

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:

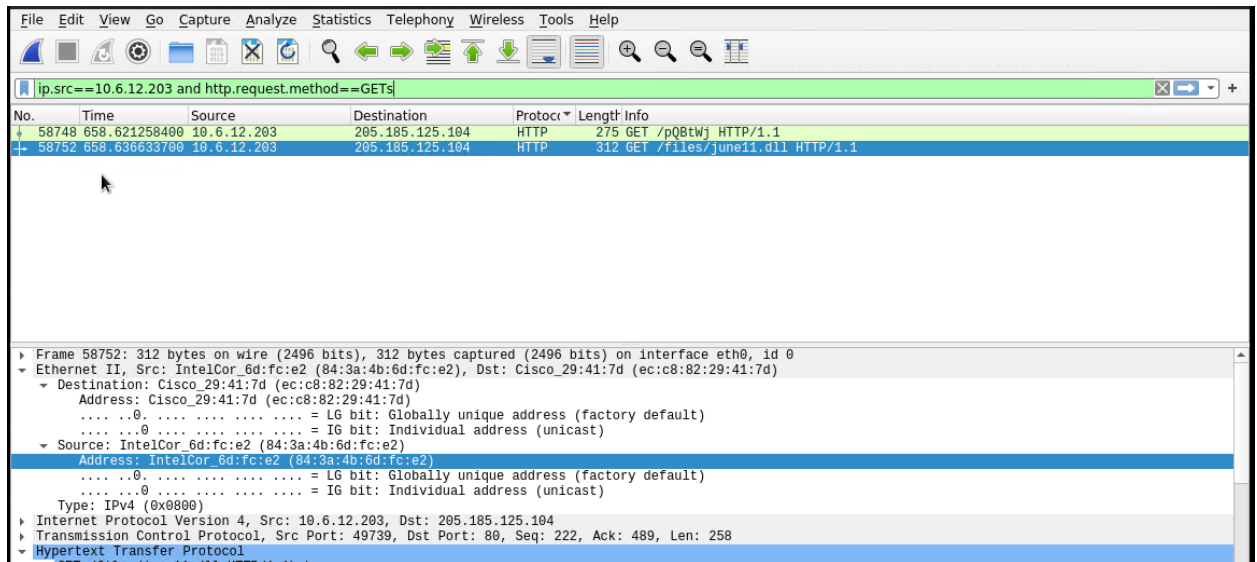
- What is the domain name of the users' custom site?
 - frank-n-ted-dc.frank-n-ted.com

