

EX NO: 5

G.Harish
192011095

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

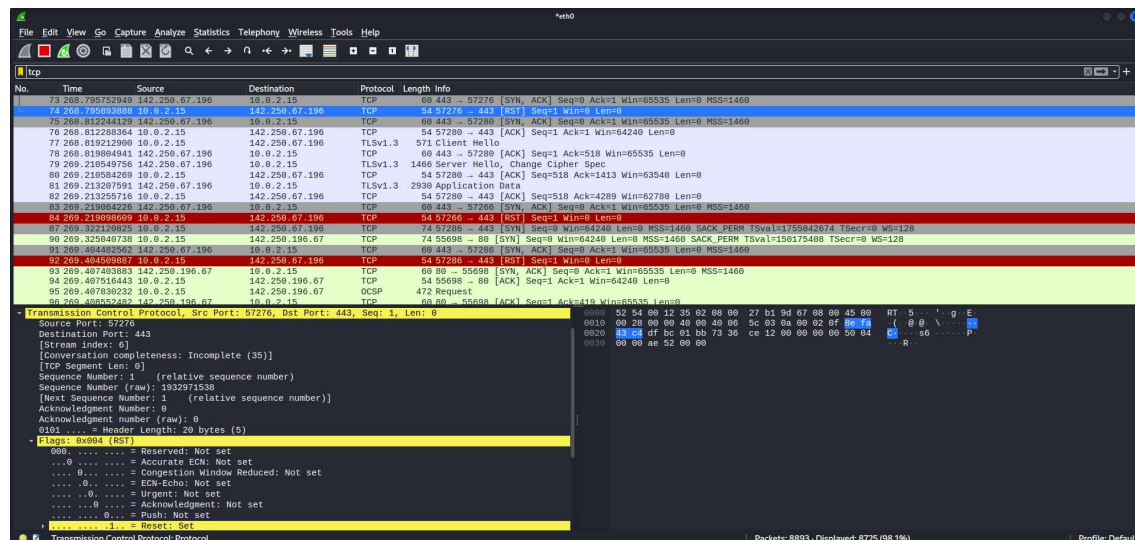
Step 1: Install and open WireShark .

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



Wireshark packet capture showing HTTP traffic. The selected packet is a POST request to /gtsic3 HTTP/1.1 from 10.0.2.15 to 142.250.196.67. The packet details show the request structure, including headers like Host, User-Agent, Accept, and Content-Type. The packet bytes show the raw data, including the POST body.

