Network Analysis

Time Thieves

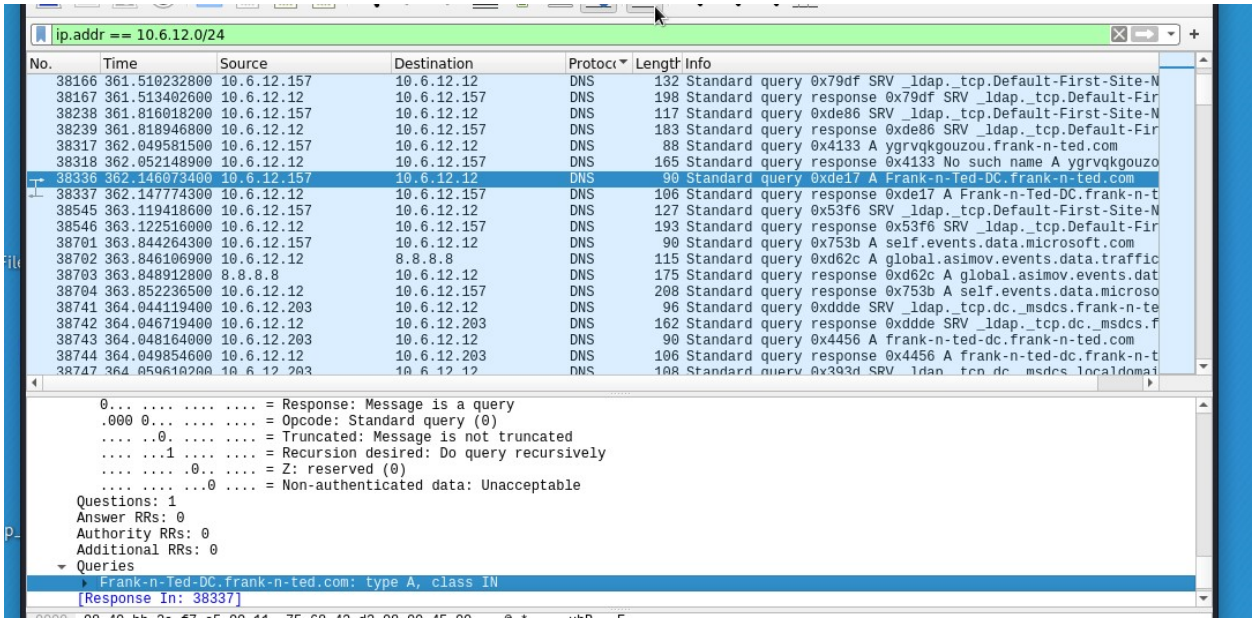
At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- 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:

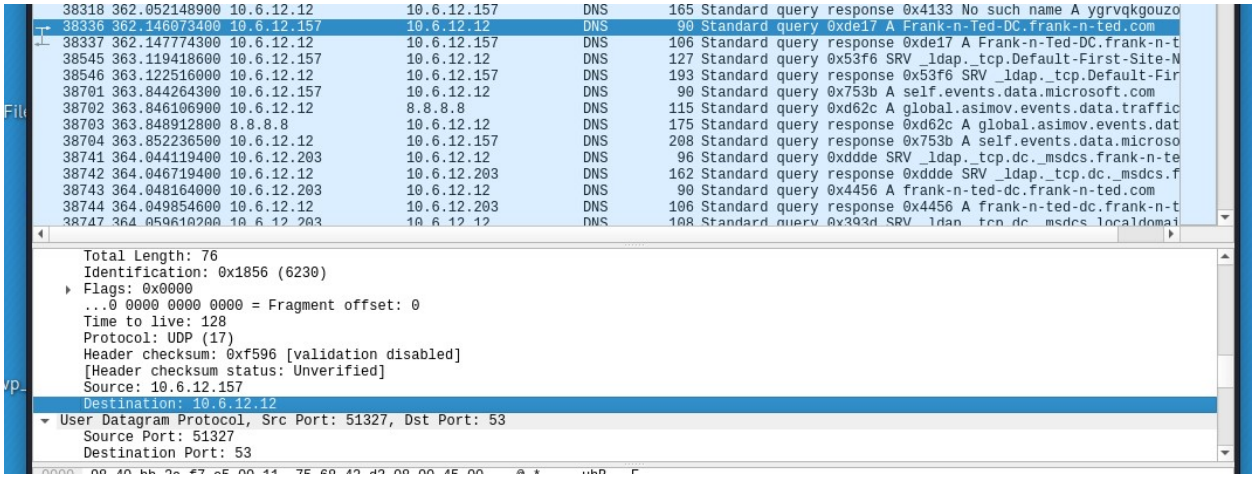
1. What is the domain name of the users' custom site?

