

# **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**



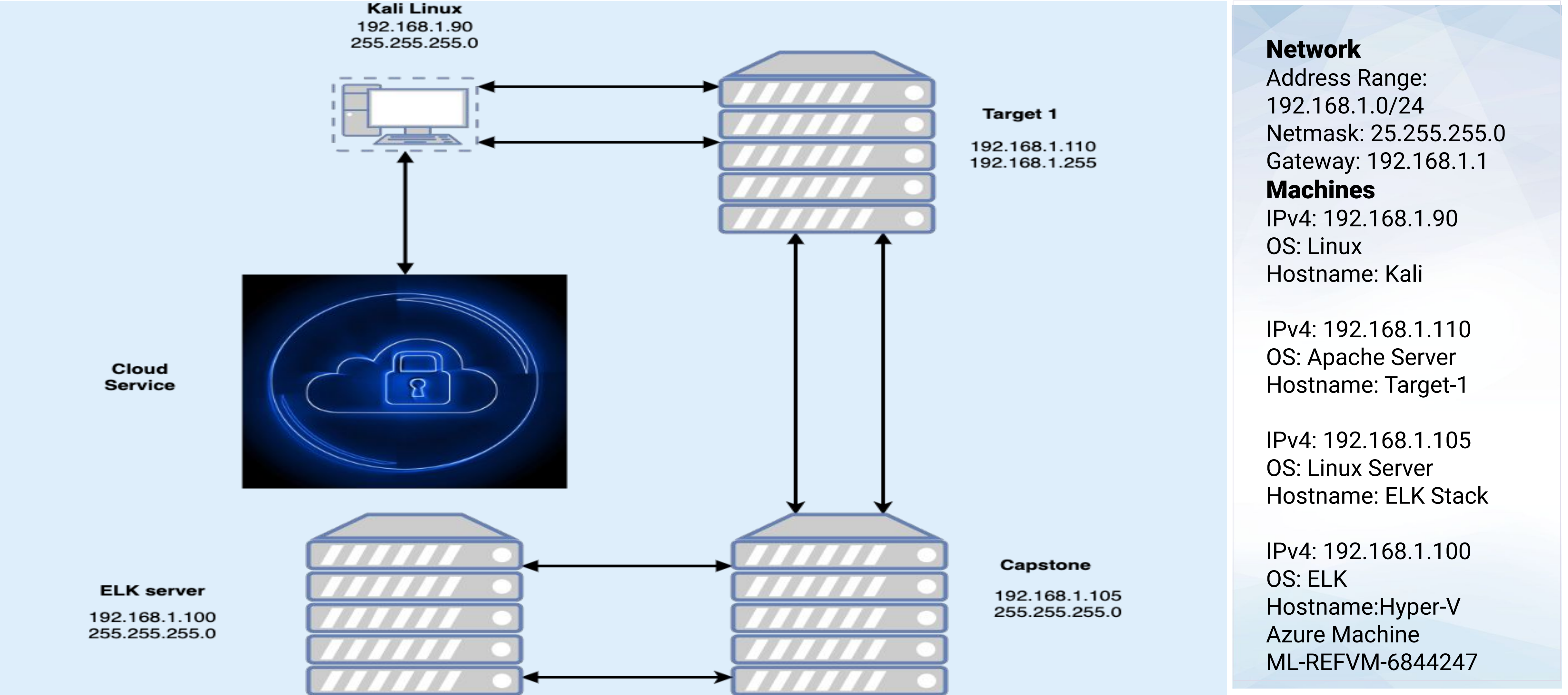
**Normal Activity**



**Malicious Activity**

# Network Topology & Critical Vulnerabilities

# Network Topology



# 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



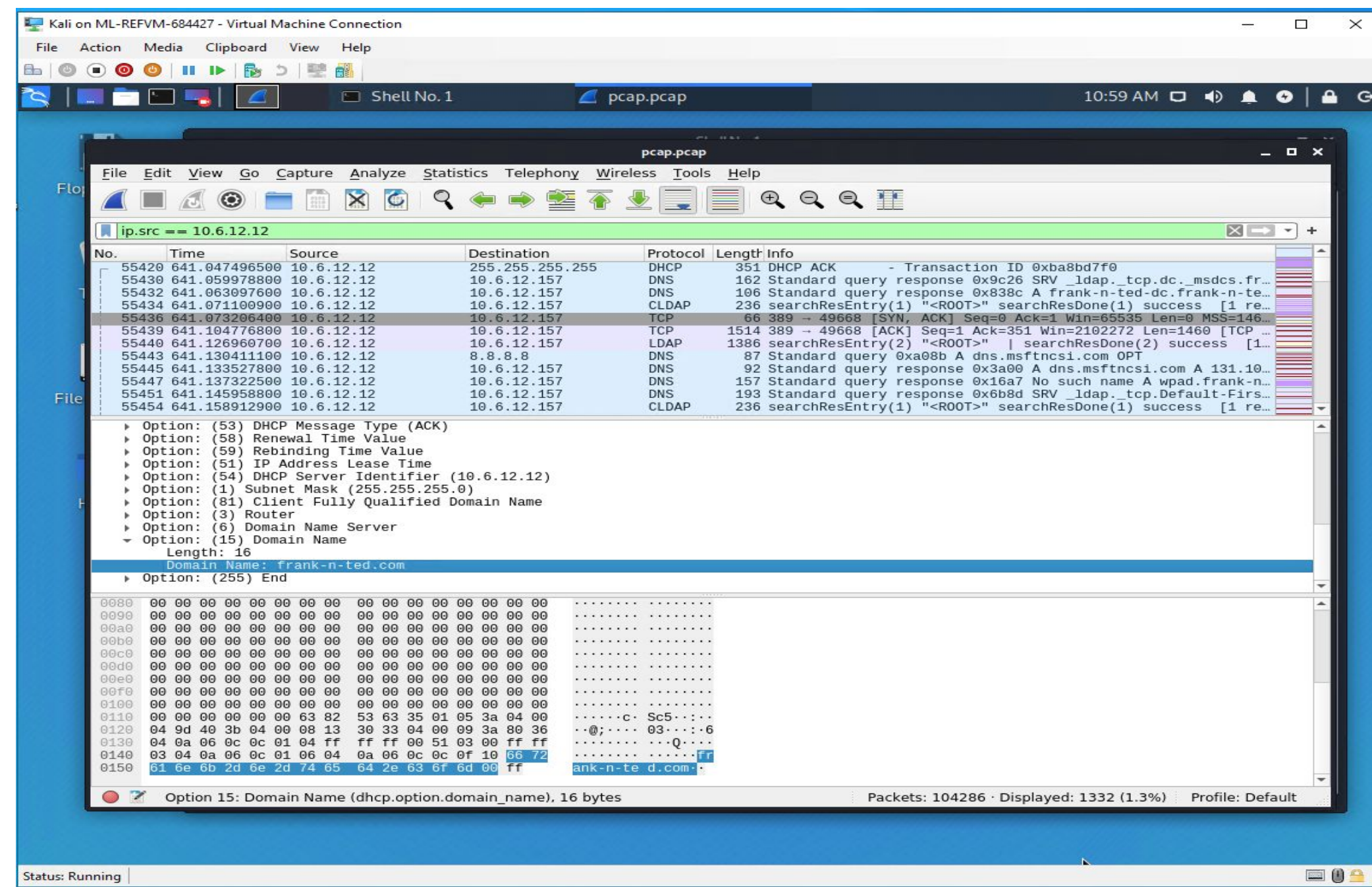
The background of the slide is a dark gray field filled with a complex, repeating pattern of geometric shapes. These shapes include squares and triangles of various sizes, some of which are slightly offset or layered, creating a three-dimensional, crystalline effect. The overall tone is monochromatic, with subtle variations in gray shades.

# Normal Activity

# Watching YouTube, reading the news

Summarize the following:

- We observed a lot of traffic using DNS
- The user was watching YouTube videos

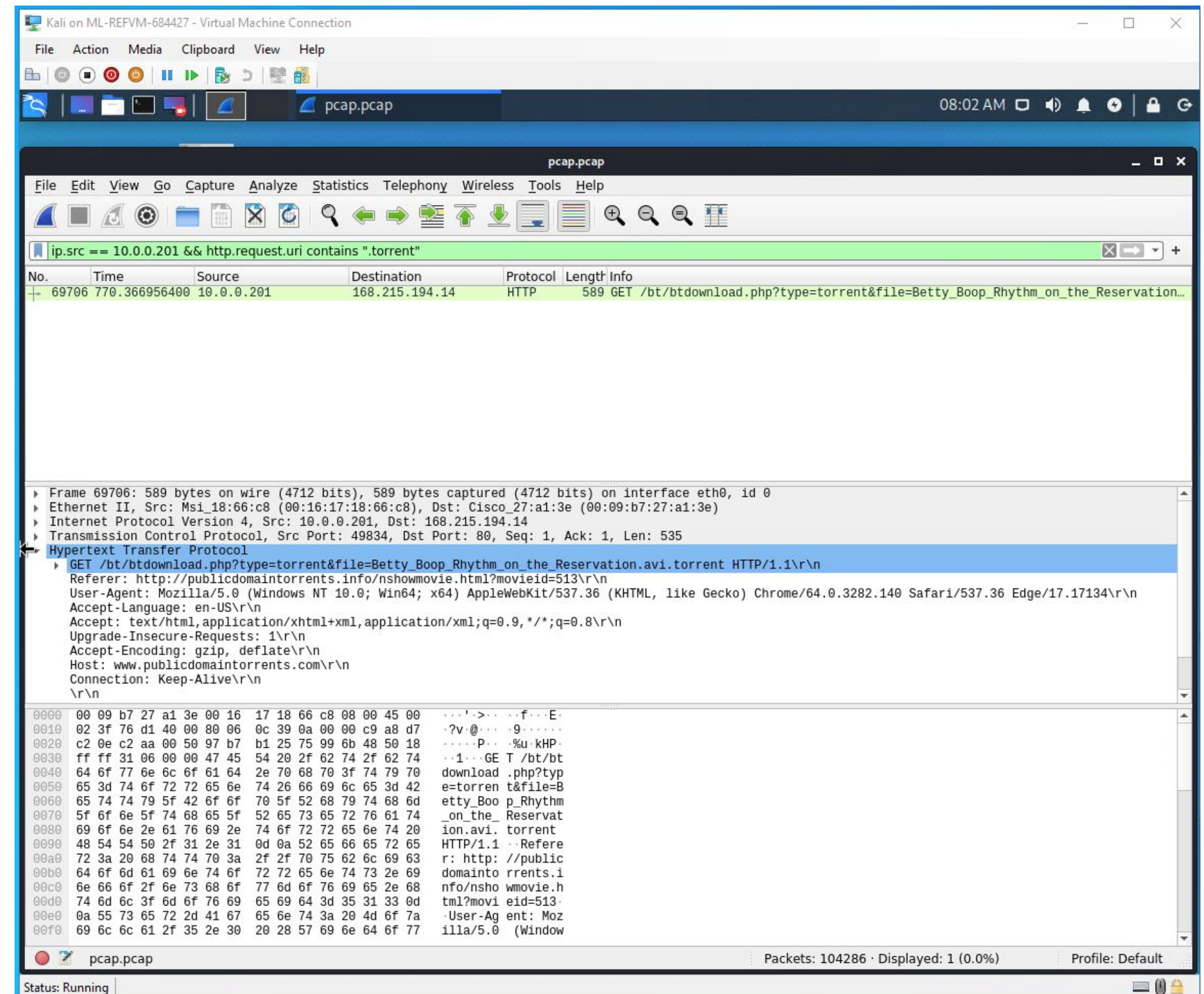
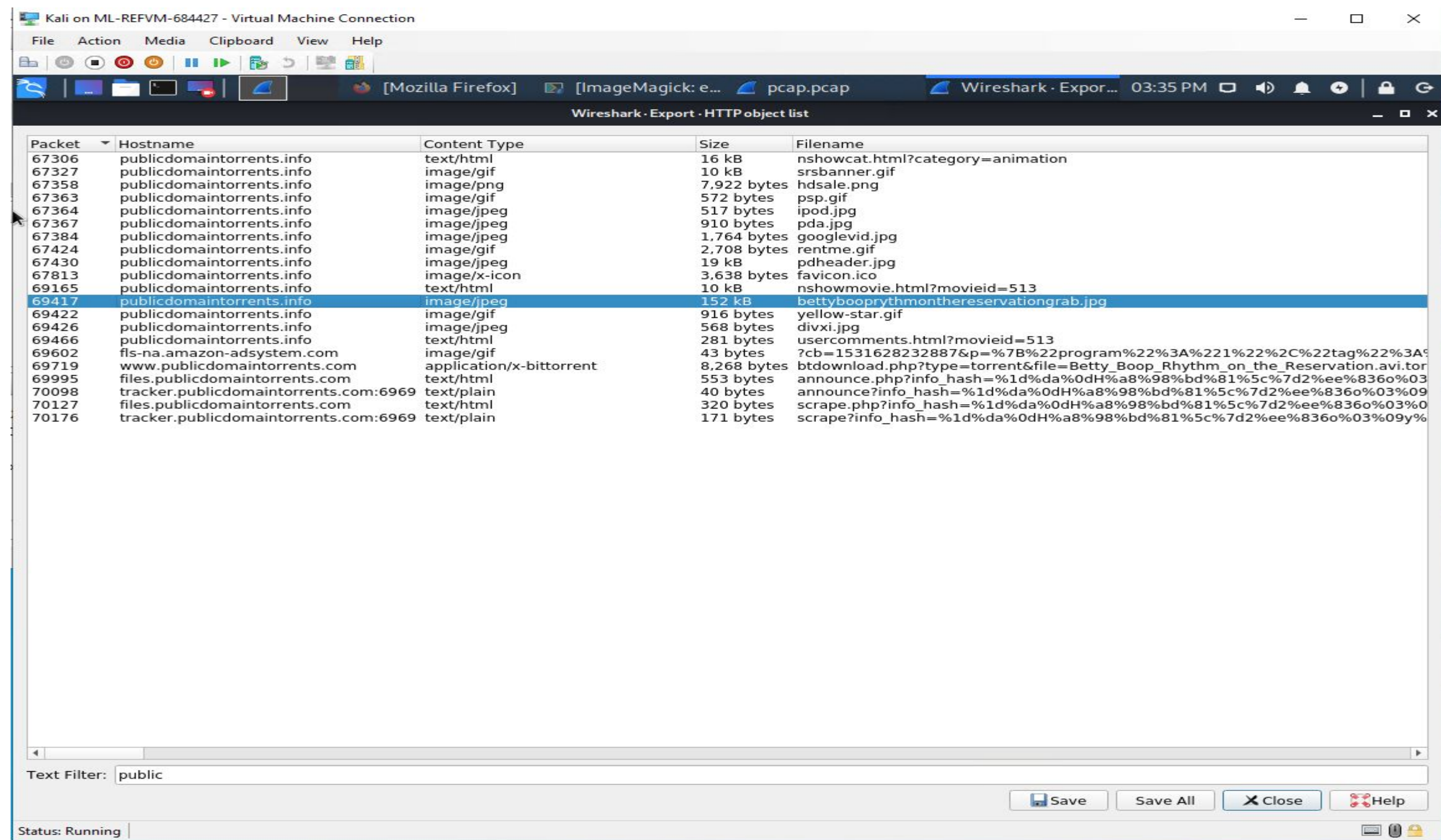