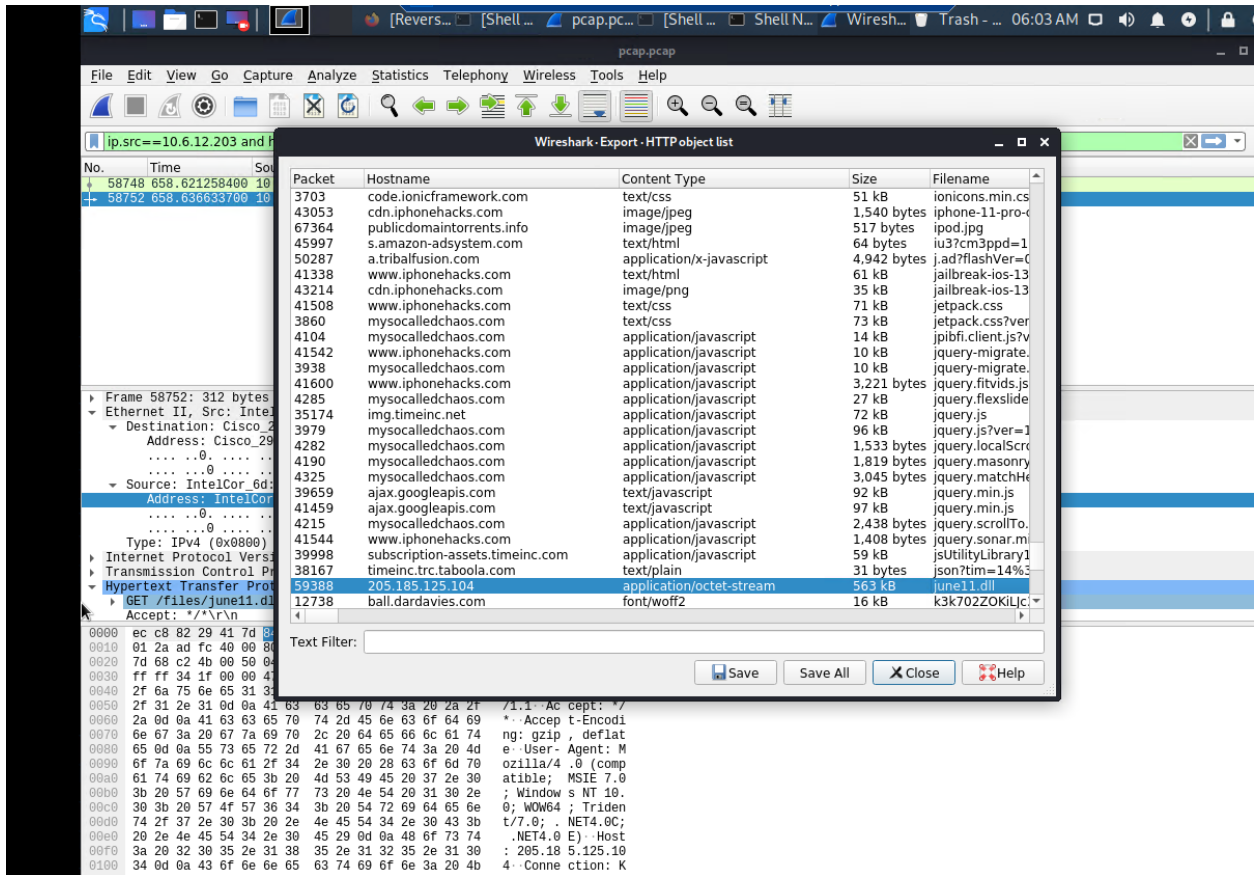
The image shows a Wireshark network traffic capture. The top toolbar includes menus like File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the toolbar is a filter bar with the expression `ip.src==10.6.12.157555`. The main packet list displays several packets, with packet 55431 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Internet Protocol Version 4.

No.	Time	Source	Destination	Protocol	Length	Info
55421	641.048373200	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any sources
55422	641.049214500	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
55423	641.050071100	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
55424	641.050936500	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
55425	641.052219600	10.6.12.157	224.0.0.251	MDNS	80	Standard query 0x0000 ANY DESKTOP-86J4BX.local, "QM" question
55426	641.053707000	10.6.12.157	224.0.0.251	MDNS	90	Standard query response 0x0000 A 10.6.12.157
55427	641.054843300	10.6.12.157	224.0.0.252	LLMNR	74	Standard query 0x094f ANY DESKTOP-86J4BX
55428	641.055829300	10.6.12.157	224.0.0.22	IGMPv3	62	Membership Report / Join group 224.0.0.251 for any sources / Join group ...
55429	641.057368600	10.6.12.157	10.6.12.12	DNS	96	Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
55431	641.061408000	10.6.12.157	10.6.12.12	DNS	90	Standard query 0x838c A frank-n-ted-dc.frank-n-ted.com
55433	641.067325100	10.6.12.157	10.6.12.12	LDAP	264	searchRequest(1) "<ROOT>" baseObject
55435	641.072155000	10.6.12.157	10.6.12.12	TCP	66	49668 → 389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
55437	641.074069000	10.6.12.157	10.6.12.12	TCP	54	49668 → 389 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
55438	641.080536000	10.6.12.157	10.6.12.12	LDAP	404	searchRequest(2) "<ROOT>" baseObject

