

Name: J Kevin Immanuel
College: VIT Chennai

Q2)

TCP;

No.	Time	Source	Destination	Protocol	Length	Info
228	4.887504448	2406:1f13:11b:9905::	2406:17400:c4:b0f8:b...	TLSv1.2	110	Application Data
229	4.887504772	2406:1f13:11b:9905::	2406:17400:c4:b0f8:b...	TCP	80	443 → 41668 [FIN, ACK] Seq=25 Ack=2 Win=424 Len=0 TSval=2485405647 TSecr=201609143
230	4.887505044	2406:17400:c4:b0f8:b...	2406:1f13:11b:9905::	TCP	74	41668 → 443 [RST] Seq=2 Win=0 Len=0
231	4.887505082	2406:17400:c4:b0f8:b...	2406:1f13:11b:9905::	TCP	74	41668 → 443 [RST] Seq=2 Win=0 Len=0
268	5.708431103	2406:17400:c4:b0f8:b...	2406:1f13:11b:9905::	TCP	80	35408 → 443 [FIN, ACK] Seq=1 Ack=1 Win=612 Len=0 TSval=2438106819 TSecr=451135592
269	5.708432316	2406:17400:c4:b0f8:b...	2406:1f13:11b:9905::	TCP	80	54452 → 443 [FIN, ACK] Seq=1 Ack=1 Win=612 Len=0 TSval=2450988410 TSecr=389768564
307	8.464507096	192.168.0.106	44.233.178.197	TCP	74	45326 → 443 [SYN] Seq=0 Win=63616 Len=0 MSS=2272 SACK_PERM=1 TSval=3566263872 TSecr=0 WS=128
310	8.724988443	192.168.0.106	44.233.178.197	TCP	74	45326 → 443 [SYN] Seq=0 Win=63616 Len=0 MSS=2272 SACK_PERM=1 TSval=3566263872 TSecr=0 WS=128
311	8.724988599	44.233.178.197	192.168.0.106	TCP	74	445 → 45326 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1440 SACK_PERM=1 TSval=457163704 TSecr=3566263872 WS=256
312	8.724981516	192.168.0.106	44.233.178.197	TCP	66	45326 → 443 [ACK] Seq=1 Ack=1 Win=63616 Len=0 TSval=3566264112 TSecr=457163704
313	8.725210355	192.168.0.106	44.233.178.197	TCP	1094	45326 → 443 [ACK] Seq=1 Ack=1 Win=63616 Len=1428 TSval=3566264112 TSecr=457163704 [TCP segment of a reassembled PDU]
314	8.725245549	192.168.0.106	44.233.178.197	TLSv1.3	582	Client Hello
315	8.724715527	2406:17400:c4:b0f8:b...	2406:16805:4607:625::	TCP	96	48582 → 443 [FIN, ACK] Seq=1 Ack=1 Win=63616 Len=0 TSval=2445488597 TSecr=2224807740
320	8.968055157	44.233.178.197	192.168.0.106	TCP	74	45326 → 443 [ACK] Seq=1 Ack=1 Win=26847 Len=0 MSS=1440 SACK_PERM=1 TSval=457163956 TSecr=3566264112 WS=256
321	8.968152420	192.168.0.106	44.233.178.197	TCP	66	45328 → 443 [ACK] Seq=1 Ack=1 Win=63616 Len=0 TSval=3566264375 TSecr=457163956
322	8.968052072	44.233.178.197	192.168.0.106	TCP	66	443 → 45326 [ACK] Seq=1 Ack=1945 Win=44000 Len=0 TSval=457163967 TSecr=3566264132
323	8.968053618	44.233.178.197	192.168.0.106	TLSv1.3	300	Server Hello, Change Cipher Spec, Application Data, Application Data
324	8.968213275	192.168.0.106	44.233.178.197	TCP	66	45326 → 443 [ACK] Seq=1945 Ack=235 Win=63488 Len=0 TSval=3566264375 TSecr=457163967

