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:

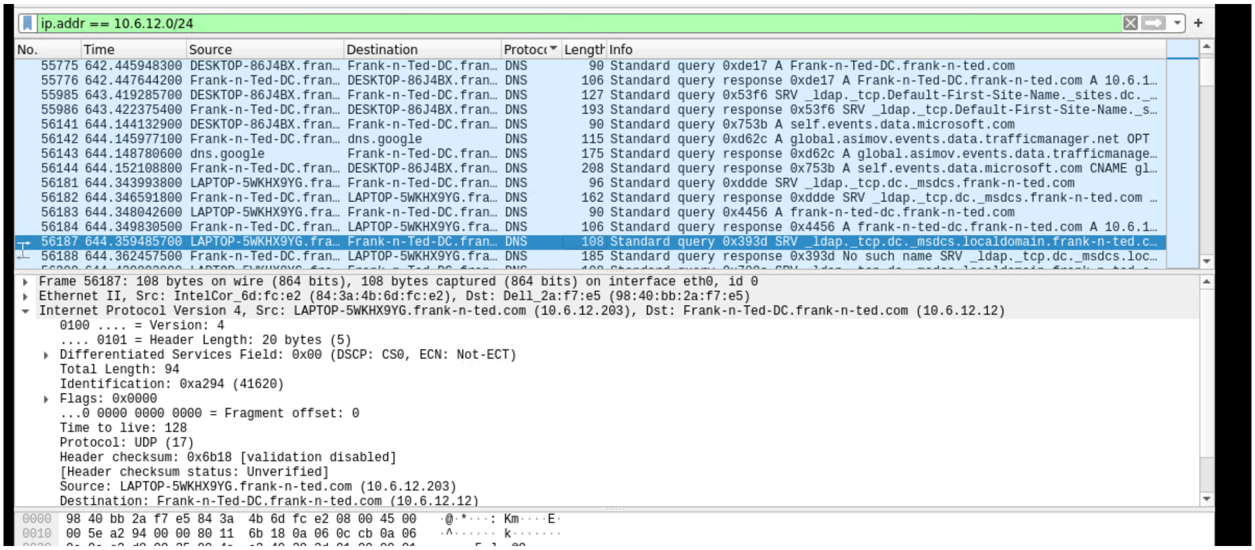
- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.
- Their IP addresses are somewhere in the range `10.6.12.0/24`.

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

   ip.addr==10.6.12.0/24



```
ip.addr == 10.6.12.0/24
```

```
No.   Time          Source              Destination         Protocol Length Info
55775 642.445948300 DESKTOP-86J4BX.fran… Frank-n-Ted-DC.fran… DNS    90 Standard query 0xde17 A Frank-n-Ted-DC.frank-n-ted.com
55776 642.447644200 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.fran… DNS   106 Standard query response 0xde17 A Frank-n-Ted-DC.frank-n-ted.com A 10.6.1…
55985 643.419285700 DESKTOP-86J4BX.fran… Frank-n-Ted-DC.fran… DNS   127 Standard query 0x53f6 SRV _ldap._tcp.Default-First-Site-Name._sites.dc._…
55986 643.422375400 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.fran… DNS   193 Standard query response 0x53f6 SRV _ldap._tcp.Default-First-Site-Name._s…
56141 644.144132900 DESKTOP-86J4BX.fran… Frank-n-Ted-DC.fran… DNS    90 Standard query 0x753b A self.events.data.microsoft.com
56142 644.145977100 Frank-n-Ted-DC.fran… dns.google          DNS   115 Standard query 0xd62c A global.asimov.events.data.trafficmanager.net OPT
56143 644.148780600 dns.google          Frank-n-Ted-DC.fran… DNS   175 Standard query response 0xd62c A global.asimov.events.data.trafficmanage…
56144 644.152108800 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.fran… DNS   208 Standard query response 0x753b A self.events.data.microsoft.com CNAME gl…
56181 644.343993800 LAPTOP-5WKHX9YG.fra… Frank-n-Ted-DC.fran… DNS    96 Standard query 0xddde SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
56182 644.346591800 Frank-n-Ted-DC.fran… LAPTOP-5WKHX9YG.fra… DNS   162 Standard query response 0xddde SRV _ldap._tcp.dc._msdcs.frank-n-ted.com …
56183 644.348042600 LAPTOP-5WKHX9YG.fra… Frank-n-Ted-DC.fran… DNS    90 Standard query 0x4456 A frank-n-ted-dc.frank-n-ted.com
56184 644.349830500 Frank-n-Ted-DC.fran… LAPTOP-5WKHX9YG.fra… DNS   106 Standard query response 0x4456 A frank-n-ted-dc.frank-n-ted.com A 10.6.1…
56187 644.359485700 LAPTOP-5WKHX9YG.fra… Frank-n-Ted-DC.fran… DNS   108 Standard query 0x393d SRV _ldap._tcp.dc._msdcs.localdomain.frank-n-ted.c…
56188 644.362457500 Frank-n-Ted-DC.fran… LAPTOP-5WKHX9YG.fra… DNS   185 Standard query response 0x393d No such name SRV _ldap._tcp.dc._msdcs.loc…
```

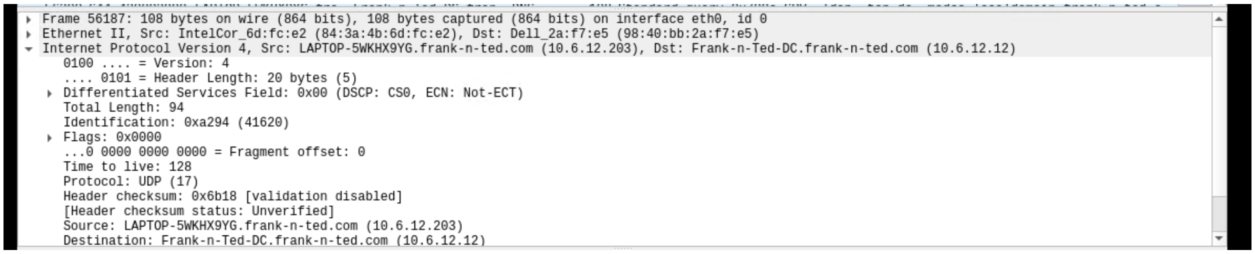
```
▸ Frame 56187: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface eth0, id 0
▸ Ethernet II, Src: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2), Dst: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5)
▾ Internet Protocol Version 4, Src: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203), Dst: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 94
    Identification: 0xa294 (41620)
  ▸ Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x6b18 [validation disabled]
    [Header checksum status: Unverified]
    Source: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203)
    Destination: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12)
```

```
0000  98 40 bb 2a f7 e5 84 3a  4b 6d fc e2 08 00 45 00   ·@·*···: Km····E·
0010  00 5e a2 94 00 00 80 11  6b 18 0a 06 0c cb 0a 06   ·^······ k·······
```

