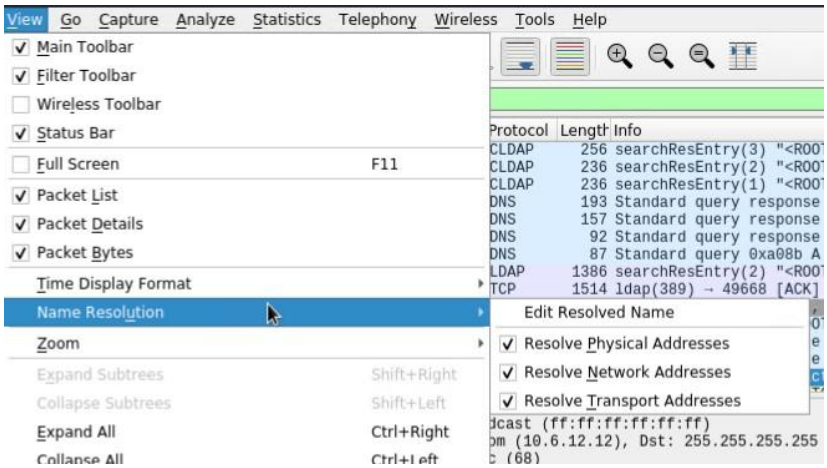
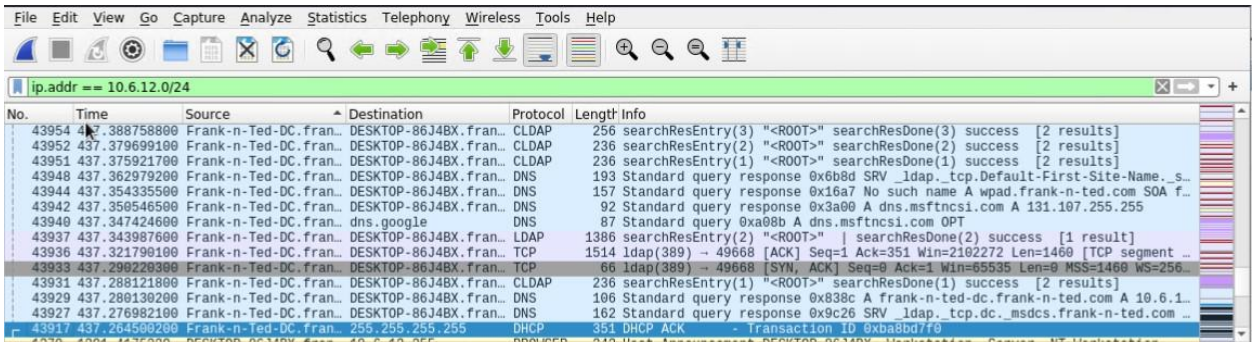
Network Forensic Analysis Report

Time Thieves

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

1. What is the domain name of the users' custom site?
   `Frank-n-Ted-DC.frank-n-ted.com`





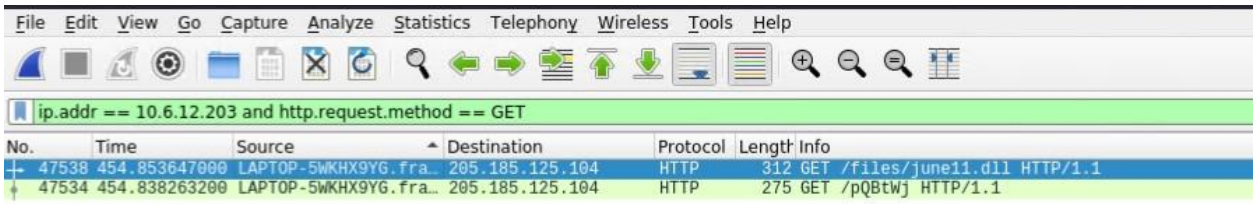
2. What is the IP address of the Domain Controller (DC) of the AD network?

