

**Department of Computer Science and Engineering**  
**U18CSI5201\_Computer Networks Laboratory**

**Reg: no:22BCS308**

**Exp: no: 4**

Simulation of Data Link layer and Network Layer Protocols.

**Aim:**

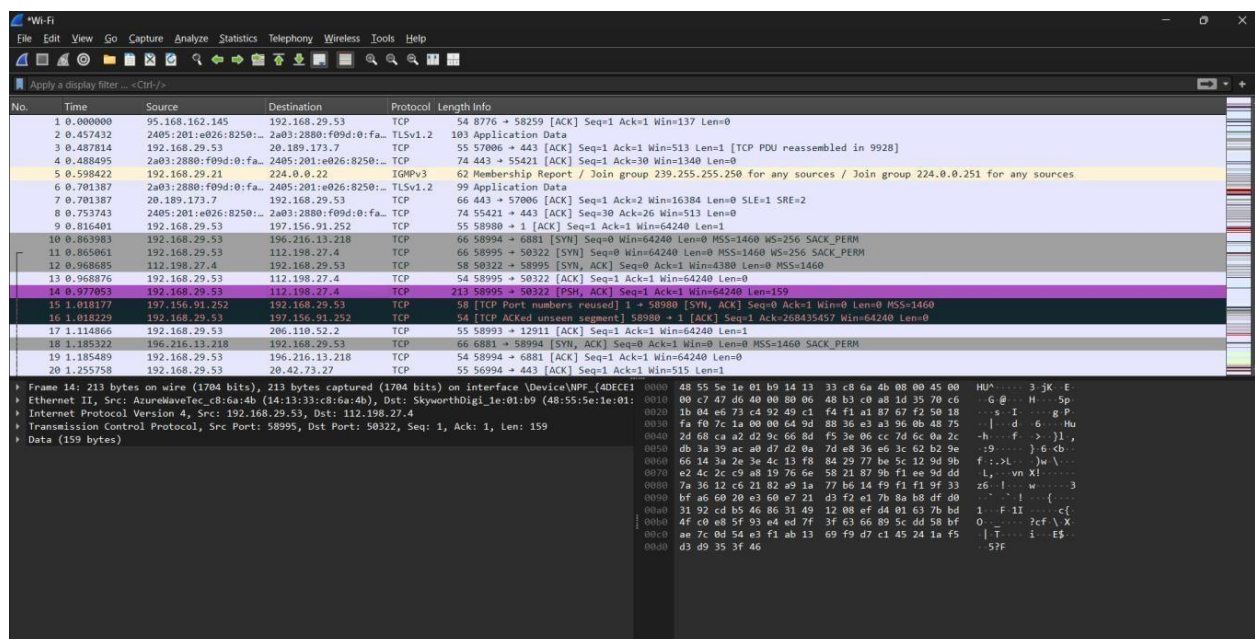
To Simulate the Data Link layer and Network Layer Protocols using the Wireshark application.

**TCP Protocol:**

- a. Demonstrate the frame transmission scenario using Sniffing tool.

*Sol:*

1. Choose the network interface to monitor, such as the Wi-Fi interface if you're connected via Wi-Fi.
2. With Wireshark running, perform activities that generate network traffic.
3. To capture TCP packets, initiate any task that involves TCP communication.
4. Wireshark captures traffic as frames, with each frame representing a network packet for analysis.



Department of Computer Science and Engineering  
U18CSI5201\_Computer Networks Laboratory

