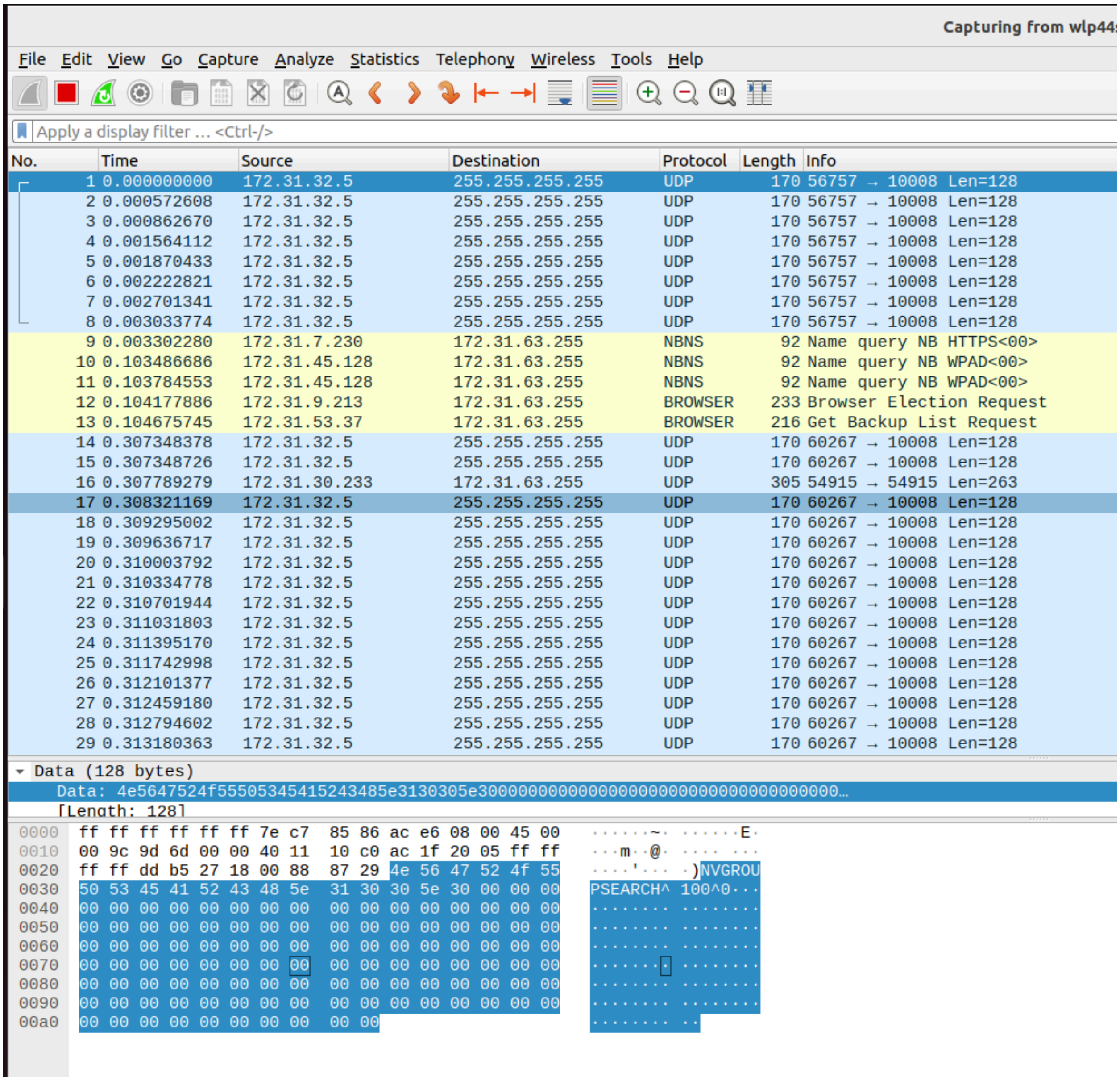
LAB 3

Name: Yogita Mundankar
Rollno. B22CS068

Ans 1:
I observe a continuous stream of packets with their ordering, time, source, destination, protocol , length , info.



Capturing from wlp44
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.31.32.5	255.255.255.255	UDP	170	56757 → 10008 Len=128
2	0.000572608	172.31.32.5	255.255.255.255	UDP	170	56757 → 10008 Len=128
3	0.000862670	172.31.32.5	255.255.255.255	UDP	170	56757 → 10008 Len=128
4	0.001564112	172.31.32.5	255.255.255.255	UDP	170	56757 → 10008 Len=128
5	0.001870433	172.31.32.5	255.255.255.255	UDP	170	56757 → 10008 Len=128
6	0.002222821	172.31.32.5	255.255.255.255	UDP	170	56757 → 10008 Len=128
7	0.002701341	172.31.32.5	255.255.255.255	UDP	170	56757 → 10008 Len=128
8	0.003033774	172.31.32.5	255.255.255.255	UDP	170	56757 → 10008 Len=128
9	0.003302280	172.31.7.230	172.31.63.255	NBNS	92	Name query NB HTTPS<00>
10	0.103486686	172.31.45.128	172.31.63.255	NBNS	92	Name query NB WPAD<00>
11	0.103784553	172.31.45.128	172.31.63.255	NBNS	92	Name query NB WPAD<00>
12	0.104177886	172.31.9.213	172.31.63.255	BROWSER	233	Browser Election Request
13	0.104675745	172.31.53.37	172.31.63.255	BROWSER	216	Get Backup List Request
14	0.307348378	172.31.32.5	255.255.255.255	UDP	170	60267 → 10008 Len=128
15	0.307348726	172.31.32.5	255.255.255.255	UDP	170	60267 → 10008 Len=128
16	0.307789279	172.31.30.233	172.31.63.255	UDP	305	54915 → 54915 Len=263
17	0.308321169	172.31.32.5	255.255.255.255	UDP	170	60267 → 10008 Len=128
18	0.309295002	172.31.32.5	255.255.255.255	UDP	170	60267 → 10008 Len=128
19	0.309636717	172.31.32.5	255.255.255.255	UDP	170	60267 → 10008 Len=128
20	0.310003792	172.31.32.5	255.255.255.255	UDP	170	60267 → 10008 Len=128
21	0.310334778	172.31.32.5	255.255.255.255	UDP	170	60267 → 10008 Len=128
22	0.310701944	172.31.32.5	255.255.255.255	UDP	170	60267 → 10008 Len=128
23	0.311031803	172.31.32.5	255.255.255.255	UDP	170	60267 → 10008 Len=128
24	0.311395170	172.31.32.5	255.255.255.255	UDP	170	60267 → 10008 Len=128
25	0.311742998	172.31.32.5	255.255.255.255	UDP	170	60267 → 10008 Len=128
26	0.312101377	172.31.32.5	255.255.255.255	UDP	170	60267 → 10008 Len=128
27	0.312459180	172.31.32.5	255.255.255.255	UDP	170	60267 → 10008 Len=128
28	0.312794602	172.31.32.5	255.255.255.255	UDP	170	60267 → 10008 Len=128
29	0.313180363	172.31.32.5	255.255.255.255	UDP	170	60267 → 10008 Len=128

```
▾ Data (128 bytes)
    Data: 4e5647524f55505345415243485e3130305e3000000000000000000000000000000000…
    [Length: 128]
```

```
0000  ff ff ff ff ff ff 7e c7  85 86 ac e6 08 00 45 00   ······~· ······E·
0010  00 9c 9d 6d 00 00 40 11  10 c0 ac 1f 20 05 ff ff   ···m··@· ···· ···
0020  ff ff dd b5 27 18 00 88  87 29 4e 56 47 52 4f 55   ····'··· ·)NVGROU
0030  50 53 45 41 52 43 48 5e  31 30 30 5e 30 00 00 00   PSEARCH^ 100^0···
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00                     ········ ··
```

Types of Captured Packets:

- Most of the packet traffic was constituted by UDP packets.
- There were some NBNS and browser packets.

Broadcast Traffic:

- The packets are broadcasted to 255.255.255.255 which is the local network broadcast address.
- Broadcast packets are used for discovery and communication when the sender does not know the ip address of the recipient.
- UDP Protocol is being used for broadcast queries.
- NBNS and Browser Election Request suggest that network might be running WIndows- based name resolution services.

