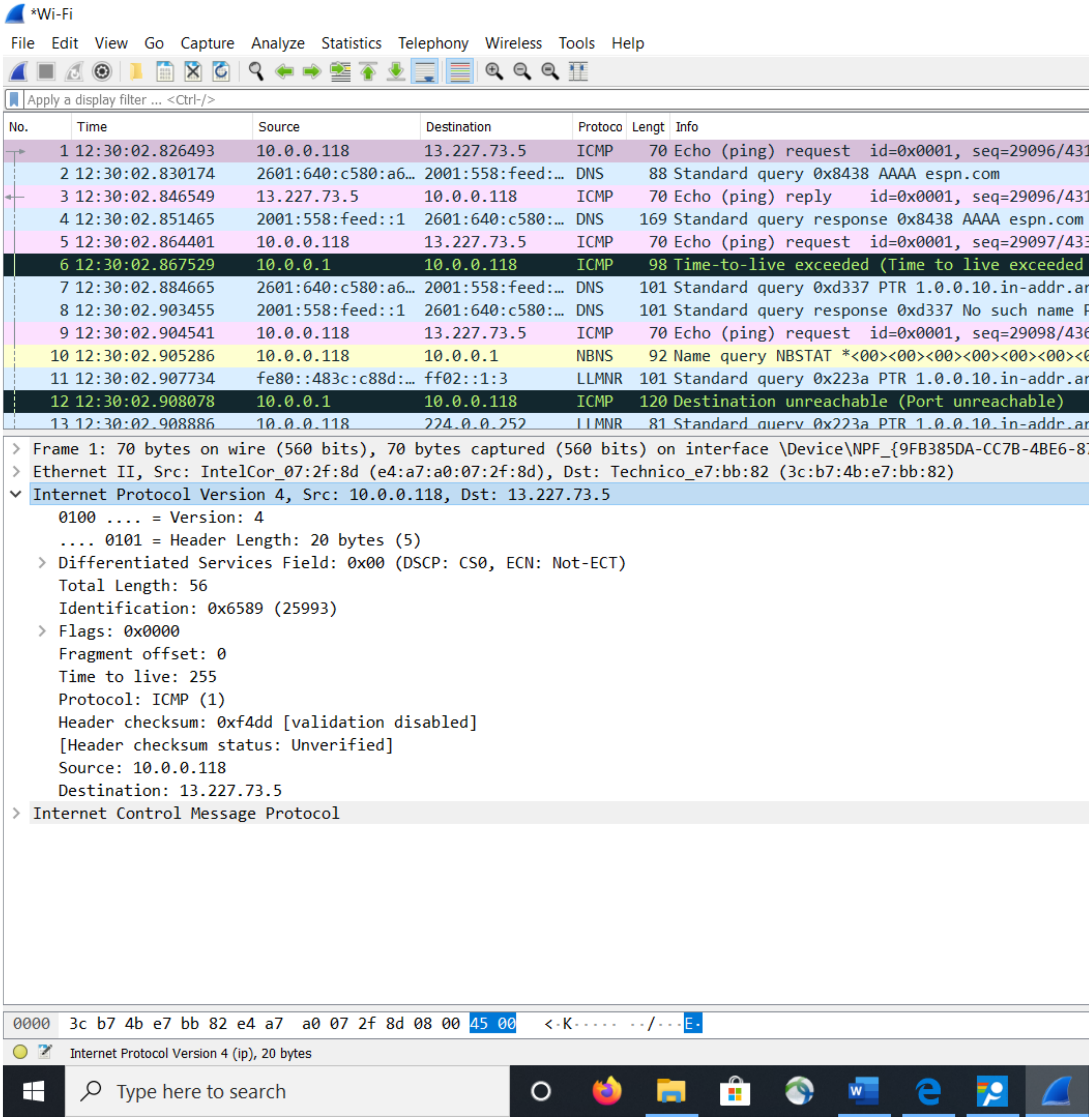
Justin Phillips

cs372 summer2020

Lab4

1. 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?

10.0.0.118 is the IP of my pc


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time             Source               Destination         Protoco Lengt Info
  1 12:30:02.826493   10.0.0.118           13.227.73.5          ICMP    70 Echo (ping) request  id=0x0001, seq=29096/431
  2 12:30:02.830174   2601:640:c580:a6…    2001:558:feed:…      DNS     88 Standard query 0x8438 AAAA espn.com
  3 12:30:02.846549   13.227.73.5          10.0.0.118           ICMP    70 Echo (ping) reply    id=0x0001, seq=29096/431
  4 12:30:02.851465   2001:558:feed::1     2601:640:c580:…      DNS    169 Standard query response 0x8438 AAAA espn.com
  5 12:30:02.864401   10.0.0.118           13.227.73.5          ICMP    70 Echo (ping) request  id=0x0001, seq=29097/43
  6 12:30:02.867529   10.0.0.1             10.0.0.118           ICMP    98 Time-to-live exceeded (Time to live exceeded
  7 12:30:02.884665   2601:640:c580:a6…    2001:558:feed:…      DNS    101 Standard query 0xd337 PTR 1.0.0.10.in-addr.ar
  8 12:30:02.903455   2001:558:feed::1     2601:640:c580:…      DNS    101 Standard query response 0xd337 No such name P
  9 12:30:02.904541   10.0.0.118           13.227.73.5          ICMP    70 Echo (ping) request  id=0x0001, seq=29098/436
 10 12:30:02.905286   10.0.0.118           10.0.0.1             NBNS    92 Name query NBSTAT *<00><00><00><00><00><00><0
 11 12:30:02.907734   fe80::483c:c88d:…    ff02::1:3            LLMNR  101 Standard query 0x223a PTR 1.0.0.10.in-addr.ar
 12 12:30:02.908078   10.0.0.1             10.0.0.118           ICMP   120 Destination unreachable (Port unreachable)
 13 12:30:02.908886   10.0.0.118           224.0.0.252          LLMNR   81 Standard query 0x223a PTR 1.0.0.10.in-addr.ar
```

```
> Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{9FB385DA-CC7B-4BE6-87
> Ethernet II, Src: IntelCor_07:2f:8d (e4:a7:a0:07:2f:8d), Dst: Technico_e7:bb:82 (3c:b7:4b:e7:bb:82)
v Internet Protocol Version 4, Src: 10.0.0.118, Dst: 13.227.73.5
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 56
     Identification: 0x6589 (25993)
   > Flags: 0x0000
     Fragment offset: 0
     Time to live: 255
     Protocol: ICMP (1)
     Header checksum: 0xf4dd [validation disabled]
     [Header checksum status: Unverified]
     Source: 10.0.0.118
     Destination: 13.227.73.5
> Internet Control Message Protocol
```

