# 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:

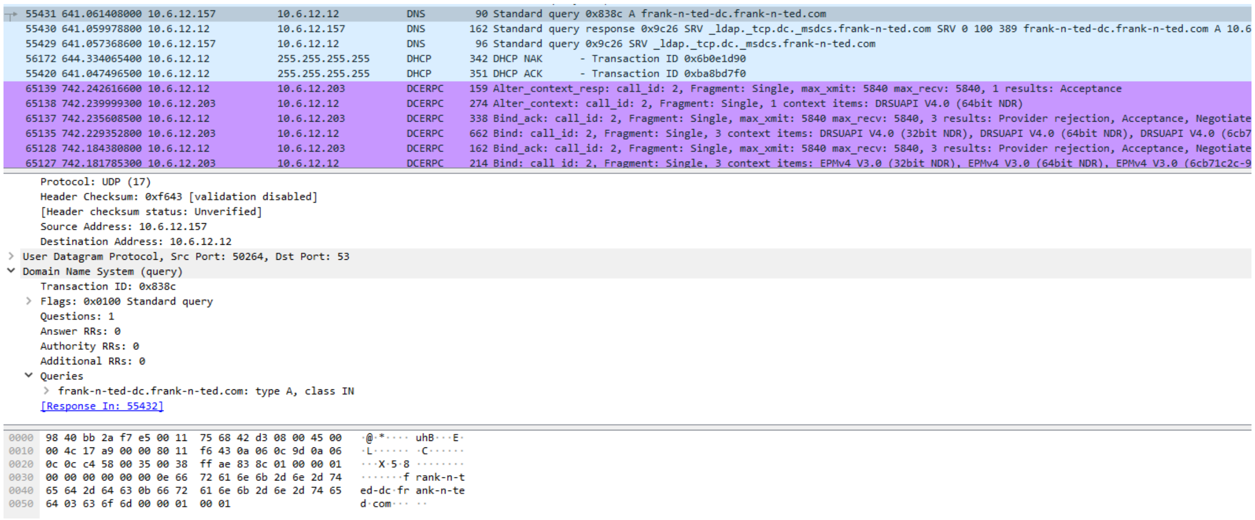
- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.
- Their IP addresses are somewhere in the range `10.6.12.0/24`.

Refer to the following filters on Wireshark:

- Domain of the site in question: **ip.addr==10.6.12.0/24**
- Traffic Inspection: **ip.addr==10.6.12.12**
- Other Inspection: **ip.addr==10.6.12.203**
- Suspected Malware Name: **ip.addr==10.6.12.203 and http.request.method==GET**

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

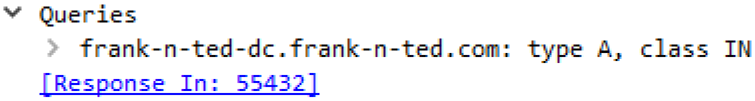
1. What is the domain name of the users' custom site?
   a. Domain Name: Frank-n-Ted-DC    frank-n-ted.com
   b. Wireshark Filter: ip.src==10.6.12.0/24



```
55431 641.061408000 10.6.12.157        10.6.12.12         DNS       90 Standard query 0x838c A frank-n-ted-dc.frank-n-ted.com
55430 641.059978800 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
55429 641.057368600 10.6.12.157        10.6.12.12         DNS       96 Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
56172 644.334065400 10.6.12.12         255.255.255.255    DHCP     342 DHCP NAK      - Transaction ID 0x6b0e1d90
55420 641.047496500 10.6.12.12         255.255.255.255    DHCP     351 DHCP ACK      - Transaction ID 0xba8bd7f0
65139 742.242616600 10.6.12.12         10.6.12.203        DCERPC   159 Alter_context_resp: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 1 results: Acceptance
65138 742.239999300 10.6.12.203        10.6.12.12         DCERPC   274 Alter_context: call_id: 2, Fragment: Single, 1 context items: DRSUAPI V4.0 (64bit NDR)
65137 742.235608500 10.6.12.12         10.6.12.203        DCERPC   338 Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 results: Provider rejection, Acceptance, Negotiate
65135 742.229352800 10.6.12.203        10.6.12.12         DCERPC   662 Bind: call_id: 2, Fragment: Single, 3 context items: DRSUAPI V4.0 (32bit NDR), DRSUAPI V4.0 (64bit NDR), DRSUAPI V4.0 (6cb7
65128 742.184380800 10.6.12.12         10.6.12.203        DCERPC   162 Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 results: Provider rejection, Acceptance, Negotiate
65127 742.181785300 10.6.12.203        10.6.12.12         DCERPC   214 Bind: call_id: 2, Fragment: Single, 3 context items: EPMv4 V3.0 (32bit NDR), EPMv4 V3.0 (64bit NDR), EPMv4 V3.0 (6cb71c2c-9
```

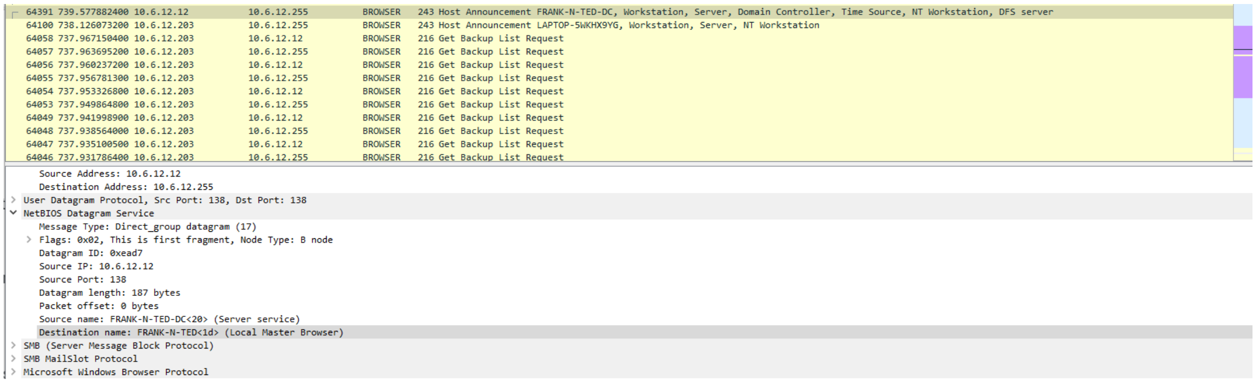
```
    Protocol: UDP (17)
    Header Checksum: 0xf643 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.6.12.157
    Destination Address: 10.6.12.12
> User Datagram Protocol, Src Port: 50264, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x838c
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > frank-n-ted-dc.frank-n-ted.com: type A, class IN
    [Response In: 55432]
```

```
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··· ··
```



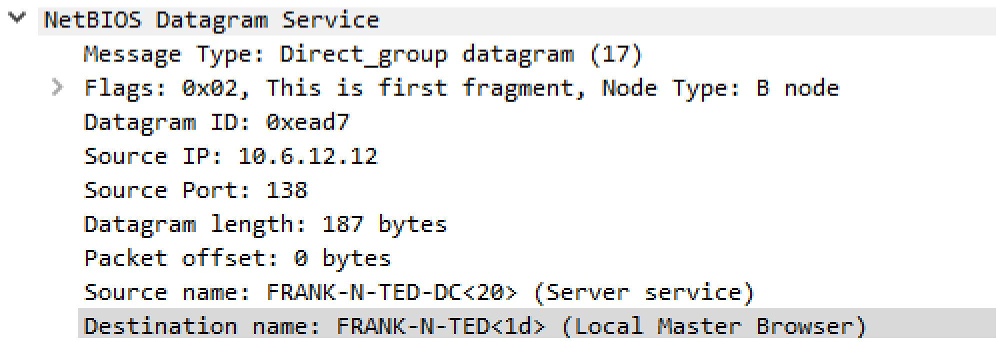
```
v Queries
  > frank-n-ted-dc.frank-n-ted.com: type A, class IN
  [Response In: 55432]
```

2. What is the IP address of the Domain Controller (DC) of the AD network?
    a. IP Address: 10.6.12.12 (Frank-n-Ted-DC)
    b. Wireshark Filter: ip.src==10.6.12.0/24



