Wireshark Lab:

IP

v

8

.0

Supplement to

*Computer Networking: A Top*

*-*

*Down*

*Approach,*

*8*

*th*

*ed.*

*,*

J.F. Kurose and K.W. Ross

*“Tell me and I forget. Show me and I remember. Involve me*

*and I understand.”*

Chinese proverb

©

2005

-

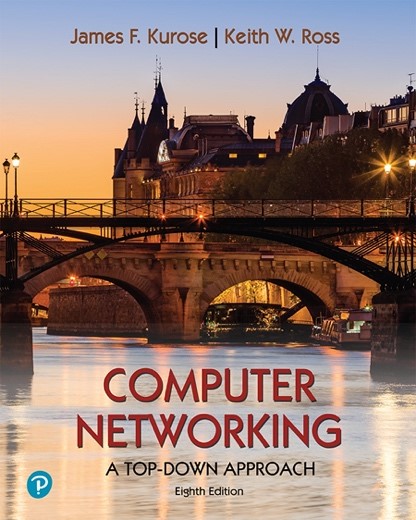
20

20

, J.F Kurose and K.W. Ross, Al

l R

ights Reserved



|  |  |
| --- | --- |
| Student’ Name: | Nguyễn Hữu Hiếu |
| Student’ ID : | 2013149 |

In this lab, we’ll investigate the IP protocol, focusing on the IP datagram. We’ll do so by analyzing a trace of IP datagrams sent and received by an execution of the traceroute program (the traceroute program itself is explored in more detail in the Wireshark ICMP lab). We’ll investigate the various fields in the IP datagram, and study IP fragmentation in detail.

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.

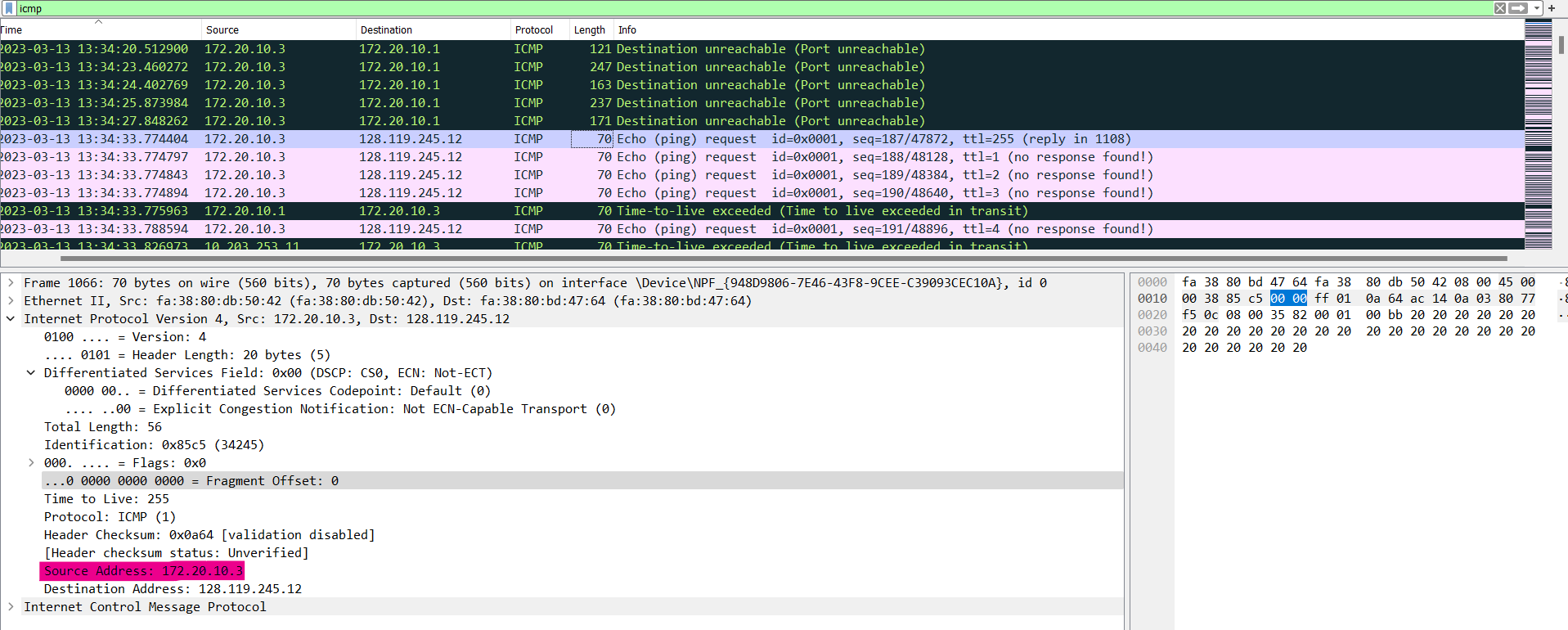


Figure : Capture for Question 1

What is the IP address of your computer?

