HO CHI MINH UNIVERSITY OF TECHNOLOGY
Faculty of Computer Science and Engineering

Computer Networks

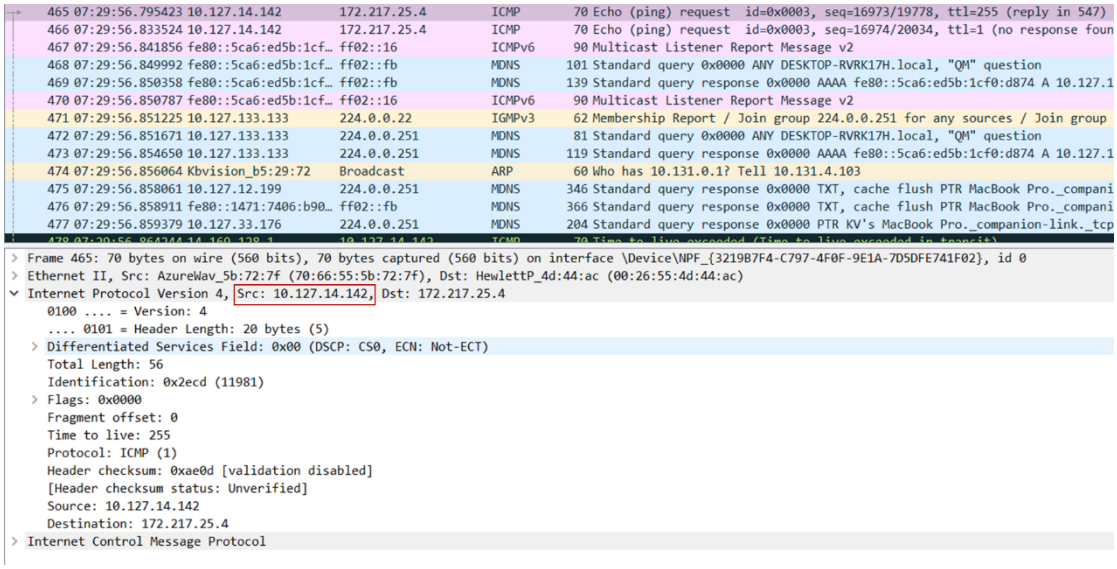
Report for lab 4a

Lecture: Nguyễn Mạnh Thìn
Student name: Đặng Trần Khánh-1852037

I. A look at the captured trace

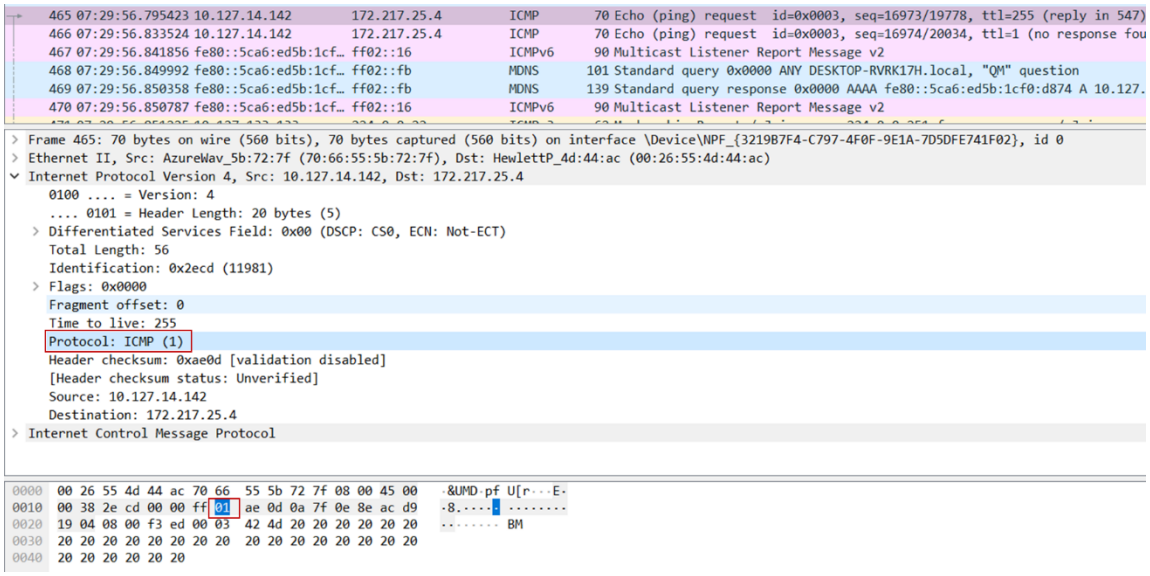
1. What is the IP address of your computer?

