CS 372 Lab 3

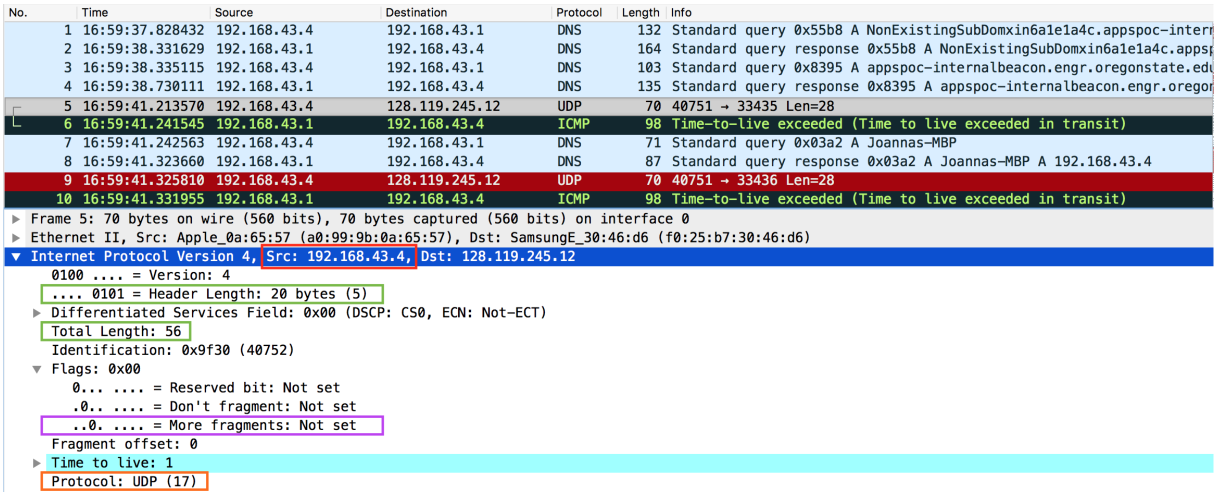
Joanna Lew

Summer 2017

Question 1

Q: 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?

A: The IP address of my computer is 192.168.53.4.



```
No.    Time             Source          Destination      Protocol  Length  Info
     1 16:59:37.828432  192.168.43.4    192.168.43.1     DNS       132 Standard query 0x55b8 A NonExistingSubDomxin6a1e1a4c.appspoc-intern
     2 16:59:38.331629  192.168.43.1    192.168.43.4     DNS       164 Standard query response 0x55b8 A NonExistingSubDomxin6a1e1a4c.appsp
     3 16:59:38.335115  192.168.43.4    192.168.43.1     DNS       103 Standard query 0x8395 A appspoc-internalbeacon.engr.oregonstate.edu
     4 16:59:38.730111  192.168.43.1    192.168.43.4     DNS       135 Standard query response 0x8395 A appspoc-internalbeacon.engr.oregon
     5 16:59:41.213570  192.168.43.4    128.119.245.12   UDP        70 40751 → 33435 Len=28
     6 16:59:41.241545  192.168.43.1    192.168.43.4     ICMP       98 Time-to-live exceeded (Time to live exceeded in transit)
     7 16:59:41.242563  192.168.43.4    192.168.43.1     DNS        71 Standard query 0x03a2 A Joannas-MBP
     8 16:59:41.323660  192.168.43.1    192.168.43.4     DNS        87 Standard query response 0x03a2 A Joannas-MBP A 192.168.43.4
     9 16:59:41.325810  192.168.43.4    128.119.245.12   UDP        70 40751 → 33436 Len=28
    10 16:59:41.331955  192.168.43.1    192.168.43.4     ICMP       98 Time-to-live exceeded (Time to live exceeded in transit)
▶ Frame 5: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
▶ Ethernet II, Src: Apple_0a:65:57 (a0:99:9b:0a:65:57), Dst: SamsungE_30:46:d6 (f0:25:b7:30:46:d6)
▼ Internet Protocol Version 4, Src: 192.168.43.4, 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: 0x9f30 (40752)
  ▼ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
  ▶ Time to live: 1
    Protocol: UDP (17)
```

Question 2

Q: Within the IP packet header, what is the value in the upper layer protocol field?