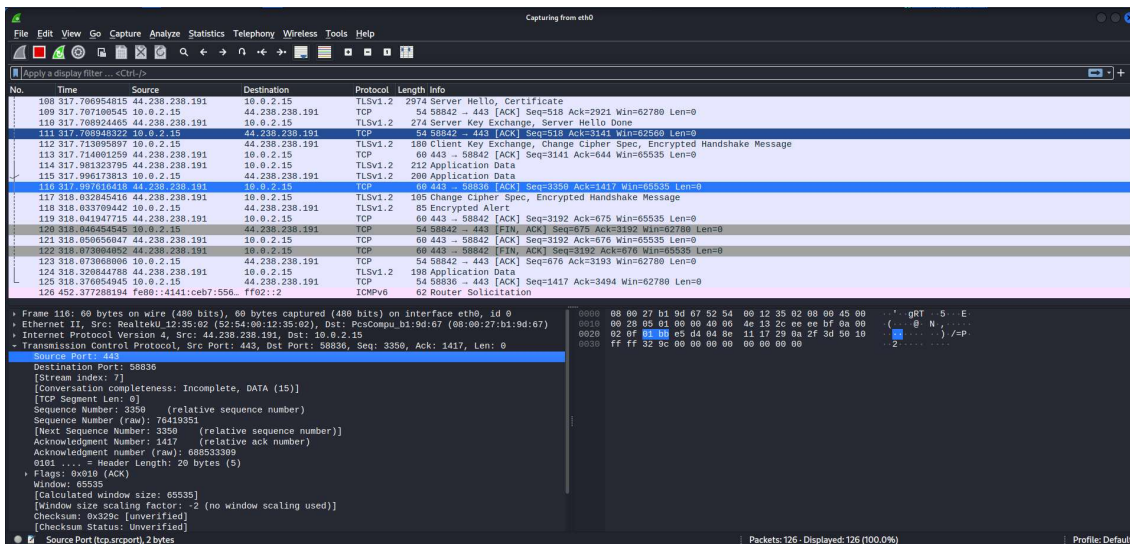
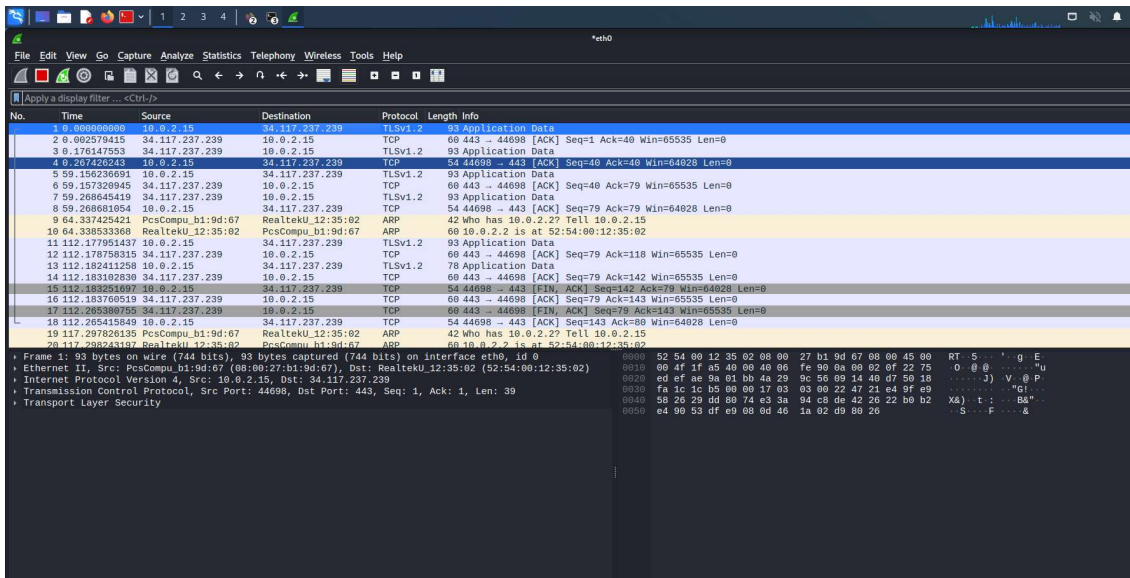
No.	Time	Source	Destination	Protocol	Length	Info
109	2.99	10.0.2.15	142.250.196.67	HTTP	472	POST /gtsic3 HTTP/1.1
110	2.99	10.0.2.15	142.250.196.67	HTTP	839	Response
311	2.79	10.0.2.15	142.250.196.67	HTTP	472	Request
321	2.79	10.0.2.15	142.250.196.67	HTTP	839	Response
410	2.82	10.0.2.15	142.250.196.67	HTTP	472	Request
417	2.82	10.0.2.15	142.250.196.67	HTTP	472	Request
433	2.83	10.0.2.15	142.250.196.67	HTTP	839	Response
469	2.85	10.0.2.15	142.250.196.67	HTTP	839	Response
1144	6.32	10.0.2.15	23.44.11.83	HTTP	469	Request
1169	6.33	10.0.2.15	23.44.11.83	HTTP	1002	Response
1171	6.33	10.0.2.15	23.44.11.83	HTTP	469	Request
1195	6.34	10.0.2.15	23.44.11.83	HTTP	469	Request
1197	6.34	10.0.2.15	23.44.11.83	HTTP	469	Request
1218	6.34	10.0.2.15	23.44.11.83	HTTP	1002	Response
1220	6.34	10.0.2.15	23.44.11.83	HTTP	1002	Response
1942	6.67	10.0.2.15	23.44.11.83	HTTP	1002	Response
8262	17.41	10.0.2.15	23.44.11.83	HTTP	469	Request
8264	17.42	10.0.2.15	23.44.11.83	HTTP	1003	Response
8339	17.90	10.0.2.15	23.44.11.83	HTTP	469	Request
8344	17.90	10.0.2.15	23.44.11.83	HTTP	1003	Response

