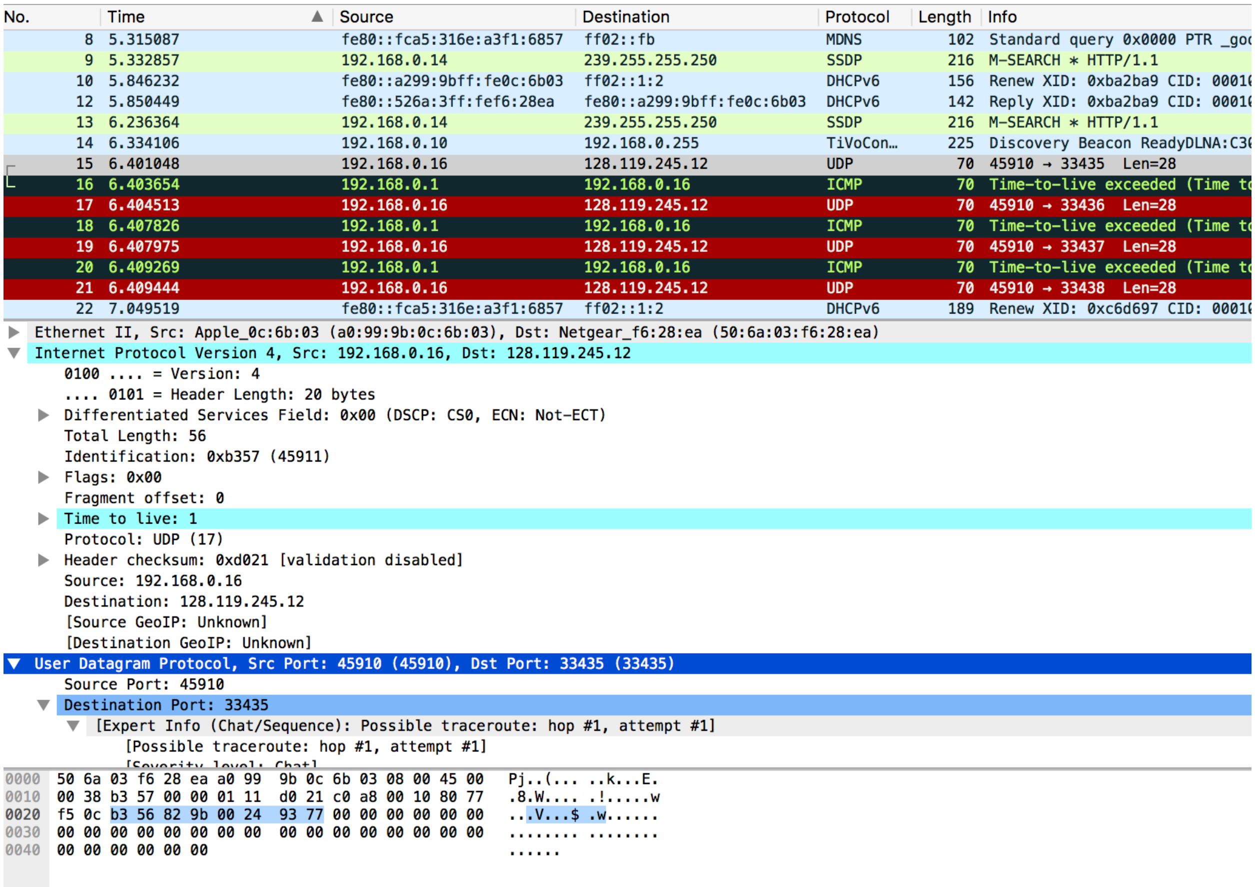
Course: Computer Networks(ECE/CSC 570)
Instructor: Mihail L. Sichitiu
Description: Spring 2016, Wireshark Assignment 2 Solutions.
Student Name: Himangshu Ranjan Borah
Student ID: 200105222
Unity ID: hborah

(All the experiments were performed in a Macintosh Machine which is a Linux based platform. So I used *traceroute* instead of *pingplotter*, hence the Transport Layer protocol will be UDP instead of ICMP for all the answers.)

Answer to Question No. 1



No.	Time	Source	Destination	Protocol	Length	Info
8	5.315087	fe80::fca5:316e:a3f1:6857	ff02::fb	MDNS	102	Standard query 0x0000 PTR _goo
9	5.332857	192.168.0.14	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
10	5.846232	fe80::a299:9bff:fe0c:6b03	ff02::1:2	DHCPv6	156	Renew XID: 0xba2ba9 CID: 0001
12	5.850449	fe80::526a:3ff:fef6:28ea	fe80::a299:9bff:fe0c:6b03	DHCPv6	142	Reply XID: 0xba2ba9 CID: 0001
13	6.236364	192.168.0.14	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
14	6.334106	192.168.0.10	192.168.0.255	TiVoCon…	225	Discovery Beacon ReadyDLNA:C3
15	6.401048	192.168.0.16	128.119.245.12	UDP	70	45910 → 33435 Len=28
16	6.403654	192.168.0.1	192.168.0.16	ICMP	70	Time-to-live exceeded (Time t
17	6.404513	192.168.0.16	128.119.245.12	UDP	70	45910 → 33436 Len=28
18	6.407826	192.168.0.1	192.168.0.16	ICMP	70	Time-to-live exceeded (Time t
19	6.407975	192.168.0.16	128.119.245.12	UDP	70	45910 → 33437 Len=28
20	6.409269	192.168.0.1	192.168.0.16	ICMP	70	Time-to-live exceeded (Time t
21	6.409444	192.168.0.16	128.119.245.12	UDP	70	45910 → 33438 Len=28
22	7.049519	fe80::fca5:316e:a3f1:6857	ff02::1:2	DHCPv6	189	Renew XID: 0xc6d697 CID: 0001

```
▶ Ethernet II, Src: Apple_0c:6b:03 (a0:99:9b:0c:6b:03), Dst: Netgear_f6:28:ea (50:6a:03:f6:28:ea)
▼ Internet Protocol Version 4, Src: 192.168.0.16, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xb357 (45911)
  ▶ Flags: 0x00
    Fragment offset: 0
  ▶ Time to live: 1
    Protocol: UDP (17)
  ▶ Header checksum: 0xd021 [validation disabled]
    Source: 192.168.0.16
    Destination: 128.119.245.12
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▼ User Datagram Protocol, Src Port: 45910 (45910), Dst Port: 33435 (33435)
    Source Port: 45910
  ▼ Destination Port: 33435
    ▼ [Expert Info (Chat/Sequence): Possible traceroute: hop #1, attempt #1]
        [Possible traceroute: hop #1, attempt #1]
        [Severity level: Chat]
```

```
0000  50 6a 03 f6 28 ea a0 99  9b 0c 6b 03 08 00 45 00   Pj..(... ..k...E.
0010  00 38 b3 57 00 00 01 11  d0 21 c0 a8 00 10 80 77   .8.W.... .!.....w
0020  f5 0c b3 56 82 9b 00 24  93 77 00 00 00 00 00 00   ...V...$ .w......
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0040  00 00 00 00 00 00                                  ......
```

