Task: Generate IP traffic and inspect IP Header.

Step 1: Contents of IP Header can be obtained online. Understand these contents and try to fill up these contents in an empty IP header sketch.

Step 2: To show your understanding of IP, sketch a figure of an IP packet you studied. It should show the position and size in bytes of the IP header fields as you can observe using Wireshark. Since you cannot easily determine sub-byte sizes, group any IP fields that are packed into the same bytes. Your figure can simply show the frame as a long, thin rectangle. Try not to look at the figure of an IPv4 packet in your text; check it afterwards to note and investigate any differences.

To work out sizes, observe that when you click on a protocol block in the middle panel (the block itself, not the "+" expander) Wireshark will highlight the corresponding bytes in the packet in the lower panel, and display the length at the bottom of the window. You may also use the overall packet size shown in the Length column or Frame detail block. Note that this method will not tell you sub-byte positions.

By looking at the IP packets in your trace, answer these questions:

1. What are the IP addresses of your computer and the remote server?

2. Does the Total Length field include the IP header plus IP payload, or just the IP payload?

3. How does the value of the Identification field change or stay the same for different packets? For instance, does it hold the same value for all packets in a TCP connection or does it differ for each packet? Is it the same in both directions? Can you see any pattern if the value does change?

4. What is the initial value of the TTL field for packets sent from your computer? Is it the maximum possible value, or some lower value?

5. How can you tell from looking at a packet that it has not been fragmented? Most often IP packets in normal operation are not fragmented. But the receiver must have a way to be sure. Hint: you may need to read your text to confirm a guess.

6. What is the length of the IP Header and how is this encoded in the header length field? Hint: notice that only 4 bits are used for this field, as the version takes up the other 4 bits of the byte. You may guess and check your text.

Step 3: IP Header Checksum

We will now look at the IP header checksum calculation by validating a packet. The checksum algorithm adds the header bytes 16 bits at a time. It is computed so that re-computing the sum across the entire IP header (including the checksum value) will produce the result of zero. A complicating factor for us is that this is done using 1s complement arithmetic, rather than 2s complement arithmetic that is normally used for computing. The steps below explain how to perform the necessary computation.

From the trace, pick a packet sent from the remote server to your computer and check that you have a non-zero value in the checksum field. The checksum value sent over the

network will be non-zero, so if you have a zero value it is because of the capture setup. Try a packet that has an IP header of 20 bytes, the minimum header size when there are no options, to make this exercise easier.

Follow these steps to check that the checksum value is correct:

1. Divide the header into 10 two byte (16 bit) words. Each word will be 4 hexadecimal digits shown in the packet data panel in the bottom of the Wireshark window, e.g., 05 8c
2. Add these 10 words using regular addition. You may add them with a hexadecimal calculator (Google to find one), or convert them to decimal, add them, and convert them back to hexadecimal. Do whatever is easiest.
3. To compute the 1s complement sum from your addition so far, take any leading digits (beyond the 4 digits of the word size) and add them back to the remainder. For example: 5a432 will become a432 + 5 = a437.

4. The end result should be 0xffff. This is actually zero in 1s complement form, or more precisely 0xffff is -0 (negative zero) while 0x0000 is +0 (positive zero).

If you cannot get your sum to come out and are sure that the checksum must be wrong, you can get Wireshark to check it. See whether it says “[correct]” already. If it does not then use the menus to go to Preferences, expand Protocols, choose IPv4 from the list, and check “validate header checksum”. Now Wireshark will check the checksum and tell you if it is correct.