

Catalina Cisneros

Lab: Wireshark IP v9.0

The screenshot shows a Wireshark capture of network traffic. The packet list pane shows several frames, with Frame 44 selected. The details pane shows the structure of the selected frame, which is a User Datagram Protocol (UDP) segment. The bytes pane shows the raw binary data of the frame.

1. Select the first UDP segment sent by your computer via the traceroute command to gaia.cs.umass.edu. What is the IP address of your computer?

→ The IP address of my computer is 192.168.86.61

The screenshot shows a Wireshark capture of network traffic. The packet list pane shows several frames, with Frame 3 selected. The details pane shows the structure of the selected frame, which is a User Datagram Protocol (UDP) segment. The bytes pane shows the raw binary data of the frame.

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

→ The TTL value in the IPv4 header is 1.

The screenshot shows a Wireshark capture of network traffic. The packet list pane shows several frames, with Frame 44 selected. The details pane shows the structure of the selected frame, which is a User Datagram Protocol (UDP) segment. The bytes pane shows the raw binary data of the frame. The header information pane shows the breakdown of the IPv4 header fields, including the TTL value.

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

→ UDP (protocol 17)

```
...0 0000 0000 0000 = Fragme
> Time to Live: 1
Protocol: UDP (17)
Header Checksum: 0x2faa [val
[Header checksum status: Unv
```

4. How many bytes are in the IP header?

→ 20 bytes

```
> Ethernet II, Src: Apple_98:d9:27 (/8:4t:43:98:d9:27), Dst: Google_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)
```

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

→ 36 bytes

→ Total Length: 56 (IP header + payload) Header Length: 20 bytes → Payload = 56 – 20 = 36 bytes, which matches the UDP Length: 36 field.

```
> Internet Protocol Version 4, Src: 192.168.86.61, Dst: 128.119.245.12
  User Datagram Protocol, Src Port: 64928, Dst Port: 33435
    Source Port: 64928
    > Destination Port: 33435
    Length: 36
    Checksum: 0xf2ff [unverified]
      Identification: 0xfdaf (64929)
```

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

→ No, not fragmented.

→ Flags: 0x0 means the More Fragments bit is not set. Fragment Offset: 0 → Both together indicate this datagram is a single, unfragmented IP packet.

```
> 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: 0xfdaf (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)
```

→ packet 44

```

> Frame 44: Packet, 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface
> Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Google_89:0e:c8 (3c:28:6d:89:8
  > 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 (DSGP: CS0, ECN: Not-ECT)
      Total Length: 56
      Identification: 0xfd1a (64929)
    > 000. .... = Flags: 0x0
      ... 0 0000 0000 0000 = Fragment Offset: 0
    > Time to Live: 1
      > [Expert Info (Note/Sequence): "Time To Live" only 1]
        ["Time To Live" only 1]
        [Severity level: Note]
        [Group: Sequence]
      Protocol: UDP (17)
      Header Checksum: 0x2faa [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 192.168.86.61
      Destination Address: 128.119.245.12
      [Stream index: 4]
    > User Datagram Protocol, Src Port: 64928, Dst Port: 33435
    > Data (28 bytes)

```

→ packet 52

```

> Frame 52: Packet, 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface
> Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Google_89:0e:c8 (3c:28:6d:89:8
  > 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 (DSGP: CS0, ECN: Not-ECT)
      Total Length: 56
      Identification: 0xfd4d (64932)
    > 000. .... = Flags: 0x0
      ... 0 0000 0000 0000 = Fragment Offset: 0
    > Time to Live: 2
      > [Expert Info (Note/Sequence): "Time To Live" only 2]
        ["Time To Live" only 2]
        [Severity level: Note]
        [Group: Sequence]
      Protocol: UDP (17)
      Header Checksum: 0x2ea7 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 192.168.86.61
      Destination Address: 128.119.245.12
      [Stream index: 4]
    > User Datagram Protocol, Src Port: 64928, Dst Port: 33438
    > Data (28 bytes)

