Network Analysis

Time Thieves

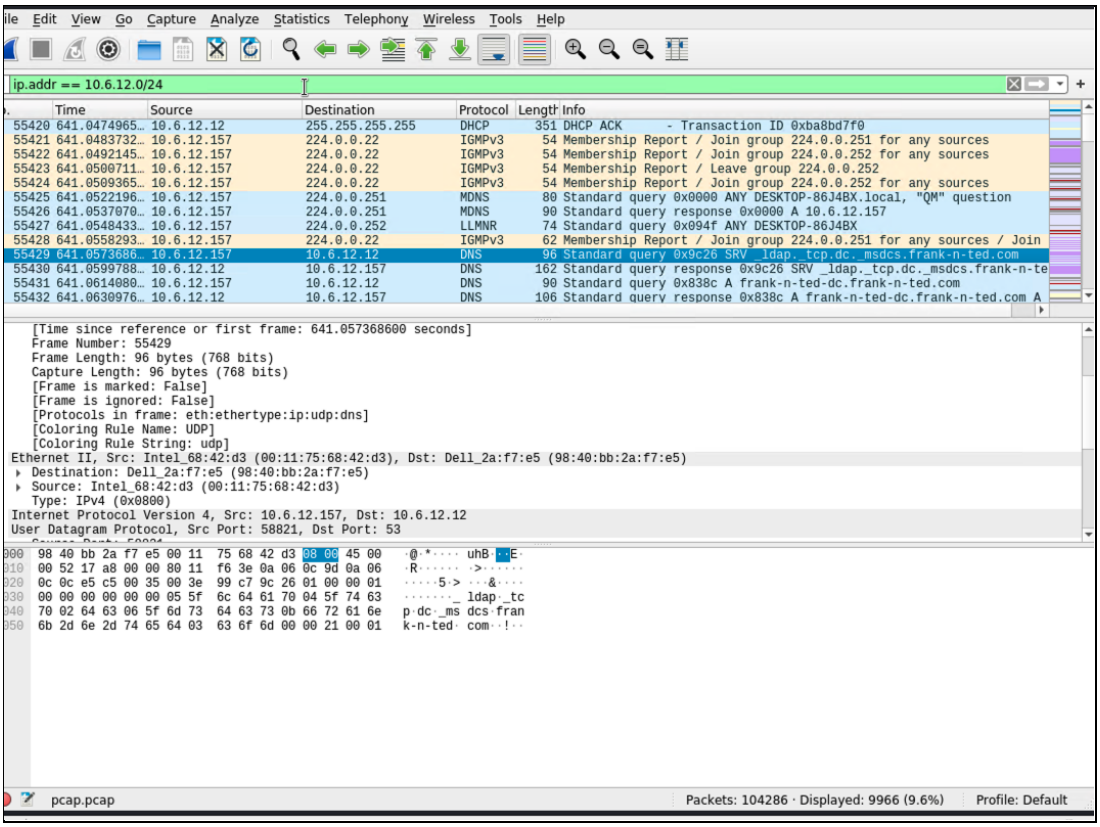
At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- 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:

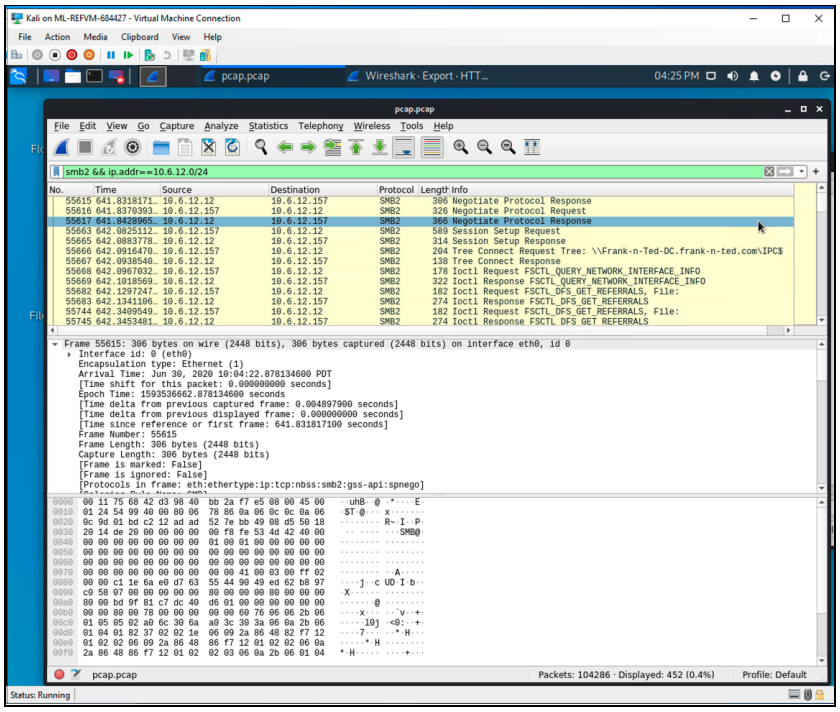
1. What is the domain name of the users' custom site?

