

Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:



Network Topology & Critical Vulnerabilities



Traffic Profile



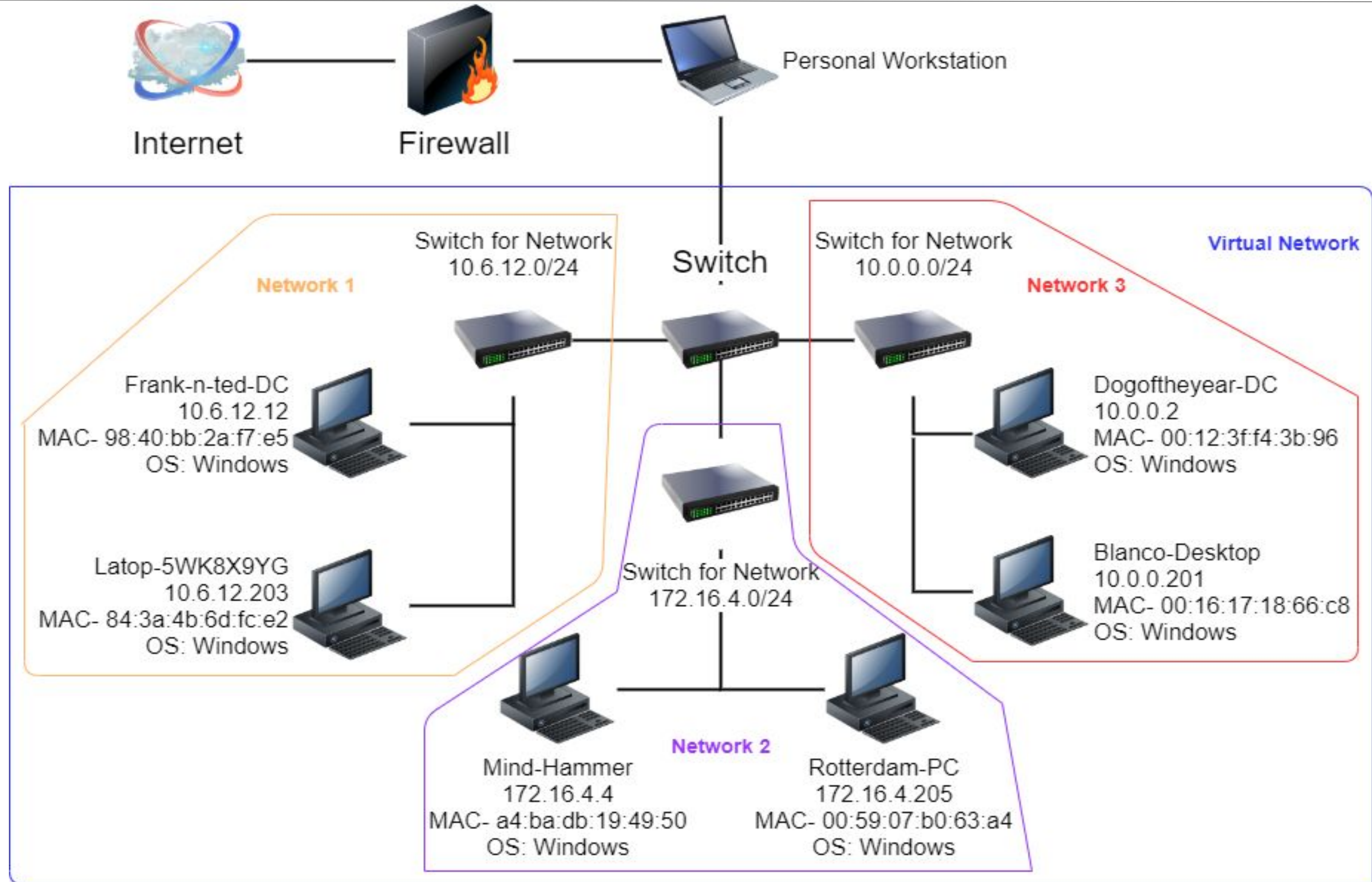
Normal Activity



Malicious Activity

Network Topology & Critical Vulnerabilities

Network Topology



Network Critical Vulnerabilities

Vulnerability	Description	Impact
Unfiltered Web Browsing	Web browsing without content filters on dangerous websites.	This can be a security threat to an organization's server. Downloading malware, viruses or illegal content can cripple a machine.
Illegal downloads	Downloading material on the internet involving violation of copyrights is illegal.	Unauthorized distribution of copyrighted materials is punishable by law and impacts an organization negatively and monetarily (Huge fines).
Torrenting	Torrenting involves downloading and uploading files through the BitTorrent Network from other users devices on the network. It's the most used form of peer-to-peer (P2P) file-sharing.	Downloading these malicious files leads to jeopardizing data safety, and legal trouble for an organization.

