Network Analysis

Time Thieves

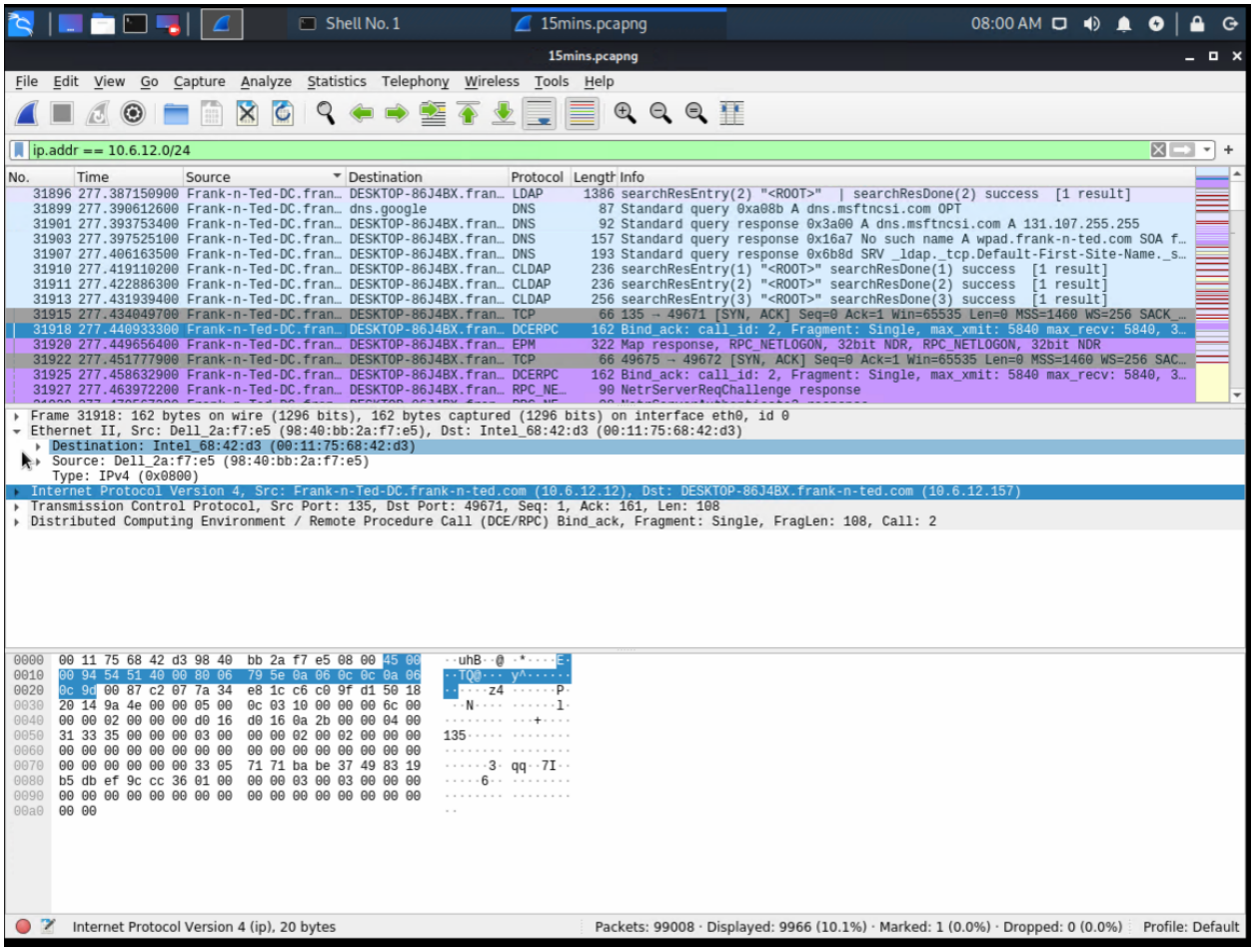
At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- 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:

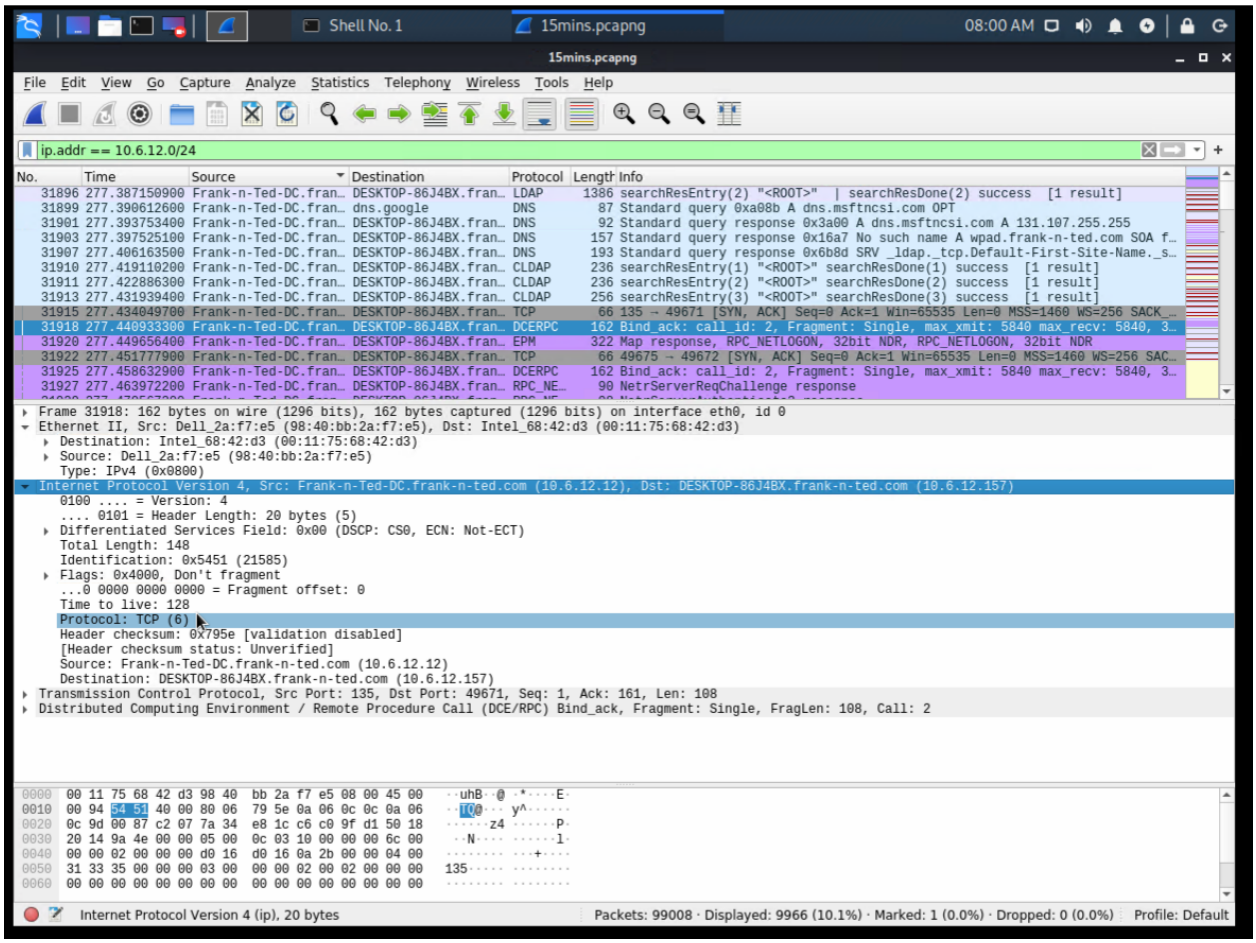
1. What is the domain name of the users' custom site?

