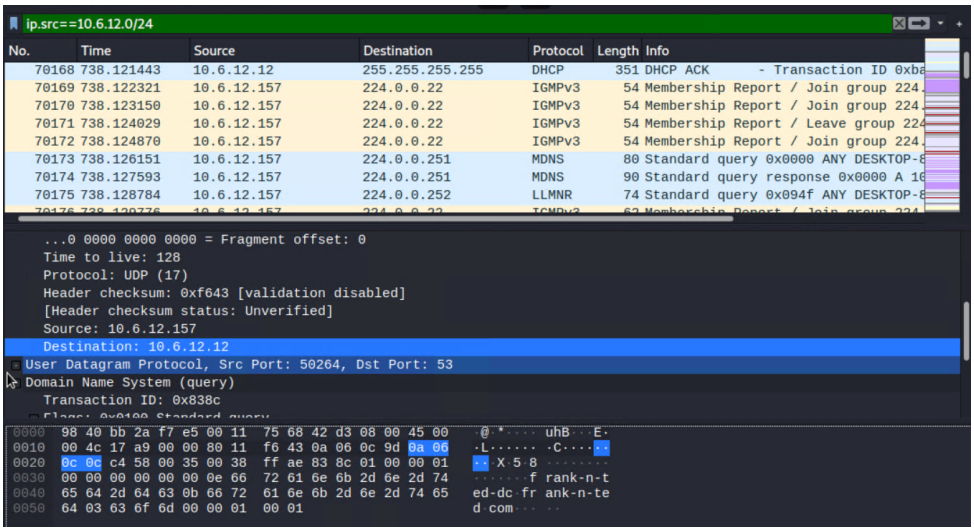
Network Analysis

Time Thieves

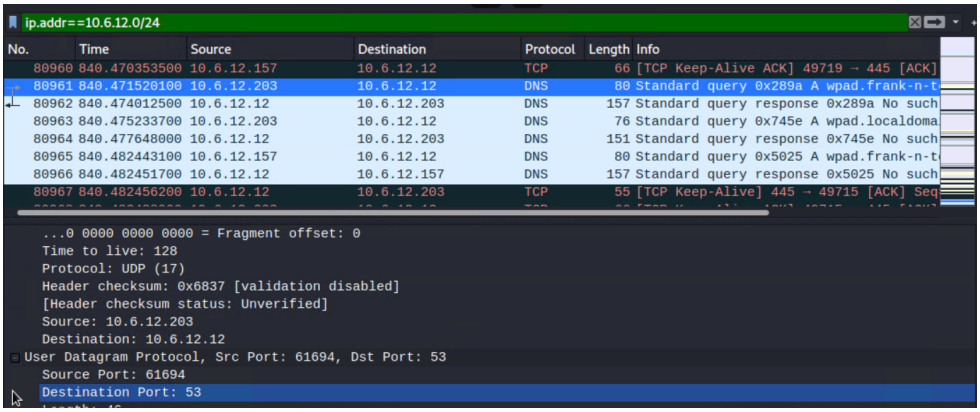
At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- 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.

1. Domain name of the users' custom site: frank-n-ted.com

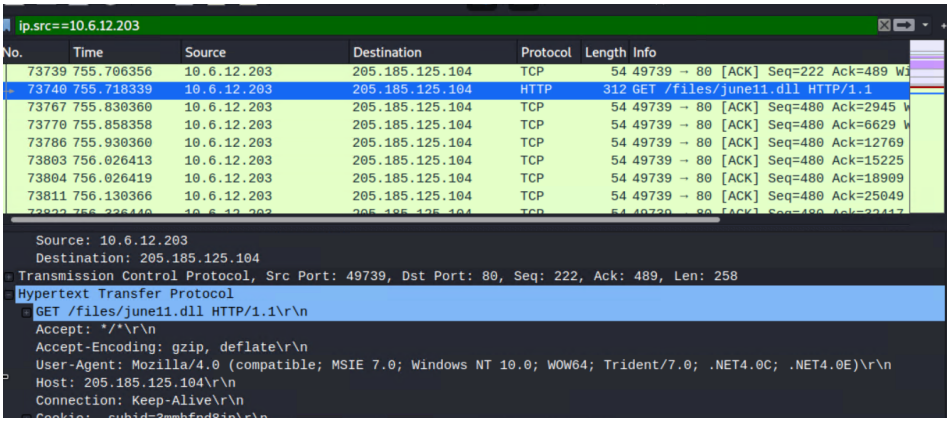
a. 

2. IP address of the Domain Controller (DC) of the AD network: 10.6.12.12

a. 

3. Name of the malware downloaded to the 10.6.12.203 machine: june11.dll

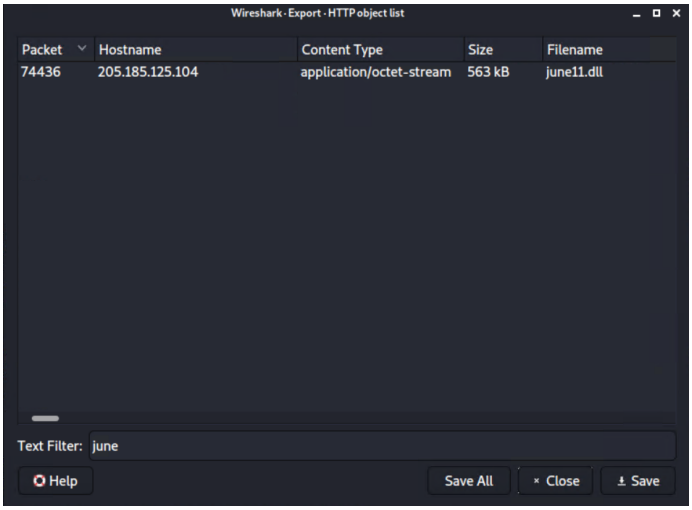
a.

