

# Network Forensic Analysis Report

Prepared By:Ketan V. Patel

## Overview

You are working as a Security Engineer for X-CORP, supporting the SOC infrastructure. The SOC analysts have noticed some discrepancies with alerting in the Kibana system and the manager has asked the Security Engineering team to investigate.

Yesterday, your team confirmed that newly created alerts are working. Today, you will monitor live traffic on the wire to detect any abnormalities that aren't reflected in the alerting system.

You are to report back all your findings to both the SOC manager and the Engineering Manager with appropriate analysis.

The Security team requested this analysis because they have evidence that people are misusing the network. Specifically, they've received tips about:

- "Time thieves" spotted watching YouTube during work hours.
- At least one Windows host infected with a virus.
- Illegal downloads.

A number of machines from foreign subnets are sending traffic to this network. Your task is to collect evidence confirming the Security team's intelligence.

# Time Thieves

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

1. What is the domain name of the users' custom site?
2. What is the IP address of the Domain Controller (DC) of the AD network?
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.
4. Upload the file to [VirusTotal.com](https://www.virustotal.com).
5. What kind of malware is this classified as?

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?

- Domain Name: **Frank-n-Ted-DC. frank-n-ted.com**
- Wireshark Filter: **ip.src==10.6.12.0/24**

The image shows a Wireshark packet capture with the filter `ip.addr == 10.6.12.0/24`. The packet list shows a DNS query (Standard query) from 10.6.12.203 to 10.6.12.12. The packet details pane shows the following information:

- Frame 67741: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface eth0, id 0
- Ethernet II, Src: IntelCor-bd:fc:e2 (84:3a:4b:6d:fc:e2), Dst: Dell17:f7:e5 (98:49:bb:2a:f7:e5)
- Internet Protocol Version 4, Src: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203), Dst: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12)
- 9100 ... = Version: 4
- ... 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 94
- Identification: 0xa299 (41625)
- Flags: 0x0000
- ... 0 0000 0000 0000 = Fragment offset: 0
- Time to live: 128
- Protocol: UDP (17)
- Header checksum: 0x6b13 [validation disabled]
- [Header checksum status: Unverified]
- Source: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203)
- Destination: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12)
- User Datagram Protocol, Src Port: 63077 (63077), Dst Port: domain (53)
- Domain Name System (query)

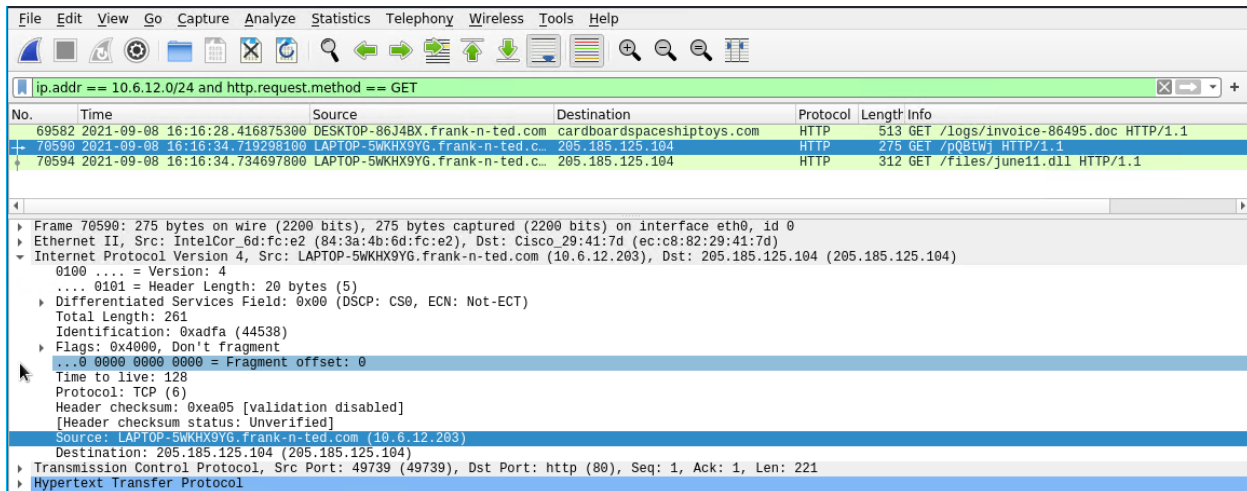
## 2. What is the IP address of the Domain Controller (DC) of the AD network?

- 10.6.12.12 (Frank-n-Ted-DC.frank-n-ted.com)
- Wireshark Filter: ip.src==10.6.12.0/24

```
▶ Frame 67747: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface eth0, id 0
▶ Ethernet II, Src: Intel 68:42:d3 (00:11:75:68:42:d3), Dst: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5)
▼ Internet Protocol Version 4, Src: DESKTOP-86J4BX.frank-n-ted.com (10.6.12.157), Dst: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12)
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 66
    Identification: 0x1912 (6418)
  ▶ Flags: 0x0000
    ... 0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0xf4e4 [validation disabled]
    [Header checksum status: Unverified]
    Source: DESKTOP-86J4BX.frank-n-ted.com (10.6.12.157)
    Destination: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12)
  ▶ User Datagram Protocol, Src Port: 56636 (56636), Dst Port: domain (53)
  ▶ Domain Name System (query)
```

