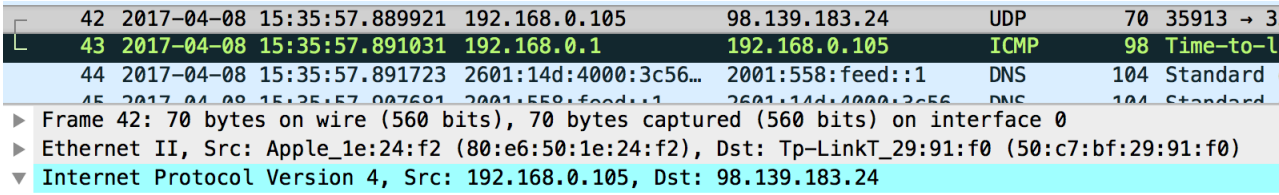
Wireshark Lab #3: IP

Suyi Liu, Yuan Jing Vincent Yan

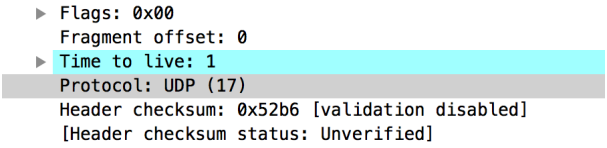
April 8, 2017

Problem 1



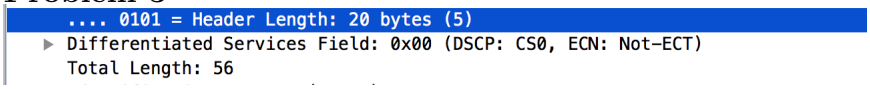
As shown, the private IP address is 192.168.0.105. (By the way, the public IP address is 66.249.76.29)

Problem 2



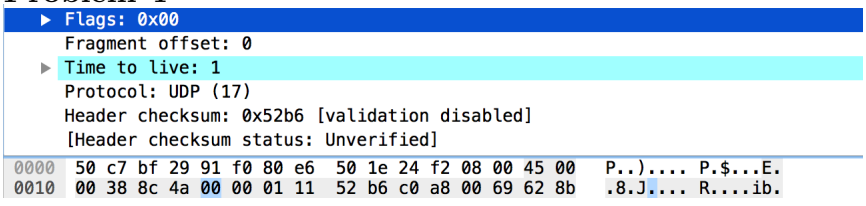
The value in the upper layer protocol field is 17 (UDP).

Problem 3



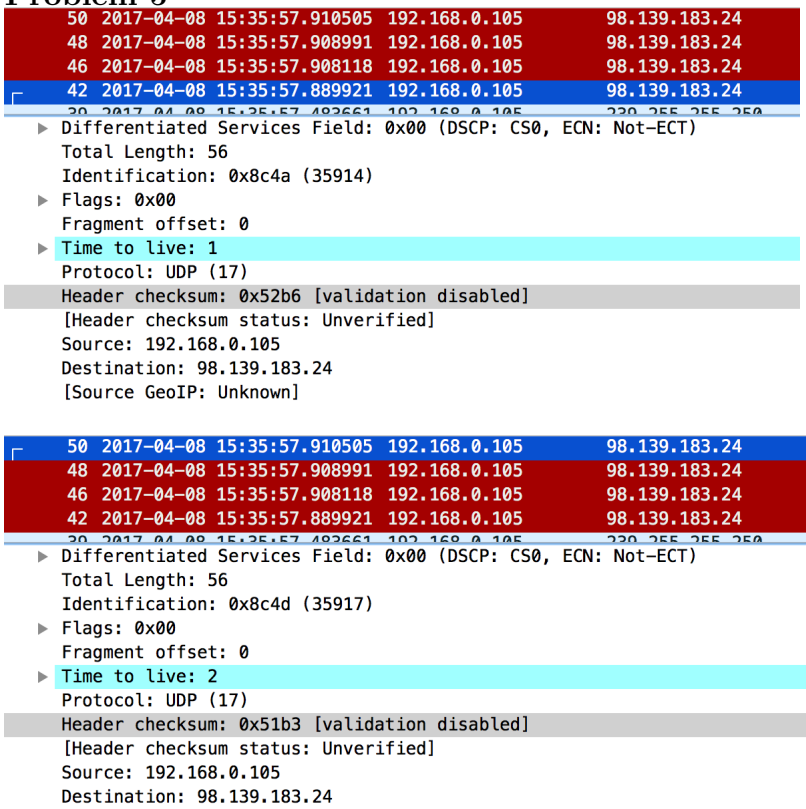
20 bytes are in the IP header. 36 bytes are in the payload of the IP datagram. Since the total length of the packet is 56 bytes, the payload is 56 - 20 = 36 bytes.