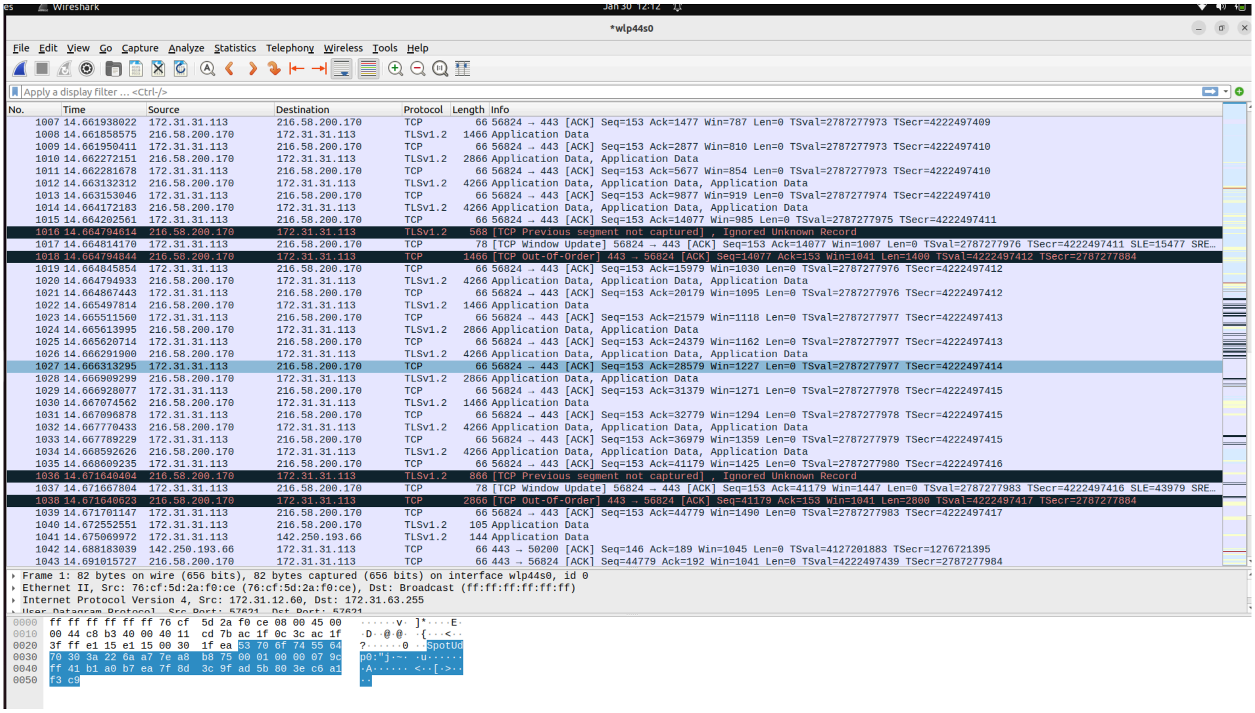
Source Destination Observation:

- Most packets originate from 172.31.32.5 and 172.31.45.128 which means that these machines are actively sending broadcast messages.
- Destination is 255.255.255.255 which means that the packets are broadcasted to all the devices.

The Bottom window with hexadecimal data:

- The hexadecimal data corresponds to NetBIOS and name service queries.
- The ASCII translation shows some readable text such as "PSearch", "NVGROUP".
- This suggests that some service discovery or network neighborhood lookup is taking place.

ANS 2:



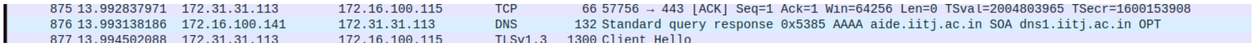
Wireshark
Jan 30 12:12
*wlp44s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time         Source          Destination     Protocol Length Info
 1007 14.661938022 172.31.31.113   216.58.200.170  TCP        66 56824 → 443 [ACK] Seq=153 Ack=1477 Win=787 Len=0 TSval=2787277973 TSecr=4222497409
 1008 14.661858575 216.58.200.170  172.31.31.113   TLSv1.2  1466 Application Data
 1009 14.661950411 172.31.31.113   216.58.200.170  TCP        66 56824 → 443 [ACK] Seq=153 Ack=2877 Win=810 Len=0 TSval=2787277973 TSecr=4222497410
 1010 14.662272151 216.58.200.170  172.31.31.113   TLSv1.2  2866 Application Data, Application Data
 1011 14.662281678 172.31.31.113   216.58.200.170  TCP        66 56824 → 443 [ACK] Seq=153 Ack=5677 Win=854 Len=0 TSval=2787277973 TSecr=4222497410
 1012 14.663132312 216.58.200.170  172.31.31.113   TLSv1.2  4266 Application Data, Application Data, Application Data
 1013 14.663153046 172.31.31.113   216.58.200.170  TCP        66 56824 → 443 [ACK] Seq=153 Ack=9877 Win=919 Len=0 TSval=2787277974 TSecr=4222497410
 1014 14.664172183 216.58.200.170  172.31.31.113   TLSv1.2  4266 Application Data, Application Data, Application Data
 1015 14.664202561 172.31.31.113   216.58.200.170  TCP        66 56824 → 443 [ACK] Seq=153 Ack=14077 Win=985 Len=0 TSval=2787277975 TSecr=4222497411
 1016 14.664794614 216.58.200.170  172.31.31.113   TLSv1.2   568 [TCP Previous segment not captured] , Ignored Unknown Record
 1017 14.664814170 172.31.31.113   216.58.200.170  TCP        78 [TCP Window Update] 56824 → 443 [ACK] Seq=153 Ack=14077 Win=1007 Len=0 TSval=2787277976 TSecr=4222497411 SLE=15477 SRE…
 1018 14.664794844 216.58.200.170  172.31.31.113   TCP      1466 [TCP Out-Of-Order] 443 → 56824 [ACK] Seq=14077 Ack=153 Win=1041 Len=1400 TSval=4222497412 TSecr=2787277884
 1019 14.664845854 172.31.31.113   216.58.200.170  TCP        66 56824 → 443 [ACK] Seq=153 Ack=15979 Win=1030 Len=0 TSval=2787277976 TSecr=4222497412
 1020 14.664794933 216.58.200.170  172.31.31.113   TLSv1.2  4266 Application Data, Application Data, Application Data
 1021 14.664867443 172.31.31.113   216.58.200.170  TCP        66 56824 → 443 [ACK] Seq=153 Ack=20179 Win=1095 Len=0 TSval=2787277976 TSecr=4222497412
 1022 14.665497814 216.58.200.170  172.31.31.113   TLSv1.2  1466 Application Data
 1023 14.665511560 172.31.31.113   216.58.200.170  TCP        66 56824 → 443 [ACK] Seq=153 Ack=21579 Win=1118 Len=0 TSval=2787277977 TSecr=4222497413
 1024 14.665613995 216.58.200.170  172.31.31.113   TLSv1.2  2866 Application Data, Application Data
 1025 14.665620714 172.31.31.113   216.58.200.170  TCP        66 56824 → 443 [ACK] Seq=153 Ack=24379 Win=1162 Len=0 TSval=2787277977 TSecr=4222497413
 1026 14.666291900 216.58.200.170  172.31.31.113   TLSv1.2  4266 Application Data, Application Data, Application Data
 1027 14.666313295 172.31.31.113   216.58.200.170  TCP        66 56824 → 443 [ACK] Seq=153 Ack=28579 Win=1227 Len=0 TSval=2787277977 TSecr=4222497414
 1028 14.666909299 216.58.200.170  172.31.31.113   TLSv1.2  2866 Application Data, Application Data
 1029 14.666928077 172.31.31.113   216.58.200.170  TCP        66 56824 → 443 [ACK] Seq=153 Ack=31379 Win=1271 Len=0 TSval=2787277978 TSecr=4222497415
 1030 14.667074562 216.58.200.170  172.31.31.113   TLSv1.2  1466 Application Data
 1031 14.667096878 172.31.31.113   216.58.200.170  TCP        66 56824 → 443 [ACK] Seq=153 Ack=32779 Win=1294 Len=0 TSval=2787277978 TSecr=4222497415
 1032 14.667770433 216.58.200.170  172.31.31.113   TLSv1.2  4266 Application Data, Application Data, Application Data
 1033 14.667789229 172.31.31.113   216.58.200.170  TCP        66 56824 → 443 [ACK] Seq=153 Ack=36979 Win=1359 Len=0 TSval=2787277979 TSecr=4222497415
 1034 14.668592626 216.58.200.170  172.31.31.113   TLSv1.2  4266 Application Data, Application Data, Application Data
 1035 14.668609235 172.31.31.113   216.58.200.170  TCP        66 56824 → 443 [ACK] Seq=153 Ack=41179 Win=1425 Len=0 TSval=2787277980 TSecr=4222497416
 1036 14.671640404 216.58.200.170  172.31.31.113   TLSv1.2   866 [TCP Previous segment not captured] , Ignored Unknown Record
 1037 14.671667804 172.31.31.113   216.58.200.170  TCP        78 [TCP Window Update] 56824 → 443 [ACK] Seq=153 Ack=41179 Win=1447 Len=0 TSval=2787277983 TSecr=4222497416 SLE=43979 SRE…
 1038 14.671640623 216.58.200.170  172.31.31.113   TCP      2866 [TCP Out-Of-Order] 443 → 56824 [ACK] Seq=41179 Ack=153 Win=1041 Len=2800 TSval=4222497417 TSecr=2787277884
 1039 14.671701147 172.31.31.113   216.58.200.170  TCP        66 56824 → 443 [ACK] Seq=153 Ack=44779 Win=1490 Len=0 TSval=2787277983 TSecr=4222497417
 1040 14.672552551 172.31.31.113   216.58.200.170  TLSv1.2   105 Application Data
 1041 14.675069972 172.31.31.113   142.250.193.66  TLSv1.2   144 Application Data
 1042 14.688183039 142.250.193.66  172.31.31.113   TCP        66 443 → 50200 [ACK] Seq=146 Ack=189 Win=1045 Len=0 TSval=4127201883 TSecr=1276721395
 1043 14.691015727 216.58.200.170  172.31.31.113   TCP        66 443 → 56824 [ACK] Seq=44779 Ack=192 Win=1041 Len=0 TSval=4222497439 TSecr=2787277984

› Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface wlp44s0, id 0
› Ethernet II, Src: 76:cf:5d:2a:f0:ce (76:cf:5d:2a:f0:ce), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
› Internet Protocol Version 4, Src: 172.31.12.60, Dst: 172.31.63.255
› User Datagram Protocol, Src Port: 57621, Dst Port: 57621

0000  ff ff ff ff ff ff 76 cf  5d 2a f0 ce 08 00 45 00   ······v· ]*····E·
0010  00 44 c8 b3 40 00 40 11  cd 7b ac 1f 0c 3c ac 1f   ·D··@·@· ·{···<··
0020  3f ff e1 15 e1 15 00 30  1f ea 53 70 6f 74 55 64   ?······0 ··SpotUd
0030  70 30 3a 22 6a a7 7e a8  b8 75 00 01 00 00 07 9c   p0:"j·~· ·u······
0040  ff 41 b1 a0 b7 ea 7f 8d  3c 9f ad 5b 80 3e c6 a1   ·A······ <··[·>··
0050  f3 c9                                              ··
```

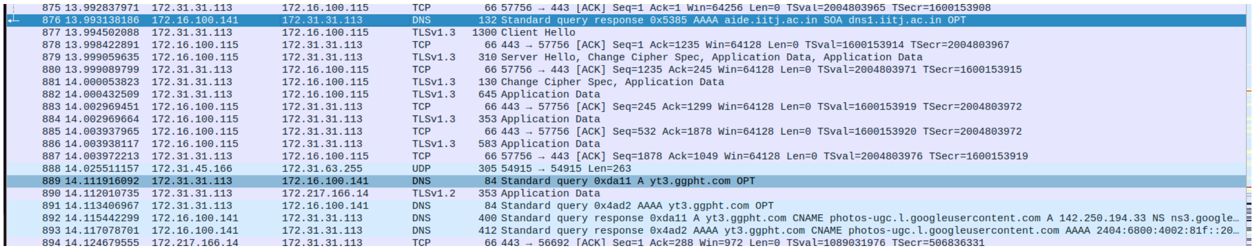
DNS for iitj.ac.in:



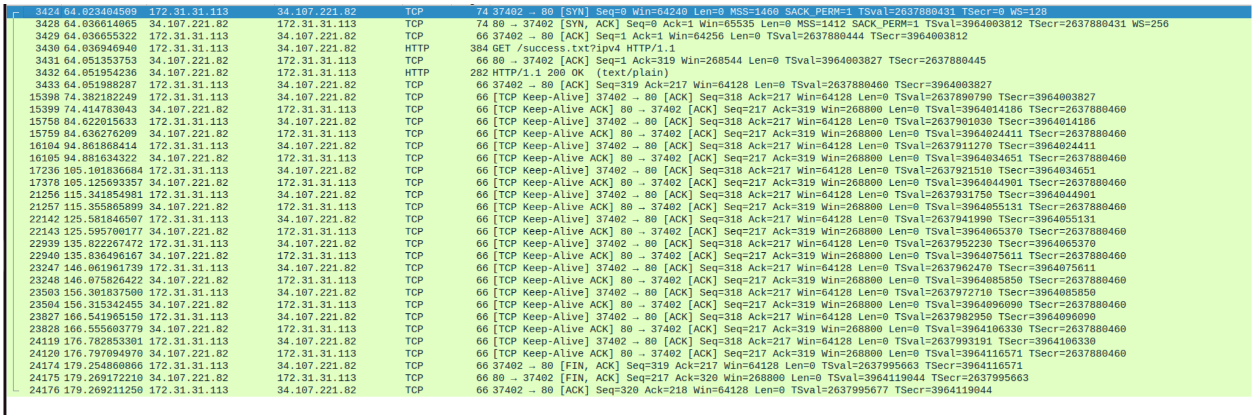
```
875 13.992837971  172.31.31.113    172.16.100.115   TCP       66 57756 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2004803965 TSecr=1600153908
876 13.993138186  172.16.100.141   172.31.31.113    DNS      132 Standard query response 0x5385 AAAA aide.iitj.ac.in SOA dns1.iitj.ac.in OPT
877 13.994502088  172.31.31.113    172.16.100.115   TLSv1.3 1300 Client Hello
```

IP Address of www.iitj.ac.in is 172.31.31.113

TCP and HTTP:

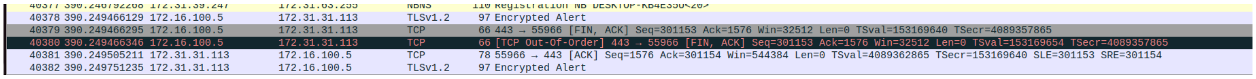


```
875 13.992837971 172.31.31.113   172.16.100.115  TCP       66 57756 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2004803965 TSecr=1600153908
876 13.993138186 172.16.100.141  172.31.31.113   DNS      132 Standard query response 0x5385 AAAA aide.iitj.ac.in SOA dns1.iitj.ac.in OPT
877 13.994502088 172.31.31.113   172.16.100.115  TLSv1.3 1300 Client Hello
878 13.998422891 172.16.100.115  172.31.31.113   TCP       66 443 → 57756 [ACK] Seq=1 Ack=1235 Win=64128 Len=0 TSval=1600153914 TSecr=2004803967
879 13.999059635 172.16.100.115  172.31.31.113   TLSv1.3  310 Server Hello, Change Cipher Spec, Application Data, Application Data
880 13.999089799 172.31.31.113   172.16.100.115  TCP       66 57756 → 443 [ACK] Seq=1235 Ack=245 Win=64128 Len=0 TSval=2004803971 TSecr=1600153915
881 14.000053823 172.31.31.113   172.16.100.115  TLSv1.3  130 Change Cipher Spec, Application Data
882 14.000432509 172.31.31.113   172.16.100.115  TLSv1.3  645 Application Data
883 14.002969451 172.16.100.115  172.31.31.113   TCP       66 443 → 57756 [ACK] Seq=245 Ack=1299 Win=64128 Len=0 TSval=1600153919 TSecr=2004803972
884 14.002969664 172.16.100.115  172.31.31.113   TLSv1.3  353 Application Data
885 14.003937965 172.16.100.115  172.31.31.113   TCP       66 443 → 57756 [ACK] Seq=532 Ack=1878 Win=64128 Len=0 TSval=1600153920 TSecr=2004803972
886 14.003938117 172.16.100.115  172.31.31.113   TLSv1.3  583 Application Data
887 14.003972213 172.31.31.113   172.16.100.115  TCP       66 57756 → 443 [ACK] Seq=1878 Ack=1049 Win=64128 Len=0 TSval=2004803976 TSecr=1600153919
888 14.025511157 172.31.45.166   172.31.63.255   UDP      305 54915 → 54915 Len=263
889 14.111916092 172.31.31.113   172.16.100.141  DNS       84 Standard query 0xda11 A yt3.ggpht.com OPT
890 14.112010735 172.31.31.113   172.217.166.14  TLSv1.2  353 Application Data
891 14.113406967 172.31.31.113   172.16.100.141  DNS       84 Standard query 0x4ad2 AAAA yt3.ggpht.com OPT
892 14.115442299 172.16.100.141  172.31.31.113   DNS      400 Standard query response 0xda11 A yt3.ggpht.com CNAME photos-ugc.l.googleusercontent.com A 142.250.194.33 NS ns3.google…
893 14.117078701 172.16.100.141  172.31.31.113   DNS      412 Standard query response 0x4ad2 AAAA yt3.ggpht.com CNAME photos-ugc.l.googleusercontent.com AAAA 2404:6800:4002:81f::20…
894 14.124679555 172.217.166.14  172.31.31.113   TCP       66 443 → 56692 [ACK] Seq=1 Ack=288 Win=972 Len=0 TSval=1089031976 TSecr=506836331
```