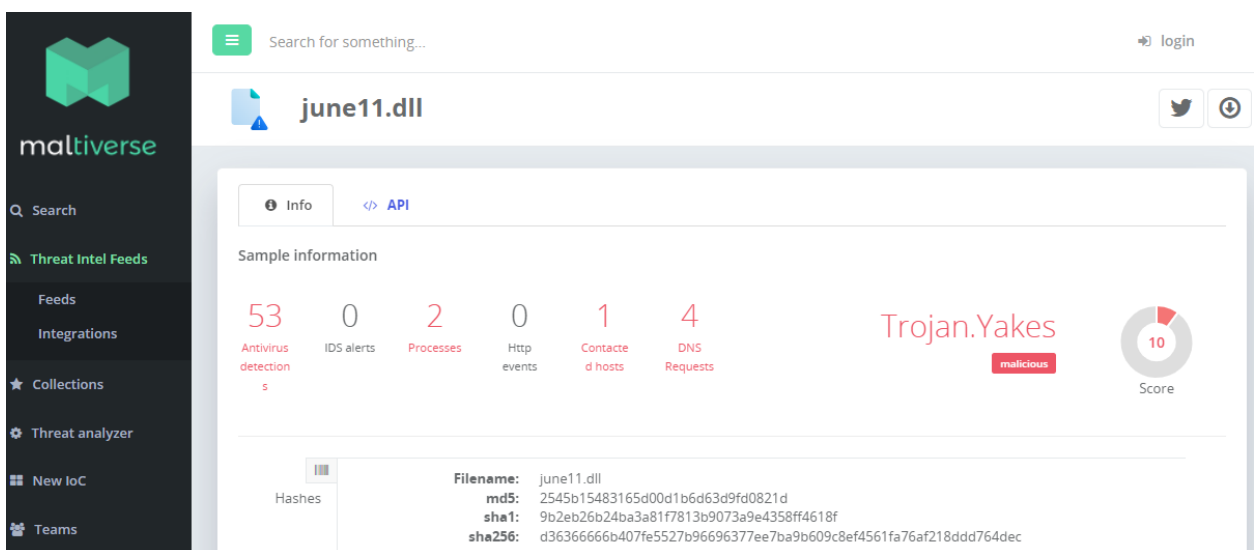
Frame 55431: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface eth0, id 0
Ethernet II, Src: Intel_68:42:d3 (00:11:75:68:42:d3), Dst: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5)
Destination: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5)
Address: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5)
...0... = LG bit: Globally unique address (factory default)
...0... = IG bit: Individual address (unicast)
Source: Intel_68:42:d3 (00:11:75:68:42:d3)
Address: Intel_68:42:d3 (00:11:75:68:42:d3)
...0... = LG bit: Globally unique address (factory default)
...0... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.6.12.157, Dst: 10.6.12.12
0100 ... = Version: 4
0101 ... = Header Length: 20 bytes (5)

- 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](https://www.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

pcap.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==172.16.4.0/24 nbns

No.	Time	Source	Destination	Protocol	Length	Info
3172	49.765857800	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<00>
3173	49.767617800	172.16.4.205	172.16.4.255	NBNS	110	Registration NB MIND-HAMMER<00>
3174	49.769371800	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<20>
3228	49.986045700	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<20>
3229	49.987058000	172.16.4.205	172.16.4.255	NBNS	110	Registration NB MIND-HAMMER<00>
3230	49.989565100	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<00>
3295	50.351056200	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<00>
3296	50.352817100	172.16.4.205	172.16.4.255	NBNS	110	Registration NB MIND-HAMMER<00>
3297	50.354574700	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<20>
3303	50.361449800	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<20>
3304	50.363211200	172.16.4.205	172.16.4.255	NBNS	110	Registration NB MIND-HAMMER<00>
3305	50.364970500	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<00>
32499	463.888982400	10.11.11.179	10.11.11.255	NBNS	110	Registration NB MACBOOKPRO-8843<00>
32518	463.947723700	10.11.11.179	10.11.11.255	NBNS	110	Registration NB MACBOOKPRO-8843<00>

Frame 3305: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface eth0, id 0

Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Address: Broadcast (ff:ff:ff:ff:ff:ff)

.....1..... = LG bit: Locally administered address (this is NOT the factory default)

.....1..... = IG bit: Group address (multicast/broadcast)

Source: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)

Address: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)

.....0..... = LG bit: Globally unique address (factory default)

