

# **Final Engagement**

**Attack, Defense & Analysis of a Vulnerable Network**

# Table of Contents

---

This document contains the following resources:



**Network Topology & Critical Vulnerabilities within the network.**



**Traffic Profile a breakdown of various network data and files.**



**Normal Activity examples of what regular network activity looks like.**

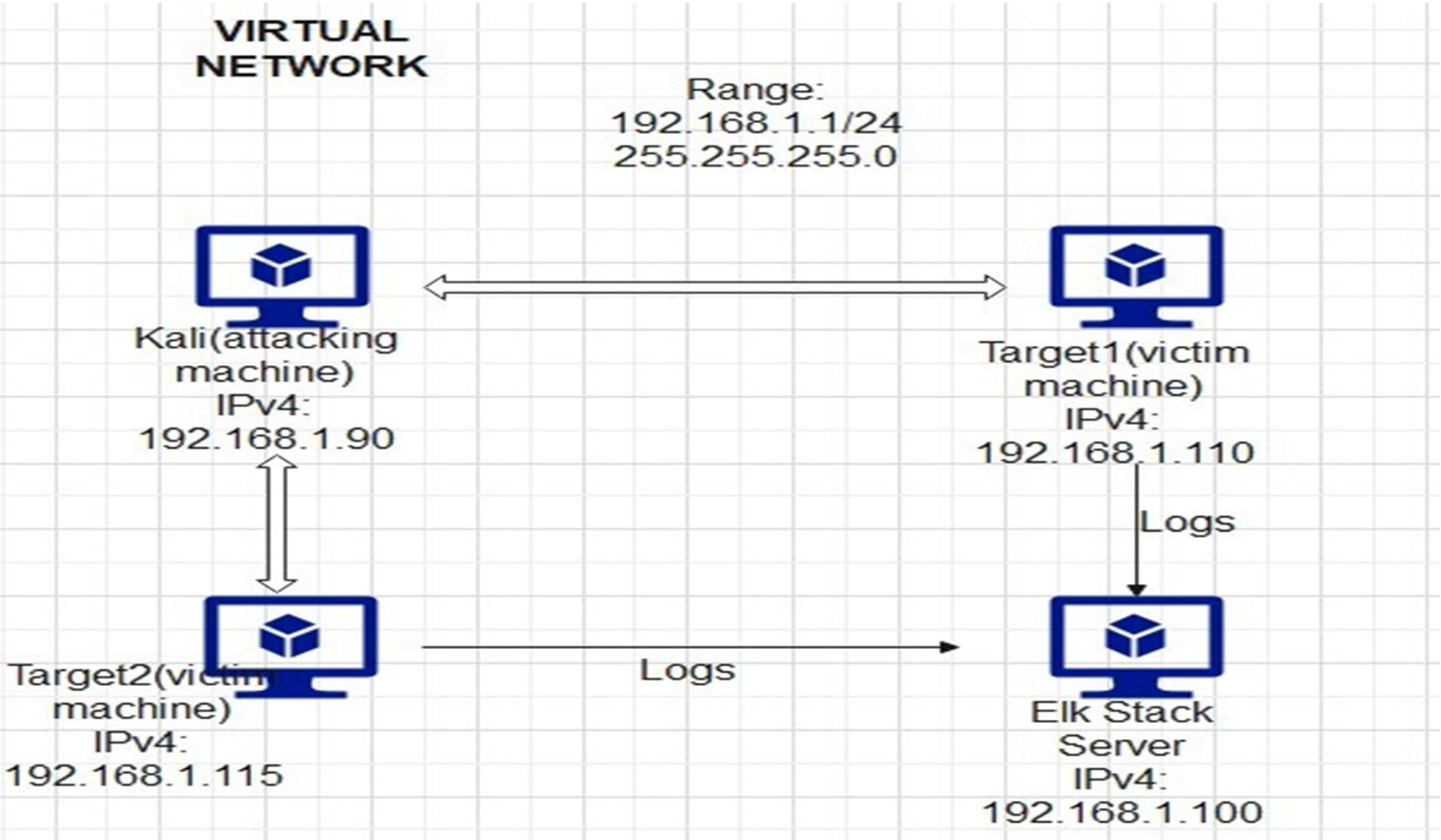


**Malicious Activity examples of what malicious network activity looks like.**



# Network Topology & Critical Vulnerabilities

# Network Topology



## Network

Address Range:  
Netmask:  
Gateway:

## Machines

IPv4:192.168.1.90  
OS: Kali linux  
Hostname:Kali

IPv4:192.168.1.110  
OS:Linux  
Hostname: Target 1

IPv4:192.168.1.100  
OS: Windows 10  
Hostname: Elk Server

IPv4:192.168.1.115  
OS:Linux  
Hostname:Target 2



# Critical Vulnerabilities: Target 1

---

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
Downloading & Piracy	Users have the ability to download files from unprotected sources.In this example the user was torrenting data.	Torrenting data on the network can be a extreme threat to the network.
Vulnerable Windows Machines	The windows 10 machines had various reports of a possible infected host.	All data in the window 10 machines can be compromised with virus or malware.
Access control	Users had the ability to create a private active directory network	Users of active directories can give themselves domain level access to the network

# Traffic Profile

## what does the network traffic look like?



# Traffic Profile

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

Feature	Value	Description
Top Talkers (IP Addresses)	172.16.4.4,10.0.0.201	Machines that sent the most traffic.
Most Common Protocols	HTTPS,UDP,TCP	Three most common protocols on the network.
# of Unique IP Addresses	810 IP addresses	Count of observed IP addresses.
Subnets	10.0.0.0/24 192.168.1.1/24 172.16.4.0/24	Observed subnet ranges.
# of Malware Species	“.dll file” “june11.dll” or dynamic link library	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.
- Monitoring logs/spreadsheet data.

### Suspicious Activity

- Sending malware, phishing attacks.
- Creating websites on the network for malicious uses.
- Manipulating timesheets, data and user interfaces/applications.
- Torrenting any media file , movie or illegal software.





# Normal Activity

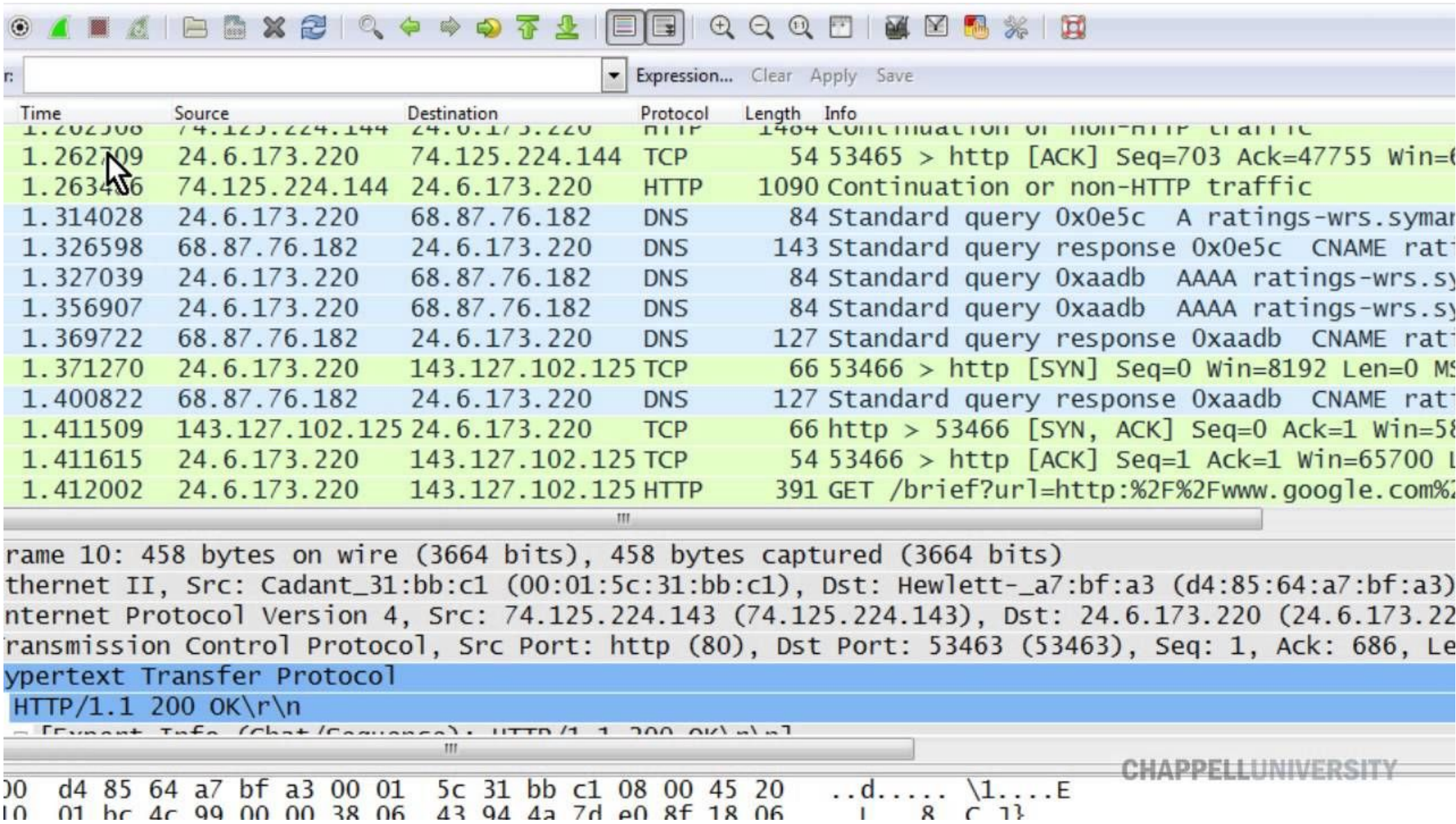
What does normal network traffic look like?