The domain name is Frank-nTed-DC.frank-n-ted.com



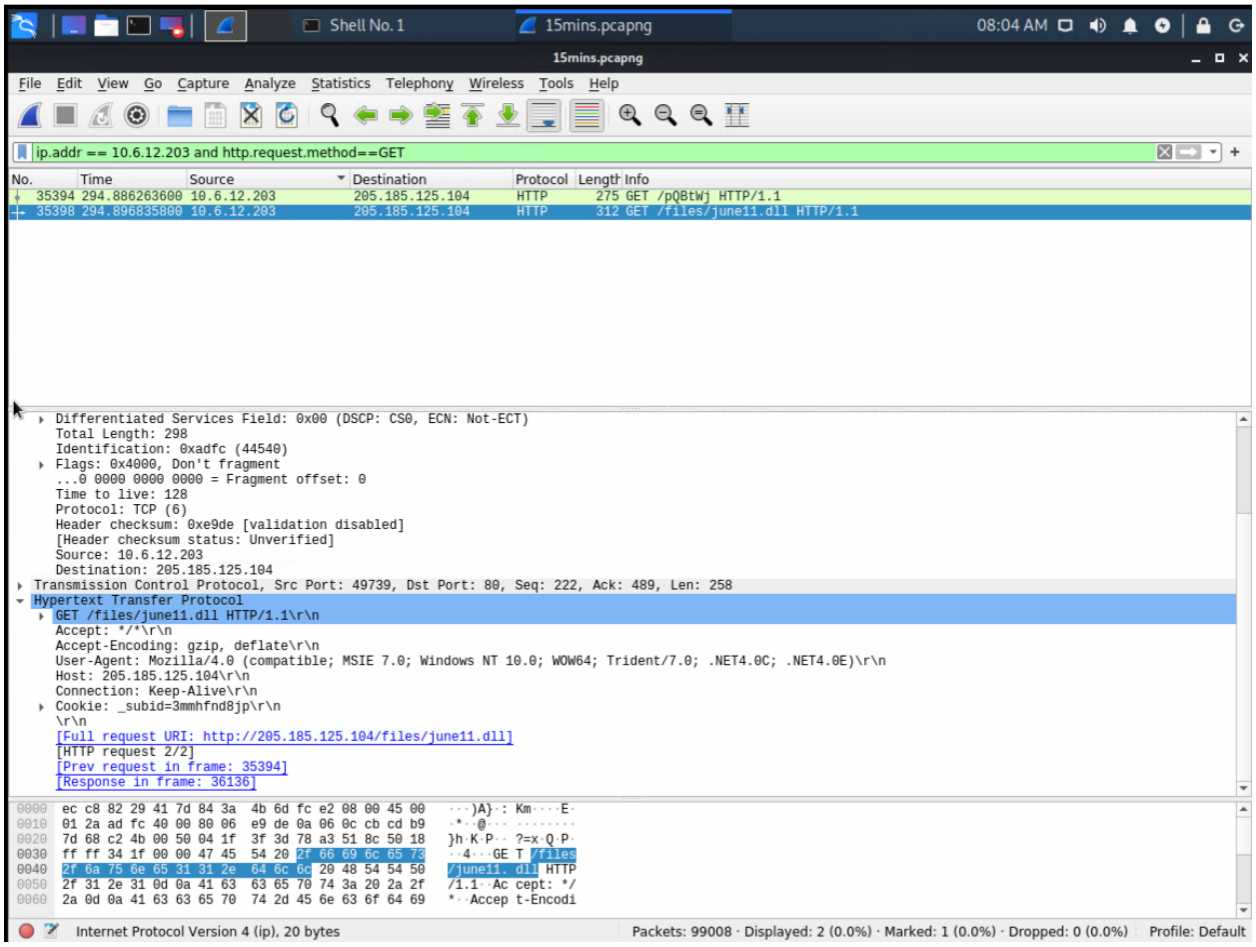
2. What is the IP address of the Domain Controller (DC) of the AD network?

