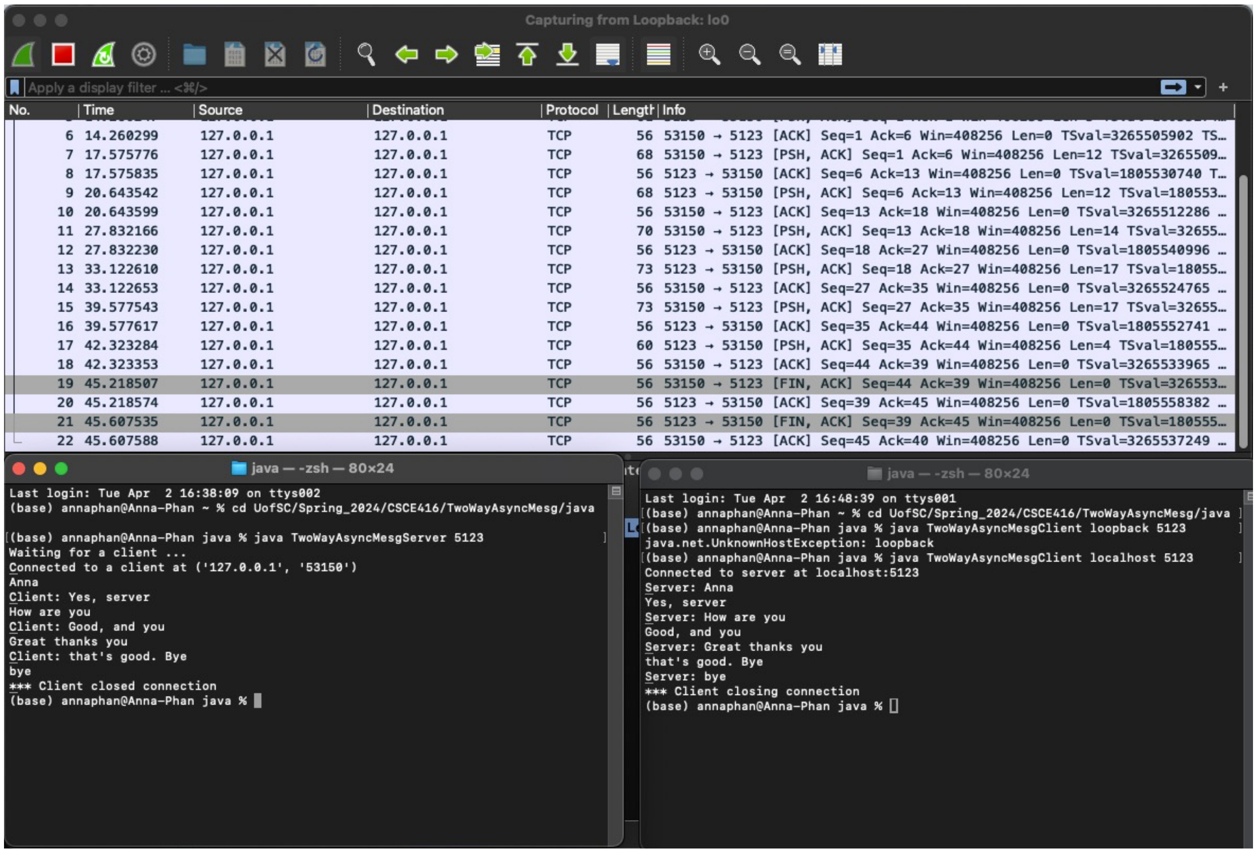
Q1 - Server was started on port **5123**

Screenshot one:



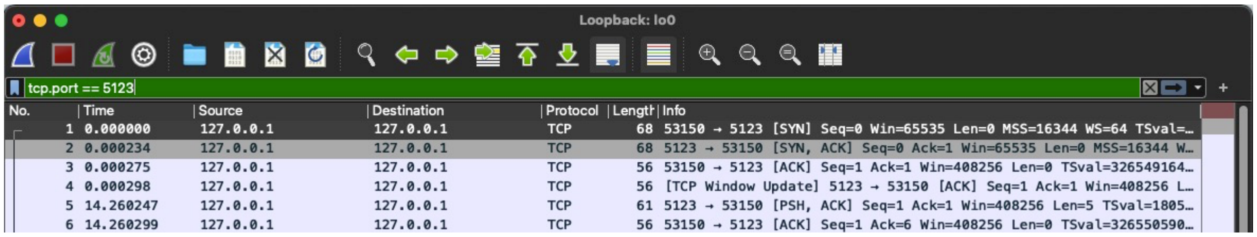
```
No.  Time       Source     Destination  Protocol Length Info
  6  14.260299  127.0.0.1  127.0.0.1    TCP       56  53150 → 5123 [ACK] Seq=1 Ack=6 Win=408256 Len=0 TSval=3265505902 TS…
  7  17.575776  127.0.0.1  127.0.0.1    TCP       68  53150 → 5123 [PSH, ACK] Seq=1 Ack=6 Win=408256 Len=12 TSval=3265509…
  8  17.575835  127.0.0.1  127.0.0.1    TCP       56  5123 → 53150 [ACK] Seq=6 Ack=13 Win=408256 Len=0 TSval=1805530740 T…
  9  20.643542  127.0.0.1  127.0.0.1    TCP       68  5123 → 53150 [PSH, ACK] Seq=6 Ack=13 Win=408256 Len=12 TSval=180553…
 10  20.643599  127.0.0.1  127.0.0.1    TCP       56  53150 → 5123 [ACK] Seq=13 Ack=18 Win=408256 Len=0 TSval=3265512286 …
 11  27.832166  127.0.0.1  127.0.0.1    TCP       70  53150 → 5123 [PSH, ACK] Seq=13 Ack=18 Win=408256 Len=14 TSval=32655…
 12  27.832230  127.0.0.1  127.0.0.1    TCP       56  5123 → 53150 [ACK] Seq=18 Ack=27 Win=408256 Len=0 TSval=1805540996 …
 13  33.122610  127.0.0.1  127.0.0.1    TCP       73  5123 → 53150 [PSH, ACK] Seq=18 Ack=27 Win=408256 Len=17 TSval=18055…
 14  33.122653  127.0.0.1  127.0.0.1    TCP       56  53150 → 5123 [ACK] Seq=27 Ack=35 Win=408256 Len=0 TSval=3265524765 …
 15  39.577543  127.0.0.1  127.0.0.1    TCP       73  53150 → 5123 [PSH, ACK] Seq=27 Ack=35 Win=408256 Len=17 TSval=32655…
 16  39.577617  127.0.0.1  127.0.0.1    TCP       56  5123 → 53150 [ACK] Seq=35 Ack=44 Win=408256 Len=0 TSval=1805552741 …
 17  42.323284  127.0.0.1  127.0.0.1    TCP       60  5123 → 53150 [PSH, ACK] Seq=35 Ack=44 Win=408256 Len=4 TSval=180555…
 18  42.323353  127.0.0.1  127.0.0.1    TCP       56  53150 → 5123 [ACK] Seq=44 Ack=39 Win=408256 Len=0 TSval=3265533965 …
 19  45.218507  127.0.0.1  127.0.0.1    TCP       56  53150 → 5123 [FIN, ACK] Seq=44 Ack=39 Win=408256 Len=0 TSval=326553…
 20  45.218574  127.0.0.1  127.0.0.1    TCP       56  5123 → 53150 [ACK] Seq=39 Ack=45 Win=408256 Len=0 TSval=1805558382 …
 21  45.607535  127.0.0.1  127.0.0.1    TCP       56  5123 → 53150 [FIN, ACK] Seq=39 Ack=45 Win=408256 Len=0 TSval=180555…
 22  45.607588  127.0.0.1  127.0.0.1    TCP       56  53150 → 5123 [ACK] Seq=45 Ack=40 Win=408256 Len=0 TSval=3265537249 …
```

```
Last login: Tue Apr  2 16:38:09 on ttys002
(base) annaphan@Anna-Phan ~ % cd UofSC/Spring_2024/CSCE416/TwoWayAsyncMesg/java

(base) annaphan@Anna-Phan java % java TwoWayAsyncMesgServer 5123
Waiting for a client ...
Connected to a client at ('127.0.0.1', '53150')
Anna
Client: Yes, server
How are you
Client: Good, and you
Great thanks you
Client: that's good. Bye
bye
*** Client closed connection
(base) annaphan@Anna-Phan java %
```

```
Last login: Tue Apr  2 16:48:39 on ttys001
(base) annaphan@Anna-Phan ~ % cd UofSC/Spring_2024/CSCE416/TwoWayAsyncMesg/java
(base) annaphan@Anna-Phan java % java TwoWayAsyncMesgClient loopback 5123
java.net.UnknownHostException: loopback
(base) annaphan@Anna-Phan java % java TwoWayAsyncMesgClient localhost 5123
Connected to server at localhost:5123
Server: Anna
Yes, server
Server: How are you
Good, and you
Server: Great thanks you
that's good. Bye
Server: bye
*** Client closing connection
(base) annaphan@Anna-Phan java %
```

