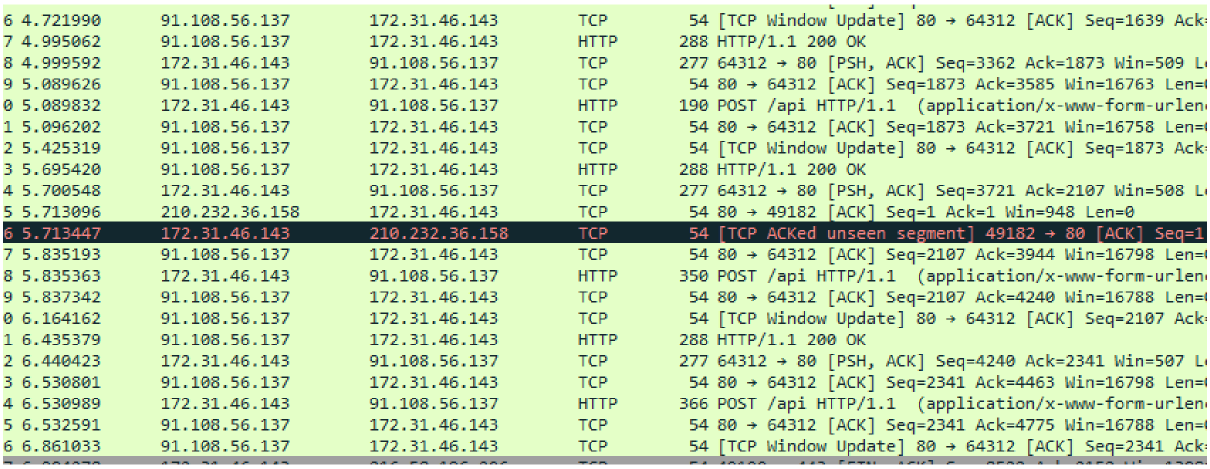
LAB REPORT 03

CYBERSECURITY

RITIK TIWARI (B21CS098)

Q1) Start packet capture in Wireshark on your wireless interface. What do you observe?

ANSWER: I can observe No. = number order of the packet captured, Time = column shows how long after I started the capture this packet was captured, Source = address of the system that sent the packet, Destination = address of the packet destination, Protocol = This is the type of packet. For example: TCP, DNS, DHCPv6, or ARP, Length = Column shows you the packet's length in bytes, info = column shows you more information about the packet contents



```
6 4.721990    91.108.56.137    172.31.46.143    TCP     54 [TCP Window Update] 80 → 64312 [ACK] Seq=1639 Ack
7 4.995062    91.108.56.137    172.31.46.143    HTTP   288 HTTP/1.1 200 OK
8 4.999592    172.31.46.143    91.108.56.137    TCP    277 64312 → 80 [PSH, ACK] Seq=3362 Ack=1873 Win=509 L
9 5.089626    91.108.56.137    172.31.46.143    TCP     54 80 → 64312 [ACK] Seq=1873 Ack=3585 Win=16763 Len=
0 5.089832    172.31.46.143    91.108.56.137    HTTP   190 POST /api HTTP/1.1  (application/x-www-form-urlen
1 5.096202    91.108.56.137    172.31.46.143    TCP     54 80 → 64312 [ACK] Seq=1873 Ack=3721 Win=16758 Len=
2 5.425319    91.108.56.137    172.31.46.143    TCP     54 [TCP Window Update] 80 → 64312 [ACK] Seq=1873 Ack
3 5.695420    91.108.56.137    172.31.46.143    HTTP   288 HTTP/1.1 200 OK
4 5.700548    172.31.46.143    91.108.56.137    TCP    277 64312 → 80 [PSH, ACK] Seq=3721 Ack=2107 Win=508 L
5 5.713096    210.232.36.158   172.31.46.143    TCP     54 80 → 49182 [ACK] Seq=1 Ack=1 Win=948 Len=0
6 5.713447    172.31.46.143    210.232.36.158   TCP     54 [TCP ACKed unseen segment] 49182 → 80 [ACK] Seq=1
7 5.835193    91.108.56.137    172.31.46.143    TCP     54 80 → 64312 [ACK] Seq=2107 Ack=3944 Win=16798 Len=
8 5.835363    172.31.46.143    91.108.56.137    HTTP   350 POST /api HTTP/1.1  (application/x-www-form-urlen
9 5.837342    91.108.56.137    172.31.46.143    TCP     54 80 → 64312 [ACK] Seq=2107 Ack=4240 Win=16788 Len=
0 6.164162    91.108.56.137    172.31.46.143    TCP     54 [TCP Window Update] 80 → 64312 [ACK] Seq=2107 Ack
1 6.435379    91.108.56.137    172.31.46.143    HTTP   288 HTTP/1.1 200 OK
2 6.440423    172.31.46.143    91.108.56.137    TCP    277 64312 → 80 [PSH, ACK] Seq=4240 Ack=2341 Win=507 L
3 6.530801    91.108.56.137    172.31.46.143    TCP     54 80 → 64312 [ACK] Seq=2341 Ack=4463 Win=16798 Len=
4 6.530989    172.31.46.143    91.108.56.137    HTTP   366 POST /api HTTP/1.1  (application/x-www-form-urlen
5 6.532591    91.108.56.137    172.31.46.143    TCP     54 80 → 64312 [ACK] Seq=2341 Ack=4775 Win=16788 Len=
6 6.861033    91.108.56.137    172.31.46.143    TCP     54 [TCP Window Update] 80 → 64312 [ACK] Seq=2341 Ack
```

