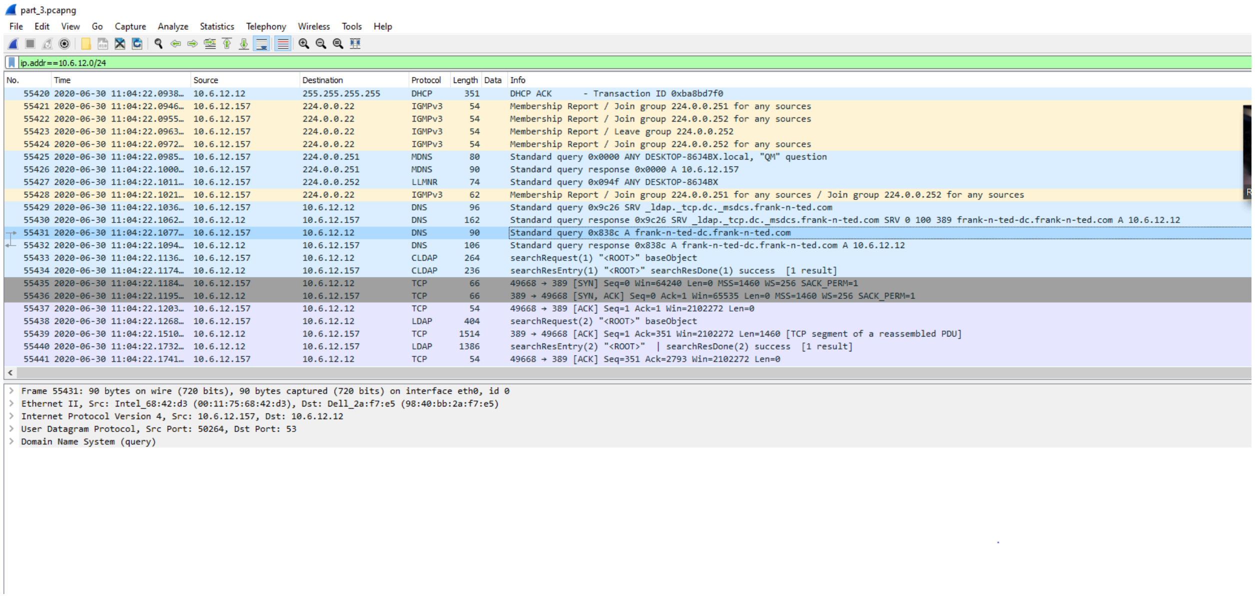
Time Thieves

At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to the 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

The traffic must be inspected to answer the following Network Report

1. What is the domain name of the users' custom site?
   - The Domain Name: Frank-n-Ted-DC.frand-n-ted.com.
   - Filter used in Wireshark: ip.addr==10.6.12.0/24