.....0..... = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 172.16.4.205, Dst: 172.16.4.255

User Datagram Protocol, Src Port: 137, Dst Port: 137

Source Port: 137

Destination Port: 137

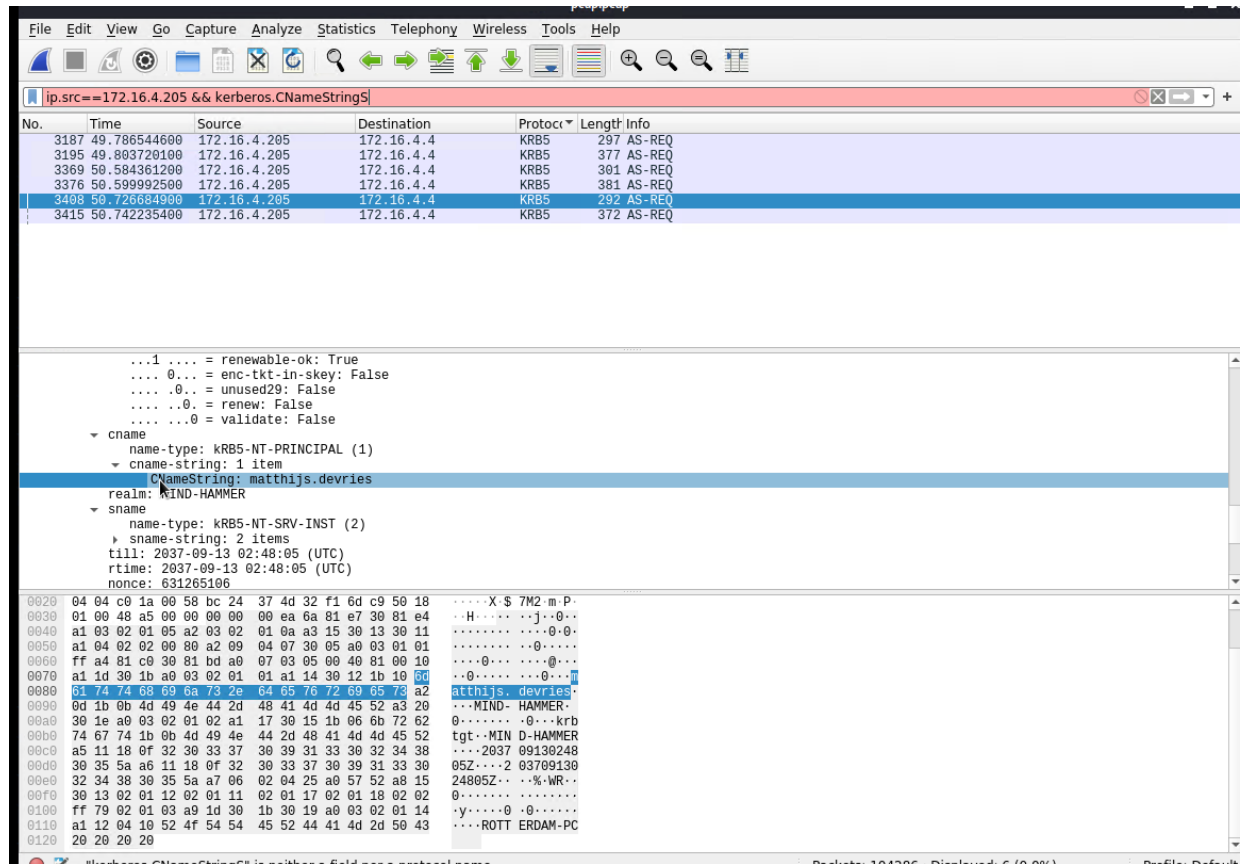
Length: 76

```

0000  ff ff ff ff ff ff 00 59 07 b0 63 a4 00 00 45 00  .....Y..C..E:
0010  00 00 00 7d 00 00 00 11 d9 23 ac 10 04 cd ac 10  ..}....#.....
0020  04 ff 00 00 00 89 00 4c 06 f8 89 e8 28 10 00 01  ....L n.....
0030  00 00 00 00 00 01 20 46 43 45 50 46 45 46 45 45  ....F CEPFEFEE
0040  46 46 43 45 45 45 42 45 46 43 4e 46 41 45 44 43  FFCEEEBE NCNFAEDC
0050  41 43 41 43 41 41 00 00 20 00 01 c0 0c 00 20  ACACAAA .....
0060  00 01 00 04 93 e0 00 06 00 00 ac 10 04 cd  ....

