Network Analysis

Time Thieves

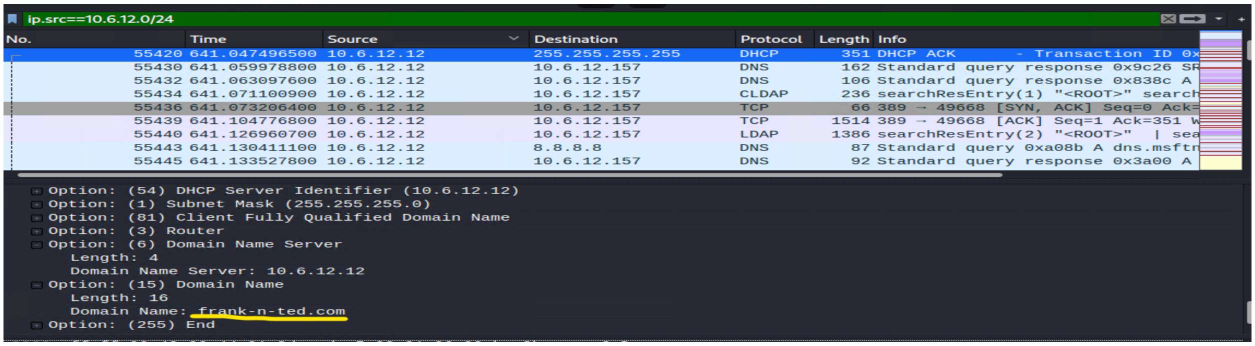
At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- 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.com

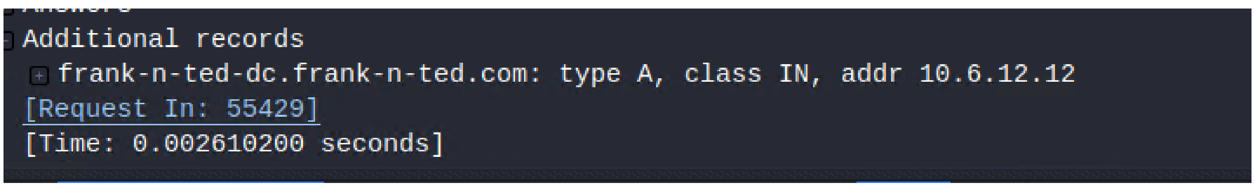
   

   ```
   ip.src==10.6.12.0/24
   No.   Time             Source         Destination       Protocol Length Info
   55420 641.047496500 10.6.12.12     255.255.255.255   DHCP      351 DHCP ACK       - Transaction ID 0x
   55430 641.059978800 10.6.12.12     10.6.12.157       DNS       162 Standard query response 0x9c26 SR
   55432 641.063097600 10.6.12.12     10.6.12.157       DNS       106 Standard query response 0x838c A
   55434 641.071100900 10.6.12.12     10.6.12.157       CLDAP     236 searchResEntry(1) "<ROOT>" search
   55436 641.073206400 10.6.12.12     10.6.12.157       TCP        66 389 → 49668 [SYN, ACK] Seq=0 Ack=
   55439 641.104776800 10.6.12.12     10.6.12.157       TCP      1514 389 → 49668 [ACK] Seq=1 Ack=351 W
   55440 641.126960700 10.6.12.12     10.6.12.157       LDAP     1386 searchResEntry(2) "<ROOT>"  | sea
   55443 641.130411100 10.6.12.12     8.8.8.8           DNS        87 Standard query 0xa08b A dns.msftn
   55445 641.133527800 10.6.12.12     10.6.12.157       DNS        92 Standard query response 0x3a00 A

   ⊞ Option: (54) DHCP Server Identifier (10.6.12.12)
   ⊞ Option: (1) Subnet Mask (255.255.255.0)
   ⊞ Option: (81) Client Fully Qualified Domain Name
   ⊞ Option: (3) Router
   ⊟ Option: (6) Domain Name Server
       Length: 4
       Domain Name Server: 10.6.12.12
   ⊟ Option: (15) Domain Name
       Length: 16
       Domain Name: frank-n-ted.com
   ⊞ Option: (255) End
   ```

