

20MCA136-NETWORKING & ADMINISTRATION LAB

WIRESHARK INSTALLATION

SUBMITTED BY,

VIVIN V. ABRAHAM

R MCA-2020-S2

Wireshark Installation

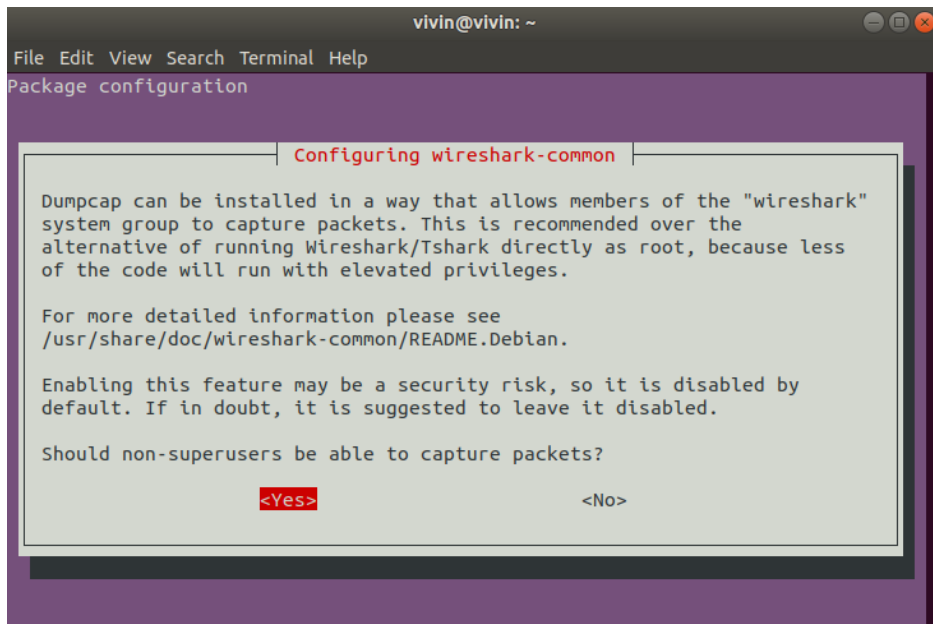
In terminal of ubuntu

sudo apt-get install wireshark

```
vivin@vivin:~$ sudo apt-get install wireshark
[sudo] password for vivin:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libc-ares2 libdouble-conversion1 libmaxminddb0 libnl-route-3-200
  libqgsttools-p1 libqt5core5a libqt5dbus5 libqt5gui5 libqt5multimedia5
  libqt5multimedia5-plugins libqt5multimediawidgets5 libqt5network5
  libqt5opengl5 libqt5sprintsupport5 libqt5svg5 libqt5widgets5 libsmi2ldbl
  libsnappy1v5 libspandsp2 libssh-gcrypt-4 libwireshark-data libwireshark11
  libwiretap8 libwscodec2 libwsutil9 libxcb-xinerama0 qt5-gtk-platformtheme
  qttranslations5-l10n wireshark-common wireshark-qt
Suggested packages:
  mmdns-bin qt5-image-formats-plugins qtwayland5 snmp-mibs-downloader
  wireshark-doc
The following NEW packages will be installed:
  libc-ares2 libdouble-conversion1 libmaxminddb0 libnl-route-3-200
  libqgsttools-p1 libqt5core5a libqt5dbus5 libqt5gui5 libqt5multimedia5
  libqt5multimedia5-plugins libqt5multimediawidgets5 libqt5network5
  libqt5opengl5 libqt5sprintsupport5 libqt5svg5 libqt5widgets5 libsmi2ldbl
  libsnappy1v5 libspandsp2 libssh-gcrypt-4 libwireshark-data libwireshark11
  libwiretap8 libwscodec2 libwsutil9 libxcb-xinerama0 qt5-gtk-platformtheme
  qttranslations5-l10n wireshark-common wireshark-qt
0 upgraded, 31 newly installed, 0 to remove and 0 not upgraded.
Need to get 30.2 MB of archives.
After this operation, 149 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 libdouble-conversion1 amd64 2.0.1-4ubuntu1 [128 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libqt5core5a amd64 5.9.5+dfsg-0ubuntu1 [128 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libqt5dbus5 amd64 5.9.5+dfsg-0ubuntu1 [128 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libqt5network5 amd64 5.9.5+dfsg-0ubuntu1 [128 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libxcb-xinerama0 amd64 1.13-2~ubuntu1 [128 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libqt5gui5 amd64 5.9.5+dfsg-0ubuntu1 [128 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libqt5widgets5 amd64 5.9.5+dfsg-0ubuntu1 [128 kB]
Get:8 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 libqt5svg5 amd64 5.9.5-0ubuntu1 [128 kB]
Get:9 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libmaxminddb0 amd64 1.3.1-1 [25.6 kB]
Get:10 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 libnl-route-3-200 amd64 3.2.29-0ubuntu1 [128 kB]
Get:11 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libqt5multimedia5 amd64 5.9.5-0ubuntu1 [128 kB]
Get:12 http://in.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libqt5opengl5 amd64 5.9.5+dfsg-0ubuntu1 [128 kB]
Get:13 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libqt5multimediawidgets5 amd64 5.9.5-0ubuntu1 [128 kB]
Get:14 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libqgsttools-p1 amd64 5.9.5-0ubuntu1 [128 kB]
Get:15 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libqt5multimedia5-plugins amd64 5.9.5-0ubuntu1 [128 kB]
Get:16 http://in.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libqt5sprintsupport5 amd64 5.9.5+dfsg-0ubuntu1 [128 kB]
Get:17 http://in.archive.ubuntu.com/ubuntu bionic/main amd64 libsmi2ldbl amd64 0.4.8+dfsg2-15 [100 kB]
Get:18 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libspandsp2 amd64 0.0.6+dfsg-0.1 [128 kB]
Get:19 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libssh-gcrypt-4 amd64 4.7.0-1 [128 kB]
Get:20 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libwscodec2 amd64 0.0.0-1 [128 kB]
Get:21 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libwiretap8 amd64 0.0.0-1 [128 kB]
Get:22 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libwireshark11 amd64 1.10.2-1 [128 kB]
Get:23 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 libwireshark-data amd64 1.10.2-1 [128 kB]
Get:24 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 qt5-gtk-platformtheme amd64 5.9.5-0ubuntu1 [128 kB]
Get:25 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 qttranslations5-l10n amd64 5.9.5-0ubuntu1 [128 kB]
Get:26 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 wireshark-common amd64 1.10.2-1 [128 kB]
Get:27 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 wireshark-qt amd64 1.10.2-1 [128 kB]
Fetched 30.2 MB in 10s (3020 kB/s)
debconf: delaying package configuration, since apt-utils is not installed
Processing triggers for mime-support (3.60ubuntu1) ...
```

