Exp no 5

Practical: 5

Aim:-

Experiments on Packet capture tools; wireshark.

Pack sniffer:-

Sniff messages being sent/recieved from/ by your computer.

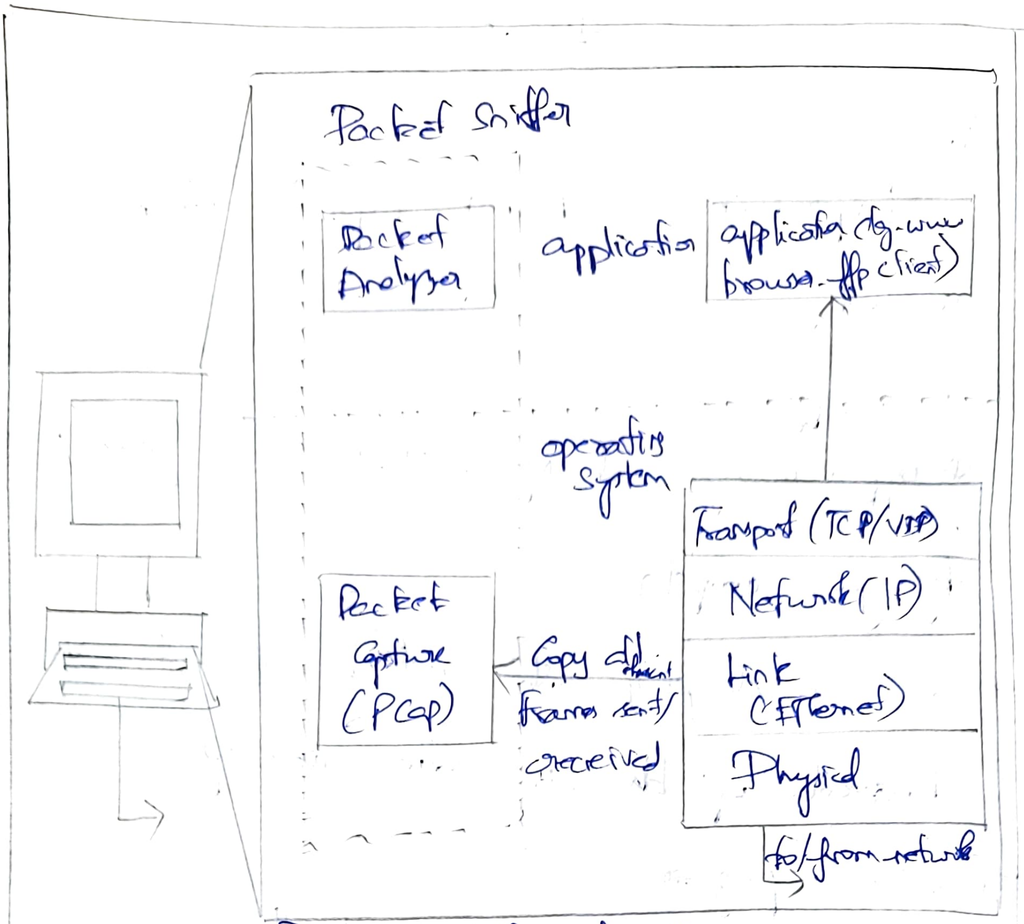
* Store & display the contents of the various Protocol fields in the message.

* Passive program.
  - Never sends packets itself
  - no packets addressed to it.
  - receives a copy of packets (sent/received)

