

Network Analysis

Time Thieves

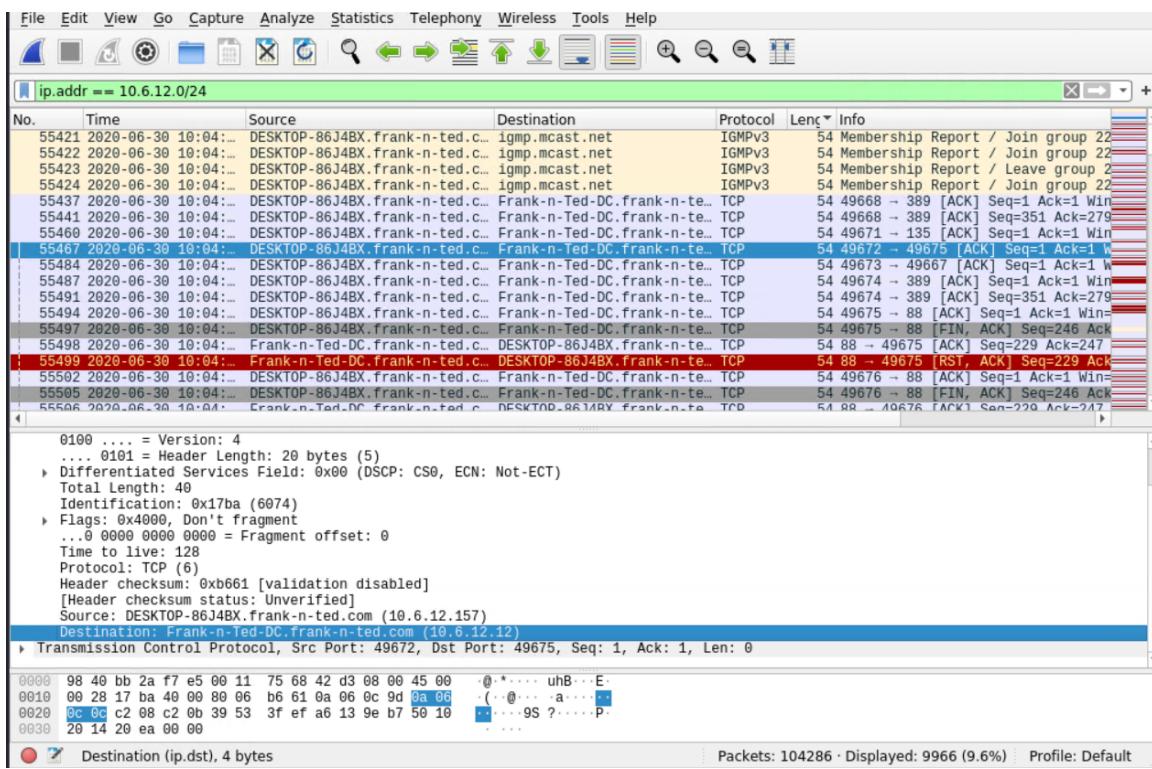
At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- 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?

- 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

pcap.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 10.6.12.0/24

No.	Time	Source	Destination	Protocol	Len	Info
55421	2020-06-30 10:04:...	DESKTOP-86J4BX.frank-n-ted.c...	igmp.mcast.net	IGMPv3	54	Membership Report / Join group 22
55422	2020-06-30 10:04:...	DESKTOP-86J4BX.frank-n-ted.c...	igmp.mcast.net	IGMPv3	54	Membership Report / Join group 22
55423	2020-06-30 10:04:...	DESKTOP-86J4BX.frank-n-ted.c...	igmp.mcast.net	IGMPv3	54	Membership Report / Leave group 2
55424	2020-06-30 10:04:...	DESKTOP-86J4BX.frank-n-ted.c...	igmp.mcast.net	IGMPv3	54	Membership Report / Join group 22
55437	2020-06-30 10:04:...	DESKTOP-86J4BX.frank-n-ted.c...	Frank-n-Ted-DC.frank-n-te...	TCP	54	49668 - 389 [ACK] Seq=1 Ack=1 Win=...
55441	2020-06-30 10:04:...	DESKTOP-86J4BX.frank-n-ted.c...	Frank-n-Ted-DC.frank-n-te...	TCP	54	49668 - 389 [ACK] Seq=351 Ack=279
55460	2020-06-30 10:04:...	DESKTOP-86J4BX.frank-n-ted.c...	Frank-n-Ted-DC.frank-n-te...	TCP	54	49671 - 135 [ACK] Seq=1 Ack=1 Win=...
55467	2020-06-30 10:04:...	DESKTOP-86J4BX.frank-n-ted.c...	Frank-n-Ted-DC.frank-n-te...	TCP	54	49672 - 49675 [ACK] Seq=1 Ack=1 Win=...
55484	2020-06-30 10:04:...	DESKTOP-86J4BX.frank-n-ted.c...	Frank-n-Ted-DC.frank-n-te...	TCP	54	49673 - 49667 [ACK] Seq=1 Ack=1 Win=...
55487	2020-06-30 10:04:...	DESKTOP-86J4BX.frank-n-ted.c...	Frank-n-Ted-DC.frank-n-te...	TCP	54	49674 - 389 [ACK] Seq=1 Ack=1 Win=...
55491	2020-06-30 10:04:...	DESKTOP-86J4BX.frank-n-ted.c...	Frank-n-Ted-DC.frank-n-te...	TCP	54	49674 - 389 [ACK] Seq=351 Ack=279
55494	2020-06-30 10:04:...	DESKTOP-86J4BX.frank-n-ted.c...	Frank-n-Ted-DC.frank-n-te...	TCP	54	49675 - 88 [ACK] Seq=1 Ack=1 Win=...
55497	2020-06-30 10:04:...	DESKTOP-86J4BX.frank-n-ted.c...	Frank-n-Ted-DC.frank-n-te...	TCP	54	49675 - 88 [FIN, ACK] Seq=246 Ack=...
55498	2020-06-30 10:04:...	Frank-n-Ted-DC.frank-n-te...	DESKTOP-86J4BX.frank-n-te...	TCP	54	88 - 49675 [ACK] Seq=229 Ack=247
- 55499	2020-06-30 10:04:...	Frank-n-Ted-DC.frank-n-te...	DESKTOP-86J4BX.frank-n-te...	TCP	54	88 - 49675 [RST, ACK] Seq=229 Ack=...
55502	2020-06-30 10:04:...	DESKTOP-86J4BX.frank-n-ted.c...	Frank-n-Ted-DC.frank-n-te...	TCP	54	49676 - 88 [ACK] Seq=1 Ack=1 Win=...
55505	2020-06-30 10:04:...	DESKTOP-86J4BX.frank-n-ted.c...	Frank-n-Ted-DC.frank-n-te...	TCP	54	49676 - 88 [FIN, ACK] Seq=246 Ack=...
55506	2020-06-30 10:04:...	Frank-n-Ted-DC.frank-n-te...	DESKTOP-86J4BX.frank-n-te...	TCP	54	88 - 49676 [ACK] Seq=229 Ack=247

