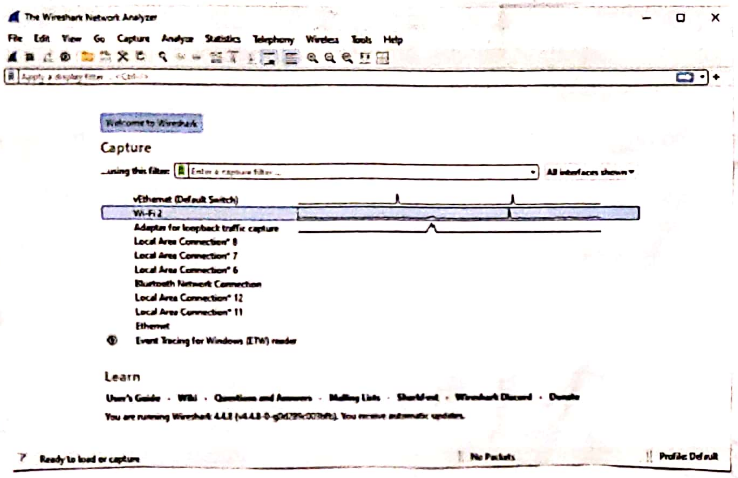
31/7/25 Experiment - 5

Aim : Experiments on Packet capture tool : wireshark.

Capturing Packets.

After downloading and installing wireshark, launch it and double click the name of a network interface


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

vEthernet (Default Switch)
Wi-Fi 2
Adapter for loopback traffic capture
Local Area Connection* 8
Local Area Connection* 7
Local Area Connection* 6
Bluetooth Network Connection
Local Area Connection* 12
Local Area Connection* 11
Ethernet
Event Tracing for Windows (ETW) reader

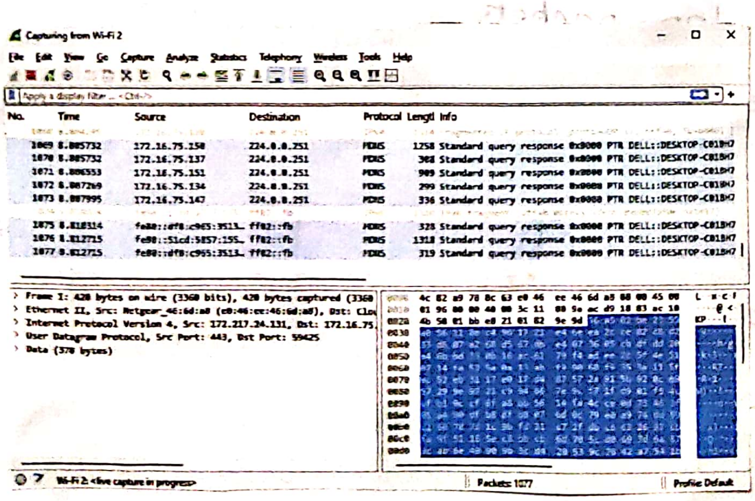
Learn

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

You are running Wireshark 4.4.8 (v4.4.8-0-g0d295c0078fb). You receive automatic updates.

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

As soon as you click the interfaces name, you'll see the packs start to accept in real time.