```

→ packet 58

```

> Frame 58: Packet, 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface
> Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Google_89:0e:c8 (3c:28:6d:89:8
  > 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 (DSGP: CS0, ECN: Not-ECT)
      Total Length: 56
      Identification: 0xfd46 (64934)
    > 000. .... = Flags: 0x0
      ... 0 0000 0000 0000 = Fragment Offset: 0
    > Time to Live: 2
      > [Expert Info (Note/Sequence): "Time To Live" only 2]
        ["Time To Live" only 2]
        [Severity level: Note]
        [Group: Sequence]
      Protocol: UDP (17)
      Header Checksum: 0x2ea5 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 192.168.86.61
      Destination Address: 128.119.245.12
      [Stream index: 4]
    > User Datagram Protocol, Src Port: 64928, Dst Port: 33440
    > Data (28 bytes)

```

7. Which fields in the IP datagram always change from one datagram to the next within this series of UDP segments? Why?

→ The fields that change from one datagram to the next are the TTL, the Identification field, the header checksum, and the UDP destination port. These change because traceroute sends each probe with a new TTL to discover the next hop, assigns a new Identification value for every datagram, recalculates the checksum based on the modified header, and varies the UDP destination port so it can match the returning ICMP messages to specific traceroute probes.

8. Which fields in this sequence of IP datagrams stay constant? Why?

→ The fields that stay constant across the sequence are the source IP address, destination IP address, IPv4 version, header length, differentiated services field, flags, fragment offset, the protocol (UDP), and the payload size. These remain unchanged because all packets are being sent from the same machine to the same destination using the same protocol settings, and none of these packets require fragmentation

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

- Packet 44: 0xfdःa1
- Packet 52: 0xfdःa4
- Packet 58: 0xfdःa9
- These values consistently increase as new packets are sent.

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

- ICMP (1)

No.	Time	Source	Destination	Protocol	Ler
53	1.880429	10.0.0.1	192.168.86.61	ICMP	
	57 1 0000000	10 0 0 1	102 160 06 61	TCPMD	

11. Are the values in the Identification fields similar in behavior to your answer to question 9?

- packet 53

```
> Frame 53: Packet, 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface
> Ethernet II, Src: Google_89:0e:c8 (3c:28:6d:89:0e:c8), Dst: Apple_98:d9:27 (78:4f:43:98:d
> Internet Protocol Version 4, Src: 10.0.0.1, 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: 0xd5c3 (54723)
  > 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 63
  Protocol: ICMP (1)
  Header Checksum: 0x843f [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.0.0.1
  Destination Address: 192.168.86.61
  [Stream index: 6]
  > Internet Control Message Protocol
```

- packet 198

```

> Frame 198: Packet, 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface
> Ethernet II, Src: Google_89:0e:c8 (3c:28:6d:89:0e:c8), Dst: Apple_98:d9:27 (78:4f:43:98:d
> Internet Protocol Version 4, Src: 10.0.0.1, 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: 576
    Identification: 0xef48 (61256)
    > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 63
    Protocol: ICMP (1)
    Header Checksum: 0x68ce [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.0.1
    Destination Address: 192.168.86.61
    [Stream index: 6]
    > Internet Control Message Protocol

```

→ packet 290

```

> Frame 290: Packet, 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface
> Ethernet II, Src: Google_89:0e:c8 (3c:28:6d:89:0e:c8), Dst: Apple_98:d9:27 (78:4f:43:98:d
> Internet Protocol Version 4, Src: 128.119.0.10, Dst: 192.168.86.61
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x0000 (0)
    > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 245
    Protocol: ICMP (1)
    Header Checksum: 0x2e5e [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.119.0.10
    Destination Address: 192.168.86.61
    [Stream index: 14]
    > Internet Control Message Protocol

```

→ No, the Identification values in the ICMP packets are not similar to the pattern seen in Question 9. In my outbound UDP packets (Q9), the Identification numbers increased sequentially. However, in the ICMP packets returned by different routers, the Identification numbers vary widely and do not follow a sequence

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

→ No. The TTL values are not similar across the ICMP packets. Each ICMP packet comes from a different router, and every router sets its own initial TTL value when generating the ICMP "Time Exceeded" message. This means the TTL values differ from packet to packet

→ Packet 53: TTL = 63

→ Packet 198: TTL = 63

→ Packet 290: TTL = 245

13. Find the first IP datagram containing the first part of the 3000 byte segment. Has that segment been fragmented across more than one IP datagram?

