

# Network Analysis

## 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?

Frank-N Ted -DC.frank-n-ted.com

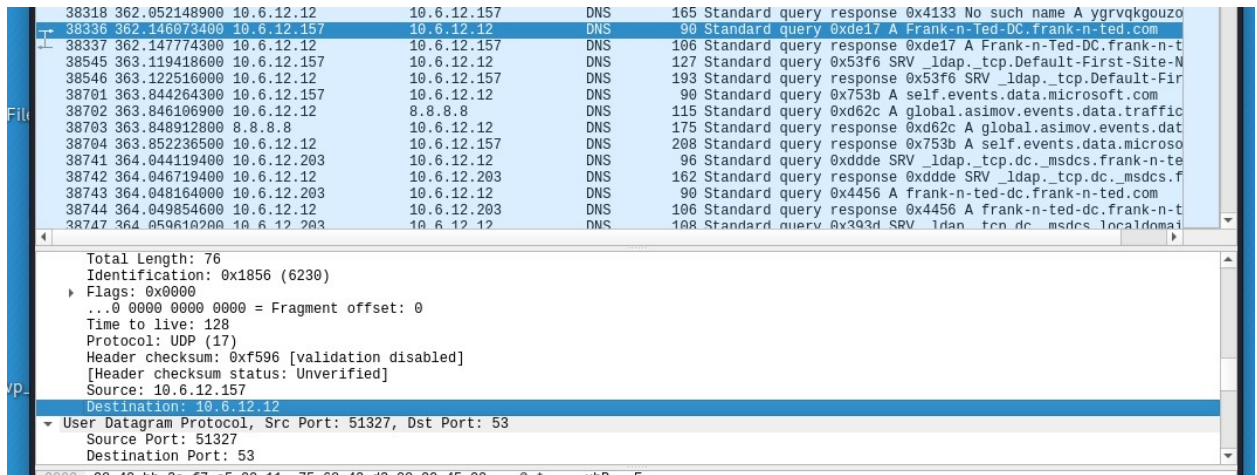
No.	Time	Source	Destination	Protocol	Length	Info
38166	361.510232800	10.6.12.157	10.6.12.12	DNS	132	Standard query 0x79df SRV _ldap._tcp.Default-First-Site-N
38167	361.513402600	10.6.12.12	10.6.12.157	DNS	198	Standard query response 0x79df SRV _ldap._tcp.Default-Fir
38238	361.816018200	10.6.12.157	10.6.12.12	DNS	117	Standard query 0xde86 SRV _ldap._tcp.Default-First-Site-N
38239	361.818946800	10.6.12.12	10.6.12.157	DNS	183	Standard query response 0xde86 SRV _ldap._tcp.Default-Fir
38317	362.049581500	10.6.12.157	10.6.12.12	DNS	88	Standard query 0x4133 A ygrvqkgouzou.frank-n-ted.com
38318	362.052148900	10.6.12.12	10.6.12.157	DNS	165	Standard query response 0x4133 No such name A ygrvqkgouzo
38336	362.146073400	10.6.12.157	10.6.12.12	DNS	90	Standard query 0xde17 A Frank-n-Ted-DC.frank-n-ted.com
38337	362.147774300	10.6.12.12	10.6.12.157	DNS	106	Standard query response 0xde17 A Frank-n-Ted-DC.frank-n-t
38545	363.119418600	10.6.12.157	10.6.12.12	DNS	127	Standard query 0x53f6 SRV _ldap._tcp.Default-First-Site-N
38546	363.122516000	10.6.12.12	10.6.12.157	DNS	193	Standard query response 0x53f6 SRV _ldap._tcp.Default-Fir
38701	363.844264300	10.6.12.157	10.6.12.12	DNS	90	Standard query 0x753b A self.events.data.microsoft.com
38702	363.846106900	10.6.12.12	8.8.8.8	DNS	115	Standard query 0xd62c A global.asimov.events.data.traffic
38703	363.848912800	8.8.8.8	10.6.12.12	DNS	175	Standard query response 0xd62c A global.asimov.events.dat
38704	363.852236500	10.6.12.12	10.6.12.157	DNS	208	Standard query response 0x753b A self.events.data.microso
38741	364.044119400	10.6.12.12	10.6.12.203	DNS	96	Standard query 0xddde SRV _ldap._tcp.dc._msdcs.frank-n-te
38742	364.046719400	10.6.12.12	10.6.12.203	DNS	162	Standard query response 0xddde SRV _ldap._tcp.dc._msdcs.f
38743	364.048164000	10.6.12.203	10.6.12.12	DNS	90	Standard query 0x4456 A frank-n-ted-dc.frank-n-ted.com
38744	364.049854600	10.6.12.12	10.6.12.203	DNS	106	Standard query response 0x4456 A frank-n-ted-dc.frank-n-t
38747	364.050610200	10.6.12.203	10.6.12.12	DNS	108	Standard query 0x393d SRV _ldap._tcp.dc._msdcs.localdomai

