

## Network Forensic Analysis Report

Submitted by: Yekaterina Alenicheva

### 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:

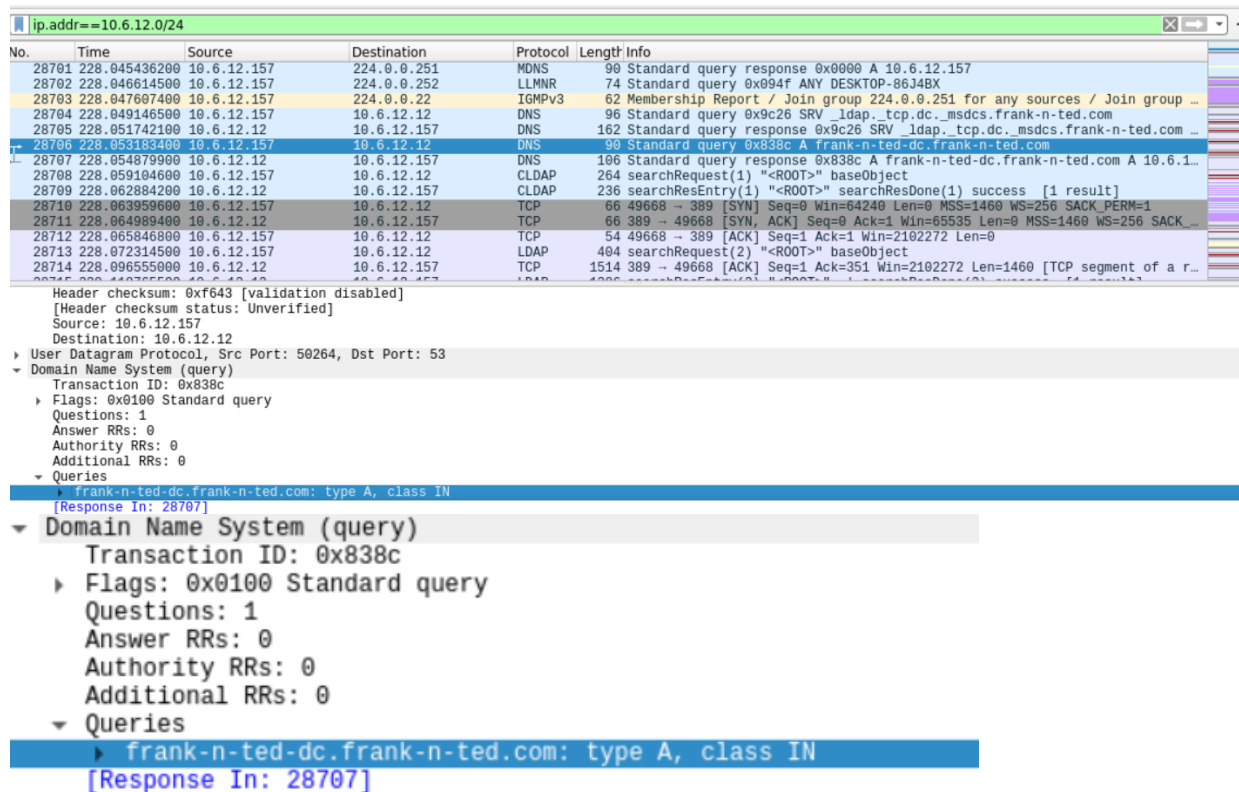
- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.
- Their IP addresses are somewhere in the range `10.6.12.0/24`.

