

Network Analysis

By Leo Katz

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?

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

Filter: `ip.src == 10.6.12.0/24`

No.	Time	Source	Destination	Protocol	Length	Info
1793	25.144487900	Frank-n-Ted-DC.frank-n-ted.com	LAPTOP-5WKHX9YG.fra...	SMB2	378	Create Response File:
1795	25.158155300	Frank-n-Ted-DC.frank-n-ted.com	LAPTOP-5WKHX9YG.fra...	SMB2	594	Find Response; Find Response, Error: STATUS_NO_MORE_FILES
3738	56.202410700	Frank-n-Ted-DC.frank-n-ted.com	LAPTOP-5WKHX9YG.fra...	NBNS	104	Name query response NB 10.6.12.12
3805	56.382529500	Frank-n-Ted-DC.frank-n-ted.com	dns.google	DNS	104	Standard query 0x147e A wns.notify.windows.com.akadns.net OPT
3807	56.388140700	Frank-n-Ted-DC.frank-n-ted.com	LAPTOP-5WKHX9YG.fra...	DNS	188	Standard query response 0x27de A client.wns.windows.com CNAME
3839	56.527543300	Frank-n-Ted-DC.frank-n-ted.com	LAPTOP-5WKHX9YG.fra...	TCP	66	[TCP Keep-Alive ACK] microsoft-ds(445) -> 49715 [ACK] Seq=865
3842	56.534405500	Frank-n-Ted-DC.frank-n-ted.com	dns.google	DNS	111	Standard query 0x8e40 A a-0001.a-afentry.net.trafficmanager..
3844	56.540300200	Frank-n-Ted-DC.frank-n-ted.com	LAPTOP-5WKHX9YG.fra...	DNS	193	Standard query response 0x5c81 A www.bing.com CNAME a-0001.a-
3874	56.718060800	Frank-n-Ted-DC.frank-n-ted.com	dns.google	DNS	104	Standard query 0xbacd A settingsfd-geo.trafficmanager.net OPT
3877	56.722392400	Frank-n-Ted-DC.frank-n-ted.com	dns.google	DNS	89	Standard query 0x3a4d m.root-servers.net OPT
3879	56.725517700	Frank-n-Ted-DC.frank-n-ted.com	dns.google	DNS	104	Standard query 0x5d36 A settingsfd-geo.trafficmanager.net OPT
3882	56.731583500	Frank-n-Ted-DC.frank-n-ted.com	LAPTOP-5WKHX9YG.fra...	DNS	154	Standard query response 0x3d12 A settings-win.data.microsoft..

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

a. 10.6.12.12

Filter: `ip.src == 10.6.12.0/24`

No.	Time	Source	Destination	Protocol	Length	Info
1793	25.144487900	Frank-n-Ted-DC.frank-n-ted.com	LAPTOP-5WKHX9YG.fra...	SMB2	378	Create Response File:
1795	25.158155300	Frank-n-Ted-DC.frank-n-ted.com	LAPTOP-5WKHX9YG.fra...	SMB2	594	Find Response; Find Response, Error: STATUS_NO_MORE_FILES
3738	56.202410700	Frank-n-Ted-DC.frank-n-ted.com	LAPTOP-5WKHX9YG.fra...	NBNS	104	Name query response NB 10.6.12.12
3805	56.382529500	Frank-n-Ted-DC.frank-n-ted.com	dns.google	DNS	104	Standard query 0x147e A wns.notify.windows.com.akadns.net OPT
3807	56.388140700	Frank-n-Ted-DC.frank-n-ted.com	LAPTOP-5WKHX9YG.fra...	DNS	188	Standard query response 0x27de A client.wns.windows.com CNAME
3839	56.527543300	Frank-n-Ted-DC.frank-n-ted.com	LAPTOP-5WKHX9YG.fra...	TCP	66	[TCP Keep-Alive ACK] microsoft-ds(445) -> 49715 [ACK] Seq=865
3842	56.534405500	Frank-n-Ted-DC.frank-n-ted.com	dns.google	DNS	111	Standard query 0x8e40 A a-0001.a-afentry.net.trafficmanager..
3844	56.540300200	Frank-n-Ted-DC.frank-n-ted.com	LAPTOP-5WKHX9YG.fra...	DNS	193	Standard query response 0x5c81 A www.bing.com CNAME a-0001.a-
3874	56.718060800	Frank-n-Ted-DC.frank-n-ted.com	dns.google	DNS	104	Standard query 0xbacd A settingsfd-geo.trafficmanager.net OPT
3877	56.722392400	Frank-n-Ted-DC.frank-n-ted.com	dns.google	DNS	89	Standard query 0x3a4d m.root-servers.net OPT
3879	56.725517700	Frank-n-Ted-DC.frank-n-ted.com	dns.google	DNS	104	Standard query 0x5d36 A settingsfd-geo.trafficmanager.net OPT
3882	56.731583500	Frank-n-Ted-DC.frank-n-ted.com	LAPTOP-5WKHX9YG.fra...	DNS	154	Standard query response 0x3d12 A settings-win.data.microsoft..

