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

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:

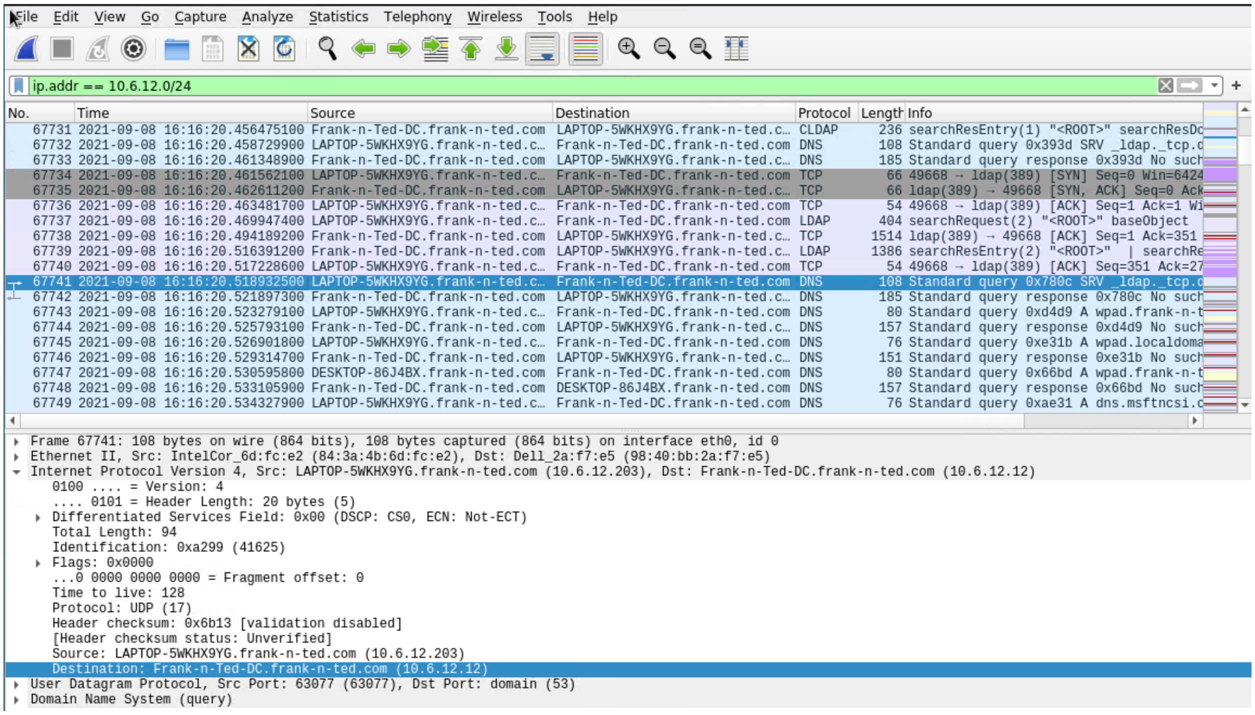
- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.
- Their IP addresses are somewhere in the range 10.6.12.0/24.

Following Wireshark Filters were Used:

- Domain of the custom site: **ip.addr == 10.6.12.0/24**
- Traffic Inspection: **ip.addr == 10.6.12.12**
- Other Traffic Inspection: **ip.addr == 10.6.12.203**
- Malware Name: **ip.addr == 10.6.12.203 and http.request.method == GET**

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**



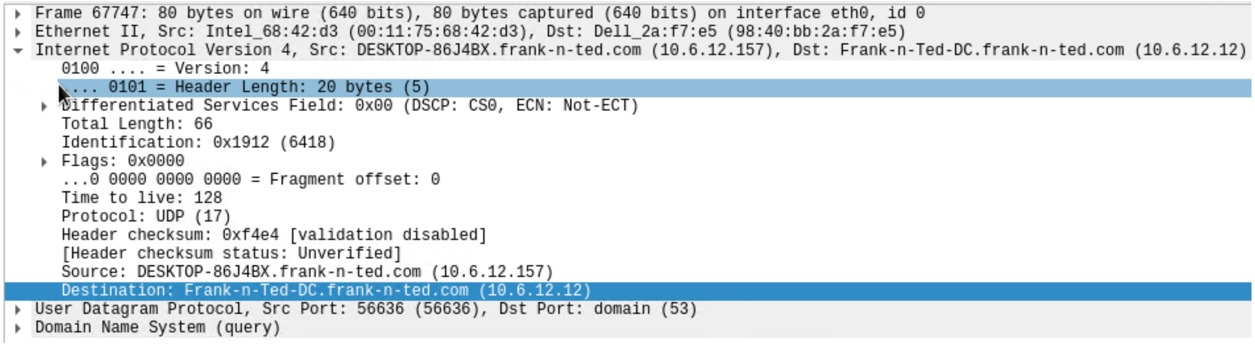
ip.addr == 10.6.12.0/24

```
No.   Time                          Source                          Destination                     Protocol Length Info
67731 2021-09-08 16:16:20.456475100 Frank-n-Ted-DC.frank-n-ted.com LAPTOP-5WKHX9YG.frank-n-ted.c… CLDAP     236 searchResEntry(1) "<ROOT>" searchResDc
67732 2021-09-08 16:16:20.458729900 LAPTOP-5WKHX9YG.frank-n-ted.c… Frank-n-Ted-DC.frank-n-ted.com DNS       108 Standard query 0x393d SRV _ldap._tcp.d
67733 2021-09-08 16:16:20.461348900 Frank-n-Ted-DC.frank-n-ted.com LAPTOP-5WKHX9YG.frank-n-ted.c… DNS       185 Standard query response 0x393d No such
67734 2021-09-08 16:16:20.461562100 LAPTOP-5WKHX9YG.frank-n-ted.c… Frank-n-Ted-DC.frank-n-ted.com TCP        66 49668 → ldap(389) [SYN] Seq=0 Win=6424
67735 2021-09-08 16:16:20.462611200 Frank-n-Ted-DC.frank-n-ted.com LAPTOP-5WKHX9YG.frank-n-ted.c… TCP        66 ldap(389) → 49668 [SYN, ACK] Seq=0 Ack
67736 2021-09-08 16:16:20.463481700 LAPTOP-5WKHX9YG.frank-n-ted.c… Frank-n-Ted-DC.frank-n-ted.com TCP        54 49668 → ldap(389) [ACK] Seq=1 Ack=1 Wi
67737 2021-09-08 16:16:20.469947400 LAPTOP-5WKHX9YG.frank-n-ted.c… Frank-n-Ted-DC.frank-n-ted.com LDAP      404 searchRequest(2) "<ROOT>" baseObject
67738 2021-09-08 16:16:20.494189200 Frank-n-Ted-DC.frank-n-ted.com LAPTOP-5WKHX9YG.frank-n-ted.c… TCP      1514 ldap(389) → 49668 [ACK] Seq=1 Ack=351
67739 2021-09-08 16:16:20.516391200 Frank-n-Ted-DC.frank-n-ted.com LAPTOP-5WKHX9YG.frank-n-ted.c… LDAP     1386 searchResEntry(2) "<ROOT>"  | searchRe
67740 2021-09-08 16:16:20.517228600 LAPTOP-5WKHX9YG.frank-n-ted.c… Frank-n-Ted-DC.frank-n-ted.com TCP        54 49668 → ldap(389) [ACK] Seq=351 Ack=27
67741 2021-09-08 16:16:20.518932500 LAPTOP-5WKHX9YG.frank-n-ted.c… Frank-n-Ted-DC.frank-n-ted.com DNS       108 Standard query 0x780c SRV _ldap._tcp.d
67742 2021-09-08 16:16:20.521897300 Frank-n-Ted-DC.frank-n-ted.com LAPTOP-5WKHX9YG.frank-n-ted.c… DNS       185 Standard query response 0x780c No such
67743 2021-09-08 16:16:20.523279100 LAPTOP-5WKHX9YG.frank-n-ted.c… Frank-n-Ted-DC.frank-n-ted.com DNS        80 Standard query 0xd4d9 A wpad.frank-n-t
67744 2021-09-08 16:16:20.525793100 Frank-n-Ted-DC.frank-n-ted.com LAPTOP-5WKHX9YG.frank-n-ted.c… DNS       157 Standard query response 0xd4d9 No such
67745 2021-09-08 16:16:20.526901800 LAPTOP-5WKHX9YG.frank-n-ted.c… Frank-n-Ted-DC.frank-n-ted.com DNS        76 Standard query 0xe31b A wpad.localdoma
67746 2021-09-08 16:16:20.529314700 Frank-n-Ted-DC.frank-n-ted.com LAPTOP-5WKHX9YG.frank-n-ted.c… DNS       151 Standard query response 0xe31b No such
67747 2021-09-08 16:16:20.530595800 DESKTOP-86J4BX.frank-n-ted.com Frank-n-Ted-DC.frank-n-ted.com DNS        80 Standard query 0x66bd A wpad.frank-n-t
67748 2021-09-08 16:16:20.533105900 Frank-n-Ted-DC.frank-n-ted.com DESKTOP-86J4BX.frank-n-ted.com DNS       157 Standard query response 0x66bd No such
67749 2021-09-08 16:16:20.534327900 LAPTOP-5WKHX9YG.frank-n-ted.c… Frank-n-Ted-DC.frank-n-ted.com DNS        76 Standard query 0xae31 A dns.msftncsi.c
```

```
Frame 67741: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface eth0, id 0
Ethernet II, Src: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2), Dst: Dell_2a:f7:e5 (98:40: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)
    0100 .... = 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?

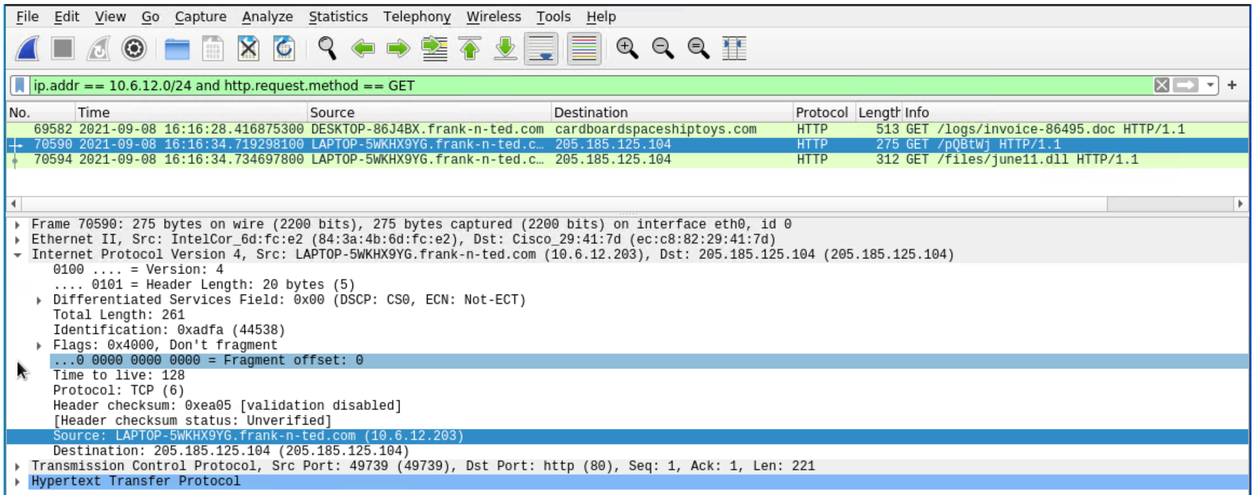
- IP Address: 10.6.12.12 (Frank-n-Ted-DC.frank-n-ted.com)
- Wireshark Filter: ip.src==10.6.12.0/24



