

Network Forensic Analysis Report

Time Thieves

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.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
 - o Once you have found the file, export it to your Kali machine's desktop.
 4. Upload the file to [VirusTotal.com](https://www.virustotal.com).
 5. What kind of malware is this classified as? Trojan.Mint.Zamg.O
-

Vulnerable Windows Machine

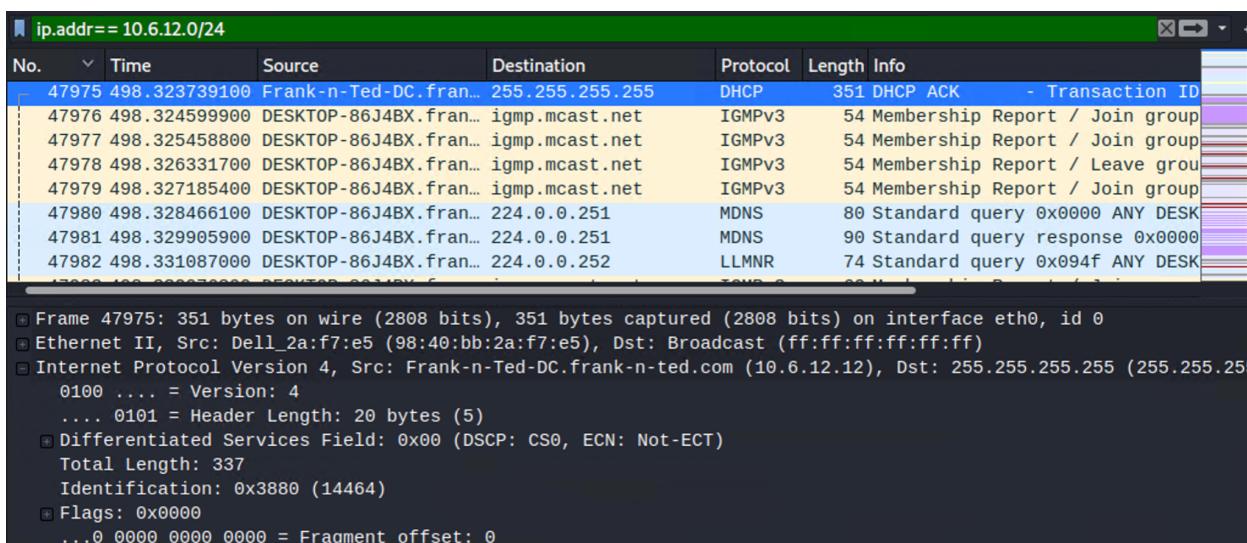
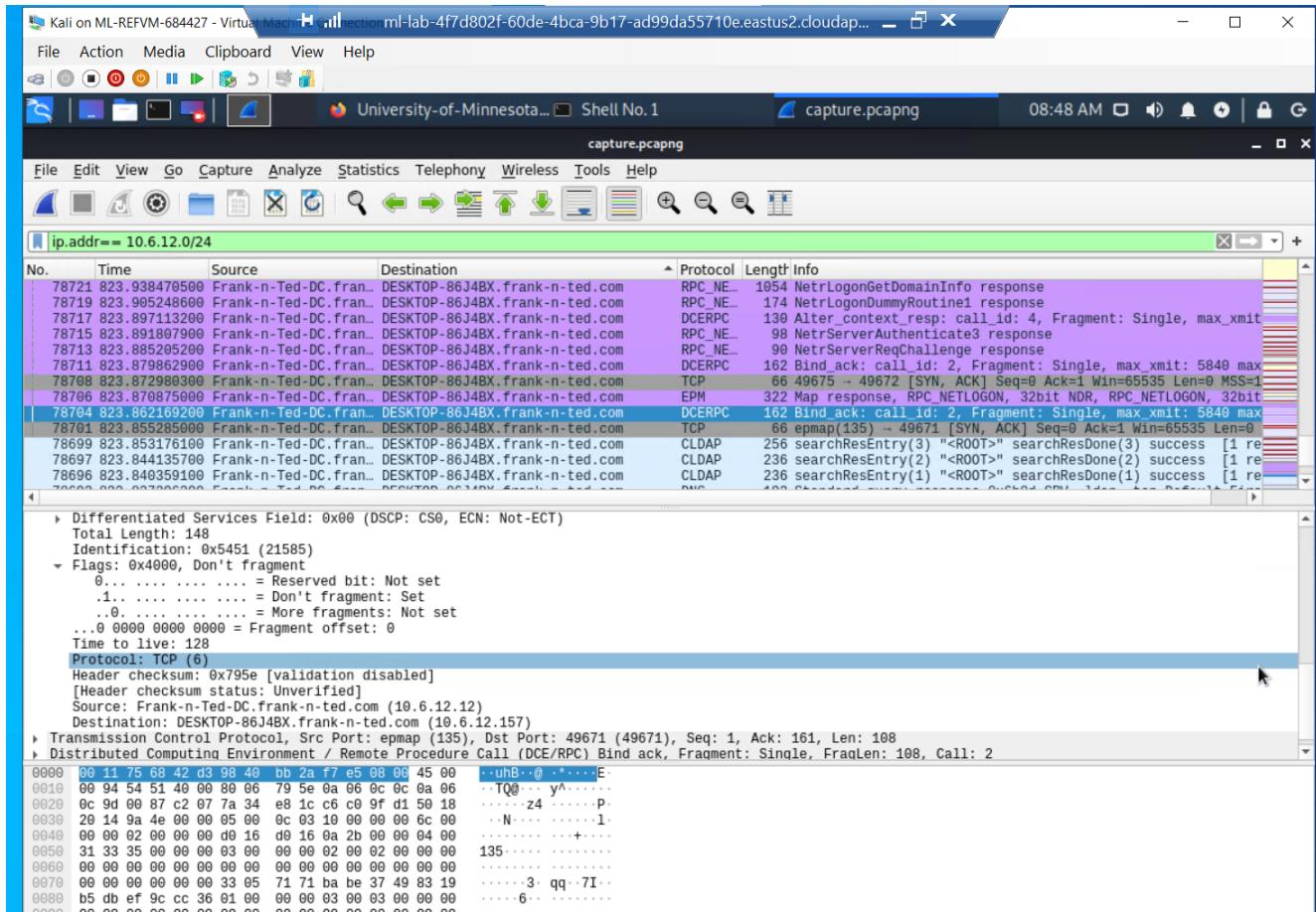
1. Find the following information about the infected Windows machine:
 - o Host name: Rotterdam-PC
 - o IP address: 172.16.4.205
 - o MAC address: 00:59:07:b0:63:a4
 2. What is the username of the Windows user whose computer is infected? matthijs.devries
 3. What is the IP address used in the actual infection traffic? 185.243.115.84
 4. As a bonus, retrieve the desktop background of the Windows host. (see screenshots section)
-

