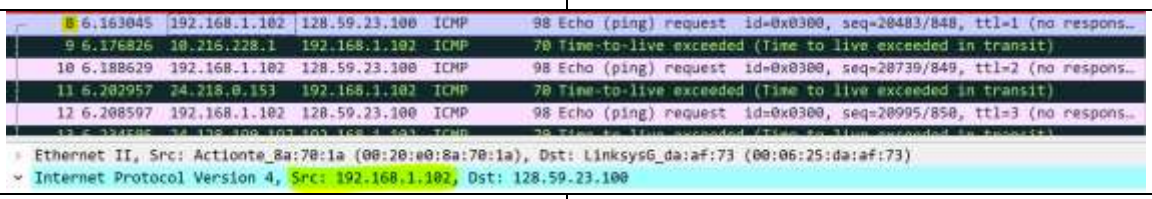
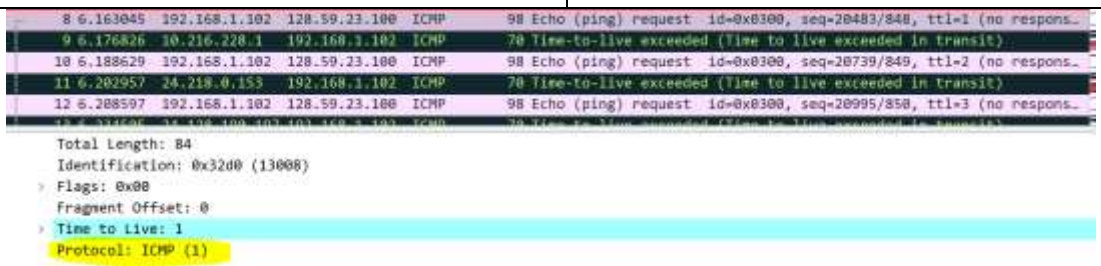
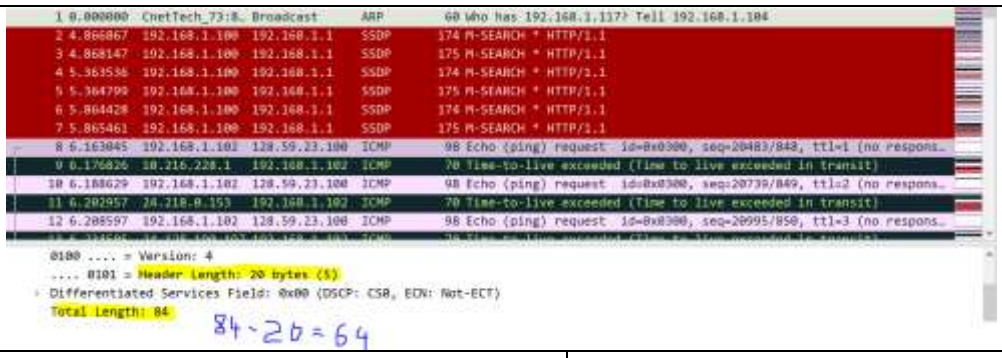
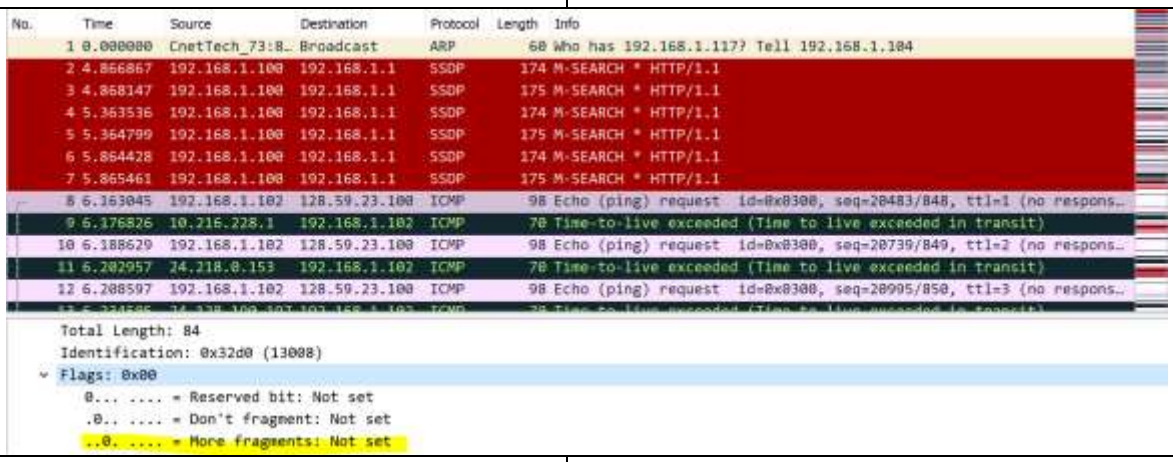
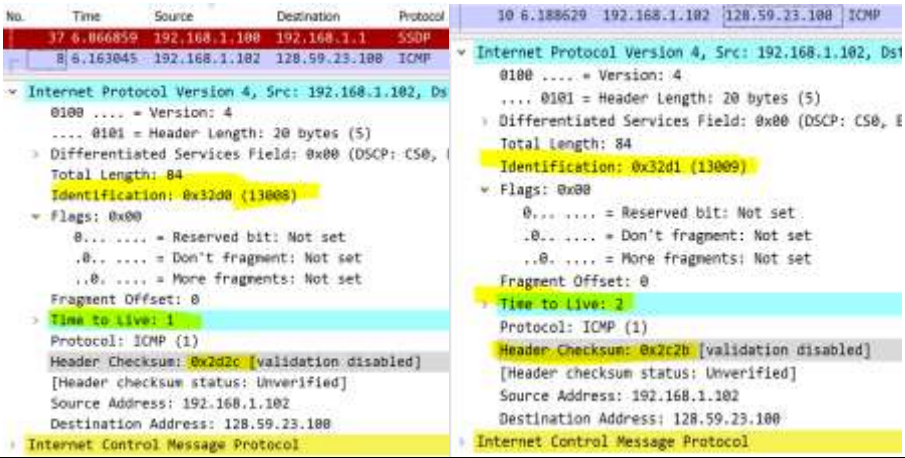
Wireshark Lab 1: IP