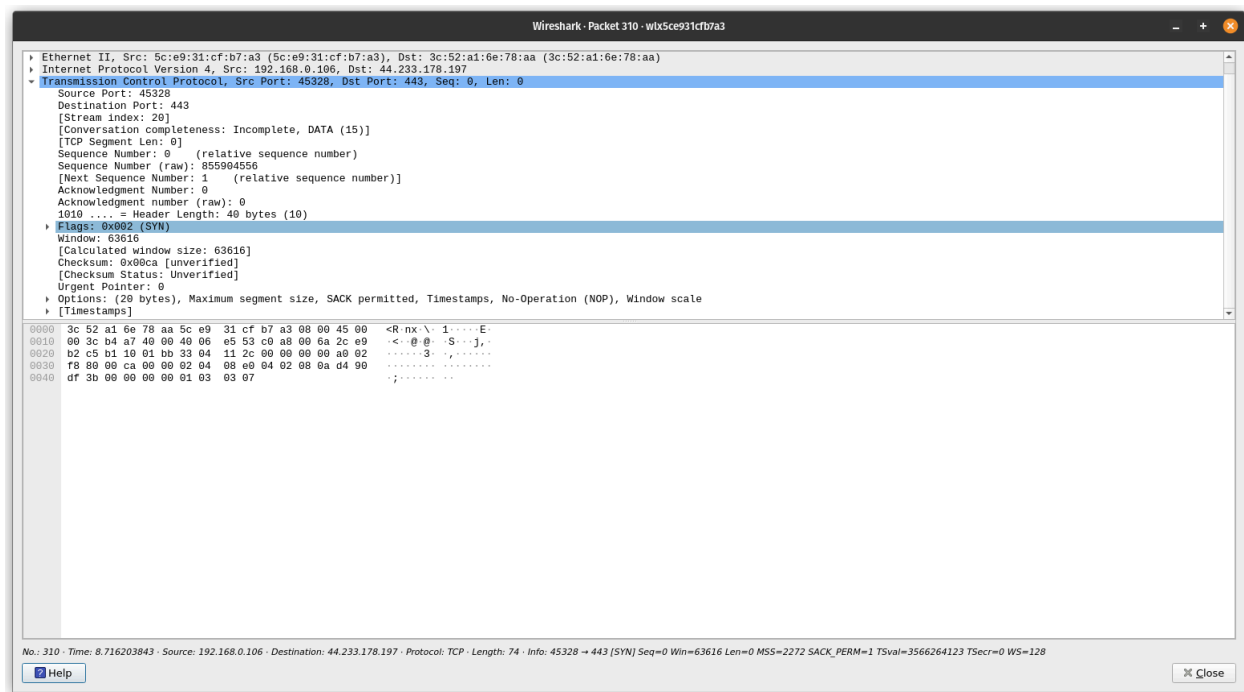
Frame 320: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface wls5ce931cfb7a3, id 0
Ethernet II, Src: 3c:52:a1:6e:78:a6 (3c:52:a1:6e:78:a6), Dst: 3c:50:31:cf:b7:a3 (3c:50:31:cf:b7:a3)
Internet Protocol Version 4, Src: 44.233.178.197, Dst: 192.168.0.106
Transmission Control Protocol, Src Port: 443, Dst Port: 45328, Seq: 0, Ack: 1, Len: 0
Source Port: 443
Destination Port: 45328
[Stream index: 20]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2413339587
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 855884557
1510 ... = Header Length: 40 bytes (10)
Flags: 0x0012 (SYN, ACK)
Window: 26847
[Calculated window size: 26847]
Checksum: 0x8009 [unverified]
[Checksum Status: Unverified]

0000 5c e0 31 cf b7 a3 3c 52 a1 6e 78 aa 00 00 45 20 \. 1 -<R -nx - E
0010 00 3c 00 00 40 00 f2 06 a7 da 2c e0 b2 5c 09 a0 <- @ - - - - -
0020 00 6a 01 b0 b1 10 8f d8 a3 c3 33 04 11 2d a0 12 - - - - -3 - - - -
0030 68 df 00 00 00 02 04 05 a0 04 02 08 0a 1b 3f h - - - - -? - - - -
0040 c4 b4 d4 9d df 3b 01 03 03 00 - - - - -

The three Dark-blue color highlighted packets are TCP packets. Each one contains a specific meaning.

