9/8/24 Practical - 5

Aim :

Experiments on packet capture tools : wireshark.

Packet shifter :

* shifts 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 packets addressed to it.

  - receives a copy of all packets.

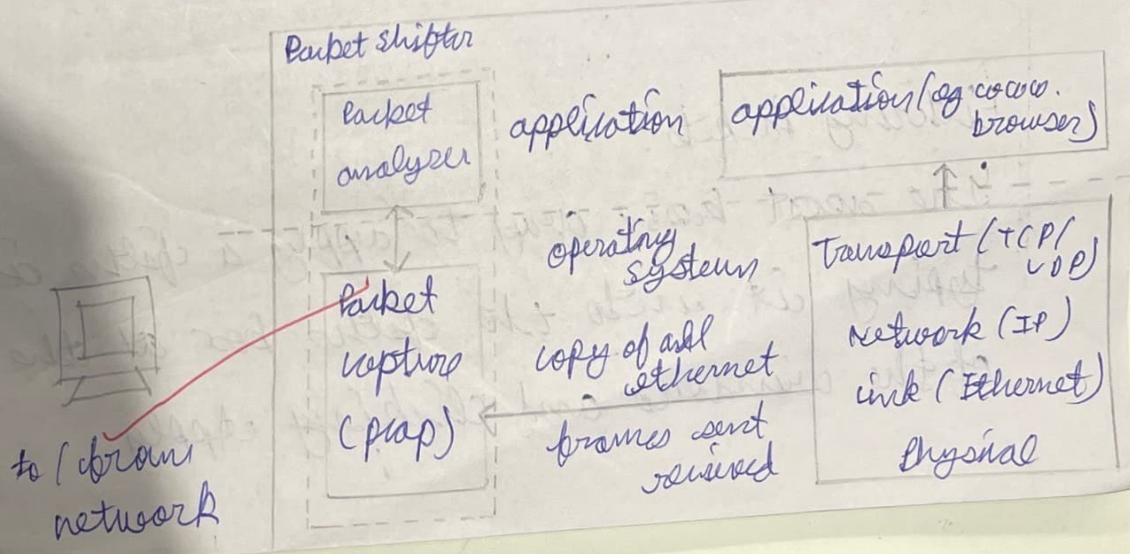
Packet sniffer structure Diagnostic tools :

* TCP dump :

  - Eg : tcpdump -enx host 10.129.41.2 - w exe 3.out

* wire shark

  - wireshark
  - wireshark - r exe 3.out



capturing Network Traffic :

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

Procedure :

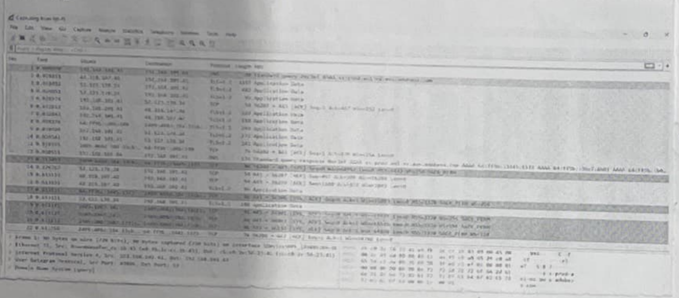
1) Select Local Area Connections in wireshark

2) Go to capture -> option

3) select stop capture automatically after 100 packets

4) Save the packets .

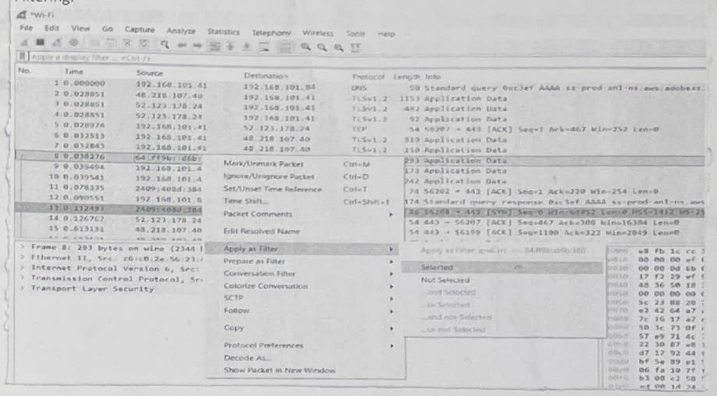
Capturing:



Filtering Packets :

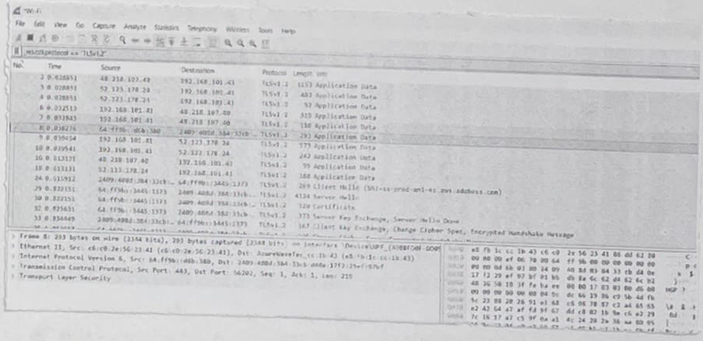
The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply .

Filtering:



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
Selected
Not Selected
...and Selected
...or Selected
...and not Selected
...or not Selected

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



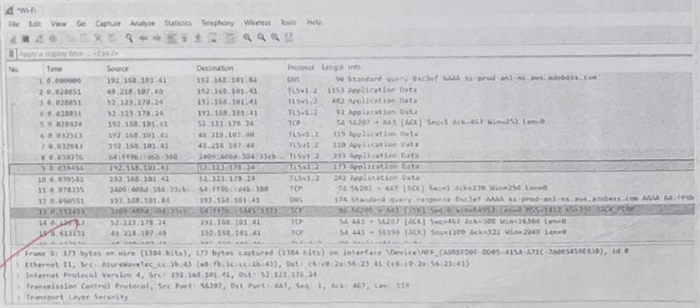
*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
_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 0.039454    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    95 Application Data
 18 0.613131    52.123.178.24           192.168.101.41          TLSv1.2   168 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  4134 Server Hello
 30 0.822151    64:ff9b::3445:1373      2409:408d:384:33cb...   TLSv1.2   128 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:d46e:1712:29ef:97bf
> Transmission Control Protocol, Src Port: 443, Dst Port: 56202, Seq: 1, Ack: 1, Len: 219
> Transport Layer Security
```

Inspecting Packets :

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

Inspecting:



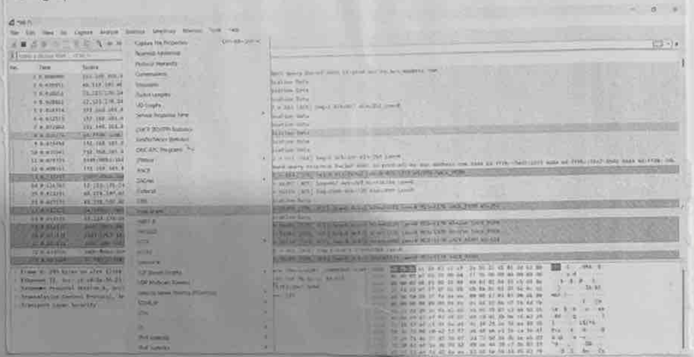
*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

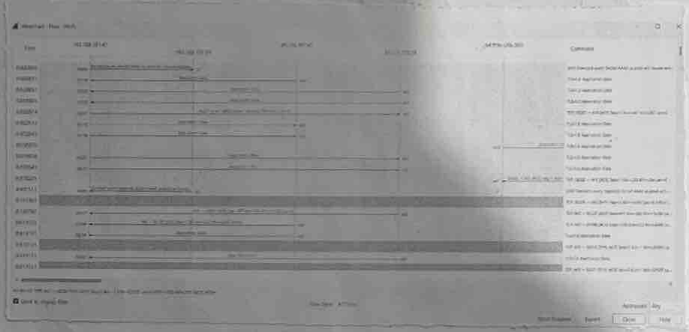
```
No.  Time        Source                  Destination             Protocol Length Info
  1 0.000000    192.168.101.41          192.168.101.84          DNS        90 Standard query 0xc3ef AAAA ss-prod-an1-ns.aws.adobess.com
  2 0.028851    48.218.107.40           192.168.101.41          TLSv1.2  1153 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
 13 0.112493    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

> Frame 9: 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits) on interface \Device\NPF_{A9BBFD0F-DD05-415A-A71C-7A005459E930}, 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.