Traffic Profile

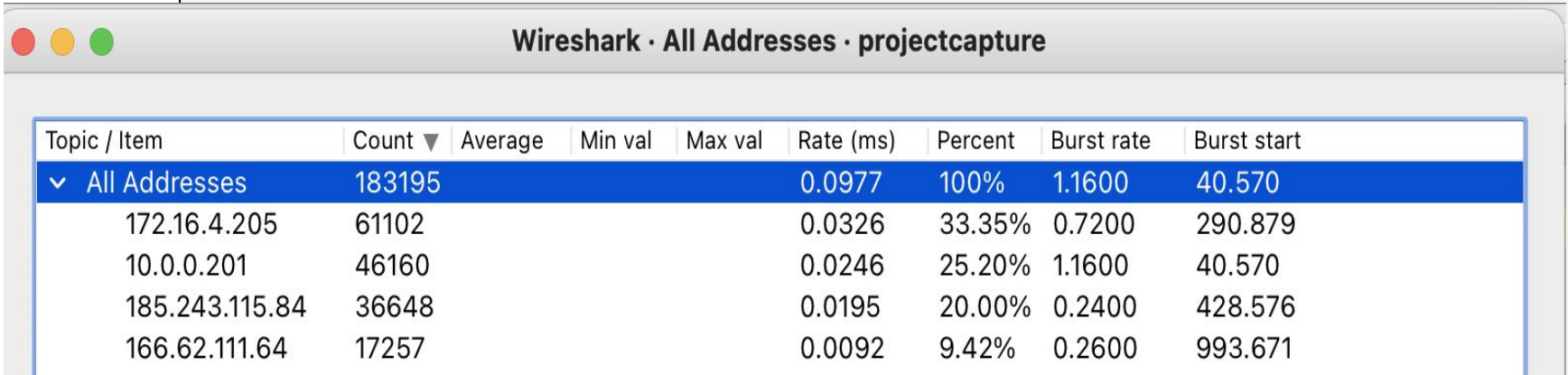
Wireshark Traffic

Using Statistics / Endpoints features in Wireshark we can isolate the clients that are using the most traffic. This can be an indication of what users are potentially breaking company policy by using the network resources for personal reasons.

projectcapture.pcapng							
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help							
Wireshark · Endpoints · projectcapture.pcapng							
Ethernet · 33 IPv4 · 810 IPv6 · 3 TCP · 1374 UDP · 1952							
Address	Packets ^	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Count
172.16.4.205	61,102	53 M	27,729	16 M	33,373	36 M	—
10.0.0.201	46,160	28 M	20,458	2,103 k	25,702	26 M	—
185.243.115.84	36,648	33 M	17,142	17 M	19,506	15 M	—
166.62.111.64	17,257	17 M	12,404	17 M	4,853	370 k	—
10.11.11.200	15,072	7,822 k	7,824	799 k	7,248	7,022 k	—
10.6.12.203	14,820	11 M	5,134	798 k	9,686	10 M	—
64.187.66.143	14,064	10 M	7,620	10 M	6,444	417 k	—
23.43.62.169	12,021	12 M	8,091	12 M	3,930	215 k	—
10.11.11.179	11,612	6,431 k	5,884	641 k	5,728	5,789 k	—
192.168.1.90	10,316	48 M	6,650	47 M	3,666	1,031 k	—
192.168.1.100	10,316	48 M	3,666	1,031 k	6,650	47 M	—
5.101.51.151	8,652	8,493 k	6,524	8,355 k	2,128	137 k	—
10.11.11.11	8,278	1,400 k	3,424	548 k	4,854	852 k	—
10.11.11.217	8,074	3,908 k	4,188	476 k	3,886	3,431 k	—
151.101.50.208	6,540	4,441 k	3,314	4,217 k	3,226	224 k	—
10.6.12.12	5,704	1,401 k	2,664	659 k	3,040	742 k	—
10.6.12.157	4,816	1,619 k	2,462	570 k	2,354	1,049 k	—
10.11.11.195	3,666	1,454 k	1,970	180 k	1,696	1,273 k	—
10.11.11.203	2,758	1,226 k	1,476	249 k	1,282	976 k	—
172.217.6.162	2,412	1,354 k	1,228	1,228 k	1,184	126 k	—
10.0.0.2	2,247	560 k	1,122	206 k	1,125	201 k	—

