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:

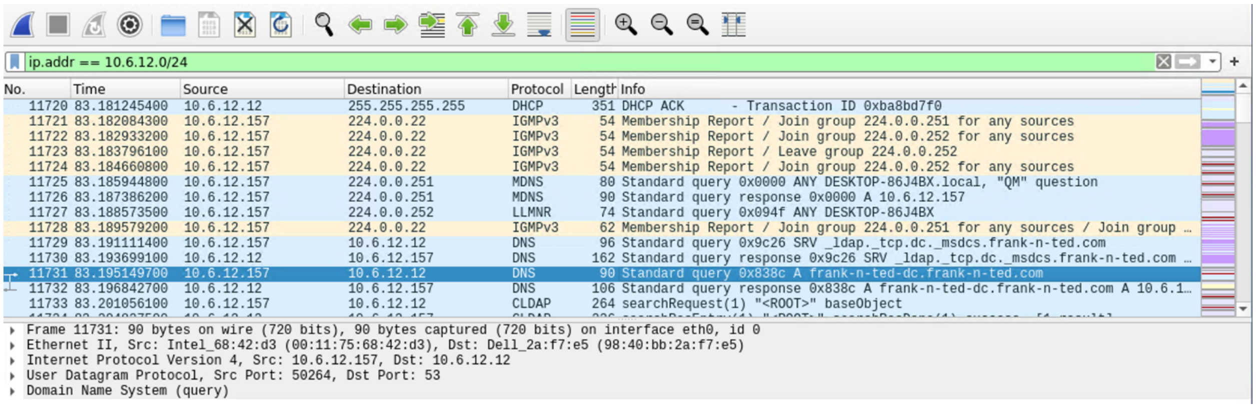
- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.
- Their IP addresses are somewhere in the range 10.6.12.0/24.

