Network Analysis Report

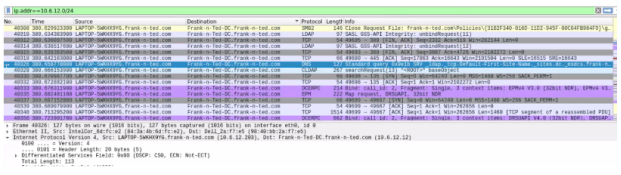
By Briana Norman

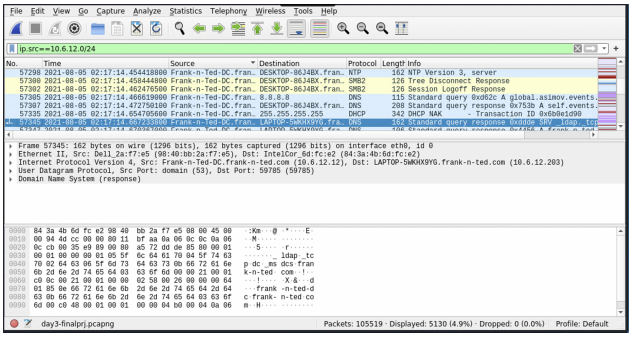
Time Thieves

⇥ Inspect the traffic captured, their IP addresses were somewhere in the range 10.6.12.0/24.

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

- **frank-n-ted.com**



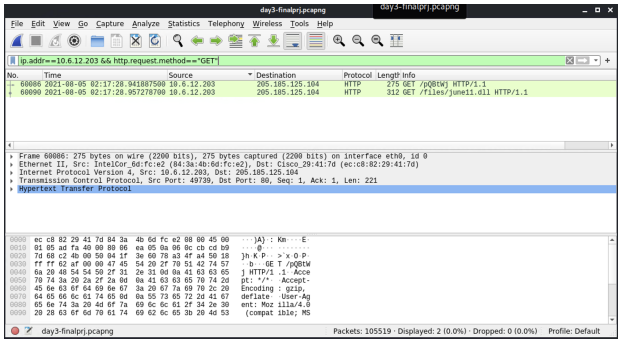


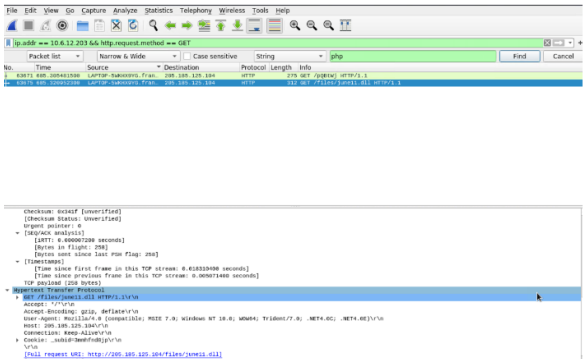
2. What is the IP address of the Domain Controller (DC) of the AD network?

