

## Wireshark – TCP Assignment

Name : Serena Anthony

Roll.NO : B210031CS

1. What are the packets involved in 3-way handshake (provide packet id and highlight those packets in screenshot)?

1	0.000000000	192.168.120.61	143.129.69.1	TCP	74 52060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=
2	0.009982186	143.129.69.1	192.168.120.61	TCP	74 80 → 52060 [SYN, ACK] Seq=0 Ack=1 Win=5792
3	0.009927788	192.168.120.61	143.129.69.1	TCP	66 52060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=

SYN: This packet is sent from the client to the server to initiate the connection.

Identification: 0x7eca (32458)



SYN-ACK: This packet is sent from the server back to the client in response to the SYN packet.

Identification: 0x2d50 (11600)



ACK: This packet is sent from the client to the server to acknowledge the receipt of the SYN-ACK packet.

Identification: 0x7ecb (32459)

```

10.000000000 192.168.128.01 143.129.08.1 TCP 66 52068 → 80 [ACK] Seq=14311834 Win=64256 Len=0
* Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface wlp0s20f3, id 0
* Ethernet II, Src: IntelCor_08:e5:d7 (08:0d:0e:06:e5:d7), Dst: Fortinet_08:00:12 (08:00:0f:00:00:12)
* Internet Protocol Version 4, Src: 192.168.128.01, Dst: 143.129.08.1
  0100 .... = Version: 4
  .... 0100 = Header Length: 20 bytes (5)
  * Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 52
  Identification: 3a7ecb (32059)

```

2. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the your client computer (your machine) and <http://fimi.uantwerpen.be/data/>?

Ans:

We find the sequence number of the TCP SYN segment by looking into the TCP SYN packet in the 3-way handshake. This value is usually a random value generated by the client to initiate connection.

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 3145061983

```

10.000000000 192.168.128.01 143.129.08.1 TCP 74 52000 → 80 [SYN] Seq=0 Win=64240 Len=0
* Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface wlp0s20f3, id 0
* Ethernet II, Src: IntelCor_08:e5:d7 (08:0d:0e:06:e5:d7), Dst: Fortinet_08:00:12 (08:00:0f:00:00:12)
* Internet Protocol Version 4, Src: 192.168.128.01, Dst: 143.129.08.1
* Transmission Control Protocol, Src Port: 52000, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 52000
  Destination Port: 80
  [Stream index: 0]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 3145061983

```

3. What is the sequence number of the SYNACK segment sent by <http://fimi.uantwerpen.be/> to the client computer in reply to the SYN? What is the value of the Acknowledgment field in the SYNACK segment?

The sequence number of the SYNACK segment is generally a random value generated by the server. The acknowledgment field acknowledges the SYN segment from the client.

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 412229550

Acknowledgment Number: 1 (relative ack number)

```

2 0.000002166 143.129.69.1 192.168.129.61 TCP 74 60 - 52880 [SYN, ACK] Seq=0 Ack=1 Win=65535
*
* Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface wlp8s20f3, id 0
* Ethernet II, Src: Fortinet_09:00:12:00:00:0f:00:00:12, Dst: IntelCor_86:c5:d7 (86:dd:8e:08:c5:d7)
* Internet Protocol Version 4, Src: 143.129.69.1, Dst: 192.168.129.61
* Transmission Control Protocol, Src Port: 80, Dst Port: 52880, Seq: 0, Ack: 1, Len: 0
  Source Port: 80
  Destination Port: 52880
  [Stream index: 0]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 412229550
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 3145061984

```

Acknowledgment number (raw): 3145061984

4. What is the length of each of the first six TCP segments?

1 0.000000000	192.168.129.61	143.129.69.1	TCP	74 52880 - 60 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=17182
2 0.000002166	143.129.69.1	192.168.129.61	TCP	74 60 - 52880 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM T
3 0.000027758	192.168.129.61	143.129.69.1	TCP	60 52880 - 60 [ACK] Seq=1 Ack=1 Win=65535 Len=0 TSval=171824678 TSecr=3
4 0.010057309	192.168.129.61	143.129.69.1	HTTP	523 GET /data/webdock.dat.gz HTTP/1.1
5 0.013585244	143.129.69.1	192.168.129.61	TCP	60 60 - 52880 [ACK] Seq=1 Ack=458 Win=6400 Len=0 TSval=3397561982 TSecr=1
6 0.350075073	143.129.69.1	192.168.129.61	TCP	2896 60 - 52880 [ACK] Seq=1 Ack=458 Win=6400 Len=2896 TSval=3397561938 TSec
7 0.350095493	192.168.129.61	143.129.69.1	TCP	60 52880 - 60 [ACK] Seq=458 Ack=2897 Win=61448 Len=0 TSval=1718246057 TS

TCP Packet 1 len = 0

TCP Packet 2 len = 0

TCP Packet 3 len = 0

HTTP packet len = 457

TCP Packet 4 len = 0

TCP Packet 5 len = 2896

TCP Packet 6 len = 0

5. What is the minimum amount of available buffer space advertised at the received for the entire trace?

```

213 6 189119159 143.129.69.1 192.168.129.62 TCP 5808 88 - 38598 [ACK] Seq=168729 Ack=458 Win=6488
* Frame 213: 5808 bytes on wire (46064 bits), 5808 bytes captured (46064 bits) on interface wlp8s20f3, id 0
Ethernet II, Src: Fortinet_08:00:0c:00:00:12, Dst: IntelCor_08:e5:d7:69:6d:8a:06:e5:d7
Internet Protocol Version 4, Src: 143.129.69.1, Dst: 192.168.129.62
Transmission Control Protocol, Src Port: 88, Dst Port: 38598, Seq: 168729, Ack: 458, Len: 5792
  Source Port: 88
  Destination Port: 38598
  [Stream index: 18]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP segment Len: 5792]
  Sequence Number: 168729 (relative sequence number)
  Sequence Number (raw): 290807342
  [Next Sequence Number: 168521 (relative sequence number)]
  Acknowledgment Number: 458 (relative ack number)
  Acknowledgment number (raw): 324628807
  1890 .... = Header Length: 32 bytes (8)
  * Flags: 0x010 (ACK)
  Window: 50
  [Calculated window size: 6488]
  [Window size scaling factor: 128]

```

imum amount of buffer space advertised at the received for the entire trace is **50**

6. What did you observe in the packet trace when you pause the downloading in between?

Ans:

When the download was paused in between I observed a stream of TCP Keep-Alive, TCP Window Full and TCP ZeroWindow packets.

[illegible]

7. Are there any TCP Out-Of-Order and/or TCP Fast Retransmission segments on the collected trace? Discuss?

Ans:

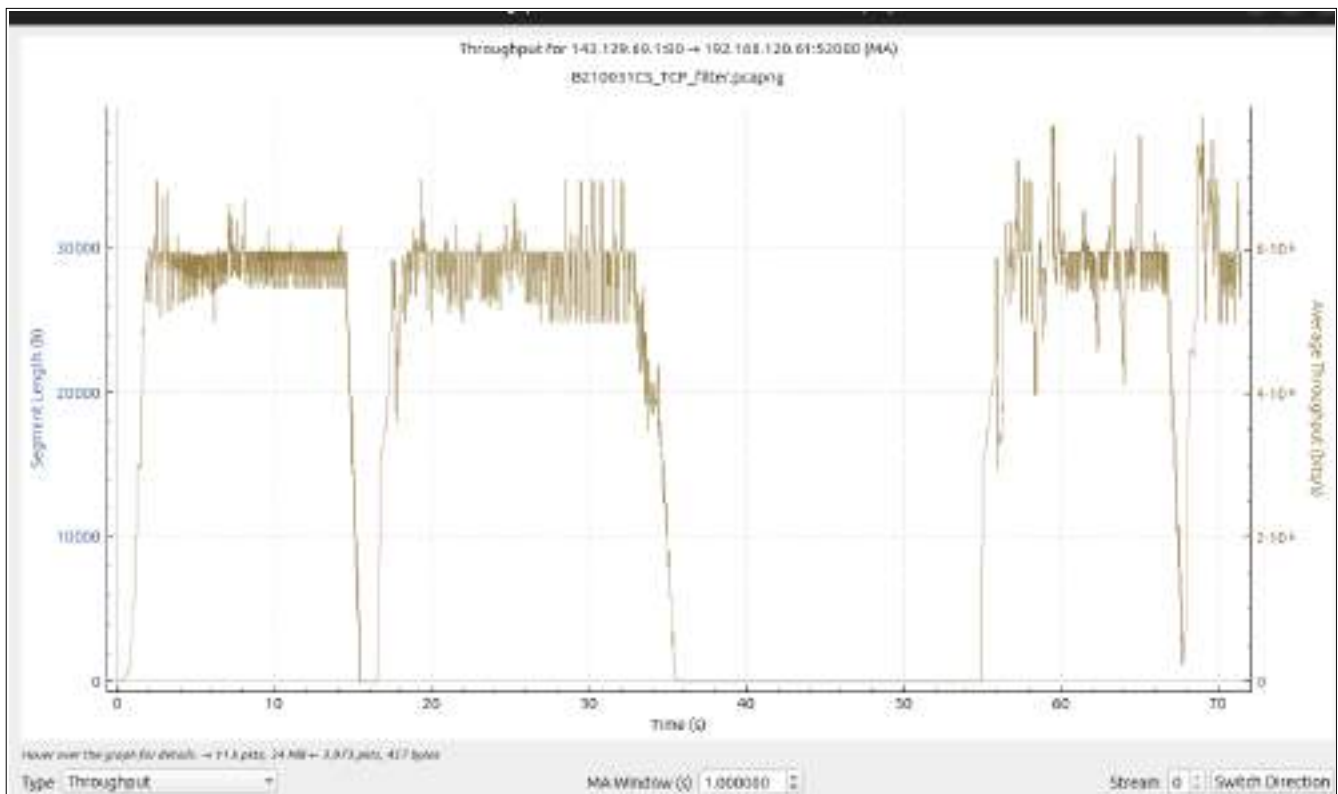


There are no tcp out-of-order and/or tcp-fast retransmission segments rather there is tcp-retransmission segments which indicate packet loss during the process. (as seen from image below)

9156	33.136881402	192.168.128.61	192.168.128.61	TCP	78 [TCP Dup ACK 914295] Seq=458 Ack=22254313
9157	33.136881402	192.168.128.61	192.168.128.61	TCP	1514 [TCP Retransmission] Seq=458 Ack=22254313
9158	33.136881402	192.168.128.61	192.168.128.61	TCP	1514 [TCP Retransmission] Seq=458 Ack=22254313
9159	33.136881402	192.168.128.61	192.168.128.61	TCP	1514 [TCP Retransmission] Seq=458 Ack=22254313
9160	33.136881402	192.168.128.61	192.168.128.61	TCP	1514 [TCP Retransmission] Seq=458 Ack=22254313
9161	33.136881402	192.168.128.61	192.168.128.61	TCP	78 [TCP Dup ACK 914295] Seq=458 Ack=22254313
9162	33.136881402	192.168.128.61	192.168.128.61	TCP	78 [TCP Dup ACK 914295] Seq=458 Ack=22254313
9163	33.136881402	192.168.128.61	192.168.128.61	TCP	78 [TCP Dup ACK 914295] Seq=458 Ack=22254313
9164	33.136881402	192.168.128.61	192.168.128.61	TCP	78 [TCP Dup ACK 914295] Seq=458 Ack=22254313
9165	33.136881402	192.168.128.61	192.168.128.61	TCP	1514 [TCP Retransmission] Seq=458 Ack=22254313
9166	33.136881402	192.168.128.61	192.168.128.61	TCP	1514 [TCP Retransmission] Seq=458 Ack=22254313
9167	33.136881402	192.168.128.61	192.168.128.61	TCP	1514 [TCP Retransmission] Seq=458 Ack=22254313
9168	33.136881402	192.168.128.61	192.168.128.61	TCP	1514 [TCP Retransmission] Seq=458 Ack=22254313
9169	33.136881402	192.168.128.61	192.168.128.61	TCP	78 [TCP Dup ACK 914295] Seq=458 Ack=22254313
9170	33.136881402	192.168.128.61	192.168.128.61	TCP	78 [TCP Dup ACK 914295] Seq=458 Ack=22254313
9171	33.136881402	192.168.128.61	192.168.128.61	TCP	78 [TCP Dup ACK 914295] Seq=458 Ack=22254313
9172	33.136881402	192.168.128.61	192.168.128.61	TCP	4410 [TCP Retransmission] Seq=458 Ack=22254313
9173	33.136881402	192.168.128.61	192.168.128.61	TCP	78 [TCP Dup ACK 914295] Seq=458 Ack=22254313
9174	33.136881402	192.168.128.61	192.168.128.61	TCP	1514 [TCP Retransmission] Seq=458 Ack=22254313
9175	33.136881402	192.168.128.61	192.168.128.61	TCP	78 [TCP Dup ACK 914295] Seq=458 Ack=22254313
9176	33.136881402	192.168.128.61	192.168.128.61	TCP	1514 [TCP Retransmission] Seq=458 Ack=22254313
9177	33.136881402	192.168.128.61	192.168.128.61	TCP	78 [TCP Dup ACK 914295] Seq=458 Ack=22254313
9178	33.136881402	192.168.128.61	192.168.128.61	TCP	1514 [TCP Retransmission] Seq=458 Ack=22254313
9179	33.136881402	192.168.128.61	192.168.128.61	TCP	78 [TCP Dup ACK 914295] Seq=458 Ack=22254313
9180	33.136881402	192.168.128.61	192.168.128.61	TCP	1514 [TCP Retransmission] Seq=458 Ack=22254313
9181	33.136881402	192.168.128.61	192.168.128.61	TCP	78 [TCP Dup ACK 914295] Seq=458 Ack=22254313
9182	33.136881402	192.168.128.61	192.168.128.61	TCP	1514 [TCP Retransmission] Seq=458 Ack=22254313

8. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value. In addition, add the screenshot by doing the following step: Select one of the TCP segments, then select the menu : Statistics->TCP Stream Graph-> Throughput.

The maximum throughput value for the TCP connection is approximately **7.842\* 10<sup>6</sup> bits/s**. (We get this value by observing the highest value from the graph below)



9. Select one of the TCP segments, then select the menu : Statistics->TCP Stream Graph-> Time-SequenceGraph (Stevens). From the graph answer the questions below:

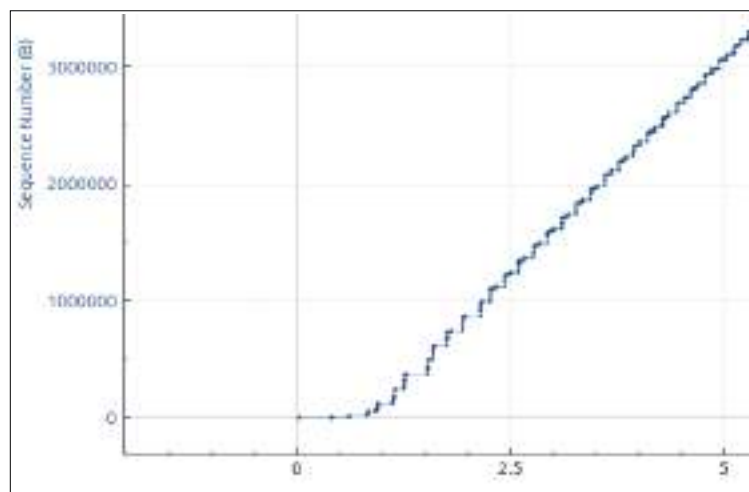
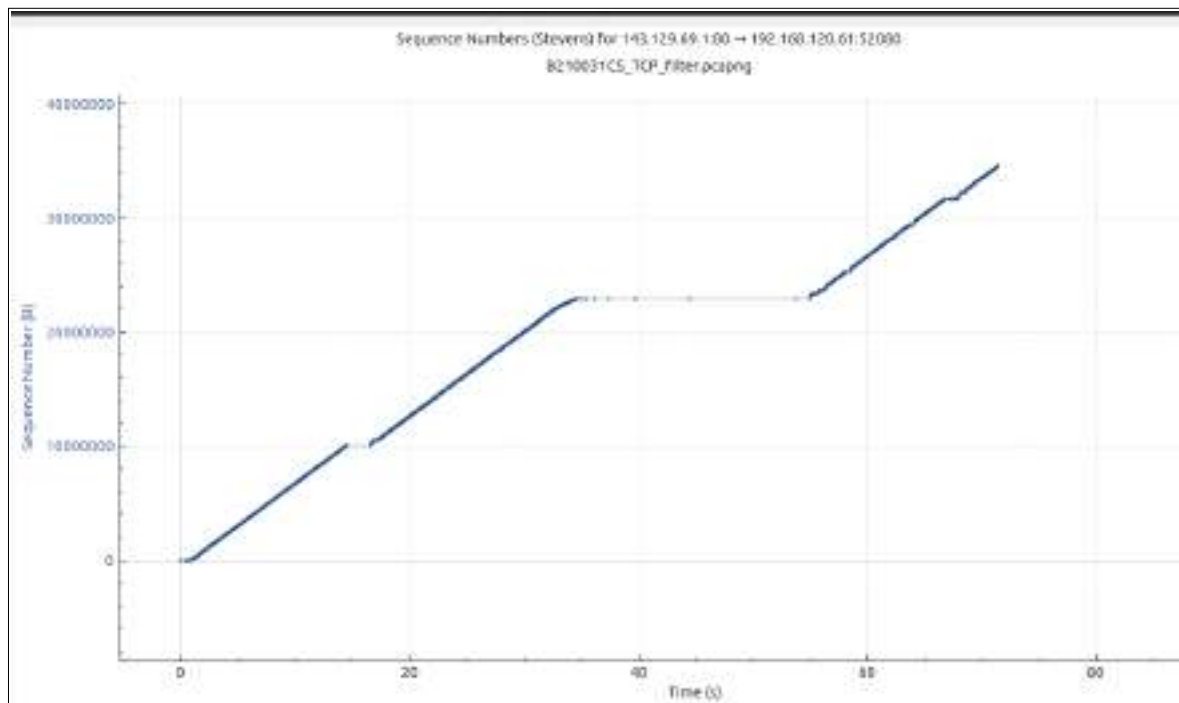
1. Where and when the slow start phase begins and ends (also attach the zoomed plot)? You can zoom the graph and see it.

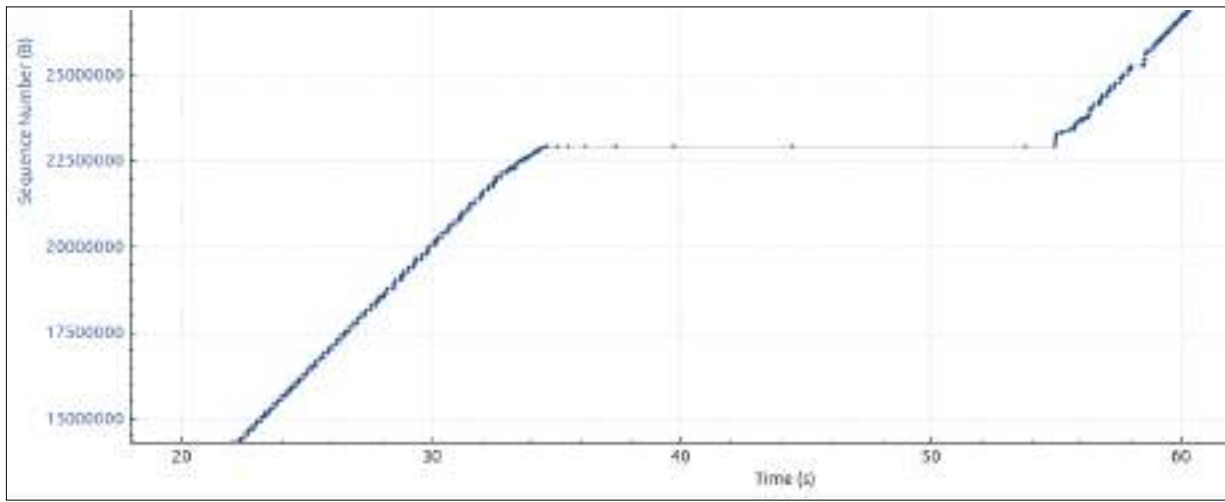
Ans:

The slow start phase is an initial phase in the TCP congestion control algorithm (begins at the start of the TCP connection or after a period of idle time where no segments are being transmitted.) It is designed to gradually increase the sending rate of data packets from the sender to probe the available network capacity and avoid overwhelming the network with traffic.

The end of the slow start phase is marked by the sender reaching either the congestion avoidance threshold or experiencing congestion, whichever comes first

From the graph, the slow start phase begins at around **1 second** and the slow end phase ends at around **32 seconds**.





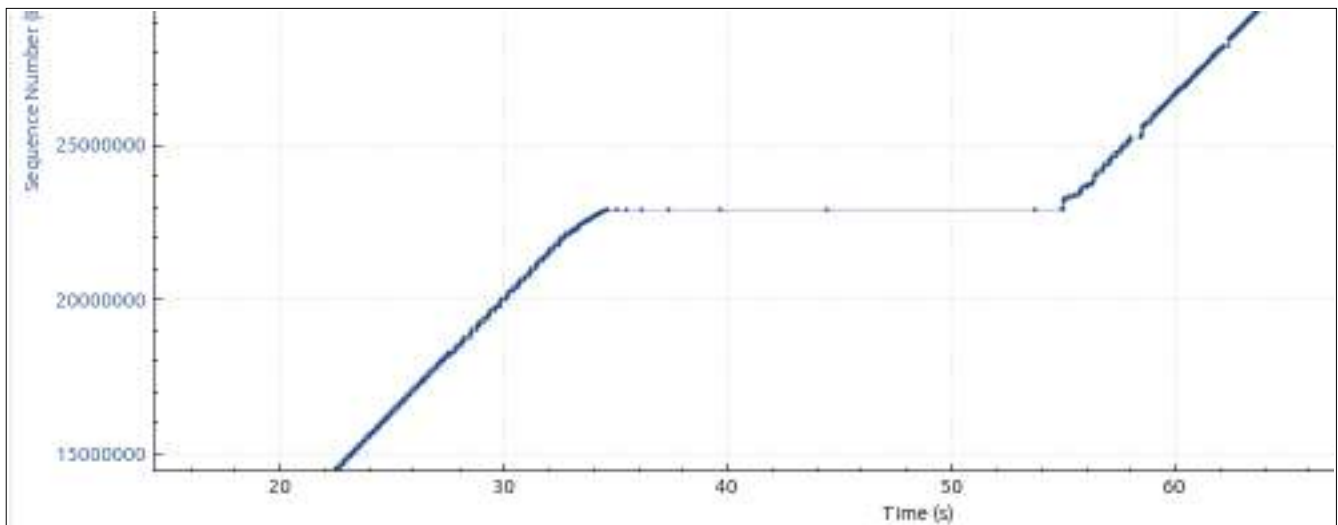
2. Where and when congestion avoidance takes over? You can zoom the graph and see it.

Ans:

Congestion avoidance takes place after the slow start phase in the TCP congestion control algorithm. Once the sender's congestion window size reaches a predefined threshold known as the congestion avoidance threshold, the congestion avoidance phase begins.

In the graph below, Congestion avoidance takes over at around **55 seconds**.





## PLAGIARISM STATEMENT

*I certify that this assignment/report is my own work, based on my personal study and/or research on my personal/lab equipment and that I have acknowledged all material and sources used in its preparation, whether they be books, articles, reports, lecture notes, and any other kind of document, electronic or personal communication. I also certify that this assignment/report has not previously been submitted for assessment in any other course, except where specific permission has been granted from all course instructors involved, or at any other time in this course, and that I have not copied in part or whole or otherwise plagiarised the work of other students and/or persons. I pledge to uphold the principles of honesty and responsibility at CSE@NITC. In addition, I understand my responsibility to report honour violations by other students if I become aware of it.*

**Name:Serena Anthony**

**Date:17/04/2024**

**Signature: S.A**