There are two IP mentioned: Source and Header. Each denote the client and server.

Frame1: SYN:



Source is 192.168.0.106 (System) and Destination is 44.233.178.197 (Server).

The SYN packet is SYNCHRONIZATION, where the client sends a request to the server establishing connection

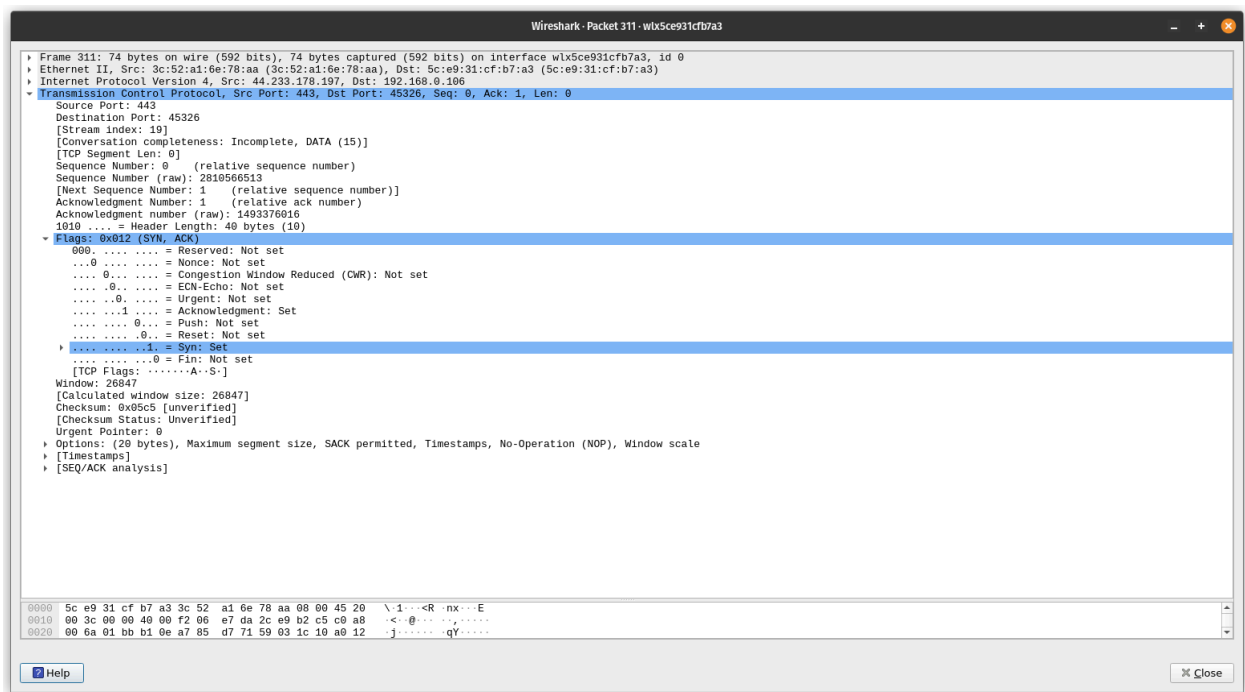
The sequence number is 0 (Although it is relative, the actual sequence number will be high). This means that this is the first request packet.

The window size is 63616

```
Flags: 0x002 (SYN)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): N
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...0 = Acknowledgment: Not set
.... .... 0... = Push: Not set
.... ..... 0.. = Reset: Not set
▶ .... .... ..1. = Syn: Set
.... .... ...0 = Fin: Not set
[TCP Flags: .....S.]
```

The flags show that only SYN is set, confirming that this is a SYNCHRONIZE packet.

FRAME 2: SYN+ACK:



Source is 44.233.178.197 (Server) and destination is 192.168.0.106 (System).

