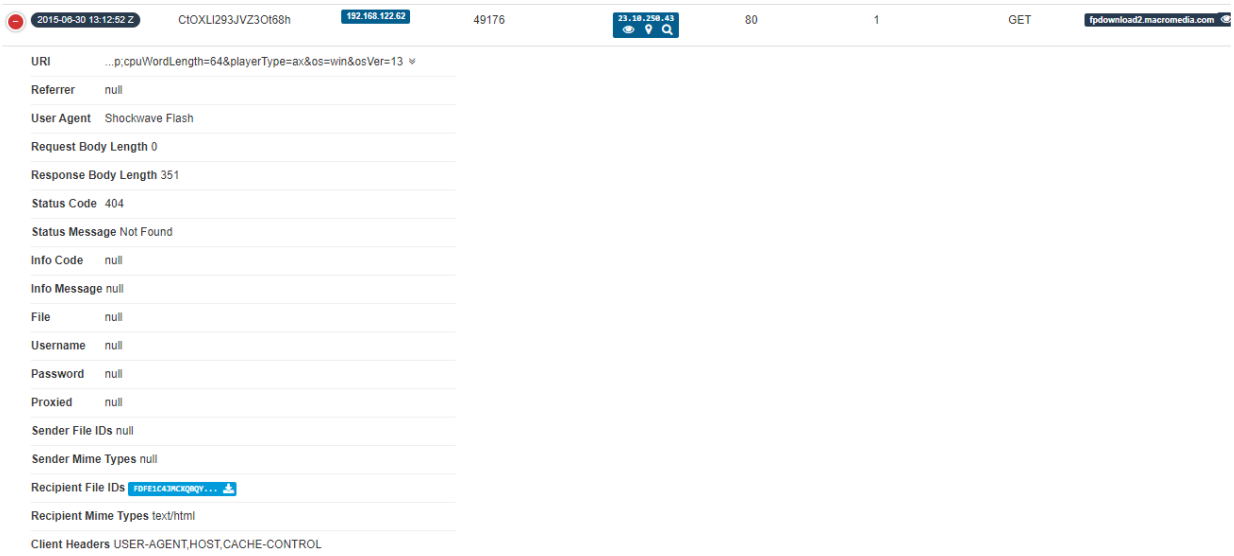
2015-08-30 13:12:51 Z	CocBdE3VP4U7EE8PX5	192.168.122.62	49174	46.30.45.65	80	2	GET	good.recycle2learn.com

URI	...umAGzO0ZUEgbogAQlryJQ-DbpgN6V0ggDE3KPZVlqx7lQnmtayh42P26QjA4
Referrer	null
User Agent	....NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
Request Body Length	0
Response Body Length	352256
Status Code	200
Status Message	OK
Info Code	null
Info Message	null
File	null
Username	null
Password	null
Proxied	null
Sender File IDs	null
Sender Mime Types	null
Recipient File IDs	FH8PWCH7ASNOLU6...
Recipient Mime Types	null
Client Headers	ACCEPT,ACCEPT-ENCODING,USER-AGENT,HOST,CONNECTION
Server Headers	null
Cookie Variables	null

When we downloaded this file and checked it on vius total we found that this file is malware.

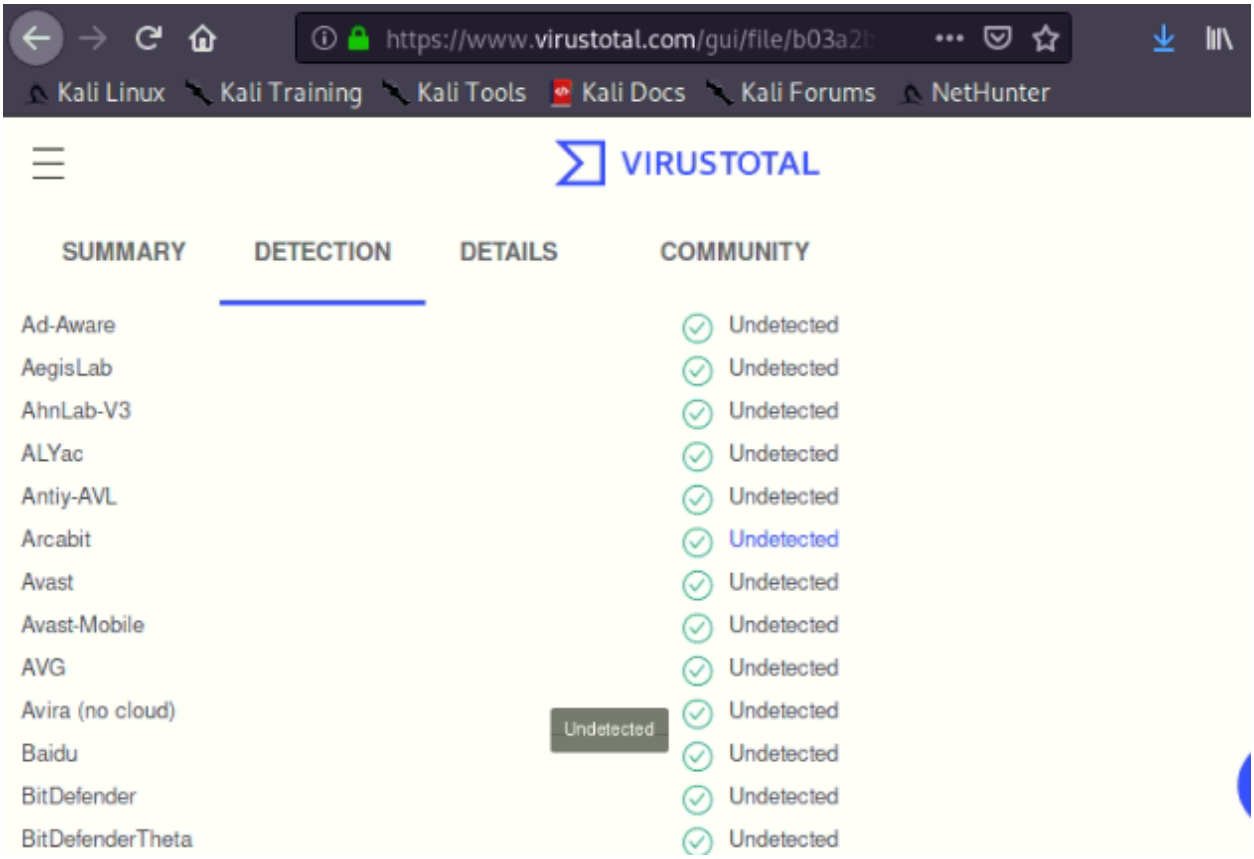


The first one occurs at 13:12:52 and contains one file and contains one file. In this file 192.168.122.62 as a sender and 46.30.45.65 is as a target on host that is fpdownload2.macromedia.com

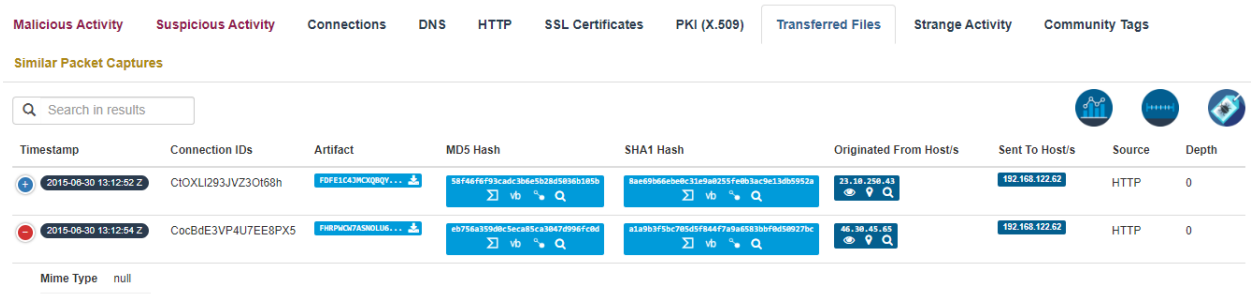


When we downloaded this file and checked it on vius total we found that this file is clean.

University of Victoria

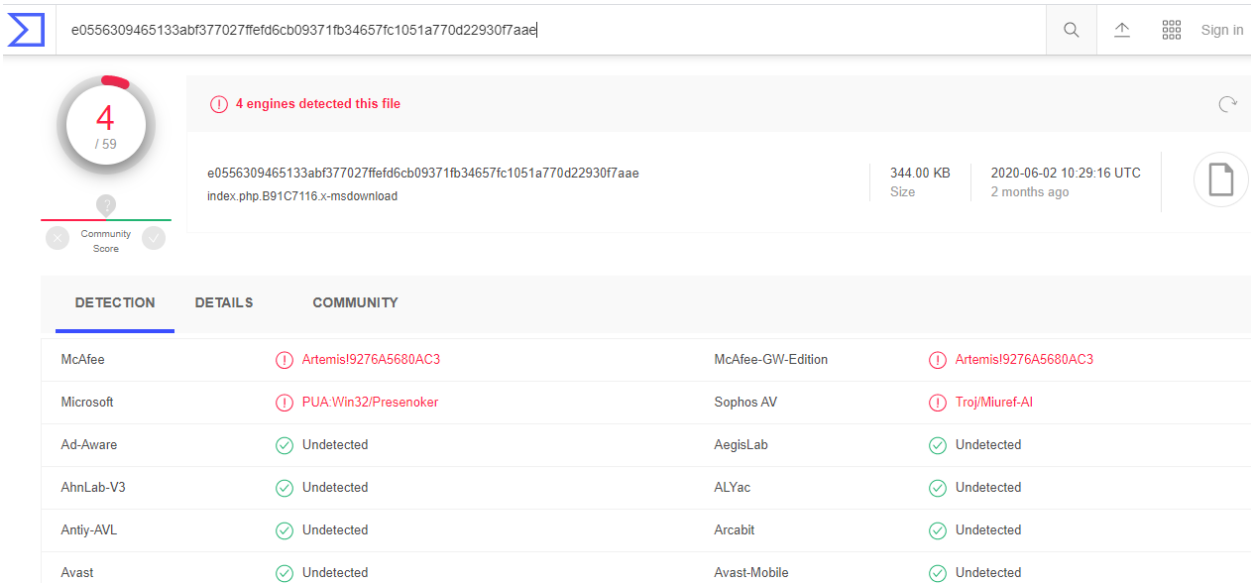


And also, in Transferred Files we have one transfer packets at the time 13:12:45



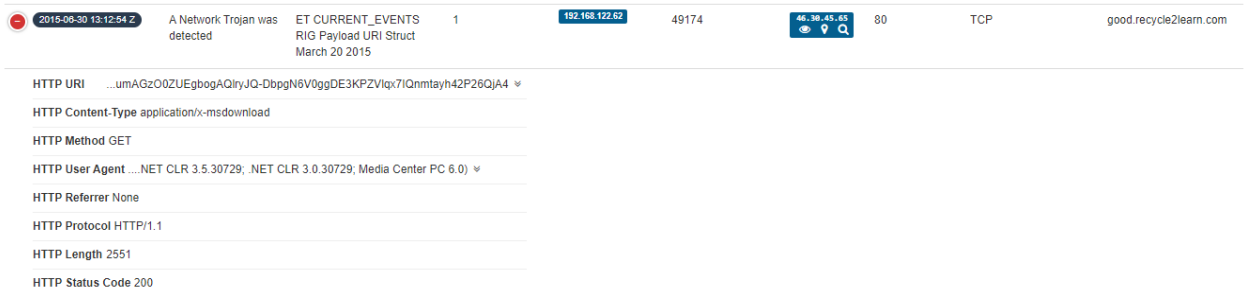
Lookup this file in virustotal indicates that 4 engines detected this file.

University of Victoria



Based on Malicious activity report on packet total, two report occurs at 13:12:54

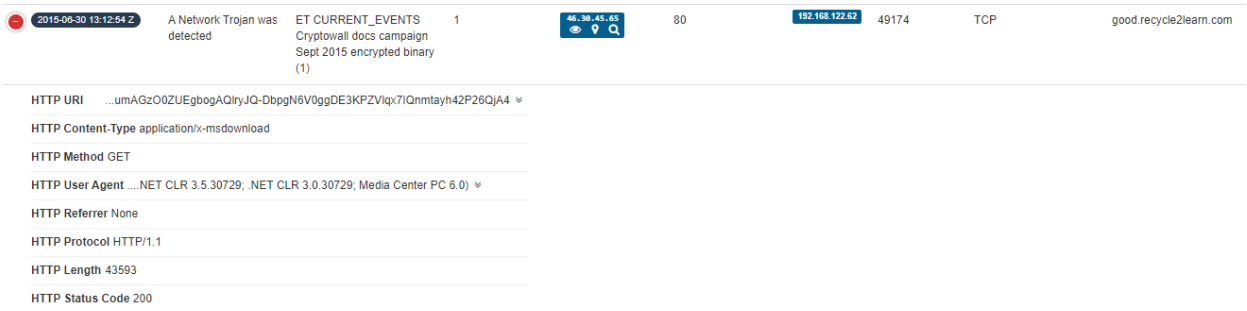
The first alert is ET CURRENT_EVENTS RIG Payload URI Struct March 20 2015. This alert is related to good.recycle2learn.com and occurs at 13:12:54. **HTTP Content-Type** application/x-msdownload. And also between host and good.recycle2learn.com.



University of Victoria

For the past year, Rig EK has been using Flash exploits based on CVE-2018-8174 as noted in this May 2018 blog post from @kafeine. Since then, other sources have reported Rig EK delivering a variety of malware like the Grobios Trojan or malware based on a Monero cryptocurrency miner. Like other EKs, Rig EK is most often used in malvertising distribution campaigns. In today's infection, Rig EK delivered AZORult, and the infection followed-up with other malware I was unable to identify.

The last alert is ET CURRENT_EVENTS Cryptowall docs campaign Sept 2015 encrypted binary. This alert is related to good.recycle2learn.com and occurs at 13:12:54. **HTTP Content-Type** application/x-msdownload. And also between good.recycle2learn.com and host.



CryptoWall is a family of file-encrypting Ransomware that first appeared in early 2014. It is notable for its use of unbreakable AES encryption, unique CHM infection mechanism, and robust C2 activity over the Tor anonymous network. The miscreants running the CryptoWall operation also provide a free single-use decryption service to prove they hold the keys necessary to restore the hijacked files.

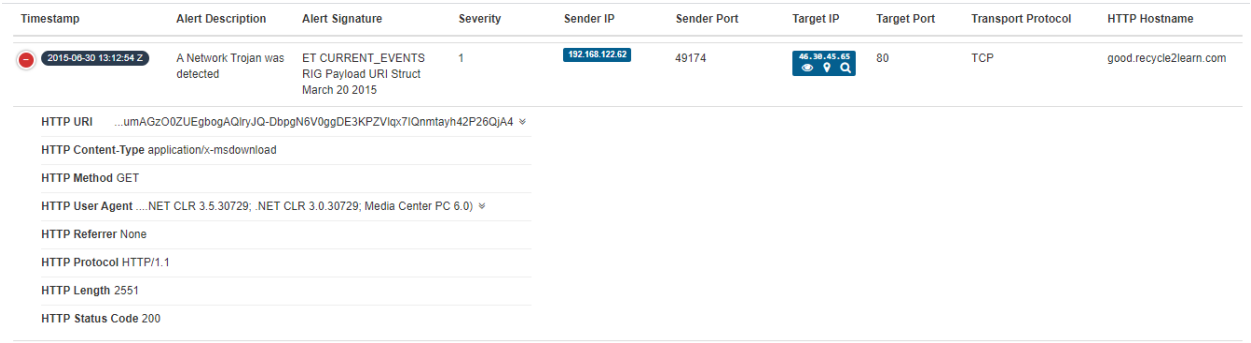
So, the website www.good.recycle2learn.com with IP address 46.30.45.65 is the site that delivered the Malware and ransomware that explain completely on question 4.

