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?

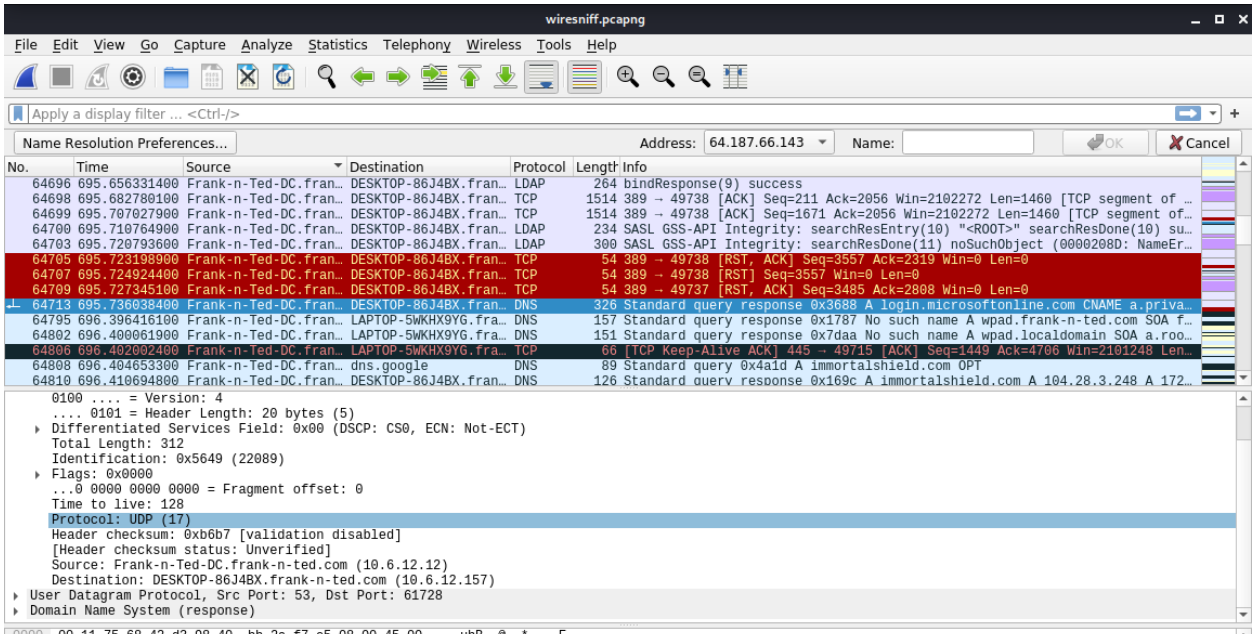
   Filter: ip.addr == 10.6.12.0/24

   Frank-n-Ted-DC.frank-n-ted.com

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

   Filter: ip.addr == 10.6.12.0/24

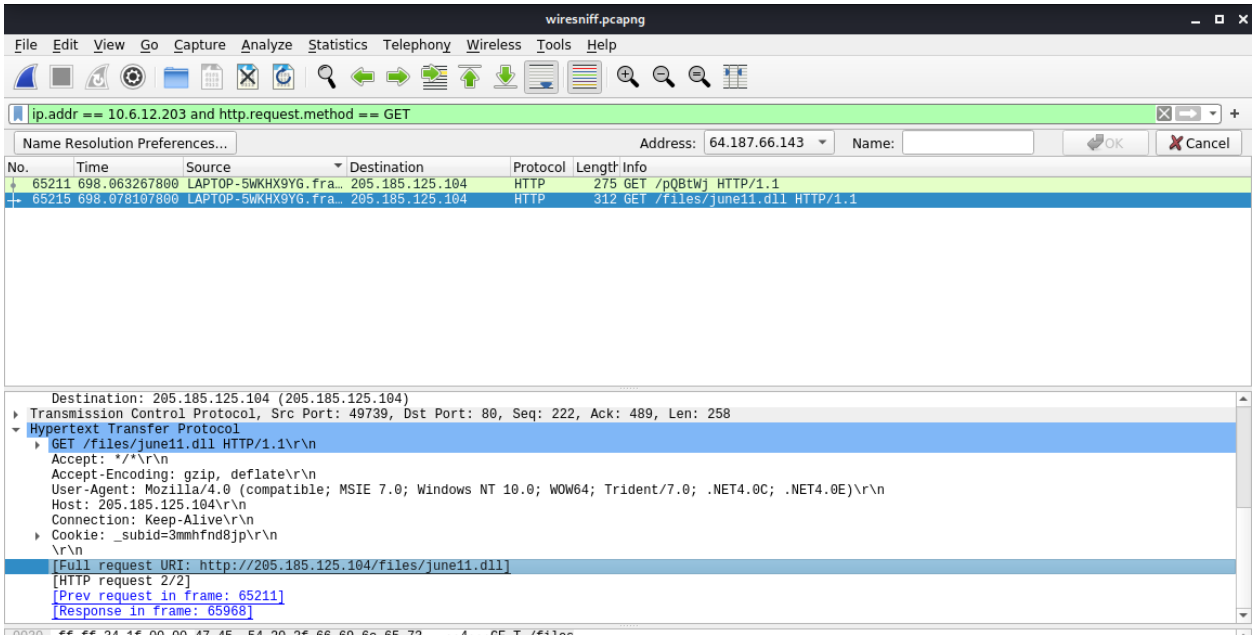
   10.6.12.12



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.