# Watching Youtube

Summarize of the following:

- What kind of traffic did you observe? We observed HTTP traffic and TCP traffic
- Which protocol(s)? http and tcp
- What, specifically, was the user doing? Which site were they browsing? The user were browsing on youtube website.
- A description of any interesting files.

There wasn't any interesting files been download.

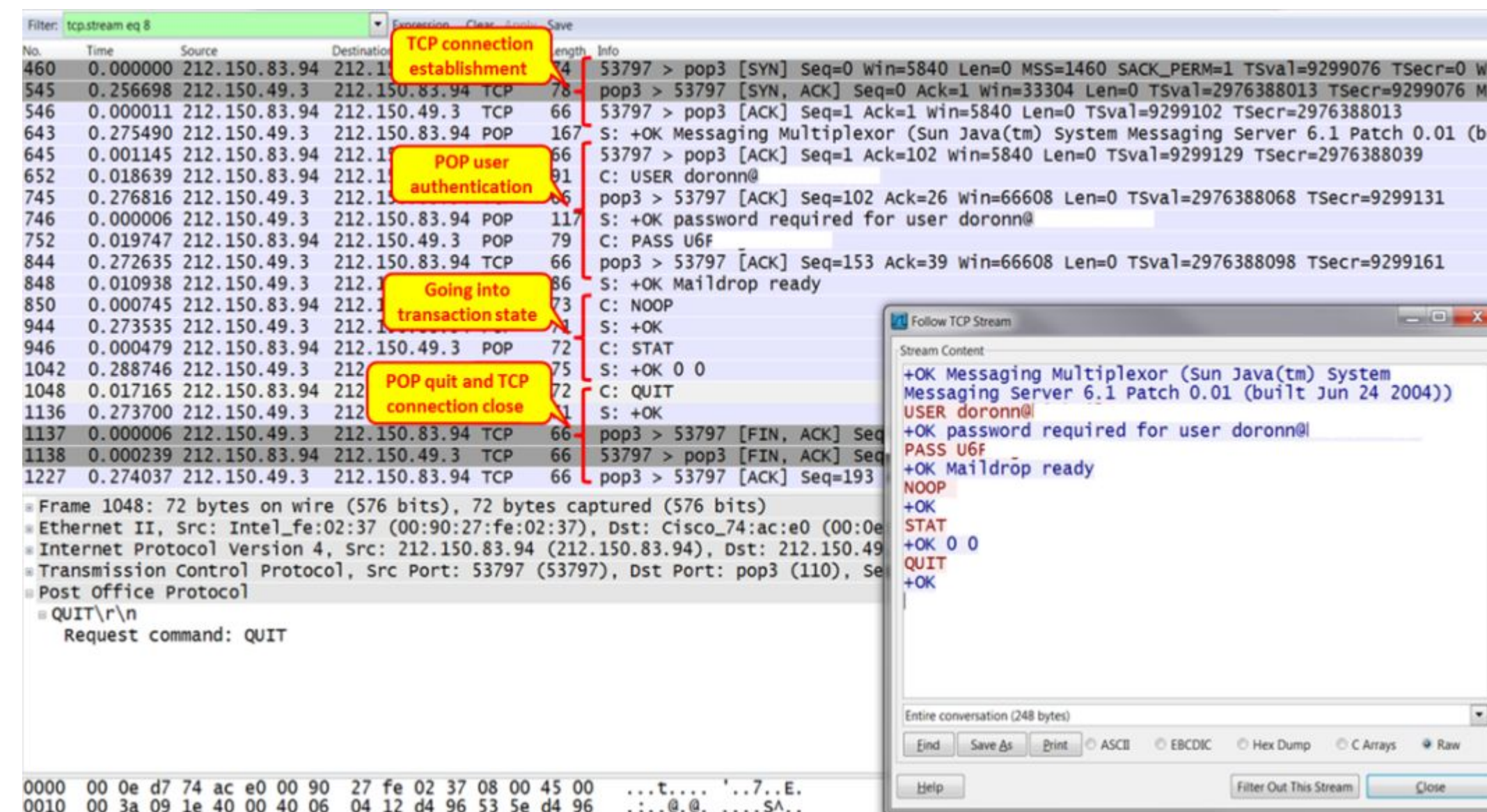




# Reading e-mails

Summarize of the following:

- What kind of traffic did you observe? Which protocol(s)? The user is access their email. Pop and TCP protocol were used.
- What, specifically, was the user doing? The user is checking email.



The image shows a Wireshark packet capture of a POP3 session. The main pane displays a list of packets with the following key events highlighted by yellow callouts:

- TCP connection establishment:** Packets 460 (SYN) and 545 (ACK).
- POP user authentication:** Packets 643 (POP), 645 (ACK), 652 (USER), 745 (ACK), 746 (PASS), and 752 (ACK).
- Going into transaction state:** Packets 844 (POP), 848 (ACK), 850 (NOOP), 944 (ACK), 946 (STAT), 1042 (ACK), 1048 (QUIT), and 1136 (ACK).
- POP quit and TCP connection close:** Packets 1137 (FIN), 1138 (ACK), and 1227 (FIN).

The 'Follow TCP Stream' window shows the decoded data for the selected stream (seq 8), displaying the POP3 protocol conversation:

```
+OK Messaging Multiplexor (Sun Java(tm) System  
Messaging Server 6.1 Patch 0.01 (built Jun 24 2004))  
USER doronn@  
+OK password required for user doronn@  
PASS U6F  
+OK Maildrop ready  
NOOP  
+OK  
STAT  
+OK 0 0  
QUIT  
+OK
```





# Malicious Activity

## What does Malicious network traffic look like?





# [Torrent Files]

## Summarize the following:

- What kind of traffic did you observe?

We observed HTTP traffic specifically for any malicious websites the user could be torrenting on.

- Which protocol(s)?