Packet sniffer structure Diagnostic Tools:-

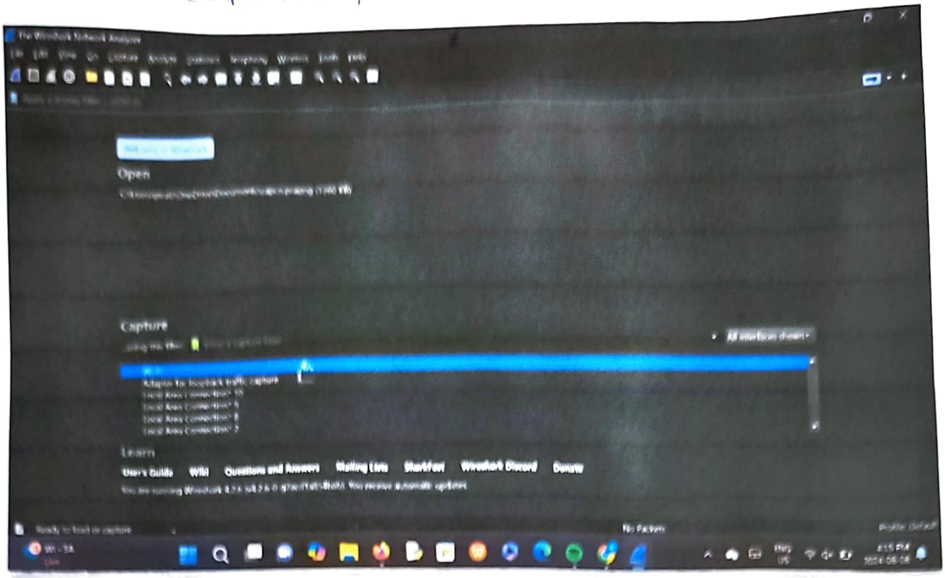
* Tcpdump:
  - Eg. tcpdump -enx host 10.129.41.2 -w ex3.out.

