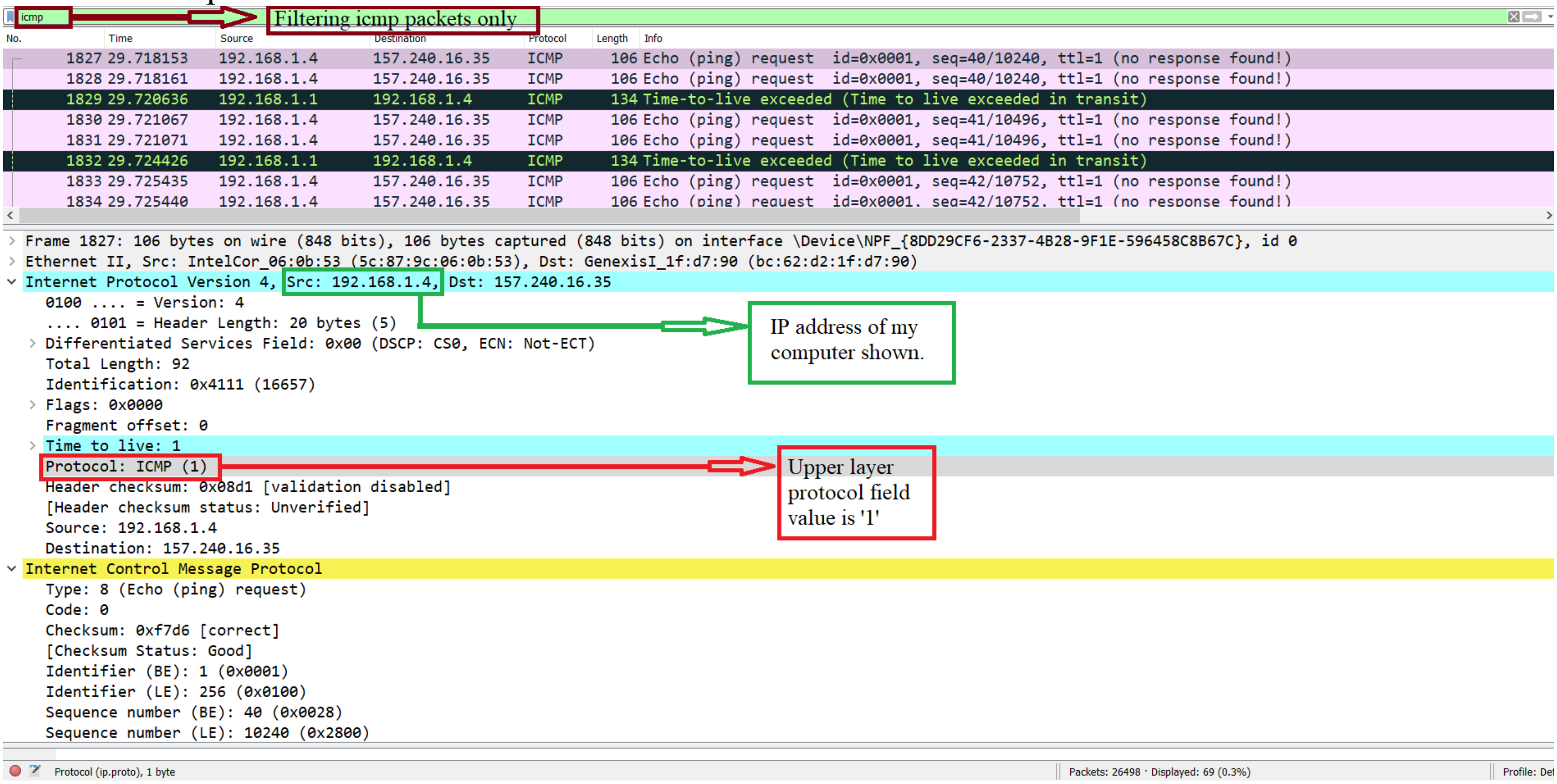
1. Pick an IP message from wireshark capture for ICMP (from ping/ traceroute). What is the value of the upper layer protocol field? What is the IP address of your computer shown?



