Practical-5

AIM:-. Experiments on packet capture tools: wireshark.

Packet sniffer:-

(.) Sniffs message being sent by your computer.

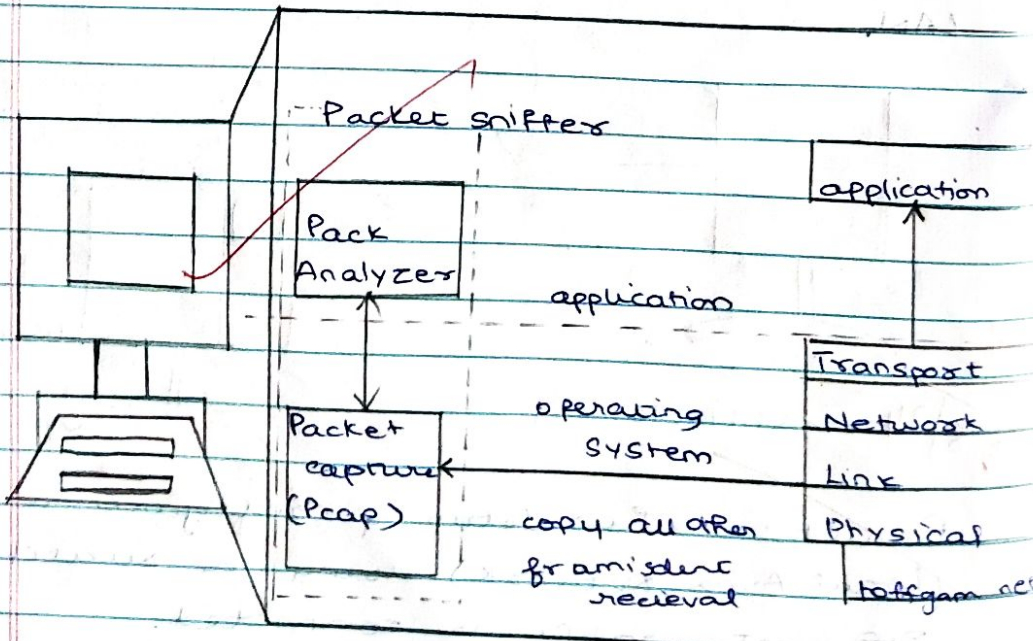
(.,) store & displays the contents of the various protocol fields in the message.

(.) passive program
- no never send packets tag
- no packets addressed it
- reciever a copy of packets

Packet sniffer structure diagnostic tools.

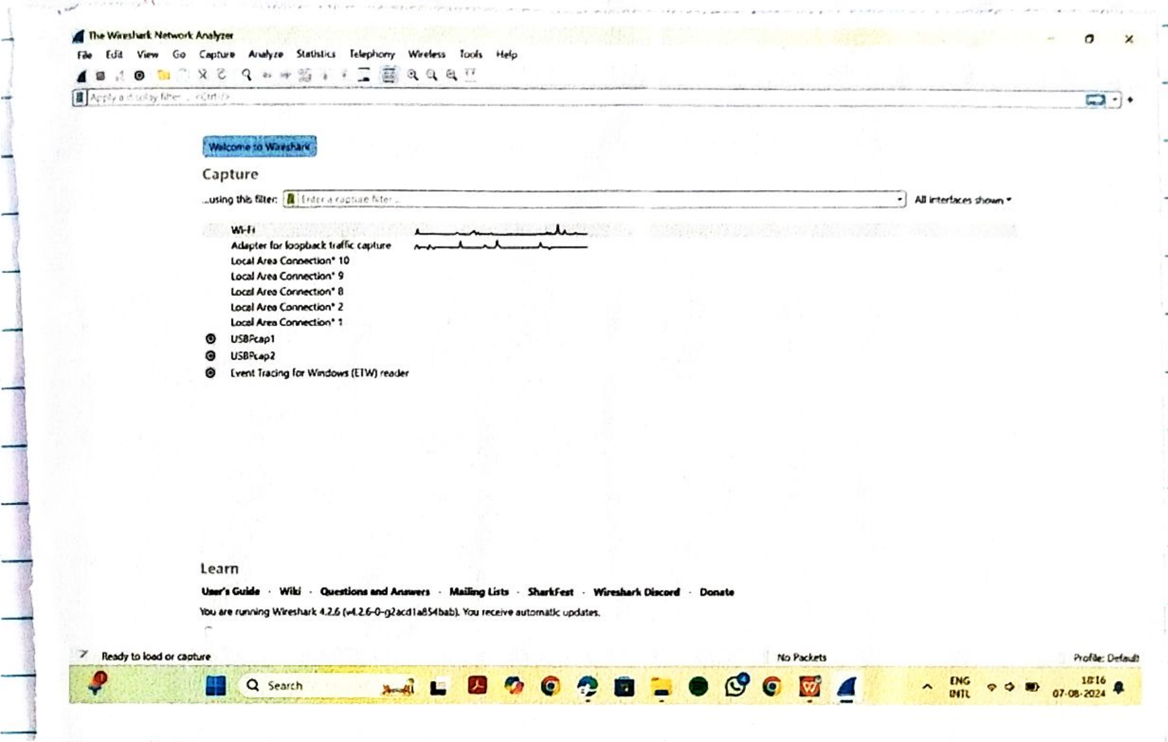
- Tcpdump
  - Eg. Acpdump -enx host 10.129.41.2 -w exe 3. out,

