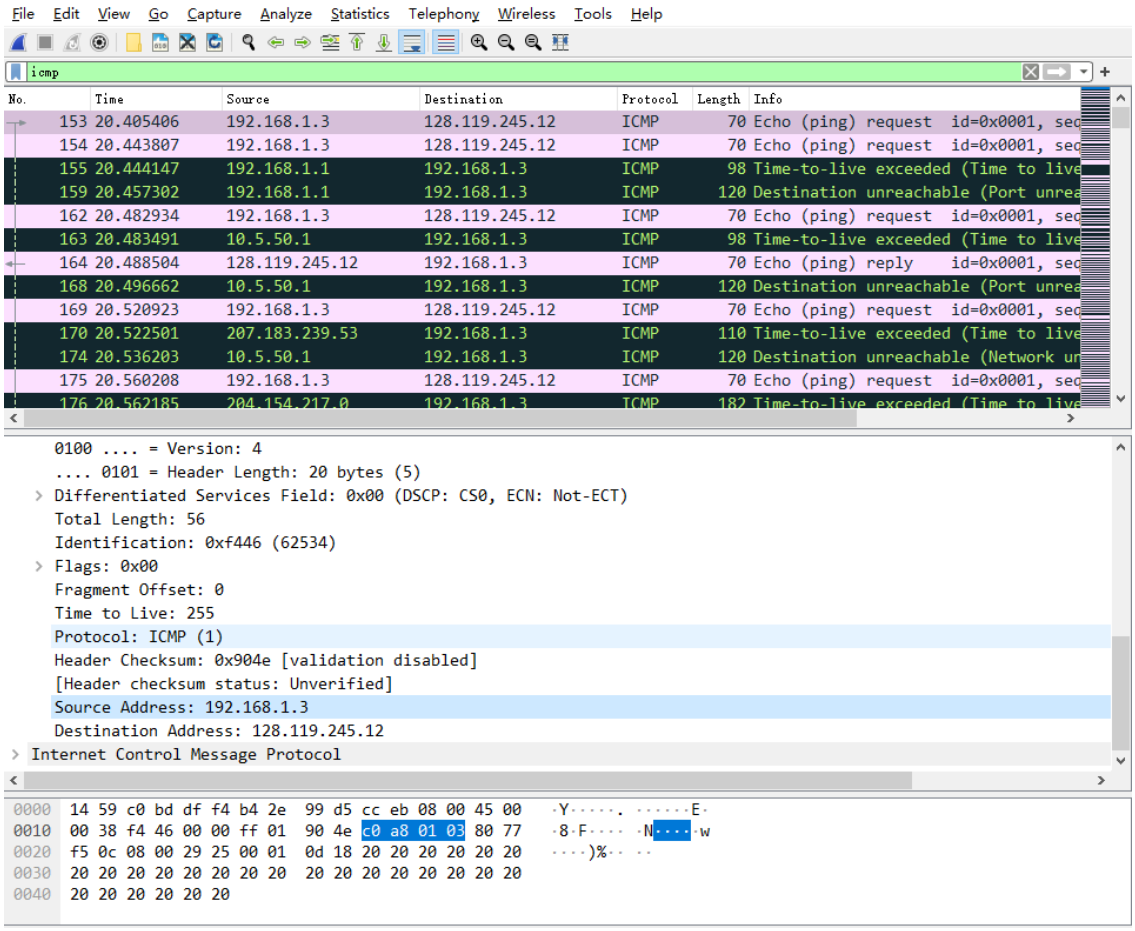
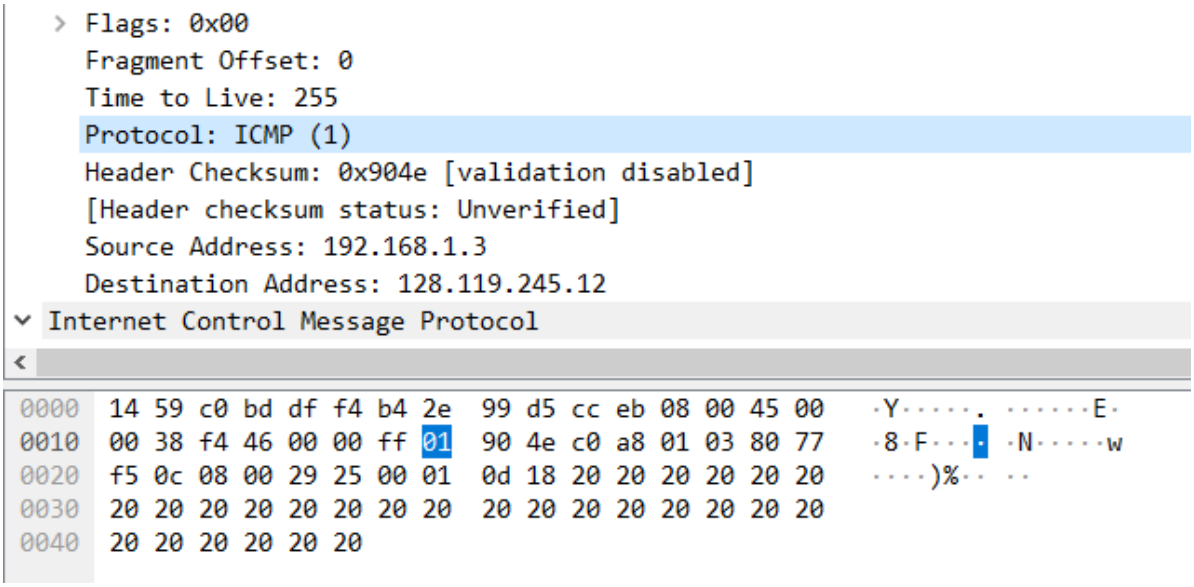
ECS152A-Programming_Assignment#1

Part1: Wireshark - IP

Answers:

1. 