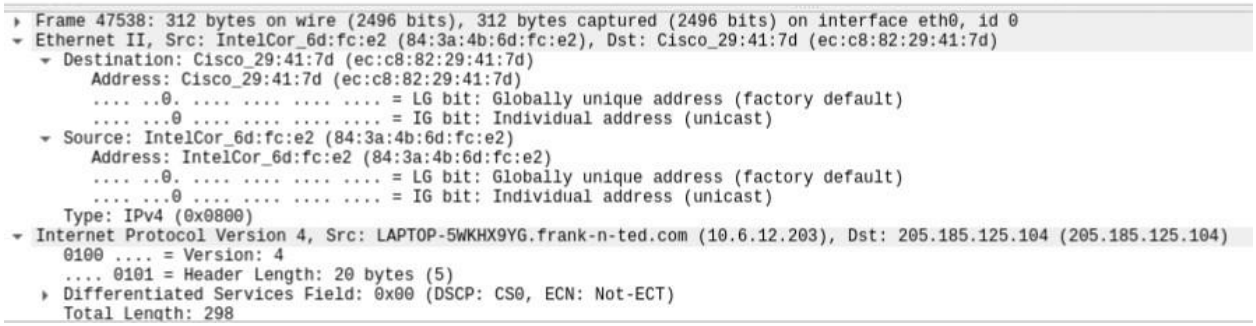
```
10.6.12.12
```

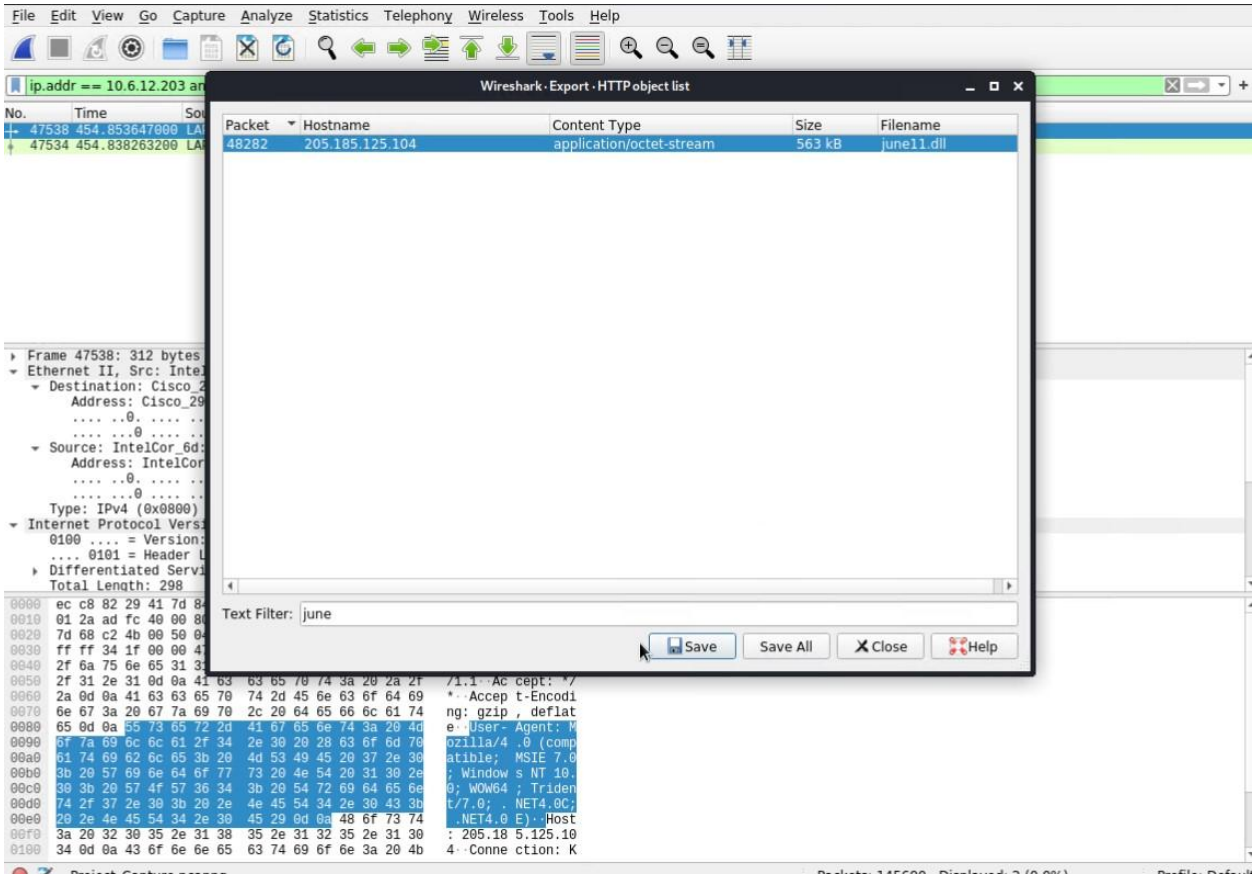
```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 337
    Identification: 0x3880 (14464)
  ▸ Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0xeb0a [validation disabled]
    [Header checksum status: Unverified]
    Source: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12)
    Destination: 255.255.255.255 (255.255.255.255)
▸ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
▸ Dynamic Host Configuration Protocol (ACK)
```