## 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.

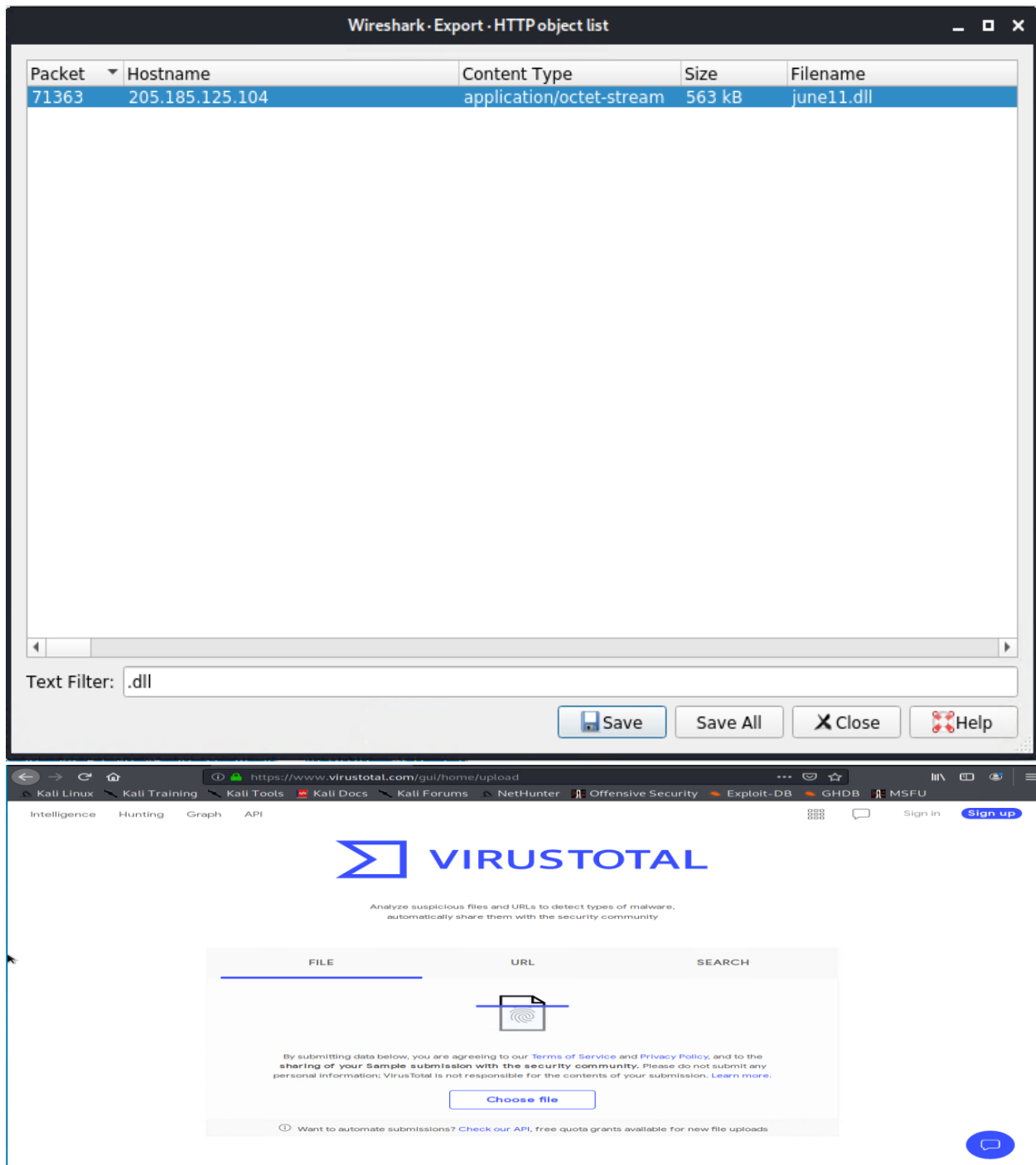
- Malware file name: **june11.dll**
- Wireshark Filter: **ip.addr == 10.6.12.0/24 and http.request.method == GET**



```
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.6.12.0/24 and http.request.method == GET
No. Time Source Destination Protocol Length Info
69582 2021-09-08 16:16:28.416875300 DESKTOP-86J4BX.frank-n-ted.com cardboardspaceshiptoy.com HTTP 513 GET /logs/invoice-86495.doc HTTP/1.1
70590 2021-09-08 16:16:34.749208100 LAPTOP-5WKHX9YG.frank-n-ted.c... 205.185.125.104 HTTP 275 GET /pQ8tWj HTTP/1.1
70594 2021-09-08 16:16:34.734697800 LAPTOP-5WKHX9YG.frank-n-ted.c... 205.185.125.104 HTTP 312 GET /files/june11.dll HTTP/1.1
Frame 70590: 275 bytes on wire (2200 bits), 275 bytes captured (2200 bits) on interface eth0, id 0
▶ Ethernet II, Src: IntelCor 6d:fc:e2 (84:3a:4b:6d:fc:e2), Dst: Cisco 29:41:7d (ec:c8:82:29:41:7d)
▼ Internet Protocol Version 4, Src: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203), Dst: 205.185.125.104 (205.185.125.104)
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 261
    Identification: 0xadfa (44538)
  ▶ Flags: 0x4000, Don't fragment
  ... 0 0000 0000 0000 = Fragment offset: 0
  Time to live: 128
  Protocol: TCP (6)
  Header checksum: 0xea05 [validation disabled]
  [Header checksum status: Unverified]
  Source: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203)
  Destination: 205.185.125.104 (205.185.125.104)
  ▶ Transmission Control Protocol, Src Port: 49739 (49739), Dst Port: http (80), Seq: 1, Ack: 1, Len: 221
  ▶ Hypertext Transfer Protocol
```

