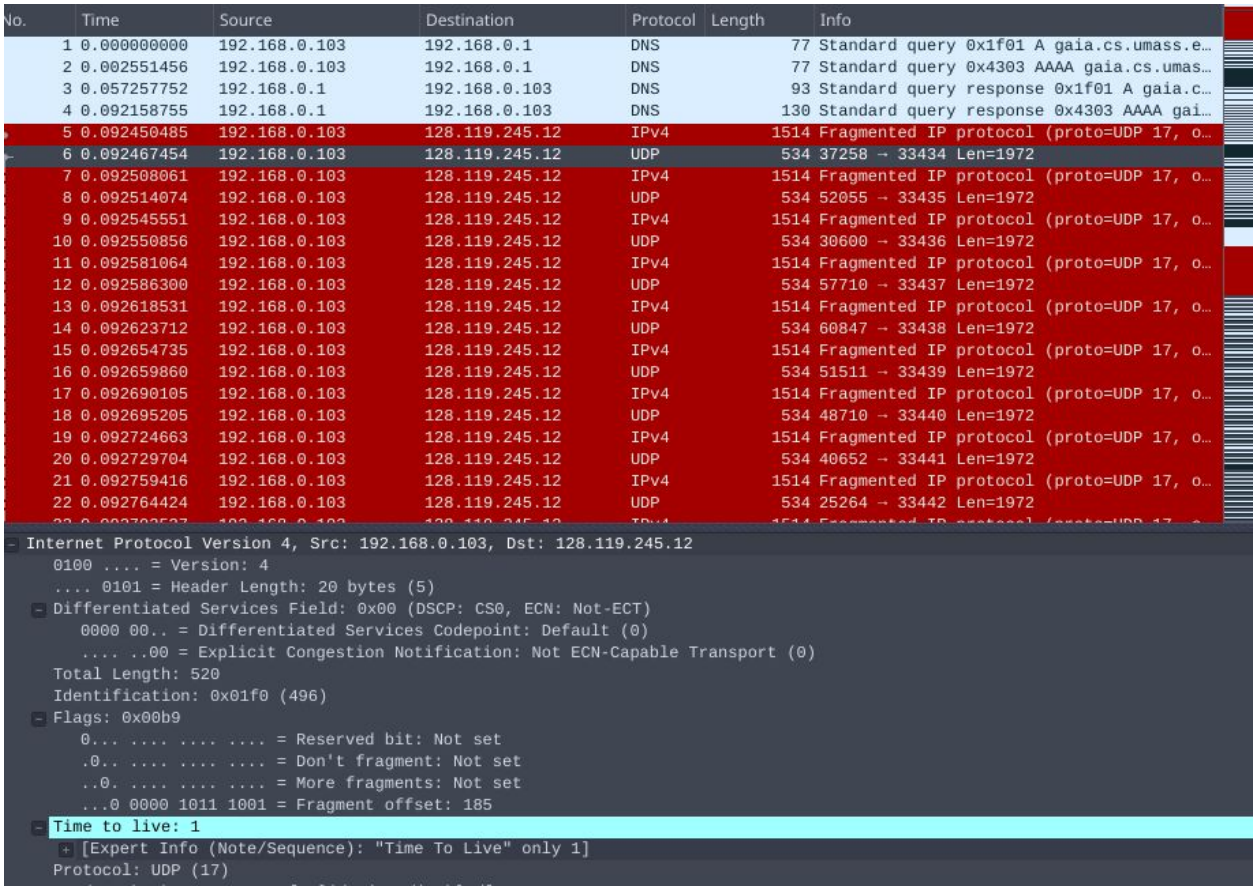
Lyndon Renaud
104 566 766
Computer Networks
Lab 3: IP