The IP address of my computer is 192.168.1.3.



Within the IP packet header, the value in the upper layer protocol field is **ICMP(1)**

3.

```
Internet Protocol Version 4, Src: 192.168.1.3, 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: 0xf446 (62534)
  > Flags: 0x00
    Fragment Offset: 0
```

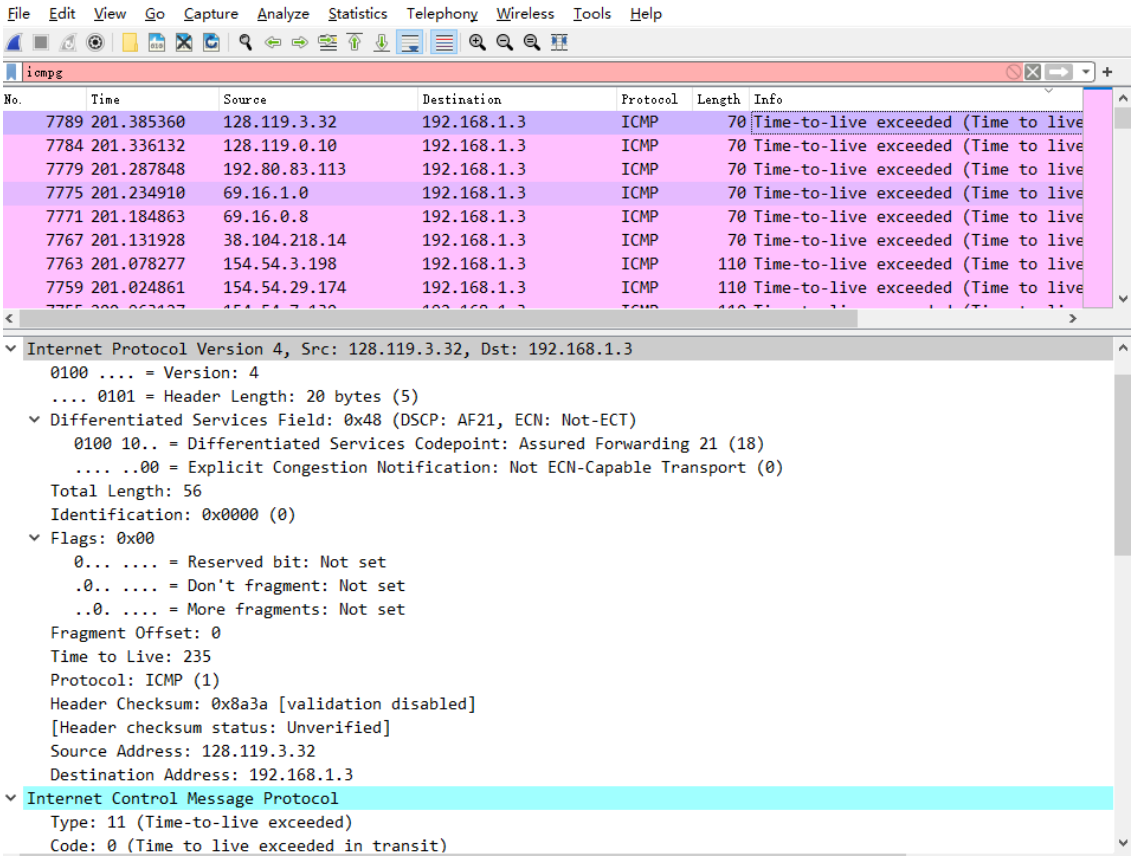
There are **20 bytes** in the IP header, and the total length of the datagram is **56 bytes**, thus, as the total length is 56 bytes and the header is 20 bytes, the number of payload bytes is calculated by 56 - 20 = 36 bytes, so the number of payload bytes is **36 bytes**.

