Lab 1: (Wireshark) Names: _____
Examining an Application Packet

1. ***Open*** Wireshark, ***connect*** to "Wireless Network Connection" (or try others, and repeat 1. & 2. until you see packets)
2. ***Start capturing***. You should see packets streaming by as in the instructor's demonstration
3. In the filter box at the top of the screen, ***type*** `http && tcp` and press enter.
4. ***Browse*** to a webpage with your favorite browser. You should see some HTTP packets appear.
5. In the packet list, ***click*** on a packet with the HTTP protocol (not HTTP/XML or anything else)
6. In the GUI frame below (the middle GUI frame) the packet list, there is a list of protocols. This list starts with "Frame NNN: NNN bytes on wire …", which is not a protocol, but instead represents the whole packet. ***Click*** on each of the protocols in this middle frame. In the bottom GUI frame, which shows the raw packet, you will see the bytes corresponding to that layer's header highlighted.
7. ***Click*** the plus sign next to each protocol's name. You will see a variety of fields stored in that protocol's header. As you click on the fields, the location of that field in the raw stream will be highlighted in the bottom frame. ***Click*** on the field with a name most like "Destination" or "Host." Write the name and formatted value of the field shown in the protocols GUI frame, as well as the raw value of the field highlighted in the bottom GUI frame.

Stack Level	Protocol name	# of header bytes	Destination/Host field		
			Name	Formatted value	Hex value
Application					
Transport					
Network					
Link					
Physical	N/A	N/A	N/A	N/A	N/A

Digging Deeper

1. Which comes first in the packet, the header for the lowest level of the stack or the highest? Why?
2. Can you figure out how to translate from the raw to the formatted output like Wireshark does?
3. Why isn't there a physical layer header?