0... .. = Response: Message is a query  
.000 0... .. = Opcode: Standard query (0)  
... .. = Truncated: Message is not truncated  
... ..1 ... = Recursion desired: Do query recursively  
... ..0... .. = Z: reserved (0)  
... ..0... .. = Non-authenticated data: Unacceptable

Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
Frank-n-Ted-DC.frank-n-ted.com: type A, class IN  
[Response in: 38337]

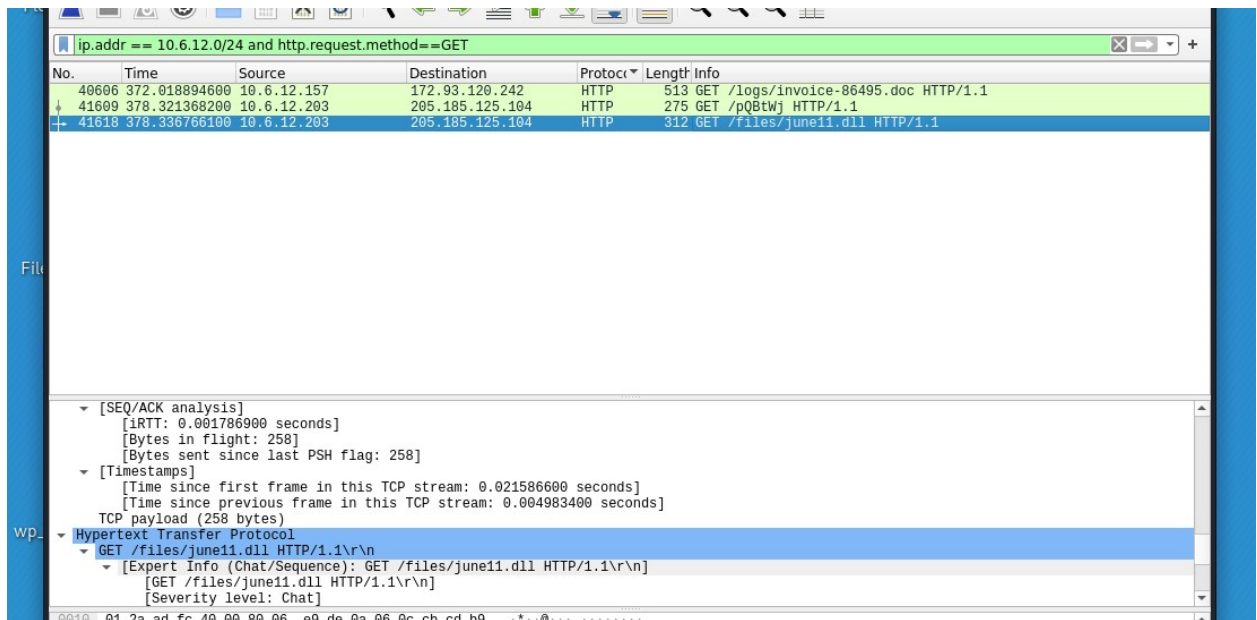
2. What is the IP address of the Domain Controller (DC) of the AD network?

