BAYANI, Femo Steven Felicisimo

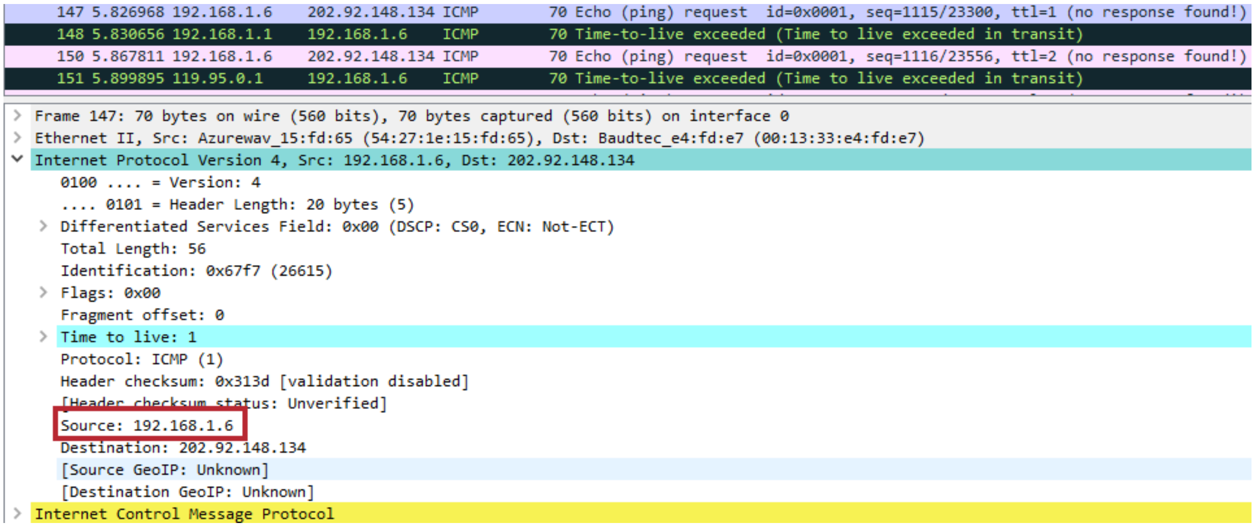
2015-07104

Wireshark Lab 8: IP

CMSC 138

1. Select the first UDP segment sent by your computer that is part of the traceroute and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

The IP address of my computer is **192.168.1.6**.

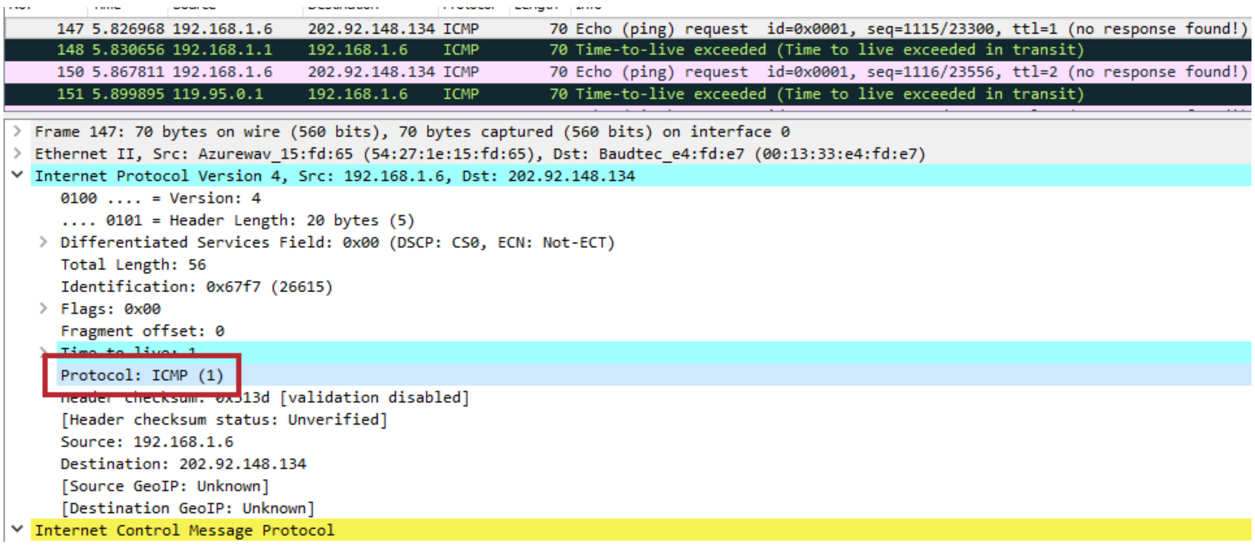


```
147 5.826968 192.168.1.6    202.92.148.134 ICMP     70 Echo (ping) request  id=0x0001, seq=1115/23300, ttl=1 (no response found!)
148 5.830656 192.168.1.1    192.168.1.6    ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
150 5.867811 192.168.1.6    202.92.148.134 ICMP     70 Echo (ping) request  id=0x0001, seq=1116/23556, ttl=2 (no response found!)
151 5.899895 119.95.0.1     192.168.1.6    ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)

> Frame 147: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: Azurewav_15:fd:65 (54:27:1e:15:fd:65), Dst: Baudtec_e4:fd:e7 (00:13:33:e4:fd:e7)
v Internet Protocol Version 4, Src: 192.168.1.6, Dst: 202.92.148.134
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x67f7 (26615)
  > Flags: 0x00
    Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x313d [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.6
    Destination: 202.92.148.134
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
> Internet Control Message Protocol
```

