Network Forensics Analysis Report

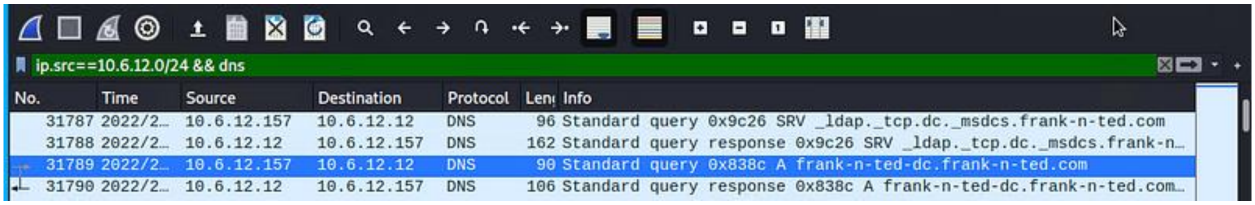
Writeup by Joseph Elbert

Email: Josephelb@comcast.net

LinkedIn: LinkedIn Profile

Time Thieves

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



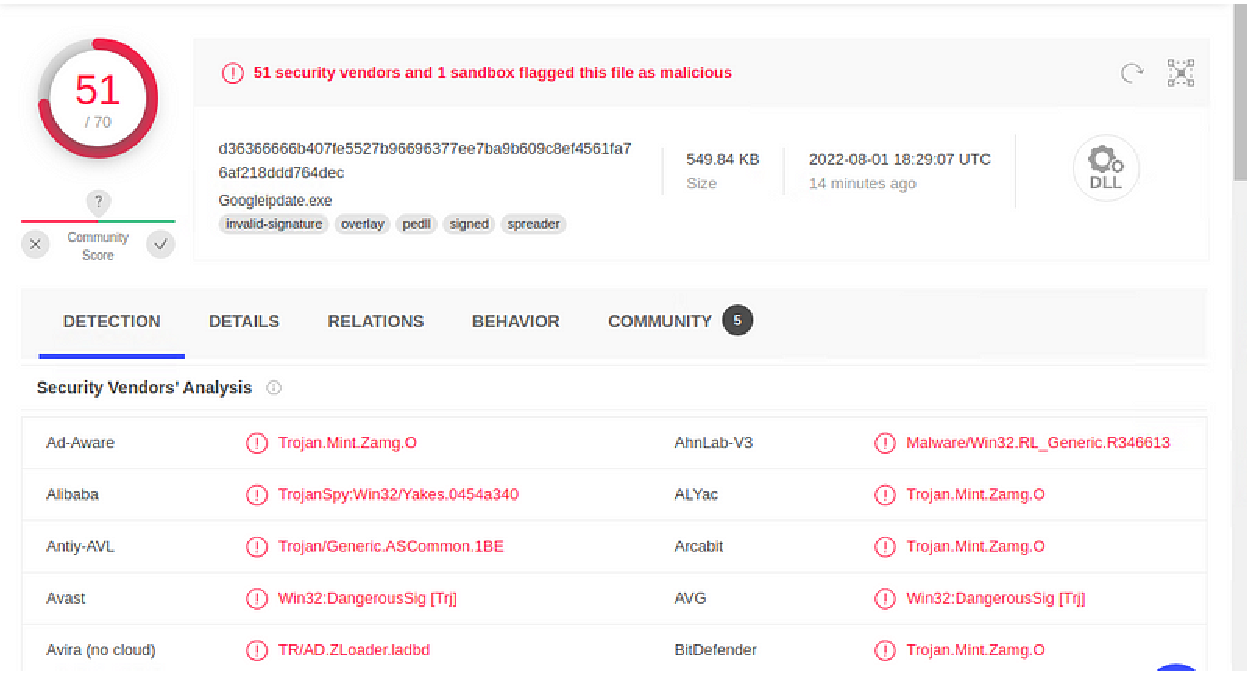
ip.src==10.6.12.0/24 && dns

```
No.    Time       Source        Destination   Protocol Len Info
 31787 2022/2…  10.6.12.157   10.6.12.12    DNS       96 Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
 31788 2022/2…  10.6.12.12    10.6.12.157   DNS      162 Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n…
 31789 2022/2…  10.6.12.157   10.6.12.12    DNS       90 Standard query 0x838c A frank-n-ted-dc.frank-n-ted.com
 31790 2022/2…  10.6.12.12    10.6.12.157   DNS      106 Standard query response 0x838c A frank-n-ted-dc.frank-n-ted.com…
```