Q2) 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.

ANSWER: What about TCP and HTTP?

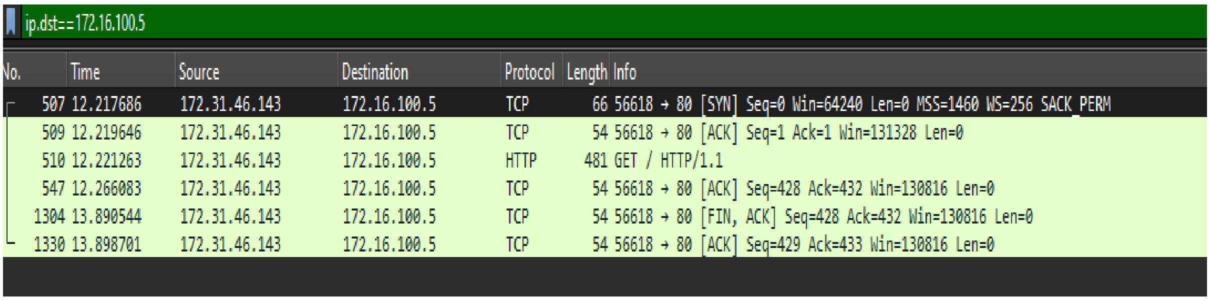
I notice first TCP protocol is employed then just after that HTTP protocol being employed. The TCP connection is established to facilitate reliable data transfer, while HTTP is used for web communication.

What is the IP address of the IITJ server?

The IP address associated with www.iitj.ac.in was determined to be 172.16.100.5. This IP appeared in both TCP and HTTP entries, indicating the use of these protocols for data exchange with the server.

Are you able to see different HTTP requests/responses?

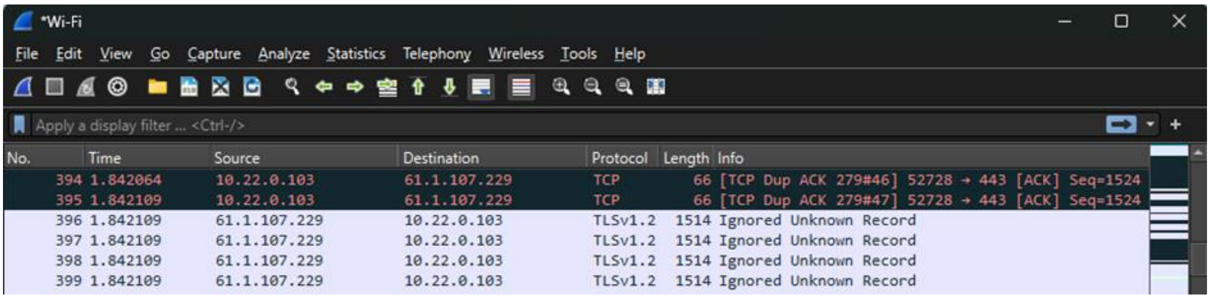
I could discern different HTTP requests and responses, illustrating the exchange of data between my computer and the IITJ server.



```
ip.dst==172.16.100.5

No.   Time       Source         Destination    Protocol Length Info
 507 12.217686  172.31.46.143  172.16.100.5   TCP       66 56618 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 509 12.219646  172.31.46.143  172.16.100.5   TCP       54 56618 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
 510 12.221263  172.31.46.143  172.16.100.5   HTTP     481 GET / HTTP/1.1
 547 12.266083  172.31.46.143  172.16.100.5   TCP       54 56618 → 80 [ACK] Seq=428 Ack=432 Win=130816 Len=0
1304 13.890544  172.31.46.143  172.16.100.5   TCP       54 56618 → 80 [FIN, ACK] Seq=428 Ack=432 Win=130816 Len=0
1330 13.898701  172.31.46.143  172.16.100.5   TCP       54 56618 → 80 [ACK] Seq=429 Ack=433 Win=130816 Len=0
```