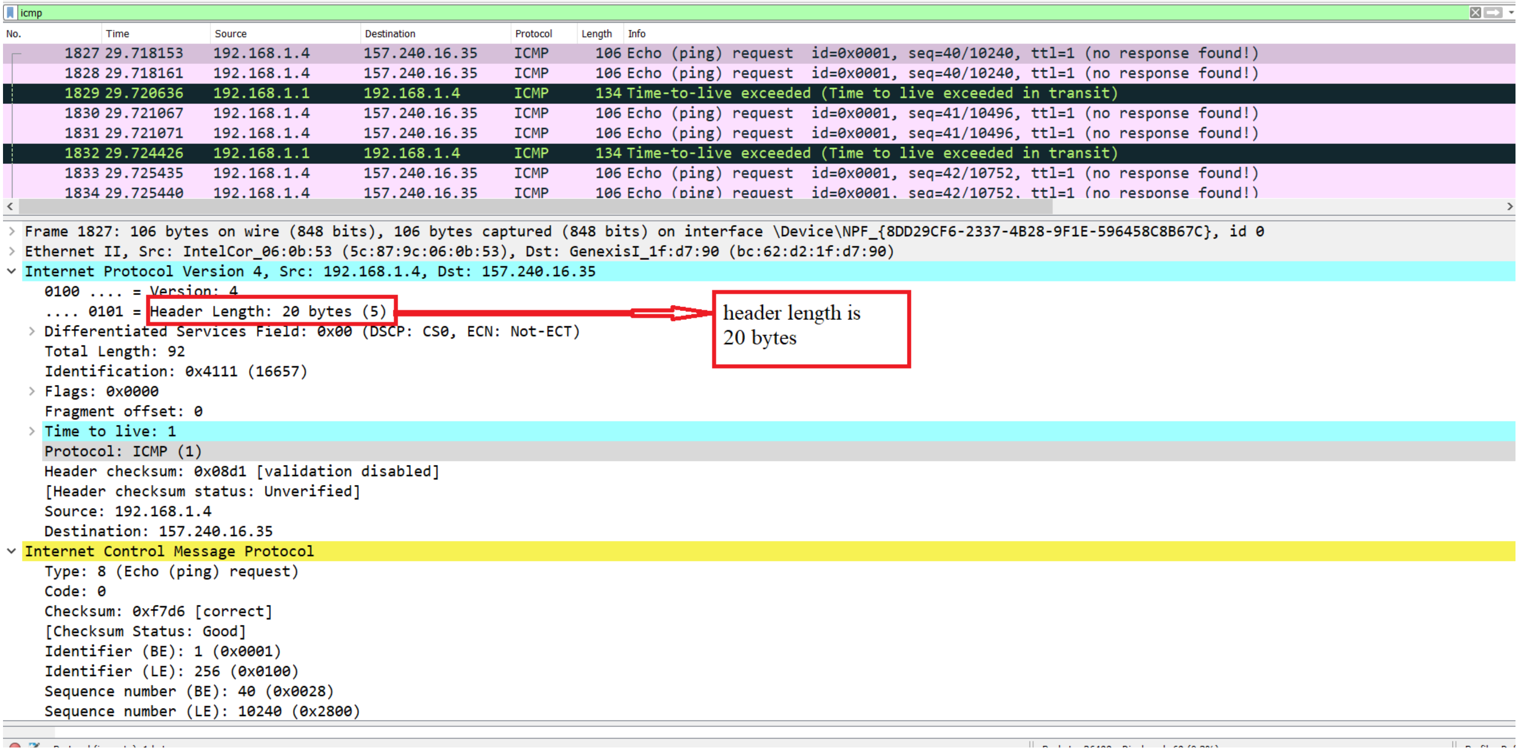
Filtering icmp packets only

```
icmp
No.    Time          Source         Destination      Protocol  Length Info
  1827 29.718153    192.168.1.4    157.240.16.35    ICMP      106 Echo (ping) request  id=0x0001, seq=40/10240, ttl=1 (no response found!)
  1828 29.718161    192.168.1.4    157.240.16.35    ICMP      106 Echo (ping) request  id=0x0001, seq=40/10240, ttl=1 (no response found!)
  1829 29.720636    192.168.1.1    192.168.1.4      ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
  1830 29.721067    192.168.1.4    157.240.16.35    ICMP      106 Echo (ping) request  id=0x0001, seq=41/10496, ttl=1 (no response found!)
  1831 29.721071    192.168.1.4    157.240.16.35    ICMP      106 Echo (ping) request  id=0x0001, seq=41/10496, ttl=1 (no response found!)
  1832 29.724426    192.168.1.1    192.168.1.4      ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
  1833 29.725435    192.168.1.4    157.240.16.35    ICMP      106 Echo (ping) request  id=0x0001, seq=42/10752, ttl=1 (no response found!)
  1834 29.725440    192.168.1.4    157.240.16.35    ICMP      106 Echo (ping) request  id=0x0001, seq=42/10752, ttl=1 (no response found!)

> Frame 1827: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{8DD29CF6-2337-4B28-9F1E-596458C8B67C}, id 0
> Ethernet II, Src: IntelCor_06:0b:53 (5c:87:9c:06:0b:53), Dst: GenexisI_1f:d7:90 (bc:62:d2:1f:d7:90)
v Internet Protocol Version 4, Src: 192.168.1.4, Dst: 157.240.16.35
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x4111 (16657)
  > Flags: 0x0000
    Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x08d1 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.4
    Destination: 157.240.16.35
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7d6 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 40 (0x0028)
    Sequence number (LE): 10240 (0x2800)

Protocol (ip.proto), 1 byte          Packets: 26498 · Displayed: 69 (0.3%)          Profile: Def
```

