Julian Chavez

Professor Dimitrios Melissourgos

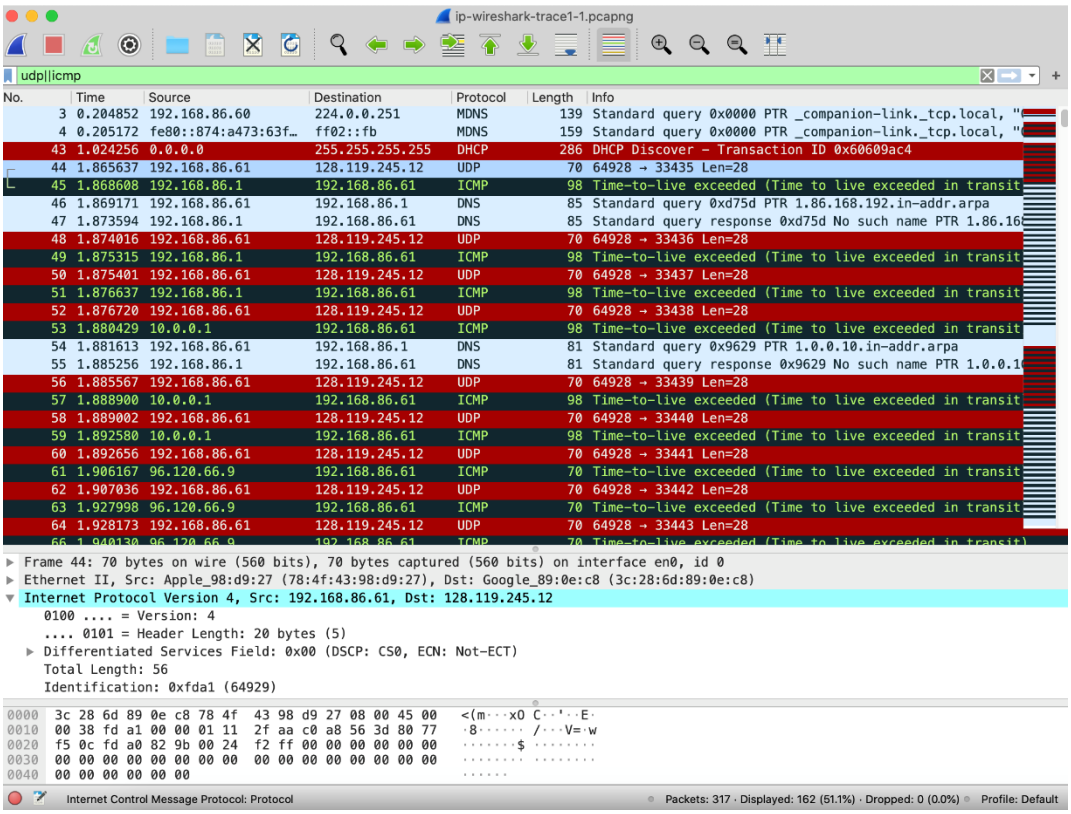
Network Systems Management

October 24, 2023

Wireshark Lab: IP

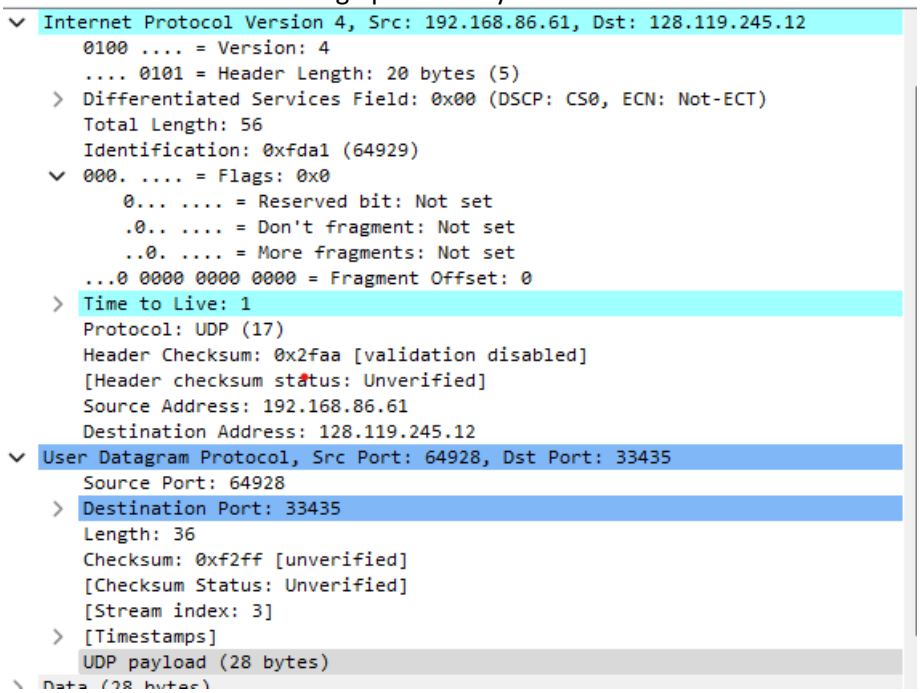
Part 1: Basic IPv4

Answer the following questions.