We can see that the IP Address of my computer is = **192.168.0.16** (Source in IP header)

Answer to Question No. 2

In the figure above, we can see that the value of the upper layer protocol field is = **17(UDP)**

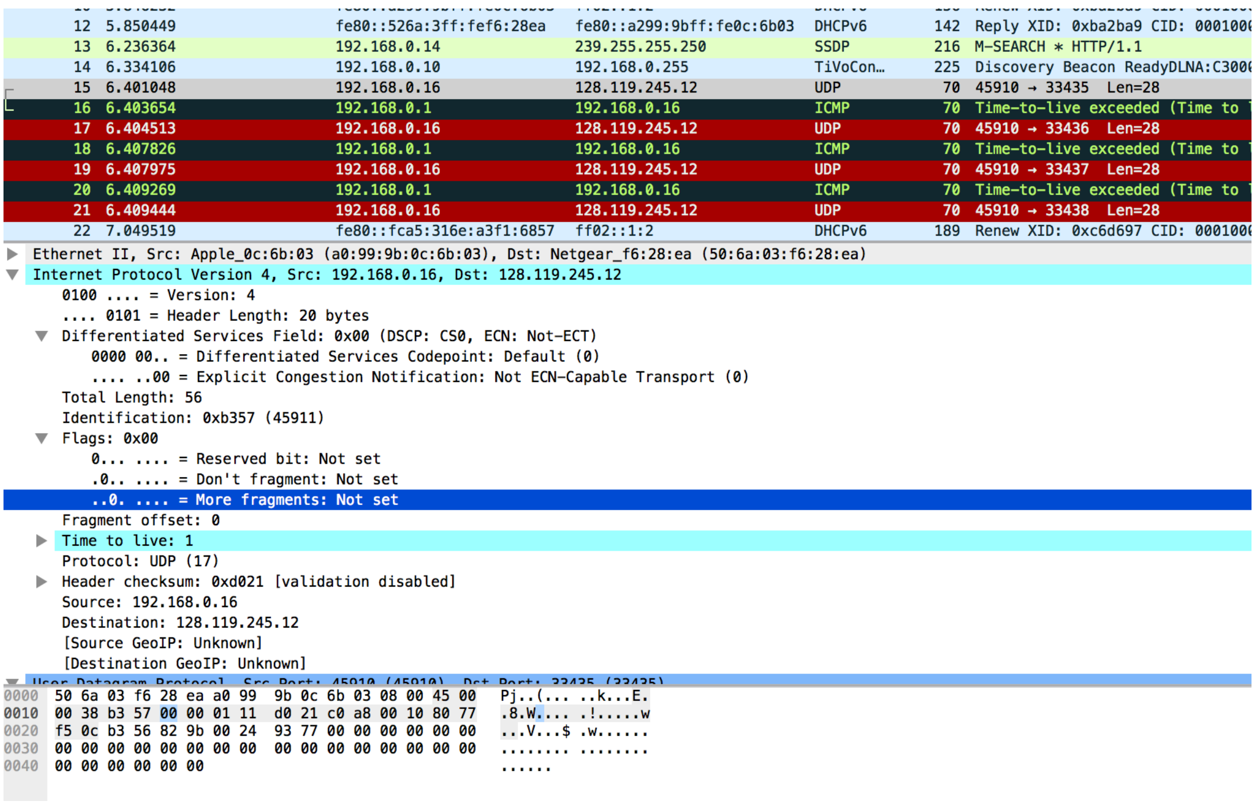
This field is used to identify which upper layer is in action currently so that the destination machine can unwrap it accordingly.

Answer to Question No. 3

From the figure above, the IP header length is = **20 Bytes.**
The payload of the IP Datagram is the actual packet size that is passed form the transport layer to the network layer.