* Wire Shark
  - wire shark -r ex3.out



Packet Sniffer structure

CAPTURING PACKETS



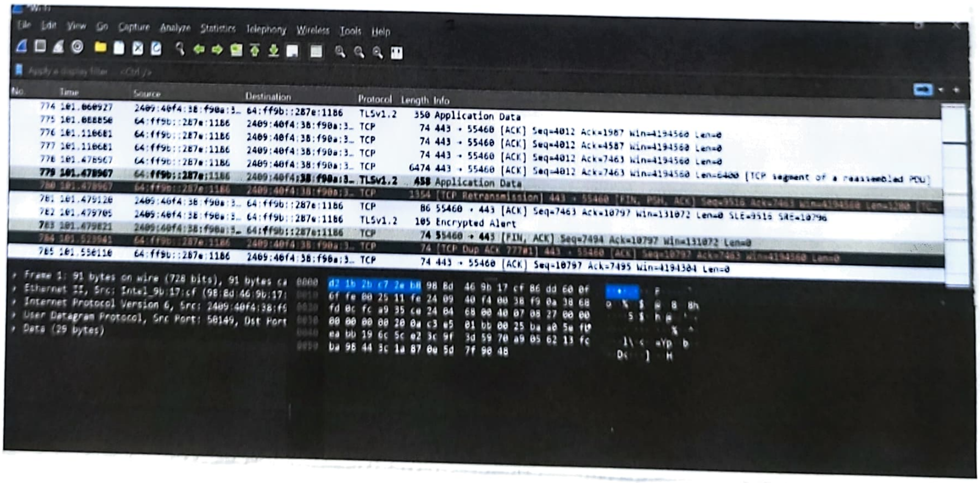
Open

Capture

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

Ready to load or capture

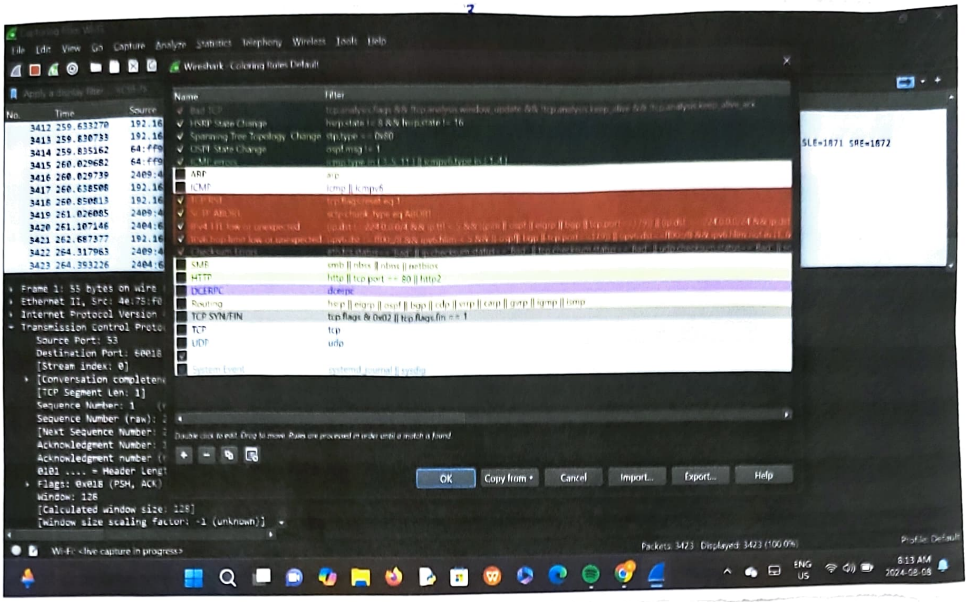
PACKET LISTS, DETAILS AND BYTES


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
 778 101.478567  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…
 781 101.479128  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
 785 101.556116  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 f0            %  ^
> 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
```

CAPTURING FILTERS



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Wireshark · Coloring Rules Default
OK
Copy from •
Cancel
Import...
Export...
Help
Packets: 3423 · Displayed: 3423 (100.0%)
Profile: Default
ENG US
8:13 AM 2024-08-08