University of Victoria

4. Identify the type of malware involved and check the payload by running the associated file (or files) against an online virus checker (i.e. VirusTotal).

According to the packet total report on Malicious activity. Two activities occur at time 13:12:54 which have an alert for network trojan .All two alerts explain separately. The screen shots are in following pictures:

The first alert is ET CURRENT_EVENTS RIG Payload URI Struct March 20 2015.



Timestamp	Alert Description	Alert Signature	Severity	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	HTTP Hostname
2015-08-30 13:12:54 Z	A Network Trojan was detected	ET CURRENT_EVENTS RIG Payload URI Struct March 20 2015	1	192.168.122.62	49174	46.30.45.65	80	TCP	good.recycle2learn.com

HTTP URI ...umAGzO0ZUEgbogAQlryJQ-DbpgN6V0ggDE3KPZVIqx7lQnmtayh42P26QjA4
HTTP Content-Type application/x-msdownload
HTTP Method GET
HTTP User Agent ....NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
HTTP Referrer None
HTTP Protocol HTTP/1.1
HTTP Length 2551
HTTP Status Code 200

For the past year, Rig EK has been using Flash exploits based on CVE-2018-8174 as noted in this May 2018 blog post from @kafeine. Since then, other sources have reported Rig EK delivering a variety of malware like the Grobios Trojan or malware based on a Monero cryptocurrency miner. Like other EKs, Rig EK is most often used in malvertising distribution campaigns. In today's infection, Rig EK delivered AZORult, and the infection followed-up with other malware I was unable to identify.

The second alert is ET CURRENT_EVENTS Cryptowall docs campaign Sept 2015 . encrypted binary (1).

University of Victoria

Timestamp	Alert Description	Alert Signature	Severity	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	HTTP Hostname
2015-06-30 13:12:54 Z	A Network Trojan was detected	ET CURRENT_EVENTS Cryptowall docs campaign Sept 2015 encrypted binary (1)	1	46.30.45.65	80	192.168.122.62	49174	TCP	good.recycle2learn.com

HTTP URI ...umAGzO0ZUEgbogAQlryJQ-DbpgN6V0ggDE3KPZVlqx7IQnmtayh42P26QjA4
HTTP Content-Type application/x-msdownload
HTTP Method GET
HTTP User Agent ....NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
HTTP Referrer None
HTTP Protocol HTTP/1.1
HTTP Length 43593
HTTP Status Code 200

CryptoWall is a family of file-encrypting Ransomware that first appeared in early 2014. It is notable for its use of unbreakable AES encryption, unique CHM infection mechanism, and robust C2 activity over the Tor anonymous network. The miscreants running the CryptoWall operation also provide a free single-use decryption service to prove they hold the keys necessary to restore the hijacked files.

In Connections Tab of packet total we found information based on time after 13:12:54.

Malicious Activity | Suspicious Activity | Connections | DNS | HTTP | SSL Certificates | PKI (X.509) | Transferred Files | Strange Activity | Community Tags

Similar Packet Captures

Search in results

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	Service	Duration	Payload Bytes Sent	Total Bytes Sent
2015-06-30 13:12:45 Z	CMvAQV2Ow0XQnWdhX2	192.168.122.62	49172	208.113.254.199	80	tcp	http	2.55	378	630
2015-06-30 13:12:45 Z	CR9x6sdRdQ0MDUCG8	192.168.122.62	54137	192.168.122.1	53	udp	dns	0.31	37	65
2015-06-30 13:12:46 Z	CMHhzK1MVthV1X1U2j	192.168.122.62	49173	208.113.254.199	80	tcp	http	6.55	382	634
2015-06-30 13:12:47 Z	Cf09Oe4APdPX0dSMLI	192.168.122.62	59978	192.168.122.1	53	udp	dns	0.14	40	68
2015-06-30 13:12:47 Z	CocBdE3VP4U7EE8PX5	192.168.122.62	49174	46.30.45.65	80	tcp	http	59.70	1229	7601
2015-06-30 13:12:48 Z	CKi8l22yrRPVILob	192.168.122.62	49175	46.30.45.65	80	tcp	http	57.17	724	1216
2015-06-30 13:12:52 Z	CKdhc21h1h9kqH5m2g	192.168.122.62	54128	192.168.122.1	53	udp	dns	0.13	44	72
2015-06-30 13:12:52 Z	CtOXLI293JVZ3Ot68h	192.168.122.62	49176	23.10.250.45	80	tcp	http	63.60	239	451
2015-06-30 13:13:14 Z	CqnGqD4OYTuQ3Bn3Wa	192.168.122.62	49177	45.225.10.217	443	tcp	null	0.29	0	52

Both parts are explained step by step.

University of Victoria

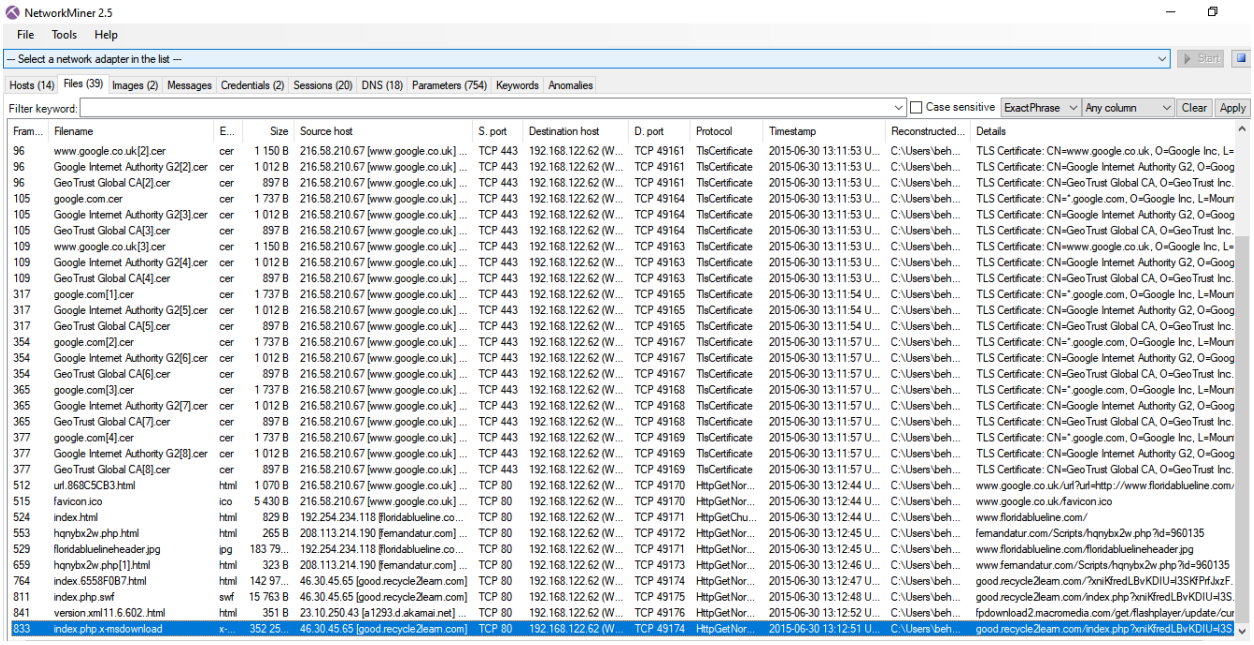
2015-06-30 13:12:52 Z	CKdhc21h1h9kqH5m2g	192.168.122.62	54128	192.168.122.1	53	udp	dns	0.15	44	72

Payload Bytes Received 195
Total Bytes Received 223
Missed Bytes 0
Packets Sent 1
Packets Received 1
Originated Locally? null
Tunnel Parent Connection ID (empty)
History Dd

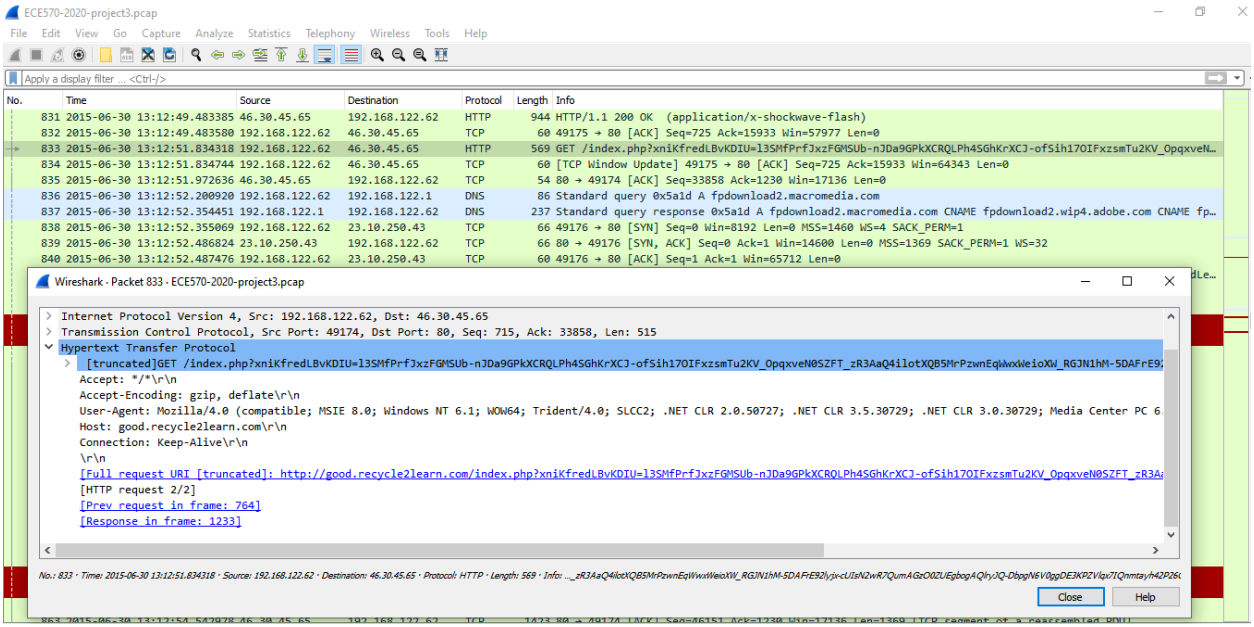
2015-06-30 13:12:52 Z	CtOXLI293JVZ3Ot68h	192.168.122.62	49176	23.10.250.43	80	tcp	http	63.60	239	451

Payload Bytes Received 520
Total Bytes Received 652
Missed Bytes 0
Packets Sent 5
Packets Received 3
Originated Locally? null
Tunnel Parent Connection ID (empty)
History ShADadR

Based on the Networkminer report, from 13:12:51 to 13:12:55 we have two frames that transfer a file in network.



One is x-msdownload on frame 833 at 13:12:51. And the other is index.php.swf is a macromedia flash player on frame 841 at 13:12:53. Networkminer helps to find a frame number. So, based on frame number the capture in wireshark is as follows:

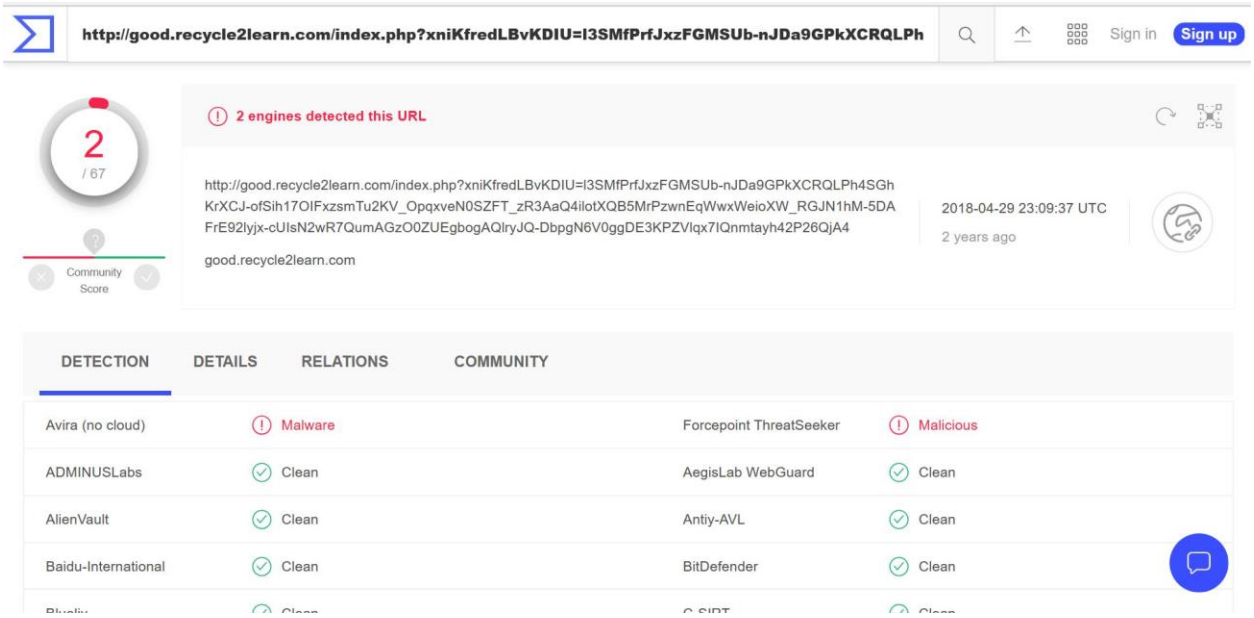


Frame 833, host machine(192.168.122.62) sent GET HTTP request to 46.30.45.65 . Based on frame details this frame is requested from frame 764 previously and will be responded to in 1233.