#### 4. Upload the file to [VirusTotal.com](https://www.virustotal.com).

- Exporting file to Kali:
  - Open File Tab
  - Export Objects
  - Select HTTP
  - Filter "\*.dll"
  - Save **june.dll**
  - Upload to VirusTotal.com



## 5. What kind of malware is this classified as?

- This is a Trojan named: Trojan.Mint.Zamg.O

49 / 67

49 security vendors flagged this file as malicious

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

549.84 KB  
Size

2021-08-28 17:19:13 UTC  
11 days ago

GoogleIupdate.exe

invalid-signature overlay pedl signed

Community Score

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	ALYac	① Trojan.Mint.Zamg.O	
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.34110.lu9@aui7OQgi	CrowdStrike Falcon	① Win/malicious_confidence_100% (W)	
Cylance	① Unsafe	Cynet	① Malicious (score: 100)	
Cyren	① W32/Trojan.SIAQ-3008	DrWeb	① Trojan.Inject3.53106	

## Vulnerable Windows Machine

1. Find the following information about the infected Windows machine:
  - Host name
  - IP address
  - MAC address
2. What is the username of the Windows user whose computer is infected?
3. What are the IP addresses used in the actual infection traffic?
4. As a bonus, retrieve the desktop background of the Windows host.

---

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
- Wireshark Filter: ip.addr == 172.16.4.0/24

The image displays two screenshots of the Wireshark network protocol analyzer. The top screenshot shows a packet list with a filter 'ip.addr == 172.16.4.0/24'. Packet 42137 is selected, showing an HTTP POST request from Rotterdam-PC.mind-hammer.net (172.16.4.205) to 31.7.62.214. The bottom screenshot shows the packet details pane for the selected packet, revealing the full HTTP request structure, including the POST method, URI, headers (User-Agent, Content-Type, Content-Length), and the body content.

**Packet List (Top Screenshot):**

No.	Time	Source	Destination	Protocol	Length	Info
42134	2021-09-08 16:13:19.930694500	Rotterdam-PC.mind-hammer.net	Rotterdam-PC.mind-hammer.net	TCP	54	https(443) → 49255 [ACK] Seq=520 Ack=2
42135	2021-09-08 16:13:19.935201700	Rotterdam-PC.mind-hammer.net	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HT
42136	2021-09-08 16:13:19.936062100	Rotterdam-PC.mind-hammer.net	31.7.62.214	TCP	54	https(443) → 49255 [ACK] Seq=520 Ack=2
42137	2021-09-08 16:13:19.940592700	Rotterdam-PC.mind-hammer.net	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HT
42138	2021-09-08 16:13:19.941446800	Rotterdam-PC.mind-hammer.net	31.7.62.214	TCP	54	https(443) → 49255 [ACK] Seq=520 Ack=2

**Packet Details (Bottom Screenshot):**

Header checksum: 0x9b06 [validation disabled]  
[Header checksum status: Unverified]  
Source: Rotterdam-PC.mind-hammer.net (172.16.4.205)  
Destination: 31.7.62.214 (31.7.62.214)  
Transmission Control Protocol, Src Port: 49255 (49255), Dst Port: https (443), Seq: 25824, Ack: 520, Len: 228

Hypertext Transfer Protocol

[Expert Info (Warning/Security): Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous misconfiguration.]

POST http://31.7.62.214/fakeurl.htm HTTP/1.1

[Expert Info (Chat/Sequence): POST http://31.7.62.214/fakeurl.htm HTTP/1.1]

Request Method: POST  
Request URI: http://31.7.62.214/fakeurl.htm  
Request Version: HTTP/1.1  
User-Agent: NetSupport Manager/1.3  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 36  
[Content length: 36]

Host: 31.7.62.214  
Connection: Keep-Alive  
[Full request URI: http://31.7.62.214/fakeurl.htm]  
[HTTP request 113/114]



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

- Username: matthijs.devries
- Wireshark Filter: ip.src==172.16.4.205 && kerberos.CNameString