   Frank-N Ted -DC.frank-n-ted.com



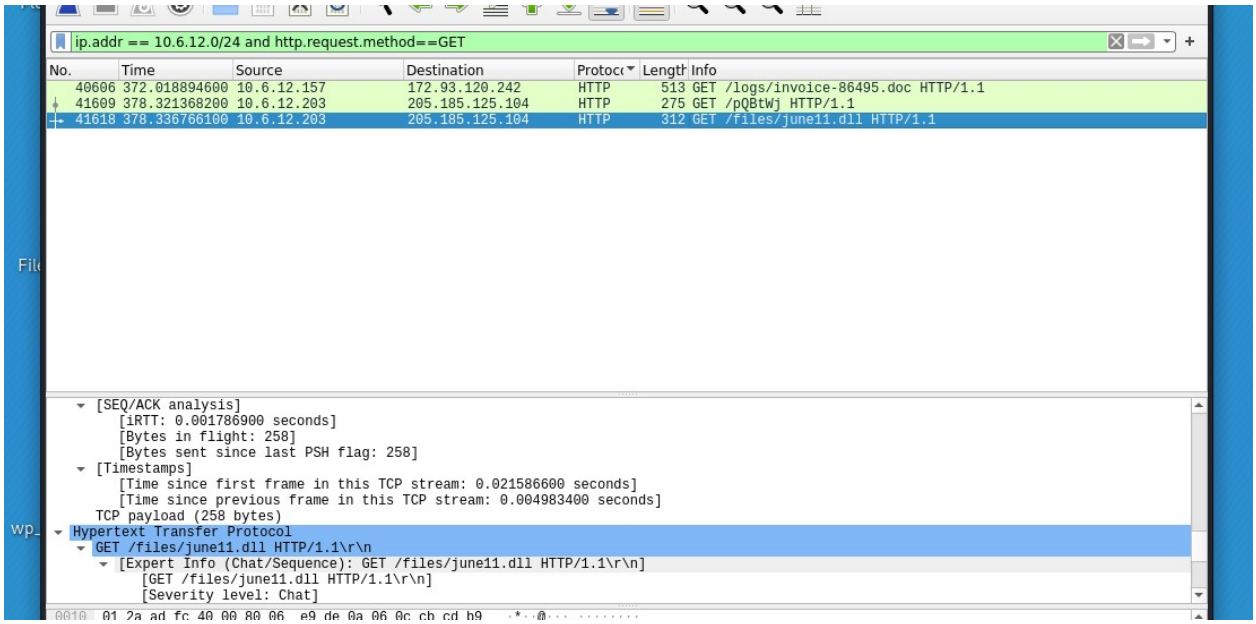
2. What is the IP address of the Domain Controller (DC) of the AD network?

