

# 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:

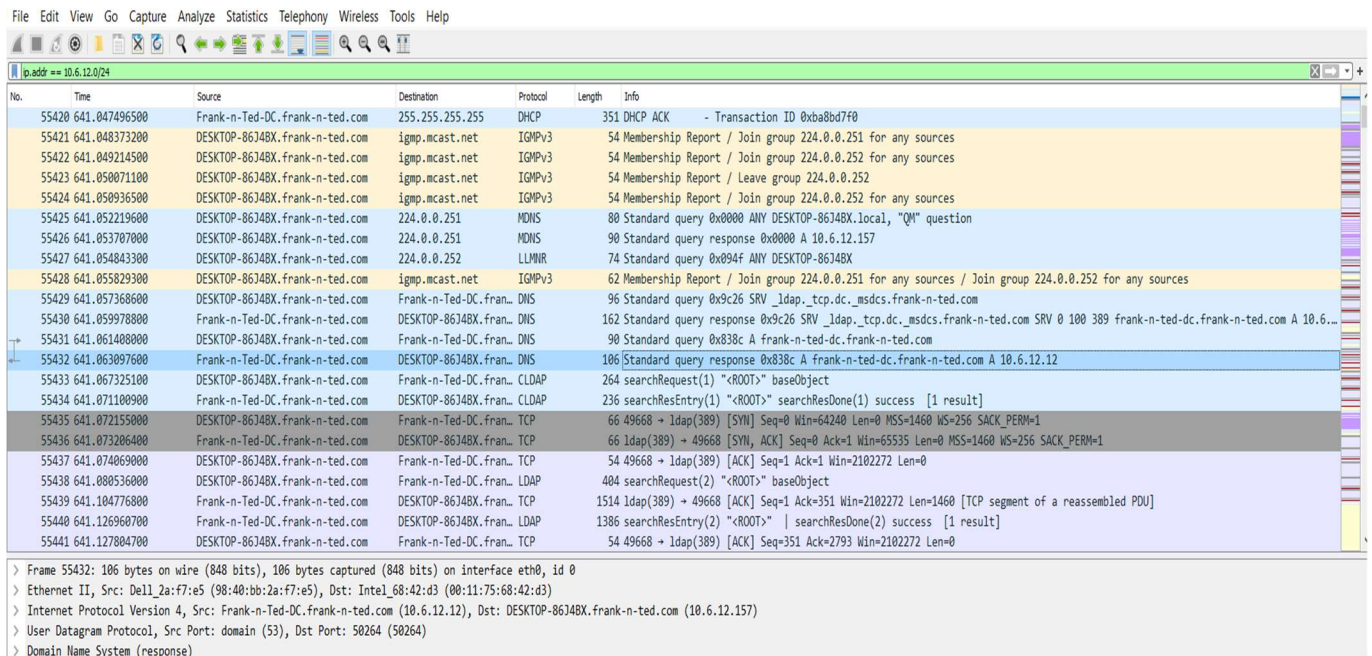
- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.
- Their IP addresses are somewhere in the range 10.6.12.0/24.

