

# Network Analysis

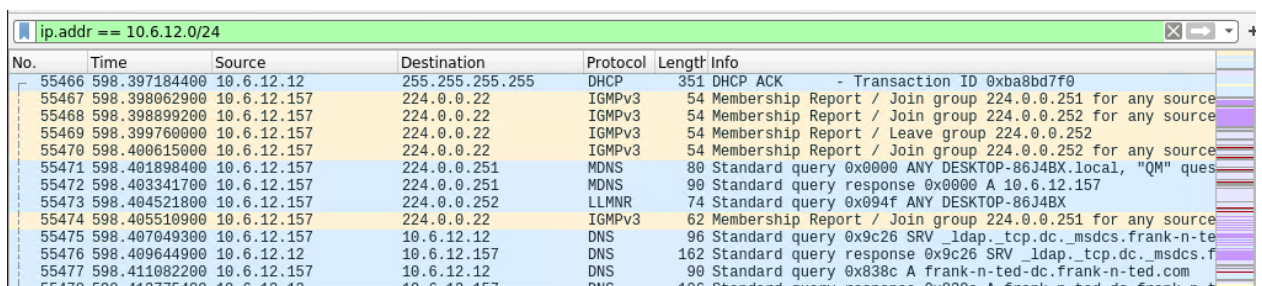
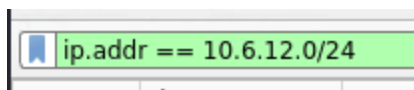
## Time Thieves

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**



No.	Time	Source	Destination	Protocol	Length	Info
55466	598.397184400	10.6.12.12	255.255.255.255	DHCP	351	DHCP ACK - Transaction ID 0xba8bd7f0
55467	598.398062900	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any source
55468	598.398899200	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any source
55469	598.399760000	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
55470	598.400615000	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any source
55471	598.401898400	10.6.12.157	224.0.0.251	MDNS	80	Standard query 0x0000 ANY DESKTOP-86J4BX.local, "QM" ques
55472	598.403341700	10.6.12.157	224.0.0.251	MDNS	90	Standard query response 0x0000 A 10.6.12.157
55473	598.404521800	10.6.12.157	224.0.0.252	LLMNR	74	Standard query 0x094f ANY DESKTOP-86J4BX
55474	598.405510900	10.6.12.157	224.0.0.22	IGMPv3	62	Membership Report / Join group 224.0.0.251 for any source
55475	598.407049300	10.6.12.157	10.6.12.12	DNS	96	Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-te
55476	598.409644900	10.6.12.12	10.6.12.157	DNS	162	Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.f
55477	598.411082200	10.6.12.157	10.6.12.12	DNS	90	Standard query 0x838c A frank-n-ted-dc.frank-n-ted.com
55478	598.412775400	10.6.12.12	10.6.12.157	DNS	106	Standard query response 0x838c A frank-n-ted-dc.frank-n-t

```
Domain Name Server: 10.6.12.12
Option: (15) Domain Name
Length: 16
Domain Name: frank-n-ted.com
Option: (255) End
```

2. What is the IP address of the Domain Controller (DC) of the AD network? **IP: 10.6.12.12**

```
Domain Name Server: 10.6.12.12
Option: (15) Domain Name
Length: 16
Domain Name: frank-n-ted.com
```

```

Internet Protocol Version 4, Src: 10.6.12.12, Dst: 255.255.255.255
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 337
    Identification: 0x3880 (14464)
  ▶ Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0xeb0a [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.6.12.12
    Destination: 255.255.255.255
User Datagram Protocol, Src Port: 67, Dst Port: 68