```
0000  3c b7 4b e7 bb 82 e4 a7  a0 07 2f 8d 08 00 45 00   <·K·····  ··/···E·
```

Internet Protocol Version 4 (ip), 20 bytes

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

Protocol: ICMP (1) (as seen above)

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.

as shown above in 1 the length of the IP header is (.... 0101 = Header Length: 20 bytes (5))

Total Length: 56 bytes - Header Length: 20 bytes (5) = 36 bytes (payload) (as seen above)

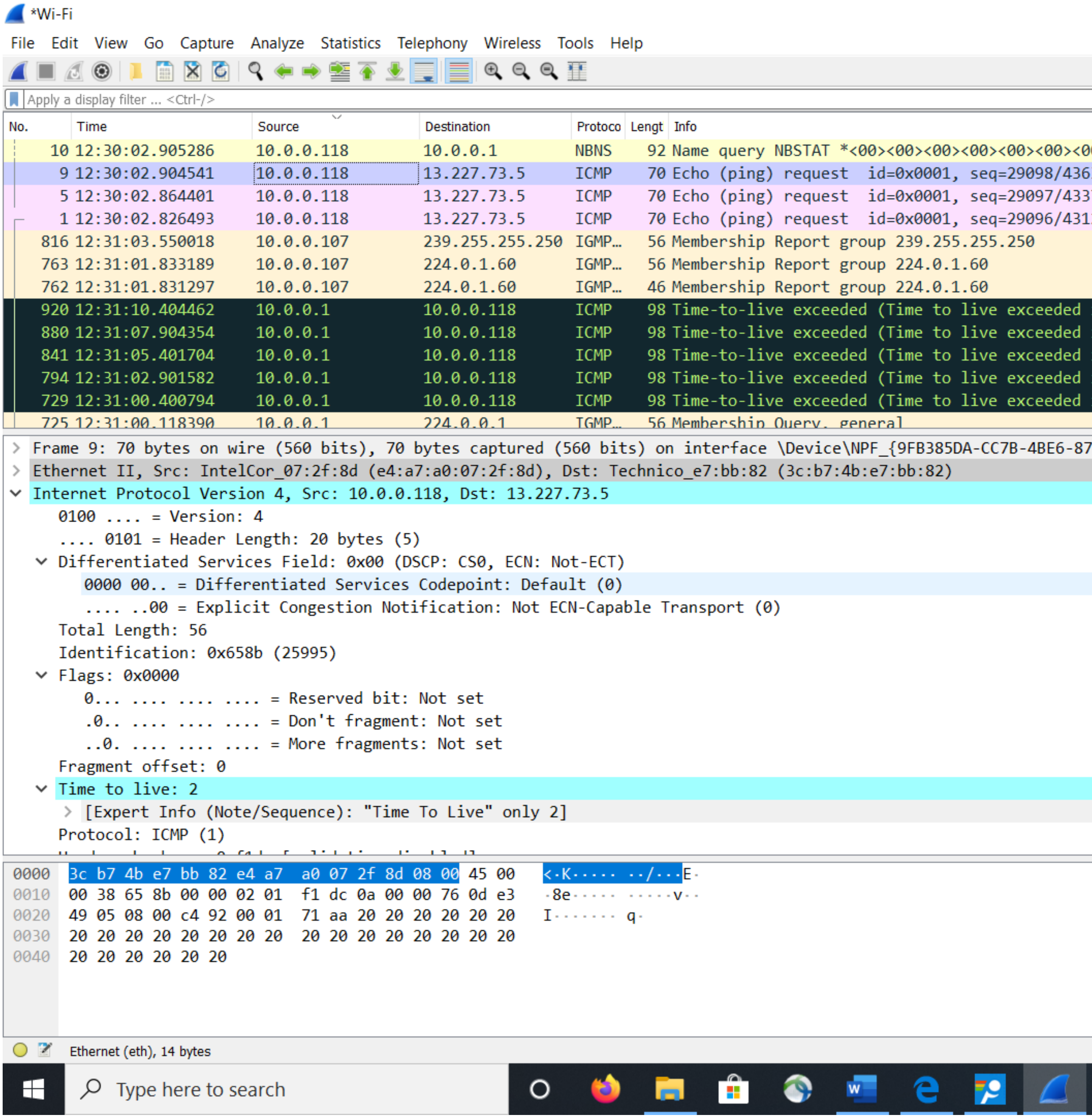
4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

Fragment offset: 0, no it isn't fragment because the bit is set to zero (as seen above)

Next, sort the traced packets according to IP source address by clicking on the Source column header; a small downward pointing arrow should appear next to the word Source. If the arrow points up, click on the Source column header again. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol portion in the "details of selected packet header" window. In the "listing of captured packets" window, you should see all of the subsequent ICMP messages (perhaps with additional interspersed packets sent by other protocols running on your computer) below this first ICMP. Use the down arrow to move through the ICMP messages sent by your computer.

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?

The Time to Live and Identification changes every packet

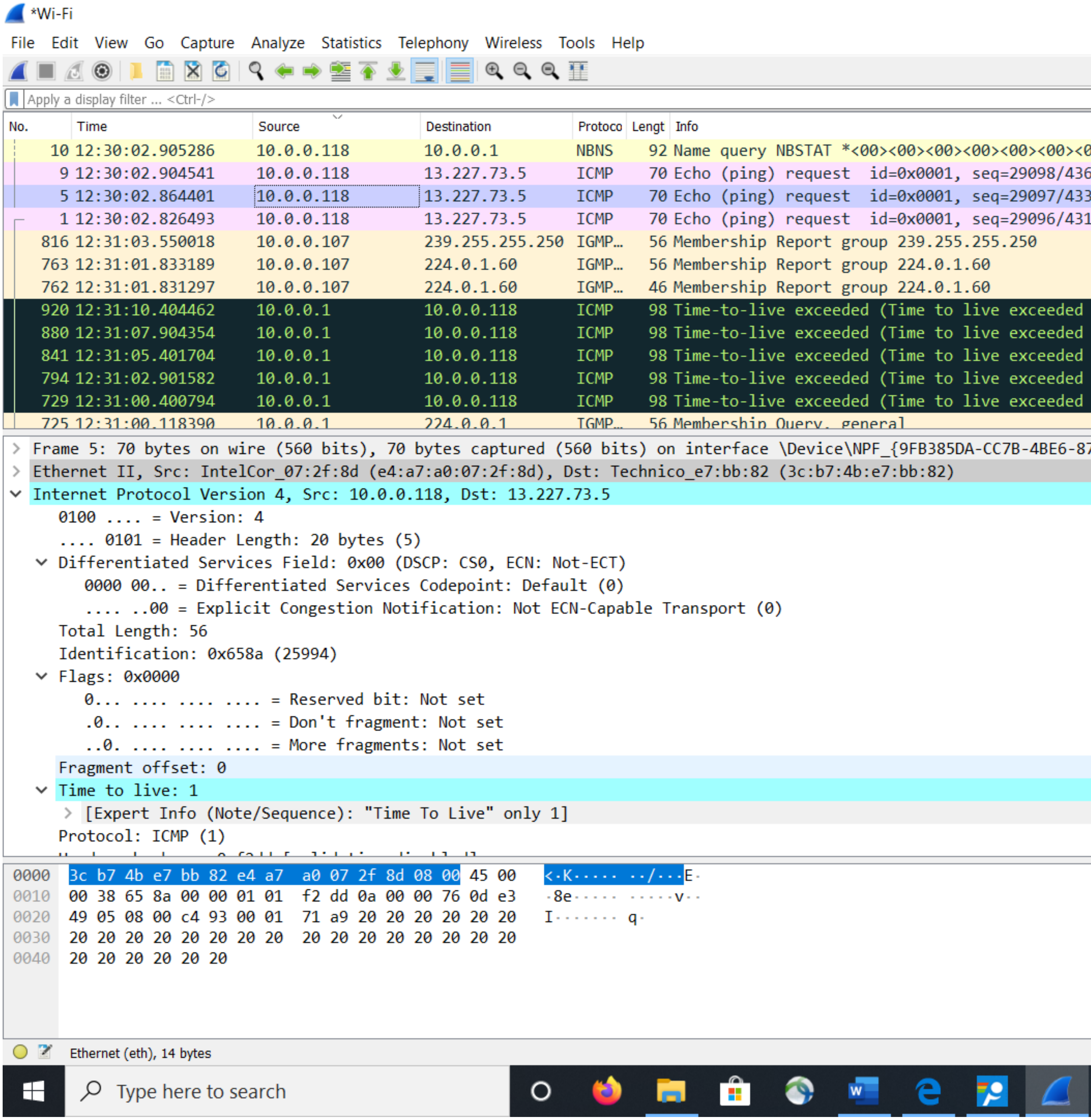

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Type here to search

```
No.    Time             Source        Destination      Protoco Lengt Info
    10 12:30:02.905286  10.0.0.118    10.0.0.1         NBNS     92 Name query NBSTAT *<00><00><00><00><00><00><0
     9 12:30:02.904541  10.0.0.118    13.227.73.5      ICMP     70 Echo (ping) request  id=0x0001, seq=29098/436
     5 12:30:02.864401  10.0.0.118    13.227.73.5      ICMP     70 Echo (ping) request  id=0x0001, seq=29097/433
     1 12:30:02.826493  10.0.0.118    13.227.73.5      ICMP     70 Echo (ping) request  id=0x0001, seq=29096/431
   816 12:31:03.550018  10.0.0.107    239.255.255.250  IGMP...  56 Membership Report group 239.255.255.250
   763 12:31:01.833189  10.0.0.107    224.0.1.60       IGMP...  56 Membership Report group 224.0.1.60
   762 12:31:01.831297  10.0.0.107    224.0.1.60       IGMP...  46 Membership Report group 224.0.1.60
   920 12:31:10.404462  10.0.0.1      10.0.0.118       ICMP     98 Time-to-live exceeded (Time to live exceeded
   880 12:31:07.904354  10.0.0.1      10.0.0.118       ICMP     98 Time-to-live exceeded (Time to live exceeded
   841 12:31:05.401704  10.0.0.1      10.0.0.118       ICMP     98 Time-to-live exceeded (Time to live exceeded
   794 12:31:02.901582  10.0.0.1      10.0.0.118       ICMP     98 Time-to-live exceeded (Time to live exceeded
   729 12:31:00.400794  10.0.0.1      10.0.0.118       ICMP     98 Time-to-live exceeded (Time to live exceeded
   725 12:31:00.118390  10.0.0.1      224.0.0.1        IGMP...  56 Membership Query, general
```

