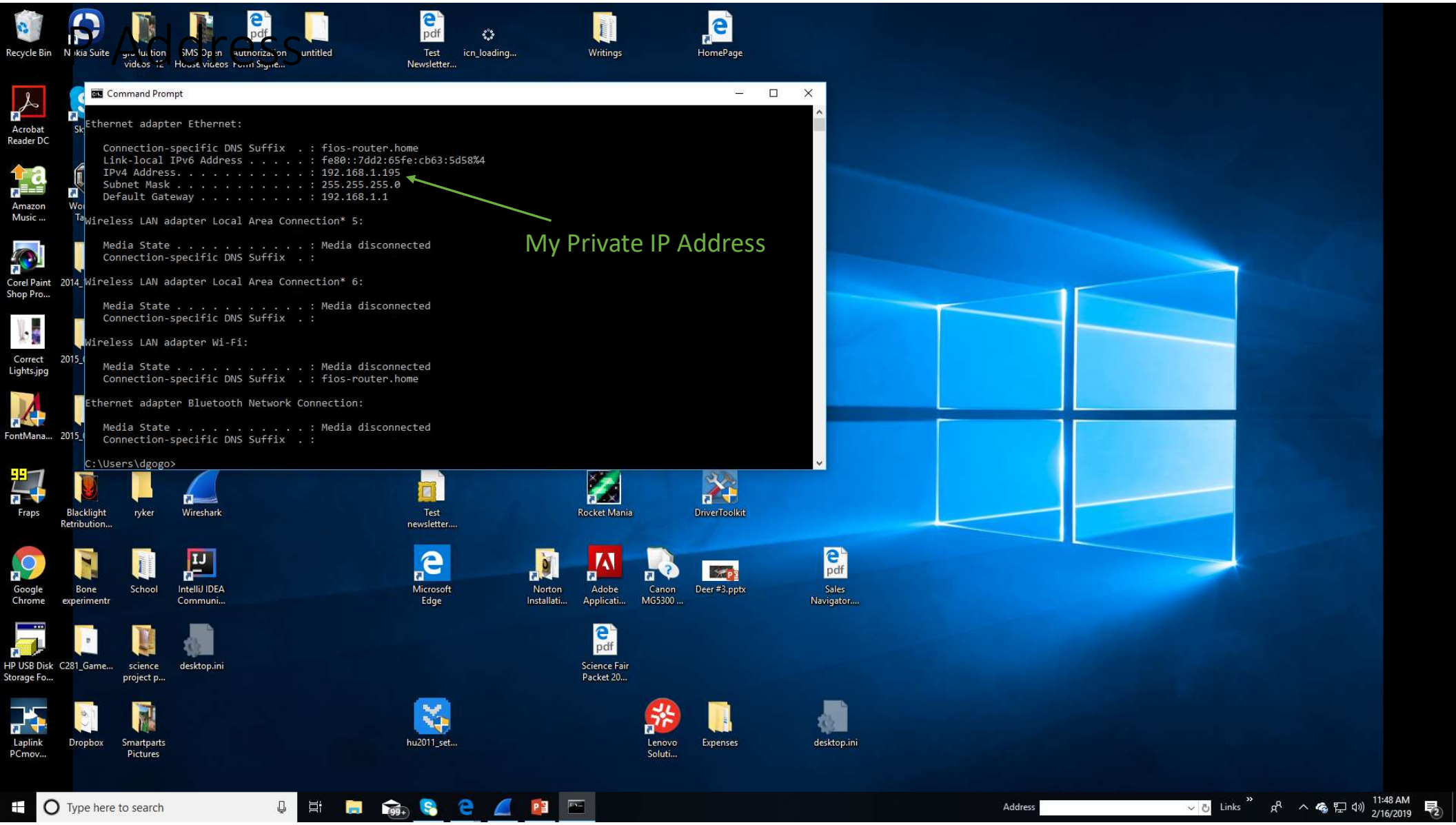
Wireshark Lab 3 - TCP

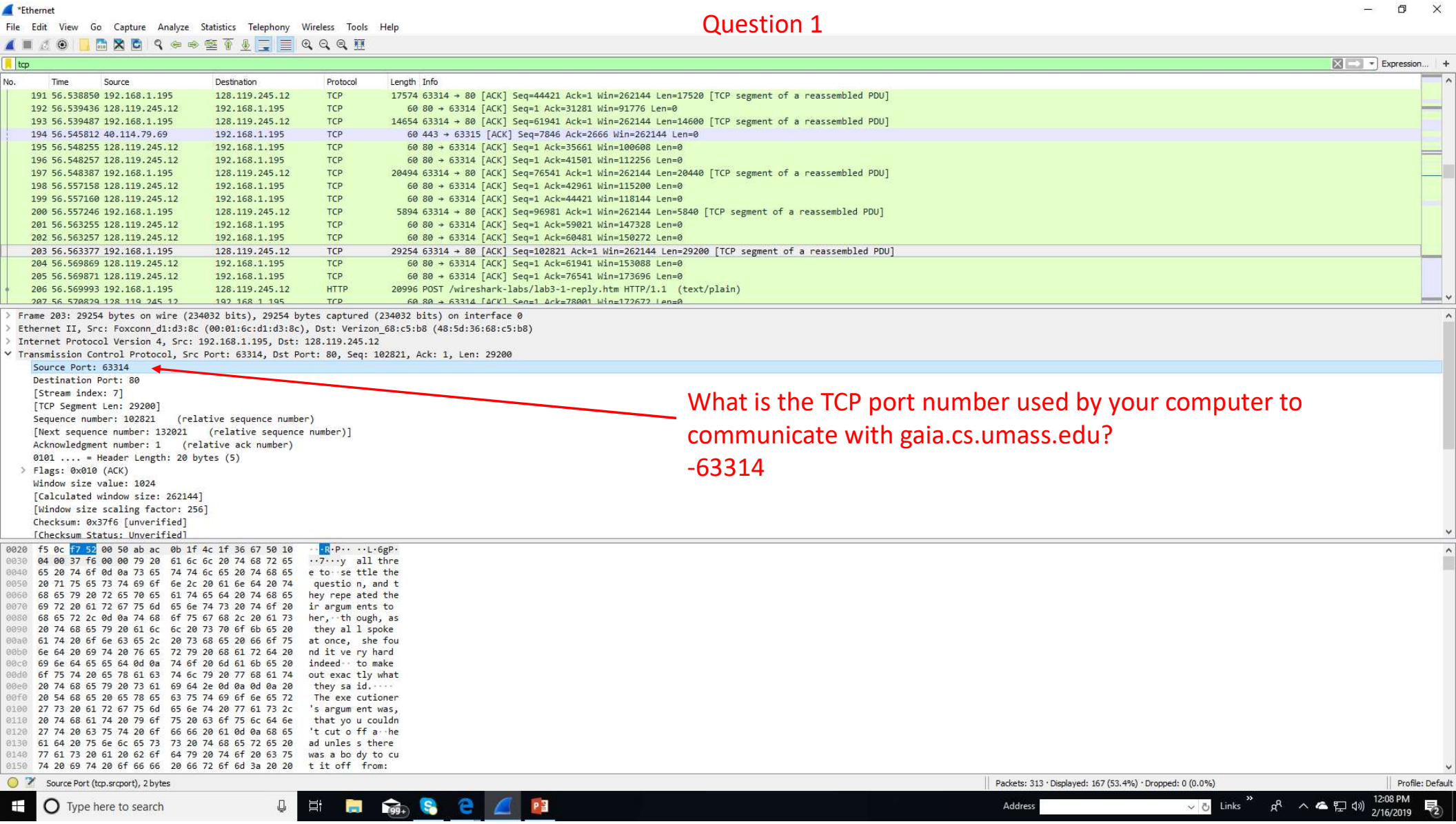
IT 520 –A – Enterprise Infrastructure & Networks

David Gogolkiewicz

IP Address


Command Prompt
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . : fios-router.home
Link-local IPv6 Address . . . . . : fe80::7dd2:65fe:cb63:5d58%4
IPv4 Address. . . . . : 192.168.1.195
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
Wireless LAN adapter Local Area Connection* 5:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 6:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Wi-Fi:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : fios-router.home
Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
C:\Users\dgogo>
My Private IP Address

