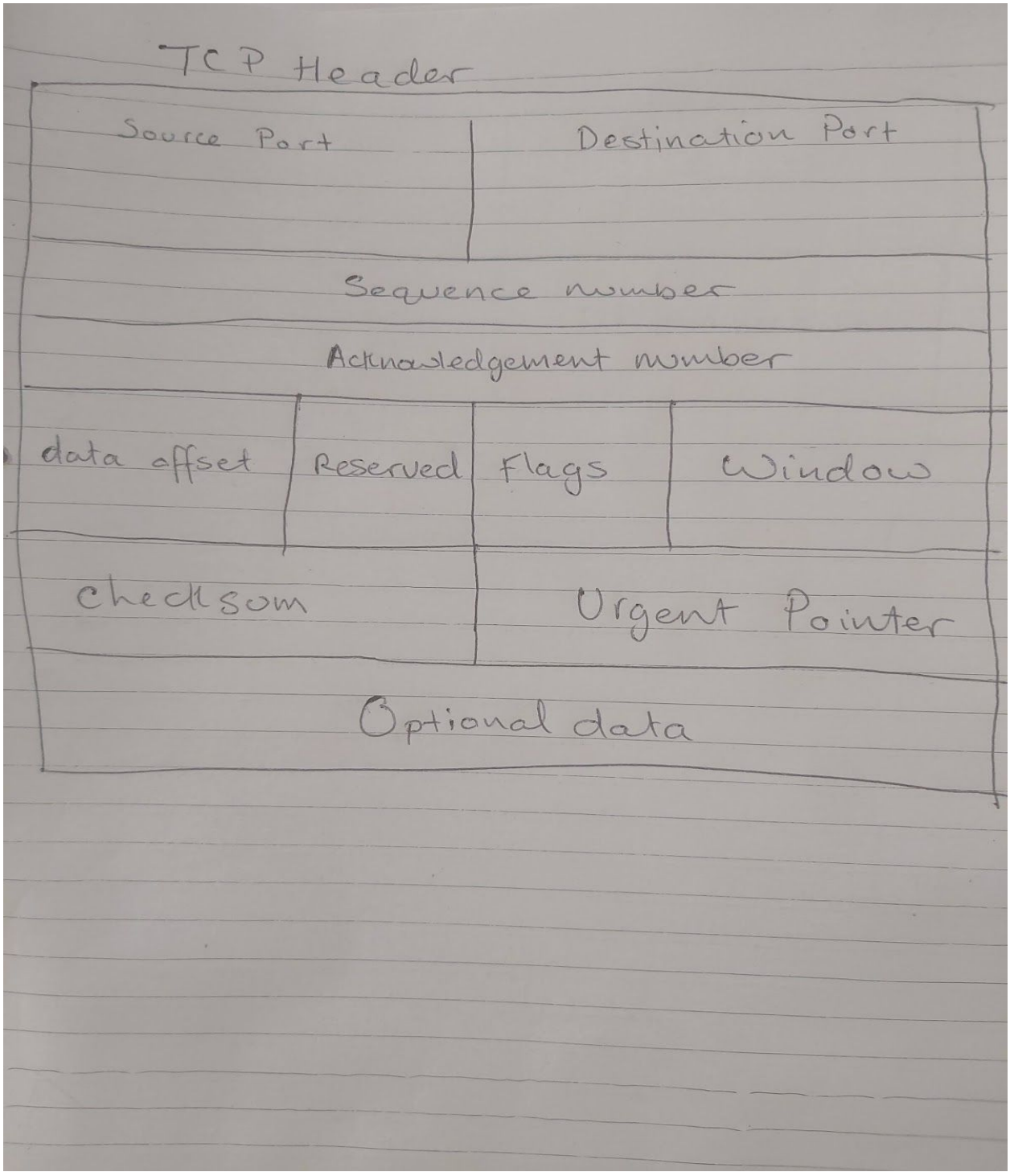
Lab 5

1.

Draw a TCP Header.

