Client/Server Chat Program Report

Wilson Sue & Charnie
December 7th, 2023

Overview **2**

Data Gathering **2**

Analysis **2**

Overview 2

Start of a Session (3-Way Handshake) & End of a session 2

The Differences between Two packets that have the Same Data 2

Analysis of Protocol Hierarchy and Flow Graph 2

Conclusion **2**

Overview

To gain a better understanding of TCP Flow and packet sending.

Data Gathering

A chat client/server program was written and then analyzed with Wireshark to better understand TCP flow.

Analysis

This report demonstrates how we've utilized Wireshark in the context of our server/client chat program to gain insight into TCP flow.

Start of a Session (3-Way Handshake) & End of a session

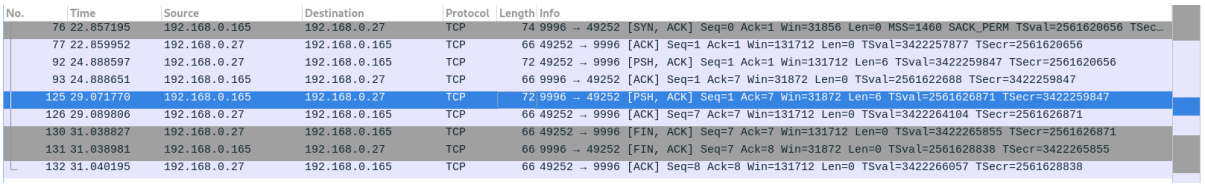
The 3-way handshake refers to the start of a session. First, the client wants to establish a connection and sends a packet with the SYN (synchronize) flag set, indicating the start of a TCP session. This packet also contains an initial sequence number (Seq) that the client will use to sequence the bytes in the packets it sends. In your capture, this is packet number 612, originating from the client's source port 43664 to the destination port 9997 on the server, with a sequence number of 0. Next, the sequence number goes up by 1 and the ACK goes up by 1 when the server acknowledges the clients connection. The next part, is when the ACK changes from 1 to 7 because "hello\n" (6 bytes so 6 + 1 = 7) is sent to the server. The next part where seq turns to 7 and Ack turns to 13 means that the client sent another package of 6 bytes and in response, the server acknowledges the previous bytes of 12 and is ready to receive the next one which is why it changed to 13. The next section, the PSH flag is triggered meaning that the hello\n is sent to server and the buffer is flushed. Once it's been pushed, seq is reset to 0. The next step, is where server sends hello\n to client and undergoes the same process where the syn and ack change to 7. Lastly, it's finished and the seq is reset to 0 again. Lastly, once the client closes the domain socket, the fin flag will be triggered and the socket will close.

So in this case, the connecting/client port is represented as 43664:
The destination port is 9997.

No.	Time	Source	Destination	Protocol	Length	Info
616	120.118262397	192.168.0.5	192.168.0.160	TCP	66	43664 → 9997 [ACK] Seq=1 Ack=1 Win=65728 Len=0 TSval=2190700112 TSecr=2258957144
635	122.720682360	192.168.0.5	192.168.0.160	TCP	66	43664 → 9997 [ACK] Seq=1 Ack=7 Win=65728 Len=0 TSval=2190702714 TSecr=2258959696
666	128.426153490	192.168.0.5	192.168.0.160	TCP	66	43664 → 9997 [ACK] Seq=7 Ack=13 Win=65728 Len=0 TSval=2190708419 TSecr=2258965401
653	126.055407531	192.168.0.5	192.168.0.160	TCP	72	43664 → 9997 [PSH, ACK] Seq=1 Ack=7 Win=65728 Len=6 TSval=2190705870 TSecr=2258959696
612	120.117322720	192.168.0.5	192.168.0.160	TCP	74	43664 → 9997 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM TSval=2190699911 TSecr=0
654	126.055480133	192.168.0.160	192.168.0.5	TCP	66	9997 → 43664 [ACK] Seq=7 Ack=7 Win=31872 Len=0 TSval=2258963082 TSecr=2190705870
634	122.670079907	192.168.0.160	192.168.0.5	TCP	72	9997 → 43664 [PSH, ACK] Seq=1 Ack=1 Win=31872 Len=6 TSval=2258959696 TSecr=2190700112
665	128.375189071	192.168.0.160	192.168.0.5	TCP	72	9997 → 43664 [PSH, ACK] Seq=7 Ack=7 Win=31872 Len=6 TSval=2258965401 TSecr=2190705870
615	120.117416412	192.168.0.160	192.168.0.5	TCP	74	9997 → 43664 [SYN, ACK] Seq=0 Ack=1 Win=31856 Len=0 MSS=1460 SACK_PERM TSval=2258957144 TSecr=2190699911 WS=128

