

CS315 : Computer Networks Lab

Assignment 7

Sourabh Bhosale (200010004)

February 14, 2023

# 1 Part 1: Basic IPv4

```
~ $ traceroute gaia.cs.umass.edu 56
traceroute to gaia.cs.umass.edu (128.119.245.12), 64 hops max, 56 byte packets
 1  10.196.3.250 (10.196.3.250)  15.274 ms  6.628 ms  5.503 ms
 2  firewall.iitdh.ac.in (10.250.209.251)  5.399 ms  4.042 ms  5.566 ms
 3  14.139.150.65 (14.139.150.65)  5.045 ms  4.033 ms  5.492 ms
 4  * * *
 5  10.255.238.225 (10.255.238.225)  52.833 ms  45.181 ms  45.047 ms
 6  180.149.48.18 (180.149.48.18)  34.422 ms  35.612 ms  35.347 ms
 7  180.149.48.2 (180.149.48.2)  153.711 ms  153.222 ms  152.793 ms
 8  180.149.48.13 (180.149.48.13)  305.472 ms
   180.149.48.20 (180.149.48.20)  165.403 ms
   180.149.48.13 (180.149.48.13)  292.882 ms
  9  180.149.48.13 (180.149.48.13)  302.429 ms  313.816 ms
fourhundredrudge-0-0-21.4079.core2.newy32aoa.net.internet2.edu (163.253.1.45)  300.182 ms
10 fourhundredrudge-0-0-19.4079.core2.newy32aoa.net.internet2.edu (163.253.1.41)  301.763 ms
nox300gw1-i2-re.nox.org (192.5.89.221)  261.425 ms
fourhundredrudge-0-0-21.4079.core2.newy32aoa.net.internet2.edu (163.253.1.45)  346.628 ms
11 192.5.89.58 (192.5.89.58)  305.887 ms
nox300gw1-i2-re.nox.org (192.5.89.221)  307.434 ms
192.5.89.58 (192.5.89.58)  262.368 ms
12 nox-mghpcc-gw1-umassnet-re2.nox.org (18.2.8.90)  348.883 ms
192.5.89.58 (192.5.89.58)  303.855 ms
nox-mghpcc-gw1-umassnet-re2.nox.org (18.2.8.90)  304.350 ms
13 nox-mghpcc-gw1-umassnet-re2.nox.org (18.2.8.90)  306.387 ms  306.740 ms
69.16.1.0 (69.16.1.0)  252.597 ms
14 69.16.1.0 (69.16.1.0)  361.174 ms  309.418 ms
core2-rt-et-8-3-0.gw.umass.edu (192.80.83.113)  306.099 ms
15 core1-rt-et-8-3-0.gw.umass.edu (192.80.83.109)  264.636 ms
n5-rt-1-1-et-0-0-0.gw.umass.edu (128.119.0.8)  340.426 ms
n5-rt-1-1-et-10-0-0.gw.umass.edu (128.119.0.10)  306.314 ms
16 cics-rt-xe-0-0-0.gw.umass.edu (128.119.3.32)  281.633 ms
n5-rt-1-1-et-0-0-0.gw.umass.edu (128.119.0.8)  303.544 ms
cics-rt-xe-0-0-0.gw.umass.edu (128.119.3.32)  306.144 ms
17 nscs1bbs1.cs.umass.edu (128.119.240.253)  311.093 ms
cics-rt-xe-0-0-0.gw.umass.edu (128.119.3.32)  322.275 ms
nscs1bbs1.cs.umass.edu (128.119.240.253)  255.270 ms
18 nscs1bbs1.cs.umass.edu (128.119.240.253)  357.192 ms  255.062 ms
gaia.cs.umass.edu (128.119.245.12)  356.282 ms !Z
19 * gaia.cs.umass.edu (128.119.245.12)  320.558 ms !Z  304.479 ms !Z
~ $ traceroute gaia.cs.umass.edu 3000
```

```
~ $ traceroute gaia.cs.umass.edu 3000
traceroute to gaia.cs.umass.edu (128.119.245.12), 64 hops max, 3000 byte packets
 1  10.196.3.250 (10.196.3.250)  13.555 ms  8.566 ms  4.763 ms
 2  firewall.iitdh.ac.in (10.250.209.251)  5.405 ms  6.569 ms  7.676 ms
 3  14.139.150.65 (14.139.150.65)  7.090 ms  5.758 ms  4.498 ms
 4  *|[A * *
 5  10.255.238.225 (10.255.238.225)  47.348 ms  46.394 ms  45.910 ms
 6  180.149.48.18 (180.149.48.18)  34.870 ms  36.668 ms  34.843 ms
 7  180.149.48.2 (180.149.48.2)  154.008 ms  154.480 ms  153.965 ms
 8  180.149.48.13 (180.149.48.13)  312.620 ms  301.625 ms  307.048 ms
 9  fourhundredrudge-0-0-20.4079.core2.newy32aoa.net.internet2.edu (163.253.1.43)  308.760 ms  302.887 ms  308.792 ms
10 nox300gw1-i2-re.nox.org (192.5.89.221)  308.525 ms  305.885 ms  309.479 ms
11 192.5.89.58 (192.5.89.58)  303.817 ms  306.966 ms  302.456 ms
12 nox-mghpcc-gw1-umassnet-re2.nox.org (18.2.8.90)  304.846 ms  323.747 ms  302.045 ms
13 69.16.1.0 (69.16.1.0)  297.204 ms  306.454 ms  309.024 ms
14 core1-rt-et-8-3-0.gw.umass.edu (192.80.83.109)  305.605 ms  263.205 ms  349.305 ms
15 n5-rt-1-1-et-0-0-0.gw.umass.edu (128.119.0.8)  306.066 ms  310.056 ms  306.322 ms
16 cics-rt-xe-0-0-0.gw.umass.edu (128.119.3.32)  315.031 ms  292.854 ms  309.741 ms
17 * * *
18 gaia.cs.umass.edu (128.119.245.12)  269.583 ms !Z  265.197 ms !Z  320.851 ms !Z
~ $
```

