|8|24

PRACTICAL-5

AIM:

Experiments on packet capture tools: wireshark.

Packet Sniffer:

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

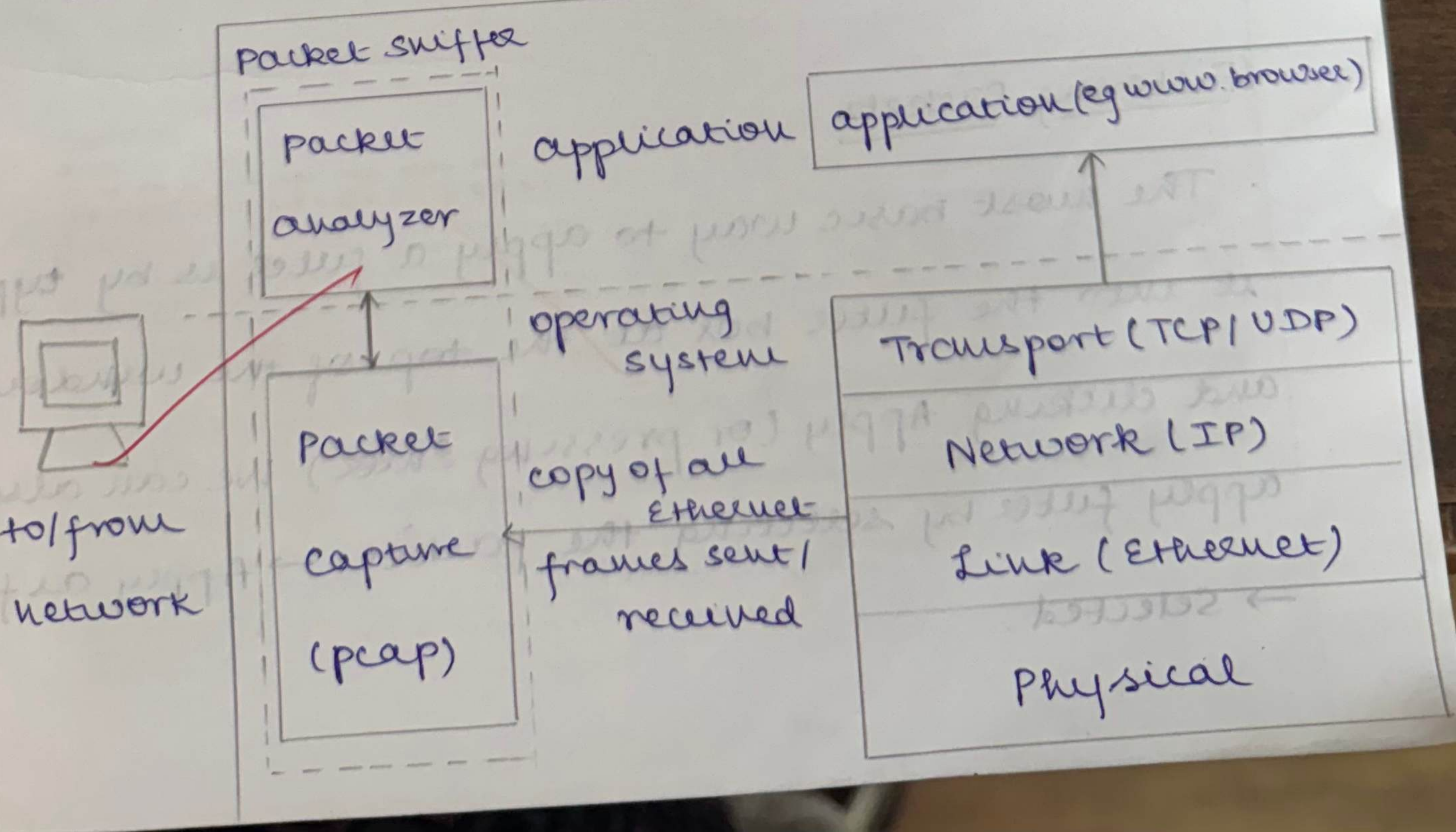
* store and display the contents of the various protocol fields in the messages.

* passive program
  - never sends packets itself.
  - no packets addressed to it.
  - receives a copy of all packets.

Packet sniffes structure Diagnostic Tools:-

* Tcp dump
  - Eg: tcpdump-enx host 10.129.41.2 -wexe3.out

* wireshark
  - wireshark -r exe3.out



Capturing Network Traffic:

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

Procedure:

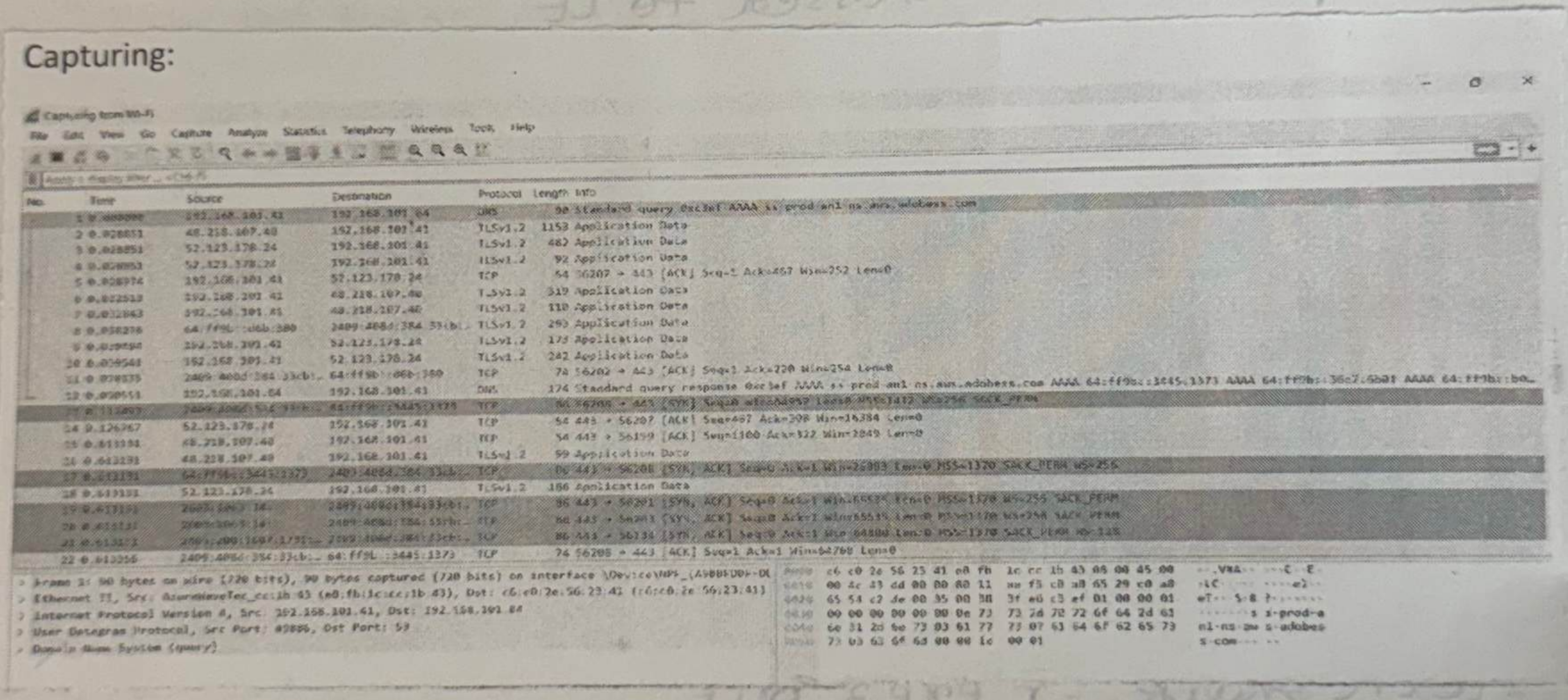
1) select Local Area connection is wireshark

2) Go to capture → option

3) select stop capture automatically after 100 packets

4) save the packets.

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  40.218.107.40         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 0.028853  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        40.218.107.40         TLSv1.2  319 Application Data
   7 0.032863  192.168.101.41        40.218.107.40         TLSv1.2  110 Application Data
   8 0.038278  64:ff9b::d6b:380      2409:4080:384:33cb:…  TLSv1.2  293 Application Data
   9 0.039054  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 0.078835  2409:4080:384:33cb:…  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::bo…
  13 0.112089  2409:4080:384:33cb:…  64:ff9b::3445:1373    TCP       86 56208 → 443 [SYN] Seq=0 Win=64800 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=398 Win=16384 Len=0
  15 0.613131  40.218.107.40         192.168.101.41        TCP       54 443 → 56199 [ACK] Seq=1100 Ack=322 Win=2049 Len=0
  16 0.613131  40.218.107.40         192.168.101.41        TLSv1.2   99 Application Data
  17 0.613131  64:ff9b::3445:1373    2409:4080:384:33cb:…  TCP       86 443 → 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  186 Application Data
  19 0.613131  2603:1063:14:…        2409:4080:384:33cb:…  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:…        2409:4080:384:33cb:…  TCP       86 443 → 56203 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1370 WS=256 SACK_PERM
  21 0.613173  2603:1007:1737:…      2409:4080:384:33cb:…  TCP       86 443 → 56134 [SYN, ACK] Seq=0 Ack=1 Win=64800 Len=0 MSS=1370 SACK_PERM WS=128
  22 0.613356  2409:4080:384:33cb:…  64:ff9b::3445:1373    TCP       74 56208 → 443 [ACK] Seq=1 Ack=1 Win=64768 Len=0
```

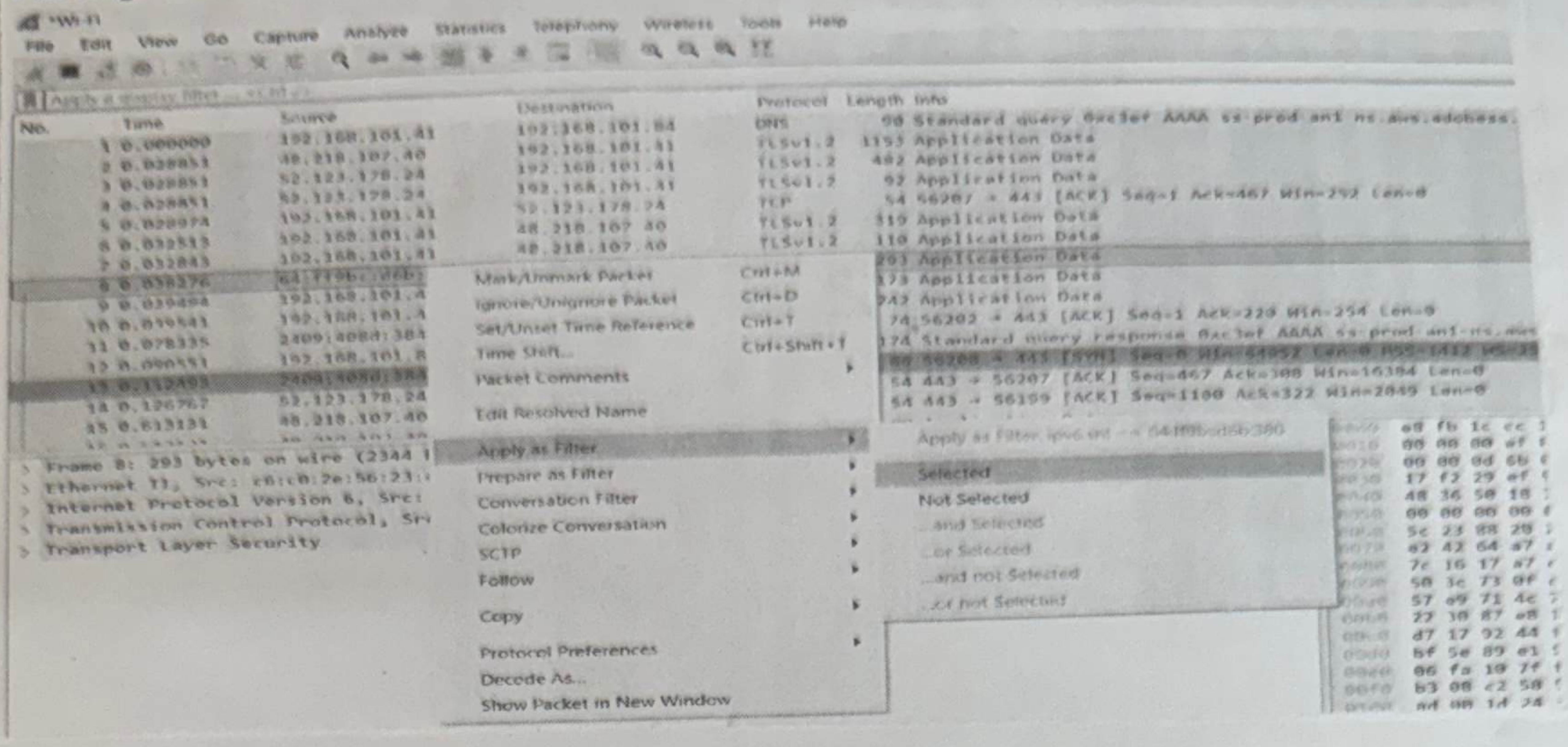
```
> Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{A9BBFD0F-DC
> Ethernet II, Src: AzureWaveTec_cc:1b:43 (e0:fb:1c:cc:1b:43), Dst: c6:c0:2e:56:23:41 (c6:c0:2e:56:23:41)
> Internet Protocol Version 4, Src: 192.168.101.41, Dst: 192.168.101.84
> User Datagram Protocol, Src Port: 49886, Dst Port: 53
> Domain Name System (query)
```