Our analysis identified the following characteristics of the traffic on the network:

Traffic Profile

Feature	Value	Description
Top Talkers (IP Addresses)	172.16.4.205 10.0.0.201 185.243.115.84	Machines that sent the most traffic. <i>Rotterdam-PC</i> <i>Blanco-Desktop</i> <i>b5689023.green.mattingsolutions.co</i>
Most Common Protocols	HTTP: Hypertext Transfer Protocol DHCP: Dynamic Host Configuration Protocol TCP: Transmission Control Protocol	Three most common protocols on the network. <i>Port 80</i> <i>Port 67/68</i> <i>Port 443/445</i>
# of Unique IP Addresses	183195	Count of observed IP addresses. <div>A screenshot of the Wireshark 'All Addresses' statistics window. The window title is 'Wireshark · All Addresses · projectcapture'. It contains a table with columns: Topic / Item, Count, Average, Min val, Max val, Rate (ms), Percent, Burst rate, and Burst start. The 'All Addresses' row is expanded and highlighted in blue, showing a count of 183195 and a rate of 0.0977. Below it, four individual IP addresses are listed: 172.16.4.205 (61102, 0.0326, 33.35%, 0.7200, 290.879), 10.0.0.201 (46160, 0.0246, 25.20%, 1.1600, 40.570), 185.243.115.84 (36648, 0.0195, 20.00%, 0.2400, 428.576), and 166.62.111.64 (17257, 0.0092, 9.42%, 0.2600, 993.671).</div>
Subnets	10.6.12.0/24	Observed subnet ranges.
# of Malware Species	1 .dll file	Malware binaries identified in traffic. <i>June11.dll</i>

Behavioral Analysis (Normal)

Purpose of Traffic on the Network

The purpose of traffic on the network could be based on factors such as a high volume of traffic over a network on a particular protocol or IP, high source and destination ports, or number of new external IP addresses

“Normal” Activity is defined as follows:

- Who are communications occurring between - source and destination IP
- What are those communications - protocol, port, frequency, volume
- At what time should communications be occurring - within normal business hours

Common examples of “Normal” activity:

- Watching videos on YouTube.
- Logging on to Facebook
- Logging on to Instagram

Behavioral Analysis (Suspicious)

Purpose of Traffic on the Network

Suspicious traffic observed on a network is any suspicious link, file or connection that is being created or received over the network.

Suspicious Activity

- **Users have set up an Active Directory network on the company server**
- **Downloading malicious files (Torrents and infected .avi files)**

Normal Activity

Normal Behavior

- **What kind of traffic did you observe? Which protocol(s)?**
Online traffic. HTTP on port 80
Port 53 DNS and UDP
- **What, specifically, was the user doing?**

NetworkMiner 2.6 interface showing DNS traffic filtered by 'youtube'. The table displays columns: Client Port, Server, Server Port, IP TTL, DNS TTL (time), Transaction ID, Type, DNS Query, DNS Answer, and Alexa Top 1M.