From the IP header, total length = 56 bytes.
Length of IP header = 20 bytes.
hence IP Datagram payload size = 56 - 20 = **36 bytes.**

Answer to Question No. 4



```
12 5.850449   fe80::526a:3ff:fef6:28ea    fe80::a299:9bff:fe0c:6b03  DHCPv6     142 Reply XID: 0xba2ba9 CID: 0001000
13 6.236364   192.168.0.14                239.255.255.250            SSDP       216 M-SEARCH * HTTP/1.1
14 6.334106   192.168.0.10                192.168.0.255              TiVoCon…   225 Discovery Beacon ReadyDLNA:C300
15 6.401048   192.168.0.16                128.119.245.12             UDP         70 45910 → 33435  Len=28
16 6.403654   192.168.0.1                 192.168.0.16               ICMP        70 Time-to-live exceeded (Time to
17 6.404513   192.168.0.16                128.119.245.12             UDP         70 45910 → 33436  Len=28
18 6.407826   192.168.0.1                 192.168.0.16               ICMP        70 Time-to-live exceeded (Time to
19 6.407975   192.168.0.16                128.119.245.12             UDP         70 45910 → 33437  Len=28
20 6.409269   192.168.0.1                 192.168.0.16               ICMP        70 Time-to-live exceeded (Time to
21 6.409444   192.168.0.16                128.119.245.12             UDP         70 45910 → 33438  Len=28
22 7.049519   fe80::fca5:316e:a3f1:6857   ff02::1:2                  DHCPv6     189 Renew XID: 0xc6d697 CID: 0001000
▶ Ethernet II, Src: Apple_0c:6b:03 (a0:99:9b:0c:6b:03), Dst: Netgear_f6:28:ea (50:6a:03:f6:28:ea)
▼ Internet Protocol Version 4, Src: 192.168.0.16, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
  ▼ 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: 56
    Identification: 0xb357 (45911)
  ▼ 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: UDP (17)
  ▶ Header checksum: 0xd021 [validation disabled]
    Source: 192.168.0.16
    Destination: 128.119.245.12
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▼ User Datagram Protocol, Src Port: 45910 (45910), Dst Port: 33435 (33435)
0000  50 6a 03 f6 28 ea a0 99  9b 0c 6b 03 08 00 45 00   Pj..(... ..k...E.
0010  00 38 b3 57 00 00 01 11  d0 21 c0 a8 00 10 80 77   .8.W.... .!.....w
0020  f5 0c b3 56 82 9b 00 24  93 77 00 00 00 00 00 00   ...V...$ .w......
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0040  00 00 00 00 00 00                                  ......
```

From the above screen we see that in the IP Header, the Flag for *More Fragments is "Not Set"* which means that there are no more fragments expected. But it might be true also when this packet is the last one in a fragmentation sequence. So we look for the second clue, the

“Fragment offset” which is **zero** in our case, denoting that the packet is the only one in it’s sequence and hence it **has not been fragmented.**

Answer to Question No. 5

The fields that keep changing between one datagram to the next:

1. Identification.
2. Header Checksum.

For each TTL value, trace route sends 3 packets. So the TTL value will also be changing after every 3 packets.

Answer to Question No. 6

Fields that are constant:

In our case, the packets that we have to check are the UDP packets. The fields that stay constant in the corresponding IP header are:

1. Version
2. Header length
3. Differentiated services
4. Protocol of upper layer
5. Source IP
6. Destination IP
7. Total length

Fields that must stay constant:

The following fields must stay constant.

1. Version
2. Header length
3. Differentiated services
4. Protocol of Upper layer
5. Source IP
6. Destination IP

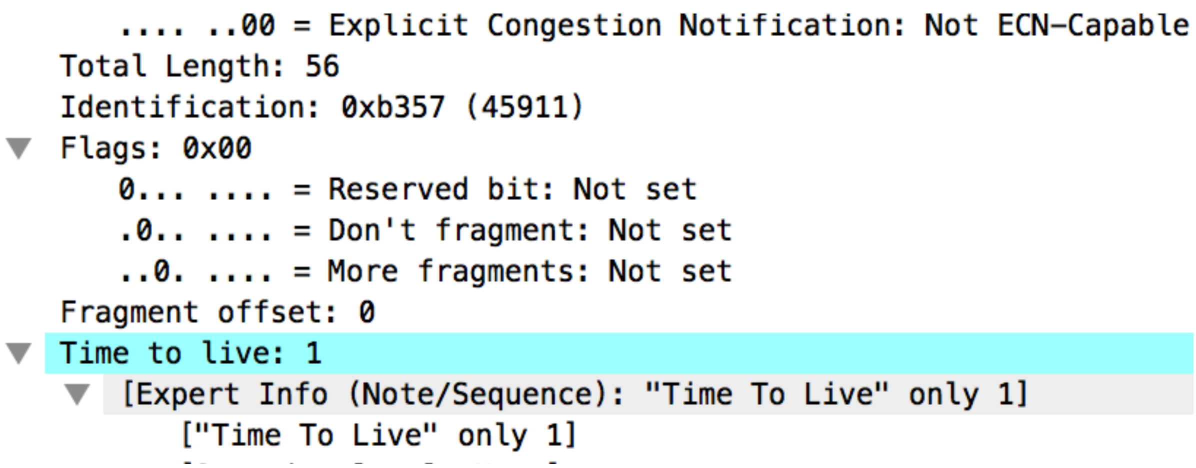
Fields that must change:

The following fields must change.