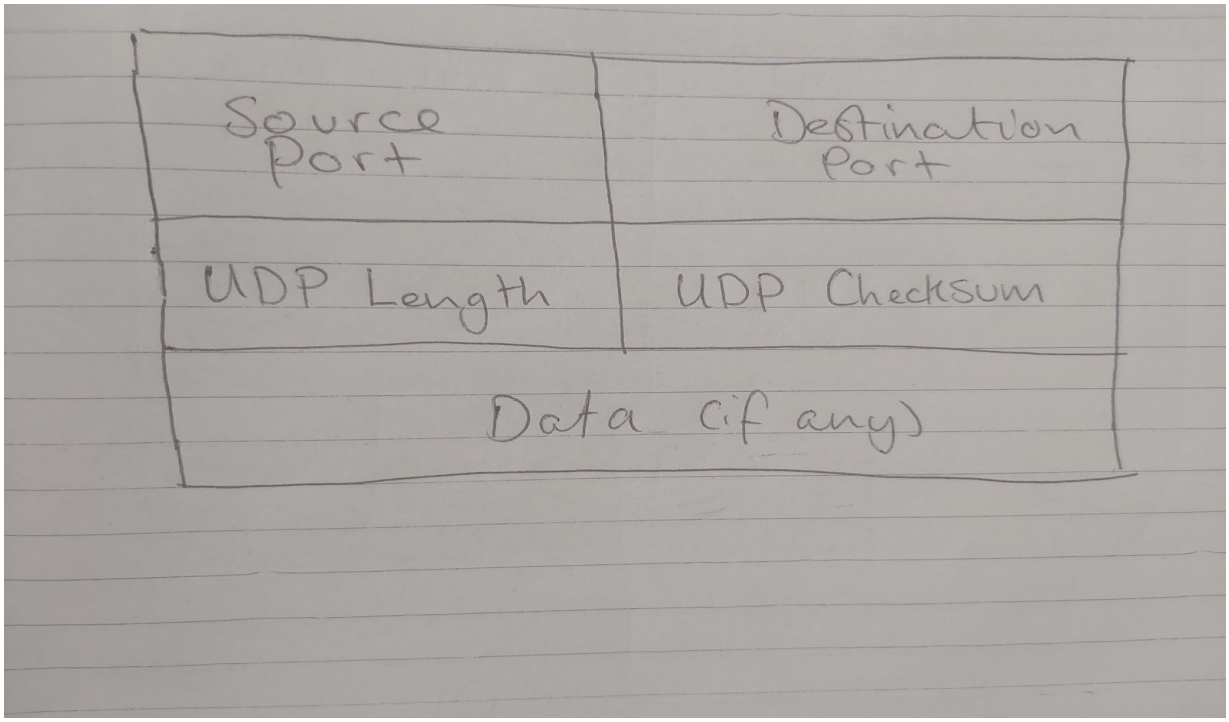


Capture packets in WireShark and explain the fields of a particular TCP packet captured

- **Source Port.** This is given as a number. It is where the data is being sent from.
- **Destination Port**. This is also a number and is where the data is being received.
- **Stream Index.** This is an index number. Wireshark gives one to every packet captured.
- **TCP Segment Len.** This is data, in bytes, to be sent as well as a header that is added to the data.
- **Sequence number.** This has "relative sequence number" in brackets after the number. The number is the byte number of the first byte sent.
- **Sequence number (raw):** This comes up as a ten digit number for me. It is bytes being sent.
- **Next Sequence number (relative sequence number):** This is the index number from the first sequence number + 1.
- **Acknowledgement number (relative ACK number):** This is the number of the next byte the receiver expects to receive
- **Acknowledgement number (raw):** This is the full bytes the receiver expects and a header length is given here.
- **Flags:** Flags establish a connection.
- **Window size value:** Each side of a TCP connection has a window size. A connection is allowed to have that number of bytes sent but unacknowledged.
- **Checksum:** This is used for error checking.
- **Urgent Pointer:** A segment of data can be flagged as urgent. The urgent pointer points to where that segment is.
- **[SEQ/ACK analysis]:** With sequence(SEQ) being bytes sent for the session and acknowledgement(ACK) the number sent by the TCP header, this section has two fields of its own:
    - **Bytes in flight:** This is bytes being transport
    - **Bytes sent since last PSH flag:** This is the number of bytes sent after the receiver was last warned that the sender has no further data to transmit for the time being.
- **Timestamps:** This is calculated in seconds. There are two sections here:
    - **Time since first frame in this TCP stream**
    - **Time since previous frame in this TCP stream**
- **TCP payload:** This is the data portion of the packet
- **TCP segment data:** The data being sent