1. What is the domain name of the users' custom site? **frank-n-ted.com**
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? **june11.dll**

Once you have found the file, export it to your Kali machine's desktop. Upload the file to VirusTotal.com.

4. What kind of malware is this classified as? **Trojan**



51 security vendors and 1 sandbox flagged this file as malicious

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Googleipdate.exe

invalid-signature overlay pedll signed spreader

549.84 KB
Size

2022-08-01 18:29:07 UTC
14 minutes ago

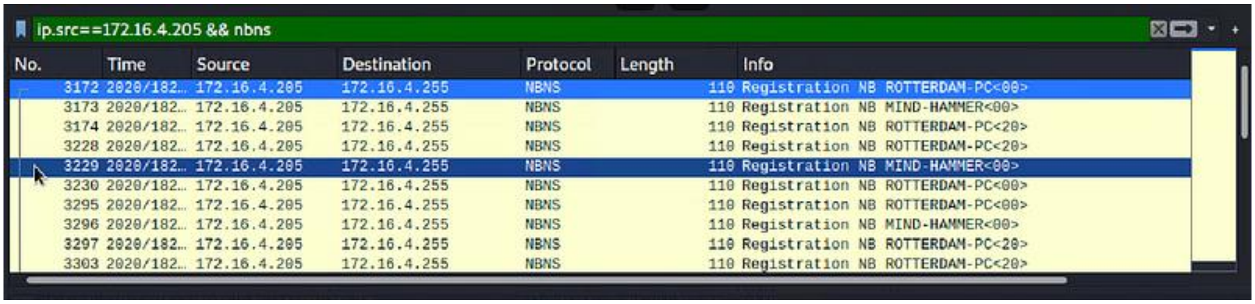
Security Vendors' Analysis

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

Vulnerable Windows Machine

1. Find the following information about the infected Windows machine:

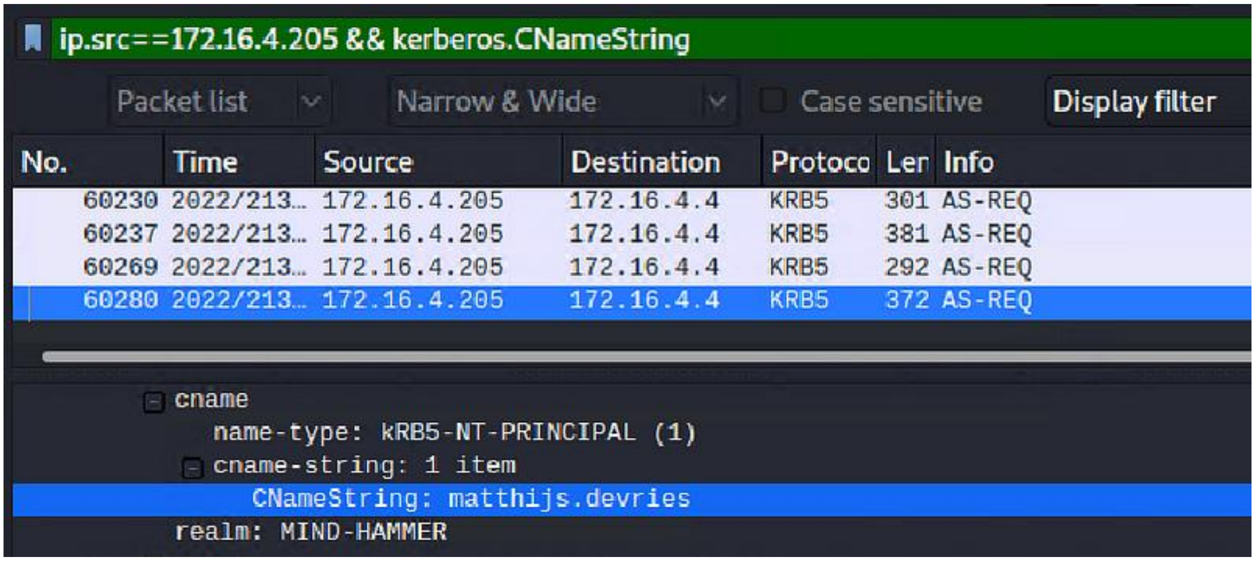
- Host name ROTTERDAM-PC
- IP address 172.16.4.4
- MAC address 00:59:07:b0:63:a4



