

Network Analysis

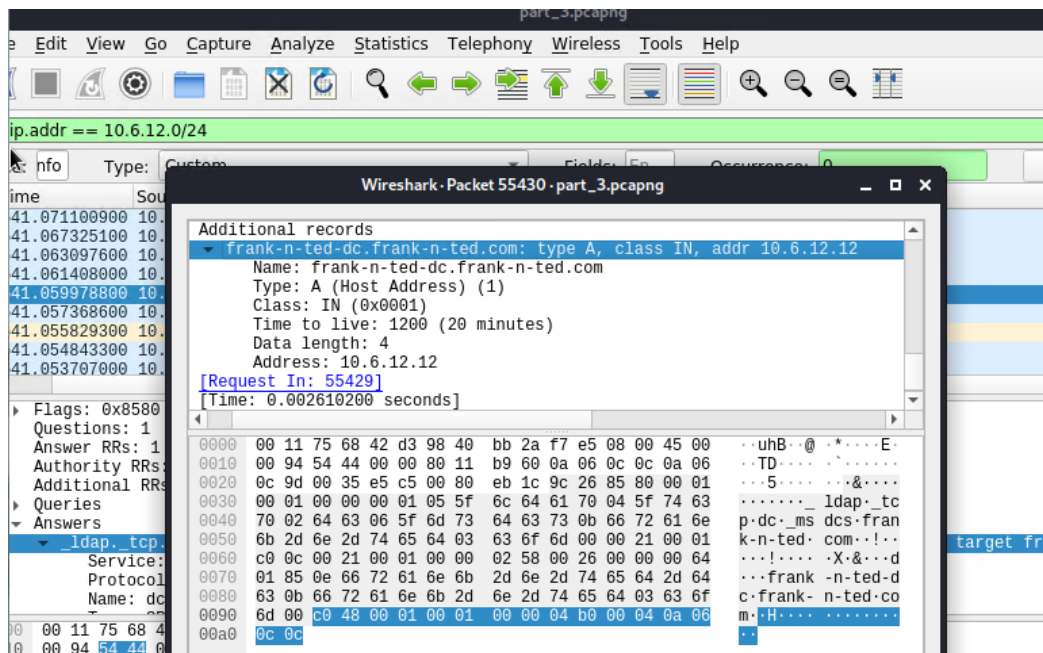
Time Thieves

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.

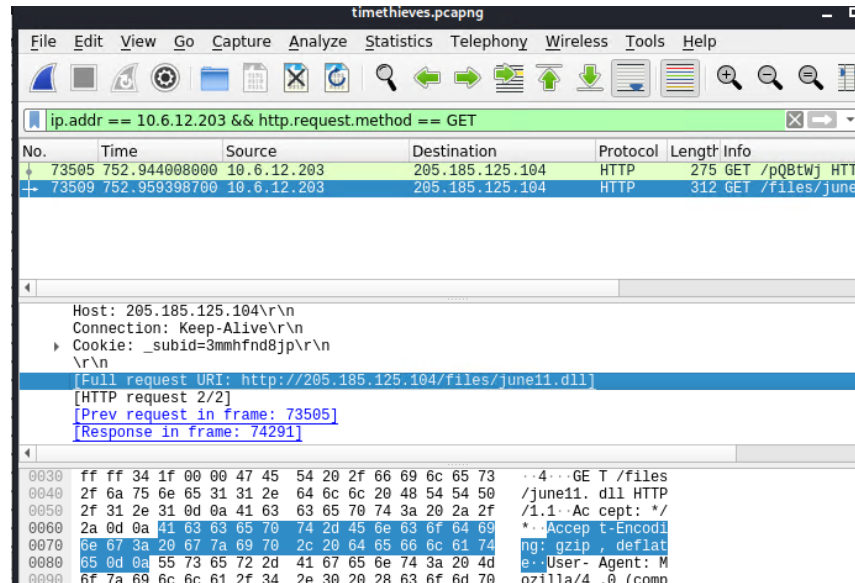
You must inspect your traffic capture to answer the following questions:

1. What is the domain name of the users' custom site?
 - a. frank-n-ted-dc.frank-n-ted.com
2. What is the IP address of the Domain Controller (DC) of the AD network?
 - a. 10.6.12.12