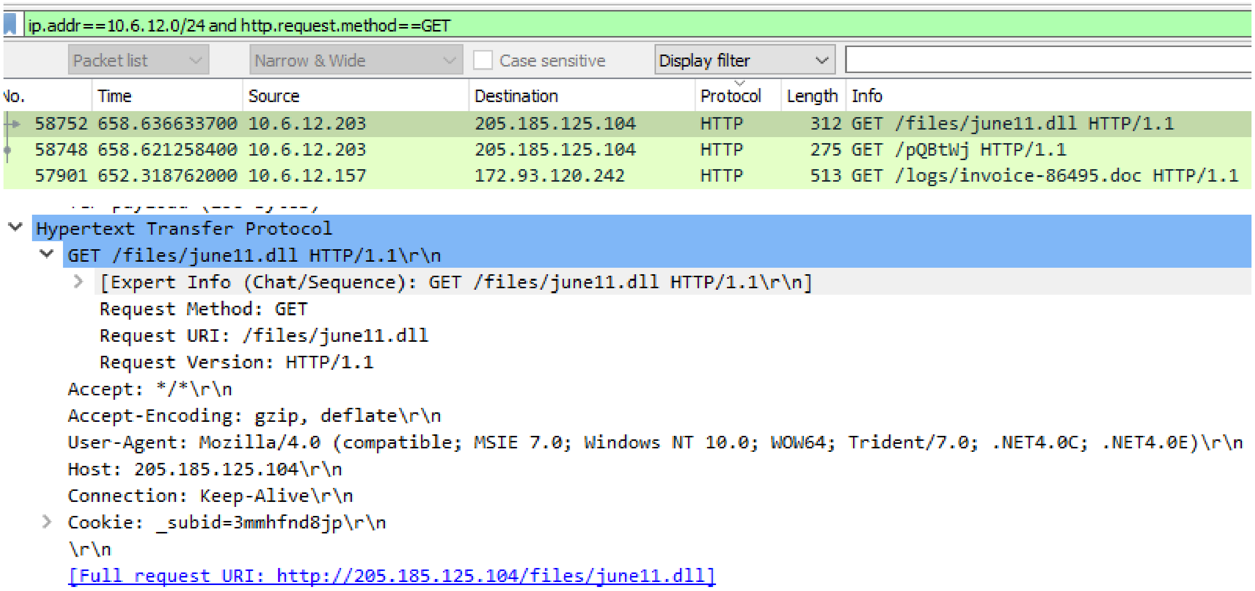
```
64391 739.577882400 10.6.12.12        10.6.12.255       BROWSER   243 Host Announcement FRANK-N-TED-DC, Workstation, Server, Domain Controller, Time Source, NT Workstation, DFS server
64100 738.126073200 10.6.12.203       10.6.12.255       BROWSER   243 Host Announcement LAPTOP-5WKHX9YG, Workstation, Server, NT Workstation
64058 737.967150400 10.6.12.203       10.6.12.12        BROWSER   216 Get Backup List Request
64057 737.963695200 10.6.12.203       10.6.12.255       BROWSER   216 Get Backup List Request
64056 737.960237200 10.6.12.203       10.6.12.12        BROWSER   216 Get Backup List Request
64055 737.956781300 10.6.12.203       10.6.12.255       BROWSER   216 Get Backup List Request
64054 737.953326800 10.6.12.203       10.6.12.12        BROWSER   216 Get Backup List Request
64053 737.949864800 10.6.12.203       10.6.12.255       BROWSER   216 Get Backup List Request
64049 737.941998900 10.6.12.203       10.6.12.12        BROWSER   216 Get Backup List Request
64048 737.938564000 10.6.12.203       10.6.12.255       BROWSER   216 Get Backup List Request
64047 737.935100500 10.6.12.203       10.6.12.12        BROWSER   216 Get Backup List Request
64046 737.931786400 10.6.12.203       10.6.12.255       BROWSER   216 Get Backup List Request
```

```
    Source Address: 10.6.12.12
    Destination Address: 10.6.12.255
> User Datagram Protocol, Src Port: 138, Dst Port: 138
v NetBIOS Datagram Service
    Message Type: Direct_group datagram (17)
  > Flags: 0x02, This is first fragment, Node Type: B node
    Datagram ID: 0xead7
    Source IP: 10.6.12.12
    Source Port: 138
    Datagram length: 187 bytes
    Packet offset: 0 bytes
    Source name: FRANK-N-TED-DC<20> (Server service)
    Destination name: FRANK-N-TED<1d> (Local Master Browser)
> SMB (Server Message Block Protocol)
> SMB MailSlot Protocol
> Microsoft Windows Browser Protocol
```



```
NetBIOS Datagram Service
    Message Type: Direct_group datagram (17)
  > Flags: 0x02, This is first fragment, Node Type: B node
    Datagram ID: 0xead7
    Source IP: 10.6.12.12
    Source Port: 138
    Datagram length: 187 bytes
    Packet offset: 0 bytes
    Source name: FRANK-N-TED-DC<20> (Server service)
    Destination name: FRANK-N-TED<1d> (Local Master Browser)
```

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
    a. Malware file name: june11.dll
    b. Wireshark Filter: ip.addr==10.6.12.0/24 and http.request.method==GET



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

No.   Time           Source        Destination      Protocol  Length Info
58752 658.636633700 10.6.12.203   205.185.125.104  HTTP      312 GET /files/june11.dll HTTP/1.1
58748 658.621258400 10.6.12.203   205.185.125.104  HTTP      275 GET /pQBtWj HTTP/1.1
57901 652.318762000 10.6.12.157   172.93.120.242   HTTP      513 GET /logs/invoice-86495.doc HTTP/1.1

