

Network Analysis

Time Thieves

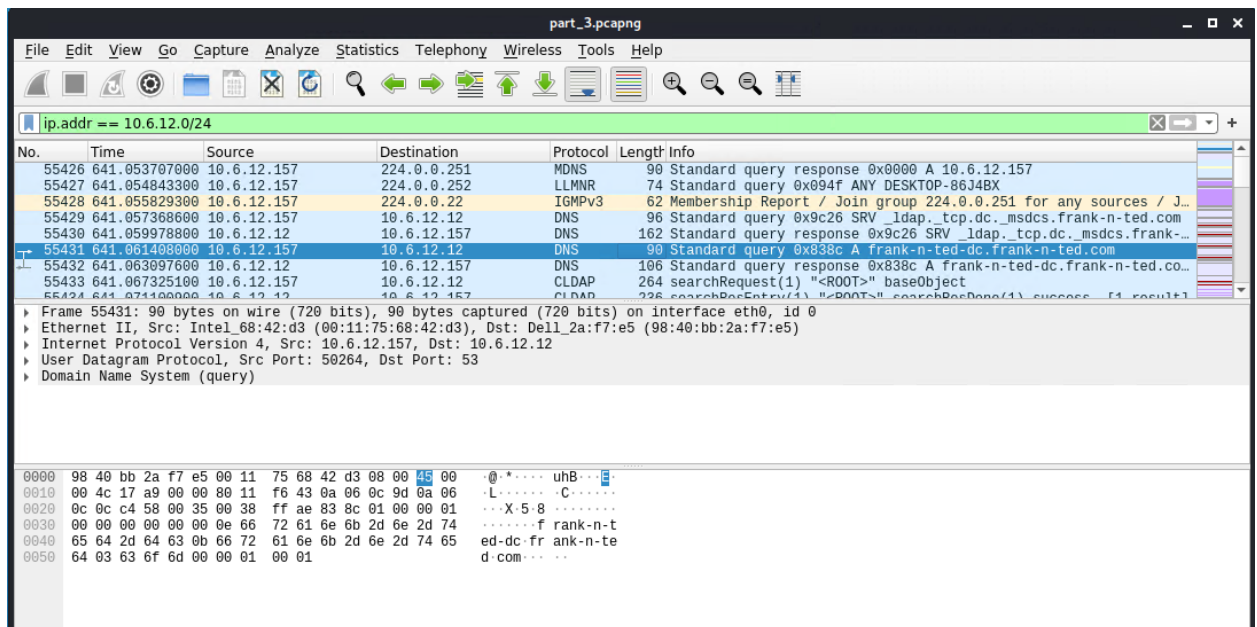
At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- 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-DC.frank-n-ted.com.



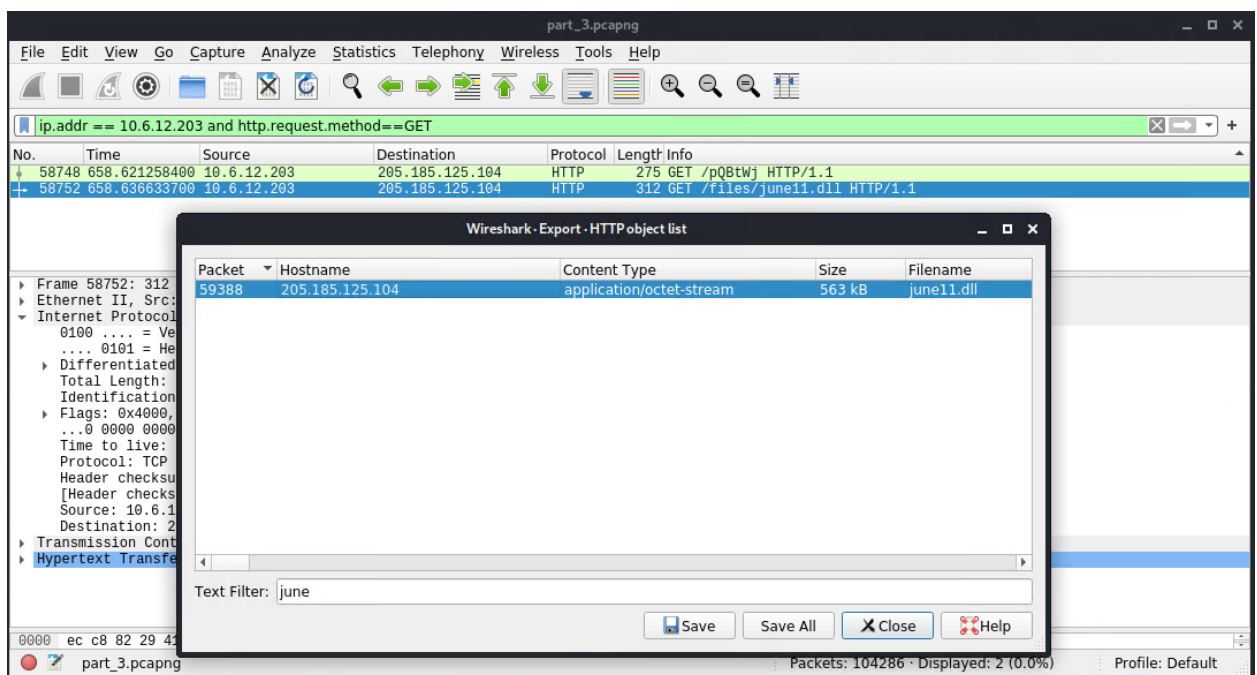
2. What is the IP address of the Domain Controller (DC) of the AD network?

