08/08/24

EXPERIMENT NO: 05 PACKET CAPTURE TOOL

Aim:

Experiments on Packet capture Tool: Wireshark

Packet Sniffer:

1. Sniffs messages being sent/received from/to by your computer.

2. Store and display the contents of the various protocols fields in the messages.

3. Passive program:
   - Never sends packet itself
   - No packets addressed to it
   - Receives a copy of all packets (sent/received)

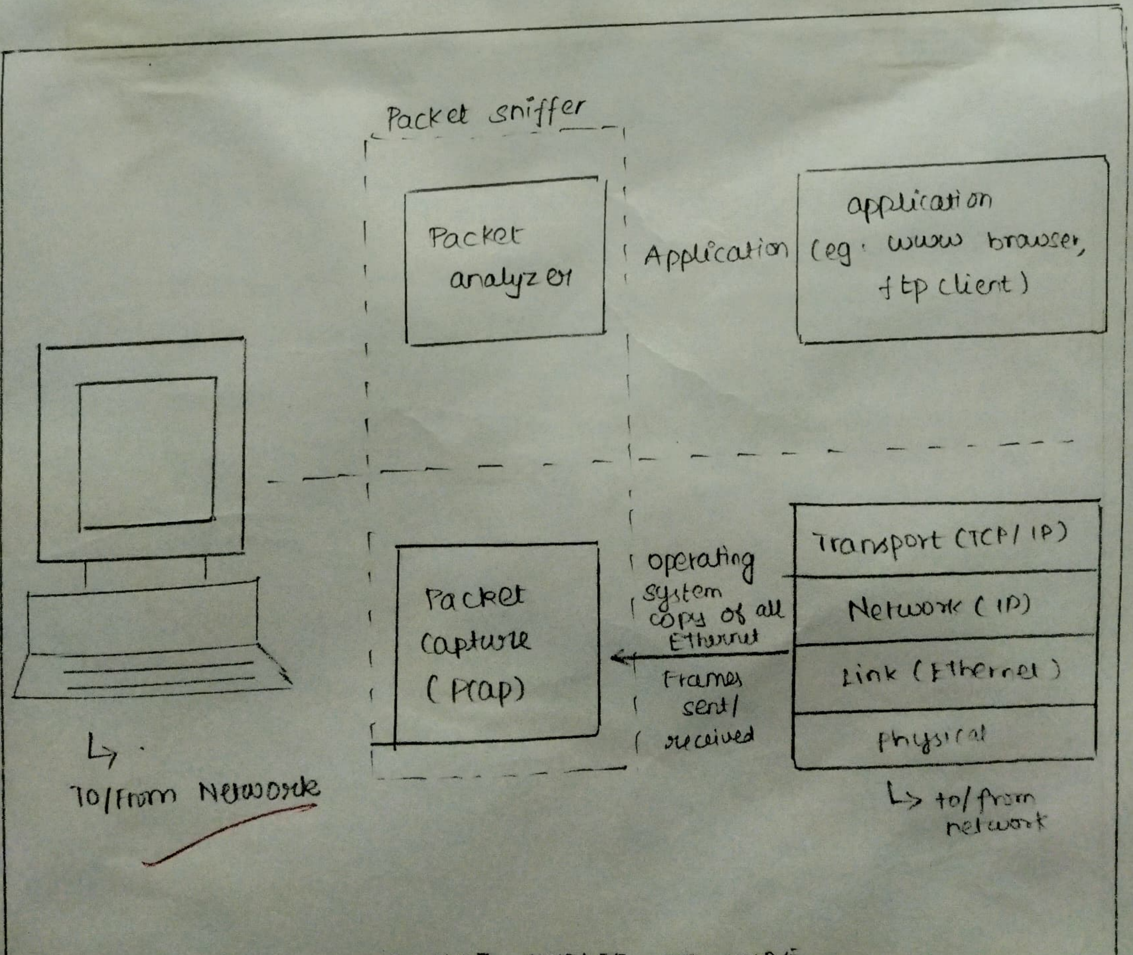
Packet Sniffer structure Diagnostic tools:

1. TCP dump

   Eg: `tcpdump -enx host 10.129 41.2 -w exe.3 out`

2. Wireshark

   - `wireshark -r exe3.out`

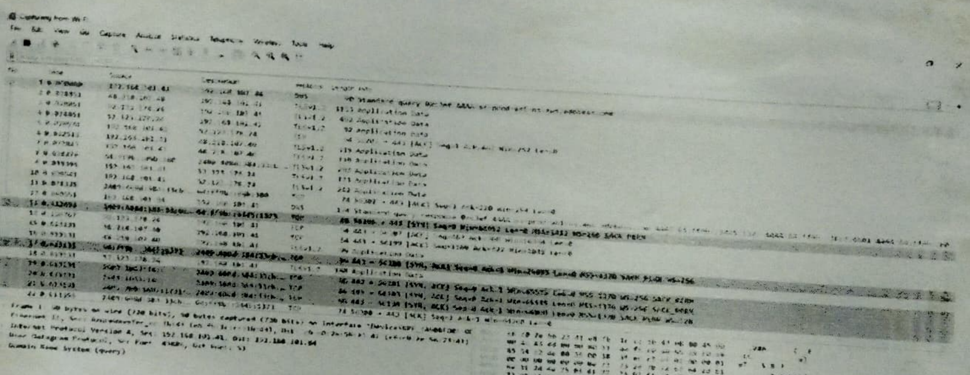


PACKET SNIFFER STRUCTURE

Capturing packets:

After downloading and installing Wireshark, launch it and double-click the name of a network interfac under capture to start capturing packets on that interfac. As soon as you click the interface's name, you'll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system

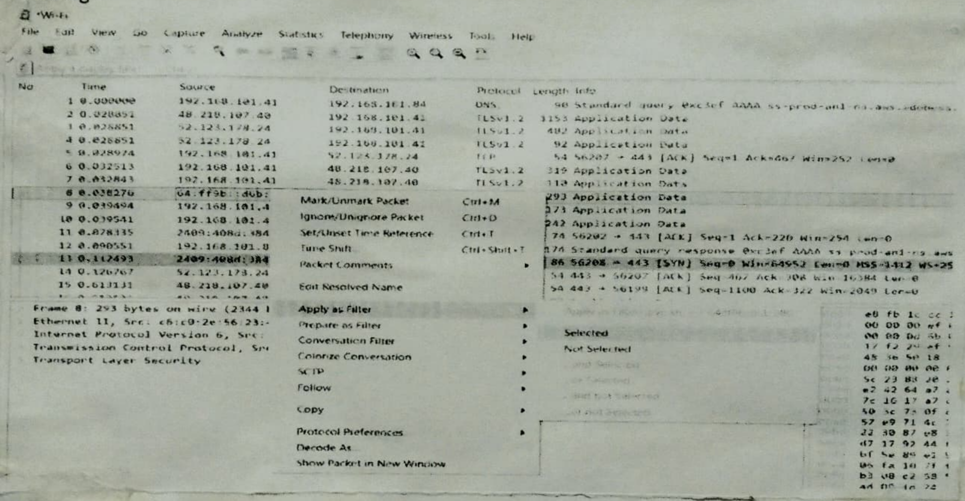
Capturing:


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

Filtering Packets :

If you're trying to inspect something specific, such as the traffic a program sends when phoning come, it helps to close down all others applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to shift through. That's were Wireshark filters in

Filtering:



```
No   Time        Source            Destination       Protocol  Length Info
   1 0.000000    192.168.101.41    192.168.101.84    DNS           90 Standard query 0xc3ef AAAA ss-prod-an1-ns.aws.adobess.
   2 0.028851    48.218.107.40     192.168.101.41    TLSv1.2     3153 Application Data
   3 0.028851    52.123.178.24     192.168.101.41    TLSv1.2      482 Application Data
   4 0.028851    52.123.178.24     192.168.101.41    TLSv1.2       92 Application Data
   5 0.028974    192.168.101.41    52.123.178.24     TCP           54 56207 → 443 [ACK] Seq=1 Ack=467 Win=252 Len=0
   6 0.032513    192.168.101.41    48.218.107.40     TLSv1.2      319 Application Data
   7 0.032843    192.168.101.41    48.218.107.40     TLSv1.2      113 Application Data
   8 0.038276    64:ff9b::d6b:                                    293 Application Data
   9 0.039494    192.168.101.4                                    173 Application Data
  10 0.039541    192.168.101.4                                    242 Application Data
  11 0.078335    2409:408d:384                                     74 56202 → 443 [ACK] Seq=1 Ack=220 Win=254 Len=0
  12 0.090551    192.168.101.8                                    174 Standard query response 0xc3ef AAAA ss-prod-an1-ns.aws
  13 0.112493    2409:408d:384                                     86 56208 → 443 [SYN] Seq=0 Win=64952 Len=0 MSS=1412 WS=25
  14 0.126767    52.123.178.24                                     54 443 → 56207 [ACK] Seq=467 Ack=308 Win=16384 Len=0
  15 0.613131    48.218.107.40                                     54 443 → 56199 [ACK] Seq=1100 Ack=322 Win=2049 Len=0
```

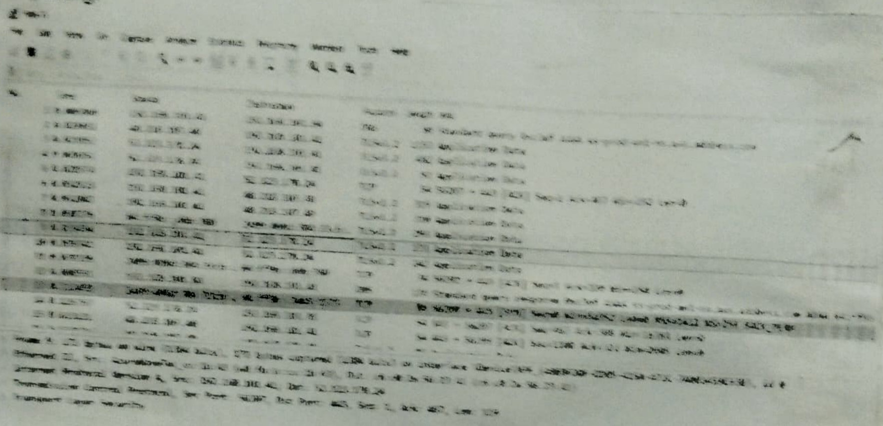
```
Frame 8: 293 bytes on wire (2344 I
Ethernet II, Src: c6:c0:2e:56:23:-
Internet Protocol Version 6, Src:
Transmission Control Protocol, Sr
Transport Layer Security
```

```
e0 fb 1c cc
00 00 00 ef
00 00 0d 5b
17 f2 2d af
45 3e 5e 18
00 00 00 0e
5c 23 88 2e
e2 42 64 a7
7c 16 17 a7
50 5c 75 0f
57 e9 71 4c
22 30 87 e8
d7 17 92 44
bf 5e 89 e3
06 fa 10 71
b3 08 c2 58
ad 05 1e 24
```

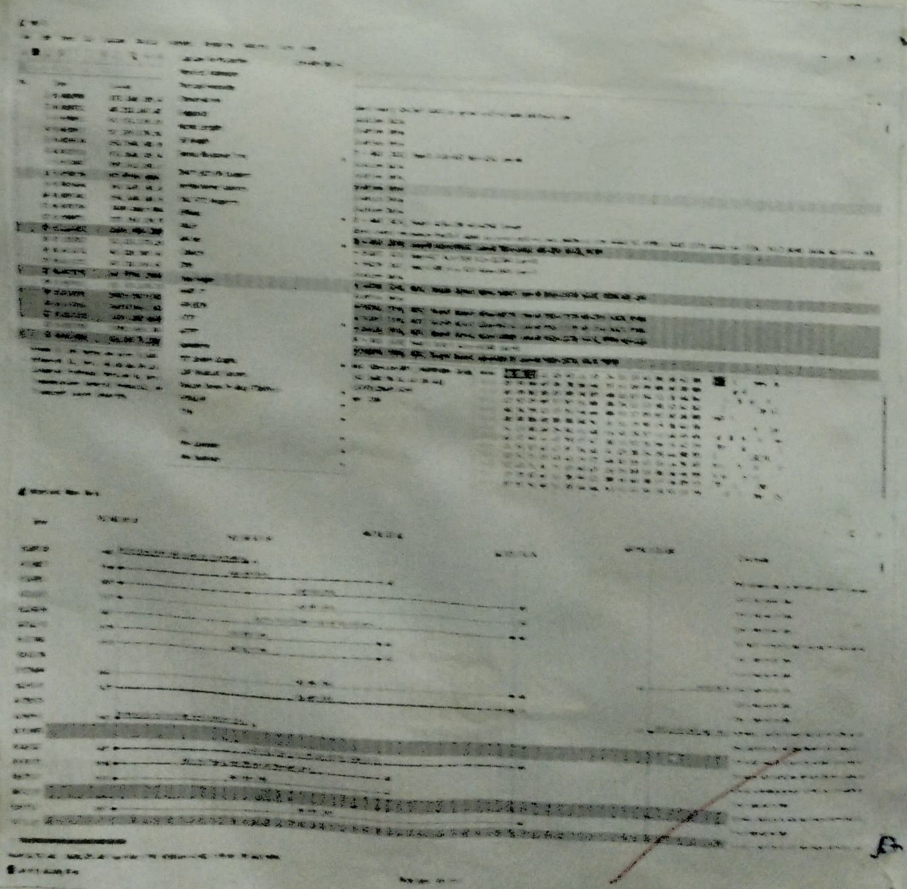
Inspecting - packets :

Click a packet to select it and you can dig down to view its details

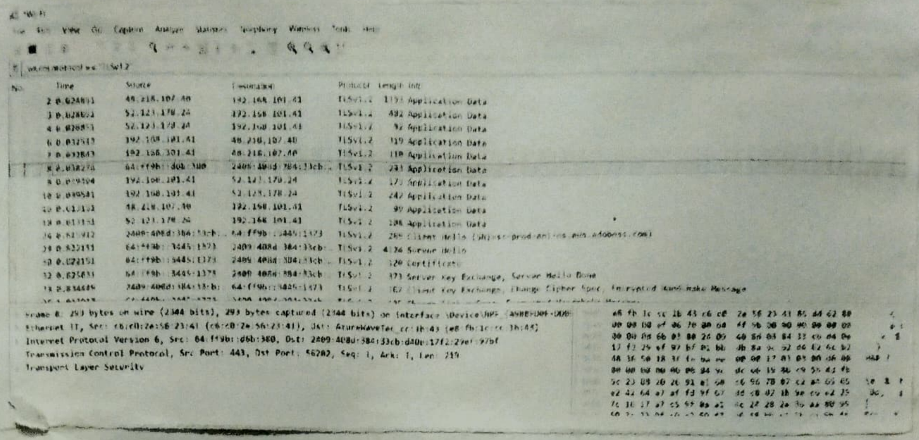
Inspecting:



Flow graph:



Flow Graph:


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

```
_ws.col.protocol == "TLSv1.2"

No.  Time      Source               Destination          Protocol Length Info
   2 0.024031  48.218.107.40        192.168.101.41       TLSv1.2  1153 Application Data
   3 0.028053  52.123.178.24        192.168.101.41       TLSv1.2   482 Application Data
   4 0.028853  52.123.178.24        192.168.101.41       TLSv1.2    92 Application Data
   6 0.032513  192.168.101.41       48.218.107.40        TLSv1.2   119 Application Data
   7 0.032843  192.168.101.41       48.218.107.40        TLSv1.2   110 Application Data
   8 0.038278  64:ff9b::d6b:380     2409:408d:384:33cb.. TLSv1.2   293 Application Data
   9 0.039394  192.168.101.41       52.123.178.24        TLSv1.2   173 Application Data
  10 0.039541  192.168.101.41       52.123.178.24        TLSv1.2   242 Application Data
  12 0.013133  48.218.107.40        192.168.101.41       TLSv1.2    99 Application Data
  13 0.013153  52.123.178.24        192.168.101.41       TLSv1.2   106 Application Data
  26 0.61912   2409:408d:384:33cb.. 64:ff9b::3445:1373   TLSv1.2   265 Client Hello (SNI=ss-prod-an1-ns.ams.adobess.com)
  28 0.622131  64:ff9b::3445:1373   2409:408d:384:33cb.. TLSv1.2  4126 Server Hello
  30 0.622151  64:ff9b::3445:1373   2409:408d:384:33cb.. TLSv1.2   520 Certificate
  32 0.625631  64:ff9b::3445:1373   2409:408d:384:33cb   TLSv1.2   373 Server Key Exchange, Server Hello Done
  34 0.634449  2409:408d:384:33cb:  64:ff9b::3445:1373   TLSv1.2   162 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message

Frame 8: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{A98EFD0F-DD0
Ethernet II, Src: c6:c0:2e:56:23:41 (c6:c0:2e:56:23:41), Dst: AzureWaveTec_cc:1b:43 (e8:fb:1c:cc:1b:43)
Internet Protocol Version 6, Src: 64:ff9b::d6b:380, Dst: 2409:408d:384:33cb:d40e:17f2:27ef:97bf
Transmission Control Protocol, Src Port: 443, Dst Port: 56202, Seq: 1, Ack: 1, Len: 219
Transport Layer Security
```

Student Observation:

1) What is promiscuous mode?

It is a mode of operation where a network device can intercept and read in its entirely each packet that process through.

2) Does ARP Packets has transport layer header? Explain:

ARP Packets do not have a transport layer header ARP operates at the link layer (2) of the OSI Model, which is responsible for local network communication between devices on the same network segment.

3) Which transport layer protocol is used by DNS?

DNS uses two transport layer protocol

1) UDP (User Datagram Protocol)

2) TCP (Transmission Control Protocol)

4) What is the port number used by http protocol?

80 is the port number used by http.

5) What is a broadcast ip address?

A broadcast ip address is a network address used to transmit to all devices connected to a multiple access communication network.

8/8/24

Result:

Thus, the features of wireshark as a capture tool is observed and studied about the encapsulation of information at various layers of protocol layer stack.