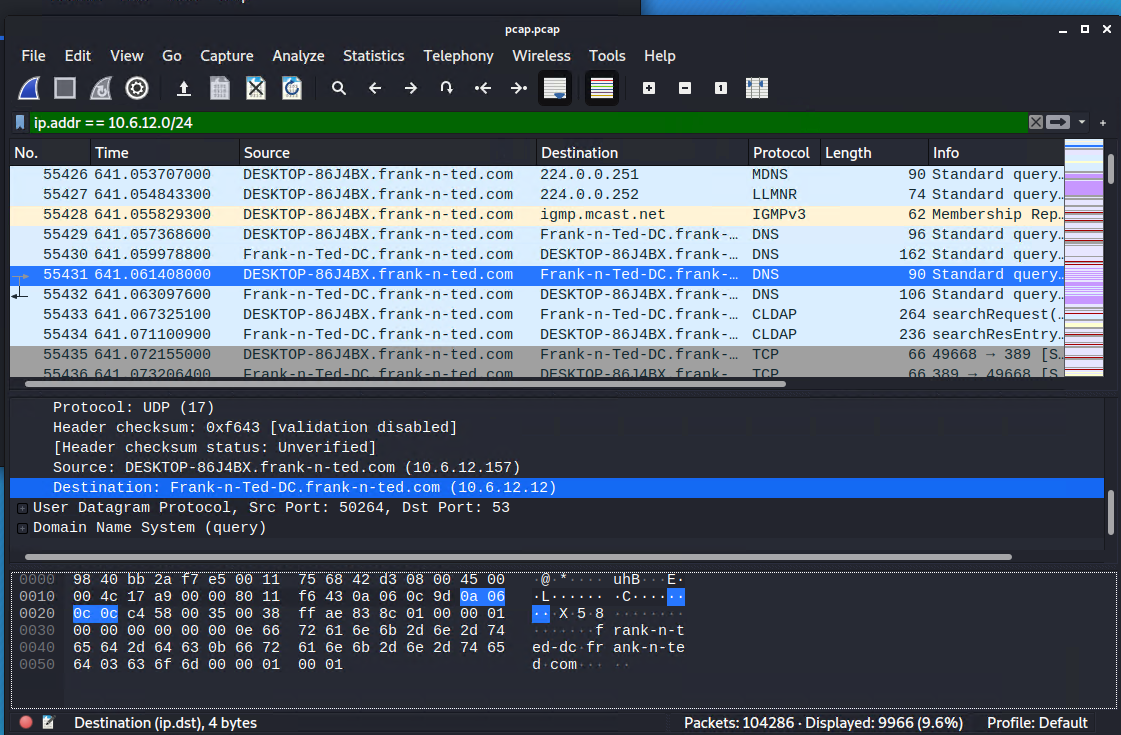
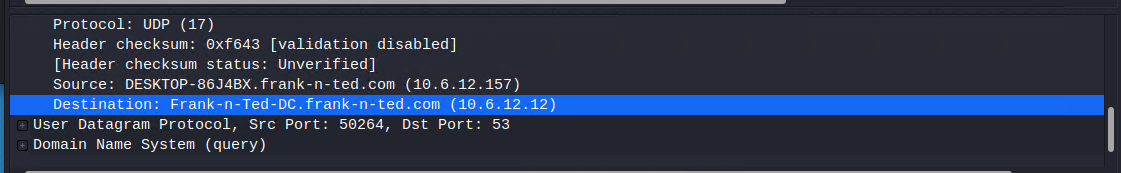
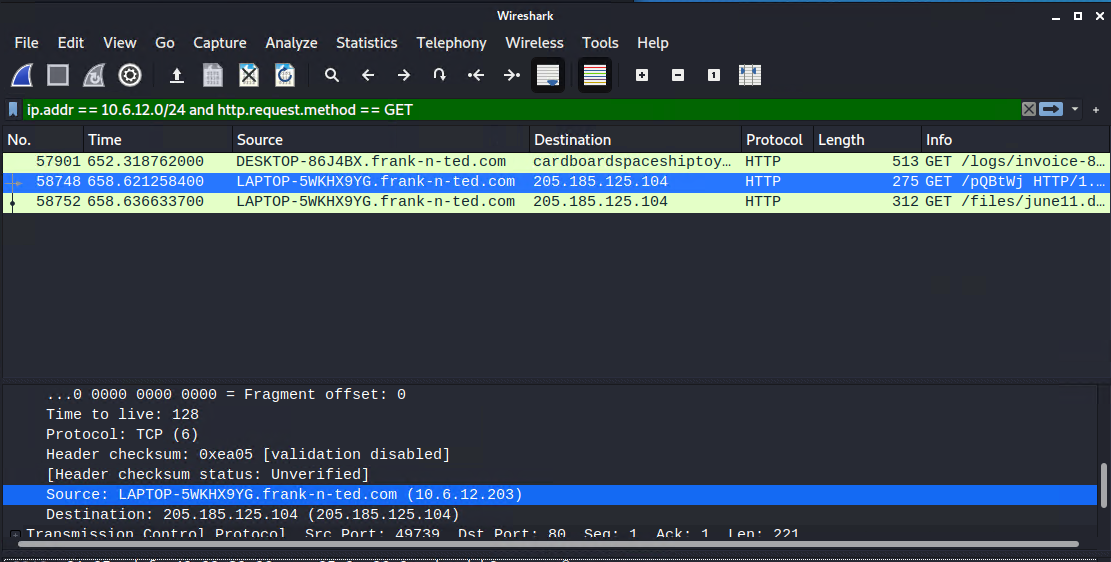
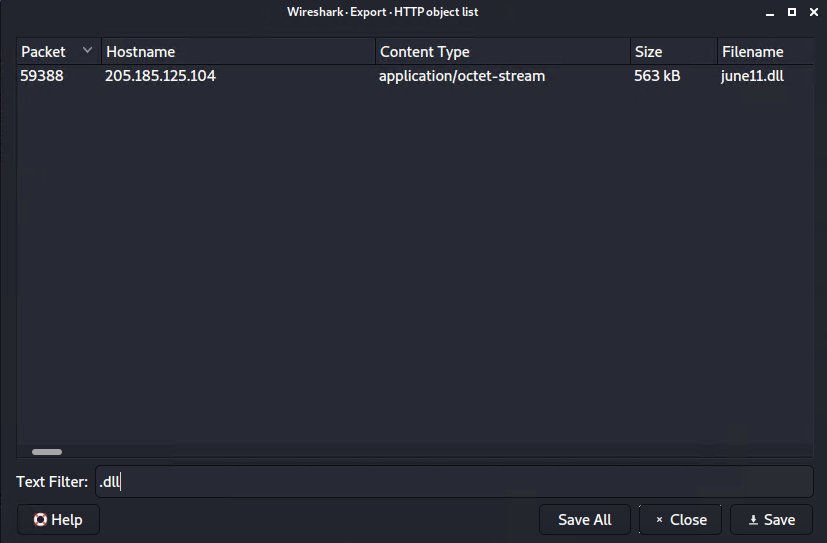