10.6.12.12

```
Internet Protocol Version 4, Src: 10.6.12.157, Dst: 10.6.12.12
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 76
    Identification: 0x17a9 (6057)
    Flags: 0x0000
      ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0xf643 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.6.12.157
    Destination: 10.6.12.12
  User Datagram Protocol, Src Port: 50264, Dst Port: 53
  Domain Name System (query)
```


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](https://www.virustotal.com). What kind of malware is this classified as?

Virus total classified this file as a trojan


d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec



50
167

?
Community Score

50 security vendors and 1 sandbox flagged this file as malicious

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

GoogleIupdate.exe

invalid-signature overlay pedl signed spreader

549.84 KB Size

2022-03-09 01:38:24 UTC 1 day ago

DLL

DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY

Ad-Aware	Trojan.Mint.Zamg.O	AhnLab-V3	Malware/Win32.RL_Generic.R346613
Alibaba	TrojanSpy:Win32/Yakes.0454a340	ALYac	Trojan.Mint.Zamg.O
Antiy-AVL	Trojan/Generic.ASCommon.1BE	Arcabit	Trojan.Mint.Zamg.O
Avast	Win32:DangerousSig [Trj]	AVG	Win32:DangerousSig [Trj]

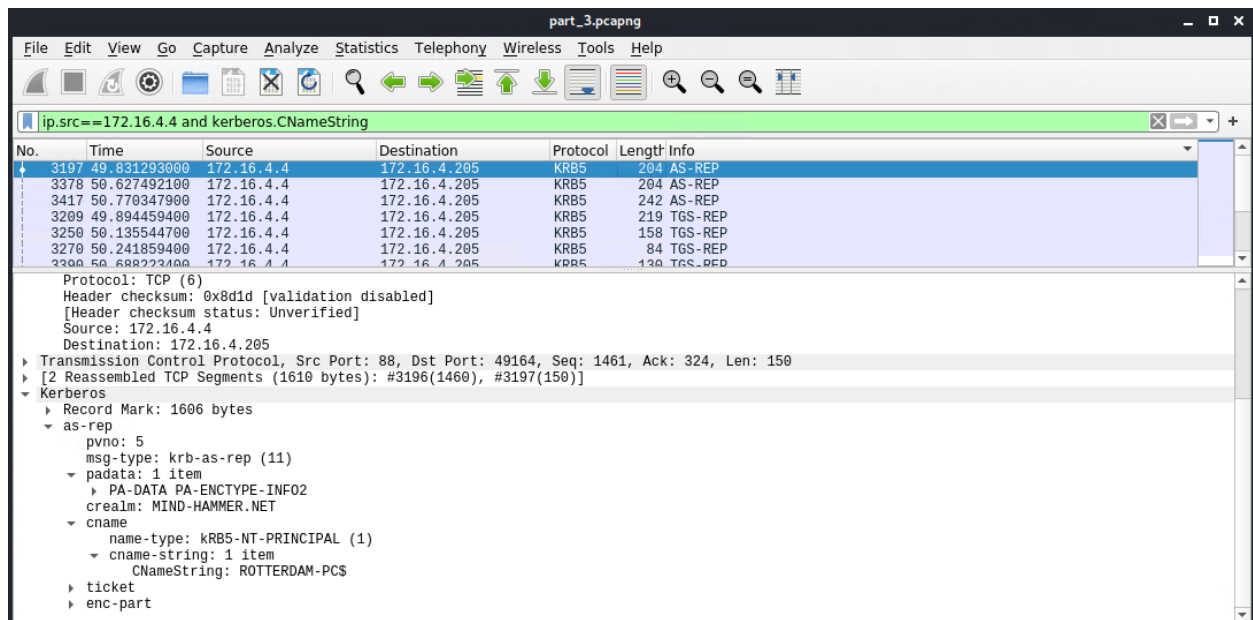
Vulnerable Windows Machines

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.

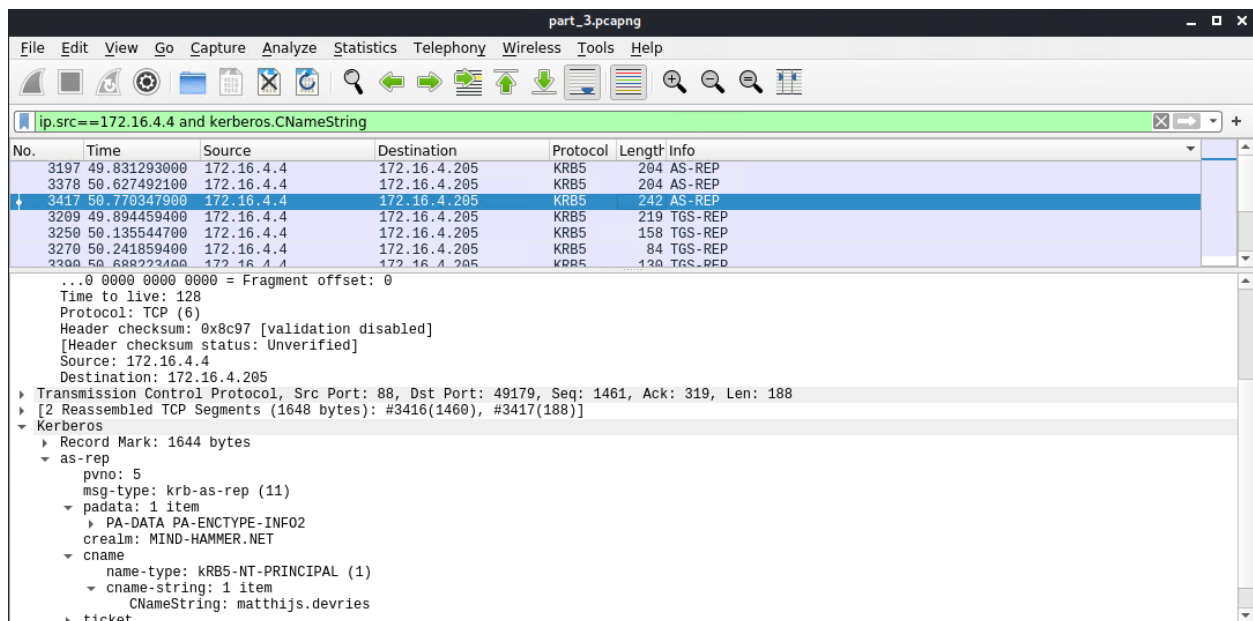
Inspect your traffic to answer the following questions:

- 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?

