

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?

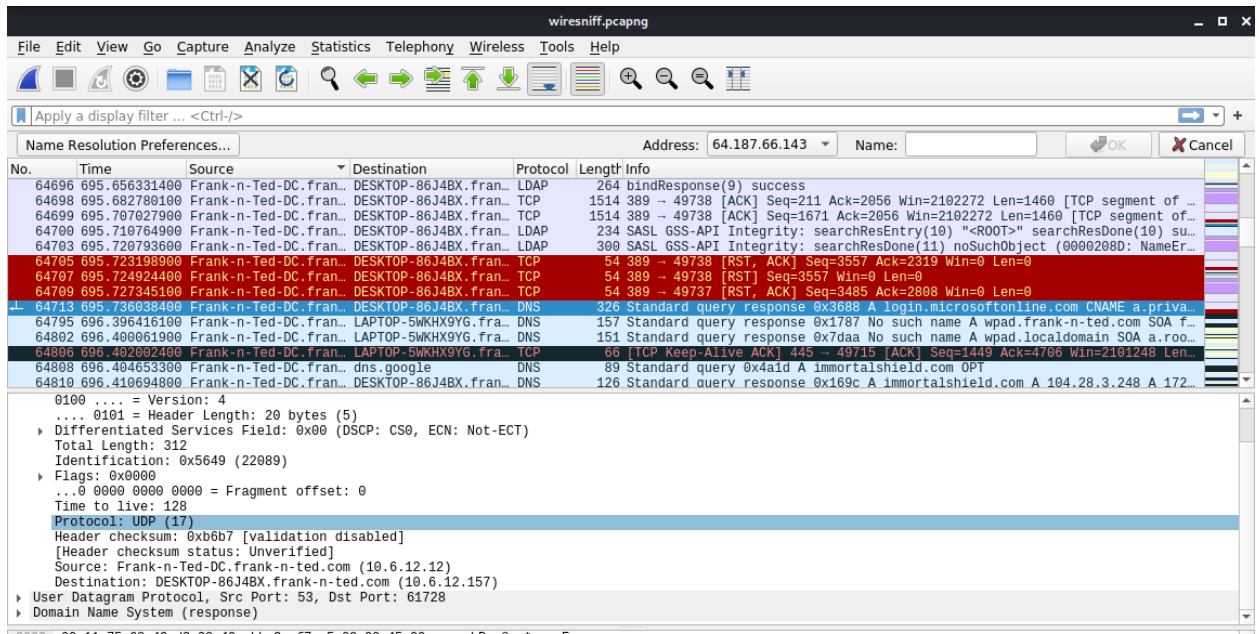
Filter: ip.addr == 10.6.12.0/24

Frank-n-Ted-DC.frank-n-ted.com

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

