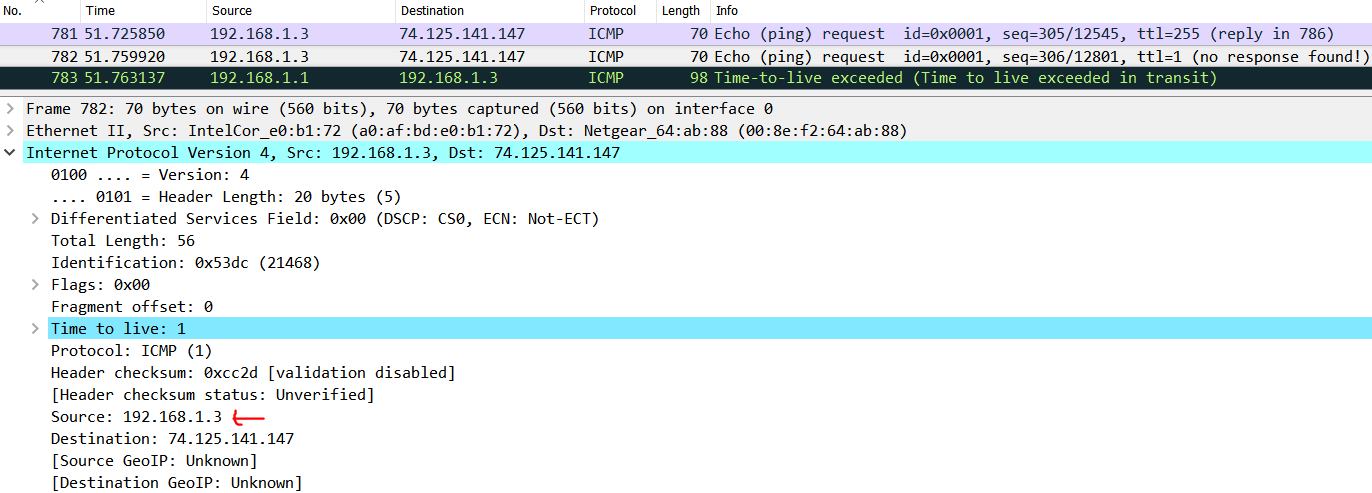
**Wireshark Lab – Assignment 2**

Sarveshwaran Sampathkumar - 017387654

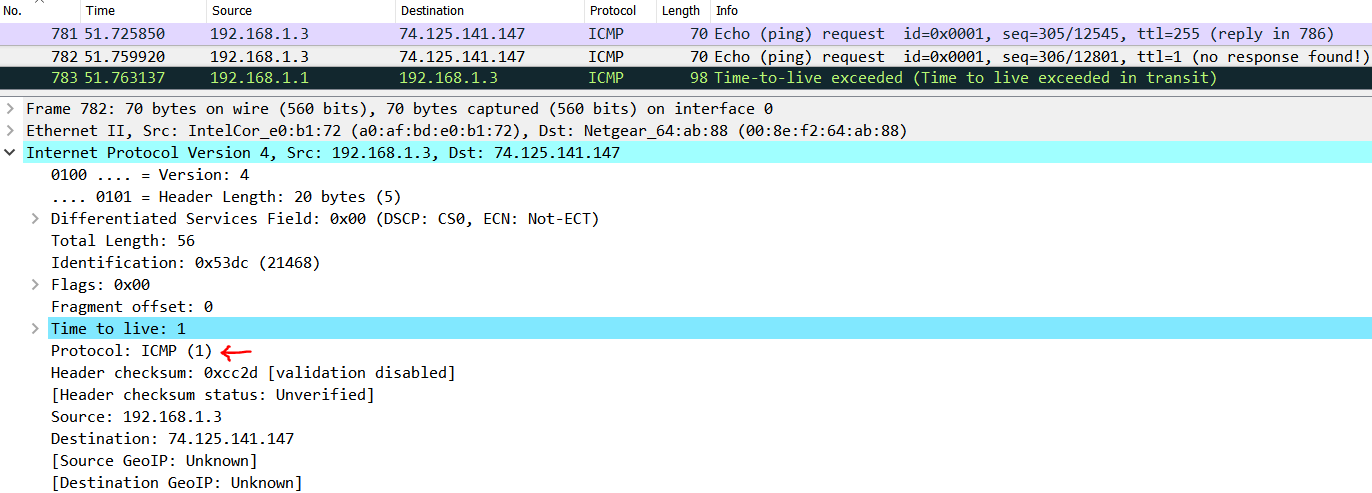
*1. Select the first ICMP Echo Request message sent by your computer and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?*

