

Wireshark Lab: IP

Yogesh P
201EE138

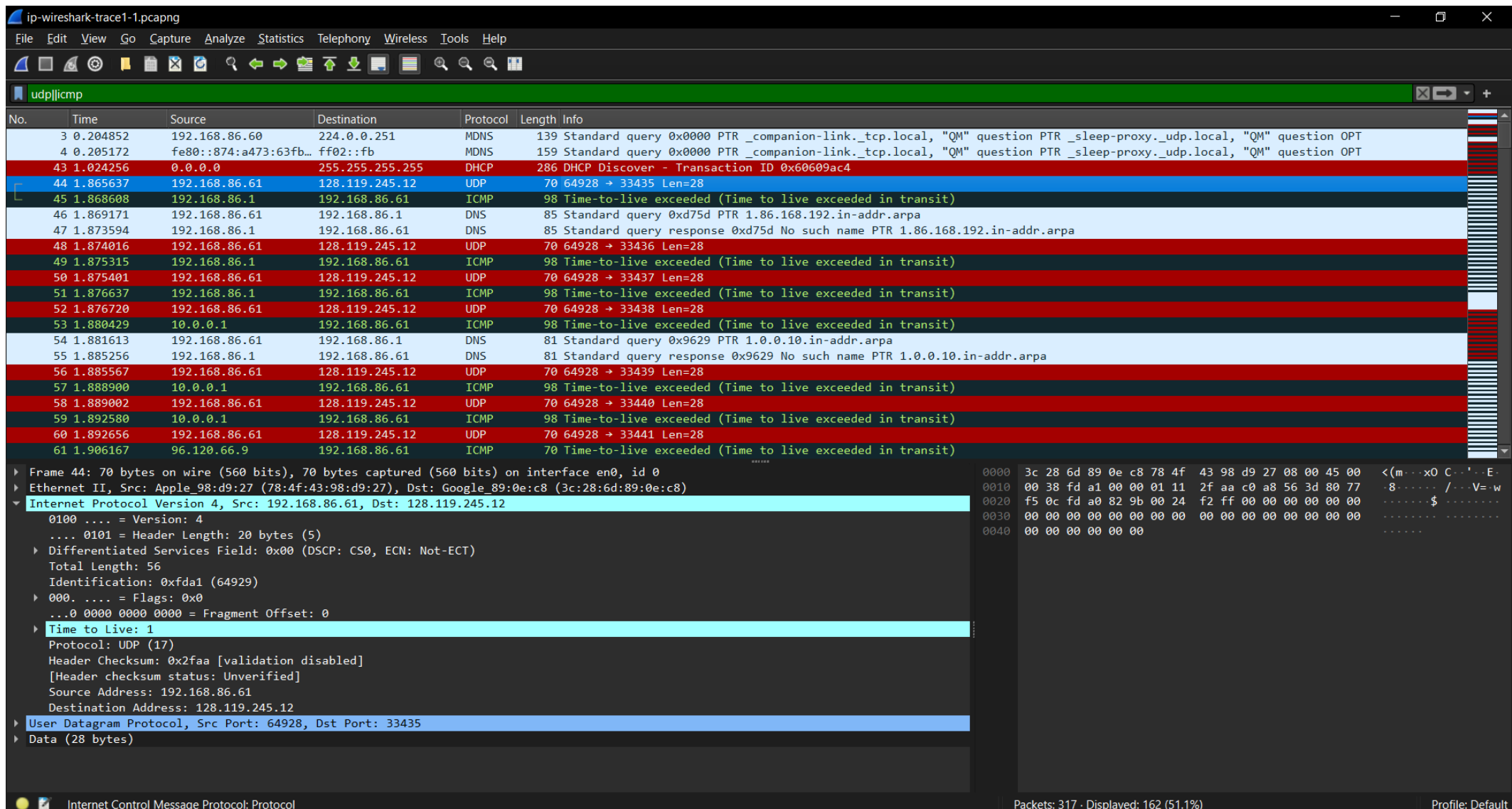


Figure 1 (first udp segment)

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.