Internet Protocol Version 4, Src: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12), Dst: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203)

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 580
Identification: 0x5000 (20480)
Flags: 0x4000, Don't fragment
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x7bd1 [validation disabled]
[Header checksum status: Unverified]
Source: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12)
Destination: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203)

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.
- a. June11.dll

The image displays a Wireshark packet capture analysis. The top section shows the packet list with three entries:

No.	Time	Source	Destination	Protocol	Length	Info
80059	822.432672300	DESKTOP-86J4BX.frank-n-ted.com	cardboardspacest...	HTTP	513	GET /logs/invoice-86495.doc HTTP/1.1
81044	828.735165700	LAPTOP-5WKHX9YG.frank-n-ted.com	205.185.125.104	HTTP	275	GET /p08twj HTTP/1.1
81048	828.750543100	LAPTOP-5WKHX9YG.frank-n-ted.com	205.185.125.104	HTTP	312	GET /files/june11.dll HTTP/1.1

The bottom section shows the packet details for the selected packet (No. 81048):

Transmission Control Protocol, Src Port: 49739 (49739), Dst Port: http (80), Seq: 222, Ack: 489, Len: 258

Hypertext Transfer Protocol

- GET /files/june11.dll HTTP/1.1\r\n
 - [Expert Info (Chat/Sequence): GET /files/june11.dll HTTP/1.1\r\n]
 - [GET /files/june11.dll HTTP/1.1\r\n]
 - [Severity level: Chat]
 - [Group: Sequence]
 - Request Method: GET
 - Request URI: /files/june11.dll
 - Request Version: HTTP/1.1
 - 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

The packet bytes section shows the raw data of the GET request, including the headers and the body.

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

VirusTotal - File - d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

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

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

50 / 69

50 security vendors and 1 sandbox flagged this file as malicious

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

549.84 KB Size

2022-04-18 23:52:42 UTC 12 days ago

GoogleIpdte.exe

invalid-signature overlay pedll signed spreader

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

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	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@aul7OOgi
Bkav Pro	W32.AIDetect.malware2	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsale	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
- IP address: 172.16.4.205
- MAC address: 00:59:07:b0:63:a4

The image shows a Wireshark packet capture interface. The top toolbar includes icons for file operations, network analysis, and search. Below the toolbar, a filter bar shows the filter 'ip.addr == 172.16.4.0/24'. The packet list pane displays a series of packets from 22673 to 22693, all originating from 'Rotterdam-PC.mind-hammer.net' and destined for 'mind-hammer-dc.mind-hammer.net'. The protocols shown are TCP and DRSUAPI. The packet details pane for packet 22693 shows a DCE/RPC request (DRSUAPI) with a 'DsCrackNames request' context item. The packet bytes pane shows the raw data of the request, including the '4-R@...' header and the '1-S...' body.

No.	Time	Source	Destination	Protocol	Length	Info
22673	220.009268100	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	TCP	56	49165 → kerberos(88) [ACK] Seq=1650 Ack=1626 Win=65536 Len=0
22674	220.010145300	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	TCP	56	49165 → kerberos(88) [FIN, ACK] Seq=1650 Ack=1626 Win=65536 Len=0
22677	220.036122100	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	TCP	1514	49162 → 49155 [ACK] Seq=1 Ack=1 Win=65536 Len=1460 [TCP segment of data length 1460 bytes]
22678	220.046133100	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	DCERPC	624	Bind: call_id: 2, Fragment: Single, 3 context items: DRSUAPI
22681	220.056761400	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	DCERPC	274	Alter_context: call_id: 2, Fragment: Single, 1 context items: DRSUAPI
22683	220.064183300	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	DRSUAPI	306	DsBind request
22685	220.073458800	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	DRSUAPI	322	DsCrackNames request
22687	220.085578700	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	DRSUAPI	322	DsCrackNames request
22689	220.095199700	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	DRSUAPI	194	DsUnbind request
22691	220.099965600	Rotterdam-PC.mind-hammer.net	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<20>
22692	220.101726500	Rotterdam-PC.mind-hammer.net	172.16.4.255	NBNS	110	Registration NB MIND-HAMMER<00>
22693	220.103482400	Rotterdam-PC.mind-hammer.net	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<00>