IP Address: 192.168.1.3



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

Protocol: ICMP (1)

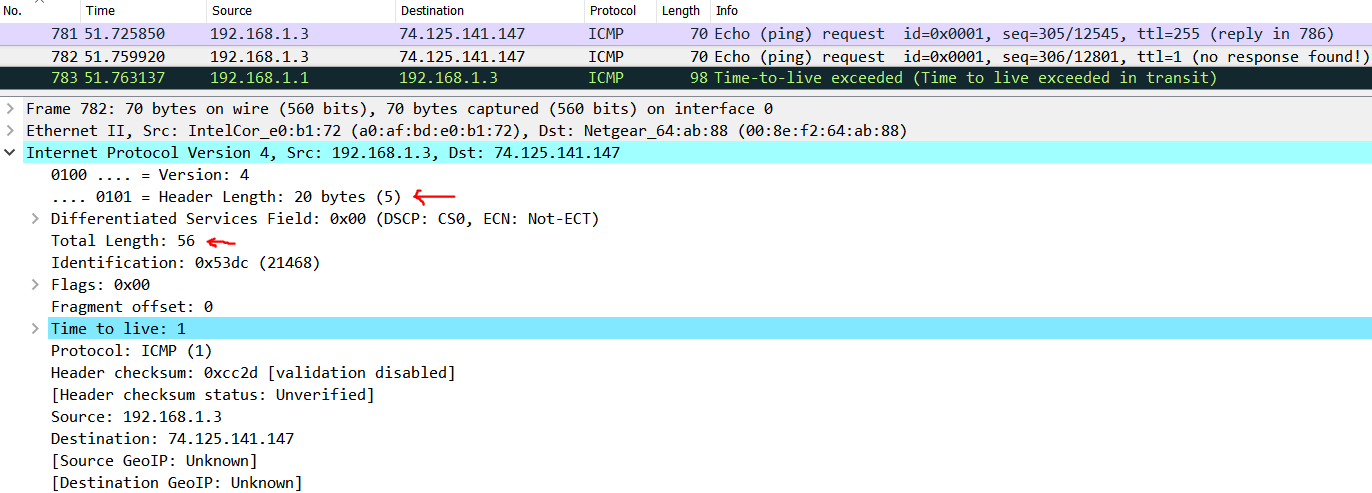


*3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.*

Bytes in the IP header: 20

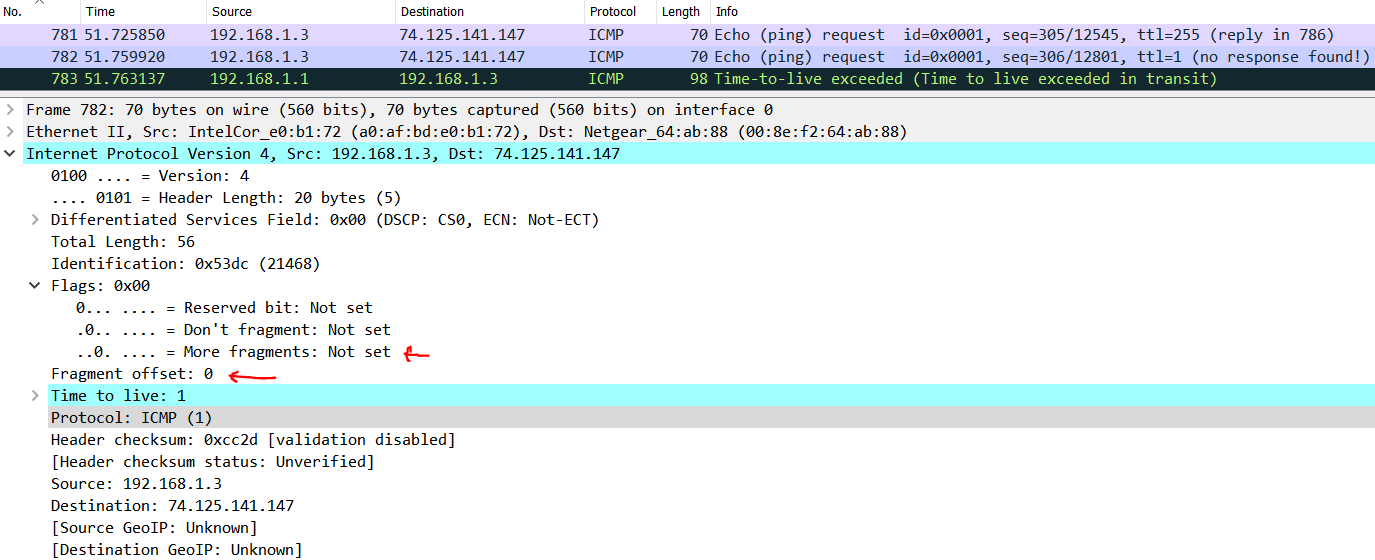
Bytes in the payload of the IP datagram: 36

Explanation: We can see that the total length as 56 Bytes. Out of which 20 Bytes are for the IP header. Hence, we can calculate the value of the payload by subtracting the IP header size from the total length. That is 56-20 = 36 Bytes



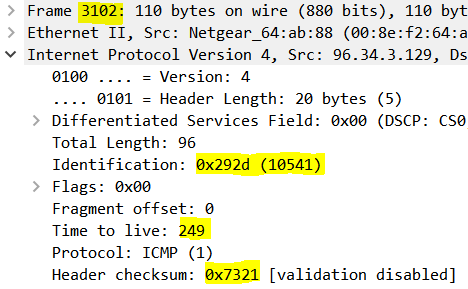
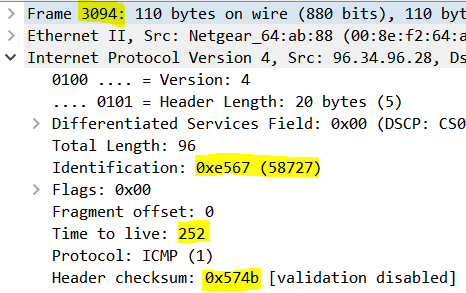
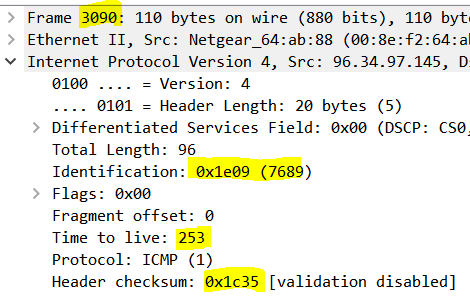
*4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.*

On expanding the flags section, we can see that the value of “More Fragments” is set to “Not Set” which indicates that this is the last fragment. Additionally, we can also see that the value of “Fragment Offset” is set to 0 which is the case for the first fragment. On combining these two we can conclude that this datagram is not fragmented.



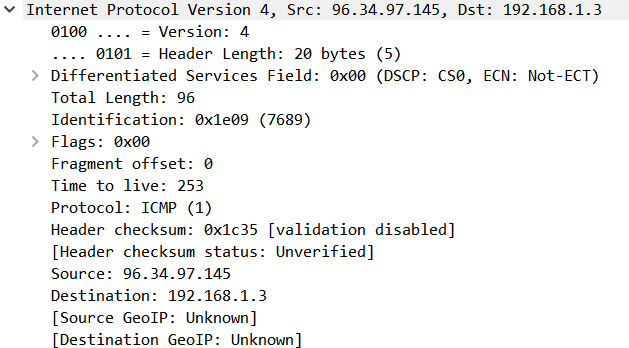
*5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?*

On analysing a series of ICMP messages sent by our computer, we can see that fields such as Frame, Identification, Time to live and Header checksum keeps changing.