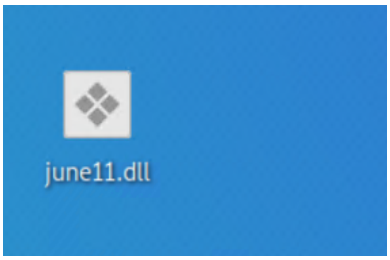

ip.src==10.6.12.203
No. Time Source Destination Protocol Length Info
73739 755.706356 10.6.12.203 205.185.125.104 TCP 54 49739 → 80 [ACK] Seq=222 Ack=489 Wi
73740 755.718339 10.6.12.203 205.185.125.104 HTTP 312 GET /files/june11.dll HTTP/1.1
73767 755.830360 10.6.12.203 205.185.125.104 TCP 54 49739 → 80 [ACK] Seq=480 Ack=2945 W
73770 755.858358 10.6.12.203 205.185.125.104 TCP 54 49739 → 80 [ACK] Seq=480 Ack=6629 W
73786 755.930360 10.6.12.203 205.185.125.104 TCP 54 49739 → 80 [ACK] Seq=480 Ack=12769
73803 756.026413 10.6.12.203 205.185.125.104 TCP 54 49739 → 80 [ACK] Seq=480 Ack=15225
73804 756.026419 10.6.12.203 205.185.125.104 TCP 54 49739 → 80 [ACK] Seq=480 Ack=18909
73811 756.130366 10.6.12.203 205.185.125.104 TCP 54 49739 → 80 [ACK] Seq=480 Ack=25049
Source: 10.6.12.203
Destination: 205.185.125.104
Transmission Control Protocol, Src Port: 49739, Dst Port: 80, Seq: 222, Ack: 489, Len: 258
Hypertext Transfer Protocol
GET /files/june11.dll HTTP/1.1\r\n
Accept: */*\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)\r\n
Host: 205.185.125.104\r\n
Connection: Keep-Alive\r\n

b.

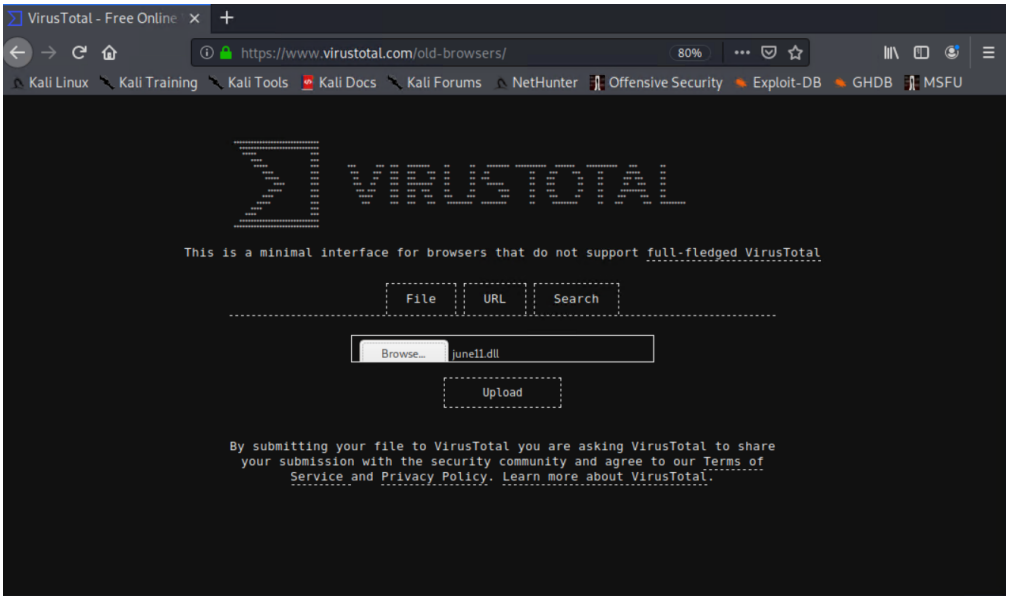

Wireshark · Follow TCP Stream (tcp.stream eq 915) · packetcapture.pcap
Content-Length: 0
Connection: keep-alive
Cache-Control: no-cache, no-store, must-revalidate,post-check=0,pre-check=0
Expires: 0
Last-Modified: Fri, 12 Jun 2020 17:15:19 GMT
Location: http://205.185.125.104/files/june11.dll
Pragma: no-cache
Set-Cookie: _subid=3mmhfnd8jp;Expires=Monday, 13-Jul-2020 17:15:19 GMT;Max-
Age=2678400;Path=/
Access-Control-Allow-Origin: *
GET /files/june11.dll HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0;
.NET4.0C; .NET4.0E)
Host: 205.185.125.104
Connection: Keep-Alive
Cookie: _subid=3mmhfnd8jp
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 12 Jun 2020 17:15:19 GMT
Content-Type: application/octet-stream
Content-Length: 563032
Last-Modified: Thu, 11 Jun 2020 22:34:56 GMT
Connection: keep-alive
ETag: "5ee2b190-89758"
X-Content-Type-Options: nosniff
Accept-Ranges: bytes
MZ.....@..... .!..L.!This
program cannot be run in DOS mode.
2 client pkts, 457 server pkts, 3 turns.

