Wireshark Lab: IP

Yogesh P
201EE138

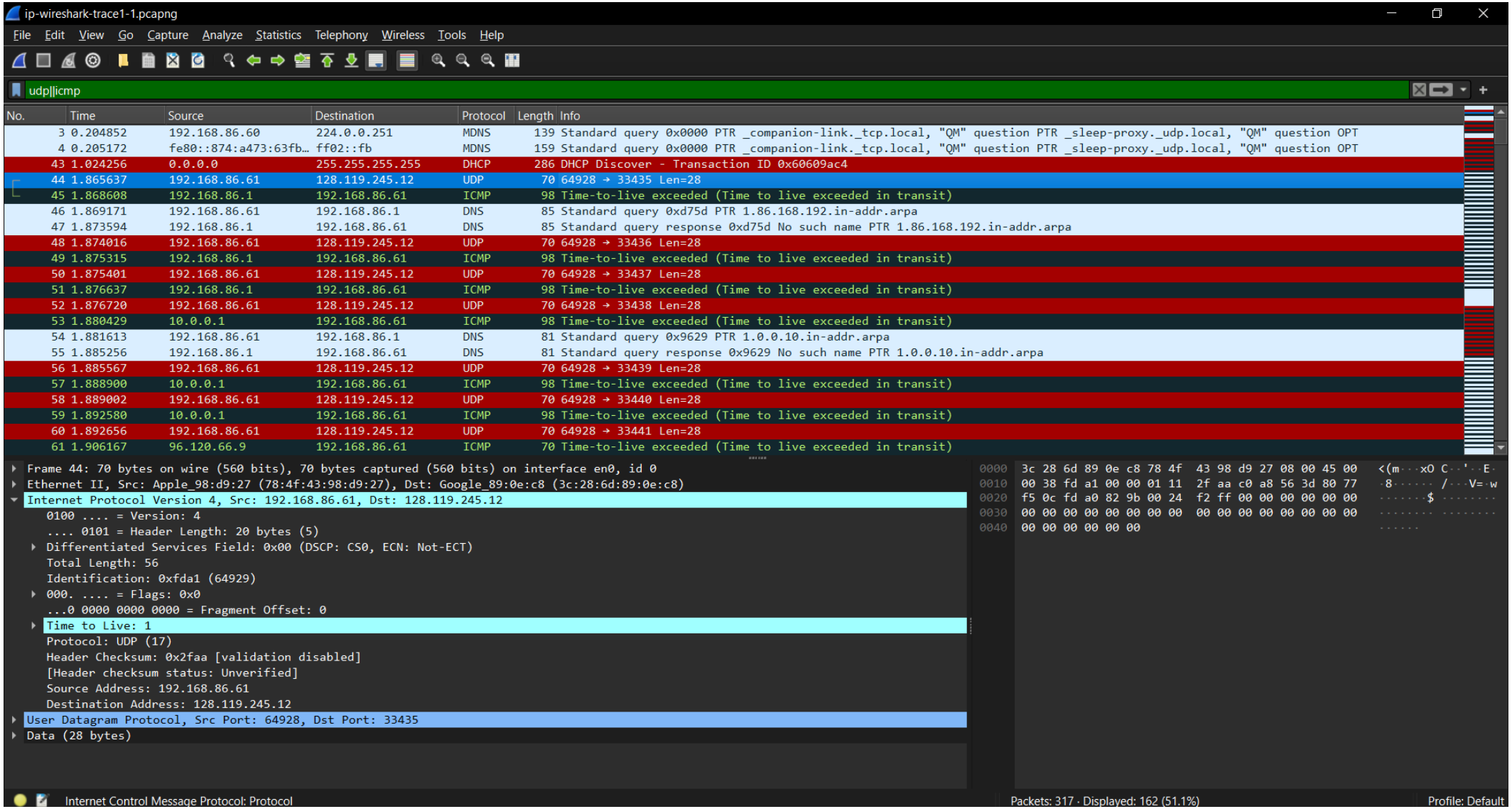

Figure 1 (first udp segment)

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 ipwireshark-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?
Ans: 192.168.86.61 is the IP address of the computer.

2. What is the value in the time-to-live (TTL) field in this IPv4 datagram's header?
Ans: The time to live is 1 second.

3. What is the value in the upper layer protocol field in this IPv4 datagram's header?
Ans: The value is UDP (17)

4. How many bytes are in the IP header?
Ans: 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.
Ans: There are 36 bytes in the payload of the IP datagram. This is obtained by subtracting the length of header from the total length of the datagram.

6. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.
Ans: The fragment offset has been set to 0 so the IP datagram has not been fragmented.

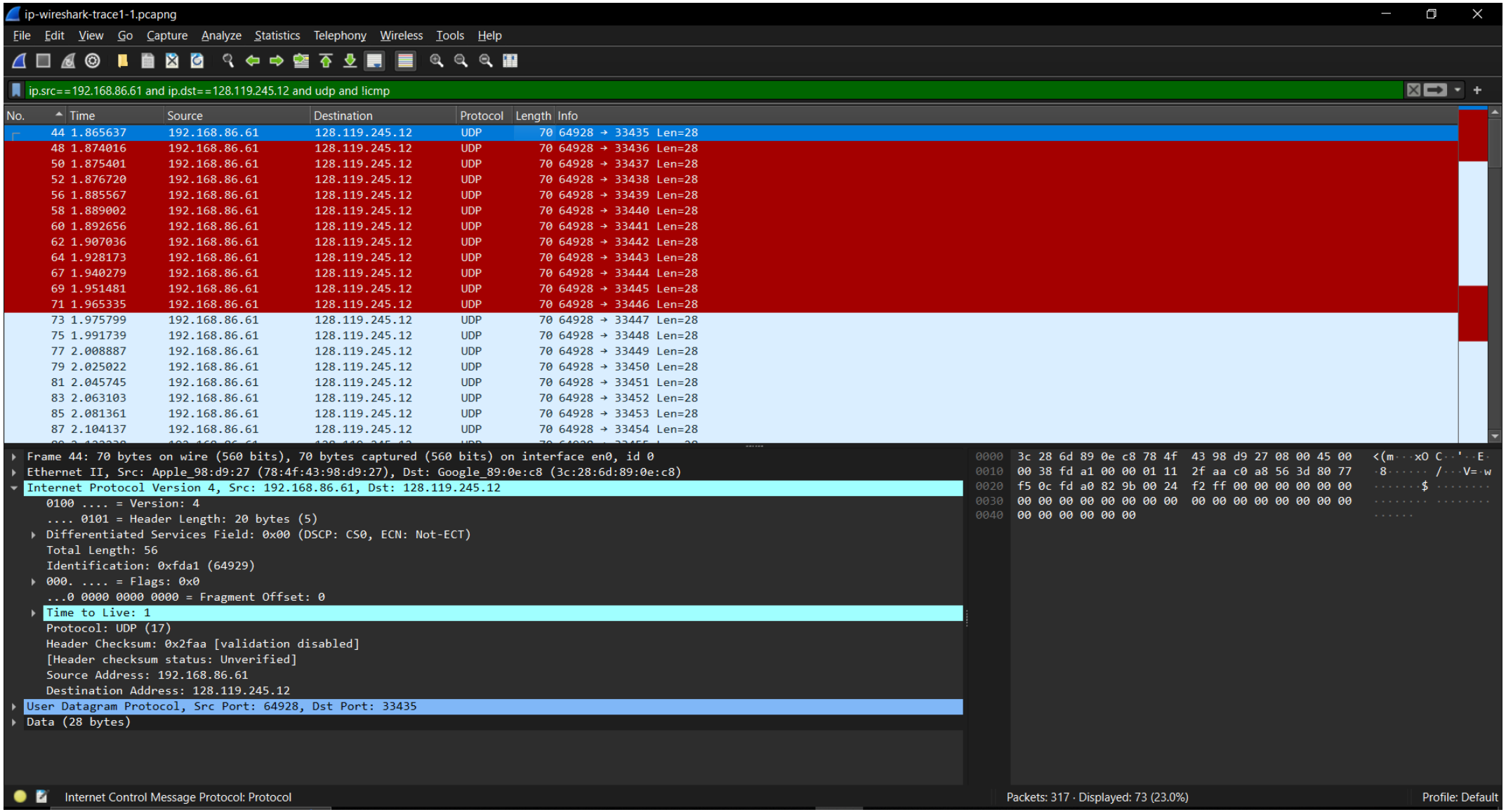

Figure 2 (packets with filter ip.src==192.168.86.61 and ip.dst==128.119.245.12 and udp and !icmp)

7. Which fields in the IP datagram always change from one datagram to the next within this series of UDP segments sent by your computer destined to 128.119.245.12, via traceroute? Why?
Ans: Checksum and Identification always change from one datagram to the next. The IP header checksum is recalculated for each datagram to ensure data integrity during transmission. The Identification field in the IP header is used for reassembling fragmented datagrams. It typically changes as different datagrams are sent.