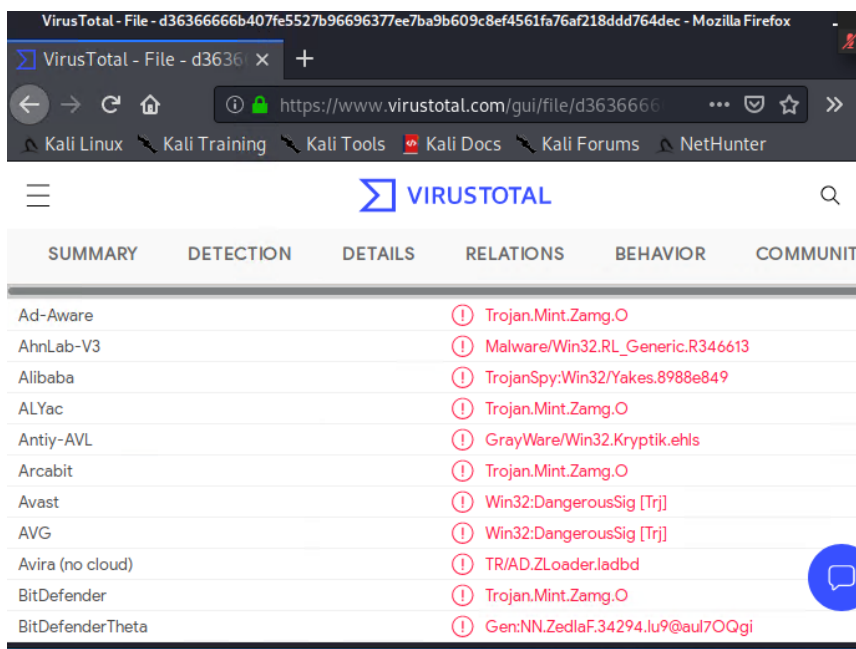
3. What is the name of the malware downloaded to the 10.6.12.203 machine? Once you have found the file, export it to your Kali machine's desktop.

