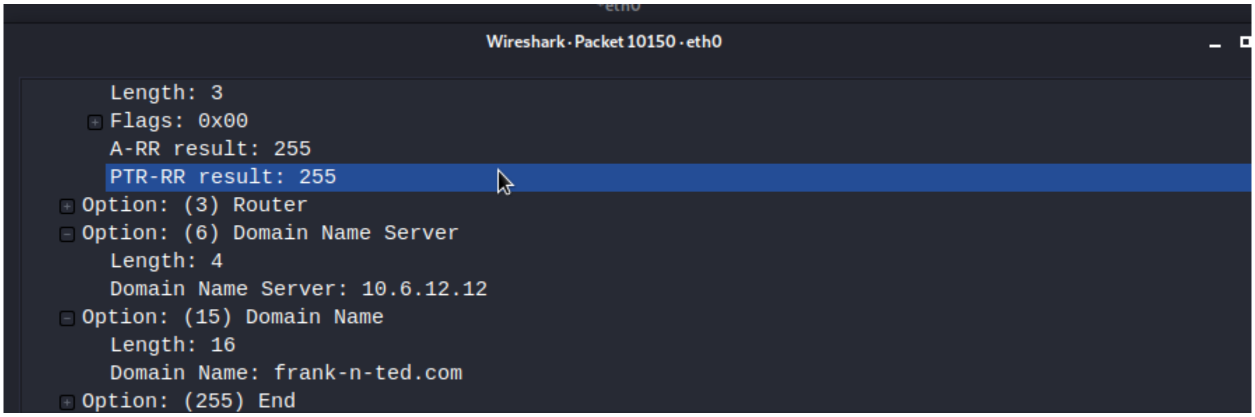
Network Forensic Analysis Report

TODO Complete this report as you complete the Network Activity on Day 3 of class.

Time Thieves

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

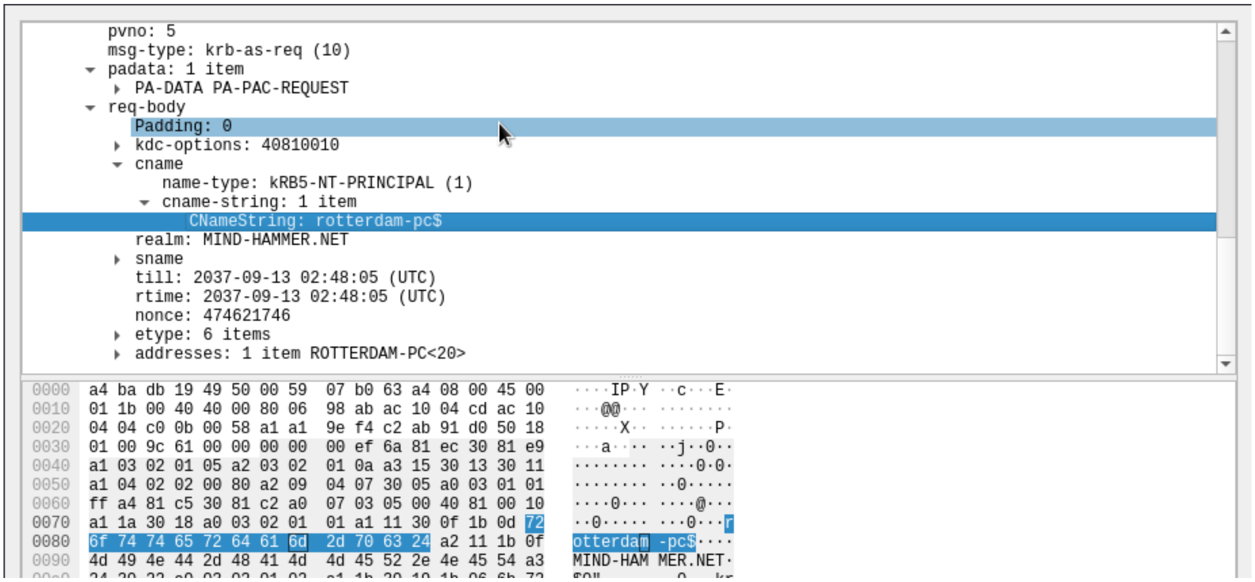
1. What is the domain name of the users' custom site? frank-n-ted.com
2. What is the IP address of the Domain Controller (DC) of the AD network? 10.6.12.12
3. What is the name of the malware downloaded to the 10.6.12.203 machine? jun11.dll
    - Once you have found the file, export it to your Kali machine's desktop.
4. Upload the file to VirusTotal.com.
5. What kind of malware is this classified as? Trojan



```
        Length: 3
      ⊞ Flags: 0x00
        A-RR result: 255
        PTR-RR result: 255
    ⊞ Option: (3) Router
    ⊟ Option: (6) Domain Name Server
        Length: 4
        Domain Name Server: 10.6.12.12
    ⊟ Option: (15) Domain Name
        Length: 16
        Domain Name: frank-n-ted.com
    ⊞ Option: (255) End
```