You must inspect your traffic capture to answer the following questions in your Network Report:

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

The domain name is **Frank-n-Ted.DC.frank-n-ted.com**

Filter: ip.addr == 10.6.12.0/24



No.	Time	Source	Destination	Protocol	Length	Info
28701	228.045436200	10.6.12.157	224.0.0.251	MDNS	90	Standard query response 0x0000 A 10.6.12.157
28702	228.046614500	10.6.12.157	224.0.0.252	LLMNR	74	Standard query 0x094f ANY DESKTOP-86J4BX
28703	228.047607400	10.6.12.157	224.0.0.22	IGMPv3	62	Membership Report / Join group 224.0.0.251 for any sources / Join group ...
28704	228.049146500	10.6.12.157	10.6.12.12	DNS	96	Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
28705	228.051742100	10.6.12.12	10.6.12.157	DNS	162	Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com ...
28706	228.053183400	10.6.12.157	10.6.12.12	DNS	90	Standard query 0x838c A frank-n-ted-dc.frank-n-ted.com
28707	228.054879900	10.6.12.12	10.6.12.157	DNS	106	Standard query response 0x838c A frank-n-ted-dc.frank-n-ted.com A 10.6.1...
28708	228.059194600	10.6.12.157	10.6.12.12	LDAP	264	searchRequest(1) "<ROOT>" baseObject
28709	228.062884200	10.6.12.12	10.6.12.157	LDAP	236	searchResEntry(1) "<ROOT>" searchResDone(1) success [1 result]
28710	228.063959600	10.6.12.157	10.6.12.12	TCP	66	49668 -> 389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
28711	228.064989400	10.6.12.12	10.6.12.157	TCP	66	389 -> 49668 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK...
28712	228.065846800	10.6.12.157	10.6.12.12	TCP	54	49668 -> 389 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
28713	228.072314500	10.6.12.157	10.6.12.12	LDAP	404	searchRequest(2) "<ROOT>" baseObject
28714	228.096555900	10.6.12.12	10.6.12.157	TCP	1514	389 -> 49668 [ACK] Seq=1 Ack=351 Win=2102272 Len=1460 [TCP segment of a r...

Header checksum: 0xf643 [validation disabled]  
[Header checksum status: Unverified]  
Source: 10.6.12.157  
Destination: 10.6.12.12  
User Datagram Protocol, Src Port: 50264, Dst Port: 53  
Domain Name System (query)  
Transaction ID: 0x838c  
Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
frank-n-ted-dc.frank-n-ted.com: type A, class IN  
[Response In: 28707]  
Domain Name System (query)  
Transaction ID: 0x838c  
Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
frank-n-ted-dc.frank-n-ted.com: type A, class IN  
[Response In: 28707]

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

IP address is **10.6.12.12** frank-n-ted-dc.frank-n-ted.com.

ip.addr==10.6.12.0/24					
No.	Time	Source	Destination	Protocol	Length Info
28701	228.045436200	10.6.12.157	224.0.0.251	MDNS	90 Standard query response 0x0000 A 10.6.12.157
28702	228.046614500	10.6.12.157	224.0.0.252	LLMNR	74 Standard query 0x094f ANY DESKTOP-86348X
28703	228.047607400	10.6.12.157	224.0.0.22	IGMPv3	62 Membership Report / Join group 224.0.0.251 for any sources / Join group ...
28704	228.049146500	10.6.12.157	10.6.12.12	DNS	96 Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
28705	228.051742100	10.6.12.12	10.6.12.157	DNS	162 Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com ...
28706	228.053183400	10.6.12.157	10.6.12.12	DNS	90 Standard query 0x838c A frank-n-ted-dc.frank-n-ted.com
28707	228.054879900	10.6.12.12	10.6.12.157	DNS	106 Standard query response 0x838c A frank-n-ted-dc.frank-n-ted.com A 10.6.1...
28708	228.059104600	10.6.12.157	10.6.12.12	CLDAP	264 searchRequest(1) "<ROOT>" baseObject
28709	228.062884200	10.6.12.12	10.6.12.157	CLDAP	236 searchResEntry(1) "<ROOT>" searchResDone(1) success [1 result]
28710	228.063959600	10.6.12.157	10.6.12.12	TCP	66 49668 → 389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
28711	228.064989400	10.6.12.12	10.6.12.157	TCP	66 389 → 49668 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK...
28712	228.065846800	10.6.12.157	10.6.12.12	TCP	54 49668 → 389 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
28713	228.072314500	10.6.12.157	10.6.12.12	LDAP	404 searchRequest(2) "<ROOT>" baseObject
28714	228.096555000	10.6.12.12	10.6.12.157	TCP	1514 389 → 49668 [ACK] Seq=1 Ack=351 Win=2102272 Len=1460 [TCP segment of a r...

