Analysis TCP normal three-way handshake working flow

The TCP handshake occurs in three separate steps

1. In the first step, the device that wants to communicate, This initial packet contains no data.

SYN flag set and includes the initial sequence number and maximum segment size (MSS) that will be used for the communication process to Host B

2. Host B responds to this packet by sending a similar packet with the SYN and ACK flags.

3. Finally, host A sends ACK flag to Host B

After above step done, two host are begin communicating properly.

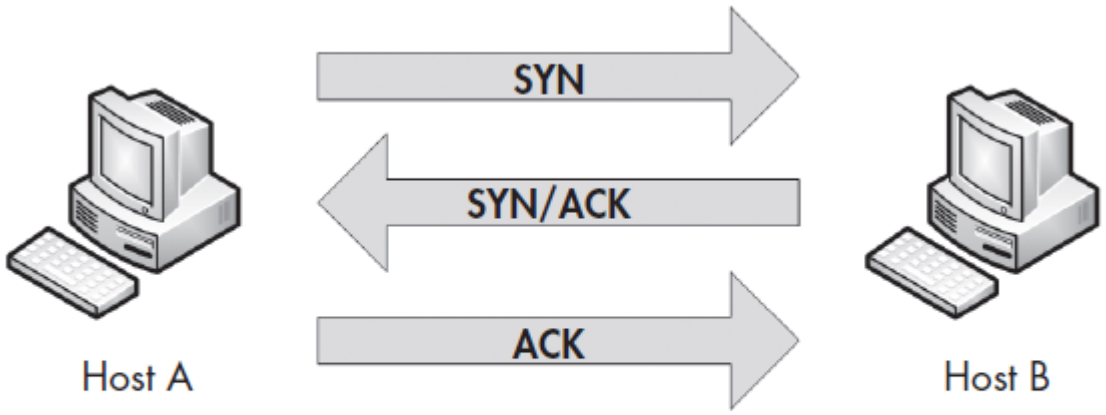
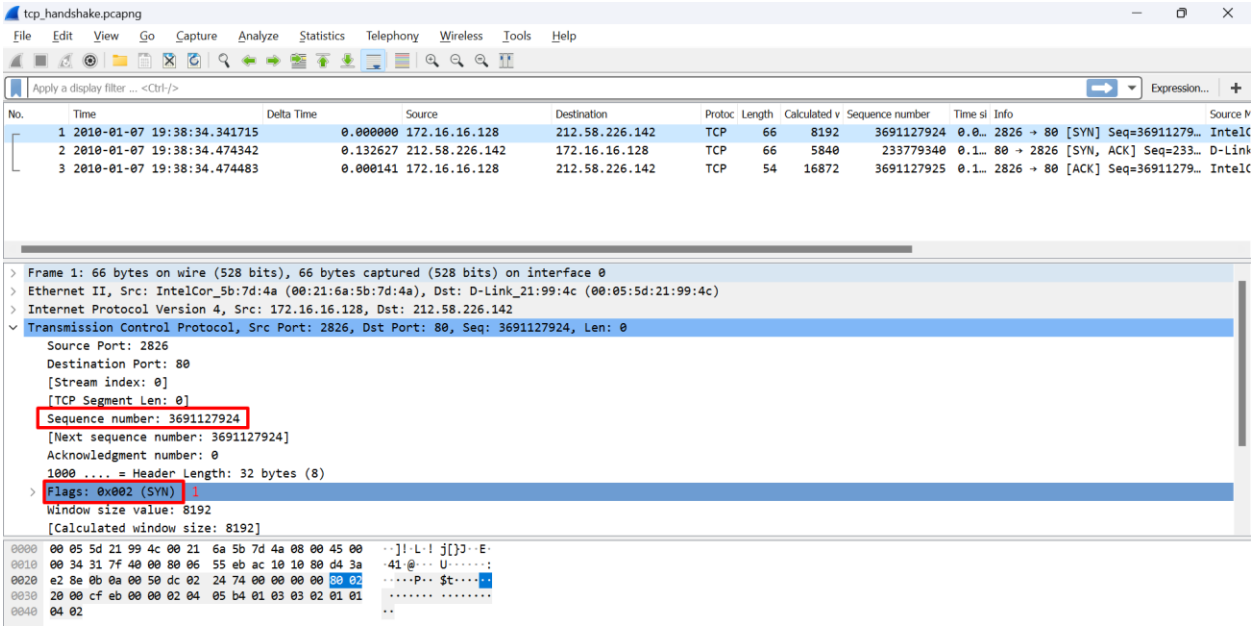


