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`
    - Once you have found the file, export it to your Kali machine's desktop.
4. Upload the file to VirusTotal.com.
5. What kind of malware is this classified as? Trojan.Mint.Zamg.O

Vulnerable Windows Machine

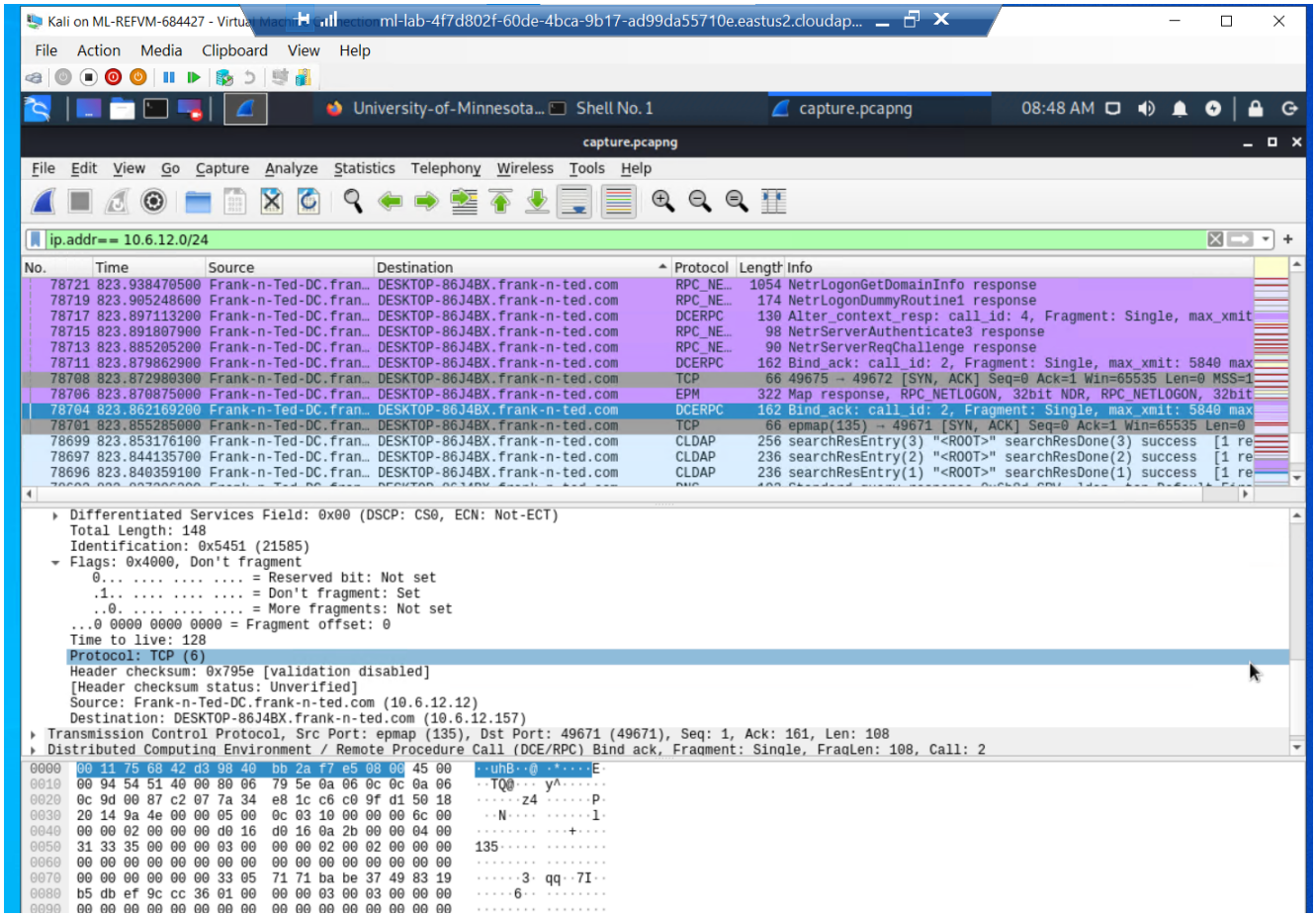
1. Find the following information about the infected Windows machine:
    - Host name: Rotterdam-PC
    - IP address: 172.16.4.205
    - MAC address: 00:59:07:b0:63:a4
2. What is the username of the Windows user whose computer is infected? matthijs.devries
3. What is the IP address used in the actual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