```
0000  c6 c0 2e 56 23 41 e0 fb  1c cc 1b 43 08 00 45 00   ...V#A.....C..E.
0010  00 4c 43 dd 00 00 80 11  aa f5 c0 a8 65 29 c0 a8   .LC.........e)..
0020  65 54 c2 de 00 35 00 38  3f e0 c3 ef 01 00 00 01   eT...5.8 ?.......
0030  00 00 00 00 00 00 0e 73  73 2d 70 72 6f 64 2d 61   .......s s-prod-a
0040  6e 31 2d 6e 73 03 61 77  73 07 61 64 6f 62 65 73   n1-ns-aw s-adobes
0050  73 03 63 6f 6d 00 00 1c  00 01                     s-com....
```

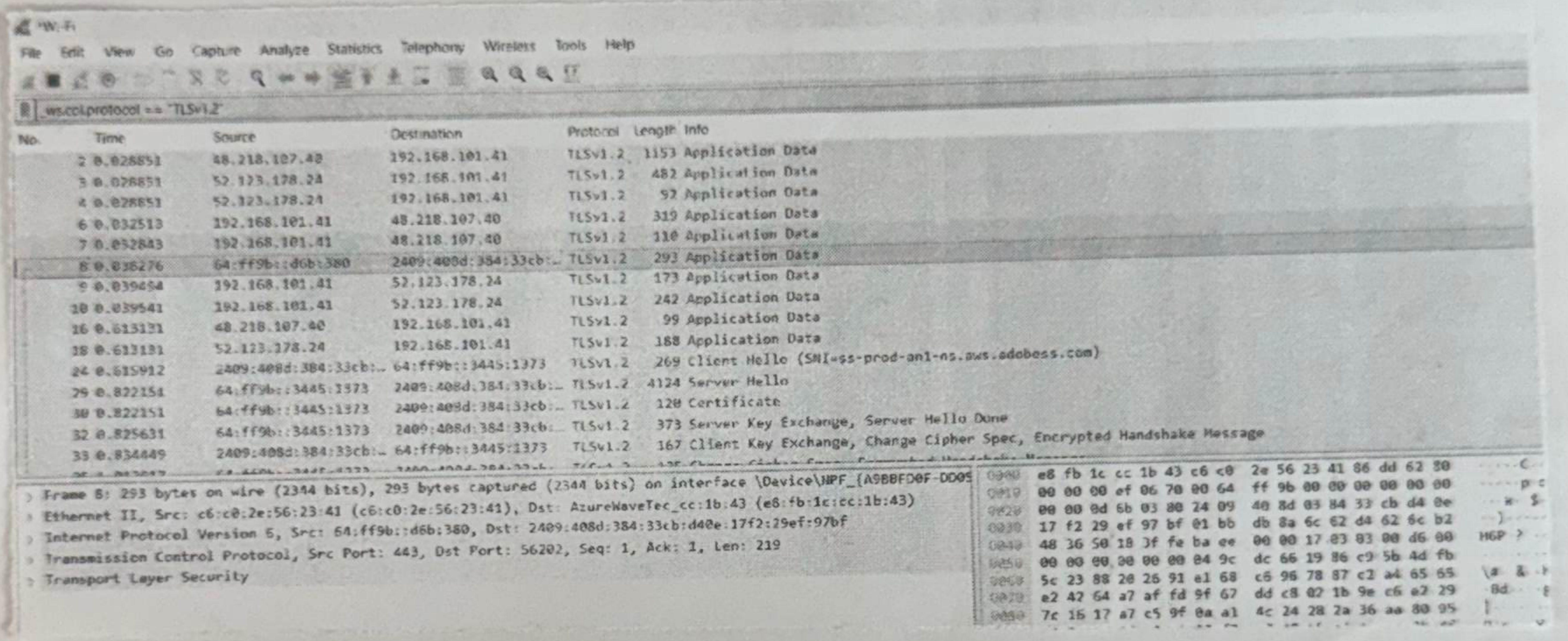
Filtering Packets:

The most basic way to ~~appy~~ 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.

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
Apply as Filter: ipv6.src == 64:ff9b::d6b:380
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:
> Internet Protocol Version 6, Src:
> Transmission Control Protocol, Src
> Transport Layer Security
```


