

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.

Command for Wireshark: `wireshark -i eth0 -k`

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

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

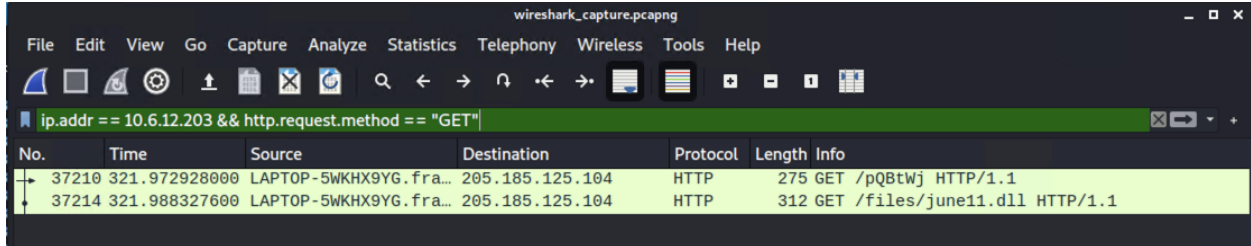
10.6.12.12

No.	Time	Source	Destination	Protocol	Length	Info
33605	304.399189300	Frank-n-Ted-DC.fran...	255.255.255.255	DHCP	351	DHCP ACK - Transaction ID 0xba8b...
33614	304.409053400	DESKTOP-86J4BX.fran...	Frank-n-Ted-DC.fran...	DNS	96	Standard query 0x9c26 SRV _ldap._tcp.
33615	304.411653600	Frank-n-Ted-DC.fran...	DESKTOP-86J4BX.fran...	DNS	162	Standard query response 0x9c26 SRV _l...
33616	304.413091800	DESKTOP-86J4BX.fran...	Frank-n-Ted-DC.fran...	DNS	90	Standard query 0x838c A frank-n-ted-d...
33617	304.414786700	Frank-n-Ted-DC.fran...	DESKTOP-86J4BX.fran...	DNS	106	Standard query response 0x838c A fran...
33618	304.419011100	DESKTOP-86J4BX.fran...	Frank-n-Ted-DC.fran...	CLDAP	264	searchRequest(1) "<R00T>" baseObject
33619	304.422788000	Frank-n-Ted-DC.fran...	DESKTOP-86J4BX.fran...	CLDAP	236	searchResEntry(1) "<R00T>" searchResD...
33620	304.423841900	DESKTOP-86J4BX.fran...	Frank-n-Ted-DC.fran...	TCP	66	49668 → ldap(389) [SYN] Seq=0 Win=642...
33621	304.424894100	Frank-n-Ted-DC.fran...	DESKTOP-86J4BX.fran...	TCP	66	ldap(389) → 49668 [SYN, ACK] Seq=0 Ac...
33622	304.425758600	DESKTOP-86J4BX.fran...	Frank-n-Ted-DC.fran...	TCP	54	49668 → ldap(389) [ACK] Seq=1 Ack=1 W...

Frame 33605: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits) on interface eth0, id 0
Ethernet II, Src: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Dynamic Host Configuration Protocol (ACK) Message type: Boot Reply (2) Hardware type: Ethernet (0x01)