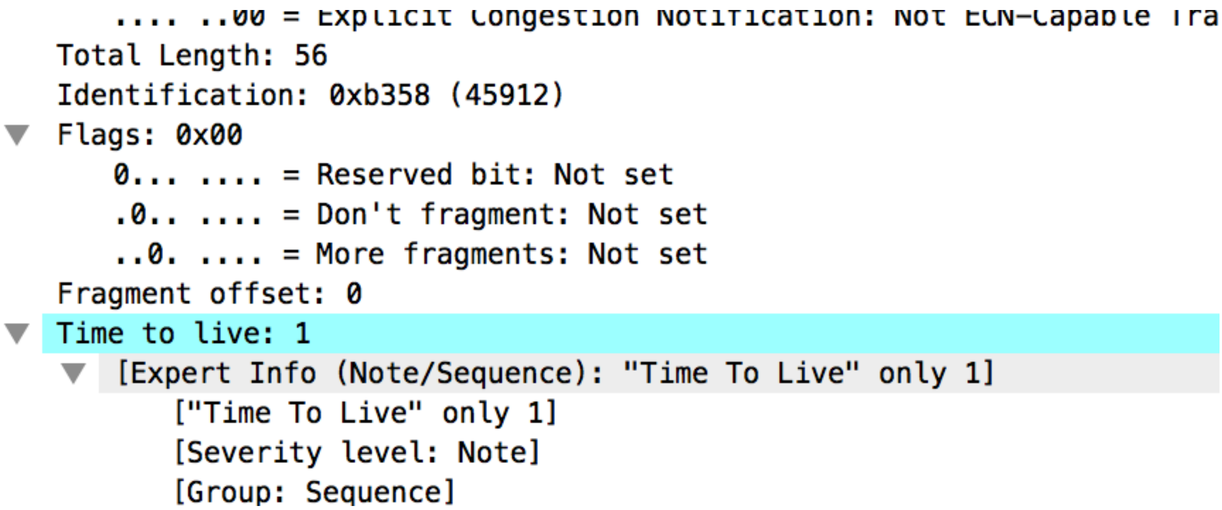
1. Identification
2. Header Checksum
3. Flags(if fragmented)
4. Time to live(TTL)

<u>Answer to Question No. 7</u>

Below are the screenshots from the first two UDP packets.



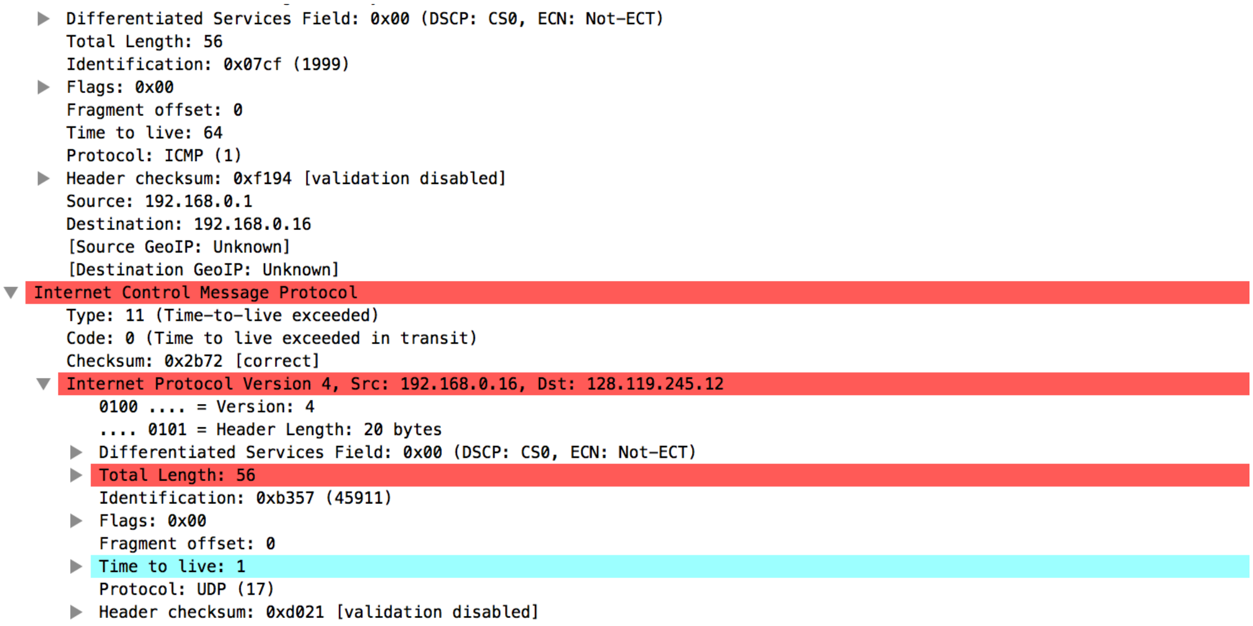
```
     .... ..00 = Explicit Congestion Notification: Not ECN-Capable
  Total Length: 56
  Identification: 0xb357 (45911)
▼ Flags: 0x00
     0... .... = Reserved bit: Not set
     .0.. .... = Don't fragment: Not set
     ..0. .... = More fragments: Not set
  Fragment offset: 0
▼ Time to live: 1
   ▼ [Expert Info (Note/Sequence): "Time To Live" only 1]
        ["Time To Live" only 1]
```



```
     .... ..00 = Explicit Congestion Notification: Not ECN-Capable Tra
  Total Length: 56
  Identification: 0xb358 (45912)
▼ 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
   ▼ [Expert Info (Note/Sequence): "Time To Live" only 1]
        ["Time To Live" only 1]
        [Severity level: Note]
        [Group: Sequence]
```

From the packets, we can see that the identification field is continually increasing by **one** whenever a new packet is being formed and sent out from the system. So, the pattern is that it keeps increasing monotonically.

