9/8/24 Practical - 5

Aim:

Experiment on packet capture tool: wire shark.

Packet sniffer:-

* sniffs messages being sent/received from/by your computer.

* store and display the contents of the various protocol fields in the messages

* Passive program

→ never sends packets itself

→ no packet addressed to it

→ receives a copy of all packets.

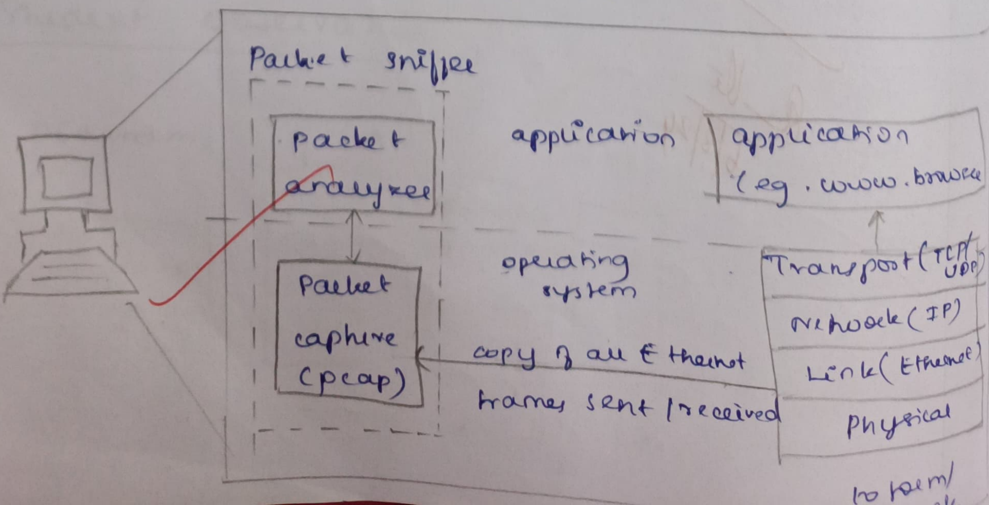
Packet sniffer structure Diagnostic Tools:

* Tcp dump

- Eg: tcpdump -enx host 10.129.41.2 · wexe3.out

* wire shark

- wireshark -r exe 3.out



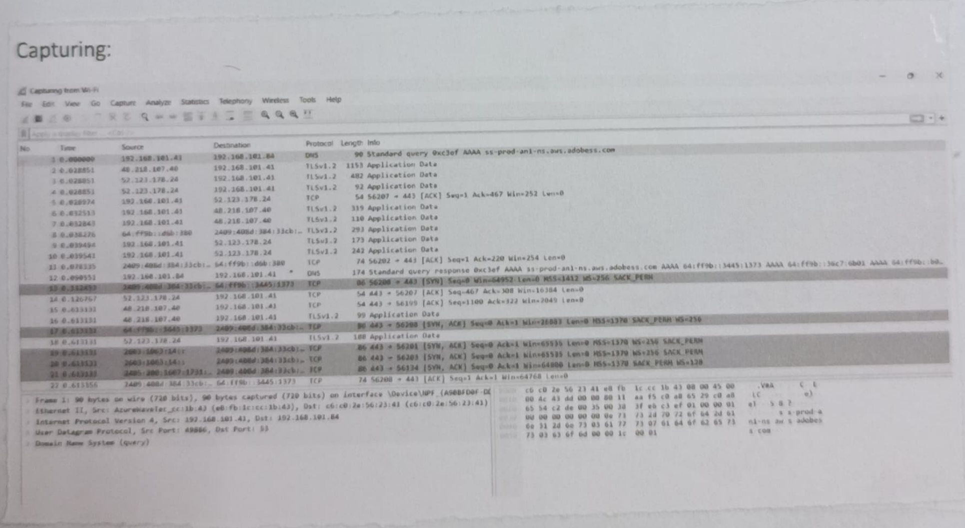
Capturing network traffic:

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

Procedure:

1) select Local Area connection in wireshark
2) Go to capture → option
3) select stop capture automatically after 100 packets
4) save the packets.

Output:



Capturing:

Capturing from 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
   1 0.000000   192.168.101.41       192.168.101.84       DNS        90 Standard query 0xc3ef AAAA ss-prod-an1-ns.aws.adobess.com
   2 0.028851   48.218.107.40        192.168.101.41       TLSv1.2  1153 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   110 Application Data
   8 0.038276   64:ff9b::d6b:380     2409:408d:384:33cb:… TLSv1.2   293 Application Data
   9 0.039494   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
  11 0.078335   2409:408d:384:33cb:… 64:ff9b::d6b:380     TCP        74 56202 → 443 [ACK] Seq=1 Ack=220 Win=254 Len=0
  12 0.090551   192.168.101.84       192.168.101.41       DNS       174 Standard query response 0xc3ef AAAA ss-prod-an1-ns.aws.adobess.com AAAA 64:ff9b::3445:1373 AAAA 64:ff9b::36c7:6b01 AAAA 64:ff9b::b0…
  13 0.112453   2409:408d:384:33cb:… 64:ff9b::3445:1373   TCP        86 56208 → 443 [SYN] Seq=0 Win=64952 Len=0 MSS=1412 WS=256 SACK_PERM
  14 0.126767   52.123.178.24        192.168.101.41       TCP        54 443 → 56207 [ACK] Seq=467 Ack=308 Win=16384 Len=0
  15 0.613131   48.218.107.40        192.168.101.41       TCP        54 443 → 56199 [ACK] Seq=1100 Ack=322 Win=2049 Len=0
  16 0.613131   48.218.107.40        192.168.101.41       TLSv1.2    99 Application Data
  17 0.613131   64:ff9b::3445:1373   2409:408d:384:33cb:… TCP        90 443 → 56208 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1370 SACK_PERM WS=256
  18 0.613131   52.123.178.24        192.168.101.41       TLSv1.2   108 Application Data
  19 0.613131   2603:1063:14::       2409:408d:384:33cb:… TCP        86 443 → 56201 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1370 WS=256 SACK_PERM
  20 0.613131   2603:1063:14::       2409:408d:384:33cb:… TCP        86 443 → 56203 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1370 WS=256 SACK_PERM
  21 0.613131   2405:200:1607:1731:… 2409:408d:384:33cb:… TCP        86 443 → 56134 [SYN, ACK] Seq=0 Ack=1 Win=64800 Len=0 MSS=1370 SACK_PERM WS=128
  22 0.613356   2409:408d:384:33cb:… 64:ff9b::3445:1373   TCP        74 56208 → 443 [ACK] Seq=1 Ack=1 Win=64768 Len=0
```

```
> Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{A9BBFD0F-DC
> Ethernet II, Src: AzureWaveTec_cc:1b:43 (e8:fb:1c:cc:1b:43), Dst: c6:c0:2e:56:23:41 (c6:c0:2e:56:23:41)
> Internet Protocol Version 4, Src: 192.168.101.41, Dst: 192.168.101.84
> User Datagram Protocol, Src Port: 49886, Dst Port: 53
> Domain Name System (query)
```

```
c6 c0 2e 56 23 41 e8 fb  1c cc 1b 43 08 00 45 00   ..V#A     C  E
00 4c 43 dd 00 00 80 11  aa f5 c0 a8 65 29 c0 a8   LC          e)
65 54 c2 de 00 35 00 38  3f eb c3 ef 01 00 00 01   eT   5 8 ?
00 00 00 00 00 00 0e 73  73 2d 70 72 6f 64 2d 61          s s-prod-a
6e 31 2d 6e 73 03 61 77  73 07 61 64 6f 62 65 73   n1-ns aw s adobes
73 03 63 6f 6d 00 00 1c  00 01                     s com
```

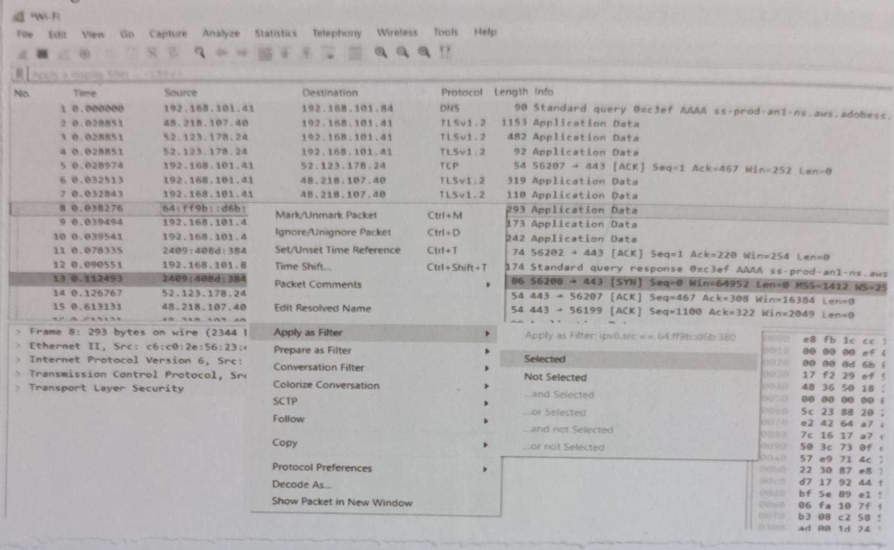
Filtering packets:

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). We can also apply filter by selecting the packet →

Apply as Filter → selected.

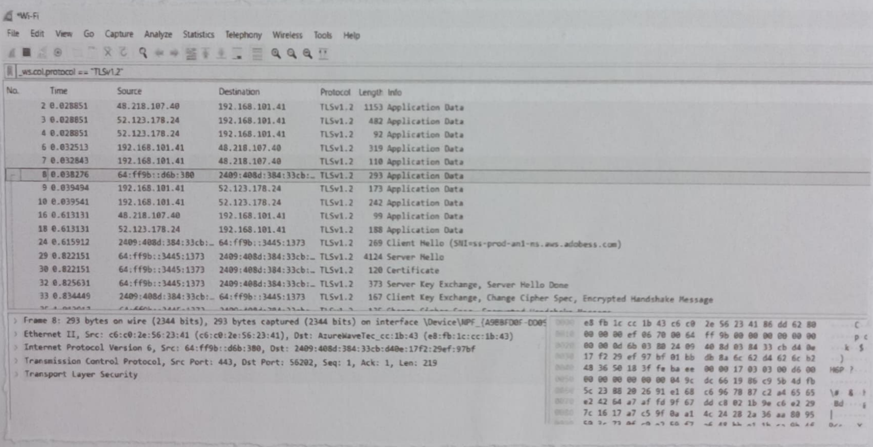
Output:

Filtering:



```
*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
    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   1153 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    110 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 l
> Ethernet II, Src: c6:c0:2e:56:23:4
> Internet Protocol Version 6, Src:
> Transmission Control Protocol, Sr
> Transport Layer Security
```

```
e8 fb 1c cc
00 00 00 ef
00 00 0d 6b
17 f2 29 ef
48 36 50 18
00 00 00 00
5c 23 88 20
e2 42 64 a7
7c 16 17 a7
50 3c 73 0f
57 e9 71 4c
22 30 87 e8
d7 17 92 44
bf 5e 89 e1
06 fa 10 7f
b3 08 c2 58
ad 00 1d 24
```



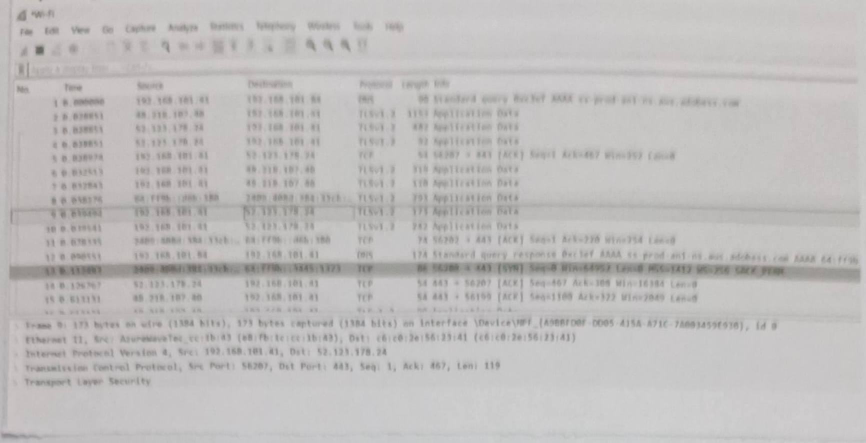
```
*Wi-Fi
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
_ws.col.protocol == "TLSv1.2"

No.   Time        Source                 Destination            Protocol  Length Info
    2 0.028851    48.218.107.40          192.168.101.41         TLSv1.2   1153 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
    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    110 Application Data
    8 0.038276    64:ff9b::d6b:380       2409:408d:384:33cb:…   TLSv1.2    293 Application Data
    9 0.039494    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
   16 0.613131    48.218.107.40          192.168.101.41         TLSv1.2     99 Application Data
   18 0.613131    52.123.178.24          192.168.101.41         TLSv1.2    188 Application Data
   24 0.615912    2409:408d:384:33cb:…   64:ff9b::3445:1373     TLSv1.2    269 Client Hello (SNI=ss-prod-an1-ns.aws.adobess.com)
   29 0.822151    64:ff9b::3445:1373     2409:408d:384:33cb:…   TLSv1.2   4124 Server Hello
   30 0.822151    64:ff9b::3445:1373     2409:408d:384:33cb:…   TLSv1.2    120 Certificate
   32 0.825631    64:ff9b::3445:1373     2409:408d:384:33cb:…   TLSv1.2    373 Server Key Exchange, Server Hello Done
   33 0.834449    2409:408d:384:33cb:…   64:ff9b::3445:1373     TLSv1.2    167 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_{A9BBFD0F-DD05
> 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:17f2:29ef:97bf
> Transmission Control Protocol, Src Port: 443, Dst Port: 56202, Seq: 1, Ack: 1, Len: 219
> Transport Layer Security