Internet Protocol Version 4, Src: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12), Dst: DESKTOP-86J4BX.frank-n-ted.com (10.6.12.157)

0100 = Version: 4
... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x5462 (21602)
Flags: 0x4000, Don't fragment
... 0 0000 0000 0000 = Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x79b9 [validation disabled]
[Header checksum status: Unverified]

Source: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12)
Destination: DESKTOP-86J4BX.frank-n-ted.com (10.6.12.157)

Transmission Control Protocol. Src Port: 88 Dst Port: 49675 Seq: 229. Ack: 247. Len: 0

```
0000  00 11 75 68 42 d3 98 40 bb 2a f5 e5 08 00 45 00 ..uhB..@.*...E.
0010  00 28 54 62 40 00 00 06 79 b9 0a 06 0c 0c 0a 06 ..(Tb@...y...:...
0020  0c 9d 00 58 c2 0b 7c 37 ae a5 3a 55 e7 36 50 14 ..X..|7 ..:U 6P..
0030  00 00 74 4f 00 00 ..t0...
```

Source (ip.src), 4 bytes

Packets: 104286 · Displayed: 5130 (4.9%) · Profile: Default

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

pcap.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.6.12.0/24 and http.request.method == GET

No.	Time	Source	Destination	Protocol	Len	Info
58748	2020-06-30 10:04:...	LAPTOP-5WKH9YG.frank-n-ted...	205.185.125.104	HTTP	275	GET /pQBtWj HTTP/1.1
+ 58752	2020-06-30 10:04:...	LAPTOP-5WKH9YG.frank-n-ted...	205.185.125.104	HTTP	312	GET /files/june11.dll HTTP/1.1
57901	2020-06-30 10:04:...	DESKTOP-86J4BX.frank-n-ted.c...	cardboardspaceshiptoyos.com	HTTP	513	GET /logs/invoice-86495.doc HTTP/1.1

Hypertext Transfer Protocol

GET /files/june11.dll HTTP/1.1\r\n

Accept: */*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)\r\nHost: 205.185.125.104\r\nConnection: Keep-Alive\r\nCookie: _subid=3mmhfnd8jp\r\nCookie pair: _subid=3mmhfnd8jp\r\n\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]

```
0010  01 2a ad fc 40 00 80 06 e9 de 0a 06 0c cb cd b9 .*.@.... ...
0020  7d 68 c2 4b 00 50 04 1f 3f 3d 78 a3 1c 80 50 18 JHK-P- ?=x-Q-P-
0030  ff ff 34 0f 00 47 45 54 20 2f 66 69 6c 65 73 ..4.. GE T /files
0040  2f 6a 75 6e 65 31 31 2e 64 6c 6c 20 48 54 54 50 /june11.dll HTTP
```

Source (ip.src), 4 bytes

Packets: 104286 · Displayed: 3 (0.0%) · Profile: Default

4. Upload the file to [VirusTotal.com](#).

52 / 68

Community Score

① 52 security vendors and 1 sandbox flagged this file as malicious

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Googleipdate.exe

invalid-signature overlay pedil signed spreader

549.84 KB | 2022-03-05 17:04:30 UTC
2 days ago

DLL

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	① Trojan.Mint.Zamg.O	AhnLab-V3		① Malware/Win32.RL_Generic.R346613
Alibaba	① TrojanSpy:Win32/Yakes.0454a340	ALYac		① Trojan.Mint.Zamg.O
Antiy-AVL	① Trojan/Generic.ASCommon!BE	Arcabit		① Trojan.Mint.Zamg.O
Avast	① Win32:DangerousSig [Trj]	AVG		① Win32:DangerousSig [Trj]
Avira (no cloud)	① TR/AD.ZLoader.ladbd	BitDefender		① Trojan.Mint.Zamg.O
BitDefenderTheta	① Gen>NN.ZedlaF.34264.lu9@au17OQgi	CAT-QuickHeal		① Ransom.LockyCiR

5. What kind of malware is this classified as?

- [Trojan.Mint.Zamg.O](#)