Detailed view of packet 22693:

- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 308
- Identification: 0x0052 (82)
- Flags: 0x4000, Don't fragment
- .. 0 0000 0000 0000 = Fragment offset: 0
- Time to live: 128
- Protocol: TCP (6)
- Header checksum: 0x9880 [validation disabled]
- [Header checksum status: Unverified]
- Source: Rotterdam-PC.mind-hammer.net (172.16.4.205)
- Destination: mind-hammer-dc.mind-hammer.net (172.16.4.4)
- Transmission Control Protocol, Src Port: 49162 (49162), Dst Port: 49155 (49155), Seq: 2771, Ack: 974, Len: 268
- Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Request, Fragment: Single, FragLen: 268, Call: 4, Ctx: 1, [Resp: #22688]
- DRSUAPI, DsCrackNames

Packet bytes (hex and ASCII):

```
0010 01 34 00 52 40 00 00 06 98 80 ac 10 04 cd ac 10 4-R@... ..  
0020 04 04 c0 0a c0 03 27 6c be 10 53 e9 ae d5 50 18 .....1..S...P.  
0030 00 fc 26 42 00 00 05 00 00 03 10 00 00 00 0c 01 ..&B.....  
0040 4c 00 04 00 00 00 9c 00 00 00 01 00 0c 00 8d 04 L.....  
0050 d3 fb 95 bf 7d e8 f9 c0 38 7a d1 c2 cd 3b da 46 ....}...8Z...;F  
0060 8c 0b 15 94 b9 f1 9e 63 4d 10 6e f8 ac 0b e3 c6 ....C M n....  
0070 a2 8f 30 90 4b 6c d6 42 2b 94 b0 e7 8d d6 43 96 ..9.K1.B+...C.  
0080 ac 3e bc b0 eb 23 8f a0 4e 49 24 cb 04 f1 db a1 >...#...NIS..  
0090 11 0b ca 45 45 c6 c4 d7 90 c7 ec 25 61 39 2b e8 ...EE.....%a9+.  
00a0 66 82 83 a4 67 d0 bb dd bc 1c e7 08 b3 53 5e ac f...g.....S^..  
00b0 7c c5 41 31 28 2b 81 90 7b c2 22 ea 7a 51 34 fc |.A1(+...{"zQ4.  
00c0 fb 8d 6a 5f f9 74 40 af 88 0e ac 14 aa 72 a8 20 ..j..t0.....r..  
00d0 93 4b 10 fd da ad bb 12 1c 57 19 32 e2 68 e1 82 .K.....W-2-h..  
00e0 6f 3c b1 8a cc fd d4 e4 b0 c9 e0 42 d2 97 09 06 oK.....B.....  
00f0 04 00 00 00 00 05 04 06 ff 00 10 00 1c 00 00 .....  

```

ip.addr == 172.16.4.205

Filter Buttons Preferences... Label: Enter a description for the filter button Filter: ip.addr == 10.6.12.0/24 OK Cancel

Comment: Enter a comment for the filter button

No.	Time	Source	Destination	Protocol	Length	Info
52206	632.501276600	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	SMB2	182	Ioctl Request FSCTL_DFS_GET_REFERRALS, File:
52208	632.506559800	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	TCP	56	49273 → microsoft-ds(445) [ACK] Seq=3881 Ack=1069 Win=64512 L
52209	632.511968800	Rotterdam-PC.mind-hammer.net	hostedby.privatelay...	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-
52211	632.513947900	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	SMB2	126	Tree Disconnect Request
52212	632.515969400	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	SMB2	126	Session Logoff Request
52215	632.520894300	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	TCP	56	49273 → microsoft-ds(445) [ACK] Seq=4025 Ack=1213 Win=64256 L
52216	632.521784300	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	TCP	56	49273 → microsoft-ds(445) [RSI, ACK] Seq=4025 Ack=1213 Win=0
52217	632.526303600	Rotterdam-PC.mind-hammer.net	hostedby.privatelay...	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-
52219	632.531679000	Rotterdam-PC.mind-hammer.net	hostedby.privatelay...	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-
52221	632.537057800	Rotterdam-PC.mind-hammer.net	hostedby.privatelay...	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-
52223	632.542427800	Rotterdam-PC.mind-hammer.net	hostedby.privatelay...	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-
52225	632.547802800	Rotterdam-PC.mind-hammer.net	hostedby.privatelay...	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-