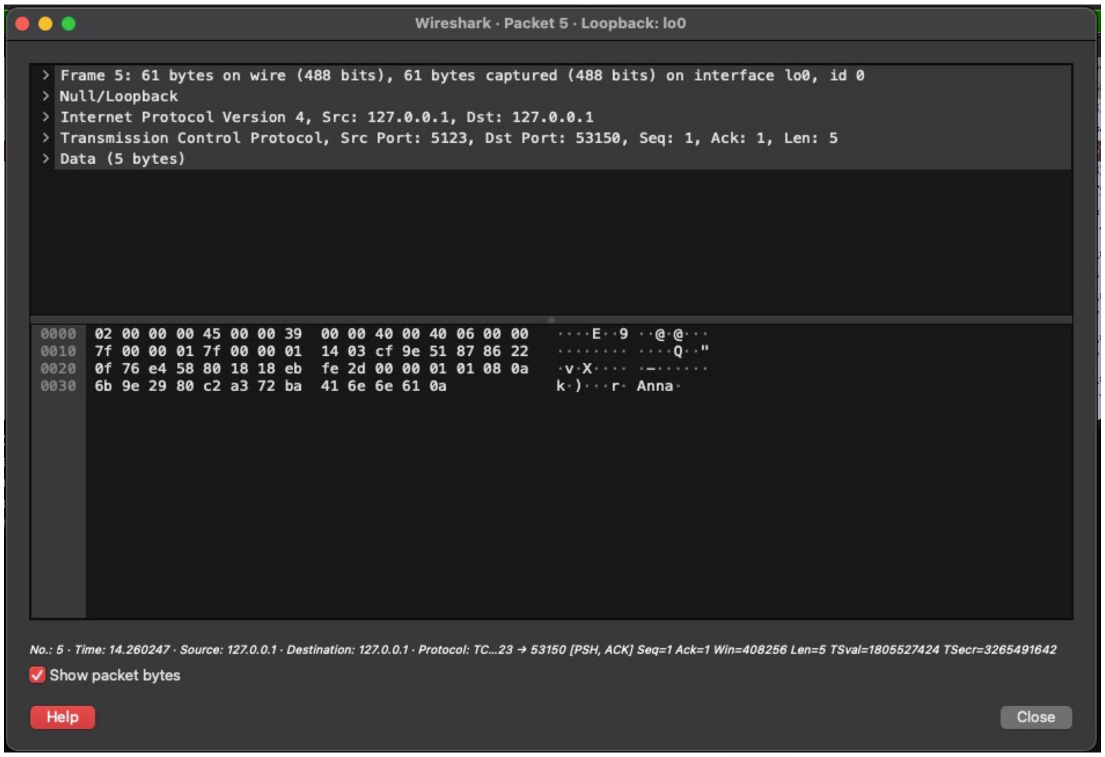
Screenshot two:



```
No.  Time       Source     Destination  Protocol Length Info
  1  0.000000   127.0.0.1  127.0.0.1    TCP       68  53150 → 5123 [SYN] Seq=0 Win=65535 Len=0 MSS=16344 WS=64 TSval=…
  2  0.000234   127.0.0.1  127.0.0.1    TCP       68  5123 → 53150 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=16344 W…
  3  0.000275   127.0.0.1  127.0.0.1    TCP       56  53150 → 5123 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=326549164…
  4  0.000298   127.0.0.1  127.0.0.1    TCP       56  [TCP Window Update] 5123 → 53150 [ACK] Seq=1 Ack=1 Win=408256 L…
  5  14.260247  127.0.0.1  127.0.0.1    TCP       61  5123 → 53150 [PSH, ACK] Seq=1 Ack=1 Win=408256 Len=5 TSval=1805…
  6  14.260299  127.0.0.1  127.0.0.1    TCP       56  53150 → 5123 [ACK] Seq=1 Ack=6 Win=408256 Len=0 TSval=326550590…
```

Q2 - Client's TCP Source port is **53150**

Screenshot three:



```
> Frame 5: 61 bytes on wire (488 bits), 61 bytes captured (488 bits) on interface lo0, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 5123, Dst Port: 53150, Seq: 1, Ack: 1, Len: 5
> Data (5 bytes)
```

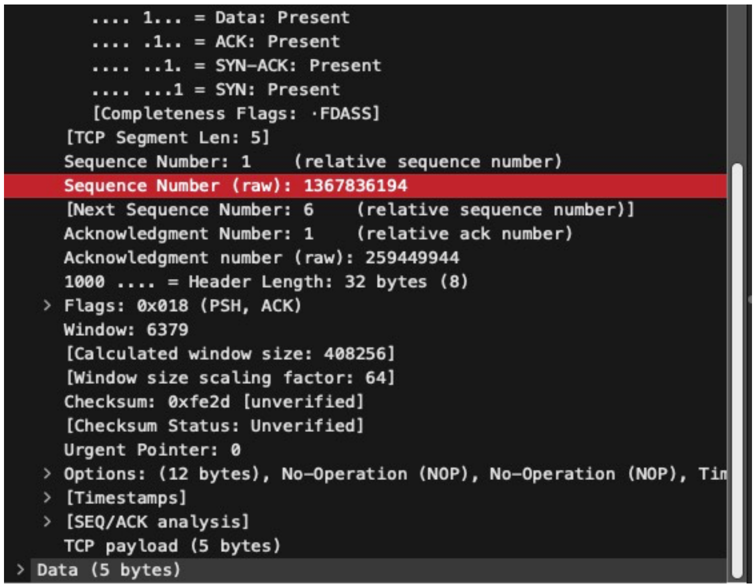
```
0000  02 00 00 00 45 00 00 39  00 00 40 00 40 06 00 00   ····E··9 ··@·@···
0010  7f 00 00 01 7f 00 00 01  14 03 cf 9e 51 87 86 22   ········ ····Q··"
0020  0f 76 e4 58 80 18 18 eb  fe 2d 00 00 01 01 08 0a   ·v·X···· ·-······
0030  6b 9e 29 80 c2 a3 72 ba  41 6e 6e 61 0a            k·)···r· Anna·
```

No.: 5 · Time: 14.260247 · Source: 127.0.0.1 · Destination: 127.0.0.1 · Protocol: TC...23 → 53150 [PSH, ACK] Seq=1 Ack=1 Win=408256 Len=5 TSval=1805527424 TSecr=3265491642

✓ Show packet bytes

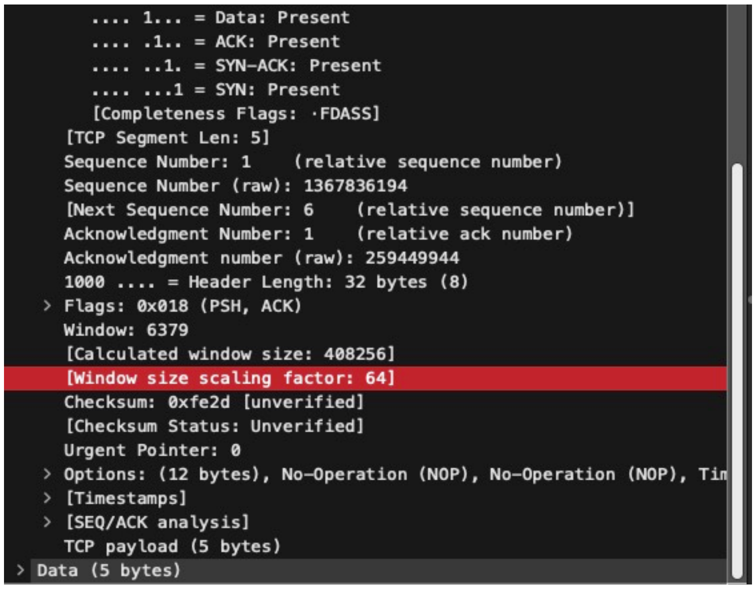
Q3 - TCP Sequence numbers don't always start at 0 because **to avoid ambiguity and make TCP more secure. Starting from 0 might create ambiguity during connection establishment or reestablishment. By starting with a non-zero initial sequence number, TCP can make it harder for attackers to predict or spoof sequence numbers in TCP packets, which helps enhance security against certain types of attacks, such as sequence number guessing attacks. Therefore, TCP starts with a random initial sequence number, typically chosen to be a large enough value to avoid collisions with previous connections and to provide a level of security against attacks.**

Screenshot Four:



```
        .... 1... = Data: Present
        .... .1.. = ACK: Present
        .... ..1. = SYN-ACK: Present
        .... ...1 = SYN: Present
        [Completeness Flags: ·FDASS]
    [TCP Segment Len: 5]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1367836194
    [Next Sequence Number: 6    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 259449944
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
    Window: 6379
    [Calculated window size: 408256]
    [Window size scaling factor: 64]
    Checksum: 0xfe2d [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Tin
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (5 bytes)
> Data (5 bytes)
```

Screenshot five:



```
        .... 1... = Data: Present
        .... .1.. = ACK: Present
        .... ..1. = SYN-ACK: Present
        .... ...1 = SYN: Present
        [Completeness Flags: ·FDASS]
    [TCP Segment Len: 5]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1367836194
    [Next Sequence Number: 6    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 259449944
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
    Window: 6379
    [Calculated window size: 408256]
    [Window size scaling factor: 64]
    Checksum: 0xfe2d [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Tin
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (5 bytes)
> Data (5 bytes)
```

Q4 - The Window Scale Factor is **used to increase the effective window size beyond the 16-bit limit imposed by the TCP header. It allows TCP to support larger window sizes, which are crucial for optimizing data transmission over high-speed and high-latency networks. By using the window scale factor, TCP can efficiently utilize available network bandwidth and reduce the impact of network latency on data transmission.**