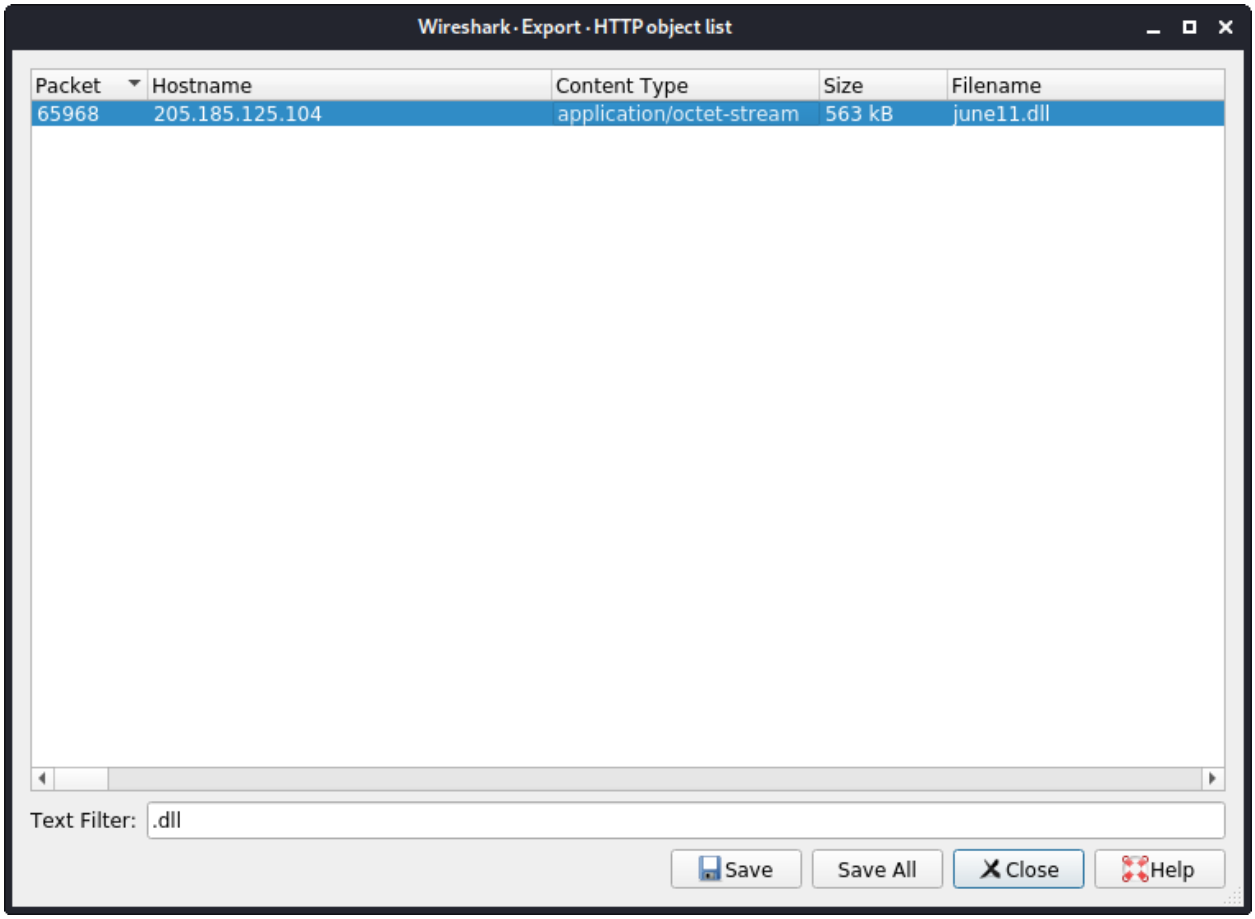
   Filter: ip.addr == 10.6.12.203 and http.request.method == GET