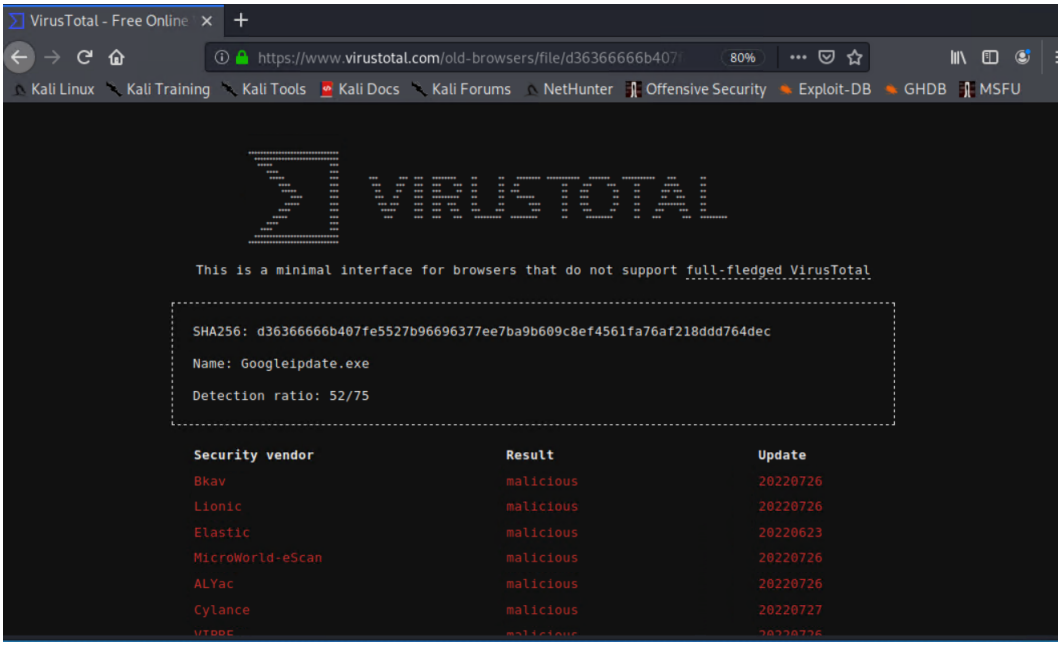
c.


Wireshark · Export · HTTP object list
Packet Hostname Content Type Size Filename
74436 205.185.125.104 application/octet-stream 563 kB june11.dll
Text Filter: june
Help
Save All
Close
Save

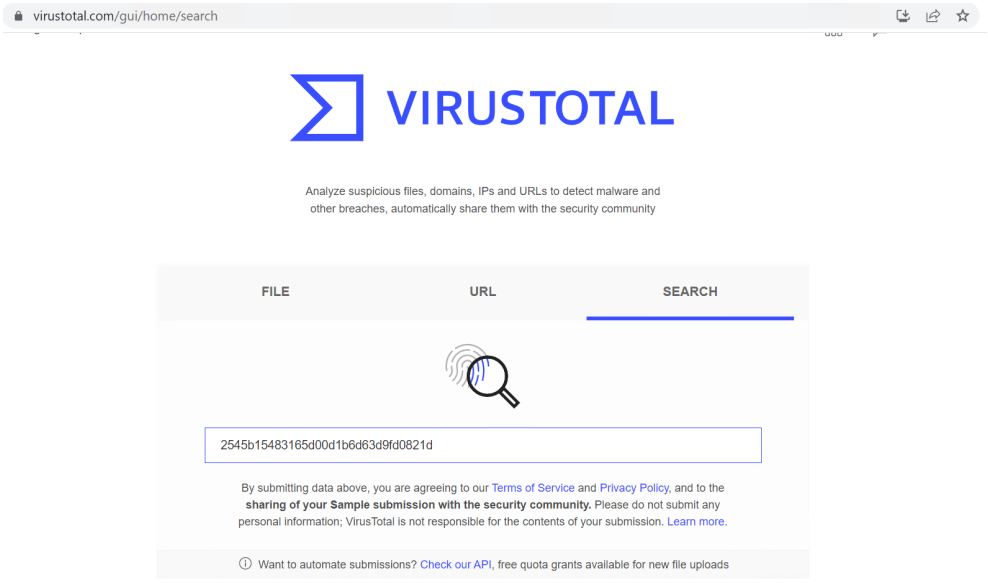
d. 

4. Malware classification: Trojan.Mint.Zamg.O (highly likely)

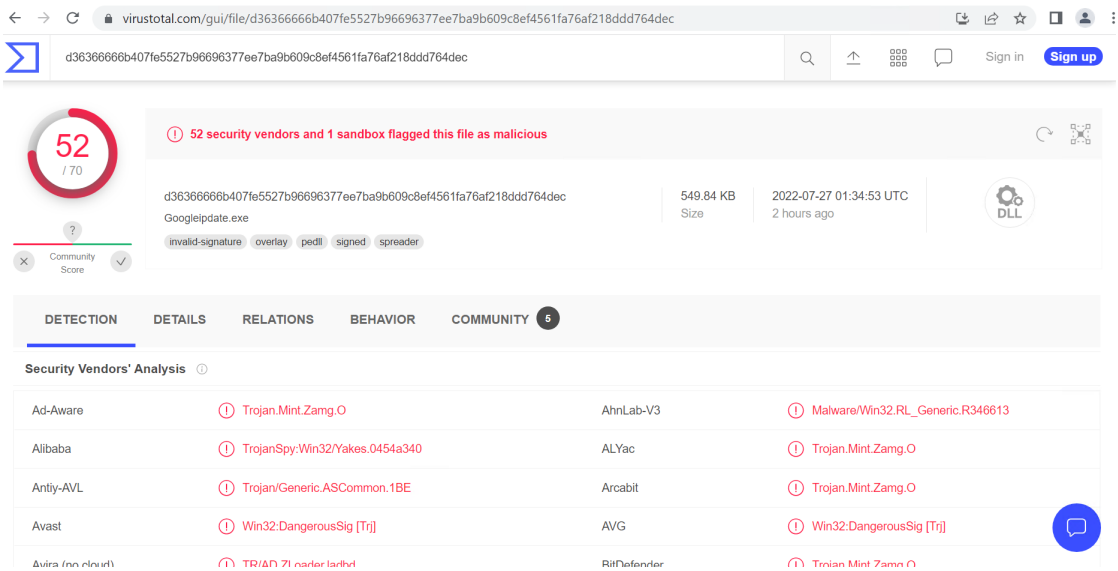
a. 

b. 

c.



d.