10.6.12.12



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

June11.dll is the malware downloaded



4. Upload the file to [VirusTotal.com](https://www.virustotal.com). What kind of malware is this classified as?

Trojan.mint.Zamg.O

VirusTotal - File - d36366 x +

virustotal.com/gui/file/d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

You are using an unsupported command-line flag: --no-sandbox. Stability and security will suffer.

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

53 / 70

53 security vendors and 1 sandbox flagged this file as malicious

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

549.84 KB Size

2022-07-28 01:49:07 UTC 25 minutes ago

GoogleIpdate.exe

invalid-signature overlay pedli signed spreader

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 5

Security Vendors' Analysis

Ad-Aware	Trojan.Mint.Zamg.O	AhnLab-V3	Malware/Win32.RL_Generic.R346613
Alibaba	TrojanSpy:Win32/Yakes.0454a340	ALYac	Trojan.Mint.Zamg.O
Antiy-AVL	Trojan/Generic.ASCommon.1BE	Arcabit	Trojan.Mint.Zamg.O
Avast	Win32:DangerousSig [Trj]	AVG	Win32:DangerousSig [Trj]
Avira (no cloud)	TR/AD.ZLoader.ladbd	BitDefender	Trojan.Mint.Zamg.O
BitDefender Theta	Gen:NN.ZedlaF.34806.lu9@aul7OQgi	Bkav Pro	W32.AIDetect.malware2
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cylance	Unsafe

## 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

```

Address: 00:59:07:b0:63:a4 (00:59:07:b0:63:a4)
.... 0. .... = LG bit: Globally unique address (factory default)
.... 0. .... = IG bit: Individual address (unicast)
▼ Source: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
Address: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
.... 0. .... = LG bit: Globally unique address (factory default)
.... 0. .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 172.16.4.205, Dst: 31.7.62.214
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

▼ Flags: 0x4000, Don't fragment
0... .... = Reserved bit: Not set
.1... .... = Don't fragment: Set
..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x9c24 [validation disabled]
[Header checksum status: Unverified]
Source: 172.16.4.205
Destination: 31.7.62.214
▼ Transmission Control Protocol, Src Port: 49255, Dst Port: 443
Source Port: 49255
Destination Port: 443
[Stream index: 2]

12573 181.57885/800 172.16.4.205 31.7.62.214 HTTP 282 POST http://
12575 181.584255800 172.16.4.205 31.7.62.214 HTTP 282 POST http://
▼ Hypertext Transfer Protocol
▼ [Expert Info (Warning/Security): Unencrypted HTTP protocol detected over encrypted port
[Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous
[Severity level: Warning]
[Group: Security]
▼ POST http://31.7.62.214/fakeurl.htm HTTP/1.1\n
▼ [Expert Info (Chat/Sequence): POST http://31.7.62.214/fakeurl.htm HTTP/1.1\n]
[POST http://31.7.62.214/fakeurl.htm HTTP/1.1\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: POST
Request URI: http://31.7.62.214/fakeurl.htm
Request Version: HTTP/1.1
User-Agent: NetSupport Manager/1.3\n
Content-Type: application/x-www-form-urlencoded\n
▼ Content-Length: 36\n
[Content length: 36]
Host: 31.7.62.214\n
Connection: Keep-Alive\n
\n

```

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



## Matthijs.devries

60143	621.212397300	172.16.4.205	172.16.4.4	KRB5	317 AS-REQ
66313	621.993034500	172.16.4.205	172.16.4.4	KRB5	301 AS-REQ
66320	622.008666900	172.16.4.205	172.16.4.4	KRB5	381 AS-REQ
66352	622.135358200	172.16.4.205	172.16.4.4	KRB5	292 AS-REQ
66359	622.150912200	172.16.4.205	172.16.4.4	KRB5	372 AS-REQ