sudo dpkg-reconfigure wireshark-common

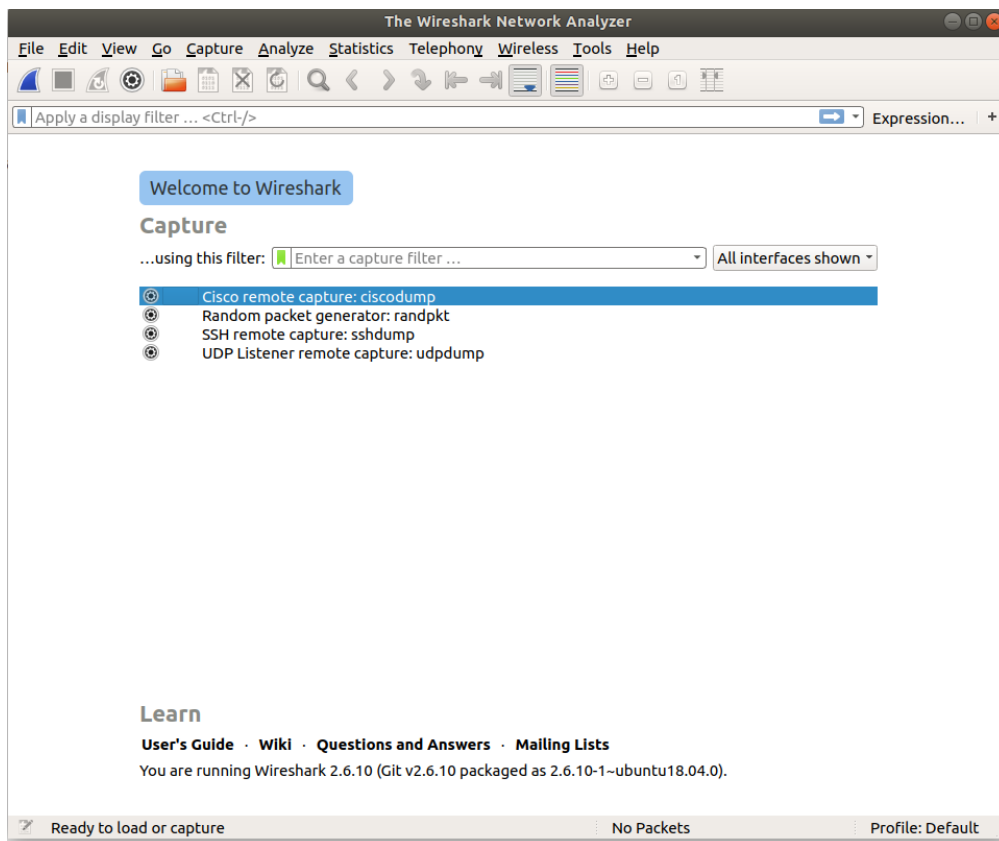
```
vivin@vivin:~$ sudo dpkg-reconfigure wireshark-common
vivin@vivin:~$
```



sudo adduser \$USER wireshark

```
vivin@vivin:~$ sudo dpkg-reconfigure wireshark-common
vivin@vivin:~$ sudo adduser $USER wireshark
Adding user `vivin' to group `wireshark' ...
Adding user vivin to group wireshark
Done.
vivin@vivin:~$
```