Answer: The IP address of my computer is 10.127.14.142



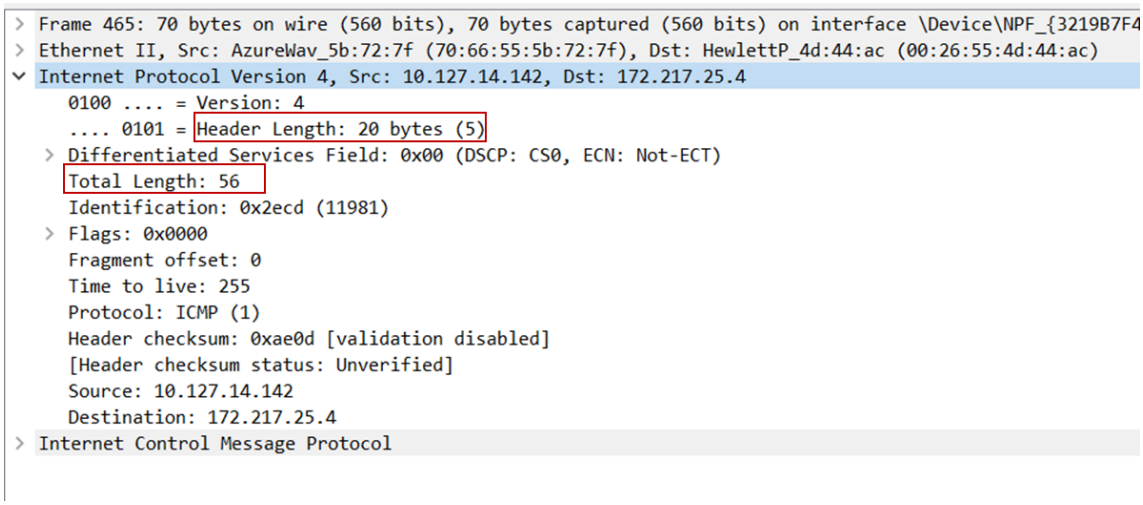
2. Within the IP packet header, what is the value in the upper layer protocol field?

Answer: The value in the upper layer protocol field is ICMP (1) 0x01 in Hexadecimal.



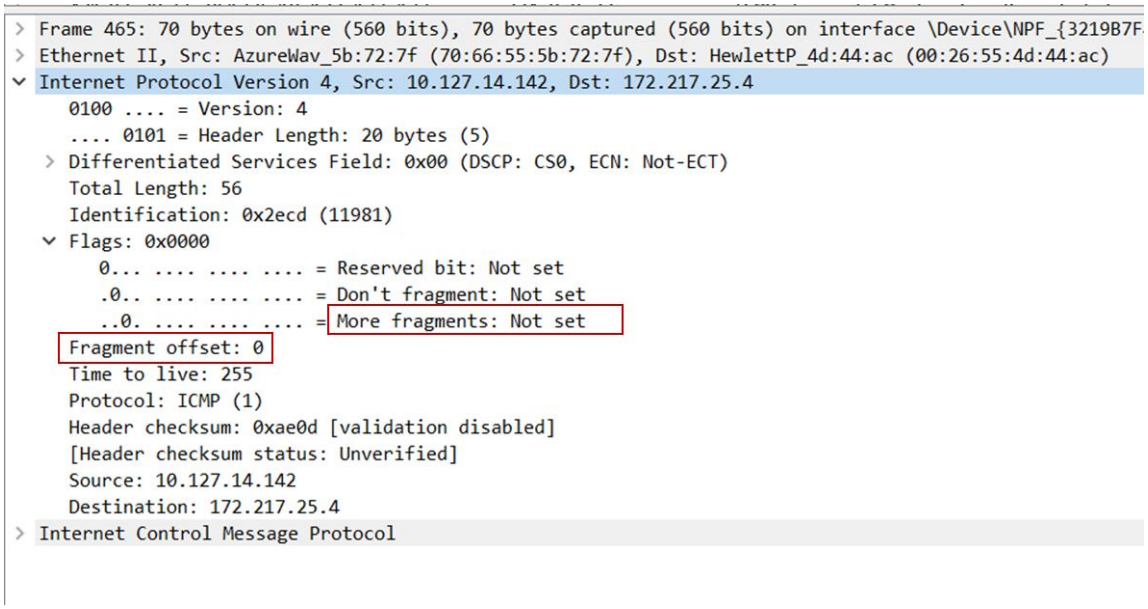
3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

Answer: There are 20 bytes in the IP header (image below). Because the total length of the IP datagram is 56 bytes, the payload consists of 56 – 20 (header bytes) = 36 bytes.



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

Answer: The fragment offset field is 0 and the more fragments field is not set, therefore this IP datagram has not 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?

Answer: Identification, Time to live and Header checksum always change from one datagram to the next within this series of ICMP messages sent by my computer.

6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

Answer:

Fields stay constant:

1/ Version (IPv4 for all packets)

2/ Header length (doesn't change since we are always using IPv4)

3/ Source IP (my computer's IP address doesn't change)

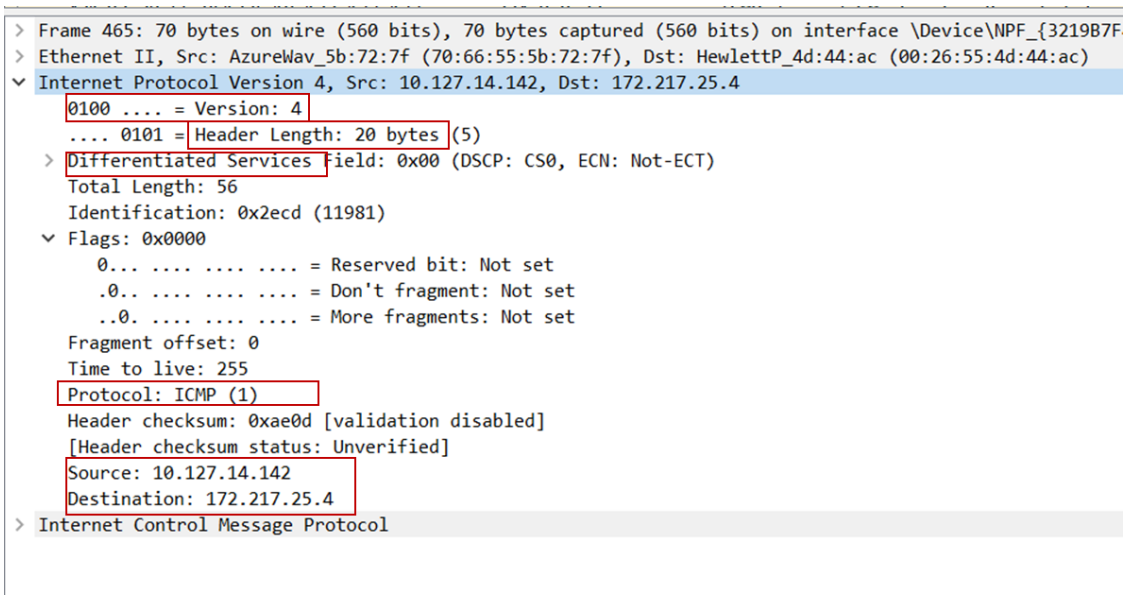
4/ Destination IP (the site IP address doesn't change)