Client Port	Server	Server Port	IP TTL	DNS TTL (time)	Transaction ID	Type	DNS Query	DNS Answer	Alexa Top 1M
58565	10.0.0.2 [DogOfTheYear-DC.dogoftheyear.net] (Windows)	53	128	00:04:59	0x33A7	0x0001 (Host Address)	fcmatch.youtube.com	216.58.218.206	N/A (Pro version only)
58565	10.0.0.2 [DogOfTheYear-DC.dogoftheyear.net] (Windows)	53	128	00:04:59	0x33A7	0x0001 (Host Address)	fcmatch.youtube.com	216.58.218.206	N/A (Pro version only)
49618	10.11.11.11 [okay-boomer-dc.okay-boomer.info] [okay-bo...	53	128	23:53:27	0x72CB	0x0005 (CNAME)	www.youtube.com	youtube-ui.l.google.com	N/A (Pro version only)
49618	10.11.11.11 [okay-boomer-dc.okay-boomer.info] [okay-bo...	53	128	00:04:56	0x72CB	0x0001 (Host Address)	youtube-ui.l.google.com	216.58.194.142	N/A (Pro version only)
49618	10.11.11.11 [okay-boomer-dc.okay-boomer.info] [okay-bo...	53	128	00:04:56	0x72CB	0x0001 (Host Address)	youtube-ui.l.google.com	172.217.12.46	N/A (Pro version only)
49618	10.11.11.11 [okay-boomer-dc.okay-boomer.info] [okay-bo...	53	128	00:04:56	0x72CB	0x0001 (Host Address)	youtube-ui.l.google.com	172.217.12.78	N/A (Pro version only)
49618	10.11.11.11 [okay-boomer-dc.okay-boomer.info] [okay-bo...	53	128	00:04:56	0x72CB	0x0001 (Host Address)	youtube-ui.l.google.com	216.58.194.46	N/A (Pro version only)
49618	10.11.11.11 [okay-boomer-dc.okay-boomer.info] [okay-bo...	53	128	00:04:56	0x72CB	0x0001 (Host Address)	youtube-ui.l.google.com	216.58.194.78	N/A (Pro version only)
49618	10.11.11.11 [okay-boomer-dc.okay-boomer.info] [okay-bo...	53	128	00:04:56	0x72CB	0x0001 (Host Address)	youtube-ui.l.google.com	172.217.6.174	N/A (Pro version only)
49618	10.11.11.11 [okay-boomer-dc.okay-boomer.info] [okay-bo...	53	128	00:04:56	0x72CB	0x0001 (Host Address)	youtube-ui.l.google.com	172.217.14.174	N/A (Pro version only)
49618	10.11.11.11 [okay-boomer-dc.okay-boomer.info] [okay-bo...	53	128	00:04:56	0x72CB	0x0001 (Host Address)	youtube-ui.l.google.com	172.217.1.142	N/A (Pro version only)
49618	10.11.11.11 [okay-boomer-dc.okay-boomer.info] [okay-bo...	53	128	00:04:56	0x72CB	0x0001 (Host Address)	youtube-ui.l.google.com	172.217.1.238	N/A (Pro version only)
49618	10.11.11.11 [okay-boomer-dc.okay-boomer.info] [okay-bo...	53	128	00:04:56	0x72CB	0x0001 (Host Address)	youtube-ui.l.google.com	172.217.9.142	N/A (Pro version only)
49618	10.11.11.11 [okay-boomer-dc.okay-boomer.info] [okay-bo...	53	128	00:04:56	0x72CB	0x0001 (Host Address)	youtube-ui.l.google.com	172.217.9.174	N/A (Pro version only)
49618	10.11.11.11 [okay-boomer-dc.okay-boomer.info] [okay-bo...	53	128	00:04:56	0x72CB	0x0001 (Host Address)	youtube-ui.l.google.com	216.58.193.142	N/A (Pro version only)
49618	10.11.11.11 [okay-boomer-dc.okay-boomer.info] [okay-bo...	53	128	00:04:56	0x72CB	0x0001 (Host Address)	youtube-ui.l.google.com	172.217.2.238	N/A (Pro version only)
49618	10.11.11.11 [okay-boomer-dc.okay-boomer.info] [okay-bo...	53	128	00:04:56	0x72CB	0x0001 (Host Address)	youtube-ui.l.google.com	172.217.9.14	N/A (Pro version only)
49618	10.11.11.11 [okay-boomer-dc.okay-boomer.info] [okay-bo...	53	128	00:04:56	0x72CB	0x0001 (Host Address)	youtube-ui.l.google.com	216.58.194.110	N/A (Pro version only)
49627	10.11.11.11 [okay-boomer-dc.okay-boomer.info] [okay-bo...	53	128	23:53:27	0x72CB	0x0005 (CNAME)	www.youtube.com	youtube-ui.l.google.com	N/A (Pro version only)

Using company hours for

NetworkMiner 2.6 interface showing traffic filtered by 'youtube'. The table displays columns: Frame nr., Timestamp, Client, Client Port, Server, Server Port, IP TTL, DNS TTL (time), Transaction ID, Type, and DNS Query.

