Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

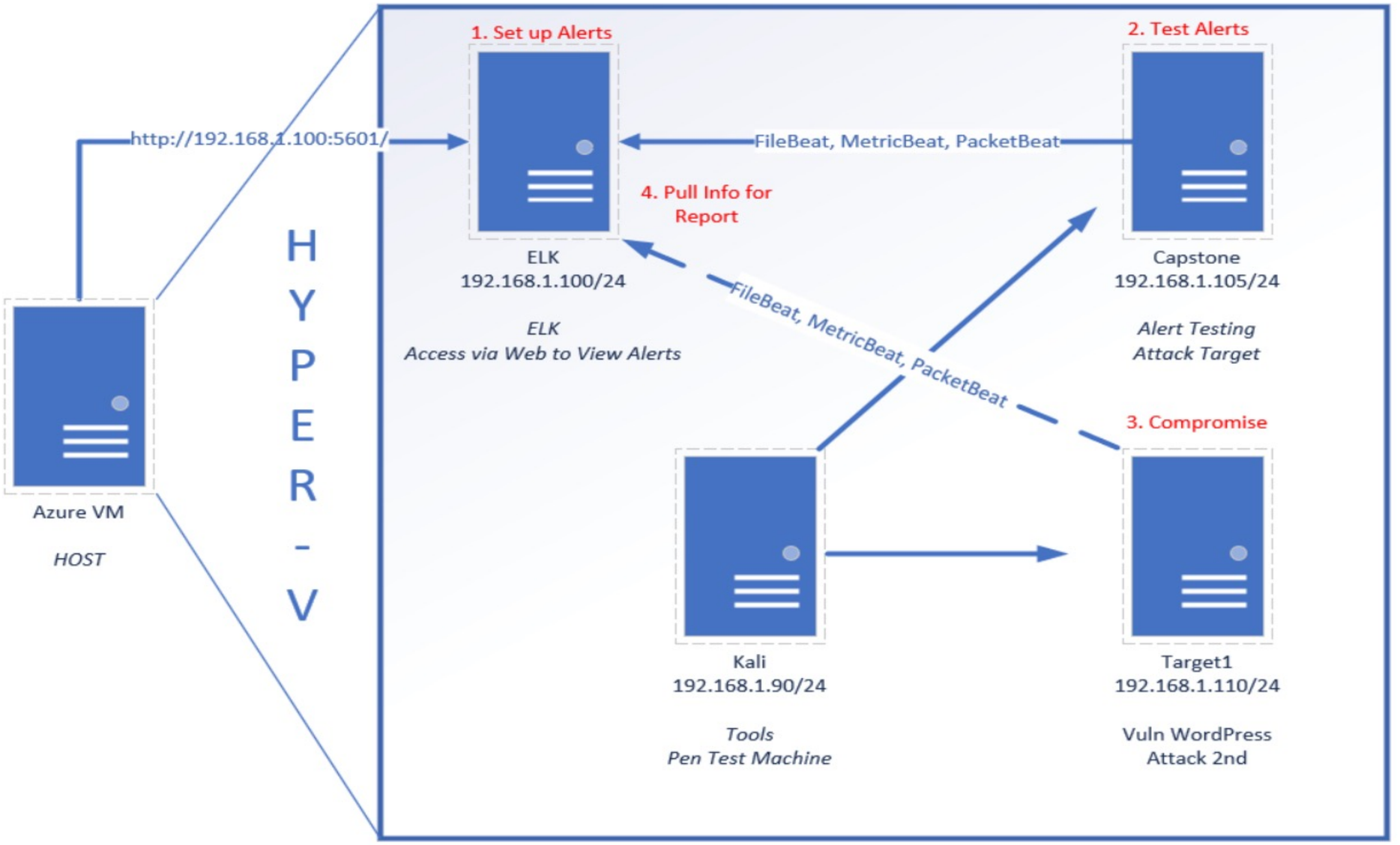
Pooja
Selena
Alajuwon
Deborah
Mustafa
Derrick
Andrea
Pierre
Emmanuel

Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range: 192.168.1.124
Netmask:255.255.0
Gateway: 192.168.1.1