ip.src==172.16.4.205 && nbns

No.	Time	Source	Destination	Protocol	Length	Info
3172	2020/182…	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<00>
3173	2020/182…	172.16.4.205	172.16.4.255	NBNS	110	Registration NB MIND-HAMMER<00>
3174	2020/182…	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<20>
3228	2020/182…	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<20>
3229	2020/182…	172.16.4.205	172.16.4.255	NBNS	110	Registration NB MIND-HAMMER<00>
3230	2020/182…	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<00>
3295	2020/182…	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<00>
3296	2020/182…	172.16.4.205	172.16.4.255	NBNS	110	Registration NB MIND-HAMMER<00>
3297	2020/182…	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<20>
3303	2020/182…	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<20>

2. What is the username of the Windows user whose computer is infected?
This website offered a Windows user account from Kerberos
traffic https://unit42.paloaltonetworks.com/using-wireshark-identifying-hosts-and-users/
So, the username is: **matthijs.devries**



ip.src==172.16.4.205 && kerberos.CNameString

No.	Time	Source	Destination	Protoco	Len	Info
60230	2022/213…	172.16.4.205	172.16.4.4	KRB5	301	AS-REQ
60237	2022/213…	172.16.4.205	172.16.4.4	KRB5	381	AS-REQ
60269	2022/213…	172.16.4.205	172.16.4.4	KRB5	292	AS-REQ
60280	2022/213…	172.16.4.205	172.16.4.4	KRB5	372	AS-REQ

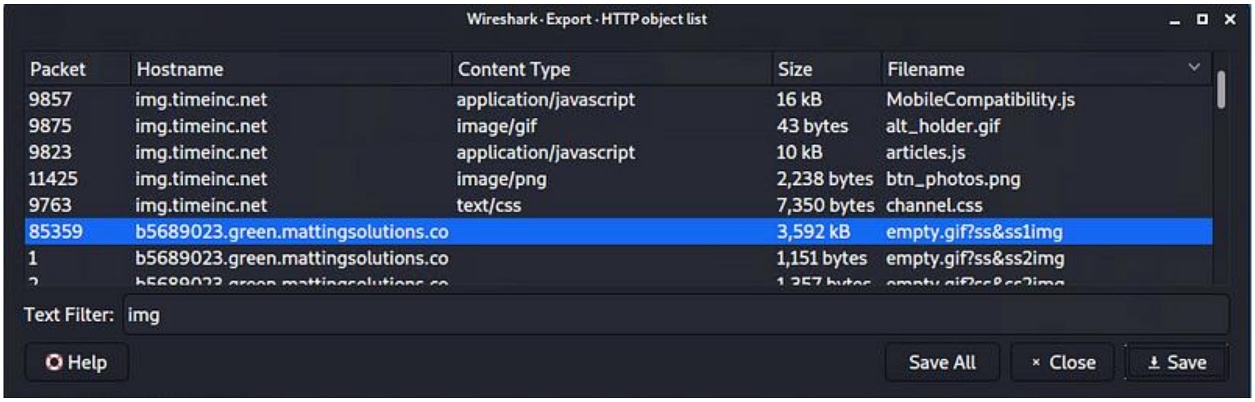
```
cname
  name-type: kRB5-NT-PRINCIPAL (1)
  cname-string: 1 item
    CNameString: matthijs.devries
realm: MIND-HAMMER
```

