Network Analysis

By Leo Katz

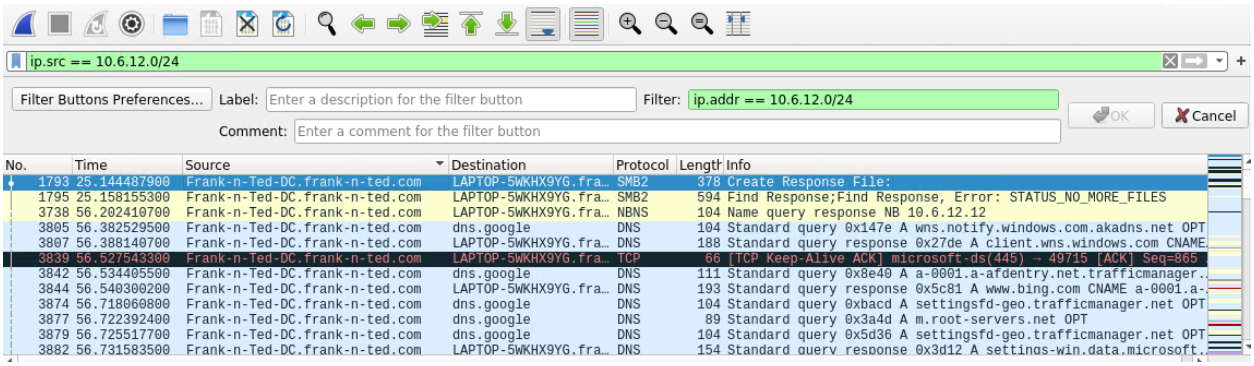
Time Thieves

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:

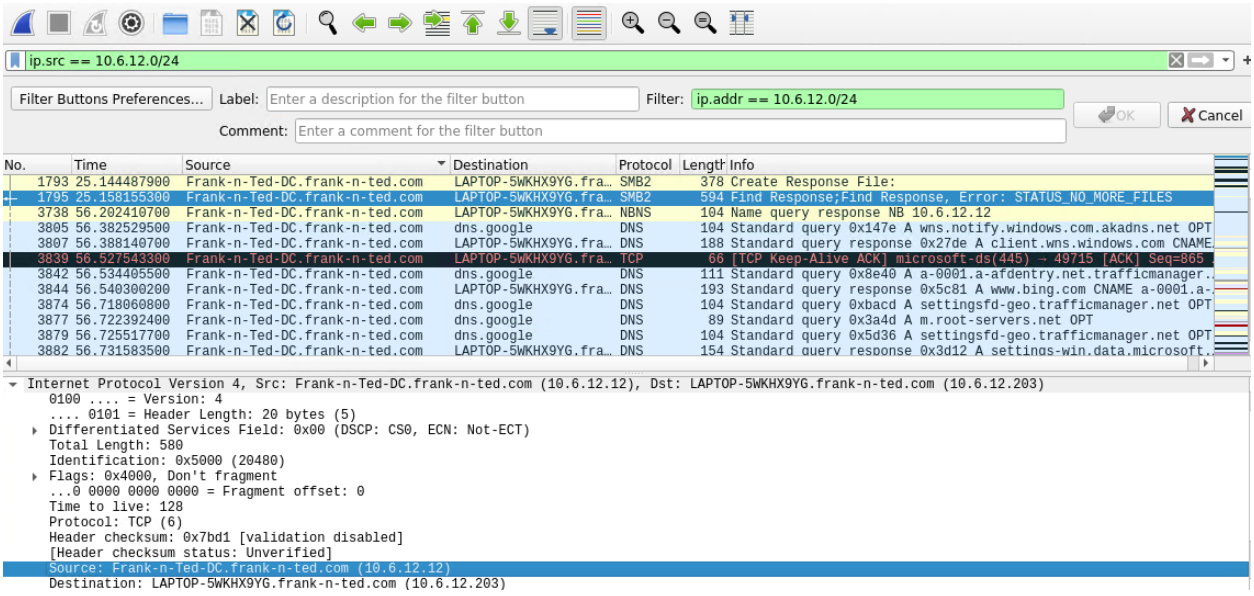
- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.
- Their IP addresses are somewhere in the range 10.6.12.0/24.

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

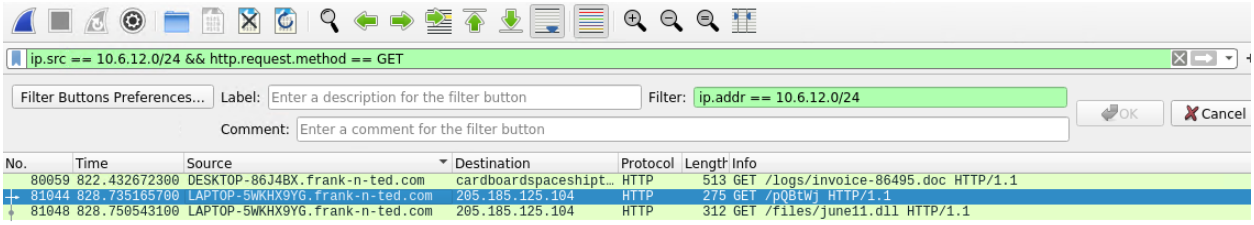
1. What is the domain name of the users' custom site?
    a. Frank-n-Ted-DC.frank-n-ted.com