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

   10.6.12.12

ip.src==10.6.12.0/24

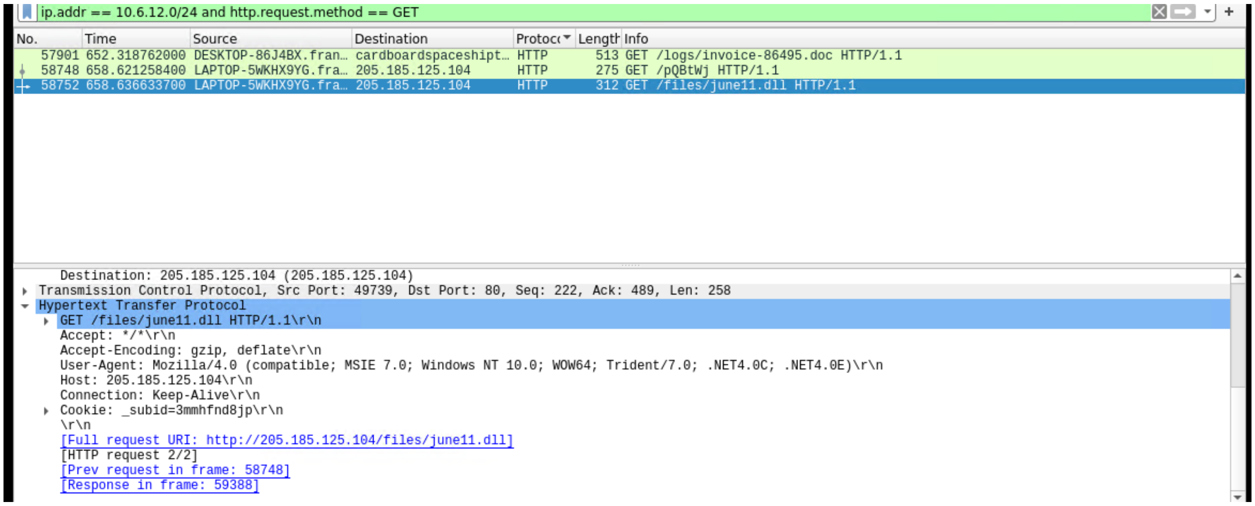


```
▸ Frame 56187: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface eth0, id 0
▸ Ethernet II, Src: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2), Dst: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5)
▾ Internet Protocol Version 4, Src: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203), Dst: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12)
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 94
     Identification: 0xa294 (41620)
   ▸ Flags: 0x0000
     ...0 0000 0000 0000 = Fragment offset: 0
     Time to live: 128
     Protocol: UDP (17)
     Header checksum: 0x6b18 [validation disabled]
     [Header checksum status: Unverified]
     Source: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203)
     Destination: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12)
```

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.

   ip.addr==10.6.12.0/24 and http.request.method == GET

   Malware name - june11.d11

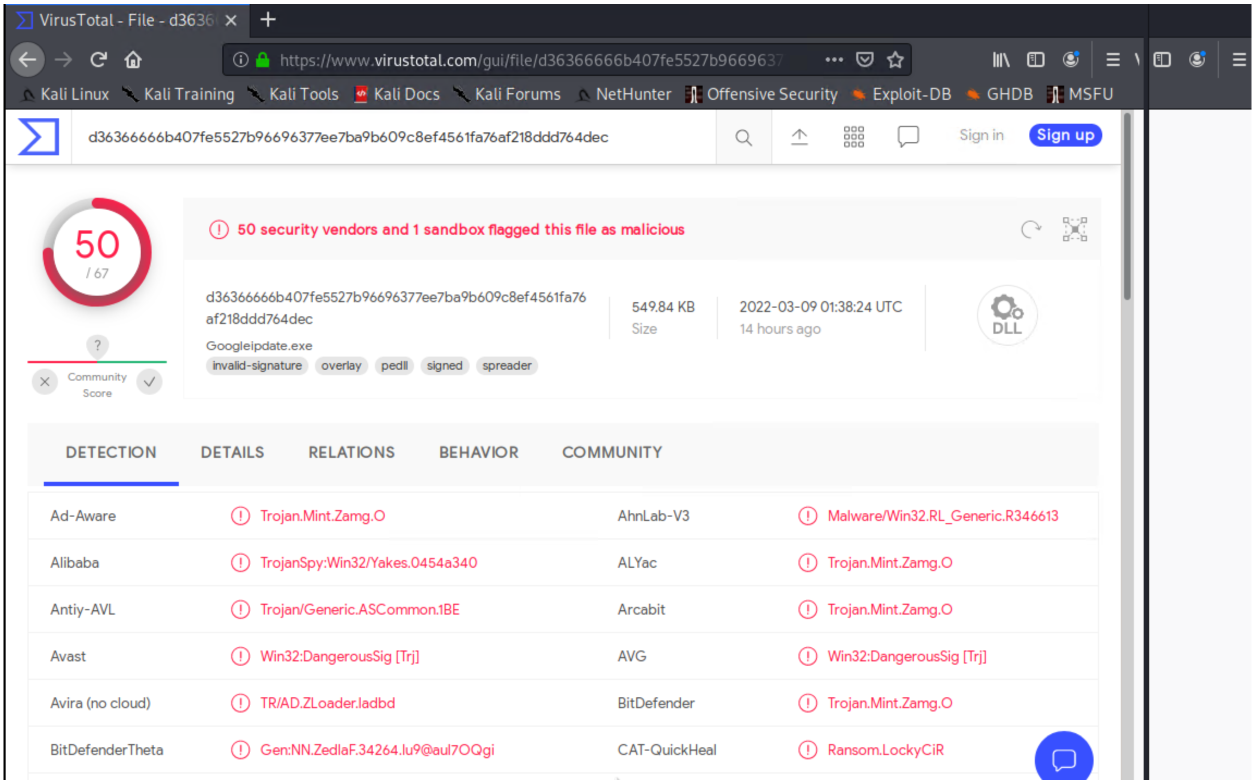


```
ip.addr == 10.6.12.0/24 and http.request.method == GET

No.    Time            Source                Destination              Protoc Length Info
 57901 652.318762000  DESKTOP-86J4BX.fran…  cardboardspaceshipt…  HTTP      513 GET /logs/invoice-86495.doc HTTP/1.1
 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
```

```
     Destination: 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]
     [Prev request in frame: 58748]
     [Response in frame: 59388]
```

