Pandit Deendayal Energy University
School of Technology
Department of ICT
Academic Year: 2022-23
Computer Communication and Networking Lab
20IC306P

Name: Janakar Patel

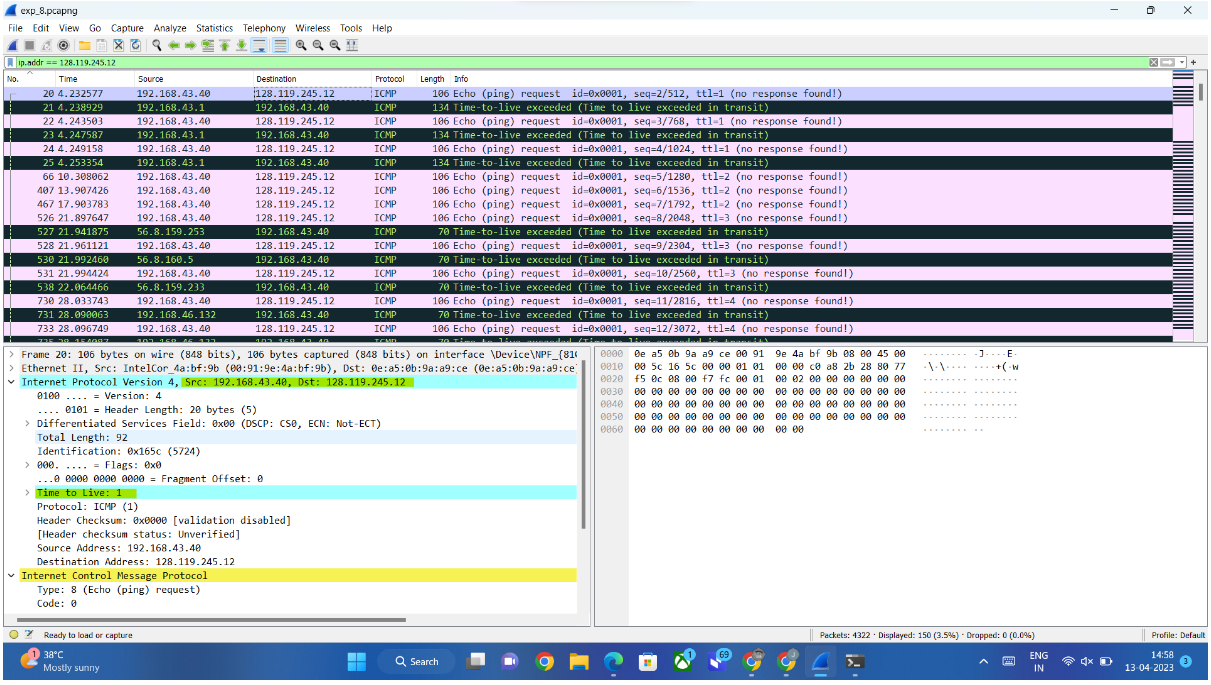
Roll No: 20BIT061

Experiment 8:

Aim: To understand the working of IP by using wire shark.
Software Tools required: - Wire-shark

Answer the following questions[1]. If you're doing this lab as part of class, your teacher will provide details about how to hand in assignments, whether written or in an LMS.

1. Select the first UDP segment sent by your computer via the `traceroute` command to gaia.cs.umass.edu. (Hint: this is 44th packet in the trace file in the *ip-wireshark-trace1-1.pcapng* file in footnote 2). Expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?



ip.addr == 128.119.245.12

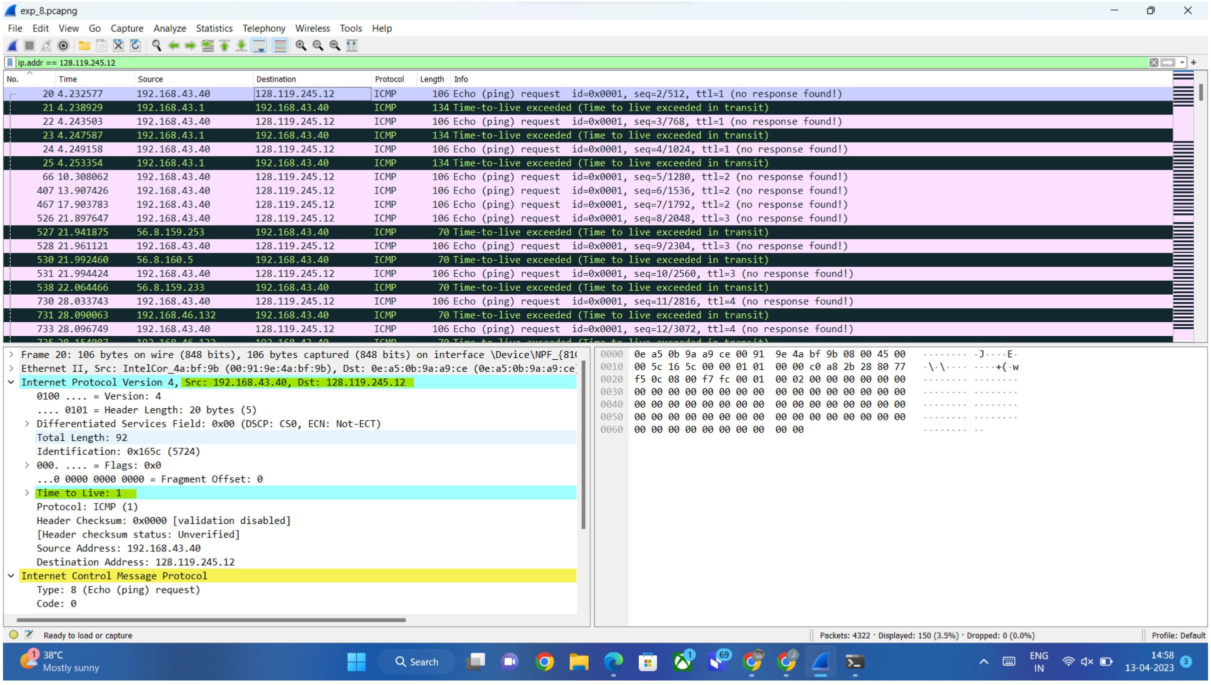
```
No.   Time       Source          Destination     Protocol Length Info
   20 4.232577   192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=2/512, ttl=1 (no response found!)
   21 4.238929   192.168.43.1    192.168.43.40   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
   22 4.243503   192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=3/768, ttl=1 (no response found!)
   23 4.247587   192.168.43.1    192.168.43.40   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
   24 4.249158   192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=4/1024, ttl=1 (no response found!)
   25 4.253354   192.168.43.1    192.168.43.40   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
   66 10.308062  192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=5/1280, ttl=2 (no response found!)
  407 13.907426  192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=6/1536, ttl=2 (no response found!)
  467 17.903783  192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=7/1792, ttl=2 (no response found!)
  526 21.897647  192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=8/2048, ttl=3 (no response found!)
  527 21.941875  56.8.159.253    192.168.43.40   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  528 21.961121  192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=9/2304, ttl=3 (no response found!)
  530 21.992460  56.8.160.5      192.168.43.40   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  531 21.994424  192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=10/2560, ttl=3 (no response found!)
  538 22.064466  56.8.159.233    192.168.43.40   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  730 28.033743  192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=11/2816, ttl=4 (no response found!)
  731 28.090063  192.168.46.132  192.168.43.40   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  733 28.096749  192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=12/3072, ttl=4 (no response found!)
```

```
> Frame 20: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{81
> Ethernet II, Src: IntelCor_4a:bf:9b (00:91:9e:4a:bf:9b), Dst: 0e:a5:0b:9a:a9:ce (0e:a5:0b:9a:a9:ce
v Internet Protocol Version 4, Src: 192.168.43.40, 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: 92
    Identification: 0x165c (5724)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.40
    Destination Address: 128.119.245.12
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
```

```
0000  0e a5 0b 9a a9 ce 00 91  9e 4a bf 9b 08 00 45 00   ········ ·J····E·
0010  00 5c 16 5c 00 00 01 01  00 00 c0 a8 2b 28 80 77   ·\·\···· ····+(·w
0020  f5 0c 08 00 f7 fc 00 01  00 02 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00                     ········ ··
```

2. What is the value in the time-to-live (TTL) field in this IPv4 datagram's header?

[1] For the author's class, when answering the following questions with hand-in assignments, students sometimes need to print out specific packets (see the introductory Wireshark lab for an explanation of how to do this) and indicate where in the packet they've found the information that answers a question. They do this by marking paper copies with a pen or annotating electronic copies with text in a colored font. There are also learning management system (LMS) modules for teachers that allow students to answer these questions online and have answers auto-graded for these Wireshark labs at http://gaia.cs.umass.edu/kurose_ross/lms.htm


exp_8.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 128.119.245.12

```
No.   Time       Source          Destination     Protocol Length Info
   20 4.232577   192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=2/512, ttl=1 (no response found!)
   21 4.238929   192.168.43.1    192.168.43.40   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
   22 4.243503   192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=3/768, ttl=1 (no response found!)
   23 4.247587   192.168.43.1    192.168.43.40   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
   24 4.249158   192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=4/1024, ttl=1 (no response found!)
   25 4.253354   192.168.43.1    192.168.43.40   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
   66 10.308062  192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=5/1280, ttl=2 (no response found!)
  407 13.907426  192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=6/1536, ttl=2 (no response found!)
  467 17.903783  192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=7/1792, ttl=2 (no response found!)
  526 21.897647  192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=8/2048, ttl=3 (no response found!)
  527 21.941875  56.8.159.253    192.168.43.40   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  528 21.961121  192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=9/2304, ttl=3 (no response found!)
  530 21.992460  56.8.160.5      192.168.43.40   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  531 21.994424  192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=10/2560, ttl=3 (no response found!)
  538 22.064466  56.8.159.233    192.168.43.40   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  730 28.033743  192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=11/2816, ttl=4 (no response found!)
  731 28.090063  192.168.46.132  192.168.43.40   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  733 28.096749  192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=12/3072, ttl=4 (no response found!)
```

```
> Frame 20: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{81(
> Ethernet II, Src: IntelCor_4a:bf:9b (00:91:9e:4a:bf:9b), Dst: 0e:a5:0b:9a:a9:ce (0e:a5:0b:9a:a9:ce
v Internet Protocol Version 4, Src: 192.168.43.40, 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: 92
    Identification: 0x165c (5724)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.40
    Destination Address: 128.119.245.12
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
```

