Network Analysis

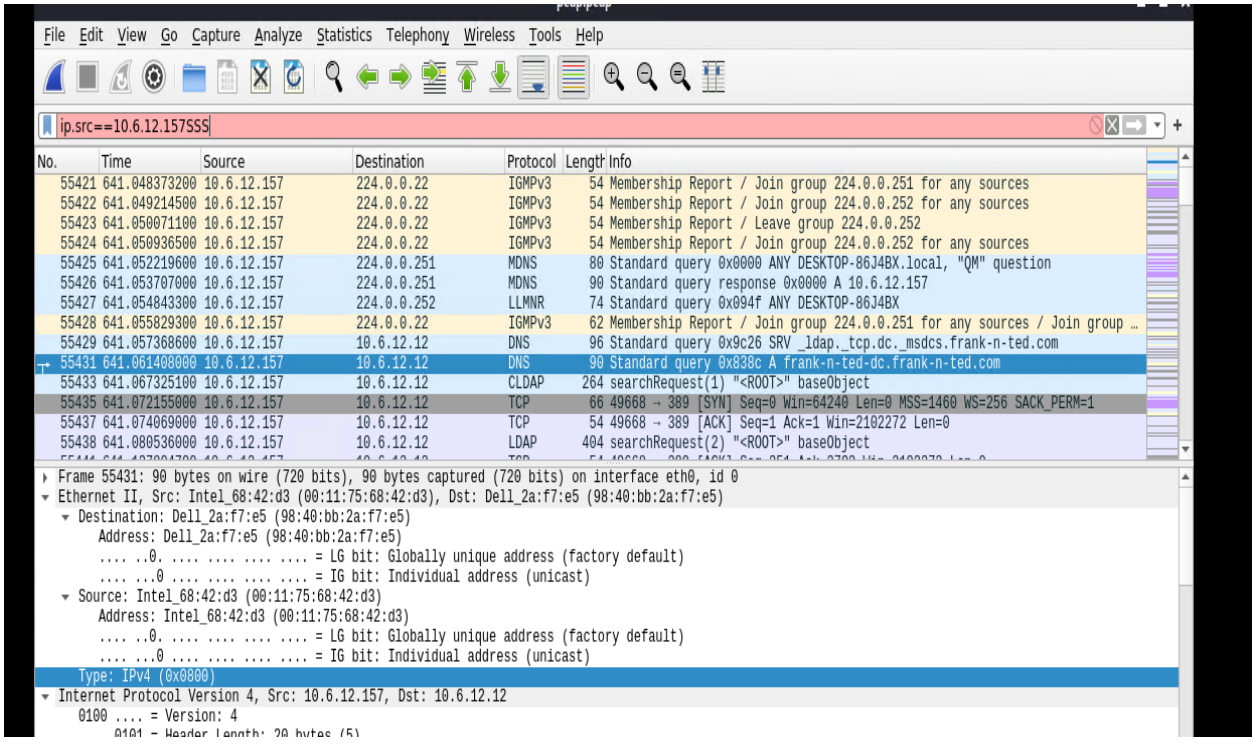
Time Thieves

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`.