   The domain name of the users' custom site is frank-n-ted.com



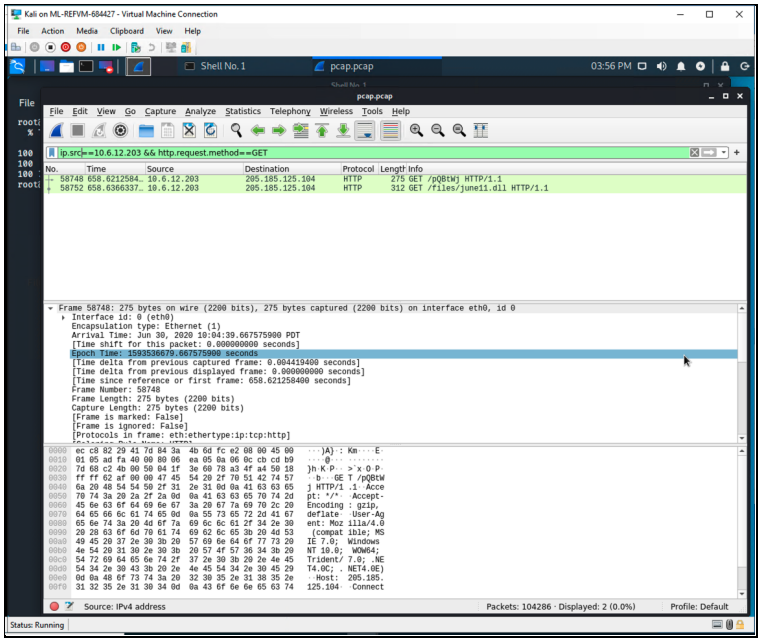
2. What is the IP address of the Domain Controller (DC) of the AD network?

   The IP Address of the DC of the Active Directory Network is 10.6.12.12, which we know because all of the SYN/ACK Responses come from that IP.



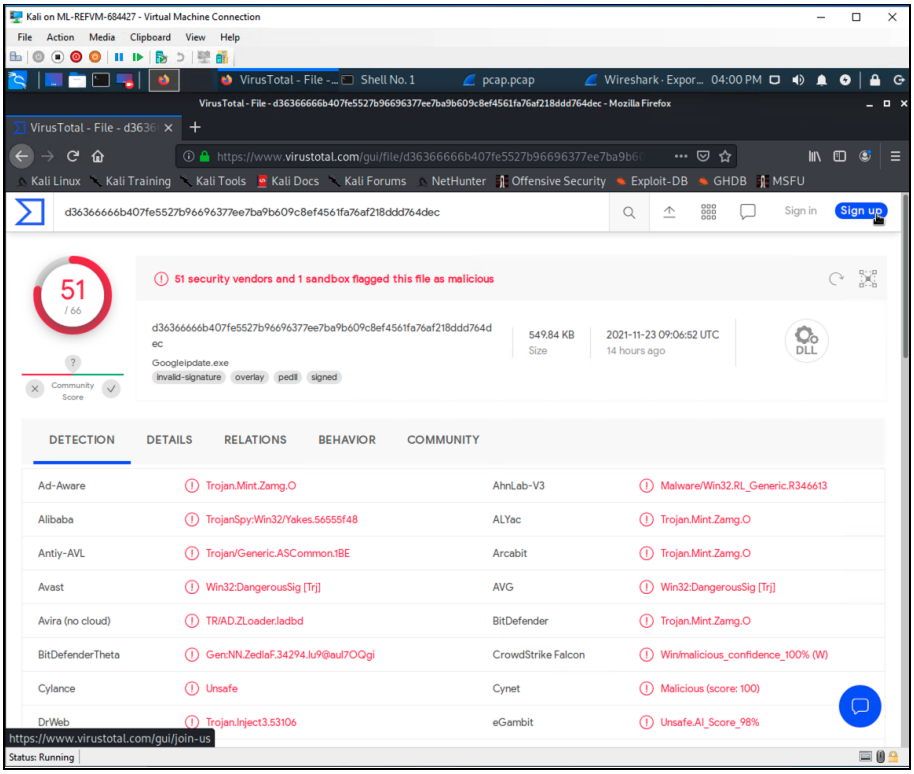
3. What is the name of the malware downloaded to the `10.6.12.203` machine? Once you have found the file, export it to your Kali machine's desktop.