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

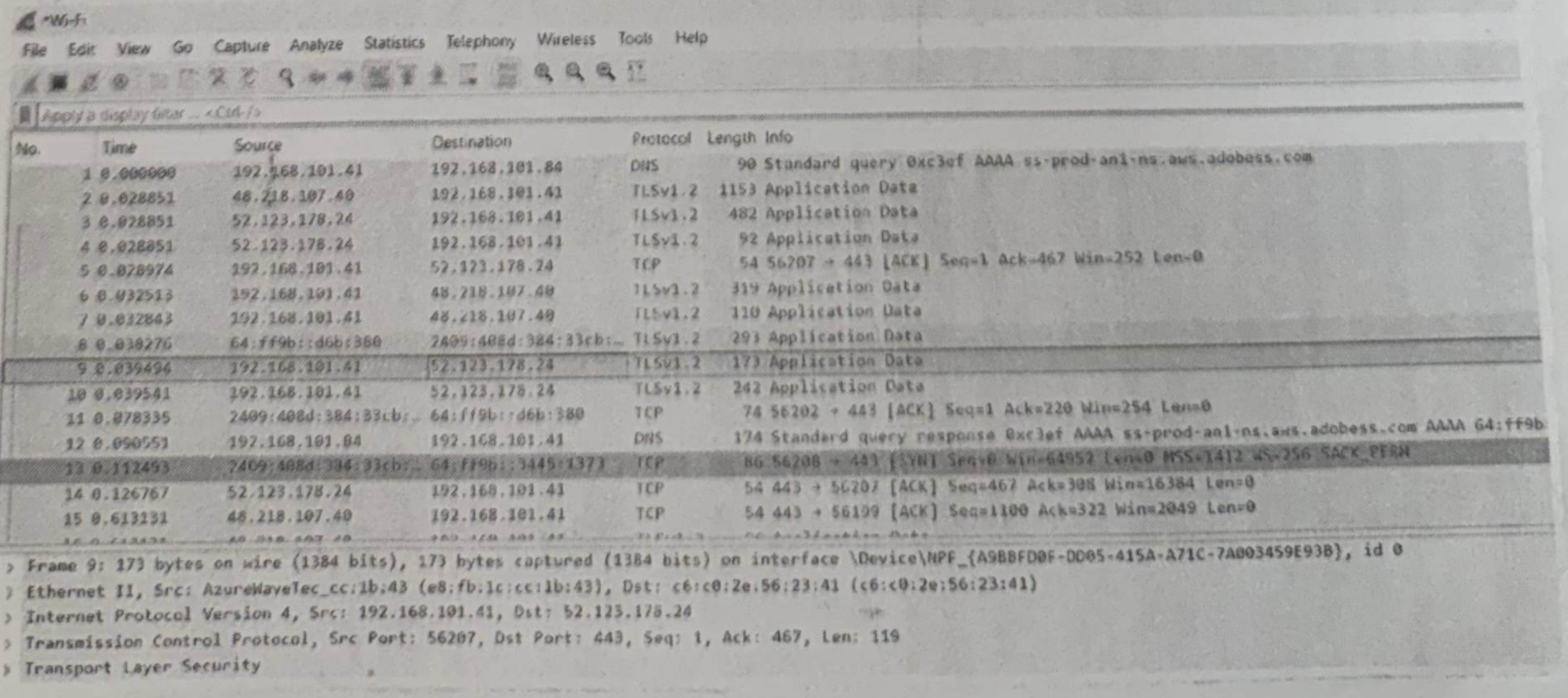
_ws.col.protocol == "TLSv1.2"

```
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 0.039494    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

0000  e8 fb 1c cc 1b 43 c6 c0  2e 56 23 41 86 dd 62 80
0010  00 00 00 ef 06 70 00 64  ff 9b 00 00 00 00 00 00
0020  00 00 0d 6b 03 80 24 09  40 8d 03 84 33 cb d4 0e
0030  17 f2 29 ef 97 bf 01 bb  db 8a 6c 62 d4 62 6c b2
0040  48 36 50 18 3f fe ba ee  00 00 17 03 03 00 d6 00
0050  00 00 00 30 00 00 04 9c  dc 66 19 86 c9 5b 4d fb
0060  5c 23 88 20 26 91 e1 68  c6 96 78 87 c2 a4 65 65
0070  e2 42 64 a7 af fd 9f 67  dd c8 02 1b 9e c6 a2 29