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

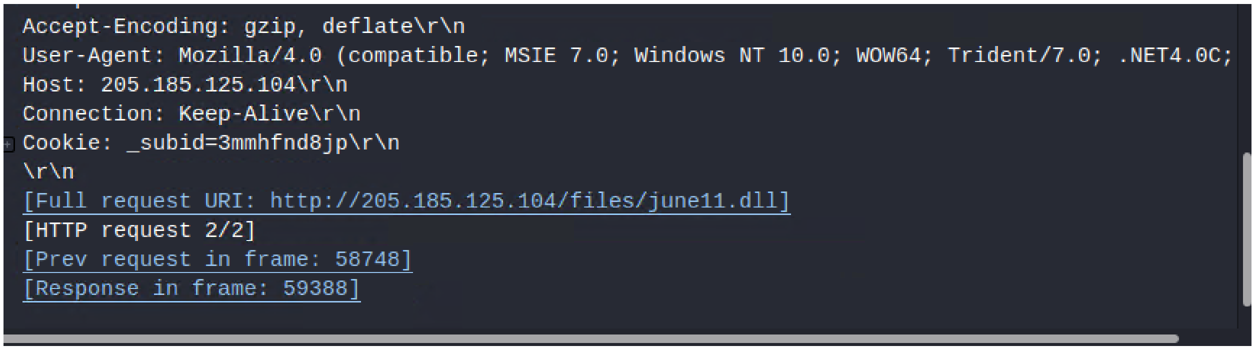
   10.6.12.12

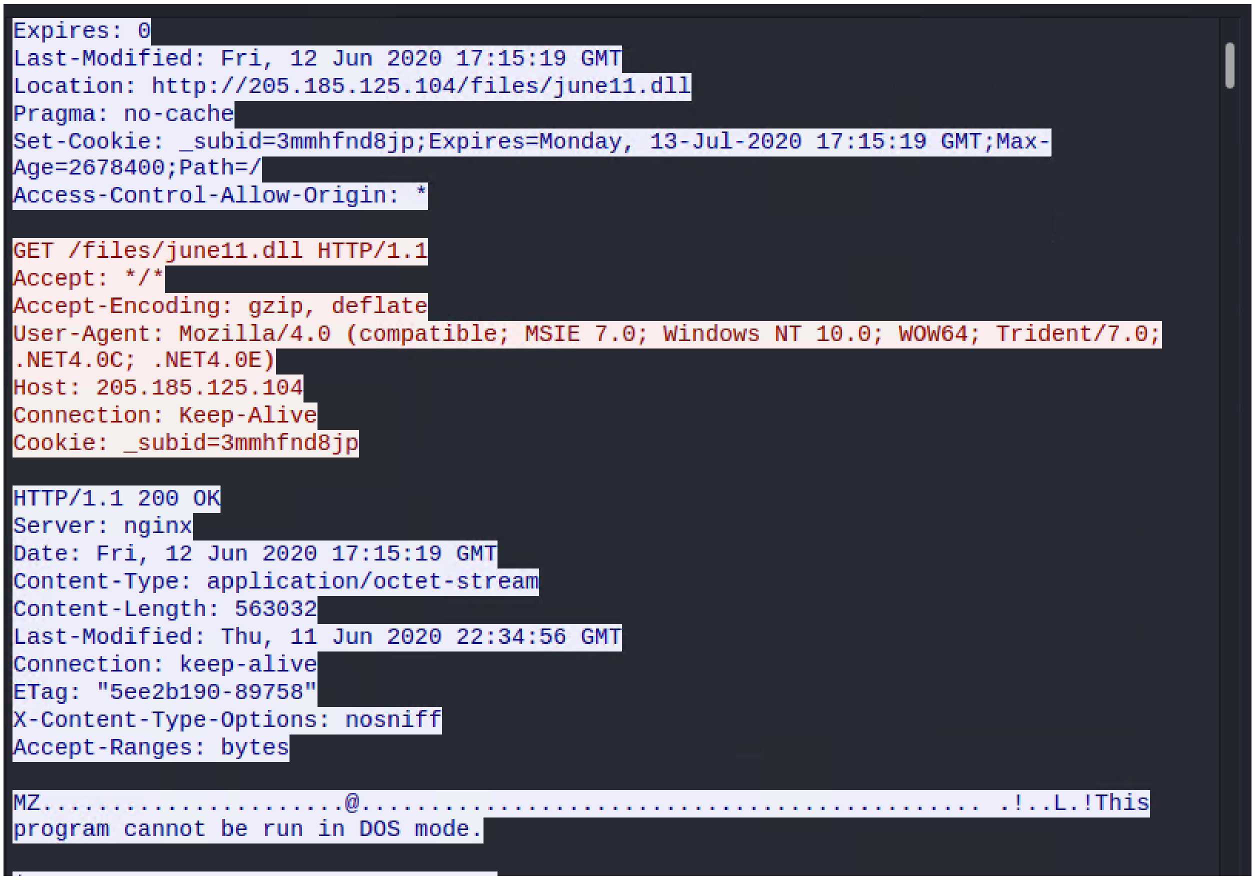
   ```
   Additional records
     ⊞ frank-n-ted-dc.frank-n-ted.com: type A, class IN, addr 10.6.12.12
   [Request In: 55429]
   [Time: 0.002610200 seconds]
   ```

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



```
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;
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: 58748]
[Response in frame: 59388]
```