e8 fb 1c cc 1b 43 c6 c0  2e 56 23 41 86 dd 62 80
00 00 00 ef 06 70 00 64  ff 9b 00 00 00 00 00 00
00 00 0d 6b 03 80 24 09  40 8d 03 84 33 cb d4 0e
17 f2 29 ef 97 bf 01 bb  db 8a 6c 62 d4 62 6c b2
48 36 50 18 3f fe ba ee  00 00 17 03 03 00 d6 00
00 00 00 00 00 00 04 9c  dc 66 19 86 c9 5b 4d fb
5c 23 88 20 26 91 e1 68  c6 96 78 87 c2 a4 65 65
e2 42 64 a7 af fd 9f 67  dd c8 02 1b 9e c6 e2 29
7c 16 17 a7 c5 9f 0a a1  4c 24 28 2a 36 aa 80 95
```

Inspecting packets:

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

Output:

Inspecting:



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

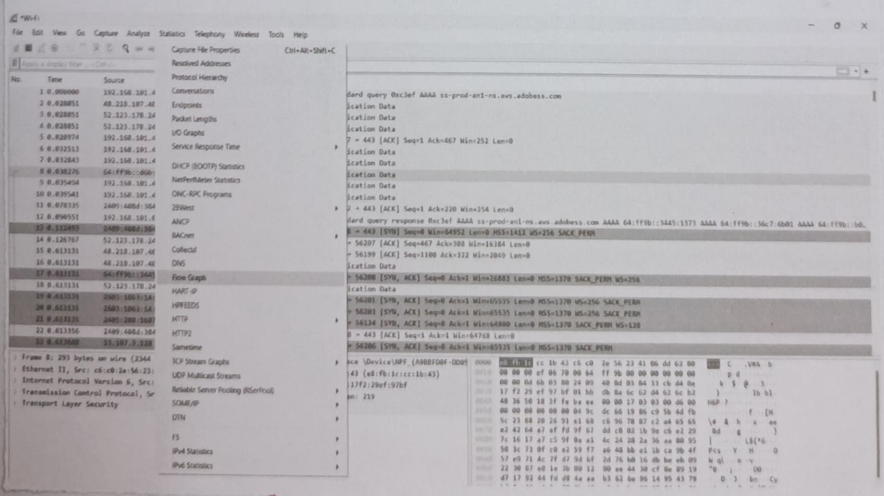
```
No.   Time        Source                Destination           Protocol Length Info
    1 0.000000    192.168.101.41        192.168.101.84        DNS        98 Standard query 0xc3ef AAAA ss-prod-an1-ns.aws.adobess.com
    2 0.028851    48.218.107.40         192.168.101.41        TLSv1.2  1151 Application 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   110 Application Data
    8 0.038276    64:ff9b::d6b:380      2409:4084:384:33cb:…  TLSv1.2   293 Application Data
    9 0.039494    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
   11 0.078335    2409:4084:384:33cb:…  64:ff9b::d6b:380      TCP        74 56202 → 443 [ACK] Seq=1 Ack=220 Win=254 Len=0
   12 0.090551    192.168.101.84        192.168.101.41        DNS       174 Standard query response 0xc3ef AAAA ss-prod-an1-ns.aws.adobess.com AAAA 64:ff9b
   13 0.112493    2409:4084:384:33cb:…  64:ff9b::3445:1373    TCP        86 56208 → 443 [SYN] Seq=0 Win=64952 Len=0 MSS=1412 WS=256 SACK_PERM
   14 0.126767    52.123.178.24         192.168.101.41        TCP        54 443 → 56207 [ACK] Seq=467 Ack=308 Win=16384 Len=0
   15 0.613131    48.218.107.40         192.168.101.41        TCP        54 443 → 56199 [ACK] Seq=1100 Ack=322 Win=2049 Len=0

> Frame 9: 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits) on interface \Device\NPF_{A9BBFD0F-DD05-415A-A71C-7A003459E930}, id 0
> Ethernet II, Src: AzureWaveTec_cc:1b:43 (e8:fb:1c:cc:1b:43), Dst: c6:c0:2e:56:23:41 (c6:c0:2e:56:23:41)
> Internet Protocol Version 4, Src: 192.168.101.41, Dst: 52.123.178.24
> Transmission Control Protocol, Src Port: 56207, Dst Port: 443, Seq: 1, Ack: 467, Len: 119
> Transport Layer Security
```

Flow graph:

we can see the flow graph of the packets by clicking on the statistics and selecting the flow graph and it displays the flow graph of the packets.

Output:

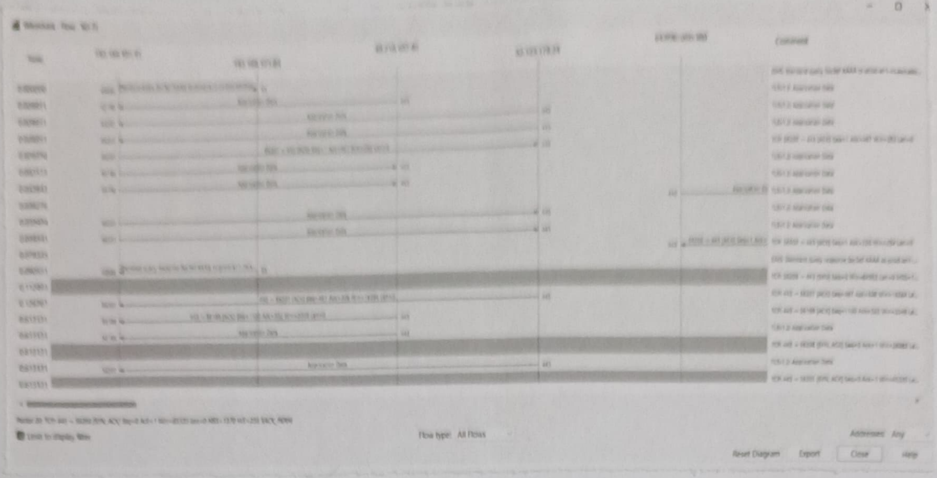
Flow graph:



```
No.   Time        Source
    1 0.000000    192.168.101.4
    2 0.028851    48.218.107.4E
    3 0.028851    52.123.178.24
    4 0.028851    52.123.178.24
    5 0.028974    192.168.101.4
    6 0.032513    192.168.101.4
    7 0.032843    192.168.101.4
    8 0.038276    64:ff9b::d6b:
    9 0.039494    192.168.101.4
   10 0.039541    192.168.101.4
   11 0.078335    2409:4084:384
   12 0.090551    192.168.101.€
   13 0.112493    2409:4084:384
   14 0.126767    52.123.178.24
   15 0.613131    48.218.107.4E
   16 0.613131    48.218.107.4E
   17 0.613131    64:ff9b::3445
   18 0.613131    52.123.178.24
   19 0.613131    2603:1063:14:
   20 0.613131    2603:1063:14:
   21 0.613131    2405:200:1607
   22 0.613356    2409:4084:384
   23 0.613608    13.107.3.128

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

```
dard query 0xc3ef AAAA ss-prod-an1-ns.aws.adobess.com
ication Data
ication Data
ication Data
7 → 443 [ACK] Seq=1 Ack=467 Win=252 Len=0
ication Data
ication Data
ication Data
ication Data
ication Data
2 → 443 [ACK] Seq=1 Ack=220 Win=254 Len=0
dard query response 0xc3ef AAAA ss-prod-an1-ns.aws.adobess.com AAAA 64:ff9b::3445:1373 AAAA 64:ff9b::36c7:6b01 AAAA 64:ff9b::b0…
8 → 443 [SYN] Seq=0 Win=64952 Len=0 MSS=1412 WS=256 SACK_PERM
→ 56207 [ACK] Seq=467 Ack=308 Win=16384 Len=0
→ 56199 [ACK] Seq=1100 Ack=322 Win=2049 Len=0
ication Data
→ 56208 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1370 SACK_PERM WS=256
ication Data
→ 56201 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1370 WS=256 SACK_PERM
→ 56203 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1370 WS=256 SACK_PERM
→ 56134 [SYN, ACK] Seq=0 Ack=1 Win=64800 Len=0 MSS=1370 SACK_PERM WS=128
8 → 443 [ACK] Seq=1 Ack=1 Win=64768 Len=0
→ 56206 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1370 SACK_PERM

ace \Device\NPF_{A9BBFD0F-DD05
43 (e8:fb:1c:cc:1b:43)
17f2:29ef:97bf
en: 219
```

```
0000  e8 fb 1c cc 1b 43 c6 c0  2e 56 23 41 86 dd 62 80   ...C  .V#A  b
0010  00 00 00 ef 06 70 00 64  ff 9b 00 00 00 00 00 00       p d
0020  00 00 0d 6b 03 80 24 09  40 8d 03 84 33 cb d4 0e     k  $ @  3
0030  17 f2 29 ef 97 bf 01 bb  db 8a 6c 62 d4 62 6c b2    )       lb bl
0040  48 36 50 18 3f fe ba ee  00 00 17 03 03 00 d6 00   H6P ?
0050  00 00 00 00 00 00 04 9c  dc 66 19 86 c9 5b 4d fb           f  [M
0060  5c 23 88 20 26 91 e1 68  c6 96 78 87 c2 a4 65 65   \#  & h   x   ee
0070  e2 42 64 a7 af fd 9f 67  dd c8 02 1b 9e c6 e2 29    Bd    g        )
0080  7c 16 17 a7 c5 9f 0a a1  4c 24 28 2a 36 aa 80 95   |        L$(*6
0090  50 3c 73 0f c0 e2 59 f7  a6 48 bb e1 1b ca 9b 4f   P<s   Y   H     O
00a0  57 e9 71 4c 7f d7 9d 6f  2d 76 b0 16 db be eb 09   W qL   o -v
00b0  22 30 87 e0 1e 3b 00 12  80 ae 44 30 cf 8e 89 19   "0   ;    D0
00c0  d7 17 92 44 fd d8 4a aa  b3 62 6e 96 14 95 43 79      D  J  bn  Cy
```



Create a Filter to display only DNS packets and provide the flow graph

Procedure:

→ Go to capture → option

→ select stop capture automatically after 100 packets

→ Then click start capture.

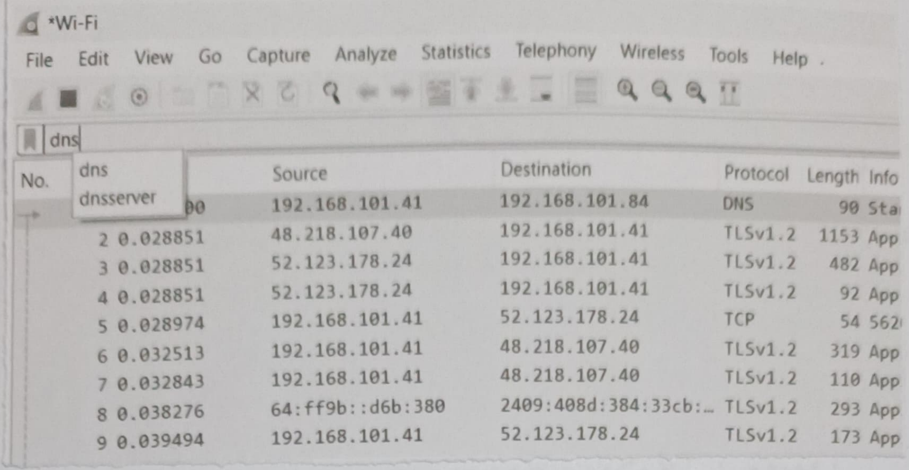
→ search DNS packets in search bar.

