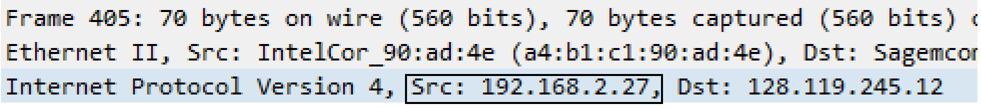
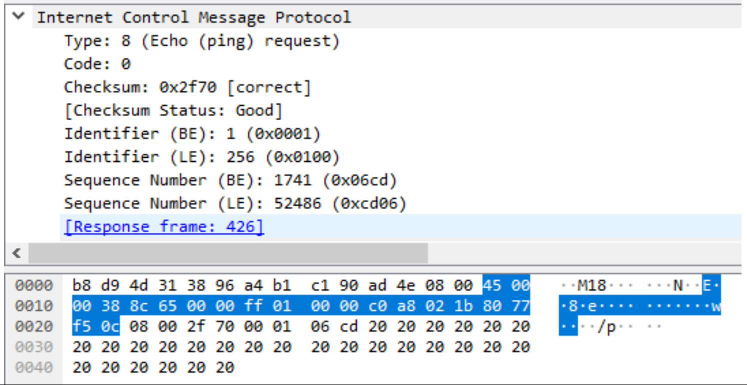
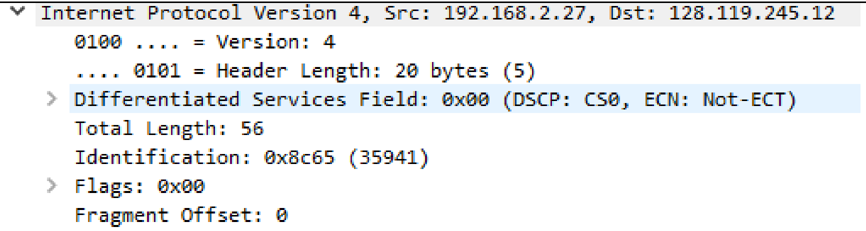
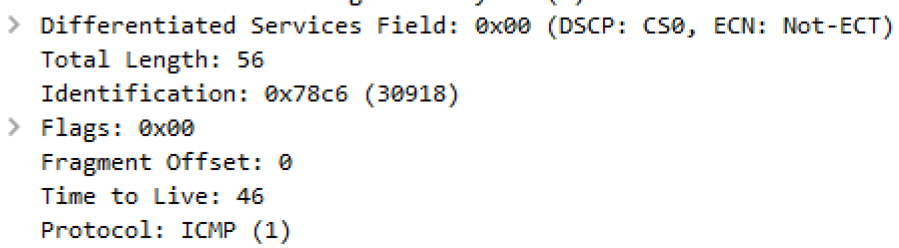
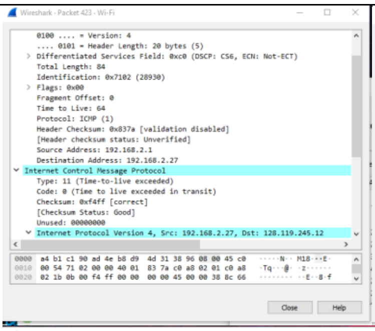
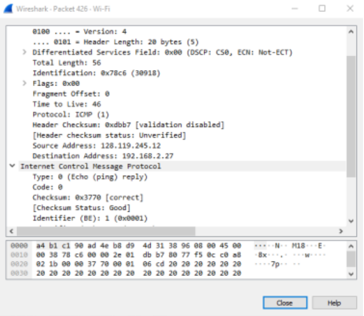
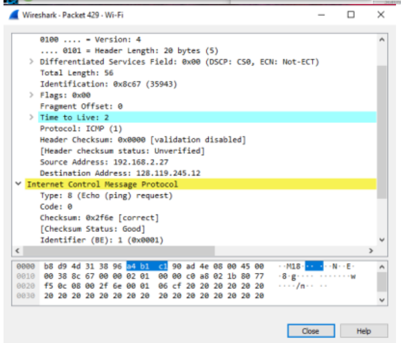
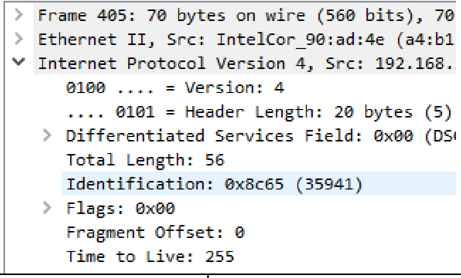
Wireshark Lab 1: IP