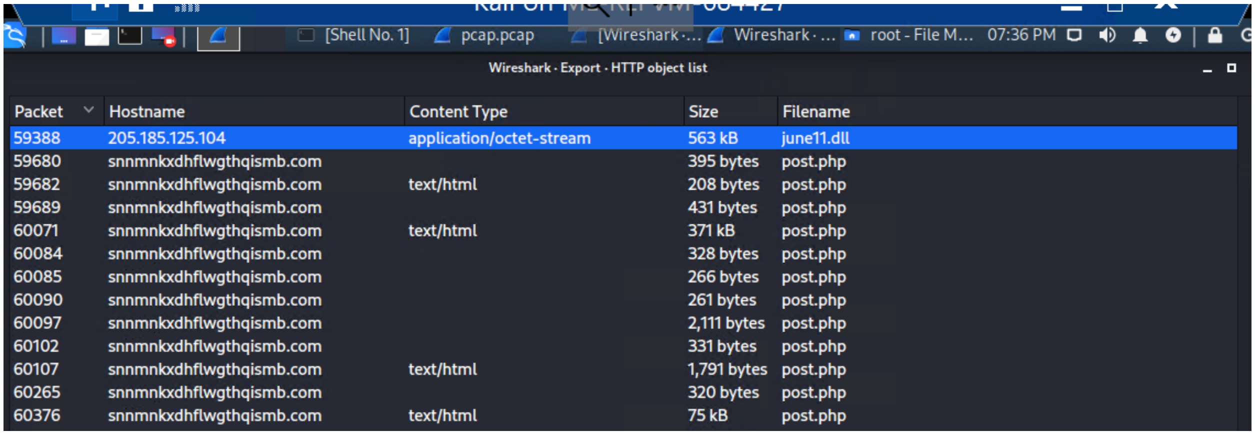


```
Expires: 0
Last-Modified: Fri, 12 Jun 2020 17:15:19 GMT
Location: http://205.185.125.104/files/june11.dll
Pragma: no-cache
Set-Cookie: _subid=3mmhfnd8jp;Expires=Monday, 13-Jul-2020 17:15:19 GMT;Max-
Age=2678400;Path=/
Access-Control-Allow-Origin: *

GET /files/june11.dll HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0;
.NET4.0C; .NET4.0E)
Host: 205.185.125.104
Connection: Keep-Alive
Cookie: _subid=3mmhfnd8jp

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 12 Jun 2020 17:15:19 GMT
Content-Type: application/octet-stream
Content-Length: 563032
Last-Modified: Thu, 11 Jun 2020 22:34:56 GMT
Connection: keep-alive
ETag: "5ee2b190-89758"
X-Content-Type-Options: nosniff
Accept-Ranges: bytes

MZ......................@.............................................  .!..L.!This
program cannot be run in DOS mode.
```

