

Network Analysis

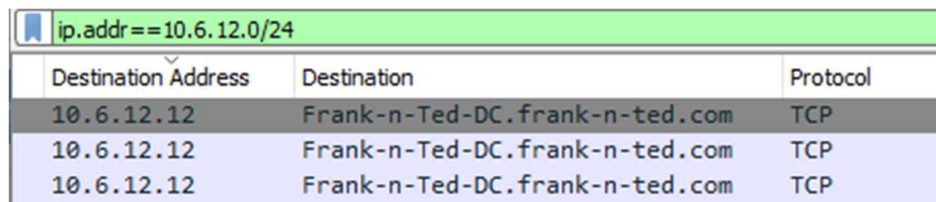
Time Thieves

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:

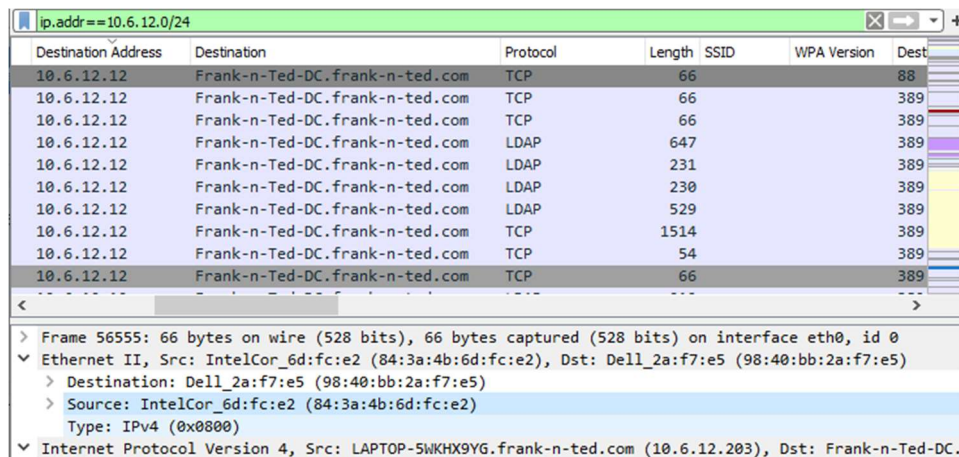
1. What is the domain name of the users' custom site?
 - a. Frank-n-Ted-DC.frank-n-ted.com
 - i. Filter used = ip.addr == 10.6.12.0/24



A screenshot of the Wireshark packet list pane. The filter bar at the top shows 'ip.addr == 10.6.12.0/24'. The list contains three entries, all with destination IP 10.6.12.12 and destination 'Frank-n-Ted-DC.frank-n-ted.com' using the TCP protocol.

Destination Address	Destination	Protocol
10.6.12.12	Frank-n-Ted-DC.frank-n-ted.com	TCP
10.6.12.12	Frank-n-Ted-DC.frank-n-ted.com	TCP
10.6.12.12	Frank-n-Ted-DC.frank-n-ted.com	TCP

2. What is the IP address of the Domain Controller (DC) of the AD network?
 - a. IP address is 10.6.12.12
 - i. Filter used = ip.addr == 10.6.12.0/24
 - ii. Internet Protocol



