

Date: 22/08/24

Lab Practical #08:

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

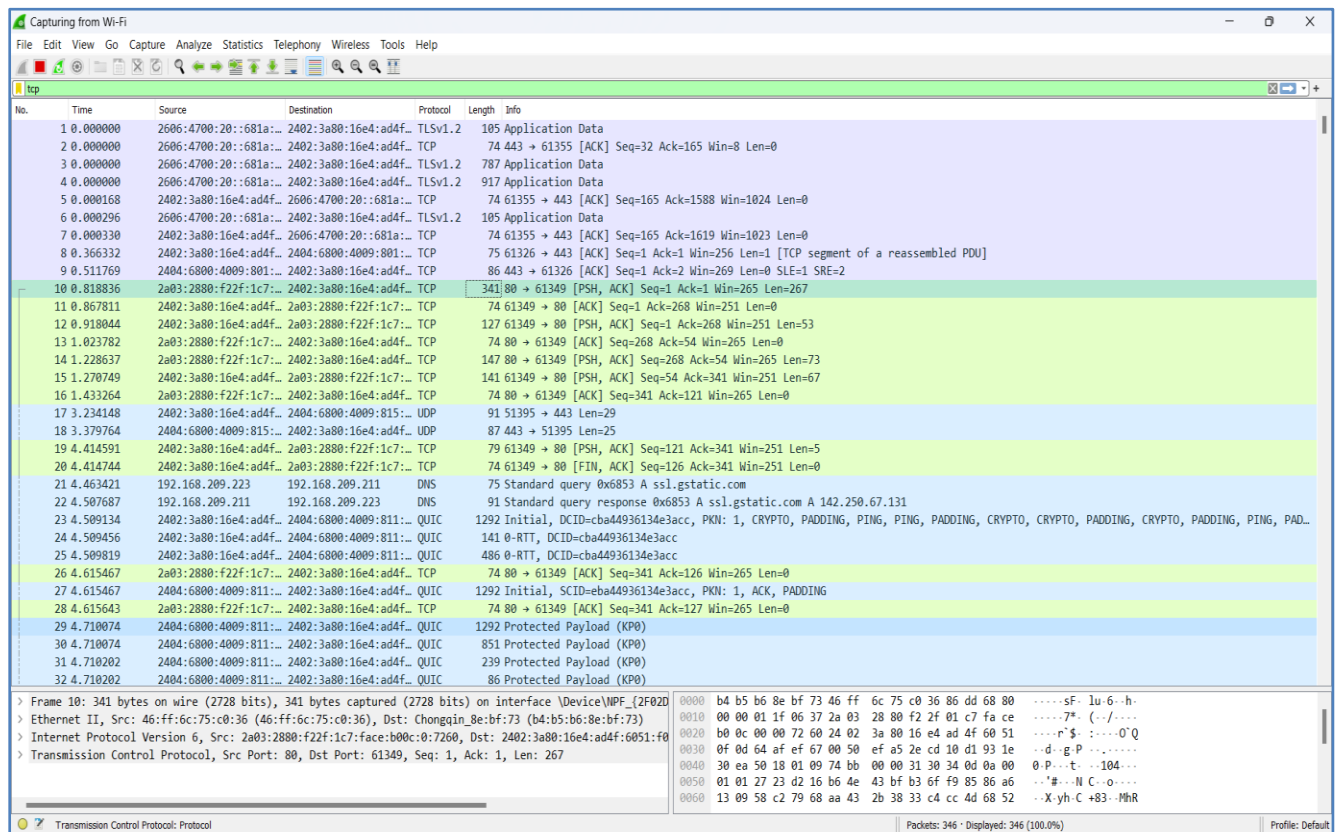
Practical Assignment #08:

1. Explain usage of Wireshark tool.

Wireshark is a widely used, open source network analyzer that can capture and display real-time details of network traffic. It is particularly useful for troubleshooting network issues, analyzing network protocols and ensuring network security. Networks must be monitored to ensure smooth operations and security.

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

TCP :



Wireshark packet capture interface showing TCP traffic. The packet list on the left shows various TCP segments. The packet details pane on the right shows the selected packet (No. 10) with its TCP header and application data. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.



22DARSHAN INSTITUTE OF ENGINEERING & TECHNOLOGY

Semester 5th | Practical Assignment | Computer Networks (2301CS501)

Date: 22/08/24

UDP :

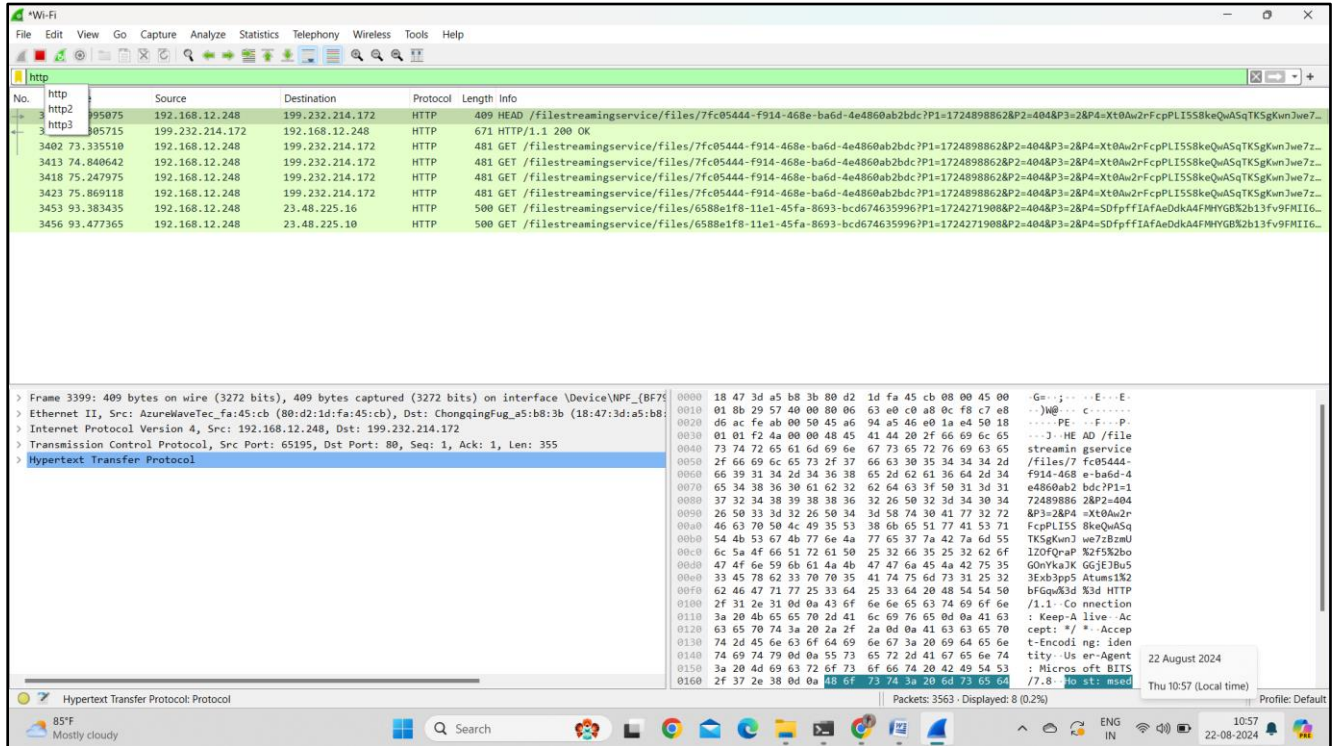
Wireshark packet capture showing UDP traffic. The packet list shows a series of UDP packets from 2402:3a80:16e4:ad4f to 2404:6800:4009:815. The packet details pane shows the structure of a UDP packet, including the header and payload. The packet bytes pane shows the raw data in hexadecimal and ASCII.

IP :

Wireshark packet capture showing IP traffic. The packet list shows a series of IP packets from 2402:3a80:16e4:ad4f to 2404:6800:4009:815. The packet details pane shows the structure of an IP packet, including the header and payload. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Date: 22/08/24

HTTP :



The image shows a Wireshark packet capture of HTTP traffic. The top pane displays a list of packets, with packet 3399 selected. The middle pane shows the packet details for Hypertext Transfer Protocol. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Packet 3399: 409 bytes on wire (3272 bits), 409 bytes captured (3272 bits) on interface \Device\NPF_{BF7...}

Ethernet II, Src: AzureWaveTec_fa:45:cb (88:d2:1d:fa:45:cb), Dst: ChongqingFug_a5:b8:3b (18:47:3d:a5:b8:3b)

Internet Protocol Version 4, Src: 192.168.12.248, Dst: 199.232.214.172

Transmission Control Protocol, Src Port: 65195, Dst Port: 80, Seq: 1, Ack: 1, Len: 355

Hypertext Transfer Protocol

Raw packet data (hex and ASCII):

```
0000 18 47 3d a5 b8 3b 80 d2 1d fa 45 cb 08 00 45 00 -G...E...E...
0010 01 8b 29 57 40 00 80 06 63 e0 c0 a8 0c f8 c7 e8 -)M@...C...
0020 06 ac fe ab 00 50 45 a6 94 a5 46 e0 1a e4 50 18 -...PE...P...
0030 01 01 f2 4a 00 00 48 45 41 44 20 2f 66 69 6c 65 -...J-HE AD /File
0040 73 74 72 65 61 6d 69 6e 67 73 65 72 76 69 63 65 -streamin gservice
0050 2f 66 69 6c 65 73 2f 37 66 63 30 35 34 34 3d 2d -/files/7 fc05444-
0060 66 39 31 34 2d 34 36 38 65 2d 62 61 36 64 2d 34 -f914-468 e-ba6d-4
0070 65 34 38 36 30 61 62 32 62 64 63 3f 50 31 3d 31 -e4860ab2 bdc?P1=1
0080 37 32 34 38 39 38 38 36 32 26 50 32 3d 34 30 34 -72489886 2&P2=404
0090 26 50 33 3d 32 26 50 34 3d 58 74 30 41 77 32 72 -&P3=2&P4 =>Xt0Aw2r
00a0 46 63 70 50 4c 49 35 53 38 6b 65 51 77 41 53 71 -FcpPLISS 8keQwASq
00b0 54 4b 53 67 4b 77 6e 4a 77 65 37 7a 42 7a 6d 55 -TKSgKwnJ we7zBzuU
00c0 6c 5a 4f 66 51 72 61 50 25 32 66 35 25 32 62 6f -1Z0FQraP %2f5K2bo
00d0 47 4f 6e 59 6b 61 4a 4b 47 47 6a 45 4a 42 75 35 -G0hYkaJK G6jE7bu5
00e0 33 45 78 62 33 70 70 35 41 74 75 6d 73 31 25 32 -3Exb3pp5 Atums1k2
00f0 62 46 47 71 77 25 33 64 25 33 64 20 48 54 54 50 -bFGq&3d %3d HTTP
0100 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e -/1.1-Co nnection
0110 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 41 63 - : Keep-A live-Ac
0120 63 65 70 74 3a 20 2a 2f 2a 0d 0a 41 63 65 70 65 -cept: */*. Accep
0130 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 69 64 65 6e -t-Encodi ng: iden
0140 74 69 74 79 0d 0a 55 73 65 72 2d 41 67 65 6e 74 -tity-Us er-Agent
0150 3a 20 4d 69 63 72 6f 73 6f 66 74 20 42 49 54 53 - : Micros oft BITS
0160 2f 37 2e 38 0d 0a 48 6f 73 74 3a 20 6d 73 65 64 -/7.8...No st: msed
```