PACKET ANALYZER TOOL

AIM:

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

PROCEDURE:

1. Capture the packets (TCP / UDP / HTTP)

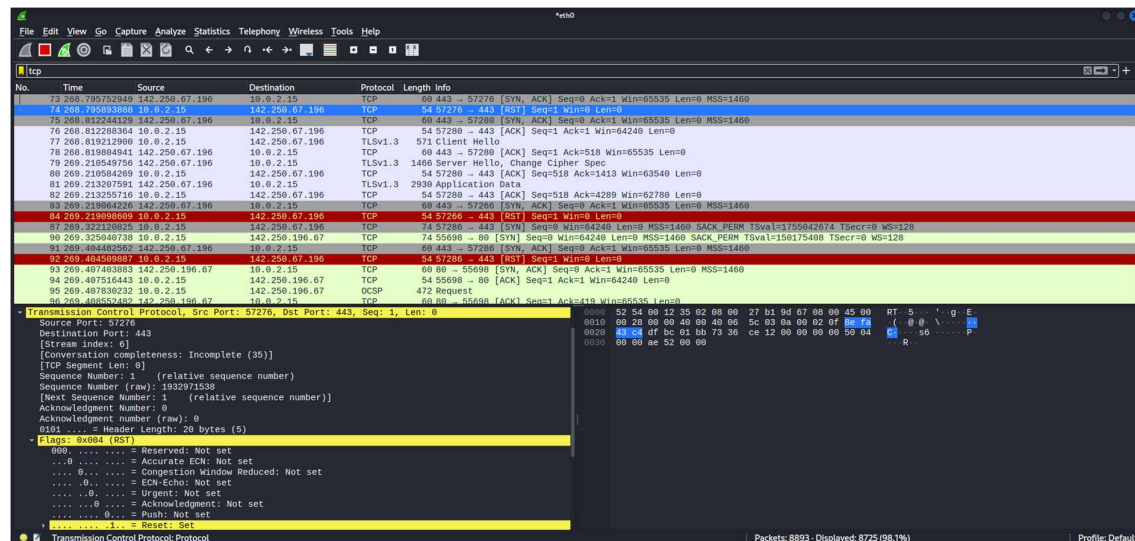2. Filter those packets

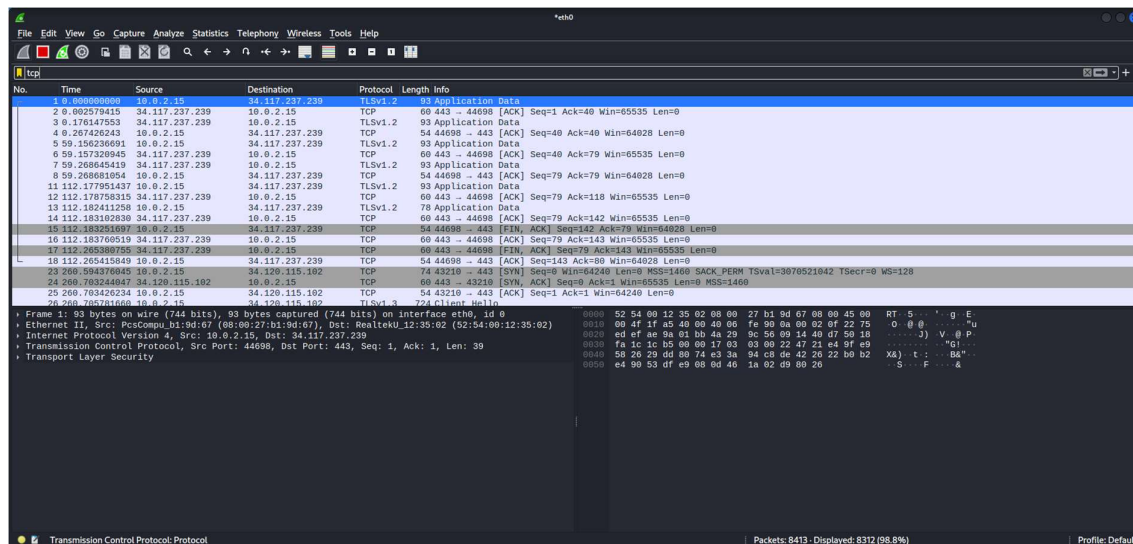3. Inspect those packets

Step 1: Install and open WireShark .