→ To see flow graph click statistics → Flow Graph.

→ Save the packets.

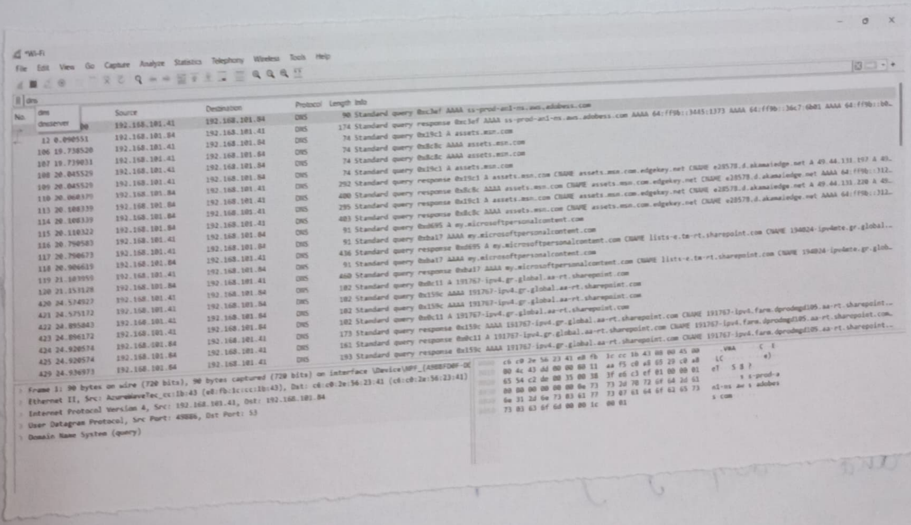
Capturing and Filtering:

For DNS:


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

No.	Source	Destination	Protocol	Length	Info
00	192.168.101.41	192.168.101.84	DNS	90	Sta
2 0.028851	48.218.107.40	192.168.101.41	TLSv1.2	1153	App
3 0.028851	52.123.178.24	192.168.101.41	TLSv1.2	482	App
4 0.028851	52.123.178.24	192.168.101.41	TLSv1.2	92	App
5 0.028974	192.168.101.41	52.123.178.24	TCP	54	562
6 0.032513	192.168.101.41	48.218.107.40	TLSv1.2	319	App
7 0.032843	192.168.101.41	48.218.107.40	TLSv1.2	110	App
8 0.038276	64:ff9b::d6b:380	2409:408d:384:33cb:…	TLSv1.2	293	App
9 0.039494	192.168.101.41	52.123.178.24	TLSv1.2	173	App

Inspecting:

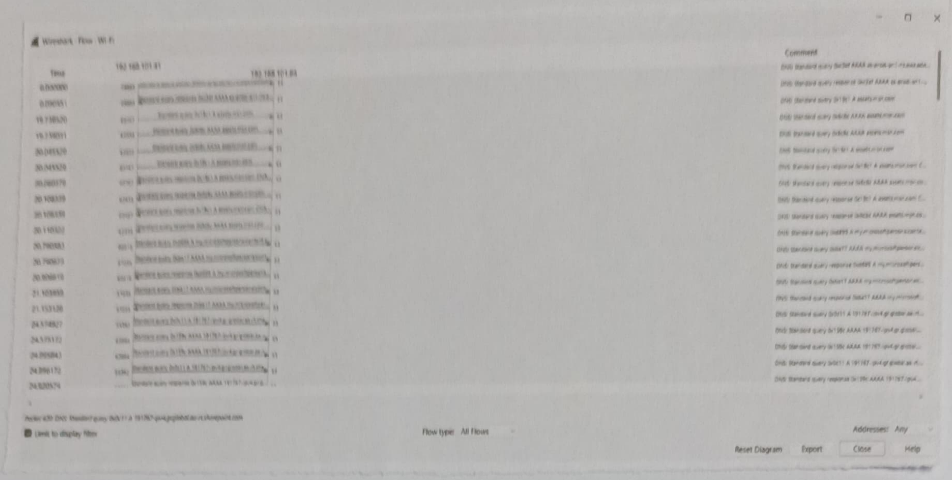

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
dns
dnsserver

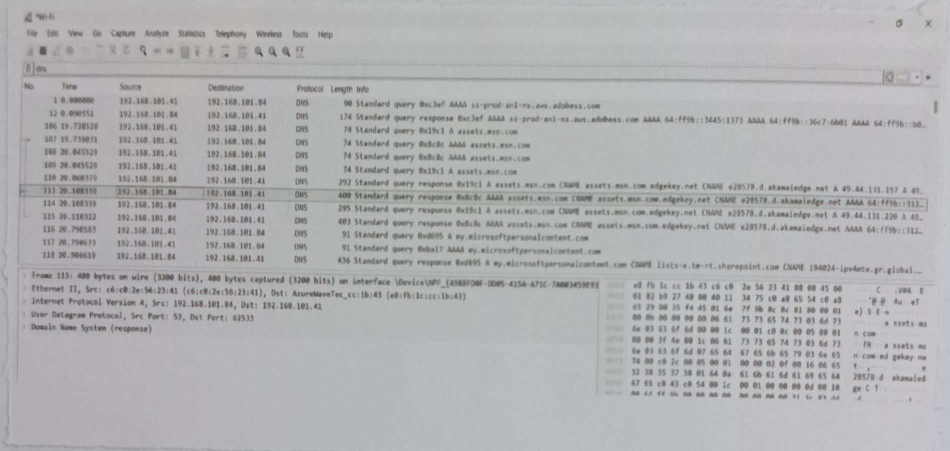
No.	Source	Destination	Protocol	Length	Info
00	192.168.101.41	192.168.101.84	DNS	90	Standard query 0xc3ef AAAA ss-prod-an1-ns.aws.adobess.com
12 0.090551	192.168.101.84	192.168.101.41	DNS	174	Standard query response 0xc3ef AAAA ss-prod-an1-ns.aws.adobess.com AAAA 64:ff9b::3445:1373 AAAA 64:ff9b::36c7:6b01 AAAA 64:ff9b::b0…
106 19.738520	192.168.101.41	192.168.101.84	DNS	74	Standard query 0x19c1 A assets.msn.com
107 19.739031	192.168.101.41	192.168.101.84	DNS	74	Standard query 0x8c8c AAAA assets.msn.com
108 20.045529	192.168.101.41	192.168.101.84	DNS	74	Standard query 0x8c8c AAAA assets.msn.com
109 20.045529	192.168.101.41	192.168.101.84	DNS	74	Standard query 0x19c1 A assets.msn.com
110 20.060375	192.168.101.84	192.168.101.41	DNS	292	Standard query response 0x19c1 A assets.msn.com CNAME assets.msn.com.edgekey.net CNAME e28578.d.akamaiedge.net A 49.44.131.197 A 49…
113 20.108339	192.168.101.84	192.168.101.41	DNS	400	Standard query response 0x8c8c AAAA assets.msn.com CNAME assets.msn.com.edgekey.net CNAME e28578.d.akamaiedge.net AAAA 64:ff9b::312…
114 20.108339	192.168.101.84	192.168.101.41	DNS	295	Standard query response 0x19c1 A assets.msn.com CNAME assets.msn.com.edgekey.net CNAME e28578.d.akamaiedge.net A 49.44.131.220 A 49…
115 20.110322	192.168.101.84	192.168.101.41	DNS	403	Standard query response 0x8c8c AAAA assets.msn.com CNAME assets.msn.com.edgekey.net CNAME e28578.d.akamaiedge.net AAAA 64:ff9b::312…
116 20.790583	192.168.101.41	192.168.101.84	DNS	91	Standard query 0xd695 A my.microsoftpersonalcontent.com
117 20.790673	192.168.101.41	192.168.101.84	DNS	91	Standard query 0xba17 AAAA my.microsoftpersonalcontent.com
118 20.906619	192.168.101.84	192.168.101.41	DNS	436	Standard query response 0xd695 A my.microsoftpersonalcontent.com CNAME lists-e.tm-rt.sharepoint.com CNAME 194024-ipv4mte.gr.global…
119 21.103959	192.168.101.41	192.168.101.84	DNS	91	Standard query 0xba17 AAAA my.microsoftpersonalcontent.com
120 21.153128	192.168.101.84	192.168.101.41	DNS	460	Standard query response 0xba17 AAAA my.microsoftpersonalcontent.com CNAME lists-e.tm-rt.sharepoint.com CNAME 194024-ipv4mte.gr.glob…
420 24.574927	192.168.101.41	192.168.101.84	DNS	102	Standard query 0x0c11 A 191767-ipv4.gr-global.aa-rt.sharepoint.com
421 24.575172	192.168.101.41	192.168.101.84	DNS	102	Standard query 0x159c AAAA 191767-ipv4.gr-global.aa-rt.sharepoint.com
422 24.895843	192.168.101.41	192.168.101.84	DNS	102	Standard query 0x159c AAAA 191767-ipv4.gr-global.aa-rt.sharepoint.com
423 24.896172	192.168.101.41	192.168.101.84	DNS	102	Standard query 0x0c11 A 191767-ipv4.gr-global.aa-rt.sharepoint.com
424 24.920574	192.168.101.84	192.168.101.41	DNS	173	Standard query response 0x159c AAAA 191767-ipv4.gr-global.aa-rt.sharepoint.com CNAME 191767-ipv4.farm.dprodmgd105.aa-rt.sharepoint…
425 24.920574	192.168.101.84	192.168.101.41	DNS	161	Standard query response 0x0c11 A 191767-ipv4.gr-global.aa-rt.sharepoint.com CNAME 191767-ipv4.farm.dprodmgd105.aa-rt.sharepoint.com…
429 24.936973	192.168.101.84	192.168.101.41	DNS	193	Standard query response 0x159c AAAA 191767-ipv4.gr-global.aa-rt.sharepoint.com CNAME 191767-ipv4.farm.dprodmgd105.aa-rt.sharepoint…

```
> Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{A9BBFD0F-DE
> Ethernet II, Src: AzureWaveTec_cc:1b:43 (e8:fb:1c:cc:1b:43), Dst: c6:c0:2e:56:23:41 (c6:c0:2e:56:23:41)
> Internet Protocol Version 4, Src: 192.168.101.41, Dst: 192.168.101.84
> User Datagram Protocol, Src Port: 49886, Dst Port: 53
> Domain Name System (query)
```

```
c6 c0 2e 56 23 41 e8 fb  1c cc 1b 43 08 00 45 00    .V#A     C  E
00 4c 43 dd 00 00 80 11  aa f5 c0 a8 65 29 c0 a8    LC         e)
65 54 c2 de 00 35 00 38  3f e6 c3 ef 01 00 00 01    eT   5 8 ?
00 00 00 00 00 00 0e 73  73 2d 70 72 6f 64 2d 61           s s-prod-a
6e 31 2d 6e 73 03 61 77  73 07 61 64 6f 62 65 73    n1-ns aw s adobes
73 03 63 6f 6d 00 00 1c  00 01                      s com
```

