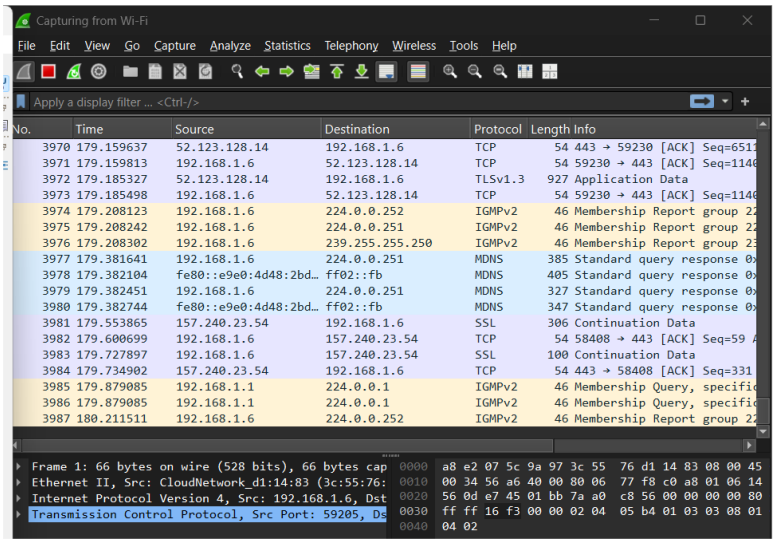
Ex no: 5 Using Wireshark to Capture Packets and Examine the packets

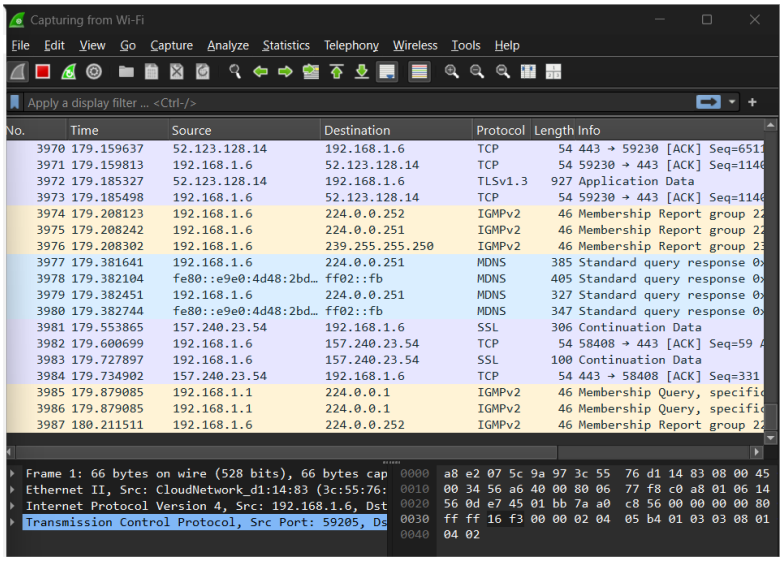
Wireshark successfully captured packets (eg: TCPpackets) exchanged during communication. Each packet contained:

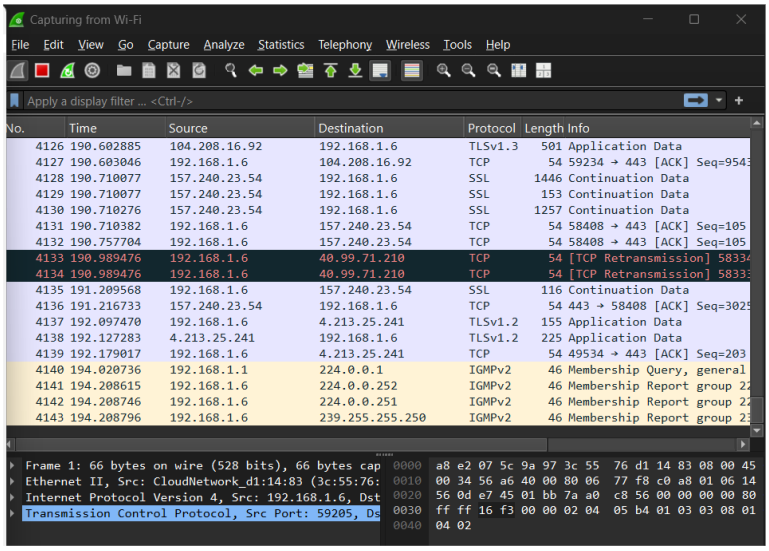
- Source/Destination IP
- Port information
- TCP flags
- Payload in hex and ASCII