→ Yes. It's split into multiple pieces. Packet 179 shows the same ID as the others and the "more fragments" flag is on.

```

I/O 12.788154 192.168.86.61 128.119.245.12 IPv4 1514 Fragmented IP
179 12.788154 192.168.86.61 128.119.245.12 IPv4 1514 Fragmented IP
180 12.788155 192.168.86.61 128.119.245.12 IPv4 1514 Fragmented IP
181 12.788155 192.168.86.61 128.119.245.12 UDP 54 64929 → 3343:
182 12.792190 192.168.86.1 192.168.86.61 ICMP 590 Time-to-live
183 12.792881 192.168.86.61 128.119.245.12 IPv4 1514 Fragmented IP

> Frame 179: Packet, 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface
> 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: 0xfdः (64930)
  > 001. .... = Flags: 0x1, More fragments
    ...0 0000 0000 0000 = Fragment Offset: 0
  < Time to Live: 1
    < [Expert Info (Note/Sequence): "Time To Live" only 1]
      ["Time To Live" only 1]
      [Severity level: Note]
      [Group: Sequence]
    Protocol: UDP (17)
    Header Checksum: 0xa05 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.86.61
    Destination Address: 128.119.245.12
    [Reassembled IPv4 in frame: 181]
    [Stream index: 4]
  > Data (1480 bytes)

```

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

→ The IP header has More Fragments = 1 and you can see the fragment offset field being used

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

→ The fragment offset is 0, and more fragments is 1, so this is the first piece

```

----- , -----
< 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

```

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

→ The Total Length is 1500 bytes, so this fragment is 1500 bytes total

```

  .... 0101 = Header Length: 20 bytes
  > Differentiated Services Field: 0x00
  Total Length: 1500
  Identification: 0xfdः (64930)
  < 001. .... = Flags: 0x1, More fragme

```

17. Inspect the second fragment. What information indicates that this is not the first fragment?

```

179 12.788154 192.168.86.61 128.119.245.12 IPv4 1514 Fragmented IP protocol (proto=UDI)
180 12.788155 192.168.86.61 128.119.245.12 IPv4 1514 Fragmented IP protocol (proto=UDI)
181 12.788155 192.168.86.61 128.119.245.12 UDP 54 64929 - 33435 Len=2972
182 12.792196 192.168.86.1 192.168.86.61 ICMP 598 Time-to-live exceeded (Time to l
183 12.792881 192.168.86.61 128.119.245.12 IPv4 1514 Fragmented IP protocol (proto=UDI)

> Frame 180: Packet, 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)
  0000 00.. = Differentiated Services Codepoint: Default (0)
  .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 1500
Identification: 0x7da2 (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]
    ["Time To Live" only 1]
    [Severity level: Note]
    [Group: Sequence]
  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]
  [Stream index: 4]
> Data (1480 bytes)

```

→ Because the fragment offset is 1480, not 0. First fragments always start at offset 0

```

.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"
    ["Time To Live" only 1]
    [Severity level: Note]
    [Group: Sequence]
  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]
  [Stream index: 4]
> Data (1480 bytes)

```

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

→ The fragment offset changed (from 0 to 1480), and the header checksum changed. The total length stays the same because both fragments are the same size

fragments: Set	fragments: Set
= Fragment Offset: 0	= Fragment Offset: 1480

→

19. Find the third fragment. What information indicates this is the last fragment?

→ Because More Fragments is 0, and the fragment offset is 2960, which means it's the final chunk of the original packet

```

more fragments: Not set
10 = Fragment Offset: 2960
[Note/Sequence): "Time To Live" o

```

20. What is the IPv6 source address of the DNS AAAA request?

→ The source IPv6 address is 2601:193:8302:4620:215c:f5ae:8b40:a27a

Frame	Time	Source	Destination	Protocol	Length	Type
20	3.814489	2601:193:8302:4620:215c:f5ae:8b40:a27a	2001:558:feed::1	DNS	91	Standard query
21	3.819370	2601:193:8302:4620:215c:f5ae:8b40:a27a	2001:558:feed::1	DNS	95	Standard query
22	3.819905	2601:193:8302:4620:215c:f5ae:8b40:a27a	2001:558:feed::1	DNS	95	Standard query
23	3.946846	2001:558:feed::1	2601:193:8302:4620:215c:f5ae:8b40:a27a	DNS	107	Standard query
24	3.952953	2001:558:feed::1	2601:193:8302:4620:215c:f5ae:8b40:a27a	DNS	241	Standard query