8.Which fields in this sequence of IP datagrams (containing UDP segments) stay constant? Why?
Ans: The fields that tend to stay constant include:
Version: The version field in the IP header remains constant within a series of datagrams. It specifies the version of the IP protocol being used, such as IPv4 or IPv6.
Header Length: This field indicates the length of the IP header. Unless there are options present in the header, the header length remains constant within the same series of datagrams.

Type of Service (TOS)/Differentiated Services Code Point (DSCP): This field may remain constant if there's no requirement for Quality of Service (QoS) differentiation within the network.
Total Length: This field specifies the total length of the IP datagram, including both the header and the payload. If the payload size remains constant across the datagrams, this field will also remain constant.
Flags and Fragment Offset: If fragmentation is not occurring, these fields typically remain constant. If fragmentation is happening, the flags might change, but the fragment offset may remain constant within a series of related fragments.
Time to Live (TTL): If the datagrams are being sent from the same source, the TTL may remain constant unless there are significant changes in the network topology.
Protocol: This field in the IP header specifies the protocol used in the data portion of the IP datagram. Since the datagrams are all containing UDP segments, this field should remain constant as well.
Source IP Address: If all the datagrams are originating from the same source, the source IP address will remain constant.
Destination IP Address: If all the datagrams are destined for the same recipient, the destination IP address will remain constant.

9. Describe the pattern you see in the values in the Identification field of the IP datagrams being sent by your computer.
Ans: The identification field follows a sequential pattern incrementing by 1 for the next packet.