| No. | Time         | Source                | Destination    | Protocol | Length | Info  |
|-----|--------------|-----------------------|----------------|----------|--------|---|
| 293 | 17:21:00.000 | fe80::3c17:9c%eth0    | ff02::1        | MDNS     | 405    | Standard query response 0x0000 TXT, cache flush TXT, cache flush NSEC, cache flush CNAME  |
| 294 | 4.917178     | 10.196.4.31           | 224.0.0.251    | MDNS     | 405    | Standard query response 0x0000 TXT, cache flush TXT, cache flush NSEC, cache flush {"nm":"Redmi Note 7 Pro", "as": "[8194]", "ip": "31"}._mi-connect._udp.local |
| 295 | 5.010185     | 10.196.4.40           | 128.119.245.12 | UDP      | 70     | 39119 -> 33435 Len=28   |
| 302 | 5.018665     | fe80::fc15:f3ff:fe... | ff02::fb       | MDNS     | 143    | Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 10.196  |
| 303 | 5.019121     | 10.196.4.108          | 224.0.0.251    | MDNS     | 123    | Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 10.196  |
| 304 | 5.020115     | fe80::c032:9cff:fe... | ff02::fb       | MDNS     | 145    | Standard query 0x0000 ANY Android-2.local, "QM" question ANY Android-2.local, "QM" question A 10.196  |
| 305 | 5.020117     | 10.196.7.34           | 224.0.0.251    | MDNS     | 125    | Standard query 0x0000 ANY Android-2.local, "QM" question ANY Android-2.local, "QM" question A 10.196  |
| 306 | 5.021833     | fe80::81d:c95d:c4c... | ff02::fb       | MDNS     | 213    | Standard query response 0x0000 PTR Varad's MacBook Pro._airplay._tcp.local PTR 3C06303D392@Varad  |
| 307 | 5.022642     | 10.196.6.92           | 224.0.0.251    | MDNS     | 193    | Standard query response 0x0000 PTR Varad's MacBook Pro._airplay._tcp.local PTR 3C06303D392@Varad  |
| 308 | 5.022643     | 10.196.4.193          | 10.196.255.255 | UDP      | 77     | 34837 -> 15600 Len=35   |
| 309 | 5.024610     | 10.196.3.250          | 10.196.4.40    | ICMP     | 98     | Time-to-live exceeded (Time to live exceeded in transit)  |
| 310 | 5.026769     | 10.196.4.40           | 10.250.200.3   | DNS      | 85     | Standard query 0xb0d5 PTR 250.3.196.10.in-addr.arpa   |
| 311 | 5.031491     | 10.250.200.3          | 10.196.4.40    | DNS      | 85     | Standard query response 0xb0d5 No such name PTR 250.3.196.10.in-addr.arpa   |
| 312 | 5.033367     | 10.196.4.40           | 128.119.245.12 | UDP      | 70     | 39119 -> 33436 Len=28   |
| 313 | 5.039727     | 10.196.3.250          | 10.196.4.40    | ICMP     | 98     | Time-to-live exceeded (Time to live exceeded in transit)  |
| 314 | 5.039991     | 10.196.4.40           | 128.119.245.12 | UDP      | 70     | 39119 -> 33437 Len=28   |
| 315 | 5.045173     | 10.196.3.250          | 10.196.4.40    | ICMP     | 98     | Time-to-live exceeded (Time to live exceeded in transit)  |
| 316 | 5.045558     | 10.196.4.40           | 128.119.245.12 | UDP      | 70     | 39119 -> 33438 Len=28   |
| 317 | 5.050637     | 10.250.209.251        | 10.196.4.40    | ICMP     | 98     | Time-to-live exceeded (Time to live exceeded in transit)  |
| 318 | 5.052191     | 10.196.4.40           | 128.119.245.12 | UDP      | 70     | 39119 -> 33439 Len=28   |
| 319 | 5.055963     | 10.250.209.251        | 10.196.4.40    | ICMP     | 98     | Time-to-live exceeded (Time to live exceeded in transit)  |
| 320 | 5.056240     | 10.196.4.40           | 128.119.245.12 | UDP      | 70     | 39119 -> 33440 Len=28   |
| 321 | 5.061468     | 10.250.209.251        | 10.196.4.40    | ICMP     | 98     | Time-to-live exceeded (Time to live exceeded in transit)  |
| 322 | 5.061880     | 10.196.4.40           | 128.119.245.12 | UDP      | 70     | 39119 -> 33441 Len=28   |
| 323 | 5.066583     | 14.139.158.65         | 10.196.4.40    | ICMP     | 70     | Time-to-live exceeded (Time to live exceeded in transit)  |
| 324 | 5.068485     | 10.196.4.40           | 10.250.200.3   | DNS      | 86     | Standard query 0x0692 PTR 65.150.139.14.in-addr.arpa  |
| 325 | 5.073950     | 10.250.200.3          | 10.196.4.40    | DNS      | 86     | Standard query response 0x0692 No such name PTR 65.150.139.14.in-addr.arpa  |
| 326 | 5.075534     | 10.196.4.40           | 128.119.245.12 | UDP      | 70     | 39119 -> 33442 Len=28   |
| 327 | 5.079288     | 14.139.158.65         | 10.196.4.40    | ICMP     | 70     | Time-to-live exceeded (Time to live exceeded in transit)  |
| 328 | 5.079478     | 10.196.4.40           | 128.119.245.12 | UDP      | 70     | 39119 -> 33443 Len=28   |
| 329 | 5.084655     | 14.139.158.65         | 10.196.4.40    | ICMP     | 70     | Time-to-live exceeded (Time to live exceeded in transit)  |
| 330 | 5.085026     | 10.196.4.40           | 128.119.245.12 | UDP      | 70     | 39119 -> 33444 Len=28   |
| 331 | 5.119673     | fe80::3c17:9c%eth0    | ff02::fb       | MDNS     | 183    | Standard query 0x0000 ANY {"nm":"Redmi Note 7 Pro", "as": "[8194]", "ip": "31"}._mi-connect._udp.local  |
| 332 | 5.119675     | 10.196.4.135          | 224.0.0.251    | MDNS     | 152    | Standard query 0x001a PTR %9E5E7C8F47989526C9BCD95D24084F6F0B27C5ED sub.googlecast._tcp.local   |