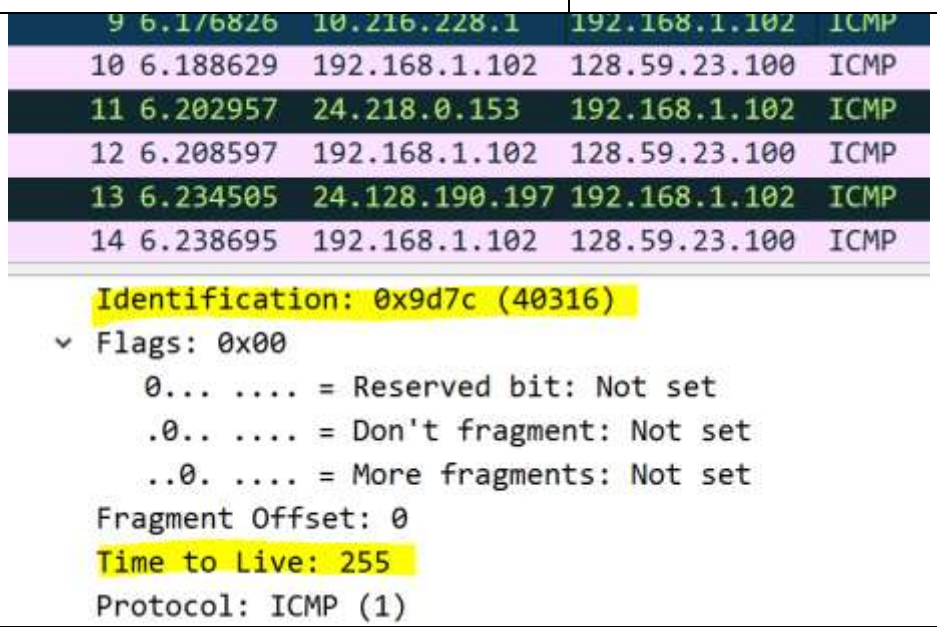
Group Details:

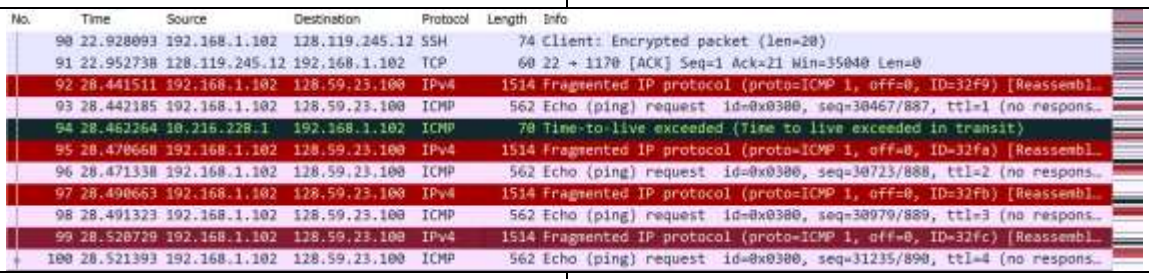
Muhammad Zaheer Hashmi - 1004299056
Hairan Zhang - 1004957601

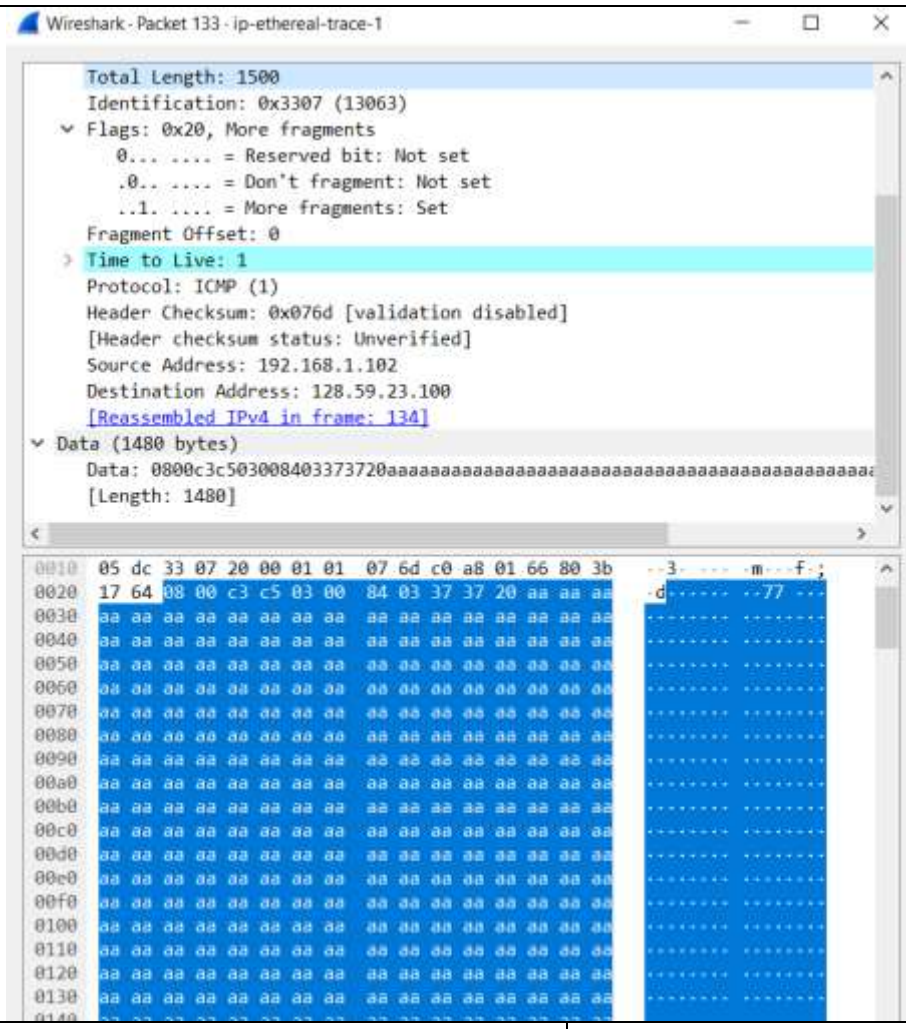
Mark:

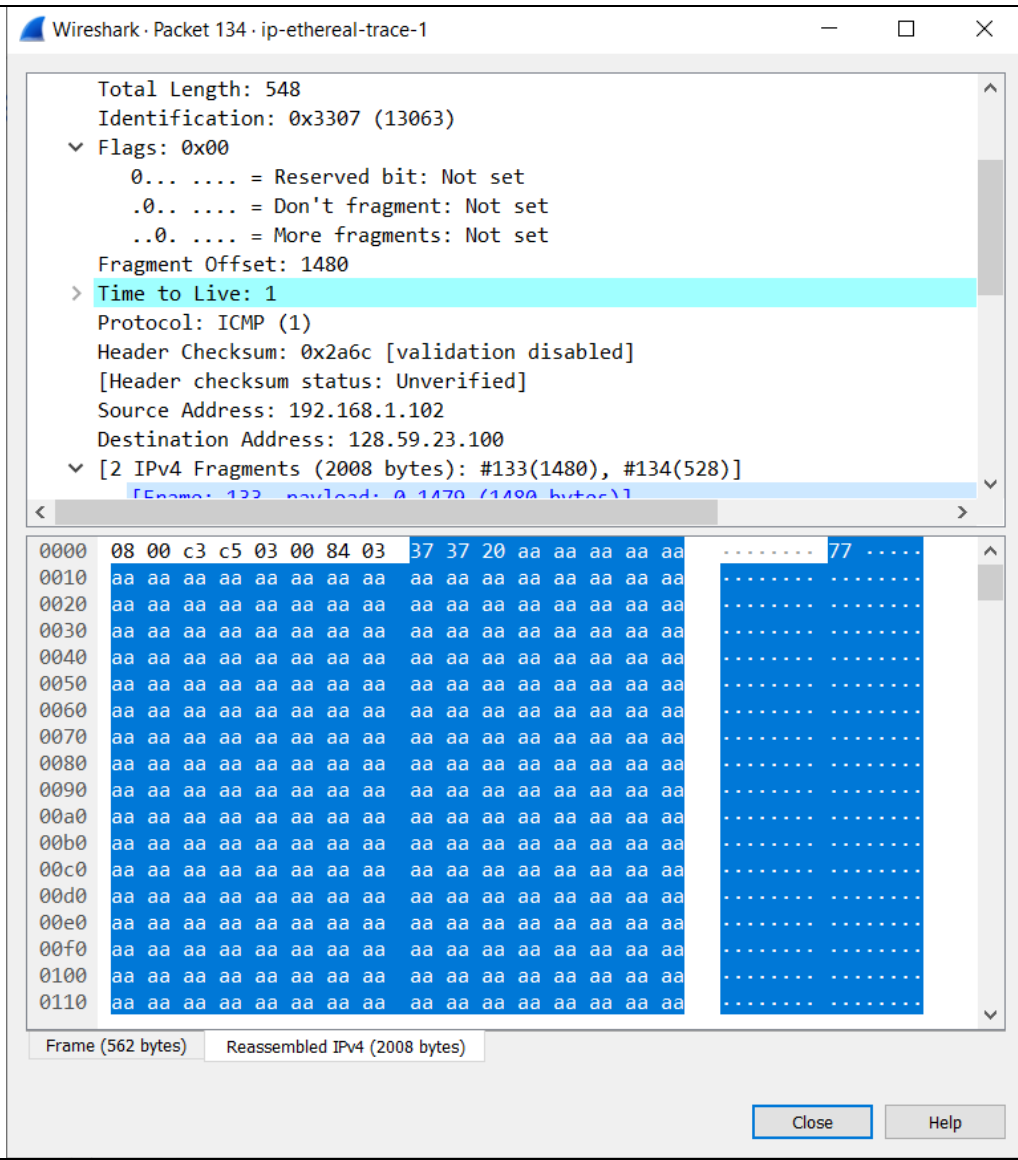
	Question	Answer
1	Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?	The IP address is 192.168.1.102
Annotated Screenshot (if needed)		
2	Within the IP packet header, what is the value in the upper layer protocol field?	The value is 1 indicating use of ICMP
Annotated Screenshot (if needed)		
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.	It total there are 84 bytes. The header has 20 bytes. This means the payload must have 64 bytes.

