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:

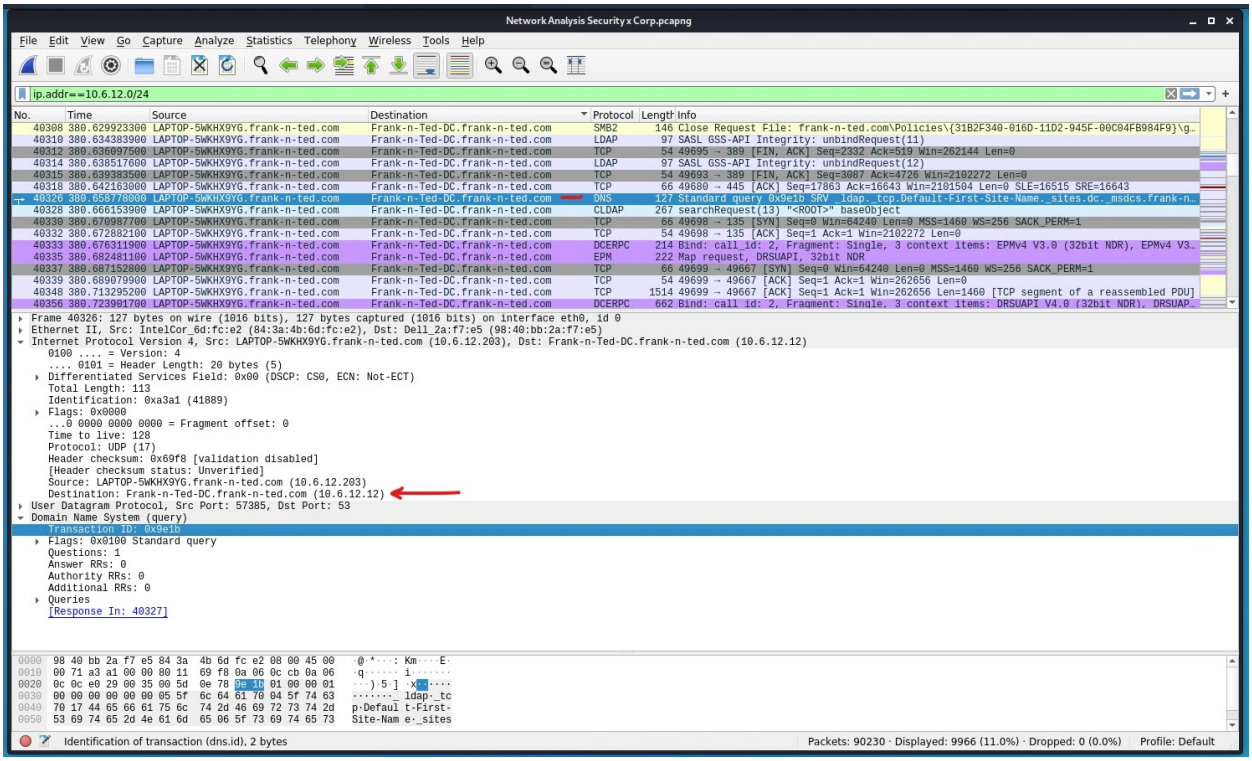
- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.
- Their IP addresses are somewhere in the range 10.6.12.0/24.

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

1. **What is the domain name of the users' custom site?**

   Filter: ip.addr==10.6.12.0/24

   "Frank-n-Ted-DC.frank-n-ted.com" was found to be the domain of the users' custom website.



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

   Filter: ip.addr==10.6.12.0/24

   "10.6.12.12" is the IP address of the Domain Controller of the AD network.

