

## IS - Experiment 10 - Packet Sniffing using Wireshark

**Aim:** Study of packet sniffer tools: WireShark Download and install wireshark and capture icmp, tcp and http packets in promiscuous mode Explore how the packets can be traced based on different filters.

### Theory:

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark lets the user put network interface controllers into promiscuous mode (if supported by the network interface controller), so they can see all the traffic visible on that interface including unicast traffic not sent to that network interface controller's MAC address. However, when capturing with a packet analyzer in promiscuous mode on a port on a network switch, not all traffic through the switch is necessarily sent to the port where the capture is done, so capturing in promiscuous mode is not necessarily sufficient to see all network traffic. Port mirroring or various network taps extend capture to any point on the network. Simple passive taps are extremely resistant to tampering.

### 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

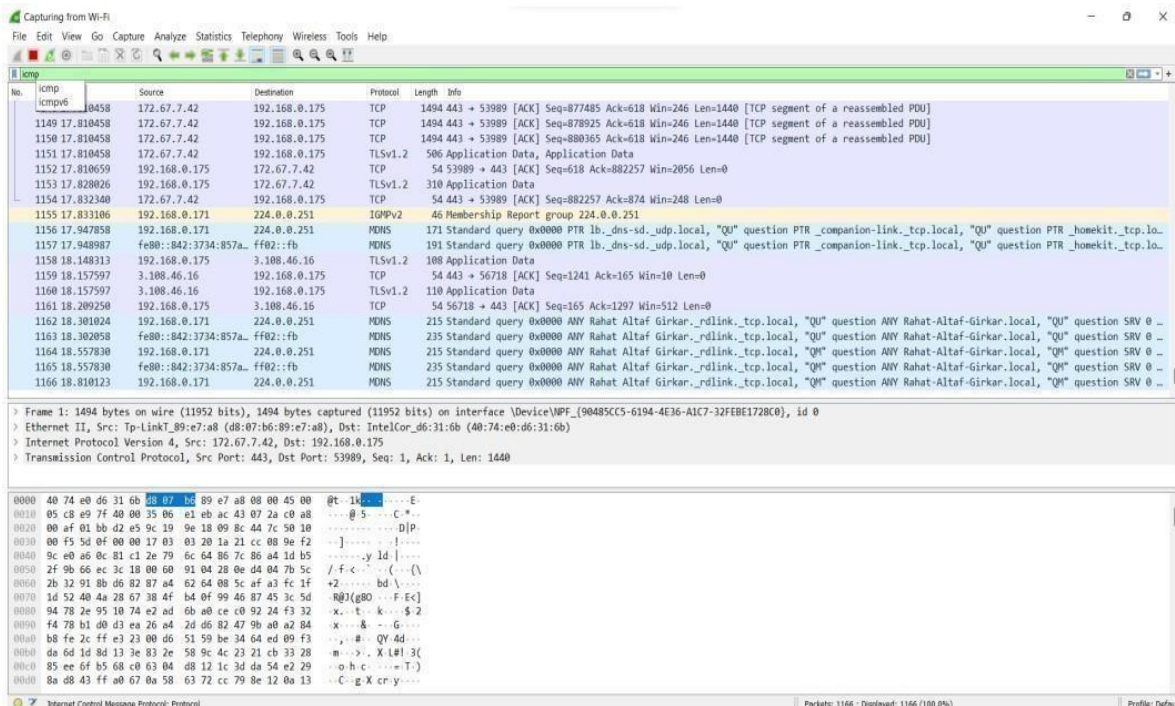
Reply from 8.8.8.8: bytes=32 time=6ms TTL=119

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



## Capturing TCP Packets:

A screenshot of the Wireshark network protocol analyzer. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The main display area shows a list of captured packets. The first packet is a TCP segment from 192.168.0.175 to 192.168.0.175, sequence number 149443, acknowledgment number 1154, and window size 1440. The packet is labeled as a 'TCP segment of a reassembled PDU'. Below the packet list, the packet details pane shows the structure of the TCP segment, including the header and the data payload. The packet bytes pane shows the raw data in hexadecimal and ASCII. The status bar at the bottom indicates that 23836 packets are displayed, representing 21094 (88.5%) of the capture.

## Capturing FTP Packets:

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.

A screenshot of the Wireshark network protocol analyzer showing a packet capture of an FTP session. The top menu bar is the same as the previous image. The main display area shows a list of captured packets. The first packet is a TCP segment from 192.168.0.175 to 192.168.0.175, sequence number 149443, acknowledgment number 1154, and window size 1440. The packet is labeled as a 'TCP segment of a reassembled PDU'. Below the packet list, the packet details pane shows the structure of the TCP segment, including the header and the data payload. The packet bytes pane shows the raw data in hexadecimal and ASCII. The status bar at the bottom indicates that 66323 packets are displayed, representing 62198 (93.8%) of the capture.