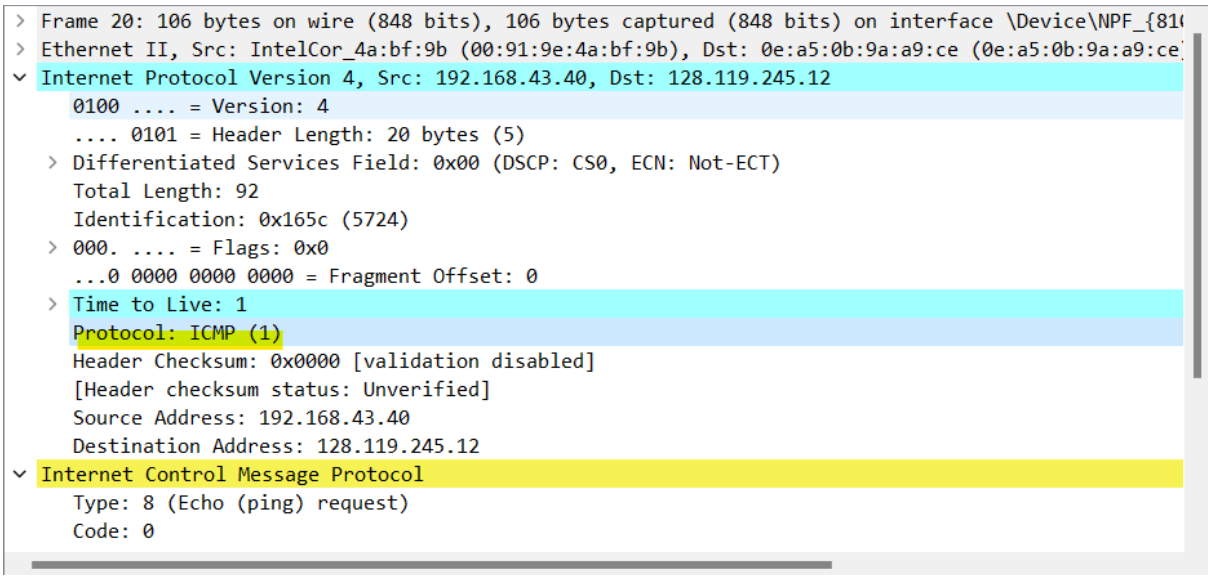
```
0000  0e a5 0b 9a a9 ce 00 91  9e 4a bf 9b 08 00 45 00   ········ ·J····E·
0010  00 5c 16 5c 00 00 01 01  00 00 c0 a8 2b 28 80 77   ·\·\···· ····+(·w
0020  f5 0c 08 00 f7 fc 00 01  00 02 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00                     ········ ··
```

Ready to load or capture

Packets: 4322 · Displayed: 150 (3.5%) · Dropped: 0 (0.0%)

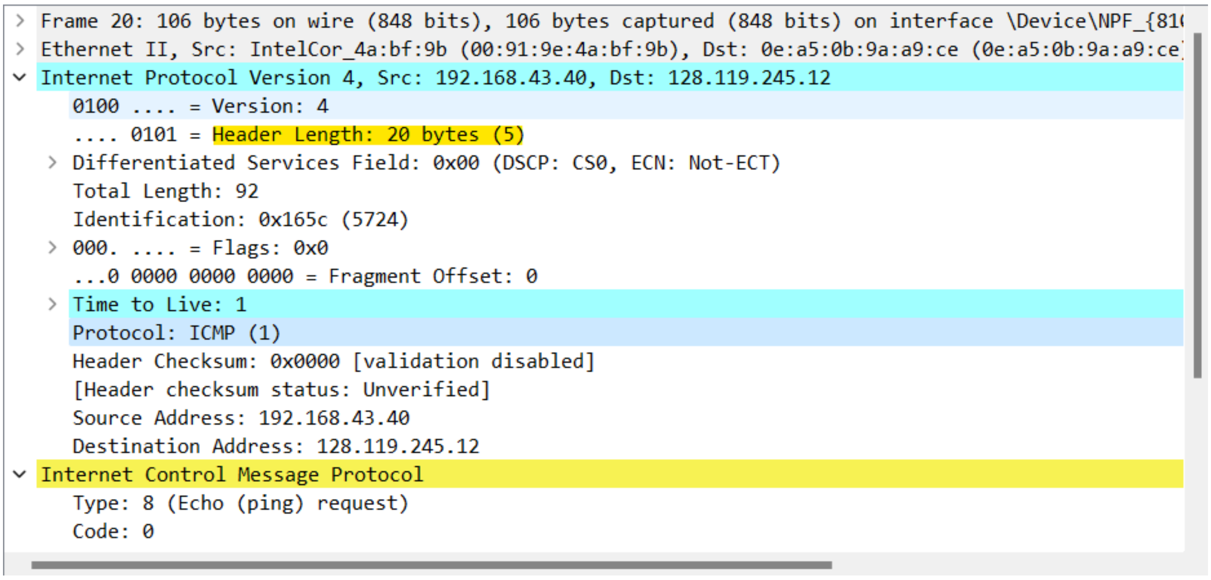
Profile: Default

3. What is the value in the upper layer protocol field in this IPv4 datagram's header? [Note: the answers for Linux/MacOS differ from Windows here].



```
> Frame 20: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{81(
> Ethernet II, Src: IntelCor_4a:bf:9b (00:91:9e:4a:bf:9b), Dst: 0e:a5:0b:9a:a9:ce (0e:a5:0b:9a:a9:ce
v Internet Protocol Version 4, Src: 192.168.43.40, 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: 92
    Identification: 0x165c (5724)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.40
    Destination Address: 128.119.245.12
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
```

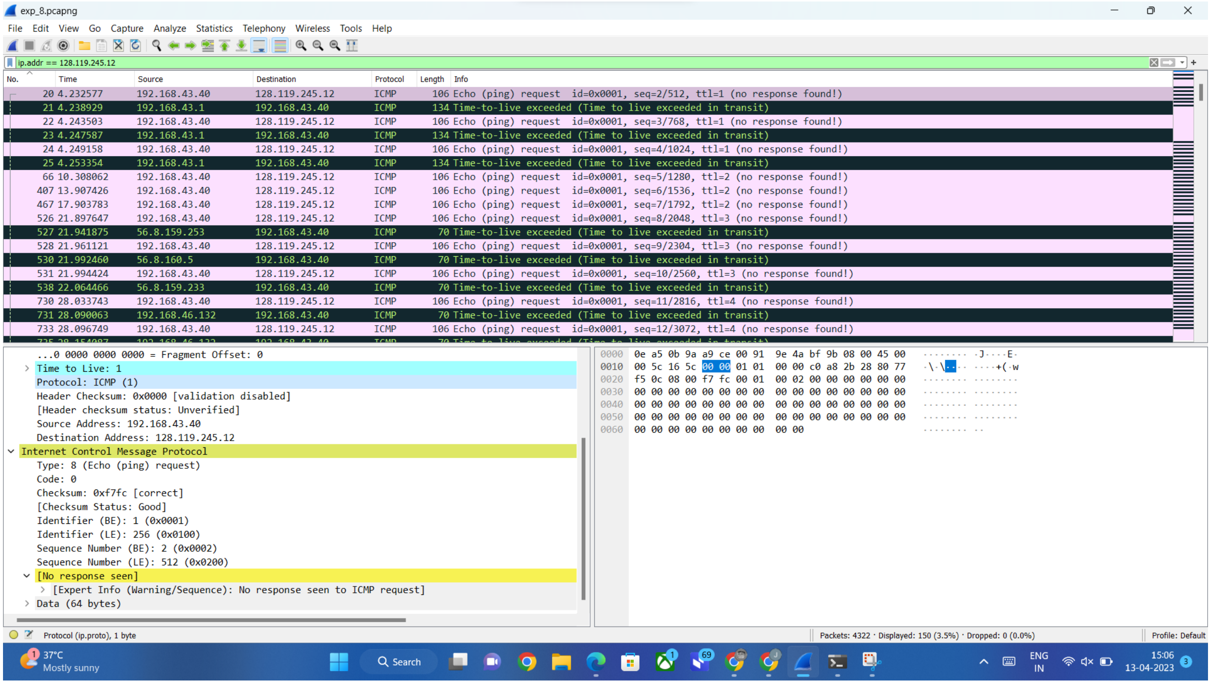
4. How many bytes are in the IP header?



```
> Frame 20: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{81(
> Ethernet II, Src: IntelCor_4a:bf:9b (00:91:9e:4a:bf:9b), Dst: 0e:a5:0b:9a:a9:ce (0e:a5:0b:9a:a9:ce)
v Internet Protocol Version 4, Src: 192.168.43.40, 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: 92
    Identification: 0x165c (5724)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.40
    Destination Address: 128.119.245.12
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
```