10.6.12.12



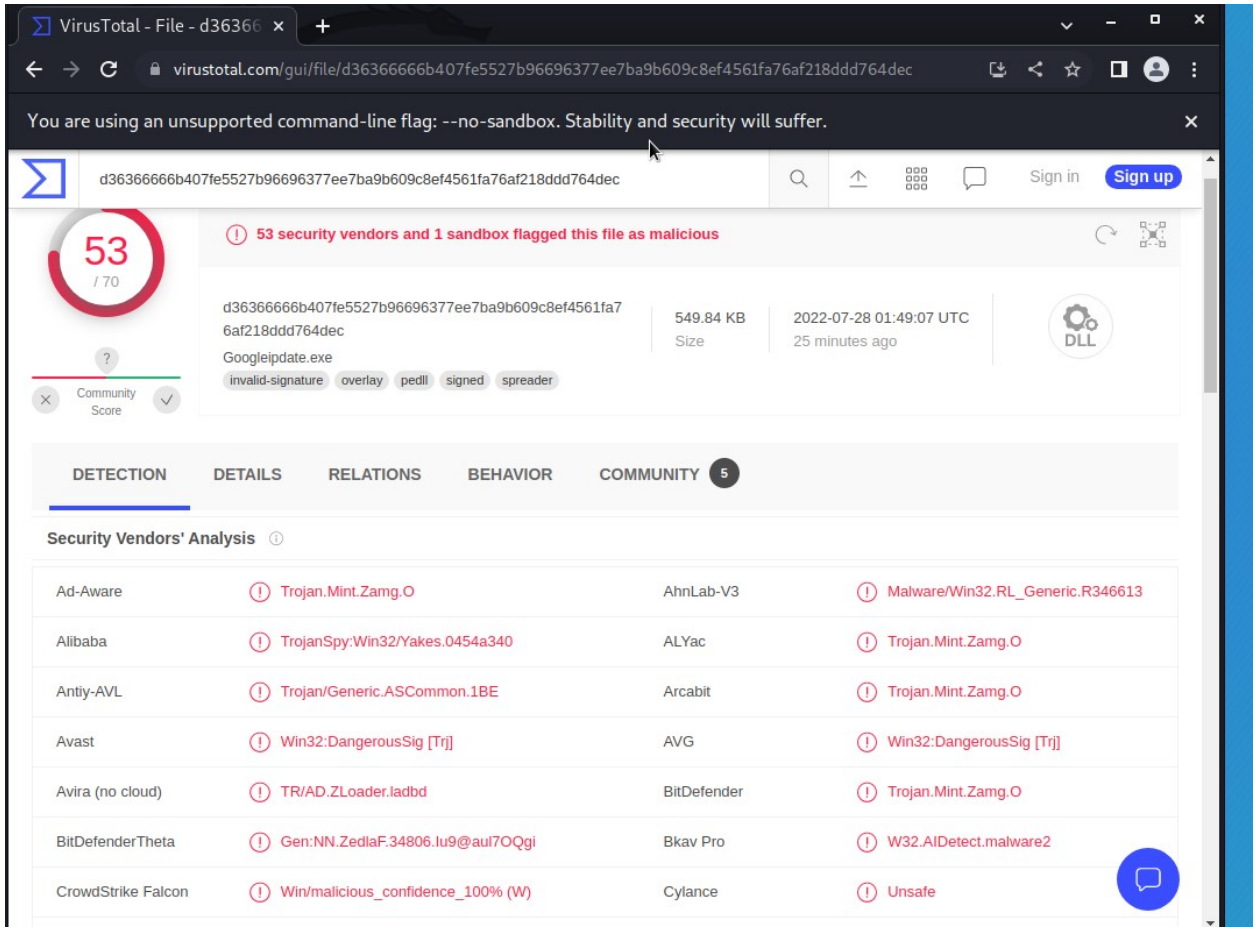
3. What is the name of the malware downloaded to the `10.6.12.203` machine? Once you have found the file, export it to your Kali machine's desktop.

   June11.dll is the malware downloaded



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

   Trojan.mint.Zamg.O



Vulnerable Windows Machines

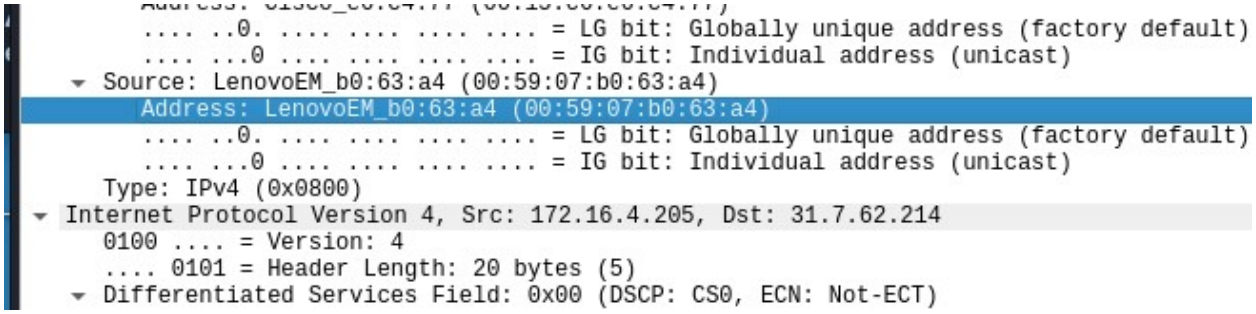
The Security team received reports of an infected Windows host on the network. They know the following:

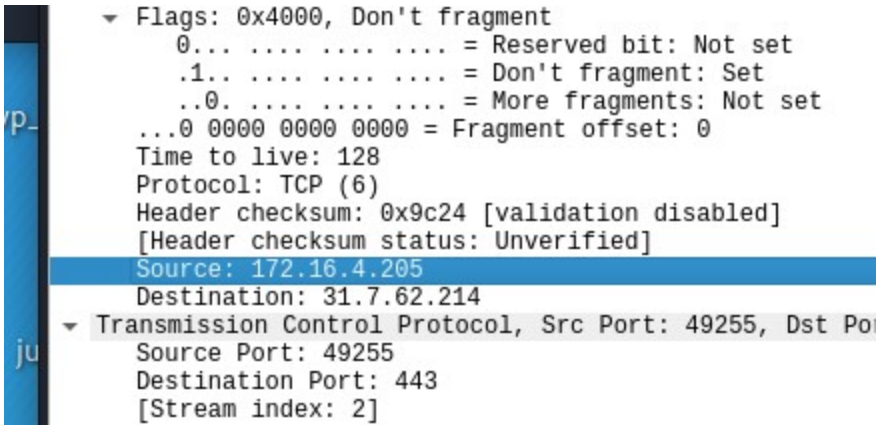
- Machines in the network live in the range `172.16.4.0/24`.
- The domain mind-hammer.net is associated with the infected computer.
- The DC for this network lives at `172.16.4.4` and is named Mind-Hammer-DC.
- The network has standard gateway and broadcast addresses.

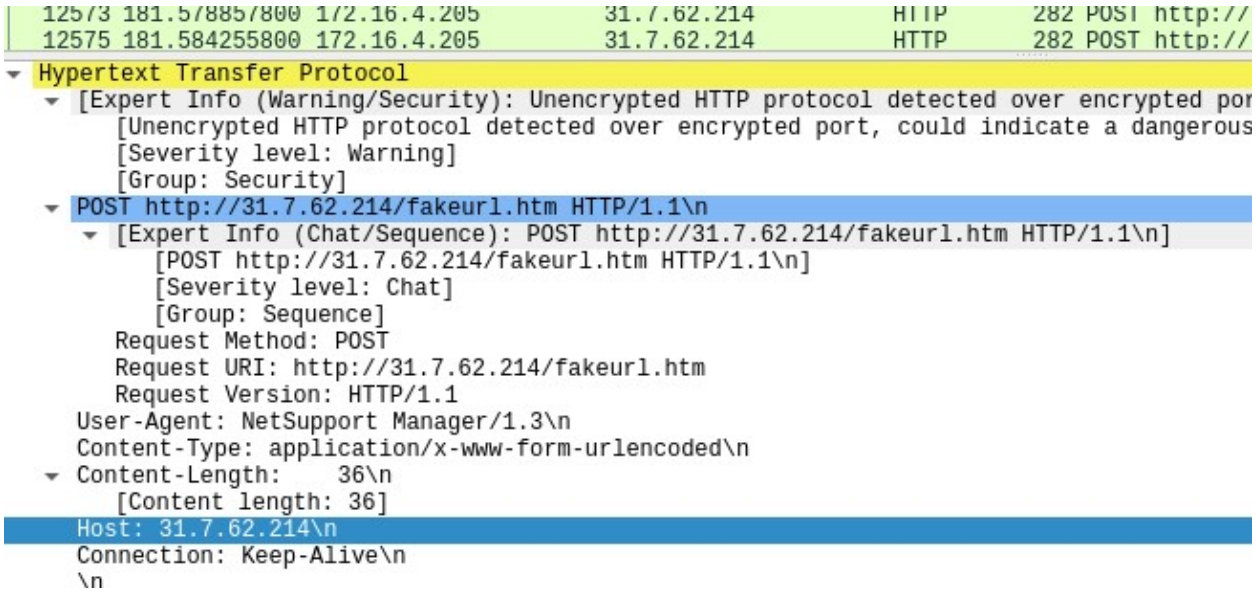
Inspect your traffic to answer the following questions:

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

- Host name: Rotterdam-PC
- IP address: 172.16.4.205
- MAC address: 00:59:07:b0:63:a4

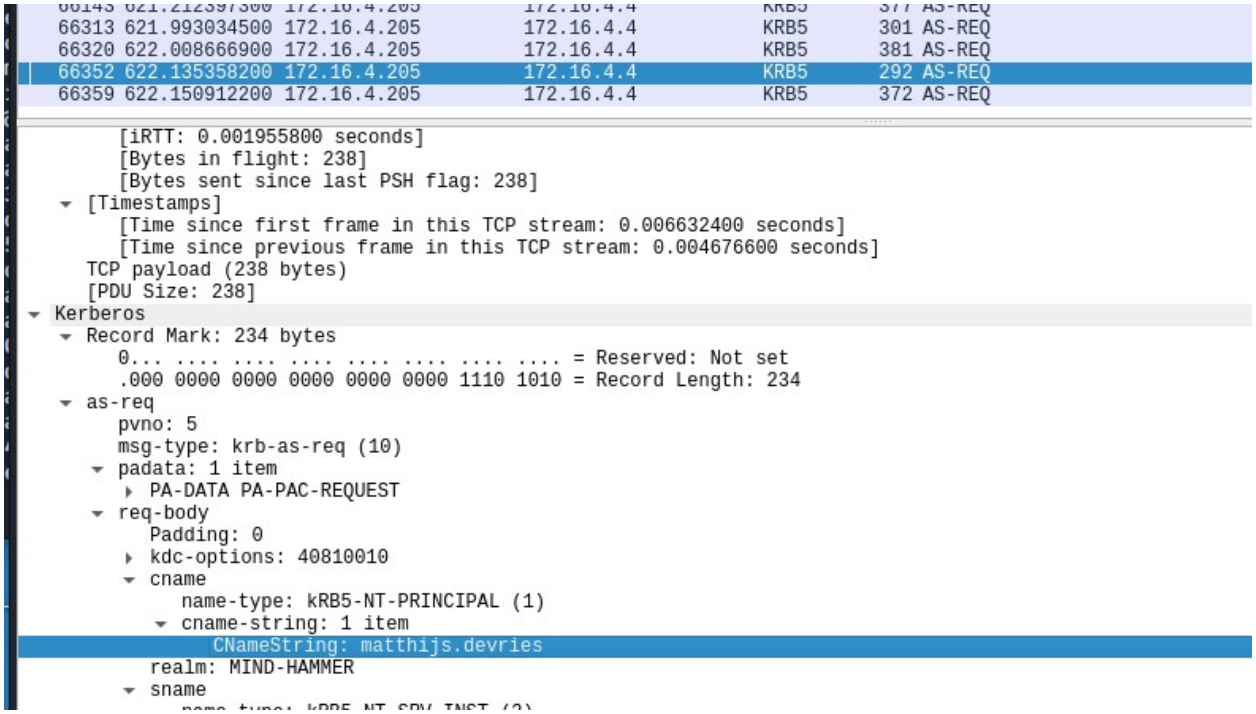






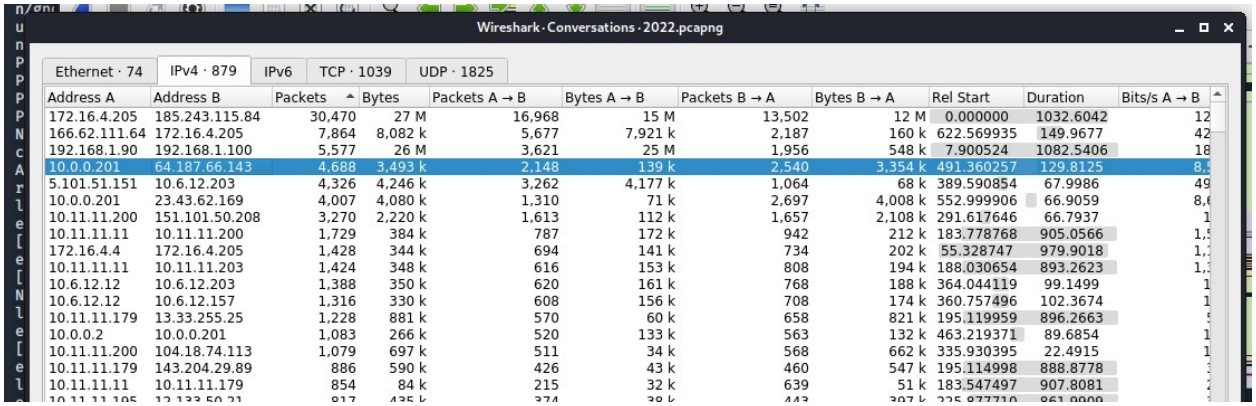
2. What is the username of the Windows user whose computer is infected?

Matthijs.devries



