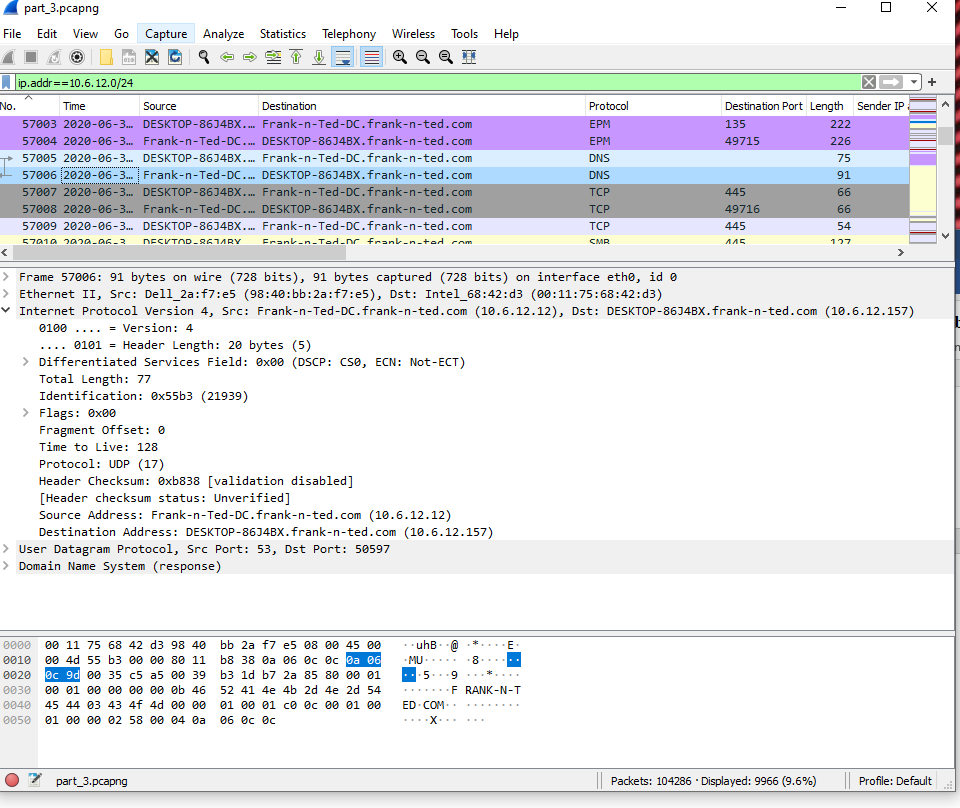
Network Analysis

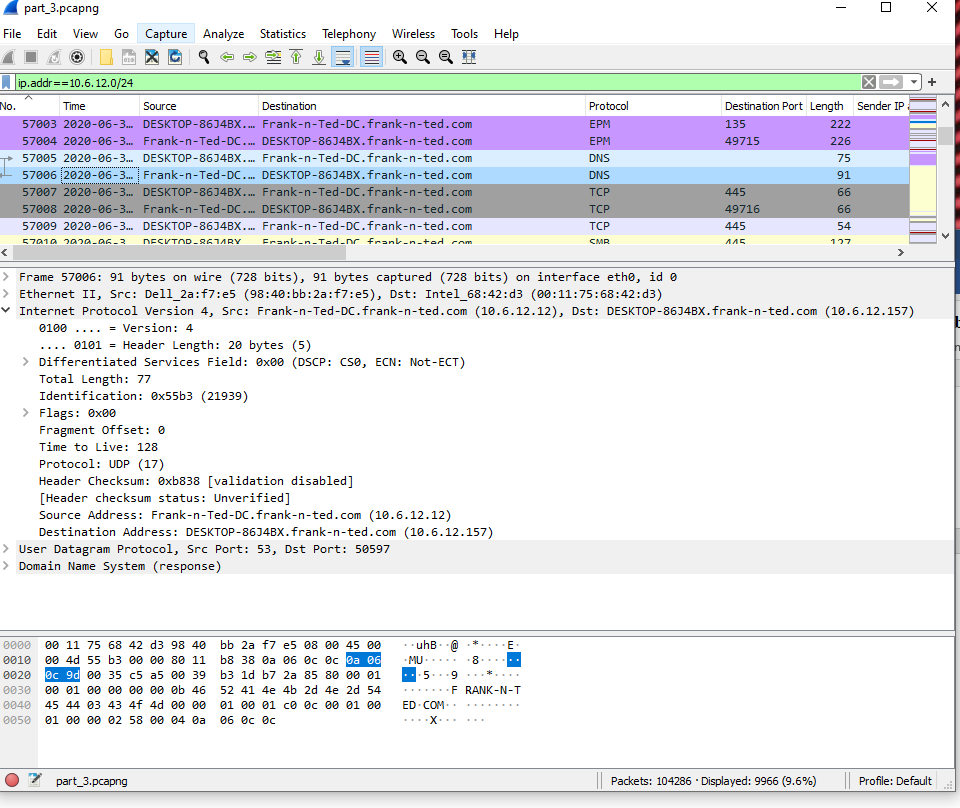
1.What is the domain name of the users' custom site?