```

3. What is the name of the malware downloaded to the 10.6.12.203 machine?

Malware file is named june11.dll

Once you have found the file, export it to your Kali machine's desktop.

```

[Bytes sent since last PSH flag: 258]
[Timestamps]
  [Time since first frame in this TCP stream: 0.021714400 seconds]
  [Time since previous frame in this TCP stream: 0.005106200 seconds]
TCP payload (258 bytes)
Hypertext Transfer Protocol

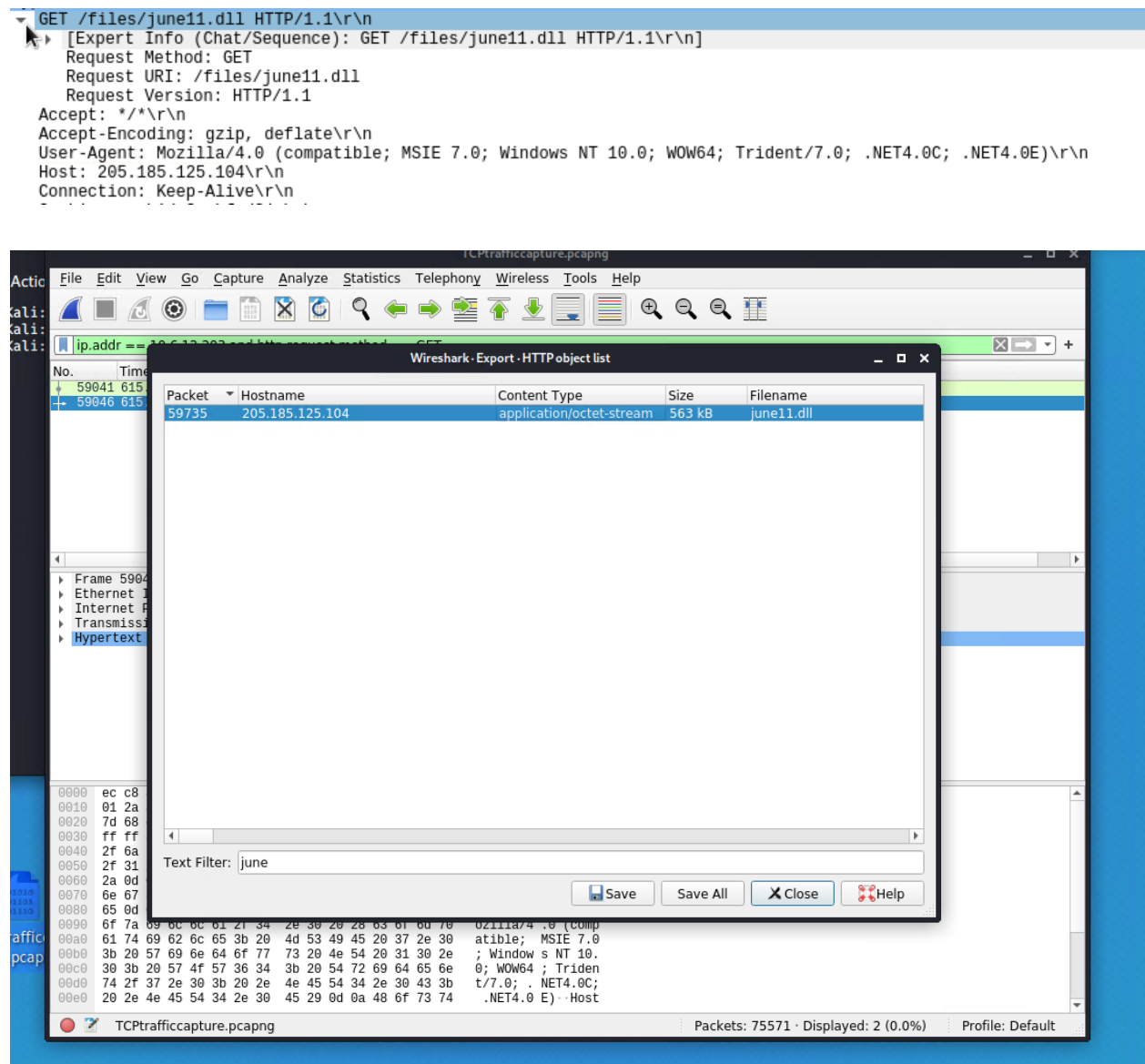
```

ip.addr == 10.6.12.203 and http.request.method == GET						
No.	Time	Source	Destination	Protocol	Length	Info
59041	615.970929300	10.6.12.203	205.185.125.104	HTTP	275	GET /pQBtWj HTTP/1.1
59046	615.986450000	10.6.12.203	205.185.125.104	HTTP	312	GET /files/june11.dll HTTP/1.1

```

TCP payload (258 bytes)
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
    Cookie: _subid=3mmhfnd8jp\r\n
  \r\n
  [Full request URI: http://205.185.125.104/files/june11.dll]
  [HTTP request 2/2]
  [Prev request in frame: 59041]
  [Response in frame: 59735]

```



4. Upload the file to [VirusTotal.com](https://www.virustotal.com). What kind of malware is this classified as? The type of malware is TROJAN.

55

170

?