Machines
IPv4:192.168.1.100
OS: Linux
Host name: ELK

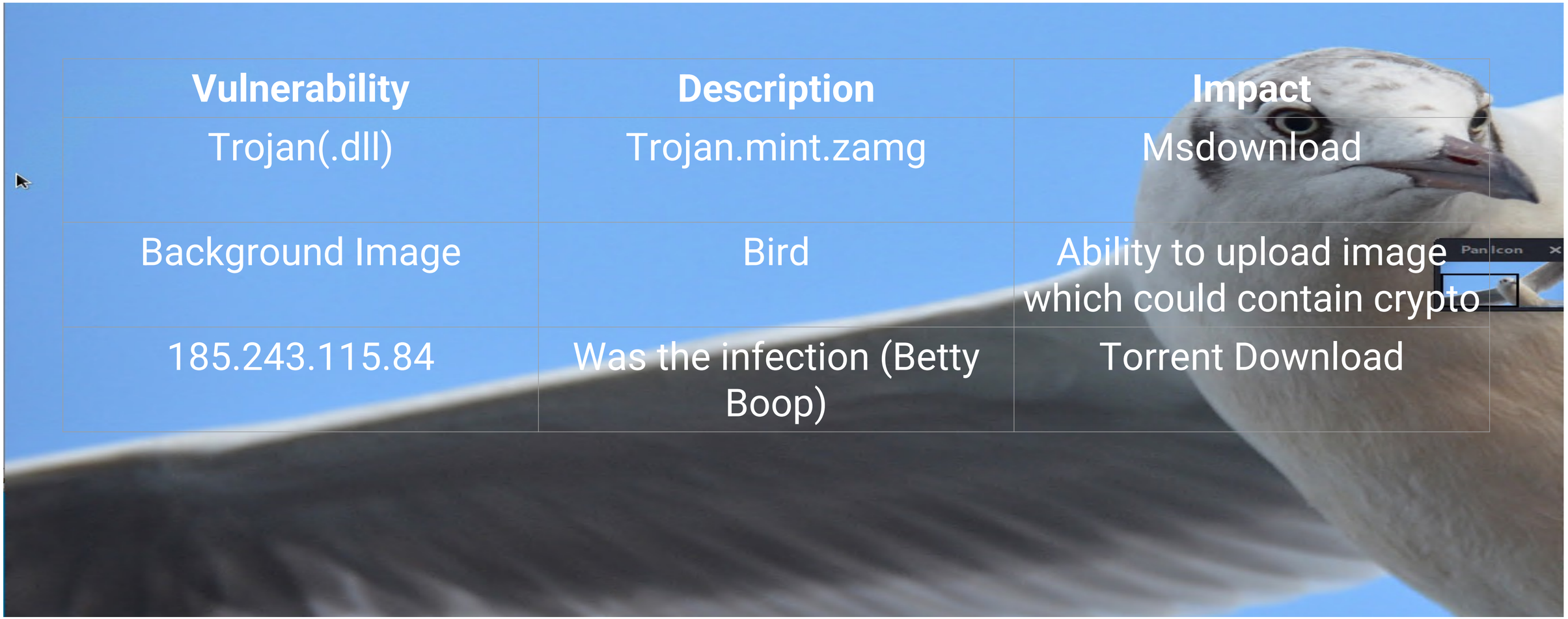
IPv4:192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4:192.168.1.110
OS: Linux
Hostname: Target 1

Critical Vulnerabilities: Target 1

Our assessment uncovered the following critical vulnerabilities in **Target**



Vulnerability	Description	Impact
Trojan(.dll)	Trojan.mint.zamg	Msdownload
Background Image	Bird	Ability to upload image which could contain crypto
185.243.115.84	Was the infection (Betty Boop)	Torrent Download

Traffic Profile

Traffic Profile

Feature	Value	Description
Top Talkers (IP Addresses)	172.16.4.205 /24	Machines that sent the most traffic.
Most Common Protocols	http Tcp Krb5 ldap	Three most common protocols on the network.
# of Unique IP Addresses	185.275.115.84 10.0.0.201 10.6.12.2003	Count of observed IP addresses.
Subnets	255.255.255.255 10.0.0.2 172.16.4.4	Observed subnet ranges.
# of Malware Species	Trojan	Number of malware binaries identified in traffic.

Behavioral Analysis

Purpose of Traffic on the Network

Users were observed engaging in the following kinds of activity.

“Normal” Activity

- Watching YouTube, reading the news.

