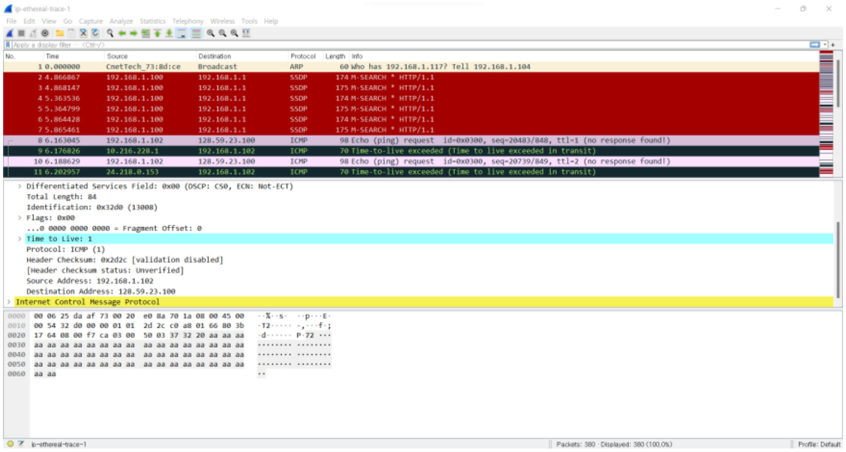
1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

192.169.1.102

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

ICMP


ip-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time       Source             Destination      Protocol Length Info
  1 0.000000   CnetTech_73:8d:ce  Broadcast        ARP        60 Who has 192.168.1.117? Tell 192.168.1.104
  2 4.866867   192.168.1.100      192.168.1.1      SSDP      174 M-SEARCH * HTTP/1.1
  3 4.868147   192.168.1.100      192.168.1.1      SSDP      175 M-SEARCH * HTTP/1.1
  4 5.363536   192.168.1.100      192.168.1.1      SSDP      174 M-SEARCH * HTTP/1.1
  5 5.364799   192.168.1.100      192.168.1.1      SSDP      175 M-SEARCH * HTTP/1.1
  6 5.864428   192.168.1.100      192.168.1.1      SSDP      174 M-SEARCH * HTTP/1.1
  7 5.865461   192.168.1.100      192.168.1.1      SSDP      175 M-SEARCH * HTTP/1.1
  8 6.163045   192.168.1.102      128.59.23.100    ICMP       98 Echo (ping) request  id=0x0300, seq=20483/848, ttl=1 (no response found!)
  9 6.176826   10.216.228.1       192.168.1.102    ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
 10 6.188629   192.168.1.102      128.59.23.100    ICMP       98 Echo (ping) request  id=0x0300, seq=20739/849, ttl=2 (no response found!)
 11 6.202957   24.218.0.153       192.168.1.102    ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
```

```
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x32d0 (13008)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
> Internet Control Message Protocol
```

```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ··%··s·  ··p···E·
0010  00 54 32 d0 00 00 01 01  2d 2c c0 a8 01 66 80 3b   ·T2·····  -,···f·;
0020  17 64 08 00 f7 ca 03 00  50 03 37 32 20 aa aa aa   ·d······  P·72 ···
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········ ········
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········ ········
0050  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ········ ········
0060  aa aa                                              ··
```

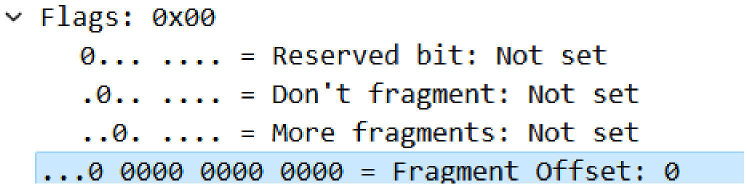
3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

IP header: 20 bytes

The Payload of IP datagram: 56 bytes (=84(total length)-20(header)-8(ICMP))

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

The data gram is not fragmented because ‘More fragments’ flag is not set.



