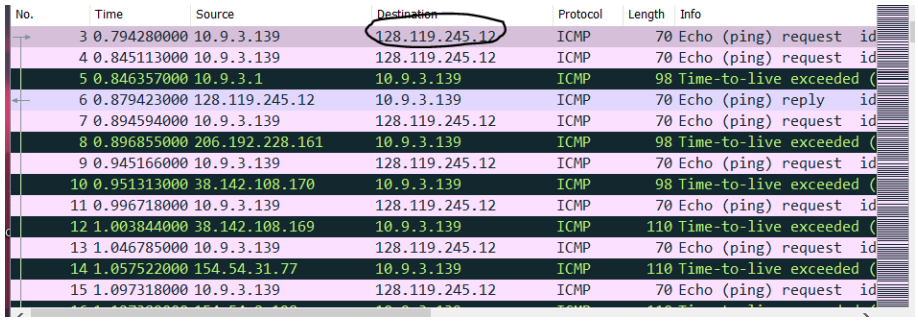
Gretel Rajamoney

5-20-2021

Wireshark Lab 4

Note: Sharing a computer with a peer due to Wireshark issues, the TA stated that it was a Wireshark issue and told me I could utilize another laptop and leave a note for the grader.

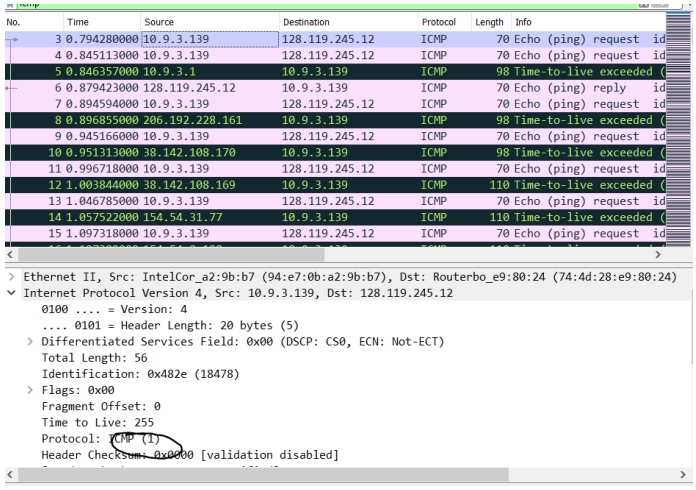
1. What is the IP address of your computer?



No.	Time	Source	Destination	Protocol	Length	Info
3	0.794280000	10.9.3.139	128.119.245.12	ICMP	70	Echo (ping) request id
4	0.845113000	10.9.3.139	128.119.245.12	ICMP	70	Echo (ping) request id
5	0.846357000	10.9.3.1	10.9.3.139	ICMP	98	Time-to-live exceeded (
6	0.879423000	128.119.245.12	10.9.3.139	ICMP	70	Echo (ping) reply id
7	0.894594000	10.9.3.139	128.119.245.12	ICMP	70	Echo (ping) request id
8	0.896855000	206.192.228.161	10.9.3.139	ICMP	98	Time-to-live exceeded (
9	0.945166000	10.9.3.139	128.119.245.12	ICMP	70	Echo (ping) request id
10	0.951313000	38.142.108.170	10.9.3.139	ICMP	98	Time-to-live exceeded (
11	0.996718000	10.9.3.139	128.119.245.12	ICMP	70	Echo (ping) request id
12	1.003844000	38.142.108.169	10.9.3.139	ICMP	110	Time-to-live exceeded (
13	1.046785000	10.9.3.139	128.119.245.12	ICMP	70	Echo (ping) request id
14	1.057522000	154.54.31.77	10.9.3.139	ICMP	110	Time-to-live exceeded (
15	1.097318000	10.9.3.139	128.119.245.12	ICMP	70	Echo (ping) request id

