20MCA136-NETWORKING & ADMINISTRATION LAB

WIRESHARK INSTALLATION

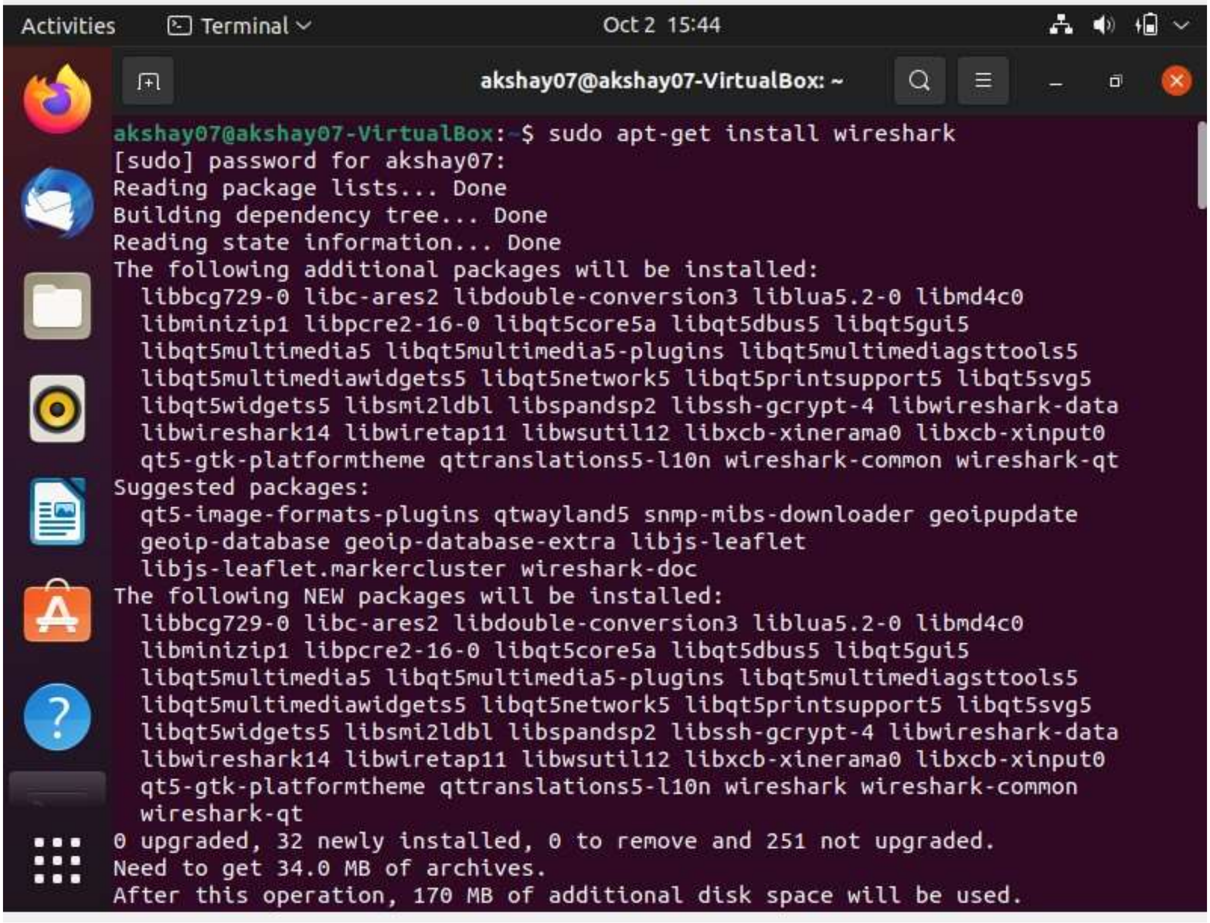
SUBMITTED BY,

AKSHAY MURALI
MCA A BATCH
ROLL NO-07

Wireshark Installation

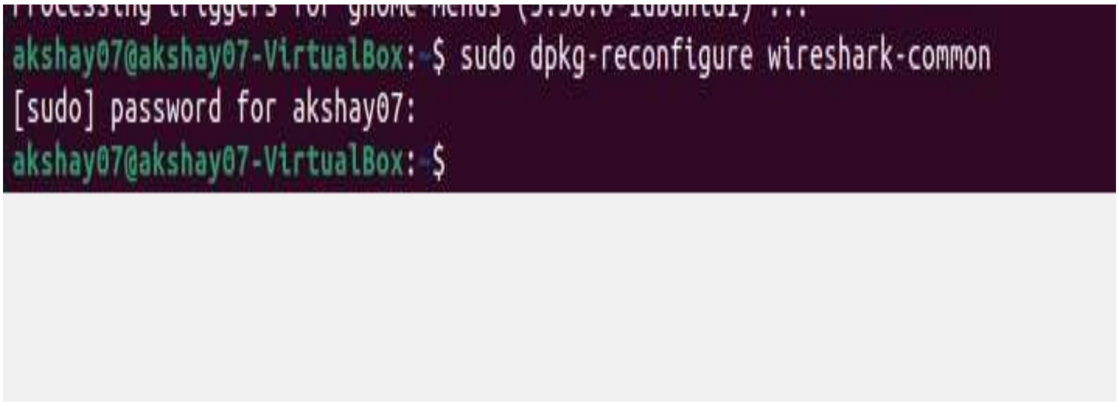
In terminal of ubuntu

sudo apt-get install wireshark

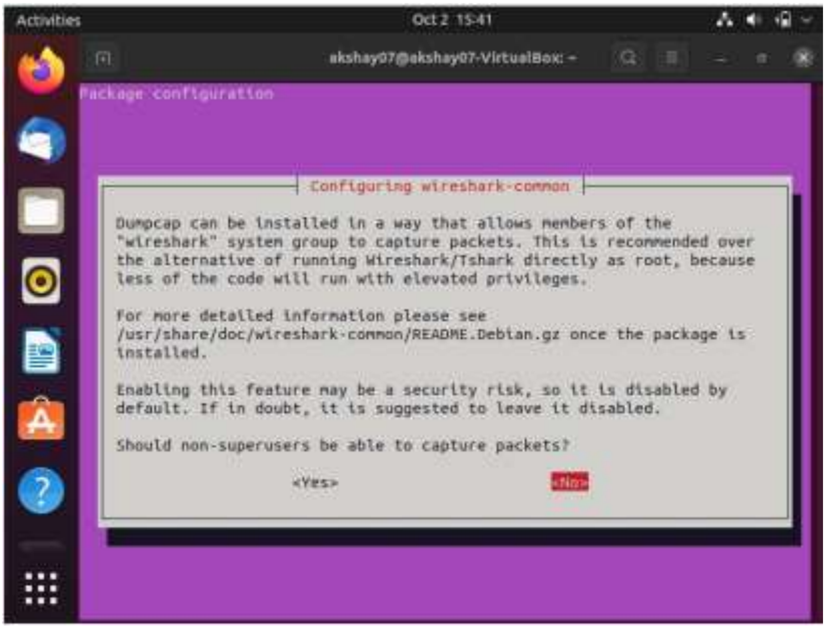


```
akshay07@akshay07-VirtualBox:~$ sudo apt-get install wireshark
[sudo] password for akshay07:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libbcg729-0 libc-ares2 libdouble-conversion3 liblua5.2-0 libmd4c0
  libminizip1 libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5
  libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediagsttools5
  libqt5multimediawidgets5 libqt5network5 libqt5printsupport5 libqt5svg5
  libqt5widgets5 libsmi2ldbl libspandsp2 libssh-gcrypt-4 libwireshark-data
  libwireshark14 libwiretap11 libwsutil12 libxcb-xinerama0 libxcb-xinput0
  qt5-gtk-platformtheme qttranslations5-l10n wireshark-common wireshark-qt
Suggested packages:
  qt5-image-formats-plugins qtwayland5 snmp-mibs-downloader geoipupdate
  geoip-database geoip-database-extra libjs-leaflet
  libjs-leaflet.markercluster wireshark-doc
The following NEW packages will be installed:
  libbcg729-0 libc-ares2 libdouble-conversion3 liblua5.2-0 libmd4c0
  libminizip1 libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5
  libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediagsttools5
  libqt5multimediawidgets5 libqt5network5 libqt5printsupport5 libqt5svg5
  libqt5widgets5 libsmi2ldbl libspandsp2 libssh-gcrypt-4 libwireshark-data
  libwireshark14 libwiretap11 libwsutil12 libxcb-xinerama0 libxcb-xinput0
  qt5-gtk-platformtheme qttranslations5-l10n wireshark wireshark-common
  wireshark-qt
0 upgraded, 32 newly installed, 0 to remove and 251 not upgraded.
Need to get 34.0 MB of archives.
After this operation, 170 MB of additional disk space will be used.
```

