

Network Analysis

Time Thieves

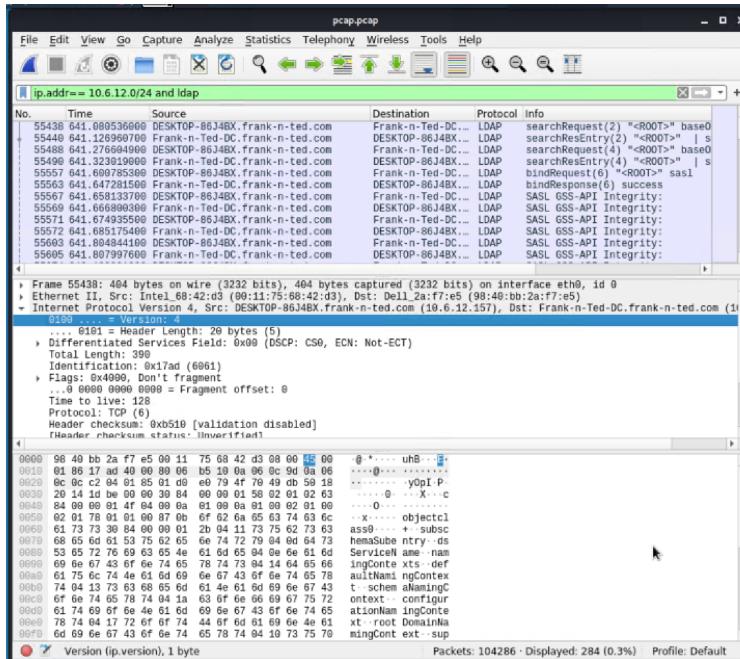
At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.
- Their IP addresses are somewhere in the range 10.6.12.0/24.

You must inspect your traffic capture to answer the following questions:

1. What is the domain name of the users' custom site?

Frank-n-ted.com

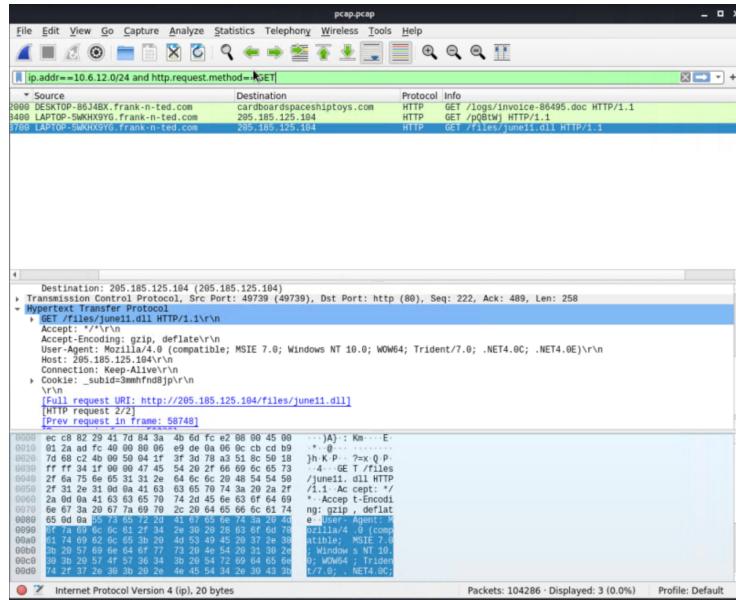


2. What is the IP address of the Domain Controller (DC) of the AD network?

10.6.12.12

3. What is the name of the malware downloaded to the 10.6.12.203 machine? Once you have found the file, export it to your Kali machine's desktop.

June11.dll



4. Upload the file to [VirusTotal.com](https://www.virustotal.com). What kind of malware is this classified as?

Trojan

The screenshot shows the VirusTotal analysis interface. It displays a list of security vendor names on the left and their corresponding analysis results on the right. The results are color-coded with red circles indicating detected threats. The vendors listed include Ad-Aware, AhnLab-V3, Alibaba, ALYac, Antiy-AVL, Arcabit, Avast, AVG, Avira (no cloud), BitDefender, and several others. The analysis results show that the file is identified as a Trojan by most of the vendors.