Illegal Downloads

1. Find the following information about the machine with IP address 10.0.0.201:
 - o MAC address: 00:16:17:18:66:c8
 - o Windows username: elmer.blanco
 - o OS version: Win 10 64bit
2. Which torrent file did the user download? Betty_Boop_Rhythm_on_the Reservation

Screenshots:

Time Thieves: IP Address



GET /files/june11.dll HTTP/1.1

No.	Time	Source	Destination	Protocol	Length	Info
89285	924.872987200	Frank-n-Ted-DC.fran...	LAPTOP-5WKHX9YG.frank-n-ted.com	EPM	226	Map response, DRSSUAPI, 32bit NDR
89301	924.955368300	LAPTOP-5WKHX9YG.fra...	Frank-n-Ted-DC.frank-n-ted.com	EPM	222	Map request, DRSSUAPI, 32bit NDR
89302	924.958988100	Frank-n-Ted-DC.fran...	LAPTOP-5WKHX9YG.frank-n-ted.com	EPM	226	Map response, DRSSUAPI, 32bit NDR
82280	841.302679100	LAPTOP-5WKHX9YG.fra...	205.185.125.104	HTTP	275	GET /P0btWj HTTP/1.1
82282	841.312213800	205.185.125.104	LAPTOP-5WKHX9YG.frank-n-ted.com	HTTP	542	HTTP/1.1 302 Found
82284	841.318076200	LAPTOP-5WKHX9YG.fra...	205.185.125.104	HTTP	312	GET /files/june11.dll HTTP/1.1
83059	850.878904500	205.185.125.104	LAPTOP-5WKHX9YG.frank-n-ted.com	HTTP	946	HTTP/1.1 200 OK
83358	852.585367400	LAPTOP-5WKHX9YG.fra...	snmmnkdxfhflwgthqismb.com	HTTP	713	POST /post.php HTTP/1.1
83360	852.593204600	snmmnkdxfhflwgthqism...	LAPTOP-5WKHX9YG.frank-n-ted.com	HTTP	436	HTTP/1.1 200 OK (text/html)
83367	852.618645000	LAPTOP-5WKHX9YG.fra...	snmmnkdxfhflwgthqismb.com	HTTP	749	POST /post.php HTTP/1.1
83861	858.889566900	snmmnkdxfhflwgthqism...	LAPTOP-5WKHX9YG.frank-n-ted.com	HTTP	1371	HTTP/1.1 200 OK (text/html)
83874	858.911353200	LAPTOP-5WKHX9YG.fra...	snmmnkdxfhflwgthqismb.com	HTTP	646	POST /post.php HTTP/1.1
83875	858.920699900	LAPTOP-5WKHX9YG.fra...	snmmnkdxfhflwgthqismb.com	HTTP	584	POST /post.php HTTP/1.1