> Frame 20: Packet, 91 bytes wire (728 bits), 91 bytes captured (728 bits) on interface en0, id 0
> Ethernet II, Src: Apple_98:09:27 (78:4f:43:98:d9:27), Dst: VantivUSA_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)
<--> 0000 00.. = Differentiated Services Codepoint: Default (0)
<-->0 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
.... 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
[Stream Index: 1]
> User Datagram Protocol, Src Port: 64430, Dst Port: 53
> Domain Name System (query)

21. What is the IPv6 destination address of this datagram?

→ The destination IPv6 address is 2001:558:feed::1

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

→ The flow label is 0x63ed0

.... = Explicit
0 = Flow Label: 0x63ed0

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

→ The payload length is 37 bytes

....
Payload Length: 37

24. What is the upper layer protocol for this datagram's payload?

→ The upper layer protocol is UDP (17)

Payload Length: 37
Next Header: UDP (17)
Hop Limit: 255

```

22 3.81990s 2601:193:8302:4b20::21c:f5ae:8b40:a2/a 2001:5b8:feed::1          DNS      95 Star
23 3.946846 2001:558:feed::1                           2601:193:8302:4620::215:c:f5ae:8b40.. DNS      107 Star
24 3.953852 2001:558:feed::1                           2601:193:8302:4620::215:c:f5ae:8b40.. DNS      241 Star
25 3.954763 2601:193:8302:4620::215:c:f5ae:8b40:a27a 2001:558:feed::1          DNS      103 Star
26 3.955402 2001:558:feed::1                           2601:193:8302:4620::215:c:f5ae:8b40.. DNS      337 Star
27 3.955405 2001:558:feed::1                           2601:193:8302:4620::215:c:f5ae:8b40.. DNS      119 Star
28 3.956819 2601:193:8302:4620::215:c:f5ae:8b40:a27a 2607:fb0b:4006:81a::200e   TCP      98 5062
29 4.099918 2607:fb0b:4006:81a::200e                2601:193:8302:4620::215:c:f5ae:8b40.. TCP      94 443

> Frame 23: Packets on wire (856 bytes), 107 bytes captured (856 bytes) interface en0, id 0
> Ethernet II, Src: VantivalUSA_81:74:5a (44:1c:12:12:01:01), Dst: Apple_98 (0:0:0:0:0:0)
> Internet Protocol Version 6, Src: 2001:558:feed::1, Dst: 2601:193:8302:4620::215:c:f5ae:8b40:a27a
> User Datagram Protocol, Src Port: 53, Dst Port: 62315
> Domain Name System (response)

Transaction ID: 0x4667
  Flags: 0x8180 Standard query response, No error
    1... .... .... .... = Response: Message is a response
    .000 0... .... .... = Opcode: Standard query (0)
    .... 0. .... .... = Authoritative: Server is not an authority for domain
    .... ..0 .... .... = Truncated: Message is not truncated
    .... ..1 .... .... = Recursion desired: Do query recursively
    .... 1.... .... = Recursion available: Server can do recursive queries
    .... ..0.... .... = Z: reserved (0)
    .... ..0.... .... = Answer authenticated: Answer/authority portion was not authenticated by the server
    .... ..0.... .... = Non-authenticated data: Unacceptable
    .... ..0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
  Queries
    > youtube.com: type A, class IN
  Answers
    > youtube.com: type A, class IN, addr 172.217.10.142
[Request_In: 19]
[Time: 132.482000 milliseconds]