> Frame 1: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface en0, id 0  
 > Ethernet II, Src: b2:4a:93:f1:85:bf (b2:4a:93:f1:85:bf), Dst: IPv6mcast\_fb (33:33:00:00:00:fb)  
 > Internet Protocol Version 6, Src: fe80::b04a:93ff:feff:185bf, Dst: ff02::fb  
 > User Datagram Protocol, Src Port: 5353, Dst Port: 5353  
 > Multicast Domain Name System (response)

0000 33 33 00 00 00 fb b2 4a 93  
 0010 3e e0 01 02 11 ff fe 80 00  
 0020 93 ff fe f1 85 bf ff 02 00  
 0030 00 00 00 00 00 00 fb 14 e9 14  
 0040 84 00 00 00 00 00 04 00 00  
 0050 31 03 31 39 36 02 31 30 07  
 0060 04 61 72 70 61 00 00 0c 80  
 0070 08 41 6e 64 72 6f 69 64 2d  
 0080 6c 00 01 46 01 42 01 35 01  
 0090 01 46 01 46 01 46 01 33 01  
 00a0 01 42 01 38 01 38 01 38 01  
 00b0 01 30 01 38 01 38 01 30 01

Packets: 12319 - Displayed: 7422 (60.2%) - Dropped: 0 (0.0%) Profile: Default

**1. Select the first UDP segment sent by your computer via the traceroute command to gaia.cs.umass.edu. Expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?**

IP address of computer : 10.196.4.40

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

Time-to-live (TTL) : 1

|   |          |                      |                |      |     |  |
|---|----------|----------------------|----------------|------|-----|--|
| 286   | 4.720252 | 10.196.10.107        | 224.0.0.251    | MDNS | 289 | Standard query response 0x0000 PTR, cache flush Android.local PTR, cache flush Android.local A,  |
| 293   | 4.916685 | fe80::3c17:9c7c:42.. | ff02::fb       | MDNS | 425 | Standard query response 0x0000 TXT, cache flush TXT, cache flush NSEC, cache flush {"nm":"Redmi  |
| 294   | 4.917178 | 10.196.8.31          | 224.0.0.251    | MDNS | 405 | Standard query response 0x0000 TXT, cache flush TXT, cache flush NSEC, cache flush {"nm":"Redmi  |
| 295   | 5.010185 | 10.196.4.40          | 128.119.245.12 | UDP  | 70  | 39119 → 33435 Len=28   |
| 302   | 5.018665 | fe80::fc15:f3ff:fe.. | ff02::fb       | MDNS | 143 | Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 10.196 |
| 303   | 5.019121 | 10.196.4.108         | 224.0.0.251    | MDNS | 123 | Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question A 10.196 |
| 304   | 5.020115 | fe80::c032:9cff:fe.. | ff02::fb       | MDNS | 145 | Standard query 0x0000 ANY Android-2.local, "QM" question ANY Android-2.local, "QM" question A 10 |
| 305   | 5.020117 | 10.196.7.34          | 224.0.0.251    | MDNS | 125 | Standard query 0x0000 ANY Android-2.local, "QM" question ANY Android-2.local, "QM" question A 10 |
| 306   | 5.021833 | fe80::81d:c95d:c4c.. | ff02::fb       | MDNS | 213 | Standard query response 0x0000 PTR Varad's MacBook Pro_airplay._tcp.local PTR 3C06303D392E@Vara  |
| 307   | 5.022642 | 10.196.6.92          | 224.0.0.251    | MDNS | 193 | Standard query response 0x0000 PTR Varad's MacBook Pro_airplay._tcp.local PTR 3C06303D392E@Vara  |
| 308   | 5.022643 | 10.196.4.193         | 10.196.255.255 | UDP  | 77  | 34837 → 15600 Len=35   |
| 309   | 5.024610 | 10.196.3.250         | 10.196.4.40    | ICMP | 98  | Time-to-live exceeded (Time to live exceeded in transit)   |
| 310   | 5.026769 | 10.196.4.40          | 10.250.200.3   | DNS  | 85  | Standard query 0xbbd5 PTR 250.3.196.10.in-addr.arpa  |
| 311   | 5.031491 | 10.250.200.3         | 10.196.4.40    | DNS  | 85  | Standard query response 0xbbd5 No such name PTR 250.3.196.10.in-addr.arpa                        |
| 312   | 5.033367 | 10.196.4.40          | 128.119.245.12 | UDP  | 70  | 39119 → 33436 Len=28   |
| 313   | 5.039727 | 10.196.3.250         | 10.196.4.40    | ICMP | 98  | Time-to-live exceeded (Time to live exceeded in transit)   |
| 314   | 5.039991 | 10.196.4.40          | 128.119.245.12 | UDP  | 70  | 39119 → 33437 Len=28   |
| 315   | 5.045173 | 10.196.3.250         | 10.196.4.40    | ICMP | 98  | Time-to-live exceeded (Time to live exceeded in transit)   |
| 316   | 5.045558 | 10.196.4.40          | 128.119.245.12 | UDP  | 70  | 39119 → 33438 Len=28   |
| 317   | 5.050637 | 10.250.209.251       | 10.196.4.40    | ICMP | 98  | Time-to-live exceeded (Time to live exceeded in transit)   |
| 318   | 5.052191 | 10.196.4.40          | 128.119.245.12 | UDP  | 70  | 39119 → 33439 Len=28   |
| > Ethernet II, Src: Apple_ad:cf:45 (14:7d:da:ad:cf:45), Dst: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8) |          |                      |                |      |     |  |
| > Internet Protocol Version 4, Src: 10.196.4.40, 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: 56  |          |                      |                |      |     |  |
| Identification: 0x98d0 (39120)  |          |                      |                |      |     |  |
| > 000. .... = Flags: 0x0  |          |                      |                |      |     |  |
| ...0 0000 0000 0000 = Fragment Offset: 0  |          |                      |                |      |     |  |
| > Time to Live: 1   |          |                      |                |      |     |  |
| 0000 02 04 96 9a 82 e8 14 7d da   |          |                      |                |      |     |  |
| 0010 00 38 98 d0 00 00 01 11 9c   |          |                      |                |      |     |  |
| 0020 f5 0c 98 cf 82 9b 00 24 5f   |          |                      |                |      |     |  |
| 0030 00 00 00 00 00 00 00 00 00   |          |                      |                |      |     |  |
| 0040 00 00 00 00 00 00 00 00 00   |          |                      |                |      |     |  |

```
[~ $ ipconfig getifaddr en0
10.196.4.40
~ $ ]
```

**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].**

Within the header, the value in the upper layer protocol field is UDP (17).

