Network Analysis

Time Thieves

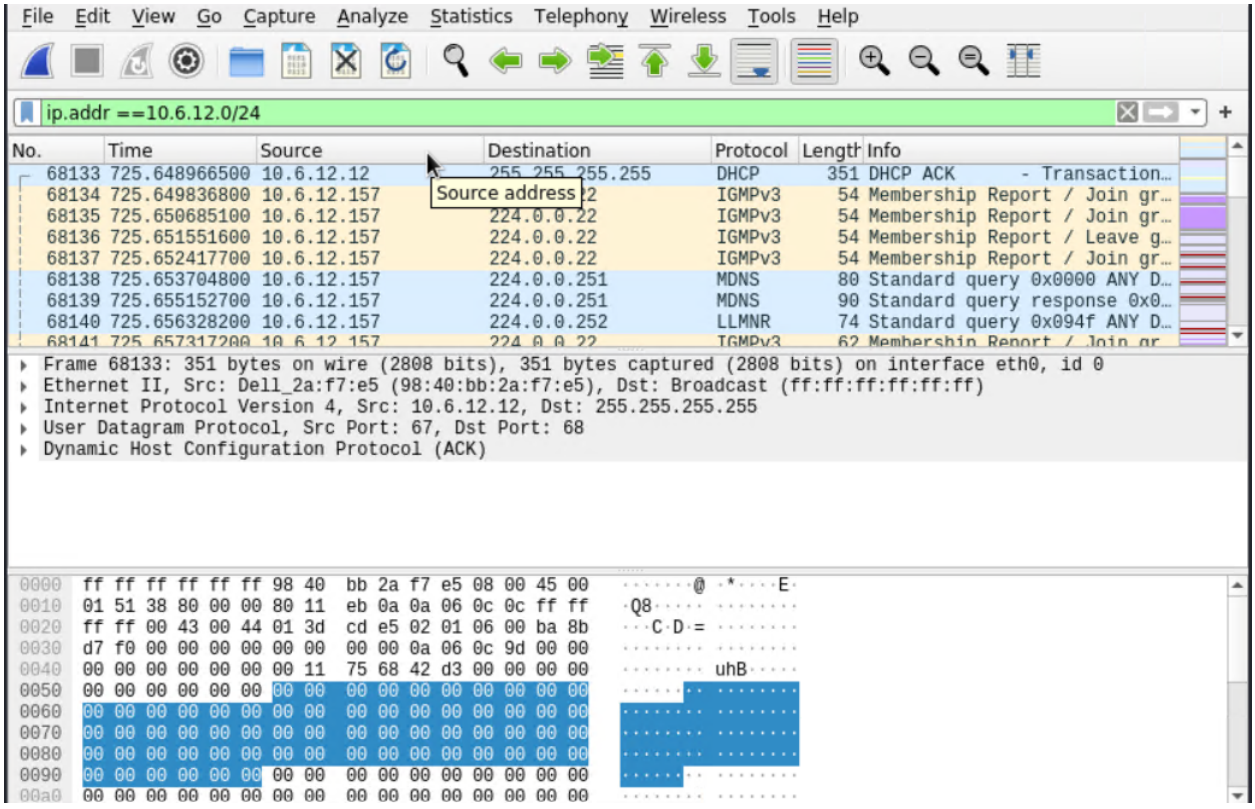
At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- 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?

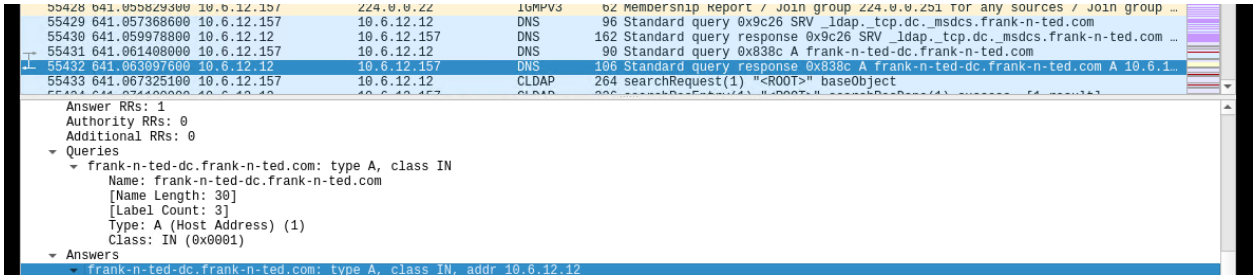
   Domain name: frank -n- Ted-DC.frank-n-ted.com