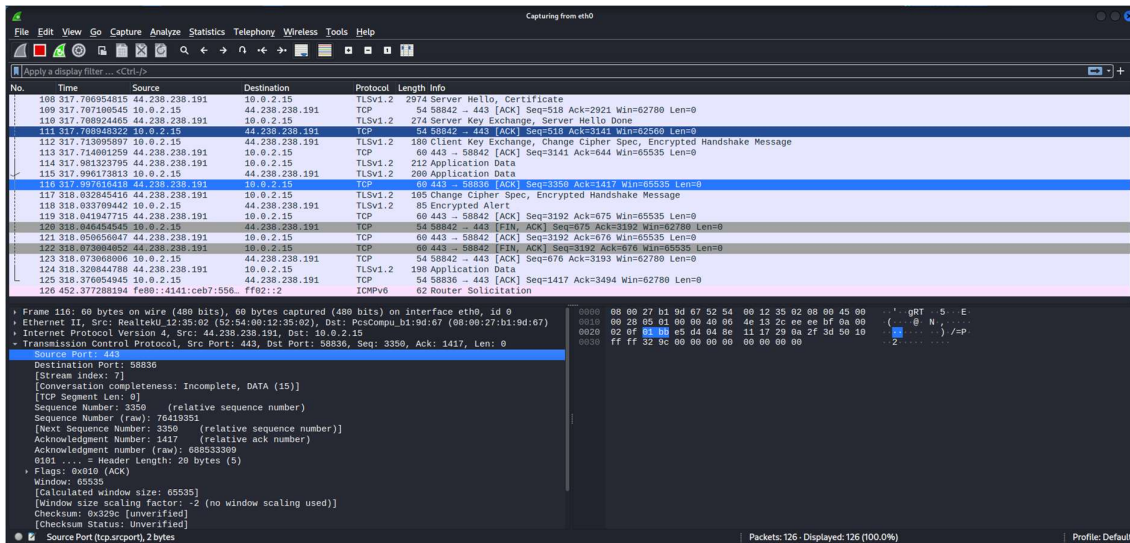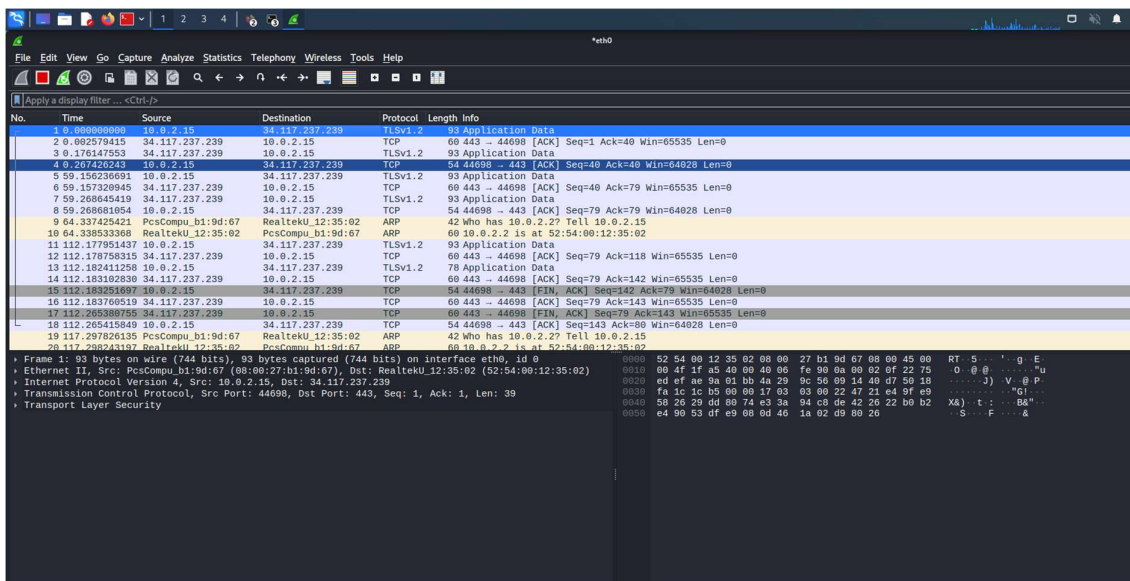**Step 2: To capture TCP / UDP /HTTP Packet.**