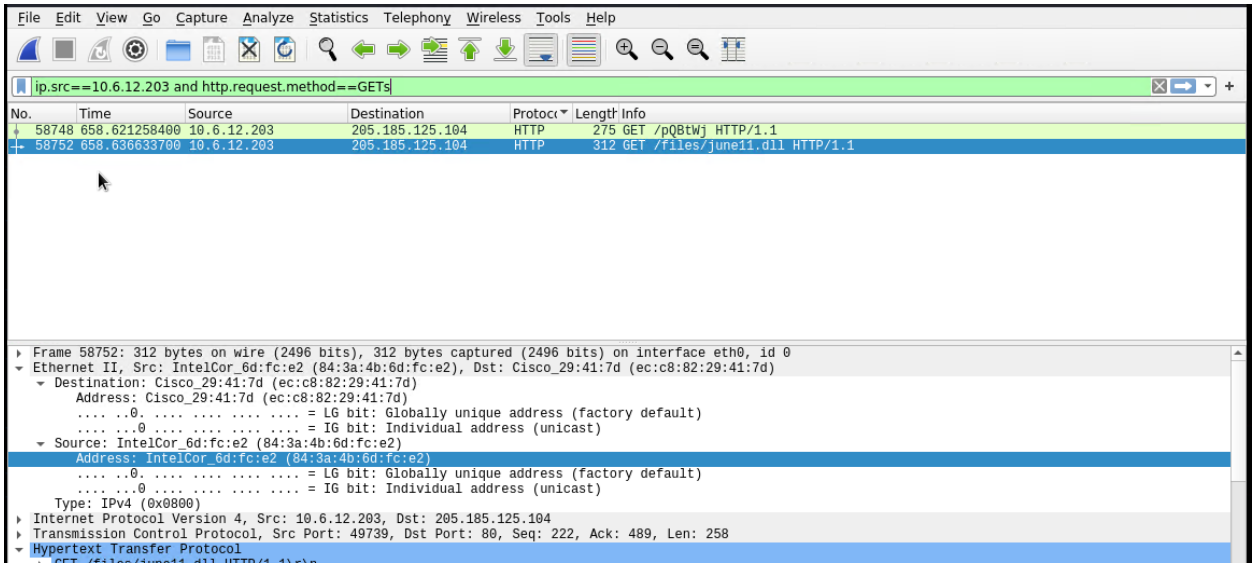
You must inspect your traffic capture to answer the following questions:

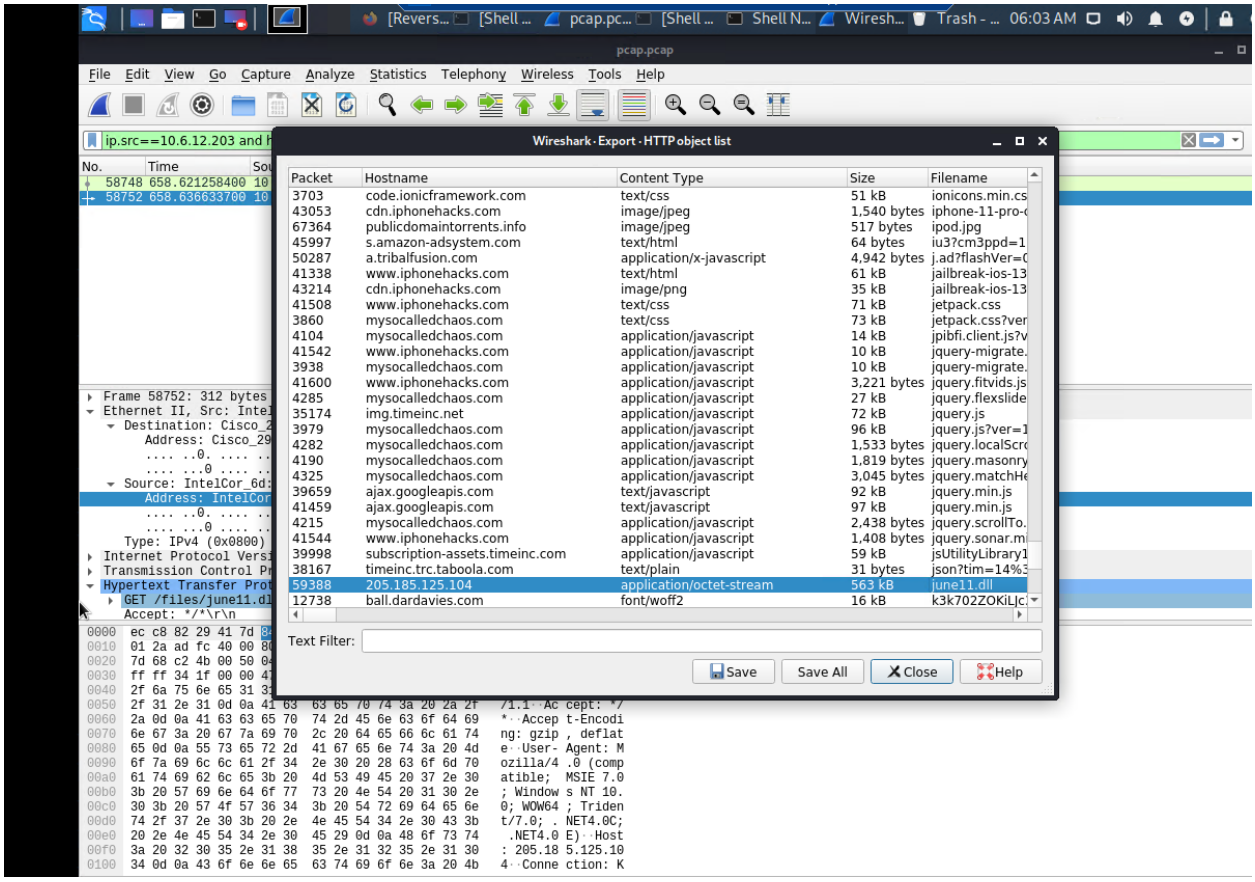
- What is the domain name of the users' custom site?
    - frank-n-ted-dc.frank-n-ted.com