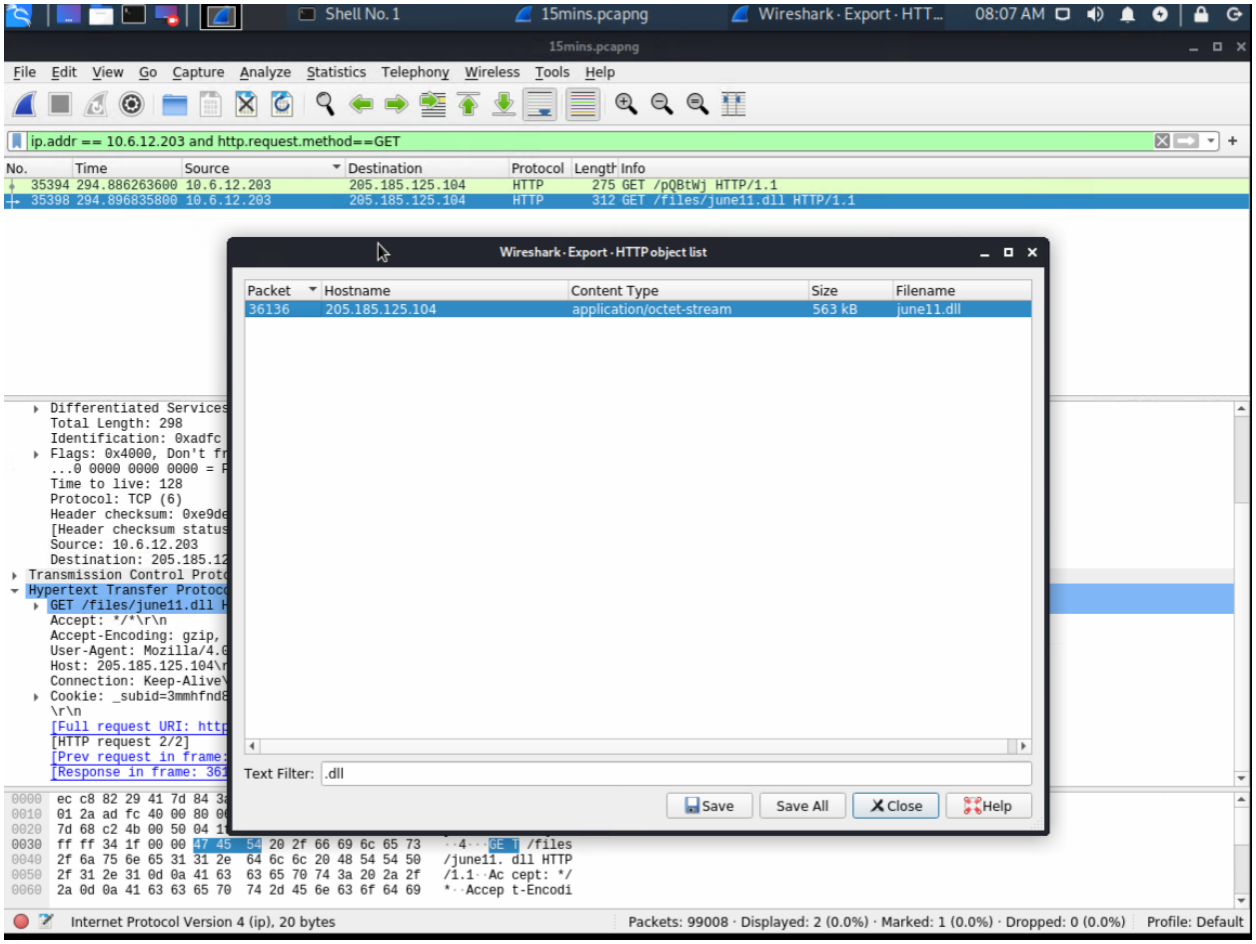
IP address is 10.6.12.12



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.

