Detect and analyze TCP/IP traffic with Wireshark

Description

I want to detect certain TCP/IP network traffic on my server, specifically web traffic.

Languages and Utilities Used

- Wireshark

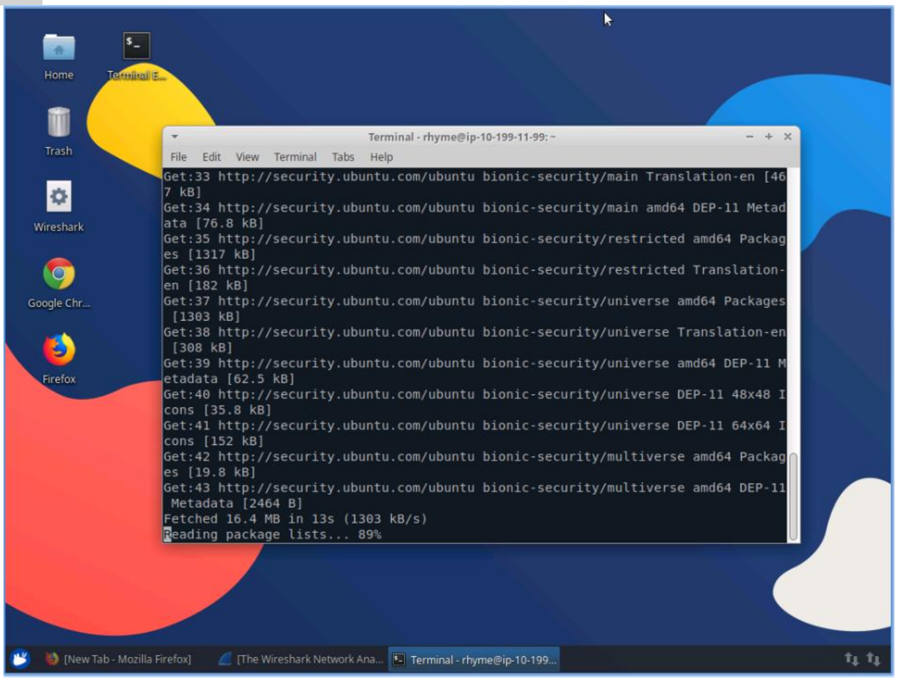
Environments Used

- Linux

Program walk-through:

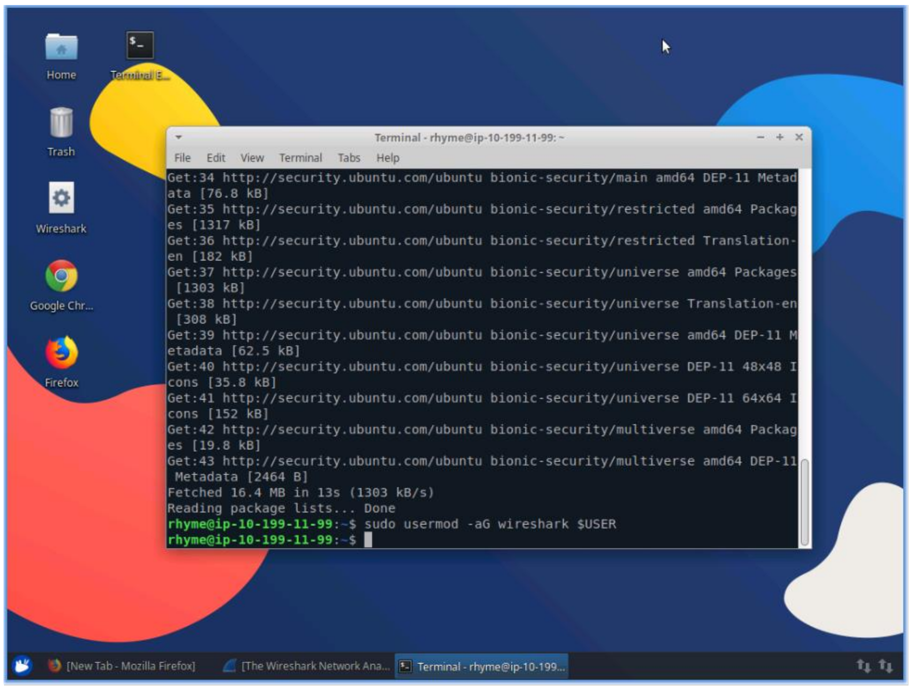
Install and set up Wireshark

To get the latest stable version of Wireshark on Ubuntu Linux I used the add-apt-repository command: *sudo add-apt-repository ppa:wireshark-dev/stable*


Home
Terminal E...
Trash
Wireshark
Google Chr...
Firefox
Terminal - rhyme@ip-10-199-11-99: ~
File Edit View Terminal Tabs Help
[New Tab - Mozilla Firefox]
[The Wireshark Network Ana...
Terminal - rhyme@ip-10-199...

```
Get:33 http://security.ubuntu.com/ubuntu bionic-security/main Translation-en [46
7 kB]
Get:34 http://security.ubuntu.com/ubuntu bionic-security/main amd64 DEP-11 Metad
ata [76.8 kB]
Get:35 http://security.ubuntu.com/ubuntu bionic-security/restricted amd64 Packag
es [1317 kB]
Get:36 http://security.ubuntu.com/ubuntu bionic-security/restricted Translation-
en [182 kB]
Get:37 http://security.ubuntu.com/ubuntu bionic-security/universe amd64 Packages
 [1303 kB]
Get:38 http://security.ubuntu.com/ubuntu bionic-security/universe Translation-en
 [308 kB]
Get:39 http://security.ubuntu.com/ubuntu bionic-security/universe amd64 DEP-11 M
etadata [62.5 kB]
Get:40 http://security.ubuntu.com/ubuntu bionic-security/universe DEP-11 48x48 I
cons [35.8 kB]
Get:41 http://security.ubuntu.com/ubuntu bionic-security/universe DEP-11 64x64 I
cons [152 kB]
Get:42 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 Packag
es [19.8 kB]
Get:43 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 DEP-11
 Metadata [2464 B]
Fetched 16.4 MB in 13s (1303 kB/s)
Reading package lists... 89%
```

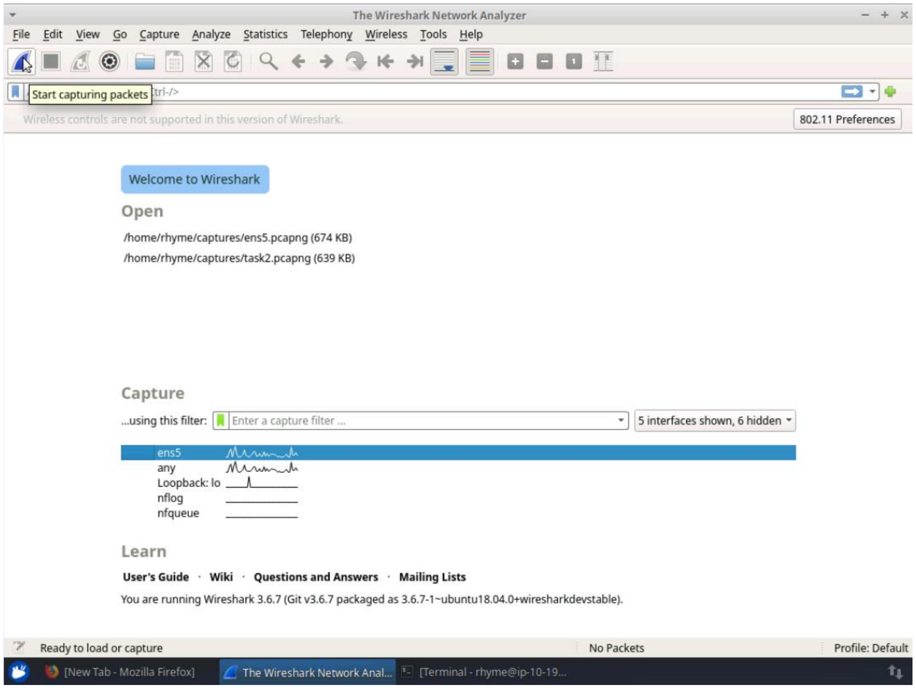
Since Wireshark should not run as superuser for security reasons I needed to set up Wireshark, for non-users belonging to the Wireshark group to get packet capture capabilities, and I did it with the command: *sudo usermod -aG wireshark $USER*


Home
Terminal E...
Trash
Wireshark
Google Chr...
Firefox
Terminal - rhyme@ip-10-199-11-99: ~
File Edit View Terminal Tabs Help
[New Tab - Mozilla Firefox]
[The Wireshark Network Ana...
Terminal - rhyme@ip-10-199...

```
Get:34 http://security.ubuntu.com/ubuntu bionic-security/main amd64 DEP-11 Metad
ata [76.8 kB]
Get:35 http://security.ubuntu.com/ubuntu bionic-security/restricted amd64 Packag
es [1317 kB]
Get:36 http://security.ubuntu.com/ubuntu bionic-security/restricted Translation-
en [182 kB]
Get:37 http://security.ubuntu.com/ubuntu bionic-security/universe amd64 Packages
 [1303 kB]
Get:38 http://security.ubuntu.com/ubuntu bionic-security/universe Translation-en
 [308 kB]
Get:39 http://security.ubuntu.com/ubuntu bionic-security/universe amd64 DEP-11 M
etadata [62.5 kB]
Get:40 http://security.ubuntu.com/ubuntu bionic-security/universe DEP-11 48x48 I
cons [35.8 kB]
Get:41 http://security.ubuntu.com/ubuntu bionic-security/universe DEP-11 64x64 I
cons [152 kB]
Get:42 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 Packag
es [19.8 kB]
Get:43 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 DEP-11
 Metadata [2464 B]
Fetched 16.4 MB in 13s (1303 kB/s)
Reading package lists... Done
rhyme@ip-10-199-11-99:~$ sudo usermod -aG wireshark $USER
rhyme@ip-10-199-11-99:~$
```

Start a packet capture on an ethernet port and save it to file

First, I chose the interface that begins with "*en*" in Wireshark, which is the wired interface that includes the ethernet packet capture.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Start capturing packets
802.11 Preferences
Welcome to Wireshark
Open
Capture
...using this filter:
Enter a capture filter ...
5 interfaces shown, 6 hidden
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
Ready to load or capture
No Packets
Profile: Default
[New Tab - Mozilla Firefox]
The Wireshark Network Anal...
[Terminal - rhyme@ip-10-19...

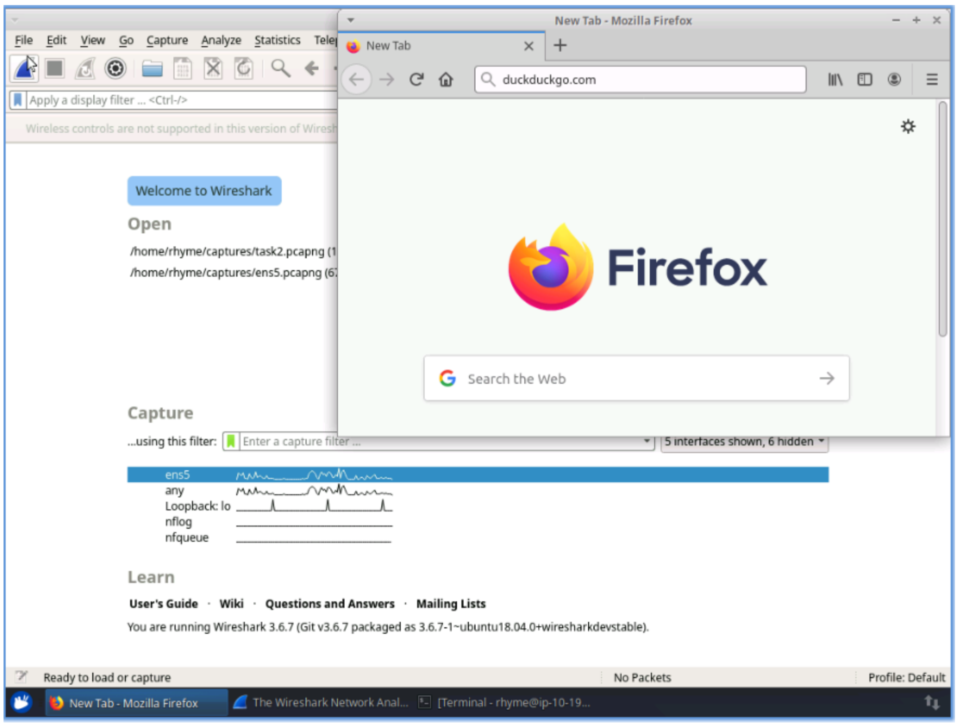
Wireless controls are not supported in this version of Wireshark.

/home/rhyme/captures/ens5.pcapng (674 KB)
/home/rhyme/captures/task2.pcapng (639 KB)

ens5
any
Loopback: lo
nflog
nfqueue

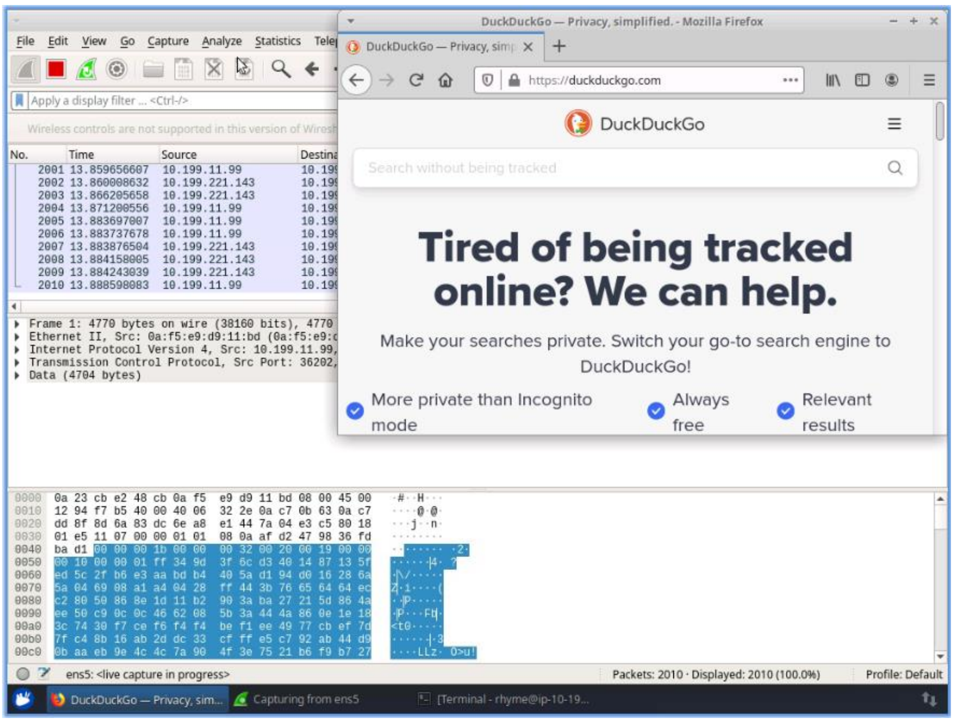
You are running Wireshark 3.6.7 (Git v3.6.7 packaged as 3.6.7-1~ubuntu18.04.0+wiresharkdevstable).

Before I started capturing packets, I opened my browser and searched for *duckduckgo.com*


File Edit View Go Capture Analyze Statistics Tele
Apply a display filter ... <Ctrl-/>
Wireless controls are not supported in this version of Wiresh
Welcome to Wireshark
Open
Capture
...using this filter:
Enter a capture filter ...
5 interfaces shown, 6 hidden
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
New Tab - Mozilla Firefox
New Tab
duckduckgo.com
Firefox
Search the Web
New Tab - Mozilla Firefox
The Wireshark Network Anal...
[Terminal - rhyme@ip-10-19...

```
/home/rhyme/captures/task2.pcapng (1
/home/rhyme/captures/ens5.pcapng (6

ens5
any
Loopback: lo
nflog
nfqueue

You are running Wireshark 3.6.7 (Git v3.6.7 packaged as 3.6.7-1~ubuntu18.04.0+wiresharkdevstable).

Ready to load or capture                No Packets                Profile: Default
```

Then I started capturing packets and immediately hit enter in the browser.


File Edit View Go Capture Analyze Statistics Tele
Apply a display filter ... <Ctrl-/>
Wireless controls are not supported in this version of Wiresh
DuckDuckGo — Privacy, simplified. - Mozilla Firefox
DuckDuckGo — Privacy, simp
https://duckduckgo.com
DuckDuckGo
Search without being tracked
DuckDuckGo — Privacy, sim...
Capturing from ens5
[Terminal - rhyme@ip-10-19...

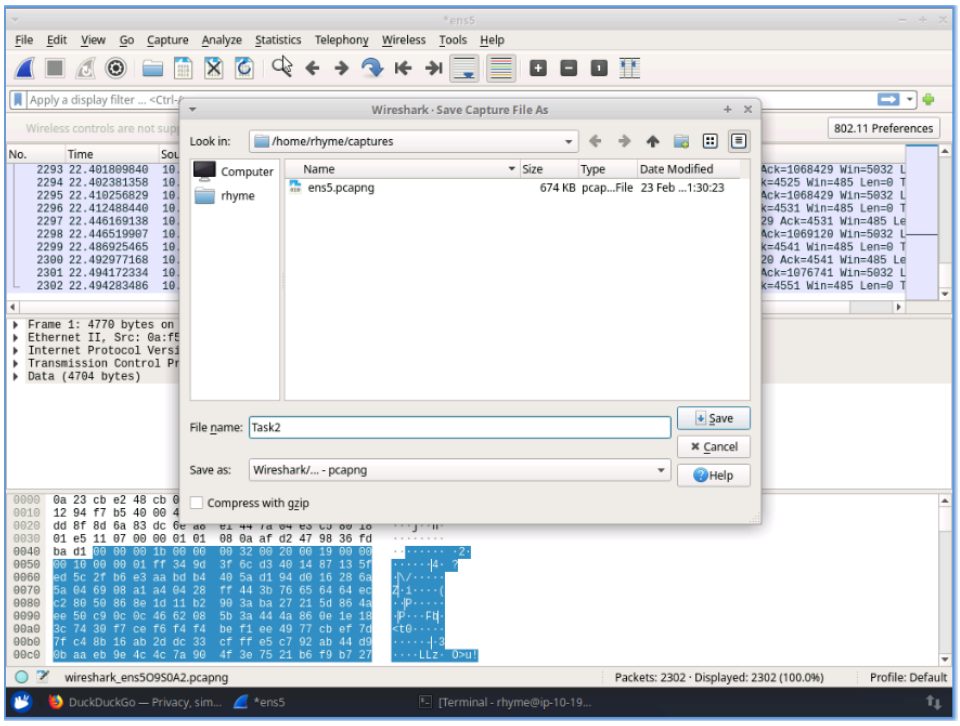
```
No.    Time          Source           Destina
  2001 13.859656607  10.199.11.99     10.199
  2002 13.860008632  10.199.221.143   10.199
  2003 13.866205658  10.199.221.143   10.199
  2004 13.871200556  10.199.11.99     10.199
  2005 13.883697007  10.199.11.99     10.199
  2006 13.883737678  10.199.11.99     10.199
  2007 13.883876504  10.199.221.143   10.199
  2008 13.884158005  10.199.221.143   10.199
  2009 13.884243039  10.199.221.143   10.199
  2010 13.888598083  10.199.11.99     10.199

▸ Frame 1: 4770 bytes on wire (38160 bits), 4770
▸ Ethernet II, Src: 0a:f5:e9:d9:11:bd (0a:f5:e9:c
▸ Internet Protocol Version 4, Src: 10.199.11.99,
▸ Transmission Control Protocol, Src Port: 36202,
▸ Data (4704 bytes)

0000  0a 23 cb e2 48 cb 0a f5  e9 d9 11 bd 08 00 45 00   ·#··H···
0010  12 94 f7 b5 40 00 40 06  32 2e 0a c7 0b 63 0a c7   ····@·@·
0020  dd 8f 8d 6a 83 dc 6e a8  e1 44 7a 04 e3 c5 80 18   ···j··n·
0030  01 e5 11 07 00 00 01 01  08 0a af d2 47 98 36 fd   ········
0040  ba d1 00 00 00 1b 00 00  00 32 00 20 00 19 00 00   ········ ·2·
0050  00 10 00 00 01 ff 34 9d  3f 6c d3 40 14 87 13 5f   ······4· ?
0060  ed 5c 2f b6 e3 aa bd b4  40 5a d1 94 d0 16 28 6a   ·\/·····
0070  5a 04 69 08 a1 a4 04 28  ff 44 3b 76 65 64 64 ec   Z·i····(
0080  c2 80 50 86 8e 1d 11 b2  90 3a ba 27 21 5d 86 4a   ··P·····
0090  ee 50 c9 0c 0c 46 62 08  5b 3a 44 4a 86 0e 1e 18   ·P···Fb·
00a0  3c 74 30 f7 ce f6 f4 f4  be f1 ee 49 77 cb ef 7d   <t0·····
00b0  7f c4 8b 16 ab 2d dc 33  cf ff e5 c7 92 ab 44 d9   ·····-·3
00c0  0b aa eb 9e 4c 4c 7a 90  4f 3e 75 21 b6 f9 b7 27   ····LLz· O>u!

ens5: <live capture in progress>      Packets: 2010 · Displayed: 2010 (100.0%)      Profile: Default
```

Tired of being tracked online? We can help.

Make your searches private. Switch your go-to search engine to DuckDuckGo!

- More private than Incognito mode
- Always free
- Relevant results

After waiting a while I stopped the capture and saved the file, as the capture can only be saved after the capture is stopped.



Wireshark · Save Capture File As

Look in: /home/rhyme/captures

Name	Size	Type	Date Modified
ens5.pcapng	674 KB	pcap...File	23 Feb ...1:30:23

File name: Task2

Save as: Wireshark/... - pcapng

Compress with gzip

```
2293 22.401809840 10.                Ack=1068429 Win=5032 L
2294 22.402381358 10.                k=4525 Win=485 Len=0 T
2295 22.410256829 10.                Ack=1068429 Win=5032 L
2296 22.412488440 10.                k=4531 Win=485 Len=0 T
2297 22.446169138 10.                29 Ack=4531 Win=485 Le
2298 22.446519907 10.                Ack=1069120 Win=5032 L
2299 22.486925465 10.                k=4541 Win=485 Len=0 T
2300 22.492977168 10.                20 Ack=4541 Win=485 Le
2301 22.494172334 10.                Ack=1076741 Win=5032 L
2302 22.494283486 10.                k=4551 Win=485 Len=0 T
```

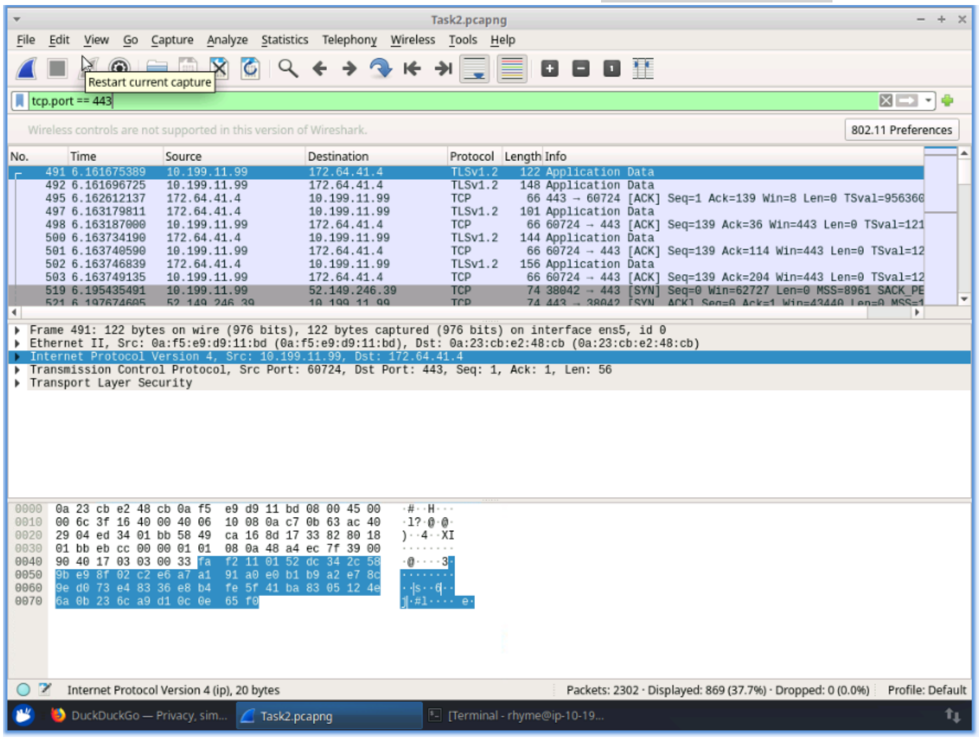
```
Frame 1: 4770 bytes on
Ethernet II, Src: 0a:f5
Internet Protocol Versi
Transmission Control Pr
Data (4704 bytes)
```

```
0000  0a 23 cb e2 48 cb 0
0010  12 94 f7 b5 40 00 4
0020  dd 8f 8d 6a 83 dc 6e a8  e1 44 7a 64 e3 c5 80 18   ···j··n·
0030  01 e5 11 07 00 00 01 01  08 0a af d2 47 98 36 fd   ········
0040  ba d1 00 00 00 1b 00 00  00 32 00 20 00 19 00 00   ·········2·
0050  00 10 00 00 01 ff 34 9d  3f 6c d3 40 14 87 13 5f   ······4· ?
0060  ed 5c 2f b6 e3 aa bd b4  40 5a d1 94 d0 16 28 6a   ·\/·····
0070  5a 04 69 08 a1 a4 04 28  ff 44 3b 76 65 64 64 ec   Z·i····(
0080  c2 80 50 86 8e 1d 11 b2  90 3a ba 27 21 5d 86 4a   ··P·····
0090  ee 50 c9 0c 0c 46 62 08  5b 3a 44 4a 86 0e 1e 18   ·P···Fb·
00a0  3c 74 30 f7 ce f6 f4 f4  be f1 ee 49 77 cb ef 7d   <t0·····
00b0  7f c4 8b 16 ab 2d dc 33  cf ff e5 c7 92 ab 44 d9   ·······3
00c0  0b aa eb 9e 4c 4c 7a 90  4f 3e 75 21 b6 f9 b7 27   ····LLz· O>u!
```

wireshark_ens5O9S0A2.pcapng   Packets: 2302 · Displayed: 2302 (100.0%)   Profile: Default

Use a display filter to detect HTTPS packets and find the duckduckgo.com IP address

In Wireshark, to display certain packets I can use a display filter, so to display only HTTPS traffic, I opened the file with the captured packets and used a filter on TCP port 443: *tcp.port == 443*



Task2.pcapng

Filter: tcp.port == 443

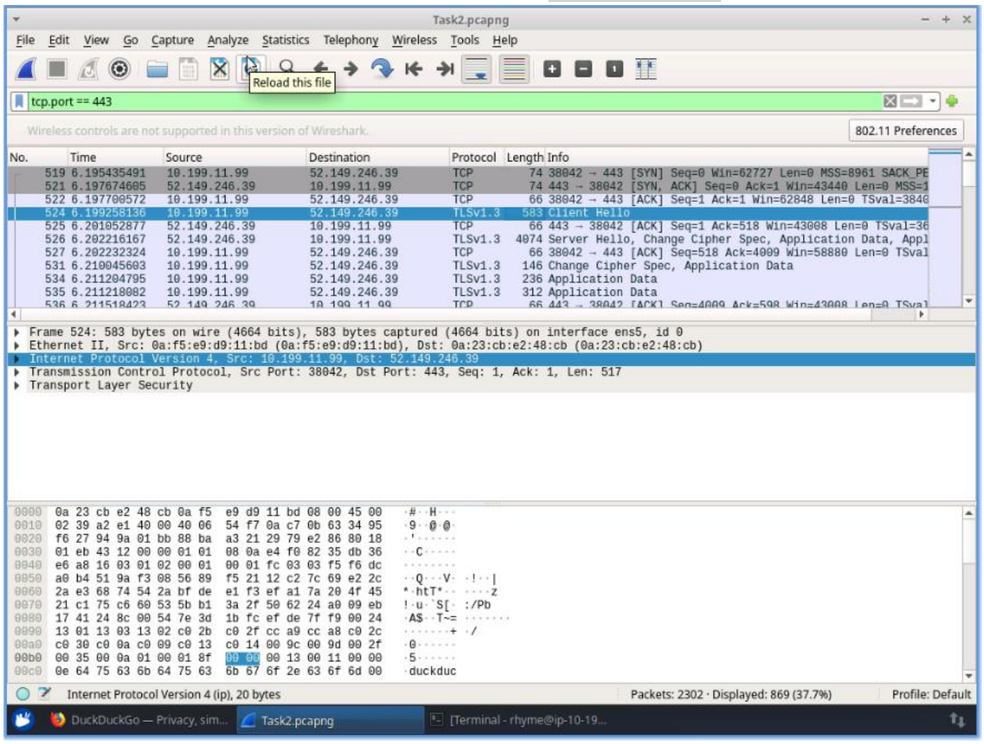
```
No.   Time         Source          Destination     Protocol Length Info
  491 6.161675389  10.199.11.99    172.64.41.4     TLSv1.2   122 Application Data
  492 6.161696725  10.199.11.99    172.64.41.4     TLSv1.2   148 Application Data
  495 6.162612137  172.64.41.4     10.199.11.99    TCP        66 443 → 60724 [ACK] Seq=1 Ack=139 Win=8 Len=0 TSval=956360
  497 6.163179811  172.64.41.4     10.199.11.99    TLSv1.2   101 Application Data
  498 6.163187000  10.199.11.99    172.64.41.4     TCP        66 60724 → 443 [ACK] Seq=139 Ack=36 Win=443 Len=0 TSval=121
  500 6.163734190  172.64.41.4     10.199.11.99    TLSv1.2   144 Application Data
  501 6.163740590  10.199.11.99    172.64.41.4     TCP        66 60724 → 443 [ACK] Seq=139 Ack=114 Win=443 Len=0 TSval=12
  502 6.163746839  172.64.41.4     10.199.11.99    TLSv1.2   156 Application Data
  503 6.163749135  10.199.11.99    172.64.41.4     TCP        66 60724 → 443 [ACK] Seq=139 Ack=204 Win=443 Len=0 TSval=12
  519 6.195435491  10.199.11.99    52.149.246.39   TCP        74 38042 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PE
  521 6.197674605  52.149.246.39   10.199.11.99    TCP        74 443 → 38042 [SYN, ACK] Seq=0 Ack=1 Win=43440 Len=0 MSS=1
```

```
Frame 491: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface ens5, id 0
Ethernet II, Src: 0a:f5:e9:d9:11:bd (0a:f5:e9:d9:11:bd), Dst: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb)
Internet Protocol Version 4, Src: 10.199.11.99, Dst: 172.64.41.4
Transmission Control Protocol, Src Port: 60724, Dst Port: 443, Seq: 1, Ack: 1, Len: 56
Transport Layer Security
```

```
0000  0a 23 cb e2 48 cb 0a f5  e9 d9 11 bd 08 00 45 00   ·#··H···
0010  00 6c 3f 16 40 00 40 06  10 08 0a c7 0b 63 ac 40   ·l?·@·@·
0020  29 04 ed 34 01 bb 58 49  ca 16 8d 17 33 82 80 18   )··4··XI
0030  01 bb eb cc 00 00 01 01  08 0a 48 a4 ec 7f 39 00   ········
0040  90 40 17 03 03 00 33 fa  f2 11 01 52 dc 34 2c 58   ·@····3·
0050  9b e9 8f 02 c2 e6 a7 a1  91 a0 e0 b1 b9 a2 e7 8c   ········
0060  9e d0 73 e4 83 36 e8 b4  fe 5f 41 ba 83 05 12 4e   ··s··6··
0070  6a 0b 23 6c a9 d1 0c 0e  65 f0                     j·#l···· e·
```

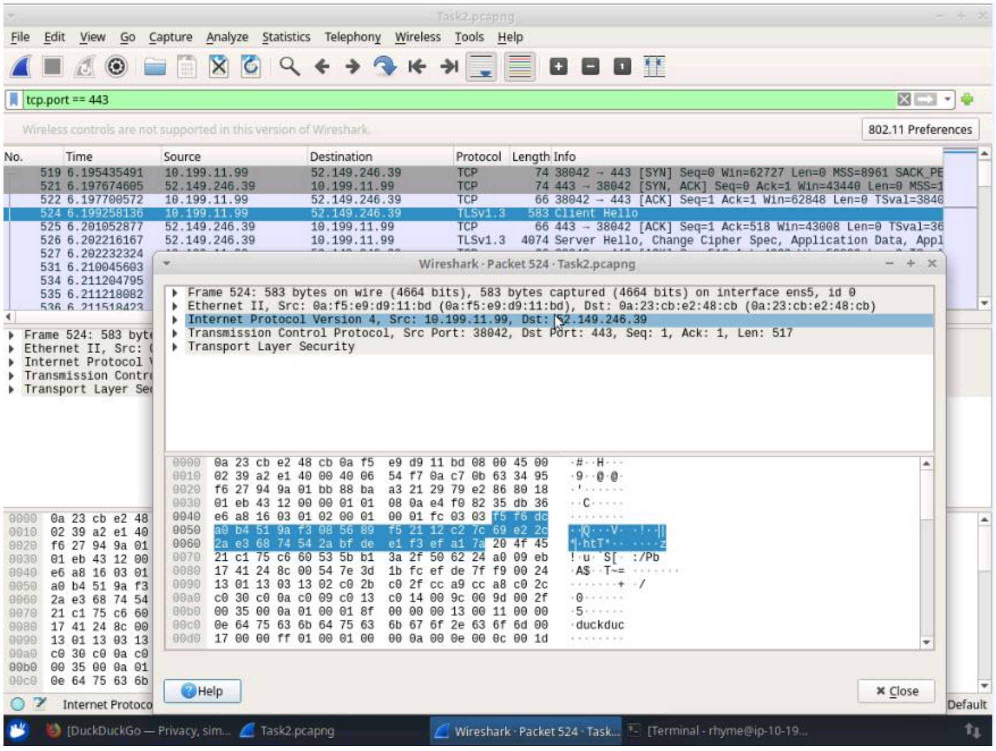
Internet Protocol Version 4 (ip), 20 bytes   Packets: 2302 · Displayed: 869 (37.7%) · Dropped: 0 (0.0%)   Profile: Default

To find the *duckduckgo.com* IP address I searched the HTTPS traffic for a TLS handshake protocol where it says “*Client Hello*” in the information.


Task2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Reload this file
802.11 Preferences

```
tcp.port == 443

Wireless controls are not supported in this version of Wireshark.

No.   Time          Source          Destination     Protocol Length Info
  519 6.195435491   10.199.11.99    52.149.246.39   TCP         74 38042 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PE
  521 6.197674605   52.149.246.39   10.199.11.99    TCP         74 443 → 38042 [SYN, ACK] Seq=0 Ack=1 Win=43440 Len=0 MSS=1
  522 6.197700572   10.199.11.99    52.149.246.39   TCP         66 38042 → 443 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=3840
  524 6.199258136   10.199.11.99    52.149.246.39   TLSv1.3    583 Client Hello
  525 6.201052877   52.149.246.39   10.199.11.99    TCP         66 443 → 38042 [ACK] Seq=1 Ack=518 Win=43008 Len=0 TSval=36
  526 6.202216167   52.149.246.39   10.199.11.99    TLSv1.3   4074 Server Hello, Change Cipher Spec, Application Data, Appl
  527 6.202232324   10.199.11.99    52.149.246.39   TCP         66 38042 → 443 [ACK] Seq=518 Ack=4009 Win=58880 Len=0 TSval
  531 6.210045603   10.199.11.99    52.149.246.39   TLSv1.3    146 Change Cipher Spec, Application Data
  534 6.211204795   10.199.11.99    52.149.246.39   TLSv1.3    236 Application Data
  535 6.211218082   10.199.11.99    52.149.246.39   TLSv1.3    312 Application Data
  536 6.211518423   52.149.246.39   10.199.11.99    TCP         66 443 → 38042 [ACK] Seq=4009 Ack=598 Win=43008 Len=0 TSval

▸ Frame 524: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface ens5, id 0
▸ Ethernet II, Src: 0a:f5:e9:d9:11:bd (0a:f5:e9:d9:11:bd), Dst: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb)
▸ Internet Protocol Version 4, Src: 10.199.11.99, Dst: 52.149.246.39
▸ Transmission Control Protocol, Src Port: 38042, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
▸ Transport Layer Security

0000  0a 23 cb e2 48 cb 0a f5  e9 d9 11 bd 08 00 45 00   ·#··H···
0010  02 39 a2 e1 40 00 40 06  54 f7 0a c7 0b 63 34 95   ·9··@·@·
0020  f6 27 94 9a 01 bb 88 ba  a3 21 29 79 e2 86 80 18   ·'······
0030  01 eb 43 12 00 00 01 01  08 0a e4 f0 82 35 db 36   ··C·····
0040  e6 a8 16 03 01 02 00 01  00 01 fc 03 03 f5 f6 dc   ········
0050  a0 b4 51 9a f3 08 56 89  f5 21 12 c2 7c 69 e2 2c   ··Q···V· ·!··|
0060  2a e3 68 74 54 2a bf de  e1 f3 ef a1 7a 20 4f 45   *·htT*·· ····z
0070  21 c1 75 c6 60 53 5b b1  3a 2f 50 62 24 a0 09 eb   !·u·`S[· :/Pb
0080  17 41 24 8c 00 54 7e 3d  1b fc ef de 7f f9 00 24   ·A$··T~= ········
0090  13 01 13 03 13 02 c0 2b  c0 2f cc a9 cc a8 c0 2c   ·······+ ·/
00a0  c0 30 c0 0a c0 09 c0 13  c0 14 00 9c 00 9d 00 2f   ·0······
00b0  00 35 00 0a 01 00 01 8f  00 00 00 13 00 11 00 00   ·5······
00c0  0e 64 75 63 6b 64 75 63  6b 67 6f 2e 63 6f 6d 00   ·duckduc

Internet Protocol Version 4 (ip), 20 bytes        Packets: 2302 · Displayed: 869 (37.7%)        Profile: Default
```

And then the destination is the *duckduckgo.com* IP address.


Task2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
802.11 Preferences
Help
Close
Default

```
tcp.port == 443

Wireless controls are not supported in this version of Wireshark.

No.   Time          Source          Destination     Protocol Length Info
  519 6.195435491   10.199.11.99    52.149.246.39   TCP         74 38042 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PE
  521 6.197674605   52.149.246.39   10.199.11.99    TCP         74 443 → 38042 [SYN, ACK] Seq=0 Ack=1 Win=43440 Len=0 MSS=1
  522 6.197700572   10.199.11.99    52.149.246.39   TCP         66 38042 → 443 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=3840
  524 6.199258136   10.199.11.99    52.149.246.39   TLSv1.3    583 Client Hello
  525 6.201052877   52.149.246.39   10.199.11.99    TCP         66 443 → 38042 [ACK] Seq=1 Ack=518 Win=43008 Len=0 TSval=36
  526 6.202216167   52.149.246.39   10.199.11.99    TLSv1.3   4074 Server Hello, Change Cipher Spec, Application Data, Appl
  527 6.202232324
  531 6.210045603
  534 6.211204795
  535 6.211218082
  536 6.211518423
```

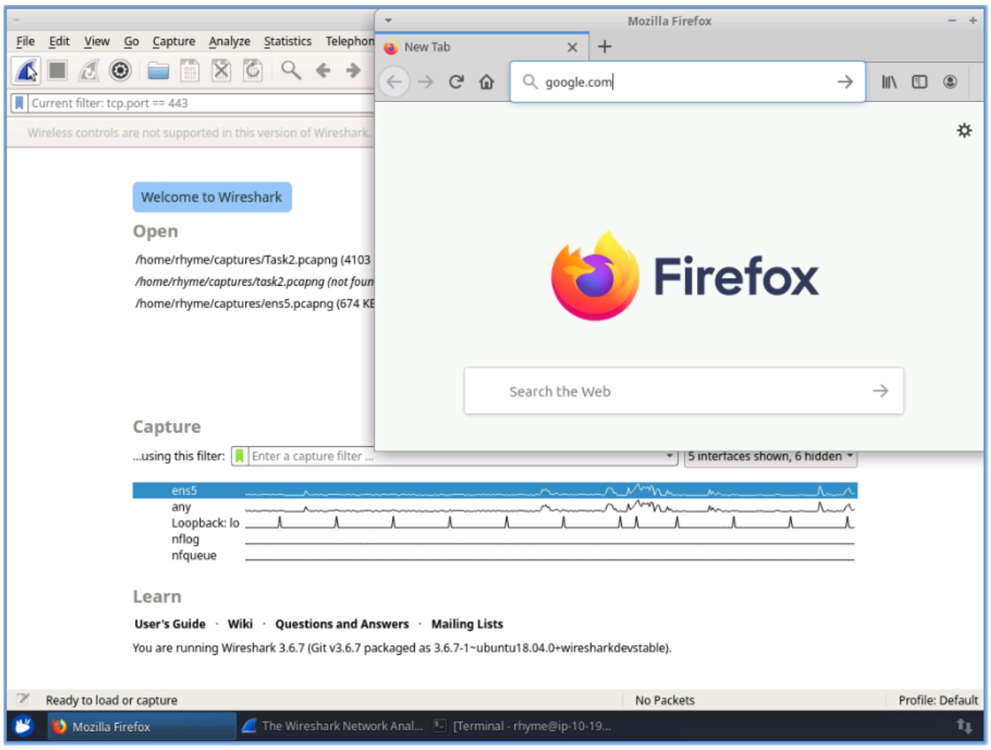
Wireshark · Packet 524 · Task2.pcapng

```
▸ Frame 524: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface ens5, id 0
▸ Ethernet II, Src: 0a:f5:e9:d9:11:bd (0a:f5:e9:d9:11:bd), Dst: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb)
▸ Internet Protocol Version 4, Src: 10.199.11.99, Dst: 52.149.246.39
▸ Transmission Control Protocol, Src Port: 38042, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
▸ Transport Layer Security

0000  0a 23 cb e2 48 cb 0a f5  e9 d9 11 bd 08 00 45 00   ·#··H···
0010  02 39 a2 e1 40 00 40 06  54 f7 0a c7 0b 63 34 95   ·9··@·@·
0020  f6 27 94 9a 01 bb 88 ba  a3 21 29 79 e2 86 80 18   ·'······
0030  01 eb 43 12 00 00 01 01  08 0a e4 f0 82 35 db 36   ··C·····
0040  e6 a8 16 03 01 02 00 01  00 01 fc 03 03 f5 f6 dc   ········
0050  a0 b4 51 9a f3 08 56 89  f5 21 12 c2 7c 69 e2 2c   ··Q···V· ·!··|
0060  2a e3 68 74 54 2a bf de  e1 f3 ef a1 7a 20 4f 45   *·htT*·· ····z
0070  21 c1 75 c6 60 53 5b b1  3a 2f 50 62 24 a0 09 eb   !·u·`S[· :/Pb
0080  17 41 24 8c 00 54 7e 3d  1b fc ef de 7f f9 00 24   ·A$··T~= ········
0090  13 01 13 03 13 02 c0 2b  c0 2f cc a9 cc a8 c0 2c   ·······+ ·/
00a0  c0 30 c0 0a c0 09 c0 13  c0 14 00 9c 00 9d 00 2f   ·0······
00b0  00 35 00 0a 01 00 01 8f  00 00 00 13 00 11 00 00   ·5······
00c0  0e 64 75 63 6b 64 75 63  6b 67 6f 2e 63 6f 6d 00   ·duckduc
00d0  17 00 00 ff 01 00 01 00  00 0a 00 0e 00 0c 00 1d   ········
```

[DuckDuckGo — Privacy, sim...
Task2.pcapng
Wireshark · Packet 524 · Task...
[Terminal - rhyme@ip-10-19...

Find the IP address of *google.com* more easily and get some packet information about that connection

To capture packets when connecting to the *google.com* website, I followed the same process as before, so before I started capturing packets, I opened my browser and searched for *google.com*


File Edit View Go Capture Analyze Statistics Telephon
Mozilla Firefox
New Tab
google.com
Welcome to Wireshark
Open
Capture
Learn
Firefox
Search the Web
Mozilla Firefox
The Wireshark Network Anal...
[Terminal - rhyme@ip-10-19...

Current filter: tcp.port == 443

Wireless controls are not supported in this version of Wireshark.

/home/rhyme/captures/Task2.pcapng (4103
/home/rhyme/captures/task2.pcapng (not foun
/home/rhyme/captures/ens5.pcapng (674 KE

...using this filter: Enter a capture filter ... 5 interfaces shown, 6 hidden

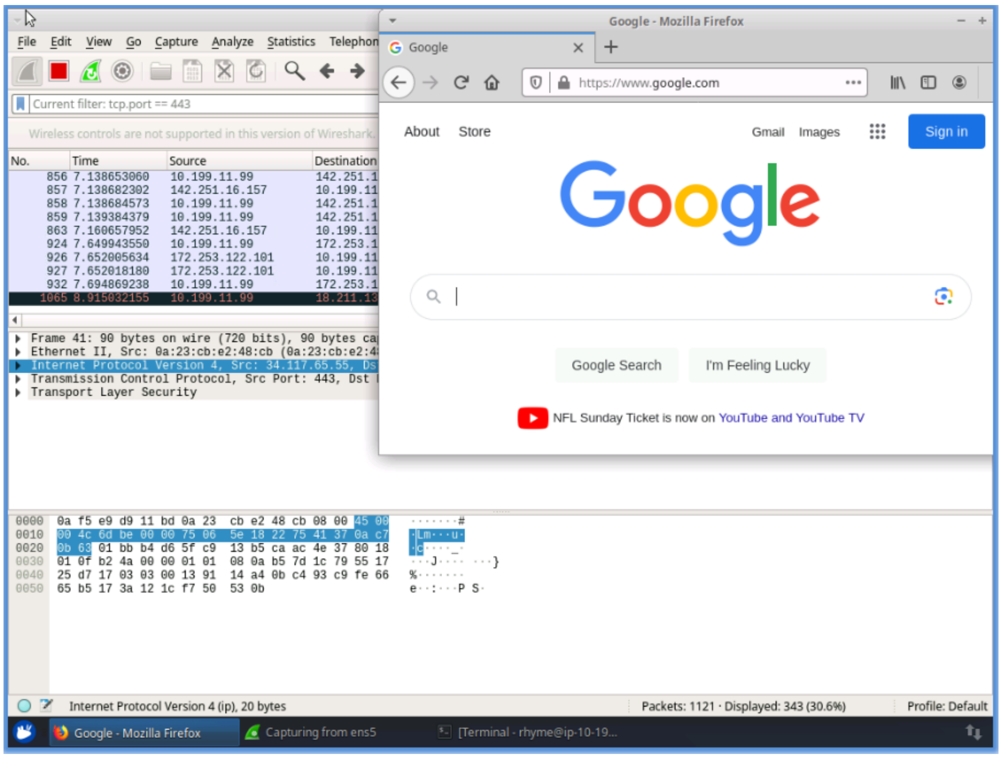
ens5
any
Loopback: lo
nflog
nfqueue

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.6.7 (Git v3.6.7 packaged as 3.6.7-1~ubuntu18.04.0+wiresharkdevstable).

Ready to load or capture | No Packets | Profile: Default

Then I started capturing packets and immediately hit enter in the browser, finally I stopped and saved the file.



Current filter: tcp.port == 443

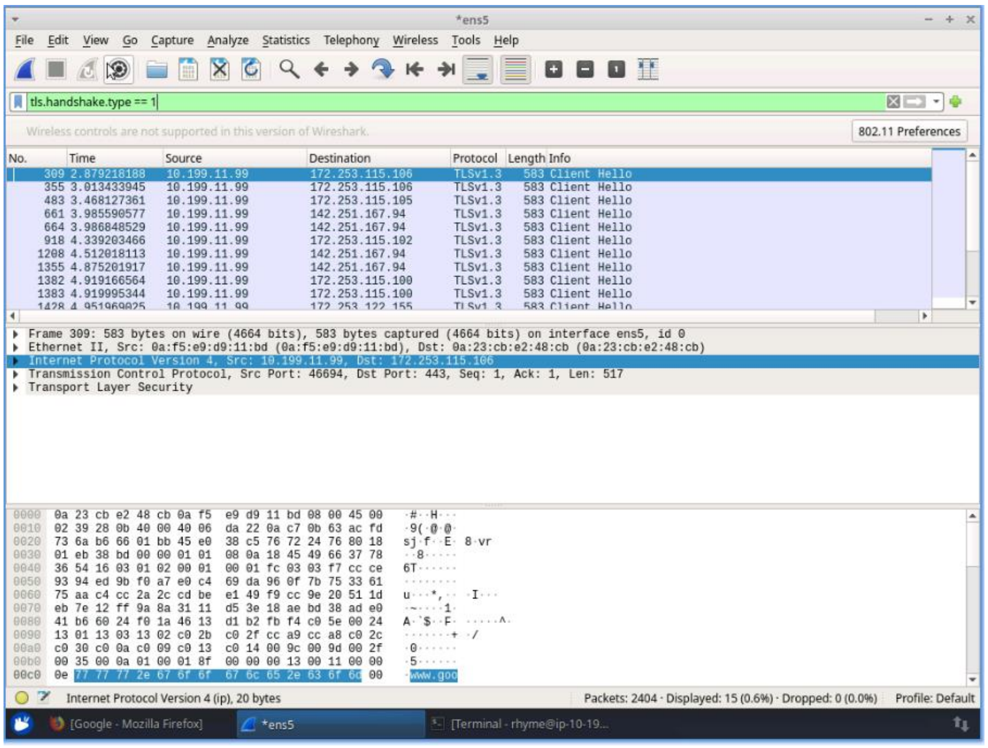
Wireless controls are not supported in this version of Wireshark.

```
No.  Time         Source          Destination
 856 7.138653060  10.199.11.99    142.251.1
 857 7.138682302  142.251.16.157  10.199.11
 858 7.138684573  10.199.11.99    142.251.1
 859 7.139384379  10.199.11.99    142.251.1
 863 7.160657952  142.251.16.157  10.199.11
 924 7.649943550  10.199.11.99    172.253.1
 926 7.652005634  172.253.122.101 10.199.11
 927 7.652018180  172.253.122.101 10.199.11
 932 7.694869238  10.199.11.99    172.253.1
1065 8.915032155  10.199.11.99    18.211.13

▸ Frame 41: 90 bytes on wire (720 bits), 90 bytes ca
▸ Ethernet II, Src: 0a:23:cb:e2:48:cb (0a:23:cb:e2:4
▸ Internet Protocol Version 4, Src: 34.117.65.55, Ds
▸ Transmission Control Protocol, Src Port: 443, Dst
▸ Transport Layer Security

0000  0a f5 e9 d9 11 bd 0a 23  cb e2 48 cb 08 00 45 00   ·······#
0010  00 4c 6d be 00 00 75 06  5e 18 22 75 41 37 0a c7   ·Lm···u·
0020  0b 63 01 bb b4 d6 5f c9  13 b5 ca ac 4e 37 80 18   ·c····_·
0030  01 0f b2 4a 00 00 01 01  08 0a b5 7d 1c 79 55 17   ···J····  ···}
0040  25 d7 17 03 03 00 13 91  14 a4 0b c4 93 c9 fe 66   %·······
0050  65 b5 17 3a 12 1c f7 50  53 0b                     e··:···P S·
```

NFL Sunday Ticket is now on YouTube and YouTube TV

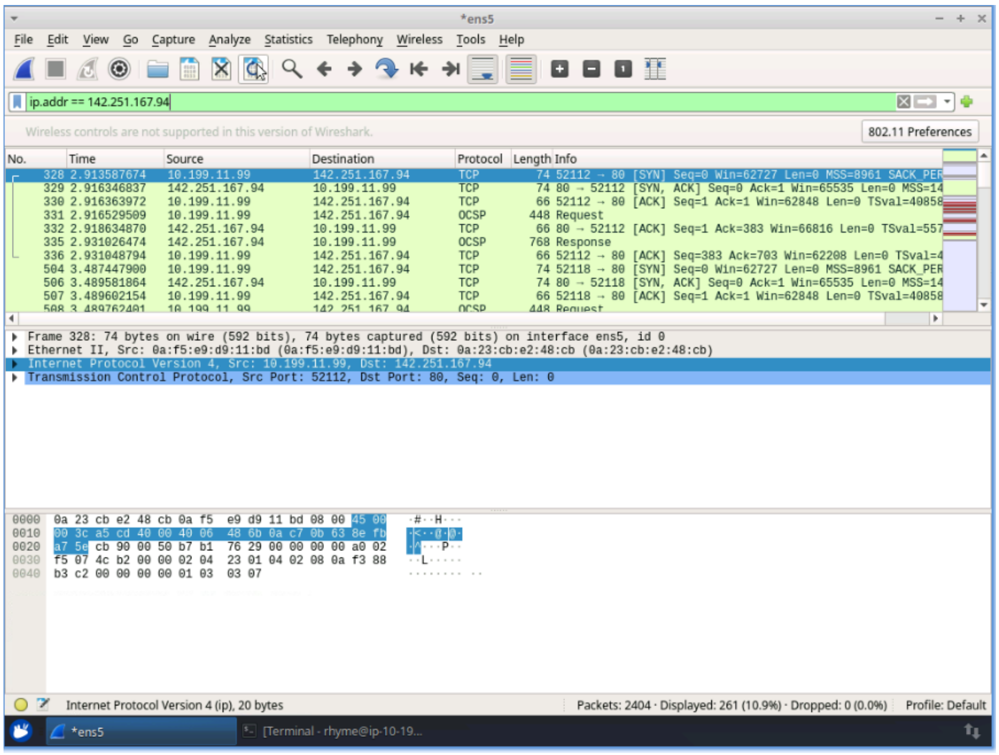
Internet Protocol Version 4 (ip), 20 bytes | Packets: 1121 · Displayed: 343 (30.6%) | Profile: Default

Now a TLS handshake display filter may be used to detect a website IP address more easily: *tls.handshake.type == 1*


*ens5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireless controls are not supported in this version of Wireshark.
802.11 Preferences
[Google - Mozilla Firefox]
*ens5
[Terminal - rhyme@ip-10-19...

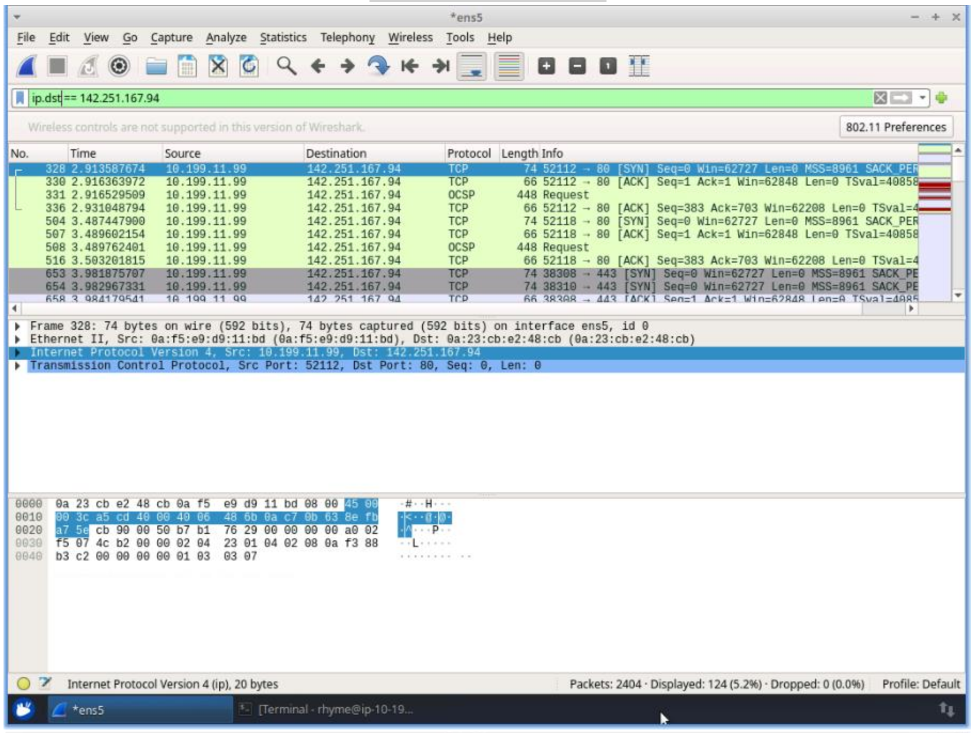
```
tls.handshake.type == 1

No.   Time          Source          Destination       Protocol  Length Info
  309 2.879218188   10.199.11.99    172.253.115.106   TLSv1.3   583 Client Hello
  355 3.013433945   10.199.11.99    172.253.115.106   TLSv1.3   583 Client Hello
  483 3.468127361   10.199.11.99    172.253.115.105   TLSv1.3   583 Client Hello
  661 3.985590577   10.199.11.99    142.251.167.94    TLSv1.3   583 Client Hello
  664 3.986848529   10.199.11.99    142.251.167.94    TLSv1.3   583 Client Hello
  918 4.339203466   10.199.11.99    172.253.115.102   TLSv1.3   583 Client Hello
 1208 4.512018113   10.199.11.99    142.251.167.94    TLSv1.3   583 Client Hello
 1355 4.875201917   10.199.11.99    142.251.167.94    TLSv1.3   583 Client Hello
 1382 4.919166564   10.199.11.99    172.253.115.100   TLSv1.3   583 Client Hello
 1383 4.919995344   10.199.11.99    172.253.115.100   TLSv1.3   583 Client Hello
 1428 4.951969025   10.199.11.99    172.253.122.155   TLSv1.3   583 Client Hello

▸ Frame 309: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface ens5, id 0
▸ Ethernet II, Src: 0a:f5:e9:d9:11:bd (0a:f5:e9:d9:11:bd), Dst: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb)
▸ Internet Protocol Version 4, Src: 10.199.11.99, Dst: 172.253.115.106
▸ Transmission Control Protocol, Src Port: 46694, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
▸ Transport Layer Security

0000  0a 23 cb e2 48 cb 0a f5  e9 d9 11 bd 08 00 45 00   ·#··H···
0010  02 39 28 0b 40 00 40 06  da 22 0a c7 0b 63 ac fd   ·9(·@·@·
0020  73 6a b6 66 01 bb 45 e0  38 c5 76 72 24 76 80 18   sj·f··E· 8·vr
0030  01 eb 38 bd 00 00 01 01  08 0a 18 45 49 66 37 78   ··8·····
0040  36 54 16 03 01 02 00 01  00 01 fc 03 03 f7 cc ce   6T······
0050  93 94 ed 9b f0 a7 e0 c4  69 da 96 0f 7b 75 33 61   ········
0060  75 aa c4 cc 2a 2c cd be  e1 49 f9 cc 9e 20 51 1d   u···*,·· ·I···
0070  eb 7e 12 ff 9a 8a 31 11  d5 3e 18 ae bd 38 ad e0   ·~····1·
0080  41 b6 60 24 f0 1a 46 13  d1 b2 fb f4 c0 5e 00 24   A·`$··F· ·····^·
0090  13 01 13 03 13 02 c0 2b  c0 2f cc a9 cc a8 c0 2c   ·······+ ·/
00a0  c0 30 c0 0a c0 09 c0 13  c0 14 00 9c 00 9d 00 2f   ·0······
00b0  00 35 00 0a 01 00 01 8f  00 00 00 13 00 11 00 00   ·5······
00c0  0e 77 77 77 2e 67 6f 6f  67 6c 65 2e 63 6f 6d 00   ·www.goo

Internet Protocol Version 4 (ip), 20 bytes     Packets: 2404 · Displayed: 15 (0.6%) · Dropped: 0 (0.0%)   Profile: Default
```

Since now Wireshark only displays the first step of the TLS handshake protocol it´s easy to see the *google.com* IP address in the destination. After I knew the *google.com* IP address I was able to use a filter to obtain all packet information for that website: *ip.addr == 142.251.167.94*

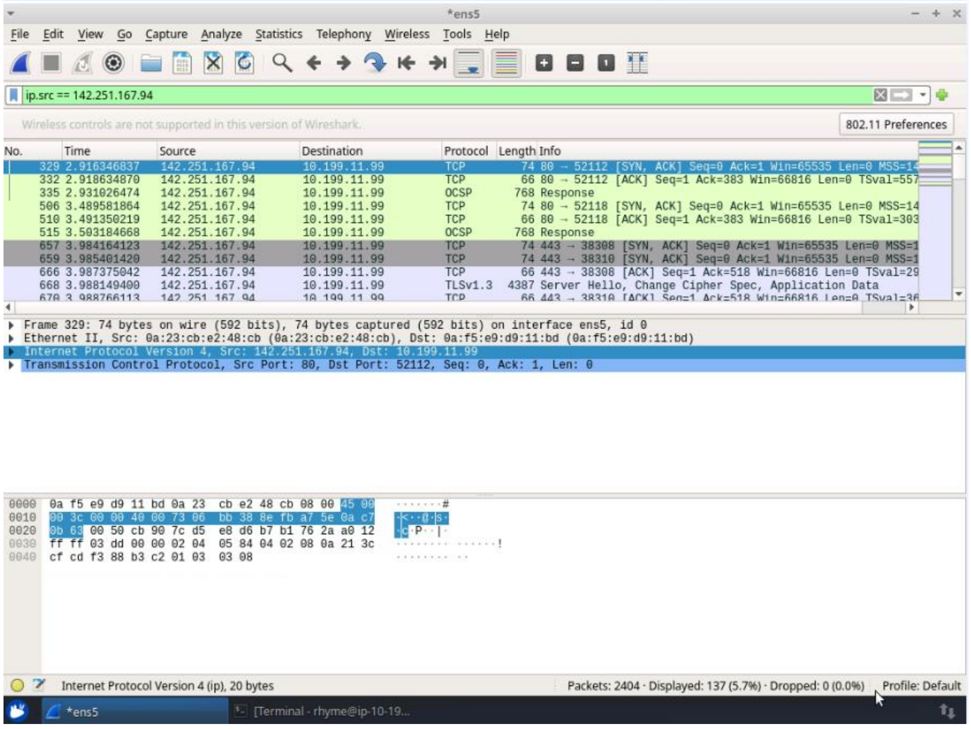

*ens5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireless controls are not supported in this version of Wireshark.
802.11 Preferences
*ens5
[Terminal - rhyme@ip-10-19...

```
ip.addr == 142.251.167.94

No.   Time          Source          Destination       Protocol  Length Info
  328 2.913587674   10.199.11.99    142.251.167.94    TCP        74 52112 → 80 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PER
  329 2.916346837   142.251.167.94  10.199.11.99      TCP        74 80 → 52112 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=14
  330 2.916363972   10.199.11.99    142.251.167.94    TCP        66 52112 → 80 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=40858
  331 2.916529509   10.199.11.99    142.251.167.94    OCSP      448 Request
  332 2.918634870   142.251.167.94  10.199.11.99      TCP        66 80 → 52112 [ACK] Seq=1 Ack=383 Win=66816 Len=0 TSval=557
  335 2.931026474   142.251.167.94  10.199.11.99      OCSP      768 Response
  336 2.931048794   10.199.11.99    142.251.167.94    TCP        66 52112 → 80 [ACK] Seq=383 Ack=703 Win=62208 Len=0 TSval=4
  504 3.487447900   10.199.11.99    142.251.167.94    TCP        74 52118 → 80 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PER
  506 3.489581864   142.251.167.94  10.199.11.99      TCP        74 80 → 52118 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=14
  507 3.489602154   10.199.11.99    142.251.167.94    TCP        66 52118 → 80 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=40858
  508 3.489762401   10.199.11.99    142.251.167.94    OCSP      448 Request

▸ Frame 328: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface ens5, id 0
▸ Ethernet II, Src: 0a:f5:e9:d9:11:bd (0a:f5:e9:d9:11:bd), Dst: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb)
▸ Internet Protocol Version 4, Src: 10.199.11.99, Dst: 142.251.167.94
▸ Transmission Control Protocol, Src Port: 52112, Dst Port: 80, Seq: 0, Len: 0

0000  0a 23 cb e2 48 cb 0a f5  e9 d9 11 bd 08 00 45 00   ·#··H···
0010  00 3c a5 cd 40 00 40 06  48 6b 0a c7 0b 63 8e fb   ·<··@·@·
0020  a7 5e cb 90 00 50 b7 b1  76 29 00 00 00 00 a0 02   ·^···P··
0030  f5 07 4c b2 00 00 02 04  23 01 04 02 08 0a f3 88   ··L·····
0040  b3 c2 00 00 00 00 01 03  03 07                     ········ ··

Internet Protocol Version 4 (ip), 20 bytes     Packets: 2404 · Displayed: 261 (10.9%) · Dropped: 0 (0.0%)   Profile: Default
```

But I can also use a filter to obtain only the packet information sent to *google.com* or sent by *google.com*: *ip.dst == 142.251.167.94* or *ip.src == 142.251.167.94*



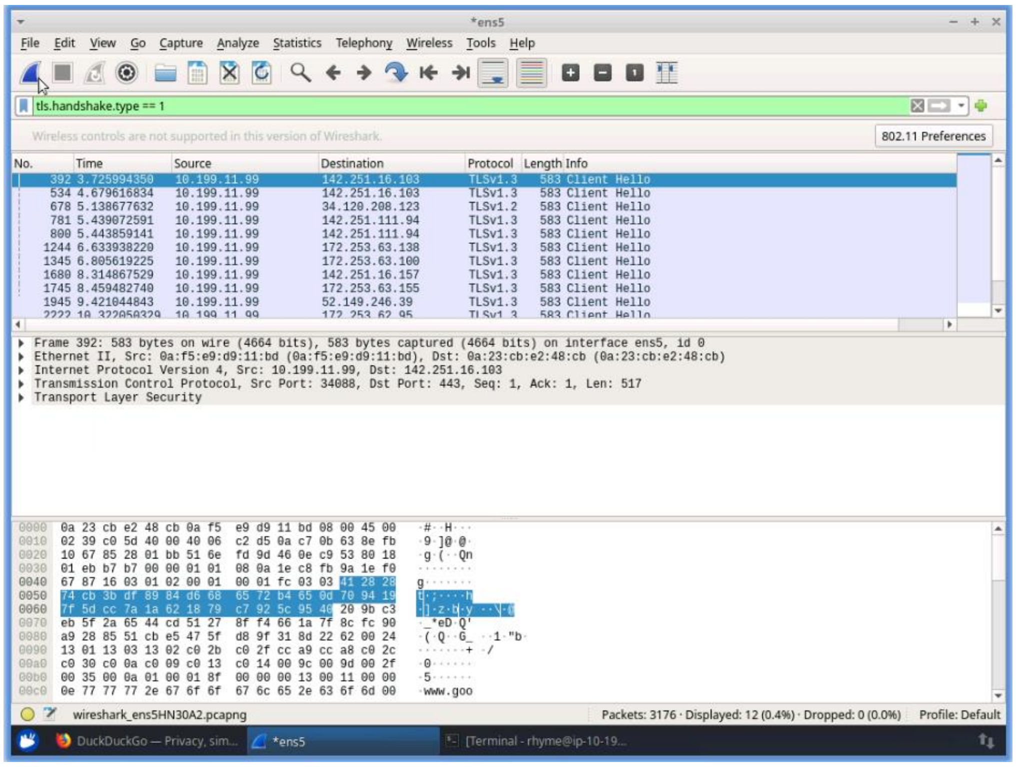
```
ip.dst == 142.251.167.94

No.  Time         Source        Destination     Protocol Length Info
328 2.913587674  10.199.11.99  142.251.167.94  TCP       74 52112 → 80 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PER
330 2.916363972  10.199.11.99  142.251.167.94  TCP       66 52112 → 80 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=40858
331 2.916529509  10.199.11.99  142.251.167.94  OCSP     448 Request
336 2.931048794  10.199.11.99  142.251.167.94  TCP       66 52112 → 80 [ACK] Seq=383 Ack=703 Win=62208 Len=0 TSval=4
504 3.487447900  10.199.11.99  142.251.167.94  TCP       74 52118 → 80 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PER
507 3.489602154  10.199.11.99  142.251.167.94  TCP       66 52118 → 80 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=40858
508 3.489762401  10.199.11.99  142.251.167.94  OCSP     448 Request
516 3.503201815  10.199.11.99  142.251.167.94  TCP       66 52118 → 80 [ACK] Seq=383 Ack=703 Win=62208 Len=0 TSval=4
653 3.981875707  10.199.11.99  142.251.167.94  TCP       74 38308 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PE
654 3.982967331  10.199.11.99  142.251.167.94  TCP       74 38310 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PE
658 3.984179541  10.199.11.99  142.251.167.94  TCP       66 38308 → 443 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=4085

Frame 328: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface ens5, id 0
Ethernet II, Src: 0a:f5:e9:d9:11:bd (0a:f5:e9:d9:11:bd), Dst: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb)
Internet Protocol Version 4, Src: 10.199.11.99, Dst: 142.251.167.94
Transmission Control Protocol, Src Port: 52112, Dst Port: 80, Seq: 0, Len: 0

0000  0a 23 cb e2 48 cb 0a f5  e9 d9 11 bd 08 00 45 00   ·#··H···
0010  00 3c a5 cd 40 00 40 06  48 6b 0a c7 0b 63 8e fb   ·<··@·@·
0020  a7 5e cb 90 00 50 b7 b1  76 29 00 00 00 00 a0 02   ·^···P··
0030  f5 07 4c b2 00 00 02 04  23 01 04 02 08 0a f3 88   ··L·····
0040  b3 c2 00 00 00 00 01 03  03 07                     ········ ··

Internet Protocol Version 4 (ip), 20 bytes    Packets: 2404 · Displayed: 124 (5.2%) · Dropped: 0 (0.0%)    Profile: Default
```



```
ip.src == 142.251.167.94

No.  Time         Source          Destination   Protocol Length Info
329 2.916346837  142.251.167.94  10.199.11.99  TCP       74 80 → 52112 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=14
332 2.918634870  142.251.167.94  10.199.11.99  TCP       66 80 → 52112 [ACK] Seq=1 Ack=383 Win=66816 Len=0 TSval=557
335 2.931026474  142.251.167.94  10.199.11.99  OCSP     768 Response
506 3.489581864  142.251.167.94  10.199.11.99  TCP       74 80 → 52118 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=14
510 3.491350219  142.251.167.94  10.199.11.99  TCP       66 80 → 52118 [ACK] Seq=1 Ack=383 Win=66816 Len=0 TSval=303
515 3.503184668  142.251.167.94  10.199.11.99  OCSP     768 Response
657 3.984164123  142.251.167.94  10.199.11.99  TCP       74 443 → 38308 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1
659 3.985401420  142.251.167.94  10.199.11.99  TCP       74 443 → 38310 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1
666 3.987375042  142.251.167.94  10.199.11.99  TCP       66 443 → 38308 [ACK] Seq=1 Ack=518 Win=66816 Len=0 TSval=29
668 3.988149400  142.251.167.94  10.199.11.99  TLSv1.3 4387 Server Hello, Change Cipher Spec, Application Data
670 3.988766113  142.251.167.94  10.199.11.99  TCP       66 443 → 38310 [ACK] Seq=1 Ack=518 Win=66816 Len=0 TSval=36

Frame 329: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface ens5, id 0
Ethernet II, Src: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb), Dst: 0a:f5:e9:d9:11:bd (0a:f5:e9:d9:11:bd)
Internet Protocol Version 4, Src: 142.251.167.94, Dst: 10.199.11.99
Transmission Control Protocol, Src Port: 80, Dst Port: 52112, Seq: 0, Ack: 1, Len: 0

0000  0a f5 e9 d9 11 bd 0a 23  cb e2 48 cb 08 00 45 00   ·······#
0010  00 3c 00 00 40 00 73 06  bb 38 8e fb a7 5e 0a c7   ·<··@·s·
0020  0b 63 00 50 cb 90 7c d5  e8 d6 b7 b1 76 2a a0 12   ·c·P··|·
0030  ff ff 03 dd 00 00 02 04  05 84 04 02 08 0a 21 3c   ········ ······!
0040  cf cd f3 88 b3 c2 01 03  03 08                     ········ ··

Internet Protocol Version 4 (ip), 20 bytes    Packets: 2404 · Displayed: 137 (5.7%) · Dropped: 0 (0.0%)    Profile: Default
```

Locate all HTTPS packets from a capture not containing a certain IP address

Now I need to capture packets for *duckduckgo.com* and *google.com* in the same file, I followed the same process as before and I stopped the capture after opening both websites, and saved the file. To check if all the IP addresses are in the file, I followed the same steps as before to see only the packets related to the first step of the TLS handshake protocol.



tls.handshake.type == 1

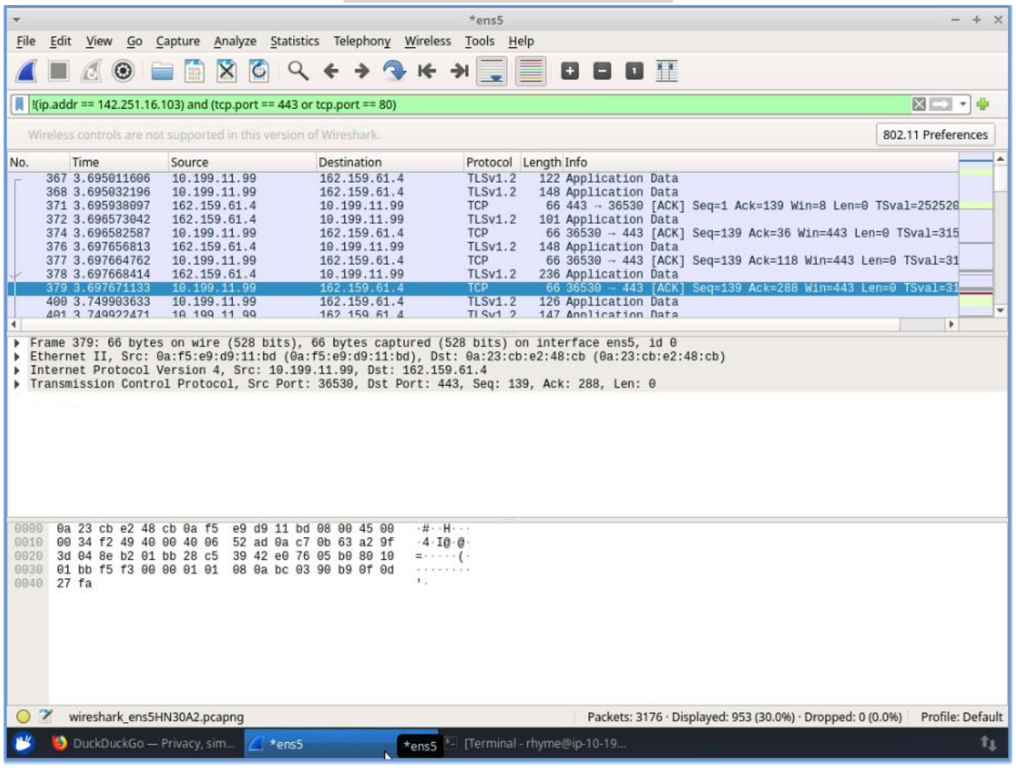
```
No.   Time          Source         Destination      Protocol  Length Info
  392 3.725994350   10.199.11.99   142.251.16.103   TLSv1.3    583 Client Hello
  534 4.679616834   10.199.11.99   142.251.16.103   TLSv1.3    583 Client Hello
  678 5.138677632   10.199.11.99   34.120.208.123   TLSv1.2    583 Client Hello
  781 5.439072591   10.199.11.99   142.251.111.94   TLSv1.3    583 Client Hello
  800 5.443859141   10.199.11.99   142.251.111.94   TLSv1.3    583 Client Hello
 1244 6.633938220   10.199.11.99   172.253.63.138   TLSv1.3    583 Client Hello
 1345 6.805619225   10.199.11.99   172.253.63.100   TLSv1.3    583 Client Hello
 1680 8.314867529   10.199.11.99   142.251.16.157   TLSv1.3    583 Client Hello
 1745 8.459482740   10.199.11.99   172.253.63.155   TLSv1.3    583 Client Hello
 1945 9.421044843   10.199.11.99   52.149.246.39    TLSv1.3    583 Client Hello
 2222 10.322050329  10.199.11.99   172.253.62.95    TLSv1.3    583 Client Hello
```

```
▸ Frame 392: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface ens5, id 0
▸ Ethernet II, Src: 0a:f5:e9:d9:11:bd (0a:f5:e9:d9:11:bd), Dst: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb)
▸ Internet Protocol Version 4, Src: 10.199.11.99, Dst: 142.251.16.103
▸ Transmission Control Protocol, Src Port: 34088, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
▸ Transport Layer Security
```

```
0000  0a 23 cb e2 48 cb 0a f5  e9 d9 11 bd 08 00 45 00   ·#··H···
0010  02 39 c0 5d 40 00 40 06  c2 d5 0a c7 0b 63 8e fb   ·9·]@·@·
0020  10 67 85 28 01 bb 51 6e  fd 9d 46 0e c9 53 80 18   ·g·(··Qn
0030  01 eb b7 b7 00 00 01 01  08 0a 1e c8 fb 9a 1e f0   ········
0040  67 87 16 03 01 02 00 01  00 01 fc 03 03 41 28 28   g·······
0050  74 cb 3b df 89 84 d6 68  65 72 b4 65 0d 70 94 19   t·;····h
0060  7f 5d cc 7a 1a 62 18 79  c7 92 5c 95 40 20 9b c3   ·]·z·b·y ··\·@
0070  eb 5f 2a 65 44 cd 51 27  8f f4 66 1a 7f 8c fc 90   ·_*eD·Q'
0080  a9 28 85 51 cb e5 47 5f  d8 9f 31 8d 22 62 00 24   ·(·Q··G_ ··1·"b·
0090  13 01 13 03 13 02 c0 2b  c0 2f cc a9 cc a8 c0 2c   ·······+ ·/
00a0  c0 30 c0 0a c0 09 c0 13  c0 14 00 9c 00 9d 00 2f   ·0······
00b0  00 35 00 0a 01 00 01 8f  00 00 00 13 00 11 00 00   ·5······
00c0  0e 77 77 77 2e 67 6f 6f  67 6c 65 2e 63 6f 6d 00   ·www.goo
```

wireshark_ens5HN30A2.pcapng   Packets: 3176 · Displayed: 12 (0.4%) · Dropped: 0 (0.0%)   Profile: Default

To display only HTTPS traffic and eliminate packets with a IP address I may use a conditional statement: *!(ip.addr == 142.251.16.103) and (tcp.port == 443 or tcp.port == 80)*



!(ip.addr == 142.251.16.103) and (tcp.port == 443 or tcp.port == 80)

```
No.  Time          Source         Destination    Protocol  Length Info
 367 3.695011606   10.199.11.99   162.159.61.4   TLSv1.2    122 Application Data
 368 3.695032196   10.199.11.99   162.159.61.4   TLSv1.2    148 Application Data
 371 3.695938097   162.159.61.4   10.199.11.99   TCP         66 443 → 36530 [ACK] Seq=1 Ack=139 Win=8 Len=0 TSval=252520
 372 3.696573042   162.159.61.4   10.199.11.99   TLSv1.2    101 Application Data
 374 3.696582587   10.199.11.99   162.159.61.4   TCP         66 36530 → 443 [ACK] Seq=139 Ack=36 Win=443 Len=0 TSval=315
 376 3.697656813   162.159.61.4   10.199.11.99   TLSv1.2    148 Application Data
 377 3.697664762   10.199.11.99   162.159.61.4   TCP         66 36530 → 443 [ACK] Seq=139 Ack=118 Win=443 Len=0 TSval=31
 378 3.697668414   162.159.61.4   10.199.11.99   TLSv1.2    236 Application Data
 379 3.697671133   10.199.11.99   162.159.61.4   TCP         66 36530 → 443 [ACK] Seq=139 Ack=288 Win=443 Len=0 TSval=31
 400 3.749903633   10.199.11.99   162.159.61.4   TLSv1.2    126 Application Data
 401 3.749922471   10.199.11.99   162.159.61.4   TLSv1.2    147 Application Data
```

```
▸ Frame 379: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface ens5, id 0
▸ Ethernet II, Src: 0a:f5:e9:d9:11:bd (0a:f5:e9:d9:11:bd), Dst: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb)
▸ Internet Protocol Version 4, Src: 10.199.11.99, Dst: 162.159.61.4
▸ Transmission Control Protocol, Src Port: 36530, Dst Port: 443, Seq: 139, Ack: 288, Len: 0
```

```
0000  0a 23 cb e2 48 cb 0a f5  e9 d9 11 bd 08 00 45 00   ·#··H···
0010  00 34 f2 49 40 00 40 06  52 ad 0a c7 0b 63 a2 9f   ·4·I@·@·
0020  3d 04 8e b2 01 bb 28 c5  39 42 e0 76 05 b0 80 10   =·····(·
0030  01 bb f5 f3 00 00 01 01  08 0a bc 03 90 b9 0f 0d   ········
0040  27 fa                                              '·
```

wireshark_ens5HN30A2.pcapng   Packets: 3176 · Displayed: 953 (30.0%) · Dropped: 0 (0.0%)   Profile: Default