



AIM: Perform Packet Capture and Sniff IP traffic using Wireshark.

Experiment 1A

Shantanu Shah

16551220126

Therion Camp 2

Aim: Perform packet capture and sniff IP traffic using Wireshark.

Theory: Packet sniffers intercept packets of data flowing across a computer network in order to view their contents. This act is called packet sniffing.

Web pages and emails are not sent through the internet as one document, rather the sending side breaks them down into many little data packets. These packets are then addressed to an IP address at the receiving end, which has to send back an acknowledgment of each packet it receives.

These packets are not transferred from the sender to the receiver through a single direct connection instead, as each packet traverses the internet enroute to its destination, it passes through a number of ~~router~~ control devices such as routers and switches. Each time a packet passes through one of these ~~router~~ control devices, it is susceptible to capture and analysis.

Anyone who has access to a router can perform packet collection and subsequent analysis. ~~Wireshark~~ ~~sniffers~~ ~~are~~ ~~examples~~ of packet sniffing tools.

Shantanu Shah

Conclusion: Thus, we have performed packet capture and sniffed IP traffic using Wireshark.

Capturing ICMP Packets:

C:\Users\Marwin Shroff>ping 8.8.8.8 Pinging 8.8.8.8 with 32 bytes of data: Reply from 8.8.8.8: bytes=32 time=5ms TTL=119

Reply from 8.8.8.8: bytes=32 time=6ms

TTL=119 Reply from 8.8.8.8: bytes=32

time=2ms TTL=119

Reply from 8.8.8.8: bytes=32 time=3ms TTL=119 Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 2ms, Maximum = 6ms, Average = 4ms

The image shows a Wireshark packet capture interface. The top pane displays a list of captured packets. The bottom pane shows the details of the selected packet (Frame 1: 1494 bytes on wire).

No.	Time	Source	Destination	Protocol	Length	Info
1494	0.000000	172.67.7.42	192.168.0.175	TCP	1494	443 → 53989 [ACK] Seq=877485 Ack=618 Win=246 Len=1440 [TCP segment of a reassembled PDU]
1495	0.000000	172.67.7.42	192.168.0.175	TCP	1494	443 → 53989 [ACK] Seq=878925 Ack=618 Win=246 Len=1440 [TCP segment of a reassembled PDU]
1496	0.000000	172.67.7.42	192.168.0.175	TCP	1494	443 → 53989 [ACK] Seq=880365 Ack=618 Win=246 Len=1440 [TCP segment of a reassembled PDU]
1497	0.000000	172.67.7.42	192.168.0.175	TLSv1.2	506	Application Data, Application Data
1498	0.000000	192.168.0.175	172.67.7.42	TCP	54	53989 → 443 [ACK] Seq=618 Ack=882257 Win=2056 Len=0
1499	0.000000	192.168.0.175	172.67.7.42	TLSv1.2	310	Application Data
1500	0.000000	172.67.7.42	192.168.0.175	TCP	54	443 → 53989 [ACK] Seq=882257 Ack=874 Win=248 Len=0
1501	0.000000	192.168.0.171	224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.251
1502	0.000000	192.168.0.171	224.0.0.251	MDNS	171	Standard query 0x0000 PTR lb._dns-sd._udp.local, "QU" question PTR _companion-link._tcp.local, "QU" question PTR _homekit._tcp.lo...
1503	0.000000	fe80::842:3734:857a::fb	ff02::fb	MDNS	191	Standard query 0x0000 PTR lb._dns-sd._udp.local, "QU" question PTR _companion-link._tcp.local, "QU" question PTR _homekit._tcp.lo...
1504	0.000000	192.168.0.175	3.108.46.16	TLSv1.2	108	Application Data
1505	0.000000	3.108.46.16	192.168.0.175	TCP	54	443 → 56718 [ACK] Seq=1241 Ack=165 Win=10 Len=0
1506	0.000000	3.108.46.16	192.168.0.175	TLSv1.2	110	Application Data
1507	0.000000	192.168.0.175	3.108.46.16	TCP	54	56718 → 443 [ACK] Seq=165 Ack=1297 Win=512 Len=0
1508	0.000000	192.168.0.171	224.0.0.251	MDNS	215	Standard query 0x0000 ANY Rahat Altarf Girkar._rdlink._tcp.local, "QU" question ANY Rahat-Altarf-Girkar.local, "QU" question SRV 0 ...
1509	0.000000	fe80::842:3734:857a::fb	ff02::fb	MDNS	235	Standard query 0x0000 ANY Rahat Altarf Girkar._rdlink._tcp.local, "QU" question ANY Rahat-Altarf-Girkar.local, "QU" question SRV 0 ...
1510	0.000000	192.168.0.171	224.0.0.251	MDNS	215	Standard query 0x0000 ANY Rahat Altarf Girkar._rdlink._tcp.local, "QU" question ANY Rahat-Altarf-Girkar.local, "QU" question SRV 0 ...
1511	0.000000	fe80::842:3734:857a::fb	ff02::fb	MDNS	235	Standard query 0x0000 ANY Rahat Altarf Girkar._rdlink._tcp.local, "QU" question ANY Rahat-Altarf-Girkar.local, "QU" question SRV 0 ...
1512	0.000000	192.168.0.171	224.0.0.251	MDNS	215	Standard query 0x0000 ANY Rahat Altarf Girkar._rdlink._tcp.local, "QU" question ANY Rahat-Altarf-Girkar.local, "QU" question SRV 0 ...