sudo dpkg-reconfigure wireshark-common

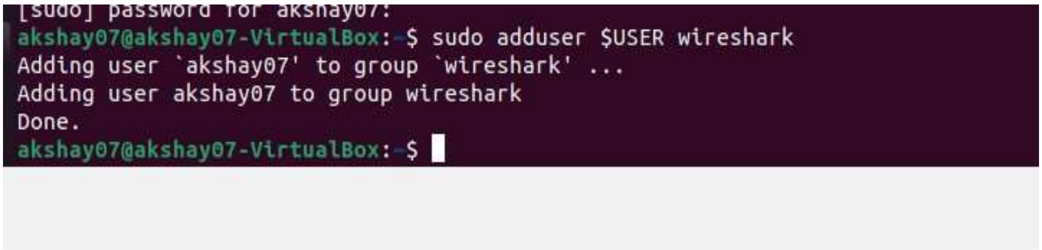


```
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
akshay07@akshay07-VirtualBox:~$ sudo dpkg-reconfigure wireshark-common
[sudo] password for akshay07:
akshay07@akshay07-VirtualBox:~$
```



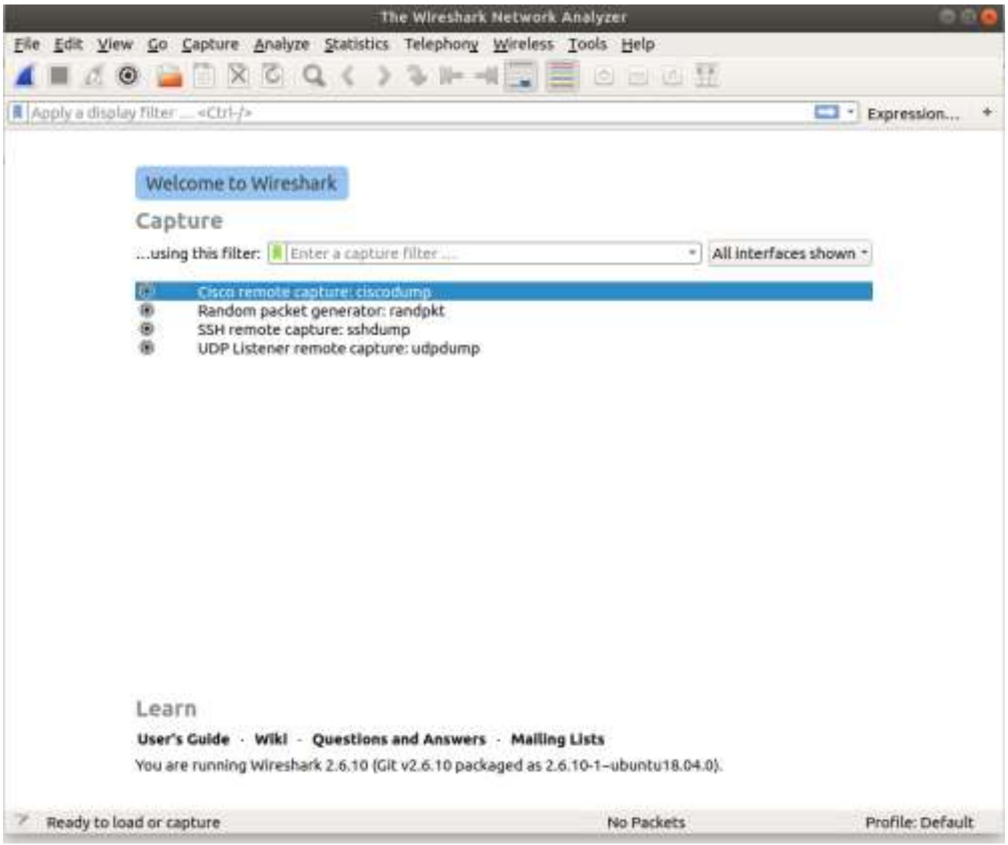
```
Package configuration

Configuring wireshark-common

Dumpcap can be installed in a way that allows members of the
"wireshark" system group to capture packets. This is recommended over
the alternative of running Wireshark/Tshark directly as root, because
less of the code will run with elevated privileges.

For more detailed information please see
/usr/share/doc/wireshark-common/README.Debian.gz once the package is
installed.

Enabling this feature may be a security risk, so it is disabled by
default. If in doubt, it is suggested to leave it disabled.

Should non-superusers be able to capture packets?

              <Yes>                              <No>
```