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

185.243.115.84

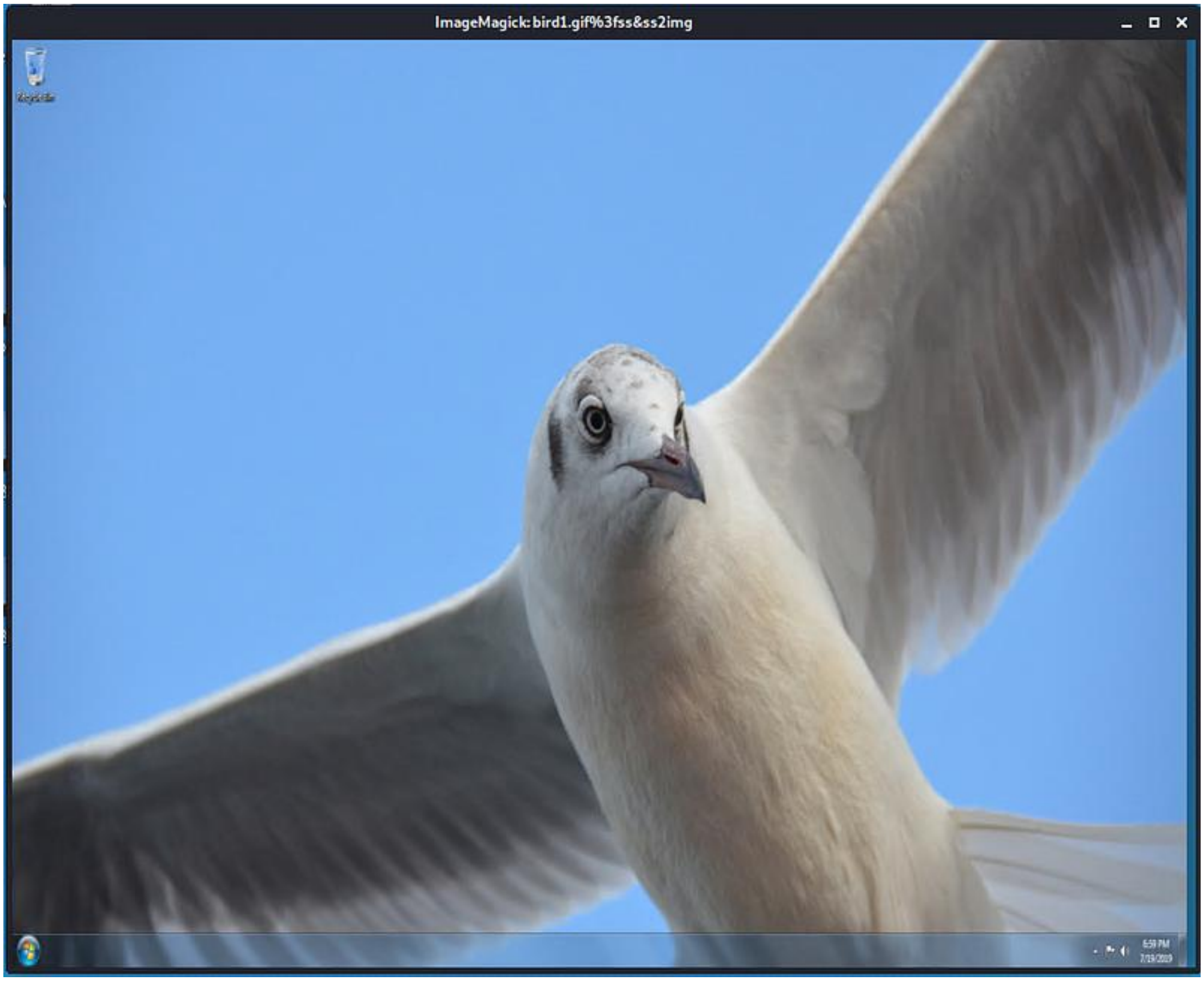
As a bonus, retrieve the desktop background of the Windows host.
Hackertarget.com gives a cheetsheet on finding an image, There were only a few files that were