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 | 1.865637 | 192.168.86.61 | 128.119.245.12 | UDP | 70 | 64928 → 33435 Len=28 |
| 48 | 1.874016 | 192.168.86.61 | 128.119.245.12 | UDP | 70 | 64928 → 33436 Len=28 |
| 50 | 1.875401 | 192.168.86.61 | 128.119.245.12 | UDP | 70 | 64928 → 33437 Len=28 |
| 52 | 1.876720 | 192.168.86.61 | 128.119.245.12 | UDP | 70 | 64928 → 33438 Len=28 |
| 56 | 1.885567 | 192.168.86.61 | 128.119.245.12 | UDP | 70 | 64928 → 33439 Len=28 |
| 58 | 1.889002 | 192.168.86.61 | 128.119.245.12 | UDP | 70 | 64928 → 33440 Len=28 |
| 60 | 1.892656 | 192.168.86.61 | 128.119.245.12 | UDP | 70 | 64928 → 33441 Len=28 |
| 62 | 1.907036 | 192.168.86.61 | 128.119.245.12 | UDP | 70 | 64928 → 33442 Len=28 |
| 64 | 1.928173 | 192.168.86.61 | 128.119.245.12 | UDP | 70 | 64928 → 33443 Len=28 |
| 67 | 1.940279 | 192.168.86.61 | 128.119.245.12 | UDP | 70 | 64928 → 33444 Len=28 |
| 69 | 1.951481 | 192.168.86.61 | 128.119.245.12 | UDP | 70 | 64928 → 33445 Len=28 |
| 71 | 1.965335 | 192.168.86.61 | 128.119.245.12 | UDP | 70 | 64928 → 33446 Len=28 |
| 73 | 1.975799 | 192.168.86.61 | 128.119.245.12 | UDP | 70 | 64928 → 33447 Len=28 |
| 75 | 1.991739 | 192.168.86.61 | 128.119.245.12 | UDP | 70 | 64928 → 33448 Len=28 |
| 77 | 2.008887 | 192.168.86.61 | 128.119.245.12 | UDP | 70 | 64928 → 33449 Len=28 |
| 79 | 2.025022 | 192.168.86.61 | 128.119.245.12 | UDP | 70 | 64928 → 33450 Len=28 |
| 81 | 2.045745 | 192.168.86.61 | 128.119.245.12 | UDP | 70 | 64928 → 33451 Len=28 |
| 83 | 2.063103 | 192.168.86.61 | 128.119.245.12 | UDP | 70 | 64928 → 33452 Len=28 |
| 85 | 2.081361 | 192.168.86.61 | 128.119.245.12 | UDP | 70 | 64928 → 33453 Len=28 |
| 87 | 2.104137 | 192.168.86.61 | 128.119.245.12 | UDP | 70 | 64928 → 33454 Len=28 |

Frame 44: 70 bytes on wire (560 bits), 70 bytes captured (560 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)

Internet Protocol Version 4, Src: 192.168.86.61, Dst: 128.119.245.12

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 56
- Identification: 0xfda1 (64929)
- 000. = Flags: 0x0
- ...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 43 98 d9 27 08 00 45 00 <(m...xO C...E.

0010 00 38 fd a1 00 00 01 11 2f aa c0 a8 56 3d 80 77 .8...../...V=w

0020 f5 0c fd a0 82 9b 00 24 f2 ff 00 00 00 00 00 00\$.....

0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00\$.....

0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00\$.....

Internet Control Message Protocol: Protocol

Packets: 317 · Displayed: 73 (23.0%) Profile: Default

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.

