Network Analysis

Time Thieves

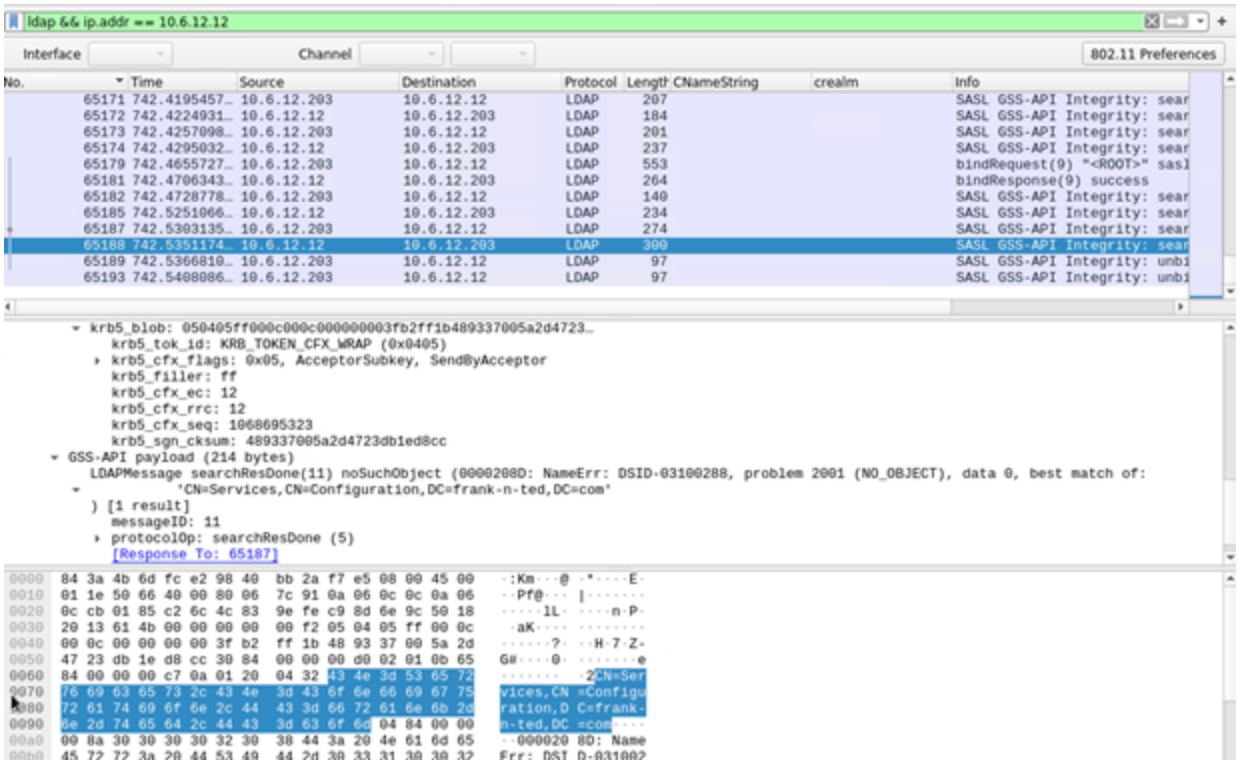
At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- 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

