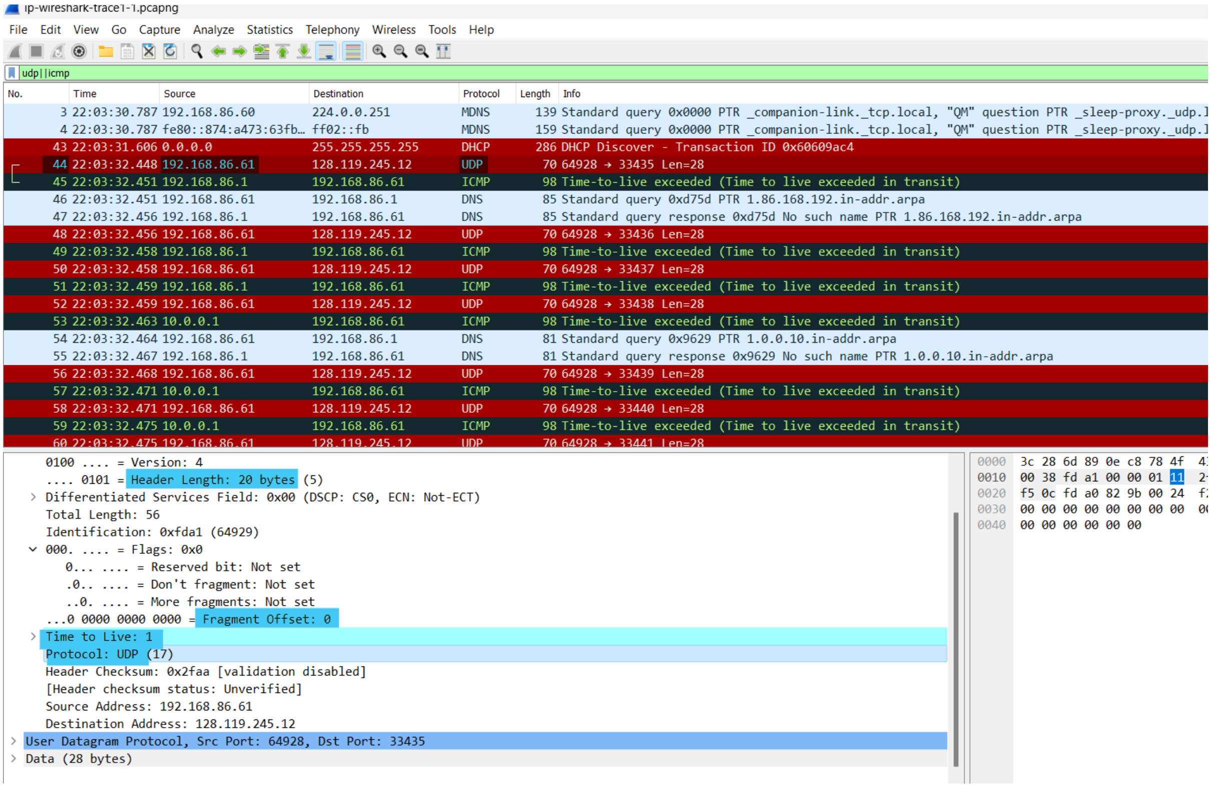
Lab 04_IP

Part 1: Basic IPv4

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?**

   The IP address of this computer: 192.168.86.61



```
No.  Time          Source                Destination      Protocol Length Info
   3 22:03:30.787 192.168.86.60         224.0.0.251      MDNS     139 Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _sleep-proxy._udp.l
   4 22:03:30.787 fe80::874:a473:63fb…  ff02::fb         MDNS     159 Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _sleep-proxy._udp.l
  43 22:03:31.606 0.0.0.0               255.255.255.255  DHCP     286 DHCP Discover - Transaction ID 0x60609ac4
  44 22:03:32.448 192.168.86.61         128.119.245.12   UDP       70 64928 → 33435 Len=28
  45 22:03:32.451 192.168.86.1          192.168.86.61    ICMP      98 Time-to-live exceeded (Time to live exceeded in transit)
  46 22:03:32.451 192.168.86.61         192.168.86.1     DNS       85 Standard query 0xd75d PTR 1.86.168.192.in-addr.arpa
  47 22:03:32.456 192.168.86.1          192.168.86.61    DNS       85 Standard query response 0xd75d No such name PTR 1.86.168.192.in-addr.arpa
  48 22:03:32.456 192.168.86.61         128.119.245.12   UDP       70 64928 → 33436 Len=28
  49 22:03:32.458 192.168.86.1          192.168.86.61    ICMP      98 Time-to-live exceeded (Time to live exceeded in transit)
  50 22:03:32.458 192.168.86.61         128.119.245.12   UDP       70 64928 → 33437 Len=28
  51 22:03:32.459 192.168.86.1          192.168.86.61    ICMP      98 Time-to-live exceeded (Time to live exceeded in transit)
  52 22:03:32.459 192.168.86.61         128.119.245.12   UDP       70 64928 → 33438 Len=28
  53 22:03:32.463 10.0.0.1              192.168.86.61    ICMP      98 Time-to-live exceeded (Time to live exceeded in transit)
  54 22:03:32.464 192.168.86.61         192.168.86.1     DNS       81 Standard query 0x9629 PTR 1.0.0.10.in-addr.arpa
  55 22:03:32.467 192.168.86.1          192.168.86.61    DNS       81 Standard query response 0x9629 No such name PTR 1.0.0.10.in-addr.arpa
  56 22:03:32.468 192.168.86.61         128.119.245.12   UDP       70 64928 → 33439 Len=28
  57 22:03:32.471 10.0.0.1              192.168.86.61    ICMP      98 Time-to-live exceeded (Time to live exceeded in transit)
  58 22:03:32.471 192.168.86.61         128.119.245.12   UDP       70 64928 → 33440 Len=28
  59 22:03:32.475 10.0.0.1              192.168.86.61    ICMP      98 Time-to-live exceeded (Time to live exceeded in transit)
  60 22:03:32.475 192.168.86.61         128.119.245.12   UDP       70 64928 → 33441 Len=28
```

```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xfda1 (64929)
  v 000. .... = Flags: 0x0
      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: 1
    Protocol: UDP (17)
    Header Checksum: 0x2faa [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.86.61
    Destination Address: 128.119.245.12
> User Datagram Protocol, Src Port: 64928, Dst Port: 33435
> Data (28 bytes)
```

```
0000  3c 28 6d 89 0e c8 78 4f  4
0010  00 38 fd a1 00 00 01 11  2
0020  f5 0c fd a0 82 9b 00 24  f
0030  00 00 00 00 00 00 00 00  0
0040  00 00 00 00 00 00
```

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

   TTL: 1

3. **What is the value in the upper layer protocol field in this IPv4 datagram's header?**

   Protocol: UDP

4. **How many bytes are in the IP header?**

   There are 20 bytes in the IP header.

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

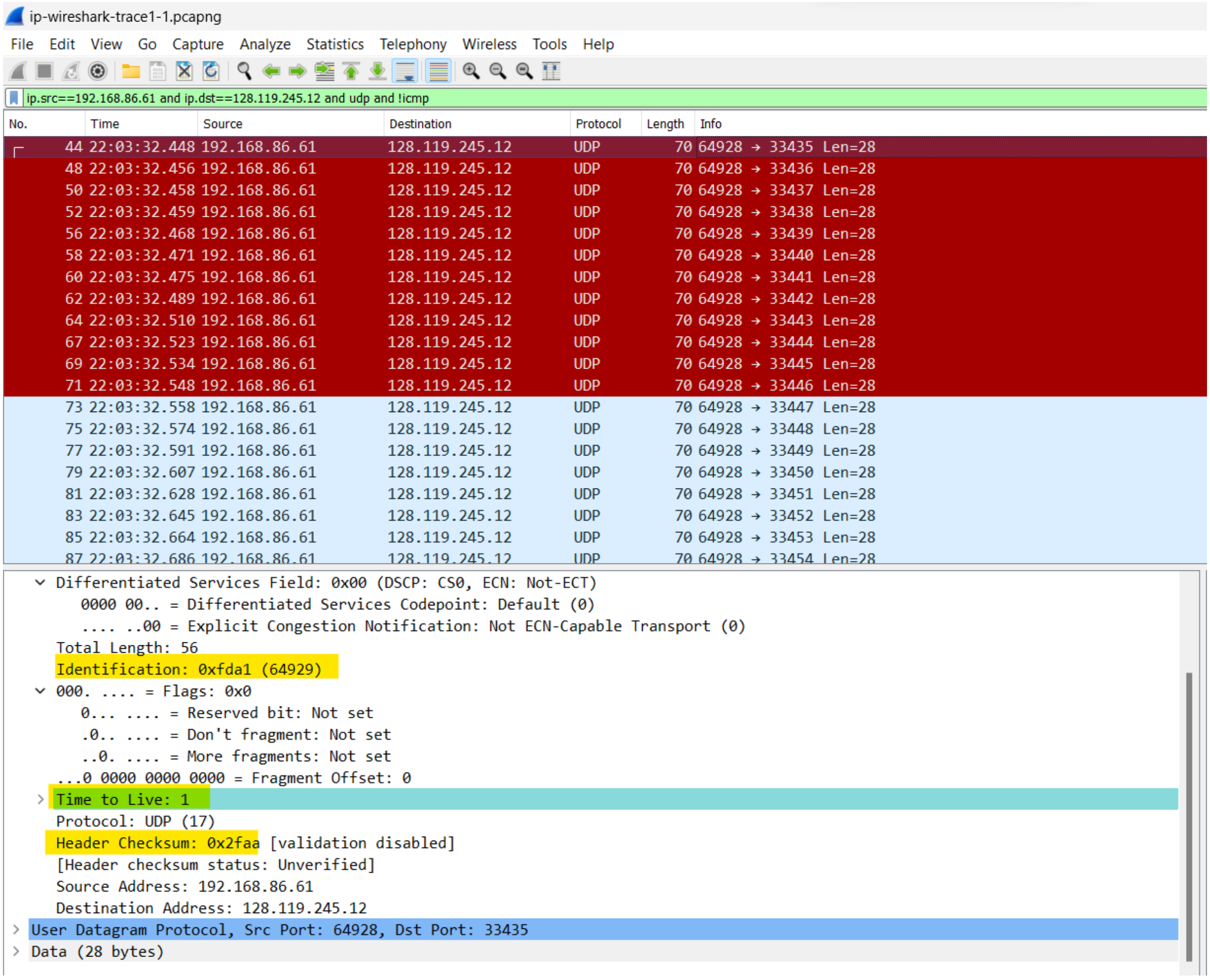
   There are 20 bytes in the IP header which leaves 36 bytes for the payload of the IP datagram because we were sending a packet of length 56 bytes.

   Total length – IP header = 56 - 20 = 36 bytes

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

   The fragment offset is set to 0, therefore, the packet has not been fragmented.

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?**
   - The Identification field (to verify packets)
   - The Time to live field (traceroute increments each subsequent packet)
   - The Header checksum field (header changes, so must checksum))
     changes from each datagram to the next.

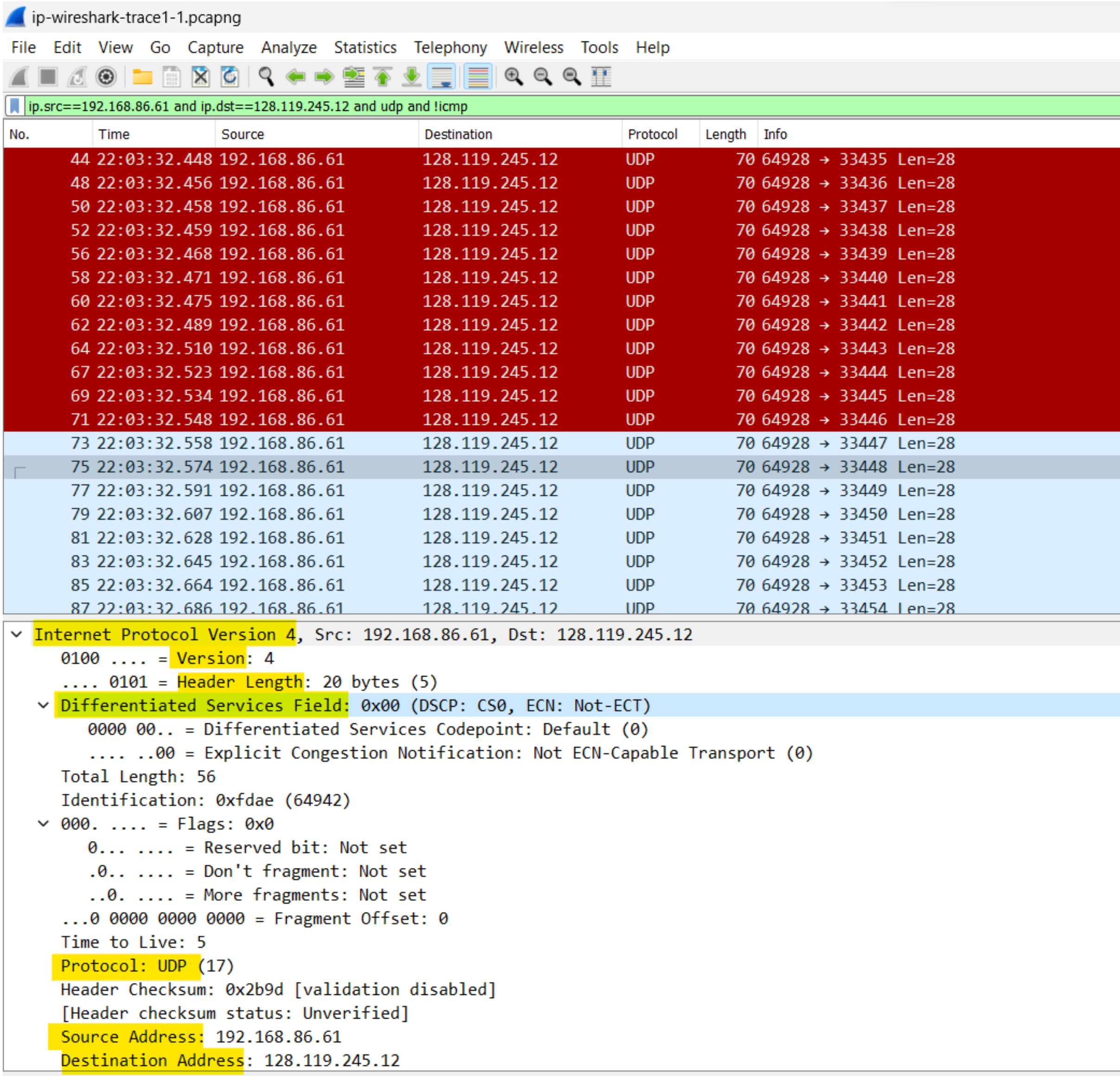

ip-wireshark-trace1-1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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 22:03:32.448  192.168.86.61   128.119.245.12   UDP       70      64928 → 33435 Len=28
  48 22:03:32.456  192.168.86.61   128.119.245.12   UDP       70      64928 → 33436 Len=28
  50 22:03:32.458  192.168.86.61   128.119.245.12   UDP       70      64928 → 33437 Len=28
  52 22:03:32.459  192.168.86.61   128.119.245.12   UDP       70      64928 → 33438 Len=28
  56 22:03:32.468  192.168.86.61   128.119.245.12   UDP       70      64928 → 33439 Len=28
  58 22:03:32.471  192.168.86.61   128.119.245.12   UDP       70      64928 → 33440 Len=28
  60 22:03:32.475  192.168.86.61   128.119.245.12   UDP       70      64928 → 33441 Len=28
  62 22:03:32.489  192.168.86.61   128.119.245.12   UDP       70      64928 → 33442 Len=28
  64 22:03:32.510  192.168.86.61   128.119.245.12   UDP       70      64928 → 33443 Len=28
  67 22:03:32.523  192.168.86.61   128.119.245.12   UDP       70      64928 → 33444 Len=28
  69 22:03:32.534  192.168.86.61   128.119.245.12   UDP       70      64928 → 33445 Len=28
  71 22:03:32.548  192.168.86.61   128.119.245.12   UDP       70      64928 → 33446 Len=28
  73 22:03:32.558  192.168.86.61   128.119.245.12   UDP       70      64928 → 33447 Len=28
  75 22:03:32.574  192.168.86.61   128.119.245.12   UDP       70      64928 → 33448 Len=28
  77 22:03:32.591  192.168.86.61   128.119.245.12   UDP       70      64928 → 33449 Len=28
  79 22:03:32.607  192.168.86.61   128.119.245.12   UDP       70      64928 → 33450 Len=28
  81 22:03:32.628  192.168.86.61   128.119.245.12   UDP       70      64928 → 33451 Len=28
  83 22:03:32.645  192.168.86.61   128.119.245.12   UDP       70      64928 → 33452 Len=28
  85 22:03:32.664  192.168.86.61   128.119.245.12   UDP       70      64928 → 33453 Len=28
  87 22:03:32.686  192.168.86.61   128.119.245.12   UDP       70      64928 → 33454 Len=28
```