Q3) What does a packet highlighted in `black' color signify?



```
Apply a display filter ... <Ctrl-/>

No.  Time      Source         Destination    Protocol Length Info
 394 1.842064  10.22.0.103    61.1.107.229   TCP        66 [TCP Dup ACK 279#46] 52728 → 443 [ACK] Seq=1524
 395 1.842109  10.22.0.103    61.1.107.229   TCP        66 [TCP Dup ACK 279#47] 52728 → 443 [ACK] Seq=1524
 396 1.842109  61.1.107.229   10.22.0.103    TLSv1.2  1514 Ignored Unknown Record
 397 1.842109  61.1.107.229   10.22.0.103    TLSv1.2  1514 Ignored Unknown Record
 398 1.842109  61.1.107.229   10.22.0.103    TLSv1.2  1514 Ignored Unknown Record
 399 1.842109  61.1.107.229   10.22.0.103    TLSv1.2  1514 Ignored Unknown Record
```

SOLUTION:

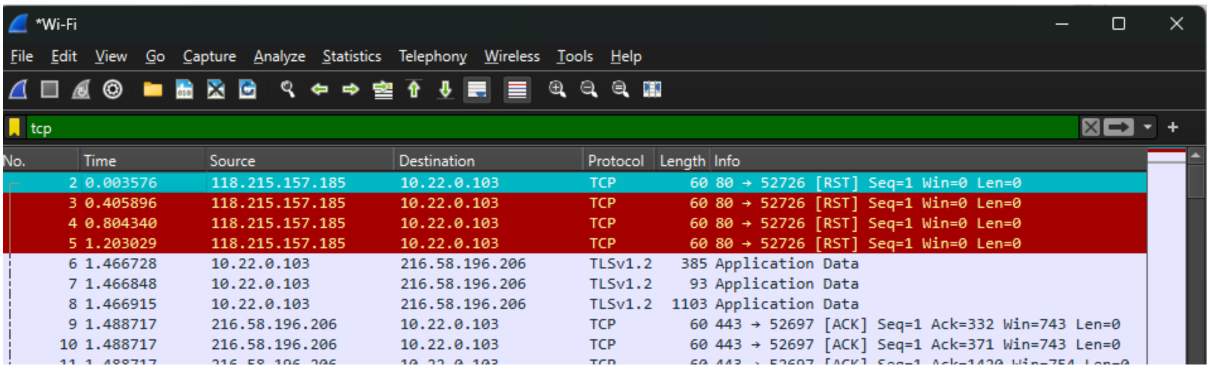
Black highlighted packet signifies that as TCP Keep-Alive ACK.

It is a type of message send by one end of a connection to the other to check if the connection is still active.

It helps maintain the connection open and ensures that both ends are still available and responsive. The Keep-Alive mechanism is used to prevent idle connections from being prematurely terminated by routers or firewalls.

Q4) Explore at least 5 different filters in Wireshark (https://wiki.wireshark.org/DisplayFilters). Ex. “http” would give you only HTTP traffic.

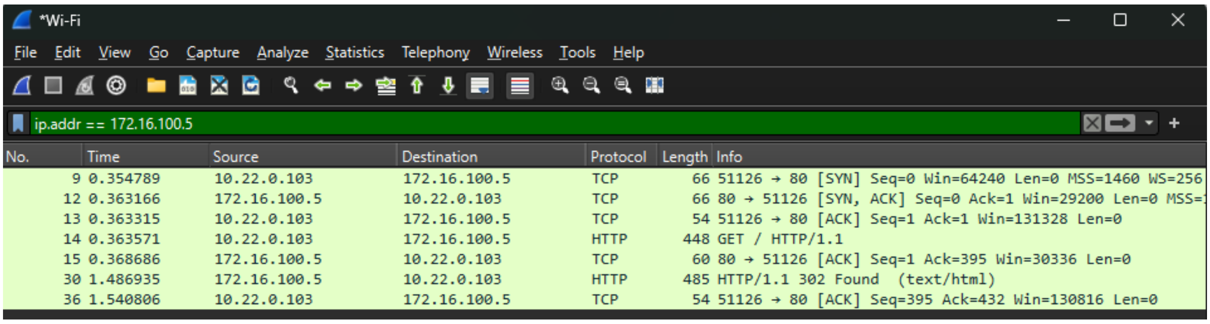
Filter by Protocol TCP



```
tcp

No.  Time      Source            Destination      Protocol Length Info
   2 0.003576  118.215.157.185   10.22.0.103      TCP        60 80 → 52726 [RST] Seq=1 Win=0 Len=0
   3 0.405896  118.215.157.185   10.22.0.103      TCP        60 80 → 52726 [RST] Seq=1 Win=0 Len=0
   4 0.804340  118.215.157.185   10.22.0.103      TCP        60 80 → 52726 [RST] Seq=1 Win=0 Len=0
   5 1.203029  118.215.157.185   10.22.0.103      TCP        60 80 → 52726 [RST] Seq=1 Win=0 Len=0
   6 1.466728  10.22.0.103       216.58.196.206   TLSv1.2   385 Application Data
   7 1.466848  10.22.0.103       216.58.196.206   TLSv1.2    93 Application Data
   8 1.466915  10.22.0.103       216.58.196.206   TLSv1.2  1103 Application Data
   9 1.488717  216.58.196.206    10.22.0.103      TCP        60 443 → 52697 [ACK] Seq=1 Ack=332 Win=743 Len=0
  10 1.488717  216.58.196.206    10.22.0.103      TCP        60 443 → 52697 [ACK] Seq=1 Ack=371 Win=743 Len=0
  11 1.488717  216.58.196.206    10.22.0.103      TCP        60 443 → 52697 [ACK] Seq=1 Ack=1420 Win=754 Len=0
```

