

# Network Analysis

## Time Thieves

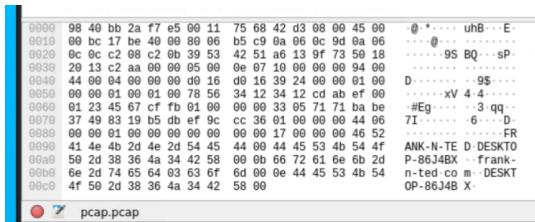
At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- 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?

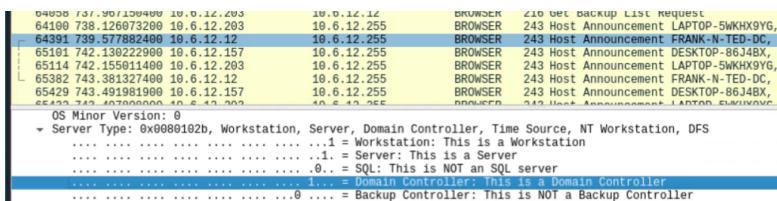
Frank-n-ted.com



```
0000  98 40 bb 2a f7 e5 00 11 75 68 42 d3 08 00 45 00  @ *.....uhB-E
0010  99 bc 17 be 49 00 89 96 b5 c9 0a 06 0c 0d 0a 06  ..@.....95 BQ-SP
0020  0c 0c c2 08 c2 0b 39 53 42 51 a6 13 9f 73 50 18  ....95 BQ-SP
0030  29 13 c2 a8 00 00 05 00 0e 07 10 00 00 00 94 00  .....
0040  44 00 04 00 00 00 00 08 16 d0 16 39 24 00 00 01 00  D.....9$...
0050  00 00 01 00 01 00 78 56 34 12 34 12 cd ab ef 00  .....xV 4 4...
0060  01 23 45 67 cf fb 01 00 00 00 33 05 71 71 ba be  #Eq... 3 qq...
0070  37 49 83 19 b5 db ef 9c cc 36 01 00 00 00 44 06  71.....6...D
0080  00 00 01 00 00 00 00 00 00 17 00 00 00 46 52  .....FR
0090  41 4e 4b 2d 4e 2d 54 45 44 00 44 45 53 4b 54 4F  ANK-N-TE D-DESKT0
00a0  50 2d 38 36 4a 34 42 58 00 00 66 72 61 6e 6b 2d  P-86J4BX - frank-
00b0  6e 2d 74 65 64 03 63 6f 6d 00 0e 44 45 53 4b 54  n-ted co m-DESKT
00c0  4f 50 2d 38 36 4a 34 42 58 00  .....OP-86J4BX-
```

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

10.6.12.12



```
0000  45 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  OS Minor Version: 0
0001  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  Server Type: 0x0000102b, Workstation, Server, Domain Controller, Time Source, NT Workstation, DFS
0002  .....1..... = Workstation: This is a Workstation
0003  .....1..... = Server: This is a Server
0004  .....0..... = SQL: This is NOT an SQL server
0005  .....1.... = Domain Controller: This is a Domain Controller
0006  .....0.... = Backup Controller: This is NOT a Backup Controller
```

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.

June11.dll

4. Upload the file to [VirusTotal.com](#). What kind of malware is this classified as?

It is classified as a Trojan.

VirusTotal - File - d3636... + https://www.virustotal.com/gui/file/d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Sign in Sign up

50 / 67

Community Score

① 50 security vendors and 1 sandbox flagged this file as malicious

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec GoogleUpdate.exe 549.84 KB 2022-03-09 01:38:24 UTC 53 minutes ago DLL

Invalid-signature overlay pedil signed spreader

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	① Trojan.Mint.Zamg.O		AhnLab-V3	① Malware/Win32.RL_Generic.R346613
Alibaba	① TrojanSpy:Win32/Yakes.0454a340		ALYac	① Trojan.Mint.Zamg.O
Antiy-AVL	① Trojan/Generic.ASCCommon.tBE		Arcabit	① Trojan.Mint.Zamg.O
Avast	① Win32:DangerousSig [Trj]		AVG	① Win32:DangerousSig [Trj]
Avira (no cloud)	① TR/AD.ZLoader.ladbd		BitDefender	① Trojan.Mint.Zamg.O
BitDefenderTheta	① Gen:NN.Zedla.F.34264.lu9@a0l7OQgi		CAT-QuickHeal	① Ransom.LockyCiR
CrowdStrike Falcon	① Win/malicious_confidence_100% (W)		Cylance	① Unsafe
Cynet	① Malicious (score: 100)		DrWeb	① Trojan.Inject3.53106

status: Running

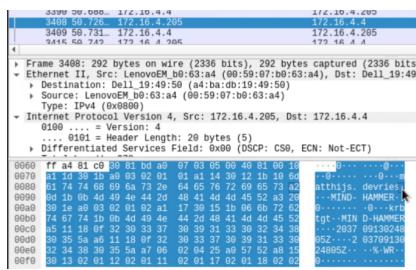
# Vulnerable Windows Machines

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.