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

The upper layer protocol field is **ICMP**.

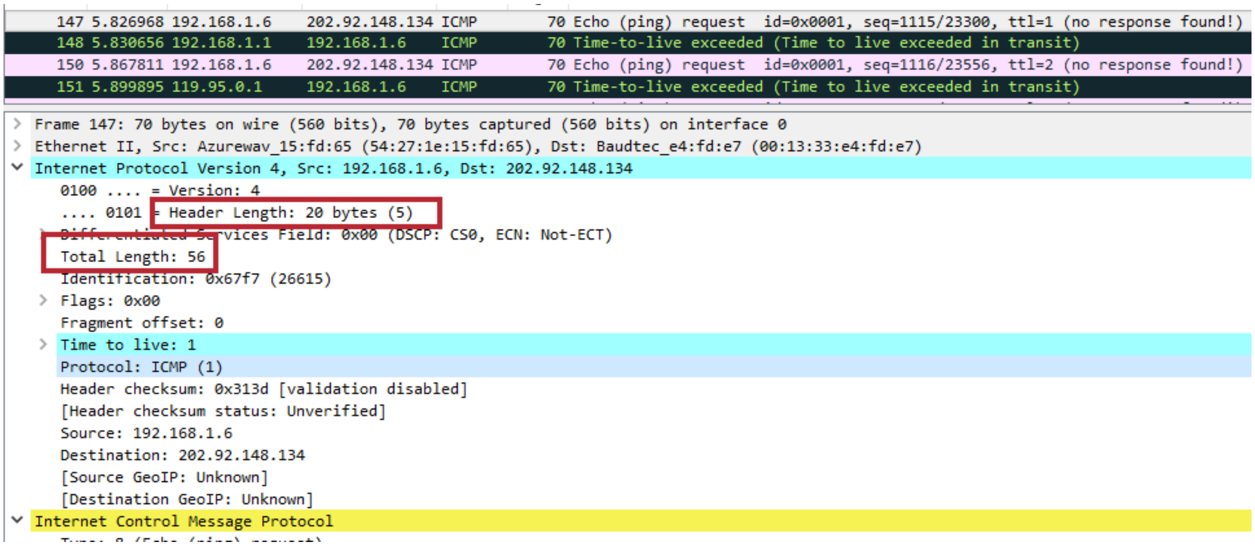


```
147 5.826968 192.168.1.6    202.92.148.134 ICMP     70 Echo (ping) request  id=0x0001, seq=1115/23300, ttl=1 (no response found!)
148 5.830656 192.168.1.1    192.168.1.6    ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
150 5.867811 192.168.1.6    202.92.148.134 ICMP     70 Echo (ping) request  id=0x0001, seq=1116/23556, ttl=2 (no response found!)
151 5.899895 119.95.0.1     192.168.1.6    ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)

> Frame 147: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: Azurewav_15:fd:65 (54:27:1e:15:fd:65), Dst: Baudtec_e4:fd:e7 (00:13:33:e4:fd:e7)
v Internet Protocol Version 4, Src: 192.168.1.6, Dst: 202.92.148.134
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x67f7 (26615)
  > Flags: 0x00
    Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x313d [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.6
    Destination: 202.92.148.134
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
v Internet Control Message Protocol
```

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 header**, and 56 bytes total length. Therefore, there are **36 bytes in the payload**. This is because number of bytes in the payload can be determined by subtracting the length of the header (20 bytes) from the total length (56 bytes).