wire shark -r exe.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

Capture

…using this filter: Enter a capture filter … All interfaces shown

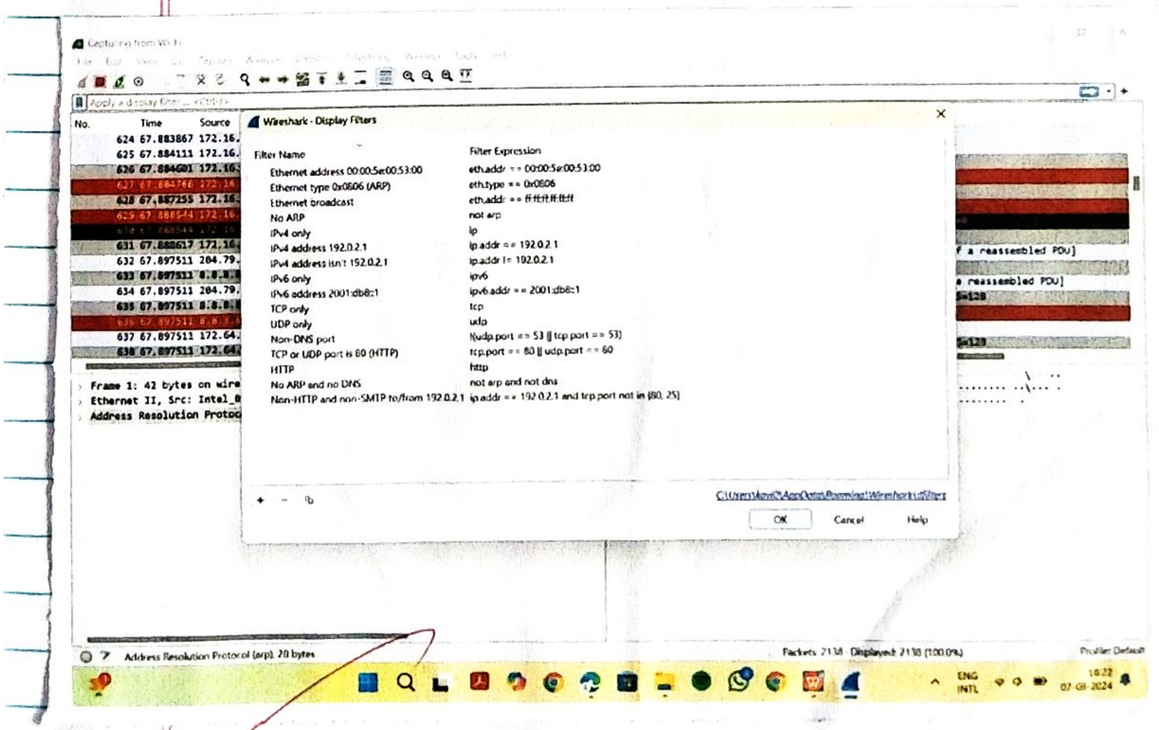
- Wi-Fi
- Adapter for loopback traffic capture
- Local Area Connection* 10
- Local Area Connection* 9
- Local Area Connection* 8
- Local Area Connection* 2
- Local Area Connection* 1
- USBPcap1
- USBPcap2
- Event Tracing for Windows (ETW) reader

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

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

Ready to load or capture | No Packets | Profile: Default



Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter … <Ctrl-/>

```
No.     Time       Source
   624 67.883867  172.16.
   625 67.884111  172.16.
   626 67.884601  172.16.
   627 67.884768  172.16
   628 67.887255  172.16.
   629 67.888544  172.16.
   630 67.888544  172.16
   631 67.888617  172.16.
   632 67.897511  204.79.
   633 67.897511  8.8.8.
   634 67.897511  204.79.
   635 67.897511  8.8.8.
   636 67.897511  8.8.8.
   637 67.897511  172.64.
   638 67.897511  172.64.

> Frame 1: 42 bytes on wire
> Ethernet II, Src: Intel_8
> Address Resolution Protoc
```

