

## Network Analysis (Wireshark)

### 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 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.

It would help if you inspected your traffic capture to answer the following questions:

1. What is the domain name of the users' custom site?

**The domain name that was found was Frank-n-ted.com.**

No.	Time	Source	Destination	Protocol	Length	Info
70057	740.153992000	10.6.12.12	255.255.255.255	DHCP	351	DHCP ACK - Transaction ID 0xba8bd7f0
70058	740.154848600	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any sources
70059	740.155707300	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
70060	740.156571800	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
70061	740.157432600	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
70062	740.158715200	10.6.12.157	224.0.0.251	MDNS	80	Standard query 0x0000 ANY DESKTOP-86J4BX.local, "QM" question
70063	740.160159000	10.6.12.157	224.0.0.251	MDNS	90	Standard query response 0x0000 A 10.6.12.157
70064	740.161340800	10.6.12.157	224.0.0.252	LLNMR	74	Standard query 0x094f ANY DESKTOP-86J4BX
70065	740.162328600	10.6.12.157	224.0.0.22	IGMPv3	62	Membership Report / Join group 224.0.0.251 for any sources / Join group ...
70066	740.163864600	10.6.12.157	10.6.12.12	DNS	96	Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
70067	740.166459500	10.6.12.12	10.6.12.157	DNS	162	Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com ...
70068	740.167903000	10.6.12.157	10.6.12.12	DNS	90	Standard query response 0x838c A frank-n-ted-dc.frank-n-ted.com
70069	740.169599400	10.6.12.12	10.6.12.157	DNS	106	Standard query response 0x000c A frank-n-ted-dc.frank-n-ted.com A 10.6.1...
70070	740.173823200	10.6.12.157	10.6.12.12	CLDAP	264	searchRequest(1) "<R00T>" baseObject

Source: Dell 2a:f7:e5 (98:40:bb:2a:f7:e5)  
Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.6.12.12, Dst: 255.255.255.255

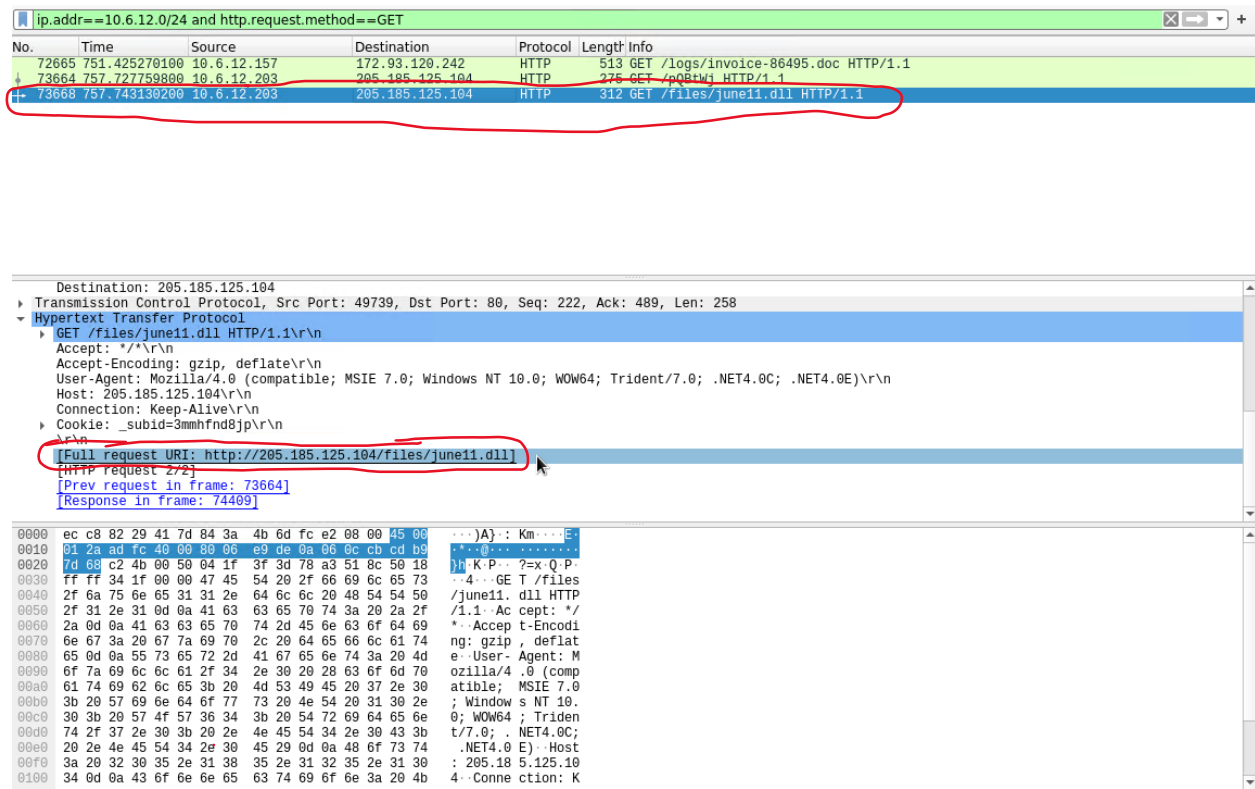
0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 337  
Identification: 0x3880 (14464)  
Flags: 0x0000  
...0 0000 0000 0000 = Fragment offset: 0  
Time to live: 128  
Protocol: UDP (17)  
Header checksum: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