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

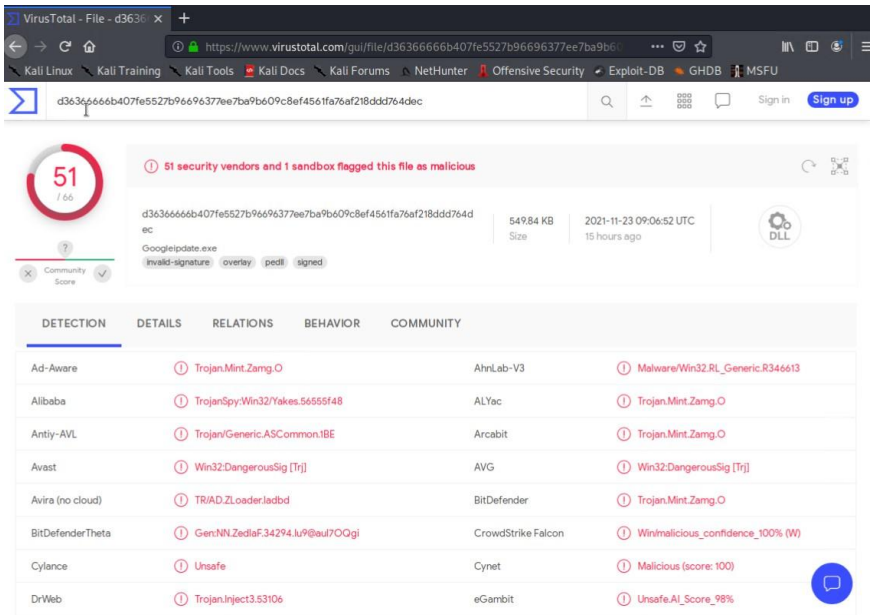
```
june11.dll
```







4. Upload the file to VirusTotal.com.

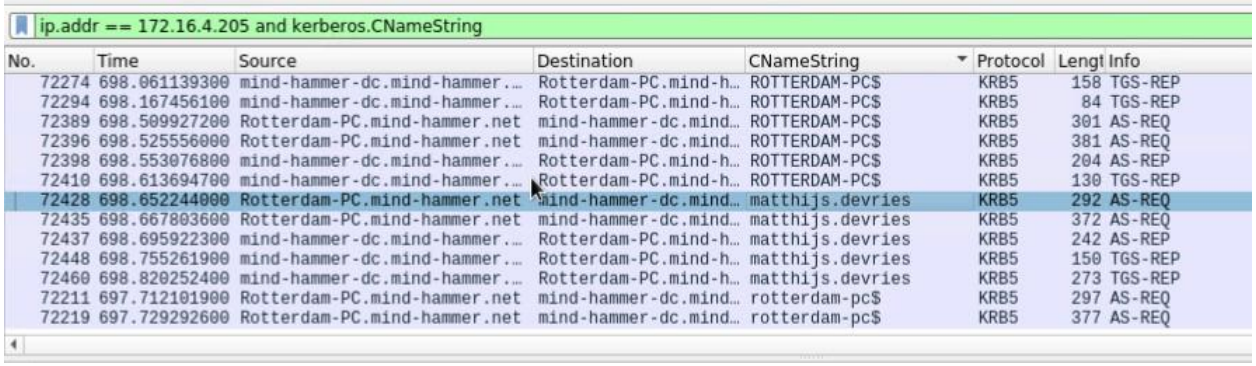


5. What kind of malware is this classified as?

   trojan.malware

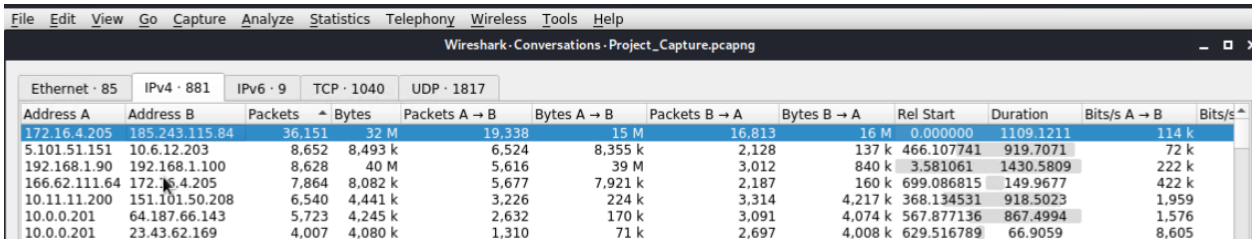
Vulnerable Windows Machine

1. Find the following information about the infected Windows machine:
   - Host name: `Rotterdam-PC.mind-hammer.net`
   - IP address: `172.16.4.205`
   - MAC address: `LenovoEM_b0:64:a4 (00:59:07:b0:63:a4)`
2. What is the username of the Windows user whose computer is infected?