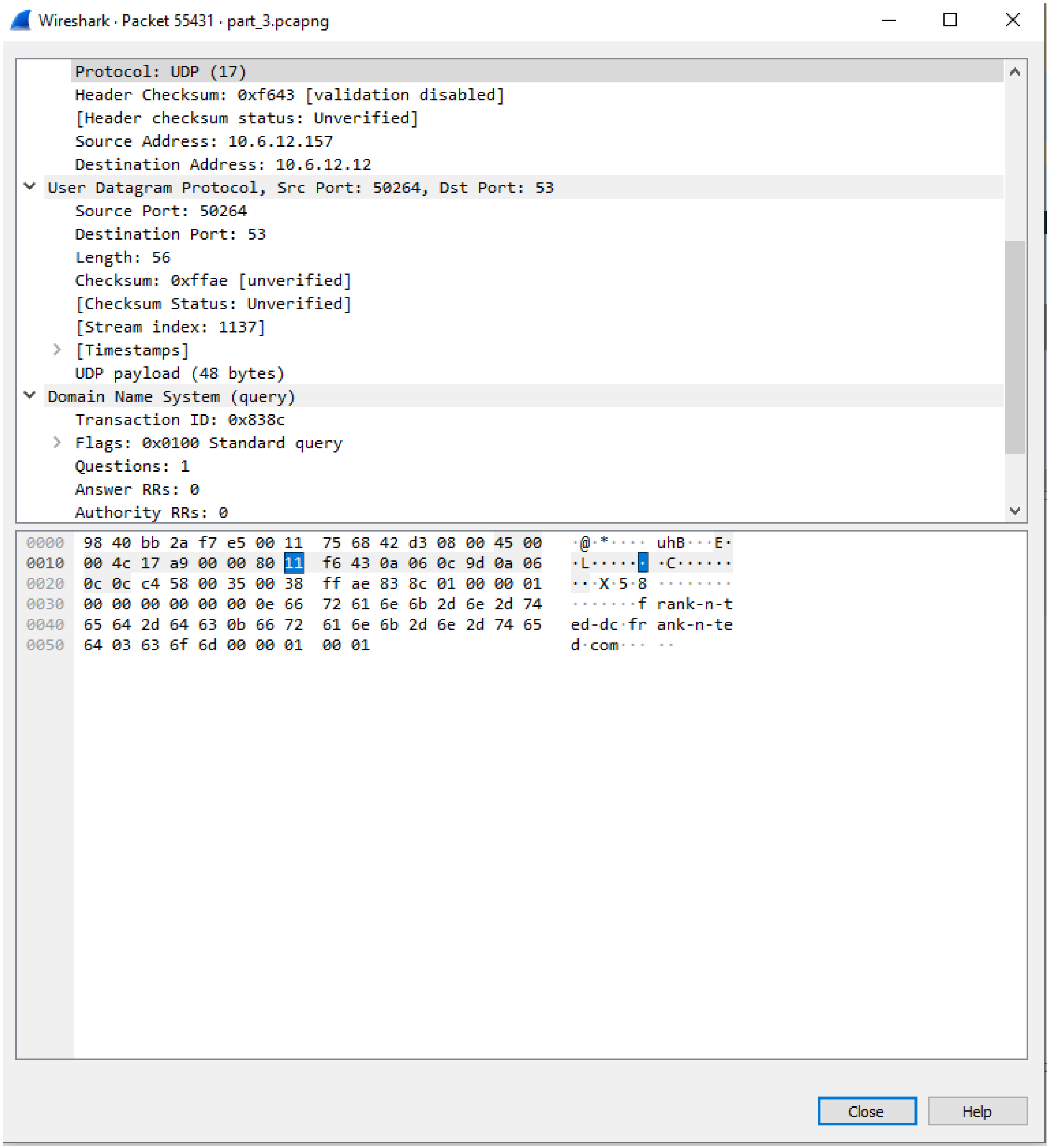


ip.addr==10.6.12.0/24

```
No.   Time                       Source        Destination      Protocol Length Data Info
55420 2020-06-30 11:04:22.0938…  10.6.12.12    255.255.255.255  DHCP     351       DHCP ACK      - Transaction ID 0xba8bd7f0
55421 2020-06-30 11:04:22.0946…  10.6.12.157   224.0.0.22       IGMPv3   54        Membership Report / Join group 224.0.0.251 for any sources
55422 2020-06-30 11:04:22.0955…  10.6.12.157   224.0.0.22       IGMPv3   54        Membership Report / Join group 224.0.0.252 for any sources
55423 2020-06-30 11:04:22.0963…  10.6.12.157   224.0.0.22       IGMPv3   54        Membership Report / Leave group 224.0.0.252
55424 2020-06-30 11:04:22.0972…  10.6.12.157   224.0.0.22       IGMPv3   54        Membership Report / Join group 224.0.0.252 for any sources
55425 2020-06-30 11:04:22.0985…  10.6.12.157   224.0.0.251      MDNS     80        Standard query 0x0000 ANY DESKTOP-86J4BX.local, "QM" question
55426 2020-06-30 11:04:22.1000…  10.6.12.157   224.0.0.251      MDNS     90        Standard query response 0x0000 A 10.6.12.157
55427 2020-06-30 11:04:22.1011…  10.6.12.157   224.0.0.252      LLMNR    74        Standard query 0x094f ANY DESKTOP-86J4BX
55428 2020-06-30 11:04:22.1021…  10.6.12.157   224.0.0.22       IGMPv3   62        Membership Report / Join group 224.0.0.251 for any sources / Join group 224.0.0.252 for any sources
55429 2020-06-30 11:04:22.1036…  10.6.12.157   10.6.12.12       DNS      96        Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
55430 2020-06-30 11:04:22.1062…  10.6.12.12    10.6.12.157      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 2020-06-30 11:04:22.1077…  10.6.12.157   10.6.12.12       DNS      90        Standard query 0x838c A frank-n-ted-dc.frank-n-ted.com
55432 2020-06-30 11:04:22.1094…  10.6.12.12    10.6.12.157      DNS      106       Standard query response 0x838c A frank-n-ted-dc.frank-n-ted.com A 10.6.12.12
55433 2020-06-30 11:04:22.1136…  10.6.12.157   10.6.12.12       CLDAP    264       searchRequest(1) "<ROOT>" baseObject
55434 2020-06-30 11:04:22.1174…  10.6.12.12    10.6.12.157      CLDAP    236       searchResEntry(1) "<ROOT>" searchResDone(1) success  [1 result]
55435 2020-06-30 11:04:22.1184…  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
55436 2020-06-30 11:04:22.1195…  10.6.12.12    10.6.12.157      TCP      66        389 → 49668 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
55437 2020-06-30 11:04:22.1203…  10.6.12.157   10.6.12.12       TCP      54        49668 → 389 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
55438 2020-06-30 11:04:22.1268…  10.6.12.157   10.6.12.12       LDAP     404       searchRequest(2) "<ROOT>" baseObject
55439 2020-06-30 11:04:22.1510…  10.6.12.12    10.6.12.157      TCP      1514      389 → 49668 [ACK] Seq=1 Ack=351 Win=2102272 Len=1460 [TCP segment of a reassembled PDU]
55440 2020-06-30 11:04:22.1732…  10.6.12.12    10.6.12.157      LDAP     1386      searchResEntry(2) "<ROOT>"  | searchResDone(2) success  [1 result]
55441 2020-06-30 11:04:22.1741…  10.6.12.157   10.6.12.12       TCP      54        49668 → 389 [ACK] Seq=351 Ack=2793 Win=2102272 Len=0
```

```
> 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)
> Internet Protocol Version 4, Src: 10.6.12.157, Dst: 10.6.12.12
> User Datagram Protocol, Src Port: 50264, Dst Port: 53
> Domain Name System (query)
```