0080  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.

Inspecting:

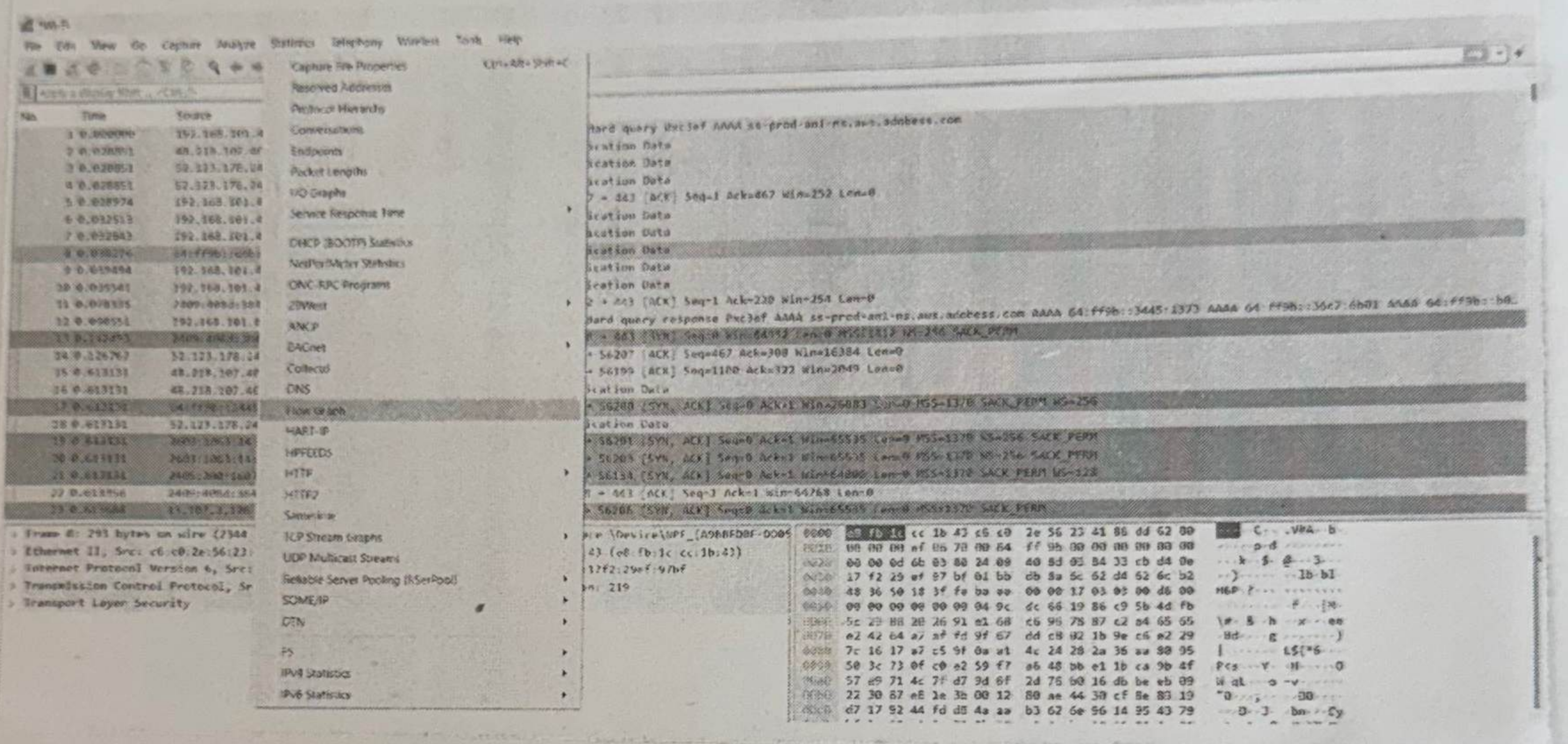

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

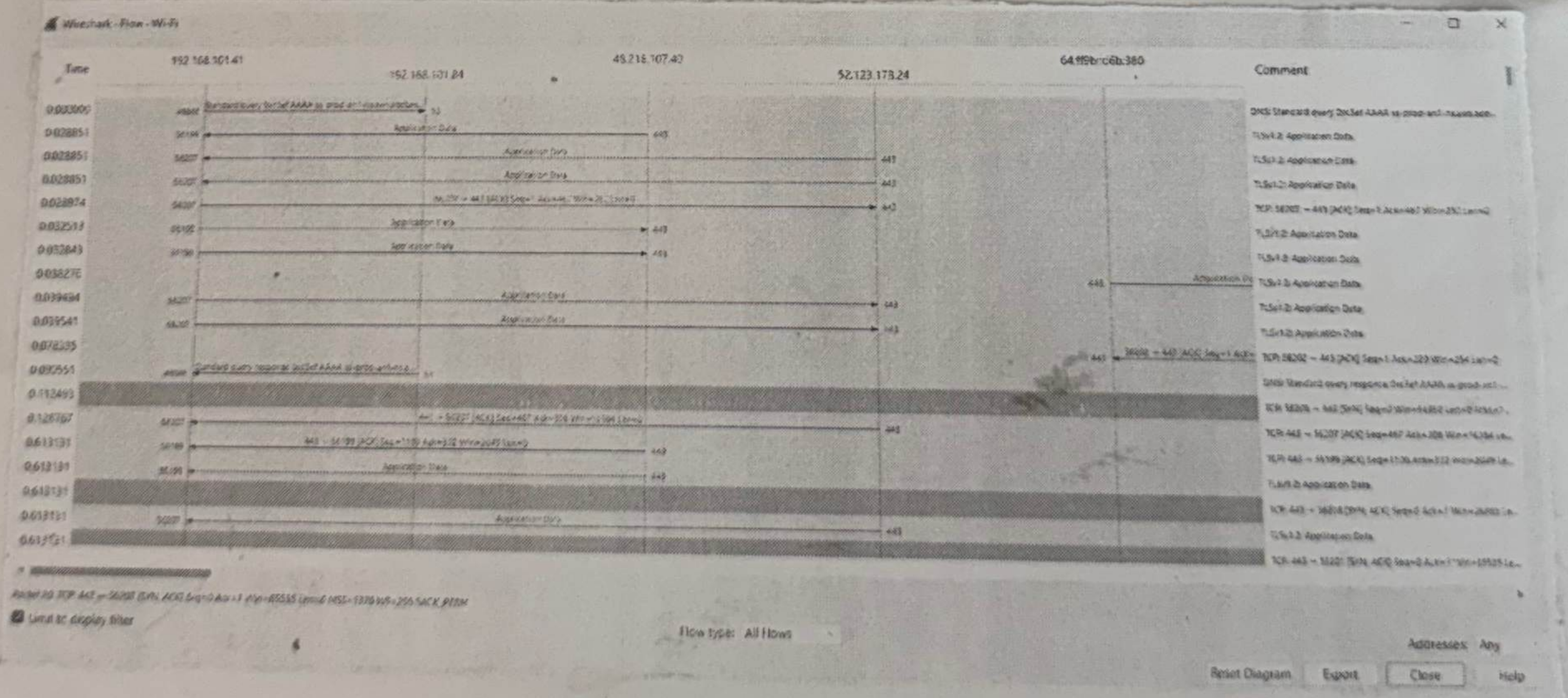
```
No.  Time        Source                Destination           Protocol Length Info
   1 0.000000    192.168.101.41        192.168.101.84        DNS        90 Standard query 0xc3ef AAAA ss-prod-an1-ns.aws.adobess.com
   2 0.028851    48.218.107.40         192.168.101.41        TLSv1.2  1153 Application 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-7A003459E93B}, 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.