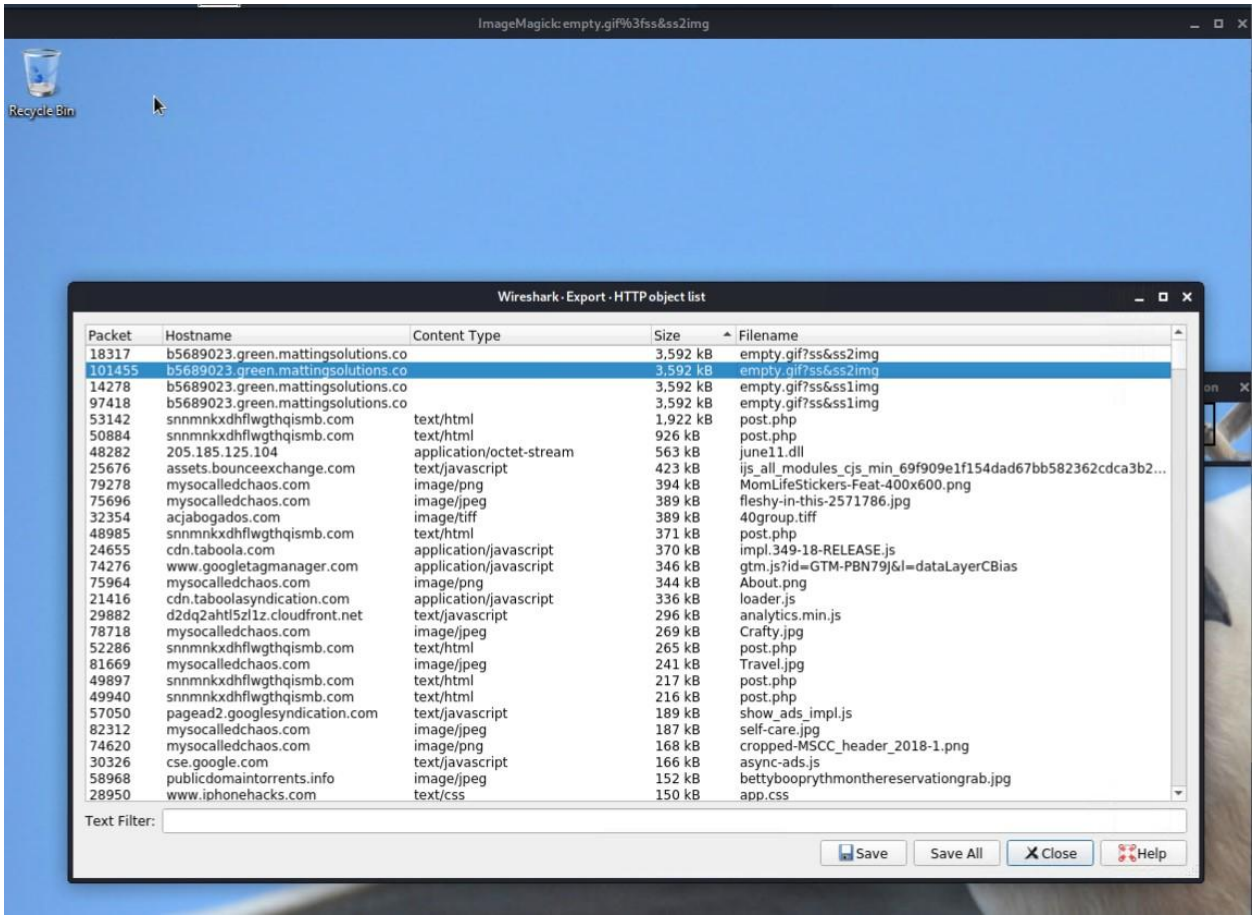



```
matthijs.devries
```

3. What are the IP addresses used in the actual infection