5. How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.
   It is total length - header length = 92 - 20 = 72 bytes.

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



exp_8.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 128.119.245.12

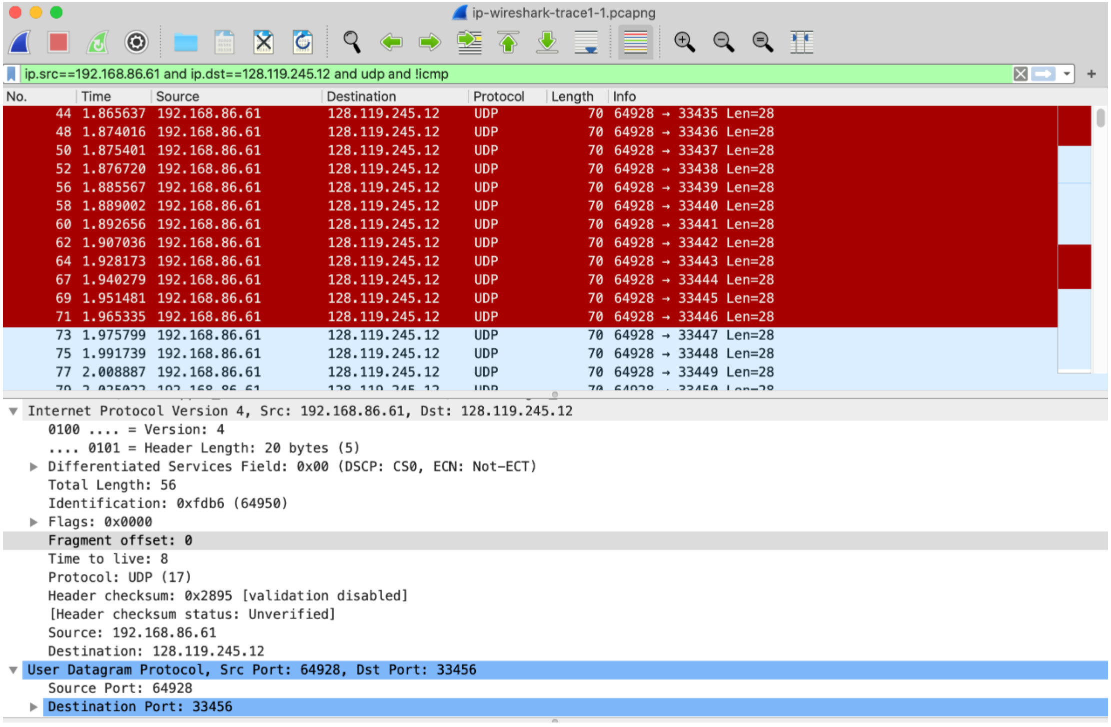
```
No.    Time         Source           Destination      Protocol  Length Info
    20 4.232577     192.168.43.40    128.119.245.12   ICMP      106 Echo (ping) request  id=0x0001, seq=2/512, ttl=1 (no response found!)
    21 4.238929     192.168.43.1     192.168.43.40    ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
    22 4.243503     192.168.43.40    128.119.245.12   ICMP      106 Echo (ping) request  id=0x0001, seq=3/768, ttl=1 (no response found!)
    23 4.247587     192.168.43.1     192.168.43.40    ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
    24 4.249158     192.168.43.40    128.119.245.12   ICMP      106 Echo (ping) request  id=0x0001, seq=4/1024, ttl=1 (no response found!)
    25 4.253354     192.168.43.1     192.168.43.40    ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
    66 10.308062    192.168.43.40    128.119.245.12   ICMP      106 Echo (ping) request  id=0x0001, seq=5/1280, ttl=2 (no response found!)
   407 13.907426    192.168.43.40    128.119.245.12   ICMP      106 Echo (ping) request  id=0x0001, seq=6/1536, ttl=2 (no response found!)
   467 17.903783    192.168.43.40    128.119.245.12   ICMP      106 Echo (ping) request  id=0x0001, seq=7/1792, ttl=2 (no response found!)
   526 21.897647    192.168.43.40    128.119.245.12   ICMP      106 Echo (ping) request  id=0x0001, seq=8/2048, ttl=3 (no response found!)
   527 21.941875    56.8.159.253     192.168.43.40    ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
   528 21.961121    192.168.43.40    128.119.245.12   ICMP      106 Echo (ping) request  id=0x0001, seq=9/2304, ttl=3 (no response found!)
   530 21.992460    56.8.160.5       192.168.43.40    ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
   531 21.994424    192.168.43.40    128.119.245.12   ICMP      106 Echo (ping) request  id=0x0001, seq=10/2560, ttl=3 (no response found!)
   538 22.064466    56.8.159.233     192.168.43.40    ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
   730 28.033743    192.168.43.40    128.119.245.12   ICMP      106 Echo (ping) request  id=0x0001, seq=11/2816, ttl=4 (no response found!)
   731 28.090063    192.168.46.132   192.168.43.40    ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
   733 28.096749    192.168.43.40    128.119.245.12   ICMP      106 Echo (ping) request  id=0x0001, seq=12/3072, ttl=4 (no response found!)
```

```
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.40
    Destination Address: 128.119.245.12
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7fc [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 2 (0x0002)
    Sequence Number (LE): 512 (0x0200)
  v [No response seen]
    > [Expert Info (Warning/Sequence): No response seen to ICMP request]
  > Data (64 bytes)
```

```
0000  0e a5 0b 9a a9 ce 00 91  9e 4a bf 9b 08 00 45 00   ········ ·J····E·
0010  00 5c 16 5c 00 00 01 01  00 00 c0 a8 2b 28 80 77   ·\·\···· ····+(·w
0020  f5 0c 08 00 f7 fc 00 01  00 02 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00                     ········ ··
```

Protocol (ip.proto), 1 byte | Packets: 4322 · Displayed: 150 (3.5%) · Dropped: 0 (0.0%) | Profile: Default

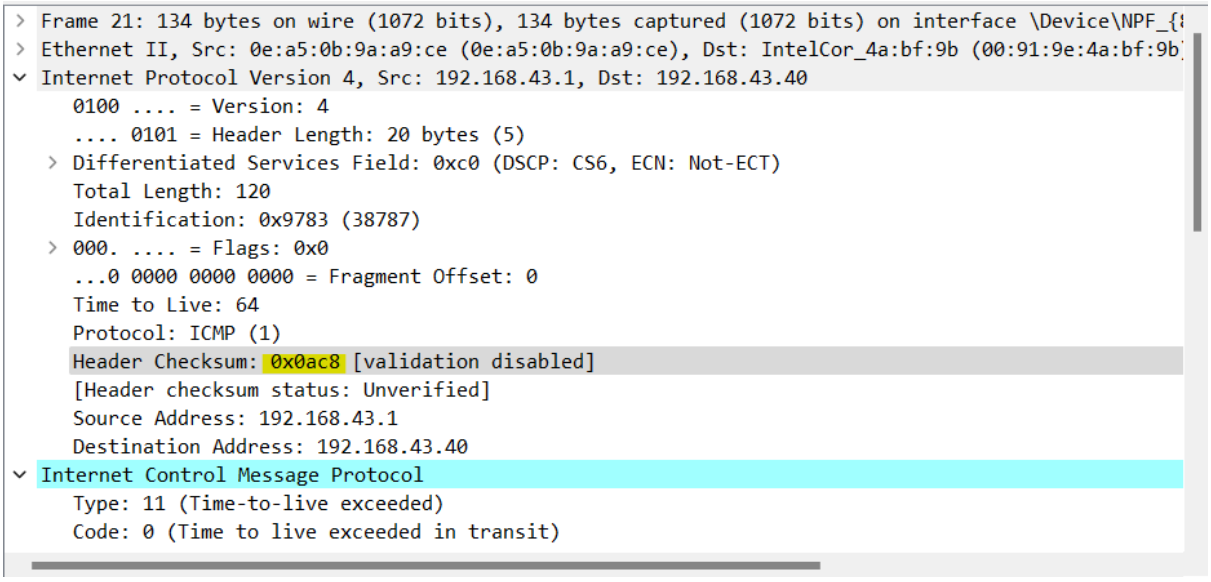
Next, let's look at the *sequence* of UDP segments being sent from your computer via `traceroute`, destined to 128.119.245.12. The display filter that you can enter to do this is "ip.src==192.168.86.61 and ip.dst==128.119.245.12 and udp and !icmp". This will allow you to easily move sequentially through just the datagrams containing just these segments. Your screen should look similar to Figure 3.



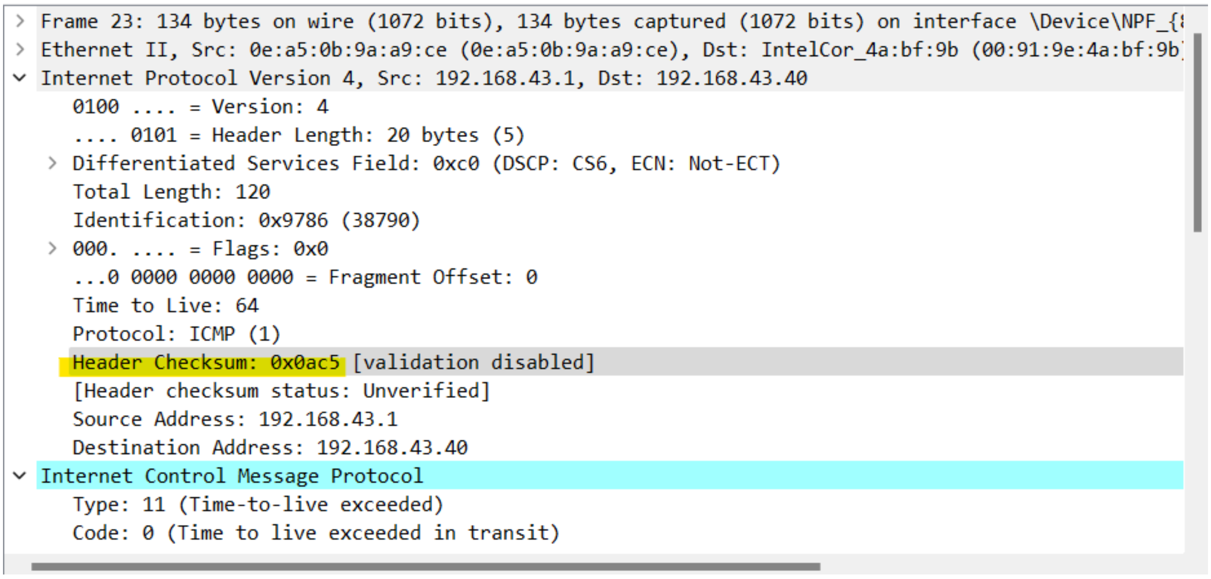
```
ip.src==192.168.86.61 and ip.dst==128.119.245.12 and udp and !icmp

No.  Time     Source          Destination      Protocol  Length  Info
 44 1.865637 192.168.86.61   128.119.245.12   UDP          70 64928 → 33435 Len=28
 48 1.874016 192.168.86.61   128.119.245.12   UDP          70 64928 → 33436 Len=28
 50 1.875401 192.168.86.61   128.119.245.12   UDP          70 64928 → 33437 Len=28
 52 1.876720 192.168.86.61   128.119.245.12   UDP          70 64928 → 33438 Len=28
 56 1.885567 192.168.86.61   128.119.245.12   UDP          70 64928 → 33439 Len=28
 58 1.889002 192.168.86.61   128.119.245.12   UDP          70 64928 → 33440 Len=28
 60 1.892656 192.168.86.61   128.119.245.12   UDP          70 64928 → 33441 Len=28
 62 1.907036 192.168.86.61   128.119.245.12   UDP          70 64928 → 33442 Len=28
 64 1.928173 192.168.86.61   128.119.245.12   UDP          70 64928 → 33443 Len=28
 67 1.940279 192.168.86.61   128.119.245.12   UDP          70 64928 → 33444 Len=28
 69 1.951481 192.168.86.61   128.119.245.12   UDP          70 64928 → 33445 Len=28
 71 1.965335 192.168.86.61   128.119.245.12   UDP          70 64928 → 33446 Len=28
 73 1.975799 192.168.86.61   128.119.245.12   UDP          70 64928 → 33447 Len=28
 75 1.991739 192.168.86.61   128.119.245.12   UDP          70 64928 → 33448 Len=28
 77 2.008887 192.168.86.61   128.119.245.12   UDP          70 64928 → 33449 Len=28
 79 2.025022 192.168.86.61   128.119.245.12   UDP          70 64928 → 33450 Len=28

▼ Internet Protocol Version 4, Src: 192.168.86.61, 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: 0xfdb6 (64950)
  ▶ Flags: 0x0000
    Fragment offset: 0
    Time to live: 8
    Protocol: UDP (17)
    Header checksum: 0x2895 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.86.61
    Destination: 128.119.245.12
▼ User Datagram Protocol, Src Port: 64928, Dst Port: 33456
    Source Port: 64928
  ▶ Destination Port: 33456
```

Figure 3: Wireshark screen shot, showing up segments in the tracefile *ip-wireshark-trace1-1.pcapng* using the display filter `ip.src==192.168.86.61 and ip.dst==128.119.245.12 and udp and !icmp`

7. Which fields in the IP datagram *always* change from one datagram to the next within this series of UDP segments sent by your computer destined to 128.119.245.12, via `traceroute`? Why?