Frame 1: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface \Device\NPF_{90485C55-6194-4E36-A1C7-32FBE1728C0}, id 0
Ethernet II, Src: Tp-LinkT_89:e7:a8 (d8:07:b6:89:e7:a8), Dst: IntelCor_d6:31:6b (40:74:e0:d6:31:6b)
Internet Protocol Version 4, Src: 172.67.7.42, Dst: 192.168.0.175
Transmission Control Protocol, Src Port: 443, Dst Port: 53989, Seq: 1, Ack: 1, Len: 1440

0000 40 74 e0 d6 31 6b d8 07 b6 89 e7 a8 08 00 45 00 @t-1k...E-
0010 05 c8 e9 7f 40 00 35 06 e1 eb ac 43 07 2a c0 a8 ...@S...C*..
0020 00 af 01 b0 d2 e5 9c 19 9e 18 09 8c 44 7c 50 10D[P..
0030 00 f5 5d 0f 00 00 17 03 03 20 1a 21 cc 08 9e f2 ...J.....l....
0040 9c e0 a6 0c 81 c1 2e 79 6c 64 86 7c 06 a4 1d b5y ld {...
0050 2f 9b 66 ec 3c 18 00 60 91 04 28 0e d4 04 7b 5c /-f-c-...(\..
0060 2b 32 91 80 d6 82 87 a4 62 64 08 5c af a3 fc 1f +2.....bd\..
0070 1d 52 40 4a 28 67 38 4f 1a 0f 99 a6 67 a5 3c 5d .R0(g80...F-E..
0080 04 78 2e 95 10 74 e2 ad 6b a0 ce 02 92 24 f3 32 .x...t...k...\$2
0090 f4 78 b1 0d d3 ea 26 a4 2d d6 82 47 9b a0 a2 84 .x...&...G...
00a0 b8 fe 2c ff e3 23 00 d6 51 59 be 34 64 ed 09 f3 ...>...QY Ad...
00b0 da 6d 1d 8d 13 3e 83 2e 58 9c 4c 23 21 cb 33 28 .m...>...X l@l 3(
00c0 85 ee 6f b5 68 c0 63 04 d8 12 1c 3d da 54 e2 29 ...o h c...-T..
00d0 8a d8 43 ff e0 67 0a 58 63 72 cc 79 8e 12 0a 13 ...C g X c r y...