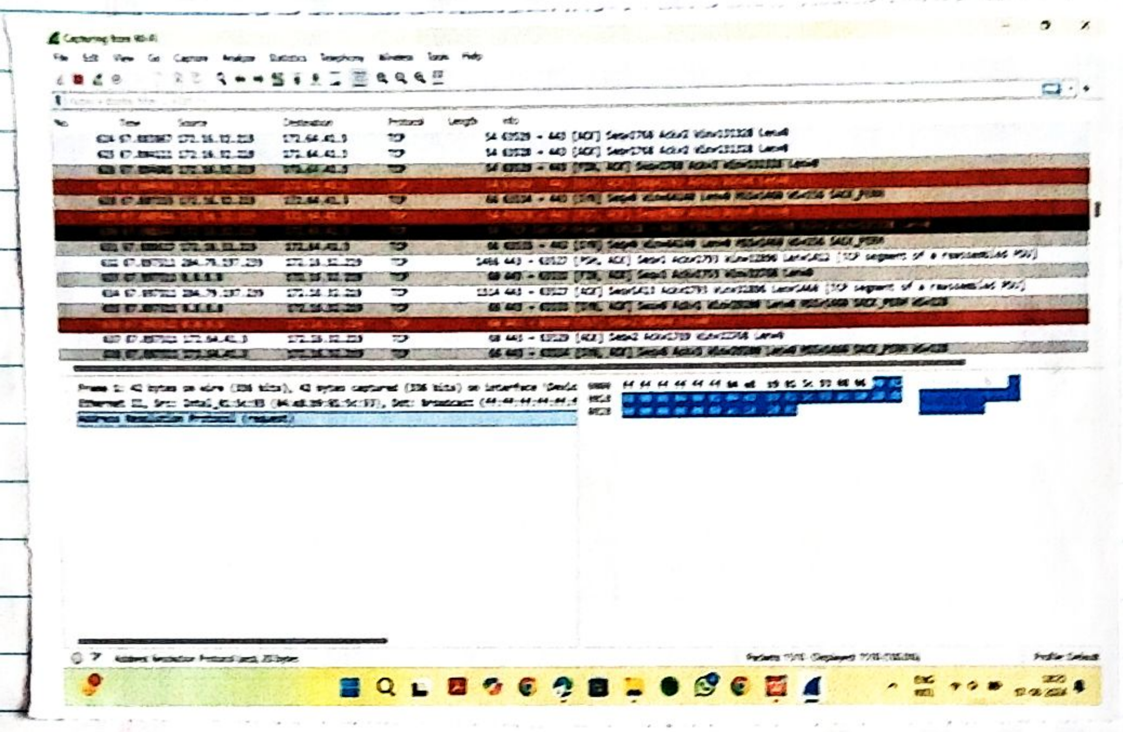
Wireshark - Display Filters

Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	eth.type == 0x0806
Ethernet broadcast	eth.addr == ff:ff:ff:ff:ff:ff
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	ip.addr == 192.0.2.1
IPv4 address isn't 192.0.2.1	ip.addr != 192.0.2.1
IPv6 only	ipv6
IPv6 address 2001:db8::1	ipv6.addr == 2001:db8::1
TCP only	tcp
UDP only	udp
Non-DNS port	!(udp.port == 53 || tcp.port == 53)
TCP or UDP port is 80 (HTTP)	tcp.port == 80 || udp.port == 80
HTTP	http
No ARP and no DNS	not arp and not dns
Non-HTTP and non-SMTP to/from 192.0.2.1	ip.addr == 192.0.2.1 and tcp.port not in {80, 25}

C:\Users\[illegible]\AppData\Roaming\Wireshark\dfilters

OK Cancel Help

Address Resolution Protocol (arp), 28 bytes | Packets: 2138 · Displayed: 2138 (100.0%) | Profile: Default