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

   Trojan.Mint.Zamg.O


VirusTotal - File - d3636
https://www.virustotal.com/gui/file/d36366666b407fe5527b9669637
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec
Sign in
Sign up
50
/ 67
?
Community Score
DLL

50 security vendors and 1 sandbox flagged this file as malicious

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Googleipdate.exe

invalid-signature overlay pedll signed spreader

549.84 KB
Size

2022-03-09 01:38:24 UTC
14 hours ago

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

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.34264.lu9@aul7OQgi	CAT-QuickHeal	ⓘ Ransom.LockyCiR

Vulnerable Windows Machines

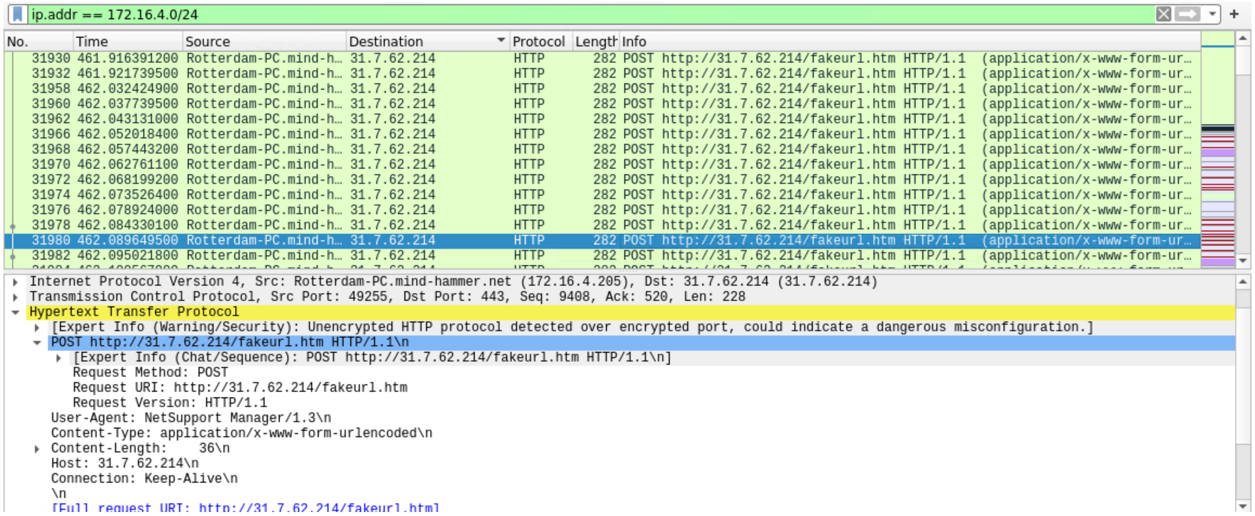
The Security team received reports of an infected Windows host on the network. They know the following:

- 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.mid-hammer.net
   - IP address: 172.16.4.205
   - MAC address: 00:59:07:b0:63:a4