Answer to Question No. 8



```
   ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 56
     Identification: 0x07cf (1999)
   ▶ Flags: 0x00
     Fragment offset: 0
     Time to live: 64
     Protocol: ICMP (1)
   ▶ Header checksum: 0xf194 [validation disabled]
     Source: 192.168.0.1
     Destination: 192.168.0.16
     [Source GeoIP: Unknown]
     [Destination GeoIP: Unknown]
▼ Internet Control Message Protocol
     Type: 11 (Time-to-live exceeded)
     Code: 0 (Time to live exceeded in transit)
     Checksum: 0x2b72 [correct]
   ▼ Internet Protocol Version 4, Src: 192.168.0.16, Dst: 128.119.245.12
        0100 .... = Version: 4
        .... 0101 = Header Length: 20 bytes
      ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      ▶ Total Length: 56
        Identification: 0xb357 (45911)
      ▶ Flags: 0x00
        Fragment offset: 0
      ▶ Time to live: 1
        Protocol: UDP (17)
      ▶ Header checksum: 0xd021 [validation disabled]
```

From the above screenshot, we can see that the value of the identification field of the ICMP reply is : 1999
From the IP header of the original packet, the ID field of the original packet for which the reply came, is = 45911

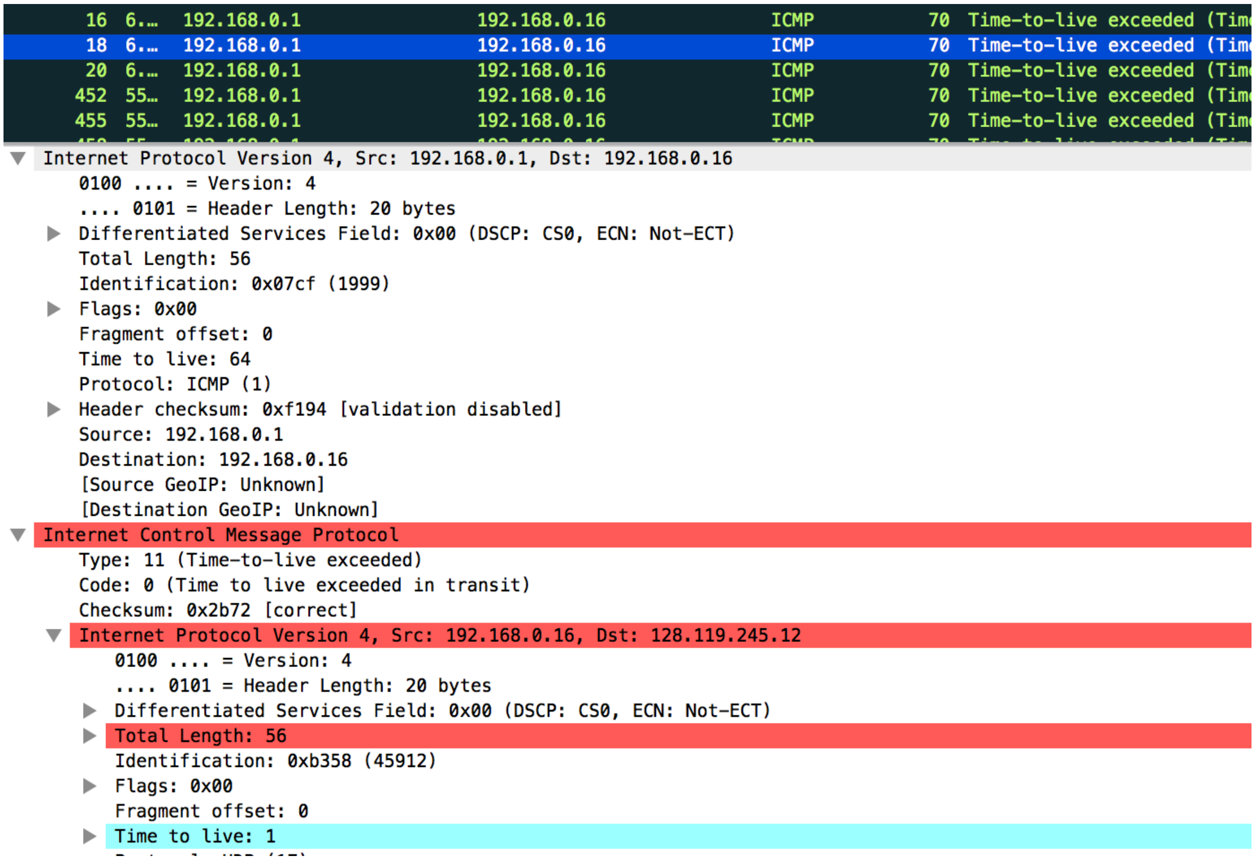
And the value of the TTL field is 64.

Answer to Question No. 9

From the above figure, and it's subsequent packets, we saw that the value of the ID field in the ICMP replies' headers kept unchanged and is 1999. However, analyzing the IP headers of the packets for which the replies came was getting changed by one at a time. So we know that the packets are being sent in order. But for the ICMP replies, the values not getting changed is little weird. As discussed with professor, this might be due to a different implementation of Wireshark capture for macintosh platform in which the experiments were performed.

The TTL values were unchanged too, which was a **normal behavior** as every ICMP reply is a new packet that is been sent from the nearest hop, which has set the TTL field to the max hop of 64.