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

   172.16.4.205, 185.243.115.84, 64.187.66.143



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

Illegal Downloads

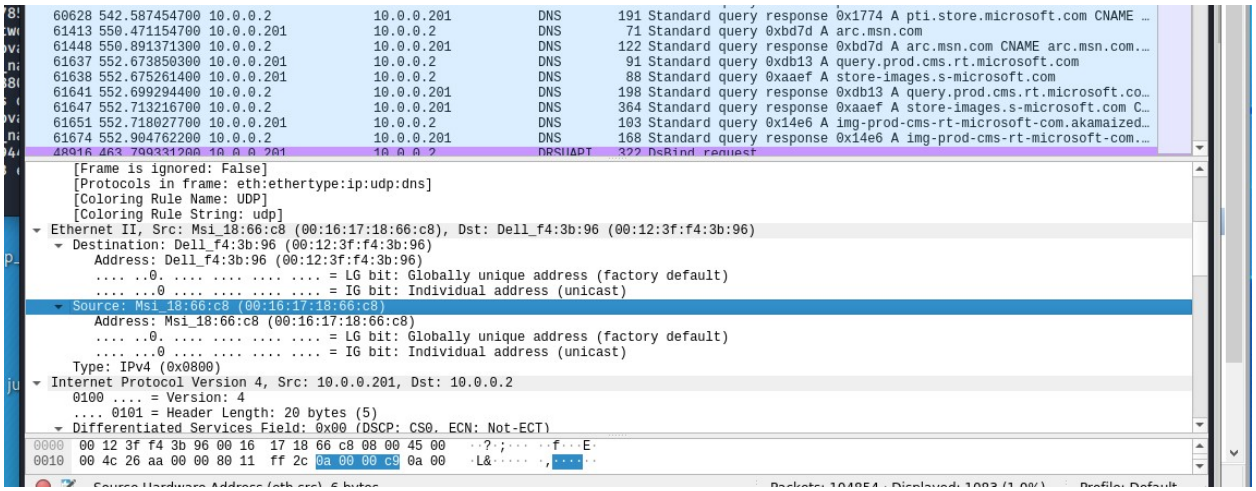
IT was informed that some users are torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringement.