Problem 4



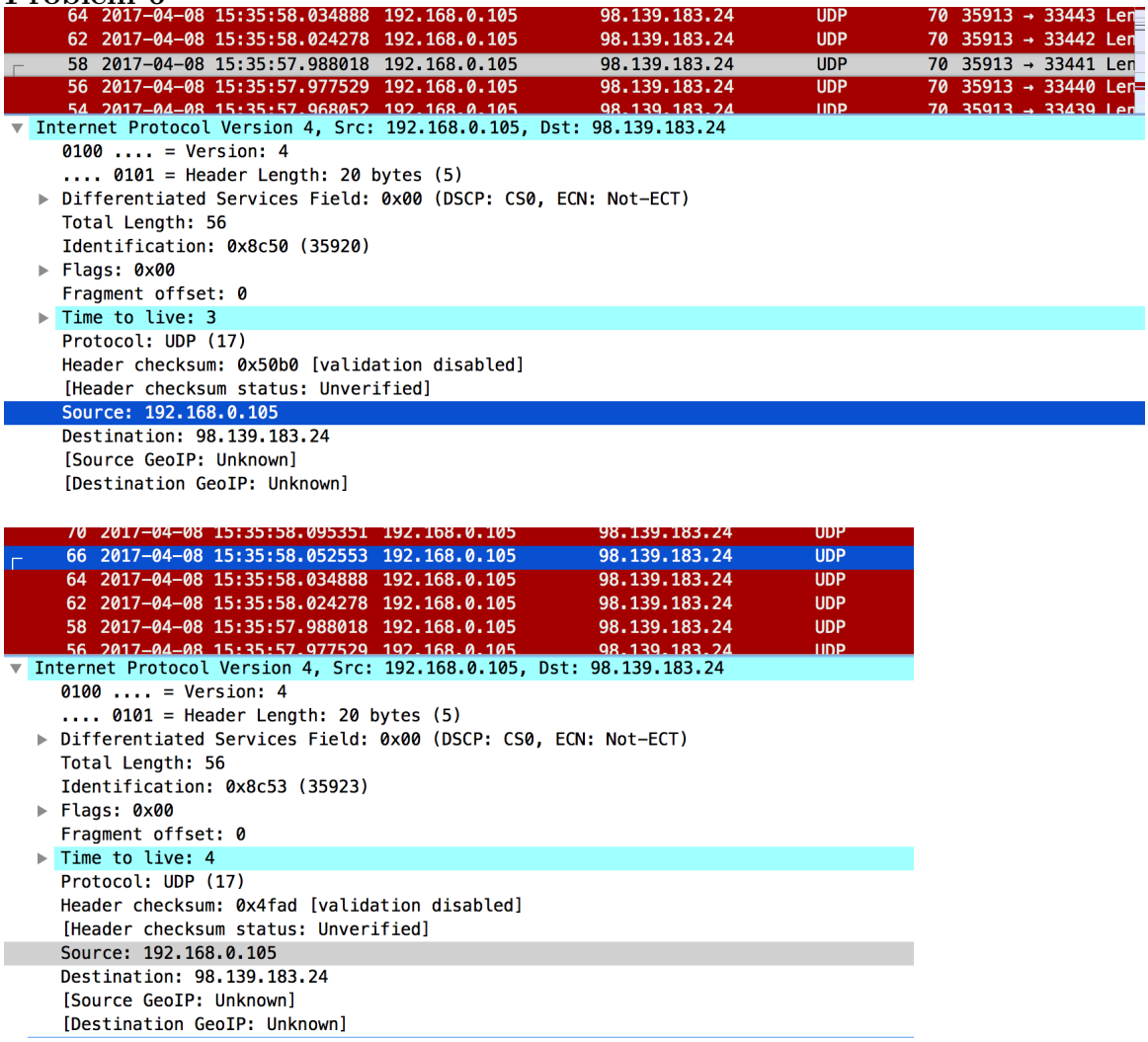
This IP datagram has not been fragmented, because by examining the packet we see that the fragmentation offset is 0 and the flag bit set to 0, indicating that this is the one and only fragment.