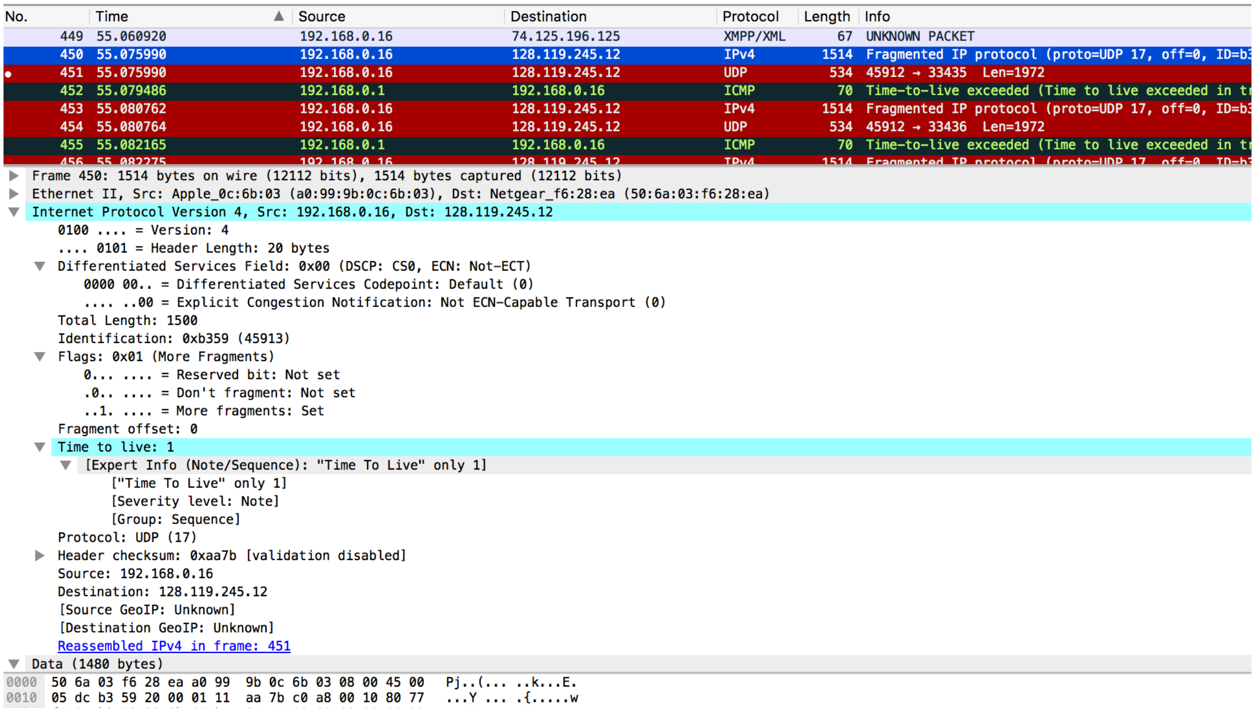
<u>The below is the second ICMP reply for reference:</u>



```
   16  6…   192.168.0.1          192.168.0.16         ICMP        70  Time-to-live exceeded (Tim
   18  6…   192.168.0.1          192.168.0.16         ICMP        70  Time-to-live exceeded (Tim
   20  6…   192.168.0.1          192.168.0.16         ICMP        70  Time-to-live exceeded (Tim
  452  55…  192.168.0.1          192.168.0.16         ICMP        70  Time-to-live exceeded (Tim
  455  55…  192.168.0.1          192.168.0.16         ICMP        70  Time-to-live exceeded (Tim
▼ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.16
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x07cf (1999)
  ▶ Flags: 0x00
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
  ▶ Header checksum: 0xf194 [validation disabled]
    Source: 192.168.0.1
    Destination: 192.168.0.16
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▼ Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0x2b72 [correct]
  ▼ Internet Protocol Version 4, Src: 192.168.0.16, Dst: 128.119.245.12
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes
    ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    ▶ Total Length: 56
      Identification: 0xb358 (45912)
    ▶ Flags: 0x00
      Fragment offset: 0
    ▶ Time to live: 1
```

<u>Answer to Question No. 10</u>

The packet below is the first fragment of the second trace route request with size 2000. We can see that the Flag "More Segments" is set, which denotes that there are more segments of the same packets coming up. Which means that the packet **indeed got fragmented** into more that one IP Datagrams.



```
No.        Time                Source              Destination          Protocol   Length  Info
     449   55.060920           192.168.0.16        74.125.196.125       XMPP/XML       67  UNKNOWN PACKET
     450   55.075990           192.168.0.16        128.119.245.12       IPv4         1514  Fragmented IP protocol (proto=UDP 17, off=0, ID=b3
●    451   55.075990           192.168.0.16        128.119.245.12       UDP           534  45912 → 33435  Len=1972
     452   55.079486           192.168.0.1         192.168.0.16         ICMP           70  Time-to-live exceeded (Time to live exceeded in tr
     453   55.080762           192.168.0.16        128.119.245.12       IPv4         1514  Fragmented IP protocol (proto=UDP 17, off=0, ID=b3
     454   55.080764           192.168.0.16        128.119.245.12       UDP           534  45912 → 33436  Len=1972
     455   55.082165           192.168.0.1         192.168.0.16         ICMP           70  Time-to-live exceeded (Time to live exceeded in tr
     456   55.082275           192.168.0.16        128.119.245.12       IPv4         1514  Fragmented IP protocol (proto=UDP 17, off=0, ID=b3
```

```
▶ Frame 450: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
▶ Ethernet II, Src: Apple_0c:6b:03 (a0:99:9b:0c:6b:03), Dst: Netgear_f6:28:ea (50:6a:03:f6:28:ea)
▼ Internet Protocol Version 4, Src: 192.168.0.16, Dst: 128.119.245.12
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes
   ▼ 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: 0xb359 (45913)
   ▼ 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
      ▼ [Expert Info (Note/Sequence): "Time To Live" only 1]
           ["Time To Live" only 1]
           [Severity level: Note]
           [Group: Sequence]
     Protocol: UDP (17)
   ▶ Header checksum: 0xaa7b [validation disabled]
     Source: 192.168.0.16
     Destination: 128.119.245.12
     [Source GeoIP: Unknown]
     [Destination GeoIP: Unknown]
     Reassembled IPv4 in frame: 451
▼ Data (1480 bytes)
0000  50 6a 03 f6 28 ea a0 99  9b 0c 6b 03 08 00 45 00   Pj..(... ..k...E.
0010  05 dc b3 59 20 00 01 11  aa 7b c0 a8 00 10 80 77   ...Y ... .{.....w
```

Answer to Question No. 11

The snapshot for this answer is same as the previous answer no. 10. The "**More segments**" bit in the flag field indicates that the datagram was fragmented. When this filed is set, it means that there are more fragments coming up, meaning that the datagram was fragmented, which is exactly the case for this datagram.

