Wireshark Packet Capture and Decode (version 1.6)

"I hear and I forget; I see and I remember; I do and I understand"

Date_____

Name_____

CIN_____

Group#_____

Go to web site http://www.wireshark.org and download a copy of the packet capture (sniffer) and analyzer for your operating system. Watch YouTube videos on Wireshark to learn how to use this packet capture software.

1. (2.5 pts) Turn on your sniffer and begin capturing IP version4 network traffic (Note: you may need to generate network traffic)

   a. What is the IP address and subnet mask of your computer? Submit a screenshot that displays these values.

   b. What is the layer-2 destination Ethernet address of broadcast (not unicast) traffic? Submit screenshot with this value circled.

   c. What is the layer-3 destination IP address of broadcast traffic that has an IP (not ARP) header? Submit screenshot with this value circled.

   d. What filtering rule can you use on your sniffer so that it will display only Ethernet frames that contain your computer's IP address? Submit a screenshot with this filter in effect.

   e. What filtering rule can you use on your sniffer so that it will display only Ethernet frames that contain your computer's Ethernet address in the Ethernet frame header? Submit a screenshot with this filter in effect.

2. (2 pts) Capture and decode an **ARP request** and the corresponding **ARP reply** packet. You may need to initially clear your ARP cache (arp –d) in command prompt window (cmd.exe) before generating an ARP packet.

   a. a. What is the hexadecimal value the field in Ethernet frame header that is used to identify that the packet is an ARP packet? Submit screenshot with this value circled.

   b. Turn in screenshots which show the decoded ARP request and ARP reply packets.

3. (2 pts) Capture and decode an IP version4 **ICMP echo request** and the corresponding **ICMP echo reply** packet by running the ping command.

   a. What is the decimal value of the protocol field in IP header that is used to indicate that the packet is an ICMP packet? Submit screenshot with this value circled.

   b. Turn in screenshots which show the decoded ICMP echo request and ICMP echo reply packets.

4. (1.5 pts) On your Windows computer, capture and decode packets generated by a tracert command from your computer to www.calstatela.edu.

    a. How does the tracert command running on the Windows client computer modify the value in the TTL field to cause the routers to reply with ICMP messages?

    b. Provide screenshots of decoded packets to support your answer in 4a.

    c. Turn in a screenshot which shows a decoded ICMP TTL exceeded packet that was generated and sent back from a router to your computer.

5. (2pts) Capture and decode packets associated with an entire http session. Provide screenshots to support your answers.

    a. Circle and Identify the packets on a screenshot that comprise the 3-way handshake used during startup of the TCP connection. What TCP flags were set to 1 during the initial 3-way handshake?

    b. What were the absolute(raw) and relative values of the initial sequence numbers used by the http client and server? Submit screenshots with these values circled. There should be a total of 4 values circled.

    c. What tcp port numbers did the web client and server use? Submit screenshot with these two values circled.

    d. During teardown of the TCP connection, what were the absolute(raw) and relative values of the final acknowledgement numbers sent by the http client and server? Submit screenshots with these values circled. There should be a total of 4 values circled.