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:

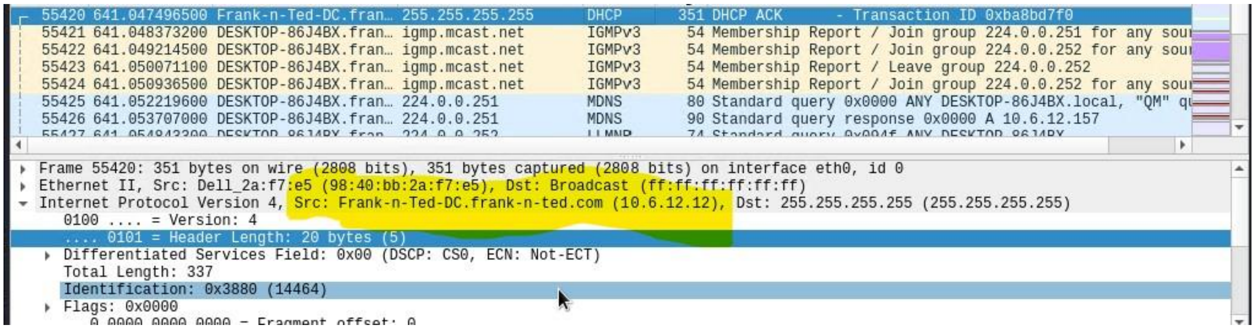
- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.
- Their IP addresses are somewhere in the range `10.6.12.0/24`.

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

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

   Filter: ip.addr==10.6.12.0/24

   The domain name is: **Frank-n-Ted-DC.frank-n-ted.com**

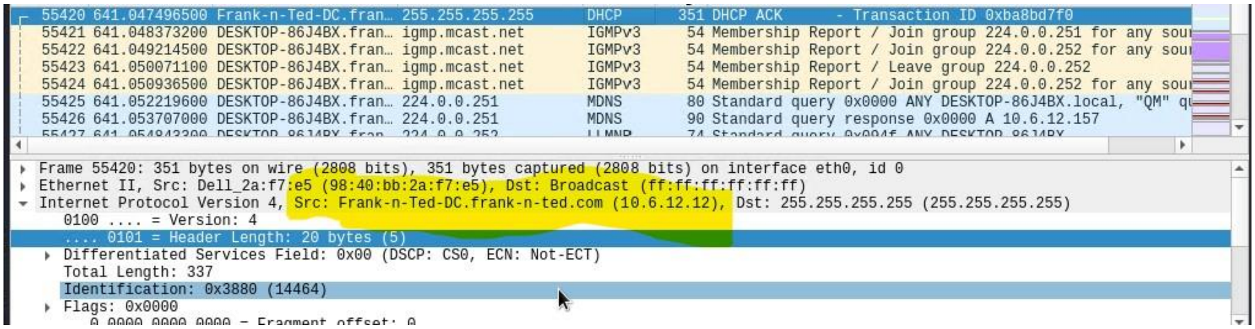
   

```
55420 641.047496500 Frank-n-Ted-DC.fran… 255.255.255.255    DHCP     351 DHCP ACK      - Transaction ID 0xba8bd7f0
55421 641.048373200 DESKTOP-86J4BX.fran… igmp.mcast.net     IGMPv3    54 Membership Report / Join group 224.0.0.251 for any sou
55422 641.049214500 DESKTOP-86J4BX.fran… igmp.mcast.net     IGMPv3    54 Membership Report / Join group 224.0.0.252 for any sou
55423 641.050071100 DESKTOP-86J4BX.fran… igmp.mcast.net     IGMPv3    54 Membership Report / Leave group 224.0.0.252
55424 641.050936500 DESKTOP-86J4BX.fran… igmp.mcast.net     IGMPv3    54 Membership Report / Join group 224.0.0.252 for any sou
55425 641.052219600 DESKTOP-86J4BX.fran… 224.0.0.251        MDNS      80 Standard query 0x0000 ANY DESKTOP-86J4BX.local, "QM" q
55426 641.053707000 DESKTOP-86J4BX.fran… 224.0.0.251        MDNS      90 Standard query response 0x0000 A 10.6.12.157
55427 641.054843300 DESKTOP-86J4BX.fran… 224.0.0.252        LLMNR     74 Standard query 0x004f ANY DESKTOP-86J4BX

Frame 55420: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits) on interface eth0, id 0
Ethernet II, Src: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12), Dst: 255.255.255.255 (255.255.255.255)
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 337
  Identification: 0x3880 (14464)
  Flags: 0x0000
    0 0000 0000 0000 = Fragment offset: 0
```

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

   Filter: ip.addr==10.6.12.0/24

   The IP address is: **10.6.12.12** (Frank-n-Ted-DC.frank-n-ted.com)



