

**Homework 2: OSI Model Report**  
**CS231P**  
4/18/2025

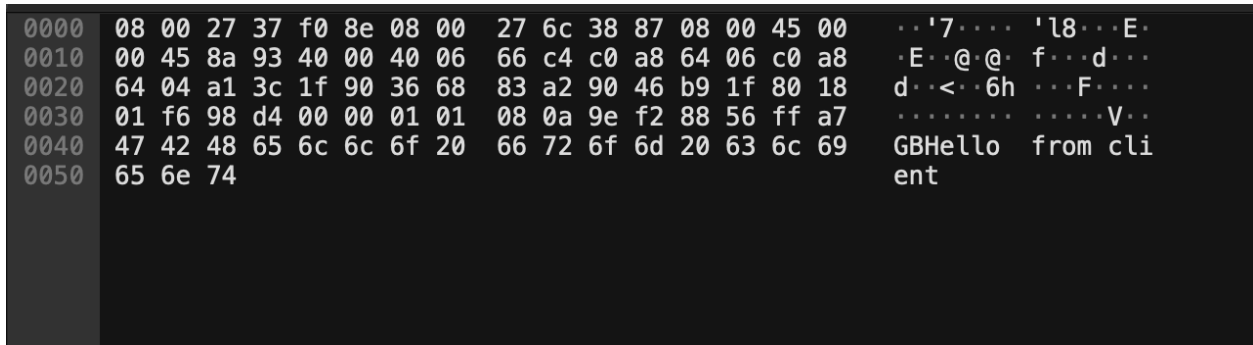
**TEAM:** Destin Wong 64848542, Midhuna Mohanraj 39922268, Eric Huang 59504944

**Q 1. The single packet that contains the message sent by Client:**

The third packet out of five in the stream contains the message sent by Client as it's the only one containing the "Hello from client" message.

1. The destination hardware address (MAC address) is encoded in bytes 0-5 as **Destination: PCSSystemtec\_37:f0:8e (08:00:27:37:f0:8e)**, the source hardware address is encoded in bytes 6-11 as **Source: PCSSystemtec\_6c:38:87 (08:00:27:6c:38:87)**. The purpose of the destination MAC address is to confirm the device to send the packet to, while the source MAC address identifies the device that sent the packet.
2. The header length is encoded in byte 14 as .... **0101 = Header Length: 20 bytes (5)**. Bytes 16 and 17 encoded as **Total Length: 69** have the total length of the packet. Byte 14 tells us how long the packet header is, bytes 16 and 17 tell how big the whole packet is, header and payload included.
3. Bytes 18-19 encoded as **Identification: 0x8a93 (35475)** have the unique identification of each packet to differentiate itself from the other packets. The other packets sent in the stream (ACK, FIN, etc) have similar IDs that are sequential.
4. The fragment offset is encoded in bytes 20-21 as ...**0 0000 0000 0000 = Fragment Offset: 0**, and indicates the index of the current packet fragment with respect to the first fragment, if it was fragmented. Since this packet isn't fragmented, it has to be 0.
5. Byte 23 encoded as **Protocol: TCP (6)** tells us what communication protocol the packet is adhering to. In our case the protocol is TCP.
6. The source IP address is encoded in bytes 26-29 as **Source Address: 192.168.100.6** and destination address is encoded in bytes 30-33 as **Destination Address: 192.168.100.4**. The source IP address identifies which IP the sender is from, while the destination address identifies the IP address of the intended receiver.
7. Bytes 34-35 as **Source Port: 41276**, which identifies the port the client uses to send the message, and bytes 36-37 is encoded as **Destination Port: 8080**, which identifies the port on the server that the client sends the message to.
8. After byte 65, **TCP segment data (17 bytes)** is encoded. In our case, the data is the message "Hello from client", and the values of the bytes converted to decimal show that exact message. The purpose of these bytes is to carry the message sent from the client to the server.

**Q. 2:** Obtain a clear screenshot of the raw block of bits of the previously mentioned single packet that contains the message sent by Client (raw blocks are located at the bottom part of Wireshark's window)



0000	08 00 27 37 f0 8e 08 00 27 6c 38 87 08 00 45 00	..'7.... 'l8...E.
0010	00 45 8a 93 40 00 40 06 66 c4 c0 a8 64 06 c0 a8	.E...@.@. f...d...
0020	64 04 a1 3c 1f 90 36 68 83 a2 90 46 b9 1f 80 18	d...<...6h ...F....
0030	01 f6 98 d4 00 00 01 01 08 0a 9e f2 88 56 ff a7	..... ....V..
0040	47 42 48 65 6c 6c 6f 20 66 72 6f 6d 20 63 6c 69	GBHello from cli
0050	65 6e 74	ent

**Split that block of bits, include it on the report, and associate each partition of bits to the layers 2 (Link), 3 (Network), 4 (Transport), and 7 (Application); by indicating the first and last byte of each layer, as an inclusive range “A-B”**

- Layer 2 (Link): 0-13
- Layer 3 (Network): 14-33
- Layer 4 (Transport): 34-53
- Layer 7 (Application layer): 54-65