worth considering because of the size of the files. This one actually looks like a screenshot of a desktop



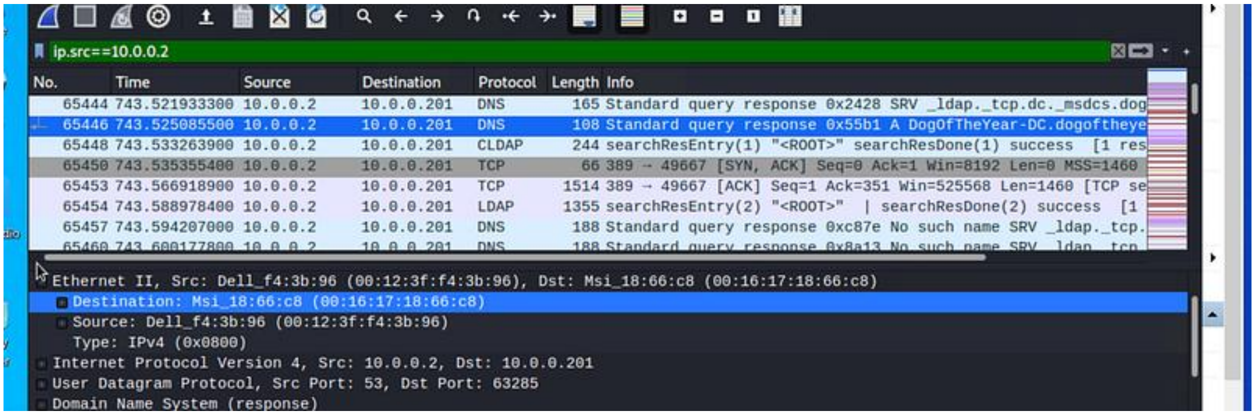
Packet	Hostname	Content Type	Size	Filename
9857	img.timeinc.net	application/javascript	16 kB	MobileCompatibility.js
9875	img.timeinc.net	image/gif	43 bytes	alt_holder.gif
9823	img.timeinc.net	application/javascript	10 kB	articles.js
11425	img.timeinc.net	image/png	2,238 bytes	btn_photos.png
9763	img.timeinc.net	text/css	7,350 bytes	channel.css
85359	b5689023.green.mattingsolutions.co		3,592 kB	empty.gif?ss&ss1img
1	b5689023.green.mattingsolutions.co		1,151 bytes	empty.gif?ss&ss2img
2	b5689023.green.mattingsolutions.co		1,357 bytes	empty.gif?ss&ss3img

