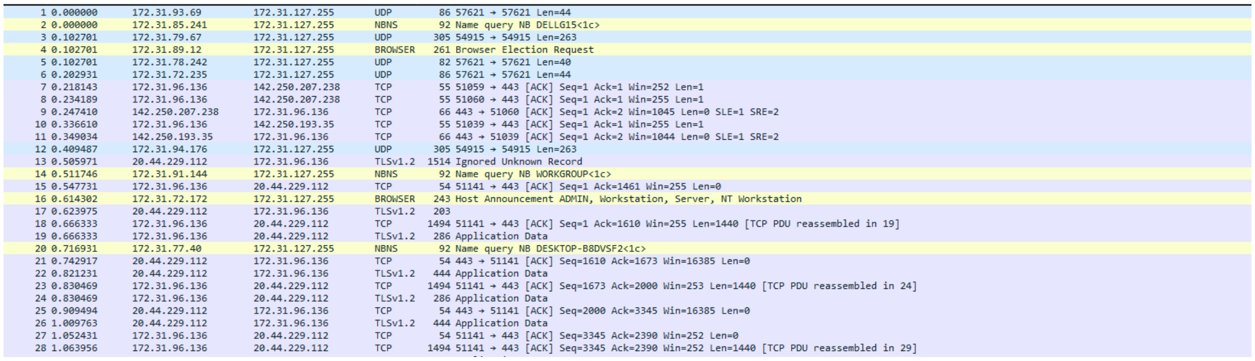
CyberSecurity Lab3

Soumen Kumar
B22ES006

1. Start packet capture in Wireshark on your wireless interface. What do you observe?



```
 1 0.000000   172.31.93.69     172.31.127.255   UDP        86 57621 → 57621 Len=44
 2 0.000000   172.31.85.241    172.31.127.255   NBNS       92 Name query NB DELLG15<1c>
 3 0.102701   172.31.79.67     172.31.127.255   UDP       305 54915 → 54915 Len=263
 4 0.102701   172.31.89.12     172.31.127.255   BROWSER   261 Browser Election Request
 5 0.102701   172.31.78.242    172.31.127.255   UDP        82 57621 → 57621 Len=40
 6 0.202931   172.31.72.235    172.31.127.255   UDP        86 57621 → 57621 Len=44
 7 0.218143   172.31.96.136    142.250.207.238  TCP        55 51059 → 443 [ACK] Seq=1 Ack=1 Win=252 Len=1
 8 0.234189   172.31.96.136    142.250.207.238  TCP        55 51060 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
 9 0.247410   142.250.207.238  172.31.96.136    TCP        66 443 → 51060 [ACK] Seq=1 Ack=2 Win=1045 Len=0 SLE=1 SRE=2
10 0.336610   172.31.96.136    142.250.193.35   TCP        55 51039 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
11 0.349034   142.250.193.35   172.31.96.136    TCP        66 443 → 51039 [ACK] Seq=1 Ack=2 Win=1044 Len=0 SLE=1 SRE=2
12 0.409487   172.31.94.176    172.31.127.255   UDP       305 54915 → 54915 Len=263
13 0.505971   20.44.229.112    172.31.96.136    TLSv1.2  1514 Ignored Unknown Record
14 0.511746   172.31.91.144    172.31.127.255   NBNS       92 Name query NB WORKGROUP<1c>
15 0.547731   172.31.96.136    20.44.229.112    TCP        54 51141 → 443 [ACK] Seq=1 Ack=1461 Win=255 Len=0
16 0.614302   172.31.72.172    172.31.127.255   BROWSER   243 Host Announcement ADMIN, Workstation, Server, NT Workstation
17 0.623975   20.44.229.112    172.31.96.136    TLSv1.2   203
18 0.666333   172.31.96.136    20.44.229.112    TCP      1494 51141 → 443 [ACK] Seq=1 Ack=1610 Win=255 Len=1440 [TCP PDU reassembled in 19]
19 0.666333   172.31.96.136    20.44.229.112    TLSv1.2   286 Application Data
20 0.716931   172.31.77.40     172.31.127.255   NBNS       92 Name query NB DESKTOP-B8DVSF2<1c>
21 0.742917   20.44.229.112    172.31.96.136    TCP        54 443 → 51141 [ACK] Seq=1610 Ack=1673 Win=16385 Len=0
22 0.821231   20.44.229.112    172.31.96.136    TLSv1.2   444 Application Data
23 0.830469   172.31.96.136    20.44.229.112    TCP      1494 51141 → 443 [ACK] Seq=1673 Ack=2000 Win=253 Len=1440 [TCP PDU reassembled in 24]
24 0.830469   172.31.96.136    20.44.229.112    TLSv1.2   286 Application Data
25 0.909494   20.44.229.112    172.31.96.136    TCP        54 443 → 51141 [ACK] Seq=2000 Ack=3345 Win=16385 Len=0
26 1.009763   20.44.229.112    172.31.96.136    TLSv1.2   444 Application Data
27 1.052431   172.31.96.136    20.44.229.112    TCP        54 51141 → 443 [ACK] Seq=3345 Ack=2390 Win=252 Len=0
28 1.063956   172.31.96.136    20.44.229.112    TCP      1494 51141 → 443 [ACK] Seq=3345 Ack=2390 Win=252 Len=1440 [TCP PDU reassembled in 29]
```

Ans- Initially after opening the capture interface over wifi,some packets are getting displayed which indicates some background network activity even when no specific application or browser is opened.

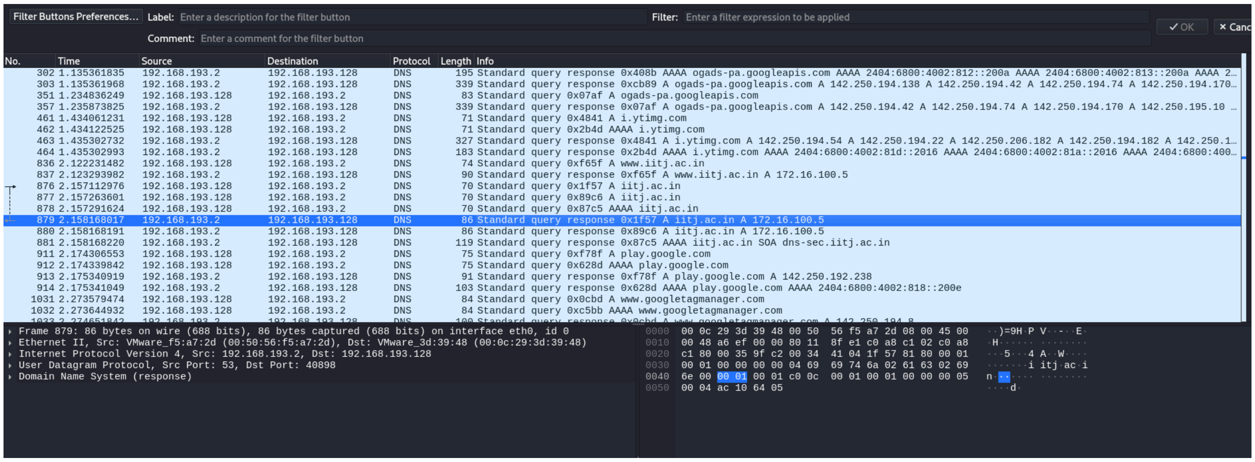
Possible reasons for this:

1. Operating systems and services often run processes in the background.
2. Local network discovery protocols like ARP, NBNS, and BROWSER are constantly active.
3. System telemetry or updates may communicate with external servers using secure protocols

2. Now visit a local website, say www.iitj.ac.in. Subsequently stop the packet capture and record your observations. Are you able to see the DNS request? What about TCP and HTTP? What is the IP address of the IITJ server? Are you able to see different HTTP requests/responses? Please justify your answer with relevant screenshots.