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 |
|-----|----------|----------------|---------------|----------|--------|--|
| 51 | 1.876637 | 192.168.86.1 | 192.168.86.61 | ICMP | 98 | Time-to-live exceeded (Time to live exceeded in transit) |
| 53 | 1.880429 | 10.0.0.1 | 192.168.86.61 | ICMP | 98 | Time-to-live exceeded (Time to live exceeded in transit) |
| 57 | 1.888900 | 10.0.0.1 | 192.168.86.61 | ICMP | 98 | Time-to-live exceeded (Time to live exceeded in transit) |
| 59 | 1.892580 | 10.0.0.1 | 192.168.86.61 | ICMP | 98 | Time-to-live exceeded (Time to live exceeded in transit) |
| 61 | 1.906167 | 96.120.66.9 | 192.168.86.61 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 63 | 1.927998 | 96.120.66.9 | 192.168.86.61 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 66 | 1.940130 | 96.120.66.9 | 192.168.86.61 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 68 | 1.950559 | 68.87.181.105 | 192.168.86.61 | ICMP | 98 | Time-to-live exceeded (Time to live exceeded in transit) |
| 70 | 1.965187 | 68.87.181.105 | 192.168.86.61 | ICMP | 98 | Time-to-live exceeded (Time to live exceeded in transit) |
| 72 | 1.975638 | 68.87.181.105 | 192.168.86.61 | ICMP | 98 | Time-to-live exceeded (Time to live exceeded in transit) |
| 74 | 1.990744 | 96.110.23.101 | 192.168.86.61 | ICMP | 110 | Time-to-live exceeded (Time to live exceeded in transit) |
| 76 | 2.008708 | 96.110.23.101 | 192.168.86.61 | ICMP | 110 | Time-to-live exceeded (Time to live exceeded in transit) |
| 78 | 2.024870 | 96.110.23.101 | 192.168.86.61 | ICMP | 110 | Time-to-live exceeded (Time to live exceeded in transit) |
| 80 | 2.044952 | 162.151.52.226 | 192.168.86.61 | ICMP | 98 | Time-to-live exceeded (Time to live exceeded in transit) |
| 82 | 2.062966 | 162.151.52.226 | 192.168.86.61 | ICMP | 98 | Time-to-live exceeded (Time to live exceeded in transit) |
| 84 | 2.081212 | 162.151.52.226 | 192.168.86.61 | ICMP | 98 | Time-to-live exceeded (Time to live exceeded in transit) |
| 86 | 2.101239 | 96.108.47.146 | 192.168.86.61 | ICMP | 110 | Time-to-live exceeded (Time to live exceeded in transit) |
| 88 | 2.122132 | 96.108.47.146 | 192.168.86.61 | ICMP | 110 | Time-to-live exceeded (Time to live exceeded in transit) |
| 90 | 2.141117 | 96.108.47.146 | 192.168.86.61 | ICMP | 110 | Time-to-live exceeded (Time to live exceeded in transit) |
| 92 | 2.160917 | 50.222.38.42 | 192.168.86.61 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |

Frame 51: 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)

Internet Protocol Version 4, Src: 192.168.86.1, Dst: 192.168.86.61

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
- Total Length: 84
- Identification: 0x688b (26763)
- 000. = Flags: 0x0
- ...0 0000 0000 = Fragment Offset: 0
- Time to Live: 64
- Protocol: ICMP (1)
- Header Checksum: 0xe3ce [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 192.168.86.1
- Destination Address: 192.168.86.61
- Internet Control Message Protocol
- Data (28 bytes)

0000 78 4f 43 98 d9 27 3c 28 6d 89 0e c8 08 00 45 c0 xOC...'<(m....E

0010 00 54 68 8b 00 00 40 01 e3 ce c0 a8 56 01 c0 a8 .Th..@.V..

0020 56 3d 0b 00 81 9f 00 00 00 00 45 00 00 38 fd a3 V=.....E. 8..

0030 00 00 01 11 2f a8 c0 a8 56 3d 80 77 f5 0c fd a0//...V=.w...