5/ Differentiated Services (since all packets are ICMP they use the same Type of Service class)

6/ Upper Layer Protocol (always using ICMP)

Fields must stay constant:

Same as fields stay constant: version, header length, source IP, destination IP, differentiated services, upper layer protocol.

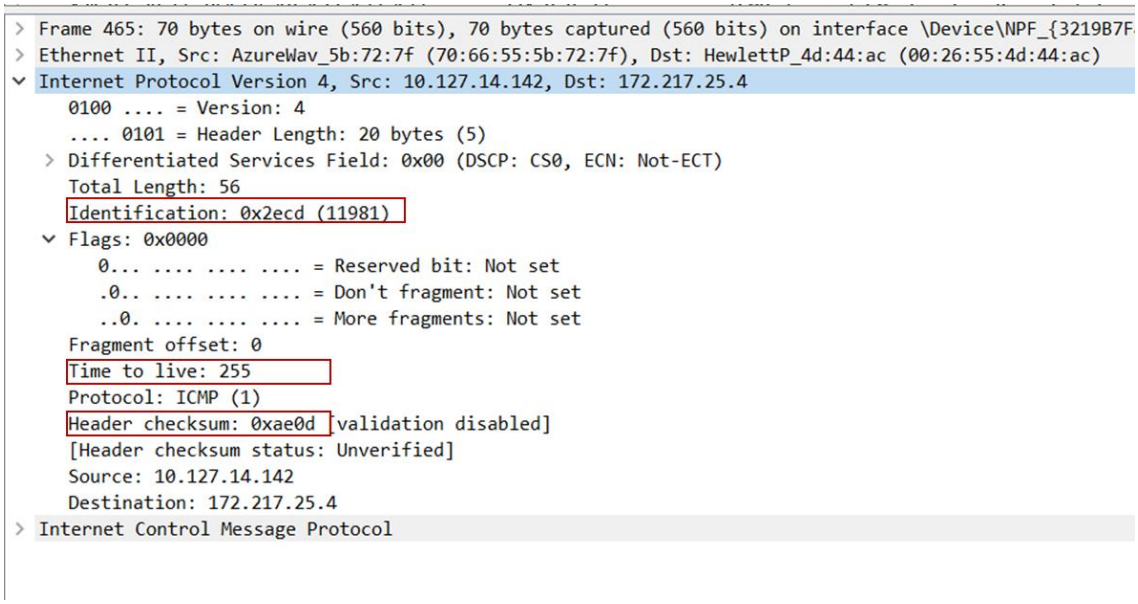


Fields must change:

1/ Identification (Each IP packet must have different id to distinguish)

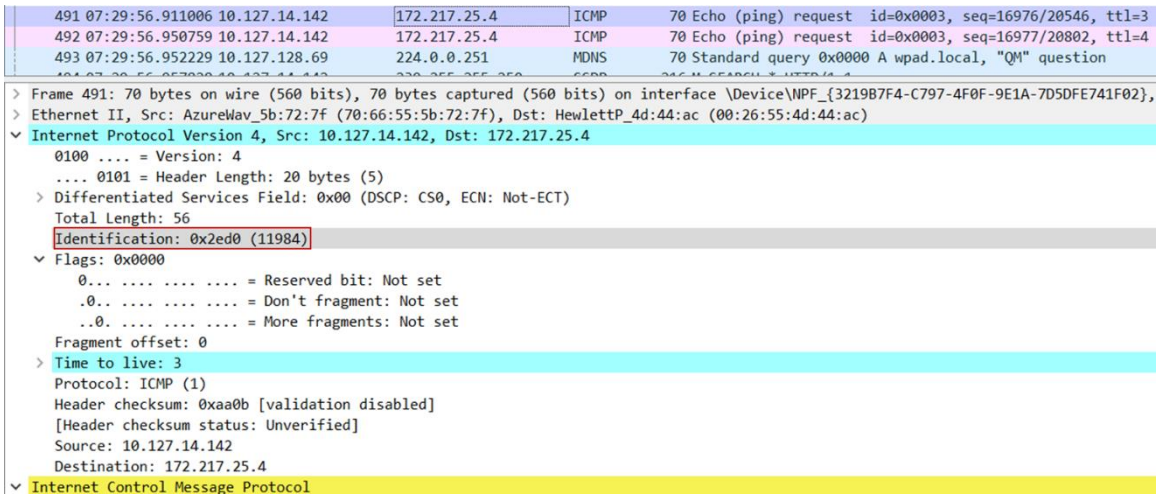
2/ Time to live (traceroute increments each subsequent packet as described in the lab specification)

