# Vivekanand Education Society's Institute of Technology

## Department of AI & DS Engineering

## Subject: Cryptography and System Security

## Class: D11AD

| | |
|---|---|
| **Roll No:** | **Name:** |
| **Practical No:** | **Title:** |
| **DOP:** | **DOS:** |
| **Grades:** | **LOs Mapped:** |
| **Signature:** | |

**Title:** Wireshark
**DOP: /3/24**
**DOS: /3/24**

**Aim:** To study wireshark packet sniffer to capture icmp, tcp, and http packets in promiscuous mode and explore how the packets can be traced based on different filters.

**Theory:**
What is Wireshark?
Wireshark is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting.

It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called a sniffer, network protocol analyzer, and network analyzer. It is also used by network security engineers to examine security problems.

**Uses of Wireshark:**
Wireshark can be used in the following ways:

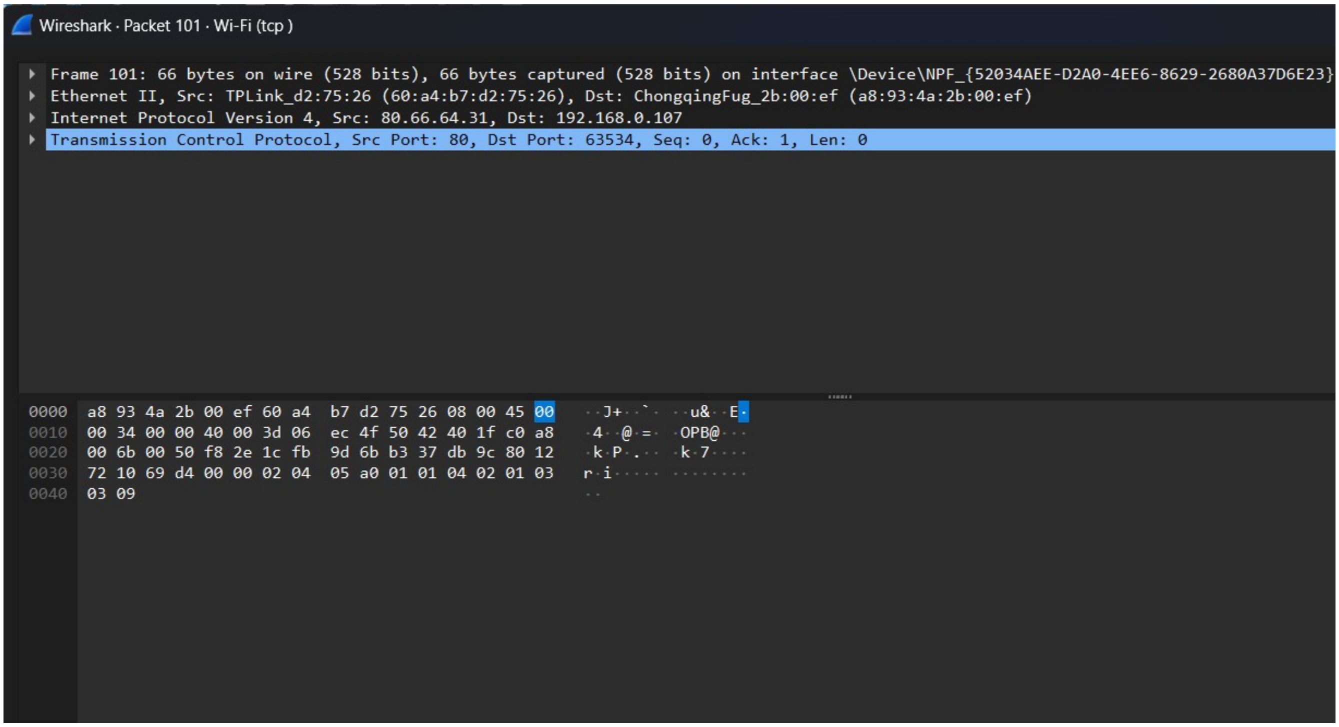
1. It is used by network security engineers to examine security problems.
2. It allows the users to watch all the traffic being passed over the network.
3. It is used by network engineers to troubleshoot network issues.
4. It also helps to troubleshoot latency issues and malicious activities on your network.
5. It can also analyze dropped packets.
6. It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.

**Output:**

1. icmp, tcp, and http packets captured screenshots with heading

A TCP PACKET :-

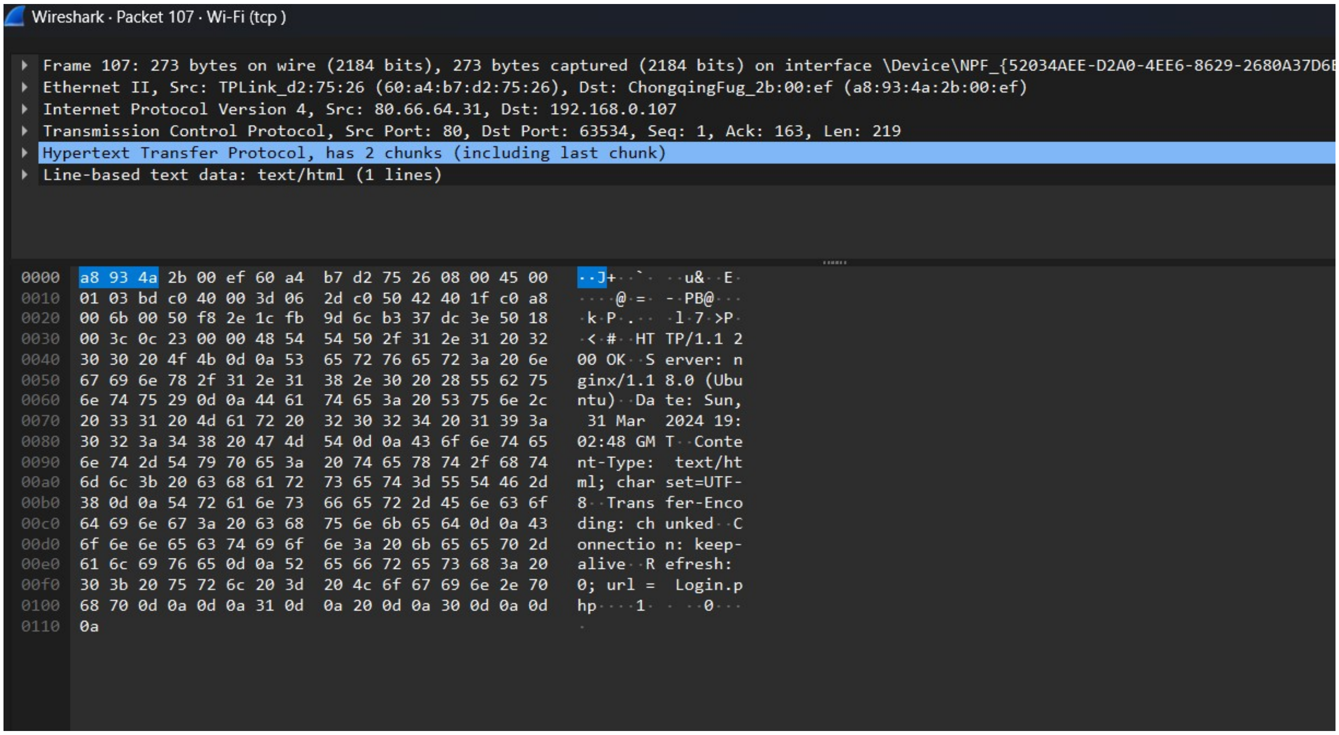
2.



Wireshark · Packet 101 · Wi-Fi (tcp )

```
▸ Frame 101: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{52034AEE-D2A0-4EE6-8629-2680A37D6E23}
▸ Ethernet II, Src: TPLink_d2:75:26 (60:a4:b7:d2:75:26), Dst: ChongqingFug_2b:00:ef (a8:93:4a:2b:00:ef)
▸ Internet Protocol Version 4, Src: 80.66.64.31, Dst: 192.168.0.107
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 63534, Seq: 0, Ack: 1, Len: 0
```

```
0000  a8 93 4a 2b 00 ef 60 a4  b7 d2 75 26 08 00 45 00   ··J+··`·  ··u&··E·
0010  00 34 00 00 40 00 3d 06  ec 4f 50 42 40 1f c0 a8   ·4··@·=·  ·OPB@···
0020  00 6b 00 50 f8 2e 1c fb  9d 6b b3 37 db 9c 80 12   ·k·P·.··  ·k·7····
0030  72 10 69 d4 00 00 02 04  05 a0 01 01 04 02 01 03   r·i·····  ········
0040  03 09                                              ··
```



Wireshark · Packet 107 · Wi-Fi (tcp )

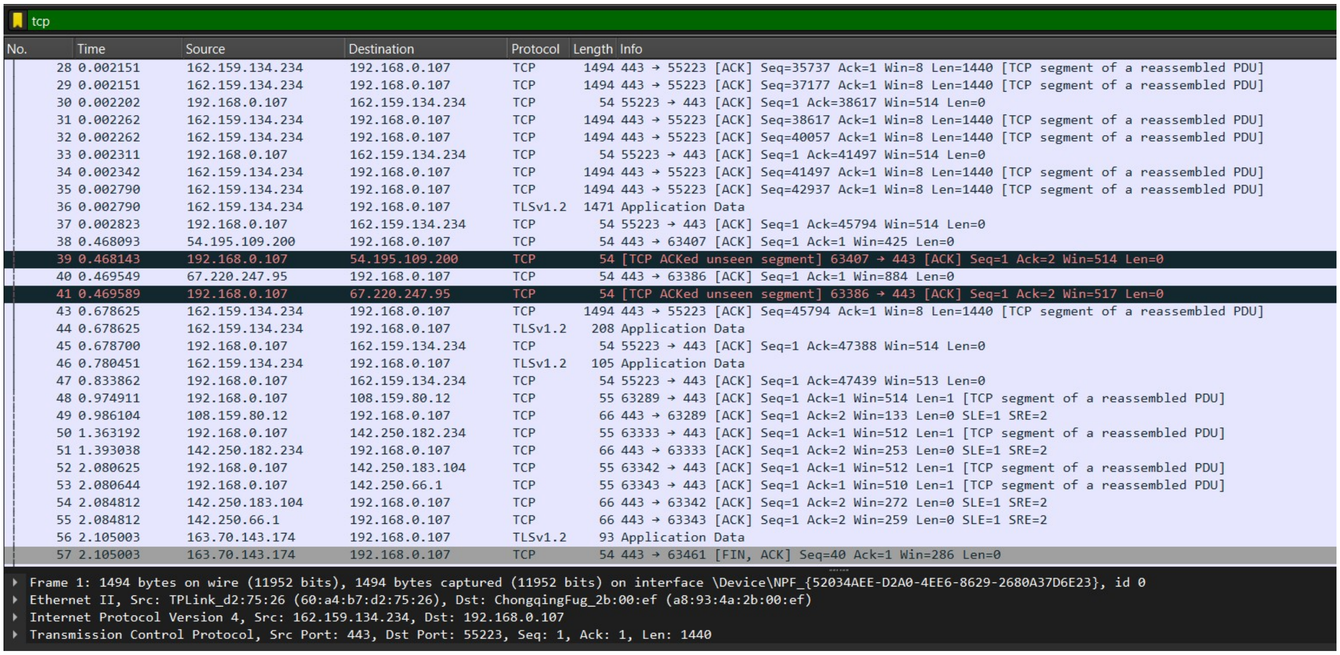
```
▸ Frame 107: 273 bytes on wire (2184 bits), 273 bytes captured (2184 bits) on interface \Device\NPF_{52034AEE-D2A0-4EE6-8629-2680A37D6E
▸ Ethernet II, Src: TPLink_d2:75:26 (60:a4:b7:d2:75:26), Dst: ChongqingFug_2b:00:ef (a8:93:4a:2b:00:ef)
▸ Internet Protocol Version 4, Src: 80.66.64.31, Dst: 192.168.0.107
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 63534, Seq: 1, Ack: 163, Len: 219
▸ Hypertext Transfer Protocol, has 2 chunks (including last chunk)
▸ Line-based text data: text/html (1 lines)
```

```
0000  a8 93 4a 2b 00 ef 60 a4  b7 d2 75 26 08 00 45 00   ··J+··`· ··u&··E·
0010  01 03 bd c0 40 00 3d 06  2d c0 50 42 40 1f c0 a8   ····@·=· -·PB@···
0020  00 6b 00 50 f8 2e 1c fb  9d 6c b3 37 dc 3e 50 18   ·k·P·.·· ·l·7·>P·
0030  00 3c 0c 23 00 00 48 54  54 50 2f 31 2e 31 20 32   ·<·#··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 53  65 72 76 65 72 3a 20 6e   00 OK··S erver: n
0050  67 69 6e 78 2f 31 2e 31  38 2e 30 20 28 55 62 75   ginx/1.1 8.0 (Ubu
0060  6e 74 75 29 0d 0a 44 61  74 65 3a 20 53 75 6e 2c   ntu)··Da te: Sun,
0070  20 33 31 20 4d 61 72 20  32 30 32 34 20 31 39 3a    31 Mar  2024 19:
0080  30 32 3a 34 38 20 47 4d  54 0d 0a 43 6f 6e 74 65   02:48 GM T··Conte
0090  6e 74 2d 54 79 70 65 3a  20 74 65 78 74 2f 68 74   nt-Type:  text/ht
00a0  6d 6c 3b 20 63 68 61 72  73 65 74 3d 55 54 46 2d   ml; char set=UTF-
00b0  38 0d 0a 54 72 61 6e 73  66 65 72 2d 45 6e 63 6f   8··Trans fer-Enco
00c0  64 69 6e 67 3a 20 63 68  75 6e 6b 65 64 0d 0a 43   ding: ch unked··C
00d0  6f 6e 6e 65 63 74 69 6f  6e 3a 20 6b 65 65 70 2d   onnectio n: keep-
00e0  61 6c 69 76 65 0d 0a 52  65 66 72 65 73 68 3a 20   alive··R efresh: 
00f0  30 3b 20 75 72 6c 20 3d  20 4c 6f 67 69 6e 2e 70   0; url =  Login.p
0100  68 70 0d 0a 0d 0a 31 0d  0a 20 0d 0a 30 0d 0a 0d   hp····1· · ··0···
0110  0a                                                 ·
```

AN HTTP PCKET:

PACKETS WITH TCP FILTER:-

3. Packet tracing screenshots using different filters



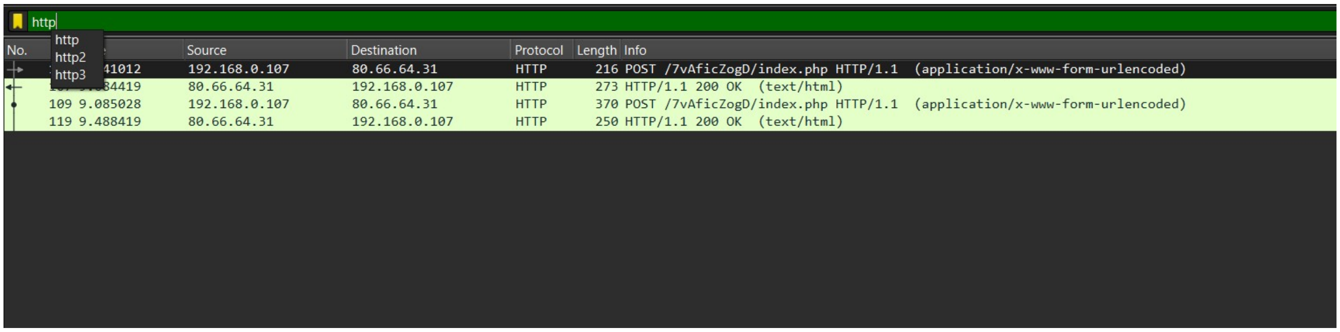
tcp

```
No.  Time        Source            Destination       Protocol Length Info
  28 0.002151    162.159.134.234   192.168.0.107     TCP      1494 443 → 55223 [ACK] Seq=35737 Ack=1 Win=8 Len=1440 [TCP segment of a reassembled PDU]
  29 0.002151    162.159.134.234   192.168.0.107     TCP      1494 443 → 55223 [ACK] Seq=37177 Ack=1 Win=8 Len=1440 [TCP segment of a reassembled PDU]
  30 0.002202    192.168.0.107     162.159.134.234   TCP        54 55223 → 443 [ACK] Seq=1 Ack=38617 Win=514 Len=0
  31 0.002262    162.159.134.234   192.168.0.107     TCP      1494 443 → 55223 [ACK] Seq=38617 Ack=1 Win=8 Len=1440 [TCP segment of a reassembled PDU]
  32 0.002262    162.159.134.234   192.168.0.107     TCP      1494 443 → 55223 [ACK] Seq=40057 Ack=1 Win=8 Len=1440 [TCP segment of a reassembled PDU]
  33 0.002311    192.168.0.107     162.159.134.234   TCP        54 55223 → 443 [ACK] Seq=1 Ack=41497 Win=514 Len=0
  34 0.002342    162.159.134.234   192.168.0.107     TCP      1494 443 → 55223 [ACK] Seq=41497 Ack=1 Win=8 Len=1440 [TCP segment of a reassembled PDU]
  35 0.002790    162.159.134.234   192.168.0.107     TCP      1494 443 → 55223 [ACK] Seq=42937 Ack=1 Win=8 Len=1440 [TCP segment of a reassembled PDU]
  36 0.002790    162.159.134.234   192.168.0.107     TLSv1.2  1471 Application Data
  37 0.002823    192.168.0.107     162.159.134.234   TCP        54 55223 → 443 [ACK] Seq=1 Ack=45794 Win=514 Len=0
  38 0.468093    54.195.109.200    192.168.0.107     TCP        54 443 → 63407 [ACK] Seq=1 Ack=1 Win=425 Len=0
  39 0.468143    192.168.0.107     54.195.109.200    TCP        54 [TCP ACKed unseen segment] 63407 → 443 [ACK] Seq=1 Ack=2 Win=514 Len=0
  40 0.469549    67.220.247.95     192.168.0.107     TCP        54 443 → 63386 [ACK] Seq=1 Ack=1 Win=884 Len=0
  41 0.469589    192.168.0.107     67.220.247.95     TCP        54 [TCP ACKed unseen segment] 63386 → 443 [ACK] Seq=1 Ack=2 Win=517 Len=0
  43 0.678625    162.159.134.234   192.168.0.107     TCP      1494 443 → 55223 [ACK] Seq=45794 Ack=1 Win=8 Len=1440 [TCP segment of a reassembled PDU]
  44 0.678625    162.159.134.234   192.168.0.107     TLSv1.2   208 Application Data
  45 0.678700    192.168.0.107     162.159.134.234   TCP        54 55223 → 443 [ACK] Seq=1 Ack=47388 Win=514 Len=0
  46 0.780451    162.159.134.234   192.168.0.107     TLSv1.2   105 Application Data
  47 0.833862    192.168.0.107     162.159.134.234   TCP        54 55223 → 443 [ACK] Seq=1 Ack=47439 Win=513 Len=0
  48 0.974911    192.168.0.107     108.159.80.12     TCP        55 63289 → 443 [ACK] Seq=1 Ack=1 Win=514 Len=1 [TCP segment of a reassembled PDU]
  49 0.986104    108.159.80.12     192.168.0.107     TCP        66 443 → 63289 [ACK] Seq=1 Ack=2 Win=133 Len=0 SLE=1 SRE=2
  50 1.363192    192.168.0.107     142.250.182.234   TCP        55 63333 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP segment of a reassembled PDU]
  51 1.393038    142.250.182.234   192.168.0.107     TCP        66 443 → 63333 [ACK] Seq=1 Ack=2 Win=253 Len=0 SLE=1 SRE=2
  52 2.080625    192.168.0.107     142.250.183.104   TCP        55 63342 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP segment of a reassembled PDU]
  53 2.080644    192.168.0.107     142.250.66.1      TCP        55 63343 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]
  54 2.084812    142.250.183.104   192.168.0.107     TCP        66 443 → 63342 [ACK] Seq=1 Ack=2 Win=272 Len=0 SLE=1 SRE=2
  55 2.084812    142.250.66.1      192.168.0.107     TCP        66 443 → 63343 [ACK] Seq=1 Ack=2 Win=259 Len=0 SLE=1 SRE=2
  56 2.105003    163.70.143.174    192.168.0.107     TLSv1.2    93 Application Data
  57 2.105003    163.70.143.174    192.168.0.107     TCP        54 443 → 63461 [FIN, ACK] Seq=40 Ack=1 Win=286 Len=0
```

```
▸ Frame 1: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface \Device\NPF_{52034AEE-D2A0-4EE6-8629-2680A37D6E23}, id 0
▸ Ethernet II, Src: TPLink_d2:75:26 (60:a4:b7:d2:75:26), Dst: ChongqingFug_2b:00:ef (a8:93:4a:2b:00:ef)
▸ Internet Protocol Version 4, Src: 162.159.134.234, Dst: 192.168.0.107
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 55223, Seq: 1, Ack: 1, Len: 1440
```

4.

5.



```
http
No.   e          Source          Destination     Protocol  Length  Info
      41012      192.168.0.107   80.66.64.31     HTTP        216   POST /7vAficZogD/index.php HTTP/1.1  (application/x-www-form-urlencoded)
      84419      80.66.64.31     192.168.0.107   HTTP        273   HTTP/1.1 200 OK  (text/html)
109 9.085028     192.168.0.107   80.66.64.31     HTTP        370   POST /7vAficZogD/index.php HTTP/1.1  (application/x-www-form-urlencoded)
119 9.488419     80.66.64.31     192.168.0.107   HTTP        250   HTTP/1.1 200 OK  (text/html)
```

## PACKETS WITHN HTTP FILTER;

**Conclusion: WE have successfully sniffed packets using wireshark applied different filters and explored packet structure.**