Computer IP Address: 128.119.245.12

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

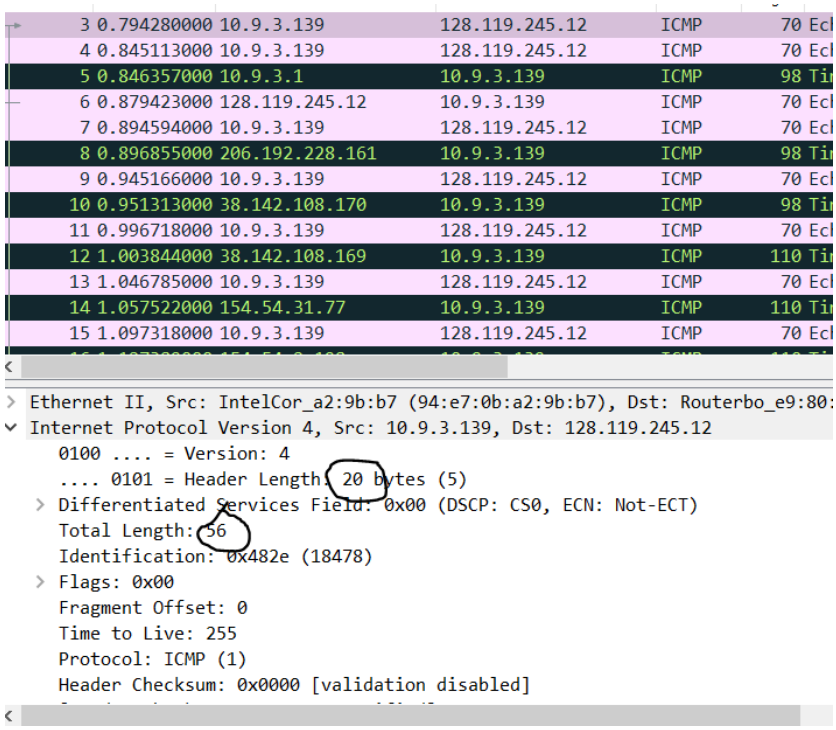


No.	Time	Source	Destination	Protocol	Length	Info
3	0.794280000	10.9.3.139	128.119.245.12	ICMP	70	Echo (ping) request id
4	0.845113000	10.9.3.139	128.119.245.12	ICMP	70	Echo (ping) request id
5	0.846357000	10.9.3.1	10.9.3.139	ICMP	98	Time-to-live exceeded (
6	0.879423000	128.119.245.12	10.9.3.139	ICMP	70	Echo (ping) reply id
7	0.894594000	10.9.3.139	128.119.245.12	ICMP	70	Echo (ping) request id
8	0.896855000	206.192.228.161	10.9.3.139	ICMP	98	Time-to-live exceeded (
9	0.945166000	10.9.3.139	128.119.245.12	ICMP	70	Echo (ping) request id
10	0.951313000	38.142.108.170	10.9.3.139	ICMP	98	Time-to-live exceeded (
11	0.996718000	10.9.3.139	128.119.245.12	ICMP	70	Echo (ping) request id
12	1.003844000	38.142.108.169	10.9.3.139	ICMP	110	Time-to-live exceeded (
13	1.046785000	10.9.3.139	128.119.245.12	ICMP	70	Echo (ping) request id
14	1.057522000	154.54.31.77	10.9.3.139	ICMP	110	Time-to-live exceeded (
15	1.097318000	10.9.3.139	128.119.245.12	ICMP	70	Echo (ping) request id

```
> Ethernet II, Src: IntelCor_a2:9b:b7 (94:e7:0b:a2:9b:b7), Dst: Routerbo_e9:80:24 (74:4d:28:e9:80:24)
v Internet Protocol Version 4, Src: 10.9.3.139, 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: 0x482e (18478)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
```

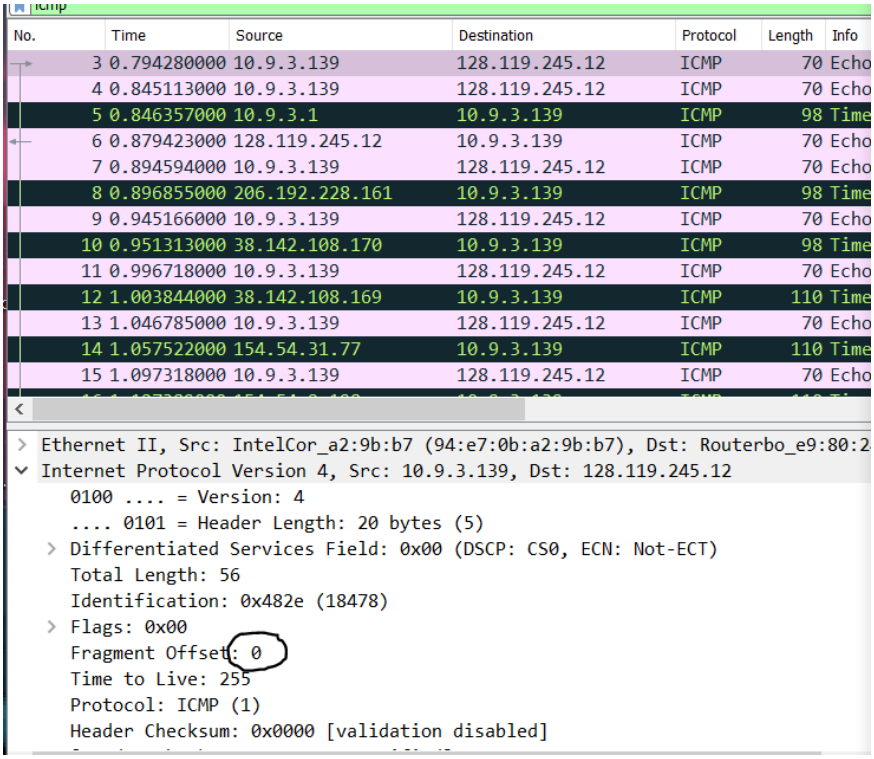
Upper Layer Protocol Field Value: ICMP 1