Frame 52216: 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)

Source: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)

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: 49273 (49273), Dst Port: microsoft-ds (445), Seq: 4025, Ack: 1213, Len: 0

VSS Monitoring Ethernet trailer, Source Port: 39424

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

- o mattijs.devries

ip.addr == 172.16.4.205 && kerberos.CNameString

Filter Buttons Preferences... Label: Enter a description for the filter button Filter: ip.addr == 10.6.12.0/24 OK Cancel

Comment: Enter a comment for the filter button

No.	Time	Source	Destination	Protocol	Length	Info
22650	219.900447600	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	KRB5	297	AS-REQ
22658	219.917629400	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	KRB5	377	AS-REQ
22828	220.698271700	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	KRB5	301	AS-REQ
22835	220.713910400	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	KRB5	381	AS-REQ
22867	220.849593000	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	KRB5	292	AS-REQ
22874	220.856144300	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	KRB5	372	AS-REQ
22660	219.945151000	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	204	AS-REP
22672	220.008398000	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	219	TGS-REP
22713	220.249451300	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	158	TGS-REP
22733	220.355755600	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	84	TGS-REP
22837	220.741423800	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	204	AS-REP
22849	220.802038500	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	KRB5	130	TGS-REP

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>

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

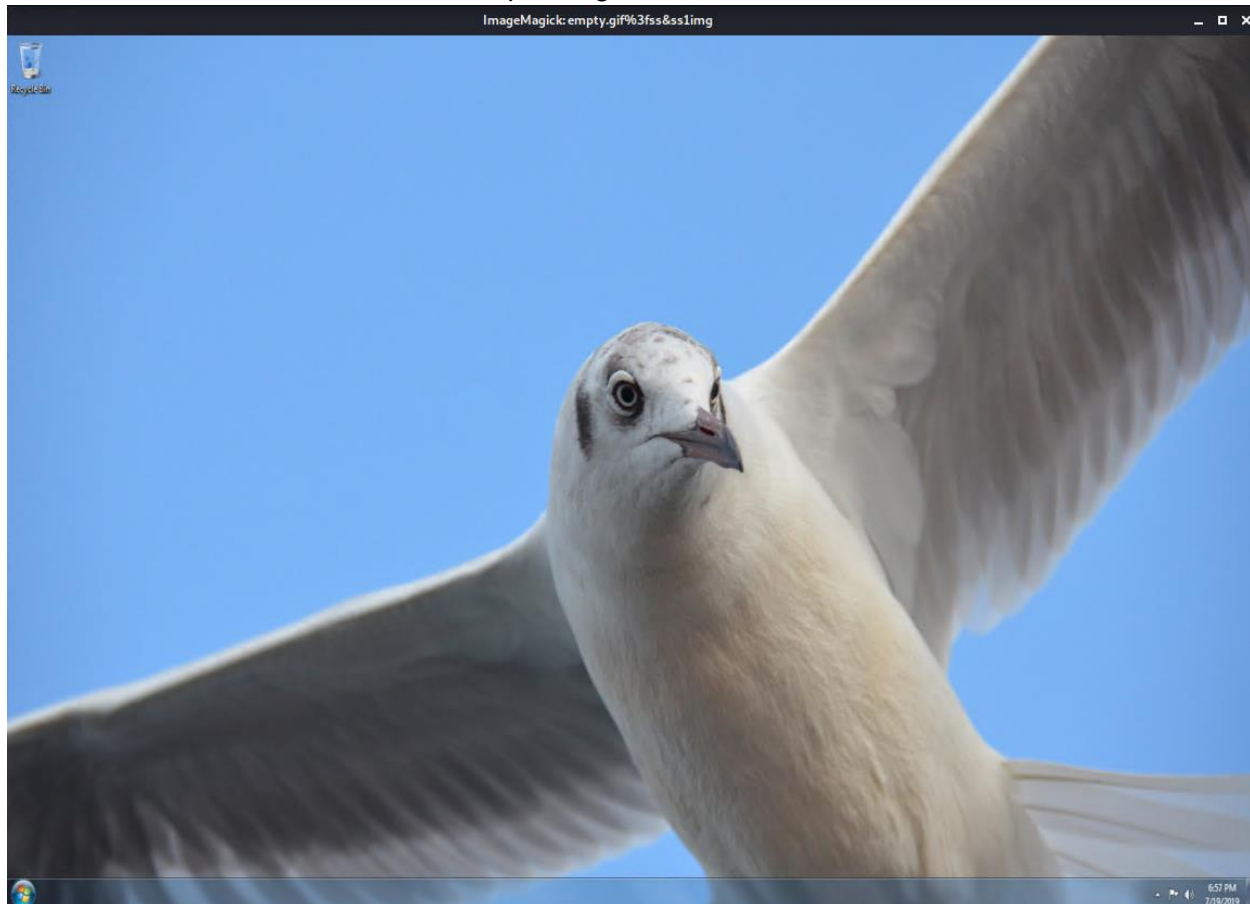
- o 172.16.4.205 and 185.243.115.84

Wireshark - Conversations - network_capture_1.pcapng

Ethernet · 77		IPv4 · 879		IPv6 · 3		TCP · 1051		UDP · 1814			
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	366.268225	265.0412	240 k	
5.101.51.151	10.6.12.203	7,896	7,763 k	5,959	7,643 k	1,937	120 k	0.000000	908.0032	67 k	
166.62.111.64	172.16.4.205	7,864	8,082 k	5,677	7,921 k	2,187	160 k	221.275170	149.9677	422 k	