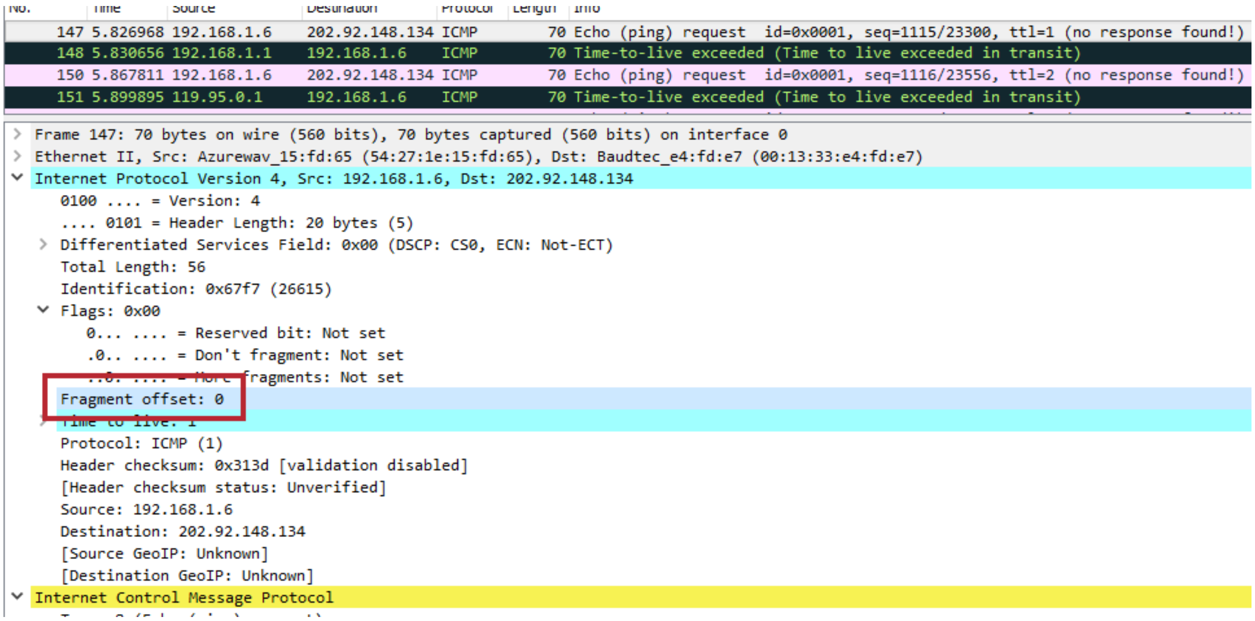


```
    147 5.826968 192.168.1.6    202.92.148.134 ICMP       70 Echo (ping) request  id=0x0001, seq=1115/23300, ttl=1 (no response found!)
    148 5.830656 192.168.1.1    192.168.1.6    ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
    150 5.867811 192.168.1.6    202.92.148.134 ICMP       70 Echo (ping) request  id=0x0001, seq=1116/23556, ttl=2 (no response found!)
    151 5.899895 119.95.0.1     192.168.1.6    ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)

> Frame 147: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: Azurewav_15:fd:65 (54:27:1e:15:fd:65), Dst: Baudtec_e4:fd:e7 (00:13:33:e4:fd:e7)
v Internet Protocol Version 4, Src: 192.168.1.6, Dst: 202.92.148.134
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x67f7 (26615)
  > Flags: 0x00
    Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x313d [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.6
    Destination: 202.92.148.134
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
```

4. Has this datagram been fragmented? Explain how you determined whether the datagram has been fragmented.

The datagram has **not** been fragmented. This is because the fragment offset is set to 0.



```
No.     Time     Source         Destination    Protocol Length Info
    147 5.826968 192.168.1.6    202.92.148.134 ICMP       70 Echo (ping) request  id=0x0001, seq=1115/23300, ttl=1 (no response found!)
    148 5.830656 192.168.1.1    192.168.1.6    ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
    150 5.867811 192.168.1.6    202.92.148.134 ICMP       70 Echo (ping) request  id=0x0001, seq=1116/23556, ttl=2 (no response found!)
    151 5.899895 119.95.0.1     192.168.1.6    ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)

> Frame 147: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: Azurewav_15:fd:65 (54:27:1e:15:fd:65), Dst: Baudtec_e4:fd:e7 (00:13:33:e4:fd:e7)
v Internet Protocol Version 4, Src: 192.168.1.6, Dst: 202.92.148.134
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x67f7 (26615)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x313d [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.6
    Destination: 202.92.148.134
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
```

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?