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

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

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

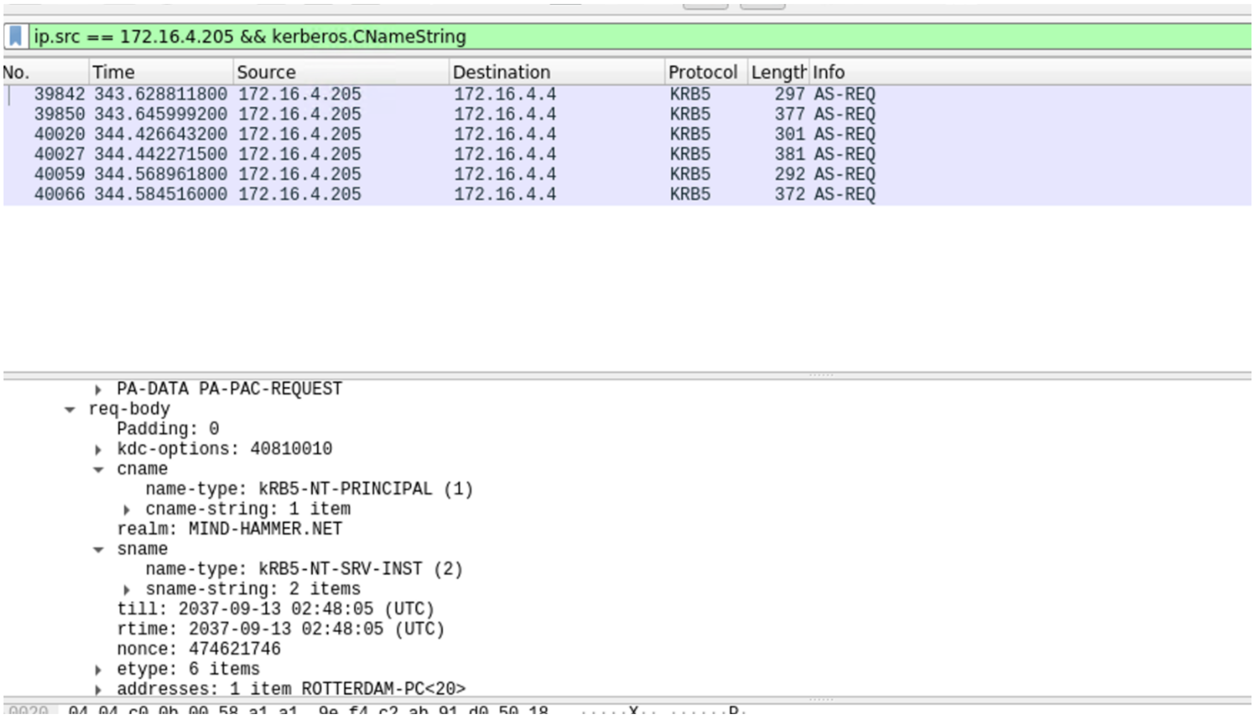
   Filter used in Wireshark: ip.addr==10.6.12.0/24



```
ip.addr == 10.6.12.0/24

No.   Time         Source        Destination      Protocol Length Info
11720 83.181245400 10.6.12.12    255.255.255.255  DHCP     351 DHCP ACK      - Transaction ID 0xba8bd7f0
11721 83.182084300 10.6.12.157   224.0.0.22       IGMPv3    54 Membership Report / Join group 224.0.0.251 for any sources
11722 83.182933200 10.6.12.157   224.0.0.22       IGMPv3    54 Membership Report / Join group 224.0.0.252 for any sources
11723 83.183796100 10.6.12.157   224.0.0.22       IGMPv3    54 Membership Report / Leave group 224.0.0.252
11724 83.184660800 10.6.12.157   224.0.0.22       IGMPv3    54 Membership Report / Join group 224.0.0.252 for any sources
11725 83.185944800 10.6.12.157   224.0.0.251      MDNS      80 Standard query 0x0000 ANY DESKTOP-86J4BX.local, "QM" question