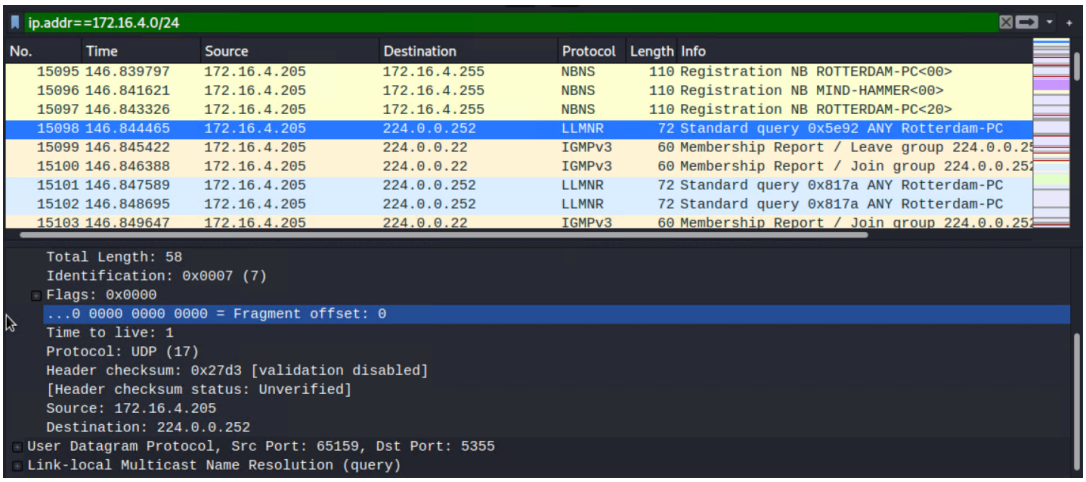
Vulnerable Windows Machines

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

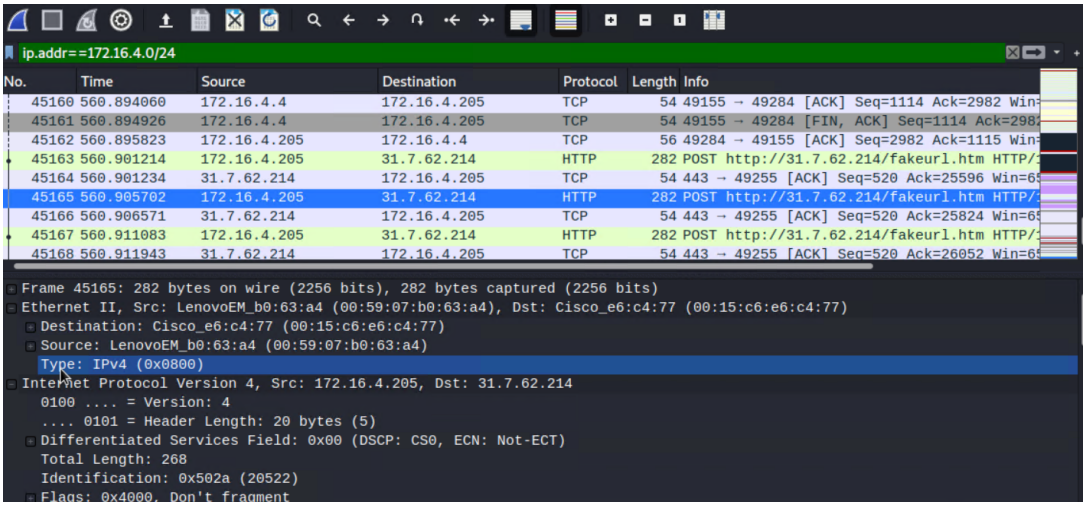
- Machines in the network live in the range 172.16.4.0/24.
- The domain mind-hammer.net is associated with the infected computer.
- The DC for this network lives at 172.16.4.4 and is named Mind-Hammer-DC.
- The network has standard gateway and broadcast addresses.

1. Information about the infected Windows machine:
    a. Host name: Rotterdam-PC
    b. IP address: 172.16.4.205
    c. MAC address: 00:59:07:b0:63:a4

d.