A: The value in the upper layer protocol field is UDP (17).
(See image from Question 1, orange box)

Question 3

Q: 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.

A: The IP header is 20 bytes. The payload is 36 bytes. To calculate the payload bytes, subtract the header length from the total length. Total Length − Header Length = 56 − 20 = 36 bytes.
(See image from Question 1, green boxes)

Question 4

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

A: No, the datagram has not been fragmented. The ”more fragments” Flag is set to 0.
(See image from Question 1, purple box)

Question 5

Q: Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?

A: The identification, time to live, and header checksum change from one datagram to the next.

Question 6

Q: Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

A: The following fields stay unchanged from one datagram to the next.

- Version should stay constant because we are using IPv4 for all packets.
- The source IP and destination IP should stay constant because we are using the same computer (source) to send to gaia.cs.umass.edu (destination).
- The Upper Layer Protocol should stay constant because traceroute passes the data to UDP.
- The Header Length is unchanged though doesn't have to be constant. IPv4 headers are typically 20 bytes but may be larger if the Options fields have been changed.
- The Differentiated Services field should stay constant because the packets are all the same type, and therefore use the same Type of Service.

The following fields must change from one datagram to the next.

- Identification is incremented for each datagram sent by the host since each datagram must have a unique ID.
- Time to live is decremented by one each time the datagram is processed by a router. This is to ensure that datagrams do not circulate forever in the network.
- Header Checksum is different for each datagram since if the header changes, the checksum also changes.

Question 7

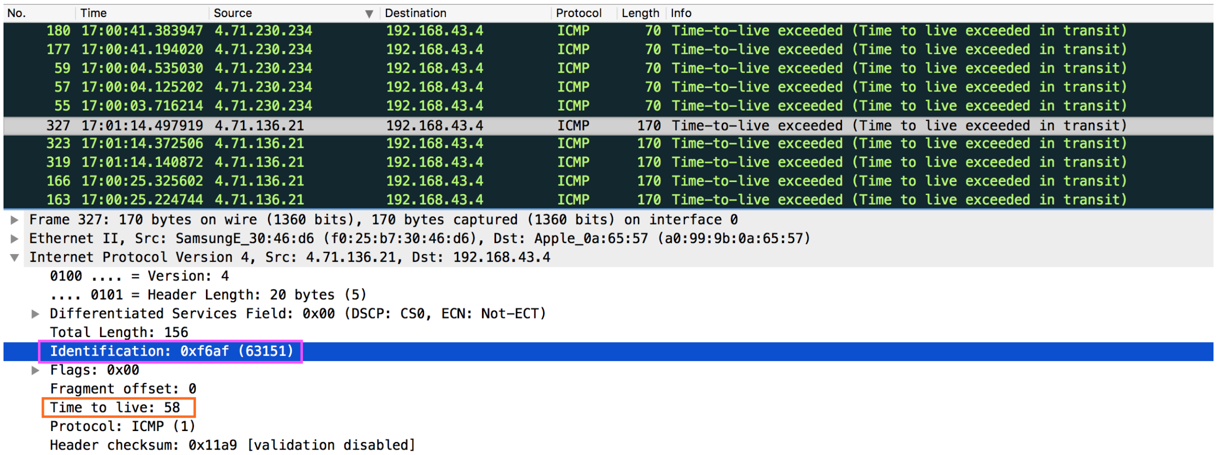
Q: Describe the pattern you see in the values in the Identification field of the IP datagram

A: The Identification field is incremented by one for each UDP packet sent by the host.

Question 8

Q: Find the series of ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router. What is the value in the Identification field and the TTL field?

A: The Identification field is 63151. The TTL field is 58.