11726 83.187386200 10.6.12.157   224.0.0.251      MDNS      90 Standard query response 0x0000 A 10.6.12.157
11727 83.188573500 10.6.12.157   224.0.0.252      LLMNR     74 Standard query 0x094f ANY DESKTOP-86J4BX
11728 83.189579200 10.6.12.157   224.0.0.22       IGMPv3    62 Membership Report / Join group 224.0.0.251 for any sources / Join group …
11729 83.191111400 10.6.12.157   10.6.12.12       DNS       96 Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
11730 83.193699100 10.6.12.12    10.6.12.157      DNS      162 Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com …
11731 83.195149700 10.6.12.157   10.6.12.12       DNS       90 Standard query 0x838c A frank-n-ted-dc.frank-n-ted.com
11732 83.196842700 10.6.12.12    10.6.12.157      DNS      106 Standard query response 0x838c A frank-n-ted-dc.frank-n-ted.com A 10.6.1…
11733 83.201056100 10.6.12.157   10.6.12.12       CLDAP    264 searchRequest(1) "<ROOT>" baseObject

▸ Frame 11731: 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)

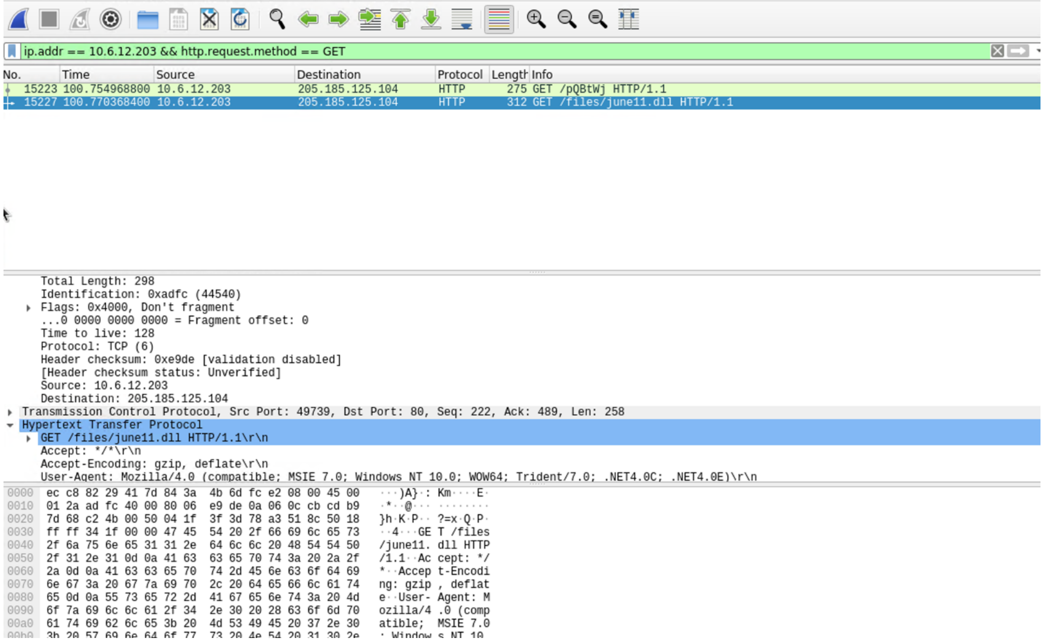