```
  ˅ 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: 0xfda1 (64929)
  ˅ 000. .... = Flags: 0x0
      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: 1
    Protocol: UDP (17)
    Header Checksum: 0x2faa [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.86.61
    Destination Address: 128.119.245.12
> User Datagram Protocol, Src Port: 64928, Dst Port: 33435
> Data (28 bytes)
```

8. **Which fields in this sequence of IP datagrams (containing UDP segments) stay constant? Why?**
    - IP version (IPv4)
    - Header length
    - Differentiated Services (since all packets are ICMP they use the same Type of Service class)
    - Source IP(sending from same place)
    - Destination IP(contacting same site)
    - Upper layer protocol



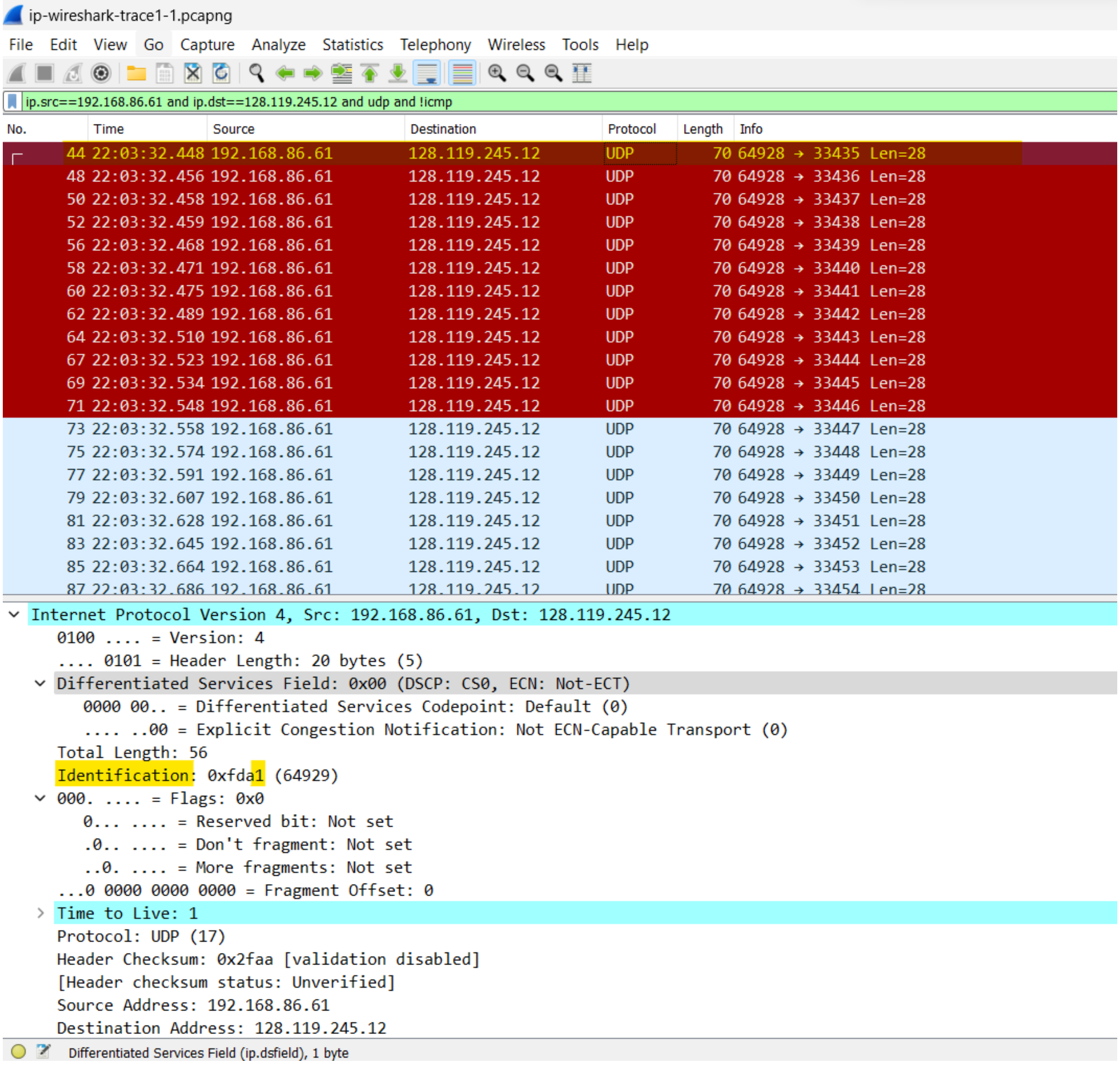
ip.src==192.168.86.61 and ip.dst==128.119.245.12 and udp and !icmp

No.	Time	Source	Destination	Protocol	Length	Info
44	22:03:32.448	192.168.86.61	128.119.245.12	UDP	70	64928 → 33435 Len=28
48	22:03:32.456	192.168.86.61	128.119.245.12	UDP	70	64928 → 33436 Len=28
50	22:03:32.458	192.168.86.61	128.119.245.12	UDP	70	64928 → 33437 Len=28
52	22:03:32.459	192.168.86.61	128.119.245.12	UDP	70	64928 → 33438 Len=28
56	22:03:32.468	192.168.86.61	128.119.245.12	UDP	70	64928 → 33439 Len=28
58	22:03:32.471	192.168.86.61	128.119.245.12	UDP	70	64928 → 33440 Len=28
60	22:03:32.475	192.168.86.61	128.119.245.12	UDP	70	64928 → 33441 Len=28
62	22:03:32.489	192.168.86.61	128.119.245.12	UDP	70	64928 → 33442 Len=28
64	22:03:32.510	192.168.86.61	128.119.245.12	UDP	70	64928 → 33443 Len=28
67	22:03:32.523	192.168.86.61	128.119.245.12	UDP	70	64928 → 33444 Len=28
69	22:03:32.534	192.168.86.61	128.119.245.12	UDP	70	64928 → 33445 Len=28
71	22:03:32.548	192.168.86.61	128.119.245.12	UDP	70	64928 → 33446 Len=28
73	22:03:32.558	192.168.86.61	128.119.245.12	UDP	70	64928 → 33447 Len=28
75	22:03:32.574	192.168.86.61	128.119.245.12	UDP	70	64928 → 33448 Len=28
77	22:03:32.591	192.168.86.61	128.119.245.12	UDP	70	64928 → 33449 Len=28
79	22:03:32.607	192.168.86.61	128.119.245.12	UDP	70	64928 → 33450 Len=28
81	22:03:32.628	192.168.86.61	128.119.245.12	UDP	70	64928 → 33451 Len=28
83	22:03:32.645	192.168.86.61	128.119.245.12	UDP	70	64928 → 33452 Len=28
85	22:03:32.664	192.168.86.61	128.119.245.12	UDP	70	64928 → 33453 Len=28
87	22:03:32.686	192.168.86.61	128.119.245.12	UDP	70	64928 → 33454 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)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 56
    Identification: 0xfdae (64942)
  000. .... = Flags: 0x0
        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: 5
    Protocol: UDP (17)
    Header Checksum: 0x2b9d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.86.61
    Destination Address: 128.119.245.12
```

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

    The pattern in the identification field is that the field increases by one in each strand of echo requests.

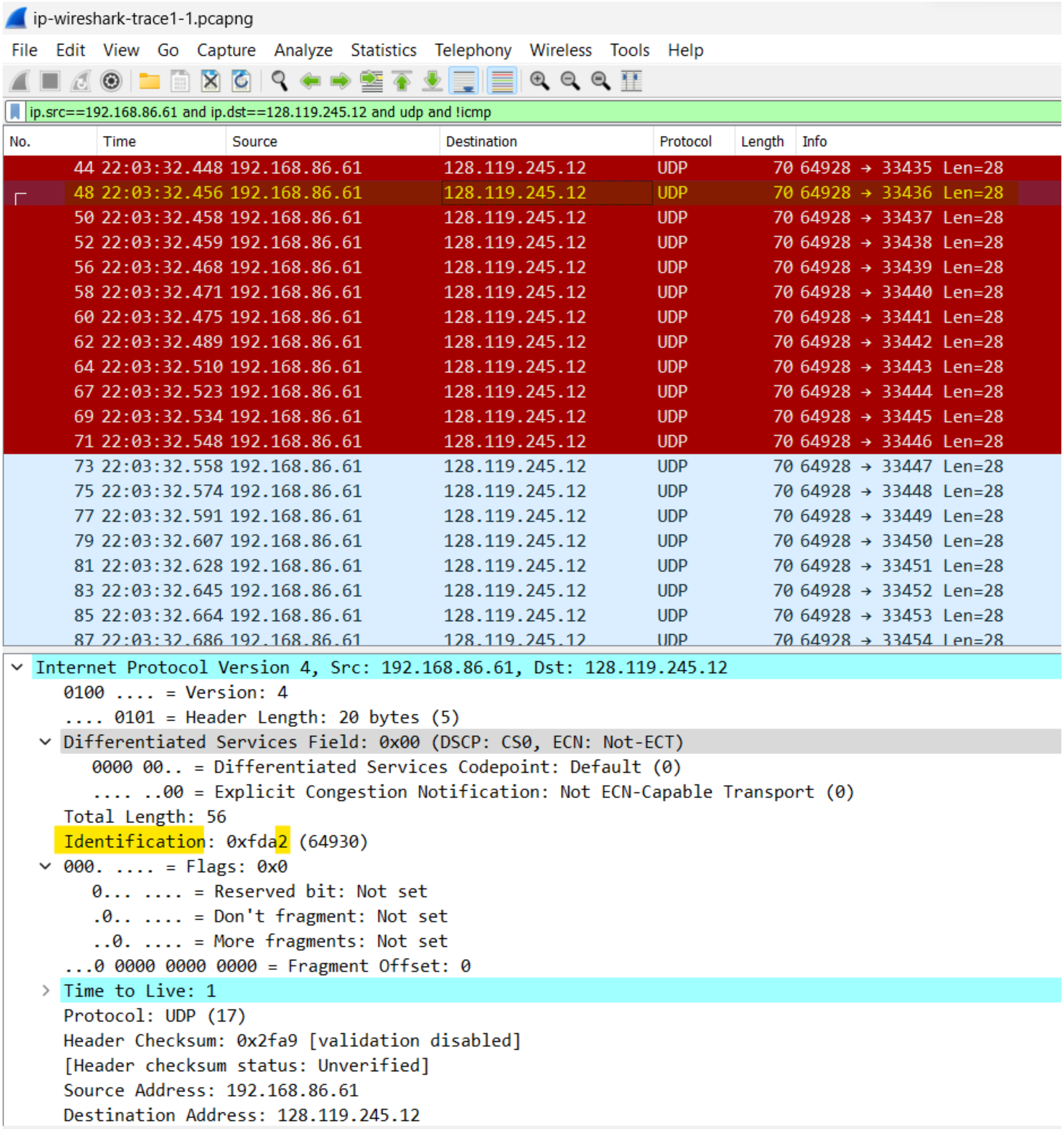


ip-wireshark-trace1-1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
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 22:03:32.448 192.168.86.61   128.119.245.12   UDP          70 64928 → 33435 Len=28
   48 22:03:32.456 192.168.86.61   128.119.245.12   UDP          70 64928 → 33436 Len=28
   50 22:03:32.458 192.168.86.61   128.119.245.12   UDP          70 64928 → 33437 Len=28
   52 22:03:32.459 192.168.86.61   128.119.245.12   UDP          70 64928 → 33438 Len=28
   56 22:03:32.468 192.168.86.61   128.119.245.12   UDP          70 64928 → 33439 Len=28
   58 22:03:32.471 192.168.86.61   128.119.245.12   UDP          70 64928 → 33440 Len=28
   60 22:03:32.475 192.168.86.61   128.119.245.12   UDP          70 64928 → 33441 Len=28
   62 22:03:32.489 192.168.86.61   128.119.245.12   UDP          70 64928 → 33442 Len=28
   64 22:03:32.510 192.168.86.61   128.119.245.12   UDP          70 64928 → 33443 Len=28
   67 22:03:32.523 192.168.86.61   128.119.245.12   UDP          70 64928 → 33444 Len=28
   69 22:03:32.534 192.168.86.61   128.119.245.12   UDP          70 64928 → 33445 Len=28
   71 22:03:32.548 192.168.86.61   128.119.245.12   UDP          70 64928 → 33446 Len=28
   73 22:03:32.558 192.168.86.61   128.119.245.12   UDP          70 64928 → 33447 Len=28
   75 22:03:32.574 192.168.86.61   128.119.245.12   UDP          70 64928 → 33448 Len=28
   77 22:03:32.591 192.168.86.61   128.119.245.12   UDP          70 64928 → 33449 Len=28
   79 22:03:32.607 192.168.86.61   128.119.245.12   UDP          70 64928 → 33450 Len=28
   81 22:03:32.628 192.168.86.61   128.119.245.12   UDP          70 64928 → 33451 Len=28
   83 22:03:32.645 192.168.86.61   128.119.245.12   UDP          70 64928 → 33452 Len=28
   85 22:03:32.664 192.168.86.61   128.119.245.12   UDP          70 64928 → 33453 Len=28
   87 22:03:32.686 192.168.86.61   128.119.245.12   UDP          70 64928 → 33454 Len=28
```