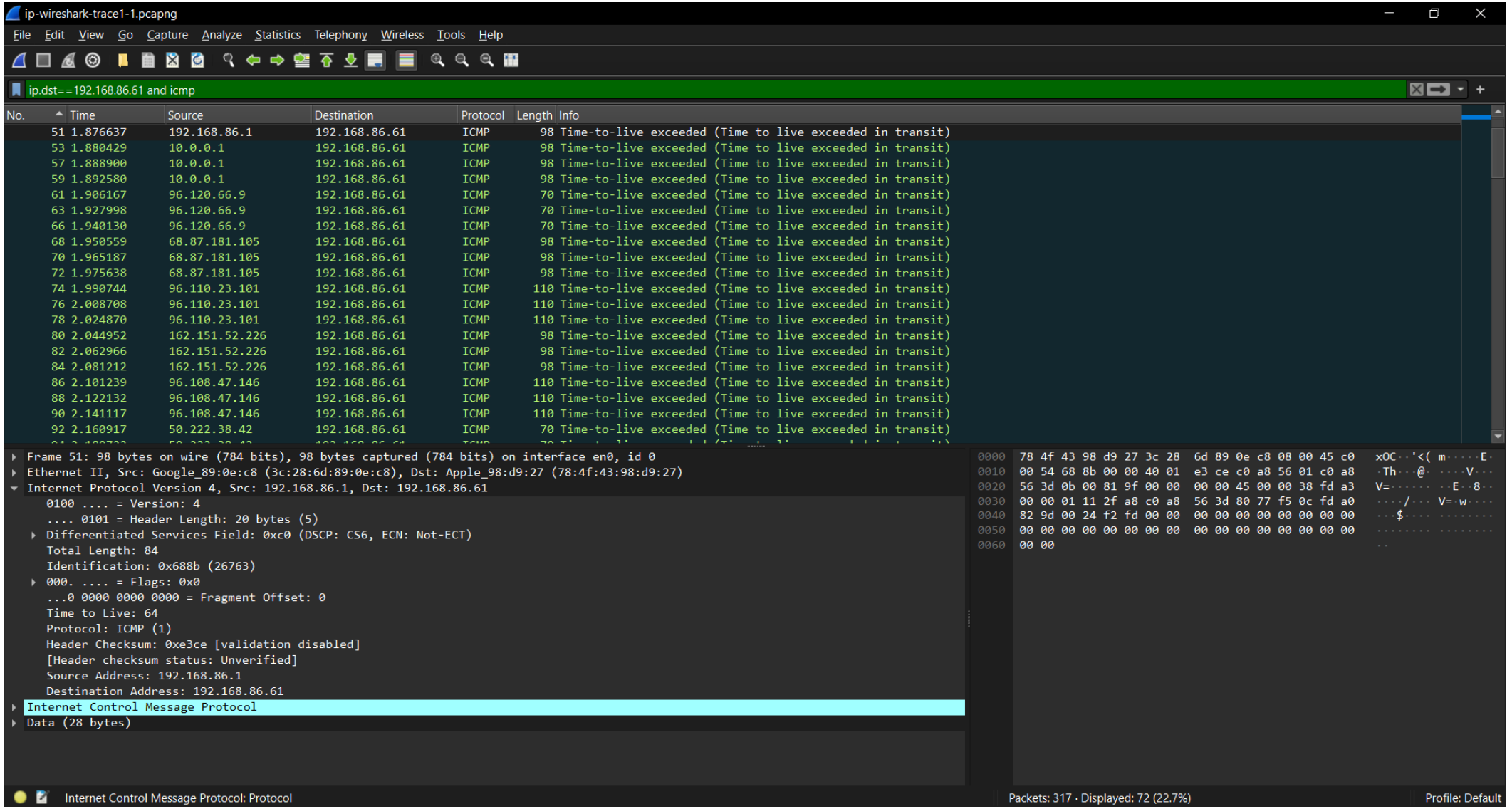

Figure 3 (Packets filtered as ip.dst==192.168.86.61 and icmp)

10. What is the upper layer protocol specified in the IP datagrams returned from the routers?
Ans: The protocol 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?
Ans: No there is no similarity in the behavior of the values in the identification fields.

12. Are the values of the TTL fields similar, across all of ICMP packets from all of the routers?
Ans: No they are not similar

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. Has that segment been fragmented across more than one IP datagram?
Ans: Yes

14. What information in the IP header indicates that this datagram been fragmented?
Ans: As seen in Figure 4 it says that this IP is reassembled in frame 181 indicating it has been fragmented.