```
No.  Time        Source
3412 259.633270  192.16
3413 259.830733  192.16
3414 259.835162  64:ff9
3415 260.029682  64:ff9
3416 260.029739  2409:4
3417 260.638508  192.16
3418 260.850813  192.16
3419 261.026085  2409:4
3420 261.107146  2404:6
3421 262.687377  192.16
3422 264.317963  2409:4
3423 264.393226  2404:6
```

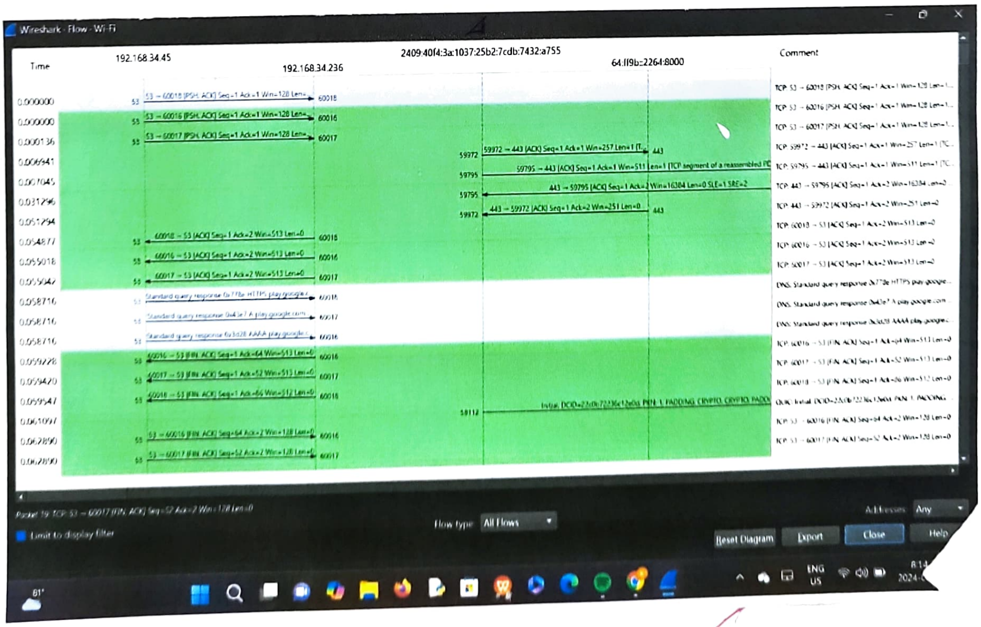
```
› Frame 1: 55 bytes on wire
› Ethernet II, Src: 4e:75:f0
› Internet Protocol Version
⌄ Transmission Control Proto
    Source Port: 53
    Destination Port: 60018
    [Stream index: 0]
  › [Conversation completene
    [TCP Segment Len: 1]
    Sequence Number: 1
    Sequence Number (raw): 2
    [Next Sequence Number: 2
    Acknowledgment Number: 1
    Acknowledgment number (r
    0101 .... = Header Lengt
  › Flags: 0x018 (PSH, ACK)
    Window: 128
    [Calculated window size: 128]
    [Window size scaling factor: -1 (unknown)]
```

SLE=1871 SRE=1872

	Name	Filter
✓	Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack
✓	HSRP State Change	hsrp.state != 8 && hsrp.state != 16
✓	Spanning Tree Topology Change	stp.type == 0x80
✓	OSPF State Change	ospf.msg != 1
✓	ICMP errors	icmp.type in { 3..5, 11 } || icmpv6.type in { 1..4 }
□	ARP	arp
□	ICMP	icmp || icmpv6
✓	TCP RST	tcp.flags.reset eq 1
✓	SCTP ABORT	sctp.chunk_type eq ABORT
✓	IPv4 TTL low or unexpected	(ip.dst != 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst == 224.0.0.0/24 && ip.dst ...
✓	IPv6 hop limit low or unexpected	(ipv6.dst != ff00::/8 && ipv6.hlim < 5 && !ospf) || (ipv6.dst == ff00::/8 && ipv6.hlim not in {1, ...
✓	Checksum Errors	eth.fcs.status == "Bad" || ip.checksum.status == "Bad" || tcp.checksum.status == "Bad" || udp.checksum.status == "Bad" || sc...
□	SMB	smb || nbss || nbns || netbios
□	HTTP	http || tcp.port == 80 || http2
□	DCERPC	dcerpc
□	Routing	hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
□	TCP SYN/FIN	tcp.flags & 0x02 || tcp.flags.fin == 1
□	TCP	tcp
□	UDP	udp
✓		
□	System Event	systemd_journal || sysdig

Double click to edit. Drag to move. Rules are processed in order until a match is found.

Wi-Fi: <live capture in progress>



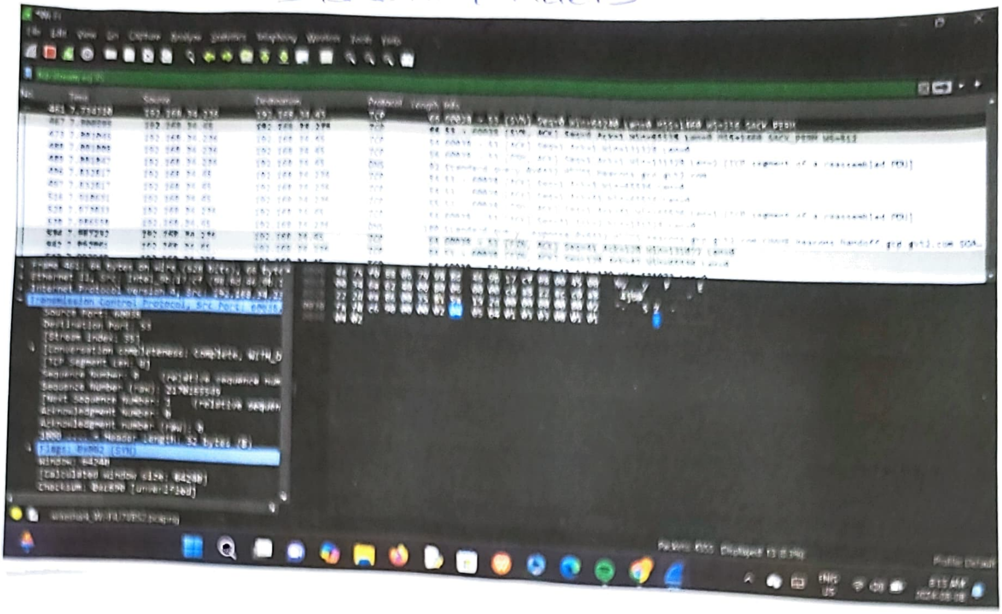
Wireshark · Flow · Wi-Fi
192.168.34.45
192.168.34.236
2409:40f4:3a:1037:25b2:7cdb:7432:a755
64:ff9b::2264:8000
53 → 60018 [PSH, ACK] Seq=1 Ack=1 Win=128 Len=...
53 → 60016 [PSH, ACK] Seq=1 Ack=1 Win=128 Len=...
53 → 60017 [PSH, ACK] Seq=1 Ack=1 Win=128 Len=...
59972 → 443 [ACK] Seq=1 Ack=1 Win=257 Len=1 [T...
59795 → 443 [ACK] Seq=1 Ack=1 Win=511 Len=1 [TCP segment of a reassembled PD
443 → 59795 [ACK] Seq=1 Ack=2 Win=16384 Len=0 SLE=1 SRE=2
443 → 59972 [ACK] Seq=1 Ack=2 Win=251 Len=0
60018 → 53 [ACK] Seq=1 Ack=2 Win=513 Len=0
60016 → 53 [ACK] Seq=1 Ack=2 Win=513 Len=0
60017 → 53 [ACK] Seq=1 Ack=2 Win=513 Len=0
Standard query response 0x778e HTTPS play.google.c...
Standard query response 0x43e7 A play.google.com ...
Standard query response 0x3d28 AAAA play.google.c...
60016 → 53 [FIN, ACK] Seq=1 Ack=64 Win=513 Len=0
60017 → 53 [FIN, ACK] Seq=1 Ack=52 Win=513 Len=0
60018 → 53 [FIN, ACK] Seq=1 Ack=66 Win=512 Len=0
Initial, DCID=22d0b72236c12e0a, PKN: 1, PADDING, CRYPTO, CRYPTO, PADD
53 → 60016 [FIN, ACK] Seq=64 Ack=2 Win=128 Len=0
53 → 60017 [FIN, ACK] Seq=52 Ack=2 Win=128 Len=0
53
60018
60016
60017
59972
59795
443
59112
Flow type
All Flows
Addresses
Any
Reset Diagram
Export
Close
Help
81°
ENG US