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

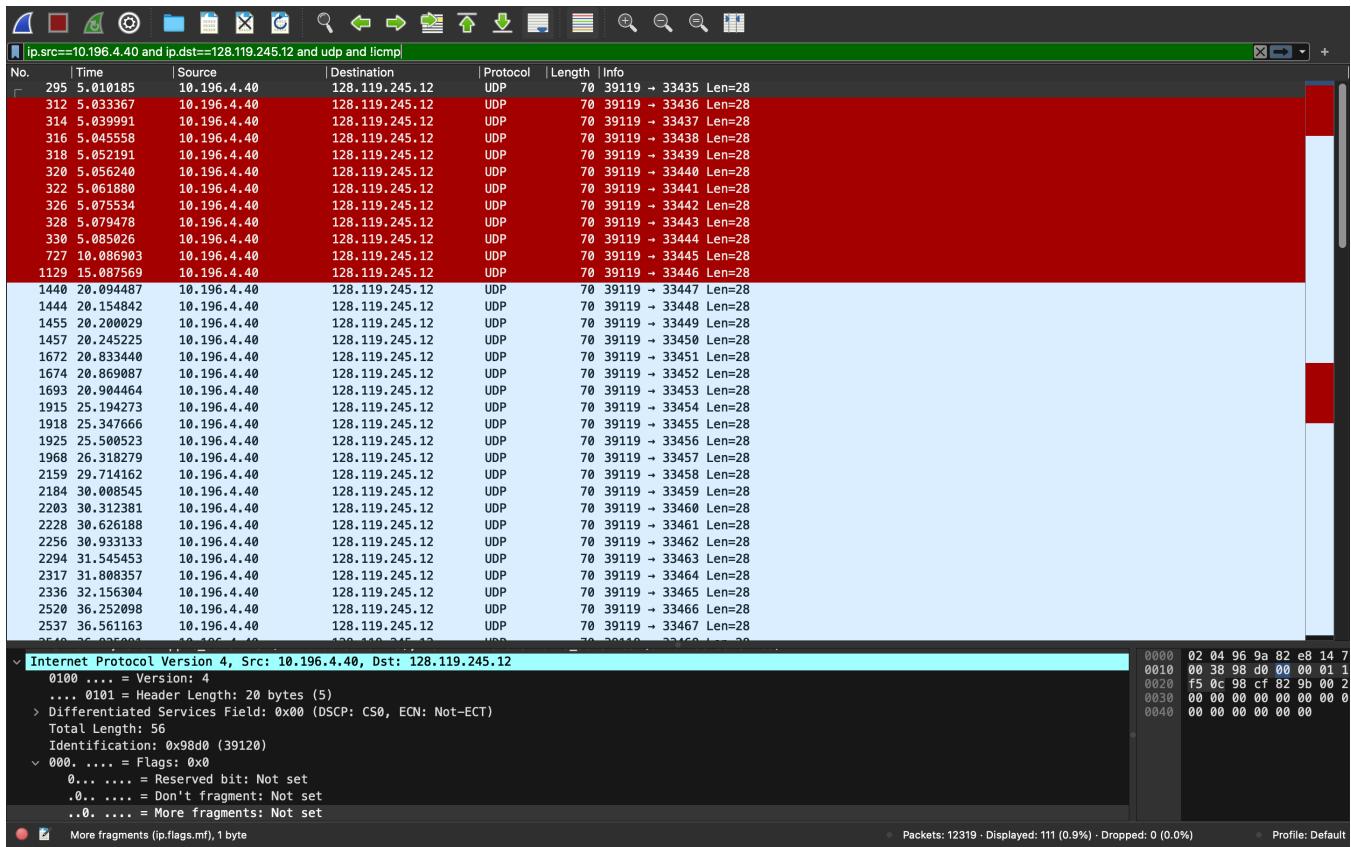
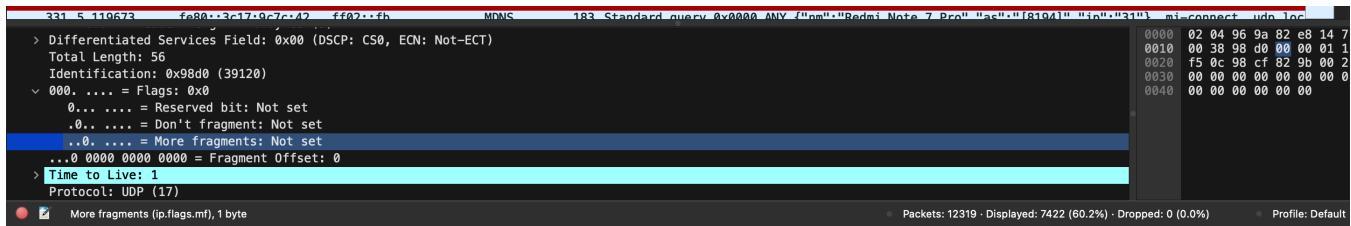
20 bytes

**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 and 56 bytes total length, this gives 36 bytes in the payload of the IP datagram.

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

The more fragments bit = 0, so the data is not 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 fields that always change across the IP datagrams are:

1. Identification(IP packets must have different ids)
2. Time to live (traceroute increments each subsequent packet)
3. Header checksum (since header changes, so must checksum)

TTL value sometimes stays the same for consecutive segments but on an average it varies.

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

The fields that stay constant across the IP datagrams are:

1. Version (since we are using IPv4 for all packets)
2. header length (since these are ICMP packets)
3. source IP (since we are sending from the same source)
4. destination IP (since we are sending to the same destination)
5. Differentiated Services (since all packets are ICMP they use the same Type of Service class)
6. Upper Layer Protocol (since these are ICMP packets)

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

Identification fields gets incremented with each ICMP Echo (ping) request.