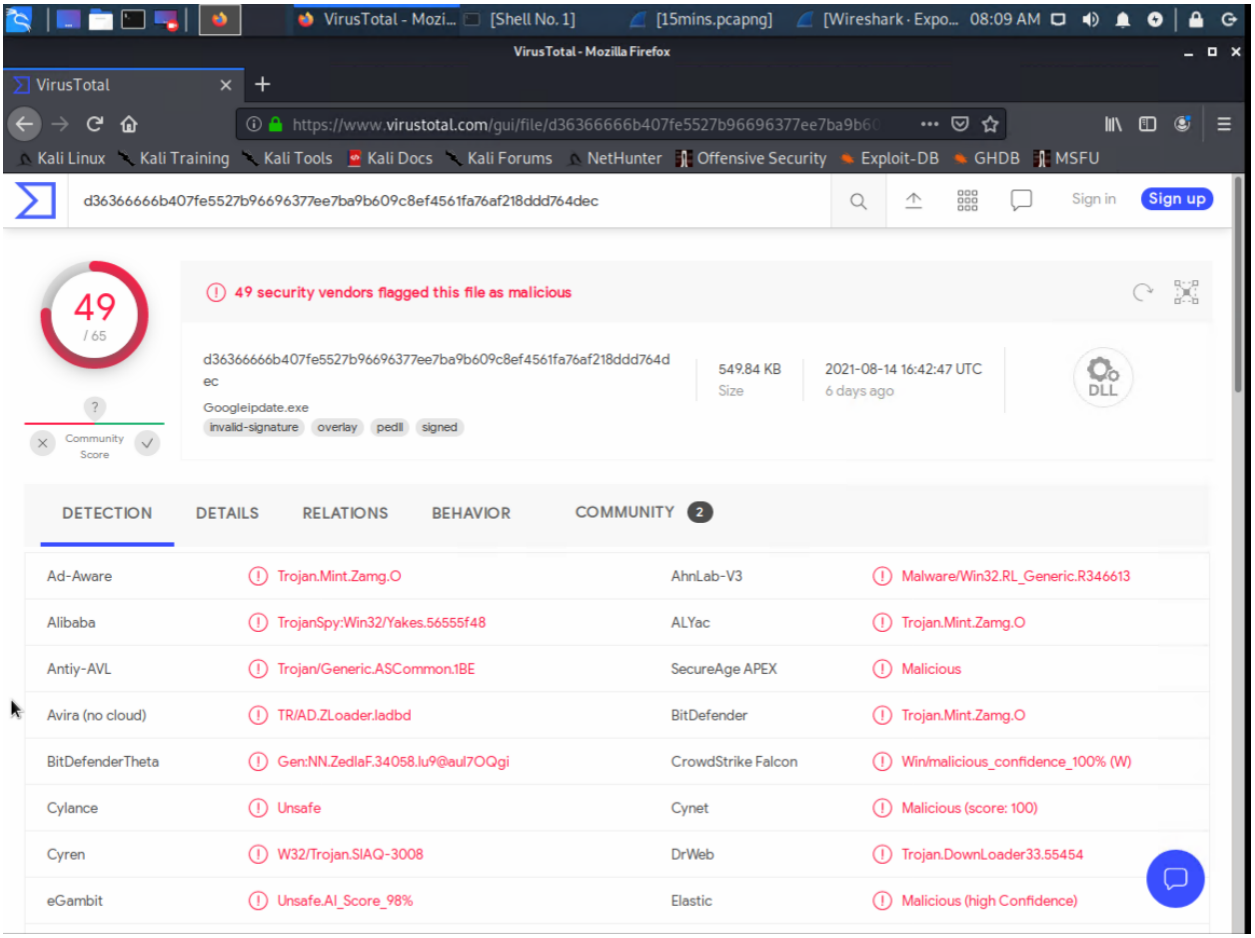
The malware file is june11.dll


Shell No. 1
15mins.pcapng
08:04 AM
15mins.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.6.12.203 and http.request.method==GET
No. Time Source Destination Protocol Length Info
35394 294.886263600 10.6.12.203 205.185.125.104 HTTP 275 GET /pQBtWj HTTP/1.1
35398 294.896835800 10.6.12.203 205.185.125.104 HTTP 312 GET /files/june11.dll HTTP/1.1
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 298
Identification: 0xadfc (44540)
Flags: 0x4000, Don't fragment
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0xe9de [validation disabled]
[Header checksum status: Unverified]
Source: 10.6.12.203
Destination: 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\n
Accept: */*\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)\r\n
Host: 205.185.125.104\r\n
Connection: Keep-Alive\r\n
Cookie: _subid=3mmhfnd8jp\r\n
\r\n
[Full request URI: http://205.185.125.104/files/june11.dll]
[HTTP request 2/2]
[Prev request in frame: 35394]
[Response in frame: 36136]
0000 ec c8 82 29 41 7d 84 3a 4b 6d fc e2 08 00 45 00
0010 01 2a ad fc 40 00 80 06 e9 de 0a 06 0c cb cd b9
0020 7d 68 c2 4b 00 50 04 1f 3f 3d 78 a3 51 8c 50 18
0030 ff ff 34 1f 00 00 47 45 54 20 2f 66 69 6c 65 73
0040 2f 6a 75 6e 65 31 31 2e 64 6c 6c 20 48 54 54 50
0050 2f 31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 2a 2f
0060 2a 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69
Internet Protocol Version 4 (ip), 20 bytes
Packets: 99008 · Displayed: 2 (0.0%) · Marked: 1 (0.0%) · Dropped: 0 (0.0%)
Profile: Default



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

This virus is classified as a trojan



Vulnerable Windows Machines

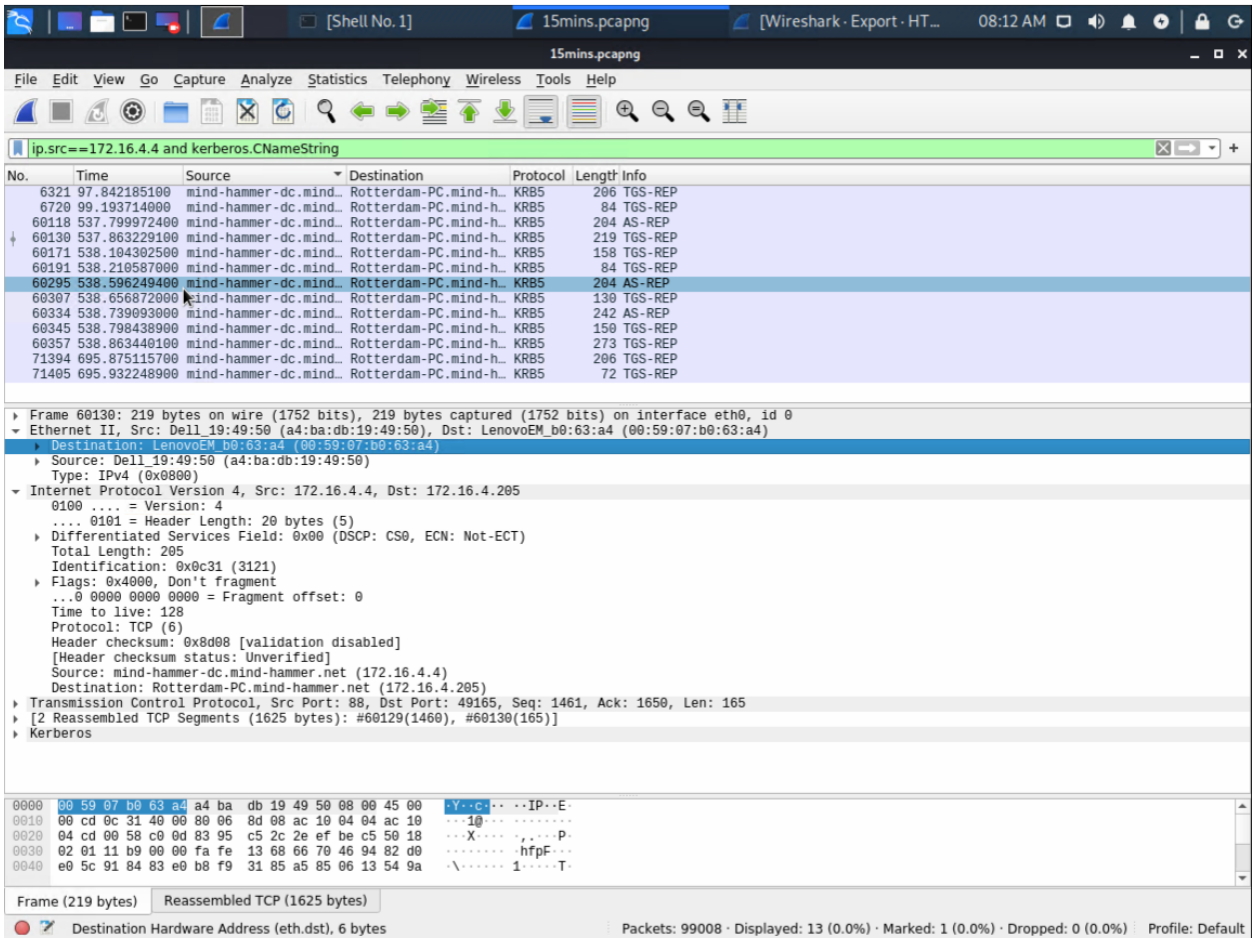
The Security team received reports of an infected Windows host on the network. They know the following:

- 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:

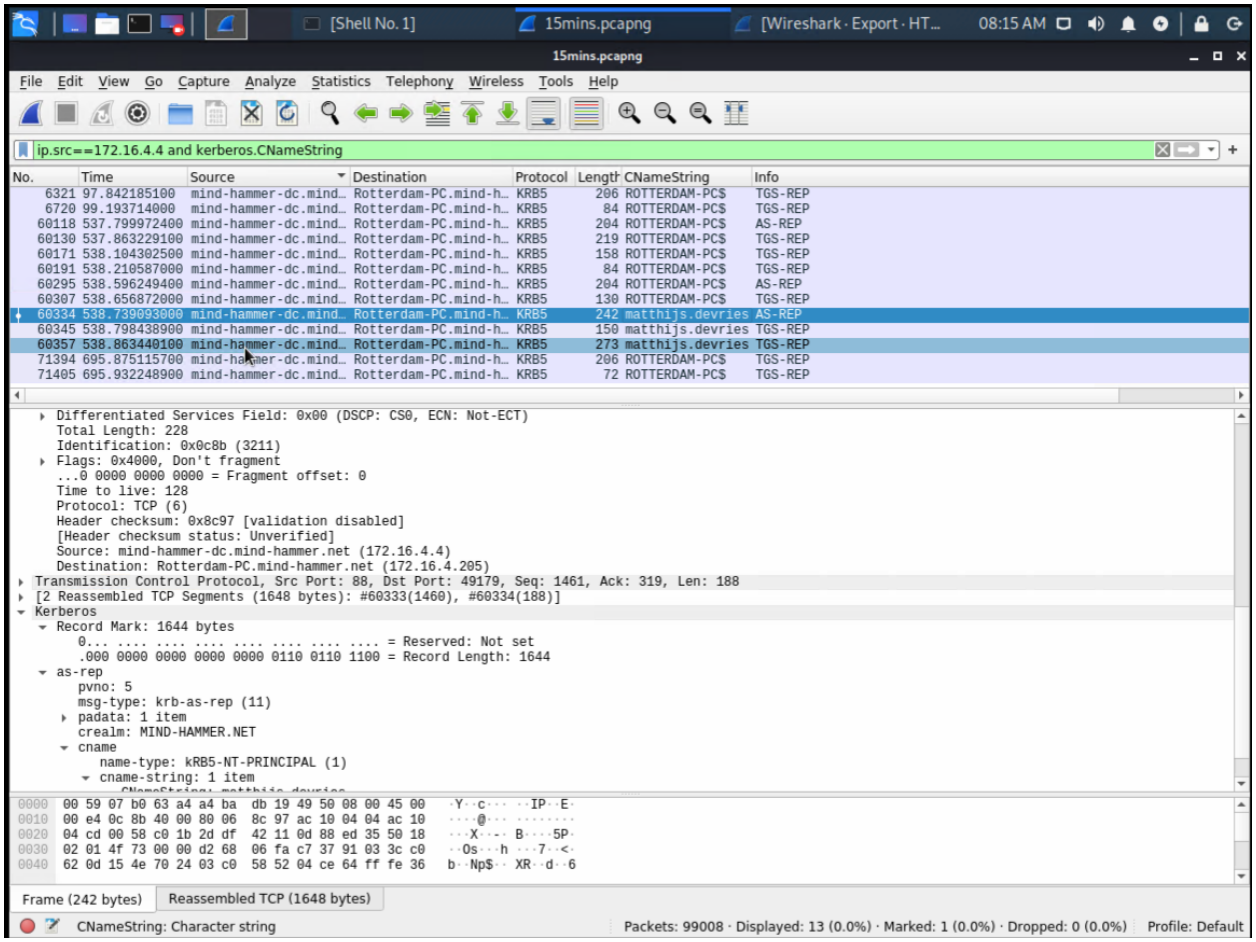
1. Find the following information about the infected Windows machine:
    - Host name: ROTTERDAM-PC

