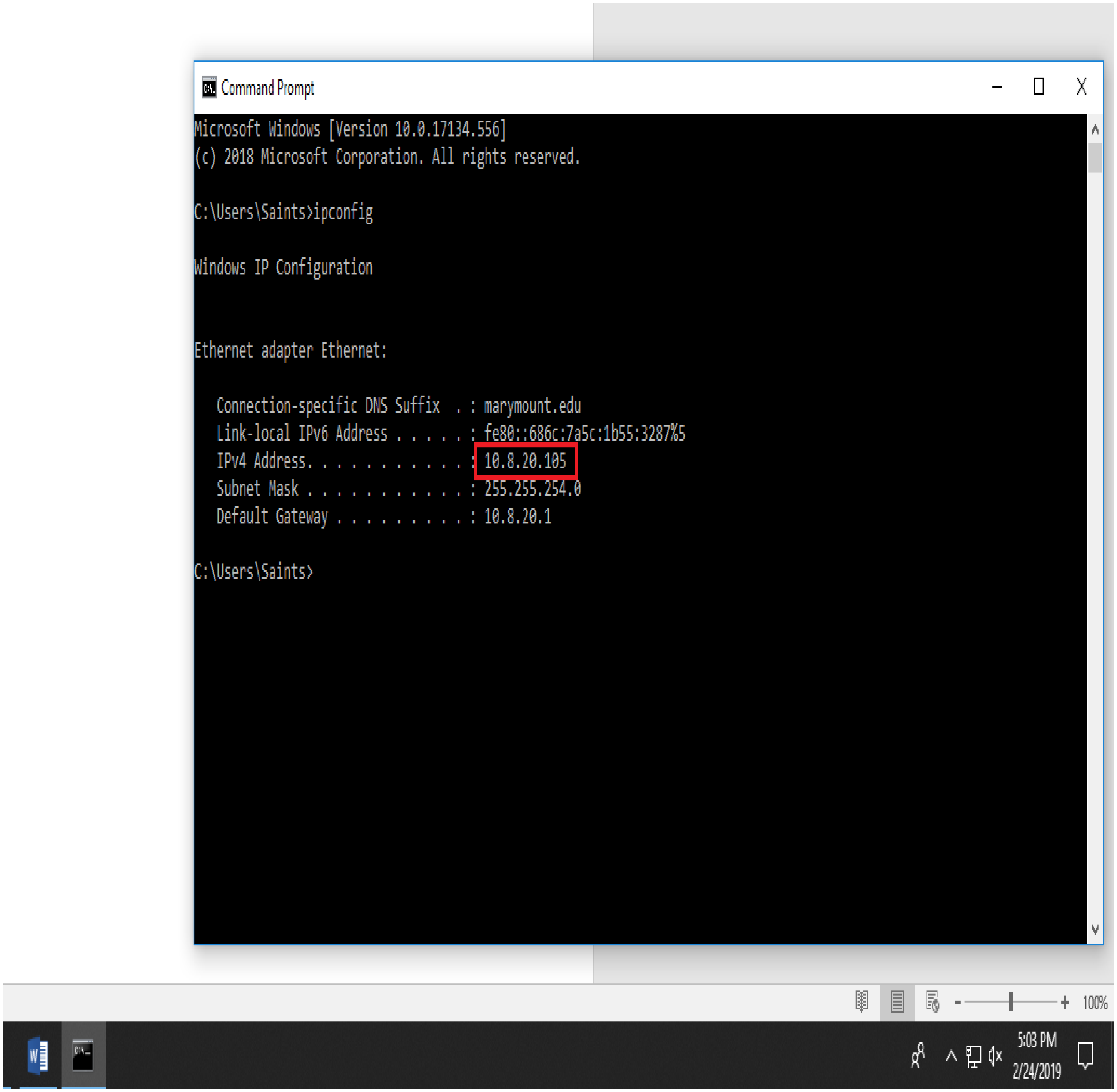
Lab3

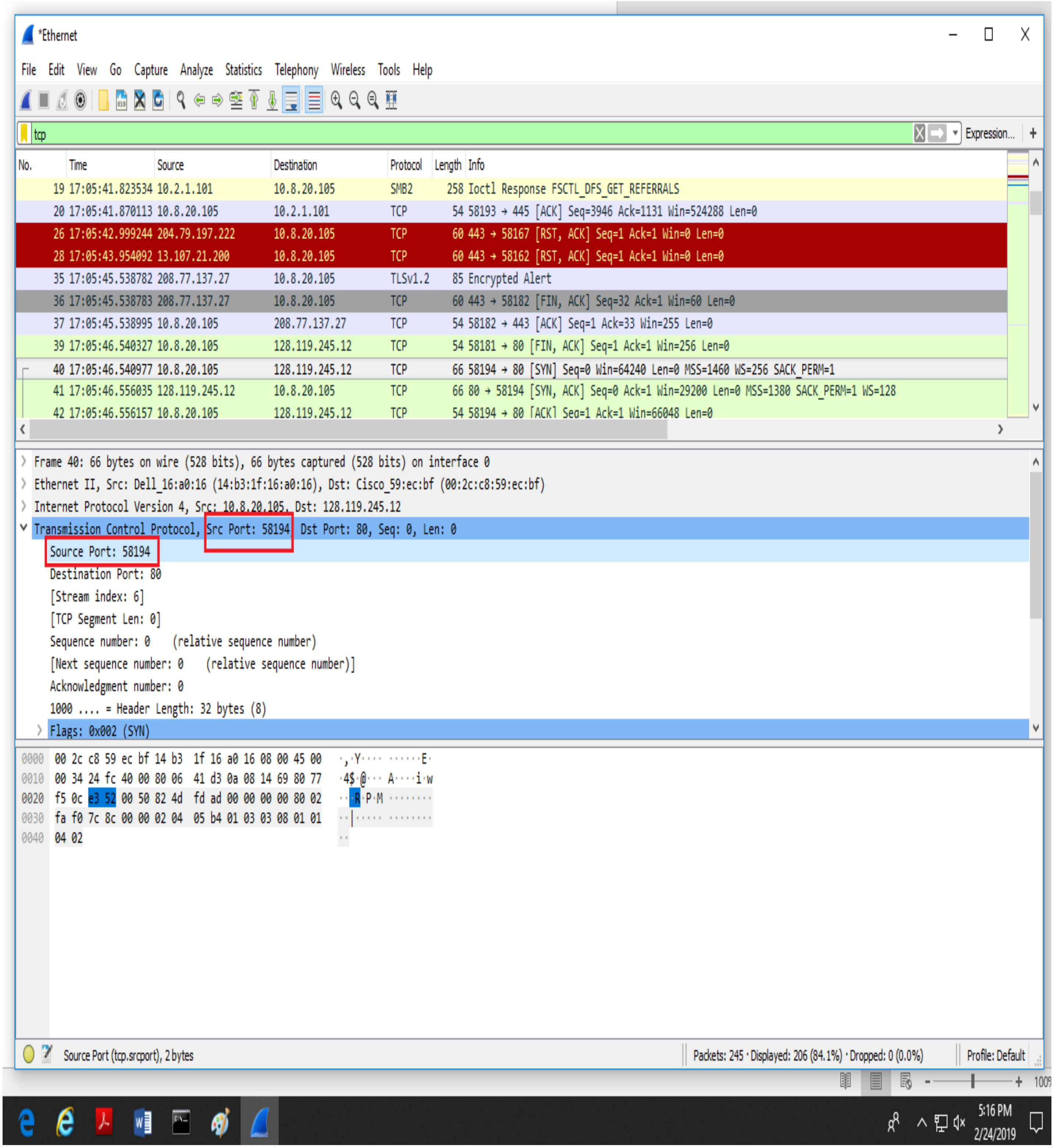
NAME: Mohammad Alhomidan ID:2510431



```
Microsoft Windows [Version 10.0.17134.556]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Saints>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : marymount.edu
   Link-local IPv6 Address . . . . . : fe80::686c:7a5c:1b55:3287%5
   IPv4 Address. . . . . . . . . . . : 10.8.20.105
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : 10.8.20.1

C:\Users\Saints>
```

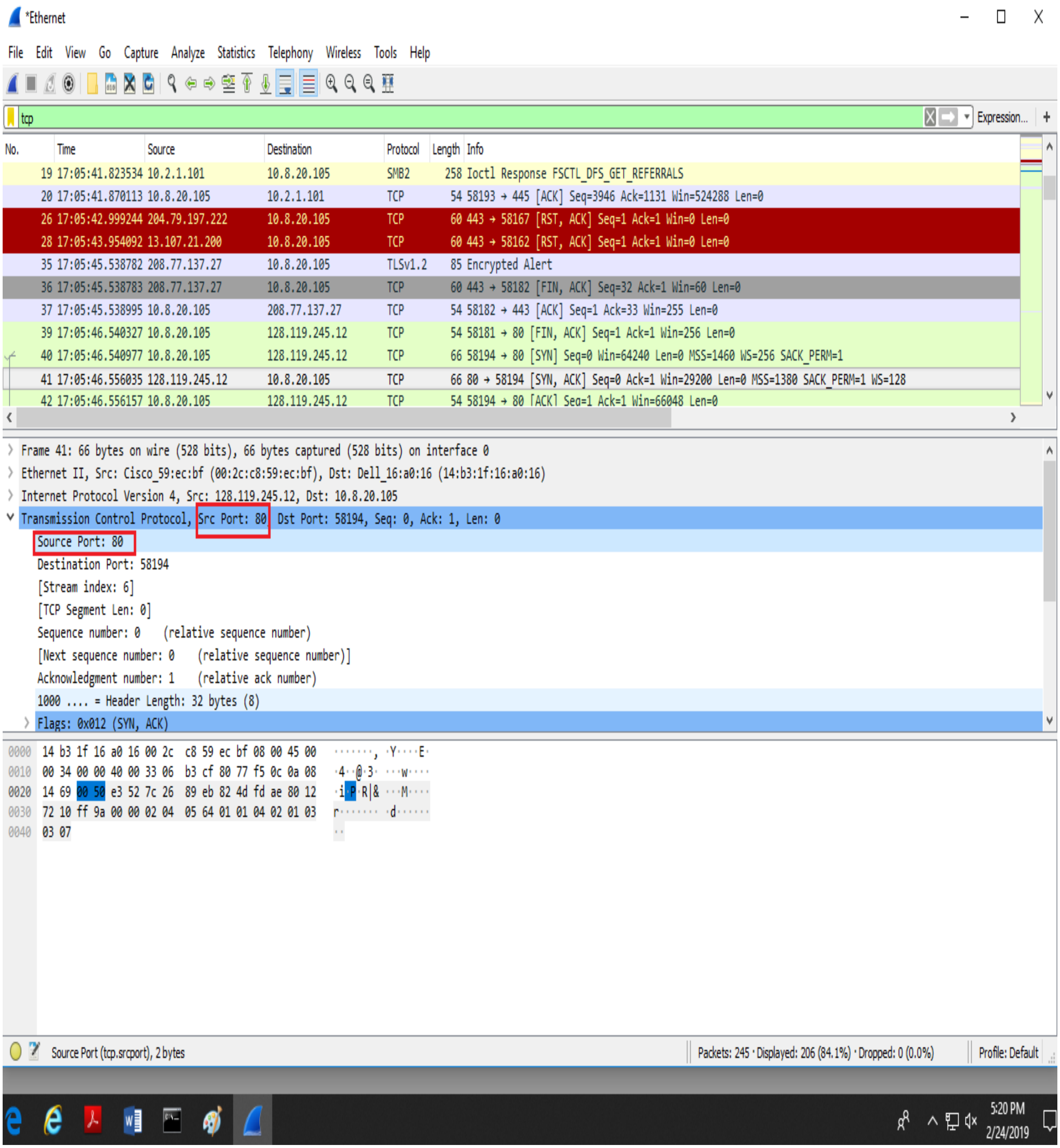
1. What is the TCP port number used by your computer to communicate with gaia.cs.umass.edu?

58194


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
Profile: Default
5:16 PM
2/24/2019

```
tcp

No.   Time            Source          Destination     Protocol Length Info
   19 17:05:41.823534 10.2.1.101      10.8.20.105     SMB2     258 Ioctl Response FSCTL_DFS_GET_REFERRALS