traffic? `185.243.115.84`



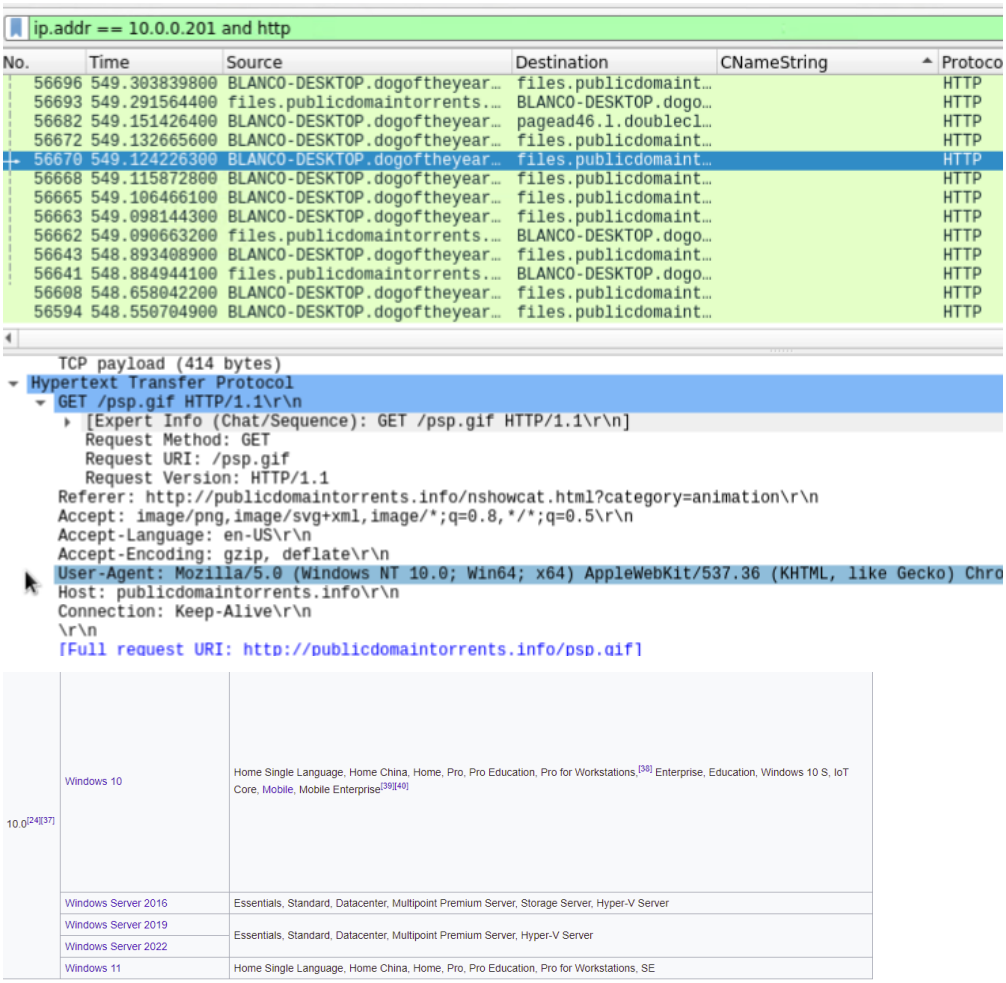
4. As a bonus, retrieve the desktop background of the Windows host.



