CS315 : Computer Networks Lab

Assignment 7

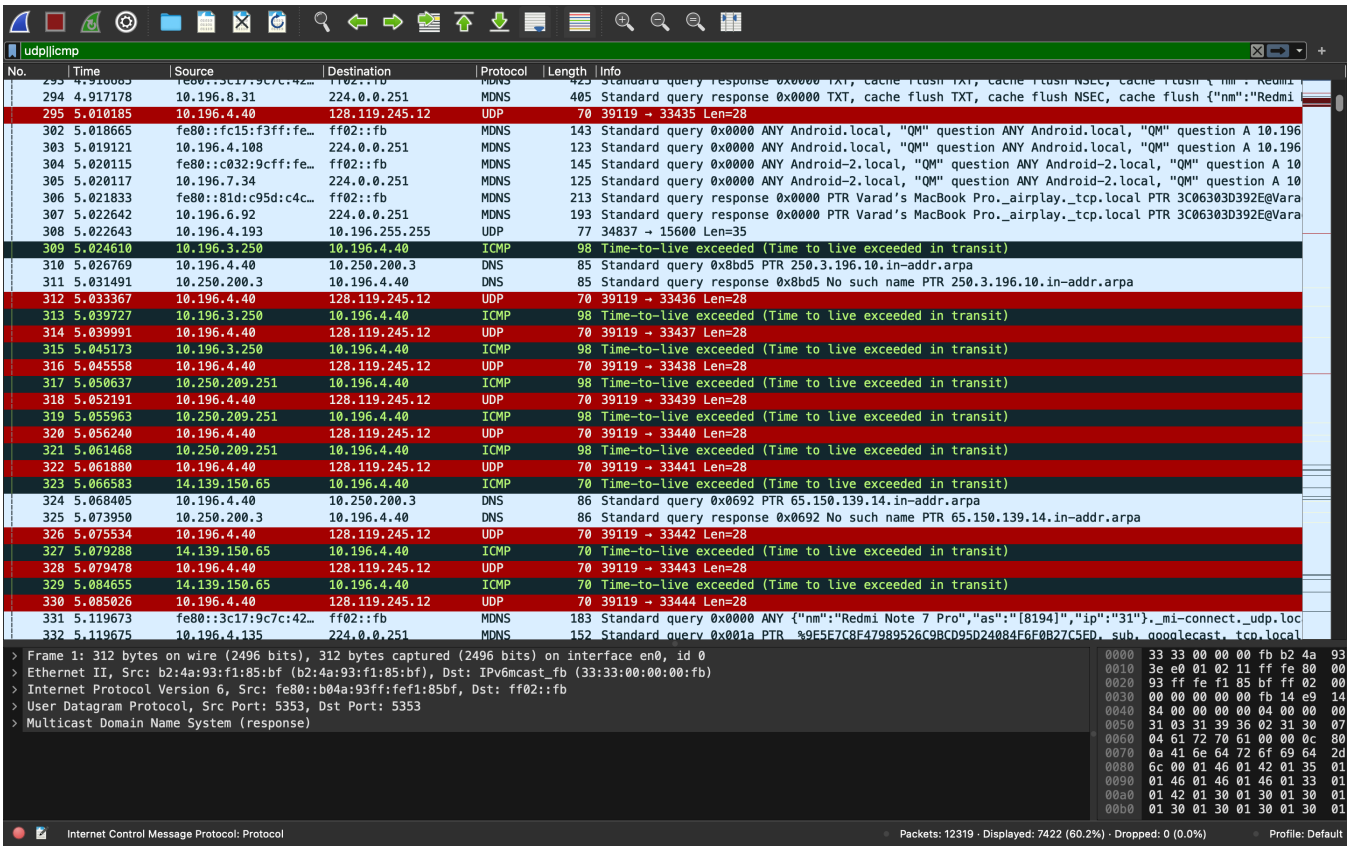
Sourabh Bhosale (200010004)

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)  292.802 ms
 9  180.149.48.13 (180.149.48.13)  302.429 ms  313.816 ms
    fourhundredge-0-0-0-21.4079.core2.newy32aoa.net.internet2.edu (163.253.1.45)  300.182 ms