```
v Internet Protocol Version 4, Src: 192.168.86.61, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 56
    Identification: 0xfda1 (64929)
  v 000. .... = Flags: 0x0
      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: 1
    Protocol: UDP (17)
    Header Checksum: 0x2faa [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.86.61
    Destination Address: 128.119.245.12
```


ip-wireshark-trace1-1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

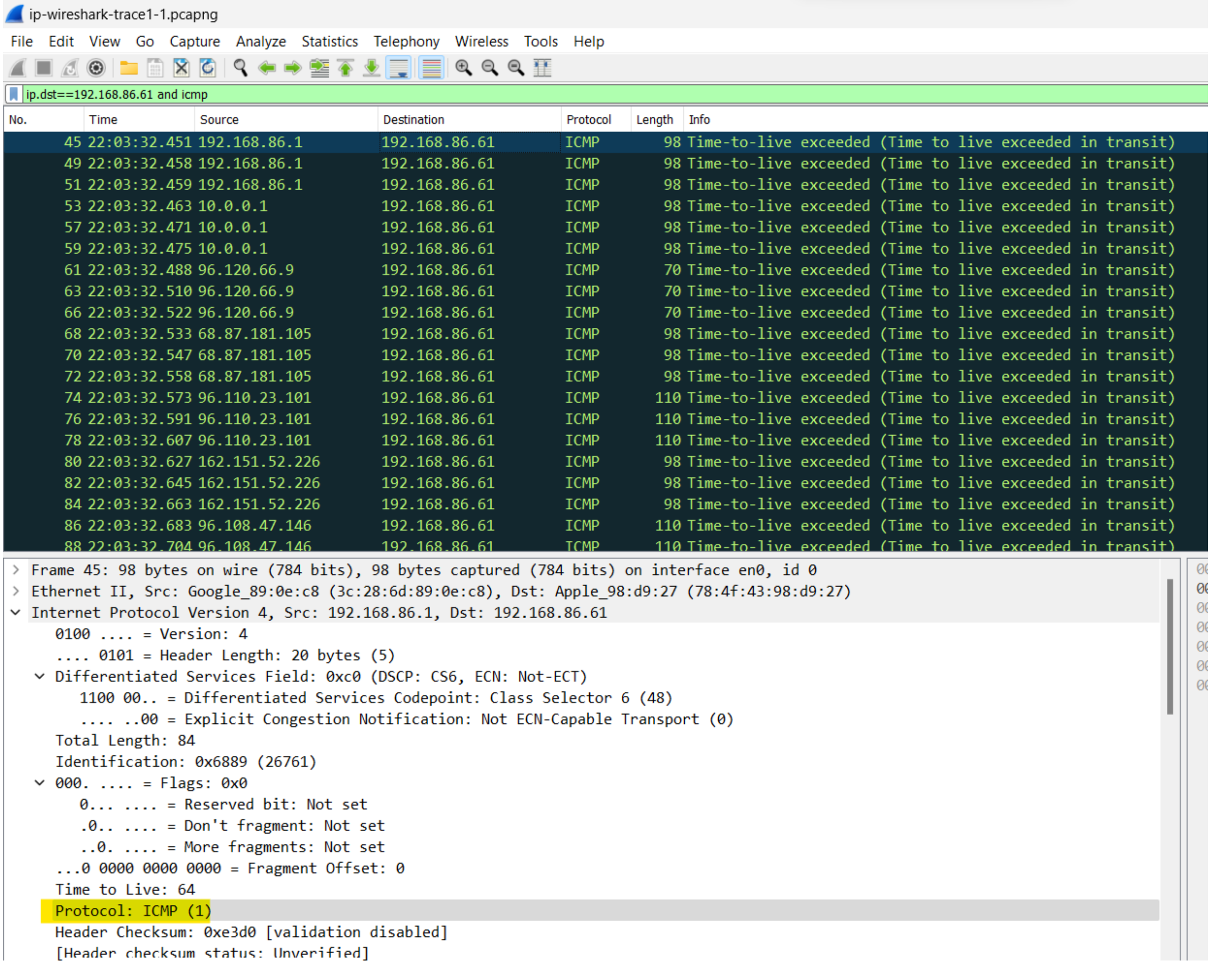
```
ip.src==192.168.86.61 and ip.dst==128.119.245.12 and udp and !icmp
```

```
No.  Time            Source          Destination     Protocol  Length  Info
  44 22:03:32.448    192.168.86.61   128.119.245.12  UDP           70  64928 → 33435 Len=28
  48 22:03:32.456    192.168.86.61   128.119.245.12  UDP           70  64928 → 33436 Len=28
  50 22:03:32.458    192.168.86.61   128.119.245.12  UDP           70  64928 → 33437 Len=28
  52 22:03:32.459    192.168.86.61   128.119.245.12  UDP           70  64928 → 33438 Len=28
  56 22:03:32.468    192.168.86.61   128.119.245.12  UDP           70  64928 → 33439 Len=28
  58 22:03:32.471    192.168.86.61   128.119.245.12  UDP           70  64928 → 33440 Len=28
  60 22:03:32.475    192.168.86.61   128.119.245.12  UDP           70  64928 → 33441 Len=28
  62 22:03:32.489    192.168.86.61   128.119.245.12  UDP           70  64928 → 33442 Len=28
  64 22:03:32.510    192.168.86.61   128.119.245.12  UDP           70  64928 → 33443 Len=28
  67 22:03:32.523    192.168.86.61   128.119.245.12  UDP           70  64928 → 33444 Len=28
  69 22:03:32.534    192.168.86.61   128.119.245.12  UDP           70  64928 → 33445 Len=28
  71 22:03:32.548    192.168.86.61   128.119.245.12  UDP           70  64928 → 33446 Len=28
  73 22:03:32.558    192.168.86.61   128.119.245.12  UDP           70  64928 → 33447 Len=28
  75 22:03:32.574    192.168.86.61   128.119.245.12  UDP           70  64928 → 33448 Len=28
  77 22:03:32.591    192.168.86.61   128.119.245.12  UDP           70  64928 → 33449 Len=28
  79 22:03:32.607    192.168.86.61   128.119.245.12  UDP           70  64928 → 33450 Len=28
  81 22:03:32.628    192.168.86.61   128.119.245.12  UDP           70  64928 → 33451 Len=28
  83 22:03:32.645    192.168.86.61   128.119.245.12  UDP           70  64928 → 33452 Len=28
  85 22:03:32.664    192.168.86.61   128.119.245.12  UDP           70  64928 → 33453 Len=28
  87 22:03:32.686    192.168.86.61   128.119.245.12  UDP           70  64928 → 33454 Len=28
```

```
v Internet Protocol Version 4, Src: 192.168.86.61, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 56
    Identification: 0xfda2 (64930)
  v 000. .... = Flags: 0x0
      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: 1
    Protocol: UDP (17)
    Header Checksum: 0x2fa9 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.86.61
    Destination Address: 128.119.245.12
```

10. What is the upper layer protocol specified in the IP datagrams returned from the routers?

Protocol: ICMP


ip-wireshark-trace1-1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst==192.168.86.61 and icmp

```
No.    Time             Source            Destination      Protocol  Length Info
    45 22:03:32.451 192.168.86.1       192.168.86.61    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
    49 22:03:32.458 192.168.86.1       192.168.86.61    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
    51 22:03:32.459 192.168.86.1       192.168.86.61    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
    53 22:03:32.463 10.0.0.1           192.168.86.61    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
    57 22:03:32.471 10.0.0.1           192.168.86.61    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
    59 22:03:32.475 10.0.0.1           192.168.86.61    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
    61 22:03:32.488 96.120.66.9        192.168.86.61    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
    63 22:03:32.510 96.120.66.9        192.168.86.61    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
    66 22:03:32.522 96.120.66.9        192.168.86.61    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
    68 22:03:32.533 68.87.181.105      192.168.86.61    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
    70 22:03:32.547 68.87.181.105      192.168.86.61    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
    72 22:03:32.558 68.87.181.105      192.168.86.61    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
    74 22:03:32.573 96.110.23.101      192.168.86.61    ICMP       110 Time-to-live exceeded (Time to live exceeded in transit)
    76 22:03:32.591 96.110.23.101      192.168.86.61    ICMP       110 Time-to-live exceeded (Time to live exceeded in transit)
    78 22:03:32.607 96.110.23.101      192.168.86.61    ICMP       110 Time-to-live exceeded (Time to live exceeded in transit)
    80 22:03:32.627 162.151.52.226     192.168.86.61    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
    82 22:03:32.645 162.151.52.226     192.168.86.61    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
    84 22:03:32.663 162.151.52.226     192.168.86.61    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
    86 22:03:32.683 96.108.47.146      192.168.86.61    ICMP       110 Time-to-live exceeded (Time to live exceeded in transit)
    88 22:03:32.704 96.108.47.146      192.168.86.61    ICMP       110 Time-to-live exceeded (Time to live exceeded in transit)
```

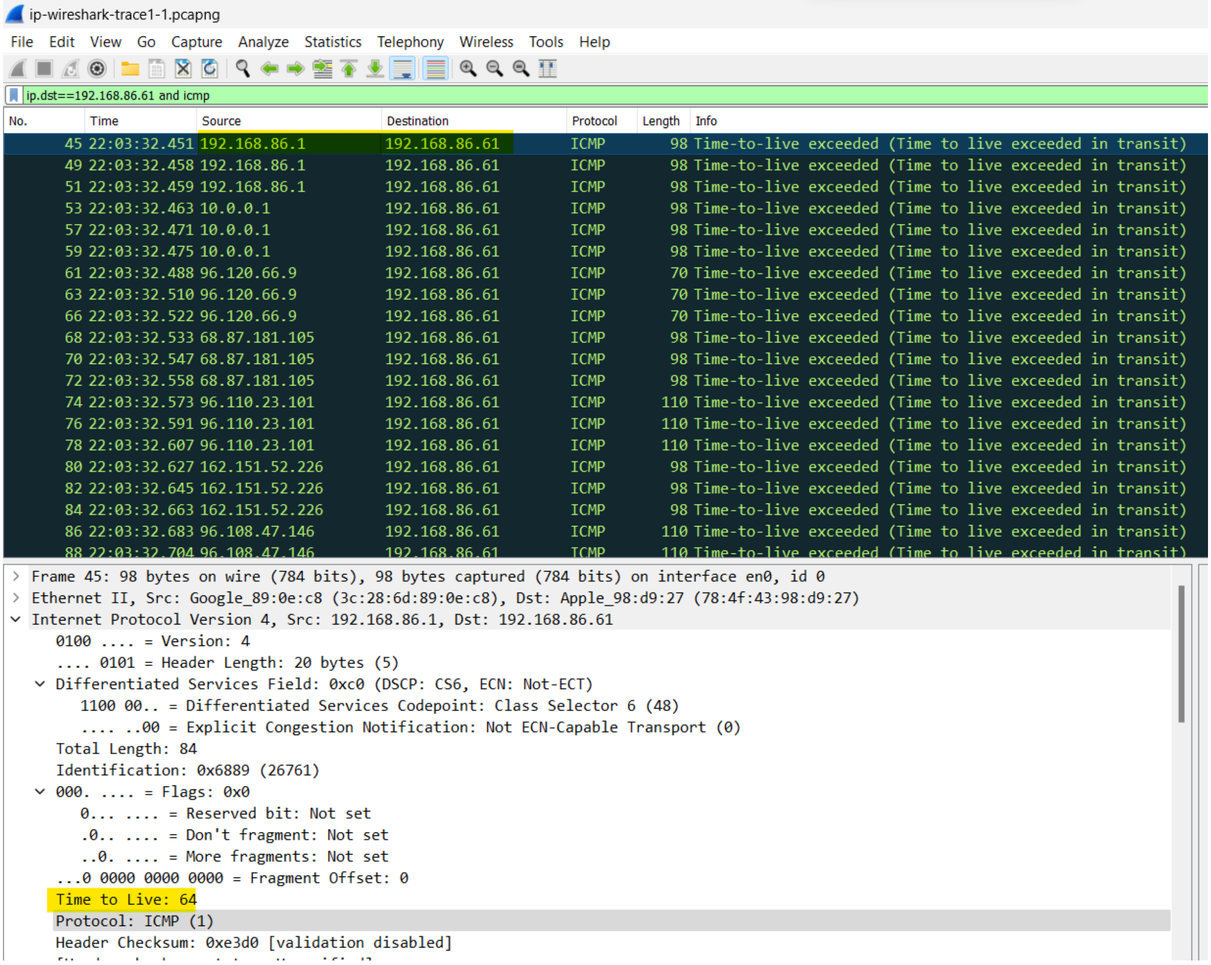
```
> Frame 45: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
> Ethernet II, Src: Google_89:0e:c8 (3c:28:6d:89:0e:c8), Dst: Apple_98:d9:27 (78:4f:43:98:d9:27)
v Internet Protocol Version 4, Src: 192.168.86.1, Dst: 192.168.86.61
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
      1100 00.. = Differentiated Services Codepoint: Class Selector 6 (48)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 84
    Identification: 0x6889 (26761)
  v 000. .... = Flags: 0x0
      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: 64
    Protocol: ICMP (1)
    Header Checksum: 0xe3d0 [validation disabled]
    [Header checksum status: Unverified]
```

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?

Yes

12. Are the values of the TTL fields similar, across all of ICMP packets from all of the routers?

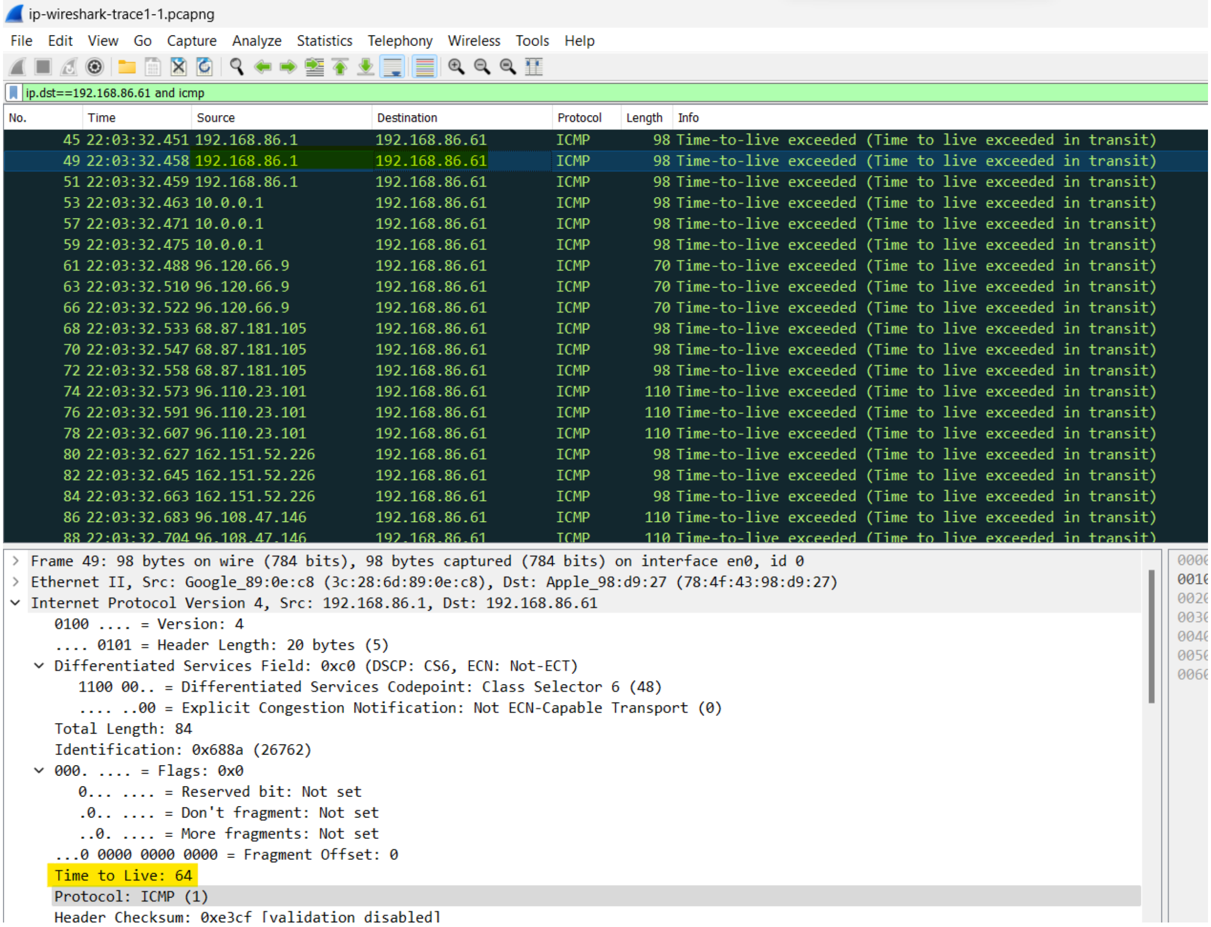
It is the same if the Source Address fields similar and vice versa.


ip-wireshark-trace1-1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.dst==192.168.86.61 and icmp
```

```
No.  Time            Source           Destination      Protocol  Length Info
  45 22:03:32.451 192.168.86.1     192.168.86.61    ICMP       98 Time-to-live exceeded (Time to live exceeded in transit)
  49 22:03:32.458 192.168.86.1     192.168.86.61    ICMP       98 Time-to-live exceeded (Time to live exceeded in transit)
  51 22:03:32.459 192.168.86.1     192.168.86.61    ICMP       98 Time-to-live exceeded (Time to live exceeded in transit)
  53 22:03:32.463 10.0.0.1         192.168.86.61    ICMP       98 Time-to-live exceeded (Time to live exceeded in transit)
  57 22:03:32.471 10.0.0.1         192.168.86.61    ICMP       98 Time-to-live exceeded (Time to live exceeded in transit)
  59 22:03:32.475 10.0.0.1         192.168.86.61    ICMP       98 Time-to-live exceeded (Time to live exceeded in transit)
  61 22:03:32.488 96.120.66.9      192.168.86.61    ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  63 22:03:32.510 96.120.66.9      192.168.86.61    ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  66 22:03:32.522 96.120.66.9      192.168.86.61    ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  68 22:03:32.533 68.87.181.105    192.168.86.61    ICMP       98 Time-to-live exceeded (Time to live exceeded in transit)
  70 22:03:32.547 68.87.181.105    192.168.86.61    ICMP       98 Time-to-live exceeded (Time to live exceeded in transit)
  72 22:03:32.558 68.87.181.105    192.168.86.61    ICMP       98 Time-to-live exceeded (Time to live exceeded in transit)
  74 22:03:32.573 96.110.23.101    192.168.86.61    ICMP      110 Time-to-live exceeded (Time to live exceeded in transit)
  76 22:03:32.591 96.110.23.101    192.168.86.61    ICMP      110 Time-to-live exceeded (Time to live exceeded in transit)
  78 22:03:32.607 96.110.23.101    192.168.86.61    ICMP      110 Time-to-live exceeded (Time to live exceeded in transit)
  80 22:03:32.627 162.151.52.226   192.168.86.61    ICMP       98 Time-to-live exceeded (Time to live exceeded in transit)
  82 22:03:32.645 162.151.52.226   192.168.86.61    ICMP       98 Time-to-live exceeded (Time to live exceeded in transit)
  84 22:03:32.663 162.151.52.226   192.168.86.61    ICMP       98 Time-to-live exceeded (Time to live exceeded in transit)
  86 22:03:32.683 96.108.47.146    192.168.86.61    ICMP      110 Time-to-live exceeded (Time to live exceeded in transit)
  88 22:03:32.704 96.108.47.146    192.168.86.61    ICMP      110 Time-to-live exceeded (Time to live exceeded in transit)
```