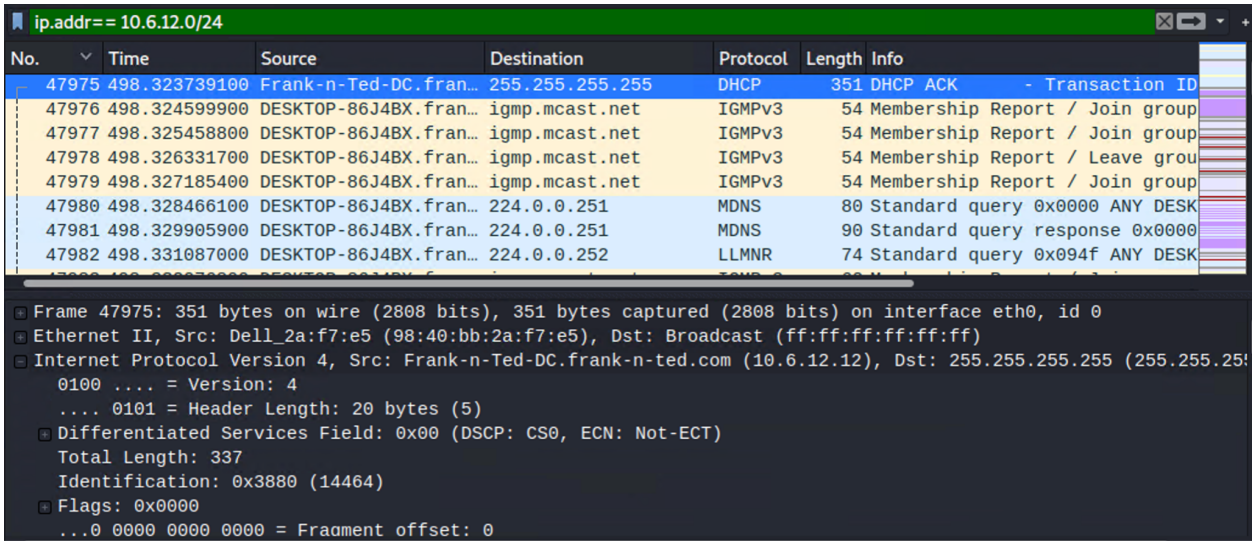
Illegal Downloads

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: Win 10 64bit
2. Which torrent file did the user download? Betty_Boop_Rhythm_on_the Reservation

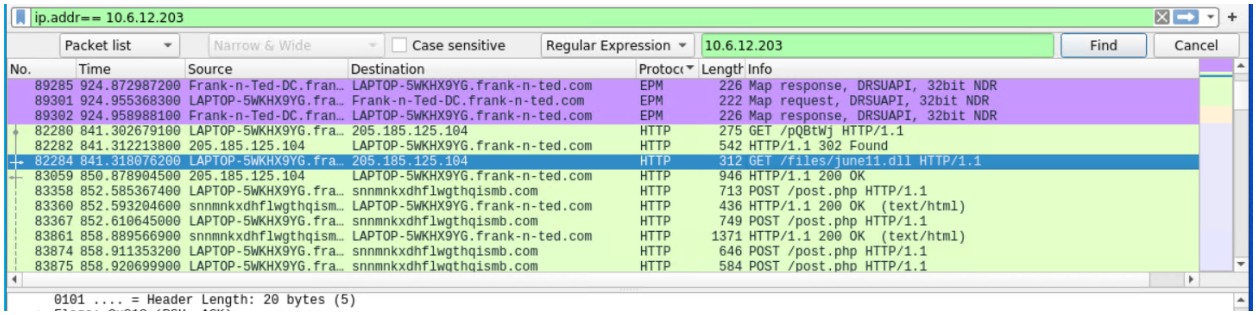
Screenshots:

Time Thieves: IP Address

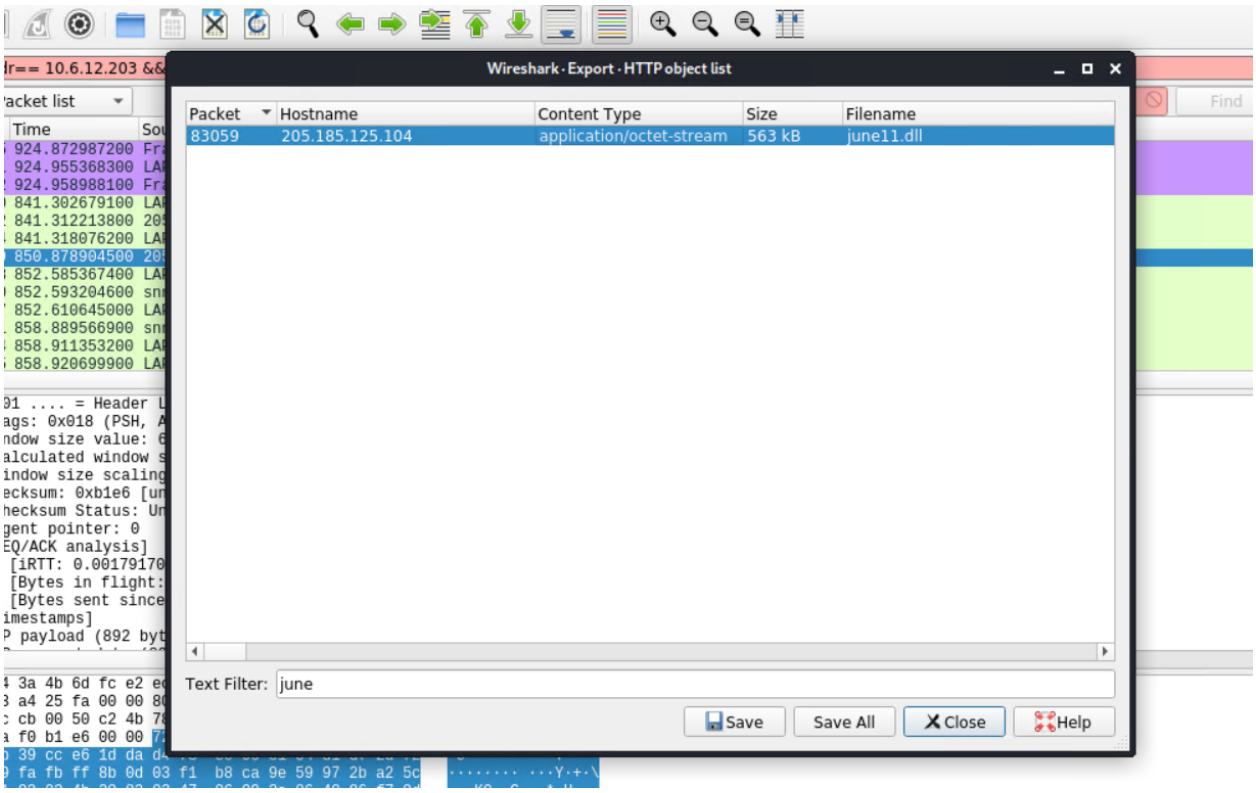




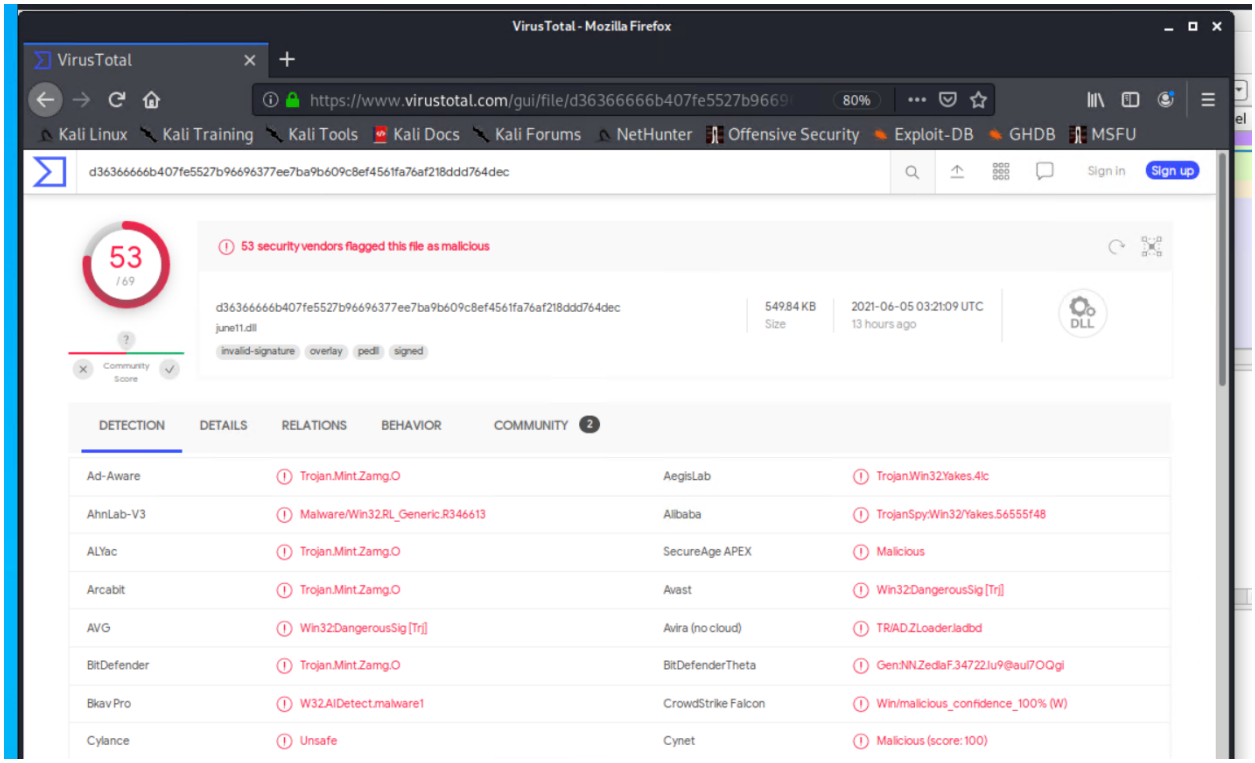
GET /files/june11.dll HTTP/1.1