192.168.1.90	192.168.1.100	5,562	26 M	3,623	26 M	1,939	556 k	6.348153	992.6524	210 k	
10.0.0.201	64.187.66.143	5,227	3,873 k	2,402	156 k	2,825	3,717 k	90.065485	860.7093	1,450	
10.0.0.201	23.43.62.169	4,007	4,080 k	1,310	71 k	2,697	4,008 k	151.705141	66.9059	8,605	
10.11.11.200	151.101.50.208	3,270	2,220 k	1,613	112 k	1,657	2,108 k	742.031422	66.7937	13 k	
10.0.0.2	10.0.0.201	2,138	529 k	1,027	264 k	1,111	264 k	61.924605	884.2207	2,396	
10.6.12.12	10.6.12.203	1,673	405 k	736	185 k	937	220 k	25.138440	888.4694	1,669	
10.6.12.12	10.6.12.157	1,475	354 k	670	165 k	805	188 k	56.839601	856.6991	1,548	
10.0.0.201	172.217.9.2	1,108	564 k	530	62 k	578	501 k	71.325252	867.4318	576	
10.11.11.11	10.11.11.200	1,100	219 k	493	98 k	607	120 k	634.192542	176.9289	4,459	
10.11.11.200	104.18.74.113	1,079	697 k	511	34 k	568	662 k	786.344185	22.4915	12 k	
10.0.0.201	96.7.89.194	974	332 k	400	66 k	574	266 k	64.750683	856.1576	616	
172.16.4.4	172.16.4.205	947	227 k	457	96 k	490	131 k	219.890699	414.0451	1,862	
10.0.0.201	168.215.194.14	858	551 k	364	34 k	494	516 k	70.726301	871.0069	319	
10.11.11.11	10.11.11.203	843	189 k	351	83 k	492	106 k	638.444425	172.6836	3,858	
10.11.11.179	13.33.255.25	728	520 k	339	34 k	389	485 k	645.533741	94.0159	2,950	
10.0.0.201	216.58.218.161	708	422 k	318	27 k	390	395 k	75.610606	855.6138	254	
10.11.11.217	172.217.6.162	697	404 k	341	35 k	356	369 k	701.008110	106.4835	2,664	
10.6.12.203	205.185.125.104	649	599 k	186	10 k	463	588 k	56.833981	851.7094	98	
10.11.11.179	143.204.29.89	449	295 k	217	22 k	232	273 k	645.528749	74.8400	2,361	
10.11.11.11	10.11.11.179	440	43 k	112	17 k	328	26 k	633.961277	84.0332	1,620	
10.11.11.11	10.11.11.195	418	35 k	103	10 k	315	25 k	636.490058	173.6506	481	
10.11.11.195	12.133.50.21	417	219 k	192	19 k	225	199 k	676.291489	102.8962	1,541	
10.11.11.179	31.13.93.26	410	291 k	171	13 k	239	278 k	664.567006	71.9760	1,532	
10.11.11.179	172.217.6.162	402	239 k	191	18 k	211	220 k	692.660302	49.3573	3,005	
10.11.11.203	188.95.248.71	376	410 k	86	5,474	290	405 k	720.676394	8.0123	5,465	
31.13.70.52	172.16.4.205	363	239 k	218	223 k	145	15 k	232.816832	138.1120	12 k	
93.95.100.178	172.16.4.205	361	209 k	209	195 k	152	14 k	286.676895	85.7427	18 k	
10.11.11.179	172.217.6.162	357	260 k	150	11 k	100	260 k	717.912047	24.1537	2,005	