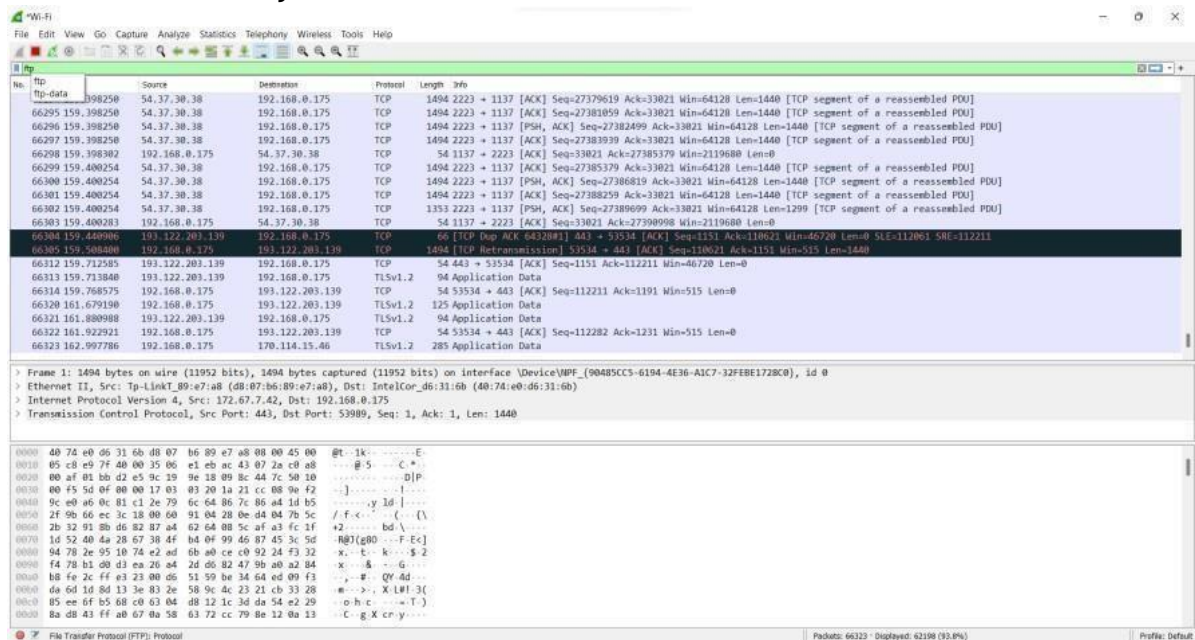
Capturing TCP Packets:

The image shows a Wireshark packet capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The main window is divided into three panes:

- Packet List:** A table showing captured packets. The first column is 'No.', the second is 'Time', the third is 'Source', the fourth is 'Destination', the fifth is 'Protocol', and the sixth is 'Length'. The packets are all TCP segments of a reassembled PDU, with sequence numbers ranging from 4521840 to 4540560.
- Packet Details:** A pane showing the structure of the selected packet (No. 1). It includes the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header.
- Packet Bytes:** A pane showing the raw bytes of the selected packet in hexadecimal and ASCII format.

The bottom status bar indicates that 23836 packets are displayed, representing 21084 (88.5%) of the total capture. The profile is set to 'Default'.

```
C:\Users\Marwin Shroff>ftp ftp.cdc.gov Connected to
ftp.cdc.gov. 220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding
now ON. User (ftp.cdc.gov:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as
password. Password: 230 User logged in.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection.
.change.dir .message pub Readme
Siteinfo w3c welcome.msg 226 Transfer complete. ftp: 67 bytes received in
0.03Seconds 2.03Kbytes/sec.
```



The image displays a Wireshark packet capture of a network traffic analysis. The top pane shows a list of captured packets, with packet 71611 selected. The middle pane shows the details of the selected packet, which is a TCP segment. The bottom pane shows the raw hex and ASCII data of the packet. The packet list shows a sequence of packets from 71609 to 71647. The packet details pane shows the structure of the TCP segment and the application data. The packet bytes pane shows the raw hex and ASCII data.