```
ip.src == 172.16.4.205 && kerberos.CNameString
```

```
No.    Time          Source        Destination  Protocol Length Info
 39842 343.628811800 172.16.4.205  172.16.4.4   KRB5      297 AS-REQ
 39850 343.645999200 172.16.4.205  172.16.4.4   KRB5      377 AS-REQ
 40020 344.426643200 172.16.4.205  172.16.4.4   KRB5      301 AS-REQ
 40027 344.442271500 172.16.4.205  172.16.4.4   KRB5      381 AS-REQ
 40059 344.568961800 172.16.4.205  172.16.4.4   KRB5      292 AS-REQ
 40066 344.584516000 172.16.4.205  172.16.4.4   KRB5      372 AS-REQ
```

```
        PA-DATA PA-PAC-REQUEST
    req-body
        Padding: 0
        kdc-options: 40810010
        cname
            name-type: kRB5-NT-PRINCIPAL (1)
            cname-string: 1 item
        realm: MIND-HAMMER.NET
        sname
            name-type: kRB5-NT-SRV-INST (2)
            sname-string: 2 items
        till: 2037-09-13 02:48:05 (UTC)
        rtime: 2037-09-13 02:48:05 (UTC)
        nonce: 474621746
        etype: 6 items
        addresses: 1 item ROTTERDAM-PC<20>
0020  04 04 c0 0b 00 58 a1 a1  9e f4 c2 ab 91 d0 50 18   .....X.. ......P.
```

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: june11.dll
    b. Filter used in Wireshark: ip.addr==10.6.12.203 and http.request.method==GET



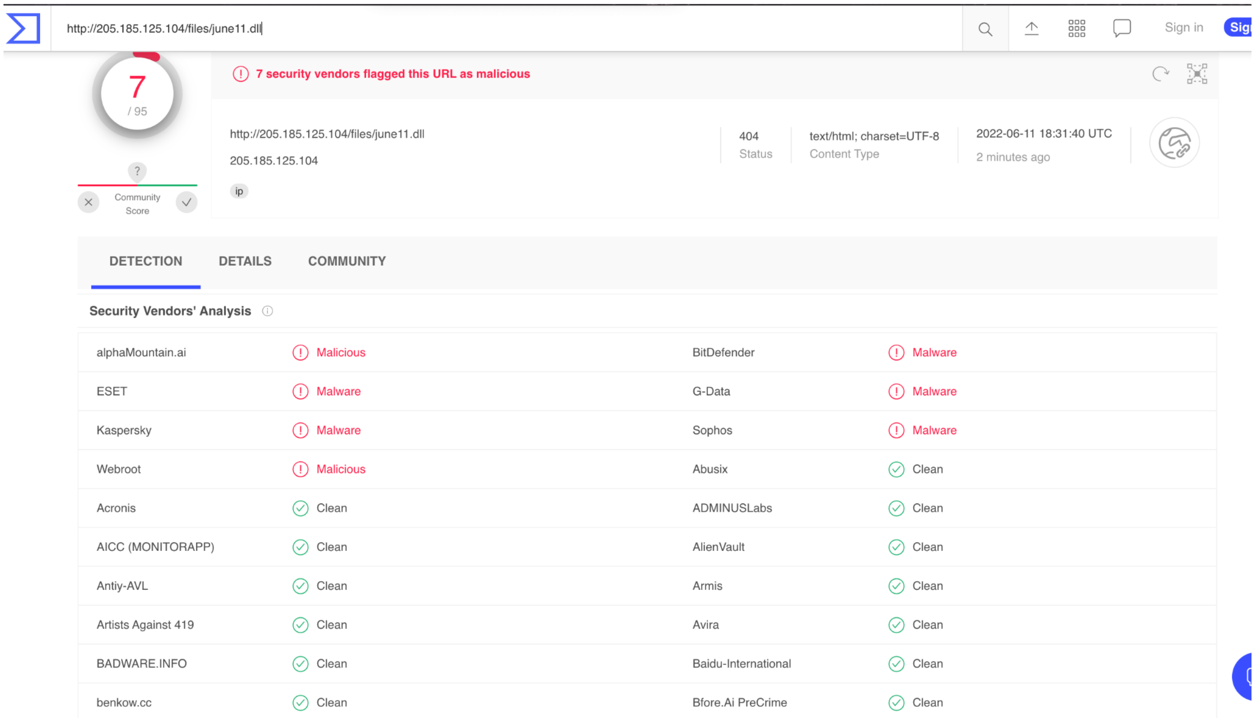
```
ip.addr == 10.6.12.203 && http.request.method == GET
```