sudo adduser $USER wireshark



```
[sudo] password for akshay07:
akshay07@akshay07-VirtualBox:~$ sudo adduser $USER wireshark
Adding user `akshay07' to group `wireshark' ...
Adding user akshay07 to group wireshark
Done.
akshay07@akshay07-VirtualBox:~$ 
```

Open Wireshark from Applications


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression… +
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

Cisco remote capture: ciscodump
Random packet generator: randpkt
SSH remote capture: sshdump
UDP Listener remote capture: udpdump

You are running Wireshark 2.6.10 (Git v2.6.10 packaged as 2.6.10-1~ubuntu18.04.0).

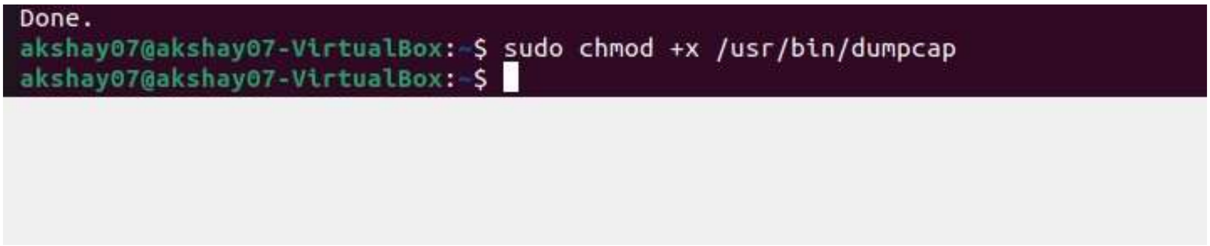
Ready to load or capture | No Packets | Profile: Default

Since showing

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

Use command

sudo chmod +x /usr/bin/dumpcap

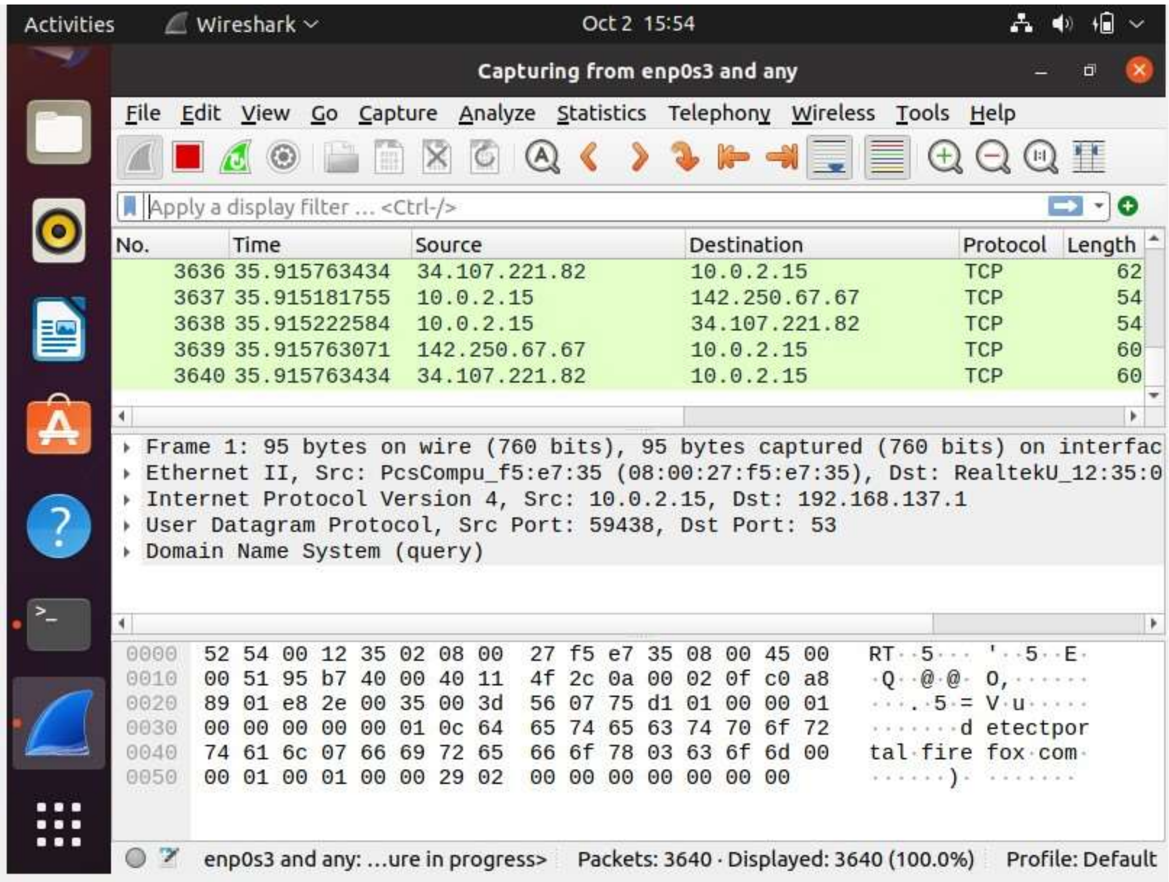


```
Done.
akshay07@akshay07-VirtualBox:~$ sudo chmod +x /usr/bin/dumpcap
akshay07@akshay07-VirtualBox:~$ 
```

