Final Engagement
Attack, Defense & Analysis of a Vulnerable Network

Cameo Reindl, Phil Snell, Abdisalan Firin, Mary Yang, Georges Avenie, Omolabake Oladimeji, and Abdirahman Abdullahi

Table of Contents

This document contains the following resources:

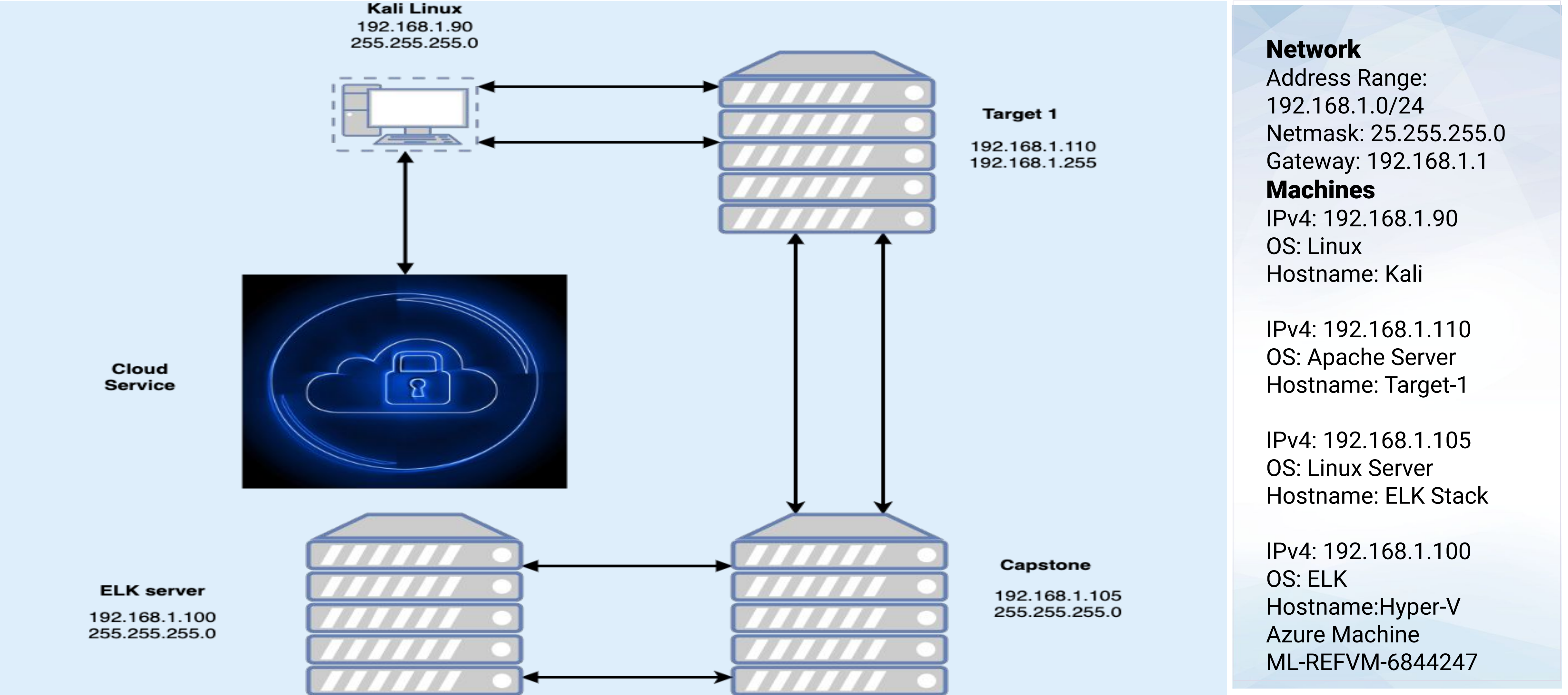**Network Topology & Critical Vulnerabilities**

