Network Analysis

Time Thieves

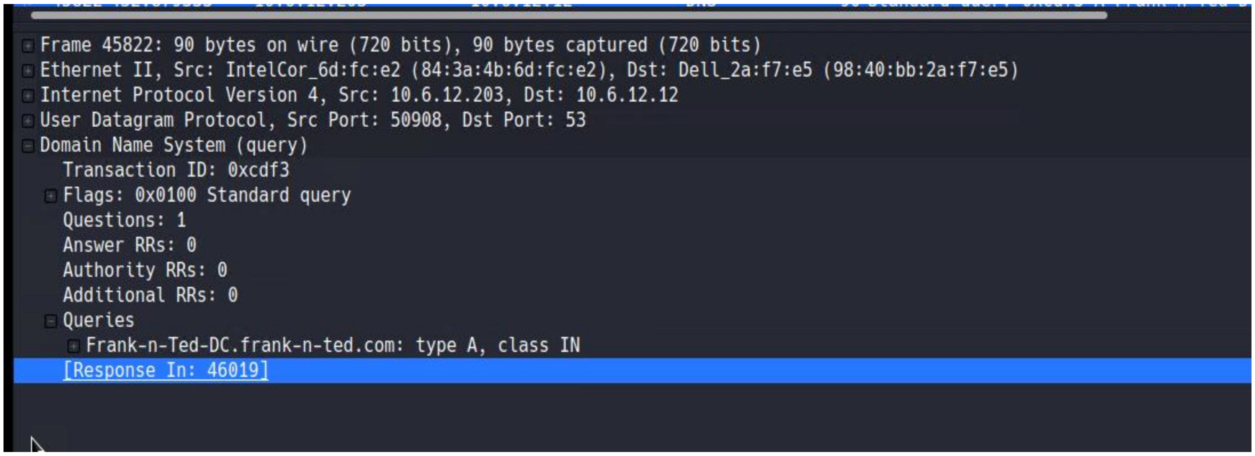
At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- 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?

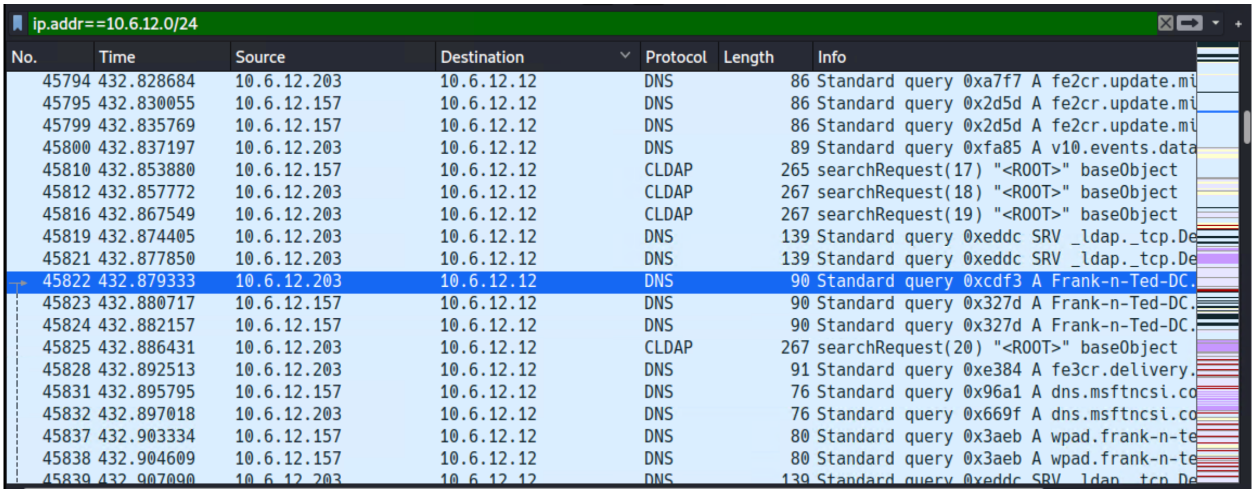
    - The Domain Name is **Frank-n-Ted-DC.frand-n-ted.com**
    - Wireshark Filter: **ip.addr==10.6.12.0/24**
    - Screenshot:



```
⊞ Frame 45822: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
⊞ 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: 10.6.12.203, Dst: 10.6.12.12
⊞ User Datagram Protocol, Src Port: 50908, Dst Port: 53
⊟ Domain Name System (query)
    Transaction ID: 0xcdf3
  ⊞ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊞ Frank-n-Ted-DC.frank-n-ted.com: type A, class IN
    [Response In: 46019]
```