Exporting the june11.dll file

File = 10.6.12.203 &...

Packet list

Packet	Hostname	Content Type	Size	Filename
83059	205.185.125.104	application/octet-stream	563 kB	june11.dll

01 = Header Length: 20 bytes (5)

91 = Header Length: 20 bytes (5)

ags: 0x018 (PSH, ACK)

nwindow size value: 65535

calculated window size: 65535

indow size scaling factor: 1

cksum: 0xb1e6 [unavailable]

hecksum Status: Unknown

gent pointer: 0

EQ/ACK analysis]

[RTT: 0.00179170]

[Bytes in flight: 0]

[Bytes sent since timestamps]

P payload (892 bytes)

Text Filter: june

Save Save All Close Help

VirusTotal:

The screenshot shows the VirusTotal analysis page for a file named `d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec`. The main summary indicates that 53 security vendors flagged the file as malicious. Below this, the file name is listed as `june11.dll`, with a size of 549.84 KB and a timestamp of 2021-06-05 03:21:09 UTC. A DLL icon is shown. The interface includes tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY. The DETECTION tab displays a list of vendor findings, such as Ad-Aware (Trojan.Mint.Zamg.O), AhnLab-V3 (Malware/Win32.RL_Generic.R346613), and AVG (Win32DangerousSig[Tr]). The COMMUNITY tab shows 2 comments.

Windows Vulnerable Machine: IP Address

The screenshot shows the Wireshark interface capturing traffic on interface `eth0`. The packet list shows several frames, with frame 4725 highlighted. The details pane below the packet list provides information about the selected frame, including its source (`Rotterdam-PC.mind-hammer.net`), destination (`172.16.4.255`), protocol (`NBNS`), length (`110` bytes), and info (`Registration NB ROTTERDAM-PC<00>`). The bottom status bar also displays the same registration information.

MAC Address:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Packet list		Narrow & Wide	Case sensitive	Regular Expression	10.6.12.203	Find Cancel
No.	Time	Source	Destination	Protocol	Length	Info
4725	70.633071600	Rotterdam-PC.mind-hammer.net	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<00>
4726	70.634831500	Rotterdam-PC.mind-hammer.net	172.16.4.255	NBNS	110	Registration NB MIND-HAMMER<00>
4727	70.636607600	Rotterdam-PC.mind-hammer.net	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<20>
4728	70.637739000	Rotterdam-PC.mind-hammer.net	224.0.0.252	LLMNR	72	Standard query 0x5e92 ANY Rotterdam-PC.mind-hammer.net
4729	70.638696800	Rotterdam-PC.mind-hammer.net	igmp.mcast.net	IGMPv3	60	Membership Report / Leave group 224.0.0.252
4730	70.639658200	Rotterdam-PC.mind-hammer.net	igmp.mcast.net	IGMPv3	60	Membership Report / Join group 224.0.0.252
4731	70.640808100	Rotterdam-PC.mind-hammer.net	224.0.0.252	LLMNR	72	Standard query 0x817a ANY Rotterdam-PC.mind-hammer.net
4732	70.641960800	Rotterdam-PC.mind-hammer.net	224.0.0.252	LLMNR	72	Standard query 0x817a ANY Rotterdam-PC.mind-hammer.net