```
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**



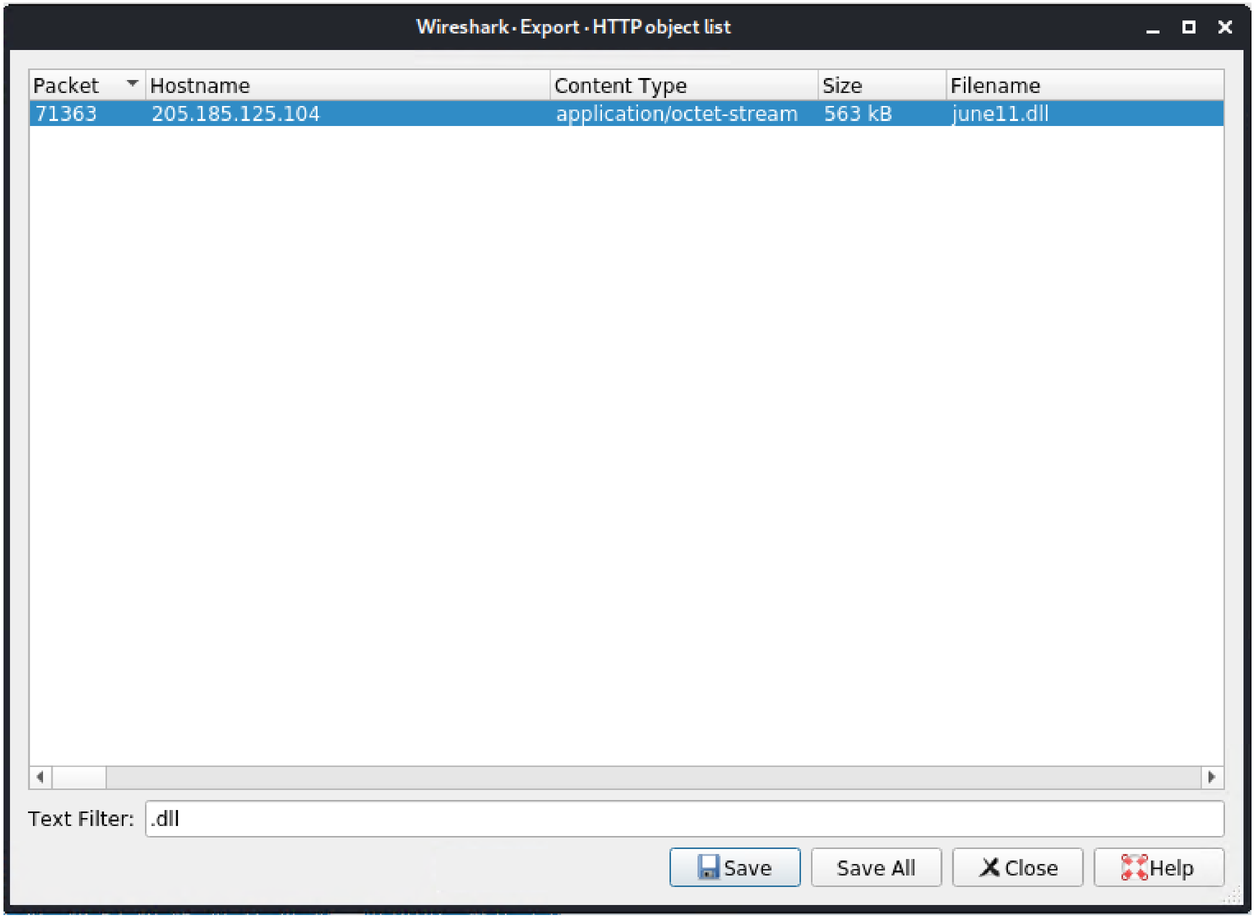
```
ip.addr == 10.6.12.0/24 and http.request.method == GET
```

```
No.    Time                          Source                           Destination                 Protocol  Length Info
 69582 2021-09-08 16:16:28.416875300 DESKTOP-86J4BX.frank-n-ted.com   cardboardspaceshiptoys.com  HTTP      513 GET /logs/invoice-86495.doc HTTP/1.1
 70590 2021-09-08 16:16:34.719298100 LAPTOP-5WKHX9YG.frank-n-ted.c…   205.185.125.104             HTTP      275 GET /pQBtWj 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.

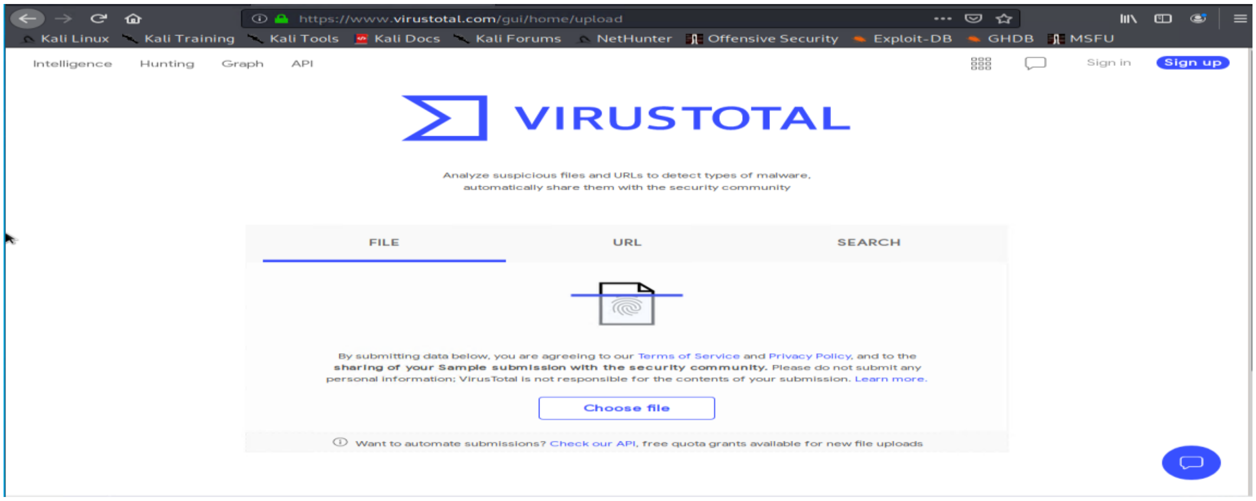
- Exporting file to Kali:
    - Open File Tab
    - Export Objects
    - Select HTTP
    - Filter “*.dll”
    - Save **june.dll**
    - Upload to VirusTotal.com



Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
71363	205.185.125.104	application/octet-stream	563 kB	june11.dll

Text Filter: .dll



https://www.virustotal.com/gui/home/upload

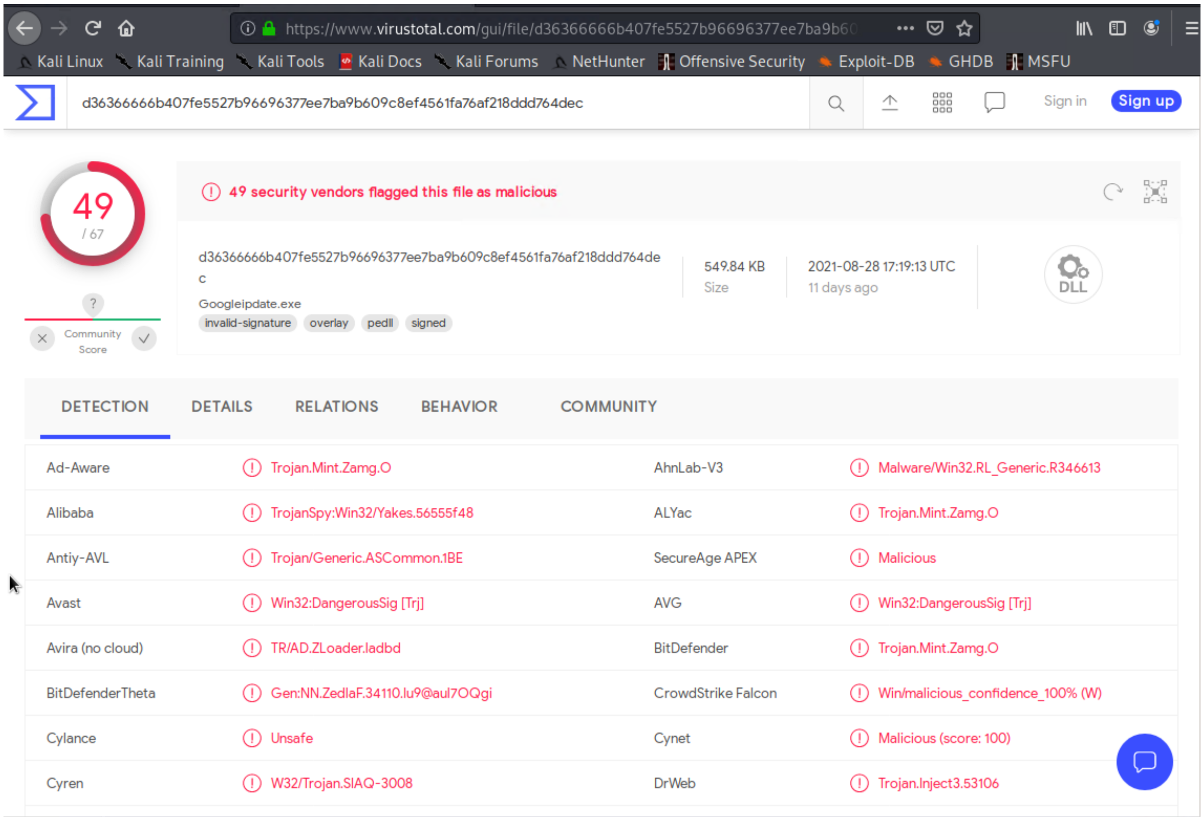
Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community

By submitting data below, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

Want to automate submissions? Check our API, free quota grants available for new file uploads

5. What kind of malware is this classified as?

    - **The Trojan name is: Trojan.Mint.Zamg.O**



d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