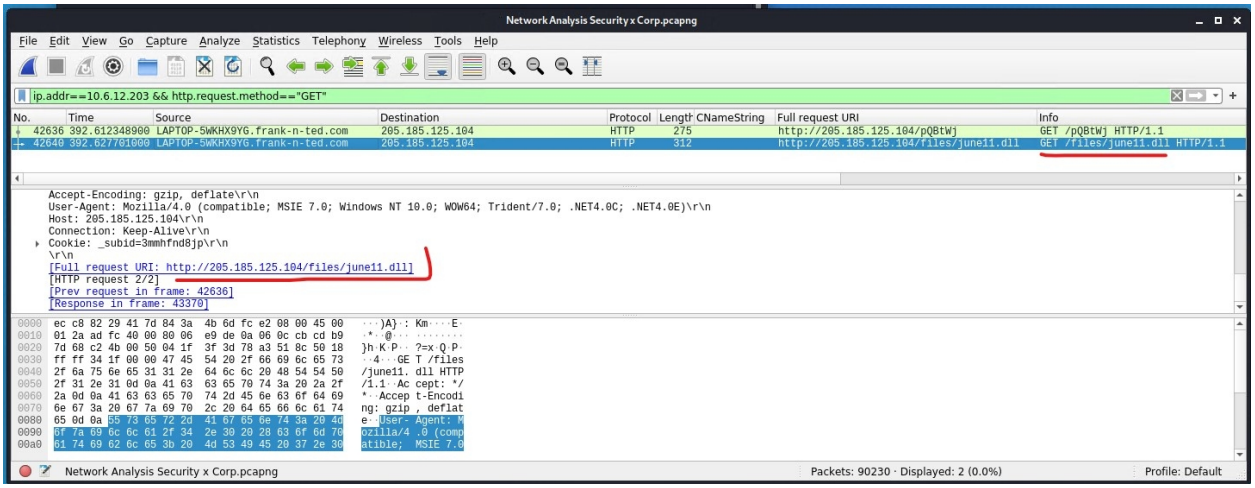
   (See Previous Screenshot)

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.**

Filter: ip.addr==10.6.12.203 && http.request.method==”GET”

The file found is the “june11.dll” (dynamic link library) file that was downloaded from 205.185.125.104

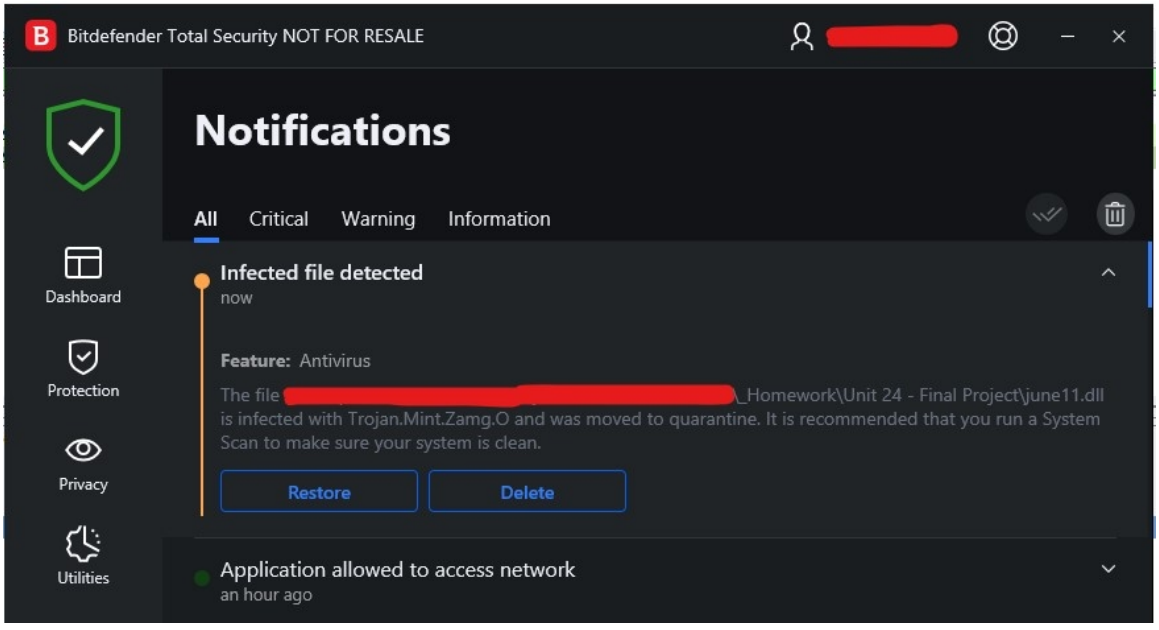
The name of the malware file downloaded is popularly known as “Google ipdate” with an intentional misspelling on the word “update.” Details screenshot in next section. The virus name is “Trojan.Mint.Zamg.O”