Hypertext Transfer Protocol
  GET /files/june11.dll HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /files/june11.dll HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /files/june11.dll
      Request Version: HTTP/1.1
  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]
```

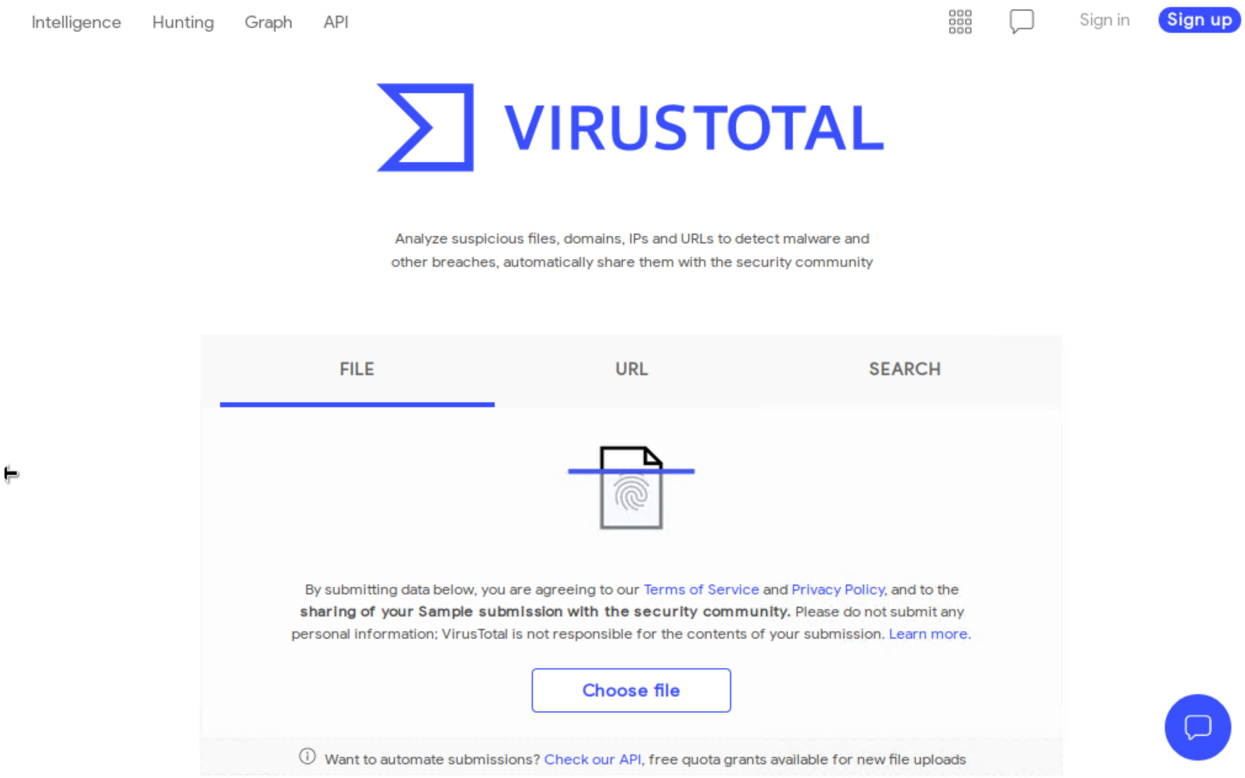
june11.dll is a file retrieved using GET

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

Extract the file for analysis:

- Open the "file" tab on Wireshark
- Export Objects
- Select HTTP
- Filter with "dll"
- Packet # 59388 for filename june11.dll
- Save

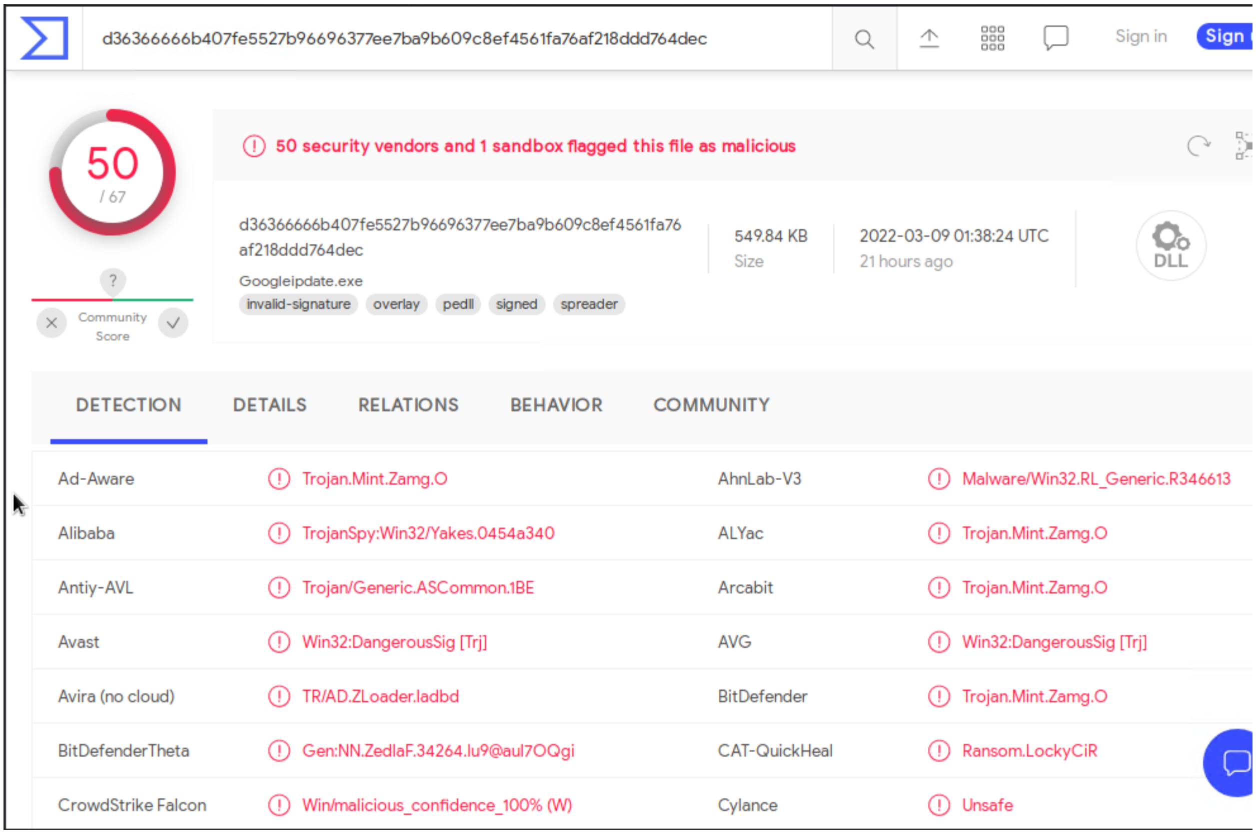
- Upload to VirusTotal.com



Analyze suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community

By submitting data below, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

ⓘ Want to automate submissions? Check our API, free quota grants available for new file uploads



d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

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
21 hours 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.34264.lu9@aul7OQgi | CAT-QuickHeal | Ransom.LockyCiR |
| CrowdStrike Falcon | Win/malicious_confidence_100% (W) | Cylance | Unsafe |

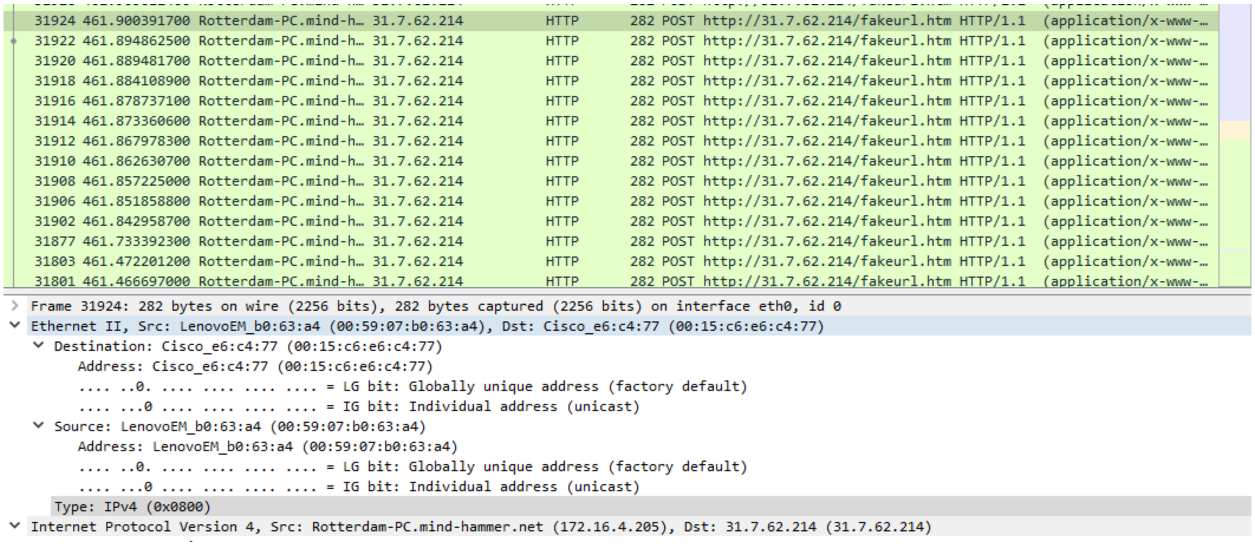
## Vulnerable Windows Machines

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.

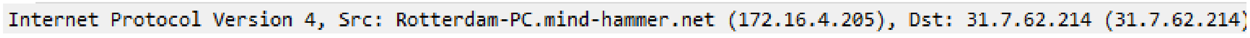
Inspect your traffic to answer the following questions:

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.addr==172.16.4.0/24

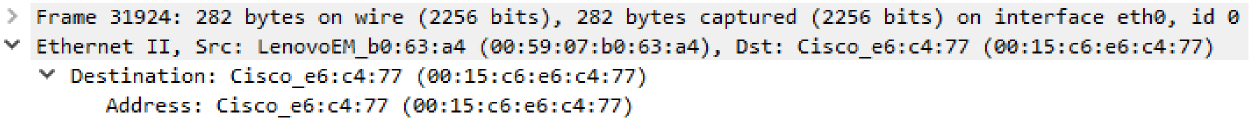