49 / 67

49 security vendors flagged this file as malicious

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764de
c

Googleipdate.exe

invalid-signature overlay pedll signed

549.84 KB
Size

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

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.34110.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 Machine

The Security team received reports of an infected Windows host on the network. They know the following:

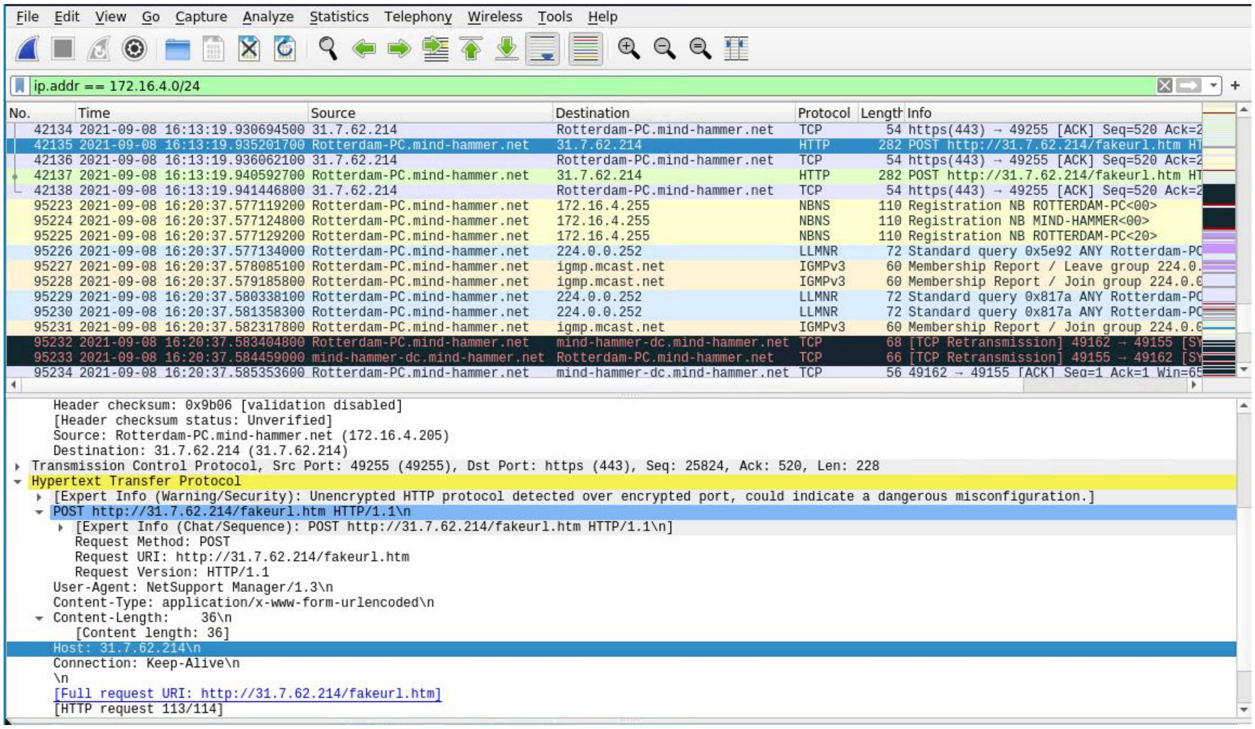
- Machines in the network live in the range 172.16.4.0/24.
- The domain mind-hammer.net is associated with the infected computer.
- The DC for this network lives at 172.16.4.4 and is named Mind-Hammer-DC.
- The network has standard gateway and broadcast addresses.

Following Wireshark Filters were Used:

- Host Name, IP Address, MAC Address: ip.addr == 172.16.4.0/24
- Traffic Inspection: ip.src == 172.16.4.4 && kerberos.CNameString
- Username: ip.src == 172.16.4.205 && kerberos.CNameString
- Malicious Traffic: ip.addr == 172.16.4.205 && ip.addr == 185.243.115.84

Inspect your traffic to answer the following questions:

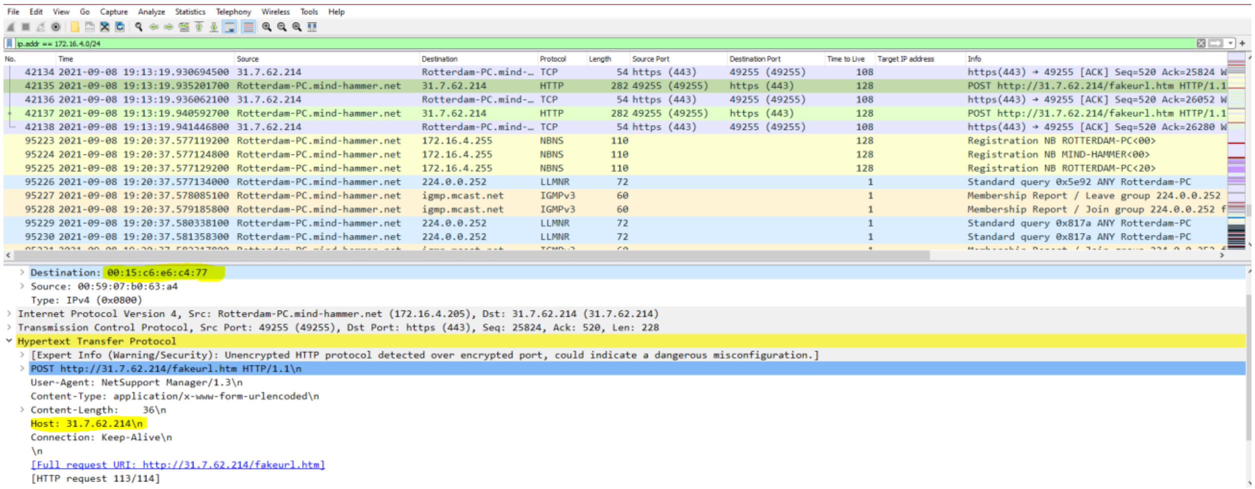
1. Find the following information about the infected Windows machine:
    - Host name: ROTTERDAM-PC
    - IP address: 172.16.4.205
    - MAC address: 00:59:07:b0:63:a4
    - Wireshark Filter: ip.addr == 172.16.4.0/24



ip.addr == 172.16.4.0/24