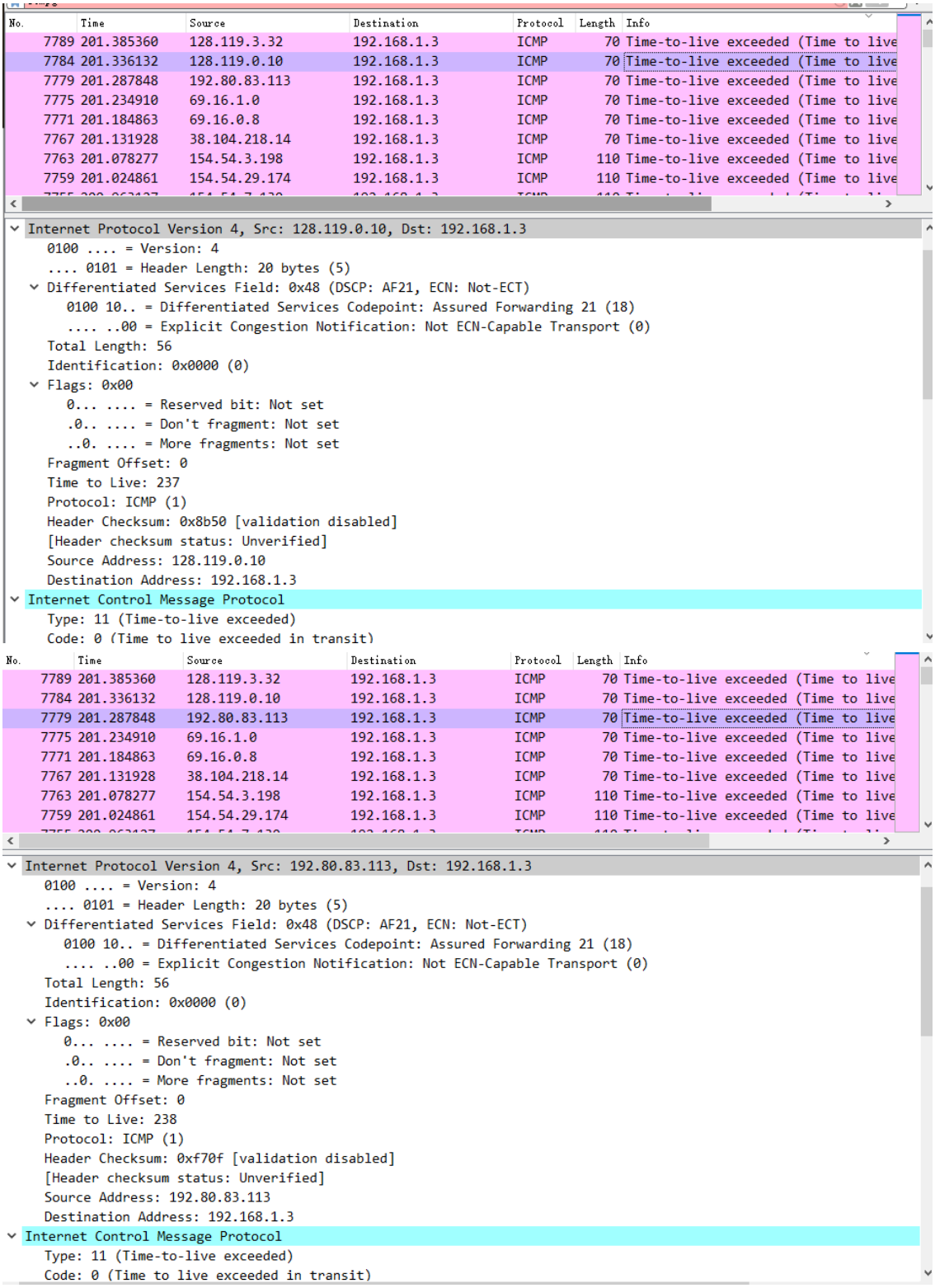
4.

```
Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
Fragment Offset: 0
```

As the Wireshark shows the fragment offset is 0, and also there is not set for more fragments, so this IP datagram has not been fragmented.

5.



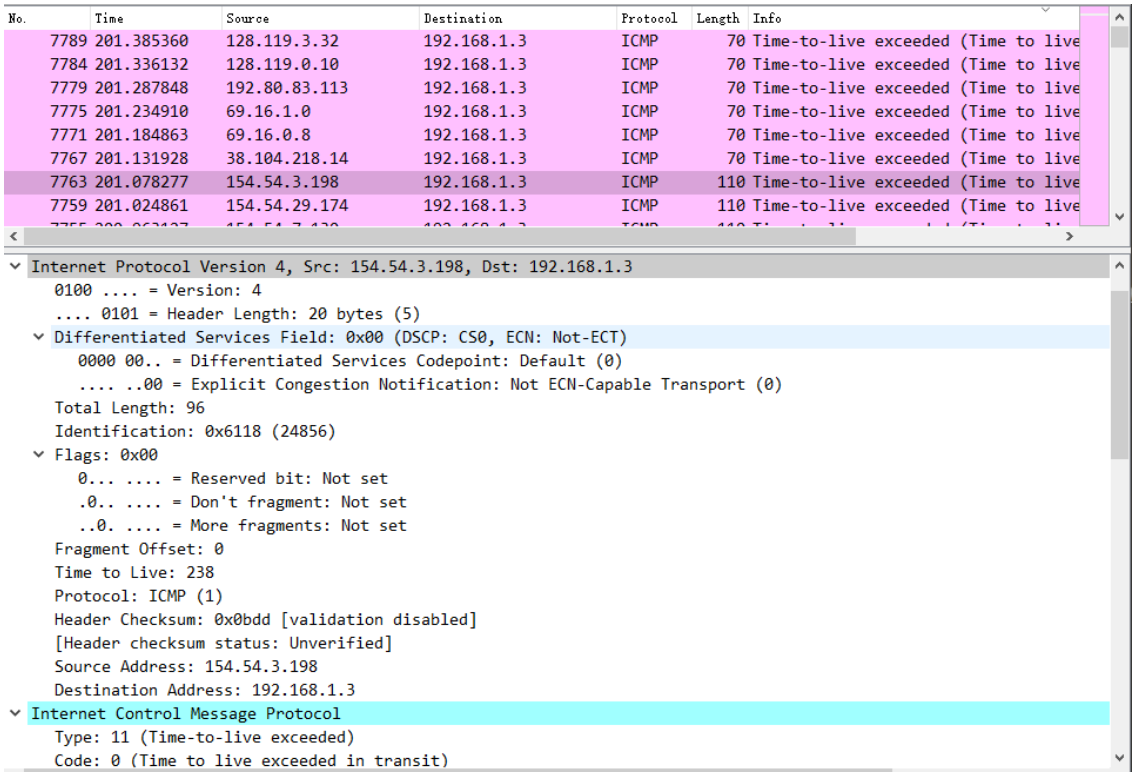


No.	Time	Source	Destination	Protocol	Length	Info
7789	201.385360	128.119.3.32	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live
7784	201.336132	128.119.0.10	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live
7779	201.287848	192.80.83.113	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live
7775	201.234910	69.16.1.0	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live
7771	201.184863	69.16.0.8	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live
7767	201.131928	38.104.218.14	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live
7763	201.078277	154.54.3.198	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live
7759	201.024861	154.54.29.174	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live

```
Internet Protocol Version 4, Src: 128.119.0.10, Dst: 192.168.1.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x48 (DSCP: AF21, ECN: Not-ECT)
      0100 10.. = Differentiated Services Codepoint: Assured Forwarding 21 (18)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 56
    Identification: 0x0000 (0)
  Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 237
    Protocol: ICMP (1)
    Header Checksum: 0x8b50 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.119.0.10
    Destination Address: 192.168.1.3
Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
```