A Look at the Captured Trace



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.0.103	192.168.0.1	DNS	77	Standard query 0x1f01 A gaia.cs.umass.e…
2	0.002551456	192.168.0.103	192.168.0.1	DNS	77	Standard query 0x4303 AAAA gaia.cs.umas…
3	0.057257752	192.168.0.1	192.168.0.103	DNS	93	Standard query response 0x1f01 A gaia.c…
4	0.092158755	192.168.0.1	192.168.0.103	DNS	130	Standard query response 0x4303 AAAA gai…
5	0.092450485	192.168.0.103	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, o…
6	0.092467454	192.168.0.103	128.119.245.12	UDP	534	37258 → 33434 Len=1972
7	0.092508061	192.168.0.103	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, o…
8	0.092514074	192.168.0.103	128.119.245.12	UDP	534	52055 → 33435 Len=1972
9	0.092545551	192.168.0.103	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, o…
10	0.092550856	192.168.0.103	128.119.245.12	UDP	534	30600 → 33436 Len=1972
11	0.092581064	192.168.0.103	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, o…
12	0.092586300	192.168.0.103	128.119.245.12	UDP	534	57710 → 33437 Len=1972
13	0.092618531	192.168.0.103	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, o…
14	0.092623712	192.168.0.103	128.119.245.12	UDP	534	60847 → 33438 Len=1972
15	0.092654735	192.168.0.103	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, o…
16	0.092659860	192.168.0.103	128.119.245.12	UDP	534	51511 → 33439 Len=1972
17	0.092690105	192.168.0.103	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, o…
18	0.092695205	192.168.0.103	128.119.245.12	UDP	534	48710 → 33440 Len=1972
19	0.092724663	192.168.0.103	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, o…
20	0.092729704	192.168.0.103	128.119.245.12	UDP	534	40652 → 33441 Len=1972
21	0.092759416	192.168.0.103	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, o…
22	0.092764424	192.168.0.103	128.119.245.12	UDP	534	25264 → 33442 Len=1972

```
Internet Protocol Version 4, Src: 192.168.0.103, 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: 520
    Identification: 0x01f0 (496)
  Flags: 0x00b9
      0... .... .... .... = Reserved bit: Not set
      .0.. .... .... .... = Don't fragment: Not set
      ..0. .... .... .... = More fragments: Not set
      ...0 0000 1011 1001 = Fragment offset: 185
  Time to live: 1
    [Expert Info (Note/Sequence): "Time To Live" only 1]
    Protocol: UDP (17)
```

1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?
The IP address of my computer is 192.168.0.103.

2. Within the IP packet header, what is the value in the upper layer protocol field?
In the IP header, the value in the upper layer protocol field is UDP (17).

3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram ? Explain how you determined the number of payload bytes.
The IP header is 20 bytes. The total length is 520 bytes, so the payload of the IP datagram is 520-20=500 bytes.

4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.
The IP datagram has been fragmented. I can tell because under Flags, Fragment offset = 185.

5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?
The identification and time to live fields change from on datagram to the next.

6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?
Fields that stay constant are header length, source IP, destination IP, version, differentiated services field, and protocol. All these fields must stay constant because UDP header length is always the same, the source and destination IP does not change, and all packets are UDP IPv4. The fields that must change are identification, time to live, and checksum. These must change because each packet is identified uniquely, time to live must increment to perform traceroute, and checksum will be different as header values are different.

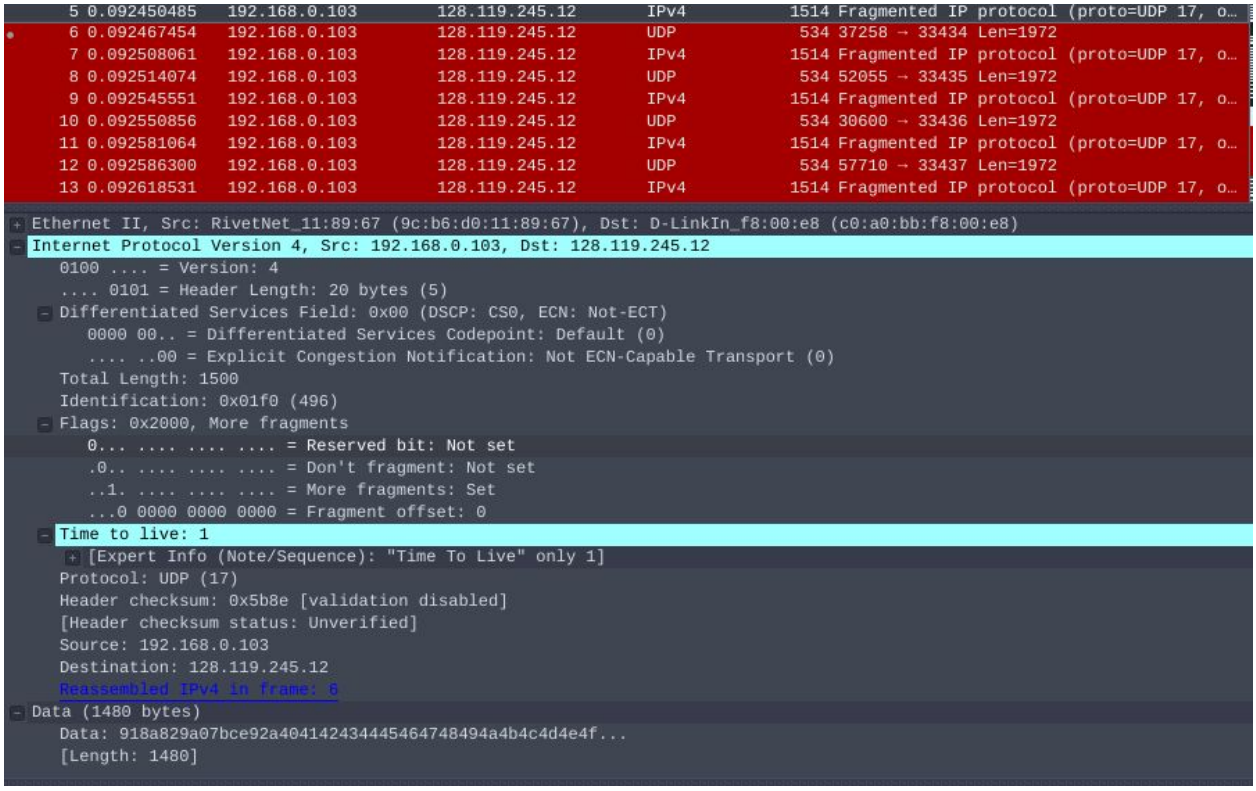
7. Describe the pattern you see in the values in the Identification field of the IP datagram.
The identification number goes up by 1 for the next packet.