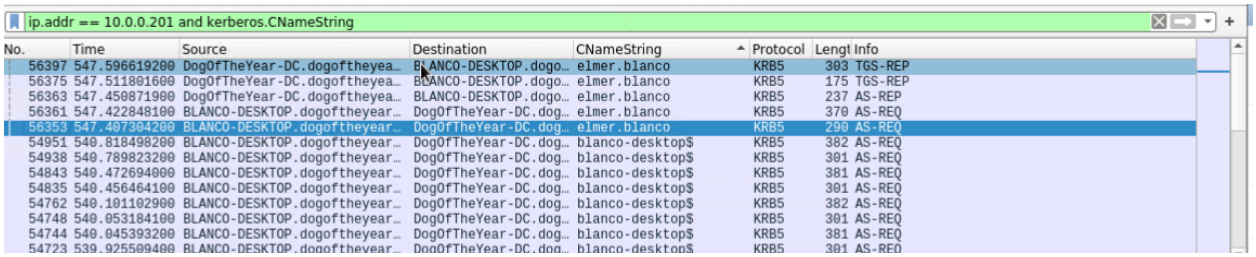
Illegal Downloads

1. Find the following information about the machine with IP address `10.0.0.201`:
    - MAC address: `Msi_18:66:c8 (00:16:17:18.66:c8)`
    - Windows username: `elmer.blanco`