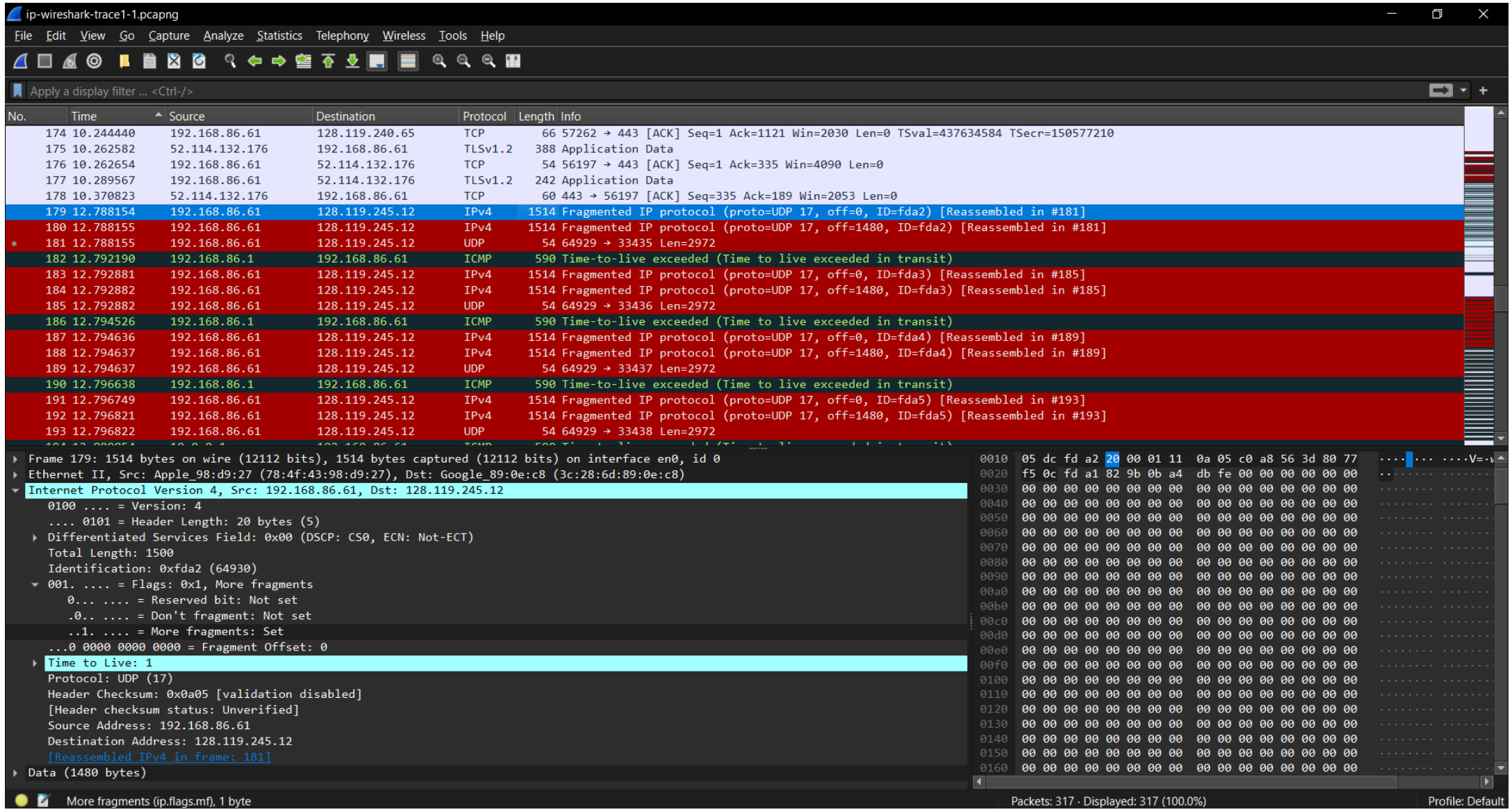

Figure 4(Fragmented IP first fragment)

15. What information in the IP header for this packet indicates whether this is the first fragment versus a latter fragment?
Ans: This packet has More Fragments set and the fragment offset set to 0 indicating that this is the first fragment.

16. How many bytes are there in is this IP datagram (header plus payload)?
Ans: The total length is the number of bytes in this datagram which is 1500 bytes.

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?
Ans: This packet has More Fragments set and the fragment offset set to a value(1480) indicating that this is not the first fragment.

18. What fields change in the IP header between the first and second fragment?
Ans: The fragment offset and the checksum are different between first and second.