8. What is the value in the Identification field and the TTL field?
Identification: 0x01f0 (496) TTL: 1

9. Do these values remain unchanged for all of the ICMP TTL - exceeded replies sent to your computer by the nearest (first hop) router? Why?
The value for identification changes but TTL does not. When a packet reaches a router, its TTL is decremented. This means all packets with TTL exceeded at the first hop must all have the same TTL.

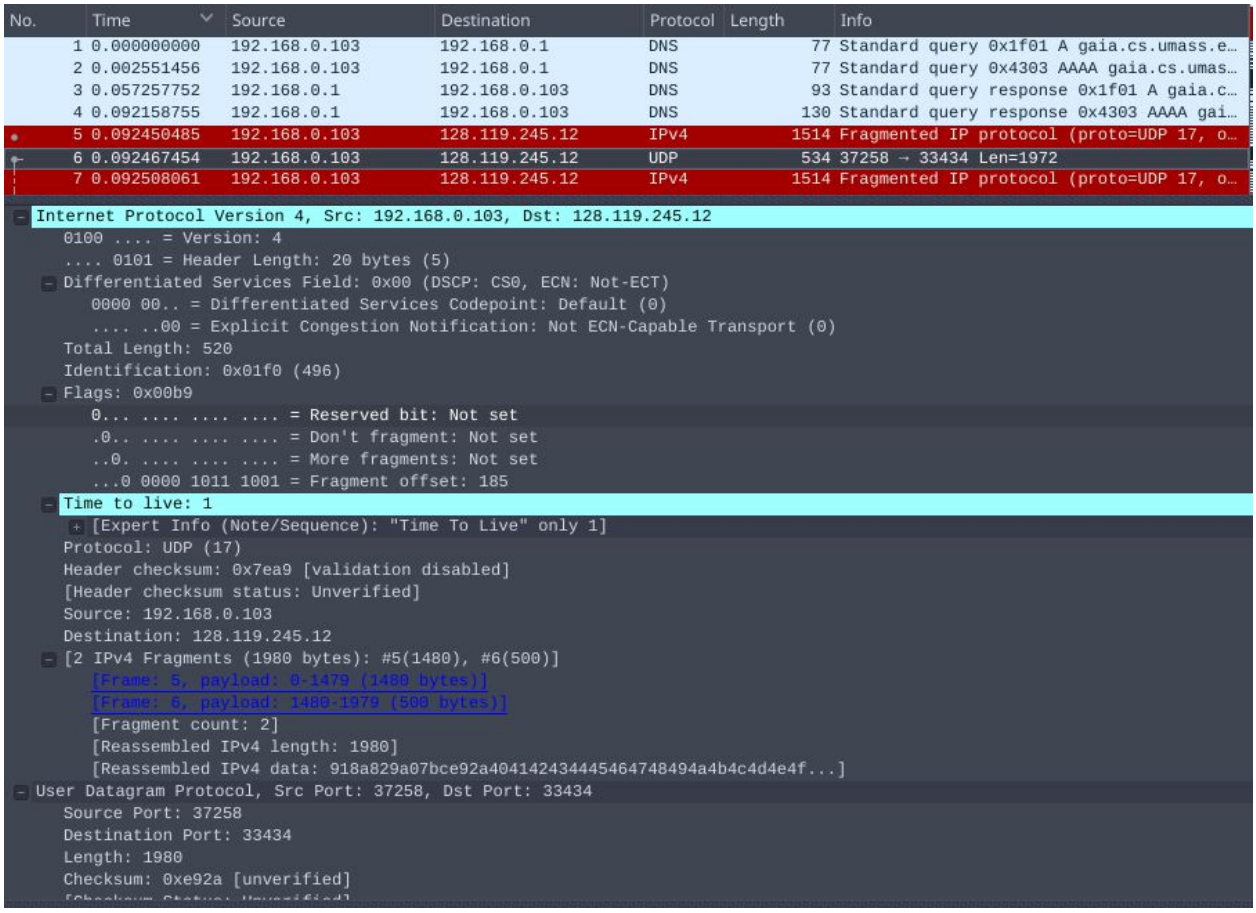
Fragmentation
10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?
The message has been fragmented across more than on IP datagram.