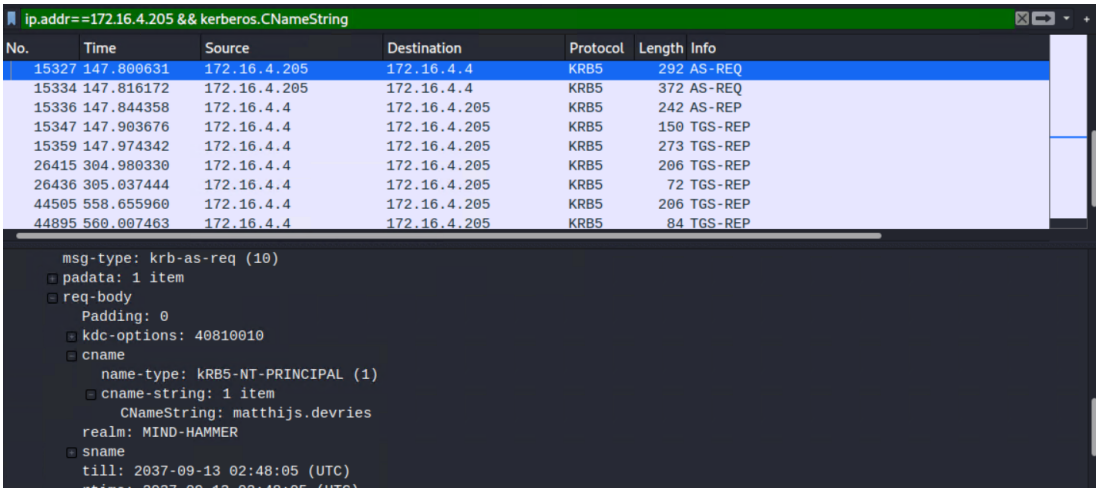


e.



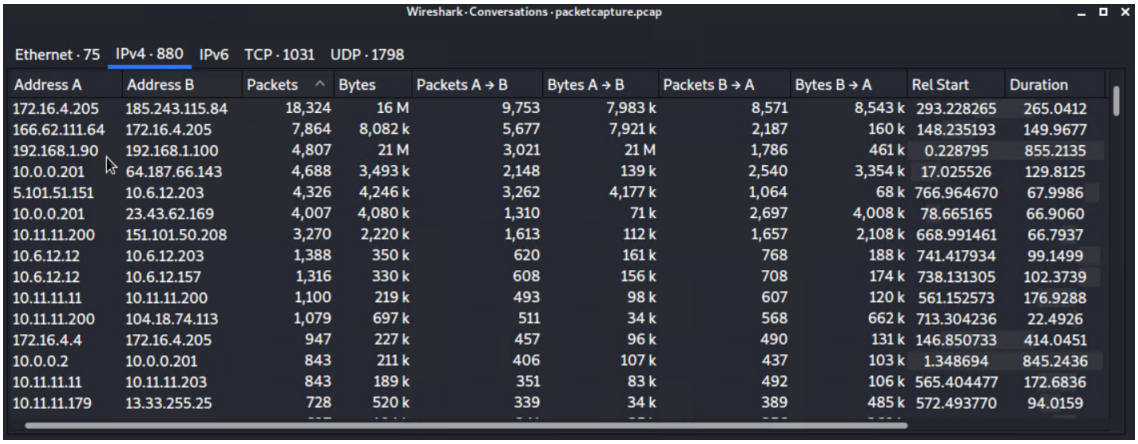
2. Username of the Windows user whose computer is infected: matthijs.devries

a.



3. The IP addresses used in the actual infection traffic: 185.243.115.84 and 172.16.4.205

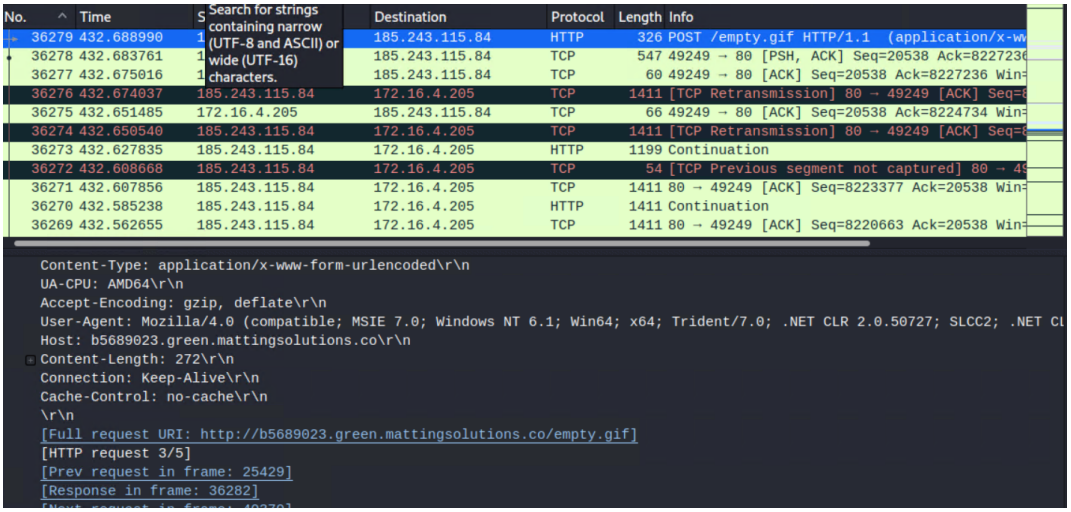
a.