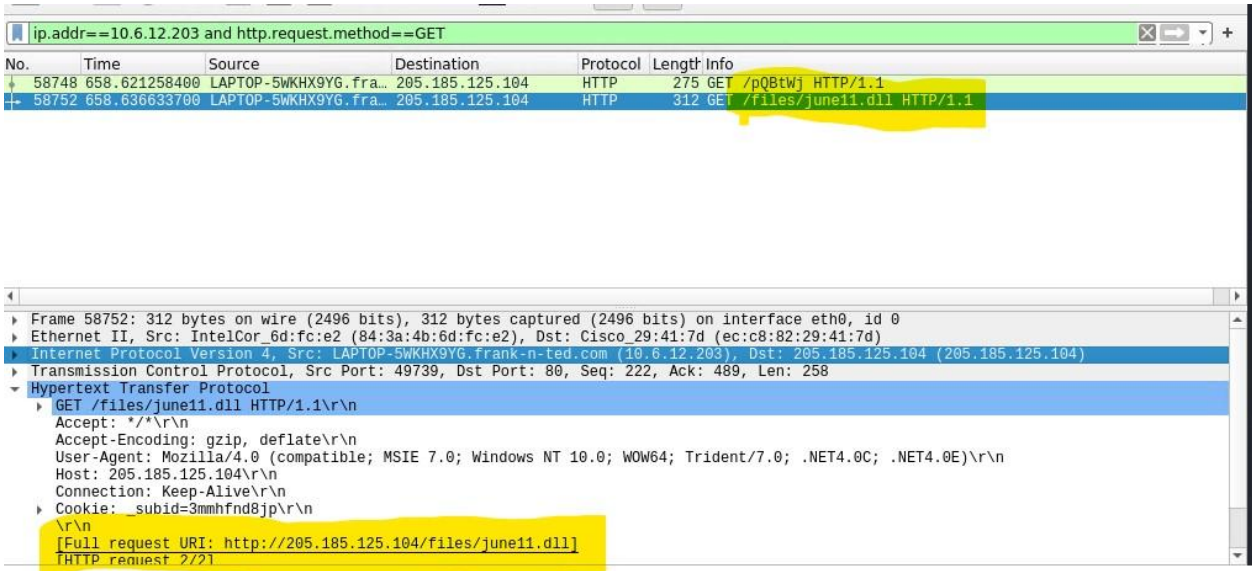
```
55420 641.047496500 Frank-n-Ted-DC.fran… 255.255.255.255      DHCP       351 DHCP ACK      - Transaction ID 0xba8bd7f0
55421 641.048373200 DESKTOP-86J4BX.fran… igmp.mcast.net       IGMPv3      54 Membership Report / Join group 224.0.0.251 for any sou
55422 641.049214500 DESKTOP-86J4BX.fran… igmp.mcast.net       IGMPv3      54 Membership Report / Join group 224.0.0.252 for any sou
55423 641.050071100 DESKTOP-86J4BX.fran… igmp.mcast.net       IGMPv3      54 Membership Report / Leave group 224.0.0.252
55424 641.050936500 DESKTOP-86J4BX.fran… igmp.mcast.net       IGMPv3      54 Membership Report / Join group 224.0.0.252 for any sou
55425 641.052219600 DESKTOP-86J4BX.fran… 224.0.0.251          MDNS        80 Standard query 0x0000 ANY DESKTOP-86J4BX.local, "QM" qu
55426 641.053707000 DESKTOP-86J4BX.fran… 224.0.0.251          MDNS        90 Standard query response 0x0000 A 10.6.12.157
55427 641.054843300 DESKTOP-86J4BX.fran… 224.0.0.252          LLMNR       74 Standard query 0x004f ANY DESKTOP-86J4BX

Frame 55420: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits) on interface eth0, id 0
Ethernet II, Src: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12), Dst: 255.255.255.255 (255.255.255.255)
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 337
  Identification: 0x3880 (14464)
  Flags: 0x0000
    0 0000 0000 0000 = Fragment offset: 0
```

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.

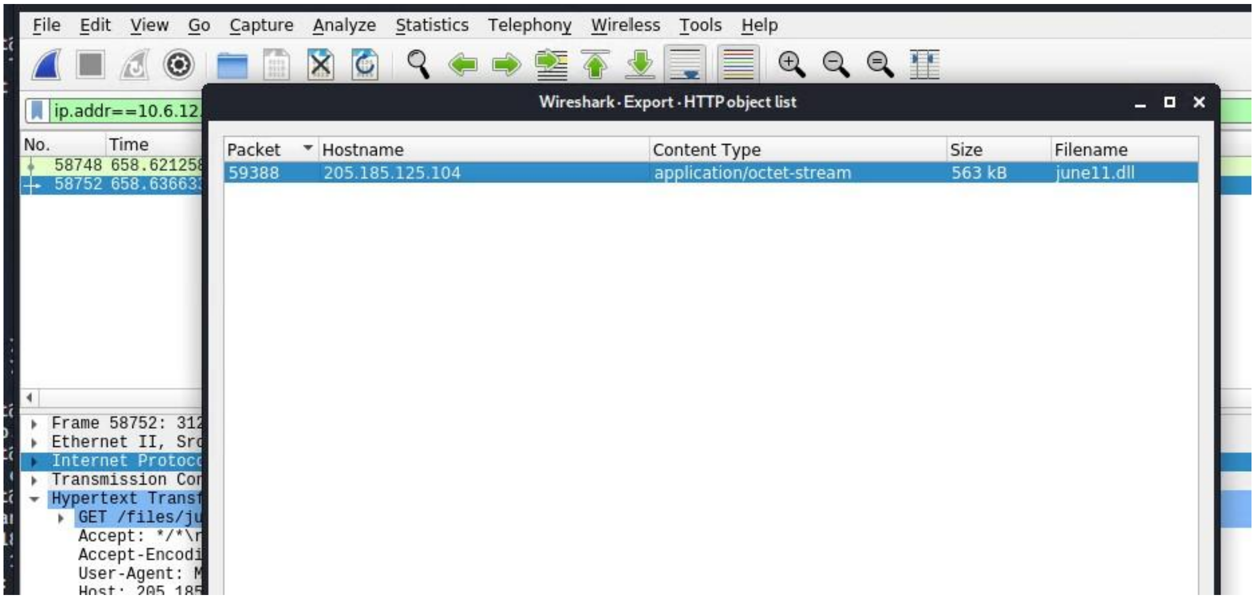
   Filter: ip.addr==10.6.12.203 and http.request.method==GET