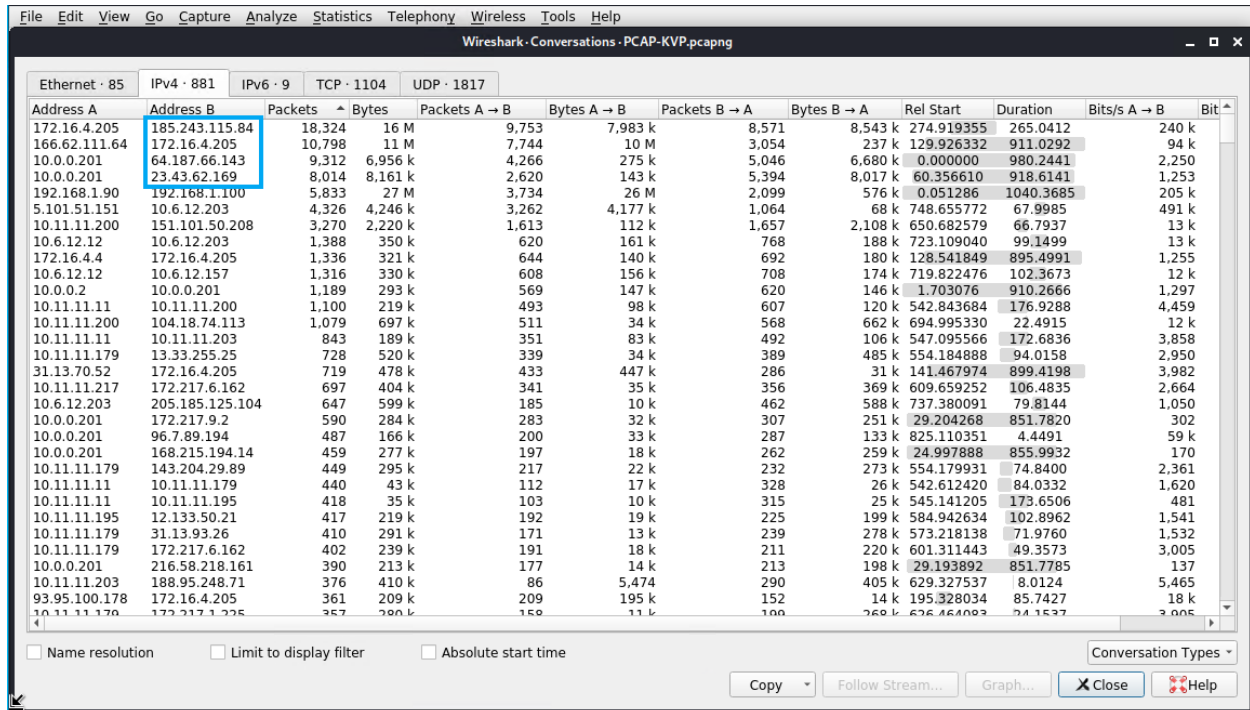
The image shows a Wireshark network traffic capture. The filter bar at the top is set to `ip.addr == 172.16.4.205 && kerberos.CNameString`. The packet list shows a series of Kerberos messages between `Rotterdam-PC.mind-hammer.net` and `mind-hammer-dc.mind-hammer.net`. The selected packet (No. 12281) is a Kerberos AS-REQ. The packet details pane shows the following structure:

```
Transmission Control Protocol, Src Port: 49178 (49178), Dst Port: kerberos (88), Seq: 1, Ack: 1, Len: 238
Kerberos
  Record Mark: 234 bytes
    0... = Reserved: Not set
    .000 0000 0000 0000 0000 1110 1010 = Record Length: 234
  as-req
    pvno: 5
    msg-type: krb-as-req (10)
    padata: 1 item
      PA-DATA PA-PAC-REQUEST
    req-body
      Padding: 0
      kdc-options: 40810010
      cname
        name-type: kRB5-NT-PRINCIPAL (1)
        cname-string: 1 item
          CNameString: matthijs.devries
      realm: MIND-HAMMER
      sname
        till: 2037-09-13 02:48:05 (UTC)
        rtime: 2037-09-13 02:48:05 (UTC)
```



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

- Filter: `ip.src==172.16.4.203` and `kerberos.CNameString`
- I found 4 IP addresses: 172.16.4.205, 185.243.115.84, 166.62.11.64 and 23.43.62.169
- Finding the IP addresses:
  - Click on the Statistics Tab
  - Select the Conversation
  - Select the IPv4
  - Sort Packets high to low