Header checksum: 0xf643 [validation disabled]  
[Header checksum status: Unverified]  
Source: 10.6.12.157  
Destination: 10.6.12.12

User Datagram Protocol, Src Port: 50264, Dst Port: 53

Domain Name System (query)  
Transaction ID: 0x838c  
Flags: 0x0100 Standard query  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0

Queries  
frank-n-ted-dc.frank-n-ted.com: type A, class IN  
[Response in: 28707]

3. What is the name of the malware downloaded to the 10.6.12.203 machine?

Malware file is **june11.dll**

Filter: ip.addr==10.16.12.203 and http.request.method==GET

Export: File > Export Objects > HTTP

ip.addr==10.6.12.203 and http.request.method==GET					
No.	Time	Source	Destination	Protocol	Length Info
32205	245.613018000	10.6.12.203	205.185.125.104	HTTP	275 GET /pQbtWj HTTP/1.1
32209	245.628416100	10.6.12.203	205.185.125.104	HTTP	312 GET /files/june11.dll HTTP/1.1

Flags: 0x018 (PSH, ACK)  
Window size value: 65535  
[Calculated window size: 65535]  
[Window size scaling factor: -2 (no window scaling used)]  
Checksum: 0x341f [unverified]  
[Checksum Status: Unverified]  
Urgent pointer: 0

[SEQ/ACK analysis]  
[Timestamps]  
TCP payload (258 bytes)

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=3mmhfd8jp\r\n  
\r\n  
[Full request URI: http://205.185.125.104/files/june11.dll]  
[HTTP request 2/2]  
[Prev request in frame: 32205]  
[Response in frame: 32959]

```

    for payload (256 bytes)
  ▾ 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
      \r\n
      [Full request URI: http://205.185.125.104/files/june11.dll]
      [HTTP request 2/2]
      [Prev request in frame: 32205]
      [Response in frame: 32206]

```

Packet	Hostname	Content Type	Size	Filename
32959	205.185.125.104	application/octet-stream	563 kB	june11.dll

Text Filter:

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

According to VirusTotal this type of malware is Trojan

**53** / 68

53 security vendors flagged this file as malicious

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

549.84 KB Size | 2021-07-12 00:39:37 UTC | 1 day ago

june11.dll

invalid-signature overlay pedll signed

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	① Trojan.Mint.Zamg.O	AhnLab-V3	① Malware/Win32.RL_Generic.R346613	
Alibaba	① TrojanSpy:Win32/Yakes.56555f48	Antiy-AVL	① Trojan/Generic.ASCommon.1BE	
SecureAge APEX	① Malicious	Avast	① Win32:DangerousSig [Trj]	
AVG	① Win32:DangerousSig [Trj]	Avira (no cloud)	① TR/AD.ZLoader.ladbd	
BitDefender	① Trojan.Mint.Zamg.O	BitDefenderTheta	① Gen:NN.ZedlaF.34790.lu9@aui7OQgi	

## Vulnerable Windows Machine

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 in your network report:

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**

Filter: `ip.src == 172.16.4.4` and `Kerberos.CnameString`

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help					
ip.src == 172.16.4.4 and kerberos.CNameString					
No.	Time	Source	Destination	Protocol	Length Info
161.901578...		mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-h...	KRB5	204 AS-REP
161.964848...		mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-h...	KRB5	219 TGS-REP
162.205913...		mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-h...	KRB5	158 TGS-REP
162.312192...		mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-h...	KRB5	84 TGS-REP
162.697867...		mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-h...	KRB5	204 AS-REP
162.758486...		mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-h...	KRB5	130 TGS-REP
162.840709...		mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-h...	KRB5	242 AS-REP
162.900060...		mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-h...	KRB5	150 TGS-REP
162.965046...		mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-h...	KRB5	273 TGS-REP
319.976733...		mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-h...	KRB5	206 TGS-REP
320.033871...		mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-h...	KRB5	72 TGS-REP
573.652360...		mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-h...	KRB5	206 TGS-REP
575.002070...		mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-h...	KRB5	84 TGS-REP