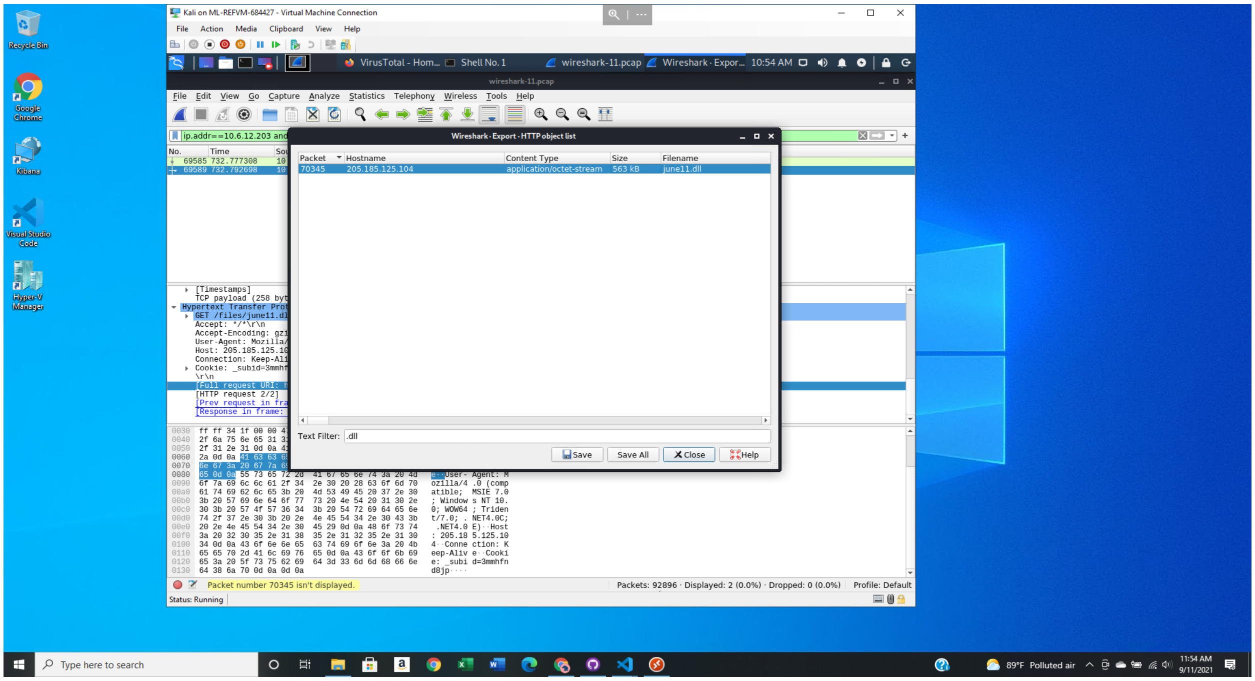
2. What is the IP address of the Domain Controller (DC) of the AD network?
   - IP address is 10.6.12.12 (Frank-n-Ted-DC.frank-n-ted.com)
   - Filter used in Wireshark: ip.addr==10.6.12.0/24



```
    Protocol: UDP (17)
    Header Checksum: 0xf643 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.6.12.157
    Destination Address: 10.6.12.12
v User Datagram Protocol, Src Port: 50264, Dst Port: 53
    Source Port: 50264
    Destination Port: 53
    Length: 56
    Checksum: 0xffae [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1137]
  > [Timestamps]
    UDP payload (48 bytes)
v Domain Name System (query)
    Transaction ID: 0x838c
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
```

```
0000  98 40 bb 2a f7 e5 00 11  75 68 42 d3 08 00 45 00   ·@·*···· uhB···E·
0010  00 4c 17 a9 00 00 80 11  f6 43 0a 06 0c 9d 0a 06   ·L······ ·C······
0020  0c 0c c4 58 00 35 00 38  ff ae 83 8c 01 00 00 01   ···X·5·8 ········
0030  00 00 00 00 00 00 0e 66  72 61 6e 6b 2d 6e 2d 74   ·······f rank-n-t
0040  65 64 2d 64 63 0b 66 72  61 6e 6b 2d 6e 2d 74 65   ed-dc·fr ank-n-te
0050  64 03 63 6f 6d 00 00 01  00 01                     d·com··· ··
```

3. What is the name of the malware downloaded to the 10.6.12.203 machine?
   - Malware file: june11.dll



Kali on ML-REFVM-684427 - Virtual Machine Connection

wireshark-11.pcap

ip.addr==10.6.12.203 and

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
70345	205.185.125.104	application/octet-stream	563 kB	june11.dll

Text Filter: .dll

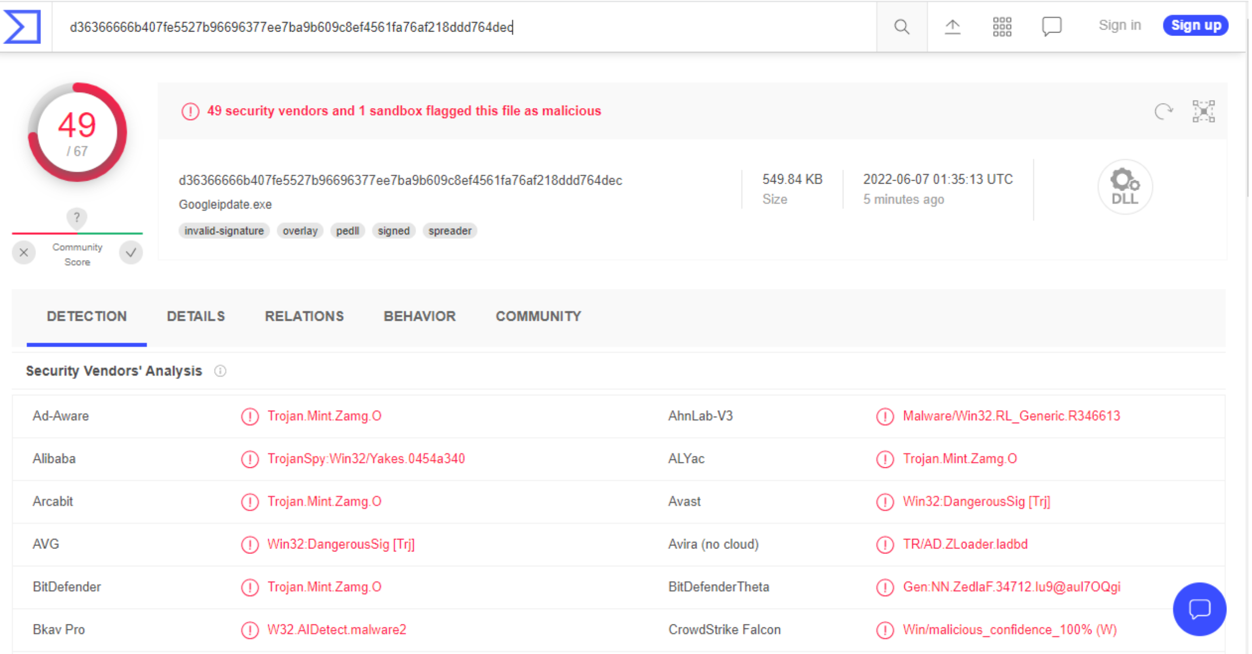
Packet number 70345 isn't displayed.

