PRACTICAL-5

AIM: Use a tool like wireshark to capture packets and examine the packets.

Filter and Examine Packets:

1. **Observe Captured Traffic**: You will see packets being captured in real time. Each line represents a network packet.

2. **Use Filters**: To focus on specific traffic, you can apply filters. For example:
    1. To filter for HTTP traffic: http
    2. To filter for a specific IP address: ip.addr == 192.168.1.1
    3. To filter for a specific protocol: tcp or udp

3. **Inspect a Packet**: Click on any packet to view detailed information. This will show you different layers of the packet (e.g., Ethernet, IP, TCP/UDP, application data).

    1. The **Packet Details** pane shows you a breakdown of the packet structure.
    2. The **Packet Bytes** pane shows the raw byte data of the packet.

Ans

Date: 08/02/25 Page No.

Topic:

Wireshark:-

Data Packets Capturing:-

(1) Top frame:-

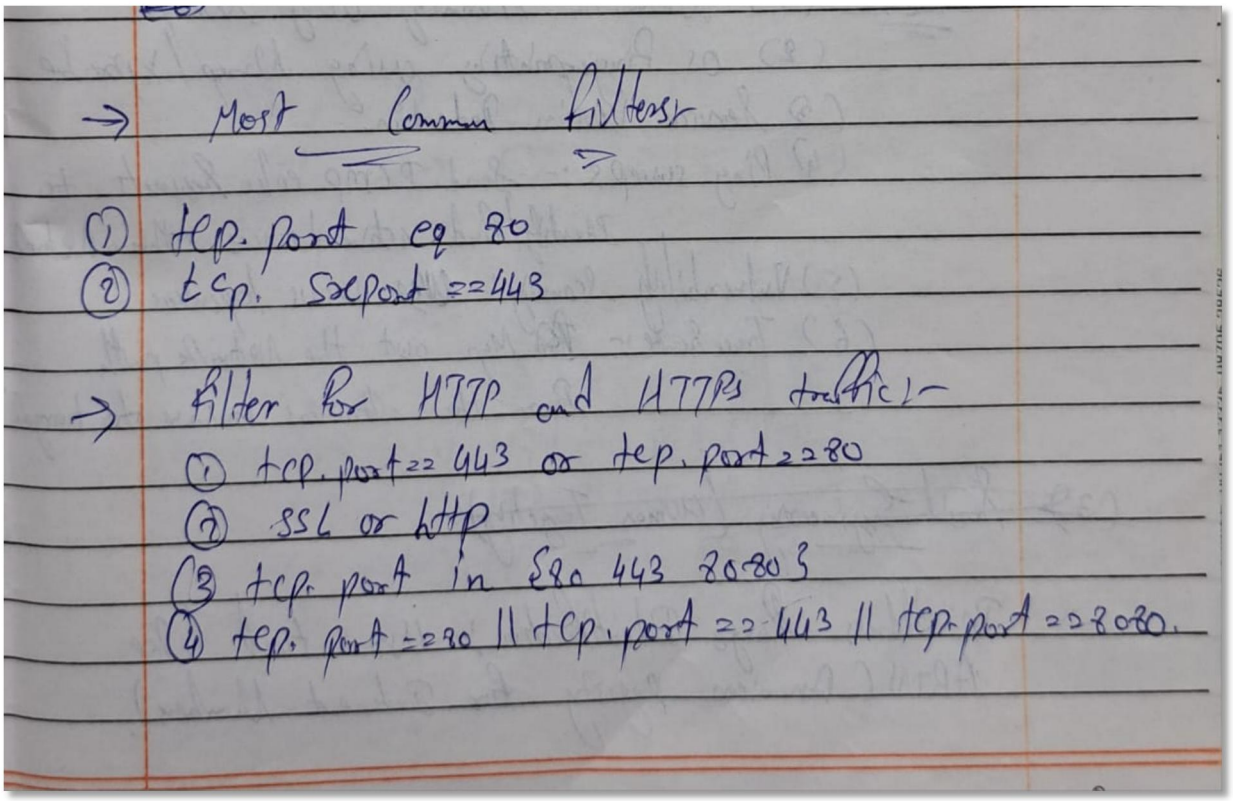
1. Number
2. Time
3. Source
4. Destination
5. protocol
6. Length
7. Info.

