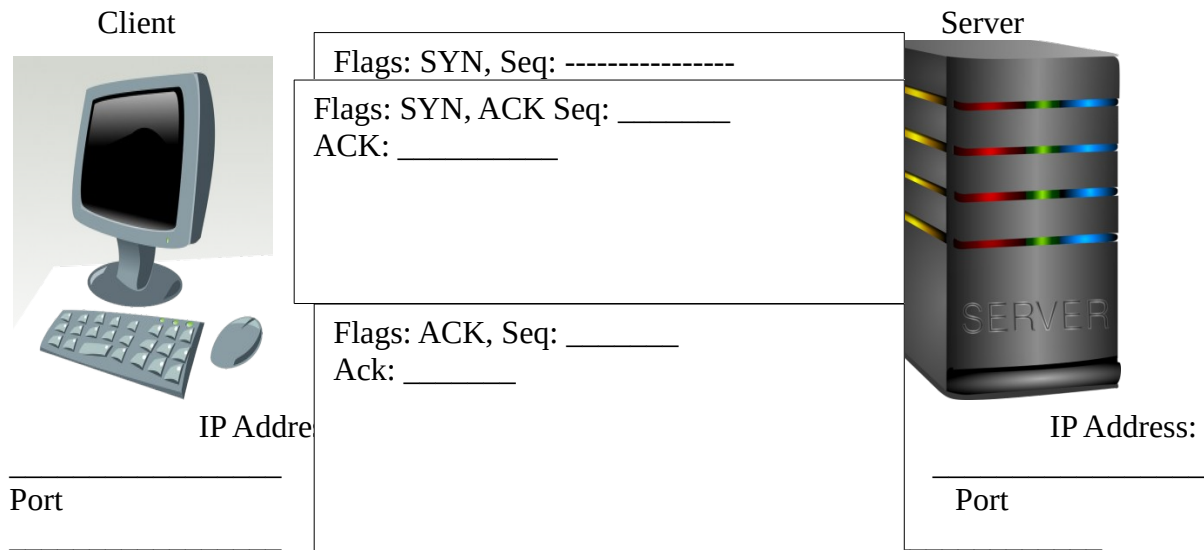


## Wireshark Exercise 2

1. Which Interface is connected to a local network (Ethernet)?
2. How many packets have passed through the interface?
3. Search back through your capture, and find an HTTP packet containing a GET command. Click on the packet in the Packet List Panel. Then expand the HTTP layer in the Packet Details Panel, from the packet.
  - a. From the Packet Details Panel, within the GET command, what is the value of the Host?
  - b. Can you see the Hex and ASCII representations of the packet in the Packet Bytes Panel?
  - c. From the Packet Bytes Panel, what are the first 4 bytes of the Hex value of the Host parameter?
4. Can you identify the rest of the TCP 3-way handshake easily?
5. From your Wireshark Capture, fill in the diagram below with the IP Addresses and Port Numbers for the Client and the Server
6. For each packet in the TCP 3-way handshake, fill in the Sequence and Acknowledgement numbers, on the diagram below.



7. After the first ping command, are the ARP and ICMP packets captured by Wireshark? YES/NO
8. After a second or third ping command, are the ARP and ICMP packets captured by Wireshark? ARP: YES/NO ICMP: YES/NO
9. Why is this?
10. Are the packets the same as the ping packets from the capture in the previous section?