The domain name is Frank-n-Ted-DC.frank-n-ted.com.

Filter: ip.addr==10.6.12.0/24

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

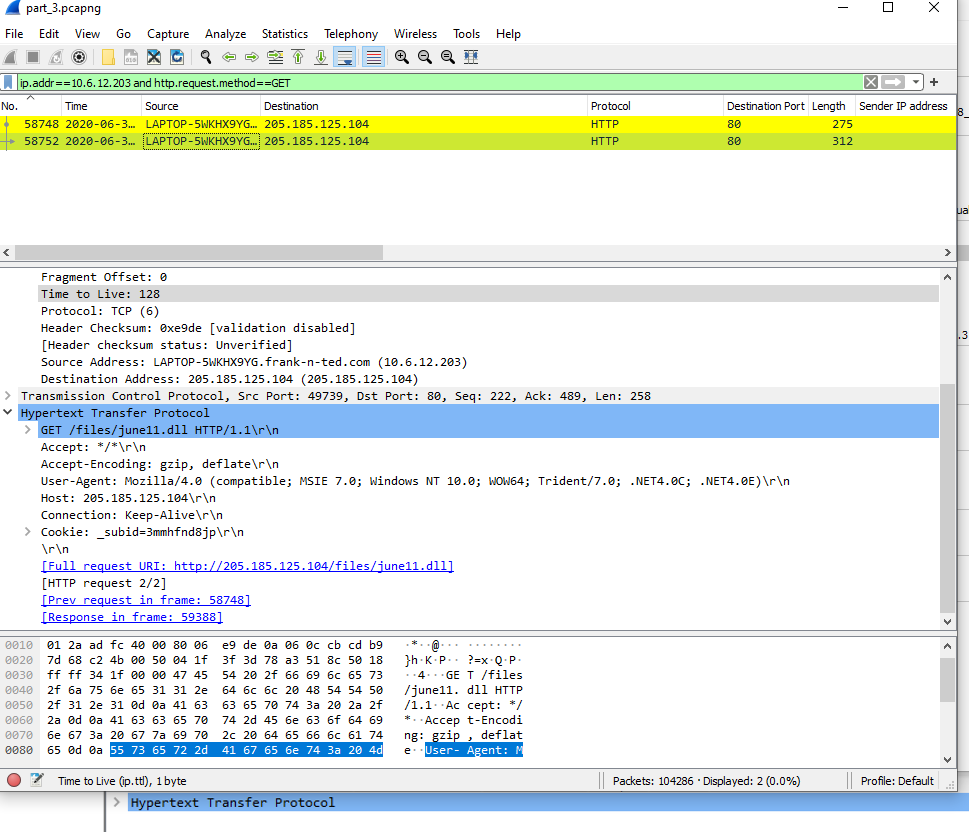
IP address is 10.6.12.12 (Frank-n-Ted-DC.frank-n-ted.com)



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.