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.”


Activities
Wireshark
Oct 2 15:54
Capturing from enp0s3 and any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length
3636	35.915763434	34.107.221.82	10.0.2.15	TCP	62
3637	35.915181755	10.0.2.15	142.250.67.67	TCP	54
3638	35.915222584	10.0.2.15	34.107.221.82	TCP	54
3639	35.915763071	142.250.67.67	10.0.2.15	TCP	60
3640	35.915763434	34.107.221.82	10.0.2.15	TCP	60

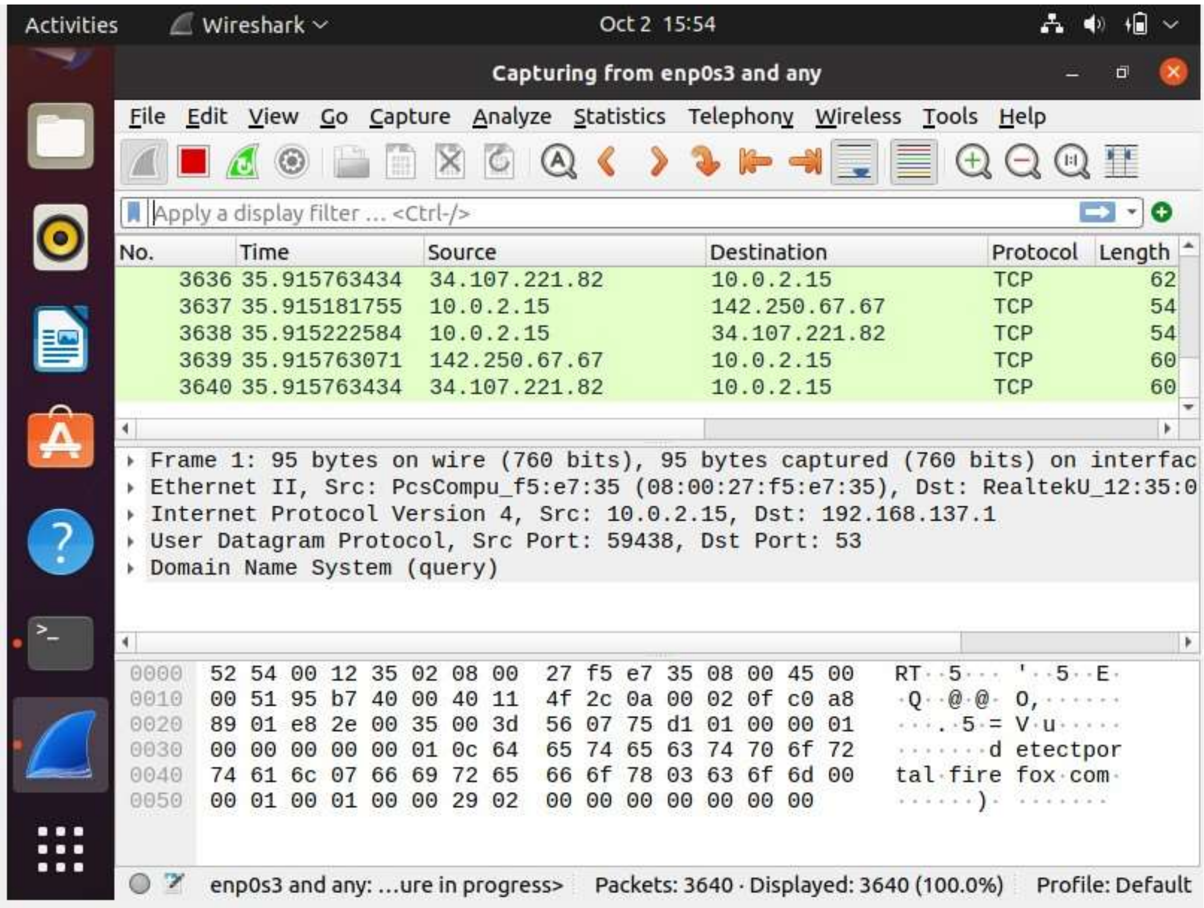
```
Frame 1: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interfac
Ethernet II, Src: PcsCompu_f5:e7:35 (08:00:27:f5:e7:35), Dst: RealtekU_12:35:0
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.137.1
User Datagram Protocol, Src Port: 59438, Dst Port: 53
Domain Name System (query)
```

```
0000  52 54 00 12 35 02 08 00  27 f5 e7 35 08 00 45 00   RT··5··· '··5··E·
0010  00 51 95 b7 40 00 40 11  4f 2c 0a 00 02 0f c0 a8   ·Q··@·@· O,······
0020  89 01 e8 2e 00 35 00 3d  56 07 75 d1 01 00 00 01   ···.·5·= V·u·····
0030  00 00 00 00 00 01 0c 64  65 74 65 63 74 70 6f 72   ·······d etectpor
0040  74 61 6c 07 66 69 72 65  66 6f 78 03 63 6f 6d 00   tal·fire fox·com·
0050  00 01 00 01 00 00 29 02  00 00 00 00 00 00 00      ······)· ·······
```