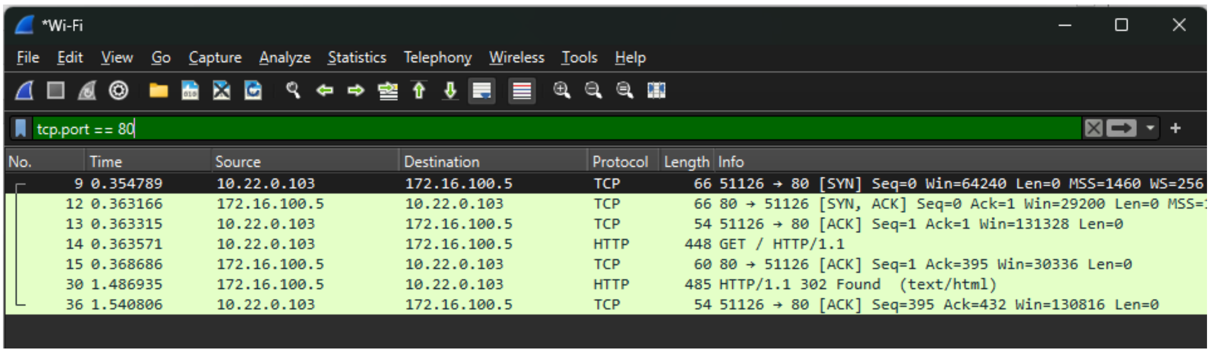
Filter by IP Address 172.16.100.5


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

```
ip.addr == 172.16.100.5
```

No.	Time	Source	Destination	Protocol	Length	Info
9	0.354789	10.22.0.103	172.16.100.5	TCP	66	51126 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
12	0.363166	172.16.100.5	10.22.0.103	TCP	66	80 → 51126 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=
13	0.363315	10.22.0.103	172.16.100.5	TCP	54	51126 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
14	0.363571	10.22.0.103	172.16.100.5	HTTP	448	GET / HTTP/1.1
15	0.368686	172.16.100.5	10.22.0.103	TCP	60	80 → 51126 [ACK] Seq=1 Ack=395 Win=30336 Len=0
30	1.486935	172.16.100.5	10.22.0.103	HTTP	485	HTTP/1.1 302 Found (text/html)
36	1.540806	10.22.0.103	172.16.100.5	TCP	54	51126 → 80 [ACK] Seq=395 Ack=432 Win=130816 Len=0