- IP address: 172.16.4.205
- MAC address: 00:59:07:b0:63:a4



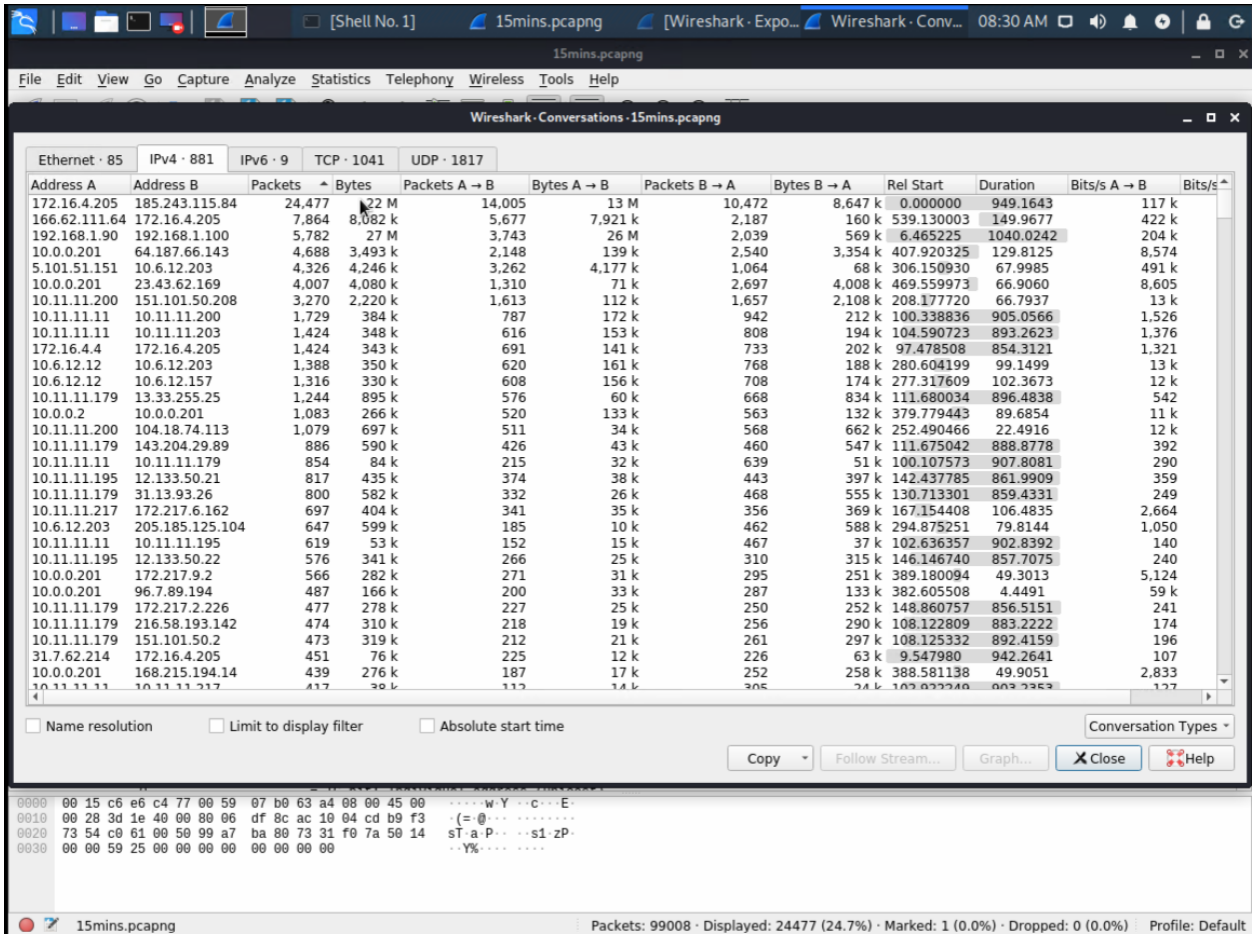
2. What is the username of the Windows user whose computer is infected?

Username is matthijs.devries.

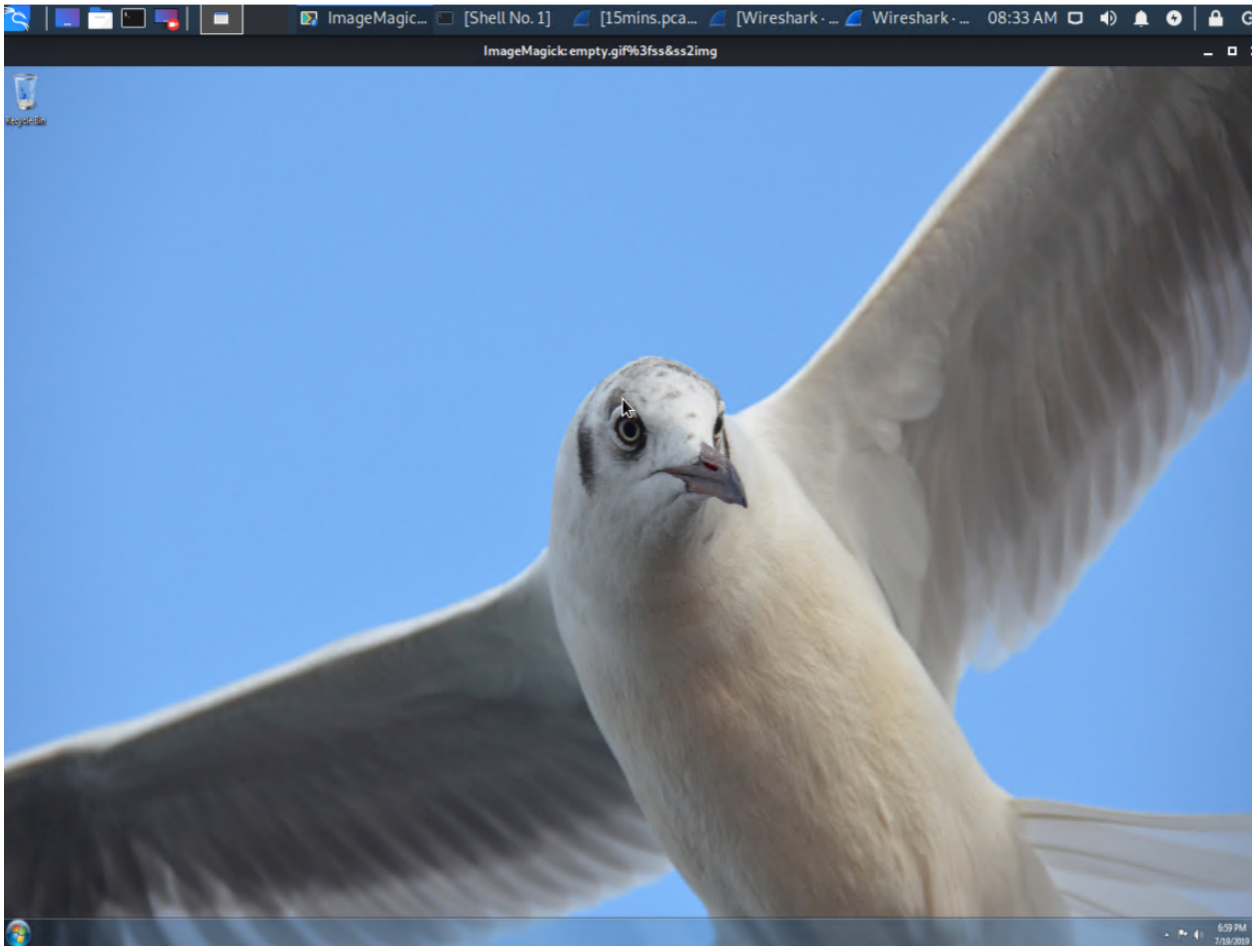


3. What are the IP addresses used in the actual infection traffic?

IPS 172.16.4.205, 185.243.115.84, and 166.62.11.64 are the infected traffic.