- **10.6.12.12**

3. What is the name of the malware downloaded to the 10.6.12.203 machine?

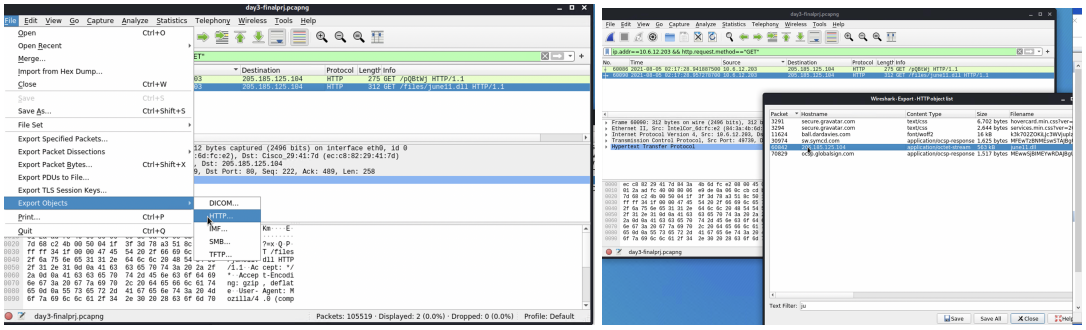
- **June11.dll**



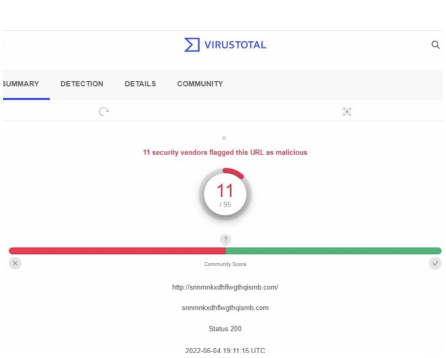


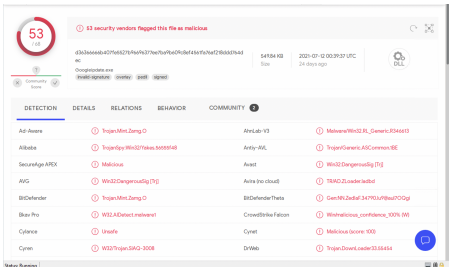
⇥ **Exported the file to Kali machine's desktop.**

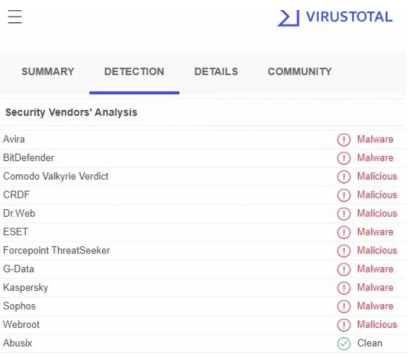
⇥ **Clicked on packet that displays malware --> File --> ExportObjects --> HTTP--> june11.dll**

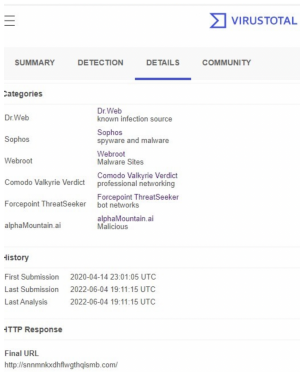


4. Uploaded the file to VirusTotal.com.



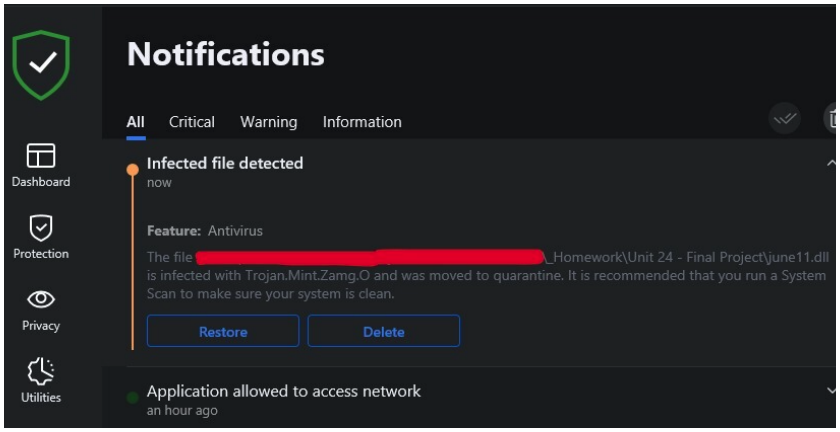






5. What kind of malware is this classified as?

⇥ ***June11.dll = Trojan***



Vulnerable Windows Machine

⇥ ***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 (malicious ip)***

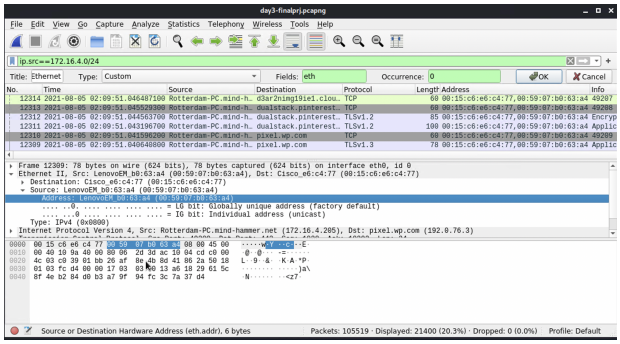
⇥ ***The network has standard gateway and broadcast addresses.***