```
Time      Comment
0.000000  TCP: 53 → 60018 [PSH, ACK] Seq=1 Ack=1 Win=128 Len=1...
0.000000  TCP: 53 → 60016 [PSH, ACK] Seq=1 Ack=1 Win=128 Len=1...
0.000136  TCP: 53 → 60017 [PSH, ACK] Seq=1 Ack=1 Win=128 Len=1...
0.006941  TCP: 59972 → 443 [ACK] Seq=1 Ack=1 Win=257 Len=1 [TC...
0.007045  TCP: 59795 → 443 [ACK] Seq=1 Ack=1 Win=511 Len=1 [TC...
0.031296  TCP: 443 → 59795 [ACK] Seq=1 Ack=2 Win=16384 Len=0 ...
0.051294  TCP: 443 → 59972 [ACK] Seq=1 Ack=2 Win=251 Len=0
0.054877  TCP: 60018 → 53 [ACK] Seq=1 Ack=2 Win=513 Len=0
0.055018  TCP: 60016 → 53 [ACK] Seq=1 Ack=2 Win=513 Len=0
0.055042  TCP: 60017 → 53 [ACK] Seq=1 Ack=2 Win=513 Len=0
0.058716  DNS: Standard query response 0x778e HTTPS play.google...
0.058716  DNS: Standard query response 0x43e7 A play.google.com ...
0.058716  DNS: Standard query response 0x3d28 AAAA play.google.c...
0.059228  TCP: 60016 → 53 [FIN, ACK] Seq=1 Ack=64 Win=513 Len=0
0.059420  TCP: 60017 → 53 [FIN, ACK] Seq=1 Ack=52 Win=513 Len=0
0.059547  TCP: 60018 → 53 [FIN, ACK] Seq=1 Ack=66 Win=512 Len=0
0.061097  QUIC: Initial, DCID=22d0b72236c12e0a, PKN: 1, PADDING, ...
0.062890  TCP: 53 → 60016 [FIN, ACK] Seq=64 Ack=2 Win=128 Len=0
0.062890  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

