Final Project Day 3 Analysis Report

Time Thieves

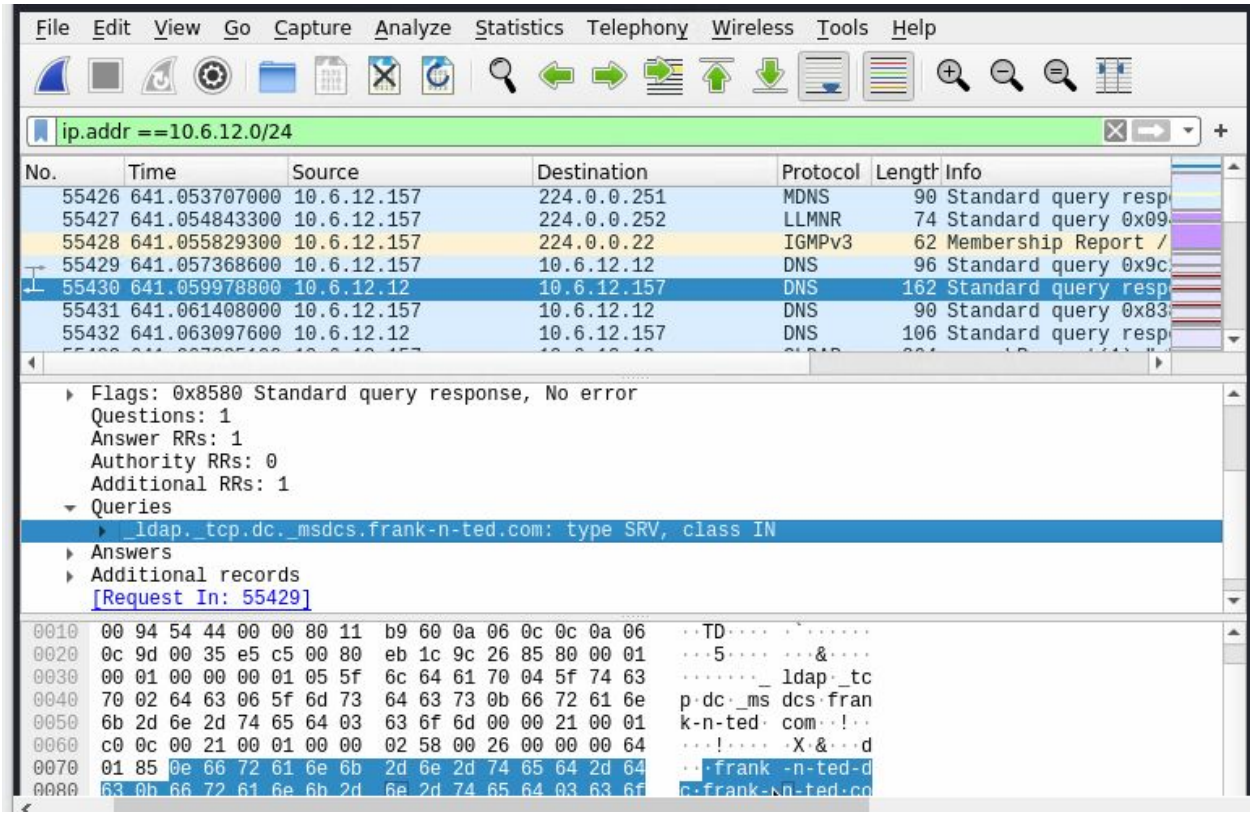
At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- 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.