Capturing from Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

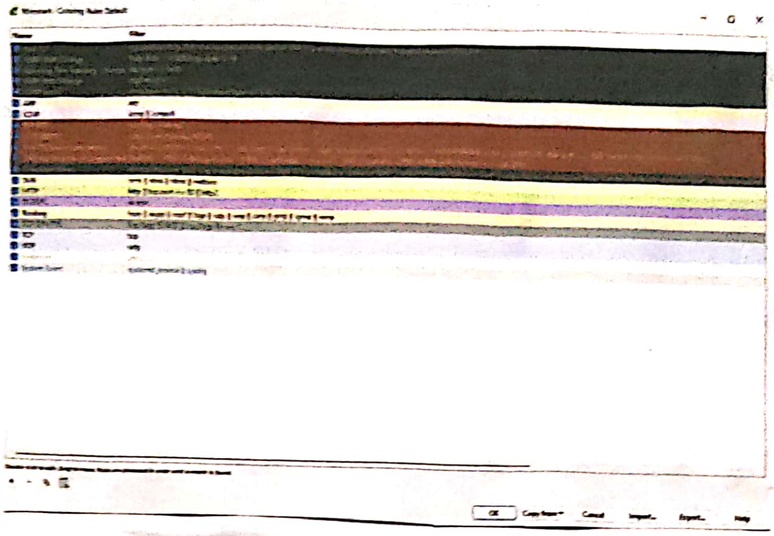
```
No.  Time      Source                  Destination  Protocol Lengt Info
1069 8.805732  172.16.75.150           224.0.0.251  MDNS     1258 Standard query response 0x0000 PTR DELL::DESKTOP-C01BH7
1070 8.805732  172.16.75.137           224.0.0.251  MDNS      308 Standard query response 0x0000 PTR DELL::DESKTOP-C01BH7
1071 8.806553  172.16.75.151           224.0.0.251  MDNS      909 Standard query response 0x0000 PTR DELL::DESKTOP-C01BH7
1072 8.807269  172.16.75.134           224.0.0.251  MDNS      299 Standard query response 0x0000 PTR DELL::DESKTOP-C01BH7
1073 8.807995  172.16.75.147           224.0.0.251  MDNS      336 Standard query response 0x0000 PTR DELL::DESKTOP-C01BH7
1075 8.810314  fe80::df8:c965:3513…    ff02::fb     MDNS      328 Standard query response 0x0000 PTR DELL::DESKTOP-C01BH7
1076 8.812715  fe80::51cd:5857:155…    ff02::fb     MDNS     1318 Standard query response 0x0000 PTR DELL::DESKTOP-C01BH7
1077 8.812715  fe80::df8:c965:3513…    ff02::fb     MDNS      319 Standard query response 0x0000 PTR DELL::DESKTOP-C01BH7
```

```
> Frame 1: 420 bytes on wire (3360 bits), 420 bytes captured (3360
> Ethernet II, Src: Netgear_46:6d:a8 (e0:46:ee:46:6d:a8), Dst: Clo
> Internet Protocol Version 4, Src: 172.217.24.131, Dst: 172.16.75.
> User Datagram Protocol, Src Port: 443, Dst Port: 59425
> Data (378 bytes)
```

```
0000  4c 82 a9 78 8c 63 e0 46  ee 46 6d a8 08 00 45 00
0010  01 96 00 00 40 00 3c 11  00 9a ac d9 18 83 ac 10
0020  4b 50 01 bb e8 21 01 82  9e 9d
```

Wi-Fi 2: <live capture in progress> | Packets: 1077 | Profile: Default

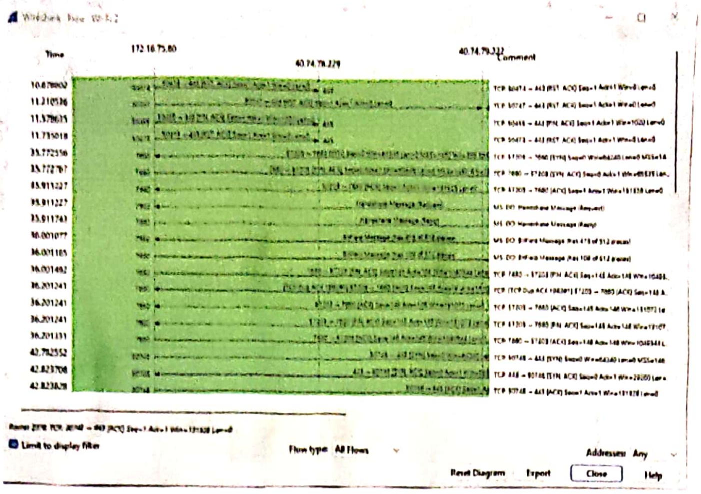
To view exactly what the colour codes mean click views colouring rules.



Capturing and analysing packets using wireshark tool.

1. Filter TCP/UDP packets

- * → Select local area connection in wireshark capture → option.
  → Select stop capture automatically after 100 packets.
- * Then click stop capture.
- * Search TCP packets in search bar
- * To see flow graph click statistics → flow graph
- * Save the packets.