Ans-

1. DNS Request: Yes, DNS queries for www.iitj.ac.in are visible, resolving to IP address 172.16.100.5.
2. TCP Handshake: The three-way handshake (SYN, SYN-ACK, ACK) is clearly observed.
3. HTTP Traffic: Multiple HTTP GET requests and corresponding responses are captured, showing successful communication with the IITJ server
4. **IP Address of IITJ Server:172.16.100.5**

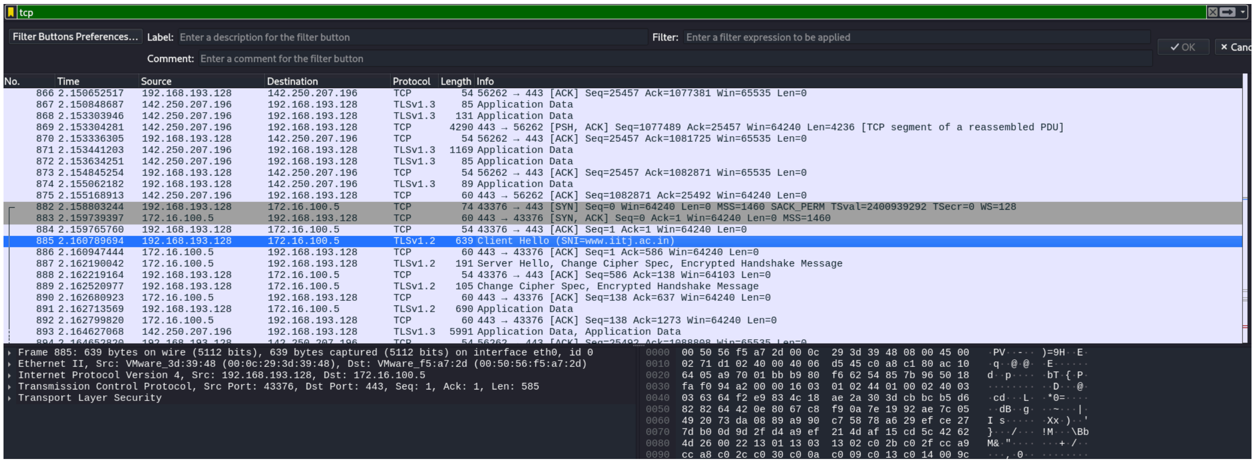

Filter Buttons Preferences…
Label: Enter a description for the filter button
Filter: Enter a filter expression to be applied
✓ OK
× Canc
Comment: Enter a comment for the filter button

```
No.     Time        Source           Destination      Protocol Length Info
    302 1.135361835 192.168.193.2    192.168.193.128  DNS      195 Standard query response 0x408b AAAA ogads-pa.googleapis.com AAAA 2404:6800:4002:812::200a AAAA 2404:6800:4002:813::200a AAAA 2…
    303 1.135361968 192.168.193.2    192.168.193.128  DNS      339 Standard query response 0xcb89 A ogads-pa.googleapis.com A 142.250.194.138 A 142.250.194.42 A 142.250.194.74 A 142.250.194.170…
    351 1.234836249 192.168.193.128  192.168.193.2    DNS       83 Standard query 0x07af A ogads-pa.googleapis.com
    357 1.235873825 192.168.193.2    192.168.193.128  DNS      339 Standard query response 0x07af A ogads-pa.googleapis.com A 142.250.194.42 A 142.250.194.74 A 142.250.194.170 A 142.250.195.10 …
    461 1.434061231 192.168.193.128  192.168.193.2    DNS       71 Standard query 0x4841 A i.ytimg.com
    462 1.434122525 192.168.193.128  192.168.193.2    DNS       71 Standard query 0x2b4d AAAA i.ytimg.com
    463 1.435302732 192.168.193.2    192.168.193.128  DNS      327 Standard query response 0x4841 A i.ytimg.com A 142.250.194.54 A 142.250.194.22 A 142.250.206.182 A 142.250.194.182 A 142.250.1…
    464 1.435302993 192.168.193.2    192.168.193.128  DNS      183 Standard query response 0x2b4d AAAA i.ytimg.com AAAA 2404:6800:4002:81d::2016 AAAA 2404:6800:4002:81a::2016 AAAA 2404:6800:400…
    836 2.122231482 192.168.193.128  192.168.193.2    DNS       74 Standard query 0xf65f A www.iitj.ac.in
    837 2.123293982 192.168.193.2    192.168.193.128  DNS       90 Standard query response 0xf65f A www.iitj.ac.in A 172.16.100.5
    876 2.157112976 192.168.193.128  192.168.193.2    DNS       70 Standard query 0x1f57 A iitj.ac.in
    877 2.157263601 192.168.193.128  192.168.193.2    DNS       70 Standard query 0x89c6 A iitj.ac.in
    878 2.157291624 192.168.193.128  192.168.193.2    DNS       70 Standard query 0x87c5 AAAA iitj.ac.in
    879 2.158168017 192.168.193.2    192.168.193.128  DNS       86 Standard query response 0x1f57 A iitj.ac.in A 172.16.100.5
    880 2.158168191 192.168.193.2    192.168.193.128  DNS       86 Standard query response 0x89c6 A iitj.ac.in A 172.16.100.5
    881 2.158168220 192.168.193.2    192.168.193.128  DNS      119 Standard query response 0x87c5 AAAA iitj.ac.in SOA dns-sec.iitj.ac.in
    911 2.174306553 192.168.193.128  192.168.193.2    DNS       75 Standard query 0xf78f A play.google.com
    912 2.174339842 192.168.193.128  192.168.193.2    DNS       75 Standard query 0x628d AAAA play.google.com
    913 2.175340919 192.168.193.2    192.168.193.128  DNS       91 Standard query response 0xf78f A play.google.com A 142.250.192.238
    914 2.175341049 192.168.193.2    192.168.193.128  DNS      103 Standard query response 0x628d AAAA play.google.com AAAA 2404:6800:4002:818::200e
   1031 2.273579474 192.168.193.128  192.168.193.2    DNS       84 Standard query 0x0cbd A www.googletagmanager.com
   1032 2.273644932 192.168.193.128  192.168.193.2    DNS       84 Standard query 0xc5bb AAAA www.googletagmanager.com
   1033 2.274651842 192.168.193.2    192.168.193.128  DNS      100 Standard query response 0x0cbd A www.googletagmanager.com A 142.250.194.8
```

```
› Frame 879: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_f5:a7:2d (00:50:56:f5:a7:2d), Dst: VMware_3d:39:48 (00:0c:29:3d:39:48)
› Internet Protocol Version 4, Src: 192.168.193.2, Dst: 192.168.193.128
› User Datagram Protocol, Src Port: 53, Dst Port: 40898
› Domain Name System (response)
```

```
0000  00 0c 29 3d 39 48 00 50  56 f5 a7 2d 08 00 45 00   ··)=9H·P V··-··E·
0010  00 48 a6 ef 00 00 80 11  8f e1 c0 a8 c1 02 c0 a8   ·H······ ········
0020  c1 80 00 35 9f c2 00 34  41 04 1f 57 81 80 00 01   ···5···4 A··W····
0030  00 01 00 00 00 00 04 69  69 74 6a 02 61 63 02 69   ·······i itj·ac·i
0040  6e 00 00 01 00 01 c0 0c  00 01 00 01 00 00 00 05   n······· ········
0050  00 04 ac 10 64 05                                  ····d·
```

DNS

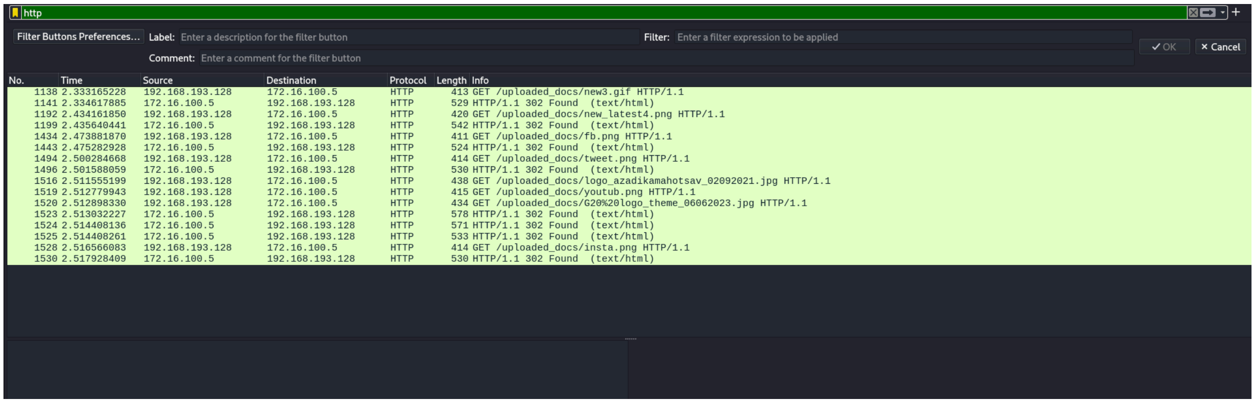

tcp
Filter Buttons Preferences…
Label: Enter a description for the filter button
Filter: Enter a filter expression to be applied
✓ OK
× Canc
Comment: Enter a comment for the filter button

```
No.     Time        Source           Destination      Protocol Length Info
    866 2.150652517 192.168.193.128  142.250.207.196  TCP       54 56262 → 443 [ACK] Seq=25457 Ack=1077381 Win=65535 Len=0
    867 2.150848687 142.250.207.196  192.168.193.128  TLSv1.3   85 Application Data
    868 2.153303946 142.250.207.196  192.168.193.128  TLSv1.3  131 Application Data
    869 2.153304281 142.250.207.196  192.168.193.128  TCP     4290 443 → 56262 [PSH, ACK] Seq=1077489 Ack=25457 Win=64240 Len=4236 [TCP segment of a reassembled PDU]
    870 2.153336305 192.168.193.128  142.250.207.196  TCP       54 56262 → 443 [ACK] Seq=25457 Ack=1081725 Win=65535 Len=0
    871 2.153441203 142.250.207.196  192.168.193.128  TLSv1.3 1169 Application Data
    872 2.153634251 142.250.207.196  192.168.193.128  TLSv1.3   85 Application Data
    873 2.154845254 192.168.193.128  142.250.207.196  TCP       54 56262 → 443 [ACK] Seq=25457 Ack=1082871 Win=65535 Len=0
    874 2.155062182 192.168.193.128  142.250.207.196  TLSv1.3   89 Application Data
    875 2.155168913 142.250.207.196  192.168.193.128  TCP       60 443 → 56262 [ACK] Seq=1082871 Ack=25492 Win=64240 Len=0
    882 2.158803244 192.168.193.128  172.16.100.5     TCP       74 43376 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2400939292 TSecr=0 WS=128
    883 2.159739397 172.16.100.5     192.168.193.128  TCP       60 443 → 43376 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
    884 2.159765760 192.168.193.128  172.16.100.5     TCP       54 43376 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
    885 2.160789694 192.168.193.128  172.16.100.5     TLSv1.2  639 Client Hello (SNI=www.iitj.ac.in)
    886 2.160947444 172.16.100.5     192.168.193.128  TCP       60 443 → 43376 [ACK] Seq=1 Ack=586 Win=64240 Len=0
    887 2.162190042 172.16.100.5     192.168.193.128  TLSv1.2  191 Server Hello, Change Cipher Spec, Encrypted Handshake Message
    888 2.162219164 192.168.193.128  172.16.100.5     TCP       54 43376 → 443 [ACK] Seq=586 Ack=138 Win=64103 Len=0
    889 2.162520977 192.168.193.128  172.16.100.5     TLSv1.2  105 Change Cipher Spec, Encrypted Handshake Message
    890 2.162680923 172.16.100.5     192.168.193.128  TCP       60 443 → 43376 [ACK] Seq=138 Ack=637 Win=64240 Len=0
    891 2.162713569 192.168.193.128  172.16.100.5     TLSv1.2  690 Application Data
    892 2.162799820 172.16.100.5     192.168.193.128  TCP       60 443 → 43376 [ACK] Seq=138 Ack=1273 Win=64240 Len=0
    893 2.164627068 142.250.207.196  192.168.193.128  TLSv1.3 5991 Application Data, Application Data
    894 2.164652820 192.168.193.128  142.250.207.196  TCP       54 56262 → 443 [ACK] Seq=25492 Ack=1088808 Win=65535 Len=0
```

```
› Frame 885: 639 bytes on wire (5112 bits), 639 bytes captured (5112 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_3d:39:48 (00:0c:29:3d:39:48), Dst: VMware_f5:a7:2d (00:50:56:f5:a7:2d)
› Internet Protocol Version 4, Src: 192.168.193.128, Dst: 172.16.100.5
› Transmission Control Protocol, Src Port: 43376, Dst Port: 443, Seq: 1, Ack: 1, Len: 585
› Transport Layer Security
```

```
0000  00 50 56 f5 a7 2d 00 0c  29 3d 39 48 08 00 45 00   ·PV··-·· )=9H··E·
0010  02 71 d1 02 40 00 40 06  d5 45 c0 a8 c1 80 ac 10   ·q··@·@· ·E······
0020  64 05 a9 70 01 bb b9 80  f6 62 54 85 7b 96 50 18   d··p···· ·bT·{·P·
0030  fa f0 94 a2 00 00 16 03  01 02 44 01 00 02 40 03   ········ ··D···@·
0040  03 63 64 f2 e9 83 4c 18  ae 2a 30 3d cb bc b5 d6   ·cd···L· ·*0=····
0050  82 82 64 42 0e 80 67 c8  f9 0a 7e 19 92 ae 7c 05   ··dB··g· ··~···|·
0060  49 20 73 da 08 89 a9 90  c7 58 78 a6 29 ef ce 27   I s····· ·Xx·)··'
0070  7d b0 0d 9d 2f d4 a9 ef  21 4d af 15 cd 5c 42 62   }···/··· !M···\Bb
0080  4d 26 00 22 13 01 13 03  13 02 c0 2b c0 2f cc a9   M&·"···· ···+·/··
0090  cc a8 c0 2c c0 30 c0 0a  c0 09 c0 13 c0 14 00 9c   ···,·0·· ········
```

TCP


http
Filter Buttons Preferences…
Label: Enter a description for the filter button
Filter: Enter a filter expression to be applied
✓ OK
× Cancel
Comment: Enter a comment for the filter button

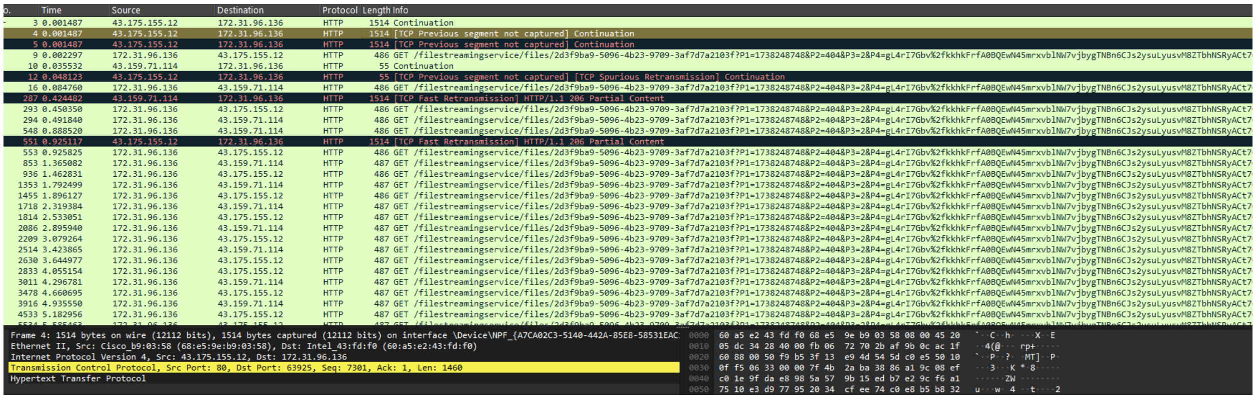
```
No.     Time        Source           Destination      Protocol Length Info
   1138 2.333165228 192.168.193.128  172.16.100.5     HTTP     413 GET /uploaded_docs/new3.gif HTTP/1.1
   1141 2.334617885 172.16.100.5     192.168.193.128  HTTP     529 HTTP/1.1 302 Found  (text/html)
   1192 2.434161850 192.168.193.128  172.16.100.5     HTTP     420 GET /uploaded_docs/new_latest4.png HTTP/1.1
   1199 2.435640441 172.16.100.5     192.168.193.128  HTTP     542 HTTP/1.1 302 Found  (text/html)
   1434 2.473881870 192.168.193.128  172.16.100.5     HTTP     411 GET /uploaded_docs/fb.png HTTP/1.1
   1443 2.475282928 172.16.100.5     192.168.193.128  HTTP     524 HTTP/1.1 302 Found  (text/html)
   1494 2.500284668 192.168.193.128  172.16.100.5     HTTP     414 GET /uploaded_docs/tweet.png HTTP/1.1
   1496 2.501588059 172.16.100.5     192.168.193.128  HTTP     530 HTTP/1.1 302 Found  (text/html)
   1516 2.511555199 192.168.193.128  172.16.100.5     HTTP     438 GET /uploaded_docs/logo_azadikamahotsav_02092021.jpg HTTP/1.1
   1519 2.512779943 192.168.193.128  172.16.100.5     HTTP     415 GET /uploaded_docs/youtub.png HTTP/1.1
   1520 2.512898330 192.168.193.128  172.16.100.5     HTTP     434 GET /uploaded_docs/G20%20logo_theme_06062023.jpg HTTP/1.1
   1523 2.513032227 172.16.100.5     192.168.193.128  HTTP     578 HTTP/1.1 302 Found  (text/html)
   1524 2.514408136 172.16.100.5     192.168.193.128  HTTP     571 HTTP/1.1 302 Found  (text/html)
   1525 2.514408261 172.16.100.5     192.168.193.128  HTTP     533 HTTP/1.1 302 Found  (text/html)
   1528 2.516566083 192.168.193.128  172.16.100.5     HTTP     414 GET /uploaded_docs/insta.png HTTP/1.1
   1530 2.517928409 172.16.100.5     192.168.193.128  HTTP     530 HTTP/1.1 302 Found  (text/html)
```