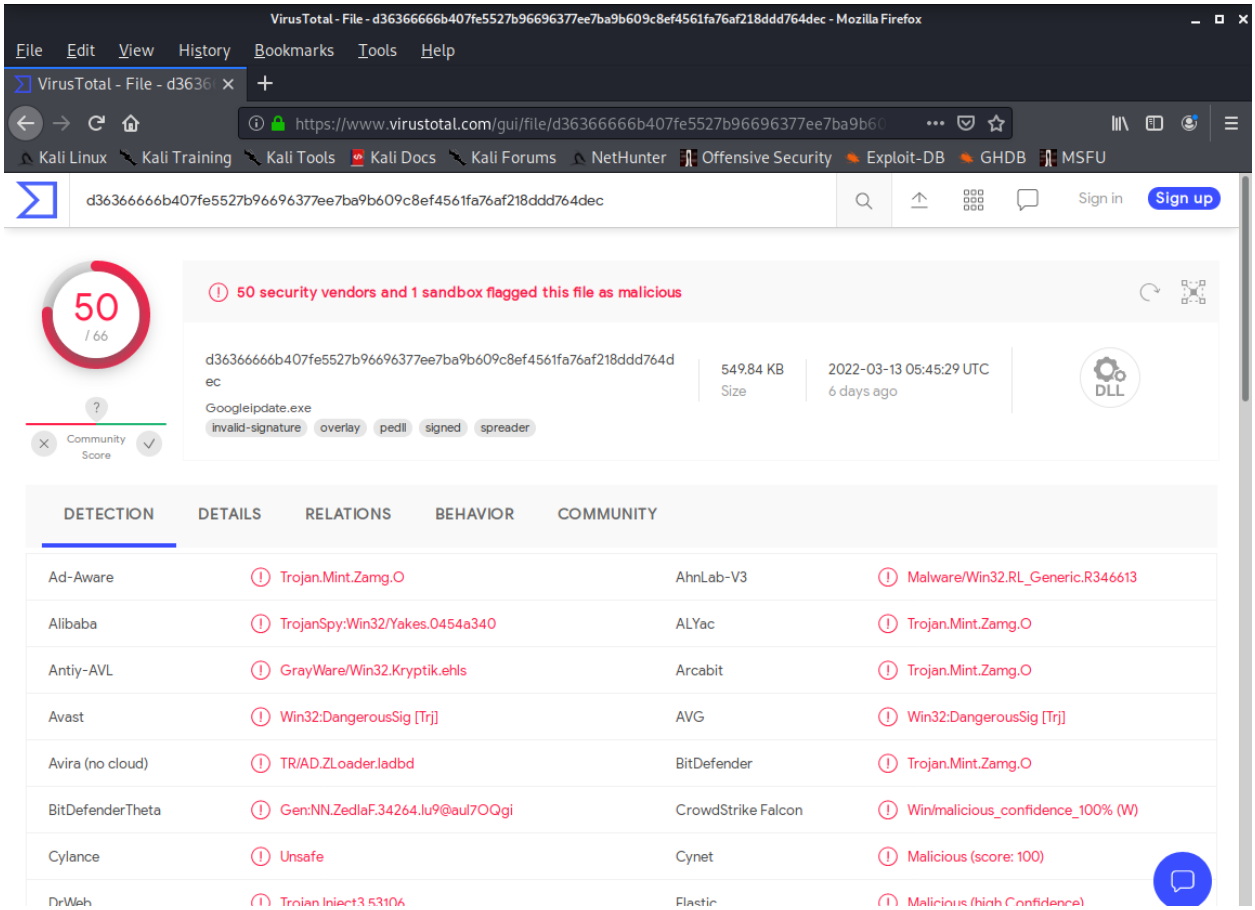
   june11.dll



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

   Trojan





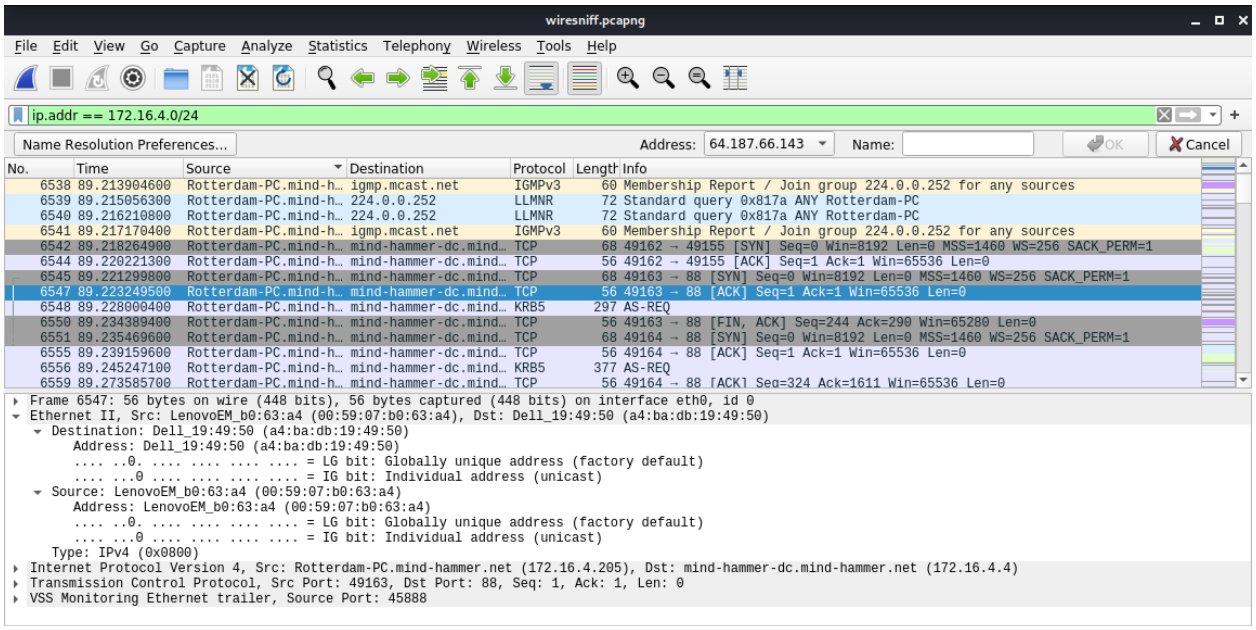
Vulnerable Windows Machines

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:

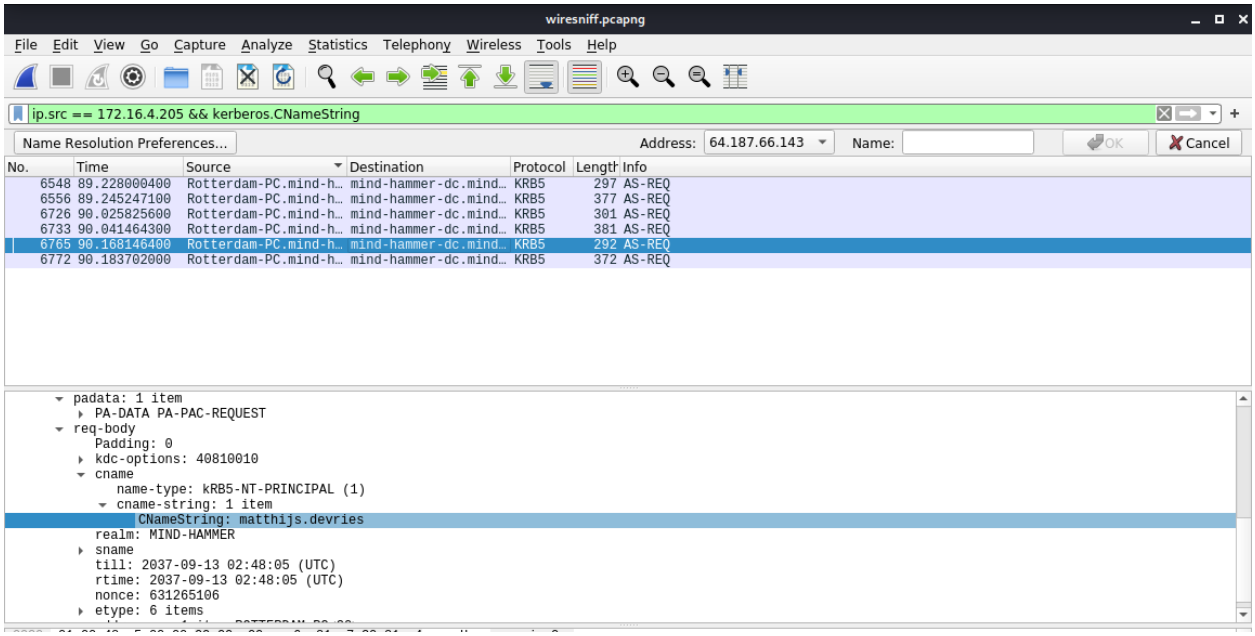
1. Find the following information about the infected Windows machine:
    - Filter: ip.addr == 172.16.4.0/24
    - Host name: Rotterdam-PC
    - IP address: 172.16.4.205
    - MAC address: 00:59:07:b0:63:a4



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

    Filter: ip.src == 172.16.4.205 && kerberos.CNameString

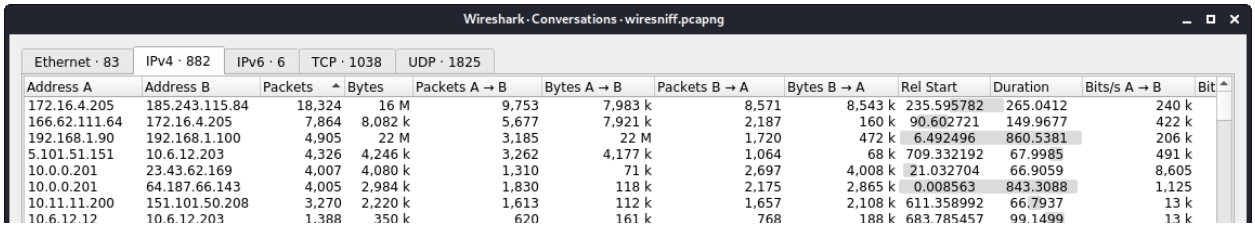
    Matthijs.devries is the windows user