The screenshot shows a Wireshark capture window with the filter set to `ip.dst==10.196.4.40 and icmp`. The packet list pane displays numerous ICMP Time-to-Live exceeded (TTL Exceeded) messages. The details pane shows the structure of one such packet, starting with the header:

```

> Frame 309: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
> Ethernet II, Src: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8), Dst: Apple_ad:cf:45 (14:7d:da:ad:cf:45)
> Internet Protocol Version 4, Src: 10.196.3.250, Dst: 10.196.4.40
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
        Total Length: 84
    Identification: 0x9038 (36920)
    < 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: 0xcc07 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.196.3.250
    Destination Address: 10.196.4.40
    > Internet Control Message Protocol
    > Data (28 bytes)

```

The bytes pane on the right shows the raw hex and ASCII data for the selected packet.

**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].**

Within the header, the value in the upper layer protocol field is ICMP (1).

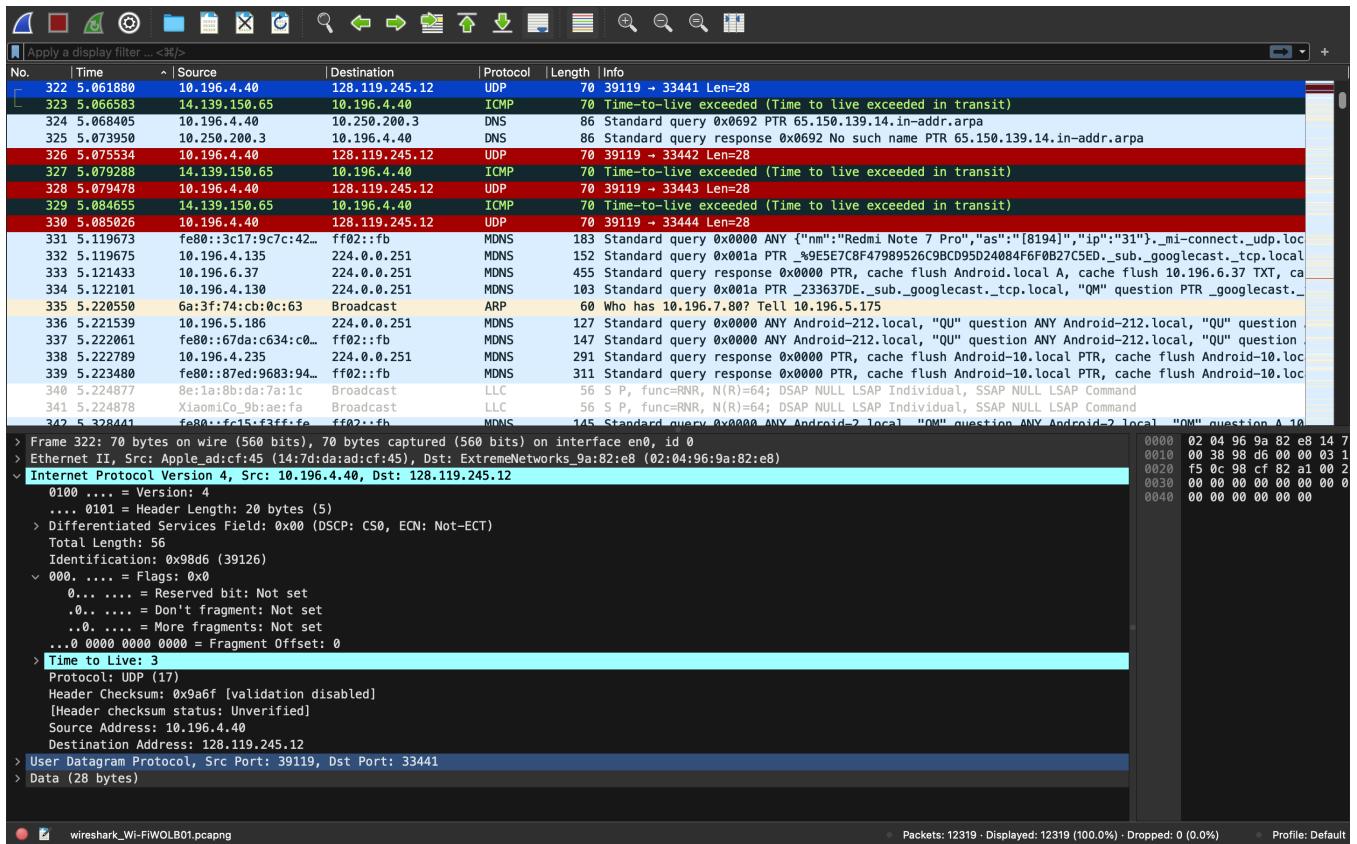
**11. Are the values in the Identification fields (across the sequence of all of ICMP packets from all of the routers) similar in behavior to your answer to question 9 above?**

No, The identification field changes behaviour.

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

No, The TTL field changes. (Somtimes it stays same for consecutive ones)

## 2 Part 2: Fragmentation



- 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!)

Yes, the result can be seen in the screenshot.