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

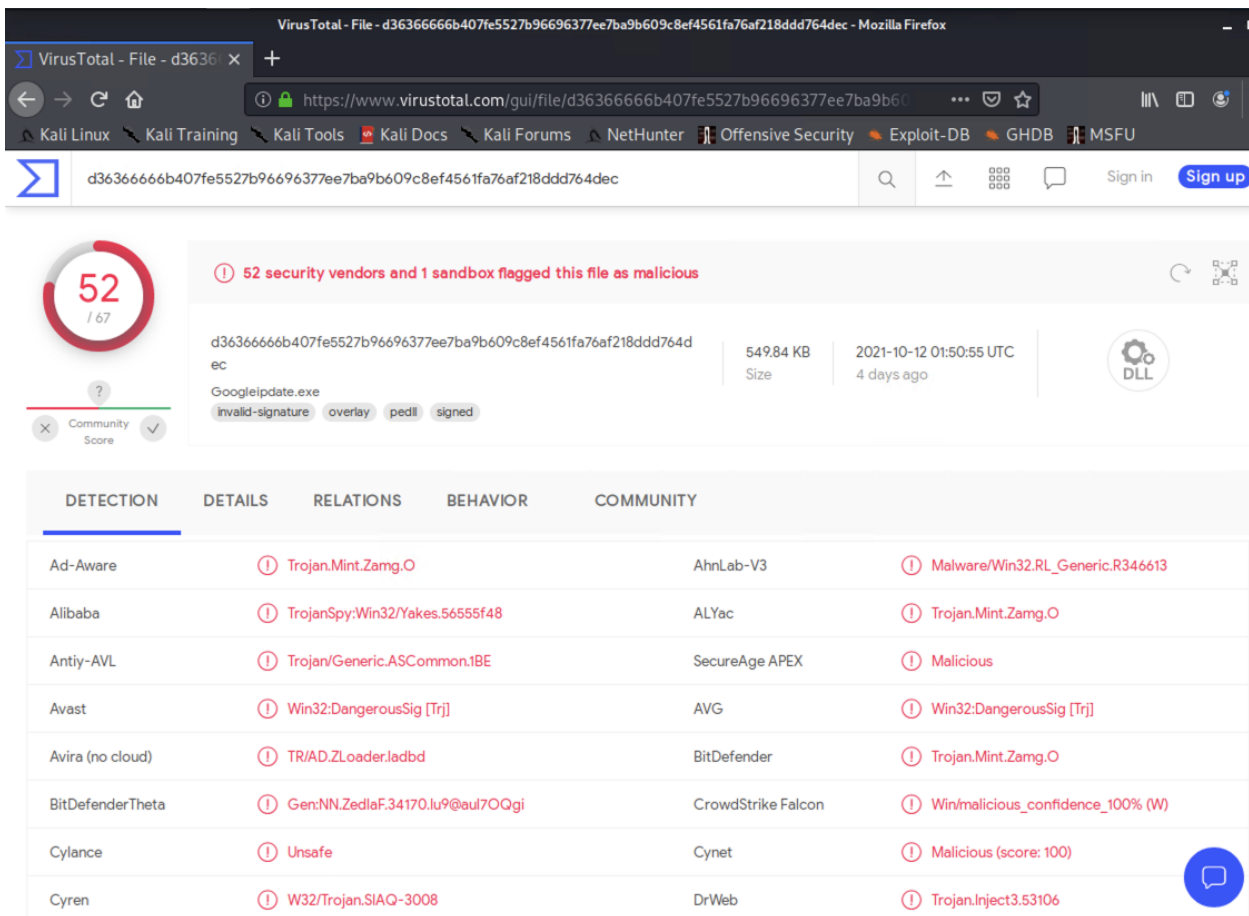


Wireshark capture showing an HTTP GET request for /files/june11.dll from 10.6.12.203 to 205.185.125.104. The filter is set to ip.addr == 10.6.12.203 && http.request.method == "GET".

No.	Time	Source	Destination	Protocol	Length	Info
37210	321.972928000	LAPTOP-5WKHX9YG.fra...	205.185.125.104	HTTP	275	GET /pQBtWj HTTP/1.1
37214	321.988327600	LAPTOP-5WKHX9YG.fra...	205.185.125.104	HTTP	312	GET /files/june11.dll HTTP/1.1

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

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

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

52 / 67

52 security vendors and 1 sandbox flagged this file as malicious

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

549.84 KB

2021-10-12 01:50:55 UTC

4 days 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
Avast	Win32:DangerousSig [Trj]		AVG	Win32:DangerousSig [Trj]
Avira (no cloud)	TR/AD.ZLoader.ladbd		BitDefender	Trojan.Mint.Zamg.O
BitDefenderTheta	Gen:NN.ZedlaF.34170.lu9@aul7OQgi		CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe		Cynet	Malicious (score: 100)
Cyren	W32/Trojan.SIAQ-3008		DrWeb	Trojan.Inject3.53106

