Lab 6: IP Wireshark Lab (Week 11)
Due: Nov 15th 11:59 PM.

Important: ONLY use the Wireshark traces provided to answer the question. Do NOT capture your own trace to answer the question.

What to Submit: Only the answers to the 10 questions

Where to Submit: Blackboard only.

Material: Watch the instructor video on IP Wireshark lab. You should be able to answer all the question after viewing the video and IP lecture videos

Use **ip_trace1** to answer the questions. I used Pingplotter to generate this trace. You can also use traceroute. For example (Mac and Unix, to send 4000 bytes packet)

```
traceroute gaia.cs.umass.edu 4000
```

/* For Q1 – Q5; sort by Destination IP address and look for the series of ICMP packets. The first one should be Packet # 3*/

Q1) Within the IP packet header, what is the value in the upper layer protocol field?

Q2) How many bytes are in the IP header? How many bytes are in the payload *of the IP datagram*?

Q3) Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

Q4) Which fields in the IP datagram *always* change from one datagram to the next within this series of ICMP?

Q5) Which fields stay constant?

/* Q6 – Q8 for Packet Size 2000 bytes. (Undo the sort i.e. sort by Packet Number (first column)) */

Find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* in *pingplotter* to be 2000.

Q6) Has that message been fragmented across more than one IP datagram? If so, how many?

Q7) 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 last fragment?

/* Q9, Q10 for Packet Size 4000 bytes*/

Find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* in *pingplotter* to be 4000.

Q9) Has that message been fragmented across more than one IP datagram? If so, how many?

Q10) 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 last fragment?