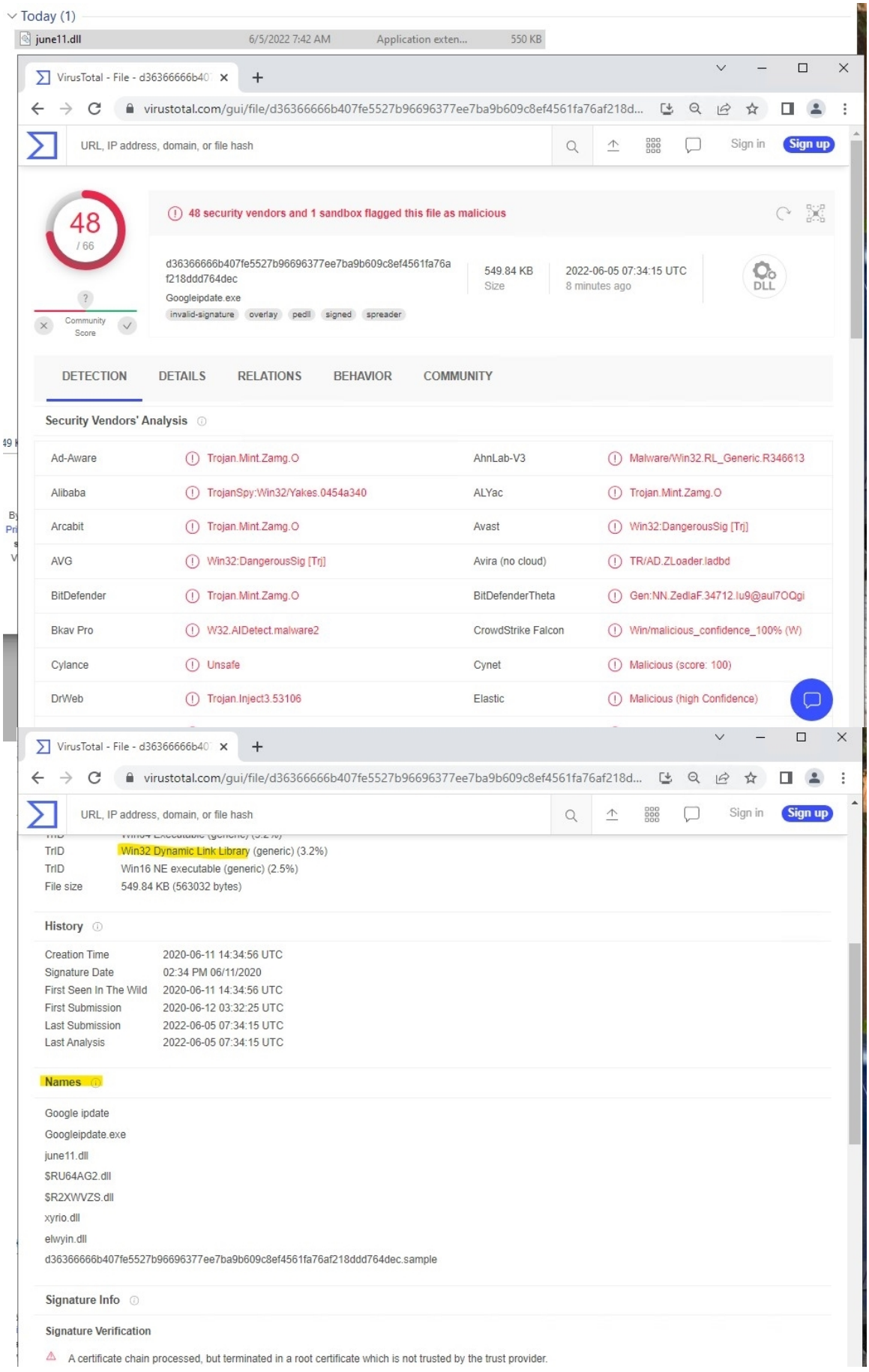


4. **Upload the file to VirusTotal.com. What kind of malware is this classified as?**

The type of malware this is classified as is a **Trojan.** “A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network.”

(See also screenshots on next page from VirusTotal.com)




Today (1)
june11.dll 6/5/2022 7:42 AM Application exten... 550 KB
VirusTotal - File - d36366666b40
virustotal.com/gui/file/d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218d...
URL, IP address, domain, or file hash
Sign in
Sign up
48 / 66
48 security vendors and 1 sandbox flagged this file as malicious
d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec
Googleipdate.exe
invalid-signature overlay pedll signed spreader
549.84 KB Size
2022-06-05 07:34:15 UTC 8 minutes ago
DLL
Community Score
DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY
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
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
BitDefenderTheta Gen:NN.ZedlaF.34712.lu9@aul7OQgi
Bkav Pro W32.AIDetect.malware2
CrowdStrike Falcon Win/malicious_confidence_100% (W)
Cylance Unsafe
Cynet Malicious (score: 100)
DrWeb Trojan.Inject3.53106
Elastic Malicious (high Confidence)
TrID Win32 Dynamic Link Library (generic) (3.2%)
TrID Win16 NE executable (generic) (2.5%)
File size 549.84 KB (563032 bytes)
History
Creation Time 2020-06-11 14:34:56 UTC
Signature Date 02:34 PM 06/11/2020
First Seen In The Wild 2020-06-11 14:34:56 UTC
First Submission 2020-06-12 03:32:25 UTC
Last Submission 2022-06-05 07:34:15 UTC
Last Analysis 2022-06-05 07:34:15 UTC
Names
Google ipdate
Googleipdate.exe
june11.dll
$RU64AG2.dll
$R2XWVZS.dll
xyrio.dll
elwyin.dll
d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec.sample
Signature Info
Signature Verification
A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider.