[!RTT: 0.001955800 seconds]

[Bytes in flight: 238]

[Bytes sent since last PSH flag: 238]

[Timestamps]

[Time since first frame in this TCP stream: 0.006632400 seconds]

[Time since previous frame in this TCP stream: 0.004676600 seconds]

TCP payload (238 bytes)

[PDU Size: 238]

Kerberos

Record Mark: 234 bytes

0... = Reserved: Not set

.000 0000 0000 0000 0000 0000 1110 1010 = Record Length: 234

as-req

pvno: 5

msg-type: krb-as-req (10)

padata: 1 item

PA-DATA PA-PAC-REQUEST

req-body

Padding: 0

kdc-options: 40810010

cname

name-type: kRB5-NT-PRINCIPAL (1)

cname-string: 1 item

CNameString: matthijs.devries

realm: MIND-HAMMER

sname

name-type: kRB5-NT-PRINCIPAL (1)

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

172.16.4.205, 185.243.115.84, 64.187.66.143

Wireshark - Conversations - 2022.pcapng										
Ethernet · 74		IPv4 · 879		IPv6	TCP · 1039		UDP · 1825			
Address A	Address B	Packets	Bytes		Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
172.16.4.205	185.243.115.84	30,470	27 M		16,968	15 M	13,502	12 M	0.000000	1032.6042
166.62.111.64	172.16.4.205	7,864	8,082 k		5,677	7,921 k	2,187	160 k	622.569935	149.9677
192.168.1.90	192.168.1.100	5,577	26 M		3,621	25 M	1,956	548 k	7.900524	1082.5406
10.0.0.201	64.187.66.143	4,688	3,493 k		2,148	139 k	2,540	3,354 k	491.360257	129.8125
5.101.51.151	10.6.12.203	4,326	4,246 k		3,262	4,177 k	1,064	68 k	389.590854	67.9986
10.0.0.201	23.43.62.169	4,007	4,080 k		1,310	71 k	2,697	4,008 k	552.999906	66.9059
10.11.11.200	151.101.50.208	3,270	2,220 k		1,613	112 k	1,657	2,108 k	291.617646	66.7937
10.11.11.11	10.11.11.200	1,729	384 k		787	172 k	942	212 k	183.778768	905.0566
172.16.4.4	172.16.4.205	1,428	344 k		694	141 k	734	202 k	55.328747	979.9018
10.11.11.11	10.11.11.203	1,424	348 k		616	153 k	808	194 k	188.030654	893.2623
10.6.12.12	10.6.12.203	1,388	350 k		620	161 k	768	188 k	364.044119	99.1499
10.6.12.12	10.6.12.157	1,316	330 k		608	156 k	708	174 k	360.757496	102.3674
10.11.11.179	13.33.255.25	1,228	881 k		570	60 k	658	821 k	195.119959	896.2663
10.0.0.2	10.0.0.201	1,083	266 k		520	133 k	563	132 k	463.219371	89.6854
10.11.11.200	104.18.74.113	1,079	697 k		511	34 k	568	662 k	335.930395	22.4915
10.11.11.179	143.204.29.89	886	590 k		426	43 k	460	547 k	195.114998	888.8778
10.11.11.11	10.11.11.179	854	84 k		215	32 k	639	51 k	183.547497	907.8081
10.11.11.105	12.132.60.21	817	495 k		274	20 k	543	207 k	225.077710	861.8000

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 in your Network Report:

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 blanco-desktop\$
- OS version Window NT 10.0

The image shows a Wireshark packet capture of a DNS query. The packet list on the left shows a query from 10.0.0.201 to 10.0.0.2. The packet details pane on the right shows the following information:

- Frame 18: 100 bytes on wire (80 bytes captured) on interface 0
- Ethernet II, Src: Msi\_18:66:c8 (00:16:17:18:66:c8), Dst: Dell\_f4:3b:96 (00:12:3f:f4:3b:96)
- Destination: Dell\_f4:3b:96 (00:12:3f:f4:3b:96)
- Address: Dell\_f4:3b:96 (00:12:3f:f4:3b:96)
- Source: Msi\_18:66:c8 (00:16:17:18:66:c8)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 10.0.0.201, Dst: 10.0.0.2
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

The packet bytes pane at the bottom shows the raw data of the packet, including the Ethernet II header and the IPv4 header.