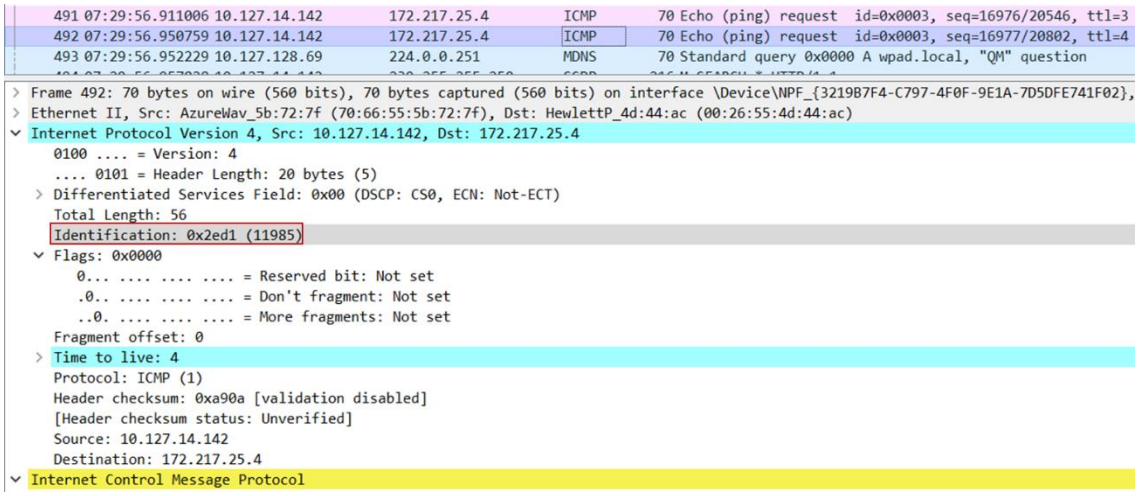
3/ Header checksum (Header changes every time, therefore checksum also has to change)



7. Describe the pattern you see in the values in the Identification field of the IP datagram

Answer: The pattern in the Identification field of IP datagram is that IP header Identification fields increment with each ICMP Echo (ping) request.

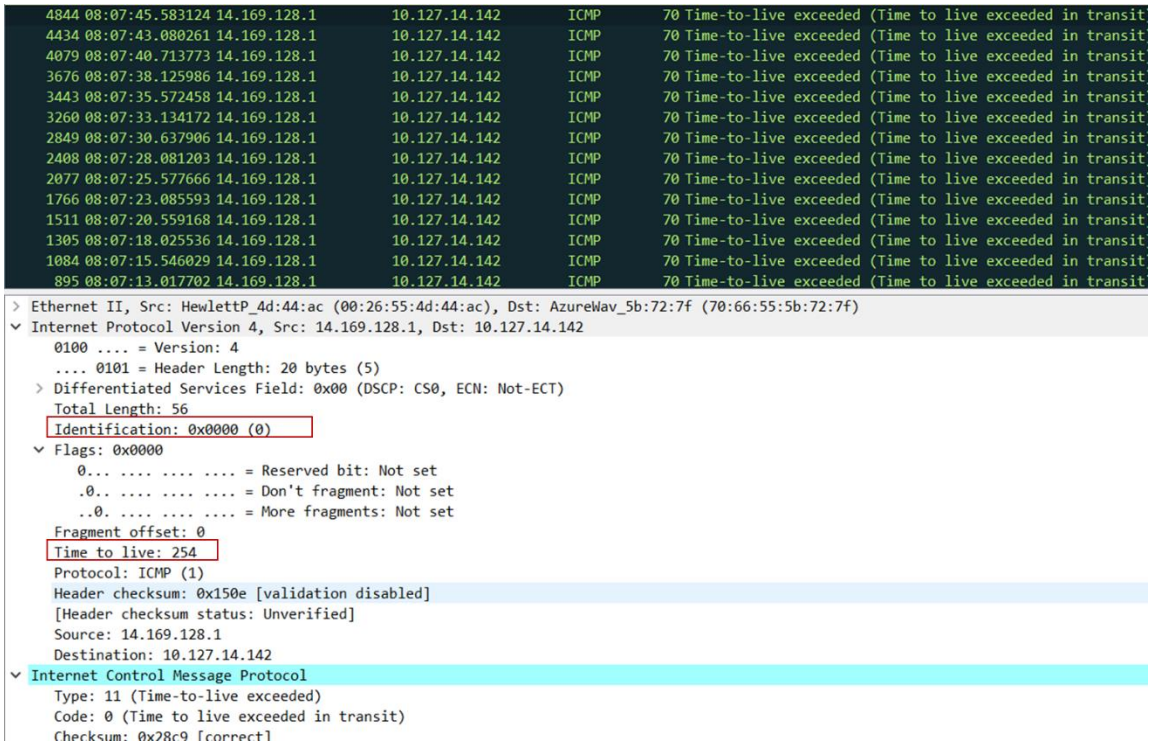




The value increments from 11984 (the first image) to 11985 (second request).

8. What is the value in the Identification field and the TTL field?

Answer: The identification field is 0x0000 (0), the TTL field is 254.