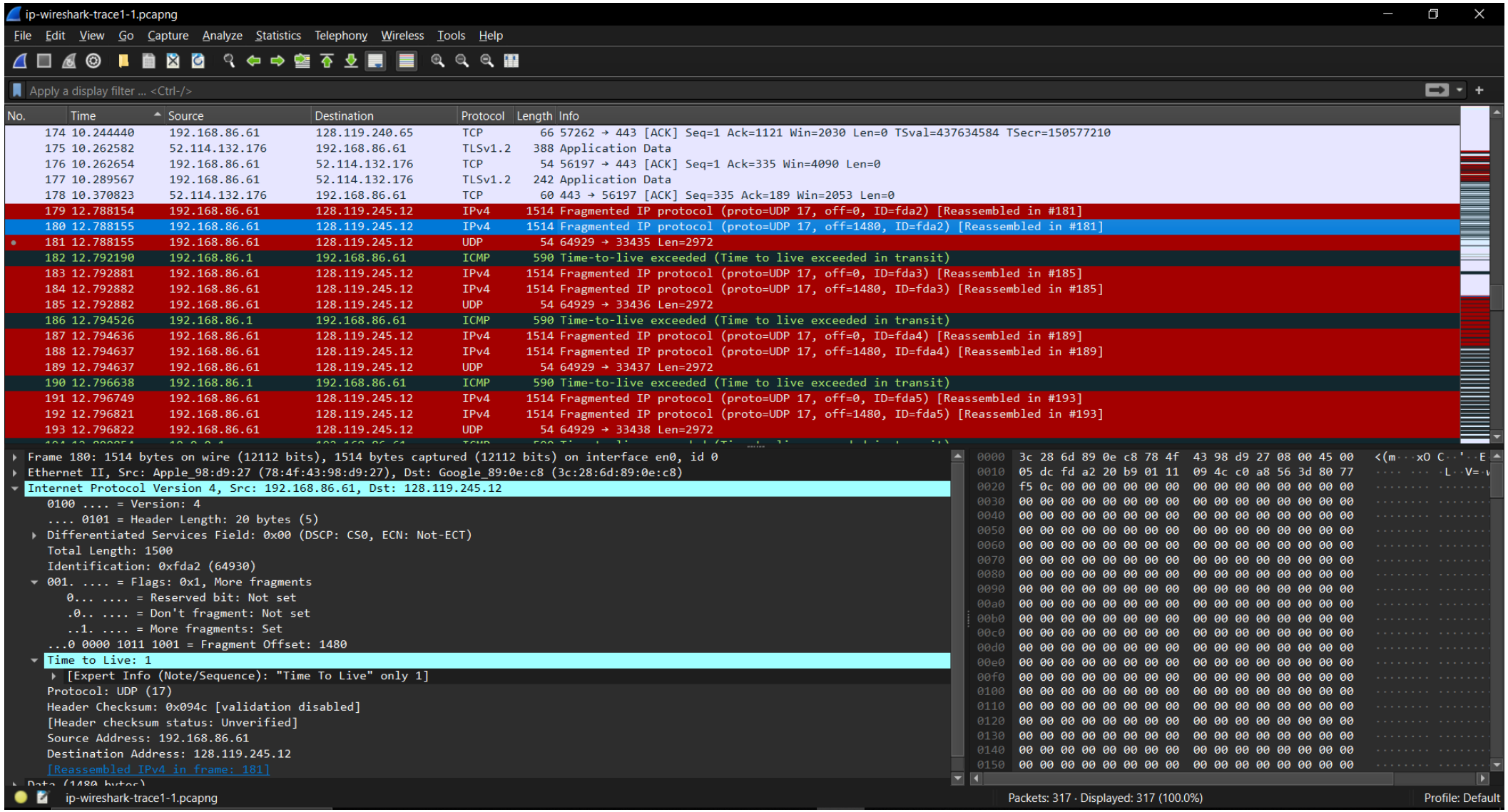

Figure 5 (Second Fragment)

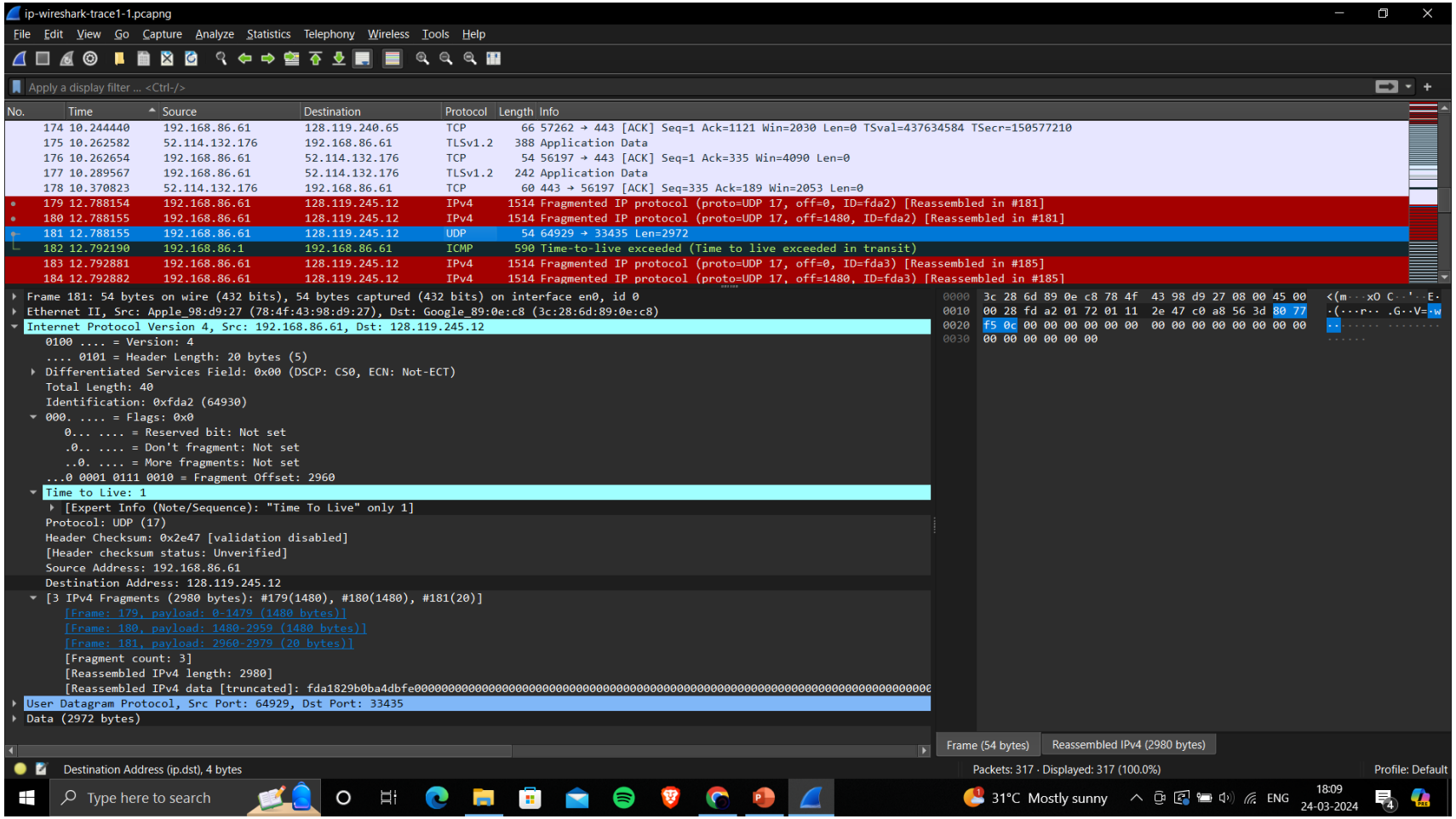

Figure 6(final fragment)

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?