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

From the below set of fields we can identify the fields which are supposed to stay constant and the fields which must change



Fields which should stay constant and must stay constant:

* Version – Here it is 4
* Header Length – Here it is 20
* Differentiated Services Field
* Protocol – Here it is ICMP (1)
* Source IP Address
* Destination IP Address

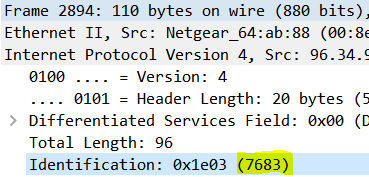
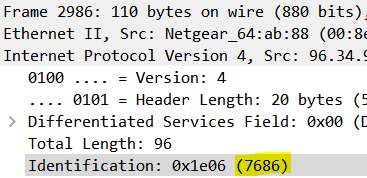
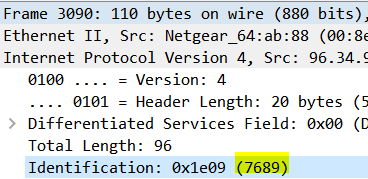
Fields which must change:

* Identification – Here it is 0x1e09. Since this field is used to identify the IP packets uniquely, this is supposed to be unique. Hence, the value of this field should change
* Time to live – Here it is 253. This value is updated by traceroute.
* Header Checksum – The value of the checksum is based on the header information. Since each header has its unique information, the checksum is also supposed to be unique. Hence, this field should change.

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

The values in the Identification field of the IP datagram decreases per datagram (when the entries are filtered to contain only ICMP messages and sorted based on Source IP)

Frame – 3090, 2986, 2894, …………..

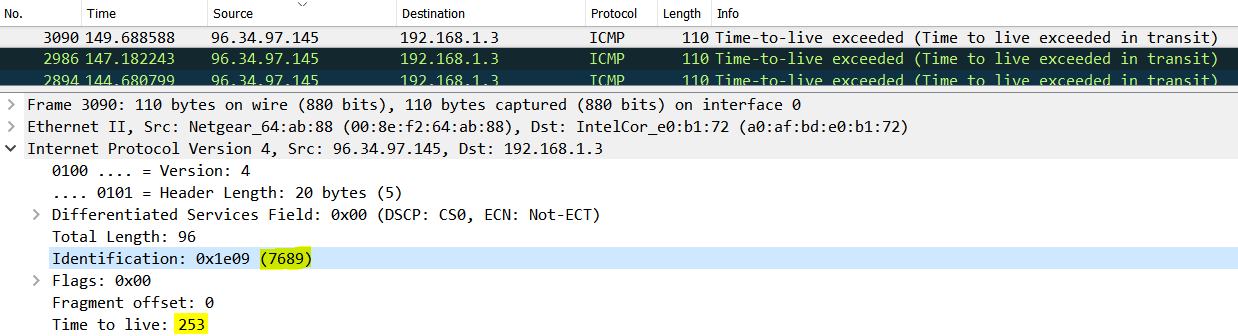


*Next (with the packets still sorted by source address) find the series of ICMP TTL exceeded replies sent to your computer by the nearest (first hop) router.*

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

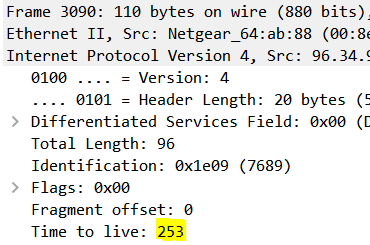
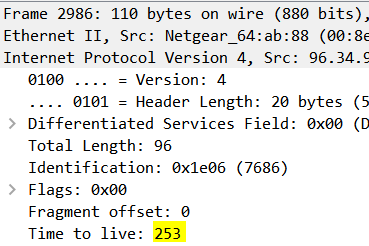
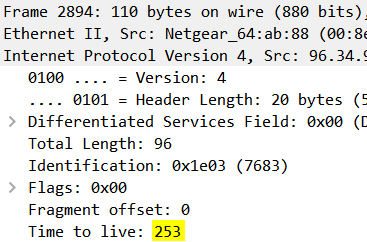
Value of the Identification field: ox1e09 (7689)