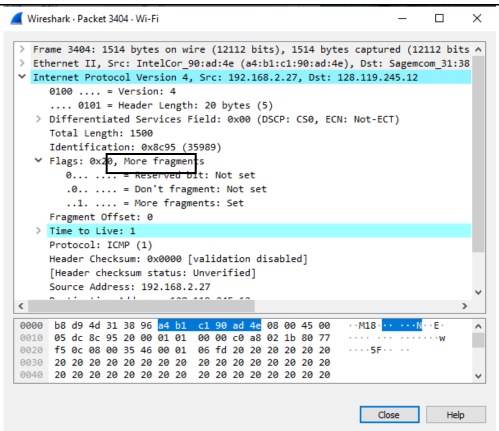
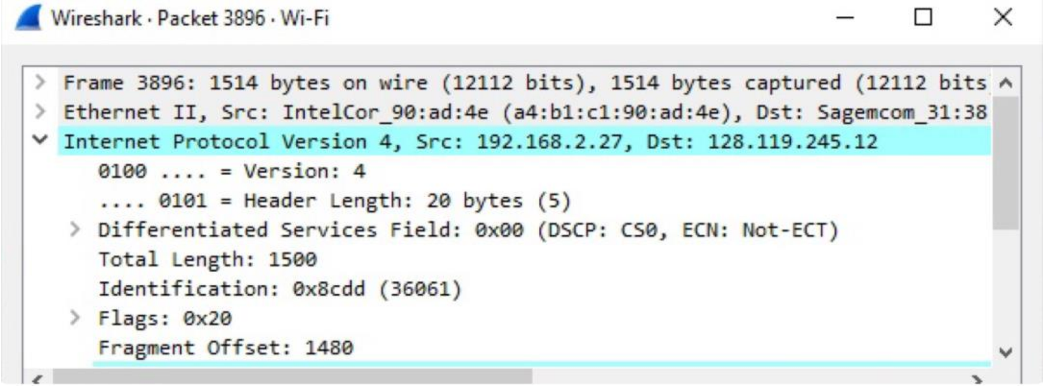
Group Details: Bikramjit Narwal (1005242300), Chao Glen Xu (1004274634)

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 of my computer is 192.168.2.27.
Annotated Screenshot (if needed)	 Frame 405: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) o Ethernet II, Src: IntelCor_90:ad:4e (a4:b1:c1:90:ad:4e), Dst: Sagemcor Internet Protocol Version 4, Src: 192.168.2.27, Dst: 128.119.245.12	
2	Within the IP packet header, what is the value in the upper layer protocol field?	The value in the upper layer protocol field is ICMP (0x01).
Annotated Screenshot (if needed)	 Internet Control Message Protocol Type: 8 (Echo (ping) request) Code: 0 Checksum: 0x2f70 [correct] [Checksum Status: Good] Identifier (BE): 1 (0x0001) Identifier (LE): 256 (0x0100) Sequence Number (BE): 1741 (0x06cd) Sequence Number (LE): 52486 (0xcd06) [Response frame: 426] 0000 b8 d9 4d 31 38 96 a4 b1 c1 90 ad 4e 08 00 45 00 ··M18··· ···N··E· 0010 00 38 8c 65 00 00 ff 01 00 00 c0 a8 02 1b 80 77 ·8·e···· ·······w 0020 f5 0c 08 00 2f 70 00 01 06 cd 20 20 20 20 20 20 ····/p·· ·· 0030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0040 20 20 20 20 20 20	
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.	In the IP header, there are 20 bytes. In total, there are 56 bytes. Due to these numbers, we get 36 bytes (56-20) in the payload of the IP address

Annotated Screenshot (if needed)	 Internet Protocol Version 4, Src: 192.168.2.27, Dst: 128.119.245.12 0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 56 Identification: 0x8c65 (35941) Flags: 0x00 Fragment Offset: 0	
4	Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.	As shown in the screenshot below, the fragment offset is set to 0. This means that the packet has not been fragmented.
Annotated Screenshot (if needed)	 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 56 Identification: 0x78c6 (30918) Flags: 0x00 Fragment Offset: 0 Time to Live: 46 Protocol: ICMP (1)	
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?	Looking at some screenshots from below, it looks like identification, time to live, and header checksum always change.
Annotated Screenshot (if needed)	 Wireshark · Packet 423 · Wi-Fi 0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT) Total Length: 84 Identification: 0x7102 (28930) Flags: 0x00 Fragment Offset: 0 Time to Live: 64 Protocol: ICMP (1) Header Checksum: 0x837a [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.2.1 Destination Address: 192.168.2.27 Internet Control Message Protocol Type: 11 (Time-to-live exceeded) Code: 0 (Time to live exceeded in transit) Checksum: 0xf4ff [correct] [Checksum Status: Good] Unused: 00000000 Internet Protocol Version 4, Src: 192.168.2.27, Dst: 128.119.245.12 0000 a4 b1 c1 90 ad 4e b8 d9 4d 31 38 96 08 00 45 c0 ······N·· M18···E· 0010 00 54 71 02 00 00 40 01 83 7a c0 a8 02 01 c0 a8 ·Tq···@· ·z······ 0020 02 1b 0b 00 f4 ff 00 00 00 00 45 00 00 38 8c 66 ········ ··E··8·f Close Help  Wireshark · Packet 426 · Wi-Fi 0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 56 Identification: 0x78c6 (30918) Flags: 0x00 Fragment Offset: 0 Time to Live: 46 Protocol: ICMP (1) Header Checksum: 0xdbb7 [validation disabled] [Header checksum status: Unverified] Source Address: 128.119.245.12 Destination Address: 192.168.2.27 Internet Control Message Protocol Type: 0 (Echo (ping) reply) Code: 0 Checksum: 0x3770 [correct] [Checksum Status: Good] Identifier (BE): 1 (0x0001) 0000 a4 b1 c1 90 ad 4e b8 d9 4d 31 38 96 08 00 45 00 ······N·· M18···E· 0010 00 38 78 c6 00 00 2e 01 db b7 80 77 f5 0c c0 a8 ·8x···.· ···w···· 0020 02 1b 00 00 37 70 00 01 06 cd 20 20 20 20 20 20 ····7p·· ·· 0030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 Close Help  Wireshark · Packet 429 · Wi-Fi 0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 56 Identification: 0x8c67 (35943) Flags: 0x00 Fragment Offset: 0 Time to Live: 2 Protocol: ICMP (1) Header Checksum: 0x0000 [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.2.27 Destination Address: 128.119.245.12 Internet Control Message Protocol Type: 8 (Echo (ping) request) Code: 0 Checksum: 0x2f6e [correct] [Checksum Status: Good] Identifier (BE): 1 (0x0001) 0000 b8 d9 4d 31 38 96 a4 b1 c1 90 ad 4e 08 00 45 00 ··M18····N··E· 0010 00 38 8c 67 00 00 02 01 00 00 c0 a8 02 1b 80 77 ·8·g···· ·······w 0020 f5 0c 08 00 2f 6e 00 01 06 cf 20 20 20 20 20 20 ····/n·· ·· 0030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 Close Help	
6	Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?	Stay constant: - Version (IPV4) - Length of header - Source IP