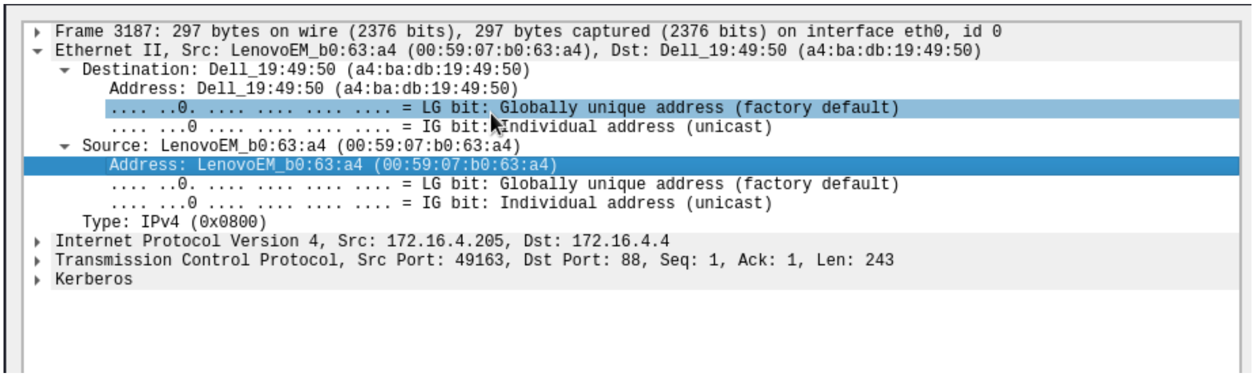
Vulnerable Windows Machine

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



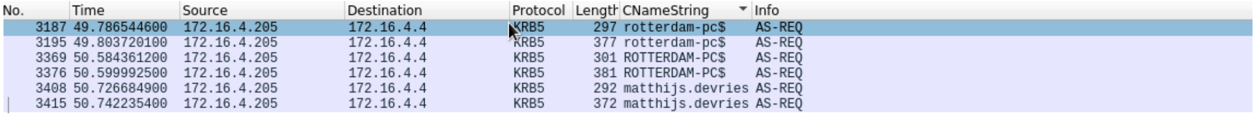
```
        pvno: 5
        msg-type: krb-as-req (10)
      ▾ padata: 1 item
        ▸ PA-DATA PA-PAC-REQUEST
      ▾ req-body
          Padding: 0
        ▸ kdc-options: 40810010
        ▾ cname
            name-type: kRB5-NT-PRINCIPAL (1)
          ▾ cname-string: 1 item
              CNameString: rotterdam-pc$
          realm: MIND-HAMMER.NET
        ▸ sname
          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>
```

```
0000  a4 ba db 19 49 50 00 59  07 b0 63 a4 08 00 45 00   ····IP·Y ··c···E·
0010  01 1b 00 40 40 00 80 06  98 ab ac 10 04 cd ac 10   ···@@··· ········
0020  04 04 c0 0b 00 58 a1 a1  9e f4 c2 ab 91 d0 50 18   ·····X·· ······P·
0030  01 00 9c 61 00 00 00 00  00 ef 6a 81 ec 30 81 e9   ···a···· ··j··0··
0040  a1 03 02 01 05 a2 03 02  01 0a a3 15 30 13 30 11   ········ ····0·0·
0050  a1 04 02 02 00 80 a2 09  04 07 30 05 a0 03 01 01   ········ ··0·····
0060  ff a4 81 c5 30 81 c2 a0  07 03 05 00 40 81 00 10   ····0··· ····@···
0070  a1 1a 30 18 a0 03 02 01  01 a1 11 30 0f 1b 0d 72   ··0····· ···0···r
0080  6f 74 74 65 72 64 61 6d  2d 70 63 24 a2 11 1b 0f   otterdam -pc$····
0090  4d 49 4e 44 2d 48 41 4d  4d 45 52 2e 4e 45 54 a3   MIND-HAM MER.NET·
```