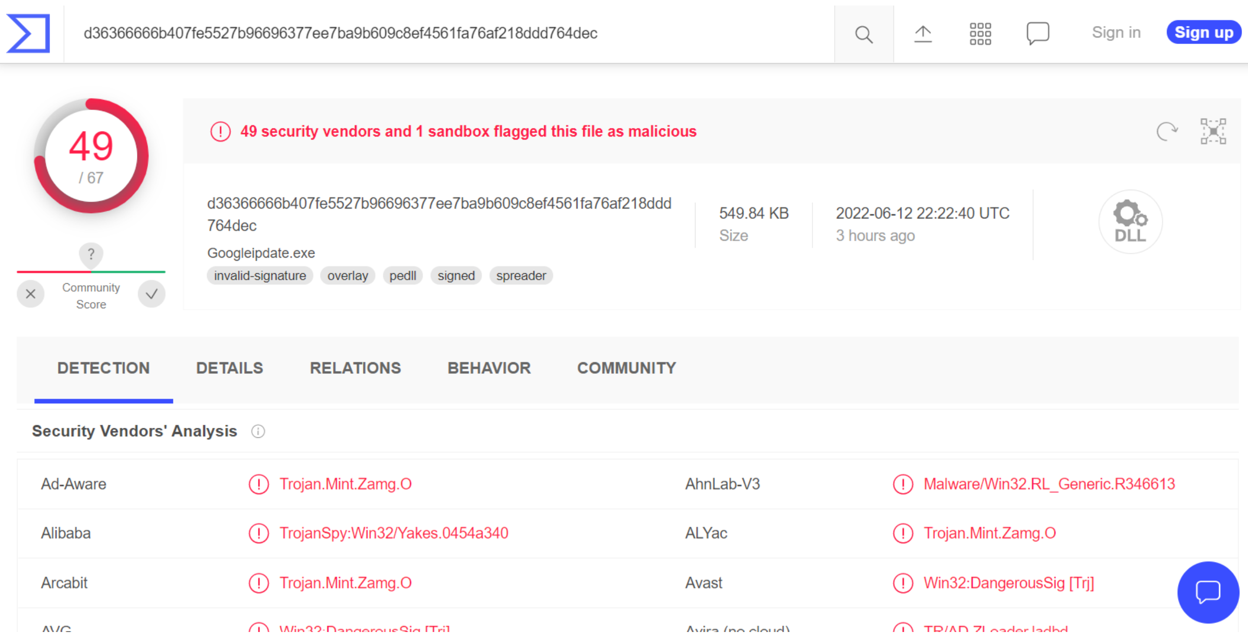


Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
59388	205.185.125.104	application/octet-stream	563 kB	june11.dll
59680	snnmnkxdhflwgthqismb.com		395 bytes	post.php
59682	snnmnkxdhflwgthqismb.com	text/html	208 bytes	post.php
59689	snnmnkxdhflwgthqismb.com		431 bytes	post.php
60071	snnmnkxdhflwgthqismb.com	text/html	371 kB	post.php
60084	snnmnkxdhflwgthqismb.com		328 bytes	post.php
60085	snnmnkxdhflwgthqismb.com		266 bytes	post.php
60090	snnmnkxdhflwgthqismb.com		261 bytes	post.php
60097	snnmnkxdhflwgthqismb.com		2,111 bytes	post.php
60102	snnmnkxdhflwgthqismb.com		331 bytes	post.php
60107	snnmnkxdhflwgthqismb.com	text/html	1,791 bytes	post.php
60265	snnmnkxdhflwgthqismb.com		320 bytes	post.php
60376	snnmnkxdhflwgthqismb.com	text/html	75 kB	post.php

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

Trojan



d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

49 / 67

Community Score

49 security vendors and 1 sandbox flagged this file as malicious

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Googleipdate.exe

invalid-signature overlay pedll signed spreader

549.84 KB
Size

2022-06-12 22:22:40 UTC
3 hours ago

Security Vendors' Analysis

Ad-Aware	Trojan.Mint.Zamg.O	AhnLab-V3	Malware/Win32.RL_Generic.R346613
Alibaba	TrojanSpy:Win32/Yakes.0454a340	ALYac	Trojan.Mint.Zamg.O
Arcabit	Trojan.Mint.Zamg.O	Avast	Win32:DangerousSig [Trj]
AVG	Win32:DangerousSig [Trj]	Avira (no cloud)	TR/AD.ZLoader.ladbd