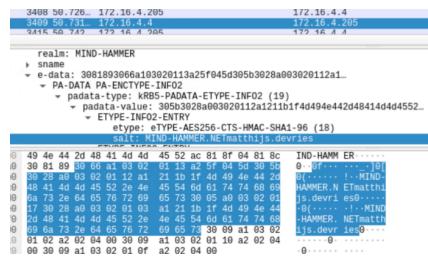
Inspect your traffic to answer the following questions:

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**



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

  - matthijs.devries



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

These 3 ip addresses have communication between each other and have the largest amount of packets and bytes used.

- 172.16.4.205
  - 185.243.115.84

- 166.62.111.64

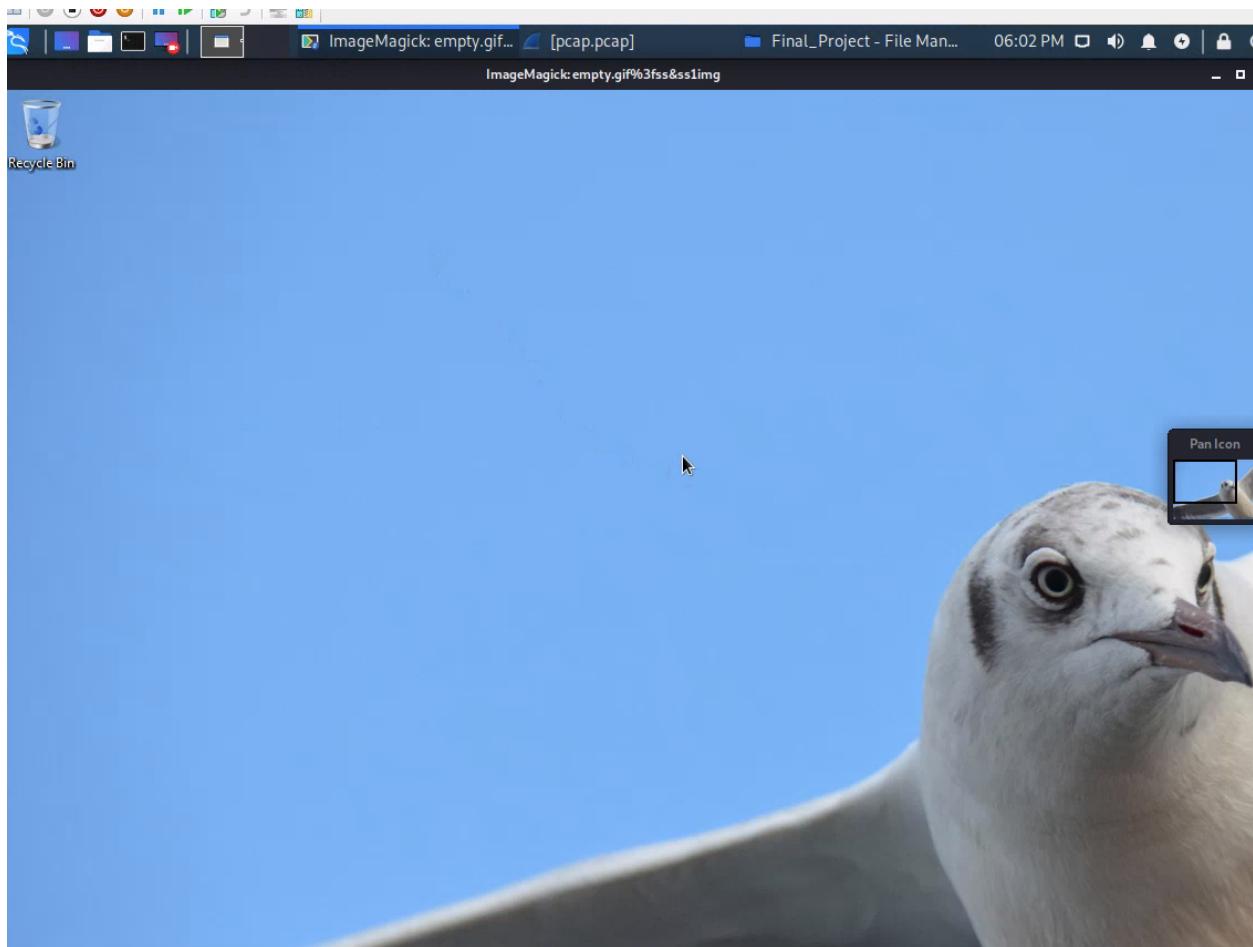
Ethernet · 74	IPv4 · 877	IPv6 · 1	TCP · 1044	UDP · 1839							
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	
172.16.4.205	185.243.115.84	30,344	16 M	15,149	9,831 k	15,195	16 M	196.154.31.4	2016.8611	1001.6762	176
166.62.111.64	172.16.4.205	15,728	16 M	11,354	15 M	4,374	321 k	51.161.259	1001.6762	176	
10.0.0.201	23.43.62.169	6,934	7,045 k	2,282	124 k	4,652	6,920 k	0.000000	900.2057	1.10	
5.101.51.151	10.6.12.203	4,326	4,246 k	3,262	4,177 k	1,064	68 k	669.890730	67.9985	491	
10.0.0.201	64.187.66.143	4,883	3,637 k	2,235	144 k	2,648	3,492 k	47.425979	854.0467	1.35	
10.11.11.200	151.101.50.208	3,270	2,220 k	1,613	112 k	1,657	2,108 k	571.917522	66.7937	13	
10.11.11.200	104.18.74.113	1,079	697 k	511	34 k	568	662 k	616.230265	22.4916	12	
10.6.12.203	205.185.125.104	647	599 k	185	10 k	462	588 k	658.615057	79.8144	1.05	
10.11.11.179	13.33.255.25	728	520 k	339	34 k	389	485 k	475.419836	94.0159	2.95	

