

# 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:

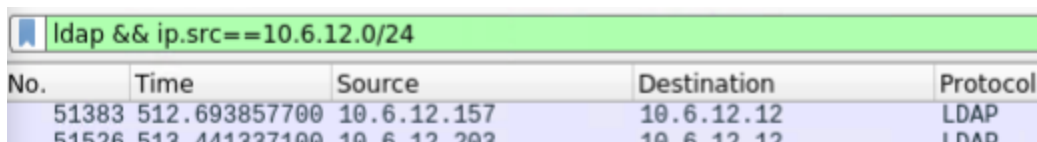
1. What is the domain name of the users' custom site?

frank-n-ted.com

```
LDAPMessage searchResEntry(21) "CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=frank-n-ted,DC=com" [2 results]
LDAPMessage searchResDone(21) success [2 results]
```

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

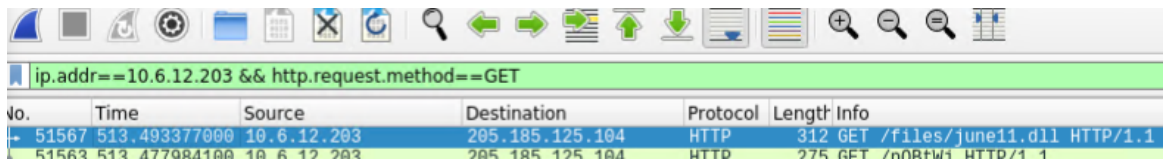
10.6.12.12



No.	Time	Source	Destination	Protocol
51383	512.693857700	10.6.12.157	10.6.12.12	LDAP
51526	513.441337100	10.6.12.203	10.6.12.12	LDAP

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

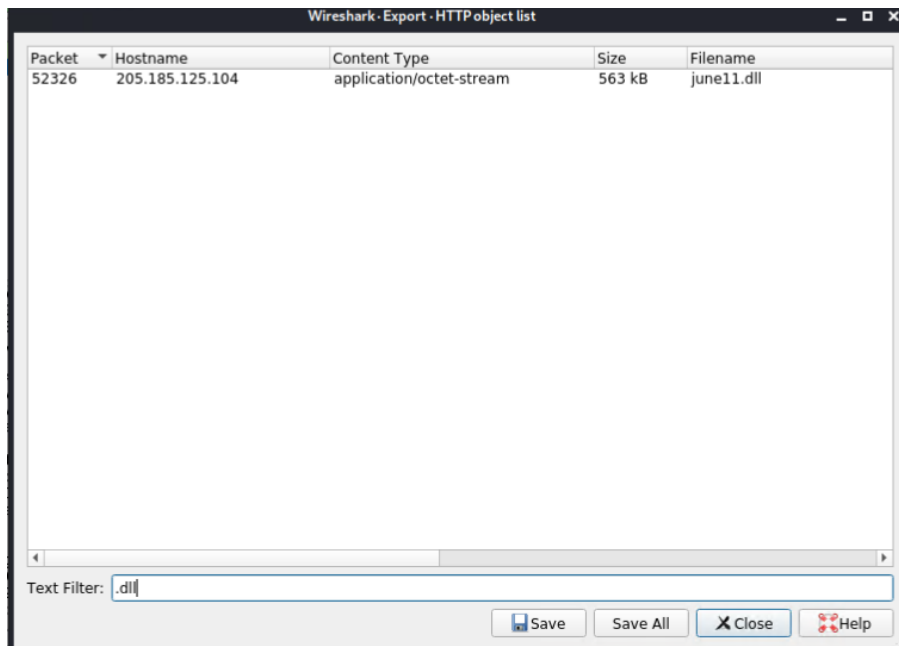


ip.addr==10.6.12.203 && http.request.method==GET

No.	Time	Source	Destination	Protocol	Length	Info
51567	513.493377000	10.6.12.203	205.185.125.104	HTTP	312	GET /files/june11.dll HTTP/1.1
51568	513.477084100	10.6.12.203	205.185.125.104	HTTP	275	GET /n0RtW1 HTTP/1.1

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

This type of malware is a Trojan.