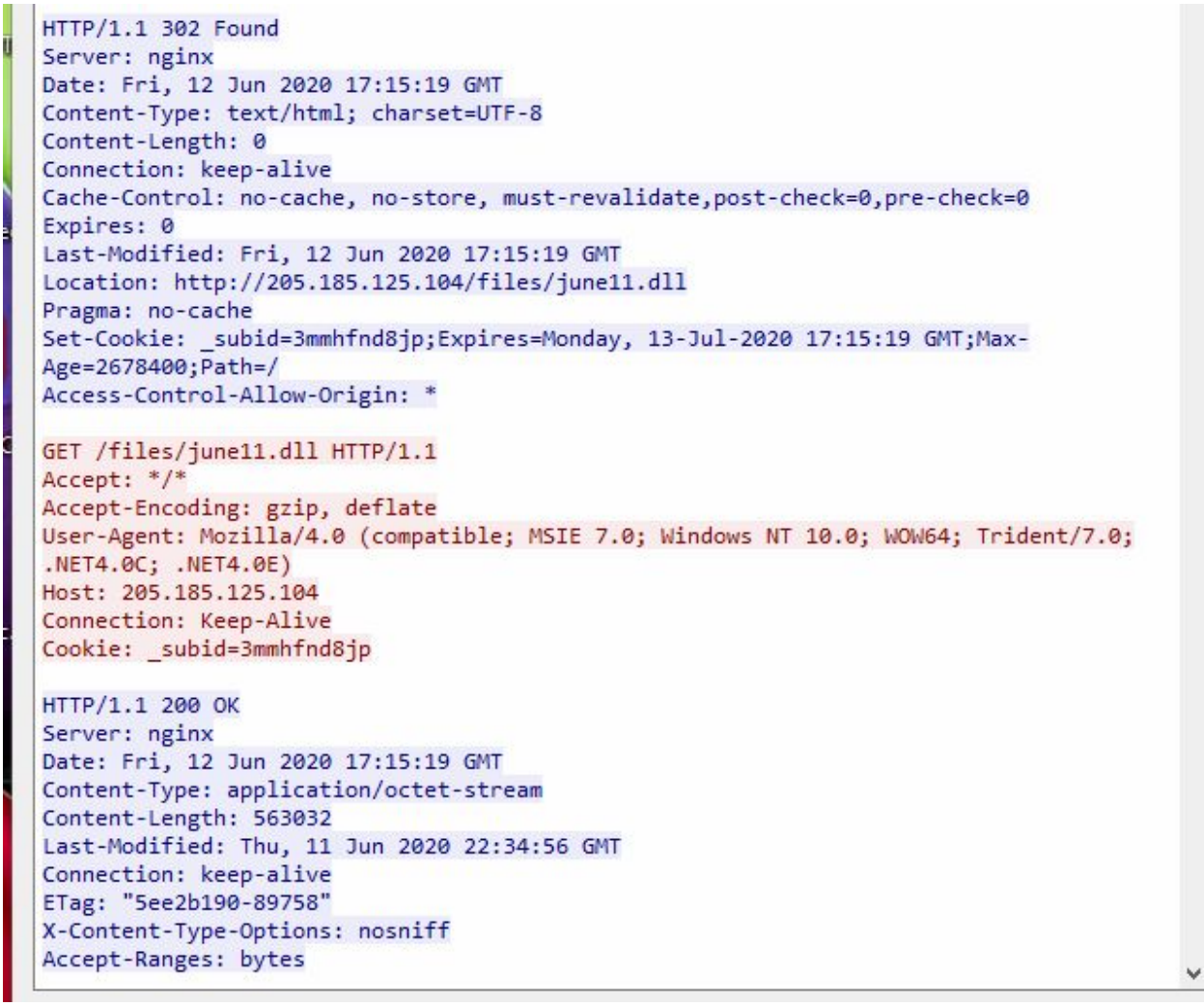
You must inspect your traffic capture to answer the following questions in your Network Report:

1. What is the domain name of the users' custom site?

   The domain is frank-n-ted.com



2. What is the IP address of the Domain Controller (DC) of the AD network? Ip address for the domain controller is 10.6.12.12
   3.What is the name of the malware downloaded to the 10.6.12.203 machine?