Frame nr.	Timestamp	Client	Client Port	Server	Server Port	IP TTL	DNS TTL (time)	Transaction ID	Type	DNS Query
56822	2021-05-29 17:30:04 UTC	10.0.0.201 [BLANCO-DESKTOP] [BLANCO-DESKTOP.do...	58565	10.0.0.2 [DogOfTheYear-DC.dogoftheyear.net] (Windows)	53	128	00:04:59	0x33A7	0x0001 (Host Address)	fcmatch.youtube.com
139771	2021-05-29 17:44:16 UTC	10.0.0.201 [BLANCO-DESKTOP] [BLANCO-DESKTOP.do...	58565	10.0.0.2 [DogOfTheYear-DC.dogoftheyear.net] (Windows)	53	128	00:04:59	0x33A7	0x0001 (Host Address)	fcmatch.youtube.com
14345	2021-05-29 17:25:10 UTC	10.11.11.11 [okay-boomer-dc.okay-boomer.info] [okay-bo...	63129	216.239.38.10	53	108	00:05:00	0xF875	0x0001 (Host Address)	youtube-ui.l.google.com

watching videos on youtube

Logging on to Facebook

Logging on to Instagram

Normal Behavior

IN SUMMARY:

- For normal behavior we observed Online HTTP traffic On port 80 and Port 53 DNS
- Users were using company hours for personal use (stealing time) browsing sites such as Youtube, Facebook, Instagram