   The name of the malware file is june11.dll.



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

   It is classified as a trojan virus.



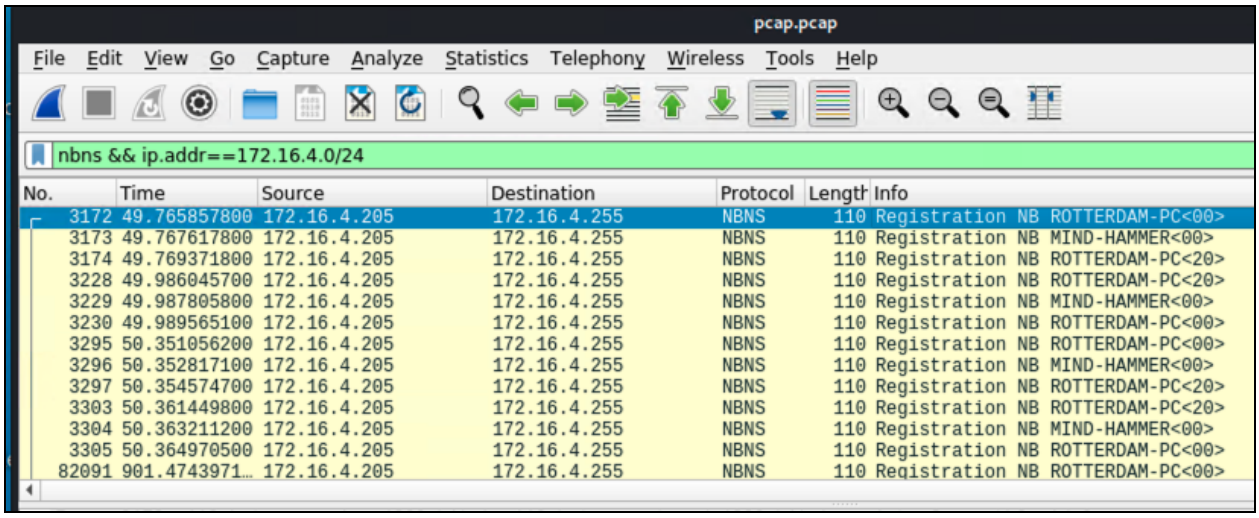
Vulnerable Windows Machines

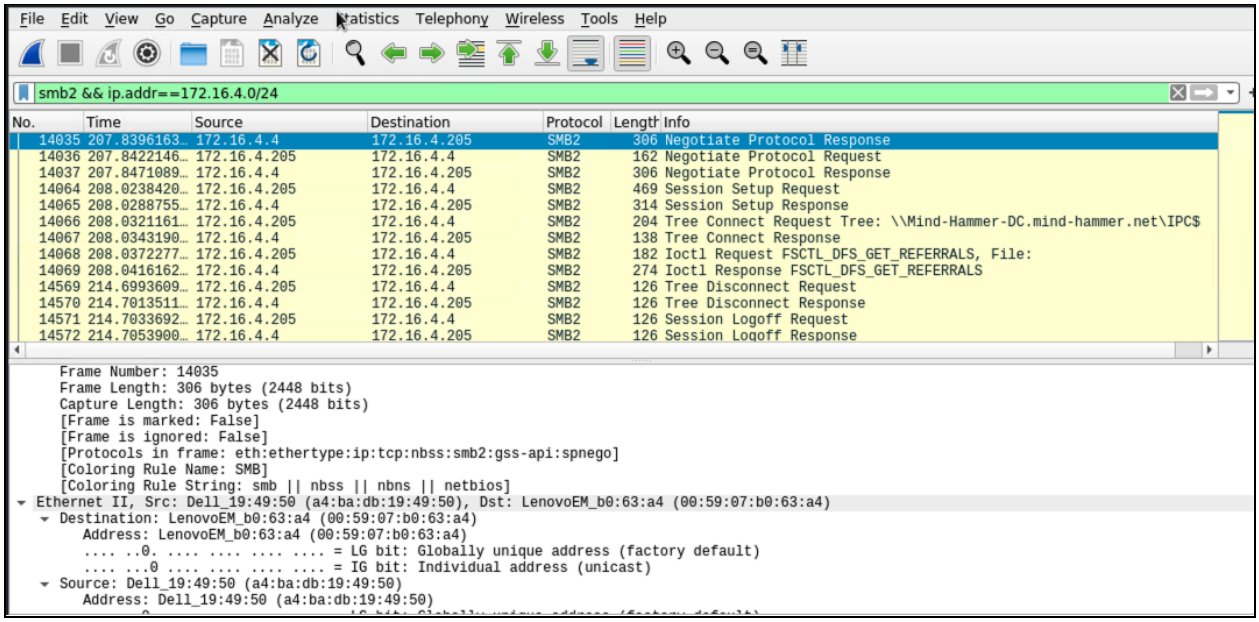
The Security team received reports of an infected Windows host on the network. They know the following:

- 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:

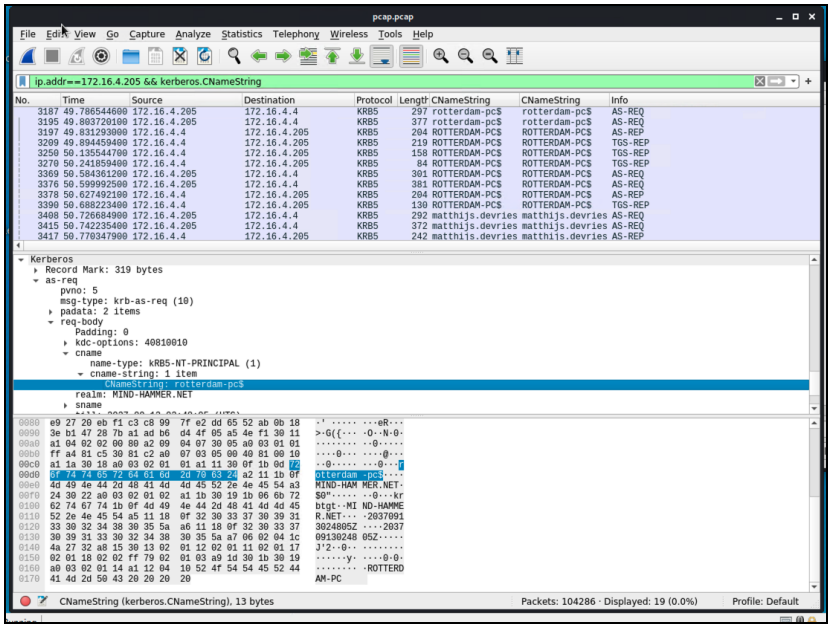
1. Find the following information about the infected Windows machine:
    - Host name: **ROTTERDAM-PC**
    - IP address: **172.16.4.205**
    - MAC address: **00:59:07:b0:63:a4**





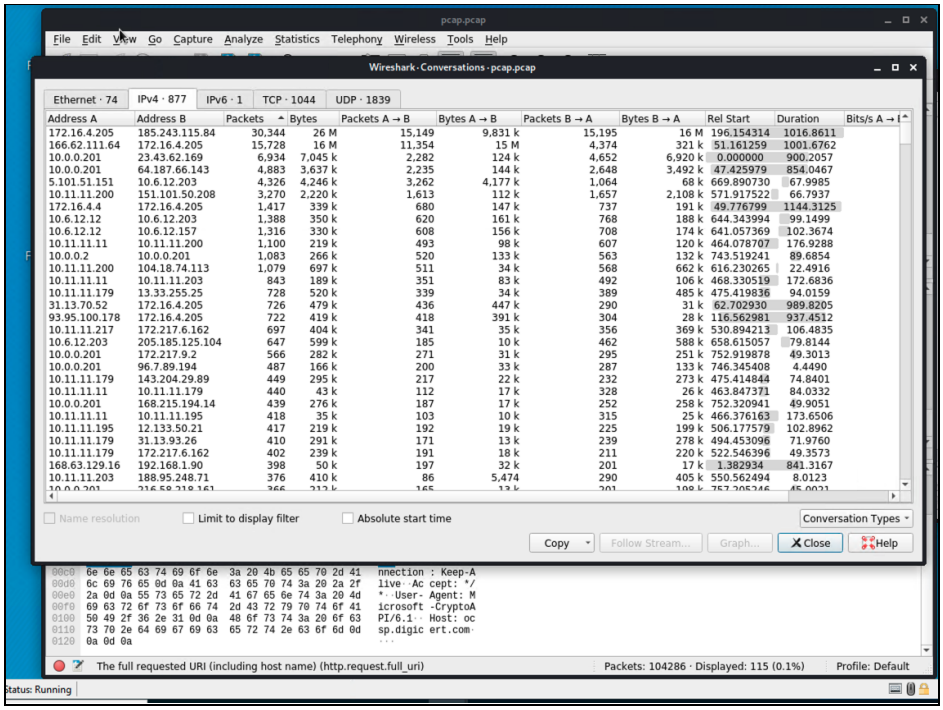
2. What is the username of the Windows user whose computer is infected?