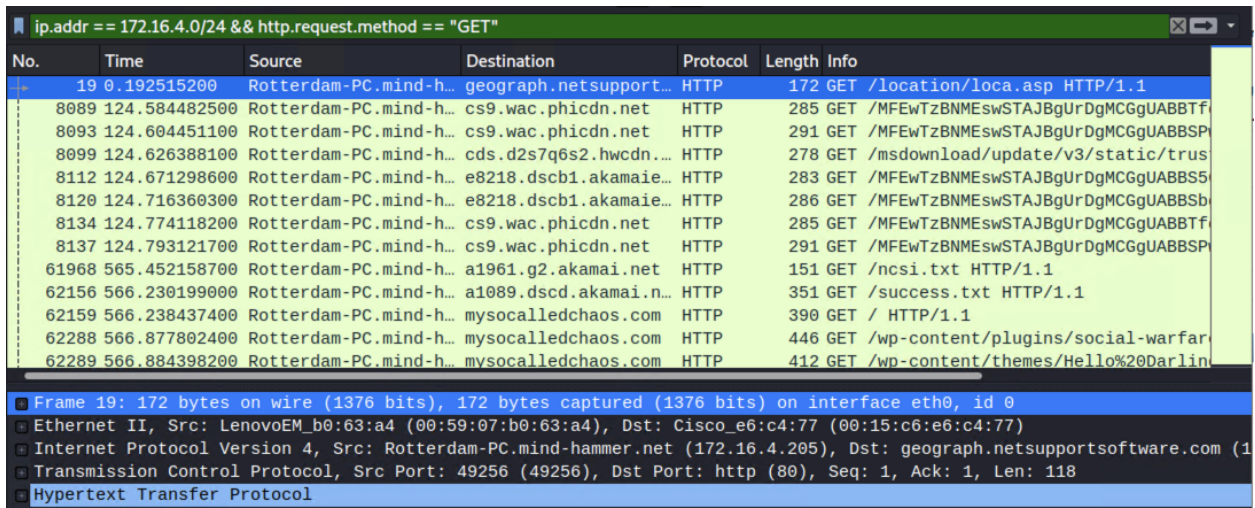
Vulnerable Windows Machines

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.net
 - IP address: 172.16.4.205
 - MAC address: 00:59:07:b0:63:a4



ip.addr == 172.16.4.0/24 && http.request.method == "GET"

No.	Time	Source	Destination	Protocol	Length	Info
19	0.192515200	Rotterdam-PC.mind-h...	geograph.netsupport...	HTTP	172	GET /location/loca.asp HTTP/1.1
8089	124.584482500	Rotterdam-PC.mind-h...	cs9.wac.phicdn.net	HTTP	285	GET /MFEwTzBNMEswSTAJBgUrDgMCGGUABBTf...
8093	124.604451100	Rotterdam-PC.mind-h...	cs9.wac.phicdn.net	HTTP	291	GET /MFEwTzBNMEswSTAJBgUrDgMCGGUABBS...
8099	124.626388100	Rotterdam-PC.mind-h...	cds.d2s7q6s2.hwcdn...	HTTP	278	GET /msdownload/update/v3/static/trus...
8112	124.671298600	Rotterdam-PC.mind-h...	e8218.dscb1.akamaie...	HTTP	283	GET /MFEwTzBNMEswSTAJBgUrDgMCGGUABBS...
8120	124.716360300	Rotterdam-PC.mind-h...	e8218.dscb1.akamaie...	HTTP	286	GET /MFEwTzBNMEswSTAJBgUrDgMCGGUABBS...
8134	124.774118200	Rotterdam-PC.mind-h...	cs9.wac.phicdn.net	HTTP	285	GET /MFEwTzBNMEswSTAJBgUrDgMCGGUABBTf...
8137	124.793121700	Rotterdam-PC.mind-h...	cs9.wac.phicdn.net	HTTP	291	GET /MFEwTzBNMEswSTAJBgUrDgMCGGUABBS...
61968	565.452158700	Rotterdam-PC.mind-h...	a1961.g2.akamai.net	HTTP	151	GET /ncsi.txt HTTP/1.1
62156	566.230199000	Rotterdam-PC.mind-h...	a1089.dscd.akamai.n...	HTTP	351	GET /success.txt HTTP/1.1
62159	566.238437400	Rotterdam-PC.mind-h...	mysocalledchaos.com	HTTP	390	GET / HTTP/1.1
62288	566.877802400	Rotterdam-PC.mind-h...	mysocalledchaos.com	HTTP	446	GET /wp-content/plugins/social-warfar...
62289	566.884398200	Rotterdam-PC.mind-h...	mysocalledchaos.com	HTTP	412	GET /wp-content/themes/Hello%20Darlin...