My IP address of my computer is 172.20.10.3

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

Within the header, the value in the upper layer protocol field is ICMP (1)

1. 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.

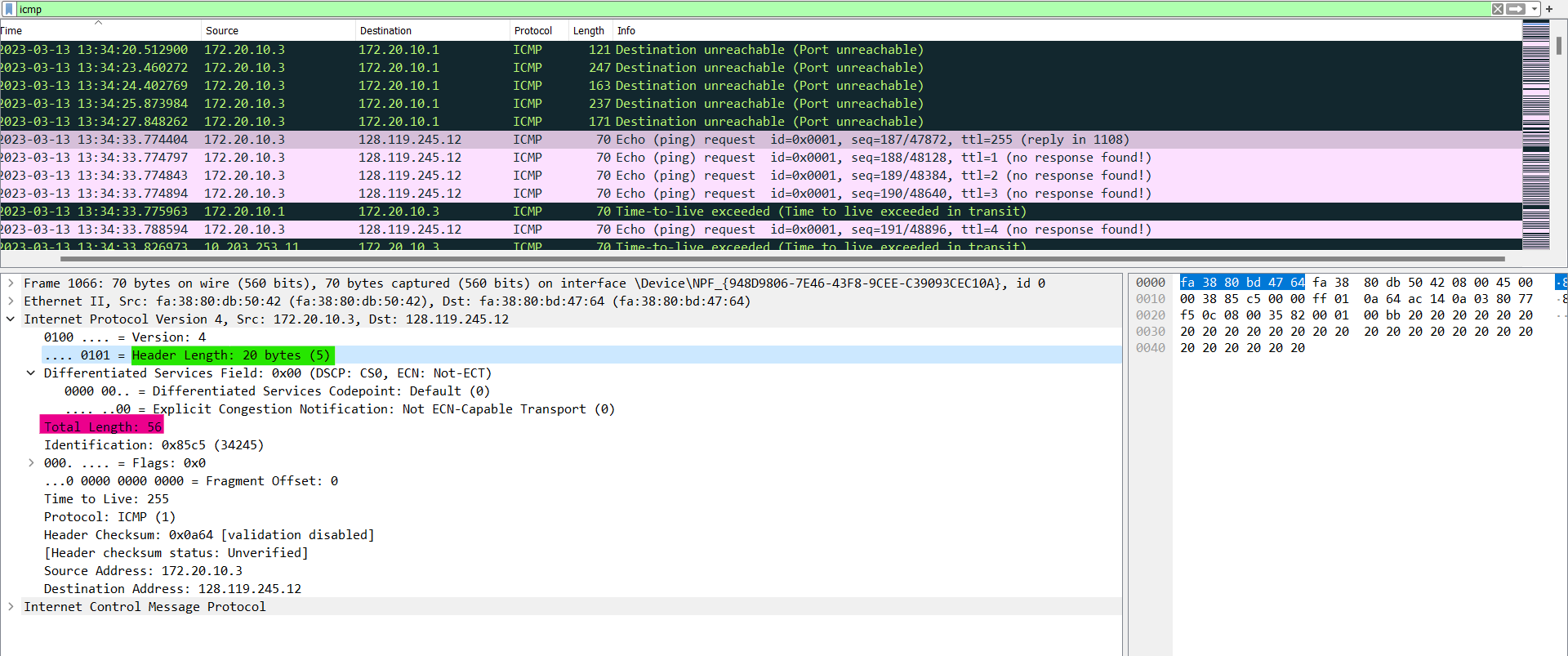


Figure : Capture for Question 3

There are 20 bytes in the IP header and 56 bytes in the total of length, so this give 36 bytes in the payload of the IP datagram.