Filter: ip.addr == 10.6.12.0/24

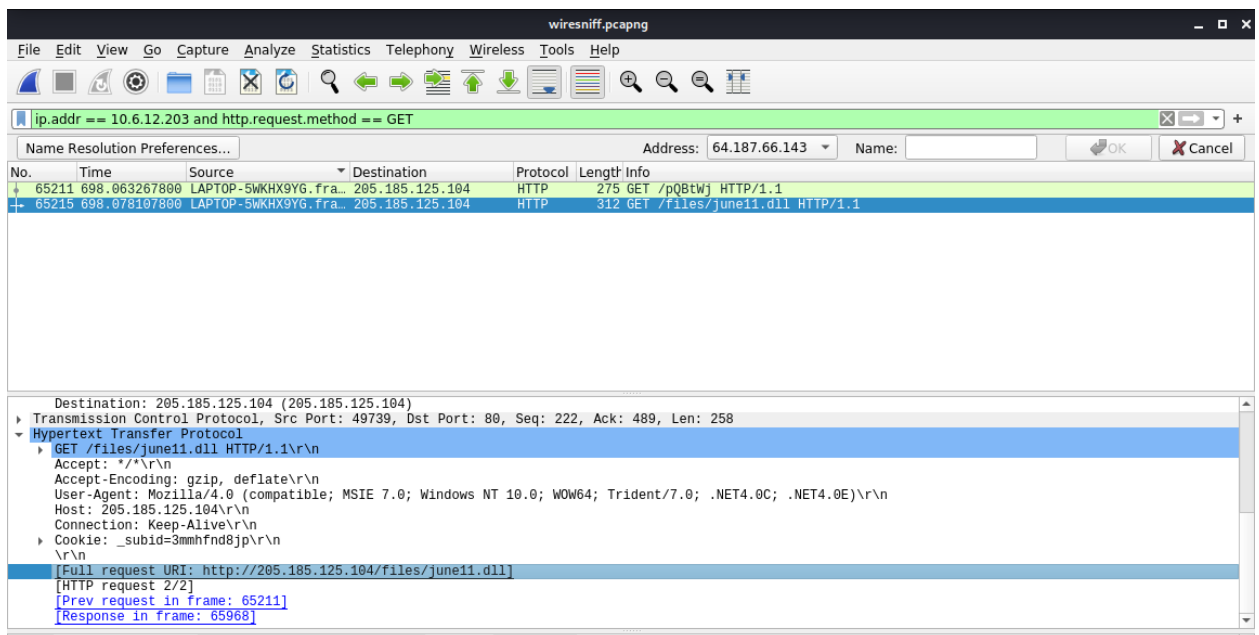
10.6.12.12



- 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.

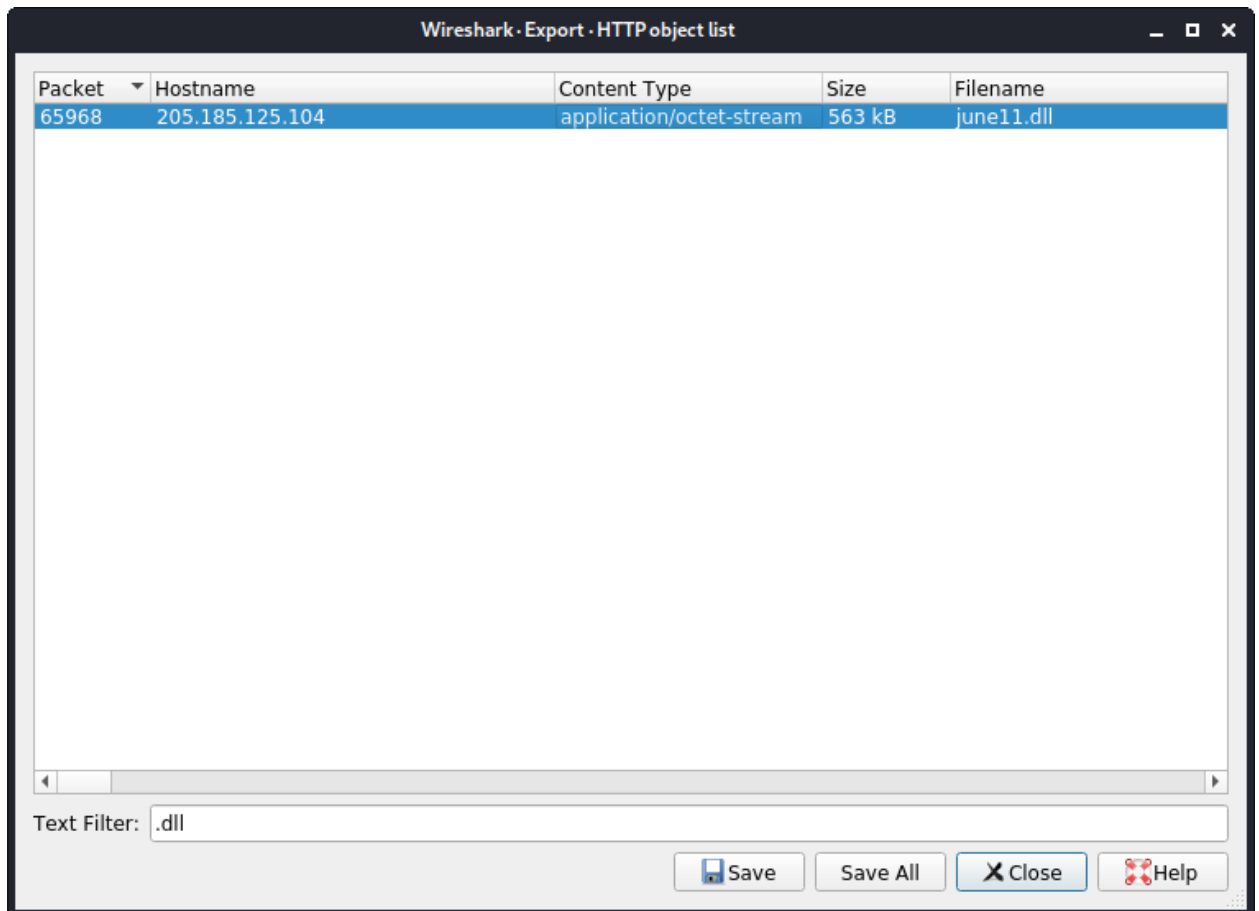
Filter: `ip.addr == 10.6.12.203 and http.request.method == GET`