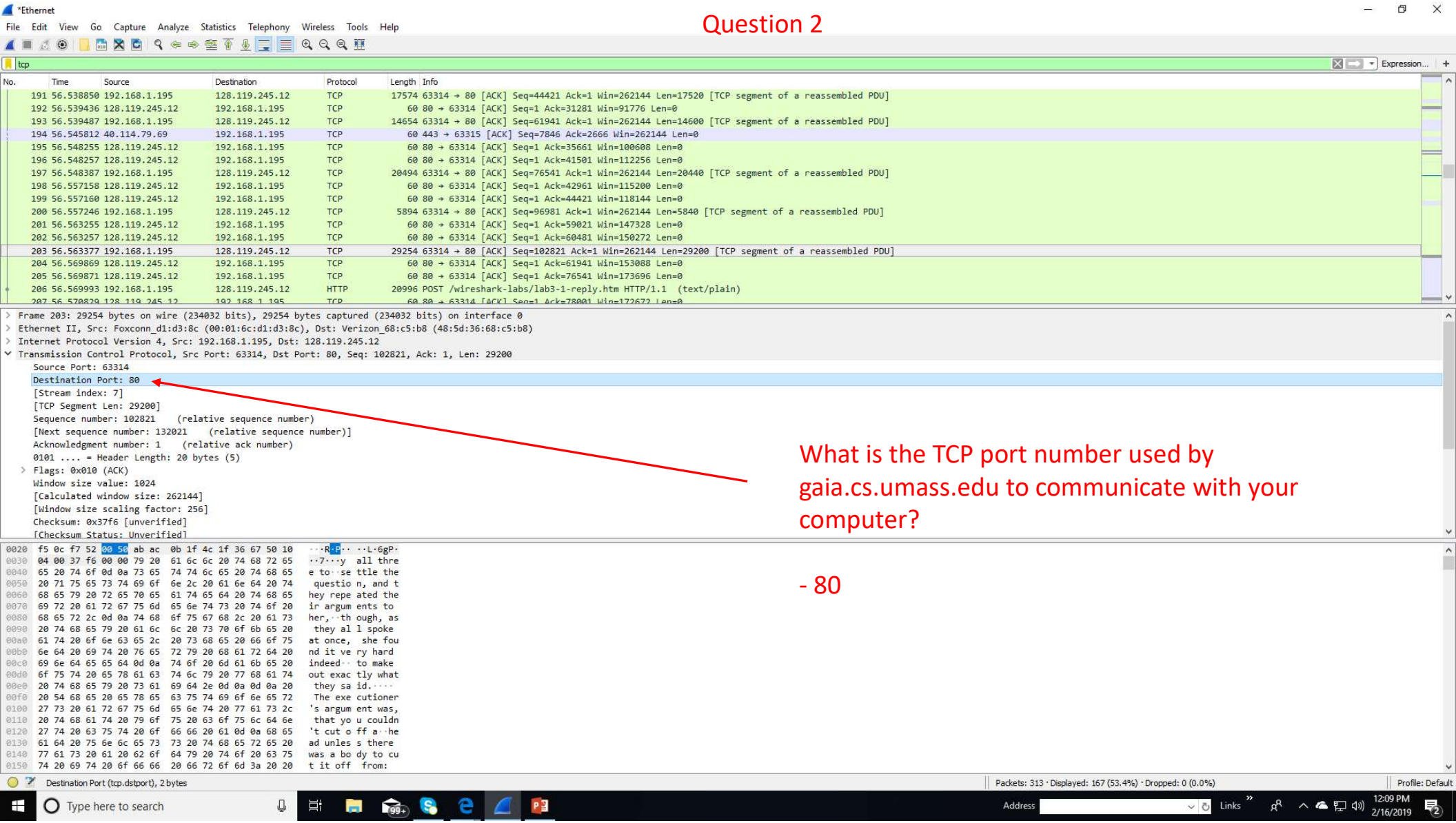
Question 1



What is the TCP port number used by your computer to communicate with gaia.cs.umass.edu?