    The username of the infected windows machine is matthijs.devries



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

   The two main IP addresses used in the actual infection traffic are 185.243.115.84 and 166.62.111.64, which were found in the conversations tab in Wireshark.



Illegal Downloads

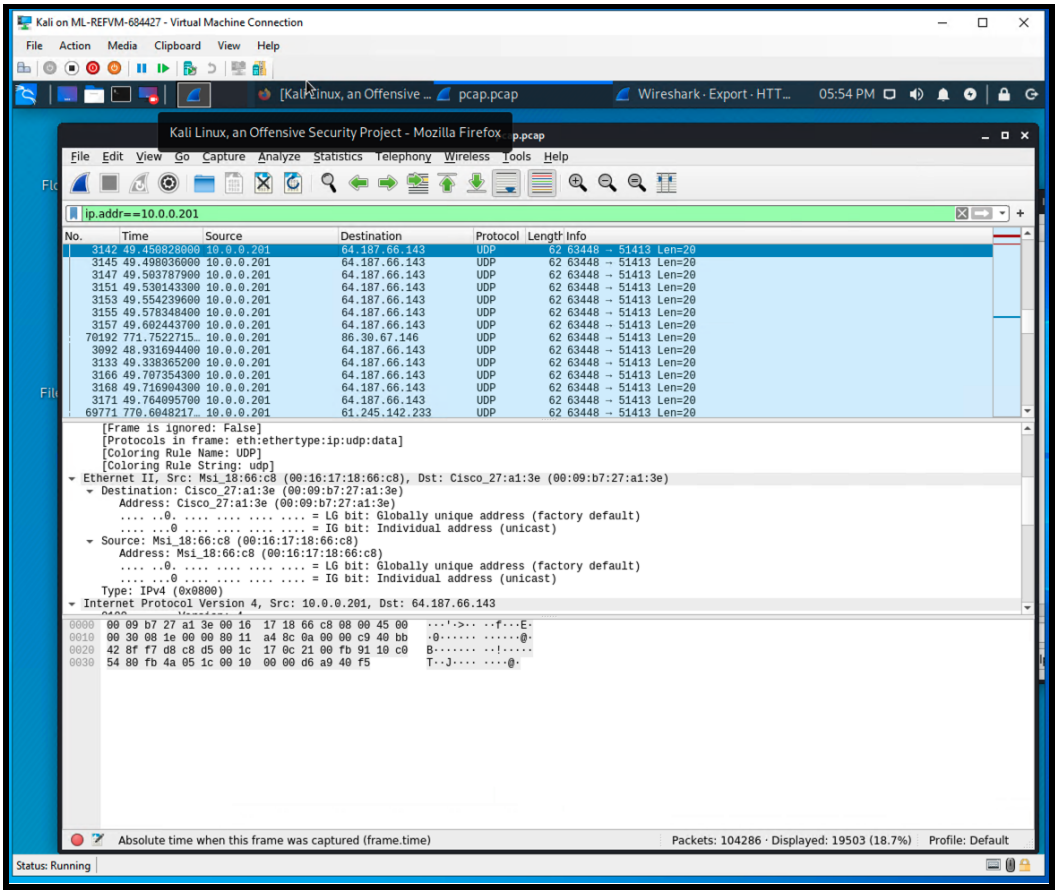
IT was informed that some users are torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringement.