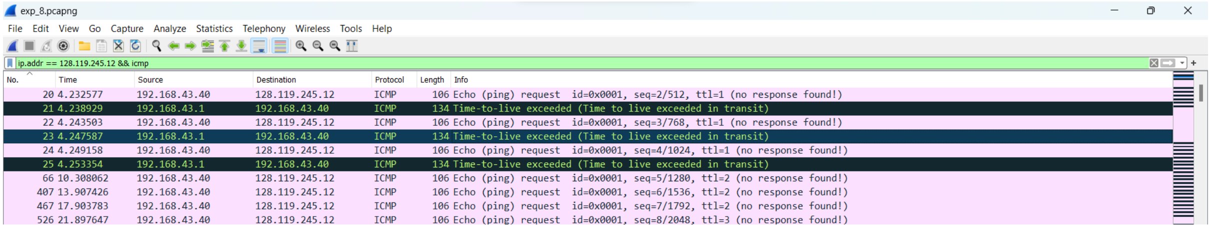
```
> Frame 21: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface \Device\NPF_{
> Ethernet II, Src: 0e:a5:0b:9a:a9:ce (0e:a5:0b:9a:a9:ce), Dst: IntelCor_4a:bf:9b (00:91:9e:4a:bf:9b
v Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.40
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 120
    Identification: 0x9783 (38787)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x0ac8 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.1
    Destination Address: 192.168.43.40
v Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
```



```
> Frame 23: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface \Device\NPF_{
> Ethernet II, Src: 0e:a5:0b:9a:a9:ce (0e:a5:0b:9a:a9:ce), Dst: IntelCor_4a:bf:9b (00:91:9e:4a:bf:9b
v Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.40
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 120
    Identification: 0x9786 (38790)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x0ac5 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.1
    Destination Address: 192.168.43.40
v Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
```

Because checksum is used for error detection and thus is unique to each datagram.

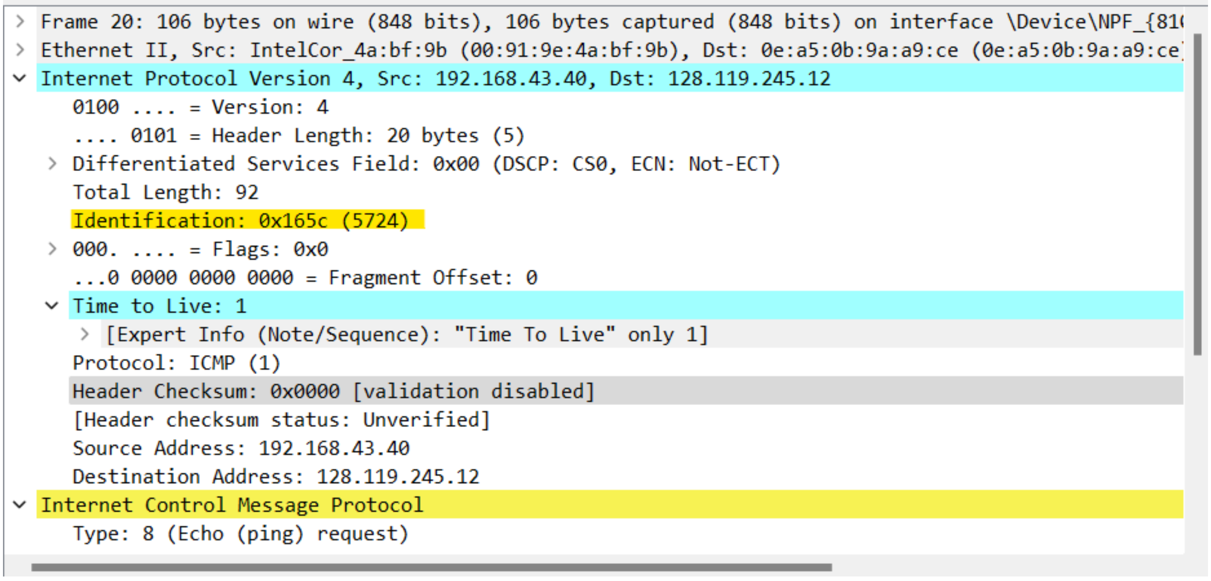
8. Which fields in this sequence of IP datagrams (containing UDP segments) stay constant? Why?



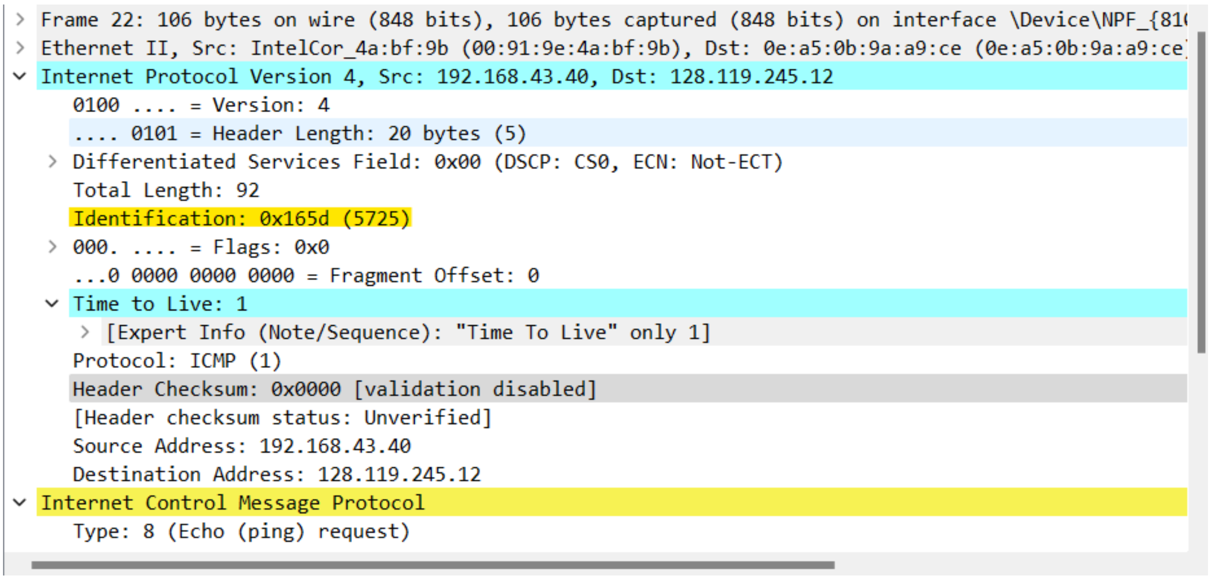
```
ip.addr == 128.119.245.12 && icmp
No.  Time       Source          Destination      Protocol Length Info
 20 4.232577   192.168.43.40   128.119.245.12   ICMP     106 Echo (ping) request  id=0x0001, seq=2/512, ttl=1 (no response found!)
 21 4.238929   192.168.43.1    192.168.43.40    ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
 22 4.243503   192.168.43.40   128.119.245.12   ICMP     106 Echo (ping) request  id=0x0001, seq=3/768, ttl=1 (no response found!)
 23 4.247587   192.168.43.1    192.168.43.40    ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
 24 4.249158   192.168.43.40   128.119.245.12   ICMP     106 Echo (ping) request  id=0x0001, seq=4/1024, ttl=1 (no response found!)
 25 4.253354   192.168.43.1    192.168.43.40    ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
 66 10.308062  192.168.43.40   128.119.245.12   ICMP     106 Echo (ping) request  id=0x0001, seq=5/1280, ttl=2 (no response found!)
407 13.907426  192.168.43.40   128.119.245.12   ICMP     106 Echo (ping) request  id=0x0001, seq=6/1536, ttl=2 (no response found!)
467 17.903783  192.168.43.40   128.119.245.12   ICMP     106 Echo (ping) request  id=0x0001, seq=7/1792, ttl=2 (no response found!)
526 21.897647  192.168.43.40   128.119.245.12   ICMP     106 Echo (ping) request  id=0x0001, seq=8/2048, ttl=3 (no response found!)
```

Source and destination address are used for host to host delivery. because host do not change networks during this transaction thus the logical addresses remain same.

9. Describe the pattern you see in the values in the Identification field of the IP datagrams being sent by your computer.