		- Destination IP - Upper layer protocol Must stay constant - Same as above Must change - Identification - Header checksum - Time to live
Annotated Screenshot (if needed)	Screenshots from Q5	
7	Describe the pattern you see in the values in the Identification field of the IP datagram	The identification field of the IP datagram increments with each ping request.
Annotated Screenshot (if needed)	In the screenshots from Q5, the identification field of the IP datagrams increment with each ping request.	
8	What is the value in the Identification field and the TTL field?	Identification field: 0x8c65 (35941) Time to live: 225
Annotated Screenshot (if needed)	 Frame 405: 70 bytes on wire (560 bits), 70 Ethernet II, Src: IntelCor_90:ad:4e (a4:b1 Internet Protocol Version 4, Src: 192.168. 0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DS Total Length: 56 Identification: 0x8c65 (35941) Flags: 0x00 Fragment Offset: 0 Time to Live: 255	
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?	Since the field has to have a unique value, the identification field must change from all the ICMP TTL-exceeded replies. Also, the TTL field does not change at all since the TTL to the first hop router is always the same.
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 the message has been fragmented across more than one IP datagram. This is indicated by the "More fragments" in the screenshot below.

Annotated Screenshot (if needed)	 Wireshark · Packet 3404 · Wi-Fi Frame 3404: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits Ethernet II, Src: IntelCor_90:ad:4e (a4:b1:c1:90:ad:4e), Dst: Sagemcom_31:38 Internet Protocol Version 4, Src: 192.168.2.27, Dst: 128.119.245.12 0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 1500 Identification: 0x8c95 (35989) Flags: 0x20, More fragments 0... .... = Reserved bit: Not set .0.. .... = Don't fragment: Not set ..1. .... = More fragments: Set Fragment Offset: 0 Time to Live: 1 Protocol: ICMP (1) Header Checksum: 0x0000 [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.2.27 0000 b8 d9 4d 31 38 96 a4 b1 c1 90 ad 4e 08 00 45 00 ··M18·······N··E· 0010 05 dc 8c 95 20 00 01 01 00 00 c0 a8 02 1b 80 77 ················w 0020 f5 0c 08 00 35 46 00 01 06 fd 20 20 20 20 20 20 ····5F·· ·· 0030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0040 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 	
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?	- More fragments flag bit is set (datagram has been fragmented) - Offset is 0, therefore it is the first fragment - Total length is 1500 (also including header)
Annotated Screenshot (if needed)	Screenshot from Q10	
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?	Information that indicates that this is not the first datagram: - Fragment offset is 1480 No more fragments since the flag is not set for more fragments.
Annotated Screenshot (if needed)	 Wireshark · Packet 3896 · Wi-Fi Frame 3896: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits Ethernet II, Src: IntelCor_90:ad:4e (a4:b1:c1:90:ad:4e), Dst: Sagemcom_31:38 Internet Protocol Version 4, Src: 192.168.2.27, Dst: 128.119.245.12 0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 1500 Identification: 0x8cdd (36061) Flags: 0x20 Fragment Offset: 1480	
13	What fields change in the IP header between the first and second fragment?	- Flags set - Fragment offset - Length - Header checksum

14	How many fragments were created from the original datagram?	Switching to 3500 bytes, 3 packets are created.
15	What fields change in the IP header among the fragments?	- Fragment offset - Checksum