```
31924 461.900391700 Rotterdam-PC.mind-h… 31.7.62.214       HTTP      282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-…
31922 461.894862500 Rotterdam-PC.mind-h… 31.7.62.214       HTTP      282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-…
31920 461.889481700 Rotterdam-PC.mind-h… 31.7.62.214       HTTP      282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-…
31918 461.884108900 Rotterdam-PC.mind-h… 31.7.62.214       HTTP      282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-…
31916 461.878737100 Rotterdam-PC.mind-h… 31.7.62.214       HTTP      282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-…
31914 461.873360600 Rotterdam-PC.mind-h… 31.7.62.214       HTTP      282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-…
31912 461.867978300 Rotterdam-PC.mind-h… 31.7.62.214       HTTP      282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-…
31910 461.862630700 Rotterdam-PC.mind-h… 31.7.62.214       HTTP      282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-…
31908 461.857225000 Rotterdam-PC.mind-h… 31.7.62.214       HTTP      282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-…
31906 461.851858800 Rotterdam-PC.mind-h… 31.7.62.214       HTTP      282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-…
31902 461.842958700 Rotterdam-PC.mind-h… 31.7.62.214       HTTP      282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-…
31877 461.733392300 Rotterdam-PC.mind-h… 31.7.62.214       HTTP      282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-…
31803 461.472201200 Rotterdam-PC.mind-h… 31.7.62.214       HTTP      282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-…
31801 461.466697000 Rotterdam-PC.mind-h… 31.7.62.214       HTTP      282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-…
```

```
> Frame 31924: 282 bytes on wire (2256 bits), 282 bytes captured (2256 bits) on interface eth0, id 0
v Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Cisco_e6:c4:77 (00:15:c6:e6:c4:77)
  v Destination: Cisco_e6:c4:77 (00:15:c6:e6:c4:77)
      Address: Cisco_e6:c4:77 (00:15:c6:e6:c4:77)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: 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)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: Rotterdam-PC.mind-hammer.net (172.16.4.205), Dst: 31.7.62.214 (31.7.62.214)
```

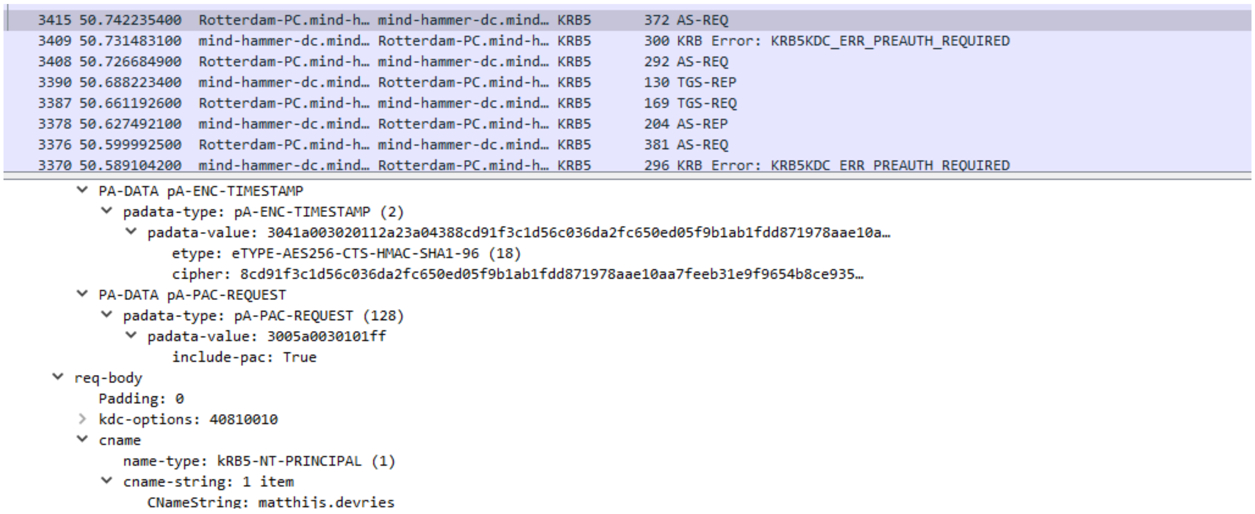


```
Internet Protocol Version 4, Src: Rotterdam-PC.mind-hammer.net (172.16.4.205), Dst: 31.7.62.214 (31.7.62.214)
```



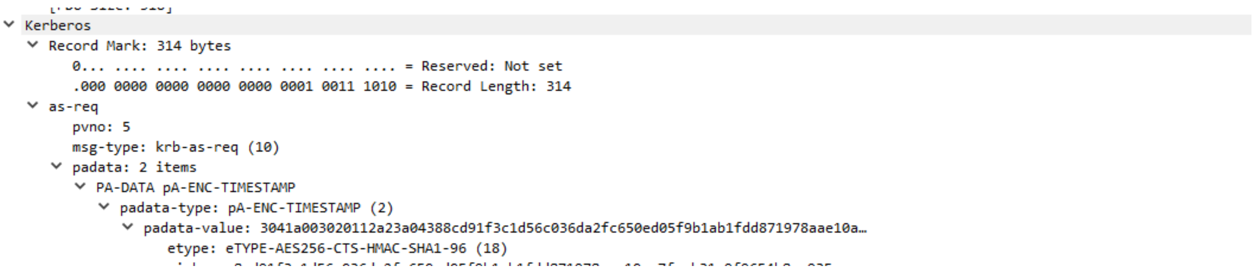
```
> Frame 31924: 282 bytes on wire (2256 bits), 282 bytes captured (2256 bits) on interface eth0, id 0
v Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Cisco_e6:c4:77 (00:15:c6:e6:c4:77)
  v Destination: Cisco_e6:c4:77 (00:15:c6:e6:c4:77)
      Address: Cisco_e6:c4:77 (00:15:c6:e6:c4:77)
```

2. What is the username of the Windows user whose computer is infected?
    - Username: matthjis.devries
    - Wireshark Filter: ip.src==172.16.4.205 && kerberos.CNameString

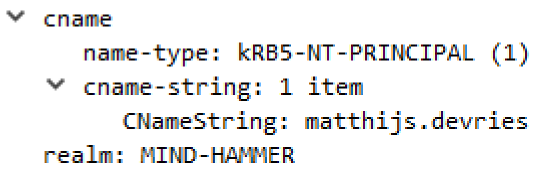


```
3415 50.742235400  Rotterdam-PC.mind-h… mind-hammer-dc.mind… KRB5       372 AS-REQ
3409 50.731483100  mind-hammer-dc.mind… Rotterdam-PC.mind-h… KRB5       300 KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
3408 50.726684900  Rotterdam-PC.mind-h… mind-hammer-dc.mind… KRB5       292 AS-REQ
3390 50.688223400  mind-hammer-dc.mind… Rotterdam-PC.mind-h… KRB5       130 TGS-REP
3387 50.661192600  Rotterdam-PC.mind-h… mind-hammer-dc.mind… KRB5       169 TGS-REQ
3378 50.627492100  mind-hammer-dc.mind… Rotterdam-PC.mind-h… KRB5       204 AS-REP
3376 50.599992500  Rotterdam-PC.mind-h… mind-hammer-dc.mind… KRB5       381 AS-REQ
3370 50.589104200  mind-hammer-dc.mind… Rotterdam-PC.mind-h… KRB5       296 KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
```

```
      v PA-DATA pA-ENC-TIMESTAMP
        v padata-type: pA-ENC-TIMESTAMP (2)
          v padata-value: 3041a003020112a23a04388cd91f3c1d56c036da2fc650ed05f9b1ab1fdd871978aae10a…
              etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
              cipher: 8cd91f3c1d56c036da2fc650ed05f9b1ab1fdd871978aae10aa7feeb31e9f9654b8ce935…
      v PA-DATA pA-PAC-REQUEST
        v padata-type: pA-PAC-REQUEST (128)
          v padata-value: 3005a0030101ff
              include-pac: True
    v req-body
        Padding: 0
      > kdc-options: 40810010
      v cname
          name-type: kRB5-NT-PRINCIPAL (1)
        v cname-string: 1 item
            CNameString: matthijs.devries
```