- ○ Ip.addr == 172.16.4.0/24



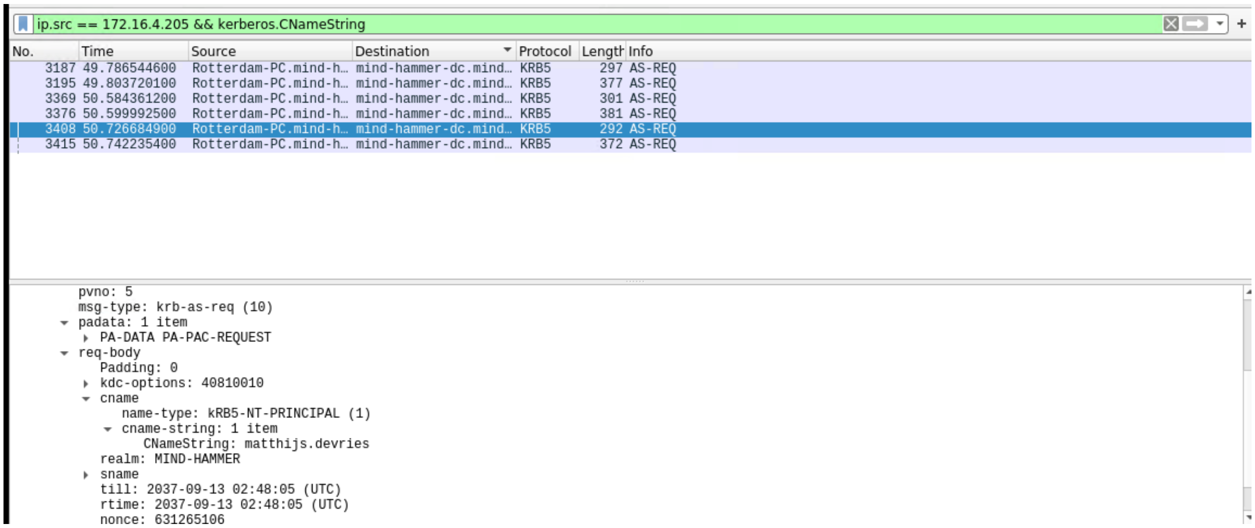
```
ip.addr == 172.16.4.0/24

No.   Time          Source                 Destination    Protocol Length Info
31930 461.916391200 Rotterdam-PC.mind-h…  31.7.62.214    HTTP        282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-form-ur…
31932 461.921739500 Rotterdam-PC.mind-h…  31.7.62.214    HTTP        282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-form-ur…
31958 462.032424900 Rotterdam-PC.mind-h…  31.7.62.214    HTTP        282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-form-ur…
31960 462.037739500 Rotterdam-PC.mind-h…  31.7.62.214    HTTP        282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-form-ur…
31962 462.043131000 Rotterdam-PC.mind-h…  31.7.62.214    HTTP        282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-form-ur…
31966 462.052018400 Rotterdam-PC.mind-h…  31.7.62.214    HTTP        282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-form-ur…
31968 462.057443200 Rotterdam-PC.mind-h…  31.7.62.214    HTTP        282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-form-ur…
31970 462.062761100 Rotterdam-PC.mind-h…  31.7.62.214    HTTP        282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-form-ur…
31972 462.068199200 Rotterdam-PC.mind-h…  31.7.62.214    HTTP        282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-form-ur…
31974 462.073526400 Rotterdam-PC.mind-h…  31.7.62.214    HTTP        282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-form-ur…
31976 462.078924000 Rotterdam-PC.mind-h…  31.7.62.214    HTTP        282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-form-ur…
31978 462.084330100 Rotterdam-PC.mind-h…  31.7.62.214    HTTP        282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-form-ur…
31980 462.089649500 Rotterdam-PC.mind-h…  31.7.62.214    HTTP        282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-form-ur…
31982 462.095021800 Rotterdam-PC.mind-h…  31.7.62.214    HTTP        282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-form-ur…
```

```
▸ Internet Protocol Version 4, Src: Rotterdam-PC.mind-hammer.net (172.16.4.205), Dst: 31.7.62.214 (31.7.62.214)
▸ Transmission Control Protocol, Src Port: 49255, Dst Port: 443, Seq: 9408, Ack: 520, Len: 228
▾ Hypertext Transfer Protocol
  ▸ [Expert Info (Warning/Security): Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous misconfiguration.]
  ▾ POST http://31.7.62.214/fakeurl.htm HTTP/1.1\n
    ▸ [Expert Info (Chat/Sequence): POST http://31.7.62.214/fakeurl.htm HTTP/1.1\n]
      Request Method: POST
      Request URI: http://31.7.62.214/fakeurl.htm
      Request Version: HTTP/1.1
    User-Agent: NetSupport Manager/1.3\n
    Content-Type: application/x-www-form-urlencoded\n
  ▸ Content-Length:    36\n
    Host: 31.7.62.214\n
    Connection: Keep-Alive\n
    \n
    [Full request URI: http://31.7.62.214/fakeurl.htm]
```

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

   matthijs.devries

   Ip.src == 172.16.4.205 && kerberos.CNameString



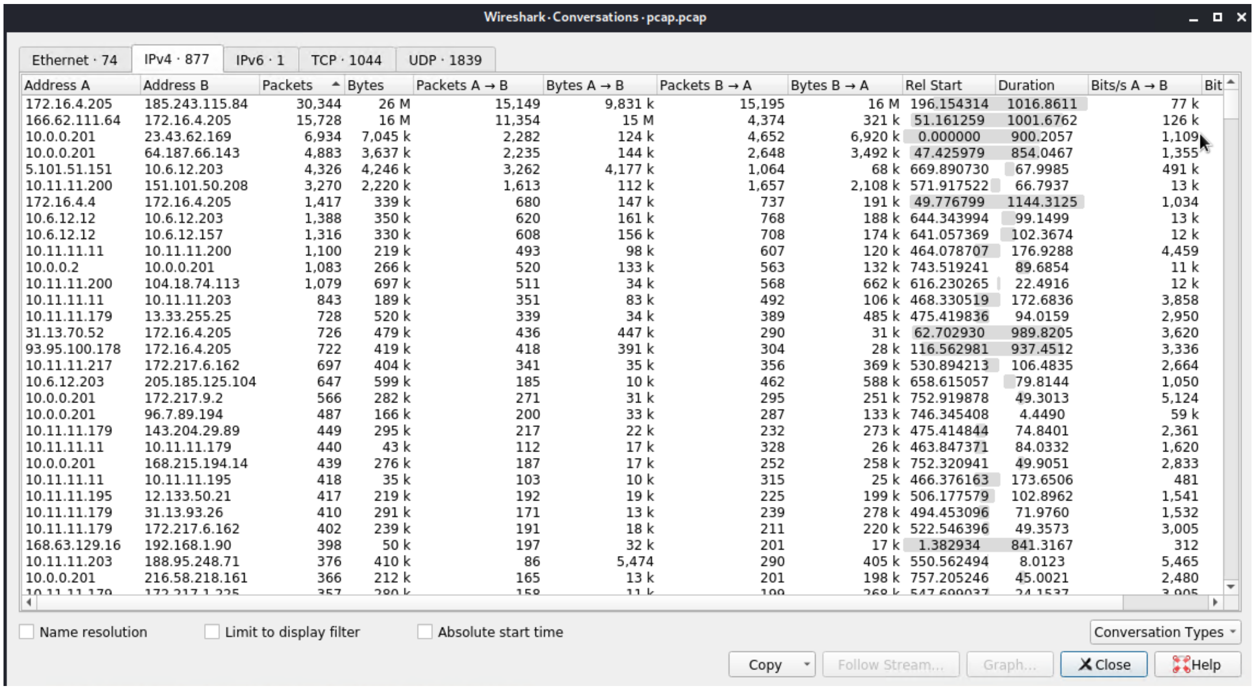
```
ip.src == 172.16.4.205 && kerberos.CNameString

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