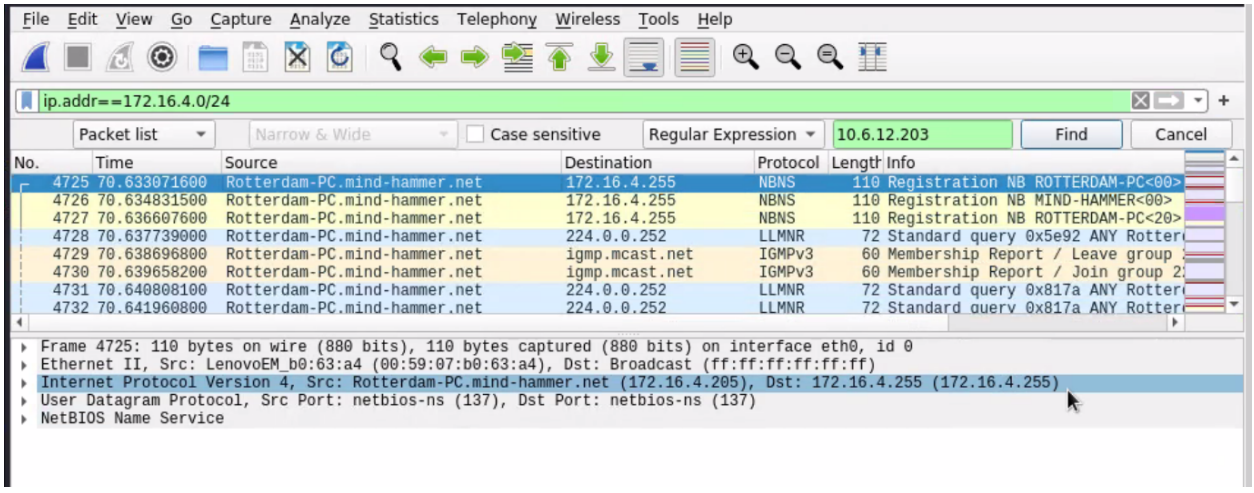
Exporting the june11.dll file



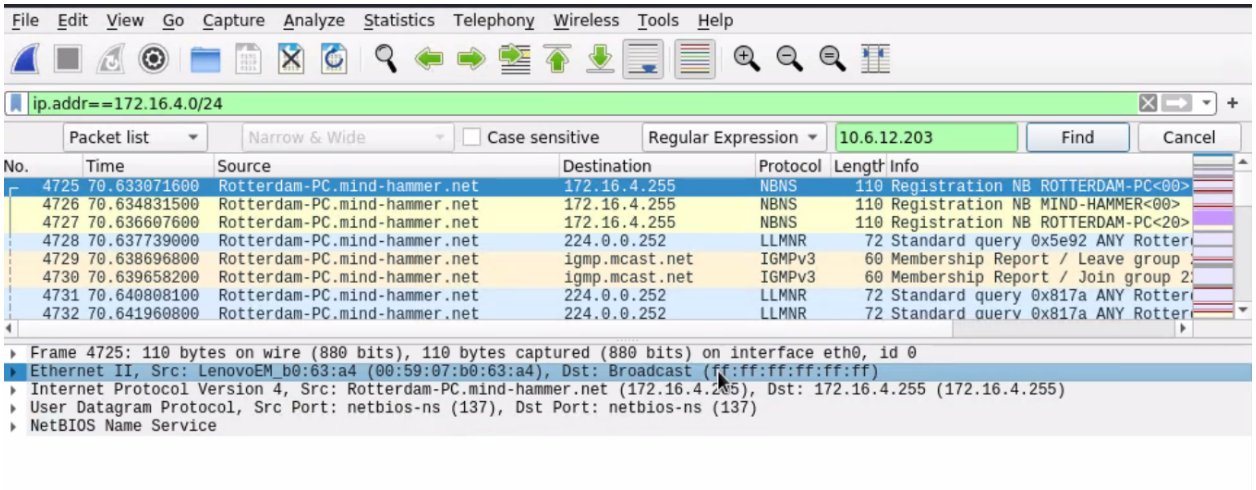
VirusTotal:



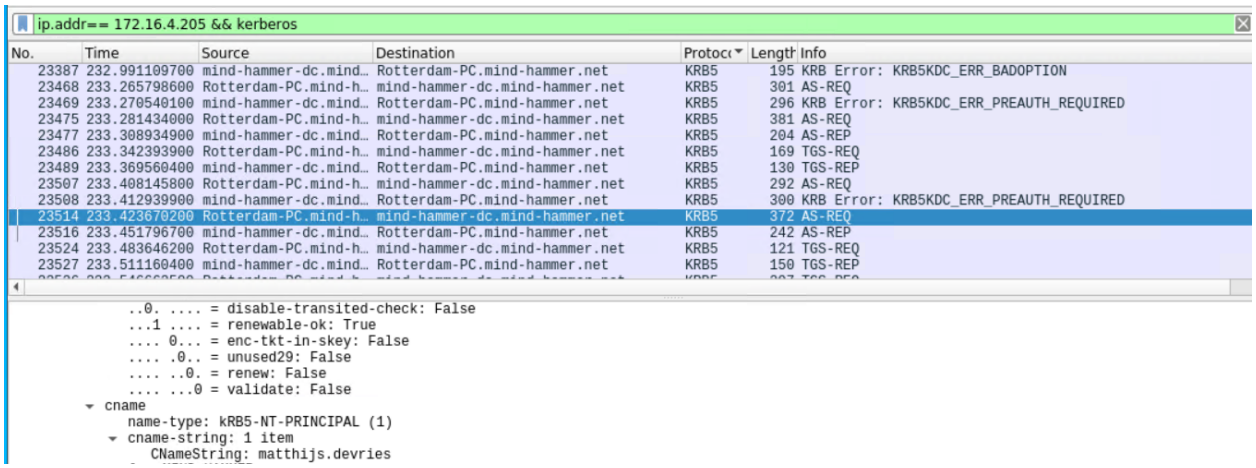
Windows Vulnerable Machine: IP Address



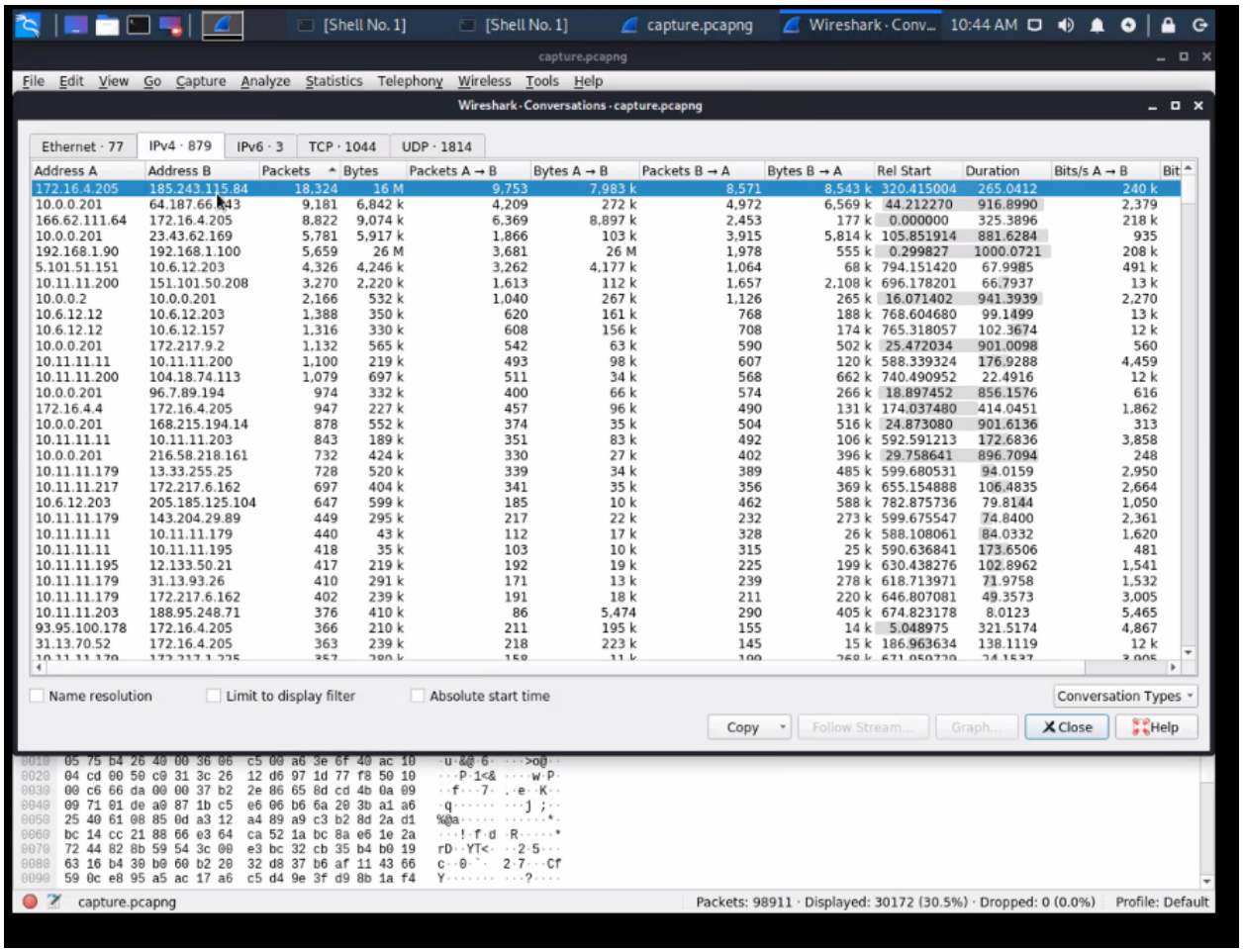
MAC Address:



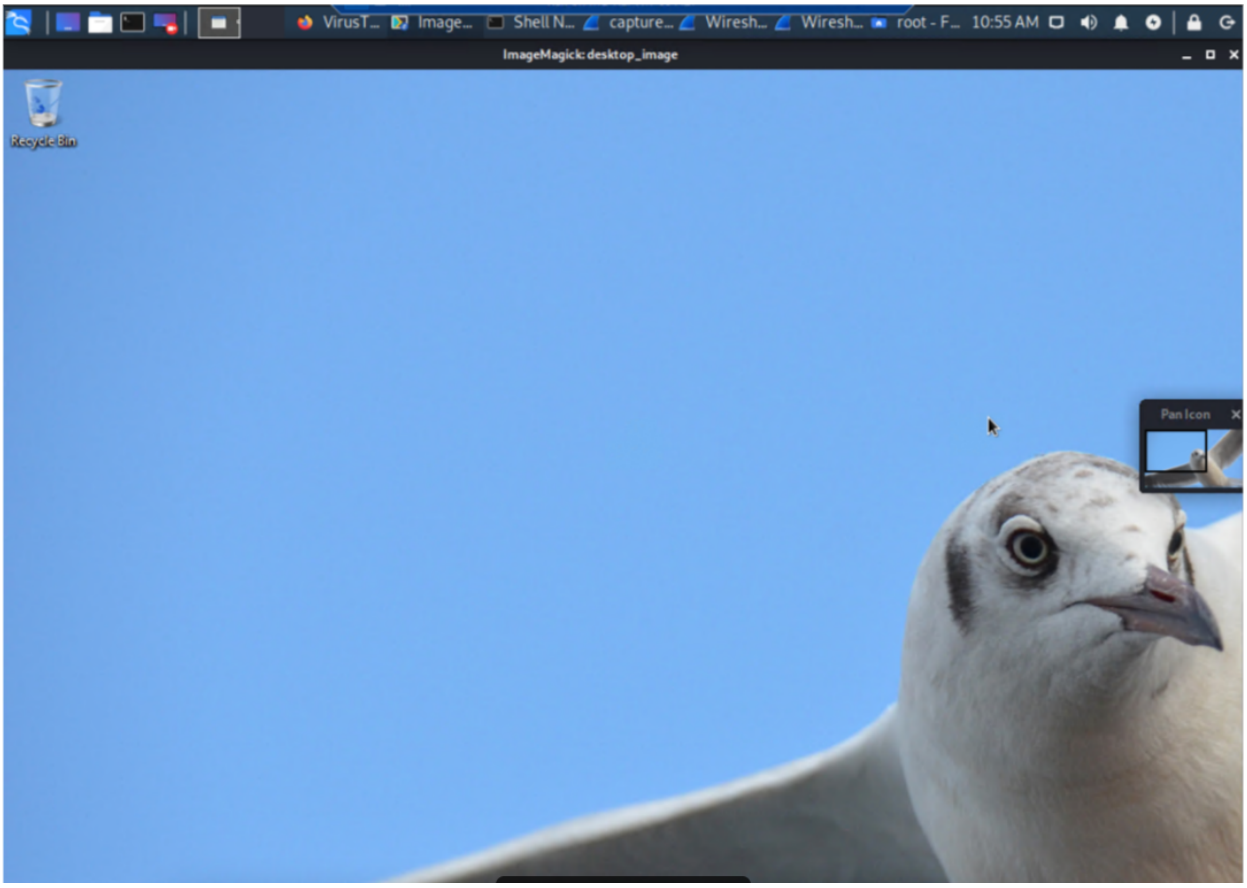
Username: matthijs.devries



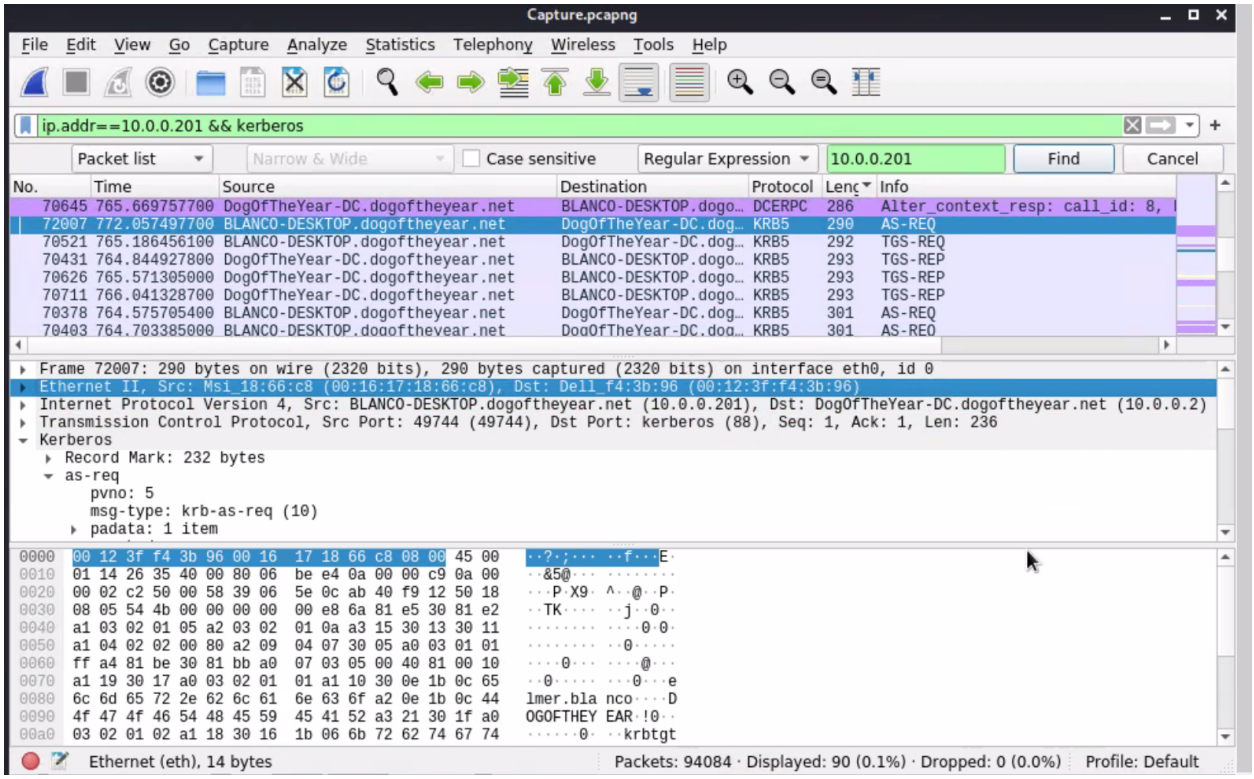
IP address used in the actual infection traffic: 185.243.115.84

