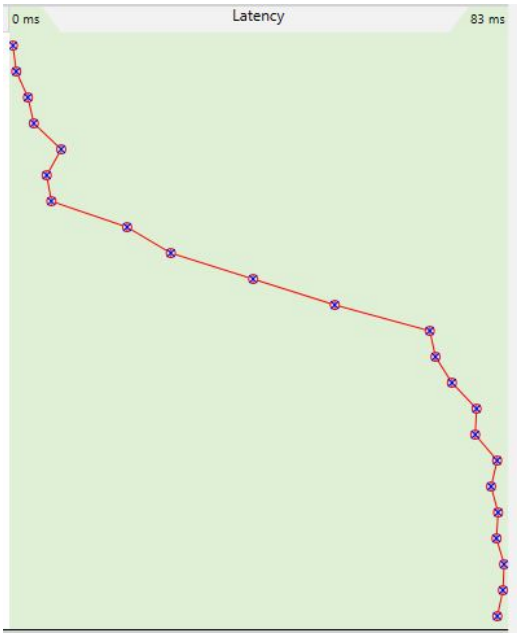
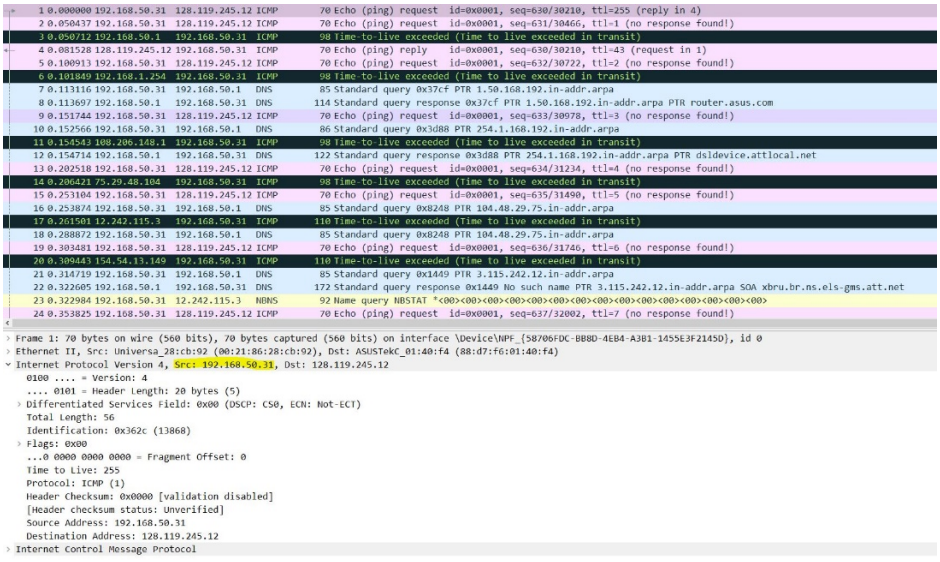
Using the 56-byte packet-size ping capture data

1. Provide a screenshot of pingplotter tracing graph for 56-byte packet size.



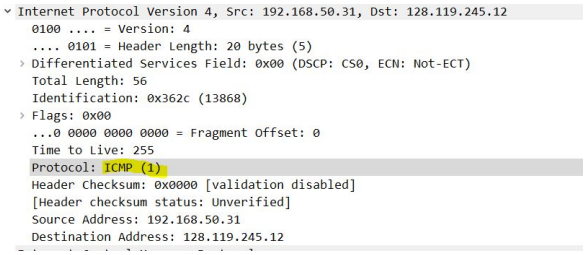
2. In Wireshark, select the first ICMP Echo Request message sent by your computer and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer? Provide relevant screenshot to illustrate and support your answer.

The IP address of my computer is 192.168.50.31.