```
      pvno: 5
      msg-type: krb-as-req (10)
    ▾ padata: 1 item
      ▸ PA-DATA PA-PAC-REQUEST
    ▾ req-body
        Padding: 0
      ▸ kdc-options: 40810010
      ▾ 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
```

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

   Ip.src == 172.16.4.205 && kerberos.CNameString

I found it in the 'statistics' tab. After which go to the 'conversations' tab. 172.16.4.205, 185.243.115.84, 23.43.62.169, and 64.187.66.143. Then go to the IPv4 tab and sort the packets from high to low.



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bit
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	77 k	
166.62.111.64	172.16.4.205	15,728	16 M	11,354	15 M	4,374	321 k	51.161259	1001.6762	126 k	
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	1,109	
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	1,355	
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	491 k	
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	13 k	
172.16.4.4	172.16.4.205	1,417	339 k	680	147 k	737	191 k	49.776799	1144.3125	1,034	
10.6.12.12	10.6.12.203	1,388	350 k	620	161 k	768	188 k	644.343994	99.1499	13 k	
10.6.12.12	10.6.12.157	1,316	330 k	608	156 k	708	174 k	641.057369	102.3674	12 k	
10.11.11.11	10.11.11.200	1,100	219 k	493	98 k	607	120 k	464.078707	176.9288	4,459	
10.0.0.2	10.0.0.201	1,083	266 k	520	133 k	563	132 k	743.519241	89.6854	11 k	
10.11.11.200	104.18.74.113	1,079	697 k	511	34 k	568	662 k	616.230265	22.4916	12 k	
10.11.11.11	10.11.11.203	843	189 k	351	83 k	492	106 k	468.330519	172.6836	3,858	
10.11.11.179	13.33.255.25	728	520 k	339	34 k	389	485 k	475.419836	94.0159	2,950	
31.13.70.52	172.16.4.205	726	479 k	436	447 k	290	31 k	62.702930	989.8205	3,620	
93.95.100.178	172.16.4.205	722	419 k	418	391 k	304	28 k	116.562981	937.4512	3,336	
10.11.11.217	172.217.6.162	697	404 k	341	35 k	356	369 k	530.894213	106.4835	2,664	
10.6.12.203	205.185.125.104	647	599 k	185	10 k	462	588 k	658.615057	79.8144	1,050	
10.0.0.201	172.217.9.2	566	282 k	271	31 k	295	251 k	752.919878	49.3013	5,124	