HTTP

3. What does a packet highlighted in `black' color signify?

Ans-

Packets highlighted in black with red text in Wireshark typically indicate packets with errors. These could be checksum errors, malformed packets, or other issues that Wireshark has detected.



```
o.    Time      Source          Destination     Protocol Length Info
-   3 0.001487  43.175.155.12   172.31.96.136   HTTP     1514 Continuation
    4 0.001487  43.175.155.12   172.31.96.136   HTTP     1514 [TCP Previous segment not captured] Continuation
    5 0.001487  43.175.155.12   172.31.96.136   HTTP     1514 [TCP Previous segment not captured] Continuation
    9 0.002297  172.31.96.136   43.175.155.12   HTTP      486 GET /filestreamingservice/files/2d3f9ba9-5096-4b23-9709-3af7d7a2103f?P1=1738248748&P2=404&P3=2&P4=gL4rI7Gbv%2fkkhkFrfA0BQEwN45mrxvblNW7vjbygTNBn6CJs2ysuLyusvM8ZTbhNSRyACt7
   10 0.035532  43.159.71.114   172.31.96.136   HTTP       55 Continuation
   12 0.048123  43.175.155.12   172.31.96.136   HTTP       55 [TCP Previous segment not captured] [TCP Spurious Retransmission] Continuation
   16 0.084760  172.31.96.136   43.159.71.114   HTTP      486 GET /filestreamingservice/files/2d3f9ba9-5096-4b23-9709-3af7d7a2103f?P1=1738248748&P2=404&P3=2&P4=gL4rI7Gbv%2fkkhkFrfA0BQEwN45mrxvblNW7vjbygTNBn6CJs2ysuLyusvM8ZTbhNSRyACt7
  287 0.424482  43.159.71.114   172.31.96.136   HTTP     1514 [TCP Fast Retransmission] HTTP/1.1 206 Partial Content
  293 0.450350  172.31.96.136   43.175.155.12   HTTP      486 GET /filestreamingservice/files/2d3f9ba9-5096-4b23-9709-3af7d7a2103f?P1=1738248748&P2=404&P3=2&P4=gL4rI7Gbv%2fkkhkFrfA0BQEwN45mrxvblNW7vjbygTNBn6CJs2ysuLyusvM8ZTbhNSRyACt7
  294 0.491840  172.31.96.136   43.159.71.114   HTTP      486 GET /filestreamingservice/files/2d3f9ba9-5096-4b23-9709-3af7d7a2103f?P1=1738248748&P2=404&P3=2&P4=gL4rI7Gbv%2fkkhkFrfA0BQEwN45mrxvblNW7vjbygTNBn6CJs2ysuLyusvM8ZTbhNSRyACt7
  548 0.888520  172.31.96.136   43.159.71.114   HTTP      486 GET /filestreamingservice/files/2d3f9ba9-5096-4b23-9709-3af7d7a2103f?P1=1738248748&P2=404&P3=2&P4=gL4rI7Gbv%2fkkhkFrfA0BQEwN45mrxvblNW7vjbygTNBn6CJs2ysuLyusvM8ZTbhNSRyACt7
  551 0.925117  43.175.155.12   172.31.96.136   HTTP     1514 [TCP Fast Retransmission] HTTP/1.1 206 Partial Content
  553 0.925825  172.31.96.136   43.175.155.12   HTTP      486 GET /filestreamingservice/files/2d3f9ba9-5096-4b23-9709-3af7d7a2103f?P1=1738248748&P2=404&P3=2&P4=gL4rI7Gbv%2fkkhkFrfA0BQEwN45mrxvblNW7vjbygTNBn6CJs2ysuLyusvM8ZTbhNSRyACt7
  853 1.365082  172.31.96.136   43.159.71.114   HTTP      487 GET /filestreamingservice/files/2d3f9ba9-5096-4b23-9709-3af7d7a2103f?P1=1738248748&P2=404&P3=2&P4=gL4rI7Gbv%2fkkhkFrfA0BQEwN45mrxvblNW7vjbygTNBn6CJs2ysuLyusvM8ZTbhNSRyACt7
  936 1.462831  172.31.96.136   43.175.155.12   HTTP      486 GET /filestreamingservice/files/2d3f9ba9-5096-4b23-9709-3af7d7a2103f?P1=1738248748&P2=404&P3=2&P4=gL4rI7Gbv%2fkkhkFrfA0BQEwN45mrxvblNW7vjbygTNBn6CJs2ysuLyusvM8ZTbhNSRyACt7
 1353 1.792499  172.31.96.136   43.159.71.114   HTTP      487 GET /filestreamingservice/files/2d3f9ba9-5096-4b23-9709-3af7d7a2103f?P1=1738248748&P2=404&P3=2&P4=gL4rI7Gbv%2fkkhkFrfA0BQEwN45mrxvblNW7vjbygTNBn6CJs2ysuLyusvM8ZTbhNSRyACt7
 1455 1.896127  172.31.96.136   43.175.155.12   HTTP      486 GET /filestreamingservice/files/2d3f9ba9-5096-4b23-9709-3af7d7a2103f?P1=1738248748&P2=404&P3=2&P4=gL4rI7Gbv%2fkkhkFrfA0BQEwN45mrxvblNW7vjbygTNBn6CJs2ysuLyusvM8ZTbhNSRyACt7
 1718 2.319384  172.31.96.136   43.159.71.114   HTTP      487 GET /filestreamingservice/files/2d3f9ba9-5096-4b23-9709-3af7d7a2103f?P1=1738248748&P2=404&P3=2&P4=gL4rI7Gbv%2fkkhkFrfA0BQEwN45mrxvblNW7vjbygTNBn6CJs2ysuLyusvM8ZTbhNSRyACt7
 1814 2.533051  172.31.96.136   43.175.155.12   HTTP      487 GET /filestreamingservice/files/2d3f9ba9-5096-4b23-9709-3af7d7a2103f?P1=1738248748&P2=404&P3=2&P4=gL4rI7Gbv%2fkkhkFrfA0BQEwN45mrxvblNW7vjbygTNBn6CJs2ysuLyusvM8ZTbhNSRyACt7
 2086 2.895940  172.31.96.136   43.159.71.114   HTTP      487 GET /filestreamingservice/files/2d3f9ba9-5096-4b23-9709-3af7d7a2103f?P1=1738248748&P2=404&P3=2&P4=gL4rI7Gbv%2fkkhkFrfA0BQEwN45mrxvblNW7vjbygTNBn6CJs2ysuLyusvM8ZTbhNSRyACt7
 2209 3.079264  172.31.96.136   43.175.155.12   HTTP      487 GET /filestreamingservice/files/2d3f9ba9-5096-4b23-9709-3af7d7a2103f?P1=1738248748&P2=404&P3=2&P4=gL4rI7Gbv%2fkkhkFrfA0BQEwN45mrxvblNW7vjbygTNBn6CJs2ysuLyusvM8ZTbhNSRyACt7
 2514 3.423865  172.31.96.136   43.159.71.114   HTTP      487 GET /filestreamingservice/files/2d3f9ba9-5096-4b23-9709-3af7d7a2103f?P1=1738248748&P2=404&P3=2&P4=gL4rI7Gbv%2fkkhkFrfA0BQEwN45mrxvblNW7vjbygTNBn6CJs2ysuLyusvM8ZTbhNSRyACt7
 2630 3.644977  172.31.96.136   43.175.155.12   HTTP      487 GET /filestreamingservice/files/2d3f9ba9-5096-4b23-9709-3af7d7a2103f?P1=1738248748&P2=404&P3=2&P4=gL4rI7Gbv%2fkkhkFrfA0BQEwN45mrxvblNW7vjbygTNBn6CJs2ysuLyusvM8ZTbhNSRyACt7
 2833 4.055154  172.31.96.136   43.175.155.12   HTTP      487 GET /filestreamingservice/files/2d3f9ba9-5096-4b23-9709-3af7d7a2103f?P1=1738248748&P2=404&P3=2&P4=gL4rI7Gbv%2fkkhkFrfA0BQEwN45mrxvblNW7vjbygTNBn6CJs2ysuLyusvM8ZTbhNSRyACt7
 3011 4.296781  172.31.96.136   43.159.71.114   HTTP      487 GET /filestreamingservice/files/2d3f9ba9-5096-4b23-9709-3af7d7a2103f?P1=1738248748&P2=404&P3=2&P4=gL4rI7Gbv%2fkkhkFrfA0BQEwN45mrxvblNW7vjbygTNBn6CJs2ysuLyusvM8ZTbhNSRyACt7
 3478 4.660695  172.31.96.136   43.175.155.12   HTTP      487 GET /filestreamingservice/files/2d3f9ba9-5096-4b23-9709-3af7d7a2103f?P1=1738248748&P2=404&P3=2&P4=gL4rI7Gbv%2fkkhkFrfA0BQEwN45mrxvblNW7vjbygTNBn6CJs2ysuLyusvM8ZTbhNSRyACt7
 3916 4.935550  172.31.96.136   43.159.71.114   HTTP      487 GET /filestreamingservice/files/2d3f9ba9-5096-4b23-9709-3af7d7a2103f?P1=1738248748&P2=404&P3=2&P4=gL4rI7Gbv%2fkkhkFrfA0BQEwN45mrxvblNW7vjbygTNBn6CJs2ysuLyusvM8ZTbhNSRyACt7
 4533 5.182956  172.31.96.136   43.175.155.12   HTTP      487 GET /filestreamingservice/files/2d3f9ba9-5096-4b23-9709-3af7d7a2103f?P1=1738248748&P2=404&P3=2&P4=gL4rI7Gbv%2fkkhkFrfA0BQEwN45mrxvblNW7vjbygTNBn6CJs2ysuLyusvM8ZTbhNSRyACt7
 5534 5.585463  172.31.96.136   43.175.155.12   HTTP      487 GET /filestreamingservice/files/2d3f9ba9-5096-4b23-9709-3af7d7a2103f?P1=1738248748&P2=404&P3=2&P4=gL4rI7Gbv%2fkkhkFrfA0BQEwN45mrxvblNW7vjbygTNBn6CJs2ysuLyusvM8ZTbhNSRyACt7
```

```
Frame 4: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{A7CA02C3-5140-442A-85E8-58531EAC
Ethernet II, Src: Cisco_b9:03:58 (68:e5:9e:b9:03:58), Dst: Intel_43:fd:f0 (60:a5:e2:43:fd:f0)
Internet Protocol Version 4, Src: 43.175.155.12, Dst: 172.31.96.136
Transmission Control Protocol, Src Port: 80, Dst Port: 63925, Seq: 7301, Ack: 1, Len: 1460
Hypertext Transfer Protocol
```

```
0000  60 a5 e2 43 fd f0 68 e5  9e b9 03 58 08 00 45 20   `··C··h· ···X··E
0010  05 dc 34 28 40 00 fb 06  72 70 2b af 9b 0c ac 1f   ··4(@··· rp+·····
0020  60 88 00 50 f9 b5 3f 13  e9 4d 54 5d c0 e5 50 10   `··P··?· ·MT]··P·
0030  0f f5 06 33 00 00 7f 4b  2a ba 38 86 a1 9c 08 ef   ···3···K *·8·····
0040  c0 1e 9f da e8 98 5a 57  9b 15 ed b7 e2 9c f6 a1   ······ZW ········
0050  75 10 e3 d9 77 95 20 34  cf ee 74 c0 e8 b5 b8 32   u···w· 4 ··t····2
```

4. Explore at least 5 different filters in Wireshark.

Ans-

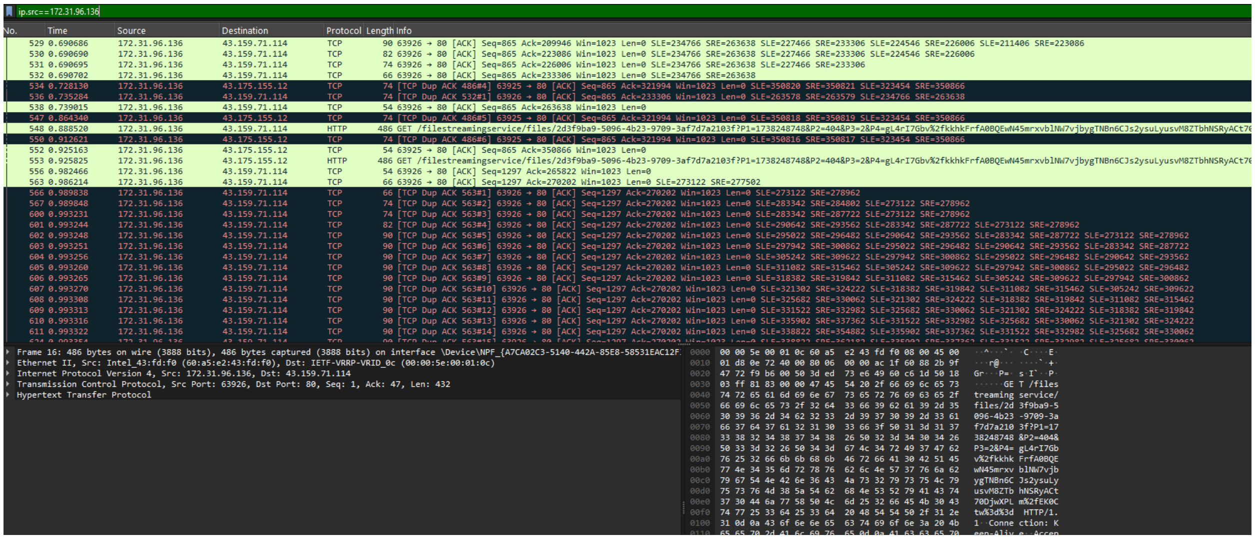
1. ip.addr == 192.xxx.x.x: Shows packets with the specified IP address as source or destination
2. tcp.port == 80: Displays only HTTP traffic
3. dns: Shows only DNS traffic
4. http.request.method == "GET": Displays only HTTP GET requests
5. frame contains "password": Shows packets containing the word "password"

5. What is the filter command for listing all outgoing traffic?

Ans-

To list all outgoing traffic, we can use the following display filter:

ip.src == [system’s_ip_address]