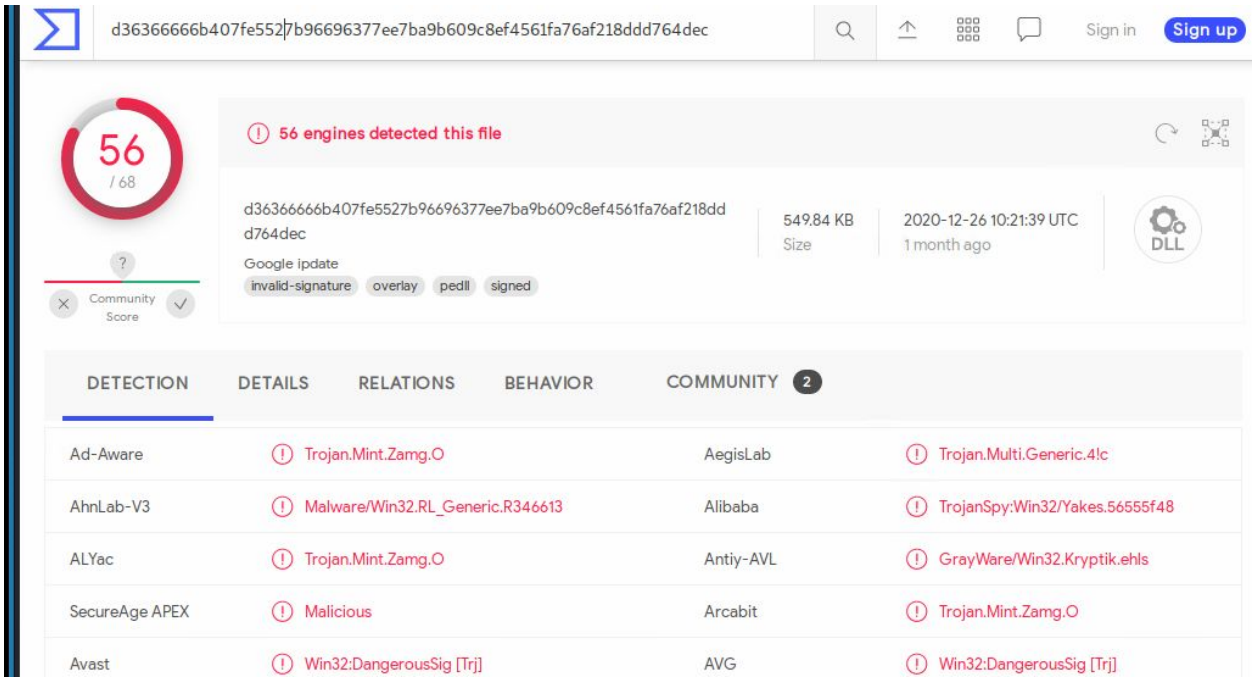


```
HTTP/1.1 302 Found
Server: nginx
Date: Fri, 12 Jun 2020 17:15:19 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Connection: keep-alive
Cache-Control: no-cache, no-store, must-revalidate,post-check=0,pre-check=0
Expires: 0
Last-Modified: Fri, 12 Jun 2020 17:15:19 GMT
Location: http://205.185.125.104/files/june11.dll
Pragma: no-cache
Set-Cookie: _subid=3mmhfnd8jp;Expires=Monday, 13-Jul-2020 17:15:19 GMT;Max-
Age=2678400;Path=/
Access-Control-Allow-Origin: *

GET /files/june11.dll HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0;
.NET4.0C; .NET4.0E)
Host: 205.185.125.104
Connection: Keep-Alive
Cookie: _subid=3mmhfnd8jp

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 12 Jun 2020 17:15:19 GMT
Content-Type: application/octet-stream
Content-Length: 563032
Last-Modified: Thu, 11 Jun 2020 22:34:56 GMT
Connection: keep-alive
ETag: "5ee2b190-89758"
X-Content-Type-Options: nosniff
Accept-Ranges: bytes
```

   june11.dll

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

4.Upload the file to VirusTotal.com.