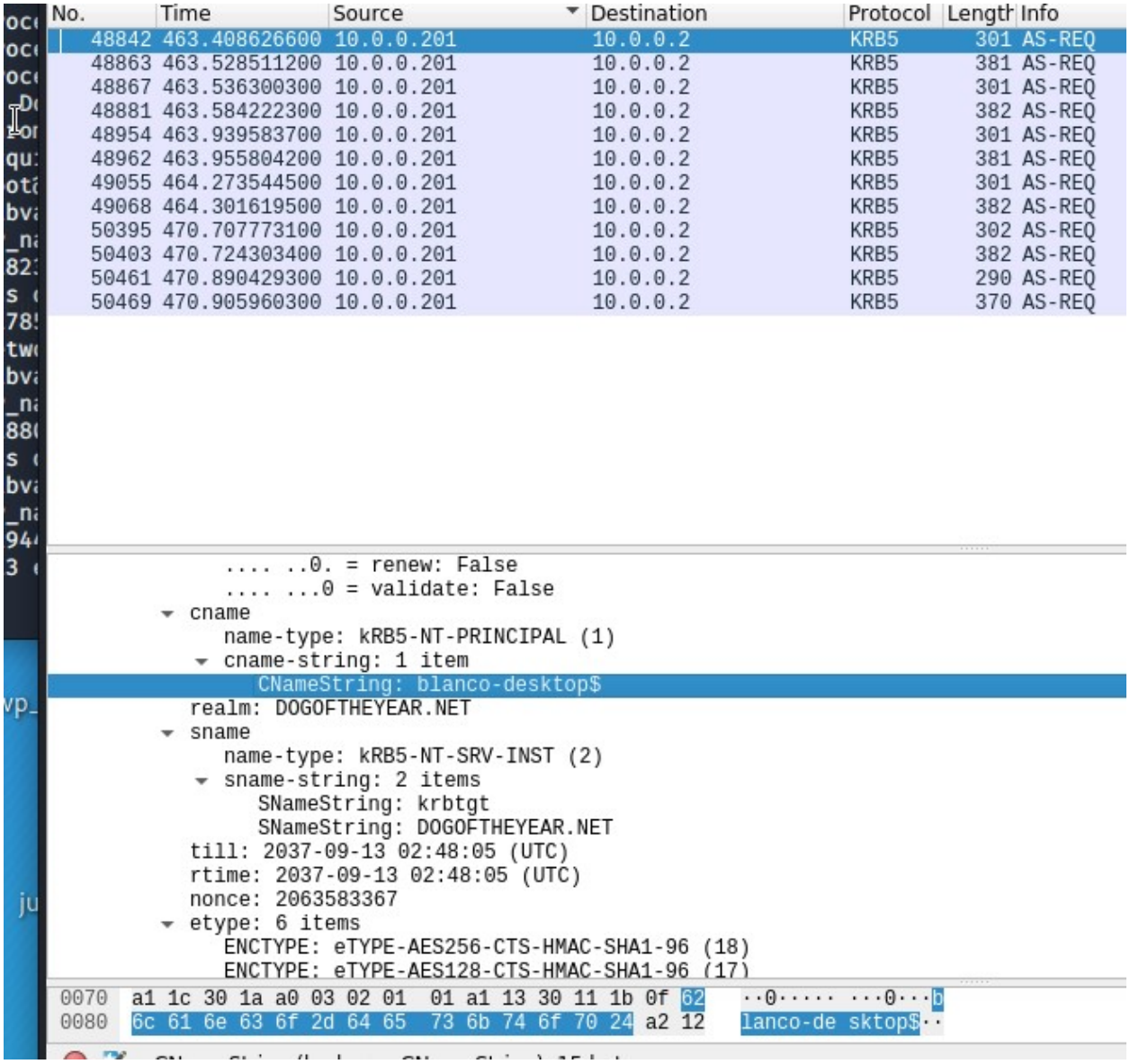
IT shared the following about the torrent activity:

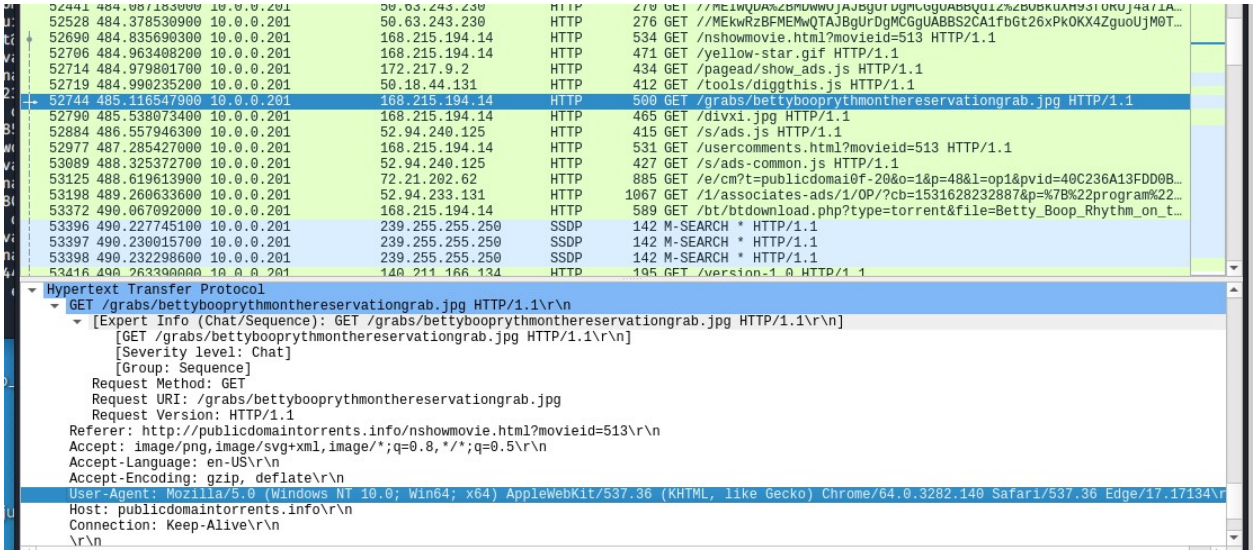
- The machines using torrents live in the range 10.0.0.0/24 and are clients of an AD domain.
- The DC of this domain lives at 10.0.0.2 and is named DogOfTheYear-DC.
- The DC is associated with the domain dogoftheyear.net.

Your task is to isolate torrent traffic and answer the following questions 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 blanco-desktop$
    - OS version Window NT 10.0




No. Time Source Destination Protocol Length Info
48842 463.408626600 10.0.0.201 10.0.0.2 KRB5 301 AS-REQ
48863 463.528511200 10.0.0.201 10.0.0.2 KRB5 381 AS-REQ
48867 463.536300300 10.0.0.201 10.0.0.2 KRB5 301 AS-REQ
48881 463.584222300 10.0.0.201 10.0.0.2 KRB5 382 AS-REQ
48954 463.939583700 10.0.0.201 10.0.0.2 KRB5 301 AS-REQ
48962 463.955804200 10.0.0.201 10.0.0.2 KRB5 381 AS-REQ
49055 464.273544500 10.0.0.201 10.0.0.2 KRB5 301 AS-REQ
49068 464.301619500 10.0.0.201 10.0.0.2 KRB5 382 AS-REQ
50395 470.707773100 10.0.0.201 10.0.0.2 KRB5 302 AS-REQ
50403 470.724303400 10.0.0.201 10.0.0.2 KRB5 382 AS-REQ
50461 470.890429300 10.0.0.201 10.0.0.2 KRB5 290 AS-REQ
50469 470.905960300 10.0.0.201 10.0.0.2 KRB5 370 AS-REQ
.... ..0. = renew: False
....0 = validate: False
cname
name-type: kRB5-NT-PRINCIPAL (1)
cname-string: 1 item
CNameString: blanco-desktop$
realm: DOGOFTHEYEAR.NET
sname
name-type: kRB5-NT-SRV-INST (2)
sname-string: 2 items
SNameString: krbtgt
SNameString: DOGOFTHEYEAR.NET
till: 2037-09-13 02:48:05 (UTC)
rtime: 2037-09-13 02:48:05 (UTC)
nonce: 2063583367
etype: 6 items
ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
0070 a1 1c 30 1a a0 03 02 01 01 a1 13 30 11 1b 0f 62 ··0····· ···0···b
0080 6c 61 6e 63 6f 2d 64 65 73 6b 74 6f 70 24 a2 12 lanco-de sktop$··



2. Which torrent file did the user download?

   Betty boop rhythm on the reservation.avi