   Export: File > Export Objects > HTTP

   The name of the file is: **june11.dll**



```
ip.addr==10.6.12.203 and http.request.method==GET

No.   Time           Source                   Destination       Protocol  Length Info
58748 658.621258400  LAPTOP-5WKHX9YG.fra…     205.185.125.104   HTTP      275 GET /pQBtWj HTTP/1.1
58752 658.636633700  LAPTOP-5WKHX9YG.fra…     205.185.125.104   HTTP      312 GET /files/june11.dll HTTP/1.1

Frame 58752: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface eth0, id 0
Ethernet II, Src: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2), Dst: Cisco_29:41:7d (ec:c8:82:29:41:7d)
Internet Protocol Version 4, Src: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203), Dst: 205.185.125.104 (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]
```

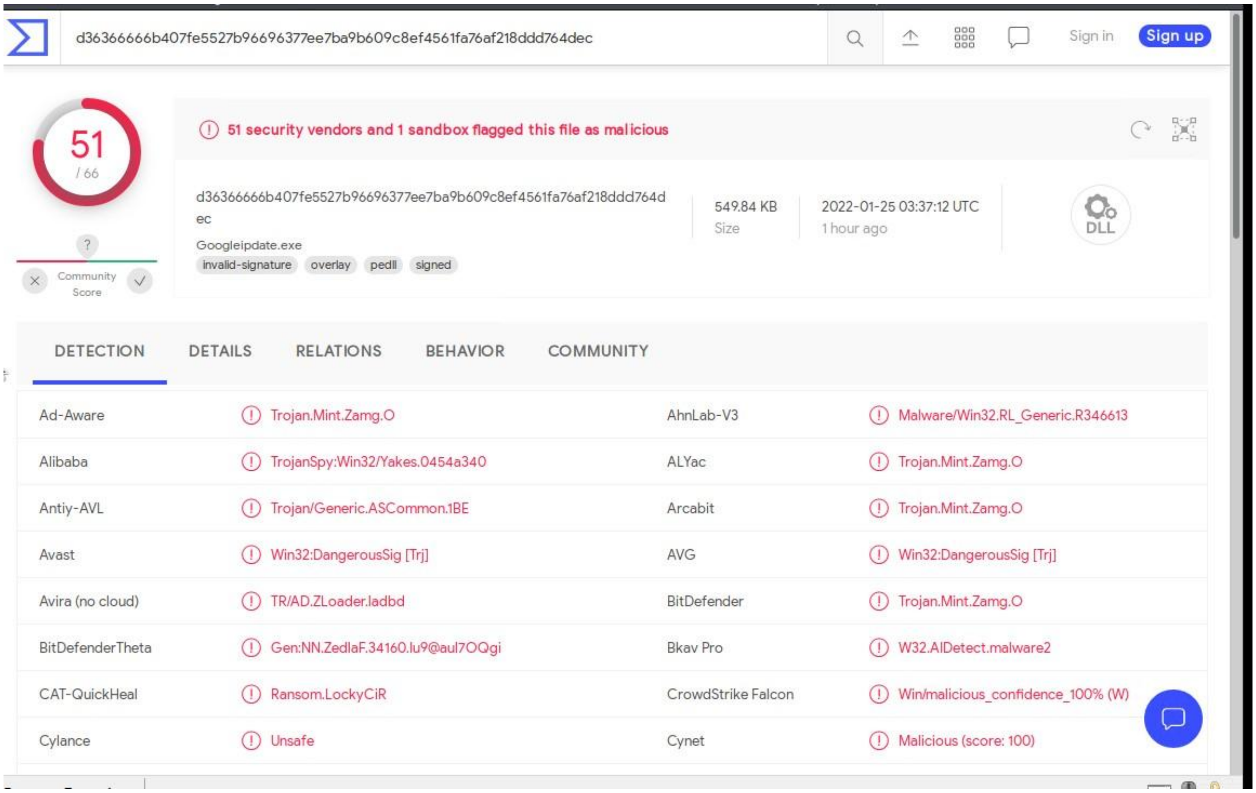

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Export · HTTP object list

```
ip.addr==10.6.12
No.   Time
58748 658.62125
58752 658.63663

Frame 58752: 312
Ethernet II, Src
Internet Protoco
Transmission Con
Hypertext Transf
  GET /files/ju
  Accept: */*\r
  Accept-Encodi
  User-Agent: M
  Host: 205.185
```