The Differences between Two packets that have the Same Data

There are many differences between two packets that have the same data (in this case “hello\n”). The biggest factor is that the source and destination ports are different depending on which mode you are in. Also, the sequence, time sequence, and acknowledge number will be different depending on which was sent first. Lastly, the amount of data that can be sent is dynamic.



No.	Time	Source	Destination	Protocol	Length	Info
76	22.857195	192.168.0.165	192.168.0.27	TCP	74	9996 → 49252 [SYN, ACK] Seq=0 Ack=1 Win=31856 Len=0 MSS=1460 SACK_PERM TSval=2561620656 TSec…
77	22.859952	192.168.0.27	192.168.0.165	TCP	66	49252 → 9996 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=3422257877 TSecr=2561620656
92	24.888597	192.168.0.27	192.168.0.165	TCP	72	49252 → 9996 [PSH, ACK] Seq=1 Ack=1 Win=131712 Len=6 TSval=3422259847 TSecr=2561620656
93	24.888651	192.168.0.165	192.168.0.27	TCP	66	9996 → 49252 [ACK] Seq=1 Ack=7 Win=31872 Len=0 TSval=2561622688 TSecr=3422259847
125	29.071770	192.168.0.165	192.168.0.27	TCP	72	9996 → 49252 [PSH, ACK] Seq=1 Ack=7 Win=31872 Len=6 TSval=2561626871 TSecr=3422259847
126	29.089806	192.168.0.27	192.168.0.165	TCP	66	49252 → 9996 [ACK] Seq=7 Ack=7 Win=131712 Len=0 TSval=3422264104 TSecr=2561626871
130	31.038827	192.168.0.27	192.168.0.165	TCP	66	49252 → 9996 [FIN, ACK] Seq=7 Ack=7 Win=131712 Len=0 TSval=3422265855 TSecr=2561626871
131	31.038981	192.168.0.165	192.168.0.27	TCP	66	9996 → 49252 [FIN, ACK] Seq=7 Ack=8 Win=31872 Len=0 TSval=2561628838 TSecr=3422265855
132	31.040195	192.168.0.27	192.168.0.165	TCP	66	49252 → 9996 [ACK] Seq=8 Ack=8 Win=131712 Len=0 TSval=3422266057 TSecr=2561628838

Analysis of Protocol Hierarchy and Flow Graph

The Protocol Hierarchy provides the representation of the 5 TCP layers involved in the data transmission over a network. The 5 layers consisting of application, transport, internet, data-link, and physical layer.

Frame: This level represents the data link layer, encompassing all the traffic captured. It indicates that 100% of the traffic (all packets and bytes captured) are frames, which include Ethernet frames and all encapsulated data.

Ethernet: Corresponding to the Link Layer, this indicates that all captured packets are Ethernet frames. Ethernet is a family of networking technologies used in local area networks (LAN). The 'Percent Packets' and 'Percent Bytes' columns both show 100%, confirming that all traffic captured is Ethernet-based.