0040 82 9d 00 24 f2 fd 00 00 00 00 00 00 00 00 00 ..\$.

0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0060 00 00 ..

Internet Control Message Protocol: Protocol

Packets: 317 · Displayed: 72 (22.7%) Profile: Default

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.

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 |
|-----|-----------|----------------|----------------|----------|--------|---|
| 174 | 10.244440 | 192.168.86.61 | 128.119.240.65 | TCP | 66 | 57262 → 443 [ACK] Seq=1 Ack=1121 Win=2030 Len=0 TSval=437634584 TSecr=150577210 |
| 175 | 10.262582 | 52.114.132.176 | 192.168.86.61 | TLSv1.2 | 388 | Application Data |
| 176 | 10.262654 | 192.168.86.61 | 52.114.132.176 | TCP | 54 | 56197 → 443 [ACK] Seq=1 Ack=335 Win=4090 Len=0 |
| 177 | 10.289567 | 192.168.86.61 | 52.114.132.176 | TLSv1.2 | 242 | Application Data |
| 178 | 10.370823 | 52.114.132.176 | 192.168.86.61 | TCP | 60 | 443 → 56197 [ACK] Seq=335 Ack=189 Win=2053 Len=0 |
| 179 | 12.788154 | 192.168.86.61 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=UDP 17, off=0, ID=fda2) [Reassembled in #181] |
| 180 | 12.788155 | 192.168.86.61 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda2) [Reassembled in #181] |
| 181 | 12.788155 | 192.168.86.61 | 128.119.245.12 | UDP | 54 | 64929 → 33435 Len=2972 |
| 182 | 12.792190 | 192.168.86.1 | 192.168.86.61 | ICMP | 590 | Time-to-live exceeded (Time to live exceeded in transit) |
| 183 | 12.792881 | 192.168.86.61 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=UDP 17, off=0, ID=fda3) [Reassembled in #185] |
| 184 | 12.792882 | 192.168.86.61 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda3) [Reassembled in #185] |
| 185 | 12.792882 | 192.168.86.61 | 128.119.245.12 | UDP | 54 | 64929 → 33436 Len=2972 |
| 186 | 12.794526 | 192.168.86.1 | 192.168.86.61 | ICMP | 590 | Time-to-live exceeded (Time to live exceeded in transit) |
| 187 | 12.794636 | 192.168.86.61 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=UDP 17, off=0, ID=fda4) [Reassembled in #189] |
| 188 | 12.794637 | 192.168.86.61 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda4) [Reassembled in #189] |
| 189 | 12.794637 | 192.168.86.61 | 128.119.245.12 | UDP | 54 | 64929 → 33437 Len=2972 |
| 190 | 12.796638 | 192.168.86.1 | 192.168.86.61 | ICMP | 590 | Time-to-live exceeded (Time to live exceeded in transit) |
| 191 | 12.796749 | 192.168.86.61 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=UDP 17, off=0, ID=fda5) [Reassembled in #193] |
| 192 | 12.796821 | 192.168.86.61 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda5) [Reassembled in #193] |
| 193 | 12.796822 | 192.168.86.61 | 128.119.245.12 | UDP | 54 | 64929 → 33438 Len=2972 |

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)

Internet Protocol Version 4, Src: 192.168.86.61, Dst: 128.119.245.12

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 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]
 - Source Address: 192.168.86.61
 - Destination Address: 128.119.245.12
 - [Reassembled IPv4 in frame: 181]

Data (1480 bytes)

More fragments (ip.flags.mf), 1 byte

Packets: 317 · Displayed: 317 (100.0%) Profile: Default

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.