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.frand-n-ted.com)**
   - Wireshark Filter: **ip.addr==10.6.12.0/24**
   - Screenshot:

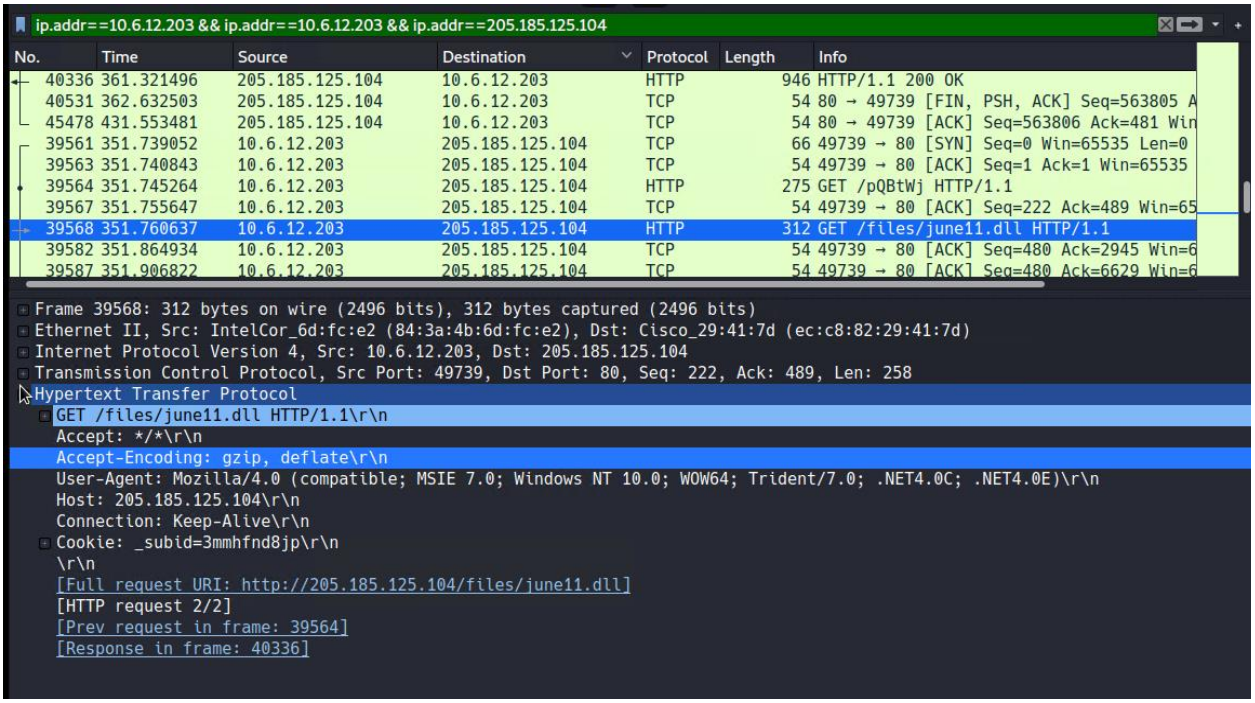


```
ip.addr==10.6.12.0/24

No.    Time        Source        Destination  Protocol Length Info
 45794 432.828684  10.6.12.203   10.6.12.12   DNS       86 Standard query 0xa7f7 A fe2cr.update.mi
 45795 432.830055  10.6.12.157   10.6.12.12   DNS       86 Standard query 0x2d5d A fe2cr.update.mi
 45799 432.835769  10.6.12.157   10.6.12.12   DNS       86 Standard query 0x2d5d A fe2cr.update.mi
 45800 432.837197  10.6.12.203   10.6.12.12   DNS       89 Standard query 0xfa85 A v10.events.data
 45810 432.853880  10.6.12.157   10.6.12.12   CLDAP    265 searchRequest(17) "<ROOT>" baseObject
 45812 432.857772  10.6.12.203   10.6.12.12   CLDAP    267 searchRequest(18) "<ROOT>" baseObject
 45816 432.867549  10.6.12.203   10.6.12.12   CLDAP    267 searchRequest(19) "<ROOT>" baseObject
 45819 432.874405  10.6.12.203   10.6.12.12   DNS      139 Standard query 0xeddc SRV _ldap._tcp.De