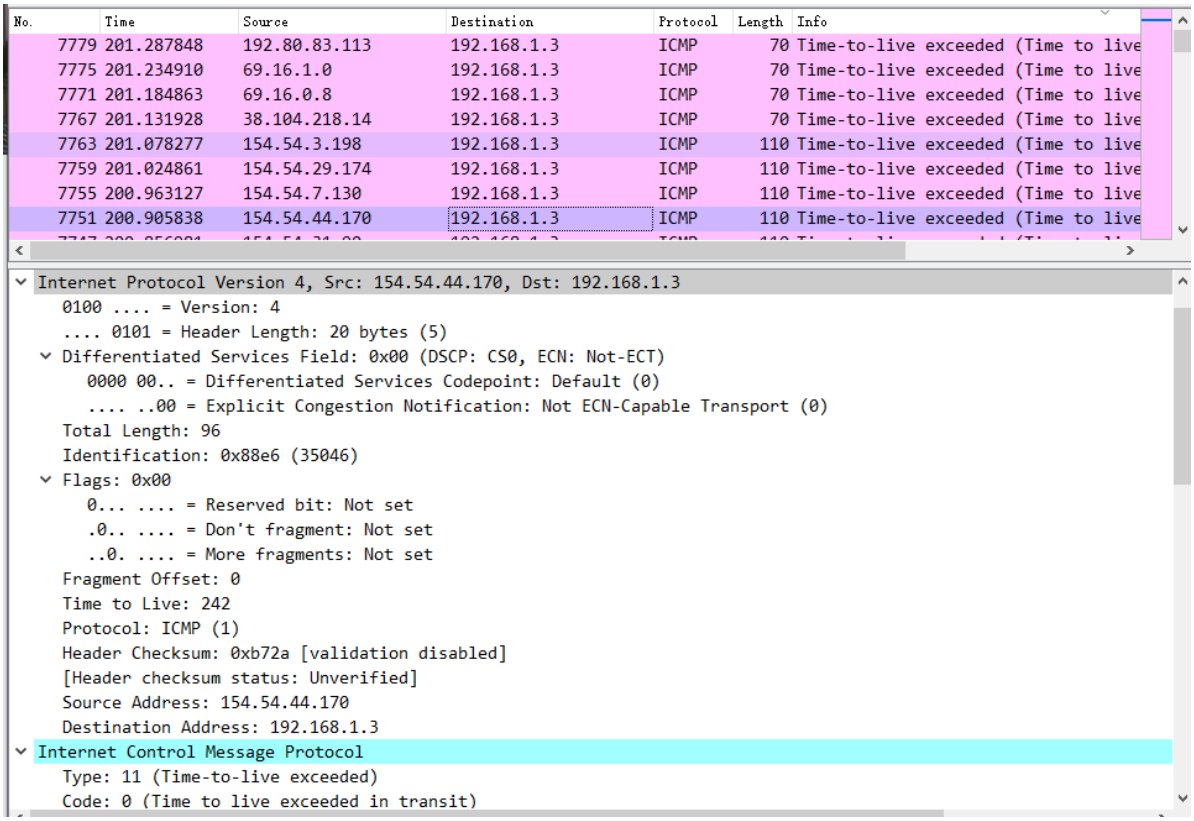
No.	Time	Source	Destination	Protocol	Length	Info
7789	201.385360	128.119.3.32	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live
7784	201.336132	128.119.0.10	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live
7779	201.287848	192.80.83.113	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live
7775	201.234910	69.16.1.0	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live
7771	201.184863	69.16.0.8	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live
7767	201.131928	38.104.218.14	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live
7763	201.078277	154.54.3.198	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live
7759	201.024861	154.54.29.174	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live

```
Internet Protocol Version 4, Src: 192.80.83.113, Dst: 192.168.1.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x48 (DSCP: AF21, ECN: Not-ECT)
      0100 10.. = Differentiated Services Codepoint: Assured Forwarding 21 (18)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 56
    Identification: 0x0000 (0)
  Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 238
    Protocol: ICMP (1)
    Header Checksum: 0xf70f [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.80.83.113
    Destination Address: 192.168.1.3
Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
```



No.	Time	Source	Destination	Protocol	Length	Info
7789	201.385360	128.119.3.32	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live
7784	201.336132	128.119.0.10	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live
7779	201.287848	192.80.83.113	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live
7775	201.234910	69.16.1.0	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live
7771	201.184863	69.16.0.8	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live
7767	201.131928	38.104.218.14	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live
7763	201.078277	154.54.3.198	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live
7759	201.024861	154.54.29.174	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live

```
Internet Protocol Version 4, Src: 154.54.3.198, Dst: 192.168.1.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 96
    Identification: 0x6118 (24856)
  Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 238
    Protocol: ICMP (1)
    Header Checksum: 0x0bdd [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 154.54.3.198
    Destination Address: 192.168.1.3
Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
```



No.	Time	Source	Destination	Protocol	Length	Info
7779	201.287848	192.80.83.113	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live
7775	201.234910	69.16.1.0	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live
7771	201.184863	69.16.0.8	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live
7767	201.131928	38.104.218.14	192.168.1.3	ICMP	70	Time-to-live exceeded (Time to live
7763	201.078277	154.54.3.198	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live
7759	201.024861	154.54.29.174	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live
7755	200.963127	154.54.7.130	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live
7751	200.905838	154.54.44.170	192.168.1.3	ICMP	110	Time-to-live exceeded (Time to live

```
Internet Protocol Version 4, Src: 154.54.44.170, Dst: 192.168.1.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 96
    Identification: 0x88e6 (35046)
  Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 242
    Protocol: ICMP (1)
    Header Checksum: 0xb72a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 154.54.44.170
    Destination Address: 192.168.1.3
Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
```

By comparing different records, the fields that always change are: **Identification**, **Time to Live**, and **Header Checksum**.