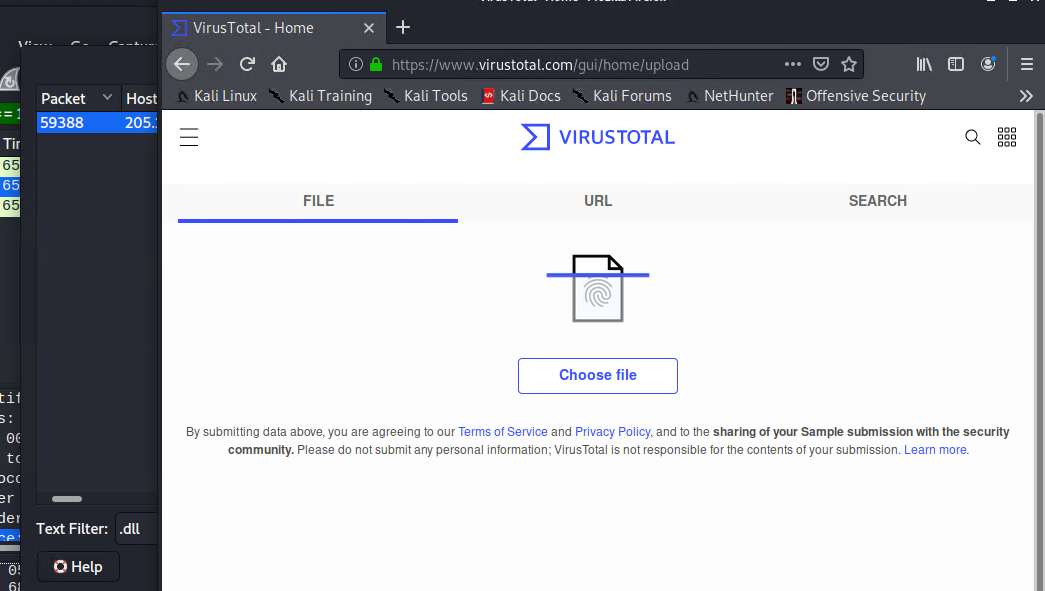
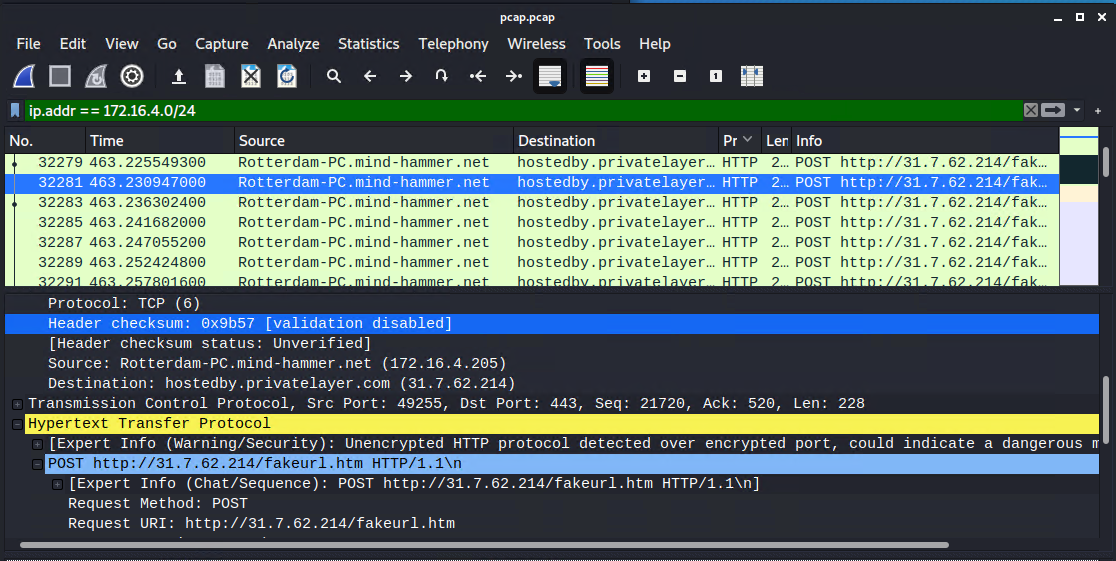
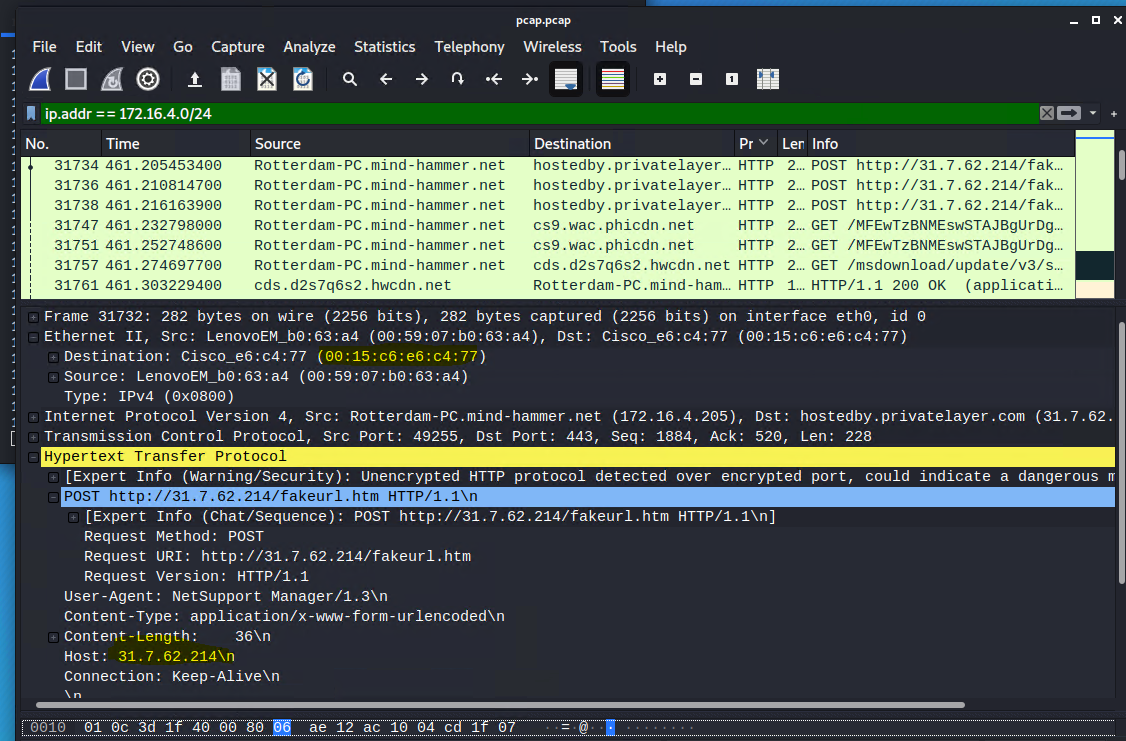
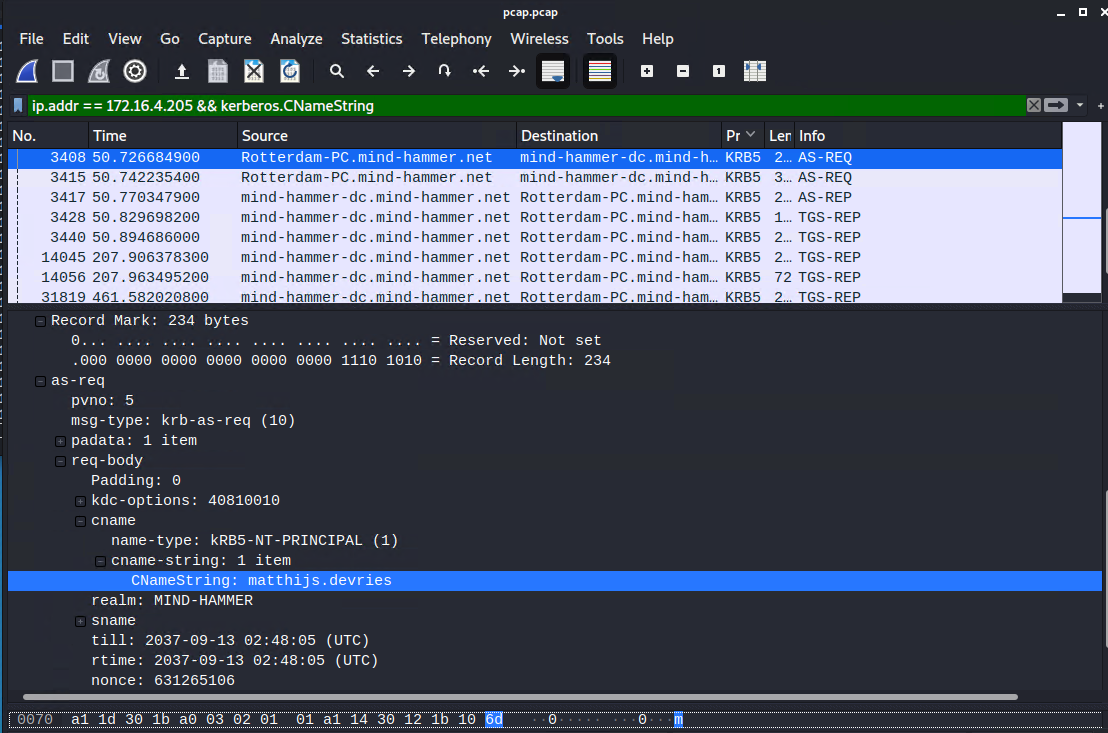