june11.dll



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

Trojan



VirusTotal - File - d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec - Mozilla Firefox

File Edit View History Bookmarks Tools Help

VirusTotal - File - d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

https://www.virustotal.com/gui/file/d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

50 / 66

50 security vendors and 1 sandbox flagged this file as malicious

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

549.84 KB Size

2022-03-13 05:45:29 UTC 6 days ago

GoogleIupdate.exe

invalid-signature overlay pedll signed spreader

Community Score

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
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.34264.lu9@aul7OQgi	CrowdStrike Falcon	Win/malicious_confidence_100% (W)	
Cylance	Unsafe	Cynet	Malicious (score: 100)	
DrWeb	Trojan.Inject3.53106	Elastic	Malicious (high Confidence)	

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:

- Filter: ip.addr == 172.16.4.0/24
- Host name: Rotterdam-PC
- IP address: 172.16.4.205
- MAC address: 00:59:07:b0:63:a4

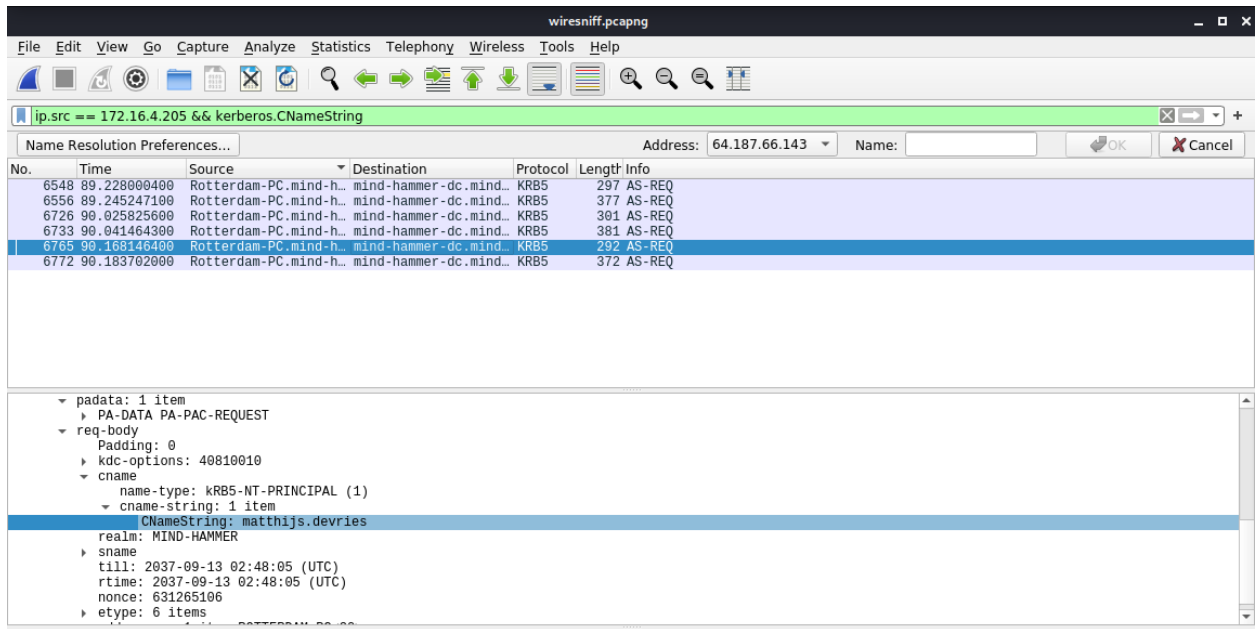
The image shows a Wireshark packet capture window titled "wireshark.pcapng". The filter bar at the top displays "ip.addr == 172.16.4.0/24". The packet list shows several packets, with packet 6547 selected. The packet details pane shows the following information:

- Frame 6547: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface eth0, id 0
- Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Dell_19:49:50 (a4:ba:db:19:49:50)
- Destination: Dell_19:49:50 (a4:ba:db:19:49:50)
- Address: Dell_19:49:50 (a4:ba:db:19:49:50)
- = LG bit: Globally unique address (factory default)
- = IG bit: Individual address (unicast)
- Source: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
- Address: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
- = LG bit: Globally unique address (factory default)
- = IG bit: Individual address (unicast)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: Rotterdam-PC.mind-hammer.net (172.16.4.205), Dst: mind-hammer-dc.mind-hammer.net (172.16.4.4)
- Transmission Control Protocol, Src Port: 49163, Dst Port: 88, Seq: 1, Ack: 1, Len: 0
- VSS Monitoring Ethernet trailer, Source Port: 45888

2. What is the username of the Windows user whose computer is infected?

Filter: ip.src == 172.16.4.205 && kerberos.CNameString

Matthijs.devries is the windows user



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

Filter: Go into statistics menu; conversations; select IPV4 Tab, sort by packets

IP Addresses 172.16.4.205, 185.243.115.84, 166.62.111.64

Wireshark - Conversations - wiresniff.pcapng											
Ethernet · 83	IPv4 · 882	IPv6 · 6	TCP · 1038	UDP · 1825							
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bit
172.16.4.205	185.243.115.84	18,324	16 M	9,753	7,983 k	8,571	8,543 k	235.595782	265.0412	240 k	
166.62.111.64	172.16.4.205	7,864	8,082 k	5,677	7,921 k	2,187	160 k	90.602721	149.9677	422 k	
192.168.1.90	192.168.1.100	4,905	22 M	3,185	22 M	1,720	472 k	6.492496	860.5381	206 k	
5.101.51.151	10.6.12.203	4,326	4,246 k	3,262	4,177 k	1,064	68 k	709.332192	67.9985	491 k	
10.0.0.201	23.43.62.169	4,007	4,080 k	1,310	71 k	2,697	4,008 k	21.032704	66.9059	8,605	
10.0.0.201	64.187.66.143	4,005	2,984 k	1,830	118 k	2,175	2,865 k	0.008563	843.3088	1,125	
10.11.11.200	151.101.50.208	3,270	2,220 k	1,613	112 k	1,657	2,108 k	611.358992	66.7937	13 k	
10.6.12.12	10.6.12.203	1,388	350 k	620	161 k	768	188 k	683.785457	99.1499	13 k	