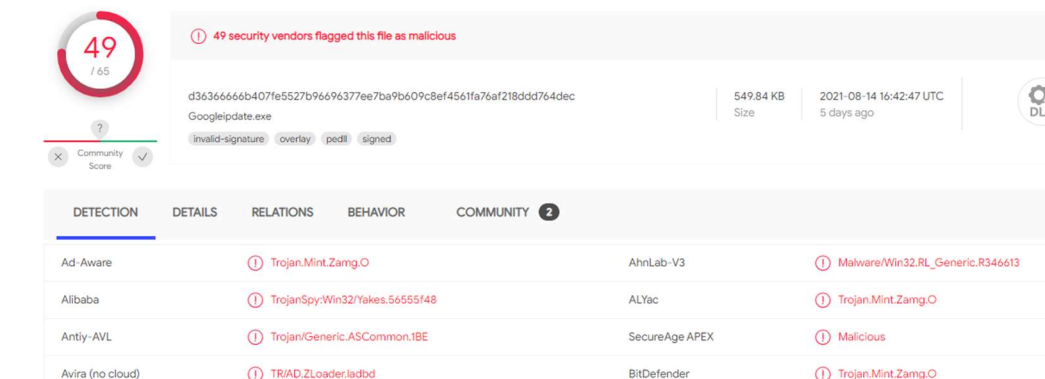
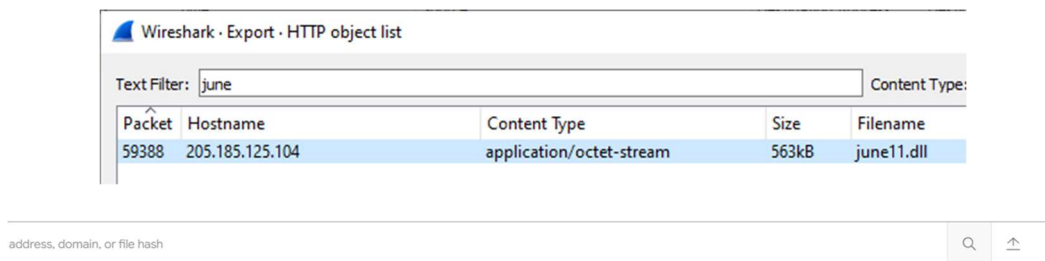
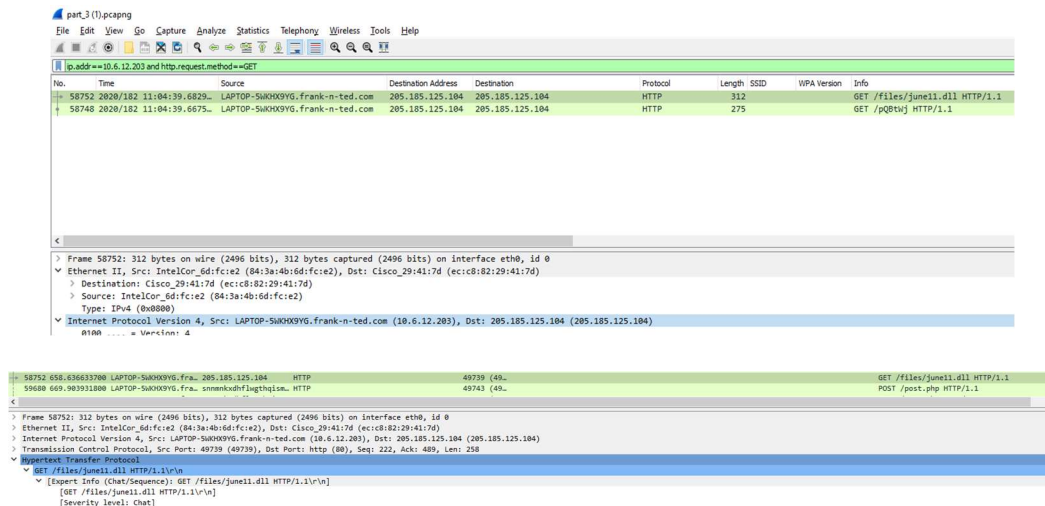
A screenshot of the Wireshark interface showing a packet list and its details. The filter bar shows 'ip.addr == 10.6.12.0/24'. The packet list shows multiple entries to 'Frank-n-Ted-DC.frank-n-ted.com' using TCP and LDAP. The details pane for the selected packet shows Ethernet II and Internet Protocol Version 4 information.