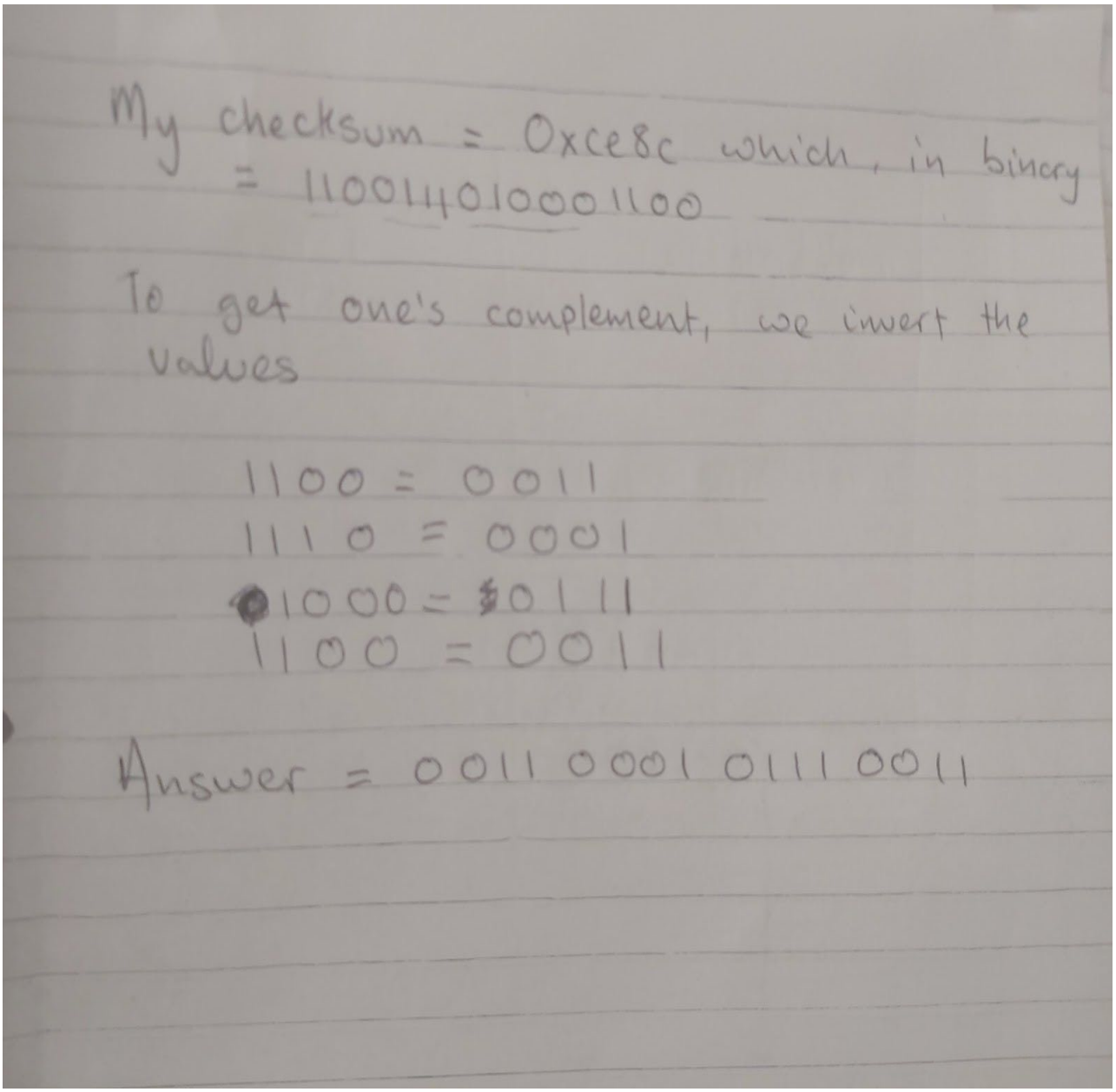
Question 2

Draw UDP Header



Capture packets using WireShark and explain the fields for a particular UDP packet captured
Under User Datagram Protocol, I can see the following headings:
- **Source Port:** This is where the data is being sent from
- **Destination Port:** This is where the data is being received.
- **Length:** This is the length of the datagram protocol.
- **Checksum:** This is for error checking
- **Checksum checking:** This is the result of the error checking
- **Stream Index:** How packets are mapped to IP addresses and ports. Two packets with the same value will be mapped to the same IP address and port.

3. Capture a UDP packet, verify the checksum using 16-bit One's Complement Sum algorithm.



4. Capture packets from a streaming service. Does it use UDP or TCP?
It uses both. UDP is used for quick communication in real-time. Video streaming services use UDP for this reason and some games do too.

5. What's TCP 3-Way Handshake? Draw a diagram to illustrate the process using real packets captured in a TCP session. Fill in the values of some key fields of the packets.

This is used to establish a reliable connection.