Vulnerable Windows Machines

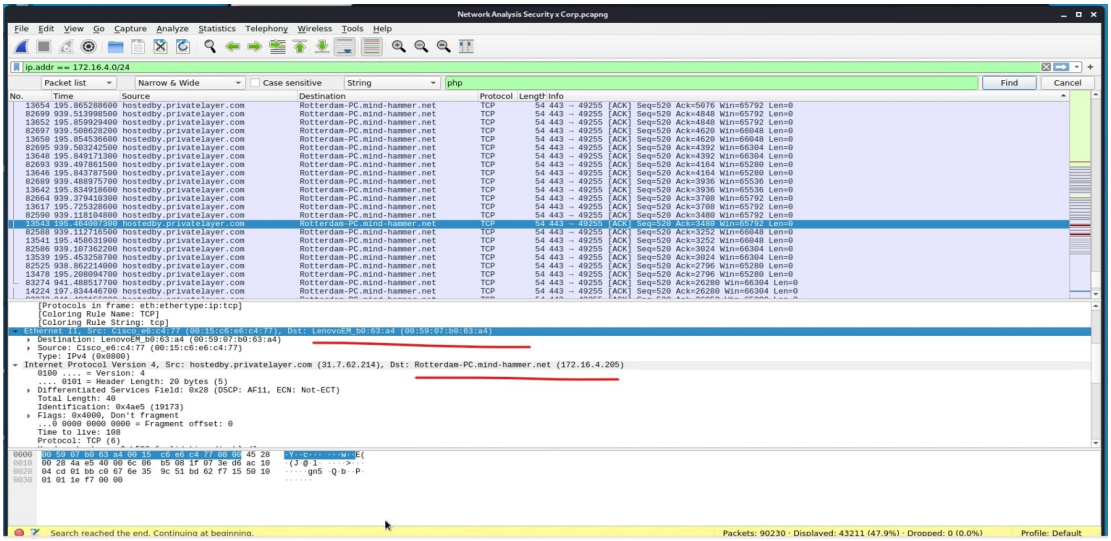
The Security team received reports of an infected Windows host on the network. They know the following:

- 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 / LenovoEM_b0:63:a4

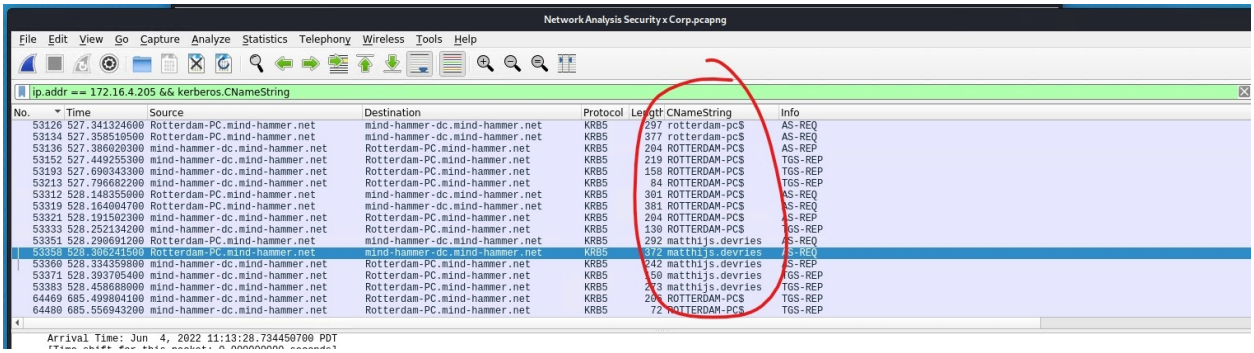
Filter: ip.addr==172.16.4.0/24



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

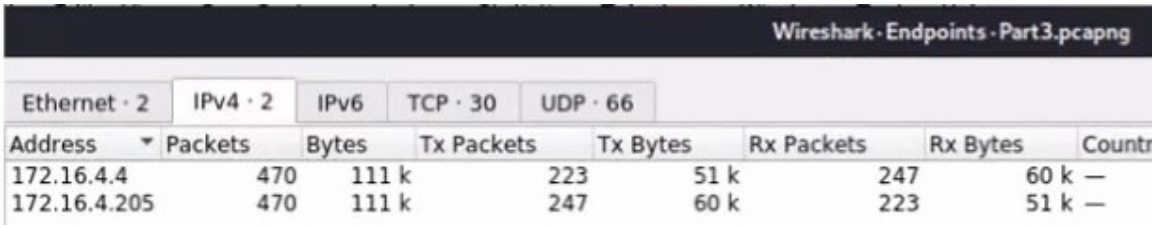
    User: matthijs.devries

Filter: ip.addr==172.16.4.205 && kerberos.CNameString



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

   Infected Computer - 172.16.4.205 (ROTTERDAM-PC)
   Attacking Computer - 172.16.4.4 (Mind-Hammer-DC)