## Capturing ARP Packets:

The screenshot shows a Wireshark packet capture on the 'arp' filter. The packet list displays 16 packets, all of which are ARP requests (Type 1) from source IP 192.168.0.175 to destination IP 192.168.0.175. The packet details pane for the selected packet (No. 1647) shows the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header. The packet bytes pane shows the raw data in hexadecimal and ASCII.

## Tracing Packets based on filters:

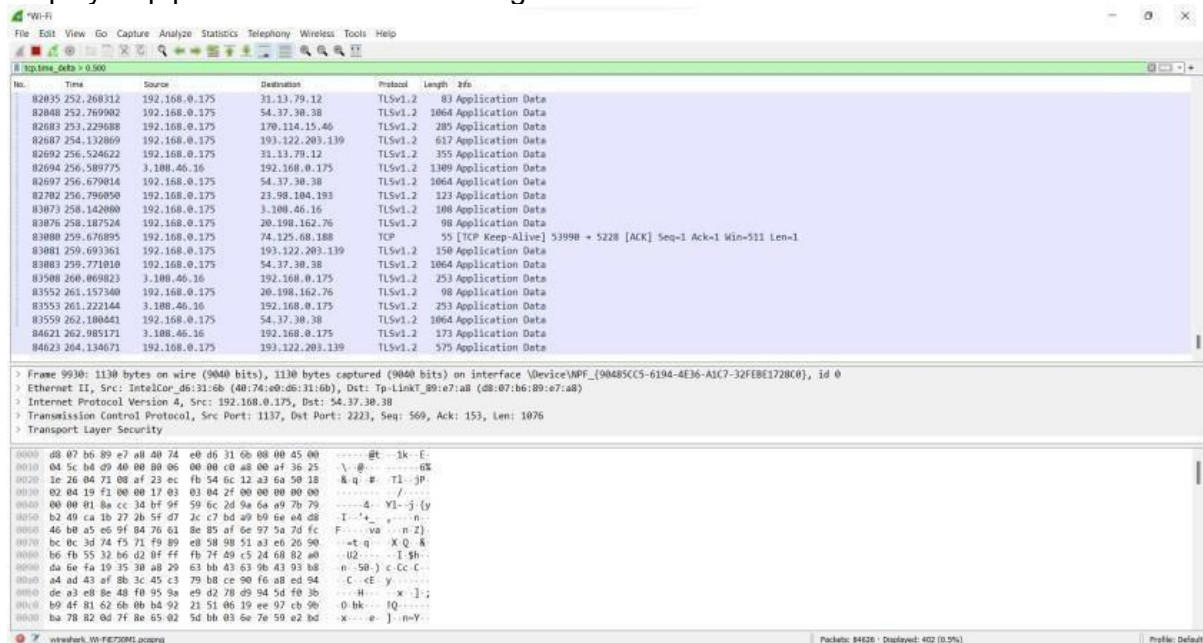
### 1. Filter Results by Port:

Traces all packets related to Port 80.

The screenshot shows a Wireshark packet capture on the 'tcp.port == 80' filter. The packet list displays 37 packets, all of which are related to port 80. The packet details pane for the selected packet (No. 10205) shows the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header. The packet bytes pane shows the raw data in hexadecimal and ASCII.