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

Ip address: 10.6.12.12 frank -n- Ted-DC.frank-n-ted.com

Filter: ip.add 10.6.12.0/24

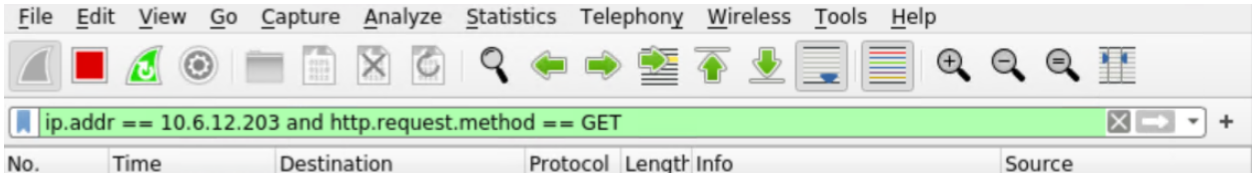


3. What is the name of the malware downloaded to the `10.6.12.203` machine? Once you have found the file, export it to your Kali machine's desktop.

File: june11.dll

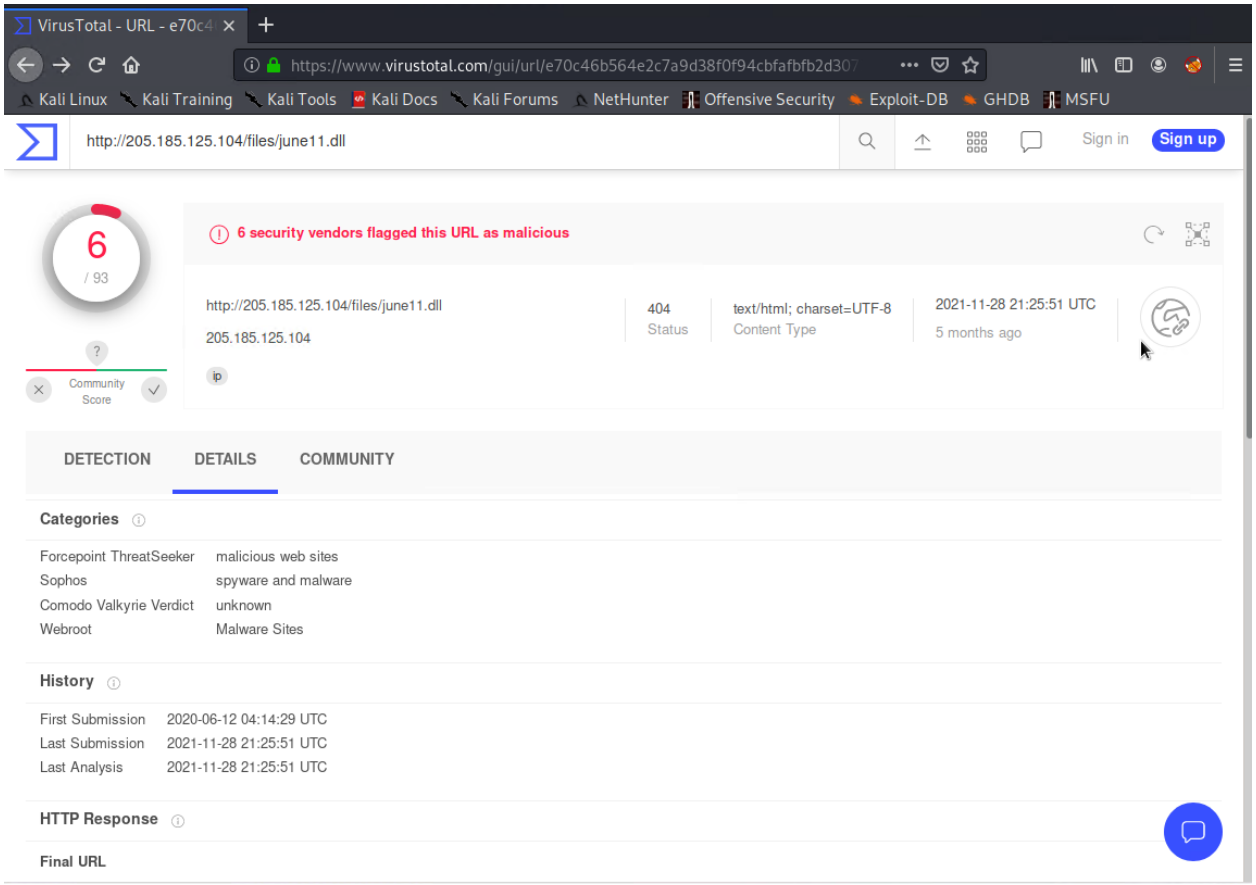
Virus: Malware

Filter: ip.addr=10.16.12.203 and http.request.method == GET



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

   This kind of malware is a TROJAN.



Vulnerable Windows Machines

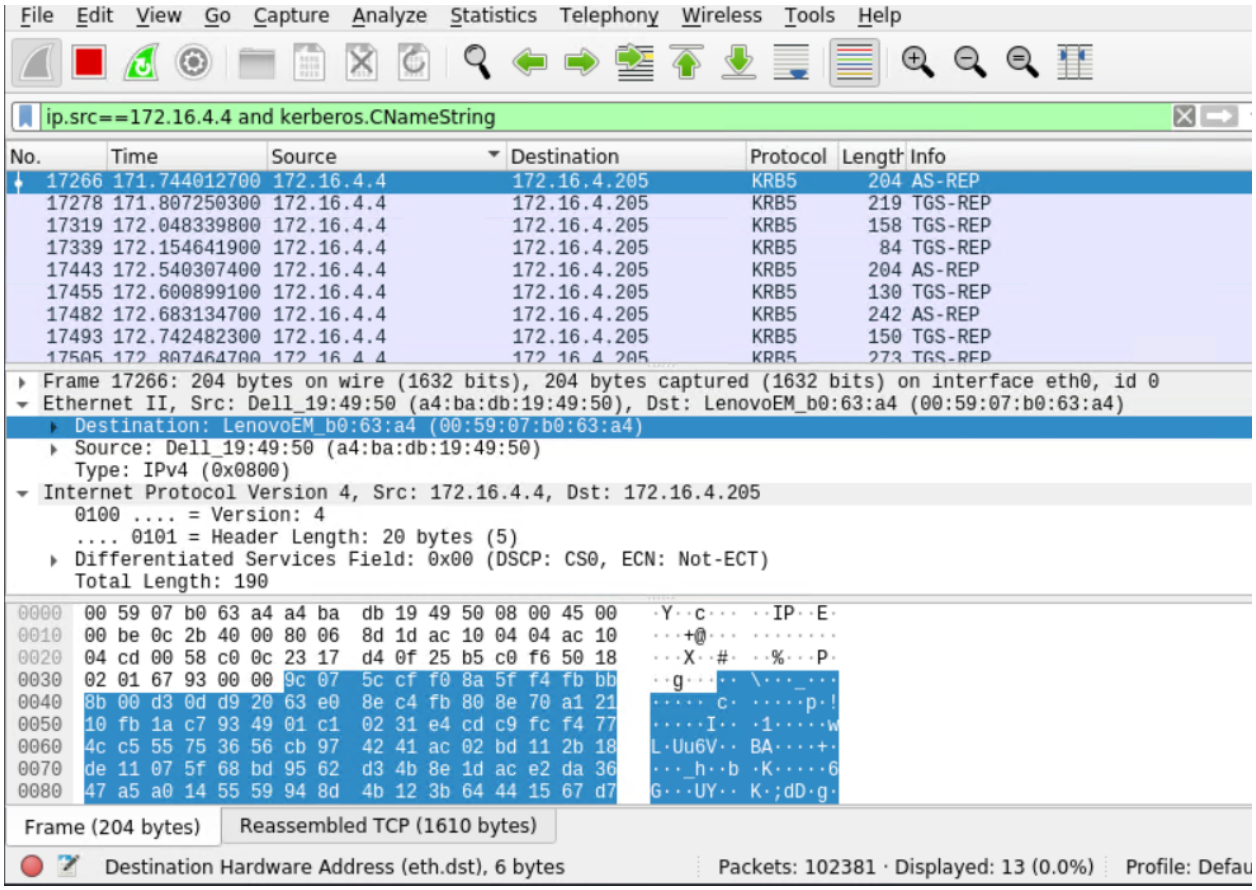
The Security team received reports of an infected Windows host on the network. They know the following:

- 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

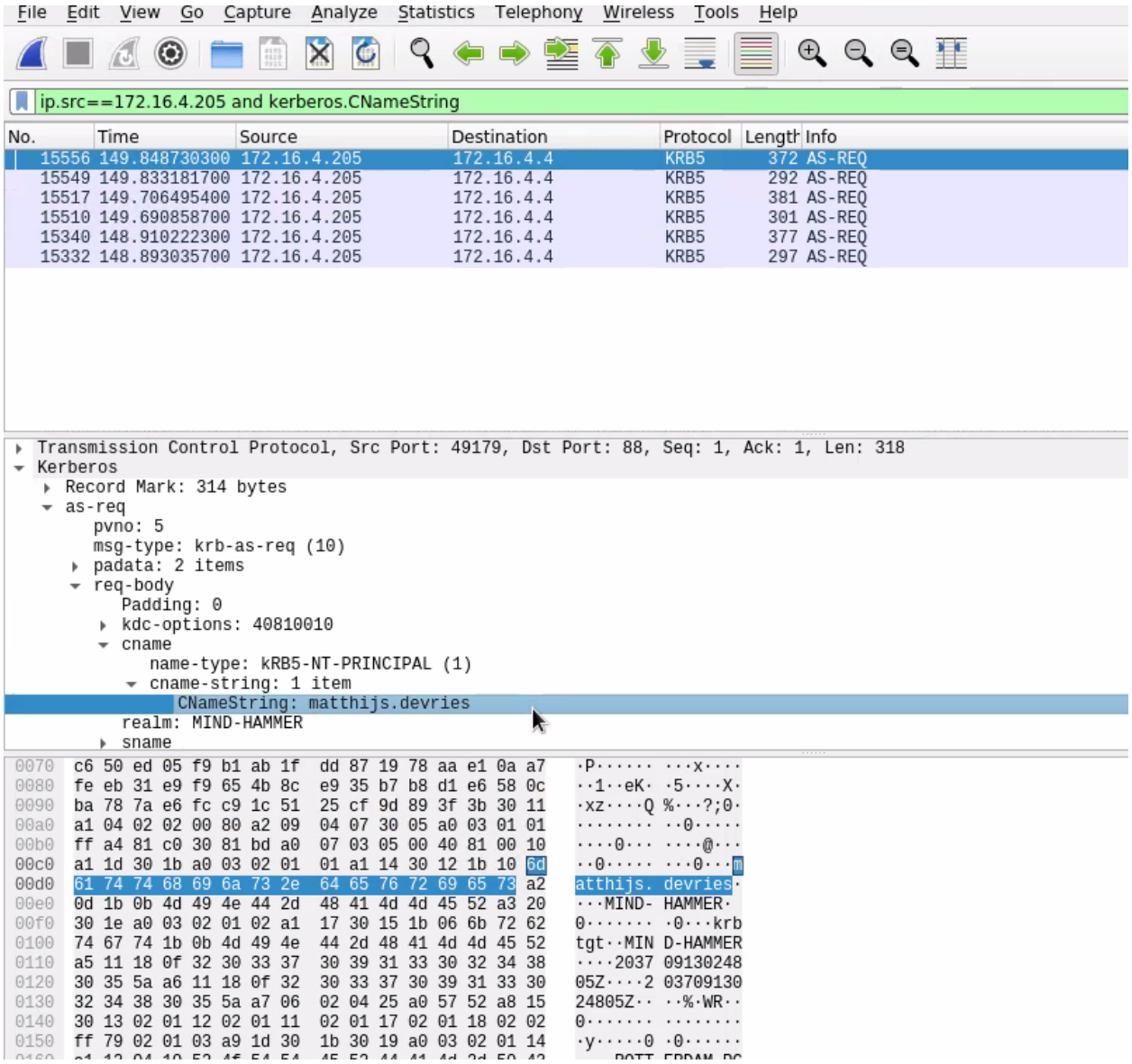
      Filter: ip.scr=172.16.4.4 and kerberos.CNameString