No.	Time	Source	Destination	Protocol	Length	Info
180	17:00:41.383947	4.71.230.234	192.168.43.4	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
177	17:00:41.194020	4.71.230.234	192.168.43.4	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
59	17:00:04.535030	4.71.230.234	192.168.43.4	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
57	17:00:04.125202	4.71.230.234	192.168.43.4	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
55	17:00:03.716214	4.71.230.234	192.168.43.4	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
327	17:01:14.497919	4.71.136.21	192.168.43.4	ICMP	170	Time-to-live exceeded (Time to live exceeded in transit)
323	17:01:14.372506	4.71.136.21	192.168.43.4	ICMP	170	Time-to-live exceeded (Time to live exceeded in transit)
319	17:01:14.140872	4.71.136.21	192.168.43.4	ICMP	170	Time-to-live exceeded (Time to live exceeded in transit)
166	17:00:25.325602	4.71.136.21	192.168.43.4	ICMP	170	Time-to-live exceeded (Time to live exceeded in transit)
163	17:00:25.224744	4.71.136.21	192.168.43.4	ICMP	170	Time-to-live exceeded (Time to live exceeded in transit)

```
▶ Frame 327: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface 0
▶ Ethernet II, Src: SamsungE_30:46:d6 (f0:25:b7:30:46:d6), Dst: Apple_0a:65:57 (a0:99:9b:0a:65:57)
▼ Internet Protocol Version 4, Src: 4.71.136.21, Dst: 192.168.43.4
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 156
    Identification: 0xf6af (63151)
  ▶ Flags: 0x00
    Fragment offset: 0
    Time to live: 58
    Protocol: ICMP (1)
    Header checksum: 0x11a9 [validation disabled]
```

Question 9

Q: Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

A: The Identification field changes for each reply because each reply must have a unique identification. If two IP datagrams have the same ID, then they are fragments of the same larger IP datagram. The Time to Live (TTL) is the same for each reply because the TTL for the first hop router is the same.

Question 10

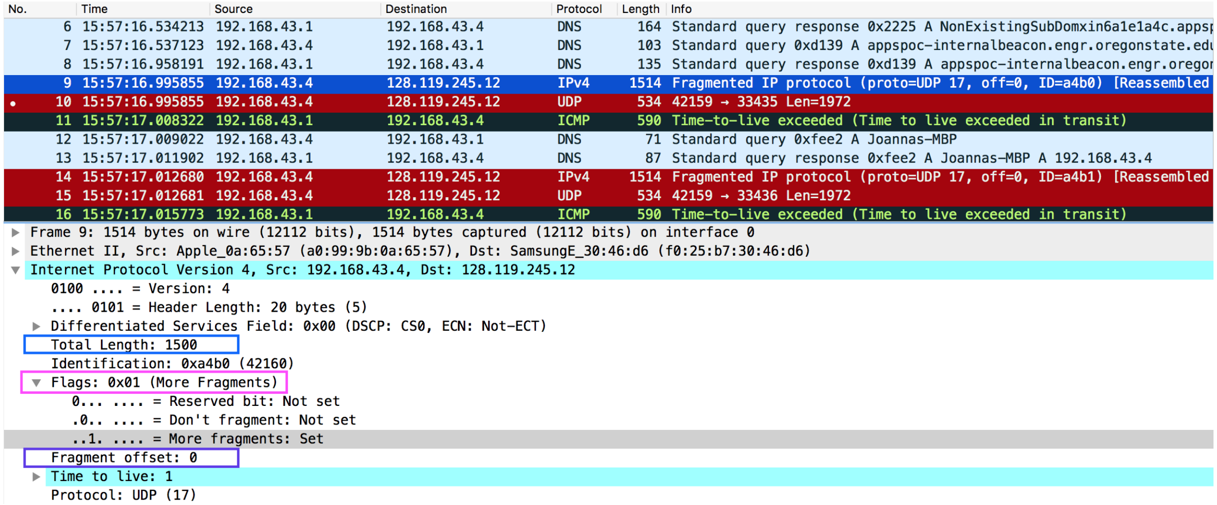
Q: Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?

A: Yes, the message was fragmented across more than one datagram.