10.0.0.201	96.7.89.194	487	166 k	200	33 k	287	133 k	746.345408	4.4490	59 k	
10.11.11.179	143.204.29.89	449	295 k	217	22 k	232	273 k	475.414844	74.8401	2,361	
10.11.11.11	10.11.11.179	440	43 k	112	17 k	328	26 k	463.847371	84.0332	1,620	
10.0.0.201	168.215.194.14	439	276 k	187	17 k	252	258 k	752.320941	49.9051	2,833	
10.11.11.11	10.11.11.195	418	35 k	103	10 k	315	25 k	466.376163	173.6506	481	
10.11.11.195	12.133.50.21	417	219 k	192	19 k	225	199 k	506.177579	102.8962	1,541	
10.11.11.179	31.13.93.26	410	291 k	171	13 k	239	278 k	494.453096	71.9760	1,532	
10.11.11.179	172.217.6.162	402	239 k	191	18 k	211	220 k	522.546396	49.3573	3,005	
168.63.129.16	192.168.1.90	398	50 k	197	32 k	201	17 k	1.382934	841.3167	312	
10.11.11.203	188.95.248.71	376	410 k	86	5,474	290	405 k	550.562494	8.0123	5,465	
10.0.0.201	216.58.218.161	366	212 k	165	13 k	201	198 k	757.205246	45.0021	2,480	
10.11.11.179	172.217.1.225	357	280 k	158	11 k	199	268 k	547.699037	24.1537	3,905	

□ Name resolution □ Limit to display filter □ Absolute start time

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

Illegal Downloads

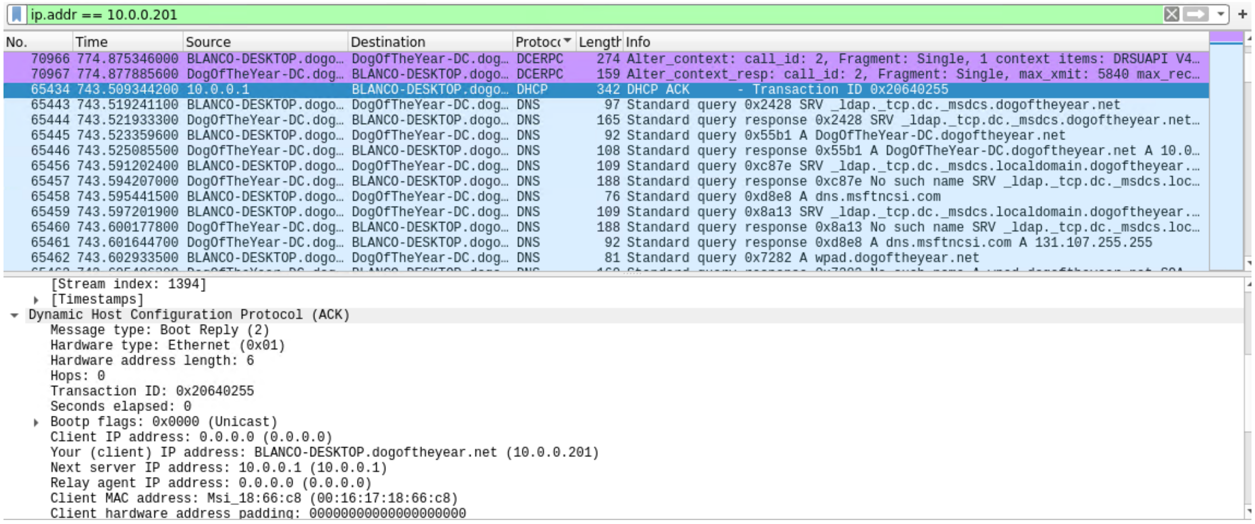
IT was informed that some users are torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringement.

IT shared the following about the torrent activity:

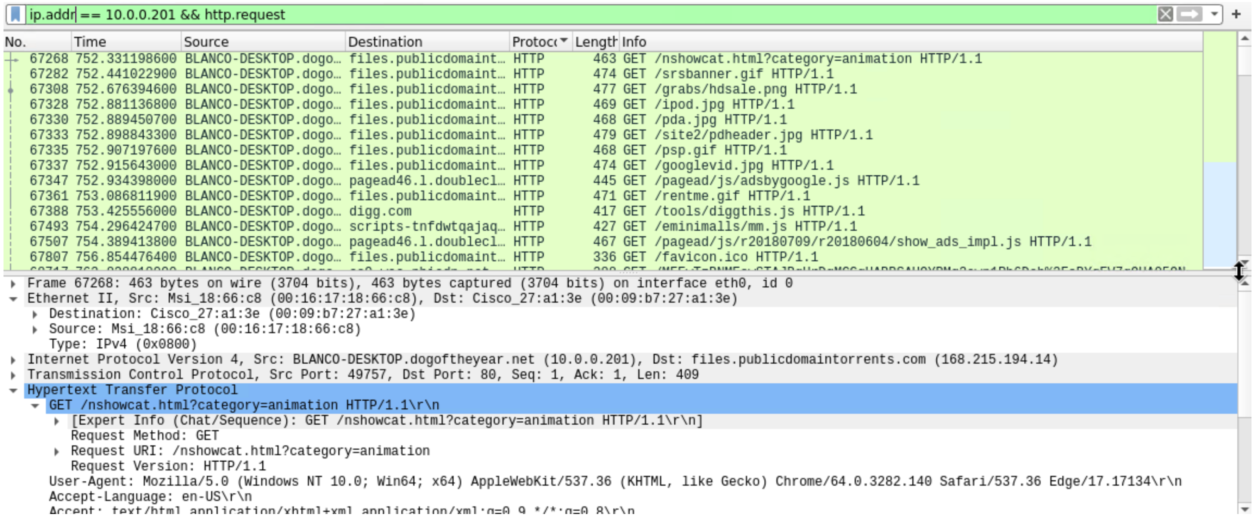
- The machines using torrents live in the range `10.0.0.0/24` and are clients of an AD domain.
- The DC of this domain lives at `10.0.0.2` and is named DogOfTheYear-DC.
- The DC is associated with the domain dogoftheyear.net.

Your task is to isolate torrent traffic and answer the following questions:

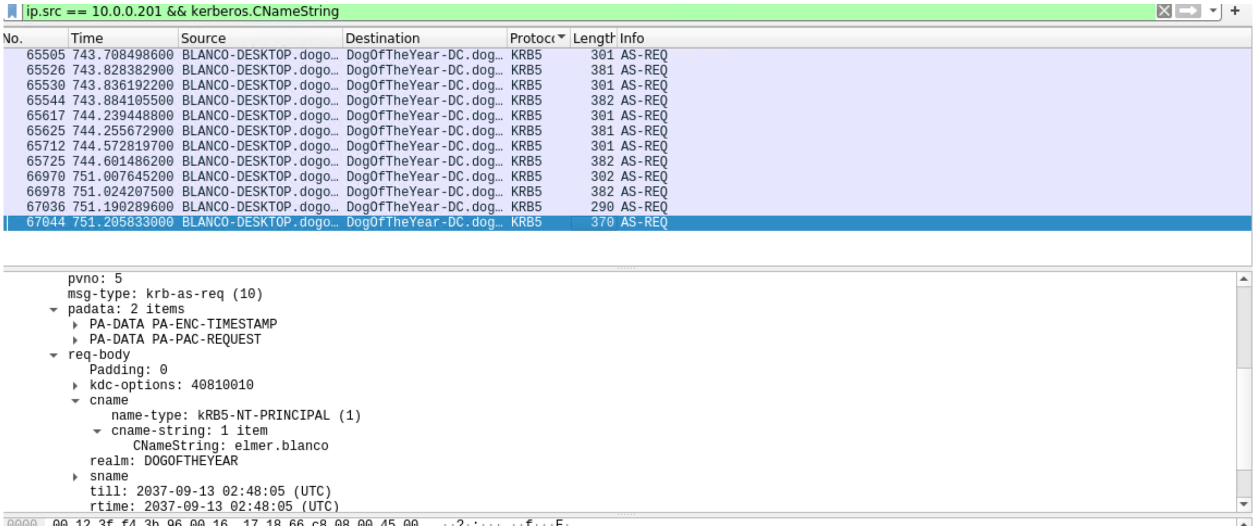
1. Find the following information about the machine with IP address `10.0.0.201`:
    - MAC address 00:16:17:18:66:c8 ‘ip.addr == 10.0.0.201’
    - Windows username elmer.blanco ‘ip.src == 10.0.0.201 && kerberos.CNameString’
    - OS version BLANCO-DESKTOP Windows NT 10.0 ‘ip.addr == 10.0.0.201 && http.request’