Open Wireshark from Applications

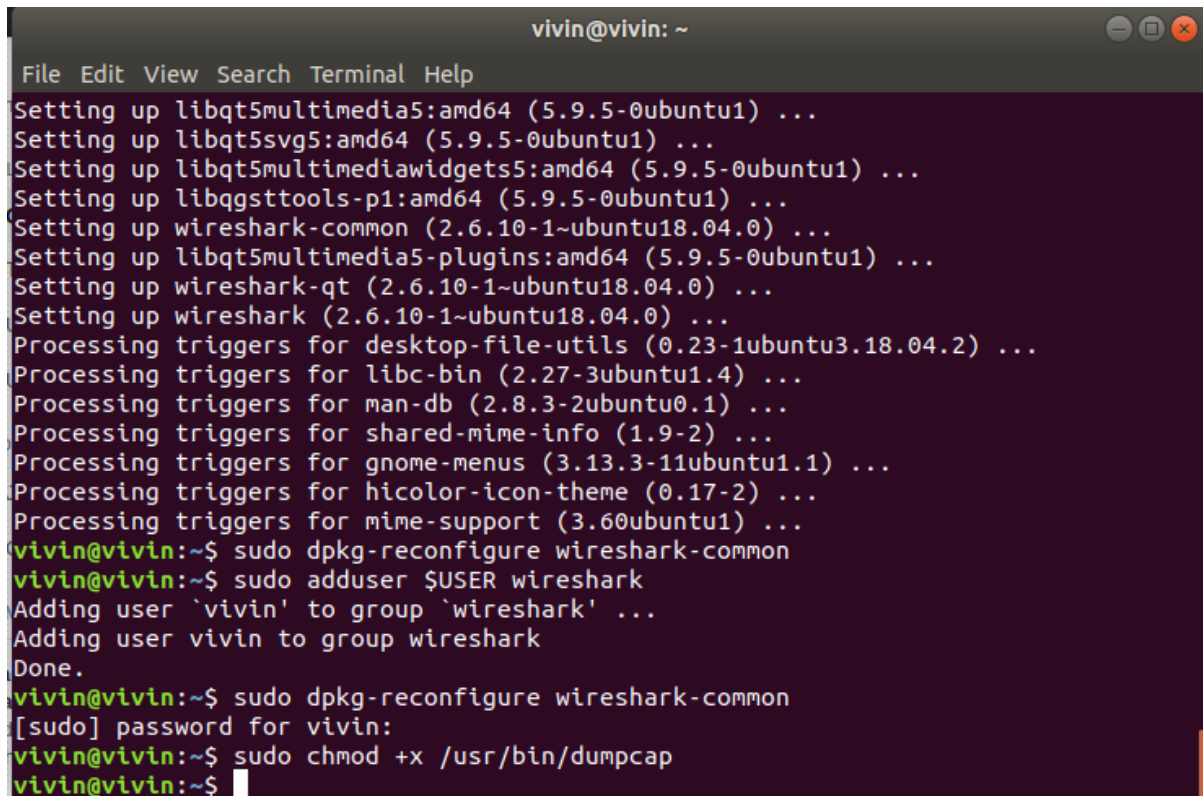


Since showing

"couldn't run /usr/bin/dumpcap in child process

Use command

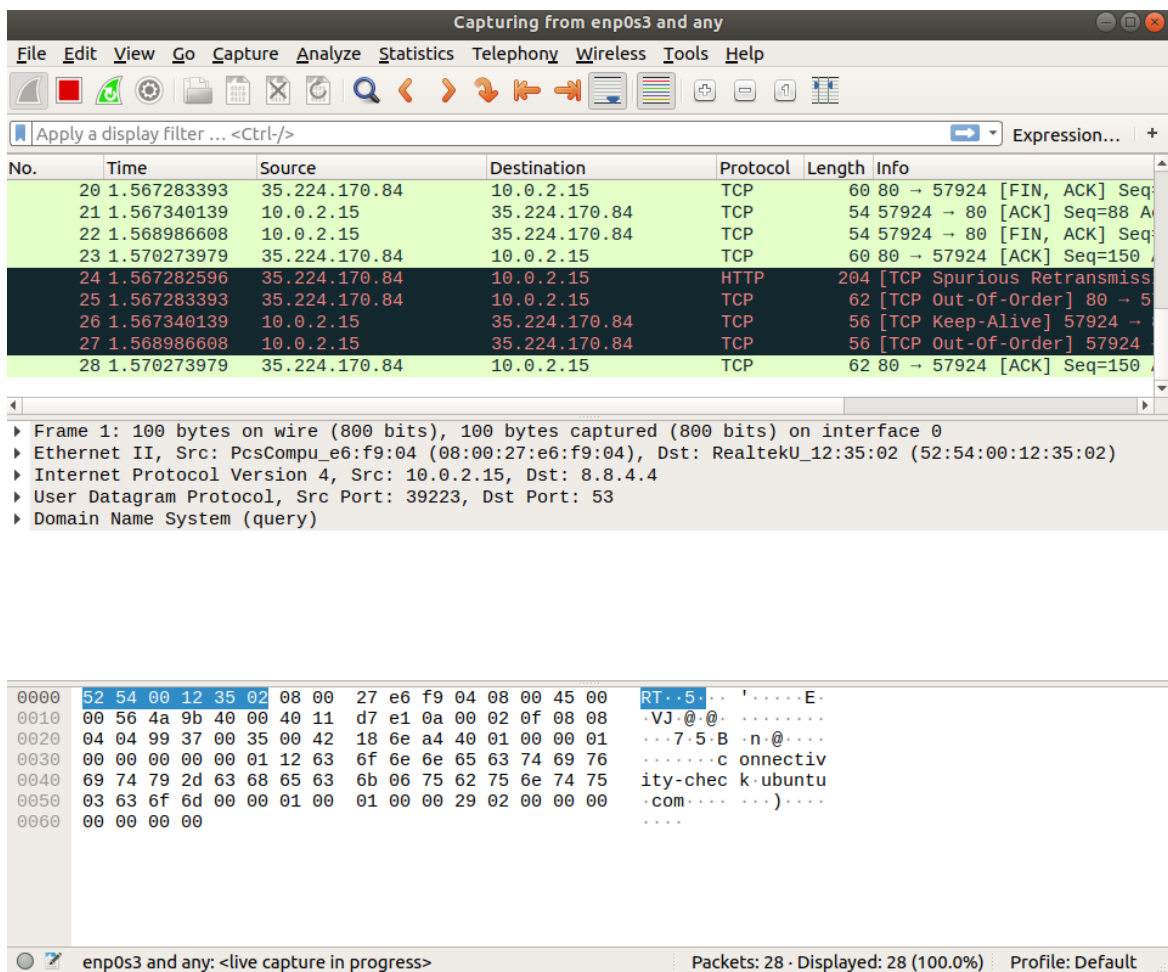
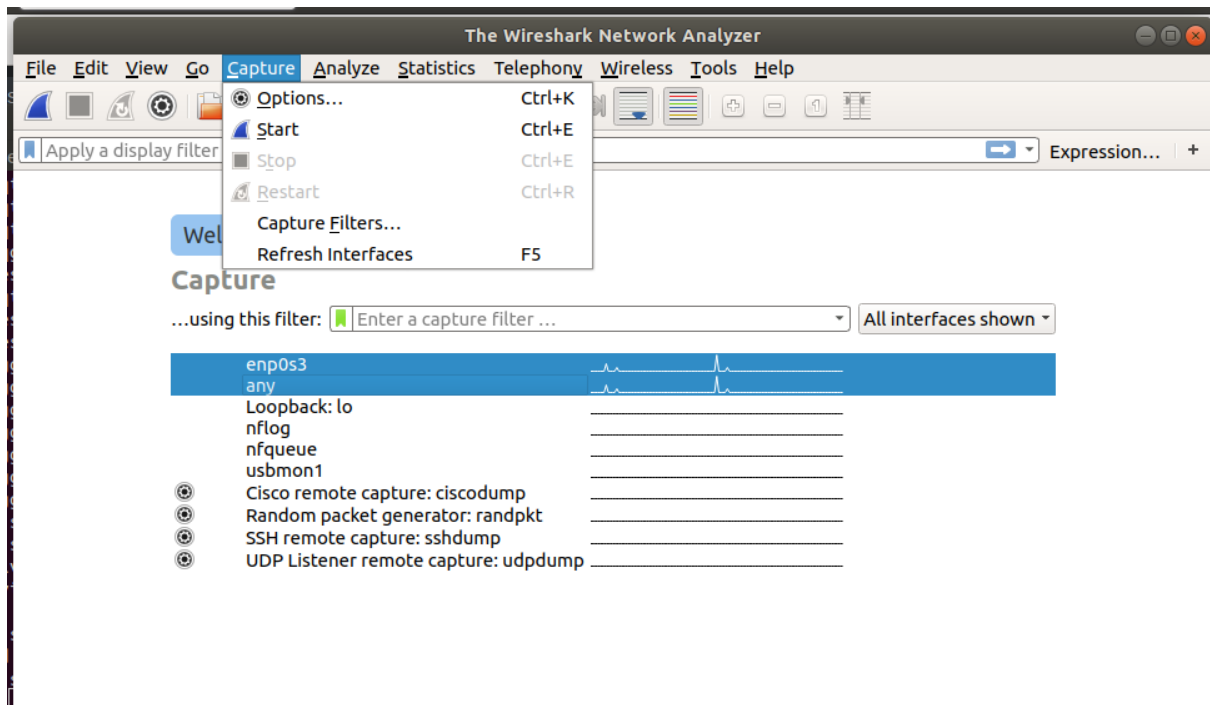
sudo chmod +x /usr/bin/dumpcap