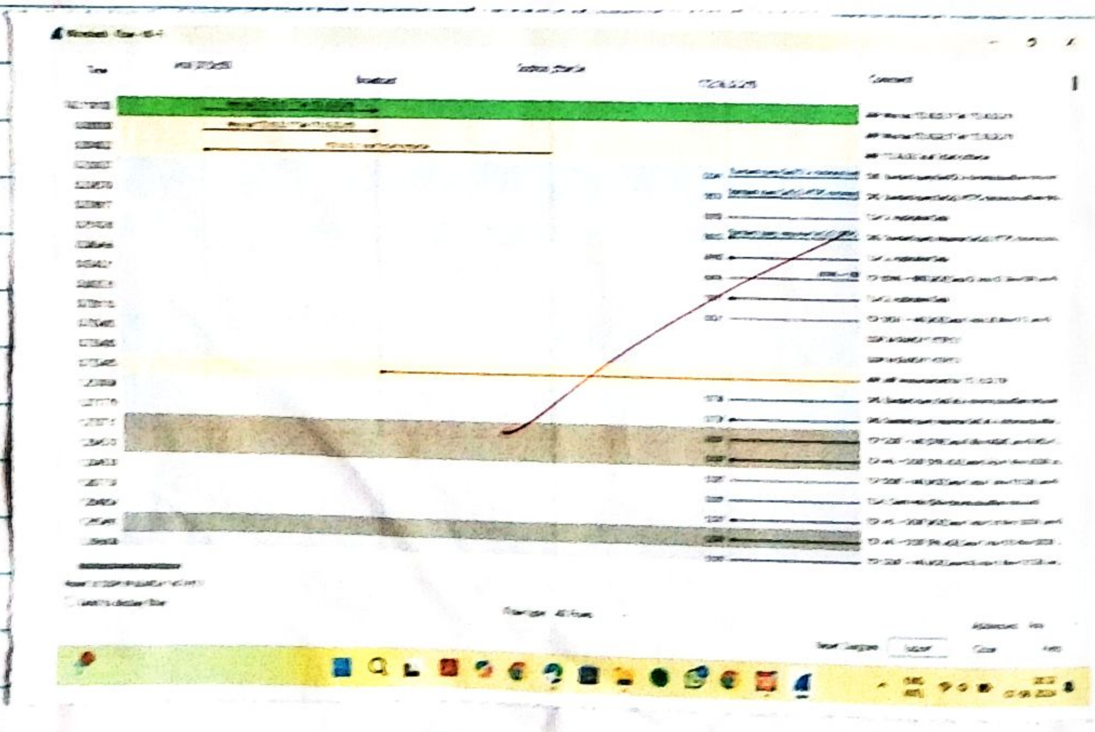

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

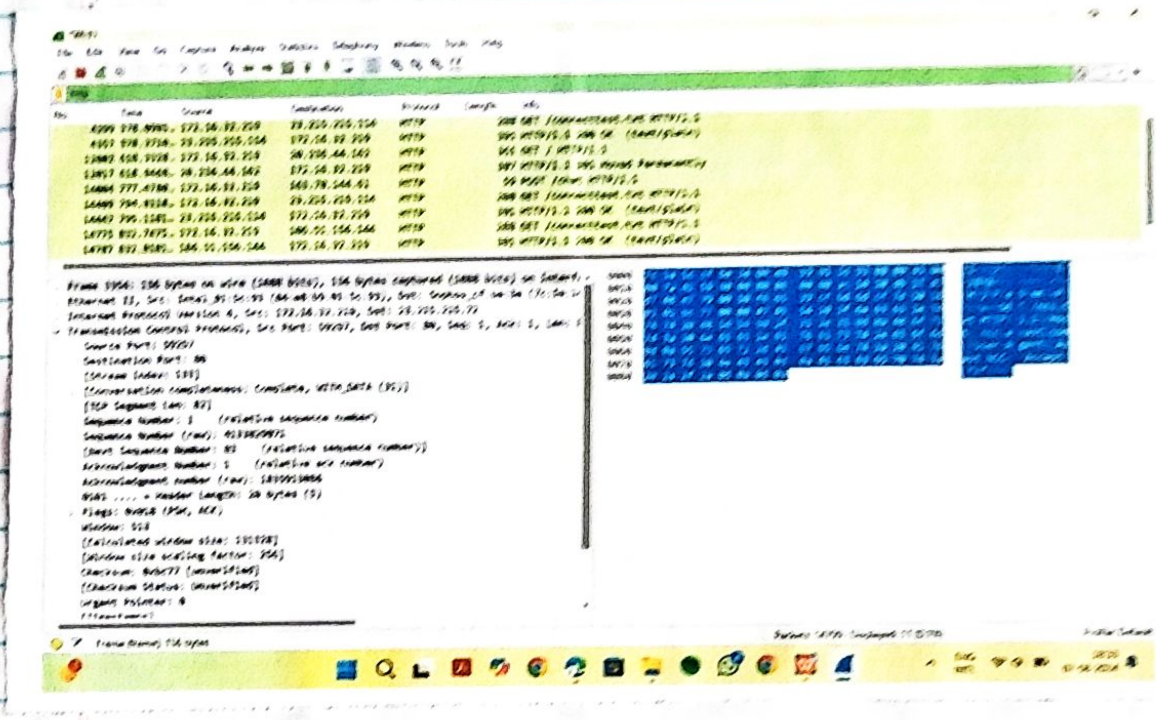
```
No.   Time       Source           Destination     Protocol  Length  Info
624 67.883867 172.16.32.233     172.64.41.3      TCP   54 63529 → 443 [ACK] Seq=1768 Ack=2 Win=131328 Len=0
625 67.884022 172.16.32.233     172.64.41.3      TCP   54 63528 → 443 [ACK] Seq=1768 Ack=2 Win=131328 Len=0
626 67.884085 172.16.32.233     172.64.41.3      TCP   54 63529 → 443 [FIN, ACK] Seq=1768 Ack=2 Win=131328 Len=0
[illegible]
628 67.887103 172.16.32.233     172.64.41.3      TCP   66 63534 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
[illegible]
[illegible]
631 67.888637 172.16.32.233     172.64.41.3      TCP   66 63533 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
632 67.897022 204.79.197.229    172.16.32.229    TCP   1466 443 → 63527 [PSH, ACK] Seq=1 Ack=1793 Win=32896 Len=1412 [TCP segment of a reassembled PDU]
633 67.897022 8.8.8.8           172.16.32.229    TCP   60 443 → 63533 [FIN, ACK] Seq=1 Ack=1793 Win=32768 Len=0
634 67.897022 204.79.197.229    172.16.32.229    TCP   1514 443 → 63527 [ACK] Seq=1413 Ack=1793 Win=32896 Len=1460 [TCP segment of a reassembled PDU]
635 67.897022 8.8.8.8           172.16.32.229    TCP   66 443 → 63533 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
[illegible]
637 67.897022 172.64.41.3       172.16.32.233    TCP   60 443 → 63529 [ACK] Seq=2 Ack=1769 Win=32768 Len=0
638 67.897022 172.64.41.3       172.16.32.233    TCP   66 443 → 63534 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Devic
Ethernet II, Src: Dell_81:5c:f8 (84:a8:39:81:5c:f7), Dst: Broadcast (ff:ff:ff:ff:ff:f
Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 84 a8 39 81 5c f7 08 06 [illegible]
0010  [illegible]
0020  [illegible]

Address Resolution Protocol (arp), 28 bytes        Packets: [illegible] · Displayed: [illegible]        Profile: Default
```