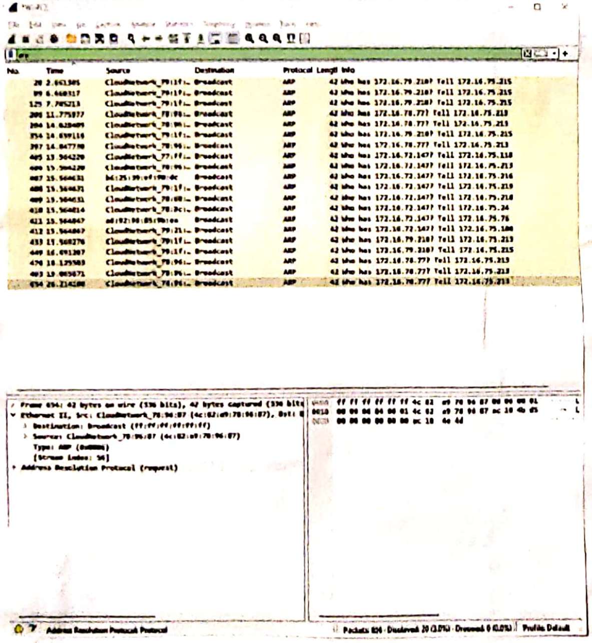
Wireshark · Flow · Wi-Fi 2

```
Time        172.16.75.80     40.74.76.229     40.74.79.222   Comment
10.678002                                                    TCP 60474 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11.210536                                                    TCP 60747 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11.578635                                                    TCP 60468 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1022 Len=0
11.735018                                                    TCP 60473 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
35.772556                                                    TCP 57208 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=14
35.772767                                                    TCP 7680 → 57208 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len..
35.911227                                                    TCP 57208 → 7680 [ACK] Seq=1 Ack=1 Win=131328 Len=0
35.911227                                                    MS DO Handshake Message (Request)
35.911743                                                    MS DO Handshake Message (Reply)
36.001077                                                    MS DO BitField Message (has 478 of 512 pieces)
36.001105                                                    MS DO BitField Message (has 108 of 512 pieces)
36.001402                                                    TCP 7680 → 57208 [FIN, ACK] Seq=148 Ack=148 Win=10485..
36.201241                                                    TCP [TCP Dup ACK 1063#1] 57208 → 7680 [ACK] Seq=148 A..
36.201241                                                    TCP 57208 → 7680 [ACK] Seq=148 Ack=148 Win=131072 Le
36.201241                                                    TCP 57208 → 7680 [FIN, ACK] Seq=148 Ack=148 Win=13107
36.201331                                                    TCP 7680 → 57208 [ACK] Seq=148 Ack=148 Win=10485441 L
42.782552                                                    TCP 60748 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=146
42.823706                                                    TCP 443 → 60748 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=
42.823828                                                    TCP 60748 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0

Frame 2078: TCP: 60748 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
```

Filter to display ARP packets

* Search ARP packets in search bar.



arp

No.	Time	Source	Destination	Protocol	Length	Info
20	2.661305	CloudNetwork_79:1f:…	Broadcast	ARP	42	Who has 172.16.79.210? Tell 172.16.75.215
99	6.660317	CloudNetwork_79:1f:…	Broadcast	ARP	42	Who has 172.16.79.210? Tell 172.16.75.215
125	7.705213	CloudNetwork_79:1f:…	Broadcast	ARP	42	Who has 172.16.79.210? Tell 172.16.75.215
205	11.775977	CloudNetwork_78:96:…	Broadcast	ARP	42	Who has 172.16.78.77? Tell 172.16.75.213
294	14.620409	CloudNetwork_78:96:…	Broadcast	ARP	42	Who has 172.16.78.77? Tell 172.16.75.213
354	14.699116	CloudNetwork_79:1f:…	Broadcast	ARP	42	Who has 172.16.79.210? Tell 172.16.75.215
397	14.847730	CloudNetwork_78:96:…	Broadcast	ARP	42	Who has 172.16.78.77? Tell 172.16.75.213
405	15.564220	CloudNetwork_77:ff:…	Broadcast	ARP	42	Who has 172.16.72.147? Tell 172.16.75.118
406	15.564220	CloudNetwork_78:96:…	Broadcast	ARP	42	Who has 172.16.72.147? Tell 172.16.75.213
407	15.564631	b6:25:39:ef:90:dc	Broadcast	ARP	42	Who has 172.16.72.147? Tell 172.16.75.216
408	15.564671	CloudNetwork_79:1f:…	Broadcast	ARP	42	Who has 172.16.72.147? Tell 172.16.75.219
409	15.564631	CloudNetwork_78:08:…	Broadcast	ARP	42	Who has 172.16.72.147? Tell 172.16.75.218
410	15.564814	CloudNetwork_78:3c:…	Broadcast	ARP	42	Who has 172.16.72.147? Tell 172.16.75.24
411	15.564867	ad:92:90:85:9b:ea	Broadcast	ARP	42	Who has 172.16.72.147? Tell 172.16.75.76
412	15.564867	CloudNetwork_79:21:…	Broadcast	ARP	42	Who has 172.16.72.147? Tell 172.16.75.100
433	15.568276	CloudNetwork_79:1f:…	Broadcast	ARP	42	Who has 172.16.79.210? Tell 172.16.75.213
449	16.691307	CloudNetwork_79:1f:…	Broadcast	ARP	42	Who has 172.16.79.210? Tell 172.16.75.215
476	18.125503	CloudNetwork_78:96:…	Broadcast	ARP	42	Who has 172.16.78.77? Tell 172.16.75.213
493	19.085671	CloudNetwork_78:96:…	Broadcast	ARP	42	Who has 172.16.78.77? Tell 172.16.75.213
654	26.214200	CloudNetwork_78:96:…	Broadcast	ARP	42	Who has 172.16.78.77? Tell 172.16.75.213

```
> Frame 654: 42 bytes on wire (336 bits), 42 bytes captured (336 bits
v Ethernet II, Src: CloudNetwork_78:96:87 (4c:82:a9:78:96:87), Dst: B
   > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
   > Source: CloudNetwork_78:96:87 (4c:82:a9:78:96:87)
     Type: ARP (0x0806)
     [Stream index: 56]
> Address Resolution Protocol (request)
```

