Wireshark Final Exam

IT 520-A – Enterprise Infrastructure & Networks
Due Date: May 1st, 2018 (Handed in at the beginning of class)

Instructions:

- This exam is due on May 1st, 2018 at 6:30 pm (beginning of class). I will NOT accept any submission after the specified date and time. If you have an excuse, let me know on time. (However, if it is an emergency, we can work it out. I might request for a proof.)

- For every response, you should take a screenshot and type the answer. I will NOT grade any question that does not have a screenshot, and a written response. Don't expect me to look for the answers from the screenshot. TYPE it. Partial answers will not be graded.

- Before you begin, take a screenshot and type your computer's IP address. If your IP changed at any point. Then you must retake the screenshot and TYPE the IP address again. (Example, if today you answered question 1, 2, and 3 using IP 10.10.10.1, and tomorrow your IP changed to 10.30.20.19. You can continue; but, you MUST take another screenshot for the new IP. If you fail to do this, I will not grade any subsequent questions.)

- If you can't afford printing, let me know on time. We can work something out. However, if you choose not to print till the last minute, and encounter errors on the day of submission. Then I can't help you.

- If a question is not clear, make note of it, and we will discuss it in the next class.

- Email me if you have any concerns.

Visit: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html

1. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?
2. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
3. What is the status code and phrase in the response?
4. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

Visit: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html

The username is "wireshark-students" (without the quotes), and the password is "network" (again, without the quotes).

5. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?
6. When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Visit: http://www.ietf.org (Hint: Filter Wireshark using "ip addr == your IP")

7. Locate the DNS query and response messages. Are they sent over UDP or TCP?
8. What is the destination port for the DNS query message?
9. What is the source port of DNS response message?
10. To what IP address is the DNS query message sent?
11. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
12. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?
13. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Do something that will cause your host to send and receive UDP packets. (example: use SNMP protocol by sending an email).

14. Select *one* UDP packet from your trace. From this packet, determine how many fields there are in the UDP header
15. By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.
16. The value in the Length field is the length of what? Verify your claim with your captured UDP packet.

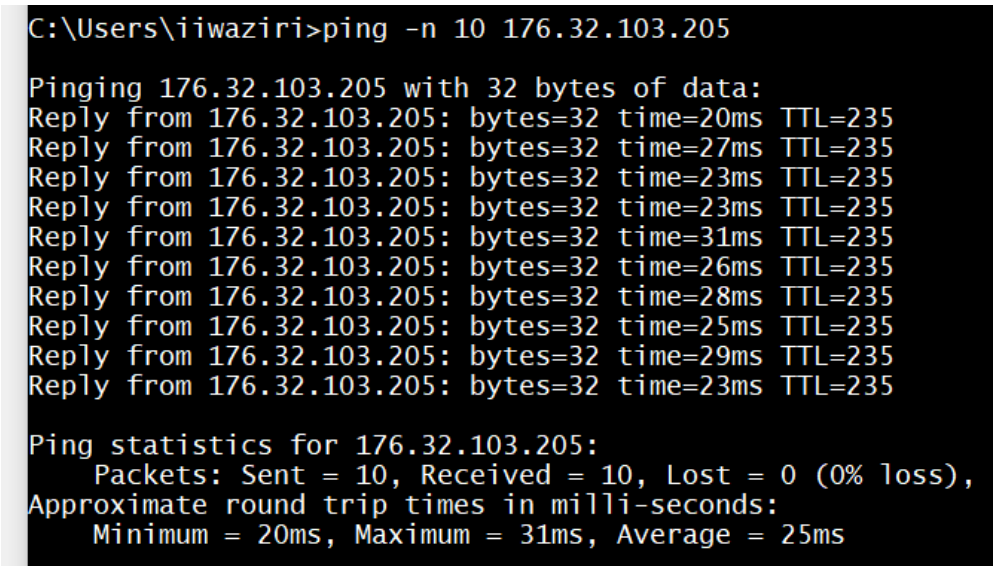

Figure 1

Use Figure 1 above to answer question 17 - 25

17. Explain what happened in Figure 1. (pay close attention to the command.)
18. Which protocol is used to carry out the instruction in Figure 1.
19. Who owns the IP?
20. In addition to a screenshot, in a tabular form, list all the hops between your computer's IP and the IP address in Figure 1. The table should include the owner, and location of the IP address.
21. What version of TLS does the IP above use? Hint: Visit the website of the owners IP address, and capture the "Client Hello" packet.
22. List all the algorithms listed in the Cipher Suite of the "Client Hello" packet in 21.
23. What TCP port number is used by the "Client Hello" packet, and why is it using that port number?
24. What are the source and destination MAC address?
25. Identify the company that manufactured the network cards with the MAC address identified in 8 above. (Hint: there are a lot of websites you can use to lookup MAC address, just like you would for an IP).

Extra Credit: (3 Marks)

Make a GitHub account and create a repository. Name the repo "wireshark_labs". Add all the labs you did in this class (both Wireshark saved files and submitted reports). Add your GitHub username to the end of this lab or email it to me.