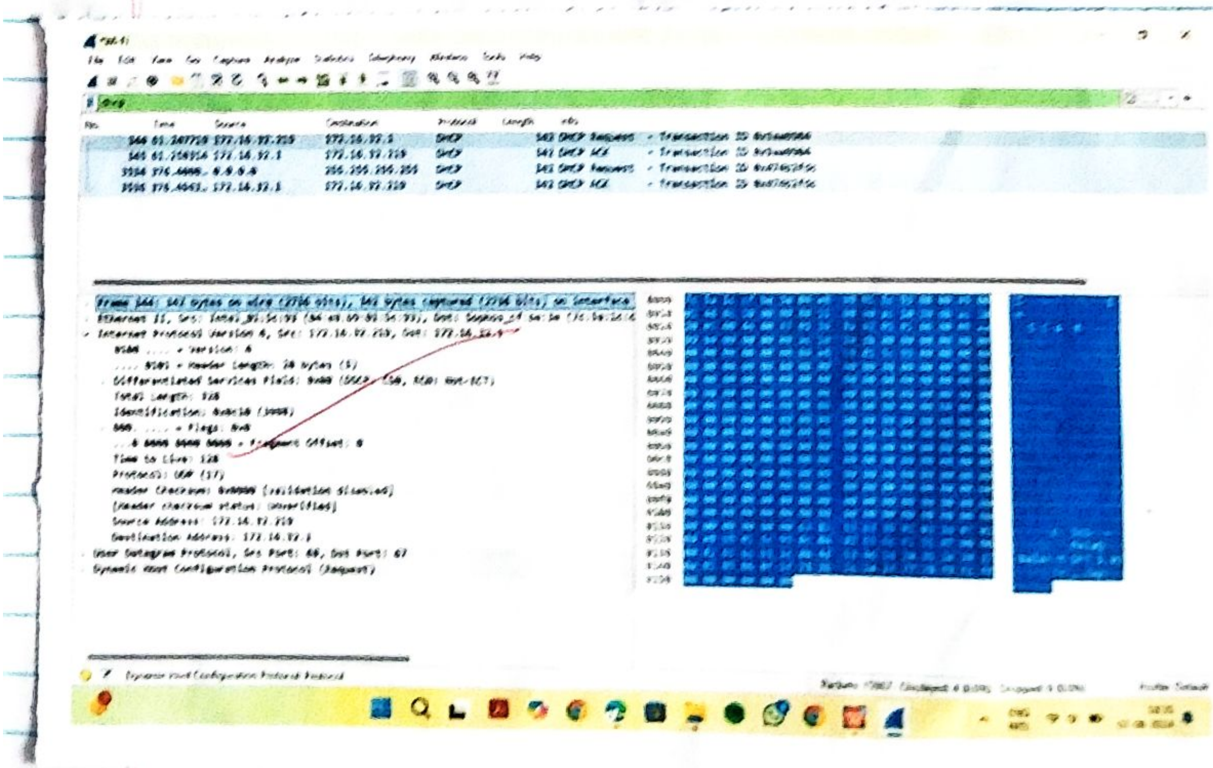
```
No.     Time        Source            Destination       Protocol  Length  Info
 4299 278.8985… 172.16.92.219     23.215.210.114    HTTP              208 GET /connecttest.txt HTTP/1.1
 4317 278.3716… 23.215.210.114    172.16.92.219     HTTP              195 HTTP/1.1 200 OK  (text/plain)
13882 618.3928… 172.16.92.219     20.236.44.162     HTTP              165 GET / HTTP/1.1
13917 618.5668… 20.236.44.162     172.16.92.219     HTTP              587 HTTP/1.1 301 Moved Permanently
14484 777.4780… 172.16.92.219     148.78.144.41     HTTP               59 POST /ohwr HTTP/1.1
14499 794.4318… 172.16.92.219     23.215.210.114    HTTP              208 GET /connecttest.txt HTTP/1.1
14467 795.1181… 23.215.210.114    172.16.92.219     HTTP              195 HTTP/1.1 200 OK  (text/plain)
14775 892.7875… 172.16.92.219     146.75.156.144    HTTP              208 GET /connecttest.txt HTTP/1.1
14787 892.9585… 146.75.156.144    172.16.92.219     HTTP              195 HTTP/1.1 200 OK  (text/plain)
```

```
Frame 3956: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interf
Ethernet II, Src: Intel_93:5c:93 (84:a8:69:93:5c:93), Dst: Sophos_cf:se:5e (7c:5e:
Internet Protocol Version 4, Src: 172.16.92.219, Dst: 23.215.210.77
Transmission Control Protocol, Src Port: 59207, Dst Port: 80, Seq: 1, Ack: 1, Len: 8
    Source Port: 59207
    Destination Port: 80
    [Stream index: 111]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 82]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 4233829871
    [Next Sequence Number: 83    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1899915886
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 513
    [Calculated window size: 131328]
    [Window size scaling factor: 256]
    Checksum: 0xbc77 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
```

Frame (frame), 136 bytes

Packets: 14999 · Displayed: 11 (0.1%)