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/s B → A
172.16.4.205	185.243.115.84	18,324	16 M	9,753	7,983 k	8,571	8,543 k	274.919355	265.0412	240 k	240 k
166.62.11.64	172.16.4.205	10,798	11 M	7,744	10 M	3,054	237 k	129.926332	911.0292	94 k	94 k
10.0.0.201	64.187.66.143	9,312	6,956 k	4,266	275 k	5,046	6,680 k	0.000000	980.2441	2,250	2,250
10.0.0.201	23.43.62.169	8,014	8,161 k	2,620	143 k	5,394	8,017 k	60.356610	918.6141	1,253	1,253
192.168.1.90	192.168.1.100	5,833	27 M	3,734	26 M	2,099	576 k	0.051286	1040.3685	205 k	205 k
5.101.51.151	10.6.12.203	4,326	4,246 k	3,262	4,177 k	1,064	68 k	748.655772	67.9985	491 k	491 k
10.11.11.200	151.101.50.208	3,270	2,220 k	1,613	112 k	1,657	2,108 k	650.682579	66.7937	13 k	13 k
10.6.12.12	10.6.12.203	1,388	350 k	620	161 k	768	188 k	723.109040	99.1499	13 k	13 k
172.16.4.4	172.16.4.205	1,336	321 k	644	140 k	692	180 k	128.541849	895.4991	1,255	1,255
10.6.12.12	10.6.12.157	1,316	330 k	608	156 k	708	174 k	719.822476	102.3673	12 k	12 k
10.0.0.2	10.0.0.201	1,189	293 k	569	147 k	620	146 k	1.703076	910.2666	1,297	1,297
10.11.11.11	10.11.11.200	1,100	219 k	493	98 k	607	120 k	542.843684	176.9288	4,459	4,459
10.11.11.200	104.18.74.113	1,079	697 k	511	34 k	568	662 k	694.995330	22.4915	12 k	12 k
10.11.11.11	10.11.11.203	843	189 k	351	83 k	492	106 k	547.095566	172.6836	3,858	3,858
10.11.11.179	13.33.255.25	728	520 k	339	34 k	389	485 k	554.184888	94.0158	2,950	2,950
31.13.70.52	172.16.4.205	719	478 k	433	447 k	286	31 k	141.467974	899.4198	3,982	3,982
10.11.11.217	172.217.6.162	697	404 k	341	35 k	356	369 k	609.659252	106.4835	2,664	2,664
10.6.12.203	205.185.125.104	647	599 k	185	10 k	462	588 k	737.380091	79.8144	1,050	1,050
10.0.0.201	172.217.9.2	590	284 k	283	32 k	307	251 k	29.204268	851.7820	302	302
10.0.0.201	96.7.89.194	487	166 k	200	33 k	287	133 k	825.110351	4.4491	59 k	59 k
10.0.0.201	168.215.194.14	459	277 k	197	18 k	262	259 k	24.997888	855.9932	170	170
10.11.11.179	143.204.29.89	449	295 k	217	22 k	232	273 k	554.179931	74.8400	2,361	2,361
10.11.11.11	10.11.11.179	440	43 k	112	17 k	328	26 k	542.612420	84.0332	1,620	1,620
10.11.11.11	10.11.11.195	418	35 k	103	10 k	315	25 k	545.141205	173.6506	481	481
10.11.11.195	12.133.50.21	417	219 k	192	19 k	225	199 k	584.942634	102.8962	1,541	1,541
10.11.11.179	31.13.93.26	410	291 k	171	13 k	239	278 k	573.218138	71.9760	1,532	1,532
10.11.11.179	172.217.6.162	402	239 k	191	18 k	211	220 k	601.311443	49.3573	3,005	3,005
10.0.0.201	216.58.218.161	390	213 k	177	14 k	213	198 k	29.193892	851.7785	137	137
10.11.11.203	188.95.248.71	376	410 k	86	5,474	290	405 k	629.327537	8.0124	5,465	5,465
93.95.100.178	172.16.4.205	361	209 k	209	195 k	152	14 k	195.328034	85.7427	18 k	18 k
10.11.11.179	172.217.1.225	357	280 k	158	11 k	199	269 k	626.464093	74.1537	3,005	3,005

- Additional Traffic from 185.243.115.84 to infected host 172.16.4.205

No.	Time	Source	Destination	Protocol	Length	Info
22342	2021-09-08 16:08:52.252367900	Rotterdam-PC.mind-hammer.net	b5689023.green.mattingsolutio...	TCP	66	49249 → http(80) [SYN, ACK] Seq=0 Win=8192
22344	2021-09-08 16:08:52.254487800	b5689023.green.mattingsolutio...	Rotterdam-PC.mind-hammer.net	TCP	66	http(80) → 49249 [SYN, ACK] Seq=0 Ack=
22345	2021-09-08 16:08:52.255446800	Rotterdam-PC.mind-hammer.net	b5689023.green.mattingsolutio...	TCP	60	49249 → http(80) [ACK] Seq=1 Ack=1 Win=
22346	2021-09-08 16:08:52.264199400	Rotterdam-PC.mind-hammer.net	b5689023.green.mattingsolutio...	TCP	546	49249 → http(80) [PSH, ACK] Seq=1 Ack=
22347	2021-09-08 16:08:52.266212300	Rotterdam-PC.mind-hammer.net	b5689023.green.mattingsolutio...	HTTP	126	POST /empty.gif HTTP/1.1 (applicatio
22351	2021-09-08 16:08:52.270040000	b5689023.green.mattingsolutio...	Rotterdam-PC.mind-hammer.net	TCP	54	http(80) → 49249 [ACK] Seq=1 Ack=493 W
22352	2021-09-08 16:08:52.270903300	b5689023.green.mattingsolutio...	Rotterdam-PC.mind-hammer.net	TCP	54	http(80) → 49249 [ACK] Seq=1 Ack=565 W
22353	2021-09-08 16:08:52.293494000	b5689023.green.mattingsolutio...	Rotterdam-PC.mind-hammer.net	TCP	1411	http(80) → 49249 [ACK] Seq=1 Ack=565 W
22354	2021-09-08 16:08:52.316091900	b5689023.green.mattingsolutio...	Rotterdam-PC.mind-hammer.net	TCP	1411	http(80) → 49249 [ACK] Seq=1358 Ack=56
22355	2021-09-08 16:08:52.338697400	b5689023.green.mattingsolutio...	Rotterdam-PC.mind-hammer.net	TCP	1411	http(80) → 49249 [ACK] Seq=2715 Ack=56
22356	2021-09-08 16:08:52.340869100	b5689023.green.mattingsolutio...	Rotterdam-PC.mind-hammer.net	TCP	135	http(80) → 49249 [PSH, ACK] Seq=4072 A
22357	2021-09-08 16:08:52.363639200	b5689023.green.mattingsolutio...	Rotterdam-PC.mind-hammer.net	TCP	1411	http(80) → 49249 [ACK] Seq=4153 Ack=56
22358	2021-09-08 16:08:52.385976100	b5689023.green.mattingsolutio...	Rotterdam-PC.mind-hammer.net	TCP	1411	http(80) → 49249 [ACK] Seq=5510 Ack=56