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

Filter: ip.addr == 172.16.4.205 && ip.addr == 185.243.115.84

wireshark.pcapng

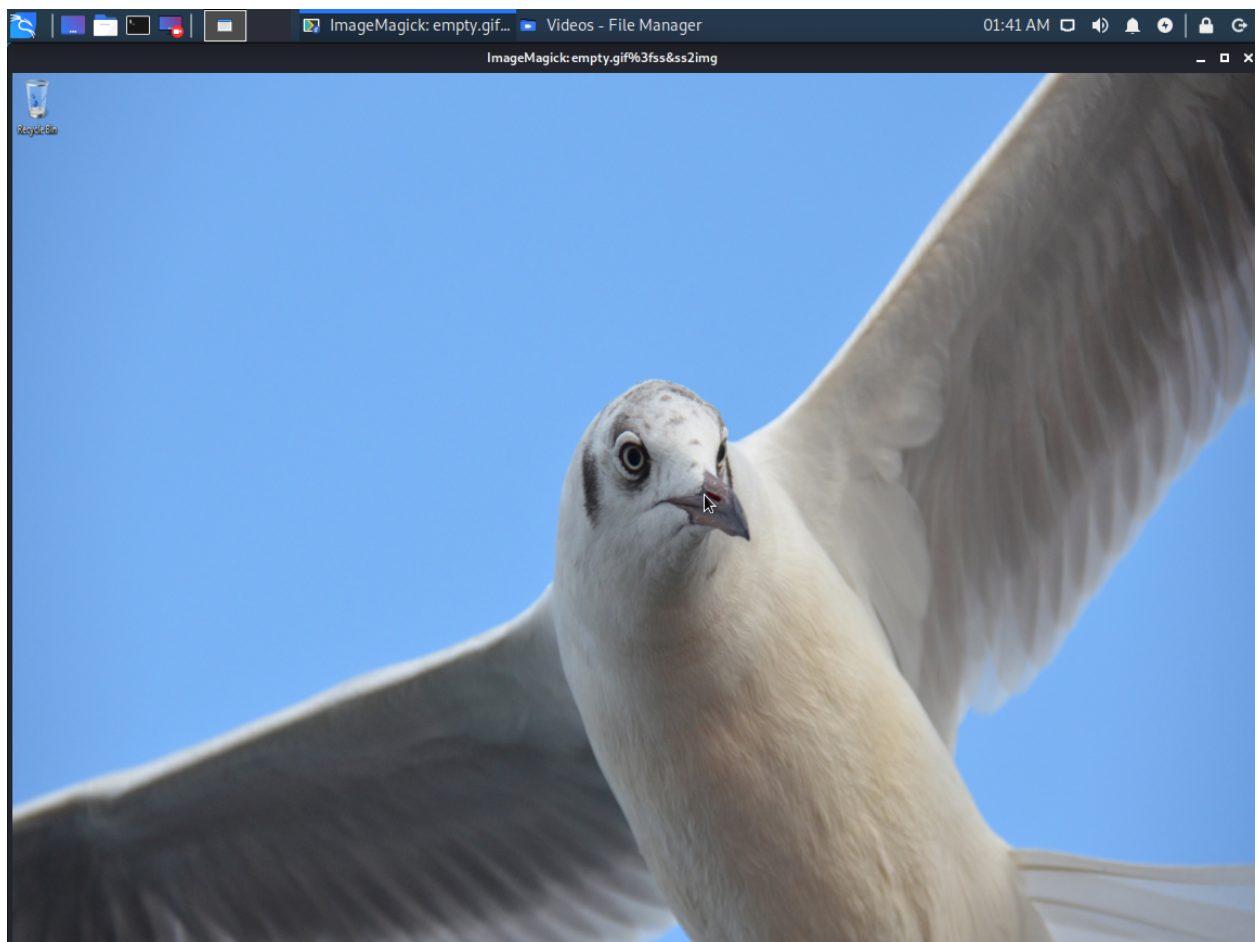
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