10  fourhundredge-0-0-0-19.4079.core2.newy32aoa.net.internet2.edu (163.253.1.41)  301.763 ms
    nox300gw1-i2-re.nox.org (192.5.89.221)  261.425 ms
    fourhundredge-0-0-0-21.4079.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  fourhundredge-0-0-0-20.4079.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
~ $
```

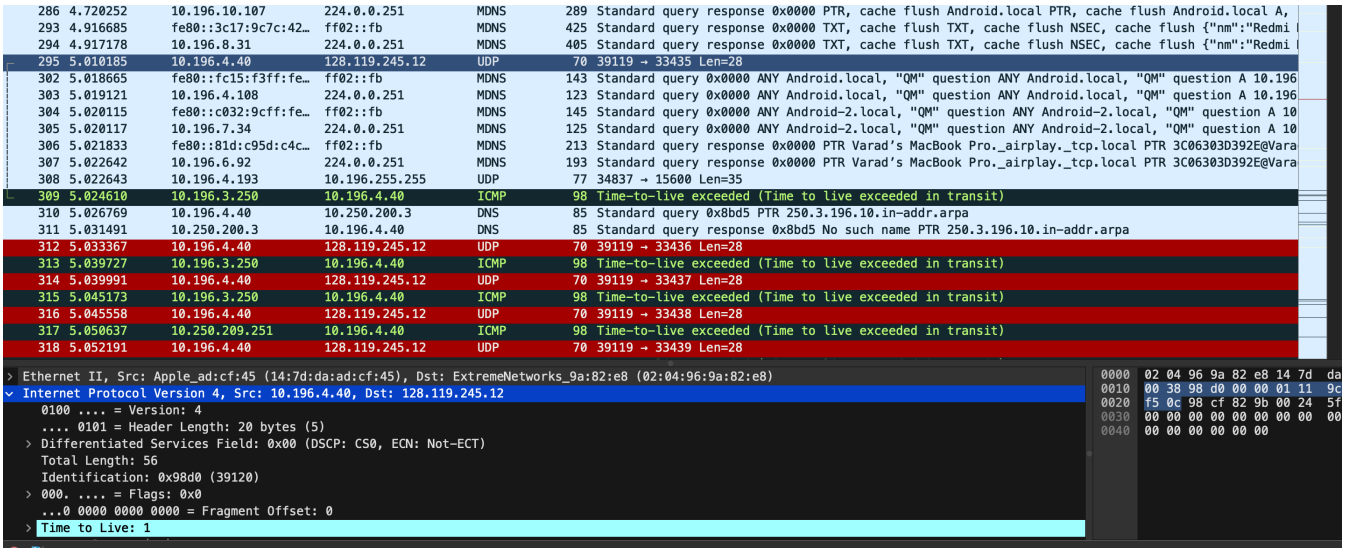


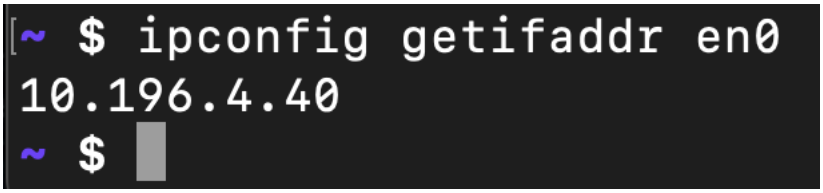