Packets: 92896 · Displayed: 2 (0.0%) · Dropped: 0 (0.0%) Profile: Default

Status: Running

- Once the file was found, the file was exported to the Kali machine.
- Filter used in Wireshark: ip.addr==10.6.12.203 and http.request.method==GET

4. Upload the file to VirusTotal.com
   - This type of malware is classified as a Trojan
   - Results:



d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

49 / 67

49 security vendors and 1 sandbox flagged this file as malicious

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec
Googleipdate.exe

invalid-signature overlay pedll signed spreader

549.84 KB
Size

2022-06-07 01:35:13 UTC
5 minutes ago

DLL

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

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
BitDefender	Trojan.Mint.Zamg.O	BitDefenderTheta	Gen:NN.ZedlaF.34712.lu9@aul7OQgi
Bkav Pro	W32.AIDetect.malware2	CrowdStrike Falcon	Win/malicious_confidence_100% (W)

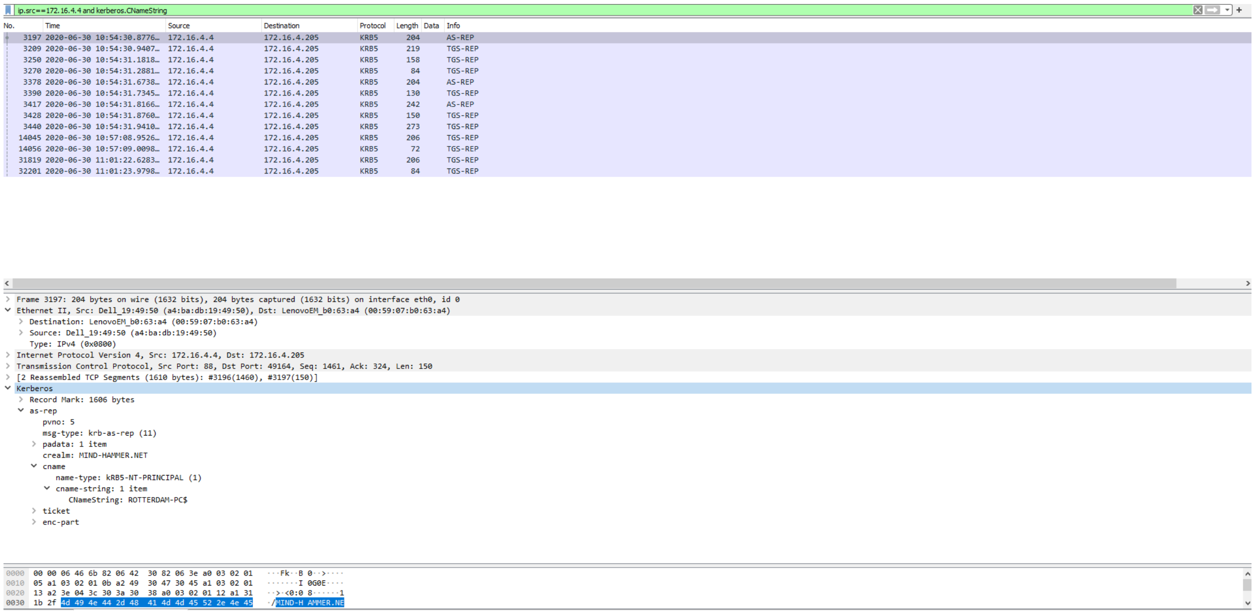
Vulnerable Windows Machines

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 172.164.0/24.
- 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 the 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 used in Wireshark: ip.src==172.16.4.4 and kerberos.CNameString



