

Network Analysis

Time Thieves

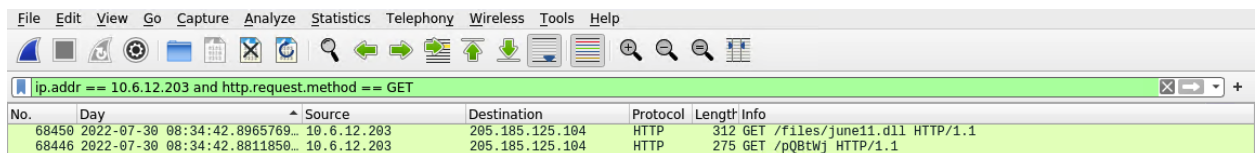
At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- 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 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.

- **June11.dll**



The screenshot shows the Wireshark interface with a filter applied: `ip.addr == 10.6.12.203 and http.request.method == GET`. The packet list shows two packets. Packet 68450 is a GET request for `/files/june11.dll` from 10.6.12.203 to 205.185.125.104. Packet 68446 is a GET request for `/pQbtWj` from 10.6.12.203 to 205.185.125.104.

No.	Time	Source	Destination	Protocol	Length	Info
68450	2022-07-30 08:34:42.8965769...	10.6.12.203	205.185.125.104	HTTP	312	GET /files/june11.dll HTTP/1.1
68446	2022-07-30 08:34:42.8811850...	10.6.12.203	205.185.125.104	HTTP	275	GET /pQbtWj HTTP/1.1

4. Upload the file to [VirusTotal.com](https://www.virustotal.com). 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.
- 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**

```
 Ethernet II, Src: Dell_19:49:50 (a4:ba:db:19:49:50), Dst: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
   Destination: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
   Source: Dell_19:49:50 (a4:ba:db:19:49:50)
   Type: IPv4 (0x0800)
 Internet Protocol Version 4, Src: 172.16.4.4, Dst: 172.16.4.205
   0100 .... = Version: 4
```

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

Matthijs. Devries Ip.addr == 172.16.4.0/24 && kerberos.CNameString

```
 Kerberos
   Record Mark: 1675 bytes
     0... .. = Reserved: Not set
     .000 0000 0000 0000 0000 0110 1000 1011 = Record Length: 1675
   tgs-rep
     pvno: 5
     msg-type: krb-tgs-rep (13)
     crealm: MIND-HAMMER.NET
     cname
       name-type: kRB5-NT-PRINCIPAL (1)
       cname-string: 1 item
         CNameString: matthijs.devries
```

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

182.243.115.84

Ways → Statistics > Conversation then, look at the TCP tab.

We went with the most amount of bytes.

Ethernet · 74		IPv4 · 879		IPv6		TCP · 1099		UDP · 1826					
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration		
172.16.4.205	49249	182.243.115.84	80	36,648	33 M	19,506	15 M	17,142	17 M	262.167251	1116.7497		

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

MAC address: 00:16:17:18:66:c8

Windows username: elmer.blanco

OS version: Windows NT 10.0; Win64; x64 (Windows 10)

```
▼ cname
  name-type: kRB5-NT-PRINCIPAL (1)
  ▼ cname-string: 1 item
    CNameString: blanco-desktop$
  realm: DOGOFtheyear.NET
```