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 *ip-wireshark-trace1-1.pcapng* file). Expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?
    - 192.168.86.61
2. What is the value in the time-to-live (TTL) field in this IPv4 datagram's header?
    - Time to Live: 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].
    - UDP 17
4. How many bytes are in the IP header?
    - 70 – the header length

5. How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.
    - Total length (56) – Header length (20) = 36 bytes
    - Information found under the IPv4 header
6. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.
    - Under IPv4 and then under 000. … = Flags show that fragments are 'Not Set.'
8. 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 do some fields change periodically?

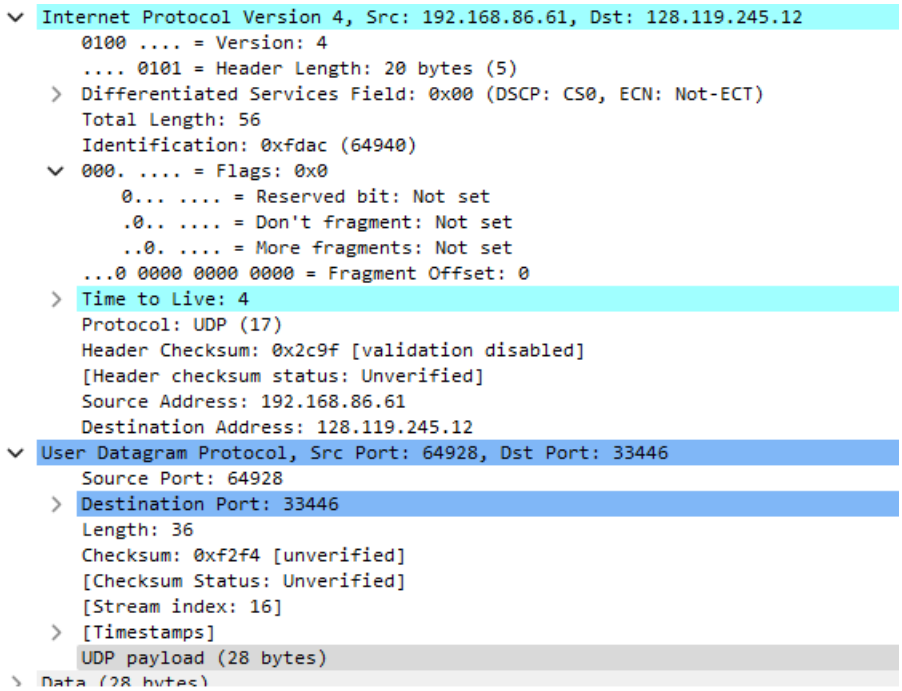


```
Internet Protocol Version 4, Src: 192.168.86.61, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xfdac (64940)
  v 000. .... = Flags: 0x0
        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: 4
    Protocol: UDP (17)
    Header Checksum: 0x2c9f [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.86.61
    Destination Address: 128.119.245.12
v User Datagram Protocol, Src Port: 64928, Dst Port: 33446
    Source Port: 64928
  > Destination Port: 33446
    Length: 36
    Checksum: 0xf2f4 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 16]
  > [Timestamps]
    UDP payload (28 bytes)
> Data (28 bytes)
```

a. Constantly: Identification, Destination Port, Checksum,
b. Periodically: Time to Live – changes because the traceroute command sends 3 packets/attempts to connect to its destination

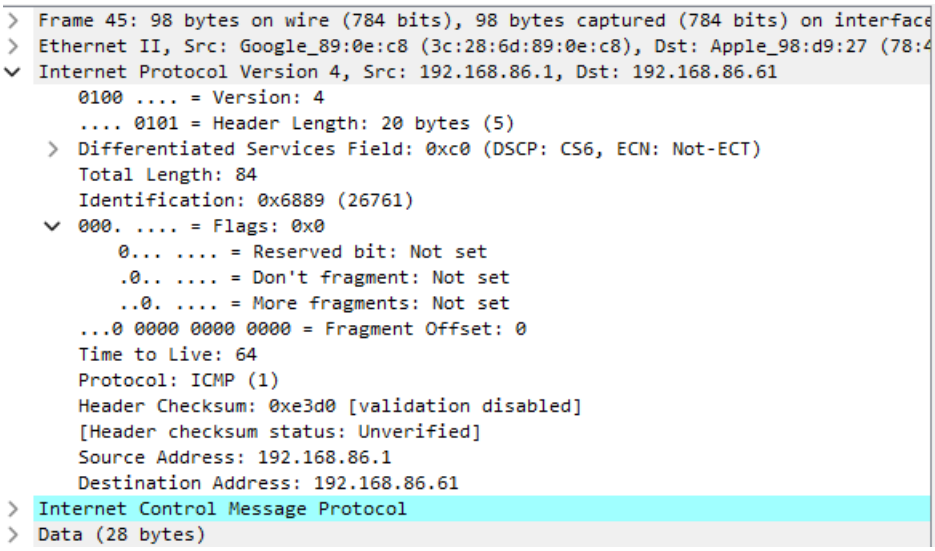
9. Which fields in this sequence of IP datagrams (containing UDP segments) stay constant? Why?

```
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)
  v 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)
    Header Checksum: 0x2faa [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.86.61
    Destination Address: 128.119.245.12
v User Datagram Protocol, Src Port: 64928, Dst Port: 33435
    Source Port: 64928
  > Destination Port: 33435
    Length: 36
    Checksum: 0xf2ff [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
  > [Timestamps]
    UDP payload (28 bytes)
> Data (28 bytes)
```