enp0s3 and any: …ure in progress> Packets: 3640 · Displayed: 3640 (100.0%) Profile: Default

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:


Activities
Wireshark
Oct 2 15:54
Capturing from enp0s3 and any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time          Source          Destination      Protocol  Length
 3636 35.915763434  34.107.221.82   10.0.2.15        TCP           62
 3637 35.915181755  10.0.2.15       142.250.67.67    TCP           54
 3638 35.915222584  10.0.2.15       34.107.221.82    TCP           54
 3639 35.915763071  142.250.67.67   10.0.2.15        TCP           60
 3640 35.915763434  34.107.221.82   10.0.2.15        TCP           60
```

```
▸ Frame 1: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interfac
▸ Ethernet II, Src: PcsCompu_f5:e7:35 (08:00:27:f5:e7:35), Dst: RealtekU_12:35:0
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.137.1
▸ User Datagram Protocol, Src Port: 59438, Dst Port: 53
▸ Domain Name System (query)
```

```
0000  52 54 00 12 35 02 08 00  27 f5 e7 35 08 00 45 00   RT··5···  '··5··E·
0010  00 51 95 b7 40 00 40 11  4f 2c 0a 00 02 0f c0 a8   ·Q··@·@·  O,······
0020  89 01 e8 2e 00 35 00 3d  56 07 75 d1 01 00 00 01   ···.·5·=  V·u·····
0030  00 00 00 00 00 01 0c 64  65 74 65 63 74 70 6f 72   ·······d  etectpor