▶ Frame 4725: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface eth0, id 0
 ▶ Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 ▶ Internet Protocol Version 4, Src: Rotterdam-PC.mind-hammer.net (172.16.4.255), Dst: 172.16.4.255 (172.16.4.255)
 ▶ User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
 ▶ NetBIOS Name Service

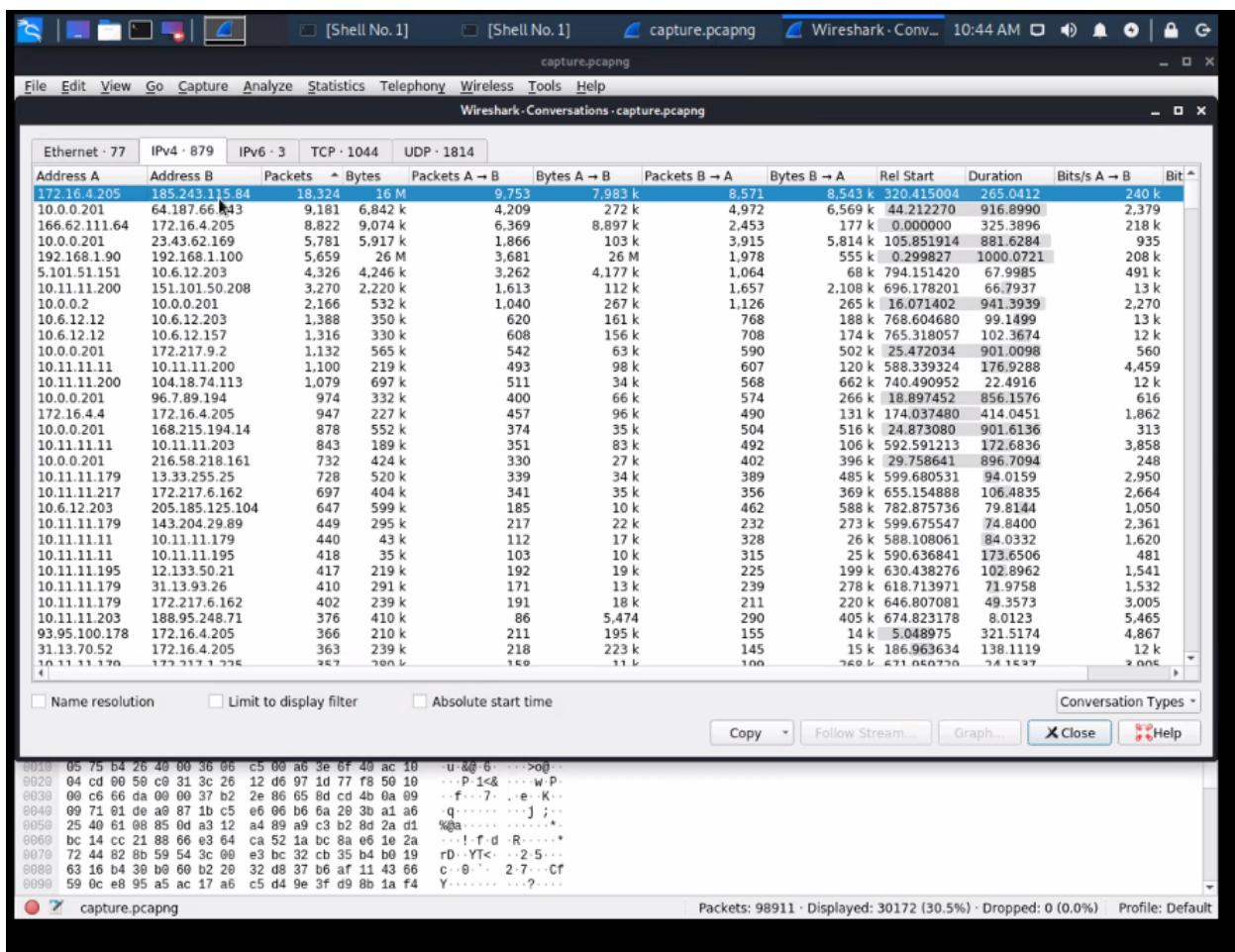
Username: matthijs.devries

ip.addr==172.16.4.205 && kerberos						
No.	Time	Source	Destination	Protocol	Length	Info
23387	232.991109700	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	195	KRB Error: KRB5KDC_ERR_BADOPTION
23468	233.265798600	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	KRB5	301	AS-REQ
23469	233.270540100	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	296	KRB Error: KRB5KDC_ERR_PREAMUTH_REQUIRED
23475	233.281434000	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	KRB5	381	AS-REQ