```
No.    Time           Source       Destination     Protocol Length Info
 15223 100.754968800 10.6.12.203  205.185.125.104 HTTP     275 GET /pQBtWj HTTP/1.1
 15227 100.770368400 10.6.12.203  205.185.125.104 HTTP     312 GET /files/june11.dll HTTP/1.1
```

```
    Total Length: 298
    Identification: 0xadfc (44540)
  ▸ Flags: 0x4000, Don't fragment
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xe9de [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.6.12.203
    Destination: 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
```

```
0000  ec c8 82 29 41 7d 84 3a  4b 6d fc e2 08 00 45 00   ···)A}·: Km····E·
0010  01 2a ad fc 40 00 80 06  e9 de 0a 06 0c cb cd b9   ·*··@··· ········
0020  7d 68 c2 4b 00 50 04 1f  3f 3d 78 a3 51 8c 50 18   }h·K·P·· ?=x·Q·P·
0030  ff ff 34 1f 00 00 47 45  54 20 2f 66 69 6c 65 73   ··4···GE T /files
0040  2f 6a 75 6e 65 31 31 2e  64 6c 6c 20 48 54 54 50   /june11. dll HTTP
0050  2f 31 2e 31 0d 0a 41 63  63 65 70 74 3a 20 2a 2f   /1.1··Ac cept: */
0060  2a 0d 0a 41 63 63 65 70  74 2d 45 6e 63 6f 64 69   *··Accep t-Encodi
0070  6e 67 3a 20 67 7a 69 70  2c 20 64 65 66 6c 61 74   ng: gzip , deflat
0080  65 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   e··User- Agent: M
0090  6f 7a 69 6c 6c 61 2f 34  2e 30 20 28 63 6f 6d 70   ozilla/4 .0 (comp
00a0  61 74 69 62 6c 65 3b 20  4d 53 49 45 20 37 2e 30   atible;  MSIE 7.0
00b0  3b 20 57 69 6e 64 6f 77  73 20 4e 54 20 31 30 2e   ; Window s NT 10
```

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



(!) 7 security vendors flagged this URL as malicious

http://205.185.125.104/files/june11.dll

205.185.125.104

ip

404
Status

text/html; charset=UTF-8
Content Type

2022-06-11 18:31:40 UTC
2 minutes ago

Security Vendors' Analysis

alphaMountain.ai	(!) Malicious	BitDefender	(!) Malware
ESET	(!) Malware	G-Data	(!) Malware
Kaspersky	(!) Malware	Sophos	(!) Malware
Webroot	(!) Malicious	Abusix	✓ Clean
Acronis	✓ Clean	ADMINUSLabs	✓ Clean
AICC (MONITORAPP)	✓ Clean	AlienVault	✓ Clean
Antiy-AVL	✓ Clean	Armis	✓ Clean
Artists Against 419	✓ Clean	Avira	✓ Clean
BADWARE.INFO	✓ Clean	Baidu-International	✓ Clean
benkow.cc	✓ Clean	Bfore.Ai PreCrime	✓ Clean

- This type of malware is classified as a Trojan

Vulnerable Windows Machines

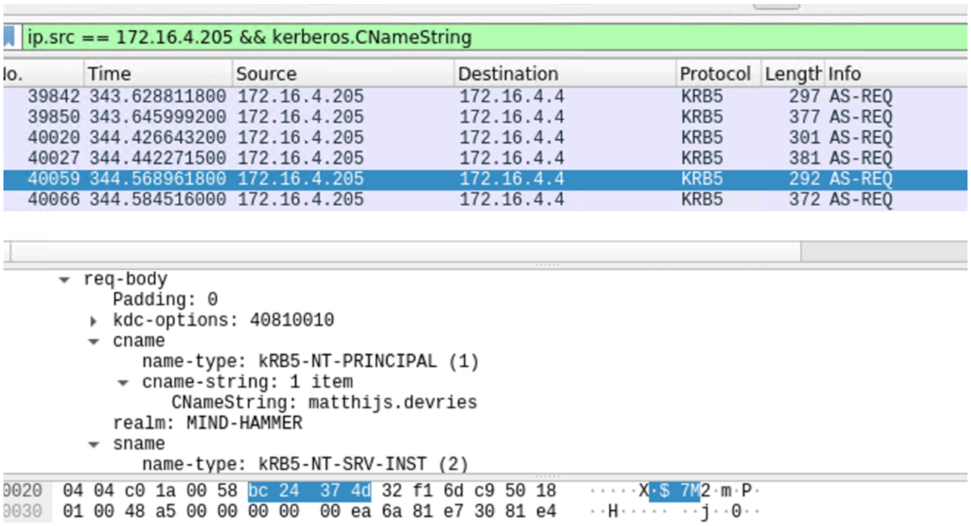
The Security team received reports of an infected Windows host on the network. They know the following:

- 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

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



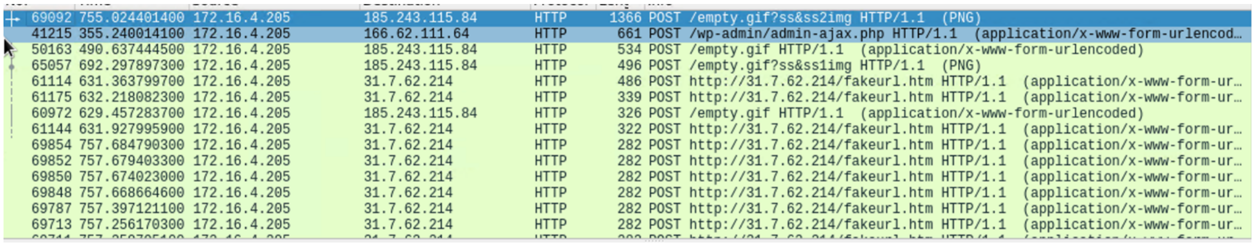
```
ip.src == 172.16.4.205 && kerberos.CNameString

lo.    Time             Source        Destination   Protocol Length Info
 39842 343.628811800 172.16.4.205  172.16.4.4    KRB5      297 AS-REQ
 39850 343.645999200 172.16.4.205  172.16.4.4    KRB5      377 AS-REQ
 40020 344.426643200 172.16.4.205  172.16.4.4    KRB5      301 AS-REQ
 40027 344.442271500 172.16.4.205  172.16.4.4    KRB5      381 AS-REQ
 40059 344.568961800 172.16.4.205  172.16.4.4    KRB5      292 AS-REQ
 40066 344.584516000 172.16.4.205  172.16.4.4    KRB5      372 AS-REQ
```

```
    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
        name-type: kRB5-NT-SRV-INST (2)
```

```
0020  04 04 c0 1a 00 58 bc 24  37 4d 32 f1 6d c9 50 18   ·····X·$ 7M2·m·P·
0030  01 00 48 a5 00 00 00 00  00 ea 6a 81 e7 30 81 e4   ··H·····  ··j··0··
```

    -

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.