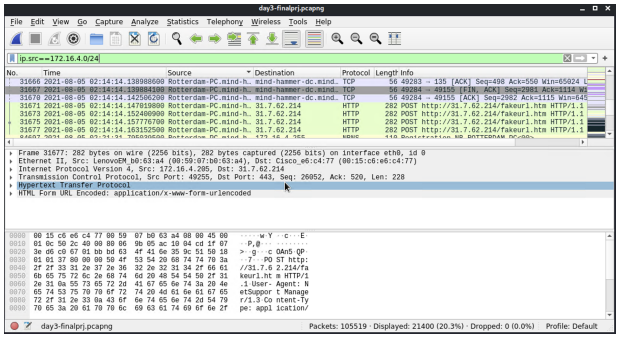
1. Find the following information about the infected Windows machine:

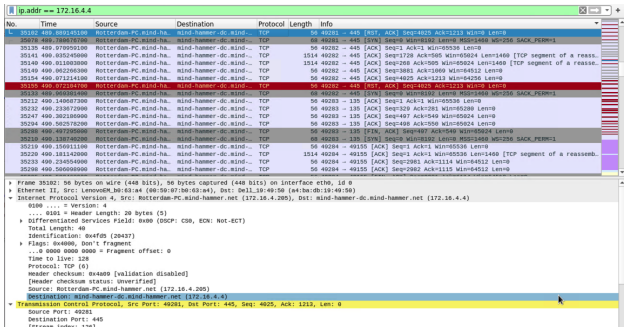
⇥ **Host name:** ***ROTTERDAM-PC***

⇥ **IP address:** ***172.16.4.205***

⇥ **MAC address:** ***00:59:07:b0:63:a4***

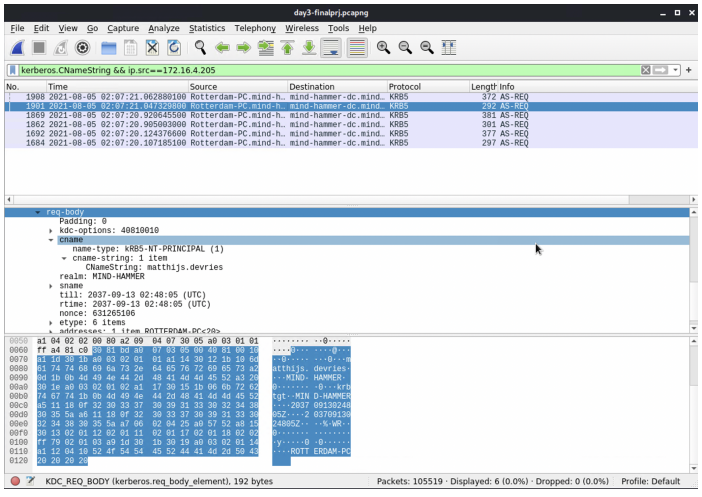


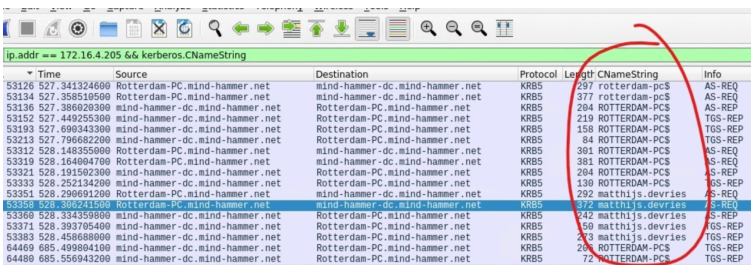




2. What is the username of the Windows user whose computer is infected? *Kerberos.CNameString && ip.src==172.16.4.205 (victim machine ip)*

