

Network Analysis

Report by: Amisha Mehta

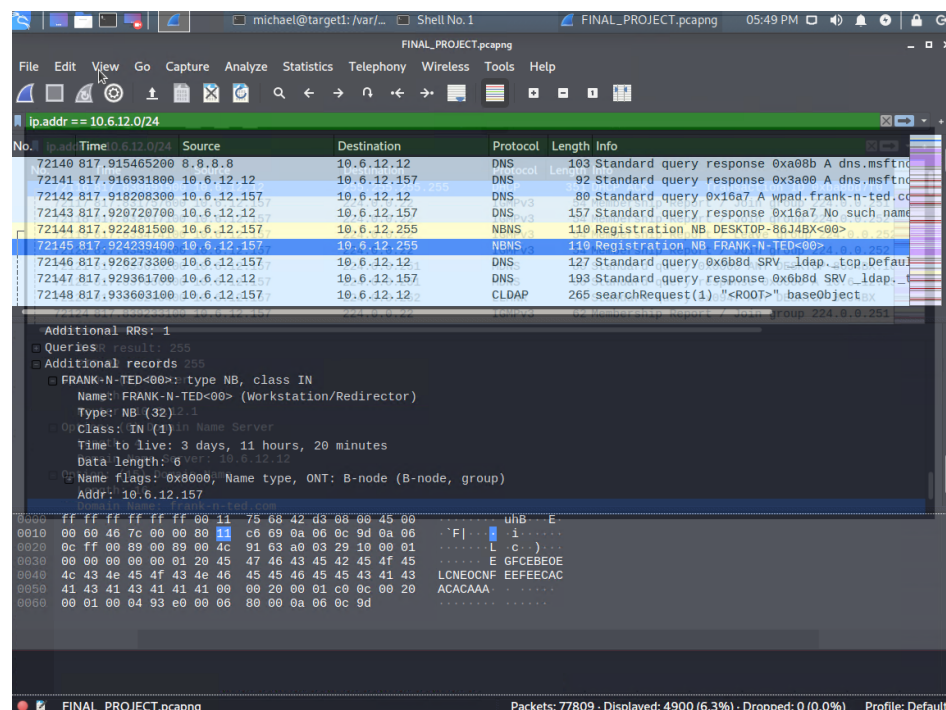
Time Thieves

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.com
 - b. Filter: ip.addr==10.6.12.0/24



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

- a. 10.6.12.12 (frank-n-ted-DC.frank-n-ted.com)
- b. Filter: ip.addr==10.6.12.0/24

ip.addr==10.6.12.0/24

No.	Time	Source	Destination	Protocol	Length	Info
55420	641.047496500	Frank-n-Ted-DC.fran...	255.255.255.255	DHCP	351	DHCP ACK - Transaction ID 0xba8bd7f0
55421	641.048373200	DESKTOP-86J4BX.fran...	igmp.mcast.net	IGMPv3	54	Membership Report / Join group 224.0.0.251
55422	641.049214500	DESKTOP-86J4BX.fran...	igmp.mcast.net	IGMPv3	54	Membership Report / Join group 224.0.0.252
55423	641.050071100	DESKTOP-86J4BX.fran...	igmp.mcast.net	IGMPv3	54	Membership Report / Leave group 224.0.0.252
55424	641.050936500	DESKTOP-86J4BX.fran...	igmp.mcast.net	IGMPv3	54	Membership Report / Join group 224.0.0.252
55425	641.052219600	DESKTOP-86J4BX.fran...	224.0.0.251	MDNS	80	Standard query 0x0000 ANY DESKTOP-86J4BX.1
55426	641.053707000	DESKTOP-86J4BX.fran...	224.0.0.251	MDNS	90	Standard query response 0x0000 A 10.6.12.15
55427	641.054843300	DESKTOP-86J4BX.fran...	224.0.0.252	LLMNR	74	Standard query 0x094f ANY DESKTOP-86J4BX
55428	641.055829300	DESKTOP-86J4BX.fran...	igmp.mcast.net	IGMPv3	62	Membership Report / Join group 224.0.0.251