Frame, **Identification**, **Time to live**, and the **Header checksum** always change.

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

The fields that stay constant are:

- Version (since we're using IPv4, as indicated by RFC 792 which pertains to ICMP)
- Header Length (since these are ICMP packets)
- Differentiated Services Field (since all packets are ICMP, they use the same Type of Service class)
- Total Length (since these are ICMP packets)
- Upper Layer Protocol (since we're using ICMP packets)
- Source Address (since we are sending from the same source)
- Destination Address (since we are contacting the same destination)

The fields that must stay constant are:

- Version (since we're using IPv4, as indicated by RFC 792 which pertains to ICMP)
- Header Length (since these are ICMP packets)
- Differentiated Services Field (since all packets are ICMP, they use the same Type of Service class)
- Total Length (since these are ICMP packets)
- Upper Layer Protocol (since we're using ICMP packets)
- Source Address (since we are sending from the same source)
- Destination Address (since we are contacting the same destination)

The fields that must change are:

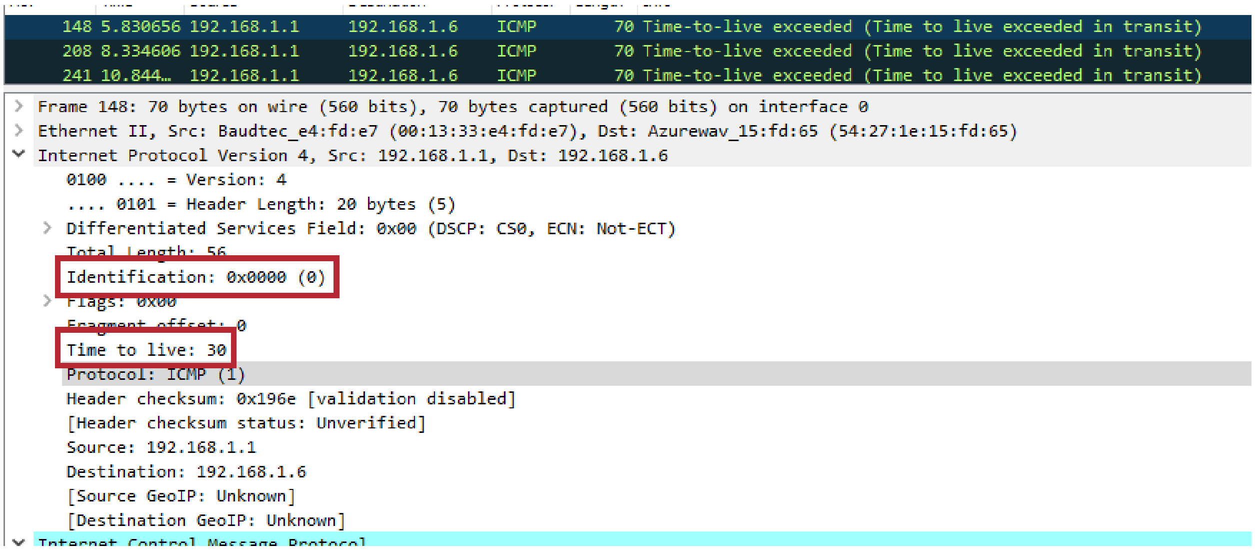
- Identification (since packets must have different IDs)
- Time to live (since traceroute increments each subsequent packet's TTL)
- Header checksum (since the header changes due to Identification and TTL, so does the checksum)

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

The values of the Identification fields **increment by one** after every ICMP Echo (ping) request.

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

The Identification field is **0x0000 (0)** and the TTL field is **30**.



```
148 5.830656 192.168.1.1      192.168.1.6    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
208 8.334606 192.168.1.1      192.168.1.6    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
241 10.844…  192.168.1.1      192.168.1.6    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)

> Frame 148: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: Baudtec_e4:fd:e7 (00:13:33:e4:fd:e7), Dst: Azurewav_15:fd:65 (54:27:1e:15:fd:65)
v Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.6
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x0000 (0)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 30
    Protocol: ICMP (1)
    Header checksum: 0x196e [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.1
    Destination: 192.168.1.6
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
v Internet Control Message Protocol
```