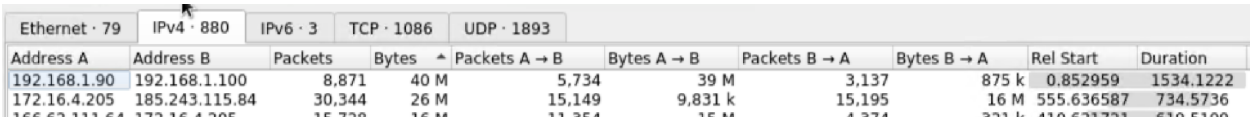
- ***Matthijs.devries***





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

→ **185.243.115.84**



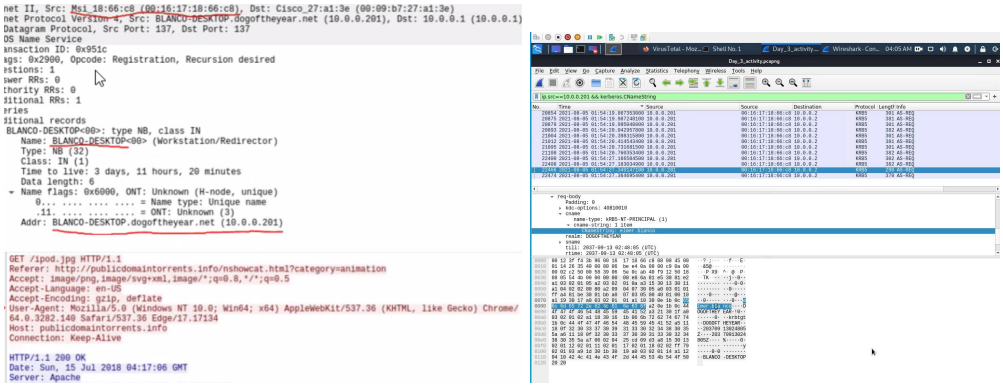
Ethernet · 79 | IPv4 · 880 | IPv6 · 3 | TCP · 1086 | UDP · 1893

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
192.168.1.90	192.168.1.100	8,871	40 M	5,734	39 M	3,137	875 k	0.852959	1534.1222
172.16.4.205	185.243.115.84	30,344	26 M	15,149	9,831 k	15,195	16 M	555.636587	734.5736

Illegal Downloads

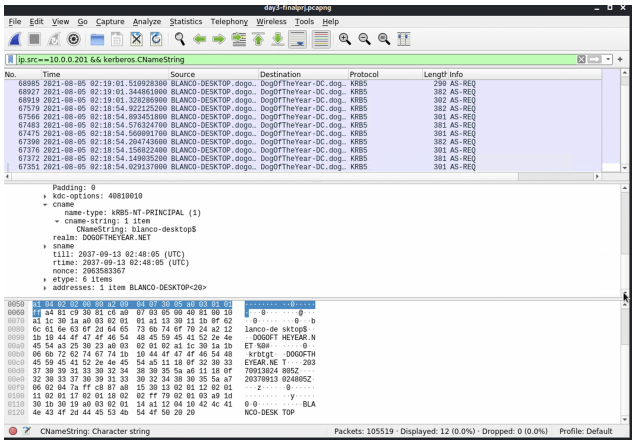
2. Find the following information about the machine with IP address 10.0.0.201:

MAC address: 00:16:17:18:66:c8
Windows username: elmer.blanco *aka* blanco-desktop
OS version: Windows 10 NT 10.0; Win64; x64



```
net II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
net Protocol Version 4, Src: BLANCO-DESKTOP.DOGOFTHEYEAR.net (10.0.0.201), Dst: 10.0.0.1 (10.0.0.1)
Datagram Protocol, Src Port: 137, Dst Port: 137
OS Name Service
nsaction ID: 0x951c
gs: 0x2900, Opcode: Registration, Recursion desired
stions: 1
swer RRs: 0
thority RRs: 0
itional RRs: 1
ries
itional records
  BLANCO-DESKTOP<00>: type NB, class IN
    Name: BLANCO-DESKTOP<00> (Workstation/Redirector)
    Type: NB (32)
    Class: IN (1)
    Time to live: 3 days, 11 hours, 20 minutes
    Data length: 6
  ▾ Name flags: 0x6000, ONT: Unknown (H-node, unique)
      0... .... .... .... = Name type: Unique name
      .11. .... .... .... = ONT: Unknown (3)
    Addr: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201)
```