Text Filter: img



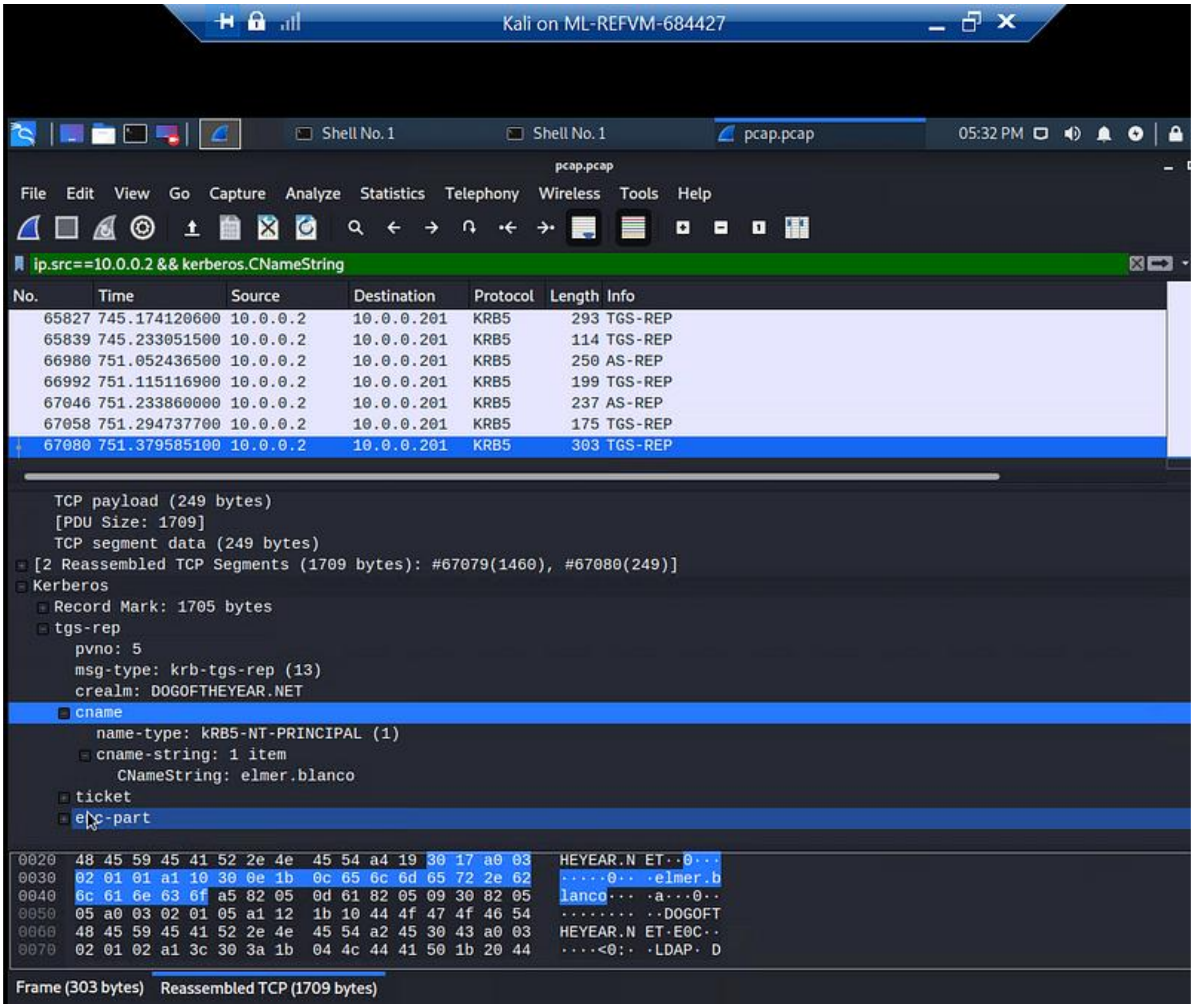
Illegal Downloads

Find the following information about the machine with IP address 10.0.0.201:
MAC address 00:16:16:18:66:c8



