

Lab Report No.	02
Lab Report Name	Wireshark in Linux
ID	IT-17037

Objective:

- The main objective of Wireshark is to capture packets that are transmitted over a network. Wireshark can capture, decode and show various details of packets transmitted over a network.
- Observation of the functional difference between different packets and the analysis of the different headers and protocol.
- Writing a filtering options and choosing different analysis options.

Theory:

What is wireshark ?

Wireshark is a popular network analyser that uses pcap library to capture network packets at different layers of the OSI model. It is easy to install and possesses a nice GUI with many features.

Why use wireshark?

Wireshark is used in different sectors and different works . This is used for

- troubleshooting network problems
- examining security problems
- debugging protocol implementations
- learning network protocol internals
- used in industry and academia

what is the main features of the wireshark?

Wireshark has a rich feature set which includes the following:

- Deep inspection of hundreds of protocols, with more being added all the time
- Live capture and offline analysis
- Standard three-pane packet browser
- Multi-platform: Runs on Windows, Linux, OS X, FreeBSD, NetBSD, and many others

- Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility
- The most powerful display filters in the industry
- Rich VoIP analysis
- Capture files compressed with gzip can be decompressed on the fly
- Coloring rules can be applied to the packet list for quick, intuitive analysis
- Output can be exported to XML, PostScript®, CSV, or plain text

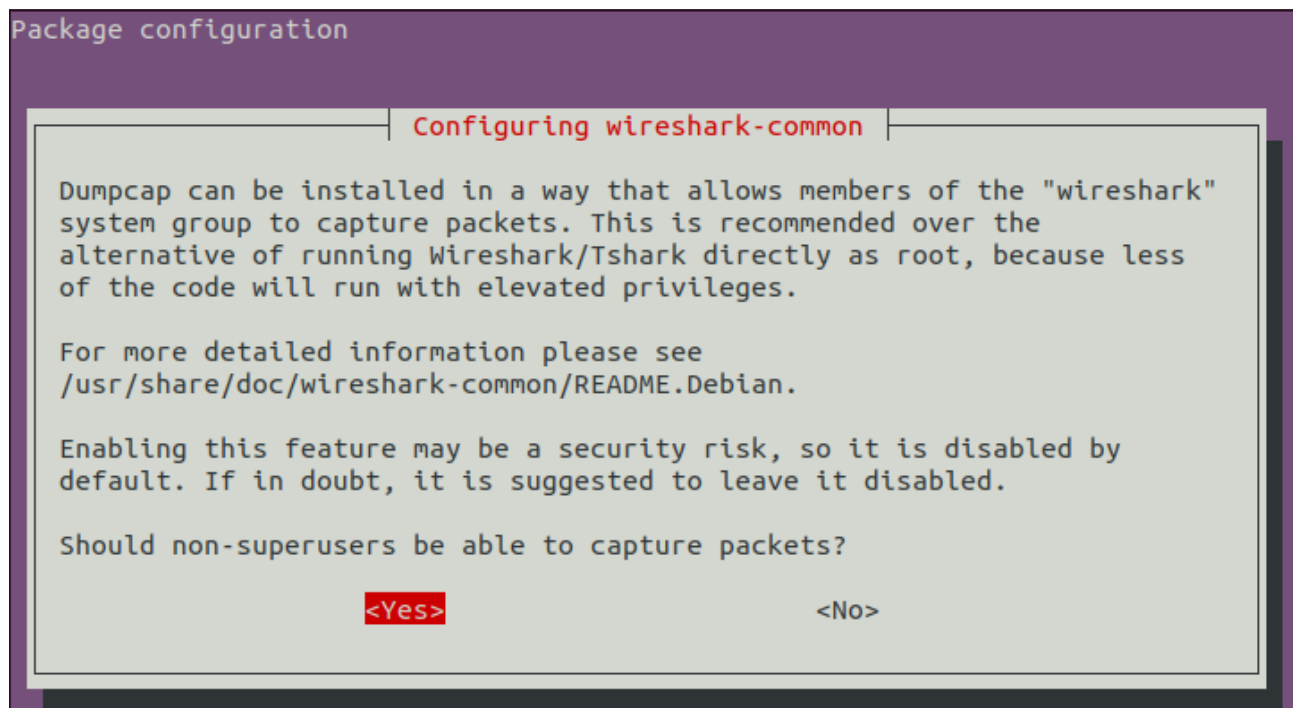
Wireshark Installation:

step-1: open the terminal. write this command:

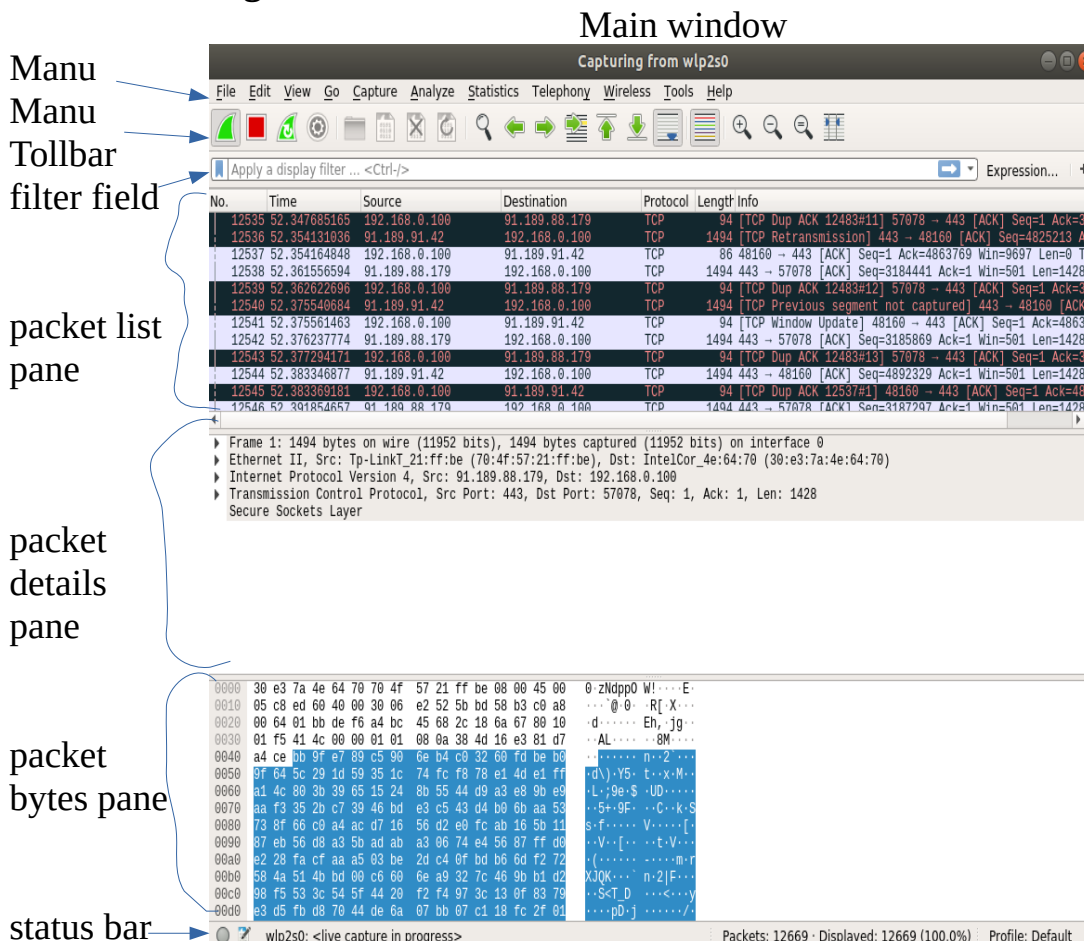
`sudo apt-get install wireshark;`

```
rafatul@rafatul-HP-Notebook:~$ sudo apt-get install wireshark;
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libllvm7
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  libc-ares2 libmaxminddb0 libnl-route-3-200 libqgsttools-p1 libqt5multimedia5
  libqt5multimedia5-plugins libqt5multimediawidgets5 libqt5opengl5
  libqt5sprintsupport5 libsmi2ldbl libspandsp2 libwireshark-data libwireshark11
  libwiretap8 libwscodec2 libwsutil9 wireshark-common wireshark-qt
Suggested packages:
  mmdb-bin snmp-mibs-downloader wireshark-doc
The following NEW packages will be installed:
  libc-ares2 libmaxminddb0 libnl-route-3-200 libqgsttools-p1 libqt5multimedia5
  libqt5multimedia5-plugins libqt5multimediawidgets5 libqt5opengl5
  libqt5sprintsupport5 libsmi2ldbl libspandsp2 libwireshark-data libwireshark11
  libwiretap8 libwscodec2 libwsutil9 wireshark-common wireshark-qt
0 upgraded, 19 newly installed, 0 to remove and 298 not upgraded.
Need to get 20.6 MB of archives.
After this operation, 107 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 libmaxminddb0 amd64 1.3.1-1 [25.6 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu bionic/main amd64 libnl-route-3-200 amd64 3.2.29-0ubuntu3 [146 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 libqt5multimedia5 amd64 5.9.5-0ubuntu1 [293 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libqt5opengl5 amd64 5.9.5+dfsg-0ubuntu2.5 [132 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 libqt5multimediawidgets5 amd64 5.9.5-0ubuntu1 [36.6 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 libqgsttools-p1 amd64 5.9.5-0ubuntu1 [72.4 kB]
Get:7 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 libqt5multimedia5-plugins amd64 5.9.5-0ubuntu1 [194 kB]
Get:8 http://us.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libqt5sprintsupport5 amd64 5.9.5+dfsg-0ubuntu2.5 [178 kB]
Get:9 http://us.archive.ubuntu.com/ubuntu bionic/main amd64 libsmi2ldbl amd64 0.4.8+dfsg2-15 [100 kB]
Get:10 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 libspandsp2 amd64 0.0.6+dfsg-0.1 [273 kB]
Get:11 http://us.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 libwireshark-data all 2.6.10-1-ubuntu18.04.0 [1,425 kB]
Get:12 http://us.archive.ubuntu.com/ubuntu bionic/main amd64 libc-ares2 amd64 1.14.0-1 [37.1 kB]
```