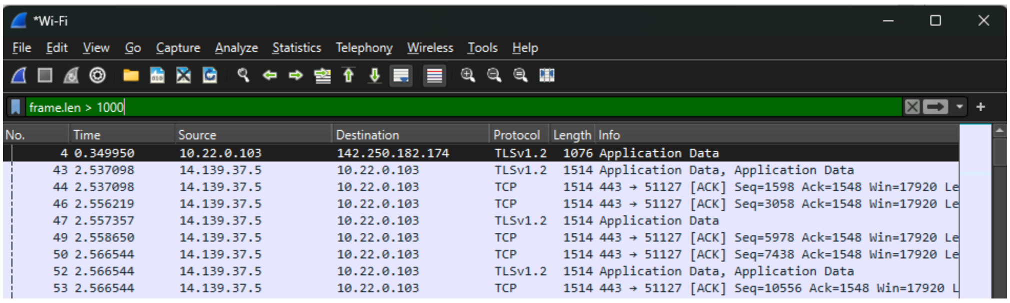
Filter by Port number 80


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

```
tcp.port == 80
```

No.	Time	Source	Destination	Protocol	Length	Info
9	0.354789	10.22.0.103	172.16.100.5	TCP	66	51126 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
12	0.363166	172.16.100.5	10.22.0.103	TCP	66	80 → 51126 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=
13	0.363315	10.22.0.103	172.16.100.5	TCP	54	51126 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
14	0.363571	10.22.0.103	172.16.100.5	HTTP	448	GET / HTTP/1.1
15	0.368686	172.16.100.5	10.22.0.103	TCP	60	80 → 51126 [ACK] Seq=1 Ack=395 Win=30336 Len=0
30	1.486935	172.16.100.5	10.22.0.103	HTTP	485	HTTP/1.1 302 Found (text/html)
36	1.540806	10.22.0.103	172.16.100.5	TCP	54	51126 → 80 [ACK] Seq=395 Ack=432 Win=130816 Len=0

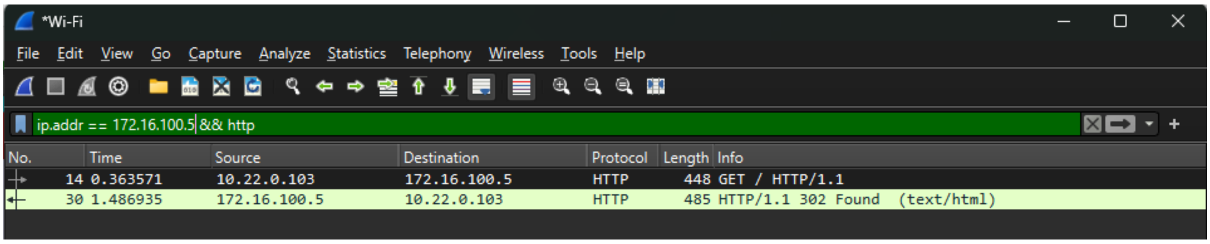
Filter by Packet length > 1000


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

```
frame.len > 1000
```

No.	Time	Source	Destination	Protocol	Length	Info
4	0.349950	10.22.0.103	142.250.182.174	TLSv1.2	1076	Application Data
43	2.537098	14.139.37.5	10.22.0.103	TLSv1.2	1514	Application Data, Application Data
44	2.537098	14.139.37.5	10.22.0.103	TCP	1514	443 → 51127 [ACK] Seq=1598 Ack=1548 Win=17920 Le
46	2.556219	14.139.37.5	10.22.0.103	TCP	1514	443 → 51127 [ACK] Seq=3058 Ack=1548 Win=17920 Le
47	2.557357	14.139.37.5	10.22.0.103	TLSv1.2	1514	Application Data
49	2.558650	14.139.37.5	10.22.0.103	TCP	1514	443 → 51127 [ACK] Seq=5978 Ack=1548 Win=17920 Le
50	2.566544	14.139.37.5	10.22.0.103	TCP	1514	443 → 51127 [ACK] Seq=7438 Ack=1548 Win=17920 Le
52	2.566544	14.139.37.5	10.22.0.103	TLSv1.2	1514	Application Data, Application Data
53	2.566544	14.139.37.5	10.22.0.103	TCP	1514	443 → 51127 [ACK] Seq=10556 Ack=1548 Win=17920 L