1. Select the first UDP segment sent by your computer via the tracer-oute command to gaia.cs.umass.edu. Expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

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





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?

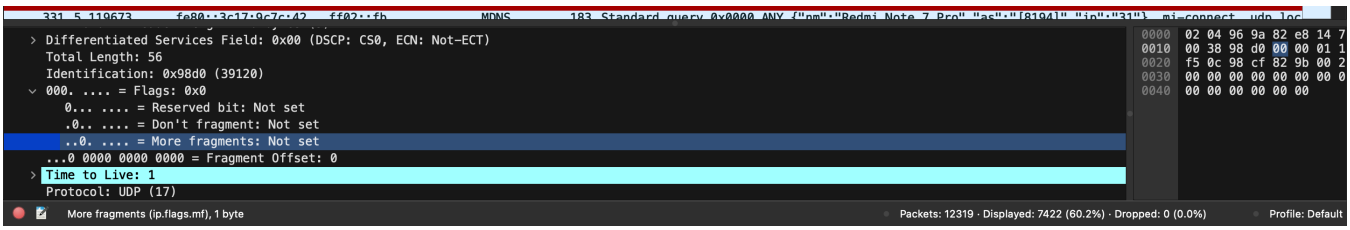
20 bytes

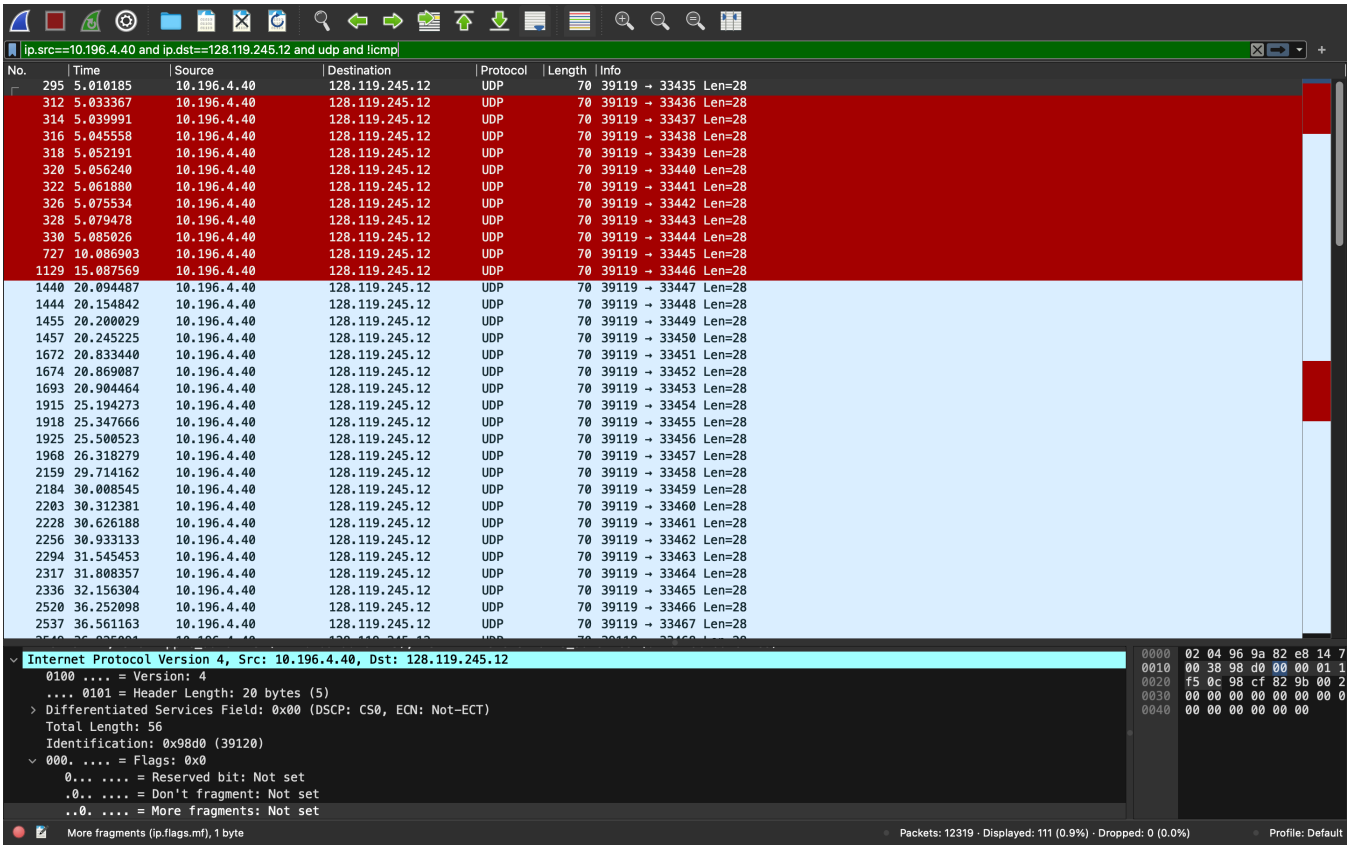