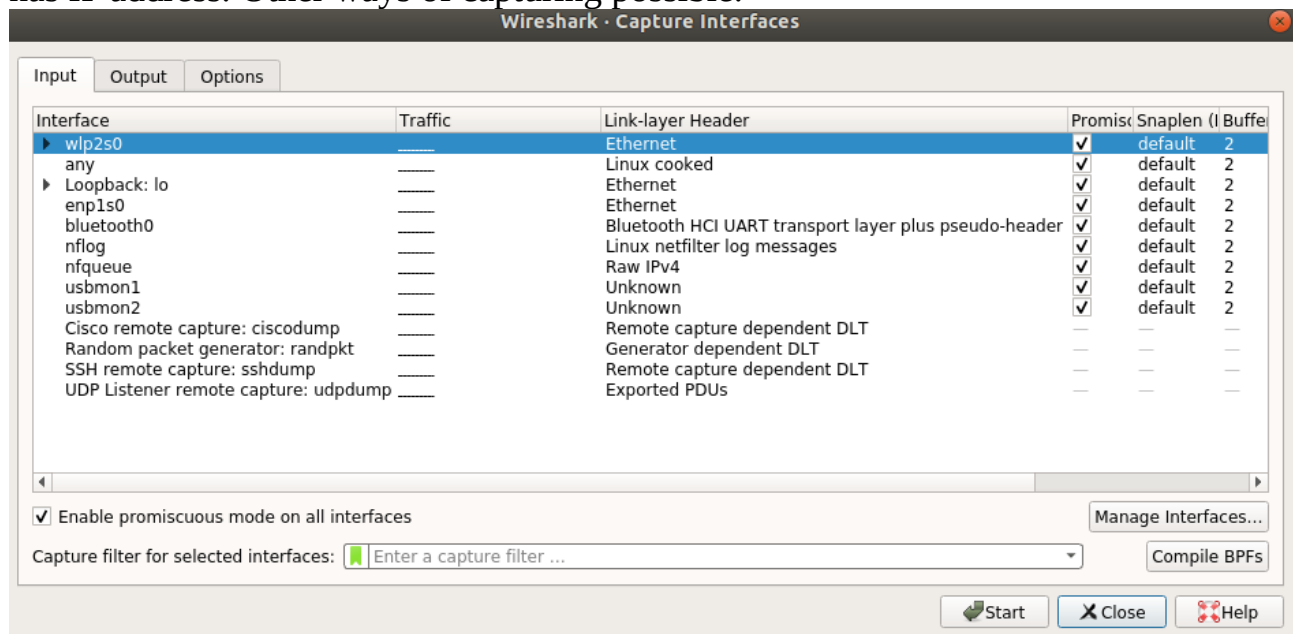
step-2: when show this interface. Select yes and press enter.