Filtered by IP address = 172.16.100.5 and protocol type HTTP

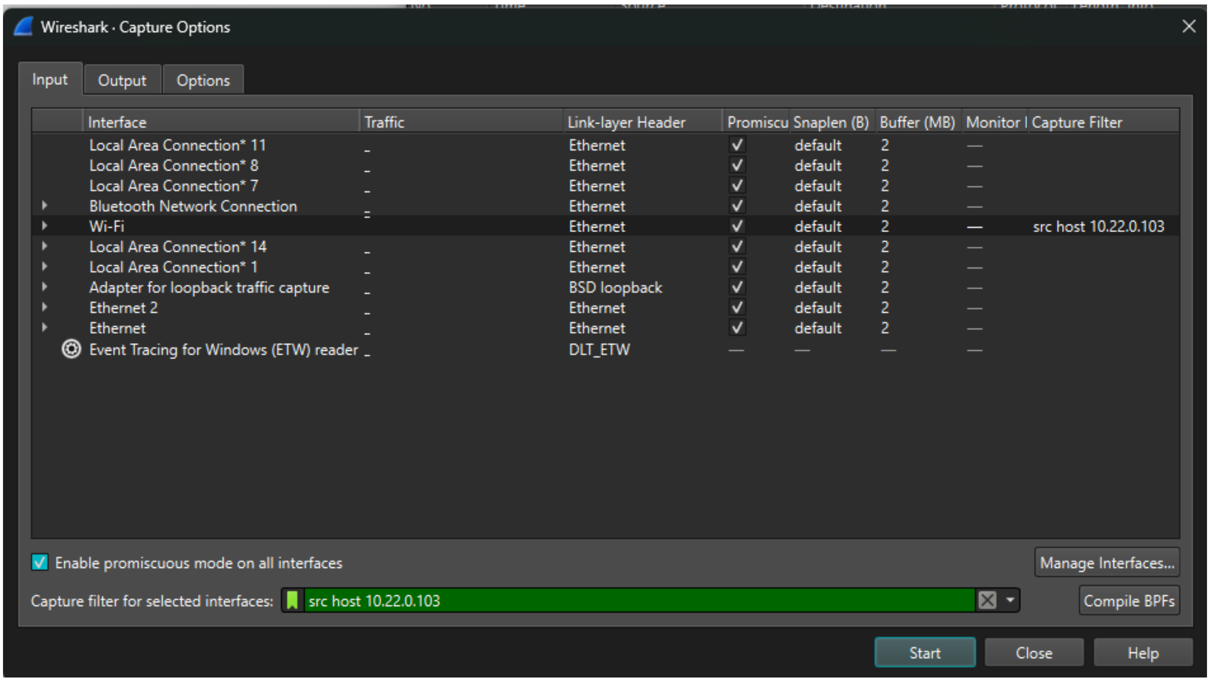

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 172.16.100.5 && http
```

No.	Time	Source	Destination	Protocol	Length	Info
14	0.363571	10.22.0.103	172.16.100.5	HTTP	448	GET / HTTP/1.1
30	1.486935	172.16.100.5	10.22.0.103	HTTP	485	HTTP/1.1 302 Found (text/html)

Q5) What is the filter command for listing all outgoing traffic?

ANSWER: src host <your_ip_address>



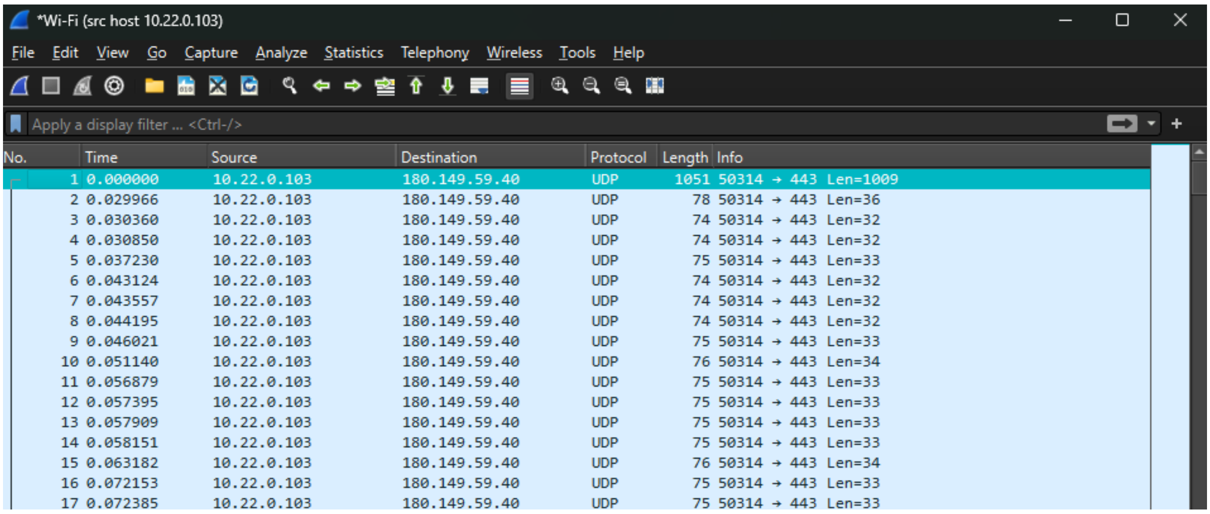
Wireshark · Capture Options

Interface	Traffic	Link-layer Header	Promiscu	Snaplen (B)	Buffer (MB)	Monitor I	Capture Filter
Local Area Connection* 11	_	Ethernet	✓	default	2	—	
Local Area Connection* 8	_	Ethernet	✓	default	2	—	
Local Area Connection* 7	_	Ethernet	✓	default	2	—	
Bluetooth Network Connection	_	Ethernet	✓	default	2	—	
Wi-Fi		Ethernet	✓	default	2	—	src host 10.22.0.103
Local Area Connection* 14	_	Ethernet	✓	default	2	—	
Local Area Connection* 1	_	Ethernet	✓	default	2	—	
Adapter for loopback traffic capture	_	BSD loopback	✓	default	2	—	
Ethernet 2	_	Ethernet	✓	default	2	—	
Ethernet	_	Ethernet	✓	default	2	—	
Event Tracing for Windows (ETW) reader	_	DLT_ETW	—	—	—	—	

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: src host 10.22.0.103

Manage Interfaces...
Compile BPFs
Start
Close
Help



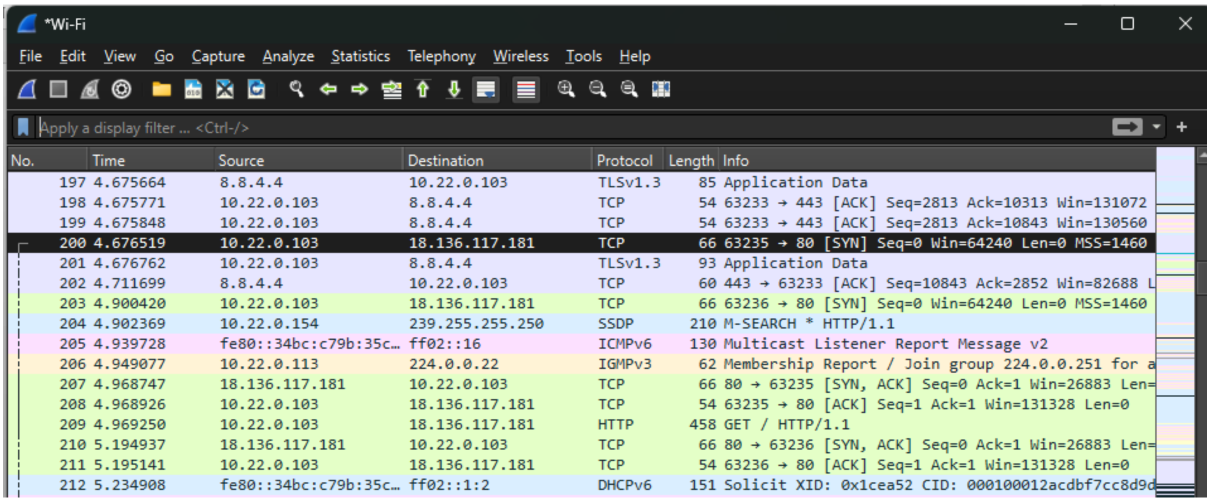
*Wi-Fi (src host 10.22.0.103)

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	10.22.0.103	180.149.59.40	UDP	1051	50314 → 443 Len=1009
2	0.029966	10.22.0.103	180.149.59.40	UDP	78	50314 → 443 Len=36
3	0.030360	10.22.0.103	180.149.59.40	UDP	74	50314 → 443 Len=32
4	0.030850	10.22.0.103	180.149.59.40	UDP	74	50314 → 443 Len=32
5	0.037230	10.22.0.103	180.149.59.40	UDP	75	50314 → 443 Len=33
6	0.043124	10.22.0.103	180.149.59.40	UDP	74	50314 → 443 Len=32
7	0.043557	10.22.0.103	180.149.59.40	UDP	74	50314 → 443 Len=32
8	0.044195	10.22.0.103	180.149.59.40	UDP	74	50314 → 443 Len=32