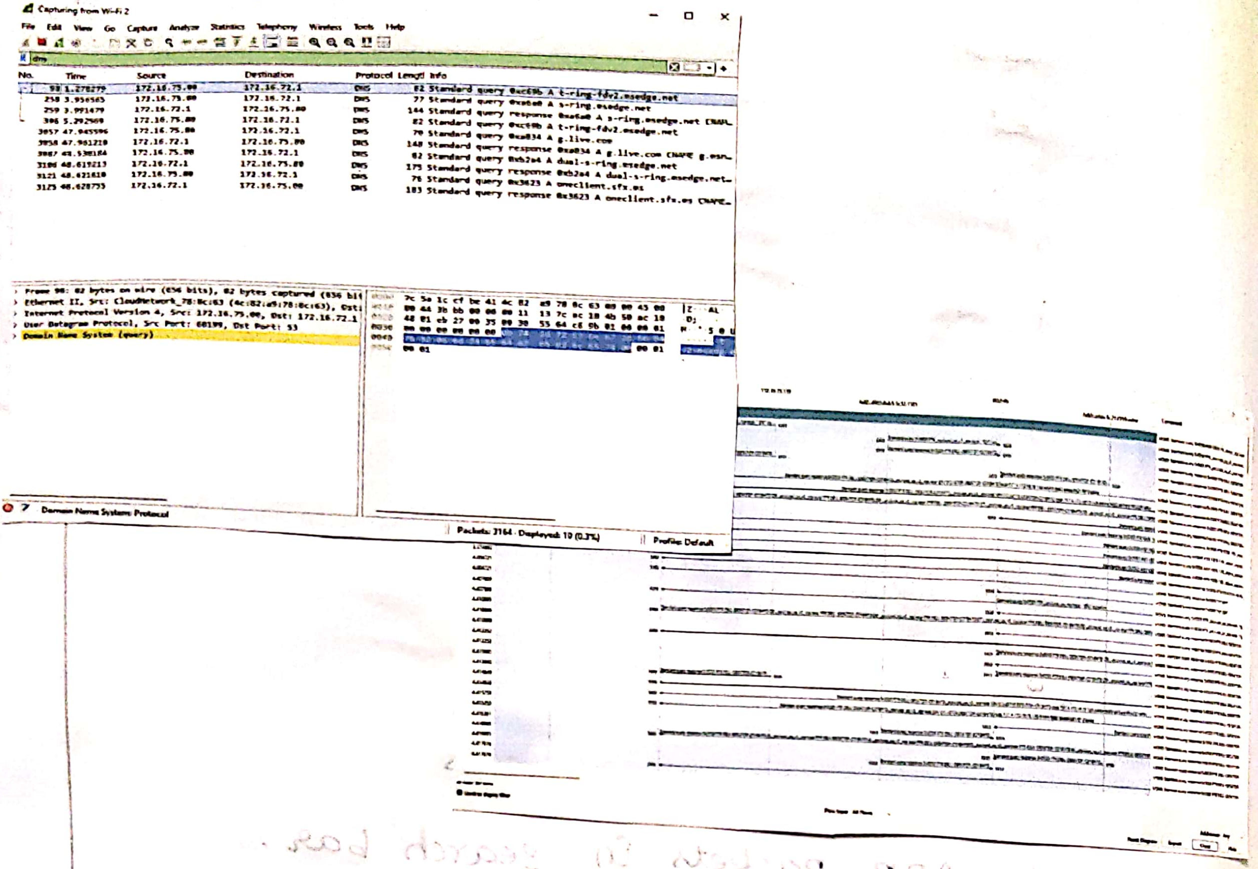
```
0000  ff ff ff ff ff ff 4c 82  a9 78 96 87 08 06 00 01
0010  08 00 06 04 00 01 4c 82  a9 78 96 87 ac 10 4b d5
0020  00 00 00 00 00 00 ac 10  4e 4d
```

Address Resolution Protocol: Protocol

Packets: 836 · Displayed: 20 (2.4%) · Dropped: 0 (0.0%) | Profile: Default

3. Filter to display only DNS packets.

- Search DNS packets in search bar.