Vulnerable Windows Machines

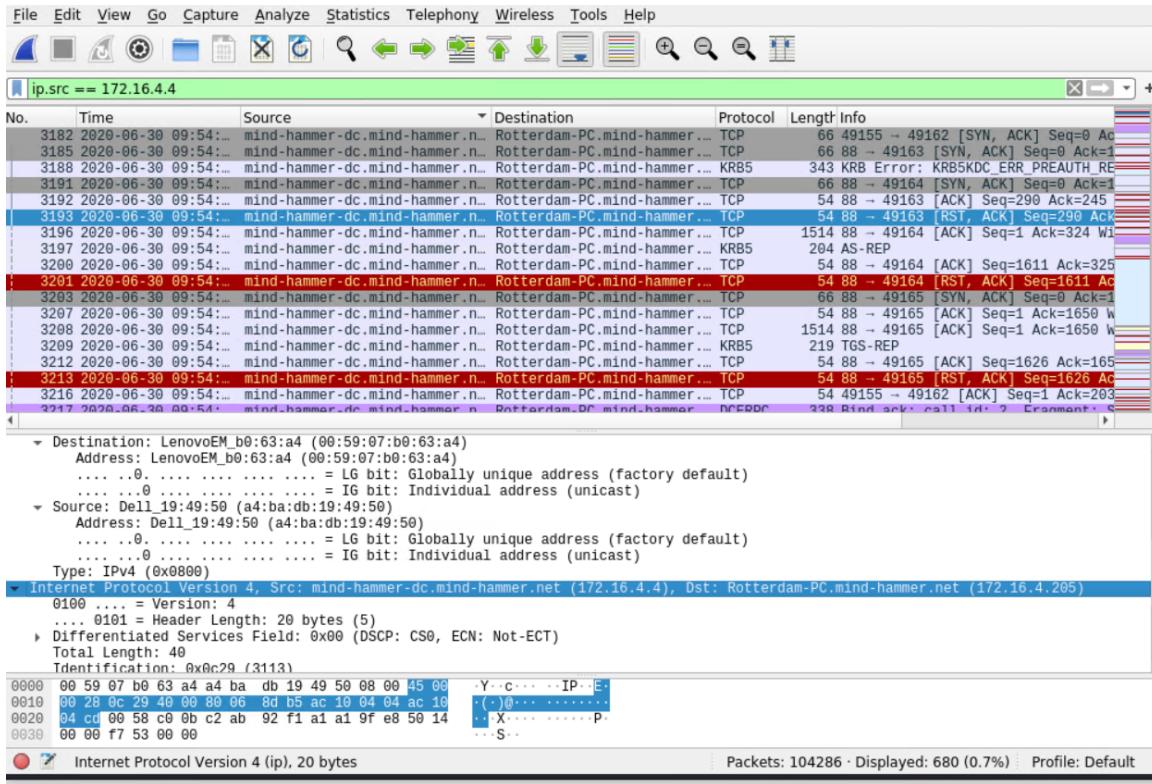
The Security team received reports of an infected Windows host on the network. They know the following:

- 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:

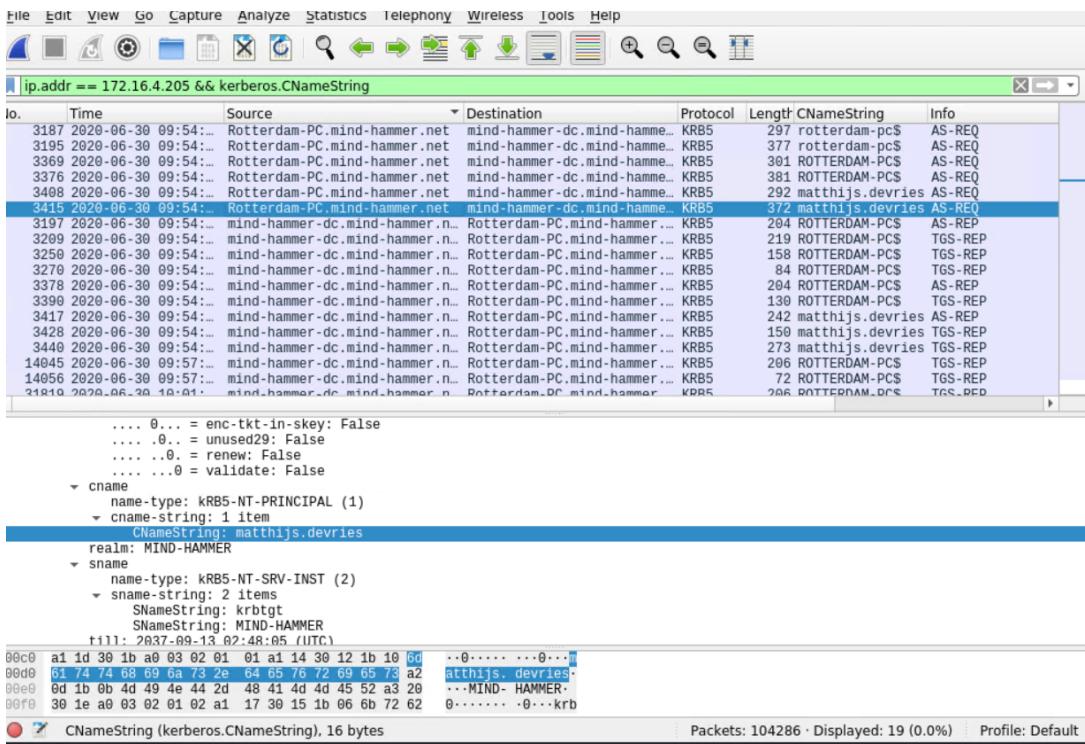
- Find the following information about the infected Windows machine:

- Host name: Rotterdam-PC
- IP address: 172.16.4.205
- MAC address: 00:59:07:b0:63:a4