9	0.046021	10.22.0.103	180.149.59.40	UDP	75	50314 → 443 Len=33
10	0.051140	10.22.0.103	180.149.59.40	UDP	76	50314 → 443 Len=34
11	0.056879	10.22.0.103	180.149.59.40	UDP	75	50314 → 443 Len=33
12	0.057395	10.22.0.103	180.149.59.40	UDP	75	50314 → 443 Len=33
13	0.057909	10.22.0.103	180.149.59.40	UDP	75	50314 → 443 Len=33
14	0.058151	10.22.0.103	180.149.59.40	UDP	75	50314 → 443 Len=33
15	0.063182	10.22.0.103	180.149.59.40	UDP	76	50314 → 443 Len=34
16	0.072153	10.22.0.103	180.149.59.40	UDP	75	50314 → 443 Len=33
17	0.072385	10.22.0.103	180.149.59.40	UDP	75	50314 → 443 Len=33

Q6) 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?

ANSWER: Yes, I can see 3-way TCP handshake SYN at No. = 200 from 10.22.0.103 (my device) to 18.136.117.181(www.cricinfo.com) then SYN + ACK at No. = 207 from 18.136.117.181 to 10.22.0.103 and ACK at No. = 208 from 10.22.0.103 to 18.136.117.181.


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

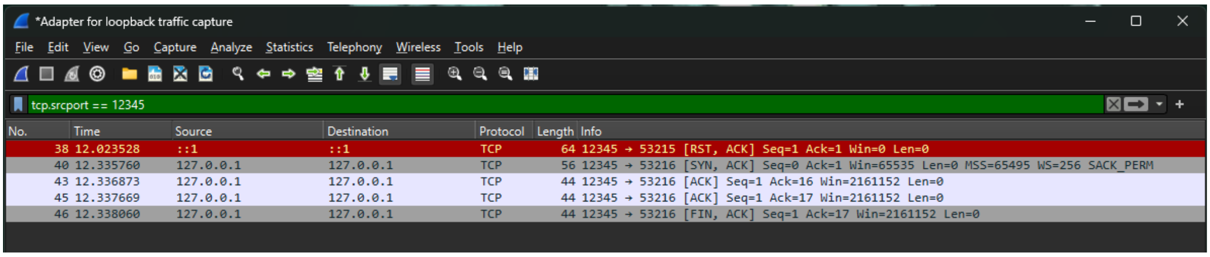
No.	Time	Source	Destination	Protocol	Length	Info
197	4.675664	8.8.4.4	10.22.0.103	TLSv1.3	85	Application Data
198	4.675771	10.22.0.103	8.8.4.4	TCP	54	63233 → 443 [ACK] Seq=2813 Ack=10313 Win=131072
199	4.675848	10.22.0.103	8.8.4.4	TCP	54	63233 → 443 [ACK] Seq=2813 Ack=10843 Win=130560
200	4.676519	10.22.0.103	18.136.117.181	TCP	66	63235 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
201	4.676762	10.22.0.103	8.8.4.4	TLSv1.3	93	Application Data
202	4.711699	8.8.4.4	10.22.0.103	TCP	60	443 → 63233 [ACK] Seq=10843 Ack=2852 Win=82688 L
203	4.900420	10.22.0.103	18.136.117.181	TCP	66	63236 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
204	4.902369	10.22.0.154	239.255.255.250	SSDP	210	M-SEARCH * HTTP/1.1
205	4.939728	fe80::34bc:c79b:35c…	ff02::16	ICMPv6	130	Multicast Listener Report Message v2
206	4.949077	10.22.0.113	224.0.0.22	IGMPv3	62	Membership Report / Join group 224.0.0.251 for a
207	4.968747	18.136.117.181	10.22.0.103	TCP	66	80 → 63235 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=