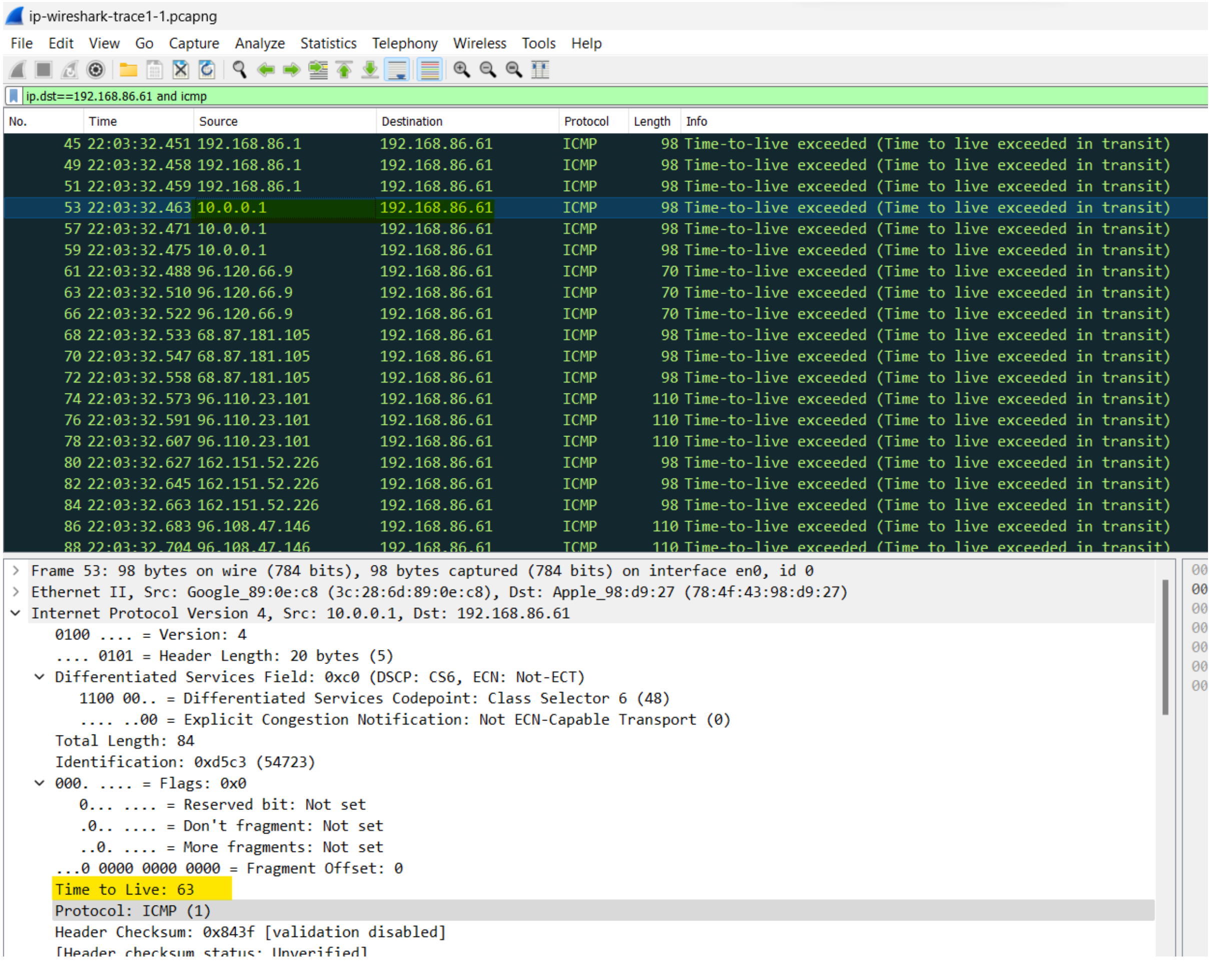
```
> Frame 45: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
> Ethernet II, Src: Google_89:0e:c8 (3c:28:6d:89:0e:c8), Dst: Apple_98:d9:27 (78:4f:43:98:d9:27)
v Internet Protocol Version 4, Src: 192.168.86.1, Dst: 192.168.86.61
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
      1100 00.. = Differentiated Services Codepoint: Class Selector 6 (48)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 84
    Identification: 0x6889 (26761)
  v 000. .... = Flags: 0x0
      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: 64
    Protocol: ICMP (1)
    Header Checksum: 0xe3d0 [validation disabled]
```


ip-wireshark-trace1-1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
0000
0010
0020
0030
0040
0050
0060

ip.dst==192.168.86.61 and icmp

```
No.   Time            Source          Destination     Protocol  Length Info
   45 22:03:32.451 192.168.86.1    192.168.86.61    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
   49 22:03:32.458 192.168.86.1    192.168.86.61    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
   51 22:03:32.459 192.168.86.1    192.168.86.61    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
   53 22:03:32.463 10.0.0.1        192.168.86.61    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
   57 22:03:32.471 10.0.0.1        192.168.86.61    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
   59 22:03:32.475 10.0.0.1        192.168.86.61    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
   61 22:03:32.488 96.120.66.9     192.168.86.61    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
   63 22:03:32.510 96.120.66.9     192.168.86.61    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
   66 22:03:32.522 96.120.66.9     192.168.86.61    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
   68 22:03:32.533 68.87.181.105   192.168.86.61    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
   70 22:03:32.547 68.87.181.105   192.168.86.61    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
   72 22:03:32.558 68.87.181.105   192.168.86.61    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
   74 22:03:32.573 96.110.23.101   192.168.86.61    ICMP       110 Time-to-live exceeded (Time to live exceeded in transit)
   76 22:03:32.591 96.110.23.101   192.168.86.61    ICMP       110 Time-to-live exceeded (Time to live exceeded in transit)
   78 22:03:32.607 96.110.23.101   192.168.86.61    ICMP       110 Time-to-live exceeded (Time to live exceeded in transit)
   80 22:03:32.627 162.151.52.226  192.168.86.61    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
   82 22:03:32.645 162.151.52.226  192.168.86.61    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
   84 22:03:32.663 162.151.52.226  192.168.86.61    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
   86 22:03:32.683 96.108.47.146   192.168.86.61    ICMP       110 Time-to-live exceeded (Time to live exceeded in transit)
   88 22:03:32.704 96.108.47.146   192.168.86.61    ICMP       110 Time-to-live exceeded (Time to live exceeded in transit)
```

```
> Frame 49: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
> Ethernet II, Src: Google_89:0e:c8 (3c:28:6d:89:0e:c8), Dst: Apple_98:d9:27 (78:4f:43:98:d9:27)
v Internet Protocol Version 4, Src: 192.168.86.1, Dst: 192.168.86.61
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
      1100 00.. = Differentiated Services Codepoint: Class Selector 6 (48)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 84
    Identification: 0x688a (26762)
  v 000. .... = Flags: 0x0
      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: 64
    Protocol: ICMP (1)
    Header Checksum: 0xe3cf [validation disabled]
```



ip.dst==192.168.86.61 and icmp

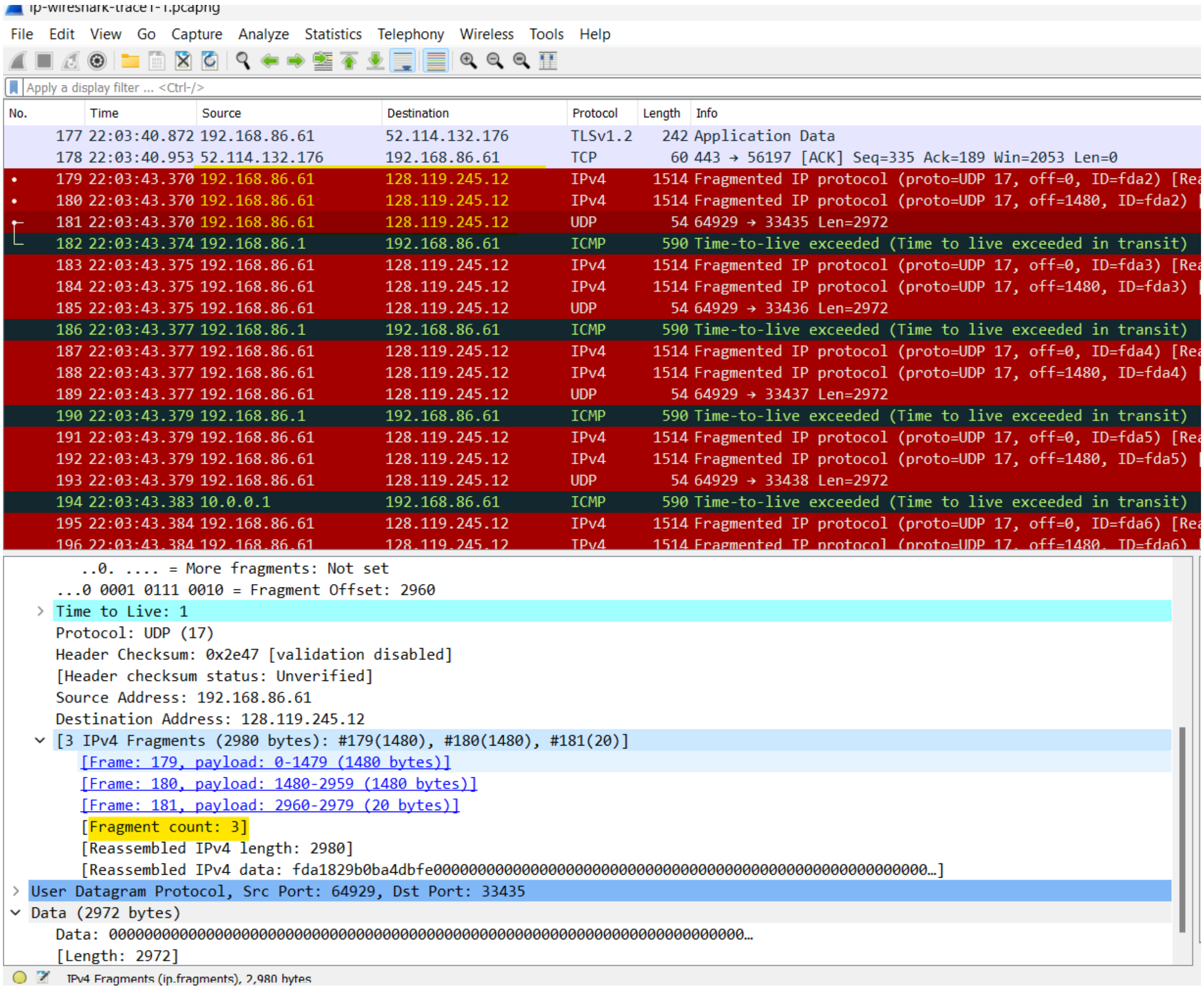
```
No.   Time         Source           Destination     Protocol  Length  Info
   45 22:03:32.451 192.168.86.1     192.168.86.61   ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
   49 22:03:32.458 192.168.86.1     192.168.86.61   ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
   51 22:03:32.459 192.168.86.1     192.168.86.61   ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
   53 22:03:32.463 10.0.0.1         192.168.86.61   ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
   57 22:03:32.471 10.0.0.1         192.168.86.61   ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
   59 22:03:32.475 10.0.0.1         192.168.86.61   ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
   61 22:03:32.488 96.120.66.9      192.168.86.61   ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
   63 22:03:32.510 96.120.66.9      192.168.86.61   ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
   66 22:03:32.522 96.120.66.9      192.168.86.61   ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
   68 22:03:32.533 68.87.181.105    192.168.86.61   ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
   70 22:03:32.547 68.87.181.105    192.168.86.61   ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
   72 22:03:32.558 68.87.181.105    192.168.86.61   ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
   74 22:03:32.573 96.110.23.101    192.168.86.61   ICMP       110 Time-to-live exceeded (Time to live exceeded in transit)
   76 22:03:32.591 96.110.23.101    192.168.86.61   ICMP       110 Time-to-live exceeded (Time to live exceeded in transit)
   78 22:03:32.607 96.110.23.101    192.168.86.61   ICMP       110 Time-to-live exceeded (Time to live exceeded in transit)
   80 22:03:32.627 162.151.52.226   192.168.86.61   ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
   82 22:03:32.645 162.151.52.226   192.168.86.61   ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
   84 22:03:32.663 162.151.52.226   192.168.86.61   ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
   86 22:03:32.683 96.108.47.146    192.168.86.61   ICMP       110 Time-to-live exceeded (Time to live exceeded in transit)
   88 22:03:32.704 96.108.47.146    192.168.86.61   ICMP       110 Time-to-live exceeded (Time to live exceeded in transit)
```

```
> Frame 53: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
> Ethernet II, Src: Google_89:0e:c8 (3c:28:6d:89:0e:c8), Dst: Apple_98:d9:27 (78:4f:43:98:d9:27)
v Internet Protocol Version 4, Src: 10.0.0.1, Dst: 192.168.86.61
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
      1100 00.. = Differentiated Services Codepoint: Class Selector 6 (48)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 84
    Identification: 0xd5c3 (54723)
  v 000. .... = Flags: 0x0
      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: 63
    Protocol: ICMP (1)
    Header Checksum: 0x843f [validation disabled]
    [Header checksum status: Unverified]
```

Part 2: Fragmentation

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[1]!)**

Yes, it had 3 fragments.