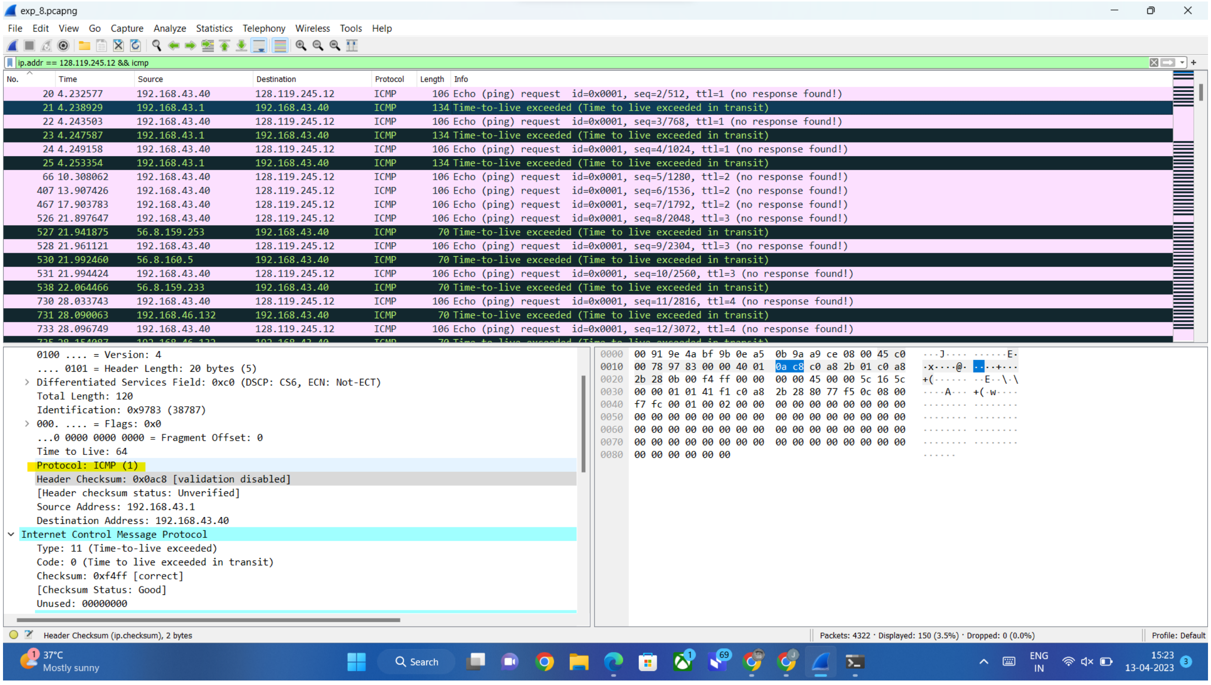
```
> Frame 20: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{81
> Ethernet II, Src: IntelCor_4a:bf:9b (00:91:9e:4a:bf:9b), Dst: 0e:a5:0b:9a:a9:ce (0e:a5:0b:9a:a9:ce
v Internet Protocol Version 4, Src: 192.168.43.40, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x165c (5724)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  v Time to Live: 1
      > [Expert Info (Note/Sequence): "Time To Live" only 1]
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.40
    Destination Address: 128.119.245.12
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
```



```
> Frame 22: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{81
> Ethernet II, Src: IntelCor_4a:bf:9b (00:91:9e:4a:bf:9b), Dst: 0e:a5:0b:9a:a9:ce (0e:a5:0b:9a:a9:ce
v Internet Protocol Version 4, Src: 192.168.43.40, 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: 92
    Identification: 0x165d (5725)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  v Time to Live: 1
    > [Expert Info (Note/Sequence): "Time To Live" only 1]
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.40
    Destination Address: 128.119.245.12
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
```

Now let's take a look at the ICMP packets being returned to your computer by the intervening routers where the TTL value was decremented to zero (and hence caused the ICMP error message to be returned to your computer). The display filter that you can use to show just these packets is "ip.dst==192.168.86.61 and icmp".

10. What is the upper layer protocol specified in the IP datagrams returned from the routers? [Note: the answers for Linux/MacOS differ from Windows here].


exp_8.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 128.119.245.12 && icmp

```
No.  Time        Source          Destination     Protocol Length Info
  20 4.232577    192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=2/512, ttl=1 (no response found!)
  21 4.238929    192.168.43.1    192.168.43.40   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
  22 4.243503    192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=3/768, ttl=1 (no response found!)
  23 4.247587    192.168.43.1    192.168.43.40   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
  24 4.249158    192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=4/1024, ttl=1 (no response found!)
  25 4.253354    192.168.43.1    192.168.43.40   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
  66 10.308062   192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=5/1280, ttl=2 (no response found!)
 407 13.907426   192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=6/1536, ttl=2 (no response found!)
 467 17.903783   192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=7/1792, ttl=2 (no response found!)
 526 21.897647   192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=8/2048, ttl=3 (no response found!)
 527 21.941875   56.8.159.253    192.168.43.40   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 528 21.961121   192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=9/2304, ttl=3 (no response found!)
 530 21.992460   56.8.160.5      192.168.43.40   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 531 21.994424   192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=10/2560, ttl=3 (no response found!)
 538 22.064466   56.8.159.233    192.168.43.40   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 730 28.033743   192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=11/2816, ttl=4 (no response found!)
 731 28.090063   192.168.46.132  192.168.43.40   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 733 28.096749   192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=12/3072, ttl=4 (no response found!)
```

```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 120
    Identification: 0x9783 (38787)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x0ac8 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.1
    Destination Address: 192.168.43.40
v Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
    [Checksum Status: Good]
    Unused: 00000000
```

```
0000  00 91 9e 4a bf 9b 0e a5  0b 9a a9 ce 08 00 45 c0   ···J···· ······E·
0010  00 78 97 83 00 00 40 01  0a c8 c0 a8 2b 01 c0 a8   ·x····@· ····+···
0020  2b 28 0b 00 f4 ff 00 00  00 00 45 00 00 5c 16 5c   +(······ ··E··\·\
0030  00 00 01 01 41 f1 c0 a8  2b 28 80 77 f5 0c 08 00   ····A··· +(·w····
0040  f7 fc 00 01 00 02 00 00  00 00 00 00 00 00 00 00   ········ ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00                                  ······
```

Header Checksum (ip.checksum), 2 bytes | Packets: 4322 · Displayed: 150 (3.5%) · Dropped: 0 (0.0%) | Profile: Default

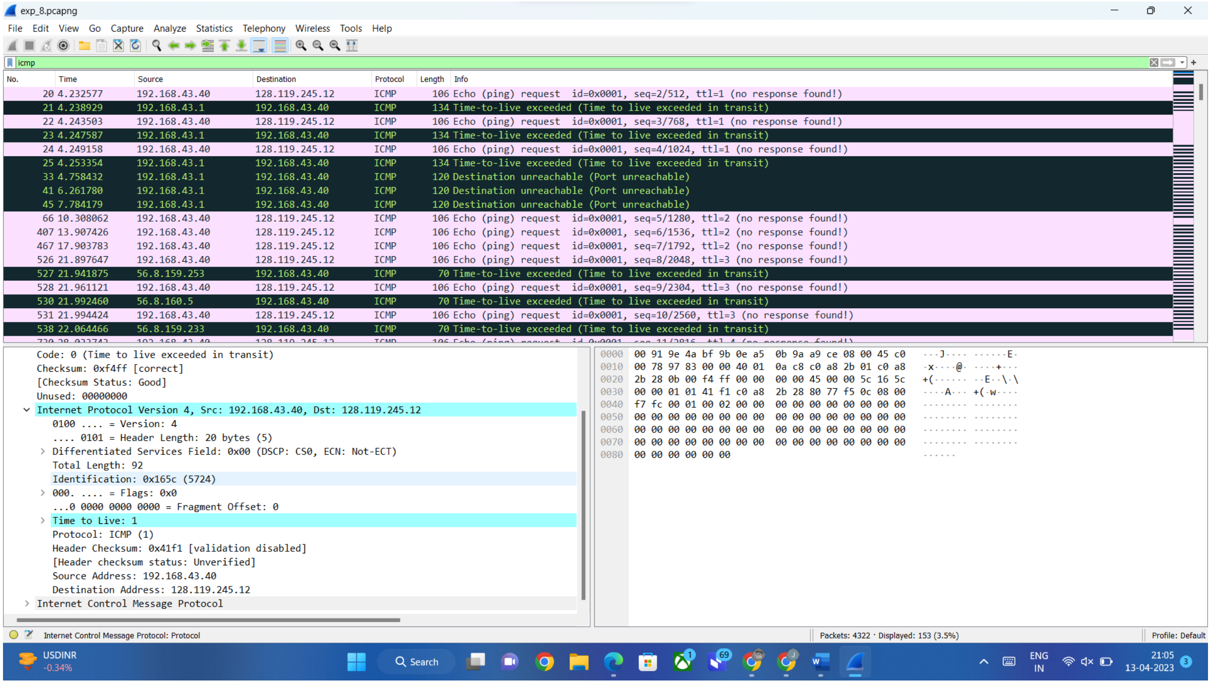
11. Are the values in the Identification fields (across the sequence of all of ICMP packets from all of the routers) similar in behavior to your answer to question 9 above?
No.It is different.

12. Are the values of the TTL fields similar, across all of ICMP packets from all of the routers?
    No, the value of TTL differs in each ICMP packet.

Part 2: Fragmentation

Sort the packet listing from Part 1, with any display filters cleared, according to time, by clicking on the *Time* column.

13. Find the first IP datagram containing the first part of the segment sent to 128.119.245.12 sent by your computer via the `traceroute` command to gaia.cs.umass.edu, *after* you specified that the `traceroute` packet length should be 3000. (Hint: This is packet 179 in the *ip-wireshark-trace1-1.pcapng* trace file in footnote 2. Packets 179, 180, and 181 are three IP datagrams created by fragmenting the first single 3000-byte UDP segment sent to 128.119.145.12). Has that segment been fragmented across more than one IP datagram? (Hint: the answer is yes[2]!)
    Yes


exp_8.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Packets: 4322 · Displayed: 153 (3.5%)
Profile: Default
USDINR
-0.34%
Search
ENG
IN
21:05
13-04-2023

```
No.  Time        Source          Destination     Protocol Length Info
  20 4.232577    192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=2/512, ttl=1 (no response found!)
  21 4.238929    192.168.43.1    192.168.43.40   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
  22 4.243503    192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=3/768, ttl=1 (no response found!)
  23 4.247587    192.168.43.1    192.168.43.40   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
  24 4.249158    192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=4/1024, ttl=1 (no response found!)
  25 4.253354    192.168.43.1    192.168.43.40   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
  33 4.758432    192.168.43.1    192.168.43.40   ICMP     120 Destination unreachable (Port unreachable)
  41 6.261780    192.168.43.1    192.168.43.40   ICMP     120 Destination unreachable (Port unreachable)
  45 7.784179    192.168.43.1    192.168.43.40   ICMP     120 Destination unreachable (Port unreachable)
  66 10.308062   192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=5/1280, ttl=2 (no response found!)
 407 13.907426   192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=6/1536, ttl=2 (no response found!)
 467 17.903783   192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=7/1792, ttl=2 (no response found!)
 526 21.897647   192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=8/2048, ttl=3 (no response found!)
 527 21.941875   56.8.159.253    192.168.43.40   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 528 21.961121   192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=9/2304, ttl=3 (no response found!)
 530 21.992460   56.8.160.5      192.168.43.40   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
 531 21.994424   192.168.43.40   128.119.245.12  ICMP     106 Echo (ping) request  id=0x0001, seq=10/2560, ttl=3 (no response found!)
 538 22.064466   56.8.159.233    192.168.43.40   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
```

```
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
    [Checksum Status: Good]
    Unused: 00000000
  ⌄ Internet Protocol Version 4, Src: 192.168.43.40, 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: 92
      Identification: 0x165c (5724)
    > 000. .... = Flags: 0x0
      ...0 0000 0000 0000 = Fragment Offset: 0
    > Time to Live: 1
      Protocol: ICMP (1)
      Header Checksum: 0x41f1 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 192.168.43.40
      Destination Address: 128.119.245.12
  > Internet Control Message Protocol
```

```
0000  00 91 9e 4a bf 9b 0e a5  0b 9a a9 ce 08 00 45 c0   ···J···· ······E·
0010  00 78 97 83 00 00 40 01  0a c8 c0 a8 2b 01 c0 a8   ·x····@· ····+···
0020  2b 28 0b 00 f4 ff 00 00  00 00 45 00 00 5c 16 5c   +(······ ··E··\·\
0030  00 00 01 01 41 f1 c0 a8  2b 28 80 77 f5 0c 08 00   ····A··· +(·w····
0040  f7 fc 00 01 00 02 00 00  00 00 00 00 00 00 00 00   ········ ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00                                  ······
```