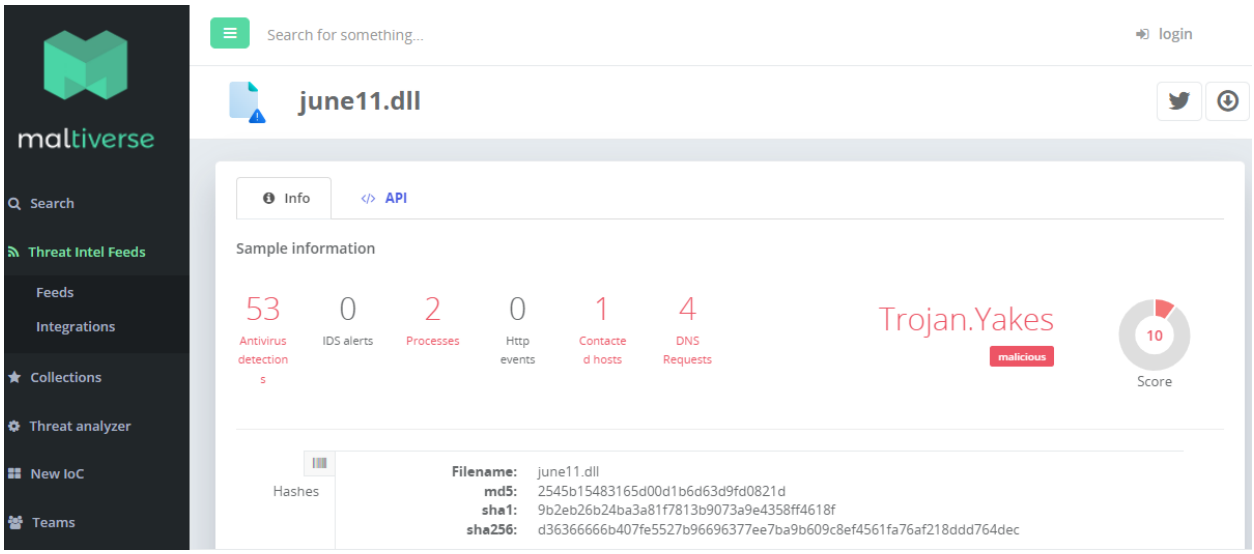
- What is the IP address of the Domain Controller (DC) of the AD network?
    - 10.6.12.12 (source in the screenshot above)