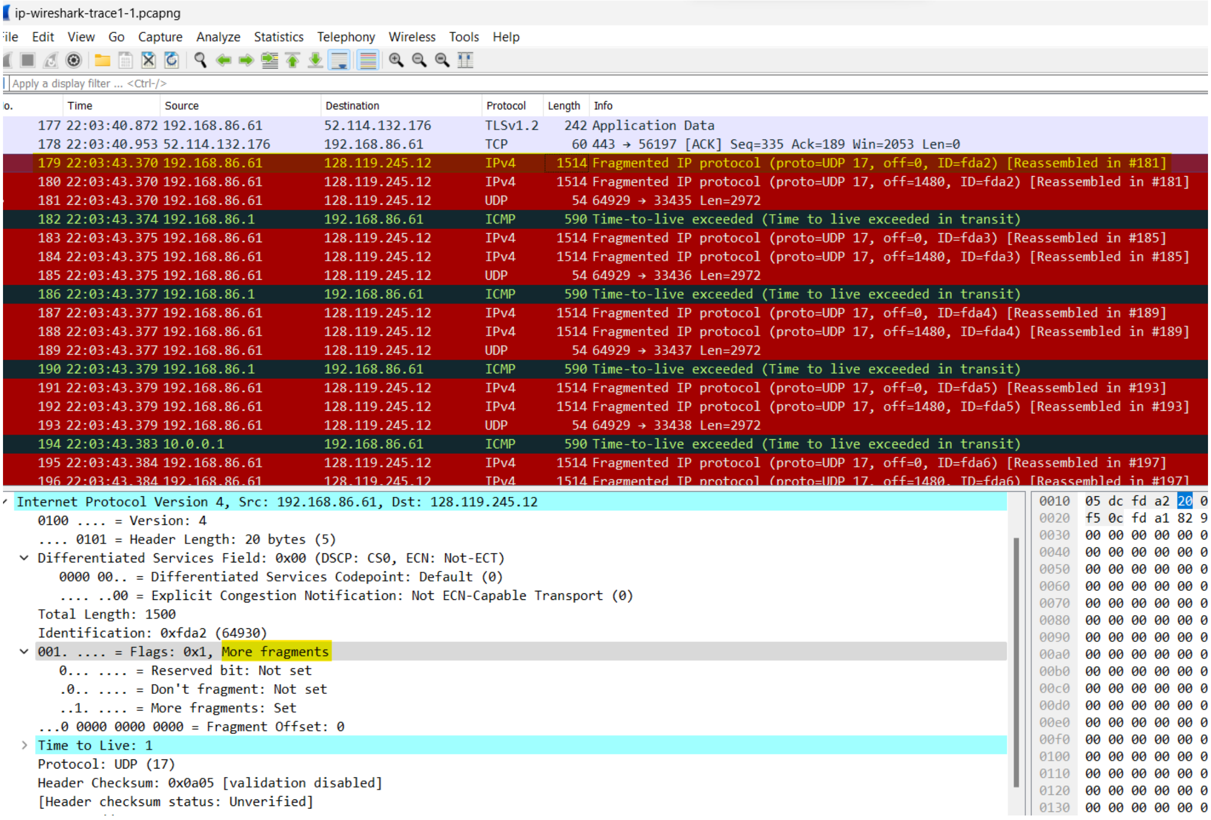

ip-wireshark-trace1-1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time         Source          Destination     Protocol Length Info
  177 22:03:40.872 192.168.86.61   52.114.132.176  TLSv1.2   242 Application Data
  178 22:03:40.953 52.114.132.176  192.168.86.61   TCP        60 443 → 56197 [ACK] Seq=335 Ack=189 Win=2053 Len=0
  179 22:03:43.370 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda2) [Rea
  180 22:03:43.370 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda2)
  181 22:03:43.370 192.168.86.61   128.119.245.12  UDP        54 64929 → 33435 Len=2972
  182 22:03:43.374 192.168.86.1    192.168.86.61   ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
  183 22:03:43.375 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda3) [Rea
  184 22:03:43.375 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda3)
  185 22:03:43.375 192.168.86.61   128.119.245.12  UDP        54 64929 → 33436 Len=2972
  186 22:03:43.377 192.168.86.1    192.168.86.61   ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
  187 22:03:43.377 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda4) [Rea
  188 22:03:43.377 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda4)
  189 22:03:43.377 192.168.86.61   128.119.245.12  UDP        54 64929 → 33437 Len=2972
  190 22:03:43.379 192.168.86.1    192.168.86.61   ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
  191 22:03:43.379 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda5) [Rea
  192 22:03:43.379 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda5)
  193 22:03:43.379 192.168.86.61   128.119.245.12  UDP        54 64929 → 33438 Len=2972
  194 22:03:43.383 10.0.0.1        192.168.86.61   ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
  195 22:03:43.384 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda6) [Rea
  196 22:03:43.384 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda6)
```

```
      ..0. .... = More fragments: Not set
    ...0 0001 0111 0010 = Fragment Offset: 2960
  > Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0x2e47 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.86.61
    Destination Address: 128.119.245.12
  v [3 IPv4 Fragments (2980 bytes): #179(1480), #180(1480), #181(20)]
      [Frame: 179, payload: 0-1479 (1480 bytes)]
      [Frame: 180, payload: 1480-2959 (1480 bytes)]
      [Frame: 181, payload: 2960-2979 (20 bytes)]
      [Fragment count: 3]
      [Reassembled IPv4 length: 2980]
      [Reassembled IPv4 data: fda1829b0ba4dbfe000000000000000000000000000000000000000000000000000…]
> User Datagram Protocol, Src Port: 64929, Dst Port: 33435
v Data (2972 bytes)
    Data: 000000000000000000000000000000000000000000000000000000000000000000000000…
    [Length: 2972]
```

14. What information in the IP header indicates that this datagram been fragmented?

In the IP header of the first fragment the more fragment flag was set. It indicates that it has another fragment.


ip-wireshark-trace1-1.pcapng
ile Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

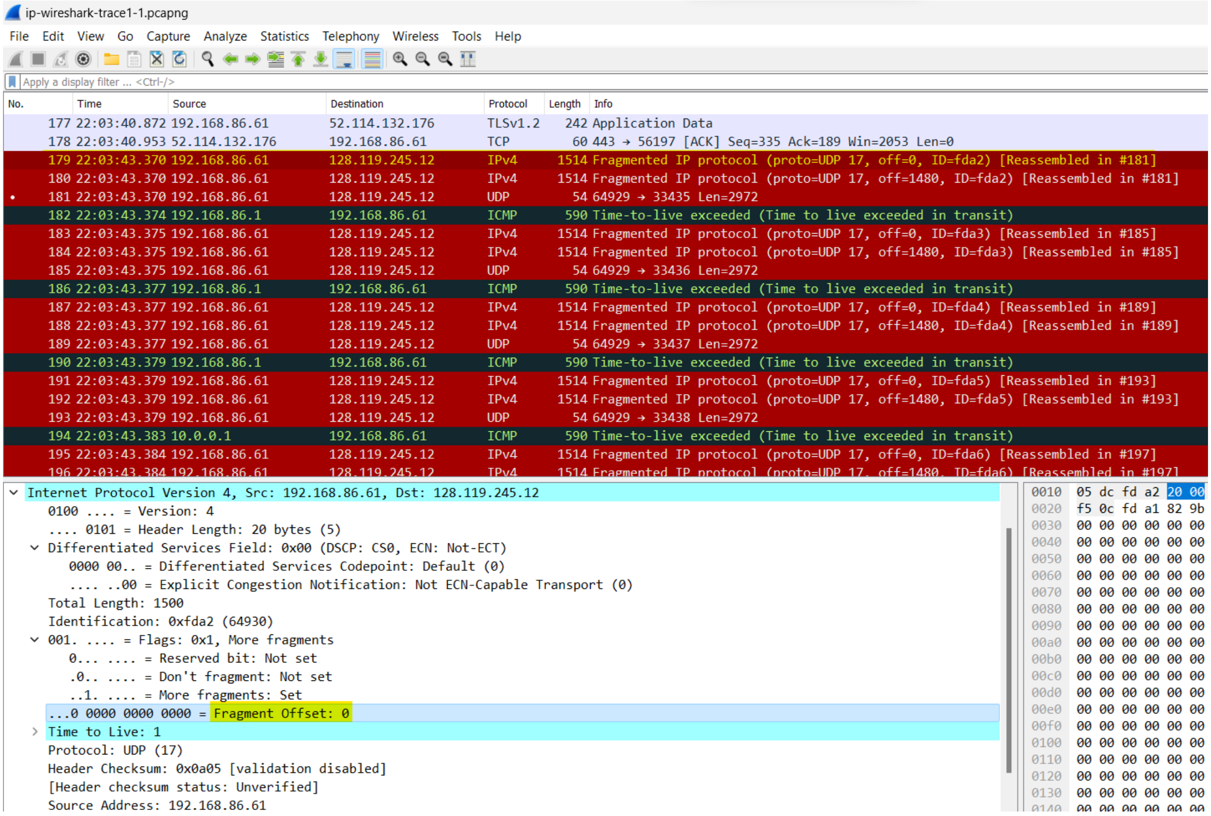
```
o.   Time         Source          Destination     Protocol Length Info
 177 22:03:40.872 192.168.86.61   52.114.132.176  TLSv1.2    242 Application Data
 178 22:03:40.953 52.114.132.176  192.168.86.61   TCP         60 443 → 56197 [ACK] Seq=335 Ack=189 Win=2053 Len=0
 179 22:03:43.370 192.168.86.61   128.119.245.12  IPv4      1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda2) [Reassembled in #181]
 180 22:03:43.370 192.168.86.61   128.119.245.12  IPv4      1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda2) [Reassembled in #181]
 181 22:03:43.370 192.168.86.61   128.119.245.12  UDP         54 64929 → 33435 Len=2972
 182 22:03:43.374 192.168.86.1    192.168.86.61   ICMP       590 Time-to-live exceeded (Time to live exceeded in transit)
 183 22:03:43.375 192.168.86.61   128.119.245.12  IPv4      1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda3) [Reassembled in #185]
 184 22:03:43.375 192.168.86.61   128.119.245.12  IPv4      1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda3) [Reassembled in #185]
 185 22:03:43.375 192.168.86.61   128.119.245.12  UDP         54 64929 → 33436 Len=2972
 186 22:03:43.377 192.168.86.1    192.168.86.61   ICMP       590 Time-to-live exceeded (Time to live exceeded in transit)
 187 22:03:43.377 192.168.86.61   128.119.245.12  IPv4      1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda4) [Reassembled in #189]
 188 22:03:43.377 192.168.86.61   128.119.245.12  IPv4      1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda4) [Reassembled in #189]
 189 22:03:43.377 192.168.86.61   128.119.245.12  UDP         54 64929 → 33437 Len=2972
 190 22:03:43.379 192.168.86.1    192.168.86.61   ICMP       590 Time-to-live exceeded (Time to live exceeded in transit)
 191 22:03:43.379 192.168.86.61   128.119.245.12  IPv4      1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda5) [Reassembled in #193]
 192 22:03:43.379 192.168.86.61   128.119.245.12  IPv4      1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda5) [Reassembled in #193]
 193 22:03:43.379 192.168.86.61   128.119.245.12  UDP         54 64929 → 33438 Len=2972
 194 22:03:43.383 10.0.0.1        192.168.86.61   ICMP       590 Time-to-live exceeded (Time to live exceeded in transit)
 195 22:03:43.384 192.168.86.61   128.119.245.12  IPv4      1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda6) [Reassembled in #197]
 196 22:03:43.384 192.168.86.61   128.119.245.12  IPv4      1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda6) [Reassembled in #197]
```

```
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)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
   Total Length: 1500
   Identification: 0xfda2 (64930)
 ⌄ 001. .... = Flags: 0x1, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
   ...0 0000 0000 0000 = Fragment Offset: 0
 › Time to Live: 1
   Protocol: UDP (17)
   Header Checksum: 0x0a05 [validation disabled]
   [Header checksum status: Unverified]
```

```
0010  05 dc fd a2 20 0
0020  f5 0c fd a1 82 9
0030  00 00 00 00 00 0
0040  00 00 00 00 00 0
0050  00 00 00 00 00 0
0060  00 00 00 00 00 0
0070  00 00 00 00 00 0
0080  00 00 00 00 00 0
0090  00 00 00 00 00 0
00a0  00 00 00 00 00 0
00b0  00 00 00 00 00 0
00c0  00 00 00 00 00 0
00d0  00 00 00 00 00 0
00e0  00 00 00 00 00 0
00f0  00 00 00 00 00 0
0100  00 00 00 00 00 0
0110  00 00 00 00 00 0
0120  00 00 00 00 00 0
0130  00 00 00 00 00 0
```

15. What information in the IP header for this packet indicates whether this is the first fragment versus a latter fragment?

Since the fragment offset is 0 => It is the first fragment.



ip-wireshark-trace1-1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

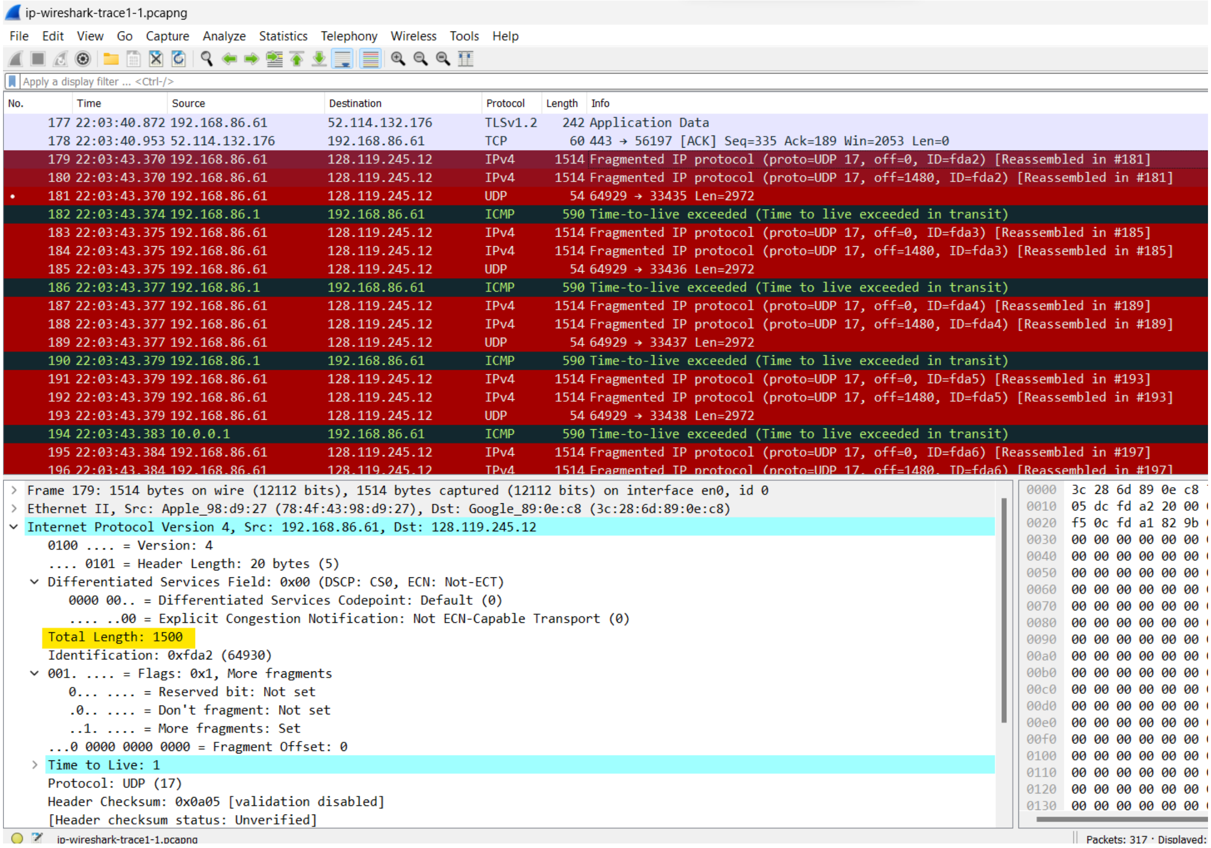
```
No.   Time         Source          Destination     Protocol Length Info
  177 22:03:40.872 192.168.86.61   52.114.132.176  TLSv1.2   242 Application Data
  178 22:03:40.953 52.114.132.176  192.168.86.61   TCP        60 443 → 56197 [ACK] Seq=335 Ack=189 Win=2053 Len=0
  179 22:03:43.370 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda2) [Reassembled in #181]
  180 22:03:43.370 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda2) [Reassembled in #181]
•  181 22:03:43.370 192.168.86.61   128.119.245.12  UDP        54 64929 → 33435 Len=2972
  182 22:03:43.374 192.168.86.1    192.168.86.61   ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
  183 22:03:43.375 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda3) [Reassembled in #185]
  184 22:03:43.375 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda3) [Reassembled in #185]
  185 22:03:43.375 192.168.86.61   128.119.245.12  UDP        54 64929 → 33436 Len=2972
  186 22:03:43.377 192.168.86.1    192.168.86.61   ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
  187 22:03:43.377 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda4) [Reassembled in #189]
  188 22:03:43.377 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda4) [Reassembled in #189]
  189 22:03:43.377 192.168.86.61   128.119.245.12  UDP        54 64929 → 33437 Len=2972
  190 22:03:43.379 192.168.86.1    192.168.86.61   ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
  191 22:03:43.379 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda5) [Reassembled in #193]
  192 22:03:43.379 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda5) [Reassembled in #193]
  193 22:03:43.379 192.168.86.61   128.119.245.12  UDP        54 64929 → 33438 Len=2972
  194 22:03:43.383 10.0.0.1        192.168.86.61   ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
  195 22:03:43.384 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda6) [Reassembled in #197]
  196 22:03:43.384 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda6) [Reassembled in #197]
```