Problem 5



As shown, identification and header checksum always change from one datagram to the next. The time-to-live field actually changes every three datagrams, due to the way *traceroute* works.

Problem 6



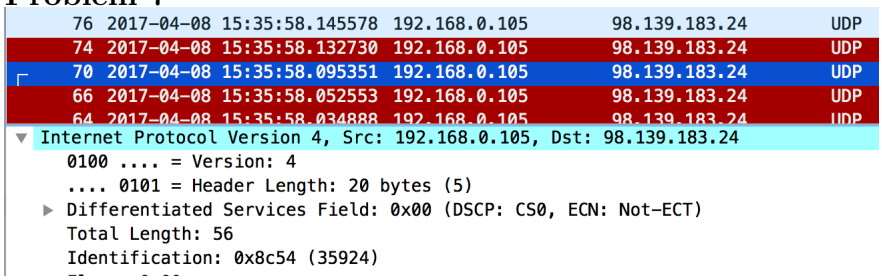
As shown, Fields that stay constant:
Version(IPv4 as always), Header Length(20 bytes), Differentiated Services Field(always same type of service), Potocol(all of them are UDP packets), Source IP(sending from same IP address), Destination IP(sending to same IP address)

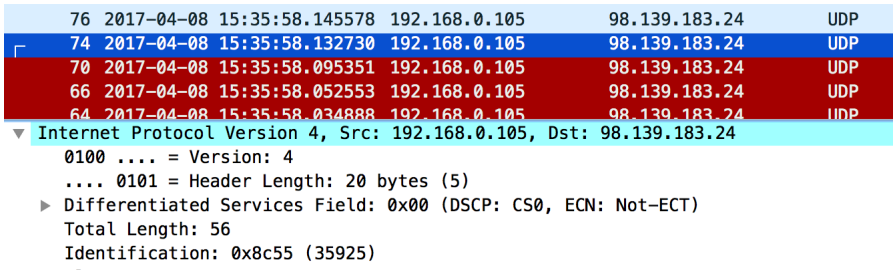
Fields must stay constant:
Version(IPv4 as always), Header Length(20 bytes), Differentiated Services Field(always same type of service), Potocol(all of them are UDP packets), Source IP(sending from same IP address), Destination IP(sending to same IP address)

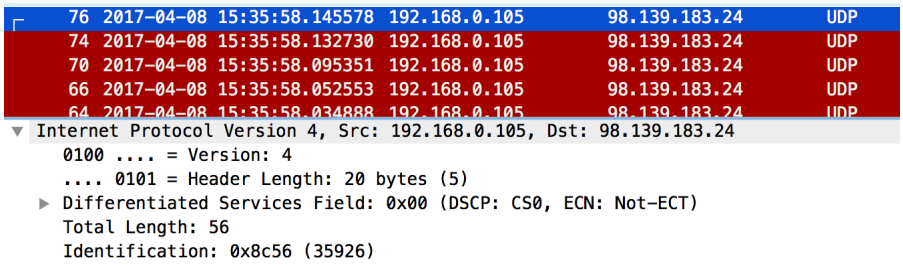
Fields must change:
Identification(Different packet have different IDs), Time to live(Traceroute pro-

gram increments TTL), Header checksum(since headers must change)