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

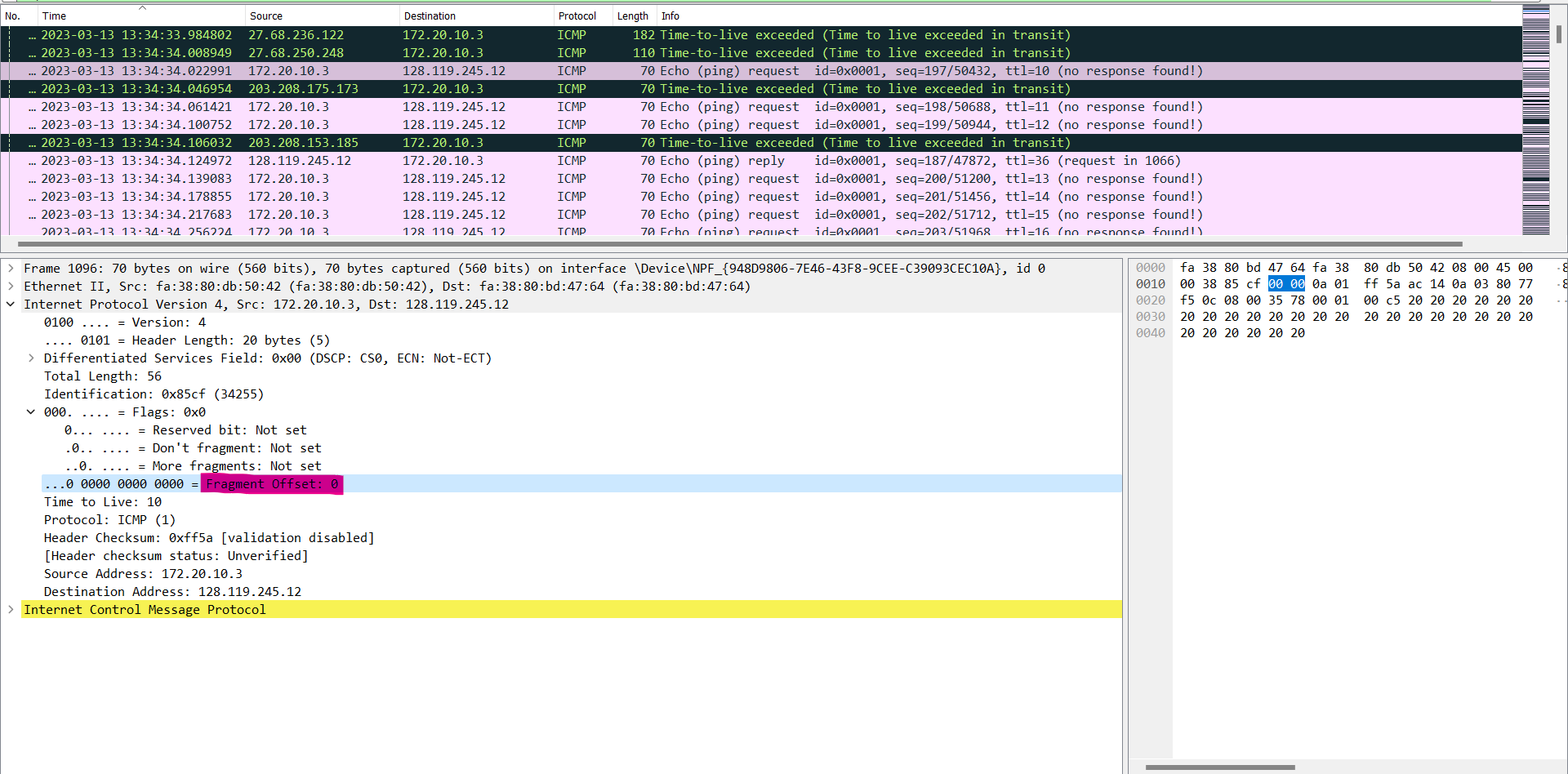


Figure : Capture for Question 4

The fragments bits equal to 0, so the data is not fragmented.

1. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?

Identification, Header Checksum, and Time to Live always change from one datagram to the next.

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

The fields that stay constant across the IP datagrams:

* Version (we are using IPV4 for all packets)
* Header length (cause that is ICMP packets)
* Source IP (we are sending from the same source, in this case, that is my IP address of my computer - 172.20.10.3)
* Destination IP (we are sending to the same destination, in this case, that is [http://gaia.cs.umass.edu](http://gaia.cs.umass.edu/))
* Differentiated Services Field (all the packets are ICMP they use the same Type of Service class)
* Upper Layer Protocol ( cause all of these are ICMP packets)

The fields must stay constant are the same to the fields thay stay constant.

The fields that must be changed are :

* Identification (IP packets must have different ids)
* Time to live (traceroute increments each subsequent packet)
* Header checksum (since header changes, so must be checkum)

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

The pattern of the values in the Identification field increament with each ICMP Echo (ping) request.