11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?



The flag bit for “More fragments” is set. This indicates the datagram is fragmented. The fragment offset is 0, meaning this packet is the first fragment. The IP datagram is 500 bytes.

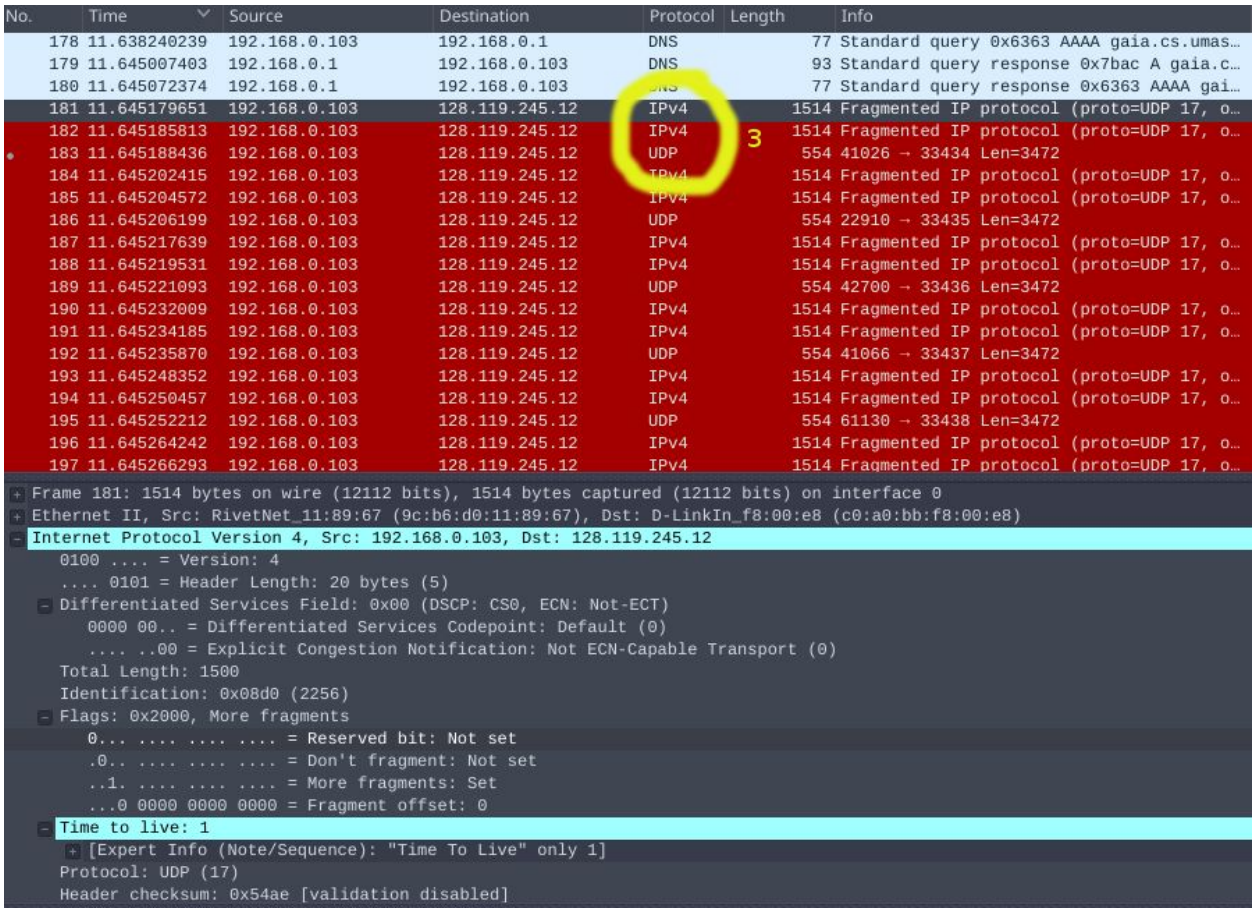
12. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?



The fragment offset > 0 indicates this is not the first fragment. Here the fragment offset is 185. There are no more fragments since the “more fragments” field is not set.

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

Fields that change are total length, more fragments, fragment offset, and checksum.



14. How many fragments were created from the original datagram?

Three fragments were created from the original datagram.

15. What fields change in the IP header among the fragments?

Fields that change are total length, more fragments, fragment offset, and checksum.