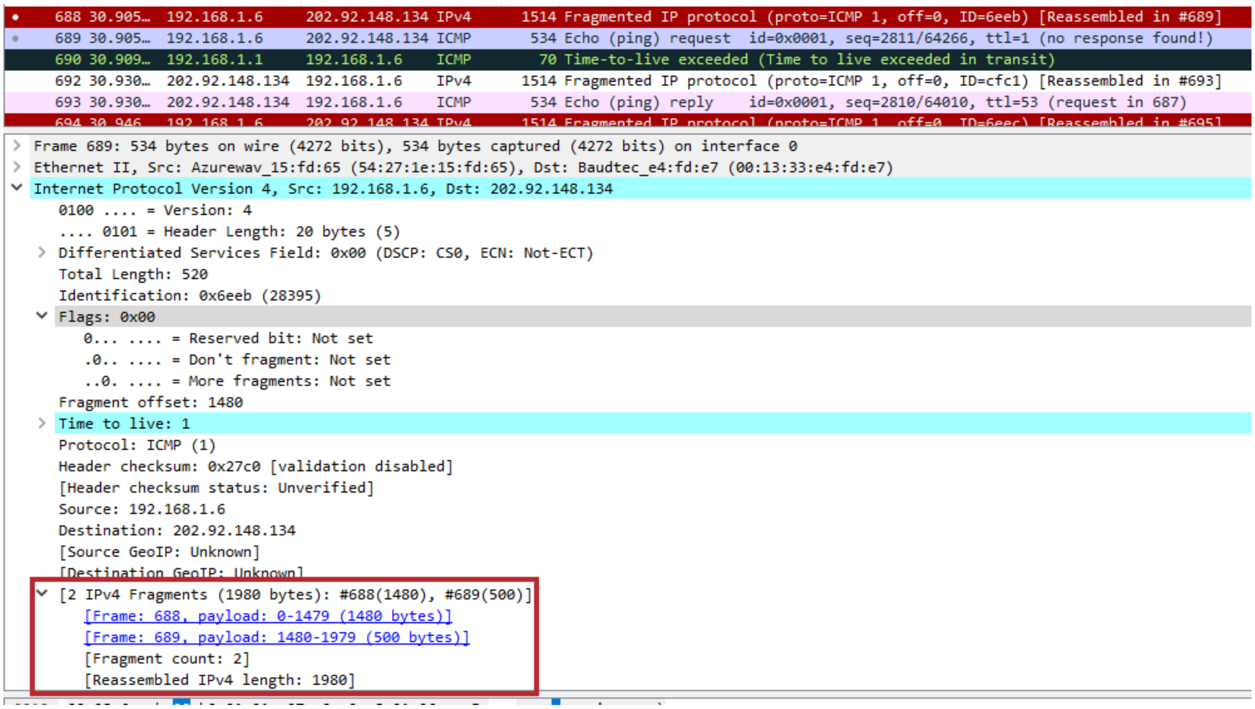
9. Do these values remain unchanged for all the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

The Identification changes because the identification field is a unique value, and that if two datagrams have the same Identification, it means that they are fragments of a datagram.

The TTL remains unchanged because the TTL from the nearest (first hop) router is always the same.

10. Find the first UDP segment that is part of the traceroute sent by your computer after you changed the packet size to 2000. Has that message been fragmented across more than one IP datagram?

The message has been fragmented across more than one IP datagram.



```
 688 30.905…  192.168.1.6     202.92.148.134 IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=6eeb) [Reassembled in #689]
 689 30.905…  192.168.1.6     202.92.148.134 ICMP      534 Echo (ping) request  id=0x0001, seq=2811/64266, ttl=1 (no response found!)
 690 30.909…  192.168.1.1     192.168.1.6    ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 692 30.930…  202.92.148.134  192.168.1.6    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=cfc1) [Reassembled in #693]
 693 30.930…  202.92.148.134  192.168.1.6    ICMP      534 Echo (ping) reply    id=0x0001, seq=2810/64010, ttl=53 (request in 687)
 694 30.946   192.168.1.6     202.92.148.134 IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=6eec) [Reassembled in #695]

> Frame 689: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface 0
> Ethernet II, Src: Azurewav_15:fd:65 (54:27:1e:15:fd:65), Dst: Baudtec_e4:fd:e7 (00:13:33:e4:fd:e7)
v Internet Protocol Version 4, Src: 192.168.1.6, Dst: 202.92.148.134
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 520
    Identification: 0x6eeb (28395)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 1480
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x27c0 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.6
    Destination: 202.92.148.134
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  v [2 IPv4 Fragments (1980 bytes): #688(1480), #689(500)]
      [Frame: 688, payload: 0-1479 (1480 bytes)]
      [Frame: 689, payload: 1480-1979 (500 bytes)]
      [Fragment count: 2]
      [Reassembled IPv4 length: 1980]
```