Suspicious Activity

- Sending malware, skype, created their own broad cast server

Normal Activity

Normal Web Browser Activity

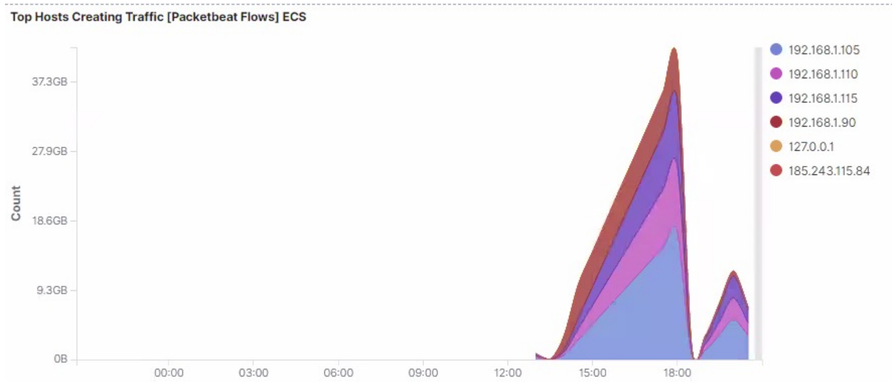
Website visited

DNS Protocol [Packetbeat] ECS

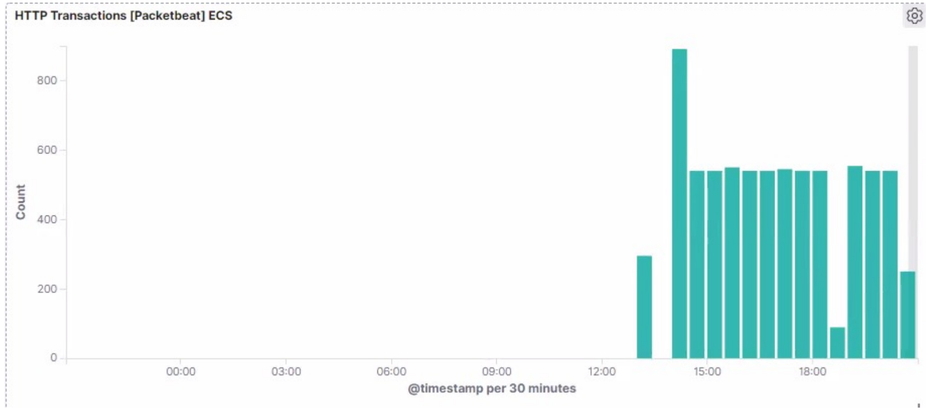
1–50 of 3519

Time	server.ip	destination.ip	dns.question.name	status
May 8, 2021 @ 20:38:55.071	168.63.129.16	168.63.129.16	www.google.com	OK
May 8, 2021 @ 20:27:55.061	168.63.129.16	168.63.129.16	www.google.com	OK
May 8, 2021 @ 20:22:54.031	168.63.129.16	168.63.129.16	www.google.com	OK
May 8, 2021 @ 20:17:55.052	168.63.129.16	168.63.129.16	www.google.com	OK
May 8, 2021 @ 20:13:55.048	168.63.129.16	168.63.129.16	www.google.com	OK
May 8, 2021 @ 20:13:43.616	168.63.129.16	168.63.129.16	safebrowsing.googleapis.com	OK
May 8, 2021 @ 20:10:55.046	168.63.129.16	168.63.129.16	www.google.com	OK
May 8, 2021 @ 20:07:55.043	168.63.129.16	168.63.129.16	www.google.com	OK