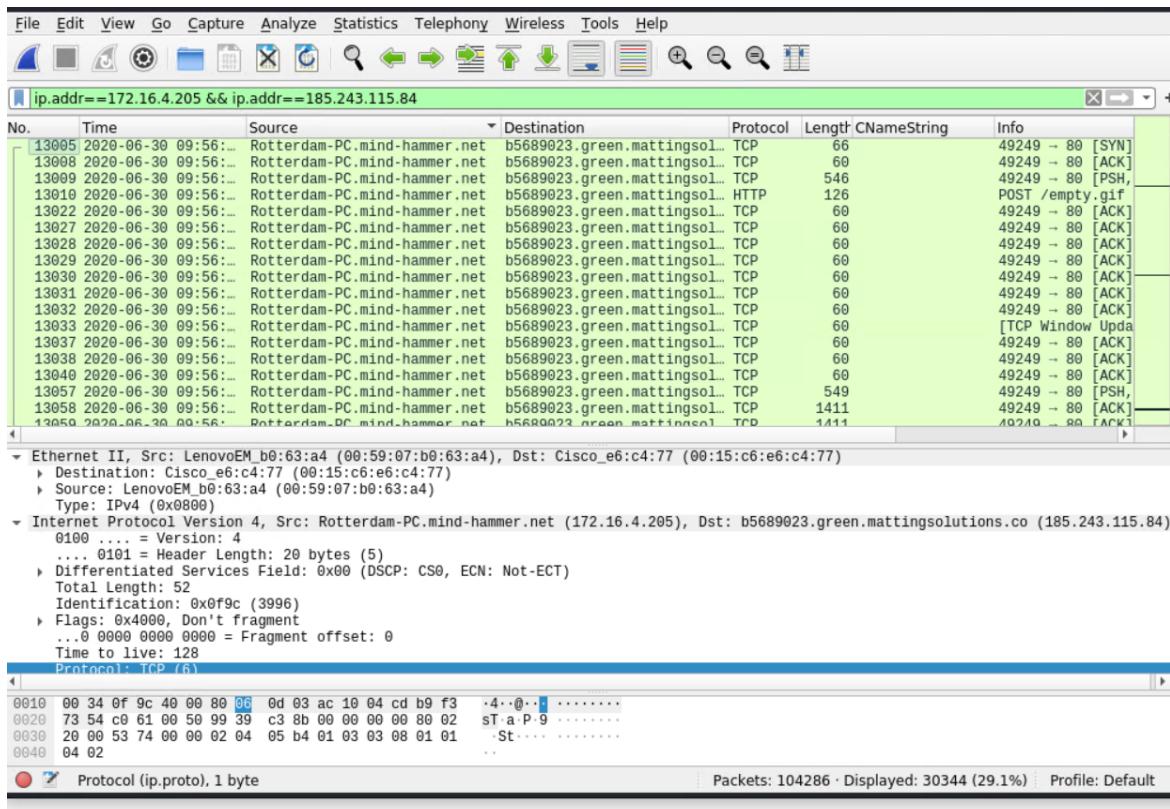
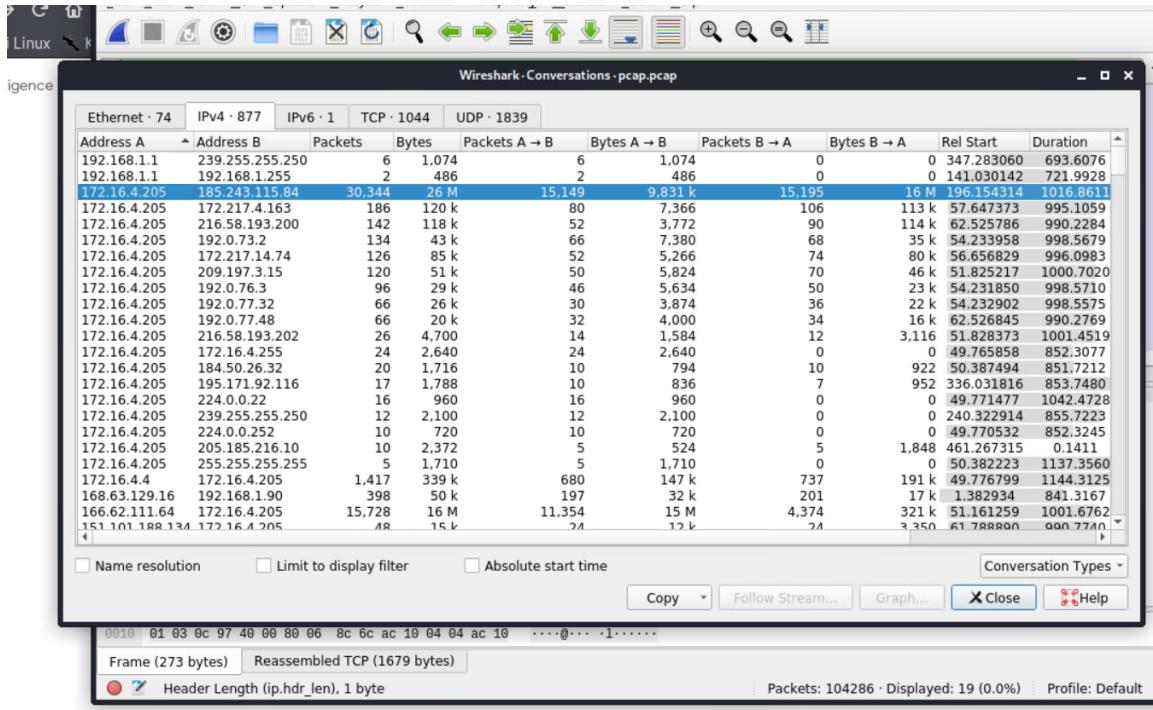
2. What is the username of the Windows user whose computer is infected?