5. How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

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 = o, 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.

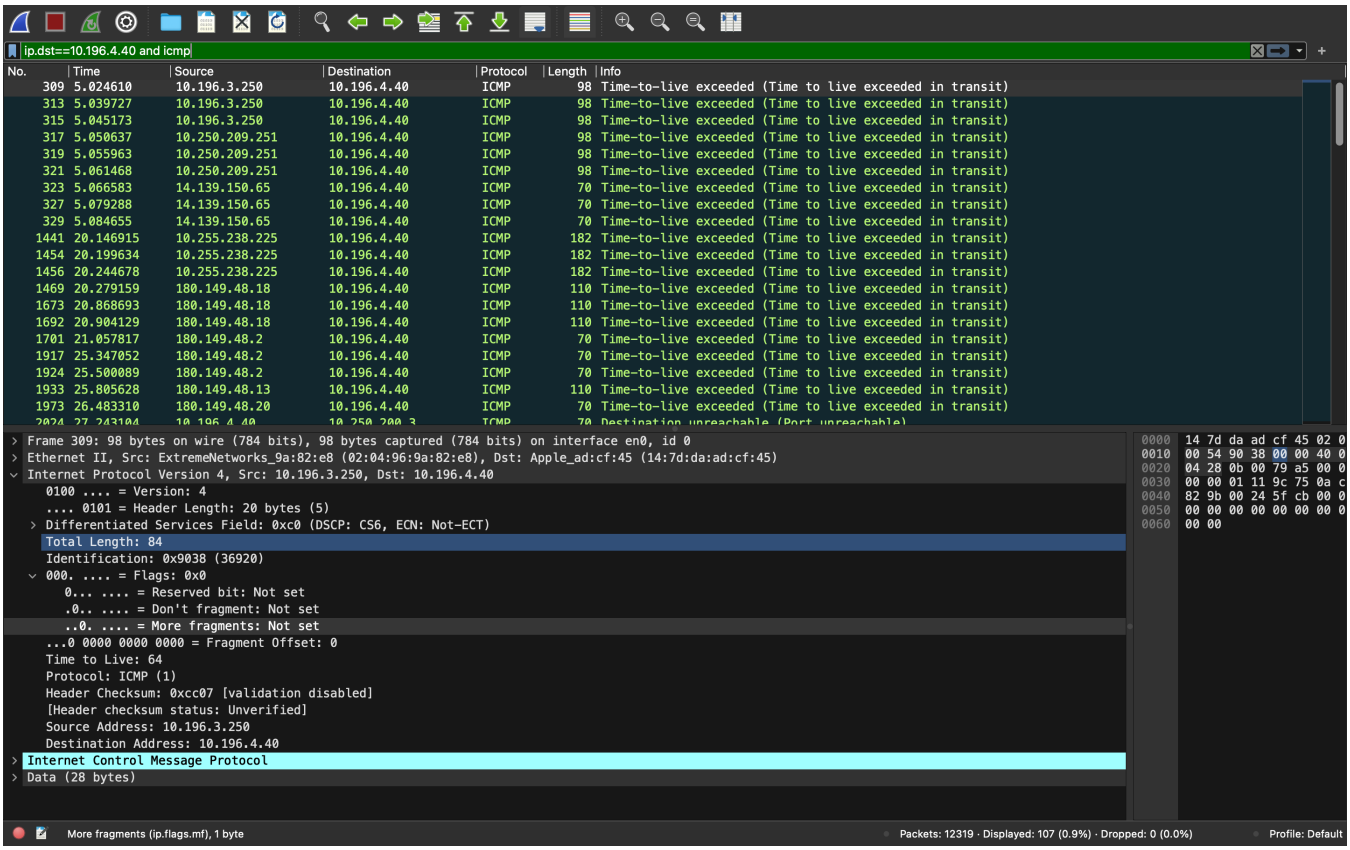
8. Which fields in this sequence of IP datagrams (containing UDP segments) stay constant? Why?

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.



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).