Problem 7

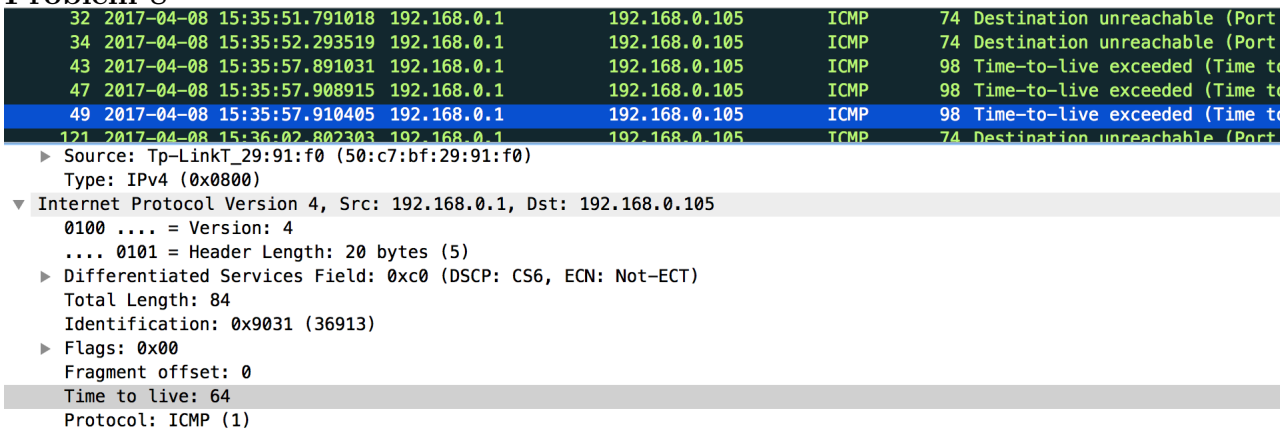






The pattern: the values in the Identification field of the IP datagram increases over time.

Problem 8



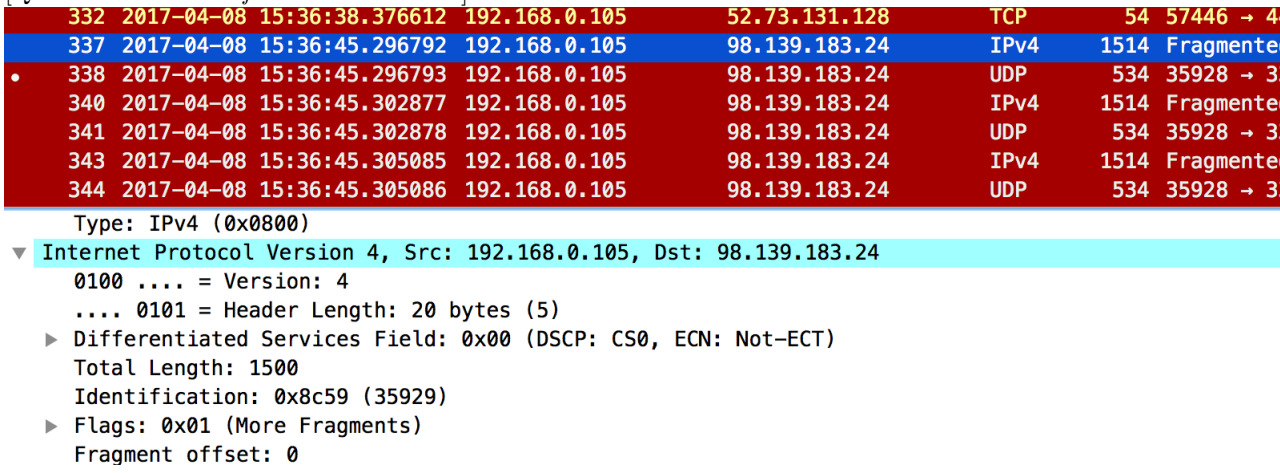
For the first ICMP TTL-exceeded reply,
Identification field: 36913; TTL field: 64

Problem 9

The Identification field changes for the ICMP TTL-exceeded replies because the identification field must be unique, unless they are fragments of a single large IP datagram.
The TTL field remains unchanged since TTL field by the first hop router are always set the same.

Problem 10

[*Question: Find the first ICMP Echo...*]



Yes, this message has been fragmented, since its flag bit is set to 1.

Problem 11

[*Question: Print out the first fragment...*]

```
    337 2017-04-08 15:36:45.296792    192.168.0.105         98.139.183.24         IPv4     1514
Fragmented IP protocol (proto=UDP 17, off=0, ID=8c59) [Reassembled in #338]
Frame 337: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
    Interface id: 0 (en0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr  8, 2017 15:36:45.296792000 EDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1491680205.296792000 seconds
    [Time delta from previous captured frame: 0.000917000 seconds]
    [Time delta from previous displayed frame: 0.000917000 seconds]
    [Time since reference or first frame: 62.180074000 seconds]
    Frame Number: 337
    Frame Length: 1514 bytes (12112 bits)
    Capture Length: 1514 bytes (12112 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:data]
    [Coloring Rule Name: TTL low or unexpected]
    [Coloring Rule String: ( ! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst ==
224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !(vrrp || carp))]
Ethernet II, Src: Apple_1e:24:f2 (80:e6:50:1e:24:f2), Dst: Tp-LinkT_29:91:f0 (50:c7:bf:29:91:f0)
    Destination: Tp-LinkT_29:91:f0 (50:c7:bf:29:91:f0)
    Source: Apple_1e:24:f2 (80:e6:50:1e:24:f2)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 98.139.183.24
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x8c59 (35929)
    Flags: 0x01 (More Fragments)
    Fragment offset: 0
    Time to live: 1
    Protocol: UDP (17)
    Header checksum: 0x2d03 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.105
    Destination: 98.139.183.24
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
    Reassembled IPv4 in frame: 338
Data (1480 bytes)
```

In the IP header, a flag bit of 1 indicates that the datagram been fragmented. A fragmentation offset of 0 indicates that this is the first fragment. This IP datagram is 1500 bytes long, including the header.

Problem 10

[*Question: Print out the second fragment...*]

```
      338 2017-04-08 15:36:45.296793    192.168.0.105         98.139.183.24         UDP      534
  35928 → 33435 Len=1972
  Frame 338: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface 0
      Interface id: 0 (en0)
      Encapsulation type: Ethernet (1)
      Arrival Time: Apr  8, 2017 15:36:45.296793000 EDT
      [Time shift for this packet: 0.000000000 seconds]
      Epoch Time: 1491680205.296793000 seconds
      [Time delta from previous captured frame: 0.000001000 seconds]
      [Time delta from previous displayed frame: 0.000001000 seconds]
      [Time since reference or first frame: 62.180075000 seconds]
      Frame Number: 338
      Frame Length: 534 bytes (4272 bits)
      Capture Length: 534 bytes (4272 bits)
      [Frame is marked: False]
      [Frame is ignored: False]
      [Protocols in frame: eth:ethertype:ip:udp:data]
      [Coloring Rule Name: TTL low or unexpected]
      [Coloring Rule String: ( ! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst ==
  224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !(vrrp || carp))]
  Ethernet II, Src: Apple_1e:24:f2 (80:e6:50:1e:24:f2), Dst: Tp-LinkT_29:91:f0 (50:c7:bf:29:91:f0)
      Destination: Tp-LinkT_29:91:f0 (50:c7:bf:29:91:f0)
      Source: Apple_1e:24:f2 (80:e6:50:1e:24:f2)
      Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 192.168.0.105, Dst: 98.139.183.24
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
      Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 520
      Identification: 0x8c59 (35929)
      Flags: 0x00
      Fragment offset: 1480
      Time to live: 1
      Protocol: UDP (17)
      Header checksum: 0x501e [validation disabled]
      [Header checksum status: Unverified]
      Source: 192.168.0.105
      Destination: 98.139.183.24
      [Source GeoIP: Unknown]
      [Destination GeoIP: Unknown]
      [2 IPv4 Fragments (1980 bytes): #337(1480), #338(500)]
  User Datagram Protocol, Src Port: 35928, Dst Port: 33435
  Data (1972 bytes)
```

In the IP header, fragmentation offset of 1480 indicates that this is not the first datagram fragment. There are no more fragments, since the flag bit is set to 0 here.

Problem 11

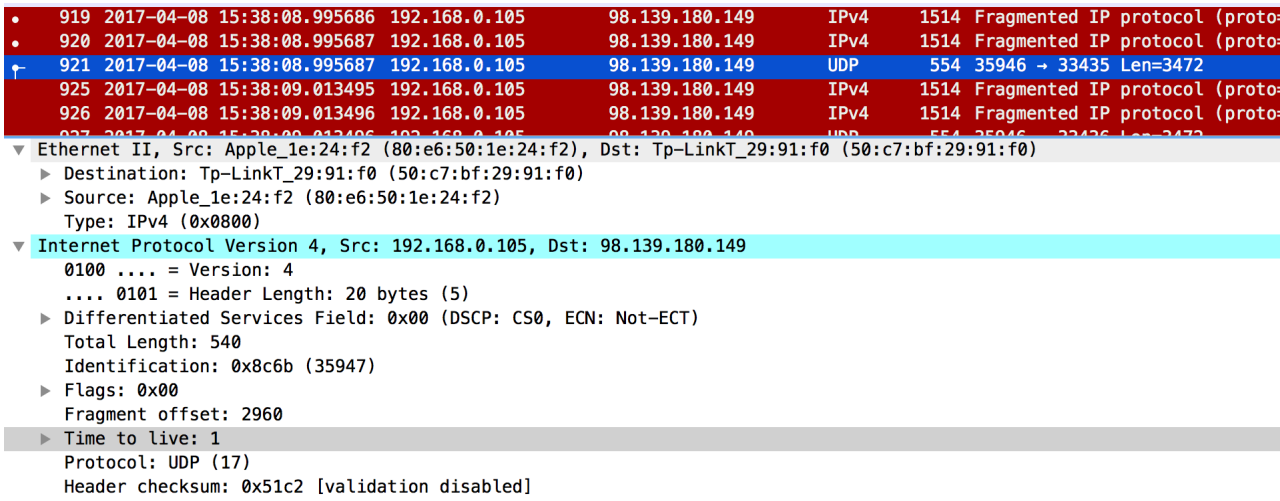
[*Question: What fields change in the IP header...*]