208	4.968926	10.22.0.103	18.136.117.181	TCP	54	63235 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
209	4.969250	10.22.0.103	18.136.117.181	HTTP	458	GET / HTTP/1.1
210	5.194937	18.136.117.181	10.22.0.103	TCP	66	80 → 63236 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=
211	5.195141	10.22.0.103	18.136.117.181	TCP	54	63236 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
212	5.234908	fe80::34bc:c79b:35c…	ff02::1:2	DHCPv6	151	Solicit XID: 0x1cea52 CID: 000100012acdbf7cc8d9d

Q7) Why does DNS follow the UDP stream while HTTP follows the TCP stream?

ANSWER: DNS follow the UDP stream while HTTP follows the TCP stream because of the following reasons:

1) UDP is much faster. TCP is slow as it requires a 3-way handshake. The load on DNS servers is also an important factor. DNS servers (since they use UDP) do not have to keep connections.
2) DNS requests are generally very small and fit well within UDP segments.
3) UDP is not reliable, but reliability can be added to the application layer. An application can use UDP and can be reliable by using a timeout and resend at the application layer.

Q8) Run your socket program (both server and client) and show the TCP communication happening at different ports.


*Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.srcport == 12345

No.	Time	Source	Destination	Protocol	Length	Info
38	12.023528	::1	::1	TCP	64	12345 → 53215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
40	12.335760	127.0.0.1	127.0.0.1	TCP	56	12345 → 53216 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
43	12.336873	127.0.0.1	127.0.0.1	TCP	44	12345 → 53216 [ACK] Seq=1 Ack=16 Win=2161152 Len=0
45	12.337669	127.0.0.1	127.0.0.1	TCP	44	12345 → 53216 [ACK] Seq=1 Ack=17 Win=2161152 Len=0
46	12.338060	127.0.0.1	127.0.0.1	TCP	44	12345 → 53216 [FIN, ACK] Seq=1 Ack=17 Win=2161152 Len=0

Here as we can see at port 12345 which is my socket program port, and in screenshot we can see 3-way TCP handshake between client and server at port 12345.