Community Score

55 security vendors and 1 sandbox flagged this file as malicious

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

549.84 KB

2022-08-20 15:58:35 UTC

Googleipdate.exe

Size

12 minutes ago

invalid-signature overlay pedli signed spreader

DLL

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 5

Security Vendors' Analysis

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	GrayWare/Win32.Kryptik.ehls	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.34606.lu9@aul7OQgi	Bkav Pro	W32.AIDetect.malware2
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cylance	Unsafe
Cynet	Malicious (score: 100)	DrWeb	Trojan.Inject3.53106
Elastic	Malicious (high Confidence)	Emsisoft	Trojan.Mint.Zamg.O (B)
eScan	Trojan.Mint.Zamg.O	ESET-NOD32	Win32/Spy.Zbot.ADI
F-Secure	Trojan.TR/AD.ZLoader.ladbd	Fortinet	W32/Kryptik.DZZ!tr
GData	Trojan.Mint.Zamg.O	Google	Detected

## Vulnerable Windows Machines

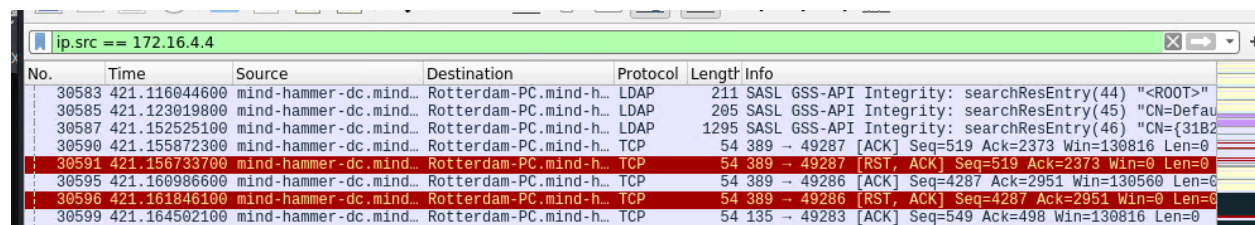
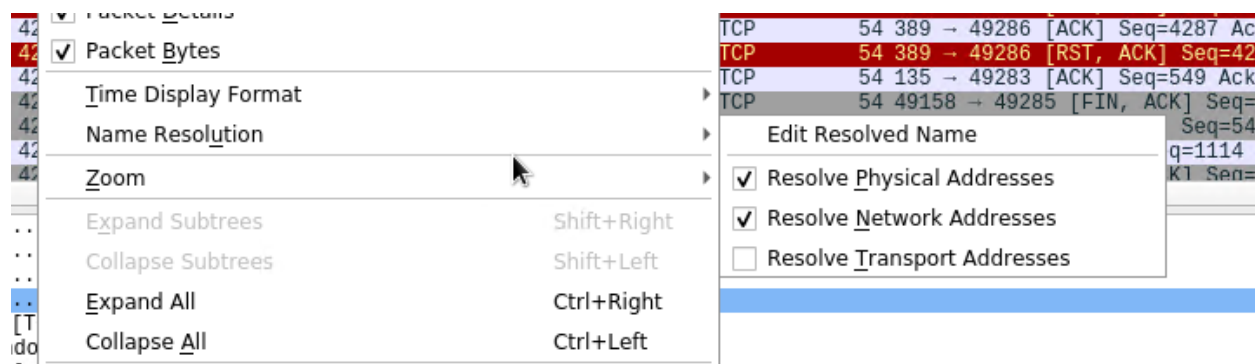
The Security team received reports of an infected Windows host on the network. They know the following:

- 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

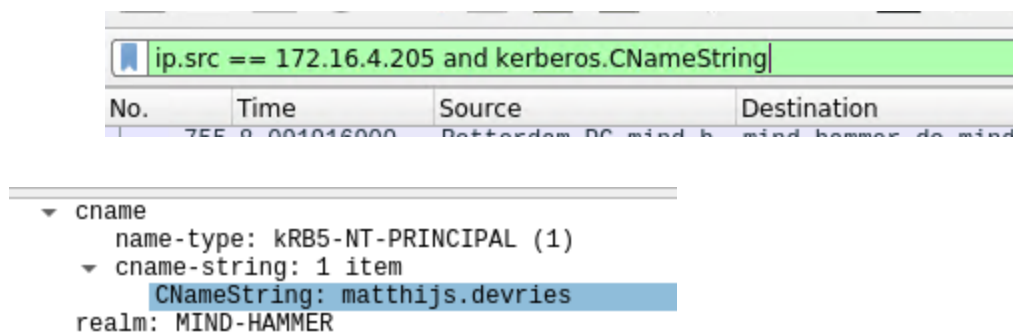


Destination: Rotterdam-PC.mind-hammer.net (172.16.4.205)

Address: LenovoEM\_b0:63:a4 (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? IP:172.16.4.205 is used in the actual infection of traffic.

However, other notable IPs connected to infected traffic are shown in the screenshot below.

Wireshark - Conversations - TCPtrafficcapture.pcapng

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start
31.7.62.214	172.16.4.205	114	32 k	0	0	114	32 k	294.18573
166.62.111.64	172.16.4.205	1	661	0	0	1	661	18.74317
172.16.4.205	185.243.115.84	5	2,848	5	2,848	0	0	153.51783

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



