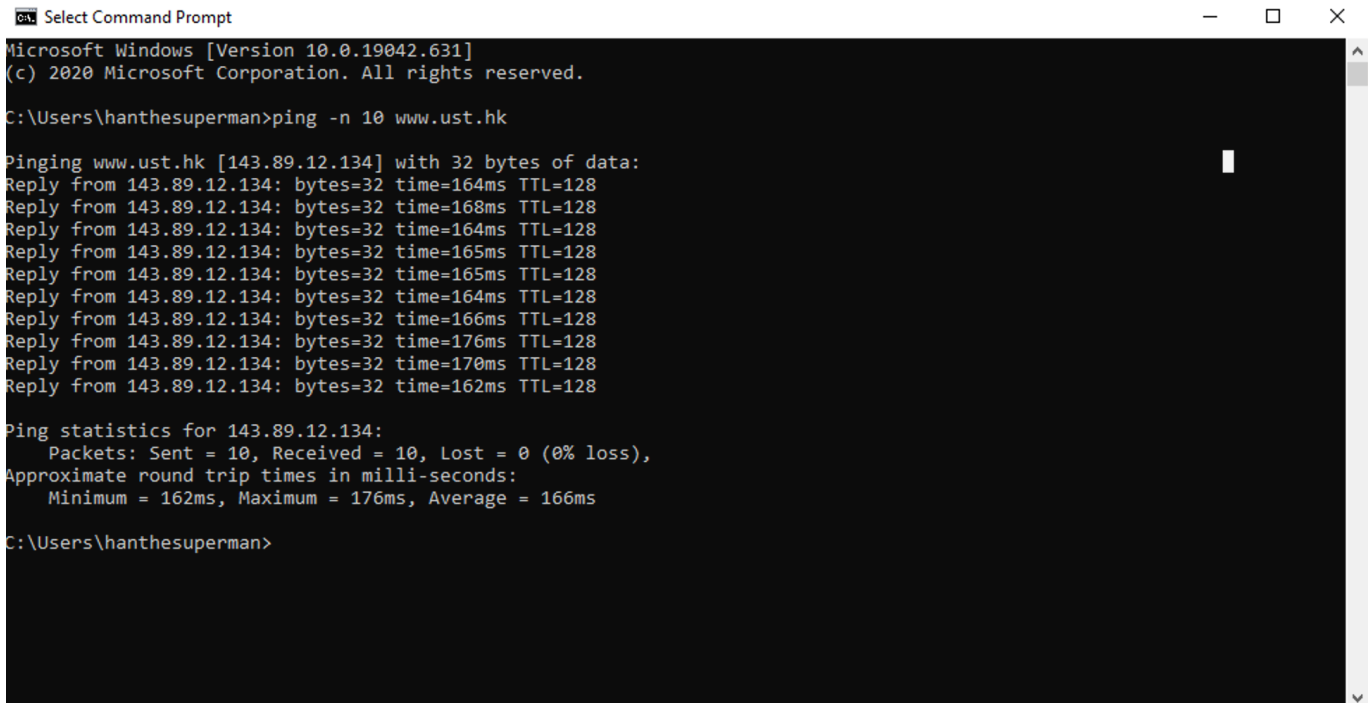


# ECS 152A - Project 1 - ICMP Wireshark Lab

Han Nguyen (917278789) & Blake McMurray (999162729)

1/17/20

## 1 ICMP and Ping



```
Select Command Prompt
Microsoft Windows [Version 10.0.19042.631]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\hanthesuperman>ping -n 10 www.ust.hk

Pinging www.ust.hk [143.89.12.134] with 32 bytes of data:
Reply from 143.89.12.134: bytes=32 time=164ms TTL=128
Reply from 143.89.12.134: bytes=32 time=168ms TTL=128
Reply from 143.89.12.134: bytes=32 time=164ms TTL=128
Reply from 143.89.12.134: bytes=32 time=165ms TTL=128
Reply from 143.89.12.134: bytes=32 time=165ms TTL=128
Reply from 143.89.12.134: bytes=32 time=164ms TTL=128
Reply from 143.89.12.134: bytes=32 time=166ms TTL=128
Reply from 143.89.12.134: bytes=32 time=176ms TTL=128
Reply from 143.89.12.134: bytes=32 time=170ms TTL=128
Reply from 143.89.12.134: bytes=32 time=162ms TTL=128

Ping statistics for 143.89.12.134:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 162ms, Maximum = 176ms, Average = 166ms

C:\Users\hanthesuperman>
```

Figure 1: Screenshot of the *ping* command in Command Prompt

No.	Time	Source	Destination	Protocol	Length	Info
4	0.148265	10.211.55.3	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=128 (reply in 5)
Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{4FC1B0C6-DEFD-4172-8260-8DA1C738ED37}, id 0						
Ethernet II, Src: Parallel_c1:9a:54 (00:1c:42:c1:9a:54), Dst: Parallel_00:00:18 (00:1c:42:00:00:18)						
Internet Protocol Version 4, Src: 10.211.55.3, Dst: 143.89.12.134						
Internet Control Message Protocol						
Type: 8 (Echo (ping) request)						
Code: 0						
Checksum: 0x4d45 [correct]						
[Checksum Status: Good]						
Identifier (BE): 1 (0x0001)						
Identifier (LE): 256 (0x0100)						
Sequence Number (BE): 22 (0x0016)						
Sequence Number (LE): 5632 (0x1600)						
[Response frame: 5]						
Data (32 bytes)						
0000	61	62	63	64	65	66 67 68 69 6a 6b 6c 6d 6e 6f 70 abcdefghijklmnop
0010	71	72	73	74	75	76 77 61 62 63 64 65 66 67 68 69 qrstuvwabcdefghi

Figure 2: Packet of ICMP Ping Request Message

## Question 1

The IP address of the host (source) is 10.211.55.3. The IP address of the destination is 143.89.12.134, as shown in Figure 2.

## Question 2

An ICMP packet does not have source and destination port numbers because the ICMP is used to communicate network-layer datagrams and information between the hosts and routers, while the ports are used to communicate between application layer processes. (Source: <http://www.cs.toronto.edu/~ahchinaei/teaching/2016jan/csc358/Assignment4wSol.pdf>)

## Question 3

From the Figure 2 above, it can be observed that the ICMP type number is 8 and the code number is 0. The other fields that the ICMP packet has is the checksum, identifier, sequence number and data size. The number bytes in checksum, sequence number and identifier are 2 bytes in each field.

## Question 4

The corresponding ping reply packet is as below:

```
No.      Time            Source            Destination      Protocol Length Info
  5 0.312683      143.89.12.134      10.211.55.3      ICMP          74      Echo (ping) reply  id=0x0001, seq=22/5632, ttl=128
(request in 4)
Frame 5: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{4FC1B0C6-DEFD-4172-8260-8DA1C738ED37}, id 0
Ethernet II, Src: Parallel_00:00:18 (00:1c:42:00:00:18), Dst: Parallel_c1:9a:54 (00:1c:42:c1:9a:54)
Internet Protocol Version 4, Src: 143.89.12.134, Dst: 10.211.55.3
Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x5545 [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 22 (0x0016)
  Sequence Number (LE): 5632 (0x1600)
  [Request frame: 4]
  [Response time: 164.418 ms]
  Data (32 bytes)
0000  61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70  abcdefghijklmnop
0010  71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi
```

Figure 3: Packet of ICMP Ping Reply Message

From the Figure 3 above, it can be observed that the ICMP type number is 0 and the code number is 0.

The other fields that the ICMP packet has is the checksum, identifier, sequence number and data size.

The number bytes in checksum, sequence number and identifier are 2 bytes in each field.

## 2 ICMP and Traceroute

As shown in Figure 4, my Mac/Linux Terminal was having issue with *traceroute* command, leading to the fact that there will be no Echo (ping) request or reply packets, so I will use the author's Wireshark *icmp-ethereal-trace-2*.

```
hanthesuperman — traceroute www.inria.fr — 139x43
Last login: Tue Jan 19 17:48:13 on ttys000

The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
HanMBP:~ hanthesuperman$ traceroute www.inria.fr
traceroute to inria.fr (128.93.162.83), 64 hops max, 52 byte packets
 1 * * *
 2 96.120.14.197 (96.120.14.197) 42.196 ms 140.756 ms 31.456 ms
 3 96.110.159.205 (96.110.159.205) 79.289 ms 23.456 ms 46.033 ms
 4 ae-2-ar01.sacramento.ca.ccal.comcast.net (162.151.18.133) 24.201 ms 34.315 ms 48.824 ms
 5 be-36431-cs03.sunnyvale.ca.ibone.comcast.net (96.110.41.105) 32.082 ms 27.949 ms
   be-36421-cs02.sunnyvale.ca.ibone.comcast.net (96.110.41.101) 36.401 ms
 6 be-1112-cr12.sunnyvale.ca.ibone.comcast.net (96.110.46.6) 55.375 ms 62.759 ms
   be-1412-cr12.sunnyvale.ca.ibone.comcast.net (96.110.46.42) 15.988 ms
 7 be-301-cr01.9greateoaks.ca.ibone.comcast.net (96.110.37.170) 114.719 ms
   be-304-cr01.9greateoaks.ca.ibone.comcast.net (96.110.37.182) 50.729 ms
   be-302-cr01.9greateoaks.ca.ibone.comcast.net (96.110.37.174) 77.513 ms
 8 be-2312-pe12.9greateoaks.ca.ibone.comcast.net (96.110.33.42) 27.153 ms 17.168 ms 43.255 ms
 9 ae7.cr3-sjc1.ip4.gtt.net (209.120.154.117) 165.303 ms 123.754 ms 41.973 ms
10 et-3-3-0.cr4-par7.ip4.gtt.net (213.200.119.214) 795.654 ms 157.746 ms 177.066 ms
11 renater-gw-ix1.gtt.net (77.67.123.206) 185.431 ms 188.870 ms 182.528 ms
12 * * *
13 inria-rocquencourt-gi3-2-inria-rtr-021.noc.renater.fr (193.51.184.177) 461.375 ms 241.458 ms 205.912 ms
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
```

Figure 4: Mac/Linux Terminal when *traceroute* to *www.inria.fr*

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping)

request id=0x0200, seq=41985/420, ttl=1 (no response found!)

Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)

Ethernet II, Src: Dell\_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG\_da:af:73 (00:06:25:da:af:73)

Internet Protocol Version 4, Src: 192.168.1.101, Dst: 138.96.146.2

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 92

Identification: 0xd2d5 (53973)

Flags: 0x00

Fragment Offset: 0

Time to Live: 1

Protocol: ICMP (1)

Header Checksum: 0x085c [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.101

Destination Address: 138.96.146.2

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x51fe [correct]

[Checksum Status: Good]

Identifier (BE): 512 (0x0200)

Identifier (LE): 2 (0x0002)

Sequence Number (BE): 41985 (0xa401)

Sequence Number (LE): 420 (0x01a4)

[No response seen]

Data (64 bytes)

```

0000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....

```

Figure 5: ICMP Packet information from the author's Wireshark

### Question 5

Based on the Figure 5, the IP address of the source host is 192.168.1.101, and the IP address of the destination host is 138.96.146.2

### Question 6

If the ICMP sent UDP packets instead, the IP protocol number is not 01. Rather, it will become 17 in decimal or 0x11 in hexa.

### Question 7

There is no difference in the content of the query fields compared to the first lab.

### Question 8

As shown in Figure 6, the ICMP error packet has an extra field of Internet Control Message Protocol, an extra header checksum and the unused 8 bytes that the error is generated compared to the original Echo (ping) request packet.

### Question 9

Based on the last three Echo (ping) reply packets, they are different from the ICMP error packets in the field of Type. Echo (ping) reply packets have type 0, while ICMP error packets have type 11.

The reason for this difference is that when the packets are sent through routers, the Time-to-Live (TTL) determines the number of packets that are passed through the routers infinitely without being received. As the Echo (ping) reply packets are marked as received by the routers and reached to the destination, it will receive Type 0.

### Question 10

Based on the Figure 4 mentioned in the assignment description, the link between router 9 and router 10 has significantly longer delay compared to others. Based on the name of the router 9 and 10, I can guess that the router 9 is located in New York City, United States, where the other end could possibly be located in France, causing the longer delay across continent.

## 3 Extra Credit

No.	Time	Source	Destination	Protocol	Length	Info
2	0.013151	10.216.228.1	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Frame 2: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)  
 Ethernet II, Src: LinksysG\_da:af:73 (00:06:25:da:af:73), Dst: Dell\_4f:36:23 (00:08:74:4f:36:23)  
 Internet Protocol Version 4, Src: 10.216.228.1, Dst: 192.168.1.101  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)  
 Total Length: 56  
 Identification: 0x9d45 (40261)  
 Flags: 0x00  
 Fragment Offset: 0  
 Time to Live: 255  
 Protocol: ICMP (1)  
 Header Checksum: 0x6cd8 [validation disabled]  
 [Header checksum status: Unverified]  
 Source Address: 10.216.228.1  
 Destination Address: 192.168.1.101  
 Internet Control Message Protocol  
 Type: 11 (Time-to-live exceeded)  
 Code: 0 (Time to live exceeded in transit)  
 Checksum: 0x2c16 [correct]  
 [Checksum Status: Good]  
 Unused: 00000000  
 Internet Protocol Version 4, Src: 192.168.1.101, Dst: 138.96.146.2  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)

/Users/hanthesuperman/Desktop/wireshark-traces/icmp-ethereal-trace-2 102 total packets, 102 shown

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 92  
 Identification: 0xd2d5 (53973)  
 Flags: 0x00  
 Fragment Offset: 0  
 Time to Live: 1  
 Protocol: ICMP (1)  
 Header Checksum: 0xd145 [validation disabled]  
 [Header checksum status: Unverified]  
 Source Address: 192.168.1.101  
 Destination Address: 138.96.146.2  
 Internet Control Message Protocol  
 Type: 8 (Echo (ping) request)  
 Code: 0  
 Checksum: 0x51fe [unverified] [in ICMP error packet]  
 [Checksum Status: Unverified]  
 Identifier (BE): 512 (0x0200)  
 Identifier (LE): 2 (0x0002)  
 Sequence Number (BE): 41985 (0xa401)  
 Sequence Number (LE): 420 (0x01a4)

Figure 6: ICMP Packet information of the Time-to-live exceeded error

# ECS 152A - Project 1 - IP Wireshark Lab

Han Nguyen (917278789) & Blake McMurray (999162729)

1/17/2020

## 1 Capturing packets from an execution of traceroute

```
hanthesuperman — -bash — 202x55
For more details, please visit https://support.apple.com/kb/HT208050.
HanMBP:~ hanthesuperman$ traceroute gaia.cs.umass.edu 56
traceroute to gaia.cs.umass.edu (128.119.245.12), 64 hops max, 56 byte packets
 1  router.asus.com (192.168.1.1)  2.389 ms  7.304 ms  0.725 ms
 2  96.120.14.197 (96.120.14.197)  10.632 ms  11.148 ms  12.178 ms
 3  96.110.159.205 (96.110.159.205)  18.038 ms  11.204 ms  12.855 ms
 4  ae-1-rur102.sacramento.ca.ccal.comcast.net (68.87.200.54)  14.235 ms  17.090 ms  14.115 ms
 5  ae-2-ar01.fresno.ca.ccal.comcast.net (68.85.120.201)  15.961 ms  35.932 ms  17.227 ms
 6  be-33667-cr02.losangeles.ca.ibone.comcast.net (68.86.93.37)  31.465 ms  23.819 ms  24.849 ms
 7  be-1102-cs01.losangeles.ca.ibone.comcast.net (96.110.39.201)  24.638 ms  25.652 ms  25.021 ms
 8  be-1112-cr12.losangeles.ca.ibone.comcast.net (96.110.45.166)  24.087 ms  24.855 ms  32.292 ms
 9  be-302-cr13.houston.tx.ibone.comcast.net (96.110.37.189)  54.972 ms  53.271 ms  52.462 ms
10  be-1113-cs01.houston.tx.ibone.comcast.net (96.110.46.105)  56.445 ms
    be-1213-cs02.houston.tx.ibone.comcast.net (96.110.46.121)  55.361 ms
    be-1413-cs04.houston.tx.ibone.comcast.net (96.110.46.153)  54.741 ms
11  be-1412-cr12.houston.tx.ibone.comcast.net (96.110.46.150)  56.548 ms
    be-1112-cr12.houston.tx.ibone.comcast.net (96.110.46.102)  52.279 ms *
12  be-301-cr14.56marietta.ga.ibone.comcast.net (96.110.32.217)  69.171 ms  65.444 ms  63.879 ms
13  be-1214-cs02.56marietta.ga.ibone.comcast.net (96.110.34.245)  63.692 ms
    be-1114-cs01.56marietta.ga.ibone.comcast.net (96.110.34.241)  64.833 ms
    be-1214-cs02.56marietta.ga.ibone.comcast.net (96.110.34.245)  64.908 ms
14  be-1413-cr13.56marietta.ga.ibone.comcast.net (96.110.34.238)  63.334 ms
    be-1313-cr13.56marietta.ga.ibone.comcast.net (96.110.34.234)  63.813 ms *
15  be-304-cr11.doraville.ga.ibone.comcast.net (96.110.39.170)  73.683 ms
    be-302-cr11.doraville.ga.ibone.comcast.net (96.110.39.50)  65.892 ms
    be-303-cr11.doraville.ga.ibone.comcast.net (96.110.39.222)  68.567 ms
16  be-1111-cs01.doraville.ga.ibone.comcast.net (96.110.34.161)  67.534 ms
    be-1311-cs03.doraville.ga.ibone.comcast.net (96.110.34.169)  64.325 ms  70.266 ms
17  be-1113-cr13.doraville.ga.ibone.comcast.net (96.110.34.194)  65.420 ms  63.216 ms
    be-1313-cr13.doraville.ga.ibone.comcast.net (96.110.34.202)  64.830 ms
18  be-301-cr11.ashburn.va.ibone.comcast.net (96.110.32.2)  76.501 ms  79.798 ms  78.484 ms
19  be-1311-cs03.ashburn.va.ibone.comcast.net (96.110.32.113)  77.553 ms
    be-1111-cs01.ashburn.va.ibone.comcast.net (96.110.32.105)  77.212 ms
    be-1311-cs03.ashburn.va.ibone.comcast.net (96.110.32.113)  79.579 ms
20  be-1213-cr13.ashburn.va.ibone.comcast.net (96.110.34.150)  76.587 ms
    be-1413-cr13.ashburn.va.ibone.comcast.net (96.110.34.158)  78.311 ms
    be-1113-cr13.ashburn.va.ibone.comcast.net (96.110.34.146)  79.378 ms
21  be-301-cr12.newark.nj.ibone.comcast.net (96.110.36.114)  83.522 ms
    be-302-cr12.newark.nj.ibone.comcast.net (96.110.36.118)  82.525 ms  83.634 ms
22  be-1112-cs01.newark.nj.ibone.comcast.net (96.110.35.81)  82.875 ms
    be-1312-cs03.newark.nj.ibone.comcast.net (96.110.35.89)  94.402 ms
    be-1212-cs02.newark.nj.ibone.comcast.net (96.110.35.85)  83.536 ms
23  96.110.42.206 (96.110.42.206)  143.331 ms
    96.110.42.194 (96.110.42.194)  89.023 ms
    96.110.42.202 (96.110.42.202)  89.530 ms
24  162.151.52.226 (162.151.52.226)  97.759 ms  90.507 ms  91.897 ms
25  96.108.47.146 (96.108.47.146)  91.897 ms  90.085 ms  91.836 ms
26  * * *
27  core1-rt-et-8-3-0.gw.umass.edu (192.80.83.109)  103.215 ms  97.145 ms  91.554 ms
28  n5-rt-1-1-et-10-0-0.gw.umass.edu (128.119.0.10)  92.792 ms
    n5-rt-1-1-et-0-0-0.gw.umass.edu (128.119.0.8)  94.519 ms  104.206 ms
29  cics-rt-xe-0-0-0.gw.umass.edu (128.119.3.32)  91.934 ms  91.019 ms  96.140 ms
30  nscs1bbs1.cs.umass.edu (128.119.240.253)  97.492 ms  95.256 ms  97.042 ms
31  gaia.cs.umass.edu (128.119.245.12)  92.614 ms IZ 92.803 ms IZ 103.659 ms IZ
HanMBP:~ hanthesuperman$
```

Figure 1: IP Traceroute with 56 bytes of packet

```
hanthesuperman$ traceroute gaia.cs.umass.edu 2000
traceroute to gaia.cs.umass.edu (128.119.245.12), 64 hops max, 2000 byte packets
 1 router.asus.com (192.168.1.1)  2.239 ms  1.106 ms  0.913 ms
 2 96.120.14.197 (96.120.14.197)  20.542 ms  13.748 ms  10.957 ms
 3 96.110.159.205 (96.110.159.205)  12.628 ms  14.392 ms  13.953 ms
 4 ae-1-rur102.sacramento.ca.ccal.comcast.net (68.87.200.54)  11.800 ms  16.517 ms  20.983 ms
 5 ae-2-ar01.fresno.ca.ccal.comcast.net (68.85.120.201)  15.904 ms  19.246 ms  17.689 ms
 6 be-33667-cr02.losangeles.ca.ibone.comcast.net (68.86.93.37)  54.127 ms  31.926 ms  28.243 ms
 7 be-1102-cs01.losangeles.ca.ibone.comcast.net (96.110.39.201)  30.995 ms  25.340 ms  27.321 ms
 8 be-1112-cr12.losangeles.ca.ibone.comcast.net (96.110.45.166)  25.784 ms  26.038 ms  27.134 ms
 9 be-301-cr13.houston.tx.ibone.comcast.net (96.110.37.185)  52.619 ms  53.701 ms  52.421 ms
10 be-1213-cs02.houston.tx.ibone.comcast.net (96.110.46.121)  52.036 ms
   be-1413-cs04.houston.tx.ibone.comcast.net (96.110.46.153)  53.777 ms
   be-1113-cs01.houston.tx.ibone.comcast.net (96.110.46.105)  54.072 ms
11 be-1112-cr12.houston.tx.ibone.comcast.net (96.110.46.102)  52.412 ms
   be-1412-cr12.houston.tx.ibone.comcast.net (96.110.46.150)  53.162 ms
   be-1312-cr12.houston.tx.ibone.comcast.net (96.110.46.134)  51.887 ms
12 be-301-cr14.56marietta.ga.ibone.comcast.net (96.110.32.217)  67.711 ms  77.232 ms  65.536 ms
13 be-1114-cs01.56marietta.ga.ibone.comcast.net (96.110.34.241)  66.595 ms  68.767 ms  67.293 ms
14 be-1413-cr13.56marietta.ga.ibone.comcast.net (96.110.34.238)  65.814 ms
   be-1313-cr13.56marietta.ga.ibone.comcast.net (96.110.34.234)  67.257 ms
   be-1113-cr13.56marietta.ga.ibone.comcast.net (96.110.34.226)  65.718 ms
15 be-303-cr11.doraville.ga.ibone.comcast.net (96.110.39.222)  65.874 ms
   be-304-cr11.doraville.ga.ibone.comcast.net (96.110.39.170)  65.370 ms
   be-302-cr11.doraville.ga.ibone.comcast.net (96.110.39.50)  67.042 ms
16 be-1311-cs03.doraville.ga.ibone.comcast.net (96.110.34.169)  72.529 ms
   be-1111-cs01.doraville.ga.ibone.comcast.net (96.110.34.161)  66.303 ms
   be-1311-cs03.doraville.ga.ibone.comcast.net (96.110.34.169)  69.592 ms
17 be-1313-cr13.doraville.ga.ibone.comcast.net (96.110.34.229)  74.864 ms
   be-1213-cr13.doraville.ga.ibone.comcast.net (96.110.34.198)  65.323 ms
   be-1113-cr13.doraville.ga.ibone.comcast.net (96.110.34.194)  65.200 ms
18 be-301-cr11.ashburn.va.ibone.comcast.net (96.110.32.2)  79.742 ms  79.981 ms  79.596 ms
19 be-1111-cs01.ashburn.va.ibone.comcast.net (96.110.32.105)  79.117 ms
   be-1311-cs03.ashburn.va.ibone.comcast.net (96.110.32.113)  78.228 ms  79.834 ms
20 be-1413-cr13.ashburn.va.ibone.comcast.net (96.110.34.158)  77.482 ms
   be-1113-cr13.ashburn.va.ibone.comcast.net (96.110.34.146)  79.555 ms  80.980 ms
21 be-302-cr12.newark.nj.ibone.comcast.net (96.110.36.118)  84.166 ms  90.722 ms
   be-301-cr12.newark.nj.ibone.comcast.net (96.110.36.114)  102.035 ms
22 be-1212-cs02.newark.nj.ibone.comcast.net (96.110.35.85)  85.850 ms
   be-1412-cs04.newark.nj.ibone.comcast.net (96.110.35.93)  86.934 ms
   be-1112-cs01.newark.nj.ibone.comcast.net (96.110.35.81)  83.331 ms
23 96.110.42.202 (96.110.42.202)  90.272 ms
   96.110.42.198 (96.110.42.198)  90.162 ms
   96.110.42.206 (96.110.42.206)  96.285 ms
24 162.151.52.226 (162.151.52.226)  99.056 ms  91.653 ms  92.220 ms
25 96.108.47.146 (96.108.47.146)  92.168 ms  92.443 ms  110.112 ms
26 * * *
27 core2-rt-et-8-3-0.gw.umass.edu (192.80.83.113)  96.738 ms  92.403 ms  93.431 ms
28 n5-rt-1-1-et-10-0-0.gw.umass.edu (128.119.0.10)  95.344 ms  97.241 ms  93.823 ms
29 cics-rt-xe-0-0-0.gw.umass.edu (128.119.3.32)  99.940 ms  92.349 ms  94.797 ms
30 * * *
31 gaia.cs.umass.edu (128.119.245.12)  101.299 ms !Z 95.227 ms !Z 95.264 ms !Z
HanMBP:~ hanthesuperman$
```

Figure 2: IP Traceroute with 2000 bytes of packet

```
hanthesuperman$ traceroute gaia.cs.umass.edu 3500
traceroute to gaia.cs.umass.edu (128.119.245.12), 64 hops max, 3500 byte packets
 1 router.asus.com (192.168.1.1)  9.336 ms  1.567 ms  1.228 ms
 2 96.120.14.197 (96.120.14.197)  19.449 ms  27.260 ms  19.349 ms
 3 96.110.159.205 (96.110.159.205)  23.392 ms  20.070 ms  21.319 ms
 4 ae-1-rur102.sacramento.ca.ccal.comcast.net (68.87.200.54)  32.621 ms  26.455 ms  16.811 ms
 5 ae-2-ar01.fresno.ca.ccal.comcast.net (68.85.120.201)  24.591 ms  37.644 ms  23.840 ms
 6 be-33667-cr02.losangeles.ca.ibone.comcast.net (68.86.93.37)  32.982 ms  34.475 ms  40.098 ms
 7 be-1102-cs01.losangeles.ca.ibone.comcast.net (96.110.39.201)  31.802 ms  31.033 ms  31.892 ms
 8 be-1112-cr12.losangeles.ca.ibone.comcast.net (96.110.45.166)  30.186 ms  33.385 ms  34.352 ms
 9 be-301-cr13.houston.tx.ibone.comcast.net (96.110.37.185)  68.453 ms  76.727 ms
   be-302-cr13.houston.tx.ibone.comcast.net (96.110.37.189)  62.609 ms
10 be-1413-cs04.houston.tx.ibone.comcast.net (96.110.46.153)  58.882 ms
   be-1313-cs03.houston.tx.ibone.comcast.net (96.110.46.137)  59.136 ms
   be-1113-cs01.houston.tx.ibone.comcast.net (96.110.46.105)  60.030 ms
11 be-1212-cr12.houston.tx.ibone.comcast.net (96.110.46.118)  59.386 ms  59.304 ms  59.376 ms
12 be-301-cr14.56marietta.ga.ibone.comcast.net (96.110.32.217)  71.373 ms  89.523 ms  70.872 ms
13 be-1414-cs04.56marietta.ga.ibone.comcast.net (96.110.34.253)  70.338 ms
   be-1314-cs03.56marietta.ga.ibone.comcast.net (96.110.34.249)  79.051 ms  72.427 ms
14 be-1113-cr13.56marietta.ga.ibone.comcast.net (96.110.34.226)  72.877 ms *
   be-1413-cr13.56marietta.ga.ibone.comcast.net (96.110.34.238)  75.984 ms
15 be-304-cr11.doraville.ga.ibone.comcast.net (96.110.39.170)  78.711 ms
   be-301-cr11.doraville.ga.ibone.comcast.net (96.110.39.46)  72.345 ms  105.716 ms
16 be-1111-cs01.doraville.ga.ibone.comcast.net (96.110.34.161)  72.958 ms
   be-1211-cs02.doraville.ga.ibone.comcast.net (96.110.34.165)  70.929 ms  109.801 ms
17 be-1213-cr13.doraville.ga.ibone.comcast.net (96.110.34.198)  73.333 ms  75.441 ms
   be-1413-cr13.doraville.ga.ibone.comcast.net (96.110.34.206)  73.055 ms
18 be-301-cr11.ashburn.va.ibone.comcast.net (96.110.32.2)  83.817 ms  84.813 ms  84.018 ms
19 be-1311-cs03.ashburn.va.ibone.comcast.net (96.110.32.113)  86.219 ms
   be-1411-cs04.ashburn.va.ibone.comcast.net (96.110.32.117)  83.435 ms
   be-1111-cs01.ashburn.va.ibone.comcast.net (96.110.32.105)  85.091 ms
20 be-1113-cr13.ashburn.va.ibone.comcast.net (96.110.34.146)  84.227 ms  82.800 ms
   be-1313-cr13.ashburn.va.ibone.comcast.net (96.110.34.154)  95.057 ms
21 be-301-cr12.newark.nj.ibone.comcast.net (96.110.36.114)  90.026 ms
   be-302-cr12.newark.nj.ibone.comcast.net (96.110.36.118)  90.378 ms  90.068 ms
22 be-1412-cs04.newark.nj.ibone.comcast.net (96.110.35.93)  91.952 ms
   be-1212-cs02.newark.nj.ibone.comcast.net (96.110.35.85)  91.133 ms
   be-1312-cs03.newark.nj.ibone.comcast.net (96.110.35.89)  122.676 ms
23 96.110.42.194 (96.110.42.194)  96.122 ms
   96.110.42.206 (96.110.42.206)  98.225 ms
   96.110.42.198 (96.110.42.198)  107.836 ms
24 162.151.52.226 (162.151.52.226)  97.270 ms  100.528 ms  100.720 ms
25 96.108.47.146 (96.108.47.146)  99.995 ms  99.411 ms  98.874 ms
26 * * *
27 core2-rt-et-8-3-0.gw.umass.edu (192.80.83.113)  105.262 ms  96.280 ms  107.981 ms
28 n5-rt-1-1-et-10-0-0.gw.umass.edu (128.119.0.10)  102.566 ms  96.071 ms  107.555 ms
29 cics-rt-xe-0-0-0.gw.umass.edu (128.119.3.32)  103.759 ms  101.756 ms  103.717 ms
30 * * *
31 gaia.cs.umass.edu (128.119.245.12)  114.830 ms !Z 95.321 ms !Z 106.934 ms !Z
HanMBP:~ hanthesuperman$
```

Figure 3: IP Traceroute with 3500 bytes of packet



## 2 A look at the captured trace

```
No.      Time            Source            Destination      Protocol Length Info
  1 0.000000      192.168.1.39      239.255.255.250  SSDP           167    M-SEARCH *
HTTP/1.1
Frame 1: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface en0, id 0
Ethernet II, Src: fa:7b:8c:4e:d7:f3 (fa:7b:8c:4e:d7:f3), Dst: IPv4mcast_7f:ff:fa (01:00:5e:
7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.1.39, Dst: 239.255.255.250
  0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
      Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 153
        Identification: 0x6e2b (28203)
        Flags: 0x00
        Fragment Offset: 0
        Time to Live: 1
        Protocol: UDP (17)
        Header Checksum: 0x995f [validation disabled]
        [Header checksum status: Unverified]
        Source Address: 192.168.1.39
        Destination Address: 239.255.255.250
User Datagram Protocol, Src Port: 57917, Dst Port: 1900
Simple Service Discovery Protocol
```

Figure 4: First ICMP Echo Request Message

### Question 1

As shown in Figure 4, my computer's IP address is: 192.168.1.39

### Question 2

As shown in Figure 4, within the IP packet header, the value in the upper layer protocol field is UDP (17) in Unix/Linux.

### Question 3

As shown in Figure 4, there are 20 bytes in the IP Header. Since there are also 153 bytes in total length, the payload of the IP datagram is  $153 - 20 = 133$  bytes.

### Question 4

As shown in Figure 5, the fragment offset bit is 0 and the bit of the *More fragments* section is also 0, hence there are no datagram fragments.

### Question 5

The fields in the IP datagram that always change from one datagram to the next within this series of ICMP messages sent by my computer are:

- Total Length in bytes (found 5 cases so far)
- Identification (since different IP packets have different identification numbers).
- Time to Live (since the router might increment the TTL count if a packet is passed through routers infinitely: Source:

<https://www.cloudflare.com/learning/cdn/glossary/time-to-live-ttl/>)

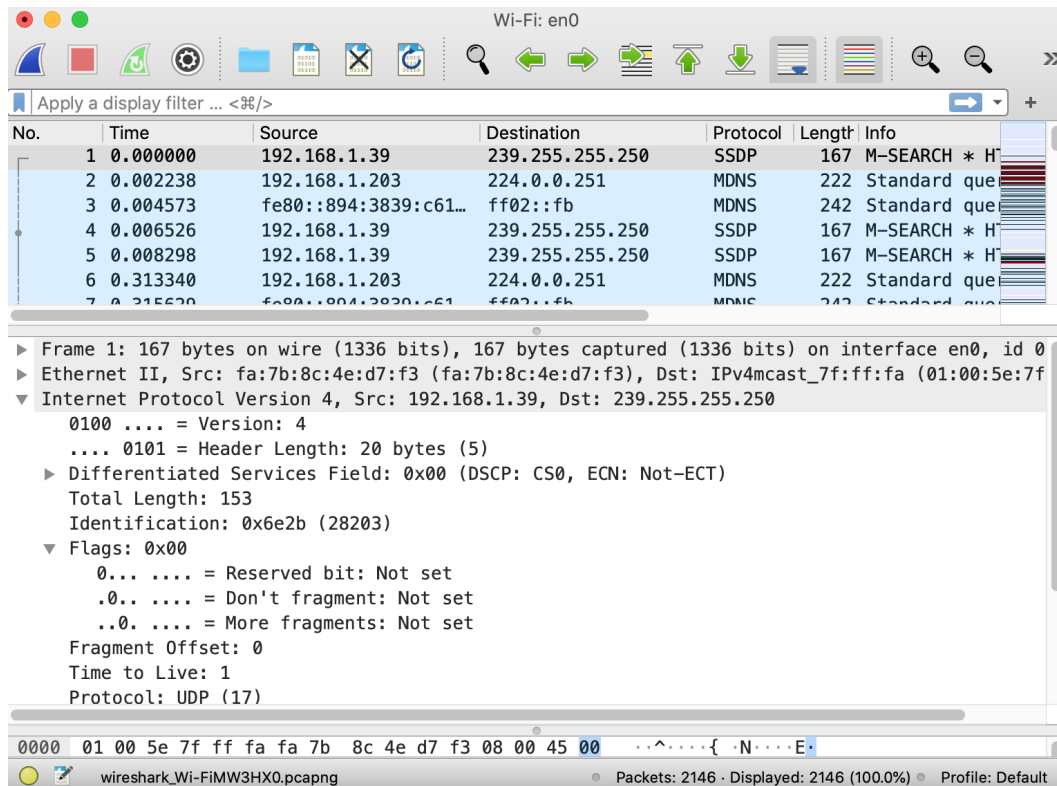


Figure 5: Data of Datagram Fragments

- Header Checksum (since the router change the checksum if the IP header changes when decrementing TTL count;

Source: <https://tools.ietf.org/html/rfc1812#section-4.2.2.5>)

## Question 6

The fields that stay constant are:

- Version (since the packets are captured in IPv4 version)
- Header Length (since the packets are captured in the ICMP)
- Differentiated Services (since the packets are captured in ICMP, they will have the same differentiated services)
- Flags and Fragment Offset (since the packets are not set to be reserved or fragmented)
- Protocol (since the packets are captured in ICMP protocol)
- Source and Destination IP Address (since the packets are sent and received by the same source from the *traceroute*)

The fields that *must* stay constant and the reasons are described as the above. The fields that *must* change and the reasons are described in the Section 2.5, except for the *Total Length in bytes*.

## Question 7

The pattern is that the values in the Identification field of the IP datagram increment by each datagram.

## Question 8

As shown in Figure 6, the Identification value is *0xfe4d*, or 65101. The Time-to-Live (TTL) value is 63.

No.	Time	Source	Destination	Protocol	Length	Info
27	2.471669	ASUSTekC_93:9f:c8	Spanning-tree-(for...	STP	52	Conf. Root = 32768/0/14:dd
1871	155.136981	::	ff02::1	ICMPv6	86	Multicast Listener Query
448	29.489772	::	ff02::1	ICMPv6	86	Multicast Listener Query
1375	125.876431	96.120.14.197	192.168.1.209	ICMP	70	Time-to-live exceeded (Tim
1371	125.857180	96.120.14.197	192.168.1.209	ICMP	70	Time-to-live exceeded (Tim
1367	125.829241	96.120.14.197	192.168.1.209	ICMP	70	Time-to-live exceeded (Tim
770	65.777262	96.120.14.197	192.168.1.209	ICMP	70	Time-to-live exceeded (Tim
767	65.766405	96.120.14.197	192.168.1.209	ICMP	70	Time-to-live exceeded (Tim
764	65.752093	96.120.14.197	192.168.1.209	ICMP	70	Time-to-live exceeded (Tim
76	7.045204	96.120.14.197	192.168.1.209	ICMP	70	Time-to-live exceeded (Tim
74	7.033005	96.120.14.197	192.168.1.209	ICMP	70	Time-to-live exceeded (Tim

▶ Frame 1375: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface en0, id 0  
 ▶ Ethernet II, Src: ASUSTekC\_93:9f:c8 (14:dd:a9:93:9f:c8), Dst: Apple\_84:13:5f (ac:bc:32:84:13:5f)  
 ▼ Internet Protocol Version 4, Src: 96.120.14.197, Dst: 192.168.1.209  
     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: 56  
     Identification: 0xfe4d (65101)  
     ▼ Flags: 0x00  
         0... .... = Reserved bit: Not set  
         .0.. .... = Don't fragment: Not set  
         ..0. .... = More fragments: Not set  
     Fragment Offset: 0  
     Time to Live: 63  
     Protocol: ICMP (1)  
     Header Checksum: 0x4bc1 [validation disabled]  
     [Header checksum status: Unverified]  
     Source Address: 96.120.14.197  
     Destination Address: 192.168.1.209  
     ▼ Internet Control Message Protocol  
         Type: 11 (Time-to-live exceeded)  
         Code: 0 (Time to live exceeded in transit)

Figure 6: The nearest hop of TTL-exceeded packet

## Question 9

The values in the Identification field of all TTL-exceeded packets at the nearest hop do not remain unchanged because different packets will have different Identification numbers. However, the values in the TTL field of all TTL-exceeded packets at the nearest hop remains unchanged since the TTL value changes only when a packet is passed through routers infinitely without being received. At the first hop, this number always remains the same until the next hop.

## Fragmentation

Since we forgot to save the Wireshark captured packets after answering previous 9 questions, we will switch to use the author's *ip-ethereal-trace-1* to answer the Question 10 - 13

## Question 10

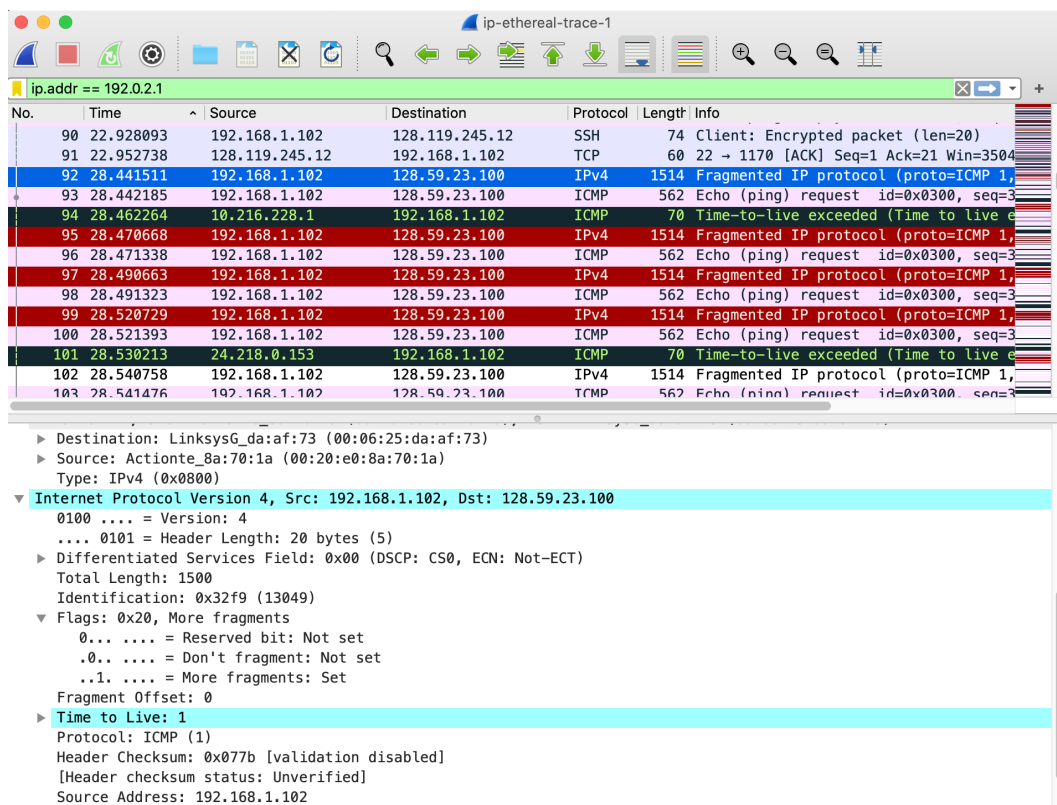


Figure 7: Fragmented IP Packet at pingplotter 1500

As shown in Figure 7, there are many IP addresses that say "Fragmented IP Protocol", so definitely the message has been fragmented across more than one IP address.

## Question 11

As shown in Figure 7, the bit value of the field *More Fragments* has been set to 1 across many IP packets, which indicates that the IP packets have been fragmented.

Since the flag offset is 0, this must be the first fragmented packet, compared to latter fragmented packets where their flag offset must be greater than 0.

This fragmented IP datagram has total length of 1500.