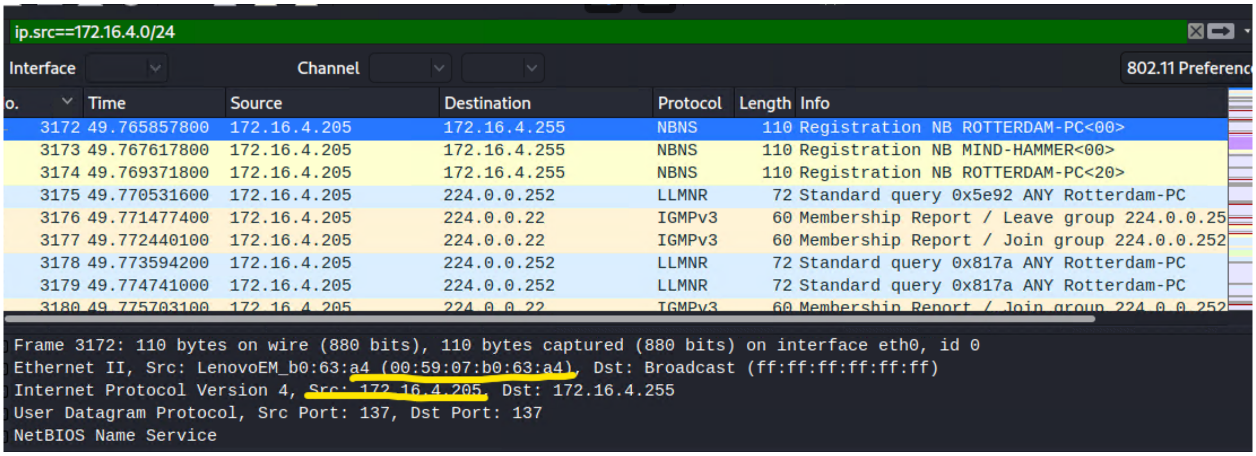
Vulnerable Windows Machines

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



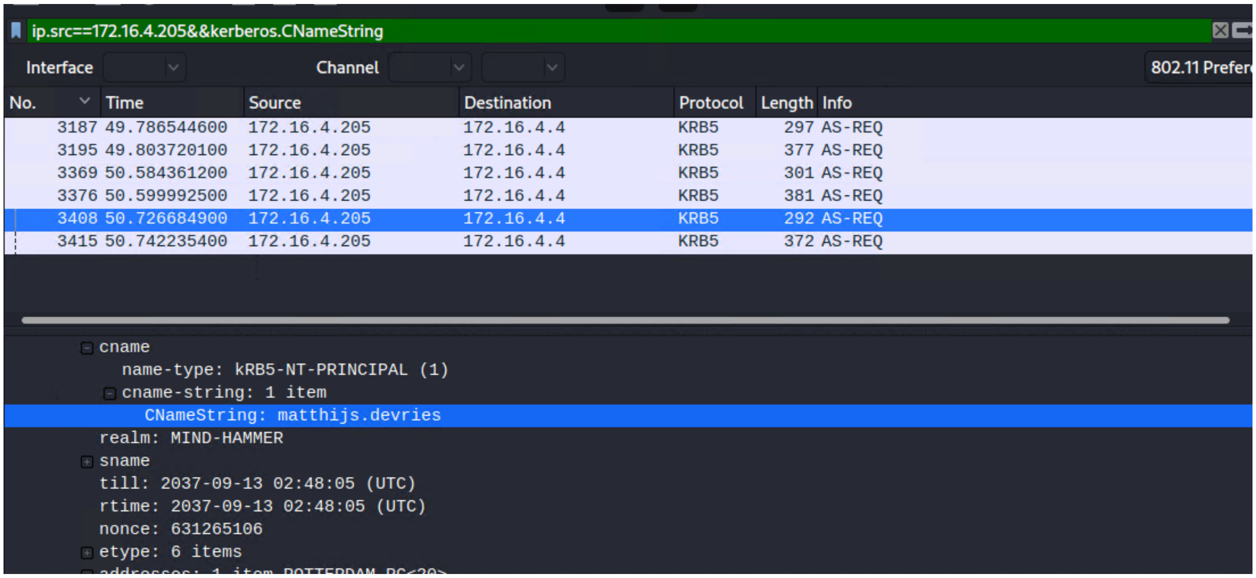
ip.src==172.16.4.0/24

```
o.     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>
  3175 49.770531600 172.16.4.205  224.0.0.252   LLMNR       72 Standard query 0x5e92 ANY Rotterdam-PC
  3176 49.771477400 172.16.4.205  224.0.0.22    IGMPv3      60 Membership Report / Leave group 224.0.0.25
  3177 49.772440100 172.16.4.205  224.0.0.22    IGMPv3      60 Membership Report / Join group 224.0.0.252
  3178 49.773594200 172.16.4.205  224.0.0.252   LLMNR       72 Standard query 0x817a ANY Rotterdam-PC
  3179 49.774741000 172.16.4.205  224.0.0.252   LLMNR       72 Standard query 0x817a ANY Rotterdam-PC
  3180 49.775703100 172.16.4.205  224.0.0.22    IGMPv3      60 Membership Report / Join group 224.0.0.252
```

```
Frame 3172: 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)
Internet Protocol Version 4, Src: 172.16.4.205, Dst: 172.16.4.255
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service
```

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

    The username is: **mattijs.dervies**

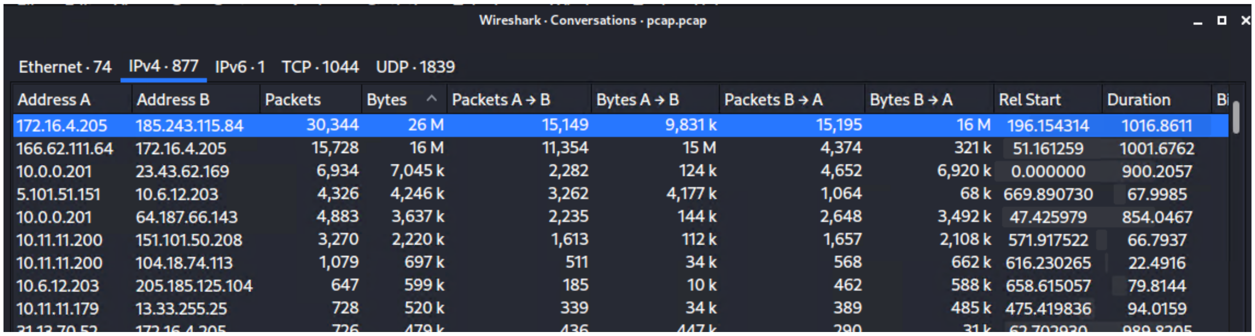


```
No.   Time          Source        Destination  Protocol Length Info
 3187 49.786544600  172.16.4.205  172.16.4.4   KRB5       297 AS-REQ
 3195 49.803720100  172.16.4.205  172.16.4.4   KRB5       377 AS-REQ
 3369 50.584361200  172.16.4.205  172.16.4.4   KRB5       301 AS-REQ
 3376 50.599992500  172.16.4.205  172.16.4.4   KRB5       381 AS-REQ
 3408 50.726684900  172.16.4.205  172.16.4.4   KRB5       292 AS-REQ
 3415 50.742235400  172.16.4.205  172.16.4.4   KRB5       372 AS-REQ
```

```
cname
  name-type: kRB5-NT-PRINCIPAL (1)
  cname-string: 1 item
    CNameString: matthijs.devries
realm: MIND-HAMMER
sname
till: 2037-09-13 02:48:05 (UTC)
rtime: 2037-09-13 02:48:05 (UTC)
nonce: 631265106
etype: 6 items
addresses: 1 item ROTTERDAM-PC<20>
```

