College of Engineering,Trivandrum

Experiment 14

Network Programming Lab

Author:
Alan Anto

Registration Number :
TVE16CS09

April 20, 2019

Contents

1 Three way hand shake connection termination

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 is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.

Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows. There is also a terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are free software, released under the terms of the GNU General Public License.Wireshark is very similar to tcpdump, but has a graphical front-end, plus some integrated sorting and filtering options.

1.2.2 Getting Wireshark

You can download Wireshark for Windows or macOS from its official website. If you're using Linux or another UNIX-like system, you'll probably find Wireshark in its package repositories. For example, if you're using Ubuntu, you'll find Wireshark in the Ubuntu Software Center.

1.2.3 TCP Protocol

Transmission Control Protocol(TCP) is a standard that defines how to establish and main- tain a network conversation via which application programs can exchange data.

The Transmission Control Protocol (TCP) is one of the main protocols of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP. TCP provides reliable, ordered, and error-checked delivery of a stream of octets (bytes) between applications running on hosts communicating via an IP network. Major internet applications such as the World Wide Web, email, remote administration, and file transfer rely on TCP.

When loading a web page, the computer sends TCP packets to the web server's address, asking it to send the web page to you. The web server responds by sending a stream of TCP packets, which the web browser stitches together to form the web page and display it to you.TCP is enables two way communication — the remote system sends packets back to acknowledge it is received your packets.

TCP guarantees the recipient will receive the packets in order by numbering them. The recipient sends messages back to the sender saying it received the messages. If the sender does not get a correct response, it will resend the packets to ensure the recipient received them. Packets are also checked for errors.Packets sent with TCP are tracked so no data is lost or corrupted in transit.

1.2.4 Threeway handshake

A three-way handshake is a method used in a TCP/IP network to create a connection between a local host/client and server. It is a three-step method that requires both the client and server to exchange SYN and ACK (acknowledgment) packets before actual data communication begins.

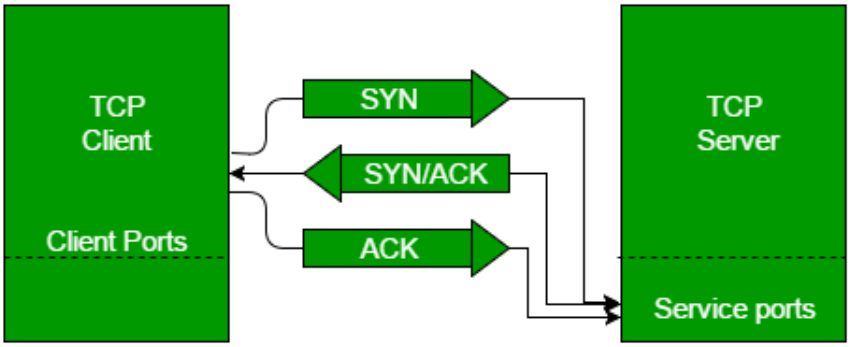
A three-way handshake is also known as a TCP handshake.A three-way handshake is primarily used to create a TCP socket connection. It works when:

1. A client node sends a SYN data packet over an IP network to a server on the same or an external network. The objective of this packet is to ask/infer if the server is open for new connections.

2. The target server must have open ports that can accept and initiate new connections. When the server receives the SYN packet from the client node, it responds and returns a confirmation receipt – the ACK packet or SYN/ACK packet.

