

**EX NO: 5**

**K. GOWTHAM**  
**192011090**

## PACKET ANALYZER TOOL

### AIM:

To Analyse the network packet transmission using packet analyzer tool (Wireshark).

### PROCEDURE:

1. Capture the packets (TCP / UDP / HTTP)
2. Filter those packets
3. Inspect those packets

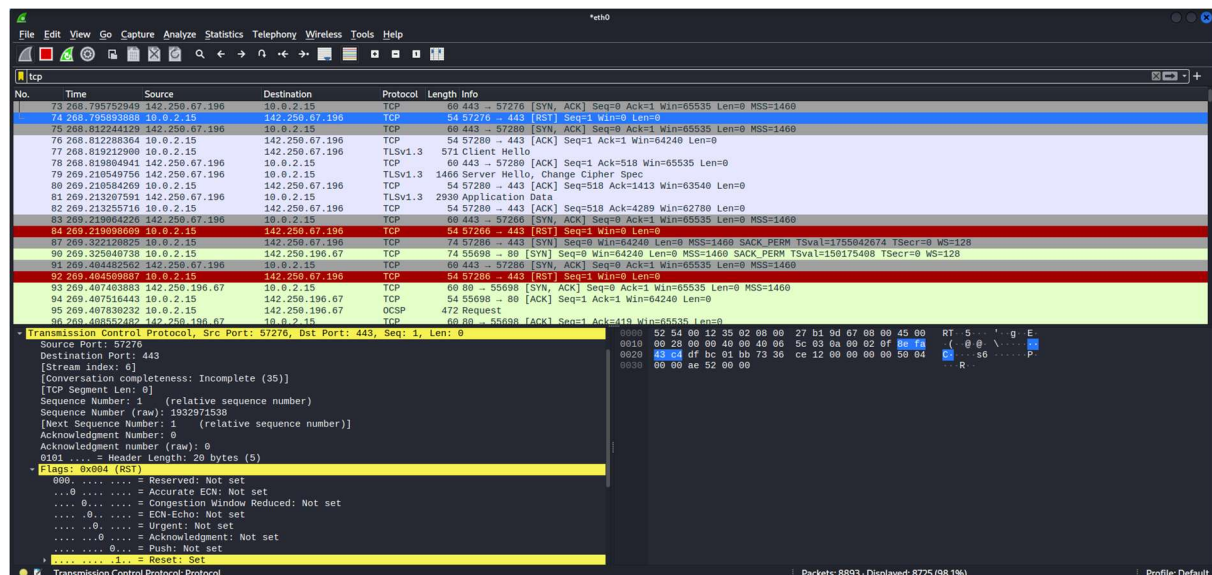
**Step 1: Install and open WireShark .**

**Step 2: To capture TCP / UDP /HTTP Packet.**

**Step 3: to Filter TCP / UDP /HTTP Packet.**

**Step4: to inspect the TCP / UDP /HTTP Packet.**

### OUTPUT



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

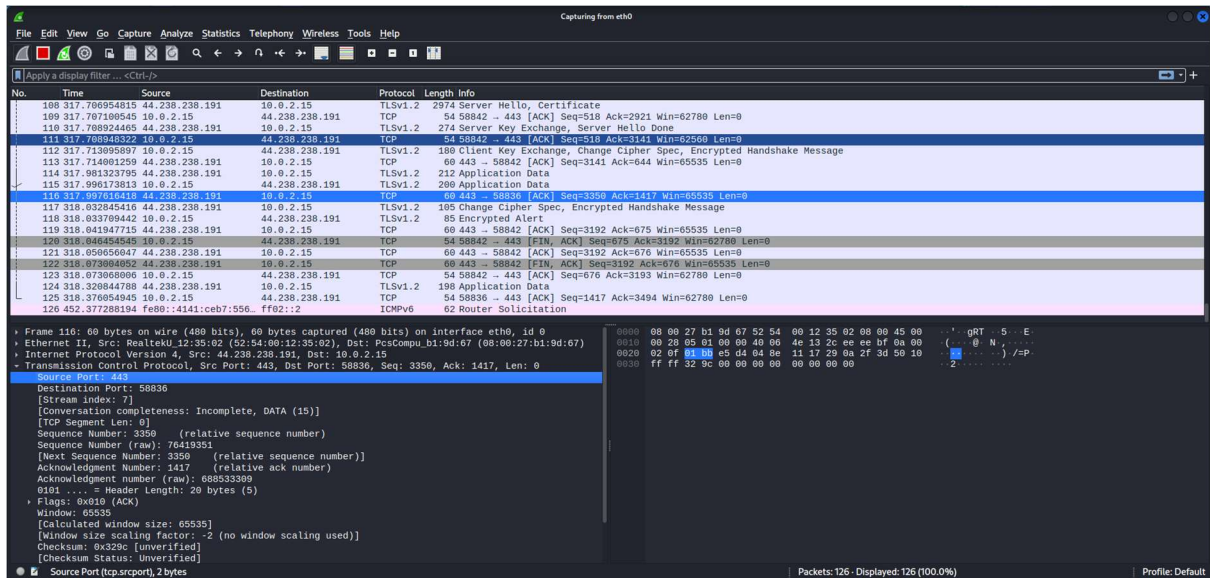
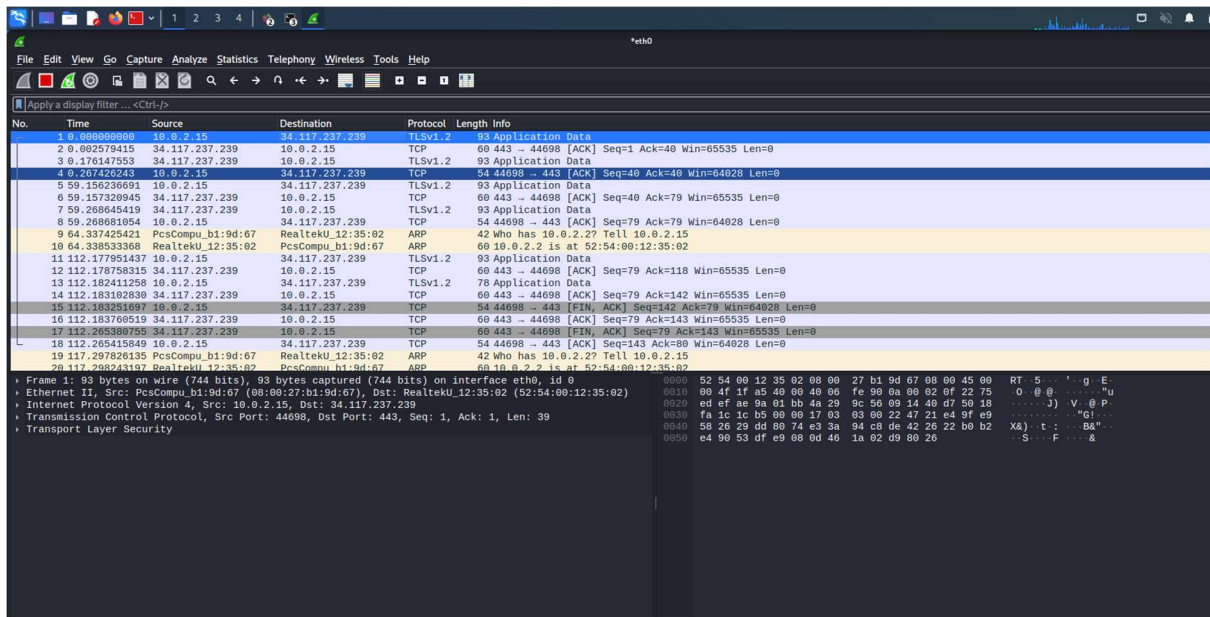
eth0