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

   185.243.115.84



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bi
172.16.4.205	185.243.115.84	30,344	26 M	15,149	9,831 k	15,195	16 M	196.154314	1016.8611	
166.62.111.64	172.16.4.205	15,728	16 M	11,354	15 M	4,374	321 k	51.161259	1001.6762	
10.0.0.201	23.43.62.169	6,934	7,045 k	2,282	124 k	4,652	6,920 k	0.000000	900.2057	
5.101.51.151	10.6.12.203	4,326	4,246 k	3,262	4,177 k	1,064	68 k	669.890730	67.9985	
10.0.0.201	64.187.66.143	4,883	3,637 k	2,235	144 k	2,648	3,492 k	47.425979	854.0467	
10.11.11.200	151.101.50.208	3,270	2,220 k	1,613	112 k	1,657	2,108 k	571.917522	66.7937	
10.11.11.200	104.18.74.113	1,079	697 k	511	34 k	568	662 k	616.230265	22.4916	
10.6.12.203	205.185.125.104	647	599 k	185	10 k	462	588 k	658.615057	79.8144	
10.11.11.179	13.33.255.25	728	520 k	339	34 k	389	485 k	475.419836	94.0159	
31.13.70.52	172.16.4.205	726	479 k	436	447 k	290	31 k	62.702930	989.8205	

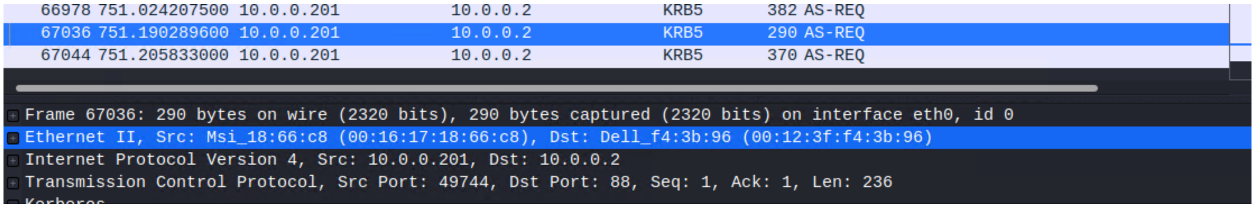
Illegal Downloads

1.Find the following information about the machine with IP address 10.0.0.201:

MAC address: 00:16:17:18:66:c8

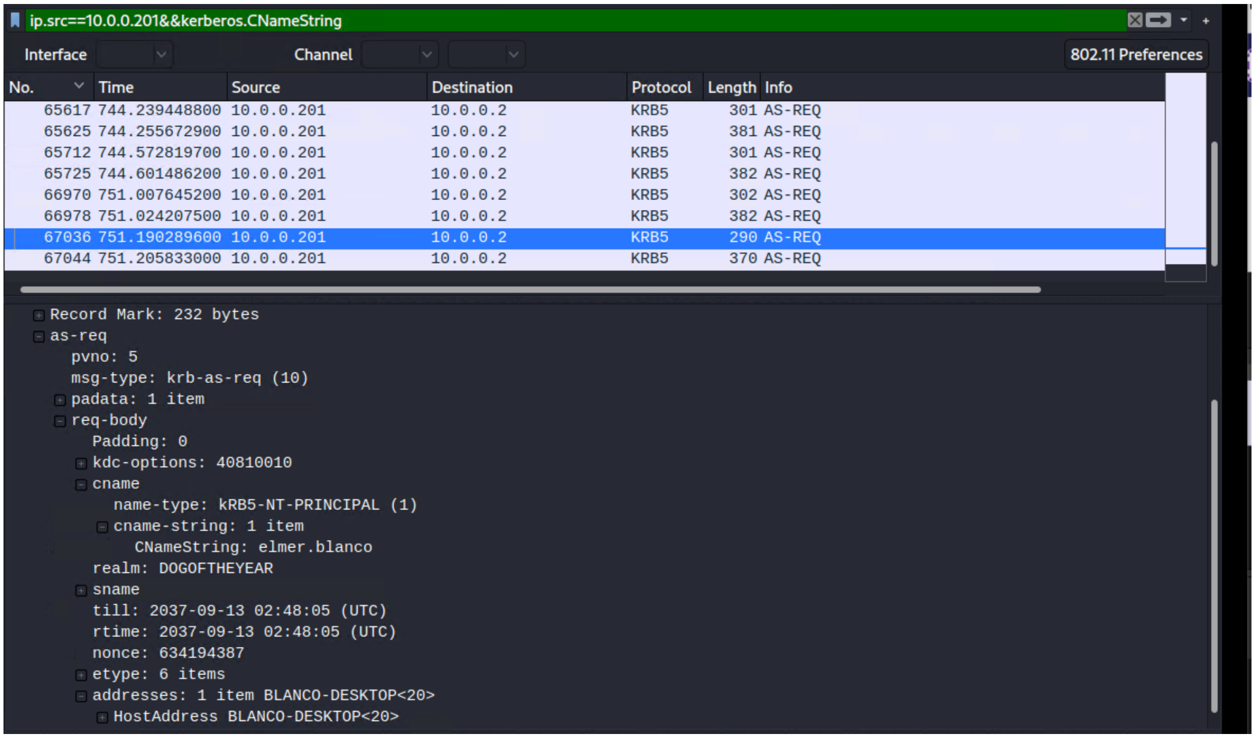
Windows username: elmer.blanco

Computer host name: BLANCO-DESKTOP



```
  66978 751.024207500 10.0.0.201          10.0.0.2            KRB5        382 AS-REQ
  67036 751.190289600 10.0.0.201          10.0.0.2            KRB5        290 AS-REQ
  67044 751.205833000 10.0.0.201          10.0.0.2            KRB5        370 AS-REQ

Frame 67036: 290 bytes on wire (2320 bits), 290 bytes captured (2320 bits) on interface eth0, id 0
Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Dell_f4:3b:96 (00:12:3f:f4:3b:96)
Internet Protocol Version 4, Src: 10.0.0.201, Dst: 10.0.0.2
Transmission Control Protocol, Src Port: 49744, Dst Port: 88, Seq: 1, Ack: 1, Len: 236
Kerberos
```



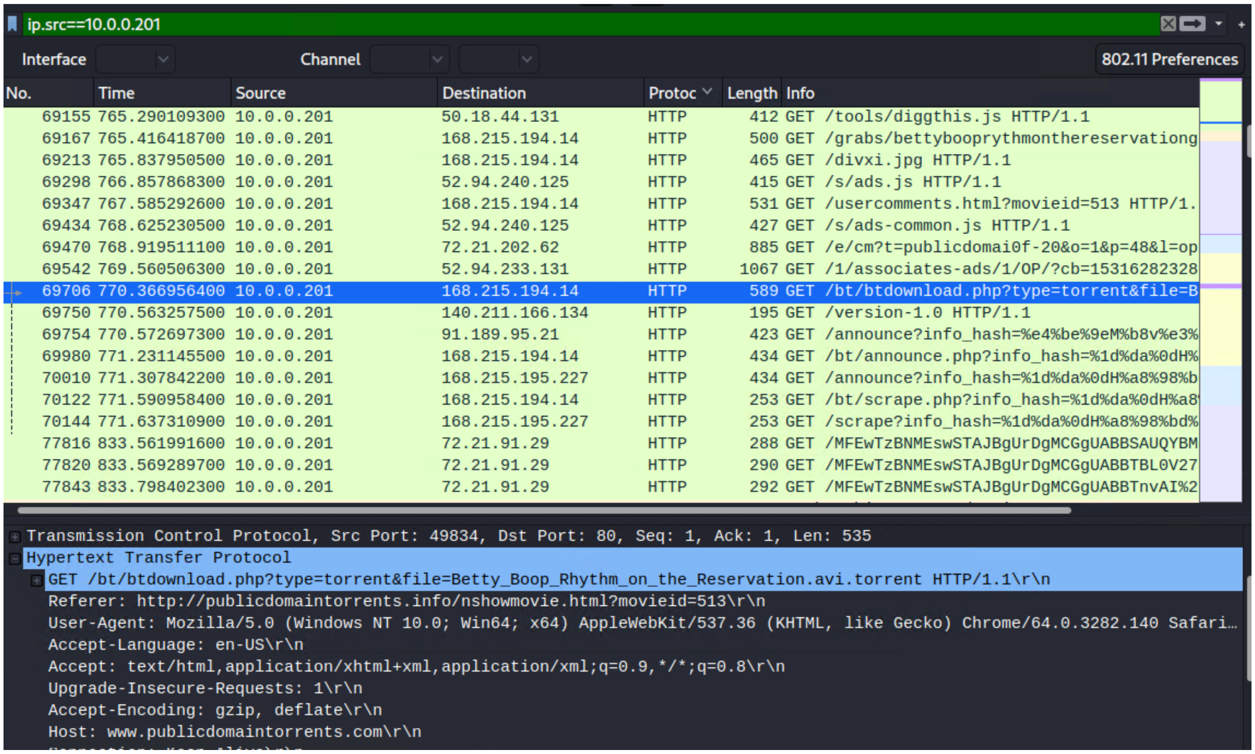
```
ip.src==10.0.0.201&&kerberos.CNameString

No.    Time          Source              Destination         Protocol  Length Info
  65617 744.239448800 10.0.0.201          10.0.0.2            KRB5        301 AS-REQ
  65625 744.255672900 10.0.0.201          10.0.0.2            KRB5        381 AS-REQ
  65712 744.572819700 10.0.0.201          10.0.0.2            KRB5        301 AS-REQ
  65725 744.601486200 10.0.0.201          10.0.0.2            KRB5        382 AS-REQ
  66970 751.007645200 10.0.0.201          10.0.0.2            KRB5        302 AS-REQ
  66978 751.024207500 10.0.0.201          10.0.0.2            KRB5        382 AS-REQ
  67036 751.190289600 10.0.0.201          10.0.0.2            KRB5        290 AS-REQ
  67044 751.205833000 10.0.0.201          10.0.0.2            KRB5        370 AS-REQ

  Record Mark: 232 bytes
  as-req
    pvno: 5
    msg-type: krb-as-req (10)
    padata: 1 item
    req-body
      Padding: 0
      kdc-options: 40810010
      cname
        name-type: kRB5-NT-PRINCIPAL (1)
        cname-string: 1 item
          CNameString: elmer.blanco
      realm: DOGOFTHEYEAR
      sname
      till: 2037-09-13 02:48:05 (UTC)
      rtime: 2037-09-13 02:48:05 (UTC)
      nonce: 634194387
      etype: 6 items
      addresses: 1 item BLANCO-DESKTOP<20>
        HostAddress BLANCO-DESKTOP<20>
```