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-DC.frank-n-ted.com

Filter: ip.addr == 10.6.12.0/24



No.	Time	Source	Destination	Protocol	Length	Info
55420	641.047496500	Frank-n-Ted-DC.frank-n-ted.com	255.255.255.255	DHCP	351	DHCP ACK - Transaction ID 0xba8bd7f0
55421	641.048373200	DESKTOP-86J48X.frank-n-ted.com	igmp.mcast.net	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any sources
55422	641.049214500	DESKTOP-86J48X.frank-n-ted.com	igmp.mcast.net	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
55423	641.050071100	DESKTOP-86J48X.frank-n-ted.com	igmp.mcast.net	IGMPv3	54	Membership Report / Leave group 224.0.0.252
55424	641.050936500	DESKTOP-86J48X.frank-n-ted.com	igmp.mcast.net	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
55425	641.052219600	DESKTOP-86J48X.frank-n-ted.com	224.0.0.251	MDNS	80	Standard query 0x0000 ANY DESKTOP-86J48X.local, "QM" question
55426	641.053707000	DESKTOP-86J48X.frank-n-ted.com	224.0.0.251	MDNS	90	Standard query response 0x0000 A 10.6.12.157
55427	641.054843300	DESKTOP-86J48X.frank-n-ted.com	224.0.0.252	LLNMR	74	Standard query 0x094f ANY DESKTOP-86J48X
55428	641.055829300	DESKTOP-86J48X.frank-n-ted.com	igmp.mcast.net	IGMPv3	62	Membership Report / Join group 224.0.0.251 for any sources / Join group 224.0.0.252 for any sources
55429	641.057368600	DESKTOP-86J48X.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	DNS	96	Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
55430	641.059978800	Frank-n-Ted-DC.frank-n-ted.com	DESKTOP-86J48X.frank-n-ted.com	DNS	162	Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com SRV 0 100 389 frank-n-ted-dc.frank-n-ted.com A 10.6.12.157
55431	641.061408000	DESKTOP-86J48X.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	DNS	90	Standard query 0x838c A frank-n-ted-dc.frank-n-ted.com
55432	641.063897600	Frank-n-Ted-DC.frank-n-ted.com	DESKTOP-86J48X.frank-n-ted.com	DNS	106	Standard query response 0x838c A frank-n-ted-dc.frank-n-ted.com A 10.6.12.12
55433	641.067325100	DESKTOP-86J48X.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	LDAP	264	searchRequest(1) "<ROOT>" baseObject
55434	641.071100900	Frank-n-Ted-DC.frank-n-ted.com	DESKTOP-86J48X.frank-n-ted.com	LDAP	236	searchResEntry(1) "<ROOT>" searchResDone(1) success [1 result]
55435	641.072155000	DESKTOP-86J48X.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	TCP	66	49668 → 49668 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
55436	641.073206400	Frank-n-Ted-DC.frank-n-ted.com	DESKTOP-86J48X.frank-n-ted.com	TCP	66	49668 → 49668 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
55437	641.074069000	DESKTOP-86J48X.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	TCP	54	49668 → 49668 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
55438	641.080536000	DESKTOP-86J48X.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	LDAP	404	searchRequest(2) "<ROOT>" baseObject
55439	641.104776800	Frank-n-Ted-DC.frank-n-ted.com	DESKTOP-86J48X.frank-n-ted.com	TCP	1514	49668 → 49668 [ACK] Seq=1 Ack=351 Win=2102272 Len=1460 [TCP segment of a reassembled PDU]
55440	641.126960700	Frank-n-Ted-DC.frank-n-ted.com	DESKTOP-86J48X.frank-n-ted.com	LDAP	1386	searchResEntry(2) "<ROOT>"   searchResDone(2) success [1 result]
55441	641.127804700	DESKTOP-86J48X.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	TCP	54	49668 → 49668 [ACK] Seq=351 Ack=2793 Win=2102272 Len=0

> Frame 55432: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface eth0, id 0  
> Ethernet II, Src: Dell\_2a:f7:e5 (98:40:bb:2a:f7:e5), Dst: Intel\_68:42:d3 (00:11:75:68:42:d3)  
> Internet Protocol Version 4, Src: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12), Dst: DESKTOP-86J48X.frank-n-ted.com (10.6.12.157)  
> User Datagram Protocol, Src Port: domain (53), Dst Port: 50264 (50264)  
> Domain Name System (response)