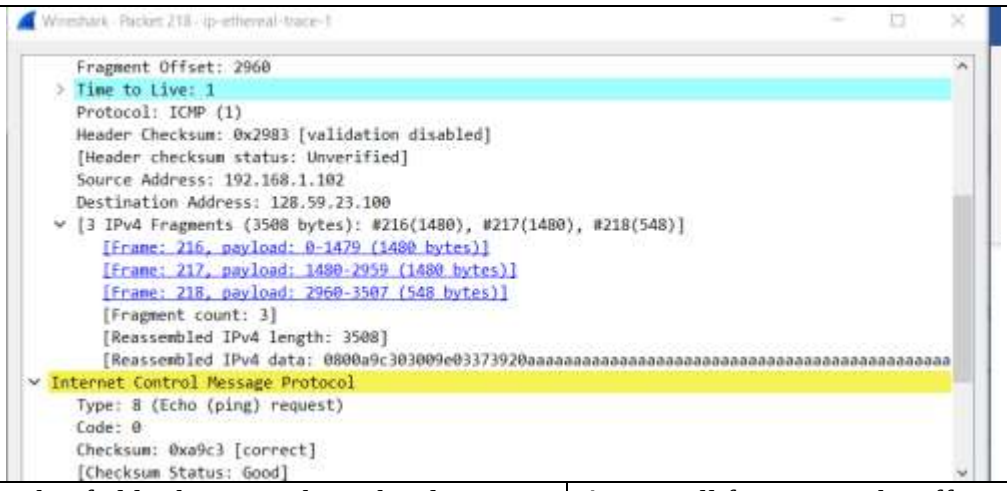
Annotated Screenshot (if needed)		
4	Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.	This datagram is not fragmented. Had it been fragmented the More fragments flag would have been set as we see below.
Annotated Screenshot (if needed)		
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?	The fields that change are time to live, checksum and the identification.
Annotated Screenshot (if needed)		
6	Which fields stay constant? Which of the fields must stay constant? Which fields	In reference to screenshots from above: Fields that stay constant are the header length,

	must change? Why?	IP version, source IP address, destination IP address, Protocol is ICMP, differentiated services. Header length must stay constant because all packets are of same type (ICMP), IP version must remain same because we are using the same IP for all, source and destinations are the same because these are the communication end hosts.
Annotated Screenshot (if needed)		
7	Describe the pattern you see in the values in the Identification field of the IP datagram	From the screenshots referred to in 5, we observed that the identification header is incremented by 1 per ping request.
Annotated Screenshot (if needed)		
8	What is the value in the Identification field and the TTL field?	TTL: 255 Identification: varies
Annotated Screenshot (if needed)		
9	Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?	Time to live remain the as it corresponds to hop count where as the identification changes by message unless if we have fragmentation on a given message.

Annotated Screenshot (if needed)	 	
10	Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?	Yes it is fragmented across more than one datagram as observed below.
Annotated Screenshot (if needed)		
11	Print out 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?	The first fragment is shown below in the pictures. The IP header Flags – More Fragments being set indicates that the datagram has been fragmented. The fragment is indicated under IPv4 headers, and that header indicates that the datagram has been fragmented. The “Fragments Offset” IP header indicates whether this is the first fragment versus the latter fragment, since first fragment would always have 0 offset and the second fragment’s offset would be greater than 0. The IP datagram contains 1480 bytes of data and 20 bytes of header data, so it is 1500 bytes in total.

Annotated Screenshot (if needed)		
12	Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?	Having a fragment offset of greater than zero indicates that this is not the first datagram fragment. There are no more fragments because the “More Fragments” flag is set to zero.

Annotated Screenshot (if needed)		
13	What fields change in the IP header between the first and second fragment?	Fragment offset, Header checksum, More Fragments Bit, Total Length
Annotated Screenshot (if needed)		
14	How many fragments were created from the original datagram?	In the original (reassembled) datagram, we find three fragments.

Annotated Screenshot (if needed)		
15	What fields change in the IP header among the fragments?	Among all fragments, the offset, checksum varies. Between the first two packets and the last packet, total length changes from 1500 to 568 bytes and the more fragments bit change from 1 to 0.
Annotated Screenshot (if needed)		