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.



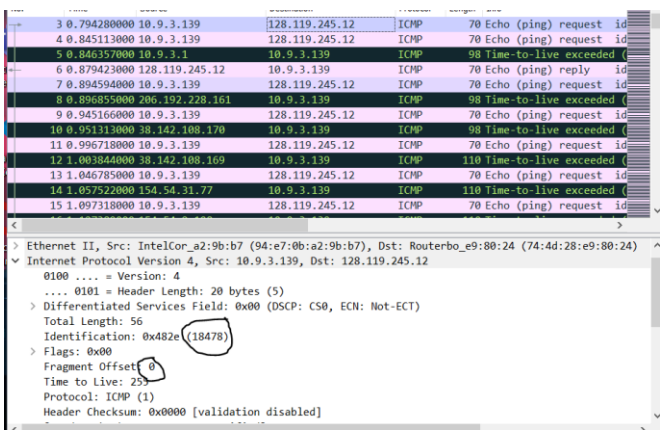
There are 20 bytes in the IP header, 56 bytes in the total length, which means that there are 36 bytes in the payload of the IP datagram because 56 – 20 is 36.

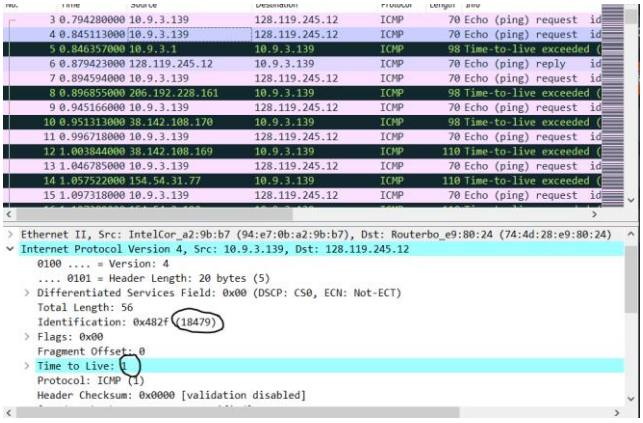
4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.



The fragment offsets a value of 0, which means that the 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?



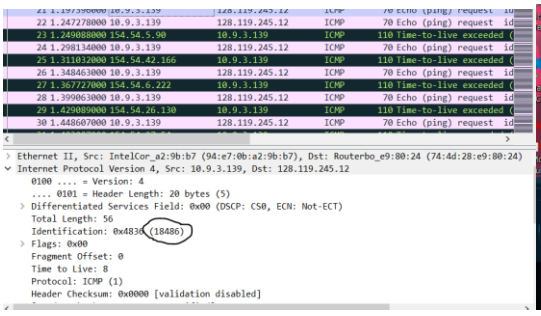


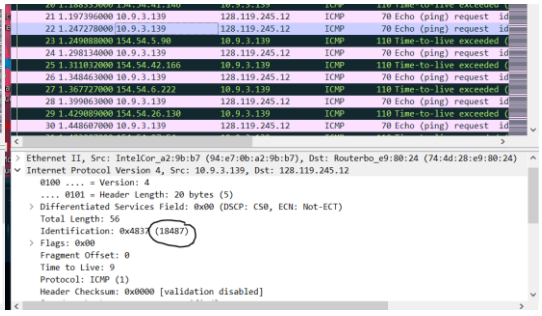
The Identification and the Fragment Offset both increase by one, as you can see in the first image the fragment offset is 1 and the identification is 18478, but in the second image the identification is 18479.