Traffic Profile

Normal Activity

Malicious Activity

Network Topology
& Critical Vulnerabilities

Network Topology

Kali Linux
192.168.1.90
255.255.255.0

Target 1
192.168.1.110
192.168.1.255

Cloud Service

ELK server
192.168.1.100
255.255.255.0

Capstone
192.168.1.105
255.255.255.0

Network
Address Range:
192.168.1.0/24
Netmask: 25.255.255.0
Gateway: 192.168.1.1
Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.110
OS: Apache Server
Hostname: Target-1

IPv4: 192.168.1.105
OS: Linux Server
Hostname: ELK Stack

IPv4: 192.168.1.100
OS: ELK
Hostname:Hyper-V
Azure Machine
ML-REFVM-6844247

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
CVE-2018-1000030 Python privilege escalation	It's a level of access and permissions needed to achieve the goal of accessing sensitive information	It takes advantage of vulnerability to provide the attacker with privileges
CVE-2021-28041 ssh remote login	It allows users to connect to different networks from their local machine	The connection between the client and the server is not encrypted and the attacker can easily recover packets and data in transfer also know as man in the middles
CVE-2019-15653 html password hash disclosure	Password disclosure via an insecure authentication mechanism	The password hash is viewable in plaintext and it is unsalted
CVE-2017-7760 exposed username and weak password	Michael's password was his name - there was no requirement or protocol in place to have a strong password	User access to the wp-config.php file via nano. This exposed MySQL password

Traffic Profile

Traffic Profile

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

Feature	Value	Description
Top Talkers (IP Addresses)	185.243.115.84 166.62.111.64	Machines that sent the most traffic.
Most Common Protocols	TCP/IP HTTP UDP	Three most common protocols on the network.
# of Unique IP Addresses	2	Count of observed IP addresses.
Subnets	192.168.1.0/24	Observed subnet ranges.
# of Malware Species	1 malware File Name: JUNE11.dll Name: Trojan.Mint.Zamg.O	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:

- Set up an Active Directory network.
- Users created their own web server on the corporate network
- Users watched videos on YouTube
- Used BitTorrent software to download movies

"Normal" Activity

- Watching YouTube, reading the news.
- Use BitTorrent to download work related files

Suspicious Activity

- Users created their own web server on the corporate network and set up Active Directory
  - New IP is in the range of 10.6.12.0/24 which is the same as the corporate
- Adware was downloaded as a result of their Youtube activity
- Use BitTorrent to download movies

Normal Activity

Watching YouTube, reading the news

Summarize the following:

- We observed a lot of traffic using DNS
- The user was watching YouTube videos
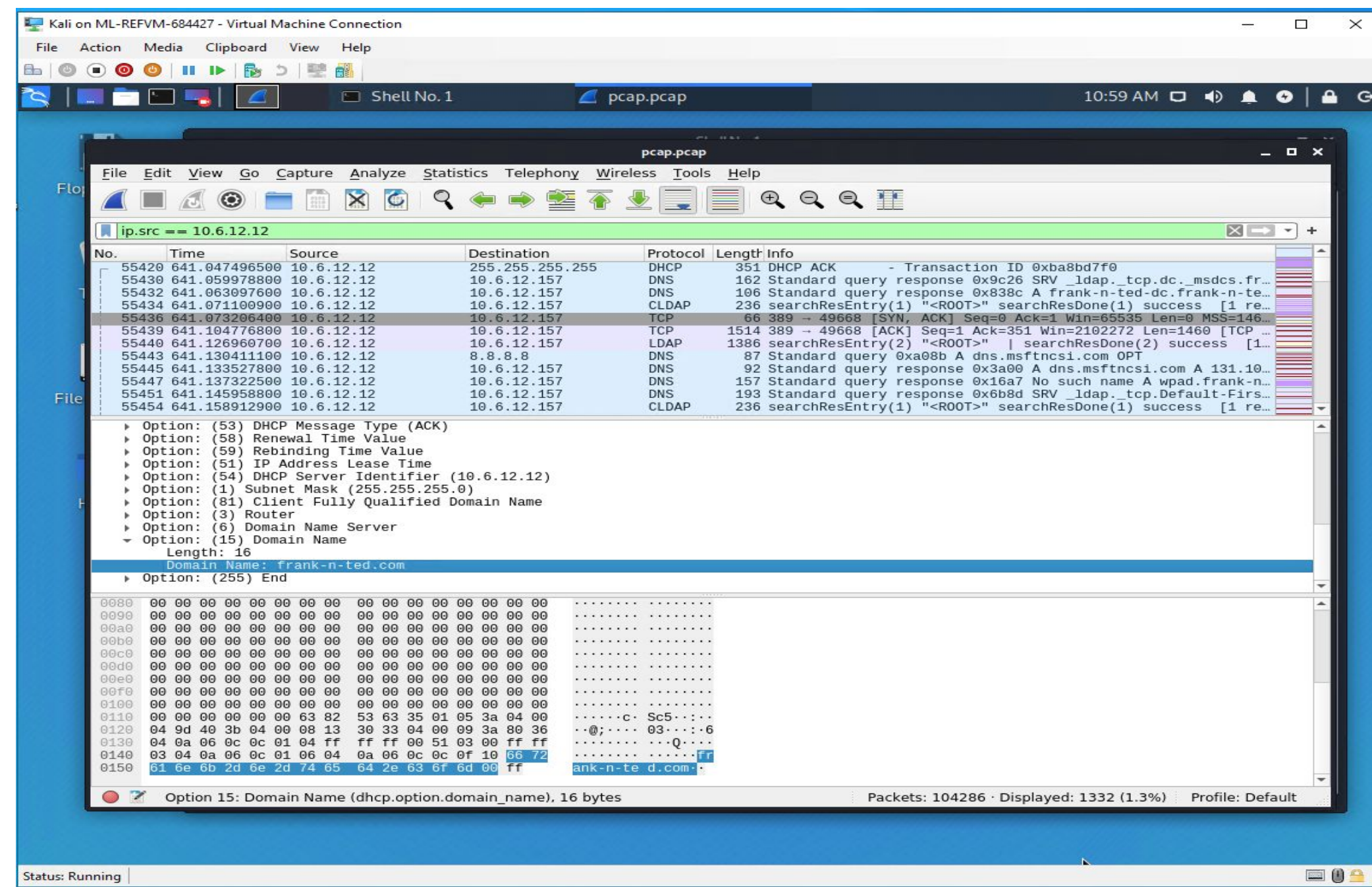
BitTorrent used to download work related files:

Summarize the following:

- We observed HTTP traffic
- Users were downloading work related files using BitTorrent
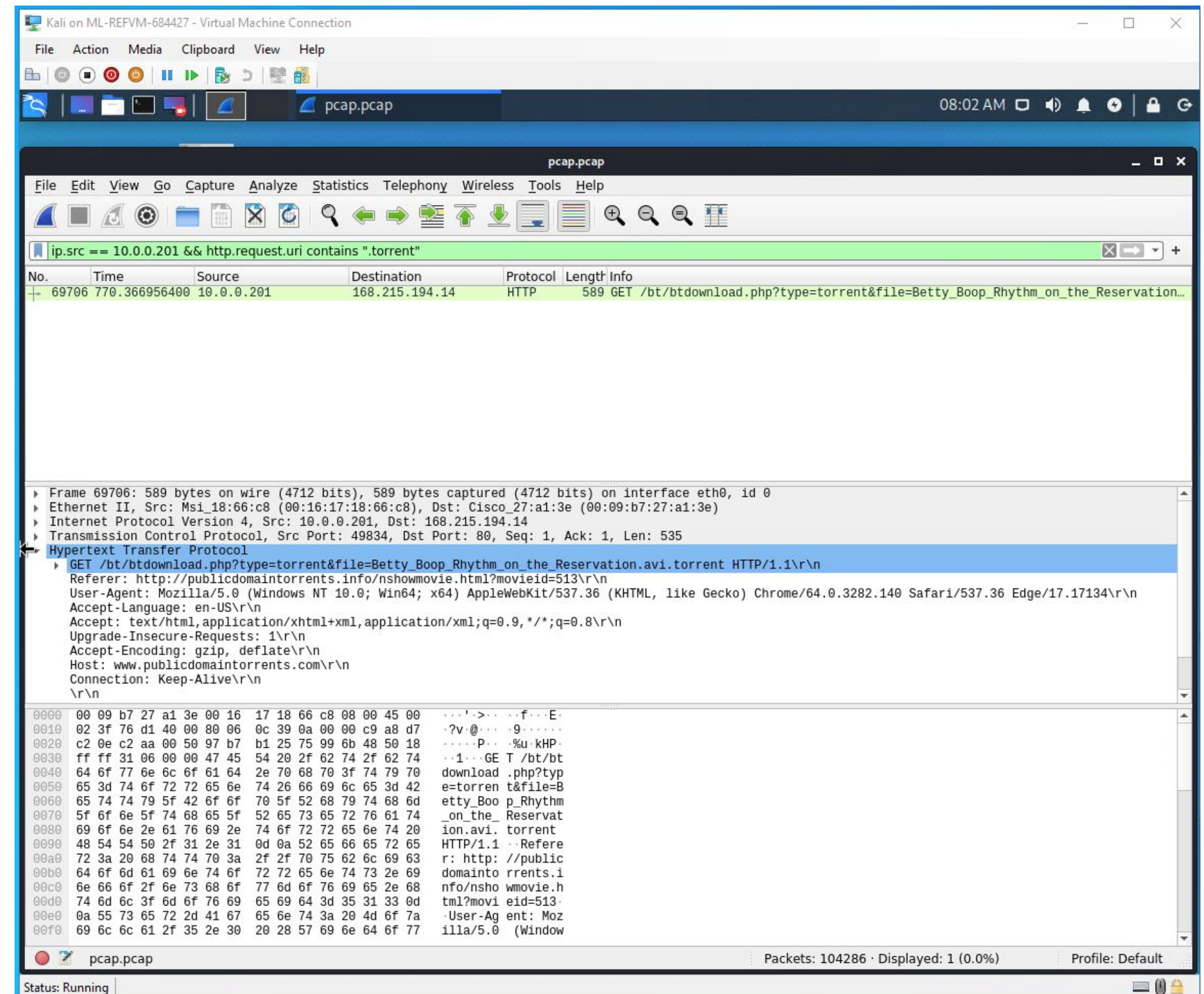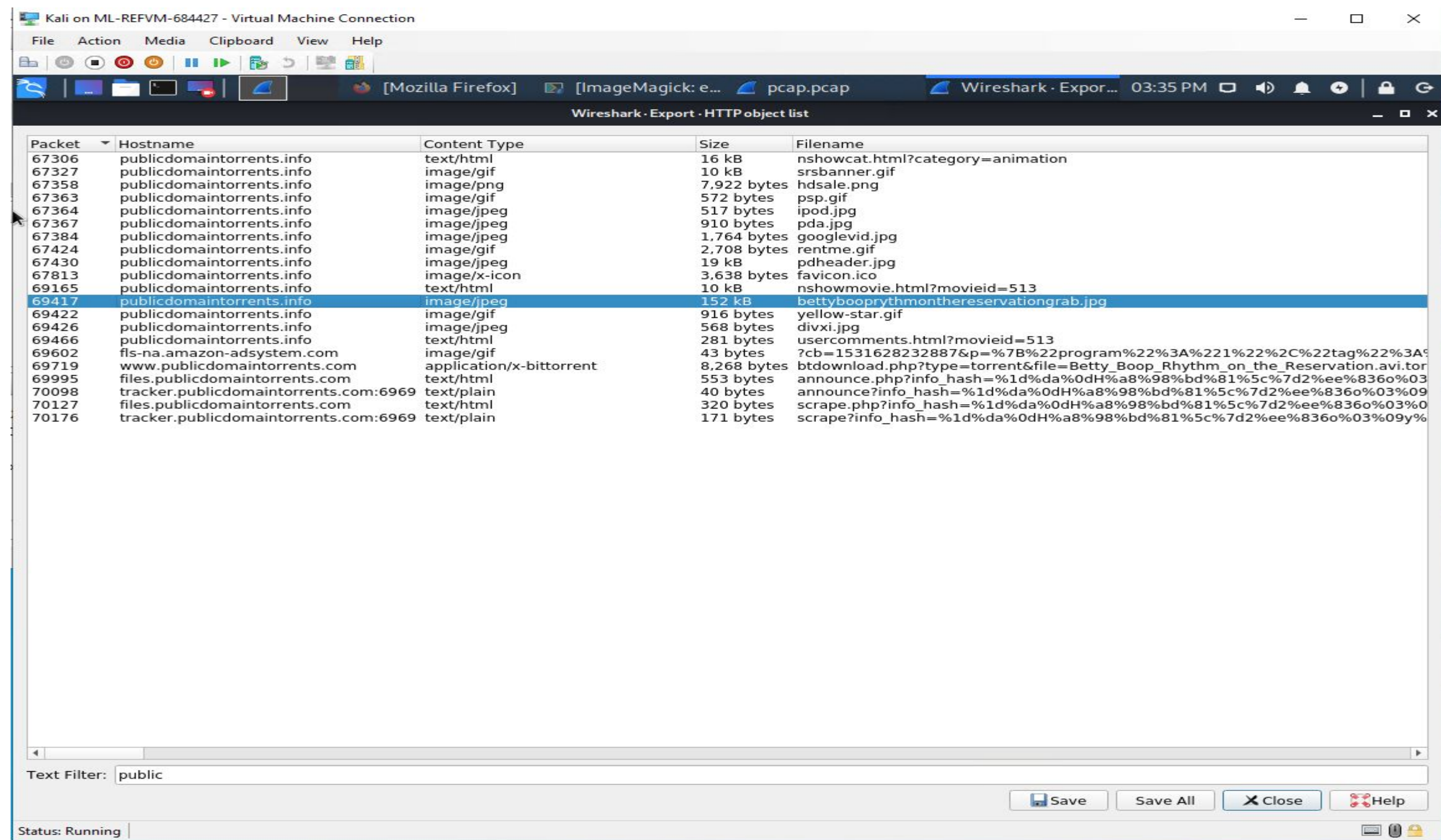
Malicious Activity