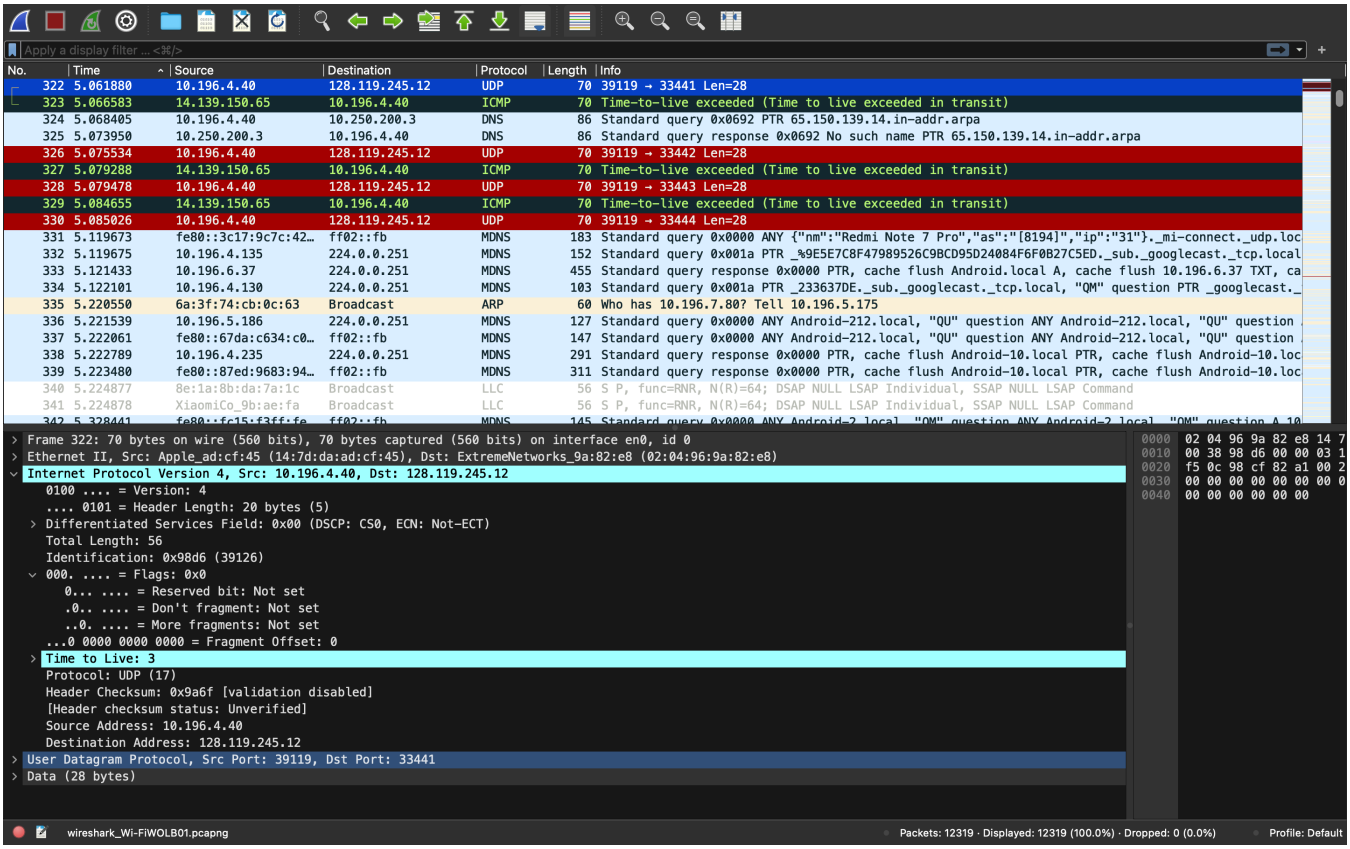
11. Are the values in the Identification fields (across the sequence of all of ICMP packets from all of the routers) similar in behavior to your answer to question 9 above?

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



1. 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 yes1!)