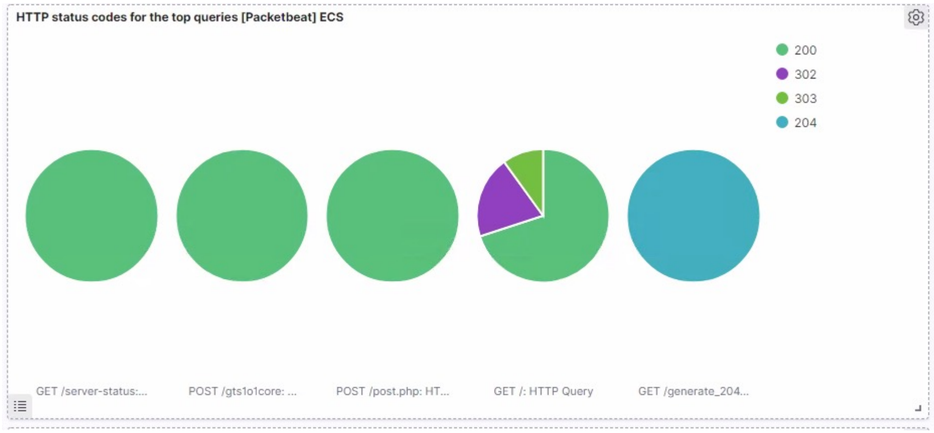
IP visited



Normal activity before spike in traffic



Interesting response codes: 302 & 303

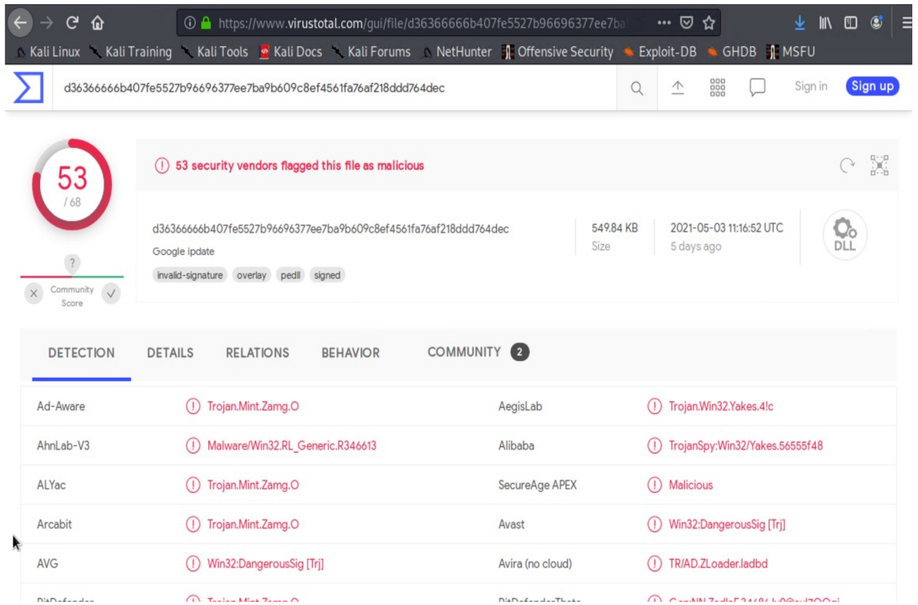


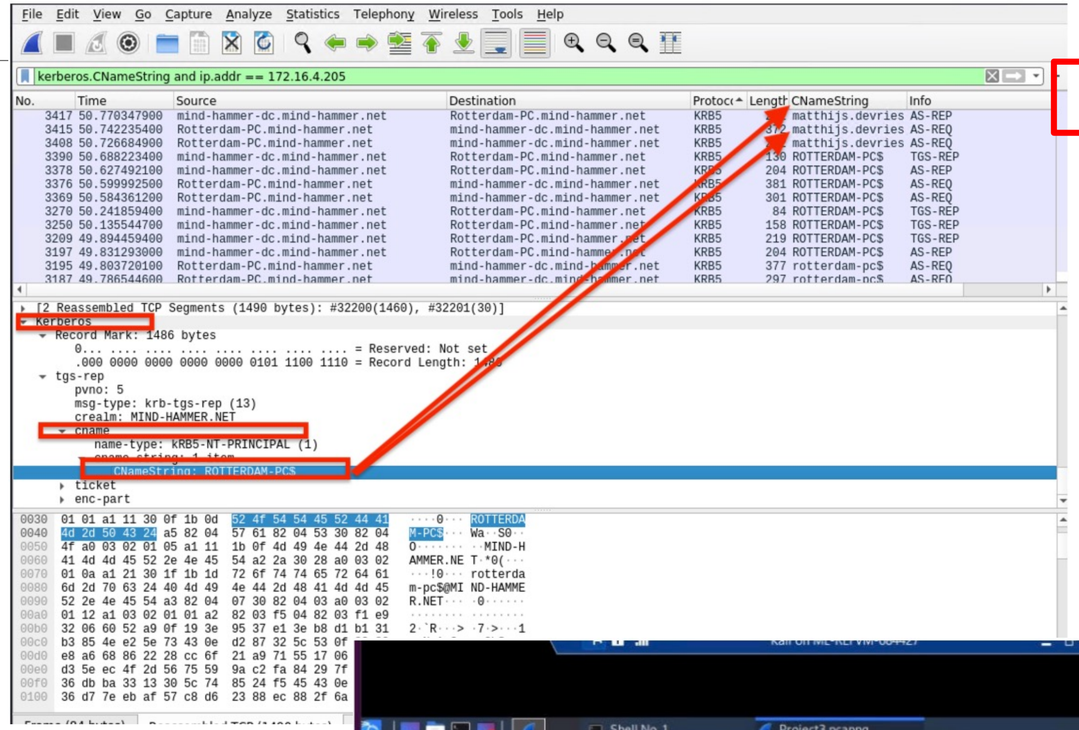
Malicious Activity