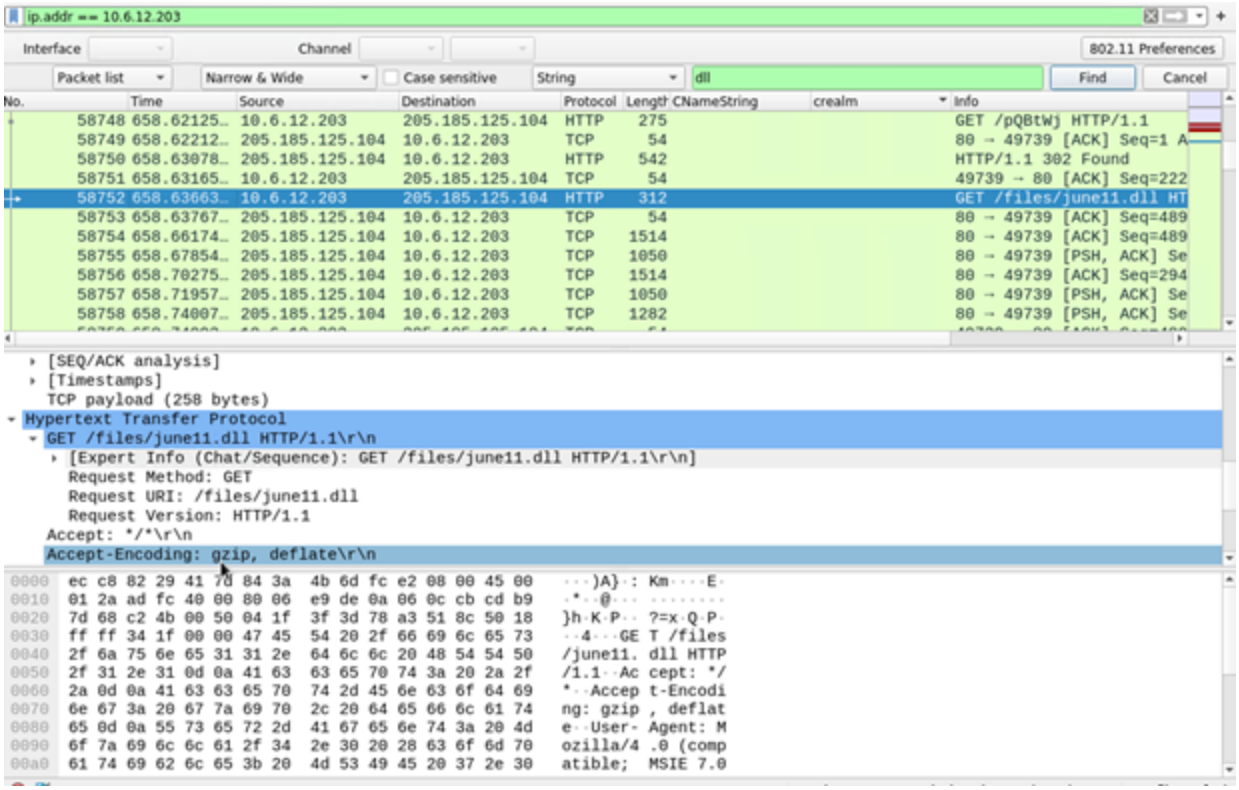


2. What is the IP address of the Domain Controller (DC) of the AD network?

   10.6.12.12

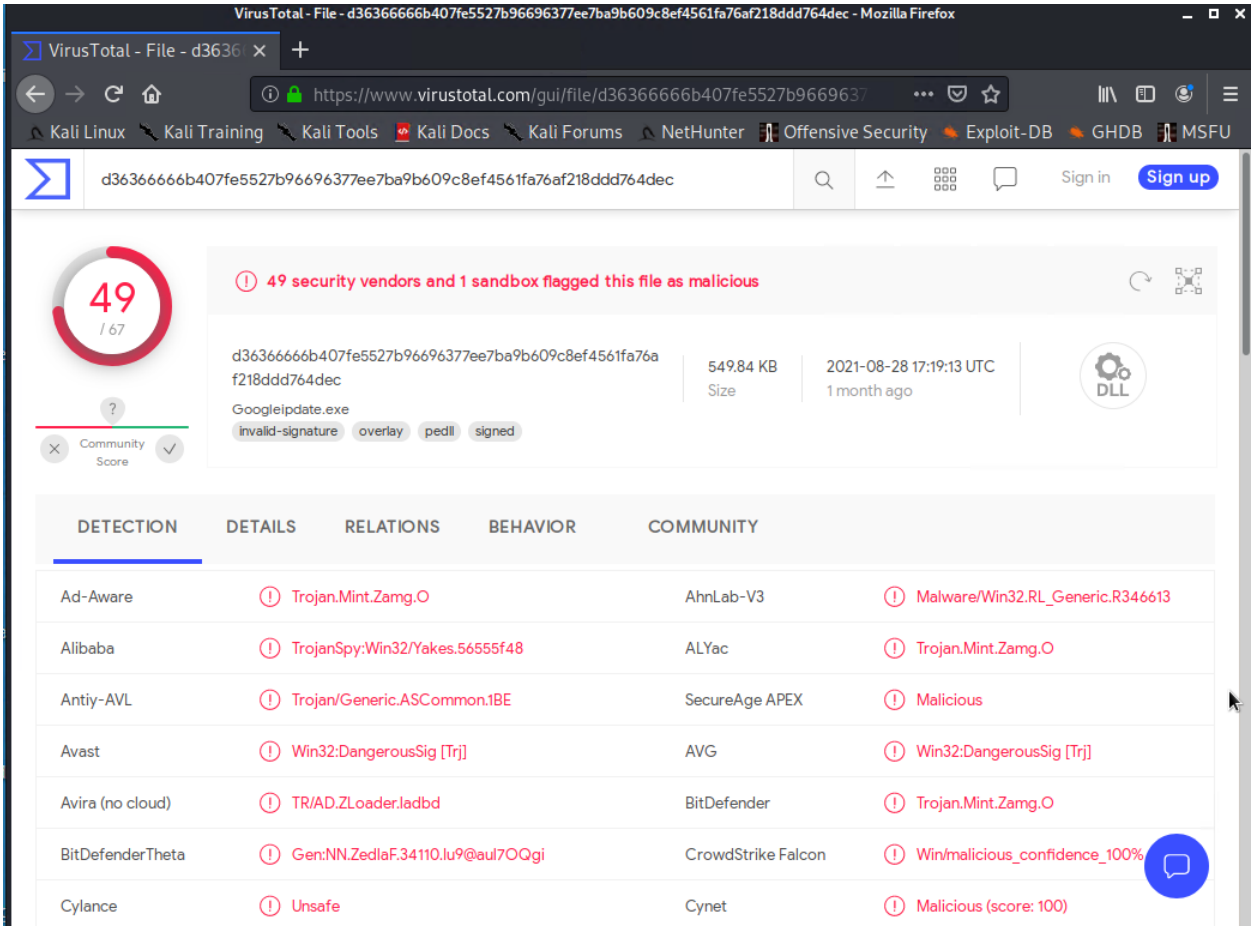
3. What is the name of the malware downloaded to the `10.6.12.203` machine? Once you have found the file, export it to your Kali machine's desktop.