Frame 19: 172 bytes on wire (1376 bits), 172 bytes captured (1376 bits) on interface eth0, id 0

Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Cisco_e6:c4:77 (00:15:c6:e6:c4:77)

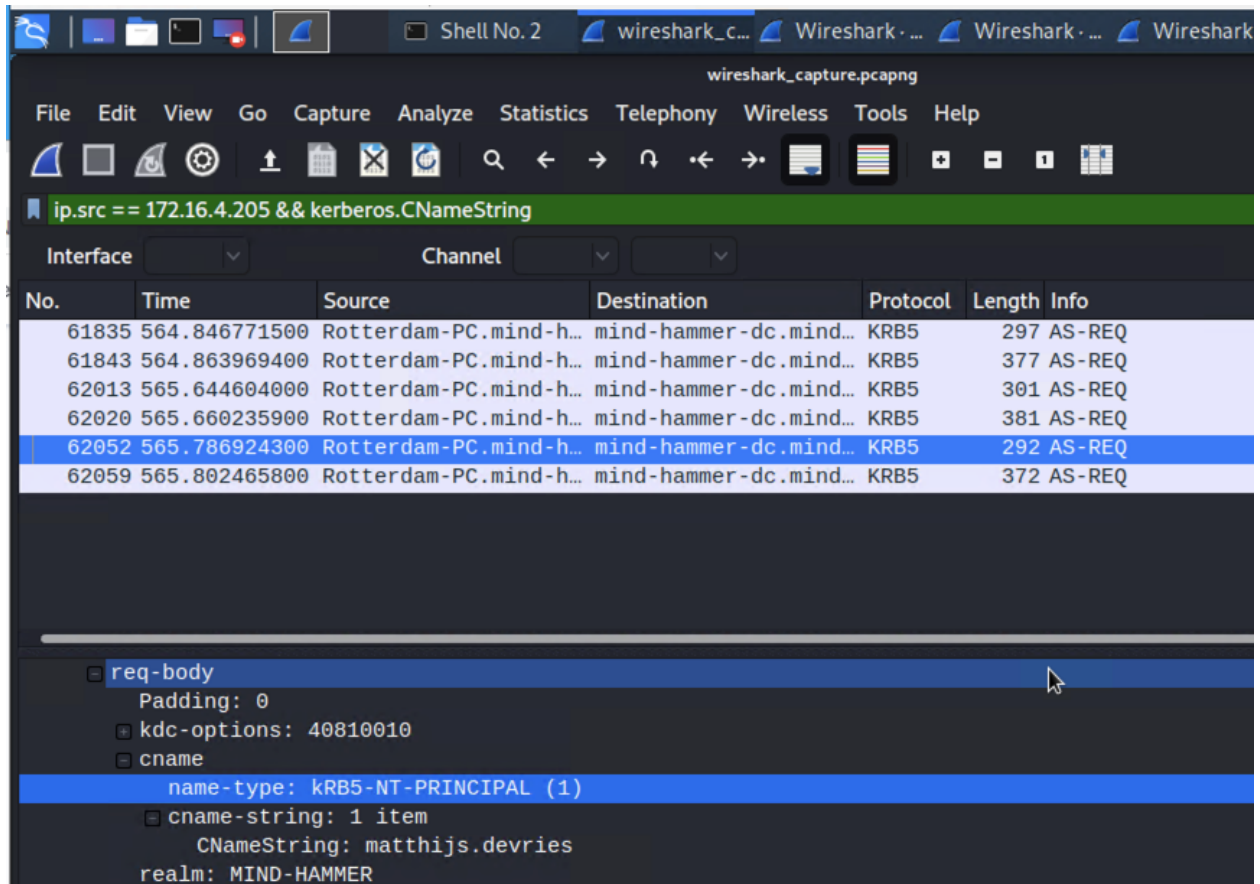
Internet Protocol Version 4, Src: Rotterdam-PC.mind-hammer.net (172.16.4.205), Dst: geograph.netsupportsoftware.com (172.16.4.4)