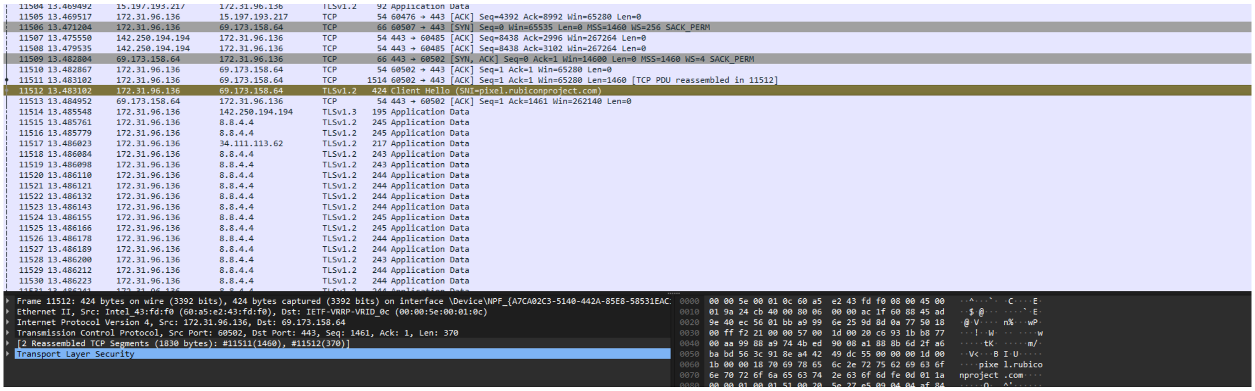
```
ip.src==172.31.96.136

No.  Time      Source         Destination     Protocol Length Info
 529 0.690686  172.31.96.136  43.159.71.114   TCP      90 63926 → 80 [ACK] Seq=865 Ack=209946 Win=1023 Len=0 SLE=234766 SRE=263638 SLE=227466 SRE=233306 SLE=224546 SRE=226006 SLE=211406 SRE=223086
 530 0.690690  172.31.96.136  43.159.71.114   TCP      82 63926 → 80 [ACK] Seq=865 Ack=223086 Win=1023 Len=0 SLE=234766 SRE=263638 SLE=227466 SRE=233306 SLE=224546 SRE=226006
 531 0.690695  172.31.96.136  43.159.71.114   TCP      74 63926 → 80 [ACK] Seq=865 Ack=226006 Win=1023 Len=0 SLE=234766 SRE=263638 SLE=227466 SRE=233306
 532 0.690702  172.31.96.136  43.159.71.114   TCP      66 63926 → 80 [ACK] Seq=865 Ack=233306 Win=1023 Len=0 SLE=234766 SRE=263638
 534 0.728130  172.31.96.136  43.175.155.12   TCP      74 [TCP Dup ACK 486#4] 63925 → 80 [ACK] Seq=865 Ack=321994 Win=1023 Len=0 SLE=350820 SRE=350821 SLE=323454 SRE=350866
 536 0.735284  172.31.96.136  43.159.71.114   TCP      74 [TCP Dup ACK 532#1] 63926 → 80 [ACK] Seq=865 Ack=233306 Win=1023 Len=0 SLE=263578 SRE=263579 SLE=234766 SRE=263638
 538 0.739015  172.31.96.136  43.159.71.114   TCP      54 63926 → 80 [ACK] Seq=865 Ack=263638 Win=1023 Len=0
 547 0.864340  172.31.96.136  43.175.155.12   TCP      74 [TCP Dup ACK 486#5] 63925 → 80 [ACK] Seq=865 Ack=321994 Win=1023 Len=0 SLE=350818 SRE=350819 SLE=323454 SRE=350866
 548 0.888520  172.31.96.136  43.159.71.114   HTTP    486 GET /filestreamingservice/files/2d3f9ba9-5096-4b23-9709-3af7d7a2103f?P1=1738248748&P2=404&P3=2&P4=gL4rI7Gbv%2fkkhkFrfA0BQEwN45mrxvblNW7vjbygTNBn6CJs2ysuLyusvM8ZTbhNSRyACt7
 550 0.912621  172.31.96.136  43.175.155.12   TCP      74 [TCP Dup ACK 486#6] 63925 → 80 [ACK] Seq=865 Ack=321994 Win=1023 Len=0 SLE=350816 SRE=350817 SLE=323454 SRE=350866
 552 0.925163  172.31.96.136  43.175.155.12   TCP      54 63925 → 80 [ACK] Seq=865 Ack=350866 Win=1023 Len=0
 553 0.925825  172.31.96.136  43.175.155.12   HTTP    486 GET /filestreamingservice/files/2d3f9ba9-5096-4b23-9709-3af7d7a2103f?P1=1738248748&P2=404&P3=2&P4=gL4rI7Gbv%2fkkhkFrfA0BQEwN45mrxvblNW7vjbygTNBn6CJs2ysuLyusvM8ZTbhNSRyACt7
 556 0.982466  172.31.96.136  43.159.71.114   TCP      54 63926 → 80 [ACK] Seq=1297 Ack=265822 Win=1023 Len=0
 563 0.986214  172.31.96.136  43.159.71.114   TCP      66 63926 → 80 [ACK] Seq=1297 Ack=270202 Win=1023 Len=0 SLE=273122 SRE=277502
 566 0.989838  172.31.96.136  43.159.71.114   TCP      66 [TCP Dup ACK 563#1] 63926 → 80 [ACK] Seq=1297 Ack=270202 Win=1023 Len=0 SLE=273122 SRE=278962
 567 0.989848  172.31.96.136  43.159.71.114   TCP      74 [TCP Dup ACK 563#2] 63926 → 80 [ACK] Seq=1297 Ack=270202 Win=1023 Len=0 SLE=283342 SRE=284802 SLE=273122 SRE=278962
 600 0.993231  172.31.96.136  43.159.71.114   TCP      74 [TCP Dup ACK 563#3] 63926 → 80 [ACK] Seq=1297 Ack=270202 Win=1023 Len=0 SLE=283342 SRE=287722 SLE=273122 SRE=278962
 601 0.993244  172.31.96.136  43.159.71.114   TCP      82 [TCP Dup ACK 563#4] 63926 → 80 [ACK] Seq=1297 Ack=270202 Win=1023 Len=0 SLE=290642 SRE=293562 SLE=283342 SRE=287722 SLE=273122 SRE=278962
 602 0.993248  172.31.96.136  43.159.71.114   TCP      90 [TCP Dup ACK 563#5] 63926 → 80 [ACK] Seq=1297 Ack=270202 Win=1023 Len=0 SLE=295022 SRE=296482 SLE=290642 SRE=293562 SLE=283342 SRE=287722 SLE=273122 SRE=278962
 603 0.993251  172.31.96.136  43.159.71.114   TCP      90 [TCP Dup ACK 563#6] 63926 → 80 [ACK] Seq=1297 Ack=270202 Win=1023 Len=0 SLE=297942 SRE=300862 SLE=295022 SRE=296482 SLE=290642 SRE=293562 SLE=283342 SRE=287722
 604 0.993256  172.31.96.136  43.159.71.114   TCP      90 [TCP Dup ACK 563#7] 63926 → 80 [ACK] Seq=1297 Ack=270202 Win=1023 Len=0 SLE=305242 SRE=309622 SLE=297942 SRE=300862 SLE=295022 SRE=296482 SLE=290642 SRE=293562
 605 0.993260  172.31.96.136  43.159.71.114   TCP      90 [TCP Dup ACK 563#8] 63926 → 80 [ACK] Seq=1297 Ack=270202 Win=1023 Len=0 SLE=311082 SRE=315462 SLE=305242 SRE=309622 SLE=297942 SRE=300862 SLE=295022 SRE=296482
 606 0.993265  172.31.96.136  43.159.71.114   TCP      90 [TCP Dup ACK 563#9] 63926 → 80 [ACK] Seq=1297 Ack=270202 Win=1023 Len=0 SLE=318382 SRE=319842 SLE=311082 SRE=315462 SLE=305242 SRE=309622 SLE=297942 SRE=300862
 607 0.993270  172.31.96.136  43.159.71.114   TCP      90 [TCP Dup ACK 563#10] 63926 → 80 [ACK] Seq=1297 Ack=270202 Win=1023 Len=0 SLE=321302 SRE=324222 SLE=318382 SRE=319842 SLE=311082 SRE=315462 SLE=305242 SRE=309622
 608 0.993308  172.31.96.136  43.159.71.114   TCP      90 [TCP Dup ACK 563#11] 63926 → 80 [ACK] Seq=1297 Ack=270202 Win=1023 Len=0 SLE=325682 SRE=330062 SLE=321302 SRE=324222 SLE=318382 SRE=319842 SLE=311082 SRE=315462
 609 0.993313  172.31.96.136  43.159.71.114   TCP      90 [TCP Dup ACK 563#12] 63926 → 80 [ACK] Seq=1297 Ack=270202 Win=1023 Len=0 SLE=331522 SRE=332982 SLE=325682 SRE=330062 SLE=321302 SRE=324222 SLE=318382 SRE=319842
 610 0.993316  172.31.96.136  43.159.71.114   TCP      90 [TCP Dup ACK 563#13] 63926 → 80 [ACK] Seq=1297 Ack=270202 Win=1023 Len=0 SLE=335902 SRE=337362 SLE=331522 SRE=332982 SLE=325682 SRE=330062 SLE=321302 SRE=324222
 611 0.993322  172.31.96.136  43.159.71.114   TCP      90 [TCP Dup ACK 563#14] 63926 → 80 [ACK] Seq=1297 Ack=270202 Win=1023 Len=0 SLE=338822 SRE=354882 SLE=335902 SRE=337362 SLE=331522 SRE=332982 SLE=325682 SRE=330062
```

```
> Frame 16: 486 bytes on wire (3888 bits), 486 bytes captured (3888 bits) on interface \Device\NPF_{A7CA02C3-5140-442A-85E8-58531EAC12F
> Ethernet II, Src: Intel_43:fd:f0 (60:a5:e2:43:fd:f0), Dst: IETF-VRRP-VRID_0c (00:00:5e:00:01:0c)
> Internet Protocol Version 4, Src: 172.31.96.136, Dst: 43.159.71.114
> Transmission Control Protocol, Src Port: 63926, Dst Port: 80, Seq: 1, Ack: 47, Len: 432
> Hypertext Transfer Protocol
```

```
0000  00 00 5e 00 01 0c 60 a5  e2 43 fd f0 08 00 45 00   ··^···`· ·C····E·
0010  01 d8 0e 72 40 00 80 06  00 00 ac 1f 60 88 2b 9f   ···r@··· ····`·+·
0020  47 72 f9 b6 00 50 3d ed  73 e6 49 60 c6 1d 50 18   Gr···P=· s·I`··P·
0030  03 ff 81 83 00 00 47 45  54 20 2f 66 69 6c 65 73   ······GE T /files
0040  74 72 65 61 6d 69 6e 67  73 65 72 76 69 63 65 2f   treaming service/
0050  66 69 6c 65 73 2f 32 64  33 66 39 62 61 39 2d 35   files/2d 3f9ba9-5
0060  30 39 36 2d 34 62 32 33  2d 39 37 30 39 2d 33 61   096-4b23 -9709-3a
0070  66 37 64 37 61 32 31 30  33 66 3f 50 31 3d 31 37   f7d7a210 3f?P1=17
0080  33 38 32 34 38 37 34 38  26 50 32 3d 34 30 34 26   38248748 &P2=404&
0090  50 33 3d 32 26 50 34 3d  67 4c 34 72 49 37 47 62   P3=2&P4= gL4rI7Gb
00a0  76 25 32 66 6b 6b 68 6b  46 72 66 41 30 42 51 45   v%2fkkhk FrfA0BQE
00b0  77 4e 34 35 6d 72 78 76  62 6c 4e 57 37 76 6a 62   wN45mrxv blNW7vjb
00c0  79 67 54 4e 42 6e 36 43  4a 73 32 79 73 75 4c 79   ygTNBn6C Js2ysuLy
00d0  75 73 76 4d 38 5a 54 62  68 4e 53 52 79 41 43 74   usvM8ZTb hNSRyACt
00e0  37 30 44 6a 77 58 50 4c  6d 25 32 66 45 4b 30 43   70DjwXPL m%2fEK0C
00f0  74 77 25 33 64 25 33 64  20 48 54 54 50 2f 31 2e   tw%3d%3d  HTTP/1.
0100  31 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 4b   1··Conne ction: K
```

6. Start a new packet capture to now visit an external website, say www.cricinfo.com. Can you show the 3-way TCP handshake happening? Can you see your IITJ proxy in between? What is its IP address?