We checked the URL in virus total and found this URL is malware and malicious.

http://good.recycle2learn.com/index.php?xniKfredLBvKDIU=l3SMfPrfJxzFGMSUb-nJDa9GPkXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_OpqxveN0SZFT_zR3AaQ4ilotXQB5MrPzwnEqWwxWeioXW_RGJN1hM-5DAFrE92lyjx-cUIsN2wR7QumAGzO0ZUEgbogAQlryJQ-DbpgN6V0ggDE3KPZVlqx7IQnmtayh42P26QjA4

University of Victoria

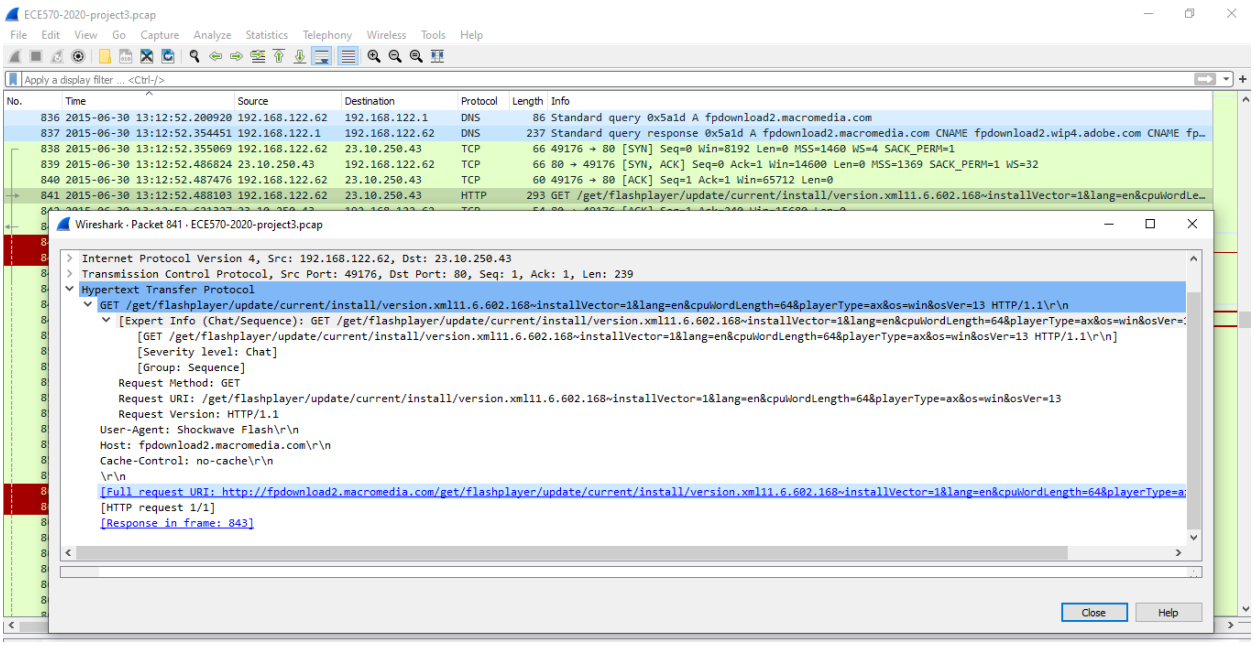


The IP address of this site (www.good.recyvle2learn.com) checked in ipvoid.com to know about situation

University of Victoria

Analysis Date	2020-07-31 00:21:17
Elapsed Time	2 seconds
Blacklist Status	BLACKLISTED 1/114
IP Address	**46.30.45.65** Find Sites | IP Whois
Reverse DNS	serv1.abitec.ru
ASN	AS210079
ASN Owner	EuroByte LLC
ISP	EuroByte LLC
Continent	Europe
Country Code	(RU) Russia
Latitude / Longitude	55.7386 / 37.6068 Google Map
City	Unknown

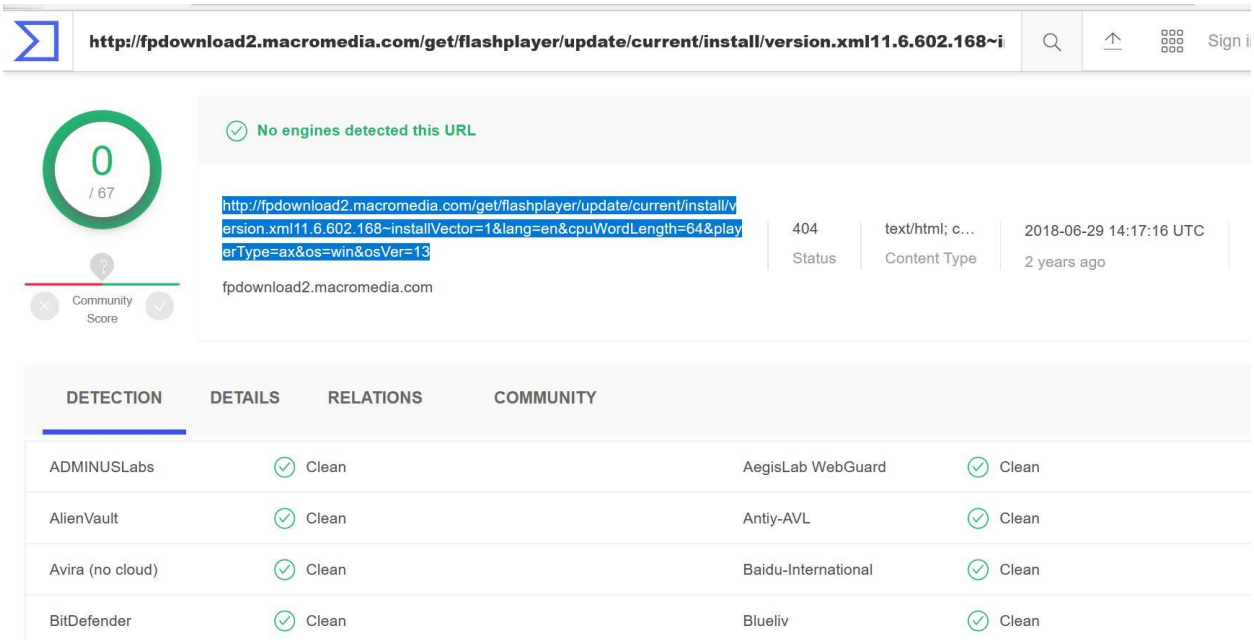
In packet 841



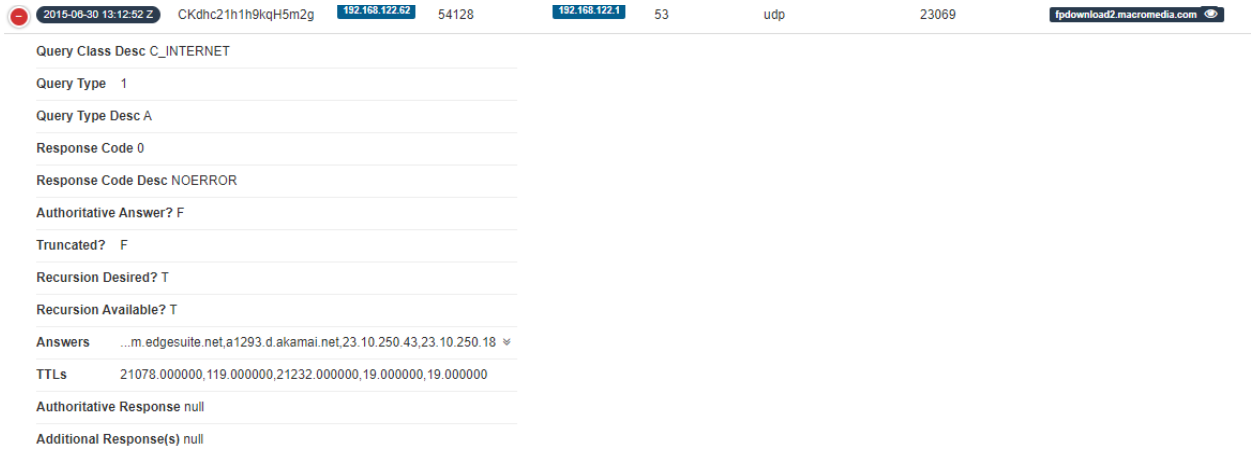
User agent here is shockwave flash which we found it malicious with 35 engines in packet 831, host is fpdownload, which is some kind of upgrading the flash player.

URL :http://fpdownload2.macromedia.com/get/flashplayer/update/current/install/version.xml11.6.602.168~installVector=1&lang=en&cpuWordLength=64&playerType=ax&os=win&osVer=13

University of Victoria



In another Tab DNS we found a little information



.

University of Victoria

In the context of a cyber-attack, a payload is the component of the attack which causes harm to the victim. Much like the Greek soldiers hiding inside the wooden horse in the tale of the Trojan Horse, a malicious payload can sit harmlessly for some time until triggered.

Attackers must first find a method to deliver the malicious payload onto the victim's computer. DNS hijacking is a common example of payload delivery techniques.
Once a payload is in place, it will usually sit dormant until being executed. An attacker can select from many different ways to execute a malicious payload. Some common ways to execute a malicious payload:
Opening an executable file: For example a victim downloads an email attachment that they believe to be a piece of pirated software and they double-click on the installation file which executes the payload.
Setting off a specific set of behavioral conditions: This is known as a logic bomb. For example, an unscrupulous employee might integrate a logic bomb into his company's network that continually checks to see if that employee is still on the payroll. When he is no longer on the payroll, the logic bomb will meet its condition and the malicious payload will be executed.
Opening certain non-executable files: Even some non-executable files can contain malicious payloads. For example there are attacks where malicious payloads are hidden in .PNG image files. When a victim opens these image files, the payload is executed.

So, we export both HTTP and FILES TRANSFER from the packet total.

HTTP payload
page1

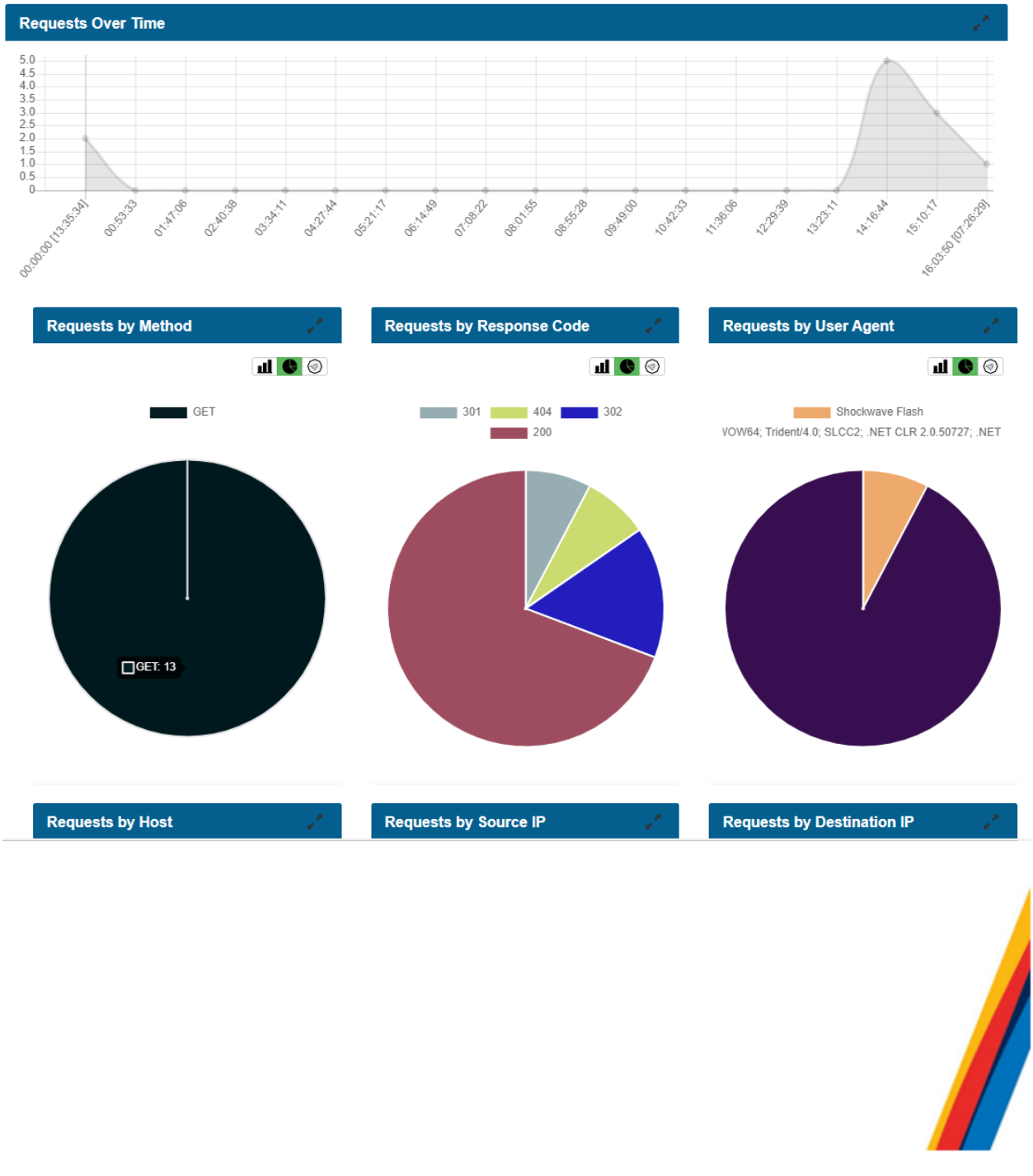
Timestamp	Connectic	Sender IP	Sender Pc	Target IP	Target Port	Transactic	Meth	Host	URI	Referrer	User Agent	Request B	Response
2015-06-30 13:11:51 Z	Cs8Y2Q2yi	192.168.122.62	49158	216.58.208.46	80	1	GET	google.comÂ	/	null	....NET CLR 3.5.3(	0	261
2015-06-30 13:11:51 Z	CMuHRQ3	192.168.122.62	49159	216.58.210.67	80	1	GET	www.google.co.ukÂ	/?gfe_rd=cr&ei=l5WSVaXXFr	null	....NET CLR 3.5.3(	0	277
2015-06-30 13:12:44 Z	CIFU4P2T(	192.168.122.62	49170	216.58.210.67	80	1	GET	www.google.co.ukÂ	...amp;ved=0CBQQFjAA&usg	null	....NET CLR 3.5.3(	0	1070
2015-06-30 13:12:44 Z	CIFU4P2T(	192.168.122.62	49170	216.58.210.67	80	2	GET	www.google.co.ukÂ	/favicon.ico	null	....NET CLR 3.5.3(	0	5430
2015-06-30 13:12:44 Z	CALygR1Jr	192.168.122.62	49171	192.254.234.118	80	1	GET	www.floridablueline.comÂ	/	...amp;ved	....NET CLR 3.5.3(	0	829
2015-06-30 13:12:45 Z	CALygR1Jr	192.168.122.62	49171	192.254.234.118	80	2	GET	www.floridablueline.comÂ	/floridabluelineheader.jpg	http://ww	....NET CLR 3.5.3(	0	183799
2015-06-30 13:12:45 Z	CMvAQV2	192.168.122.62	49172	208.113.214.190	80	1	GET	fernandatur.comÂ	/Scripts/hqnybx2w.php?id=9	http://ww	....NET CLR 3.5.3(	0	265
2015-06-30 13:12:46 Z	CMHhzK1(	192.168.122.62	49173	208.113.214.190	80	1	GET	www.fernandatur.comÂ	/Scripts/hqnybx2w.php?id=9	http://ww	....NET CLR 3.5.3(	0	323
2015-06-30 13:12:47 Z	CocBdE3V	192.168.122.62	49174	46.30.45.65	80	1	GET	good.recycle2learn.com	...zwnEqWwxWeioXW_RGJN	http://ww	....NET CLR 3.5.3(	0	142971
2015-06-30 13:12:48 Z	CtGI8l22yi	192.168.122.62	49175	46.30.45.65	80	1	GET	good.recycle2learn.com	...GzO0ZUEgbogAQlryJQ-Dbp	...4SGhKrX(	....NET CLR 3.5.3(	0	15763
2015-06-30 13:12:51 Z	CocBdE3V	192.168.122.62	49174	46.30.45.65	80	2	GET	good.recycle2learn.com	...umAGzO0ZUEgbogAQlryJQ	null	....NET CLR 3.5.3(	0	352256
2015-06-30 13:12:52 Z	CtOXLI293	192.168.122.62	49176	23.10.250.43	80	1	GET	fpdownload2.macromedia.c	...p;cpuWordLength=64&play	null	Shockwave Flash	0	351
2015-06-30 13:12:55 Z	CALygR1Jr	192.168.122.62	49171	192.254.234.118	80	3	GET	www.floridablueline.comÂ	/favicon.ico	null	....NET CLR 3.5.3(	0	0