6.

The Version, header length, source IP, destination IP, differentiated services, upper layer protocol stay constant.

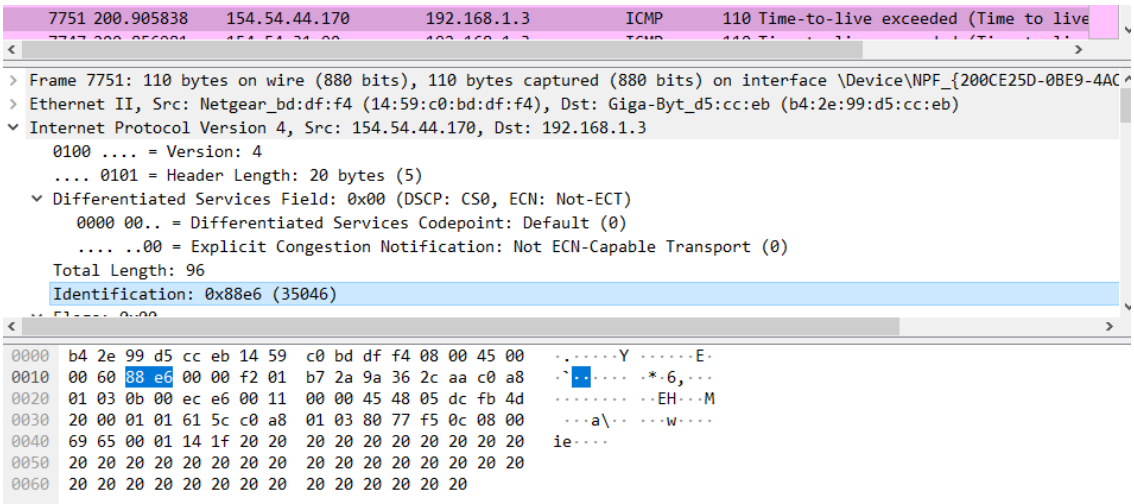
The version, header length, source IP, destination IP, and differentiated services must stay constant.

The identification, time to live, and header checksum must changed.

Reason:

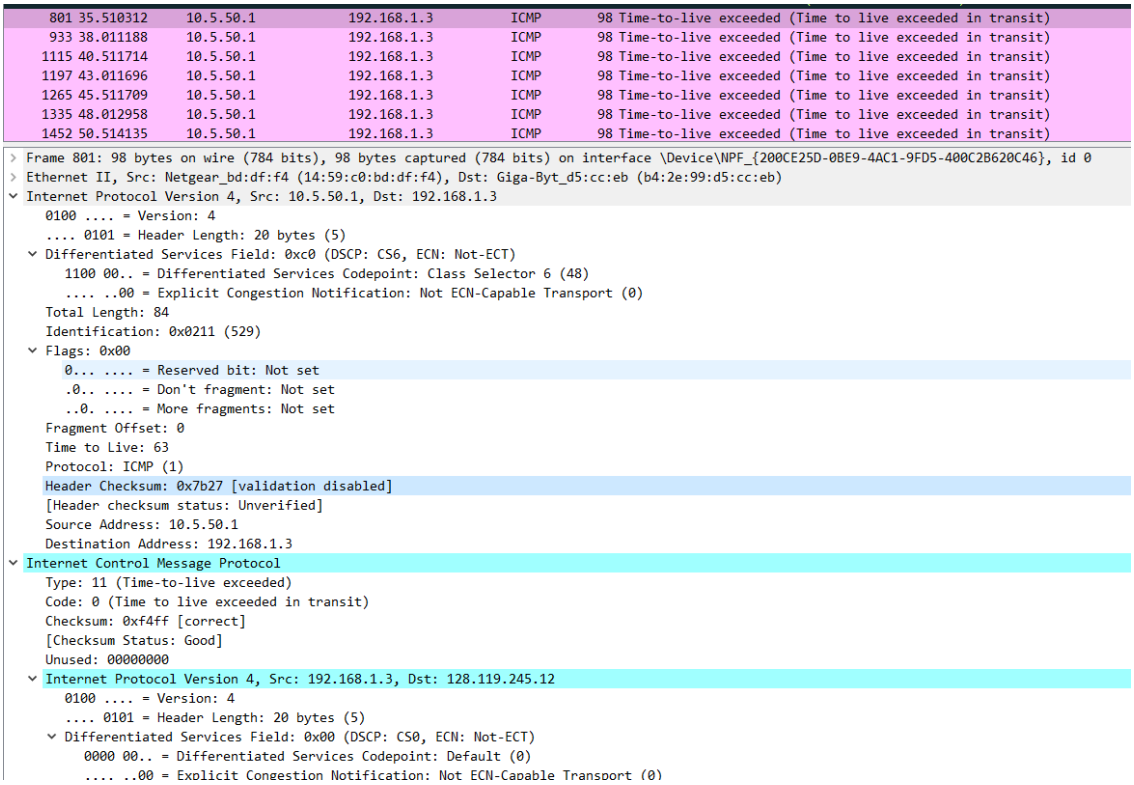
- Version: as the computer is using IPv4 for all packets, the version should always stay constant, and it must stay constant or it might cause error on transiting packets.
- Header length: as all the packets are ICMP packets, they are following the same formatting rule, thus there should share the same header length as the ICMP request. Thus the header length field must stay constant.
- Source IP: since all the packets were sent from my computer, the Source IP field should always stay constant.
- Destination IP: since all the packets were send to the gaia.cs.umass.edu, the destination IP should always stay constant.
- Differentiated services: as all the packets are ICMP packets, they share the same services, so this field should stay constant.
- Upper layer protocol: as all the packets are ICMP format, they share the same format, so the upper layer protocol field should stay constant.
- Identification: since each packets are different, and they should have something to identify they are different, they should have different ID, so the identification field should be different.
- Time to live: each packets may live different time in the traceroute, so this field should be different
- Header checksum: since the header in each packets may be different, so the header checksum should also be different for each packets.

