Network Analysis

NIKKI Ghadimi

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:

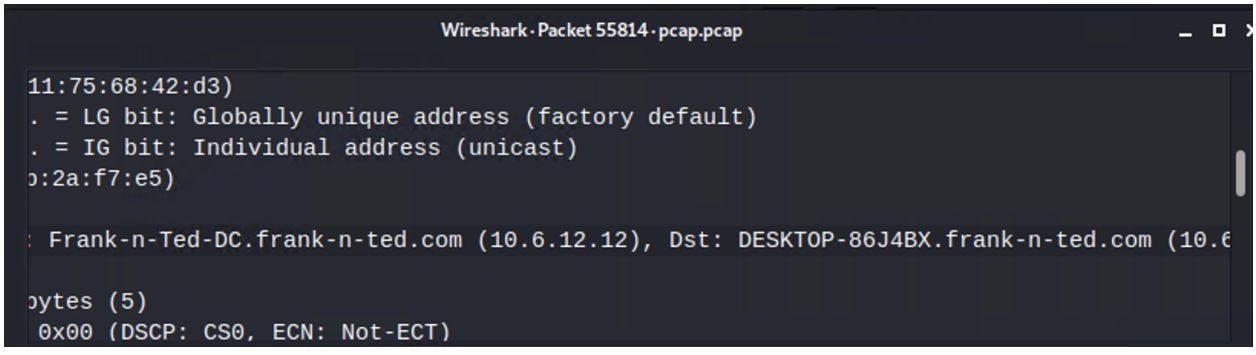
- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.
- Their IP addresses are somewhere in the range `10.6.12.0/24`.

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 of the user's custom cite is: Frank-n-Ted-DC.frank-n-ted.com

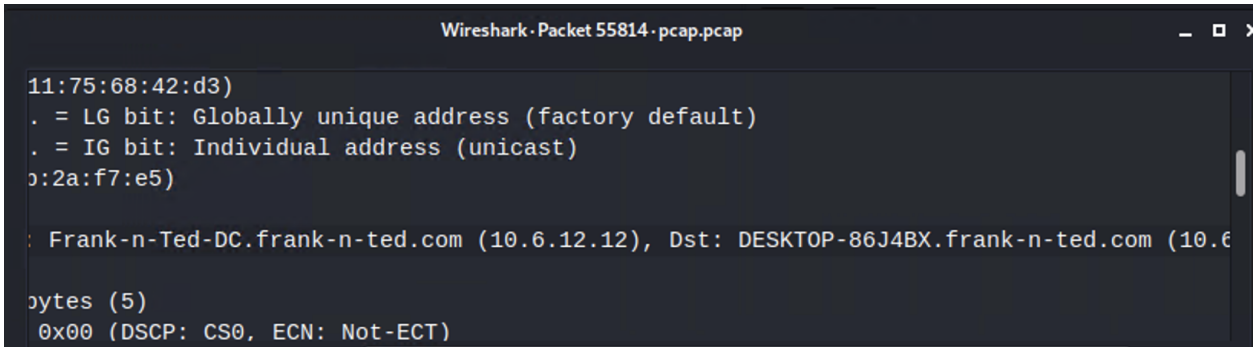
   Filter: ip.addr==10.6.12.0/24



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

   The IP address of the Domain Controller (DC) of the AD network is: 10.6.12.12

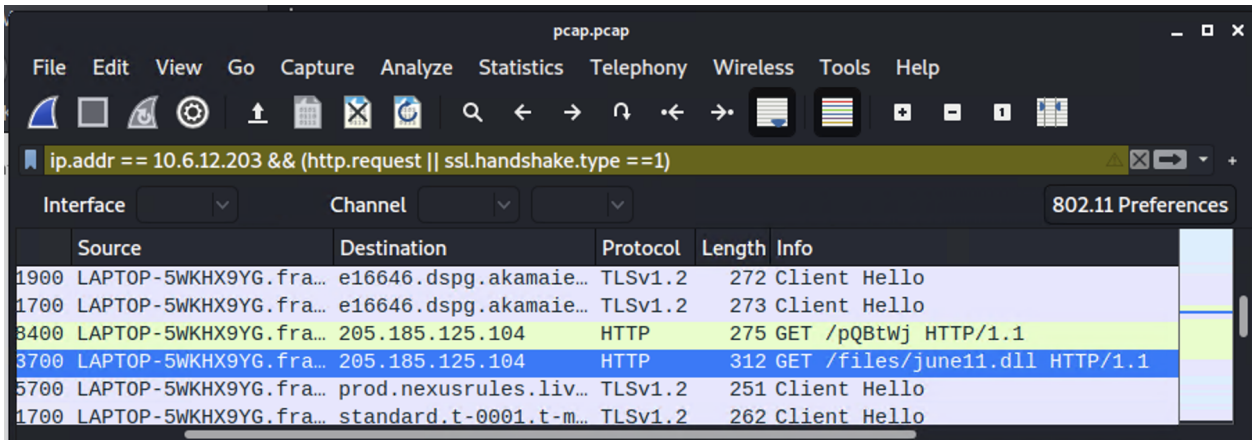
   Filter: ip.addr==10.6.12.0/24



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.