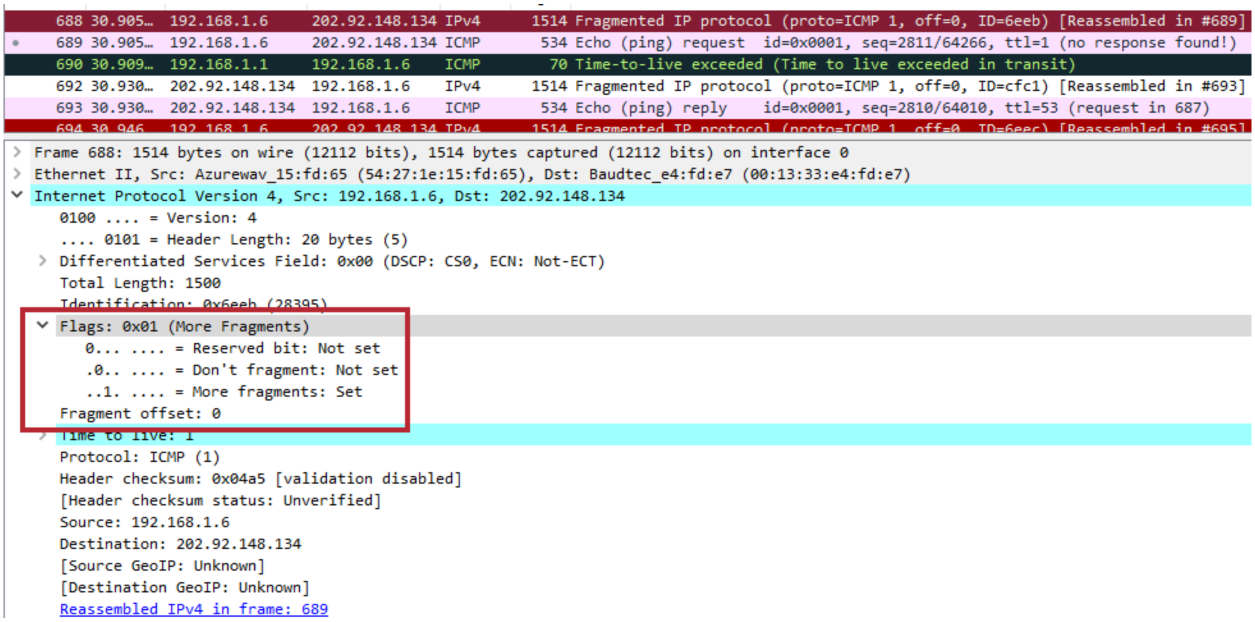
11. Show the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram has been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?

The Flags bit for fragments is set to 1, indicating that the datagram has been fragmented.

The Fragment offset is set to 0, indicating that it is the first fragment.

The Fragment offset indicates whether a fragment is the first fragment versus a latter one

The IP datagram’s total length is 1980 bytes (refer to the supporting screenshot to #10).