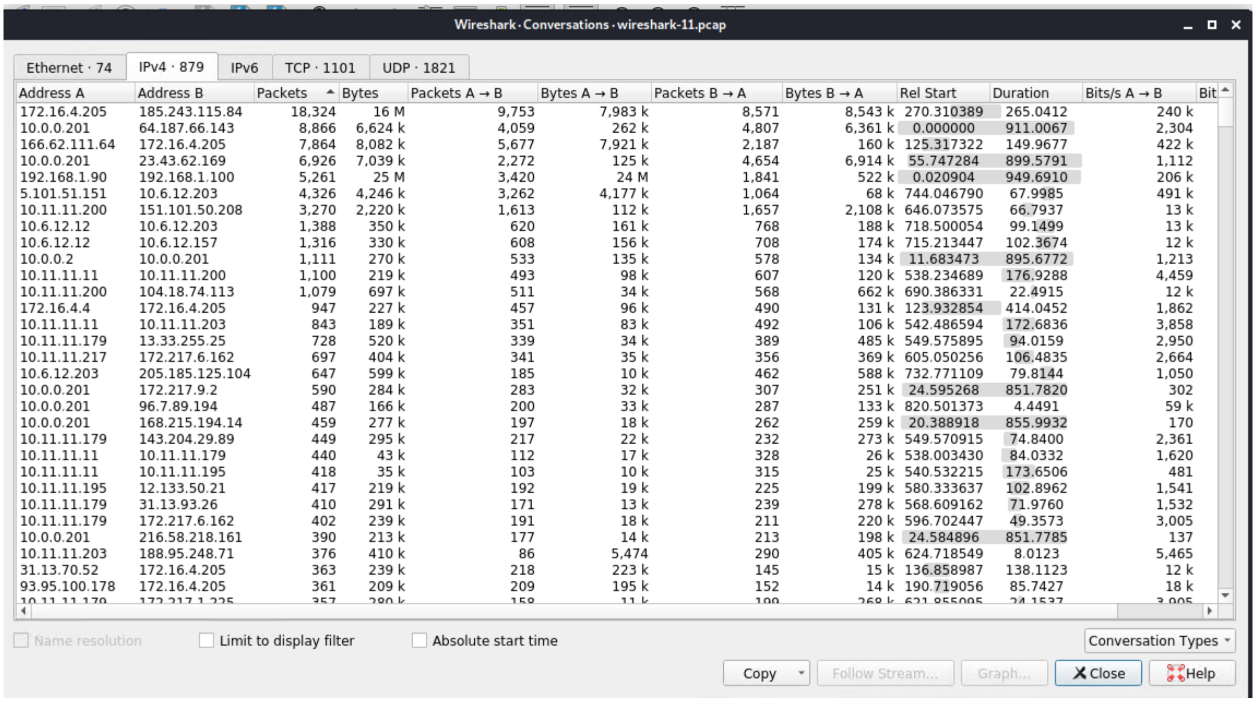
```
ip.src==172.16.4.4 and kerberos.CNameString

No.    Time                        Source       Destination   Protocol  Length  Data  Info
 3197  2020-06-30 10:54:30.8776…   172.16.4.4   172.16.4.205  KRB5        204         AS-REP
 3209  2020-06-30 10:54:30.9407…   172.16.4.4   172.16.4.205  KRB5        219         TGS-REP
 3250  2020-06-30 10:54:31.1818…   172.16.4.4   172.16.4.205  KRB5        158         TGS-REP
 3270  2020-06-30 10:54:31.2881…   172.16.4.4   172.16.4.205  KRB5         84         TGS-REP
 3378  2020-06-30 10:54:31.6738…   172.16.4.4   172.16.4.205  KRB5        204         AS-REP
 3390  2020-06-30 10:54:31.7345…   172.16.4.4   172.16.4.205  KRB5        130         TGS-REP
 3417  2020-06-30 10:54:31.8166…   172.16.4.4   172.16.4.205  KRB5        242         AS-REP
 3428  2020-06-30 10:54:31.8760…   172.16.4.4   172.16.4.205  KRB5        150         TGS-REP
 3440  2020-06-30 10:54:31.9410…   172.16.4.4   172.16.4.205  KRB5        273         TGS-REP
14045  2020-06-30 10:57:08.9526…   172.16.4.4   172.16.4.205  KRB5        206         TGS-REP
14056  2020-06-30 10:57:09.0098…   172.16.4.4   172.16.4.205  KRB5         72         TGS-REP
31819  2020-06-30 11:01:22.6283…   172.16.4.4   172.16.4.205  KRB5        206         TGS-REP
32201  2020-06-30 11:01:23.9798…   172.16.4.4   172.16.4.205  KRB5         84         TGS-REP
```

```
> Frame 3197: 204 bytes on wire (1632 bits), 204 bytes captured (1632 bits) on interface eth0, id 0
v Ethernet II, Src: Dell_19:49:50 (a4:ba:db:19:49:50), Dst: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
  > Destination: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
  > Source: Dell_19:49:50 (a4:ba:db:19:49:50)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.16.4.4, Dst: 172.16.4.205
> Transmission Control Protocol, Src Port: 88, Dst Port: 49164, Seq: 1461, Ack: 324, Len: 150
> [2 Reassembled TCP Segments (1610 bytes): #3196(1460), #3197(150)]
v Kerberos
  > Record Mark: 1606 bytes
  v as-rep
      pvno: 5
      msg-type: krb-as-rep (11)
    > padata: 1 item
      crealm: MIND-HAMMER.NET
    v cname
        name-type: kRB5-NT-PRINCIPAL (1)
      v cname-string: 1 item
          CNameString: ROTTERDAM-PC$
    > ticket
    > enc-part
```

```
0000  00 00 06 46 6b 82 06 42  30 82 06 3e a0 03 02 01   ···Fk··B 0··>····
0010  05 a1 03 02 01 0b a2 49  30 47 30 45 a1 03 02 01   ·······I 0G0E····
0020  13 a2 3e 04 3c 30 3a 30  38 a0 03 02 01 12 a1 31   ··>·<0:0 8······1
0030  1b 2f 4d 49 4e 44 2d 48  41 4d 4d 45 52 2e 4e 45   ·/MIND-H AMMER.NE
```

2. What is the username of the Windows user whose computer is infected?
    - Filter used in Wireshark: ip.src==172.16.4.205 and kerberos.CNameString
3. What are the IP addresses used in the actual infection traffic?
    - Based on the Conversation statistics and the filtering by the highest amount of packets between the IP addresses- 172.16.4.205, 185.243.115.84, 166.62.11.64 are the infected traffic.