Frame 18512: 204 bytes on wire (1632 bits), 204 bytes captured (1632 bits) on interface eth0, id 0  
 Ethernet II, Src: Dell\_19:49:50 (a4:ba:db:19:49:50), Dst: LenovoEM\_b0:63:a4 (00:59:07:b0:63:a4)  
 Internet Protocol Version 4, Src: 172.16.4.4, Dst: 172.16.4.205  
 Transmission Control Protocol, Src Port: 88, Dst Port: 49164, Seq: 1461, Ack: 324, Len: 150  
 [2 Reassembled TCP Segments (1610 bytes): #18511(1460), #18512(150)]

2. What is the username of the Windows user whose computer is infected?  
The username is **matthijs.devries**

Filter: ip.src == 172.16.4.205 and Kerberos.CnameString

ip.src == 172.16.4.205 and kerberos.CNameString					
No.	Time	Source	Destination	Protocol	Length Info
161.856889...		Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind...	KRB5	297 AS-REQ
161.874109...		Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind...	KRB5	377 AS-REQ
162.654727...		Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind...	KRB5	301 AS-REQ
162.670341...		Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind...	KRB5	381 AS-REQ
162.797077...		Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind...	KRB5	292 AS-REQ
162.812583...		Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind...	KRB5	372 AS-REQ

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

According to Statistics > Conversations IPv4 > 172.16.4.205 > search for highest packets bytes number that indicated suspicious traffic between IPs. As results found the the communication between 172.16.4.205 and 185.243.115.84 are infected traffic. Apply filter to find details of the communication between two Ips.

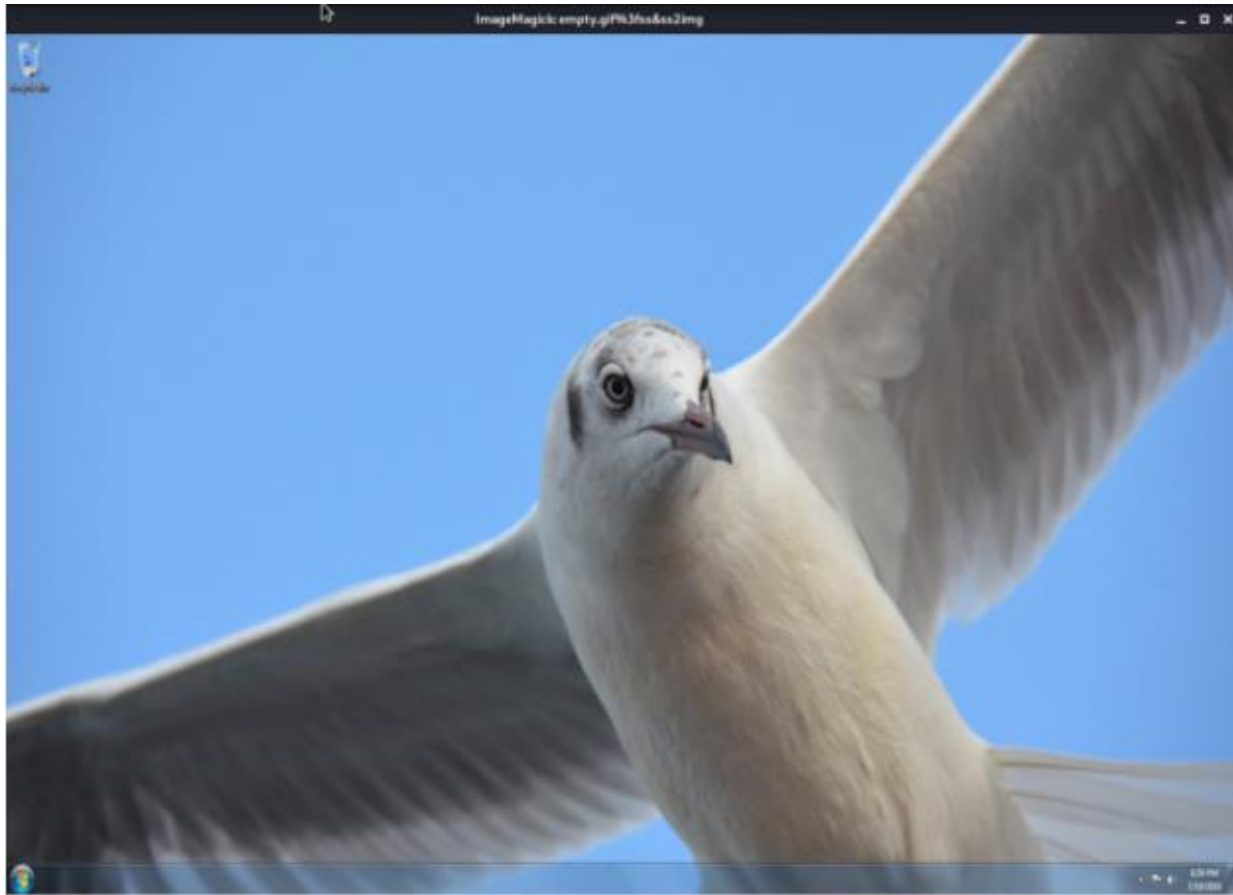
Filter: ip.addr == 172.16.4.205 and ip.addr == 185.243.115.84