Value of the Time to live field: 253



*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?*

Considering the source to be 96.34.97.145, we can see that the TTL value remains constant (253) but the value of the identification field changes. This is because, identification field is used to identify the IP packets uniquely and hence this is supposed to be unique.

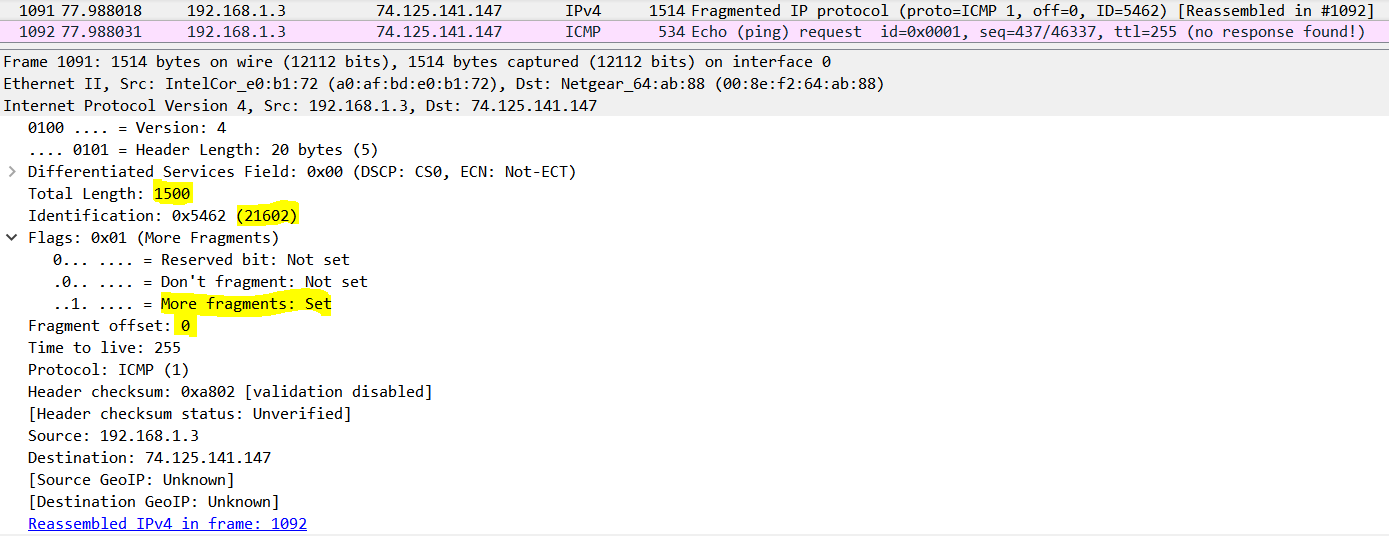
  

*10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?*

Consider the below two frames:

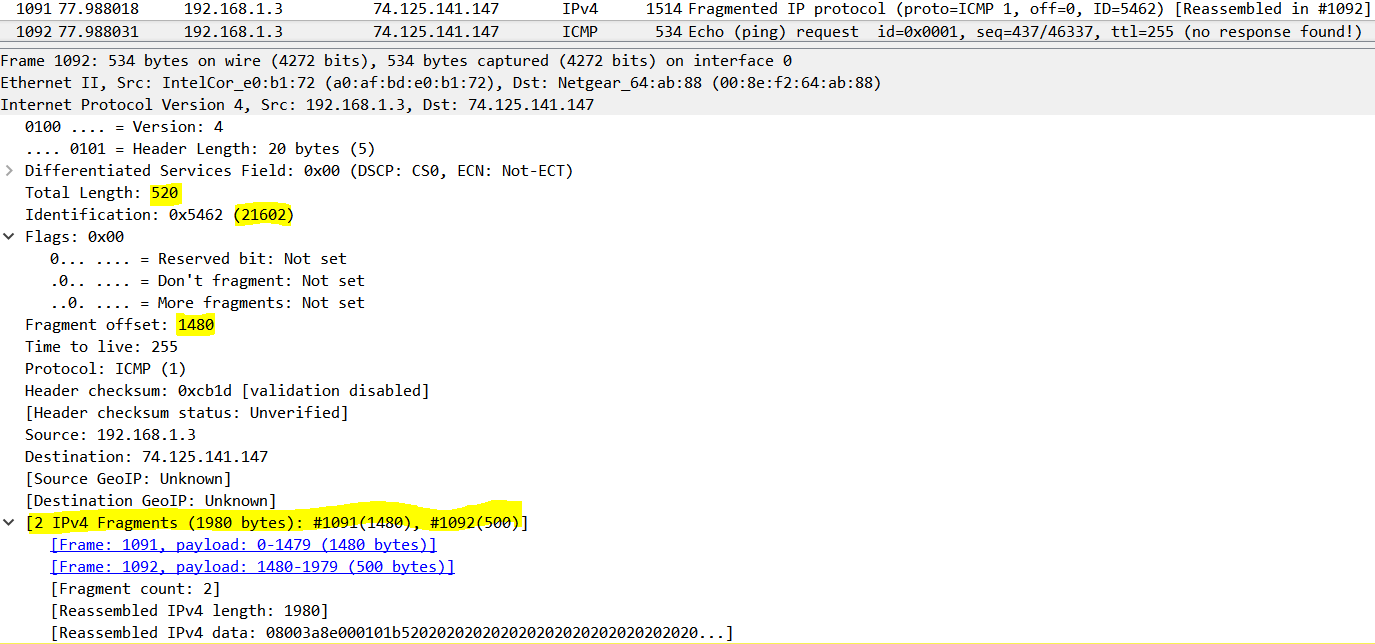
Frame: 1091

We can see that the total length here is 1500 and the identification is 21602. The flag “More Fragments” is set to “Set”, meaning there are more fragments available.