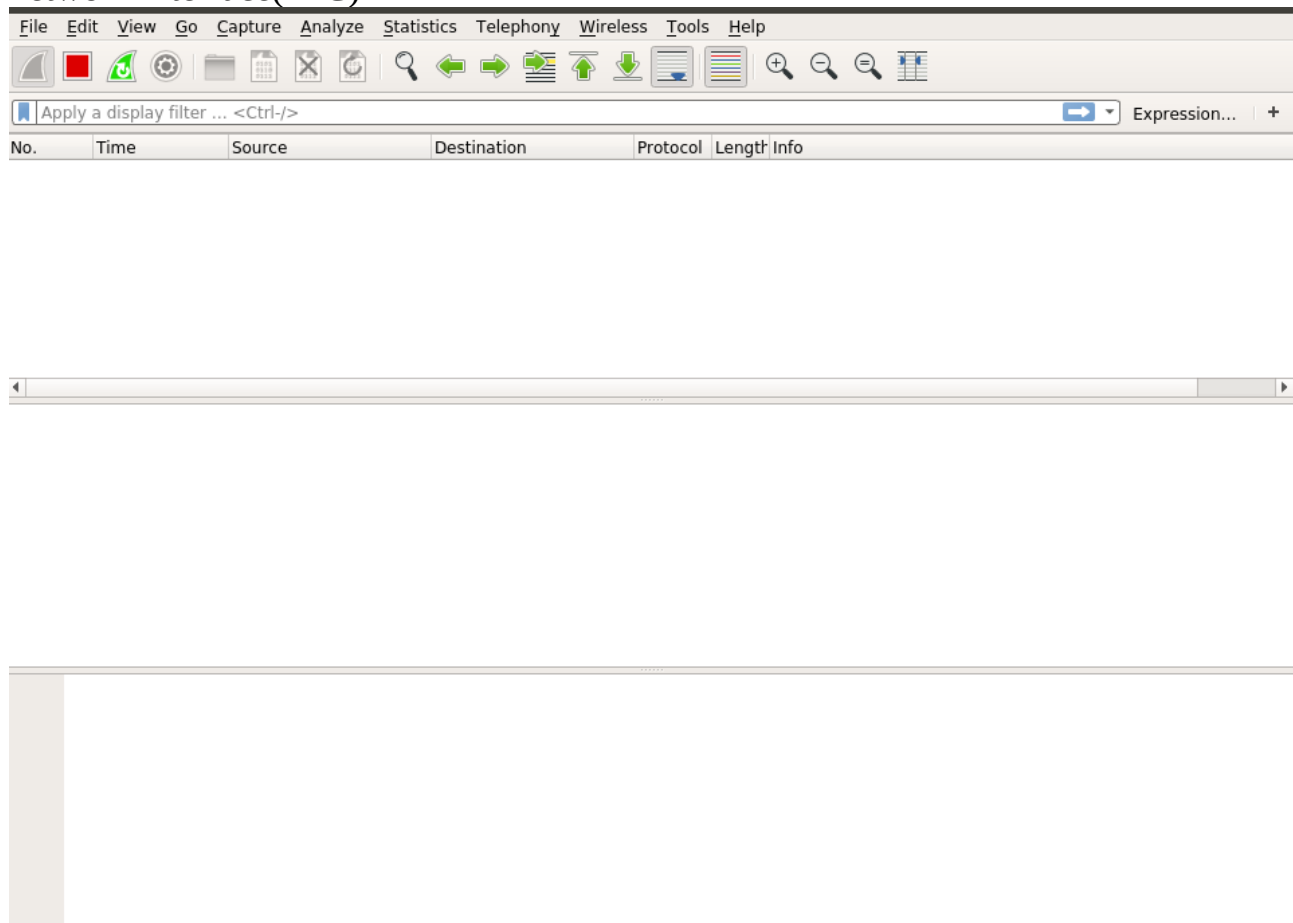
Wireshark usage:



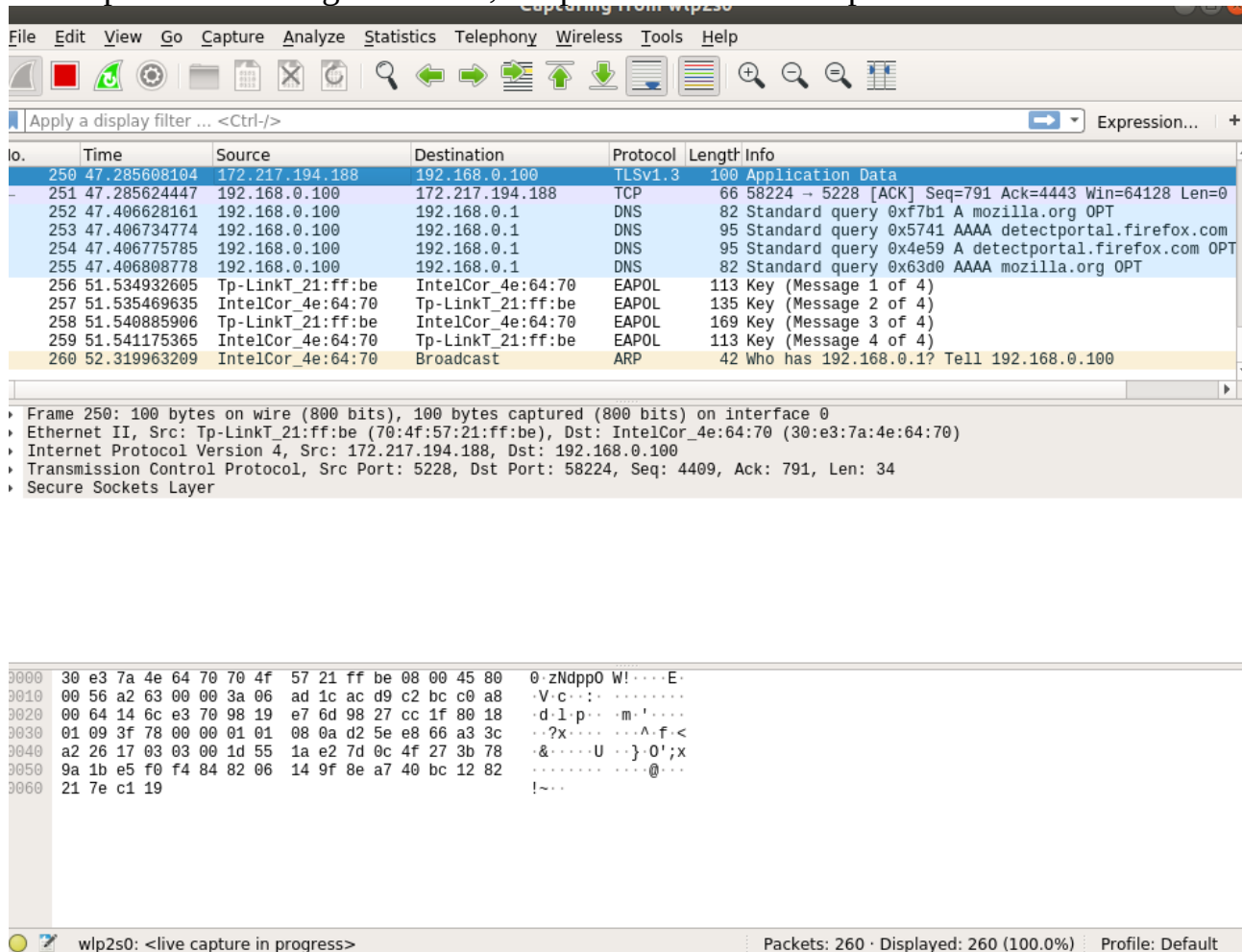
To capture: go to capture menu and select options. Start capturing on interface that has IP address. Other ways of capturing possible.



once the capturing starts, main window will be blank until the data is exchanged on network interface(NIC)



When packets exchanged on NIC, the packets will be dumped to main window.



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

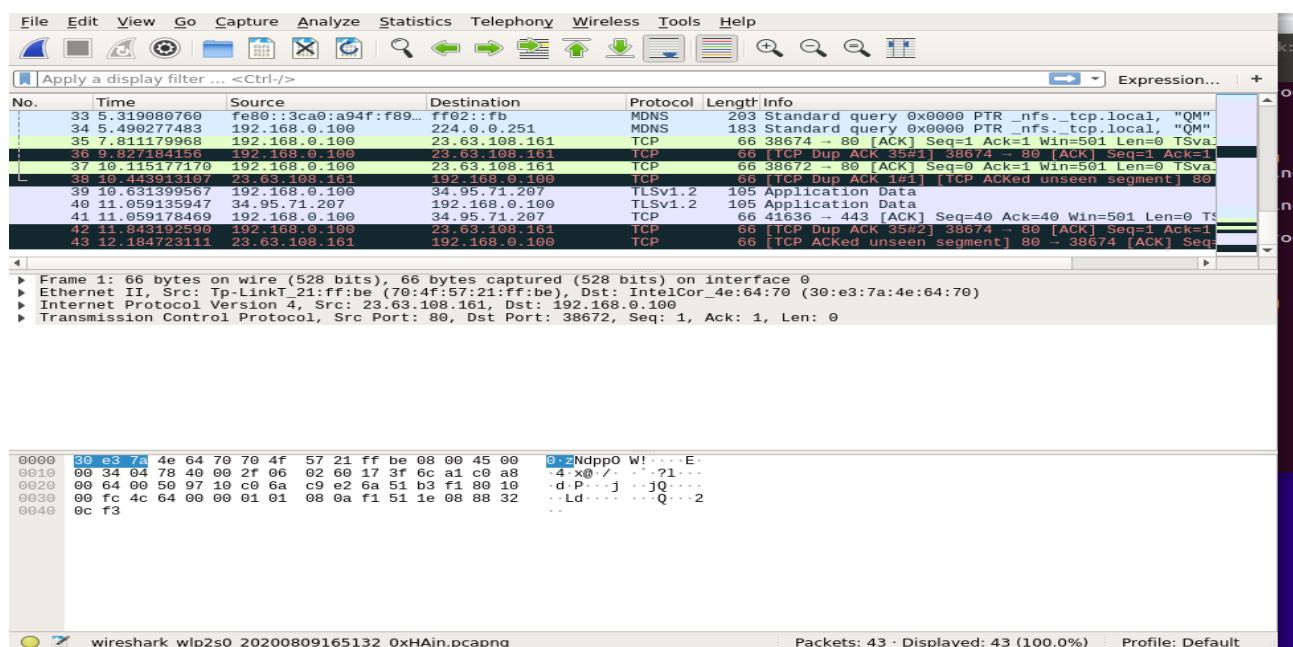
Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
250	47.285608104	172.217.194.188	192.168.0.100	TLSv1.3	100	Application Data
251	47.285624447	192.168.0.100	172.217.194.188	TCP	66	58224 → 5228 [ACK] Seq=791 Ack=4443 Win=64128 Len=0
252	47.406628161	192.168.0.100	192.168.0.1	DNS	82	Standard query 0xf7b1 A mozilla.org OPT
253	47.406734774	192.168.0.100	192.168.0.1	DNS	95	Standard query 0x5741 AAAA detectportal.firefox.com OPT
254	47.406775785	192.168.0.100	192.168.0.1	DNS	95	Standard query 0x4e59 A detectportal.firefox.com OPT
255	47.406808778	192.168.0.100	192.168.0.1	DNS	82	Standard query 0x63d0 AAAA mozilla.org OPT
256	51.534932605	Tp-LinkT_21:ff:be	IntelCor_4e:64:70	EAPOL	113	Key (Message 1 of 4)
257	51.535469635	Tp-LinkT_21:ff:be	IntelCor_4e:64:70	EAPOL	135	Key (Message 2 of 4)
258	51.540885906	Tp-LinkT_21:ff:be	IntelCor_4e:64:70	EAPOL	169	Key (Message 3 of 4)
259	51.541175365	IntelCor_4e:64:70	Tp-LinkT_21:ff:be	EAPOL	113	Key (Message 4 of 4)
260	52.319963209	IntelCor_4e:64:70	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.100