Question 11

Q: Screenshot the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram has 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?

A: The "More Fragments" Flag is set, indicating that the datagram has been fragmented. A Fragment Offset value of 0 indicates that it is the first fragment. The IP datagram has a total length of 1500 bytes, of which 20 bytes are the header.

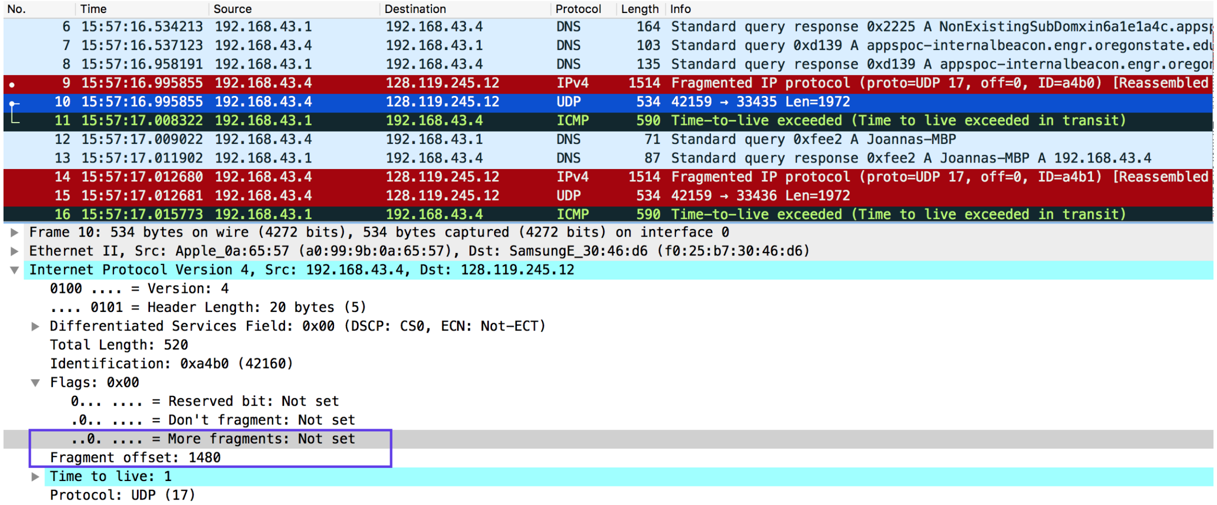


```
No.   Time             Source          Destination      Protocol  Length  Info
   6  15:57:16.534213  192.168.43.1    192.168.43.4     DNS        164  Standard query response 0x2225 A NonExistingSubDomxin6a1e1a4c.appsp
   7  15:57:16.537123  192.168.43.4    192.168.43.1     DNS        103  Standard query 0xd139 A appspoc-internalbeacon.engr.oregonstate.edu
   8  15:57:16.958191  192.168.43.1    192.168.43.4     DNS        135  Standard query response 0xd139 A appspoc-internalbeacon.engr.orego
   9  15:57:16.995855  192.168.43.4    128.119.245.12   IPv4      1514  Fragmented IP protocol (proto=UDP 17, off=0, ID=a4b0) [Reassembled
• 10  15:57:16.995855  192.168.43.4    128.119.245.12   UDP        534  42159 → 33435 Len=1972
  11  15:57:17.008322  192.168.43.1    192.168.43.4     ICMP       590  Time-to-live exceeded (Time to live exceeded in transit)
  12  15:57:17.009022  192.168.43.4    192.168.43.1     DNS         71  Standard query 0xfee2 A Joannas-MBP
  13  15:57:17.011902  192.168.43.1    192.168.43.4     DNS         87  Standard query response 0xfee2 A Joannas-MBP A 192.168.43.4
  14  15:57:17.012680  192.168.43.4    128.119.245.12   IPv4      1514  Fragmented IP protocol (proto=UDP 17, off=0, ID=a4b1) [Reassembled
  15  15:57:17.012681  192.168.43.4    128.119.245.12   UDP        534  42159 → 33436 Len=1972
  16  15:57:17.015773  192.168.43.1    192.168.43.4     ICMP       590  Time-to-live exceeded (Time to live exceeded in transit)
▶ Frame 9: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▶ Ethernet II, Src: Apple_0a:65:57 (a0:99:9b:0a:65:57), Dst: SamsungE_30:46:d6 (f0:25:b7:30:46:d6)
▼ Internet Protocol Version 4, Src: 192.168.43.4, 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: 0xa4b0 (42160)
  ▼ Flags: 0x01 (More Fragments)
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    Fragment offset: 0
  ▶ Time to live: 1
    Protocol: UDP (17)
```