```
> Frame 9: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{9FB385DA-CC7B-4BE6-87
> Ethernet II, Src: IntelCor_07:2f:8d (e4:a7:a0:07:2f:8d), Dst: Technico_e7:bb:82 (3c:b7:4b:e7:bb:82)
v Internet Protocol Version 4, Src: 10.0.0.118, Dst: 13.227.73.5
    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: 56
    Identification: 0x658b (25995)
  v Flags: 0x0000
      0... .... .... .... = Reserved bit: Not set
      .0.. .... .... .... = Don't fragment: Not set
      ..0. .... .... .... = More fragments: Not set
    Fragment offset: 0
  v Time to live: 2
    > [Expert Info (Note/Sequence): "Time To Live" only 2]
    Protocol: ICMP (1)
```

```
0000  3c b7 4b e7 bb 82 e4 a7  a0 07 2f 8d 08 00 45 00   <·K····· ··/···E·
0010  00 38 65 8b 00 00 02 01  f1 dc 0a 00 00 76 0d e3   ·8e····· ·····v··
0020  49 05 08 00 c4 92 00 01  71 aa 20 20 20 20 20 20   I······· q·
0030  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0040  20 20 20 20 20 20
```

Ethernet (eth), 14 bytes


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Type here to search

```
No.   Time             Source       Destination      Protoco Lengt Info
   10 12:30:02.905286  10.0.0.118   10.0.0.1         NBNS     92 Name query NBSTAT *<00><00><00><00><00><00><0
    9 12:30:02.904541  10.0.0.118   13.227.73.5      ICMP     70 Echo (ping) request  id=0x0001, seq=29098/436
    5 12:30:02.864401  10.0.0.118   13.227.73.5      ICMP     70 Echo (ping) request  id=0x0001, seq=29097/433
    1 12:30:02.826493  10.0.0.118   13.227.73.5      ICMP     70 Echo (ping) request  id=0x0001, seq=29096/431
  816 12:31:03.550018  10.0.0.107   239.255.255.250  IGMP…    56 Membership Report group 239.255.255.250
  763 12:31:01.833189  10.0.0.107   224.0.1.60       IGMP…    56 Membership Report group 224.0.1.60
  762 12:31:01.831297  10.0.0.107   224.0.1.60       IGMP…    46 Membership Report group 224.0.1.60
  920 12:31:10.404462  10.0.0.1     10.0.0.118       ICMP     98 Time-to-live exceeded (Time to live exceeded
  880 12:31:07.904354  10.0.0.1     10.0.0.118       ICMP     98 Time-to-live exceeded (Time to live exceeded
  841 12:31:05.401704  10.0.0.1     10.0.0.118       ICMP     98 Time-to-live exceeded (Time to live exceeded
  794 12:31:02.901582  10.0.0.1     10.0.0.118       ICMP     98 Time-to-live exceeded (Time to live exceeded
  729 12:31:00.400794  10.0.0.1     10.0.0.118       ICMP     98 Time-to-live exceeded (Time to live exceeded
  725 12:31:00.118390  10.0.0.1     224.0.0.1        IGMP…    56 Membership Query, general
```

```
> Frame 5: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{9FB385DA-CC7B-4BE6-87
> Ethernet II, Src: IntelCor_07:2f:8d (e4:a7:a0:07:2f:8d), Dst: Technico_e7:bb:82 (3c:b7:4b:e7:bb:82)
v Internet Protocol Version 4, Src: 10.0.0.118, Dst: 13.227.73.5
    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: 56
    Identification: 0x658a (25994)
  v Flags: 0x0000
      0... .... .... .... = Reserved bit: Not set
      .0.. .... .... .... = Don't fragment: Not set
      ..0. .... .... .... = More fragments: Not set
    Fragment offset: 0
  v Time to live: 1
    > [Expert Info (Note/Sequence): "Time To Live" only 1]
    Protocol: ICMP (1)
```

```
0000  3c b7 4b e7 bb 82 e4 a7  a0 07 2f 8d 08 00 45 00   <·K····· ··/···E·
0010  00 38 65 8a 00 00 01 01  f2 dd 0a 00 00 76 0d e3   ·8e····· ·····v··
0020  49 05 08 00 c4 93 00 01  71 a9 20 20 20 20 20 20   I······· q·
0030  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0040  20 20 20 20 20 20
```

Ethernet (eth), 14 bytes

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

the header Length, version, total length, Ip source and dst, differentiated services and protocol all remain constant. The fields that must remain constant are the addresses, version, and header length. The fields that must change are the TTL and identification. These must change because in the TTL this is how we trace the route and Identification changes because this is how we track the datagram. (This is observed in the screen shot above even though it’s a small sample size we can still observe it)

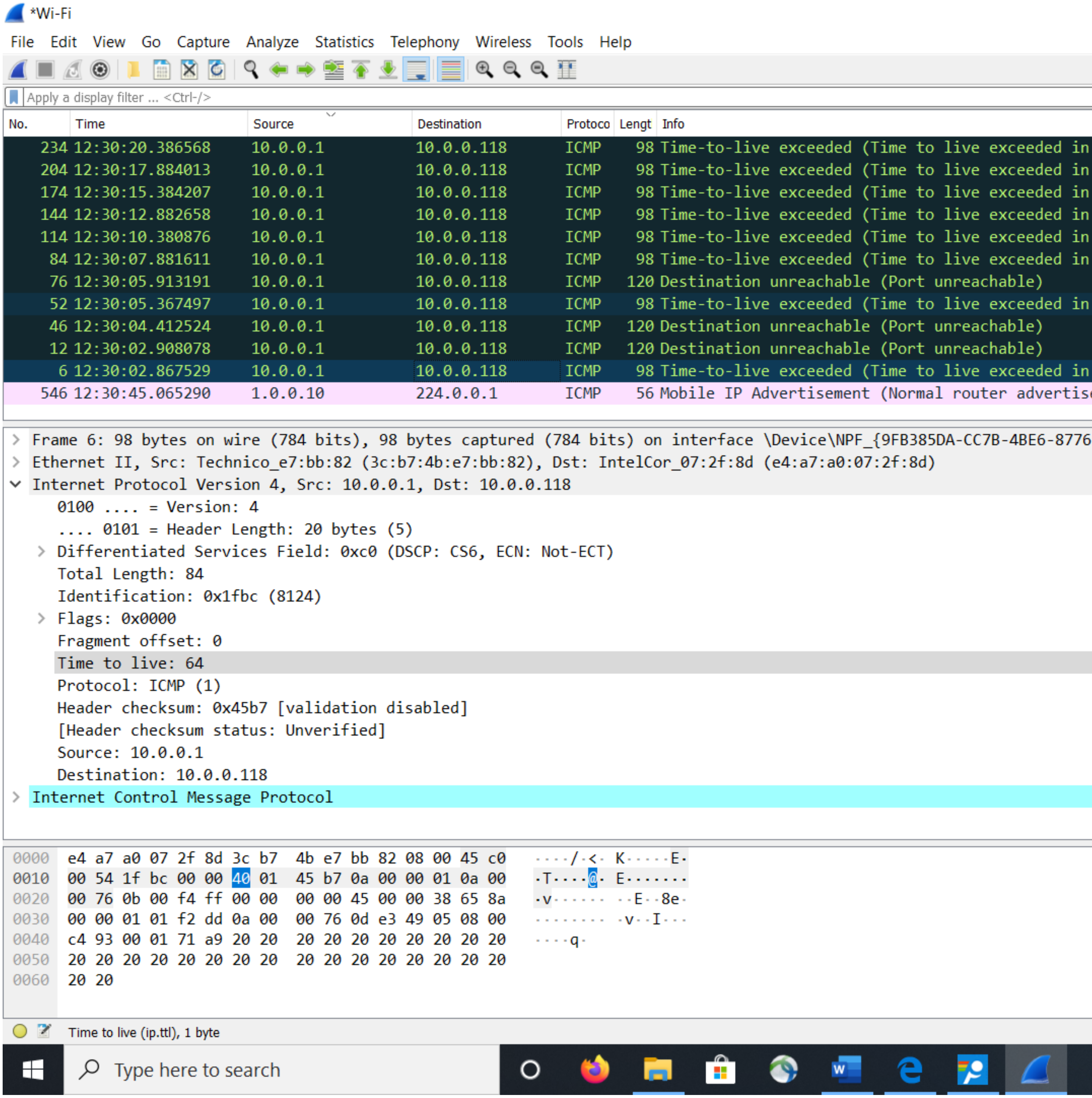
7. Describe the pattern you see in the values in the Identification field of the IP datagram

The next id field gets incremented by 1. (This is observed in the screen shot above)

Next (with the packets still sorted by source address) find the series of ICMP TTL exceeded replies sent to your computer by the nearest (first hop) router.

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

Identification: 0x1fbc (8124) Time to live: 64


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Type here to search