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



Illegal Downloads

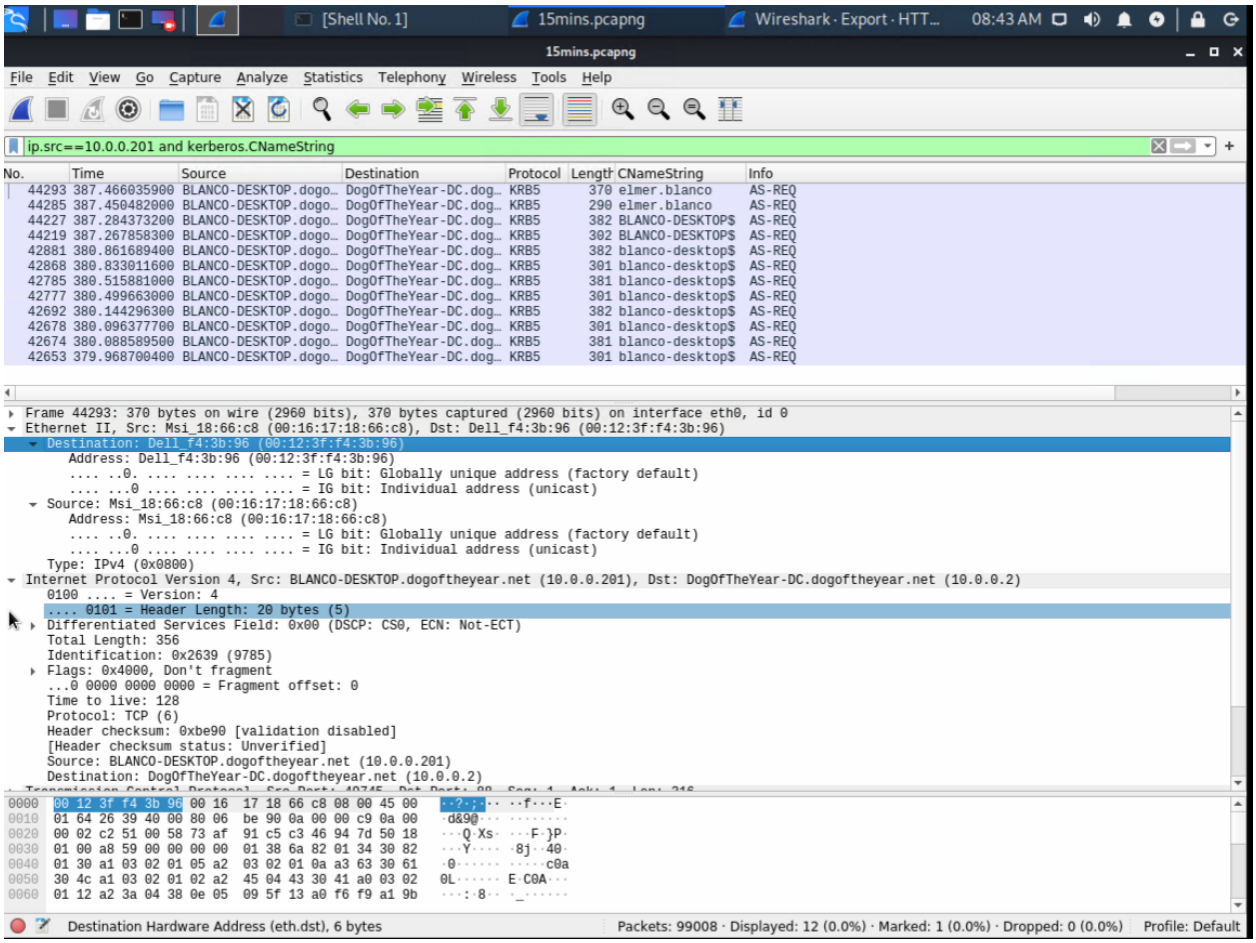
IT was informed that some users are torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringement.

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.