Wireshark - Export - HTTP object list

Packet	Hostname	Content Type	Size	Filename
52326	205.185.125.104	application/octet-stream	563 kB	june11.dll

Text Filter: .dll

Save Save All Close Help

51 / 69

51 security vendors flagged this file as malicious

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

549.84 KB Size

2021-06-20 02:27:22 UTC 11 days ago

June11.dll

invalid-signature overlay pedi signed

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 2

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.ASCCommon.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.34758.lu9@eul7OQgi
Bkav Pro	W32.AI.Detect.malware1	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 100)

## 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.mind-hammer
  - IP address: 172.16.4.205
  - MAC address: 00:59:07:b0:63:a4

File Edit View Go Capture Analyze Statistics Telephony Wirele			
ip.src == 172.16.4.4			
No.	Time	Source	Destination
76455	757.502573100	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...
76457	757.509504400	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...
76459	757.517765700	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...
76461	757.530122900	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...
76463	757.541960200	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...
76465	757.548164500	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...
76468	757.551194200	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...
76472	757.585045600	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...
76473	757.589259900	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...
76475	757.601362700	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...
76477	757.603486800	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...
76481	757.638579000	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...
76482	757.642799000	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...
76484	757.649863800	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...

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

ip.src==172.16.4.205

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 10

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools					
ip.src==10.0.0.201 and kerberos.CNameString					
No.	Time	Source	Destination	Protocol	
65495	743.708498600	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dog...	KRB5	
65500	28382900	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dog...	KRB5	
65530	743.836192200	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dog...	KRB5	
65544	743.884105500	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dog...	KRB5	
65617	744.239448800	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dog...	KRB5	
65625	744.255672900	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dog...	KRB5	
65712	744.572819700	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dog...	KRB5	
65725	744.601486200	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dog...	KRB5	
66970	751.007645200	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dog...	KRB5	
66978	751.024207500	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dog...	KRB5	
67036	751.190289600	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dog...	KRB5	
67044	751.205833000	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dog...	KRB5	

2. Which torrent file did the user download?

Betty\_Boop\_Rhythm\_on\_the\_Reservation.avi.torrent

ip.src==10.0.0.201 && http.request.method==GET			
Destination	Protocol	Length	Info
.dogo...files.publicdomainint...	HTTP	534	GET /nshowmovie.html?movieid=513 HTTP/1.1
.dogo...files.publicdomainint...	HTTP	471	GET /yellow-star.gif HTTP/1.1
.dogo...files.publicdomainint...	HTTP	500	GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1
.dogo...files.publicdomainint...	HTTP	465	GET /divx1.jpg HTTP/1.1
.dogo...files.publicdomainint...	HTTP	531	GET /usercomments.html?movieid=513 HTTP/1.1
.dogo...files.publicdomainint...	HTTP	589	GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on...
.dogo...files.publicdomainint...	HTTP	434	GET /bt/announce.php?info_hash=%1d%da%0d%a8%98%bd%81%5c%7d2%
.dogo...files.publicdomainint...	HTTP	253	GET /bt/scrape.php?info_hash=%1d%da%0d%a8%98%bd%81%5c%7d2%
.dogo...fls-na.amazon-adsys...	HTTP	1067	GET /1/associates-ads/1/OP/?cb=1531628232887&p=%7B%22program%
.dogo...ftp.osuosl.org	HTTP	195	GET /version-1.0 HTTP/1.1
.dogo...moonstar.publicdoma...	HTTP	434	GET /announce?info_hash=%1d%da%0d%a8%98%bd%81%5c%7d2%
.dogo...moonstar.publicdoma...	HTTP	253	GET /scrape?info_hash=%1d%da%0d%a8%98%bd%81%5c%7d2%
.dogo...ocsp.godaddy.com.ak...	HTTP	274	GET //MEQwQjBAND4wPDAJBgUrDgMCGUAABTkIInKBAZKxKf0qh0pel31fHJ9...