Yes, the result can be seen in the screenshot.

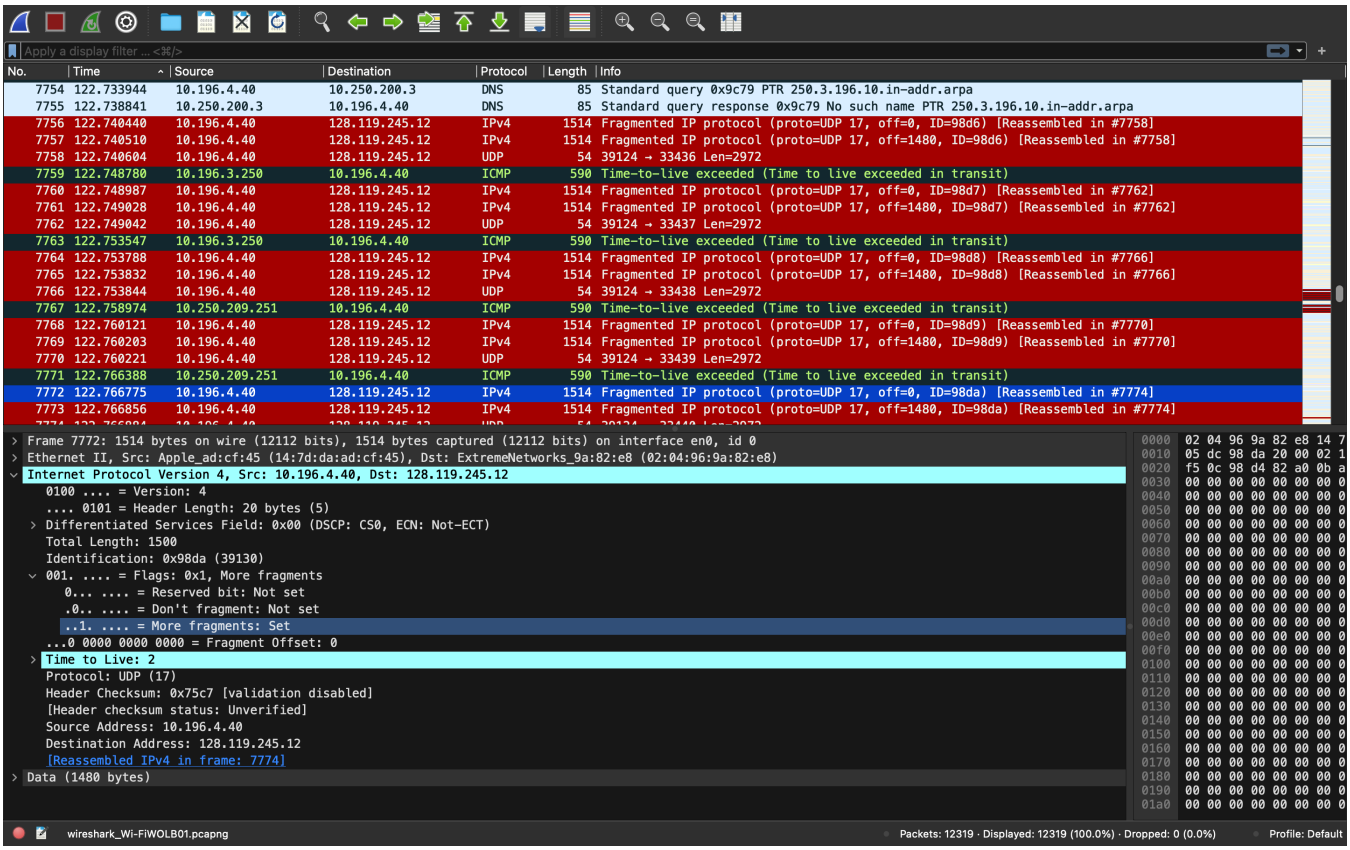


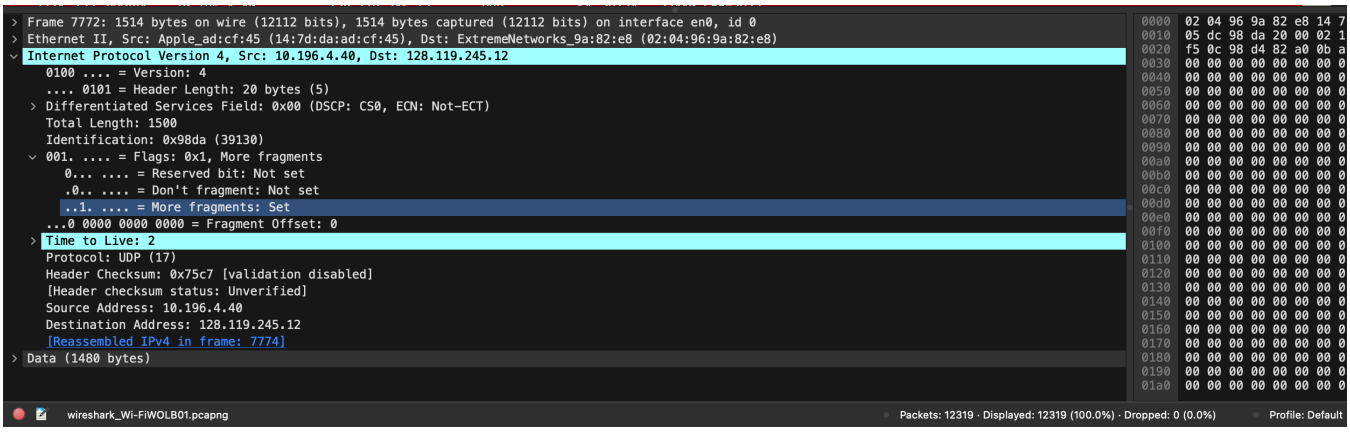
Figure 1: First fragment

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.



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?

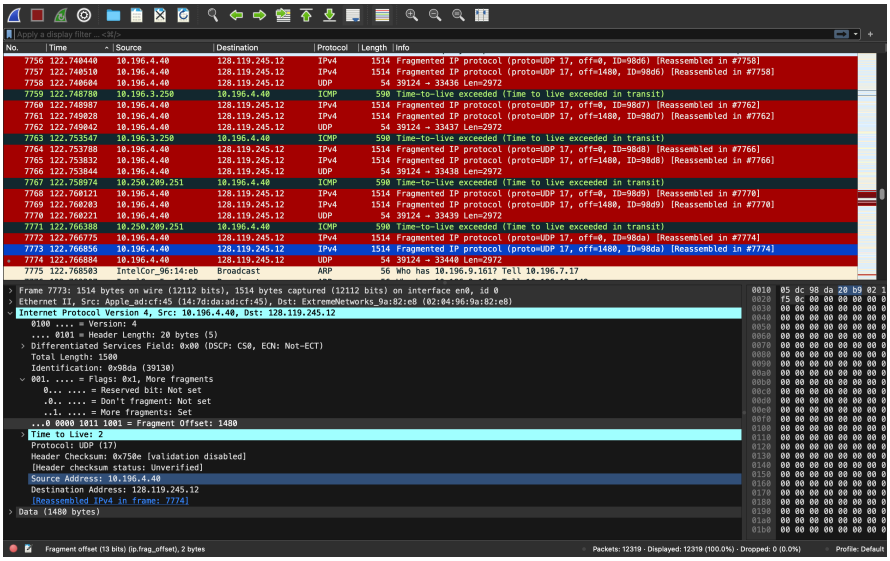


Figure 2: Second fragment

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?