IP address of my computer shown.

Upper layer protocol field value is '1'

2. How many bytes are there in the IP datagram? How did you determine this value?

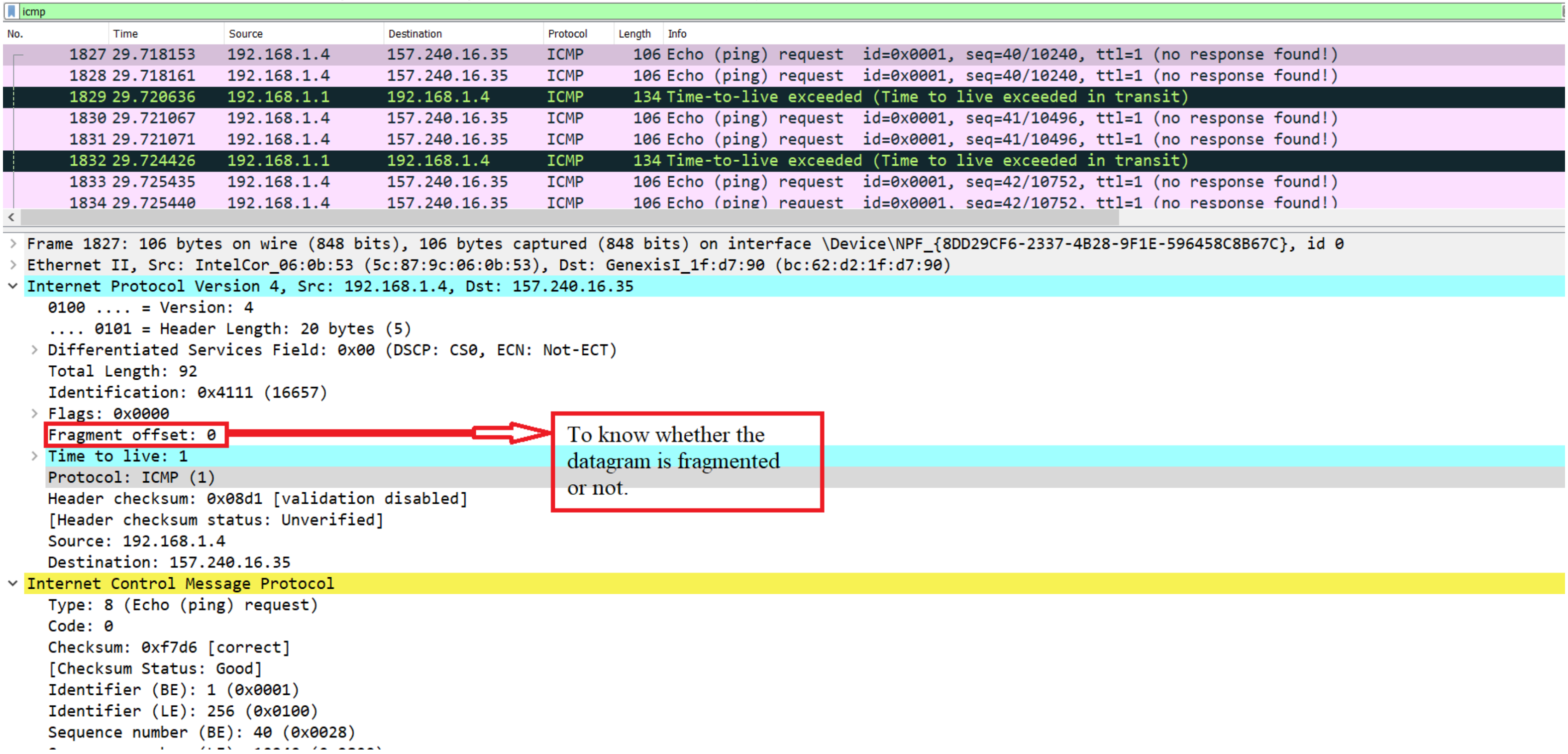


```
icmp
No.    Time          Source         Destination      Protocol  Length Info
  1827 29.718153    192.168.1.4    157.240.16.35    ICMP      106 Echo (ping) request  id=0x0001, seq=40/10240, ttl=1 (no response found!)
  1828 29.718161    192.168.1.4    157.240.16.35    ICMP      106 Echo (ping) request  id=0x0001, seq=40/10240, ttl=1 (no response found!)
  1829 29.720636    192.168.1.1    192.168.1.4      ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
  1830 29.721067    192.168.1.4    157.240.16.35    ICMP      106 Echo (ping) request  id=0x0001, seq=41/10496, ttl=1 (no response found!)
  1831 29.721071    192.168.1.4    157.240.16.35    ICMP      106 Echo (ping) request  id=0x0001, seq=41/10496, ttl=1 (no response found!)
  1832 29.724426    192.168.1.1    192.168.1.4      ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
  1833 29.725435    192.168.1.4    157.240.16.35    ICMP      106 Echo (ping) request  id=0x0001, seq=42/10752, ttl=1 (no response found!)
  1834 29.725440    192.168.1.4    157.240.16.35    ICMP      106 Echo (ping) request  id=0x0001, seq=42/10752, ttl=1 (no response found!)

> Frame 1827: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{8DD29CF6-2337-4B28-9F1E-596458C8B67C}, id 0
> Ethernet II, Src: IntelCor_06:0b:53 (5c:87:9c:06:0b:53), Dst: GenexisI_1f:d7:90 (bc:62:d2:1f:d7:90)
v Internet Protocol Version 4, Src: 192.168.1.4, Dst: 157.240.16.35
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x4111 (16657)
  > Flags: 0x0000
    Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x08d1 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.4
    Destination: 157.240.16.35
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7d6 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 40 (0x0028)
    Sequence number (LE): 10240 (0x2800)
```

header length is 20 bytes

IP datagram is 36 bytes. (Total length – header length) that is 56 bytes – 20 bytes = 36 bytes.