The protocols that were used was HTTP

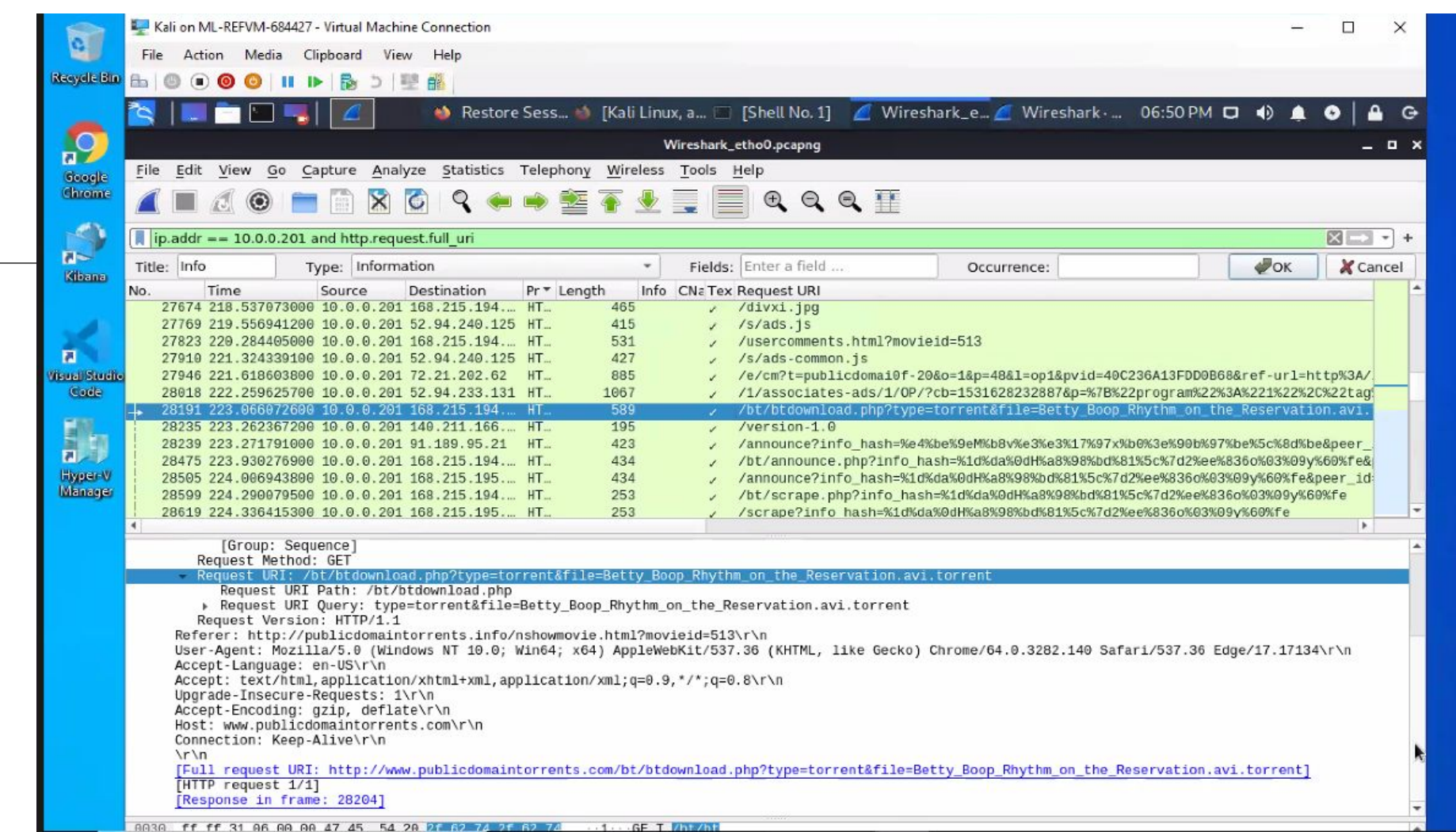
- What, specifically, was the user doing? Which site were they browsing? Etc.

The user decided to download torrent files from the network.

They received this file from publicdomaintorrents.info which isn't a secure website.

- Any interesting files.

The file downloaded is called.Betty\_Boop\_Rhythm\_on\_the\_Reservation.avi.torrent. This data is a AVI file (also known as Audio Video Interleave). Specifically this file is of the 1939 film “Rhythm on the Reservation”.





# [Malicious Web Server] frank-n-ted.com

## Summarize the following:

- What kind of traffic did you observe?

We searched specifically for IP address that received many GET and 200, request as our SOC team was informed of their constant youtube activity.

- The protocols used was HTTP. The user was using various GET request and getting response code 200 (which is success status response code indicates that the request has succeeded.)

