HW2

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window. Please take a screenshot and explain your answer briefly.

2. What is an ARP protocol? How do you find out ARP packets by using Wireshark? (Hint: typing “arp” in display filter) Please take a screenshot and explain your answer briefly.

3. What is an ICMP protocol? How do you find out ICMP packets by using Wireshark? (Hint: you can create ICMP packets manually by typing “ping 8.8.8.8” in command line) Please take a screenshot and explain your answer briefly.

4. What is an DNS protocol? How do you find out DNS packets by using Wireshark? Please take a screenshot and explain your answer briefly.

5. While Wireshark is running, enter the URL: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html and show the HTTP packets information . (Hint: typing “http” in display filter)Please take a screenshot and explain your answer briefly.

6. Reffered to question 5, how long did it take when the HTTP GET message was sent until the HTTP OK reply was received?Please take a screenshot and explain your answer briefly.

7. Assume that you are encountering a DDoS attack, how do you get the number of packets incoming to your computer per minute? Please take a screenshot and explain your answer briefly.

8. What is TLS protocol? Why can’t we see the content of data under TLS protocol?

9. Why can’t Wireshark show MAC address of remote hosts?

10. What’s the difference between “Capture filter” and “Display filter” in Wireshark?