1. What is the IP header length in bytes? (Wireshark translates the integer value in the Header length (HLen) field to the actual number of bytes for you.)

20

2. What is the integer value actually contained in the IP header’s Header length field? “Raw” packet data, as transmitted “on the wire” or stored in memory, is displayed in the Packet Bytes pane at the bottom. Select Header length: in the Packet Details pane, and the corresponding byte in the Packet Bytes pane that contains the 4-bit header length will be highlighted. If the Packet Bytes pane is not being displayed, use the View tab to enable it. Since the highlighted byte contains two 4-bit fields, you’ll need to separate the header length from the Version number. Use the IP Packet Header diagram (Figure 3.16) above as a reference, and think about this carefully. The field originally called Type of Service (TOS) in Figure 3.16 above has been redefined by the IETF as the Differentiated Services Field. Wireshark uses this newer term to identify that field.

5

3. What is the Total Length of the IP packet? Does this include the IP header? Does it include the Data-link layer (Ethernet or WiFi) frame header?

132

4. What is the Time To Live (TTL) value? What does this represent? Can you make an “educated guess” as to how many routers this packet has crossed on its way to your computer? (Answering this requires a bit of intuition and an assumption).

57, it’s the amount of time that packet store that caches for. This number decreases as it goes over 3rd layer devices and recommended amount is around 64 so I would guess that there is about 7-8 routers or nodes. When pinging with tracert, ICMP returns with 8 hops or nodes.

5. Which Internet Layer 3 Transport protocol header is carried within this IP packet?

TCP

6. Are there any options present at the end of the IP header (after the Destination Address)? If so, what are they?

none

7. Clear the HTTP filter by clicking at the right of the Display Filter field, so that you are once again displaying all of the captured packets. Try Statistics | Packet Lengths again (without a filter). What are the most common packet length ranges? Why do you think this is the case?

1280- 2559, had the most with 40% and I would guess this is the packets that contained images and other medias that have more memories that’s needed and has been separated into multiple packets.