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

10.6.12.12

Filter: ip.addr == 10.6.12.0/24

No.	Time	Source	Destination	Protocol	Length	Info
55420	641.047496500	Frank-n-Ted-DC.frank-n-ted.com	255.255.255.255	DHCP	351	DHCP ACK - Transaction ID 0xba8bd7f0
55421	641.048373200	DESKTOP-86J4BX.frank-n-ted.com	igmp.mcast.net	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any sources
55422	641.049214500	DESKTOP-86J4BX.frank-n-ted.com	igmp.mcast.net	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
55423	641.050071100	DESKTOP-86J4BX.frank-n-ted.com	igmp.mcast.net	IGMPv3	54	Membership Report / Leave group 224.0.0.252
55424	641.050936500	DESKTOP-86J4BX.frank-n-ted.com	igmp.mcast.net	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
55425	641.052219600	DESKTOP-86J4BX.frank-n-ted.com	224.0.0.251	MDNS	80	Standard query 0x0000 ANY DESKTOP-86J4BX.local, "QM" question
55426	641.053707000	DESKTOP-86J4BX.frank-n-ted.com	224.0.0.251	MDNS	90	Standard query response 0x0000 A 10.6.12.157
55427	641.054843300	DESKTOP-86J4BX.frank-n-ted.com	224.0.0.252	LLNMR	74	Standard query 0x094f ANY DESKTOP-86J4BX
55428	641.055829300	DESKTOP-86J4BX.frank-n-ted.com	igmp.mcast.net	IGMPv3	62	Membership Report / Join group 224.0.0.251 for any sources / Join group 224.0.0.252 for any sources
55429	641.057368600	DESKTOP-86J4BX.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	DNS	96	Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
55430	641.059978800	Frank-n-Ted-DC.frank-n-ted.com	DESKTOP-86J4BX.frank-n-ted.com	DNS	162	Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com SRV 0 100 389 frank-n-ted-dc.frank-n-ted.com A 10.6.12.12
55431	641.061408000	DESKTOP-86J4BX.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	DNS	90	Standard query 0x838c A frank-n-ted-dc.frank-n-ted.com
55432	641.063097600	Frank-n-Ted-DC.frank-n-ted.com	DESKTOP-86J4BX.frank-n-ted.com	DNS	106	Standard query response 0x838c A frank-n-ted-dc.frank-n-ted.com A 10.6.12.12
55433	641.067325100	DESKTOP-86J4BX.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	LDAP	264	searchRequest(1) "<root>" baseObject
55434	641.071100900	Frank-n-Ted-DC.frank-n-ted.com	DESKTOP-86J4BX.frank-n-ted.com	LDAP	236	searchResEntry(1) "<root>" searchResDone(1) success [1 result]
55435	641.072155000	DESKTOP-86J4BX.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	TCP	66	49668 → 1dap(389) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
55436	641.073206400	Frank-n-Ted-DC.frank-n-ted.com	DESKTOP-86J4BX.frank-n-ted.com	TCP	66	1dap(389) → 49668 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
55437	641.074069000	DESKTOP-86J4BX.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	TCP	54	49668 → 1dap(389) [ACK] Seq=1 Ack=1 Win=2102272 Len=0
55438	641.080536000	Frank-n-Ted-DC.frank-n-ted.com	DESKTOP-86J4BX.frank-n-ted.com	LDAP	404	searchRequest(2) "<root>" baseObject
55439	641.104776800	Frank-n-Ted-DC.frank-n-ted.com	DESKTOP-86J4BX.frank-n-ted.com	TCP	1514	1dap(389) → 49668 [ACK] Seq=1 Ack=351 Win=2102272 Len=1460 [TCP segment of a reassembled PDU]
55440	641.126960700	Frank-n-Ted-DC.frank-n-ted.com	DESKTOP-86J4BX.frank-n-ted.com	LDAP	1386	searchResEntry(2) "<root>"   searchResDone(2) success [1 result]
55441	641.127804700	DESKTOP-86J4BX.frank-n-ted.com	Frank-n-Ted-DC.frank-n-ted.com	TCP	54	49668 → 1dap(389) [ACK] Seq=351 Ack=2793 Win=2102272 Len=0

> 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)  
> User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)  
> Dynamic Host Configuration Protocol (ACK)

## 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

No.	Time	Source	Destination	Protocol	Length	Info
58748	658.621258400	LAPTOP-SWKHX9YG.frank-n-ted.com	205.185.125.104	HTTP	275	GET /pQ8tWj HTTP/1.1
58752	658.636633700	LAPTOP-SWKHX9YG.frank-n-ted.com	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-SWKHX9YG.frank-n-ted.com (10.6.12.203), Dst: 205.185.125.104 (205.185.125.104)  
> Transmission Control Protocol, Src Port: 49739 (49739), Dst Port: http (80), Seq: 222, Ack: 489, Len: 258  
> Hypertext Transfer Protocol