Users created their own web server on the corporate network and set up Active Directory

- Observed the DNS protocol
- It appears that the user has created a domain called frank-n-ted-dc.frank-n-ted.com
- IP address of the DC of the AD network is 10.6.12.12
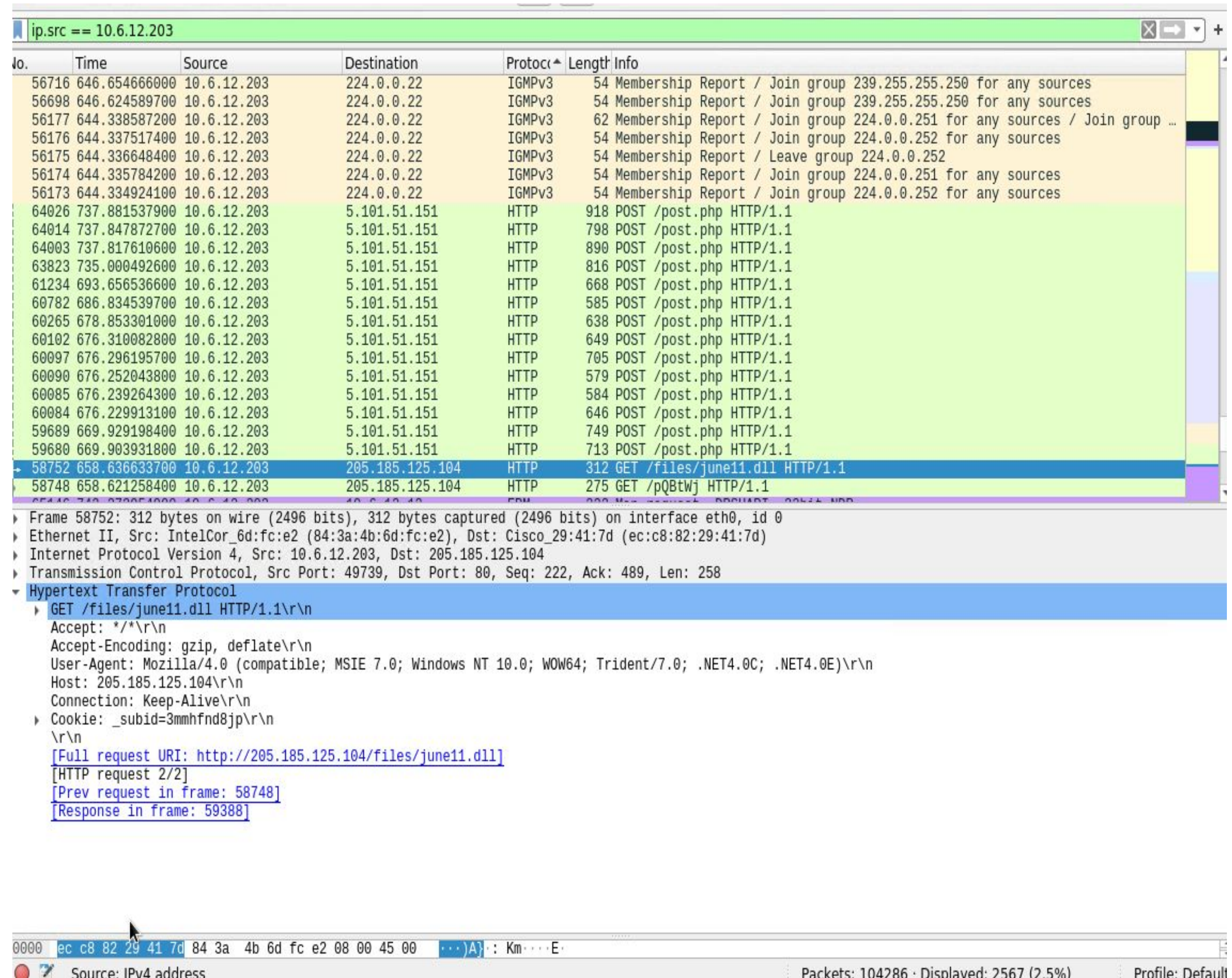
Adware was downloaded as a result of Users' Browsing activity

Summarize the following:

- Observed the HTTP traffic
- The user was likely browsing various sites and as a result of that clicked on a malicious adware that downloaded a malicious script onto
   their computer.
- Found a suspicious file called june11.dll
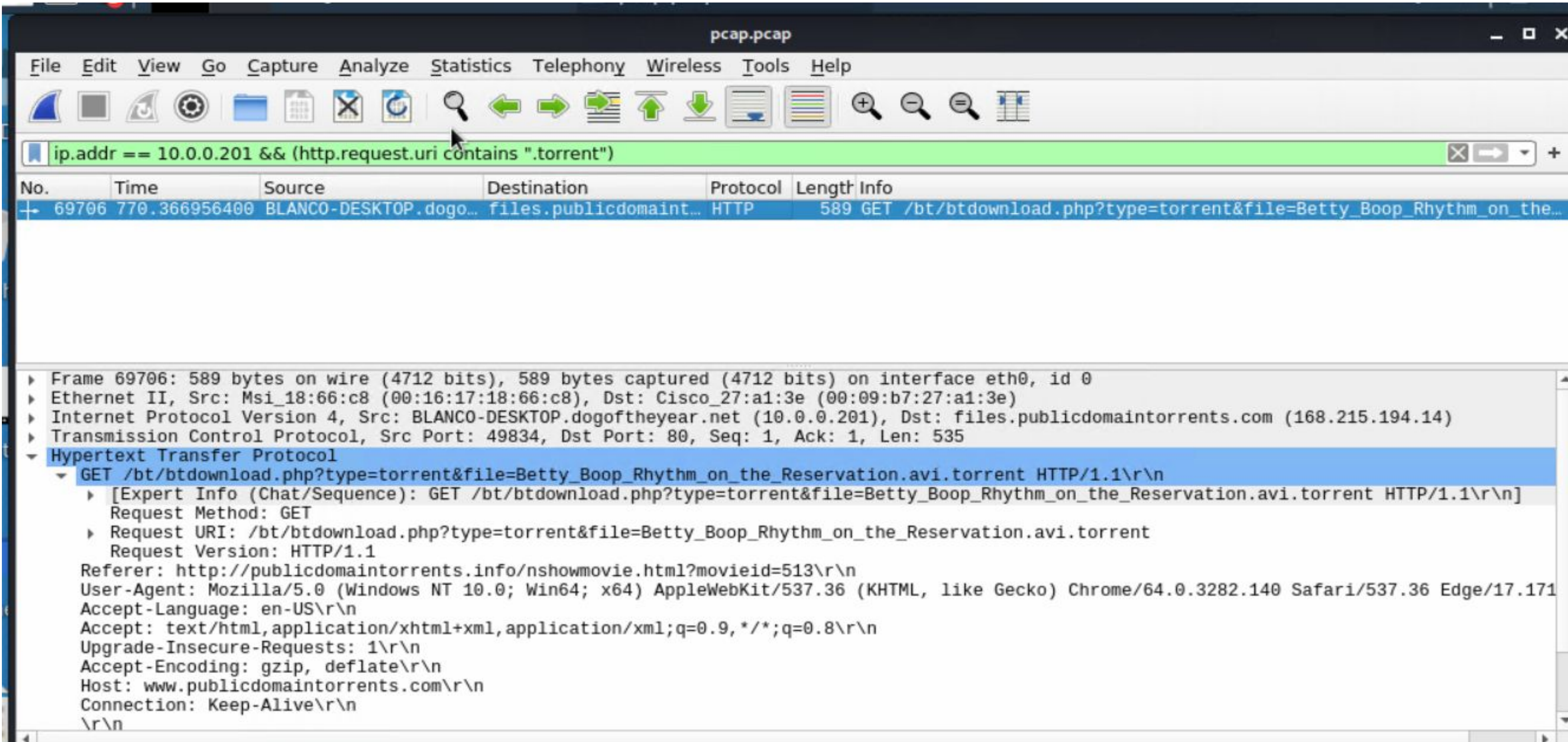
Proof of malicious file

BitTorrent:

- BitTorrent, when downloading videos from the internet, will take bits and pieces from others who already have the video on their own computer. This makes the download process faster. The more people who have downloaded the video, the quicker the download.
- The users downloaded a movie through BitTorrent on HTTP.
  - Using BitTorrent for work purposes is allowed.
  - The movie downloaded was strictly against the company's copyright infringement policy and therefore illegal.

Betty Boop:

That's all folks!
A little something special for all of you!
Next Slide.