4. Found a desktop image by searching in the Export Objects HTTP screen, and found entries that seemed odd.

Packet	Hostname	Content Type	Size	Filename
27702	b5689023.green.mattingsolutions.co		3,592 kB	empty.gif?ss&ss1img
31721	b5689023.green.mattingsolutions.co		3,592 kB	empty.gif?ss&ss2img
35066	img.timeinc.net	text/css	90 kB	main.css
35091	img.timeinc.net	text/css	21 kB	fixed-header-footer.css
35120	img.timeinc.net	text/css	14 kB	photos.css
35124	img.timeinc.net	text/css	7,350 bytes	channel.css
35151	img.timeinc.net	application/javascript	33 kB	main.js
35174	img.timeinc.net	application/javascript	72 kB	jquery.js
35183	img.timeinc.net	application/javascript	751 bytes	showLinks.js
35184	img.timeinc.net	application/javascript	10 kB	articles.js
35194	img.timeinc.net	application/javascript	2,996 bytes	photoessay.js
35198	img.timeinc.net	application/javascript	319 bytes	frequency_capping.min.js
35202	img.timeinc.net	application/javascript	11 kB	mobileExperience.js
35213	img.timeinc.net	application/javascript	16 kB	MobileCompatibility.js
35231	img.timeinc.net	image/gif	43 bytes	alt_holder.gif
35259	img.timeinc.net	application/javascript	71 kB	time_s_code.js
35453	img.timeinc.net	image/jpeg	124 kB	libya_ruins_01.jpg
36661	img.timeinc.net	image/png	2,238 bytes	btn_photos.png
36671	img.timeinc.net	image/png	3,449 bytes	inputBG.png
36685	img.timeinc.net	image/png	13 kB	newsletterLogo.png
36701	img.timeinc.net	image/png	2,068 bytes	share-tools.png
41306	img.timeinc.net	image/x-icon	1,150 bytes	favicon.ico

Text Filter: img

Save Save All Close Help



## 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:

1. Find the following information about the machine with IP address 10.0.0.201:

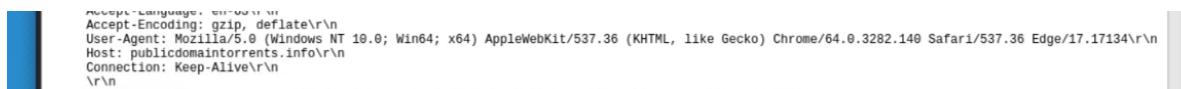
- o MAC address: 00:16:17:18:66:c8



- o Windows username: elmer blanco



- o OS version: Windows NT 10.0



2. Which torrent file did the user download?

The user downloaded “betty boop rhythm on the reservation” from the site publicdomaintorrents.com (Betty\_Boop\_Rhythm\_on\_the\_Reservation.avi.torrent)