Name Resolution Preferences... Address: 64.187.66.143 Name: OK Cancel

No.	Time	Source	Destination	Protocol	Length	Info
16826	235.595781600	Rotterdam-PC.mind-h...	b5689023.green.matt...	TCP	66	49249 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
16829	235.598859700	Rotterdam-PC.mind-h...	b5689023.green.matt...	TCP	60	49249 → 80 [ACK] Seq=1 Ack=1 Win=66304 Len=0
16830	235.607598500	Rotterdam-PC.mind-h...	b5689023.green.matt...	TCP	546	49249 → 80 [PSH, ACK] Seq=1 Ack=1 Win=66304 Len=492 [TCP segment of a re...
16831	235.609619400	Rotterdam-PC.mind-h...	b5689023.green.matt...	HTTP	126	POST /empty.gif HTTP/1.1 (application/x-www-form-urlencoded)
16843	235.730326400	Rotterdam-PC.mind-h...	b5689023.green.matt...	TCP	60	49249 → 80 [ACK] Seq=565 Ack=1358 Win=66304 Len=0
16848	235.800412600	Rotterdam-PC.mind-h...	b5689023.green.matt...	TCP	60	49249 → 80 [ACK] Seq=565 Ack=2715 Win=66304 Len=0
16849	235.801341000	Rotterdam-PC.mind-h...	b5689023.green.matt...	TCP	60	49249 → 80 [ACK] Seq=565 Ack=4153 Win=66304 Len=0
16850	235.802299500	Rotterdam-PC.mind-h...	b5689023.green.matt...	TCP	60	49249 → 80 [ACK] Seq=565 Ack=6867 Win=66304 Len=0
16851	235.803261800	Rotterdam-PC.mind-h...	b5689023.green.matt...	TCP	60	49249 → 80 [ACK] Seq=565 Ack=8224 Win=66304 Len=0
16852	235.804223400	Rotterdam-PC.mind-h...	b5689023.green.matt...	TCP	60	49249 → 80 [ACK] Seq=565 Ack=9614 Win=66304 Len=0
16853	235.805181600	Rotterdam-PC.mind-h...	b5689023.green.matt...	TCP	60	49249 → 80 [ACK] Seq=565 Ack=10971 Win=65024 Len=0
16854	235.806150200	Rotterdam-PC.mind-h...	b5689023.green.matt...	TCP	60	[TCP Window Update] 49249 → 80 [ACK] Seq=565 Ack=10971 Win=66304 Len=0
16858	235.853325200	Rotterdam-PC.mind-h...	b5689023.green.matt...	TCP	60	49249 → 80 [ACK] Seq=565 Ack=12328 Win=66304 Len=0
16859	235.854272500	Rotterdam-PC.mind-h...	b5689023.green.matt...	TCP	60	49249 → 80 [ACK] Seq=565 Ack=13685 Win=66304 Len=0

UA-CPU: AMD64\r\n
 Accept-Encoding: gzip, deflate\r\n
 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729)\r\n
 Host: b5689023.green.mattingsolutions.co\r\n
 Content-Length: 72\r\n
 Connection: Keep-Alive\r\n
 Cache-Control: no-cache\r\n
 \r\n
 [Full request URI: http://b5689023.green.mattingsolutions.co/empty.gif]\r\n
 [HTTP request 1/5]\r\n
 [Response in frame: 16860]\r\n
 [Next request in frame: 16907]\r\n
 File Data: 72 bytes\r\n
 HTML Form URL Encoded: application/x-www-form-urlencoded



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:
 - Filters: ip.addr == 10.0.0.201 && kerberos.CNameString; ip.addr == 10.0.0.201 && HTTP
 - MAC address: 00:16:17:18:66:c8
 - Windows username: elmer.blanco
 - OS version: Windows 10

The image shows a Wireshark packet capture window titled "wireshark.pcapng". The filter bar at the top contains the filter: "ip.addr == 10.0.0.201 && kerberos.CNameString". The packet list pane shows a list of packets, with packet 74949 selected. The packet details pane shows the structure of the selected packet, which is a Kerberos AS-REQ message. The "cname" field is expanded, showing the "CNameString" as "elmer.blanco" and the "realm" as "DOGOFTHEYEAR".

No.	Time	Source	Destination	Protocol	Length	Info
72450	783.325555100	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dogo...	KRB5	382	AS-REQ
72535	783.689925200	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dogo...	KRB5	301	AS-REQ
72543	783.697143300	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dogo...	KRB5	381	AS-REQ
72626	784.014287100	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dogo...	KRB5	301	AS-REQ
72639	784.052886200	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dogo...	KRB5	382	AS-REQ
73974	790.449107900	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dogo...	KRB5	302	AS-REQ
73982	790.465643900	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dogo...	KRB5	382	AS-REQ
74949	790.631752100	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dogo...	KRB5	290	AS-REQ
74948	790.647296000	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dogo...	KRB5	370	AS-REQ
72438	783.385881700	DogOfTheYear-DC.dogo...	BLANCO-DESKTOP.dogo...	KRB5	250	AS-REP
72452	783.353889100	DogOfTheYear-DC.dogo...	BLANCO-DESKTOP.dogo...	KRB5	250	AS-REP
72464	783.419219900	DogOfTheYear-DC.dogo...	BLANCO-DESKTOP.dogo...	KRB5	293	TGS-REP
72545	783.725397100	DogOfTheYear-DC.dogo...	BLANCO-DESKTOP.dogo...	KRB5	250	AS-REP
72557	783.790168400	DogOfTheYear-DC.dogo...	BLANCO-DESKTOP.dogo...	KRB5	273	TGS-REP