When capturing in WireShark, I see a [SYN] (client connects to server), a [SYN, ACK] on the next line (server responds to client request) and an [ACK] on the line after that (client acknowledges response to server and reliable connection has now been established).
Wireshark values:

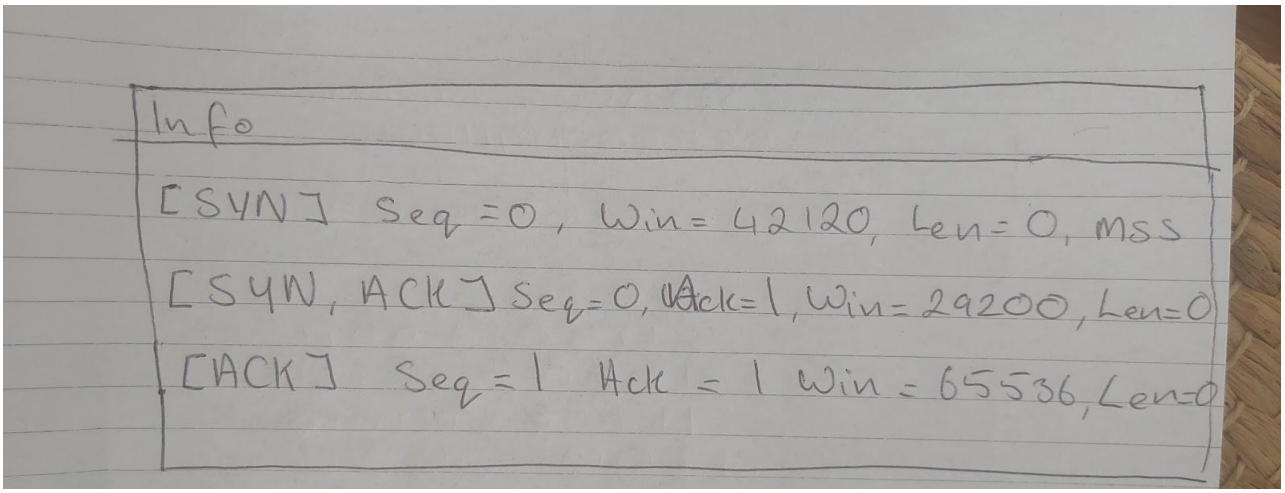
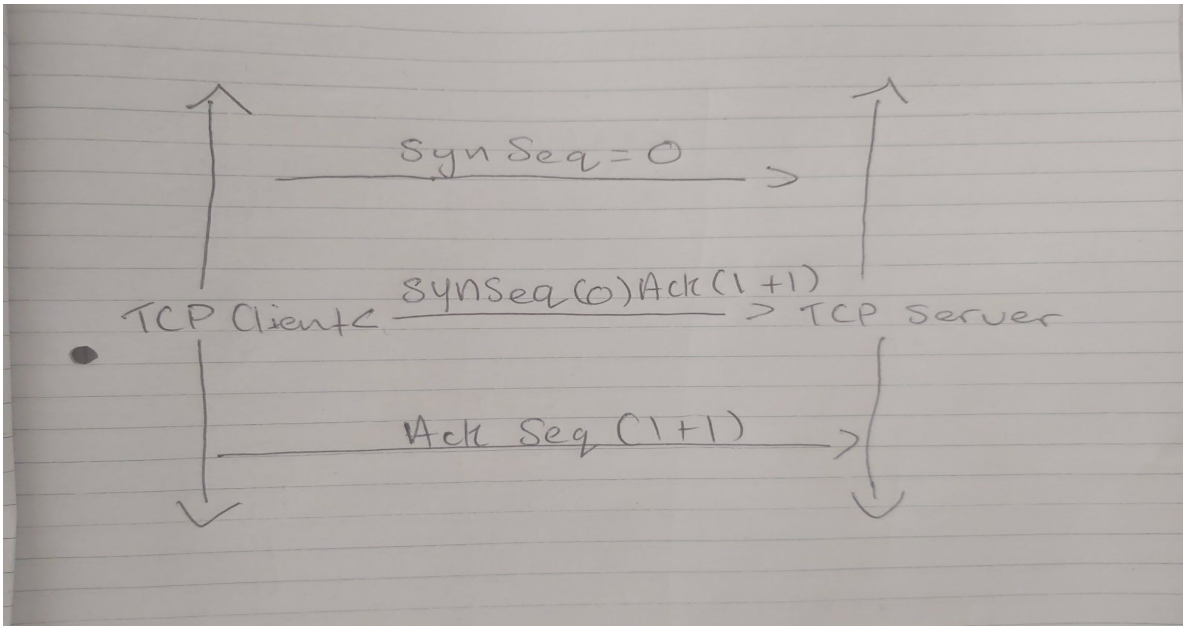
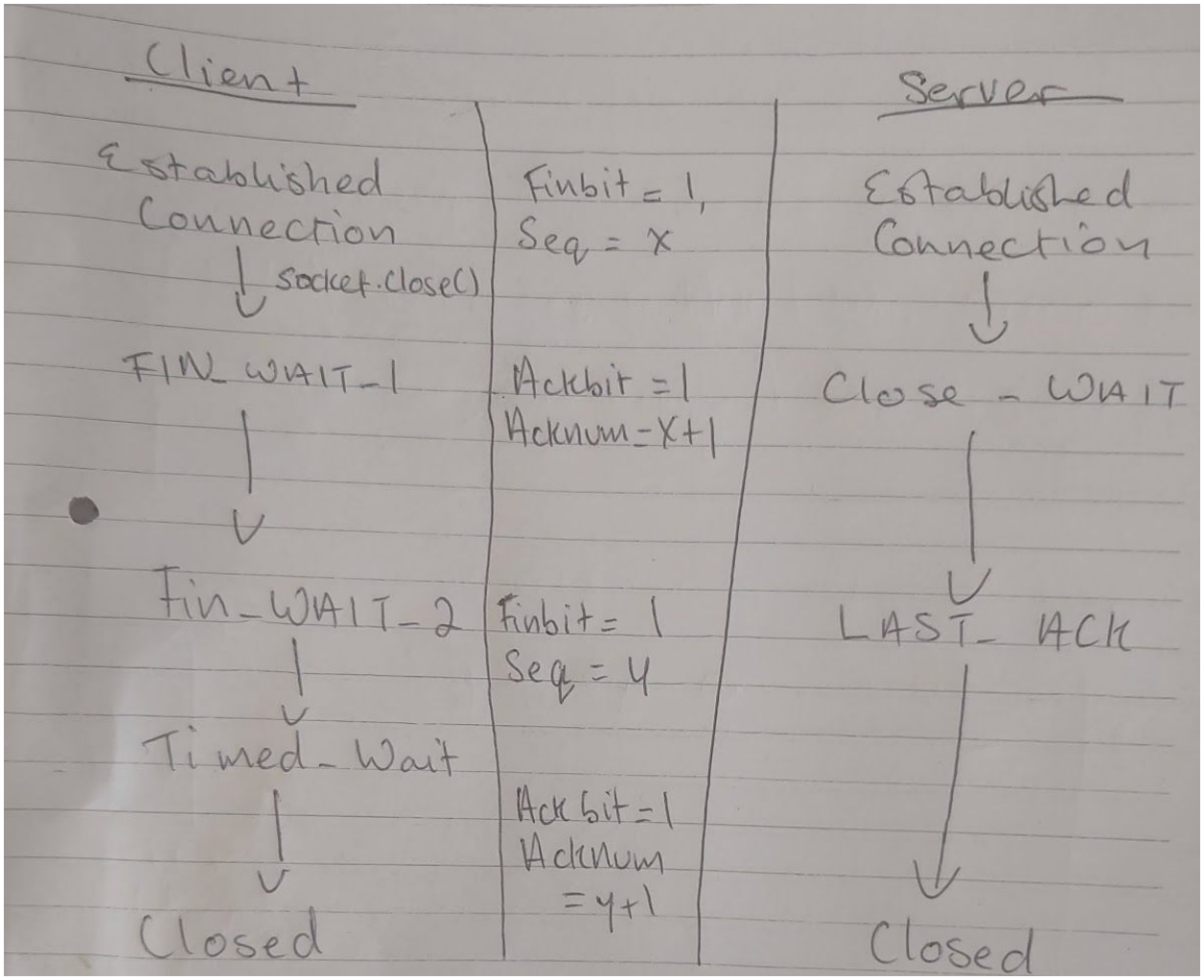


Diagram:



6. What's TCP 4-Way teardown? Draw a diagram to illustrate the process using real packets captured in a TCP session. Fill in the values of some key fields of the packets

This is how a connection is closed. The FIN flag is used here. Diagram below:



Bonus: Find two interview questions about TCP, and provide the answer. Please provide the reference.

Question One: What is a loopback address?
Answer: A loopback address is an IP address used for testing network cards.
Question source: Question 7 at https://www.imedita.com/blog/tcp-ip-interview-questions/

Question Two: What Is The Role Of TCP/IP In Data Transmission From Source To Destination?
Answer: TCP provides the end-to-end communications. This determines how data should be sent (broken up, for example). IP deals with where it should be sent (address, route etc).
Question source: Question 33 at https://www.imedita.com/blog/tcp-ip-interview-questions/