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

   Username: matthijs.devries

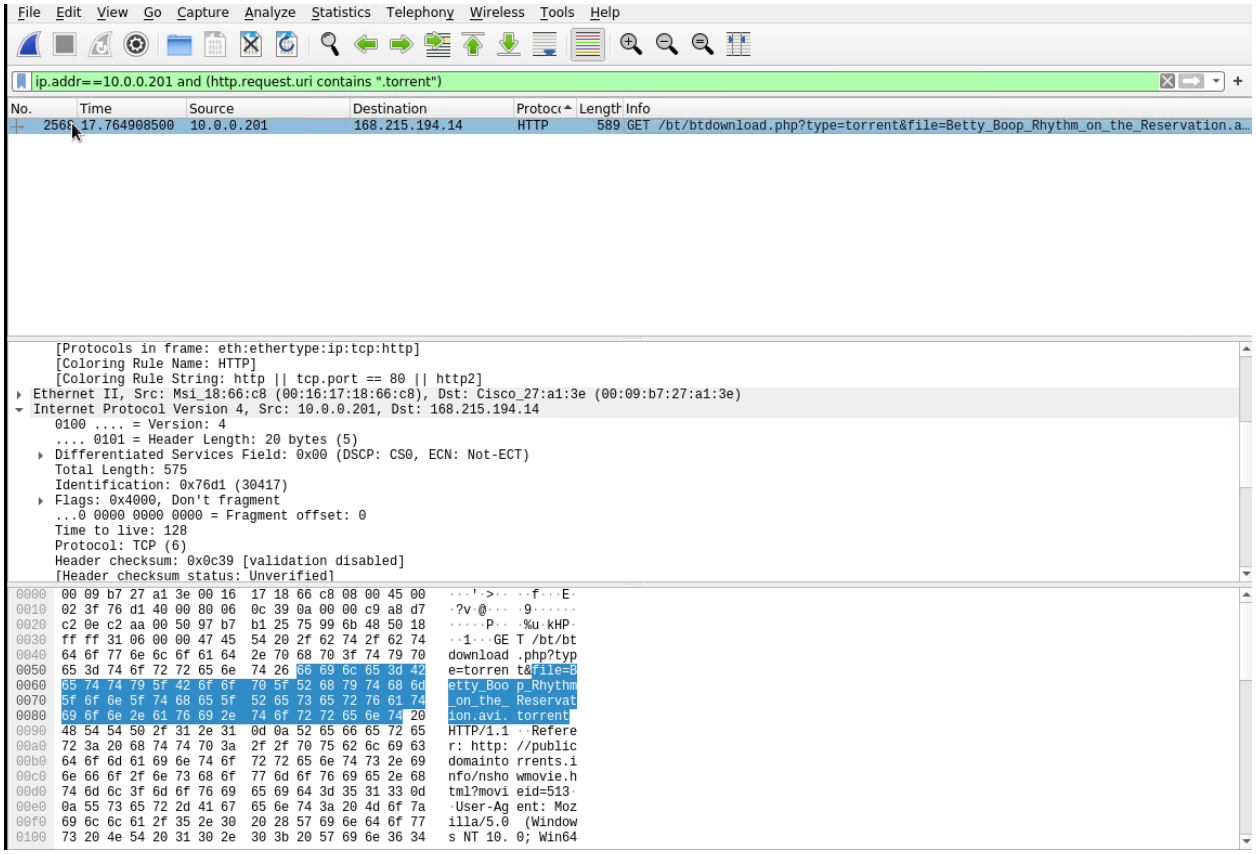
   Filter: ip.scr==172.16.4.205 and kerberos.CNameString



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

   Ip address that infect traffic is 168.215.104.14

   Filter: ip.addr==10.0.0.201 and (http.request.uri contains”.torrent”)



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
    - Windows username
    - OS version

2. Which torrent file did the user download?