23477	233.308934900	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	294	AS-REP
23486	233.342393900	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	KRB5	169	TGS-REQ
23489	233.369560400	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	130	TGS-REP
23507	233.408145800	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	KRB5	292	AS-REQ
23508	233.412939900	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	300	KRB Error: KRB5KDC_ERR_PREAMUTH_REQUIRED
23514	233.423670200	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	KRB5	372	AS-REQ
23516	233.451796700	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	242	AS-REP
23524	233.483646200	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	KRB5	121	TGS-REQ
23527	233.511160400	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	150	TGS-REP

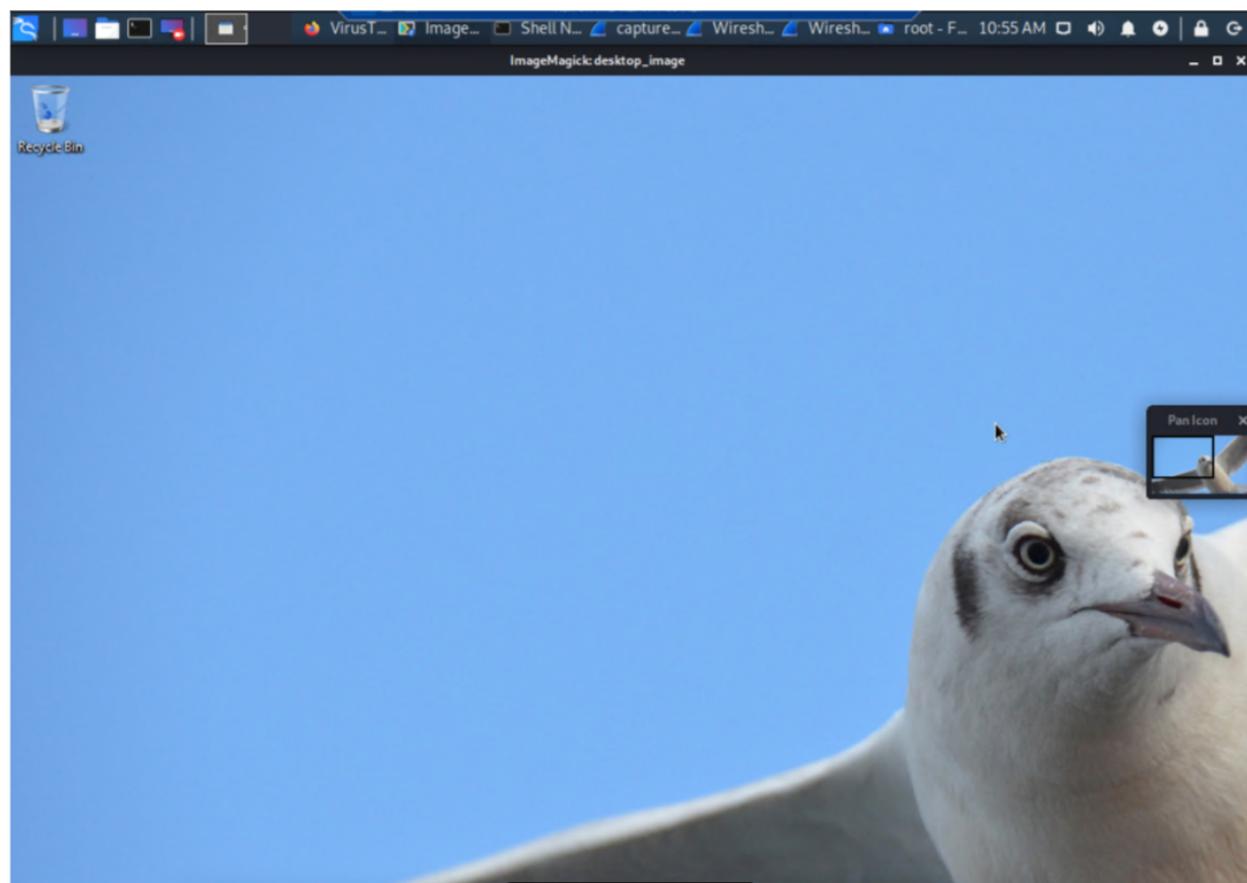
```

..0. .... = disable-transited-check: False
..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
  