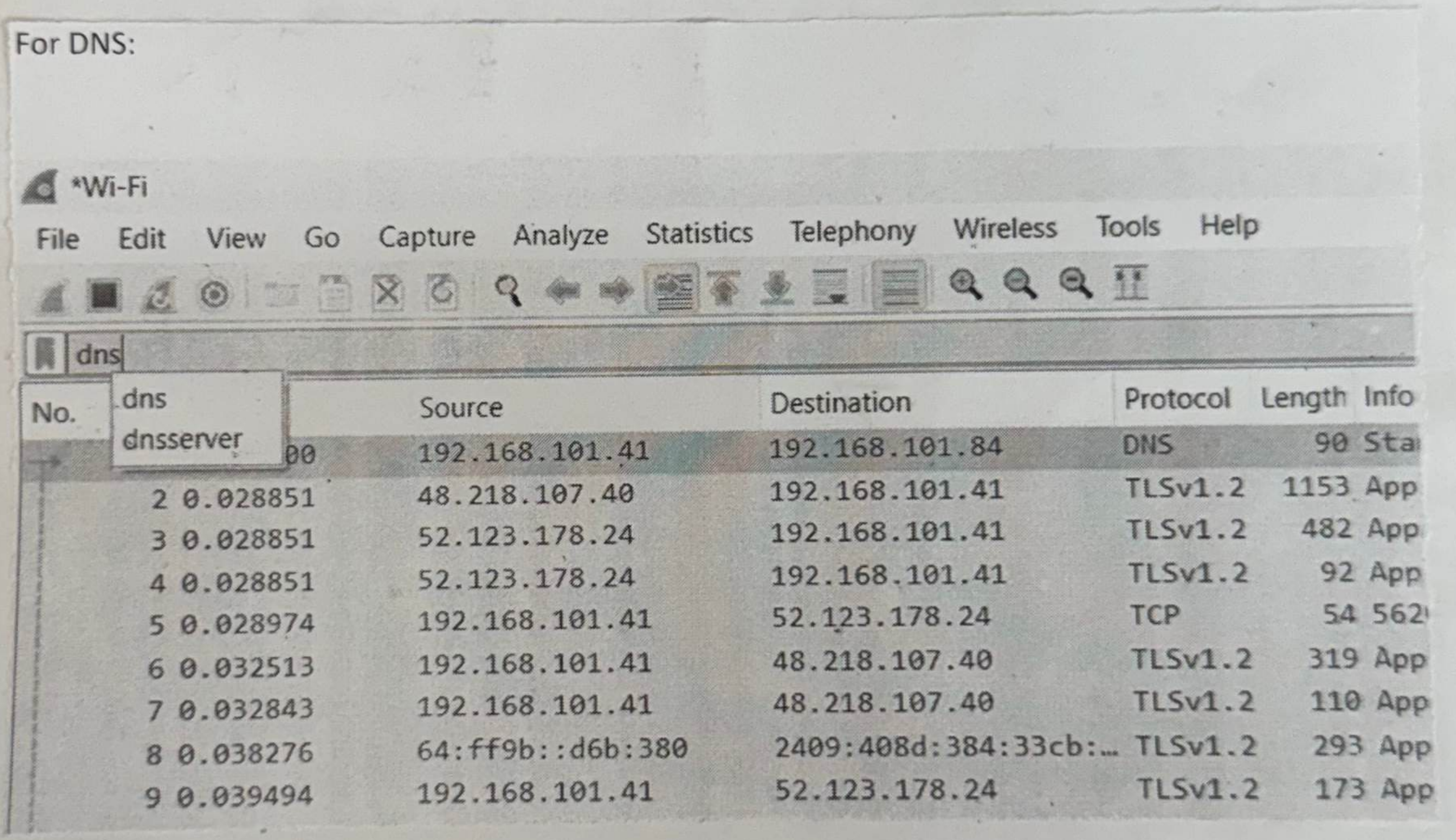
→ Then click start capture.

→ search DNS packets in search bar.