```
⌄ Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  ...0 0000 0000 0000 = Fragment Offset: 0
```

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?

Identification field, Header Checksum, TTL, and sequence number always change.

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

Flags, Fragment offset, and Identifier stayed constant. “More Fragments” Field, Fragment offset, and Identifier must be constant. The reason is that ICMP message sent by my computer is not fragmented, and router has to know where the ICMP message came from. Identification field, Header Checksum, TTL, and sequence number must change. The reason is that router needs to distinguish multiple ICMP messages, and then send appropriate corresponding responds to my computer.

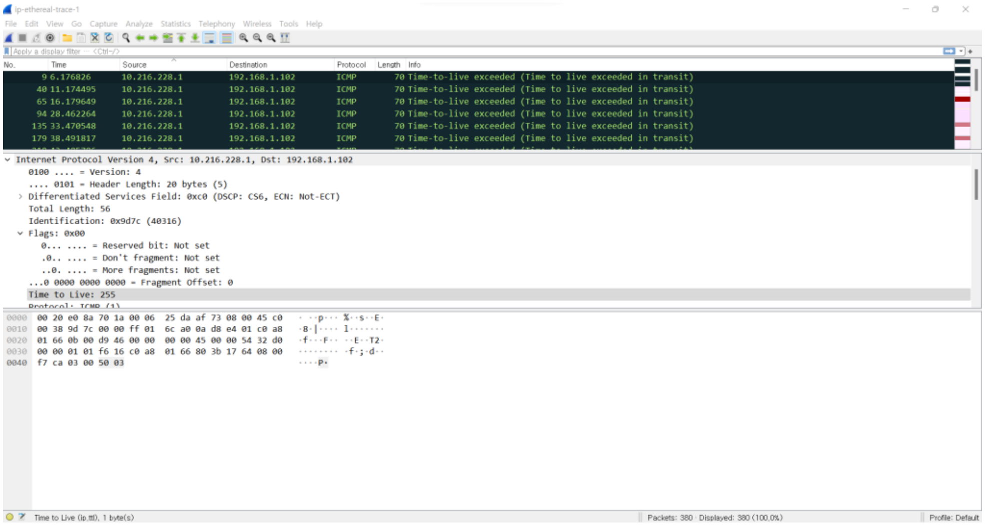
7. Describe the pattern you see in the values in the Identification field of the IP datagram

The higher byte of 16-bit value of the Identification field is 32 in hexadecimal e.g., 0x32__ .

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

Identification Field: 0x9d73

TTL Field: 255


ip-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ··· <Ctrl-/>

```
No.   Time         Source         Destination     Protocol  Length  Info
    9 6.176826     10.216.228.1   192.168.1.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   40 11.174495    10.216.228.1   192.168.1.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   65 16.179649    10.216.228.1   192.168.1.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   94 28.462264    10.216.228.1   192.168.1.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  135 33.470548    10.216.228.1   192.168.1.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  179 38.491817    10.216.228.1   192.168.1.102   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
```

```
v Internet Protocol Version 4, Src: 10.216.228.1, Dst: 192.168.1.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x9d7c (40316)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
```

```
0000  00 20 e0 8a 70 1a 00 06  25 da af 73 08 00 45 c0   · ··p··· %··s··E·
0010  00 38 9d 7c 00 00 ff 01  6c a0 0a d8 e4 01 c0 a8   ·8·|···· l·······
0020  01 66 0b 00 d9 46 00 00  00 00 45 00 00 54 32 d0   ·f···F·· ··E··T2·
0030  00 00 01 01 f6 16 c0 a8  01 66 80 3b 17 64 08 00   ········ ·f·;·d··
0040  f7 ca 03 00 50 03                                  ····P·
```

Time to Live (ip.ttl), 1 byte(s) | Packets: 380 · Displayed: 380 (100.0%) | Profile: Default

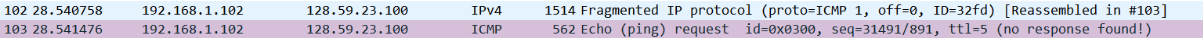
9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

Only the TTL field remained for all ICMP TTL-exceeded replies sent to my computer by the first hop.

The reason is to define the router where TTL is exceeded.

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? [Note: if you find your packet has not been fragmented, you should download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the ipethereal-trace-1packet trace. If your computer has an Ethernet interface, a packet size of 2000 should cause fragmentation.

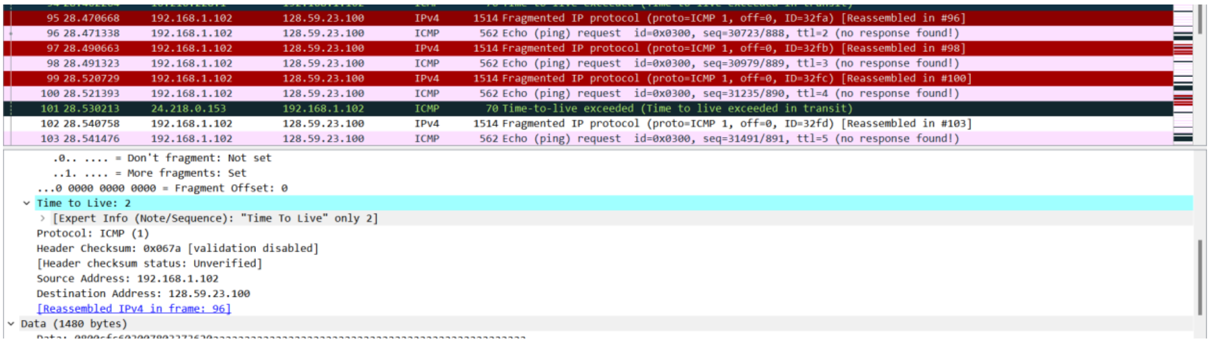
Yes, the message had been fragmented into two IP datagram