# BitTorrent used to download work related files:

## 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

The image shows a Wireshark network traffic capture. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The filter bar at the top shows 'ip.src == 10.6.12.0/24'. The packet list on the left shows several packets, with packet 55432 selected. The packet details pane on the right shows the structure of the selected packet, which is a DNS Standard query response. The packet bytes pane at the bottom shows the raw data of the selected packet, with the domain name 'frank-n-ted-dc.frank-n-ted.com' highlighted in blue.

No.	Time	Source	Destination	Protocol	Length	Info
55420	641.047496500	10.6.12.12	255.255.255.255	DHCP	351	DHCP ACK - Transaction ID 0xba8bd7f0
55421	641.048373200	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any sources
55422	641.049214500	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
55423	641.050071100	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
55424	641.050936500	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
55425	641.052219600	10.6.12.157	224.0.0.251	MDNS	80	Standard query 0x0000 ANY DESKTOP-86J4BX.local, "QM" question
55426	641.053707000	10.6.12.157	224.0.0.251	MDNS	90	Standard query response 0x0000 A 10.6.12.157
55427	641.054843300	10.6.12.157	224.0.0.252	LLMNR	74	Standard query 0x094f ANY DESKTOP-86J4BX
55428	641.055829300	10.6.12.157	224.0.0.22	IGMPv3	62	Membership Report / Join group 224.0.0.251 for any sources / Join group ...
55429	641.057368600	10.6.12.157	10.6.12.12	DNS	96	Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
55430	641.059978800	10.6.12.12	10.6.12.157	DNS	162	Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com ...
55431	641.061408000	10.6.12.157	10.6.12.12	DNS	90	Standard query 0x838c A frank-n-ted-dc.frank-n-ted.com
55432	641.063097600	10.6.12.12	10.6.12.157	DNS	106	Standard query response 0x838c A frank-n-ted-dc.frank-n-ted.com A 10.6.1...
55433	641.067325100	10.6.12.157	10.6.12.12	CLDAP	264	searchRequest(1) "<R00T>" baseObject
55434	641.071100900	10.6.12.12	10.6.12.157	CLDAP	236	searchResEntry(1) "<R00T>" searchResDone(1) success [1 result]

Frame 55432: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface eth0, id 0

Ethernet II, Src: Dell\_2a:f7:e5 (98:40:bb:2a:f7:e5), Dst: Intel\_68:42:d3 (00:11:75:68:42:d3)

Internet Protocol Version 4, Src: 10.6.12.12, Dst: 10.6.12.157

User Datagram Protocol, Src Port: 53, Dst Port: 50264

Domain Name System (response)

Transaction ID: 0x838c

Flags: 0x8580 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

Queries

Answers

frank-n-ted-dc.frank-n-ted.com: type A, class IN, addr 10.6.12.12

[Request In: 55431]

[Time: 0.001689600 seconds]

0000 00 11 75 68 42 d3 98 40 bb 2a f7 e5 08 00 45 00 ..uhB..@.\*...E.

0010 00 5c 54 45 00 00 80 11 b9 97 0a 06 0c 0c 0a 06 .\TE.....

0020 0c 9d 00 35 c4 58 00 48 a0 38 83 8c 85 80 00 01 ...5.X.H.8....

0030 00 01 00 00 00 00 0e 66 72 61 6e 6b 2d 6e 2d 74 .....f rank-n-t

0040 65 64 2d 64 63 0b 72 61 6e 6b 2d 6e 2d 74 65 ed-dc.fr ank-n-te

0050 64 03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 00 01 d.com.....

0060 00 00 04 b0 00 04 0a 06 0c 0c .....

Bytes 54-85: Name (dns.qry.name)

Packets: 104286 · Displayed: 5130 (4.9%)