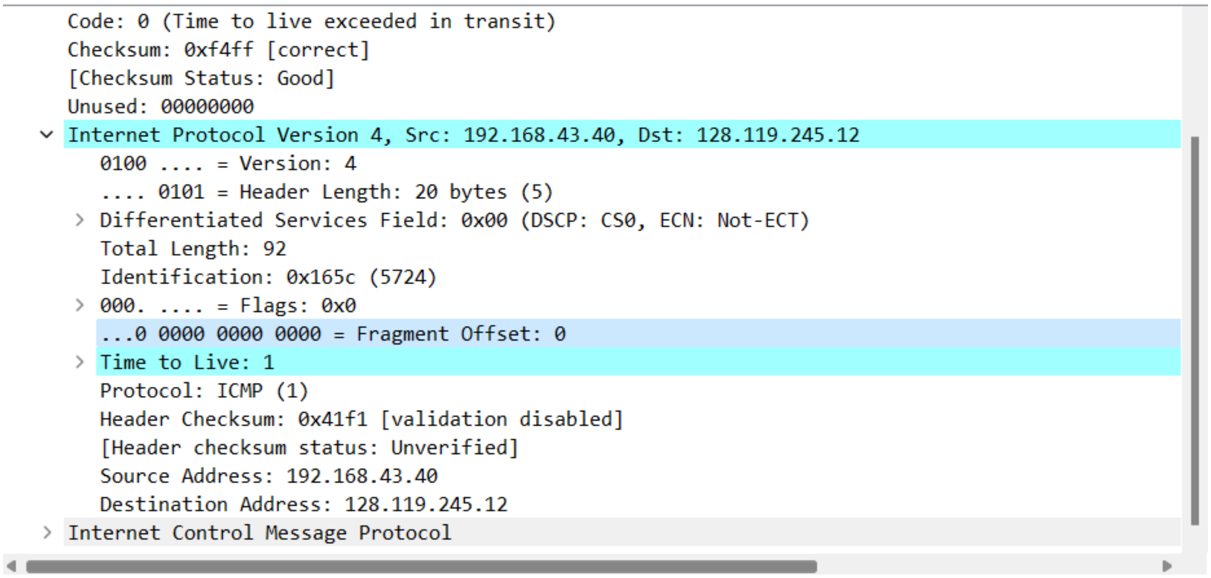
Internet Control Message Protocol: Protocol

14. What information in the IP header indicates that this datagram been fragmented?
    It indicates fragment offset : 0
15. What information in the IP header for this packet indicates whether this is the first fragment versus a latter fragment?

    The Flags bit for more fragments is set, indicating that the datagram has been fragmented. Since the fragment offset is 0, we know that this is the first fragment. This first datagram has a total length of 1500, including the header.

16. How many bytes are there in is this IP datagram (header plus payload)?
    20 bytes

[2]



```
Code: 0 (Time to live exceeded in transit)
Checksum: 0xf4ff [correct]
[Checksum Status: Good]
Unused: 00000000
Internet Protocol Version 4, Src: 192.168.43.40, 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: 92
  Identification: 0x165c (5724)
  000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 1
  Protocol: ICMP (1)
  Header Checksum: 0x41f1 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.43.40
  Destination Address: 128.119.245.12
Internet Control Message Protocol
```

17. Now inspect the datagram containing the second fragment of the fragmented UDP segment. What information in the IP header indicates that this is *not* the first datagram fragment?

    We can tell that this is not the first fragment, since the fragment offset is 1480. It is the last fragment, since the more fragments flag is not set.

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

    The IP header fields that changed between the fragments are: total length, flags, fragment offset, and checksum.

19. Now find the IP datagram containing the third fragment of the original UDP segment. What information in the IP header indicates that this is the last fragment of that segment?

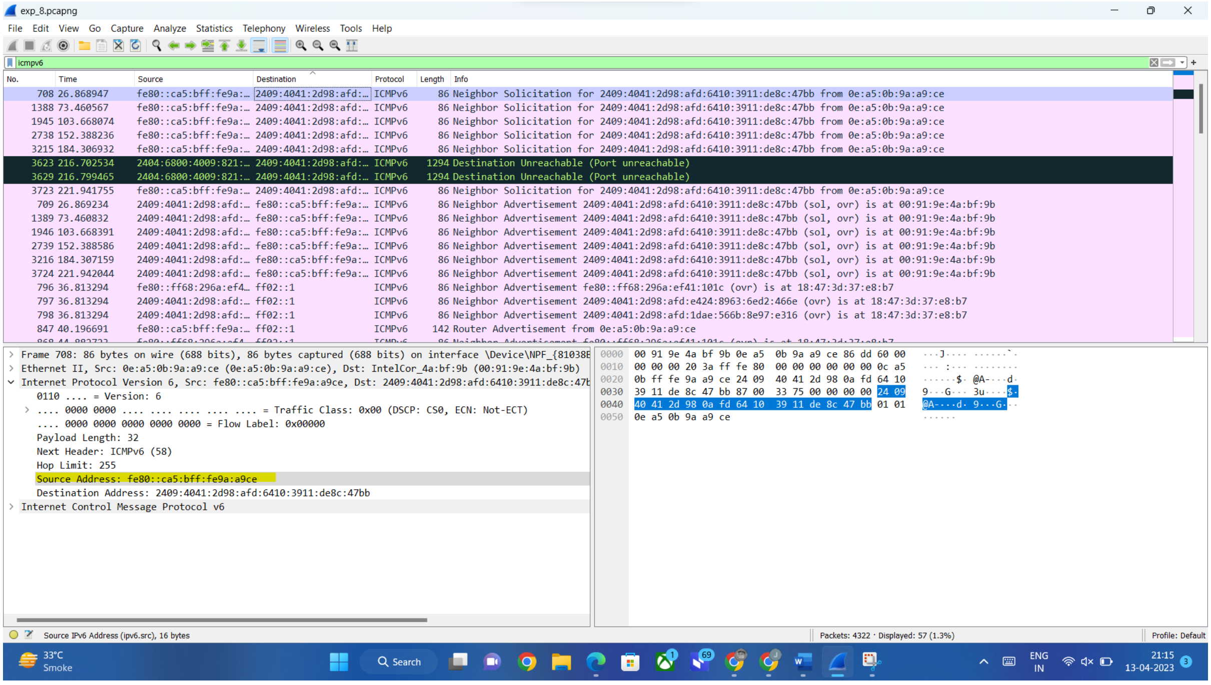
    The IP header fields that changed between all of the packets are: fragment offset, and checksum. Between the first two packets and the last packet, we see a change in total length, and also in the flags.

Part 3: IPv6

Answer the following questions:

20. What is the IPv6 address of the computer making the DNS AAAA request? This is the source address of the 20th packet in the trace. Give the IPv6 source address for this datagram in the exact same form as displayed in the Wireshark window[3].

[3]