Transmission Control Protocol, Src Port: 49256 (49256), Dst Port: http (80), Seq: 1, Ack: 1, Len: 118

Hypertext Transfer Protocol

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

matthijs.devries and ROTTERDAM-PC\$



wireshark_capture.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 172.16.4.205 && kerberos.CNameString

Interface Channel

No.	Time	Source	Destination	Protocol	Length	Info
61835	564.846771500	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	KRB5	297	AS-REQ
61843	564.863969400	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	KRB5	377	AS-REQ
62013	565.644604000	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	KRB5	301	AS-REQ
62020	565.660235900	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	KRB5	381	AS-REQ
62052	565.786924300	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	KRB5	292	AS-REQ
62059	565.802465800	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	KRB5	372	AS-REQ

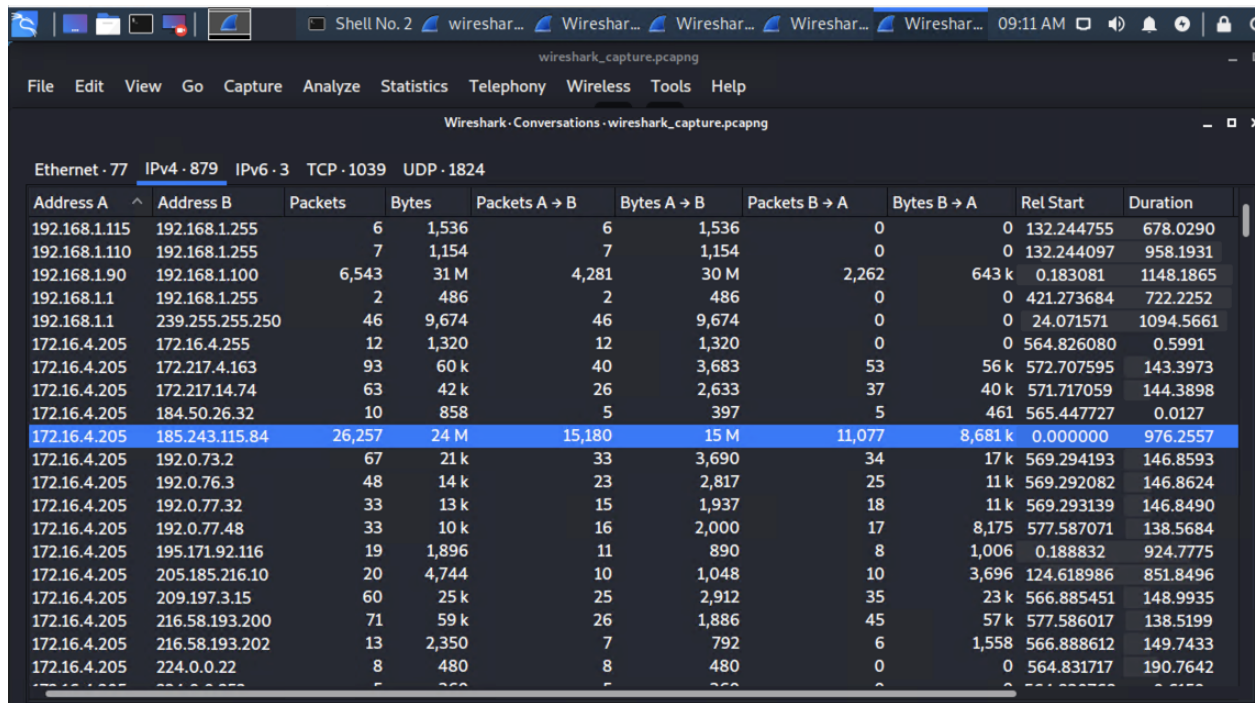
req-body

- Padding: 0
- kdc-options: 40810010
- cname
 - name-type: kRB5-NT-PRINCIPAL (1)
 - cname-string: 1 item
 - CNameString: ROTTERDAM-PC\$
 - realm: MIND-HAMMER.NET

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

Statistics → Conversation → click IPv4 → filter by IP for 17

185.243.115.84



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
192.168.1.115	192.168.1.255	6	1,536	6	1,536	0	0	132.244755	678.0290
