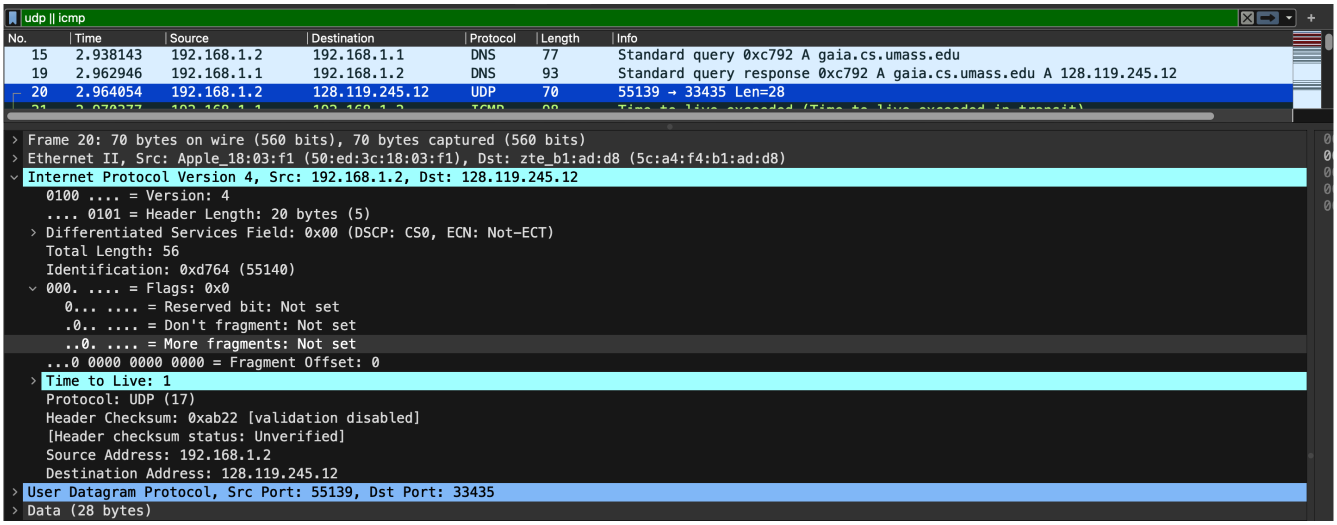
Student Information

Full Name : Mehmet Rüçhan Yavuzdemir
Id Number: 2522159

1 Basic IPv4



```
udp || icmp
No.  Time      Source       Destination     Protocol Length Info
 15  2.938143  192.168.1.2  192.168.1.1     DNS      77     Standard query 0xc792 A gaia.cs.umass.edu
 19  2.962946  192.168.1.1  192.168.1.2     DNS      93     Standard query response 0xc792 A gaia.cs.umass.edu A 128.119.245.12
 20  2.964054  192.168.1.2  128.119.245.12  UDP      70     55139 → 33435 Len=28
 21  2.970277  192.168.1.1  192.168.1.2     ICMP     98     Time-to-live exceeded (Time to live exceeded in transit)

> Frame 20: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: Apple_18:03:f1 (50:ed:3c:18:03:f1), Dst: zte_b1:ad:d8 (5c:a4:f4:b1:ad:d8)
v Internet Protocol Version 4, Src: 192.168.1.2, 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: 0xd764 (55140)
  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: 0xab22 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.2
    Destination Address: 128.119.245.12
> User Datagram Protocol, Src Port: 55139, Dst Port: 33435
> Data (28 bytes)
```

Figure 1: Answer 1-2-3-4-5-6

Answer 1

The IP address of my computer is `192.168.1.2`.

Answer 2

TTL (Time to Live) value in the IPv4 datagram's header is set to `1`.

Answer 3

The value of the upper layer protocol field in the IPv4 datagram's header is `17`, which stands for UDP.