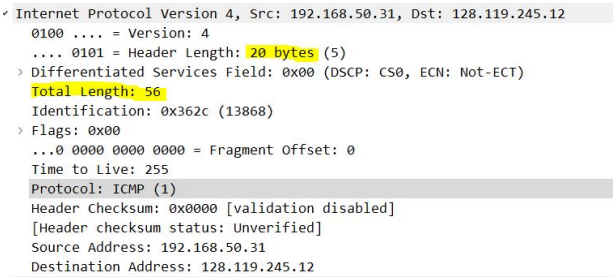
3. Within the IP packet header, what is the value in the upper layer protocol field? Provide screenshot(s) to illustrate and support your answer.

ICMP (1)



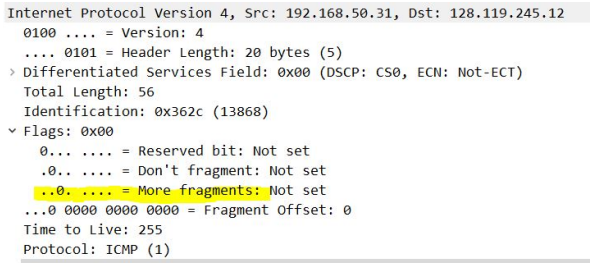
4. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes. Provide screen-shot(s) to illustrate and support your answer.

The IP header 20 bytes. Payload header bytes is the total length minus the IP header bytes which is 56-20 which is 36 bytes.



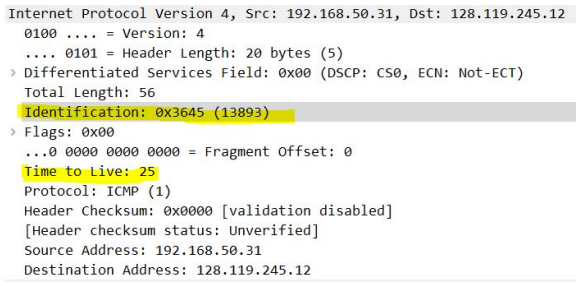
5. Has this IP datagram been fragmented? Explain how you determined whether the data-gram has been fragmented. Provide screenshot(s) to illustrate and support your answer.

The IP datagram has not been fragmented because the more fragments bit = 0 so the data is not fragmented.



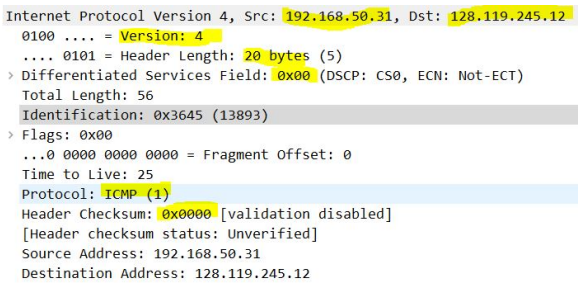
6. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer? Provide screenshot(s) to illustrate and support your answer.

The identification field and the time to live is always changing.

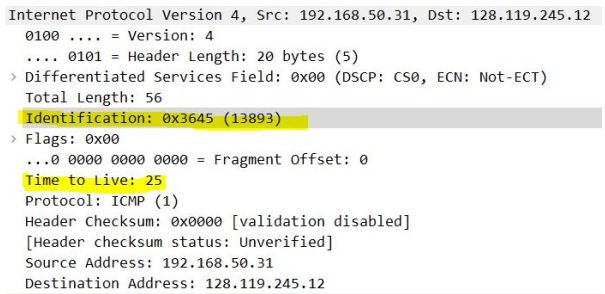


7. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why? Provide screenshot(s) to illustrate and support your answer.

The fields that stay constant and must stay constant are version since we are using version IPv4, header length since we are using IPv4, source IP since my computers IP doesn't change, destination IP since we are sending to the same host, differentiated services since we are sending to the same protocol every time, upper layer protocol since it is the same protocol every time, header checksum since validation is disabled.