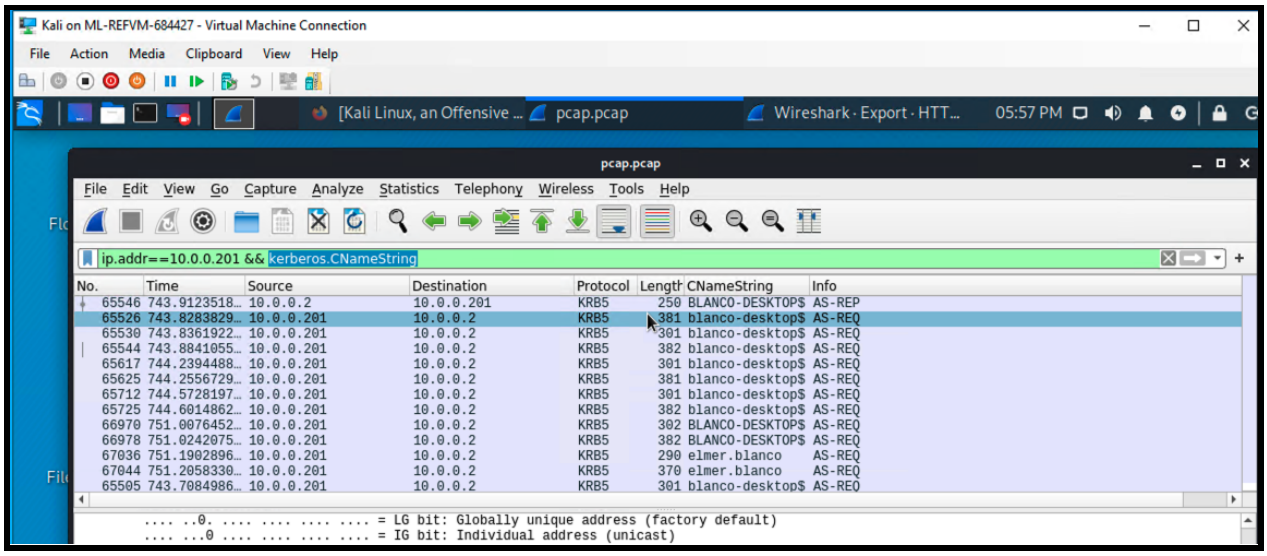
IT shared the following about the torrent activity:

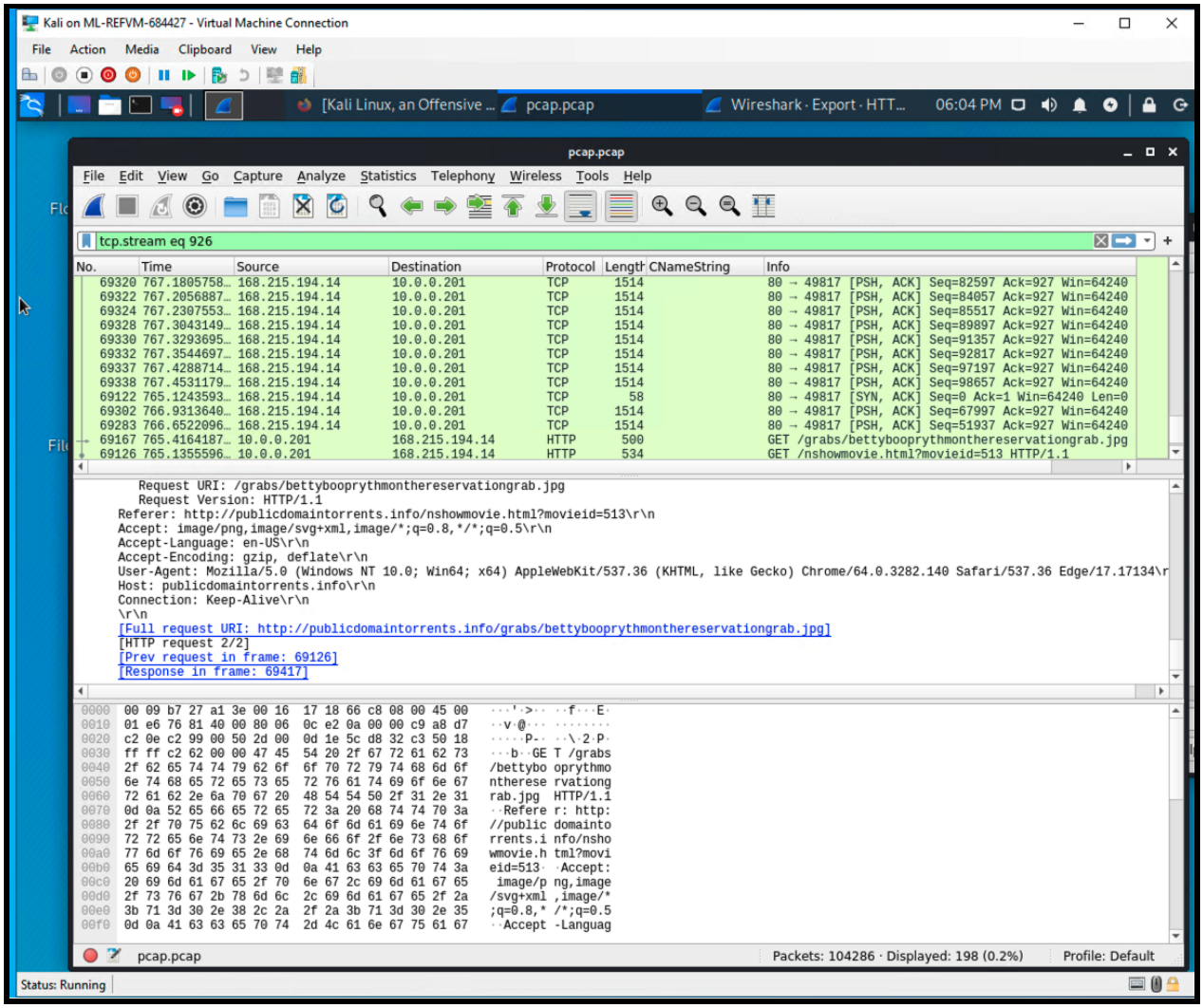
- The machines using torrents live in the range `10.0.0.0/24` and are clients of an AD domain.
- The DC of this domain lives at `10.0.0.2` and is named DogOfTheYear-DC.
- The DC is associated with the domain dogoftheyear.net.