   June11.dll



4. Upload the file to VirusTotal.com. What kind of malware is this classified as?

   Trojan



Vulnerable Windows Machines

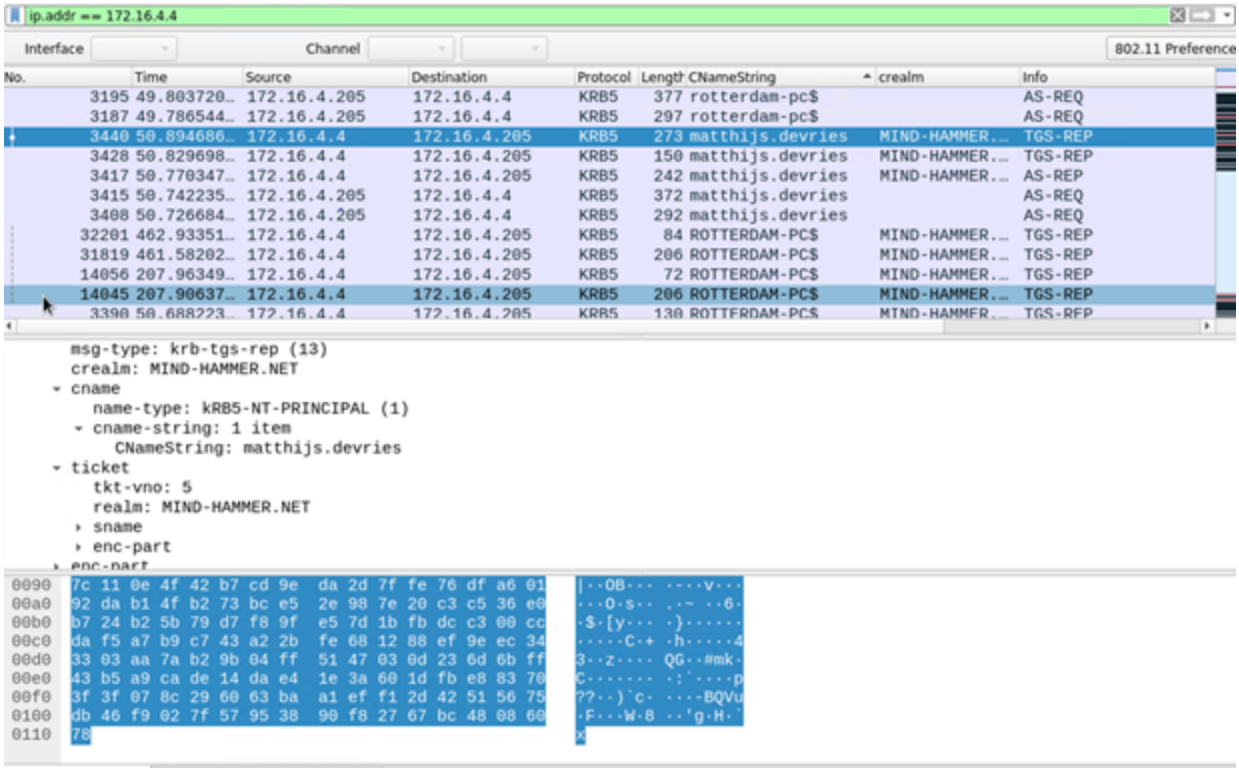
The Security team received reports of an infected Windows host on the network. They know the following:

- 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**
    - 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, 166.62.11.64, 172.16.4.205

4. As a bonus, retrieve the desktop background of the Windows host.

Illegal Downloads

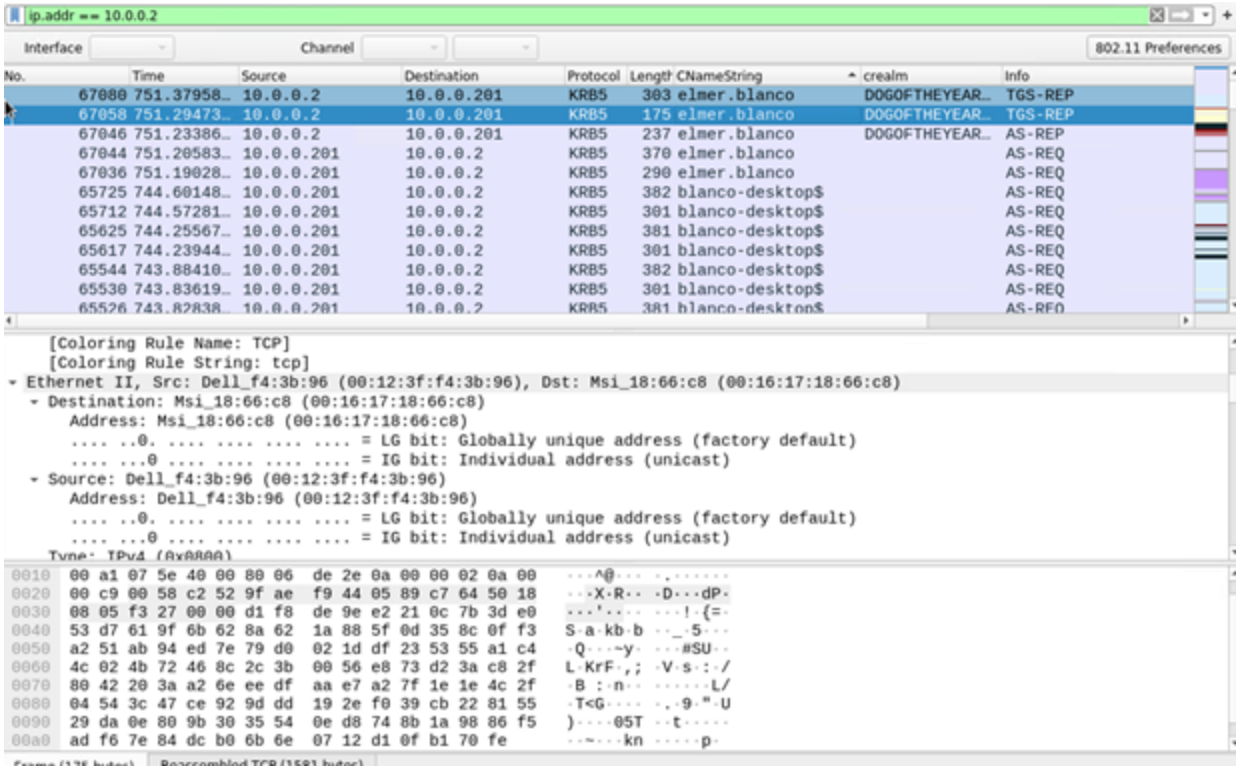
IT was informed that some users are torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringement.

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.