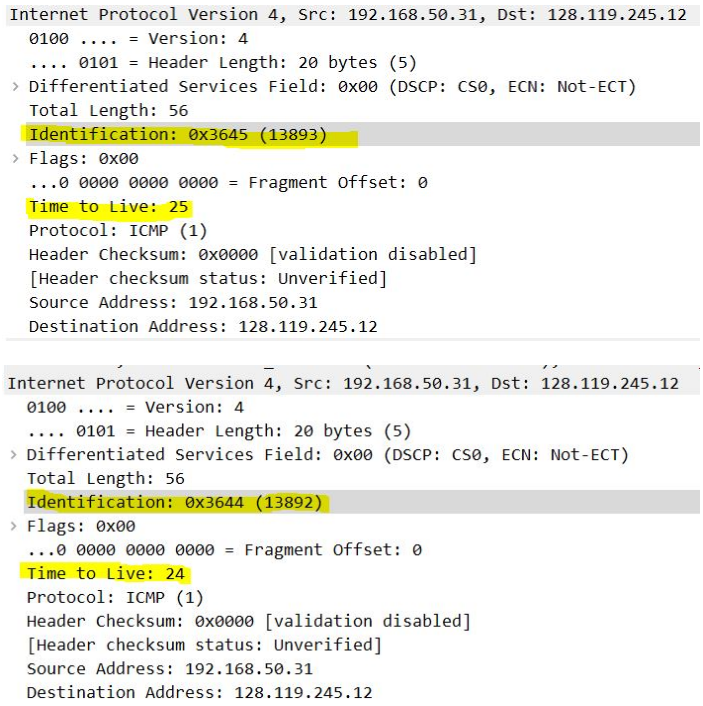


The fields that must change are the Identification field since each IP datagram has a different ID and the time to live since that is how trace routing works.



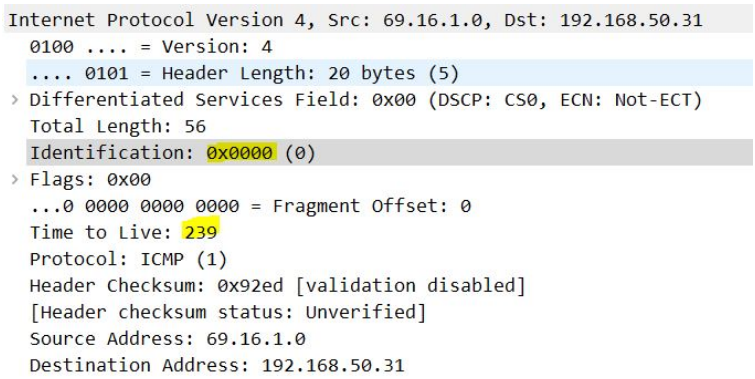
8. Describe the pattern you see in the values in the Identification field of the IP datagram. Provide screenshot(s) to illustrate and support your answer.

The identification field is only incrementing by one at every request for example the first request is 13892 the second request is 13893.



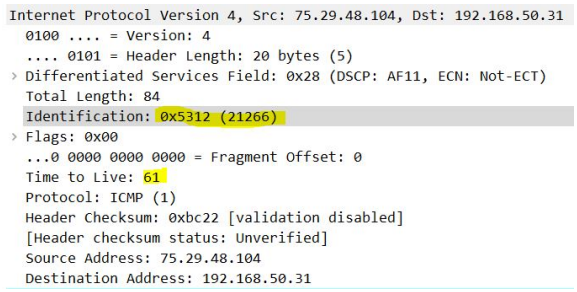
9. What is the value in the Identification field and the TTL field? Provide screenshot(s) to illustrate and support your answer.

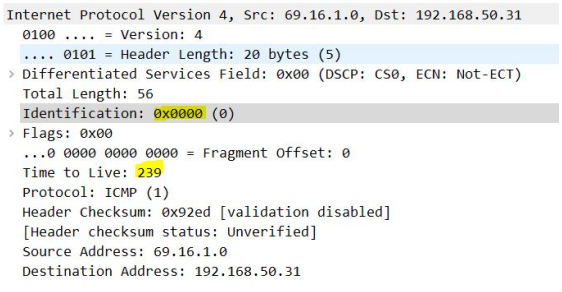
The Identification value is 0 and the time to live value is 239.