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

The Identification : 46110

The TTL : 239

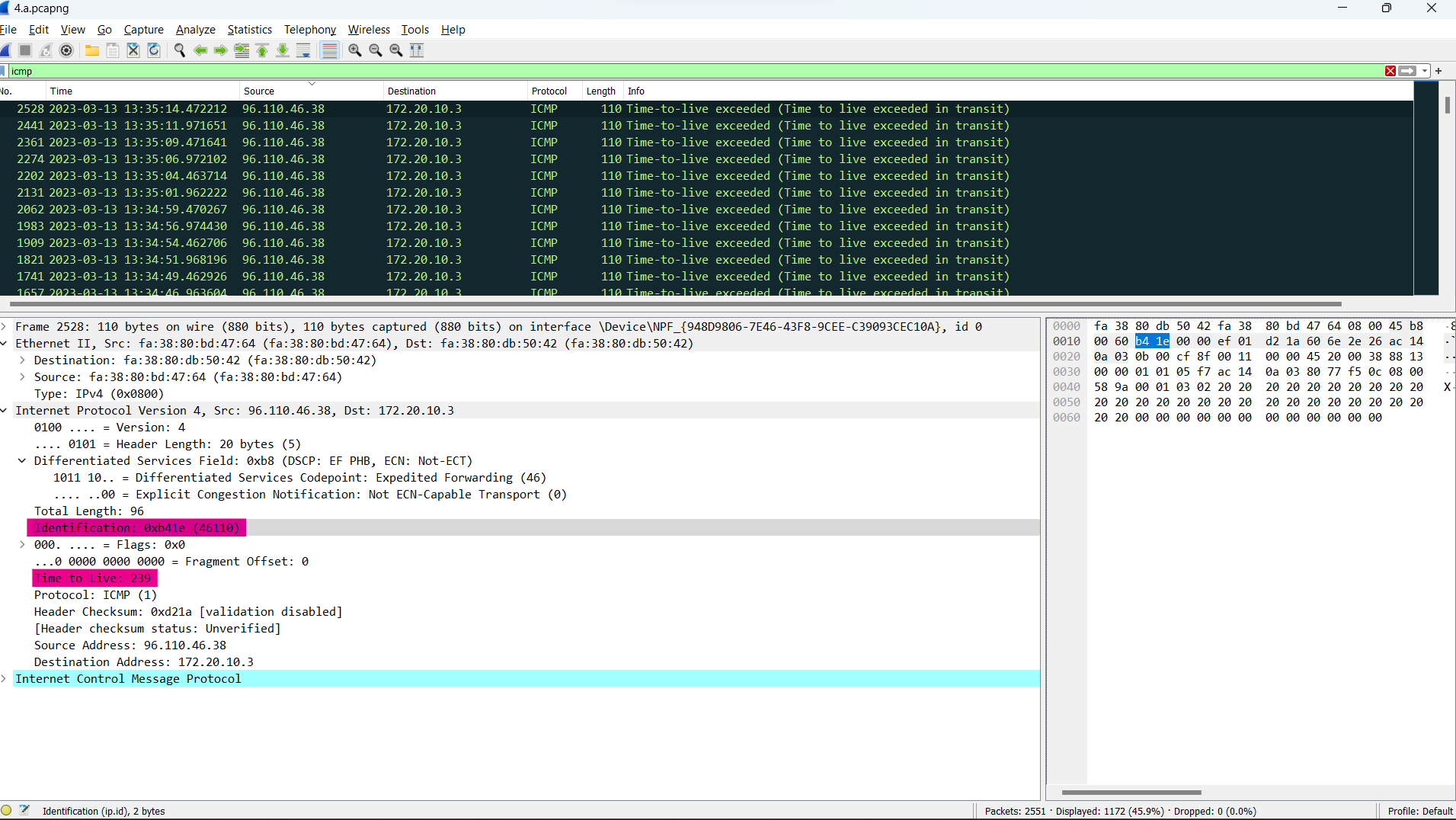


Figure : Capture for Question 8

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

The identification field changes for all the ICMP TTL-exceeded replies sent, because the identification field is a unique value. When two or more IP datagrams have the same identification value, then it means that these IP datagrams are fragments of a single large IP datagram.

Fragmentation

Sort the packet listing according to time again by clicking on the *Time* column.

1. 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?