Frame 250: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0
Ethernet II, Src: Tp-LinkT_21:ff:be (70:4f:57:21:ff:be), Dst: IntelCor_4e:64:70 (30:e3:7a:4e:64:70)
Internet Protocol Version 4, Src: 172.217.194.188, Dst: 192.168.0.100
Transmission Control Protocol, Src Port: 5228, Dst Port: 58224, Seq: 4409, Ack: 791, Len: 34
Secure Sockets Layer

wlp2s0: <live capture in progress> Packets: 260 · Displayed: 260 (100.0%) Profile: Default

Capturing can be stopped by clicking on stop the running capture button on the main toolbar.



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
33	5.319080760	ff80::3ca0:a94f:f89...	ff02::fb	MDNS	203	Standard query 0x0000 PTR _nfs._tcp.local, "QM"
34	5.490277483	192.168.0.100	224.0.0.251	MDNS	183	Standard query 0x0000 PTR _nfs._tcp.local, "QM"
35	7.811179968	192.168.0.100	23.63.108.161	TCP	66	38674 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=...
36	9.822610190	192.168.0.100	23.63.108.161	TCP	66	[TCP Dup ACK 35#2] 38674 → 80 [ACK] Seq=1 Ack=1
37	10.115177170	192.168.0.100	23.63.108.161	TCP	66	38672 → 80 [ACK] Seq=0 Ack=1 Win=501 Len=0 [Sval=...
38	10.443913107	23.63.108.161	192.168.0.100	TCP	66	[TCP Dup ACK 1#1] [TCP ACKed unseen segment] 80
39	10.631399567	192.168.0.100	34.95.71.207	TLSv1.2	105	Application Data
40	11.059135947	34.95.71.207	192.168.0.100	TLSv1.2	105	Application Data
41	11.059178469	192.168.0.100	34.95.71.207	TCP	66	41636 → 443 [ACK] Seq=40 Ack=40 Win=501 Len=0 TS...
42	11.843192590	192.168.0.100	23.63.108.161	TCP	66	[TCP Dup ACK 35#2] 38674 → 80 [ACK] Seq=1 Ack=1
43	12.184723111	23.63.108.161	192.168.0.100	TCP	66	[TCP ACKed unseen segment] 80 → 38674 [ACK] Seq=...

