

# Network Analysis

## Time Thieves

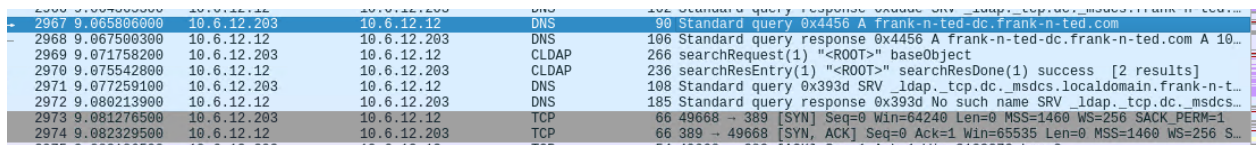
At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- 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**



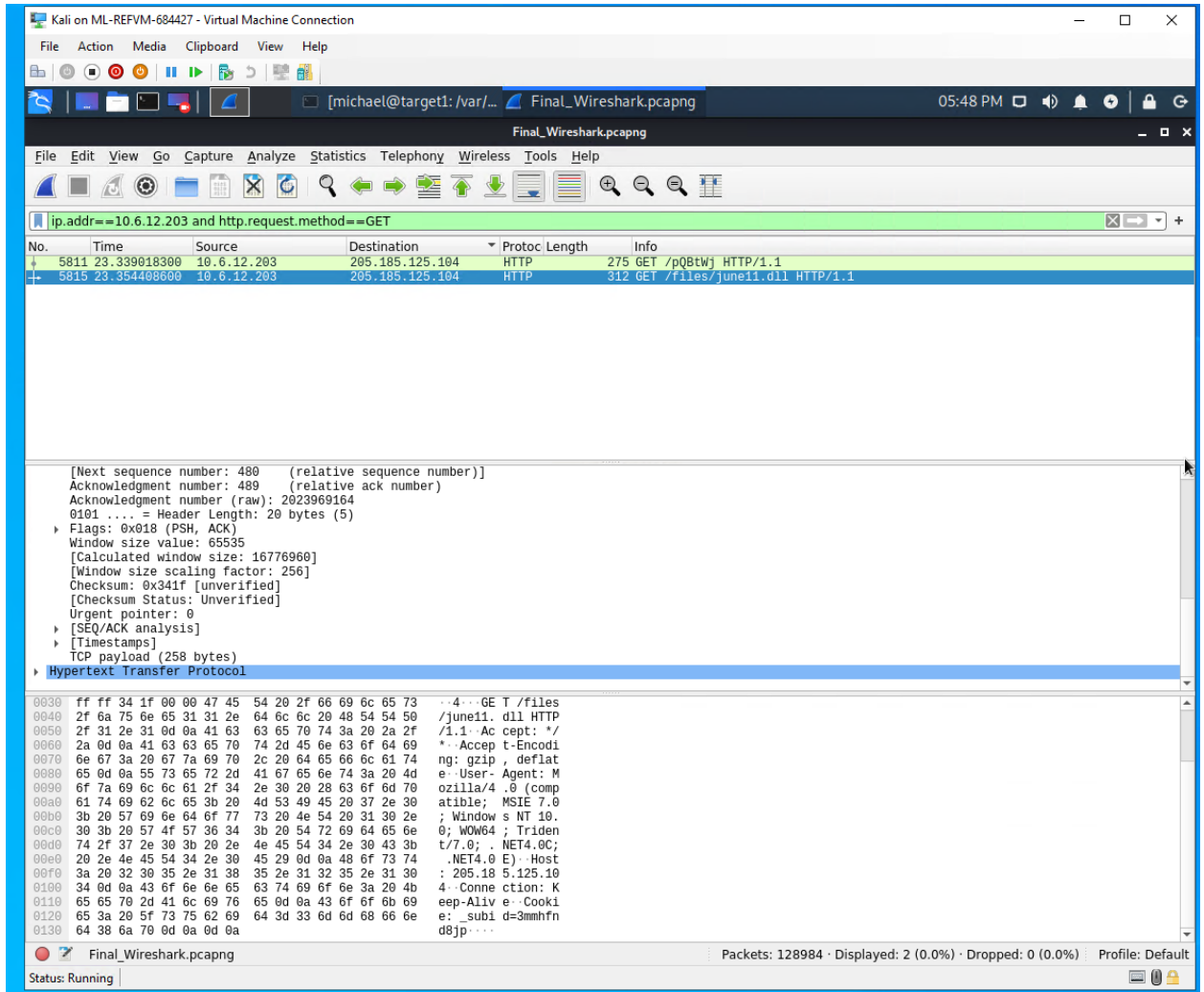
2967	9.065806000	10.6.12.203	10.6.12.12	DNS	90 Standard query response 0x4456 A frank-n-ted-dc.frank-n-ted.com
2968	9.067500300	10.6.12.12	10.6.12.203	DNS	106 Standard query response 0x4456 A frank-n-ted-dc.frank-n-ted.com A 10...
2969	9.071758200	10.6.12.203	10.6.12.12	LDAP	266 searchRequest(1) "<R00T>" baseObject
2970	9.075542800	10.6.12.12	10.6.12.203	LDAP	236 searchResEntry(1) "<R00T>" searchResDone(1) success [2 results]
2971	9.077259100	10.6.12.203	10.6.12.12	DNS	108 Standard query 0x393d SRV _ldap._tcp.dc._msdcs.localdomain.frank-n-t...
2972	9.080213900	10.6.12.12	10.6.12.203	DNS	185 Standard query response 0x393d No such name SRV _ldap._tcp.dc._msdcs...
2973	9.081276500	10.6.12.203	10.6.12.12	TCP	66 49668 → 389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2974	9.082329500	10.6.12.12	10.6.12.203	TCP	66 389 → 49668 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 S...