```
 3424 64.023404509  172.31.31.113  34.107.221.82  TCP   74 37402 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2637880431 TSecr=0 WS=128
 3428 64.036614065  34.107.221.82  172.31.31.113  TCP   74 80 → 37402 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM=1 TSval=3964003812 TSecr=2637880431 WS=256
 3429 64.036655322  172.31.31.113  34.107.221.82  TCP   66 37402 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2637880444 TSecr=3964003812
 3430 64.036946940  172.31.31.113  34.107.221.82  HTTP 384 GET /success.txt?ipv4 HTTP/1.1
 3431 64.051353753  34.107.221.82  172.31.31.113  TCP   66 80 → 37402 [ACK] Seq=1 Ack=319 Win=268544 Len=0 TSval=3964003827 TSecr=2637880445
 3432 64.051954236  34.107.221.82  172.31.31.113  HTTP 282 HTTP/1.1 200 OK  (text/plain)
 3433 64.051988287  172.31.31.113  34.107.221.82  TCP   66 37402 → 80 [ACK] Seq=319 Ack=217 Win=64128 Len=0 TSval=2637880460 TSecr=3964003827
15398 74.382182249  172.31.31.113  34.107.221.82  TCP   66 [TCP Keep-Alive] 37402 → 80 [ACK] Seq=318 Ack=217 Win=64128 Len=0 TSval=2637890790 TSecr=3964003827
15399 74.414783043  34.107.221.82  172.31.31.113  TCP   66 [TCP Keep-Alive ACK] 80 → 37402 [ACK] Seq=217 Ack=319 Win=268800 Len=0 TSval=3964014186 TSecr=2637880460
15758 84.622015633  172.31.31.113  34.107.221.82  TCP   66 [TCP Keep-Alive] 37402 → 80 [ACK] Seq=318 Ack=217 Win=64128 Len=0 TSval=2637901030 TSecr=3964014186
15759 84.636276209  34.107.221.82  172.31.31.113  TCP   66 [TCP Keep-Alive ACK] 80 → 37402 [ACK] Seq=217 Ack=319 Win=268800 Len=0 TSval=3964024411 TSecr=2637880460
16104 94.861868414  172.31.31.113  34.107.221.82  TCP   66 [TCP Keep-Alive] 37402 → 80 [ACK] Seq=318 Ack=217 Win=64128 Len=0 TSval=2637911270 TSecr=3964024411
16105 94.881634322  34.107.221.82  172.31.31.113  TCP   66 [TCP Keep-Alive ACK] 80 → 37402 [ACK] Seq=217 Ack=319 Win=268800 Len=0 TSval=3964034651 TSecr=2637880460
17236 105.101836684 172.31.31.113  34.107.221.82  TCP   66 [TCP Keep-Alive] 37402 → 80 [ACK] Seq=318 Ack=217 Win=64128 Len=0 TSval=2637921510 TSecr=3964034651
17378 105.125693357 34.107.221.82  172.31.31.113  TCP   66 [TCP Keep-Alive ACK] 80 → 37402 [ACK] Seq=217 Ack=319 Win=268800 Len=0 TSval=3964044901 TSecr=2637880460
21256 115.341854981 172.31.31.113  34.107.221.82  TCP   66 [TCP Keep-Alive] 37402 → 80 [ACK] Seq=318 Ack=217 Win=64128 Len=0 TSval=2637931750 TSecr=3964044901
21257 115.355865899 34.107.221.82  172.31.31.113  TCP   66 [TCP Keep-Alive ACK] 80 → 37402 [ACK] Seq=217 Ack=319 Win=268800 Len=0 TSval=3964055131 TSecr=2637880460
22142 125.581846507 172.31.31.113  34.107.221.82  TCP   66 [TCP Keep-Alive] 37402 → 80 [ACK] Seq=318 Ack=217 Win=64128 Len=0 TSval=2637941990 TSecr=3964055131
22143 125.595700177 34.107.221.82  172.31.31.113  TCP   66 [TCP Keep-Alive ACK] 80 → 37402 [ACK] Seq=217 Ack=319 Win=268800 Len=0 TSval=3964065370 TSecr=2637880460
22939 135.822267472 172.31.31.113  34.107.221.82  TCP   66 [TCP Keep-Alive] 37402 → 80 [ACK] Seq=318 Ack=217 Win=64128 Len=0 TSval=2637952230 TSecr=3964065370
22940 135.836496167 34.107.221.82  172.31.31.113  TCP   66 [TCP Keep-Alive ACK] 80 → 37402 [ACK] Seq=217 Ack=319 Win=268800 Len=0 TSval=3964075611 TSecr=2637880460
23247 146.061961739 172.31.31.113  34.107.221.82  TCP   66 [TCP Keep-Alive] 37402 → 80 [ACK] Seq=318 Ack=217 Win=64128 Len=0 TSval=2637962470 TSecr=3964075611
23248 146.075826422 34.107.221.82  172.31.31.113  TCP   66 [TCP Keep-Alive ACK] 80 → 37402 [ACK] Seq=217 Ack=319 Win=268800 Len=0 TSval=3964085850 TSecr=2637880460
23503 156.301837500 172.31.31.113  34.107.221.82  TCP   66 [TCP Keep-Alive] 37402 → 80 [ACK] Seq=318 Ack=217 Win=64128 Len=0 TSval=2637972710 TSecr=3964085850
23504 156.315342455 34.107.221.82  172.31.31.113  TCP   66 [TCP Keep-Alive ACK] 80 → 37402 [ACK] Seq=217 Ack=319 Win=268800 Len=0 TSval=3964096090 TSecr=2637880460
23827 166.541965150 172.31.31.113  34.107.221.82  TCP   66 [TCP Keep-Alive] 37402 → 80 [ACK] Seq=318 Ack=217 Win=64128 Len=0 TSval=2637982950 TSecr=3964096090
23828 166.555603779 34.107.221.82  172.31.31.113  TCP   66 [TCP Keep-Alive ACK] 80 → 37402 [ACK] Seq=217 Ack=319 Win=268800 Len=0 TSval=3964106330 TSecr=2637880460
24119 176.782853301 172.31.31.113  34.107.221.82  TCP   66 [TCP Keep-Alive] 37402 → 80 [ACK] Seq=318 Ack=217 Win=64128 Len=0 TSval=2637993191 TSecr=3964106330
24120 176.797094970 34.107.221.82  172.31.31.113  TCP   66 [TCP Keep-Alive ACK] 80 → 37402 [ACK] Seq=217 Ack=319 Win=268800 Len=0 TSval=3964116571 TSecr=2637880460
24174 179.254860866 172.31.31.113  34.107.221.82  TCP   66 37402 → 80 [FIN, ACK] Seq=319 Ack=217 Win=64128 Len=0 TSval=2637995663 TSecr=3964116571
24175 179.269172210 34.107.221.82  172.31.31.113  TCP   66 80 → 37402 [FIN, ACK] Seq=217 Ack=320 Win=268800 Len=0 TSval=3964119044 TSecr=2637995663
24176 179.269211250 172.31.31.113  34.107.221.82  TCP   66 37402 → 80 [ACK] Seq=320 Ack=218 Win=64128 Len=0 TSval=2637995677 TSecr=3964119044
```

ANS 3:



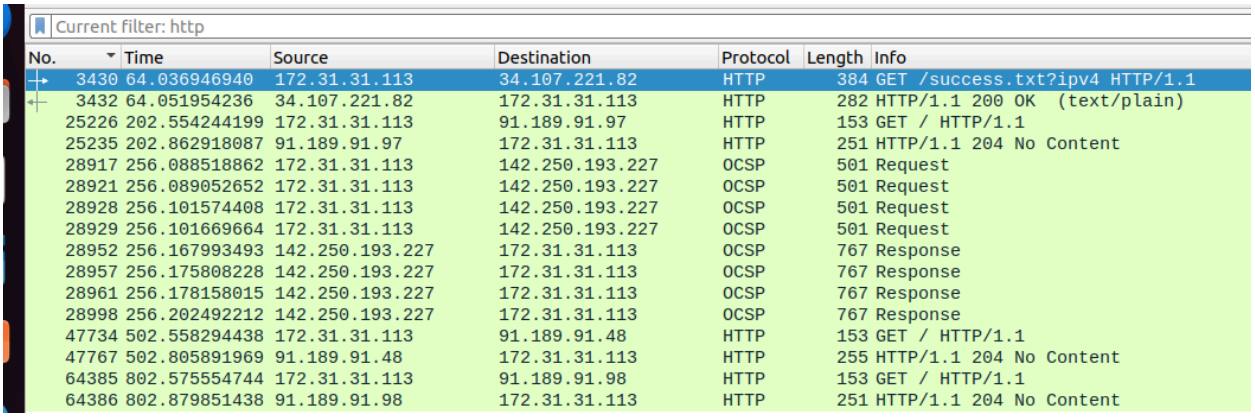
```
40377 390.246792268 172.31.39.247     172.31.63.255     NBNS      110 Registration NB DESKTOP-KB4E35O<20>
40378 390.249466129 172.16.100.5      172.31.31.113     TLSv1.2    97 Encrypted Alert