Frame 55420: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits) on interface eth0, id 0

Ethernet II, Src: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12), Dst: 255.255.255.255 (255.255.255.255)

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

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
 - b. Filter: ip.addr==10.16.12.203 && http
 - c. Export: File>Export Objects>HTTP>june11.dll

ip.addr==10.6.12.203 && http

No.	Time	Source	Destination	Proto	Length	Info
58752	658.636633700	10.6.12.203	205.185.125...	HTTP	312	GET /files/june11.dll HTTP/1.1
58748	658.621258400	10.6.12.203	205.185.125...	HTTP	275	GET /pQBtwj HTTP/1.1
59388	668.197470500	205.185.125...	10.6.12.203	HTTP	946	HTTP/1.1 200 OK
59682	669.911770400	5.101.51.151	10.6.12.203	HTTP	436	HTTP/1.1 200 OK (text/html)
60071	676.208169900	5.101.51.151	10.6.12.203	HTTP	1371	HTTP/1.1 200 OK (text/html)
60107	676.349463900	5.101.51.151	10.6.12.203	HTTP	583	HTTP/1.1 200 OK (text/html)
60376	680.655793900	5.101.51.151	10.6.12.203	HTTP	487	HTTP/1.1 200 OK (text/html)
60775	686.819937200	5.101.51.151	10.6.12.203	HTTP	268	HTTP/1.1 200 OK (text/html)
60835	687.584408000	5.101.51.151	10.6.12.203	HTTP	846	HTTP/1.1 200 OK (text/html)
60879	688.215331700	5.101.51.151	10.6.12.203	HTTP	93	HTTP/1.1 200 OK (text/html)