7.



The pattern of the identification field shows the specific id number for a packet

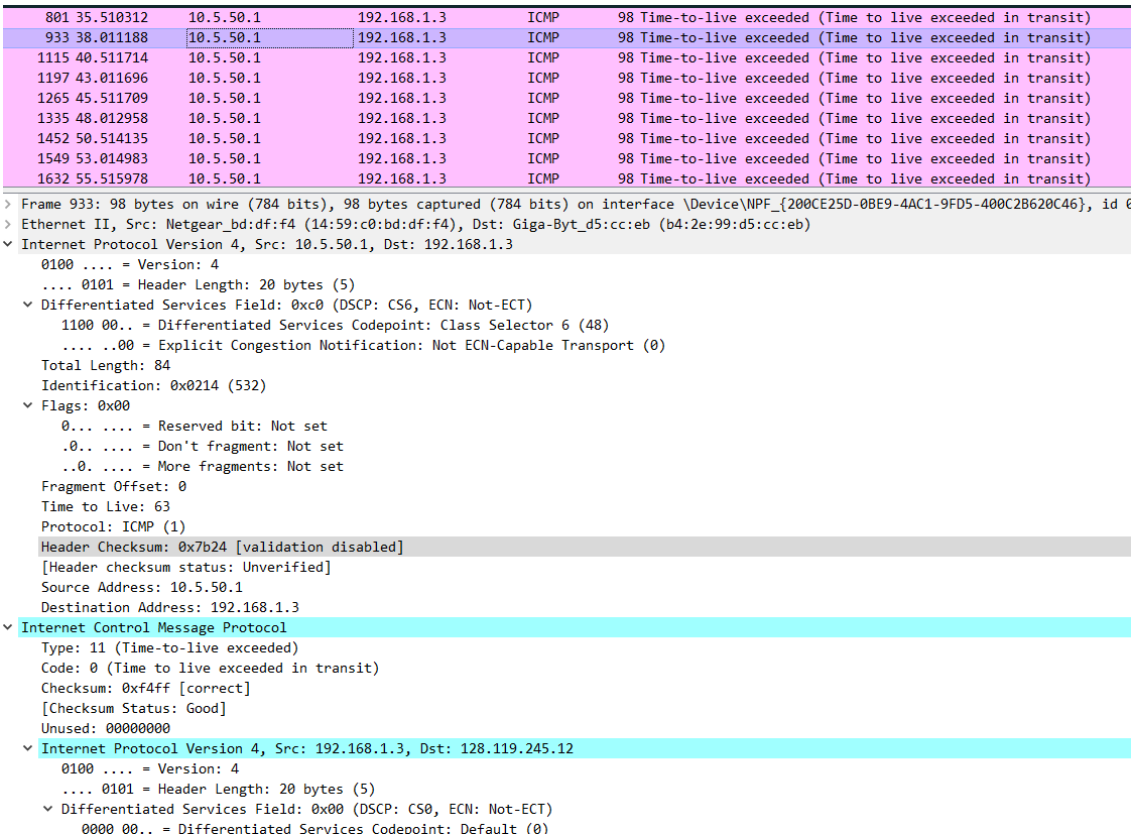
8.