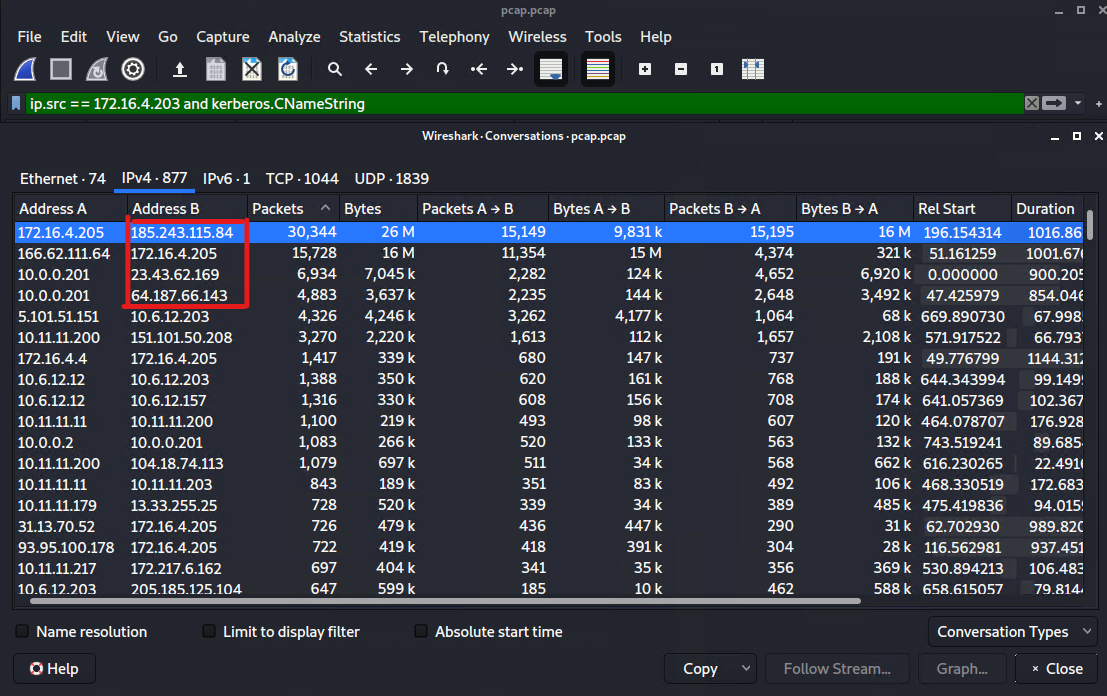
# **Network Forensic Analysis Report**

## **Time Thieves**

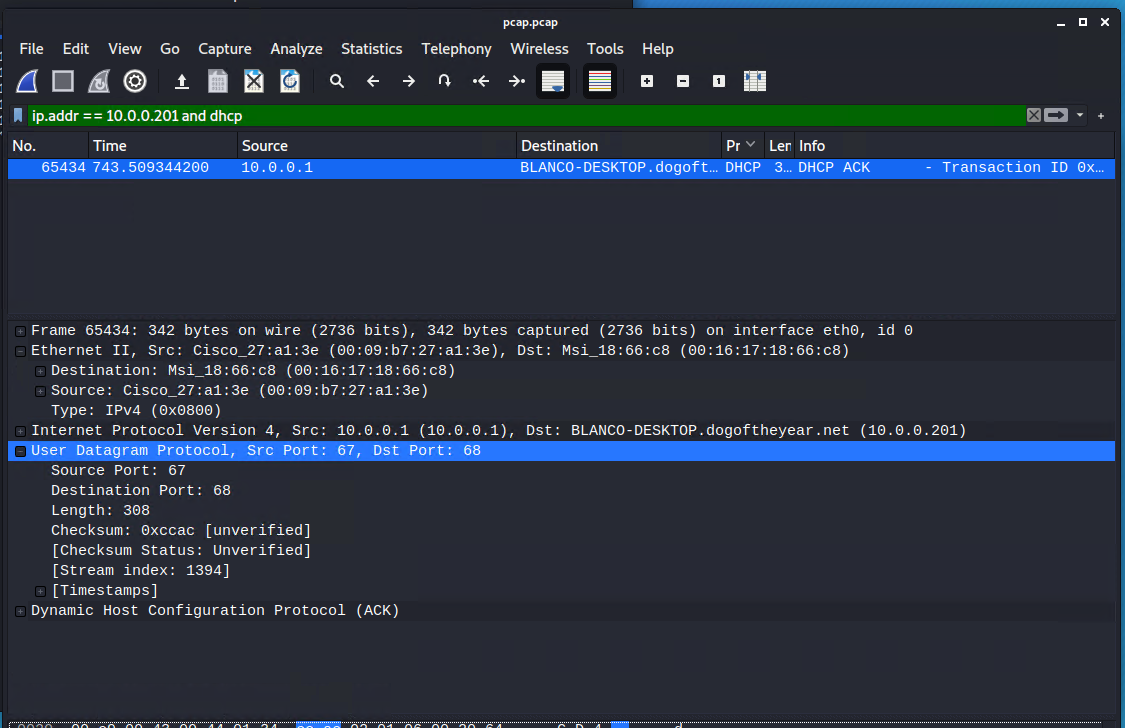
You must inspect your traffic capture to answer the following questions:

1. What is the domain name of the users' custom site?
   * **Domain Name:** Frank-n-Ted-DC. frank-n-ted.com
   * **WireShark query**: ip.src==10.6.12.0/24
   * **Screen: **
2. What is the IP address of the Domain Controller (DC) of the AD network?
   * **IP Address**: 10.6.12.12 (Frank-n-Ted-DC.frank-n-ted.com)
   * **WireShark query**: ip.src==10.6.12.0/24
   * **Screen:**
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.