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 |
|-----|-----------|----------------|----------------|----------|--------|---|
| 174 | 10.244440 | 192.168.86.61 | 128.119.240.65 | TCP | 66 | 57262 → 443 [ACK] Seq=1 Ack=1121 Win=2030 Len=0 TSval=437634584 TSecr=150577210 |
| 175 | 10.262582 | 52.114.132.176 | 192.168.86.61 | TLSv1.2 | 388 | Application Data |
| 176 | 10.262654 | 192.168.86.61 | 52.114.132.176 | TCP | 54 | 56197 → 443 [ACK] Seq=1 Ack=335 Win=4090 Len=0 |
| 177 | 10.289567 | 192.168.86.61 | 52.114.132.176 | TLSv1.2 | 242 | Application Data |
| 178 | 10.370823 | 52.114.132.176 | 192.168.86.61 | TCP | 60 | 443 → 56197 [ACK] Seq=335 Ack=189 Win=2053 Len=0 |
| 179 | 12.788154 | 192.168.86.61 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=UDP 17, off=0, ID=fda2) [Reassembled in #181] |
| 180 | 12.788155 | 192.168.86.61 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda2) [Reassembled in #181] |
| 181 | 12.788155 | 192.168.86.61 | 128.119.245.12 | UDP | 54 | 64929 → 33435 Len=2972 |
| 182 | 12.792190 | 192.168.86.61 | 192.168.86.61 | ICMP | 590 | Time-to-live exceeded (Time to live exceeded in transit) |
| 183 | 12.792881 | 192.168.86.61 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=UDP 17, off=0, ID=fda3) [Reassembled in #185] |
| 184 | 12.792882 | 192.168.86.61 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda3) [Reassembled in #185] |
| 185 | 12.792882 | 192.168.86.61 | 128.119.245.12 | UDP | 54 | 64929 → 33436 Len=2972 |
| 186 | 12.794526 | 192.168.86.61 | 192.168.86.61 | ICMP | 590 | Time-to-live exceeded (Time to live exceeded in transit) |
| 187 | 12.794636 | 192.168.86.61 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=UDP 17, off=0, ID=fda4) [Reassembled in #189] |
| 188 | 12.794637 | 192.168.86.61 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda4) [Reassembled in #189] |
| 189 | 12.794637 | 192.168.86.61 | 128.119.245.12 | UDP | 54 | 64929 → 33437 Len=2972 |
| 190 | 12.796638 | 192.168.86.61 | 192.168.86.61 | ICMP | 590 | Time-to-live exceeded (Time to live exceeded in transit) |
| 191 | 12.796749 | 192.168.86.61 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=UDP 17, off=0, ID=fda5) [Reassembled in #193] |
| 192 | 12.796821 | 192.168.86.61 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=UDP 17, off=1480, ID=fda5) [Reassembled in #193] |
| 193 | 12.796822 | 192.168.86.61 | 128.119.245.12 | UDP | 54 | 64929 → 33438 Len=2972 |

Frame 180: 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)

Internet Protocol Version 4, Src: 192.168.86.61, Dst: 128.119.245.12

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 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
- [Expert Info (Note/Sequence): "Time To Live" only 1]
- Protocol: UDP (17)
- Header Checksum: 0x094c [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 192.168.86.61
- Destination Address: 128.119.245.12
- [Reassembled IPv4 in frame: 181]

0000 3c 28 6d 89 0e c8 78 4f 43 98 d9 27 08 00 45 00 <(m...xO C...E

0010 05 dc fd a2 20 b9 01 11 09 4c c0 a8 56 3d 80 77 <... ..L..V=

0020 f5 0c 00 00 00 00 00 00 00 00 00 00 00 00 00

0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Packets: 317 · Displayed: 317 (100.0%) Profile: Default

Figure 5 (Second Fragment)