Wireshark · Endpoints · Part3.pcapng

Ethernet · 2 | IPv4 · 2 | IPv6 | TCP · 30 | UDP · 66

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Countr
172.16.4.4	470	111 k	223	51 k	247	60 k	—
172.16.4.205	470	111 k	247	60 k	223	51 k	—

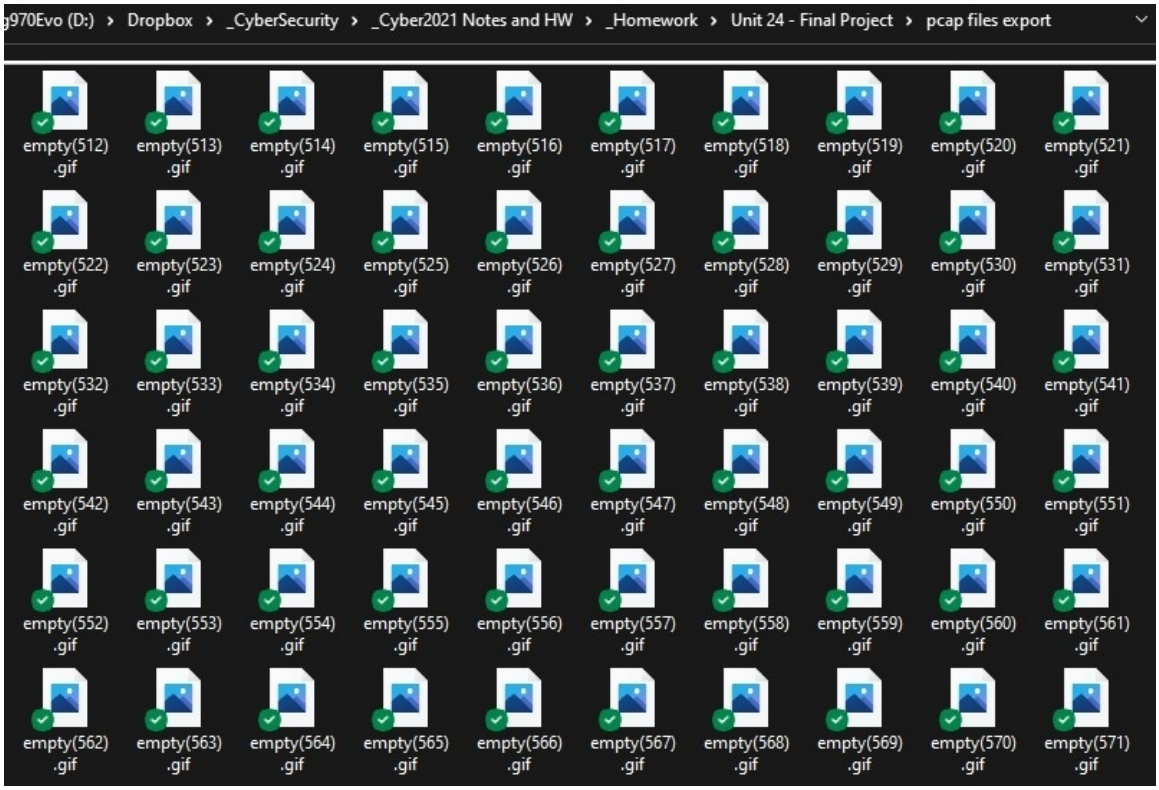
   As a bonus, the infected computer was infected with a Trojan.Agent.EHBD by the 40group.tiff image file that was downloaded to their computer, likely from malicious sites that they have been visiting or downloading from.