Frame 22342: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
Ethernet II, Src: LenovoEM b0:63:a4 (08:59:97:b0:63:a4), Dst: Cisco e6:c4:77 (08:15:c6:e6:c4:77)
Internet Protocol Version 4, Src: Rotterdam-PC.mind-hammer.net (172.16.4.205), Dst: b5689023.green.mattingsolutions.co (185.243.115.84)
Transmission Control Protocol, Src Port: 49249 (49249), Dst Port: http (80), Seq: 0, Len: 0
Source Port: 49249 (49249)
Destination Port: http (80)
[Stream index: 232]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Sequence number (raw): 2570699659
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 0
Acknowledgment number (raw): 0
1000 .... = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
Window size value: 8192
[Calculated window size: 8192]
Checksum: 0x5374 [unverified]
[Checksum Status: Unverified]
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
[Timestamps]

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.

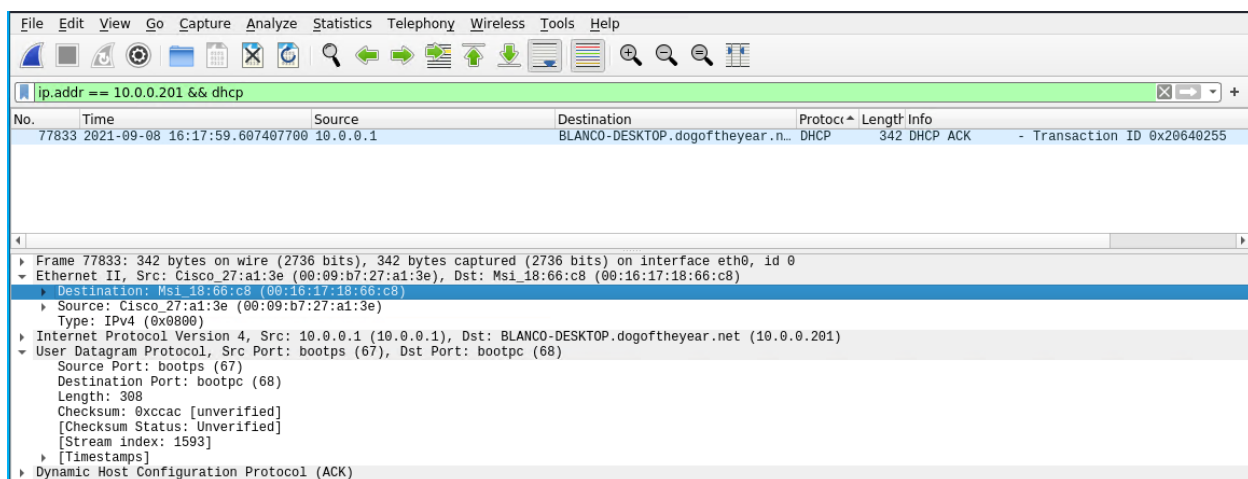
Wireshark Filters Used:

- MAC Address: ip.addr == 10.0.0.201 && dhcp
- Username: ip.src == 10.0.0.201 && kerberos.CNameString
- Operating System: ip.addr == 10.0.0.201 && http.request
- Torrent Download: ip.addr == 10.0.0.201 && http.request.method == "GET"

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**:
  - a. MAC address: **00:16:17:18:66:c8**
  - b. Windows username: **elmer.blanco**
  - c. OS version: **BLANCO-DESKTOP Windows NT 10.0**

- Wireshark Filter for MAC Address: **ip.addr == 10.0.0.201 && dhcp**



- Wireshark Filter for Username: **ip.addr == 10.0.0.201 && kerberos.CNameString**