Question 12

Q: Screenshot 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?

A: The Fragment Offset is 1480, indicating that 1480 bytes of data have been sent prior to the current fragment. Therefore, it must not be the first datagram fragment. There are no more fragments after the current fragment since the "More Fragments" Flag is not set.



```
No.   Time             Source          Destination      Protocol  Length  Info
   6  15:57:16.534213  192.168.43.1    192.168.43.4     DNS        164  Standard query response 0x2225 A NonExistingSubDomxin6a1e1a4c.appsp
   7  15:57:16.537123  192.168.43.4    192.168.43.1     DNS        103  Standard query 0xd139 A appspoc-internalbeacon.engr.oregonstate.edu
   8  15:57:16.958191  192.168.43.1    192.168.43.4     DNS        135  Standard query response 0xd139 A appspoc-internalbeacon.engr.orego
•  9  15:57:16.995855  192.168.43.4    128.119.245.12   IPv4      1514  Fragmented IP protocol (proto=UDP 17, off=0, ID=a4b0) [Reassembled
  10  15:57:16.995855  192.168.43.4    128.119.245.12   UDP        534  42159 → 33435 Len=1972
  11  15:57:17.008322  192.168.43.1    192.168.43.4     ICMP       590  Time-to-live exceeded (Time to live exceeded in transit)
  12  15:57:17.009022  192.168.43.4    192.168.43.1     DNS         71  Standard query 0xfee2 A Joannas-MBP
  13  15:57:17.011902  192.168.43.1    192.168.43.4     DNS         87  Standard query response 0xfee2 A Joannas-MBP A 192.168.43.4
  14  15:57:17.012680  192.168.43.4    128.119.245.12   IPv4      1514  Fragmented IP protocol (proto=UDP 17, off=0, ID=a4b1) [Reassembled
  15  15:57:17.012681  192.168.43.4    128.119.245.12   UDP        534  42159 → 33436 Len=1972
  16  15:57:17.015773  192.168.43.1    192.168.43.4     ICMP       590  Time-to-live exceeded (Time to live exceeded in transit)
▶ Frame 10: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface 0
▶ Ethernet II, Src: Apple_0a:65:57 (a0:99:9b:0a:65:57), Dst: SamsungE_30:46:d6 (f0:25:b7:30:46:d6)
▼ Internet Protocol Version 4, Src: 192.168.43.4, 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: 520
    Identification: 0xa4b0 (42160)
  ▼ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 1480
  ▶ Time to live: 1
    Protocol: UDP (17)
```