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: **00:09:b7:27:a1:3e**
    - Windows username: **elmer.blanco**
    - OS version: **Windows 10 (Windows NT 10.0)**




Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
[Kali Linux, an Offensive ... pcap.pcap Wireshark · Export · HTT... 05:57 PM
pcap.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==10.0.0.201 && kerberos.CNameString
No. Time Source Destination Protocol Length CNameString Info
65546 743.9123518… 10.0.0.2 10.0.0.201 KRB5 250 BLANCO-DESKTOP$ AS-REP
65526 743.8283829… 10.0.0.201 10.0.0.2 KRB5 381 blanco-desktop$ AS-REQ
65530 743.8361922… 10.0.0.201 10.0.0.2 KRB5 301 blanco-desktop$ AS-REQ
65544 743.8841055… 10.0.0.201 10.0.0.2 KRB5 382 blanco-desktop$ AS-REQ
65617 744.2394488… 10.0.0.201 10.0.0.2 KRB5 301 blanco-desktop$ AS-REQ
65625 744.2556729… 10.0.0.201 10.0.0.2 KRB5 381 blanco-desktop$ AS-REQ
65712 744.5728197… 10.0.0.201 10.0.0.2 KRB5 301 blanco-desktop$ AS-REQ
65725 744.6014862… 10.0.0.201 10.0.0.2 KRB5 382 blanco-desktop$ AS-REQ
66970 751.0076452… 10.0.0.201 10.0.0.2 KRB5 302 BLANCO-DESKTOP$ AS-REQ
66978 751.0242075… 10.0.0.201 10.0.0.2 KRB5 382 BLANCO-DESKTOP$ AS-REQ
67036 751.1902896… 10.0.0.201 10.0.0.2 KRB5 290 elmer.blanco AS-REQ
67044 751.2058330… 10.0.0.201 10.0.0.2 KRB5 370 elmer.blanco AS-REQ
65505 743.7084986… 10.0.0.201 10.0.0.2 KRB5 301 blanco-desktop$ AS-REQ
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)


Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
[Kali Linux, an Offensive ... pcap.pcap Wireshark · Export · HTT... 06:04 PM
pcap.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 926
No. Time Source Destination Protocol Length CNameString Info
69320 767.1805758… 168.215.194.14 10.0.0.201 TCP 1514 80 → 49817 [PSH, ACK] Seq=82597 Ack=927 Win=64240
69322 767.2056887… 168.215.194.14 10.0.0.201 TCP 1514 80 → 49817 [PSH, ACK] Seq=84057 Ack=927 Win=64240
69324 767.2307553… 168.215.194.14 10.0.0.201 TCP 1514 80 → 49817 [PSH, ACK] Seq=85517 Ack=927 Win=64240
69328 767.3043149… 168.215.194.14 10.0.0.201 TCP 1514 80 → 49817 [PSH, ACK] Seq=89897 Ack=927 Win=64240
69330 767.3293695… 168.215.194.14 10.0.0.201 TCP 1514 80 → 49817 [PSH, ACK] Seq=91357 Ack=927 Win=64240
69332 767.3544697… 168.215.194.14 10.0.0.201 TCP 1514 80 → 49817 [PSH, ACK] Seq=92817 Ack=927 Win=64240
69337 767.4288714… 168.215.194.14 10.0.0.201 TCP 1514 80 → 49817 [PSH, ACK] Seq=97197 Ack=927 Win=64240
69338 767.4531179… 168.215.194.14 10.0.0.201 TCP 1514 80 → 49817 [PSH, ACK] Seq=98657 Ack=927 Win=64240
69122 765.1243593… 168.215.194.14 10.0.0.201 TCP 58 80 → 49817 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
69302 766.9313640… 168.215.194.14 10.0.0.201 TCP 1514 80 → 49817 [PSH, ACK] Seq=67997 Ack=927 Win=64240
69283 766.6522096… 168.215.194.14 10.0.0.201 TCP 1514 80 → 49817 [PSH, ACK] Seq=51937 Ack=927 Win=64240
69167 765.4164187… 10.0.0.201 168.215.194.14 HTTP 500 GET /grabs/bettybooprythmonthereservationgrab.jpg
69126 765.1355596… 10.0.0.201 168.215.194.14 HTTP 534 GET /nshowmovie.html?movieid=513 HTTP/1.1
Request URI: /grabs/bettybooprythmonthereservationgrab.jpg
Request Version: HTTP/1.1
Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\r\n
Accept: image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5\r\n
Accept-Language: en-US\r\n
Accept-Encoding: gzip, deflate\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
Host: publicdomaintorrents.info\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://publicdomaintorrents.info/grabs/bettybooprythmonthereservationgrab.jpg]
[HTTP request 2/2]
[Prev request in frame: 69126]
[Response in frame: 69417]
0000 00 09 b7 27 a1 3e 00 16 17 18 66 c8 08 00 45 00 ···'·>·· ··f···E·
0010 01 e6 76 81 40 00 80 06 0c e2 0a 00 00 c9 a8 d7 ··v·@··· ········
0020 c2 0e c2 99 00 50 2d 00 0d 1e 5c d8 32 c3 50 18 ·····P-· ··\·2·P·
0030 ff ff c2 62 00 00 47 45 54 20 2f 67 72 61 62 73 ···b··GE T /grabs
0040 2f 62 65 74 74 79 62 6f 6f 70 72 79 74 68 6d 6f /bettybo oprythmo
0050 6e 74 68 65 72 65 73 65 72 76 61 74 69 6f 6e 67 ntherese rvationg
0060 72 61 62 2e 6a 70 67 20 48 54 54 50 2f 31 2e 31 rab.jpg HTTP/1.1
0070 0d 0a 52 65 66 65 72 65 72 3a 20 68 74 74 70 3a ··Refere r: http:
0080 2f 2f 70 75 62 6c 69 63 64 6f 6d 61 69 6e 74 6f //public domainto
0090 72 72 65 6e 74 73 2e 69 6e 66 6f 2f 6e 73 68 6f rrents.i nfo/nsho
00a0 77 6d 6f 76 69 65 2e 68 74 6d 6c 3f 6d 6f 76 69 wmovie.h tml?movi
00b0 65 69 64 3d 35 31 33 0d 0a 41 63 63 65 70 74 3a eid=513· ·Accept:
00c0 20 69 6d 61 67 65 2f 70 6e 67 2c 69 6d 61 67 65 image/p ng,image
00d0 2f 73 76 67 2b 78 6d 6c 2c 69 6d 61 67 65 2f 2a /svg+xml ,image/*
00e0 3b 71 3d 30 2e 38 2c 2a 2f 2a 3b 71 3d 30 2e 35 ;q=0.8,* /*;q=0.5
00f0 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 ··Accept -Languag
pcap.pcap
Packets: 104286 · Displayed: 198 (0.2%)
Profile: Default
Status: Running

2. Which torrent file did the user download?

The user torrented a file called Betty_Boop_Rythm.