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

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

OUTPUT

Screenshot 1 — *eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: `http`

No.	Time	Source	Destination	Protocol	Length	Info
95	269.407830232	10.0.2.15	142.250.196.67	OCSP	472	Request
100	269.507697024	142.250.196.67	10.0.2.15	OCSP	839	Response
311	279.670420679	10.0.2.15	142.250.196.67	OCSP	472	Request
321	279.888491653	142.250.196.67	10.0.2.15	OCSP	839	Response
410	282.552216921	10.0.2.15	142.250.196.67	OCSP	472	Request
417	282.583786787	10.0.2.15	142.250.196.67	OCSP	472	Request
433	283.267645362	142.250.196.67	10.0.2.15	OCSP	839	Response
469	285.418358340	142.250.196.67	10.0.2.15	OCSP	839	Response
1144	632.338786761	10.0.2.15	23.44.11.83	OCSP	469	Request
1169	633.140646099	23.44.11.83	10.0.2.15	OCSP	1002	Response
1171	633.141887550	10.0.2.15	23.44.11.83	OCSP	469	Request
1195	634.168423587	10.0.2.15	23.44.11.83	OCSP	469	Request
1197	634.170485520	10.0.2.15	23.44.11.83	OCSP	469	Request
1218	634.691692017	23.44.11.83	10.0.2.15	OCSP	1002	Response
1220	634.691692137	23.44.11.83	10.0.2.15	OCSP	1002	Response
1942	667.271884077	23.44.11.83	10.0.2.15	OCSP	1002	Response
8262	1741.9849321...	10.0.2.15	23.44.11.83	OCSP	469	Request
8264	1742.1152752...	23.44.11.83	10.0.2.15	OCSP	1003	Response
8339	1790.8480095...	10.0.2.15	23.44.11.83	OCSP	469	Request
8344	1790.9175659...	23.44.11.83	10.0.2.15	OCSP	1003	Response

> Frame 95: 472 bytes on wire (3776 bits), 472 bytes captured (3776 bits) on interface eth0, id 0
> Ethernet II, Src: PcsCompu_b1:9d: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: 142.250.196.67
> Transmission Control Protocol, Src Port: 55698, Dst Port: 80, Seq: 1, Ack: 1, Len: 418
v Hypertext Transfer Protocol
  > POST /gts1c3 HTTP/1.1\r\n
    Host: ocsp.pki.goog\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0\r\n
    Accept: */*\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Content-Type: application/ocsp-request\r\n
  > Content-Length: 83\r\n
    Connection: keep-alive\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://ocsp.pki.goog/gts1c3]
    [HTTP request 1/1]
    [Response in frame: 100]
    File Data: 83 bytes

```
0000  52 54 00 12 35 02 08 00  27 b1 9d 67 08 00 45 00   RT··5···'··g··E·
0010  01 ca 69 d0 40 00 40 06  70 11 0a 00 02 0f 8e fa   ··i·@·@· p·······
0020  c4 43 d9 92 00 50 2f 45  5d 64 0b 97 c6 02 50 18   ·C···P/E ]d····P·
0030  fa f0 61 09 00 00 50 4f  53 54 20 2f 67 74 73 31   ··a···PO ST /gts1
0040  63 33 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73   c3 HTTP/ 1.1··Hos
0050  74 3a 20 6f 63 73 70 2e  70 6b 69 2e 67 6f 6f 67   t: ocsp. pki.goog
0060  0d 0a 55 73 65 72 2d 41  67 65 6e 74 3a 20 4d 6f   ··User-A gent: Mo
0070  7a 69 6c 6c 61 2f 35 2e  30 20 28 58 31 31 3b 20   zilla/5. 0 (X11;
0080  4c 69 6e 75 78 20 78 38  36 5f 36 34 3b 20 72 76   Linux x8 6_64; rv
0090  3a 31 30 32 2e 30 29 20  47 65 63 6b 6f 2f 32 30   :102.0)  Gecko/20
00a0  31 30 30 31 30 31 20 46  69 72 65 66 6f 78 2f 31   100101 F irefox/1
00b0  30 32 2e 30 0d 0a 41 63  63 65 70 74 3a 20 2a 2f   02.0··Ac cept: */
00c0  2a 0d 0a 41 63 63 65 70  74 2d 4c 61 6e 67 75 61   *··Accep t-Langua
00d0  67 65 3a 20 65 6e 2d 55  53 2c 65 6e 3b 71 3d 30   ge: en-U S,en;q=0
00e0  2e 35 0d 0a 41 63 63 65  70 74 2d 45 6e 63 6f 64   .5··Acce pt-Encod
00f0  69 6e 67 3a 20 67 7a 69  70 2c 20 64 65 66 6c 61   ing: gzi p, defla
0100  74 65 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   te··Conn ection:
0110  6b 65 65 70 2d 61 6c 69  76 65 0d 0a 50 72 61 67   keep-ali ve··Prag
0120  6d 61 3a 20 6e 6f 2d 63  61 63 68 65 0d 0a 43 61   ma: no-c ache··Ca
0130  63 68 65 2d 43 6f 6e 74  72 6f 6c 3a 20 6e 6f 2d   che-Cont rol: no-
0140  63 61 63 68 65 0d 0a 0d  0a 30 6e 30 6b 65 52 70   cache··· ·0n0keRp
0150  2d 61 6c 69 76 65 0d 0a   -alive··
```