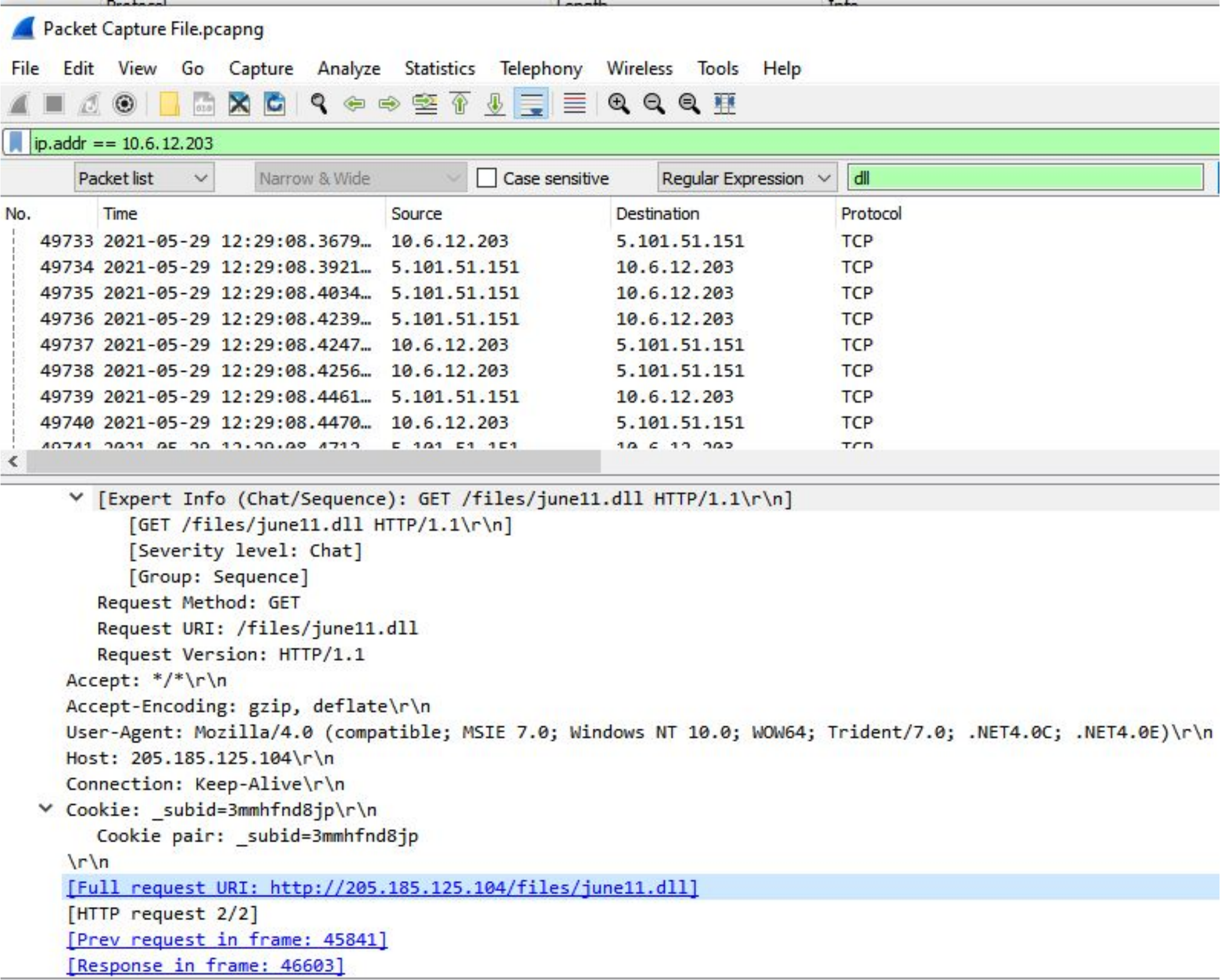
Hosts (1132) Files (2050) Images (210) Messages Credentials (108) Sessions (2610) DNS (5017) Parameters (50516) Keywords Anomalies											
Filter keyword: youtube <input type="checkbox"/> Case sensitive ExactPhrase Any column Clear Apply											
Frame nr.	Timestamp	Client	Client Port	Server	Server Port	IP TTL	DNS TTL (time)	Transaction ID	Type	DNS Query	
56822	2021-05-29 17:30:04 UTC	10.0.0.201 [BLANCO-DESKTOP] [BLANCO-DESKTOP.do...	58565	10.0.0.2 [DogOfTheYear-DC.dogoftheyear.net] (Windows)	53	128	00:04:59	0x33A7	0x0001 (Host Address)	fcmatch.youtube.com	
139771	2021-05-29 17:44:16 UTC	10.0.0.201 [BLANCO-DESKTOP] [BLANCO-DESKTOP.do...	58565	10.0.0.2 [DogOfTheYear-DC.dogoftheyear.net] (Windows)	53	128	00:04:59	0x33A7	0x0001 (Host Address)	fcmatch.youtube.com	
19395	2021-05-29 17:25:10 UTC	10.11.11.11 [okay-boomer-dc.okay-boomer.info] [okay-bo...	63129	216.239.38.10	53	108	00:05:00	0xF875	0x0001 (Host Address)	youtube.googleapis.com	
106825	2021-05-29 17:39:54 UTC	10.11.11.179 [MACBOOKPRO-8843] [Roger-MacBook-Pro...	49524	10.11.11.11 [okay-boomer-dc.okay-boomer.info] [okay-bo...	53	128	00:00:00	0x0635	0x0000	www.facebook.com	
71338	2021-05-29 17:32:27 UTC	172.16.4.205 [Rotterdam-PC] [ROTTERDAM-PC] [rotterda...	49771	172.16.4.4 [Mind-Hammer-DC.mind-hammer.net] (Windows)	53	128	00:59:59	0x218E	0x0005 (CNAME)	api.instagram.com	
71338	2021-05-29 17:32:27 UTC	172.16.4.205 [Rotterdam-PC] [ROTTERDAM-PC] [rotterda...	49771	172.16.4.4 [Mind-Hammer-DC.mind-hammer.net] (Windows)	53	128	00:00:16	0x218E	0x0001 (Host Address)	instagram.c10r.facebook.com	
71403	2021-05-29 17:32:27 UTC	172.16.4.205 [Rotterdam-PC] [ROTTERDAM-PC] [rotterda...	54103	172.16.4.4 [Mind-Hammer-DC.mind-hammer.net] (Windows)	53	128	00:00:16	0xC53D	0x0001 (Host Address)	instagram.c10r.facebook.com	
154231	2021-05-29 17:46:38 UTC	172.16.4.205 [Rotterdam-PC] [ROTTERDAM-PC] [rotterda...	49771	172.16.4.4 [Mind-Hammer-DC.mind-hammer.net] (Windows)	53	128	00:59:59	0x218E	0x0005 (CNAME)	api.instagram.com	
154231	2021-05-29 17:46:38 UTC	172.16.4.205 [Rotterdam-PC] [ROTTERDAM-PC] [rotterda...	49771	172.16.4.4 [Mind-Hammer-DC.mind-hammer.net] (Windows)	53	128	00:00:16	0x218E	0x0001 (Host Address)	instagram.c10r.facebook.com	
154296	2021-05-29 17:46:39 UTC	172.16.4.205 [Rotterdam-PC] [ROTTERDAM-PC] [rotterda...	54103	172.16.4.4 [Mind-Hammer-DC.mind-hammer.net] (Windows)	53	128	00:00:16	0xC53D	0x0001 (Host Address)	instagram.c10r.facebook.com	