- 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





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



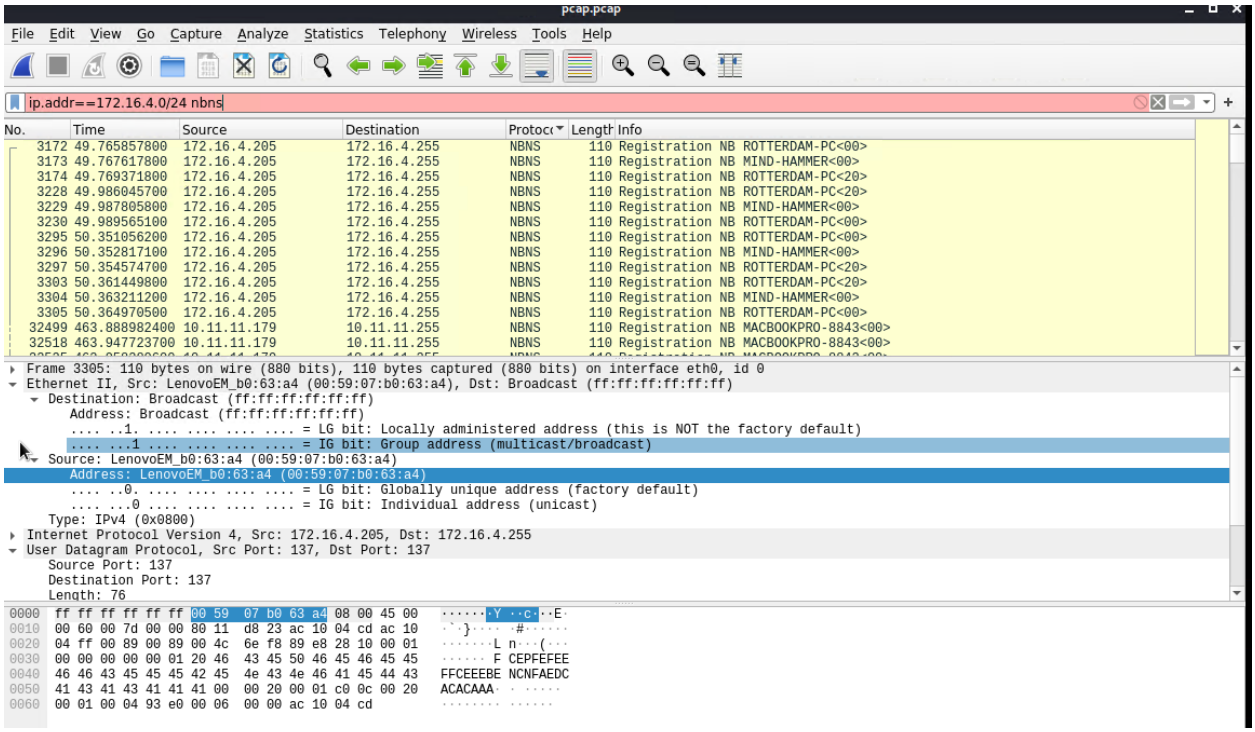
Vulnerable Windows Machines

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

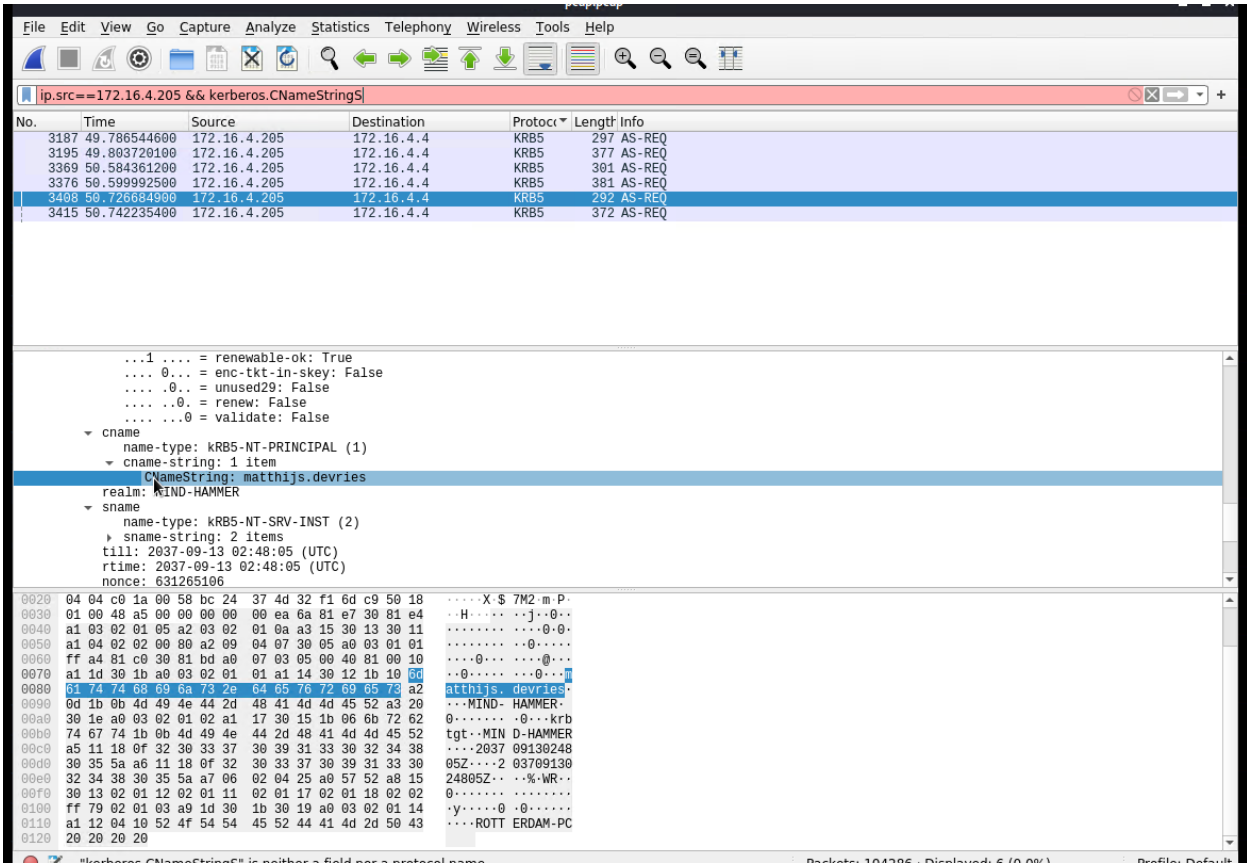
- Machines in the network live in the range `172.16.4.0/24`.
- The domain mind-hammer.net is associated with the infected computer.
- The DC for this network lives at `172.16.4.4` and is named Mind-Hammer-DC.
- The network has standard gateway and broadcast addresses.