University of Victoria

Page2

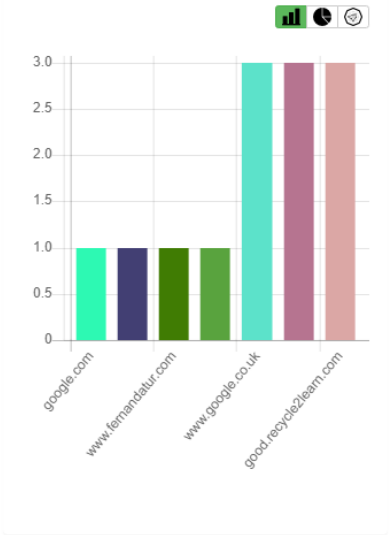
Request B	Response	Status Coc	Status Me	Info Code	Info Mess	File	Username	Password	Proxied	Sender Fil	Sender Mi	Recipient	Recipient	Client Hea	Server He	Cookie Va	URI Variables
0	261	302	Found	null	null	null	null	null	null	null	null	FZUYUM1I	text/html	ACCEPT,A	null	null	/
0	277	302	Found	null	null	null	null	null	null	null	null	FQFIHU3F	text/html	ACCEPT,A	null	null	/?gfe_rd,ei
0	1070	200	OK	null	null	null	null	null	null	null	null	FVBL1H1F	text/plain	ACCEPT,A	null	PREF,NID,	/url?url,rct,frm,q,es
0	5430	200	OK	null	null	null	null	null	null	null	null	FB9ZMI3K	image/x-i	ACCEPT,A	null	PREF,NID,	/favicon.ico
0	829	200	OK	null	null	null	null	null	null	null	null	FIA30B1ZE	text/html	ACCEPT,R	null	null	/
0	183799	200	OK	null	null	null	null	null	null	null	null	FIC2ID2EN	image/jpe	ACCEPT,R	null	null	/floridabluelinehea
0	265	301	Moved Pe	null	null	null	null	null	null	null	null	FIPQYF2ZJ	text/html	ACCEPT,R	null	null	/Scripts/hqnybx2w.p
0	323	200	OK	null	null	null	null	null	null	null	null	F4JAYX1V	applicatio	ACCEPT,R	null	null	/Scripts/hqnybx2w.p
0	142971	200	OK	null	null	null	null	null	null	null	null	FEEAQ5N4	text/html	ACCEPT,R	null	null	/?xniKfredLBvKDIU
0	15763	200	OK	null	null	null	null	null	null	null	null	FSQGDL2C	applicatio	ACCEPT,A	null	null	/index.php?xniKfrec
0	352256	200	OK	null	null	null	null	null	null	null	null	FHRPWCV	null	ACCEPT,A	null	null	/index.php?xniKfrec
0	351	404	Not Found	null	null	null	null	null	null	null	null	FDFE1C4JI	text/html	USER-AGE	null	null	...602.168~installVec
0	0	200	OK	null	null	null	null	null	null	null	null	null	null	ACCEPT,A	null	null	/favicon.ico

Diagram of HTTP report on packettotal

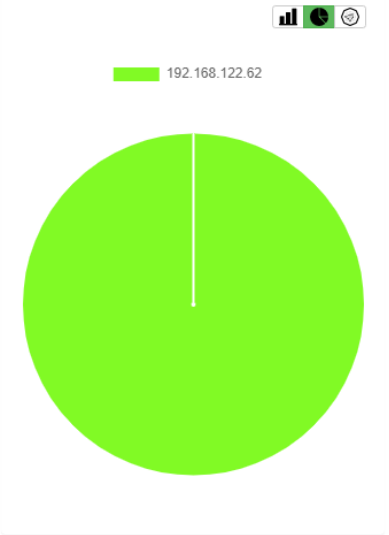


University of Victoria

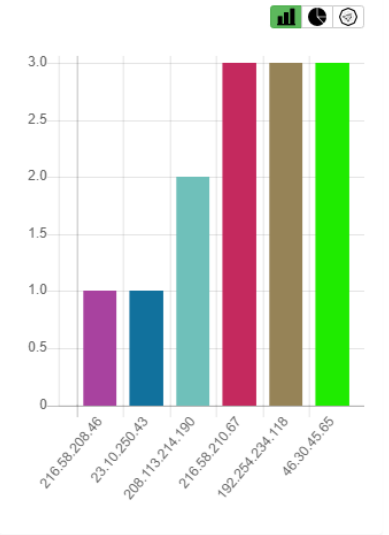
Requests by Host



Requests by Source IP



Requests by Destination IP



Requests by Source Port

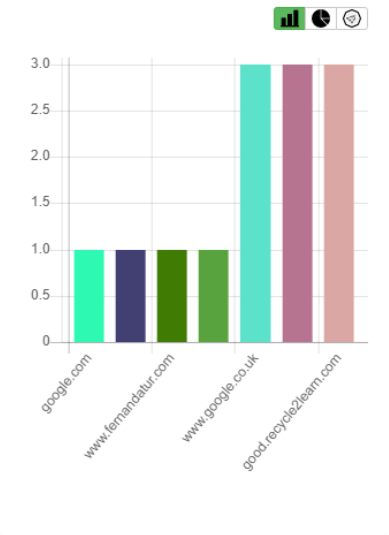
Requests by Destination Port

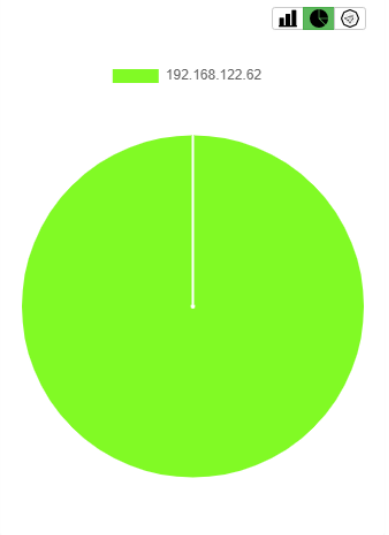
Requests by URI

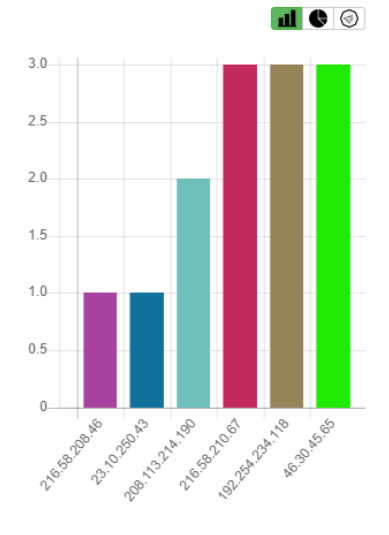
Requests by Host

Requests by Source IP

Requests by Destination IP





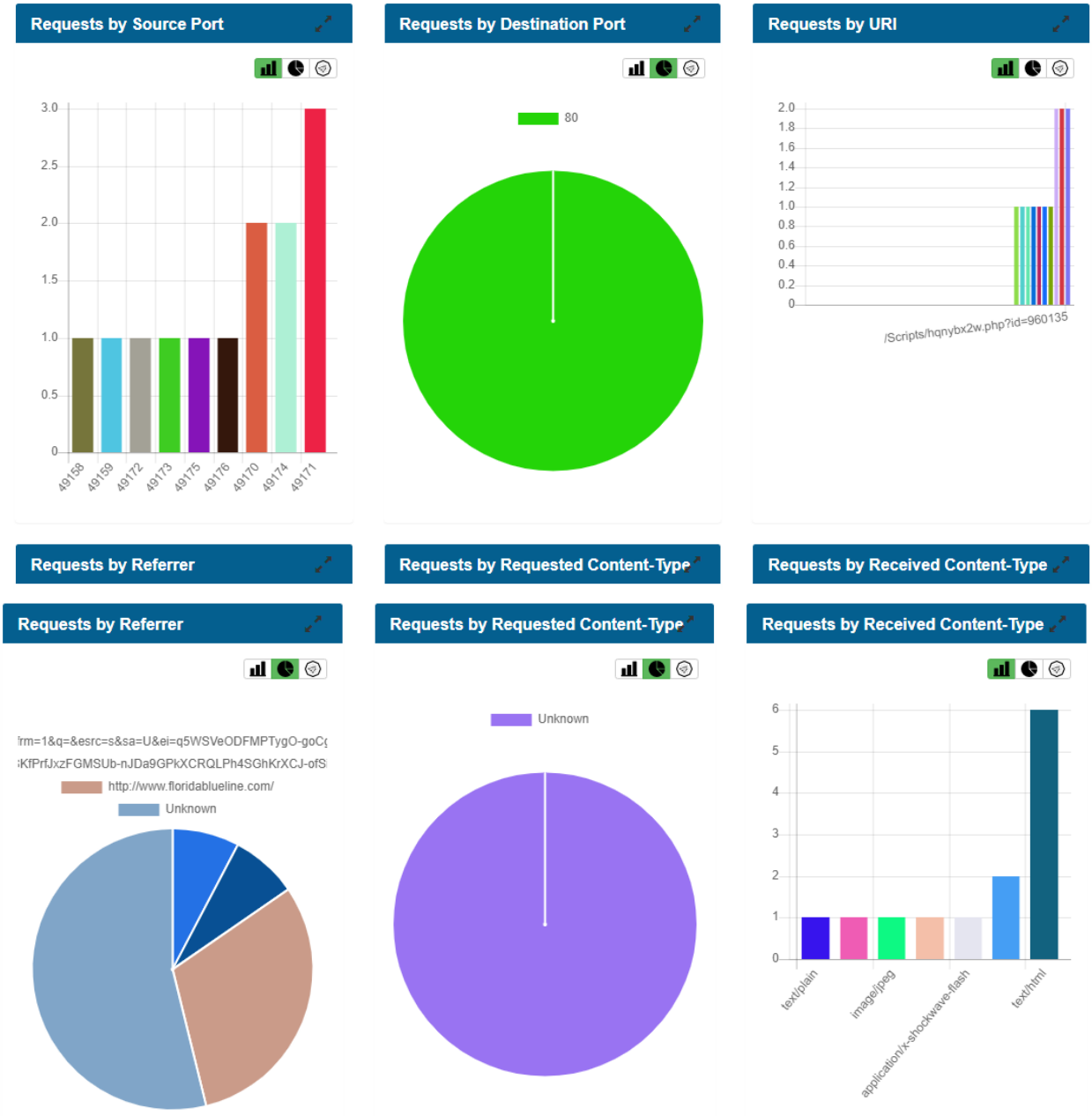


Requests by Source Port

Requests by Destination Port

Requests by URI

University of Victoria



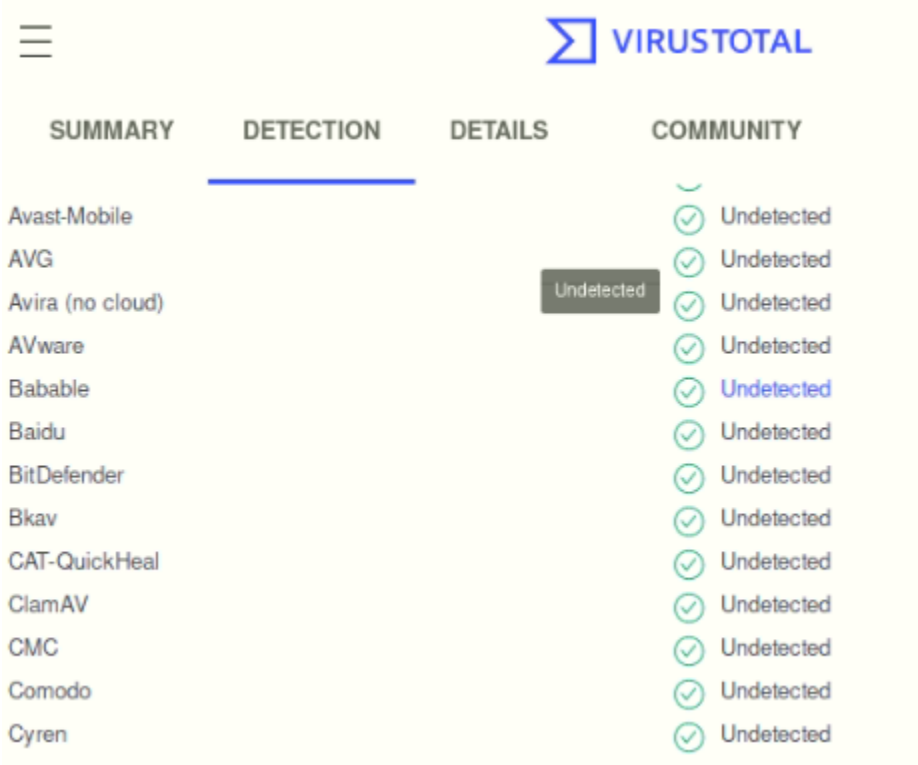
The Files Transfer payload as follows:

University of Victoria

	Timestamp	Connection IDs	Artifact	MD5 Hash	SHA1 Hash	Originated From Host/	Sent To Host/s	Source	Depth	Mime Type	File Name	Total Bytes
2	2015-06-30 13:12:44 Z	CIFU4P2TqMGvSgfc62	FVBL1H1FVSERAS	1332bd535c01fd4	da951504bb632	216.58.210.67	192.168.122.62	HTTP	0	text/plain	null	null
3	2015-06-30 13:12:44 Z	CIFU4P2TqMGvSgfc62	FB9ZMI3KOMATO	a300693728f5caa	e2020bf4f2b65f	216.58.210.67	192.168.122.62	HTTP	0	image/x-icon	null	null
4	2015-06-30 13:12:45 Z	CALygR1JnJXOgNnETj	FIA30B1ZBQ86MY	6535a237a2652f5	462fdab7eaf516	192.254.234.118	192.168.122.62	HTTP	0	text/html	null	null
5	2015-06-30 13:12:45 Z	CALygR1JnJXOgNnETj	FIC2ID2ENIQ6Z2U	cb5d1061b1ef3b2	8fbec3e6569cef	192.254.234.118	192.168.122.62	HTTP	0	image/jpeg	null	183799
6	2015-06-30 13:12:45 Z	CMvAQV2OwfXQnWdF	FIPQYF2ZJIGGRO7	1675befb11864f1	f162bf38954f6a5	208.113.214.190	192.168.122.62	HTTP	0	text/html	null	null
7	2015-06-30 13:12:47 Z	CMHhzK1MVihV1X1U2	F4JAYX1VSTBLTTS	b69afae73df2f68	713824ab0f35a5	208.113.214.190	192.168.122.62	HTTP	0	application/javascript	null	null
8	2015-06-30 13:12:48 Z	CocBdE3VP4U7EE8PX5	FEEAQ5NAFXOGS	4634a93740f1492	b87777893cda31	46.30.45.65	192.168.122.62	HTTP	0	text/html	null	null
9	2015-06-30 13:12:49 Z	CtGI8l22yrRPVlLob	FSQGDL2CN1BEPC	4a08a4536bb6b2f	bcb562479d2c19	46.30.45.65	192.168.122.62	HTTP	0	application/x-shockwa	null	15763
10	2015-06-30 13:12:52 Z	CtOXLI293JVZ3Ot68h	FDFE1C4JMCXQBC	58f46f6f93cadc3b	8ae69b66ebe0c	23.10.250.43	192.168.122.62	HTTP	0	text/html	null	351
11	2015-06-30 13:12:54 Z	CocBdE3VP4U7EE8PX5	FHRPWCW7ASNO	eb756a359d0c5ec	a1a9b3f5bc705c	46.30.45.65	192.168.122.62	HTTP	0	null	null	352256