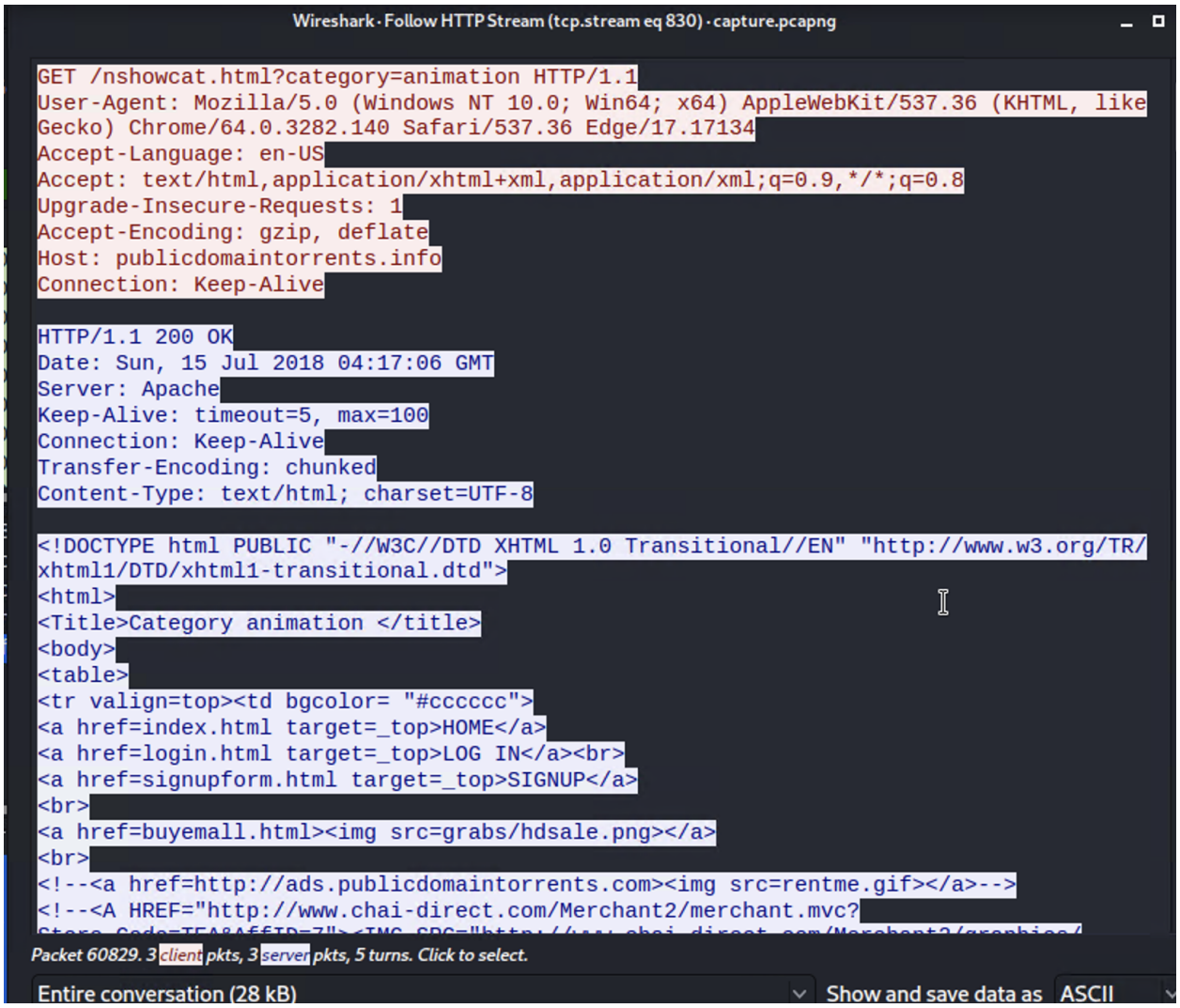


Desktop background of the Windows host



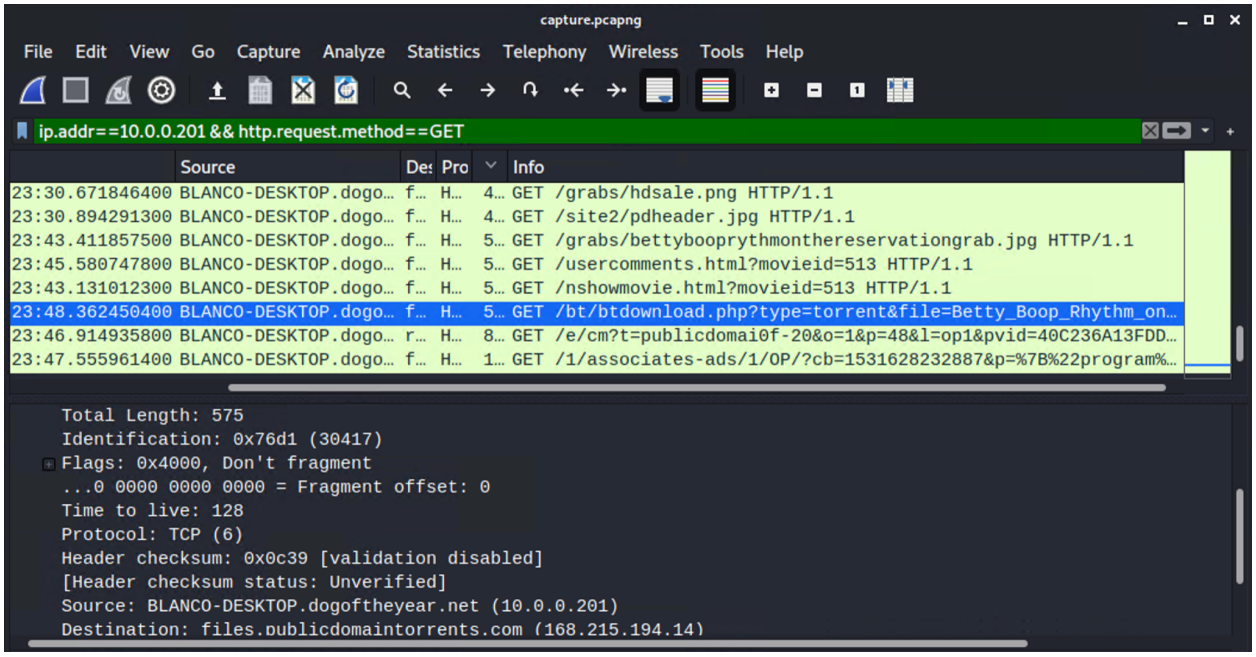
Illegal Downloads:

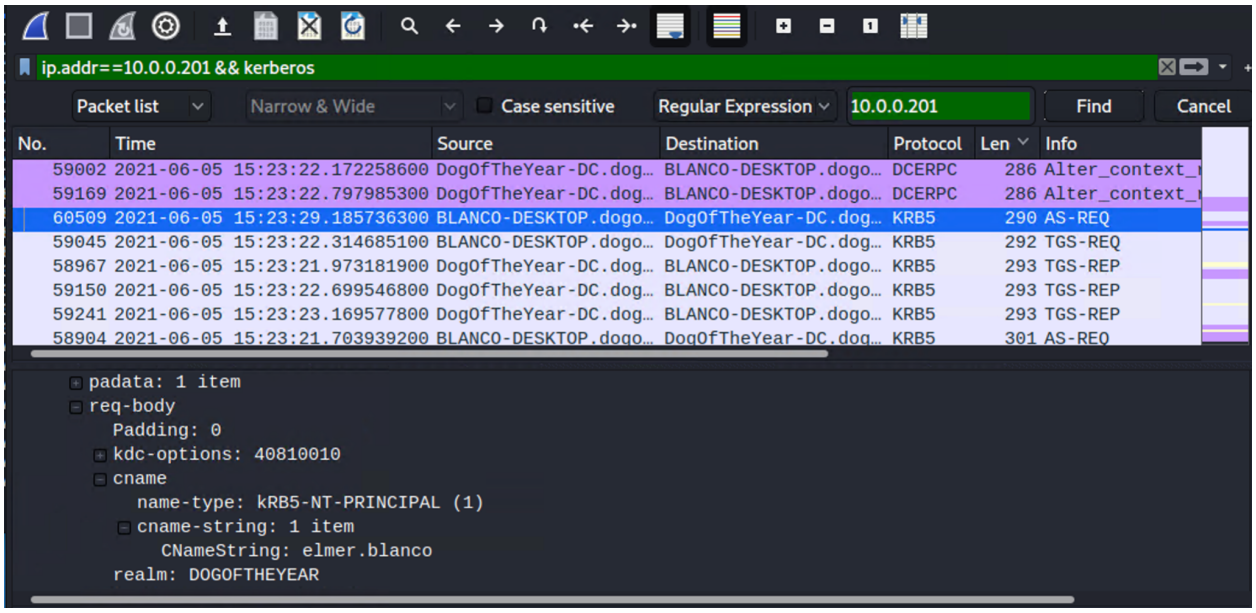



Wireshark · Follow HTTP Stream (tcp.stream eq 830) · capture.pcapng
GET /nshowcat.html?category=animation HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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">
HOME
LOG IN
SIGNUP

<img src=grabs/hdsale.png>

<!--<img src=rentme.gif>-->
<!--<A HREF="http://www.chai-direct.com/Merchant2/merchant.mvc?
Packet 60829. 3 client pkts, 3 server pkts, 5 turns. Click to select.
Entire conversation (28 kB)
Show and save data as
ASCII


capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==10.0.0.201 && http.request.method==GET
Source Des Pro Info
23:30.671846400 BLANCO-DESKTOP.dogo… f… H… 4… GET /grabs/hdsale.png HTTP/1.1
23:30.894291300 BLANCO-DESKTOP.dogo… f… H… 4… GET /site2/pdheader.jpg HTTP/1.1
23:43.411857500 BLANCO-DESKTOP.dogo… f… H… 5… GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1
23:45.580747800 BLANCO-DESKTOP.dogo… f… H… 5… GET /usercomments.html?movieid=513 HTTP/1.1
23:43.131012300 BLANCO-DESKTOP.dogo… f… H… 5… GET /nshowmovie.html?movieid=513 HTTP/1.1
23:48.362450400 BLANCO-DESKTOP.dogo… f… H… 5… GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on…
23:46.914935800 BLANCO-DESKTOP.dogo… r… H… 8… GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=op1&pvid=40C236A13FDD…
23:47.555961400 BLANCO-DESKTOP.dogo… f… H… 1… GET /1/associates-ads/1/OP/?cb=1531628232887&p=%7B%22program%…
Total Length: 575
Identification: 0x76d1 (30417)
Flags: 0x4000, Don't fragment
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x0c39 [validation disabled]
[Header checksum status: Unverified]
Source: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201)
Destination: files.publicdomaintorrents.com (168.215.194.14)


ip.addr==10.0.0.201 && kerberos
Packet list Narrow & Wide Case sensitive Regular Expression 10.0.0.201 Find Cancel
No. Time Source Destination Protocol Len Info
59002 2021-06-05 15:23:22.172258600 DogOfTheYear-DC.dog… BLANCO-DESKTOP.dogo… DCERPC 286 Alter_context_
59169 2021-06-05 15:23:22.797985300 DogOfTheYear-DC.dog… BLANCO-DESKTOP.dogo… DCERPC 286 Alter_context_
60509 2021-06-05 15:23:29.185736300 BLANCO-DESKTOP.dogo… DogOfTheYear-DC.dog… KRB5 290 AS-REQ
59045 2021-06-05 15:23:22.314685100 BLANCO-DESKTOP.dogo… DogOfTheYear-DC.dog… KRB5 292 TGS-REQ
58967 2021-06-05 15:23:21.973181900 DogOfTheYear-DC.dog… BLANCO-DESKTOP.dogo… KRB5 293 TGS-REP
59150 2021-06-05 15:23:22.699546800 DogOfTheYear-DC.dog… BLANCO-DESKTOP.dogo… KRB5 293 TGS-REP
59241 2021-06-05 15:23:23.169577800 DogOfTheYear-DC.dog… BLANCO-DESKTOP.dogo… KRB5 293 TGS-REP
58904 2021-06-05 15:23:21.703939200 BLANCO-DESKTOP.dogo… 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