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

   The fields that must stay constant at the length of the header, the source IP, the destination IP, the upper layer protocol, and the version. The length of the header stays constant because the size will not change, the source IP stays constant because you are sending from the same place, the destination IP stays constant because you are sending to the same place, the upper layer protocol stays constant because you always use the ICMP, lastly the version remains at a constant at version 4. Lastly the fields that must change are the identification and the header checksum. The header checksum must change because the header also changes, and the identification must change in order to verify packets.

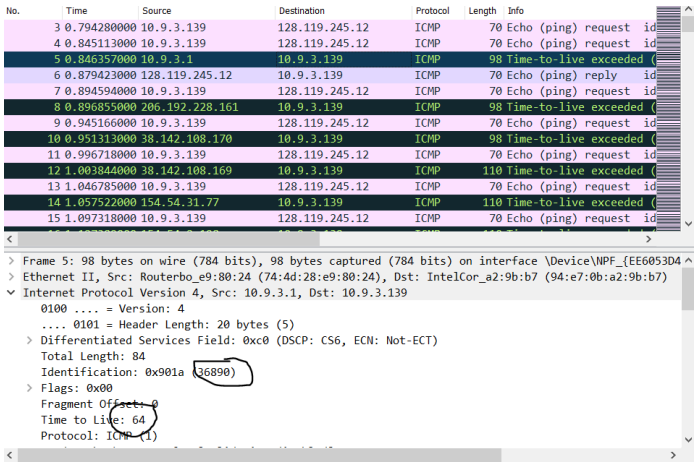
7. Describe the pattern you see in the values in the Identification field of the IP datagram.





In the first image the identification is 18486, in the second image the identification is 18487. The pattern is that the identification increases by one in each strand.

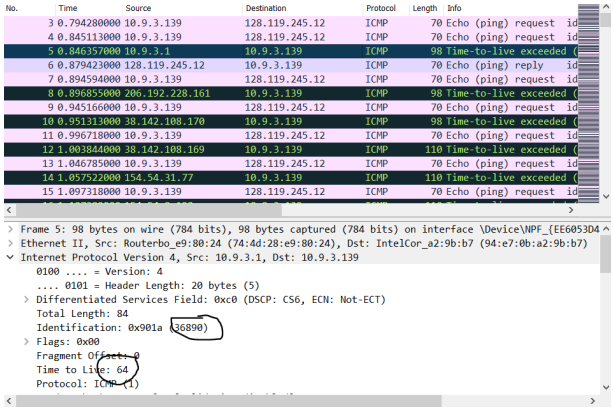
8. What is the value in the Identification field and the TTL field?



Identification Field: 36890

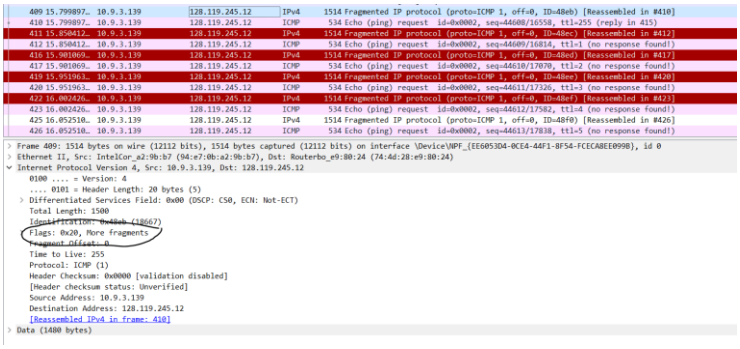
TTL Field: 64

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?



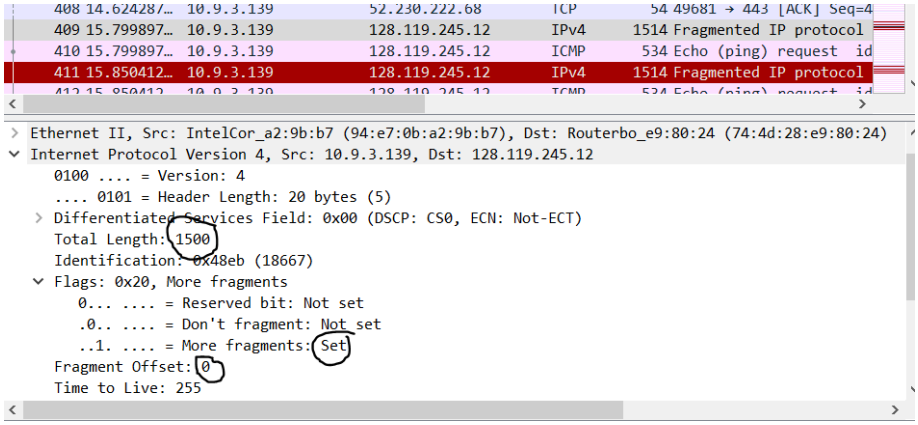
Since the identification has to have a unique value each time, this field changes. In the case that there are replied with the same value, the replies must be considered fragments of a bigger packet. The time to live length also remains unchanged because the time to live to the first hop router is always the same regardless.