```
No.  Time              Source      Destination  Protoco Lengt Info
 234 12:30:20.386568   10.0.0.1    10.0.0.118   ICMP     98 Time-to-live exceeded (Time to live exceeded in
 204 12:30:17.884013   10.0.0.1    10.0.0.118   ICMP     98 Time-to-live exceeded (Time to live exceeded in
 174 12:30:15.384207   10.0.0.1    10.0.0.118   ICMP     98 Time-to-live exceeded (Time to live exceeded in
 144 12:30:12.882658   10.0.0.1    10.0.0.118   ICMP     98 Time-to-live exceeded (Time to live exceeded in
 114 12:30:10.380876   10.0.0.1    10.0.0.118   ICMP     98 Time-to-live exceeded (Time to live exceeded in
  84 12:30:07.881611   10.0.0.1    10.0.0.118   ICMP     98 Time-to-live exceeded (Time to live exceeded in
  76 12:30:05.913191   10.0.0.1    10.0.0.118   ICMP    120 Destination unreachable (Port unreachable)
  52 12:30:05.367497   10.0.0.1    10.0.0.118   ICMP     98 Time-to-live exceeded (Time to live exceeded in
  46 12:30:04.412524   10.0.0.1    10.0.0.118   ICMP    120 Destination unreachable (Port unreachable)
  12 12:30:02.908078   10.0.0.1    10.0.0.118   ICMP    120 Destination unreachable (Port unreachable)
   6 12:30:02.867529   10.0.0.1    10.0.0.118   ICMP     98 Time-to-live exceeded (Time to live exceeded in
 546 12:30:45.065290   1.0.0.10    224.0.0.1    ICMP     56 Mobile IP Advertisement (Normal router advertis
```

```
> Frame 6: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{9FB385DA-CC7B-4BE6-8776
> Ethernet II, Src: Technico_e7:bb:82 (3c:b7:4b:e7:bb:82), Dst: IntelCor_07:2f:8d (e4:a7:a0:07:2f:8d)
v Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.118
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x1fbc (8124)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x45b7 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.0.1
    Destination: 10.0.0.118
> Internet Control Message Protocol
```

```
0000  e4 a7 a0 07 2f 8d 3c b7  4b e7 bb 82 08 00 45 c0   ····/·<· K·····E·
0010  00 54 1f bc 00 00 40 01  45 b7 0a 00 00 01 0a 00   ·T····@· E·······
0020  00 76 0b 00 f4 ff 00 00  00 00 45 00 00 38 65 8a   ·v······ ··E··8e·
0030  00 00 01 01 f2 dd 0a 00  00 76 0d e3 49 05 08 00   ········ ·v··I···
0040  c4 93 00 01 71 a9 20 20  20 20 20 20 20 20 20 20   ····q·
0050  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0060  20 20
```

Time to live (ip.ttl), 1 byte

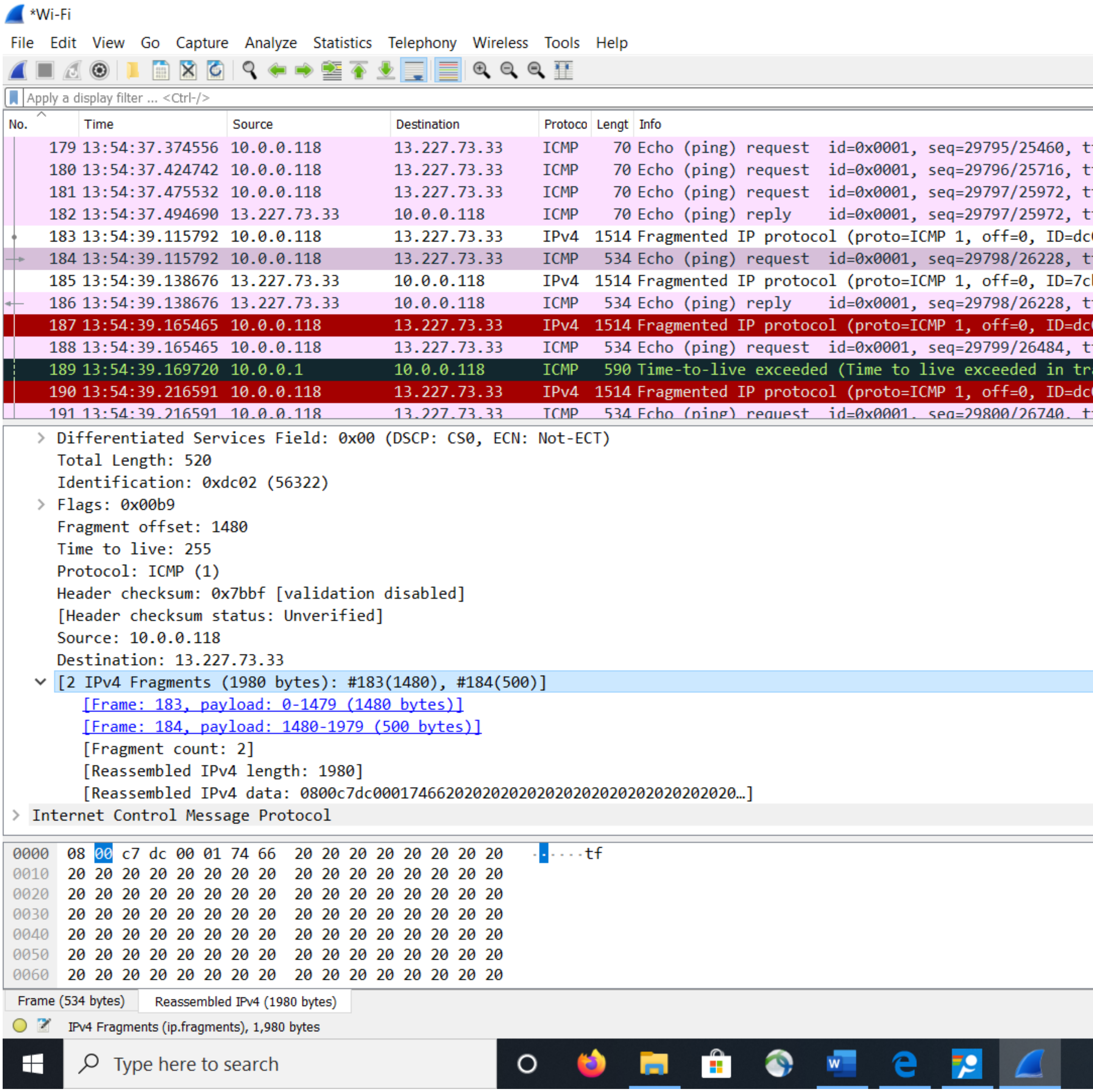
9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

The TTL remains the same because it hasn’t left this hop yet.

Fragmentation, Sort the packet listing according to time again by clicking on the Time column.

10. 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?

The packet has been fragmented across more then one datagram


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time             Source        Destination    Protoco Lengt Info
  179 13:54:37.374556  10.0.0.118    13.227.73.33   ICMP      70 Echo (ping) request  id=0x0001, seq=29795/25460, t
  180 13:54:37.424742  10.0.0.118    13.227.73.33   ICMP      70 Echo (ping) request  id=0x0001, seq=29796/25716, t
  181 13:54:37.475532  10.0.0.118    13.227.73.33   ICMP      70 Echo (ping) request  id=0x0001, seq=29797/25972, t
  182 13:54:37.494690  13.227.73.33  10.0.0.118     ICMP      70 Echo (ping) reply    id=0x0001, seq=29797/25972, t
  183 13:54:39.115792  10.0.0.118    13.227.73.33   IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=dc
  184 13:54:39.115792  10.0.0.118    13.227.73.33   ICMP     534 Echo (ping) request  id=0x0001, seq=29798/26228, t
  185 13:54:39.138676  13.227.73.33  10.0.0.118     IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=7c
  186 13:54:39.138676  13.227.73.33  10.0.0.118     ICMP     534 Echo (ping) reply    id=0x0001, seq=29798/26228, t
  187 13:54:39.165465  10.0.0.118    13.227.73.33   IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=dc
  188 13:54:39.165465  10.0.0.118    13.227.73.33   ICMP     534 Echo (ping) request  id=0x0001, seq=29799/26484, t
  189 13:54:39.169720  10.0.0.1      10.0.0.118     ICMP     590 Time-to-live exceeded (Time to live exceeded in tr
  190 13:54:39.216591  10.0.0.118    13.227.73.33   IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=dc
  191 13:54:39.216591  10.0.0.118    13.227.73.33   ICMP     534 Echo (ping) request  id=0x0001, seq=29800/26740, t
```