A terminal window titled 'vivin@vivin: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal output shows the installation of various packages including libqt5multimedia5, libqt5svg5, libqt5multimediawidgets5, libqgsttools-p1, wireshark-common, libqt5multimedia5-plugins, wireshark-qt, and wireshark. It then shows the processing of triggers for desktop-file-utils, libc-bin, man-db, shared-mime-info, gnome-menus, hicolor-icon-theme, and mime-support. The user 'vivin' is added to the 'wireshark' group. Finally, the command 'sudo dpkg-reconfigure wireshark-common' is run, followed by 'sudo chmod +x /usr/bin/dumpcap', which completes successfully.

```
vivin@vivin: ~  
File Edit View Search Terminal Help  
Setting up libqt5multimedia5:amd64 (5.9.5-0ubuntu1) ...  
Setting up libqt5svg5:amd64 (5.9.5-0ubuntu1) ...  
Setting up libqt5multimediawidgets5:amd64 (5.9.5-0ubuntu1) ...  
Setting up libqgsttools-p1:amd64 (5.9.5-0ubuntu1) ...  
Setting up wireshark-common (2.6.10-1~ubuntu18.04.0) ...  
Setting up libqt5multimedia5-plugins:amd64 (5.9.5-0ubuntu1) ...  
Setting up wireshark-qt (2.6.10-1~ubuntu18.04.0) ...  
Setting up wireshark (2.6.10-1~ubuntu18.04.0) ...  
Processing triggers for desktop-file-utils (0.23-1ubuntu3.18.04.2) ...  
Processing triggers for libc-bin (2.27-3ubuntu1.4) ...  
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...  
Processing triggers for shared-mime-info (1.9-2) ...  
Processing triggers for gnome-menus (3.13.3-11ubuntu1.1) ...  
Processing triggers for hicolor-icon-theme (0.17-2) ...  
Processing triggers for mime-support (3.60ubuntu1) ...  
vivin@vivin:~$ sudo dpkg-reconfigure wireshark-common  
vivin@vivin:~$ sudo adduser $USER wireshark  
Adding user `vivin' to group `wireshark' ...  
Adding user vivin to group wireshark  
Done.  
vivin@vivin:~$ sudo dpkg-reconfigure wireshark-common  
[sudo] password for vivin:  
vivin@vivin:~$ sudo chmod +x /usr/bin/dumpcap  
vivin@vivin:~$
```