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?



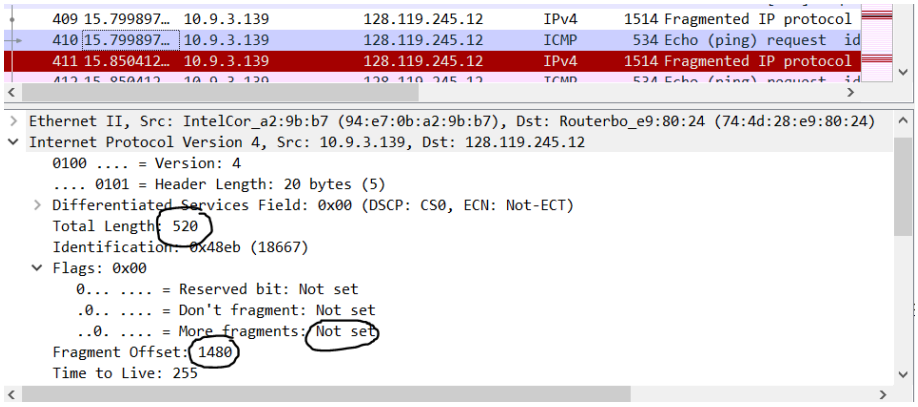
The message has been fragmented across more than one IP datagram because the flag stating “more fragments” has been set.

11. Screenshot the first fragment of the fragmented IP datagram. What information in the IP header indicated 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?



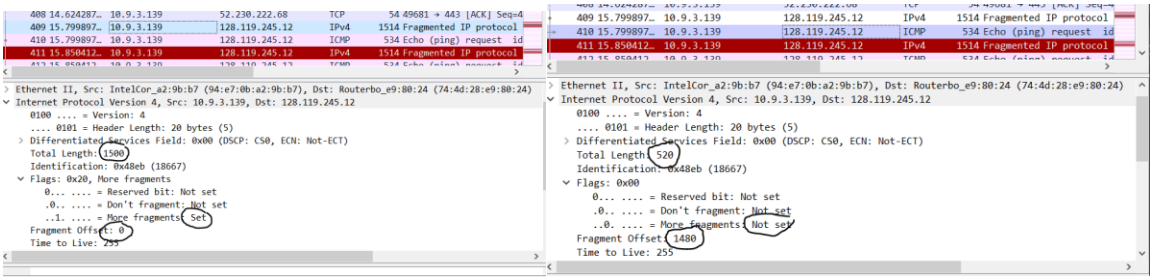
Since the flag stating more fragments has been set, we know that the datagram has been fragmented. Since the fragment offset has been set to a value of 0, we can confirm that this is the first fragment and not a latter fragment. The IP datagram has a total length of 1500 bytes.

12. Screenshot the second fragment of the fragmented IP datagram. What information in the IP header indicated that this is not the first datagram fragment? Are there more fragments? How can you tell?



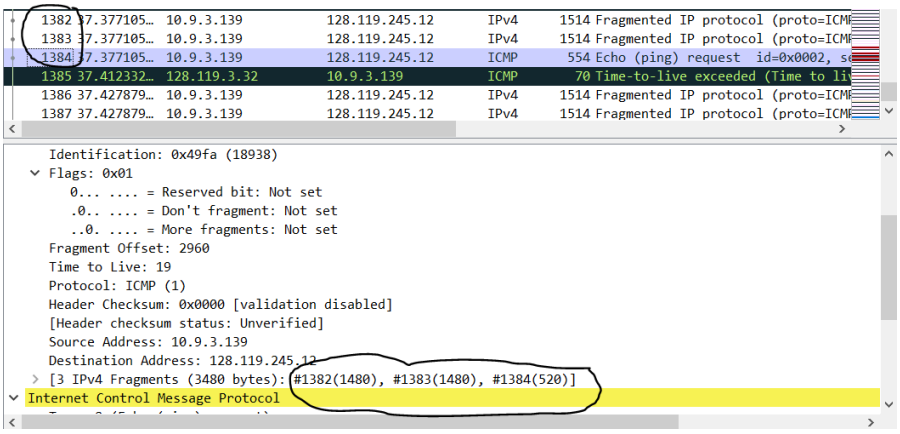
The flag stating more fragments has not been set, therefore we know that there are no more fragments. The fragment offset in this has a value of 1480 as oppose to 0. Finally, the total length of the IP datagram is 520 bytes instead of 1500 bytes.