Ans: The More Fragments field is not set indicating this is the final fragment.

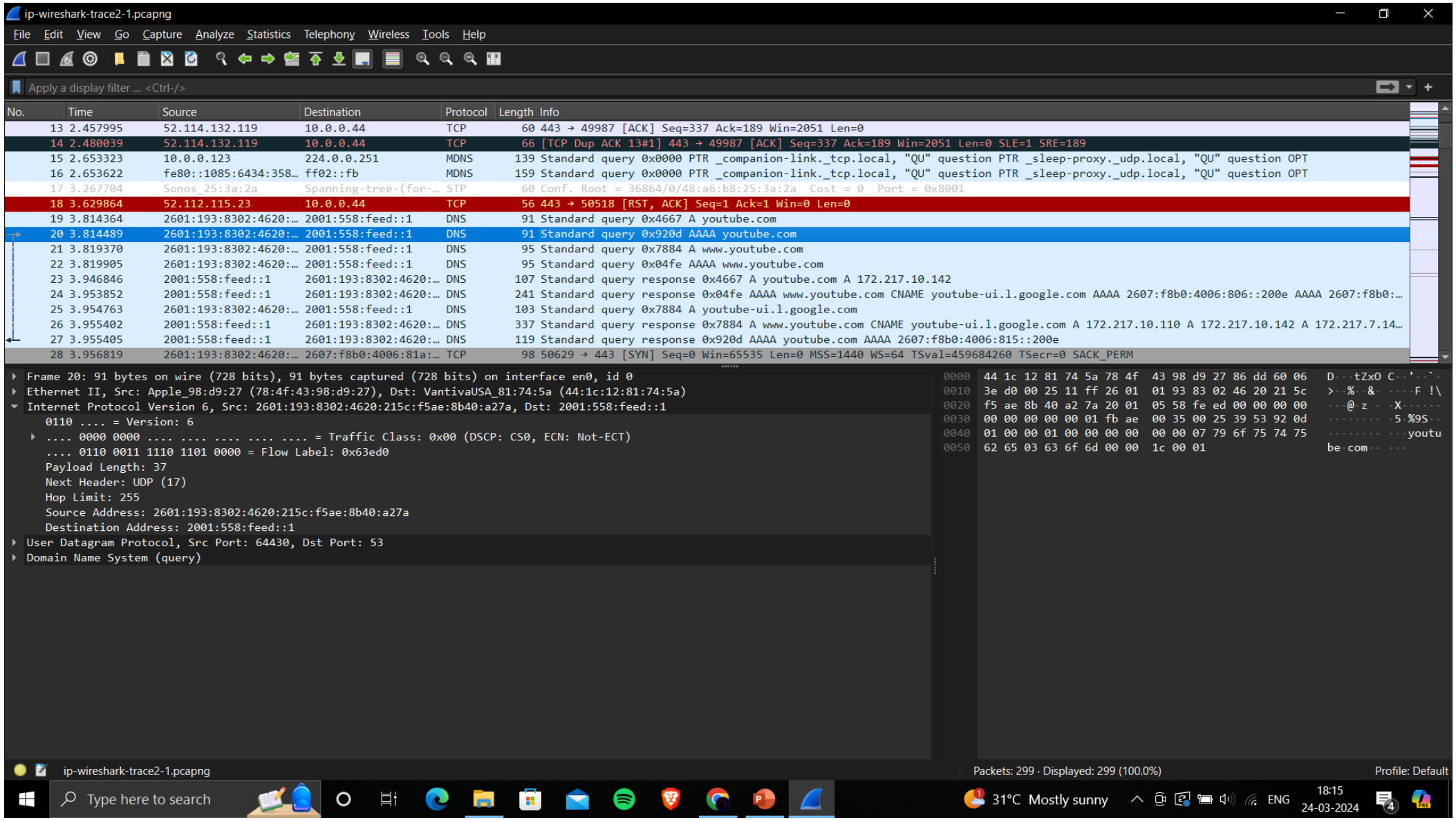

Figure 7(IPv6)

20. What is the IPv6 address of the computer making the DNS AAAA request?
Ans: 2601:193:8302:4620:215c:f5ae:8b40:a27a

21. What is the IPv6 destination address for this datagram?
Ans: 2001:558:feed::1

22. What is the value of the flow label for this datagram?
Ans: 0x63ed0

23. How much payload data is carried in this datagram?
Ans: 37 bytes

24. What is the upper layer protocol to which this datagram's payload will be delivered at the destination?
Ans: UDP (17)

25. How many IPv6 addresses are returned in the response to this AAAA request
Ans: One IPv6 address is returned in the response.

26. What is the first of the IPv6 addresses returned by the DNS for youtube.com
Ans: 2607:f8b0:4006:815::200e

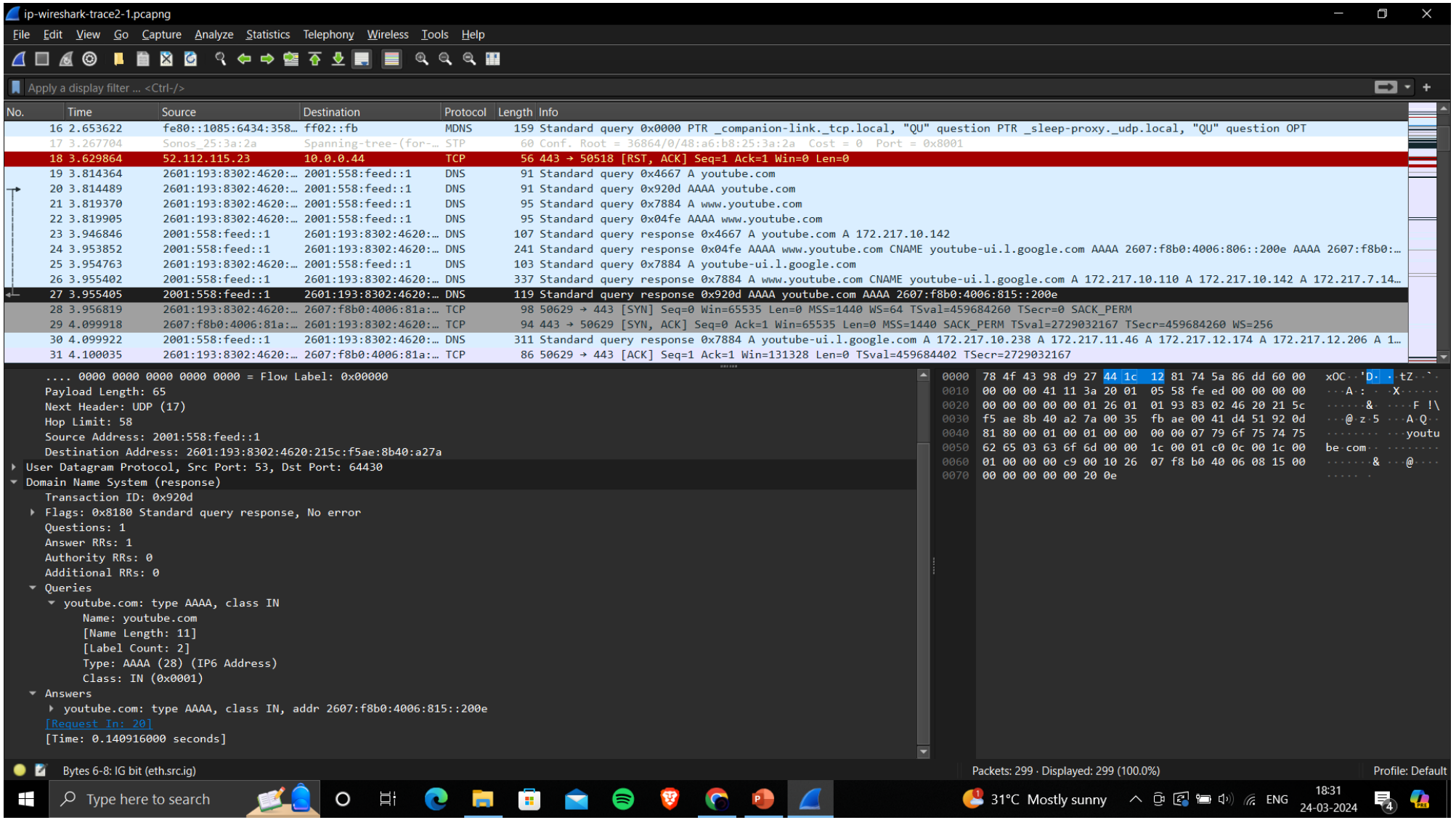

Figure 8(IPv6 Response)