Capturing from Wi-Fi 2

dns

```
No.   Time       Source        Destination   Protocol Length Info
  98 1.278279   172.16.75.00  172.16.72.1   DNS   82 Standard query 0xc69b A t-ring-fdv2.msedge.net
 258 3.956565   172.16.75.00  172.16.72.1   DNS   77 Standard query 0xa6a0 A s-ring.msedge.net
 259 3.991479   172.16.72.1   172.16.75.00  DNS  144 Standard query response 0xa6a0 A s-ring.msedge.net CNAM…
 306 5.292569   172.16.75.00  172.16.72.1   DNS   82 Standard query 0xc69b A t-ring-fdv2.msedge.net
3057 47.945596  172.16.75.00  172.16.72.1   DNS   70 Standard query 0xa834 A g.live.com
3058 47.961210  172.16.72.1   172.16.75.00  DNS  148 Standard query response 0xa834 A g.live.com CNAME g.msn…
3087 48.538184  172.16.75.00  172.16.72.1   DNS   82 Standard query 0xb2a4 A dual-s-ring.msedge.net
3108 48.619213  172.16.72.1   172.16.75.00  DNS  175 Standard query response 0xb2a4 A dual-s-ring.msedge.net…
3121 48.621610  172.16.75.00  172.16.72.1   DNS   76 Standard query 0x3623 A oneclient.sfx.ms
3125 48.628755  172.16.72.1   172.16.75.00  DNS  183 Standard query response 0x3623 A oneclient.sfx.ms CNAME…
```

```
> Frame 98: 82 bytes on wire (656 bits), 82 bytes captured (656 bit
> Ethernet II, Src: CloudNetwork_78:8c:63 (4c:82:a9:78:8c:63), Dst:
> Internet Protocol Version 4, Src: 172.16.75.00, Dst: 172.16.72.1
> User Datagram Protocol, Src Port: 60199, Dst Port: 53
> Domain Name System (query)
```

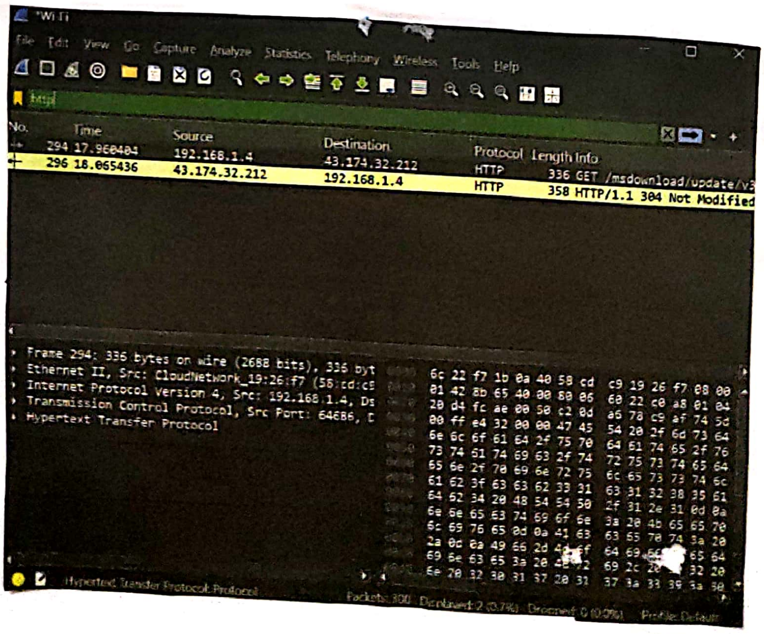
```
7c 5a 1c cf be 41 4c 82  a9 78 8c 63 08 00 45 00
00 44 3b bb 00 00 80 11  13 7c ac 10 4b 50 ac 10
48 01 eb 27 00 35 00 30  55 64 c6 9b 01 00 00 01
00 00 00 00 00 00
00 01
```

Domain Name System: Protocol

Packets: 3164 · Displayed: 10 (0.3%)   Profile: Default

4. Create a filter to display only HTTP packets

- Search HTTP packets in search bar
- Save the packets.



*Wi-Fi

http

```
No.   Time        Source         Destination    Protocol Length Info
 294 17.960404   192.168.1.4    43.174.32.212  HTTP   336 GET /msdownload/update/v3
 296 18.065436   43.174.32.212  192.168.1.4    HTTP   358 HTTP/1.1 304 Not Modified
```

```
> Frame 294: 336 bytes on wire (2688 bits), 336 byt
> Ethernet II, Src: CloudNetwork_19:26:f7 (58:cd:c9
> Internet Protocol Version 4, Src: 192.168.1.4, Ds
> Transmission Control Protocol, Src Port: 64686, D
> Hypertext Transfer Protocol
```