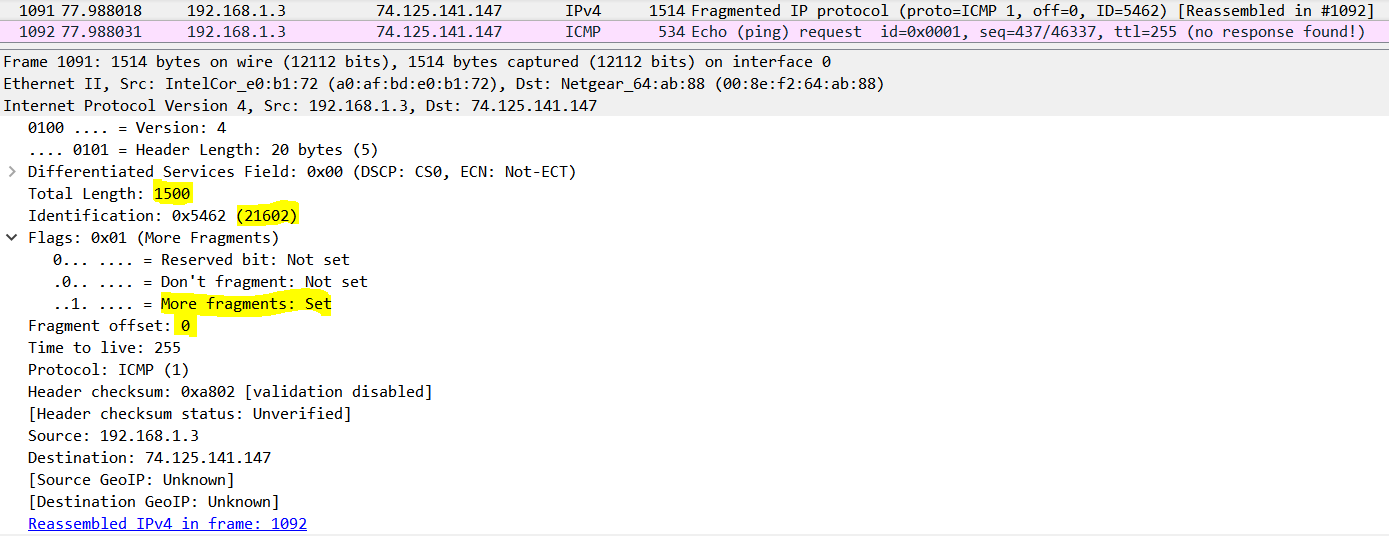
Frame: 1092

Here the identification- 21602, is same as the above, showing that the data is being fragmented. “Fragment Offset” flag along with “More fragments” flag confirms the same.



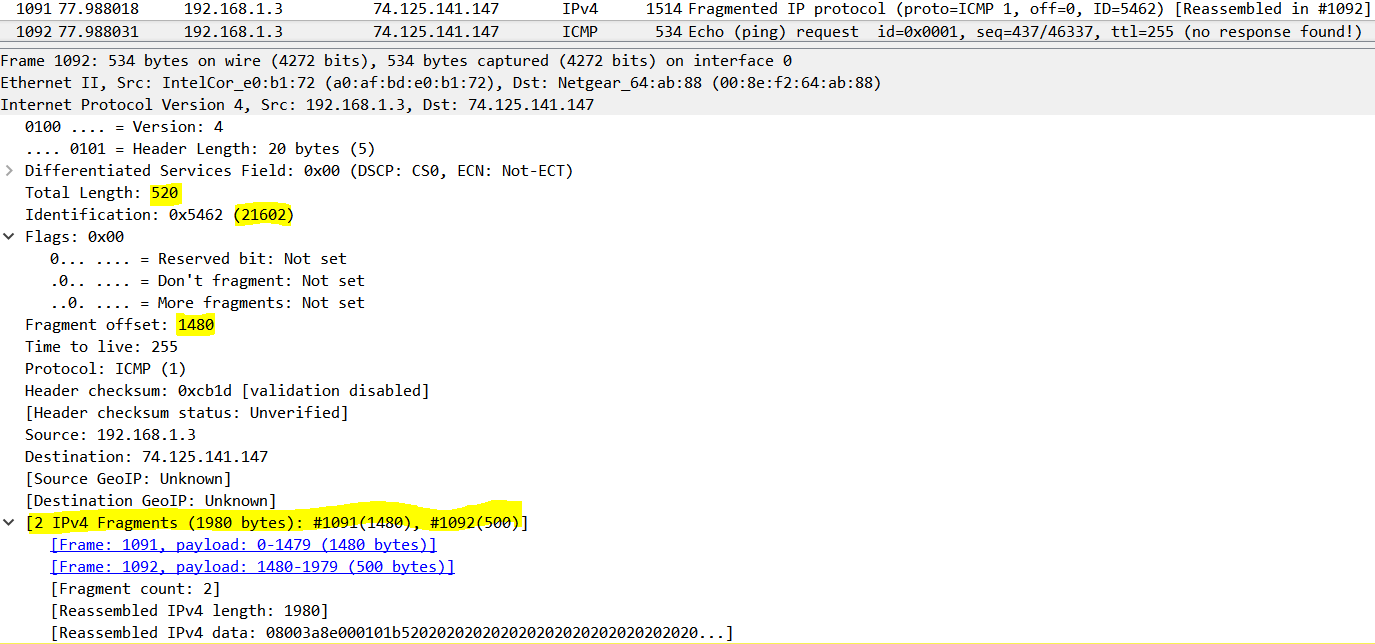
*11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?*

* The flag “More Fragments” in first frame is set to “Set”, meaning there are more fragments available
* The flag “Fragment Offset” is set to 0 which indicates that this is the first fragment.
* Frame 1091 contains 1480 bytes