40379 390.249466295 172.16.100.5      172.31.31.113     TCP        66 443 → 55966 [FIN, ACK] Seq=301153 Ack=1576 Win=32512 Len=0 TSval=153169640 TSecr=4089357865
40380 390.249466346 172.16.100.5      172.31.31.113     TCP        66 [TCP Out-Of-Order] 443 → 55966 [FIN, ACK] Seq=301153 Ack=1576 Win=32512 Len=0 TSval=153169654 TSecr=4089357865
40381 390.249505211 172.31.31.113     172.16.100.5      TCP        78 55966 → 443 [ACK] Seq=1576 Ack=301154 Win=544384 Len=0 TSval=4089362865 TSecr=153169640 SLE=301153 SRE=301154
40382 390.249751235 172.31.31.113     172.16.100.5      TLSv1.2    97 Encrypted Alert
```

In Wireshark, a packet highlighted in black typically signifies a "Malformed Packet." This means the packet does not conform to the expected format of the protocol it is using. This could be due to various reasons, such as corruption during transmission, improper formatting, or an invalid checksum.

When you see a black-highlighted packet, it may indicate that the packet is not interpretable by Wireshark as it does not comply with the expected protocol structure, or it could also indicate some error in the packet's integrity.

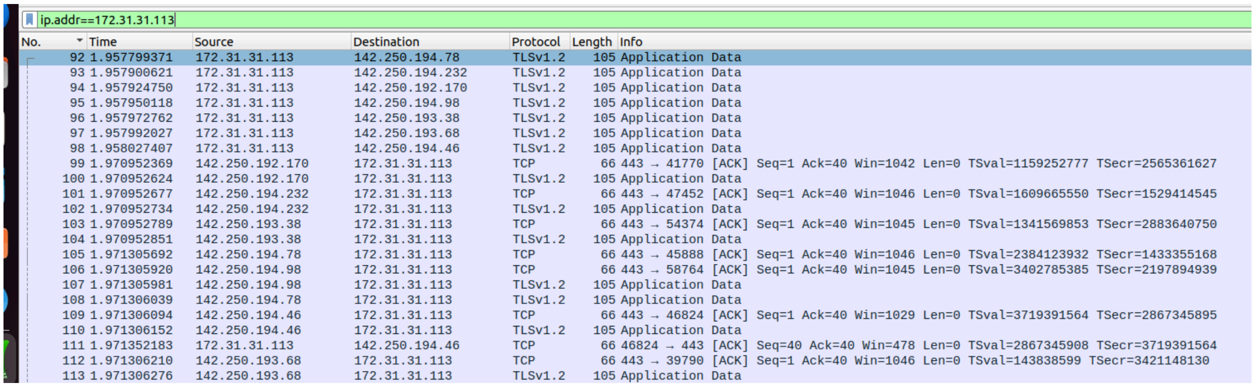
ANS 4:

1) http filter:



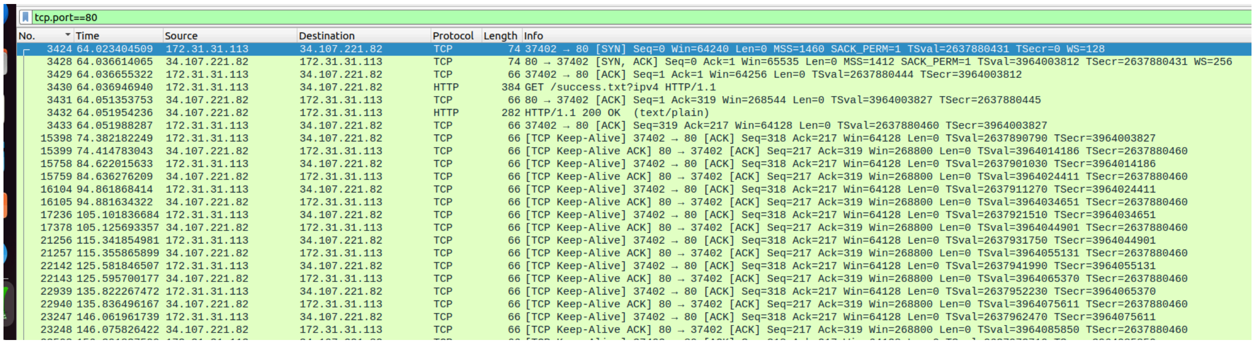
```
Current filter: http
No.    Time           Source          Destination      Protocol Length Info
 3430  64.036946940   172.31.31.113   34.107.221.82    HTTP     384 GET /success.txt?ipv4 HTTP/1.1
 3432  64.051954236   34.107.221.82   172.31.31.113    HTTP     282 HTTP/1.1 200 OK  (text/plain)
25226 202.554244199   172.31.31.113   91.189.91.97     HTTP     153 GET / HTTP/1.1
25235 202.862918087   91.189.91.97    172.31.31.113    HTTP     251 HTTP/1.1 204 No Content
28917 256.088518862   172.31.31.113   142.250.193.227  OCSP     501 Request
28921 256.089052652   172.31.31.113   142.250.193.227  OCSP     501 Request
28928 256.101574408   172.31.31.113   142.250.193.227  OCSP     501 Request
28929 256.101669664   172.31.31.113   142.250.193.227  OCSP     501 Request
28952 256.167993493   142.250.193.227 172.31.31.113    OCSP     767 Response
28957 256.175808228   142.250.193.227 172.31.31.113    OCSP     767 Response
28961 256.178158015   142.250.193.227 172.31.31.113    OCSP     767 Response
28998 256.202492212   142.250.193.227 172.31.31.113    OCSP     767 Response
47734 502.558294438   172.31.31.113   91.189.91.48     HTTP     153 GET / HTTP/1.1
47767 502.805891969   91.189.91.48    172.31.31.113    HTTP     255 HTTP/1.1 204 No Content
64385 802.575554744   172.31.31.113   91.189.91.98     HTTP     153 GET / HTTP/1.1
64386 802.879851438   91.189.91.98    172.31.31.113    HTTP     251 HTTP/1.1 204 No Content
```

2) ip.addr==172.31.31.113 (gives traffic based on the ip address)



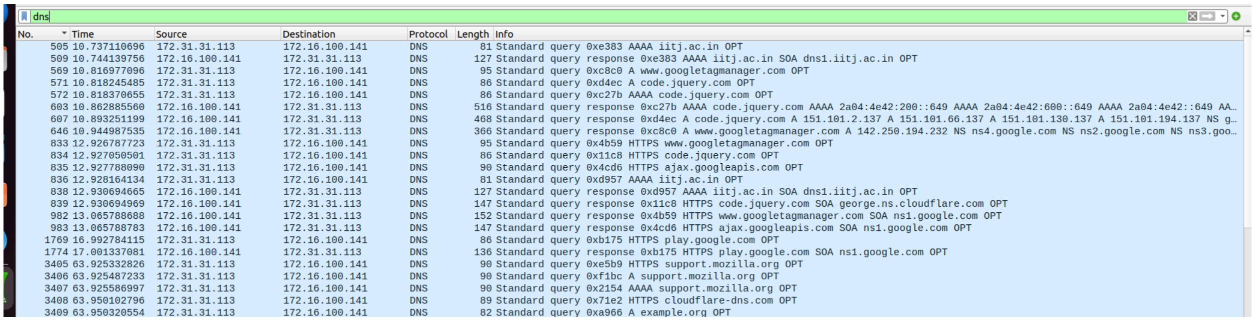
```
ip.addr==172.31.31.113
No.  Time         Source           Destination      Protocol Length Info
 92 1.957799371   172.31.31.113    142.250.194.78   TLSv1.2  105 Application Data
 93 1.957900621   172.31.31.113    142.250.194.232  TLSv1.2  105 Application Data
 94 1.957924750   172.31.31.113    142.250.192.170  TLSv1.2  105 Application Data
 95 1.957950118   172.31.31.113    142.250.194.98   TLSv1.2  105 Application Data
 96 1.957972762   172.31.31.113    142.250.193.38   TLSv1.2  105 Application Data
 97 1.957992027   172.31.31.113    142.250.193.68   TLSv1.2  105 Application Data
 98 1.958027407   172.31.31.113    142.250.194.46   TLSv1.2  105 Application Data
 99 1.970952369   142.250.192.170  172.31.31.113    TCP       66 443 → 41770 [ACK] Seq=1 Ack=40 Win=1042 Len=0 TSval=1159252777 TSecr=2565361627
100 1.970952624   142.250.192.170  172.31.31.113    TLSv1.2  105 Application Data
101 1.970952677   142.250.194.232  172.31.31.113    TCP       66 443 → 47452 [ACK] Seq=1 Ack=40 Win=1046 Len=0 TSval=1609665550 TSecr=1529414545
102 1.970952734   142.250.194.232  172.31.31.113    TLSv1.2  105 Application Data
103 1.970952789   142.250.193.38   172.31.31.113    TCP       66 443 → 54374 [ACK] Seq=1 Ack=40 Win=1045 Len=0 TSval=1341569853 TSecr=2883640750
104 1.970952851   142.250.193.38   172.31.31.113    TLSv1.2  105 Application Data
105 1.971305692   142.250.194.78   172.31.31.113    TCP       66 443 → 45888 [ACK] Seq=1 Ack=40 Win=1046 Len=0 TSval=2384123932 TSecr=1433355168
106 1.971305920   142.250.194.98   172.31.31.113    TCP       66 443 → 58764 [ACK] Seq=1 Ack=40 Win=1045 Len=0 TSval=3402785385 TSecr=2197894939
107 1.971305981   142.250.194.98   172.31.31.113    TLSv1.2  105 Application Data
108 1.971306039   142.250.194.78   172.31.31.113    TLSv1.2  105 Application Data
109 1.971306094   142.250.194.46   172.31.31.113    TCP       66 443 → 46824 [ACK] Seq=1 Ack=40 Win=1029 Len=0 TSval=3719391564 TSecr=2867345895
110 1.971306152   142.250.194.46   172.31.31.113    TLSv1.2  105 Application Data
111 1.971352183   172.31.31.113    142.250.194.46   TCP       66 46824 → 443 [ACK] Seq=40 Ack=40 Win=478 Len=0 TSval=2867345908 TSecr=3719391564
112 1.971306210   142.250.193.68   172.31.31.113    TCP       66 443 → 39790 [ACK] Seq=1 Ack=40 Win=1046 Len=0 TSval=143838599 TSecr=3421148130
113 1.971306276   142.250.193.68   172.31.31.113    TLSv1.2  105 Application Data
```

3) tcp.port==80 (filters traffic based on port number)