exp_8.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmpv6

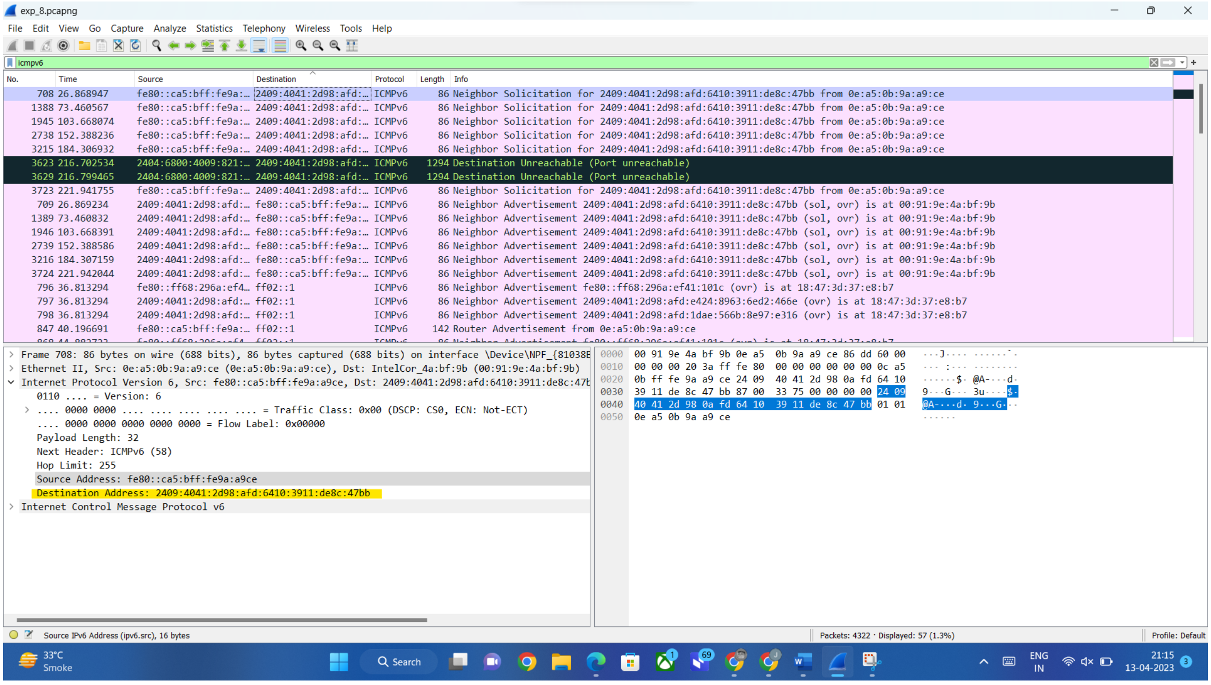
```
No.      Time        Source                 Destination            Protocol  Length Info
   708 26.868947     fe80::ca5:bff:fe9a:…   2409:4041:2d98:afd:…   ICMPv6      86 Neighbor Solicitation for 2409:4041:2d98:afd:6410:3911:de8c:47bb from 0e:a5:0b:9a:a9:ce
  1388 73.460567     fe80::ca5:bff:fe9a:…   2409:4041:2d98:afd:…   ICMPv6      86 Neighbor Solicitation for 2409:4041:2d98:afd:6410:3911:de8c:47bb from 0e:a5:0b:9a:a9:ce
  1945 103.668074    fe80::ca5:bff:fe9a:…   2409:4041:2d98:afd:…   ICMPv6      86 Neighbor Solicitation for 2409:4041:2d98:afd:6410:3911:de8c:47bb from 0e:a5:0b:9a:a9:ce
  2738 152.388236    fe80::ca5:bff:fe9a:…   2409:4041:2d98:afd:…   ICMPv6      86 Neighbor Solicitation for 2409:4041:2d98:afd:6410:3911:de8c:47bb from 0e:a5:0b:9a:a9:ce
  3215 184.306932    fe80::ca5:bff:fe9a:…   2409:4041:2d98:afd:…   ICMPv6      86 Neighbor Solicitation for 2409:4041:2d98:afd:6410:3911:de8c:47bb from 0e:a5:0b:9a:a9:ce
  3623 216.702534    2404:6800:4009:821:…   2409:4041:2d98:afd:…   ICMPv6    1294 Destination Unreachable (Port unreachable)
  3629 216.799465    2404:6800:4009:821:…   2409:4041:2d98:afd:…   ICMPv6    1294 Destination Unreachable (Port unreachable)
  3723 221.941755    fe80::ca5:bff:fe9a:…   2409:4041:2d98:afd:…   ICMPv6      86 Neighbor Solicitation for 2409:4041:2d98:afd:6410:3911:de8c:47bb from 0e:a5:0b:9a:a9:ce
   709 26.869234     2409:4041:2d98:afd:…   fe80::ca5:bff:fe9a:…   ICMPv6      86 Neighbor Advertisement 2409:4041:2d98:afd:6410:3911:de8c:47bb (sol, ovr) is at 00:91:9e:4a:bf:9b
  1389 73.460832     2409:4041:2d98:afd:…   fe80::ca5:bff:fe9a:…   ICMPv6      86 Neighbor Advertisement 2409:4041:2d98:afd:6410:3911:de8c:47bb (sol, ovr) is at 00:91:9e:4a:bf:9b
  1946 103.668391    2409:4041:2d98:afd:…   fe80::ca5:bff:fe9a:…   ICMPv6      86 Neighbor Advertisement 2409:4041:2d98:afd:6410:3911:de8c:47bb (sol, ovr) is at 00:91:9e:4a:bf:9b
  2739 152.388586    2409:4041:2d98:afd:…   fe80::ca5:bff:fe9a:…   ICMPv6      86 Neighbor Advertisement 2409:4041:2d98:afd:6410:3911:de8c:47bb (sol, ovr) is at 00:91:9e:4a:bf:9b
  3216 184.307159    2409:4041:2d98:afd:…   fe80::ca5:bff:fe9a:…   ICMPv6      86 Neighbor Advertisement 2409:4041:2d98:afd:6410:3911:de8c:47bb (sol, ovr) is at 00:91:9e:4a:bf:9b
  3724 221.942044    2409:4041:2d98:afd:…   fe80::ca5:bff:fe9a:…   ICMPv6      86 Neighbor Advertisement 2409:4041:2d98:afd:6410:3911:de8c:47bb (sol, ovr) is at 00:91:9e:4a:bf:9b
   796 36.813294     fe80::ff68:296a:ef4…   ff02::1                ICMPv6      86 Neighbor Advertisement fe80::ff68:296a:ef41:101c (ovr) is at 18:47:3d:37:e8:b7
   797 36.813294     2409:4041:2d98:afd:…   ff02::1                ICMPv6      86 Neighbor Advertisement 2409:4041:2d98:afd:e424:8963:6ed2:466e (ovr) is at 18:47:3d:37:e8:b7
   798 36.813294     2409:4041:2d98:afd:…   ff02::1                ICMPv6      86 Neighbor Advertisement 2409:4041:2d98:afd:1dae:566b:8e97:e316 (ovr) is at 18:47:3d:37:e8:b7
   847 40.196691     fe80::ca5:bff:fe9a:…   ff02::1                ICMPv6     142 Router Advertisement from 0e:a5:0b:9a:a9:ce
   868 44.882723     fe80::ff68:296a:ef4…   ff02::1                ICMPv6      86 Neighbor Advertisement fe80::ff68:296a:ef41:101c (ovr) is at 18:47:3d:37:e8:b7
```

```
> Frame 708: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{81038E
> Ethernet II, Src: 0e:a5:0b:9a:a9:ce (0e:a5:0b:9a:a9:ce), Dst: IntelCor_4a:bf:9b (00:91:9e:4a:bf:9b)
v Internet Protocol Version 6, Src: fe80::ca5:bff:fe9a:a9ce, Dst: 2409:4041:2d98:afd:6410:3911:de8c:47b
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 32
    Next Header: ICMPv6 (58)
    Hop Limit: 255
    Source Address: fe80::ca5:bff:fe9a:a9ce
    Destination Address: 2409:4041:2d98:afd:6410:3911:de8c:47bb
> Internet Control Message Protocol v6
```

```
0000  00 91 9e 4a bf 9b 0e a5  0b 9a a9 ce 86 dd 60 00   ···J···· ······`·
0010  00 00 00 20 3a ff fe 80  00 00 00 00 00 00 0c a5   ··· :··· ········
0020  0b ff fe 9a a9 ce 24 09  40 41 2d 98 0a fd 64 10   ······$· @A-···d·
0030  39 11 de 8c 47 bb 87 00  33 75 00 00 00 00 24 09   9···G··· 3u····$·
0040  40 41 2d 98 0a fd 64 10  39 11 de 8c 47 bb 01 01   @A-···d· 9···G···
0050  0e a5 0b 9a a9 ce                                  ······
```

Source IPv6 Address (ipv6.src), 16 bytes   Packets: 4322 · Displayed: 57 (1.3%)   Profile: Default

21. What is the IPv6 destination address for this datagram? Give this IPv6 address in the exact same form as displayed in the Wireshark window.



exp_8.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmpv6

```
No.      Time        Source                 Destination            Protocol  Length Info
   708 26.868947     fe80::ca5:bff:fe9a:…   2409:4041:2d98:afd:…   ICMPv6      86 Neighbor Solicitation for 2409:4041:2d98:afd:6410:3911:de8c:47bb from 0e:a5:0b:9a:a9:ce
  1388 73.460567     fe80::ca5:bff:fe9a:…   2409:4041:2d98:afd:…   ICMPv6      86 Neighbor Solicitation for 2409:4041:2d98:afd:6410:3911:de8c:47bb from 0e:a5:0b:9a:a9:ce
  1945 103.668074    fe80::ca5:bff:fe9a:…   2409:4041:2d98:afd:…   ICMPv6      86 Neighbor Solicitation for 2409:4041:2d98:afd:6410:3911:de8c:47bb from 0e:a5:0b:9a:a9:ce
  2738 152.388236    fe80::ca5:bff:fe9a:…   2409:4041:2d98:afd:…   ICMPv6      86 Neighbor Solicitation for 2409:4041:2d98:afd:6410:3911:de8c:47bb from 0e:a5:0b:9a:a9:ce
  3215 184.306932    fe80::ca5:bff:fe9a:…   2409:4041:2d98:afd:…   ICMPv6      86 Neighbor Solicitation for 2409:4041:2d98:afd:6410:3911:de8c:47bb from 0e:a5:0b:9a:a9:ce
  3623 216.702534    2404:6800:4009:821:…   2409:4041:2d98:afd:…   ICMPv6    1294 Destination Unreachable (Port unreachable)
  3629 216.799465    2404:6800:4009:821:…   2409:4041:2d98:afd:…   ICMPv6    1294 Destination Unreachable (Port unreachable)
  3723 221.941755    fe80::ca5:bff:fe9a:…   2409:4041:2d98:afd:…   ICMPv6      86 Neighbor Solicitation for 2409:4041:2d98:afd:6410:3911:de8c:47bb from 0e:a5:0b:9a:a9:ce
   709 26.869234     2409:4041:2d98:afd:…   fe80::ca5:bff:fe9a:…   ICMPv6      86 Neighbor Advertisement 2409:4041:2d98:afd:6410:3911:de8c:47bb (sol, ovr) is at 00:91:9e:4a:bf:9b
  1389 73.460832     2409:4041:2d98:afd:…   fe80::ca5:bff:fe9a:…   ICMPv6      86 Neighbor Advertisement 2409:4041:2d98:afd:6410:3911:de8c:47bb (sol, ovr) is at 00:91:9e:4a:bf:9b
  1946 103.668391    2409:4041:2d98:afd:…   fe80::ca5:bff:fe9a:…   ICMPv6      86 Neighbor Advertisement 2409:4041:2d98:afd:6410:3911:de8c:47bb (sol, ovr) is at 00:91:9e:4a:bf:9b
  2739 152.388586    2409:4041:2d98:afd:…   fe80::ca5:bff:fe9a:…   ICMPv6      86 Neighbor Advertisement 2409:4041:2d98:afd:6410:3911:de8c:47bb (sol, ovr) is at 00:91:9e:4a:bf:9b
  3216 184.307159    2409:4041:2d98:afd:…   fe80::ca5:bff:fe9a:…   ICMPv6      86 Neighbor Advertisement 2409:4041:2d98:afd:6410:3911:de8c:47bb (sol, ovr) is at 00:91:9e:4a:bf:9b
  3724 221.942044    2409:4041:2d98:afd:…   fe80::ca5:bff:fe9a:…   ICMPv6      86 Neighbor Advertisement 2409:4041:2d98:afd:6410:3911:de8c:47bb (sol, ovr) is at 00:91:9e:4a:bf:9b
   796 36.813294     fe80::ff68:296a:ef4…   ff02::1                ICMPv6      86 Neighbor Advertisement fe80::ff68:296a:ef41:101c (ovr) is at 18:47:3d:37:e8:b7
   797 36.813294     2409:4041:2d98:afd:…   ff02::1                ICMPv6      86 Neighbor Advertisement 2409:4041:2d98:afd:e424:8963:6ed2:466e (ovr) is at 18:47:3d:37:e8:b7
   798 36.813294     2409:4041:2d98:afd:…   ff02::1                ICMPv6      86 Neighbor Advertisement 2409:4041:2d98:afd:1dae:566b:8e97:e316 (ovr) is at 18:47:3d:37:e8:b7
   847 40.196691     fe80::ca5:bff:fe9a:…   ff02::1                ICMPv6     142 Router Advertisement from 0e:a5:0b:9a:a9:ce
   868 44.882723     fe80::ff68:296a:ef4…   ff02::1                ICMPv6      86 Neighbor Advertisement fe80::ff68:296a:ef41:101c (ovr) is at 18:47:3d:37:e8:b7
```

```
> Frame 708: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{81038E
> Ethernet II, Src: 0e:a5:0b:9a:a9:ce (0e:a5:0b:9a:a9:ce), Dst: IntelCor_4a:bf:9b (00:91:9e:4a:bf:9b)
v Internet Protocol Version 6, Src: fe80::ca5:bff:fe9a:a9ce, Dst: 2409:4041:2d98:afd:6410:3911:de8c:47b
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 32
    Next Header: ICMPv6 (58)
    Hop Limit: 255
    Source Address: fe80::ca5:bff:fe9a:a9ce
    Destination Address: 2409:4041:2d98:afd:6410:3911:de8c:47bb
> Internet Control Message Protocol v6
```

```
0000  00 91 9e 4a bf 9b 0e a5  0b 9a a9 ce 86 dd 60 00   ···J···· ······`·
0010  00 00 00 20 3a ff fe 80  00 00 00 00 00 00 0c a5   ··· :··· ········
0020  0b ff fe 9a a9 ce 24 09  40 41 2d 98 0a fd 64 10   ······$· @A-···d·
0030  39 11 de 8c 47 bb 87 00  33 75 00 00 00 00 24 09   9···G··· 3u····$·
0040  40 41 2d 98 0a fd 64 10  39 11 de 8c 47 bb 01 01   @A-···d· 9···G···
0050  0e a5 0b 9a a9 ce                                  ······
```