Question 13

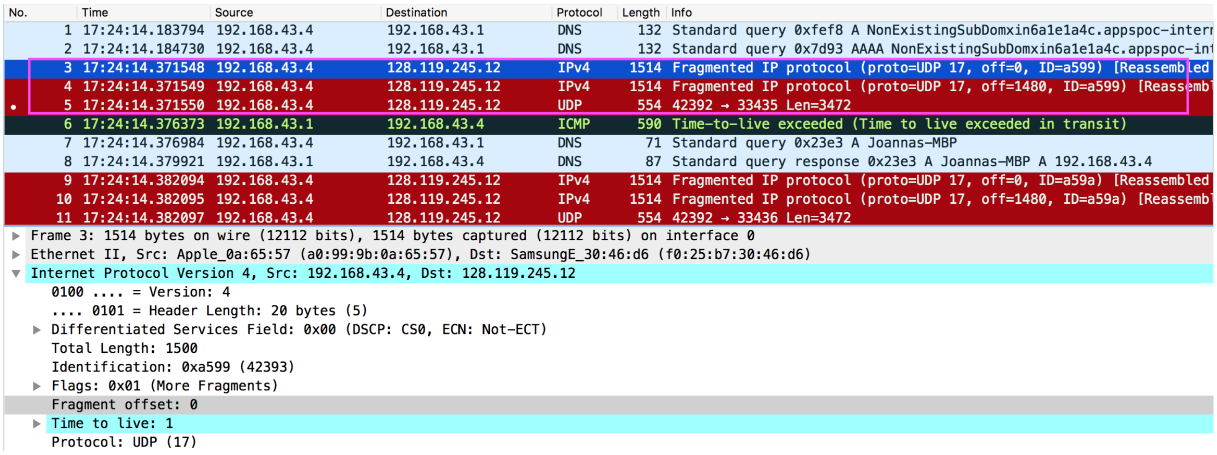
Q: What fields change in the IP header between the first and second fragment?

A: The Total Length, Flags, Fragment Offset, and Header Checksum are different for the two fragments.

Question 14

Q: Now find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 3500. How many fragments were created from the original datagram?

A: Three fragments were created.



```
No.    Time             Source          Destination      Protocol  Length  Info
     1 17:24:14.183794  192.168.43.4    192.168.43.1     DNS        132  Standard query 0xfef8 A NonExistingSubDomxin6a1e1a4c.appspoc-interr
     2 17:24:14.184730  192.168.43.4    192.168.43.1     DNS        132  Standard query 0x7d93 AAAA NonExistingSubDomxin6a1e1a4c.appspoc-int
     3 17:24:14.371548  192.168.43.4    128.119.245.12   IPv4      1514  Fragmented IP protocol (proto=UDP 17, off=0, ID=a599) [Reassembled
     4 17:24:14.371549  192.168.43.4    128.119.245.12   IPv4      1514  Fragmented IP protocol (proto=UDP 17, off=1480, ID=a599) [Reassembl
•    5 17:24:14.371550  192.168.43.4    128.119.245.12   UDP        554  42392 → 33435 Len=3472
     6 17:24:14.376373  192.168.43.1    192.168.43.4     ICMP       590  Time-to-live exceeded (Time to live exceeded in transit)
     7 17:24:14.376984  192.168.43.4    192.168.43.1     DNS         71  Standard query 0x23e3 A Joannas-MBP
     8 17:24:14.379921  192.168.43.1    192.168.43.4     DNS         87  Standard query response 0x23e3 A Joannas-MBP A 192.168.43.4
     9 17:24:14.382094  192.168.43.4    128.119.245.12   IPv4      1514  Fragmented IP protocol (proto=UDP 17, off=0, ID=a59a) [Reassembled
    10 17:24:14.382095  192.168.43.4    128.119.245.12   IPv4      1514  Fragmented IP protocol (proto=UDP 17, off=1480, ID=a59a) [Reassembl
    11 17:24:14.382097  192.168.43.4    128.119.245.12   UDP        554  42392 → 33436 Len=3472
▶ Frame 3: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▶ Ethernet II, Src: Apple_0a:65:57 (a0:99:9b:0a:65:57), Dst: SamsungE_30:46:d6 (f0:25:b7:30:46:d6)
▼ Internet Protocol Version 4, Src: 192.168.43.4, 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: 0xa599 (42393)
  ▶ Flags: 0x01 (More Fragments)
    Fragment offset: 0
  ▶ Time to live: 1
    Protocol: UDP (17)
```

Question 15

Q: What fields change in the IP header among the fragments?

A: The Total Length and Flags are the same for the first two packets but different for the third. The Fragment Offset and Header Checksum are different for all three fragments.

	Packet 1	Packet 2	Packet 3
Total Length	1500	1500	540
Flags	0x01	0x01	0x00
Fragment Offsest	0	1480	2960
Header Checksum	0x8d47	0x8c8e	0xaf95