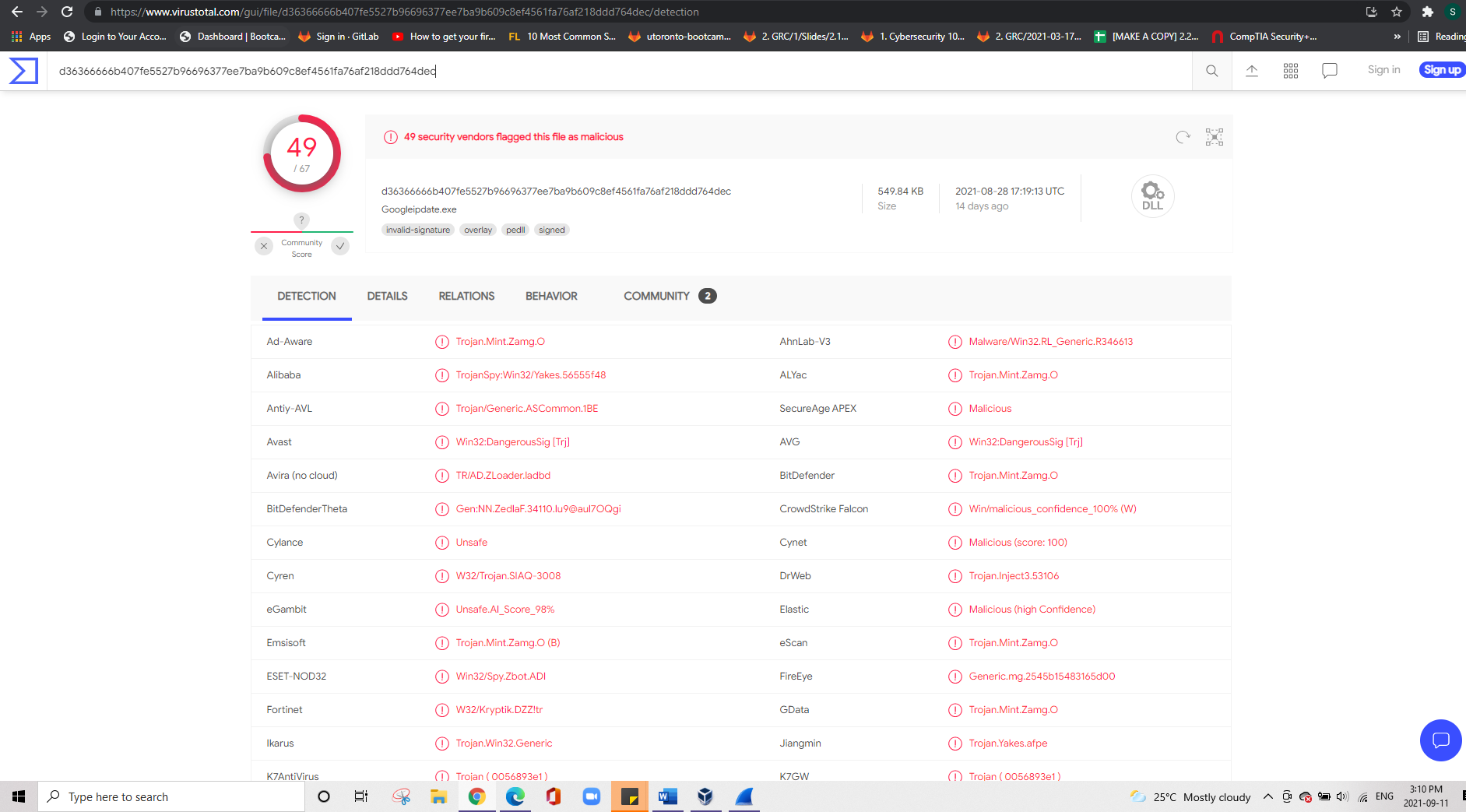
Malware file is june11.dll.

Filter: ip.addr==10.6.12.203 and http.request.method==GET



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

Malware is Trojan.