Reg: no:22BCS308

Exp: no: 4

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl>/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	95.168.162.145	192.168.29.53	TCP	54	8776 → 58259 [ACK] Seq=1 Ack=1 Win=137 Len=0
2	0.457432	2405:201:e026:8250::	2a03:2880:f09d:0:fa...	TLSv1.2	103	Application Data
3	0.487814	192.168.29.53	20.189.173.7	TCP	55	57006 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP PDU reassembled in 9928]
4	0.488495	2a03:2880:f09d:0:fa...	2405:201:e026:8250::	TCP	74	443 → 55421 [ACK] Seq=1 Ack=30 Win=1340 Len=0
5	0.598422	192.168.29.21	224.0.0.22	IGMPv3	62	Membership Report / Join group 239.255.255.250 for any sources / Join group 224.0.0.251 for any sources
6	0.701387	2a03:2880:f09d:0:fa...	2405:201:e026:8250::	TLSv1.2	99	Application Data
7	0.701387	20.189.173.7	192.168.29.53	TCP	66	443 → 57006 [ACK] Seq=1 Ack=2 Win=16384 Len=0 SLE=1 SRE=2
8	0.753743	2405:201:e026:8250::	2a03:2880:f09d:0:fa...	TCP	74	55421 → 443 [ACK] Seq=30 Ack=26 Win=513 Len=0
9	0.816401	192.168.29.53	197.156.91.252	TCP	55	58980 → 1 [ACK] Seq=1 Ack=1 Win=64240 Len=1
10	0.863983	192.168.29.53	196.216.13.218	TCP	66	58994 → 6881 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
11	0.865061	192.168.29.53	112.198.27.4	TCP	66	58995 → 50322 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
12	0.968685	112.198.27.4	192.168.29.53	TCP	58	50322 → 58995 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460
13	0.968876	192.168.29.53	112.198.27.4	TCP	54	58995 → 50322 [ACK] Seq=1 Ack=1 Win=64240 Len=0
14	0.977053	192.168.29.53	112.198.27.4	TCP	213	58995 → 50322 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=159
15	1.018177	197.156.91.252	192.168.29.53	TCP	58	[TCP Port numbers reused] 1 → 58980 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0 MSS=1460
16	1.018229	192.168.29.53	197.156.91.252	TCP	54	[TCP ACKed unseen segment] 58980 → 1 [ACK] Seq=1 Ack=268435457 Win=64240 Len=0
17	1.114866	192.168.29.53	206.110.52.2	TCP	55	58993 → 12911 [ACK] Seq=1 Ack=1 Win=64240 Len=1
18	1.185332	196.216.13.218	192.168.29.53	TCP	66	6881 → 58994 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0 MSS=1460 SACK_PERM
19	1.185489	192.168.29.53	196.216.13.218	TCP	54	58994 → 6881 [ACK] Seq=1 Ack=1 Win=64240 Len=0
20	1.255758	192.168.29.53	20.42.73.27	TCP	55	56994 → 443 [ACK] Seq=1 Ack=1 Win=515 Len=1

▼ Frame 14: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bits) on interface \Device\NPF\_{4DECE115-919A-43CE-B75C-24595927E4B3}

Section number: 1

Interface id: 0 (\Device\NPF\_{4DECE115-919A-43CE-B75C-24595927E4B3})

Encapsulation type: Ethernet (1)

Arrival Time: Sep 14, 2024 21:00:37.354393000 India Standard Time

UTC Arrival Time: Sep 14, 2024 15:30:37.354393000 UTC

Epoch Arrival Time: 1726327837.354393000

[Time shift for this packet: 0.000000000 seconds]

[Time delta from previous captured frame: 0.008177000 seconds]

[Time delta from previous displayed frame: 0.008177000 seconds]

[Time since reference or first frame: 0.977053000 seconds]

Frame Number: 14

Frame Length: 213 bytes (1704 bits)

Capture Length: 213 bytes (1704 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp:data]

[Coloring Rule Name: TCP]

[Coloring Rule String: tcp]

Ethernet II, Src: AzureWaveFec\_c8:6a:4b (14:13:33:c8:6a:4b), Dst: SkyworthDigi\_Ie:01:b9 (48:55:5e:1e:01:b9)

0000 48 55 5e 1e 01 b9 14 13 33 c8 6a 4b 08 00 45 00 HUA... 3 JK E  
0010 00 c7 d6 40 00 80 06 48 b3 c0 a8 1d 35 70 c6 ...G @... H... Sp  
0020 1b 04 e6 73 c4 92 49 c1 f4 f1 a1 87 67 f2 50 18 ...s T... g P  
0030 fa f6 7c 1a 00 00 64 9d 80 36 e3 a3 96 0b 48 75 ...|... d... 6... Hu  
0040 2d 68 ce a2 d2 9c 66 8d f5 3e 06 cc 7d 6c 0a 2c ...h... f... > j l,  
0050 db 3a 39 ac a0 d7 d2 0a 7d e8 36 e6 3c 62 b2 9e ...9... ) 6 db  
0060 66 14 3a 2e 3e 4c 13 f8 84 29 77 be 5c 12 9d 9b ...f...>L...>u\...  
0070 e2 4c 2c c9 a8 19 76 6e 50 21 87 9b f1 ee 9d dd ...L...v n Xl...  
0080 7a 36 12 c6 21 82 a9 1a 77 b6 14 f9 f1 f1 9f 33 26 11... e... 3  
0090 bf a6 60 20 e3 60 e7 21 d3 f2 e1 7b 8a b8 df d0 ...-... l...{-...  
00a0 31 92 cd b5 46 86 31 49 12 08 ef d4 01 63 7b bd 1...F 1l... c{  
00b0 4f c0 e8 5f 93 e4 ed 7f 3f 63 66 89 5c dd 58 bf 0...-... 2cf \X  
00c0 ae 7c 0d 54 e3 f1 ab 13 69 f9 d7 c1 45 24 1a f5 ...l T... i... E\$  
00d0 d3 d9 35 3f 46 ...57F

▼ Frame 14: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bits) on interface \Device\NPF\_{4DECE115-919A-43CE-B75C-24595927E4B3}

Section number: 1

Interface id: 0 (\Device\NPF\_{4DECE115-919A-43CE-B75C-24595927E4B3})

Encapsulation type: Ethernet (1)

Arrival Time: Sep 14, 2024 21:00:37.354393000 India Standard Time

UTC Arrival Time: Sep 14, 2024 15:30:37.354393000 UTC

Epoch Arrival Time: 1726327837.354393000

[Time shift for this packet: 0.000000000 seconds]

[Time delta from previous captured frame: 0.008177000 seconds]

[Time delta from previous displayed frame: 0.008177000 seconds]

[Time since reference or first frame: 0.977053000 seconds]

Frame Number: 14

Frame Length: 213 bytes (1704 bits)

Capture Length: 213 bytes (1704 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp:data]

[Coloring Rule Name: TCP]

[Coloring Rule String: tcp]

**Department of Computer Science and Engineering**  
**U18CSI5201\_Computer Networks Laboratory**

**Reg: no:22BCS308**

**Exp: no: 4**

- b. Demonstrate the packet transmission scenario using Sniffing tool.

*Sol:*

```
▼ Internet Protocol Version 4, Src: 192.168.29.53, Dst: 112.198.27.4
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 199
    Identification: 0x47d6 (18390)
  ▶ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x48b3 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.29.53
    Destination Address: 112.198.27.4
    [Stream index: 5]

▼ Transmission Control Protocol, Src Port: 58995, Dst Port: 50322, Seq: 1, Ack: 1, Len: 159
  Source Port: 58995
  Destination Port: 50322
  [Stream index: 5]
  [Stream Packet Number: 4]
  ▶ [Conversation completeness: Complete, WITH_DATA (47)]
  [TCP Segment Len: 159]
  Sequence Number: 1      (relative sequence number)
  Sequence Number (raw): 1237447921
  [Next Sequence Number: 160      (relative sequence number)]
  Acknowledgment Number: 1      (relative ack number)
  Acknowledgment number (raw): 2710005746
  0101 .... = Header Length: 20 bytes (5)
  ▶ Flags: 0x018 (PSH, ACK)
    Window: 64240
    [Calculated window size: 64240]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x7c1a [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▶ [Timestamps]
  ▶ [SEQ/ACK analysis]
    TCP payload (159 bytes)
```

Department of Computer Science and Engineering  
U18CSI5201\_Computer Networks Laboratory

Reg: no:22BCS308

Exp: no: 4

## HTTP protocol:

a. Demonstrate the frame transmission scenario using Sniffing tool.

Sol:

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The packet list pane shows several captured packets, with packet 1074 selected. The packet details pane for packet 1074 shows the following structure:

- Ethernet II, Src: QindaoIntel\_c9:a5:48 (bc:5c:17:c9:a5:48), Dst: AzureWaveTec\_c8:6a:4b (14:13:33:c8:6a:4b)
- Internet Protocol Version 4, Src: 192.168.29.21, Dst: 192.168.29.53
- Hypertext Transfer Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII column shows the following text:

```
GET /ssdp/device-desc.xml HTTP/1.1
```

```
▼ Frame 1074: 1240 bytes on wire (9920 bits), 1240 bytes captured (9920 bits) on interface \Device\NPF_{4DECE115-919A-43CE-B75C-24595927E4B3}
  Section number: 1
  ▶ Interface id: 0 (\Device\NPF_{4DECE115-919A-43CE-B75C-24595927E4B3})
  Encapsulation type: Ethernet (1)
  Arrival Time: Sep 14, 2024 21:01:00.945862000 India Standard Time
  UTC Arrival Time: Sep 14, 2024 15:31:00.945862000 UTC
  Epoch Arrival Time: 1726327860.945862000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.003707000 seconds]
  [Time delta from previous displayed frame: 0.005257000 seconds]
  [Time since reference or first frame: 24.568522000 seconds]
  Frame Number: 1074
  Frame Length: 1240 bytes (9920 bits)
  Capture Length: 1240 bytes (9920 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:http:xml]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
```



- b. Demonstrate the packet transmission scenario using Sniffing tool.

*Sol:*

```
▼ Internet Protocol Version 4, Src: 192.168.29.21, Dst: 192.168.29.53
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1226
    Identification: 0xcd7a (52602)
  ▶ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xad18 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.29.21
    Destination Address: 192.168.29.53
    [Stream index: 21]
▼ Transmission Control Protocol, Src Port: 8008, Dst Port: 59025, Seq: 1, Ack: 246, Len: 1186
  Source Port: 8008
  Destination Port: 59025
  [Stream index: 90]
  [Stream Packet Number: 6]
  ▶ [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 1186]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 1317094730
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Application-URL:http://192.168.29.21:8008/apps/\r\n
  ▶ Content-Length:1067\r\n
    Content-Type:application/xml\r\n
    \r\n
    [Request in frame: 1071]
    [Time since request: 0.005257000 seconds]
    [Request URI: /ssdp/device-desc.xml]
    [Full request URI: http://192.168.29.21:8008/ssdp/device-desc.xml]
    File Data: 1067 bytes
```

**Result:**

The Experiment was successfully completed and demonstrated packet and frame transmission.