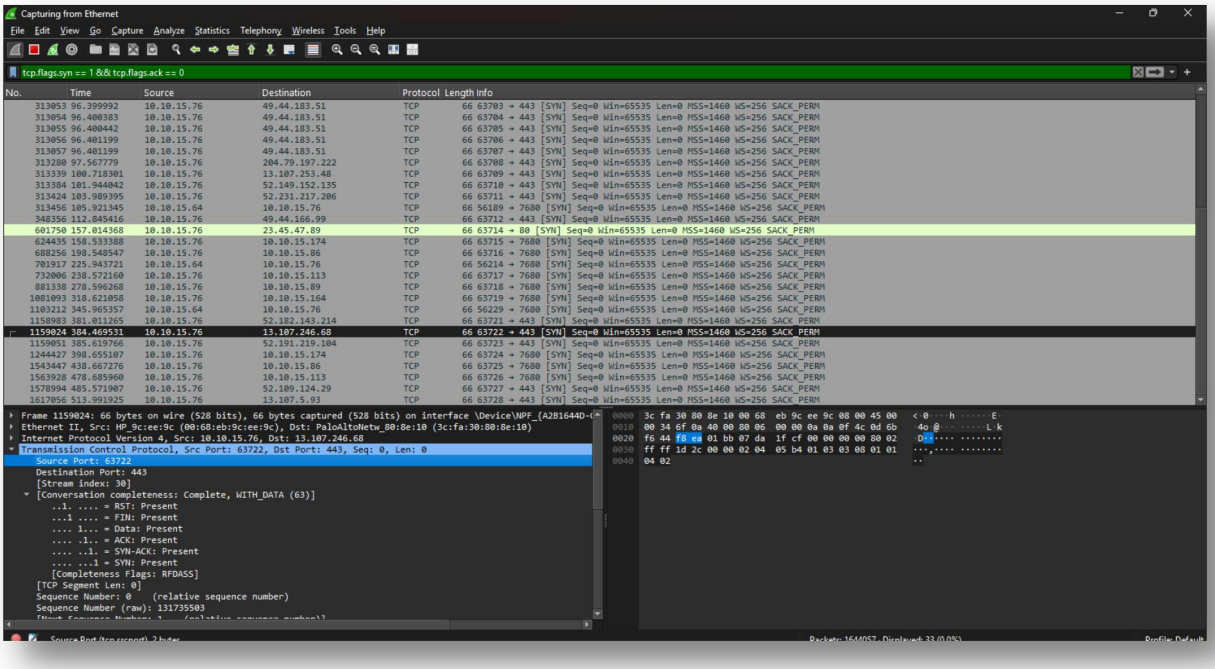
(2) Middle frame:-

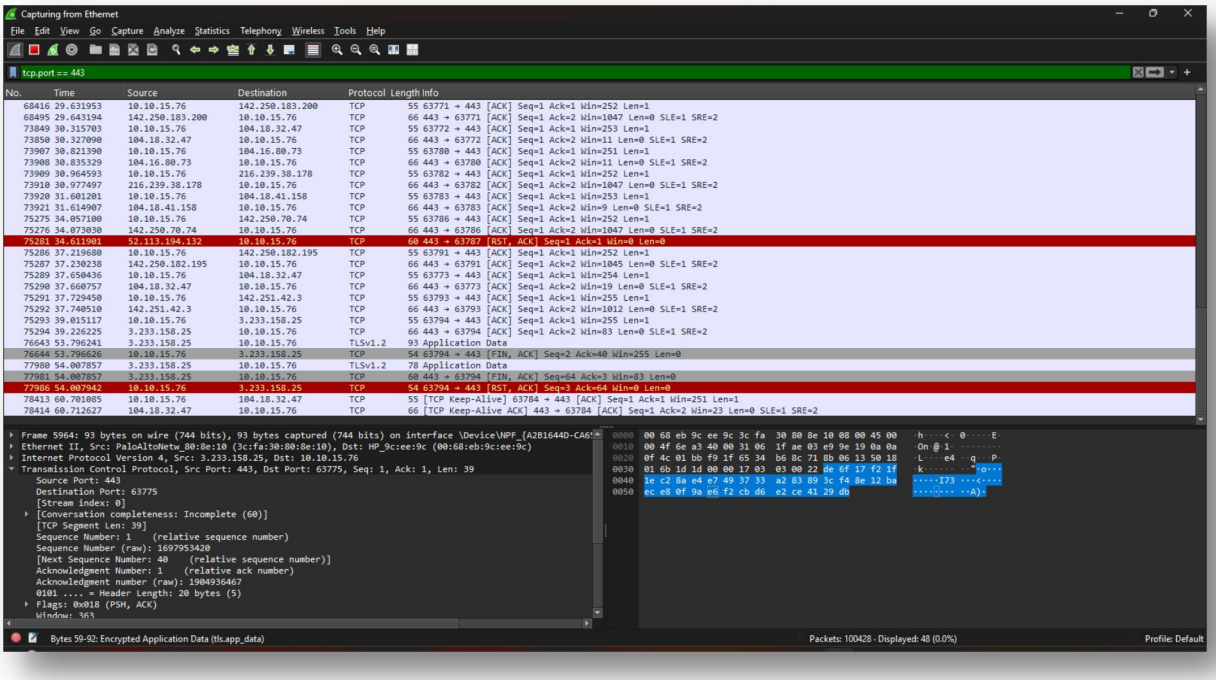
1. Frame
2. Linux Cooked Capture
3. Internet protocol version, Source, destination
4. Transmission Control protocol, src port, dst port, Seq, len.

(3) Bottom frame:- Data.

→ Filters:- Wireshark provides powerful filters capture and display filters to focus or specific packets of interest.


Most Common filters
1. tcp.port eq 80
2. tcp.srcport == 443
Filter for HTTP and HTTPS traffic
1. tcp.port == 443 or tcp.port == 80
2. ssl or http
3. tcp.port in {80 443 8080}
4. tcp.port == 80 || tcp.port == 443 || tcp.port == 8080.