   The name of the malware downloaded to the `10.6.12.203` machine is june11.dll

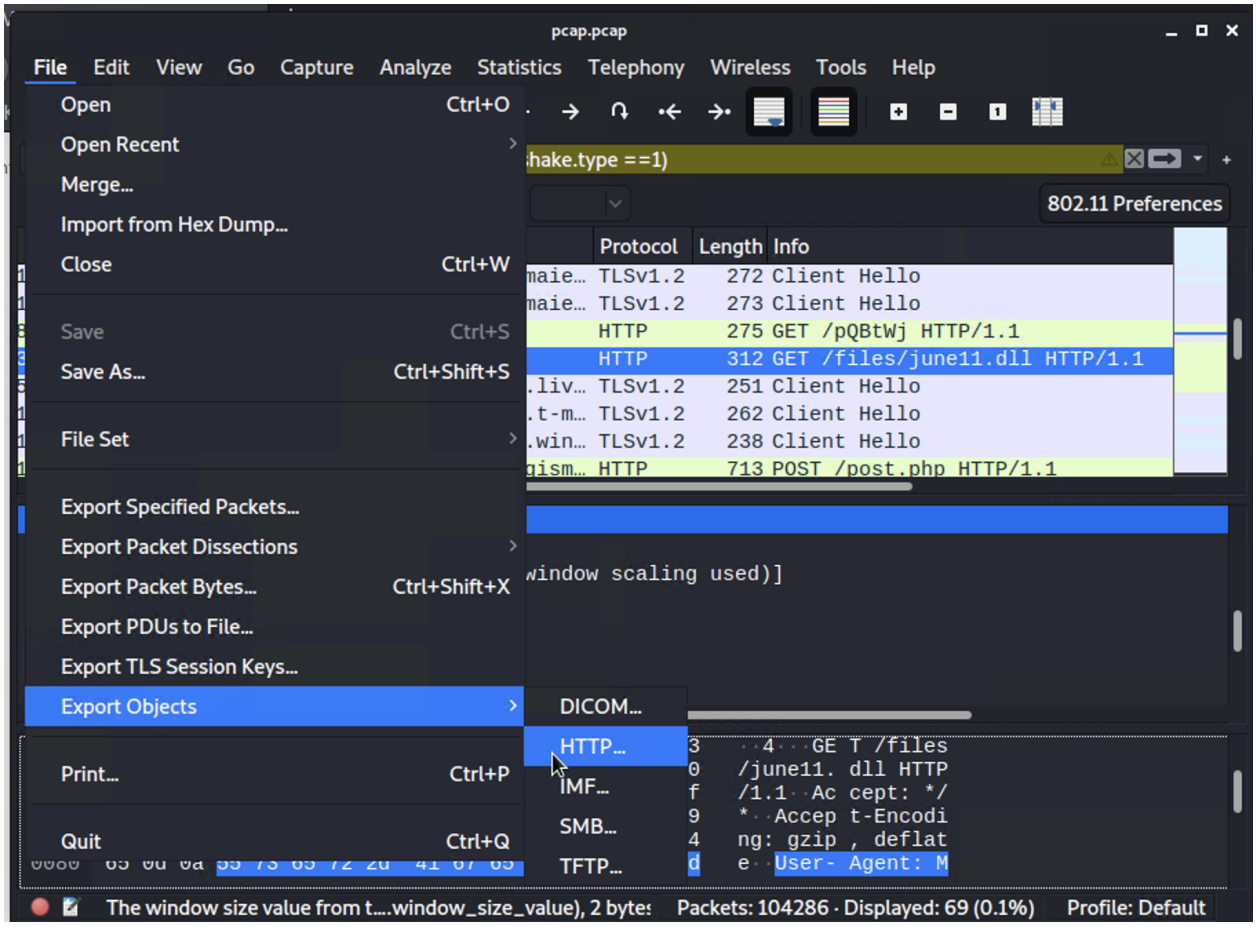
   Filter: ip.addr==10.6.12.203 and http.request.method==GET