No.	Time	Source	Destination	Protocol	Length	Info
48842	463.408626600	10.0.0.201	10.0.0.2	KRB5	301	AS-REQ
48863	463.528511200	10.0.0.201	10.0.0.2	KRB5	381	AS-REQ
48867	463.536300300	10.0.0.201	10.0.0.2	KRB5	301	AS-REQ
48881	463.584222300	10.0.0.201	10.0.0.2	KRB5	382	AS-REQ
48954	463.939583700	10.0.0.201	10.0.0.2	KRB5	301	AS-REQ
48962	463.955804200	10.0.0.201	10.0.0.2	KRB5	381	AS-REQ
49055	464.273544500	10.0.0.201	10.0.0.2	KRB5	301	AS-REQ
49068	464.301619500	10.0.0.201	10.0.0.2	KRB5	382	AS-REQ
50395	470.707773100	10.0.0.201	10.0.0.2	KRB5	302	AS-REQ
50403	470.724303400	10.0.0.201	10.0.0.2	KRB5	382	AS-REQ
50461	470.890429300	10.0.0.201	10.0.0.2	KRB5	290	AS-REQ
50469	470.905960300	10.0.0.201	10.0.0.2	KRB5	370	AS-REQ

```

.... ..0. = renew: False
.... ..0 = validate: False
  ▼ cname
    name-type: KRB5-NT-PRINCIPAL (1)
    ▼ cname-string: 1 item
      CNameString: blanco-desktop$
    realm: DOGOFTHEYEAR.NET
    ▼ sname
      name-type: KRB5-NT-SRV-INST (2)
      ▼ sname-string: 2 items
        SNameString: krbtgt
        SNameString: DOGOFTHEYEAR.NET
      till: 2037-09-13 02:48:05 (UTC)
      rtime: 2037-09-13 02:48:05 (UTC)
      nonce: 2063583367
    ▼ etype: 6 items
      ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
      ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)

```

```

0070 a1 1c 30 1a a0 03 02 01 01 a1 13 30 11 1b 0f 62 ..0..... ..0...b
0080 6c 61 6e 63 6f 2d 64 65 73 6b 74 6f 70 24 a2 12 blanco-de sktop$..