```
69092 755.024401400 172.16.4.205    185.243.115.84   HTTP    1366 POST /empty.gif?ss&ss2img HTTP/1.1  (PNG)
41215 355.240014100 172.16.4.205    166.62.111.64    HTTP     661 POST /wp-admin/admin-ajax.php HTTP/1.1  (application/x-www-form-urlencod…
50163 490.637444500 172.16.4.205    185.243.115.84   HTTP     534 POST /empty.gif HTTP/1.1  (application/x-www-form-urlencoded)
65057 692.297897300 172.16.4.205    185.243.115.84   HTTP     496 POST /empty.gif?ss&ss1img HTTP/1.1  (PNG)
61114 631.363799700 172.16.4.205    31.7.62.214      HTTP     486 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-form-ur…
61175 632.218082300 172.16.4.205    31.7.62.214      HTTP     339 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-form-ur…
60972 629.457283700 172.16.4.205    185.243.115.84   HTTP     326 POST /empty.gif HTTP/1.1  (application/x-www-form-urlencoded)
61144 631.927995900 172.16.4.205    31.7.62.214      HTTP     322 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-form-ur…
69854 757.684790300 172.16.4.205    31.7.62.214      HTTP     282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-form-ur…
69852 757.679403300 172.16.4.205    31.7.62.214      HTTP     282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-form-ur…
69850 757.674023000 172.16.4.205    31.7.62.214      HTTP     282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-form-ur…
69848 757.668664600 172.16.4.205    31.7.62.214      HTTP     282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-form-ur…
69787 757.397121100 172.16.4.205    31.7.62.214      HTTP     282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-form-ur…
69713 757.256170300 172.16.4.205    31.7.62.214      HTTP     282 POST http://31.7.62.214/fakeurl.htm HTTP/1.1  (application/x-www-form-ur…
```

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.

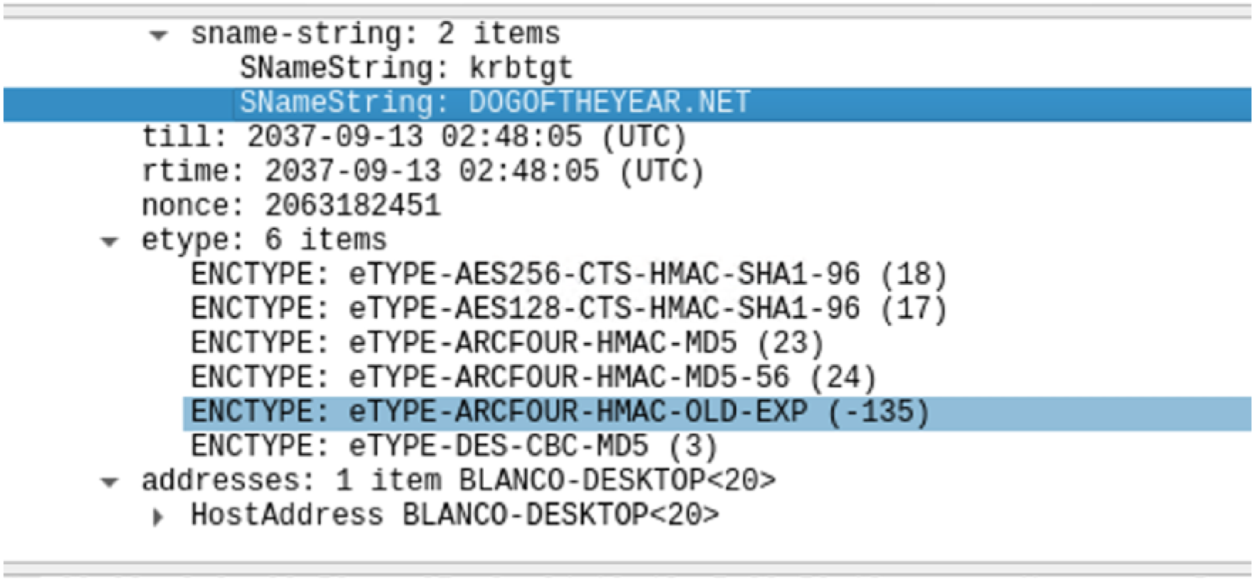
IT shared the following about the torrent activity:

- 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 in your Network Report:

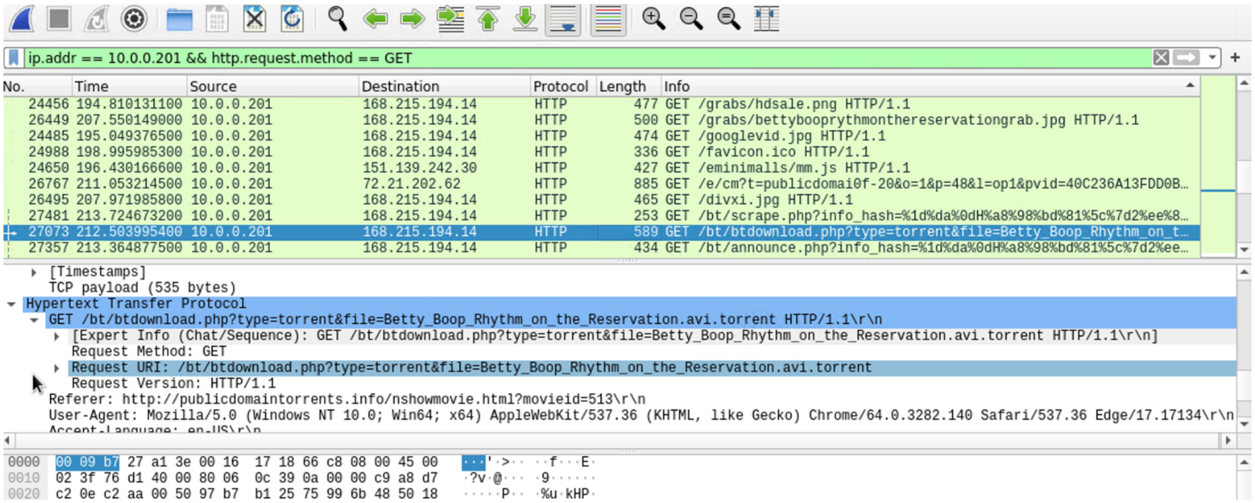
1. Find the following information about the machine with IP address 10.0.0.201:

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