Destination Address	Destination	Protocol	Length	SSID	WPA Version	Dest
10.6.12.12	Frank-n-Ted-DC.frank-n-ted.com	TCP	66			88
10.6.12.12	Frank-n-Ted-DC.frank-n-ted.com	TCP	66			389
10.6.12.12	Frank-n-Ted-DC.frank-n-ted.com	TCP	66			389
10.6.12.12	Frank-n-Ted-DC.frank-n-ted.com	LDAP	647			389
10.6.12.12	Frank-n-Ted-DC.frank-n-ted.com	LDAP	231			389
10.6.12.12	Frank-n-Ted-DC.frank-n-ted.com	LDAP	230			389
10.6.12.12	Frank-n-Ted-DC.frank-n-ted.com	LDAP	529			389
10.6.12.12	Frank-n-Ted-DC.frank-n-ted.com	TCP	1514			389
10.6.12.12	Frank-n-Ted-DC.frank-n-ted.com	TCP	54			389
10.6.12.12	Frank-n-Ted-DC.frank-n-ted.com	TCP	66			389

Details of the selected packet (Frame 56555):

- Ethernet II, Src: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2), Dst: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5)
 - Destination: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5)
 - Source: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2)
 - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203), Dst: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12)

3. What is the name of the malware downloaded to the 10.6.12.203 machine?
 - a. File name: "june11.dll"
 - i. Filter used = ip.addr==10.16.12.203 and http.request.method==GET
 1. Export Process:
 - a. File > Export Objects > HTTP
 - b. Once you have found the file, export it to your Kali machine's desktop.
 - i. Upload the file to [VirusTotal.com](https://www.virustotal.com).
4. What kind of malware is this classified as?
 - a. Trojan



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
 - i. Filter used = ip.addr==172.16.4.0/24 and !ip.addr==172.16.4.4

Filter: ip.addr==172.16.4.0/24 and !ip.addr==172.16.4.4

No.	Time	Source	Destination Address	Destination
13003	2020/182 10:56:57.1985...	Rotterdam-PC.mind-hammer.net	54.230.89.184	d3ar2nimg19ie1.cloudfront.net
13004	2020/182 10:56:57.1995...	d3ar2nimg19ie1.cloudfront.net	172.16.4.205	Rotterdam-PC.mind-hammer.net
13005	2020/182 10:56:57.2006...	Rotterdam-PC.mind-hammer.net	185.243.115.84	b5689023.green.mattingsolutions.
13006	2020/182 10:56:57.2016...	d3ar2nimg19ie1.cloudfront.net	172.16.4.205	Rotterdam-PC.mind-hammer.net
13007	2020/182 10:56:57.2027...	b5689023.green.mattingsolutions...	172.16.4.205	Rotterdam-PC.mind-hammer.net
13008	2020/182 10:56:57.2037...	Rotterdam-PC.mind-hammer.net	185.243.115.84	b5689023.green.mattingsolutions.
13009	2020/182 10:56:57.2124...	Rotterdam-PC.mind-hammer.net	185.243.115.84	b5689023.green.mattingsolutions.
13010	2020/182 10:56:57.2144...	Rotterdam-PC.mind-hammer.net	185.243.115.84	b5689023.green.mattingsolutions.
13011	2020/182 10:56:57.2154...	Rotterdam-PC.mind-hammer.net	54.230.89.184	d3ar2nimg19ie1.cloudfront.net
13012	2020/182 10:56:57.2164...	d3ar2nimg19ie1.cloudfront.net	172.16.4.205	Rotterdam-PC.mind-hammer.net
13013	2020/182 10:56:57.2174...	Rotterdam-PC.mind-hammer.net	54.230.89.184	d3ar2nimg19ie1.cloudfront.net

Frame 13014: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: Cisco_e6:c4:77 (00:15:c6:e6:c4:77), Dst: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
Destination: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)

Filter: ip.addr == 172.16.4.205 && bootp

No.	Time	Source	Destination	Protocol	Tag
23687	335.628617000	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	DHCP	
1025...	1187.3371614...	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	DHCP	
31783	461.405481600	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	DHCP	

