Final Engagement
Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

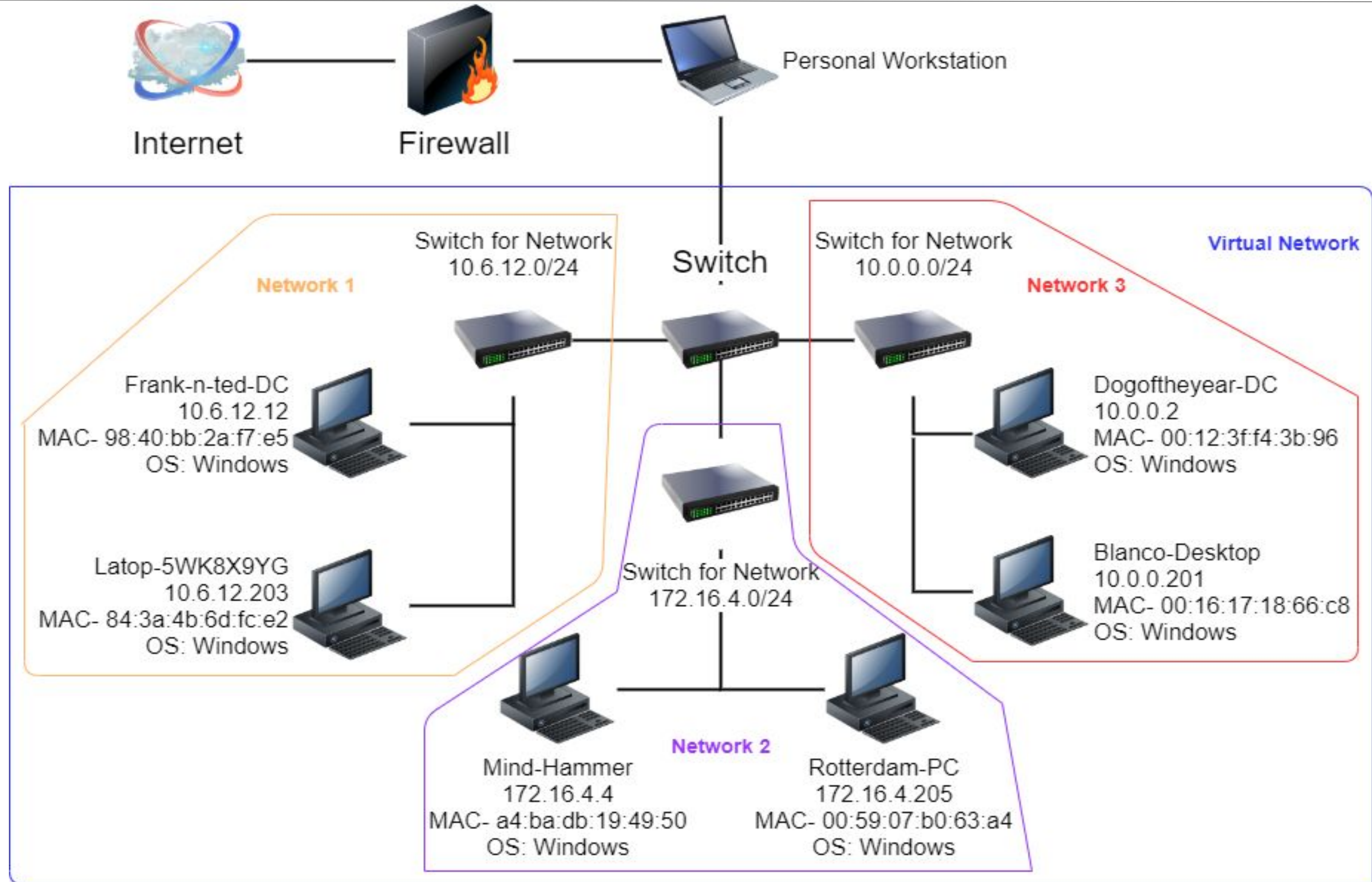**Network Topology & Critical Vulnerabilities**