Hosts (1132) Files (2050) Images (210) Messages Credentials (108) Sessions (2610) DNS (5017) Parameters (50516) Keywords Anomalies											
Filter keyword: Walmart <input type="checkbox"/> Case sensitive ExactPhrase Any column Clear Apply											
Frame nr.	Timestamp	Client	Client Port	Server	Server Port	IP TTL	DNS TTL (time)	Transaction ID	Type	DNS Query	
56401	2021-05-29 17:30:02 UTC	10.0.0.201 [BLANCO-DESKTOP] [BLANCO-DESKTOP.do...	53417	10.0.0.2 [DogOfTheYear-DC.dogoftheyear.net] (Windows)	53	128	00:04:48	0x4AF3	0x0005 (CNAME)	beacon.walmart.com	
56401	2021-05-29 17:30:02 UTC	10.0.0.201 [BLANCO-DESKTOP] [BLANCO-DESKTOP.do...	53417	10.0.0.2 [DogOfTheYear-DC.dogoftheyear.net] (Windows)	53	128	00:04:59	0x4AF3	0x0001 (Host Address)	beacon-cdn.walmart.com.akadns.net	
139344	2021-05-29 17:44:14 UTC	10.0.0.201 [BLANCO-DESKTOP] [BLANCO-DESKTOP.do...	53417	10.0.0.2 [DogOfTheYear-DC.dogoftheyear.net] (Windows)	53	128	00:04:48	0x4AF3	0x0005 (CNAME)	beacon.walmart.com	
139344	2021-05-29 17:44:14 UTC	10.0.0.201 [BLANCO-DESKTOP] [BLANCO-DESKTOP.do...	53417	10.0.0.2 [DogOfTheYear-DC.dogoftheyear.net] (Windows)	53	128	00:04:59	0x4AF3	0x0001 (Host Address)	beacon-cdn.walmart.com.akadns.net	

Malicious Activity

Illegal Downloads

- What kind of traffic did you observe?
Lots of downloading and searching websites for suspicious files. Downloading malicious files between machines.
Which protocol(s)? HTTP port 80
- What, specifically, was the user doing?
Downloading Malware (June11.dll from source IP 205.185.125.104) and a video file (Betty_Boop_Rhythm_on_the_reservation.avi)
- What are the IP addresses used in the actual infection traffic?
10.0.0.201
10.6.12.203



Malicious Behavior

Summarize the following:

- They were visiting websites outside of normal activity using HTTP & TCP protocols.
- The User was downloading torrents; and the malware was downloaded from another machine
 - A torrent file, betty_boop_rhythm_on_the_reservation.avi
 - A june11.dll malware file

```
[Bytes sent since last PSH flag: 535]
[Timestamps]
[Time since first frame in this TCP stream: 0.012277000 seconds]
[Time since previous frame in this TCP stream: 0.009435900 seconds]
TCP payload (535 bytes)
Hypertext Transfer Protocol
GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
[GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)\r\n
Host: 205.185.125.104\r\n
Connection: Keep-Alive\r\n
Cookie: _subid=3mmhfd8jp\r\n
Cookie pair: _subid=3mmhfd8jp
\r\n
[Full request URI: http://205.185.125.104/files/june11.dll]
[HTTP request 2/2]
[Prev request in frame: 45841]
[Response in frame: 46603]
```



Malicious Screenshots

Packet Capture File.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.0.0.201

Packet list Narrow & Wide Case sensitive Regular Expression .avi Find Cancel

No.	Time	Source	Destination	Protocol	Length
57090	2021-05-29 12:30:05.5247...	10.0.0.201	168.215.194.14	HTTP	
57107	2021-05-29 12:30:05.6131...	50.18.44.131	10.0.0.201	HTTP	
57185	2021-05-29 12:30:06.5446...	10.0.0.201	52.94.240.125	HTTP	
57239	2021-05-29 12:30:07.2720...	10.0.0.201	168.215.194.14	HTTP	
57309	2021-05-29 12:30:08.2371...	168.215.194.14	10.0.0.201	HTTP	
57312	2021-05-29 12:30:08.2447...	52.94.240.125	10.0.0.201	HTTP	
57314	2021-05-29 12:30:08.2649...	168.215.194.14	10.0.0.201	HTTP	
57318	2021-05-29 12:30:08.2969...	168.215.194.14	10.0.0.201	HTTP	
57326	2021-05-29 12:30:08.3120...	10.0.0.201	52.94.240.125	HTTP	
57348	2021-05-29 12:30:08.5706...	52.94.240.125	10.0.0.201	HTTP	