 45821 432.877850  10.6.12.203   10.6.12.12   DNS      139 Standard query 0xeddc SRV _ldap._tcp.De
 45822 432.879333  10.6.12.203   10.6.12.12   DNS       90 Standard query 0xcdf3 A Frank-n-Ted-DC.
 45823 432.880717  10.6.12.157   10.6.12.12   DNS       90 Standard query 0x327d A Frank-n-Ted-DC.
 45824 432.882157  10.6.12.157   10.6.12.12   DNS       90 Standard query 0x327d A Frank-n-Ted-DC.
 45825 432.886431  10.6.12.203   10.6.12.12   CLDAP    267 searchRequest(20) "<ROOT>" baseObject
 45828 432.892513  10.6.12.203   10.6.12.12   DNS       91 Standard query 0xe384 A fe3cr.delivery.
 45831 432.895795  10.6.12.157   10.6.12.12   DNS       76 Standard query 0x96a1 A dns.msftncsi.co
 45832 432.897018  10.6.12.203   10.6.12.12   DNS       76 Standard query 0x669f A dns.msftncsi.co
 45837 432.903334  10.6.12.157   10.6.12.12   DNS       80 Standard query 0x3aeb A wpad.frank-n-te
 45838 432.904609  10.6.12.157   10.6.12.12   DNS       80 Standard query 0x3aeb A wpad.frank-n-te
 45839 432.907090  10.6.12.203   10.6.12.12   DNS      139 Standard query 0xeddc SRV _ldap._tcp.De
```