- matthijs.devries

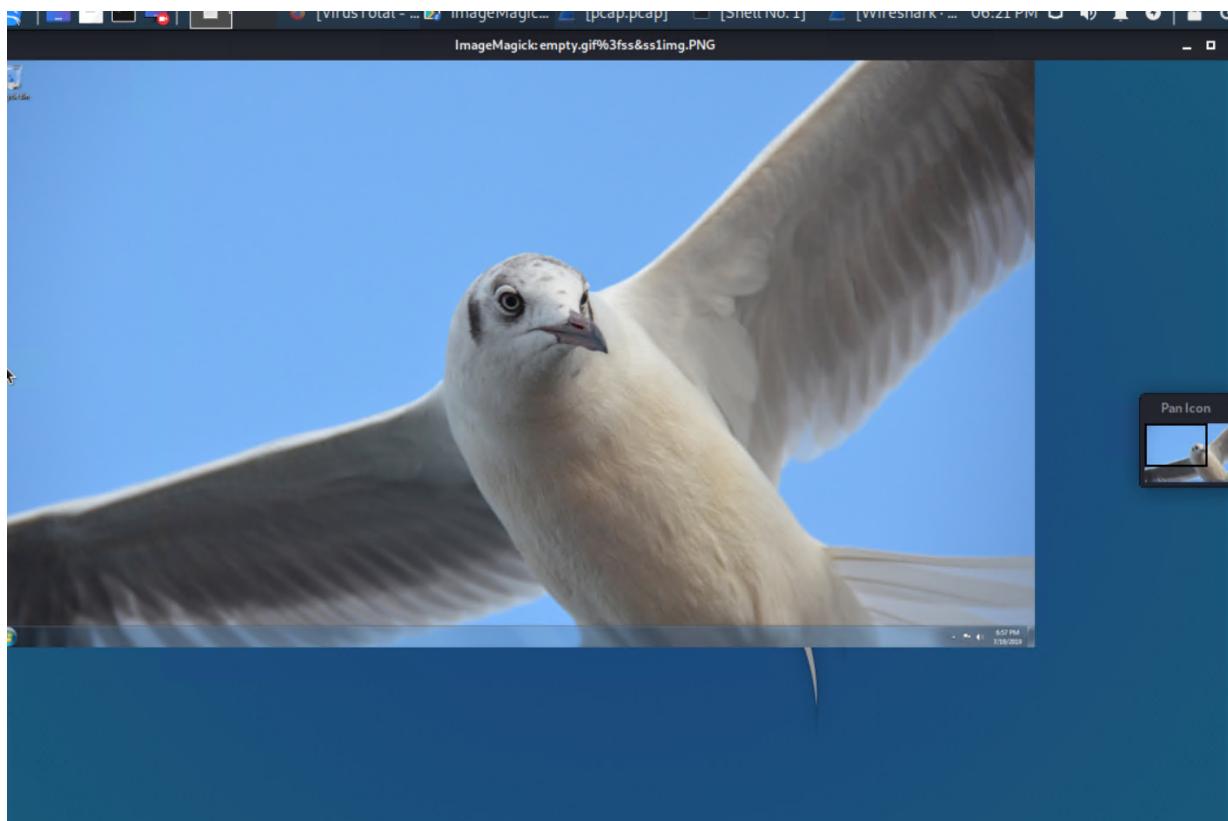
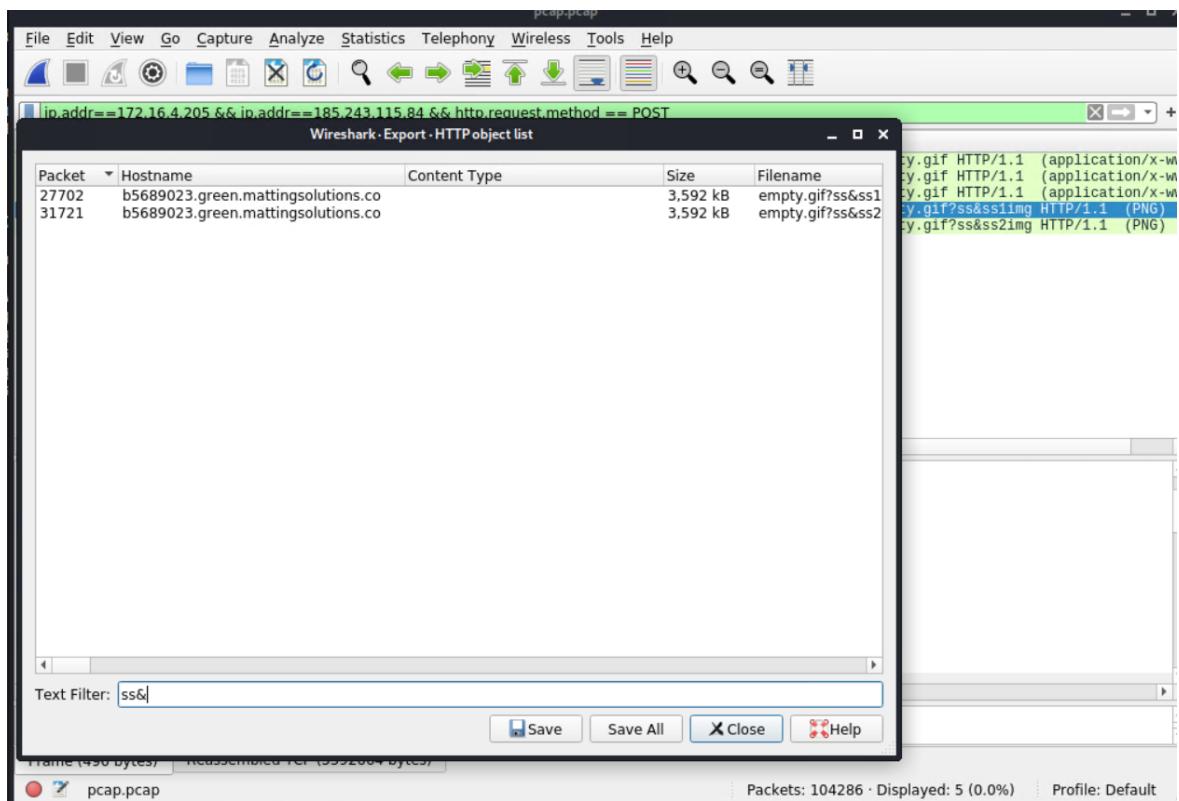