```
    ▾ sname-string: 2 items
          SNameString: krbtgt
          SNameString: DOGOFTHEYEAR.NET
  till: 2037-09-13 02:48:05 (UTC)
  rtime: 2037-09-13 02:48:05 (UTC)
  nonce: 2063182451
▾ etype: 6 items
      ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
      ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
      ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
      ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (24)
      ENCTYPE: eTYPE-ARCFOUR-HMAC-OLD-EXP (-135)
      ENCTYPE: eTYPE-DES-CBC-MD5 (3)
▾ addresses: 1 item BLANCO-DESKTOP<20>
    ▸ HostAddress BLANCO-DESKTOP<20>
```

2. Which torrent file did the user download?
    - The torrent file is Betty_Boop_Rythm_on_the_Reservation.avi.torrent



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

```
No.   Time          Source       Destination     Protocol Length Info
24456 194.810131100 10.0.0.201   168.215.194.14  HTTP     477 GET /grabs/hdsale.png HTTP/1.1
26449 207.550149000 10.0.0.201   168.215.194.14  HTTP     500 GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1
24485 195.049376500 10.0.0.201   168.215.194.14  HTTP     474 GET /googlevid.jpg HTTP/1.1
24988 198.995985300 10.0.0.201   168.215.194.14  HTTP     336 GET /favicon.ico HTTP/1.1
24650 196.430166600 10.0.0.201   151.139.242.30  HTTP     427 GET /eminimalls/mm.js HTTP/1.1
26767 211.053214500 10.0.0.201   72.21.202.62    HTTP     885 GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=op1&pvid=40C236A13FDD0B…
26495 207.971985800 10.0.0.201   168.215.194.14  HTTP     465 GET /divxi.jpg HTTP/1.1
27481 213.724673200 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%8…
27073 212.503995400 10.0.0.201   168.215.194.14  HTTP     589 GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_t…
27357 213.364877500 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…
```

```
    ▸ [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
    ▸ [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
```

```
0000  00 09 b7 27 a1 3e 00 16  17 18 66 c8 08 00 45 00   ···'·>·· ··f···E·
0010  02 3f 76 d1 40 00 80 06  0c 39 0a 00 00 c9 a8 d7   ·?v·@··· ·9······
0020  c2 0e c2 aa 00 50 97 b7  b1 25 75 99 6b 48 50 18   ·····P·· ·%u·kHP·
```