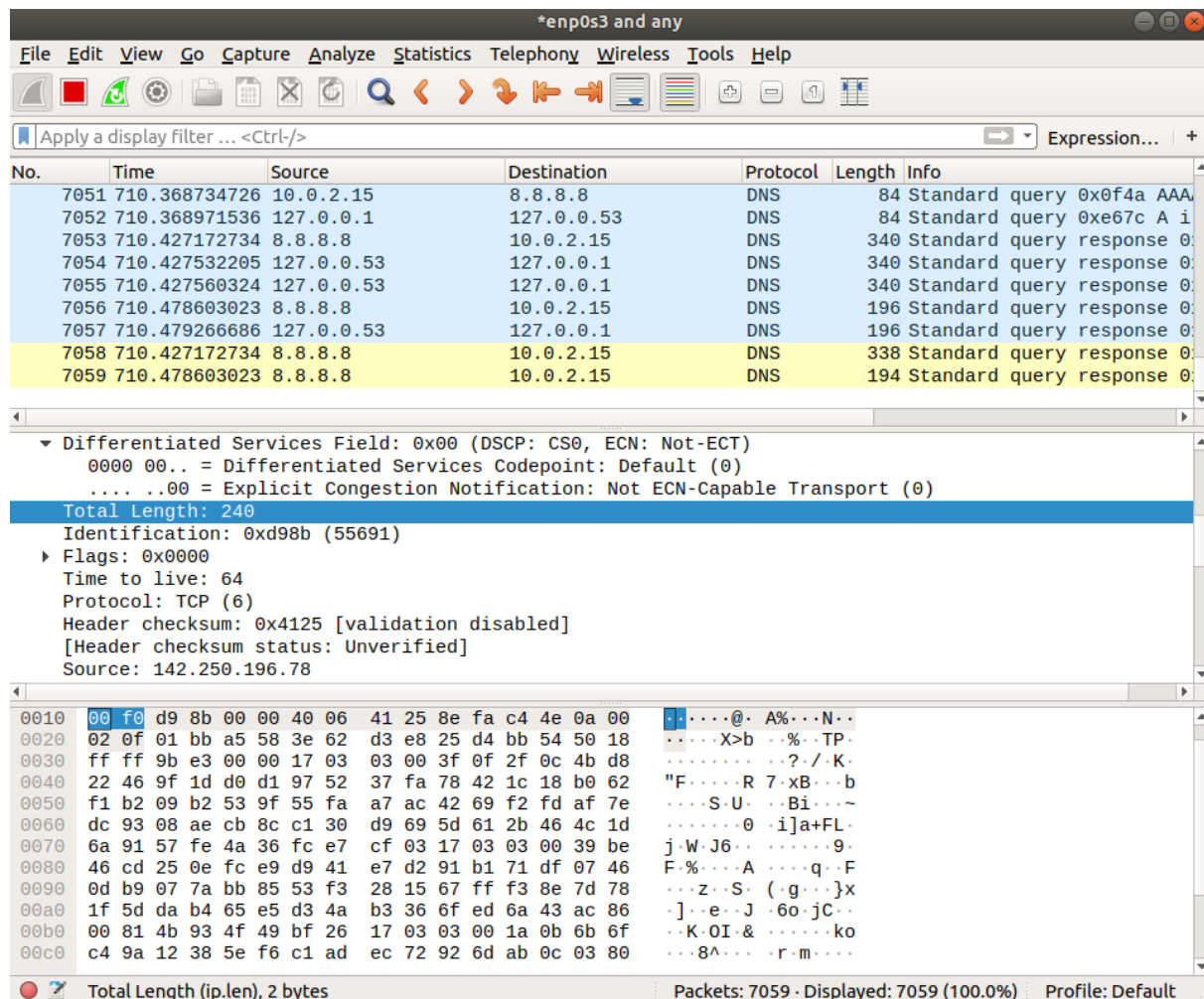
Capturing Data Packets on Wireshark

- When you open Wireshark, you see a screen that shows you a list of all of the network connections you can monitor. You also have a capture filter field, so you only capture the network traffic you want to see.
- You can select one or more of the network interfaces using “shift left-click.” Once you have the network interface selected, you can start the capture, and there are several ways to do that.
- Click the first button on the toolbar, titled “Start Capturing Packets.”



Analyzing Data Packets on Wireshark

- Wireshark shows you three different panes for inspecting packet data. The Packet List, the top pane, is a list of all the packets in the capture. When you click on a packet, the other two panes change to show you the details about the selected packet. You can also tell if the packet is part of a conversation. Here are some details about each column in the top pane:



In panel

- No.:** This is the number order of the packet that got captured. The bracket indicates that this packet is part of a conversation.
- Time:** This column shows you how long after you started the capture that this packet got captured. You can change this value in the Settings menu if you need something different displayed.

- **Source:** This is the address of the system that sent the packet.
- **Destination:** This is the address of the destination of that packet.
- **Protocol:** This is the type of packet, for example, TCP, DNS, DHCPv6, or ARP.
- **Length:** This column shows you the length of the packet in bytes.
- **Info:** This column shows you more information about the packet contents, and will vary depending on what kind of packet it is.

Find details of a particular packet by clicking that on first panel

Details can take on the below panels or new window

The image shows a Wireshark packet capture window titled "*enp0s3 and any". The filter bar at the top shows "ip.dst == 10.0.2.15". The packet list pane displays several packets, with the selected packet (Frame 10856) highlighted in blue. The details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (TCP) fields. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
10855	0.000000	10.0.2.15	10.0.2.15	TLSv1.3	998	Application Data, Application Data, Application Data
10856	0.000000	10.0.2.15	10.0.2.15	TCP	60	443 → 43160 [ACK] Seq=3825 Ack=1020 Win=65535 Len=0
10857	0.000000	10.0.2.15	10.0.2.15	TCP	60	443 → 43162 [ACK] Seq=3825 Ack=582 Win=65535 Len=0
10858	0.000000	10.0.2.15	10.0.2.15	TLSv1.3	2934	Server Hello, Change Cipher Spec, Application Data
10859	0.000000	10.0.2.15	10.0.2.15	TCP	60	443 → 43162 [ACK] Seq=3825 Ack=1020 Win=65535 Len=0
10860	0.000000	10.0.2.15	10.0.2.15	TLSv1.3	998	Application Data, Application Data, Application Data
10861	0.000000	10.0.2.15	10.0.2.15	TLSv1.3	1494	Server Hello, Change Cipher Spec, Application Data
10862	0.000000	10.0.2.15	10.0.2.15	TCP	1494	443 → 43160 [PSH, ACK] Seq=3825 Ack=1020 Win=65535 Len=1440 [...]
10863	0.000000	10.0.2.15	10.0.2.15	TLSv1.3	1599	Application Data
10864	0.000000	10.0.2.15	10.0.2.15	TCP	1494	443 → 43152 [PSH, ACK] Seq=1441 Ack=518 Win=65535 Len=1440 [T...]