4. Upload the file to [VirusTotal.com](https://www.virustotal.com). What kind of malware is this classified as?

Trojan

## Vulnerable Windows Machines

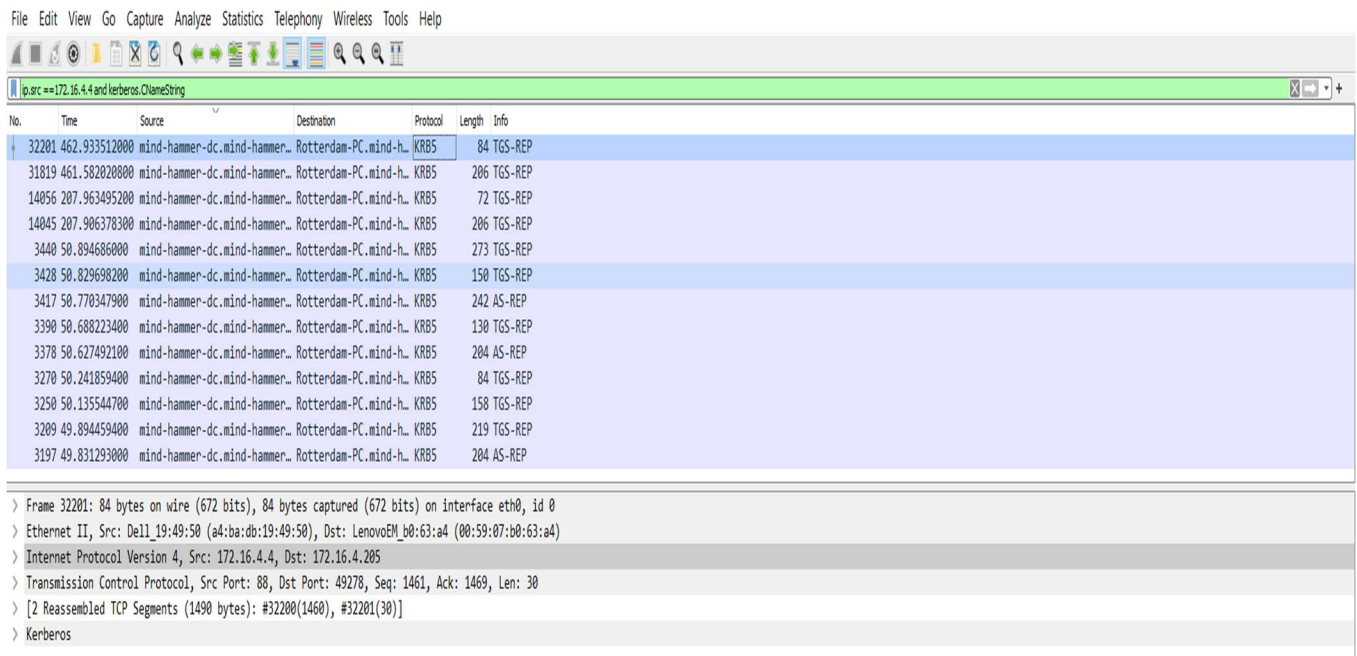
The Security team received reports of an infected Windows host on the network. They know the following:

- 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



The image shows a Wireshark packet capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The packet list pane shows a series of packets, with packet 32201 selected. The packet details pane shows the following information:

No.	Time	Source	Destination	Protocol	Length	Info
32201	462.933512000	mind-hammer-dc.mind-hammer..	Rotterdam-PC.mind-h..	KRB5	84	TGS-REP
31819	461.582020000	mind-hammer-dc.mind-hammer..	Rotterdam-PC.mind-h..	KRB5	206	TGS-REP
14056	207.963495200	mind-hammer-dc.mind-hammer..	Rotterdam-PC.mind-h..	KRB5	72	TGS-REP
14045	207.906378300	mind-hammer-dc.mind-hammer..	Rotterdam-PC.mind-h..	KRB5	206	TGS-REP
3440	50.894686000	mind-hammer-dc.mind-hammer..	Rotterdam-PC.mind-h..	KRB5	273	TGS-REP
3428	50.829698200	mind-hammer-dc.mind-hammer..	Rotterdam-PC.mind-h..	KRB5	150	TGS-REP
3417	50.770347900	mind-hammer-dc.mind-hammer..	Rotterdam-PC.mind-h..	KRB5	242	AS-REP
3390	50.688223400	mind-hammer-dc.mind-hammer..	Rotterdam-PC.mind-h..	KRB5	130	TGS-REP
3378	50.627492100	mind-hammer-dc.mind-hammer..	Rotterdam-PC.mind-h..	KRB5	204	AS-REP
3270	50.241859400	mind-hammer-dc.mind-hammer..	Rotterdam-PC.mind-h..	KRB5	84	TGS-REP
3250	50.135544700	mind-hammer-dc.mind-hammer..	Rotterdam-PC.mind-h..	KRB5	158	TGS-REP
3209	49.894459400	mind-hammer-dc.mind-hammer..	Rotterdam-PC.mind-h..	KRB5	219	TGS-REP
3197	49.831293000	mind-hammer-dc.mind-hammer..	Rotterdam-PC.mind-h..	KRB5	204	AS-REP