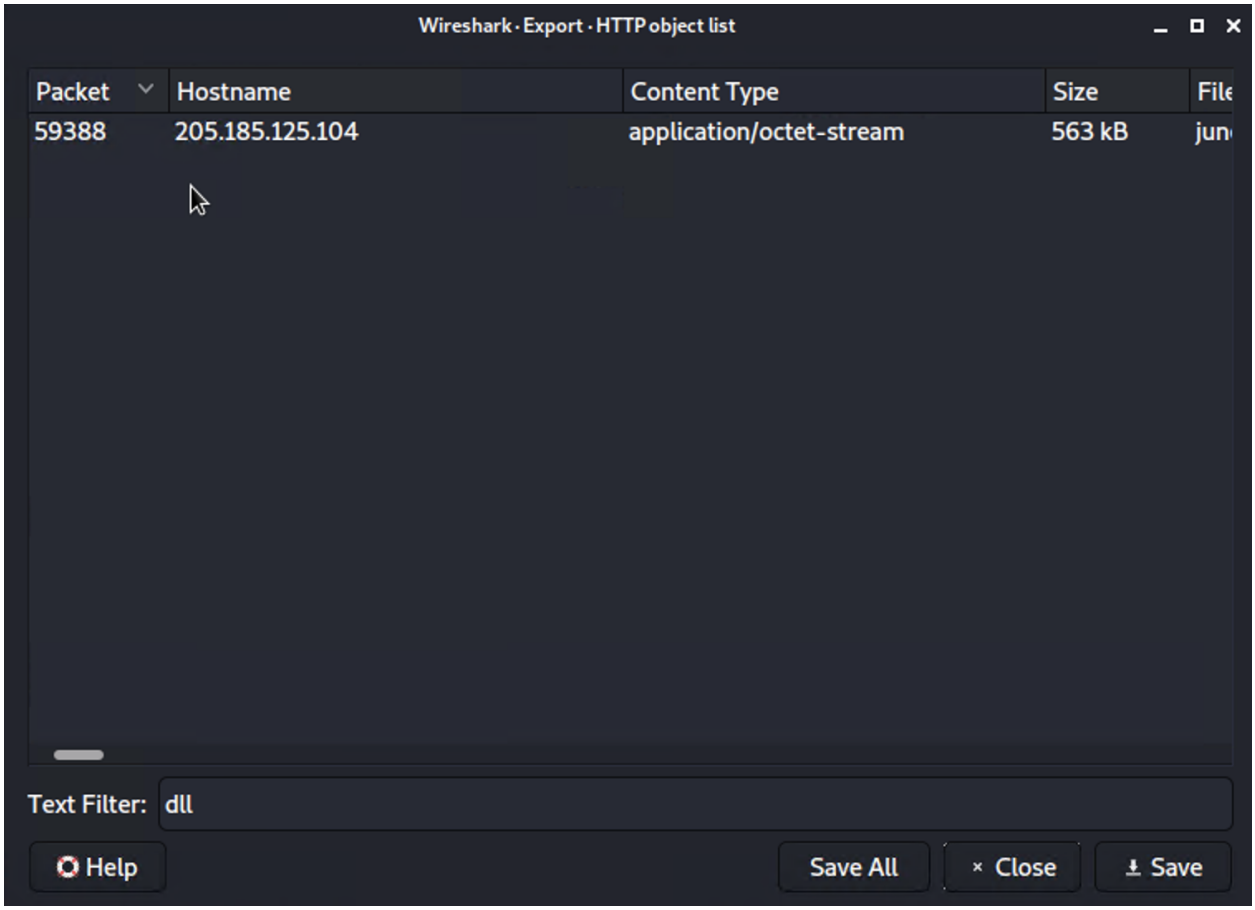


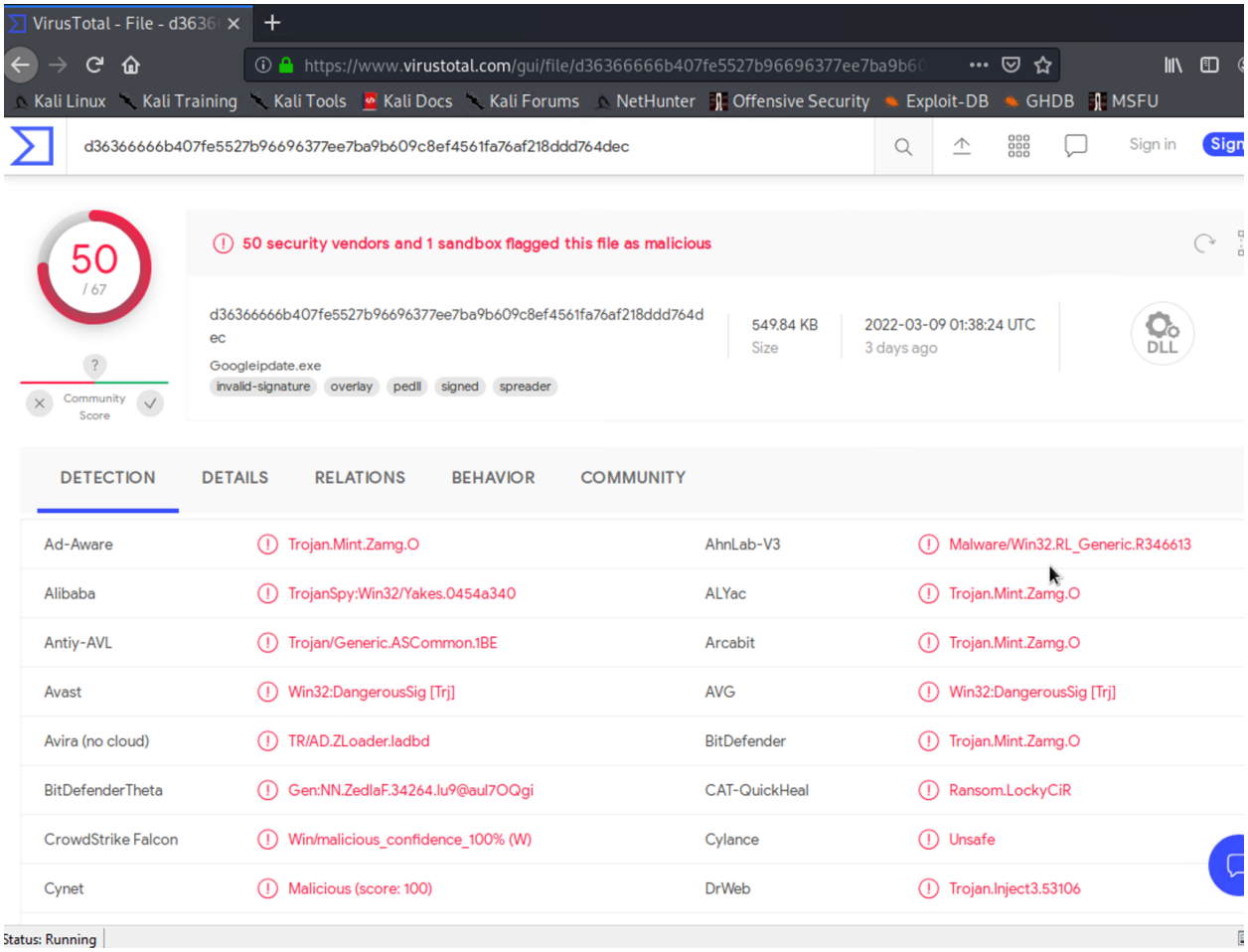
4. Upload the file to VirusTotal.com. What kind of malware is this classified as?

   Export: file>Export Objects>HTTP

   The malware is this classified as Trojan- malicious 50/67


pcap.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+Shift+X
Export PDUs to File...
Export TLS Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
DICOM...
HTTP...
IMF...
SMB...
TFTP...
802.11 Preferences
Protocol Length Info
TLSv1.2 272 Client Hello
TLSv1.2 273 Client Hello
HTTP 275 GET /pQBtWj HTTP/1.1
HTTP 312 GET /files/june11.dll HTTP/1.1
TLSv1.2 251 Client Hello
TLSv1.2 262 Client Hello
TLSv1.2 238 Client Hello
HTTP 713 POST /post.php HTTP/1.1
The window size value from t....window_size_value), 2 byte
Packets: 104286 · Displayed: 69 (0.1%)
Profile: Default


Wireshark · Export · HTTP object list
Packet
Hostname
Content Type
Size
File
59388
205.185.125.104
application/octet-stream
563 kB
jun
Text Filter:
dll
Help
Save All
Close
Save


VirusTotal - File - d3636
https://www.virustotal.com/gui/file/d36366666b407fe5527b96696377ee7ba9b60
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec
Sign in
Sign
50
/ 67
Community Score
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
3 days ago
DLL
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY
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
Cynet
Malicious (score: 100)
DrWeb
Trojan.Inject3.53106
Status: Running