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	18,324	16 M	9,753	7,983 k	8,571	8,543 k	270.310389	265.0412	240 k	
10.0.0.201	64.187.66.143	8,866	6,624 k	4,059	262 k	4,807	6,361 k	0.000000	911.0067	2,304	
166.62.111.64	172.16.4.205	7,864	8,082 k	5,677	7,921 k	2,187	160 k	125.317322	149.9677	422 k	
10.0.0.201	23.43.62.169	6,926	7,039 k	2,272	125 k	4,654	6,914 k	55.747284	899.5791	1,112	
192.168.1.90	192.168.1.100	5,261	25 M	3,420	24 M	1,841	522 k	0.020904	949.6910	206 k	
5.101.51.151	10.6.12.203	4,326	4,246 k	3,262	4,177 k	1,064	68 k	744.046790	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	646.073575	66.7937	13 k	
10.6.12.12	10.6.12.203	1,388	350 k	620	161 k	768	188 k	718.500054	99.1499	13 k	
10.6.12.12	10.6.12.157	1,316	330 k	608	156 k	708	174 k	715.213447	102.3674	12 k	
10.0.0.2	10.0.0.201	1,111	270 k	533	135 k	578	134 k	11.683473	895.6772	1,213	
10.11.11.11	10.11.11.200	1,100	219 k	493	98 k	607	120 k	538.234689	176.9288	4,459	
10.11.11.200	104.18.74.113	1,079	697 k	511	34 k	568	662 k	690.386331	22.4915	12 k	
172.16.4.4	172.16.4.205	947	227 k	457	96 k	490	131 k	123.932854	414.0452	1,862	
10.11.11.11	10.11.11.203	843	189 k	351	83 k	492	106 k	542.486594	172.6836	3,858	
10.11.11.179	13.33.255.25	728	520 k	339	34 k	389	485 k	549.575895	94.0159	2,950	
10.11.11.217	172.217.6.162	697	404 k	341	35 k	356	369 k	605.050256	106.4835	2,664	
10.6.12.203	205.185.125.104	647	599 k	185	10 k	462	588 k	732.771109	79.8144	1,050	
10.0.0.201	172.217.9.2	590	284 k	283	32 k	307	251 k	24.595268	851.7820	302	
10.0.0.201	96.7.89.194	487	166 k	200	33 k	287	133 k	820.501373	4.4491	59 k	
10.0.0.201	168.215.194.14	459	277 k	197	18 k	262	259 k	20.388918	855.9932	170	
10.11.11.179	143.204.29.89	449	295 k	217	22 k	232	273 k	549.570915	74.8400	2,361	
10.11.11.11	10.11.11.179	440	43 k	112	17 k	328	26 k	538.003430	84.0332	1,620	
10.11.11.11	10.11.11.195	418	35 k	103	10 k	315	25 k	540.532215	173.6506	481	
10.11.11.195	12.133.50.21	417	219 k	192	19 k	225	199 k	580.333637	102.8962	1,541	
10.11.11.179	31.13.93.26	410	291 k	171	13 k	239	278 k	568.609162	71.9760	1,532	
10.11.11.179	172.217.6.162	402	239 k	191	18 k	211	220 k	596.702447	49.3573	3,005	
10.0.0.201	216.58.218.161	390	213 k	177	14 k	213	198 k	24.584896	851.7785	137	
10.11.11.203	188.95.248.71	376	410 k	86	5,474	290	405 k	624.718549	8.0123	5,465	
31.13.70.52	172.16.4.205	363	239 k	218	223 k	145	15 k	136.858987	138.1123	12 k	
93.95.100.178	172.16.4.205	361	209 k	209	195 k	152	14 k	190.719056	85.7427	18 k	
10.11.11.179	172.217.1.225	357	280 k	158	11 k	199	268 k	621.855095	24.1537	3,005	

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.