```
ip.addr == 10.0.0.201

No.   Time          Source                  Destination             Protocol Length Info
70966 774.875346000 BLANCO-DESKTOP.dogo…   DogOfTheYear-DC.dog…   DCERPC   274 Alter_context: call_id: 2, Fragment: Single, 1 context items: DRSUAPI V4…
70967 774.877885600 DogOfTheYear-DC.dog…   BLANCO-DESKTOP.dogo…   DCERPC   159 Alter_context_resp: call_id: 2, Fragment: Single, max_xmit: 5840 max_rec…
65434 743.509344200 10.0.0.1                BLANCO-DESKTOP.dogo…   DHCP     342 DHCP ACK      - Transaction ID 0x20640255
65443 743.519241100 BLANCO-DESKTOP.dogo…   DogOfTheYear-DC.dog…   DNS       97 Standard query 0x2428 SRV _ldap._tcp.dc._msdcs.dogoftheyear.net
65444 743.521933300 DogOfTheYear-DC.dog…   BLANCO-DESKTOP.dogo…   DNS      165 Standard query response 0x2428 SRV _ldap._tcp.dc._msdcs.dogoftheyear.net…
65445 743.523359600 BLANCO-DESKTOP.dogo…   DogOfTheYear-DC.dog…   DNS       92 Standard query 0x55b1 A DogOfTheYear-DC.dogoftheyear.net
65446 743.525085500 DogOfTheYear-DC.dog…   BLANCO-DESKTOP.dogo…   DNS      108 Standard query response 0x55b1 A DogOfTheYear-DC.dogoftheyear.net A 10.0…
65456 743.591202400 BLANCO-DESKTOP.dogo…   DogOfTheYear-DC.dog…   DNS      109 Standard query 0xc87e SRV _ldap._tcp.dc._msdcs.localdomain.dogoftheyear.…
65457 743.594207000 DogOfTheYear-DC.dog…   BLANCO-DESKTOP.dogo…   DNS      188 Standard query response 0xc87e No such name SRV _ldap._tcp.dc._msdcs.loc…
65458 743.595441500 BLANCO-DESKTOP.dogo…   DogOfTheYear-DC.dog…   DNS       76 Standard query 0xd8e8 A dns.msftncsi.com
65459 743.597201900 BLANCO-DESKTOP.dogo…   DogOfTheYear-DC.dog…   DNS      109 Standard query 0x8a13 SRV _ldap._tcp.dc._msdcs.localdomain.dogoftheyear.…
65460 743.600177800 DogOfTheYear-DC.dog…   BLANCO-DESKTOP.dogo…   DNS      188 Standard query response 0x8a13 No such name SRV _ldap._tcp.dc._msdcs.loc…
65461 743.601644700 DogOfTheYear-DC.dog…   BLANCO-DESKTOP.dogo…   DNS       92 Standard query response 0xd8e8 A dns.msftncsi.com A 131.107.255.255
65462 743.602933500 BLANCO-DESKTOP.dogo…   DogOfTheYear-DC.dog…   DNS       81 Standard query 0x7282 A wpad.dogoftheyear.net

    [Stream index: 1394]
  ▸ [Timestamps]
▾ Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x20640255
    Seconds elapsed: 0
  ▸ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201)
    Next server IP address: 10.0.0.1 (10.0.0.1)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Msi_18:66:c8 (00:16:17:18:66:c8)
    Client hardware address padding: 00000000000000000000
```



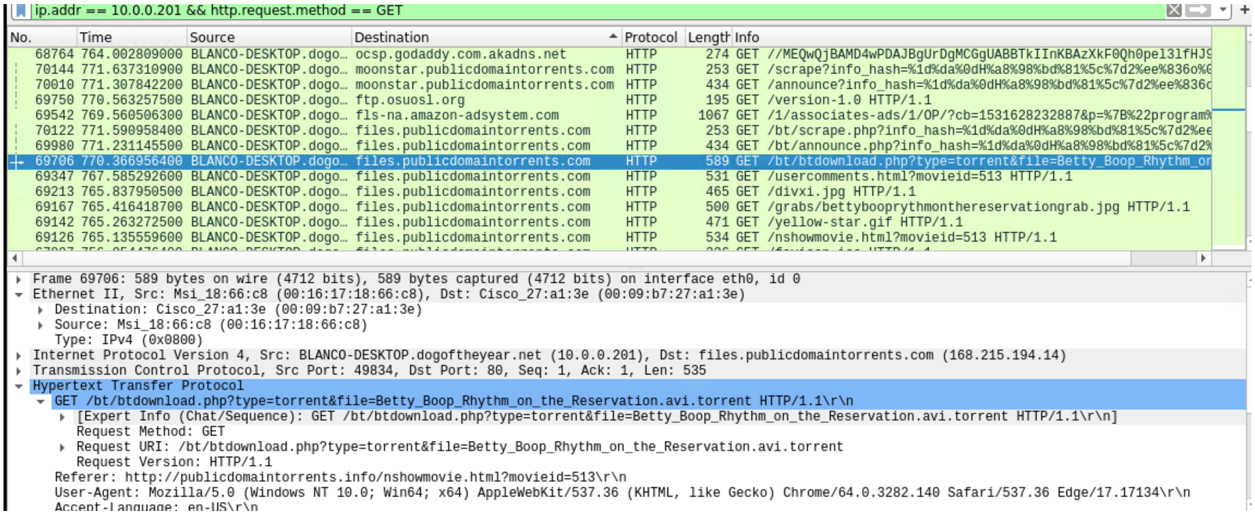
```
ip.addr == 10.0.0.201 && http.request

No.   Time          Source                  Destination             Protocol Length Info
67268 752.331198600 BLANCO-DESKTOP.dogo…   files.publicdomaint…   HTTP     463 GET /nshowcat.html?category=animation HTTP/1.1
67282 752.441022900 BLANCO-DESKTOP.dogo…   files.publicdomaint…   HTTP     474 GET /srsbanner.gif HTTP/1.1
67308 752.676394600 BLANCO-DESKTOP.dogo…   files.publicdomaint…   HTTP     477 GET /grabs/hdsale.png HTTP/1.1
67328 752.881136800 BLANCO-DESKTOP.dogo…   files.publicdomaint…   HTTP     469 GET /ipod.jpg HTTP/1.1
67330 752.889450700 BLANCO-DESKTOP.dogo…   files.publicdomaint…   HTTP     468 GET /pda.jpg HTTP/1.1
67333 752.898843300 BLANCO-DESKTOP.dogo…   files.publicdomaint…   HTTP     479 GET /site2/pdheader.jpg HTTP/1.1
67335 752.907197600 BLANCO-DESKTOP.dogo…   files.publicdomaint…   HTTP     468 GET /psp.gif HTTP/1.1
67337 752.915643000 BLANCO-DESKTOP.dogo…   files.publicdomaint…   HTTP     474 GET /googlevid.jpg HTTP/1.1
67347 752.934398000 BLANCO-DESKTOP.dogo…   pagead46.l.doublecl…   HTTP     445 GET /pagead/js/adsbygoogle.js HTTP/1.1
67361 753.086811900 BLANCO-DESKTOP.dogo…   files.publicdomaint…   HTTP     471 GET /rentme.gif HTTP/1.1
67388 753.425556000 BLANCO-DESKTOP.dogo…   digg.com                HTTP     417 GET /tools/diggthis.js HTTP/1.1
67493 754.296424700 BLANCO-DESKTOP.dogo…   scripts-tnfdwtqajaq…   HTTP     427 GET /eminimalls/mm.js HTTP/1.1
67507 754.389413800 BLANCO-DESKTOP.dogo…   pagead46.l.doublecl…   HTTP     467 GET /pagead/js/r20180709/r20180604/show_ads_impl.js HTTP/1.1
67807 756.854476400 BLANCO-DESKTOP.dogo…   files.publicdomaint…   HTTP     336 GET /favicon.ico HTTP/1.1