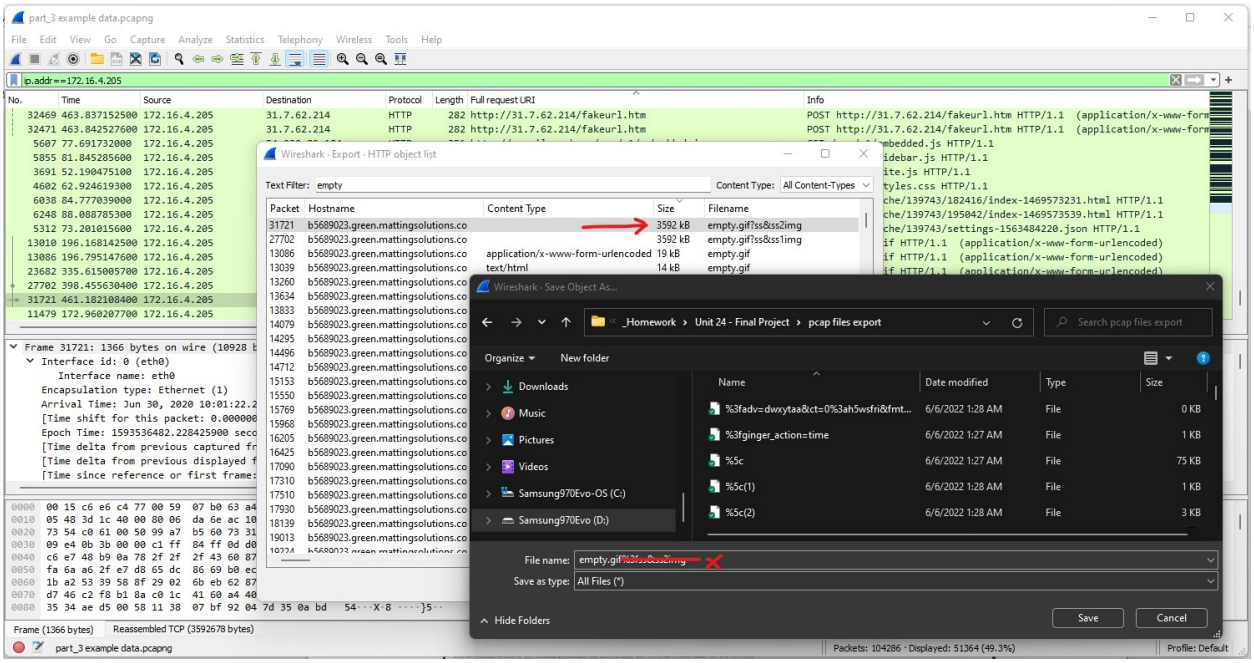
4. **As a bonus, retrieve the desktop background of the Windows host.**

   File > Export Objects > HTTP...

   There was a ton of “empty.gif” file fragments downloaded when exporting the files from the pcap file. Of all the photos, none of the ones exported represented a background as they were too small, and the source of them were all part of web-page elements with no guarantee that it was downloaded and used for a background.

   With that possibility, going back to scan all of the objects, there is a large high resolution “background” worth file size available that was not available to preview because the extension had extra text attached to it. By saving it and editing the filename to follow Windows naming syntax rules, the file displayed the background shot with the Windows toolbar, Start menu, and Recycle Bin showing.





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.

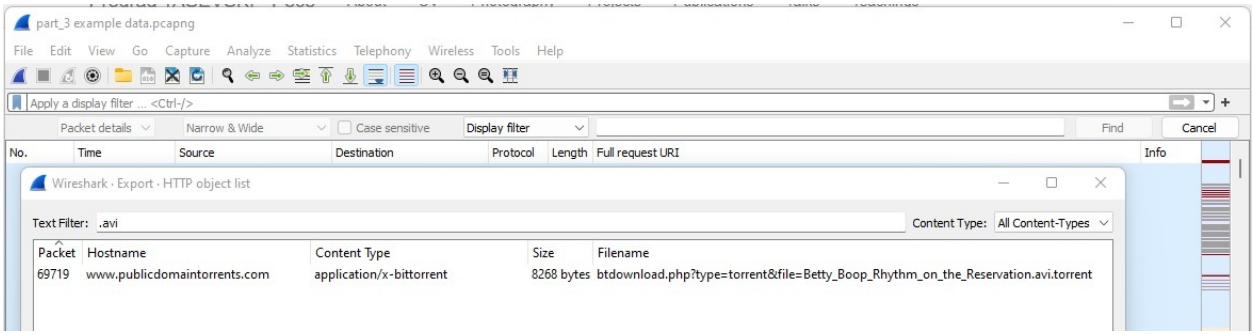
Your task is to isolate torrent traffic and answer the following questions in your Network Report:

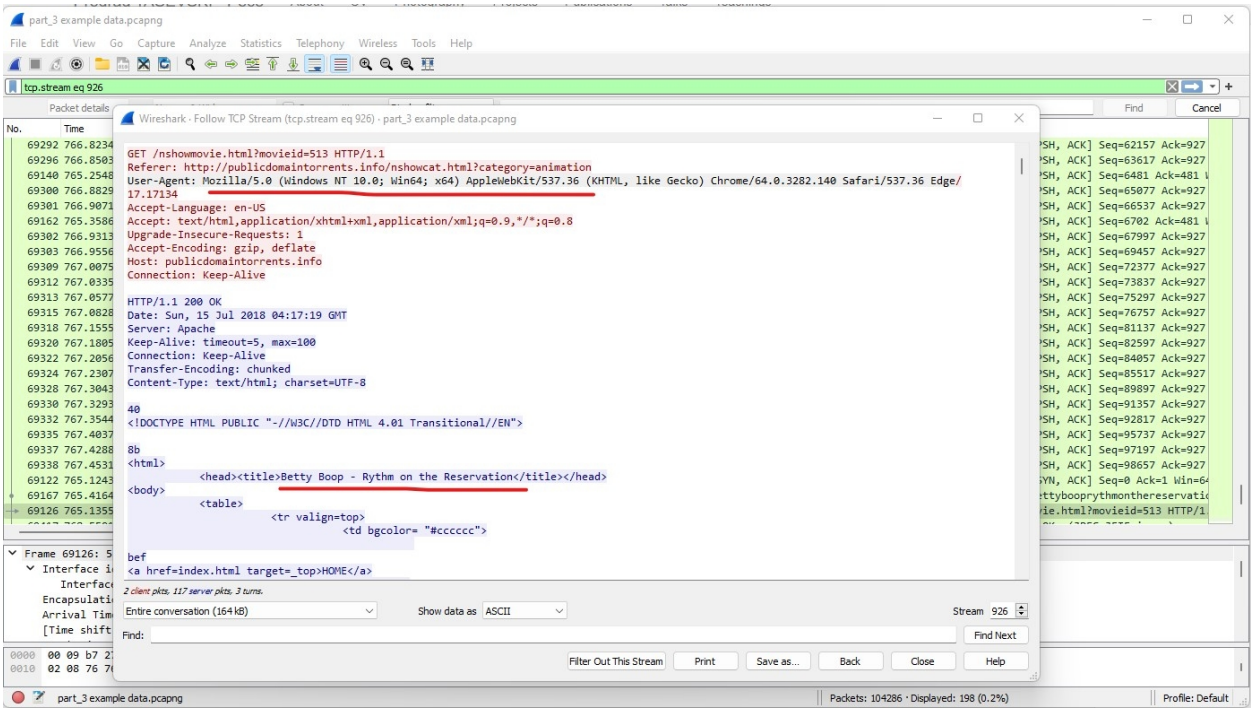
1. Find the following information about the machine with IP address `10.0.0.201`:
- **MAC address:** Msi_18:66:c8 (00:16:17:18:66:c8)
- **Windows username:** BLACO (user?), **Hostname:** BLANCO-DESKTOP
- **OS version:** Microsoft Windows 10 (Windows NT 10.0; Win64; x64)