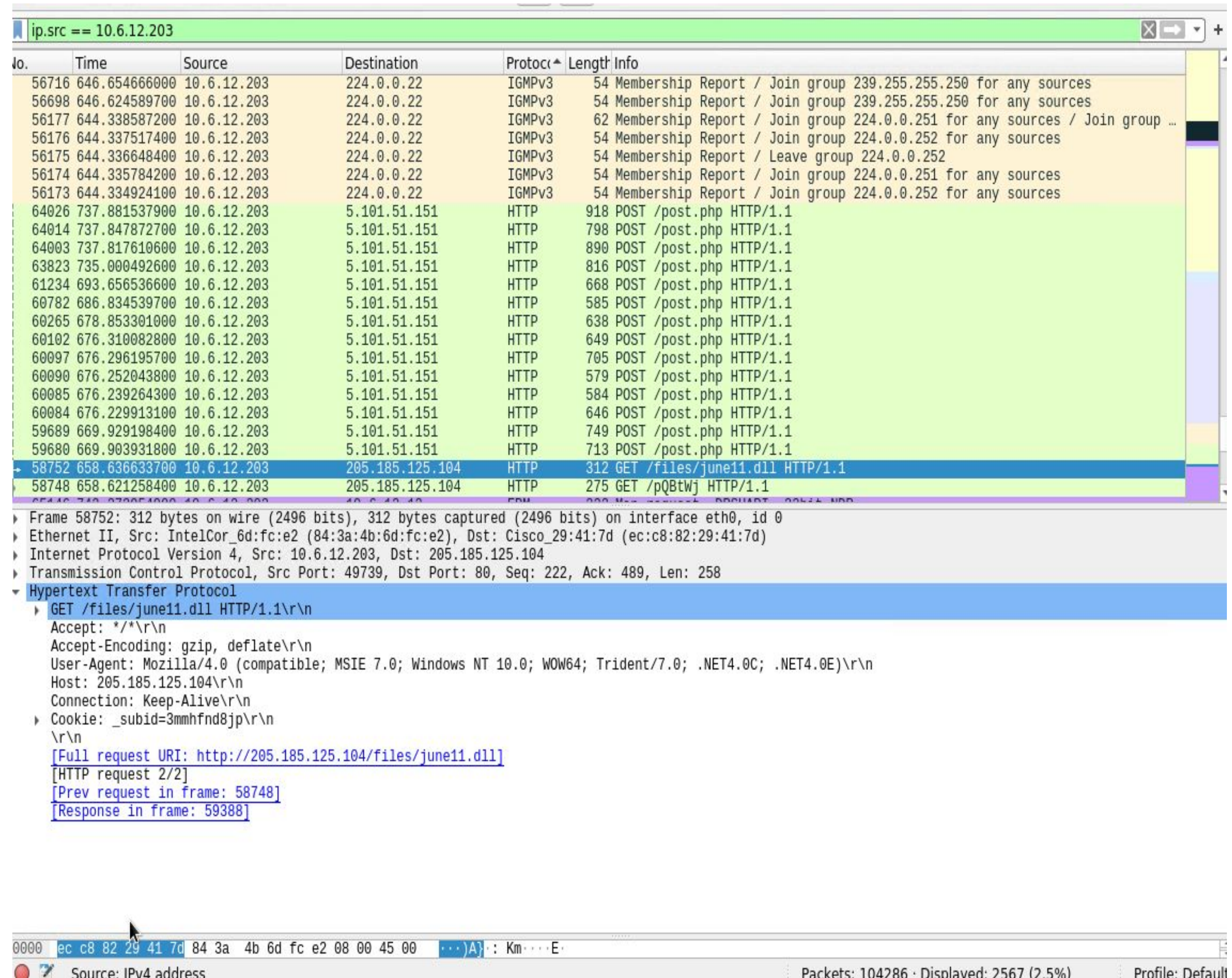
Profile: Default



# 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



The image shows a Wireshark packet capture window. The top pane displays a list of network packets. The selected packet (No. 58752) is an HTTP GET request for /files/june11.dll. The middle pane shows the details of this packet, including the Ethernet II header, Internet Protocol Version 4 header, and the Hypertext Transfer Protocol section. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
56716	646.654666000	10.6.12.203	224.0.0.22	IGMPv3	54	Membership Report / Join group 239.255.255.250 for any sources
56698	646.624589700	10.6.12.203	224.0.0.22	IGMPv3	54	Membership Report / Join group 239.255.255.250 for any sources
56177	644.338587200	10.6.12.203	224.0.0.22	IGMPv3	62	Membership Report / Join group 224.0.0.251 for any sources / Join group ...
56176	644.337517400	10.6.12.203	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
56175	644.336648400	10.6.12.203	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
56174	644.335784200	10.6.12.203	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any sources
56173	644.334924100	10.6.12.203	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
64026	737.881537900	10.6.12.203	5.101.51.151	HTTP	918	POST /post.php HTTP/1.1
64014	737.847872700	10.6.12.203	5.101.51.151	HTTP	798	POST /post.php HTTP/1.1
64003	737.817610600	10.6.12.203	5.101.51.151	HTTP	890	POST /post.php HTTP/1.1
63823	735.000492600	10.6.12.203	5.101.51.151	HTTP	816	POST /post.php HTTP/1.1
61234	693.656536600	10.6.12.203	5.101.51.151	HTTP	668	POST /post.php HTTP/1.1
60782	686.834539700	10.6.12.203	5.101.51.151	HTTP	585	POST /post.php HTTP/1.1
60265	678.853301000	10.6.12.203	5.101.51.151	HTTP	638	POST /post.php HTTP/1.1
60102	676.310082800	10.6.12.203	5.101.51.151	HTTP	649	POST /post.php HTTP/1.1
60097	676.296195700	10.6.12.203	5.101.51.151	HTTP	705	POST /post.php HTTP/1.1
60090	676.252043800	10.6.12.203	5.101.51.151	HTTP	579	POST /post.php HTTP/1.1
60085	676.239264300	10.6.12.203	5.101.51.151	HTTP	584	POST /post.php HTTP/1.1
60084	676.229913100	10.6.12.203	5.101.51.151	HTTP	646	POST /post.php HTTP/1.1
59689	669.929198400	10.6.12.203	5.101.51.151	HTTP	749	POST /post.php HTTP/1.1
59680	669.903931800	10.6.12.203	5.101.51.151	HTTP	713	POST /post.php HTTP/1.1
58752	658.636633700	10.6.12.203	205.185.125.104	HTTP	312	GET /files/june11.dll HTTP/1.1
58748	658.621258400	10.6.12.203	205.185.125.104	HTTP	275	GET /pQBtWj HTTP/1.1