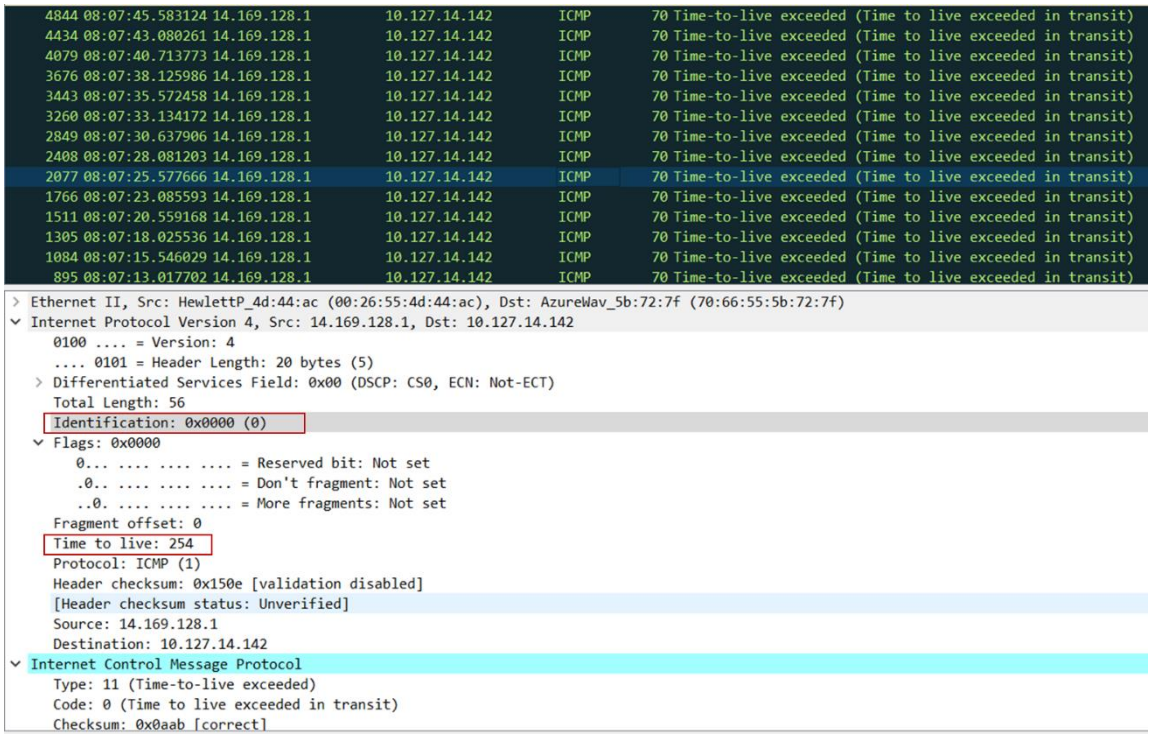


9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

Answer:

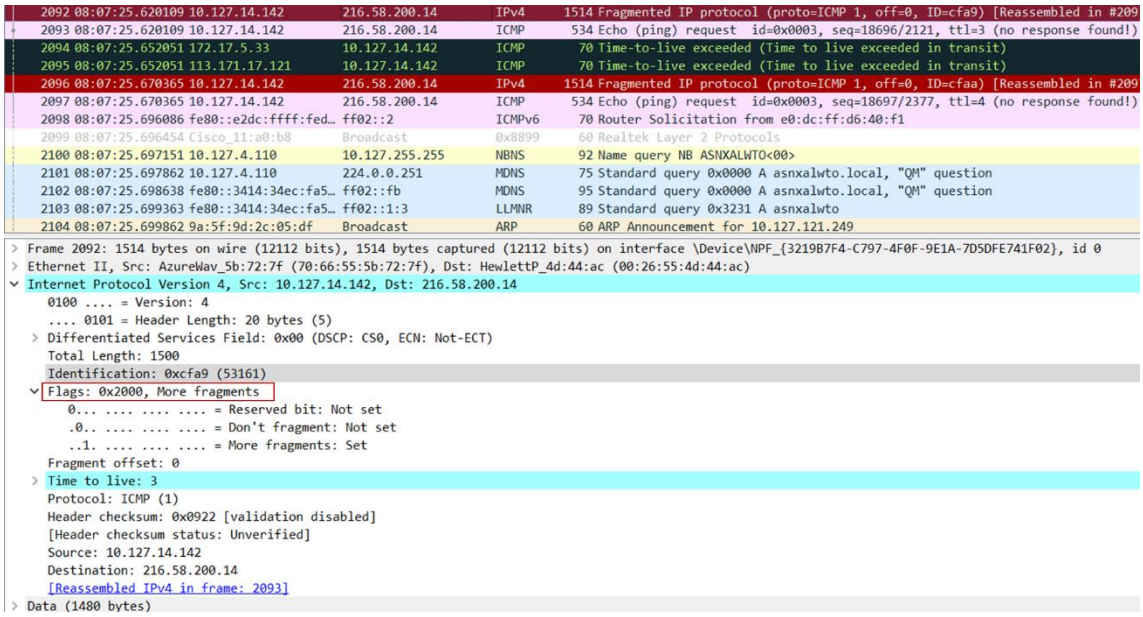
The TTL will remain unchanged because the first hop router is always the same. Identification field for all ICMP TTL-exceeded replies will change because it is assigned a unique value. When two or more IP datagrams have the same identification value that means that these IP datagrams are fragments of a single large IP datagram.

In the image below (the next ICMP of the question 8), identification field remains at 0, the time to live also remains at 254.