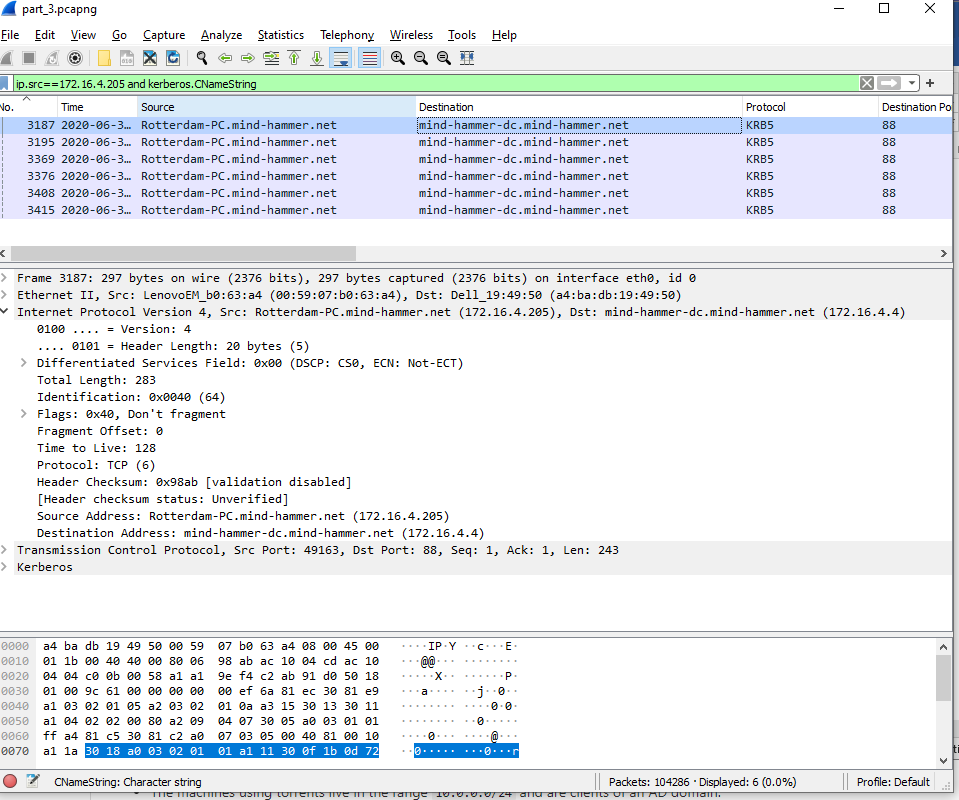
Vulnerable Windows Machines

Find the following information about the infected Windows machine:

Host name: ROTTERDAM-PC

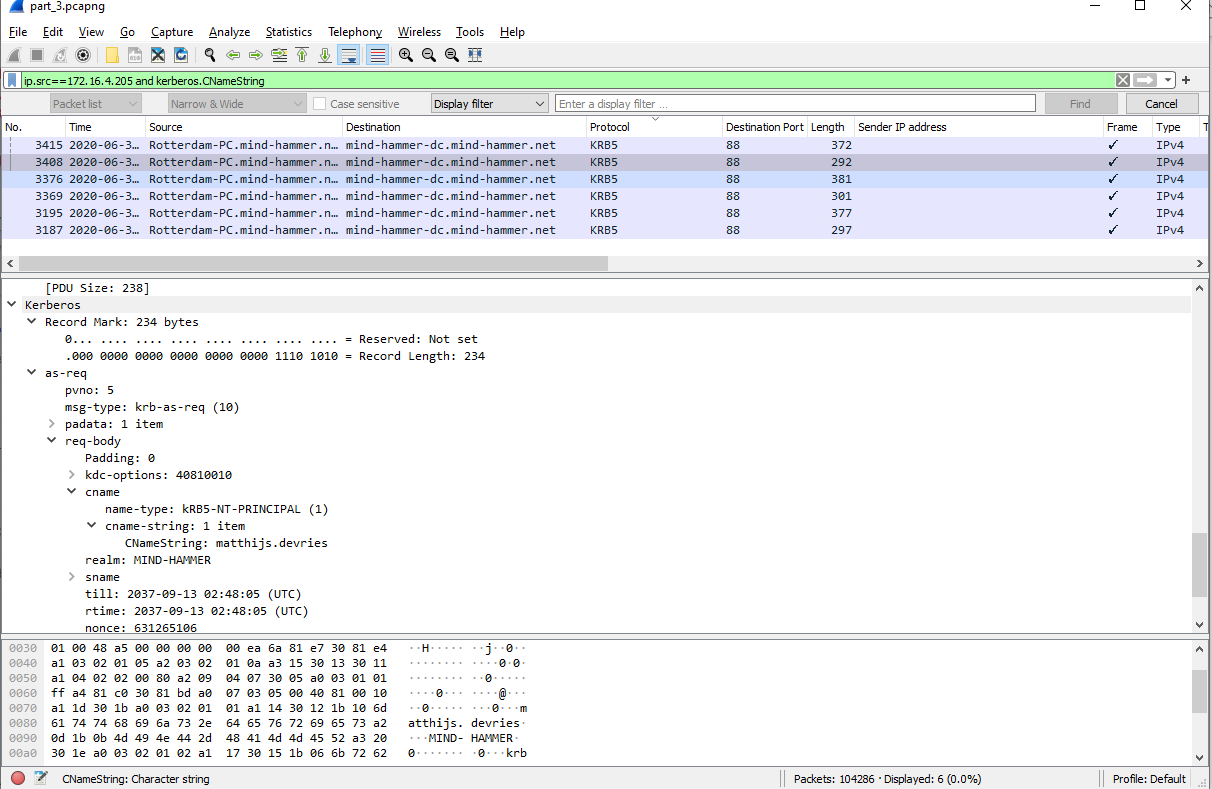
IP address: 172.16.4.205

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



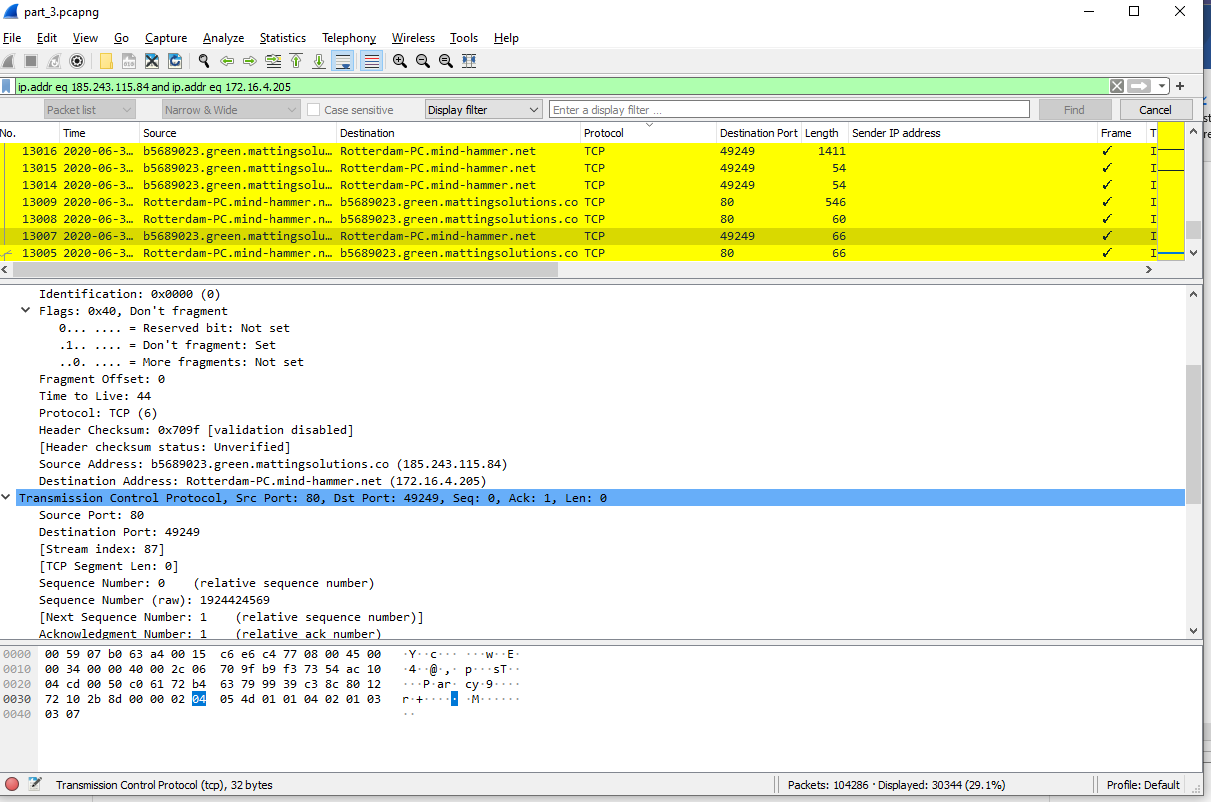
2.What is the username of the Windows user whose computer is infected?