Figure 6-20: The TCP three-way handshake

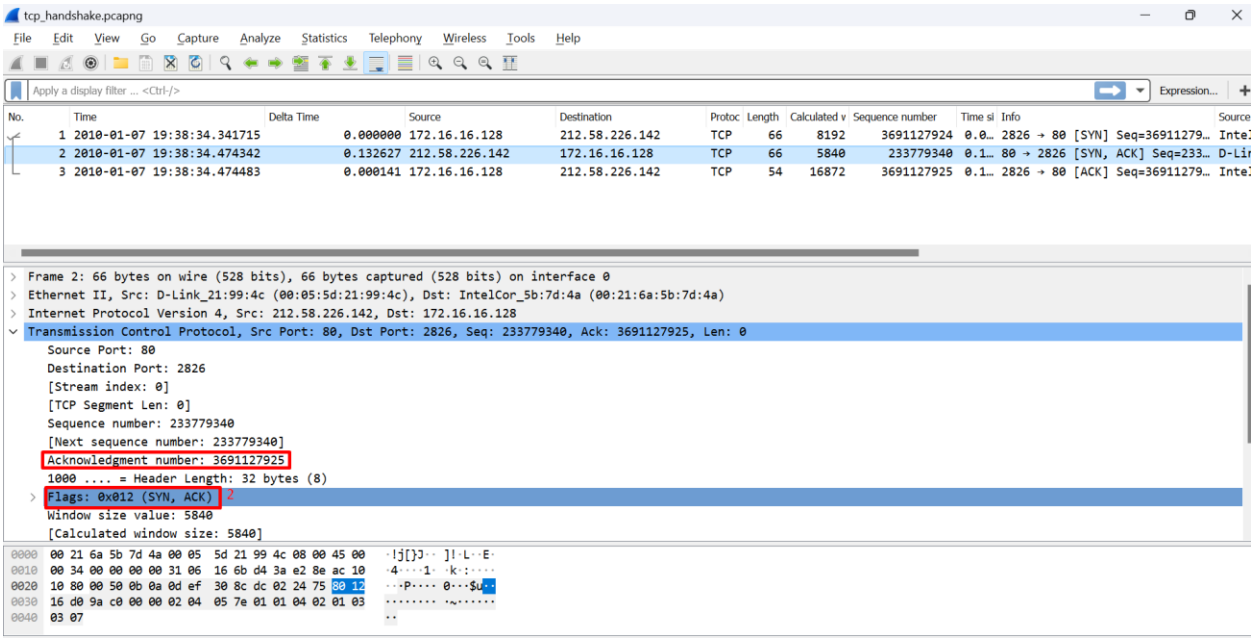
1. TCP flag sent from host A to Host B (3691127924)



2. Host B reply packet to Host A (SYN/ACK)

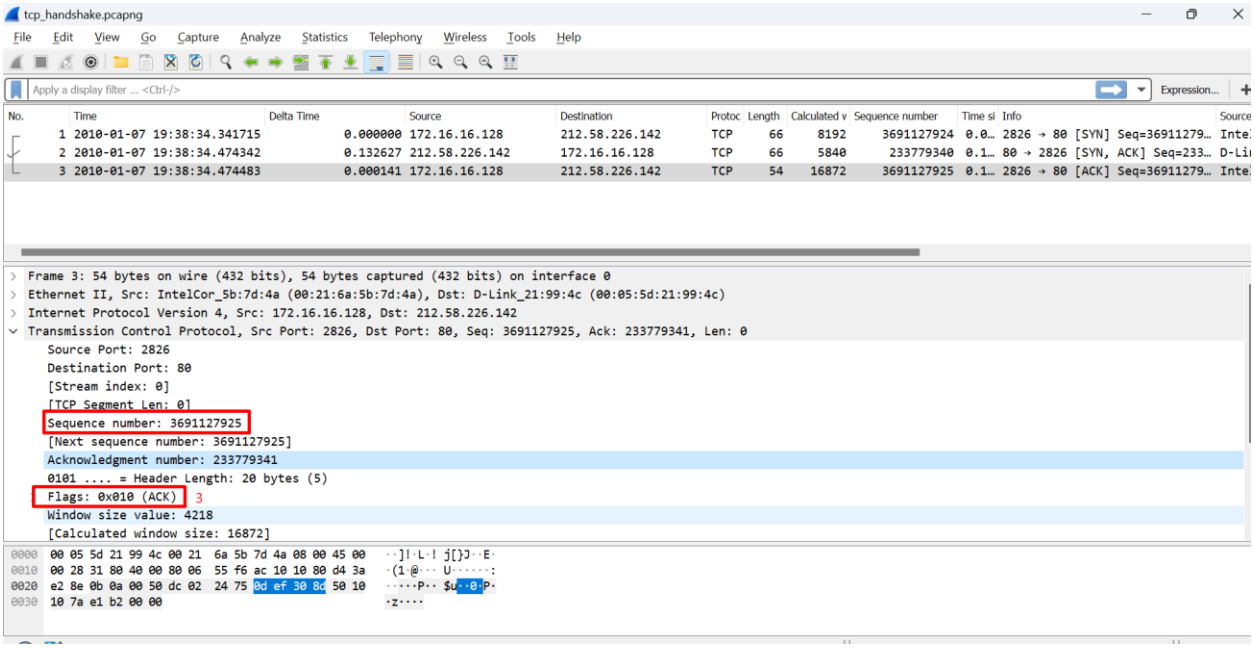
Initial Sequence is 233779340 and acknowledgment Sequence Number is 3691127925

Remark : why one more than the Acknowledgement sequence number included in the previous packet, because this field is used to specify the next sequence number the host expects to receive



3. Host A sent to Host B for final ACK packet

This packet, as expected, contains the sequence number 3691127925



Reference Book from PRACTICAL PACKET ANALYSIS by C H R I S S A N D E R S