-63314

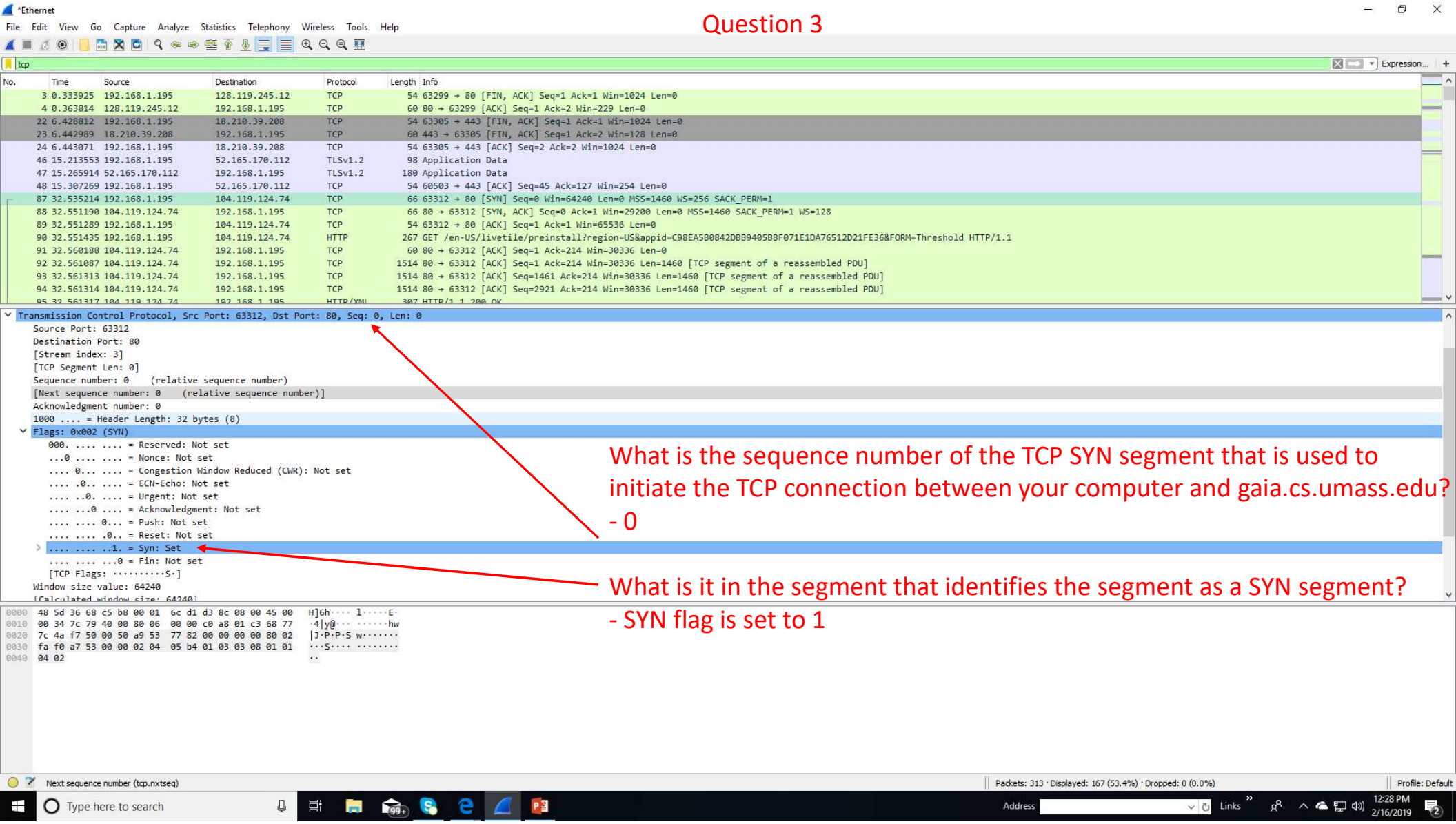
Question 2



What is the TCP port number used by gaia.cs.umass.edu to communicate with your computer?