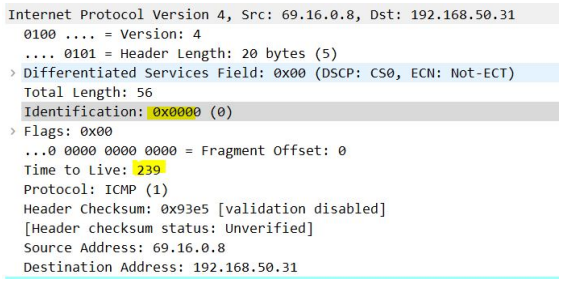


10. Do these values remain unchanged for all the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why? Provide screenshot(s) to illustrate and support your answer.

The values of the identification field for all the ICMP TTL-exceeded replies do change since the identification field is a unique value. If two or more IP datagrams have the same identification value its because those IP datagrams are fragments to one large IP datagram.

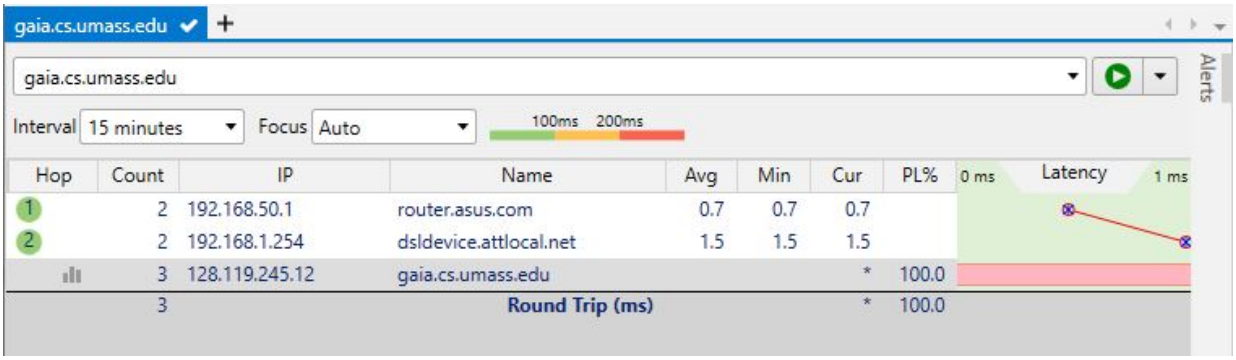






Using the 2000-byte packet-size ping capture data

11. Provide a screenshot of pingplotter tracing graph for 2000-byte packet size.



12. In Wireshark, 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? Explain how you determined whether the datagram has been fragmented. Provide screenshot(s) to illustrate and support your answer.

Yes, it has been fragments across two IP datagrams. It has been fragmented because it provides a fragment field.

```
Internet Protocol Version 4, Src: 192.168.50.31, 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: 520
  Identification: 0x397e (14718)
> Flags: 0x00
  ...0 0101 1100 1000 = Fragment Offset: 1480
  Time to Live: 255
  Protocol: ICMP (1)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.50.31
  Destination Address: 128.119.245.12
v [2 IPv4 Fragments (1980 bytes): #9(1480), #10(500)]
    [Frame: 9, payload: 0-1479 (1480 bytes)]
    [Frame: 10, payload: 1480-1979 (500 bytes)]
    [Fragment count: 2]
    [Reassembled IPv4 length: 1980]
    [Reassembled IPv4 data: 08003559000106ea2020202020202020202020202020202020202020202020202020202020…]
```

13. From 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? Provide screenshot(s) to illustrate and support your answer.

I turned off the Resembled fragment IPv4 Datagrams for this. In the Flags it shows a bit is set indicating the datagram has been fragmented and there are more fragments. And the fragment offset is zero meaning it is the first fragment. The IP datagram is 1500 bytes.

14. From 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? Provide screenshot(s) to illustrate and support your answer.

From the fragmented IP datagram, the fragment offset is 1480 meaning it is the total offset. The reason we know this is the total is because there are no more fragments as well according to the more fragments bit not being set.

```
Internet Protocol Version 4, Src: 192.168.50.31, 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: 520
  Identification: 0x397e (14718)
v Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  ...0 0101 1100 1000 = Fragment Offset: 1480
  Time to Live: 255
  Protocol: ICMP (1)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.50.31
  Destination Address: 128.119.245.12
```

15. What fields change in the IP header between the first and second fragment? Provide screenshot(s) to illustrate and support your answer.

