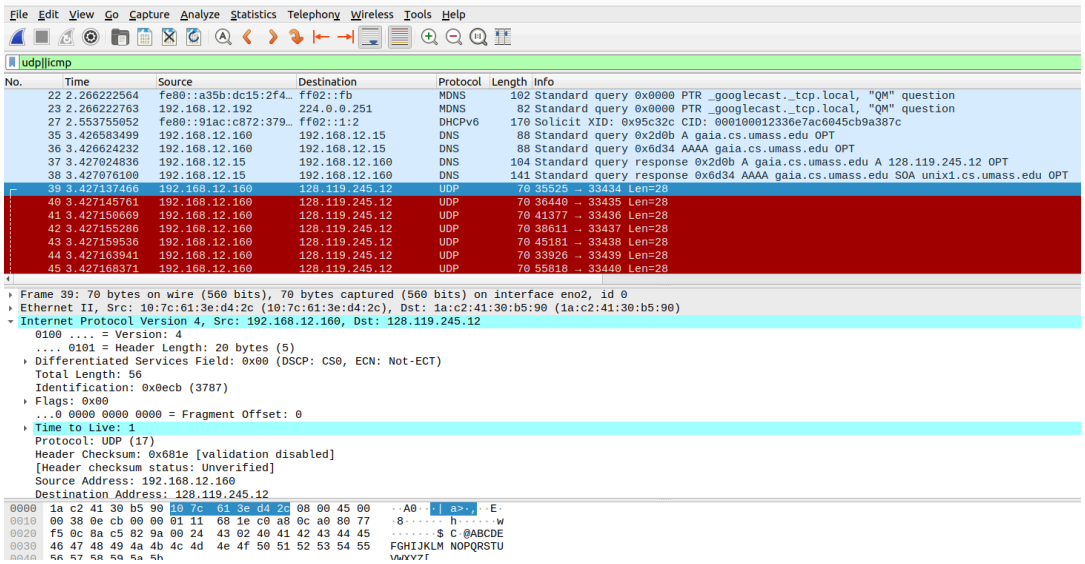
Sarwar, Andre, and Mohammed
Lab 6
November 1, 2024

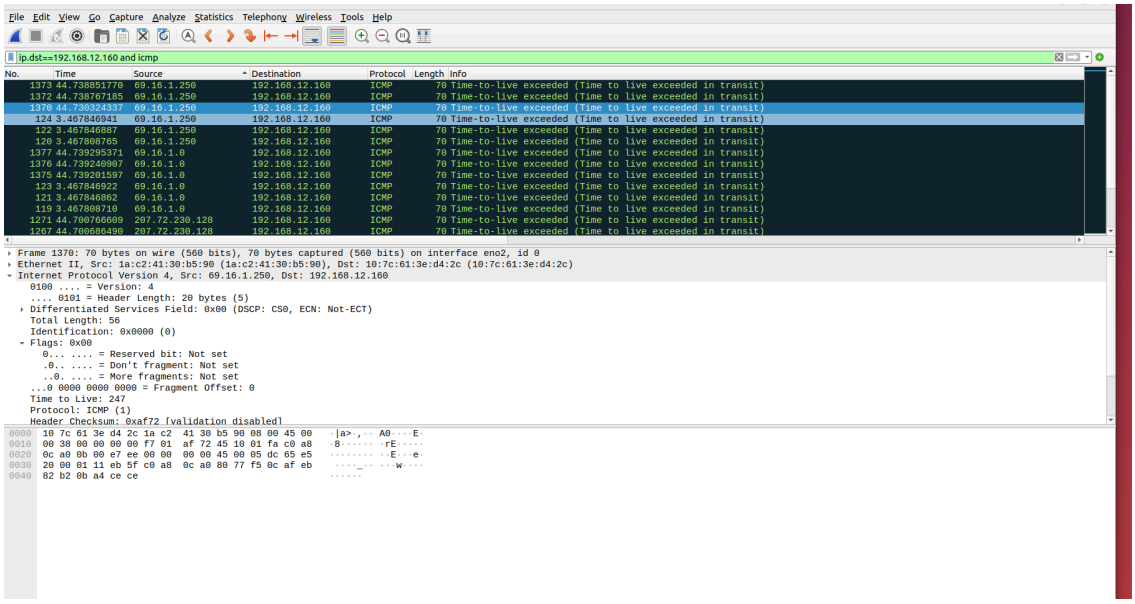
1. Select the first UDP segment sent by your computer via the traceroute command to gaia.cs.umass.edu. (Hint: this is 44th packet in the trace file in the ipwireshark-trace1-1.pcapng file in footnote 2). Expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?



   - The first UDP segment is packet number 39. The IP address of our computer 192.168.12.160.
2. What is the value in the time-to-live (TTL) field in this IPv4 datagram's header?
   - The value is 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].
   - The upper layer protocol is UDP (17).
4. How many bytes are in the IP header?
   - The IP header is 20 bytes.
5. How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.
   - The total length is 56 bytes. We know that the IP header is 20 bytes, which means there are 36 bytes remaining. This difference, 36, is the amount of Payload bytes.
6. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.
   - The IP datagram has not been fragmented. We determined this by examining the fragment offset. The fragment offset is 0.