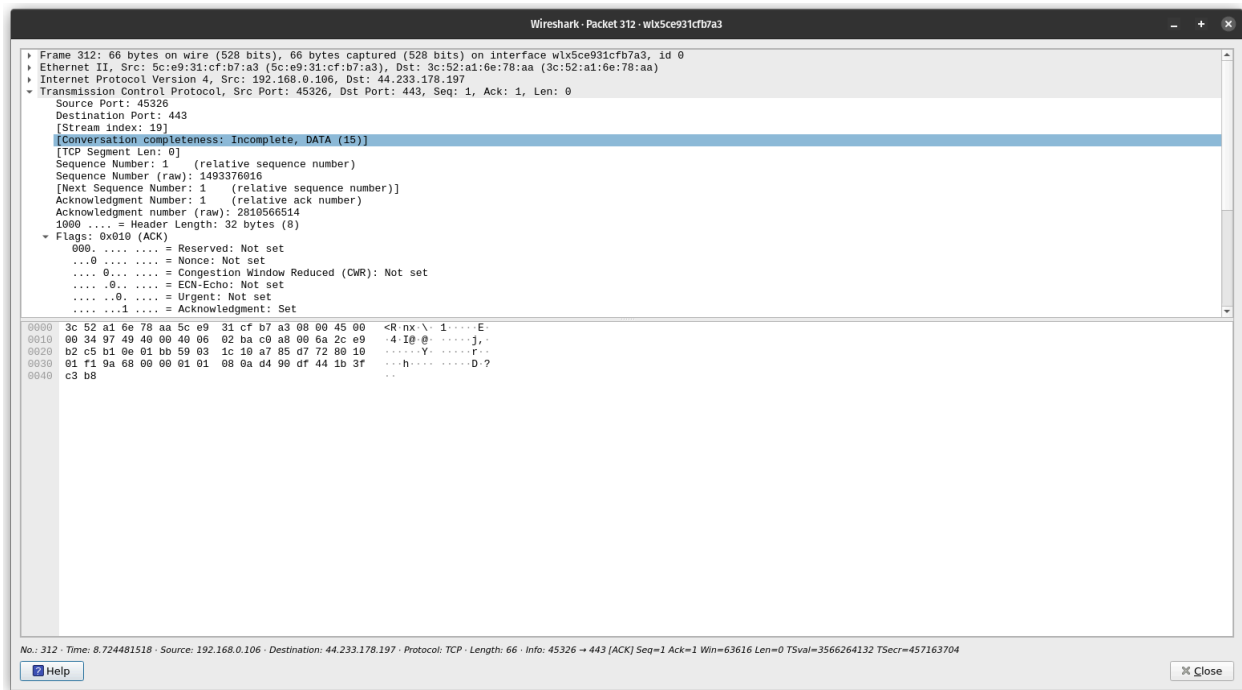
This is the second packet: SYN+ACK. This packet is a reply from server to client, acknowledging the client's request and the server is ready to establish a connection.

The window size mentioned is 26847.

According to the flags, the SYN and ACK bits are set.

Sequence number is 0 and ACK number is 1

FRAME 3: ACK:



Source is 192.168.0.106 (System) and Destination is 44.233.178.197 (Server).

This is from client to server, acknowledging the server's response and is ready to start establishing connection.

Window size is 497

Under flags section, only ACK is set

Sequence number is 1 and Ack number is 1

Query frame:

The image shows a Wireshark packet capture of a DNS query. The packet list on the left shows 'Frame 202: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface wlx5ce931cfb7a3, id 0'. The packet details pane shows the following structure:

- Ethernet II, Src: 5c:e9:31:cf:b7:a3 (5c:e9:31:cf:b7:a3), Dst: 3c:52:a1:6e:78:aa (3c:52:a1:6e:78:aa)
- Internet Protocol Version 4, Src: 192.168.0.106, Dst: 8.8.8.8
- User Datagram Protocol, Src Port: 54086, Dst Port: 53
- Domain Name System (query)
 - Transaction ID: 0x0fdd
 - Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - wireshark.org: type A, class IN
 - Name: wireshark.org
 - [Name Length: 13]
 - [Label Count: 2]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)