Inspect your traffic to answer the following questions:

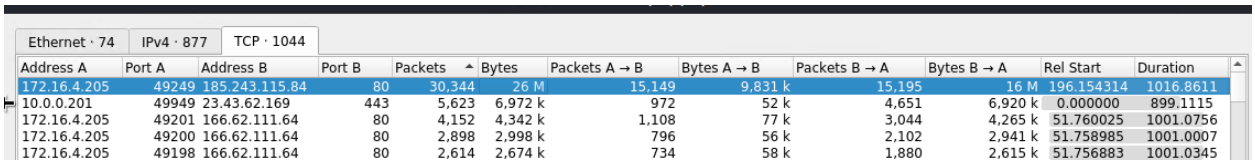
- Find the following information about the infected Windows machine:
    - Host name: ROTTERDAMN-PC
    - IP address: 172.16.4.205
    - MAC address: 00:59:07:B0:63:A4



- What is the username of the Windows user whose computer is infected?
    - Matthijs.devries



- What are the IP addresses used in the actual infection traffic?
    - 172.16.4.205 infected 185.243.115.84, based on large number of packets transmitted to the IP



Illegal Downloads

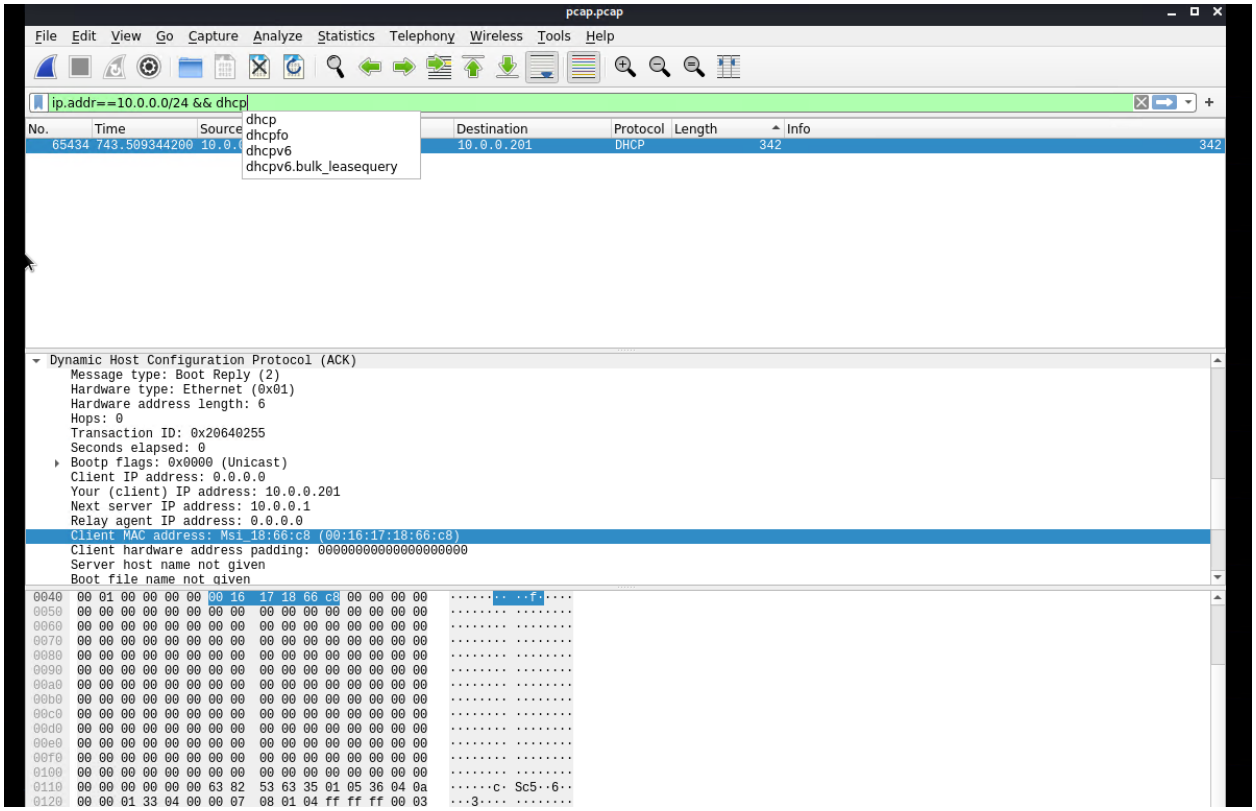
IT was informed that some users are torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringement.