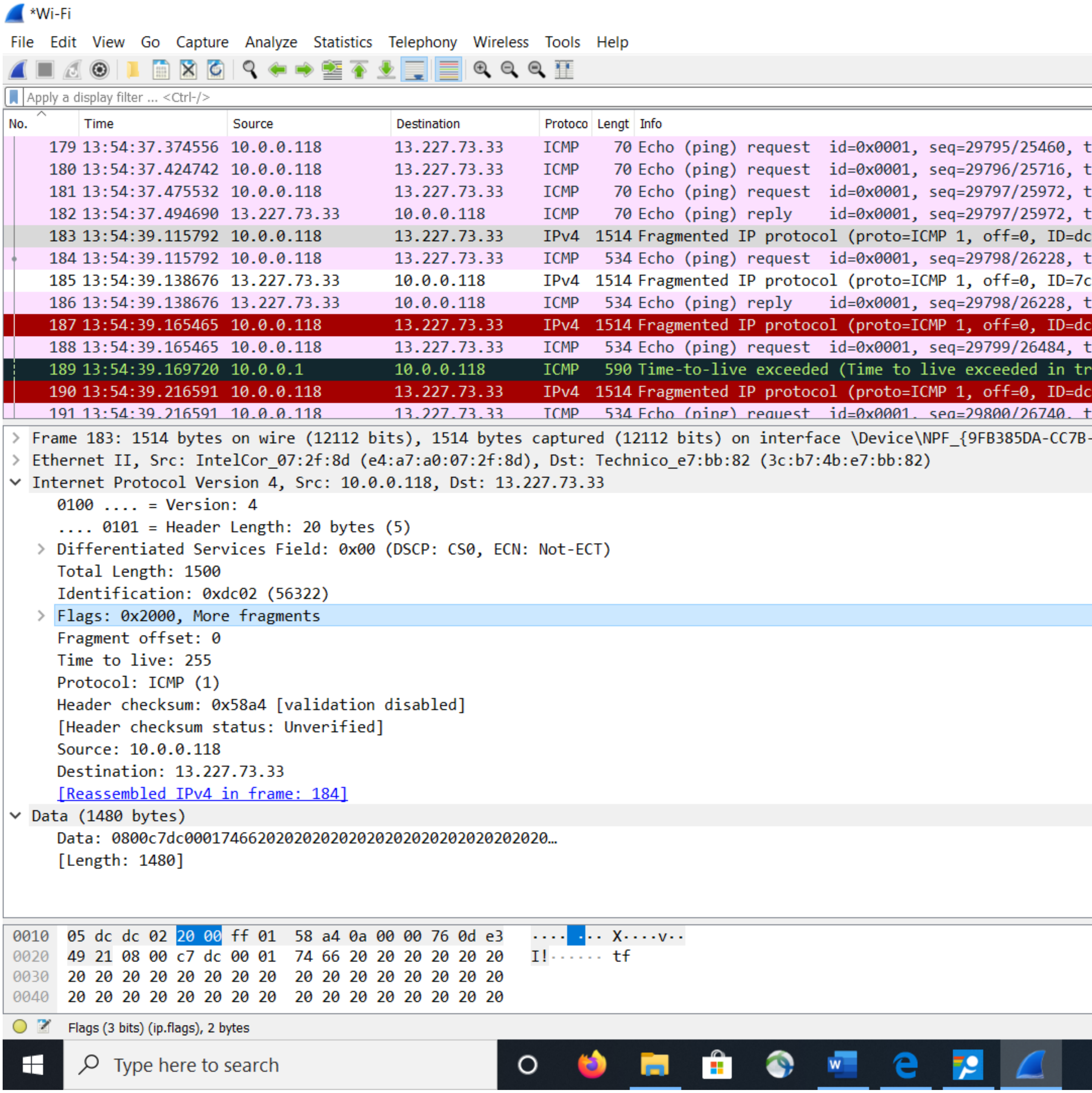
```
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 520
    Identification: 0xdc02 (56322)
  > Flags: 0x00b9
    Fragment offset: 1480
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x7bbf [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.0.118
    Destination: 13.227.73.33
  v [2 IPv4 Fragments (1980 bytes): #183(1480), #184(500)]
       [Frame: 183, payload: 0-1479 (1480 bytes)]
       [Frame: 184, payload: 1480-1979 (500 bytes)]
       [Fragment count: 2]
       [Reassembled IPv4 length: 1980]
       [Reassembled IPv4 data: 0800c7dc00017466202020202020202020202020202020…]
> Internet Control Message Protocol
```

```
0000  08 00 c7 dc 00 01 74 66  20 20 20 20 20 20 20 20   ······tf
0010  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0020  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0030  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0040  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0050  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0060  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
```

Frame (534 bytes)
Reassembled IPv4 (1980 bytes)
IPv4 Fragments (ip.fragments), 1,980 bytes
Type here to search

11. Screenshot the first fragment of the fragmented IP datagram (with sufficient details to answer these questions). 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?

In flags it states that that there's more fragments, the frag offset is set to zero and the total length of this is 1500 – 20 (header) = 1480bytes of data


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Type here to search

```
No.   Time             Source        Destination   Protoco Lengt Info
  179 13:54:37.374556  10.0.0.118    13.227.73.33  ICMP      70 Echo (ping) request  id=0x0001, seq=29795/25460, t
  180 13:54:37.424742  10.0.0.118    13.227.73.33  ICMP      70 Echo (ping) request  id=0x0001, seq=29796/25716, t
  181 13:54:37.475532  10.0.0.118    13.227.73.33  ICMP      70 Echo (ping) request  id=0x0001, seq=29797/25972, t
  182 13:54:37.494690  13.227.73.33  10.0.0.118    ICMP      70 Echo (ping) reply    id=0x0001, seq=29797/25972, t
  183 13:54:39.115792  10.0.0.118    13.227.73.33  IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=dc
  184 13:54:39.115792  10.0.0.118    13.227.73.33  ICMP     534 Echo (ping) request  id=0x0001, seq=29798/26228, t
  185 13:54:39.138676  13.227.73.33  10.0.0.118    IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=7c
  186 13:54:39.138676  13.227.73.33  10.0.0.118    ICMP     534 Echo (ping) reply    id=0x0001, seq=29798/26228, t
  187 13:54:39.165465  10.0.0.118    13.227.73.33  IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=dc
  188 13:54:39.165465  10.0.0.118    13.227.73.33  ICMP     534 Echo (ping) request  id=0x0001, seq=29799/26484, t
  189 13:54:39.169720  10.0.0.1      10.0.0.118    ICMP     590 Time-to-live exceeded (Time to live exceeded in tr
  190 13:54:39.216591  10.0.0.118    13.227.73.33  IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=dc
  191 13:54:39.216591  10.0.0.118    13.227.73.33  ICMP     534 Echo (ping) request  id=0x0001, seq=29800/26740, t
```