Profile: Default



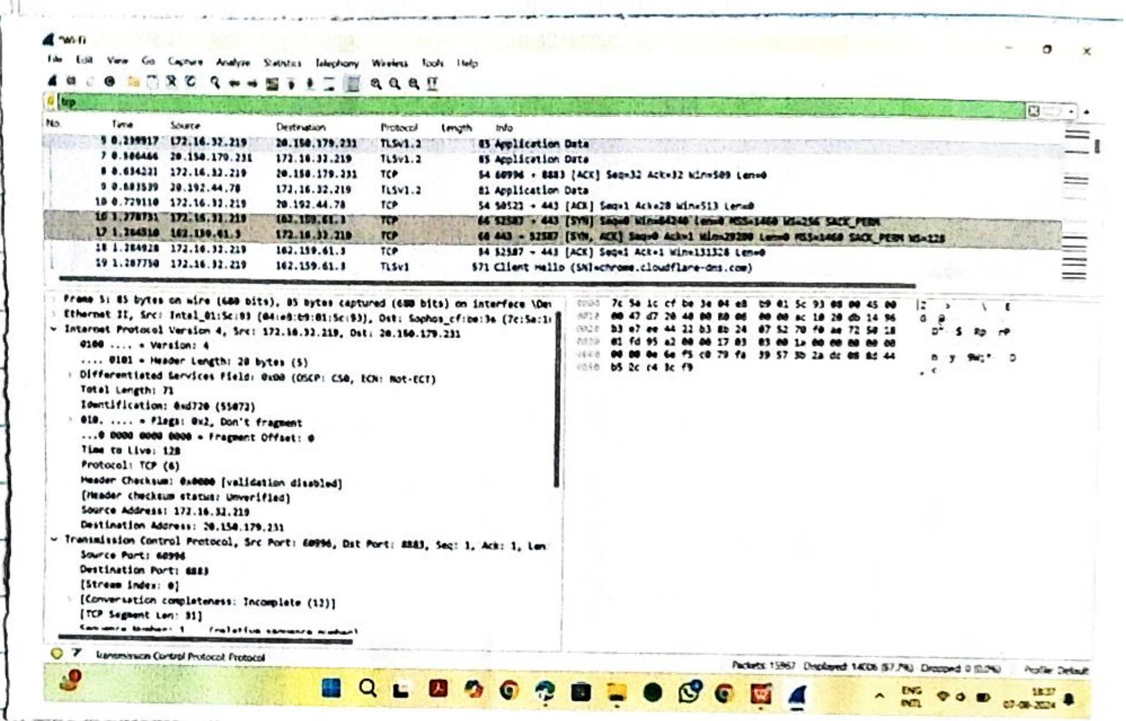
```
No.     Time        Source            Destination       Protocol  Length  Info
  544 61.247719 172.16.92.219     172.16.92.1       DHCP              342 DHCP Request  - Transaction ID 0x5aa0f066
  545 61.258914 172.16.92.1       172.16.92.219     DHCP              342 DHCP ACK      - Transaction ID 0x5aa0f066
 3554 376.4408… 0.0.0.0           255.255.255.255   DHCP              342 DHCP Request  - Transaction ID 0xd7f652f5c
 3556 376.4643… 172.16.92.1       172.16.92.219     DHCP              342 DHCP ACK      - Transaction ID 0xd7f652f5c
```

```
Frame 544: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface
Ethernet II, Src: Intel_93:5c:93 (84:a8:69:93:5c:93), Dst: Sophos_cf:se:5e (7c:5e:1e:
Internet Protocol Version 4, Src: 172.16.92.219, Dst: 172.16.92.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 328
    Identification: 0xbc10 (48144)
    000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.16.92.219
    Destination Address: 172.16.92.1
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Request)
```

Dynamic Host Configuration Protocol: Protocol

Packets: 15887 · Displayed: 4 (0.0%)

Profile: Default


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

```
No.   Time        Source          Destination     Protocol  Length  Info
  5 0.239917   172.16.32.219   20.150.179.231   TLSv1.2      85 Application Data
  7 0.506466   20.150.179.231  172.16.32.219    TLSv1.2      85 Application Data
  8 0.634221   172.16.32.219   20.150.179.231   TCP          54 60996 → 8883 [ACK] Seq=32 Ack=32 Win=509 Len=0
  9 0.683539   20.192.44.78    172.16.32.219    TLSv1.2      81 Application Data
 10 0.729110   172.16.32.219   20.192.44.78     TCP          54 50521 → 443 [ACK] Seq=1 Ack=28 Win=513 Len=0
 16 1.278731   172.16.32.219   162.159.61.3     TCP          66 52587 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 17 1.284810   162.159.61.3    172.16.32.219    TCP          66 443 → 52587 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
 18 1.284928   172.16.32.219   162.159.61.3     TCP          54 52587 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
 19 1.287750   172.16.32.219   162.159.61.3     TLSv1       571 Client Hello (SNI=chrome.cloudflare-dns.com)
```