Security Vendor	Analysis Result
Ad-Aware	Trojan.Mint.Zamg.O
AhnLab-V3	Malware/Win32.RL_Generic.R346613
Alibaba	TrojanSpy.Win32/Yakes.0454a340
ALYac	Trojan.Mint.Zamg.O
Antiy-AVL	Trojan/Generic.ASCommon.1BE
Arcabit	Trojan.Mint.Zamg.O
Avast	Win32:DangerousSig [Trj]
AVG	Win32:DangerousSig [Trj]
Avira (no cloud)	TR/AD.ZLoader.ladbd
BitDefender	Trojan.Mint.Zamg.O

Vulnerable Windows Machines

The Security team received reports of an infected Windows host on the network. They know the following:

- Machines in the network live in the range 172.16.4.0/24.
- The domain mind-hammer.net is associated with the infected computer.
- The DC for this network lives at 172.16.4.4 and is named Mind-Hammer-DC.
- The network has standard gateway and broadcast addresses.

Inspect your traffic to answer the following questions:

1. Find the following information about the infected Windows machine:

- **Host name:** Rotterdam-PC.mind.hammer.net
- **IP address:** 172.16.4.205
- **MAC address:** 00:59:07:b0:63:a4

2. What is the username of the Windows user whose computer is infected?

matthijs.devries

3. What are the IP addresses used in the actual infection traffic?

185.243.115.84, 172.16.4.205

Wireshark · Conversations · pcap.pcap							
Ethernet · 74	IPv4 · 877	IPv6 · 1	TCP · 1044	UDP · 1839			
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
172.16.4.205	185.243.115.84	30,344	26 M	15,149	9,831 k	15,195	
166.62.111.64	172.16.4.205	15,728	16 M	11,354	15 M	4,374	
10.0.0.201	23.43.62.169	6,934	7,045 k	2,282	124 k	4,652	
10.0.0.201	64.187.66.143	4,883	3,637 k	2,235	144 k	2,648	
5.101.51.151	10.6.12.203	4,326	4,246 k	3,262	4,177 k	1,064	

IT was informed that some users are torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringement.

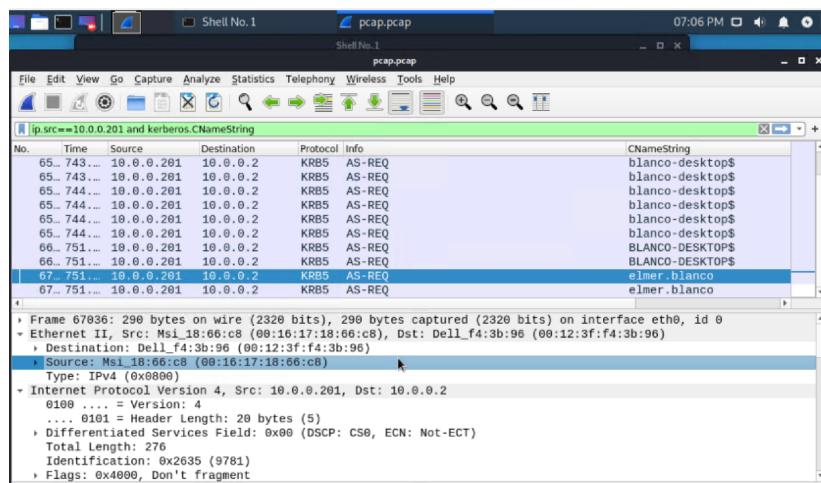
IT shared the following about the torrent activity:

- The machines using torrents live in the range 10.0.0.0/24 and are clients of an AD domain.
- The DC of this domain lives at 10.0.0.2 and is named DogOfTheYear-DC.
- The DC is associated with the domain dogoftheyear.net.

Your task is to isolate torrent traffic and answer the following questions in your Network Report:

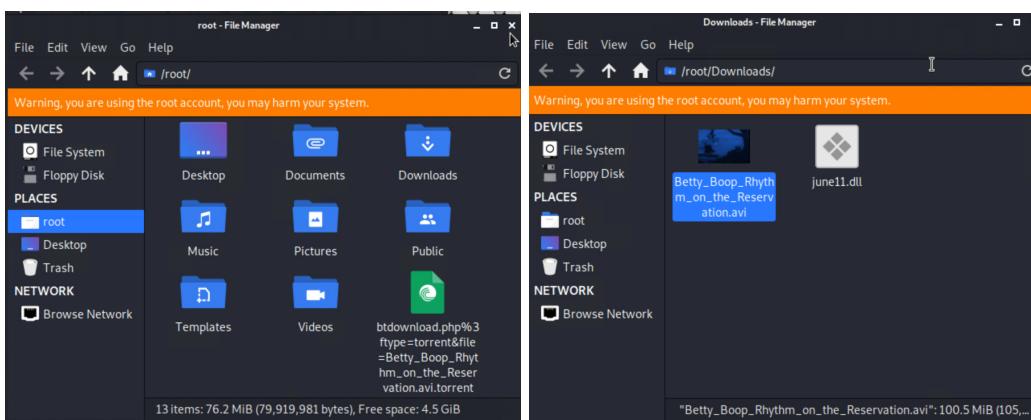
1. Find the following information about the machine with IP address 10.0.0.201:

- MAC address: **00:16:17:18:66:c8**
- Windows username: **elmer.blanco**
- OS version: **Windows NT 10.0; Win64**



2. Which torrent file did the user download?

Betty_Boop_Rhythm_on_the_Reservation.avi.torrent



Screenshot showing a dual-terminal session and a network traffic capture.

Terminal Session:

- Two terminal windows are open: "Shell No.1" and "Shell No.2".
- "Shell No.1" shows the command "Samba is not being run as an AD Domain Controller: Masking samba-ad-dc.service" and the output "qBittorrent v4.4.3.1".
- "Shell No.2" is active, showing a video player window displaying the title "Rhythm on the Reservation".
- The video player interface includes controls for play/pause, volume, and speed, and displays the file size as 100.5 MB and download speed as 0 B/s (0 B).

Network Traffic Capture:

- A Wireshark window titled "pcap.pcap" is open, showing a list of captured HTTP objects.
- The table lists 70176 packets, with the last few entries shown below:

Packet	Hostname	Content Type	Size	Filename
67306	publicdomaintorrents.info	text/html	16 kB	nshowcat.html?category=animation
67327	publicdomaintorrents.info	image/gif	10 kB	srsbanner.gif
67358	publicdomaintorrents.info	image/png	7,922 bytes	hdSale.png
67363	publicdomaintorrents.info	image/gif	572 bytes	psp.gif
67364	publicdomaintorrents.info	image/jpeg	517 bytes	iPod.jpg
67367	publicdomaintorrents.info	image/jpeg	910 bytes	pda.jpg
67384	publicdomaintorrents.info	image/jpeg	1,764 bytes	googlevid.jpg
67424	publicdomaintorrents.info	image/gif	2,708 bytes	rentme.gif
67430	publicdomaintorrents.info	image/jpeg	19 kB	pdheader.jpg
67813	publicdomaintorrents.info	image/x-icon	3,638 bytes	favicon.ico
69165	publicdomaintorrents.info	text/html	10 kB	nshowmovie.html?movieid=513
69417	publicdomaintorrents.info	image/jpeg	152 kB	bettybooprythmonthereservationgrab.jpg
69422	publicdomaintorrents.info	image/gif	916 bytes	yellow-star.gif
69426	publicdomaintorrents.info	image/jpeg	568 bytes	divxi.jpg
69466	publicdomaintorrents.info	text/html	281 bytes	usercomments.html?movieid=513
69602	fls-na.amazon-adsystem.com	image/gif	43 bytes	?cb=1531628232887&p=%7B%22program%22%3A%221%22%2C%22tag%22%3A%22p
69719	www.publicdomaintorrents.com	application/x-bittorrent	8,768 bytes	btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservatio
69756	download.dluge-torrent.org		7 bytes	version=1.0
69761	torrent.ubuntu.com:6969	text/plain	431 bytes	announce?info_hash=%e4%be%9eM%b8v%e3%e3%17%97x%b0%3e%90%97%be%5c
69995	files.publicdomaintorrents.com	text/html	553 bytes	announce.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d%ee%8360%03%09%
70098	tracker.publicdomaintorrents.co...	text/plain	40 bytes	announce?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d%ee%8360%03%09%
70127	files.publicdomaintorrents.com	text/html	320 bytes	scrape.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d%ee%8360%03%09%
70176	tracker.publicdomaintorrents.co...	text/plain	171 bytes	scrape?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d%ee%8360%03%09%