● ☑ Hypertext Transfer Protocol: Protocol   Packets: 8452 · Displayed: 20 (0.2%)   Profile: Default

---

Screenshot 2 — *eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: `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 → 44698 [ACK] Seq=1 Ack=40 Win=65535 Len=0
3	0.176147553	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	44698 → 443 [ACK] Seq=40 Ack=40 Win=64028 Len=0
5	59.156236691	10.0.2.15	34.117.237.239	TLSv1.2	93	Application Data
6	59.157320945	34.117.237.239	10.0.2.15	TCP	60	443 → 44698 [ACK] Seq=40 Ack=79 Win=65535 Len=0
7	59.268645419	34.117.237.239	10.0.2.15	TLSv1.2	93	Application Data
8	59.268681054	10.0.2.15	34.117.237.239	TCP	54	44698 → 443 [ACK] Seq=79 Ack=79 Win=64028 Len=0
11	112.179951437	10.0.2.15	34.117.237.239	TLSv1.2	93	Application Data
12	112.178758315	34.117.237.239	10.0.2.15	TCP	60	443 → 44698 [ACK] Seq=79 Ack=118 Win=65535 Len=0
13	112.182411258	10.0.2.15	34.117.237.239	TLSv1.2	78	Application Data
14	112.183102830	34.117.237.239	10.0.2.15	TCP	60	443 → 44698 [ACK] Seq=142 Win=65535 Len=0
15	112.183251697	10.0.2.15	34.117.237.239	TCP	54	44698 → 443 [FIN, ACK] Seq=142 Ack=79 Win=64028 Len=0
16	112.183760519	34.117.237.239	10.0.2.15	TCP	60	443 → 44698 [ACK] Seq=79 Ack=143 Win=65535 Len=0
17	112.265380755	34.117.237.239	10.0.2.15	TCP	60	443 → 44698 [FIN, ACK] Seq=79 Ack=143 Win=65535 Len=0
18	112.265415849	10.0.2.15	34.117.237.239	TCP	54	44698 → 443 [ACK] Seq=143 Ack=80 Win=64028 Len=0
23	260.594376045	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	260.703244047	34.120.115.102	10.0.2.15	TCP	74	443 → 43210 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
25	260.703426234	10.0.2.15	34.120.115.102	TCP	54	43210 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
26	260.705781660	10.0.2.15	34.120.115.102	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_b1:9d: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: 44698, Dst Port: 443, Seq: 1, Ack: 1, Len: 39
> Transport Layer Security

```
0000  52 54 00 12 35 02 08 00  27 b1 9d 67 08 00 45 00   RT··5···'··g··E·
0010  00 4f 1f a5 40 00 40 06  fe 90 0a 00 02 0f 22 75   ·O··@·@· ······"u
0020  ed ef ae 9a 01 bb 4a 29  9c 56 09 14 40 d7 50 18   ······J) ·V·@·P·
0030  fa 1c 1c b5 00 00 17 03  03 00 22 47 21 e4 9f e9   ········ ··"G!···
0040  58 26 29 dd 80 74 e3 3a  94 c8 de 42 26 22 b0 b2   X&)··t·: ···B&"··
0050  e4 90 53 df e9 08 0d 46  1a 02 d9 80 26            ··S····F ····&
```

● ☑ Transmission Control Protocol: Protocol   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.