```
102 28.540758   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fd) [Reassembled in #103]
103 28.541476   192.168.1.102   128.59.23.100   ICMP    562 Echo (ping) request  id=0x0300, seq=31491/891, ttl=5 (no response found!)
```

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?

IP header indicates that the datagram been fragmented by setting ‘More fragments’ flag. Moreover, IP header indicates the first fragment by writing ‘fragment offset’ as 0, and then the latter fragment by writing the byte where latter fragment should be placed. This IP datagram is 1514 byte long. (The payload is 1480bytes long)



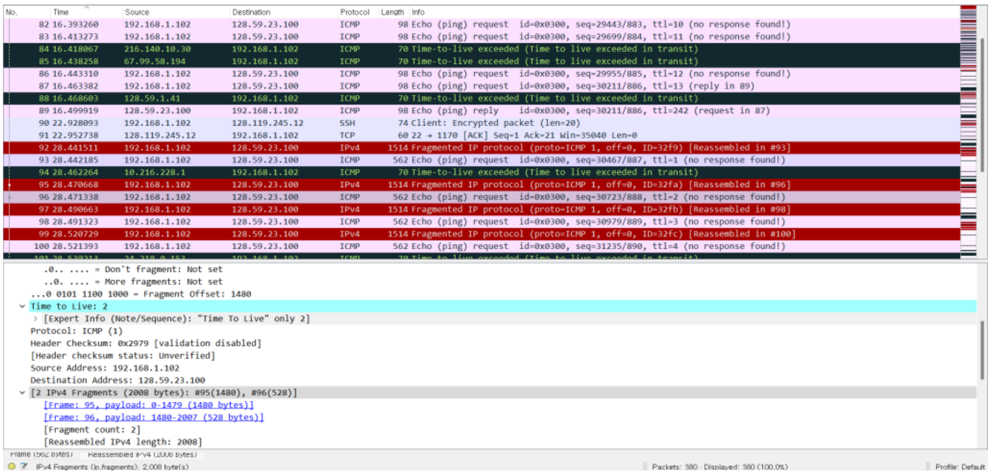
```
 95 28.470668   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Reassembled in #96]
 96 28.471338   192.168.1.102   128.59.23.100   ICMP    562 Echo (ping) request  id=0x0300, seq=30723/888, ttl=2 (no response found!)
 97 28.490663   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Reassembled in #98]
 98 28.491323   192.168.1.102   128.59.23.100   ICMP    562 Echo (ping) request  id=0x0300, seq=30979/889, ttl=3 (no response found!)
 99 28.520729   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fc) [Reassembled in #100]
100 28.521393   192.168.1.102   128.59.23.100   ICMP    562 Echo (ping) request  id=0x0300, seq=31235/890, ttl=4 (no response found!)
101 28.530213   24.218.0.153    192.168.1.102   ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
102 28.540758   192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fd) [Reassembled in #103]
103 28.541476   192.168.1.102   128.59.23.100   ICMP    562 Echo (ping) request  id=0x0300, seq=31491/891, ttl=5 (no response found!)