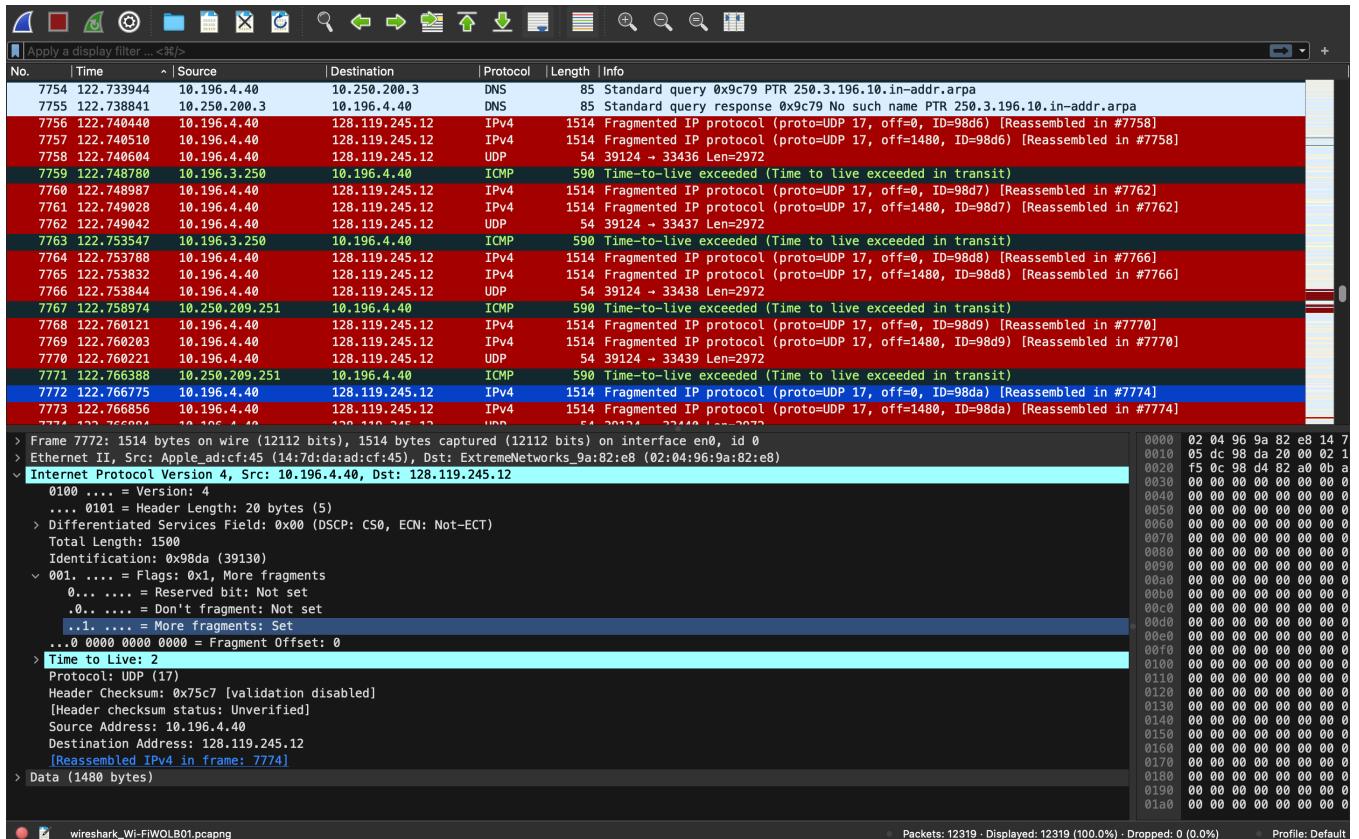


Figure 1: First fragment

## 2. What information in the IP header indicates that this datagram has been fragmented?

The "More fragments" bit is set, indicating the datagram been fragmented and there are more fragments coming.. We can see the message also "Fragmented IP protocol".

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

The “Fragment offset” is zero, indicating this is the first fragment.

```

> Frame 7772: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface en0, id 0
> Ethernet II, Src: Apple_ad:cfc45 (14:7d:da:ad:cfc45), Dst: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8)
> Internet Protocol Version 4, Src: 10.196.4.40, 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: 1500
    Identification: 0x98da (39130)
  > 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: 2
  Protocol: UDP (17)
  Header Checksum: 0x75c7 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.196.4.40
  Destination Address: 128.119.245.12
  [Reassembled IPv4 in frame: 7774]
> Data (1480 bytes)

0000 02 04 96 9a 82 e8 14 7
0010 05 dc 98 da 20 00 02 1
0020 f5 0c 98 d4 82 a0 0b a
0030 00 00 00 00 00 00 00 0
0040 00 00 00 00 00 00 00 0
0050 00 00 00 00 00 00 00 0
0060 00 00 00 00 00 00 00 0
0070 00 00 00 00 00 00 00 0
0080 00 00 00 00 00 00 00 0
0090 00 00 00 00 00 00 00 0
00a0 00 00 00 00 00 00 00 0
00b0 00 00 00 00 00 00 00 0
00c0 00 00 00 00 00 00 00 0
00d0 00 00 00 00 00 00 00 0
00e0 00 00 00 00 00 00 00 0
00f0 00 00 00 00 00 00 00 0
0100 00 00 00 00 00 00 00 0
0110 00 00 00 00 00 00 00 0
0120 00 00 00 00 00 00 00 0
0130 00 00 00 00 00 00 00 0
0140 00 00 00 00 00 00 00 0
0150 00 00 00 00 00 00 00 0
0160 00 00 00 00 00 00 00 0
0170 00 00 00 00 00 00 00 0
0180 00 00 00 00 00 00 00 0
0190 00 00 00 00 00 00 00 0
01a0 00 00 00 00 00 00 00 0

  ● wireshark_Wi-FiWLB01.pcapng   ● Packets: 12319 · Displayed: 12319 (100.0%) · Dropped: 0 (0.0%)   ● Profile: Default

```

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

The total length of this IP datagram is 1500 bytes which includes 20 bytes header length.