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

**The IP Address of the Domain Controller of the AD network is 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.

The name of the malware that was downloaded was June11.dll.



The image displays a Wireshark packet capture interface. The top pane shows a list of network packets. The third packet, with No. 73664, is selected and highlighted in blue. It is an HTTP GET request from 10.6.12.203 to 205.185.125.104 for the file /files/june11.dll. A red circle highlights this packet in the list. The middle pane shows the details of the selected packet, specifically the Hypertext Transfer Protocol section. The 'Full request URI' field is highlighted with a red circle and contains the value 'http://205.185.125.104/files/june11.dll'. The bottom pane shows the raw packet data in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
72665	751.425270100	10.6.12.157	172.93.120.242	HTTP	513	GET /logs/invoice-86495.doc HTTP/1.1
73664	757.727759800	10.6.12.203	205.185.125.104	HTTP	275	GET /p08tWj HTTP/1.1
73668	757.743130200	10.6.12.203	205.185.125.104	HTTP	312	GET /files/june11.dll HTTP/1.1

Destination: 205.185.125.104  
Transmission Control Protocol, Src Port: 49739, Dst Port: 80, Seq: 222, Ack: 489, Len: 258  
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  
[Full request URI: http://205.185.125.104/files/june11.dll]  
[HTTP request 2/2]  
[Prev request in frame: 73664]  
[Response in frame: 74409]

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

After uploading this URL to the website, I was able to find that this kind of malware is spyware and malware.

VirusTotal - URL - e70c4

https://www.virustotal.com/gui/url/e70c46b564e2c7a9d38f0f94cbfafb2d30713

Kali LinuxKali TrainingKali ToolsKali DocsKali ForumsNetHunterOffensive SecurityExploit-DBGHDBMSFU

http://205.185.125.104/files/june11.dll

Sign inSign up

6

/ 93

Community Score

6 security vendors flagged this URL as malicious

http://205.185.125.104/files/june11.dll

205.185.125.104

404 Status

text/html; charset=UTF-8 Content Type

2021-11-28 21:25:51 UTC 5 months ago

DETECTION

DETAILS

COMMUNITY

Security Vendors' Analysis

ESET	Malware	Forcepoint ThreatSeeker	Malicious
Fortinet	Malware	Kaspersky	Malware
Sophos	Malware	Webroot	Malicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AICC (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean
Antiy-AVL	Clean	Armis	Clean

The screenshot shows the VirusTotal website interface. The browser address bar displays the URL: `https://www.virustotal.com/gui/url/e70c46b564e2c7a9d38f0f94cbfafbf2d307`. The page title is "VirusTotal - URL - e70c4". The main content area shows a URL analysis for `http://205.185.125.104/files/june11.dll`. A red banner at the top indicates "6 security vendors flagged this URL as malicious". Below this, a table shows the analysis details:

URL	Status	Content Type	Analysis Date
<code>http://205.185.125.104/files/june11.dll</code>	404	text/html; charset=UTF-8	2021-11-28 21:25:51 UTC
<code>205.185.125.104</code>			5 months ago

Below the table, there are tabs for "DETECTION", "DETAILS", and "COMMUNITY". The "DETECTION" tab is selected. Under "Categories", the following information is listed:

Category	Description
Forcepoint ThreatSeeker	malicious web sites
Sophos	spyware and malware
Comodo Valkyrie Verdict	unknown
Webroot	Malware Sites

Under "History", the following information is listed:

Event	Date
First Submission	2020-06-12 04:14:29 UTC
Last Submission	2021-11-28 21:25:51 UTC
Last Analysis	2021-11-28 21:25:51 UTC

Under "HTTP Response", the "Final URL" is listed as `http://205.185.125.104/files/june11.dll`.