- 80

Question 3



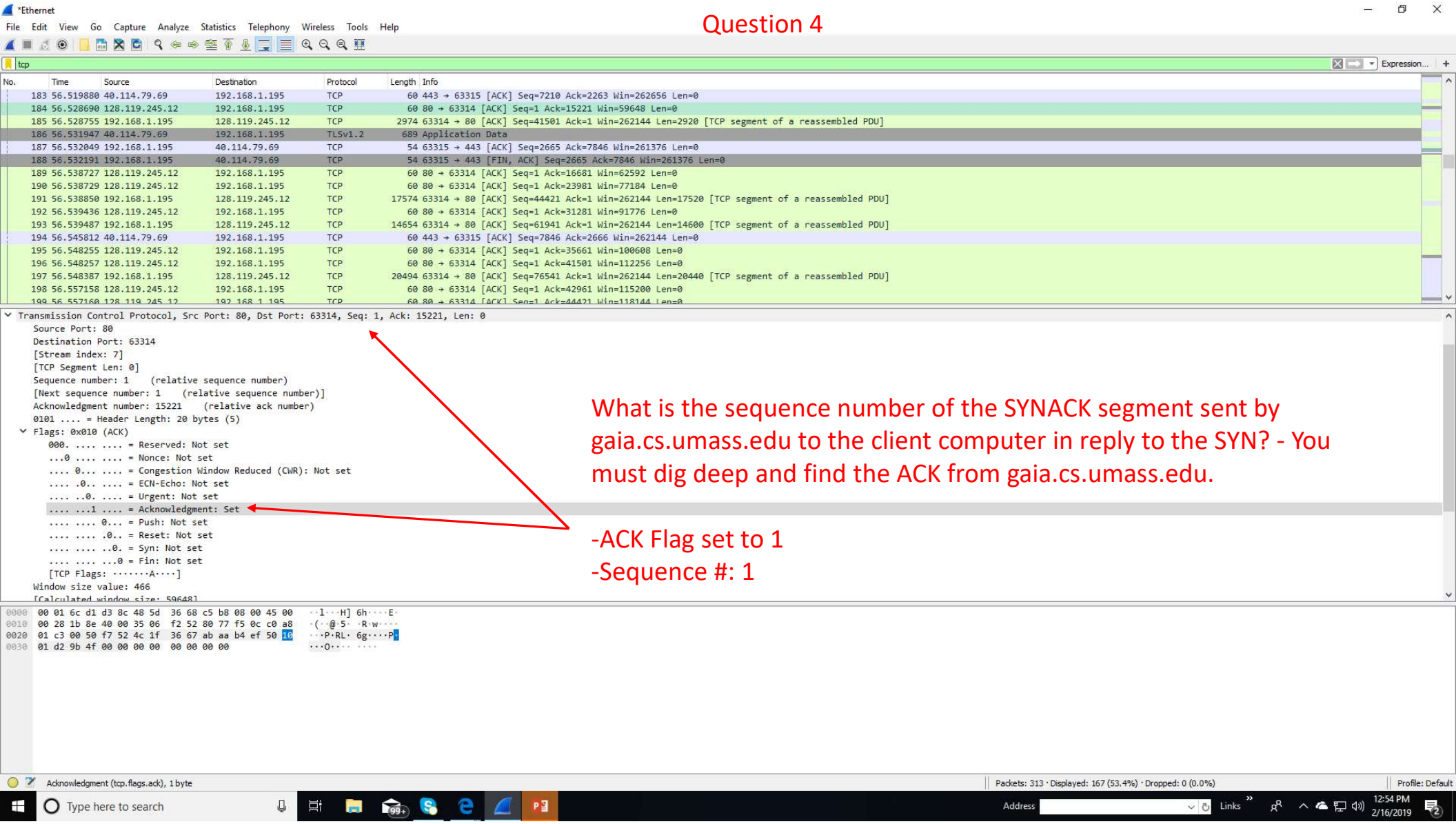
What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between your computer and gaia.cs.umass.edu?

- 0

What is it in the segment that identifies the segment as a SYN segment?