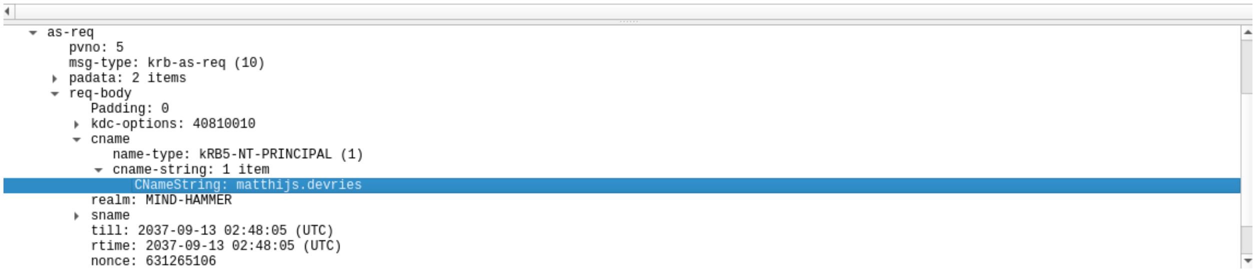


```
▸ Frame 3187: 297 bytes on wire (2376 bits), 297 bytes captured (2376 bits) on interface eth0, id 0
▾ Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Dell_19:49:50 (a4:ba:db:19:49:50)
  ▾ Destination: Dell_19:49:50 (a4:ba:db:19:49:50)
      Address: Dell_19:49:50 (a4:ba:db:19:49:50)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ 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)
▸ Internet Protocol Version 4, Src: 172.16.4.205, Dst: 172.16.4.4
▸ Transmission Control Protocol, Src Port: 49163, Dst Port: 88, Seq: 1, Ack: 1, Len: 243
▸ Kerberos
```

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



```
No.    Time          Source        Destination   Protocol Length CNameString       Info
  3187 49.786544600  172.16.4.205  172.16.4.4    KRB5     297 rotterdam-pc$     AS-REQ
  3195 49.803720100  172.16.4.205  172.16.4.4    KRB5     377 rotterdam-pc$     AS-REQ
  3369 50.584361200  172.16.4.205  172.16.4.4    KRB5     301 ROTTERDAM-PC$     AS-REQ
  3376 50.599992500  172.16.4.205  172.16.4.4    KRB5     381 ROTTERDAM-PC$     AS-REQ
  3408 50.726684900  172.16.4.205  172.16.4.4    KRB5     292 matthijs.devries  AS-REQ
  3415 50.742235400  172.16.4.205  172.16.4.4    KRB5     372 matthijs.devries  AS-REQ
```



```
▾ 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: matthijs.devries
      realm: MIND-HAMMER
    ▸ sname
      till: 2037-09-13 02:48:05 (UTC)
      rtime: 2037-09-13 02:48:05 (UTC)
      nonce: 631265106
```

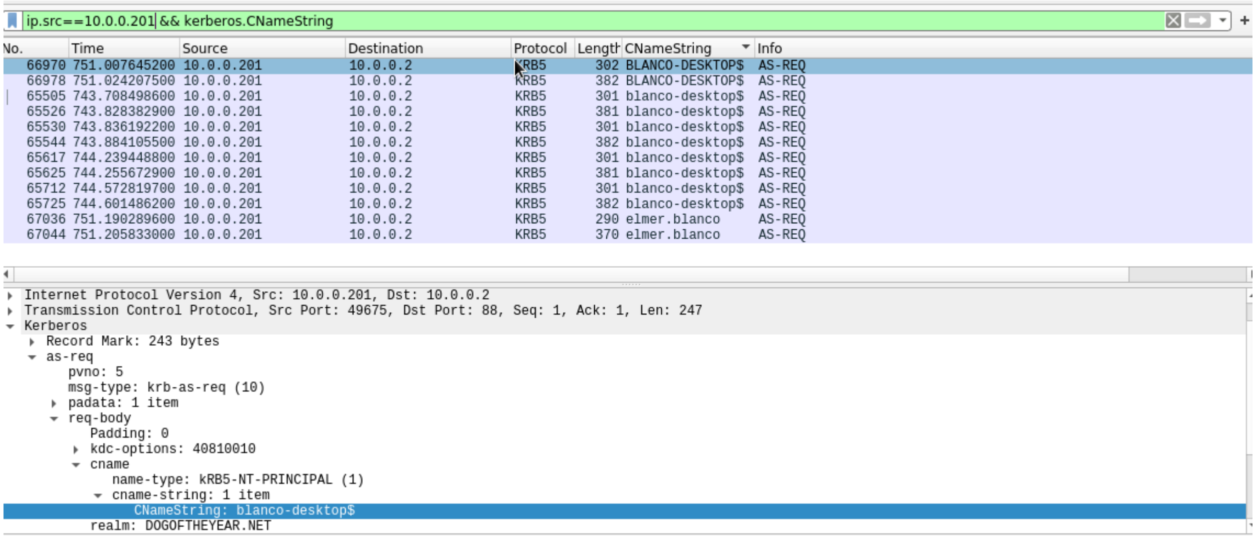
3. What are the IP addresses used in the actual infection traffic? 172.16.4.205, 185.243.115.84