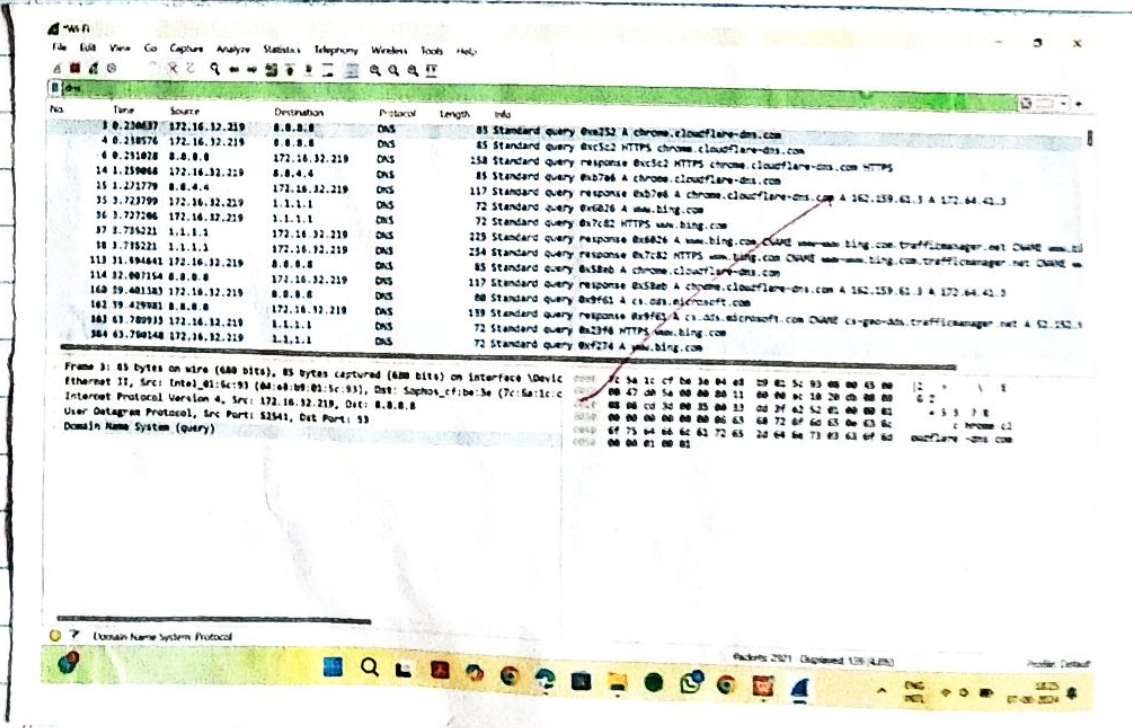
```
> Frame 5: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Dev
> Ethernet II, Src: Intel_01:5c:93 (04:e8:b9:01:5c:93), Dst: Sophos_cf:be:3e (7c:5a:1
v Internet Protocol Version 4, Src: 172.16.32.219, Dst: 20.150.179.231
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 71
    Identification: 0xd720 (55072)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.16.32.219
    Destination Address: 20.150.179.231
v Transmission Control Protocol, Src Port: 60996, Dst Port: 8883, Seq: 1, Ack: 1, Len
    Source Port: 60996
    Destination Port: 8883
    [Stream index: 0]
  > [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 31]
    Sequence Number: 1    (relative sequence number)
```

```
0000  7c 5a 1c cf be 3e 04 e8  b9 01 5c 93 08 00 45 00   |Z   >   \  E
0010  00 47 d7 20 40 00 80 06  00 00 ac 10 20 db 14 96   G @
0020  b3 e7 ee 44 22 b3 8b 24  07 52 70 f0 ae 72 50 18    D" $ Rp rP
0030  01 fd 95 a2 00 00 17 03  03 00 1a 00 00 00 00 00
0040  00 00 0e 6e f5 c0 79 fa  39 57 3b 2a dc 08 8d 44    n y 9W;* D
0050  b5 2c c4 3c f9                                      ,<
```