      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    ...0 0000 0000 0000 = Fragment Offset: 0
  ⌄ Time to Live: 2
    › [Expert Info (Note/Sequence): "Time To Live" only 2]
    Protocol: ICMP (1)
    Header Checksum: 0x067a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
    [Reassembled IPv4 in frame: 96]
⌄ Data (1480 bytes)
```

(Frame: 95)

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 IP header indicates that this is not the first datagram fragment by writing a location after the first fragment(e.x.1480) in ‘Fragment Offset’, and IP header indicates there are more fragments by setting “More fragments” flag.

(If ‘More Fragments’ flag is cleared, then there is no more fragment after this fragment.)



```
No.   Time        Source           Destination      Protocol Length Info
 82 16.393260   192.168.1.102   128.59.23.100    ICMP     98 Echo (ping) request  id=0x0300, seq=29443/883, ttl=10 (no response found!)
 83 16.413273   192.168.1.102   128.59.23.100    ICMP     98 Echo (ping) request  id=0x0300, seq=29699/884, ttl=11 (no response found!)
 84 16.418067   216.140.10.30   192.168.1.102    ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
 85 16.438258   67.99.58.194    192.168.1.102    ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
 86 16.443310   192.168.1.102   128.59.23.100    ICMP     98 Echo (ping) request  id=0x0300, seq=29955/885, ttl=12 (no response found!)
 87 16.463382   192.168.1.102   128.59.23.100    ICMP     98 Echo (ping) request  id=0x0300, seq=30211/886, ttl=13 (reply in 89)
 88 16.468603   128.59.1.41     192.168.1.102    ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
 89 16.499919   128.59.23.100   192.168.1.102    ICMP     98 Echo (ping) reply    id=0x0300, seq=30211/886, ttl=242 (request in 87)
 90 22.928093   192.168.1.102   128.119.245.12   SSH      74 Client: Encrypted packet (len=20)
 91 22.952738   128.119.245.12  192.168.1.102    TCP      60 22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0
 92 28.441511   192.168.1.102   128.59.23.100    IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
 93 28.442185   192.168.1.102   128.59.23.100    ICMP    562 Echo (ping) request  id=0x0300, seq=30467/887, ttl=1 (no response found!)
 94 28.462264   10.216.228.1    192.168.1.102    ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
 95 28.470668   192.168.1.102   128.59.23.100    IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Reassembled in #96]
 96 28.471338   192.168.1.102   128.59.23.100    ICMP    562 Echo (ping) request  id=0x0300, seq=30723/888, ttl=2 (no response found!)
 97 28.490663   192.168.1.102   128.59.23.100    IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Reassembled in #98]
 98 28.491323   192.168.1.102   128.59.23.100    ICMP    562 Echo (ping) request  id=0x0300, seq=30979/889, ttl=3 (no response found!)
 99 28.520729   192.168.1.102   128.59.23.100    IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fc) [Reassembled in #100]
100 28.521393   192.168.1.102   128.59.23.100    ICMP    562 Echo (ping) request  id=0x0300, seq=31235/890, ttl=4 (no response found!)

      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0101 1100 1000 = Fragment Offset: 1480
  ⌄ Time to Live: 2
    › [Expert Info (Note/Sequence): "Time To Live" only 2]
    Protocol: ICMP (1)
    Header Checksum: 0x2979 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
  ⌄ [2 IPv4 Fragments (2008 bytes): #95(1480), #96(528)]
      [Frame: 95, payload: 0-1479 (1480 bytes)]
      [Frame: 96, payload: 1480-2007 (528 bytes)]
      [Fragment count: 2]
      [Reassembled IPv4 length: 2008]
Frame (562 bytes)   Reassembled IPv4 (2008 bytes)
IPv4 Fragments (ip.fragments), 2,008 byte(s)        Packets: 380 · Displayed: 380 (100.0%)        Profile: Default
```

(Frame: 96)

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

Flag, “Fragment Offset”, and Checksum changed in the IP header between the first and second fragment.

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

Three fragments were created from the original datagram.

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

Flag, “Fragment Offset”, and Checksum changed in the IP header among the fragments.