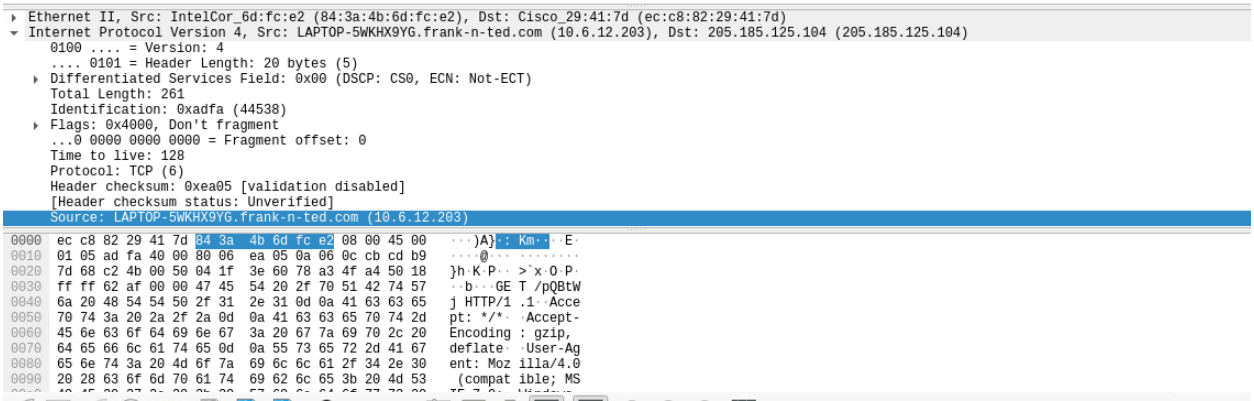


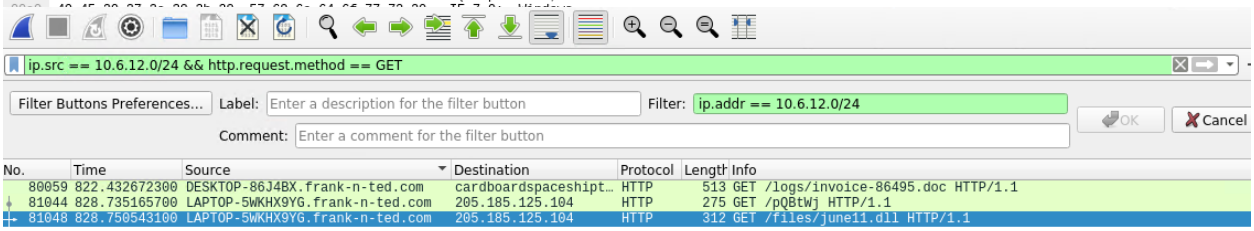
2. What is the IP address of the Domain Controller (DC) of the AD network?
    a. 10.6.12.12

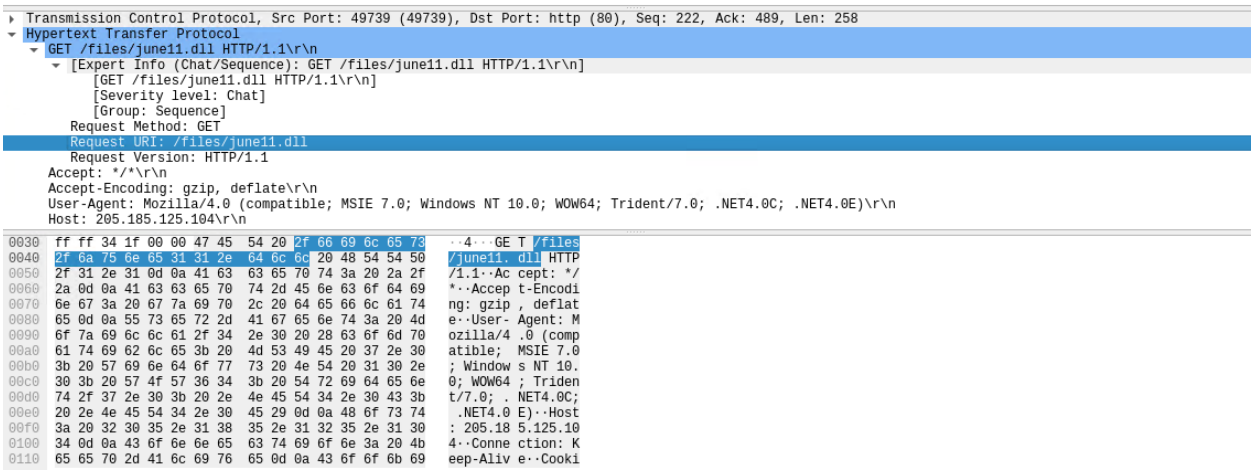


3. What is the name of the malware downloaded to the 10.6.12.203 machine? Once you have found the file, export it to your Kali machine's desktop.
    a. June11.dll