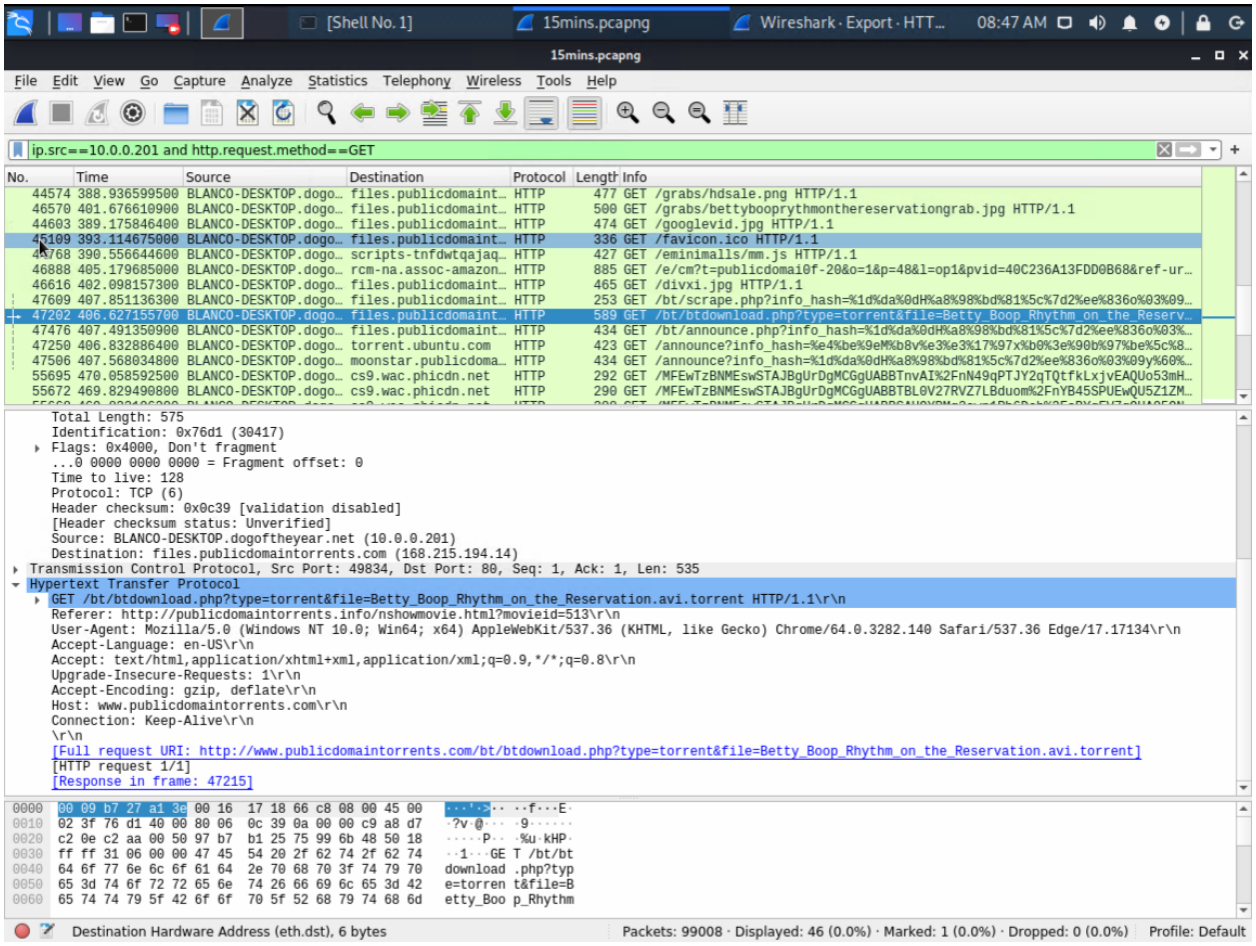
Your task is to isolate torrent traffic and answer the following questions:

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: BLANCO-DESKTOP



2. Which torrent file did the user download?

The torrent file is BEtty_Boop_Rythm_on_the_Reservation.avi.torrent


[Shell No. 1]
15mins.pcapng
Wireshark · Export · HTT...
08:47 AM
15mins.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.src==10.0.0.201 and http.request.method==GET
No. Time Source Destination Protocol Length Info
44574 388.936599500 BLANCO-DESKTOP.dogo… files.publicdomaint… HTTP 477 GET /grabs/hdsale.png HTTP/1.1
46570 401.676610900 BLANCO-DESKTOP.dogo… files.publicdomaint… HTTP 500 GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1
44603 389.175846400 BLANCO-DESKTOP.dogo… files.publicdomaint… HTTP 474 GET /googlevid.jpg HTTP/1.1
45109 393.114675000 BLANCO-DESKTOP.dogo… files.publicdomaint… HTTP 336 GET /favicon.ico HTTP/1.1
46768 390.556644600 BLANCO-DESKTOP.dogo… scripts-tnfdwtqajaq… HTTP 427 GET /eminimalls/mm.js HTTP/1.1
46888 405.179685000 BLANCO-DESKTOP.dogo… rcm-na.assoc-amazon… HTTP 885 GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=op1&pvid=40C236A13FDD0B68&ref-ur…
46616 402.098157300 BLANCO-DESKTOP.dogo… files.publicdomaint… HTTP 465 GET /divxi.jpg HTTP/1.1
47609 407.851136300 BLANCO-DESKTOP.dogo… files.publicdomaint… HTTP 253 GET /bt/scrape.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%09…
47202 406.627155700 BLANCO-DESKTOP.dogo… files.publicdomaint… HTTP 589 GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reserv…
47476 407.491350900 BLANCO-DESKTOP.dogo… files.publicdomaint… HTTP 434 GET /bt/announce.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%…
47250 406.832886400 BLANCO-DESKTOP.dogo… torrent.ubuntu.com HTTP 423 GET /announce?info_hash=%e4%be%9eM%b8v%e3%e3%17%97x%b0%3e%90b%97%be%5c%8…
47506 407.568034800 BLANCO-DESKTOP.dogo… moonstar.publicdoma… HTTP 434 GET /announce?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%09y%60%…
55695 470.058592500 BLANCO-DESKTOP.dogo… cs9.wac.phicdn.net HTTP 292 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTnvAI%2FnN49qPTJY2qTQtfkLxjvEAQUo53mH…
55672 469.829490800 BLANCO-DESKTOP.dogo… cs9.wac.phicdn.net HTTP 290 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZM…
Total Length: 575
Identification: 0x76d1 (30417)
Flags: 0x4000, Don't fragment
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x0c39 [validation disabled]
[Header checksum status: Unverified]
Source: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201)
Destination: 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
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]
[Response in frame: 47215]
0000 00 09 b7 27 a1 3e 00 16 17 18 66 c8 08 00 45 00
0010 02 3f 76 d1 40 00 80 06 0c 39 0a 00 00 c9 a8 d7
0020 c2 0e c2 aa 00 50 97 b7 b1 25 75 99 6b 48 50 18
0030 ff ff 31 06 00 00 47 45 54 20 2f 62 74 2f 62 74
0040 64 6f 77 6e 6c 6f 61 64 2e 70 68 70 3f 74 79 70
0050 65 3d 74 6f 72 72 65 6e 74 26 66 69 6c 65 3d 42
0060 65 74 74 79 5f 42 6f 6f 70 5f 52 68 79 74 68 6d
Destination Hardware Address (eth.dst), 6 bytes
Packets: 99008 · Displayed: 46 (0.0%) · Marked: 1 (0.0%) · Dropped: 0 (0.0%)
Profile: Default