Watching Youtube video

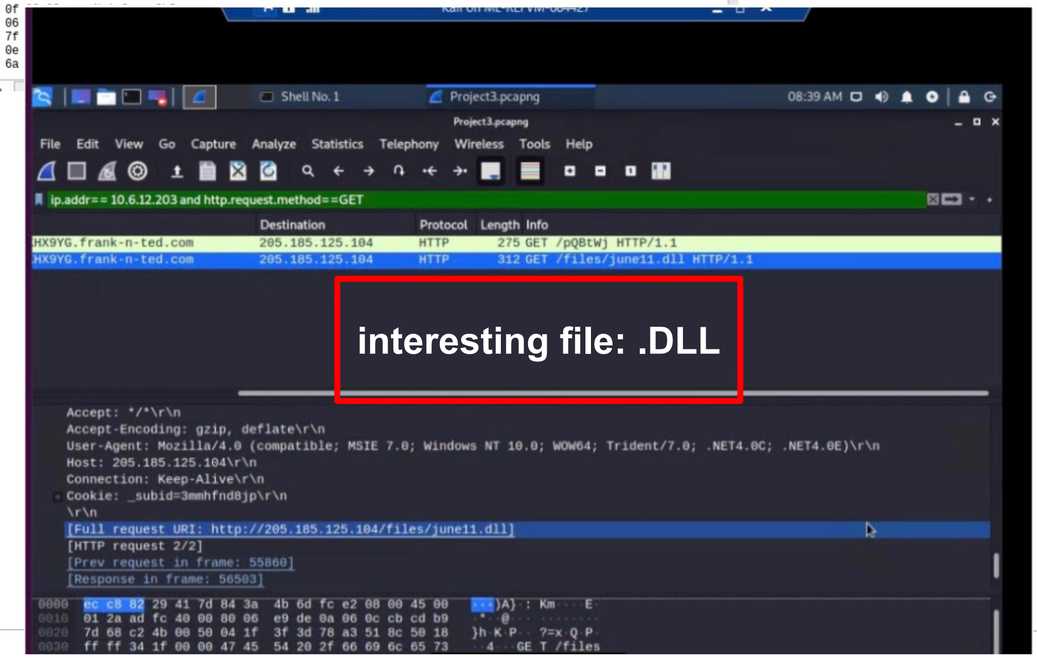
Summarize the following:

- What kind of traffic did you observe? Which protocol(s)?
  - HTTP reposed “GET” response with response code “200”
  - Download .dll Malware file