The packet bytes pane shows the raw data of the query frame:

```
0000  3c 52 a1 6e 78 aa 5c e9 31 cf b7 a3 08 00 45 00  -R-nx-\ 1....E-
0010  00 3b c9 67 00 00 11 00 28 c0 a8 00 6a 08 08    .;g-@- .(...)..
0020  08 08 d3 46 00 35 00 27 1f 24 0f dd 01 00 00 01  .F-5- .-$.....
0030  00 00 00 00 00 00 09 77 69 72 65 73 68 61 72 6b  .....w ireshark
0040  03 6f 72 67 00 00 01 00 01                      .org.... .
```

This is the query frame. This frame has a query to 8.8.8.8 to resolve wireshark.org into its ip addresses.

Response frame:

Wireshark · Packet 203 · wlx5ce931c7b7a3

```
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.0.106
User Datagram Protocol, Src Port: 53, Dst Port: 54086
Domain Name System (response)
  Transaction ID: 0x0fdd
  Flags: 0x8100 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 0
  Additional RRs: 0
  Queries
    wireshark.org: type A, class IN
      Name: wireshark.org
      [Name Length: 13]
      [Label Count: 2]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  Answers
    wireshark.org: type A, class IN, addr 104.26.10.240
    wireshark.org: type A, class IN, addr 104.26.11.240
    wireshark.org: type A, class IN, addr 172.67.75.39
    [Request In: 202]
    [Time: 0.004204016 seconds]
```

0000	5c e9 31 cf b7 a3 3c 52	a1 6e 78 aa 08 00 45 80	\1...cR nx...E
0010	00 6b 5c f7 00 00 7b 19	10 e9 08 08 08 08 c0 a8	-kV...[]
0020	00 6a 00 35 d3 46 00 57	f0 20 0f dd 81 80 00 01	.j 5-P-W
0030	00 03 00 00 00 00 09 77	69 72 65 73 68 61 72 6bw ireshark
0040	03 6f 72 67 00 00 01 00	01 c0 0c 00 01 00 01 00	..org.....
0050	00 00 52 00 04 68 1a 0a	f0 c0 0c 00 01 00 01 00	..R..h.....
0060	00 00 52 00 04 68 1a 0b	f0 c0 0c 00 01 00 01 00	..R..h.....
0070	00 00 52 00 04 ac 43 4b	27	..R...CK '

This is the response from 8.8.8.8, giving us the IP addresses of wireshark.org

UDP:

DNS protocol uses UDP, we will analyze the same frames:

The image shows a Wireshark packet capture of a DNS query. The packet list on the left shows 'Frame 202: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface wlx5ce931cfb7a3, id 0'. The packet details pane on the right shows the following structure:

- Ethernet II, Src: 5c:e9:31:cf:b7:a3 (5c:e9:31:cf:b7:a3), Dst: 3c:52:a1:6e:78:aa (3c:52:a1:6e:78:aa)
- Internet Protocol Version 4, Src: 192.168.0.106, Dst: 8.8.8.8
- User Datagram Protocol, Src Port: 54086, Dst Port: 53
 - Source Port: 54086
 - Destination Port: 53
 - Length: 39
 - Checksum: 0x1f24 [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 14]
 - [Timestamps]
 - UDP payload (31 bytes)
- Domain Name System (query)

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII:

```
0000  3c 52 a1 6e 78 aa bc e9 31 cf b7 a3 08 00 45 00  <R-nx-vv1....E-
0010  00 0b 09 67 00 00 40 11 d0 28 c0 a8 00 6a 08 08  .;g-@-.(...j..
0020  08 00 d3 46 00 35 00 27 1f 24 0f dd 01 00 00 01  ..F-5-.-$. ....
0030  00 00 00 00 00 00 09 77 69 72 65 73 68 61 72 6b  .....w ireshark
0040  03 6f 72 67 00 00 01 00 01                      .org.....
```

Here we can see there is a section about User Datagram Protocol. It has a Source port 54086, Destination port 53, length of data (including headers) as 39. The data itself is the DNS query/response. There is a checksum to check if the packet received has no error/data loss.