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

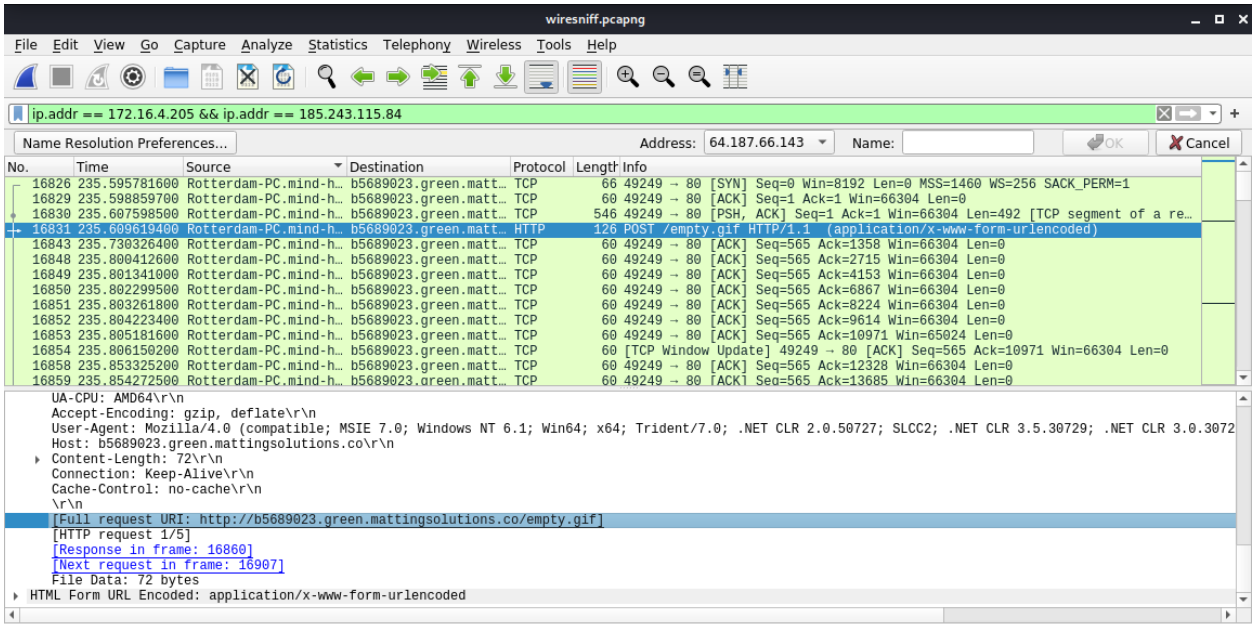
   Filter: Go into statistics menu; conversations; select IPV4 Tab, sort by packets

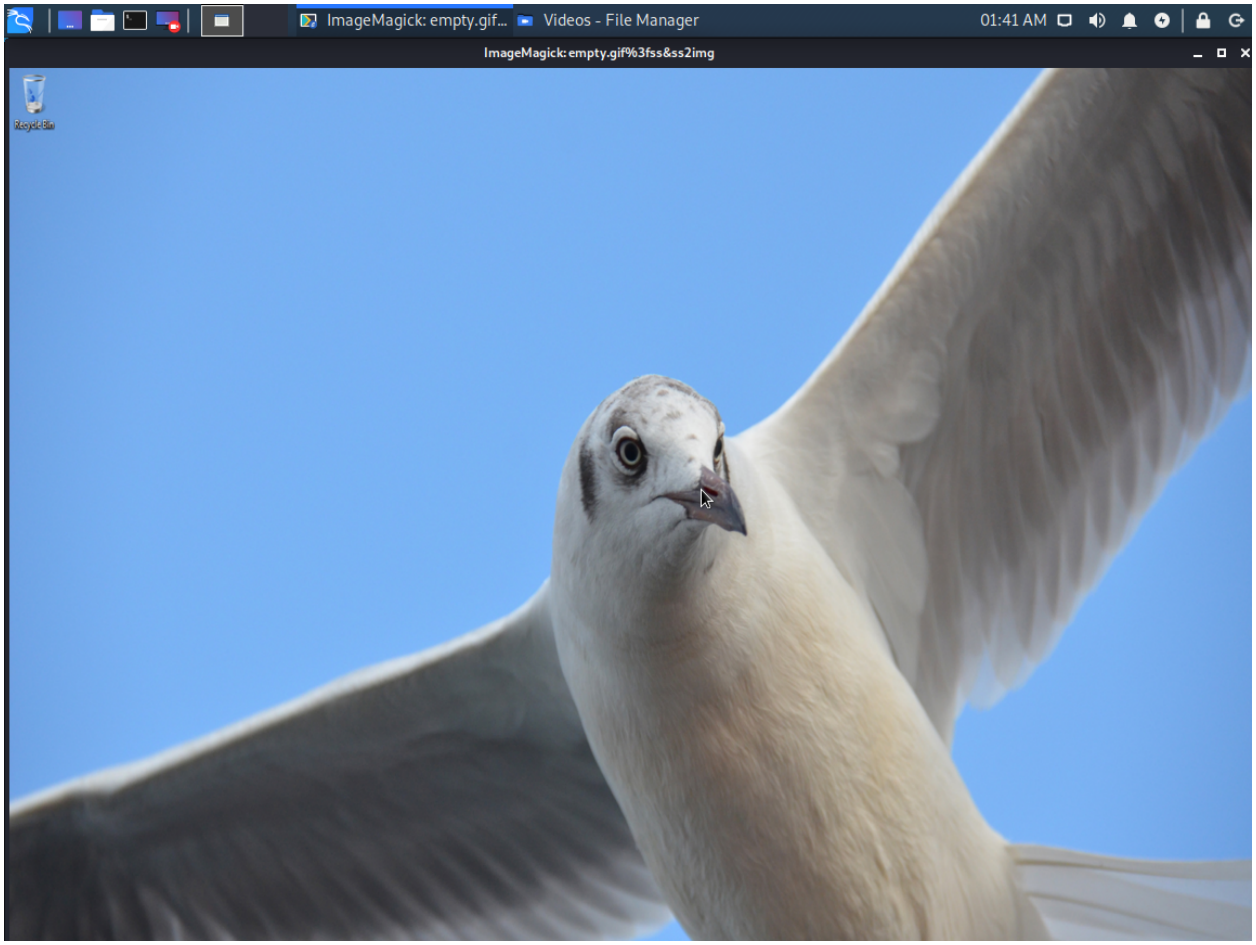
   IP Addresses 172.16.4.205, 185.243.115.84, 166.62.111.64



