HW3

1. How do you find the HTTP Packet Counter statistics using Wireshark? Please take a screenshot and justify your answer.

2. Write down two benefit to use QUIC protocol instead of traditional TCP protocol.

3. What should the display filter be when we want to capture non-IP traffic. Please take a screenshot and justify your answer.

4. What is the Time to Live (TTL) of a packet? please find the field in a packet using Wireshark and take a screenshot.

5. HTTP/3 uses QUIC protocol to transmit data. What protocol does QUIC use in transport layer? (Hint: use display filter: quic) Please use Wireshark to find the answer and take a screenshot.

6. How long did it take from when the HTTP (Hypertext Transfer Protocol) GET message was sent until the HTTP OK reply was received? (Hint: You can visit http://neverssl.com/ for non-encrypted HTTP connection)

Please take a screenshot and justify your answer.

7. How can a computer know that if a packet is an IPv4 or IPv6 packet? Please find the field in a packet using Wireshark and take a screenshot.

8. Please find out the Time to live field from a DNS packet. Please take a screenshot and justify your answer.

9. Now that we've seen how Wireshark displays the captured packet traffic for large HTML files, we can look at what happens when your browser downloads a file with embedded objects, i.e., a file that includes other objects (in the example below, image files) that are stored on another server(s).

   Do the following:

- Start up your web browser, and make sure your browser's cache is cleared, as discussed above. (To do this under Firefox, select Tools->Clear Recent History and check the Cache box, or for Internet Explorer, select Tools->Internet Options->Delete File; these actions will remove cached files from your browser's cache)
- Start up the Wireshark packet sniffer

- Enter the following URL into your browser
  http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html
  Your browser should display a short HTML file with two images. These two images are referenced in the base HTML file. That is, the images themselves are not contained in the HTML; instead the URLs for the images are contained in the downloaded HTML file. As discussed in the textbook, your browser will have to retrieve these logos from the indicated web sites. Our publisher's logo is retrieved from the gaia.cs.umass.edu web site. The image of the cover for our 5th edition (one of our favorite covers) is stored at the caite.cs.umass.edu server.
  (These are two different web servers inside cs.umass.edu).
- Stop Wireshark packet capture, and enter "http" in the display-filter-specification
  window, so that only captured HTTP messages will be displayed.

  Answer the following questions:

a) How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
b) Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.