CT2108 Lab – IP Datagram Header and Fragmentation Analysis

In order to generate a trace of IP datagrams for this lab, we will use the ping program to send datagrams of different sizes towards a destination server. Start Wireshark running on your PC or laptop then open a command prompt on your computer and issue the following commands, each command should result in four ICMP Echo Request and Echo Response messages. In your trace, you should be able to see the series of ICMP Echo Request and Echo Response messages.

C:\> ping www.rte.ie

C:\> ping –l 3500 www.rte.ie

Stop the Wireshark packet capture and answer the following 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 the IP 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. Select the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* in *ping* to be 3500. Has that message been fragmented across more than one IP datagram? If your computer has an Ethernet interface, a packet size of 3500 *should* cause fragmentation.
6. Examine 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?
7. Examine the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are there more fragments? How can you tell?
8. What fields change in the IP header between the first and second fragment?
9. Examine the last fragment of the fragmented IP datagram. What information in the IP header indicates that this is the last datagram fragment?
10. How many fragments in total were created from the original datagram?