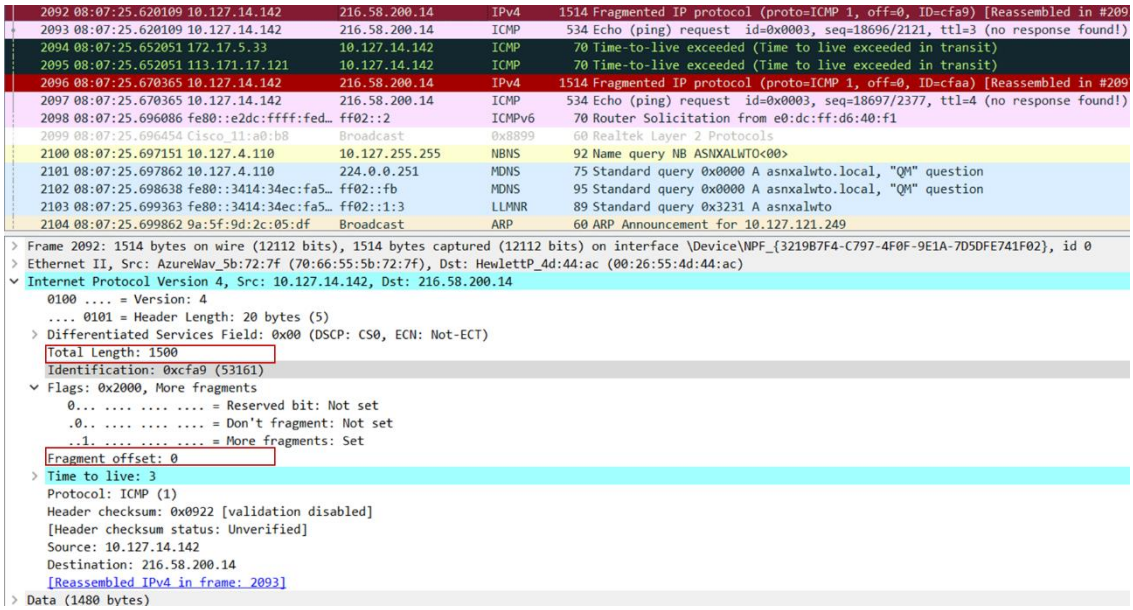
10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?

Answer: Yes, this packet has been fragmented across more than one IP datagram. The flags field shows that there are more fragments of this IP datagram.



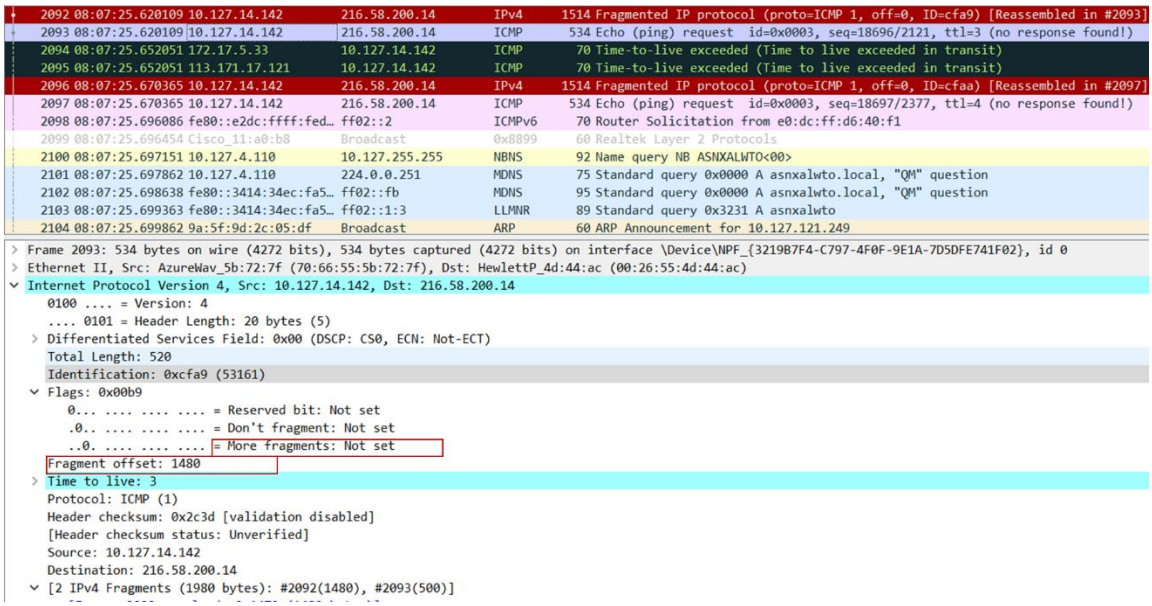
11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?

Answer: The more fragments field is set, which indicates the datagram has been fragmented. The fragment offset (0) points out that this is the first fragment. The length of this fragment is 1500.



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 there more fragments? How can you tell?

Answer: The fragment offset (1480) indicates that this is not the first datagram fragment. There are no more fragments as the More fragments field is not set.