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

   Filter: ip.addr == 172.16.4.205 && ip.addr == 185.243.115.84


wiresniff.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 172.16.4.205 && ip.addr == 185.243.115.84
Name Resolution Preferences...
Address: 64.187.66.143
Name:
OK
Cancel
No. Time Source Destination Protocol Length Info
16826 235.595781600 Rotterdam-PC.mind-h… b5689023.green.matt… TCP 66 49249 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
16829 235.598859700 Rotterdam-PC.mind-h… b5689023.green.matt… TCP 60 49249 → 80 [ACK] Seq=1 Ack=1 Win=66304 Len=0
16830 235.607598500 Rotterdam-PC.mind-h… b5689023.green.matt… TCP 546 49249 → 80 [PSH, ACK] Seq=1 Ack=1 Win=66304 Len=492 [TCP segment of a re…
16831 235.609619400 Rotterdam-PC.mind-h… b5689023.green.matt… HTTP 126 POST /empty.gif HTTP/1.1 (application/x-www-form-urlencoded)
16843 235.730326400 Rotterdam-PC.mind-h… b5689023.green.matt… TCP 60 49249 → 80 [ACK] Seq=565 Ack=1358 Win=66304 Len=0
16848 235.800412600 Rotterdam-PC.mind-h… b5689023.green.matt… TCP 60 49249 → 80 [ACK] Seq=565 Ack=2715 Win=66304 Len=0
16849 235.801341000 Rotterdam-PC.mind-h… b5689023.green.matt… TCP 60 49249 → 80 [ACK] Seq=565 Ack=4153 Win=66304 Len=0
16850 235.802299500 Rotterdam-PC.mind-h… b5689023.green.matt… TCP 60 49249 → 80 [ACK] Seq=565 Ack=6867 Win=66304 Len=0
16851 235.803261800 Rotterdam-PC.mind-h… b5689023.green.matt… TCP 60 49249 → 80 [ACK] Seq=565 Ack=8224 Win=66304 Len=0
16852 235.804223400 Rotterdam-PC.mind-h… b5689023.green.matt… TCP 60 49249 → 80 [ACK] Seq=565 Ack=9614 Win=66304 Len=0
16853 235.805181600 Rotterdam-PC.mind-h… b5689023.green.matt… TCP 60 49249 → 80 [ACK] Seq=565 Ack=10971 Win=65024 Len=0
16854 235.806150200 Rotterdam-PC.mind-h… b5689023.green.matt… TCP 60 [TCP Window Update] 49249 → 80 [ACK] Seq=565 Ack=10971 Win=66304 Len=0
16858 235.853325200 Rotterdam-PC.mind-h… b5689023.green.matt… TCP 60 49249 → 80 [ACK] Seq=565 Ack=12328 Win=66304 Len=0
16859 235.854272500 Rotterdam-PC.mind-h… b5689023.green.matt… TCP 60 49249 → 80 [ACK] Seq=565 Ack=13685 Win=66304 Len=0
UA-CPU: AMD64\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.3072
Host: b5689023.green.mattingsolutions.co\r\n
Content-Length: 72\r\n
Connection: Keep-Alive\r\n
Cache-Control: no-cache\r\n
\r\n
[Full request URI: http://b5689023.green.mattingsolutions.co/empty.gif]
[HTTP request 1/5]
[Response in frame: 16860]
[Next request in frame: 16907]
File Data: 72 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded


ImageMagick: empty.gif...
Videos - File Manager
01:41 AM
ImageMagick: empty.gif%3fss&ss2img
Recycle Bin

Illegal Downloads

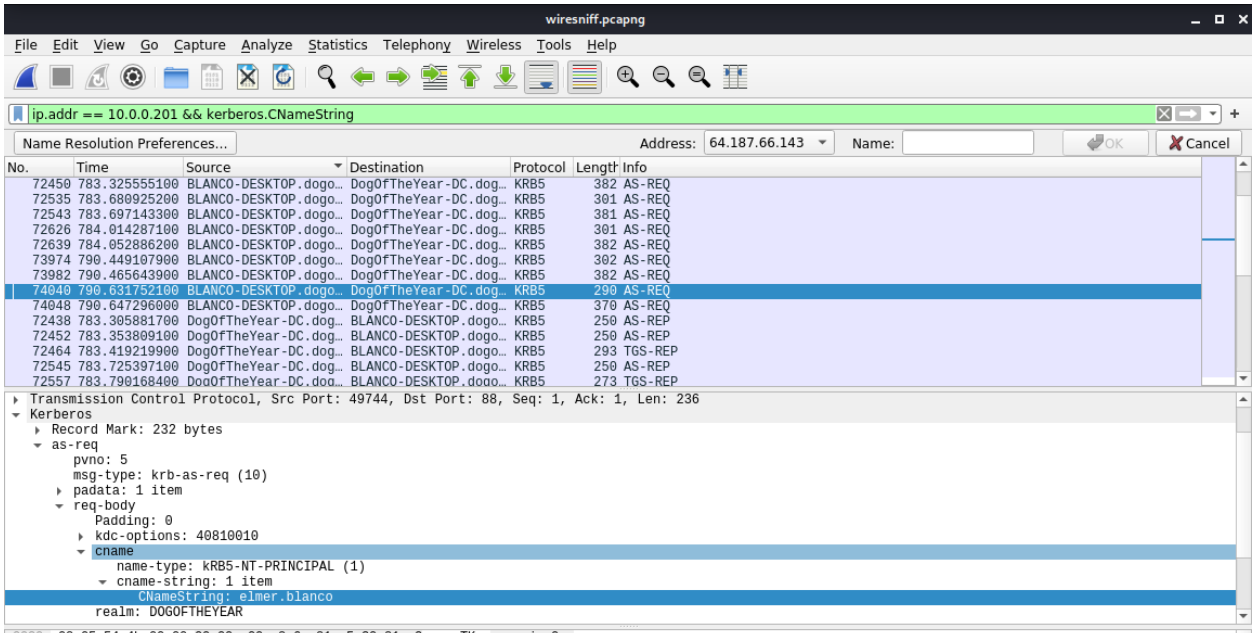
IT was informed that some users are torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringement.

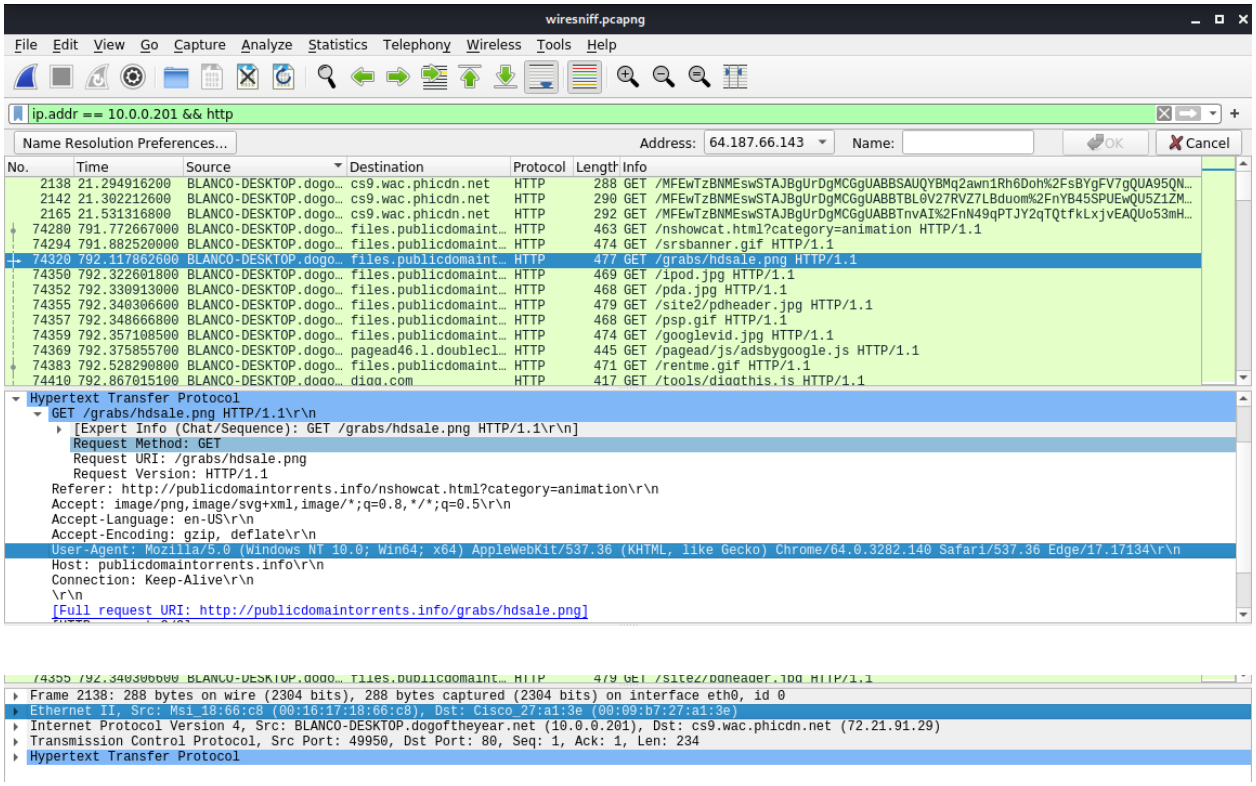
IT shared the following about the torrent activity:

- 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`:
    - Filters: ip.addr == 10.0.0.201 && kerberos.CNameStraing; ip.addr == 10.0.0.201 && HTTP
    - MAC address: 00:16:17:18:66:c8
    - Windows username: elmer.blanco
    - OS version: Windows 10

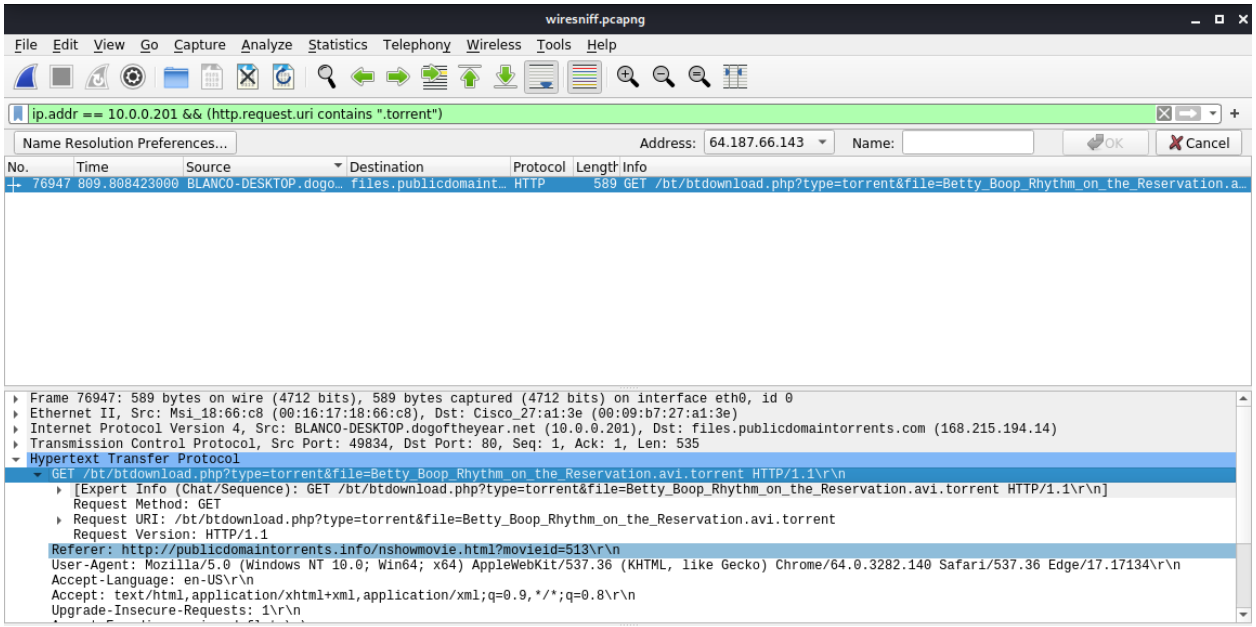




2. Which torrent file did the user download?

   Filter: ip.addr == 10.0.0.201 && (http.request.uri contains ".torrent")

   Betty_Boop_Rythm_on_the_Reservation.avi.torrent



Sources:

Can wireshark automatically resolve the IP address into host names? Wireshark Q&A. (n.d.). Retrieved March 19, 2022, from https://osqa-ask.wireshark.org/questions/37680/can-wireshark-automatically-resolve-the-ip-address-into-host-names/