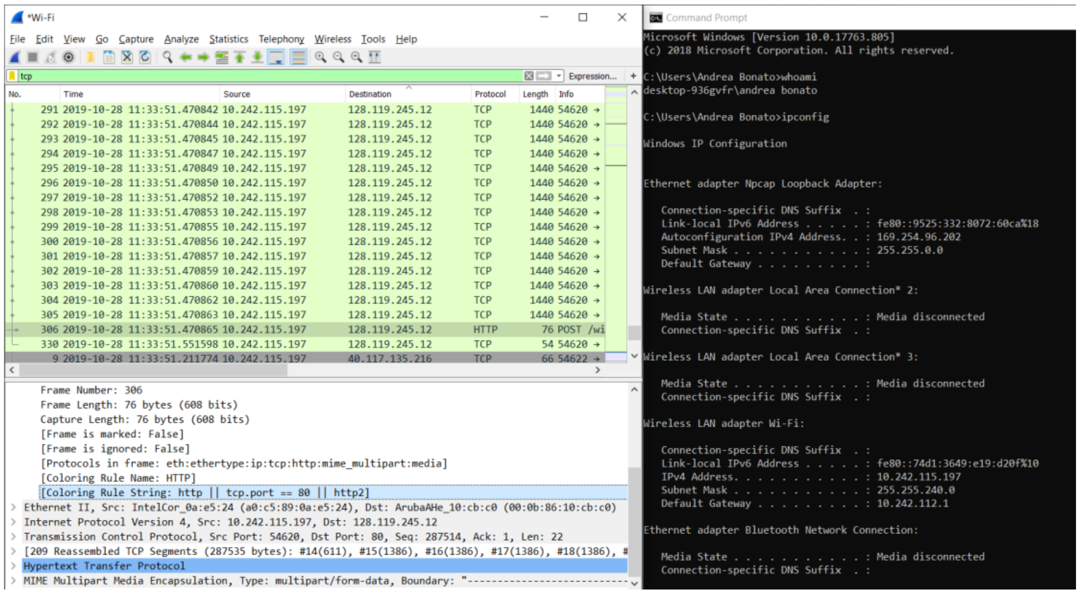
COMP-3670 Fall 2019

Assignment 2

Andrea Bonato (104760390)

Wireshark Lab: TCP v7.0

Figure 1 – Uploading a file



```
*Wi-Fi
tcp
No.   Time                          Source           Destination      Protocol  Length Info
  291 2019-10-28 11:33:51.470842 10.242.115.197     128.119.245.12   TCP       1440 54620 →
  292 2019-10-28 11:33:51.470844 10.242.115.197     128.119.245.12   TCP       1440 54620 →
  293 2019-10-28 11:33:51.470845 10.242.115.197     128.119.245.12   TCP       1440 54620 →
  294 2019-10-28 11:33:51.470847 10.242.115.197     128.119.245.12   TCP       1440 54620 →
  295 2019-10-28 11:33:51.470849 10.242.115.197     128.119.245.12   TCP       1440 54620 →
  296 2019-10-28 11:33:51.470850 10.242.115.197     128.119.245.12   TCP       1440 54620 →
  297 2019-10-28 11:33:51.470852 10.242.115.197     128.119.245.12   TCP       1440 54620 →
  298 2019-10-28 11:33:51.470853 10.242.115.197     128.119.245.12   TCP       1440 54620 →
  299 2019-10-28 11:33:51.470855 10.242.115.197     128.119.245.12   TCP       1440 54620 →
  300 2019-10-28 11:33:51.470856 10.242.115.197     128.119.245.12   TCP       1440 54620 →
  301 2019-10-28 11:33:51.470857 10.242.115.197     128.119.245.12   TCP       1440 54620 →
  302 2019-10-28 11:33:51.470859 10.242.115.197     128.119.245.12   TCP       1440 54620 →
  303 2019-10-28 11:33:51.470860 10.242.115.197     128.119.245.12   TCP       1440 54620 →
  304 2019-10-28 11:33:51.470862 10.242.115.197     128.119.245.12   TCP       1440 54620 →
  305 2019-10-28 11:33:51.470863 10.242.115.197     128.119.245.12   TCP       1440 54620 →
  306 2019-10-28 11:33:51.470865 10.242.115.197     128.119.245.12   HTTP        76 POST /wi
  330 2019-10-28 11:33:51.551598 10.242.115.197     128.119.245.12   TCP         54 54620 →
    9 2019-10-28 11:33:51.211774 10.242.115.197     40.117.135.216   TCP         66 54622 →

    Frame Number: 306
    Frame Length: 76 bytes (608 bits)
    Capture Length: 76 bytes (608 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:mime_multipart:media]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: IntelCor_0a:e5:24 (a0:c5:89:0a:e5:24), Dst: ArubaAHe_10:cb:c0 (00:0b:86:10:cb:c0)
> Internet Protocol Version 4, Src: 10.242.115.197, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54620, Dst Port: 80, Seq: 287514, Ack: 1, Len: 22
> [209 Reassembled TCP Segments (287535 bytes): #14(611), #15(1386), #16(1386), #17(1386), #18(1386), #
> Hypertext Transfer Protocol
> MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "--------------------------
```

```
Command Prompt
Microsoft Windows [Version 10.0.17763.805]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Andrea Bonato>whoami
desktop-936gvfr\andrea bonato

C:\Users\Andrea Bonato>ipconfig

Windows IP Configuration


Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9525:332:8072:60ca%18
   Autoconfiguration IPv4 Address. . : 169.254.96.202
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::74d1:3649:e19:d20f%10
   IPv4 Address. . . . . . . . . . . : 10.242.115.197
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.242.112.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

1. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?

   The source IP address used by the client computer is 10.242.115.197. The TCP port number used by the client computer is 54620. This is shown in **figure 1.**

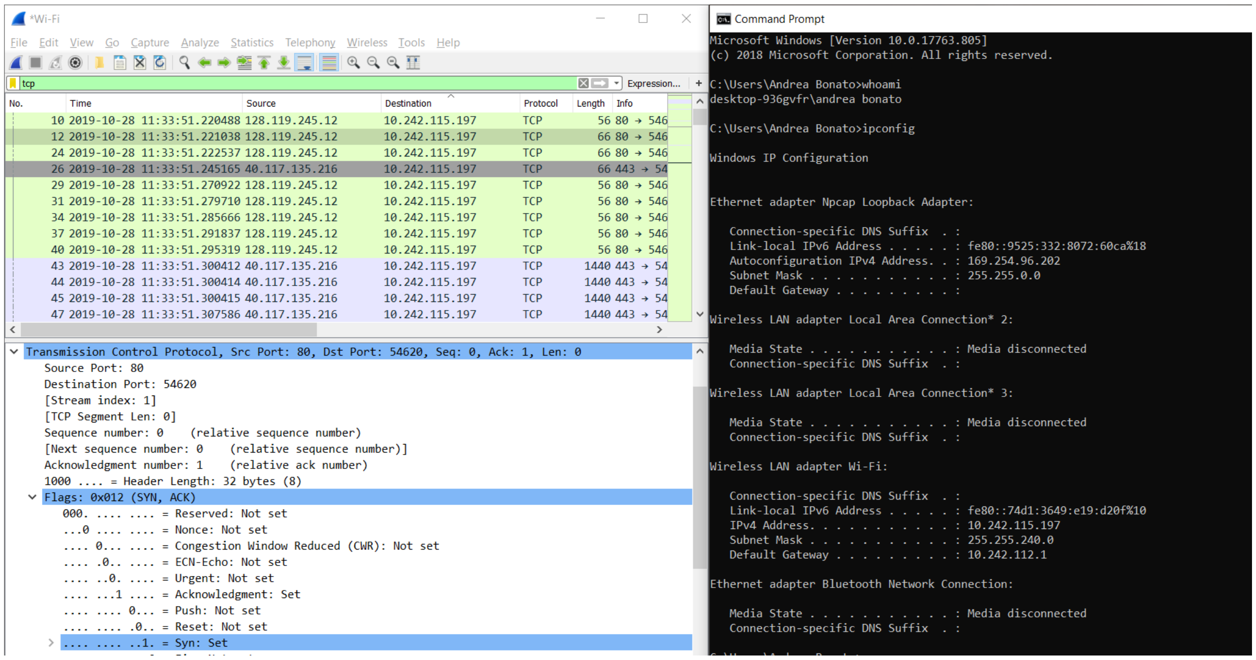
2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

   The IP address of gaia.cs.umass.edu is 128.119.245.12. The port number that it is sending and receiving TCP segments through is 80. This is shown in **figure 1.**

3. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?

   The source IP address used by my computer is 10.242.115.197. The TCP port number used by the client computer is 54620. This is shown in **figure 1.**

Figure 2 – SYN flag and sequencing

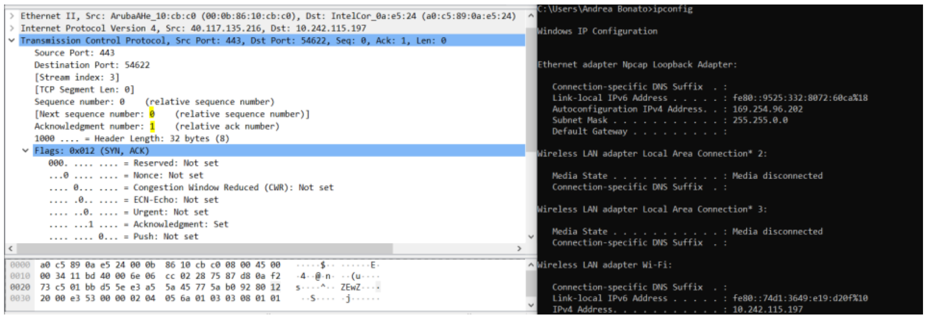


```
No.  Time                         Source          Destination     Protocol  Length  Info
  10 2019-10-28 11:33:51.220488 128.119.245.12  10.242.115.197  TCP         56 80 → 546
  12 2019-10-28 11:33:51.221038 128.119.245.12  10.242.115.197  TCP         66 80 → 546
  24 2019-10-28 11:33:51.222537 128.119.245.12  10.242.115.197  TCP         66 80 → 546
  26 2019-10-28 11:33:51.245165 40.117.135.216  10.242.115.197  TCP         66 443 → 54
  29 2019-10-28 11:33:51.270922 128.119.245.12  10.242.115.197  TCP         56 80 → 546
  31 2019-10-28 11:33:51.279710 128.119.245.12  10.242.115.197  TCP         56 80 → 546
  34 2019-10-28 11:33:51.285666 128.119.245.12  10.242.115.197  TCP         56 80 → 546
  37 2019-10-28 11:33:51.291837 128.119.245.12  10.242.115.197  TCP         56 80 → 546
  40 2019-10-28 11:33:51.295319 128.119.245.12  10.242.115.197  TCP         56 80 → 546
  43 2019-10-28 11:33:51.300412 40.117.135.216  10.242.115.197  TCP       1440 443 → 54
  44 2019-10-28 11:33:51.300414 40.117.135.216  10.242.115.197  TCP       1440 443 → 54
  45 2019-10-28 11:33:51.300415 40.117.135.216  10.242.115.197  TCP       1440 443 → 54
  47 2019-10-28 11:33:51.307586 40.117.135.216  10.242.115.197  TCP       1440 443 → 54

Transmission Control Protocol, Src Port: 80, Dst Port: 54620, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 54620
    [Stream index: 1]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    1000 .... = Header Length: 32 bytes (8)
  Flags: 0x012 (SYN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..1. = Syn: Set
```

```
Microsoft Windows [Version 10.0.17763.805]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Andrea Bonato>whoami
desktop-936gvfr\andrea bonato

C:\Users\Andrea Bonato>ipconfig

Windows IP Configuration


Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9525:332:8072:60ca%18
   Autoconfiguration IPv4 Address. . : 169.254.96.202
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::74d1:3649:e19:d20f%10
   IPv4 Address. . . . . . . . . . . : 10.242.115.197
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.242.112.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

4. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as SYN segment?
   As shown in **figure 2**, the sequence number of the TCP SYN is 0 since it is used to start the TCP connection between the client and the website gaia.cs.uass.edu. It shows that the segment is a SYN segment because the SYN flag equals 1.

5. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the acknowledgeme3nt field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?
   As shown in the figure below, the sequence number of the SYNACK segment sent by gaia.cs.umass.edu is 0 and the value of the acknowledgement field is 1. This segment can be identified as a SYNACK segment if both SYN flag and the ACK flags are set to 1.

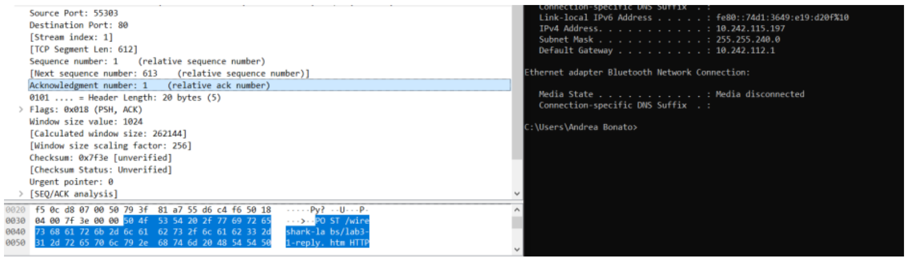


```
> Ethernet II, Src: ArubaAHe_10:cb:c0 (00:0b:86:10:cb:c0), Dst: IntelCor_0a:e5:24 (a0:c5:89:0a:e5:24)
> Internet Protocol Version 4, Src: 40.117.135.216, Dst: 10.242.115.197
v Transmission Control Protocol, Src Port: 443, Dst Port: 54622, Seq: 0, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 54622
    [Stream index: 3]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    1000 .... = Header Length: 32 bytes (8)
  v Flags: 0x012 (SYN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set

0000  a0 c5 89 0a e5 24 00 0b  86 10 cb c0 08 00 45 00   .....$.. ......E.
0010  00 34 11 bd 40 00 6e 06  cc 02 28 75 87 d8 0a f2   .4..@.n. ..(u....
0020  73 c5 01 bb d5 5e e3 a5  5a 45 77 5a b0 92 80 12   s....^.. ZEwZ....
0030  20 00 e3 53 00 00 02 04  05 6a 01 03 03 08 01 01    ..S.... .j......
```

```
C:\Users\Andrea Bonato>ipconfig

Windows IP Configuration


Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9525:332:8072:60ca%18
   Autoconfiguration IPv4 Address. . : 169.254.96.202
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::74d1:3649:e19:d20f%10
   IPv4 Address. . . . . . . . . . . : 10.242.115.197
```

6. What is the sequence number of the TCP segment containing the HTTP POST command?

The sequence number oft the TCP segment containing the HTTP POST command is 1. This is shown in the image below.



```
Source Port: 55303
Destination Port: 80
[Stream index: 1]
[TCP Segment Len: 612]
Sequence number: 1    (relative sequence number)
[Next sequence number: 613    (relative sequence number)]
Acknowledgment number: 1    (relative ack number)
0101 .... = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
Window size value: 1024
[Calculated window size: 262144]
[Window size scaling factor: 256]
Checksum: 0x7f3e [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
> [SEQ/ACK analysis]

0020  f5 0c d8 07 00 50 79 3f  81 a7 55 d6 c4 f6 50 18   ·····Py? ··U···P·
0030  04 00 7f 3e 00 00 50 4f  53 54 20 2f 77 69 72 65   ···>··PO ST /wire
0040  73 68 61 72 6b 2d 6c 61  62 73 2f 6c 61 62 33 2d   shark-la bs/lab3-
0050  31 2d 72 65 70 6c 79 2e  68 74 6d 20 48 54 54 50   1-reply. htm HTTP
```

```
   Link-local IPv6 Address . . . . . : fe80::74d1:3649:e19:d20f%10
   IPv4 Address. . . . . . . . . . . : 10.242.115.197
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.242.112.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>
```

7. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection? When was the ACK for each segment received? Given the difference between when each TCP segment was sent, and when its acknowledgement was received, what is the RTT value for each of the six segments. What is the estimated RTT value after the receipt of each ACK?

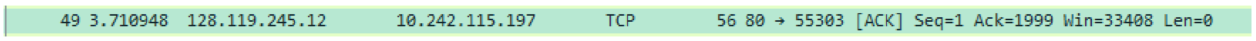
Segment	Sent Time	ACK Received Time	Round Trip Time	EstimatedRTT
1	0.066123	0.122956	0.056833	0.056833
1387	0.122958	0.122959	0.000001	0.048308175
2773	0.122960	0.123223	0.000265	0.042302778125
5545	0.123640	0.123836	0.000196	0.037039430859375
5708	0.270897	0.328977	0.058080	0.039669502001953125
6991	0.500629	0.510955	0.010326	0.0360015642551708984375

8. What is the length of each of the first six TCP segments?

The length of the first segment is 448 bytes and the remaining segments are 1440 bytes per segment.

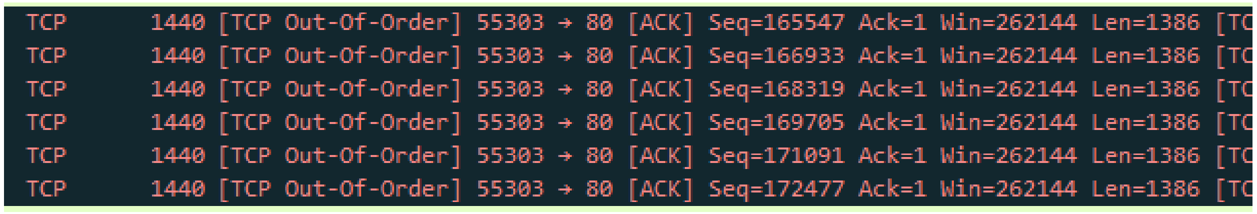
9. What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

The minimum amount of buffer space that is seen on the gaia.cs.umass.edu server is 33408 bytes and shown in the image below from the win section.

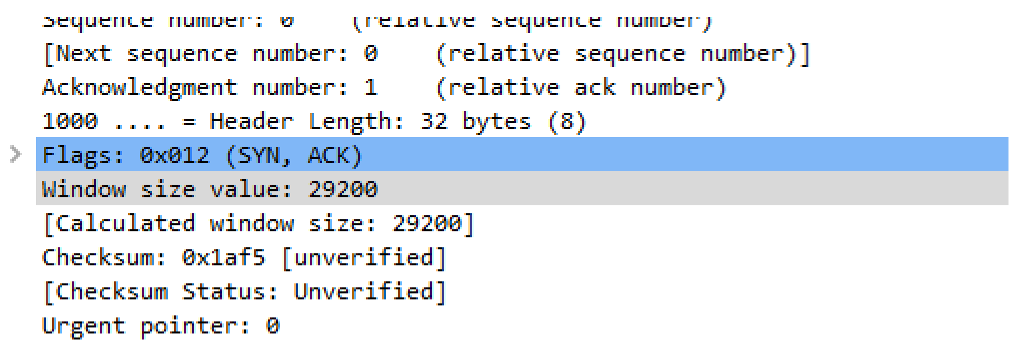


```
49 3.710948   128.119.245.12       10.242.115.197       TCP        56 80 → 55303 [ACK] Seq=1 Ack=1999 Win=33408 Len=0
```

The receiver window grows until a maximum buffer size of 29200 as shown in the image below.



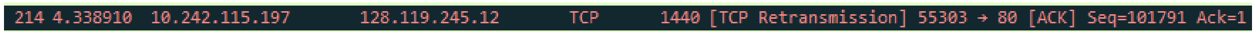
```
TCP        1440 [TCP Out-Of-Order] 55303 → 80 [ACK] Seq=165547 Ack=1 Win=262144 Len=1386 [TC
TCP        1440 [TCP Out-Of-Order] 55303 → 80 [ACK] Seq=166933 Ack=1 Win=262144 Len=1386 [TC
TCP        1440 [TCP Out-Of-Order] 55303 → 80 [ACK] Seq=168319 Ack=1 Win=262144 Len=1386 [TC
TCP        1440 [TCP Out-Of-Order] 55303 → 80 [ACK] Seq=169705 Ack=1 Win=262144 Len=1386 [TC
TCP        1440 [TCP Out-Of-Order] 55303 → 80 [ACK] Seq=171091 Ack=1 Win=262144 Len=1386 [TC
TCP        1440 [TCP Out-Of-Order] 55303 → 80 [ACK] Seq=172477 Ack=1 Win=262144 Len=1386 [TC
```



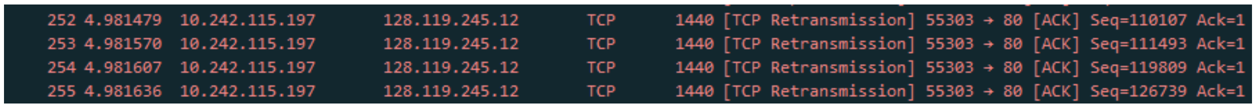
```
Sequence number: 0    (relative sequence number)
[Next sequence number: 0    (relative sequence number)]
Acknowledgment number: 1    (relative ack number)
1000 .... = Header Length: 32 bytes (8)
> Flags: 0x012 (SYN, ACK)
Window size value: 29200
[Calculated window size: 29200]
Checksum: 0x1af5 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
```

Looking at this trace, this trace throttled due to the size of the buffer.