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.syn == 1 && tcp.flags.ack == 0
No. Time Source Destination Protocol Length Info
313053 96.399992 10.10.15.76 49.44.183.51 TCP 66 63703 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
313054 96.400383 10.10.15.76 49.44.183.51 TCP 66 63704 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
313055 96.400442 10.10.15.76 49.44.183.51 TCP 66 63705 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
313056 96.401199 10.10.15.76 49.44.183.51 TCP 66 63706 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
313057 96.401199 10.10.15.76 49.44.183.51 TCP 66 63707 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
313280 97.567779 10.10.15.76 204.79.197.222 TCP 66 63708 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
313339 100.718301 10.10.15.76 13.107.253.48 TCP 66 63709 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
313384 101.944042 10.10.15.76 52.149.152.135 TCP 66 63710 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
313424 103.989395 10.10.15.76 52.231.217.206 TCP 66 63711 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
313456 105.921345 10.10.15.64 10.10.15.76 TCP 66 56189 → 7680 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
348358 112.845416 10.10.15.76 49.44.166.99 TCP 66 63712 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
601750 157.014368 10.10.15.76 23.45.47.89 TCP 66 63714 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
624435 158.533388 10.10.15.76 10.10.15.174 TCP 66 63715 → 7680 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
688256 198.548547 10.10.15.76 10.10.15.86 TCP 66 63716 → 7680 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
701917 225.943721 10.10.15.64 10.10.15.76 TCP 66 56214 → 7680 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
732006 238.572160 10.10.15.76 10.10.15.113 TCP 66 63717 → 7680 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
881338 278.596268 10.10.15.76 10.10.15.89 TCP 66 63718 → 7680 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1081093 318.621058 10.10.15.76 10.10.15.164 TCP 66 63719 → 7680 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1103212 345.965357 10.10.15.64 10.10.15.76 TCP 66 56229 → 7680 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1158983 381.011265 10.10.15.76 52.182.143.214 TCP 66 63721 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1159024 384.469531 10.10.15.76 13.107.246.68 TCP 66 63722 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1159051 385.619766 10.10.15.76 52.191.219.104 TCP 66 63723 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1244427 398.655107 10.10.15.76 10.10.15.174 TCP 66 63724 → 7680 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1543447 438.667276 10.10.15.76 10.10.15.86 TCP 66 63725 → 7680 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1563928 478.685960 10.10.15.76 10.10.15.113 TCP 66 63726 → 7680 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1578994 485.571907 10.10.15.76 52.109.124.29 TCP 66 63727 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1617056 513.991925 10.10.15.76 13.107.5.93 TCP 66 63728 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
Frame 1159024: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{A2B1644D-(
Ethernet II, Src: HP_9c:ee:9c (00:68:eb:9c:ee:9c), Dst: PaloAltoNetw_80:8e:10 (3c:fa:30:80:8e:10)
Internet Protocol Version 4, Src: 10.10.15.76, Dst: 13.107.246.68
Transmission Control Protocol, Src Port: 63722, Dst Port: 443, Seq: 0, Len: 0
Source Port: 63722
Destination Port: 443
[Stream index: 30]
[Conversation completeness: Complete, WITH_DATA (63)]
..1. .... = RST: Present
...1 .... = FIN: Present
.... 1... = Data: Present
.... .1.. = ACK: Present
.... ..1. = SYN-ACK: Present
....1 = SYN: Present
[Completeness Flags: RFDASS]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 1317735503
0000 3c fa 30 80 8e 10 00 68 eb 9c ee 9c 08 00 45 00
0010 00 34 6f 0a 40 00 80 06 00 00 0a 0a 0f 4c 0d 6b
0020 f6 44 f8 ea 01 bb 07 da 1f cf 00 00 00 00 80 02
0030 ff ff 1d 2c 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 443
No. Time Source Destination Protocol Length Info
68416 29.631953 10.10.15.76 142.250.183.200 TCP 55 63771 → 443 [ACK] Seq=1 Ack=1 Win=252 Len=1
68495 29.643194 142.250.183.200 10.10.15.76 TCP 66 443 → 63771 [ACK] Seq=1 Ack=2 Win=1047 Len=0 SLE=1 SRE=2
73849 30.315703 10.10.15.76 104.18.32.47 TCP 55 63772 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1
73850 30.327090 104.18.32.47 10.10.15.76 TCP 66 443 → 63772 [ACK] Seq=1 Ack=2 Win=11 Len=0 SLE=1 SRE=2
73907 30.821390 10.10.15.76 104.16.80.73 TCP 55 63780 → 443 [ACK] Seq=1 Ack=1 Win=251 Len=1
73908 30.835329 104.16.80.73 10.10.15.76 TCP 66 443 → 63780 [ACK] Seq=1 Ack=2 Win=11 Len=0 SLE=1 SRE=2
73909 30.964593 10.10.15.76 216.239.38.178 TCP 55 63782 → 443 [ACK] Seq=1 Ack=1 Win=252 Len=1
73910 30.977497 216.239.38.178 10.10.15.76 TCP 66 443 → 63782 [ACK] Seq=1 Ack=2 Win=1047 Len=0 SLE=1 SRE=2
73920 31.601201 10.10.15.76 104.18.41.158 TCP 55 63783 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1
73921 31.614907 104.18.41.158 10.10.15.76 TCP 66 443 → 63783 [ACK] Seq=1 Ack=2 Win=9 Len=0 SLE=1 SRE=2
75275 34.057100 10.10.15.76 142.250.70.74 TCP 55 63786 → 443 [ACK] Seq=1 Ack=1 Win=252 Len=1
75276 34.073030 142.250.70.74 10.10.15.76 TCP 66 443 → 63786 [ACK] Seq=1 Ack=2 Win=1047 Len=0 SLE=1 SRE=2
75281 34.611901 52.113.194.132 10.10.15.76 TCP 60 443 → 63787 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75286 37.219680 10.10.15.76 142.250.182.195 TCP 55 63791 → 443 [ACK] Seq=1 Ack=1 Win=252 Len=1
75287 37.230238 142.250.182.195 10.10.15.76 TCP 66 443 → 63791 [ACK] Seq=1 Ack=2 Win=1045 Len=0 SLE=1 SRE=2
75289 37.650436 10.10.15.76 104.18.32.47 TCP 55 63773 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1
75290 37.660757 104.18.32.47 10.10.15.76 TCP 66 443 → 63773 [ACK] Seq=1 Ack=2 Win=19 Len=0 SLE=1 SRE=2
75291 37.729450 10.10.15.76 142.251.42.3 TCP 55 63793 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
75292 37.740510 142.251.42.3 10.10.15.76 TCP 66 443 → 63793 [ACK] Seq=1 Ack=2 Win=1012 Len=0 SLE=1 SRE=2
75293 39.015117 10.10.15.76 3.233.158.25 TCP 55 63794 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
75294 39.226225 3.233.158.25 10.10.15.76 TCP 66 443 → 63794 [ACK] Seq=1 Ack=2 Win=83 Len=0 SLE=1 SRE=2
76643 53.796241 3.233.158.25 10.10.15.76 TLSv1.2 93 Application Data
76644 53.796626 10.10.15.76 3.233.158.25 TCP 54 63794 → 443 [FIN, ACK] Seq=2 Ack=40 Win=255 Len=0
77980 54.007857 3.233.158.25 10.10.15.76 TLSv1.2 78 Application Data
77981 54.007857 3.233.158.25 10.10.15.76 TCP 60 443 → 63794 [FIN, ACK] Seq=64 Ack=3 Win=83 Len=0
77986 54.007942 10.10.15.76 3.233.158.25 TCP 54 63794 → 443 [RST, ACK] Seq=3 Ack=64 Win=0 Len=0
78413 60.701085 10.10.15.76 104.18.32.47 TCP 55 [TCP Keep-Alive] 63784 → 443 [ACK] Seq=1 Ack=1 Win=251 Len=1
78414 60.712627 104.18.32.47 10.10.15.76 TCP 66 [TCP Keep-Alive ACK] 443 → 63784 [ACK] Seq=1 Ack=2 Win=23 Len=0 SLE=1 SRE=2
Frame 5964: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\NPF_{A2B1644D-CA6
Ethernet II, Src: PaloAltoNetw_00:8e:10 (3c:fa:30:00:8e:10), Dst: HP_9c:ee:9c (00:68:eb:9c:ee:9c)
Internet Protocol Version 4, Src: 3.233.158.25, Dst: 10.10.15.76
Transmission Control Protocol, Src Port: 443, Dst Port: 63775, Seq: 1, Ack: 1, Len: 39
Source Port: 443
Destination Port: 63775
[Stream index: 0]
[Conversation completeness: Incomplete (60)]
[TCP Segment Len: 39]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 1697953420
[Next Sequence Number: 40 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1904936467
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSM, ACK)
0000 00 68 eb 9c ee 9c 3c fa 30 80 8e 10 08 00 45 00
0010 00 4f 6e a3 40 00 31 06 1f ae 03 e9 9e 19 0a 0a
0020 0f 4c 01 bb f9 1f 65 34 b6 8c 71 8b 06 13 50 18
0030 01 6b 1d 1d 00 00 17 03 03 00 22 de 6f 17 f2 1f
0040 1e c2 8a e4 e7 49 37 33 a2 83 89 3c f4 8e 12 ba
0050 ec e8 0f 9a e6 f2 cb d6 e2 ce 41 29 db
Bytes 59-92: Encrypted Application Data (tls.app_data)
Packets: 100428 · Displayed: 48 (0.0%)
Profile: Default