## 2. Filter by Delta Time:

Displays tcp packets with delta time of greater than 0.500 sec

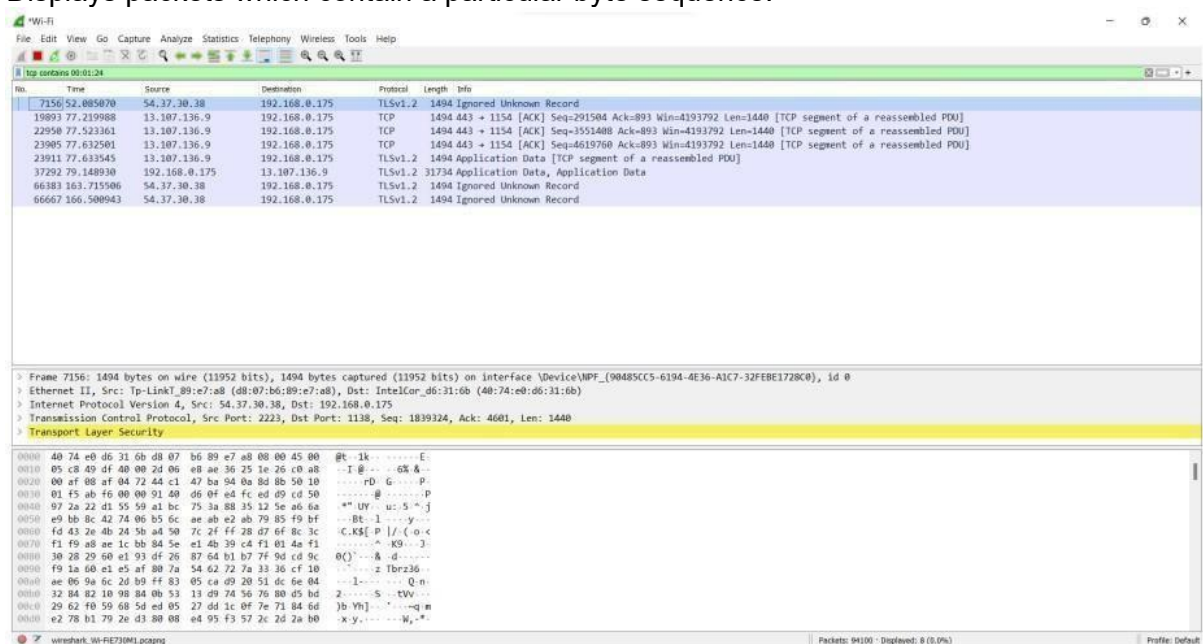


The screenshot shows the Wireshark interface with the filter bar set to `tcp.time_delta > 0.500`. The packet list displays 20 packets, all of which are TCP segments. The packet details pane shows the selected packet (9930) as an Ethernet II frame, an Internet Protocol Version 4 packet, and a Transmission Control Protocol (TCP) segment. The packet bytes pane shows the raw data of the selected packet.

| No.   | Time       | Source        | Destination     | Protocol | Length | Info  |
|-------|------------|---------------|-----------------|----------|--------|---|
| 82035 | 252.268312 | 192.168.0.175 | 31.13.79.12     | TLsv1.2  | 83     | Application Data  |
| 82048 | 252.269002 | 192.168.0.175 | 54.37.30.38     | TLsv1.2  | 1064   | Application Data  |
| 82083 | 253.229088 | 192.168.0.175 | 178.114.15.46   | TLsv1.2  | 285    | Application Data  |
| 82087 | 254.132069 | 192.168.0.175 | 193.122.203.139 | TLsv1.2  | 617    | Application Data  |
| 82692 | 256.524622 | 192.168.0.175 | 31.13.79.12     | TLsv1.2  | 355    | Application Data  |
| 82694 | 256.589775 | 3.108.46.16   | 192.168.0.175   | TLsv1.2  | 1309   | Application Data  |
| 82697 | 256.679814 | 192.168.0.175 | 54.37.30.38     | TLsv1.2  | 1064   | Application Data  |
| 82702 | 256.790050 | 192.168.0.175 | 23.98.104.193   | TLsv1.2  | 123    | Application Data  |
| 83073 | 258.142080 | 192.168.0.175 | 3.108.46.16     | TLsv1.2  | 108    | Application Data  |
| 83076 | 258.187524 | 192.168.0.175 | 20.198.162.76   | TLsv1.2  | 98     | Application Data  |
| 83080 | 259.670895 | 192.168.0.175 | 74.125.68.188   | TCP      | 55     | [TCP Keep-Alive] 53990 → 5228 [ACK] Seq=1 Ack=1 Win=511 Len=1 |
| 83081 | 259.693361 | 192.168.0.175 | 193.122.203.139 | TLsv1.2  | 150    | Application Data  |
| 83083 | 259.771010 | 192.168.0.175 | 54.37.30.38     | TLsv1.2  | 1064   | Application Data  |
| 83508 | 260.069823 | 3.108.46.16   | 192.168.0.175   | TLsv1.2  | 253    | Application Data  |
| 83552 | 261.157360 | 192.168.0.175 | 20.198.162.76   | TLsv1.2  | 98     | Application Data  |
| 83553 | 261.222144 | 3.108.46.16   | 192.168.0.175   | TLsv1.2  | 253    | Application Data  |
| 83559 | 262.180441 | 192.168.0.175 | 54.37.30.38     | TLsv1.2  | 1064   | Application Data  |
| 84621 | 262.985171 | 3.108.46.16   | 192.168.0.175   | TLsv1.2  | 173    | Application Data  |
| 84623 | 264.134071 | 192.168.0.175 | 193.122.203.139 | TLsv1.2  | 575    | Application Data  |

## 3. Filter by Byte Sequence:

Displays packets which contain a particular byte sequence.