   * **IP Address**: june11.dll
   * **WireShark query**: ip.addr == 10.6.12.0/24 and http.request.method == GET
   * **Screen:**
4. Upload the file to [VirusTotal.com](https://www.virustotal.com/gui/).
   * **Exporting file to Kali:**
     1. **File Tab → Export Objects → HTTP**
     2. **Text Filter: .dll**
     3. **Save june.dll**
     4. **Upload to VirusTotal.com**
   * **Screen:**
   * ****
5. What kind of malware is this classified as?
   * **The Trojan name is: Trojan.Mint.Zamg.O**
   * **Screen:**

## **Vulnerable Windows Machine**

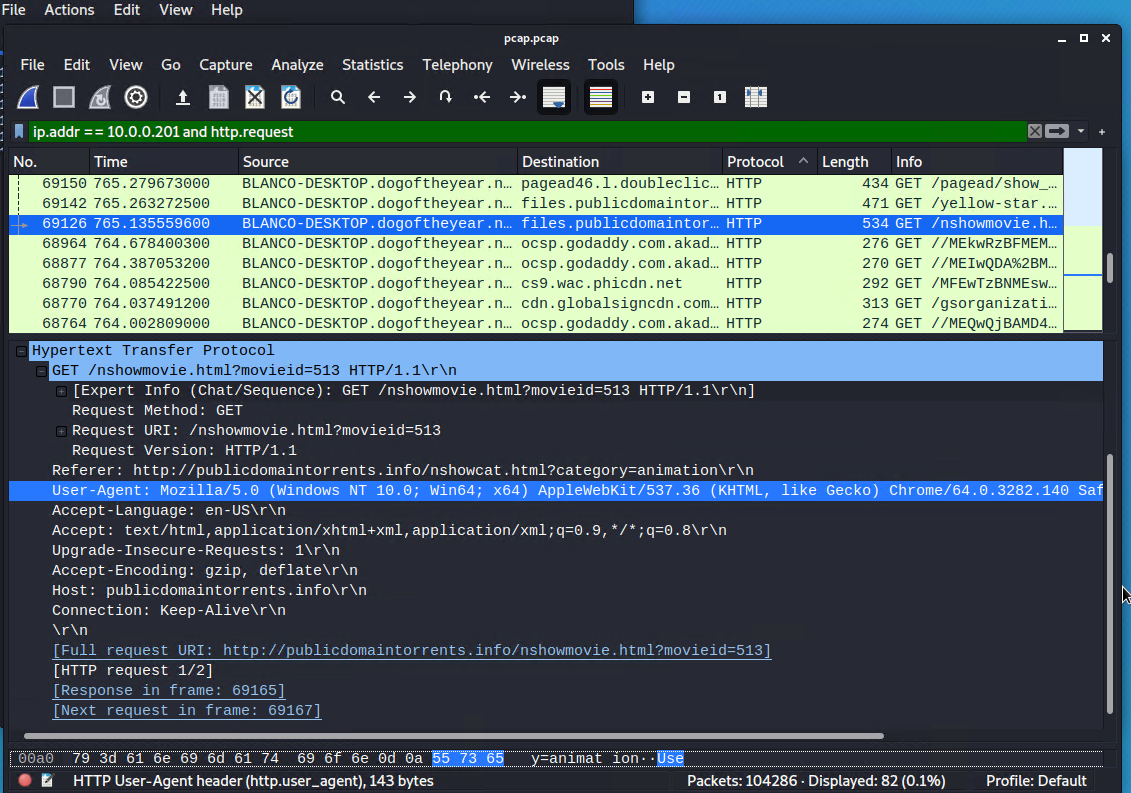
1. Find the following information about the infected Windows machine:  
   * **Host name: Rotterdam-PC**
   * **IP address: 172.16.4.205**
   * **MAC address: 00:59:07:b0:63:a4**
   * **Wireshark query: ip.addr == 172.16.4.0/24**
   * **Screen:**
   * ****
2. What is the username of the Windows user whose computer is infected?
   * **Username: matthijs.devries**
   * **Wireshark query: ip.src==172.16.4.205 && kerberos.CNameString**
   * **Screen:**
3. What are the IP addresses used in the actual infection traffic?