Transmission Control Protocol: Protocol

Packets: 15967 · Displayed: 14006 (87.7%) · Dropped: 0 (0.0%) · Profile: Default

ENG
INTL
18:37
07-08-2024


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

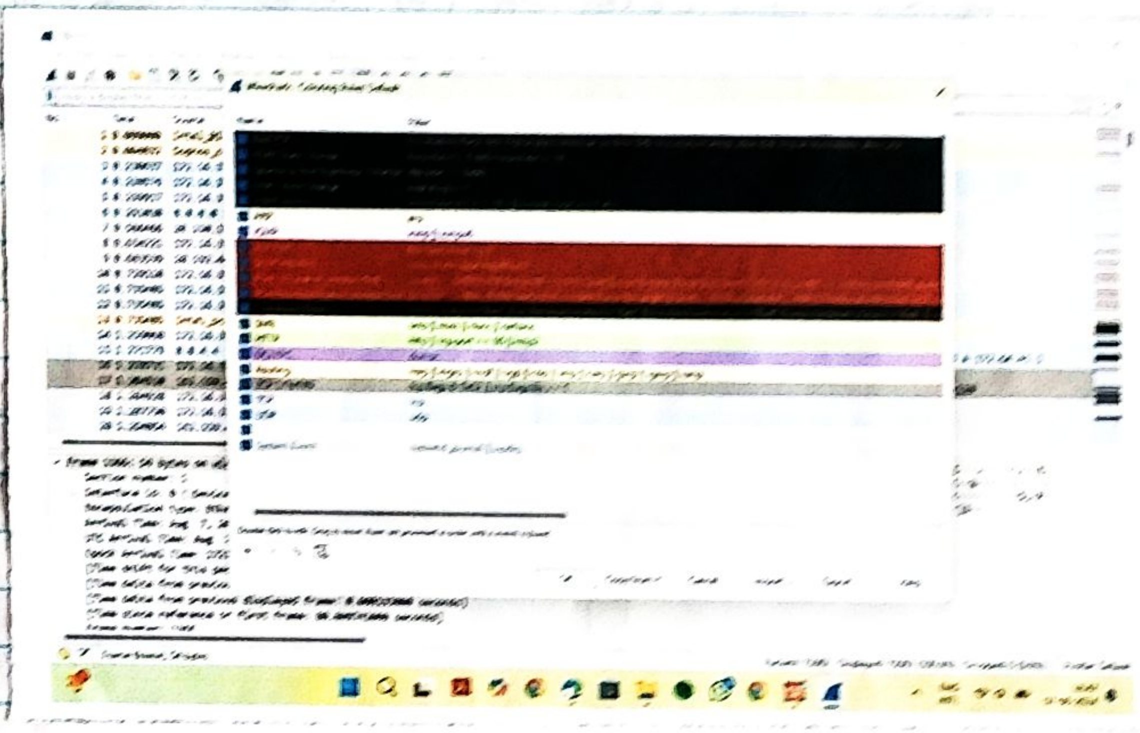
```
No.   Time         Source          Destination     Protocol  Length  Info
  3 0.230637    172.16.32.219   8.8.8.8          DNS          85 Standard query 0xa252 A chrome.cloudflare-dns.com
  4 0.238576    172.16.32.219   8.8.8.8          DNS          85 Standard query 0xc5c2 HTTPS chrome.cloudflare-dns.com
  6 0.251028    8.8.8.8         172.16.32.219    DNS         158 Standard query response 0xc5c2 HTTPS chrome.cloudflare-dns.com HTTPS
 14 1.259068    172.16.32.219   8.8.4.4          DNS          85 Standard query 0xb7e6 A chrome.cloudflare-dns.com
 15 1.271779    8.8.4.4         172.16.32.219    DNS         117 Standard query response 0xb7e6 A chrome.cloudflare-dns.com A 162.159.61.3 A 172.64.41.3
 35 3.723799    172.16.32.219   1.1.1.1          DNS          72 Standard query 0x6026 A www.bing.com
 36 3.727206    172.16.32.219   1.1.1.1          DNS          72 Standard query 0x7c82 HTTPS www.bing.com
 37 3.735221    1.1.1.1         172.16.32.219    DNS         225 Standard query response 0x6026 A www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www.bi
 38 3.735221    1.1.1.1         172.16.32.219    DNS         254 Standard query response 0x7c82 HTTPS www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME w
113 31.894641   172.16.32.219   8.8.8.8          DNS          85 Standard query 0x58eb A chrome.cloudflare-dns.com
114 32.007154   8.8.8.8         172.16.32.219    DNS         117 Standard query response 0x58eb A chrome.cloudflare-dns.com A 162.159.61.3 A 172.64.41.3
160 39.401383   172.16.32.219   8.8.8.8          DNS          80 Standard query 0x9f61 A cs.dds.microsoft.com
162 39.429981   8.8.8.8         172.16.32.219    DNS         139 Standard query response 0x9f61 A cs.dds.microsoft.com CNAME cs-geo-dds.trafficmanager.net A 52.152.1
383 63.789933   172.16.32.219   1.1.1.1          DNS          72 Standard query 0x2396 HTTPS www.bing.com
384 63.790148   172.16.32.219   1.1.1.1          DNS          72 Standard query 0xf274 A www.bing.com
```

```
Frame 3: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Devic
Ethernet II, Src: Intel_01:5c:93 (04:e8:b9:01:5c:93), Dst: Sophos_cf:be:3e (7c:5a:1c:c
Internet Protocol Version 4, Src: 172.16.32.219, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 52541, Dst Port: 53
Domain Name System (query)
```

```
0000  7c 5a 1c cf be 3e 04 e8  b9 01 5c 93 08 00 45 00   |Z   >   \  E
0010  00 47 d8 5a 00 00 80 11  00 00 ac 10 20 db 08 08    G Z
0020  08 08 cd 3d 00 35 00 33  dd 3f 62 52 01 00 00 01      = 5 3  ?bR
0030  00 00 00 00 00 00 06 63  68 72 6f 6d 65 0a 63 6c         c hrome cl
0040  6f 75 64 66 6c 61 72 65  2d 64 6e 73 03 63 6f 6d   oudflare -dns com
0050  00 00 01 00 01
```

Domain Name System: Protocol

Packets: 2021 · Displayed: 138 (6.8%) · Profile: Default



Date:

Student's Observation :-

1) What is promiscous mode?

promiscuous mode is a netcome interface card setting that allows card to intercept and read all network packets on network segment.

2) Drs ARP packets has transport layer header? Explain.

No ARP Packets do not have transport layer header.

3) which transport layer protocal is used by DNS ?

DNS primarily uses UDP for its transport layer protocol.

4) what is the port number used http protocol?

HFTP protocol uses number 80 by default.

5) what is Broadcast ip address?

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 tool wireshark is studied and observed.