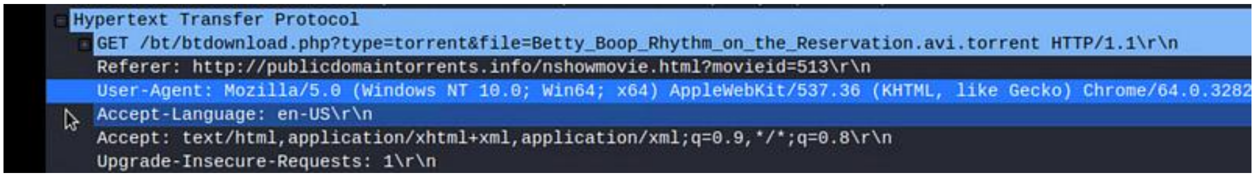
```
ip.src==10.0.0.2

No.    Time        Source      Destination  Protocol Length Info
 65444 743.521933300 10.0.0.2  10.0.0.201   DNS       165 Standard query response 0x2428 SRV _ldap._tcp.dc._msdcs.dog
 65446 743.525085500 10.0.0.2  10.0.0.201   DNS       108 Standard query response 0x55b1 A DogOfTheYear-DC.dogoftheye
 65448 743.533263900 10.0.0.2  10.0.0.201   CLDAP     244 searchResEntry(1) "<ROOT>" searchResDone(1) success  [1 res
 65450 743.535355400 10.0.0.2  10.0.0.201   TCP        66 389 → 49667 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
 65453 743.566918900 10.0.0.2  10.0.0.201   TCP      1514 389 → 49667 [ACK] Seq=1 Ack=351 Win=525568 Len=1460 [TCP se
 65454 743.588978400 10.0.0.2  10.0.0.201   LDAP     1355 searchResEntry(2) "<ROOT>"  | searchResDone(2) success  [1
 65457 743.594207000 10.0.0.2  10.0.0.201   DNS       188 Standard query response 0xc87e No such name SRV _ldap._tcp.
 65460 743.600177800 10.0.0.2  10.0.0.201   DNS       188 Standard query response 0x8a13 No such name SRV _ldap._tcp

Ethernet II, Src: Dell_f4:3b:96 (00:12:3f:f4:3b:96), Dst: Msi_18:66:c8 (00:16:17:18:66:c8)
  Destination: Msi_18:66:c8 (00:16:17:18:66:c8)
  Source: Dell_f4:3b:96 (00:12:3f:f4:3b:96)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.0.2, Dst: 10.0.0.201
User Datagram Protocol, Src Port: 53, Dst Port: 63285
Domain Name System (response)
```