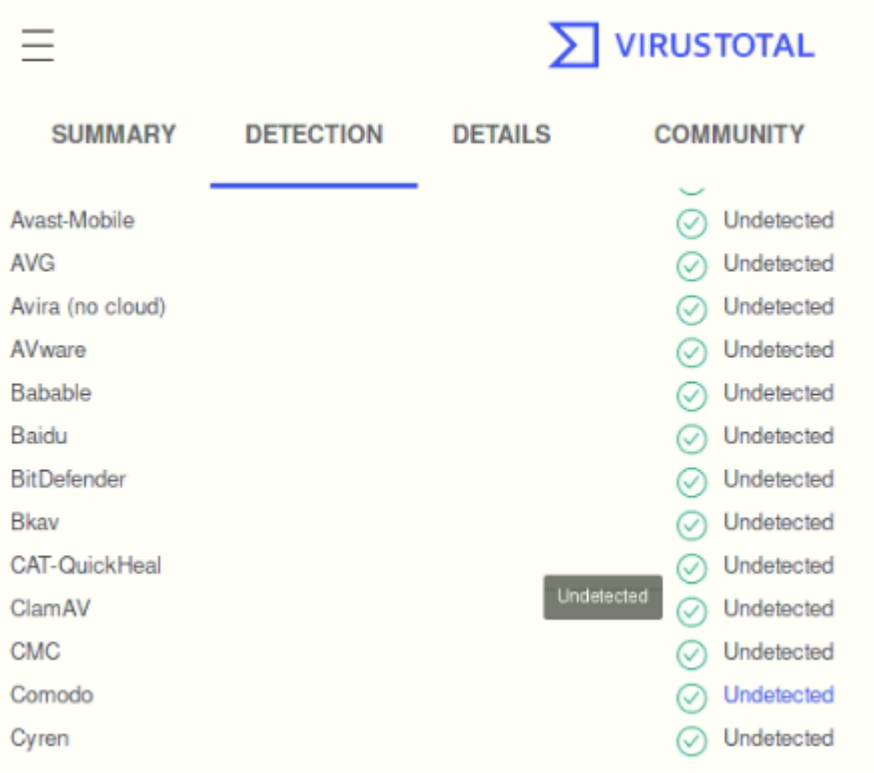
Screen shots of all HTTP payloads are as a following pictures respectively based on table above:

Google.com



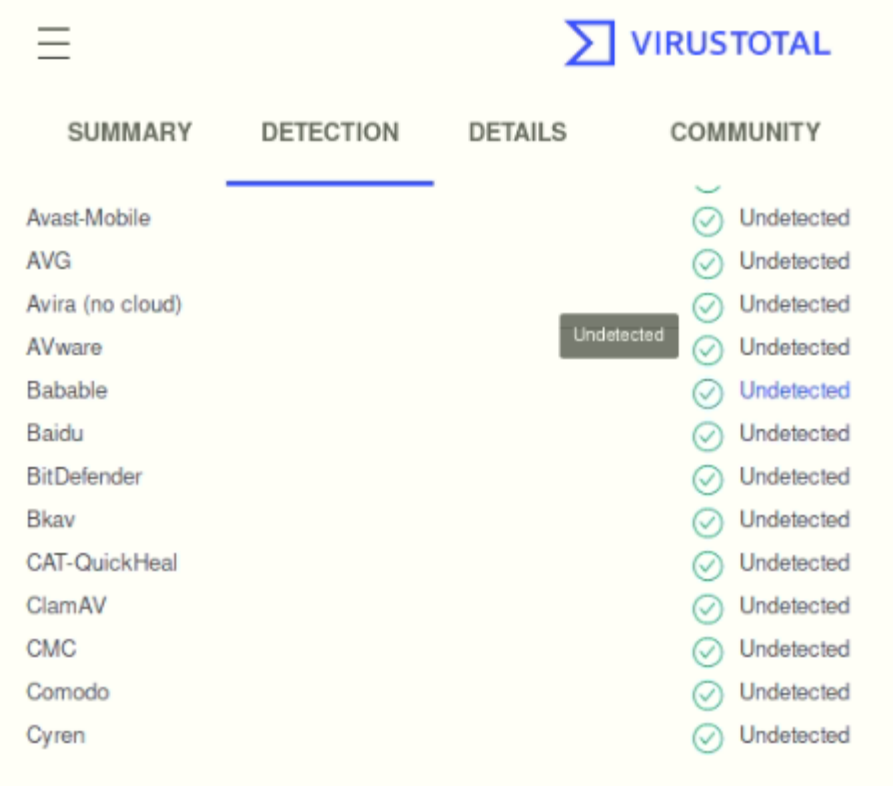
www.google.co.uk

University of Victoria



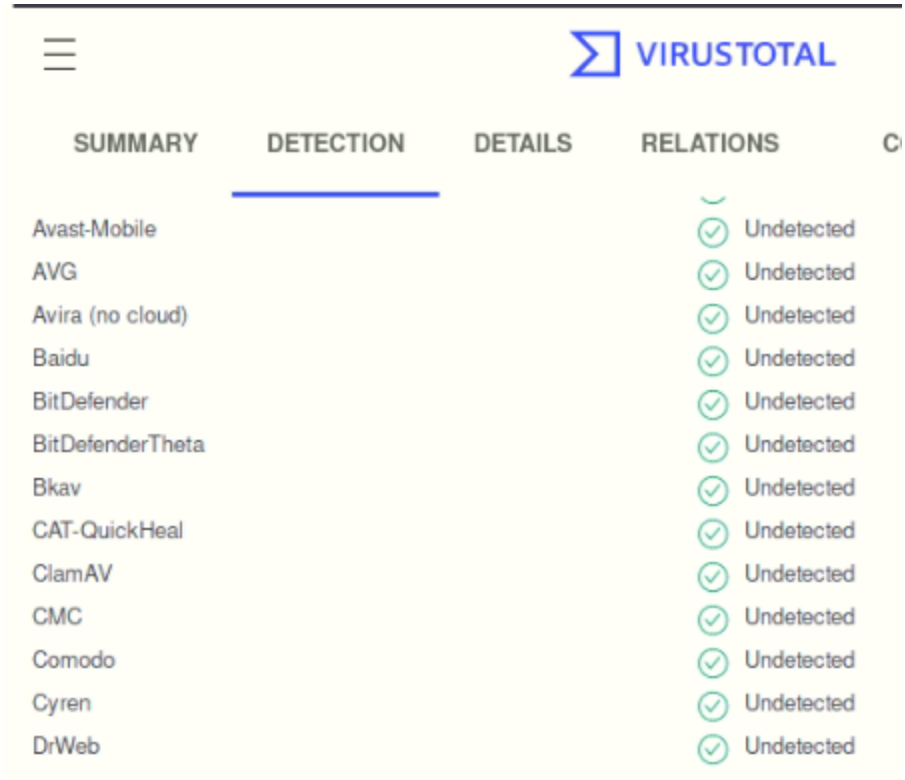
www.google.co.uk

University of Victoria



www.google.co.uk

University of Victoria



www.floridablueline.com

University of Victoria

VIRUSTOTAL

SUMMARY | DETECTION | DETAILS | COMMUNITY

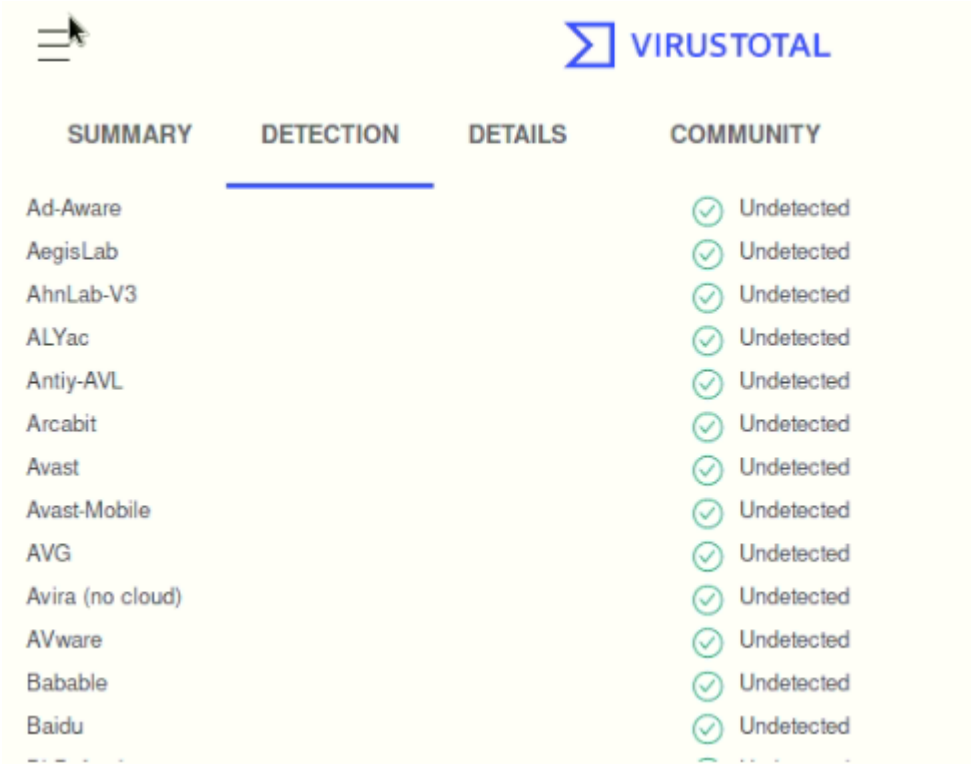
Ad-Aware	Trojan.GenericKD.31150873
AegisLab	Trojan.Script.Generic.4!c
AhnLab-V3	HTML/Redirect
ALYac	Trojan.GenericKD.31150873
Antiy-AVL	Trojan/JS.Redirector.nt
Arcabit	Trojan.Generic.D1DB5319
Avast	HTML:Includer-BR [Trj]
AVG	HTML:Includer-BR [Trj]
Avira (no cloud)	HTML/Rce.Gen2
BitDefender	Trojan.GenericKD.31150873
CAT-QuickHeal	JS.Redirector.AN
Emsisoft	Trojan.GenericKD.31150873 (B)
eScan	Trojan.GenericKD.31150873
F-Secure	Malware.HTML/Rce.Gen2
FireEye	Trojan.GenericKD.31150873
Fortinet	HTML/InjectedPhp.NZ!tr
GData	Script.Packed.IFrame.K@gen
Ikarus	Trojan.Script
Kaspersky	HEUR:Trojan.Script.Generic
MAX	Malware (ai Score=99)
Microsoft	Trojan:HTML/Redirector.EP
NANO-Antivirus	Trojan.Html.Iframe.dcipov
Qihoo-360	Generic/Trojan.Script.ed4
Sophos AV	Troj/JSRedir-NZ
Symantec	Trojan.Gen.2

University of Victoria

VIPRE	LooksLike.JS.Redirector.nt (v)
ZoneAlarm by Check Point	HEUR:Trojan.Script.Generic
Avast-Mobile	Undetected
Baidu	Undetected
BitDefenderTheta	Undetected

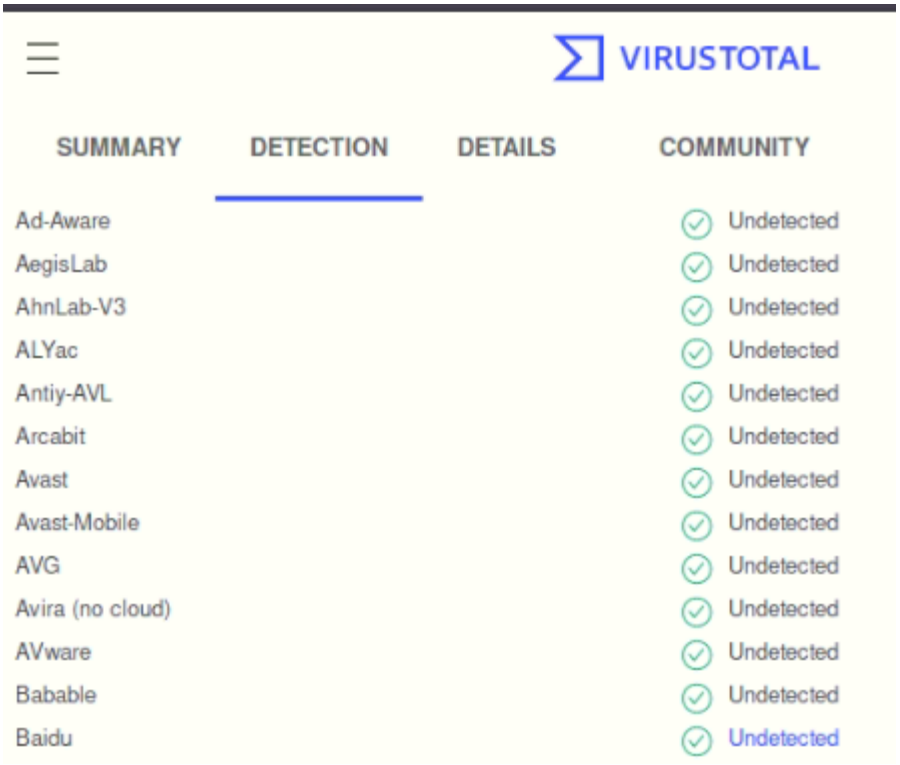
27 transcripts, malware found

www.floridablueline.com



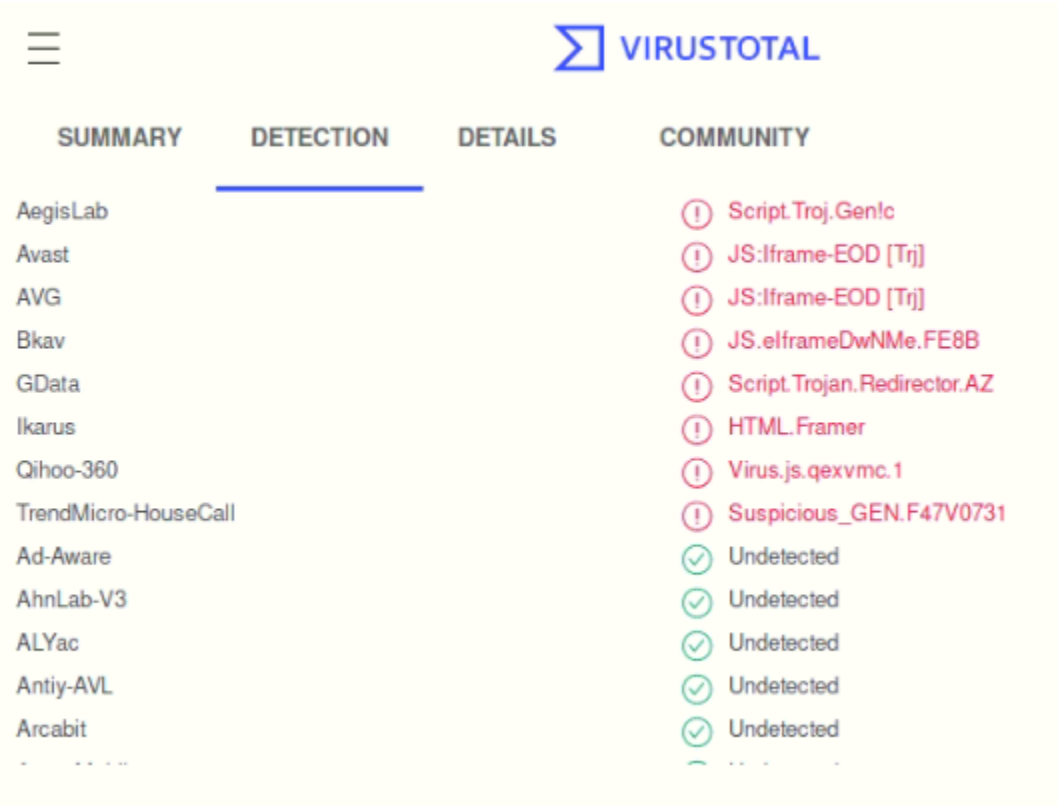
Fernandatur.com

University of Victoria



www.fernandatur.com

University of Victoria



Good.recycle2learn.com

University of Victoria

VIRUSTOTAL

SUMMARY | DETECTION | DETAILS | COMMUNITY

AegisLab	Trojan.HTML.Generic.4!c
ESET-NOD32	JS/Kryptik.AVE
Ikarus	JS.Exploit
Kaspersky	HEUR:Exploit.Script.Generic
McAfee-GW-Edition	BehavesLike.HTML.ExploitBlacole.cr
Microsoft	Trojan:Script/Wacatac.C!ml
Qihoo-360	Generic/Trojan.Exploit.b4f
Rising	Trojan.Kryptik!8.8 (TOPIS:E0:0xbvllh1xeV)
Sangfor Engine Zero	Malware
Sophos AV	Troj/ExpJS-KX
Symantec	Trojan.Gen.7
ZoneAlarm by Check Point	HEUR:Exploit.Script.Generic
Ad-Aware	Undetected