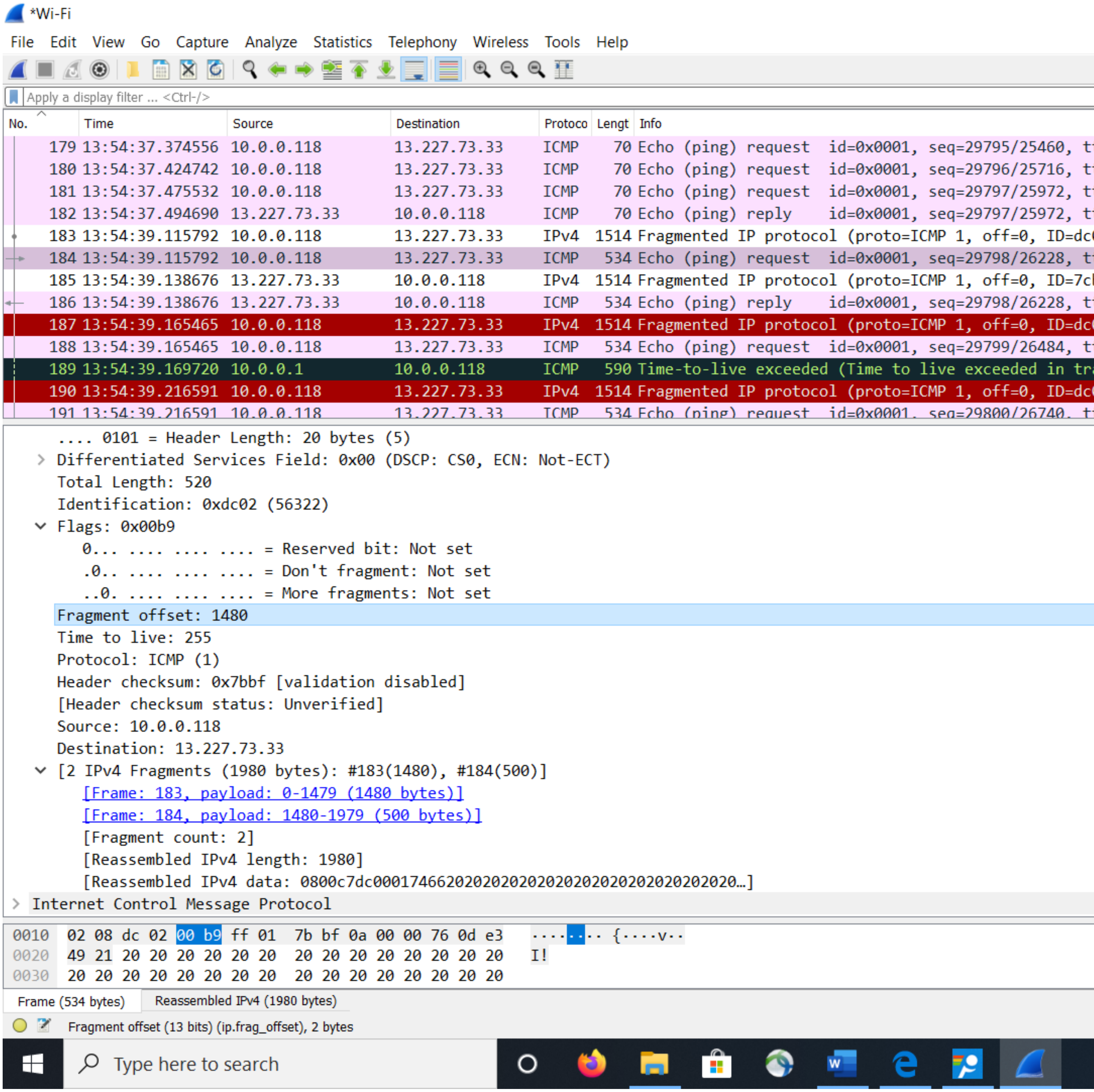
```
> Frame 183: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{9FB385DA-CC7B-
> Ethernet II, Src: IntelCor_07:2f:8d (e4:a7:a0:07:2f:8d), Dst: Technico_e7:bb:82 (3c:b7:4b:e7:bb:82)
v Internet Protocol Version 4, Src: 10.0.0.118, Dst: 13.227.73.33
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 1500
     Identification: 0xdc02 (56322)
   > Flags: 0x2000, More fragments
     Fragment offset: 0
     Time to live: 255
     Protocol: ICMP (1)
     Header checksum: 0x58a4 [validation disabled]
     [Header checksum status: Unverified]
     Source: 10.0.0.118
     Destination: 13.227.73.33
     [Reassembled IPv4 in frame: 184]
v Data (1480 bytes)
     Data: 0800c7dc00017466202020202020202020202020202020…
     [Length: 1480]
```

```
0010  05 dc dc 02 20 00 ff 01  58 a4 0a 00 00 76 0d e3   ···· ··· X····v··
0020  49 21 08 00 c7 dc 00 01  74 66 20 20 20 20 20 20   I!······ tf
0030  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0040  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
```

Flags (3 bits) (ip.flags), 2 bytes

12. Screenshot the second fragment of the fragmented IP datagram (with sufficient details to answer these questions). What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?

The info stating that it isn't the 1st datagram is the offset is set to 1480 and it also states that there are 2 payloads in the fragment section



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time            Source         Destination    Protoco Lengt Info
  179 13:54:37.374556 10.0.0.118     13.227.73.33   ICMP      70 Echo (ping) request  id=0x0001, seq=29795/25460, t
  180 13:54:37.424742 10.0.0.118     13.227.73.33   ICMP      70 Echo (ping) request  id=0x0001, seq=29796/25716, t
  181 13:54:37.475532 10.0.0.118     13.227.73.33   ICMP      70 Echo (ping) request  id=0x0001, seq=29797/25972, t
  182 13:54:37.494690 13.227.73.33   10.0.0.118     ICMP      70 Echo (ping) reply    id=0x0001, seq=29797/25972, t
  183 13:54:39.115792 10.0.0.118     13.227.73.33   IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=dc
  184 13:54:39.115792 10.0.0.118     13.227.73.33   ICMP     534 Echo (ping) request  id=0x0001, seq=29798/26228, t
  185 13:54:39.138676 13.227.73.33   10.0.0.118     IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=7c
  186 13:54:39.138676 13.227.73.33   10.0.0.118     ICMP     534 Echo (ping) reply    id=0x0001, seq=29798/26228, t
  187 13:54:39.165465 10.0.0.118     13.227.73.33   IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=dc
  188 13:54:39.165465 10.0.0.118     13.227.73.33   ICMP     534 Echo (ping) request  id=0x0001, seq=29799/26484, t
  189 13:54:39.169720 10.0.0.1       10.0.0.118     ICMP     590 Time-to-live exceeded (Time to live exceeded in tr
  190 13:54:39.216591 10.0.0.118     13.227.73.33   IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=dc
  191 13:54:39.216591 10.0.0.118     13.227.73.33   ICMP     534 Echo (ping) request  id=0x0001, seq=29800/26740, t
```

```
      .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 520
      Identification: 0xdc02 (56322)
    v Flags: 0x00b9
        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: 0x7bbf [validation disabled]
      [Header checksum status: Unverified]
      Source: 10.0.0.118
      Destination: 13.227.73.33
    v [2 IPv4 Fragments (1980 bytes): #183(1480), #184(500)]
        [Frame: 183, payload: 0-1479 (1480 bytes)]
        [Frame: 184, payload: 1480-1979 (500 bytes)]
        [Fragment count: 2]
        [Reassembled IPv4 length: 1980]
        [Reassembled IPv4 data: 0800c7dc0001746620202020202020202020202020202020…]
  > Internet Control Message Protocol
```

