TCS332 Fundamental of Information Security and Blockchain

B. Tech CSE III Semester

Topic: TCP 3 way handshake (Exercise)

Instructor:

Dr Mohammad Wazid

Professor, Department of CSE
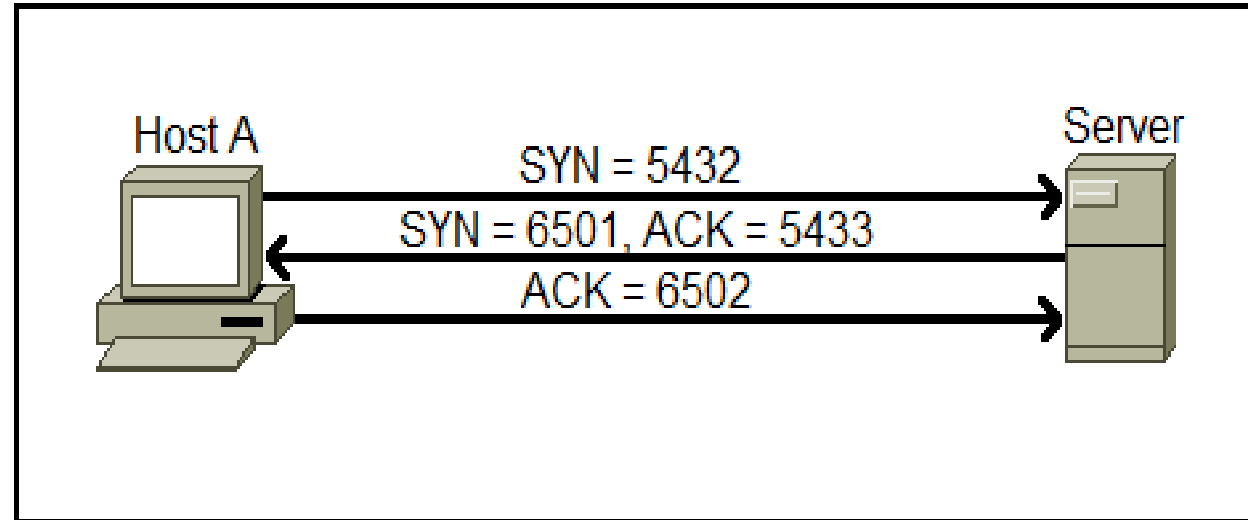
Graphic Era (Deemed to be University), Dehradun, India

Email: wazidkec2005@gmail.com

Homepage: https://sites.google.com/site/mwazidiiith/home

Topic: TCP 3 way handshake

TCP three-way handshake

- For example,

Exercise using Wireshark and TCP trace file

- Inspect the provided TCP trace file and answer the following questions:
- **Q1: In the connection establishment (i.e., in TCP 3 way handshake) what is the IP address of client and server.**

Answer:

Apply following filter:

tcp.flags.syn==1

Source IP (client): 192.168.1.122

Destination IP (server): 64.238.147.133

Q2: What are the source and destination port numbers.

Answer: Source port (client): 60643

Destination port (server): 80

Q3: In how many packets syn flag is set to 1.

Answer:2

Use filter: tcp.flags.syn==1

Q4: In the scenario of connection establishment provide the values of different sequence numbers and acknowledgement numbers:
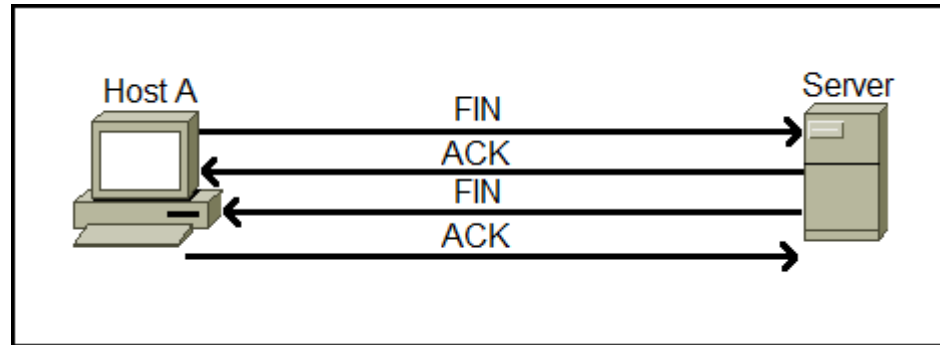
Answer:

Seq 0 (from client to server)

Seq 0 Ack 1 (from server to client)

Seq 1 Ack 1 (from client to server)

TCP connection termination

- After the data transmission process is finished, TCP will terminate the connection between two endpoints.

- This four-step process is illustrated below:

Connection termination (in TCP)

- Inspect the provided TCP trace file and answer the following questions:

- **Q1: In the connection termination (closing) what is the IP address of client and server.**

Answer:

Apply following filter:

tcp.flags.fin==1 (because fin bit will be set to 1)

Source IP (client): 192.168.1.122

Destination IP (server): 64.238.147.133

Q2: What are the source and destination port numbers.

Answer: Source IP (client): 60643

Destination IP (server): 80

Q3: In how many packets fin flag is set to 1.

Answer:2

Use filter: tcp.flags.fin==1

Q4: In the scenario of connection termination provide the values of different sequence numbers and acknowledgement numbers:

Answer:

Use filter: tcp.flags.fin==1

Seq 192 Ack 1056771 (from client to server)

Seq 1056771 Ack 193 (from server to client)

References

2. Data Communications and Networking Textbook by Behrouz A. Forouzan

1.9