0... .. = Broadcast flag: Unicast
.000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: Rotterdam-PC.mind-hammer.net (172.16.4.205)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 0.0.0.0 (0.0.0.0)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
Client hardware address padding: 00000000000000000000

2. What is the username of the Windows user whose computer is infected?
 - Matthijs.devries
 - i. Filter used = ip.src==172.16.4.4 and kerberos.CNamesString
 - 1. Right Click > Follow > TCP Stream

Wireshark · Follow TCP Stream (tcp.stream eq 25) · part_3 (1).pcapng

```

...:j..60..2.....
.c0a0L.....E.C0A.....:8...<.V.6./.P.....X..
...1..eK..5...X..xz...Q%...?;0.....@.....
0.....0...matthijs.devries.
..MIND-HAMMER. 0.....0...krbtgt..MIND-HAMMER....20370913024805Z....
20370913024805Z....%.WR..0.....y.....0.0.....ROTTERDAM-PC
...lk..h0..d.....90705.....0*0(.....!..MIND-
HAMMER.NETmatthijs.devries...MIND-HAMMER.NET..0.....0...matthijs.devries...a..
0..|.....MIND-HAMMER.NET.$0".....0...krbtgt..MIND-HAMMER.NET...:0..6.....

```

ip.src==172.16.4.4 and kerberos.CNameString

No.	Time	Source	Destination Address	Destination
3197	2020/182 10:54:30.8776...	mind-hammer-dc.mind-hammer.net	172.16.4.205	Rotterdam-PC.mind-hammer.net
3209	2020/182 10:54:30.9407...	mind-hammer-dc.mind-hammer.net	172.16.4.205	Rotterdam-PC.mind-hammer.net
3250	2020/182 10:54:31.1818...	mind-hammer-dc.mind-hammer.net	172.16.4.205	Rotterdam-PC.mind-hammer.net
3270	2020/182 10:54:31.2881...	mind-hammer-dc.mind-hammer.net	172.16.4.205	Rotterdam-PC.mind-hammer.net
3378	2020/182 10:54:31.6738...	mind-hammer-dc.mind-hammer.net	172.16.4.205	Rotterdam-PC.mind-hammer.net
3390	2020/182 10:54:31.7345...	mind-hammer-dc.mind-hammer.net	172.16.4.205	Rotterdam-PC.mind-hammer.net

Wireshark · Conversations · part_3 (1).pcapng

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	P
Rotterdam-PC.mind-hammer.net	b5689023.green.mattingsolutions.co	30,344	26M	15,149	9831k	15,195	16M	196
mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	15,728	16M	11,354	15M	4,374	321k	51
BLANCO-DESKTOP.dogoftheyear.net	a1449.dscg2.akamai.net	6,934	7045k	2,282	124k			

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

- Address A = 172.16.4.205 | Address B = 185.243.115.84 (30,344 Packets)
- Address A = 166.62.111.64 | Address B = 172.16.4.205 (15,728 Packets)
 - i. Filter used = ip.addr==172.16.4.205 and ip.addr==185.243.115.84
 - ii. Expose Infected Traffic Process:
 - 1. Statistics > Conversations > IPv4 > Packets (descending)

Wireshark · Conversations · part_3 (1).pcapng

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
172.16.4.205	185.243.115.84	30,344	26M	15,149	9831k	15,195	16M	196	154314 1016.8611
166.62.111.64	172.16.4.205	15,728	16M	11,354	15M	4,374	321k	51	161259 1001.6762

- Suspicious Activity:
 - i. IP address 185.234.115.84 | Domain b569023.green.mattingsolutions.co
 - ii. A large amount of http.request.method=="POST" found but did not find an origination http.request.method=="GET"
 - iii. IP address 185.234.115.84 was trying to "POST" file named "empty.gif"

http.request.method=="POST"