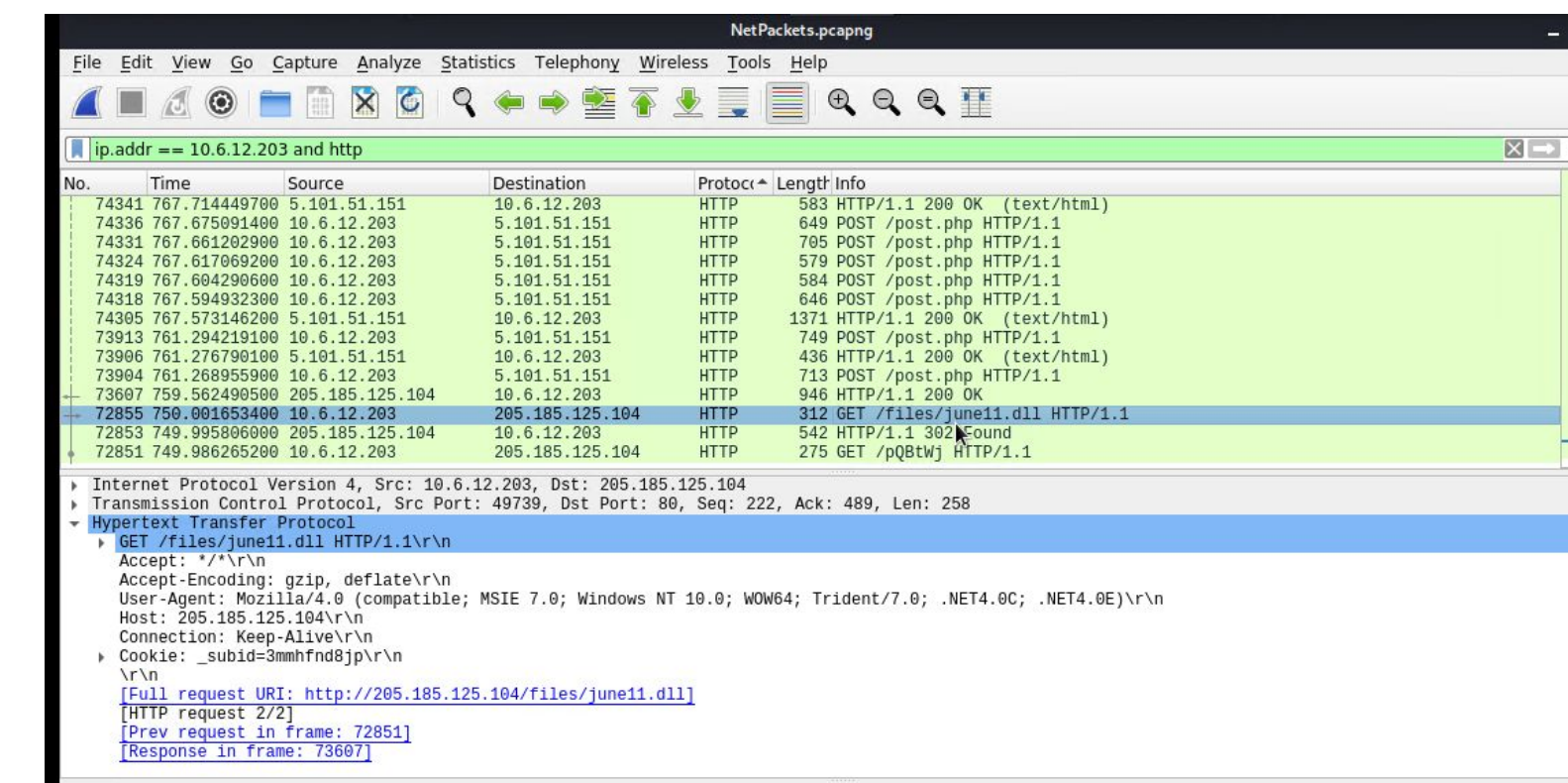
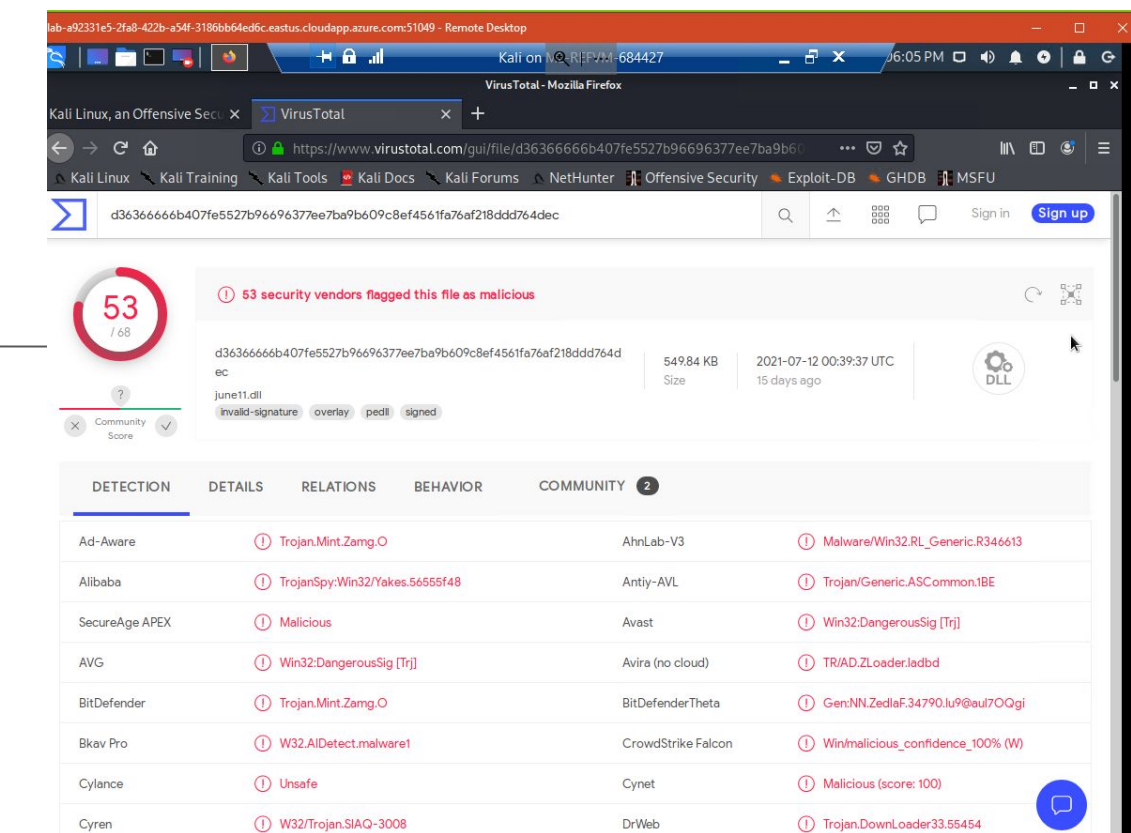
- What, specifically, was the user doing? Which site were they browsing?