☐ Name resolution
 ☐ Limit to display filter
 ☐ Absolute start time
 Conversation Types ▾
 Copy ▾ Follow Stream... Graph... X Close Help

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



Illegal Downloads

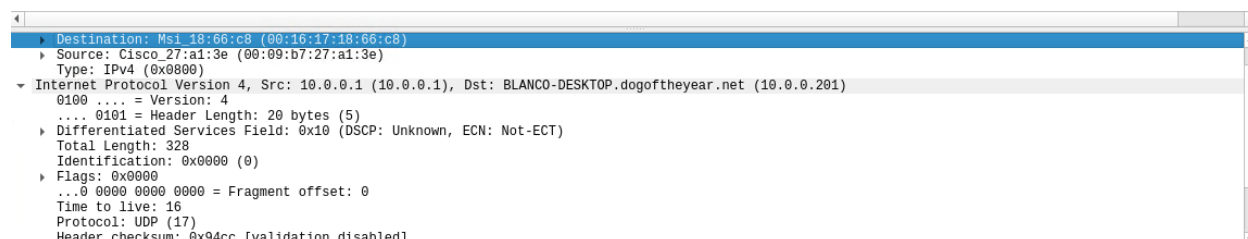
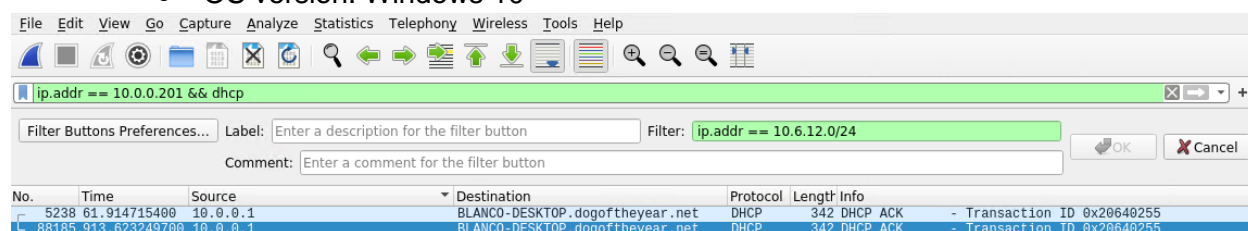
IT was informed that some users are torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringement.

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 Help

ip.addr == 10.0.0.201 && kerberos.CNameString

Filter Buttons Preferences... Label: Enter a description for the filter button Filter: ip.addr == 10.6.12.0/24 OK Cancel