```
0010  02 08 dc 02 00 b9 ff 01  7b bf 0a 00 00 76 0d e3   ········ {····v··
0020  49 21 20 20 20 20 20 20  20 20 20 20 20 20 20 20   I!
0030  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
```

Frame (534 bytes)
Reassembled IPv4 (1980 bytes)
Fragment offset (13 bits) (ip.frag_offset), 2 bytes
Type here to search

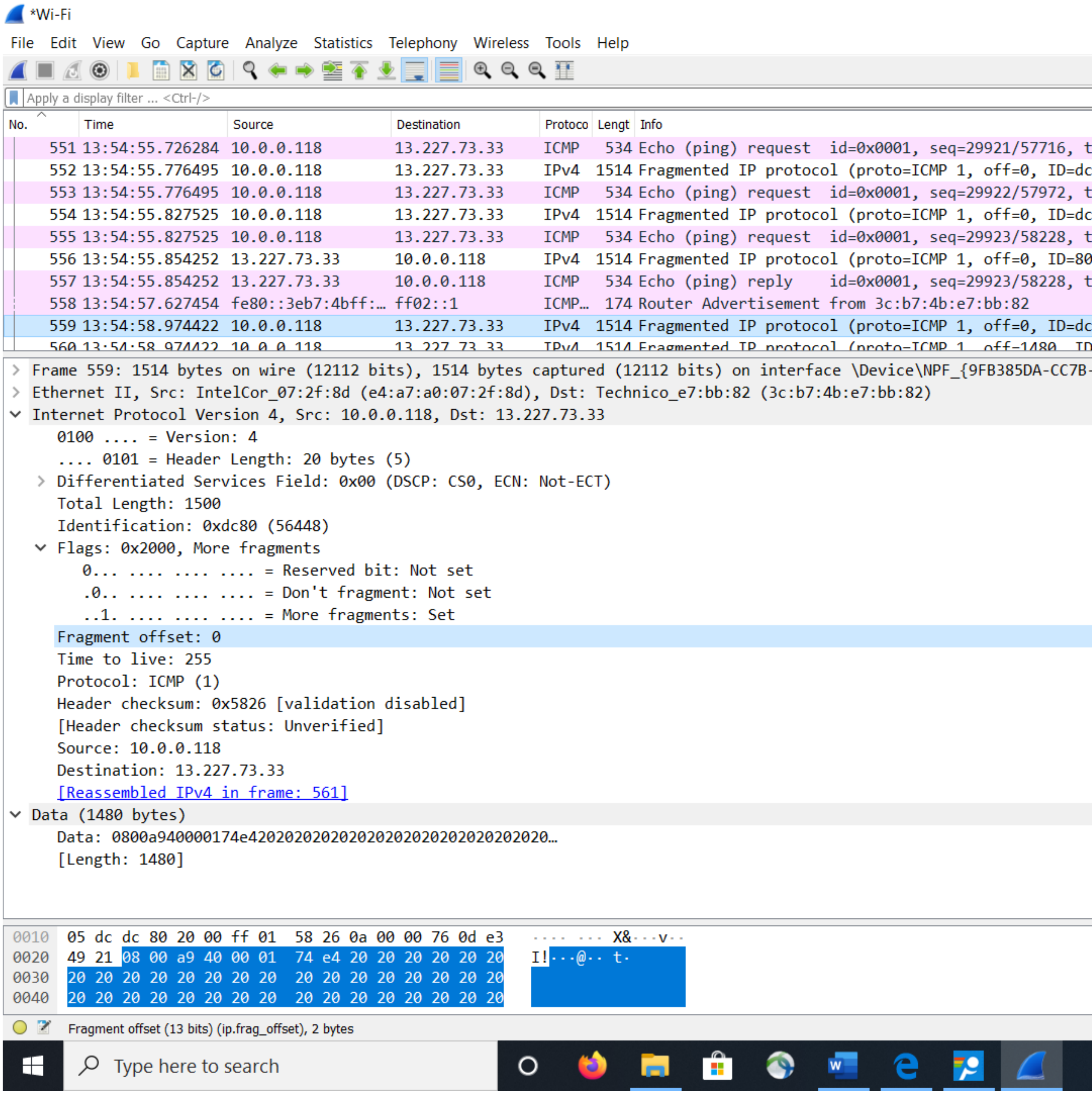
13. What fields change in the IP header between the first and second fragment?

The fragment offset, total length, more fragments bit and flags remained the same between the first and second fragments

Now find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 3500.

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

As one can see in the last screen shot there was 3 fragments created from the original

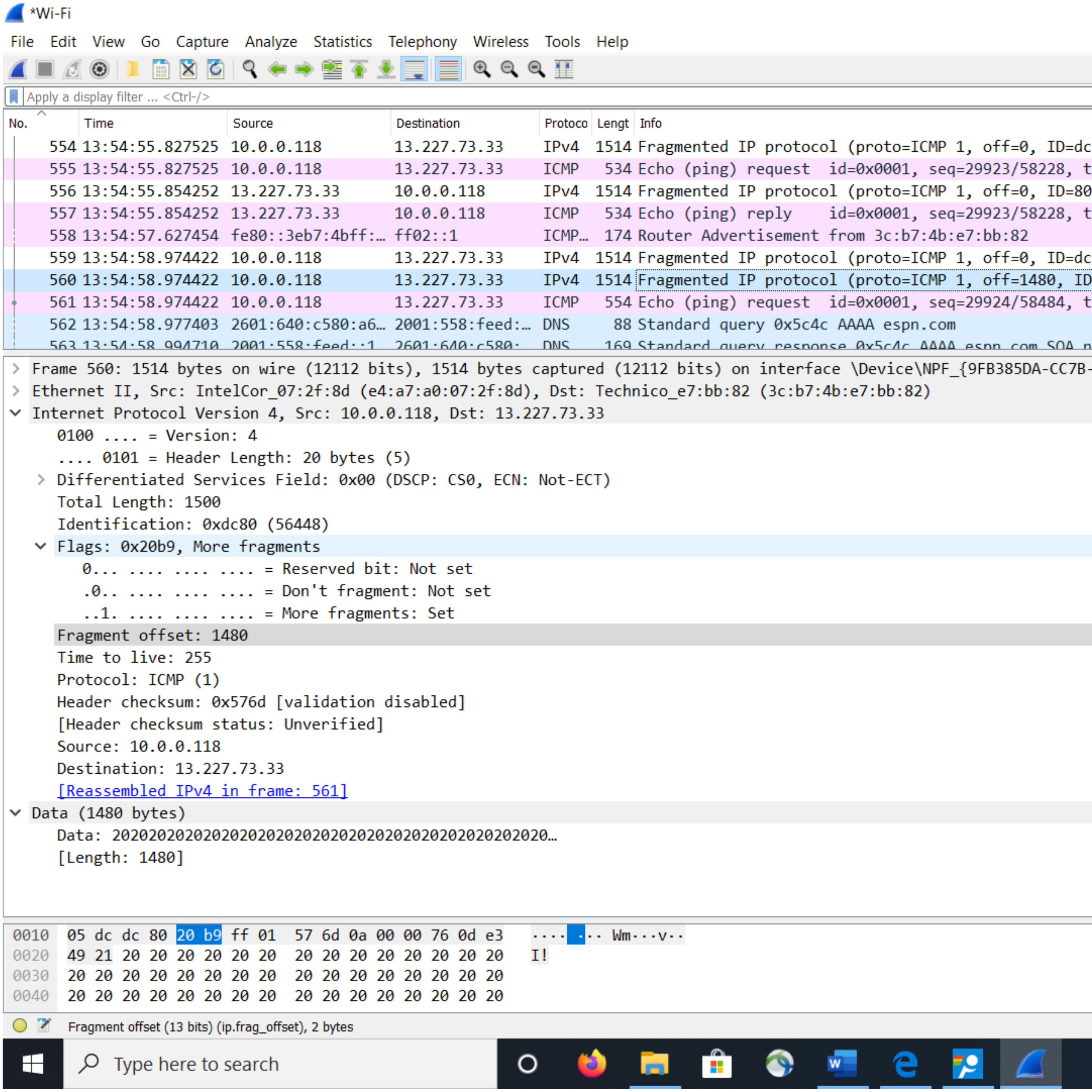

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Type here to search

```
No.  Time            Source            Destination   Protoco Lengt Info
 551 13:54:55.726284 10.0.0.118        13.227.73.33  ICMP     534 Echo (ping) request  id=0x0001, seq=29921/57716, t
 552 13:54:55.776495 10.0.0.118        13.227.73.33  IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=dc
 553 13:54:55.776495 10.0.0.118        13.227.73.33  ICMP     534 Echo (ping) request  id=0x0001, seq=29922/57972, t
 554 13:54:55.827525 10.0.0.118        13.227.73.33  IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=dc
 555 13:54:55.827525 10.0.0.118        13.227.73.33  ICMP     534 Echo (ping) request  id=0x0001, seq=29923/58228, t
 556 13:54:55.854252 13.227.73.33      10.0.0.118    IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=80
 557 13:54:55.854252 13.227.73.33      10.0.0.118    ICMP     534 Echo (ping) reply    id=0x0001, seq=29923/58228, t
 558 13:54:57.627454 fe80::3eb7:4bff:… ff02::1       ICMP…    174 Router Advertisement from 3c:b7:4b:e7:bb:82
 559 13:54:58.974422 10.0.0.118        13.227.73.33  IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=dc
 560 13:54:58.974422 10.0.0.118        13.227.73.33  IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID
```

```
> Frame 559: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{9FB385DA-CC7B-
> Ethernet II, Src: IntelCor_07:2f:8d (e4:a7:a0:07:2f:8d), Dst: Technico_e7:bb:82 (3c:b7:4b:e7:bb:82)
v Internet Protocol Version 4, Src: 10.0.0.118, Dst: 13.227.73.33
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 1500
     Identification: 0xdc80 (56448)
   v Flags: 0x2000, 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: 0x5826 [validation disabled]
     [Header checksum status: Unverified]
     Source: 10.0.0.118
     Destination: 13.227.73.33
     [Reassembled IPv4 in frame: 561]
v Data (1480 bytes)
     Data: 0800a940000174e42020202020202020202020202020202020…
     [Length: 1480]
```