june11.dll is a well-known malware

5. What kind of malware is this classified as?

Trojan horse

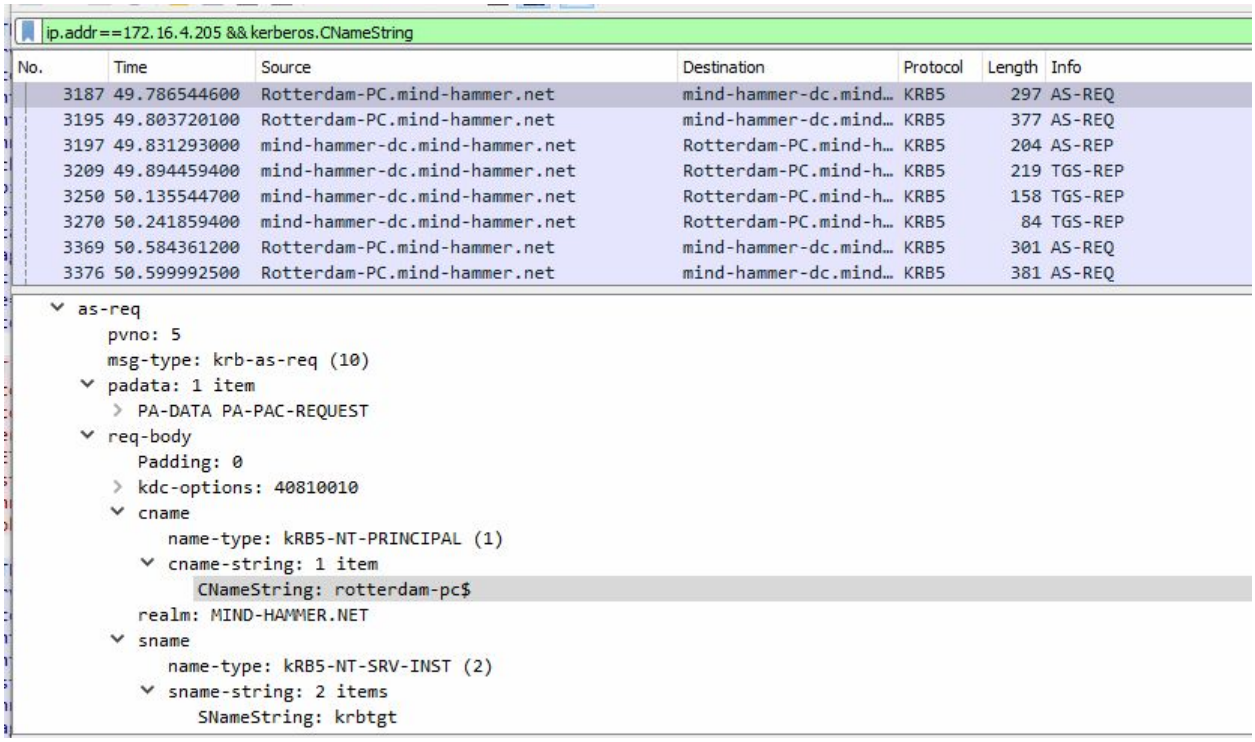
Vulnerable Windows Machines

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. It is 172.16.4.205
- 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.

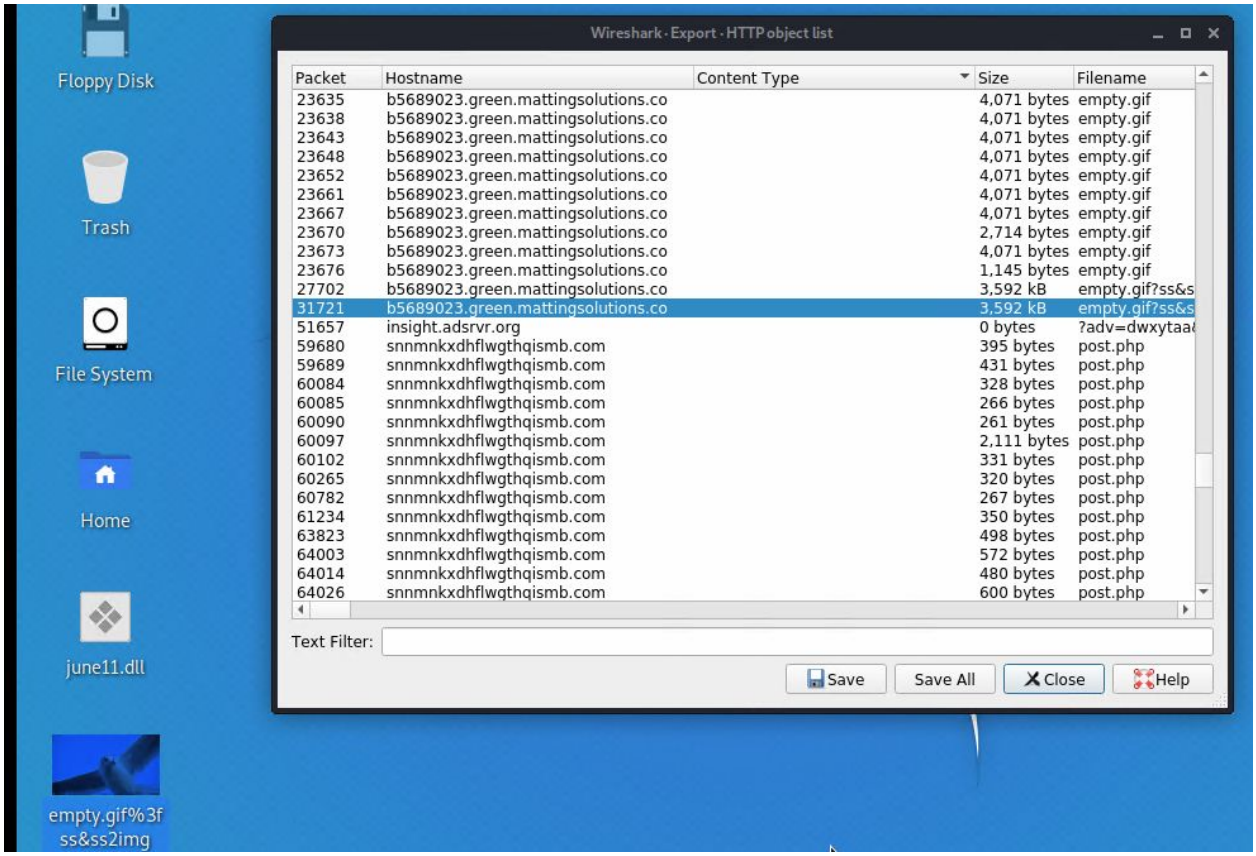
Inspect your traffic to answer the following questions in your network report:

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? rotterdam-pc



3. What are the IP addresses used in the actual infection traffic? 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 in your Network Report:

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: blanco-desktop
    - OS version: Windows
2. Which torrent file did the user download?

The user downloaded Betty_Booop_Rythm_on_the_Reservation.avi.torrent