3. Is the datagram fragmented? How did you know?



```
icmp
No.    Time       Source        Destination     Protocol  Length  Info
1827 29.718153   192.168.1.4   157.240.16.35   ICMP      106 Echo (ping) request  id=0x0001, seq=40/10240, ttl=1 (no response found!)
1828 29.718161   192.168.1.4   157.240.16.35   ICMP      106 Echo (ping) request  id=0x0001, seq=40/10240, ttl=1 (no response found!)
1829 29.720636   192.168.1.1   192.168.1.4     ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
1830 29.721067   192.168.1.4   157.240.16.35   ICMP      106 Echo (ping) request  id=0x0001, seq=41/10496, ttl=1 (no response found!)
1831 29.721071   192.168.1.4   157.240.16.35   ICMP      106 Echo (ping) request  id=0x0001, seq=41/10496, ttl=1 (no response found!)
1832 29.724426   192.168.1.1   192.168.1.4     ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
1833 29.725435   192.168.1.4   157.240.16.35   ICMP      106 Echo (ping) request  id=0x0001, seq=42/10752, ttl=1 (no response found!)
1834 29.725440   192.168.1.4   157.240.16.35   ICMP      106 Echo (ping) request  id=0x0001, seq=42/10752, ttl=1 (no response found!)

> Frame 1827: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{8DD29CF6-2337-4B28-9F1E-596458C8B67C}, id 0
> Ethernet II, Src: IntelCor_06:0b:53 (5c:87:9c:06:0b:53), Dst: GenexisI_1f:d7:90 (bc:62:d2:1f:d7:90)
v Internet Protocol Version 4, Src: 192.168.1.4, Dst: 157.240.16.35
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x4111 (16657)
  > Flags: 0x0000
    Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x08d1 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.4
    Destination: 157.240.16.35
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7d6 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 40 (0x0028)
```

To know whether the datagram is fragmented or not.

The fragment offset is zero. Therefore the datagram is not fragmented.

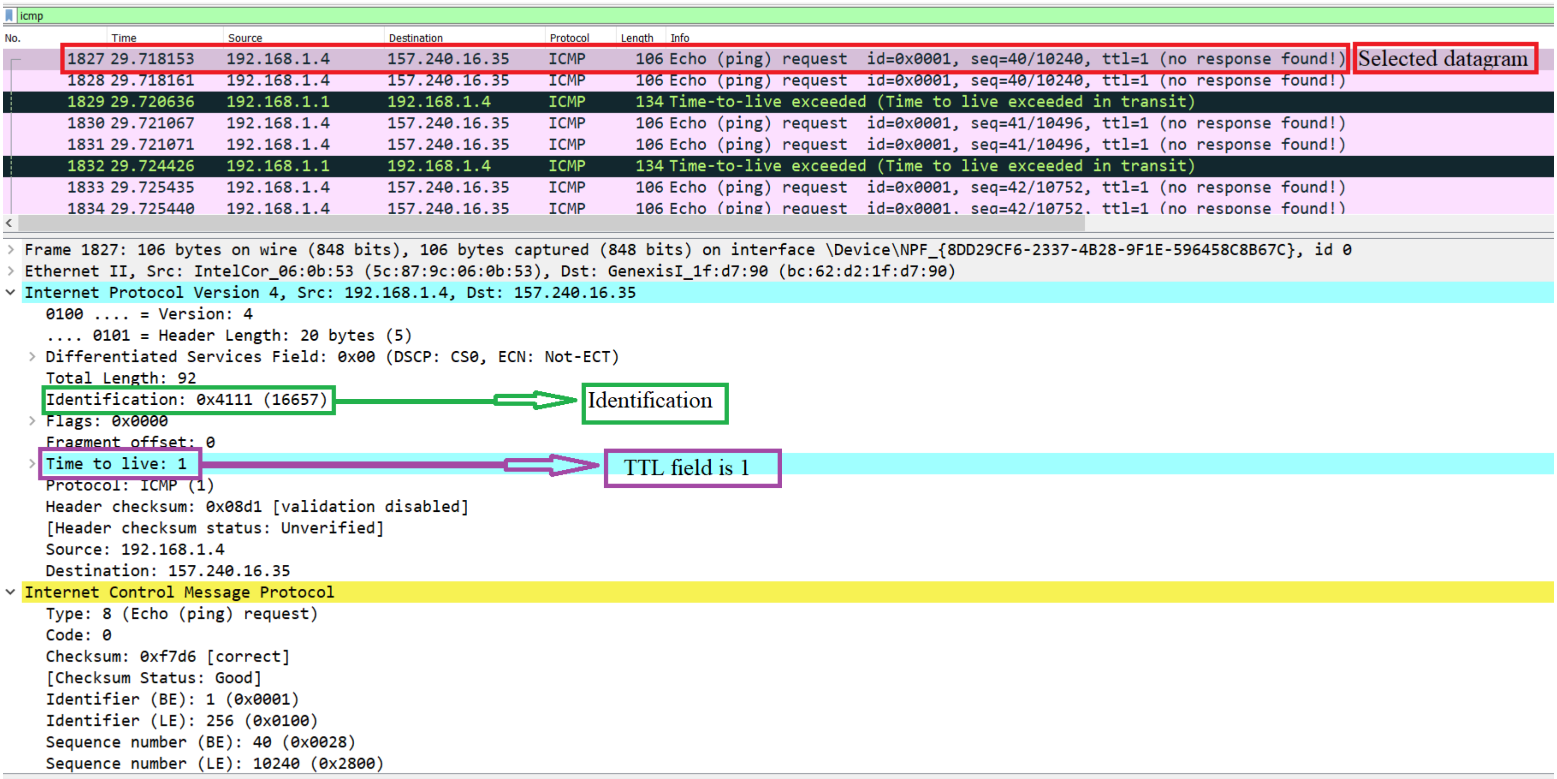
4. Which fields stay constant between IP datagrams? Which do not?