Comment: Enter a comment for the filter button

No.	Time	Source	Destination	Protocol	Length	Info
5467	62.812989900	DogOfTheYear-DC.dogoftheyear.net	BLANCO-DESKTOP.dogoftheyear.net	KRB5	114	TGS-REP
5544	63.043192400	DogOfTheYear-DC.dogoftheyear.net	BLANCO-DESKTOP.dogoftheyear.net	KRB5	250	AS-REP
5557	63.109455300	DogOfTheYear-DC.dogoftheyear.net	BLANCO-DESKTOP.dogoftheyear.net	KRB5	293	TGS-REP
5610	63.413960700	DogOfTheYear-DC.dogoftheyear.net	BLANCO-DESKTOP.dogoftheyear.net	KRB5	227	TGS-REP
5639	63.579503300	DogOfTheYear-DC.dogoftheyear.net	BLANCO-DESKTOP.dogoftheyear.net	KRB5	293	TGS-REP
5651	63.638415600	DogOfTheYear-DC.dogoftheyear.net	BLANCO-DESKTOP.dogoftheyear.net	KRB5	114	TGS-REP
6886	69.457772200	DogOfTheYear-DC.dogoftheyear.net	BLANCO-DESKTOP.dogoftheyear.net	KRB5	250	AS-REP
6898	69.520469300	DogOfTheYear-DC.dogoftheyear.net	BLANCO-DESKTOP.dogoftheyear.net	KRB5	199	TGS-REP
6952	69.639239900	DogOfTheYear-DC.dogoftheyear.net	BLANCO-DESKTOP.dogoftheyear.net	KRB5	237	AS-REP
6964	69.700103800	DogOfTheYear-DC.dogoftheyear.net	BLANCO-DESKTOP.dogoftheyear.net	KRB5	175	TGS-REP
6980	69.764976600	DogOfTheYear-DC.dogoftheyear.net	BLANCO-DESKTOP.dogoftheyear.net	KRB5	303	TGS-REP

```

msg-type: krb-tgs-rep (13)
crealm: DOGOFtheyear.NET
  cname
    name-type: KRB5-NT-PRINCIPAL (1)
    cname-string: 1 item
      CNameString: elmer.blanco
  ticket
    tkt-vno: 5
    realm: DOGOFtheyear.NET
    sname
    enc-part
    enc-part
      etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
      cipher: c6b5e1d784ab90561ed053fa21b43a6ccb36d9289fd6f50e...

```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.0.0.201 && http.request

Filter Buttons Preferences... Label: Enter a description for the filter button Filter: ip.addr == 10.6.12.0/24 OK Cancel

Comment: Enter a comment for the filter button

No.	Time	Source	Destination	Protocol	Length	Info
7181	70.736559400	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	463	GET /nshowcat.html?category=animation HTTP/1.1
7195	70.846382400	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	474	GET /srsbanner.gif HTTP/1.1
7221	71.081760300	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	477	GET /grabs/hdsale.png HTTP/1.1
7253	71.286488600	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	469	GET /ipod.jpg HTTP/1.1
7255	71.294821100	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	468	GET /pda.jpg HTTP/1.1
7258	71.304214100	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	479	GET /site2/pdheader.jpg HTTP/1.1
7260	71.312572100	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	468	GET /psp.gif HTTP/1.1
7262	71.321010900	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	474	GET /googlevid.jpg HTTP/1.1
7272	71.339771000	BLANCO-DESKTOP.dogoftheyear.net	pagead46.l.doubleclick.net	HTTP	445	GET /pagead/js/adsbygoogle.js HTTP/1.1
7286	71.492183100	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	471	GET /rentme.gif HTTP/1.1
7313	71.839915600	BLANCO-DESKTOP.dogoftheyear.net	digg.com	HTTP	417	GET /tools/diggthis.js HTTP/1.1
7427	72.701790000	BLANCO-DESKTOP.dogoftheyear.net	scripts-tnfdwtoaiaoiwsartb.stacko	HTTP	427	GET /eminimalis/mm.js HTTP/1.1

```

GET /nshowcat.html?category=animation HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): GET /nshowcat.html?category=animation HTTP/1.1\r\n]
  [GET /nshowcat.html?category=animation HTTP/1.1\r\n]
  [Severity level: Chat]
  [Group: Sequence]
  Request Method: GET
  Request URI: /nshowcat.html?category=animation
  Request Version: HTTP/1.1
  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
  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
  Host: publicdomaintorrents.info\r\n

```

2. Which torrent file did the user download?

- o Betty_Boop_Rythm_on_the_Reservation.avi



ip.addr == 10.0.0.201 && http.request.method == GET

Filter Buttons Preferences... Label: Enter a description for the filter button Filter: ip.addr == 10.6.12.0/24
Comment: Enter a comment for the filter button OK Cancel