IT shared the following about the torrent activity:

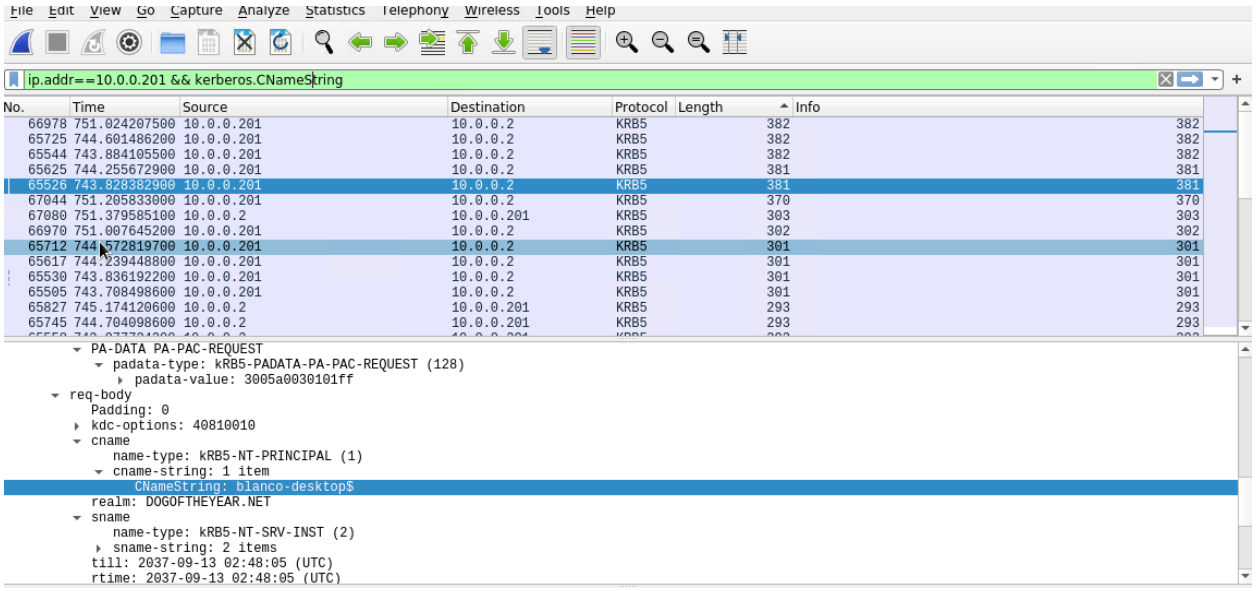
- The machines using torrents live in the range `10.0.0.0/24` and are clients of an AD domain.
- The DC of this domain lives at `10.0.0.2` and is named DogOfTheYear-DC.
- The DC is associated with the domain dogoftheyear.net.