```
v Internet Protocol Version 4, Src: 192.168.86.61, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 1500
    Identification: 0xfda2 (64930)
  v 001. .... = Flags: 0x1, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0x0a05 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.86.61
```

```
0010  05 dc fd a2 20 00
0020  f5 0c fd a1 82 9b
0030  00 00 00 00 00 00
0040  00 00 00 00 00 00
0050  00 00 00 00 00 00
0060  00 00 00 00 00 00
0070  00 00 00 00 00 00
0080  00 00 00 00 00 00
0090  00 00 00 00 00 00
00a0  00 00 00 00 00 00
00b0  00 00 00 00 00 00
00c0  00 00 00 00 00 00
00d0  00 00 00 00 00 00
00e0  00 00 00 00 00 00
00f0  00 00 00 00 00 00
0100  00 00 00 00 00 00
0110  00 00 00 00 00 00
0120  00 00 00 00 00 00
0130  00 00 00 00 00 00
0140  00 00 00 00 00 00
```

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

1500 bytes



ip-wireshark-trace1-1.pcapng

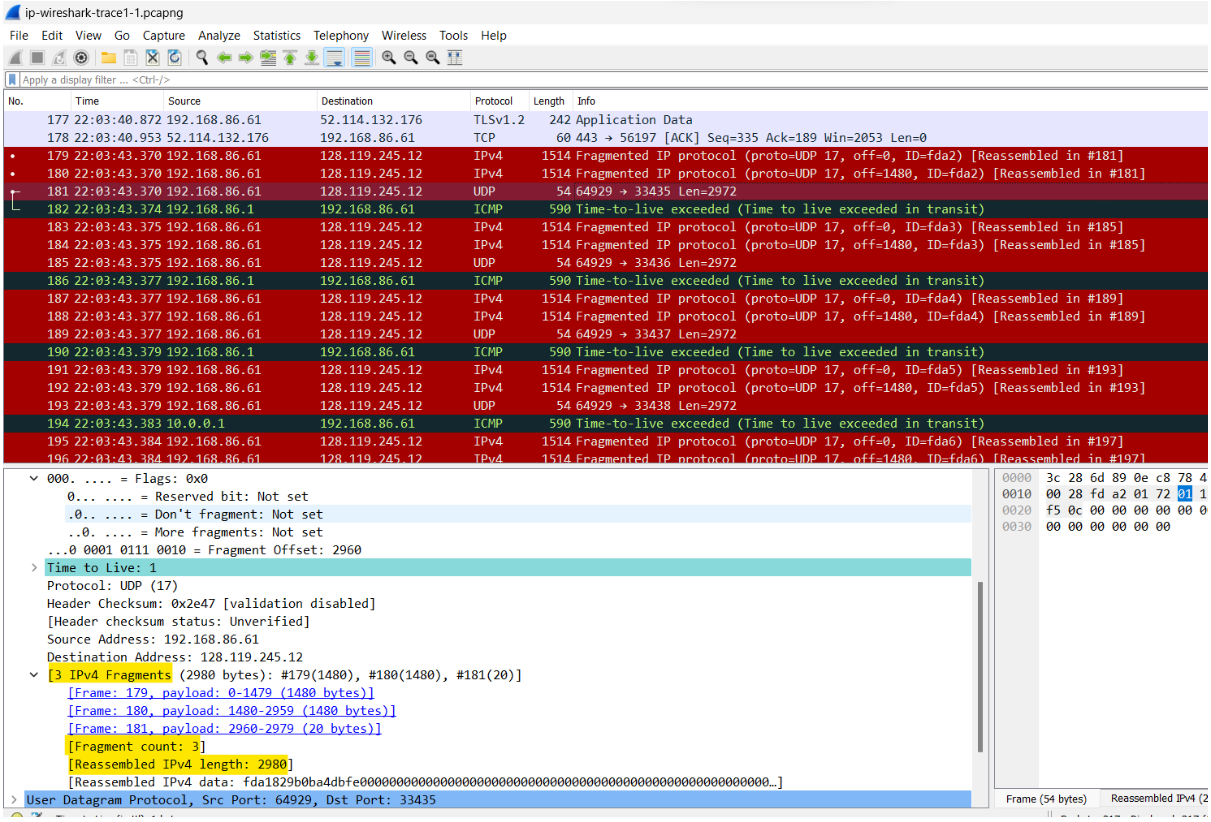
```
No.  Time         Source          Destination     Protocol Length Info
177 22:03:40.872 192.168.86.61   52.114.132.176  TLSv1.2   242 Application Data
178 22:03:40.953 52.114.132.176  192.168.86.61   TCP        60 443 → 56197 [ACK] Seq=335 Ack=189 Win=2053 Len=0
179 22:03:43.370 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda2) [Reassembled in #181]
180 22:03:43.370 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda2) [Reassembled in #181]
181 22:03:43.370 192.168.86.61   128.119.245.12  UDP        54 64929 → 33435 Len=2972
182 22:03:43.374 192.168.86.1    192.168.86.61   ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
183 22:03:43.375 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda3) [Reassembled in #185]
184 22:03:43.375 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda3) [Reassembled in #185]
185 22:03:43.375 192.168.86.61   128.119.245.12  UDP        54 64929 → 33436 Len=2972
186 22:03:43.377 192.168.86.1    192.168.86.61   ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
187 22:03:43.377 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda4) [Reassembled in #189]
188 22:03:43.377 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda4) [Reassembled in #189]
189 22:03:43.377 192.168.86.61   128.119.245.12  UDP        54 64929 → 33437 Len=2972
190 22:03:43.379 192.168.86.1    192.168.86.61   ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
191 22:03:43.379 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda5) [Reassembled in #193]
192 22:03:43.379 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda5) [Reassembled in #193]
193 22:03:43.379 192.168.86.61   128.119.245.12  UDP        54 64929 → 33438 Len=2972
194 22:03:43.383 10.0.0.1        192.168.86.61   ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
195 22:03:43.384 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda6) [Reassembled in #197]
196 22:03:43.384 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda6) [Reassembled in #197]
```

```
> Frame 179: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface en0, id 0
> Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Google_89:0e:c8 (3c:28:6d:89:0e:c8)
v Internet Protocol Version 4, Src: 192.168.86.61, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 1500
    Identification: 0xfda2 (64930)
  v 001. .... = Flags: 0x1, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0x0a05 [validation disabled]
    [Header checksum status: Unverified]
```

```
0000  3c 28 6d 89 0e c8
0010  05 dc fd a2 20 00
0020  f5 0c fd a1 82 9b
0030  00 00 00 00 00 00
0040  00 00 00 00 00 00
0050  00 00 00 00 00 00
0060  00 00 00 00 00 00
0070  00 00 00 00 00 00
0080  00 00 00 00 00 00
0090  00 00 00 00 00 00
00a0  00 00 00 00 00 00
00b0  00 00 00 00 00 00
00c0  00 00 00 00 00 00
00d0  00 00 00 00 00 00
00e0  00 00 00 00 00 00
00f0  00 00 00 00 00 00
0100  00 00 00 00 00 00
0110  00 00 00 00 00 00
0120  00 00 00 00 00 00
0130  00 00 00 00 00 00
```

ip-wireshark-trace1-1.pcapng

Packets: 317 · Displayed:



ip-wireshark-trace1-1.pcapng

```
No.  Time         Source          Destination     Protocol Length Info
177 22:03:40.872 192.168.86.61   52.114.132.176  TLSv1.2   242 Application Data
178 22:03:40.953 52.114.132.176  192.168.86.61   TCP        60 443 → 56197 [ACK] Seq=335 Ack=189 Win=2053 Len=0
179 22:03:43.370 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda2) [Reassembled in #181]
180 22:03:43.370 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda2) [Reassembled in #181]
181 22:03:43.370 192.168.86.61   128.119.245.12  UDP        54 64929 → 33435 Len=2972
182 22:03:43.374 192.168.86.1    192.168.86.61   ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
183 22:03:43.375 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda3) [Reassembled in #185]
184 22:03:43.375 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda3) [Reassembled in #185]
185 22:03:43.375 192.168.86.61   128.119.245.12  UDP        54 64929 → 33436 Len=2972
186 22:03:43.377 192.168.86.1    192.168.86.61   ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
187 22:03:43.377 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda4) [Reassembled in #189]
188 22:03:43.377 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda4) [Reassembled in #189]
189 22:03:43.377 192.168.86.61   128.119.245.12  UDP        54 64929 → 33437 Len=2972
190 22:03:43.379 192.168.86.1    192.168.86.61   ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
191 22:03:43.379 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda5) [Reassembled in #193]
192 22:03:43.379 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda5) [Reassembled in #193]
193 22:03:43.379 192.168.86.61   128.119.245.12  UDP        54 64929 → 33438 Len=2972
194 22:03:43.383 10.0.0.1        192.168.86.61   ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
195 22:03:43.384 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda6) [Reassembled in #197]
196 22:03:43.384 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda6) [Reassembled in #197]
```

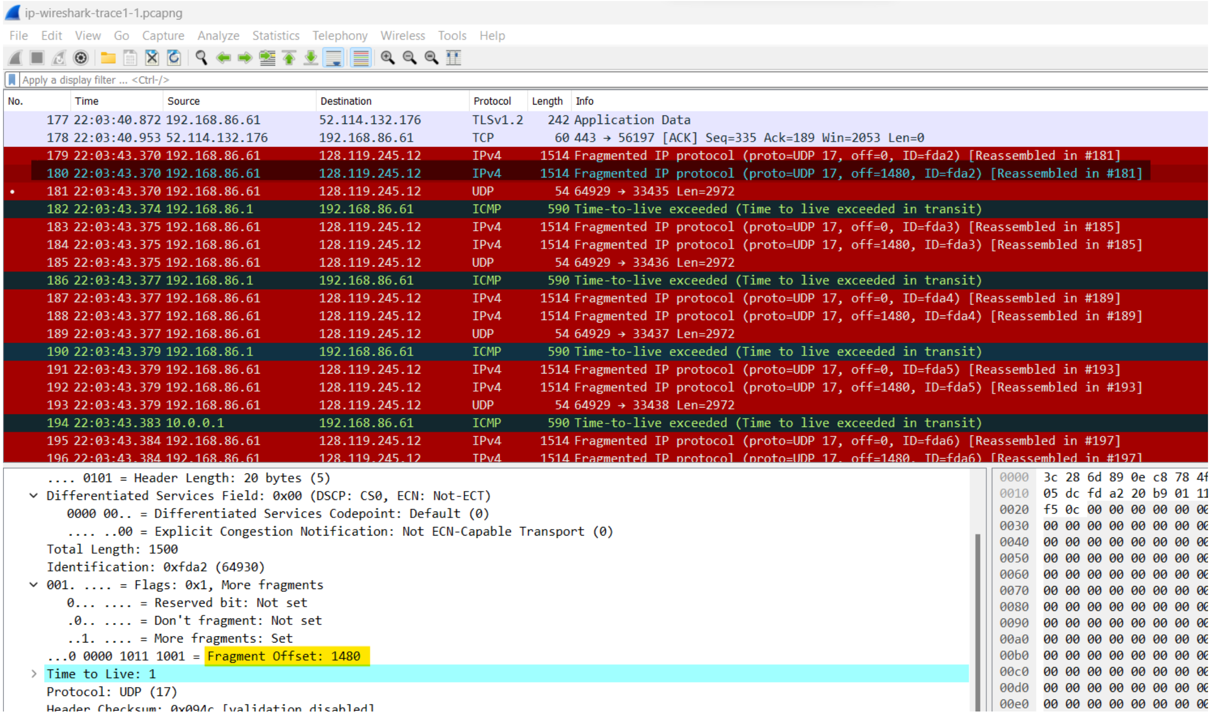
```
  v 000. .... = Flags: 0x0
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0001 0111 0010 = Fragment Offset: 2960
  > Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0x2e47 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.86.61
    Destination Address: 128.119.245.12
  v [3 IPv4 Fragments (2980 bytes): #179(1480), #180(1480), #181(20)]
      [Frame: 179, payload: 0-1479 (1480 bytes)]
      [Frame: 180, payload: 1480-2959 (1480 bytes)]
      [Frame: 181, payload: 2960-2979 (20 bytes)]
      [Fragment count: 3]
      [Reassembled IPv4 length: 2980]
      [Reassembled IPv4 data: fda1829b0ba4dbfe000000000000000000000000000000000000000000000000000000…]
> User Datagram Protocol, Src Port: 64929, Dst Port: 33435
```

```
0000  3c 28 6d 89 0e c8 78 4
0010  00 28 fd a2 01 72 01 1
0020  f5 0c 00 00 00 00 00 0
0030  00 00 00 00 00 00
```

Frame (54 bytes) Reassembled IPv4 (2

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.


ip-wireshark-trace1-1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.    Time         Source          Destination     Protocol Length Info
   177 22:03:40.872 192.168.86.61   52.114.132.176  TLSv1.2   242 Application Data
   178 22:03:40.953 52.114.132.176  192.168.86.61   TCP        60 443 → 56197 [ACK] Seq=335 Ack=189 Win=2053 Len=0
   179 22:03:43.370 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda2) [Reassembled in #181]
   180 22:03:43.370 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda2) [Reassembled in #181]
•  181 22:03:43.370 192.168.86.61   128.119.245.12  UDP        54 64929 → 33435 Len=2972
   182 22:03:43.374 192.168.86.1    192.168.86.61   ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
   183 22:03:43.375 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda3) [Reassembled in #185]
   184 22:03:43.375 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda3) [Reassembled in #185]
   185 22:03:43.375 192.168.86.61   128.119.245.12  UDP        54 64929 → 33436 Len=2972
   186 22:03:43.377 192.168.86.1    192.168.86.61   ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
   187 22:03:43.377 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda4) [Reassembled in #189]
   188 22:03:43.377 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda4) [Reassembled in #189]
   189 22:03:43.377 192.168.86.61   128.119.245.12  UDP        54 64929 → 33437 Len=2972
   190 22:03:43.379 192.168.86.1    192.168.86.61   ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
   191 22:03:43.379 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda5) [Reassembled in #193]
   192 22:03:43.379 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda5) [Reassembled in #193]
   193 22:03:43.379 192.168.86.61   128.119.245.12  UDP        54 64929 → 33438 Len=2972
   194 22:03:43.383 10.0.0.1        192.168.86.61   ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
   195 22:03:43.384 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda6) [Reassembled in #197]
   196 22:03:43.384 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda6) [Reassembled in #197]
```

```
    .... 0101 = Header Length: 20 bytes (5)
  ∨ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 1500
    Identification: 0xfda2 (64930)
  ∨ 001. .... = Flags: 0x1, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    ...0 0000 1011 1001 = Fragment Offset: 1480
  › Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0x094c [validation disabled]
```

```
0000  3c 28 6d 89 0e c8 78 4f
0010  05 dc fd a2 20 b9 01 11
0020  f5 0c 00 00 00 00 00 00
0030  00 00 00 00 00 00 00 00
0040  00 00 00 00 00 00 00 00
0050  00 00 00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00
0070  00 00 00 00 00 00 00 00
0080  00 00 00 00 00 00 00 00
0090  00 00 00 00 00 00 00 00
00a0  00 00 00 00 00 00 00 00
00b0  00 00 00 00 00 00 00 00
00c0  00 00 00 00 00 00 00 00
00d0  00 00 00 00 00 00 00 00
00e0  00 00 00 00 00 00 00 00
```

