Date: 13 / 08 / 2025

Lab Practical #09:

Study Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)

Practical Assignment #09:

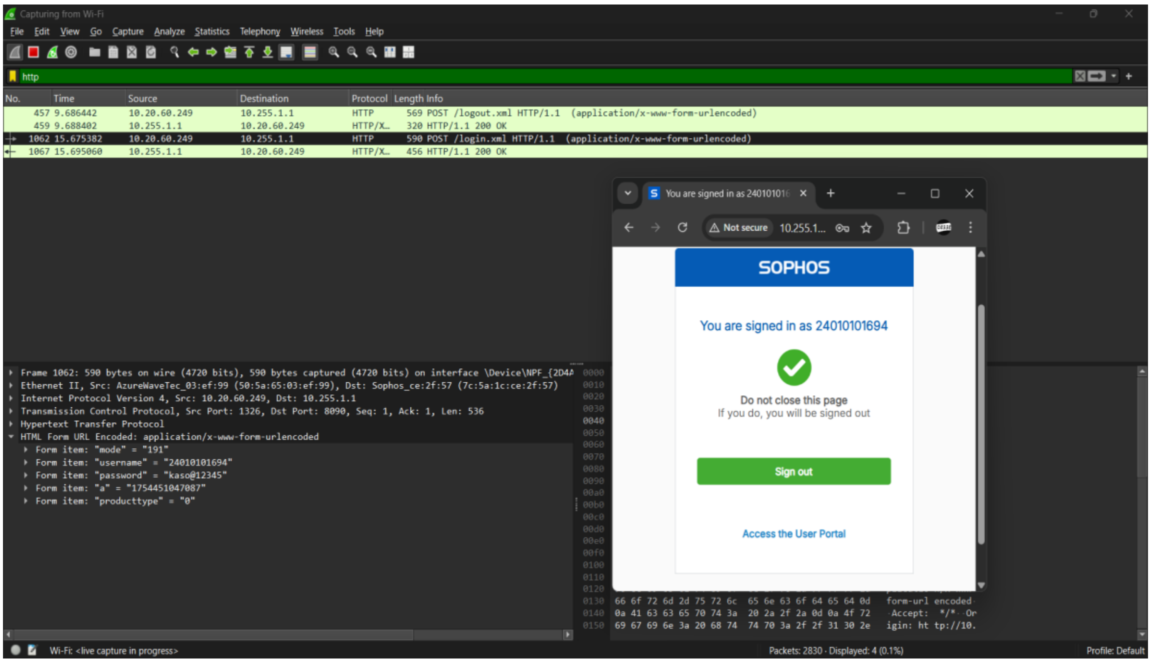
1. **Explain usage of Wireshark tool.**
2. **Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)**

Ans-1:

- Wireshark is a free open-source tool that analyzes network traffic in real-time for Windows, Mac, Unix, and Linux systems. It captures data packets passing through a network interface (such as Ethernet, LAN, or SDRs) and translates that data into valuable information for IT professionals and cybersecurity teams.

Ans-2:

- **HTTP (Hypertext Transfer Protocol)**


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time       Source         Destination   Protocol Length Info
  457 9.686442   10.20.60.249   10.255.1.1    HTTP     569 POST /logout.xml HTTP/1.1  (application/x-www-form-urlencoded)
  459 9.688402   10.255.1.1     10.20.60.249  HTTP/X…  320 HTTP/1.1 200 OK
 1062 15.675382  10.20.60.249   10.255.1.1    HTTP     590 POST /login.xml HTTP/1.1  (application/x-www-form-urlencoded)
 1067 15.695060  10.255.1.1     10.20.60.249  HTTP/X…  456 HTTP/1.1 200 OK
```

```
Frame 1062: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\NPF_{2D4A
Ethernet II, Src: AzureWaveTec_03:ef:99 (50:5a:65:03:ef:99), Dst: Sophos_ce:2f:57 (7c:5a:1c:ce:2f:57)
Internet Protocol Version 4, Src: 10.20.60.249, Dst: 10.255.1.1
Transmission Control Protocol, Src Port: 1326, Dst Port: 8090, Seq: 1, Ack: 1, Len: 536
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
    Form item: "mode" = "191"
    Form item: "username" = "24010101694"
    Form item: "password" = "kaso@12345"
    Form item: "a" = "1754451047087"
    Form item: "producttype" = "0"
```