Packet	Hostname	Content Type	Size	Filename
59388	205.185.125.104	application/octet-stream	563 kB	june11.dll

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

This type of malware is classified as: A **Trojan**



d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

51 security vendors and 1 sandbox flagged this file as malicious

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Googleipdate.exe

invalid-signature overlay pedll signed

549.84 KB Size

2022-01-25 03:37:12 UTC 1 hour ago

Ad-Aware	Trojan.Mint.Zamg.O	AhnLab-V3	Malware/Win32.RL_Generic.R346613
Alibaba	TrojanSpy:Win32/Yakes.0454a340	ALYac	Trojan.Mint.Zamg.O
Antiy-AVL	Trojan/Generic.ASCommon.1BE	Arcabit	Trojan.Mint.Zamg.O
Avast	Win32:DangerousSig [Trj]	AVG	Win32:DangerousSig [Trj]
Avira (no cloud)	TR/AD.ZLoader.ladbd	BitDefender	Trojan.Mint.Zamg.O
BitDefenderTheta	Gen:NN.ZedlaF.34160.lu9@aul7OQgi	Bkav Pro	W32.AIDetect.malware2
CAT-QuickHeal	Ransom.LockyCiR	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 100)

Vulnerable Windows Machines

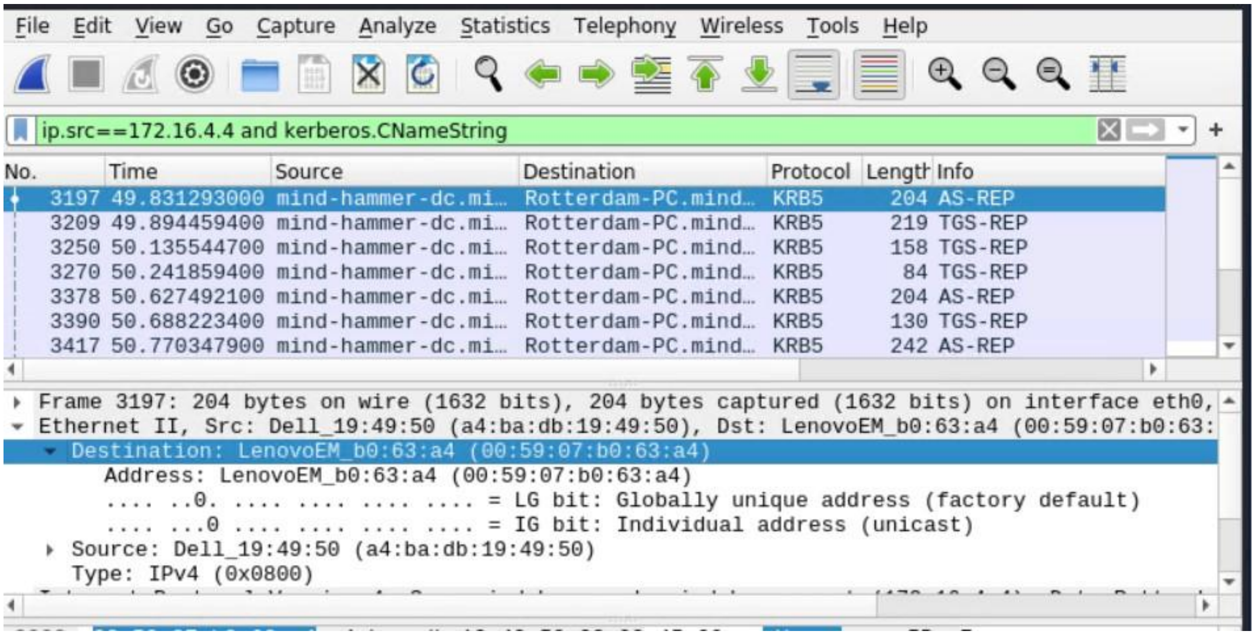
The Security team received reports of an infected Windows host on the network. They know the following:

- 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**

Filter: ip.src==172.16.4.4 and kerberos.CNameString



ip.src==172.16.4.4 and kerberos.CNameString

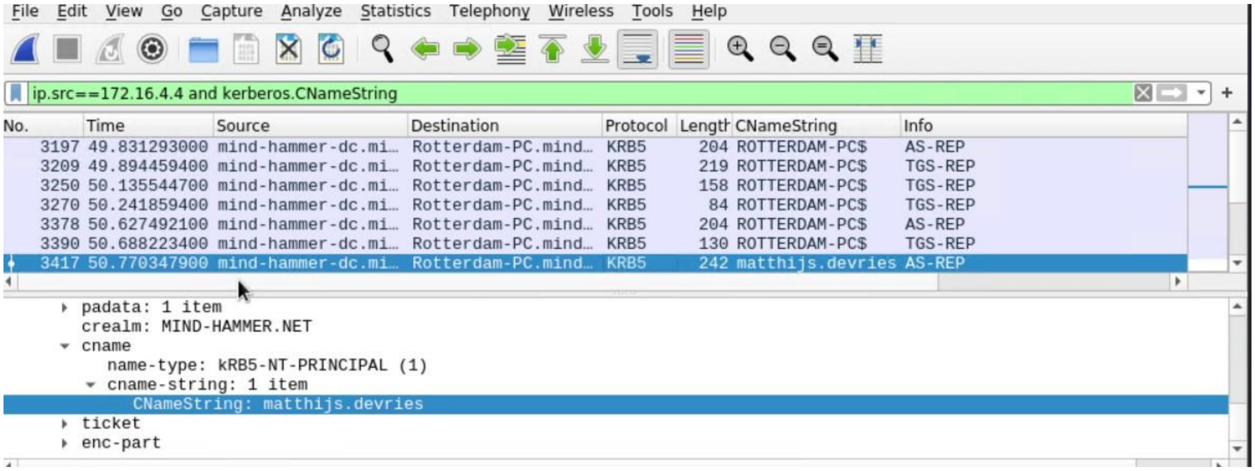
```
No.    Time          Source               Destination          Protocol Length Info
  3197 49.831293000 mind-hammer-dc.mi…  Rotterdam-PC.mind…  KRB5      204 AS-REP
  3209 49.894459400 mind-hammer-dc.mi…  Rotterdam-PC.mind…  KRB5      219 TGS-REP
  3250 50.135544700 mind-hammer-dc.mi…  Rotterdam-PC.mind…  KRB5      158 TGS-REP
  3270 50.241859400 mind-hammer-dc.mi…  Rotterdam-PC.mind…  KRB5       84 TGS-REP
  3378 50.627492100 mind-hammer-dc.mi…  Rotterdam-PC.mind…  KRB5      204 AS-REP
  3390 50.688223400 mind-hammer-dc.mi…  Rotterdam-PC.mind…  KRB5      130 TGS-REP
  3417 50.770347900 mind-hammer-dc.mi…  Rotterdam-PC.mind…  KRB5      242 AS-REP
```

```
▸ Frame 3197: 204 bytes on wire (1632 bits), 204 bytes captured (1632 bits) on interface eth0,
▾ Ethernet II, Src: Dell_19:49:50 (a4:ba:db:19:49:50), Dst: LenovoEM_b0:63:a4 (00:59:07:b0:63:
  ▾ Destination: 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)
  ▸ Source: Dell_19:49:50 (a4:ba:db:19:49:50)
    Type: IPv4 (0x0800)
```

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

Filter: ip.src==172.16.4.4 and kerberos.CNameString

The username is: **matthijs.devries**

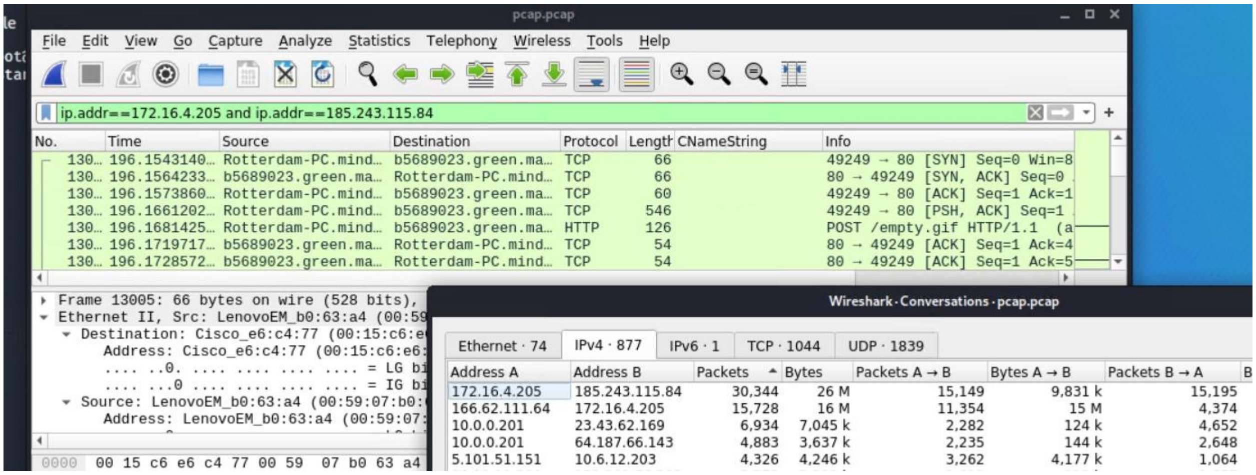

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.src==172.16.4.4 and kerberos.CNameString

No.   Time          Source               Destination        Protocol Length CNameString      Info
 3197 49.831293000 mind-hammer-dc.mi… Rotterdam-PC.mind… KRB5     204 ROTTERDAM-PC$    AS-REP
 3209 49.894459400 mind-hammer-dc.mi… Rotterdam-PC.mind… KRB5     219 ROTTERDAM-PC$    TGS-REP
 3250 50.135544700 mind-hammer-dc.mi… Rotterdam-PC.mind… KRB5     158 ROTTERDAM-PC$    TGS-REP
 3270 50.241859400 mind-hammer-dc.mi… Rotterdam-PC.mind… KRB5      84 ROTTERDAM-PC$    TGS-REP
 3378 50.627492100 mind-hammer-dc.mi… Rotterdam-PC.mind… KRB5     204 ROTTERDAM-PC$    AS-REP
 3390 50.688223400 mind-hammer-dc.mi… Rotterdam-PC.mind… KRB5     130 ROTTERDAM-PC$    TGS-REP
 3417 50.770347900 mind-hammer-dc.mi… Rotterdam-PC.mind… KRB5     242 matthijs.devries AS-REP