Answer 4

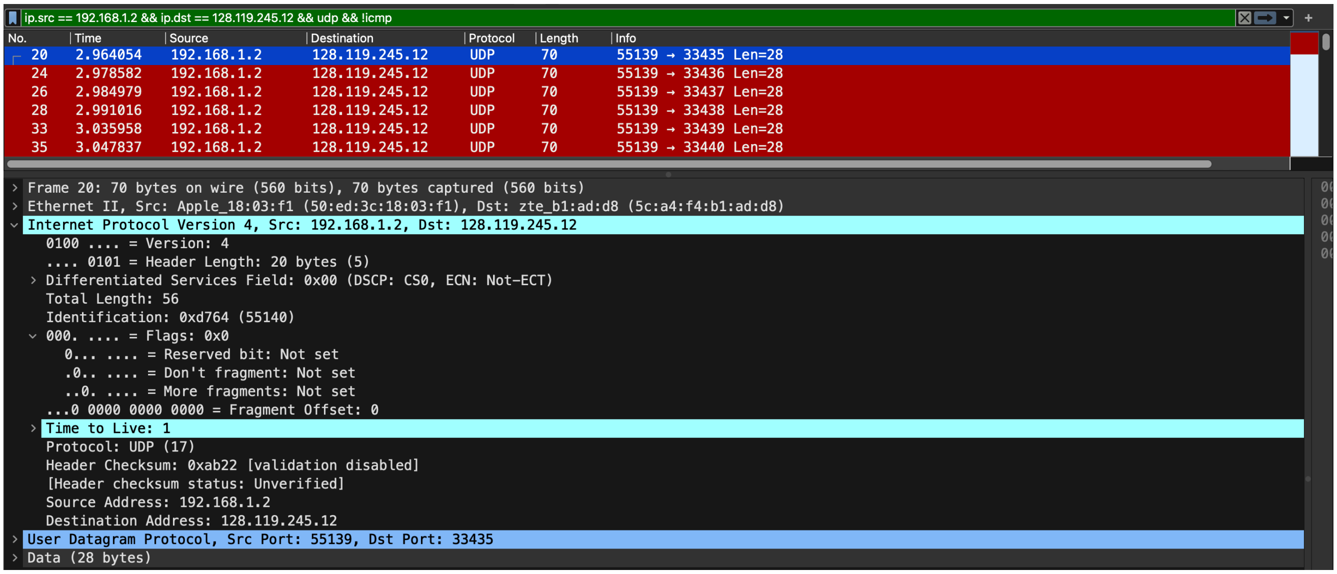
There are `20` bytes in the IP header, which can be seen under the field `Header Length`.

Answer 5

There are 36 bytes in the IP payload. That's because the total length is the summation of header length and payload length. The total length is 56 bytes (`Total Length`), and the header length is 20 bytes (`Header Length`).

Answer 6

No, it hasn't. That's because the `More Fragments` bit has not been set to 1, meaning there will be no more fragments, and the datagram has not been fragmented as it is the first UDP segment.



```
ip.src == 192.168.1.2 && ip.dst == 128.119.245.12 && udp && !icmp
No.    Time        Source          Destination      Protocol  Length  Info
 20    2.964054    192.168.1.2     128.119.245.12   UDP       70      55139 → 33435 Len=28
 24    2.978582    192.168.1.2     128.119.245.12   UDP       70      55139 → 33436 Len=28
 26    2.984979    192.168.1.2     128.119.245.12   UDP       70      55139 → 33437 Len=28
 28    2.991016    192.168.1.2     128.119.245.12   UDP       70      55139 → 33438 Len=28
 33    3.035958    192.168.1.2     128.119.245.12   UDP       70      55139 → 33439 Len=28
 35    3.047837    192.168.1.2     128.119.245.12   UDP       70      55139 → 33440 Len=28
```

```
> Frame 20: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: Apple_18:03:f1 (50:ed:3c:18:03:f1), Dst: zte_b1:ad:d8 (5c:a4:f4:b1:ad:d8)
v Internet Protocol Version 4, Src: 192.168.1.2, 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: 0xd764 (55140)
  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: 0xab22 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.2
    Destination Address: 128.119.245.12
> User Datagram Protocol, Src Port: 55139, Dst Port: 33435
> Data (28 bytes)
```

Figure 2: Answer 7-8-9

Answer 7

The `Identification` field always changes from datagram to datagram, because it should uniquely identify the datagram being sent. In my traceroute implementation, each IP datagram is sent 3 times. Hence, in each IP datagram, the `Time to Leave` field is not unique and does not always change. Finally, in my .pcap file, the `Header Checksum` seems to be changed in each IP datagram, however, two different IP datagrams may have the same checksum value. This mostly depends on how it's calculated.