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

```

  ● wireshark_Wi-FiWLB01.pcapng   ● Packets: 12319 · Displayed: 12319 (100.0%) · Dropped: 0 (0.0%)   ● Profile: Default
No. Time           [Source]          [Destination]        Protocol Length Info
7756 122.744449 10.196.4.40      128.119.245.12     IPv4   1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=9860) [Reassembled in #7758]
7757 122.746510 10.196.4.40      128.119.245.12     IPv4   1514 Fragmented IP protocol (proto=UDP 17, off=148, ID=9860) [Reassembled in #7758]
7758 122.746864 10.196.4.40      128.119.245.12     UDP    54 39124 - 33436 Len=2972
7759 122.746780 10.196.3.258     10.196.4.40       ICMP  598 Time-to-Live exceeded (Time to live exceeded in transit)
7760 122.746864 10.196.4.40      128.119.245.12     IPv4   1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=9867) [Reassembled in #7762]
7761 122.746823 10.196.4.40      128.119.245.12     UDP    54 39124 - 33437 Len=2972
7762 122.746842 10.196.4.40      128.119.245.12     UDP    54 39124 - 33437 Len=2972
7763 122.753547 10.196.3.258     10.196.4.40       ICMP  598 Time-to-Live exceeded (Time to live exceeded in transit)
7764 122.753788 10.196.4.40      128.119.245.12     IPv4   1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=9860) [Reassembled in #7766]
7765 122.753803 10.196.4.40      128.119.245.12     IPv4   1514 Fragmented IP protocol (proto=UDP 17, off=148, ID=9860) [Reassembled in #7766]
7766 122.753844 10.196.4.40      128.119.245.12     UDP    54 39124 - 33438 Len=2972
7767 122.758974 10.250.209.251  10.196.4.40       ICMP  598 Time-to-Live exceeded (Time to live exceeded in transit)
7768 122.768121 10.196.4.40      128.119.245.12     IPv4   1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=9869) [Reassembled in #7770]
7769 122.768029 10.196.4.40      128.119.245.12     IPv4   1514 Fragmented IP protocol (proto=UDP 17, off=148, ID=9869) [Reassembled in #7770]
7770 122.768039 10.196.4.40      128.119.245.12     UDP    54 39124 - 33439 Len=2972
7771 122.766388 10.250.209.251  10.196.4.40       ICMP  598 Time-to-Live exceeded (Time to live exceeded in transit)
7772 122.766775 10.196.4.40      128.119.245.12     IPv4   1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=9860) [Reassembled in #7774]
7773 122.766856 10.196.4.40      128.119.245.12     UDP    54 39124 - 33448 Len=2972
7774 122.766884 10.196.4.40      128.119.245.12     UDP    54 39124 - 33448 Len=2972
7775 122.766883 IntelCor_3614eb Broadcast ARP    56 Who has 10.196.5.153? {v1, 10.196.7.17}

  ● wireshark_Wi-FiWLB01.pcapng   ● Packets: 12319 · Displayed: 12319 (100.0%) · Dropped: 0 (0.0%)   ● Profile: Default

```

Figure 2: Second fragment

Header checksum and fragment offset changes.

## 6. 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?

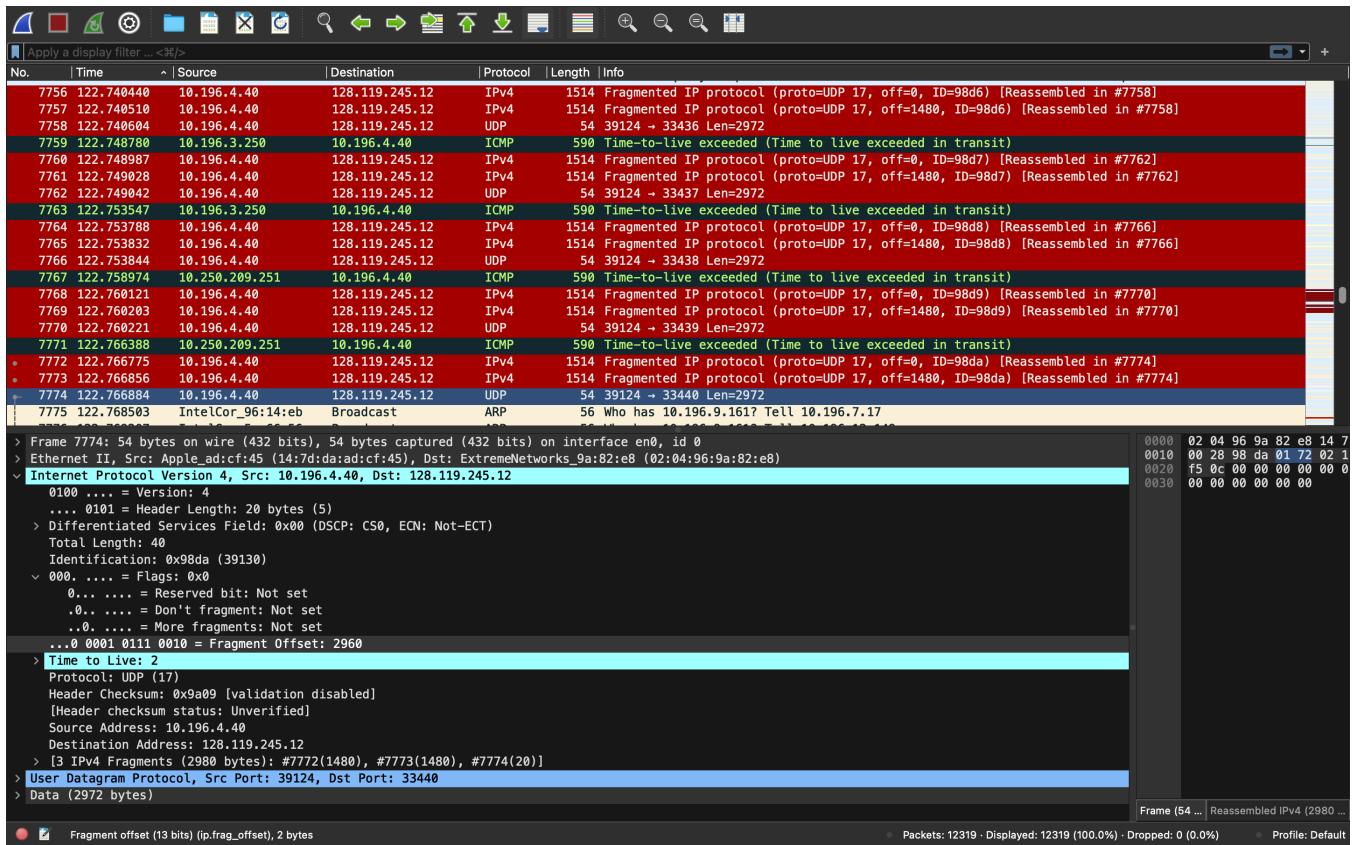
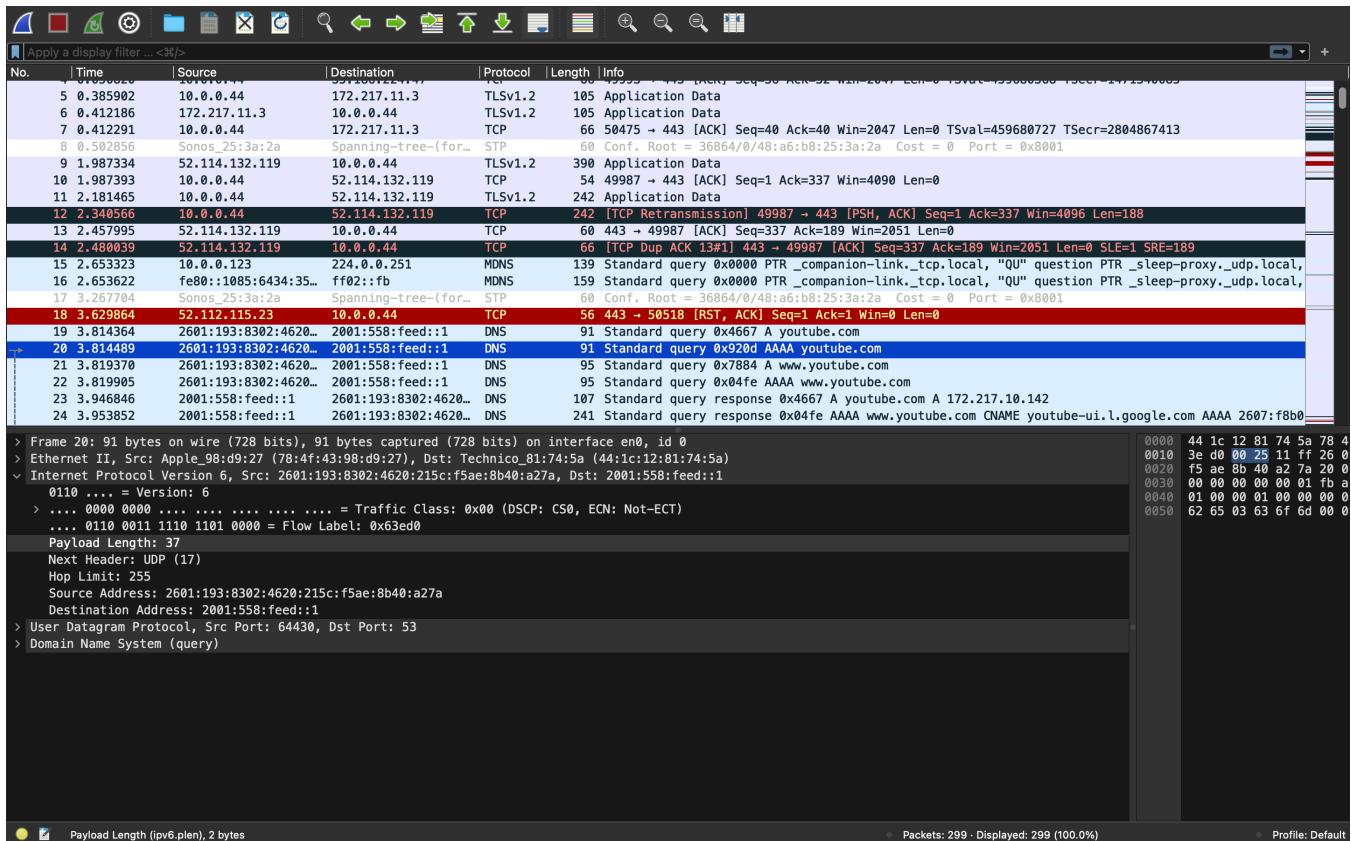