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 are time to live and identification. These change because there are different datagrams being sent.
8. Which fields in this sequence of IP datagrams (containing UDP segments) stay constant? Why?
    - The fields in this sequence that stay constant are the header length, the Protocol: UDP (17), the source and destination addresses, IPV4, and checksum. These stay the same because they are set within this example IPV4 sequence from the destination to the source.
9. Describe the pattern you see in the values in the Identification field of the IP datagrams being sent by your computer.
    - The pattern that we see in the values in the identification field of the IP datagrams is that the values are increasing.

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].



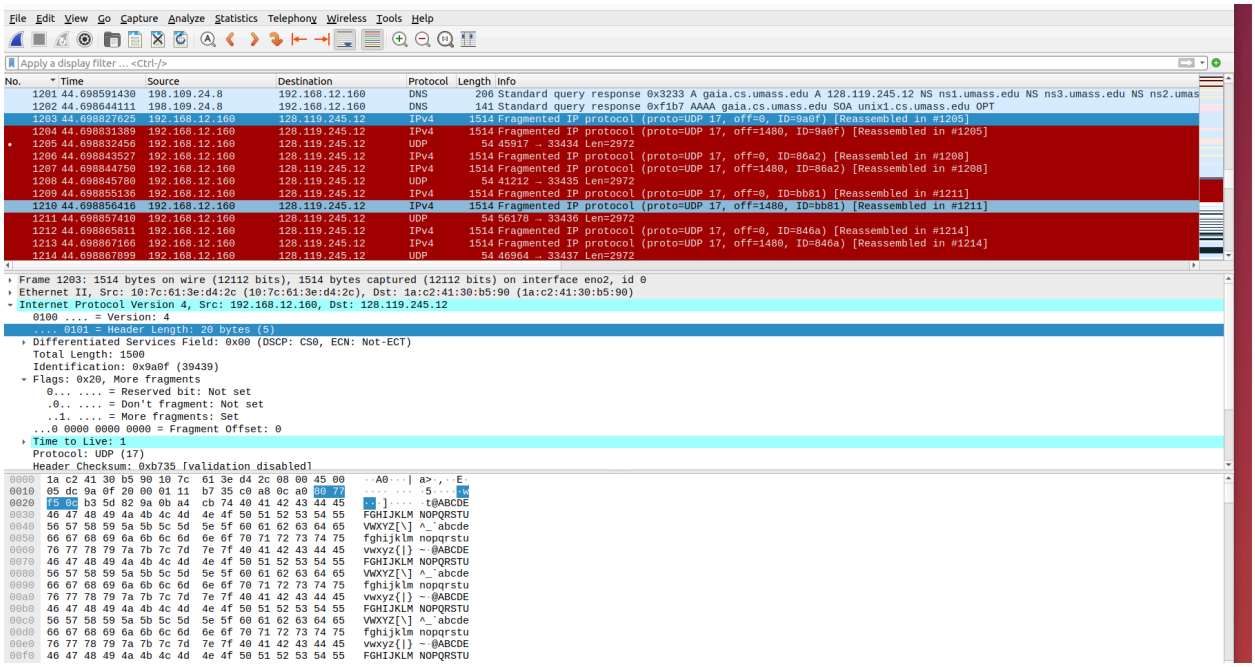
    - The upper layer protocol specified is Protocol: ICMP (1).
11. Are the values in the Identification fields (across the sequence of all of ICMP packets from all of the routers) similar in behavior to your answer to question 9 above?
    - Yes, the values in the identification fields are similar to the behaviors observed in question 9.
12. Are the values of the TTL fields similar, across all of ICMP packets from all of the routers?

- No, the values are different as they are incrementing as they come from different routers.

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. (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 yes4!)

- The answer is yes.