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

Illegal Downloads

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

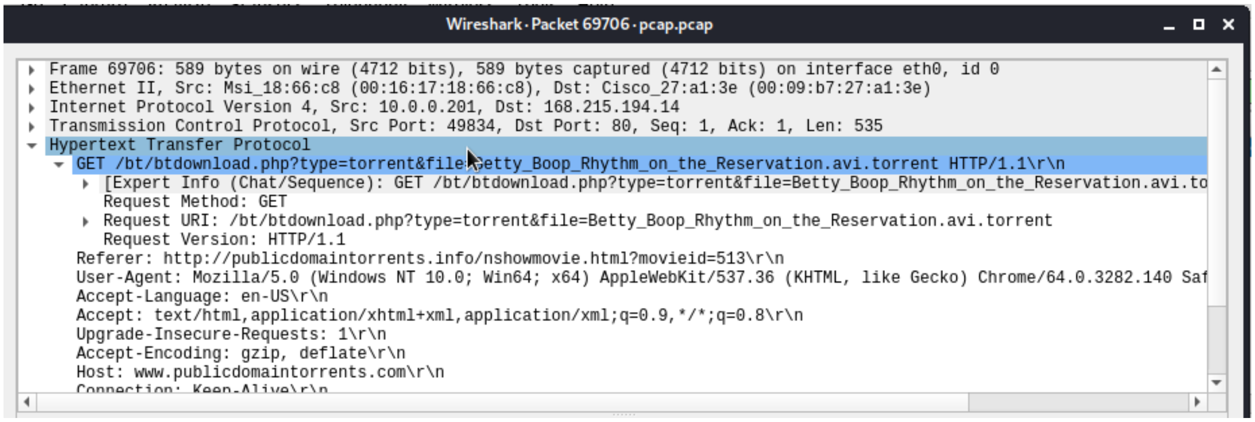


```
ip.src==10.0.0.201 && kerberos.CNameString

No.   Time           Source       Destination   Protocol Length CNameString     Info
66970 751.007645200 10.0.0.201   10.0.0.2      KRB5      302 BLANCO-DESKTOP$  AS-REQ
66978 751.024207500 10.0.0.201   10.0.0.2      KRB5      382 BLANCO-DESKTOP$  AS-REQ
65505 743.708498600 10.0.0.201   10.0.0.2      KRB5      301 blanco-desktop$  AS-REQ
65526 743.828382900 10.0.0.201   10.0.0.2      KRB5      381 blanco-desktop$  AS-REQ
65530 743.836192200 10.0.0.201   10.0.0.2      KRB5      301 blanco-desktop$  AS-REQ
65544 743.884105500 10.0.0.201   10.0.0.2      KRB5      382 blanco-desktop$  AS-REQ
65617 744.239448800 10.0.0.201   10.0.0.2      KRB5      301 blanco-desktop$  AS-REQ
65625 744.255672900 10.0.0.201   10.0.0.2      KRB5      381 blanco-desktop$  AS-REQ
65712 744.572819700 10.0.0.201   10.0.0.2      KRB5      301 blanco-desktop$  AS-REQ
65725 744.601486200 10.0.0.201   10.0.0.2      KRB5      382 blanco-desktop$  AS-REQ
67036 751.190289600 10.0.0.201   10.0.0.2      KRB5      290 elmer.blanco     AS-REQ
67044 751.205833000 10.0.0.201   10.0.0.2      KRB5      370 elmer.blanco     AS-REQ
```

```
▸ Internet Protocol Version 4, Src: 10.0.0.201, Dst: 10.0.0.2
▸ Transmission Control Protocol, Src Port: 49675, Dst Port: 88, Seq: 1, Ack: 1, Len: 247
▾ Kerberos
  ▸ Record Mark: 243 bytes
  ▾ as-req
      pvno: 5
      msg-type: krb-as-req (10)
    ▸ padata: 1 item
    ▾ req-body
        Padding: 0
      ▸ kdc-options: 40810010
      ▾ cname
          name-type: kRB5-NT-PRINCIPAL (1)
        ▾ cname-string: 1 item
            CNameString: blanco-desktop$
        realm: DOGOFTHEYEAR.NET
```

2. Which torrent file did the user download? Betty_Boop_Rhythm_on_the_Reservation.avi.to



```
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)
Internet Protocol Version 4, Src: 10.0.0.201, Dst: 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.to
    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 Saf
  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
  Host: www.publicdomaintorrents.com\r\n
  Connection: Keep-Alive\r\n
```