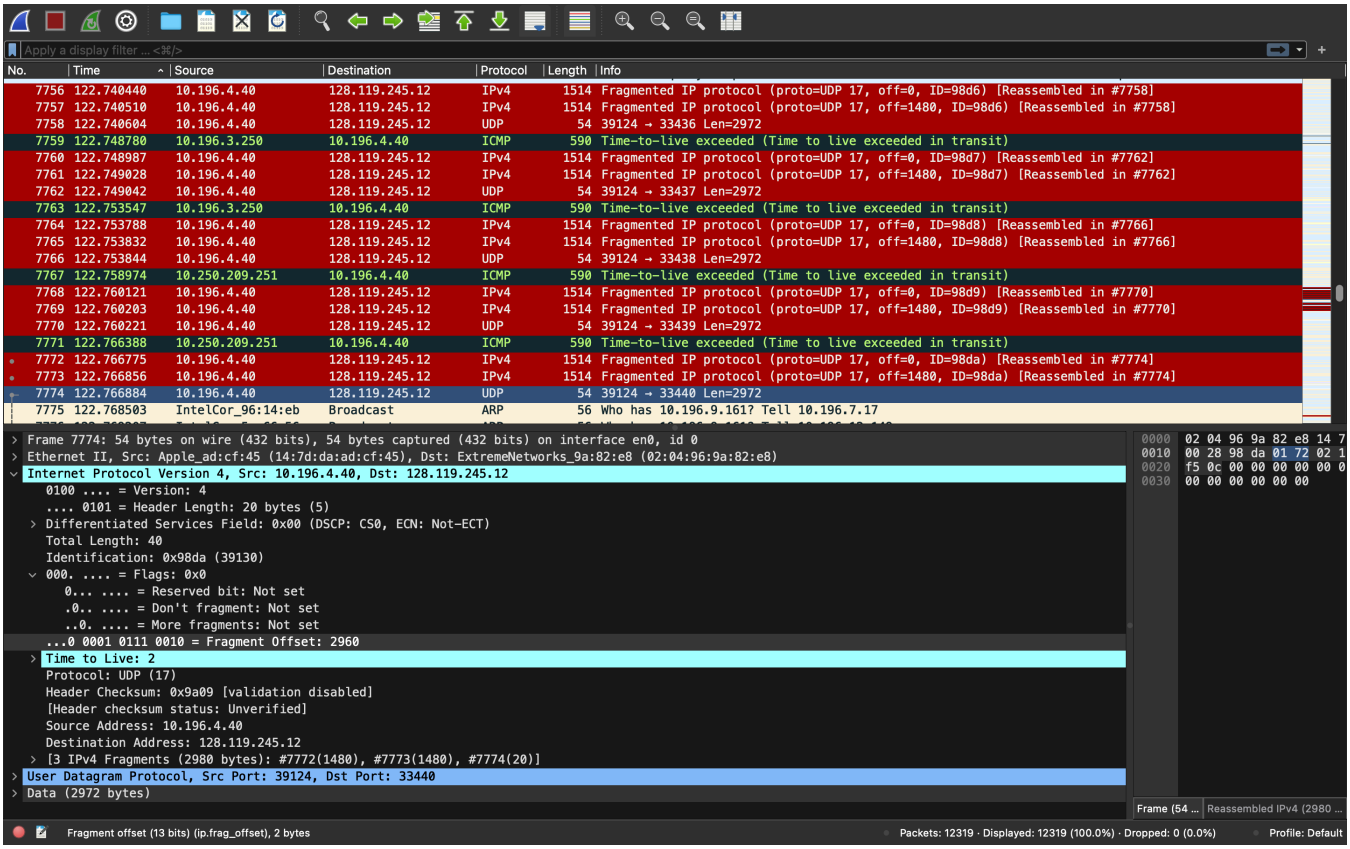
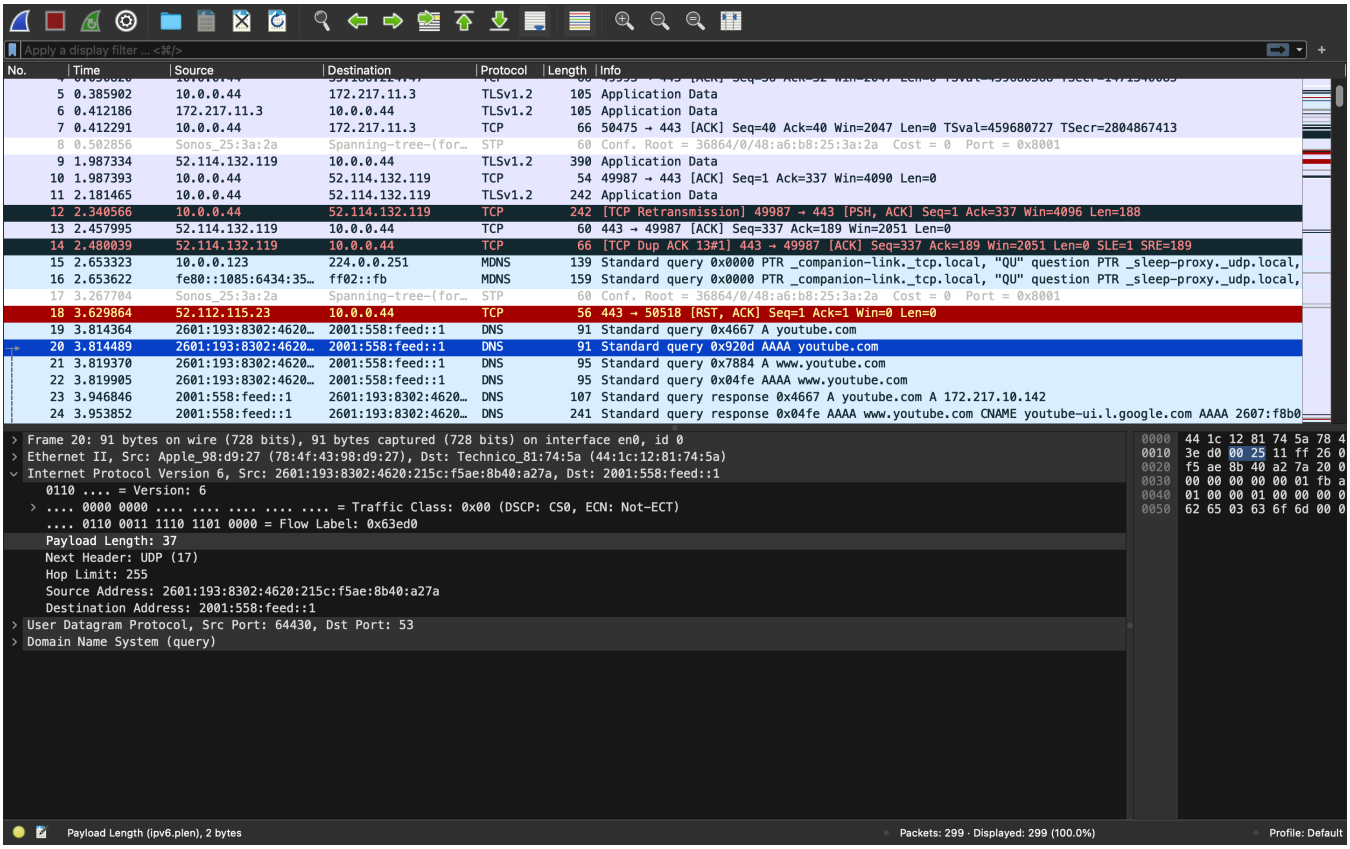


Figure 3: Second fragment

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

3 Part 3: IPv6



1. 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: 0x63ed0

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

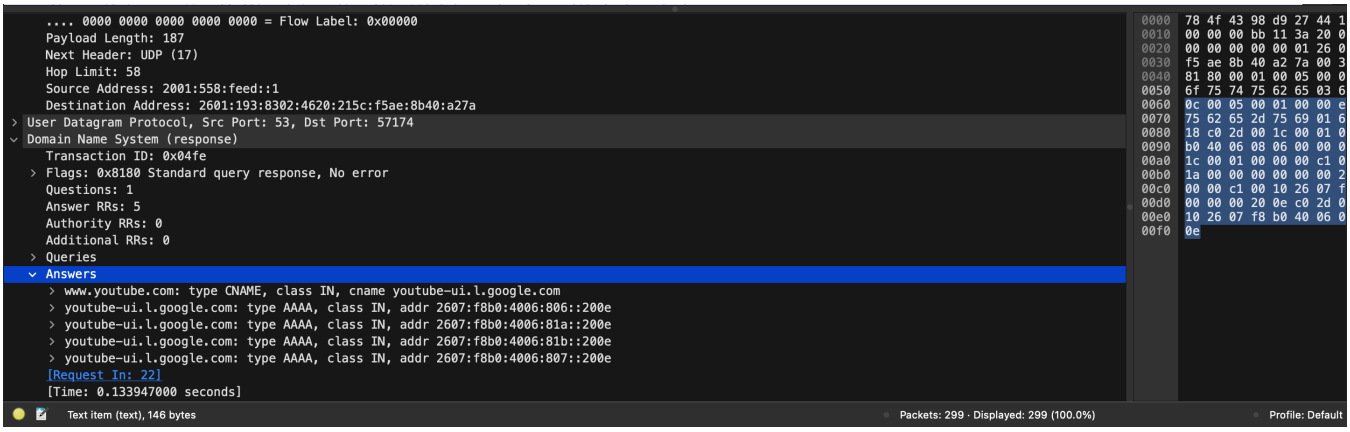
37 bytes of payload data is carried in this datagram.

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.



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