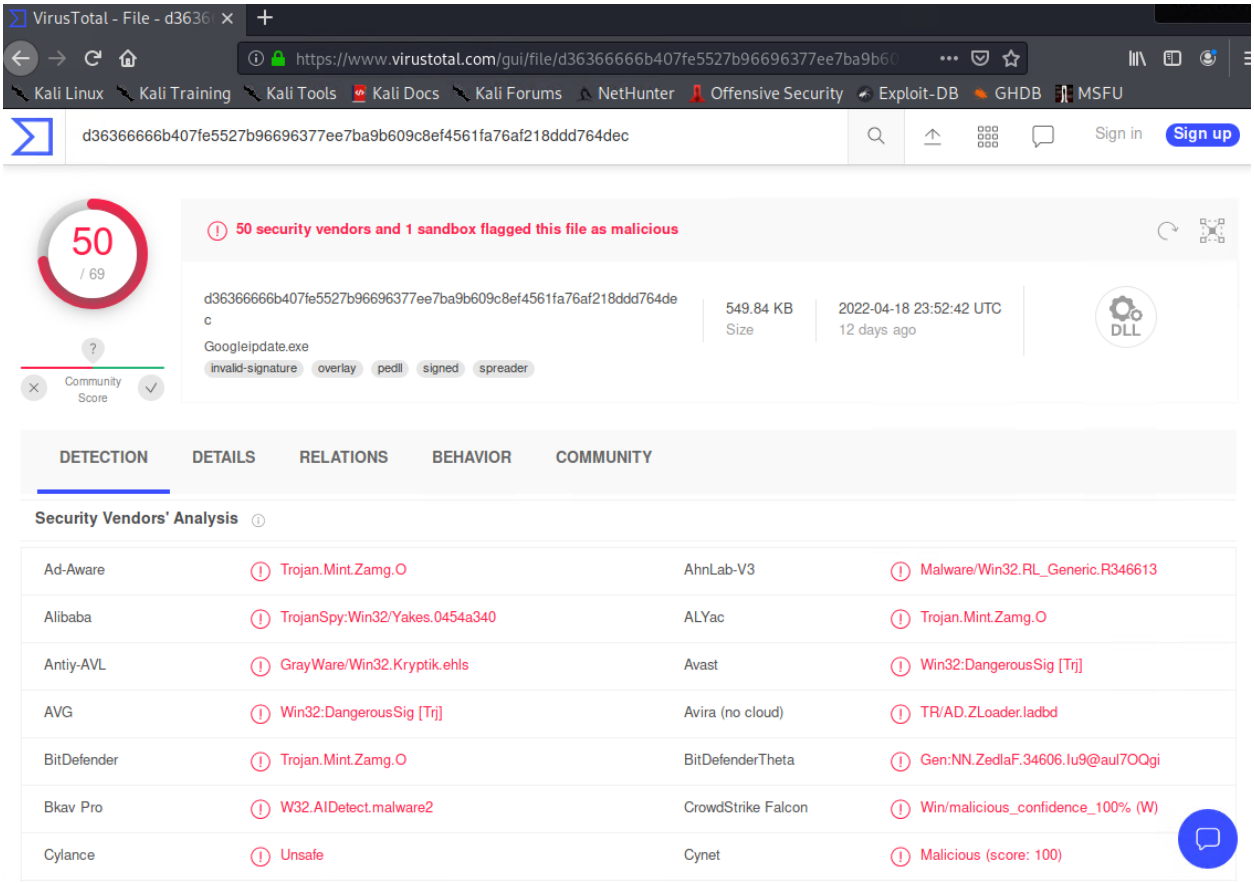








4. Upload the file to VirusTotal.com. What kind of malware is this classified as?
    a. Trojan



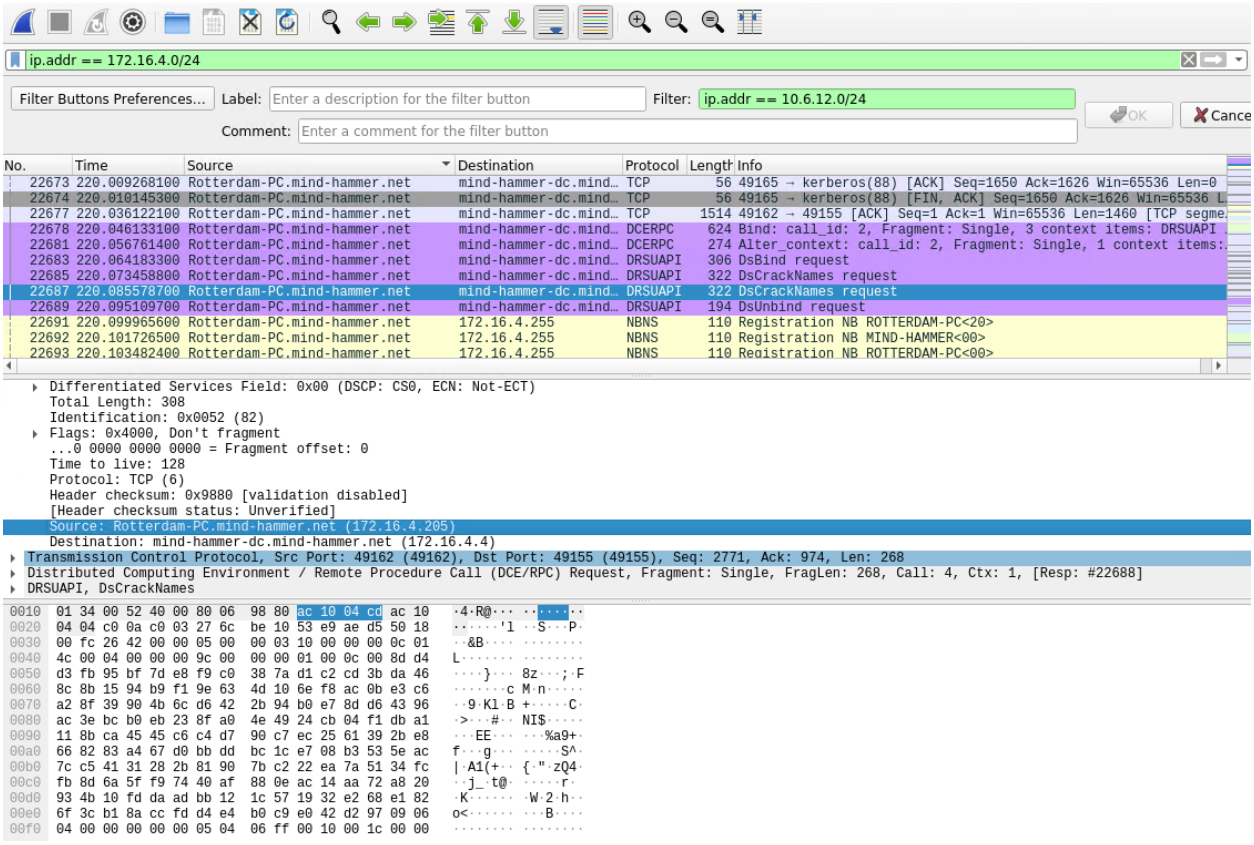
Vulnerable Windows Machines

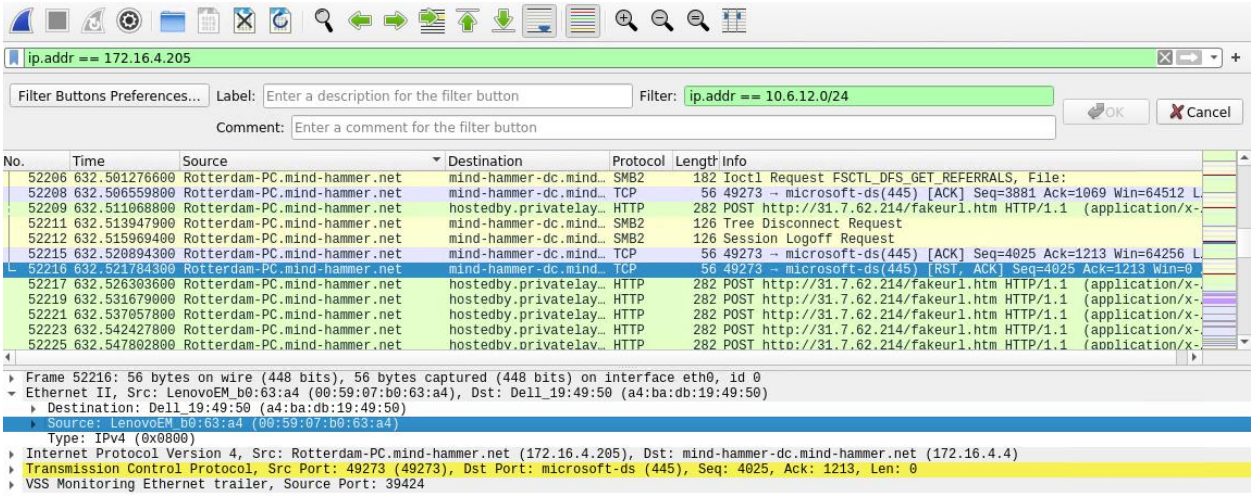