▸ Frame 67268: 463 bytes on wire (3704 bits), 463 bytes captured (3704 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)
  ▸ Destination: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
  ▸ 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: files.publicdomaintorrents.com (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
    ▸ [Expert Info (Chat/Sequence): GET /nshowcat.html?category=animation HTTP/1.1\r\n]
      Request Method: GET
    ▸ Request URI: /nshowcat.html?category=animation
      Request Version: HTTP/1.1
    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
```



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

No.   Time          Source                Destination            Protocol Length Info
65505 743.708498600 BLANCO-DESKTOP.dogo… DogOfTheYear-DC.dog… KRB5      301 AS-REQ
65526 743.828382900 BLANCO-DESKTOP.dogo… DogOfTheYear-DC.dog… KRB5      381 AS-REQ
65530 743.836192200 BLANCO-DESKTOP.dogo… DogOfTheYear-DC.dog… KRB5      301 AS-REQ
65544 743.884105500 BLANCO-DESKTOP.dogo… DogOfTheYear-DC.dog… KRB5      382 AS-REQ
65617 744.239448800 BLANCO-DESKTOP.dogo… DogOfTheYear-DC.dog… KRB5      301 AS-REQ
65625 744.255672900 BLANCO-DESKTOP.dogo… DogOfTheYear-DC.dog… KRB5      381 AS-REQ
65712 744.572819700 BLANCO-DESKTOP.dogo… DogOfTheYear-DC.dog… KRB5      301 AS-REQ
65725 744.601486200 BLANCO-DESKTOP.dogo… DogOfTheYear-DC.dog… KRB5      382 AS-REQ
66970 751.007645200 BLANCO-DESKTOP.dogo… DogOfTheYear-DC.dog… KRB5      302 AS-REQ
66978 751.024207500 BLANCO-DESKTOP.dogo… DogOfTheYear-DC.dog… KRB5      382 AS-REQ
67036 751.190289600 BLANCO-DESKTOP.dogo… DogOfTheYear-DC.dog… KRB5      290 AS-REQ
67044 751.205833000 BLANCO-DESKTOP.dogo… DogOfTheYear-DC.dog… KRB5      370 AS-REQ
```

```
      pvno: 5
      msg-type: krb-as-req (10)
    ▾ padata: 2 items
      ▸ PA-DATA PA-ENC-TIMESTAMP
      ▸ PA-DATA PA-PAC-REQUEST
    ▾ 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)
0000  00 12 3f f4 3b 96 00 16  17 18 66 c8 08 00 45 00   ..?.;... ..f...E.
```

2. Which torrent file did the user download?



```
ip.addr == 10.0.0.201 && http.request.method == GET

No.   Time          Source                Destination                        Protocol Length Info
68764 764.002809000 BLANCO-DESKTOP.dogo… ocsp.godaddy.com.akadns.net         HTTP      274 GET //MEQwQjBAMD4wPDAJBgUrDgMCGgUABBTkIInKBAzXkF0Qh0pel3lfHJ9
70144 771.637310900 BLANCO-DESKTOP.dogo… moonstar.publicdomaintorrents.com  HTTP      253 GET /scrape?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%0
70010 771.307842200 BLANCO-DESKTOP.dogo… moonstar.publicdomaintorrents.com  HTTP      434 GET /announce?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836c
69750 770.563257500 BLANCO-DESKTOP.dogo… ftp.osuosl.org                     HTTP      195 GET /version-1.0 HTTP/1.1
69542 769.560506300 BLANCO-DESKTOP.dogo… fls-na.amazon-adsystem.com         HTTP     1067 GET /1/associates-ads/1/OP/?cb=1531628232887&p=%7B%22program%
70122 771.590958400 BLANCO-DESKTOP.dogo… files.publicdomaintorrents.com     HTTP      253 GET /bt/scrape.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee
69980 771.231145500 BLANCO-DESKTOP.dogo… files.publicdomaintorrents.com     HTTP      434 GET /bt/announce.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%
69706 770.366956400 BLANCO-DESKTOP.dogo… files.publicdomaintorrents.com     HTTP      589 GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_or
69347 767.585292600 BLANCO-DESKTOP.dogo… files.publicdomaintorrents.com     HTTP      531 GET /usercomments.html?movieid=513 HTTP/1.1
69213 765.837950500 BLANCO-DESKTOP.dogo… files.publicdomaintorrents.com     HTTP      465 GET /divxi.jpg HTTP/1.1
69167 765.416418700 BLANCO-DESKTOP.dogo… files.publicdomaintorrents.com     HTTP      500 GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1
69142 765.263272500 BLANCO-DESKTOP.dogo… files.publicdomaintorrents.com     HTTP      471 GET /yellow-star.gif HTTP/1.1
69126 765.135559600 BLANCO-DESKTOP.dogo… files.publicdomaintorrents.com     HTTP      534 GET /nshowmovie.html?movieid=513 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)
  ▸ Destination: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
  ▸ 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: files.publicdomaintorrents.com (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
    ▸ [Expert Info (Chat/Sequence): GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n]
      Request Method: GET
    ▸ Request URI: /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
      Request Version: HTTP/1.1
    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
```