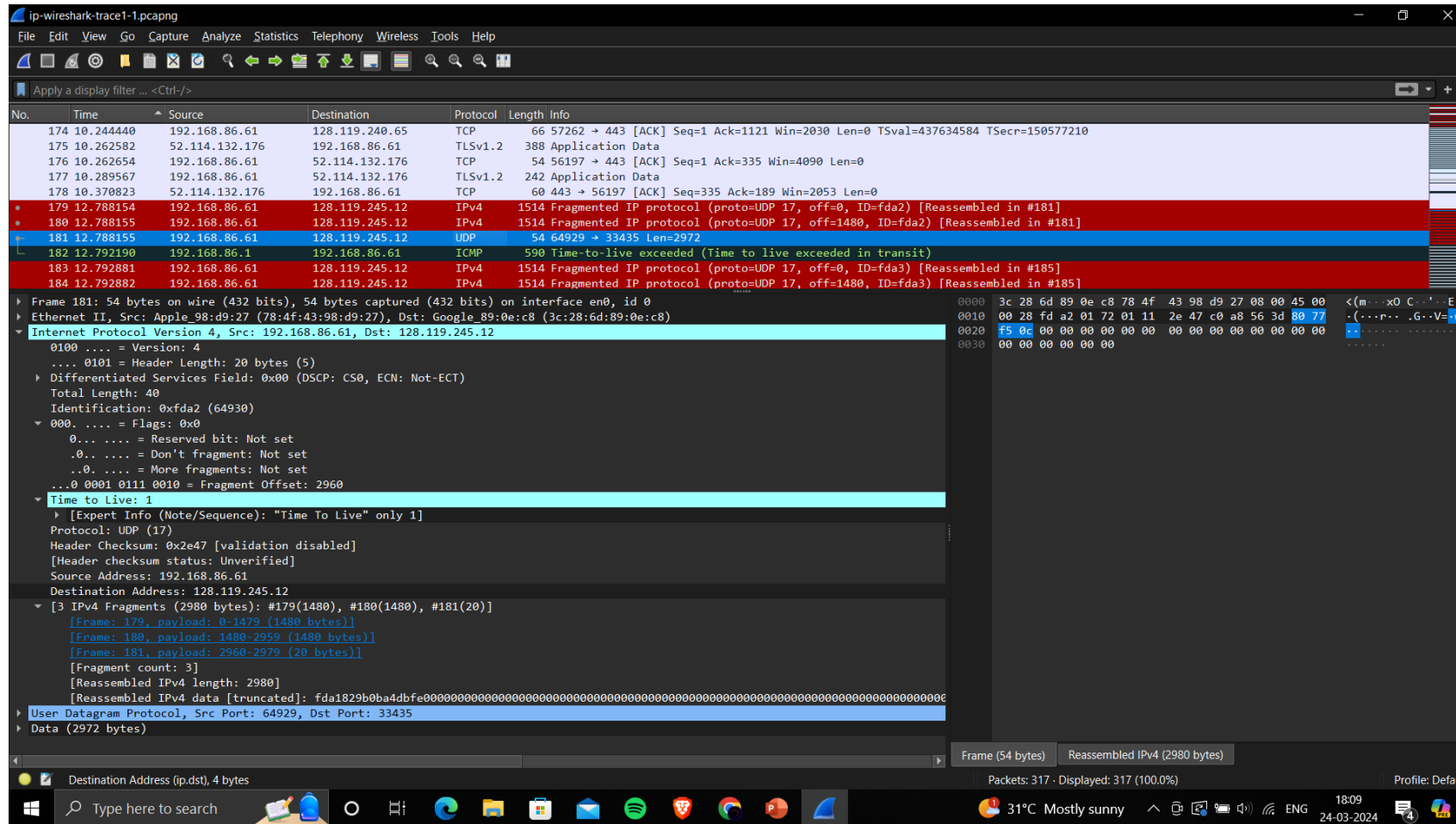


Figure 6(final fragment)

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.

