Team Details: Jared Hynes (jlh484) and Mark Malysa (mbm206)
Collaboration: Collaborated with each other. Used this site (https://wiki.wireshark.org/CaptureSetup/NetworkInterfaces) to learn more about interfaces on Wireshark. Also used some other pages from the Wireshark Wiki to learn more about where everything was. We collaborated equally on the Python scripts and analyzed the network traffic together on one machine.

Part A. Protocol Basics

1. What transport-layer protocol is used in your capture? **TCP**

2. What port number did the server use? **30069**

3. What ephemeral port did the client use? (in part1, and part2) **Part 1: 47534 and Part 2: 54900**

4. What interface was used when you ran the C&S on the same machine(rlab5)? **Loopback**

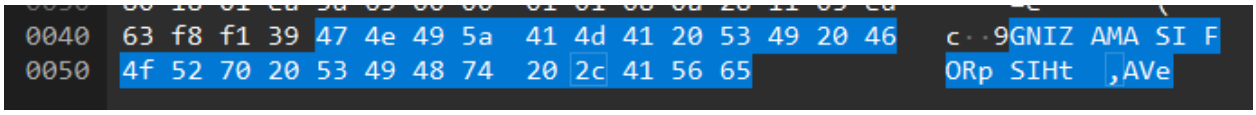
5. What interface was used when you ran the C&S on different machines (client on rlab5)? **Ethernet**

Part B. Application Layer

7. In part1, Which packet carries the “Welcome to CS 352!” message? How many bytes of payload are in that packet? **18**

8. In part2, Identify one packet carrying a client message. **Packet #6.** Show which field contains the application data. **The TCP field contains the data. It can be seen under “TCP payload”. It was 25 bytes in this case.**

9. In part2, Identify the corresponding echo reply from the server. Indicate the line #, or copy paste that line. **Packet #8 is the corresponding echo reply from the server.**



Part C. Packet Sizes

9. How many total bytes were sent from client → server, **735 bytes,** from server → client? (in both cases-part1 and part2) **685 bytes**

10. Which packet in the capture is largest in terms of payload size? **In both captures, packets number 13 and 14 were the largest in terms of payload size. (34 bytes)**