3. What is the IP address used in the actual infection traffic?

- 185.243.115.84



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.

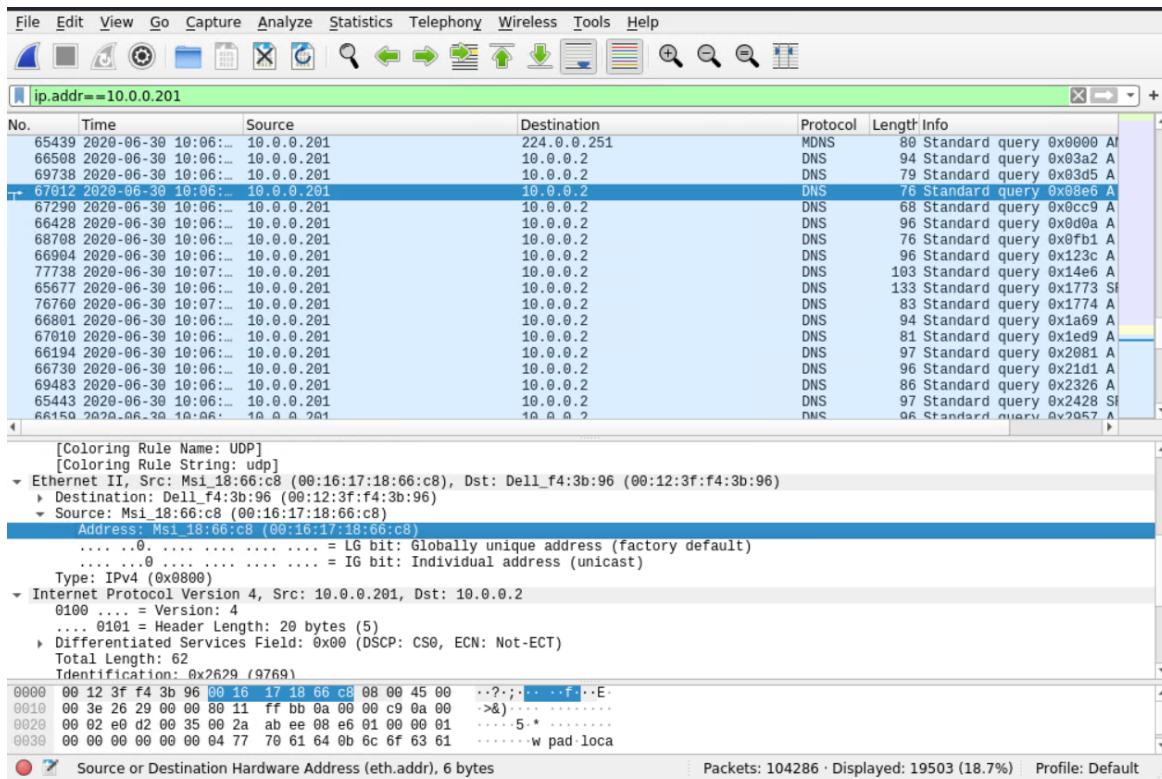
IT shared the following about the torrent activity:

- 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 NT 10.0](#)



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==10.0.0.201 && kerberos.CNameString