```
v Kerberos
  v Record Mark: 314 bytes
      0... .... .... .... .... .... .... .... = Reserved: Not set
      .000 0000 0000 0000 0000 0001 0011 1010 = Record Length: 314
  v as-req
      pvno: 5
      msg-type: krb-as-req (10)
    v padata: 2 items
      v PA-DATA pA-ENC-TIMESTAMP
        v padata-type: pA-ENC-TIMESTAMP (2)
          v padata-value: 3041a003020112a23a04388cd91f3c1d56c036da2fc650ed05f9b1ab1fdd871978aae10a…
              etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
```



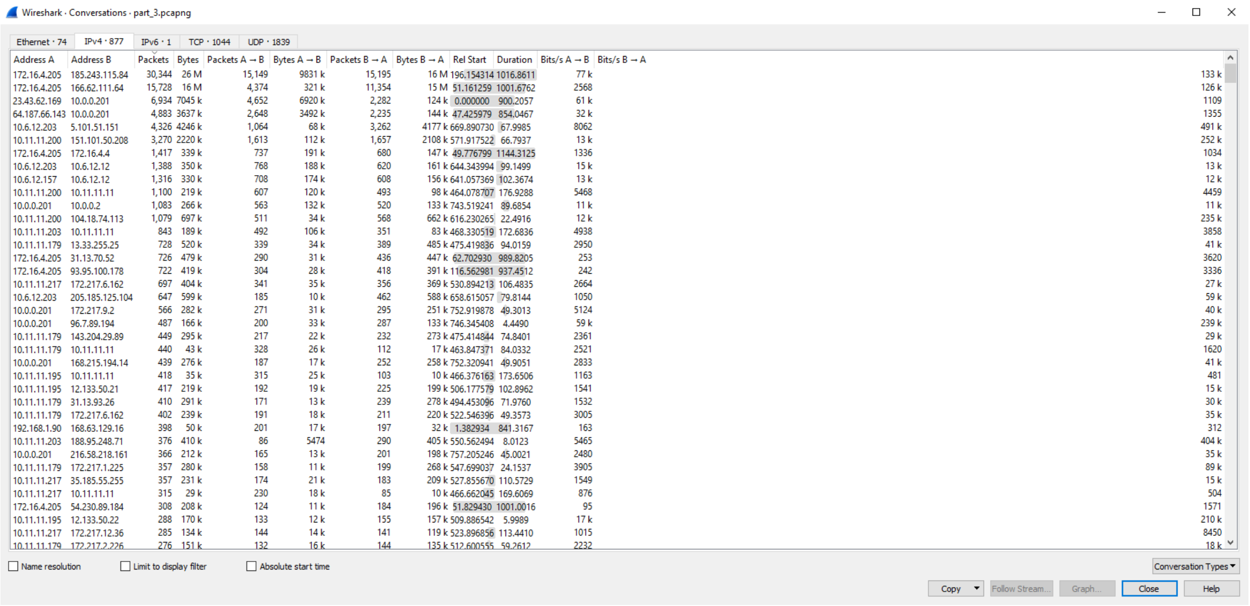
```
v cname
    name-type: kRB5-NT-PRINCIPAL (1)
  v cname-string: 1 item
      CNameString: matthijs.devries
  realm: MIND-HAMMER
```

3. What are the IP addresses used in the actual infection traffic?
    - 172.16.4.205, 185.243.115.84, 166.62.11.64, 23.43.62.169

To find this we can analyze our current search query.

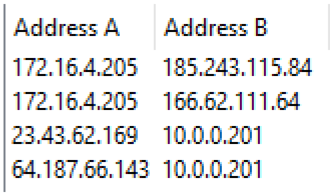
Filter: ip.src==172.16.4.203

- Select “Statistics” from the top
- Select Conversation
- Select IPV4
- Sort Highest to lowest



| 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 | Bits/s B → A |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 172.16.4.205 | 185.243.115.84 | 30,344 | 26 M | 15,149 | 9831 k | 15,195 | 16 M | 196.154314 | 1016.8611 | 77 k | 133 k |
| 172.16.4.205 | 166.62.111.64 | 15,728 | 16 M | 4,374 | 321 k | 11,354 | 15 M | 51.161259 | 1001.6762 | 2568 | 126 k |
| 23.43.62.169 | 10.0.0.201 | 6,934 | 7045 k | 4,652 | 6920 k | 2,282 | 124 k | 0.000000 | 900.2057 | 61 k | 1109 |
| 64.187.66.143 | 10.0.0.201 | 4,883 | 3637 k | 2,648 | 3492 k | 2,235 | 144 k | 47.425979 | 854.0467 | 32 k | 1355 |
| 10.6.12.203 | 5.101.51.151 | 4,326 | 4246 k | 1,064 | 68 k | 3,262 | 4177 k | 669.890730 | 67.9985 | 8062 | 491 k |
| 10.11.11.200 | 151.101.50.208 | 3,270 | 2220 k | 1,613 | 112 k | 1,657 | 2108 k | 571.917522 | 66.7937 | 13 k | 252 k |
| 172.16.4.205 | 172.16.4.4 | 1,417 | 339 k | 737 | 191 k | 680 | 147 k | 49.776799 | 1144.3125 | 1336 | 1034 |
| 10.6.12.203 | 10.6.12.12 | 1,388 | 350 k | 768 | 188 k | 620 | 161 k | 644.343994 | 99.1499 | 15 k | 13 k |
| 10.6.12.157 | 10.6.12.12 | 1,316 | 330 k | 708 | 174 k | 608 | 156 k | 641.057369 | 102.3674 | 13 k | 12 k |
| 10.11.11.200 | 10.11.11.11 | 1,100 | 219 k | 607 | 120 k | 493 | 98 k | 464.078707 | 176.9288 | 5468 | 4459 |
| 10.0.0.201 | 10.0.0.2 | 1,083 | 266 k | 563 | 132 k | 520 | 133 k | 743.519241 | 89.6854 | 11 k | 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 | 235 k |
| 10.11.11.203 | 10.11.11.11 | 843 | 189 k | 492 | 106 k | 351 | 83 k | 468.330519 | 172.6836 | 4938 | 3858 |
| 10.11.11.179 | 13.33.255.25 | 728 | 520 k | 339 | 34 k | 389 | 485 k | 475.419836 | 94.0159 | 2950 | 41 k |
| 172.16.4.205 | 31.13.70.52 | 726 | 479 k | 290 | 31 k | 436 | 447 k | 62.702930 | 989.8205 | 253 | 3620 |
| 172.16.4.205 | 93.95.100.178 | 722 | 419 k | 304 | 28 k | 418 | 391 k | 116.562981 | 937.4512 | 242 | 3336 |
| 10.11.11.217 | 172.217.6.162 | 697 | 404 k | 341 | 35 k | 356 | 369 k | 530.894213 | 106.4835 | 2664 | 27 k |
| 10.6.12.203 | 205.185.125.104 | 647 | 599 k | 185 | 10 k | 462 | 588 k | 658.615057 | 79.8144 | 1050 | 59 k |
| 10.0.0.201 | 172.217.9.2 | 566 | 282 k | 271 | 31 k | 295 | 251 k | 752.919878 | 49.3013 | 5124 | 40 k |
| 10.0.0.201 | 96.7.89.194 | 487 | 166 k | 200 | 33 k | 287 | 133 k | 746.345408 | 4.4490 | 59 k | 239 k |
| 10.11.11.179 | 143.204.29.89 | 449 | 295 k | 217 | 22 k | 232 | 273 k | 475.414844 | 74.8401 | 2361 | 29 k |
| 10.11.11.179 | 10.11.11.11 | 440 | 43 k | 328 | 26 k | 112 | 17 k | 463.847371 | 84.0332 | 2521 | 1620 |
| 10.0.0.201 | 168.215.194.14 | 439 | 276 k | 187 | 17 k | 252 | 258 k | 752.320941 | 49.9051 | 2833 | 41 k |
| 10.11.11.195 | 10.11.11.11 | 418 | 35 k | 315 | 25 k | 103 | 10 k | 466.376163 | 173.6506 | 1163 | 481 |
| 10.11.11.195 | 12.133.50.21 | 417 | 219 k | 192 | 19 k | 225 | 199 k | 506.177579 | 102.8962 | 1541 | 15 k |
| 10.11.11.179 | 31.13.93.26 | 410 | 291 k | 171 | 13 k | 239 | 278 k | 494.453096 | 71.9760 | 1532 | 30 k |
| 10.11.11.179 | 172.217.6.162 | 402 | 239 k | 191 | 18 k | 211 | 220 k | 522.546396 | 49.3573 | 3005 | 35 k |
| 192.168.1.90 | 168.63.129.16 | 398 | 50 k | 201 | 17 k | 197 | 32 k | 1.382934 | 841.3167 | 163 | 312 |
| 10.11.11.203 | 188.95.248.71 | 376 | 410 k | 86 | 5474 | 290 | 405 k | 550.562494 | 8.0123 | 5465 | 404 k |
| 10.0.0.201 | 216.58.218.161 | 366 | 212 k | 165 | 13 k | 201 | 198 k | 757.205246 | 45.0021 | 2480 | 35 k |
| 10.11.11.179 | 172.217.1.225 | 357 | 280 k | 158 | 11 k | 199 | 268 k | 547.699037 | 24.1537 | 3905 | 89 k |
| 10.11.11.217 | 35.185.55.255 | 357 | 231 k | 174 | 21 k | 183 | 209 k | 527.855670 | 110.5729 | 1549 | 15 k |
| 10.11.11.217 | 10.11.11.11 | 315 | 29 k | 230 | 18 k | 85 | 10 k | 466.662045 | 169.6069 | 876 | 504 |
| 172.16.4.205 | 54.230.89.184 | 308 | 208 k | 124 | 11 k | 184 | 196 k | 51.829430 | 1001.0016 | 95 | 1571 |
| 10.11.11.195 | 12.133.50.22 | 288 | 170 k | 133 | 12 k | 155 | 157 k | 509.886542 | 5.9989 | 17 k | 210 k |
| 10.11.11.217 | 172.217.12.36 | 285 | 134 k | 144 | 14 k | 141 | 119 k | 523.896856 | 113.4410 | 1015 | 8450 |
| 10.11.11.179 | 172.217.2.226 | 276 | 151 k | 132 | 16 k | 144 | 135 k | 512.600555 | 59.2612 | 2232 | 18 k |

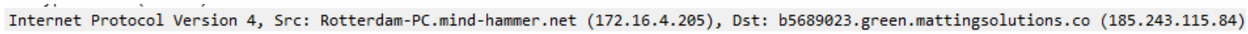
☐ Name resolution ☐ Limit to display filter ☐ Absolute start time



| Address A | Address B |
|---|---|
| 172.16.4.205 | 185.243.115.84 |
| 172.16.4.205 | 166.62.111.64 |
| 23.43.62.169 | 10.0.0.201 |
| 64.187.66.143 | 10.0.0.201 |

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

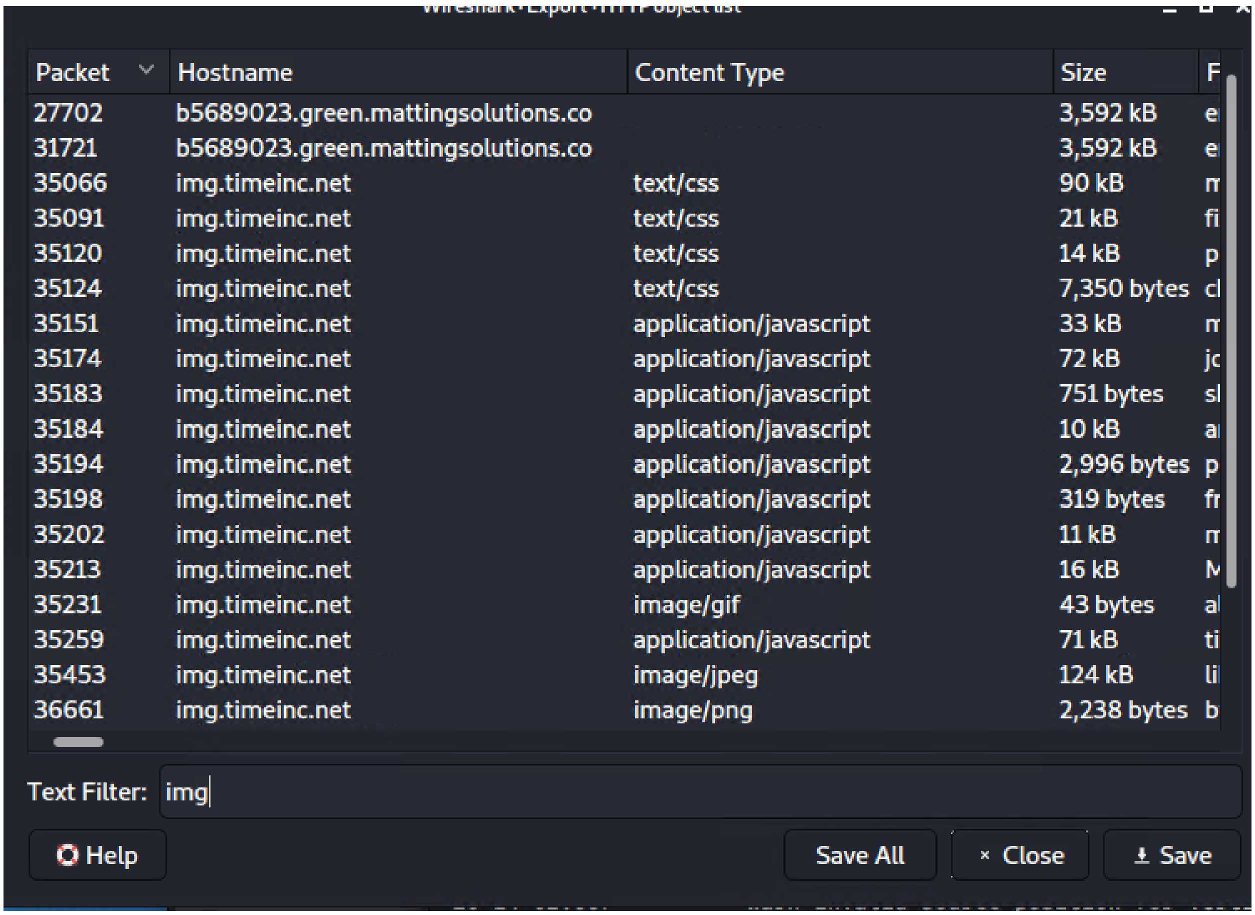
Let’s look at the destination or our user.