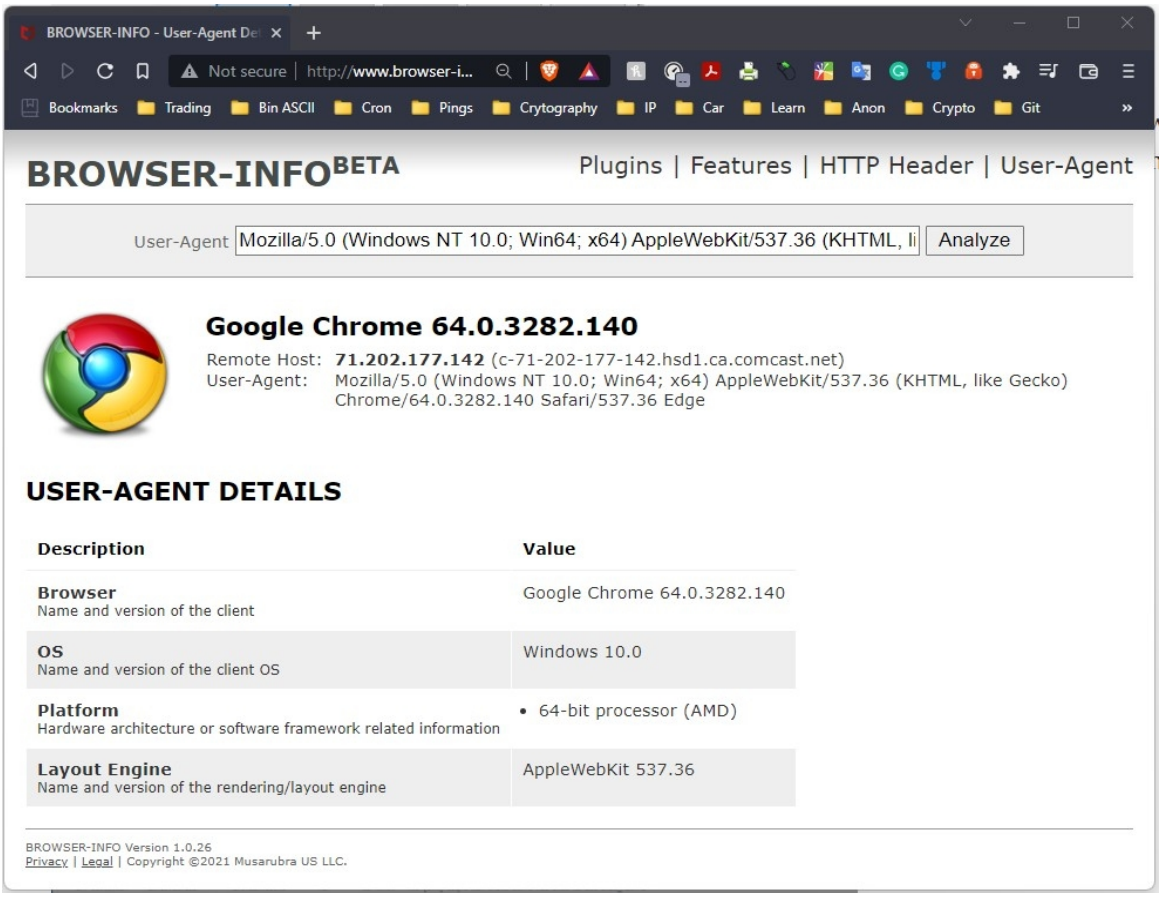
```
▸ Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
▸ Internet Protocol Version 4, Src: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201), Dst: 10.0.0.1 (10.0.0.1)
▸ User Datagram Protocol, Src Port: 137, Dst Port: 137
▾ NetBIOS Name Service
    Transaction ID: 0x951c
  ▸ Flags: 0x2900, Opcode: Registration, Recursion desired
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▸ Queries
  ▾ Additional records
    ▾ BLANCO-DESKTOP<00>: type NB, class IN
        Name: BLANCO-DESKTOP<00> (Workstation/Redirector)
        Type: NB (32)
        Class: IN (1)
        Time to live: 3 days, 11 hours, 20 minutes
        Data length: 6
      ▾ Name flags: 0x6000, ONT: Unknown (H-node, unique)
          0... .... .... .... = Name type: Unique name
          .11. .... .... .... = ONT: Unknown (3)
        Addr: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201)
```

2. Which torrent file did the user download?

"Betty_Boop_Rhythm_on_the_Reservation.avi" was the file downloaded via torrent.




part_3 example data.pcapng
Wireshark · Follow TCP Stream (tcp.stream eq 926) · part_3 example data.pcapng
GET /nshowmovie.html?movieid=513 HTTP/1.1
Referer: http://publicdomaintorrents.info/nshowcat.html?category=animation
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 04:17:19 GMT
Server: Apache
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
40
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
8b
<html>
<head><title>Betty Boop - Rythm on the Reservation</title></head>
<body>
<table>
<tr valign=top>
<td bgcolor= "#cccccc">
bef
HOME
Entire conversation (164 kB)
Show data as ASCII
Stream 926
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help


BROWSER-INFO - User-Agent Det
Not secure | http://www.browser-i...
Bookmarks
Trading
Bin ASCII
Cron
Pings
Crytography
IP
Car
Learn
Anon
Crypto
Git
BROWSER-INFO BETA
Plugins | Features | HTTP Header | User-Agent
User-Agent
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
Analyze
Google Chrome 64.0.3282.140
Remote Host: 71.202.177.142 (c-71-202-177-142.hsd1.ca.comcast.net)
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
USER-AGENT DETAILS
Description
Value
Browser
Name and version of the client
Google Chrome 64.0.3282.140
OS
Name and version of the client OS
Windows 10.0
Platform
Hardware architecture or software framework related information
64-bit processor (AMD)
Layout Engine
Name and version of the rendering/layout engine
AppleWebKit 537.36
BROWSER-INFO Version 1.0.26
Privacy | Legal | Copyright ©2021 Musarubra US LLC.

File Name: Betty_Boop_Rhythm_on_the_Reservation.avi
File Size: 100.50 MB
Resolution: 720x480
Duration: 00:06:02