```
0130  66 6f 72 6d 2d 75 72 6c  65 6e 63 6f 64 65 64 0d   form-url encoded·
0140  0a 41 63 63 65 70 74 3a  20 2a 2f 2a 0d 0a 4f 72   ·Accept:  */*··Or
0150  69 67 69 6e 3a 20 68 74  74 70 3a 2f 2f 31 30 2e   igin: ht tp://10.
```

You are signed in as 24010101694

Do not close this page
If you do, you will be signed out

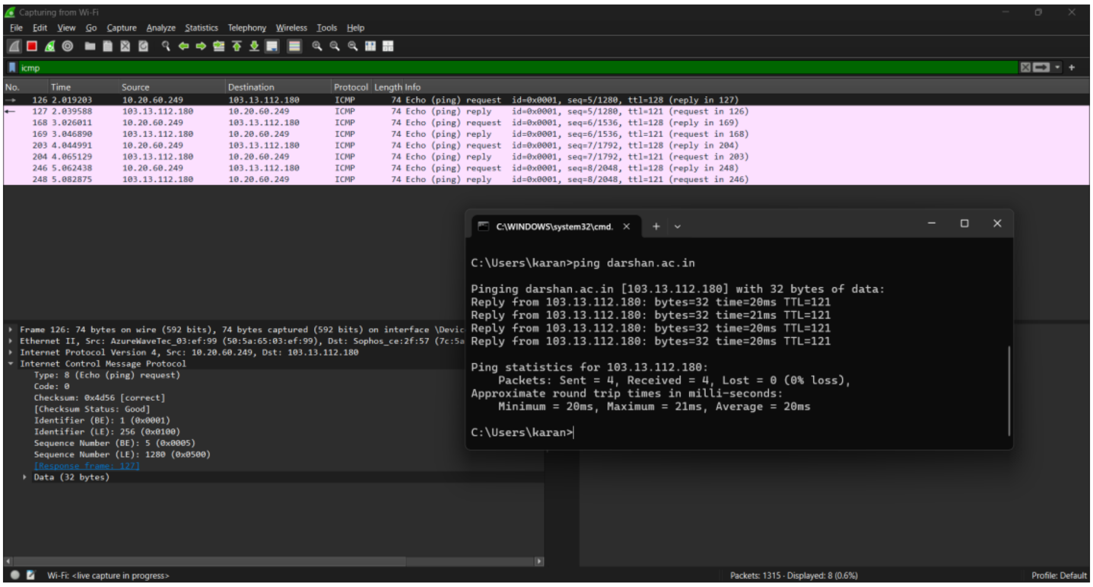
Wi-Fi: <live capture in progress>

Packets: 2830 · Displayed: 4 (0.1%)

Profile: Default

Date: 13 / 08 / 2025

- **IP (Internet Protocol)**


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
C:\WINDOWS\system32\cmd.
Wi-Fi: <live capture in progress>
Packets: 1315 · Displayed: 8 (0.6%)
Profile: Default

```
No.    Time       Source          Destination     Protocol Length Info
  126 2.019203   10.20.60.249    103.13.112.180  ICMP      74 Echo (ping) request  id=0x0001, seq=5/1280, ttl=128 (reply in 127)
  127 2.039588   103.13.112.180  10.20.60.249    ICMP      74 Echo (ping) reply    id=0x0001, seq=5/1280, ttl=121 (request in 126)
  168 3.026011   10.20.60.249    103.13.112.180  ICMP      74 Echo (ping) request  id=0x0001, seq=6/1536, ttl=128 (reply in 169)
  169 3.046890   103.13.112.180  10.20.60.249    ICMP      74 Echo (ping) reply    id=0x0001, seq=6/1536, ttl=121 (request in 168)
  203 4.044991   10.20.60.249    103.13.112.180  ICMP      74 Echo (ping) request  id=0x0001, seq=7/1792, ttl=128 (reply in 204)
  204 4.065129   103.13.112.180  10.20.60.249    ICMP      74 Echo (ping) reply    id=0x0001, seq=7/1792, ttl=121 (request in 203)
  246 5.062438   10.20.60.249    103.13.112.180  ICMP      74 Echo (ping) request  id=0x0001, seq=8/2048, ttl=128 (reply in 248)
  248 5.082875   103.13.112.180  10.20.60.249    ICMP      74 Echo (ping) reply    id=0x0001, seq=8/2048, ttl=121 (request in 246)
```

```
> Frame 126: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Devic
> Ethernet II, Src: AzureWaveTec_03:ef:99 (50:5a:65:03:ef:99), Dst: Sophos_ce:2f:57 (7c:5a
> Internet Protocol Version 4, Src: 10.20.60.249, Dst: 103.13.112.180
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d56 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 5 (0x0005)
    Sequence Number (LE): 1280 (0x0500)
    [Response frame: 127]
  > Data (32 bytes)
```

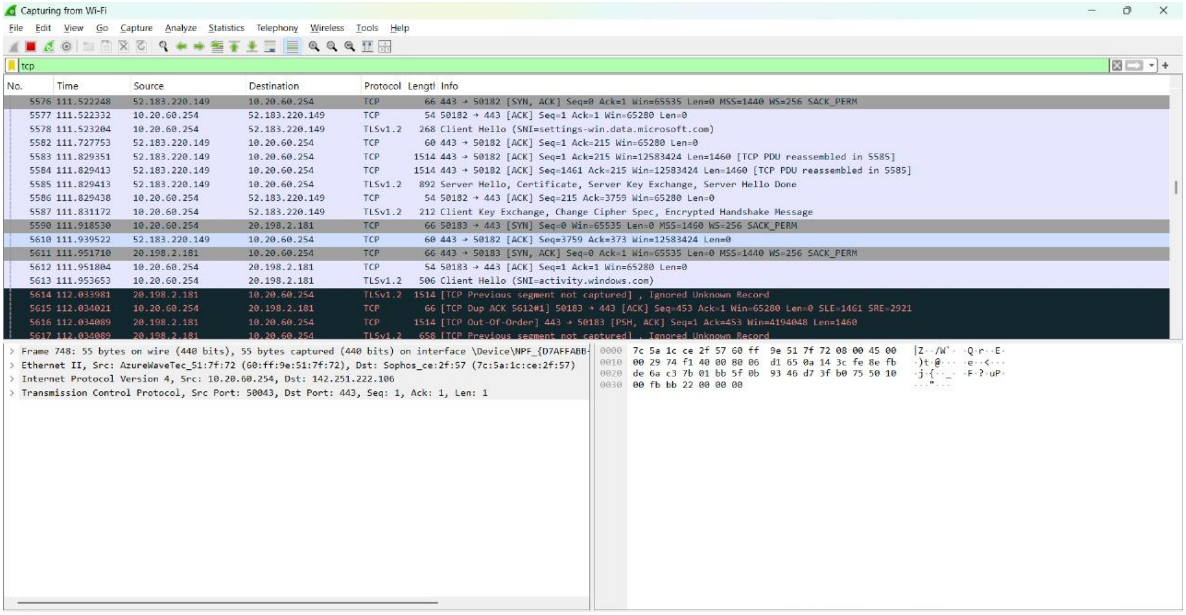
```
C:\Users\karan>ping darshan.ac.in

Pinging darshan.ac.in [103.13.112.180] with 32 bytes of data:
Reply from 103.13.112.180: bytes=32 time=20ms TTL=121
Reply from 103.13.112.180: bytes=32 time=21ms TTL=121
Reply from 103.13.112.180: bytes=32 time=20ms TTL=121
Reply from 103.13.112.180: bytes=32 time=20ms TTL=121

Ping statistics for 103.13.112.180:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 21ms, Average = 20ms

C:\Users\karan>
```

- **TCP (Transmission Control Protocol)**


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

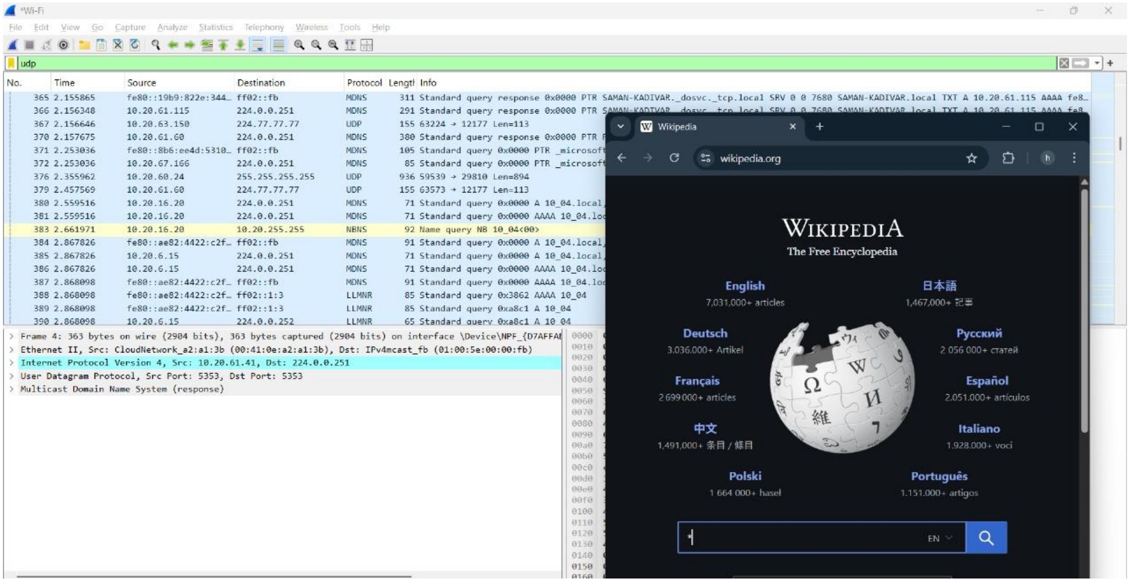
```
No.   Time        Source          Destination     Protocol Lengtl Info
 5576 111.522248  52.183.220.149  10.20.60.254    TCP       66 443 → 50182 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
 5577 111.522332  10.20.60.254    52.183.220.149  TCP       54 50182 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
 5578 111.523204  10.20.60.254    52.183.220.149  TLSv1.2  268 Client Hello (SNI=settings-win.data.microsoft.com)
 5582 111.727753  52.183.220.149  10.20.60.254    TCP       60 443 → 50182 [ACK] Seq=1 Ack=215 Win=65280 Len=0
 5583 111.829351  52.183.220.149  10.20.60.254    TCP     1514 443 → 50182 [ACK] Seq=1 Ack=215 Win=12583424 Len=1460 [TCP PDU reassembled in 5585]
 5584 111.829413  52.183.220.149  10.20.60.254    TCP     1514 443 → 50182 [ACK] Seq=1461 Ack=215 Win=12583424 Len=1460 [TCP PDU reassembled in 5585]
 5585 111.829413  52.183.220.149  10.20.60.254    TLSv1.2  892 Server Hello, Certificate, Server Key Exchange, Server Hello Done
 5586 111.829438  10.20.60.254    52.183.220.149  TCP       54 50182 → 443 [ACK] Seq=215 Ack=3759 Win=65280 Len=0
 5587 111.831172  10.20.60.254    52.183.220.149  TLSv1.2  212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 5590 111.918530  10.20.60.254    20.198.2.181    TCP       66 50183 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 5610 111.939522  52.183.220.149  10.20.60.254    TCP       60 443 → 50182 [ACK] Seq=3759 Ack=373 Win=12583424 Len=0
 5611 111.951710  20.198.2.181    10.20.60.254    TCP       66 443 → 50183 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
 5612 111.951804  10.20.60.254    20.198.2.181    TCP       54 50183 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
 5613 111.953653  10.20.60.254    20.198.2.181    TLSv1.2  506 Client Hello (SNI=activity.windows.com)
 5614 112.033981  20.198.2.181    10.20.60.254    TLSv1.2 1514 [TCP Previous segment not captured] , Ignored Unknown Record
 5615 112.034021  10.20.60.254    20.198.2.181    TCP       66 [TCP Dup ACK 5612#1] 50183 → 443 [ACK] Seq=453 Ack=1 Win=65280 Len=0 SLE=1461 SRE=2921
 5616 112.034089  20.198.2.181    10.20.60.254    TCP     1514 [TCP Out-Of-Order] 443 → 50183 [PSH, ACK] Seq=1 Ack=453 Win=4194048 Len=1460
 5617 112.034089  20.198.2.181    10.20.60.254    TLSv1.2  658 [TCP Previous segment not captured] , Ignored Unknown Record
```

```
> Frame 748: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{D7AFFABB-
> Ethernet II, Src: AzureWaveTec_51:7f:72 (60:ff:9e:51:7f:72), Dst: Sophos_ce:2f:57 (7c:5a:1c:ce:2f:57)
> Internet Protocol Version 4, Src: 10.20.60.254, Dst: 142.251.222.106
> Transmission Control Protocol, Src Port: 50043, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
```

```
0000  7c 5a 1c ce 2f 57 60 ff  9e 51 7f 72 08 00 45 00   |Z··/W`· ·Q·r··E·
0010  00 29 74 f1 40 00 80 06  d1 65 0a 14 3c fe 8e fb   ·)t·@··· ·e··<···
0020  de 6a c3 7b 01 bb 5f 0b  93 46 d7 3f b0 75 50 10   ·j·{··_· ·F·?·uP·
0030  00 fb bb 22 00 00 00                               ···"···
```

Date: 13 / 08 / 2025

- **UDP (User Datagram Protocol)**



```
No.   Time      Source                 Destination      Protocol Length Info
  365 2.155865  fe80::19b9:822e:344…   ff02::fb         MDNS     311 Standard query response 0x0000 PTR SAMAN-KADIVAR._dosvc._tcp.local SRV 0 0 7680 SAMAN-KADIVAR.local TXT A 10.20.61.115 AAAA fe8…
  366 2.156348  10.20.61.115           224.0.0.251      MDNS     291 Standard query response 0x0000 PTR SAMAN-KADIVAR._dosvc._tcp.local SRV 0 0 7680 SAMAN-KADIVAR.local TXT A 10.20.61.115 AAAA fe8…
  367 2.156646  10.20.63.150           224.77.77.77     UDP      155 63224 → 12177 Len=113
  370 2.157675  10.20.61.60            224.0.0.251      MDNS     380 Standard query response 0x0000 PTR F
  371 2.253036  fe80::8b6:ee4d:5310…   ff02::fb         MDNS     105 Standard query 0x0000 PTR _microsoft
  372 2.253036  10.20.67.166           224.0.0.251      MDNS      85 Standard query 0x0000 PTR _microsoft
  376 2.355962  10.20.60.24            255.255.255.255  UDP      936 59539 → 29810 Len=894
  379 2.457569  10.20.61.60            224.77.77.77     UDP      155 63573 → 12177 Len=113
  380 2.559516  10.20.16.20            224.0.0.251      MDNS      71 Standard query 0x0000 A 10_04.local,
  381 2.559516  10.20.16.20            224.0.0.251      MDNS      71 Standard query 0x0000 AAAA 10_04.loc
  383 2.661971  10.20.16.20            10.20.255.255    NBNS      92 Name query NB 10_04<00>
  384 2.867826  fe80::ae82:4422:c2f…   ff02::fb         MDNS      91 Standard query 0x0000 A 10_04.local,
  385 2.867826  10.20.6.15             224.0.0.251      MDNS      71 Standard query 0x0000 A 10_04.local,
  386 2.867826  10.20.6.15             224.0.0.251      MDNS      71 Standard query 0x0000 AAAA 10_04.loc
  387 2.868098  fe80::ae82:4422:c2f…   ff02::fb         MDNS      91 Standard query 0x0000 AAAA 10_04.loc
  388 2.868098  fe80::ae82:4422:c2f…   ff02::1:3        LLMNR     85 Standard query 0x3862 AAAA 10_04
  389 2.868098  fe80::ae82:4422:c2f…   ff02::1:3        LLMNR     85 Standard query 0xa8c1 A 10_04
  390 2.868098  10.20.6.15             224.0.0.252      LLMNR     65 Standard query 0xa8c1 A 10_04

> Frame 4: 363 bytes on wire (2904 bits), 363 bytes captured (2904 bits) on interface \Device\NPF_{D7AFFAE
> Ethernet II, Src: CloudNetwork_a2:a1:3b (00:41:0e:a2:a1:3b), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
> Internet Protocol Version 4, Src: 10.20.61.41, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
> Multicast Domain Name System (response)
```