  ▸ padata: 1 item
    crealm: MIND-HAMMER.NET
  ▾ cname
      name-type: kRB5-NT-PRINCIPAL (1)
    ▾ cname-string: 1 item
        CNameString: matthijs.devries
  ▸ ticket
  ▸ enc-part
```

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

   Statistics > Conversations > IPv4 (tab) > Packets (high to low)

   Filter: ip.addr==172.16.4.205 and ip.addr==185.243.115.84


pcap.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Conversations · pcap.pcap
Ethernet · 74
IPv4 · 877
IPv6 · 1
TCP · 1044
UDP · 1839

```
ip.addr==172.16.4.205 and ip.addr==185.243.115.84

No.   Time           Source               Destination          Protocol Length CNameString Info
130… 196.1543140… Rotterdam-PC.mind… b5689023.green.ma… TCP       66             49249 → 80 [SYN] Seq=0 Win=8
130… 196.1564233… b5689023.green.ma… Rotterdam-PC.mind… TCP       66             80 → 49249 [SYN, ACK] Seq=0
130… 196.1573860… Rotterdam-PC.mind… b5689023.green.ma… TCP       60             49249 → 80 [ACK] Seq=1 Ack=1
130… 196.1661202… Rotterdam-PC.mind… b5689023.green.ma… TCP      546             49249 → 80 [PSH, ACK] Seq=1
130… 196.1681425… Rotterdam-PC.mind… b5689023.green.ma… HTTP     126             POST /empty.gif HTTP/1.1  (a
130… 196.1719717… b5689023.green.ma… Rotterdam-PC.mind… TCP       54             80 → 49249 [ACK] Seq=1 Ack=4
130… 196.1728572… b5689023.green.ma… Rotterdam-PC.mind… TCP       54             80 → 49249 [ACK] Seq=1 Ack=5

▸ Frame 13005: 66 bytes on wire (528 bits),
▾ Ethernet II, Src: LenovoEM_b0:63:a4 (00:59
  ▾ Destination: Cisco_e6:c4:77 (00:15:c6:e
      Address: Cisco_e6:c4:77 (00:15:c6:e6:
      .... ..0. .... .... .... .... = LG bi
      .... ...0 .... .... .... .... = IG bi
  ▾ Source: LenovoEM_b0:63:a4 (00:59:07:b0:
      Address: LenovoEM_b0:63:a4 (00:59:07:

0000  00 15 c6 e6 c4 77 00 59  07 b0 63 a4
```

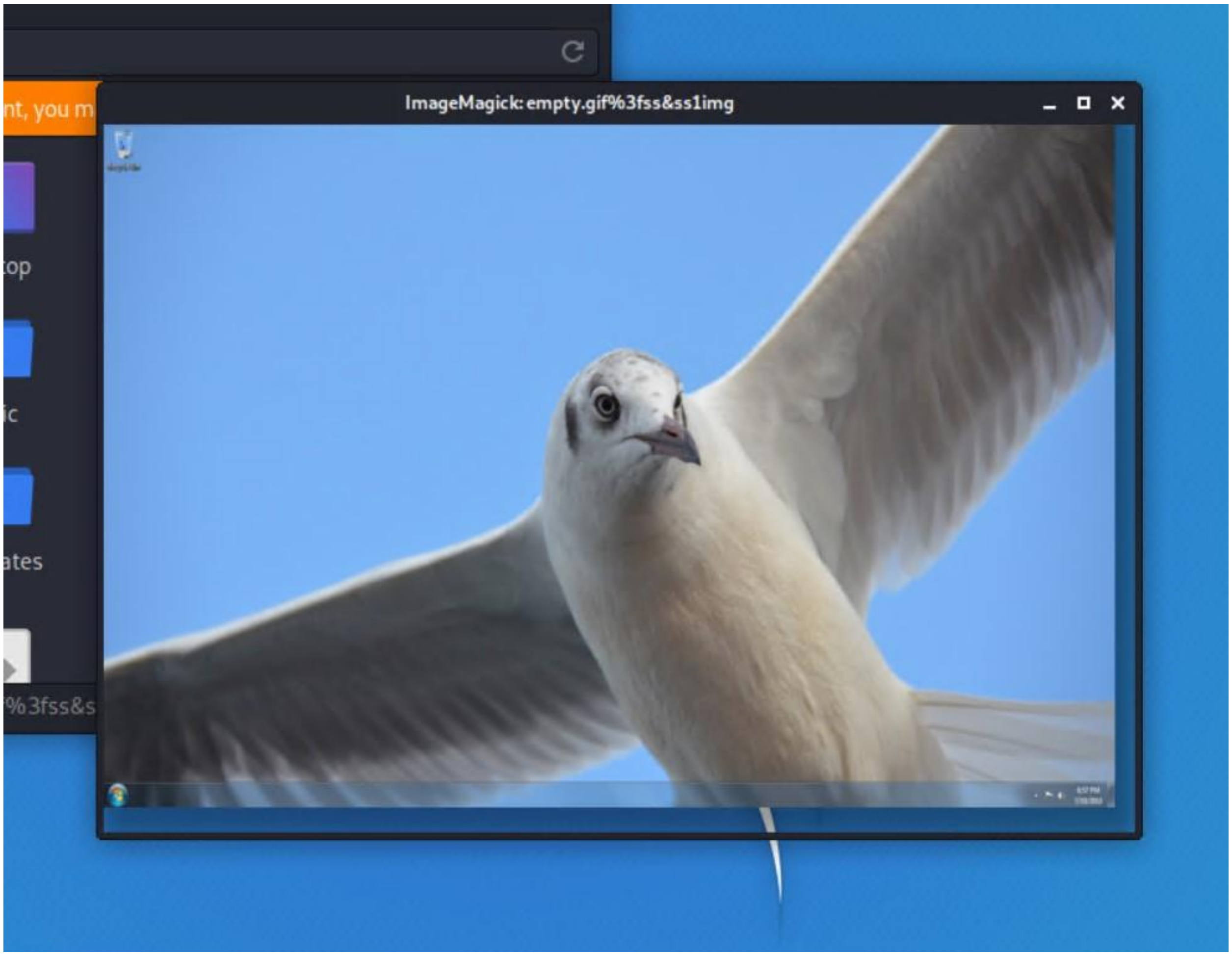
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A
172.16.4.205	185.243.115.84	30,344	26 M	15,149	9,831 k	15,195
166.62.111.64	172.16.4.205	15,728	16 M	11,354	15 M	4,374
10.0.0.201	23.43.62.169	6,934	7,045 k	2,282	124 k	4,652
10.0.0.201	64.187.66.143	4,883	3,637 k	2,235	144 k	2,648
5.101.51.151	10.6.12.203	4,326	4,246 k	3,262	4,177 k	1,064

Based on the Conversations statistics, as well as filtering the packets by highest amounts between IPs: **172.16.4.205, 185.243.115.84, and 166.62.111.64 are the infected traffic.**

There are a large number of POST methods for empty.gif being sent without any corresponding GET requests. This is odd and should flag the alerts.

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

   File > Export Objects > HTTP



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:

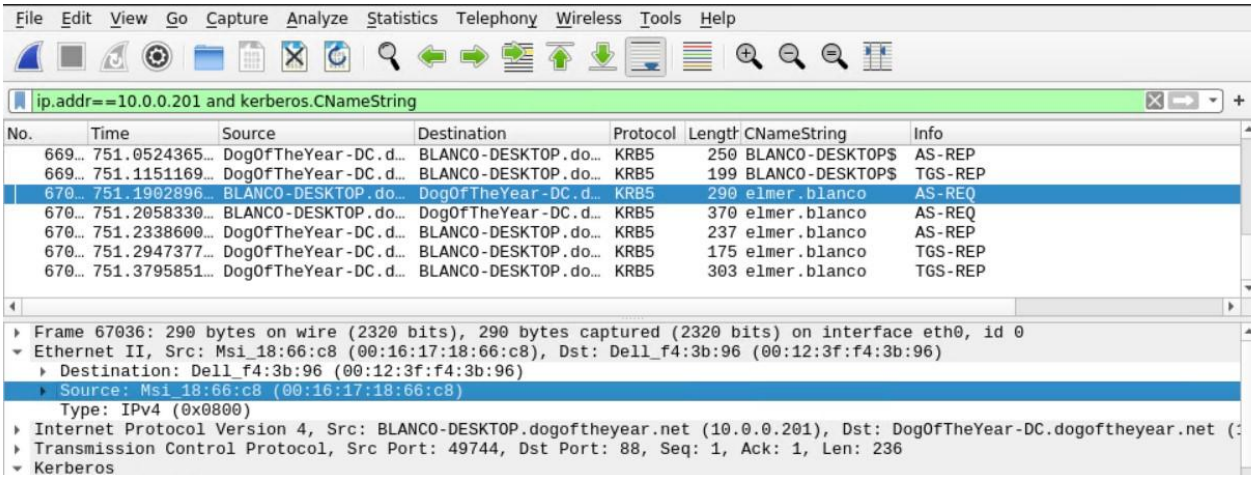
- The machines using torrents live in the range `10.0.0.0/24` and are clients of an AD domain.

- 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 (Host name): **BLANCO-DESKTOP**

Filter: ip.addr==10.0.0.201 and kerberos.CNameString



