EXPERIMENT - XVI
WIRESHARK : THREE WAY HANDSHAKING OF TCP

April 13, 2020

ADITHYA D RAJAGOPAL
ROLL NO : 9
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
COLLEGE OF ENGINEERING TRIVANDRUM

AIM

Using Wireshark observe three way handshaking connection establishment, data transfer and three way handshaking connection termination in client server communication using TCP.

THEORY

Wireshark

Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible. Here, we make use of the packet capturing ability of Wireshark to capture the 3 way handshaking signal packets in a TCP transmission.

What is three way handshaking and how does it work?

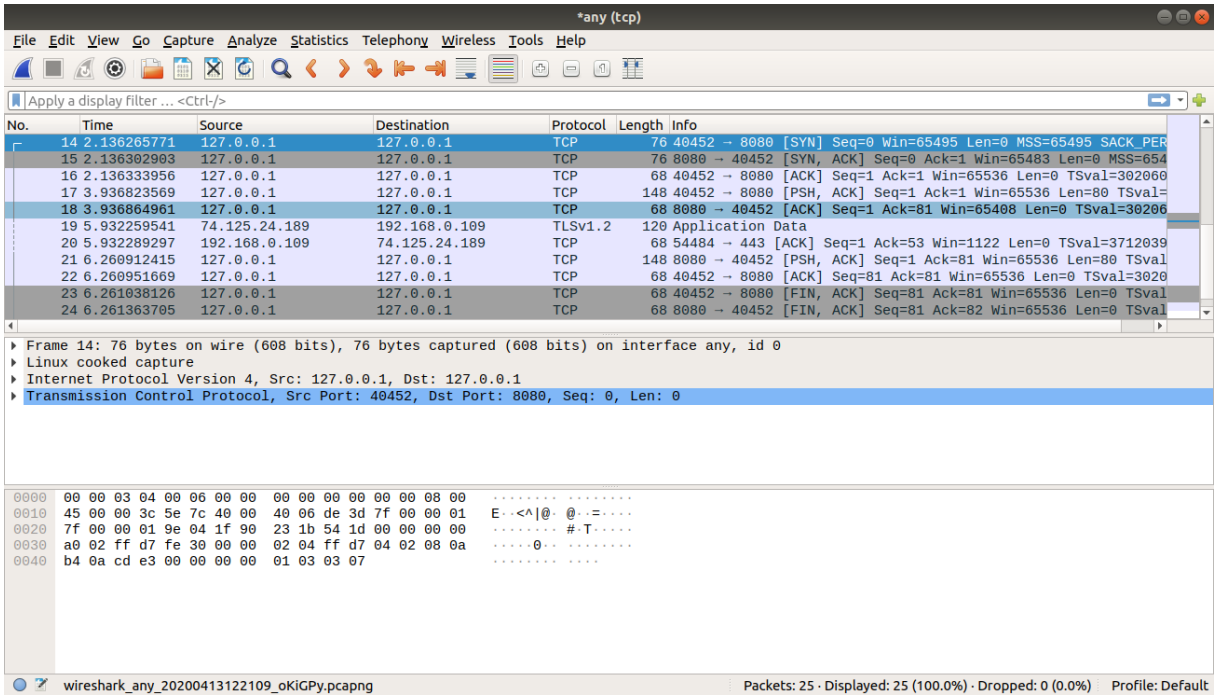
TCP provides reliable communication using the concept called Positive Acknowledgement with Re-transmission(PAR). A device using PAR resends the data unit until it receives an acknowledgement. If the data unit received at the receiver's end is damaged, then the receiver discards the segment. So the sender has to resend the data unit for which positive acknowledgement is not received. From this, we can understand that three segments are exchanged between sender(client) and receiver(server) for a reliable TCP connection to get established. These three steps can be explained as follows:

- Step 1(SYN): Here, the client wants to establish a connection with server, so it sends a segment with SYN(Synchronize Sequence Number) which informs the server that the client is likely to start communication and with what sequence number it starts the segments with.
- Step 2(SYN + ACK): In response, the server replies with a SYN-ACK. The acknowledgment number is set to one more than the received sequence number, and the sequence number that the server chooses for the packet is another random number.
- Step 3(ACK): Finally, the client sends an ACK back to the server. The sequence number is set to the received acknowledgement value, and the acknowledgement number is set to one more than the received sequence number.

PROCEDURE

1. Run a basic TCP oriented client-server program.
2. Since TCP is a connection oriented protocol and follows three way handshaking, we can see the three packets SYN, SYN-ACK and ACK which establishes the connection.
3. After connection, corresponding to the message sent, an acknowledgement signal will also be sent back as seen in the output.
4. Upon termination, a FIN signal will be sent back and forth.
5. Upon applying the TCP filter, we can specifically capture the packets which are a part of the ongoing transmission.

OUTPUT


*any (tcp)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
14 2.136265771 127.0.0.1 127.0.0.1 TCP 76 40452 → 8080 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PER
15 2.136302903 127.0.0.1 127.0.0.1 TCP 76 8080 → 40452 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=654
16 2.136333956 127.0.0.1 127.0.0.1 TCP 68 40452 → 8080 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=302060
17 3.936823569 127.0.0.1 127.0.0.1 TCP 148 40452 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=80 TSval=
18 3.936864961 127.0.0.1 127.0.0.1 TCP 68 8080 → 40452 [ACK] Seq=1 Ack=81 Win=65408 Len=0 TSval=30206
19 5.932259541 74.125.24.189 192.168.0.109 TLSv1.2 120 Application Data
20 5.932289297 192.168.0.109 74.125.24.189 TCP 68 54484 → 443 [ACK] Seq=1 Ack=53 Win=1122 Len=0 TSval=3712039
21 6.260912415 127.0.0.1 127.0.0.1 TCP 148 8080 → 40452 [PSH, ACK] Seq=1 Ack=81 Win=65536 Len=80 TSval
22 6.260951669 127.0.0.1 127.0.0.1 TCP 68 40452 → 8080 [ACK] Seq=81 Ack=81 Win=65536 Len=0 TSval=3020
23 6.261038126 127.0.0.1 127.0.0.1 TCP 68 40452 → 8080 [FIN, ACK] Seq=81 Ack=81 Win=65536 Len=0 TSval
24 6.261363705 127.0.0.1 127.0.0.1 TCP 68 8080 → 40452 [FIN, ACK] Seq=81 Ack=82 Win=65536 Len=0 TSval
Frame 14: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 40452, Dst Port: 8080, Seq: 0, Len: 0
0000 00 00 03 04 00 06 00 00 00 00 00 00 08 00
0010 45 00 00 3c 5e 7c 40 00 40 06 de 3d 7f 00 00 01
0020 7f 00 00 01 9e 04 1f 90 23 1b 54 1d 00 00 00 00
0030 a0 02 ff d7 fe 30 00 00 02 04 ff d7 04 02 08 0a
0040 b4 0a cd e3 00 00 00 00 01 03 03 07
wireshark_any_20200413122109_oKiGPy.pcapng
Packets: 25 · Displayed: 25 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

RESULT

The three way handshaking connection establishment, data transfer and three way handshaking termination in client server communication using TCP have been observed using Wireshark and the above output was obtained.