→ To see flow graph click statistics → Flow graph

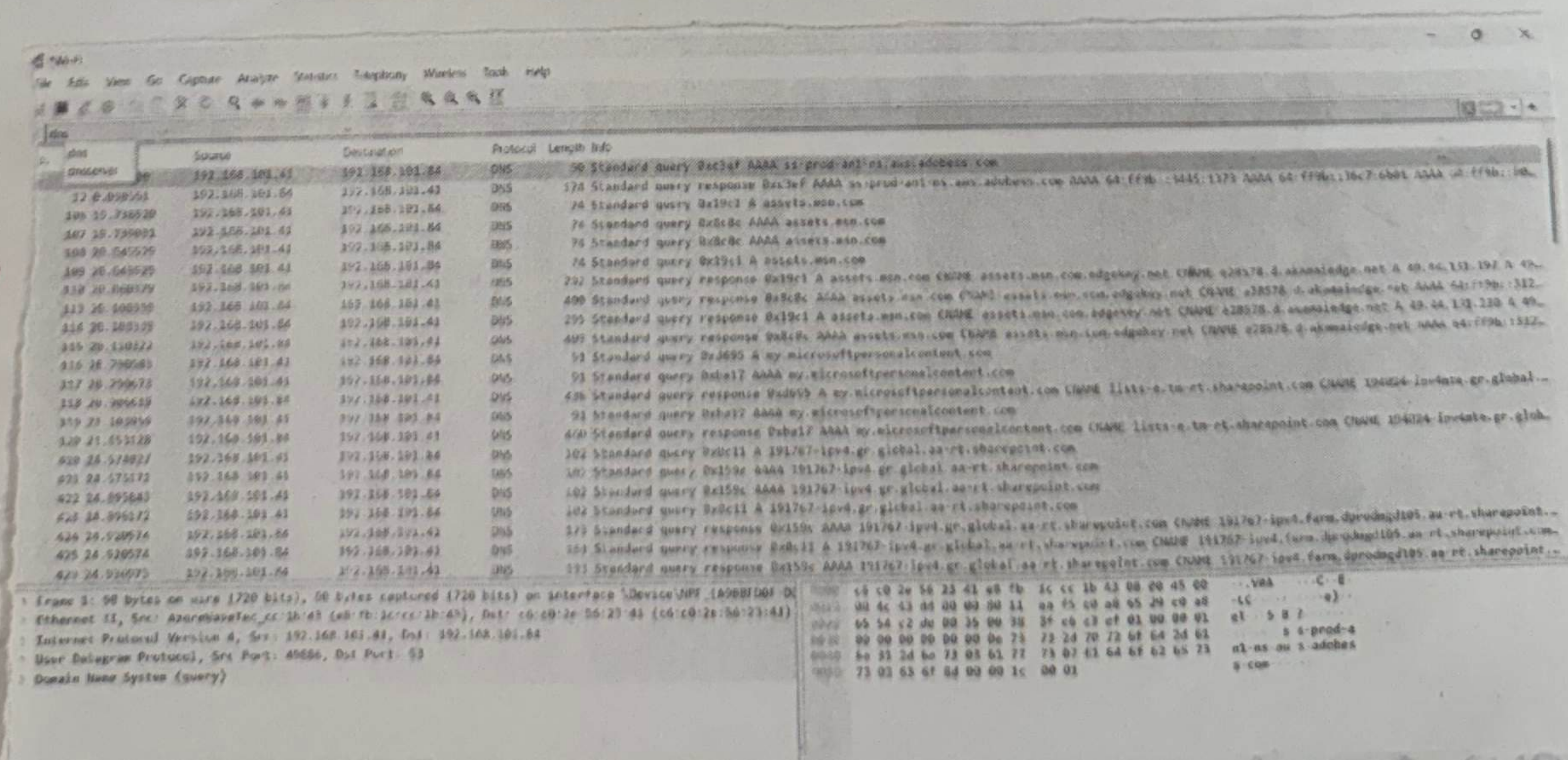
→ save the packets.

Capturing and Filtering:


For DNS:

*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
```


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

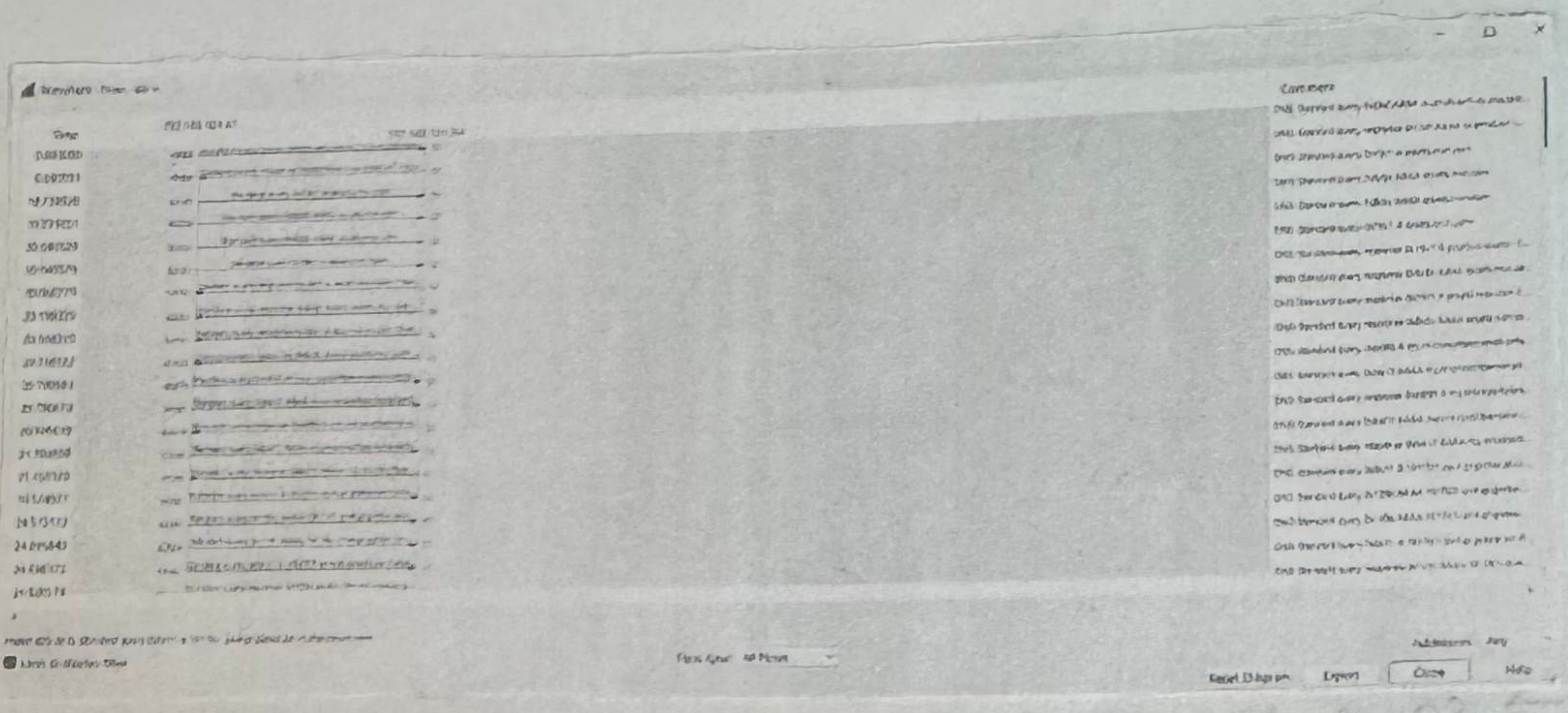
```
                    Source           Destination      Protocol Length Info
                    192.168.101.41   192.168.101.84   DNS        90 Standard query 0xc3ef AAAA ss-prod-an1-es.aws.adobess.com
   12 0.098561      192.168.101.84   192.168.101.41   DNS       174 Standard query response 0xc3ef AAAA ss-prod-an1-es.aws.adobess.com AAAA 64:ff9b::3445:1373 AAAA 64:ff9b::36c7:6b01 AAAA 64:ff9b::36…
  106 19.738520     192.168.101.41   192.168.101.84   DNS        74 Standard query 0x19c1 A assets.msn.com
  107 19.739001     192.168.101.41   192.168.101.84   DNS        76 Standard query 0x8c8c AAAA assets.msn.com
  108 20.645529     192.168.101.41   192.168.101.84   DNS        76 Standard query 0x8c8c AAAA assets.msn.com
  109 20.649629     192.168.101.41   192.168.101.84   DNS        74 Standard query 0x19c1 A assets.msn.com
  110 20.868579     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 20.100330     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 20.180339     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 49.44.131.120 A 49…
  115 20.110822     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 20.798081     192.168.101.41   192.168.101.84   DNS        91 Standard query 0xd695 A my.microsoftpersonalcontent.com
  117 20.299673     192.168.101.41   192.168.101.84   DNS        91 Standard query 0xba17 AAAA my.microsoftpersonalcontent.com
  118 20.989619     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 21.103856     192.168.101.41   192.168.101.84   DNS        91 Standard query 0xba17 AAAA my.microsoftpersonalcontent.com
  120 21.653128     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 24.574827     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…
  427 24.936075     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-D…
> 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)
```

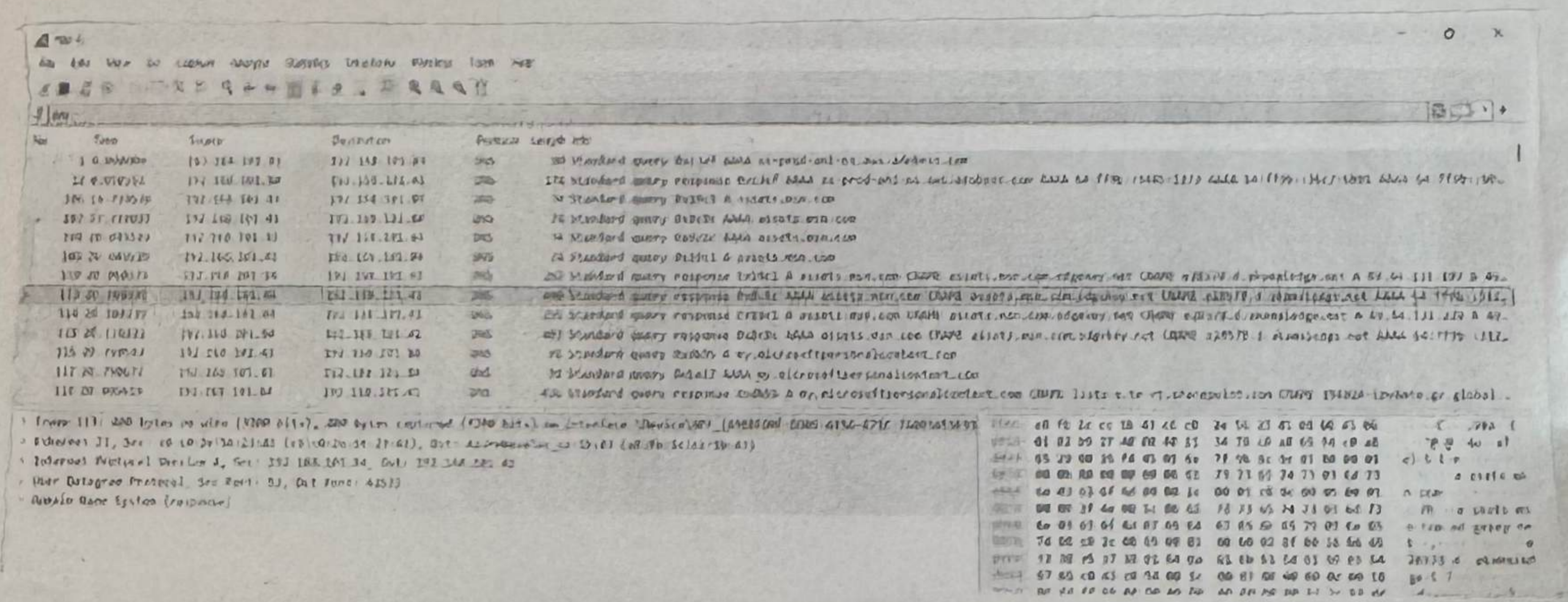
```
0000  c6 c0 2e 56 23 41 e8 fb  1c cc 1b 43 08 00 45 00   ...V#A.....C..E.
0010  00 4c 43 d4 00 00 80 11  aa f5 c0 a8 65 29 c0 a8   .LC.........e)..
0020  65 54 c2 de 00 35 00 38  3f c6 c3 ef 01 00 00 01   eT...5.8?.......
0030  00 00 00 00 00 00 0e 73  73 2d 70 72 6f 64 2d 61   .......ss-prod-a
0040  6e 31 2d 65 73 03 61 77  73 07 61 64 6f 62 65 73   n1-es.aws.adobes
0050  03 63 6f 6d 00 00 1c 00  01                        .com.....
```

16/8/24

Inspecting:



Flow Graph:



9/8/24

Result:

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