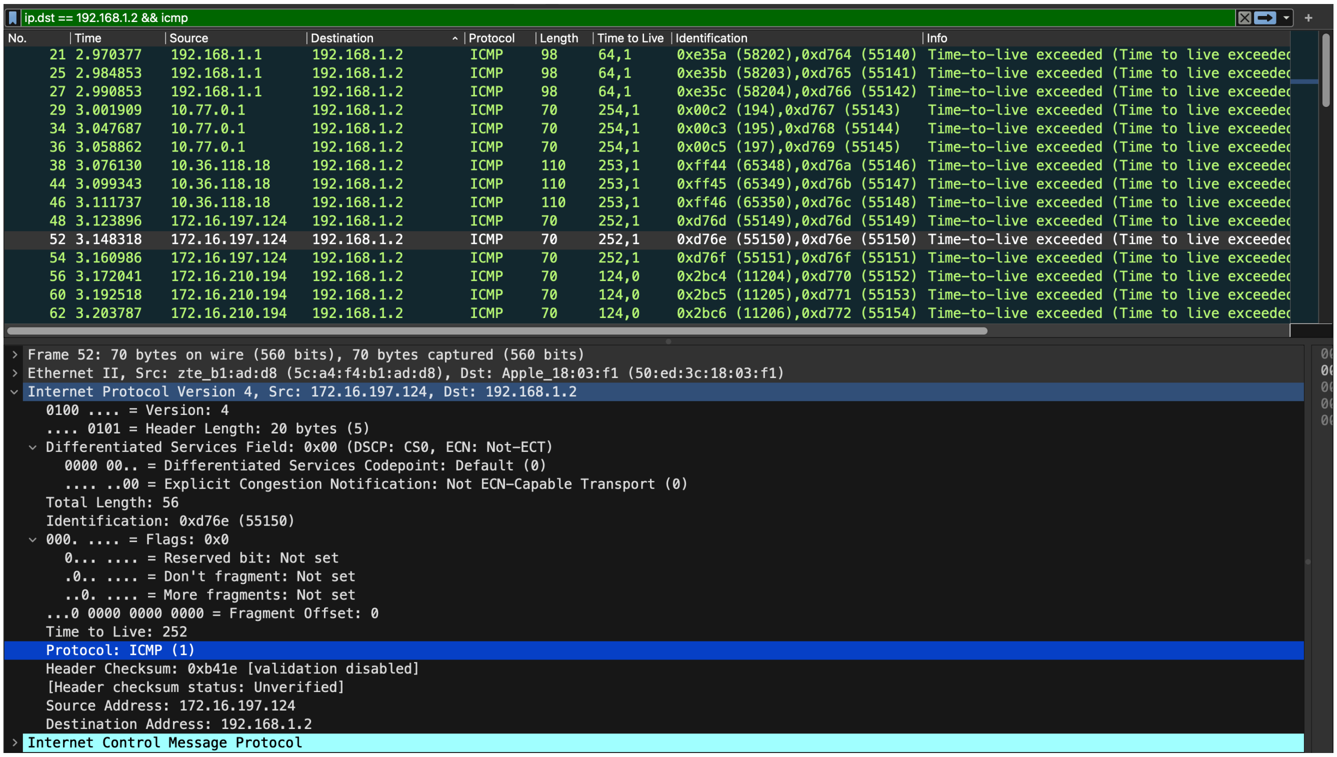
Answer 8

In this sequence of IP datagrams, these fields stay constant:

- `Version`: Since for all UDP segments, IPv4 is used.
- `Header Length`: It is 20 bytes for each packet.
- `Differentiated Services Field`: There are no differences in services, it's always 0 in my .pcap file
- `Total Length`: Since we explicitly tell the `traceroute` program that the UDP datagram size will be 56 bytes.
- `Flags`: There are no flags used, they were all 0 for all UDP segments.
- `Protocol`: As an upper-layer protocol, UDP is used for all packets.
- `Source Address`: Since we explicitly filter the packet for our needs, it is constant for these filtered UDP segments.
- `Destination Address`: Since we explicitly filter the packet for our needs, it is constant for these filtered UDP segments.