```
No.   Time                          Source                        Destination                   Protocol Length Info
42134 2021-09-08 16:13:19.930694500 31.7.62.214                   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 31.7.62.214                   Rotterdam-PC.mind-hammer.net  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 31.7.62.214                   Rotterdam-PC.mind-hammer.net  TCP       54 https(443) → 49255 [ACK] Seq=520 Ack=2
95223 2021-09-08 16:20:37.577119200 Rotterdam-PC.mind-hammer.net  172.16.4.255                  NBNS     110 Registration NB ROTTERDAM-PC<00>
95224 2021-09-08 16:20:37.577124800 Rotterdam-PC.mind-hammer.net  172.16.4.255                  NBNS     110 Registration NB MIND-HAMMER<00>
95225 2021-09-08 16:20:37.577129200 Rotterdam-PC.mind-hammer.net  172.16.4.255                  NBNS     110 Registration NB ROTTERDAM-PC<20>
95226 2021-09-08 16:20:37.577134000 Rotterdam-PC.mind-hammer.net  224.0.0.252                   LLMNR     72 Standard query 0x5e92 ANY Rotterdam-PC
95227 2021-09-08 16:20:37.578085100 Rotterdam-PC.mind-hammer.net  igmp.mcast.net                IGMPv3    60 Membership Report / Leave group 224.0.
95228 2021-09-08 16:20:37.579185800 Rotterdam-PC.mind-hammer.net  igmp.mcast.net                IGMPv3    60 Membership Report / Join group 224.0.0
95229 2021-09-08 16:20:37.580338100 Rotterdam-PC.mind-hammer.net  224.0.0.252                   LLMNR     72 Standard query 0x817a ANY Rotterdam-PC
95230 2021-09-08 16:20:37.581358300 Rotterdam-PC.mind-hammer.net  224.0.0.252                   LLMNR     72 Standard query 0x817a ANY Rotterdam-PC
95231 2021-09-08 16:20:37.582317800 Rotterdam-PC.mind-hammer.net  igmp.mcast.net                IGMPv3    60 Membership Report / Join group 224.0.0
95232 2021-09-08 16:20:37.583404800 Rotterdam-PC.mind-hammer.net  mind-hammer-dc.mind-hammer.net TCP      68 [TCP Retransmission] 49162 → 49155 [SY
95233 2021-09-08 16:20:37.584459000 mind-hammer-dc.mind-hammer.net Rotterdam-PC.mind-hammer.net TCP      66 [TCP Retransmission] 49155 → 49162 [SY
95234 2021-09-08 16:20:37.585353600 Rotterdam-PC.mind-hammer.net  mind-hammer-dc.mind-hammer.net TCP      56 49162 → 49155 [ACK] Seq=1 Ack=1 Win=65
```

```
    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\n
    ▸ [Expert Info (Chat/Sequence): POST http://31.7.62.214/fakeurl.htm HTTP/1.1\n]
      Request Method: POST
      Request URI: http://31.7.62.214/fakeurl.htm
      Request Version: HTTP/1.1
    User-Agent: NetSupport Manager/1.3\n
    Content-Type: application/x-www-form-urlencoded\n
  ▾ Content-Length:    36\n
      [Content length: 36]
    Host: 31.7.62.214\n
    Connection: Keep-Alive\n
    \n
    [Full request URI: http://31.7.62.214/fakeurl.htm]
    [HTTP request 113/114]
```


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

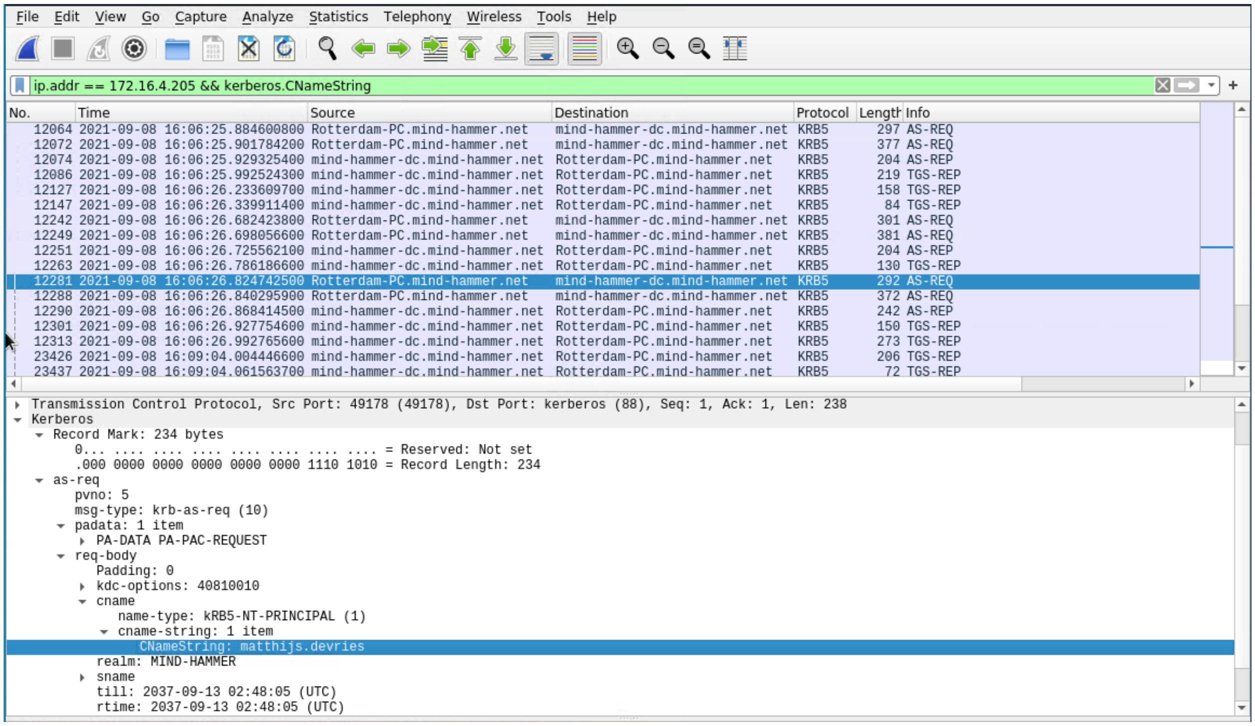
ip.addr == 172.16.4.0/24

No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Time to Live	Target IP address	Info
42134	2021-09-08 19:13:19.930694500	31.7.62.214	Rotterdam-PC.mind-…	TCP	54	https (443)	49255 (49255)	108		https(443) → 49255 [ACK] Seq=520 Ack=25824 W
42135	2021-09-08 19:13:19.935201700	Rotterdam-PC.mind-hammer.net	31.7.62.214	HTTP	282	49255 (49255)	https (443)	128		POST http://31.7.62.214/fakeurl.htm HTTP/1.1
42136	2021-09-08 19:13:19.936062100	31.7.62.214	Rotterdam-PC.mind-…	TCP	54	https (443)	49255 (49255)	108		https(443) → 49255 [ACK] Seq=520 Ack=26052 W
42137	2021-09-08 19:13:19.940592700	Rotterdam-PC.mind-hammer.net	31.7.62.214	HTTP	282	49255 (49255)	https (443)	128		POST http://31.7.62.214/fakeurl.htm HTTP/1.1
42138	2021-09-08 19:13:19.941446800	31.7.62.214	Rotterdam-PC.mind-…	TCP	54	https (443)	49255 (49255)	108		https(443) → 49255 [ACK] Seq=520 Ack=26280 W
95223	2021-09-08 19:20:37.577119200	Rotterdam-PC.mind-hammer.net	172.16.4.255	NBNS	110			128		Registration NB ROTTERDAM-PC<00>
95224	2021-09-08 19:20:37.577124800	Rotterdam-PC.mind-hammer.net	172.16.4.255	NBNS	110			128		Registration NB MIND-HAMMER<00>
95225	2021-09-08 19:20:37.577129200	Rotterdam-PC.mind-hammer.net	172.16.4.255	NBNS	110			128		Registration NB ROTTERDAM-PC<20>
95226	2021-09-08 19:20:37.577134000	Rotterdam-PC.mind-hammer.net	224.0.0.252	LLMNR	72			1		Standard query 0x5e92 ANY Rotterdam-PC
95227	2021-09-08 19:20:37.578085100	Rotterdam-PC.mind-hammer.net	igmp.mcast.net	IGMPv3	60			1		Membership Report / Leave group 224.0.0.252
95228	2021-09-08 19:20:37.579185800	Rotterdam-PC.mind-hammer.net	igmp.mcast.net	IGMPv3	60			1		Membership Report / Join group 224.0.0.252 f
95229	2021-09-08 19:20:37.580338100	Rotterdam-PC.mind-hammer.net	224.0.0.252	LLMNR	72			1		Standard query 0x817a ANY Rotterdam-PC
95230	2021-09-08 19:20:37.581358300	Rotterdam-PC.mind-hammer.net	224.0.0.252	LLMNR	72			1		Standard query 0x817a ANY Rotterdam-PC