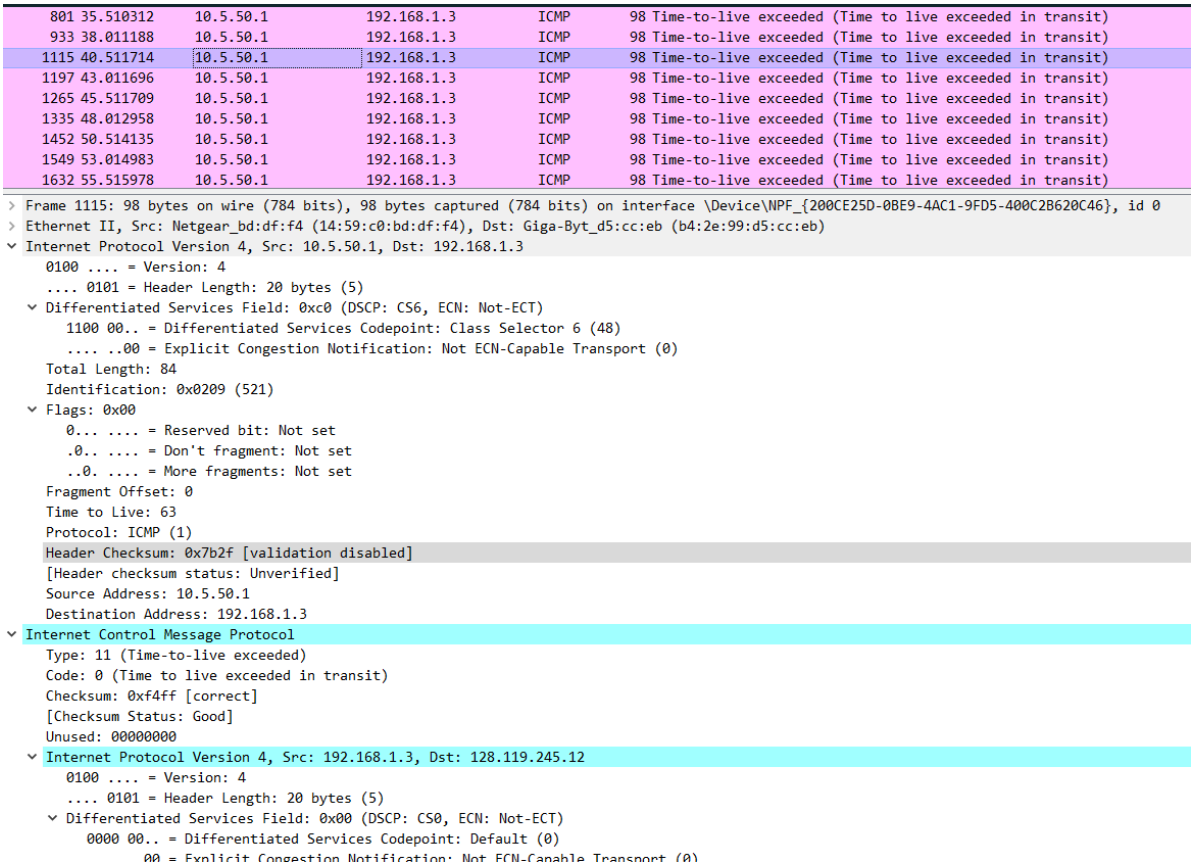


Value in Identification field: 0x0210(528)

Value in time to live field: 63

9.

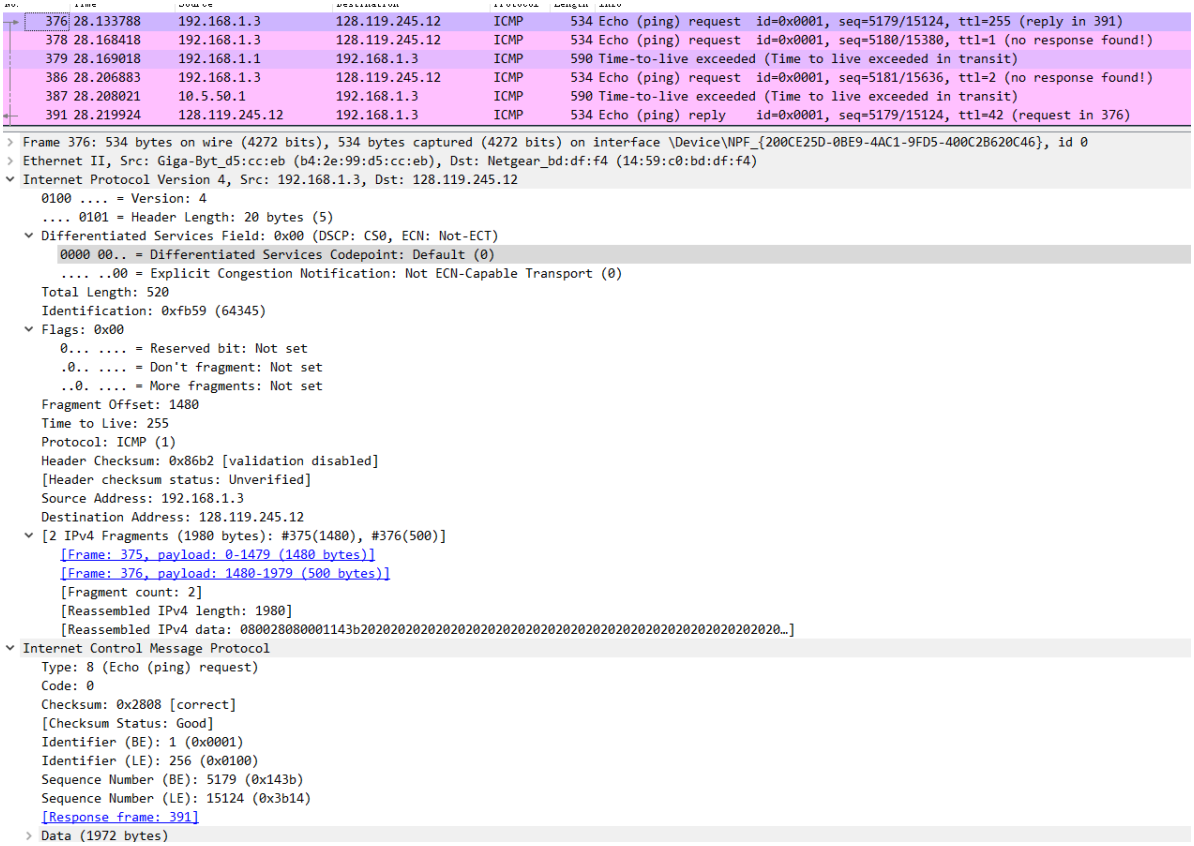




For the identification field, the value always changes to identify different packets.

For the time to live field, since the TTL for the first hop router keep does not change, so the value in this field keep the same and will not change.

10.



Yes, this packet has been fragmented to more than 1 datagram.