Answer 9

For each UDP segment from top to down, the value in the `Identification` field increases by 1.



```
ip.dst == 192.168.1.2 && icmp
No.     Time      Source          Destination     Protocol Length Time to Live Identification                Info
     21 2.970377  192.168.1.1     192.168.1.2     ICMP     98     64,1         0xe35a (58202),0xd764 (55140) Time-to-live exceeded (Time to live exceedec
     25 2.984853  192.168.1.1     192.168.1.2     ICMP     98     64,1         0xe35b (58203),0xd765 (55141) Time-to-live exceeded (Time to live exceedec
     27 2.990853  192.168.1.1     192.168.1.2     ICMP     98     64,1         0xe35c (58204),0xd766 (55142) Time-to-live exceeded (Time to live exceedec
     29 3.001909  10.77.0.1       192.168.1.2     ICMP     70     254,1        0x00c2 (194),0xd767 (55143)   Time-to-live exceeded (Time to live exceedec
     34 3.047687  10.77.0.1       192.168.1.2     ICMP     70     254,1        0x00c3 (195),0xd768 (55144)   Time-to-live exceeded (Time to live exceedec
     36 3.058862  10.77.0.1       192.168.1.2     ICMP     70     254,1        0x00c5 (197),0xd769 (55145)   Time-to-live exceeded (Time to live exceedec
     38 3.076130  10.36.118.18    192.168.1.2     ICMP     110    253,1        0xff44 (65348),0xd76a (55146) Time-to-live exceeded (Time to live exceedec
     44 3.099343  10.36.118.18    192.168.1.2     ICMP     110    253,1        0xff45 (65349),0xd76b (55147) Time-to-live exceeded (Time to live exceedec
     46 3.111737  10.36.118.18    192.168.1.2     ICMP     110    253,1        0xff46 (65350),0xd76c (55148) Time-to-live exceeded (Time to live exceedec
     48 3.123896  172.16.197.124  192.168.1.2     ICMP     70     252,1        0xd76d (55149),0xd76d (55149) Time-to-live exceeded (Time to live exceedec
     52 3.148318  172.16.197.124  192.168.1.2     ICMP     70     252,1        0xd76e (55150),0xd76e (55150) Time-to-live exceeded (Time to live exceedec
     54 3.160986  172.16.197.124  192.168.1.2     ICMP     70     252,1        0xd76f (55151),0xd76f (55151) Time-to-live exceeded (Time to live exceedec
     56 3.172041  172.16.210.194  192.168.1.2     ICMP     70     124,0        0x2bc4 (11204),0xd770 (55152) Time-to-live exceeded (Time to live exceedec
     60 3.192518  172.16.210.194  192.168.1.2     ICMP     70     124,0        0x2bc5 (11205),0xd771 (55153) Time-to-live exceeded (Time to live exceedec
     62 3.203787  172.16.210.194  192.168.1.2     ICMP     70     124,0        0x2bc6 (11206),0xd772 (55154) Time-to-live exceeded (Time to live exceedec
```

```
> Frame 52: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: zte_b1:ad:d8 (5c:a4:f4:b1:ad:d8), Dst: Apple_18:03:f1 (50:ed:3c:18:03:f1)
v Internet Protocol Version 4, Src: 172.16.197.124, Dst: 192.168.1.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v 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: 56
    Identification: 0xd76e (55150)
  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: 252
    Protocol: ICMP (1)
    Header Checksum: 0xb41e [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.16.197.124
    Destination Address: 192.168.1.2
> Internet Control Message Protocol
```

Figure 3: Answer 10-11-12

Answer 10

The upper layer protocol field specified in the IP datagram's header is ICMP. Please note that the MacOS operating system is running on the device used.

Answer 11

No, the behavior is not similar to what we've seen in Answer 9. Although there are groups of ICMP packets that their `Identification` field increases by 1, this is not a general case. Some numbers are skipped, or a random number is picked, etc. No global pattern exists, but there may be a local pattern.

Answer 12

No, there are different TTL values in the ICMP packets being sent from different routers. However, ICMP packets being sent from the same router have the same TTL values.