Traffic Profile

Normal Activity

Malicious Activity

Network Topology & Critical Vulnerabilities

Network Topology

Network Critical Vulnerabilities

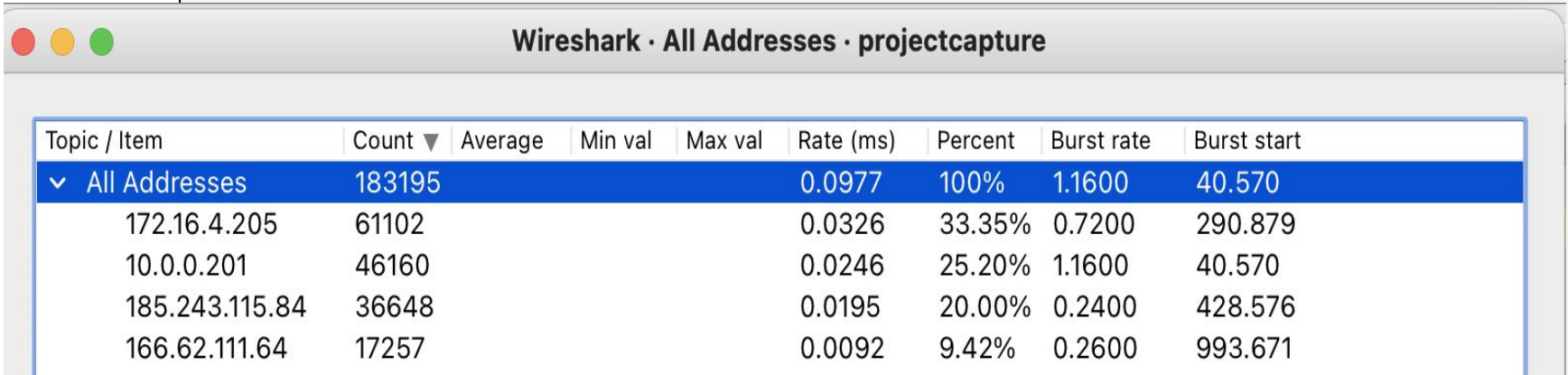| Vulnerability	Description	Impact
Unfiltered Web Browsing	Web browsing without content filters on dangerous websites.	This can be a security threat to an organization's server. Downloading malware, viruses or illegal content can cripple a machine.
Illegal downloads	Downloading material on the internet 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.

Address	Packets ^	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Cou
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	2,347	568 k	1,132	286 k	1,215	281 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.** *Rotterdam-PC* *Blanco-Desktop* *b5689023.green.mattingsolutions.co*
Most Common Protocols	*HTTP: Hypertext Transfer Protocol* *DHCP: Dynamic Host Configuration Protocol* *TCP: Transmission Control Protocol*	**Three most common protocols on the network.** *Port 80* *Port 67/68* *Port 443/445*
# of Unique IP Addresses	*183195*	*Count of observed IP addresses.*
Subnets	*10.6.12.0/24*	*Observed subnet ranges.*
# of Malware Species	*1 .dll file*	**Malware binaries identified in traffic.** *June11.dll*

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?***

  Using company hours for

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 ☐ Case sensitive ExactPhrase ▾ Any column ▾ Clear App

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-boo...	63129	216.239.38.10	53	108	00:05:00	0xF875	0x0001 (Host Address)	youtube-ui.l.google.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-boo...	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] [R̶O̶T̶T̶E̶R̶D̶A̶M̶-̶P̶C̶] [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

172.16.4.205 [Rotterdam-PC] [ROTTERDAM-PC] [rotterdam-pc] (Windows)

Hosts (1132) | Files (2050) | Images (210) | Messages | Credentials (108) | Sessions (2610) | DNS (5017) | Parameters (50516) | Keywords | Anomalies