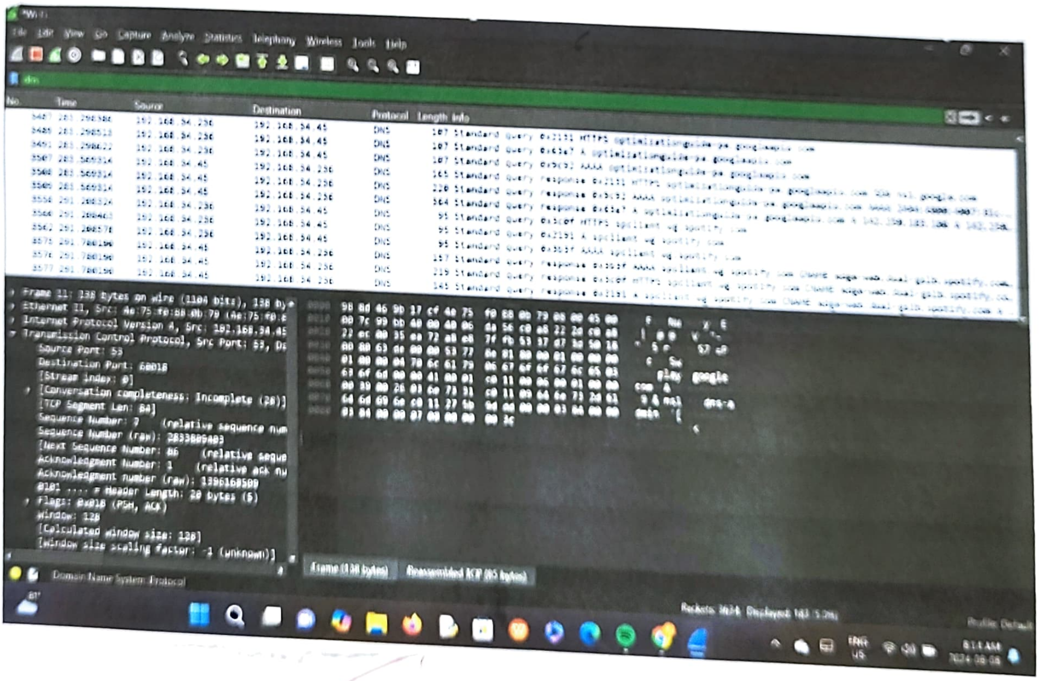
■ Limit to display filter

DISPLAYING FILTERS



```
Frame 481: 66 bytes on wire (528 bits), 66 bytes
Ethernet II, Src: Intel_
Internet Protocol Version 4, Src: 192.168.34.23
Transmission Control Protocol, Src Port: 60018,
    Source Port: 60018
    Destination Port: 53
    [Stream index: 35]
    [Conversation completeness: Complete, WITH_b
    [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: 0xc890 [unverified]
```