Good.recycle2learn.com

University of Victoria

VIRUSTOTAL

SUMMARY | DETECTION | DETAILS | COMMUNITY 4

Ad-Aware	Script.SWF.Exploit.CVE-2015-3105.C500
AegisLab	Hacktool.SWF.Agent.3!c
AhnLab-V3	SWF/Exploit
ALYac	Script.SWF.Exploit.CVE-2015-3105.C500
Antiy-AVL	Trojan[Exploit]/SWF.SWF.Generic
Arcabit	Script.SWF.Exploit.CVE-2015-3105.C500
Avast	SWF:Malware-gen [Trj]
AVG	SWF:Malware-gen [Trj]
Avira (no cloud)	EXP/Agent.EB.48
BitDefender	Script.SWF.Exploit.CVE-2015-3105.C500
CAT-QuickHeal	SWF.Kit.Nuclear.N
ClamAV	Swf.Exploit.Kit-99
Comodo	Malware@#2iqyxbwc2cazk

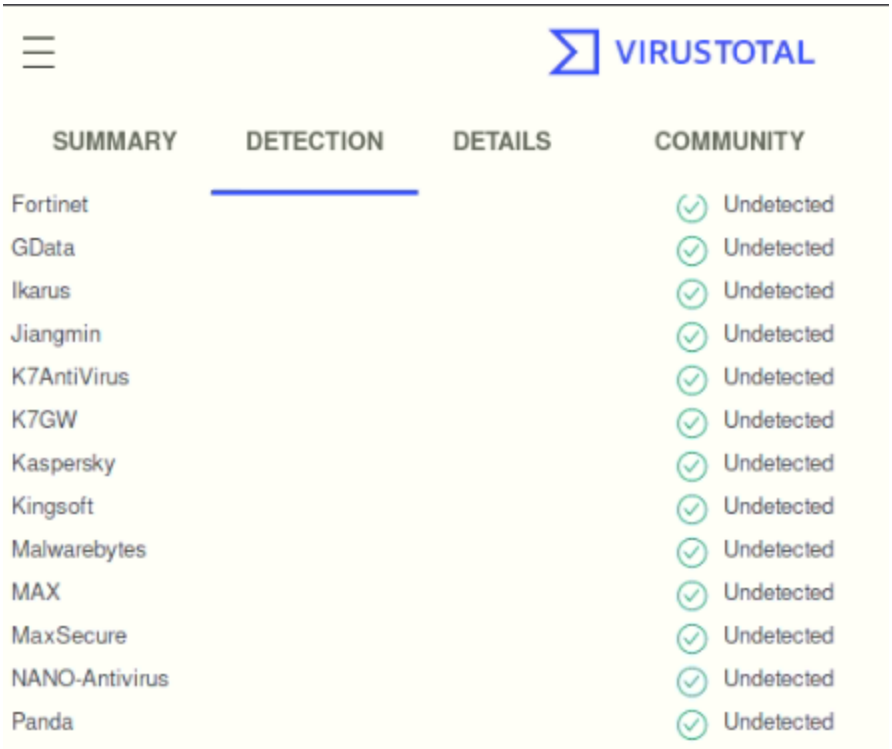
University of Victoria

Cyren	SWF/SWF/Exploit
DrWeb	Exploit.SWF.1232
Emsisoft	Script.SWF.Exploit.CVE-2015-3105.C500 (B)
eScan	Script.SWF.Exploit.CVE-2015-3105.C500
ESET-NOD32	SWF/Exploit.ExKit.AS
F-Prot	SWF/SWF/Exploit
F-Secure	Exploit.EXP/Agent.EB.48
FireEye	Script.SWF.Exploit.CVE-2015-3105.C500
GData	Script.SWF.Exploit.CVE-2015-3105.C500
Ikarus	Trojan.SWF.Exploit
Kaspersky	Exploit.SWF.Agent.ro
MAX	Malware (ai Score=100)
McAfee	SWF/Exploit-Rig.a
McAfee-GW-Edition	BehavesLike.Flash.Exploit.mg
NANO-Antivirus	Trojan.Swf.Mlw.ebrtvr
Qihoo-360	Generic/Trojan.Exploit.7f1
Sophos AV	Troj/SWFExp-HN
Symantec	Trojan.Gen.2
Tencent	Win32.Exploit.Agent.Pbpg
TrendMicro	EXPL_CVE20153090
Zillya	Exploit.Agent.Script.854
ZoneAlarm by Check Point	Exploit.SWF.Agent.ro
Avast-Mobile	Undetected
Baidu	Undetected
BitDefenderTheta	Undetected

35 engines detected malware, trojan scripts,swf exploit

Good.recycle2learn.com

University of Victoria



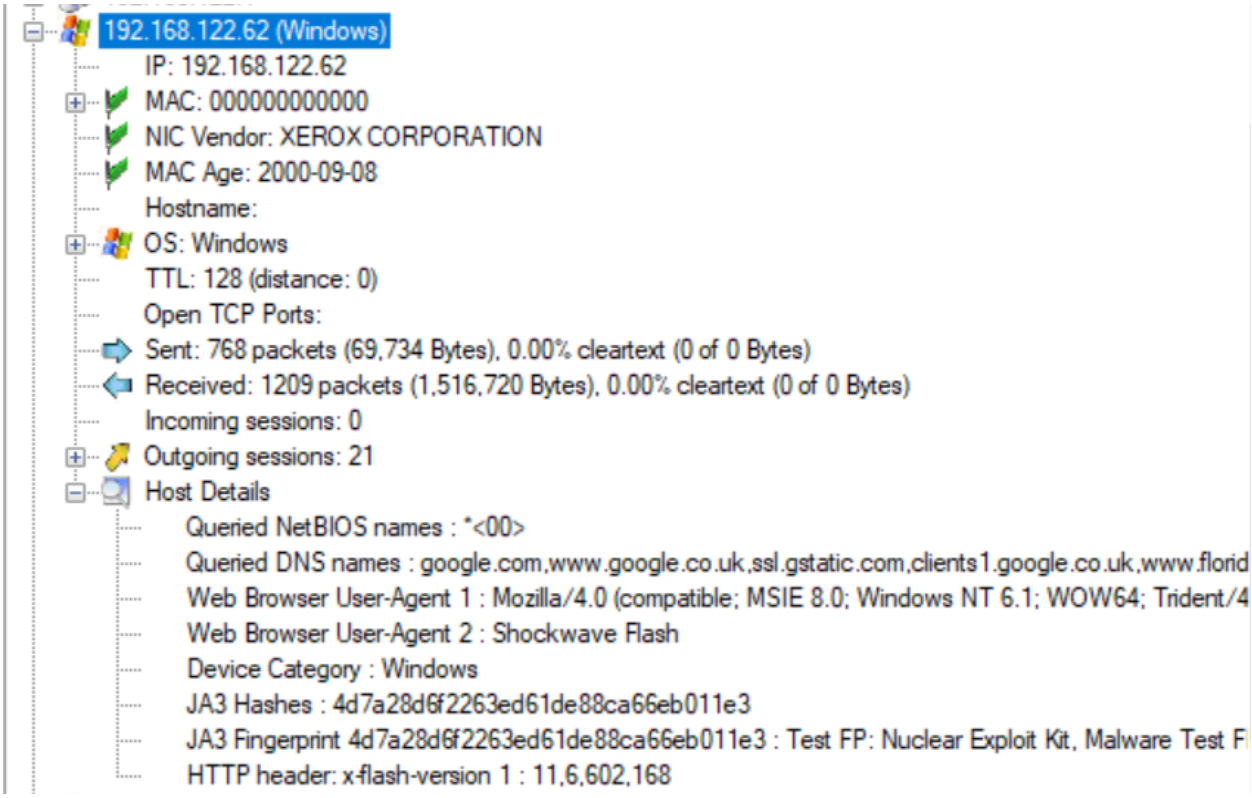
Fpdownload2.macromedia.com

University of Victoria

VIRUSTOTAL

SUMMARY | DETECTION | DETAILS | COMMUNITY

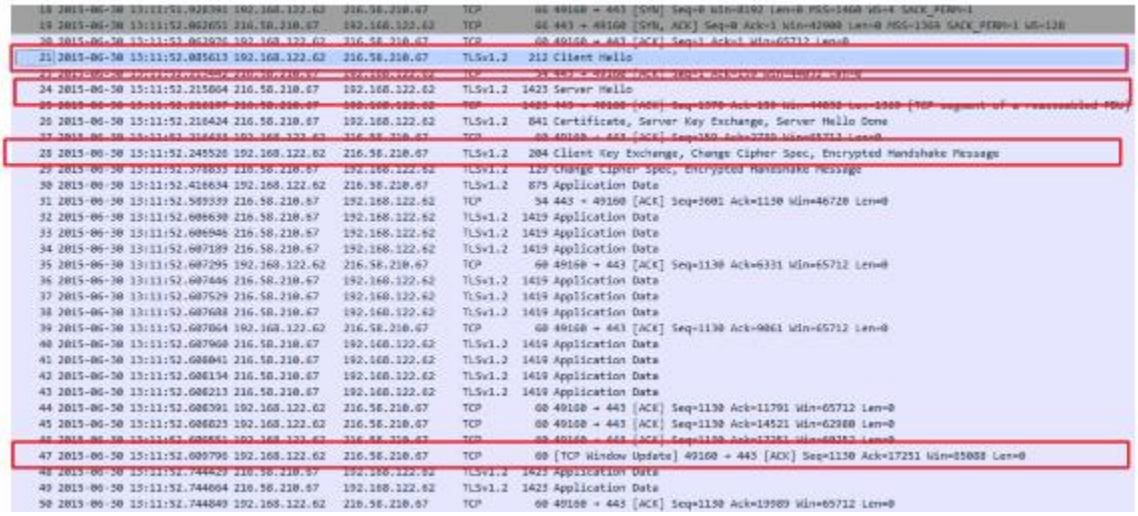
Ad-Aware	Undetected
AegisLab	Undetected
AhnLab-V3	Undetected
ALYac	Undetected
Antiy-AVL	Undetected
Arcabit	Undetected
Avast	Undetected
Avast-Mobile	Undetected
AVG	Undetected
Avira (no cloud)	Undetected
Baidu	Undetected
BitDefender	Undetected
BitDefenderTheta	Undetected



JA3: 4d7a28d6f2263ed61de88ca66eb011e3
It is a fingerprint for Emotet.
In these malware examples, the command and control server always responds to the malware client in exactly the same way, it does not deviate. So even though the traffic is encrypted and one may not know the command and control server's IPs or domains as they are constantly changing,

In this pcap file we have windows update, and messages like Hello Client.and also the first frames of pcap has a lot of TLS files. These are weird, so based on the behaviour of packets in wireshark and searching on the internet we found some clues.
Some part of our pcap file that include windows update, and messages like Hello Client is as a follows:

University of Victoria



TLS and it's predecessor, SSL,are used to encrypt communication for both common applications, to keep your data secure, and malware, so it can hide in the noise. To initiate a SSL session, a client will send a SSL Client Hello packet following the TCP 3-way handshake. This packet and the way in which it is generated is dependent on packages and methods used when building the client application. The server, if accepting SSL connections, will respond with a SSL Server Hello packet that is formulated based on server-side libraries and configurations as well as details in the Client Hello. Because SSL negotiations are transmitted in the clear, it's possible to fingerprint and identify client applications using the details in the SSL Client Hello packet.
The JA3 method is used to gather the decimal values of the bytes for the following fields in the Client Hello packet: Version, Accepted Ciphers, List of Extensions, Elliptic Curves, and Elliptic Curve Formats. It then concatenates those values together in order, using a "," to delimit each field and a "-" to delimit each value in each field.

Emotet is a Trojan that do infection via malicious script, macro-enabled document files, or malicious JavaScript file. Emotet may try to persuade users to click the malicious files.

University of Victoria

5. Identify other malicious hosts or sites with which the compromised host interacted. Only malicious hosts should be included in this list. Provide your response in a table listing the following.

Table below includes all probable malicious hosts/websites which host IP 192.168.122.62. Even though we explained some of them in above questions

Host name/URL	IP Address	Role	service	Communication protocol	Start Date/time	End date/time
floridablueline.com, www.floridablueline.com	192.254.234.118	Compromised website	http	tcp	13:12:44	13:13:55
fernandatur.com, www.fernandatur.com	208.113.214.190	Redirect host	http	tcp	13:12:44	13:13:55
good.recycle2learn.com	46.30.45.65	Delivered malware	http	tcp	13:12:47	13:13:55
a1293.d.akamai.net, fpdownload.macromedia.com.edgesuite.net, fpdownload2.macromedia.com	23.10.250.43	Web Server banner Not found for get flash player update	http	tcp	13:12:52	13:13:55

University of Victoria

------	43.225.38.217	Encrypted traffic	null	tcp	13:13:14	13:15:25
time.microsoft.akadns.net, time.windows.com	23.99.222.162	Looks not malicious	null	udp	13:16:13	13:16:14
-------	111.121.193.242	Spam traffic	null	tcp	13:15:55	13:15:58
-------	78.129.168.237	Traffic	null	udp	13:16:17	13:16:20
Unknown host	37.55.107.202	Continus traffic	null	tcp	13:16:28	13:17:45
a1293.d.akamai.net, fpdownload.macromedia.com.edgesuite.net	23.10.250.18	DNS hijacking, MAC spoofing	null	tcp		