Transmission Control Protocol, Src Port: 49744, Dst Port: 88, Seq: 1, Ack: 1, Len: 236

Kerberos

- Record Mark: 232 bytes
- as-req
 - pvno: 5
 - msg-type: krb-as-req (10)
 - padata: 1 item
 - req-body
 - Padding: 0
 - kdc-options: 40810010
 - cname
 - name-type: KRB5-NT-PRINCIPAL (1)
 - cname-string: 1 item
 - CNameString: elmer.blanco
 - realm: DOGOFTHEYEAR

wireshniff.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.0.0.201 && http

Name Resolution Preferences... Address: 64.187.66.143 Name: OK Cancel

No.	Time	Source	Destination	Protocol	Length	Info
2138	21.294916200	BLANCO-DESKTOP.dogo...	cs9.wac.phicdn.net	HTTP	288	GET /MFewTzBNMEswSTAJBgUrDgMCGGUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QN...
2142	21.302212600	BLANCO-DESKTOP.dogo...	cs9.wac.phicdn.net	HTTP	290	GET /MFewTzBNMEswSTAJBgUrDgMCGGUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZM...
2165	21.531316800	BLANCO-DESKTOP.dogo...	cs9.wac.phicdn.net	HTTP	292	GET /MFewTzBNMEswSTAJBgUrDgMCGGUABBTnvAI%2FnN49qPTJY2qTtKfLxjvEAQUo53mH...
74280	791.772667000	BLANCO-DESKTOP.dogo...	files.publicdomaint...	HTTP	463	GET /nshowcat.html?category=animation HTTP/1.1
74294	791.882520900	BLANCO-DESKTOP.dogo...	files.publicdomaint...	HTTP	474	GET /srsbanner.gif HTTP/1.1
74320	792.117862600	BLANCO-DESKTOP.dogo...	files.publicdomaint...	HTTP	477	GET /grabs/hdsale.png HTTP/1.1
74350	792.322601800	BLANCO-DESKTOP.dogo...	files.publicdomaint...	HTTP	469	GET /ipod.jpg HTTP/1.1
74352	792.330913900	BLANCO-DESKTOP.dogo...	files.publicdomaint...	HTTP	468	GET /pda.jpg HTTP/1.1
74355	792.340306600	BLANCO-DESKTOP.dogo...	files.publicdomaint...	HTTP	479	GET /site2/pdheader.jpg HTTP/1.1
74357	792.348666800	BLANCO-DESKTOP.dogo...	files.publicdomaint...	HTTP	468	GET /psp.gif HTTP/1.1
74359	792.357108500	BLANCO-DESKTOP.dogo...	files.publicdomaint...	HTTP	474	GET /googlevid.jpg HTTP/1.1
74369	792.375855700	BLANCO-DESKTOP.dogo...	pagead46.l.doublecl...	HTTP	445	GET /pagead/js/adsbygoogle.js HTTP/1.1
74383	792.528290800	BLANCO-DESKTOP.dogo...	files.publicdomaint...	HTTP	471	GET /rentme.gif HTTP/1.1
74410	792.867015100	BLANCO-DESKTOP.dogo...	diag.com	HTTP	417	GET /tools/diaothis.is HTTP/1.1

▼ Hypertext Transfer Protocol

GET /grabs/hdsale.png HTTP/1.1\r\n

▶ [Expert Info (Chat/Sequence): GET /grabs/hdsale.png HTTP/1.1\r\n]

Request Method: GET

Request URI: /grabs/hdsale.png

Request Version: HTTP/1.1

Referer: http://publicdomaintorrents.info/nshowcat.html?category=animation\r\n

Accept: image/png, image/svg+xml, image/*;q=0.8,*/*;q=0.5\r\n

Accept-Language: en-US\r\n

Accept-Encoding: gzip, deflate\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