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.

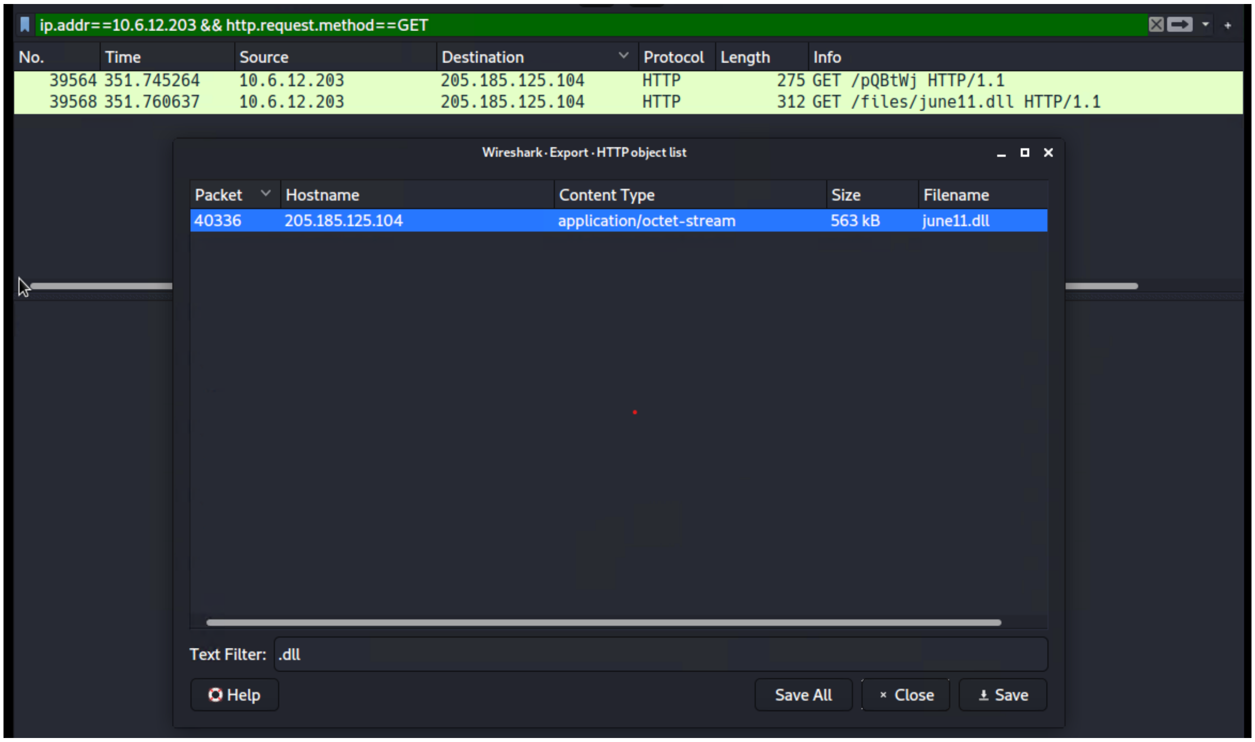
   - Malware File was **june11.dll**
   - Screenshot:



```
ip.addr==10.6.12.203 && ip.addr==10.6.12.203 && ip.addr==205.185.125.104

No.    Time        Source           Destination      Protocol Length Info
 40336 361.321496  205.185.125.104  10.6.12.203      HTTP     946 HTTP/1.1 200 OK
 40531 362.632503  205.185.125.104  10.6.12.203      TCP       54 80 → 49739 [FIN, PSH, ACK] Seq=563805 A
 45478 431.553481  205.185.125.104  10.6.12.203      TCP       54 80 → 49739 [ACK] Seq=563806 Ack=481 Win
 39561 351.739052  10.6.12.203      205.185.125.104  TCP       66 49739 → 80 [SYN] Seq=0 Win=65535 Len=0
 39563 351.740843  10.6.12.203      205.185.125.104  TCP       54 49739 → 80 [ACK] Seq=1 Ack=1 Win=65535
 39564 351.745264  10.6.12.203      205.185.125.104  HTTP     275 GET /pQBtWj HTTP/1.1
 39567 351.755647  10.6.12.203      205.185.125.104  TCP       54 49739 → 80 [ACK] Seq=222 Ack=489 Win=65
 39568 351.760637  10.6.12.203      205.185.125.104  HTTP     312 GET /files/june11.dll HTTP/1.1
 39582 351.864934  10.6.12.203      205.185.125.104  TCP       54 49739 → 80 [ACK] Seq=480 Ack=2945 Win=6
 39587 351.906822  10.6.12.203      205.185.125.104  TCP       54 49739 → 80 [ACK] Seq=480 Ack=6629 Win=6

⊞ Frame 39568: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits)
⊞ Ethernet II, Src: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2), Dst: Cisco_29:41:7d (ec:c8:82:29:41:7d)
⊞ Internet Protocol Version 4, Src: 10.6.12.203, Dst: 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: 39564]
    [Response in frame: 40336]
```