No.	Time	Source	Destination	Protocol	Length	Info
67046	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	BLANCO-DESKTOP.dogoftheyear.net	KRB5	237	AS-REP
65505	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	DogOfTheYear-DC.dogoftheyear.net	KRB5	301	AS-REQ
65526	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	DogOfTheYear-DC.dogoftheyear.net	KRB5	381	AS-REQ
65530	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	DogOfTheYear-DC.dogoftheyear.net	KRB5	301	AS-REQ
65544	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	DogOfTheYear-DC.dogoftheyear.net	KRB5	382	AS-REQ
65617	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	DogOfTheYear-DC.dogoftheyear.net	KRB5	301	AS-REQ
65625	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	DogOfTheYear-DC.dogoftheyear.net	KRB5	381	AS-REQ
65712	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	DogOfTheYear-DC.dogoftheyear.net	KRB5	301	AS-REQ
65725	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	DogOfTheYear-DC.dogoftheyear.net	KRB5	382	AS-REQ
66970	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	DogOfTheYear-DC.dogoftheyear.net	KRB5	302	AS-REQ
66978	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	DogOfTheYear-DC.dogoftheyear.net	KRB5	382	AS-REQ
67036	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	DogOfTheYear-DC.dogoftheyear.net	KRB5	290	AS-REQ
67044	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	DogOfTheYear-DC.dogoftheyear.net	KRB5	370	AS-REQ
65558	2020-06-30 10:06:...	DogOfTheYear-DC.dogoftheyear.net	BLANCO-DESKTOP.dogoftheyear.net	KRB5	293	TGS-REP
65639	2020-06-30 10:06:...	DogOfTheYear-DC.dogoftheyear.net	BLANCO-DESKTOP.dogoftheyear.net	KRB5	273	TGS-REP
65655	2020-06-30 10:06:...	DogOfTheYear-DC.dogoftheyear.net	BLANCO-DESKTOP.dogoftheyear.net	KRB5	114	TGS-REP
65745	2020-06-30 10:06:...	DogOfTheYear-DC.dogoftheyear.net	BLANCO-DESKTOP.dogoftheyear.net	KRB5	293	TGS-REP
65708	2020-06-30 10:06:...	DogOfTheYear-DC.dogoftheyear.net	BLANCO-DESKTOP.dogoftheyear.net	KRB5	227	TGS-REP

```

▼ as-req
  pno: 5
  msg-type: krb-as-req (10)
  ▶ padata: 1 item
    ▶ req-body
      Padding: 0
      ▶ kdc-options: 40810010
      ▶ cname
        name-type: KRB5-NT-PRINCIPAL (1)
      ▶ cname-string: 1 item
        CNameString: elmer.blanco
      realm: DOGOFTHEYEAR
      ▶ sname
        name-type: KRB5-NT-SRV-INST (2)
      ▶ sname-string: 2 items
        0070 a1 19 03 17 a0 03 02 b1 01 a1 10 30 0e 1b 0c b5 ..0....0...0...0
        0080 b6 6d 65 72 2e 62 6c 61 6e 63 6f a2 0e 1b 0c 44 1mer.bla nco...D
        0090 4f 47 4f 46 54 48 45 59 45 41 52 a3 21 30 1f a0 060FTHEY EAR!0...
        03 02 01 02 a1 18 30 16 1b 06 6b 72 62 74 67 74 .....0..krbtgt

```

CNameString (kerberos.CNameString), 12 bytes

Packets: 104286 · Displayed: 28 (0.0%) · Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==10.0.0.201 && http

No.	Time	Source	Destination	Protocol	Length	Info
69213	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	465	GET /divx1.jpg HTTP/1.1
69470	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	rcm-na.assoc-amazon.com	HTTP	885	GET /e/cm?t=publicdomain
67493	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	scripts-tnfdwtqajaq1wartzb.stac...	HTTP	427	GET /eminimalls/mm.js H
67807	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	336	GET /favicon.ico HTTP/1
67337	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	474	GET /googlevid.jpg HTTP
69167	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	500	GET /grabs/bettybooprt!
67308	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	477	GET /grabs/hdsale.png H
68779	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	cdn.globalsigncdn.com.cdn.cloud...	HTTP	313	GET /gsorganizationvals!
67328	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	469	GET /ipod.jpg HTTP/1.1
67268	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	463	GET /nshowcat.html?cate
69126	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	534	GET /nshowmovie.html?mov
67347	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	pagead46.l.doubleclick.net	HTTP	445	GET /pagead/jjs/adbygoog
67507	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	pagead46.l.doubleclick.net	HTTP	467	GET /pagead/jss/r20180709
69150	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	pagead46.l.doubleclick.net	HTTP	434	GET /pagead/show_ads.js
67330	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	468	GET /pda.jpg HTTP/1.1
67335	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	466	GET /psp.gif HTTP/1.1
67361	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	471	GET /rentme.gif HTTP/1.
68730	2020-06-30 10:06:...	BLANCO-DESKTOP.dogoftheyear.net	cdn.globalsigncdn.com.cdn.cloud	HTTP	201	GET /root1/MEMuSIRTMEY!

```

Destination: files.publicdomaintorrents.com (168.215.194.14)
Transmission Control Protocol, Src Port: 49817, Dst Port: 80, Seq: 1, Ack: 1, Len: 480
Hypertext Transfer Protocol
  ▶ GET /nshowmovie.html?movieid=513 HTTP/1.1\r\n
    ▶ [Expert Info (Chat/Sequence): GET /nshowmovie.html?movieid=513 HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /nshowmovie.html?movieid=513
      Request Version: HTTP/1.1
      Referer: http://publicdomaintorrents.info/nshowcat.html?category=animation\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
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
Accent-Encoding: gzip, deflate\r\n

```

HTTP User-Agent header (http.user_agent), 143 bytes

Packets: 104286 · Displayed: 92 (0.1%) · Profile: Default

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

pcap.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src==10.0.0.201 & ip.dst==168.215.194.14 & http.request.method ==GET

Source	Destination	Protocol	Length	Info
06-30 10:06:.. BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	434	GET /bt/announce.php?info_hash=%1d...
06-30 10:06:.. BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	589	GET /bt/btdownload.php?type=torre...
06-30 10:06:.. BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	253	GET /bt/scrape.php?info_hash=%1d%...
06-30 10:06:.. BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	465	GET /divxi.jpg HTTP/1.1
06-30 10:06:.. BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	336	GET /favicon.ico HTTP/1.1
06-30 10:06:.. BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	474	GET /googlevid.jpg HTTP/1.1
06-30 10:06:.. BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	500	GET /grabs/bettybooprythmontherese...
06-30 10:06:.. BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	477	GET /grabs/hdsale.png HTTP/1.1
06-30 10:06:.. BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	469	GET /ipod.jpg HTTP/1.1
06-30 10:06:.. BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	463	GET /nshowcat.html?category=animat...
06-30 10:06:.. BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	534	GET /nshowmovie.html?movieid=513 H...
06-30 10:06:.. BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	468	GET /pda.jpg HTTP/1.1
06-30 10:06:.. BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	468	GET /psp.gif HTTP/1.1
06-30 10:06:.. BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	471	GET /rentme.gif HTTP/1.1
06-30 10:06:.. BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	479	GET /site2/pheader.jpg HTTP/1.1
06-30 10:06:.. BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	474	GET /srssbanner.gif HTTP/1.1
06-30 10:06:.. BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	531	GET /usercomments.html?movieid=513...
06-30 10:06:.. BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	471	GET /yellow-star.gif HTTP/1.1