b. June11.dll



4. Upload the file to [VirusTotal.com](https://www.virustotal.com). What kind of malware is this classified as?

a. Trojan



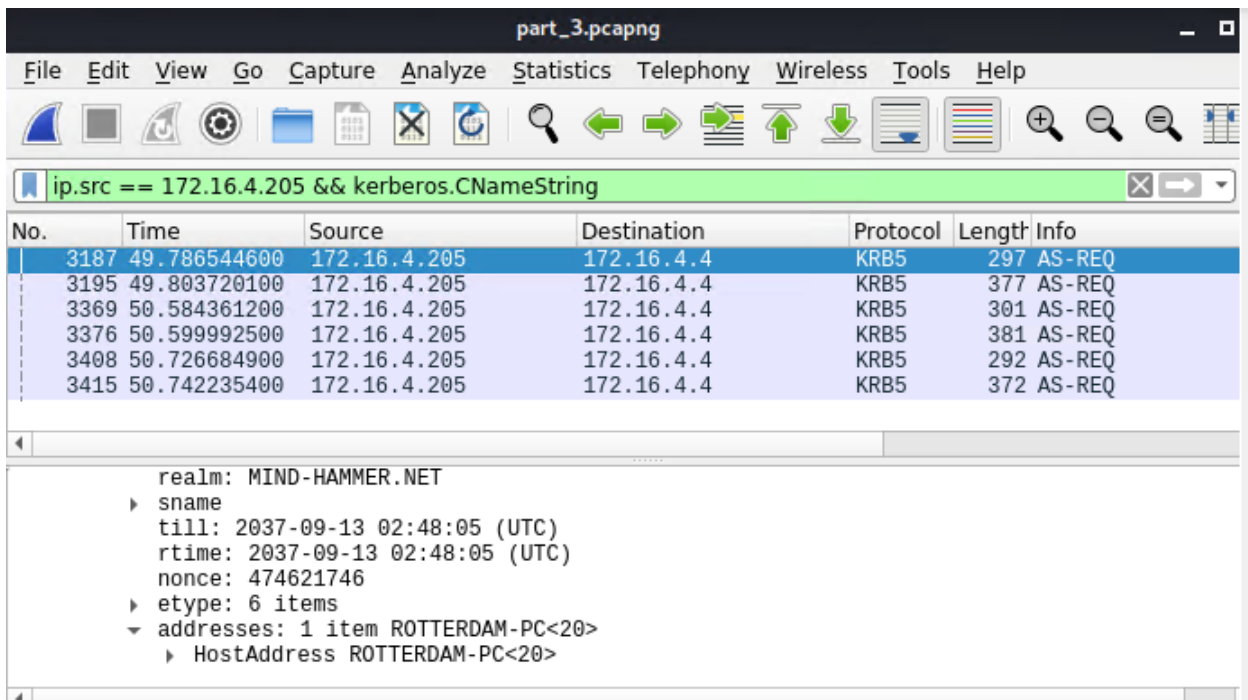
Vulnerable Windows Machines

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



The image shows a Wireshark packet capture window titled "part_3.pcapng". The filter bar contains the expression "ip.src == 172.16.4.205 && kerberos.CNameString". The packet list shows six Kerberos AS-REQ messages (No. 3187, 3195, 3369, 3376, 3408, 3415) from source 172.16.4.205 to destination 172.16.4.4. The packet details pane shows the structure of the first AS-REQ message (No. 3187):

```
realm: MIND-HAMMER.NET
  sname
  till: 2037-09-13 02:48:05 (UTC)
  rtime: 2037-09-13 02:48:05 (UTC)
  nonce: 474621746
  etype: 6 items
  addresses: 1 item ROTTERDAM-PC<20>
    HostAddress ROTTERDAM-PC<20>
```

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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
ip.src == 172.16.4.205 && kerberos.CNameString						
Title: nfo	Type: Custom	Fields: kerber		Occurrence: 0		OK
No.	Time	Source	Destination	Protocol	Length	Info
3369	50.584361200	172.16.4.205	172.16.4.4	KRB5	301	ROTTERDAM-PC\$
3376	50.599992500	172.16.4.205	172.16.4.4	KRB5	381	ROTTERDAM-PC\$
3408	50.726684900	172.16.4.205	172.16.4.4	KRB5	292	matthijs.devries
3415	50.742235400	172.16.4.205	172.16.4.4	KRB5	372	matthijs.devries
3187	49.786544600	172.16.4.205	172.16.4.4	KRB5	297	rotterdam-pc\$
3195	49.803720100	172.16.4.205	172.16.4.4	KRB5	377	rotterdam-pc\$

▼ Frame 3376: 381 bytes on wire (3048 bits), 381 bytes captured (3048 bits) on interface eth0, id 0
 ▼ Interface id: 0 (eth0)

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

- 166.62.111.64 -> 172.16.4.205
- 31.7.62.214 -> 172.16.4.205 (unencrypted HTTP detected over encrypted port)
- 172.16.4.205 -> 185.243.115.84 (large number of POST requests of an empty.gif from infected host to this IP)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
ip.addr == 172.16.4.205 && http.request.method == POST && not (ip.addr == 166.62.111.64)						
No.	Time	Source	Destination	Protocol	Length	Info
31908	461.857225000	172.16.4.205	31.7.62.214	HTTP	282	POST
31910	461.862630700	172.16.4.205	31.7.62.214	HTTP	282	POST
31912	461.867978300	172.16.4.205	31.7.62.214	HTTP	282	POST
31914	461.873360600	172.16.4.205	31.7.62.214	HTTP	282	POST
31916	461.878737100	172.16.4.205	31.7.62.214	HTTP	282	POST
31918	461.884108900	172.16.4.205	31.7.62.214	HTTP	282	POST
31920	461.889481700	172.16.4.205	31.7.62.214	HTTP	282	POST
31922	461.894862500	172.16.4.205	31.7.62.214	HTTP	282	POST
31924	461.900391700	172.16.4.205	31.7.62.214	HTTP	282	POST
31926	461.905611400	172.16.4.205	31.7.62.214	HTTP	282	POST
31928	461.911002900	172.16.4.205	31.7.62.214	HTTP	282	POST
31930	461.916391200	172.16.4.205	31.7.62.214	HTTP	282	POST
31932	461.921739500	172.16.4.205	31.7.62.214	HTTP	282	POST
31958	462.032424900	172.16.4.205	31.7.62.214	HTTP	282	POST
31960	462.037739500	172.16.4.205	31.7.62.214	HTTP	282	POST

▼ Hypertext Transfer Protocol

▼ [Expert Info (Warning/Security): Unencrypted HTTP protocol detected over encrypted port, could indicate a ...
 [Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous misconfiguration.]
 [Severity level: Warning]
 [Group: Security]