Source IPv6 Address (ipv6.src), 16 bytes   Packets: 4322 · Displayed: 57 (1.3%)   Profile: Default

22. What is the value of the flow label for this datagram?
0

23. How much payload data is carried in this datagram?

24 bytes

24. What is the upper layer protocol to which this datagram's payload will be delivered at the destination?

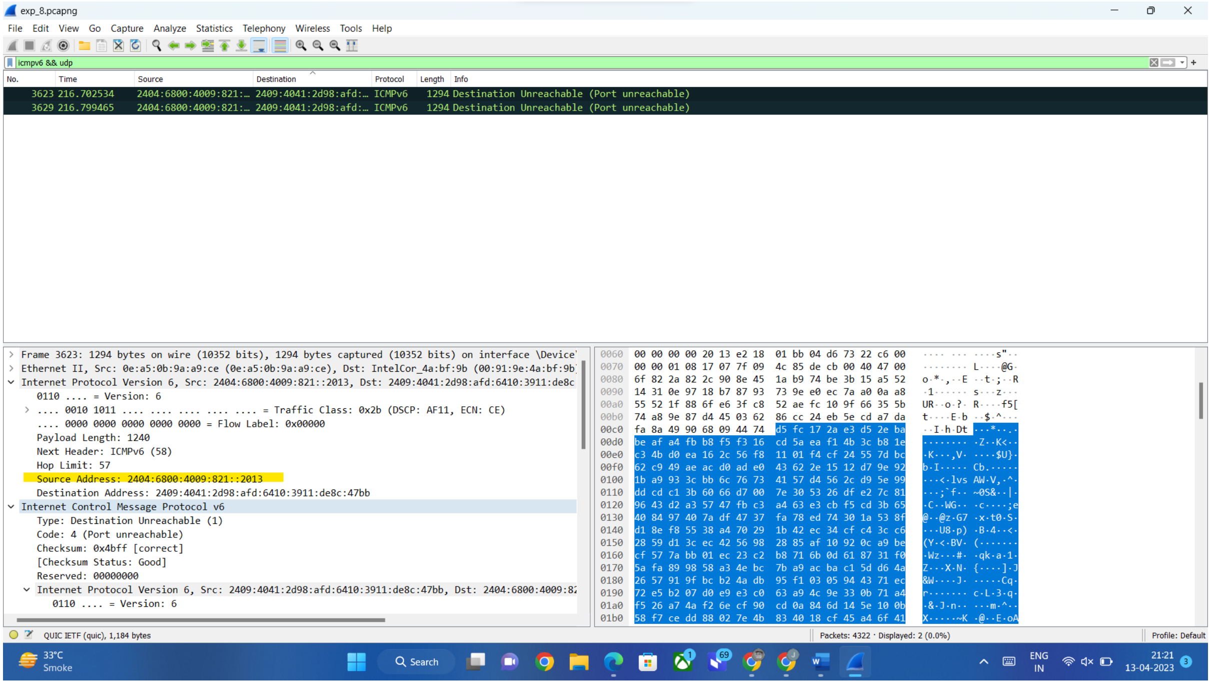
    The upper layer protocol to which this datagram's payload will be delivered at the destination is UDP

Lastly, find the IPv6 DNS response to the IPv6 DNS AAAA request made in the 20th packet in this trace. This DNS response contains IPv6 addresses for youtube.com.

25. How many IPv6 addresses are returned in the response to this AAAA request?

    Three IPv6 addresses are returned in the response to this AAAA request.

26. What is the first of the IPv6 addresses returned by the DNS for youtube.com (in the *ip-wireshark-trace2-1.pcapng* trace file, this is also the address that is numerically the smallest)? Give this IPv6 address in the exact same shorthand form as displayed in the Wireshark window.


exp_8.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmpv6 && udp
33°C
Smoke
Search
ENG
IN
21:21
13-04-2023

```
No.   Time        Source                Destination           Protocol Length Info
 3623 216.702534  2404:6800:4009:821:…  2409:4041:2d98:afd:…  ICMPv6   1294 Destination Unreachable (Port unreachable)
 3629 216.799465  2404:6800:4009:821:…  2409:4041:2d98:afd:…  ICMPv6   1294 Destination Unreachable (Port unreachable)
```

```
> Frame 3623: 1294 bytes on wire (10352 bits), 1294 bytes captured (10352 bits) on interface \Device
> Ethernet II, Src: 0e:a5:0b:9a:a9:ce (0e:a5:0b:9a:a9:ce), Dst: IntelCor_4a:bf:9b (00:91:9e:4a:bf:9b
v Internet Protocol Version 6, Src: 2404:6800:4009:821::2013, Dst: 2409:4041:2d98:afd:6410:3911:de8c
    0110 .... = Version: 6
  > .... 0010 1011 .... .... .... .... .... = Traffic Class: 0x2b (DSCP: AF11, ECN: CE)
    .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 1240
    Next Header: ICMPv6 (58)
    Hop Limit: 57
    Source Address: 2404:6800:4009:821::2013
    Destination Address: 2409:4041:2d98:afd:6410:3911:de8c:47bb
v Internet Control Message Protocol v6
    Type: Destination Unreachable (1)
    Code: 4 (Port unreachable)
    Checksum: 0x4bff [correct]
    [Checksum Status: Good]
    Reserved: 00000000
  v Internet Protocol Version 6, Src: 2409:4041:2d98:afd:6410:3911:de8c:47bb, Dst: 2404:6800:4009:82
      0110 .... = Version: 6
```

```
0060  00 00 00 00 20 13 e2 18  01 bb 04 d6 73 22 c6 00   ···· ··· ····s"··
0070  00 00 01 08 17 07 7f 09  4c 85 de cb 00 40 47 00   ········ L····@G·
0080  6f 82 2a 82 2c 90 8e 45  1a b9 74 be 3b 15 a5 52   o·*·,··E ··t·;··R
0090  14 31 0e 97 18 b7 87 93  73 9e e0 ec 7a a0 0a a8   ·1······ s···z···
00a0  55 52 1f 88 6f e6 3f c8  52 ae fc 10 9f 66 35 5b   UR··o·?· R····f5[
00b0  74 a8 9e 87 d4 45 03 62  86 cc 24 eb 5e cd a7 da   t····E·b ··$·^···
00c0  fa 8a 49 90 68 09 44 74  d5 fc 17 2a e3 d5 2e ba   ··I·h·Dt ···*··.·
00d0  be af a4 fb b8 f5 f3 16  cd 5a ea f1 4b 3c b8 1e   ········ ·Z··K<··
00e0  c3 4b d0 ea 16 2c 56 f8  11 01 f4 cf 24 55 7d bc   ·K···,V· ····$U}·
00f0  62 c9 49 ae ac d0 ad e0  43 62 2e 15 12 d7 9e 92   b·I····· Cb.·····
0100  1b a9 93 3c bb 6c 76 73  41 57 d4 56 2c d9 5e 99   ···<·lvs AW·V,·^·
0110  dd cd c1 3b 60 66 d7 00  7e 30 53 26 df e2 7c 81   ···;`f·· ~0S&··|·
0120  96 43 d2 a3 57 47 fb c3  a4 63 e3 cb f5 cd 3b 65   ·C··WG·· ·c····;e
0130  40 84 97 40 7a df 47 37  fa 78 ed 74 30 1a 53 8f   @··@z·G7 ·x·t0·S·
0140  d1 8e f8 55 38 a4 70 29  1b 42 ec 34 cf c4 3c c6   ···U8·p) ·B·4··<·
0150  28 59 d1 3c ec 42 56 98  28 85 af 10 92 0c a9 be   (Y·<·BV· (·······
0160  cf 57 7a bb 01 ec 23 c2  b8 71 6b 0d 61 87 31 f0   ·Wz···#· ·qk·a·1·
0170  5a fa 89 98 58 a3 4e bc  7b a9 ac ba c1 5d d6 4a   Z···X·N· {····]·J
0180  26 57 91 9f bc b2 4a db  95 f1 03 05 94 43 71 ec   &W····J· ·····Cq·
0190  72 e5 b2 07 d0 e9 e3 c0  63 a9 4c 9e 33 0b 71 a4   r······· c·L·3·q·
01a0  f5 26 a7 4a f2 6e cf 90  cd 0a 84 6d 14 5e 10 0b   ·&·J·n·· ···m·^··
01b0  58 f7 ce dd 88 02 7e 4b  83 40 18 cf 45 a4 6f 41   X·····~K ·@··E·oA
```

```
QUIC IETF (quic), 1,184 bytes     Packets: 4322 · Displayed: 2 (0.0%)     Profile: Default
```