Accept: */*\r\n

Accept-Encoding: gzip, deflate\r\n

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)\r\n

Host: 205.185.125.104\r\n

Connection: Keep-Alive\r\n

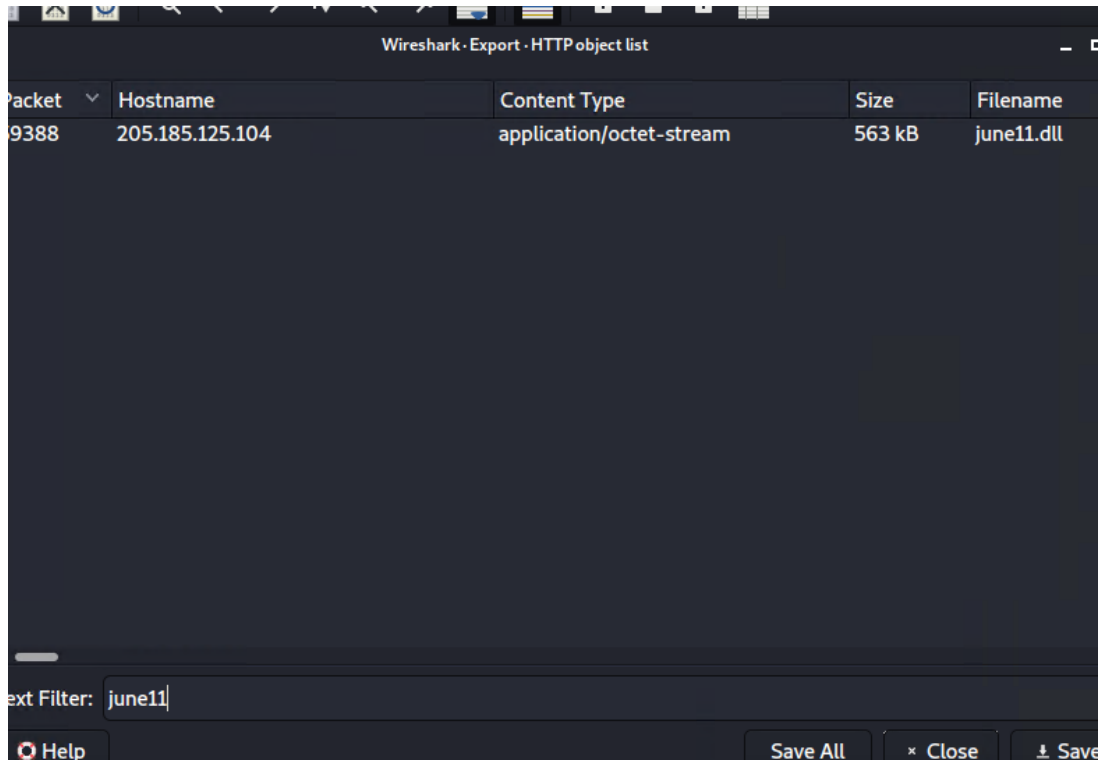
Cookie: _subid=3mmhfdn8jp\r\n

[Full request URI: http://205.185.125.104/files/june11.dll]

[HTTP request 2/2]

[Prev request in frame: 58748]

[Response in frame: 59388]



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

https://www.virustotal.com/gui/file/d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

49 / 67

4 security vendors tagged this file as malicious

GoogleUpdate.exe
invalid-signature overlay pedl signed

549.84 KB
Size

2021-08-28 17:19:13 UTC
3 days ago

DLL

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	Trojan.Mint.Zamg.O	AhnLab-V3	Malware/Win32.RL_Generic.R346613	
Alibaba	TrojanSpy:Win32/Yakes.56555f48	ALYac	Trojan.Mint.Zamg.O	
Antiy-AVL	Trojan/Generic.ASCommon.1BE	SecureAge APEX	Malicious	
Avast	Win32:DangerousSig [Trj]	AVG	Win32:DangerousSig [Trj]	
Avira (no cloud)	TR/AD.ZLoader.ladbd	BitDefender	Trojan.Mint.Zamg.O	
BitDefenderTheta	Gen:NN.ZedlaF.34110.lu9@aul7OQgi	CrowdStrike Falcon	Win/malicious_confidence_100% (W)	
Cylance	Unsafe	Cynet	Malicious (score: 100)	
Cyren	W32/Trojan.SIAQ-3008	DrWeb	Trojan.Inject.3.53106	
eGambit	Unsafe.AI_Score_98%	Elastic	Malicious (high Confidence)	

Vulnerable Windows Machines

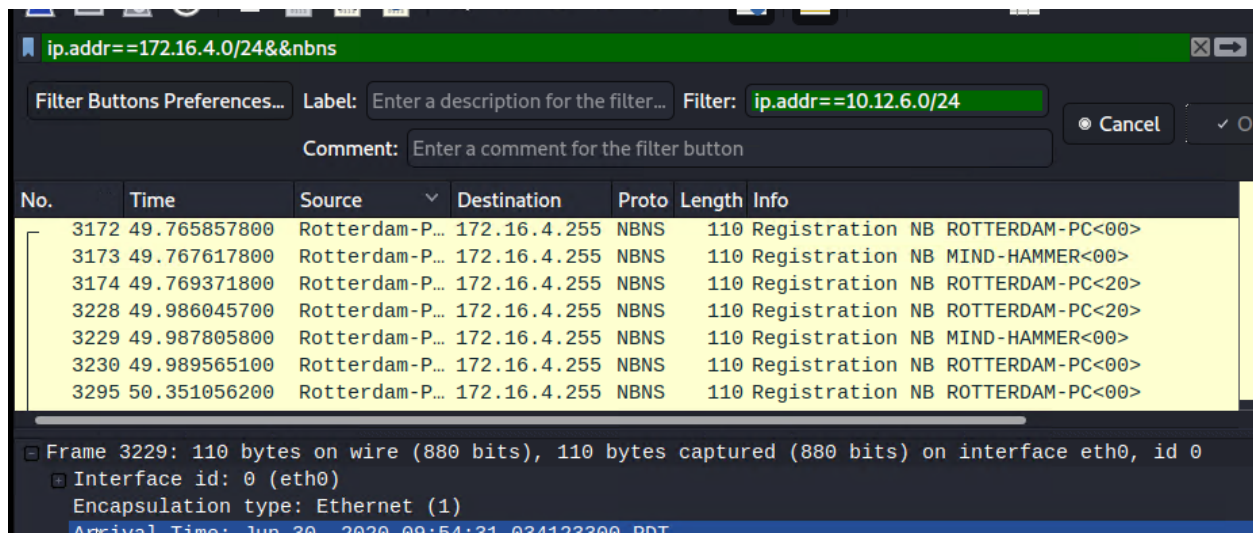
The Security team received reports of an infected Windows host on the network. They know the following:

- 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**

Filter: **ip.addr==172.16.4.0/24&&nbns**



The image shows a Wireshark packet capture window with a filter applied: `ip.addr==172.16.4.0/24&&nbns`. The packet list shows several NBNS registration packets from Rotterdam-PC (172.16.4.205) to Mind-Hammer-DC (172.16.4.4). The selected packet is Frame 3229, which is an NBNS registration from Rotterdam-PC to Mind-Hammer-DC. The packet details pane shows the frame structure: Ethernet II (Type: IPv4), Internet Protocol Version 4, and User Datagram Protocol.

No.	Time	Source	Destination	Proto	Length	Info
3172	49.765857800	Rotterdam-P...	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<00>
3173	49.767617800	Rotterdam-P...	172.16.4.255	NBNS	110	Registration NB MIND-HAMMER<00>
3174	49.769371800	Rotterdam-P...	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<20>
3228	49.986045700	Rotterdam-P...	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<20>
3229	49.987805800	Rotterdam-P...	172.16.4.255	NBNS	110	Registration NB MIND-HAMMER<00>
3230	49.989565100	Rotterdam-P...	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<00>
3295	50.351056200	Rotterdam-P...	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<00>

Frame 3229: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface eth0, id 0
Interface id: 0 (eth0)
Encapsulation type: Ethernet (1)
Arrival Time: Jun 30, 2020 09:54:31.034123300 PDT

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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==172.16.4.205 and kerberos.CNameString

No.	Time	Source	Destination	Protocol	Length	CNameString	Info
3250	50.135544700	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	KRB5	158	ROTTERDAM-PC\$	TGS-REP
3270	50.241859400	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	KRB5	84	ROTTERDAM-PC\$	TGS-REP
3369	50.584361200	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	KRB5	381	ROTTERDAM-PC\$	AS-REQ
3376	50.599992500	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	KRB5	381	ROTTERDAM-PC\$	AS-REQ
3378	50.627492100	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	KRB5	204	ROTTERDAM-PC\$	AS-REP
3390	50.688223400	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	KRB5	130	ROTTERDAM-PC\$	TGS-REP
3408	50.726684900	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	KRB5	292	matthijs.devries	AS-REQ
3415	50.742235400	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	KRB5	372	matthijs.devries	AS-REQ
3417	50.770347900	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	KRB5	242	matthijs.devries	AS-REP

```

...1 ... = renewable-ok: True
... 0... = enc-tkt-in-skey: False
... ..0.. = unused29: False
... ..0.. = renew: False
... ...0 = validate: False
cname
  name-type: kRB5-NT-PRINCIPAL (1)
  cname-string: 1 item
    CNameString: matthijs.devries
realm: MIND-HAMMER
ename

```

0070 a1 1d 30 1b a0 03 02 01 01 a1 14 30 12 1b 10 6d ..0.....0...
0080 61 74 74 68 69 6a 73 2e 64 65 76 72 69 65 73 a2 matthijs.devries
0090 0d 1b 0b 4d 49 4e 44 2d 48 41 4d 4d 45 52 a3 20 ...MIND- HAMMER

- What are the IP addresses used in the actual infection traffic?
 - 172.16.4.205, 185.243.115.84, 166.62.11.64 are the infected traffic.