Flow graph:





```
dns
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.com
   12 0.090551    192.168.101.84    192.168.101.41    DNS      174 Standard query response 0xc3ef AAAA ss-prod-an1-ns.aws.adobess.com AAAA 64:ff9b::3445:1373 AAAA 64:ff9b::36c7:6b01 AAAA 64:ff9b::b0…
  106 19.738520   192.168.101.41    192.168.101.84    DNS       74 Standard query 0x19c1 A assets.msn.com
  107 19.739031   192.168.101.41    192.168.101.84    DNS       74 Standard query 0x8c8c AAAA assets.msn.com
  108 20.045529   192.168.101.41    192.168.101.84    DNS       74 Standard query 0x8c8c AAAA assets.msn.com
  109 20.045529   192.168.101.41    192.168.101.84    DNS       74 Standard query 0x19c1 A assets.msn.com
  110 20.060379   192.168.101.84    192.168.101.41    DNS      292 Standard query response 0x19c1 A assets.msn.com CNAME assets.msn.com.edgekey.net CNAME e28578.d.akamaiedge.net A 49.44.131.197 A 49…
  113 20.108330   192.168.101.84    192.168.101.41    DNS      400 Standard query response 0x8c8c AAAA assets.msn.com CNAME assets.msn.com.edgekey.net CNAME e28578.d.akamaiedge.net AAAA 64:ff9b::312…
  114 20.108339   192.168.101.84    192.168.101.41    DNS      295 Standard query response 0x19c1 A assets.msn.com CNAME assets.msn.com.edgekey.net CNAME e28578.d.akamaiedge.net A 49.44.131.220 A 49…
  115 20.110322   192.168.101.84    192.168.101.41    DNS      403 Standard query response 0x8c8c AAAA assets.msn.com CNAME assets.msn.com.edgekey.net CNAME e28578.d.akamaiedge.net AAAA 64:ff9b::312…
  116 20.790583   192.168.101.41    192.168.101.84    DNS       91 Standard query 0xd695 A my.microsoftpersonalcontent.com
  117 20.790673   192.168.101.41    192.168.101.84    DNS       91 Standard query 0xba17 AAAA my.microsoftpersonalcontent.com
  118 20.906619   192.168.101.84    192.168.101.41    DNS      436 Standard query response 0xd695 A my.microsoftpersonalcontent.com CNAME lists-e.tm-rt.sharepoint.com CNAME 194024-ipv4mte.gr.global…

> Frame 113: 400 bytes on wire (3200 bits), 400 bytes captured (3200 bits) on interface \Device\NPF_{A988FD0F-DD05-415A-A71C-7A003459E93
> 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 4, Src: 192.168.101.84, Dst: 192.168.101.41
> User Datagram Protocol, Src Port: 53, Dst Port: 62533
> Domain Name System (response)

e8 fb 1c cc 1b 43 c6 c0  2e 56 23 41 08 00 45 00   ·····C··.V#A··E·
01 82 b9 27 40 00 40 11  34 75 c0 a8 65 54 c0 a8   ···'@·@·4u··eT··
65 29 00 35 f4 45 01 6e  7f 9b 8c 8c 81 80 00 01   e)·5·E·n········
00 06 00 00 00 00 06 61  73 73 65 74 73 03 6d 73   ·······assets·ms
6e 03 63 6f 6d 00 00 1c  00 01 c0 0c 00 05 00 01   n·com···········
00 00 3f 4e 00 1c 06 61  73 73 65 74 73 03 6d 73   ··?N···assets·ms
6e 03 63 6f 6d 07 65 64  67 65 6b 65 79 03 6e 65   n·com·edgekey·ne
74 00 c0 2c 00 05 00 01  00 00 02 0f 00 16 06 65   t··,···········e
32 38 35 37 38 01 64 0a  61 6b 61 6d 61 69 65 64   28578·d·akamaied
67 65 c0 43 c0 54 00 1c  00 01 00 00 00 0d 00 10   ge·C·T··········
```

Result:

Thus, the experiments an packet capture tools like capturing, inspecting, filtering and displaying flow graph in wireshark is succesfully executed.

9/8/24