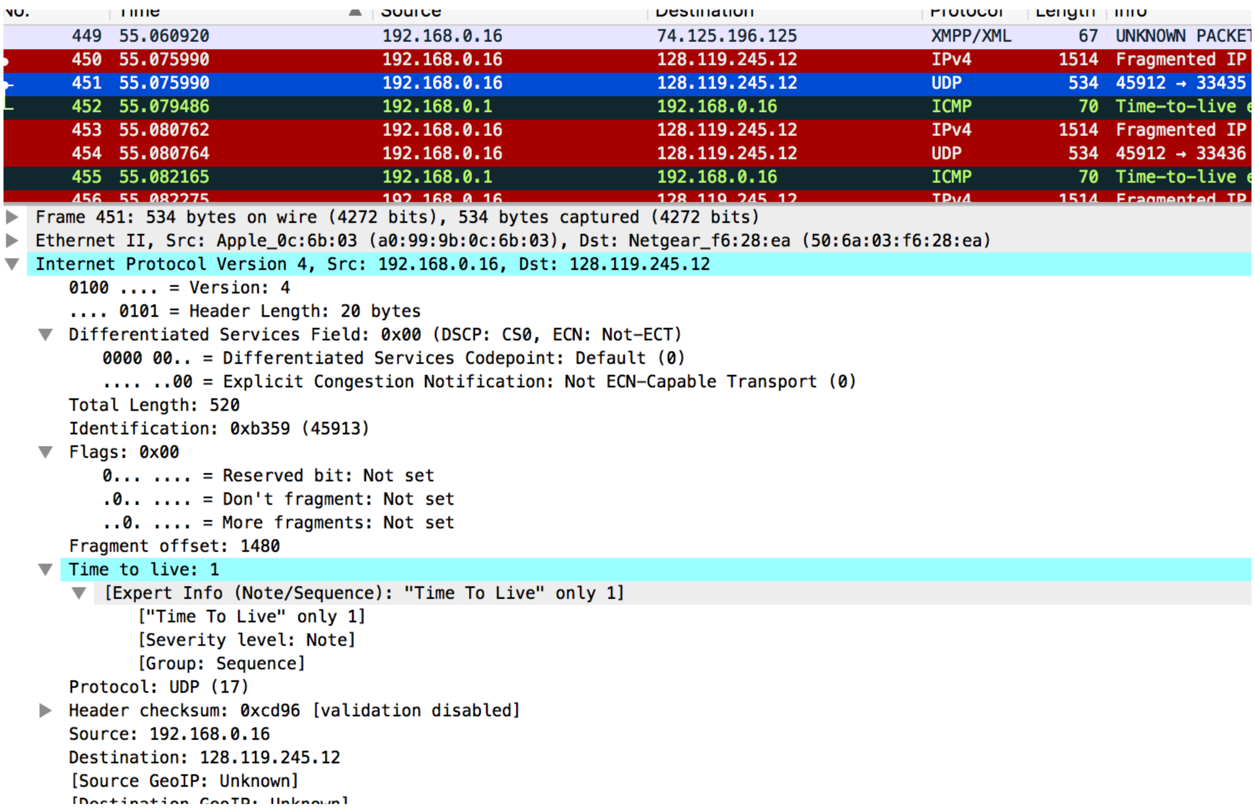
The "**Fragment Offset**" field indicates which part of the actual datagram this particular fragment represents. So when it is 0, then means it's the first fragment in the sequence. If not 0, then it's a latter segment.

The length of this datagram is = **1500 bytes.(MTU Length)**

Answer to Question No. 12

The second fragment is shown below.