Vulnerable Windows Machines

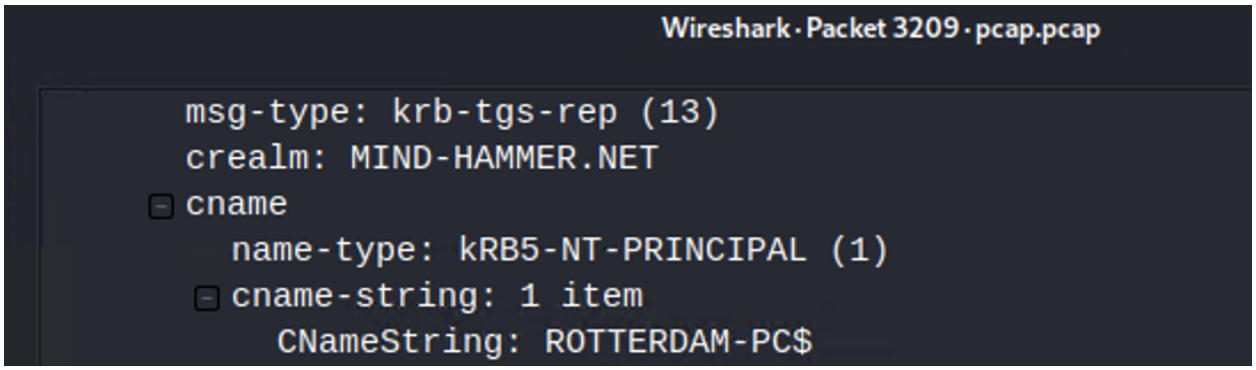
The Security team received reports of an infected Windows host on the network. They know the following:

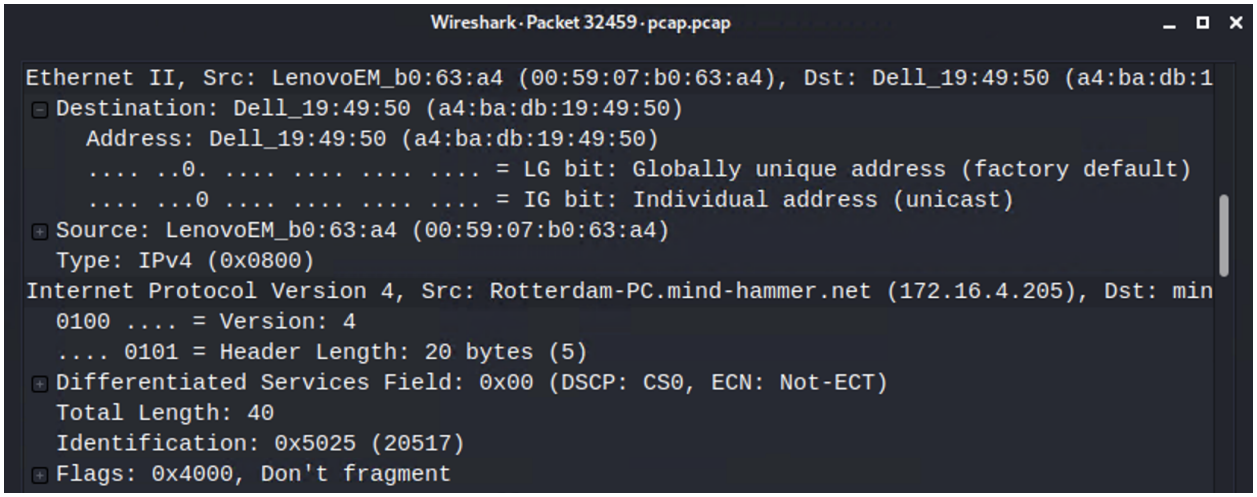
- Machines in the network live in the range `172.16.4.0/24`.
- The domain mind-hammer.net is associated with the infected computer.
- The DC for this network lives at `172.16.4.4` and is named Mind-Hammer-DC.
- The network has standard gateway and broadcast addresses.

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.src==172.16.44 and kerberos.CNameString

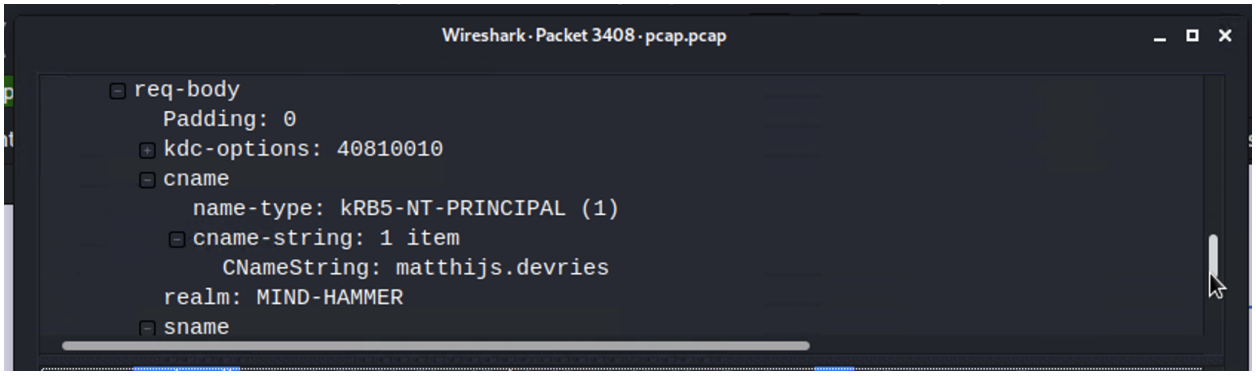




2. What is the username of the Windows user whose computer is infected?

The username of the Windows user whose computer is infected is: matthijs.devries

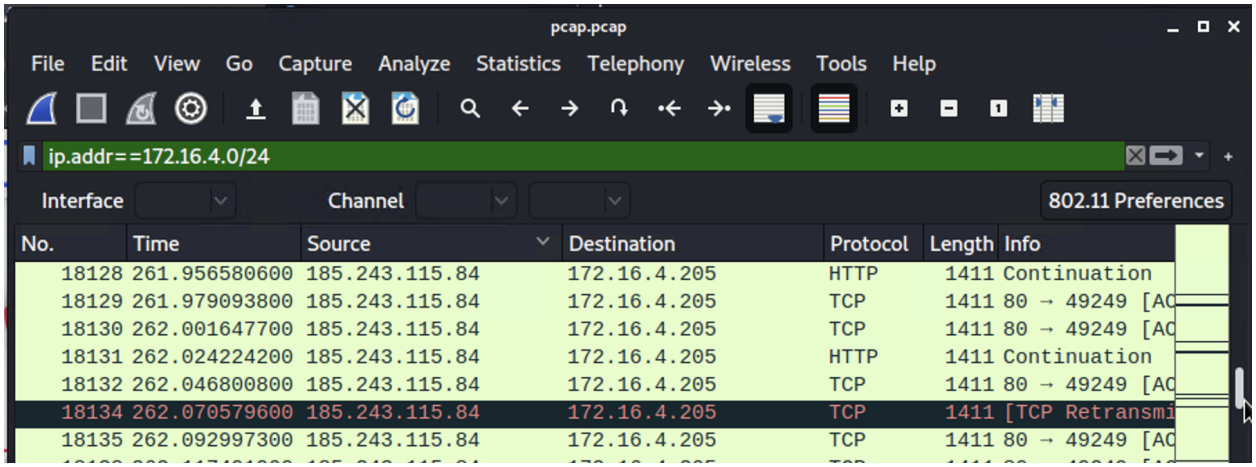
Filter: ip.src==172.16.4.205 and Kerberos.CNameString

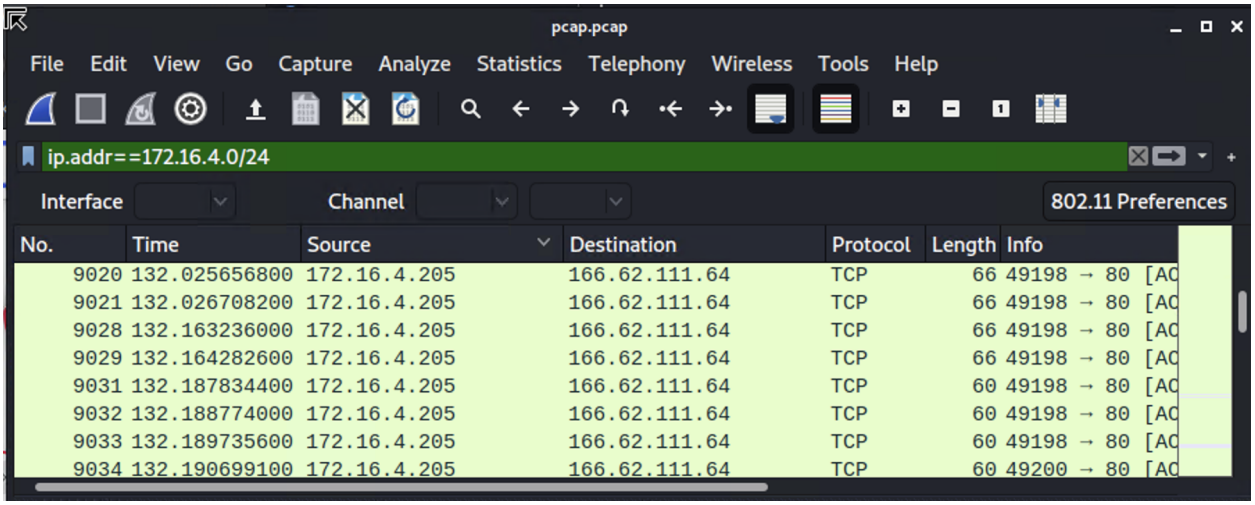


3. What are the IP addresses used in the actual infection traffic?

The IP addresses used in the actual infection traffic are:172.16.4.205, 172.16.4.4, 166.62.11.64

Filter: ip.addr==172.16.4.205 and ip.add==185.243.115.84





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.

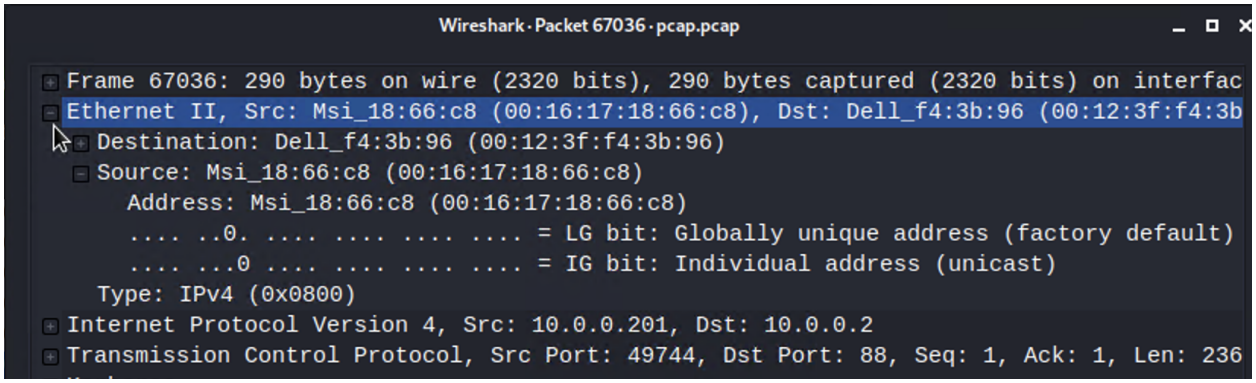
IT shared the following about the torrent activity:

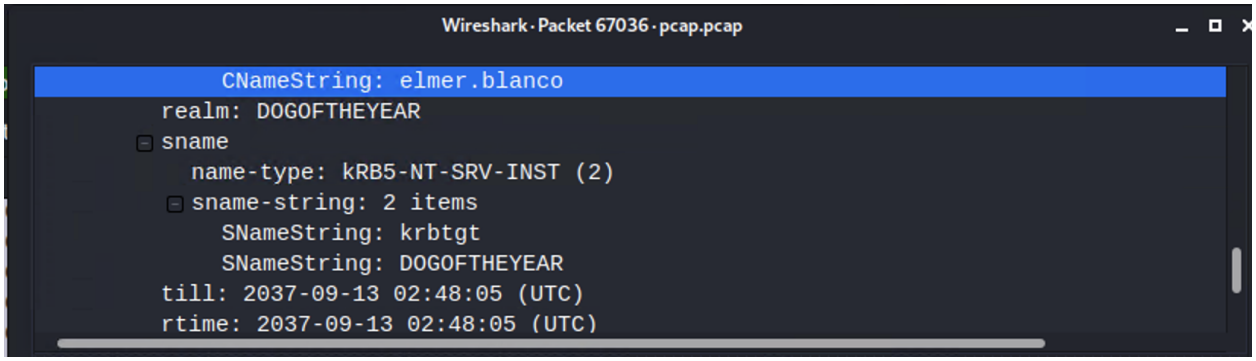
- The machines using torrents live in the range `10.0.0.0/24` and are clients of an AD domain.
- The DC of this domain lives at `10.0.0.2` and is named DogOfTheYear-DC.
- The DC is associated with the domain dogoftheyear.net.

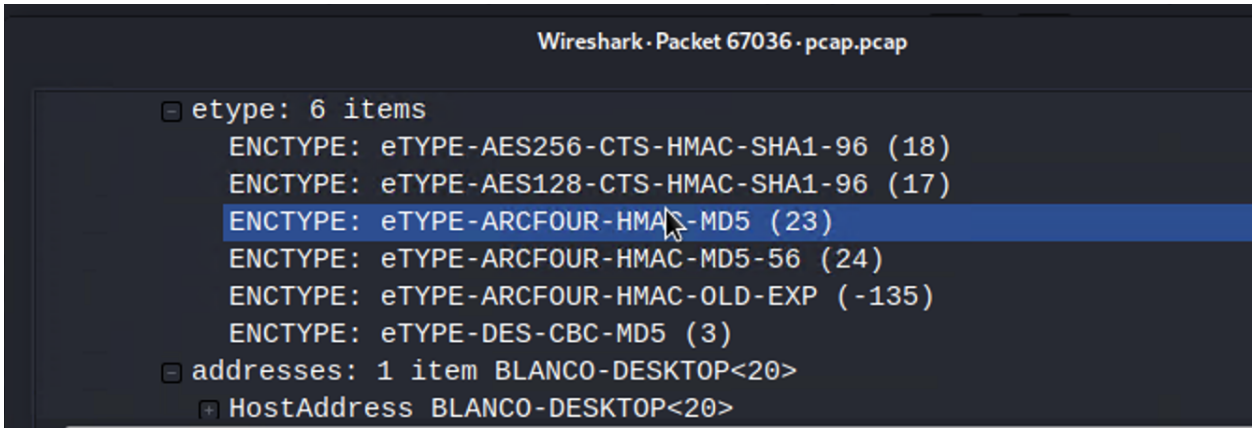
Your task is to isolate torrent traffic and answer the following questions:

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

Filter: ip.src==10.0.0.201 and kerberos.CNameString



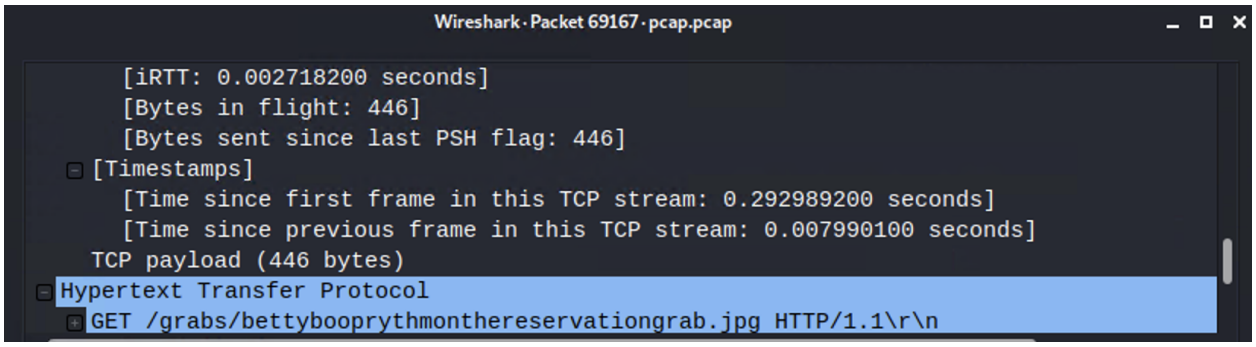


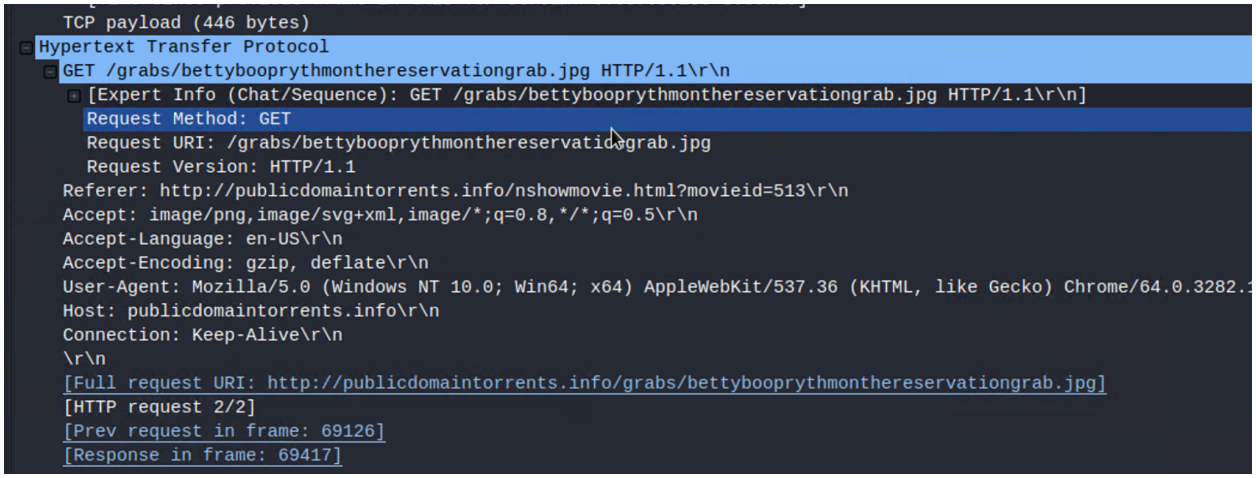


2. Which torrent file did the user download?

   The the user downloaded: Betty_Boop_Rythm_on_the_Reservation.avi.torrent

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




TCP payload (446 bytes)
Hypertext Transfer Protocol
GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1\r\n]
Request Method: GET
Request URI: /grabs/bettybooprythmonthereservationgrab.jpg
Request Version: HTTP/1.1
Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\r\n
Accept: image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5\r\n
Accept-Language: en-US\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.
Host: publicdomaintorrents.info\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://publicdomaintorrents.info/grabs/bettybooprythmonthereservationgrab.jpg]
[HTTP request 2/2]
[Prev request in frame: 69126]
[Response in frame: 69417]