The users figured a way to create an active directory network.

- A description of any interesting files.

One of the interesting files included a malicious DLL file. We scanned the virus under VirusTotal.com. to find all possible vulnerabilities.

The results came in as a Trojan virus with up to 53 adware/malware problems.



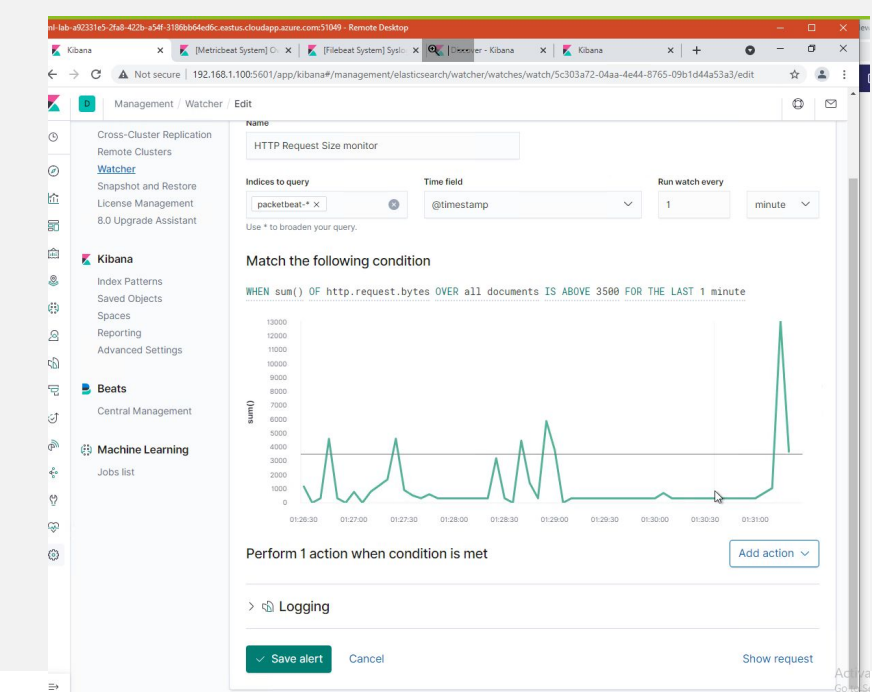


# Mitigations Strategies



# Mitigation strategies

- Alerts (ones specifically to scan any time files are uploaded to the network).
- Creating firewall rules to block common malicious websites.
- Education (creating powerpoints or meetings that show common techniques that the network can be attacked or data can be compromised).





The end  
Questions, comments, concerns?