No.	Time	Source	Destination	Protocol	Length	Info
71609	183.560720	54.37.30.38	192.168.0.175	TCP	1494	2223 → 1137 [ACK] Seq=32540819 Ack=40091 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
71610	183.561608	54.37.30.38	192.168.0.175	TCP	1494	2223 → 1137 [ACK] Seq=32542259 Ack=40091 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
71611	183.561608	54.37.30.38	192.168.0.175	TLSv1.2	1494	Application Data [TCP segment of a reassembled PDU]
71612	183.561608	54.37.30.38	192.168.0.175	TCP	1494	2223 → 1137 [ACK] Seq=32540819 Ack=40091 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
71613	183.561608	54.37.30.38	192.168.0.175	TCP	1494	2223 → 1137 [PSH, ACK] Seq=32546579 Ack=40091 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
71614	183.561618	192.168.0.175	54.37.30.38	TCP	54	1137 → 2223 [ACK] Seq=40091 Ack=32540819 Win=2119680 Len=0
71615	183.562675	54.37.30.38	192.168.0.175	TLSv1.2	1494	Application Data [TCP segment of a reassembled PDU]
71616	183.562675	54.37.30.38	192.168.0.175	TCP	1494	2223 → 1137 [ACK] Seq=32549459 Ack=40091 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
71617	183.562675	54.37.30.38	192.168.0.175	TCP	1494	2223 → 1137 [ACK] Seq=32550899 Ack=40091 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
71618	183.562675	54.37.30.38	192.168.0.175	TLSv1.2	1494	Application Data [TCP segment of a reassembled PDU]
71619	183.562689	192.168.0.175	54.37.30.38	TCP	54	1137 → 2223 [ACK] Seq=40091 Ack=32553779 Win=2119680 Len=0
71620	183.562686	54.37.30.38	192.168.0.175	TCP	1494	2223 → 1137 [ACK] Seq=32553779 Ack=40091 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
71621	183.562866	54.37.30.38	192.168.0.175	TLSv1.2	674	Application Data
71622	183.562881	192.168.0.175	54.37.30.38	TCP	54	1137 → 2223 [ACK] Seq=40091 Ack=32555839 Win=2119680 Len=0
71637	183.944243	192.168.0.175	172.67.72.209	TCP	55	[TCP Keep-Alive] 1134 + 443 [ACK] Seq=1181 Ack=37347 Win=131584 Len=1
71638	183.948275	172.67.72.209	192.168.0.175	TCP	66	[TCP Keep-Alive] 443 + 1134 [ACK] Seq=37347 Ack=1182 Win=71680 Len=0 SLE=1181 SRE=1182
71644	184.060454	192.168.0.175	193.122.203.139	TLSv1.2	1454	Application Data
71646	184.273264	193.122.203.139	192.168.0.175	TLSv1.2	93	Application Data
71647	184.322728	192.168.0.175	193.122.203.139	TCP	54	53534 + 443 [ACK] Seq=120757 Ack=1431 Min=514 Len=0

Packet 1: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface \Device\NPF{90485CC5-6194-4E36-A3C7-32FE8E128C0B}, id 0
 Ethernet II, Src: Tc-Link#0:87:a8 (d8:07:b6:89:e7:a8), Dst: IntelCor_d6:31:6b (d0:74:e0:d6:31:6b)
 Internet Protocol Version 4, Src: 172.67.72.209, Dst: 192.168.0.175
 Transmission Control Protocol, Src Port: 443, Dst Port: 53989, Seq: 1, Ack: 1, Len: 1440

0000 40 74 e0 d6 31 6b d8 07 b6 89 e7 a8 08 00 45 00 #t-1k-...-E-
 0010 05 c8 e9 7f 40 00 35 06 1e c0 a4 03 87 2a c0 a8 #-5-...C-
 0020 00 af 01 b5 d0 e5 9c 19 9c 18 09 8c 44 7c 50 18 0-...-DIP-
 0030 00 f5 54 00 00 17 03 03 20 1a 21 c0 08 0e f2 --...-Id-
 0040 9c e0 a6 ec 3c 08 00 91 04 28 06 04 04 70 5c -F-...C-D-
 0050 2f 9b 06 ec 3c 08 00 91 04 28 06 04 04 70 5c -F-...C-D-
 0060 2b 32 91 05 05 82 87 a4 62 64 08 5c af a3 fc f -z-...-bd-
 0070 1d 52 40 4a 28 67 38 4f b4 0f 99 46 87 45 3c 54 -R0-...-F-
 0080 54 78 2e 95 70 70 00 00 00 00 00 00 00 00 00 00 -...-k-...-F-
 0090 f4 78 1b d0 d3 e6 26 a4 2d 06 82 47 9b a0 e2 84 -x-...-G-
 0100 b8 fe 2c ff 23 00 06 51 59 b6 34 24 64 ed 09 f3 -...-QV-
 0110 d6 6d 1d 8d 13 2e 83 2e 58 9c 4c 23 21 cb 33 28 -m-...-X-
 0120 85 ee 6f b5 68 cb 63 a4 d8 12 3d 3d 54 54 29 29 -o-...-T-
 0130 8a d3 4f f0 67 0a 58 63 72 cc 79 8e 12 0a 13 -C-...-X-
 0140