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

**10.6.12.12**

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**



The image shows a Wireshark capture of an HTTP GET request. The filter is set to `ip.addr==10.6.12.203 and http.request.method==GET`. The packet list shows a GET request from 10.6.12.203 to 205.185.125.104 for the file `/files/june11.dll`. The packet details pane shows the following information:

- [Next sequence number: 480 (relative sequence number)]
- Acknowledgment number: 489 (relative ack number)
- Acknowledgment number (raw): 2023969164
- 0101 .... = Header Length: 20 bytes (5)
- Flags: 0x018 (PSH, ACK)
- Window size value: 65535
- [Calculated window size: 16776960]
- [Window size scaling factor: 256]
- Checksum: 0x341f [unverified]
- [Checksum Status: Unverified]
- Urgent pointer: 0
- [SEQ/ACK analysis]
- [Timestamps]
- TCP payload (258 bytes)
- Hypertext Transfer Protocol

The packet bytes pane shows the raw data of the HTTP request, including the GET method and the file path `/files/june11.dll`.

4. Upload the file to [VirusTotal.com](https://www.virustotal.com). What kind of malware is this classified as?  
**This particular malware is a trojan.**

53 / 68

53 security vendors flagged this file as malicious

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

549.84 KB Size

2021-08-24 01:32:27 UTC 1 day ago

GoogleIupdate.exe

invalid-signature overlay pedll signed

Community Score

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	Trojan.Mint.Zamg.O	AhnLab-V3	Malware/Win32.RL_Generic.R346613	
Alibaba	TrojanSpy:Win32/Yakes.56555f48	ALYac	Trojan.Mint.Zamg.O	
Antiy-AVL	Trojan/Generic.ASCommon.1BE	SecureAge APEX	Malicious	
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.34088.lu9@aul7OQgi	
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cylance	Unsafe	
Cyren	Malicious (score: 100)	Cyren	W32/Trojan.SIAQ-3008	

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

Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

[michael@target1: /var/... Final\_Wireshark.pcapng Wireshark - Export - HTTP 06:25 PM