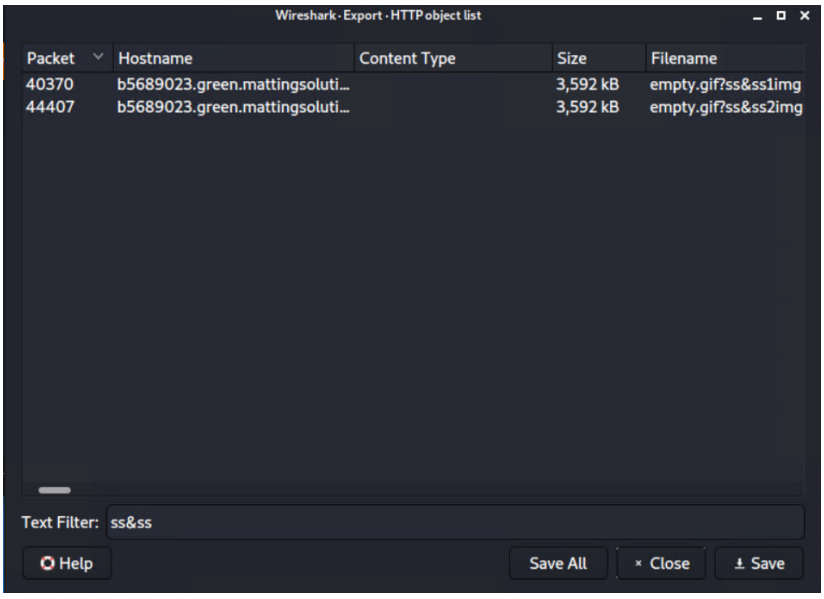
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
172.16.4.205	185.243.115.84	18,324	16 M	9,753	7,983 k	8,571	8,543 k	293.228265	265.0412
166.62.111.64	172.16.4.205	7,864	8,082 k	5,677	7,921 k	2,187	160 k	148.235193	149.9677
192.168.1.90	192.168.1.100	4,807	21 M	3,021	21 M	1,786	461 k	0.228795	855.2135
10.0.0.201	64.187.66.143	4,688	3,493 k	2,148	139 k	2,540	3,354 k	17.025526	129.8125
5.101.51.151	10.6.12.203	4,326	4,246 k	3,262	4,177 k	1,064	68 k	766.964670	67.9986
10.0.0.201	23.43.62.169	4,007	4,080 k	1,310	71 k	2,697	4,008 k	78.665165	66.9060
10.11.11.200	151.101.50.208	3,270	2,220 k	1,613	112 k	1,657	2,108 k	668.991461	66.7937
10.6.12.12	10.6.12.203	1,388	350 k	620	161 k	768	188 k	741.417934	99.1499
10.6.12.12	10.6.12.157	1,316	330 k	608	156 k	708	174 k	738.131305	102.3739
10.11.11.11	10.11.11.200	1,100	219 k	493	98 k	607	120 k	561.152573	176.9288
10.11.11.200	104.18.74.113	1,079	697 k	511	34 k	568	662 k	713.304236	22.4926
172.16.4.4	172.16.4.205	947	227 k	457	96 k	490	131 k	146.850733	414.0451
10.0.0.2	10.0.0.201	843	211 k	406	107 k	437	103 k	1.348694	845.2436
10.11.11.11	10.11.11.203	843	189 k	351	83 k	492	106 k	565.404477	172.6836
10.11.11.179	13.33.255.25	728	520 k	339	34 k	389	485 k	572.493770	94.0159

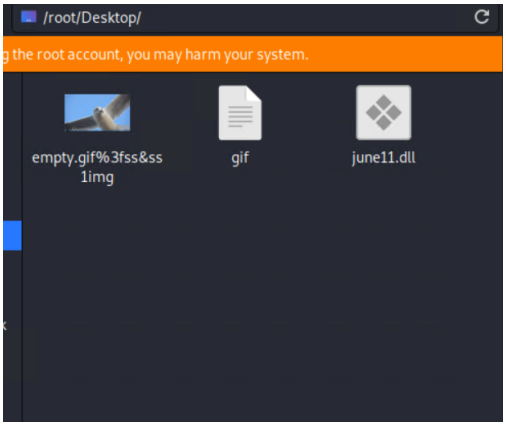
4. The desktop background of the Windows host

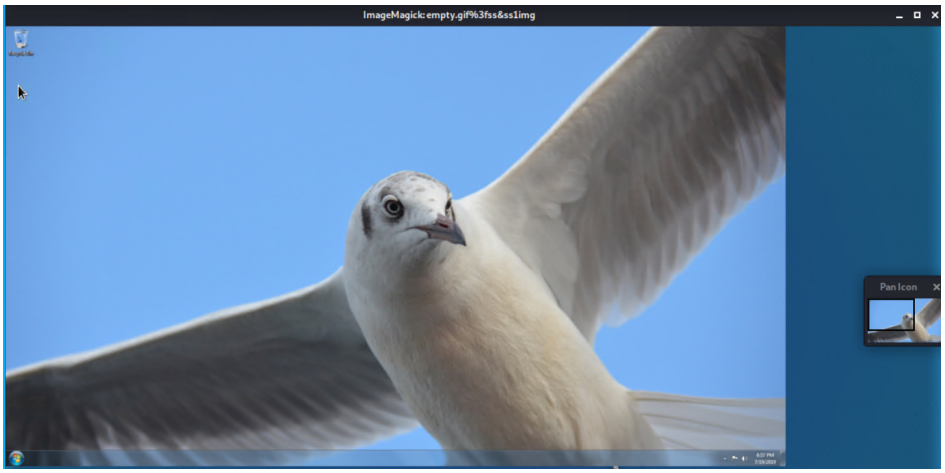
a.



b.



c. 

d. 