Host: publicdomaintorrents.info\r\n

Connection: Keep-Alive\r\n

\r\n

[Full request URI: http://publicdomaintorrents.info/grabs/hdsale.png]

74355 792.340306600 BLANCO-DESKTOP.dogo... files.publicdomaint... HTTP 479 GET /site2/pdheader.jpg HTTP/1.1

▶ Frame 2138: 288 bytes on wire (2304 bits), 288 bytes captured (2304 bits) on interface eth0, id 0

▶ Ethernet II, Src: Msi 18:66:c8 (08:16:17:18:66:c8), Dst: Cisco 27:a1:3e (08:09:b7:27:a1:3e)

▶ Internet Protocol Version 4, Src: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201), Dst: cs9.wac.phicdn.net (72.21.91.29)

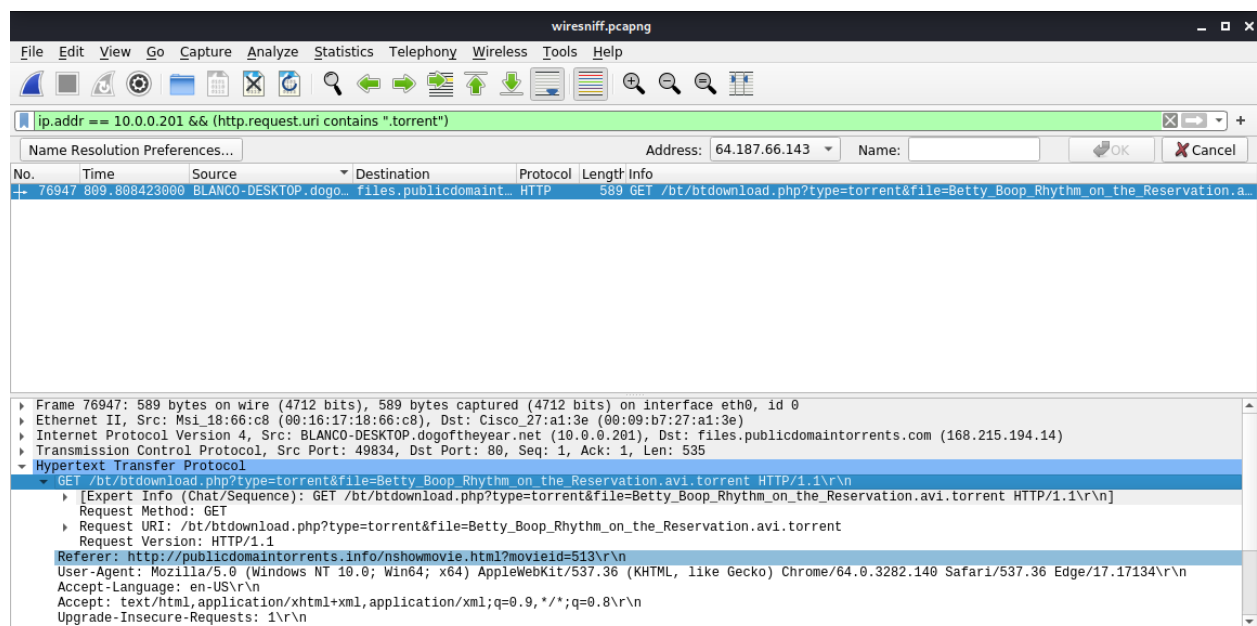
▶ Transmission Control Protocol, Src Port: 49950, Dst Port: 80, Seq: 1, Ack: 1, Len: 234

▶ Hypertext Transfer Protocol

2. Which torrent file did the user download?

Filter: ip.addr == 10.0.0.201 && (http.request.uri contains ".torrent")

Betty_Boop_Rythm_on_the_Reservation.avi.torrent



Sources:

Can wireshark automatically resolve the IP address into host names? Wireshark Q&A.
 (n.d.). Retrieved March 19, 2022, from
<https://osqa-ask.wireshark.org/questions/37680/can-wireshark-automatically-resolve-the-ip-address-into-host-names/>