```
ip.addr==10.0.0.201 and kerberos.CNameString
```

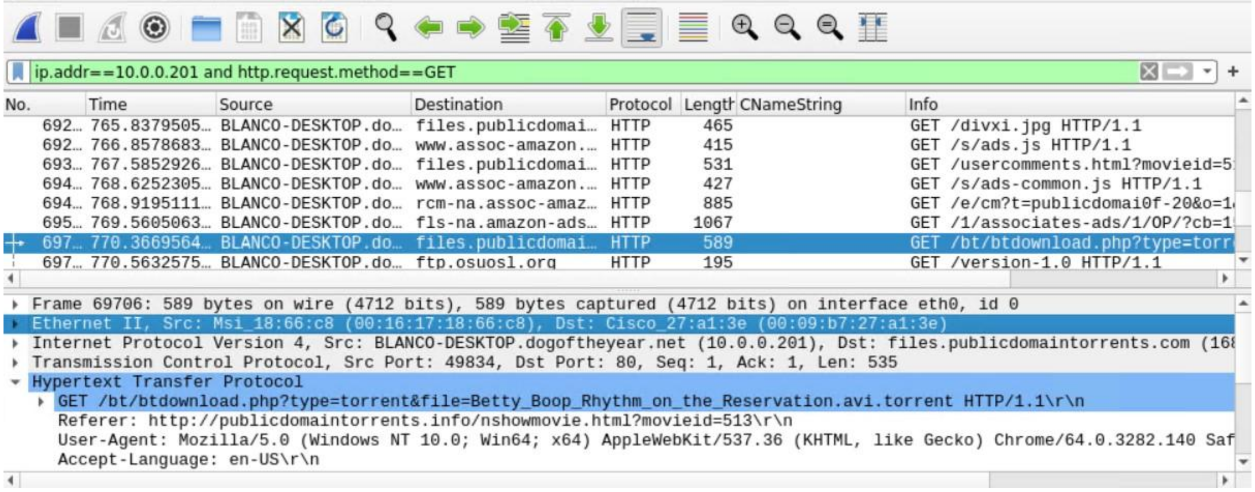
```
No.      Time           Source               Destination          Protocol  Length CNameString      Info
   669… 751.0524365… DogOfTheYear-DC.d… BLANCO-DESKTOP.do… KRB5       250 BLANCO-DESKTOP$  AS-REP
   669… 751.1151169… DogOfTheYear-DC.d… BLANCO-DESKTOP.do… KRB5       199 BLANCO-DESKTOP$  TGS-REP
   670… 751.1902896… BLANCO-DESKTOP.do… DogOfTheYear-DC.d… KRB5       290 elmer.blanco     AS-REQ
   670… 751.2058330… BLANCO-DESKTOP.do… DogOfTheYear-DC.d… KRB5       370 elmer.blanco     AS-REQ
   670… 751.2338600… DogOfTheYear-DC.d… BLANCO-DESKTOP.do… KRB5       237 elmer.blanco     AS-REP
   670… 751.2947377… DogOfTheYear-DC.d… BLANCO-DESKTOP.do… KRB5       175 elmer.blanco     TGS-REP
   670… 751.3795851… DogOfTheYear-DC.d… BLANCO-DESKTOP.do… KRB5       303 elmer.blanco     TGS-REP
```

```
▸ 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)
  ▸ Destination: Dell_f4:3b:96 (00:12:3f:f4:3b:96)
  ▸ Source: Msi_18:66:c8 (00:16:17:18:66:c8)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201), Dst: DogOfTheYear-DC.dogoftheyear.net (
▸ Transmission Control Protocol, Src Port: 49744, Dst Port: 88, Seq: 1, Ack: 1, Len: 236
▾ Kerberos
```

2. Which torrent file did the user download?

    Filter: ip.addr==10.0.0.201 and http.request.method==get

    The torrent file downloaded was:
    Betty_Boop_Rythm_on_the_Reservation.avi.torrent



ip.addr==10.0.0.201 and http.request.method==GET

No.	Time	Source	Destination	Protocol	Length	CNameString	Info
692…	765.8379505…	BLANCO-DESKTOP.do…	files.publicdomai…	HTTP	465		GET /divxi.jpg HTTP/1.1
692…	766.8578683…	BLANCO-DESKTOP.do…	www.assoc-amazon.…	HTTP	415		GET /s/ads.js HTTP/1.1
693…	767.5852926…	BLANCO-DESKTOP.do…	files.publicdomai…	HTTP	531		GET /usercomments.html?movieid=5
694…	768.6252305…	BLANCO-DESKTOP.do…	www.assoc-amazon.…	HTTP	427		GET /s/ads-common.js HTTP/1.1
694…	768.9195111…	BLANCO-DESKTOP.do…	rcm-na.assoc-amaz…	HTTP	885		GET /e/cm?t=publicdomai0f-20&o=1
695…	769.5605063…	BLANCO-DESKTOP.do…	fls-na.amazon-ads…	HTTP	1067		GET /1/associates-ads/1/OP/?cb=1
697…	770.3669564…	BLANCO-DESKTOP.do…	files.publicdomai…	HTTP	589		GET /bt/btdownload.php?type=torr
697…	770.5632575…	BLANCO-DESKTOP.do…	ftp.osuosl.org	HTTP	195		GET /version-1.0 HTTP/1.1

```
▸ Frame 69706: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits) on interface eth0, id 0
▸ Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
▸ Internet Protocol Version 4, Src: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201), Dst: files.publicdomaintorrents.com (16
▸ 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 Saf
    Accept-Language: en-US\r\n
```