*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?*

* The flag “Fragment Offset” is set to 1480 which indicates that this is not the first fragment.
* No. There are no more fragments. The flag “More Fragments” in second frame is set to “Not Set”, meaning there are no more fragments available.
* The total IP datagram is 1980 bytes. Frame 1091 contains 1480 bytes and Frame 1092 contains 500 bytes. This information is seen in Frame 1092 (highlighted below)



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

The fields which changes between first and second fragment are

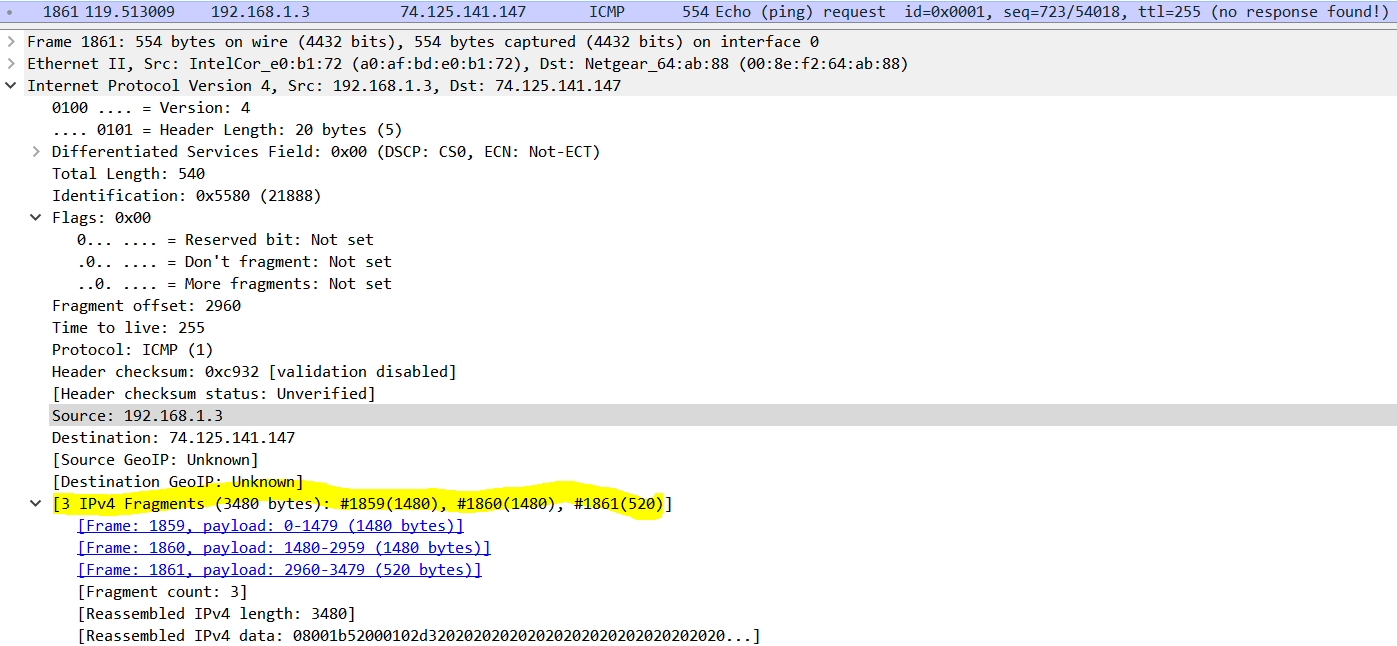
1. Total length
2. Flag – More Fragments
3. Fragment Offset
4. Header Checksum

*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.*

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

There are three fragments which are created from the original datagram.

* Frame 1859
* Frame 1860
* Frame 1861



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

The fields which change among those fragments are as follows

1. Total Length (Same for first two frames – 1500, For third frame it is 540)
2. Flag – “More Fragments” (Same for first two frames. Flag is set to – “Set”, For third frame it is set to “Not Set”)
3. Flag – “Fragment Offset”
4. Header Checksum