Ethernet · 76		IPv4 · 882		IPv6	TCP · 1050		UDP · 1825					
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Durati			
10.11.11.195	12.133.50.21	417	219 k	192	19 k	225	199 k	618.247945	102.			
10.11.11.11	10.11.11.195	418	35 k	103	10 k	315	25 k	578.446497	173.			
10.11.11.11	10.11.11.179	440	43 k	112	17 k	328	26 k	575.917738	84.			
10.11.11.179	143.204.29.89	449	295 k	217	22 k	232	273 k	587.485181	74.8			
10.6.12.203	205.185.125.104	647	599 k	185	10 k	462	588 k	770.685389	79.8			
10.11.11.217	172.217.6.162	697	404 k	341	35 k	356	369 k	642.964546	106.			
93.95.100.178	172.16.4.205	722	419 k	418	391 k	304	28 k	228.633333	937.			
31.13.70.52	172.16.4.205	726	479 k	436	447 k	290	31 k	174.773289	989.			
10.11.11.179	13.33.255.25	728	520 k	339	34 k	389	485 k	587.490187	94.0			
10.0.0.201	216.58.218.161	732	424 k	330	27 k	402	396 k	17.567069	896.			
10.11.11.11	10.11.11.203	843	189 k	351	83 k	492	106 k	580.404235	172.			
10.0.0.201	168.215.194.14	878	552 k	374	35 k	504	516 k	12.682745	901.			
10.0.0.201	96.7.89.194	974	332 k	400	66 k	574	266 k	6.707118	856.			
10.11.11.200	104.18.74.113	1,079	697 k	511	34 k	568	662 k	728.300606	22.4			
10.11.11.11	10.11.11.200	1,100	219 k	493	98 k	607	120 k	576.148994	176.			
10.0.0.201	172.217.9.2	1,132	565 k	542	63 k	590	502 k	13.281690	901.			
168.63.129.16	192.168.1.90	1,133	120 k	506	66 k	627	53 k	429.380897	482.			
172.16.4.4	172.16.4.205	1,417	339 k	680	147 k	737	191 k	161.847139	1144.			
10.6.12.12	10.6.12.157	1,450	352 k	662	164 k	788	187 k	0.006842	855.			
10.6.12.12	10.6.12.203	1,624	398 k	720	183 k	904	215 k	0.000000	855.			
10.0.0.2	10.0.0.201	2,166	532 k	1,040	267 k	1,126	265 k	3.881039	941.			
10.11.11.200	151.101.50.208	3,270	2,220 k	1,613	112 k	1,657	2,108 k	683.987858	66.7			
5.101.51.151	10.6.12.203	4,326	4,246 k	3,262	4,177 k	1,064	68 k	781.964292	67.9			
192.168.1.90	192.168.1.100	6,728	30 M	4,317	29 M	2,411	647 k	0.282509	1399.			
10.0.0.201	23.43.62.169	8,014	8,161 k	2,620	143 k	5,394	8,017 k	93.661570	918.			
10.0.0.201	64.187.66.143	9,376	6,986 k	4,296	278 k	5,080	6,708 k	32.021926	981.			
166.62.111.64	172.16.4.205	15,728	16 M	11,354	15 M	4,374	321 k	163.231603	1001.			
172.16.4.205	185.243.115.84	35,680	32 M	18,744	14 M	16,936	17 M	308.224682	1095.			