Figure 3: Second fragment

The "more fragments" bit is clear, indicating this is the last fragment.

### 3 Part 3: IPv6



- 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 window1.**

IPv6 address of the computer making the DNS AAAA request(Src):

2601:193:8302:4620:215c:f5ae:8b40:a27a

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

IPv6 destination address for this datagram (Dst): 2001:558:feed::1

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

Flow Label: ox63edo

**4. How much payload data is carried in this datagram?**

37 bytes of payload data is carried in this datagram.

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

UDP (17)

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

Only 1 IPv6 addresse are returned in the response to this AAAA request.

The screenshot shows a Wireshark capture of an AAAA request and its response. The request (packet 1) is a User Datagram Protocol (UDP) packet with a flow label of 0x000000, payload length of 187, and destination port 53. The response (packet 2) is a Domain Name System (DNS) message with a transaction ID of 0x04fe, flags indicating a standard query response, and no errors. It contains 5 answer records for the domain www.youtube.com, each with type AAAA, class IN, and different IPv6 addresses. The interface is 'Text Item (text), 146 bytes' and the profile is 'Default'. The status bar indicates 299 packets displayed.

```
.... 0000 0000 0000 0000 0000 = Flow Label: 0x000000
Payload Length: 187
Next Header: UDP (17)
Hop Limit: 58
Source Address: 2001:558:feed::1
Destination Address: 2601:193:8302:4620:215c:f5ae:8b40:a27a
> User Datagram Protocol, Src Port: 53, Dst Port: 53174
< Domain Name System (response)
  Transaction ID: 0x04fe
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 5
  Authority RRs: 0
  Additional RRs: 0
  > Queries
    > Answers
      > www.youtube.com: type CNAME, class IN, cname youtube-ui.l.google.com
      > youtube-ui.l.google.com: type AAAA, class IN, addr 2607:f8b0:4006:806::200e
      > youtube-ui.l.google.com: type AAAA, class IN, addr 2607:f8b0:4006:81a::200e
      > youtube-ui.l.google.com: type AAAA, class IN, addr 2607:f8b0:4006:81b::200e
      > youtube-ui.l.google.com: type AAAA, class IN, addr 2607:f8b0:4006:807::200e
[Request In: 22]
[Time: 0.133947000 seconds]
```

0000 78 4f 43 98 d9 27 44 1  
0010 00 00 00 bb 11 3a 20 0  
0020 00 00 00 00 00 01 26 0  
0030 f5 ae 8b 40 a2 7a 00 3  
0040 81 80 00 01 00 05 00 0  
0050 6f 75 74 75 62 65 03 6  
0060 0c 00 05 00 01 00 00 e  
0070 75 62 65 2d 75 69 01 6  
0080 18 c0 2d 00 1c 00 01 0  
0090 b0 40 06 08 06 00 00 0  
00a0 1c 00 01 00 00 00 c1 0  
00b0 1a 00 00 00 00 00 00 2  
00c0 00 00 c1 00 10 26 07 f  
00d0 00 00 00 20 0e c0 2d 0  
00e0 10 26 07 f8 b0 40 06 0  
00f0 0e

**7. 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.**

youtube.com: type AAAA, class IN, addr 2607:f8b0:4006:815::200e