Wireshark Filter: **ip.addr == 10.0.0.201 && kerberos.CNameString**

No.	Time	Source	Destination	Protocol	Length	Info
79537	2021-09-08 16:18:07.303899600	BLANCO-DESKTOP.dogoftheyear.n...	DogOfTheYear-DC.dogoftheyear....	KRB5	370	AS-REQ
79527	2021-09-08 16:18:07.288344600	BLANCO-DESKTOP.dogoftheyear.n...	DogOfTheYear-DC.dogoftheyear....	KRB5	290	AS-REQ
79459	2021-09-08 16:18:07.122233100	BLANCO-DESKTOP.dogoftheyear.n...	DogOfTheYear-DC.dogoftheyear....	KRB5	382	AS-REQ
79451	2021-09-08 16:18:07.105745300	BLANCO-DESKTOP.dogoftheyear.n...	DogOfTheYear-DC.dogoftheyear....	KRB5	302	AS-REQ
78159	2021-09-08 16:18:00.699547600	BLANCO-DESKTOP.dogoftheyear.n...	DogOfTheYear-DC.dogoftheyear....	KRB5	382	AS-REQ
78146	2021-09-08 16:18:00.670867400	BLANCO-DESKTOP.dogoftheyear.n...	DogOfTheYear-DC.dogoftheyear....	KRB5	301	AS-REQ
78063	2021-09-08 16:18:00.353743100	BLANCO-DESKTOP.dogoftheyear.n...	DogOfTheYear-DC.dogoftheyear....	KRB5	381	AS-REQ
78055	2021-09-08 16:18:00.337514700	BLANCO-DESKTOP.dogoftheyear.n...	DogOfTheYear-DC.dogoftheyear....	KRB5	301	AS-REQ
77943	2021-09-08 16:17:59.982150200	BLANCO-DESKTOP.dogoftheyear.n...	DogOfTheYear-DC.dogoftheyear....	KRB5	382	AS-REQ
77929	2021-09-08 16:17:59.934232200	BLANCO-DESKTOP.dogoftheyear.n...	DogOfTheYear-DC.dogoftheyear....	KRB5	301	AS-REQ
77925	2021-09-08 16:17:59.926447900	BLANCO-DESKTOP.dogoftheyear.n...	DogOfTheYear-DC.dogoftheyear....	KRB5	381	AS-REQ
77904	2021-09-08 16:17:59.806557700	BLANCO-DESKTOP.dogoftheyear.n...	DogOfTheYear-DC.dogoftheyear....	KRB5	301	AS-REQ

**Kerberos**

- Record Mark: 232 bytes
- 0 ..... = Reserved: Not set
- 0000 0000 0000 0000 0000 1110 1000 = Record Length: 232
- as-req
  - pvno: 5
  - msg-type: krb-as-req (10)
  - padata: 1 item
    - PA-DATA PA-PAC-REQUEST
  - req-body
    - padding: 0
    - kdc-options: 40810010
    - cname
      - name-type: KRB5-NT-PRINCIPAL (1)
      - cname-string: 1 item
        - CNameString: elmer.blanco
    - realm: DOGOFTHEYEAR
    - sname
    - till: 2037-09-13 02:48:05 (UTC)
    - rtime: 2037-09-13 02:48:05 (UTC)
    - nonce: 634194387
    - etype: 6 items
    - addresses: 1 item BLANCO-DESKTOP<20>

- Wireshark Filter for Username: **ip.addr == 10.0.0.201 && http.request**

Wireshark Filter: **ip.addr == 10.0.0.201 && http.request.method**

No.	Time	Source	Destination	Protocol	Length	Info
81810	2021-09-08 16:18:21.233626900	BLANCO-DESKTOP.dogoftheyear.n...	files.publicdomaintorrents.com	HTTP	534	GET /nshowmovie.html?movieid=513 HTTP/1.1
81648	2021-09-08 16:18:20.776461400	BLANCO-DESKTOP.dogoftheyear.n...	ocsp.godaddy.com.akadns.net	HTTP	276	GET //MEKwRzBFMEwQTAJBgUrdgMCgGUABBS2
81549	2021-09-08 16:18:20.485129900	BLANCO-DESKTOP.dogoftheyear.n...	ocsp.godaddy.com.akadns.net	HTTP	270	GET //MEIwQDAK2BMDww0JAJBgUrdgMCgGUABE
81404	2021-09-08 16:18:20.183487400	BLANCO-DESKTOP.dogoftheyear.n...	cs9.wac.phicdn.net	HTTP	292	GET //MFEwTzBNMEswSTAJBgUrdgMCgGUABBRh
81384	2021-09-08 16:18:20.135474400	BLANCO-DESKTOP.dogoftheyear.n...	cdn.globalsigncdn.com.cdn.clo...	HTTP	313	GET //gsorganizationvalsha2g2/ME0wSzBJM
81378	2021-09-08 16:18:20.100924200	BLANCO-DESKTOP.dogoftheyear.n...	ocsp.godaddy.com.akadns.net	HTTP	274	GET //MEQwQjBAMD4wPDAJBgUrdgMCgGUABBTk
81373	2021-09-08 16:18:20.092968100	BLANCO-DESKTOP.dogoftheyear.n...	cs9.wac.phicdn.net	HTTP	286	GET //MFEwTzBNMEswSTAJBgUrdgMCgGUABBOQX
81370	2021-09-08 16:18:20.086471900	BLANCO-DESKTOP.dogoftheyear.n...	cs9.wac.phicdn.net	HTTP	286	GET //MFEwTzBNMEswSTAJBgUrdgMCgGUABBOQX
81344	2021-09-08 16:18:19.950838200	BLANCO-DESKTOP.dogoftheyear.n...	cdn.globalsigncdn.com.cdn.clo...	HTTP	291	GET //rootr1/MEwWSJBIMEYwRDAJBgUrdgMCgG
81339	2021-09-08 16:18:19.941345500	BLANCO-DESKTOP.dogoftheyear.n...	cs9.wac.phicdn.net	HTTP	286	GET //MFEwTzBNMEswSTAJBgUrdgMCgGUABBOQX
81337	2021-09-08 16:18:19.935895000	BLANCO-DESKTOP.dogoftheyear.n...	cs9.wac.phicdn.net	HTTP	286	GET //MFEwTzBNMEswSTAJBgUrdgMCgGUABBOQX
81331	2021-09-08 16:18:19.926878900	BLANCO-DESKTOP.dogoftheyear.n...	cs9.wac.phicdn.net	HTTP	288	GET //MFEwTzBNMEswSTAJBgUrdgMCgGUABBSAU
80984	2021-09-08 16:18:12.952538300	BLANCO-DESKTOP.dogoftheyear.n...	files.publicdomaintorrents.com	HTTP	336	GET /favicon.ico HTTP/1.1
80056	2021-09-08 16:18:10.487453800	BLANCO-DESKTOP.dogoftheyear.n...	pagead46.l.doubleclick.net	HTTP	467	GET /pagead/js/r/20180709/r/20180604/shc
80019	2021-09-08 16:18:10.394487300	BLANCO-DESKTOP.dogoftheyear.n...	scripts-tfnfdwtqiaq1wsartb.st...	HTTP	427	GET /eminimalis/mm.js HTTP/1.1