```

- 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

Ethernet · 74		IPv4 · 877		TCP · 1044									
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration		
172.16.4.205	49249	185.243.115.84	80	30,344	26 M	15,149	9,831 k	15,195	16 M	196.154314	1016.8611		
10.0.0.201	49949	23.43.62.169	443	5,623	6,972 k	972	52 k	4,651	6,920 k	0.000000	899.1115		
172.16.4.205	49201	166.62.111.64	80	4,152	4,342 k	1,108	77 k	3,044	4,265 k	51.760025	1001.0756		
172.16.4.205	49200	166.62.111.64	80	2,898	2,998 k	796	56 k	2,102	2,941 k	51.758985	1001.0007		
172.16.4.205	49198	166.62.111.64	80	2,614	2,674 k	734	58 k	1,880	2,615 k	51.756883	1001.0345		

Illegal Downloads

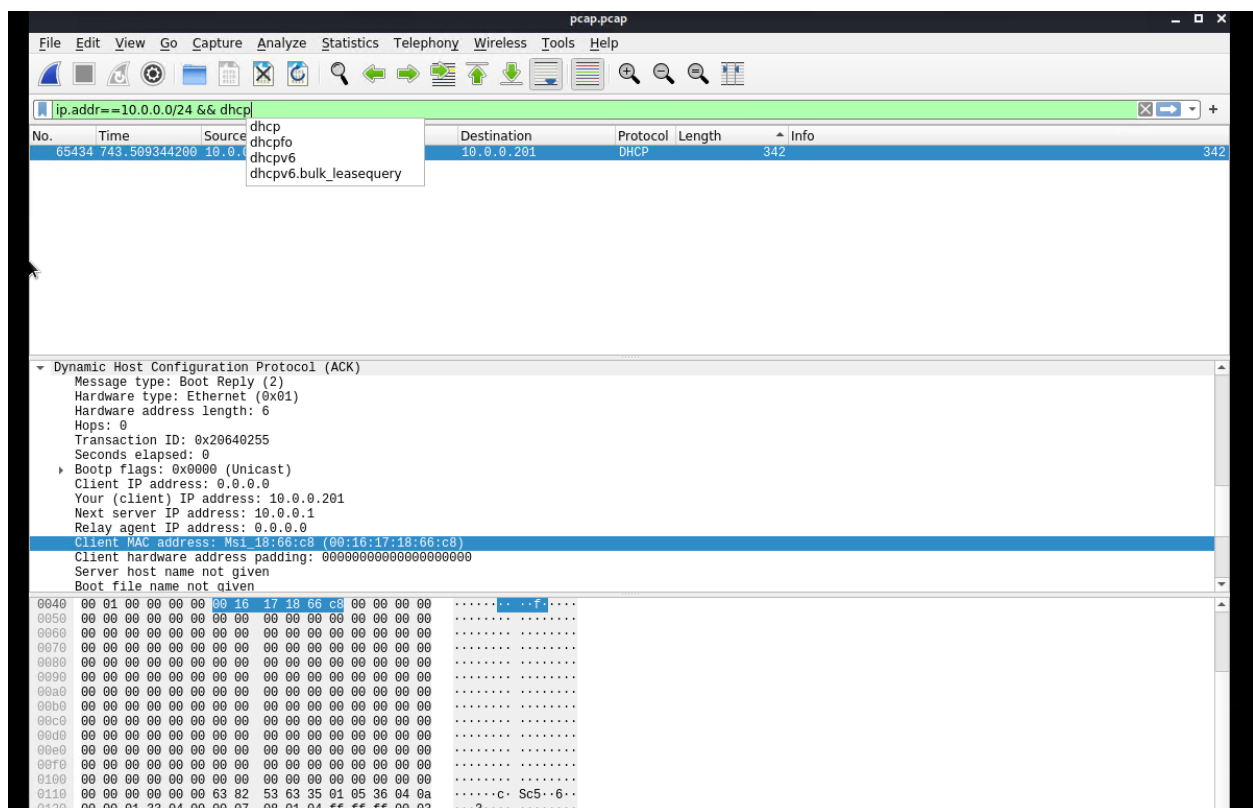
IT was informed that some users are torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringement.