```
  > Destination: 00:15:c6:e6:c4:77
  > Source: 00:59:07:b0:63:a4
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: Rotterdam-PC.mind-hammer.net (172.16.4.205), Dst: 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
v 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\n
    User-Agent: NetSupport Manager/1.3\n
    Content-Type: application/x-www-form-urlencoded\n
  > Content-Length:    36\n
    Host: 31.7.62.214\n
    Connection: Keep-Alive\n
    \n
    [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



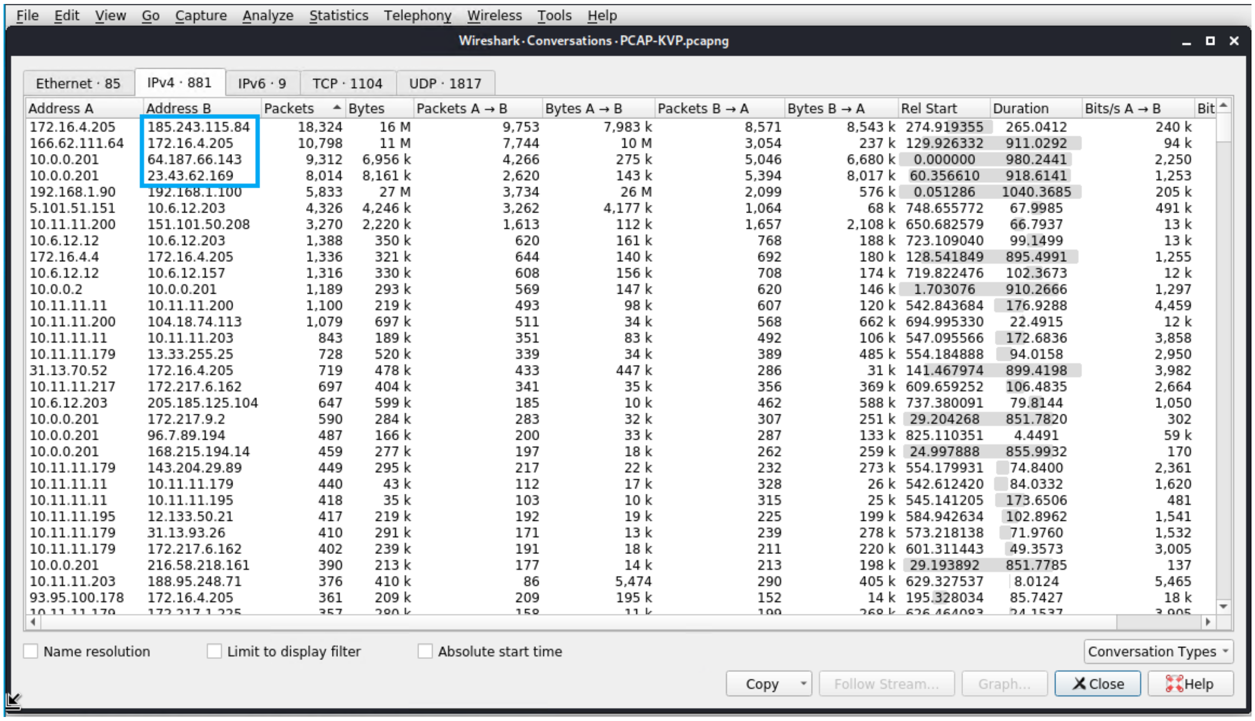
ip.addr == 172.16.4.205 && kerberos.CNameString

```
No.   Time                          Source                          Destination                     Protocol Length Info
12064 2021-09-08 16:06:25.884600800 Rotterdam-PC.mind-hammer.net    mind-hammer-dc.mind-hammer.net  KRB5     297 AS-REQ
12072 2021-09-08 16:06:25.901784200 Rotterdam-PC.mind-hammer.net    mind-hammer-dc.mind-hammer.net  KRB5     377 AS-REQ
12074 2021-09-08 16:06:25.929325400 mind-hammer-dc.mind-hammer.net  Rotterdam-PC.mind-hammer.net    KRB5     204 AS-REP
12086 2021-09-08 16:06:25.992524300 mind-hammer-dc.mind-hammer.net  Rotterdam-PC.mind-hammer.net    KRB5     219 TGS-REP
12127 2021-09-08 16:06:26.233609700 mind-hammer-dc.mind-hammer.net  Rotterdam-PC.mind-hammer.net    KRB5     158 TGS-REP
12147 2021-09-08 16:06:26.339911400 mind-hammer-dc.mind-hammer.net  Rotterdam-PC.mind-hammer.net    KRB5      84 TGS-REP
12242 2021-09-08 16:06:26.682423800 Rotterdam-PC.mind-hammer.net    mind-hammer-dc.mind-hammer.net  KRB5     301 AS-REQ
12249 2021-09-08 16:06:26.698056600 Rotterdam-PC.mind-hammer.net    mind-hammer-dc.mind-hammer.net  KRB5     381 AS-REQ
12251 2021-09-08 16:06:26.725562100 mind-hammer-dc.mind-hammer.net  Rotterdam-PC.mind-hammer.net    KRB5     204 AS-REP
12263 2021-09-08 16:06:26.786186600 mind-hammer-dc.mind-hammer.net  Rotterdam-PC.mind-hammer.net    KRB5     130 TGS-REP
12281 2021-09-08 16:06:26.824742500 Rotterdam-PC.mind-hammer.net    mind-hammer-dc.mind-hammer.net  KRB5     292 AS-REQ
12288 2021-09-08 16:06:26.840295900 Rotterdam-PC.mind-hammer.net    mind-hammer-dc.mind-hammer.net  KRB5     372 AS-REQ
12290 2021-09-08 16:06:26.868414500 mind-hammer-dc.mind-hammer.net  Rotterdam-PC.mind-hammer.net    KRB5     242 AS-REP
12301 2021-09-08 16:06:26.927754600 mind-hammer-dc.mind-hammer.net  Rotterdam-PC.mind-hammer.net    KRB5     150 TGS-REP
12313 2021-09-08 16:06:26.992765600 mind-hammer-dc.mind-hammer.net  Rotterdam-PC.mind-hammer.net    KRB5     273 TGS-REP
23426 2021-09-08 16:09:04.004446600 mind-hammer-dc.mind-hammer.net  Rotterdam-PC.mind-hammer.net    KRB5     206 TGS-REP
23437 2021-09-08 16:09:04.061563700 mind-hammer-dc.mind-hammer.net  Rotterdam-PC.mind-hammer.net    KRB5      72 TGS-REP
```

```
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 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?

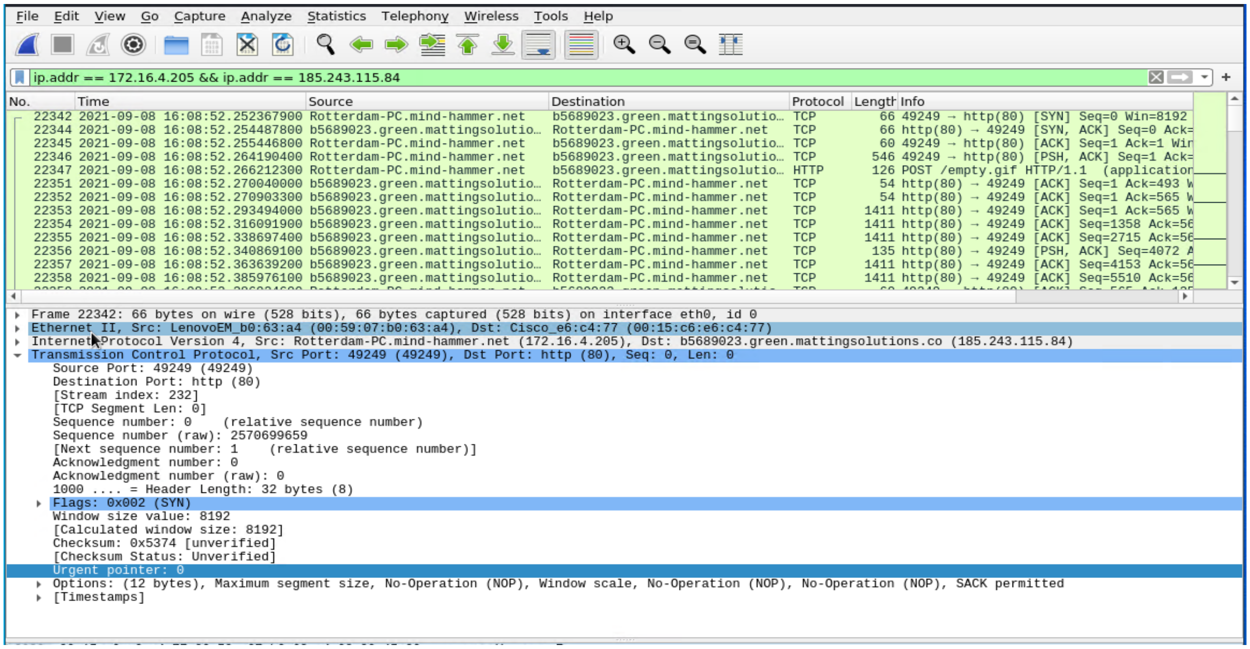
- Filter: ip.src==172.16.4.203 and kerberos.CNameString
- I found 4 IP addresses: 172.16.4.205, 185.243.115.84, 166.62.11.64 and 23.43.62.169
- Finding the IP addresses:
    - Click on the Statistics Tab
    - Select the Conversation
    - Select the IPv4
    - Sort Packets high to low


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Conversations · PCAP-KVP.pcapng
Ethernet · 85
IPv4 · 881
IPv6 · 9
TCP · 1104
UDP · 1817

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	274.919355	265.0412	240 k	
166.62.111.64	172.16.4.205	10,798	11 M	7,744	10 M	3,054	237 k	129.926332	911.0292	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	
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	
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	
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	
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	
10.6.12.12	10.6.12.203	1,388	350 k	620	161 k	768	188 k	723.109040	99.1499	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	
10.6.12.12	10.6.12.157	1,316	330 k	608	156 k	708	174 k	719.822476	102.3673	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	
10.11.11.11	10.11.11.200	1,100	219 k	493	98 k	607	120 k	542.843684	176.9288	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	
10.11.11.11	10.11.11.203	843	189 k	351	83 k	492	106 k	547.095566	172.6836	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	
31.13.70.52	172.16.4.205	719	478 k	433	447 k	286	31 k	141.467974	899.4198	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	
10.6.12.203	205.185.125.104	647	599 k	185	10 k	462	588 k	737.380091	79.8144	1,050	
10.0.0.201	172.217.9.2	590	284 k	283	32 k	307	251 k	29.204268	851.7820	302	
10.0.0.201	96.7.89.194	487	166 k	200	33 k	287	133 k	825.110351	4.4491	59 k	
10.0.0.201	168.215.194.14	459	277 k	197	18 k	262	259 k	24.997888	855.9932	170	
10.11.11.179	143.204.29.89	449	295 k	217	22 k	232	273 k	554.179931	74.8400	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	
10.11.11.11	10.11.11.195	418	35 k	103	10 k	315	25 k	545.141205	173.6506	481	
10.11.11.195	12.133.50.21	417	219 k	192	19 k	225	199 k	584.942634	102.8962	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	
10.11.11.179	172.217.6.162	402	239 k	191	18 k	211	220 k	601.311443	49.3573	3,005	
10.0.0.201	216.58.218.161	390	213 k	177	14 k	213	198 k	29.193892	851.7785	137	
10.11.11.203	188.95.248.71	376	410 k	86	5,474	290	405 k	629.327537	8.0124	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	
10.11.11.179	172.217.1.225	357	280 k	158	11 k	199	268 k	626.464083	24.1537	3,905	

□ Name resolution □ Limit to display filter □ Absolute start time

- Additional Traffic from 185.243.115.84 to infected host 17216.4.205

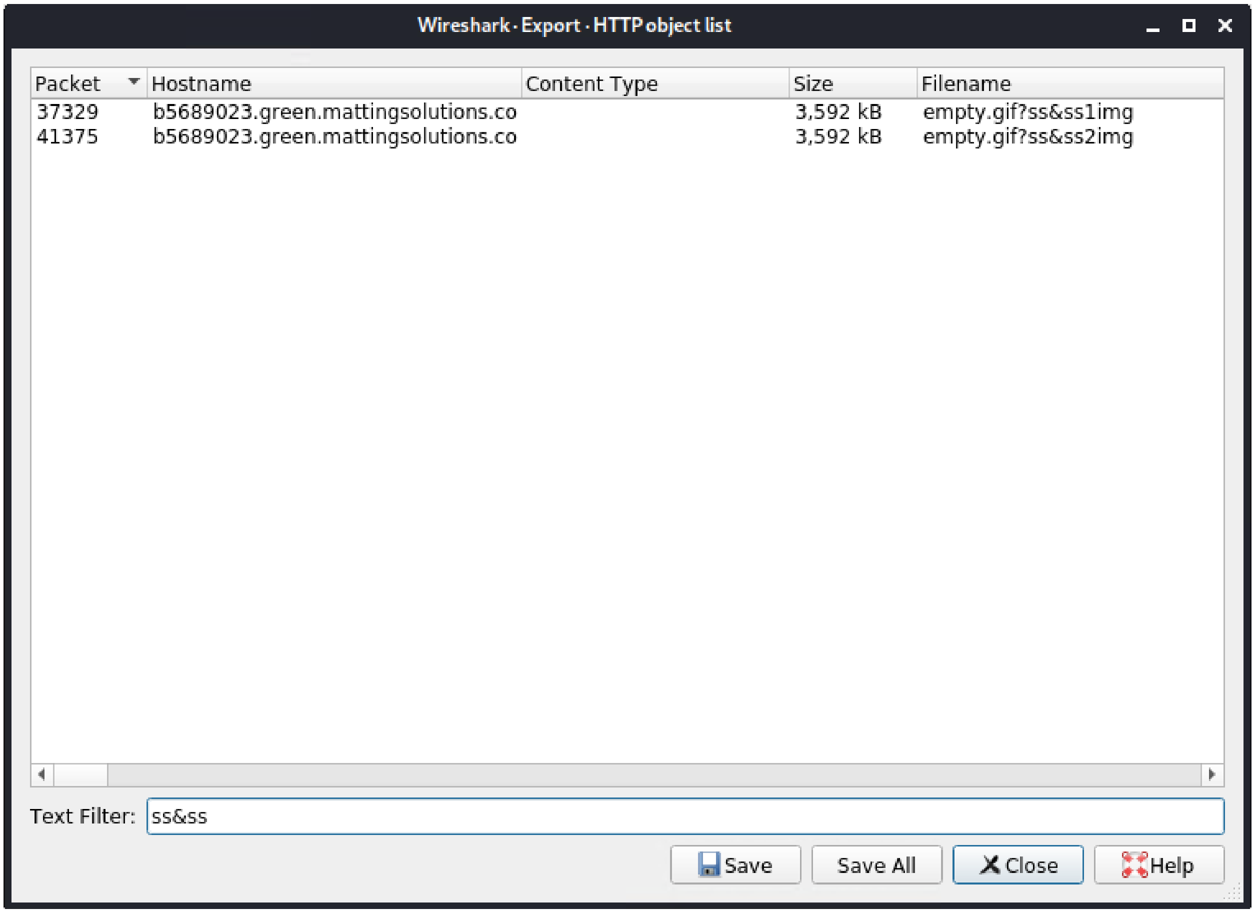


```
ip.addr == 172.16.4.205 && ip.addr == 185.243.115.84
```

```
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] 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 16:08:52.264190400 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  (application
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 (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: 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]
    Urgent pointer: 0
  ▸ 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.


Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
37329	b5689023.green.mattingsolutions.co		3,592 kB	empty.gif?ss&ss1img
41375	b5689023.green.mattingsolutions.co		3,592 kB	empty.gif?ss&ss2img

Text Filter: ss&ss

Recycle Bin
6:59 PM
7/19/2019

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.

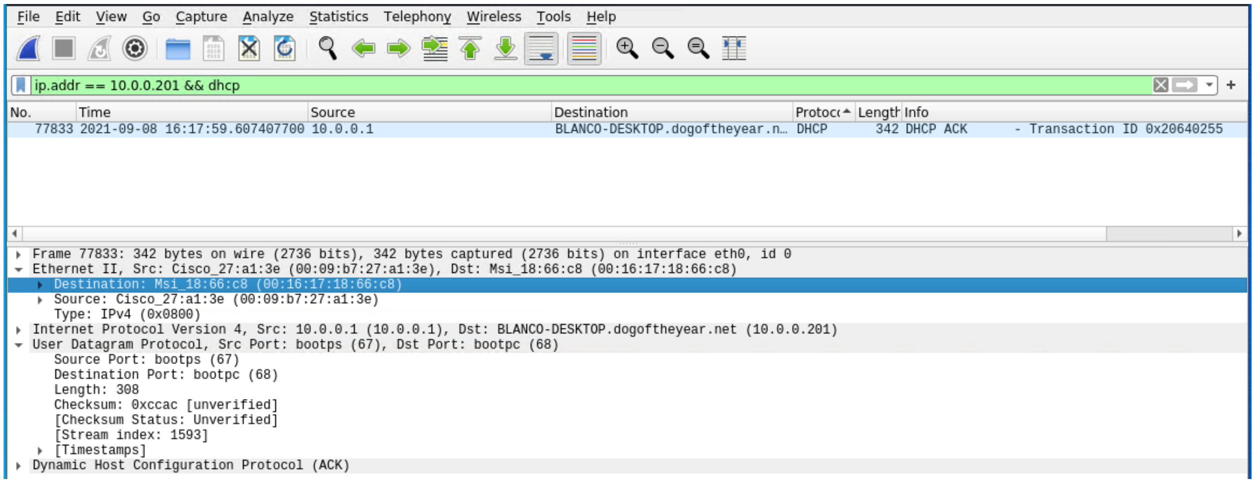
Wireshark Filters Used:

- 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**

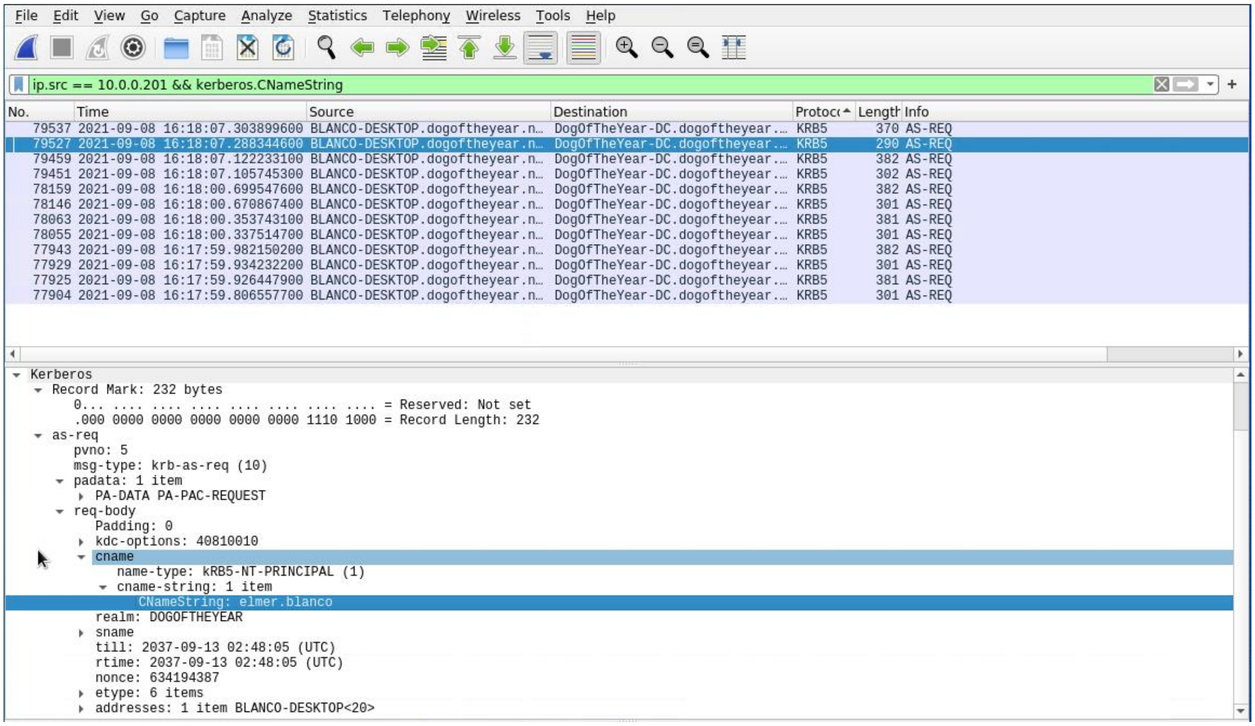
- Wireshark Filter for MAC Address: **ip.addr == 10.0.0.201 && dhcp**



```
ip.addr == 10.0.0.201 && dhcp
No.   Time                          Source     Destination                     Protoc Length Info
 77833 2021-09-08 16:17:59.607407700 10.0.0.1   BLANCO-DESKTOP.dogoftheyear.n… DHCP      342 DHCP ACK       - Transaction ID 0x20640255

▸ Frame 77833: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface eth0, id 0
▾ Ethernet II, Src: Cisco_27:a1:3e (00:09:b7:27:a1:3e), Dst: Msi_18:66:c8 (00:16:17:18:66:c8)
  ▸ Destination: Msi_18:66:c8 (00:16:17:18:66:c8)
  ▸ Source: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.0.0.1 (10.0.0.1), Dst: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201)
▾ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
    Source Port: bootps (67)
    Destination Port: bootpc (68)
    Length: 308
    Checksum: 0xccac [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1593]
  ▸ [Timestamps]
▸ Dynamic Host Configuration Protocol (ACK)
```

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

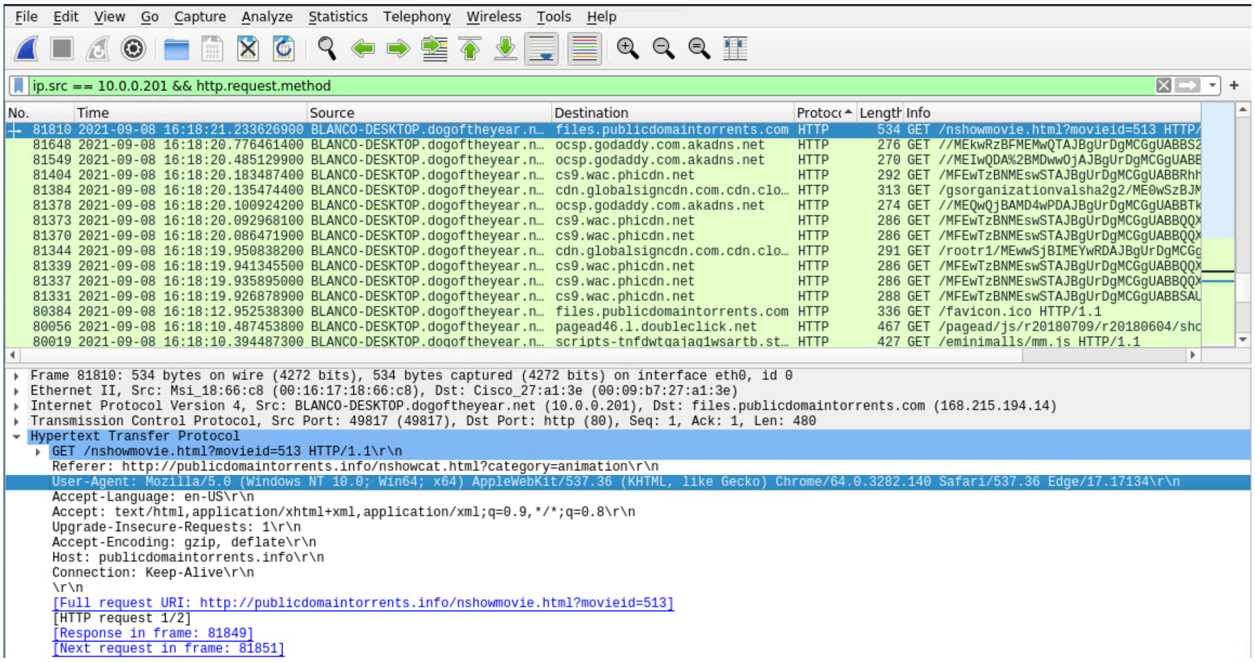


```
ip.src == 10.0.0.201 && kerberos.CNameString
```

```
No.   Time                          Source                        Destination                   Protoc 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
    .000 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 **OS Type and Version**: **ip.addr == 10.0.0.201 && http.request**



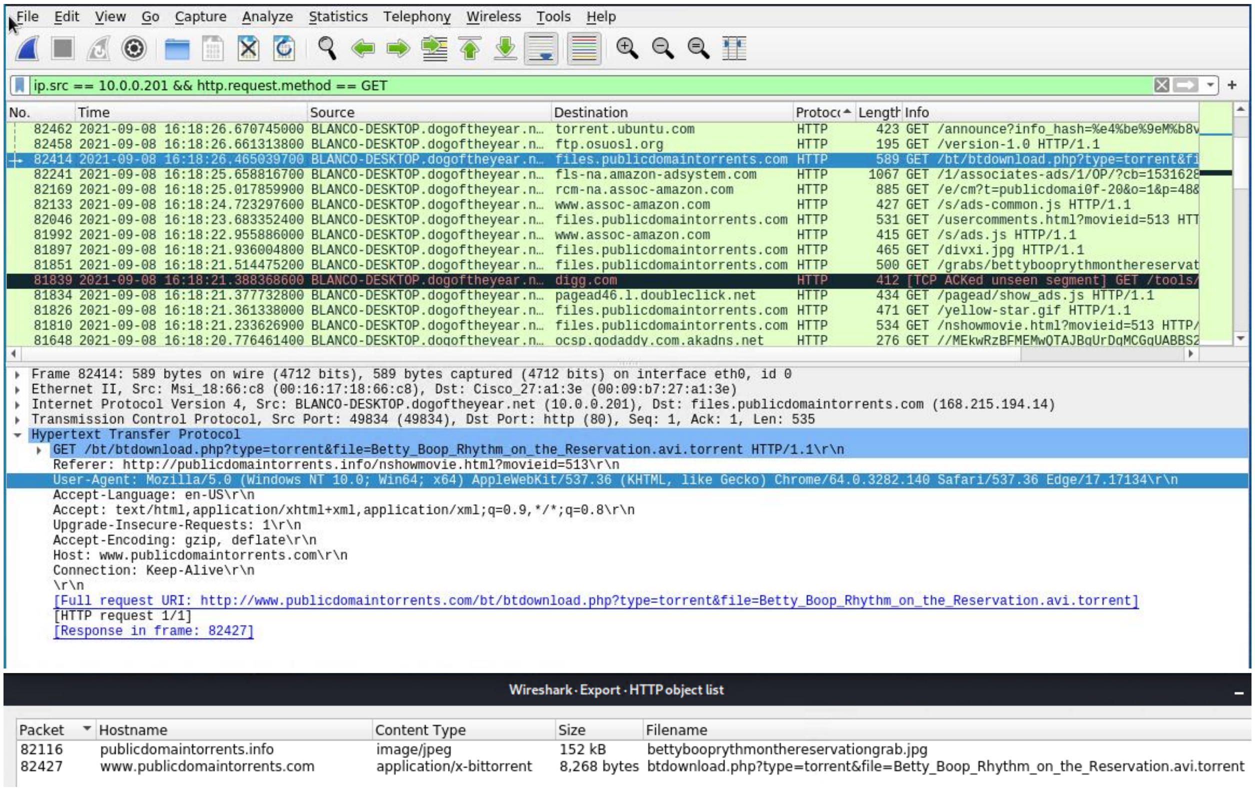
```
ip.src == 10.0.0.201 && http.request.method
```

```
No.   Time                          Source                        Destination                     Protoc 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/
81648 2021-09-08 16:18:20.776461400 BLANCO-DESKTOP.dogoftheyear.n… ocsp.godaddy.com.akadns.net    HTTP   276 GET //MEkwRzBFMEMwQTAJBgUrDgMCGgUABBS2
81549 2021-09-08 16:18:20.485129900 BLANCO-DESKTOP.dogoftheyear.n… ocsp.godaddy.com.akadns.net    HTTP   270 GET //MEIwQDA%2BMDwwOjAJBgUrDgMCGgUABE
81404 2021-09-08 16:18:20.183487400 BLANCO-DESKTOP.dogoftheyear.n… cs9.wac.phicdn.net             HTTP   292 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBRhh
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 /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQQX
81370 2021-09-08 16:18:20.086471900 BLANCO-DESKTOP.dogoftheyear.n… cs9.wac.phicdn.net             HTTP   286 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQQX
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 /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQQX
81337 2021-09-08 16:18:19.935895000 BLANCO-DESKTOP.dogoftheyear.n… cs9.wac.phicdn.net             HTTP   286 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQQX
81331 2021-09-08 16:18:19.926878900 BLANCO-DESKTOP.dogoftheyear.n… cs9.wac.phicdn.net             HTTP   288 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAU
80384 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/r20180709/r20180604/shc
80019 2021-09-08 16:18:10.394487300 BLANCO-DESKTOP.dogoftheyear.n… scripts-tnfdwtqajaq1wsartb.st… HTTP   427 GET /eminimalls/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 (00:16:17:18:66:c8), Dst: Cisco_27:a1:3e (00:09: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.



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

```
No.   Time                          Source                          Destination                      Protoc Length Info
82462 2021-09-08 16:18:26.670745000 BLANCO-DESKTOP.dogoftheyear.n… torrent.ubuntu.com               HTTP    423 GET /announce?info_hash=%e4%be%9eM%b8v
82458 2021-09-08 16:18:26.661313800 BLANCO-DESKTOP.dogoftheyear.n… ftp.osuosl.org                   HTTP    195 GET /version-1.0 HTTP/1.1
82414 2021-09-08 16:18:26.465039700 BLANCO-DESKTOP.dogoftheyear.n… files.publicdomaintorrents.com   HTTP    589 GET /bt/btdownload.php?type=torrent&fi
82241 2021-09-08 16:18:25.658816700 BLANCO-DESKTOP.dogoftheyear.n… fls-na.amazon-adsystem.com       HTTP   1067 GET /1/associates-ads/1/OP/?cb=1531628
82169 2021-09-08 16:18:25.017859900 BLANCO-DESKTOP.dogoftheyear.n… rcm-na.assoc-amazon.com          HTTP    885 GET /e/cm?t=publicdomai0f-20&o=1&p=48&
82133 2021-09-08 16:18:24.723297600 BLANCO-DESKTOP.dogoftheyear.n… www.assoc-amazon.com             HTTP    427 GET /s/ads-common.js HTTP/1.1
82046 2021-09-08 16:18:23.683352400 BLANCO-DESKTOP.dogoftheyear.n… files.publicdomaintorrents.com   HTTP    531 GET /usercomments.html?movieid=513 HTT
81992 2021-09-08 16:18:22.955886000 BLANCO-DESKTOP.dogoftheyear.n… www.assoc-amazon.com             HTTP    415 GET /s/ads.js HTTP/1.1
81897 2021-09-08 16:18:21.936004800 BLANCO-DESKTOP.dogoftheyear.n… files.publicdomaintorrents.com   HTTP    465 GET /divxi.jpg HTTP/1.1
81851 2021-09-08 16:18:21.514475200 BLANCO-DESKTOP.dogoftheyear.n… files.publicdomaintorrents.com   HTTP    500 GET /grabs/bettybooprythmonthereservat
81839 2021-09-08 16:18:21.388368600 BLANCO-DESKTOP.dogoftheyear.n… digg.com                         HTTP    412 [TCP ACKed unseen segment] GET /tools/
81834 2021-09-08 16:18:21.377732800 BLANCO-DESKTOP.dogoftheyear.n… pagead46.l.doubleclick.net       HTTP    434 GET /pagead/show_ads.js HTTP/1.1
81826 2021-09-08 16:18:21.361338000 BLANCO-DESKTOP.dogoftheyear.n… files.publicdomaintorrents.com   HTTP    471 GET /yellow-star.gif HTTP/1.1
81810 2021-09-08 16:18:21.233626900 BLANCO-DESKTOP.dogoftheyear.n… files.publicdomaintorrents.com   HTTP    534 GET /nshowmovie.html?movieid=513 HTTP/
81648 2021-09-08 16:18:20.776461400 BLANCO-DESKTOP.dogoftheyear.n… ocsp.godaddy.com.akadns.net      HTTP    276 GET //MEkwRzBFMEMwQTAJBgUrDgMCGgUABBS2
```

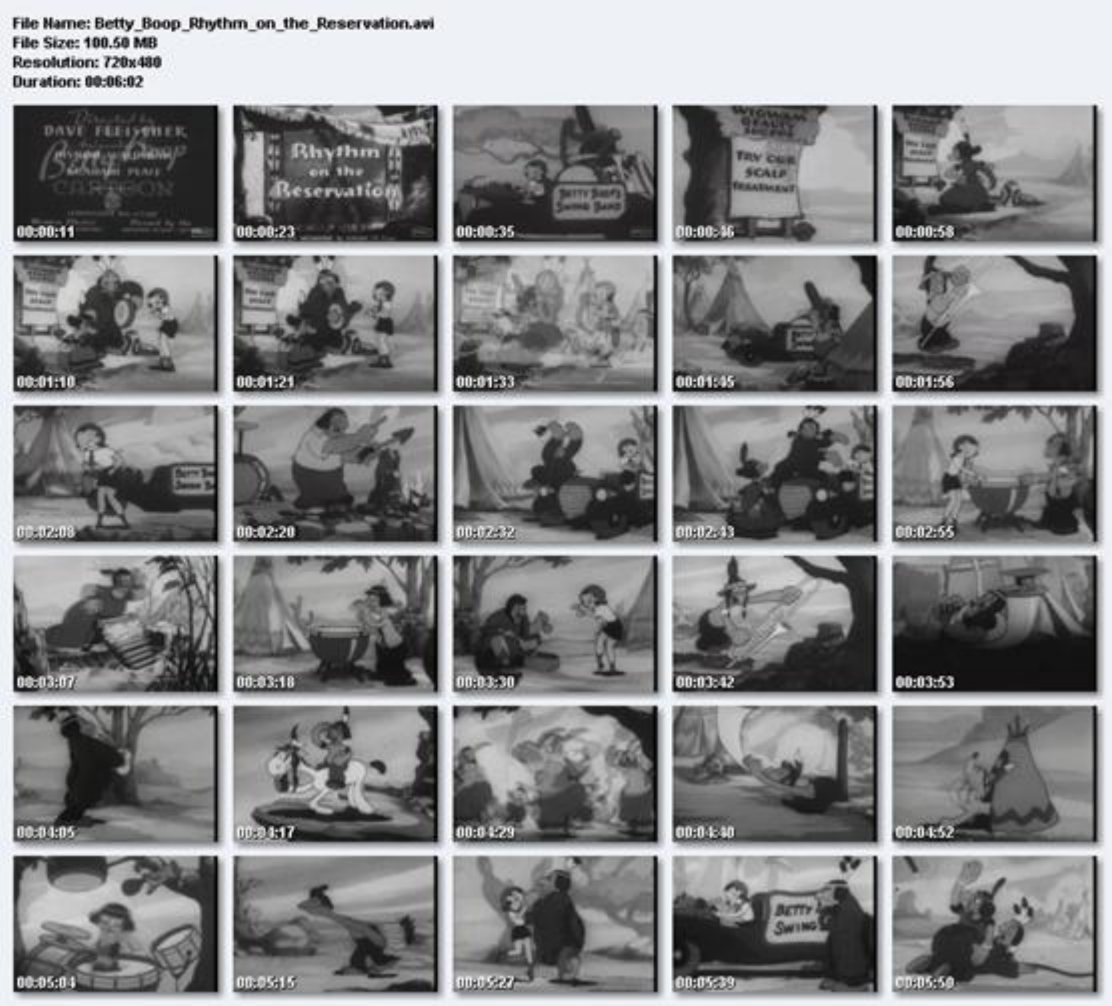
```
▸ Frame 82414: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits) on interface eth0, id 0
▸ Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
▸ Internet Protocol Version 4, Src: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201), Dst: files.publicdomaintorrents.com (168.215.194.14)
▸ Transmission Control Protocol, Src Port: 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 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: 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: 82427]
```

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
82116	publicdomaintorrents.info	image/jpeg	152 kB	bettybooprythmonthereservationgrab.jpg
82427	www.publicdomaintorrents.com	application/x-bittorrent	8,268 bytes	btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent

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