```
Internet Protocol Version 4, Src: Rotterdam-PC.mind-hammer.net (172.16.4.205), Dst: b5689023.green.mattingsolutions.co (185.243.115.84)
```

Green.mattingsolutions. We know it has to be an image file so let’s go to:

- File
- Export Objects > HTTP
- In the text filter let’s search for “img”



| Packet | Hostname | Content Type | Size | F |
|---|---|---|---|---|
| 27702 | b5689023.green.mattingsolutions.co | | 3,592 kB | e |
| 31721 | b5689023.green.mattingsolutions.co | | 3,592 kB | e |
| 35066 | img.timeinc.net | text/css | 90 kB | m |
| 35091 | img.timeinc.net | text/css | 21 kB | fi |
| 35120 | img.timeinc.net | text/css | 14 kB | p |
| 35124 | img.timeinc.net | text/css | 7,350 bytes | cl |
| 35151 | img.timeinc.net | application/javascript | 33 kB | m |
| 35174 | img.timeinc.net | application/javascript | 72 kB | jc |
| 35183 | img.timeinc.net | application/javascript | 751 bytes | sl |
| 35184 | img.timeinc.net | application/javascript | 10 kB | ai |
| 35194 | img.timeinc.net | application/javascript | 2,996 bytes | p |
| 35198 | img.timeinc.net | application/javascript | 319 bytes | fr |
| 35202 | img.timeinc.net | application/javascript | 11 kB | m |
| 35213 | img.timeinc.net | application/javascript | 16 kB | M |
| 35231 | img.timeinc.net | image/gif | 43 bytes | al |
| 35259 | img.timeinc.net | application/javascript | 71 kB | ti |
| 35453 | img.timeinc.net | image/jpeg | 124 kB | li |
| 36661 | img.timeinc.net | image/png | 2,238 bytes | b |

Text Filter: img

Right at the top there’s two files called green.mattingsolutions. Let’s try the one labeled 27702.

## 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:

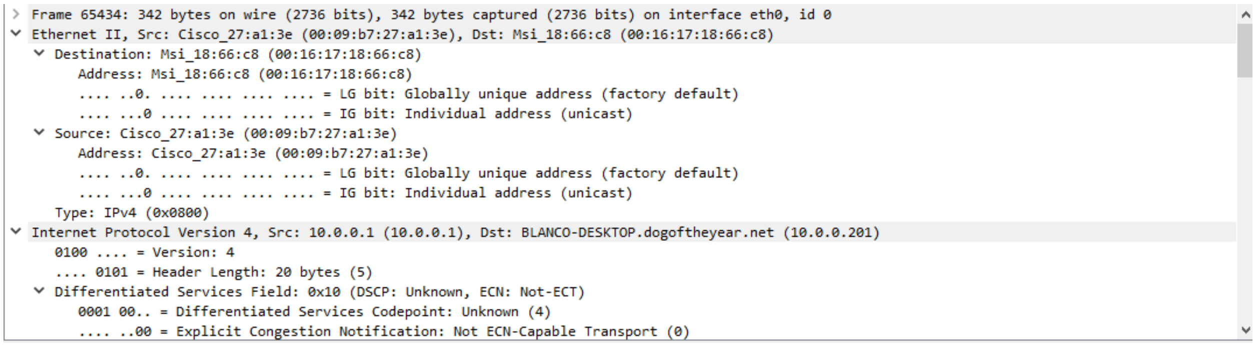
- The machines using torrents live in the range `10.0.0.0/24` and are clients of an AD domain.
- The DC of this domain lives at `10.0.0.2` and is named DogOfTheYear-DC.
- The DC is associated with the domain dogoftheyear.net.

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`:

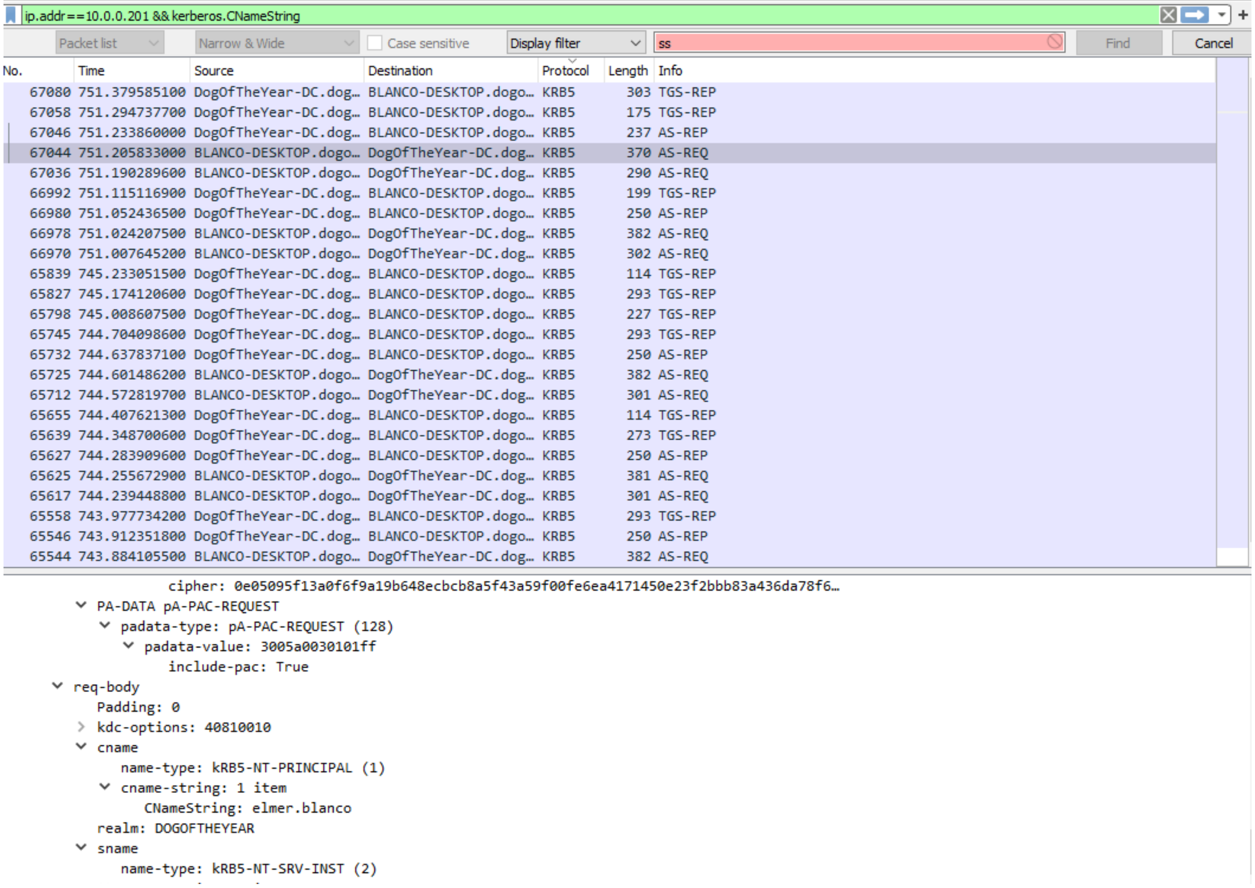
  - MAC address: 00:16:17:18:66:c8
  - Windows username: elmer.blanco
  - OS version

Filter for MAC address: ip.addr==10.0.0.201 && dhcp