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



The fields that have been changed between the first and the second fragments are the total length has changes from 1500 bytes to 520 bytes, the more fragments flag has been set in the first fragment but not set in the second fragment, and the fragment offset in the first fragment is 0 and in the second fragment is 1480.

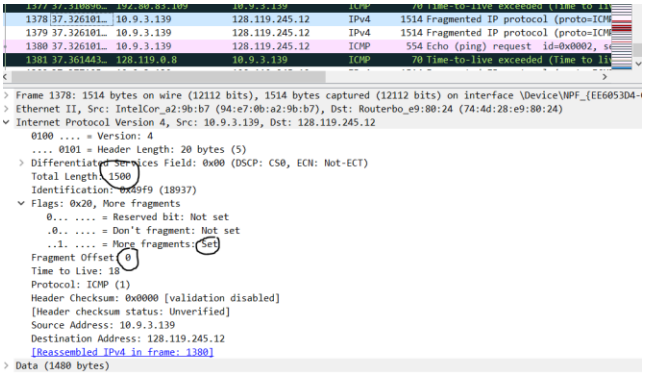
14. How many fragments were created from the original datagram?



There were three fragments created when switching to 3500 bytes.

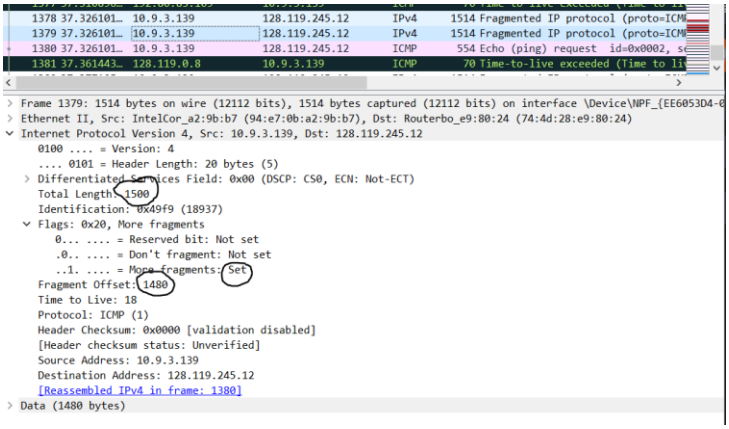
15. What fields change in the IP header among the fragments?

First Fragment:



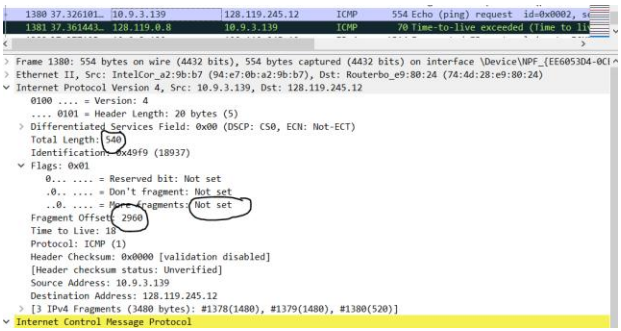
The total length of the first fragment is 1500 bytes, the more fragments flag has been set, and lastly the fragment offset of the first fragment is 0 bytes.

Second Fragment:



The total length of the second fragment is 1500 bytes, the more fragments flag has been set, and lastly the fragment offset of the second fragment is 1480 bytes.

Third Fragment:



The total length of the third fragment is 540 bytes, the more fragments flag has not been set, and lastly the fragment offset of the third fragment is 2960 bytes

The difference between all three fragments is the fragment offset values. Both the first and second fragments have a total length of 1500 bytes, meanwhile the third fragment only has a length of 540 bytes. Both the first and second fragments also have their flags set meaning that they have been fragmented across more than one IP datagram. Meanwhile the third fragment does not have a flag set meaning that is has not been fragmented across more than one IP datagram.