tcp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	34.117.237.239	TLSv1.2	93	Application Data
2	0.002579415	34.117.237.239	10.0.2.15	TCP	60	443 → 44998 [ACK] Seq=1 Ack=40 Win=65535 Len=0
3	0.176147953	34.117.237.239	10.0.2.15	TLSv1.2	93	Application Data
4	0.267426243	10.0.2.15	34.117.237.239	TCP	54	44998 → 443 [ACK] Seq=40 Ack=40 Win=64028 Len=0
5	0.592366991	10.0.2.15	34.117.237.239	TLSv1.2	93	Application Data
6	0.597320945	34.117.237.239	10.0.2.15	TCP	60	443 → 44998 [ACK] Seq=40 Ack=79 Win=65535 Len=0
7	0.268645419	34.117.237.239	10.0.2.15	TLSv1.2	93	Application Data
8	0.5926881054	10.0.2.15	34.117.237.239	TCP	54	44998 → 443 [ACK] Seq=79 Ack=79 Win=64028 Len=0
11	12.177951437	10.0.2.15	34.117.237.239	TLSv1.2	93	Application Data
12	12.178788315	34.117.237.239	10.0.2.15	TCP	60	443 → 44998 [ACK] Seq=79 Ack=118 Win=65535 Len=0
13	12.182412558	10.0.2.15	34.117.237.239	TLSv1.2	78	Application Data
14	12.183102830	34.117.237.239	10.0.2.15	TCP	60	443 → 44998 [ACK] Seq=79 Ack=142 Win=65535 Len=0
15	12.183251697	10.0.2.15	34.117.237.239	TCP	54	44998 → 443 [FIN, ACK] Seq=142 Ack=79 Win=64028 Len=0
16	12.183700519	34.117.237.239	10.0.2.15	TCP	60	443 → 44998 [ACK] Seq=79 Ack=143 Win=65535 Len=0
17	12.265389755	34.117.237.239	10.0.2.15	TCP	60	443 → 44998 [FIN, ACK] Seq=79 Ack=143 Win=65535 Len=0
18	12.265415849	10.0.2.15	34.117.237.239	TCP	54	44998 → 443 [ACK] Seq=143 Ack=80 Win=64028 Len=0
25	26.004871684	10.0.2.15	34.120.115.102	TCP	74	43210 → 443 [SYN, Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3070521042 TSecr=0 WS=128
24	26.07344047	34.120.115.102	10.0.2.15	TCP	60	443 → 43210 [SYN, Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
25	26.078342634	10.0.2.15	34.120.115.102	TCP	54	43210 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0

Frame 14: 93 bytes on wire (744 bits), 93 bytes captured (744 bytes) on interface eth0, id 0  
 Ethernet II, Src: PcsCompu, Btl:9d:67: (08:00:27:b1:9d:67), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)  
 Internet Protocol Version 4, Src: 10.0.2.15, Dst: 34.117.237.239  
 Transmission Control Protocol, Src Port: 44998, Dst Port: 443, Seq: 1, Ack: 1, Len: 39  
 Transport Layer Security

Packets: 8413 - Displayed: 8312 (98.8%) Profile: Default



## Result

Hence the analysing of the network packet transmission using packet analyzer tool (Wireshark) is performed successfully.