   * **Wireshark query:** ip.src==172.16.4.203 and kerberos.CNameString
   * Found IP addresses: 185.243.115.84, 172.16.4.205, 23.43.62.169, 64.187.66.143
   * **Finding IP addresses:**
     1. Statistics Tab → Conversation
     2. Select - IPv4
     3. Sort Packets high to low
   * **Screen:**
4. As a bonus, retrieve the desktop background of the Windows host.

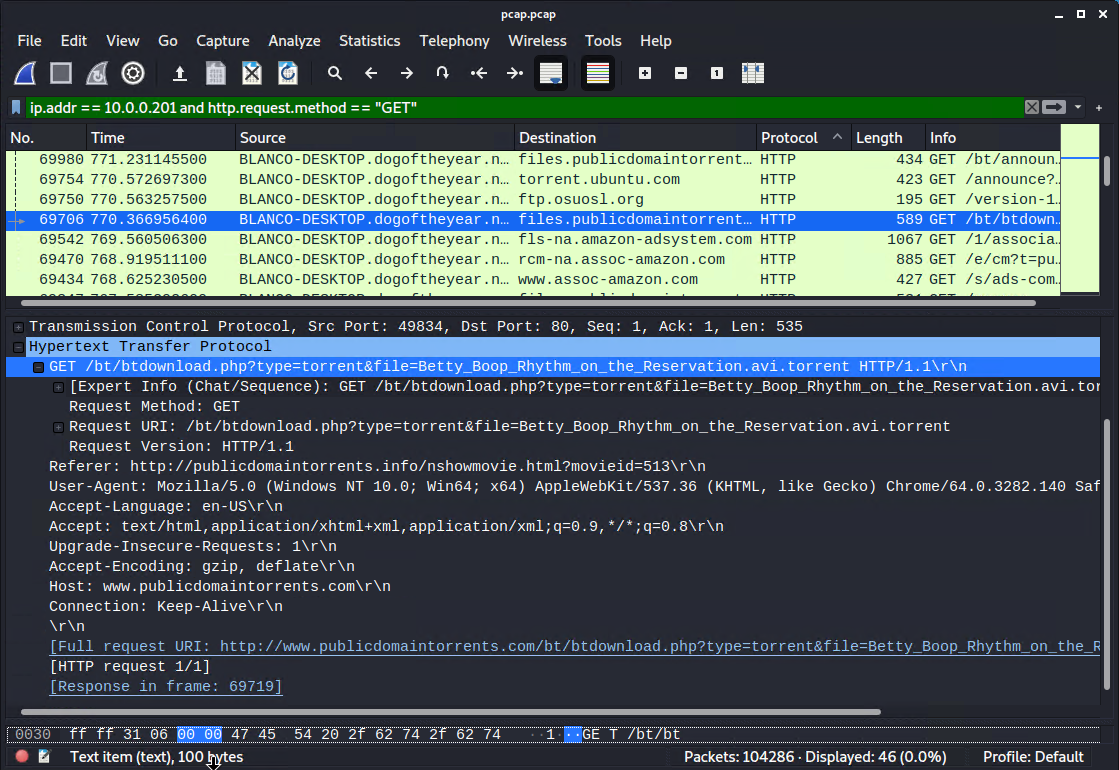
## **Illegal Downloads**

1. 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**
   * **OS version: BLANCO-DESKTOP Windows NT 10.0**
   * **Wireshark Filter for MAC Address: ip.addr == 10.0.0.201 and dhcp**

**Query: ip.addr == 10.0.0.201 and kerberos.CNameString**

**Query OS Type and Version: ip.addr == 10.0.0.201 and http.request**

****

1. Which torrent file did the user download?
   * **Downloaded**: Betty\_Boop\_Rhythm\_on\_the\_Reservation.avi.torrent
   * **Wireshark query:** ip.addr == 10.0.0.201 && http.request.method == "GET"
   * **To find torrent:** use query and Sort the packets by the Destination files.publicdomaintorrents.com (168.215.194.14).
   * Look for Download requests.
   * **screen:**