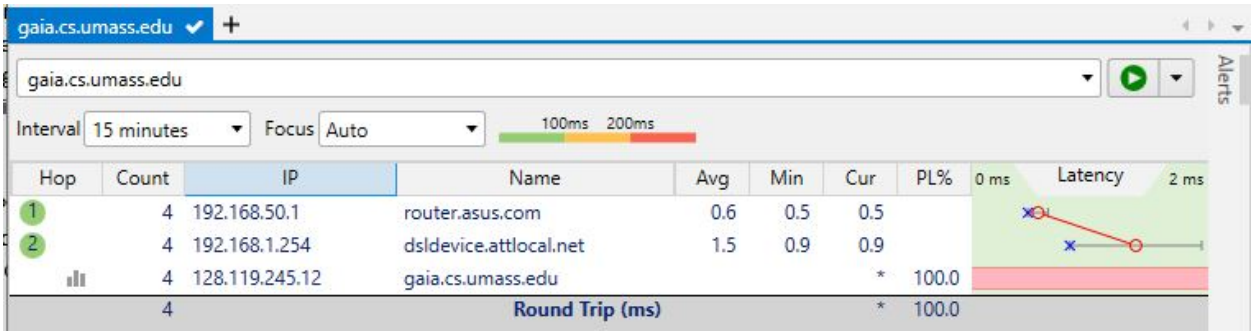
The total length, the more fragments bit, and fragment offset.

```
Internet Protocol Version 4, Src: 192.168.50.31, 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: 0x397e (14718)
v Flags: 0x20, More fragments
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..1. .... = More fragments: Set
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 255
  Protocol: ICMP (1)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.50.31
  Destination Address: 128.119.245.12
```

```
Internet Protocol Version 4, Src: 192.168.50.31, 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: 520
  Identification: 0x397e (14718)
v Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  ...0 0101 1100 1000 = Fragment Offset: 1480
  Time to Live: 255
  Protocol: ICMP (1)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.50.31
  Destination Address: 128.119.245.12
```

Using the 3500-byte packet-size ping capture data

16. Provide a screenshot of pingplotter tracing graph for 3500-byte packet size.



17. In Wireshark, how many fragments were created from the original datagram? Provide screenshot(s) to illustrate and support your answer.

There were 3 packets created from the original datagram.

```
2 0.273528 192.168.50.31  128.119.245.12 ICMP      15… Echo (ping) request  id=0x0001, seq=2082/8712, ttl=255 (no response found!)
3 0.273528 192.168.50.31  128.119.245.12 IPv4      15… Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3aa2)
4 0.273528 192.168.50.31  128.119.245.12 IPv4      554 Fragmented IP protocol (proto=ICMP 1, off=2960, ID=3aa2)
```

18. What fields change in the IP header among the fragments? Provide screenshot(s) to illustrate and support your answer.

The fields that change in the IP header are the total length, fragment offset, and flags.

```
Internet Protocol Version 4, Src: 192.168.50.31, 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: 0x3aa2 (15010)
v Flags: 0x20, More fragments
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..1. .... = More fragments: Set
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 255
  Protocol: ICMP (1)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.50.31
  Destination Address: 128.119.245.12
```

```
Internet Protocol Version 4, Src: 192.168.50.31, 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: 0x3aa2 (15010)
v Flags: 0x20, More fragments
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..1. .... = More fragments: Set
  ...0 0101 1100 1000 = Fragment Offset: 1480
  Time to Live: 255
  Protocol: ICMP (1)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.50.31
  Destination Address: 128.119.245.12
```

```
Internet Protocol Version 4, Src: 192.168.50.31, 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: 540
  Identification: 0x3aa2 (15010)
v Flags: 0x01
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  ...0 1011 1001 0000 = Fragment Offset: 2960
  Time to Live: 255
  Protocol: ICMP (1)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.50.31
  Destination Address: 128.119.245.12
```