- OS version: `Windows NT 10.0`

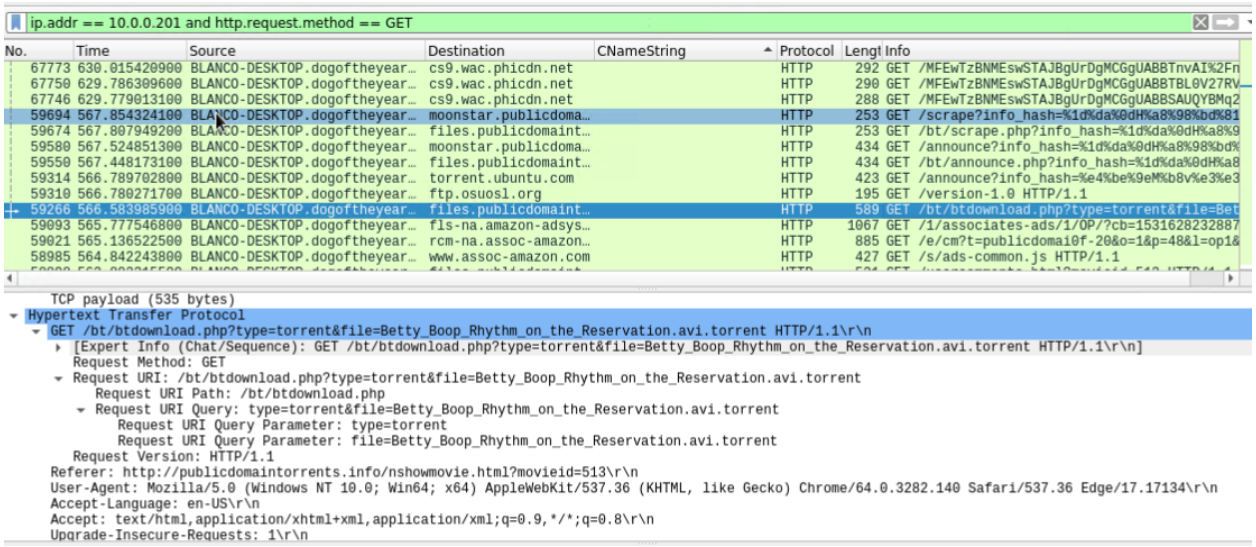


10.0[24][37]	Windows 10	Home Single Language, Home China, Home, Pro, Pro Education, Pro for Workstations,[38] Enterprise, Education, Windows 10 S, IoT Core, Mobile, Mobile Enterprise[39][40]
	Windows Server 2016	Essentials, Standard, Datacenter, Multipoint Premium Server, Storage Server, Hyper-V Server
	Windows Server 2019	Essentials, Standard, Datacenter, Multipoint Premium Server, Hyper-V Server
	Windows Server 2022	
	Windows 11	Home Single Language, Home China, Home, Pro, Pro Education, Pro for Workstations, SE



2. Which torrent file did the user download?

```
Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
```


ip.addr == 10.0.0.201 and http.request.method == GET
No. Time Source Destination CNameString Protocol Lengt Info
67773 630.015420900 BLANCO-DESKTOP.dogoftheyear… cs9.wac.phicdn.net HTTP 292 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTnvAI%2Fn
67750 629.786309600 BLANCO-DESKTOP.dogoftheyear… cs9.wac.phicdn.net HTTP 290 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RV
67746 629.779013100 BLANCO-DESKTOP.dogoftheyear… cs9.wac.phicdn.net HTTP 288 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2
59694 567.854324100 BLANCO-DESKTOP.dogoftheyear… moonstar.publicdoma… HTTP 253 GET /scrape?info_hash=%1d%da%0dH%a8%98%bd%81
59674 567.807949200 BLANCO-DESKTOP.dogoftheyear… files.publicdomaint… HTTP 253 GET /bt/scrape.php?info_hash=%1d%da%0dH%a8%9
59580 567.524851300 BLANCO-DESKTOP.dogoftheyear… moonstar.publicdoma… HTTP 434 GET /announce?info_hash=%1d%da%0dH%a8%98%bd%
59550 567.448173100 BLANCO-DESKTOP.dogoftheyear… files.publicdomaint… HTTP 434 GET /bt/announce.php?info_hash=%1d%da%0dH%a8
59314 566.789702800 BLANCO-DESKTOP.dogoftheyear… torrent.ubuntu.com HTTP 423 GET /announce?info_hash=%e4%be%9eM%b8v%e3%e3
59310 566.780271700 BLANCO-DESKTOP.dogoftheyear… ftp.osuosl.org HTTP 195 GET /version-1.0 HTTP/1.1
59266 566.583985900 BLANCO-DESKTOP.dogoftheyear… files.publicdomaint… HTTP 589 GET /bt/btdownload.php?type=torrent&file=Bet
59093 565.777546800 BLANCO-DESKTOP.dogoftheyear… fls-na.amazon-adsys… HTTP 1067 GET /1/associates-ads/1/OP/?cb=1531628232887
59021 565.136522500 BLANCO-DESKTOP.dogoftheyear… rcm-na.assoc-amazon… HTTP 885 GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=op1&
58985 564.842243800 BLANCO-DESKTOP.dogoftheyear… www.assoc-amazon.com HTTP 427 GET /s/ads-common.js HTTP/1.1
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]
Request Method: GET
Request URI: /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
Request URI Path: /bt/btdownload.php
Request URI Query: type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
Request URI Query Parameter: type=torrent
Request URI Query Parameter: 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/17.17134\r\n
Accept-Language: en-US\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Upgrade-Insecure-Requests: 1\r\n