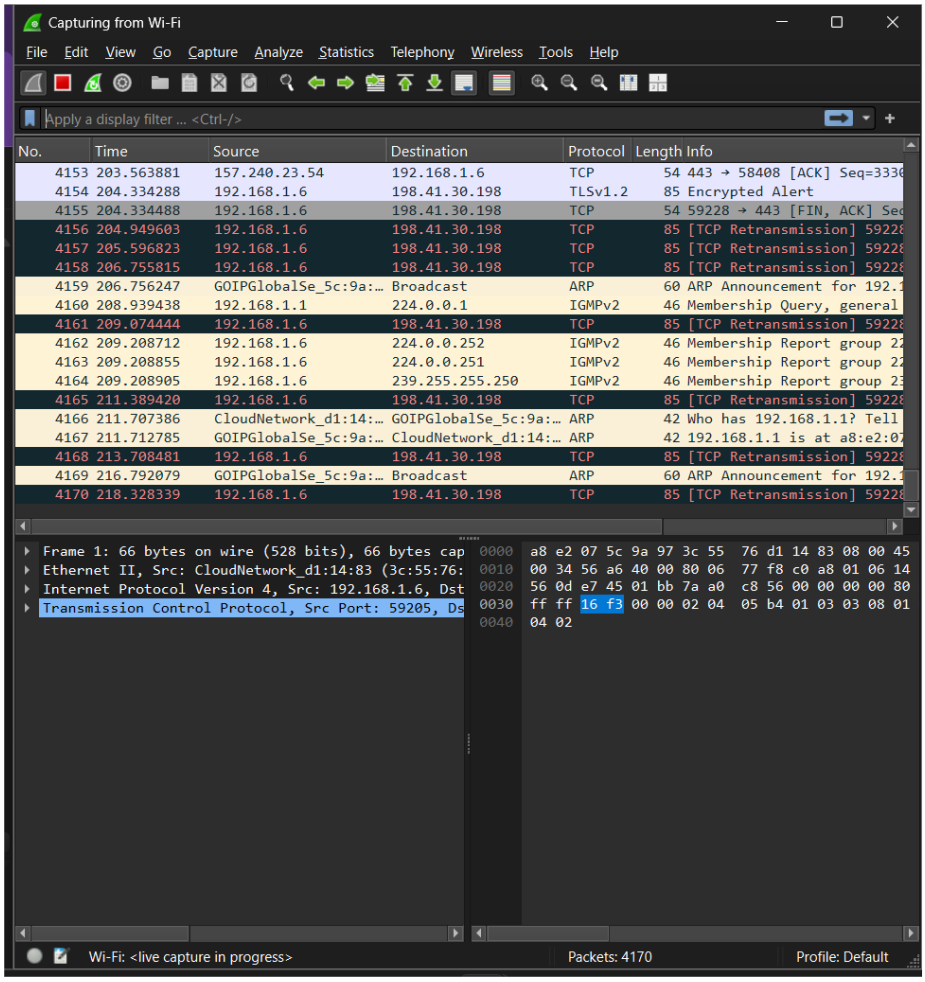
The captured screenshot shows a TCP message transmission initiated by the Echo Client to the Server.

Output :






Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
4126 190.602885 104.208.16.92 192.168.1.6 TLSv1.3 501 Application Data
4127 190.603046 192.168.1.6 104.208.16.92 TCP 54 59234 → 443 [ACK] Seq=954
4128 190.710077 157.240.23.54 192.168.1.6 SSL 1446 Continuation Data
4129 190.710077 157.240.23.54 192.168.1.6 SSL 153 Continuation Data
4130 190.710276 157.240.23.54 192.168.1.6 SSL 1257 Continuation Data
4131 190.710382 192.168.1.6 157.240.23.54 TCP 54 58408 → 443 [ACK] Seq=105
4132 190.757704 192.168.1.6 157.240.23.54 TCP 54 58408 → 443 [ACK] Seq=105
4133 190.989476 192.168.1.6 40.99.71.210 TCP 54 [TCP Retransmission] 5833
4134 190.989476 192.168.1.6 40.99.71.210 TCP 54 [TCP Retransmission] 5833
4135 191.209568 192.168.1.6 157.240.23.54 SSL 116 Continuation Data
4136 191.216733 157.240.23.54 192.168.1.6 TCP 54 443 → 58408 [ACK] Seq=302
4137 192.097470 192.168.1.6 4.213.25.241 TLSv1.2 155 Application Data
4138 192.127283 4.213.25.241 192.168.1.6 TLSv1.2 225 Application Data
4139 192.179017 192.168.1.6 4.213.25.241 TCP 54 49534 → 443 [ACK] Seq=203
4140 194.020736 192.168.1.1 224.0.0.1 IGMPv2 46 Membership Query, general
4141 194.208615 192.168.1.6 224.0.0.252 IGMPv2 46 Membership Report group 2
4142 194.208746 192.168.1.6 224.0.0.251 IGMPv2 46 Membership Report group 2
4143 194.208796 192.168.1.6 239.255.255.250 IGMPv2 46 Membership Report group 2
Frame 1: 66 bytes on wire (528 bits), 66 bytes cap
Ethernet II, Src: CloudNetwork_d1:14:83 (3c:55:76:
Internet Protocol Version 4, Src: 192.168.1.6, Dst
Transmission Control Protocol, Src Port: 59205, Ds
0000 a8 e2 07 5c 9a 97 3c 55 76 d1 14 83 08 00 45
0010 00 34 56 a6 40 00 80 06 77 f8 c0 a8 01 06 14
0020 56 0d e7 45 01 bb 7a a0 c8 56 00 00 00 00 80
0030 ff ff 16 f3 00 00 02 04 05 b4 01 03 03 08 01
0040 04 02


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
4153 203.563881 157.240.23.54 192.168.1.6 TCP 54 443 → 58408 [ACK] Seq=3336
4154 204.334288 192.168.1.6 198.41.30.198 TLSv1.2 85 Encrypted Alert
4155 204.334488 192.168.1.6 198.41.30.198 TCP 54 59228 → 443 [FIN, ACK] Seq
4156 204.949603 192.168.1.6 198.41.30.198 TCP 85 [TCP Retransmission] 59228
4157 205.596823 192.168.1.6 198.41.30.198 TCP 85 [TCP Retransmission] 59228
4158 206.755815 192.168.1.6 198.41.30.198 TCP 85 [TCP Retransmission] 59228
4159 206.756247 GOIPGlobalSe_5c:9a:... Broadcast ARP 60 ARP Announcement for 192.1
4160 208.939438 192.168.1.1 224.0.0.1 IGMPv2 46 Membership Query, general
4161 209.074444 192.168.1.6 198.41.30.198 TCP 85 [TCP Retransmission] 59228
4162 209.208712 192.168.1.6 224.0.0.252 IGMPv2 46 Membership Report group 2
4163 209.208855 192.168.1.6 224.0.0.251 IGMPv2 46 Membership Report group 2
4164 209.208905 192.168.1.6 239.255.255.250 IGMPv2 46 Membership Report group 2
4165 211.389420 192.168.1.6 198.41.30.198 TCP 85 [TCP Retransmission] 59228
4166 211.707386 CloudNetwork_d1:14:... GOIPGlobalSe_5c:9a:... ARP 42 Who has 192.168.1.1? Tell
4167 211.712785 GOIPGlobalSe_5c:9a:... CloudNetwork_d1:14:... ARP 42 192.168.1.1 is at a8:e2:07
4168 213.708481 192.168.1.6 198.41.30.198 TCP 85 [TCP Retransmission] 59228
4169 216.792079 GOIPGlobalSe_5c:9a:... Broadcast ARP 60 ARP Announcement for 192.1
4170 218.328339 192.168.1.6 198.41.30.198 TCP 85 [TCP Retransmission] 59228
Frame 1: 66 bytes on wire (528 bits), 66 bytes cap
Ethernet II, Src: CloudNetwork_d1:14:83 (3c:55:76:
Internet Protocol Version 4, Src: 192.168.1.6, Dst
Transmission Control Protocol, Src Port: 59205, Ds
0000 a8 e2 07 5c 9a 97 3c 55 76 d1 14 83 08 00 45
0010 00 34 56 a6 40 00 80 06 77 f8 c0 a8 01 06 14
0020 56 0d e7 45 01 bb 7a a0 c8 56 00 00 00 00 80
0030 ff ff 16 f3 00 00 02 04 05 b4 01 03 03 08 01
0040 04 02
Wi-Fi: <live capture in progress>
Packets: 4170
Profile: Default