	Destination Address	Destination	Proto	Length	Info
r.net	166.62.111.64	mysocalledchaos.com	HTTP	661	POST /wp-admin/admin-ajax.php HTTP/1.1 (app
r.net	185.243.115.84	b5689023.green.mattingsolutions...	HTTP	126	POST /empty.gif HTTP/1.1 (application/x-www
r.net	185.243.115.84	b5689023.green.mattingsolutions...	HTTP	534	POST /empty.gif HTTP/1.1 (application/x-www
r.net	185.243.115.84	b5689023.green.mattingsolutions...	HTTP	326	POST /empty.gif HTTP/1.1 (application/x-www
r.net	185.243.115.84	b5689023.green.mattingsolutions...	HTTP	496	POST /empty.gif?ss&ss1img HTTP/1.1 (PNG)
r.net	185.243.115.84	b5689023.green.mattingsolutions...	HTTP	1366	POST /empty.gif?ss&ss2img HTTP/1.1 (PNG)

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:
 - MAC address 00:16:17:18:66:c8
 - Windows username elmer.blanco
 - Computer Host Name BLANCO-DESKTOP\$
 - i. Filter used = ip.addr==10.0.0.201 && bootp

ip.addr == 10.0.0.201 && bootp					
No.	Time	Source	Destination	Protocol	Tag
65434	743.509344200	10.0.0.1	BLANCO-DESKTOP.dogo...	DHCP	
0... .. = Broadcast flag: Unicast					
.000 0000 0000 0000 = Reserved flags: 0x0000					
Client IP address: 0.0.0.0 (0.0.0.0)					
Your (client) IP address: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201)					
Next server IP address: 10.0.0.1 (10.0.0.1)					
Relay agent IP address: 0.0.0.0 (0.0.0.0)					
Client MAC address: Msi_18:66:c8 (00:16:17:18:66:c8)					

2. Which torrent file did the user download?
 - Betty_Boop_Rythm_on_the_Reservation.avi.torrent
 - i. Filter used = ip.addr==10.0.0.201 and (http.request.uri contains ".torrent")

ip.addr == 10.0.0.201 and http.request.method == "GET" and http.request.uri contains ".torrent"					
Time	Source	Destination Address	Destination	Protocol	
69786.2928/182.11:06:31.4132..	BLANCO-DESKTOP.dogoftheyear.net	168.215.194.14	files.publicdomaintorrents.com	HTTP	
[Time since first frame in this TCP stream: 0.012269100 seconds]					
[Time since previous frame in this TCP stream: 0.009429400 seconds]					
TCP payload (535 bytes)					
Hypertext Transfer Protocol					
GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n					
[Expert Info (Chat/Sequence): GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rythm_on_the_Reservation.avi.t					
Request Method: GET					
Request URI: /bt/btdownload.php?type=torrent&file=Betty_Boop_Rythm_on_the_Reservation.avi.torrent					
Request URI Path: /bt/btdownload.php					
Request URI Query: type=torrent&file=Betty_Boop_Rythm_on_the_Reservation.avi.torrent					
Request URI Query Parameter: type=torrent					
Request URI Query Parameter: file=Betty_Boop_Rythm_on_the_Reservation.avi.torrent					
350	65 3d 74 6f 72 72 65 6e 74 26 06 09 6c 65 3d 42	e=torrent&file=			
360	65 74 79 5f 42 6f 6f 70 5f 52 68 79 74 68 6d	Betty_Boop_Rythm			
370	5f 6f 6e 5f 74 68 65 5f 52 65 73 65 72 76 61 7a	on_the_Reservation			
380	60 6f 6e 2a 63 76 69 3e 74 6f 72 72 65 6e 2a 79	on.avi.torrent			
390	48 54 54 50 2f 31 2e 31 0d 0a 52 65 66 65 72 65	HTTP/1.1 ..Refere			