```

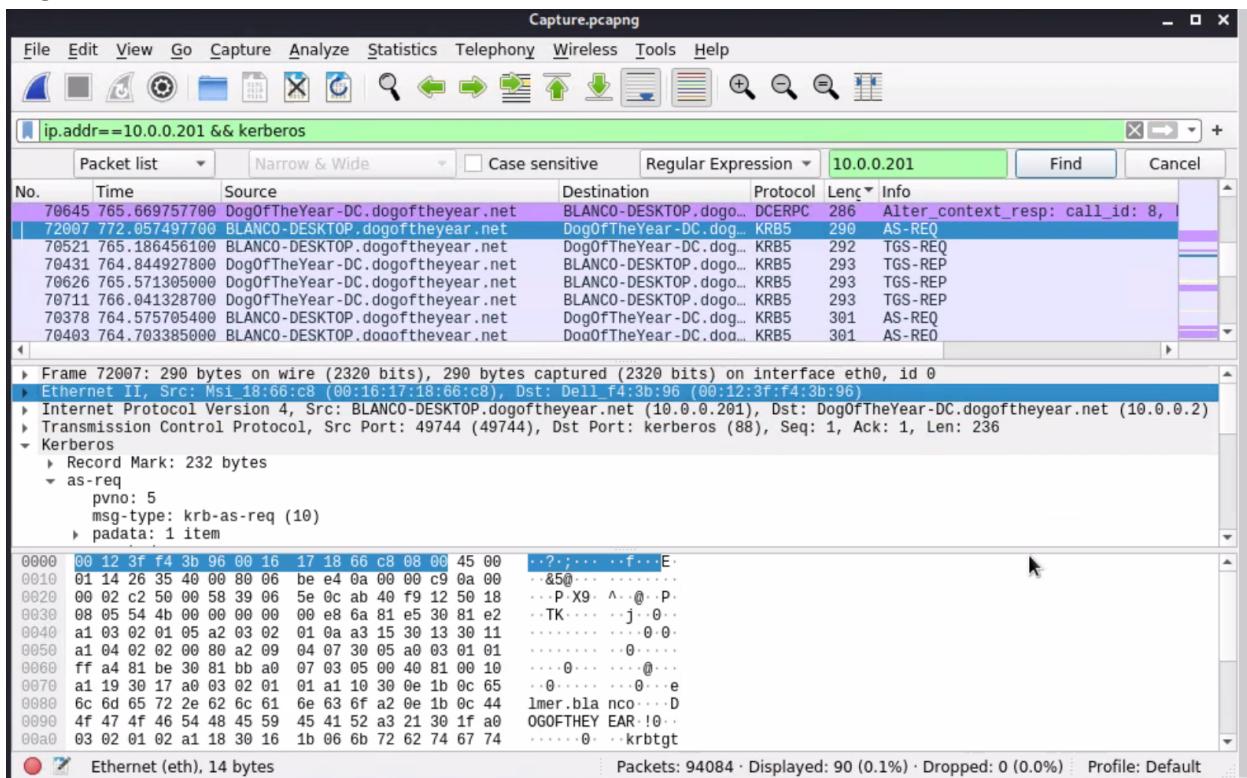
IP address used in the actual infection traffic: 185.243.115.84



Desktop background of the Windows host



Illegal Downloads:



Wireshark - Follow HTTP Stream (tcp.stream eq 830) · capture.pcapng

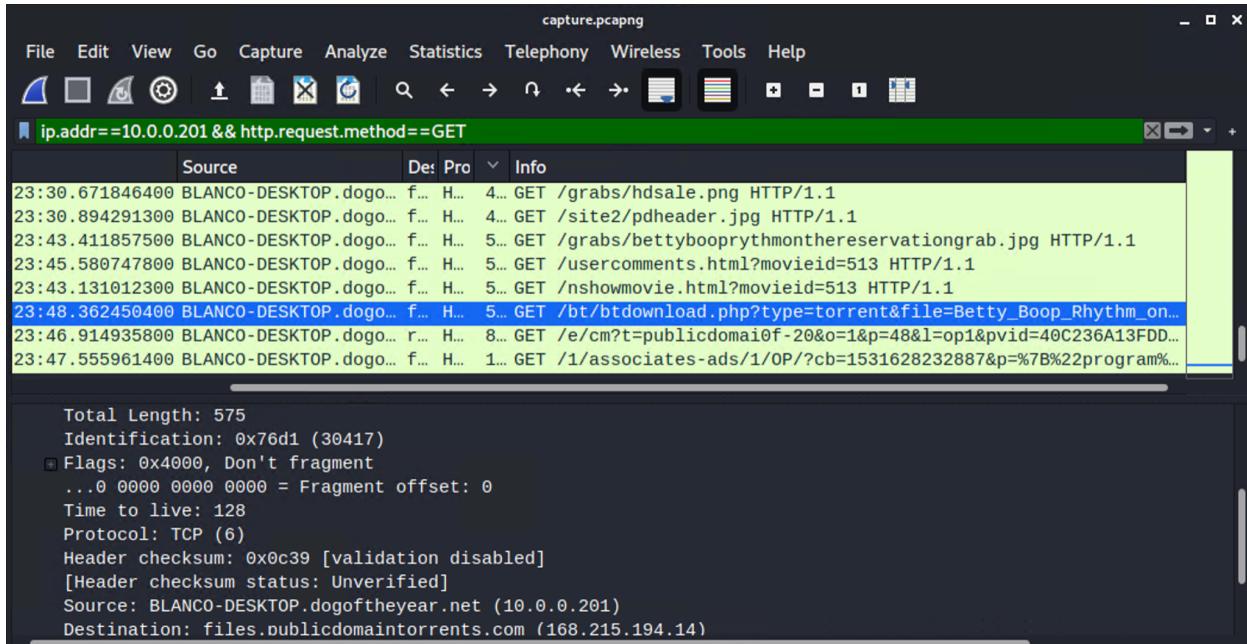
```
GET /nshowcat.html?category=animation HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Host: publicdomaintorrents.info
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Sun, 15 Jul 2018 04:17:06 GMT
Server: Apache
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
<Title>Category animation </title>
<body>
<table>
<tr valign=top><td bgcolor= "#cccccc">
<a href=index.html target=_top>HOME</a>
<a href=login.html target=_top>LOG IN</a><br>
<a href=signupform.html target=_top>SIGNUP</a>
<br>
<a href=buyemall.html><img src=grabs/hdsale.png></a>
<br>
<! --<a href=http://ads.publicdomaintorrents.com><img src=rentme.gif></a>-->
<! --<A href="http://www.chai-direct.com/Merchant2/merchant.mvc?Store_Code=TEA&AffID=7"><IMG SRC="http://www.chai-direct.com/Merchant2/graphics/
```

Packet 60829. 3 client pkts, 3 server pkts, 5 turns. Click to select.

Entire conversation (28 kB) Show and save data as ASCII



ip.addr==10.0.0.201 & kerberos

Packet list

No.	Time	Source	Destination	Protocol	Len	Info
59002	2021-06-05 15:23:22.172258600	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dog...	DCERPC	286	Alter_context_...
59169	2021-06-05 15:23:22.797985300	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dog...	DCERPC	286	Alter_context_...
60509	2021-06-05 15:23:29.185736300	BLANCO-DESKTOP.dog...	DogOfTheYear-DC.dog...	KRB5	290	AS-REQ
59045	2021-06-05 15:23:22.314685100	BLANCO-DESKTOP.dog...	DogOfTheYear-DC.dog...	KRB5	292	TGS-REQ
58967	2021-06-05 15:23:21.973181900	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dog...	KRB5	293	TGS-REP
59150	2021-06-05 15:23:22.699546800	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dog...	KRB5	293	TGS-REP
59241	2021-06-05 15:23:23.169577800	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dog...	KRB5	293	TGS-REP
58904	2021-06-05 15:23:21.703939200	BLANCO-DESKTOP.dog...	DogOfTheYear-DC.dog...	KRB5	301	AS-REQ

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

Torrent file: Betty_Boop_Rhythm_on_the Reservation