The fields that stay constant:

a)Version (IPv4)
b)Length of header
c)Source IP (Sending from the same source)
d)Destination IP (Receiver is the same)
e)Upper layer protocol (using ICMP always)

The fields that change:
a)Header checksum
b)Identification
c)TTL(based on number of hops it changes)

5. What is the value of the identification and time to live fields of the datagram you picked? Do they remain unchanged for the TTL exceeded replies from the first router?



```
icmp
No.     Time          Source         Destination     Protocol  Length Info
   1827 29.718153     192.168.1.4    157.240.16.35   ICMP      106 Echo (ping) request  id=0x0001, seq=40/10240, ttl=1 (no response found!)
   1828 29.718161     192.168.1.4    157.240.16.35   ICMP      106 Echo (ping) request  id=0x0001, seq=40/10240, ttl=1 (no response found!)
   1829 29.720636     192.168.1.1    192.168.1.4     ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
   1830 29.721067     192.168.1.4    157.240.16.35   ICMP      106 Echo (ping) request  id=0x0001, seq=41/10496, ttl=1 (no response found!)
   1831 29.721071     192.168.1.4    157.240.16.35   ICMP      106 Echo (ping) request  id=0x0001, seq=41/10496, ttl=1 (no response found!)
   1832 29.724426     192.168.1.1    192.168.1.4     ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
   1833 29.725435     192.168.1.4    157.240.16.35   ICMP      106 Echo (ping) request  id=0x0001, seq=42/10752, ttl=1 (no response found!)
   1834 29.725440     192.168.1.4    157.240.16.35   ICMP      106 Echo (ping) request  id=0x0001, seq=42/10752, ttl=1 (no response found!)

> Frame 1827: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{8DD29CF6-2337-4B28-9F1E-596458C8B67C}, id 0
> Ethernet II, Src: IntelCor_06:0b:53 (5c:87:9c:06:0b:53), Dst: GenexisI_1f:d7:90 (bc:62:d2:1f:d7:90)
v Internet Protocol Version 4, Src: 192.168.1.4, Dst: 157.240.16.35
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x4111 (16657)
  > Flags: 0x0000
    Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x08d1 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.4
    Destination: 157.240.16.35
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7d6 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 40 (0x0028)
    Sequence number (LE): 10240 (0x2800)
```

Identification field is 16657 which should be different from all other replies because this field should have unique values. If they are the same then that means the datagram is fragmented.

The TTL field does not change as the time to live to the first hop router is always same.