For IP 43.225.38.217 shows TCp traffic and also one engin found it malicious

University of Victoria

ip.addr == 43.225.38.217

No.	Time	Source	Destination	Protocol	Length	Info
1253	2015-06-30 13:13:14.087639	192.168.122.62	43.225.38.217	TCP	66	49177 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1254	2015-06-30 13:13:14.481484	43.225.38.217	192.168.122.62	TCP	54	443 → 49177 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1255	2015-06-30 13:13:14.990962	192.168.122.62	43.225.38.217	TCP	66	[TCP Retransmission] 49177 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256
1256	2015-06-30 13:13:15.391086	43.225.38.217	192.168.122.62	TCP	54	443 → 49177 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1257	2015-06-30 13:13:15.895782	192.168.122.62	43.225.38.217	TCP	62	[TCP Retransmission] 49177 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PE
1262	2015-06-30 13:13:16.290494	43.225.38.217	192.168.122.62	TCP	54	443 → 49177 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1264	2015-06-30 13:13:46.300391	192.168.122.62	43.225.38.217	TCP	66	49178 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1265	2015-06-30 13:13:46.688117	43.225.38.217	192.168.122.62	TCP	54	443 → 49178 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1266	2015-06-30 13:13:47.204972	192.168.122.62	43.225.38.217	TCP	66	[TCP Retransmission] 49178 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256
1267	2015-06-30 13:13:47.597715	43.225.38.217	192.168.122.62	TCP	54	443 → 49178 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1268	2015-06-30 13:13:48.109606	192.168.122.62	43.225.38.217	TCP	62	[TCP Retransmission] 49178 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PE
1269	2015-06-30 13:13:48.502950	43.225.38.217	192.168.122.62	TCP	54	443 → 49178 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1276	2015-06-30 13:14:18.503667	192.168.122.62	43.225.38.217	TCP	66	49179 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1277	2015-06-30 13:14:18.901948	43.225.38.217	192.168.122.62	TCP	54	443 → 49179 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1278	2015-06-30 13:14:19.407842	192.168.122.62	43.225.38.217	TCP	66	[TCP Retransmission] 49179 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256
1279	2015-06-30 13:14:19.808323	43.225.38.217	192.168.122.62	TCP	54	443 → 49179 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1280	2015-06-30 13:14:20.310993	192.168.122.62	43.225.38.217	TCP	62	[TCP Retransmission] 49179 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PE
1281	2015-06-30 13:14:20.704101	43.225.38.217	192.168.122.62	TCP	54	443 → 49179 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1282	2015-06-30 13:14:50.716365	192.168.122.62	43.225.38.217	TCP	66	49180 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1283	2015-06-30 13:14:51.111412	43.225.38.217	192.168.122.62	TCP	54	443 → 49180 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1284	2015-06-30 13:14:51.620631	192.168.122.62	43.225.38.217	TCP	66	[TCP Retransmission] 49180 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256
1285	2015-06-30 13:14:52.012913	43.225.38.217	192.168.122.62	TCP	54	443 → 49180 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1286	2015-06-30 13:14:52.525314	192.168.122.62	43.225.38.217	TCP	62	[TCP Retransmission] 49180 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PE
1287	2015-06-30 13:14:52.915870	43.225.38.217	192.168.122.62	TCP	54	443 → 49180 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1288	2015-06-30 13:15:22.930091	192.168.122.62	43.225.38.217	TCP	66	49181 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1289	2015-06-30 13:15:23.315772	43.225.38.217	192.168.122.62	TCP	54	443 → 49181 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Search in results

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	Service	Duration	Payload Bytes Sent	Total Bytes Sent	Payload Bytes Received	Total B
2015-06-30 13:13:15 Z	CWfNU2C0uEEsTdN3b	192.168.122.62	49177	43.225.38.217	443	tcp	null	0.39	0	48	0	40
2015-06-30 13:13:46 Z	CxkLlp3FbMMHN2QfQd	192.168.122.62	49178	43.225.38.217	443	tcp	null	0.39	0	52	0	40
2015-06-30 13:13:47 Z	CVAIDQ22kkMnJ65wd2	192.168.122.62	49178	43.225.38.217	443	tcp	null	0.39	0	52	0	40
2015-06-30 13:13:48 Z	C21JhEr8YO7T6pg78	192.168.122.62	49178	43.225.38.217	443	tcp	null	0.39	0	48	0	40
2015-06-30 13:14:18 Z	CfjLHP1IffJ4s9AkMj	192.168.122.62	49179	43.225.38.217	443	tcp	null	0.40	0	52	0	40
2015-06-30 13:14:19 Z	CQsIH24UhMcYUp1Tjd	192.168.122.62	49179	43.225.38.217	443	tcp	null	0.40	0	52	0	40
2015-06-30 13:14:20 Z	CXpopX29JQiyXQ3B43	192.168.122.62	49179	43.225.38.217	443	tcp	null	0.39	0	48	0	40
2015-06-30 13:14:50 Z	CUcxOsG2OI0dSAiD8	192.168.122.62	49180	43.225.38.217	443	tcp	null	0.40	0	52	0	40
2015-06-30 13:14:51 Z	Ctgu0J1jlVhGkeeAVi	192.168.122.62	49180	43.225.38.217	443	tcp	null	0.39	0	52	0	40
2015-06-30 13:14:52 Z	Ccu86e4PUcYOZI6tEI	192.168.122.62	49180	43.225.38.217	443	tcp	null	0.39	0	48	0	40

http://43.225.38.217/

1 / 77

Community Score

One engine detected this URL

http://43.225.38.217/

43.225.38.217

ip

2020-04-16 05:22:49 UTC

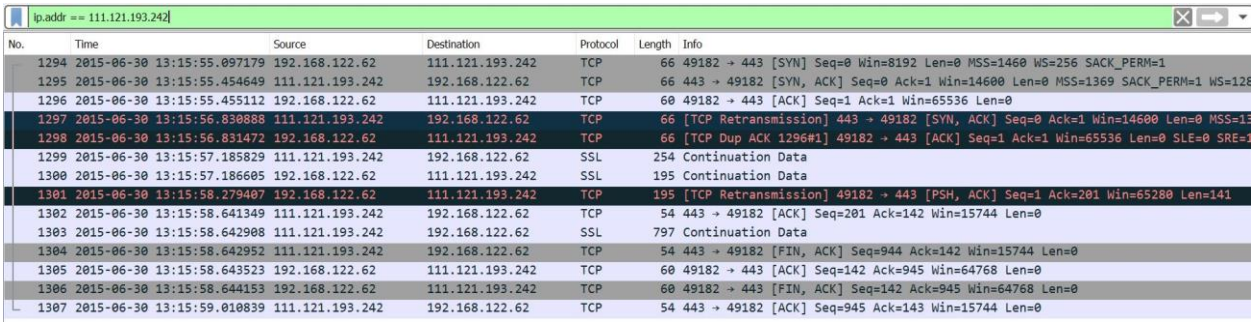
3 months ago

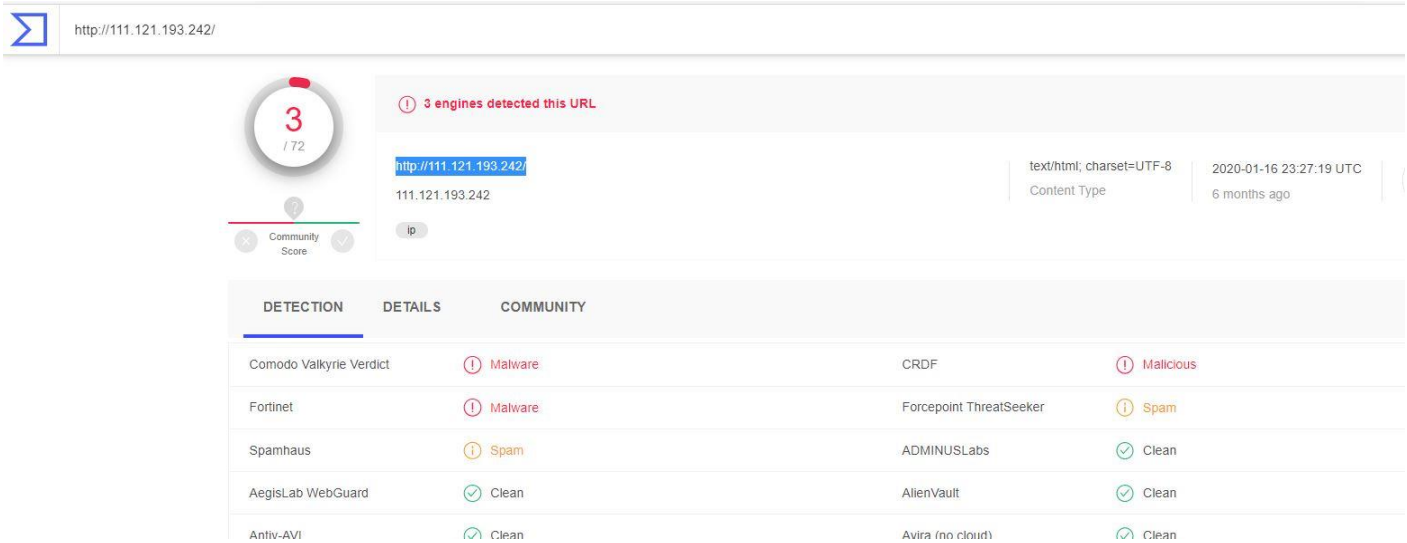
DETECTION DETAILS COMMUNITY

Forcepoint ThreatSeeker	Malicious	ADMINUSLabs	Clean
AegisLab WebGuard	Clean	AlienVault	Clean
Antiy-AVL	Clean	Artists Against 419	Clean

University of Victoria

For IP 111.121.193.242 virus total shows malicious and also listed in blacklist Ip





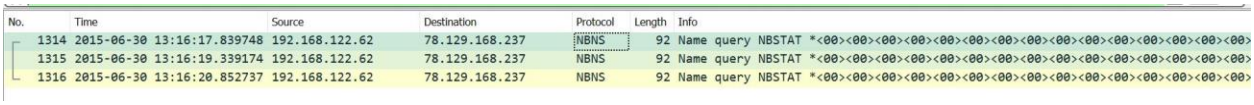
University of Victoria

111.121.193.242 Check IP Address

IP Address Information

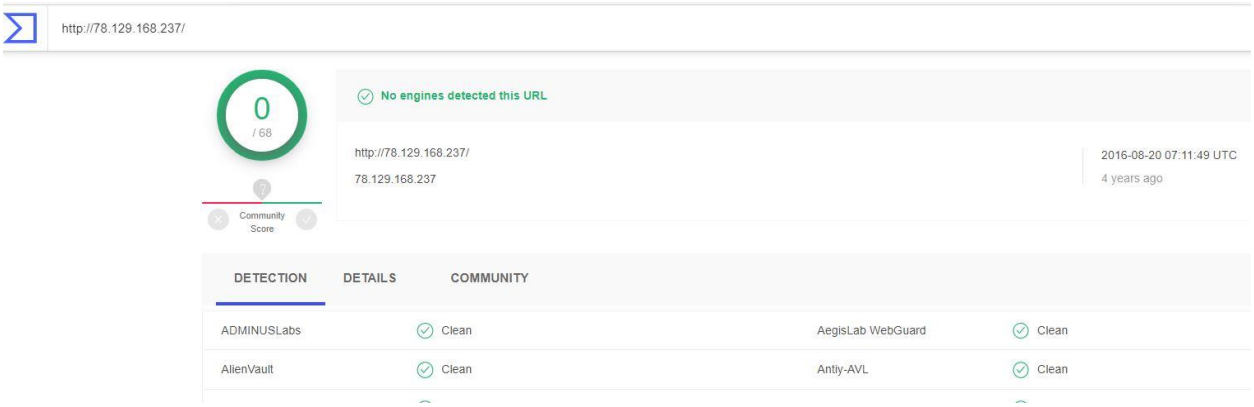
Analysis Date	2020-08-03 00:21:06
Elapsed Time	1 seconds
Blacklist Status	BLACKLISTED 1/114
IP Address	**111.121.193.242** Find Sites | IP Whois
Reverse DNS	Unknown
ASN	AS4134
ASN Owner	Chinanet
ISP	China Telecom
Continent	Asia
Country Code	(CN) China
Latitude / Longitude	34.7725 / 113.7266 Google Map
City	Unknown
Region	Unknown

For IP 78.129.168.237

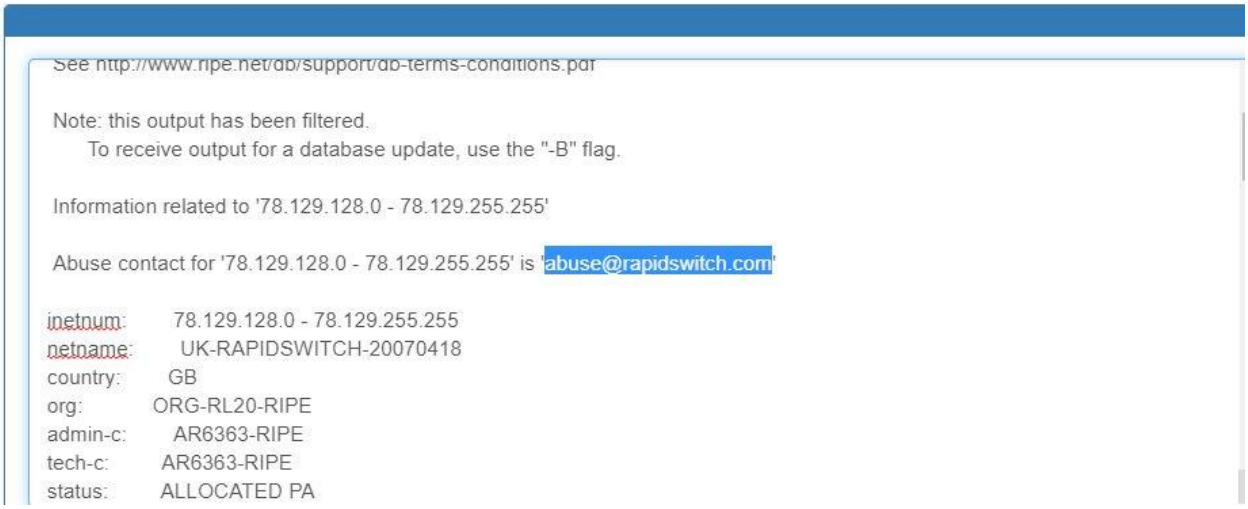


No.	Time	Source	Destination	Protocol	Length	Info
1314	2015-06-30 13:16:17.839748	192.168.122.62	78.129.168.237	NBNS	92	Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
1315	2015-06-30 13:16:19.339174	192.168.122.62	78.129.168.237	NBNS	92	Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
1316	2015-06-30 13:16:20.852737	192.168.122.62	78.129.168.237	NBNS	92	Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>