Flow graph:





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

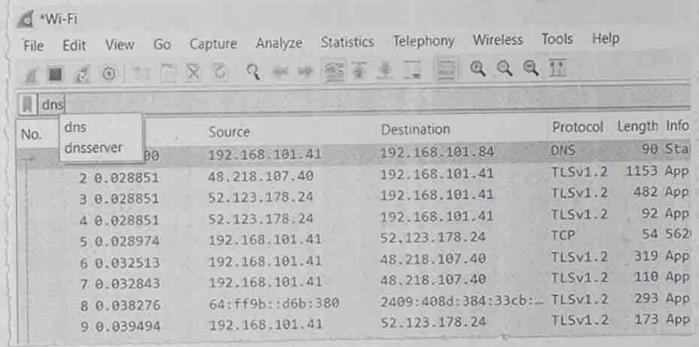
-> Search DNS packets in search bar

-> To see flow graph click statistics -> Flow graph.

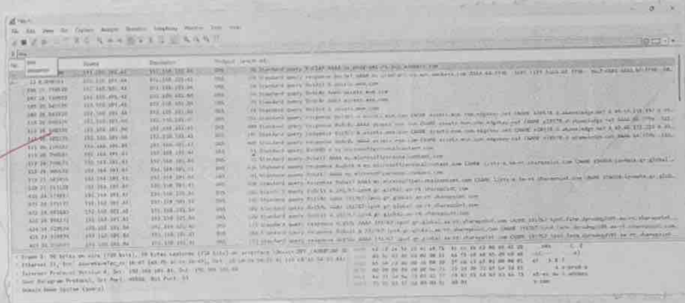
-> Save the packets.

Capturing and Filtering:

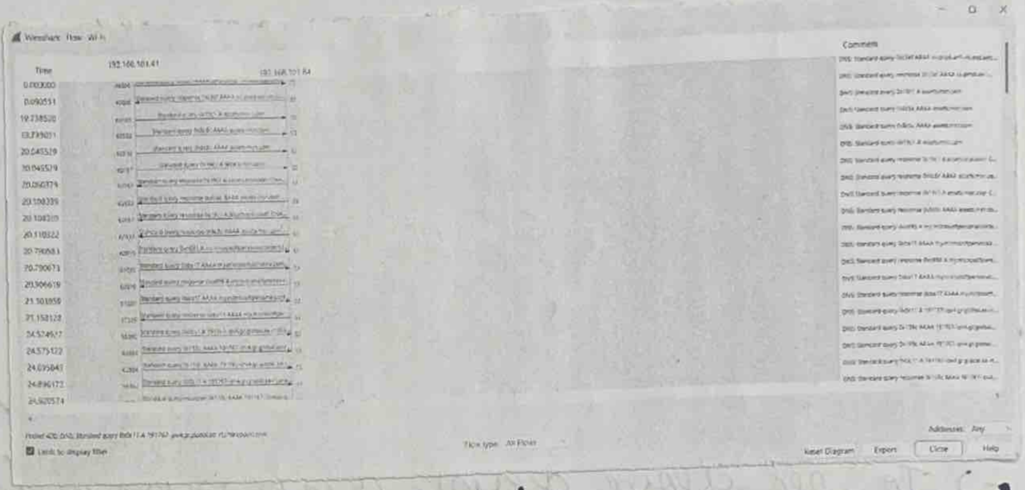
For DNS:



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



Wireshark · Flow · Wi-Fi

```
Time        192.168.101.41        192.168.101.84
0.000000
0.090551
19.738520
19.739011
20.045529
20.045529
20.060374
20.108339
20.108335
20.110322
20.790583
20.790671
20.906619
21.503858
21.158128
24.574517
24.575122
24.095041
24.896173
24.920574
```

Comments

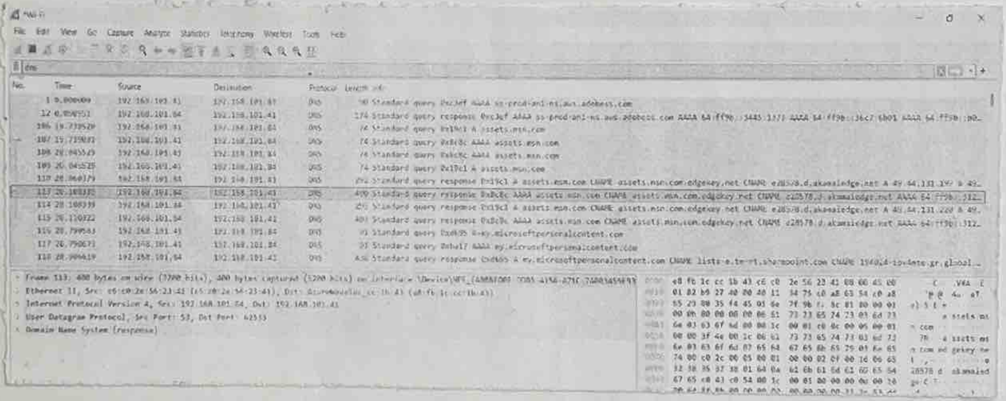
Packet 400: DNS: Standard query 0xfa11 A 19.17.63 ...

☑ Limit to display filter

Flow type: All Flows

Addresses: Any

Flow Graph :



*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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-ani-ns.aws.adobess.com
  12 0.090551    192.168.101.84   192.168.101.41   DNS      174 Standard query response 0xc3ef AAAA ss-prod-ani-ns.aws.adobess.com AAAA 64:ff9b::3445:1371 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 19.739011   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 49.44.131.192 A 49.…
 113 20.108335   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      292 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      400 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       93 Standard query 0xd695 A my.microsoftpersonalcontent.com
 117 20.790671   192.168.101.41   192.168.101.84   DNS       93 Standard query 0xba17 AAAA my.microsoftpersonalcontent.com
 118 20.906619   192.168.101.84   192.168.101.41   DNS      456 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_{A8B8ID09-7D85-4156-871C-7A883459F93
> Ethernet II, Src: e6:c0:2e:56:23:41 (e6:c0:2e:56:23:41), Dst: AzureWaveTec_cc:1b:43 (a8: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)
```

```
0000  a8 fb 1c cc 1b 43 c6 c0  2e 56 23 41 08 00 45 00    .....C. .V#A..E.
0010  01 82 b9 27 40 00 40 11  34 75 c0 a8 65 54 c0 a8    ...'@.@. 4u..eT..
0020  65 29 00 35 f4 45 01 6e  7f 9b 8c 8c 81 80 00 01    e).5.E.n ........
0030  00 0n 00 00 00 00 06 61  73 73 65 74 73 03 6d 73    .......a ssets.ms
0040  6e 03 63 6f 6d 00 00 1c  00 01 c0 0c 00 05 00 01    n.com... ........
0050  00 00 3f 4e 00 1c 06 61  73 73 65 74 73 03 6d 73    ..?N...a ssets.ms
0060  6e 03 63 6f 6d 07 65 64  67 65 6b 65 79 03 6e 65    n.com.ed gekey.ne
0070  74 00 c0 2c 00 05 00 01  00 00 02 0f 00 16 06 65    t..,.... .......e
0080  32 38 35 37 38 01 64 0a  61 6b 61 6d 61 69 65 64    28578.d. akamaied
0090  67 65 c0 43 c0 54 00 1c  00 01 00 00 00 0c 00 10    ge.C.T.. ........
```

Result :

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

9/8/24