1] Filter Results by Port:

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
10205	55.181214	192.168.0.175	23.47.229.231	TCP	66	1139 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
10206	55.183774	23.47.229.231	192.168.0.175	TCP	66	80 → 1139 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
10209	55.185835	192.168.0.175	23.47.229.231	TCP	54	1139 → 80 [ACK] Seq=1 Ack=1 Wln=132352 Len=0
10210	55.193880	192.168.0.175	23.47.229.231	HTTP	450	GET /WP/EvtSBNWswGTA3BgUvDgPKGtIABRBrZhwARTMRyEyspRAZsQfhagQQUgrMPZFOnB9xsJ13rK2f2ttk1V8BCHHXVSxwTWTLxp9eLa80K30 HTTP/1...
10213	55.187221	23.47.229.231	192.168.0.175	TCP	54	80 → 1139 [ACK] Seq=1 Ack=397 Wln=64128 Len=0
10217	55.189187	23.47.229.231	192.168.0.175	HTTP	413	HTTP/1.1 304 Not Modified
10220	55.194643	192.168.0.175	118.214.137.233	TCP	66	1140 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
10221	55.200316	118.214.137.233	192.168.0.175	TCP	66	80 → 1140 [SYN, ACK] Seq=0 Ack=1 Wln=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
10222	55.200809	192.168.0.175	118.214.137.233	TCP	54	1140 → 80 [ACK] Seq=1 Ack=1 Wln=132352 Len=0
10223	55.202184	192.168.0.175	118.214.137.233	HTTP	281	GET / HTTP/1.1
10224	55.205189	118.214.137.233	192.168.0.175	TCP	54	80 → 1140 [ACK] Seq=1 Ack=228 Wln=64128 Len=0
10225	55.205189	118.214.137.233	192.168.0.175	HTTP	317	HTTP/1.1 304 Not Modified
10234	55.238964	192.168.0.175	23.47.229.231	TCP	54	1139 → 80 [ACK] Seq=397 Ack=360 Wln=132096 Len=0
10245	55.254326	192.168.0.175	118.214.137.233	TCP	54	1140 → 80 [ACK] Seq=228 Ack=264 Wln=132096 Len=0
10250	55.284987	192.168.0.175	183.87.86.186	TCP	66	1141 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
10256	55.289006	183.87.86.186	192.168.0.175	TCP	66	80 → 1141 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
10261	55.289262	192.168.0.175	183.87.86.186	TCP	54	1141 → 80 [ACK] Seq=1 Ack=1 Wln=132352 Len=0
10262	55.289470	192.168.0.175	183.87.86.186	HTTP	263	GET /c/oca.cr1 HTTP/1.1
10263	55.291143	183.87.86.186	192.168.0.175	TCP	54	80 → 1141 [ACK] Seq=1 Ack=210 Wln=64128 Len=0
10264	55.304330	183.87.86.186	192.168.0.175	HTTP	361	METHOD: 1.304 Not Modified

- > Frame 10205: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{90485C55-6194-4E36-A1C7-32FEBE172BC0}, id 0
- > Ethernet II, Src: IntelCor_d6:31:0b (40:74:e0:d6:31:0b), Dst: Tp-Link_89:e7:a8 (d8:07:b6:89:e7:a8)
- > Internet Protocol Version 4, Src: 192.168.0.175, Dst: 23.47.229.231
- > Transmission Control Protocol, Src Port: 1139, Dst Port: 80, Seq: 0, Len: 0

```

0000 d8 07 b6 89 e7 a8 74 e0 d6 31 60 80 00 45 00 .....@T--ik...E-
0010 00 34 fe ac 40 00 00 06 00 00 c0 00 af 17 24 ....4n.....
0020 e7 e7 04 73 00 50 f0 e4 c0 00 00 00 00 00 02 ...$...
0030 fa f0 fe 94 00 02 04 05 b4 01 03 03 00 01 01 ...f...
0040 04 02
    
```