Windows username elmer.blanco



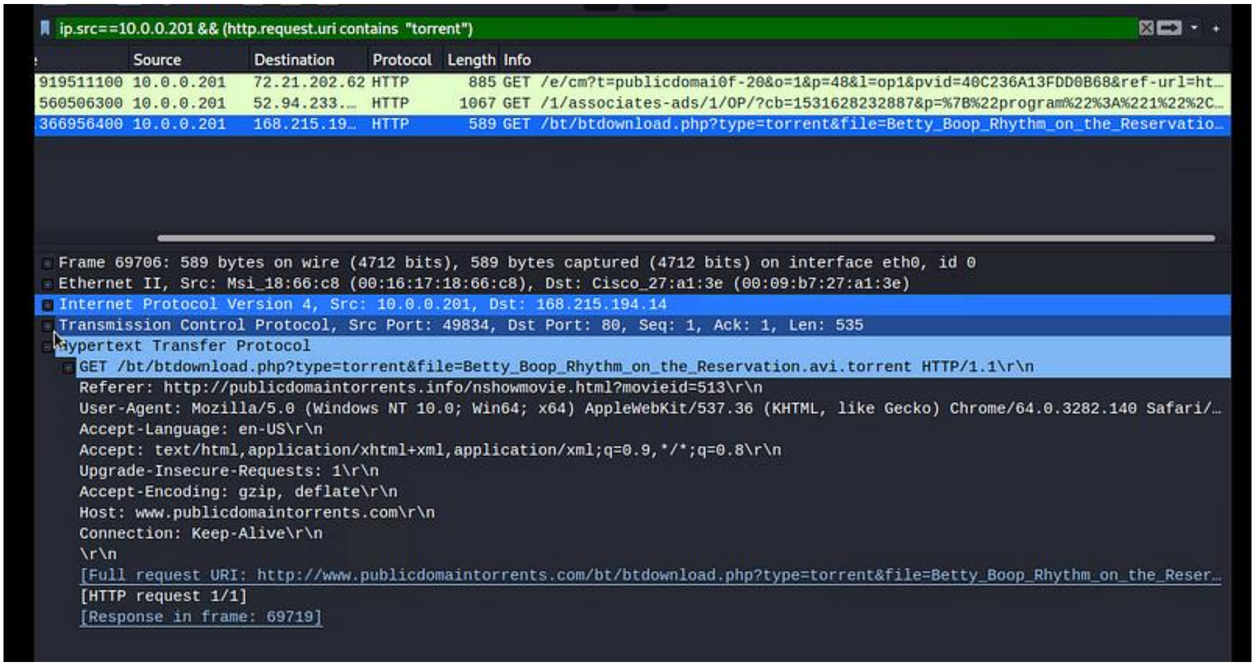
```
ip.src==10.0.0.2 && kerberos.CNameString

No.    Time          Source    Destination  Protocol Length Info
 65827 745.174120600 10.0.0.2  10.0.0.201   KRB5      293 TGS-REP
 65839 745.233051500 10.0.0.2  10.0.0.201   KRB5      114 TGS-REP
 66980 751.052436500 10.0.0.2  10.0.0.201   KRB5      250 AS-REP
 66992 751.115116900 10.0.0.2  10.0.0.201   KRB5      199 TGS-REP
 67046 751.233860000 10.0.0.2  10.0.0.201   KRB5      237 AS-REP
 67058 751.294737700 10.0.0.2  10.0.0.201   KRB5      175 TGS-REP
 67080 751.379585100 10.0.0.2  10.0.0.201   KRB5      303 TGS-REP

    TCP payload (249 bytes)
    [PDU Size: 1709]
    TCP segment data (249 bytes)
  [2 Reassembled TCP Segments (1709 bytes): #67079(1460), #67080(249)]
  Kerberos
    Record Mark: 1705 bytes
    tgs-rep
      pvno: 5
      msg-type: krb-tgs-rep (13)
      crealm: DOGOFTHEYEAR.NET
      cname
        name-type: kRB5-NT-PRINCIPAL (1)
        cname-string: 1 item
          CNameString: elmer.blanco
      ticket
      enc-part

0020  48 45 59 45 41 52 2e 4e  45 54 a4 19 30 17 a0 03   HEYEAR.N ET··0···
0030  02 01 01 a1 10 30 0e 1b  0c 65 6c 6d 65 72 2e 62   ·····0·· ·elmer.b
0040  6c 61 6e 63 6f a5 82 05  0d 61 82 05 09 30 82 05   lanco··· ·a···0··
0050  05 a0 03 02 01 05 a1 12  1b 10 44 4f 47 4f 46 54   ········ ··DOGOFT
0060  48 45 59 45 41 52 2e 4e  45 54 a2 45 30 43 a0 03   HEYEAR.N ET·E0C··
0070  02 01 02 a1 3c 30 3a 1b  04 4c 44 41 50 1b 20 44   ····<0:· ·LDAP· D

Frame (303 bytes)   Reassembled TCP (1709 bytes)
```

OS version Windows NT 10.0



```
Hypertext Transfer Protocol
  GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n
  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
  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
```

Which torrent file did the user download? **Betty_Boop_Rhythm_on_the_Reservation.avi.torrent**



```
ip.src==10.0.0.201 && (http.request.uri contains "torrent")
```

```
           Source      Destination  Protocol Length Info
919511100 10.0.0.201  72.21.202.62 HTTP      885 GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=op1&pvid=40C236A13FDD0B68&ref-url=ht…
560506300 10.0.0.201  52.94.233.…  HTTP     1067 GET /1/associates-ads/1/OP/?cb=1531628232887&p=%7B%22program%22%3A%221%22%2C…
366956400 10.0.0.201  168.215.19…  HTTP      589 GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservatio…
```

```
Frame 69706: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits) on interface eth0, id 0
Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
Internet Protocol Version 4, Src: 10.0.0.201, Dst: 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
  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/…
  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_Reser…
  [HTTP request 1/1]
  [Response in frame: 69719]
```