```
tcp.port==80
No.    Time          Source         Destination    Protocol Length Info
 3424 64.023404509  172.31.31.113  34.107.221.82  TCP       74 37402 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2637880431 TSecr=0 WS=128
 3428 64.036614065  34.107.221.82  172.31.31.113  TCP       74 80 → 37402 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM=1 TSval=3964003812 TSecr=2637880431 WS=256
 3429 64.036655322  172.31.31.113  34.107.221.82  TCP       66 37402 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2637880444 TSecr=3964003812
 3430 64.036946940  172.31.31.113  34.107.221.82  HTTP     384 GET /success.txt?ipv4 HTTP/1.1
 3431 64.051353753  34.107.221.82  172.31.31.113  TCP       66 80 → 37402 [ACK] Seq=1 Ack=319 Win=268544 Len=0 TSval=3964003827 TSecr=2637880445
 3432 64.051954236  34.107.221.82  172.31.31.113  HTTP     282 HTTP/1.1 200 OK  (text/plain)
 3433 64.051988287  172.31.31.113  34.107.221.82  TCP       66 37402 → 80 [ACK] Seq=319 Ack=217 Win=64128 Len=0 TSval=2637880460 TSecr=3964003827
15398 74.382182249  172.31.31.113  34.107.221.82  TCP       66 [TCP Keep-Alive] 37402 → 80 [ACK] Seq=318 Ack=217 Win=64128 Len=0 TSval=2637890790 TSecr=3964003827
15399 74.414783043  34.107.221.82  172.31.31.113  TCP       66 [TCP Keep-Alive ACK] 80 → 37402 [ACK] Seq=217 Ack=319 Win=268800 Len=0 TSval=3964014186 TSecr=2637880460
15758 84.622015633  172.31.31.113  34.107.221.82  TCP       66 [TCP Keep-Alive] 37402 → 80 [ACK] Seq=318 Ack=217 Win=64128 Len=0 TSval=2637901030 TSecr=3964014186
15759 84.636276209  34.107.221.82  172.31.31.113  TCP       66 [TCP Keep-Alive ACK] 80 → 37402 [ACK] Seq=217 Ack=319 Win=268800 Len=0 TSval=3964024411 TSecr=2637880460
16104 94.861868414  172.31.31.113  34.107.221.82  TCP       66 [TCP Keep-Alive] 37402 → 80 [ACK] Seq=318 Ack=217 Win=64128 Len=0 TSval=2637911270 TSecr=3964024411
16105 94.881634322  34.107.221.82  172.31.31.113  TCP       66 [TCP Keep-Alive ACK] 80 → 37402 [ACK] Seq=217 Ack=319 Win=268800 Len=0 TSval=3964034651 TSecr=2637880460
17236 105.101836684 172.31.31.113  34.107.221.82  TCP       66 [TCP Keep-Alive] 37402 → 80 [ACK] Seq=318 Ack=217 Win=64128 Len=0 TSval=2637921510 TSecr=3964034651
17378 105.125693357 34.107.221.82  172.31.31.113  TCP       66 [TCP Keep-Alive ACK] 80 → 37402 [ACK] Seq=217 Ack=319 Win=268800 Len=0 TSval=3964044901 TSecr=2637880460
21256 115.341854981 172.31.31.113  34.107.221.82  TCP       66 [TCP Keep-Alive] 37402 → 80 [ACK] Seq=318 Ack=217 Win=64128 Len=0 TSval=2637931750 TSecr=3964044901
21257 115.355865899 34.107.221.82  172.31.31.113  TCP       66 [TCP Keep-Alive ACK] 80 → 37402 [ACK] Seq=217 Ack=319 Win=268800 Len=0 TSval=3964055131 TSecr=2637880460
22142 125.581846507 172.31.31.113  34.107.221.82  TCP       66 [TCP Keep-Alive] 37402 → 80 [ACK] Seq=318 Ack=217 Win=64128 Len=0 TSval=2637941990 TSecr=3964055131
22143 125.595700177 34.107.221.82  172.31.31.113  TCP       66 [TCP Keep-Alive ACK] 80 → 37402 [ACK] Seq=217 Ack=319 Win=268800 Len=0 TSval=3964065370 TSecr=2637880460
22939 135.822267472 172.31.31.113  34.107.221.82  TCP       66 [TCP Keep-Alive] 37402 → 80 [ACK] Seq=318 Ack=217 Win=64128 Len=0 TSval=2637952230 TSecr=3964065370
22940 135.836496167 34.107.221.82  172.31.31.113  TCP       66 [TCP Keep-Alive ACK] 80 → 37402 [ACK] Seq=217 Ack=319 Win=268800 Len=0 TSval=3964075611 TSecr=2637880460
23247 146.061961739 172.31.31.113  34.107.221.82  TCP       66 [TCP Keep-Alive] 37402 → 80 [ACK] Seq=318 Ack=217 Win=64128 Len=0 TSval=2637962470 TSecr=3964075611
23248 146.075826422 34.107.221.82  172.31.31.113  TCP       66 [TCP Keep-Alive ACK] 80 → 37402 [ACK] Seq=217 Ack=319 Win=268800 Len=0 TSval=3964085850 TSecr=2637880460
```

4) dns (filters dns traffic)



```
dns
No.   Time          Source          Destination     Protocol Length Info
 505 10.737110696  172.31.31.113   172.16.100.141  DNS       81 Standard query 0xe383 AAAA iitj.ac.in OPT
 509 10.744139756  172.16.100.141  172.31.31.113   DNS      127 Standard query response 0xe383 AAAA iitj.ac.in SOA dns1.iitj.ac.in OPT
 569 10.816977096  172.31.31.113   172.16.100.141  DNS       95 Standard query 0xc8c0 A www.googletagmanager.com OPT
 571 10.818245485  172.31.31.113   172.16.100.141  DNS       86 Standard query 0xd4ec A code.jquery.com OPT
 572 10.818370655  172.31.31.113   172.16.100.141  DNS       86 Standard query 0xc27b AAAA code.jquery.com OPT
 603 10.862885560  172.16.100.141  172.31.31.113   DNS      516 Standard query response 0xc27b AAAA code.jquery.com AAAA 2a04:4e42:200::649 AAAA 2a04:4e42:600::649 AAAA 2a04:4e42::649 AA…
 607 10.893251199  172.16.100.141  172.31.31.113   DNS      468 Standard query response 0xd4ec A code.jquery.com A 151.101.2.137 A 151.101.66.137 A 151.101.130.137 A 151.101.194.137 NS g…
 646 10.944987535  172.16.100.141  172.31.31.113   DNS      366 Standard query response 0xc8c0 A www.googletagmanager.com A 142.250.194.232 NS ns4.google.com NS ns2.google.com NS ns3.goo…
 833 12.926787723  172.31.31.113   172.16.100.141  DNS       95 Standard query 0x4b59 HTTPS www.googletagmanager.com OPT
 834 12.927050501  172.31.31.113   172.16.100.141  DNS       86 Standard query 0x11c8 HTTPS code.jquery.com OPT
 835 12.927788090  172.31.31.113   172.16.100.141  DNS       90 Standard query 0x4cd6 HTTPS ajax.googleapis.com OPT
 836 12.928164134  172.31.31.113   172.16.100.141  DNS       81 Standard query 0xd957 AAAA iitj.ac.in OPT
 838 12.930694665  172.16.100.141  172.31.31.113   DNS      127 Standard query response 0xd957 AAAA iitj.ac.in SOA dns1.iitj.ac.in OPT
 839 12.930694969  172.16.100.141  172.31.31.113   DNS      147 Standard query response 0x11c8 HTTPS code.jquery.com SOA george.ns.cloudflare.com OPT
 982 13.065788688  172.16.100.141  172.31.31.113   DNS      152 Standard query response 0x4b59 HTTPS www.googletagmanager.com SOA ns1.google.com OPT
 983 13.065788783  172.16.100.141  172.31.31.113   DNS      147 Standard query response 0x4cd6 HTTPS ajax.googleapis.com SOA ns1.google.com OPT
1769 16.992784115  172.31.31.113   172.16.100.141  DNS       86 Standard query 0xb175 HTTPS play.google.com OPT
1774 17.001337081  172.16.100.141  172.31.31.113   DNS      136 Standard query response 0xb175 HTTPS play.google.com SOA ns1.google.com OPT
3405 63.925332826  172.31.31.113   172.16.100.141  DNS       90 Standard query 0xe5b9 HTTPS support.mozilla.org OPT
3406 63.925487233  172.31.31.113   172.16.100.141  DNS       90 Standard query 0xf1bc A support.mozilla.org OPT
3407 63.925586997  172.31.31.113   172.16.100.141  DNS       90 Standard query 0x2154 AAAA support.mozilla.org OPT
3408 63.950102796  172.31.31.113   172.16.100.141  DNS       89 Standard query 0x71e2 HTTPS cloudflare-dns.com OPT
3409 63.950320554  172.31.31.113   172.16.100.141  DNS       82 Standard query 0xa966 A example.org OPT
```

5)

ANS 4:

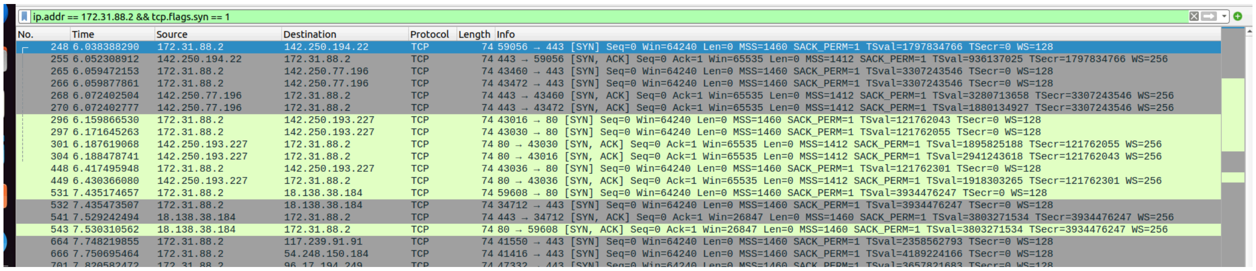
To list all outgoing traffic we use :

ip.src==172.31.88.2

172.31.88.2 - is the ip address of my machine

So this filters out all the packets where the source ip address is my machine's ip address which is basically the outgoing traffic.

6)



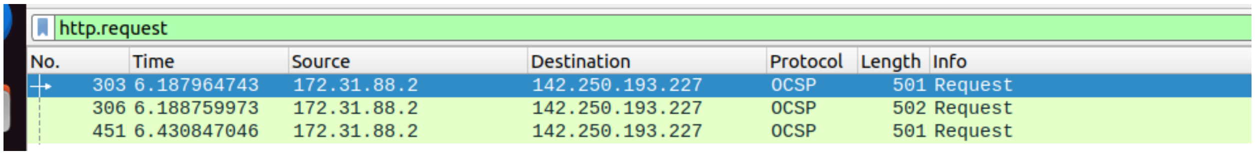
```
ip.addr == 172.31.88.2 && tcp.flags.syn == 1
No.  Time         Source           Destination      Protocol Length Info
 248 6.038388290  172.31.88.2      142.250.194.22   TCP       74 59056 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1797834766 TSecr=0 WS=128
 255 6.052308912  142.250.194.22   172.31.88.2      TCP       74 443 → 59056 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM=1 TSval=936137025 TSecr=1797834766 WS=256
 265 6.059472153  172.31.88.2      142.250.77.196   TCP       74 43460 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3307243546 TSecr=0 WS=128
 266 6.059877861  172.31.88.2      142.250.77.196   TCP       74 43472 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3307243546 TSecr=0 WS=128
 268 6.072402504  142.250.77.196   172.31.88.2      TCP       74 443 → 43460 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM=1 TSval=3280713658 TSecr=3307243546 WS=256
 270 6.072402777  142.250.77.196   172.31.88.2      TCP       74 443 → 43472 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM=1 TSval=1880134927 TSecr=3307243546 WS=256
 296 6.159866530  172.31.88.2      142.250.193.227  TCP       74 43016 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=121762043 TSecr=0 WS=128
 297 6.171645263  172.31.88.2      142.250.193.227  TCP       74 43030 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=121762055 TSecr=0 WS=128
 301 6.187619068  142.250.193.227  172.31.88.2      TCP       74 80 → 43030 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM=1 TSval=1895825188 TSecr=121762055 WS=256
 304 6.188478741  142.250.193.227  172.31.88.2      TCP       74 80 → 43016 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM=1 TSval=2941243618 TSecr=121762043 WS=256
 448 6.417495948  172.31.88.2      142.250.193.227  TCP       74 43036 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=121762301 TSecr=0 WS=128
 449 6.430366080  142.250.193.227  172.31.88.2      TCP       74 80 → 43036 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM=1 TSval=1918303265 TSecr=121762301 WS=256
 531 7.435174657  172.31.88.2      18.138.38.184    TCP       74 59608 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3934476247 TSecr=0 WS=128