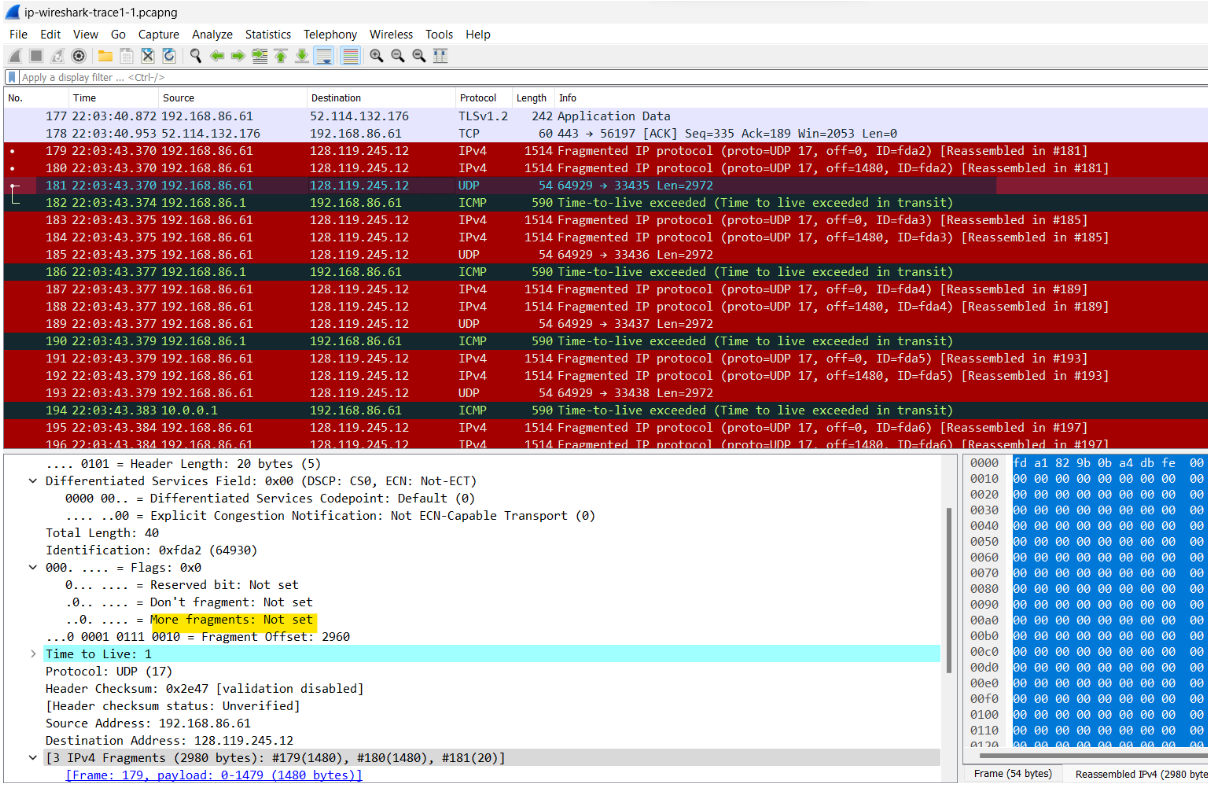
18. What fields change in the IP header between the first and second fragment?

The IP header fields that changed between the fragments are:

- Header Checksum
- Fragment Offset

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?

More fragment, fragment offset. It is the last fragment, since the more fragments flag is not set.

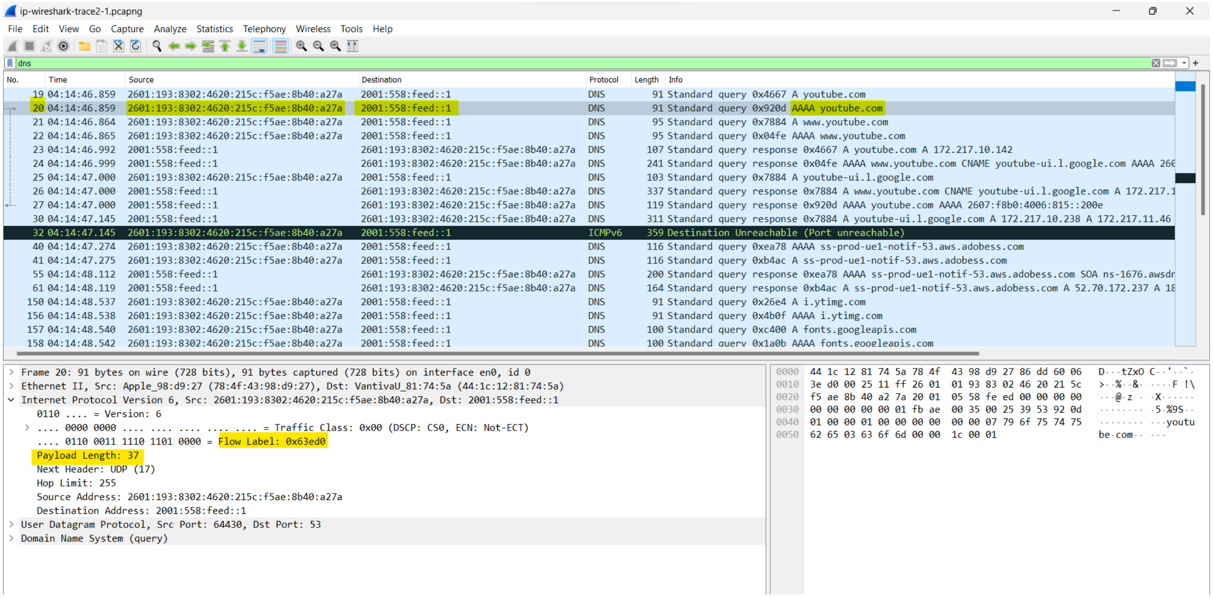

ip-wireshark-trace1-1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time         Source          Destination     Protocol Length Info
177 22:03:40.872 192.168.86.61   52.114.132.176  TLSv1.2   242 Application Data
178 22:03:40.953 52.114.132.176  192.168.86.61   TCP        60 443 → 56197 [ACK] Seq=335 Ack=189 Win=2053 Len=0
179 22:03:43.370 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda2) [Reassembled in #181]
180 22:03:43.370 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda2) [Reassembled in #181]
181 22:03:43.370 192.168.86.61   128.119.245.12  UDP        54 64929 → 33435 Len=2972
182 22:03:43.374 192.168.86.1    192.168.86.61   ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
183 22:03:43.375 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda3) [Reassembled in #185]
184 22:03:43.375 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda3) [Reassembled in #185]
185 22:03:43.375 192.168.86.61   128.119.245.12  UDP        54 64929 → 33436 Len=2972
186 22:03:43.377 192.168.86.1    192.168.86.61   ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
187 22:03:43.377 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda4) [Reassembled in #189]
188 22:03:43.377 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda4) [Reassembled in #189]
189 22:03:43.377 192.168.86.61   128.119.245.12  UDP        54 64929 → 33437 Len=2972
190 22:03:43.379 192.168.86.1    192.168.86.61   ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
191 22:03:43.379 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda5) [Reassembled in #193]
192 22:03:43.379 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda5) [Reassembled in #193]
193 22:03:43.379 192.168.86.61   128.119.245.12  UDP        54 64929 → 33438 Len=2972
194 22:03:43.383 10.0.0.1        192.168.86.61   ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
195 22:03:43.384 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fda6) [Reassembled in #197]
196 22:03:43.384 192.168.86.61   128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda6) [Reassembled in #197]
```

```
    .... 0101 = Header Length: 20 bytes (5)
  ∨ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 40
    Identification: 0xfda2 (64930)
  ∨ 000. .... = Flags: 0x0
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0001 0111 0010 = Fragment Offset: 2960
  > Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0x2e47 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.86.61
    Destination Address: 128.119.245.12
  ∨ [3 IPv4 Fragments (2980 bytes): #179(1480), #180(1480), #181(20)]
      [Frame: 179, payload: 0-1479 (1480 bytes)]
```

```
0000  fd a1 82 9b 0b a4 db fe  00
0010  00 00 00 00 00 00 00 00  00
0020  00 00 00 00 00 00 00 00  00
0030  00 00 00 00 00 00 00 00  00
0040  00 00 00 00 00 00 00 00  00
0050  00 00 00 00 00 00 00 00  00
0060  00 00 00 00 00 00 00 00  00
0070  00 00 00 00 00 00 00 00  00
0080  00 00 00 00 00 00 00 00  00
0090  00 00 00 00 00 00 00 00  00
00a0  00 00 00 00 00 00 00 00  00
00b0  00 00 00 00 00 00 00 00  00
00c0  00 00 00 00 00 00 00 00  00
00d0  00 00 00 00 00 00 00 00  00
00e0  00 00 00 00 00 00 00 00  00
00f0  00 00 00 00 00 00 00 00  00
0100  00 00 00 00 00 00 00 00  00
0110  00 00 00 00 00 00 00 00  00
0120  00 00 00 00 00 00 00 00  00
```

Part 3: IPv6


ip-wireshark-trace2-1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.  Time          Source                                 Destination                            Protocol Length Info
 19 04:14:46.859  2601:193:8302:4620:215c:f5ae:8b40:a27a  2001:558:feed::1                       DNS       91 Standard query 0x4667 A youtube.com
 20 04:14:46.859  2601:193:8302:4620:215c:f5ae:8b40:a27a  2001:558:feed::1                       DNS       91 Standard query 0x920d AAAA youtube.com
 21 04:14:46.864  2601:193:8302:4620:215c:f5ae:8b40:a27a  2001:558:feed::1                       DNS       95 Standard query 0x7884 A www.youtube.com
 22 04:14:46.865  2601:193:8302:4620:215c:f5ae:8b40:a27a  2001:558:feed::1                       DNS       95 Standard query 0x04fe AAAA www.youtube.com
 23 04:14:46.992  2001:558:feed::1                        2601:193:8302:4620:215c:f5ae:8b40:a27a DNS      107 Standard query response 0x4667 A youtube.com A 172.217.10.142
 24 04:14:46.999  2001:558:feed::1                        2601:193:8302:4620:215c:f5ae:8b40:a27a DNS      241 Standard query response 0x04fe AAAA www.youtube.com CNAME youtube-ui.l.google.com AAAA 26(
 25 04:14:47.000  2601:193:8302:4620:215c:f5ae:8b40:a27a  2001:558:feed::1                       DNS      103 Standard query 0x7884 A youtube-ui.l.google.com
 26 04:14:47.000  2001:558:feed::1                        2601:193:8302:4620:215c:f5ae:8b40:a27a DNS      337 Standard query response 0x7884 A www.youtube.com CNAME youtube-ui.l.google.com A 172.217.1
 27 04:14:47.000  2001:558:feed::1                        2601:193:8302:4620:215c:f5ae:8b40:a27a DNS      119 Standard query response 0x920d AAAA youtube.com AAAA 2607:f8b0:4006:815::200e
 30 04:14:47.145  2001:558:feed::1                        2601:193:8302:4620:215c:f5ae:8b40:a27a DNS      311 Standard query response 0x7884 A youtube-ui.l.google.com A 172.217.10.238 A 172.217.11.46
 32 04:14:47.145  2601:193:8302:4620:215c:f5ae:8b40:a27a  2001:558:feed::1                       ICMPv6   359 Destination Unreachable (Port unreachable)
 40 04:14:47.274  2601:193:8302:4620:215c:f5ae:8b40:a27a  2001:558:feed::1                       DNS      116 Standard query 0xea78 AAAA ss-prod-ue1-notif-53.aws.adobess.com
 41 04:14:47.275  2601:193:8302:4620:215c:f5ae:8b40:a27a  2001:558:feed::1                       DNS      116 Standard query 0xb4ac A ss-prod-ue1-notif-53.aws.adobess.com
 55 04:14:48.112  2001:558:feed::1                        2601:193:8302:4620:215c:f5ae:8b40:a27a DNS      200 Standard query response 0xea78 AAAA ss-prod-ue1-notif-53.aws.adobess.com SOA ns-1676.awsdr
 61 04:14:48.119  2001:558:feed::1                        2601:193:8302:4620:215c:f5ae:8b40:a27a DNS      164 Standard query response 0xb4ac A ss-prod-ue1-notif-53.aws.adobess.com A 52.70.172.237 A 18
150 04:14:48.537  2601:193:8302:4620:215c:f5ae:8b40:a27a  2001:558:feed::1                       DNS       91 Standard query 0x26e4 A i.ytimg.com
156 04:14:48.538  2601:193:8302:4620:215c:f5ae:8b40:a27a  2001:558:feed::1                       DNS       91 Standard query 0x4b0f AAAA i.ytimg.com
157 04:14:48.540  2601:193:8302:4620:215c:f5ae:8b40:a27a  2001:558:feed::1                       DNS      100 Standard query 0xc400 A fonts.googleapis.com
158 04:14:48.542  2601:193:8302:4620:215c:f5ae:8b40:a27a  2001:558:feed::1                       DNS      100 Standard query 0x1a0b AAAA fonts.googleapis.com
```

```
> Frame 20: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface en0, id 0
> Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: VantivaU_81:74:5a (44:1c:12:81:74:5a)
∨ Internet Protocol Version 6, Src: 2601:193:8302:4620:215c:f5ae:8b40:a27a, Dst: 2001:558:feed::1
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0110 0011 1110 1101 0000 = Flow Label: 0x63ed0
    Payload Length: 37
    Next Header: UDP (17)
    Hop Limit: 255
    Source Address: 2601:193:8302:4620:215c:f5ae:8b40:a27a
    Destination Address: 2001:558:feed::1
> User Datagram Protocol, Src Port: 64430, Dst Port: 53
> Domain Name System (query)
```

```
0000  44 1c 12 81 74 5a 78 4f  43 98 d9 27 86 dd 60 06   D···tZxO C··'··`·
0010  3e d0 00 25 11 ff 26 01  01 93 83 02 46 20 21 5c   >··%··&· ····F !\
0020  f5 ae 8b 40 a2 7a 20 01  05 58 fe ed 00 00 00 00   ···@·z · ·X······
0030  00 00 00 00 00 01 fb ae  00 35 00 25 39 53 92 0d   ········ ·5·%9S··
0040  01 00 00 01 00 00 00 00  00 00 07 79 6f 75 74 75   ········ ···youtu
0050  62 65 03 63 6f 6d 00 00  1c 00 01                  be·com·· ···
```

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[1].

Source IP address: 2601:193:8302:4620:215c:f5ae:8b40:a27a

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.