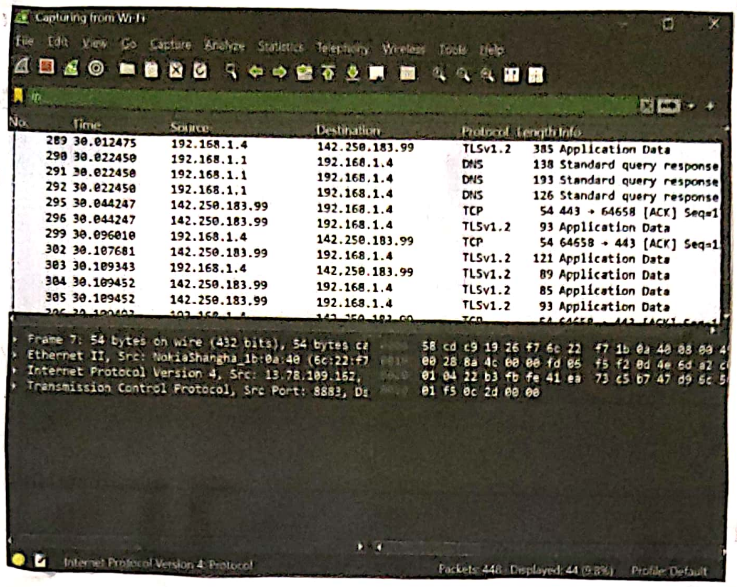
```
6c 22 f7 1b 0a 40 58 cd  c9 19 26 f7 08 00
01 42 8b 65 40 00 80 06  60 22 c0 a8 01 04
20 d4 fc ae 00 50 c2 0d  a6 78 c9 af 74 5d
00 ff e4 32 00 00 47 45  54 20 2f 6d 73 64
6e 6c 6f 61 64 2f 75 70  64 61 74 65 2f 76
73 74 61 74 69 63 2f 74  72 75 73 74 65 64
65 6e 2f 70 69 6e 72 75  6c 65 73 73 74 6c
61 62 3f 63 63 62 33 31  63 31 32 38 35 61
64 52 34 20 48 54 54 50  2f 31 2e 31 0d 0a
6e 6e 65 63 74 69 6f 6e  3a 20 4b 65 65 70
6c 69 76 65 0d 0a 41 63  63 65 70 74 3a 20
2a 0d 0a 49 66 2d 4d 6f  64 69 66 69 65 64
69 6e 63 65 3a 20 4e 72  69 2c 20 [illegible] 32 20
6e 20 32 30 31 37 20 31  37 3a 33 39 3a 30
```

Hypertext Transfer Protocol: Protocol

Packets: 300 · Displayed: 2 (0.7%) · Dropped: 0 (0.0%)   Profile: Default

5. Filter to display IP / ICMP packets

- Search ICMP / IP in search bar.



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

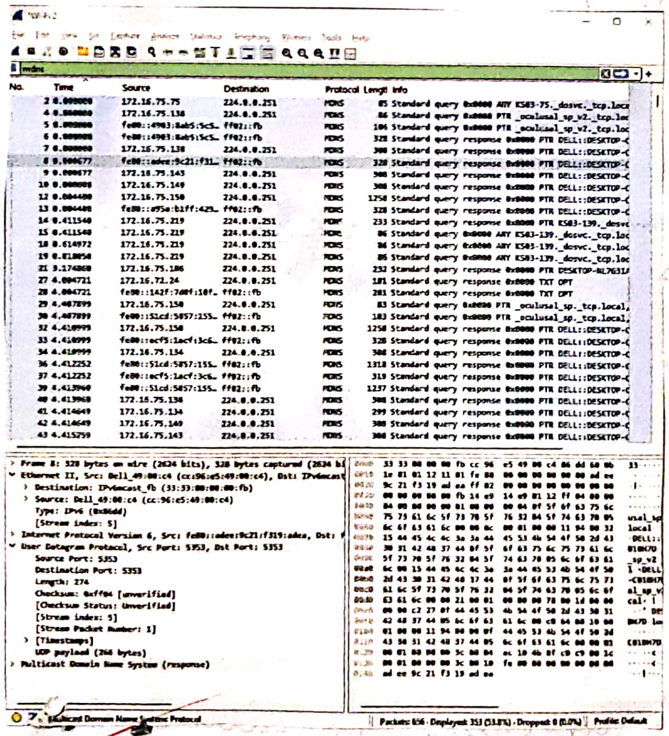
```
No.  Time       Source          Destination     Protocol Length Info
289 30.012475   192.168.1.4     142.250.183.99  TLSv1.2  385 Application Data
290 30.022450   192.168.1.1     192.168.1.4     DNS      138 Standard query response
291 30.022450   192.168.1.1     192.168.1.4     DNS      193 Standard query response
292 30.022450   192.168.1.1     192.168.1.4     DNS      126 Standard query response
295 30.044247   142.250.183.99  192.168.1.4     TCP       54 443 → 64658 [ACK] Seq=1
296 30.044247   142.250.183.99  192.168.1.4     TLSv1.2   93 Application Data
299 30.096010   192.168.1.4     142.250.183.99  TCP       54 64658 → 443 [ACK] Seq=1
302 30.107681   142.250.183.99  192.168.1.4     TLSv1.2  121 Application Data
303 30.109343   192.168.1.4     142.250.183.99  TLSv1.2   89 Application Data
304 30.109452   142.250.183.99  192.168.1.4     TLSv1.2   85 Application Data
305 30.109452   142.250.183.99  192.168.1.4     TLSv1.2   93 Application Data
```

```
> Frame 7: 54 bytes on wire (432 bits), 54 bytes ca      58 cd c9 19 26 f7 6c 22  f7 1b 0a 40 08 00 4
> Ethernet II, Src: NokiaShangha_1b:0a:40 (6c:22:f7      00 28 8a 4c 00 00 fd 05  f5 f2 0d 4e 6d a2 c
> Internet Protocol Version 4, Src: 13.78.109.152,       01 04 22 b3 fb fe 41 ea  73 c5 b7 47 d9 6c 5
> Transmission Control Protocol, Src Port: 8883, Ds      01 f5 0c 2d 00 00
```