Final\_Wireshark.pcapng

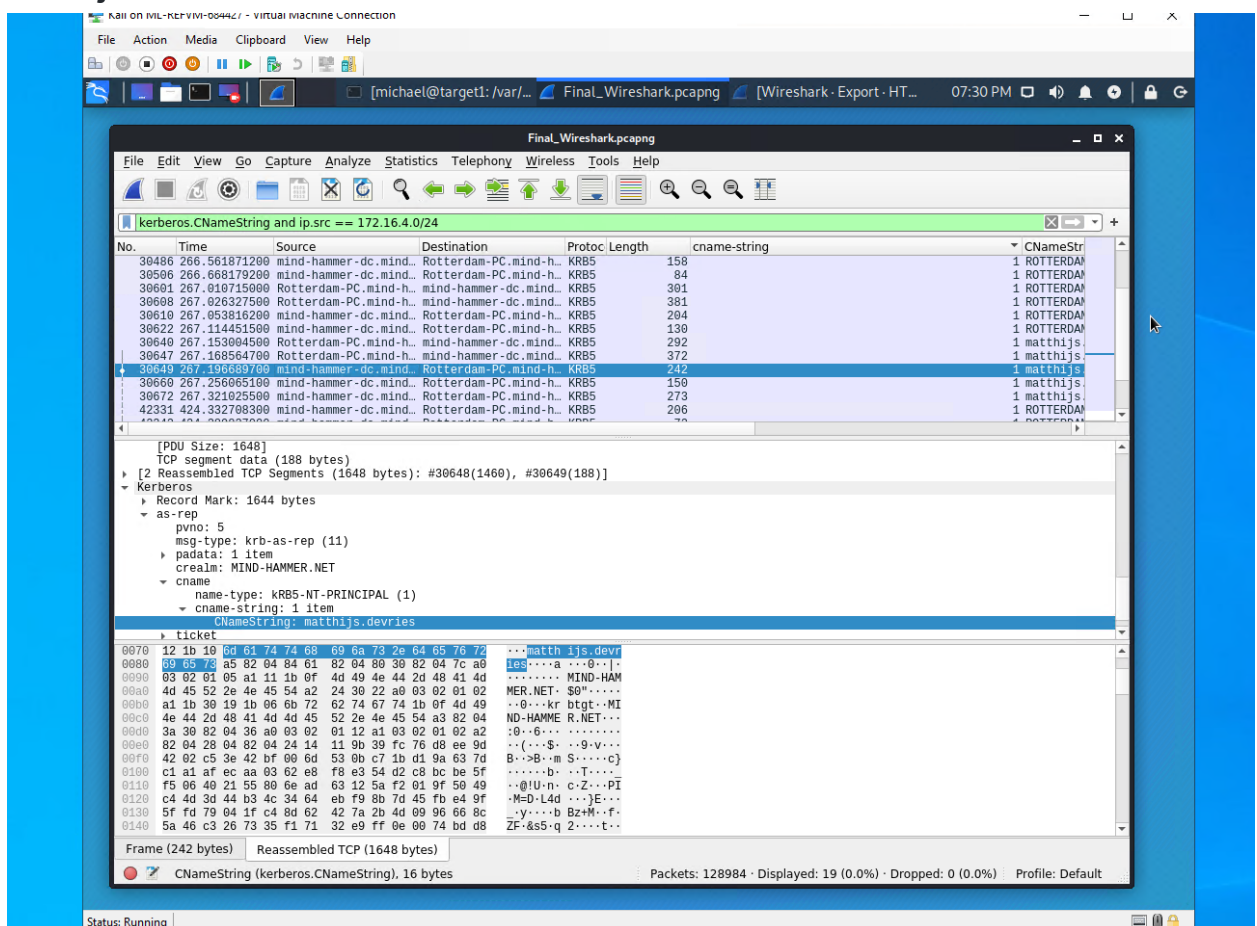
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==172.16.4.0/24

No.	Time	Source	Destination	Protocol	Length	Info
30828	267.908238700	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	DNS	82	Standard query 0xf71a A cds.j3z9t3p6.hwcdn.net
30829	267.909819200	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	DNS	98	Standard query response 0xf71a A cds.j3z9t3p6.hwcdn.net A 209.197.3...
30832	267.911924100	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	DNS	132	Standard query response 0xc7d6 A fonts.googleapis.com CNAME googlead...
30833	267.913240300	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	DNS	83	Standard query 0x3a0f A code.ionicframework.com
30834	267.915077400	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	DNS	115	Standard query response 0x3a0f A code.ionicframework.com A 104.25.12...
30835	267.917979300	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	DNS	181	Standard query response 0x737e A a.mailmunch.co CNAME d3ar2nimg19ie1...
30836	267.919338500	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	DNS	85	Standard query 0x1cb8 A googleapis.l.google.com
30837	267.921001500	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	DNS	101	Standard query response 0x1cb8 A googleapis.l.google.com A 216.58...
30838	267.922380500	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	DNS	89	Standard query 0x0cc2 A d3ar2nimg19ie1.cloudfront.net
30839	267.924836600	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	DNS	153	Standard query response 0x0cc2 A d3ar2nimg19ie1.cloudfront.net A 54...
30840	267.928669600	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	DNS	240	Standard query response 0xb297 A assets.pinterest.com CNAME s.pinimg...
30841	267.930170000	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	DNS	94	Standard query 0x403d A dualstack.pinterest.map.fastly.net
30842	267.931935300	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	DNS	110	Standard query response 0x403d A dualstack.pinterest.map.fastly.net ...
30843	267.933100100	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	DNS	73	Standard query 0x306f A www.dwin2.com

► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 81  
Identification: 0x0ce8 (3304)  
► Flags: 0x0000  
...0 0000 0000 0000 = Fragment offset: 0  
Time to live: 128  
Protocol: UDP (17)  
Header checksum: 0xc0c2 [validation disabled]  
[Header checksum status: Unverified]  
Source: mind-hammer-dc.mind-hammer.net (172.16.4.4)  
Destination: Rotterdam-PC.mind-hammer.net (172.16.4.205)  
► User Datagram Protocol, Src Port: 53, Dst Port: 51725  
▼ Domain Name System (response)  
Transaction ID: 0x1a22  
► Flags: 0x8180 Standard query response, No error  
Questions: 1

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, and 162.62.111.64** there is an abnormally high packet transfer between these ips that stands out.

Wireshark · Conversations · Final_Wireshark.pcapng							
Ethernet · 85		IPv4 · 883		IPv6 · 7	TCP · 1129	UDP · 1837	
Address A	Address B	Packets	Bytes		Packets A → B	Bytes A → B	Packets B → A
172.16.4.205	185.243.115.84	22,018	19 M		11,243	8,093 k	10,775
166.62.111.64	172.16.4.205	15,728	16 M		11,354	15 M	4,374
10.0.0.201	64.187.66.143	9,376	6,986 k		4,296	278 k	5,080

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



## 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**
- OS version **Windows NT 10.0; Win64; x 64**

Ethernet II, Src: Dell\_f4:3b:96 (00:12:3f:f4:3b:96), Dst: Msi\_18:66:c8 (00:16:17:18:66:c8)  
 Destination: Msi\_18:66:c8 (00:16:17:18:66:c8)

Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

Final\_Wireshark.pcapng root - File Manager 07:12 AM

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==172.16.4.205 && ip.addr==185.243.115.84

Protoc	Length	cname-string	CNameString	Info
en.matt...	HTTP	326		POST /empty.gif HTTP/1.1 (application/x-www-form-urlencoded)
mind-h...	TCP	54		80 → 49249 [ACK] Seq=8227236 Ack=21031 Win=75776 Len=0
mind-h...	TCP	54		80 → 49249 [ACK] Seq=8227236 Ack=21031 Win=78464 Len=0
mind-h...	HTTP	341		HTTP/1.1 200 OK
en.matt...	TCP	60		49249 → 80 [ACK] Seq=21303 Ack=8227523 Win=648448 Len=0
en.matt...	TCP	512		49249 → 80 [PSH, ACK] Seq=21303 Ack=8227523 Win=648448 Len=4...
en.matt...	TCP	1411		49249 → 80 [ACK] Seq=21761 Ack=8227523 Win=648448 Len=1357 [...]
en.matt...	TCP	1411		49249 → 80 [ACK] Seq=23118 Ack=8227523 Win=648448 Len=1357 [...]
en.matt...	TCP	1411		49249 → 80 [ACK] Seq=24475 Ack=8227523 Win=648448 Len=1357 [...]
en.matt...	TCP	1411		49249 → 80 [ACK] Seq=25832 Ack=8227523 Win=648448 Len=1357 [...]
en.matt...	TCP	1411		49249 → 80 [ACK] Seq=27189 Ack=8227523 Win=648448 Len=1357 [...]
en.matt...	TCP	1411		49249 → 80 [ACK] Seq=28546 Ack=8227523 Win=648448 Len=1357 [...]
en.matt...	TCP	1411		49249 → 80 [ACK] Seq=29903 Ack=8227523 Win=648448 Len=1357 [...]

Transmission Control Protocol, Src Port: 49824, Dst Port: 80, Seq: 1, Ack: 1, Len: 831

Hypertext Transfer Protocol

[truncated]GET /e/cm?t=publicdomain9f-20&o=1&p=48&l=op1&pvid=40C236A13FDD0B68&ref-url=http%3A//publicdomaintorrents.info/nshowmovie.html%3Fmovieid%3D...  
 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/17.17134\r\n  
 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



2. Which torrent file did the user download?

**Betty\_Boop\_Rythm\_on\_the\_Reservation.avi.torrent**