```
> Frame 65434: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface eth0, id 0
v Ethernet II, Src: Cisco_27:a1:3e (00:09:b7:27:a1:3e), Dst: Msi_18:66:c8 (00:16:17:18:66:c8)
  v Destination: Msi_18:66:c8 (00:16:17:18:66:c8)
      Address: Msi_18:66:c8 (00:16:17:18:66:c8)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
      Address: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 10.0.0.1 (10.0.0.1), Dst: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
      0001 00.. = Differentiated Services Codepoint: Unknown (4)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
```

Wireshark Filter for Username: ip.addr==10.0.0.201 && kerberos.CNameString



```
ip.addr==10.0.0.201 && kerberos.CNameString
ss

No.   Time         Source                   Destination              Protocol  Length Info
67080 751.379585100 DogOfTheYear-DC.dog… BLANCO-DESKTOP.dogo… KRB5      303 TGS-REP
67058 751.294737700 DogOfTheYear-DC.dog… BLANCO-DESKTOP.dogo… KRB5      175 TGS-REP
67046 751.233860000 DogOfTheYear-DC.dog… BLANCO-DESKTOP.dogo… KRB5      237 AS-REP
67044 751.205833000 BLANCO-DESKTOP.dogo… DogOfTheYear-DC.dog… KRB5      370 AS-REQ
67036 751.190289600 BLANCO-DESKTOP.dogo… DogOfTheYear-DC.dog… KRB5      290 AS-REQ
66992 751.115116900 DogOfTheYear-DC.dog… BLANCO-DESKTOP.dogo… KRB5      199 TGS-REP
66980 751.052436500 DogOfTheYear-DC.dog… BLANCO-DESKTOP.dogo… KRB5      250 AS-REP
66978 751.024207500 BLANCO-DESKTOP.dogo… DogOfTheYear-DC.dog… KRB5      382 AS-REQ
66970 751.007645200 BLANCO-DESKTOP.dogo… DogOfTheYear-DC.dog… KRB5      302 AS-REQ
65839 745.233051500 DogOfTheYear-DC.dog… BLANCO-DESKTOP.dogo… KRB5      114 TGS-REP
65827 745.174120600 DogOfTheYear-DC.dog… BLANCO-DESKTOP.dogo… KRB5      293 TGS-REP
65798 745.008607500 DogOfTheYear-DC.dog… BLANCO-DESKTOP.dogo… KRB5      227 TGS-REP
65745 744.704098600 DogOfTheYear-DC.dog… BLANCO-DESKTOP.dogo… KRB5      293 TGS-REP
65732 744.637837100 DogOfTheYear-DC.dog… BLANCO-DESKTOP.dogo… KRB5      250 AS-REP
65725 744.601486200 BLANCO-DESKTOP.dogo… DogOfTheYear-DC.dog… KRB5      382 AS-REQ
65712 744.572819700 BLANCO-DESKTOP.dogo… DogOfTheYear-DC.dog… KRB5      301 AS-REQ
65655 744.407621300 DogOfTheYear-DC.dog… BLANCO-DESKTOP.dogo… KRB5      114 TGS-REP
65639 744.348700600 DogOfTheYear-DC.dog… BLANCO-DESKTOP.dogo… KRB5      273 TGS-REP
65627 744.283909600 DogOfTheYear-DC.dog… BLANCO-DESKTOP.dogo… KRB5      250 AS-REP
65625 744.255672900 BLANCO-DESKTOP.dogo… DogOfTheYear-DC.dog… KRB5      381 AS-REQ
65617 744.239448800 BLANCO-DESKTOP.dogo… DogOfTheYear-DC.dog… KRB5      301 AS-REQ
65558 743.977734200 DogOfTheYear-DC.dog… BLANCO-DESKTOP.dogo… KRB5      293 TGS-REP
65546 743.912351800 DogOfTheYear-DC.dog… BLANCO-DESKTOP.dogo… KRB5      250 AS-REP
65544 743.884105500 BLANCO-DESKTOP.dogo… DogOfTheYear-DC.dog… KRB5      382 AS-REQ
```