10. Are there any retransmitted segments in the trace file? What did you check for in order to answer this question?



```
214 4.338910  10.242.115.197    128.119.245.12    TCP    1440 [TCP Retransmission] 55303 → 80 [ACK] Seq=101791 Ack=1
```



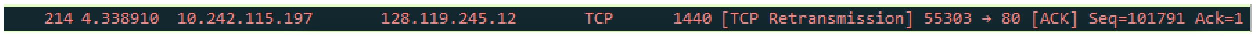
```
252 4.981479  10.242.115.197    128.119.245.12    TCP    1440 [TCP Retransmission] 55303 → 80 [ACK] Seq=110107 Ack=1
253 4.981570  10.242.115.197    128.119.245.12    TCP    1440 [TCP Retransmission] 55303 → 80 [ACK] Seq=111493 Ack=1
254 4.981607  10.242.115.197    128.119.245.12    TCP    1440 [TCP Retransmission] 55303 → 80 [ACK] Seq=119809 Ack=1
255 4.981636  10.242.115.197    128.119.245.12    TCP    1440 [TCP Retransmission] 55303 → 80 [ACK] Seq=126739 Ack=1
```

As shown in the images above, there were several times where there was a retransmission segment. In order to check this, I checked the segment stack that is outputted when filtered by TCP.

11. How much data does the receiver is typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment?

ACK	Sequence Number	Acknowledge Data
1	1999	448
2	3385	1440
3	4771	1440
4	6157	1440
5	7543	1440
6	8929	1440
7	10315	1440

1440 * 2 = 2880 is when the segment is ACKing every other segment. It is shown in No. 214

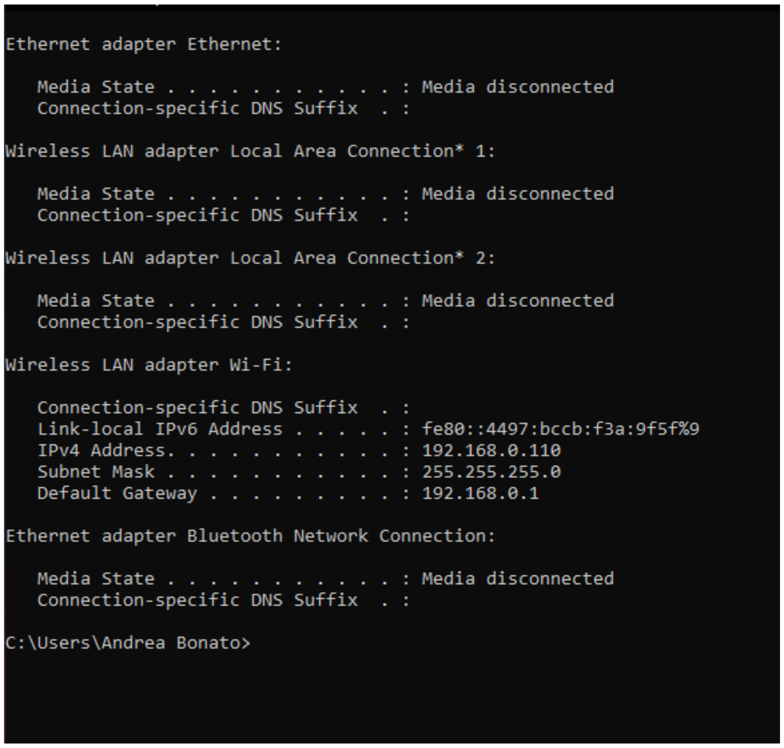


```
214 4.338910  10.242.115.197    128.119.245.12    TCP    1440 [TCP Retransmission] 55303 → 80 [ACK] Seq=101791 Ack=1
```

12. What is the throughput for the TCP connection? Explain how you calculated this value?

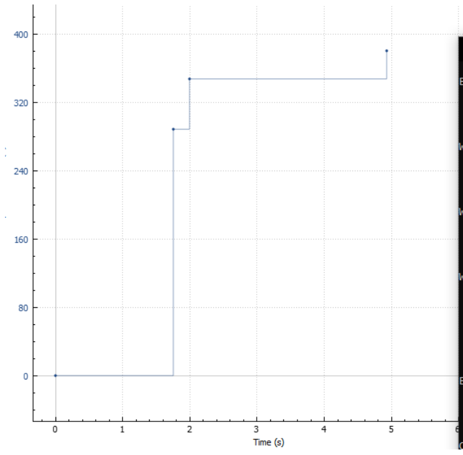
When taking the window size, and converting it to bits, one can divide it by the latency to calculate the throughput for the TCP connection. The size of the given file is 280KB which is equivalent two 280,000 bytes. The first time is 0.399183s and the final time is 0.536283s. The difference in time is 0.1371 seconds. Thus, the throughput is 280,000/0.1371 = 2,041,304.88694383 bytes/second.

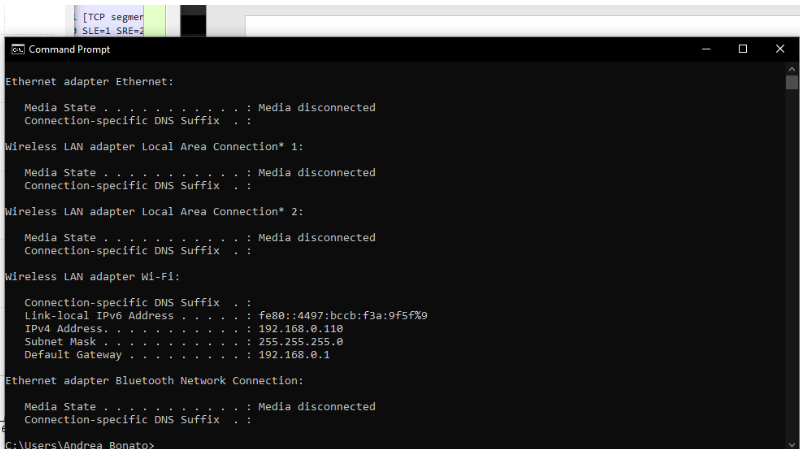
Figure 3 – Change of location



```
Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4497:bccb:f3a:9f5f%9
   IPv4 Address. . . . . . . . . . . : 192.168.0.110
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>
```

13. Use the time-sequence-graph plotting tool to view the sequence number versus time plot o segments being sent from the client to the gaia.cs.umass.edu server. Can you identify where TCP's slow start phase begins and ends, and where congestion avoidance takes over? Comment on ways in which the measured data differs from the idealized behaviour of TCP that we've studied in the text.



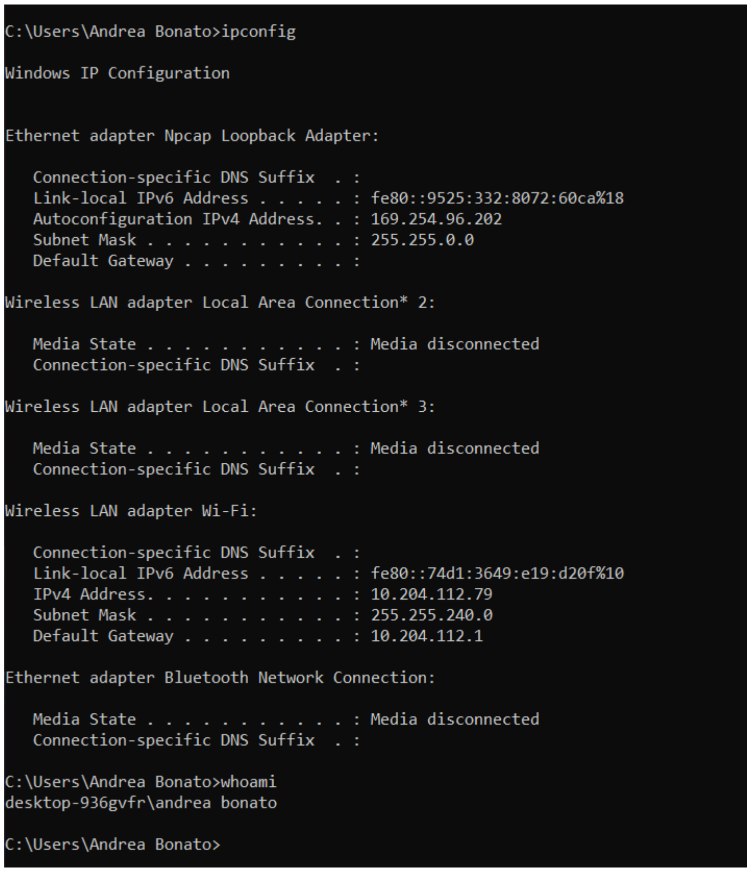


```
[TCP segmen
SLE=1 SRE=2
```

```
Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4497:bccb:f3a:9f5f%9
   IPv4 Address. . . . . . . . . . . : 192.168.0.110
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>
```

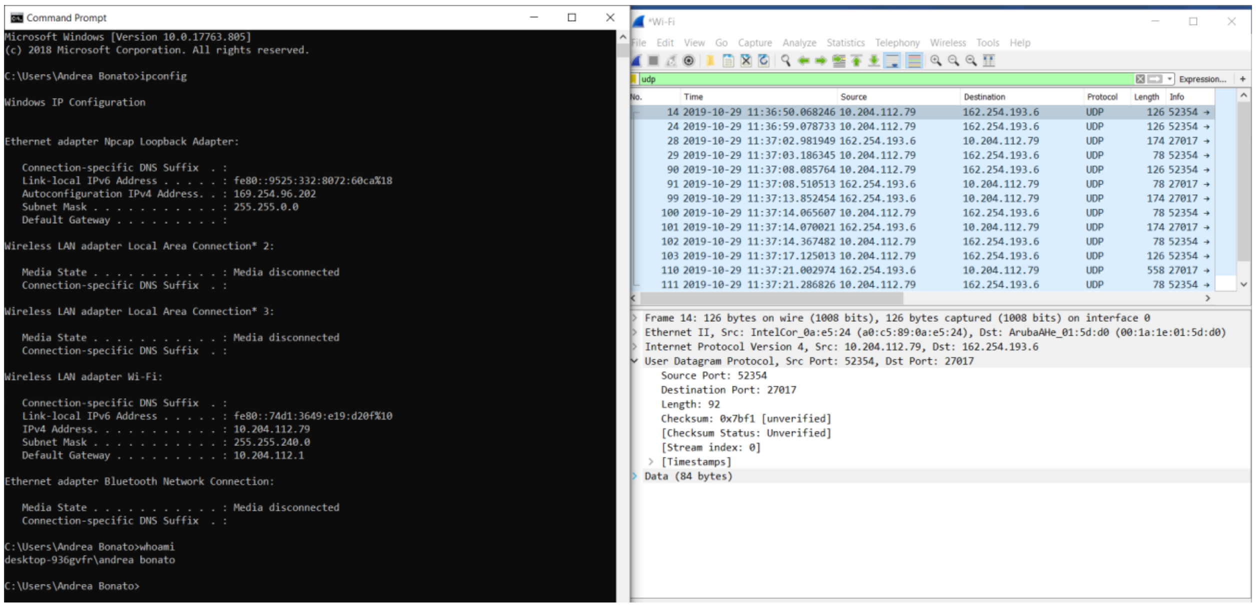
By looking at the graph we can see that the phase started slowly around 0-2 seconds which can be considered the slow start. The congestion avoidance takes over after the 2nd second. The measured data differs from the behaviour of TCP that we studied because it seems that the HTTP server has an enforced rate limit of some sort. This does not seem to be caused by the flow control of the window and server.

Section 2 – Wire Shark Lab UDP



```
C:\Users\Andrea Bonato>ipconfig

Windows IP Configuration


Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9525:332:8072:60ca%18
   Autoconfiguration IPv4 Address. . : 169.254.96.202
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::74d1:3649:e19:d20f%10
   IPv4 Address. . . . . . . . . . . : 10.204.112.79
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.204.112.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>whoami
desktop-936gvfr\andrea bonato

C:\Users\Andrea Bonato>
```

1. Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. Name these fields.



```
Microsoft Windows [Version 10.0.17763.805]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Andrea Bonato>ipconfig

Windows IP Configuration


Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9525:332:8072:60ca%18
   Autoconfiguration IPv4 Address. . : 169.254.96.202
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::74d1:3649:e19:d20f%10
   IPv4 Address. . . . . . . . . . . : 10.204.112.79
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.204.112.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>whoami
desktop-936gvfr\andrea bonato

C:\Users\Andrea Bonato>
```

Command Prompt
*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
Expression...

```
No.  Time                       Source          Destination     Protocol Length Info
 14 2019-10-29 11:36:50.068246 10.204.112.79   162.254.193.6   UDP      126 52354 →
 24 2019-10-29 11:36:59.078733 10.204.112.79   162.254.193.6   UDP      126 52354 →
 28 2019-10-29 11:37:02.981949 162.254.193.6   10.204.112.79   UDP      174 27017 →
 29 2019-10-29 11:37:03.186345 10.204.112.79   162.254.193.6   UDP       78 52354 →
 90 2019-10-29 11:37:08.085764 10.204.112.79   162.254.193.6   UDP      126 52354 →
 91 2019-10-29 11:37:08.510513 162.254.193.6   10.204.112.79   UDP       78 27017 →
 99 2019-10-29 11:37:13.852454 162.254.193.6   10.204.112.79   UDP      174 27017 →
100 2019-10-29 11:37:14.065607 10.204.112.79   162.254.193.6   UDP       78 52354 →
101 2019-10-29 11:37:14.070021 162.254.193.6   10.204.112.79   UDP      174 27017 →
102 2019-10-29 11:37:14.367482 10.204.112.79   162.254.193.6   UDP       78 52354 →
103 2019-10-29 11:37:17.125013 10.204.112.79   162.254.193.6   UDP      126 52354 →
110 2019-10-29 11:37:21.002974 162.254.193.6   10.204.112.79   UDP      558 27017 →
111 2019-10-29 11:37:21.286826 10.204.112.79   162.254.193.6   UDP       78 52354 →

> Frame 14: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface 0
> Ethernet II, Src: IntelCor_0a:e5:24 (a0:c5:89:0a:e5:24), Dst: ArubaAHe_01:5d:d0 (00:1a:1e:01:5d:d0)
> Internet Protocol Version 4, Src: 10.204.112.79, Dst: 162.254.193.6
v User Datagram Protocol, Src Port: 52354, Dst Port: 27017
    Source Port: 52354
    Destination Port: 27017
    Length: 92
    Checksum: 0x7bf1 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
> Data (84 bytes)
```

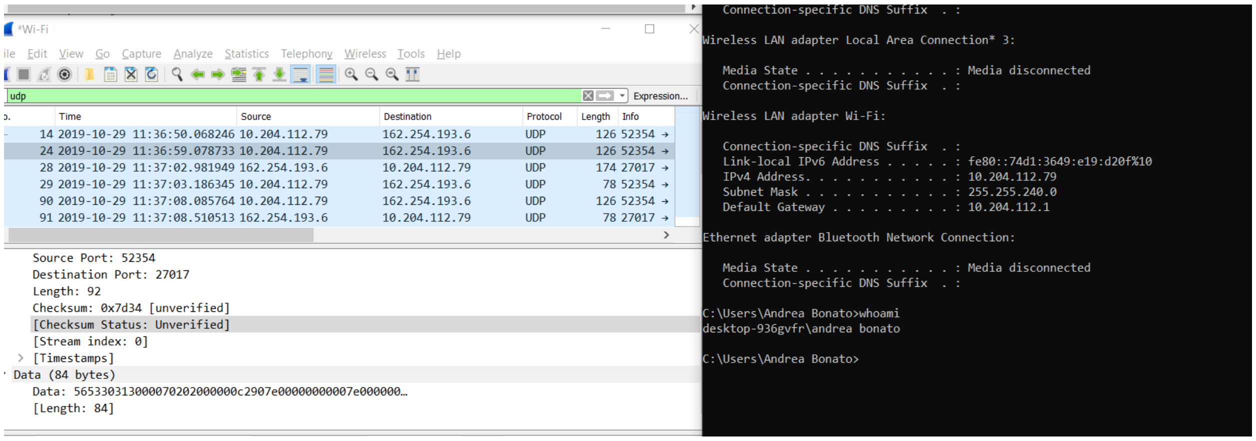
As shown above, there are 4 fields in the UDP header. These fields are source port, destination port, length, and checksum.

2. By consulting the displayed information in Wireshark's packet content field for this packet, determine the length of each of the UDP header fields.

   The header is 8 bytes, so each header field must be 2 bytes long.

3. The value in the Length field is the length of what? Verify you claim with your captured UDP packet.

   The length field in the header is the length of the UDP segment. In includes the size of the data and the header combines. It is 92 bytes in total, where the data itself is 84 bytes and the header is 8 bytes.



```
*Wi-Fi
udp
No.  Time                        Source         Destination    Protocol Length Info
  14 2019-10-29 11:36:50.068246 10.204.112.79  162.254.193.6  UDP         126 52354 →
  24 2019-10-29 11:36:59.078733 10.204.112.79  162.254.193.6  UDP         126 52354 →
  28 2019-10-29 11:37:02.981949 162.254.193.6  10.204.112.79  UDP         174 27017 →
  29 2019-10-29 11:37:03.186345 10.204.112.79  162.254.193.6  UDP          78 52354 →
  90 2019-10-29 11:37:08.085764 10.204.112.79  162.254.193.6  UDP         126 52354 →
  91 2019-10-29 11:37:08.510513 162.254.193.6  10.204.112.79  UDP          78 27017 →

    Source Port: 52354
    Destination Port: 27017
    Length: 92
    Checksum: 0x7d34 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
  Data (84 bytes)
    Data: 56533031300007020200000c2907e00000000007e000000…
    [Length: 84]
```

```
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::74d1:3649:e19:d20f%10
   IPv4 Address. . . . . . . . . . . : 10.204.112.79
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.204.112.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>whoami
desktop-936gvfr\andrea bonato

C:\Users\Andrea Bonato>
```

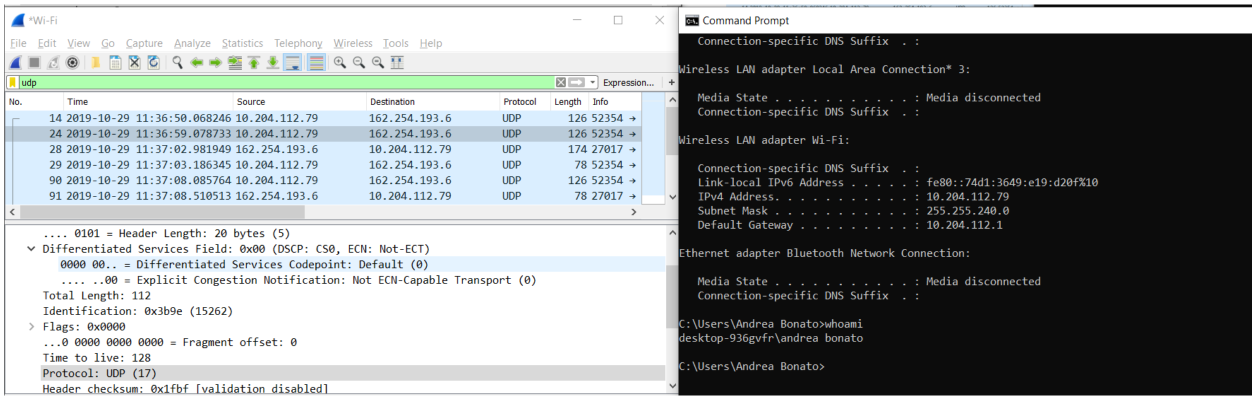
4. What is the maximum number of bytes that be included in a UDP payload?

   The maximum number of bytes that can be included in a UDP payload is (2^16 – 1) - the header all in bytes. This meant that 65536 bytes – 1 byte – 8 bytes = 65527 bytes.

5. What is the largest possible source port?

   Like the question 4, the largest source port will be 2^16 – 1 which is calculated to be 65535.

6. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. To answer this question, you'll need to look into the Protocol field of the IP diagram containing this UDP segment.



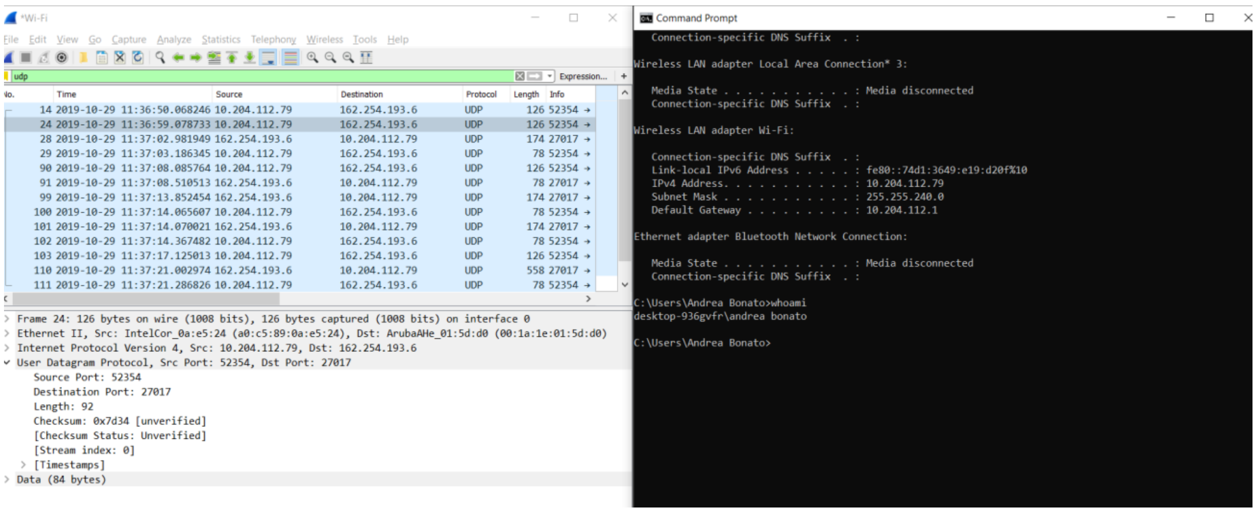
```
*Wi-Fi
udp
No.  Time                        Source         Destination    Protocol Length Info
  14 2019-10-29 11:36:50.068246 10.204.112.79  162.254.193.6  UDP         126 52354 →
  24 2019-10-29 11:36:59.078733 10.204.112.79  162.254.193.6  UDP         126 52354 →
  28 2019-10-29 11:37:02.981949 162.254.193.6  10.204.112.79  UDP         174 27017 →
  29 2019-10-29 11:37:03.186345 10.204.112.79  162.254.193.6  UDP          78 52354 →
  90 2019-10-29 11:37:08.085764 10.204.112.79  162.254.193.6  UDP         126 52354 →
  91 2019-10-29 11:37:08.510513 162.254.193.6  10.204.112.79  UDP          78 27017 →

    .... 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: 112
    Identification: 0x3b9e (15262)
  > Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x1fbf [validation disabled]
```

```
Command Prompt
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::74d1:3649:e19:d20f%10
   IPv4 Address. . . . . . . . . . . : 10.204.112.79
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.204.112.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>whoami
desktop-936gvfr\andrea bonato

C:\Users\Andrea Bonato>
```

As shown in the screen shot above, the protocol UDP number is 17 in decimal notation and 0x11 when converted to hexadecimal

7. Examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. Describe the relationship between the port numbers in the two packets.

Packet 1: Sent

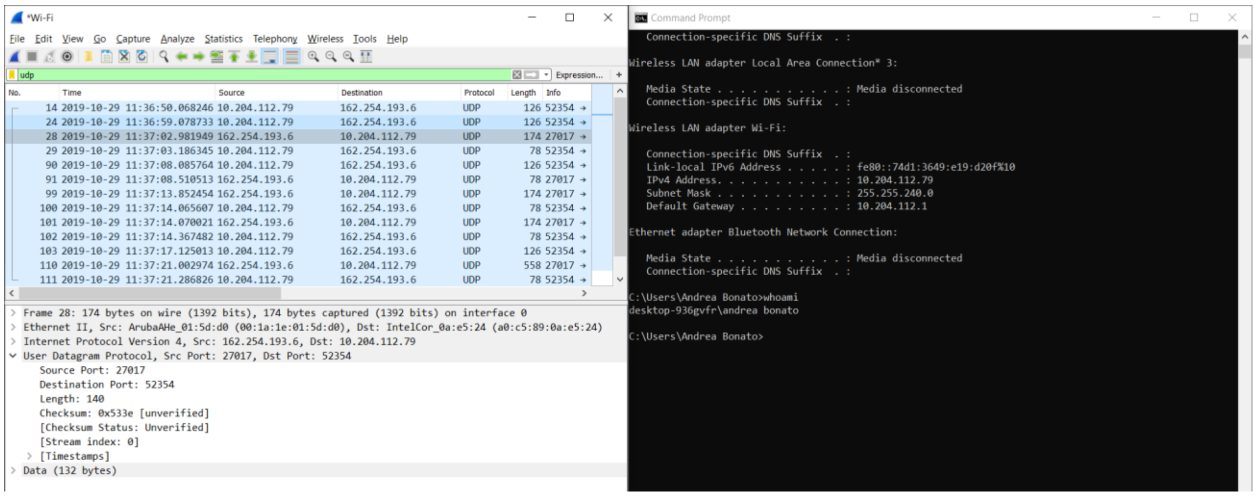

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
Expression...
Command Prompt

```
No.  Time                        Source          Destination     Protocol Length Info
  14 2019-10-29 11:36:50.068246 10.204.112.79   162.254.193.6   UDP        126 52354 →
  24 2019-10-29 11:36:59.078733 10.204.112.79   162.254.193.6   UDP        126 52354 →
  28 2019-10-29 11:37:02.981949 162.254.193.6   10.204.112.79   UDP        174 27017 →
  29 2019-10-29 11:37:03.186345 10.204.112.79   162.254.193.6   UDP         78 52354 →
  90 2019-10-29 11:37:08.085764 10.204.112.79   162.254.193.6   UDP        126 52354 →
  91 2019-10-29 11:37:08.510513 162.254.193.6   10.204.112.79   UDP         78 27017 →
  99 2019-10-29 11:37:13.852454 162.254.193.6   10.204.112.79   UDP        174 27017 →
 100 2019-10-29 11:37:14.065607 10.204.112.79   162.254.193.6   UDP         78 52354 →
 101 2019-10-29 11:37:14.070021 162.254.193.6   10.204.112.79   UDP        174 27017 →
 102 2019-10-29 11:37:14.367482 10.204.112.79   162.254.193.6   UDP         78 52354 →
 103 2019-10-29 11:37:17.125013 10.204.112.79   162.254.193.6   UDP        126 52354 →
 110 2019-10-29 11:37:21.002974 162.254.193.6   10.204.112.79   UDP        558 27017 →
 111 2019-10-29 11:37:21.286826 10.204.112.79   162.254.193.6   UDP         78 52354 →

> Frame 24: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface 0
> Ethernet II, Src: IntelCor_0a:e5:24 (a0:c5:89:0a:e5:24), Dst: ArubaAHe_01:5d:d0 (00:1a:1e:01:5d:d0)
> Internet Protocol Version 4, Src: 10.204.112.79, Dst: 162.254.193.6
v User Datagram Protocol, Src Port: 52354, Dst Port: 27017
    Source Port: 52354
    Destination Port: 27017
    Length: 92
    Checksum: 0x7d34 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
> Data (84 bytes)
```

```
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::74d1:3649:e19:d20f%10
   IPv4 Address. . . . . . . . . . . : 10.204.112.79
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.204.112.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>whoami
desktop-936gvfr\andrea bonato

C:\Users\Andrea Bonato>
```

Packet 2: Received

.

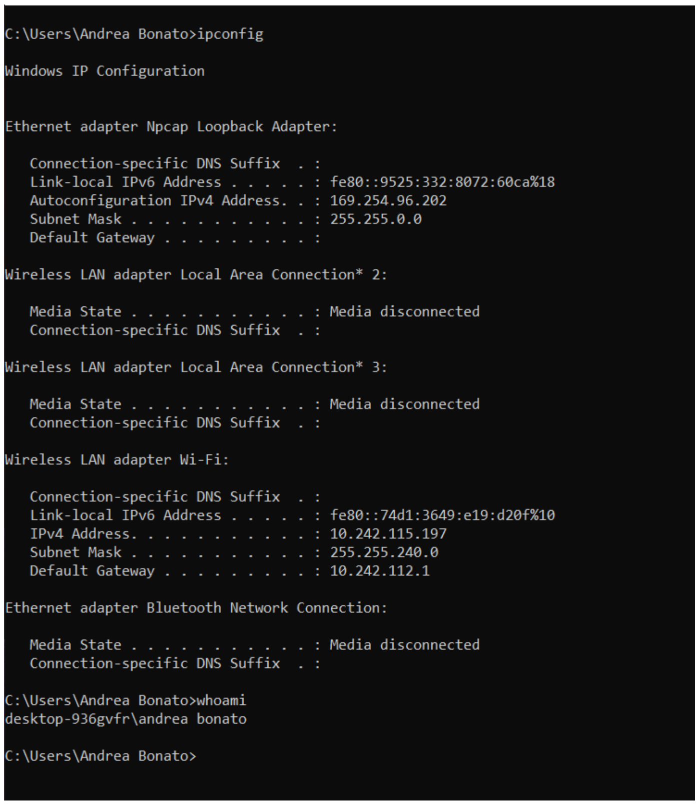

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
Expression...
Command Prompt

```
No.  Time                        Source          Destination     Protocol Length Info
  14 2019-10-29 11:36:50.068246 10.204.112.79   162.254.193.6   UDP        126 52354 →
  24 2019-10-29 11:36:59.078733 10.204.112.79   162.254.193.6   UDP        126 52354 →
  28 2019-10-29 11:37:02.981949 162.254.193.6   10.204.112.79   UDP        174 27017 →
  29 2019-10-29 11:37:03.186345 10.204.112.79   162.254.193.6   UDP         78 52354 →
  90 2019-10-29 11:37:08.085764 10.204.112.79   162.254.193.6   UDP        126 52354 →
  91 2019-10-29 11:37:08.510513 162.254.193.6   10.204.112.79   UDP         78 27017 →
  99 2019-10-29 11:37:13.852454 162.254.193.6   10.204.112.79   UDP        174 27017 →
 100 2019-10-29 11:37:14.065607 10.204.112.79   162.254.193.6   UDP         78 52354 →
 101 2019-10-29 11:37:14.070021 162.254.193.6   10.204.112.79   UDP        174 27017 →
 102 2019-10-29 11:37:14.367482 10.204.112.79   162.254.193.6   UDP         78 52354 →
 103 2019-10-29 11:37:17.125013 10.204.112.79   162.254.193.6   UDP        126 52354 →
 110 2019-10-29 11:37:21.002974 162.254.193.6   10.204.112.79   UDP        558 27017 →
 111 2019-10-29 11:37:21.286826 10.204.112.79   162.254.193.6   UDP         78 52354 →

> Frame 28: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface 0
> Ethernet II, Src: ArubaAHe_01:5d:d0 (00:1a:1e:01:5d:d0), Dst: IntelCor_0a:e5:24 (a0:c5:89:0a:e5:24)
> Internet Protocol Version 4, Src: 162.254.193.6, Dst: 10.204.112.79
v User Datagram Protocol, Src Port: 27017, Dst Port: 52354
    Source Port: 27017
    Destination Port: 52354
    Length: 140
    Checksum: 0x533e [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
> Data (132 bytes)
```

```
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::74d1:3649:e19:d20f%10
   IPv4 Address. . . . . . . . . . . : 10.204.112.79
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.204.112.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>whoami
desktop-936gvfr\andrea bonato

C:\Users\Andrea Bonato>
```

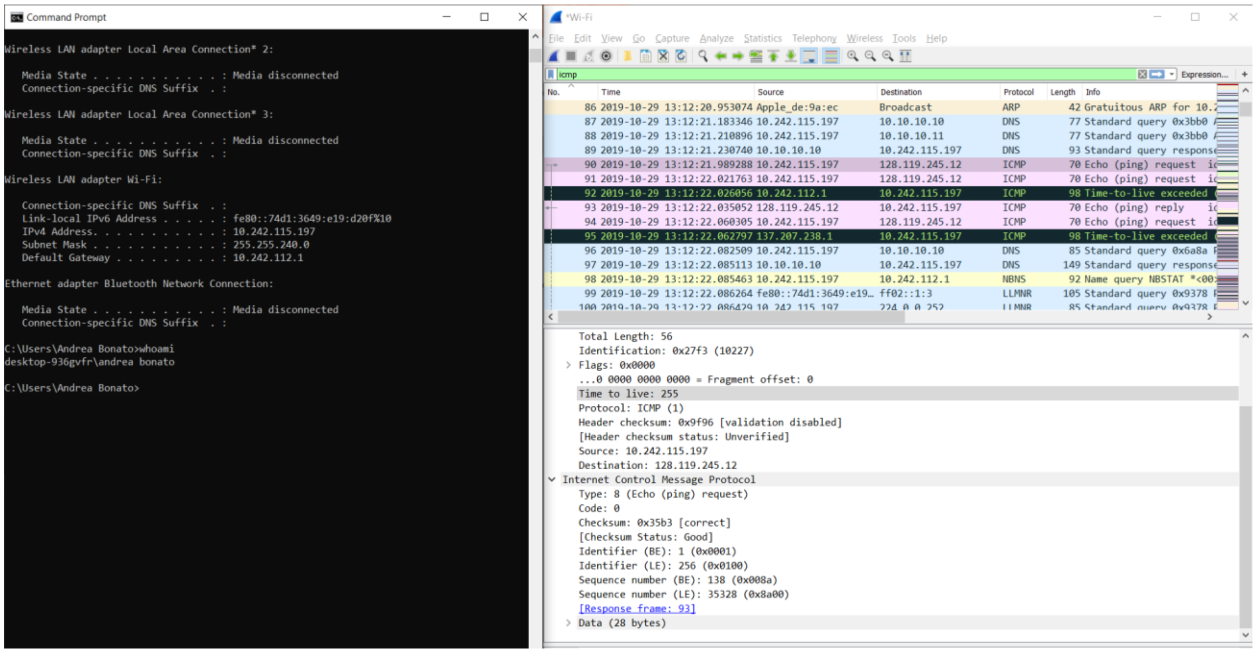
The source port of the UDP packet sent by the client is the same as the destination of the packet received, similarly, the destination port of the client is the source port number of the response.