Destination: files.publicdomaintorrents.com (168.215.194.14)

Transmission Control Protocol, Src Port: 49834, Dst Port: 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
 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
 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
 Accent-Encoded: gzip, deflate\r\n

0010 02 3f 76 d1 40 00 80 06 0c 39 0a 00 00 c9 a8 d7 .?v@... .9.....
 0020 c2 0e c2 aa 00 50 97 b7 b1 25 75 99 6b 48 50 18P...%u kHP...
 0030 ff ff 31 06 00 00 47 45 54 20 2f 62 74 2f 62 74 .1..GE T /bt/bt
 0040 64 6f 77 6e 6c 6f 61 64 2e 70 68 70 3f 74 79 70 download .php?typ

Header checksum status (ip.checksum.status) :: Packets: 104286 · Displayed: 18 (0.0%) · Profile: Default

pcap.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

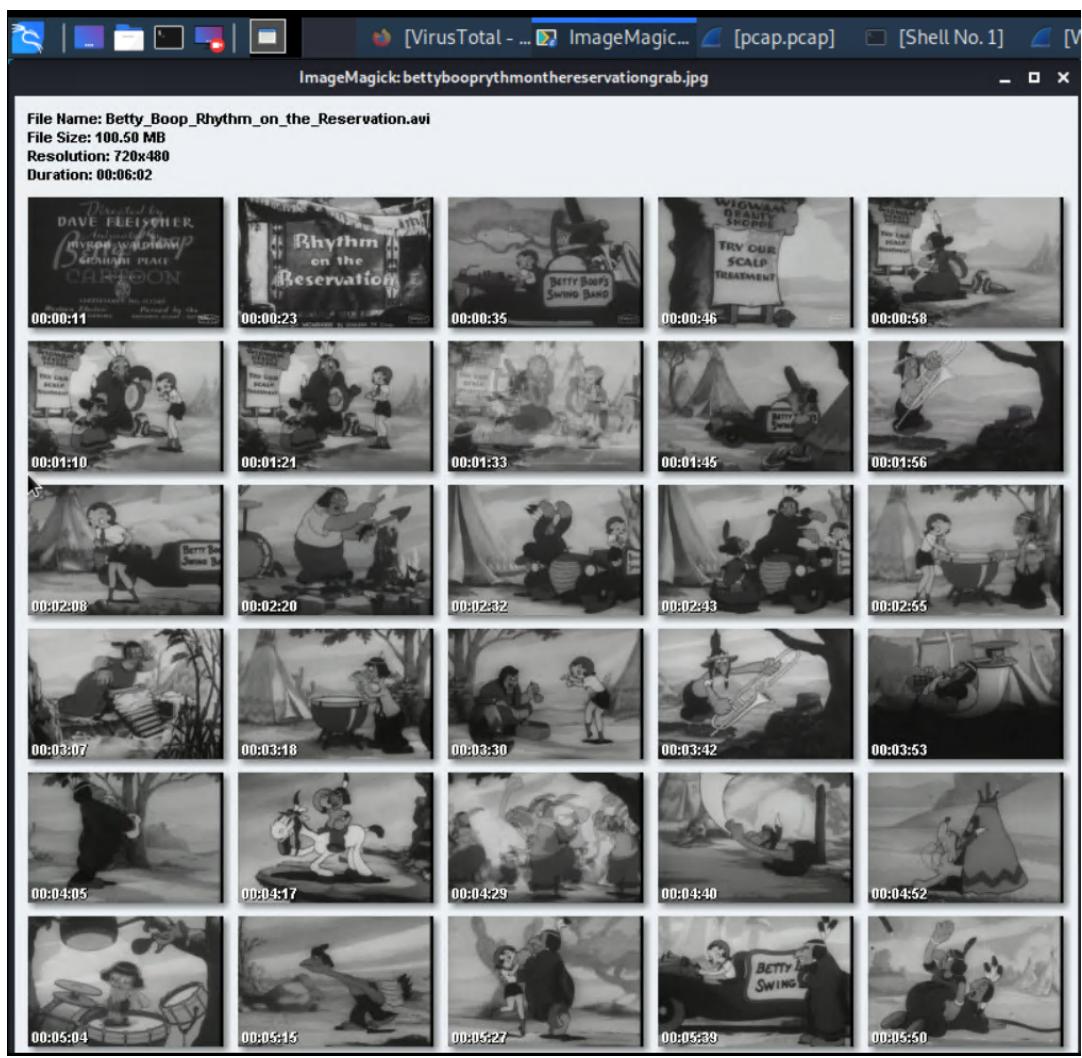
Wireshark - Export - HTTP object list

Packet	Hostname	Content Type	Size	Filename
69417	publicdomaintorrents.info	image/jpeg	152 kB	bettybooprythmonthereservationgrab.jpg
69719	www.publicdomaintorrents.com	application/x-bittorrent	8,268 bytes	btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_...

Text Filter: betty

Save Save All Close Help

0030 ff ff 31 06 00 00 47 45 54 20 2f 62 74 2f 62 74 .1..GE T /bt/bt
 0040 64 6f 77 6e 6c 6f 61 64 2e 70 68 70 3f 74 79 70 download .php?typ



Prepared by Ognen Nastoski

March 8, 2022