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Tp-LinkT_21:ff:be (70:4f:57:21:ff:be), Dst: IntelCor_4e:64:70 (30:e3:7a:4e:64:70)
Internet Protocol Version 4, Src: 23.63.108.161, Dst: 192.168.0.100
Transmission Control Protocol, Src Port: 80, Dst Port: 38672, Seq: 1, Ack: 1, Len: 0

wireshark_wlp2s0_20200809165132_0xHAjn.pcapng Packets: 43 · Displayed: 43 (100.0%) Profile: Default

File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help

http
Expression...

No.	Time	Source	Destination	Protocol	Length	Info
3	0.590639880	192.168.0.100	172.217.163.67	TCP	66	56738 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=11
4	0.636555723	172.217.163.67	192.168.0.100	TCP	66	[TCP ACKed unseen segment] 443 → 56738 [ACK] Seq=1 A
5	2.638642440	192.168.0.100	172.217.167.131	TCP	66	41492 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=26
6	2.638685021	192.168.0.100	172.217.167.131	TCP	66	41494 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=26
7	2.638695507	192.168.0.100	74.125.68.188	TCP	66	38032 → 5228 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=7
8	2.686837131	172.217.167.131	192.168.0.100	TCP	66	[TCP ACKed unseen segment] 443 → 41492 [ACK] Seq=1 A
9	2.687810536	172.217.167.131	192.168.0.100	TCP	66	[TCP ACKed unseen segment] 443 → 41494 [ACK] Seq=1 A
10	2.742953391	74.125.68.188	192.168.0.100	TCP	66	[TCP ACKed unseen segment] 5228 → 38032 [ACK] Seq=1
11	4.690655895	192.168.0.100	142.250.67.46	TCP	66	41456 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=19
12	4.690827747	192.168.0.100	142.250.67.46	TCP	66	41420 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=19
13	4.763199875	142.250.67.46	192.168.0.100	TCP	66	[TCP ACKed unseen segment] 443 → 41456 [ACK] Seq=1 A

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

Ethernet II, Src: Tp-LinkT_21:ff:be (70:4f:57:21:ff:be), Dst: IntelCor_4e:64:70 (30:e3:7a:4e:64:70)

Address Resolution Protocol (request)

```

0000  30 e3 7a 4e 64 70 70 4f 57 21 ff be 08 06 00 01  0-zNdp0 W!.....
0010  08 00 06 04 00 01 70 4f 57 21 ff be c0 a8 00 01  .....p0 W!.....
0020  00 00 00 00 00 00 c0 a8 00 64                   .....d

```

wlp2s0: <live capture in progress>
Packets: 13 · Displayed: 13 (100.0%)
Profile: Default

- Packets and protocols can be analysed after capture.
- Individual fields in protocols can be easily seen.
- Graphs and flow diagrams can be helpful in analysis

Analysis is performed manually

Packet details pane

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
555	191.097689278	172.217.163.195	192.168.0.100	TCP	66	[TCP Keep-Alive ACK] 443 → 49140 [ACK] Seq=1912 Ack=
556	191.187108846	142.250.67.46	192.168.0.100	TCP	66	[TCP Keep-Alive ACK] 443 → 41420 [ACK] Seq=2068 Ack=
557	192.106168235	Tp-LinkT_21:ff:be	IntelCor_4e:64:70	ARP	42	Who has 192.168.0.100? Tell 192.168.0.1
558	192.106192402	IntelCor_4e:64:70	Tp-LinkT_21:ff:be	ARP	42	192.168.0.100 is at 30:e3:7a:4e:64:70

Frame 481: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

- Ethernet II, Src: Tp-LinkT_21:ff:be (70:4f:57:21:ff:be), Dst: IntelCor_4e:64:70 (30:e3:7a:4e:64:70)
 - Destination: IntelCor_4e:64:70 (30:e3:7a:4e:64:70)
 - Source: Tp-LinkT_21:ff:be (70:4f:57:21:ff:be)
 - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 23.63.108.161, Dst: 192.168.0.100
- Transmission Control Protocol, Src Port: 80, Dst Port: 39026, Seq: 409, Ack: 297, Len: 0
 - Source Port: 80
 - Destination Port: 39026
 - [Stream index: 13]
 - [TCP Segment Len: 0]
 - Sequence number: 409 (relative sequence number)
 - [Next sequence number: 409 (relative sequence number)]
 - Acknowledgment number: 297 (relative ack number)
 - 1000 ... = Header Length: 32 bytes (8)
 - Flags: 0x010 (ACK)
 - Window size value: 235
 - [Calculated window size: 30000]
 - [Window size scaling factor: 128]
 - Checksum: 0xce37 [unverified]
 - [Checksum Status: Unverified]
 - Urgent pointer: 0
 - Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
 - [SEQ/ACK analysis]
 - [Timestamps]

0000 30 e3 7a 4e 64 70 70 4f 57 21 ff be 08 00 45 00 0 ·zNdp0 W! ····E·

0010 00 34 68 bb 40 00 2f 06 9e 1c 17 3f 6c a1 c0 a8 ·4h·@·/· ···?1···

0020 00 64 00 50 98 72 fe d9 95 ef a2 92 0e e9 80 10 ·d·P·r· ······

0030 00 eb ce 37 00 00 01 01 08 0a f1 54 30 09 88 34 ···7···· ···T0··4

0040 da 13 ..

packet Byte pane consists of offset, Hex and ASCII fields.