192.168.1.110	192.168.1.255	7	1,154	7	1,154	0	0	132.244097	958.1931
192.168.1.90	192.168.1.100	6,543	31 M	4,281	30 M	2,262	643 k	0.183081	1148.1865
192.168.1.1	192.168.1.255	2	486	2	486	0	0	421.273684	722.2252
192.168.1.1	239.255.255.250	46	9,674	46	9,674	0	0	24.071571	1094.5661
172.16.4.205	172.16.4.255	12	1,320	12	1,320	0	0	564.826080	0.5991
172.16.4.205	172.217.4.163	93	60 k	40	3,683	53	56 k	572.707595	143.3973
172.16.4.205	172.217.14.74	63	42 k	26	2,633	37	40 k	571.717059	144.3898
172.16.4.205	184.50.26.32	10	858	5	397	5	461	565.447727	0.0127
172.16.4.205	185.243.115.84	26,257	24 M	15,180	15 M	11,077	8,681 k	0.000000	976.2557
172.16.4.205	192.0.73.2	67	21 k	33	3,690	34	17 k	569.294193	146.8593
172.16.4.205	192.0.76.3	48	14 k	23	2,817	25	11 k	569.292082	146.8624
172.16.4.205	192.0.77.32	33	13 k	15	1,937	18	11 k	569.293139	146.8490
172.16.4.205	192.0.77.48	33	10 k	16	2,000	17	8,175	577.587071	138.5684
172.16.4.205	195.171.92.116	19	1,896	11	890	8	1,006	0.188832	924.7775
172.16.4.205	205.185.216.10	20	4,744	10	1,048	10	3,696	124.618986	851.8496
172.16.4.205	209.197.3.15	60	25 k	25	2,912	35	23 k	566.885451	148.9935
172.16.4.205	216.58.193.200	71	59 k	26	1,886	45	57 k	577.586017	138.5199
172.16.4.205	216.58.193.202	13	2,350	7	792	6	1,558	566.888612	149.7433
172.16.4.205	224.0.0.22	8	480	8	480	0	0	564.831717	190.7642

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.