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\$

No.	Time	Source	Destination	Protocol	Length	Info
66978	751.024207500	10.0.0.201	10.0.0.2	KRB5	382	
65725	744.601486200	10.0.0.201	10.0.0.2	KRB5	382	
65544	743.884105500	10.0.0.201	10.0.0.2	KRB5	382	
65625	744.255672900	10.0.0.201	10.0.0.2	KRB5	381	
65526	743.828382900	10.0.0.201	10.0.0.2	KRB5	381	
67044	751.205833000	10.0.0.201	10.0.0.2	KRB5	370	
67080	751.379585100	10.0.0.2	10.0.0.201	KRB5	303	
66970	751.007645200	10.0.0.201	10.0.0.2	KRB5	302	
65712	744.572819700	10.0.0.201	10.0.0.2	KRB5	301	
65617	744.239448800	10.0.0.201	10.0.0.2	KRB5	301	
65530	743.836192200	10.0.0.201	10.0.0.2	KRB5	301	
65505	743.708498600	10.0.0.201	10.0.0.2	KRB5	301	
65827	745.174120000	10.0.0.2	10.0.0.201	KRB5	293	
65745	744.704098600	10.0.0.2	10.0.0.201	KRB5	293	
65520	743.837392000	10.0.0.2	10.0.0.201	KRB5	293	
PA-DATA PA-PAC-REQUEST						
padata-type: KRB5-PADATA-PA-PAC-REQUEST (128)						
padata-value: 3005a0030101ff						
req-body						
padding: 0						
kdc-options: 40810010						
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						
till: 2037-09-13 02:48:05 (UTC)						
rtime: 2037-09-13 02:48:05 (UTC)						

- OS version: Windows NT 10.0

No.	Time	Source	Destination	Protocol	Length	Info
69347	767.585292600	10.0.0.201	168.215.194.14	HTTP	531	
69167	765.416418700	10.0.0.201	168.215.194.14	HTTP	500	
67333	752.898843300	10.0.0.201	168.215.194.14	HTTP	479	
67308	752.676394600	10.0.0.201	168.215.194.14	HTTP	477	
67337	752.915643000	10.0.0.201	168.215.194.14	HTTP	474	
67282	752.441022900	10.0.0.201	168.215.194.14	HTTP	474	
69142	765.263272500	10.0.0.201	168.215.194.14	HTTP	471	
67361	753.086811900	10.0.0.201	168.215.194.14	HTTP	471	
67328	752.881136800	10.0.0.201	168.215.194.14	HTTP	469	
67335	752.907197600	10.0.0.201	168.215.194.14	HTTP	468	
67330	752.889450700	10.0.0.201	168.215.194.14	HTTP	468	
67507	754.389413800	10.0.0.201	172.217.9.2	HTTP	467	
69213	765.837950500	10.0.0.201	168.215.194.14	HTTP	465	
67268	752.331198600	10.0.0.201	168.215.194.14	HTTP	463	
67343	753.087090000	10.0.0.201	168.215.194.14	HTTP	445	
...0 0000 0000 0000 = Fragment offset: 0						
Time to live: 128						
Protocol: TCP (6)						
Header checksum: 0x0d54 [validation disabled]						
[Header checksum status: Unverified]						
Source: 10.0.0.201						
Destination: 168.215.194.14						
Transmission Control Protocol, Src Port: 49757, Dst Port: 80, Seq: 1, Ack: 1, Len: 409						
Hypertext Transfer Protocol						
GET /nshowcat.html?category=animation HTTP/1.1\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						

- 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	769.568596300	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
67300	752.800456200	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..GET /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 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

```