*[Note: if you find your packet has not been fragmented, you should download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the ipethereal-trace-1packet trace. If your computer has an Ethernet interface, a packet size of 2000 should cause fragmentation.[[1]](#footnote-1)]*

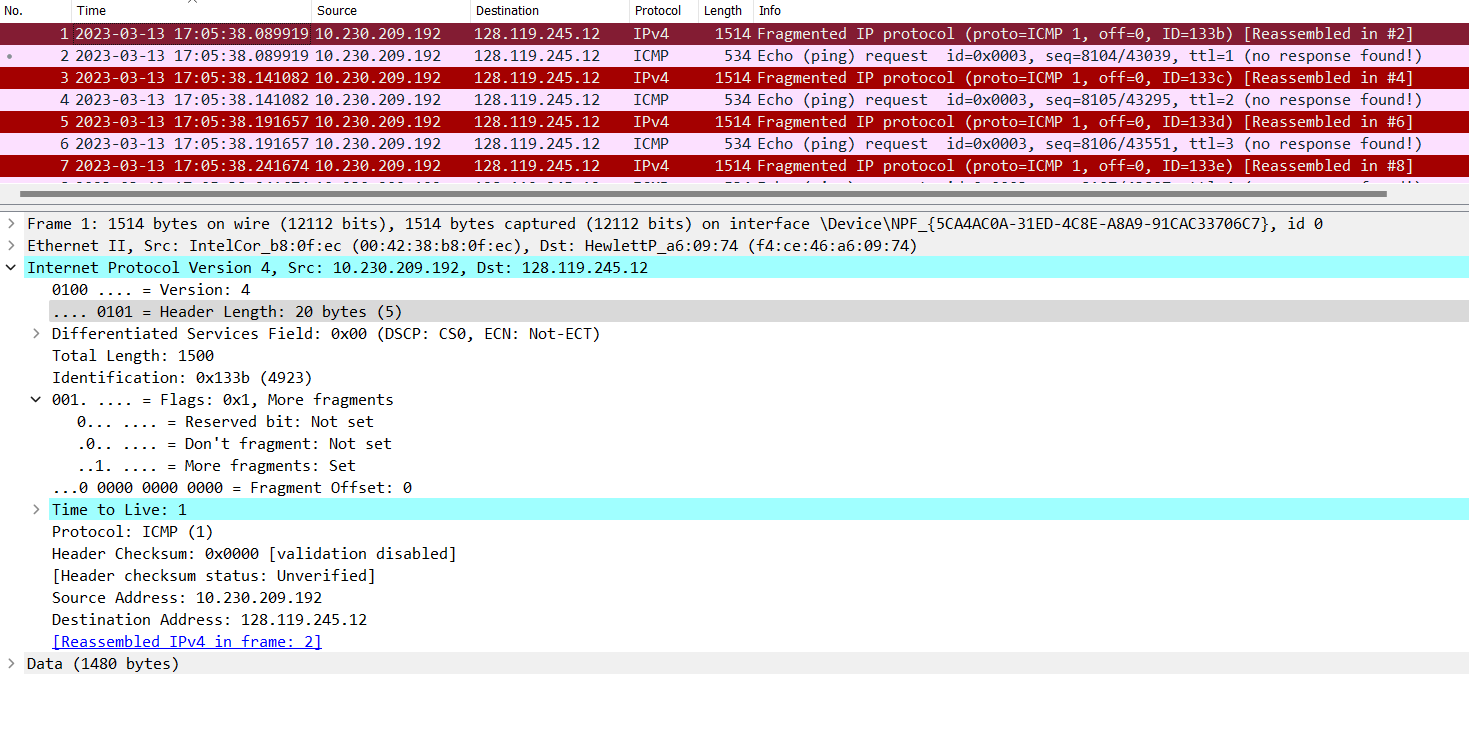


Figure : Packet Size in pingplotter changed to 2000

In this question, I had to change my Wifi, so my IP address (source IP) was changed too.

Ans: Yes, the message has been fragmented across more than one IP datagram.

1. 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?

This datagram‘s Identification is 4293.

The Flags bit for “More fragments” is set (highlight by the green), indicating that the datagram has been fragmented.

The “Fragment Offset” is 0 (highlight by the purple), so that indicate this is first fragment.

This first datagram has total length is 1500 (highlight by the orange), with 20 bytes of Header and 1480 bytes of data.