```

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

→ It returned 4 IPv6 addresses.

```

23 J.940840 2001:5b8:feed::1           2601:193:8302:4b20::21c:f5ae:8b40.. DNS      107 Star
24 3.953852 2001:558:feed::1           2601:193:8302:4620::215:c:f5ae:8b40.. DNS      241 Star
25 3.954763 2601:193:8302:4620::215:c:f5ae:8b40:a27a 2001:558:feed::1          DNS      103 Star
26 3.955402 2001:558:feed::1           2601:193:8302:4620::215:c:f5ae:8b40.. DNS      337 Star
27 3.955405 2001:558:feed::1           2601:193:8302:4620::215:c:f5ae:8b40.. DNS      119 Star
28 3.956819 2601:193:8302:4620::215:c:f5ae:8b40:a27a 2607:fb0b:4006:81a::200e   TCP      98 5062
29 4.099918 2607:fb0b:4006:81a::200e    2601:193:8302:4620::215:c:f5ae:8b40.. TCP      94 443

  Questions: 1
  Answers
    > www.youtube.com: type AAAA, class IN
      Name: www.youtube.com
      Type: NAME (5) (Canonical NAME for an alias)
      Class: IN (0x0001)
      Time to live: 193 (5 hours, 58 minutes, 42 seconds)
      Data length: 22
      CNAME: youtube-ui.l.google.com
    > youtube-ui.l.google.com: type AAAA, class IN, addr 2607:fb0b:4006:806::200e
      Name: youtube-ui.l.google.com
      Type: AAAA (28) (IP6 Address)
      Class: IN (0x0001)
      Time to live: 193 (3 minutes, 13 seconds)
      Data length: 16
      AAAA Address: 2607:fb0b:4006:806::200e
    > youtube-ui.l.google.com: type AAAA, class IN, addr 2607:fb0b:4006:81a::200e
      Name: youtube-ui.l.google.com
      Type: AAAA (28) (IP6 Address)
      Class: IN (0x0001)
      Time to live: 193 (3 minutes, 13 seconds)
      Data length: 16
      AAAA Address: 2607:fb0b:4006:81a::200e
    > youtube-ui.l.google.com: type AAAA, class IN, addr 2607:fb0b:4006:81b::200e
      Name: youtube-ui.l.google.com
      Type: AAAA (28) (IP6 Address)
      Class: IN (0x0001)
      Time to live: 193 (3 minutes, 13 seconds)
      Data length: 16
      AAAA Address: 2607:fb0b:4006:81b::200e
    > youtube-ui.l.google.com: type AAAA, class IN, addr 2607:fb0b:4006:807::200e
      Name: youtube-ui.l.google.com
      Type: AAAA (28) (IP6 Address)
      Class: IN (0x0001)
      Time to live: 193 (3 minutes, 13 seconds)
      Data length: 16
      AAAA Address: 2607:fb0b:4006:807::200e
[Request_In: 21]
[Time: 133.947000 milliseconds]

```

26. What is the first IPv6 address returned for youtube.com?

→ The first AAAA address is: 2607:f8b0:4006:806::200e

```

Time to live: 193 (5 hours, 58 minutes, 42 seconds)
Data length: 22
CNAME: youtube-ui.l.google.com
  > youtube-ui.l.google.com: type AAAA, class IN, addr 2607:f8b0:4006:806::200e
    Name: youtube-ui.l.google.com
    Type: AAAA (28) (IP6 Address)
    Class: IN (0x0001)
    Time to live: 193 (3 minutes, 13 seconds)
    Data length: 16
    AAAA Address: 2607:f8b0:4006:806::200e
  > youtube-ui.l.google.com: type AAAA, class IN, addr 2607:f8b0:4006:807::200e
    Name: youtube-ui.l.google.com
    Type: AAAA (28) (IP6 Address)
    Class: IN (0x0001)
    Time to live: 193 (3 minutes, 13 seconds)
    Data length: 16
    AAAA Address: 2607:f8b0:4006:807::200e
  > youtube-ui.l.google.com: type AAAA, class IN, addr 2607:f8b0:4006:808::200e
    Name: youtube-ui.l.google.com
    Type: AAAA (28) (IP6 Address)
    Class: IN (0x0001)
    Time to live: 193 (3 minutes, 13 seconds)
    Data length: 16
    AAAA Address: 2607:f8b0:4006:808::200e
  > youtube-ui.l.google.com: type AAAA, class IN, addr 2607:f8b0:4006:809::200e
    Name: youtube-ui.l.google.com
    Type: AAAA (28) (IP6 Address)
    Class: IN (0x0001)
    Time to live: 193 (3 minutes, 13 seconds)
    Data length: 16
    AAAA Address: 2607:f8b0:4006:809::200e
[Request_In: 22]
[Time: 134.947000 milliseconds]

```