The fragment offset is not 0, and is 1480. So as explained earlier, it means that the fragments represents the data starting from the location 1480 and hence it's **not the first fragment.**



```
No.   Time              Source          Destination      Protocol  Length Info
  449 55.060920         192.168.0.16    74.125.196.125   XMPP/XML      67 UNKNOWN PACKET
  450 55.075990         192.168.0.16    128.119.245.12   IPv4        1514 Fragmented IP
  451 55.075990         192.168.0.16    128.119.245.12   UDP          534 45912 → 33435
  452 55.079486         192.168.0.1     192.168.0.16     ICMP          70 Time-to-live e
  453 55.080762         192.168.0.16    128.119.245.12   IPv4        1514 Fragmented IP
  454 55.080764         192.168.0.16    128.119.245.12   UDP          534 45912 → 33436
  455 55.082165         192.168.0.1     192.168.0.16     ICMP          70 Time-to-live e
  456 55.082275         192.168.0.16    128.119.245.12   IPv4        1514 Fragmented IP
▶ Frame 451: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits)
▶ Ethernet II, Src: Apple_0c:6b:03 (a0:99:9b:0c:6b:03), Dst: Netgear_f6:28:ea (50:6a:03:f6:28:ea)
▼ Internet Protocol Version 4, Src: 192.168.0.16, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
  ▼ 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: 0xb359 (45913)
  ▼ 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
    ▼ [Expert Info (Note/Sequence): "Time To Live" only 1]
        ["Time To Live" only 1]
        [Severity level: Note]
        [Group: Sequence]
    Protocol: UDP (17)
  ▶ Header checksum: 0xcd96 [validation disabled]
    Source: 192.168.0.16
    Destination: 128.119.245.12
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

The More fragments field in flag is **Not Set**, which means that there are no more fragments expected. So it must be the last fragment.

Answer to Question No. 13

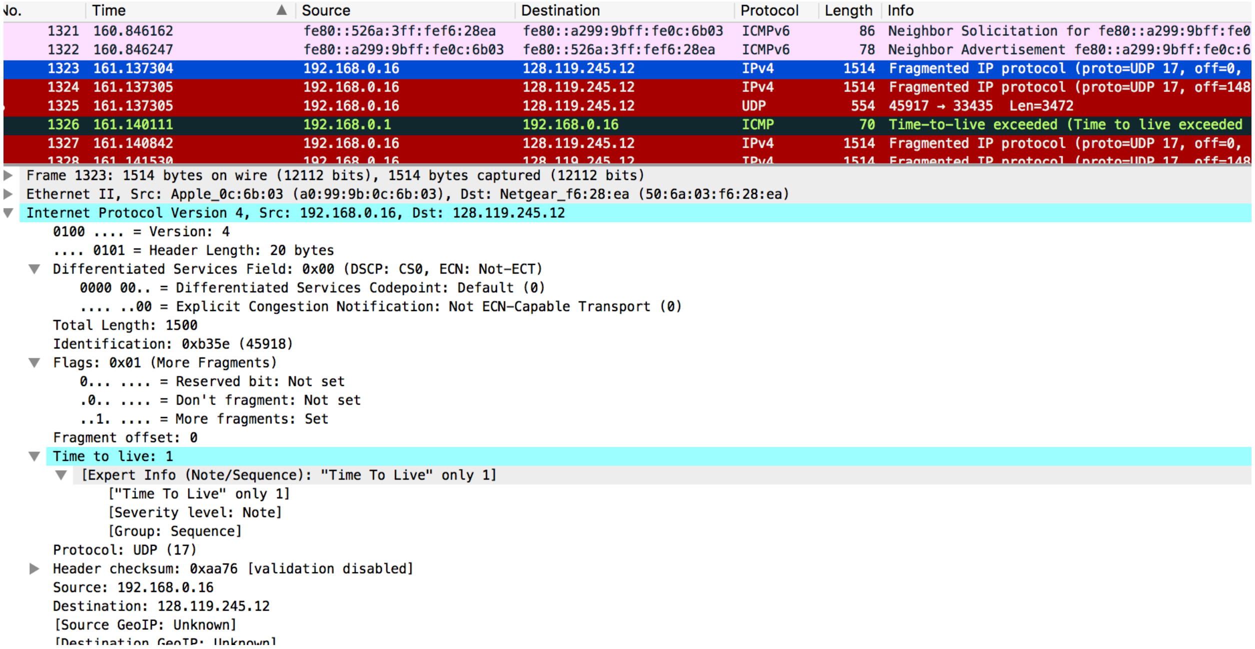
The fields changes are,

1. Fragment Offset
2. More Fragments Bit inside flag field
3. Header Checksum
4. Total Length

Answer to Question No. 14

The 3500 request's first packet.

This packet has been fragmented into **3 parts**. We can see in the figure below that we have two packets of size 1500 and one of size 540.



```
No.     Time         ▲  Source                     Destination                Protocol  Length  Info
   1321 160.846162      fe80::526a:3ff:fef6:28ea   fe80::a299:9bff:fe0c:6b03  ICMPv6        86  Neighbor Solicitation for fe80::a299:9bff:fe0
   1322 160.846247      fe80::a299:9bff:fe0c:6b03  fe80::526a:3ff:fef6:28ea   ICMPv6        78  Neighbor Advertisement fe80::a299:9bff:fe0c:6
   1323 161.137304      192.168.0.16               128.119.245.12             IPv4        1514  Fragmented IP protocol (proto=UDP 17, off=0,
   1324 161.137305      192.168.0.16               128.119.245.12             IPv4        1514  Fragmented IP protocol (proto=UDP 17, off=148
   1325 161.137305      192.168.0.16               128.119.245.12             UDP          554  45917 → 33435  Len=3472
   1326 161.140111      192.168.0.1                192.168.0.16               ICMP          70  Time-to-live exceeded (Time to live exceeded
   1327 161.140842      192.168.0.16               128.119.245.12             IPv4        1514  Fragmented IP protocol (proto=UDP 17, off=0,
   1328 161.141530      192.168.0.16               128.119.245.12             IPv4        1514  Fragmented IP protocol (proto=UDP 17, off=148
▶ Frame 1323: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
▶ Ethernet II, Src: Apple_0c:6b:03 (a0:99:9b:0c:6b:03), Dst: Netgear_f6:28:ea (50:6a:03:f6:28:ea)
▼ Internet Protocol Version 4, Src: 192.168.0.16, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
  ▼ 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: 0xb35e (45918)
  ▼ 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
    ▼ [Expert Info (Note/Sequence): "Time To Live" only 1]
          ["Time To Live" only 1]
          [Severity level: Note]
          [Group: Sequence]
    Protocol: UDP (17)
  ▶ Header checksum: 0xaa76 [validation disabled]
    Source: 192.168.0.16
    Destination: 128.119.245.12
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

The first 2 packets above has the more fragments bit **set** and the last one has the more fragments bit **not set**.

Answer to Question No. 15

The changed fields between all the fragments:

1. Fragment Offset
2. Header Checksum

Between the first 2 fragments and the last segment, we also see a change in the total length and More Fragments bit inside the flag. The total length of the first fragments are 1500 while that of the last one is 540. This fragmentation happens due to the MTU limit. The first 2 packets above has the more fragments bit **set** and the last one has the more fragments bit **not set**.