   a. Source Port, Header Length, Total Length, Destination, Protocol, IP version
   b. The traceroute always shows the IP to the final destination of the packet
   c. Since the packets being sent are the same, the lengths of packets stay consistent

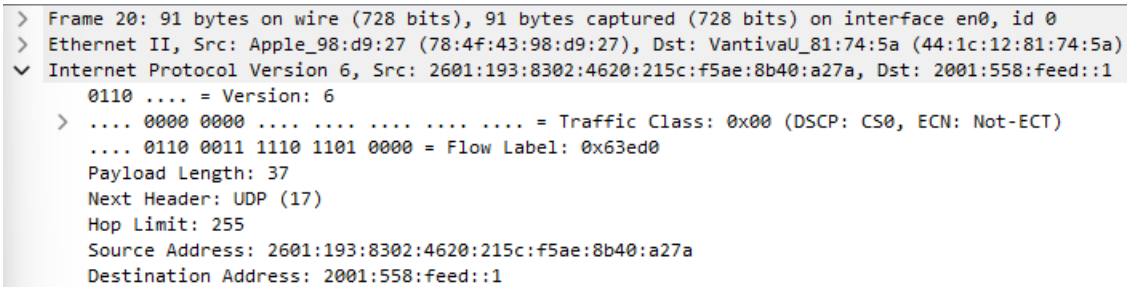
10. Describe the pattern you see in the values in the Identification field of the IP datagrams being sent by your computer.
    a. Each of the packets increments by one in the identification field.
11. What is the upper layer protocol specified in the IP datagrams returned from the routers? [Note: the answers for Linux/MacOS differ from Windows here].
    a. ICMP
12. 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 10 above?
    a. There are a handful of fields that hold the same ID number, there are about three packets or so that have different destinations. The behavior is the packet received by the user, instead of the other way around.
    b. The source is different every time because we are using different hops.
13. Are the values of the TTL fields similar, across all of ICMP packets from all of the routers?
    a. The TTL ranges are very different from the previous question. The TTL range from the lower sixties to the upper two hundreds. Coming from a different routers, the TTL is much higher



Part 2: IPv6

Answer the following questions:

14. 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 window[1].
    - 2601:193:8302:4620:215c:f5ae:8b40:a27a

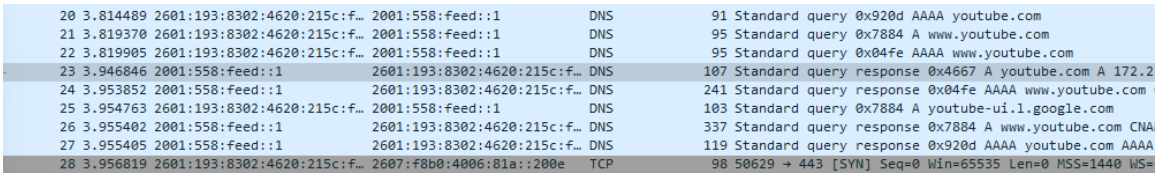


15. What is the IPv6 destination address for this datagram? Give this IPv6 address in the exact same form as displayed in the Wireshark window.
    - 2001:558:feed::1
16. How much payload data is carried in this datagram?
    - The payload length is 37

[1] Recall that an IPv6 address is shown as 8 sets of 4 hexadecimal digits, with each set separated by colons, and with leading zeros omitted. If an IPv6 address has two colons in a row ('::'), this is shorthand meaning that all of the intervening bytes between the two colons are zero. Thus, for example, `fe80::1085:6434:583:e79` is shorthand for `fe80:0000:0000:0000:1085:6434:0583:0e79`. Make sure you understand this example.

Lastly, find the IPv6 DNS response to the IPv6 DNS AAAA request made in the 20th packet in this trace. This DNS response contains IPv6 addresses for youtube.com.

1. How many IPv6 addresses are returned in the response to this AAAA request?
    - 7



2. 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.
    - 2607:f8b0:81a::200e?