0040  74 61 6c 07 66 69 72 65  66 6f 78 03 63 6f 6d 00   tal·fire  fox·com·
0050  00 01 00 01 00 00 29 02  00 00 00 00 00 00 00      ······)·  ·······
```

enp0s3 and any: …ure in progress> Packets: 3640 · Displayed: 3640 (100.0%) Profile: Default

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.

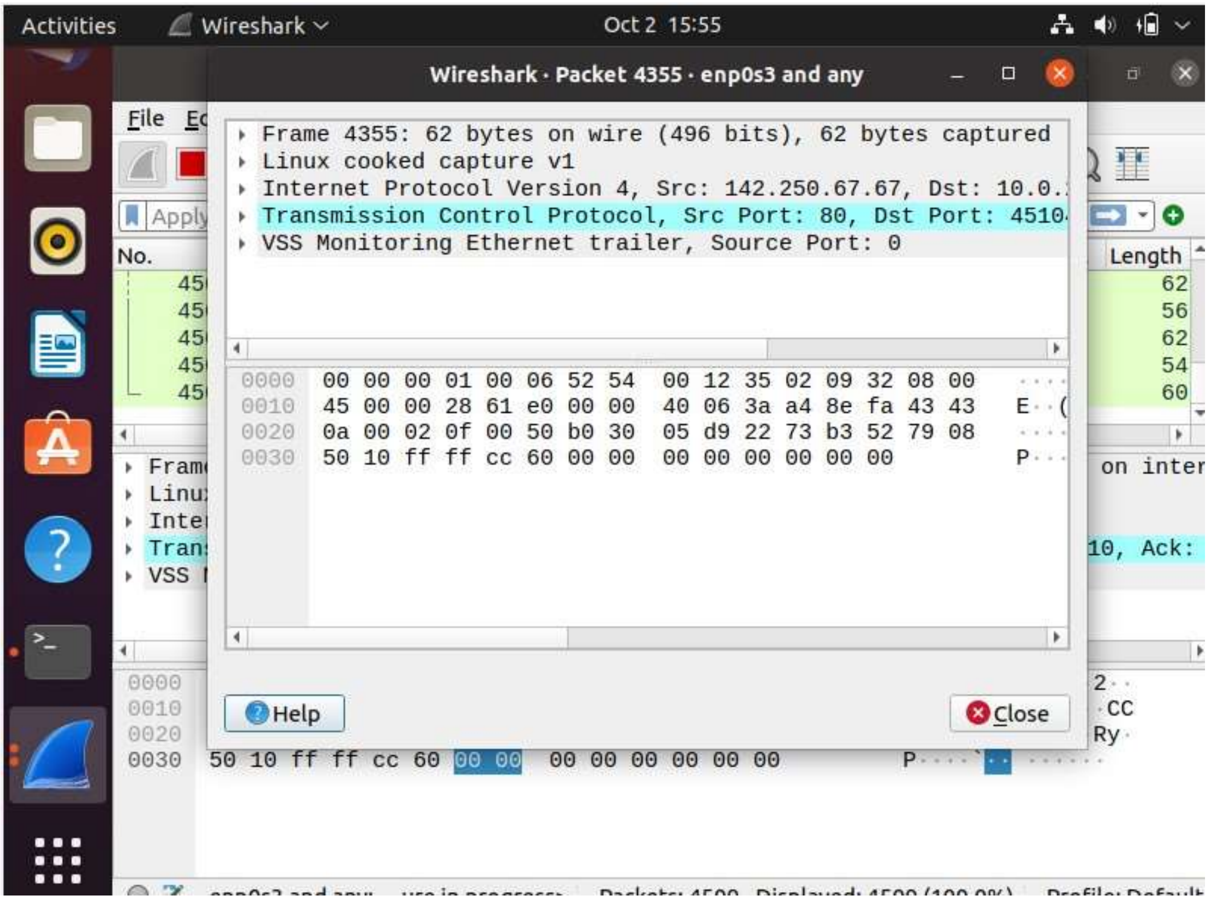
- **Length**: This column shows you the length of the packet in bytes.
- **Info**: This column shows you more information about the packet contents, and will vary depending on what kind of packet it is.

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

Details can take on the below panels or new window

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

Some fieldS



```
Frame 4355: 62 bytes on wire (496 bits), 62 bytes captured
Linux cooked capture v1
Internet Protocol Version 4, Src: 142.250.67.67, Dst: 10.0.
Transmission Control Protocol, Src Port: 80, Dst Port: 4510
VSS Monitoring Ethernet trailer, Source Port: 0
```

```
0000  00 00 00 01 00 06 52 54  00 12 35 02 09 32 08 00   ····
0010  45 00 00 28 61 e0 00 00  40 06 3a a4 8e fa 43 43   E··(
0020  0a 00 02 0f 00 50 b0 30  05 d9 22 73 b3 52 79 08   ····
0030  50 10 ff ff cc 60 00 00  00 00 00 00 00 00         P···
```