Destination IP address: 2001:558:feed::1

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

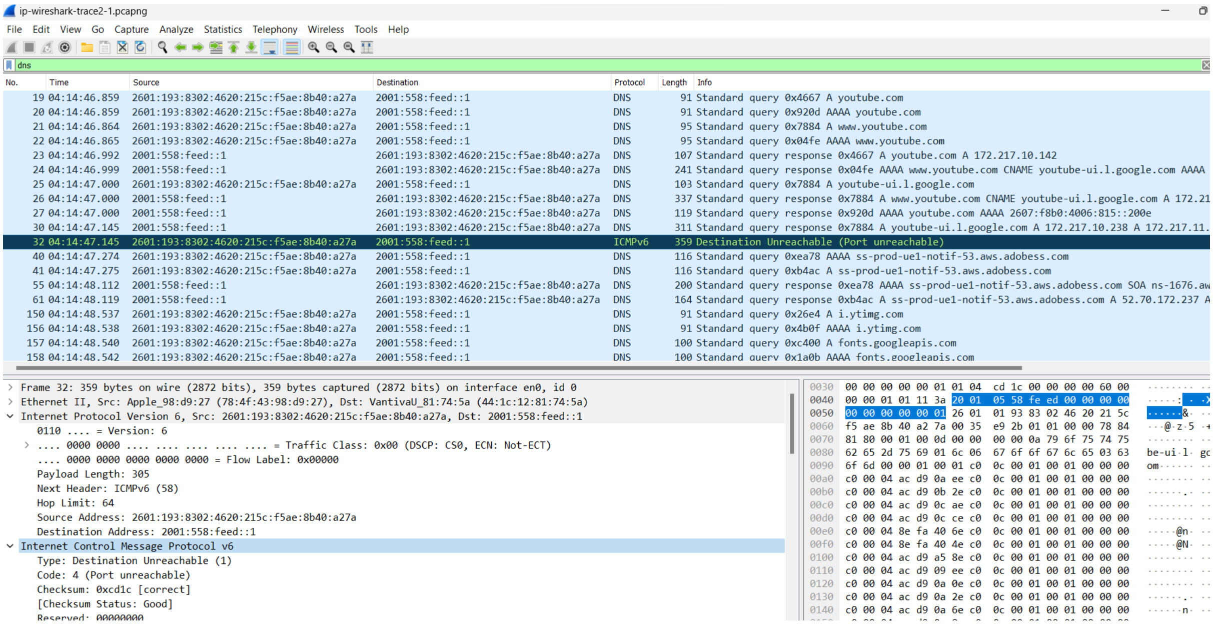
Flow Label: 0x63ed0

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

Payload length: 37

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

ICMPv6 with destination address: 2001:558:feed::1


ip-wireshark-trace2-1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.  Time          Source                                  Destination                             Protocol  Length Info
  19 04:14:46.859  2601:193:8302:4620:215c:f5ae:8b40:a27a  2001:558:feed::1                        DNS          91 Standard query 0x4667 A youtube.com
  20 04:14:46.859  2601:193:8302:4620:215c:f5ae:8b40:a27a  2001:558:feed::1                        DNS          91 Standard query 0x920d AAAA youtube.com
  21 04:14:46.864  2601:193:8302:4620:215c:f5ae:8b40:a27a  2001:558:feed::1                        DNS          95 Standard query 0x7884 A www.youtube.com
  22 04:14:46.865  2601:193:8302:4620:215c:f5ae:8b40:a27a  2001:558:feed::1                        DNS          95 Standard query 0x04fe AAAA www.youtube.com
  23 04:14:46.992  2001:558:feed::1                        2601:193:8302:4620:215c:f5ae:8b40:a27a  DNS         107 Standard query response 0x4667 A youtube.com A 172.217.10.142
  24 04:14:46.999  2001:558:feed::1                        2601:193:8302:4620:215c:f5ae:8b40:a27a  DNS         241 Standard query response 0x04fe AAAA www.youtube.com CNAME youtube-ui.l.google.com AAAA
  25 04:14:47.000  2601:193:8302:4620:215c:f5ae:8b40:a27a  2001:558:feed::1                        DNS         103 Standard query 0x7884 A youtube-ui.l.google.com
  26 04:14:47.000  2001:558:feed::1                        2601:193:8302:4620:215c:f5ae:8b40:a27a  DNS         337 Standard query response 0x7884 A www.youtube.com CNAME youtube-ui.l.google.com A 172.21
  27 04:14:47.000  2001:558:feed::1                        2601:193:8302:4620:215c:f5ae:8b40:a27a  DNS         119 Standard query response 0x920d AAAA youtube.com AAAA 2607:f8b0:4006:815::200e
  30 04:14:47.145  2001:558:feed::1                        2601:193:8302:4620:215c:f5ae:8b40:a27a  DNS         311 Standard query response 0x7884 A youtube-ui.l.google.com A 172.217.10.238 A 172.217.11.
  32 04:14:47.145  2601:193:8302:4620:215c:f5ae:8b40:a27a  2001:558:feed::1                        ICMPv6      359 Destination Unreachable (Port unreachable)
  40 04:14:47.274  2601:193:8302:4620:215c:f5ae:8b40:a27a  2001:558:feed::1                        DNS         116 Standard query 0xea78 AAAA ss-prod-ue1-notif-53.aws.adobess.com
  41 04:14:47.275  2601:193:8302:4620:215c:f5ae:8b40:a27a  2001:558:feed::1                        DNS         116 Standard query 0xb4ac A ss-prod-ue1-notif-53.aws.adobess.com
  55 04:14:48.112  2001:558:feed::1                        2601:193:8302:4620:215c:f5ae:8b40:a27a  DNS         200 Standard query response 0xea78 AAAA ss-prod-ue1-notif-53.aws.adobess.com SOA ns-1676.aw
  61 04:14:48.119  2001:558:feed::1                        2601:193:8302:4620:215c:f5ae:8b40:a27a  DNS         164 Standard query response 0xb4ac A ss-prod-ue1-notif-53.aws.adobess.com A 52.70.172.237 A
 150 04:14:48.537  2601:193:8302:4620:215c:f5ae:8b40:a27a  2001:558:feed::1                        DNS          91 Standard query 0x26e4 A i.ytimg.com
 156 04:14:48.538  2601:193:8302:4620:215c:f5ae:8b40:a27a  2001:558:feed::1                        DNS          91 Standard query 0x4b0f AAAA i.ytimg.com
 157 04:14:48.540  2601:193:8302:4620:215c:f5ae:8b40:a27a  2001:558:feed::1                        DNS         100 Standard query 0xc400 A fonts.googleapis.com
 158 04:14:48.542  2601:193:8302:4620:215c:f5ae:8b40:a27a  2001:558:feed::1                        DNS         100 Standard query 0x1a0b AAAA fonts.googleapis.com
```

```
> Frame 32: 359 bytes on wire (2872 bits), 359 bytes captured (2872 bits) on interface en0, id 0
> Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: VantivaU_81:74:5a (44:1c:12:81:74:5a)
v Internet Protocol Version 6, Src: 2601:193:8302:4620:215c:f5ae:8b40:a27a, Dst: 2001:558:feed::1
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 305
    Next Header: ICMPv6 (58)
    Hop Limit: 64
    Source Address: 2601:193:8302:4620:215c:f5ae:8b40:a27a
    Destination Address: 2001:558:feed::1
v Internet Control Message Protocol v6
    Type: Destination Unreachable (1)
    Code: 4 (Port unreachable)
    Checksum: 0xcd1c [correct]
    [Checksum Status: Good]
    Reserved: 00000000
```

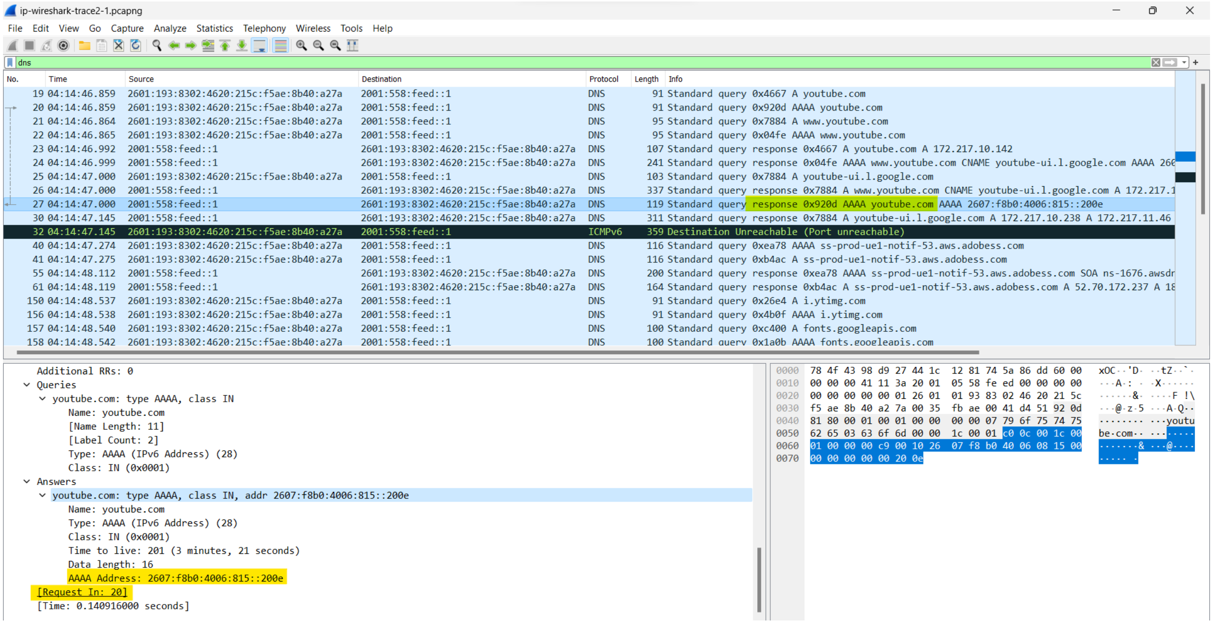
```
0030  00 00 00 00 00 01 01 04  cd 1c 00 00 00 00 60 00   ········ ··
0040  00 00 01 01 11 3a 20 01  05 58 fe ed 00 00 00 00   ·····:·  ·X
0050  00 00 00 00 00 01 26 01  01 93 83 02 46 20 21 5c   ······&· ··
0060  f5 ae 8b 40 a2 7a 00 35  e9 2b 01 01 00 00 78 84   ···@·z·5 ·+
0070  81 80 00 01 00 0d 00 00  00 00 0a 79 6f 75 74 75   ········ ··
0080  62 65 2d 75 69 01 6c 06  67 6f 6f 67 6c 65 03 63   be-ui·l· gc
0090  6f 6d 00 00 01 00 01 c0  0c 00 01 00 01 00 00 00   om······ ··
00a0  c0 00 04 ac d9 0a ee c0  0c 00 01 00 01 00 00 00   ········ ··
00b0  c0 00 04 ac d9 0b 2e c0  0c 00 01 00 01 00 00 00   ······.· ··
00c0  c0 00 04 ac d9 0c ae c0  0c 00 01 00 01 00 00 00   ········ ··
00d0  c0 00 04 ac d9 0c ce c0  0c 00 01 00 01 00 00 00   ········ ··
00e0  c0 00 04 8e fa 40 6e c0  0c 00 01 00 01 00 00 00   ·····@n· ··
00f0  c0 00 04 8e fa 40 4e c0  0c 00 01 00 01 00 00 00   ·····@N· ··
0100  c0 00 04 ac d9 a5 8e c0  0c 00 01 00 01 00 00 00   ········ ··
0110  c0 00 04 ac d9 09 ee c0  0c 00 01 00 01 00 00 00   ········ ··
0120  c0 00 04 ac d9 0a 0e c0  0c 00 01 00 01 00 00 00   ········ ··
0130  c0 00 04 ac d9 0a 2e c0  0c 00 01 00 01 00 00 00   ······.· ··
0140  c0 00 04 ac d9 0a 6e c0  0c 00 01 00 01 00 00 00   ······n· ··
```

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

2 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.

AAAA 2607:f8b0:4006:815::200e



dns

```
No.   Time          Source                                   Destination                              Protocol  Length Info
   19 04:14:46.859  2601:193:8302:4620:215c:f5ae:8b40:a27a   2001:558:feed::1                         DNS        91 Standard query 0x4667 A youtube.com
   20 04:14:46.859  2601:193:8302:4620:215c:f5ae:8b40:a27a   2001:558:feed::1                         DNS        91 Standard query 0x920d AAAA youtube.com
   21 04:14:46.864  2601:193:8302:4620:215c:f5ae:8b40:a27a   2001:558:feed::1                         DNS        95 Standard query 0x7884 A www.youtube.com
   22 04:14:46.865  2601:193:8302:4620:215c:f5ae:8b40:a27a   2001:558:feed::1                         DNS        95 Standard query 0x04fe AAAA www.youtube.com
   23 04:14:46.992  2001:558:feed::1                         2601:193:8302:4620:215c:f5ae:8b40:a27a   DNS       107 Standard query response 0x4667 A youtube.com A 172.217.10.142
   24 04:14:46.999  2001:558:feed::1                         2601:193:8302:4620:215c:f5ae:8b40:a27a   DNS       241 Standard query response 0x04fe AAAA www.youtube.com CNAME youtube-ui.l.google.com AAAA 260
   25 04:14:47.000  2601:193:8302:4620:215c:f5ae:8b40:a27a   2001:558:feed::1                         DNS       103 Standard query 0x7884 A youtube-ui.l.google.com
   26 04:14:47.000  2001:558:feed::1                         2601:193:8302:4620:215c:f5ae:8b40:a27a   DNS       337 Standard query response 0x7884 A www.youtube.com CNAME youtube-ui.l.google.com A 172.217.1
   27 04:14:47.000  2001:558:feed::1                         2601:193:8302:4620:215c:f5ae:8b40:a27a   DNS       119 Standard query response 0x920d AAAA youtube.com AAAA 2607:f8b0:4006:815::200e
   30 04:14:47.145  2001:558:feed::1                         2601:193:8302:4620:215c:f5ae:8b40:a27a   DNS       311 Standard query response 0x7884 A youtube-ui.l.google.com A 172.217.10.238 A 172.217.11.46
   32 04:14:47.145  2601:193:8302:4620:215c:f5ae:8b40:a27a   2001:558:feed::1                         ICMPv6    359 Destination Unreachable (Port unreachable)
   40 04:14:47.274  2601:193:8302:4620:215c:f5ae:8b40:a27a   2001:558:feed::1                         DNS       116 Standard query 0xea78 AAAA ss-prod-ue1-notif-53.aws.adobess.com
   41 04:14:47.275  2601:193:8302:4620:215c:f5ae:8b40:a27a   2001:558:feed::1                         DNS       116 Standard query 0xb4ac A ss-prod-ue1-notif-53.aws.adobess.com
   55 04:14:48.112  2001:558:feed::1                         2601:193:8302:4620:215c:f5ae:8b40:a27a   DNS       200 Standard query response 0xea78 AAAA ss-prod-ue1-notif-53.aws.adobess.com SOA ns-1676.awsdr
   61 04:14:48.119  2001:558:feed::1                         2601:193:8302:4620:215c:f5ae:8b40:a27a   DNS       164 Standard query response 0xb4ac A ss-prod-ue1-notif-53.aws.adobess.com A 52.70.172.237 A 18
  150 04:14:48.537  2601:193:8302:4620:215c:f5ae:8b40:a27a   2001:558:feed::1                         DNS        91 Standard query 0x26e4 A i.ytimg.com
  156 04:14:48.538  2601:193:8302:4620:215c:f5ae:8b40:a27a   2001:558:feed::1                         DNS        91 Standard query 0x4b0f AAAA i.ytimg.com
  157 04:14:48.540  2601:193:8302:4620:215c:f5ae:8b40:a27a   2001:558:feed::1                         DNS       100 Standard query 0xc400 A fonts.googleapis.com
  158 04:14:48.542  2601:193:8302:4620:215c:f5ae:8b40:a27a   2001:558:feed::1                         DNS       100 Standard query 0x1a0b AAAA fonts.googleapis.com
```

```
    Additional RRs: 0
  ˅ Queries
    ˅ youtube.com: type AAAA, class IN
        Name: youtube.com
        [Name Length: 11]
        [Label Count: 2]
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
  ˅ Answers
    ˅ youtube.com: type AAAA, class IN, addr 2607:f8b0:4006:815::200e
        Name: youtube.com
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
        Time to live: 201 (3 minutes, 21 seconds)
        Data length: 16
        AAAA Address: 2607:f8b0:4006:815::200e
    [Request In: 20]
    [Time: 0.140916000 seconds]
```

```
0000  78 4f 43 98 d9 27 44 1c  12 81 74 5a 86 dd 60 00   xOC··'D· ··tZ··`·
0010  00 00 00 41 11 3a 20 01  05 58 fe ed 00 00 00 00   ···A·: · ·X······
0020  00 00 00 00 00 01 26 01  01 93 83 02 46 20 21 5c   ······&· ····F !\
0030  f5 ae 8b 40 a2 7a 00 35  fb ae 00 41 d4 51 92 0d   ···@·z·5 ···A·Q··
0040  81 80 00 01 00 01 00 00  00 00 07 79 6f 75 74 75   ········ ···youtu
0050  62 65 03 63 6f 6d 00 00  1c 00 01 c0 0c 00 1c 00   be·com·· ········
0060  01 00 00 00 c9 00 10 26  07 f8 b0 40 06 08 15 00   ·······& ···@····
0070  00 00 00 00 00 20 0e                               ····· ·
```