Networking Lab Assignment 16

Wireshark : TCP

Albin Antony

3 April 2019

1 Wireshark : TCP

1.1 Aim

Using Wireshark observe Three Way Handshaking Connection Establishment, Data Transfer and Three Way Handshaking Connection Termination in client server communication using TCP.

1.2 Theory

1.2.1 Wireshark

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color coding, and other features that let you dig deep into network traffic and inspect individual packets.

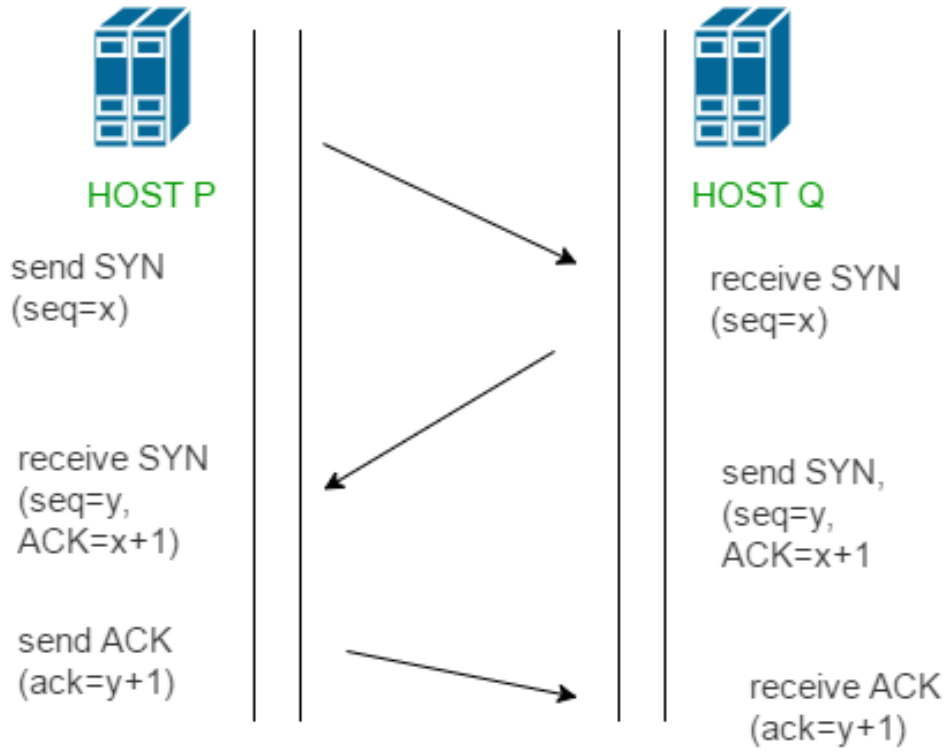
1.2.2 Capturing Packets

After downloading and installing Wireshark, you can launch it and double-click the name of a network interface under Capture to start capturing packets on that interface. For example, if you want to capture traffic on your wireless network, click your wireless interface.

1.2.3 Filtering Packets

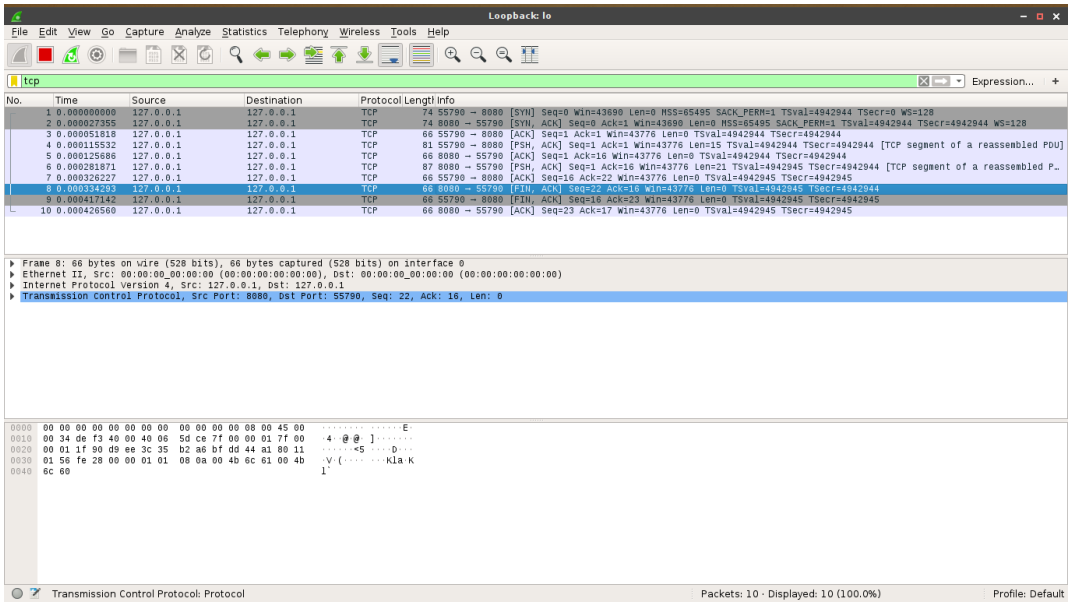
The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type “dns” and you’ll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.

1.2.4 Three Way Hand Shake



- (SYN) : In the first step, client wants to establish a connection with server, so it sends a segment with SYN(Synchronize Sequence Number) which informs server that client is likely to start communication and with what sequence number it starts segments.
- (SYN + ACK): Server responds to the client request with SYN-ACK signal bits set. Acknowledgement(ACK) signifies the response of segment it received and SYN signifies with what sequence number it is likely to start the segments
- (ACK) : In the final part client acknowledges the response of server and they both establish a reliable connection with which they will start eh actual data transfer

1.3 Output



1.4 Result

Installed wireshark and captured TCP packets on localhost.The packets were filtered as tcp. Three Way Handshaking Connection Establishment, Data Transfer and Three Way Handshaking Connection Termination was observed and deduced.