Statistics > Conversations > IPv4 (tab) > Packets (high to low)

Filter: ip.addr==172.16.4.205 and ip.addr==185.243.115.84

Wireshark · Conversations · pcap.pcap

Ethernet · 74		IPv4 · 877	IPv6 · 1	TCP · 1044	UDP · 1839					
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	30,344	26 M	15,149	9,831 k	15,195	16 M	196.154314	1016.8611	
166.62.111.64	172.16.4.205	15,728	16 M	11,354	15 M	4,374	321 k	51.161259	1001.6762	
10.0.0.201	23.43.62.169	6,934	7,045 k	2,282	124 k	4,652	6,920 k	0.000000	900.2057	
10.0.0.201	64.187.66.143	4,883	3,637 k	2,235	144 k	2,648	3,492 k	47.425979	854.0467	
5.101.51.151	10.6.12.203	4,326	4,246 k	3,262	4,177 k	1,064	68 k	669.890730	67.9985	
10.11.11.200	151.101.50.208	3,270	2,220 k	1,613	112 k	1,657	2,108 k	571.917522	66.7937	
172.16.4.4	172.16.4.205	1,417	339 k	680	147 k	737	191 k	49.776799	1144.3125	
10.6.12.12	10.6.12.203	1,388	350 k	620	161 k	768	188 k	644.343994	99.1499	
10.6.12.12	10.6.12.157	1,316	330 k	608	156 k	708	174 k	641.057369	102.3674	
10.11.11.11	10.11.11.200	1,100	219 k	493	98 k	607	120 k	464.078707	176.9288	
10.0.0.2	10.0.0.201	1,083	266 k	520	133 k	563	132 k	743.519241	89.6854	
10.11.11.200	104.18.74.113	1,079	697 k	511	34 k	568	662 k	616.230265	22.4916	
10.11.11.11	10.11.11.203	843	189 k	351	83 k	492	106 k	468.330519	172.6836	
10.11.11.179	13.33.255.25	728	520 k	339	34 k	389	485 k	475.419836	94.0159	

ip.addr==185.243.115.84 and ip.addr==172.16.4.205 and http.request.method=="POST"

No.	Time	Source	Destination	Protocol	Length	Info
13010	196.168142500	Rotterdam-PC.mind-h...	b5689023.green.matt...	HTTP	126	POST /empty.gif HTTP/1.1 (application/x-www-form)
13086	196.795147600	Rotterdam-PC.mind-h...	b5689023.green.matt...	HTTP	534	POST /empty.gif HTTP/1.1 (application/x-www-form)
23682	335.615005700	Rotterdam-PC.mind-h...	b5689023.green.matt...	HTTP	326	POST /empty.gif HTTP/1.1 (application/x-www-form)
27702	398.455630400	Rotterdam-PC.mind-h...	b5689023.green.matt...	HTTP	496	POST /empty.gif?ss&ss1img HTTP/1.1 (PNG)
31721	461.182108400	Rotterdam-PC.mind-h...	b5689023.green.matt...	HTTP	1366	POST /empty.gif?ss&ss2img HTTP/1.1 (PNG)

Frame 31721: 1366 bytes on wire (10928 bits), 1366 bytes captured (10928 bits) on interface eth0, id 0
 Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Cisco_e6:c4:77 (00:15:c6:e6:c4:77)
 Internet Protocol Version 4, Src: Rotterdam-PC.mind-hammer.net (172.16.4.205), Dst: b5689023.green.mattingsolutions.co (185.243.115.84)