ip.addr==172.16.4.205 && ip.addr==185.243.115.84					
Io.	Time	Source	Destination	Protocol	Length Info
308.	224682.	Rotterdam-PC.mind-hammer.net	b5689023.green.matt...	TCP	66 49249 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
308.	226772.	b5689023.green.mattingsolution...	Rotterdam-PC.mind-h...	TCP	66 80 → 49249 [SYN, ACK] Seq=0 Ack=1 Win=29200 Le
308.	227736.	Rotterdam-PC.mind-hammer.net	b5689023.green.matt...	TCP	60 49249 → 80 [ACK] Seq=1 Ack=1 Win=66304 Len=0
308.	236484.	Rotterdam-PC.mind-hammer.net	b5689023.green.matt...	TCP	546 49249 → 80 [PSH, ACK] Seq=1 Ack=1 Win=66304 Le
308.	238516.	Rotterdam-PC.mind-hammer.net	b5689023.green.matt...	HTTP	126 POST /empty.gif HTTP/1.1 (application/x-www-f
308.	242321.	b5689023.green.mattingsolution...	Rotterdam-PC.mind-h...	TCP	54 80 → 49249 [ACK] Seq=1 Ack=493 Win=30336 Len=0
308.	243187.	b5689023.green.mattingsolution...	Rotterdam-PC.mind-h...	TCP	54 80 → 49249 [ACK] Seq=1 Ack=565 Win=30336 Len=0
308.	265781.	b5689023.green.mattingsolution...	Rotterdam-PC.mind-h...	TCP	1411 80 → 49249 [ACK] Seq=1 Ack=565 Win=30336 Len=1
308.	288381.	b5689023.green.mattingsolution...	Rotterdam-PC.mind-h...	TCP	1411 80 → 49249 [ACK] Seq=1358 Ack=565 Win=30336 Le
308.	310959.	b5689023.green.mattingsolution...	Rotterdam-PC.mind-h...	TCP	1411 80 → 49249 [ACK] Seq=2715 Ack=565 Win=30336 Le
308.	313107.	b5689023.green.mattingsolution...	Rotterdam-PC.mind-h...	TCP	135 80 → 49249 [PSH, ACK] Seq=4072 Ack=565 Win=303
308.	335730.	b5689023.green.mattingsolution...	Rotterdam-PC.mind-h...	TCP	1411 80 → 49249 [ACK] Seq=4153 Ack=565 Win=30336 Le
308.	358290.	b5689023.green.mattingsolution...	Rotterdam-PC.mind-h...	TCP	1411 80 → 49249 [ACK] Seq=5510 Ack=565 Win=30336 Le
<ul style="list-style-type: none"> <li>Frame 28704: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0</li> <li>Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Cisco_e6:c4:77 (00:15:c6:e6:c4:77)</li> <li>Internet Protocol Version 4, Src: Rotterdam-PC.mind-hammer.net (172.16.4.205), Dst: b5689023.green.mattingsolutions.co (185.243.</li> <li>Transmission Control Protocol, Src Port: 49249, Dst Port: 80, Seq: 0, Len: 0</li> </ul>					