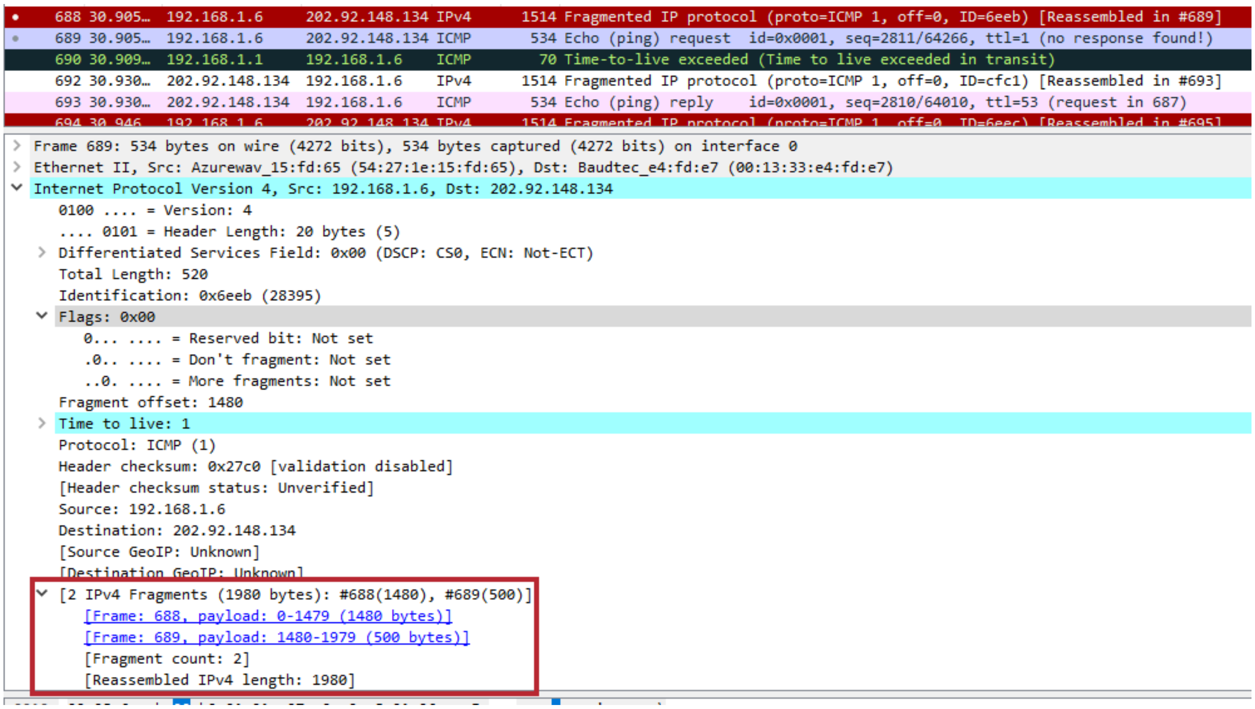
```
  688 30.905… 192.168.1.6     202.92.148.134 IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=6eeb) [Reassembled in #689]
• 689 30.905… 192.168.1.6     202.92.148.134 ICMP      534 Echo (ping) request  id=0x0001, seq=2811/64266, ttl=1 (no response found!)
  690 30.909… 192.168.1.1     192.168.1.6    ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  692 30.930… 202.92.148.134  192.168.1.6    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=cfc1) [Reassembled in #693]
  693 30.930… 202.92.148.134  192.168.1.6    ICMP      534 Echo (ping) reply    id=0x0001, seq=2810/64010, ttl=53 (request in 687)
  694 30.946… 192.168.1.6     202.92.148.134 IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=6eec) [Reassembled in #695]

> Frame 688: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
> Ethernet II, Src: Azurewav_15:fd:65 (54:27:1e:15:fd:65), Dst: Baudtec_e4:fd:e7 (00:13:33:e4:fd:e7)
v Internet Protocol Version 4, Src: 192.168.1.6, Dst: 202.92.148.134
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x6eeb (28395)
  v Flags: 0x01 (More Fragments)
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x04a5 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.6
    Destination: 202.92.148.134
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
    Reassembled IPv4 in frame: 689
```

12. Show 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 Fragment offset is set to 1480, indicating that it is not the first datagram fragment, as it should be set to 0 if it was the first fragment.

There are no more fragments because the “More fragments” flag is set to 0.



```
•  688 30.905… 192.168.1.6     202.92.148.134 IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=6eeb) [Reassembled in #689]
•  689 30.905… 192.168.1.6     202.92.148.134 ICMP     534 Echo (ping) request  id=0x0001, seq=2811/64266, ttl=1 (no response found!)
   690 30.909… 192.168.1.1     192.168.1.6    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   692 30.930… 202.92.148.134  192.168.1.6    IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=cfc1) [Reassembled in #693]
   693 30.930… 202.92.148.134  192.168.1.6    ICMP     534 Echo (ping) reply    id=0x0001, seq=2810/64010, ttl=53 (request in 687)
   694 30.946  192.168.1.6     202.92.148.134 IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=6eec) [Reassembled in #695]
```

```
> Frame 689: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface 0
> Ethernet II, Src: Azurewav_15:fd:65 (54:27:1e:15:fd:65), Dst: Baudtec_e4:fd:e7 (00:13:33:e4:fd:e7)
v Internet Protocol Version 4, Src: 192.168.1.6, Dst: 202.92.148.134
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 520
    Identification: 0x6eeb (28395)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 1480
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x27c0 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.6
    Destination: 202.92.148.134
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  v [2 IPv4 Fragments (1980 bytes): #688(1480), #689(500)]
      [Frame: 688, payload: 0-1479 (1480 bytes)]
      [Frame: 689, payload: 1480-1979 (500 bytes)]
      [Fragment count: 2]
      [Reassembled IPv4 length: 1980]
```