The username is matthijs.devries.





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

172.16.4.205, 185.243.115.84, are the infected traffic.

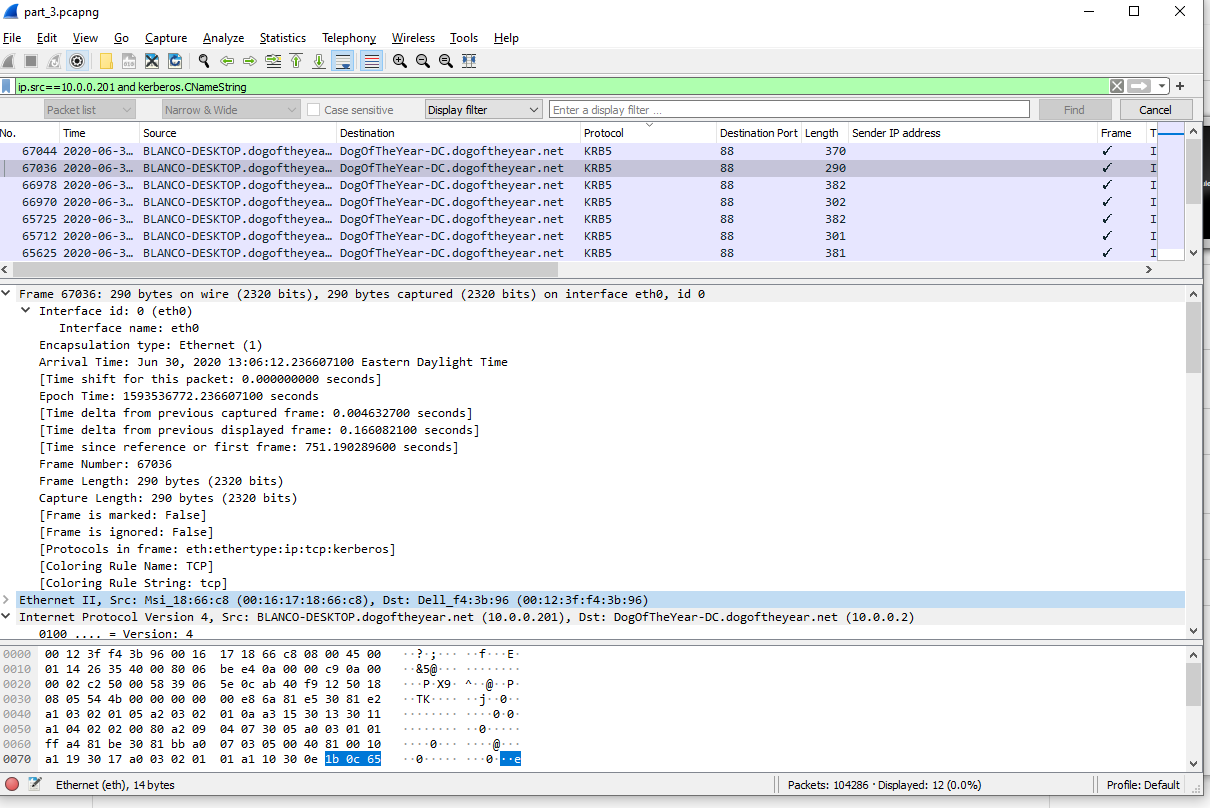
Illegal Downloads

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

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

Host Name (OS version): BLANCO-DESKTOP

Filter: ip.src==10.0.0.201 and kerberos.CNameString



2.Which torrent file did the user download?

Filter: ip.addr==10.0.0.201 and http.request.method==GET