## Question 12

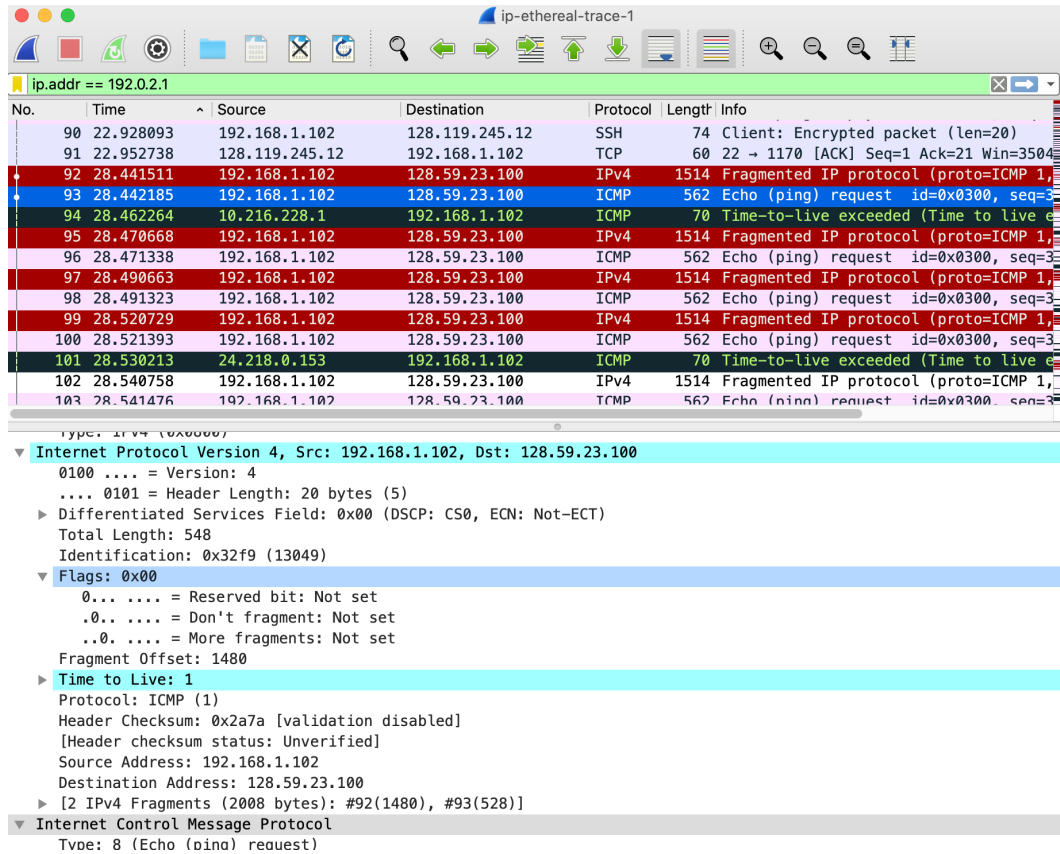


Figure 8: Second Fragmented IP Packet at pingplotter 1500

As shown in Figure 8, the second fragment of the fragmented IP packet has the fragment offset of 1480, which indicates that this is not the first fragment (first fragment must have fragment offset as 0). However, this is the final fragment of the fragmented IP packet, since the bit value of the *More Fragments* is set to 0.

## Question 13

The fields that change between the first and the second fragment of the fragmented IP packet are:

- Total length (1500 in the first and 548 in the second)
- Flags, Fragment Offset and *More Fragments* bit (as above)
- Header Checksum (0x077b in the first and 0x2a7a in the second)

## Question 14

As shown in Figure 9, there are three fragments of message after setting the pingplotter to 3500 (UDP and ICMP can be merged since it runs on Macbook Terminal).

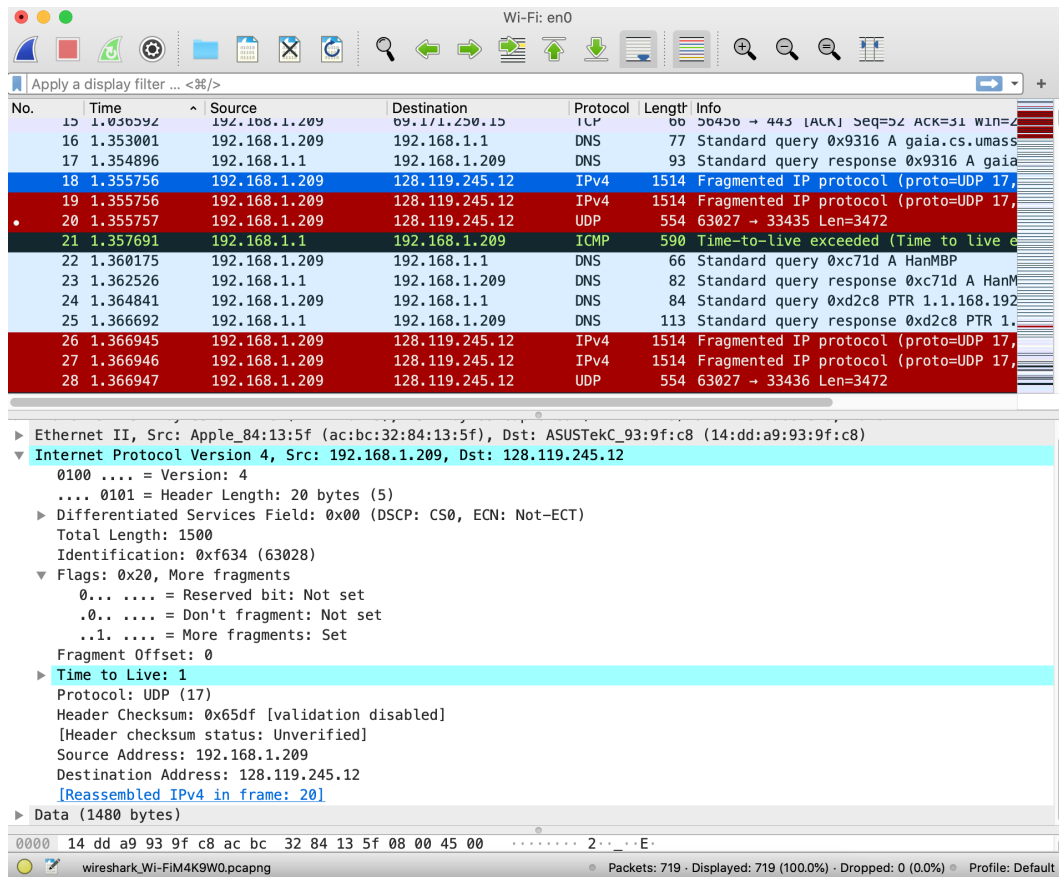


Figure 9: Fragmented IP Packet at pingplotter 3500

## Question 15

The fields in the IP header that change across the fragments of the fragmented IP packet are:

- Fragment Offset (0, 1480, 2960)
- Total Length (1500, 1500, 540)
- Header Checksum (0x65df, 0x6526, 0x882d)