[Bytes sent since last PSH flag: 535]

Timestamps

[Time since first frame in this TCP stream: 0.012277000 seconds]

[Time since previous frame in this TCP stream: 0.009435900 seconds]

TCP payload (535 bytes)

Hypertext Transfer Protocol

GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n]

[GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n]

[Severity level: Chat]

[Group: Sequence]

0000 00 09 b7 27 a1 3e 00 16 17 18 66 c8 08 00 45 00 ...'>...f...E

0010 02 3f 76 d1 40 00 80 06 0c 39 0a 00 00 c9 a8 d7 ...v:@...9.....

0020 c2 0e c2 aa 00 50 97 b7 b1 25 75 99 6b 48 50 18P...%u.kHP

0030 ff ff 31 06 00 00 47 45 54 20 2f 62 74 2f 62 74 ..1...GE T /bt/bt

0040 64 6f 77 6e 6c 6f 61 64 2e 70 68 70 3f 74 79 70 download .php?typ

0050 65 3d 74 6f 72 72 65 6e 74 26 66 69 6c 65 3d 42 e=torren t&file=B

0060 65 74 74 79 5f 42 6f 6f 70 5f 52 68 79 74 68 6d etty_Boo p_Rhythm

0070 5f 6f 6e 5f 74 68 65 5f 52 65 73 65 72 76 61 74 _on_the_ Reservat

0080 69 6f 6e 2e 61 76 69 2e 74 6f 72 72 65 6e 74 20 ion.avi. torrent

0090 48 54 54 50 2f 31 2e 31 0d 0a 52 65 66 65 72 65 HTTP/1.1 ..Refere

00a0 72 3a 20 68 74 74 70 3a 2f 2f 70 75 62 6c 69 63 r: http: //public

00b0 64 6f 6d 61 69 6e 74 6f 72 72 65 6e 74 73 2e 69 domain to rrents.i

00c0 6e 66 6f 2f 6e 73 68 6f 77 6d 6f 76 69 65 2e 68 nfo/nsho wmovie.h

00d0 74 6d 6c 3f 6d 6f 76 69 65 69 64 3d 35 31 33 0d tml?movi eid=513

No packet contained that string in its Info column.

Packets: 178973 · Displayed: 32714 (18.3%) Profile: Default

Packet Capture File.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.6.12.203

Packet list Narrow & Wide Case sensitive Regular Expression dll

No.	Time	Source	Destination	Protocol
49733	2021-05-29 12:29:08.3679...	10.6.12.203	5.101.51.151	TCP
49734	2021-05-29 12:29:08.3921...	5.101.51.151	10.6.12.203	TCP
49735	2021-05-29 12:29:08.4034...	5.101.51.151	10.6.12.203	TCP
49736	2021-05-29 12:29:08.4239...	5.101.51.151	10.6.12.203	TCP
49737	2021-05-29 12:29:08.4247...	10.6.12.203	5.101.51.151	TCP
49738	2021-05-29 12:29:08.4256...	10.6.12.203	5.101.51.151	TCP
49739	2021-05-29 12:29:08.4461...	5.101.51.151	10.6.12.203	TCP
49740	2021-05-29 12:29:08.4470...	10.6.12.203	5.101.51.151	TCP
49741	2021-05-29 12:29:08.4712...	5.101.51.151	10.6.12.203	TCP

[Expert Info (Chat/Sequence): GET /files/june11.dll HTTP/1.1\r\n]

[GET /files/june11.dll HTTP/1.1\r\n]

[Severity level: Chat]

[Group: Sequence]

Request Method: GET

Request URI: /files/june11.dll

Request Version: HTTP/1.1

Accept: */*\r\n

Accept-Encoding: gzip, deflate\r\n

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)\r\n

Host: 205.185.125.104\r\n

Connection: Keep-Alive\r\n

Cookie: _subid=3mmhfd8jp\r\n

Cookie pair: _subid=3mmhfd8jp

\r\n

[Full request URI: http://205.185.125.104/files/june11.dll]

[HTTP request 2/2]

[Prev request in frame: 45841]

[Response in frame: 46603]

17



The End