## 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?

**The username that was found was under Mattijs.devries**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src==172.16.4.205 and kerberos.CNameString

No.	Time	Source	Destination	Protocol	Length	Info
15556	149.848730300	172.16.4.205	172.16.4.4	KRB5	372	AS-REQ
15549	149.833191700	172.16.4.205	172.16.4.4	KRB5	292	AS-REQ
15517	149.706495400	172.16.4.205	172.16.4.4	KRB5	381	AS-REQ
15510	149.690858700	172.16.4.205	172.16.4.4	KRB5	381	AS-REQ
15340	148.910222300	172.16.4.205	172.16.4.4	KRB5	377	AS-REQ
15332	148.893035700	172.16.4.205	172.16.4.4	KRB5	297	AS-REQ

padata: 1 item

req-body

padding: 0

kdc-options: 40810010

cname

name-type: KRB5-NT-PRINCIPAL (1)

cname-string: 1 item

CNameString: mattijs.devries

realm: MIND-HAMMER

sname

till: 2037-09-13 02:48:05 (UTC)

rtime: 2037-09-13 02:48:05 (UTC)

nonce: 631265106

etype: 6 items

addresses: 1 item ROTTERDAM-PC<20>

0020 04 04 c0 1a 00 58 bc 24 37 40 32 f1 6d c9 50 18 .....X:\$ 7/2-m P.

0030 01 00 48 a5 00 00 00 00 00 ea 6a 81 e7 30 81 e4 . H.....j..0..

0040 a1 03 02 01 05 a2 03 02 01 0a a3 15 30 13 30 11 .....0..0..

0050 a1 04 02 02 00 80 a2 09 04 07 30 05 a0 03 01 01 .....0.....

0060 ff a4 81 c0 30 81 bd a0 07 03 05 00 40 81 00 10 .....0.....

0070 a1 1d 30 1b a0 03 02 01 01 a1 14 30 12 1b 10 6d .....0.....m

0080 61 74 74 68 69 6a 73 2e 64 65 76 72 69 65 73 a2 attijds.devries

0090 0d 1b 0b 4d 49 4e 44 2d 48 41 4d 4d 45 52 a3 20 ..MIND- HAMMER

00a0 30 1e a0 03 02 01 02 a1 17 30 15 1b 06 0b 72 02 0.....0..krb

00b0 74 67 74 1b 0b 4d 49 4e 44 2d 48 41 4d 4d 45 52 tgt: MIN D-HAMMER

00c0 a5 11 18 0f 32 30 33 37 30 39 31 33 30 32 34 38 ....2037 09130248

00d0 30 35 5a a6 11 18 0f 32 30 33 37 30 39 31 33 30 05Z...2 03709130

00e0 32 34 38 30 35 5a a7 06 02 04 25 a0 57 52 a8 15 24805Z...%WR..

00f0 30 13 02 01 12 02 01 11 02 01 17 02 01 18 02 02 0.....0.....

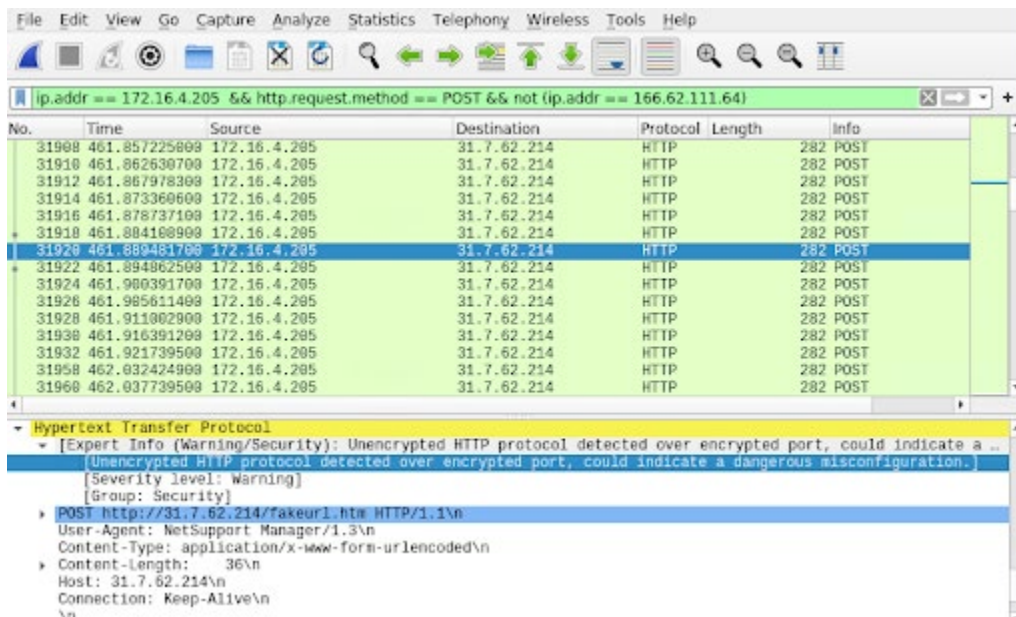
0100 ff 79 02 01 03 a9 1d 30 1b 30 19 a0 03 02 01 14 .y.....0..0.....