Ans-



```
11504 13.469492  15.197.193.217  172.31.96.136   TLSv1.2   92 Application Data
11505 13.469517  172.31.96.136   15.197.193.217  TCP       54 60476 → 443 [ACK] Seq=4392 Ack=8992 Win=65280 Len=0
11506 13.471204  172.31.96.136   69.173.158.64   TCP       66 60507 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
11507 13.475550  142.250.194.194 172.31.96.136   TCP       54 443 → 60485 [ACK] Seq=8438 Ack=2996 Win=267264 Len=0
11508 13.479535  142.250.194.194 172.31.96.136   TCP       54 443 → 60485 [ACK] Seq=8438 Ack=3102 Win=267264 Len=0
11509 13.482804  69.173.158.64   172.31.96.136   TCP       66 443 → 60502 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 WS=4 SACK_PERM
11510 13.482867  172.31.96.136   69.173.158.64   TCP       54 60502 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
11511 13.483102  172.31.96.136   69.173.158.64   TCP     1514 60502 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1460 [TCP PDU reassembled in 11512]
11512 13.483102  172.31.96.136   69.173.158.64   TLSv1.2  424 Client Hello (SNI=pixel.rubiconproject.com)
11513 13.484952  69.173.158.64   172.31.96.136   TCP       54 443 → 60502 [ACK] Seq=1 Ack=1461 Win=262140 Len=0
11514 13.485548  172.31.96.136   142.250.194.194 TLSv1.3  195 Application Data
11515 13.485761  172.31.96.136   8.8.4.4         TLSv1.2  245 Application Data
11516 13.485779  172.31.96.136   8.8.4.4         TLSv1.2  245 Application Data
11517 13.486023  172.31.96.136   34.111.113.62   TLSv1.2  217 Application Data
11518 13.486084  172.31.96.136   8.8.4.4         TLSv1.2  243 Application Data
11519 13.486098  172.31.96.136   8.8.4.4         TLSv1.2  243 Application Data
11520 13.486110  172.31.96.136   8.8.4.4         TLSv1.2  244 Application Data
11521 13.486121  172.31.96.136   8.8.4.4         TLSv1.2  244 Application Data
11522 13.486132  172.31.96.136   8.8.4.4         TLSv1.2  244 Application Data
11523 13.486143  172.31.96.136   8.8.4.4         TLSv1.2  244 Application Data
11524 13.486155  172.31.96.136   8.8.4.4         TLSv1.2  245 Application Data
11525 13.486166  172.31.96.136   8.8.4.4         TLSv1.2  245 Application Data
11526 13.486178  172.31.96.136   8.8.4.4         TLSv1.2  244 Application Data
11527 13.486189  172.31.96.136   8.8.4.4         TLSv1.2  244 Application Data
11528 13.486200  172.31.96.136   8.8.4.4         TLSv1.2  243 Application Data
11529 13.486212  172.31.96.136   8.8.4.4         TLSv1.2  244 Application Data
11530 13.486223  172.31.96.136   8.8.4.4         TLSv1.2  244 Application Data
```

```
> Frame 11512: 424 bytes on wire (3392 bits), 424 bytes captured (3392 bits) on interface \Device\NPF_{A7CA02C3-5140-442A-85E8-58531EAC
> Ethernet II, Src: Intel_43:fd:f0 (60:a5:e2:43:fd:f0), Dst: IETF-VRRP-VRID_0c (00:00:5e:00:01:0c)
> Internet Protocol Version 4, Src: 172.31.96.136, Dst: 69.173.158.64
> Transmission Control Protocol, Src Port: 60502, Dst Port: 443, Seq: 1461, Ack: 1, Len: 370
> [2 Reassembled TCP Segments (1830 bytes): #11511(1460), #11512(370)]
> Transport Layer Security
```

```
0000  00 00 5e 00 01 0c 60 a5  e2 43 fd f0 08 00 45 00   ··^···`· ·C····E·
0010  01 9a 24 cb 40 00 80 06  00 00 ac 1f 60 88 45 ad   ··$·@··· ····`·E·
0020  9e 40 ec 56 01 bb a9 99  6e 25 9d 8d 0a 77 50 18   ·@·V···· n%··wP·
0030  00 ff f2 21 00 00 57 00  1d 00 20 c6 93 1b b8 77   ···!··W· ·· ····w
0040  00 aa 99 88 a9 74 4b ed  90 08 a1 88 8b 6d 2f a6   ·····tK· ·····m/·
0050  ba bd 56 3c 91 8e a4 42  49 dc 55 00 00 00 1d 00   ··V<···B I·U·····
0060  1b 00 00 18 70 69 78 65  6c 2e 72 75 62 69 63 6f   ····pixe l.rubico
0070  6e 70 72 6f 6a 65 63 74  2e 63 6f 6d fe 0d 01 1a   nproject .com····
```

The screenshot confirm the TCP 3-way handshake between the client (172.31.96.136) and the server (69.173.158.64):

1. SYN Packet: The client sends a SYN to initiate the connection.
2. SYN-ACK Packet: The server responds with SYN-ACK to acknowledge and synchronize.
3. ACK Packet: The client sends an ACK to complete the handshake.

This establishes a reliable TCP connection between the machine and the external server.

Now,about the proxy server :

- There is no visible proxy server as per my observation.
- Traffic flows directly from my machine (172.31.96.136) to the external server of espncricinfo.
- There might be a transparent proxy, which might be implemented at the gateway level (172.31.64.1), but it does not modify packet headers or appear explicitly in the packet capture.

7. Why does DNS follow the UDP stream while HTTP follows the TCP stream?

Ans-
DNS typically uses UDP because:

- It's faster for small queries
- It's connectionless, reducing overhead
- Most DNS queries fit in a single UDP packet

HTTP uses TCP because:

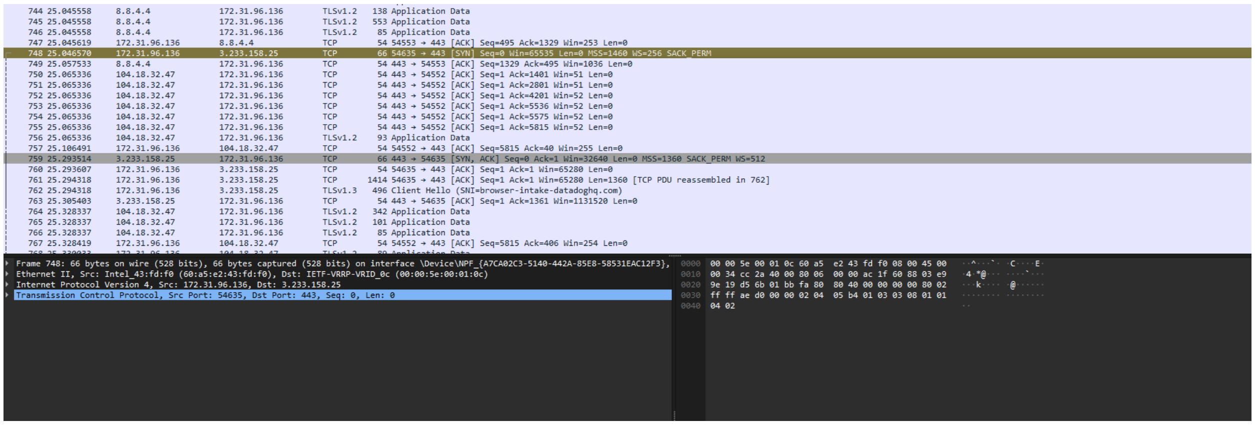
- It ensures reliable, ordered delivery of data
- It provides flow control and congestion control
- Web pages often require multiple packets, making TCP's connection-oriented nature beneficial

8. Execute the socket program (both server and client) to demonstrate TCP communication on different ports. Capture the network packets using Wireshark and analyze them to justify the communication process.

Ans-

The screenshot below demonstrates local socket communication with the following characteristics:

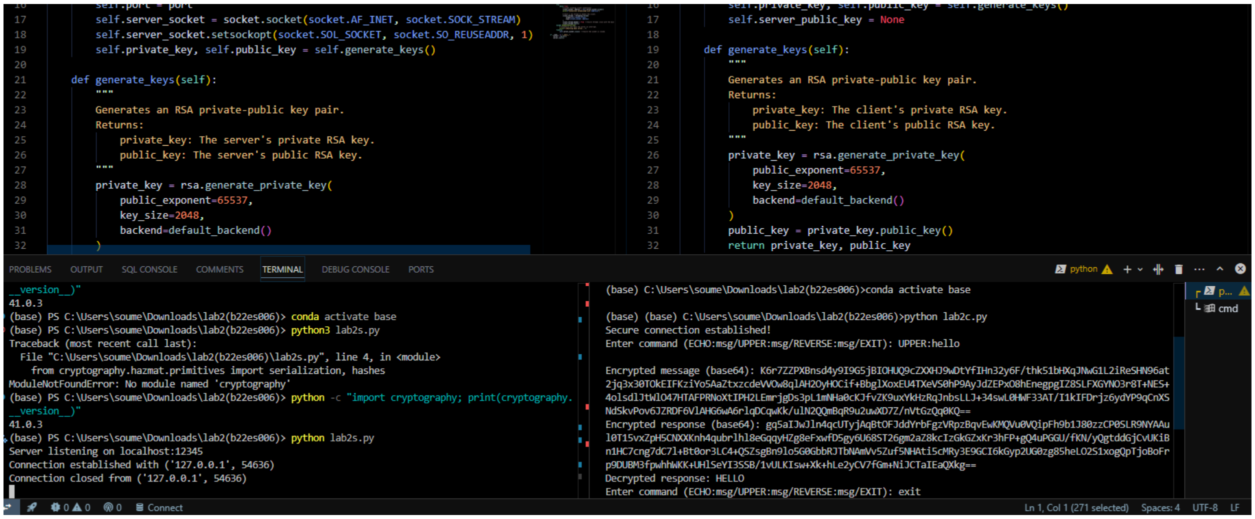
- Source and Destination: Both at IP 172.31.96.136, indicating localhost communication
- Data Exchange: Bidirectional TCP segments containing application data
- Protocol Mechanisms:
    - Sequence numbers maintain packet ordering
    - PSH/ACK flags confirm reliable data delivery
    - Application data packets show successful data transfer



```
744 25.045558   8.8.4.4          172.31.96.136    TLSv1.2   138 Application Data
745 25.045558   8.8.4.4          172.31.96.136    TLSv1.2   553 Application Data
746 25.045558   8.8.4.4          172.31.96.136    TLSv1.2    85 Application Data
747 25.045619   172.31.96.136    8.8.4.4          TCP        54 54553 → 443 [ACK] Seq=495 Ack=1329 Win=253 Len=0
748 25.046570   172.31.96.136    3.233.158.25     TCP        66 54635 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
749 25.057533   8.8.4.4          172.31.96.136    TCP        54 443 → 54553 [ACK] Seq=1329 Ack=495 Win=1036 Len=0
750 25.065336   104.18.32.47     172.31.96.136    TCP        54 443 → 54552 [ACK] Seq=1 Ack=1401 Win=51 Len=0
751 25.065336   104.18.32.47     172.31.96.136    TCP        54 443 → 54552 [ACK] Seq=1 Ack=2801 Win=51 Len=0
752 25.065336   104.18.32.47     172.31.96.136    TCP        54 443 → 54552 [ACK] Seq=1 Ack=4201 Win=52 Len=0
753 25.065336   104.18.32.47     172.31.96.136    TCP        54 443 → 54552 [ACK] Seq=1 Ack=5536 Win=52 Len=0
754 25.065336   104.18.32.47     172.31.96.136    TCP        54 443 → 54552 [ACK] Seq=1 Ack=5575 Win=52 Len=0
755 25.065336   104.18.32.47     172.31.96.136    TCP        54 443 → 54552 [ACK] Seq=1 Ack=5815 Win=52 Len=0
756 25.065336   104.18.32.47     172.31.96.136    TLSv1.2    93 Application Data
757 25.106491   172.31.96.136    104.18.32.47     TCP        54 54552 → 443 [ACK] Seq=5815 Ack=40 Win=255 Len=0
759 25.293514   3.233.158.25     172.31.96.136    TCP        66 443 → 54635 [SYN, ACK] Seq=0 Ack=1 Win=32640 Len=0 MSS=1360 SACK_PERM WS=512
760 25.293607   172.31.96.136    3.233.158.25     TCP        54 54635 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
761 25.294318   172.31.96.136    3.233.158.25     TCP      1414 54635 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1360 [TCP PDU reassembled in 762]
762 25.294318   172.31.96.136    3.233.158.25     TLSv1.3   496 Client Hello (SNI=browser-intake-datadoghq.com)
763 25.305403   3.233.158.25     172.31.96.136    TCP        54 443 → 54635 [ACK] Seq=1 Ack=1361 Win=1131520 Len=0
764 25.328337   104.18.32.47     172.31.96.136    TLSv1.2   342 Application Data
765 25.328337   104.18.32.47     172.31.96.136    TLSv1.2   101 Application Data
766 25.328337   104.18.32.47     172.31.96.136    TLSv1.2    85 Application Data
767 25.328419   172.31.96.136    104.18.32.47     TCP        54 54552 → 443 [ACK] Seq=5815 Ack=406 Win=254 Len=0
```

```
▸ Frame 748: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{A7CA02C3-5140-442A-85E8-58531EAC12F3},
▸ Ethernet II, Src: Intel_43:fd:f0 (60:a5:e2:43:fd:f0), Dst: IETF-VRRP-VRID_0c (00:00:5e:00:01:0c)
▸ Internet Protocol Version 4, Src: 172.31.96.136, Dst: 3.233.158.25
▸ Transmission Control Protocol, Src Port: 54635, Dst Port: 443, Seq: 0, Len: 0
```

```
0000  00 00 5e 00 01 0c 60 a5  e2 43 fd f0 08 00 45 00   ··^···`· ·C····E·
0010  00 34 cc 2a 40 00 80 06  00 00 ac 1f 60 88 03 e9   ·4·*@··· ····`···
0020  9e 19 d5 6b 01 bb fa 80  80 40 00 00 00 00 80 02   ···k···· ·@······
0030  ff ff ae d0 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··
```



```python
        self.port = port
        self.server_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        self.server_socket.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
        self.private_key, self.public_key = self.generate_keys()

    def generate_keys(self):
        """
        Generates an RSA private-public key pair.
        Returns:
            private_key: The server's private RSA key.
            public_key: The server's public RSA key.
        """
        private_key = rsa.generate_private_key(
            public_exponent=65537,
            key_size=2048,
            backend=default_backend()
        )
```

```python
        self.private_key, self.public_key = self.generate_keys()
        self.server_public_key = None

    def generate_keys(self):
        """
        Generates an RSA private-public key pair.
        Returns:
            private_key: The client's private RSA key.
            public_key: The client's public RSA key.
        """
        private_key = rsa.generate_private_key(
            public_exponent=65537,
            key_size=2048,
            backend=default_backend()
        )
        public_key = private_key.public_key()
        return private_key, public_key
```

```
__version__)"
41.0.3
(base) PS C:\Users\soume\Downloads\lab2(b22es006)> conda activate base
(base) PS C:\Users\soume\Downloads\lab2(b22es006)> python3 lab2s.py
Traceback (most recent call last):
  File "C:\Users\soume\Downloads\lab2(b22es006)\lab2s.py", line 4, in <module>
    from cryptography.hazmat.primitives import serialization, hashes
ModuleNotFoundError: No module named 'cryptography'
(base) PS C:\Users\soume\Downloads\lab2(b22es006)> python -c "import cryptography; print(cryptography.
__version__)"
41.0.3
(base) PS C:\Users\soume\Downloads\lab2(b22es006)> python lab2s.py
Server listening on localhost:12345
Connection established with ('127.0.0.1', 54636)
Connection closed from ('127.0.0.1', 54636)
```

```
(base) C:\Users\soume\Downloads\lab2(b22es006)>conda activate base

(base) (base) C:\Users\soume\Downloads\lab2(b22es006)>python lab2c.py
Secure connection established!
Enter command (ECHO:msg/UPPER:msg/REVERSE:msg/EXIT): UPPER:hello

Encrypted message (base64): K6r7ZZPXBnsd4y9I9G5jBIOHUQ9cZXXHJ9wDtYfIHn32y6F/thk51bHXqJNwG1L2iReSHN96at
2jq3x30TOkEIFKziYo5AaZtxzcdeVVOw8qlAH2OyHOCif+BbglXoxEU4TXeVS0hP9AyJdZEPxO8hEnegpgIZ8SLFXGYNO3r8T+NES+
4olsdlJtWlO47HTAFPRNoXtIPH2LEmrjgDs3pL1mNHa0cKJfvZK9uxYkHzRqJnbsLLJ+34swL0HWF33AT/I1kIFDrjz6ydYP9qCnXS
NdSkvPov6JZRDF6VlAHG6wA6rlqDCqwKk/ulN2QQmBqR9u2uwXD7Z/nVtGzQq0KQ==
Encrypted response (base64): gq5aIJwJln4qcUTyjAqBtOFJddYrbFgzVRpzBqvEwKMQVu0VQipFh9b1J80zzCP0SLR9NYAAu
l0T15vxZpH5CNXXKnh4qubrlhl8eGqqyHZg8eFxwfD5gy6U68ST26gm2aZ8kcIzGkGZxKr3hFP+gQ4uPGGU/fKN/yQgtddGjCvUKiB
n1HC7cng7dC7l+Bt0or3LC4+QSZsgBn9lo5G0GbbRJTbNAmVv5Zuf5NHAti5cMRy3E9GCI6kGyp2UG0zg85heLO2S1xogQpTjoBoFr
p9DUBM3fpwhhWKK+UHlSeYI3SSB/1vULKIsw+Xk+hLe2yCV7fGm+NiJCTaIEaQXkg==
Decrypted response: HELLO
Enter command (ECHO:msg/UPPER:msg/REVERSE:msg/EXIT): exit
```