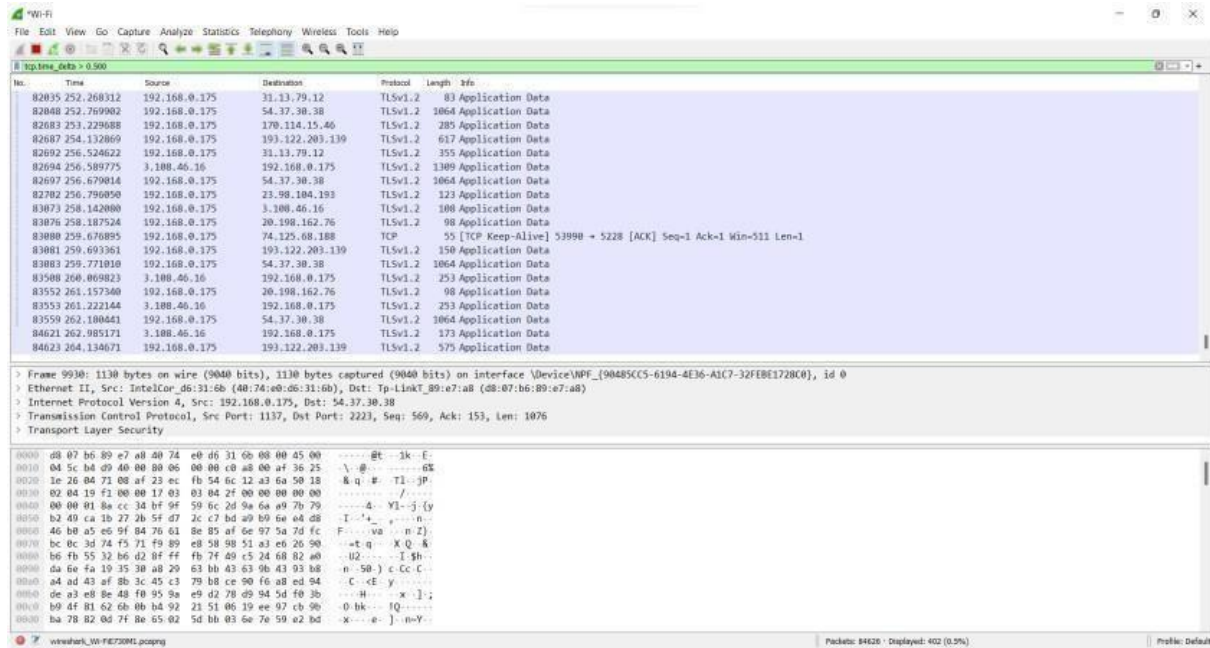
Bases 38-41: Sequence Number (seq) (tcp.seq raw)

Packets: 7778 - Downloaded: 52 (0.6%)