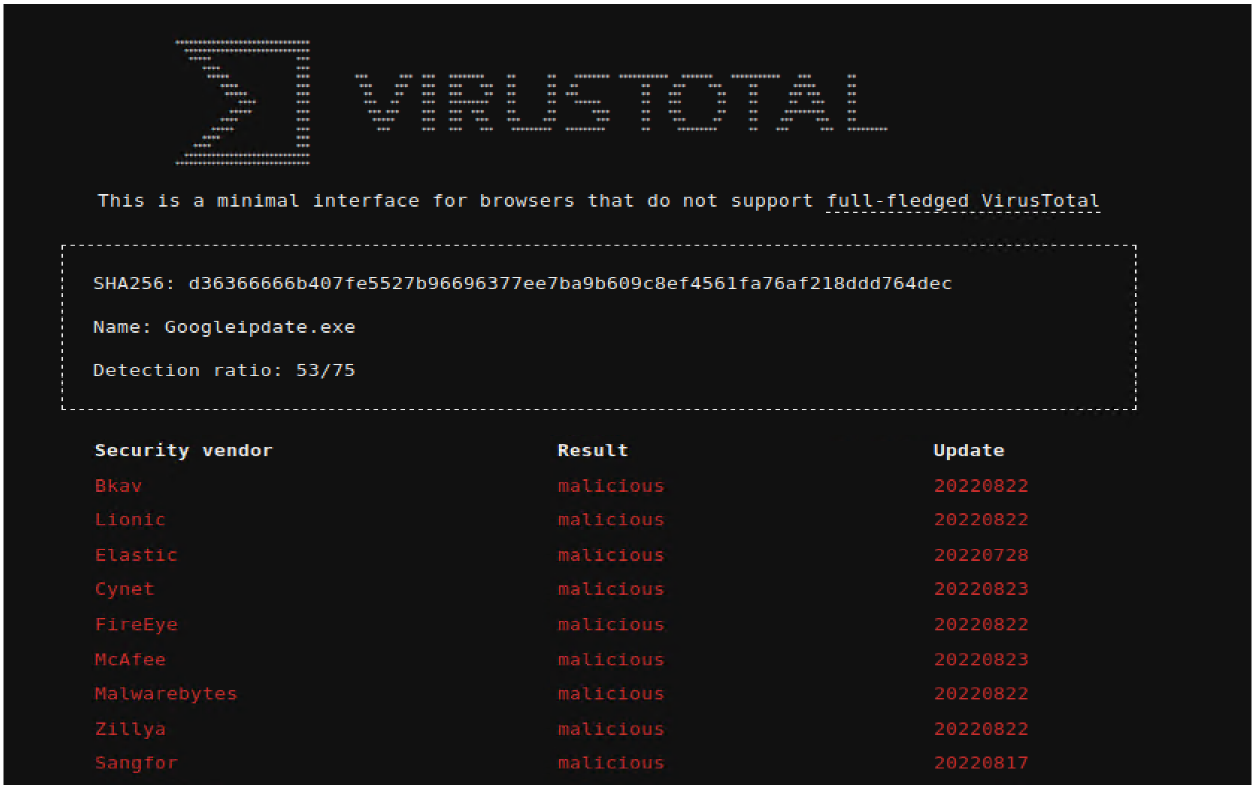
```
ip.addr==10.6.12.203 && http.request.method==GET
No.    Time        Source          Destination      Protocol  Length  Info
 39564 351.745264  10.6.12.203     205.185.125.104  HTTP         275 GET /pQBtWj HTTP/1.1
 39568 351.760637  10.6.12.203     205.185.125.104  HTTP         312 GET /files/june11.dll HTTP/1.1
```

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
40336	205.185.125.104	application/octet-stream	563 kB	june11.dll

Text Filter: .dll

4. Upload the file to VirusTotal.com. What kind of malware is this classified as?
    - After uploading the file to VirusTotal.com, This malware file is classified as malicious.



```
This is a minimal interface for browsers that do not support full-fledged VirusTotal

SHA256: d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Name: Googleipdate.exe

Detection ratio: 53/75

Security vendor                        Result                          Update
Bkav                                   malicious                       20220822
Lionic                                 malicious                       20220822
Elastic                                malicious                       20220728
Cynet                                  malicious                       20220823
FireEye                                malicious                       20220822
McAfee                                 malicious                       20220823
Malwarebytes                           malicious                       20220822
Zillya                                 malicious                       20220822
Sangfor                                malicious                       20220817
```