Frame 58752: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface eth0, id 0  
Ethernet II, Src: IntelCor\_6d:fc:e2 (84:3a:4b:6d:fc:e2), Dst: Cisco\_29:41:7d (ec:c8:82:29:41:7d)  
Internet Protocol Version 4, Src: 10.6.12.203, Dst: 205.185.125.104  
Transmission Control Protocol, Src Port: 49739, Dst Port: 80, Seq: 222, Ack: 489, Len: 258  
Hypertext Transfer Protocol  
GET /files/june11.dll HTTP/1.1\r\nAccept: \*/\*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)\r\nHost: 205.185.125.104\r\nConnection: Keep-Alive\r\nCookie: \_subid=3mmhfd8jp\r\n\r\n[Full request URI: http://205.185.125.104/files/june11.dll]  
[HTTP request 2/2]  
[Prev request in frame: 58748]  
[Response in frame: 59388]

0000 ec c8 82 29 41 7d 84 3a 4b 6d fc e2 08 00 45 00 ...A}: Km...E  
Source: IPv4 address Packets: 104286 · Displayed: 2567 (2.5%) Profile: Default



# Proof of malicious file

Security

VirusTotal - File - d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec - Mozilla Firefox

← → ↺ 🏠

https://www.virustotal.com/gui/file/d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

⋮ 🛡️ ⭐

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

🔍 ⬆️ 🗄️ 💬

Sign in Sign up

51

/ 66

?

Community Score

⚠️ 51 security vendors and 1 sandbox flagged this file as malicious

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

549.84 KB Size

2021-11-30 23:52:26 UTC 8 days ago

Googleipdate.exe

invalid-signature overlay pedll signed

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

Ad-Aware	⚠️ Trojan.Mint.Zamg.O	AhnLab-V3	⚠️ Malware/Win32.RL_Generic.R346613
Alibaba	⚠️ TrojanSpy:Win32/Yakes.8988e849	ALYac	⚠️ Trojan.Mint.Zamg.O
Antiy-AVL	⚠️ Trojan/Generic.ASCommon.1BE	Arcabit	⚠️ Trojan.Mint.Zamg.O
Avast	⚠️ Win32:DangerousSig [Trj]	AVG	⚠️ Win32:DangerousSig [Trj]