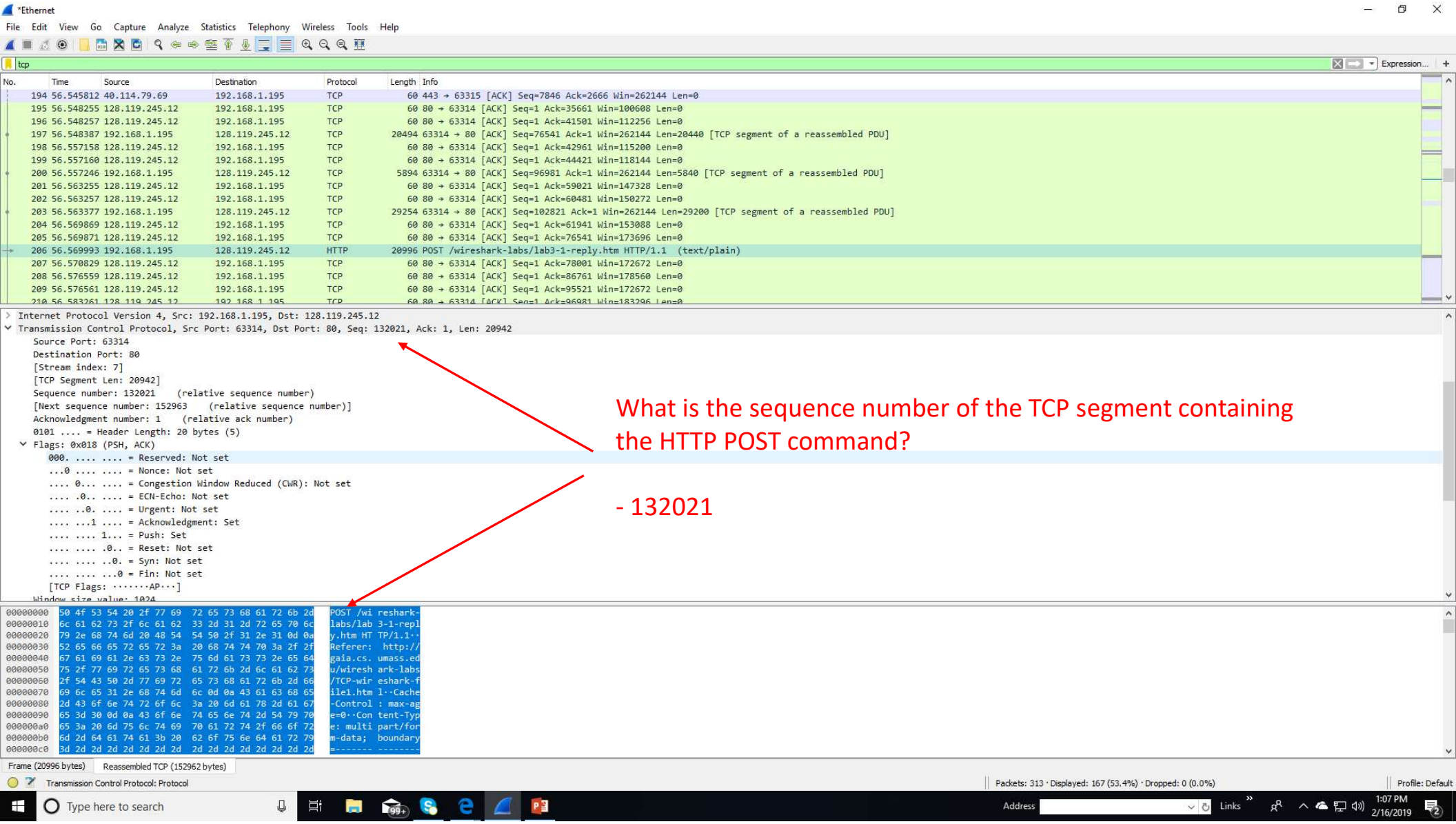
- SYN flag is set to 1

Question 4



What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? - You must dig deep and find the ACK from gaia.cs.umass.edu.