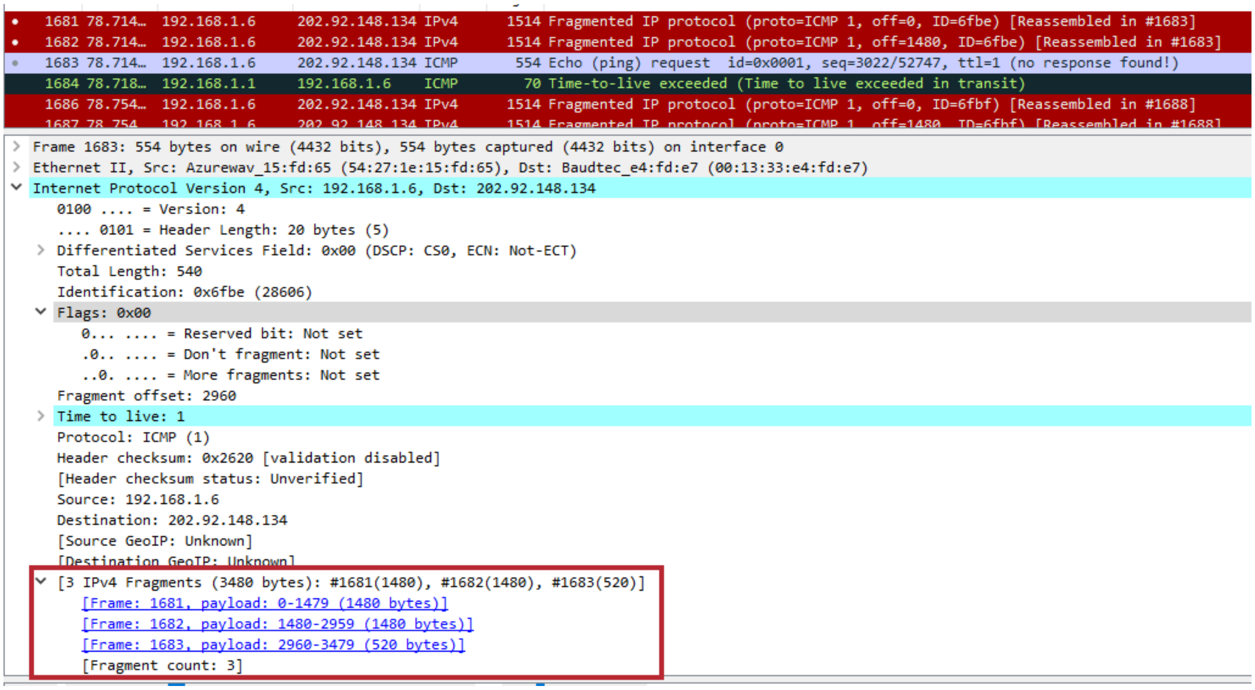
13. What fields change in the IP header between the first and second fragment?

The fields that change are:

- Total Length
- Flags
- Fragment offset
- Header checksum

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

Three fragments were created from the original datagram.



```
•  1681 78.714…  192.168.1.6    202.92.148.134 IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=6fbe) [Reassembled in #1683]
•  1682 78.714…  192.168.1.6    202.92.148.134 IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=6fbe) [Reassembled in #1683]
•  1683 78.714…  192.168.1.6    202.92.148.134 ICMP     554 Echo (ping) request  id=0x0001, seq=3022/52747, ttl=1 (no response found!)
   1684 78.718…  192.168.1.1    192.168.1.6    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   1686 78.754…  192.168.1.6    202.92.148.134 IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=6fbf) [Reassembled in #1688]
   1687 78.754…  192.168.1.6    202.92.148.134 IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=6fbf) [Reassembled in #1688]

> Frame 1683: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0
> Ethernet II, Src: Azurewav_15:fd:65 (54:27:1e:15:fd:65), Dst: Baudtec_e4:fd:e7 (00:13:33:e4:fd:e7)
v Internet Protocol Version 4, Src: 192.168.1.6, Dst: 202.92.148.134
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 540
    Identification: 0x6fbe (28606)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 2960
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x2620 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.6
    Destination: 202.92.148.134
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  v [3 IPv4 Fragments (3480 bytes): #1681(1480), #1682(1480), #1683(520)]
      [Frame: 1681, payload: 0-1479 (1480 bytes)]
      [Frame: 1682, payload: 1480-2959 (1480 bytes)]
      [Frame: 1683, payload: 2960-3479 (520 bytes)]
      [Fragment count: 3]
```

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

The fields that change are:

- Total length (the first two both have 1500 bytes while the last has 540 bytes)
- Flags (the first two have the same flags set, while the last fragment has the "More fragments" flag set to 0)
- Fragment offset
- Header checksum