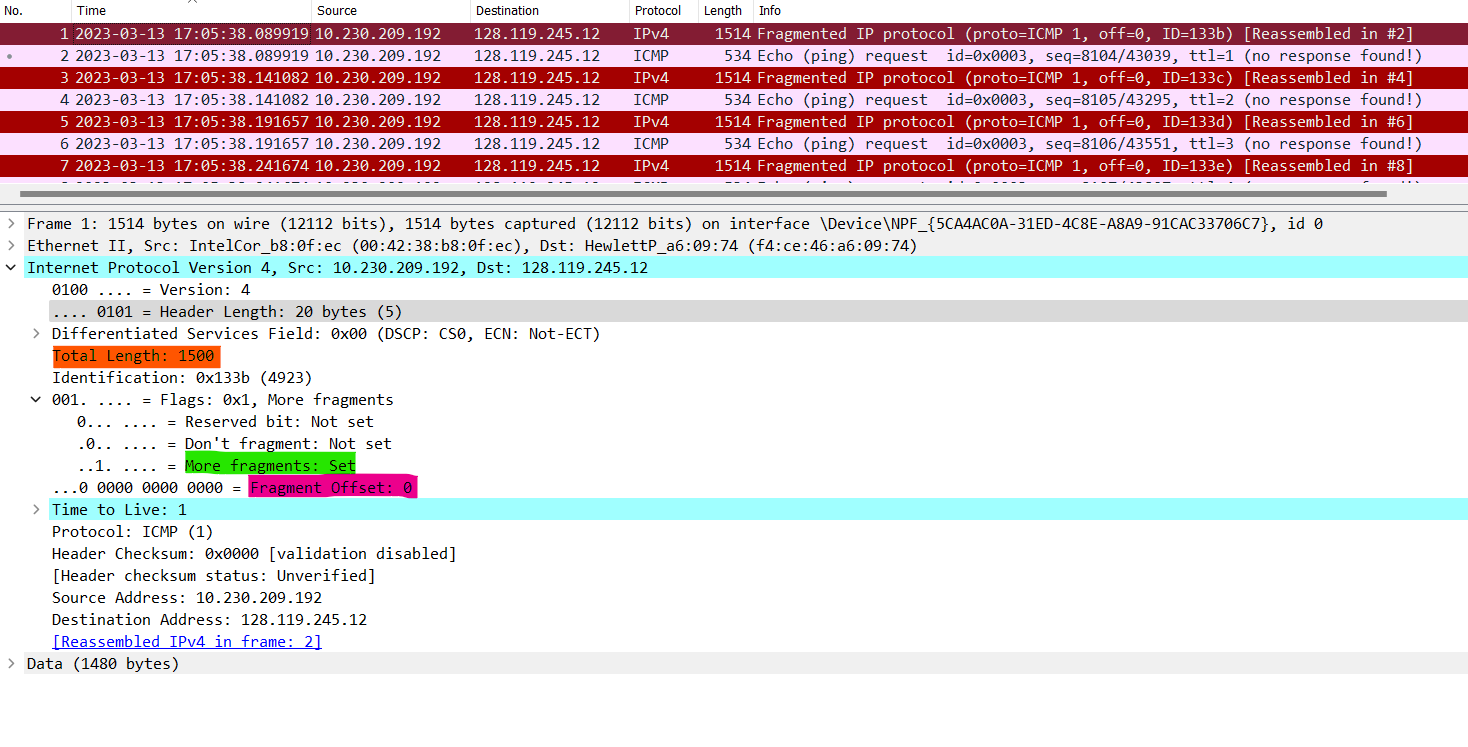


Figure 6:Packet size 2000 - First fragment - Question 11

1. 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?