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 in your Network Report:

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.blanko**
- OS version: **BLANKO-DESKTOP**

Filter: ip.src == 10.0.0.201 and Kerberos.CNameString

The image shows a Wireshark packet capture window with a filter set to 'ip.src == 10.0.0.201 and kerberos.CNameString'. The packet list shows several AS-REQ (Authentication Service Request) messages from BLANCO-DESKTOP.dogoftheyear.net to DogOfTheYear-DC.dogoftheyear.net. The selected packet is a TCP segment (Frame 1156) with source port 49678 and destination port 88. The packet details pane shows the following information:

- Frame 1156: 301 bytes on wire (2408 bits), 301 bytes captured (2408 bits) on interface eth0, id 0
- Ethernet II, Src: Msi 18:66:c8 (00:16:17:18:66:c8), Dst: Dell f4:3b:96 (00:12:3f:f4:3b:96)
- Internet Protocol Version 4, Src: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201), Dst: DogOfTheYear-DC.dogoftheyear.net (10.0.0.2)
- 0100 .... = Version: 4
- .... 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 287
- Identification: 0x24c0 (9408)
- Flags: 0x4000, Don't fragment
- 0... .. = Reserved bit: Not set
- .1.. .. = Don't fragment: Set
- ..0. .... = More fragments: Not set
- ...0 0000 0000 0000 = Fragment offset: 0
- Time to live: 128
- Protocol: TCP (6)
- Header checksum: 0xc04e [validation disabled]
- [Header checksum status: Unverified]
- Source: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201)
- Destination: DogOfTheYear-DC.dogoftheyear.net (10.0.0.2)
- Transmission Control Protocol, Src Port: 49678, Dst Port: 88, Seq: 1, Ack: 1, Len: 247

Below the packet details, the frame structure is shown:

- Frame 1156: 301 bytes on wire (2408 bits), 301 bytes captured (2408 bits) on interface eth0, id 0
- Ethernet II, Src: Msi 18:66:c8 (00:16:17:18:66:c8), Dst: Dell f4:3b:96 (00:12:3f:f4:3b:96)

2. Which torrent file did the user download? The torrent file is **Betty\_Boop\_Rythm\_on\_the\_Reservation.avi.torrent**

2. Which torrent file did the user download? The torrent file is **Betty\_Boop\_Rythm\_on\_the\_Reservation.avi.torrent**

Filter: ip.addr == 10.0.0.201 and http.request.uri contains ".torrent"

The image shows a Wireshark packet capture window with a filter set to 'ip.addr == 10.0.0.201 and http.request.uri contains ".torrent"'. The packet list shows a single HTTP GET request from BLANCO-DESKTOP.dogoftheyear.net to files.publicdomaintorrents.com. The selected packet is an HTTP GET request (Frame 5711) with source port 589 and destination port 80. The packet details pane shows the following information:

- HTTP payload (589 bytes)
- 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
- Host: www.publicdomaintorrents.com\r\n
- Connection: Keep-Alive\r\n
- \r\n
- [Full request URI: http://www.publicdomaintorrents.com/bt/btdownload.php?type=torrent&file=Betty\_Boop\_Rhythm\_on\_the\_Reservation.avi.torrent]
- [HTTP request 1/1]
- [Response in frame: 5711]

The packet list shows the following information:

- o. Time Source Destination Protocol Length Info
- 30.7287566... BLANCO-DESKTOP.dogoftheyear.net files.publicdomaint... HTTP 589 GET /bt/btdownload.php?type=torrent&file=Betty\_Boop\_Rhythm\_on\_the\_Reservation.avi.torrent