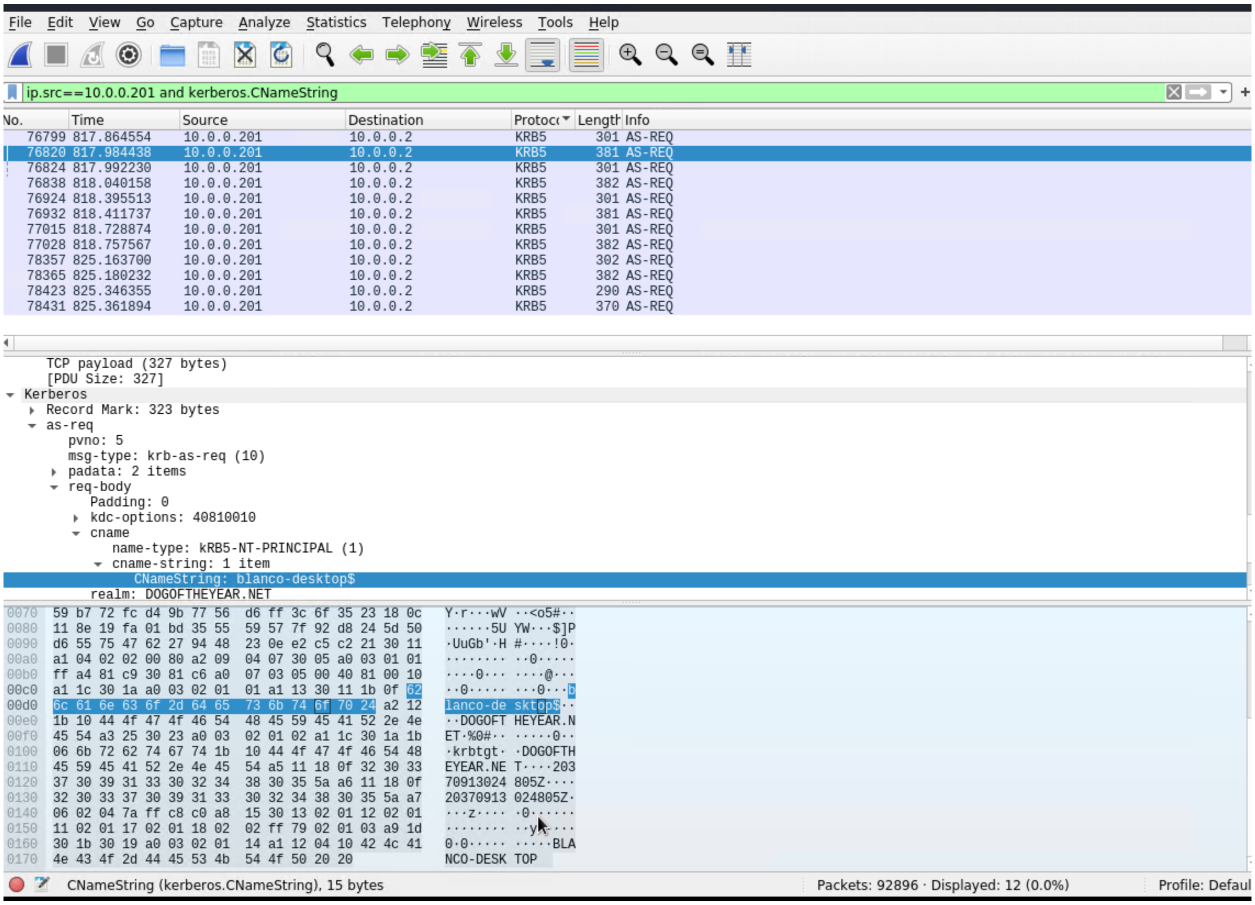
IT shared the following about the torrent activity:

- The machine using torrents live in the range 10.0.0.0/24 and are clients of 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.

The task is to isolate the torrent traffic and answer the following questions for the Network Report:

1. Find the following information about the machine with the IP address of 10.0.0.201:
   - MAC address: 00:16:17:18:66:c8
   - Windows username: elmer.blanco

- OS version: BLANCO-DESKTOP



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src==10.0.0.201 and kerberos.CNameString

```
No.    Time       Source      Destination  Protocol Length Info
 76799 817.864554 10.0.0.201  10.0.0.2     KRB5     301 AS-REQ
 76820 817.984438 10.0.0.201  10.0.0.2     KRB5     381 AS-REQ
 76824 817.992230 10.0.0.201  10.0.0.2     KRB5     301 AS-REQ
 76838 818.040158 10.0.0.201  10.0.0.2     KRB5     382 AS-REQ
 76924 818.395513 10.0.0.201  10.0.0.2     KRB5     301 AS-REQ
 76932 818.411737 10.0.0.201  10.0.0.2     KRB5     381 AS-REQ
 77015 818.728874 10.0.0.201  10.0.0.2     KRB5     301 AS-REQ
 77028 818.757567 10.0.0.201  10.0.0.2     KRB5     382 AS-REQ
 78357 825.163700 10.0.0.201  10.0.0.2     KRB5     302 AS-REQ
 78365 825.180232 10.0.0.201  10.0.0.2     KRB5     382 AS-REQ
 78423 825.346355 10.0.0.201  10.0.0.2     KRB5     290 AS-REQ
 78431 825.361894 10.0.0.201  10.0.0.2     KRB5     370 AS-REQ
```

```
    TCP payload (327 bytes)
    [PDU Size: 327]
Kerberos
    Record Mark: 323 bytes
    as-req
        pvno: 5
        msg-type: krb-as-req (10)
        padata: 2 items
        req-body
            Padding: 0
            kdc-options: 40810010
            cname
                name-type: kRB5-NT-PRINCIPAL (1)
                cname-string: 1 item
                    CNameString: blanco-desktop$
            realm: DOGOFTHEYEAR.NET
```