0110 a1 12 04 10 52 4f 54 54 45 52 44 41 4d 2d 50 43 ....ROTT ERDAM-PC

0120 20 20 20 20

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

**The infected device has the IP address of 172.16.4.205. There are indicators that we can see are 205.185.216.10, 185.243.115.84, and 166.62.111.64.**



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

**Unfortunately, I could not find 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:** NT 10.0

Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

pcap.pcap 07:17 A

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

kerberos.CNameString

No.	Time	Source	Destination	Protocol	Length	CNameString	Info
65745	744.704098600	10.0.0.2	10.0.0.201	KRB5	293	BLANCO-DESKTOP\$	TGS-REP
65798	745.008607500	10.0.0.2	10.0.0.201	KRB5	227	BLANCO-DESKTOP\$	TGS-REP
65827	745.174120600	10.0.0.2	10.0.0.201	KRB5	293	BLANCO-DESKTOP\$	TGS-REP
65839	745.233051500	10.0.0.2	10.0.0.201	KRB5	114	BLANCO-DESKTOP\$	TGS-REP
66970	751.007645200	10.0.0.201	10.0.0.2	KRB5	302	BLANCO-DESKTOP\$	AS-REQ
66978	751.024207500	10.0.0.201	10.0.0.2	KRB5	382	BLANCO-DESKTOP\$	AS-REQ
66980	751.052436500	10.0.0.2	10.0.0.201	KRB5	250	BLANCO-DESKTOP\$	AS-REP
66992	751.115116900	10.0.0.2	10.0.0.201	KRB5	199	BLANCO-DESKTOP\$	TGS-REP
67036	751.190289600	10.0.0.201	10.0.0.2	KRB5	290	elmer.blanco	AS-REQ
67044	751.205833000	10.0.0.201	10.0.0.2	KRB5	370	elmer.blanco	AS-REQ
67046	751.233860000	10.0.0.2	10.0.0.201	KRB5	237	elmer.blanco	AS-REP
67058	751.294737700	10.0.0.2	10.0.0.201	KRB5	175	elmer.blanco	TGS-REP
67080	751.379585100	10.0.0.2	10.0.0.201	KRB5	303	elmer.blanco	TGS-REP

req-body

Padding: 0

kdc-options: 40810010

- 0... .. = reserved: False
- 1... .. = forwardable: True
- ..0... .. = forwarded: False
- ...0... .. = proxiable: False
- ....0... .. = proxy: False
- ....0... .. = allow-postdate: False
- ....0... .. = postdated: False
- ....0... .. = unused7: False
- 1... .. = renewable: True
- ..0... .. = unused9: False
- ..0... .. = unused10: False
- ..0... .. = opt-hardware-auth: False
- ....0... .. = unused12: False

```

0020 00 02 c2 50 00 58 39 06 5e 0c ab 40 f9 12 50 18 ...P.X9- A..@..P.
0030 08 05 54 4b 00 00 00 00 00 e8 6a 81 e5 30 81 e2 ..TK... ..j..0..
0040 a1 03 02 01 05 a2 03 02 01 0a a3 15 30 13 30 11 ..... ..0.0.
0050 a1 04 02 02 00 80 a2 09 04 07 30 05 a0 03 01 01 ..... ..0.....
0060 ff a4 81 be 30 81 bb a0 07 03 05 00 40 81 00 10 ..... ..0.....
0070 a1 19 30 17 a0 03 02 01 01 a1 18 30 0e 1b 0c 65 ..... ..0...e
0080 6c 60 65 72 2e 62 6c 61 6e 63 6f a2 0e 1b 0c 44 lmer.bla nco...D

```

2. Which torrent file did the user download?

**The torrent file that the user downloaded was the Betty\_Boop\_Rhythm\_on\_theReservation.avi.torrent HTTP/1.1\r\n.**