```
                cipher: 0e05095f13a0f6f9a19b648ecbcb8a5f43a59f00fe6ea4171450e23f2bbb83a436da78f6…
        v PA-DATA pA-PAC-REQUEST
          v padata-type: pA-PAC-REQUEST (128)
            v padata-value: 3005a0030101ff
                include-pac: True
      v req-body
          Padding: 0
        > kdc-options: 40810010
        v cname
            name-type: kRB5-NT-PRINCIPAL (1)
          v cname-string: 1 item
              CNameString: elmer.blanco
          realm: DOGOFTHEYEAR
        v sname
            name-type: kRB5-NT-SRV-INST (2)
```

Elmer.blanco

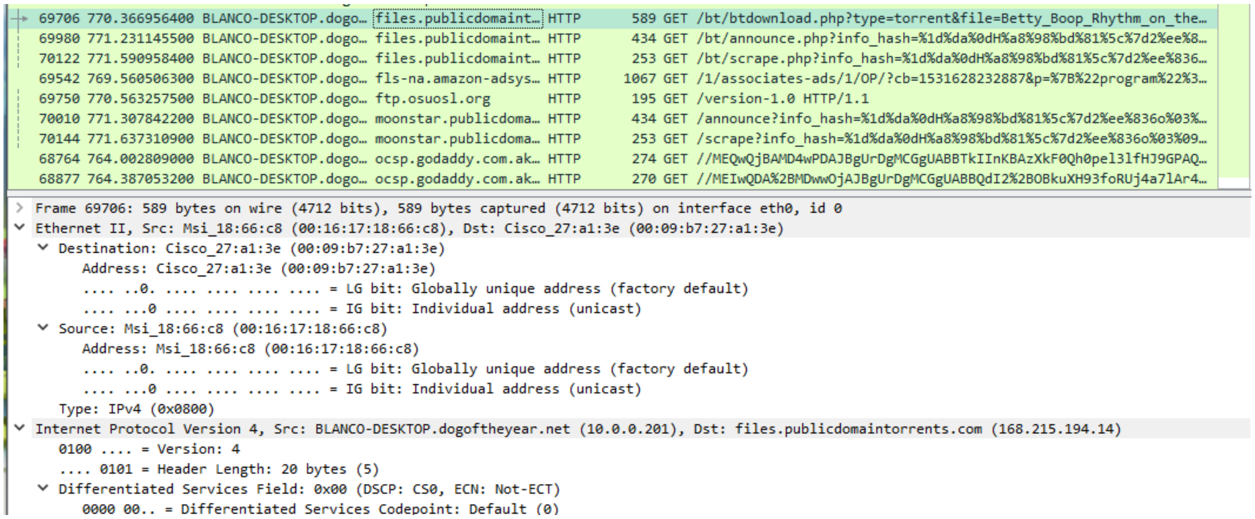
OS Type and Version: ip.addr ==  10.0.0.201 && http.request

2. Which torrent file did the user download?

Filter: ip.addr==10.0.0.201 && http.request.method==GET

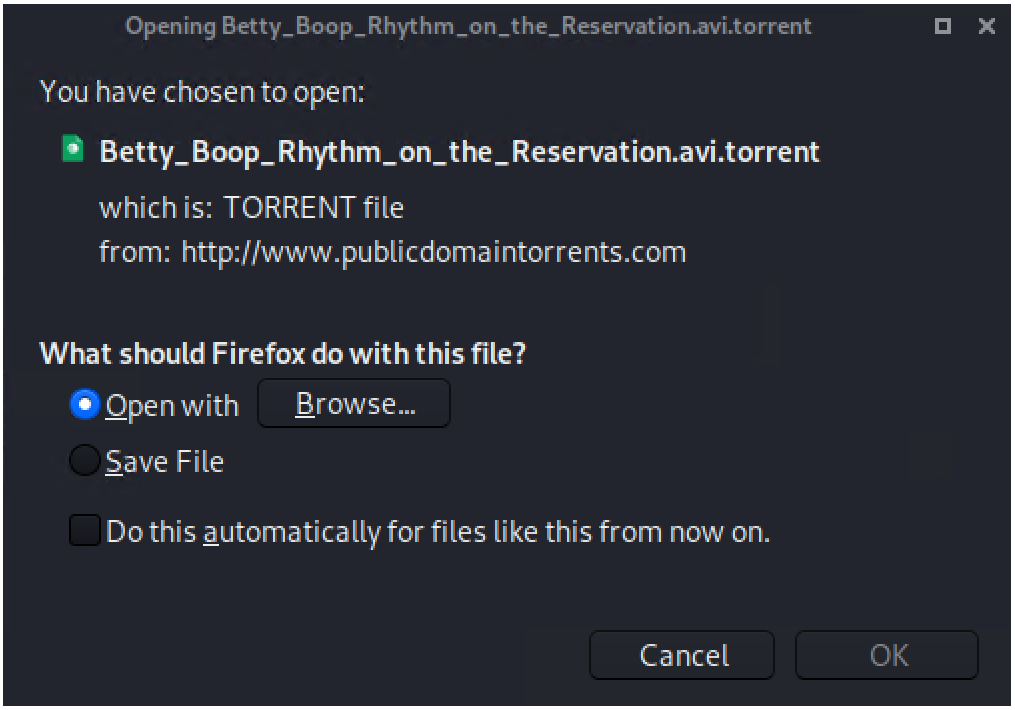
Sort the packets by “Destination” and search for files.publicdomaintorrents.com (168.215.194.14)

Look through the packets and find Download requests



```
69706 770.366956400 BLANCO-DESKTOP.dogo… files.publicdomaint… HTTP      589 GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the…
69980 771.231145500 BLANCO-DESKTOP.dogo… files.publicdomaint… HTTP      434 GET /bt/announce.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%8…
70122 771.590958400 BLANCO-DESKTOP.dogo… files.publicdomaint… HTTP      253 GET /bt/scrape.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836…
69542 769.560506300 BLANCO-DESKTOP.dogo… fls-na.amazon-adsys… HTTP     1067 GET /1/associates-ads/1/OP/?cb=1531628232887&p=%7B%22program%22%3…
69750 770.563257500 BLANCO-DESKTOP.dogo… ftp.osuosl.org       HTTP      195 GET /version-1.0 HTTP/1.1
70010 771.307842200 BLANCO-DESKTOP.dogo… moonstar.publicdoma… HTTP      434 GET /announce?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%…
70144 771.637310900 BLANCO-DESKTOP.dogo… moonstar.publicdoma… HTTP      253 GET /scrape?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%09…
68764 764.002809000 BLANCO-DESKTOP.dogo… ocsp.godaddy.com.ak… HTTP      274 GET //MEQwQjBAMD4wPDAJBgUrDgMCGgUABBTkIInKBAzXkF0Qh0pel3lfHJ9GPAQ…
68877 764.387053200 BLANCO-DESKTOP.dogo… ocsp.godaddy.com.ak… HTTP      270 GET //MEIwQDA%2BMDwwOjAJBgUrDgMCGgUABBQdI2%2BOBkuXH93foRUj4a7lAr4…

> Frame 69706: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits) on interface eth0, id 0
v Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
  v Destination: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
      Address: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: Msi_18:66:c8 (00:16:17:18:66:c8)
      Address: Msi_18:66:c8 (00:16:17:18:66:c8)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201), Dst: files.publicdomaintorrents.com (168.215.194.14)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
```



Opening Betty_Boop_Rhythm_on_the_Reservation.avi.torrent

You have chosen to open:

**Betty_Boop_Rhythm_on_the_Reservation.avi.torrent**

which is: TORRENT file
from: http://www.publicdomaintorrents.com

**What should Firefox do with this file?**

● Open with

○ Save File

□ Do this automatically for files like this from now on.

This is the downloaded torrent file.