The Security team received reports of an infected Windows host on the network. They know the following:

- 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.

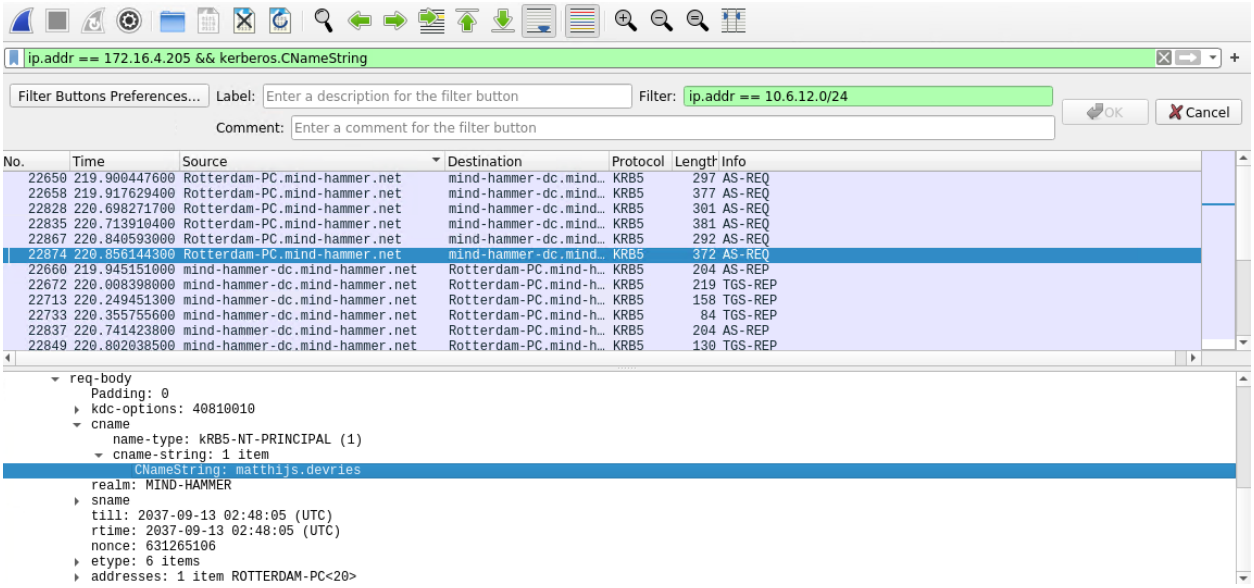
Inspect your traffic to answer the following questions:

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





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



3. What are the IP addresses used in the actual infection traffic?
    - 172.16.4.205 and 185.243.115.84

Wireshark · Conversations · network_capture_1.pcapng

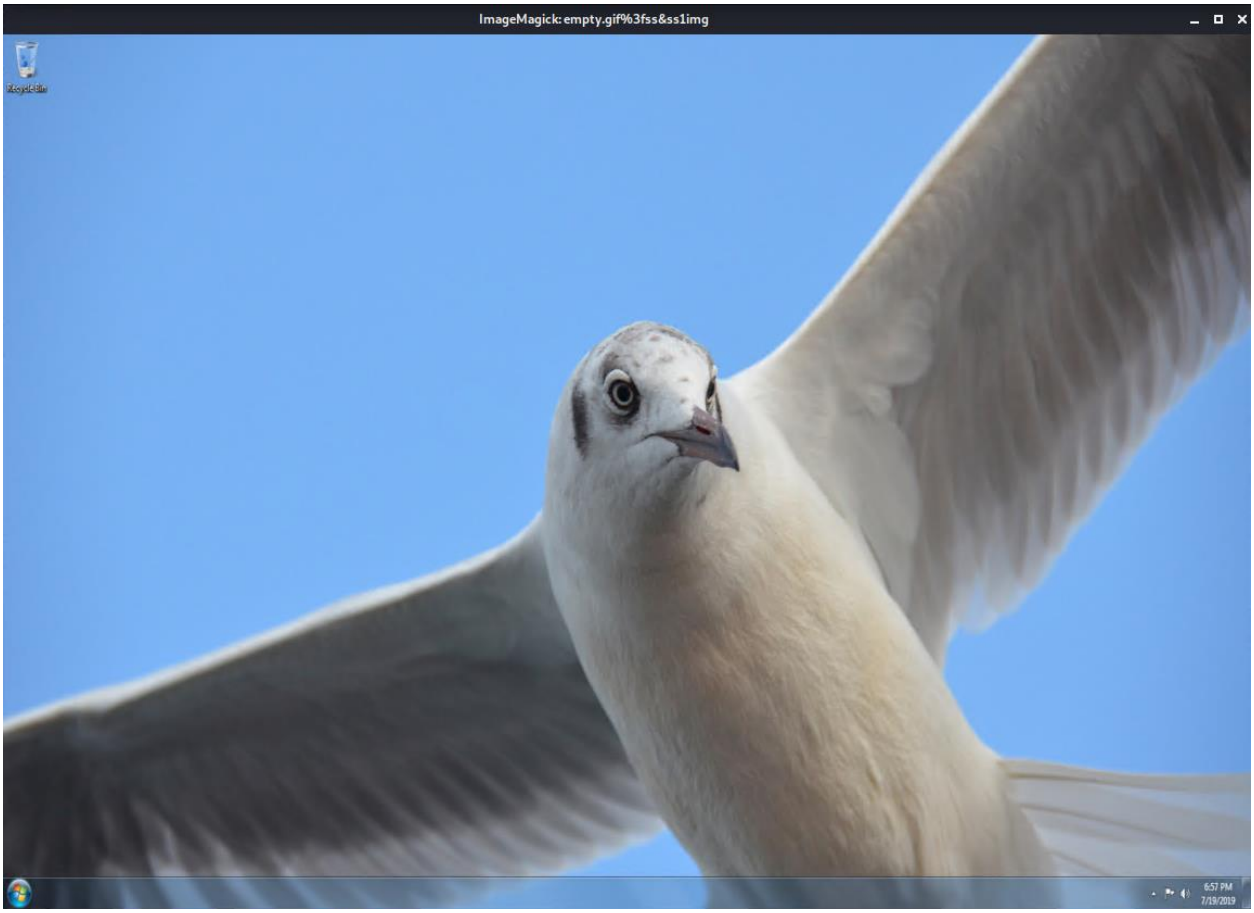
Ethernet · 77 | IPv4 · 879 | IPv6 · 3 | TCP · 1051 | UDP · 1814