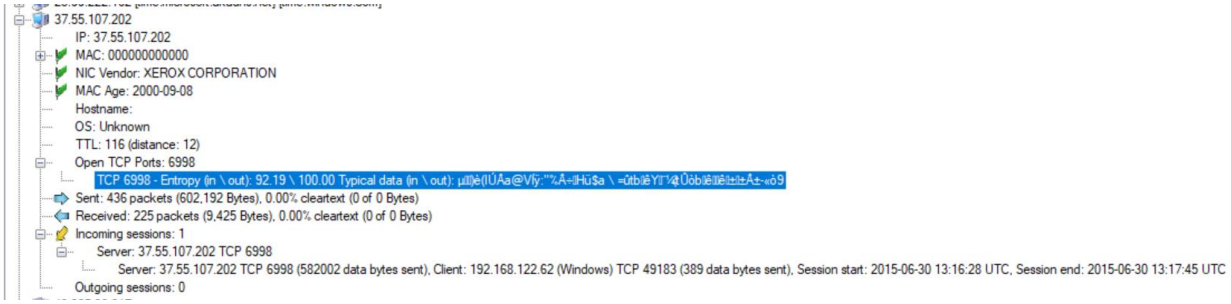
University of Victoria



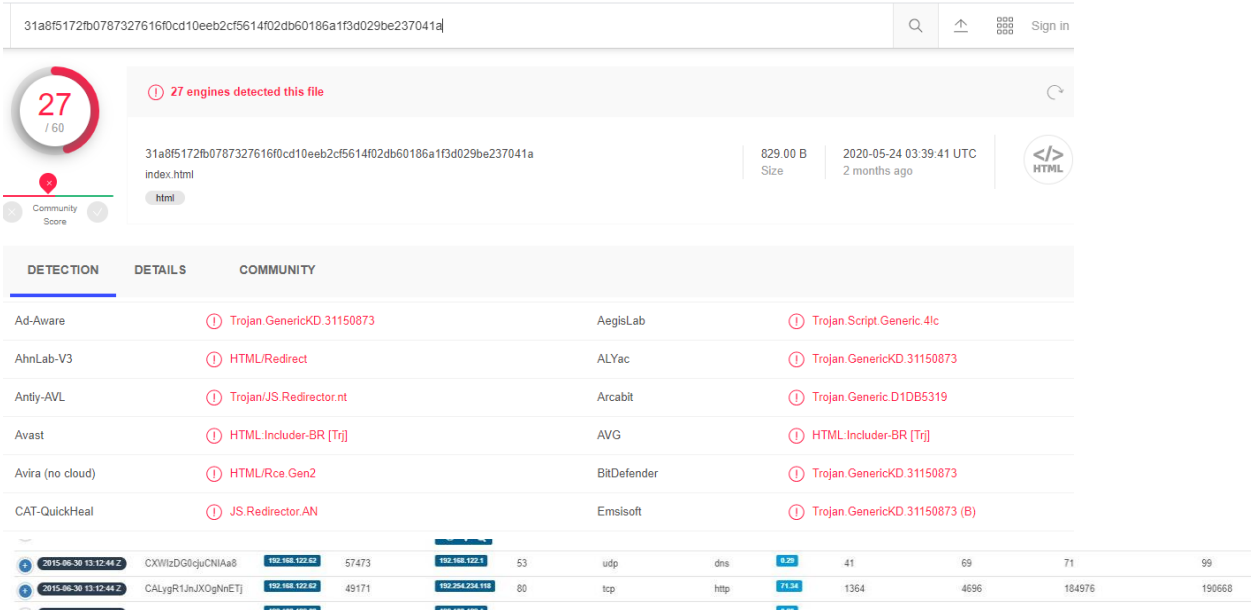
WhoIs



For IP 37.55.107.202

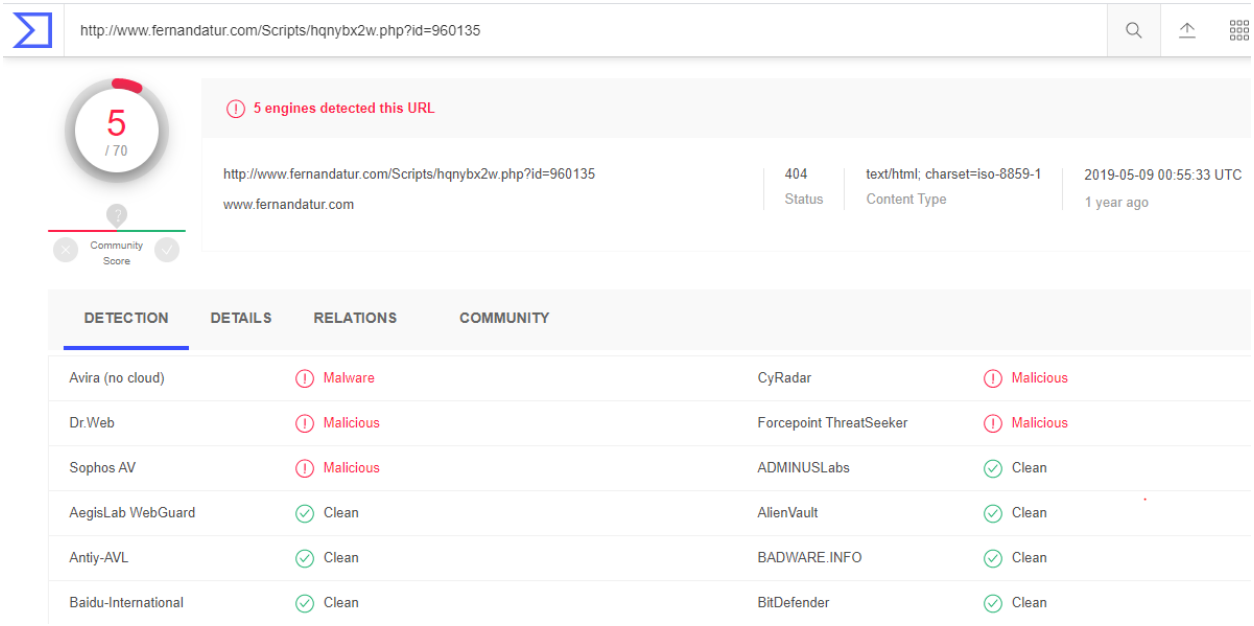


For IP 192.254.234.118 (detailed screenshot provided in Q2and 3 to avoid repetition)



For IP 208.113.214.190 (detailed screenshot provided in Q2and 3 to avoid repetition)

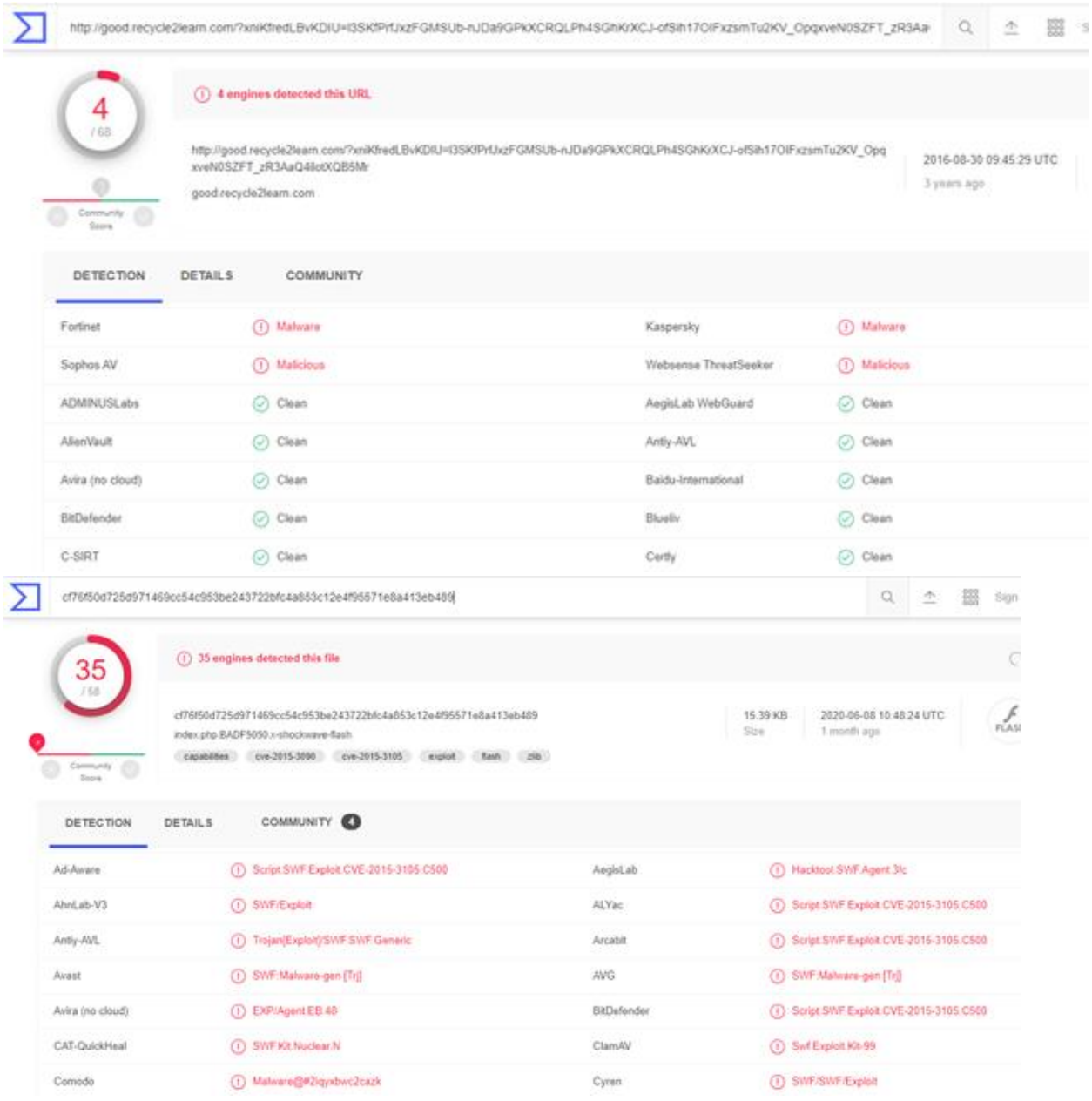
University of Victoria



For IP 46.30.45.65 (detailed screenshot provided in Q2and 3 to avoid repetition)

Analysis Date	2020-07-31 00:21:17
Elapsed Time	2 seconds
Blacklist Status	BLACKLISTED 1/114
IP Address	46.30.45.65 Find Sites | IP Whois
Reverse DNS	serv1.abitec.ru
ASN	AS210079
ASN Owner	EuroByte LLC
ISP	EuroByte LLC
Continent	Europe
Country Code	(RU) Russia
Latitude / Longitude	55.7386 / 37.6068 Google Map
City	Unknown

University of Victoria



For IP 23.10.250.18

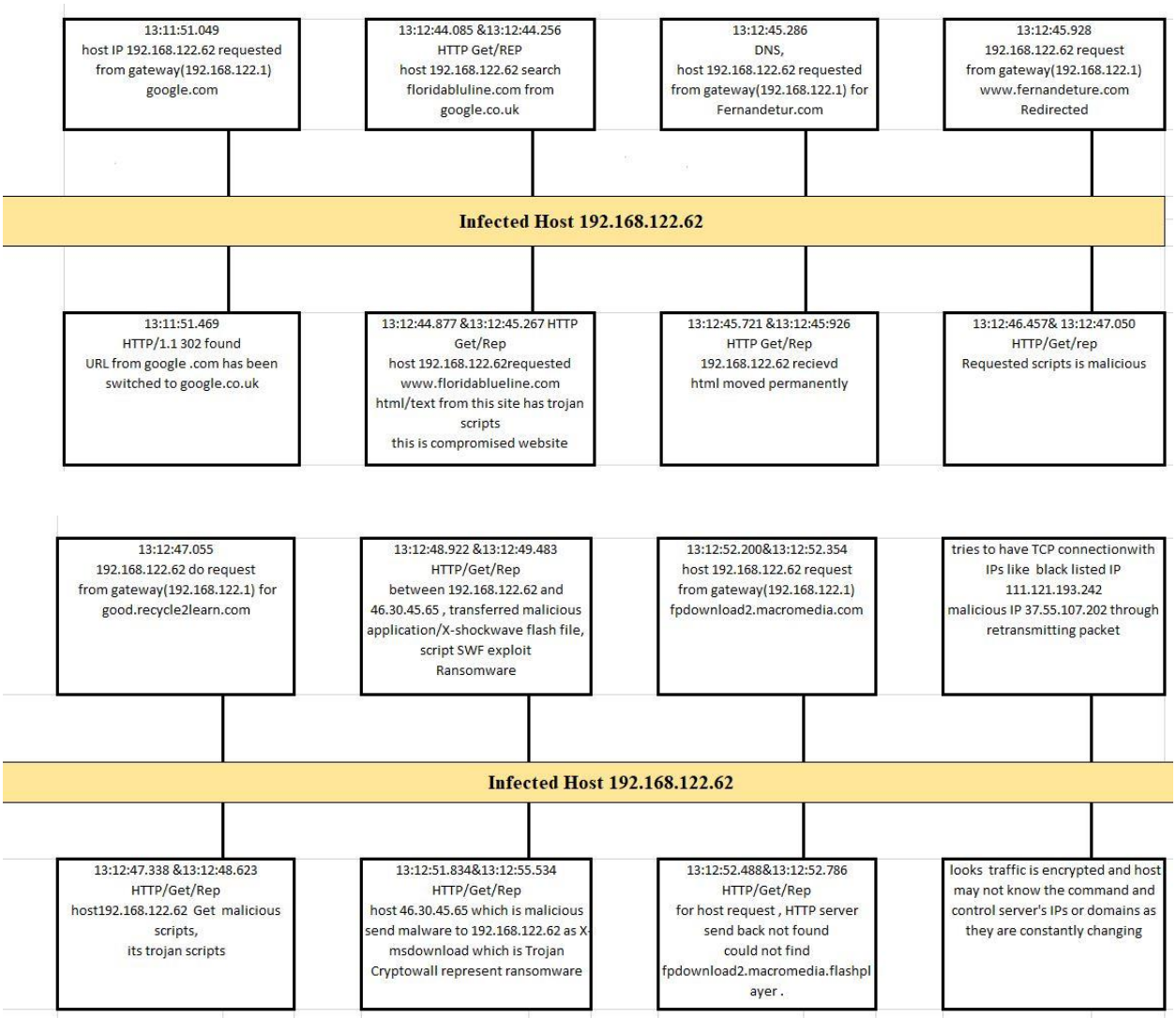
Attacker uses IP address 23.10.250.43 the server ip address is 23.10.250.18 for web server banner in fact Mac spoofing and DNS hijacking.

University of Victoria

6. Give an outline of the attack scenario by describing it in a few paragraphs and by providing a graphical sketch. The attack scenario must include both the infection and post-infection steps

From the first point User in host IP 192.168.122.62 wants to access the web site “ www.google.com”, so they type www.google.com in to their browser and after usual DNS resolution to find IP address for www.google.com, 216.58.208.46, a connection is initiated via TCP to the web server(SYN,SYN/ACK,ACK) ,in this process in packet 8 through HTTP1/1 “302 found” from google.com it switched to google.co.uk. From there user search for floridablueline.com, but we see in packet 524 through 527 when the host received text/html from floridablueline, this file recognized malicious with 27 engines by virustotal. So the infection process starts , and in this website another jpeg file which looks clean but as an interchange file back to the host . floridablueline is the compromised website.
From this point host 192.168.122.62 request access to fernandatur.com, however through transferring several packets we see in packet 553/575 HTTP server respond back with permanent moved, redirection occurred to www.fernandatur.com and that text/html file is script malware. By checking the script within GET request come up from 192.168.122.62 has trojan and script malware. From this point host forwarded to good.recycle2learn.com with IP 46.30.45.65 which is in blacklisted IP address, from packet 758 access requested and packet 764 HTTP when access requested, we have trojan scripts and based on analysis tools and virus total, we have ET CURRENT_EVENTS RIG EK Landing and ET CURRENT_EVENTS Cryptowall docs campaign that represent ransomware. Means the attacker uses script malware and tries to force the host to update and get it infected. We see the host through packet 811/831 received x-shockwave flash which was found by 35 engines in virus total malware, so from this point the attacker has complete control. And another Host IPs address after that which some of them are malicious like 43.225.38.217 and blacklisted like 111.121.193.242 and they have retransmitted continus TCP connection with 192.168.122.62 and looks is in add-arpa which instead of giving back domain name just give the host IPs. so look the traffic is encrypted and host may not know the command and control server's IPs or domains as they are constantly changing.In this

scenario may be attacker uses IP address 23.10.250.43 the server ip address is 23.10.250.18 for web server banner in fact Mac spoofing.



(based on the question body we provided answers on text and graph sketch. All screenshots related to attack scenarios shown in above questions to avoid repetition)

University of Victoria

7. Discuss remediation and mitigation solutions for such threats.

Most ransomware occured because of user-initiated actions such as clicking on malicious links or visiting a malicious or compromised website. In this threat user went to compromised website, floridablue, and then clicked on malicious links which redirect it to malicious website and got infected.Mitigating the risk of ransomware can be done by several methods like regularly scanning the system and network with antivirus program let automatically update the signature. And use whitelisting software which prevent unauthorised applications from executing.adding a warning banner to all emails which remind users about checking security of popups and attachments.
Try to keep all hardware,operating systems,software and applications patched and up to date to have fewer vulnerabilities.
And try to do regularly and automatically backup files, even though it will not stop malware but can make damage of that attack much less.
Another important action to avoid ransomware is training end users about phishing and be aware before visiting unknown websites and also close their browser when they do not use it and stop installing software or giving administrative privileges without knowing the source.