COLOURING RULES



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

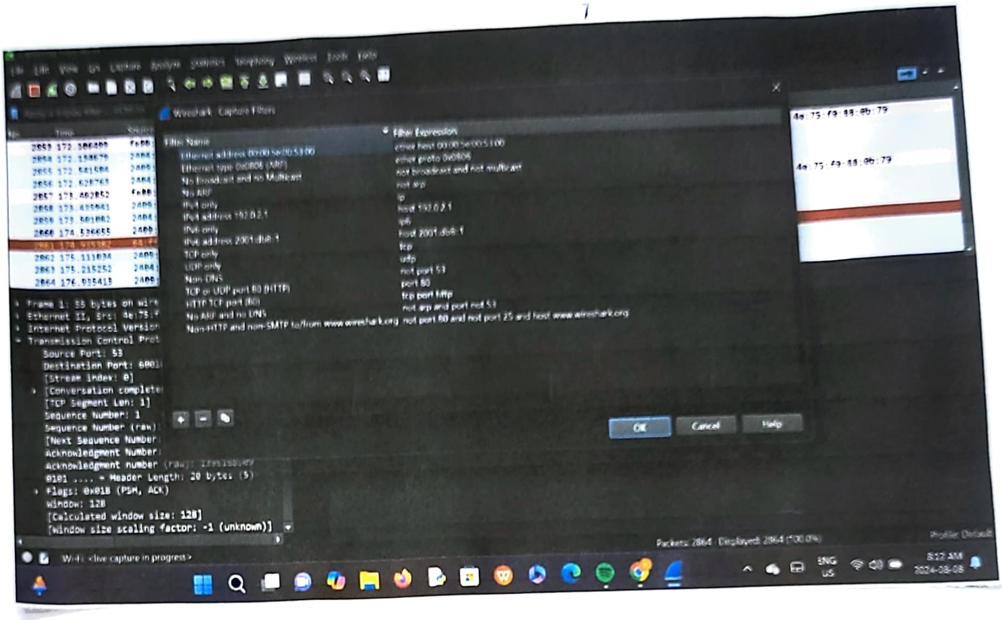
```
No.  Time        Source          Destination     Protocol Length Info
3487 283.298386  192.168.34.236  192.168.34.45   DNS      107 Standard query 0x2131 HTTPS optimizationguide-pa.googleapis.com
3488 283.298513  192.168.34.236  192.168.34.45   DNS      107 Standard query 0xc6a7 A optimizationguide-pa.googleapis.com
3491 283.298622  192.168.34.236  192.168.34.45   DNS      107 Standard query 0xb5c3 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
3508 283.569314  192.168.34.45   192.168.34.236  DNS      220 Standard query response 0xb5c3 AAAA optimizationguide-pa.googleapis.com SOA ns1.google.com
3509 283.569314  192.168.34.45   192.168.34.236  DNS      364 Standard query response 0xc6a7 A optimizationguide-pa.googleapis.com AAAA 2404:6800:4007:81c...
3554 291.208324  192.168.34.236  192.168.34.45   DNS       95 Standard query 0x3c0f HTTPS spclient.wg.spotify.com A 142.250.183.106 A 142.250...
3566 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 0x3b5f AAAA spclient.wg.spotify.com
3575 291.780190  192.168.34.45   192.168.34.236  DNS      157 Standard query response 0x3b5f AAAA spclient.wg.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.com
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
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: 7    (relative sequence num
    Sequence Number (raw): 2833809403
    [Next Sequence Number: 86    (relative seque
    Acknowledgment Number: 1    (relative ack nu
    Acknowledgment number (raw): 1396160509
    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
0010  00 7c 99 bb 40 00 40 06  da 56 c0 a8 22 2d c0 a8
0020  22 ec 00 35 ea 72 a8 e8  7f fb 53 37 d7 3d 50 18
0030  00 80 63 de 00 00 53 77  8e 81 80 00 01 00 00 00
0040  01 00 00 04 70 6c 61 79  06 67 6f 6f 67 6c 65 03
0050  63 6f 6d 00 00 41 00 01  c0 11 00 06 00 01 00 00
0060  00 39 00 26 03 6e 73 31  c0 11 09 64 6e 73 2d 61
0070  64 6d 69 6e c0 11 27 5b  ...
```

Frame (138 bytes)
Reassembled TCP (85 bytes)
Domain Name System Protocol
Packets: 3634 · Displayed: 143 (3.9%)
Profile: Default
ENG US
8:14 AM
2024-08-08

WoRK flow GRAPH



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

```
2853 172.106499   fe80:
2854 172.158679   2409:
2855 172.541584   2409:
2856 172.628763   2404:
2857 173.482852   fe80:
2858 173.435841   2409:
2859 173.501082   2404:
2860 174.526655   2409:
2861 174.935382   64:f
2862 175.111034   2409:
2863 175.215252   2404:
2864 176.935413   2409:
```

```
› Frame 1: 55 bytes on wire
› Ethernet II, Src: 4e:75:f
› Internet Protocol Version
⌄ Transmission Control Prot
    Source Port: 53
    Destination Port: 6001
    [Stream index: 0]
  › [Conversation complete
    [TCP Segment Len: 1]
    Sequence Number: 1
    Sequence Number (raw):
    [Next Sequence Number:
    Acknowledgment Number:
    Acknowledgment number (raw): 1[illegible]
    0101 .... = Header Length: 20 bytes (5)
  › Flags: 0x018 (PSH, ACK)
    Window: 128
    [Calculated window size: 128]
    [Window size scaling factor: -1 (unknown)]
```

4e:75:f9:88:0b:79

4e:75:f9:88:0b:79

Wi-Fi: <live capture in progress>

Packets: 2864 · Displayed: 2864 (100.0%)

Profile: Default

Student's observation:-

1.) What is Promiscous mode?

Promiscuous mode is a network interface card (NIC) setting that allows card to intercept or read all network packets on network segment.

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

No, ARP Packets do not have the transport layer header.

3.) Which transport layer protocol is used by DNS?

DNS (Domain name system) primarily uses UDP for its transport layer protocol.

4.) What is the port number used http protocol

HTTP protocol uses port number 80 by default.

5.) What is broadcast in address?

9/8/24

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

Result:- Thus the experiments on packet capture and wireshark are studied and observed.