-ACK Flag set to 1
-Sequence #: 1


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
Expression...
No. Time Source Destination Protocol Length Info
194 56.545812 40.114.79.69 192.168.1.195 TCP 60 443 → 63315 [ACK] Seq=7846 Ack=2666 Win=262144 Len=0
195 56.548255 128.119.245.12 192.168.1.195 TCP 60 80 → 63314 [ACK] Seq=1 Ack=35661 Win=100608 Len=0
196 56.548257 128.119.245.12 192.168.1.195 TCP 60 80 → 63314 [ACK] Seq=1 Ack=41501 Win=112256 Len=0
197 56.548387 192.168.1.195 128.119.245.12 TCP 20494 63314 → 80 [ACK] Seq=76541 Ack=1 Win=262144 Len=20440 [TCP segment of a reassembled PDU]
198 56.557158 128.119.245.12 192.168.1.195 TCP 60 80 → 63314 [ACK] Seq=1 Ack=42961 Win=115200 Len=0
199 56.557160 128.119.245.12 192.168.1.195 TCP 60 80 → 63314 [ACK] Seq=1 Ack=44421 Win=118144 Len=0
200 56.557246 192.168.1.195 128.119.245.12 TCP 5894 63314 → 80 [ACK] Seq=96981 Ack=1 Win=262144 Len=5840 [TCP segment of a reassembled PDU]
201 56.563255 128.119.245.12 192.168.1.195 TCP 60 80 → 63314 [ACK] Seq=1 Ack=59021 Win=147328 Len=0
202 56.563257 128.119.245.12 192.168.1.195 TCP 60 80 → 63314 [ACK] Seq=1 Ack=60481 Win=150272 Len=0
203 56.563377 192.168.1.195 128.119.245.12 TCP 29254 63314 → 80 [ACK] Seq=102821 Ack=1 Win=262144 Len=29200 [TCP segment of a reassembled PDU]
204 56.569869 128.119.245.12 192.168.1.195 TCP 60 80 → 63314 [ACK] Seq=1 Ack=61941 Win=153088 Len=0
205 56.569871 128.119.245.12 192.168.1.195 TCP 60 80 → 63314 [ACK] Seq=1 Ack=76541 Win=173696 Len=0
206 56.569993 192.168.1.195 128.119.245.12 HTTP 20996 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
207 56.570829 128.119.245.12 192.168.1.195 TCP 60 80 → 63314 [ACK] Seq=1 Ack=78001 Win=172672 Len=0
208 56.576559 128.119.245.12 192.168.1.195 TCP 60 80 → 63314 [ACK] Seq=1 Ack=86761 Win=178560 Len=0
209 56.576561 128.119.245.12 192.168.1.195 TCP 60 80 → 63314 [ACK] Seq=1 Ack=95521 Win=172672 Len=0
Internet Protocol Version 4, Src: 192.168.1.195, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 63314, Dst Port: 80, Seq: 132021, Ack: 1, Len: 20942
Source Port: 63314
Destination Port: 80
[Stream index: 7]
[TCP Segment Len: 20942]
Sequence number: 132021 (relative sequence number)
[Next sequence number: 152963 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, 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
.... 1... = Push: Set
.... .0.. = Reset: Not set
....0. = Syn: Not set
....0 = Fin: Not set
[TCP Flags: ·····AP···]
Window size value: 1024
00000000 50 4f 53 54 20 2f 77 69 72 65 73 68 61 72 6b 2d POST /wi reshark-
00000010 6c 61 62 73 2f 6c 61 62 33 2d 31 2d 72 65 70 6c labs/lab 3-1-repl
00000020 79 2e 68 74 6d 20 48 54 54 50 2f 31 2e 31 0d 0a y.htm HT TP/1.1··
00000030 52 65 66 65 72 65 72 3a 20 68 74 74 70 3a 2f 2f Referer: http://
00000040 67 61 69 61 2e 63 73 2e 75 6d 61 73 73 2e 65 64 gaia.cs. umass.ed
00000050 75 2f 77 69 72 65 73 68 61 72 6b 2d 6c 61 62 73 u/wiresh ark-labs
00000060 2f 54 43 50 2d 77 69 72 65 73 68 61 72 6b 2d 66 /TCP-wir eshark-f
00000070 69 6c 65 31 2e 68 74 6d 6c 0d 0a 43 61 63 68 65 ile1.htm l··Cache
00000080 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 -Control : max-ag
00000090 65 3d 30 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 e=0··Con tent-Typ
000000a0 65 3a 20 6d 75 6c 74 69 70 61 72 74 2f 66 6f 72 e: multi part/for
000000b0 6d 2d 64 61 74 61 3b 20 62 6f 75 6e 64 61 72 79 m-data; boundary
000000c0 3d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d =------- --------
What is the sequence number of the TCP segment containing the HTTP POST command?
- 132021
Frame (20996 bytes)
Reassembled TCP (152962 bytes)
Transmission Control Protocol: Protocol
Packets: 313 · Displayed: 167 (53.4%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
Address
Links
1:07 PM
2/16/2019

C:\Users\dgogo\AppData\Local\Temp\wireshark_0AEACC56-2C54-40D3-A2B1-E5A421CEA2E2_20190216112206_a16340.pcapng 313 total packets, 8 shown

```
No.     Time           Source                Destination           Protocol Length Info
    221 56.599061      128.119.245.12        192.168.1.195         HTTP     831    HTTP/1.1 200 OK  (text/html)
Frame 221: 831 bytes on wire (6648 bits), 831 bytes captured (6648 bits) on interface 0
Ethernet II, Src: Verizon_68:c5:b8 (48:5d:36:68:c5:b8), Dst: Foxconn_d1:d3:8c (00:01:6c:d1:d3:8c)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.195
Transmission Control Protocol, Src Port: 80, Dst Port: 63314, Seq: 1, Ack: 152963, Len: 777
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Sat, 16 Feb 2019 16:23:00 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Sat, 23 Oct 2010 11:38:58 GMT\r\n
    ETag: "1a2-4934734677880"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 418\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.029068000 seconds]
    [Request in frame: 206]
    File Data: 418 bytes
Line-based text data: text/html (11 lines)
```