 532 7.435473507  172.31.88.2      18.138.38.184    TCP       74 34712 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3934476247 TSecr=0 WS=128
 541 7.529242494  18.138.38.184    172.31.88.2      TCP       74 443 → 34712 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1460 SACK_PERM=1 TSval=3803271534 TSecr=3934476247 WS=256
 543 7.530310562  18.138.38.184    172.31.88.2      TCP       74 80 → 59608 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1460 SACK_PERM=1 TSval=3803271534 TSecr=3934476247 WS=256
 664 7.748219855  172.31.88.2      117.239.91.91    TCP       74 41550 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2358562793 TSecr=0 WS=128
 666 7.750695464  172.31.88.2      54.248.150.184   TCP       74 41416 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4189224166 TSecr=0 WS=128
 701 7.820582472  172.31.88.2      96.17.194.249    TCP       74 47332 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3657821683 TSecr=0 WS=128
```

Used the display filter:

ip.addr == 172.31.88.2 && tcp.flags.syn == 1

To view the 3 way handshake protocol

IITJ Proxy: ip address: 142.250.193.227



http.request

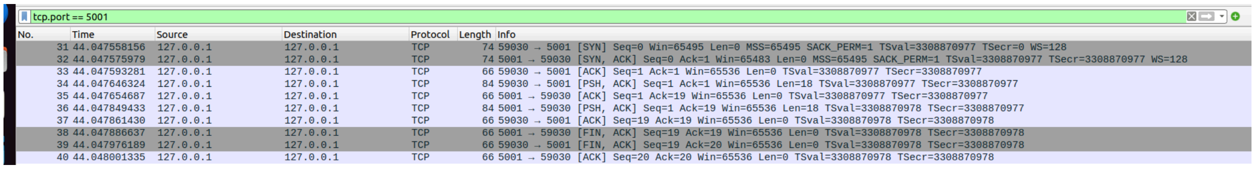
No.	Time	Source	Destination	Protocol	Length	Info
303	6.187964743	172.31.88.2	142.250.193.227	OCSP	501	Request
306	6.188759973	172.31.88.2	142.250.193.227	OCSP	502	Request
451	6.430847046	172.31.88.2	142.250.193.227	OCSP	501	Request

7)
DNS converts the human friendly domain name into IP Address and uses UDP as:

- UDP is fast and provides connectionless delivery
- Although it does not not guarantee delivery and order of delivery but for a use case like getting the ip address , real time response is preferred over reliable delivery.

HTTP is used to load web pages which include images, videos and pages.
So, reliability of loading is more important than the speed of delivery.
Hence, it uses TCP protocol which provides connection oriented, reliable and ordered delivery of packets.

8)



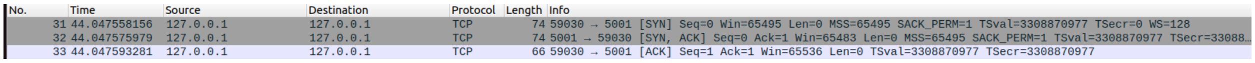
tcp.port == 5001

No.	Time	Source	Destination	Protocol	Length	Info
31	44.047558156	127.0.0.1	127.0.0.1	TCP	74	59030 → 5001 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=3308870977 TSecr=0 WS=128
32	44.047575979	127.0.0.1	127.0.0.1	TCP	74	5001 → 59030 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=3308870977 TSecr=3308870977 WS=128
33	44.047593281	127.0.0.1	127.0.0.1	TCP	66	59030 → 5001 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=3308870977 TSecr=3308870977
34	44.047646324	127.0.0.1	127.0.0.1	TCP	84	59030 → 5001 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=18 TSval=3308870977 TSecr=3308870977
35	44.047654687	127.0.0.1	127.0.0.1	TCP	66	5001 → 59030 [ACK] Seq=1 Ack=19 Win=65536 Len=0 TSval=3308870977 TSecr=3308870977
36	44.047849433	127.0.0.1	127.0.0.1	TCP	84	5001 → 59030 [PSH, ACK] Seq=1 Ack=19 Win=65536 Len=18 TSval=3308870978 TSecr=3308870977
37	44.047861430	127.0.0.1	127.0.0.1	TCP	66	59030 → 5001 [ACK] Seq=19 Ack=19 Win=65536 Len=0 TSval=3308870978 TSecr=3308870978
38	44.047886637	127.0.0.1	127.0.0.1	TCP	66	5001 → 59030 [FIN, ACK] Seq=19 Ack=19 Win=65536 Len=0 TSval=3308870978 TSecr=3308870978
39	44.047976189	127.0.0.1	127.0.0.1	TCP	66	59030 → 5001 [FIN, ACK] Seq=19 Ack=20 Win=65536 Len=0 TSval=3308870978 TSecr=3308870978
40	44.048001335	127.0.0.1	127.0.0.1	TCP	66	5001 → 59030 [ACK] Seq=20 Ack=20 Win=65536 Len=0 TSval=3308870978 TSecr=3308870978

The source and destination address are the same ip address: 127.0.0.1 as the server and client are running on the same machine (loopback interface is used for communicating)

Protocol used is TCP
Source port no. 59030
Destination Port no. 5001
Following are the parts of communication taking place between the server and client:

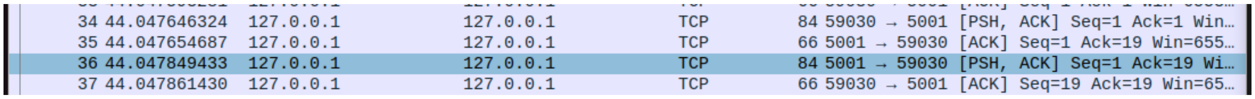
- ❖ 3 way handshake to establish connection between server and client is as follows:



No.	Time	Source	Destination	Protocol	Length	Info
31	44.047558156	127.0.0.1	127.0.0.1	TCP	74	59030 → 5001 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=3308870977 TSecr=0 WS=128
32	44.047575979	127.0.0.1	127.0.0.1	TCP	74	5001 → 59030 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=3308870977 TSecr=33088…
33	44.047593281	127.0.0.1	127.0.0.1	TCP	66	59030 → 5001 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=3308870977 TSecr=3308870977

- A SYN packet from port 59030 to port 5001
- A SYN-ACK packet from port 5001 to 59030
- An ACK packet from port 59030 to 5001

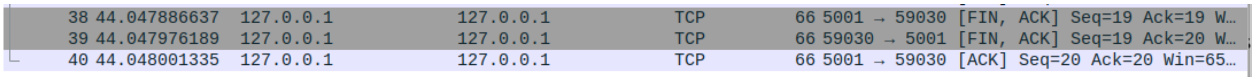
- Data transfer :



```
34 44.047646324  127.0.0.1          127.0.0.1          TCP       84 59030 → 5001 [PSH, ACK] Seq=1 Ack=1 Win…
35 44.047654687  127.0.0.1          127.0.0.1          TCP       66 5001 → 59030 [ACK] Seq=1 Ack=19 Win=655…
36 44.047849433  127.0.0.1          127.0.0.1          TCP       84 5001 → 59030 [PSH, ACK] Seq=1 Ack=19 Wi…
37 44.047861430  127.0.0.1          127.0.0.1          TCP       66 59030 → 5001 [ACK] Seq=19 Ack=19 Win=65…
```

  - PSH indicates data being pushed over the connection.
  - ACK is to acknowledge the data received.

- Terminate Connection:



```
38 44.047886637  127.0.0.1          127.0.0.1          TCP       66 5001 → 59030 [FIN, ACK] Seq=19 Ack=19 W…
39 44.047976189  127.0.0.1          127.0.0.1          TCP       66 59030 → 5001 [FIN, ACK] Seq=19 Ack=20 W…
40 44.048001335  127.0.0.1          127.0.0.1          TCP       66 5001 → 59030 [ACK] Seq=20 Ack=20 Win=65…
```

  - FIN ACK to terminate the connection