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

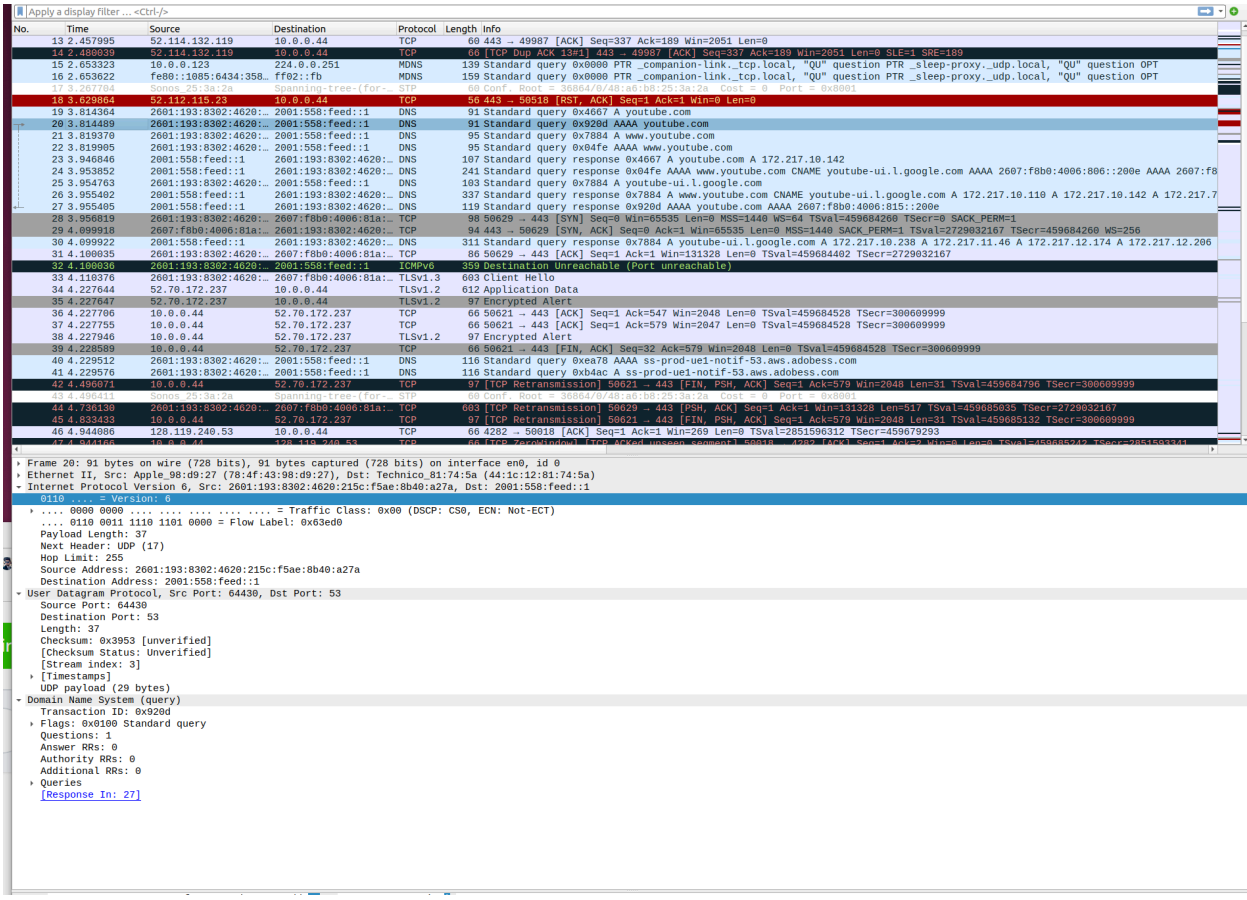


- The More Fragments section states “set”. Also, the datagram has “Fragmented IP protocol” in its info.

15. What information in the IP header for this packet indicates whether this is the first fragment versus a latter fragment?
    - You can tell this is the first fragment because the fragment offset is 0.
16. How many bytes are there in is this IP datagram (header plus payload)?
    - The amount of bytes in this IP datagram 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?
    - The fragment offset has a value, in this case 1400.

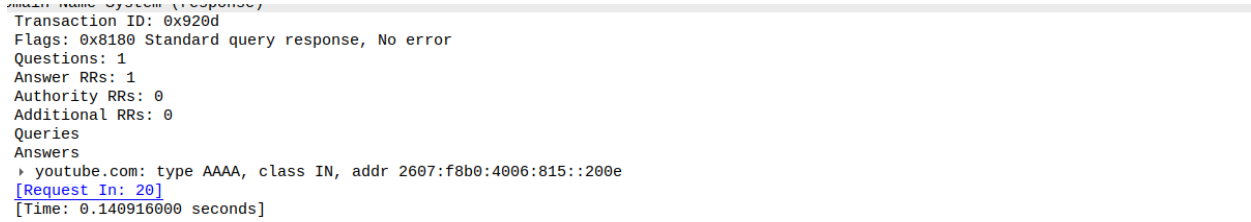
18. What fields change in the IP header between the first and second fragment?
    - The checksum values change, the fragment offset changes, and the checksum changes.
19. Now find the IP datagram containing the third fragment of the original UDP segment. What information in the IP header indicates that this is the last fragment of that segment?
    - The fragment offset matches the first fragment, that being Fragment Offset: 0.

20. 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 window5.
    - 2601:193:8302:4620:215c:f5ae:8b40:a27a.



21. What is the IPv6 destination address for this datagram? Give this IPv6 address in the exact same form as displayed in the Wireshark window.
    - 2001:558:feed::1
22. What is the value of the flow label for this datagram?
    - The value of the flow label is 0x63ed0.
23. How much payload data is carried in this datagram?
    - The payload length is 37.

24. What is the upper layer protocol to which this datagram's payload will be delivered at the destination?
    - The upper layer protocol is UDP (17) for the destination 2001:558:feed::1
25. How many IPv6 addresses are returned in the response to this AAAA request?
    - There is 1 IPv6 address being returned.



26. 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.
    - The first of the IPV6 addresses returned by the DNS is AAAA Address: 2607:f8b0:4006:815::200e