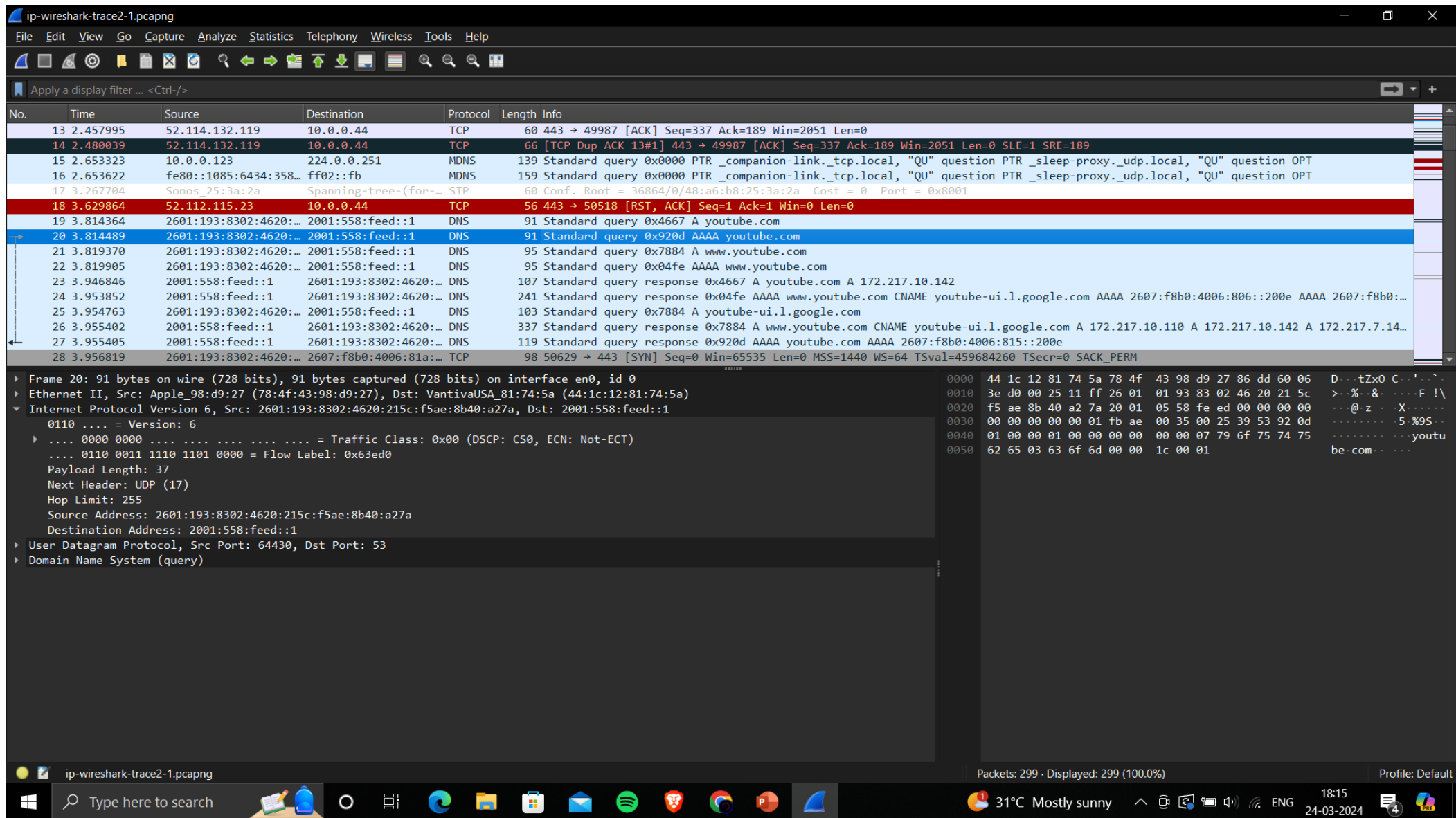


Figure 7(IPv6)