2. Which torrent file did the user download?

Betty_Boop_Rhythm_on_the_Reservation.avi.torrent



ip.src==10.0.0.201

```
No.   Time          Source      Destination      Protoc Length Info
69155 765.290109300 10.0.0.201  50.18.44.131     HTTP    412 GET /tools/diggthis.js HTTP/1.1
69167 765.416418700 10.0.0.201  168.215.194.14   HTTP    500 GET /grabs/bettybooprythmonthereservationg
69213 765.837950500 10.0.0.201  168.215.194.14   HTTP    465 GET /divxi.jpg HTTP/1.1
69298 766.857868300 10.0.0.201  52.94.240.125    HTTP    415 GET /s/ads.js HTTP/1.1
69347 767.585292600 10.0.0.201  168.215.194.14   HTTP    531 GET /usercomments.html?movieid=513 HTTP/1.
69434 768.625230500 10.0.0.201  52.94.240.125    HTTP    427 GET /s/ads-common.js HTTP/1.1
69470 768.919511100 10.0.0.201  72.21.202.62     HTTP    885 GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=op
69542 769.560506300 10.0.0.201  52.94.233.131    HTTP   1067 GET /1/associates-ads/1/OP/?cb=15316282328
69706 770.366956400 10.0.0.201  168.215.194.14   HTTP    589 GET /bt/btdownload.php?type=torrent&file=B
69750 770.563257500 10.0.0.201  140.211.166.134  HTTP    195 GET /version-1.0 HTTP/1.1
69754 770.572697300 10.0.0.201  91.189.95.21     HTTP    423 GET /announce?info_hash=%e4%be%9eM%b8v%e3%
69980 771.231145500 10.0.0.201  168.215.194.14   HTTP    434 GET /bt/announce.php?info_hash=%1d%da%0dH%
70010 771.307842200 10.0.0.201  168.215.195.227  HTTP    434 GET /announce?info_hash=%1d%da%0dH%a8%98%b
70122 771.590958400 10.0.0.201  168.215.194.14   HTTP    253 GET /bt/scrape.php?info_hash=%1d%da%0dH%a8
70144 771.637310900 10.0.0.201  168.215.195.227  HTTP    253 GET /scrape?info_hash=%1d%da%0dH%a8%98%bd%
77816 833.561991600 10.0.0.201  72.21.91.29      HTTP    288 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBM
77820 833.569289700 10.0.0.201  72.21.91.29      HTTP    290 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27
77843 833.798402300 10.0.0.201  72.21.91.29      HTTP    292 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTnvAI%2
```

```
⊞ 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…
    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
```