11.

```
> Frame 375: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface
> Ethernet II, Src: Giga-Byt_d5:cc:eb (b4:2e:99:d5:cc:eb), Dst: Netgear_bd:df:f4 (14:59:c0:b
v Internet Protocol Version 4, Src: 192.168.1.3, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 1500
    Identification: 0xfb59 (64345)
  v Flags: 0x20, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x6397 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.3
    Destination Address: 128.119.245.12
    [Reassembled IPv4 in frame: 376]
> Data (1480 bytes)
```

The Flags fields shows the packet has been fragmented to more datagrams as there is a 1 in the 'More fragments' field. Since the fragment offset is 0, it indicates that the current datagram is the first fragment, with the length of 1500 bytes.

12.

```
   376 28.133788    192.168.1.3          128.119.245.12       ICMP     534 Echo (ping) request  id=0x0001, seq=5179/15124, ttl=255 (reply in 391)
   378 28.168418    192.168.1.3          128.119.245.12       ICMP     534 Echo (ping) request  id=0x0001, seq=5180/15380, ttl=1 (no response found!)
   379 28.169018    192.168.1.1          192.168.1.3          ICMP     590 Time-to-live exceeded (Time to live exceeded in transit)

> Frame 376: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface \Device\NPF_{200CE25D-0BE9-4AC1-9FD5-400C2B620C46}, id 0
> Ethernet II, Src: Giga-Byt_d5:cc:eb (b4:2e:99:d5:cc:eb), Dst: Netgear_bd:df:f4 (14:59:c0:bd:df:f4)
v Internet Protocol Version 4, Src: 192.168.1.3, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 520
    Identification: 0xfb59 (64345)
  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: 255
    Protocol: ICMP (1)
    Header Checksum: 0x86b2 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.3
    Destination Address: 128.119.245.12
  v [2 IPv4 Fragments (1980 bytes): #375(1480), #376(500)]
      [Frame: 375, payload: 0-1479 (1480 bytes)]
      [Frame: 376, payload: 1480-1979 (500 bytes)]
      [Fragment count: 2]
      [Reassembled IPv4 length: 1980]
      [Reassembled IPv4 data: 08002808000143b2020202020202020202020202020202020202020202020202020202020202020…]
```

In the above graph, as we can find the Fragment offset is 1480, we can tell that this datagram is not the first fragment. Since the 'More fragment' field under the Flags is 0, there is no more fragments.

13. By comparing the above two graves in 11&12, the fields changed between the first and second fragment are: Flags, Fragment offset, header checksum, and total length.

14.

```
> Frame 49: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \
> Ethernet II, Src: Giga-Byt_d5:cc:eb (b4:2e:99:d5:cc:eb), Dst: Netgear_bd:df:f4 (14:59:c0:b
v Internet Protocol Version 4, Src: 192.168.1.3, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 1500
    Identification: 0xfc33 (64563)
  v Flags: 0x20, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x62bd [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.3
    Destination Address: 128.119.245.12
    [Reassembled IPv4 in frame: 51]
> Data (1480 bytes)
```

```
v [3 IPv4 Fragments (3480 bytes): #49(1480), #50(1480), #51(520)]
    [Frame: 49, payload: 0-1479 (1480 bytes)]
    [Frame: 50, payload: 1480-2959 (1480 bytes)]
    [Frame: 51, payload: 2960-3479 (520 bytes)]
    [Fragment count: 3]
    [Reassembled IPv4 length: 3480]
```

There are 3 fragments were created from the original datagram after set the packet size in *pingplotter* to be 3500.

15.

First Fragment:

```
> Frame 49: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \
> Ethernet II, Src: Giga-Byt_d5:cc:eb (b4:2e:99:d5:cc:eb), Dst: Netgear_bd:df:f4 (14:59:c0:b
v Internet Protocol Version 4, Src: 192.168.1.3, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 1500
    Identification: 0xfc33 (64563)
  v Flags: 0x20, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x62bd [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.3
    Destination Address: 128.119.245.12
    [Reassembled IPv4 in frame: 51]
> Data (1480 bytes)
```

Second Fragment:

```
> Frame 50: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \
> Ethernet II, Src: Giga-Byt_d5:cc:eb (b4:2e:99:d5:cc:eb), Dst: Netgear_bd:df:f4 (14:59:c0:b
v Internet Protocol Version 4, Src: 192.168.1.3, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 1500
    Identification: 0xfc33 (64563)
  v Flags: 0x20, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    Fragment Offset: 1480
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x6204 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.3
    Destination Address: 128.119.245.12
    [Reassembled IPv4 in frame: 51]
> Data (1480 bytes)
```

Third Fragment:

```
> Frame 51: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface \Device\NPF_{200CE25D-6
> Ethernet II, Src: Giga-Byt_d5:cc:eb (b4:2e:99:d5:cc:eb), Dst: Netgear_bd:df:f4 (14:59:c0:bd:df:f4)
v Internet Protocol Version 4, Src: 192.168.1.3, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 540
    Identification: 0xfc33 (64563)
  v Flags: 0x01
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 2960
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x850b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.3
    Destination Address: 128.119.245.12
  v [3 IPv4 Fragments (3480 bytes): #49(1480), #50(1480), #51(520)]
      [Frame: 49, payload: 0-1479 (1480 bytes)]
      [Frame: 50, payload: 1480-2959 (1480 bytes)]
      [Frame: 51, payload: 2960-3479 (520 bytes)]
      [Fragment count: 3]
      [Reassembled IPv4 length: 3480]
      [Reassembled IPv4 data: 08000910000115152020202020202020202020202020202020202020202020202020202020…]
```

By comparing the above three graphs, fields changed among the fragments are: Flags, Header checksum, total length. and fragment offset.