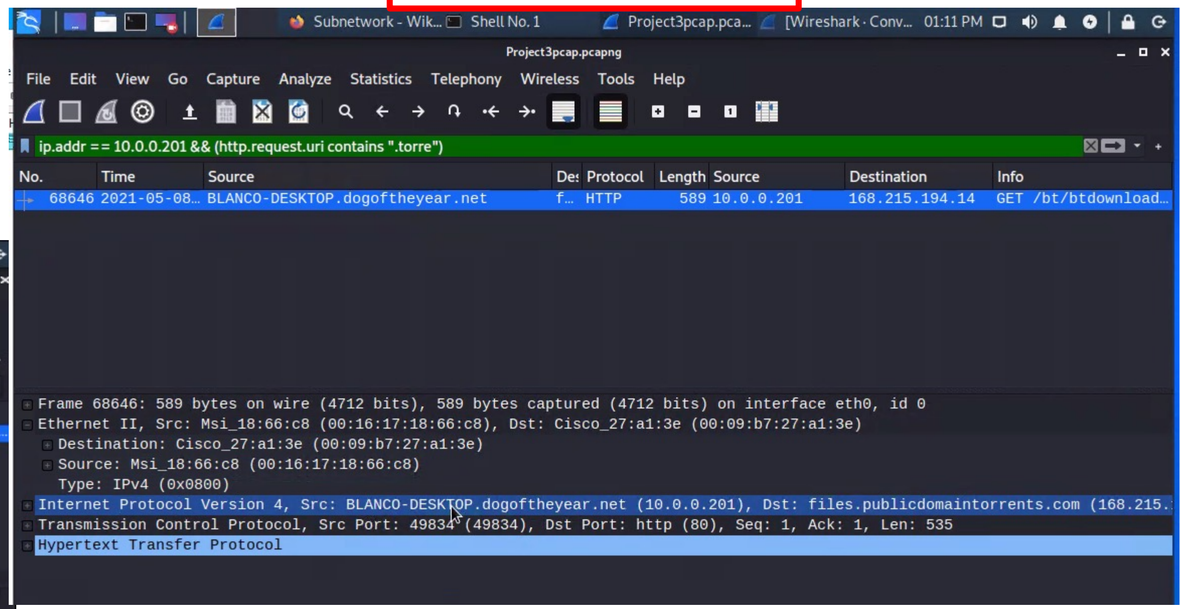
User: matthijs



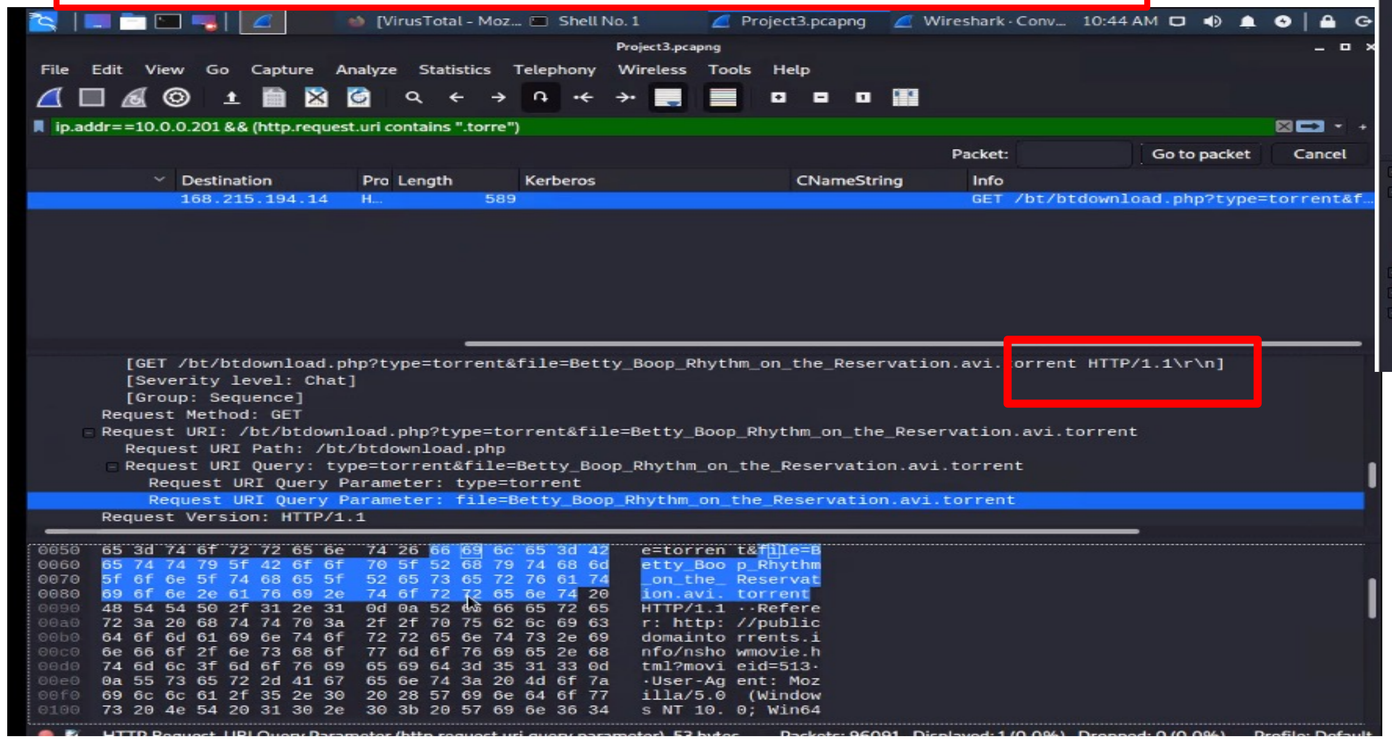
Torrent download

- Type of Traffic: Bittorrent
- Type of protocol: HTTP

User: BLANCO



Interesting file: Torrent with large packet and bit size



Torrent file with large packet and bit size is suspicious

The End