As shown in the previous print outs, total length, offset, flags, and header checksum fields change in the IP header between the first and second fragment.

Problem 12

```
    919 2017-04-08 15:38:08.995686 192.168.0.105   98.139.180.149   IPv4   1514 Fragmented IP protocol (proto=
    920 2017-04-08 15:38:08.995687 192.168.0.105   98.139.180.149   IPv4   1514 Fragmented IP protocol (proto=
•   921 2017-04-08 15:38:08.995687 192.168.0.105   98.139.180.149   UDP     554 35946 → 33435 Len=3472
    925 2017-04-08 15:38:09.013495 192.168.0.105   98.139.180.149   IPv4   1514 Fragmented IP protocol (proto=
    926 2017-04-08 15:38:09.013496 192.168.0.105   98.139.180.149   IPv4   1514 Fragmented IP protocol (proto=
    927 2017-04-08 15:38:09.013496 192.168.0.105   98.139.180.149   UDP     554 35946 → 33436 Len=3472
▼ Ethernet II, Src: Apple_1e:24:f2 (80:e6:50:1e:24:f2), Dst: Tp-LinkT_29:91:f0 (50:c7:bf:29:91:f0)
  ▶ Destination: Tp-LinkT_29:91:f0 (50:c7:bf:29:91:f0)
  ▶ Source: Apple_1e:24:f2 (80:e6:50:1e:24:f2)
    Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 192.168.0.105, Dst: 98.139.180.149
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x8c6b (35947)
  ▶ Flags: 0x01 (More Fragments)
    Fragment offset: 0
  ▶ Time to live: 1
    Protocol: UDP (17)
    Header checksum: 0x2f74 [validation disabled]
```

```
    919 2017-04-08 15:38:08.995686 192.168.0.105   98.139.180.149   IPv4   1514 Fragmented IP protocol (proto=
    920 2017-04-08 15:38:08.995687 192.168.0.105   98.139.180.149   IPv4   1514 Fragmented IP protocol (proto=
•   921 2017-04-08 15:38:08.995687 192.168.0.105   98.139.180.149   UDP     554 35946 → 33435 Len=3472
    925 2017-04-08 15:38:09.013495 192.168.0.105   98.139.180.149   IPv4   1514 Fragmented IP protocol (proto=
    926 2017-04-08 15:38:09.013496 192.168.0.105   98.139.180.149   IPv4   1514 Fragmented IP protocol (proto=
▼ Ethernet II, Src: Apple_1e:24:f2 (80:e6:50:1e:24:f2), Dst: Tp-LinkT_29:91:f0 (50:c7:bf:29:91:f0)
  ▶ Destination: Tp-LinkT_29:91:f0 (50:c7:bf:29:91:f0)
  ▶ Source: Apple_1e:24:f2 (80:e6:50:1e:24:f2)
    Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 192.168.0.105, Dst: 98.139.180.149
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x8c6b (35947)
  ▶ Flags: 0x01 (More Fragments)
    Fragment offset: 1480
  ▶ Time to live: 1
    Protocol: UDP (17)
    Header checksum: 0x2ebb [validation disabled]
```



As shown above, 3 fragments were created from the original datagram.

Problem 13

Please look at the screenshots from **Problem 12** for reference. Fragmentation offset, flag bit(changes between the second last fragment and the last one), header checksum and total length(changes between the second last fragment and the last one) change among the fragments.