CS 334: Computer Networks Wireshark Assignment No 1

Write answer to each question, following the question. Include the snapshots of your screen wherever you feel it is necessary to support your answer or else where it is explicitly specified. Submit the pdf version of the file by email latest by 23:59 hrs on 22nd Sep 2018.

Instructions:

1. Start Wireshark on any network interface of your machine
2. Start your browser with the following URL http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html
3. Answer the following questions:

Q1. What are the network interfaces available on your computer? Which network did you eventually select in your experiments.

Q2. Which application layer protocol is used in this case?

Q3. What are the other protocols used and displayed in the unfiltered packet listing window of wireshark, besides the one that you answered in Q2?

Q4. What is the IPA of your machine? What is the IPA of the destination machine? Is there any way by which you can ascertain that the IPA of the destination indeed is the same as that you observed in wireshark? If so, how ?

Q5. What is the class of the IPA of the source machine ? That of destination machine?

Select the first wireshark block i.e. "frame" in the **packet-header details** window. The packet- header-details window shows the details of the protocols associated with the selected packet. Note, however that the first Wireshark block – shown as "Frame" - is actually not a protocol, but it is a record that describes overall information about the packet, including when it was captured and how many bits long it is.

Answer the following questions from this:

Q6. How many bits were captured in this packet? At what time was this packet captured?

Q7. What is the interface id used? What is the address of the interface?

The second block is "Ethernet". Note that you may have taken a trace on a computer using 802.11 yet still see an Ethernet block instead of an 802.11 block. Why? It happens because we asked Wireshark to capture traffic in Ethernet format on the capture options, so it converted the real 802.11 header into a pseudo-Ethernet header.

After the block “Ethernet” are shown blocks for different protocol layers i.e. IP, TCP, and HTTP. Note that the order of the blocks shown is from the bottom of the protocol stack upwards. This is because as packets are passed down the stack, the header information of the lower layer protocol is added to the front of the information from the higher layer protocol, as in Fig. 1-15 in the text book. That is, the lower layer protocols come first in the packet “on the wire”.

For all the subsequent questions, you may have to expand appropriate block i.e. IP, TCP or HTTP and get the required information.

Q8. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

Q10. Print the two HTTP messages (GET and OK) referred to in question above. To do so, select Print from the Wireshark File command menu, and select the “Selected Packet Only” and “Print as displayed” radial buttons, and then click OK.

Q11. What is the destination physical address of the first packet captured? What device does it belong to? Show where in the capture would you find this information.

Q12. How many bytes of header does the first frame sent have? Show where in the capture would you find this information.

Q13. By looking at the Ethernet header of a frame, can we determine if it contains an IP packet? Show where in the capture would you find this information.

Q14. Is it possible to know if the first packet captured has TCP or UDP as transport protocol by looking at the IP header? Explain and show where in the capture would you find this information.

Q15. In the SYN, ACK. What are the source and destination ports? Are these the same for the client and the server? Explain why.

Q16. Why does the Server Hello message sent by the server have 1 as a relative sequence number and 185 as a relative acknowledgement number.

For the following question: Right-click a TCP capture → TCP preferences → Uncheck the box “Show relative sequence number”

Q17. What is the first sequence number sent by the server to the client. Why is it not the 0 displayed by wireshark?

*****

***

*