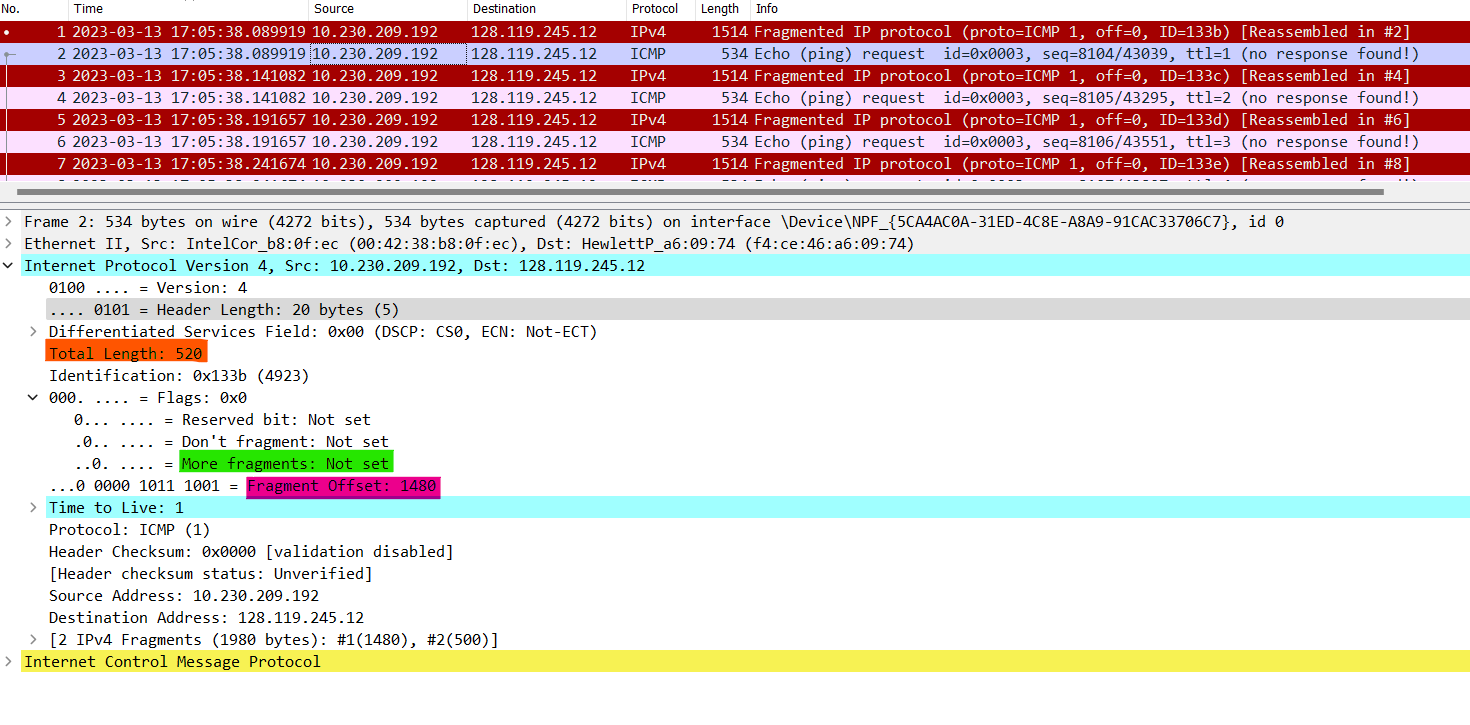


Figure : Packet size 2000 - Second fragment - Question 12

This datagram has the same Identification (4293) as the one in Question 11, so two IP datagrams are fragments of a single large IP datagram.

The Fragment Offset (sign by the purple) is 1480, indicating that this is not the first one. It is the last fragment, since the more fragments flag is not set.

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

The field changes in the IP header between the first and the second fragment:

* Flags bit for “Fragment Offset”: The first one is 0, and the second is 1480.

Now find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 3500.