Illegal Downloads

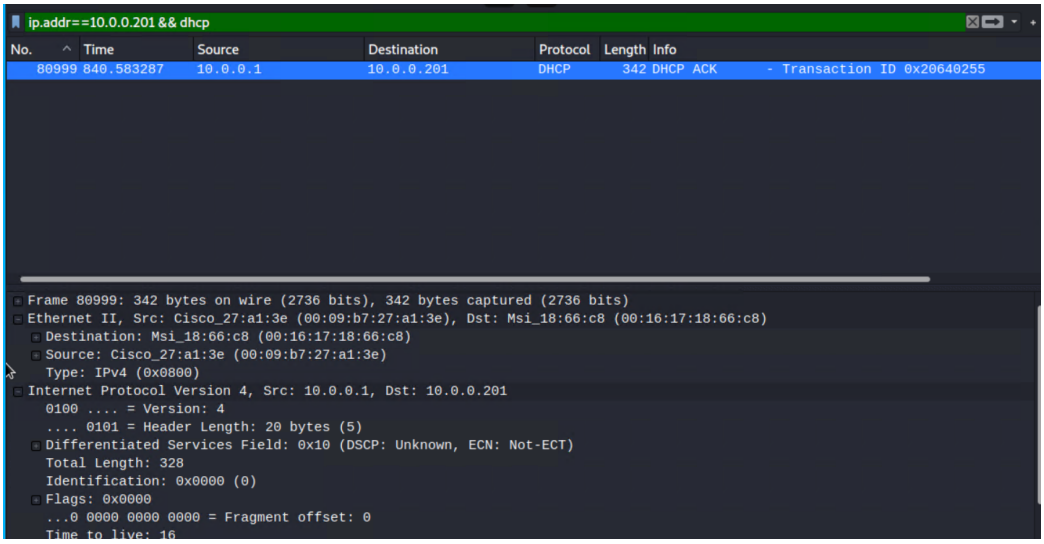
IT was informed that some users are torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringement.

IT shared the following about the torrent activity:

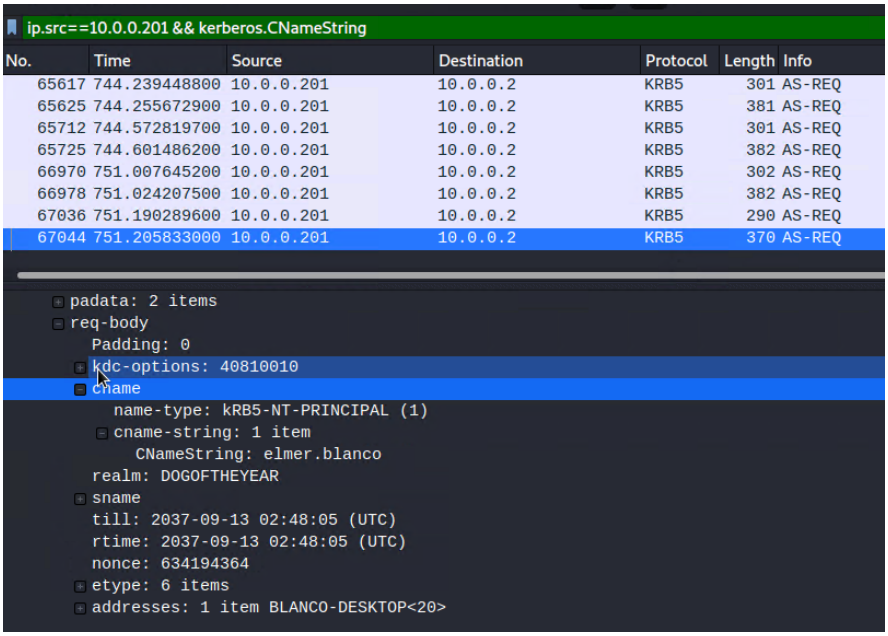
- The machines using torrents live in the range 10.0.0.0/24 and are clients of an AD domain.
- The DC of this domain lives at 10.0.0.2 and is named DogOfTheYear-DC.
- The DC is associated with the domain dogoftheyear.net.

1. Find the following information about the machine with IP address 10.0.0.201:
    a. MAC address: 00:16:17:18:66:c8
    b. Windows username: elmer.blanco
    c. OS version: Windows 10.0

d.

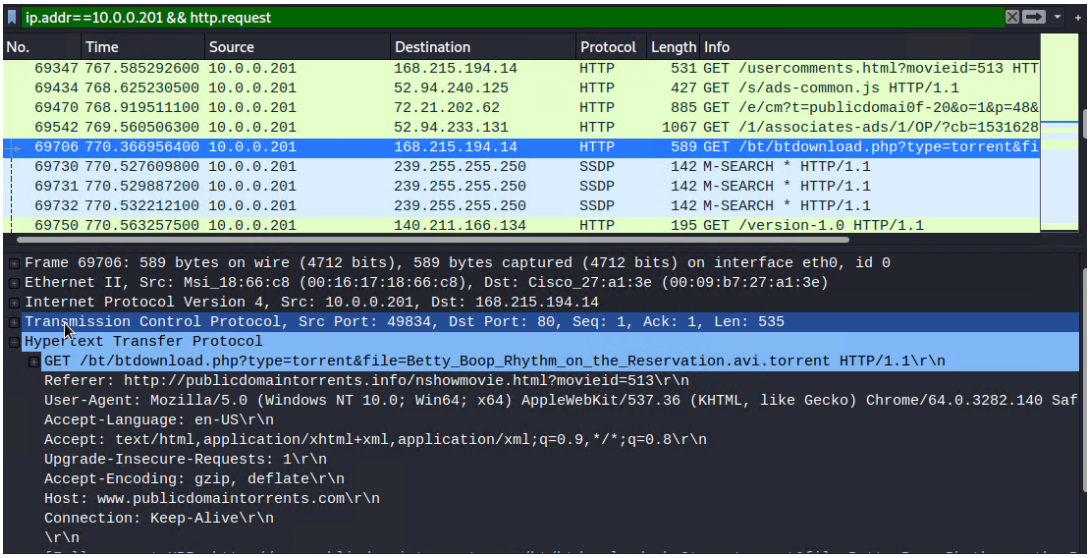


e.