Frame 10856: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface 0

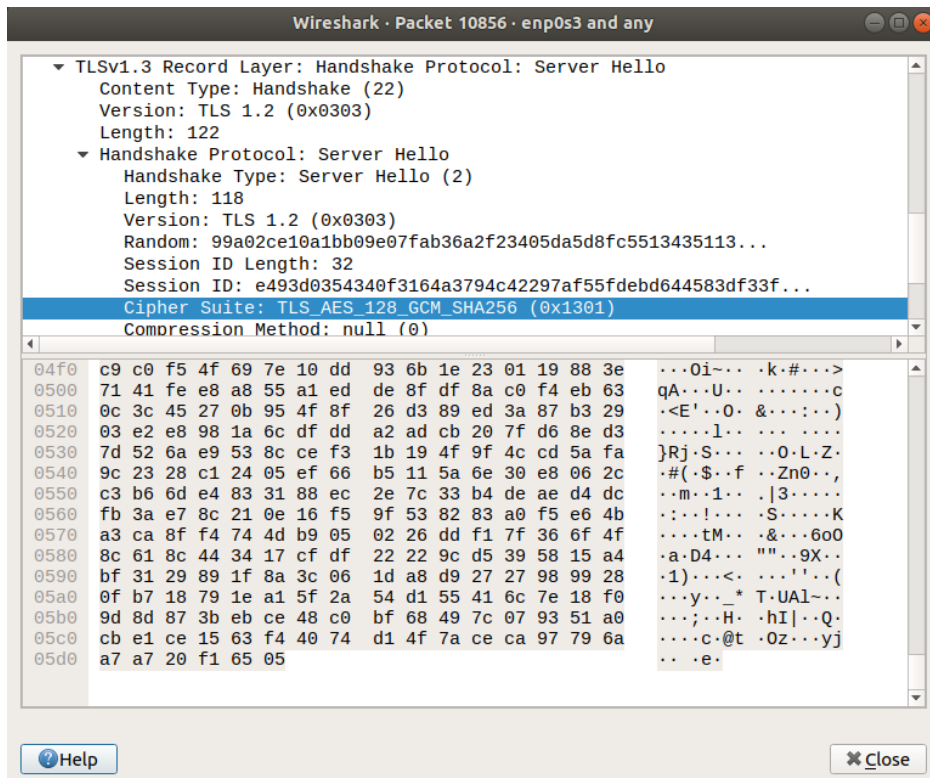
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_e6:f9:04 (08:00:27:e6:f9:04)

Internet Protocol Version 4, Src: 52.84.6.3, Dst: 10.0.2.15

Transmission Control Protocol, Src Port: 443, Dst Port: 43152, Seq: 1, Ack: 518, Len: 1440

Source Port: 443
Destination Port: 43152
[Stream index: 57]
[TCP Segment Len: 1440]
Sequence number: 1 (relative sequence number)
[Next sequence number: 1441 (relative sequence number)]
Acknowledgment number: 518 (relative ack number)
0101 = Header Length: 20 bytes (5)

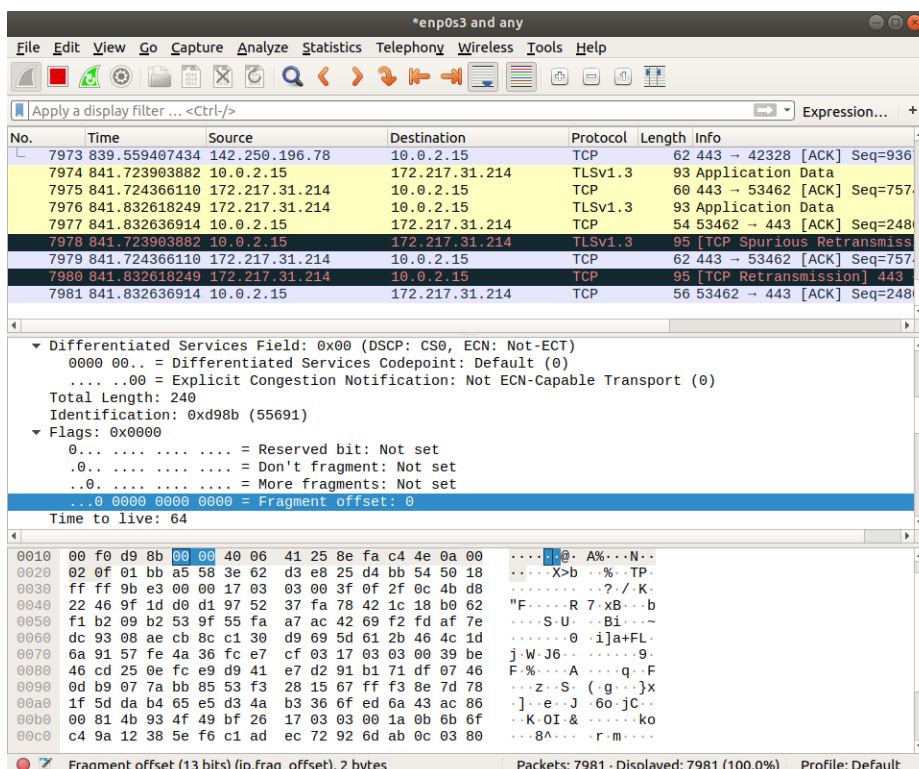
0000 08 00 27 e6 f9 04 52 54 00 12 35 02 08 00 45 00 ...RT...5...E.
0010 05 c8 df a8 00 00 40 06 4f 22 34 54 06 03 0a 00@ 0"4T....
0020 02 0f 01 bb a8 90 43 77 7c 02 ef 54 00 74 50 18Cw |..T.tP.
0030 ff ff de 6f 00 00 16 03 03 00 7a 02 00 00 76 03o.....Z...v.
0040 03 99 a0 2c e1 0a 1b b0 9e 07 fa b3 6a 2f 23 40j/#@
0050 5d a5 d8 fc 55 13 43 51 13 5f c5 30 e6 75 5d b3]...U.CQ...0.u].
0060 b7 20 e4 93 d0 35 43 40 f3 16 4a 37 94 c4 22 975C@...J7...".
0070 af 55 fd eb d6 44 58 3d f3 3f ef 4f e9 eb 30 21 ..U...DX= ? 0 0!
0080 4e 2f 13 01 00 00 2e 00 2b 00 02 03 04 00 33 00 N/.....+...3.
0090 24 00 1d 00 20 b3 f3 76 05 8c a6 d0 0b 5b c9 78 \$. ...v[.x
00a0 dc 2b 60 ea 57 00 f2 06 bc e3 a0 92 18 80 39 d0 .+..W.....9.
00b0 97 40 4c f7 5a 14 03 03 00 01 01 17 03 03 00 1b .@L.Z.....