```
0010  05 dc dc 80 20 00 ff 01  58 26 0a 00 00 76 0d e3   ···· ··· X&···v··
0020  49 21 08 00 a9 40 00 01  74 e4 20 20 20 20 20 20   I!···@·· t·
0030  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0040  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
```

Fragment offset (13 bits) (ip.frag_offset), 2 bytes

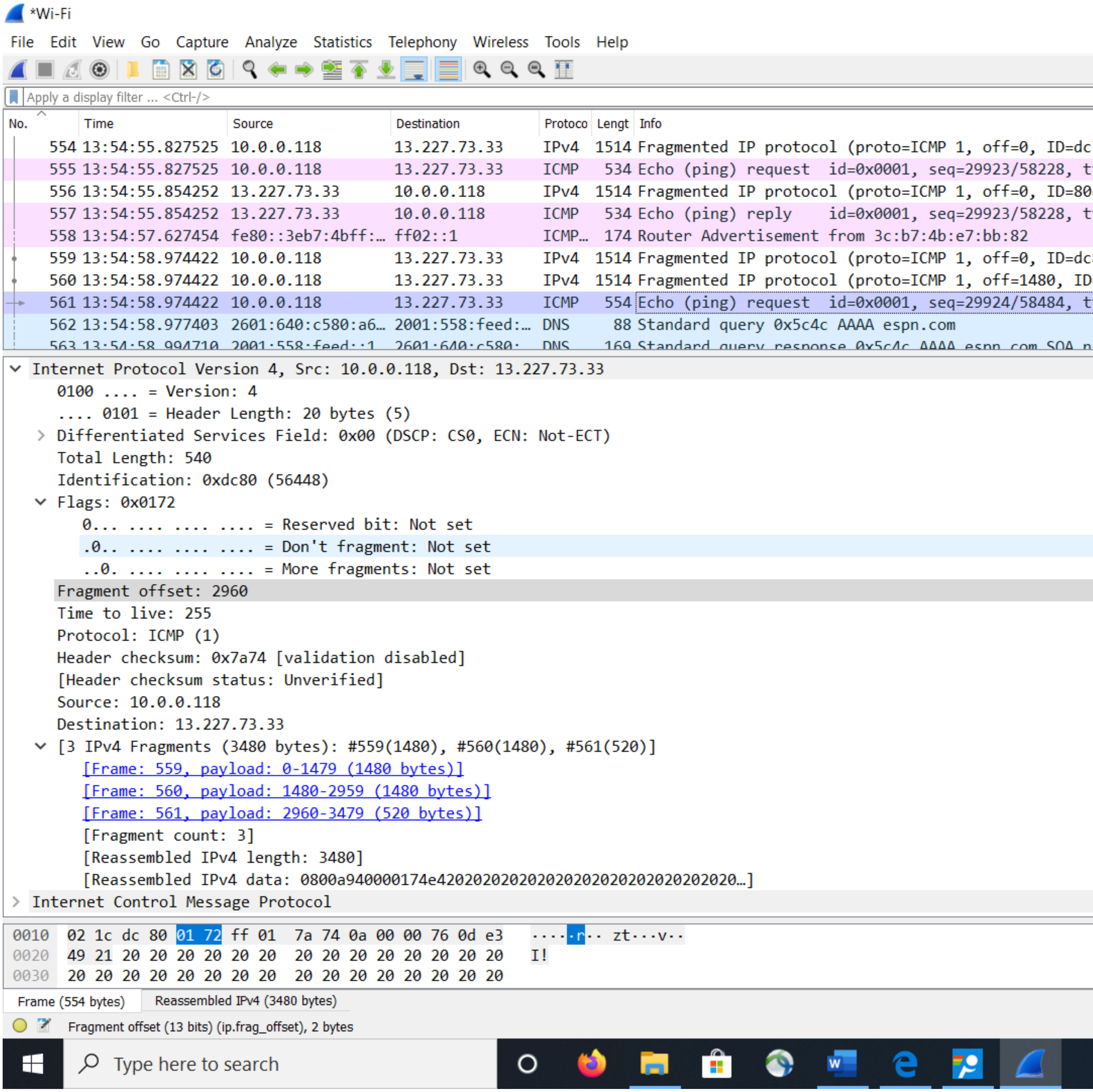

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Type here to search

```
No.  Time             Source                 Destination          Protoco Lengt Info
 554 13:54:55.827525 10.0.0.118             13.227.73.33         IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=dc
 555 13:54:55.827525 10.0.0.118             13.227.73.33         ICMP     534 Echo (ping) request  id=0x0001, seq=29923/58228, t
 556 13:54:55.854252 13.227.73.33           10.0.0.118           IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=80
 557 13:54:55.854252 13.227.73.33           10.0.0.118           ICMP     534 Echo (ping) reply    id=0x0001, seq=29923/58228, t
 558 13:54:57.627454 fe80::3eb7:4bff:…      ff02::1              ICMP…    174 Router Advertisement from 3c:b7:4b:e7:bb:82
 559 13:54:58.974422 10.0.0.118             13.227.73.33         IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=dc
 560 13:54:58.974422 10.0.0.118             13.227.73.33         IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID
 561 13:54:58.974422 10.0.0.118             13.227.73.33         ICMP     554 Echo (ping) request  id=0x0001, seq=29924/58484, t
 562 13:54:58.977403 2601:640:c580:a6…      2001:558:feed:…      DNS       88 Standard query 0x5c4c AAAA espn.com
 563 13:54:58.994710 2001:558:feed::1       2601:640:c580:…      DNS      169 Standard query response 0x5c4c AAAA espn.com SOA n
```

```
> Frame 560: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{9FB385DA-CC7B-
> Ethernet II, Src: IntelCor_07:2f:8d (e4:a7:a0:07:2f:8d), Dst: Technico_e7:bb:82 (3c:b7:4b:e7:bb:82)
v Internet Protocol Version 4, Src: 10.0.0.118, Dst: 13.227.73.33
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0xdc80 (56448)
  v Flags: 0x20b9, 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: 0x576d [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.0.118
    Destination: 13.227.73.33
    [Reassembled IPv4 in frame: 561]
v Data (1480 bytes)
    Data: 2020202020202020202020202020202020202020202020202020…
    [Length: 1480]
```

```
0010  05 dc dc 80 20 b9 ff 01  57 6d 0a 00 00 76 0d e3   ........ Wm...v..
0020  49 21 20 20 20 20 20 20  20 20 20 20 20 20 20 20   I!
0030  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0040  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
```

Fragment offset (13 bits) (ip.frag_offset), 2 bytes


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Type here to search

```
No.  Time             Source                Destination          Protoco Lengt Info
 554 13:54:55.827525 10.0.0.118           13.227.73.33         IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=dc
 555 13:54:55.827525 10.0.0.118           13.227.73.33         ICMP     534 Echo (ping) request  id=0x0001, seq=29923/58228, t
 556 13:54:55.854252 13.227.73.33         10.0.0.118           IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=80
 557 13:54:55.854252 13.227.73.33         10.0.0.118           ICMP     534 Echo (ping) reply    id=0x0001, seq=29923/58228, t
 558 13:54:57.627454 fe80::3eb7:4bff:…    ff02::1              ICMP…    174 Router Advertisement from 3c:b7:4b:e7:bb:82
 559 13:54:58.974422 10.0.0.118           13.227.73.33         IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=dc
 560 13:54:58.974422 10.0.0.118           13.227.73.33         IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID
 561 13:54:58.974422 10.0.0.118           13.227.73.33         ICMP     554 Echo (ping) request  id=0x0001, seq=29924/58484, t
 562 13:54:58.977403 2601:640:c580:a6…    2001:558:feed:…      DNS       88 Standard query 0x5c4c AAAA espn.com
 563 13:54:58.994710 2001:558:feed::1     2601:640:c580:…      DNS      169 Standard query response 0x5c4c AAAA espn.com SOA n
```

```
v Internet Protocol Version 4, Src: 10.0.0.118, Dst: 13.227.73.33
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 540
     Identification: 0xdc80 (56448)
   v Flags: 0x0172
        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: 0x7a74 [validation disabled]
     [Header checksum status: Unverified]
     Source: 10.0.0.118
     Destination: 13.227.73.33
   v [3 IPv4 Fragments (3480 bytes): #559(1480), #560(1480), #561(520)]
        [Frame: 559, payload: 0-1479 (1480 bytes)]
        [Frame: 560, payload: 1480-2959 (1480 bytes)]
        [Frame: 561, payload: 2960-3479 (520 bytes)]
        [Fragment count: 3]
        [Reassembled IPv4 length: 3480]
        [Reassembled IPv4 data: 0800a940000174e42020202020202020202020202020202020…]
> Internet Control Message Protocol
```

```
0010  02 1c dc 80 01 72 ff 01  7a 74 0a 00 00 76 0d e3   .....r.. zt...v..
0020  49 21 20 20 20 20 20 20  20 20 20 20 20 20 20 20   I!
0030  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
```

Frame (554 bytes)   Reassembled IPv4 (3480 bytes)

Fragment offset (13 bits) (ip.frag_offset), 2 bytes

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

The fragment offset, total length, more fragments bit and flags are not the same in all 3, some are the same in the 1st and 2nd