```

52441	484.087183000	10.0.0.201	50.63.243.230	HTTP	276	GET	/MEKwRzBFMEMwQTAJBgUrdgMCgGUABBS2CA1fbGt26xPkOKX4ZguoUjM0T...
52528	484.378530900	10.0.0.201	50.63.243.230	HTTP	276	GET	/MEKwRzBFMEMwQTAJBgUrdgMCgGUABBS2CA1fbGt26xPkOKX4ZguoUjM0T...
52690	484.835690300	10.0.0.201	168.215.194.14	HTTP	534	GET	/nshowmovie.html?movieid=513 HTTP/1.1
52706	484.963408200	10.0.0.201	168.215.194.14	HTTP	471	GET	/yellow-star.gif HTTP/1.1
52714	484.979801700	10.0.0.201	172.217.9.2	HTTP	434	GET	/pagead/show_ads.js HTTP/1.1
52719	484.990235200	10.0.0.201	50.18.44.131	HTTP	412	GET	/tools/diggthis.js HTTP/1.1
52744	485.116547900	10.0.0.201	168.215.194.14	HTTP	500	GET	/grabs/bettybooprhythmthereservationgrab.jpg HTTP/1.1
52790	485.538073400	10.0.0.201	168.215.194.14	HTTP	465	GET	/divx1.jpg HTTP/1.1
52884	486.557946300	10.0.0.201	52.94.240.125	HTTP	415	GET	/s/ads.js HTTP/1.1
52977	487.285427000	10.0.0.201	168.215.194.14	HTTP	531	GET	/usercomments.html?movieid=513 HTTP/1.1
53089	488.325372700	10.0.0.201	52.94.240.125	HTTP	427	GET	/s/ads-common.js HTTP/1.1
53125	488.619613900	10.0.0.201	72.21.202.62	HTTP	885	GET	/e/cm?t=publicdomain0f-20&o=1&p=48&l=op1&pvid=40C236A13FDD0B...
53198	489.260633600	10.0.0.201	52.94.233.131	HTTP	1067	GET	/1/associates-ads/1/OP/?cb=1531628232887&p=%7B%22program%22...
53372	490.067092000	10.0.0.201	168.215.194.14	HTTP	589	GET	/bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_t...
53396	490.227745100	10.0.0.201	239.255.255.250	SSDP	142	M-SEARCH	* HTTP/1.1
53397	490.230015700	10.0.0.201	239.255.255.250	SSDP	142	M-SEARCH	* HTTP/1.1
53398	490.232298600	10.0.0.201	239.255.255.250	SSDP	142	M-SEARCH	* HTTP/1.1
53416	490.263390000	10.0.0.201	140.211.166.134	HTTP	195	GET	/version-1.0 HTTP/1.1

Hypertext Transfer Protocol

GET /grabs/bettybooprhythmthereservationgrab.jpg HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /grabs/bettybooprhythmthereservationgrab.jpg HTTP/1.1\r\n]
[GET /grabs/bettybooprhythmthereservationgrab.jpg HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /grabs/bettybooprhythmthereservationgrab.jpg
Request Version: HTTP/1.1
Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\r\n
Accept: image/png,image/svg+xml,image/\*;q=0.8,\*/\*;q=0.5\r\n
Accept-Language: en-US\r\n
Accept-Encoding: gzip, deflate\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
Host: publicdomaintorrents.info\r\n
Connection: Keep-Alive\r\n
\r\n

2. Which torrent file did the user download?

Betty boop rhythm on the reservation.avi

52977	487.285427000	10.0.0.201	168.215.194.14	HTTP	531	GET	/usercomments.html?movieid=513 HTTP/1.1
53089	488.325372700	10.0.0.201	52.94.240.125	HTTP	427	GET	/s/ads-common.js HTTP/1.1
53125	488.619613900	10.0.0.201	72.21.202.62	HTTP	885	GET	/e/cm?t=publicdomain0f-20&o=1&p=48&l=op1&pvid=40C236A13FDD0B...
53198	489.260633600	10.0.0.201	52.94.233.131	HTTP	1067	GET	/1/associates-ads/1/OP/?cb=1531628232887&p=%7B%22program%22...
53372	490.067092000	10.0.0.201	168.215.194.14	HTTP	589	GET	/bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_t...
53396	490.227745100	10.0.0.201	239.255.255.250	SSDP	142	M-SEARCH	* HTTP/1.1
53397	490.230015700	10.0.0.201	239.255.255.250	SSDP	142	M-SEARCH	* HTTP/1.1
53398	490.232298600	10.0.0.201	239.255.255.250	SSDP	142	M-SEARCH	* HTTP/1.1
53416	490.263390000	10.0.0.201	140.211.166.134	HTTP	195	GET	/version-1.0 HTTP/1.1

[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
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
Accept-Encoding: gzip, deflate\r\n
Host: www.publicdomaintorrents.com\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://www.publicdomaintorrents.com/bt/btdownload.php?type=torrent&file=Betty\_Boop\_Rhythm\_on\_the\_Reservation.avi.torrent]
[HTTP request 1/1]
[Response in frame: 53385]