Find the fields from 3 rd panel by clicking them and the field will automatically select from 2 nd panel

Some fields

1.Fragment offset



2. Time to live

The screenshot shows a Wireshark packet capture window titled '*enp0s3 and any'. The packet list displays several TCP segments, many of which are retransmissions. The packet details pane for the selected packet (No. 8549) shows the following information:

- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- 0000 00.. = Differentiated Services Codepoint: Default (0)
- 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
- Total Length: 240
- Identification: 0xd98b (55691)
- Flags: 0x0000
 - 0... .. = Reserved bit: Not set
 - .0... .. = Don't fragment: Not set
 - ..0... .. = More fragments: Not set
 - ...0 0000 0000 0000 = Fragment offset: 0
- Time to live: 64

The packet bytes pane shows the raw data of the packet, including the IP header and the payload.

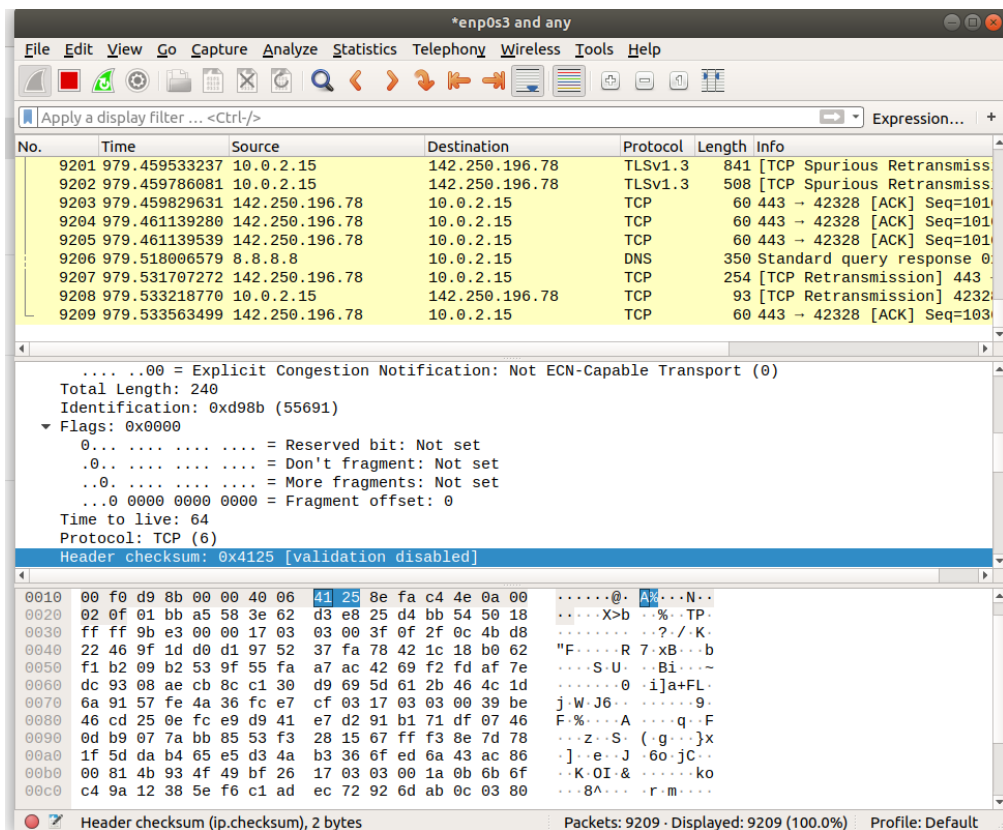
3. Protocol

The screenshot shows a Wireshark packet capture window titled '*enp0s3 and any'. The packet list displays several TCP and TLSv1.3 segments. The packet details pane for the selected packet (No. 8619) shows the following information:

- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- 0000 00.. = Differentiated Services Codepoint: Default (0)
- 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
- Total Length: 240
- Identification: 0xd98b (55691)
- Flags: 0x0000
 - 0... .. = Reserved bit: Not set
 - .0... .. = Don't fragment: Not set
 - ..0... .. = More fragments: Not set
 - ...0 0000 0000 0000 = Fragment offset: 0
- Time to live: 64
- Protocol: TCP (6)

The packet bytes pane shows the raw data of the packet, including the IP header and the payload.