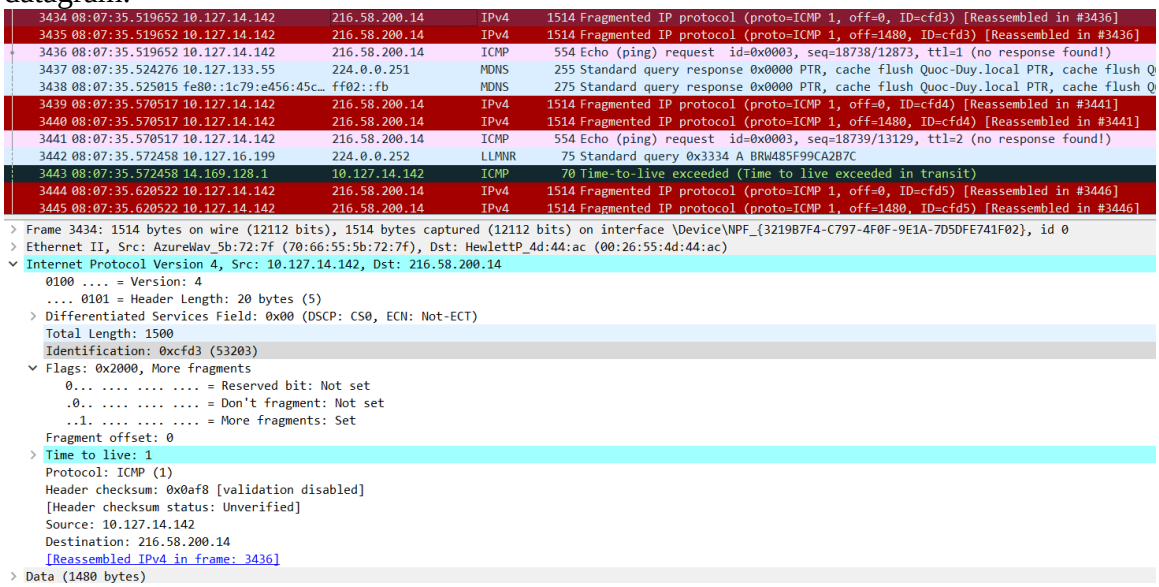


13. What fields change in the IP header between the first and second fragment?

Answer: The IP header fields that changed between the fragments are: total length, flags, fragment offset and checksum.

14. How many fragments were created from the original datagram?

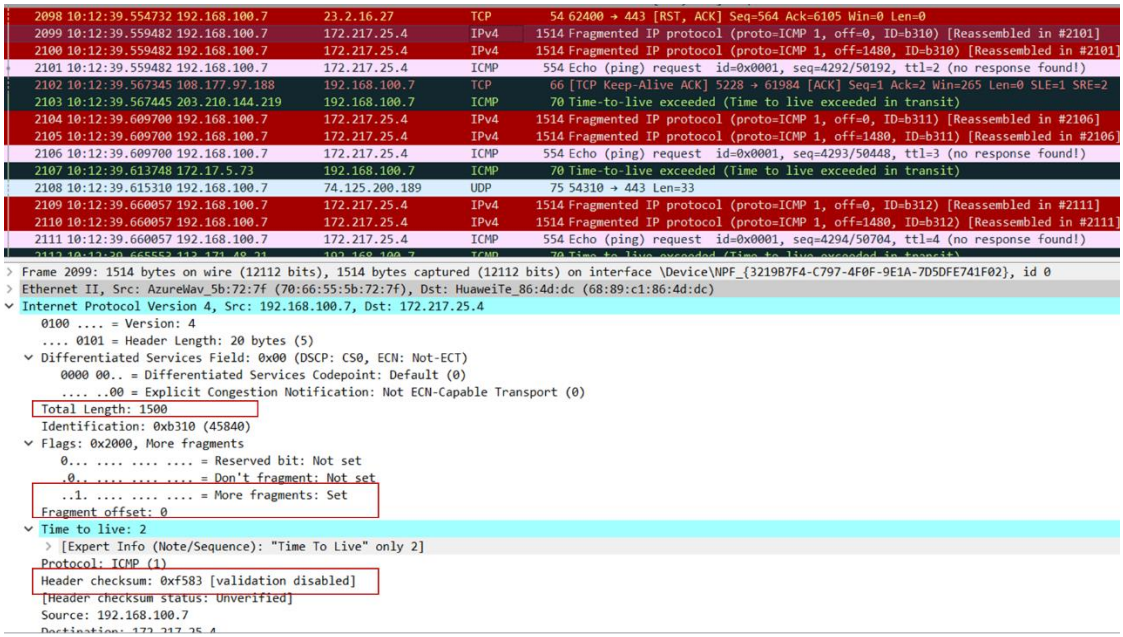
Answer: According to the screenshot, there were 3 fragments created from the original datagram.



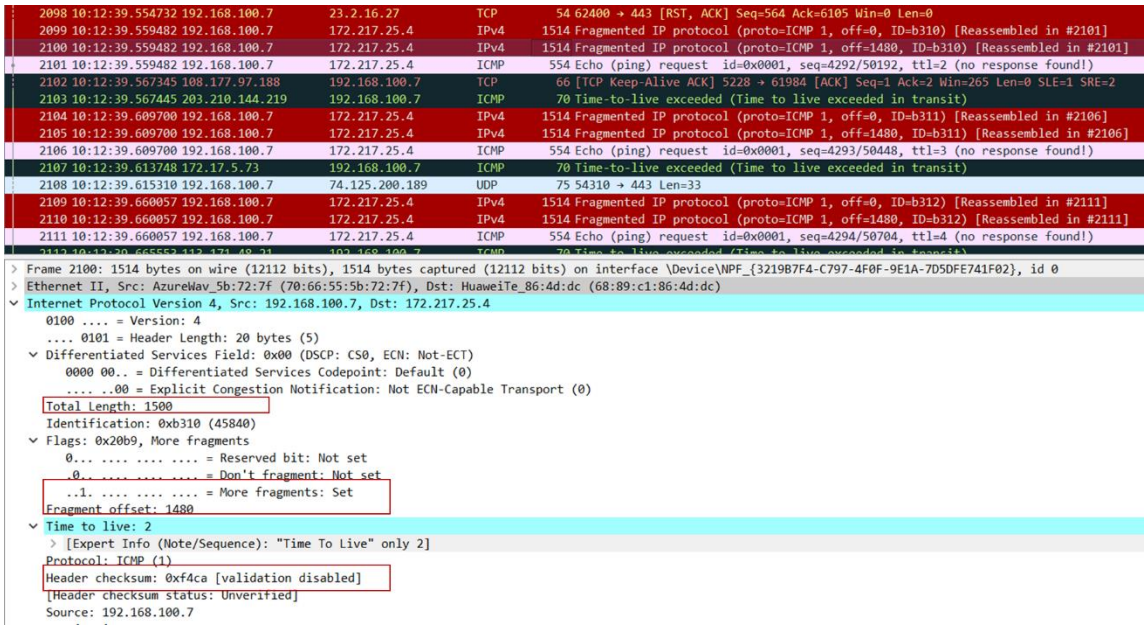
15. What fields change in the IP header among the fragments?