# BitTorrent:

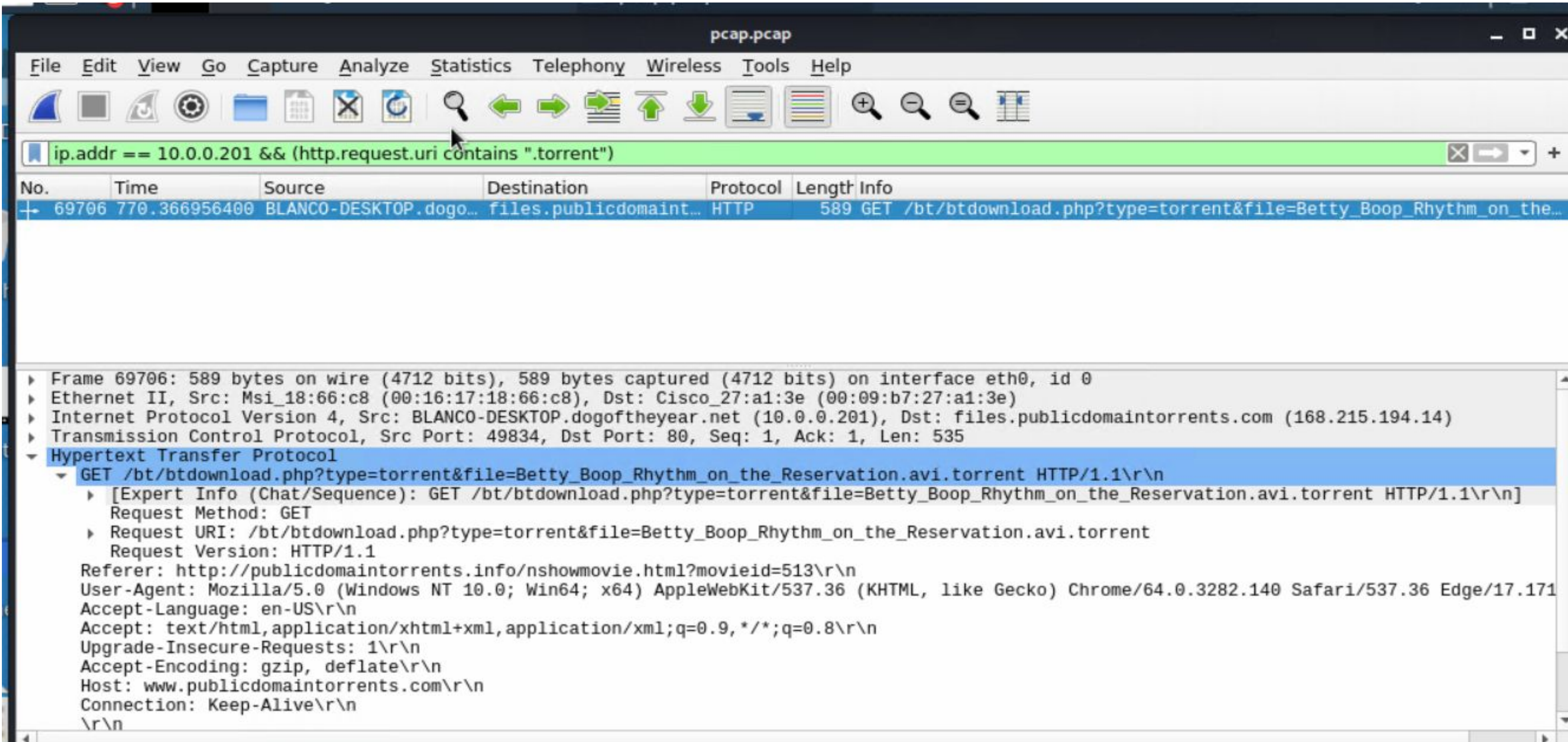
---

- 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:



The image shows a Wireshark packet capture window titled "pcap.pcap". The filter bar at the top contains the expression "ip.addr == 10.0.0.201 && (http.request.uri contains \".torrent\")". The packet list shows a single packet, No. 69706, at time 770.366956400, from source BLANCO-DESKTOP.dogoftheyear.net to destination files.publicdomaintorrents.com, protocol HTTP, length 589 bytes. The packet details pane shows the following information:

- Frame 69706: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits) on interface eth0, id 0
- Ethernet II, Src: Msi\_18:66:c8 (00:16:17:18:66:c8), Dst: Cisco\_27:a1:3e (00:09:b7:27:a1:3e)
- Internet Protocol Version 4, Src: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201), Dst: files.publicdomaintorrents.com (168.215.194.14)
- Transmission Control Protocol, Src Port: 49834, Dst Port: 80, Seq: 1, Ack: 1, Len: 535
- 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]Request Method: GET
    - Request URI: /bt/btdownload.php?type=torrent&file=Betty\_Boop\_Rhythm\_on\_the\_Reservation.avi.torrent
    - Request Version: HTTP/1.1
    - Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\r\n
    - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.171
    - Accept-Language: en-US\r\n
    - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8\r\n
    - Upgrade-Insecure-Requests: 1\r\n
    - Accept-Encoding: gzip, deflate\r\n
    - Host: www.publicdomaintorrents.com\r\n
    - Connection: Keep-Alive\r\n
    - \r\n



File Name: Betty\_Boop\_Rhythm\_on\_the\_Reservation.avi  
File Size: 100.50 MB  
Resolution: 720x480  
Duration: 00:06:02





That's all folks!  
That's all folks!

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



***Happy  
Graduation!***



**CONGRATULATIONS  
GRADUATE!**

**SEE YOU AT THE TOP**