Profile: Default

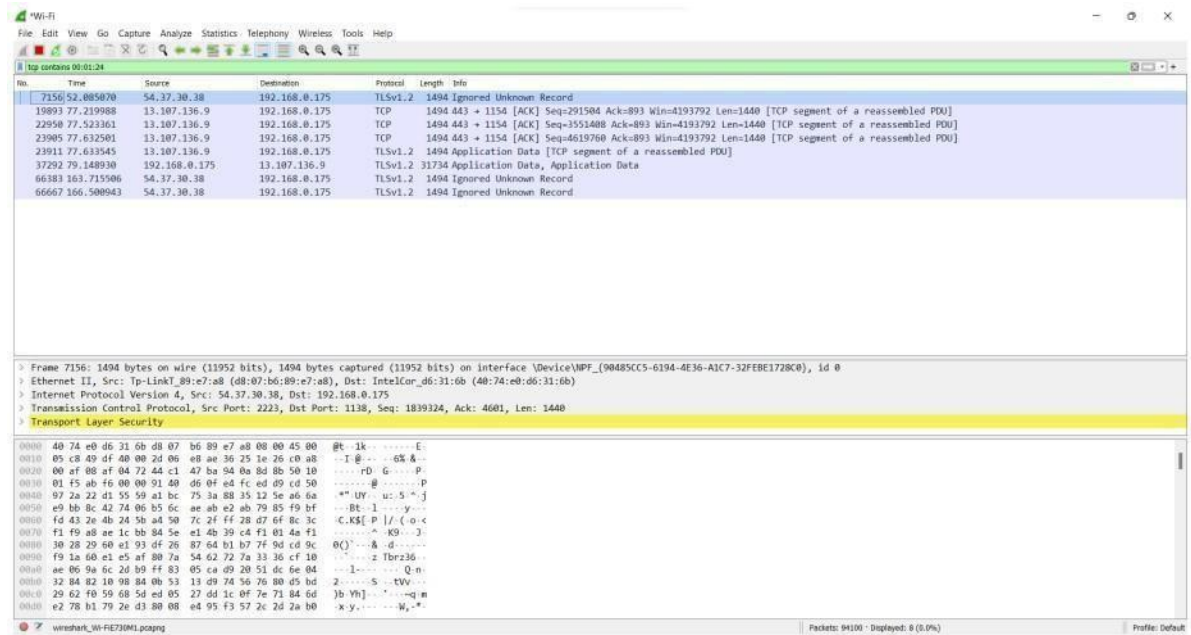
2] Filter by Delta Time :

Displays tcp packets with delta time of greater than 0.500 sec



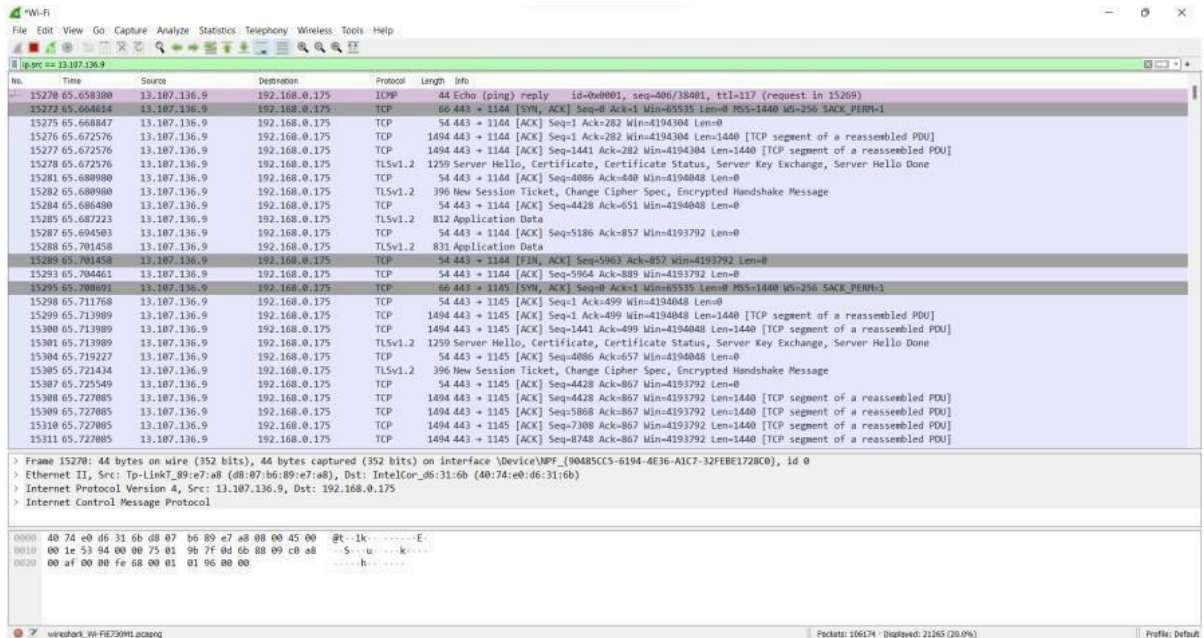
3] Filter by Byte Sequence:

Displays packets which contain a particular byte sequence.



4] Filter by Source IP Address:

Displays packets which have source IP address same as the one provided in the argument.



CONCLUSION

Thus, we have successfully studied packet sniffing tools (Wireshark) and explored how packets can be traced based on different filters