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bit
172.16.4.205	185.243.115.84	18,324	16 M	9,753	7,983 k	8,571	8,543 k	366.268225	265.0412	240 k	
5.101.51.151	10.6.12.203	7,896	7,763 k	5,959	7,643 k	1,937	120 k	0.000000	908.0032	67 k	
166.62.111.64	172.16.4.205	7,864	8,082 k	5,677	7,921 k	2,187	160 k	221.275170	149.9677	422 k	
192.168.1.90	192.168.1.100	5,562	26 M	3,623	26 M	1,939	556 k	6.348153	992.6524	210 k	
10.0.0.201	64.187.66.143	5,227	3,873 k	2,402	156 k	2,825	3,717 k	90.065485	860.7093	1,450	
10.0.0.201	23.43.62.169	4,007	4,080 k	1,310	71 k	2,697	4,008 k	151.705141	66.9059	8,605	
10.11.11.200	151.101.50.208	3,270	2,220 k	1,613	112 k	1,657	2,108 k	742.031422	66.7937	13 k	
10.0.0.2	10.0.0.201	2,138	529 k	1,027	264 k	1,111	264 k	61.924605	884.2207	2,396	
10.6.12.12	10.6.12.203	1,673	405 k	736	185 k	937	220 k	25.138440	888.4694	1,669	
10.6.12.12	10.6.12.157	1,475	354 k	670	165 k	805	188 k	56.839601	856.6991	1,548	
10.0.0.201	172.217.9.2	1,108	564 k	530	62 k	578	501 k	71.325252	867.4318	576	
10.11.11.11	10.11.11.200	1,100	219 k	493	98 k	607	120 k	634.192542	176.9289	4,459	
10.11.11.200	104.18.74.113	1,079	697 k	511	34 k	568	662 k	786.344185	22.4915	12 k	
10.0.0.201	96.7.89.194	974	332 k	400	66 k	574	266 k	64.750683	856.1576	616	
172.16.4.4	172.16.4.205	947	227 k	457	96 k	490	131 k	219.890699	414.0451	1,862	
10.0.0.201	168.215.194.14	858	551 k	364	34 k	494	516 k	70.726301	871.0069	319	
10.11.11.11	10.11.11.203	843	189 k	351	83 k	492	106 k	638.444425	172.6836	3,858	
10.11.11.179	13.33.255.25	728	520 k	339	34 k	389	485 k	645.533741	94.0159	2,950	
10.0.0.201	216.58.218.161	708	422 k	318	27 k	390	395 k	75.610606	855.6138	254	
10.11.11.217	172.217.6.162	697	404 k	341	35 k	356	369 k	701.008110	106.4835	2,664	
10.6.12.203	205.185.125.104	649	599 k	186	10 k	463	588 k	56.833981	851.7094	98	
10.11.11.179	143.204.29.89	449	295 k	217	22 k	232	273 k	645.528749	74.8400	2,361	
10.11.11.11	10.11.11.179	440	43 k	112	17 k	328	26 k	633.961277	84.0332	1,620	
10.11.11.11	10.11.11.195	418	35 k	103	10 k	315	25 k	636.490058	173.6506	481	
10.11.11.195	12.133.50.21	417	219 k	192	19 k	225	199 k	676.291489	102.8962	1,541	
10.11.11.179	31.13.93.26	410	291 k	171	13 k	239	278 k	664.567006	71.9760	1,532	
10.11.11.179	172.217.6.162	402	239 k	191	18 k	211	220 k	692.660302	49.3573	3,005	
10.11.11.203	188.95.248.71	376	410 k	86	5,474	290	405 k	720.676394	8.0123	5,465	
31.13.70.52	172.16.4.205	363	239 k	218	223 k	145	15 k	232.816832	138.1120	12 k	
93.95.100.178	172.16.4.205	361	209 k	209	195 k	152	14 k	286.676895	85.7427	18 k	
10.11.11.179	172.217.1.225	357	280 k	158	11 k	199	268 k	717.812947	24.1537	3,005	

Name resolution | Limit to display filter | Absolute start time | Conversation Types

Copy | Follow Stream... | Graph... | Close | Help

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



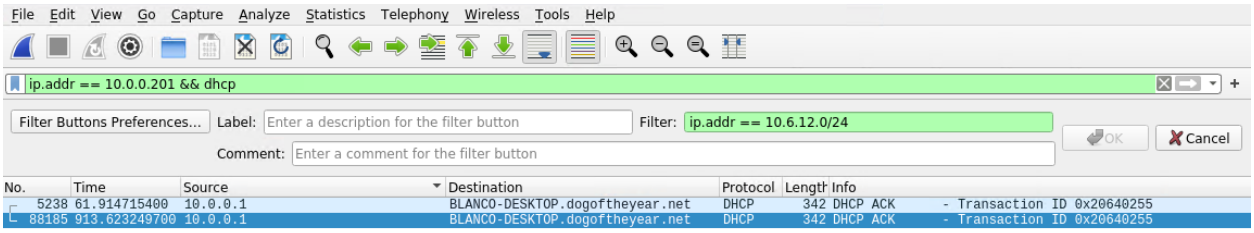
Illegal Downloads

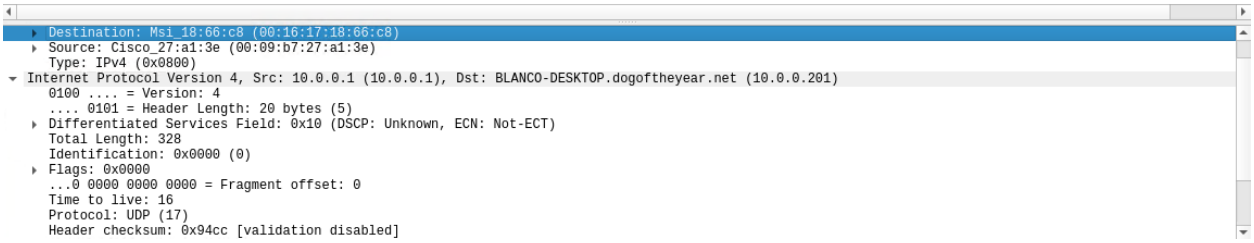
IT was informed that some users are torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringement.
IT shared the following about the torrent activity:

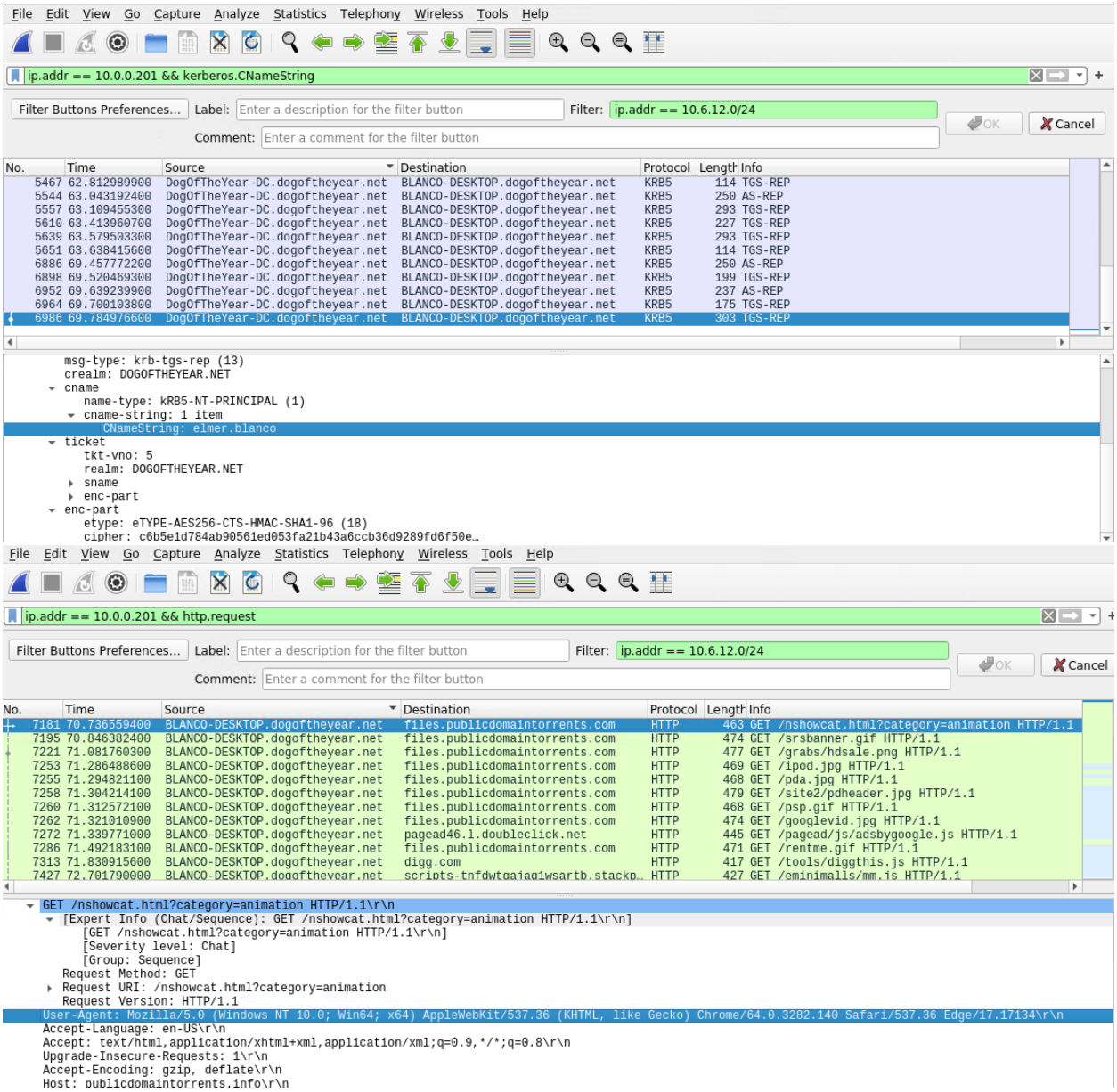
- The machines using torrents live in the range 10.0.0.0/24 and are clients of an AD domain.
- The DC of this domain lives at 10.0.0.2 and is named DogOfTheYear-DC.
- The DC is associated with the domain dogoftheyear.net.

Your task is to isolate torrent traffic and answer the following questions:

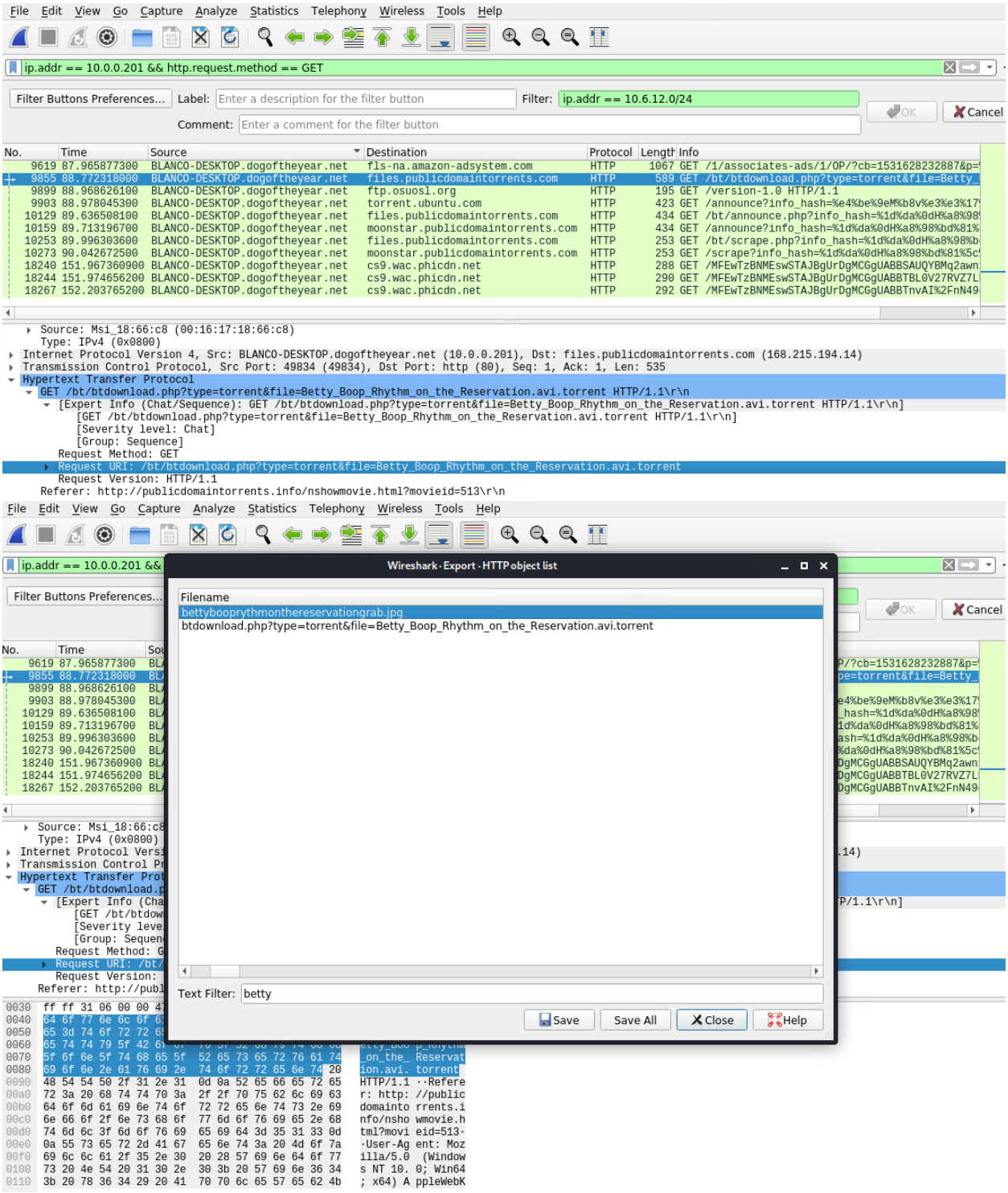
1. Find the following information about the machine with IP address 10.0.0.201:
    - MAC address: 00:16:17:18:66:c8
    - Windows username: elmer.blanco
    - OS version: Windows 10







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


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.0.0.201 && http.request.method == GET
Filter Buttons Preferences...
Label: Enter a description for the filter button
Filter: ip.addr == 10.6.12.0/24
Comment: Enter a comment for the filter button
OK
Cancel
No. Time Source Destination Protocol Length Info
9619 87.965877300 BLANCO-DESKTOP.dogoftheyear.net fls-na.amazon-adsystem.com HTTP 1067 GET /1/associates-ads/1/OP/?cb=1531628232887&p=
9855 88.772318000 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com HTTP 589 GET /bt/btdownload.php?type=torrent&file=Betty_
9899 88.968626100 BLANCO-DESKTOP.dogoftheyear.net ftp.osuosl.org HTTP 195 GET /version-1.0 HTTP/1.1
9903 88.978045300 BLANCO-DESKTOP.dogoftheyear.net torrent.ubuntu.com HTTP 423 GET /announce?info_hash=%e4%be%9eM%b8v%e3%e3%17
10129 89.636508100 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com HTTP 434 GET /bt/announce.php?info_hash=%1d%da%0dH%a8%98
10159 89.713196700 BLANCO-DESKTOP.dogoftheyear.net moonstar.publicdomaintorrents.com HTTP 434 GET /announce?info_hash=%1d%da%0dH%a8%98%bd%81%
10253 89.996303600 BLANCO-DESKTOP.dogoftheyear.net files.publicdomaintorrents.com HTTP 253 GET /bt/scrape.php?info_hash=%1d%da%0dH%a8%98%b
10273 90.042672500 BLANCO-DESKTOP.dogoftheyear.net moonstar.publicdomaintorrents.com HTTP 253 GET /scrape?info_hash=%1d%da%0dH%a8%98%bd%81%5c
18240 151.967360900 BLANCO-DESKTOP.dogoftheyear.net cs9.wac.phicdn.net HTTP 288 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn
18244 151.974656200 BLANCO-DESKTOP.dogoftheyear.net cs9.wac.phicdn.net HTTP 290 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7L
18267 152.203765200 BLANCO-DESKTOP.dogoftheyear.net cs9.wac.phicdn.net HTTP 292 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTnvAI%2FnN49
Source: Msi_18:66:c8 (00:16:17:18:66:c8)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201), Dst: files.publicdomaintorrents.com (168.215.194.14)
Transmission Control Protocol, Src Port: 49834 (49834), Dst Port: http (80), Seq: 1, Ack: 1, Len: 535
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]
[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
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
Wireshark · Export · HTTP object list
Filename
bettybooprythmonthereservationgrab.jpg
btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
Text Filter: betty
Save
Save All
Close
Help


ImageMagick: bettybooprythmonthereservationgrab.jpg
File Name: Betty_Boop_Rhythm_on_the_Reservation.avi
File Size: 100.50 MB
Resolution: 720x480
Duration: 00:06:02
Rhythm on the Reservation
00:00:11
00:00:23
00:00:35
00:00:46
00:00:58
00:01:10
00:01:21
00:01:33
00:01:45
00:01:56
00:02:08
00:02:20
00:02:32
00:02:43
00:02:55
00:03:07
00:03:18
00:03:30
00:03:42
00:03:53
00:04:05
00:04:17
00:04:29
00:04:40
00:04:52
00:05:04
00:05:15
00:05:27
00:05:39
00:05:50