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? **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. **june11.dll**

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

   This is a Trojan Horse which soon after infection caused 10.6.12.203 to send http POST requests to snnmnkxdhflwgthqismb.com (ip 5.101.51.151).

Vulnerable Windows Machines

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

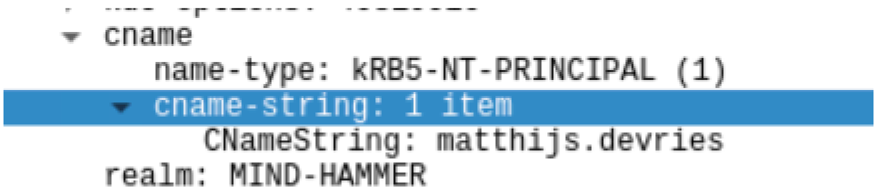
- Machines in the network live in the range `172.16.4.0/24`.
- The domain mind-hammer.net is associated with the infected computer.
- The DC for this network lives at `172.16.4.4` and is named Mind-Hammer-DC.
- The network has standard gateway and broadcast addresses.

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



```
▾ cname
    name-type: kRB5-NT-PRINCIPAL (1)
  ▾ cname-string: 1 item
      CNameString: matthijs.devries
  realm: MIND-HAMMER
```

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

    185.243.115.84 and 31.7.62.214

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

    I'm no expert on winged creatures, but it looks like a Seagull:

Illegal Downloads

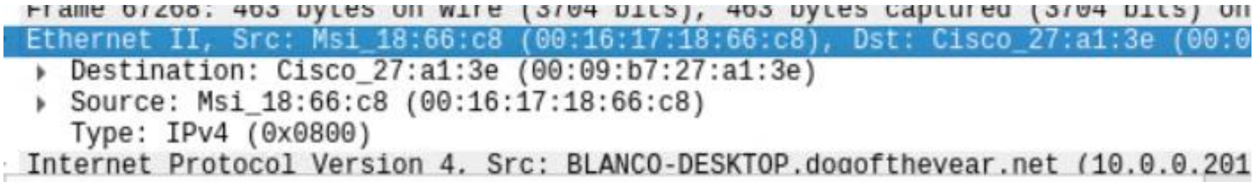
IT was informed that some users are torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringement.

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.

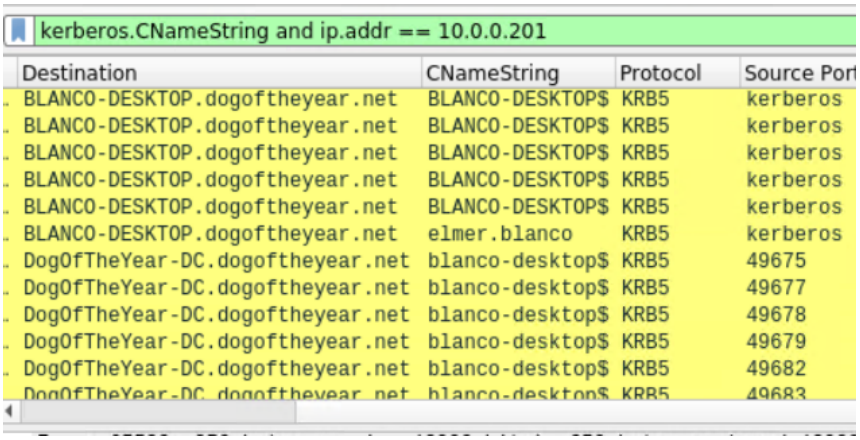
Your task is to isolate torrent traffic and answer the following questions:

1. Find the following information about the machine with IP address `10.0.0.201`:
    - MAC address **00:16:17:18:66:c8**



```
Frame 67268: 463 bytes on wire (3704 bits), 463 bytes captured (3704 bits) on
Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Cisco_27:a1:3e (00:0
  ▸ Destination: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
  ▸ Source: Msi_18:66:c8 (00:16:17:18:66:c8)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201
```

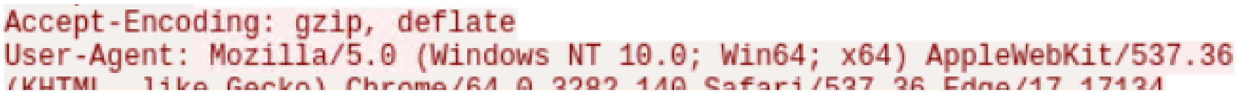
- Windows username: **elmer.blanco**



kerberos.CNameString and ip.addr == 10.0.0.201

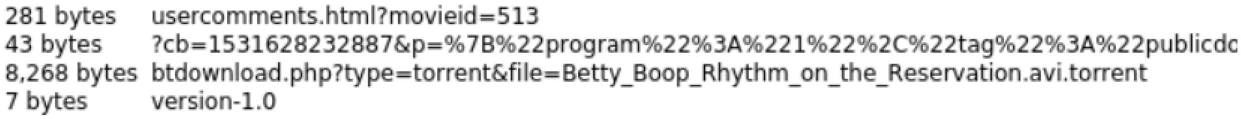
Destination	CNameString	Protocol	Source Port
BLANCO-DESKTOP.dogoftheyear.net	BLANCO-DESKTOP$	KRB5	kerberos
BLANCO-DESKTOP.dogoftheyear.net	BLANCO-DESKTOP$	KRB5	kerberos
BLANCO-DESKTOP.dogoftheyear.net	BLANCO-DESKTOP$	KRB5	kerberos
BLANCO-DESKTOP.dogoftheyear.net	BLANCO-DESKTOP$	KRB5	kerberos
BLANCO-DESKTOP.dogoftheyear.net	BLANCO-DESKTOP$	KRB5	kerberos
BLANCO-DESKTOP.dogoftheyear.net	elmer.blanco	KRB5	kerberos
DogOfTheYear-DC.dogoftheyear.net	blanco-desktop$	KRB5	49675
DogOfTheYear-DC.dogoftheyear.net	blanco-desktop$	KRB5	49677
DogOfTheYear-DC.dogoftheyear.net	blanco-desktop$	KRB5	49678
DogOfTheYear-DC.dogoftheyear.net	blanco-desktop$	KRB5	49679
DogOfTheYear-DC.dogoftheyear.net	blanco-desktop$	KRB5	49682
DogOfTheYear-DC.dogoftheyear.net	blanco-desktop$	KRB5	49683

- OS version: **Windows 10**



```
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134
```

2. Which torrent file did the user download?
   Betty_Boop_Rhythm_on_the_Reservation.avi.torrent



```
281 bytes     usercomments.html?movieid=513
43 bytes      ?cb=1531628232887&p=%7B%22program%22%3A%221%22%2C%22tag%22%3A%22publicdc
8,268 bytes   btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
7 bytes       version-1.0
```