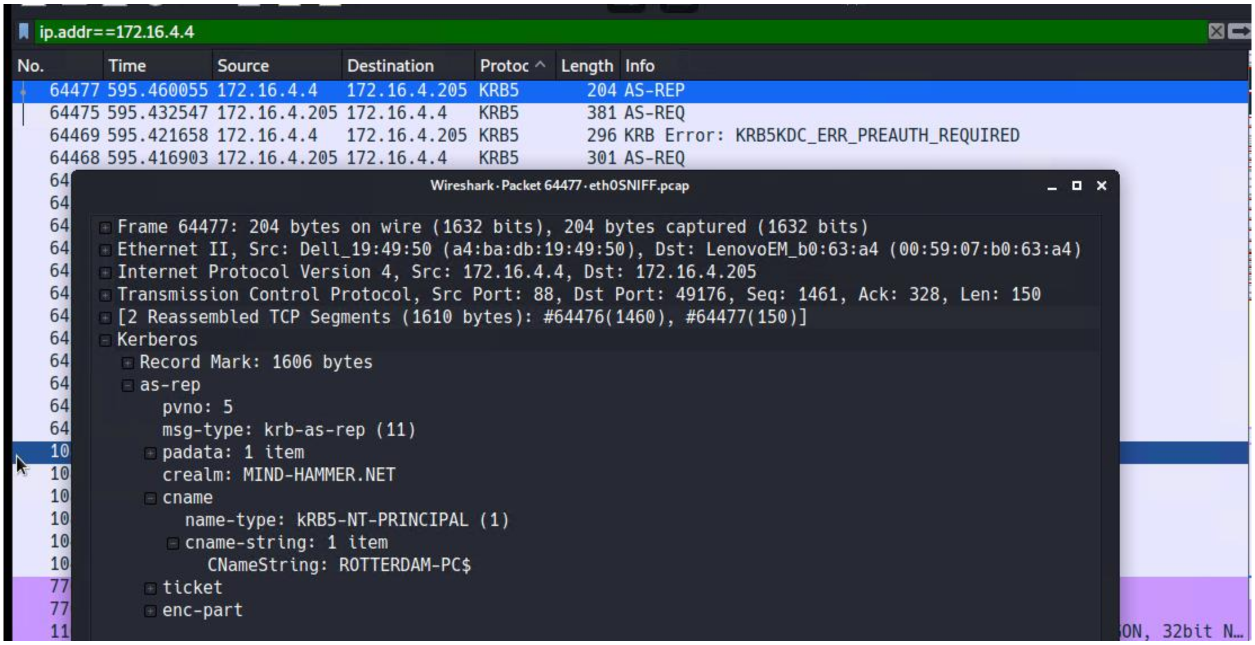
Vulnerable Windows Machines

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: **LenovoEM (00:59:07:b0:63:a4)**
    - Wireshark Filter: **Filter used in Wireshark: ip.src==172.16.4.205**
    - Screenshot:



ip.addr==172.16.4.4

```
No.   Time       Source       Destination  Protoc Length Info
64477 595.460055 172.16.4.4   172.16.4.205 KRB5      204 AS-REP
64475 595.432547 172.16.4.205 172.16.4.4   KRB5      381 AS-REQ
64469 595.421658 172.16.4.4   172.16.4.205 KRB5      296 KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
64468 595.416903 172.16.4.205 172.16.4.4   KRB5      301 AS-REQ
```

Wireshark · Packet 64477 · eth0SNIFF.pcap

```
Frame 64477: 204 bytes on wire (1632 bits), 204 bytes captured (1632 bits)
Ethernet II, Src: Dell_19:49:50 (a4:ba:db:19:49:50), Dst: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
Internet Protocol Version 4, Src: 172.16.4.4, Dst: 172.16.4.205
Transmission Control Protocol, Src Port: 88, Dst Port: 49176, Seq: 1461, Ack: 328, Len: 150
[2 Reassembled TCP Segments (1610 bytes): #64476(1460), #64477(150)]
Kerberos
  Record Mark: 1606 bytes
  as-rep
    pvno: 5
    msg-type: krb-as-rep (11)
    padata: 1 item
    crealm: MIND-HAMMER.NET
    cname
      name-type: kRB5-NT-PRINCIPAL (1)
      cname-string: 1 item
        CNameString: ROTTERDAM-PC$
    ticket
    enc-part
```

2. What is the username of the Windows user whose computer is infected?
    - mattijes.devries
3. What are the IP addresses used in the actual infection traffic?
    - IP address that is used in actual infection traffic is 185.243.115.84