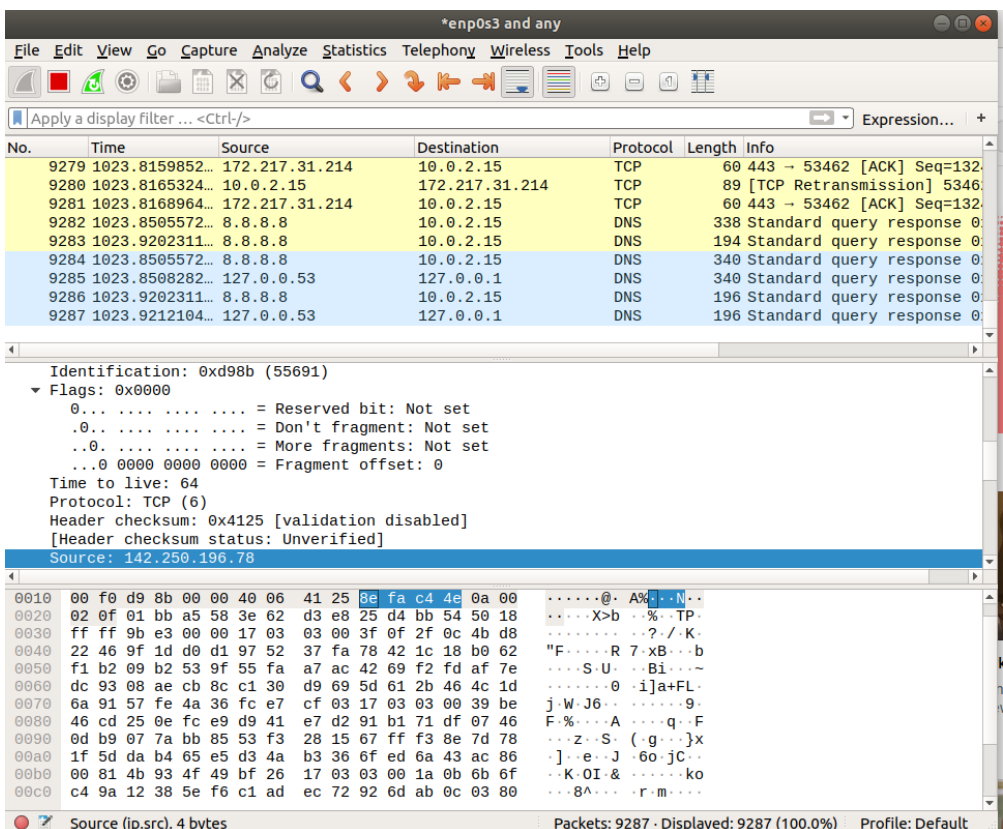
4. Header Checksum



Wireshark packet capture showing a TCP segment. The packet is from 10.0.2.15 to 142.250.196.78. The header checksum is highlighted in blue.

Header checksum: 0x4125 [validation disabled]

6. Source address



Wireshark packet capture showing a TCP segment. The packet is from 10.0.2.15 to 172.217.31.214. The source address is highlighted in blue.

Source (ip.src), 4 bytes

7. Destination address

The screenshot shows the Wireshark interface with the display filter `ip.dst == 10.0.2.15` applied. The packet list shows several TCP packets from source 10.0.2.15 to destination 172.217.31.214. The packet details pane shows the flags for the selected packet (No. 9951) as `0x0000`, indicating a reset (RST). The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
9943	1205.0855321...	10.0.2.15	172.217.31.214	TCP	54	53462 → 443 [ACK] Seq=443
9944	1205.0863281...	172.217.31.214	10.0.2.15	TCP	2914	[TCP Retransmission] 443
9945	1205.0863421...	10.0.2.15	172.217.31.214	TCP	54	53462 → 443 [ACK] Seq=443
9946	1205.0873327...	172.217.31.214	10.0.2.15	TCP	1484	[TCP Retransmission] 443
9947	1205.0875367...	10.0.2.15	172.217.31.214	TCP	54	53462 → 443 [ACK] Seq=443
9948	1205.0907968...	172.217.31.214	10.0.2.15	TCP	3858	[TCP Retransmission] 443
9949	1205.0909819...	10.0.2.15	172.217.31.214	TCP	54	53462 → 443 [ACK] Seq=443
9950	1205.0911317...	10.0.2.15	172.217.31.214	TCP	93	[TCP Retransmission] 5346
9951	1205.0914259...	172.217.31.214	10.0.2.15	TCP	60	443 → 53462 [ACK] Seq=160

Flags: 0x0000
0... .. = Reserved bit: Not set
.0... .. = Don't fragment: Not set
..0... .. = More fragments: Not set
...0 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: TCP (6)
Header checksum: 0x4125 [validation disabled]
[Header checksum status: Unverified]
Source: 142.250.196.78
Destination: 10.0.2.15

Destination (ip.dst), 4 bytes Packets: 9951 · Displayed: 9951 (100.0%) Profile: Default

8. Next Sequence number

The screenshot shows the Wireshark interface with the display filter `ip.dst == 10.0.2.15` applied. The packet list shows several TLS and TCP packets from source 52.84.6.3 to destination 10.0.2.15. The packet details pane shows the next sequence number for the selected packet (No. 10856) as 1441.

No.	Time	Source	Destination	Protocol	Length	Info
10845	1315.4488061...	52.84.6.3	10.0.2.15	TLSv1.3	998	Application Data, Applica
10846	1315.4488066...	52.84.6.3	10.0.2.15	TCP	60	443 → 43160 [ACK] Seq=382
10850	1315.4582060...	52.84.6.3	10.0.2.15	TCP	60	443 → 43162 [ACK] Seq=382
10851	1315.4582066...	52.84.6.3	10.0.2.15	TLSv1.3	2934	Server Hello, Change Ciph
10852	1315.4582066...	52.84.6.3	10.0.2.15	TCP	60	443 → 43162 [ACK] Seq=382
10854	1315.4597911...	52.84.6.3	10.0.2.15	TLSv1.3	998	Application Data, Applica
10856	1315.4752745...	52.84.6.3	10.0.2.15	TLSv1.3	1494	Server Hello, Change Ciph
10857	1315.4752753...	52.84.6.3	10.0.2.15	TCP	1494	443 → 43160 [PSH, ACK] Seq=
10858	1315.4752753...	52.84.6.3	10.0.2.15	TLSv1.3	1599	Application Data
10859	1315.4752754...	52.84.6.3	10.0.2.15	TCP	1494	443 → 43152 [PSH, ACK] Seq=

Frame 10856: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface 0
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_e6:f9:04 (08:00:27:e6:f9:04)
Internet Protocol Version 4, Src: 52.84.6.3, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 443, Dst Port: 43152, Seq: 1, Ack: 518, Len: 1440
Source Port: 443
Destination Port: 43152
[Stream index: 57]
[TCP Segment Len: 1440]
Sequence number: 1 (relative sequence number)
[Next sequence number: 1441 (relative sequence number)]
Acknowledgment number: 518 (relative ack number)
0101 = Header Length: 20 bytes (5)

Next sequence number (tcp.nextseq) Packets: 12851 · Displayed: 6336 (49.3%) Profile: Default