172.16.4.205, 185.243.115.84, 166.62.11.64

Wireshark - Conversations - part_3.pcapng

Ethernet · 74IPv4 · 877IPv6 · 1TCP · 1044UDP · 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	
172.16.4.205	185.243.115.84	30,344	26 M	15,149	9,831 k	15,195	16 M	196.154314	1016.8611		
172.16.111.64	172.16.4.205	15,728	16 M	11,354	15 M	4,374	321 k	51.161259	1001.6762		
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		
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		
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		
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		
172.16.4.4	172.16.4.205	1,417	339 k	680	147 k	737	191 k	49.776799	1144.3125		
10.6.12.12	10.6.12.203	1,388	350 k	620	161 k	768	188 k	644.343994	99.1499		
10.6.12.12	10.6.12.157	1,316	330 k	608	156 k	708	174 k	641.057369	102.3674		
10.11.11.11	10.11.11.200	1,100	219 k	493	98 k	607	120 k	464.078707	176.9288		
10.0.0.2	10.0.0.201	1,083	266 k	520	133 k	563	132 k	743.519241	89.6854		
10.11.11.200	104.18.74.113	1,079	697 k	511	34 k	568	662 k	616.230265	22.4916		
10.11.11.11	10.11.11.203	843	189 k	351	83 k	492	106 k	468.330519	172.6836		
10.11.11.179	13.33.255.25	728	520 k	339	34 k	389	485 k	475.419836	94.0159		
31.13.70.52	172.16.4.205	726	479 k	436	447 k	290	31 k	62.702930	989.8205		
93.95.100.178	172.16.4.205	722	419 k	418	391 k	304	28 k	116.562981	937.4512		
10.11.11.217	172.217.6.162	697	404 k	341	35 k	356	369 k	530.894213	106.4835		
10.6.12.203	205.185.125.104	647	599 k	185	10 k	462	588 k	658.615057	79.8144		

☐ Name resolution☐ Limit to display filter☐ Absolute start time

Conversation Types ▾

Copy ▾Follow Stream...Graph...

CloseHelp

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:

- 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
 - Host Name: BLANCO-DESKTOP

part_3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src==10.0.0.201 and kerberos.CNameString

No.	Time	Source	Destination	Protocol	Length	Info
65505	743.708498600	10.0.0.201	10.0.0.2	KRB5	301	AS-REQ
65520	743.828382900	10.0.0.201	10.0.0.2	KRB5	301	AS-REQ
65530	743.836192200	10.0.0.201	10.0.0.2	KRB5	301	AS-REQ

Source: Msi_18:66:c8 (00:16:17:18:66:c8)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.0.201, Dst: 10.0.0.2
Transmission Control Protocol, Src Port: 49677, Dst Port: 88, Seq: 1, Ack: 1, Len: 327
Kerberos
Record Mark: 323 bytes
as-req
pvno: 5
msg-type: krb-as-req (10)
padata: 2 items
req-body
padding: 0
kdc-options: 40810010
cname
name-type: KRB5-NT-PRINCIPAL (1)
cname-string: 1 item
CNameString: blanco-desktop\$
realm: DOGOFtheyear.NET
sname
till: 2037-09-13 02:48:05 (UTC)
rtime: 2037-09-13 02:48:05 (UTC)
nonce: 2063583424
etype: 6 items
addresses: 1 item BLANCO-DESKTOP<20>

2. Which torrent file did the user download?

****Betty_Boop_Rythm_on_the_Reservation.avi.torrent**

part_3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==10.0.0.201 and http.request.method==GET

No.	Time	Source	Destination	Protocol	Length	Info
68717	763.828818000	10.0.0.201	72.21.91.29	HTTP	288	GET /MFewTzBNMEswSTAJBgUrdgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgF...
77816	833.561991600	10.0.0.201	72.21.91.29	HTTP	288	GET /MFewTzBNMEswSTAJBgUrdgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgF...
77820	833.569289700	10.0.0.201	72.21.91.29	HTTP	290	GET /MFewTzBNMEswSTAJBgUrdgMCGgUABBTBL0V27RVZ7L8duom%2FnYB45SP...
77843	833.798402300	10.0.0.201	72.21.91.29	HTTP	292	GET /MFewTzBNMEswSTAJBgUrdgMCGgUABBTnvAI%2FnN49qPTJY2qT0tfkLxJ...
70010	771.307842200	10.0.0.201	168.215.195.227	HTTP	434	/announce?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%
69754	770.572697300	10.0.0.201	91.189.95.21	HTTP	423	/announce?info_hash=%e4%be%9eM%b8v%e3%e3%17%97%xb0%3e%90b%
69900	771.231145500	10.0.0.201	168.215.194.14	HTTP	434	/bt/announce.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee...
69706	770.366956400	10.0.0.201	168.215.194.14	HTTP	589	/bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on...
70122	771.590958400	10.0.0.201	168.215.194.14	HTTP	253	/bt/scrape.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%
69213	765.837950500	10.0.0.201	168.215.194.14	HTTP	405	/divx1.jpg 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)
Destination: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
Source: Msi_18:66:c8 (00:16:17:18:66:c8)
Type: IPv4 (0x0800)
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 Safari/537.36 Edge/17.1713...
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