EXERCISE - 8

Wireshark Lab: IP, ICMP

EXERCISE QUESTIONS :

1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

2. Within the IP packet header, what is the value in the upper layer protocol field?

3. How many bytes are in the IP header? How many bytes are in the payload *of theIP datagram*? Explain how you determined the number of payload bytes.

4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

5. Which fields in the IP datagram *always* change from one datagram to the next within this series of ICMP messages sent by your computer?

6. Which fields stay constant?

7. Find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* to 2000 (Use command ping –s 2000 www.yahoo.com to change the MTU of the packet). Has that message beenfragmented across more than one IP datagram

8. Write down the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?

9. What information in the IP header indicates that this is not the first datagram fragment? Are there more fragments? How can you tell?

10. What fields change in the IP header between the first and second fragment?