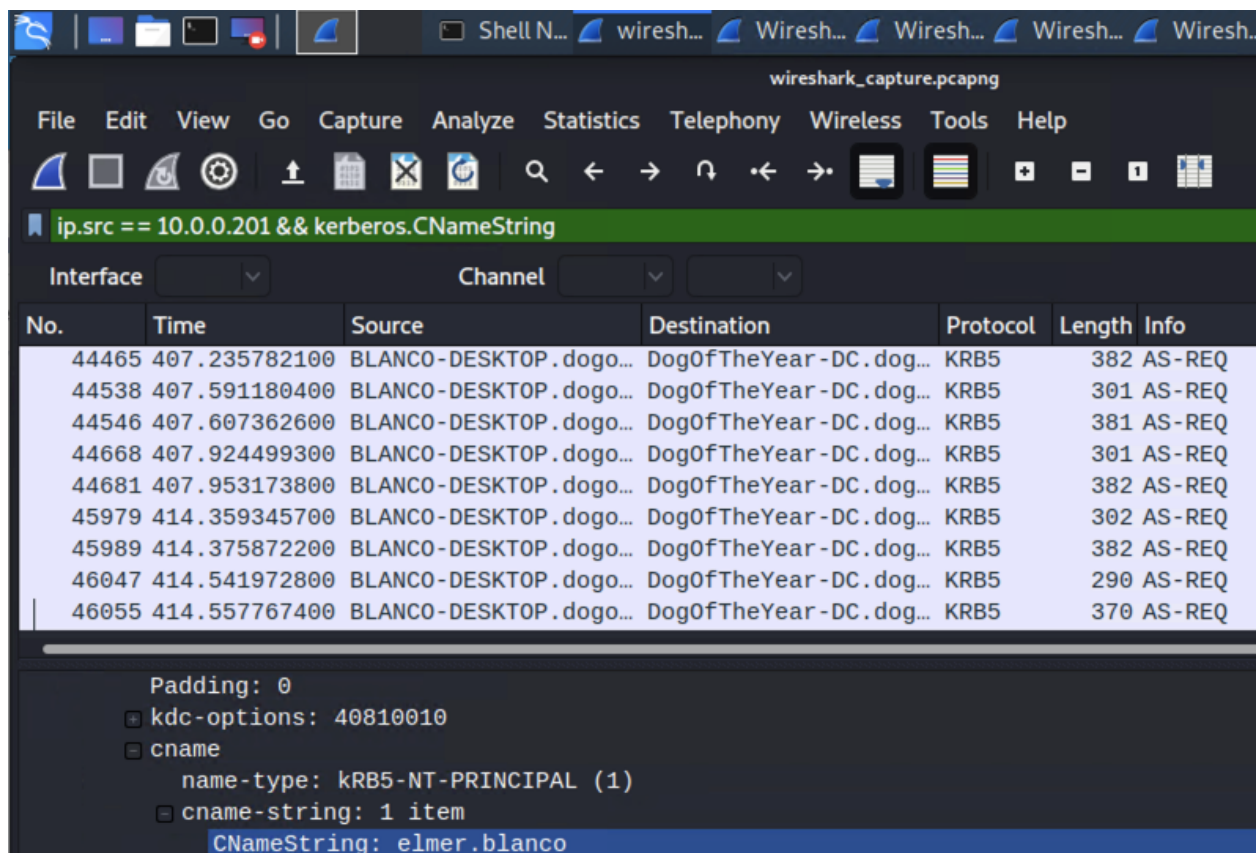
Your task is to isolate torrent traffic and answer the following questions:

1. Find the following information about the machine with IP address 10.0.0.201:

- MAC address: 00:16:17:18:66:c8

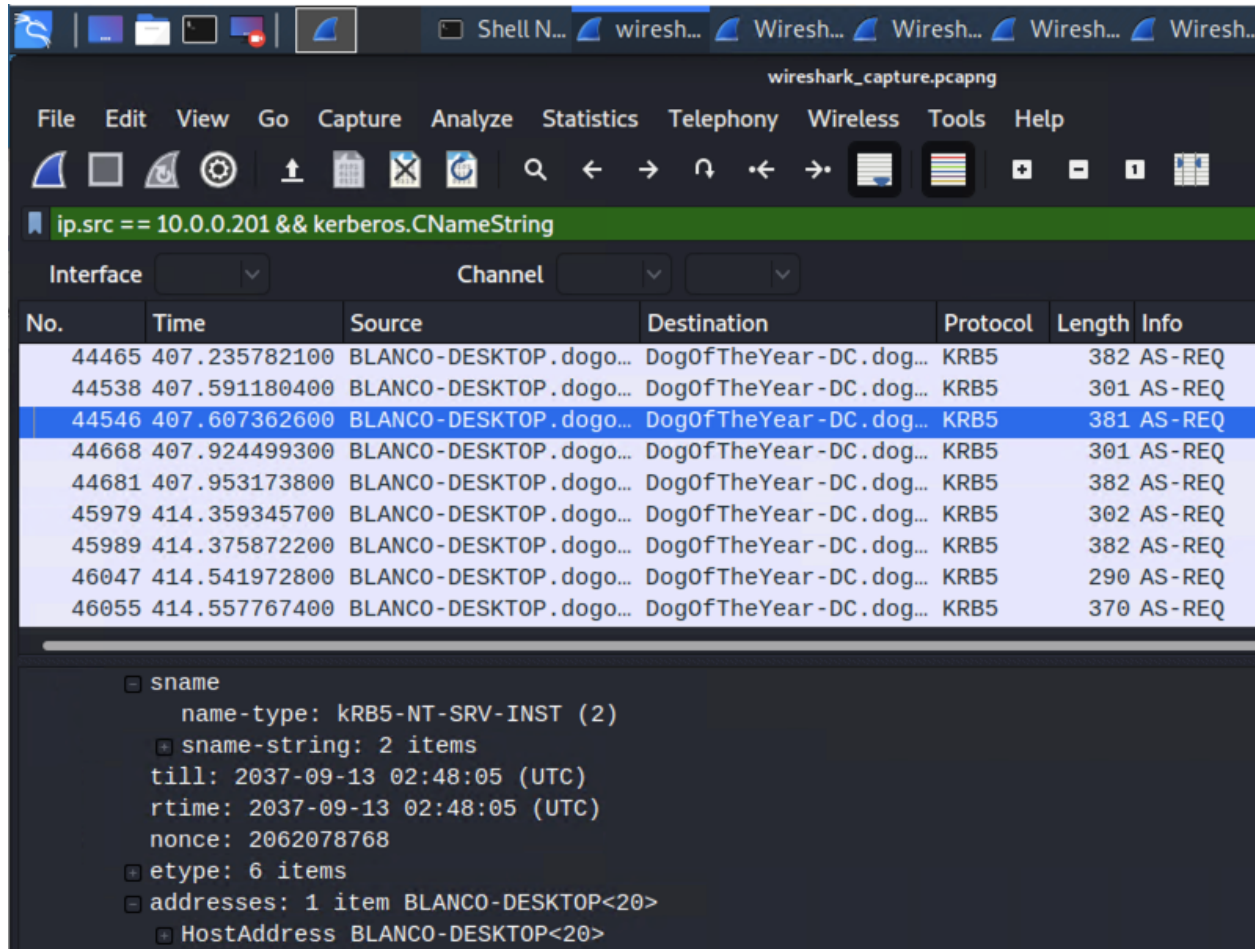
- Windows username

Elmer.blanco



- HOST name

BLANCO-DESKTOP<20>



2. Which torrent file did the user download?

Betty_Boop_Rhythm_on_the_Reservation.avi.torrent

File Action Media Clipboard View Help

Shell N... wiresh... Wiresh... Wiresh... Wiresh... Wiresh... Wiresh... 09:56 AM

wireshark_capture.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 10.0.0.201 && (http.request.uri contains ".torrent")

Interface Channel 802.11 Preferences

No.	Time	Source	Destination	Protocol	Length	Info
48939	433.718641500	BLANCO-DESKTOP.dogo...	files.publicdomaint...	HTTP	589	GET /bt/btdownload.php?type=torrent&file=Betty_B

Destination: files.publicdomaintorrents.com (168.215.194.14)

- Transmission Control Protocol, Src Port: 49834 (49834), Dst Port: http (80), Seq: 1, Ack: 1, Len: 535
- Hypertext Transfer Protocol
 - GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n
 - 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\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