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

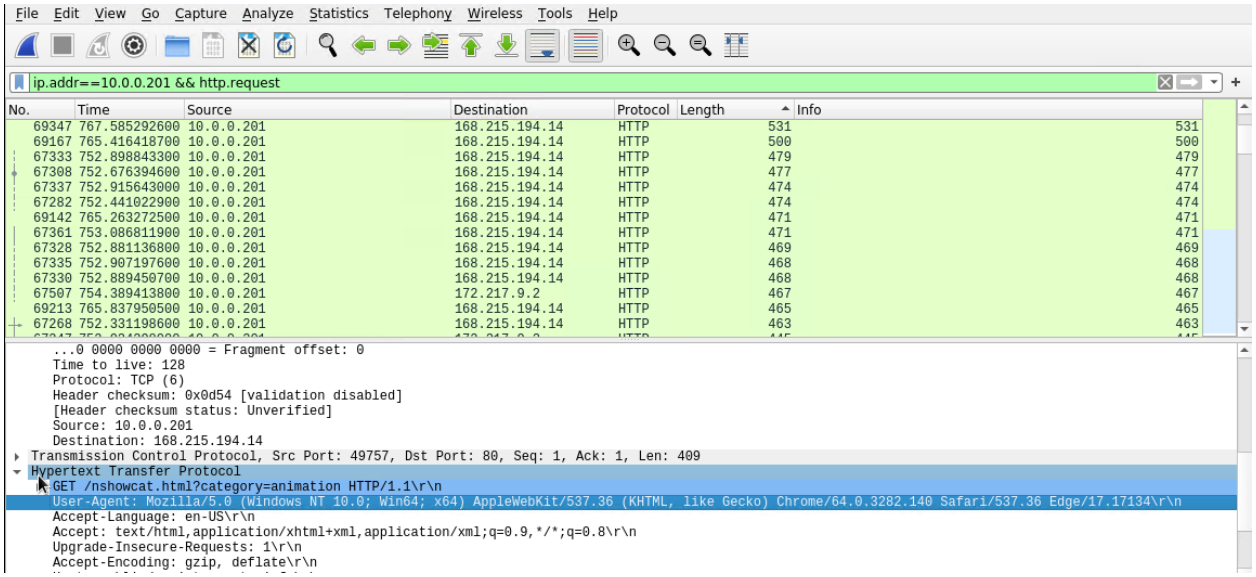
- Find the following information about the machine with IP address `10.0.0.201`:
    - MAC address: 00:16:17:18:66:c8