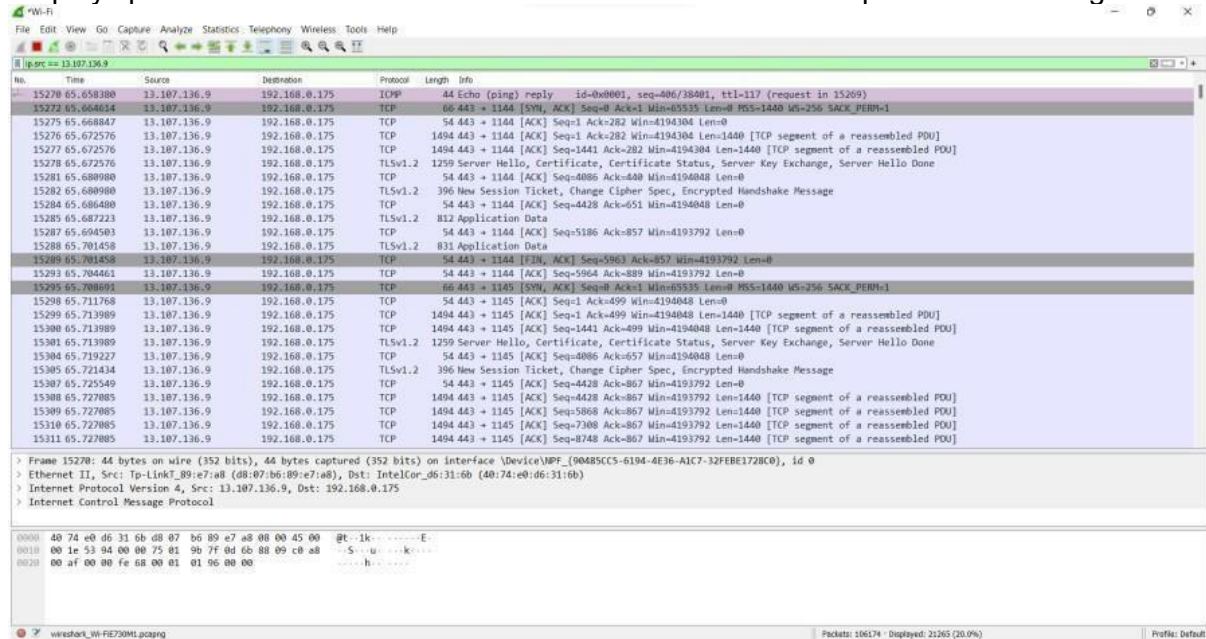


The screenshot shows the Wireshark interface with the filter bar set to `tcp.contains 00:01:24`. The packet list displays 10 packets, all of which are TCP segments. The packet details pane shows the selected packet (7156) as an Ethernet II frame, an Internet Protocol Version 4 packet, and a Transmission Control Protocol (TCP) segment. The packet bytes pane shows the raw data of the selected packet.

| No.   | Time       | Source        | Destination   | Protocol | Length | Info   |
|-------|------------|---------------|---------------|----------|--------|--|
| 7156  | 52.085670  | 54.37.30.38   | 192.168.0.175 | TLsv1.2  | 1494   | Ignored Unknown Record   |
| 19893 | 77.210988  | 13.107.136.9  | 192.168.0.175 | TCP      | 1494   | 443 → 1154 [ACK] Seq=291504 Ack=893 Win=4193792 Len=1440 [TCP segment of a reassembled PDU]  |
| 22950 | 77.523361  | 13.107.136.9  | 192.168.0.175 | TCP      | 1494   | 443 → 1154 [ACK] Seq=3551408 Ack=893 Win=4193792 Len=1440 [TCP segment of a reassembled PDU] |
| 23905 | 77.632501  | 13.107.136.9  | 192.168.0.175 | TCP      | 1494   | 443 → 1154 [ACK] Seq=4619760 Ack=893 Win=4193792 Len=1440 [TCP segment of a reassembled PDU] |
| 23911 | 77.633545  | 13.107.136.9  | 192.168.0.175 | TLsv1.2  | 1494   | Application Data [TCP segment of a reassembled PDU]  |
| 37292 | 79.148930  | 192.168.0.175 | 13.107.136.9  | TLsv1.2  | 31734  | Application Data, Application Data   |
| 46383 | 163.715086 | 54.37.30.38   | 192.168.0.175 | TLsv1.2  | 1494   | Ignored Unknown Record   |
| 66667 | 166.508943 | 54.37.30.38   | 192.168.0.175 | TLsv1.2  | 1494   | Ignored Unknown Record   |

#### 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 on the basis of different filters.