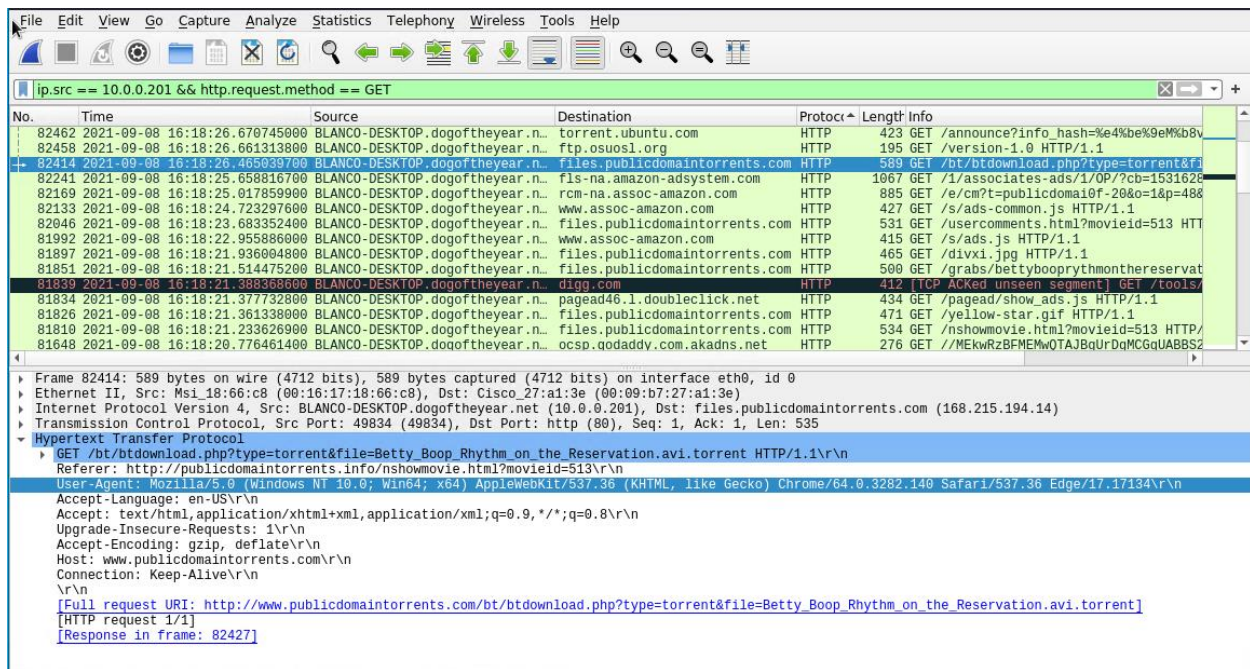
**Frame 81810: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface eth0, id 0**

- 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: files.publicdomaintorrents.com (168.215.194.14)
- Transmission Control Protocol, Src Port: 49817 (49817), Dst Port: http (80), Seq: 1, Ack: 1, Len: 480
- Hypertext Transfer Protocol
  - GET /nshowmovie.html?movieid=513 HTTP/1.1\r\n
  - Referer: http://publicdomaintorrents.info/nshowcat.html?category=animation\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
  - 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
  - Connection: Keep-Alive\r\n
  - \r\n
  - [Full request URI: http://publicdomaintorrents.info/nshowmovie.html?movieid=513]
  - [HTTP request 1/2]
  - [Response in frame: 81849]
  - [Next request in frame: 81851]



## 2. Which torrent file did the user download?

- There were few that were downloaded, but below clip was show with the name:
- **Betty\_Boop\_Rhythm\_on\_the\_Reservation.avi.torrent**
  - Wireshark Filter: ip.addr == 10.0.0.201 && http.request.method == "GET"
  - Finding the torrent:
  - Apply the Wireshark Filter above.
  - Sort the packets by the Destination files.publicdomaintorrents.com (168.215.194.14).
  - Look for Download requests.



On the next page is the movie clip snapshot.

This movie clip snapshot was downloaded from the following website.

<http://www.publicdomaintorrents.info/grabs/bettybooprythmonthereservationgrab.jpg>

File Name: Betty\_Boop\_Rhythm\_on\_the\_Reservation.avi  
File Size: 100.50 MB  
Resolution: 720x480  
Duration: 00:06:02