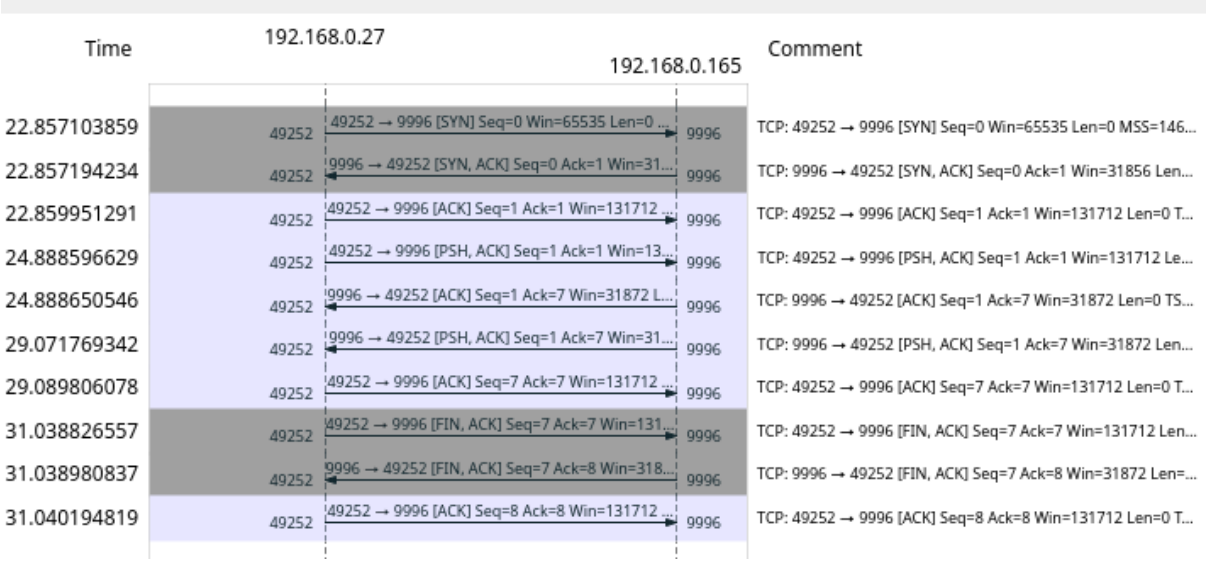
Internet Protocol Version 4 (IPv4): The hierarchy moves up to the network layer with IPv4. Again, it shows 100% for both percent packets and bytes, meaning all Ethernet frames encapsulate an IPv4 packet. The 'Percent Bytes' column, however, shows 28.9%, which likely indicates the proportion of bytes used by the IPv4 headers compared to the entire Ethernet frame.

Transmission Control Protocol (TCP): Within the IPv4 packets, TCP is used as the transport layer protocol for all packets, shown by 100% in the 'Percent Packets' column. The 'Percent Bytes' at 50.9% suggests that slightly over half of the bytes within the IPv4 packets are TCP headers and data.

Data: At the core of the TCP packets, 20% of the packets contain actual payload data, which is only 1.7% of the bytes. This suggests that the majority of the packets are likely to be carrying TCP control information, such as acknowledgments or handshakes, rather than payload data.

Protocol	Percent Packets	Packets	Percent Bytes
Frame	100.0	10	100.0
Ethernet	100.0	10	20.2
Internet Protocol Version 4	100.0	10	28.9
Transmission Control Protocol	100.0	10	50.9
Data	20.0	2	1.7

The Flow Graph in network analysis is a visual representation of the communication flow between hosts in a network. It provides a graphical overview of data packets exchanged between source and destination endpoints, allowing for quick identification of patterns and potential problems. The process of the flow is the same as the process previously described in the start and end of a session.



Conclusion

After a thorough examination of the TCP traffic flow through the usage of Wireshark on our client/server chat program. We had gained a better understanding of the complexities of TCP traffic flow. The three-way handshake was scrutinized to understand the establishment of a TCP connection. Packet captures revealed the precise sequence of Seq, SYN, and ACK packets, which form the foundation of a reliable TCP session. Another thing, PSH which is when the packets are sent successfully happens when the receiver is ready and accepted the ACK. Additionally, the FIN flag occurs once the socket has been closed and the SYN is reset to 0. The next topic which is Wire Shark's analysis section, covers two important diagrams which are the Protocol hierarchy and Flow Graph. The protocol Hierarchy displays the multi-layered approach of network protocols, with each layer — Frame, Ethernet, IPv4, and TCP — contributing to the successful encapsulation and transportation of data. Next, the Flow Graph is a graphical interface between captured packet flow which displays the necessary flags like seq,SYN, ACK, PSH, and FIN. Thus, displaying the process in which the packets were sent. In the end, the analysis revealed that even for small data transfers like "hello\n", the network communication is a complex interplay of various protocols, each with a specific role and function. Wireshark has proven how versatile ,and crucial it will be for future projects.