Section 3 – Wireshark Lab IP



```
C:\Users\Andrea Bonato>ipconfig

Windows IP Configuration


Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9525:332:8072:60ca%18
   Autoconfiguration IPv4 Address. . : 169.254.96.202
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::74d1:3649:e19:d20f%10
   IPv4 Address. . . . . . . . . . . : 10.242.115.197
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.242.112.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>whoami
desktop-936gvfr\andrea bonato

C:\Users\Andrea Bonato>
```

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?

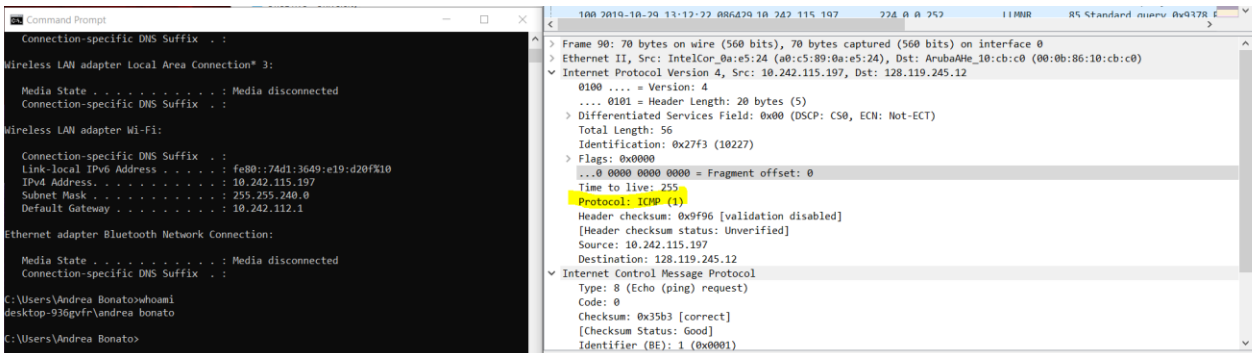

Command Prompt
*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Expression...

```
Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::74d1:3649:e19:d20f%10
   IPv4 Address. . . . . . . . . . . : 10.242.115.197
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.242.112.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>whoami
desktop-936gvfr\andrea bonato

C:\Users\Andrea Bonato>
```

```
No.  Time                       Source                  Destination      Protocol Length Info
 86 2019-10-29 13:12:20.953074 Apple_de:9a:ec          Broadcast        ARP       42 Gratuitous ARP for 10.2
 87 2019-10-29 13:12:21.183346 10.242.115.197          10.10.10.10      DNS       77 Standard query 0x3bb0 
 88 2019-10-29 13:12:21.210896 10.242.115.197          10.10.10.11      DNS       77 Standard query 0x3bb0 
 89 2019-10-29 13:12:21.230740 10.10.10.10             10.242.115.197   DNS       93 Standard query response
 90 2019-10-29 13:12:21.989288 10.242.115.197          128.119.245.12   ICMP      70 Echo (ping) request  i
 91 2019-10-29 13:12:22.021763 10.242.115.197          128.119.245.12   ICMP      70 Echo (ping) request  i
 92 2019-10-29 13:12:22.026056 10.242.112.1            10.242.115.197   ICMP      98 Time-to-live exceeded 
 93 2019-10-29 13:12:22.035052 128.119.245.12          10.242.115.197   ICMP      70 Echo (ping) reply    i
 94 2019-10-29 13:12:22.060305 10.242.115.197          128.119.245.12   ICMP      70 Echo (ping) request  i
 95 2019-10-29 13:12:22.062797 137.207.238.1           10.242.115.197   ICMP      98 Time-to-live exceeded 
 96 2019-10-29 13:12:22.082509 10.242.115.197          10.10.10.10      DNS       85 Standard query 0x6a8a 
 97 2019-10-29 13:12:22.085113 10.10.10.10             10.242.115.197   DNS      149 Standard query response
 98 2019-10-29 13:12:22.085463 10.242.115.197          10.242.112.1     NBNS      92 Name query NBSTAT *<00
 99 2019-10-29 13:12:22.086264 fe80::74d1:3649:e19…    ff02::1:3        LLMNR    105 Standard query 0x9378 
100 2019-10-29 13:12:22.086429 10.242.115.197          224.0.0.252      LLMNR     85 Standard query 0x9378 

    Total Length: 56
    Identification: 0x27f3 (10227)
  > Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x9f96 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.242.115.197
    Destination: 128.119.245.12
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x35b3 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 138 (0x008a)
    Sequence number (LE): 35328 (0x8a00)
    [Response frame: 93]
  > Data (28 bytes)
```

The IP address of my computer, as given by the Source for the echo request, is 10.242.115.197.

2. Within the IP packet header, what is the value in the upper layer protocol field?



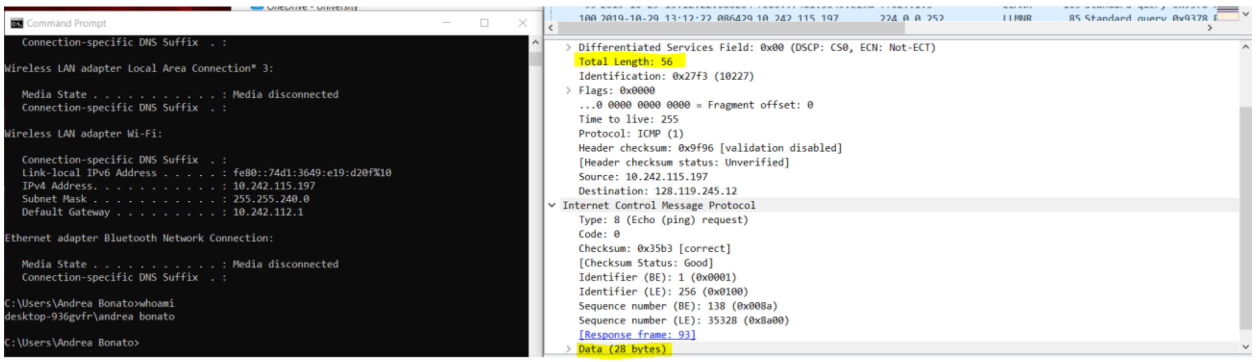
```
Command Prompt
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::74d1:3649:e19:d20f%10
   IPv4 Address. . . . . . . . . . . : 10.242.115.197
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.242.112.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>whoami
desktop-936gvfr\andrea bonato

C:\Users\Andrea Bonato>
```

```
100 2019-10-29 13:12:22 086429 10 242 115 197      224 0 0 252       LLMNR      85 Standard query 0x9378 F
> Frame 90: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: IntelCor_0a:e5:24 (a0:c5:89:0a:e5:24), Dst: ArubaAHe_10:cb:c0 (00:0b:86:10:cb:c0)
v Internet Protocol Version 4, Src: 10.242.115.197, 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: 0x27f3 (10227)
  > Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x9f96 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.242.115.197
    Destination: 128.119.245.12
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x35b3 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
```

The IP packet header contains the upper layer protocol field that states ICMP(1)

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.
   There are 28 bytes in the header, and the payload contains the length – header size bytes. This calculates to 28 bytes for the payload

.



```
Command Prompt
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::74d1:3649:e19:d20f%10
   IPv4 Address. . . . . . . . . . . : 10.242.115.197
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.242.112.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>whoami
desktop-936gvfr\andrea bonato

C:\Users\Andrea Bonato>
```

```
100 2019-10-29 13:12:22 086429 10 242 115 197      224 0 0 252       LLMNR      85 Standard query 0x9378 F
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x27f3 (10227)
  > Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x9f96 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.242.115.197
    Destination: 128.119.245.12
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x35b3 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 138 (0x008a)
    Sequence number (LE): 35328 (0x8a00)
    [Response frame: 93]
  > Data (28 bytes)
```

4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.
   There has been no fragmentation here since we do not see any IPv4 fragments in either of the previous screen shots.

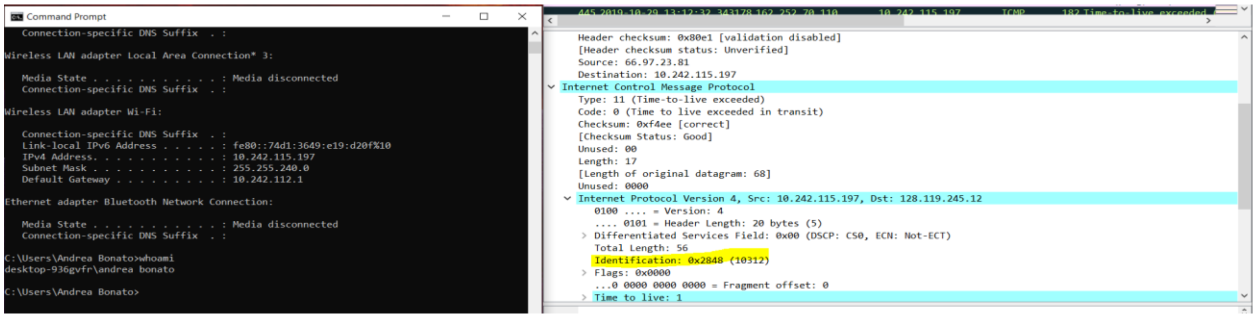
5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?
   There are two fields in the datagram that change from one datagram to another. The Time to Live field is changing between IP datagrams and so is the identification field.

6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?
   There are several fields that stay constant from one datagram to another. One field is the version. In every datagram, IPv4 was used. Similarly, because of IPv4, the length of the header itself remains the same between each datagram. Finally, the source and destination IP address remain the same between the client and the host.

The fields that change are the identification field and the time to live field. This is how Wireshark are able to trace the packets.

7. Describe the pattern you see in the values in the Identification field of the IP datagram. Next find the series of ICMP TTL exceeded replies sent to your computer by the nearest router.
The values in the identification field seem to be increasing and incrementing per datagram. The following images will be the comparison of two datagrams and their identifications.