Answer: The fields changing in the IP header among the fragments are the fragment offset, 0 for the first, 1480 for the second and 2960 for the third. The checksum was also different among the fragments. The first 2 packets also have lengths of 1500 and more fragments flags set, while the last fragment is shorter (540) and does not have a flag set.

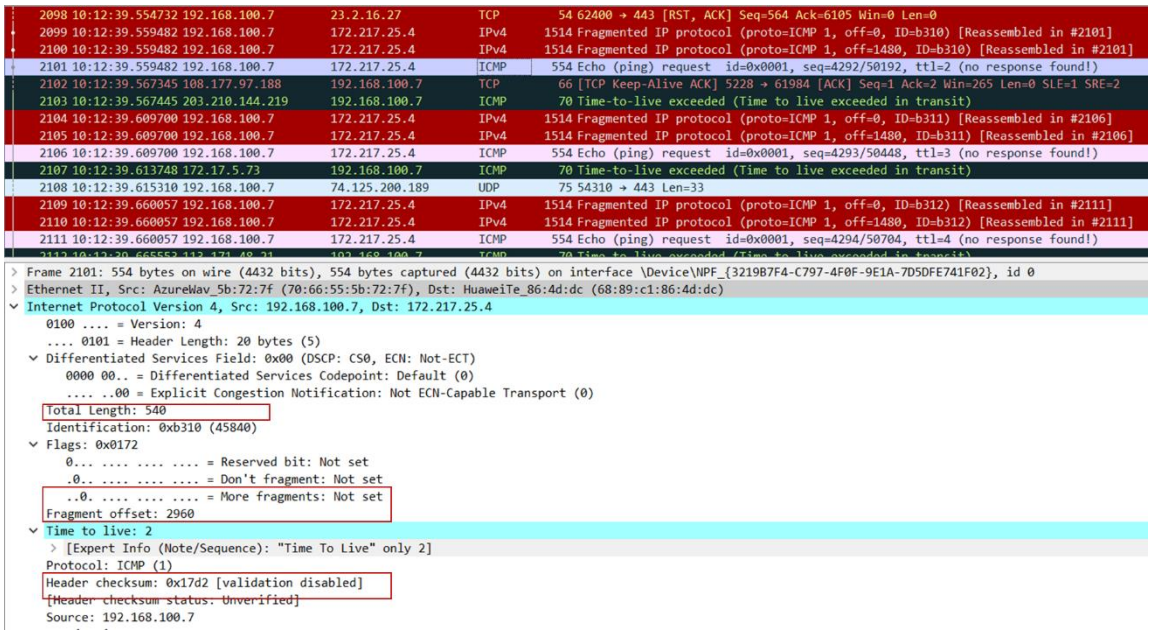
The first fragment:



The second fragment:



The third fragment:


2098 10:12:39.554732 192.168.100.7 23.2.16.27 TCP 54 62400 → 443 [RST, ACK] Seq=564 Ack=6105 Win=0 Len=0
2099 10:12:39.559482 192.168.100.7 172.217.25.4 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=b310) [Reassembled in #2101]
2100 10:12:39.559482 192.168.100.7 172.217.25.4 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=b310) [Reassembled in #2101]
2101 10:12:39.559482 192.168.100.7 172.217.25.4 ICMP 554 Echo (ping) request id=0x0001, seq=4292/50192, ttl=2 (no response found!)
2102 10:12:39.567345 108.177.97.188 192.168.100.7 TCP 66 [TCP Keep-Alive ACK] 5228 → 61984 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
2103 10:12:39.567445 203.210.144.219 192.168.100.7 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
2104 10:12:39.609700 192.168.100.7 172.217.25.4 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=b311) [Reassembled in #2106]
2105 10:12:39.609700 192.168.100.7 172.217.25.4 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=b311) [Reassembled in #2106]
2106 10:12:39.609700 192.168.100.7 172.217.25.4 ICMP 554 Echo (ping) request id=0x0001, seq=4293/50448, ttl=3 (no response found!)
2107 10:12:39.613748 172.17.5.73 192.168.100.7 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
2108 10:12:39.615310 192.168.100.7 74.125.200.189 UDP 75 54310 → 443 Len=33
2109 10:12:39.660057 192.168.100.7 172.217.25.4 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=b312) [Reassembled in #2111]
2110 10:12:39.660057 192.168.100.7 172.217.25.4 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=b312) [Reassembled in #2111]
2111 10:12:39.660057 192.168.100.7 172.217.25.4 ICMP 554 Echo (ping) request id=0x0001, seq=4294/50704, ttl=4 (no response found!)
Frame 2101: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface \Device\NPF_{3219B7F4-C797-4F0F-9E1A-7D5DFE741F02}, id 0
Ethernet II, Src: AzureWav_5b:72:7f (70:66:55:5b:72:7f), Dst: HuaweiTe_86:4d:dc (68:89:c1:86:4d:dc)
Internet Protocol Version 4, Src: 192.168.100.7, Dst: 172.217.25.4
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 540
Identification: 0xb310 (45840)
Flags: 0x0172
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
Fragment offset: 2960
Time to live: 2
[Expert Info (Note/Sequence): "Time To Live" only 2]
Protocol: ICMP (1)
Header checksum: 0x17d2 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.100.7