▶ POST http://31.7.62.214/fakeurl.htm HTTP/1.1
 User-Agent: NetSupport Manager/1.3
 Content-Type: application/x-www-form-urlencoded
 Content-Length: 36
 Host: 31.7.62.214
 Connection: Keep-Alive

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: 00:12:3f:f4:3b:96
 - Windows username: elmer.blanco
 - OS version: Windows 10

The image shows a Wireshark packet capture window titled "part_3.pcapng". The filter bar contains the expression "ip.addr == 10.0.0.201 && kerberos.CNameString". The packet list shows several Kerberos messages (KRB5) from source 10.0.0.2 to destination 10.0.0.201. The selected packet (packet 67080) is expanded, showing the Ethernet II header and the IP header. The Ethernet II header shows the source MAC as Dell_f4:3b:96 (00:12:3f:f4:3b:96) and the destination MAC as Msi_18:66:c8 (00:16:17:18:66:c8). The IP header shows the source as 10.0.0.2 and the destination as 10.0.0.201. The packet details pane shows the Kerberos message structure, including the CNameString field.

Time	Source	Destination	Protocol	Length	Info
67080	751.379585100 10.0.0.2	10.0.0.201	KRB5	303	elmer.blanco
67058	751.294737700 10.0.0.2	10.0.0.201	KRB5	175	elmer.blanco
66992	751.115116900 10.0.0.2	10.0.0.201	KRB5	199	BLANCO-DESKTOP\$
65839	745.233051500 10.0.0.2	10.0.0.201	KRB5	114	BLANCO-DESKTOP\$
65827	745.174120600 10.0.0.2	10.0.0.201	KRB5	293	BLANCO-DESKTOP\$
65798	745.008607500 10.0.0.2	10.0.0.201	KRB5	227	BLANCO-DESKTOP\$
65745	744.704098600 10.0.0.2	10.0.0.201	KRB5	293	BLANCO-DESKTOP\$

[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]
Ethernet II, Src: Dell_f4:3b:96 (00:12:3f:f4:3b:96), Dst: Msi_18:66:c8 (00:16:17:18:66:c8)
▼ Destination: Msi_18:66:c8 (00:16:17:18:66:c8)
Address: Msi_18:66:c8 (00:16:17:18:66:c8)
.....0. = LG bit: Globally unique address (factory default)
.....0. = IG bit: Individual address (unicast)
▼ Source: Dell_f4:3b:96 (00:12:3f:f4:3b:96)
Address: Dell_f4:3b:96 (00:12:3f:f4:3b:96)

00 00 16 17 18 66 c8 00 12 3f f4 3b 96 08 00 45 00f...?;...E.
10 01 21 07 68 40 00 80 06 dd a4 0a 00 00 02 0a 00 ...!h@...
20 00 c9 00 58 c2 55 60 c1 b0 a1 c4 30 82 ba 50 18 ...X-U`...0..P.
30 08 05 d5 8c 00 00 2f 70 e3 62 4c f2 01 fd 4b 5f .../p..bL...K_

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

The image shows a Wireshark network traffic capture. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. A filter bar at the top displays the filter: `ip.addr == 10.0.0.201 && http.request.method == GET`. The main packet list table shows several HTTP GET requests. The selected packet (packet 69706) is an HTTP GET request to 168.215.194.14. The packet details pane shows the TCP payload (535 bytes) and the Hypertext Transfer Protocol section, which contains the request line: `GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n`. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
69980	771.231145500	10.0.0.201	168.215.194.14	HTTP	434	GET
69754	770.572697300	10.0.0.201	91.189.95.21	HTTP	423	GET
69750	770.563257500	10.0.0.201	140.211.166.134	HTTP	195	GET
69706	770.366956400	10.0.0.201	168.215.194.14	HTTP	589	GET
69542	769.560506300	10.0.0.201	52.94.233.131	HTTP	1067	GET
69470	768.919511100	10.0.0.201	72.21.202.62	HTTP	885	GET
69434	768.625230500	10.0.0.201	52.94.240.125	HTTP	427	GET

TCP payload (535 bytes)

Hypertext Transfer Protocol

- GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n
 - [Expert Info (Chat/Sequence): GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n]
 - [Severity level: Chat]
 - [Group: Sequence]
 - Request Method: GET

0000 00 09 b7 27 a1 3e 00 16 17 18 66 c8 08 00 45 00 ...'>...f...E