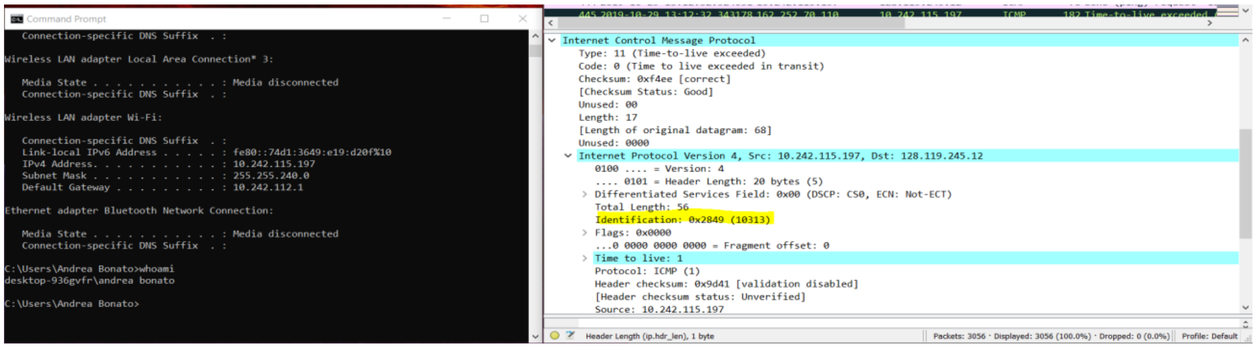
Datagram 1



```
Command Prompt
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::74d1:3649:e19:d20f%10
   IPv4 Address. . . . . . . . . . . : 10.242.115.197
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.242.112.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>whoami
desktop-936gvfr\andrea bonato

C:\Users\Andrea Bonato>
```

```
445 2019-10-29 13:12:32.343178 162.252.70.110      10.242.115.197      ICMP      182 Time-to-live exceeded
    Header checksum: 0x80e1 [validation disabled]
    [Header checksum status: Unverified]
    Source: 66.97.23.81
    Destination: 10.242.115.197
v Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ee [correct]
    [Checksum Status: Good]
    Unused: 00
    Length: 17
    [Length of original datagram: 68]
    Unused: 0000
  v Internet Protocol Version 4, Src: 10.242.115.197, 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: 0x2848 (10312)
    > Flags: 0x0000
      ...0 0000 0000 0000 = Fragment offset: 0
    > Time to live: 1
```

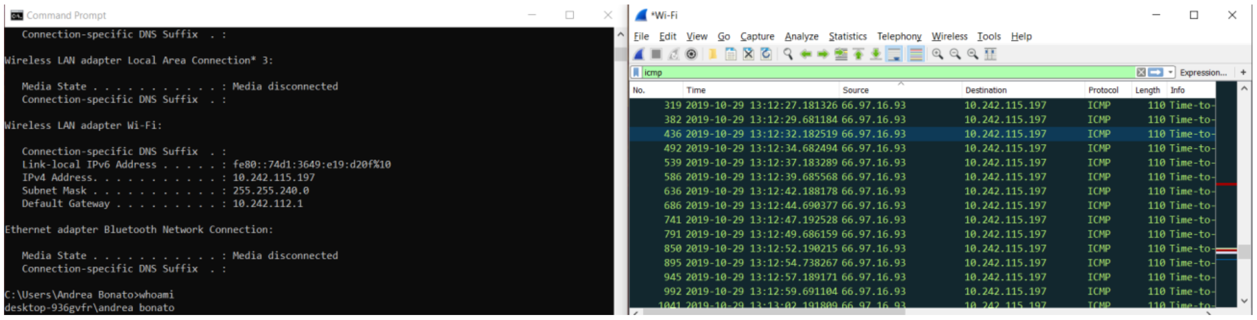
Datagram 2



```
Command Prompt
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::74d1:3649:e19:d20f%10
   IPv4 Address. . . . . . . . . . . : 10.242.115.197
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.242.112.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>whoami
desktop-936gvfr\andrea bonato

C:\Users\Andrea Bonato>
```

```
445 2019-10-29 13:12:32.343178 162.252.70.110      10.242.115.197      ICMP      182 Time-to-live exceeded
v Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ee [correct]
    [Checksum Status: Good]
    Unused: 00
    Length: 17
    [Length of original datagram: 68]
    Unused: 0000
  v Internet Protocol Version 4, Src: 10.242.115.197, 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: 0x2849 (10313)
    > Flags: 0x0000
      ...0 0000 0000 0000 = Fragment offset: 0
    > Time to live: 1
      Protocol: ICMP (1)
      Header checksum: 0x9d41 [validation disabled]
      [Header checksum status: Unverified]
      Source: 10.242.115.197

Header Length (ip.hdr_len), 1 byte    Packets: 3056 · Displayed: 3056 (100.0%) · Dropped: 0 (0.0%)    Profile: Default
```

The following image is a list of time limit exceeded with the closest router.



```
Command Prompt
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::74d1:3649:e19:d20f%10
   IPv4 Address. . . . . . . . . . . : 10.242.115.197
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.242.112.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>whoami
desktop-936gvfr\andrea bonato
```

```
*Wi-Fi
icmp
No.   Time                       Source        Destination      Protocol  Length Info
  319 2019-10-29 13:12:27.181326 66.97.16.93   10.242.115.197   ICMP      110 Time-to-
  382 2019-10-29 13:12:29.681184 66.97.16.93   10.242.115.197   ICMP      110 Time-to-
  436 2019-10-29 13:12:32.182519 66.97.16.93   10.242.115.197   ICMP      110 Time-to-
  492 2019-10-29 13:12:34.682494 66.97.16.93   10.242.115.197   ICMP      110 Time-to-
  539 2019-10-29 13:12:37.183289 66.97.16.93   10.242.115.197   ICMP      110 Time-to-
  586 2019-10-29 13:12:39.685568 66.97.16.93   10.242.115.197   ICMP      110 Time-to-
  636 2019-10-29 13:12:42.188178 66.97.16.93   10.242.115.197   ICMP      110 Time-to-
  686 2019-10-29 13:12:44.690377 66.97.16.93   10.242.115.197   ICMP      110 Time-to-
  741 2019-10-29 13:12:47.192528 66.97.16.93   10.242.115.197   ICMP      110 Time-to-
  791 2019-10-29 13:12:49.686159 66.97.16.93   10.242.115.197   ICMP      110 Time-to-
  850 2019-10-29 13:12:52.190215 66.97.16.93   10.242.115.197   ICMP      110 Time-to-
  895 2019-10-29 13:12:54.738267 66.97.16.93   10.242.115.197   ICMP      110 Time-to-
  945 2019-10-29 13:12:57.189171 66.97.16.93   10.242.115.197   ICMP      110 Time-to-
  992 2019-10-29 13:12:59.691104 66.97.16.93   10.242.115.197   ICMP      110 Time-to-
 1041 2019-10-29 13:13:02.191809 66.97.16.93   10.242.115.197   ICMP      110 Time-to-
```

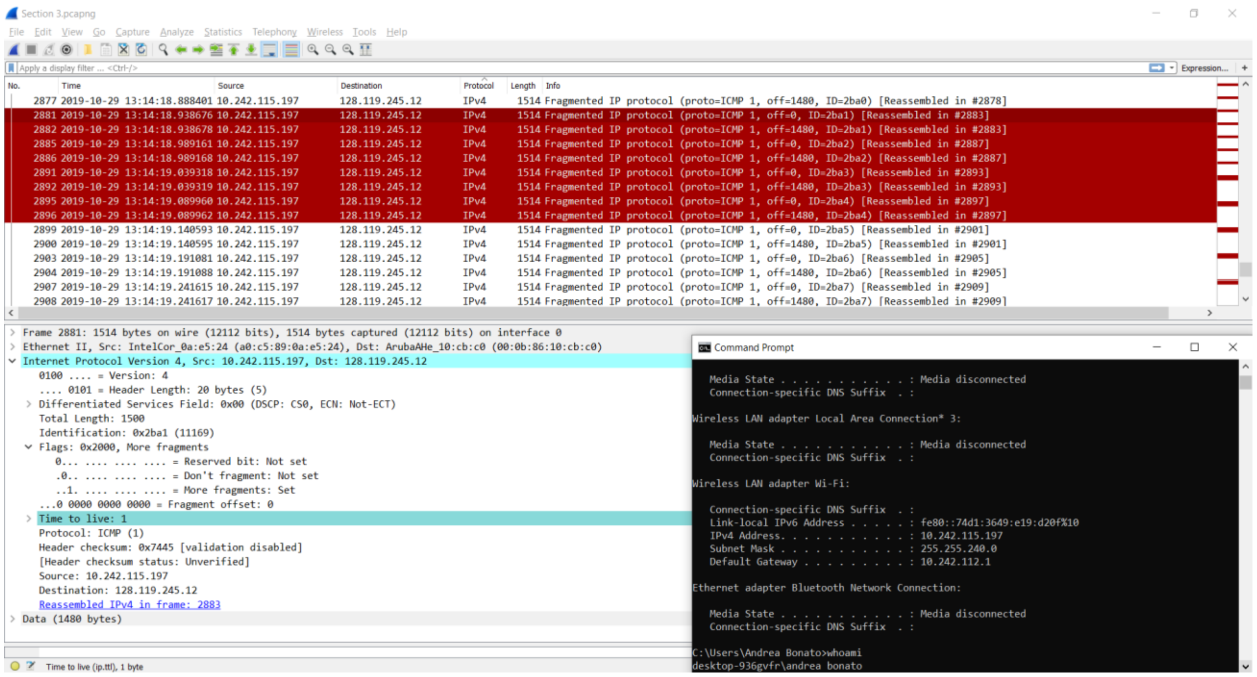
8. What is the value in the Identification field and the TTL field?
The value in the identification field is 10313 as shown in the screen shots. The TTL field in this example is 1.

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?

   In this test, the identification values increment and increase between each ICMP TTL-Exceeded reply. The TTL field varies between time and does cycle through 1 on multiple occasions.

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

    As shown in the following image. There is the presence of IPv4 fragments. Wireshark shows the breakdown of the different sequences and segments and it generally resembles fragmented datagrams.