Frame 95: 472 bytes on wire (3776 bits), 472 bytes captured (3776 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu... (08:00:27:11:0d:07), Dst: RealtekU... (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.250.196.67
Transmission Control Protocol, Src Port: 55698, Dst Port: 80, Seq: 1, Ack: 1, Len: 418
Hypertext Transfer Protocol
POST /gtsic3 HTTP/1.1
Host: ocpp.pki.goog/v1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20180101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/octet-stream
Content-Length: 83
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
[Full request URI: http://ocpp.pki.goog/gtsic3]
[HTTP request 1/1]
[Hypertext Transfer Protocol: 180]
File Data: 83 bytes
Hypertext Transfer Protocol: Protocol
Packets: 8452 - Displayed: 20 (0.2%)

Wireshark packet capture showing TCP traffic. The selected packet is a SYN packet from 10.0.2.15 to 142.250.196.67. The packet details show the TCP header and options, including the SYN flag and window size. The packet bytes show the raw data, including the SYN sequence number.

No.	Time	Source	Destination	Protocol	Length	Info
2	0.002579415	10.0.2.15	142.250.196.67	TLSv1.2	60	443 -> 44998 [ACK] Seq=1 Ack=40 Win=65535 Len=0
3	0.176147553	10.0.2.15	142.250.196.67	TLSv1.2	93	Application Data
4	0.207426243	10.0.2.15	142.250.196.67	TCP	54	44998 -> 443 [ACK] Seq=40 Ack=40 Win=64028 Len=0
5	0.156236691	10.0.2.15	142.250.196.67	TLSv1.2	93	Application Data
6	0.157329945	10.0.2.15	142.250.196.67	TCP	60	443 -> 44998 [ACK] Seq=40 Ack=79 Win=65535 Len=0
7	0.156845419	10.0.2.15	142.250.196.67	TLSv1.2	93	Application Data
8	0.156881854	10.0.2.15	142.250.196.67	TCP	54	44998 -> 443 [ACK] Seq=79 Ack=79 Win=64028 Len=0
11	112.177951437	10.0.2.15	142.250.196.67	TLSv1.2	93	Application Data
12	112.178750315	10.0.2.15	142.250.196.67	TCP	60	443 -> 44998 [ACK] Seq=79 Ack=110 Win=65535 Len=0
13	112.182411258	10.0.2.15	142.250.196.67	TLSv1.2	78	Application Data
14	112.183102830	10.0.2.15	142.250.196.67	TCP	60	443 -> 44998 [ACK] Seq=79 Ack=143 Win=65535 Len=0
15	112.183292860	10.0.2.15	142.250.196.67	TCP	54	44998 -> 443 [FIN, ACK] Seq=143 Ack=79 Win=64028 Len=0
16	112.183769519	10.0.2.15	142.250.196.67	TCP	60	443 -> 44998 [ACK] Seq=79 Ack=143 Win=65535 Len=0
17	112.265388750	10.0.2.15	142.250.196.67	TCP	60	443 -> 44998 [FIN, ACK] Seq=79 Ack=143 Win=65535 Len=0
18	112.265415840	10.0.2.15	142.250.196.67	TCP	54	44998 -> 443 [ACK] Seq=143 Ack=80 Win=64028 Len=0
23	260.554370845	10.0.2.15	142.120.115.102	TCP	74	43210 -> 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3070521042 TSecr=0 WS=128
24	260.703244847	10.0.2.15	142.120.115.102	TCP	60	443 -> 43210 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
25	260.703425234	10.0.2.15	142.120.115.102	TCP	54	43210 -> 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
26	260.703741668	10.0.2.15	142.120.115.102	TLSv1.3	724	Client Hello

Frame 1: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu... (08:00:27:11:0d:07), Dst: RealtekU... (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.250.196.67
Transmission Control Protocol, Src Port: 44998, Dst Port: 443, Seq: 1, Ack: 1, Len: 39
Transport Layer Security
Packets: 8413 - Displayed: 8312 (98.6%)



Result

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