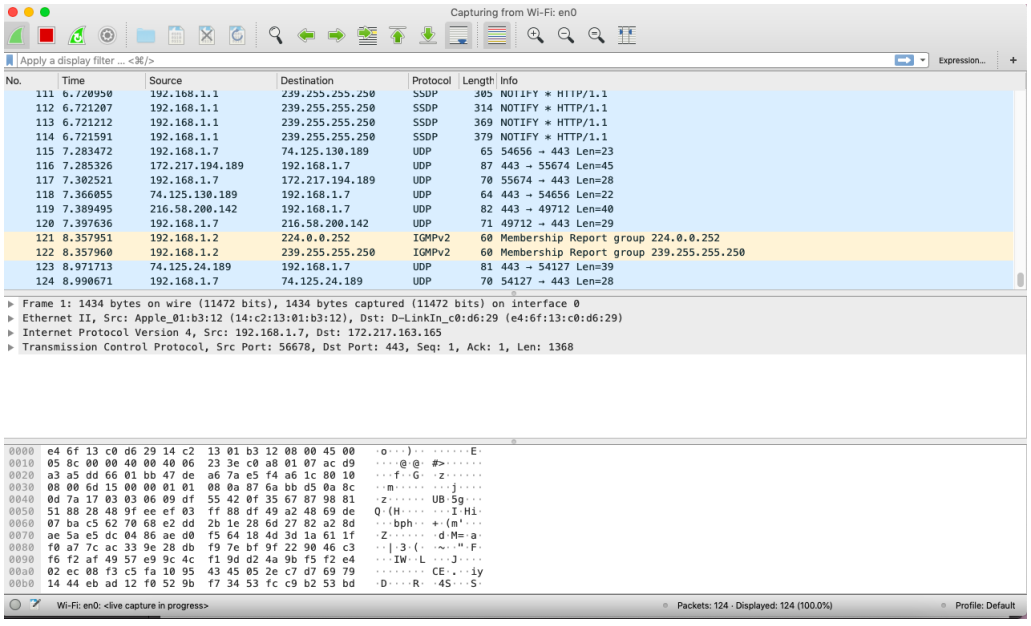
3. The client node receives the SYN/ACK from the server and responds with an ACK packet.

Upon completion of this process, the connection is created and the host and server can communicate.



1.2.5 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.

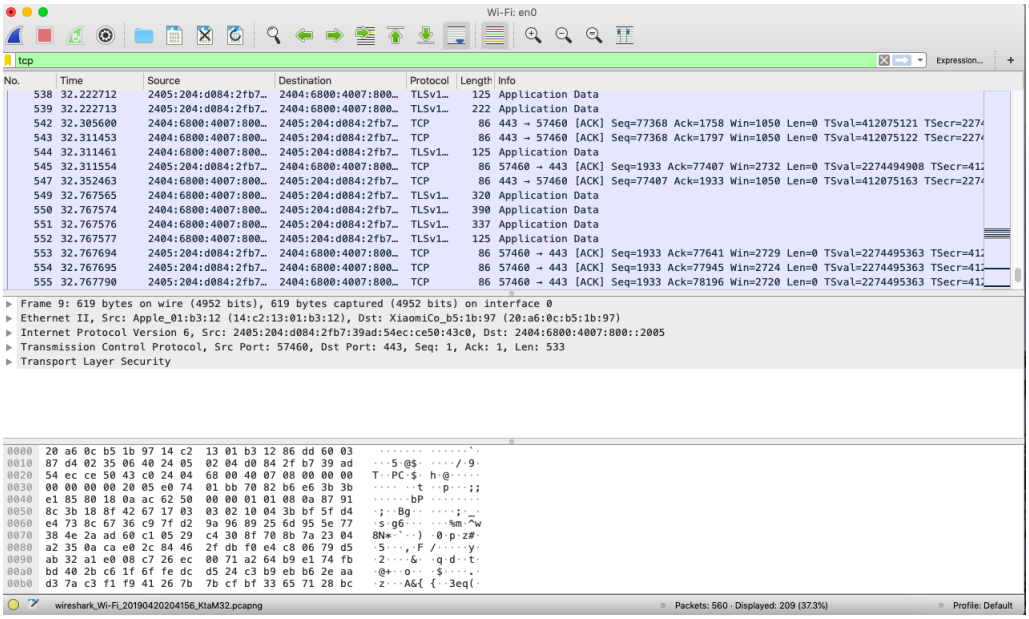


1.2.6 Filtering Packets

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.

2 Output



3 Result

Wireshark was installed and three way handshaking protocol was observed.