Section 3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.  Time                       Source          Destination     Protocol Length Info
2877 2019-10-29 13:14:18.888401 10.242.115.197  128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2ba0) [Reassembled in #2878]
2881 2019-10-29 13:14:18.938676 10.242.115.197  128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=2ba1) [Reassembled in #2883]
2882 2019-10-29 13:14:18.938678 10.242.115.197  128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2ba1) [Reassembled in #2883]
2885 2019-10-29 13:14:18.989161 10.242.115.197  128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=2ba2) [Reassembled in #2887]
2886 2019-10-29 13:14:18.989168 10.242.115.197  128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2ba2) [Reassembled in #2887]
2891 2019-10-29 13:14:19.039318 10.242.115.197  128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=2ba3) [Reassembled in #2893]
2892 2019-10-29 13:14:19.039319 10.242.115.197  128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2ba3) [Reassembled in #2893]
2895 2019-10-29 13:14:19.089960 10.242.115.197  128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=2ba4) [Reassembled in #2897]
2896 2019-10-29 13:14:19.089962 10.242.115.197  128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2ba4) [Reassembled in #2897]
2899 2019-10-29 13:14:19.140593 10.242.115.197  128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=2ba5) [Reassembled in #2901]
2900 2019-10-29 13:14:19.140595 10.242.115.197  128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2ba5) [Reassembled in #2901]
2903 2019-10-29 13:14:19.191081 10.242.115.197  128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=2ba6) [Reassembled in #2905]
2904 2019-10-29 13:14:19.191088 10.242.115.197  128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2ba6) [Reassembled in #2905]
2907 2019-10-29 13:14:19.241615 10.242.115.197  128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=2ba7) [Reassembled in #2909]
2908 2019-10-29 13:14:19.241617 10.242.115.197  128.119.245.12  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2ba7) [Reassembled in #2909]
```

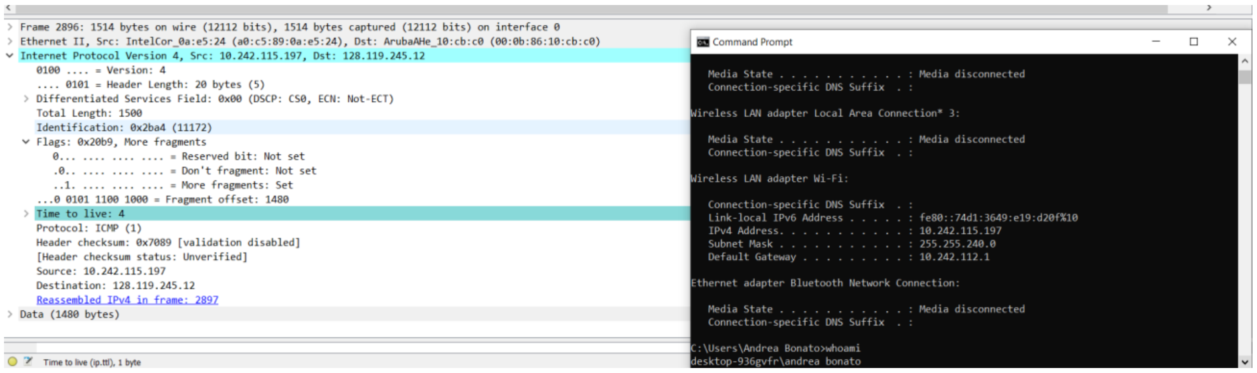
```
> Frame 2881: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
> Ethernet II, Src: IntelCor_0a:e5:24 (a0:c5:89:0a:e5:24), Dst: ArubaAHe_10:cb:c0 (00:0b:86:10:cb:c0)
v Internet Protocol Version 4, Src: 10.242.115.197, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x2ba1 (11169)
  v Flags: 0x2000, More fragments
      0... .... .... .... = Reserved bit: Not set
      .0.. .... .... .... = Don't fragment: Not set
      ..1. .... .... .... = More fragments: Set
    ...0 0000 0000 0000 = Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x7445 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.242.115.197
    Destination: 128.119.245.12
    Reassembled IPv4 in frame: 2883
> Data (1480 bytes)
```

```
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::74d1:3649:e19:d20f%10
   IPv4 Address. . . . . . . . . . . : 10.242.115.197
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.242.112.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>whoami
desktop-936gvfr\andrea bonato
```

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?

    As shown in the image above, the flag that states that More fragments are “set” is how the header explains that it is a fragment and there are more of them. The fragment offset is equal to 0 which indicates that it is the first fragment.

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?



```
> Frame 2896: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
> Ethernet II, Src: IntelCor_0a:e5:24 (a0:c5:89:0a:e5:24), Dst: ArubaAHe_10:cb:c0 (00:0b:86:10:cb:c0)
v Internet Protocol Version 4, Src: 10.242.115.197, 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: 0x2ba4 (11172)
  v Flags: 0x20b9, More fragments
      0... .... .... .... = Reserved bit: Not set
      .0.. .... .... .... = Don't fragment: Not set
      ..1. .... .... .... = More fragments: Set
    ...0 0101 1100 1000 = Fragment offset: 1480
  > Time to live: 4
    Protocol: ICMP (1)
    Header checksum: 0x7089 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.242.115.197
    Destination: 128.119.245.12
    Reassembled IPv4 in frame: 2897
> Data (1480 bytes)

Time to live (ip.ttl), 1 byte
```

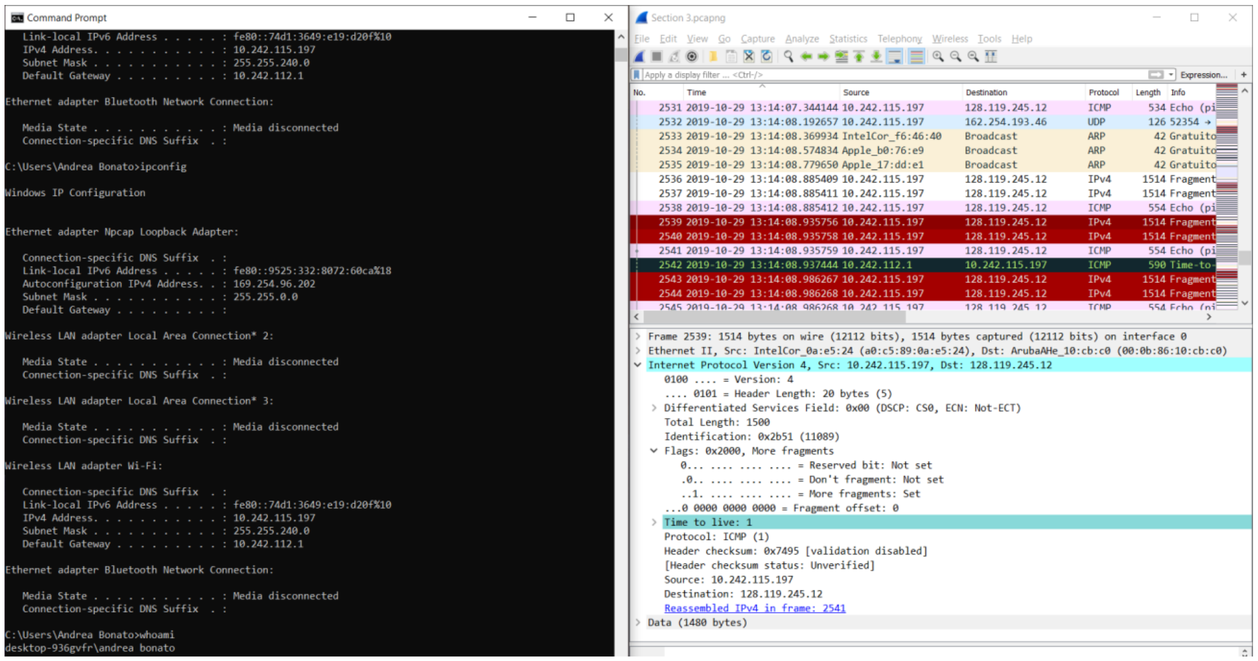
Command Prompt

```
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::74d1:3649:e19:d20f%10
   IPv4 Address. . . . . . . . . . . : 10.242.115.197
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.242.112.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>whoami
desktop-936gvfr\andrea bonato
```

As shown above, the fragment offset is 1480. This means that it is the second fragment. The More Fragment flag still says set, that means that there more fragments available. If it was set to “clear” then it would be the last fragment

13. What fields change in the IP header between the first and second fragment? Now find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in ping plotter to be 3500. How many fragments were created from the original datagram? What fields change in the IP header among the fragments?

The total length, and the fragment offset are the only two values that changed between the first and second fragment.



Command Prompt

```
   Link-local IPv6 Address . . . . . : fe80::74d1:3649:e19:d20f%10
   IPv4 Address. . . . . . . . . . . : 10.242.115.197
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.242.112.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>ipconfig

Windows IP Configuration


Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9525:332:8072:60ca%18
   Autoconfiguration IPv4 Address. . : 169.254.96.202
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::74d1:3649:e19:d20f%10
   IPv4 Address. . . . . . . . . . . : 10.242.115.197
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.242.112.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>whoami
desktop-936gvfr\andrea bonato
```

Section 3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.   Time                       Source             Destination      Protocol Length Info
 2531 2019-10-29 13:14:07.344144 10.242.115.197     128.119.245.12   ICMP      534 Echo (pi
 2532 2019-10-29 13:14:08.192657 10.242.115.197     162.254.193.46   UDP       126 52354 →
 2533 2019-10-29 13:14:08.369934 IntelCor_f6:46:40  Broadcast        ARP        42 Gratuito
 2534 2019-10-29 13:14:08.574834 Apple_b0:76:e9     Broadcast        ARP        42 Gratuito
 2535 2019-10-29 13:14:08.779650 Apple_17:dd:e1     Broadcast        ARP        42 Gratuito
 2536 2019-10-29 13:14:08.885409 10.242.115.197     128.119.245.12   IPv4     1514 Fragment
 2537 2019-10-29 13:14:08.885411 10.242.115.197     128.119.245.12   IPv4     1514 Fragment
 2538 2019-10-29 13:14:08.885412 10.242.115.197     128.119.245.12   ICMP      554 Echo (pi
 2539 2019-10-29 13:14:08.935756 10.242.115.197     128.119.245.12   IPv4     1514 Fragment
 2540 2019-10-29 13:14:08.935758 10.242.115.197     128.119.245.12   IPv4     1514 Fragment
 2541 2019-10-29 13:14:08.935759 10.242.115.197     128.119.245.12   ICMP      554 Echo (pi
 2542 2019-10-29 13:14:08.937444 10.242.112.1       10.242.115.197   ICMP      590 Time-to-
 2543 2019-10-29 13:14:08.986267 10.242.115.197     128.119.245.12   IPv4     1514 Fragment
 2544 2019-10-29 13:14:08.986268 10.242.115.197     128.119.245.12   IPv4     1514 Fragment
 2545 2019-10-29 13:14:08.986268 10.242.115.197     128.119.245.12   ICMP      554 Echo (pi

> Frame 2539: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
> Ethernet II, Src: IntelCor_0a:e5:24 (a0:c5:89:0a:e5:24), Dst: ArubaAHe_10:cb:c0 (00:0b:86:10:cb:c0)
v Internet Protocol Version 4, Src: 10.242.115.197, 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: 0x2b51 (11089)
  v Flags: 0x2000, More fragments
      0... .... .... .... = Reserved bit: Not set
      .0.. .... .... .... = Don't fragment: Not set
      ..1. .... .... .... = More fragments: Set
    ...0 0000 0000 0000 = Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x7495 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.242.115.197
    Destination: 128.119.245.12
    Reassembled IPv4 in frame: 2541
> Data (1480 bytes)
```

As shown in the screen shot above, there were 3 total fragments that were made. Compared to the first fragment, the other fragments have different fragment offsets. However, all fragments seem to have different lengths, and other offsets.