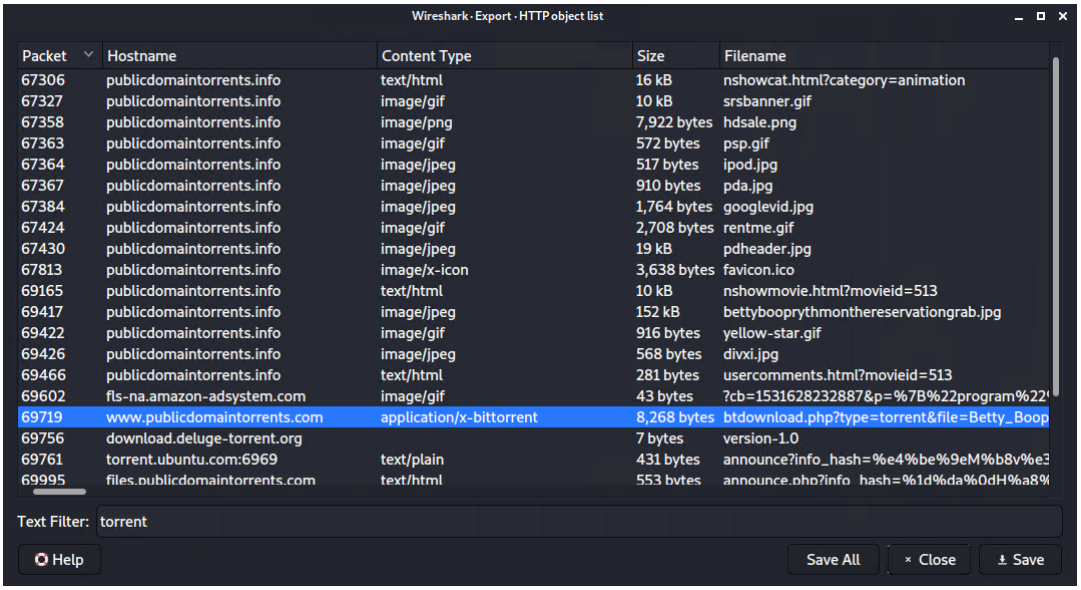


2. Torrent file the user download: Betty_Boop_Rhythm_on_the_Reservation.avi.torrent

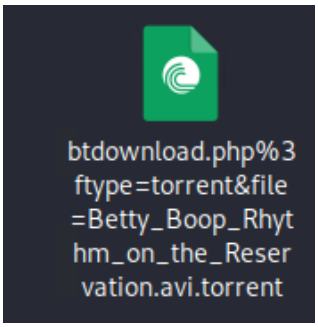
a.


ip.addr==10.0.0.201 && http.request
No. Time Source Destination Protocol Length Info
69347 767.585292600 10.0.0.201 168.215.194.14 HTTP 531 GET /usercomments.html?movieid=513 HTT
69434 768.625230500 10.0.0.201 52.94.240.125 HTTP 427 GET /s/ads-common.js HTTP/1.1
69470 768.919511100 10.0.0.201 72.21.202.62 HTTP 885 GET /e/cm?t=publicdomai0f-20&o=1&p=48&
69542 769.560506300 10.0.0.201 52.94.233.131 HTTP 1067 GET /1/associates-ads/1/OP/?cb=1531628
69706 770.366956400 10.0.0.201 168.215.194.14 HTTP 589 GET /bt/btdownload.php?type=torrent&fi
69730 770.527609800 10.0.0.201 239.255.255.250 SSDP 142 M-SEARCH * HTTP/1.1
69731 770.529887200 10.0.0.201 239.255.255.250 SSDP 142 M-SEARCH * HTTP/1.1
69732 770.532212100 10.0.0.201 239.255.255.250 SSDP 142 M-SEARCH * HTTP/1.1
69750 770.563257500 10.0.0.201 140.211.166.134 HTTP 195 GET /version-1.0 HTTP/1.1
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 Saf
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

b.


Wireshark · Export · HTTP object list
Packet Hostname Content Type Size Filename
67306 publicdomaintorrents.info text/html 16 kB nshowcat.html?category=animation
67327 publicdomaintorrents.info image/gif 10 kB srsbanner.gif
67358 publicdomaintorrents.info image/png 7,922 bytes hdsale.png
67363 publicdomaintorrents.info image/gif 572 bytes psp.gif
67364 publicdomaintorrents.info image/jpeg 517 bytes ipod.jpg
67367 publicdomaintorrents.info image/jpeg 910 bytes pda.jpg
67384 publicdomaintorrents.info image/jpeg 1,764 bytes googlevid.jpg
67424 publicdomaintorrents.info image/gif 2,708 bytes rentme.gif
67430 publicdomaintorrents.info image/jpeg 19 kB pdheader.jpg
67813 publicdomaintorrents.info image/x-icon 3,638 bytes favicon.ico
69165 publicdomaintorrents.info text/html 10 kB nshowmovie.html?movieid=513
69417 publicdomaintorrents.info image/jpeg 152 kB bettybooprythmonthereservationgrab.jpg
69422 publicdomaintorrents.info image/gif 916 bytes yellow-star.gif
69426 publicdomaintorrents.info image/jpeg 568 bytes divxi.jpg
69466 publicdomaintorrents.info text/html 281 bytes usercomments.html?movieid=513
69602 fls-na.amazon-adsystem.com image/gif 43 bytes ?cb=1531628232887&p=%7B%22program%22
69719 www.publicdomaintorrents.com application/x-bittorrent 8,268 bytes btdownload.php?type=torrent&file=Betty_Boop
69756 download.deluge-torrent.org 7 bytes version-1.0
69761 torrent.ubuntu.com:6969 text/plain 431 bytes announce?info_hash=%e4%be%9eM%b8v%e3
69995 files.publicdomaintorrents.com text/html 553 bytes announce.php?info_hash=%1d%da%0dH%a8%
Text Filter: torrent
Help
Save All
Close
Save

c.


btdownload.php%3ftype=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent