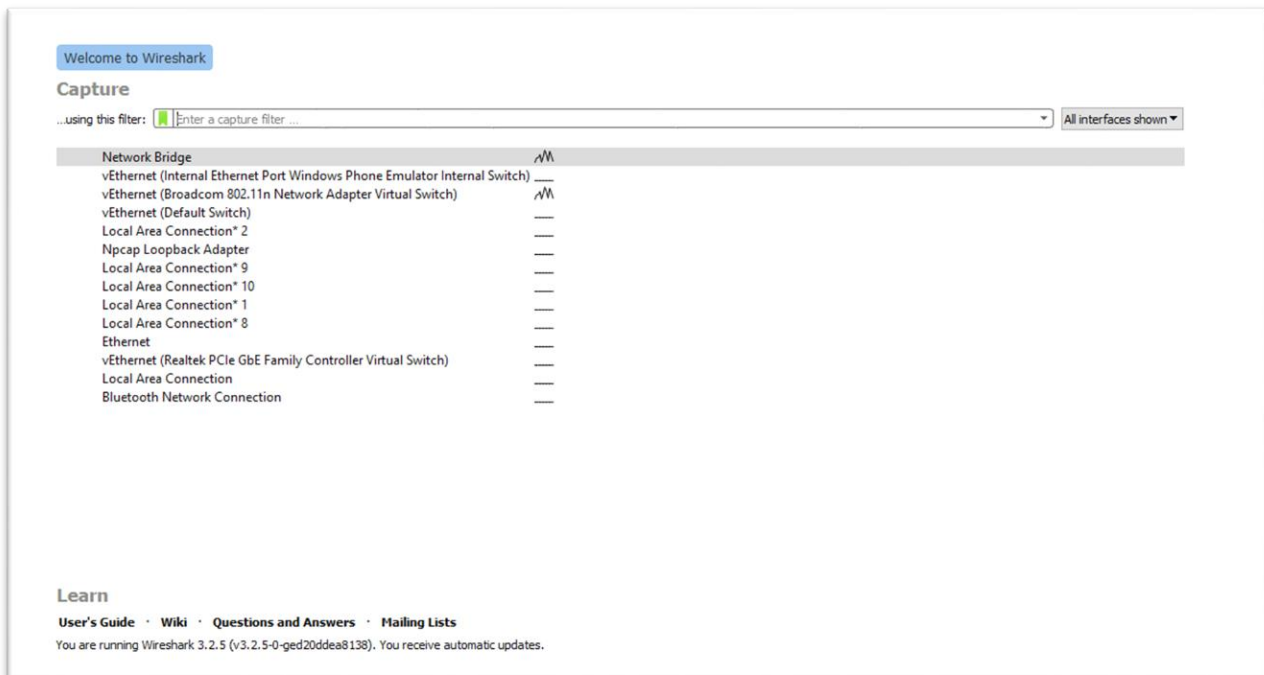


TASK 2

Capture the packets using Wireshark

Welcome Screen of Wireshark

- Select Interface & start Capturing Packets



TCP Packets List

- Use capture filter **tcp** to capture only TCP packets

tcp									
Io.	Time	Source	Destination	Protocol	Length	Internet Protocol Version 6	Info		
82	19.888992	2402:3a80:8eb:a206:...	64:ff9b::3472:1000	TCP	75	✓	1052 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP segment of a reassembled PDU]		
83	20.122280	64:ff9b::3472:1000	2402:3a80:8eb:a206:...	TCP	86	✓	443 → 1052 [ACK] Seq=1 Ack=2 Win=2045 Len=0 SLE=1 SRE=2		
84	20.246997	2402:3a80:8eb:a206:...	64:ff9b::3472:1000	TCP	75	✓	1051 → 443 [ACK] Seq=1 Ack=2 Win=254 Len=1 [TCP segment of a reassembled PDU]		
85	20.434937	64:ff9b::3472:1000	2402:3a80:8eb:a206:...	TCP	86	✓	443 → 1051 [ACK] Seq=1 Ack=2 Win=2045 Len=0 SLE=1 SRE=2		
86	22.025786	2402:3a80:8eb:a206:...	2606:4700:20:1ac43:...	TCP	75	✓	1053 → 443 [ACK] Seq=1 Ack=1 Win=257 Len=1 [TCP segment of a reassembled PDU]		
87	22.256560	2606:4700:20:1ac43:...	2402:3a80:8eb:a206:...	TCP	86	✓	443 → 1053 [ACK] Seq=1 Ack=2 Win=66 Len=0 SLE=1 SRE=2		
88	22.352761	2402:3a80:8eb:a206:...	2606:4700:20:1681a:...	TCP	75	✓	1056 → 443 [ACK] Seq=1 Ack=2 Win=258 Len=1 [TCP segment of a reassembled PDU]		
89	22.543678	2606:4700:20:1681a:...	2402:3a80:8eb:a206:...	TCP	86	✓	443 → 1056 [ACK] Seq=1 Ack=2 Win=66 Len=0 SLE=1 SRE=2		
90	22.752833	2402:3a80:8eb:a206:...	2606:4700:20:1681a:...	TCP	75	✓	1054 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP segment of a reassembled PDU]		
91	24.212769	2402:3a80:8eb:a206:...	2404:6800:4009:806:...	TCP	75	✓	1041 → 443 [ACK] Seq=1 Ack=1 Win=259 Len=1 [TCP segment of a reassembled PDU]		
92	24.308601	2404:6800:4009:806:...	2402:3a80:8eb:a206:...	TCP	86	✓	443 → 1041 [ACK] Seq=1 Ack=2 Win=388 Len=0 SLE=1 SRE=2		

Packet Information

```
> Frame 93: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{086B55E0-F055-453C-9742-F49AB7E8040E}, 10 B
> Ethernet II, Src: HonHaiPr_dc:38:d3 (e4:d5:3d:dc:38:d3), Dst: e2:b5:92:36:6b:96 (e2:b5:92:36:6b:96)
> Internet Protocol Version 6, Src: 2402:3a80:8eb:a206:c191:956b:bd0c:f3b3, Dst: 2606:4700:20::681a:bf0
> Transmission Control Protocol, Src Port: 3055, Dst Port: 443, Seq: 1, Len: 1, Win: 1
```

Packet Information in hexadecimal

0000	e2 d5 92 36 6b 96 e4 d5 3d dc 38 d3 8b ad b0 00	S.Kb,OUN =.8LT.-
0010	8d ef 00 15 06 ff 24 02 3a 80 08 eb a2 06 c1 91\$. :...sAj
0020	95 6b bd 0c f3 b3 26 06 47 00 00 20 00 00 00	n,]-3.&
0030	00 00 68 1a 0b f0 04 1f 01 bb a2 f1 4f c9 5c 4a	...0... .s1 I*.
0040	e4 69 50 10 01 04 f2 7d 00 00 00	U.&...2' ...

Observe the TCP packets and inside that observe the headers from Transport layer, Network layer and Data link layer.

Transport Layer Headers

```

' Transmission Control Protocol, Src Port: 1052, Dst Port: 443, Seq: 2, Ack: 1, Len: 0
  Source Port: 1052
  Destination Port: 443
  [Stream index: 6]
  [TCP Segment Len: 0]
  Sequence number: 2      (relative sequence number)
  Sequence number (raw): 647810703
  [Next sequence number: 3      (relative sequence number)]
  Acknowledgment number: 1      (relative ack number)
  Acknowledgment number (raw): 2063451464
  0101 .... = Header Length: 20 bytes (5)
  ▾ Flags: 0x011 (FIN, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    .... 0... = Congestion Window Reduced (CWR): Not set
    .... .0.. = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...1 = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    ▾ .... .... ...1 = Fin: Set
      ▾ [Expert Info (Chat/Sequence): Connection finish (FIN)]
        [Connection finish (FIN)]
        [Severity level: Chat]
        [Group: Sequence]
        [TCP Flags: .....A...F]
      Window size value: 258
      [Calculated window size: 258]
      [Window size scaling factor: -1 (unknown)]
      Checksum: 0x55be [unverified]
      [Checksum Status: Unverified]
      Urgent pointer: 0
  ▾ [Timestamps]
    [Time since first frame in this TCP stream: 17.195194000 seconds]
    [Time since previous frame in this TCP stream: 16.961906000 seconds]

```

Network Layer Headers

```

Internet Protocol Version 6, Src: 2402:3a80:8eb:a206:c191:956b:bd0c:f3b3, Dst: 64:ff9b::3472:1000
  0110 .... = Version: 6
  ▾ .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0000 00.. .... = Differentiated Services Codepoint: Default (0)
      .... ..00 .... = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    .... 0010 0101 1000 0010 1101 = Flow Label: 0x2582d
  Payload Length: 20
  Next Header: TCP (6)
  Hop Limit: 255
  Source: 2402:3a80:8eb:a206:c191:956b:bd0c:f3b3
  Destination: 64:ff9b::3472:1000
  [Destination Embedded IPv4: 52.114.16.0]

```

Data Link Layer Headers

```

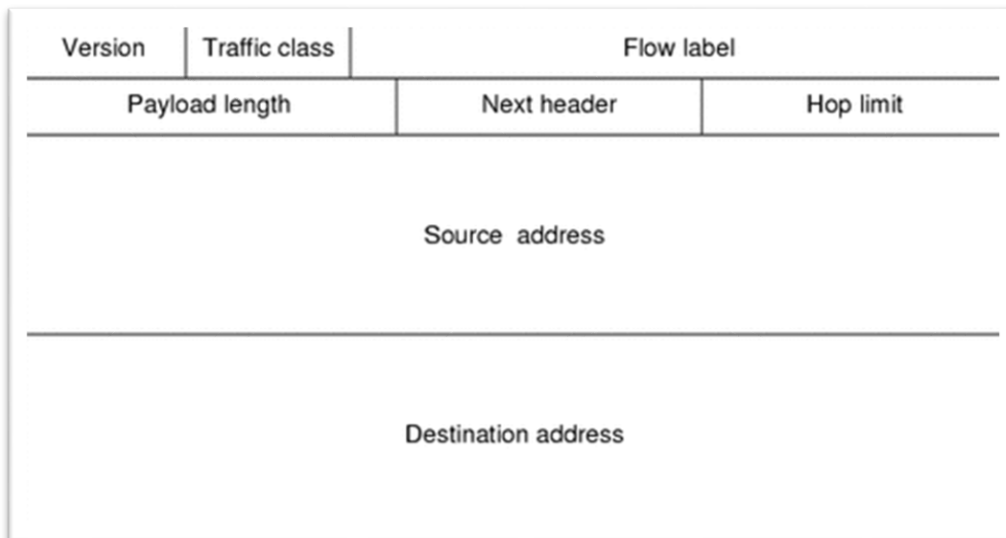
Ethernet II, Src: HonHaiPr_dc:38:d3 (e4:d5:3d:dc:38:d3), Dst: e2:b5:92:36:6b:96 (e2:b5:92:36:6b:96)
  ▾ Destination: e2:b5:92:36:6b:96 (e2:b5:92:36:6b:96)
    Address: e2:b5:92:36:6b:96 (e2:b5:92:36:6b:96)
    .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)
    .... ...0 .... = IG bit: Individual address (unicast)
  ▾ Source: HonHaiPr_dc:38:d3 (e4:d5:3d:dc:38:d3)
    Address: HonHaiPr_dc:38:d3 (e4:d5:3d:dc:38:d3)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ...0 .... = IG bit: Individual address (unicast)
  Type: IPv6 (0x86dd)
  Type: IPv6 (0x86dd)

```

Observe what is inside the IP header.

IPV6 Header

- Format



- IPV6 Header Information

```

Internet Protocol Version 6, Src: 2402:3a80:8eb:a206:c191:956b:bd0c:f3b3, Dst: 64:ff9b::34/2:1000
  0110 .... = Version: 6
  ▾ .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0000 00.. .... = Differentiated Services Codepoint: Default (0)
    .... ..00 .... = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    .... 0010 0101 1000 0010 1101 = Flow Label: 0x2582d
  Payload Length: 20
  Next Header: TCP (6)
  Hop Limit: 255
  Source: 2402:3a80:8eb:a206:c191:956b:bd0c:f3b3
  Destination: 64:ff9b::3472:1000
  [Destination Embedded IPv4: 52.114.16.0]

```