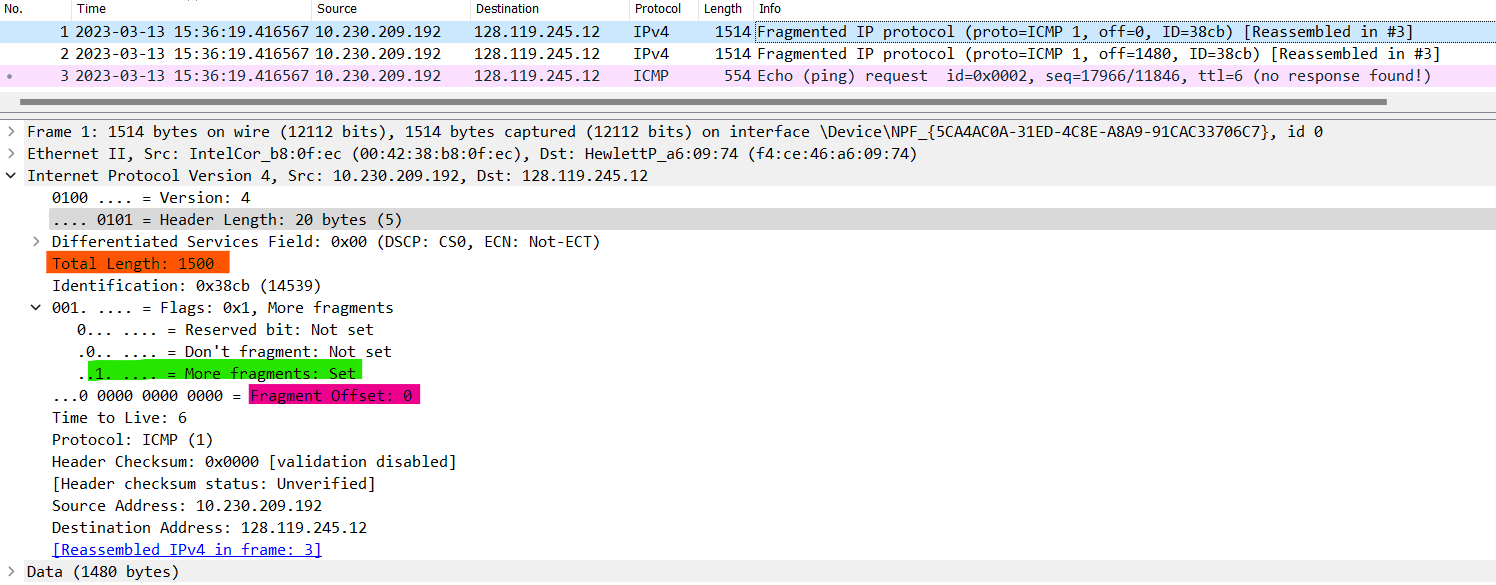


Figure : Packet size 3500 - First fragment

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

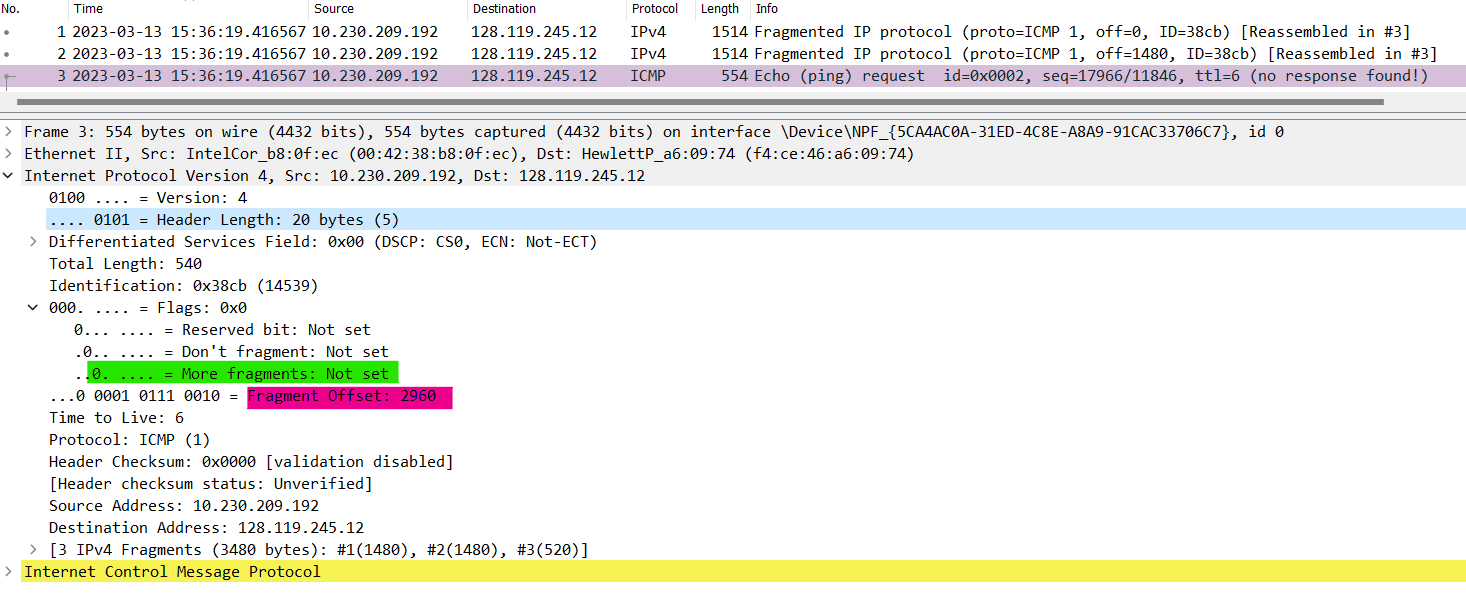


Figure : Packet size 3500 - Last fragment

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

We see only one difference between the first and the second because there are three fragments for the large IP datagram. So it’s just changed the Fragment Offset. But if we compare the first and the last one. Actually, there are three changes: the *Fragment Offset*, the *Total length*, and the flags bit for *More fragments*.

You can see the difference beetwen *Figure 8* in Question 13 and *Figure 9* in Question 14 to make it clear.

1. [↑](#footnote-ref-1)