The packet details pane for packet 32201 shows the following information:

- > Frame 32201: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface eth0, id 0
- > Ethernet II, Src: Dell\_19:49:50 (a4:ba:db:19:49:50), Dst: LenovoEM\_b0:63:a4 (00:59:07:b0:63:a4)
- > Internet Protocol Version 4, Src: 172.16.4.4, Dst: 172.16.4.205
- > Transmission Control Protocol, Src Port: 88, Dst Port: 49278, Seq: 1461, Ack: 1469, Len: 30
- > [2 Reassembled TCP Segments (1490 bytes): #32200(1460), #32201(30)]
- > Kerberos

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

matthijs.devries



ip.src == 172.16.4.205 and kerberos.CNameString

No.	Time	Source	Destination	Protocol	Length	Info
3415	50.742235400	Rotterdam-PC.mind-hammer.n...	mind-hammer-dc.mind...	KRB5	372	AS-REQ
3408	50.726684900	Rotterdam-PC.mind-hammer.n...	mind-hammer-dc.mind...	KRB5	292	AS-REQ
3376	50.599992500	Rotterdam-PC.mind-hammer.n...	mind-hammer-dc.mind...	KRB5	381	AS-REQ
3369	50.584361200	Rotterdam-PC.mind-hammer.n...	mind-hammer-dc.mind...	KRB5	301	AS-REQ
3195	49.803720100	Rotterdam-PC.mind-hammer.n...	mind-hammer-dc.mind...	KRB5	377	AS-REQ
3187	49.786544600	Rotterdam-PC.mind-hammer.n...	mind-hammer-dc.mind...	KRB5	297	AS-REQ

```

.... ..0. = unused22: False
.... ...0 = unused23: False
0... .... = unused24: False
.0.. .... = unused25: False
..0. .... = disable-transited-check: False
...1 .... = renewable-ok: True
.... 0... = enc-tkt-in-skey: False
.... .0.. = unused29: False
.... ..0. = renew: False
.... ...0 = validate: False
v cname
  name-type: kRB5-NT-PRINCIPAL (1)
  v 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>

```

```

0080 fe eb 31 e9 f9 65 4b 8c e9 35 b7 b8 d1 e6 58 0c ..1..eK. .5....X.
0090 ba 78 7a e6 fc c9 1c 51 25 cf 9d 89 3f 3b 30 11 .xz....Q %...?;0.
00a0 a1 04 02 02 00 80 a2 09 04 07 30 05 a0 03 01 01 ..... ..0.....
00b0 ff a4 81 c0 30 81 bd a0 07 03 05 00 40 81 00 10 ....0... ..@...
00c0 a1 1d 30 1b a0 03 02 01 01 a1 14 30 12 1b 10 6d ..0..... ..0...m
00d0 61 74 74 68 69 6a 73 2e 64 65 76 72 69 65 73 atthijs. devries.
00e0 0d 1b 0b 4d 49 4e 44 2d 48 41 4d 4d 45 52 a3 20 ...MIND- HAMMER.
00f0 30 1e a0 03 02 01 02 a1 17 30 15 1b 06 6b 72 62 0..... .0...krb
0100 74 67 74 1b 0b 4d 49 4e 44 2d 48 41 4d 4d 45 52 tgt..MIN D-HAMMER
0110 a5 11 18 0f 32 30 33 37 30 39 31 33 30 32 34 38 ....2037 09130248
0120 30 35 5a a6 11 18 0f 32 30 33 37 30 39 31 33 30 05Z....2 03709130
0130 32 34 38 30 35 5a a7 06 02 04 25 a0 57 52 a8 15 24805Z.. ..%.WR..
0140 30 13 02 01 12 02 01 11 02 01 17 02 01 18 02 02 0.....
0150 ff 79 02 01 03 a9 1d 30 1b 30 19 a0 03 02 01 14 .y.....0 .0.....
0160 a1 12 04 10 52 4f 54 54 45 52 44 41 4d 2d 50 43 ....ROTT ERDAM-PC
0170 20 20 20 20

```

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

172.16.4.205, 185.243.115.84, 166.62.11.64 are the infected traffic.

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

# 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: Windows 10
2. Which torrent file did the user download?

Betty\_Boop\_Rythm\_on\_the\_Reservation.avi.torrent

Filter: ip.addr == 10.0.0.201 and http.request.method == GET or ip.addr == 10.0.0.201 and (http.request.uri contains ".torrent")