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 NT 10 x64**

ip.addr==10.0.0.201 and kerberos.CNameString

No.	Time	Source	Destination	Protocol	Length	CNameString	Info
66970	751.007645200	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dog...	KRB5	302	BLANCO-DESKTOP\$	AS-REQ
66978	751.024207500	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dog...	KRB5	382	BLANCO-DESKTOP\$	AS-REQ
66980	751.052436500	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dogo...	KRB5	250	BLANCO-DESKTOP\$	AS-REP
66992	751.115116900	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dogo...	KRB5	199	BLANCO-DESKTOP\$	TGS-REP
67036	751.190289600	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dog...	KRB5	290	elmer.blanco	AS-REQ
67044	751.205833000	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dog...	KRB5	370	elmer.blanco	AS-REQ
67046	751.233860000	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dogo...	KRB5	237	elmer.blanco	AS-REP
67058	751.294737700	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dogo...	KRB5	175	elmer.blanco	TGS-REP
67080	751.379585100	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dogo...	KRB5	303	elmer.blanco	TGS-REP

```

.0.. .... = unused25: False
..0. .... = disable-transited-check: False
...1 .... = renewable-ok: True
.... 0... = enc-tkt-in-skey: False
.... .0.. = unused29: False
.... ..0. = renew: False
.... .... = validate: False
cname

```

ip.addr==10.0.0.201

Packet details ▾ Narrow & Wide ▾ Case sensitive String user-agent Find Ca

No.	Time	Source	Destination	Pr	Length	Info
67337	752.915643000	BLANCO-DESK...	files.publi...	HTTP	474	GET /googlevid.jpg HTTP/1.1
67347	752.934398000	BLANCO-DESK...	pagead46.1...	HTTP	445	GET /pagead/js/adsbygoogle.js HTTP/1.1
67358	753.074527900	files.publi...	BLANCO-DESK...	HTTP	918	HTTP/1.1 200 OK (PNG)
67361	753.086811900	BLANCO-DESK...	files.publi...	HTTP	471	GET /rentme.gif HTTP/1.1
67363	753.101635100	files.publi...	BLANCO-DESK...	HTTP	868	HTTP/1.1 200 OK (GIF89a)
67364	753.114735100	files.publi...	BLANCO-DESK...	HTTP	814	HTTP/1.1 200 OK (JPEG JFIF image)
67367	753.135638300	files.publi...	BLANCO-DESK...	HTTP	1207	HTTP/1.1 200 OK (JPEG JFIF image)
67384	753.416088600	files.publi...	BLANCO-DESK...	HTTP	601	HTTP/1.1 200 OK (JPEG JFIF image)

```

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/67.0.3490.80 Safari/537.36\r\n
Host: publicdomaintorrents.info\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://publicdomaintorrents.info/googlevid.jpg]
[HTTP request 2/2]
[Prev request in frame: 67282]

```

2. Which torrent file did the user download?
 - Betty boop rhythm on the reservations.avi.torrent

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... Filter: ip.addr==10.0.0.201 Cancel OK

Comment: Enter a comment for the filter button

No.	Time	Source	Destination	Proto	Length	Info
69706	770.366956400	BLANCO-DESK...	files.publi...	HTTP	589	GET /bt/btdownload.php?type=torrent&file=
70122	771.590958400	BLANCO-DESK...	files.publi...	HTTP	253	GET /bt/scrape.php?info_hash=%1d%da%0dH%
69213	765.837950500	BLANCO-DESK...	files.publi...	HTTP	465	GET /divxi.jpg HTTP/1.1
69470	768.919511100	BLANCO-DESK...	rcm-na.asso...	HTTP	885	GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=
67493	754.296424700	BLANCO-DESK...	scripts-tnf...	HTTP	427	GET /eminimalls/mm.js HTTP/1.1
67807	756.854476400	BLANCO-DESK...	files.publi...	HTTP	336	GET /favicon.ico HTTP/1.1
67337	752.915643000	BLANCO-DESK...	files.publi...	HTTP	474	GET /googlevid.jpg HTTP/1.1

ence): GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1

load.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent

.1

aintorrents.info/nshowmovie.html?movieid=513\r\n

Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 E

n

tion/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n

: 1\r\n

flate\r\n

rents.com\r\n

n

/www.publicdomaintorrents.com/bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.a

1

0000 48 54 54 50 2f 31 2e 34 0d 0a 52 65 66 65 72 65 HTTP/1.1 Refere