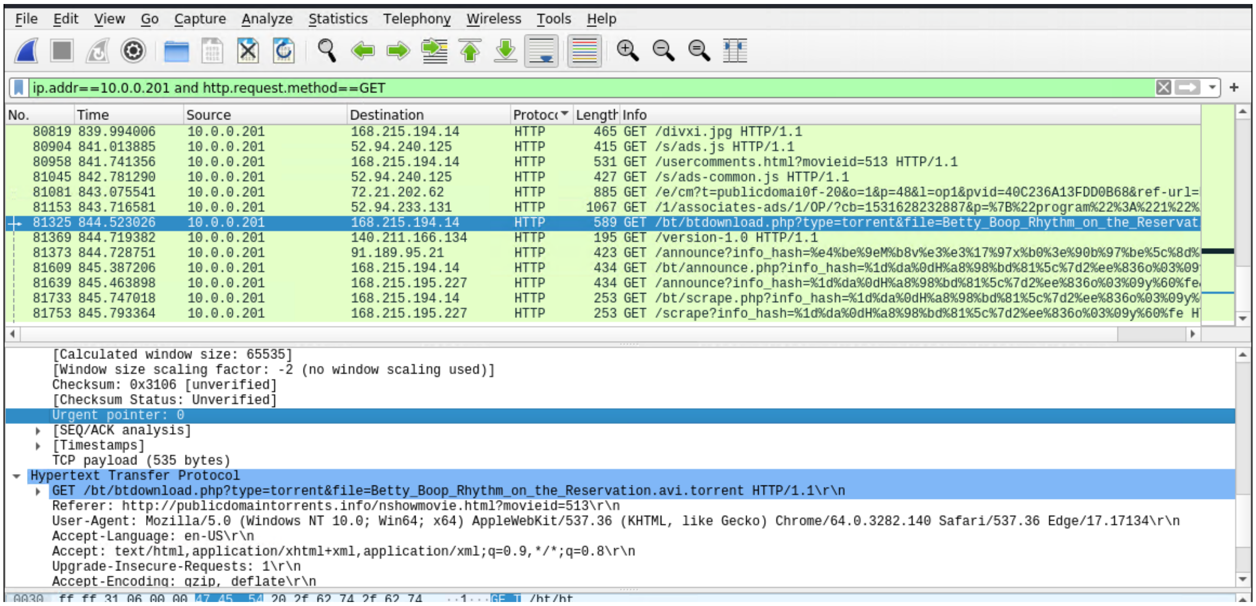
```
0070  59 b7 72 fc d4 9b 77 56  d6 ff 3c 6f 35 23 18 0c   Y·r···wV ··<o5#··
0080  11 8e 19 fa 01 bd 35 55  59 57 7f 92 d8 24 5d 50   ······5U YW···$]P
0090  d6 55 75 47 62 27 94 48  23 0e e2 c5 c2 21 30 11   ·UuGb'·H #····!0·
00a0  a1 04 02 02 00 80 a2 09  04 07 30 05 a0 03 01 01   ········ ··0·····
00b0  ff a4 81 c9 30 81 c6 a0  07 03 05 00 40 81 00 10   ····0··· ····@···
00c0  a1 1c 30 1a a0 03 02 01  01 a1 13 30 11 1b 0f 62   ··0····· ···0···b
00d0  6c 61 6e 63 6f 2d 64 65  73 6b 74 6f 70 24 a2 12   lanco-de sktop$··
00e0  1b 10 44 4f 47 4f 46 54  48 45 59 45 41 52 2e 4e   ··DOGOFT HEYEAR.N
00f0  45 54 a3 25 30 23 a0 03  02 01 02 a1 1c 30 1a 1b   ET·%0#·· ·····0··
0100  06 6b 72 62 74 67 74 1b  10 44 4f 47 4f 46 54 48   ·krbtgt· ·DOGOFTH
0110  45 59 45 41 52 2e 4e 45  54 a5 11 18 0f 32 30 33   EYEAR.NE T····203
0120  37 30 39 31 33 30 32 34  38 30 35 5a a6 11 18 0f   70913024 805Z····
0130  32 30 33 37 30 39 31 33  30 32 34 38 30 35 5a a7   20370913 024805Z·
0140  06 02 04 7a ff c8 c0 a8  15 30 13 02 01 12 02 01   ···z···· ·0······
0150  11 02 01 17 02 01 18 02  02 ff 79 02 01 03 a9 1d   ········ ··y·····
0160  30 1b 30 19 a0 03 02 01  14 a1 12 04 10 42 4c 41   0·0····· ·····BLA
0170  4e 43 4f 2d 44 45 53 4b  54 4f 50 20 20            NCO-DESK TOP
```

CNameString (kerberos.CNameString), 15 bytes

Packets: 92896 · Displayed: 12 (0.0%)

Profile: Defaul

2. Which torrent file did the user download?
   - The torrent downloaded **Betty_Boop_Rythm_on_the_Reservation.avi.torrent.
   - Filter used in Wireshark: ip.addr==10.0.0.201 and http.request.method==GET



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

```
No.   Time       Source       Destination      Protocol Length Info
80819 839.994006 10.0.0.201   168.215.194.14   HTTP     465 GET /divxi.jpg HTTP/1.1
80904 841.013885 10.0.0.201   52.94.240.125    HTTP     415 GET /s/ads.js HTTP/1.1
80958 841.741356 10.0.0.201   168.215.194.14   HTTP     531 GET /usercomments.html?movieid=513 HTTP/1.1
81045 842.781290 10.0.0.201   52.94.240.125    HTTP     427 GET /s/ads-common.js HTTP/1.1
81081 843.075541 10.0.0.201   72.21.202.62     HTTP     885 GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=op1&pvid=40C236A13FDD0B68&ref-url=
81153 843.716581 10.0.0.201   52.94.233.131    HTTP    1067 GET /1/associates-ads/1/OP/?cb=1531628232887&p=%7B%22program%22%3A%221%22%
81325 844.523026 10.0.0.201   168.215.194.14   HTTP     589 GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservat
81369 844.719382 10.0.0.201   140.211.166.134  HTTP     195 GET /version-1.0 HTTP/1.1
81373 844.728751 10.0.0.201   91.189.95.21     HTTP     423 GET /announce?info_hash=%e4%be%9eM%b8v%e3%e3%17%97x%b0%3e%90b%97%be%5c%8d%
81609 845.387206 10.0.0.201   168.215.194.14   HTTP     434 GET /bt/announce.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%09
81639 845.463898 10.0.0.201   168.215.195.227  HTTP     434 GET /announce?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%09y%60%fe
81733 845.747018 10.0.0.201   168.215.194.14   HTTP     253 GET /bt/scrape.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%09y%
81753 845.793364 10.0.0.201   168.215.195.227  HTTP     253 GET /scrape?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%09y%60%fe H
```

```
    [Calculated window size: 65535]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x3106 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
    TCP payload (535 bytes)
▾ 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
```

```
0030  ff ff 31 06 00 00 47 45  54 20 2f 62 74 2f 62 74   ..1...GE T /bt/bt
```