No.	Time	Source	Destination	Protocol	Length	Info
9619	87.965877300	BLANCO-DESKTOP.dogoftheyear.net	fls-na.amazon-adsystem.com	HTTP	1067	GET /1/associates-ads/1/OP/?cb=1531628232887&p=
9855	88.772318000	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	589	GET /bt/btdownload.php?type=torrent&file=Betty
9899	88.968626100	BLANCO-DESKTOP.dogoftheyear.net	ftp.osuosl.org	HTTP	195	GET /version-1.0 HTTP/1.1
9903	88.978045300	BLANCO-DESKTOP.dogoftheyear.net	torrent.ubuntu.com	HTTP	423	GET /announce?info_hash=%e4%be%9e%8b%8v%e3%k1%7
10129	89.636508100	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	434	GET /bt/announce.php?info_hash=%1d%da%0d%8%a8%98%
10159	89.713196700	BLANCO-DESKTOP.dogoftheyear.net	moonstar.publicdomaintorrents.com	HTTP	434	GET /announce?info_hash=%1d%da%0d%8%a8%98%bd%81%
10253	89.996303600	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com	HTTP	253	GET /bt/scrape.php?info_hash=%1d%da%0d%8%a8%98%b
10273	90.042672500	BLANCO-DESKTOP.dogoftheyear.net	moonstar.publicdomaintorrents.com	HTTP	253	GET /scrape?info_hash=%1d%da%0d%8%a8%98%bd%81%5c
18240	151.967360900	BLANCO-DESKTOP.dogoftheyear.net	cs9.wac.phicdn.net	HTTP	288	GET /MFEwTzBNMEswSTA3BgUrDgMCGGUABBSAUQYBMq2awn
18244	151.974656200	BLANCO-DESKTOP.dogoftheyear.net	cs9.wac.phicdn.net	HTTP	290	GET /MFEwTzBNMEswSTA3BgUrDgMCGGUABBTBL0V27RVZ7L
18267	152.203765200	BLANCO-DESKTOP.dogoftheyear.net	cs9.wac.phicdn.net	HTTP	292	GET /MFEwTzBNMEswSTA3BgUrDgMCGGUABBTnVAI%2FnN49

Source: Msi_18:66:c8 (00:16:17:18:66:c8)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201), Dst: 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
[Expert Info (Chat/Sequence): GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1
[GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
Request Version: HTTP/1.1
Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513



ip.addr == 10.0.0.201 &&

Filter Buttons Preferences... Label: Enter a description for the filter button Filter: ip.addr == 10.6.12.0/24
Comment: Enter a comment for the filter button OK Cancel

No.	Time	Source	Destination	Protocol	Length	Info
9619	87.965877300	BL				
9855	88.772318000	BL				
9899	88.968626100	BL				
9903	88.978045300	BL				
10129	89.636508100	BL				
10159	89.713196700	BL				
10253	89.996303600	BL				
10273	90.042672500	BL				
18240	151.967360900	BL				
18244	151.974656200	BL				
18267	152.203765200	BL				

Source: Msi_18:66:c8 (00:16:17:18:66:c8)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201), Dst: 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
[Expert Info (Chat/Sequence): GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1
[GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
Request Version: HTTP/1.1
Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513

0030 ff ff 31 06 00 00 41 00 00 00 00 00 00 00 00 00
0040 64 6f 77 6e 6c 6f 6e 6f 6e 6f 6e 6f 6e 6f 6e
0050 65 3d 74 6f 72 72 6f 6e 6f 6e 6f 6e 6f 6e 6f
0060 65 74 74 79 5f 42 6f 6e 6f 6e 6f 6e 6f 6e 6f
0070 5f 6f 6e 5f 74 68 65 5f 52 65 73 65 72 76 61 74
0080 69 6f 6e 2e 61 76 69 2e 74 6f 72 72 65 6e 74 20
0090 48 54 54 50 2f 31 2e 31 0d 0a 52 65 66 65 72 65
00a0 72 3a 20 68 74 74 70 3a 2f 2f 70 75 62 6c 69 63
00b0 64 6f 6d 61 69 6e 74 6f 72 72 65 6e 74 73 2e 69
00c0 6e 66 6f 2f 6e 73 68 6f 77 6d 6f 76 69 65 2e 68
00d0 74 6d 6c 3f 6d 6f 76 69 65 69 64 3d 35 31 33 0d
00e0 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a
00f0 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77
0100 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 34
0110 3b 20 78 36 34 29 20 41 70 70 6c 65 57 65 62 40

Text Filter: betty

Save Save All Close Help

File Name: Betty_Boop_Rhythm_on_the_Reservation.avi

File Size: 100.50 MB

Resolution: 720x480

Duration: 00:06:02