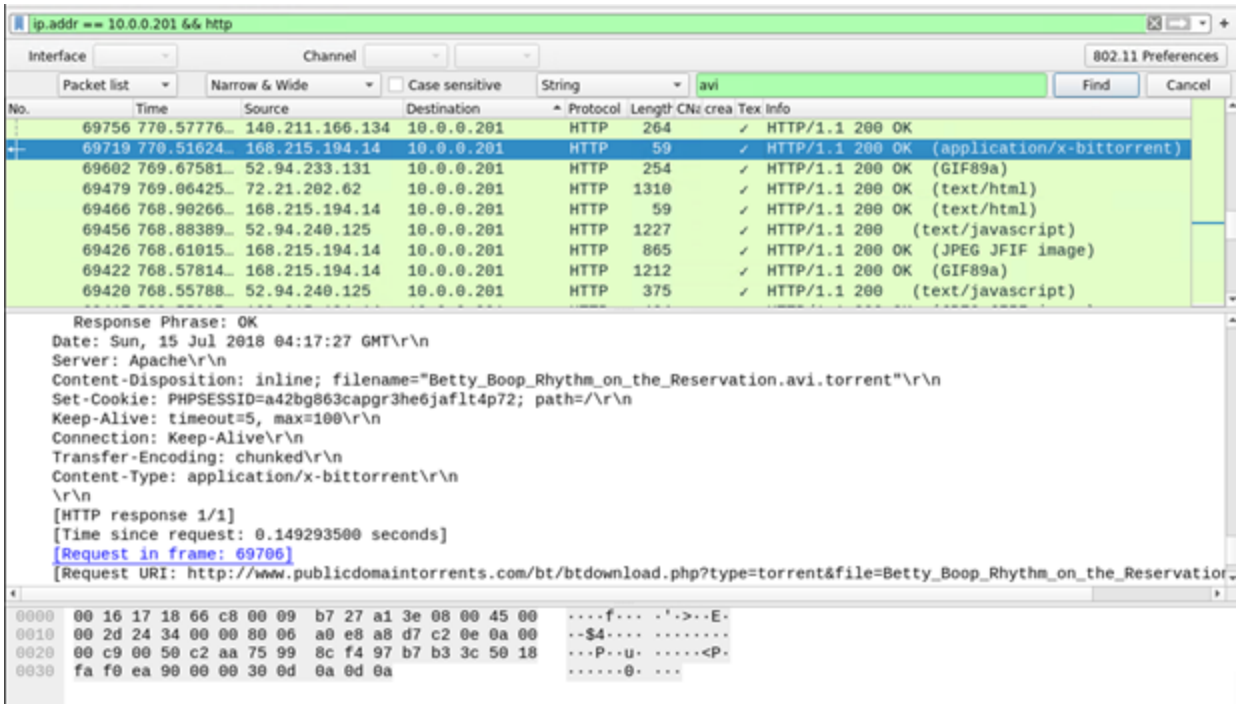
Your task is to isolate torrent traffic and answer the following questions:

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**



2. Which torrent file did the user download?

   Betty_Boop_Rythm_on_the_Reservation.avi.torrent


ip.addr == 10.0.0.201 && http
Interface
Channel
802.11 Preferences
Packet list
Narrow & Wide
Case sensitive
String
avi
Find
Cancel
No. Time Source Destination Protocol Length CNa crea Tex Info
69756 770.57776… 140.211.166.134 10.0.0.201 HTTP 264 ✓ HTTP/1.1 200 OK
69719 770.51624… 168.215.194.14 10.0.0.201 HTTP 59 ✓ HTTP/1.1 200 OK (application/x-bittorrent)
69602 769.67581… 52.94.233.131 10.0.0.201 HTTP 254 ✓ HTTP/1.1 200 OK (GIF89a)
69479 769.06425… 72.21.202.62 10.0.0.201 HTTP 1310 ✓ HTTP/1.1 200 OK (text/html)
69466 768.90266… 168.215.194.14 10.0.0.201 HTTP 59 ✓ HTTP/1.1 200 OK (text/html)
69456 768.88389… 52.94.240.125 10.0.0.201 HTTP 1227 ✓ HTTP/1.1 200 (text/javascript)
69426 768.61015… 168.215.194.14 10.0.0.201 HTTP 865 ✓ HTTP/1.1 200 OK (JPEG JFIF image)
69422 768.57814… 168.215.194.14 10.0.0.201 HTTP 1212 ✓ HTTP/1.1 200 OK (GIF89a)
69420 768.55788… 52.94.240.125 10.0.0.201 HTTP 375 ✓ HTTP/1.1 200 (text/javascript)
Response Phrase: OK
Date: Sun, 15 Jul 2018 04:17:27 GMT\r\n
Server: Apache\r\n
Content-Disposition: inline; filename="Betty_Boop_Rhythm_on_the_Reservation.avi.torrent"\r\n
Set-Cookie: PHPSESSID=a42bg863capgr3he6jaflt4p72; path=/\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Transfer-Encoding: chunked\r\n
Content-Type: application/x-bittorrent\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.149293500 seconds]
[Request in frame: 69706]
[Request URI: http://www.publicdomaintorrents.com/bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation
0000 00 16 17 18 66 c8 00 09 b7 27 a1 3e 08 00 45 00 ····f··· ·'·>··E·
0010 00 2d 24 34 00 00 80 06 a0 e8 a8 d7 c2 0e 0a 00 ·-$4···· ····
0020 00 c9 00 50 c2 aa 75 99 8c f4 97 b7 b3 3c 50 18 ···P··u· ·····<P·
0030 fa f0 ea 90 00 00 30 0d 0a 0d 0a ····0· ···