Packet Byte pane

0000 30 e3 7a 4e 64 70 70 4f 57 21 ff be 08 00 45 00 0 ·zNdp0 W! ····E·

0010 00 34 68 bb 40 00 2f 06 9e 1c 17 3f 6c a1 c0 a8 ·4h·@·/· ···?1···

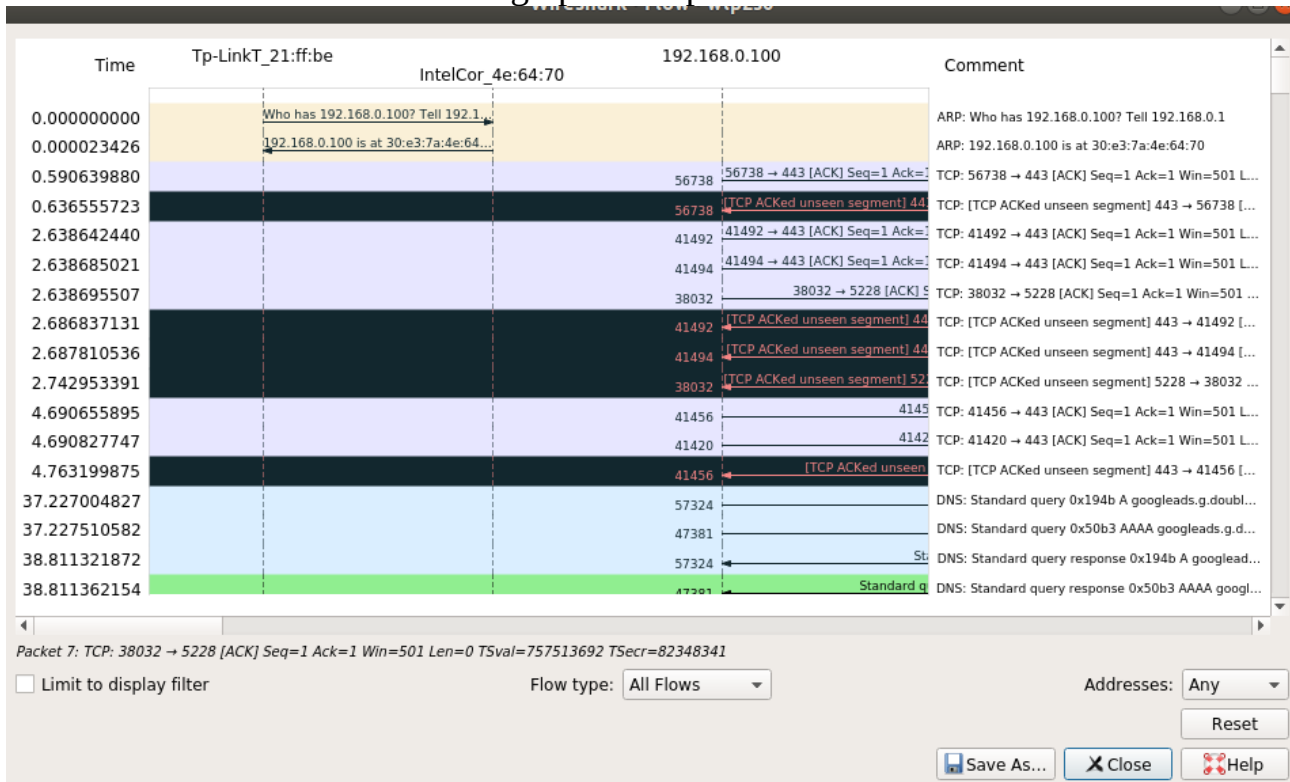
0020 00 64 00 50 98 72 fe d9 95 ef a2 92 0e e9 80 10 ·d·P·r· ······

0030 00 eb ce 37 00 00 01 01 08 0a f1 54 30 09 88 34 ···7···· ···T0··4

0040 da 13 ..

Tcp plots and flow graph are available in statistics menu.

Statistics- Flow graph example



Discussion: In this lab we know about wireshark, how to install wireshark, how to use woreshark, and protocol and TCP analysis. I faced some problem butget help help internet for solve.