Internet Protocol Version 4: Protocol

Packets: 448 · Displayed: 44 (9.8%) · Profile: Default

6. Filter no display only DHCP Packets.



*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
mdns

```
No. Time      Source                   Destination  Protocol Length Info
 2 0.000000   172.16.75.75             224.0.0.251  MDNS     85 Standard query 0x0000 ANY KS03-75._dosvc._tcp.loca
 4 0.000000   172.16.75.138            224.0.0.251  MDNS     86 Standard query 0x0000 PTR _oculusal_sp_v2._tcp.loc
 5 0.000000   fe80::4903:8ab5:5c5…     ff02::fb     MDNS    106 Standard query 0x0000 PTR _oculusal_sp_v2._tcp.loc
 6 0.000000   fe80::4903:8ab5:5c5…     ff02::fb     MDNS    328 Standard query response 0x0000 PTR DELL::DESKTOP-C
 7 0.000000   172.16.75.138            224.0.0.251  MDNS    308 Standard query response 0x0000 PTR DELL::DESKTOP-C
 8 0.000677   fe80::adee:9c21:f31…     ff02::fb     MDNS    328 Standard query response 0x0000 PTR DELL::DESKTOP-C
 9 0.000677   172.16.75.143            224.0.0.251  MDNS    308 Standard query response 0x0000 PTR DELL::DESKTOP-C
10 0.000000   172.16.75.149            224.0.0.251  MDNS    308 Standard query response 0x0000 PTR DELL::DESKTOP-C
12 0.004400   172.16.75.150            224.0.0.251  MDNS   1258 Standard query response 0x0000 PTR DELL::DESKTOP-C
13 0.004400   fe80::a95a:b1ff:429…     ff02::fb     MDNS    328 Standard query response 0x0000 PTR DELL::DESKTOP-C
14 0.411540   172.16.75.219            224.0.0.251  MDNS    233 Standard query response 0x0000 PTR KS03-139._desvc
15 0.411540   172.16.75.219            224.0.0.251  MDNS     86 Standard query 0x0000 ANY KS03-139._dosvc._tcp.loc
18 0.614972   172.16.75.219            224.0.0.251  MDNS     86 Standard query 0x0000 ANY KS03-139._dosvc._tcp.loc
19 0.818050   172.16.75.219            224.0.0.251  MDNS     86 Standard query 0x0000 ANY KS03-139._dosvc._tcp.loc
21 3.174860   172.16.75.186            224.0.0.251  MDNS    232 Standard query response 0x0000 PTR DESKTOP-NL7631A
27 4.004721   172.16.72.24             224.0.0.251  MDNS    181 Standard query response 0x0000 TXT OPT
28 4.004721   fe80::142f:7d0f:10f…     ff02::fb     MDNS    201 Standard query response 0x0000 TXT OPT
29 4.407899   172.16.75.150            224.0.0.251  MDNS     83 Standard query 0x0000 PTR _oculusal_sp._tcp.local,
30 4.407899   fe80::51cd:5857:155…     ff02::fb     MDNS    103 Standard query 0x0000 PTR _oculusal_sp._tcp.local,
32 4.410999   172.16.75.150            224.0.0.251  MDNS   1258 Standard query response 0x0000 PTR DELL::DESKTOP-C
33 4.410999   fe80::ecf5:1acf:3c6…     ff02::fb     MDNS    328 Standard query response 0x0000 PTR DELL::DESKTOP-C
34 4.410999   172.16.75.134            224.0.0.251  MDNS    308 Standard query response 0x0000 PTR DELL::DESKTOP-C
36 4.412252   fe80::51cd:5857:155…     ff02::fb     MDNS   1318 Standard query response 0x0000 PTR DELL::DESKTOP-C
37 4.412252   fe80::ecf5:1acf:3c6…     ff02::fb     MDNS    319 Standard query response 0x0000 PTR DELL::DESKTOP-C
39 4.413960   fe80::51cd:5857:155…     ff02::fb     MDNS   1237 Standard query response 0x0000 PTR DELL::DESKTOP-C
40 4.413960   172.15.75.138            224.0.0.251  MDNS    308 Standard query response 0x0000 PTR DELL::DESKTOP-C