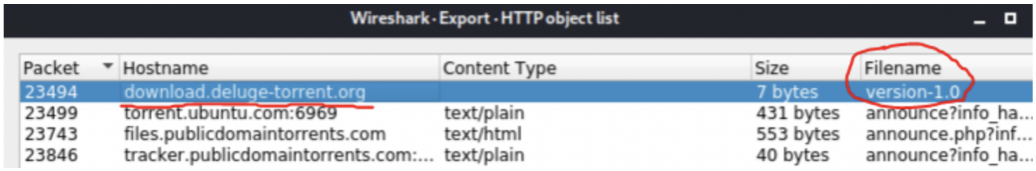
```
GET /ipod.jpg HTTP/1.1
Referer: http://publicdomaintorrents.info/nshowcat.html?category=animation
Accept: image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
64.0.3282.140 Safari/537.36 Edge/17.17134
Host: publicdomaintorrents.info
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Sun, 15 Jul 2018 04:17:06 GMT
Server: Apache
```

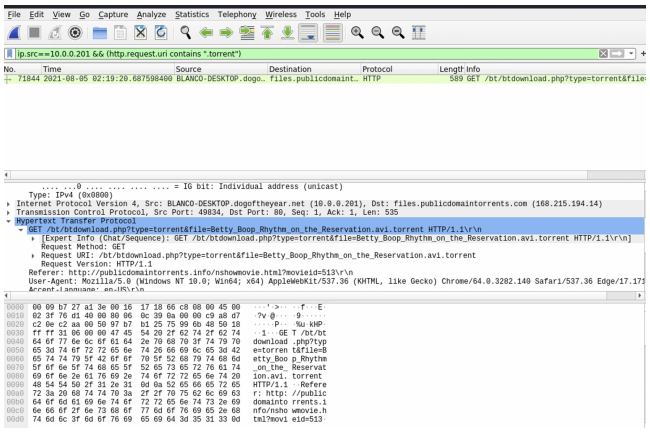


2. Which torrent file did the user download?

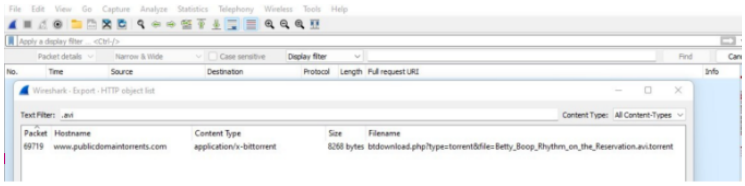
→ ***File: Betty_Boop_Rhythm_on_the_Reservation.avi***

→ ***Source: download.deluge-torrent.org***


Wireshark · Export · HTTP object list
Packet Hostname Content Type Size Filename
23494 download.deluge-torrent.org 7 bytes version-1.0
23499 torrent.ubuntu.com:6969 text/plain 431 bytes announce?info_ha...
23743 files.publicdomaintorrents.com text/html 553 bytes announce.php?inf...
23846 tracker.publicdomaintorrents.com:... text/plain 40 bytes announce?info_ha...


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.src==10.0.0.201 && (http.request.uri contains ".torrent")
No. Time Source Destination Protocol Length Info
71844 2021-08-05 02:19:20.687598400 BLANCO-DESKTOP.dogo... files.publicdomaint... HTTP 589 GET /bt/btdownload.php?type=torrent&file
Hypertext Transfer Protocol
GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n
Request URI: /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
Request Version: HTTP/1.1
Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\r\n
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/17.17


File Name: Betty_Boop_Rhythm_on_the_Reservation.avi
File Size: 108.58 MB
Resolution: 720x480
Duration: 00:06:02


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Export · HTTP object list
Text Filter: .avi
Content Type: All Content-Types
Packet Hostname Content Type Size Filename
69719 www.publicdomaintorrents.com application/x-bittorrent 8268 bytes btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent