Ex-NO 5

PRATICAL - 5

AIM

Experiment on packet capture tool wireshark

Packet sniffer

-> Sniffs message being sent received from by your computer

-> store and display the content of the various protocol - files in the message

-> passive program

-> never sent packet itself

-> no packets addressed to it

-> recive a copy of packet (sent / recived)

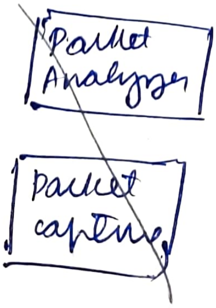
Packet sniffer structure Diagnostic Tools

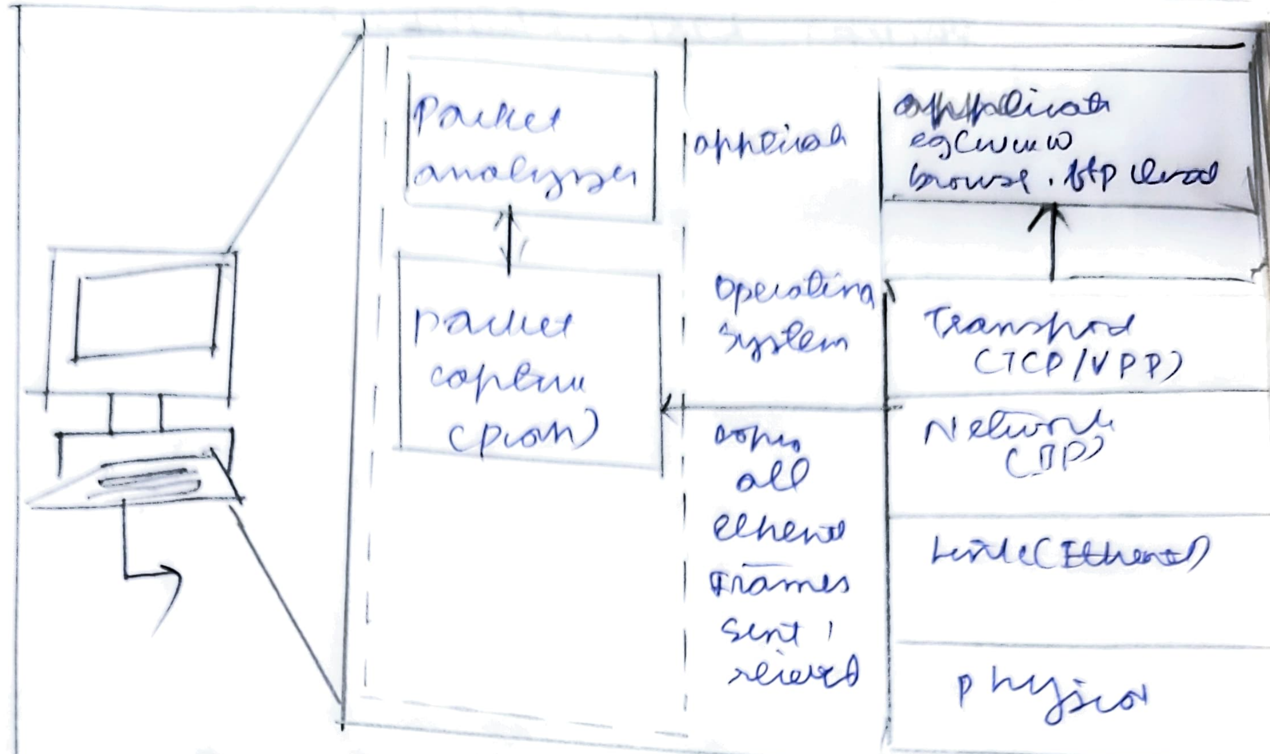
Tcp dump

- Eg - tcpdump - enn host 10.129.41.20 en.3-out

wire shark

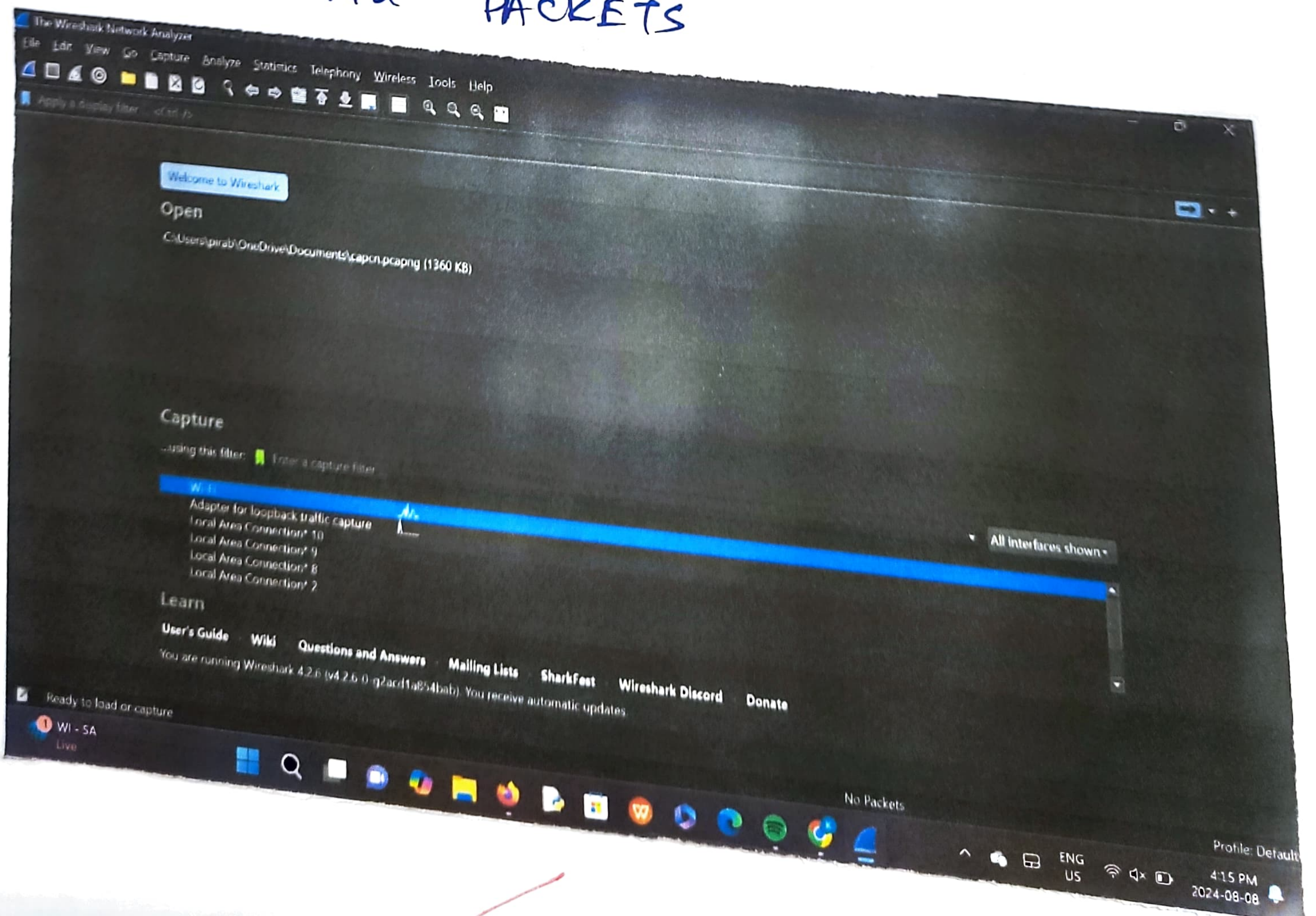
- wire shark - r ene 3.out





Packet sniffer structure

CAPTURING PACKETS


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter <Ctrl-/>
Welcome to Wireshark
All interfaces shown
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
WI - SA
Live
No Packets
Profile: Default
ENG
US
4:15 PM
2024-08-08

Open

C:\Users\pirab\OneDrive\Documents\capcn.pcapng (1360 KB)

Capture

...using this filter: Enter a capture filter ...

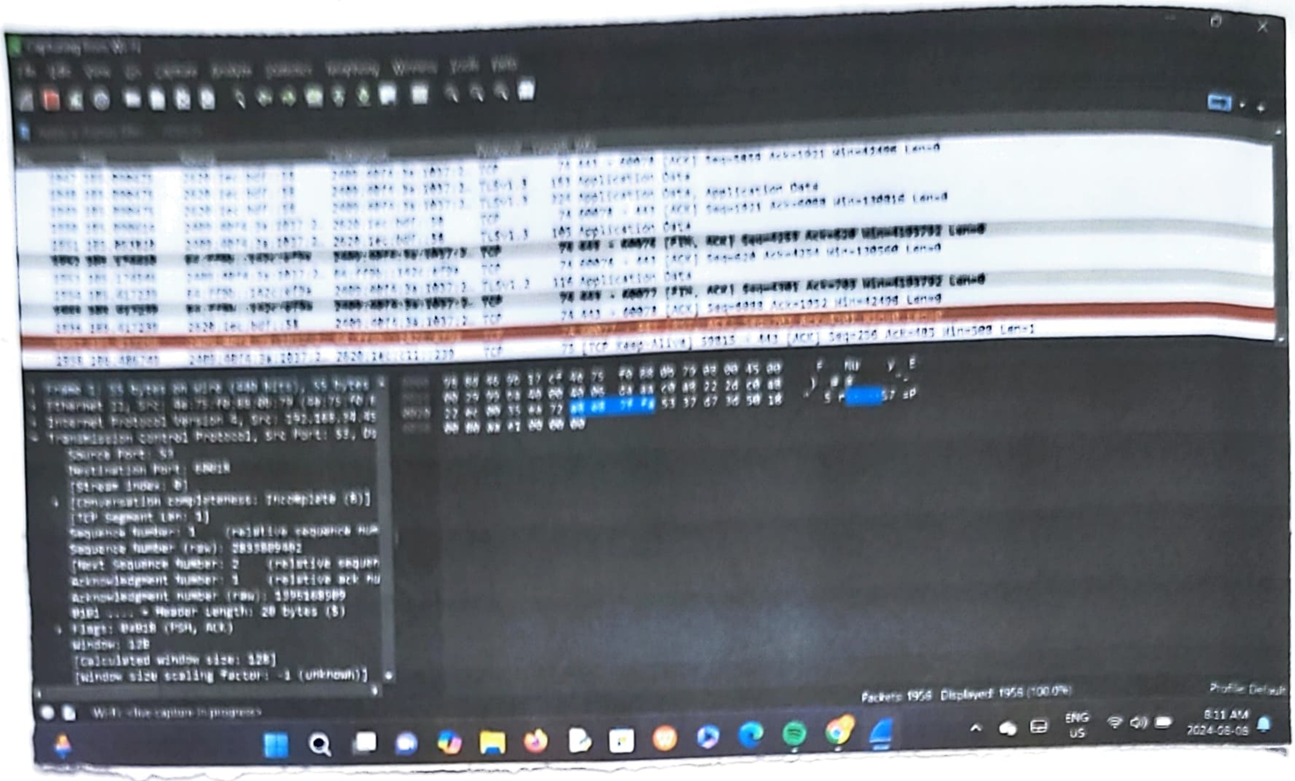
Wi-Fi
Adapter for loopback traffic capture
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 2

Learn

You are running Wireshark 4.2.6 (v4.2.6-0-g2acd1a854bab). You receive automatic updates.

Ready to load or capture

PACKET LISTS, DETAILS AND BYTES

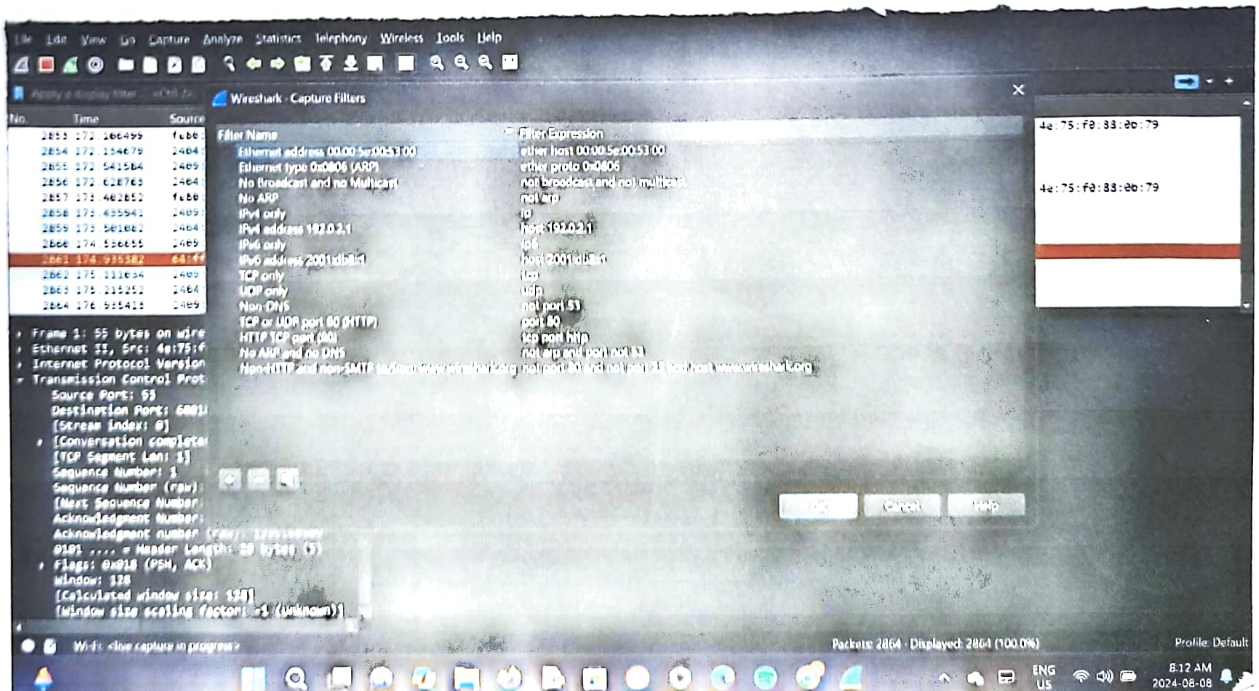


```
> Frame 1: 55 bytes on wire (440 bits), 55 bytes
> Ethernet II, Src: 4e:75:f0:88:0b:79 (4e:75:f0:8
> Internet Protocol Version 4, Src: 192.168.34.85
v Transmission Control Protocol, Src Port: 53, Ds
    Source Port: 53
    Destination Port: 68018
    [Stream index: 0]
  > [Conversation completeness: Incomplete (8)]
    [TCP Segment Len: 1]
    Sequence Number: 1    (relative sequence num
    Sequence Number (raw): 2833809402
    [Next Sequence Number: 2    (relative sequen
    Acknowledgment Number: 1    (relative ack nu
    Acknowledgment number (raw): 1395168909
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 128
    [Calculated window size: 128]
    [Window size scaling factor: -1 (unknown)]
```

Packets: 1956 · Displayed: 1956 (100.0%)   Profile: Default

Wi-Fi: <live capture in progress>

CAPTURING FILTERS



Wireshark · Capture Filters

Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	ether host 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	ether proto 0x0806
No Broadcast and no Multicast	not broadcast and not multicast
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	host 192.0.2.1
IPv6 only	ip6
IPv6 address 2001:db8::1	host 2001:db8::1
TCP only	tcp
UDP only	udp
Non-DNS	not port 53
TCP or UDP port 80 (HTTP)	port 80
HTTP TCP port (80)	tcp port http
No ARP and no DNS	not arp and port not 53
Non-HTTP and non-SMTP to/from www.wireshark.org	not port 80 and not port 25 and host www.wireshark.org

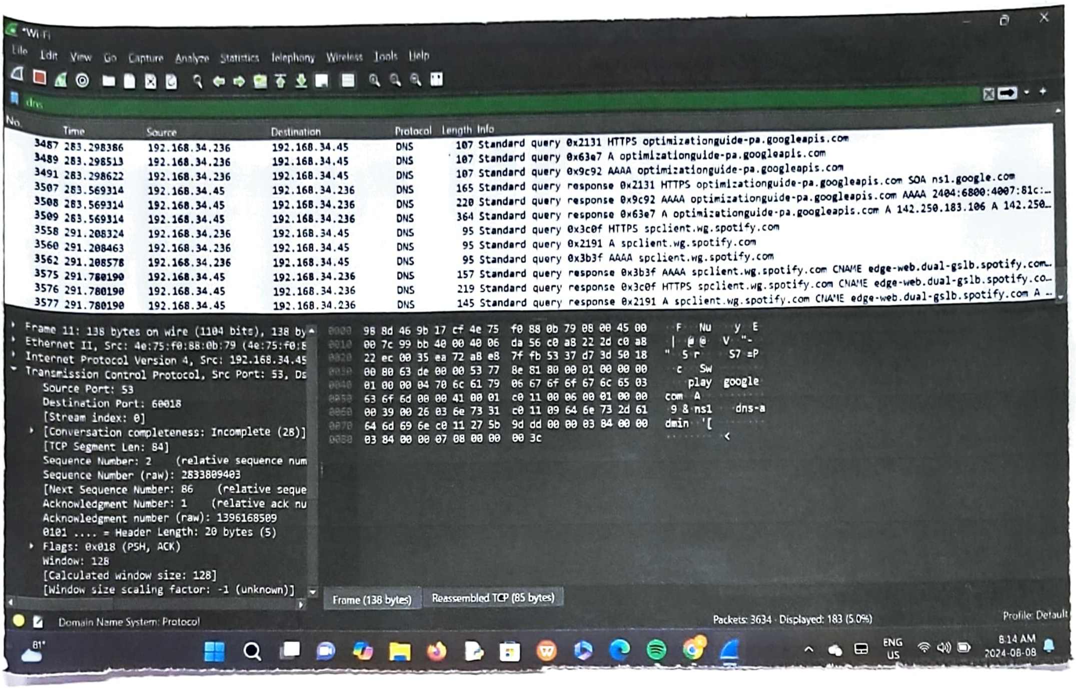
```
> Frame 1: 55 bytes on wire
> Ethernet II, Src: 4e:75:f
> Internet Protocol Version
v Transmission Control Prot
    Source Port: 53
    Destination Port: 6801
    [Stream index: 0]
  > [Conversation complete
    [TCP Segment Len: 1]
    Sequence Number: 1
    Sequence Number (raw):
    [Next Sequence Number:
    Acknowledgment Number:
    Acknowledgment number (raw): 1395168909
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 128
    [Calculated window size: 128]
    [Window size scaling factor: -1 (unknown)]
```

4e:75:f0:88:0b:79

4e:75:f0:88:0b:79

Packets: 2864 · Displayed: 2864 (100.0%)   Profile: Default

Wi-Fi: <live capture in progress>


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

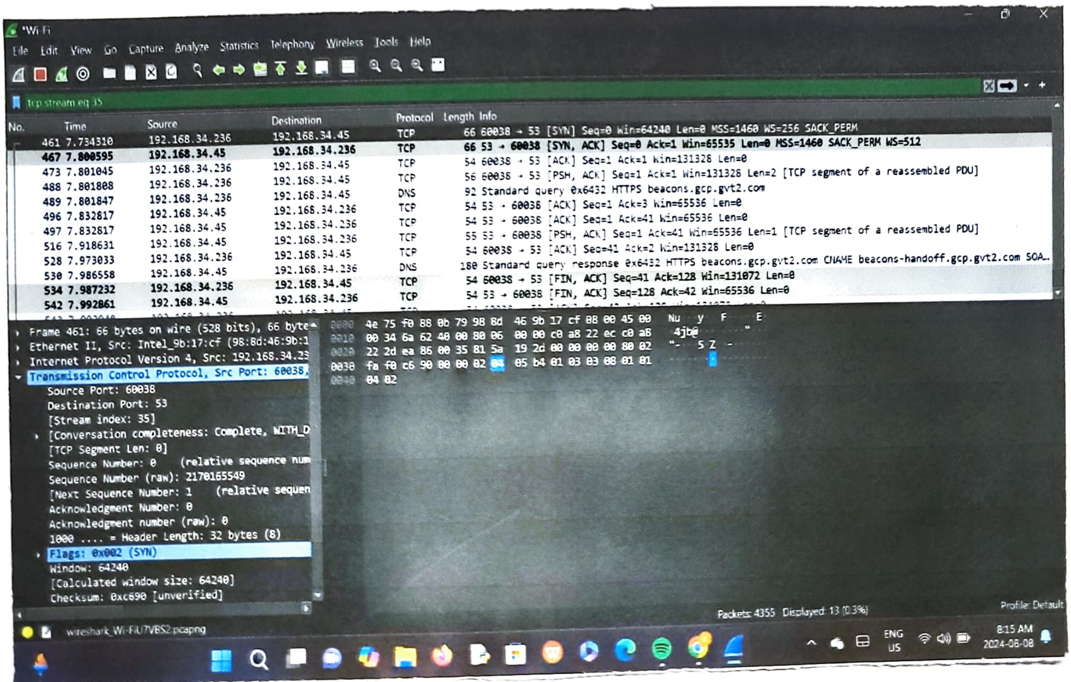
```
No.   Time        Source          Destination     Protocol Length Info
 3487 283.298386  192.168.34.236  192.168.34.45   DNS      107 Standard query 0x2131 HTTPS optimizationguide-pa.googleapis.com
 3489 283.298513  192.168.34.236  192.168.34.45   DNS      107 Standard query 0x63e7 A optimizationguide-pa.googleapis.com
 3491 283.298622  192.168.34.236  192.168.34.45   DNS      107 Standard query 0x9c92 AAAA optimizationguide-pa.googleapis.com
 3507 283.569314  192.168.34.45   192.168.34.236  DNS      165 Standard query response 0x2131 HTTPS optimizationguide-pa.googleapis.com SOA ns1.google.com
 3508 283.569314  192.168.34.45   192.168.34.236  DNS      220 Standard query response 0x9c92 AAAA optimizationguide-pa.googleapis.com AAAA 2404:6800:4007:81c:…
 3509 283.569314  192.168.34.45   192.168.34.236  DNS      364 Standard query response 0x63e7 A optimizationguide-pa.googleapis.com A 142.250.183.106 A 142.250…
 3558 291.208324  192.168.34.236  192.168.34.45   DNS       95 Standard query 0x3c0f HTTPS spclient.wg.spotify.com
 3560 291.208463  192.168.34.236  192.168.34.45   DNS       95 Standard query 0x2191 A spclient.wg.spotify.com
 3562 291.208578  192.168.34.236  192.168.34.45   DNS       95 Standard query 0x3b3f AAAA spclient.wg.spotify.com
 3575 291.780190  192.168.34.45   192.168.34.236  DNS      157 Standard query response 0x3b3f AAAA spclient.wg.spotify.com CNAME edge-web.dual-gslb.spotify.com…
 3576 291.780190  192.168.34.45   192.168.34.236  DNS      219 Standard query response 0x3c0f HTTPS spclient.wg.spotify.com CNAME edge-web.dual-gslb.spotify.co…
 3577 291.780190  192.168.34.45   192.168.34.236  DNS      145 Standard query response 0x2191 A spclient.wg.spotify.com CNAME edge-web.dual-gslb.spotify.com A …
```

```
> Frame 11: 138 bytes on wire (1104 bits), 138 by
> Ethernet II, Src: 4e:75:f0:88:0b:79 (4e:75:f0:8
> Internet Protocol Version 4, Src: 192.168.34.45
v Transmission Control Protocol, Src Port: 53, Ds
    Source Port: 53
    Destination Port: 60018
    [Stream index: 0]
  > [Conversation completeness: Incomplete (28)]
    [TCP Segment Len: 84]
    Sequence Number: 2    (relative sequence num
    Sequence Number (raw): 2833809403
    [Next Sequence Number: 86    (relative seque
    Acknowledgment Number: 1    (relative ack nu
    Acknowledgment number (raw): 1396168509
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 128
    [Calculated window size: 128]
    [Window size scaling factor: -1 (unknown)]
```

```
0000  98 8d 46 9b 17 cf 4e 75  f0 88 0b 79 08 00 45 00   F  Nu   y E
0010  00 7c 99 bb 40 00 40 06  da 56 c0 a8 22 2d c0 a8   | @ @  V  "-
0020  22 ec 00 35 ea 72 a8 e8  7f fb 53 37 d7 3d 50 18  "  5 r    S7 =P
0030  00 80 63 de 00 00 53 77  8e 81 80 00 01 00 00 00    c   Sw
0040  01 00 00 04 70 6c 61 79  06 67 6f 6f 67 6c 65 03      play  google
0050  63 6f 6d 00 00 41 00 01  c0 11 00 06 00 01 00 00  com  A
0060  00 39 00 26 03 6e 73 31  c0 11 09 64 6e 73 2d 61   9 & ns1   dns-a
0070  64 6d 69 6e c0 11 27 5b  9d dd 00 00 03 84 00 00  dmin  '[
0080  03 84 00 00 07 08 00 00  00 3c                          <
```

Packets: 3634 · Displayed: 183 (5.0%)

DISPLAYING FILTERS


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 35

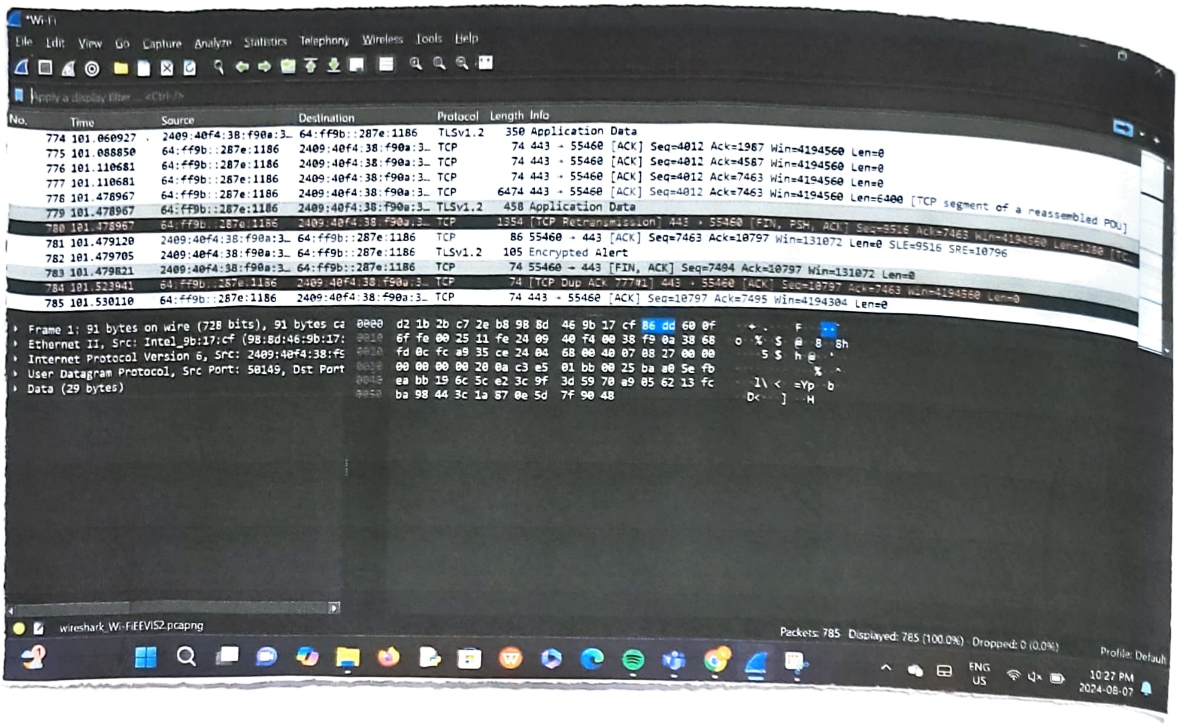
```
No.  Time      Source          Destination     Protocol Length Info
 461 7.734310  192.168.34.236  192.168.34.45   TCP       66 60038 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 467 7.800595  192.168.34.45   192.168.34.236  TCP       66 53 → 60038 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=512
 473 7.801045  192.168.34.236  192.168.34.45   TCP       54 60038 → 53 [ACK] Seq=1 Ack=1 Win=131328 Len=0
 488 7.801808  192.168.34.236  192.168.34.45   TCP       56 60038 → 53 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=2 [TCP segment of a reassembled PDU]
 489 7.801847  192.168.34.236  192.168.34.45   DNS       92 Standard query 0x6432 HTTPS beacons.gcp.gvt2.com
 496 7.832817  192.168.34.45   192.168.34.236  TCP       54 53 → 60038 [ACK] Seq=1 Ack=3 Win=65536 Len=0
 497 7.832817  192.168.34.45   192.168.34.236  TCP       54 53 → 60038 [ACK] Seq=1 Ack=41 Win=65536 Len=0
 516 7.918631  192.168.34.45   192.168.34.236  TCP       55 53 → 60038 [PSH, ACK] Seq=1 Ack=41 Win=65536 Len=1 [TCP segment of a reassembled PDU]
 528 7.973033  192.168.34.236  192.168.34.45   TCP       54 60038 → 53 [ACK] Seq=41 Ack=2 Win=131328 Len=0
 530 7.986558  192.168.34.45   192.168.34.236  DNS      180 Standard query response 0x6432 HTTPS beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com SOA…
 534 7.987232  192.168.34.236  192.168.34.45   TCP       54 60038 → 53 [FIN, ACK] Seq=41 Ack=128 Win=131072 Len=0
 542 7.992861  192.168.34.45   192.168.34.236  TCP       54 53 → 60038 [FIN, ACK] Seq=128 Ack=42 Win=65536 Len=0
```

```
> Frame 461: 66 bytes on wire (528 bits), 66 byte
> Ethernet II, Src: Intel_9b:17:cf (98:8d:46:9b:1
> Internet Protocol Version 4, Src: 192.168.34.23
v Transmission Control Protocol, Src Port: 60038,
    Source Port: 60038
    Destination Port: 53
    [Stream index: 35]
  > [Conversation completeness: Complete, WITH_D
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence num
    Sequence Number (raw): 2170165549
    [Next Sequence Number: 1    (relative sequen
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0xc690 [unverified]
```

```
0000  4e 75 f0 88 0b 79 98 8d  46 9b 17 cf 08 00 45 00  Nu  y  F    E
0010  00 34 6a 62 40 00 80 06  00 00 c0 a8 22 ec c0 a8   4jb@        "
0020  22 2d ea 86 00 35 81 5a  19 2d 00 00 00 00 80 02  "-   5 Z  -
0030  fa f0 c6 90 00 00 02 04  05 b4 01 03 03 08 01 01
0040  04 02
```

Packets: 4355 · Displayed: 13 (0.3%)

COLOURING RULES



*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
774 101.060927  2409:40f4:38:f90a:3…  64:ff9b::287e:1186    TLSv1.2   350 Application Data
775 101.088850  64:ff9b::287e:1186    2409:40f4:38:f90a:3…  TCP        74 443 → 55460 [ACK] Seq=4012 Ack=1987 Win=4194560 Len=0
776 101.110681  64:ff9b::287e:1186    2409:40f4:38:f90a:3…  TCP        74 443 → 55460 [ACK] Seq=4012 Ack=4587 Win=4194560 Len=0
777 101.110681  64:ff9b::287e:1186    2409:40f4:38:f90a:3…  TCP        74 443 → 55460 [ACK] Seq=4012 Ack=7463 Win=4194560 Len=0
778 101.478967  64:ff9b::287e:1186    2409:40f4:38:f90a:3…  TCP      6474 443 → 55460 [ACK] Seq=4012 Ack=7463 Win=4194560 Len=6400 [TCP segment of a reassembled PDU]
779 101.478967  64:ff9b::287e:1186    2409:40f4:38:f90a:3…  TLSv1.2   458 Application Data
780 101.478967  64:ff9b::287e:1186    2409:40f4:38:f90a:3…  TCP      1354 [TCP Retransmission] 443 → 55460 [FIN, PSH, ACK] Seq=9516 Ack=7463 Win=4194560 Len=1280 [TC…
781 101.479120  2409:40f4:38:f90a:3…  64:ff9b::287e:1186    TCP        86 55460 → 443 [ACK] Seq=7463 Ack=10797 Win=131072 Len=0 SLE=9516 SRE=10796
782 101.479705  2409:40f4:38:f90a:3…  64:ff9b::287e:1186    TLSv1.2   105 Encrypted Alert
783 101.479821  2409:40f4:38:f90a:3…  64:ff9b::287e:1186    TCP        74 55460 → 443 [FIN, ACK] Seq=7494 Ack=10797 Win=131072 Len=0
784 101.523941  64:ff9b::287e:1186    2409:40f4:38:f90a:3…  TCP        74 [TCP Dup ACK 777#1] 443 → 55460 [ACK] Seq=10797 Ack=7463 Win=4194560 Len=0
785 101.530110  64:ff9b::287e:1186    2409:40f4:38:f90a:3…  TCP        74 443 → 55460 [ACK] Seq=10797 Ack=7495 Win=4194304 Len=0
```

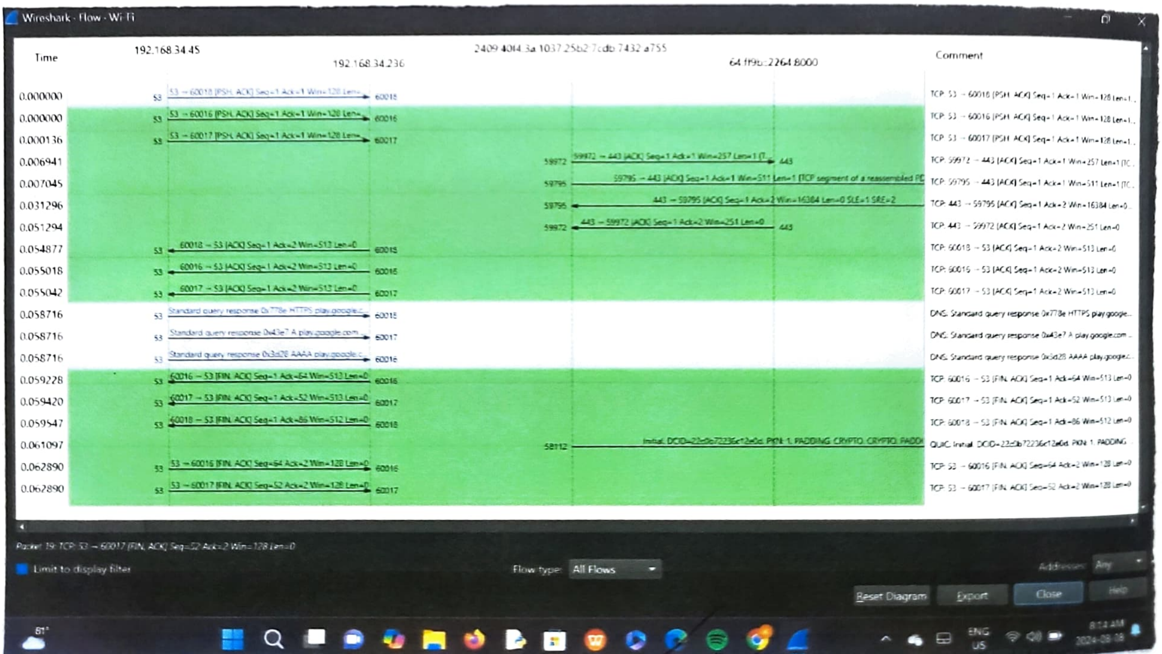
```
› Frame 1: 91 bytes on wire (728 bits), 91 bytes ca     0000  d2 1b 2b c7 2e b8 98 8d  46 9b 17 cf 86 dd 60 0f   ·+.···F···
› Ethernet II, Src: Intel_9b:17:cf (98:8d:46:9b:17:     0010  6f fe 00 25 11 fe 24 09  40 f4 00 38 f9 0a 38 68   o·%·$·@·8·8h
› Internet Protocol Version 6, Src: 2409:40f4:38:f9     0020  fd 0c fc a9 35 ce 24 04  68 00 40 07 08 27 00 00   ····5·$·h·@··
› User Datagram Protocol, Src Port: 50149, Dst Port     0030  00 00 00 00 20 0a c3 e5  01 bb 00 25 ba a0 5e fb   ···········%·^
› Data (29 bytes)                                        0040  ea bb 19 6c 5c e2 3c 9f  3d 59 70 a9 05 62 13 fc   ···l\·<·=Yp·b
                                                         0050  ba 98 44 3c 1a 87 0e 5d  7f 90 48                  ··D<···]··H
```

wireshark_Wi-FiEEVIS2.pcapng

Packets: 785 · Displayed: 785 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

WORK FLOW GRAPH



```
Time       192.168.34.45   192.168.34.236   2409:40f4:3a:1037:25b2:7cdb:7432:a755   64:ff9b::2264:8000   Comment

0.000000   53    53 → 60018 [PSH, ACK] Seq=1 Ack=1 Win=128 Len=…   60018        TCP: 53 → 60018 [PSH, ACK] Seq=1 Ack=1 Win=128 Len=1…
0.000000   53    53 → 60016 [PSH, ACK] Seq=1 Ack=1 Win=128 Len=…   60016        TCP: 53 → 60016 [PSH, ACK] Seq=1 Ack=1 Win=128 Len=1…
0.000136   53    53 → 60017 [PSH, ACK] Seq=1 Ack=1 Win=128 Len=…   60017        TCP: 53 → 60017 [PSH, ACK] Seq=1 Ack=1 Win=128 Len=1…
0.006941   59972   59972 → 443 [ACK] Seq=1 Ack=1 Win=257 Len=1 [T…   443      TCP: 59972 → 443 [ACK] Seq=1 Ack=1 Win=257 Len=1 [TC…
0.007045   59795   59795 → 443 [ACK] Seq=1 Ack=1 Win=511 Len=1 [TCP segment of a reassembled PD   TCP: 59795 → 443 [ACK] Seq=1 Ack=1 Win=511 Len=1 [TC…
0.031296   59795   443 → 59795 [ACK] Seq=1 Ack=2 Win=16384 Len=0 SLE=1 SRE=2   TCP: 443 → 59795 [ACK] Seq=1 Ack=2 Win=16384 Len=0…
0.051294   59972   443 → 59972 [ACK] Seq=1 Ack=2 Win=251 Len=0   443       TCP: 443 → 59972 [ACK] Seq=1 Ack=2 Win=251 Len=0
0.054877   53    60018 → 53 [ACK] Seq=1 Ack=2 Win=513 Len=0   60018             TCP: 60018 → 53 [ACK] Seq=1 Ack=2 Win=513 Len=0
0.055018   53    60016 → 53 [ACK] Seq=1 Ack=2 Win=513 Len=0   60016             TCP: 60016 → 53 [ACK] Seq=1 Ack=2 Win=513 Len=0
0.055042   53    60017 → 53 [ACK] Seq=1 Ack=2 Win=513 Len=0   60017             TCP: 60017 → 53 [ACK] Seq=1 Ack=2 Win=513 Len=0
0.058716   53    Standard query response 0x778e HTTPS play.google.c…   60018    DNS: Standard query response 0x778e HTTPS play.google…
0.058716   53    Standard query response 0x43e7 A play.google.com …   60017     DNS: Standard query response 0x43e7 A play.google.com …
0.058716   53    Standard query response 0x3d28 AAAA play.google.c…   60016    DNS: Standard query response 0x3d28 AAAA play.google.c…
0.059228   53    60016 → 53 [FIN, ACK] Seq=1 Ack=64 Win=513 Len=0   60016       TCP: 60016 → 53 [FIN, ACK] Seq=1 Ack=64 Win=513 Len=0
0.059420   53    60017 → 53 [FIN, ACK] Seq=1 Ack=52 Win=513 Len=0   60017       TCP: 60017 → 53 [FIN, ACK] Seq=1 Ack=52 Win=513 Len=0
0.059547   53    60018 → 53 [FIN, ACK] Seq=1 Ack=86 Win=512 Len=0   60018       TCP: 60018 → 53 [FIN, ACK] Seq=1 Ack=86 Win=512 Len=0
0.061097   58112   Initial, DCID=22d0b72236c12e0d, PKN: 1, PADDING, CRYPTO, CRYPTO, PADD   QUIC: Initial, DCID=22d0b72236c12e0d, PKN: 1, PADDING …
0.062890   53    53 → 60016 [FIN, ACK] Seq=64 Ack=2 Win=128 Len=0   60016       TCP: 53 → 60016 [FIN, ACK] Seq=64 Ack=2 Win=128 Len=0
0.062890   53    53 → 60017 [FIN, ACK] Seq=52 Ack=2 Win=128 Len=0   60017       TCP: 53 → 60017 [FIN, ACK] Seq=52 Ack=2 Win=128 Len=0
```

Packet 19: TCP: 53 → 60017 [FIN, ACK] Seq=52 Ack=2 Win=128 Len=0

■ Limit to display filter

Flow type: All Flows

Addresses: Any

student observation

1) what is promisiuso mode

promisuso mode is a netiowo interface card (NIC) setting ~~that~~ allows card to intercept and read all network packet on network segement

2) Does ARP packets has transport layer ~~Radas~~ header ? explain

No ARP packets do not have transport layer haeder

3) which transport layer protocol is used by DNS

DNS (Domain name system)? premarily uses UDP for its transport layer protocol

4) what is the port number used http protocol ? ~~HTTP~~ http protocol uses port number 80 by default

5) what is broadcast in address?

It is a broadcast IP address which is used to send packets to all devices on a specific network Segement

9/8/24

RESULT

Thus the experiment on packet capture tool wireshark is studied