Filter keyword: Walmart ☐ 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
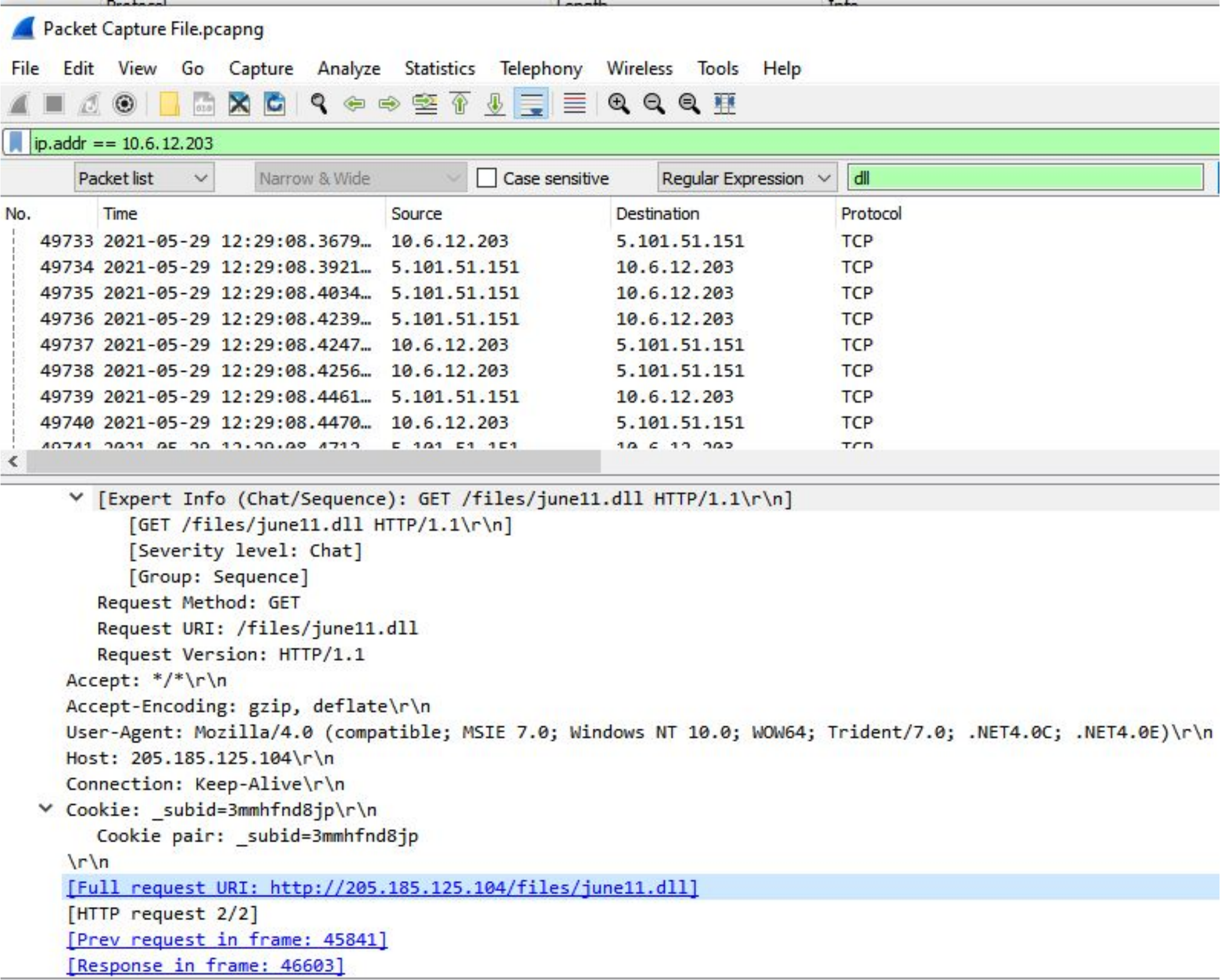
Malicious Behavior

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

Malicious Screenshots

The End