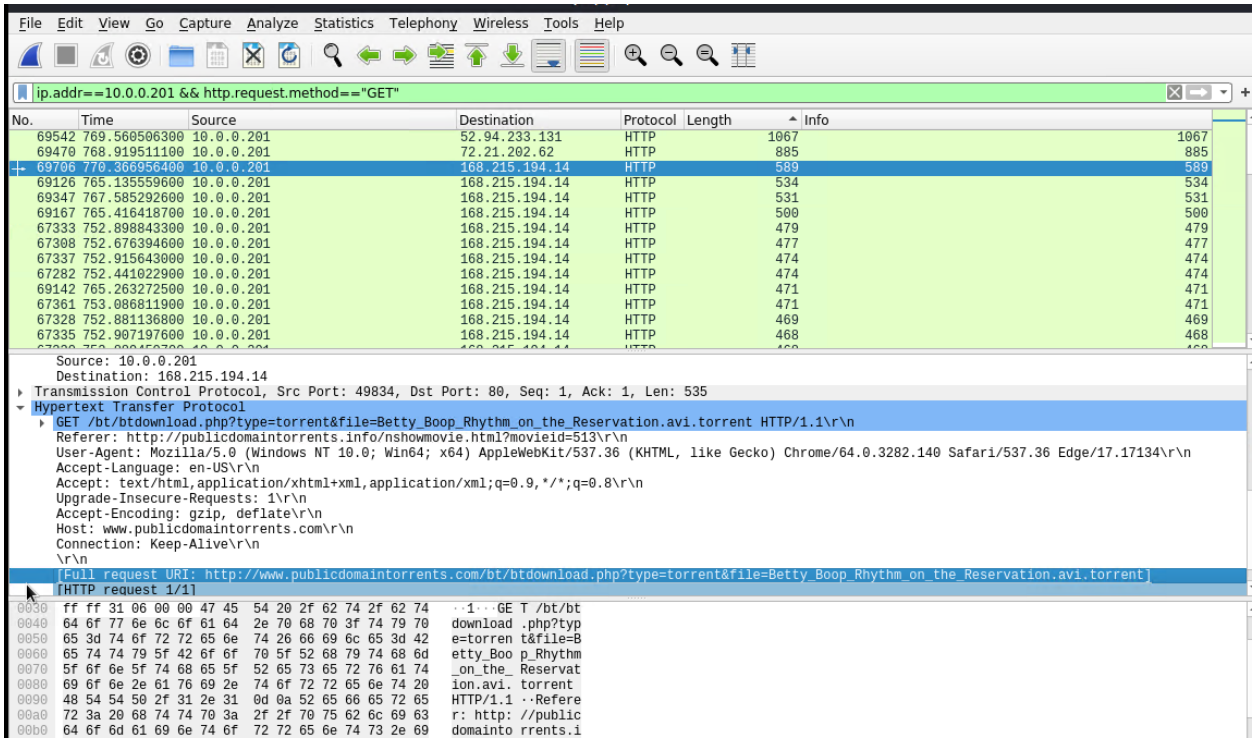
    - Windows username: blanco-desktop$



- OS version: Windows NT 10.0



- Which torrent file did the user download?
  - Betty_Boop_Rythm_on_the_Reservation.avi.torrent


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==10.0.0.201 && http.request.method=="GET"
No. Time Source Destination Protocol Length Info
69542 769.560506300 10.0.0.201 52.94.233.131 HTTP 1067 1067
69470 768.919511100 10.0.0.201 72.21.202.62 HTTP 885 885
69706 770.366956400 10.0.0.201 168.215.194.14 HTTP 589 589
69126 765.135559600 10.0.0.201 168.215.194.14 HTTP 534 534
69347 767.585292600 10.0.0.201 168.215.194.14 HTTP 531 531
69167 765.416418700 10.0.0.201 168.215.194.14 HTTP 500 500
67333 752.898843300 10.0.0.201 168.215.194.14 HTTP 479 479
67308 752.676394600 10.0.0.201 168.215.194.14 HTTP 477 477
67337 752.915643000 10.0.0.201 168.215.194.14 HTTP 474 474
67282 752.441022900 10.0.0.201 168.215.194.14 HTTP 474 474
69142 765.263272500 10.0.0.201 168.215.194.14 HTTP 471 471
67361 753.086811900 10.0.0.201 168.215.194.14 HTTP 471 471
67328 752.881136800 10.0.0.201 168.215.194.14 HTTP 469 469
67335 752.907197600 10.0.0.201 168.215.194.14 HTTP 468 468
Source: 10.0.0.201
Destination: 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
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/17.17134\r\n
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
[Full request URI: http://www.publicdomaintorrents.com/bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent]
[HTTP request 1/1]
0030 ff ff 31 06 00 00 47 45 54 20 2f 62 74 2f 62 74 ··1···GE T /bt/bt
0040 64 6f 77 6e 6c 6f 61 64 2e 70 68 70 3f 74 79 70 download .php?typ
0050 65 3d 74 6f 72 72 65 6e 74 26 66 69 6c 65 3d 42 e=torren t&file=B
0060 65 74 74 79 5f 42 6f 6f 70 5f 52 68 79 74 68 6d etty_Boo p_Rhythm
0070 5f 6f 6e 5f 74 68 65 5f 52 65 73 65 72 76 61 74 _on_the_ Reservat
0080 69 6f 6e 2e 61 76 69 2e 74 6f 72 72 65 6e 74 20 ion.avi. torrent
0090 48 54 54 50 2f 31 2e 31 0d 0a 52 65 66 65 72 65 HTTP/1.1 ··Refere
00a0 72 3a 20 68 74 74 70 3a 2f 2f 70 75 62 6c 69 63 r: http: //public
00b0 64 6f 6d 61 69 6e 74 6f 72 72 65 6e 74 73 2e 69 domainto rrents.i