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

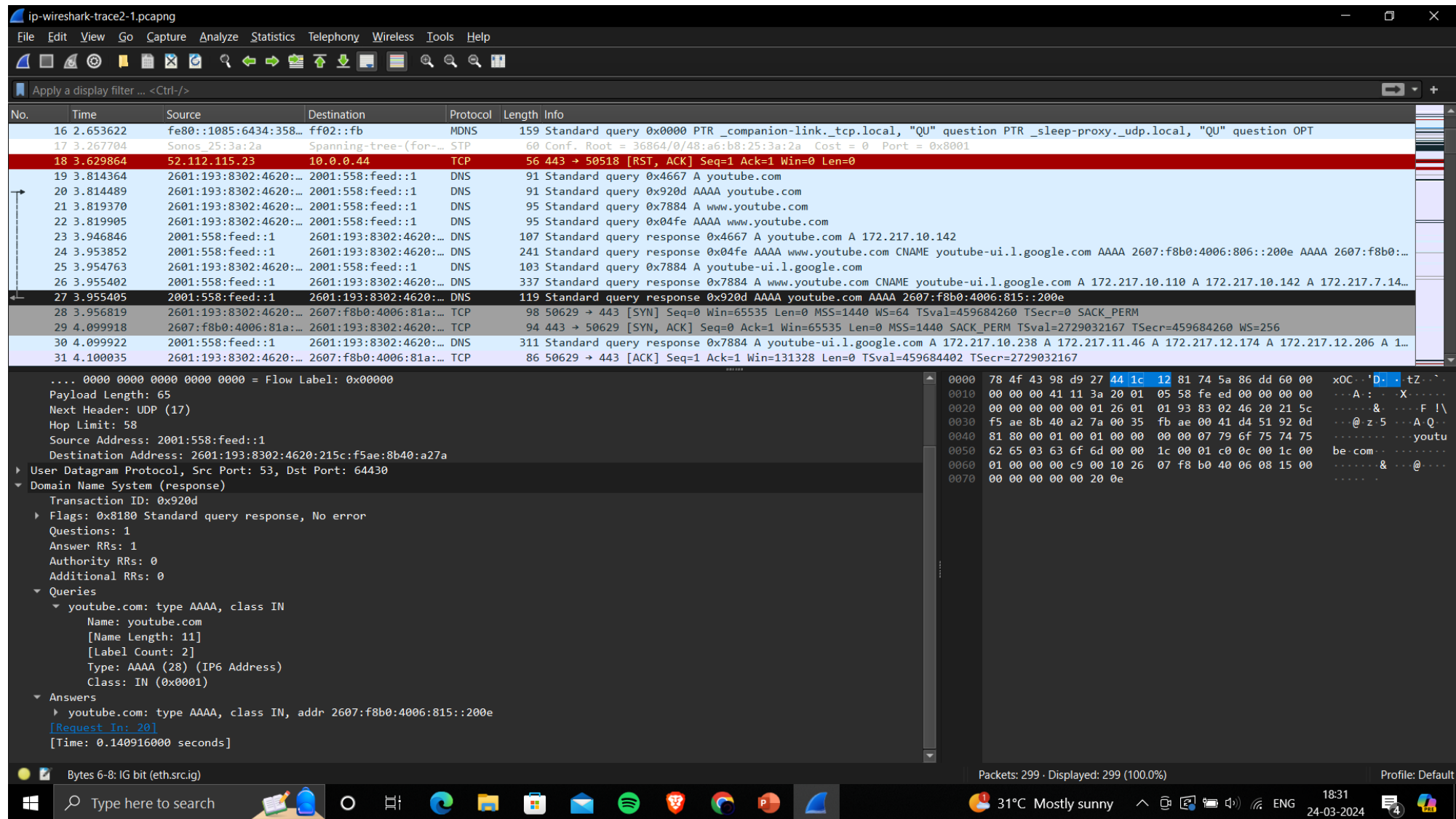


Figure 8(IPv6 Response)