41 4.414649   172.16.75.134            224.0.0.251  MDNS    299 Standard query response 0x0000 PTR DELL::DESKTOP-C
42 4.414649   172.16.75.140            224.0.0.251  MDNS    308 Standard query response 0x0000 PTR DELL::DESKTOP-C
43 4.415259   172.16.75.143            224.0.0.251  MDNS    308 Standard query response 0x0000 PTR DELL::DESKTOP-C
```

```
> Frame 8: 328 bytes on wire (2624 bits), 328 bytes captured (2624 bi
v Ethernet II, Src: Dell_49:00:c4 (cc:96:e5:49:00:c4), Dst: IPv6mcast
   > Destination: IPv6mcast_fb (33:33:00:00:00:fb)
   > Source: Dell_49:00:c4 (cc:96:e5:49:00:c4)
     Type: IPv6 (0x86dd)
     [Stream index: 5]
> Internet Protocol Version 6, Src: fe80::adee:9c21:f319:adea, Dst: f
v User Datagram Protocol, Src Port: 5353, Dst Port: 5353
     Source Port: 5353
     Destination Port: 5353
     Length: 274
     Checksum: 0xff04 [unverified]
     [Checksum Status: Unverified]
     [Stream index: 5]
     [Stream Packet Number: 1]
   > [Timestamps]
     UDP payload (266 bytes)
> Multicast Domain Name System (response)
```

```
0000  33 33 00 00 00 fb cc 96  e5 49 00 c4 86 dd 60 0b   33······
0010  1e 01 01 12 11 01 fe 80  00 00 00 00 00 00 ad ee   ········
0020  9c 21 f3 19 ad ea ff 02  00 00 00 00 00 00 00 00   ·!······
0030  00 00 00 00 00 fb 14 e9  14 e9 01 12 ff 04 00 00   ········
0040  04 00 00 00 00 01 00 00  00 04 0f 5f 6f 63 75 6c   ········
0050  75 73 61 6c 5f 73 70 5f  76 32 04 5f 74 63 70 05   usal_sp
0060  6c 6f 63 61 6c 00 00 0c  00 01 00 00 11 94 00 32   local
0070  15 44 45 4c 4c 3a 3a 44  45 53 4b 54 4f 50 2d 43   ·DELL::
0080  30 31 42 48 37 44 0f 5f  6f 63 75 6c 75 73 61 6c   01BH7D
0090  5f 73 70 5f 76 32 04 5f  74 63 70 05 6c 6f 63 61   _sp_v2
00a0  6c 00 15 44 45 4c 4c 3a  3a 44 45 53 4b 54 4f 50   l ·DELL
00b0  2d 43 30 31 42 48 37 44  0f 5f 6f 63 75 6c 75 73   -C01BH7
00c0  61 6c 5f 73 70 5f 76 32  04 5f 74 63 70 05 6c 6f   al_sp_v
00d0  63 61 6c 00 00 21 00 01  00 00 00 78 00 1d 00 00   cal· !
00e0  00 00 c2 27 0f 44 45 53  4b 54 4f 50 2d 43 30 31   ··' DE
00f0  42 48 37 44 05 6c 6f 63  61 6c 00 c0 64 00 10 00   BH7D lo
0100  01 00 00 11 94 00 00 0f  44 45 53 4b 54 4f 50 2d   ········
0110  43 30 31 42 48 37 44 05  6c 6f 63 61 6c 00 00 01   C01BH7D
0120  00 01 00 00 00 3c 00 04  ac 10 4b 8f c0 c9 00 1c   ·····<
0130  00 01 00 00 00 3c 00 10  fe 00 00 00 00 00 00 00   ·····<
0140  ad ee 9c 21 f3 19 ad ea                            ··!···
```

Multicast Domain Name System Protocol

Packets: 656 · Displayed: 353 (53.8%) · Dropped: 0 (0.0%) · Profile: Default

Student Observation :

1) what is promiscous mode ?

It is a network interface mode in which a network card captures all the network packets regardless of their destination MAC address.

2) Does ARP header have transport layer header

Ans) No ARP is a part of Network layer.

3) which transport layer protocol is used by DNS ?

DNS uses both : UDP and TCP.

4) what is the port number used by HTTP protocol ?

Ans) Port 80.

5) what is broadcast IP address ?

Ans) It is used to send data to all host on specific network segments.

Result : The Experiments on Packet capture tool: wireshark is carried out.

7/9/18