   20 17:05:41.870113 10.8.20.105     10.2.1.101      TCP       54 58193 → 445 [ACK] Seq=3946 Ack=1131 Win=524288 Len=0
   26 17:05:42.999244 204.79.197.222  10.8.20.105     TCP       60 443 → 58167 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   28 17:05:43.954092 13.107.21.200   10.8.20.105     TCP       60 443 → 58162 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   35 17:05:45.538782 208.77.137.27   10.8.20.105     TLSv1.2   85 Encrypted Alert
   36 17:05:45.538783 208.77.137.27   10.8.20.105     TCP       60 443 → 58182 [FIN, ACK] Seq=32 Ack=1 Win=60 Len=0
   37 17:05:45.538995 10.8.20.105     208.77.137.27   TCP       54 58182 → 443 [ACK] Seq=1 Ack=33 Win=255 Len=0
   39 17:05:46.540327 10.8.20.105     128.119.245.12  TCP       54 58181 → 80 [FIN, ACK] Seq=1 Ack=1 Win=256 Len=0
   40 17:05:46.540977 10.8.20.105     128.119.245.12  TCP       66 58194 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   41 17:05:46.556035 128.119.245.12  10.8.20.105     TCP       66 80 → 58194 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1380 SACK_PERM=1 WS=128
   42 17:05:46.556157 10.8.20.105     128.119.245.12  TCP       54 58194 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0

> Frame 40: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Dell_16:a0:16 (14:b3:1f:16:a0:16), Dst: Cisco_59:ec:bf (00:2c:c8:59:ec:bf)
> Internet Protocol Version 4, Src: 10.8.20.105, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 58194, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 58194
    Destination Port: 80
    [Stream index: 6]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)

0000  00 2c c8 59 ec bf 14 b3  1f 16 a0 16 08 00 45 00   ·,·Y···· ······E·
0010  00 34 24 fc 40 00 80 06  41 d3 0a 08 14 69 80 77   ·4$·@··· A····i·w
0020  f5 0c e3 52 00 50 82 4d  fd ad 00 00 00 00 80 02   ···R·P·M ········
0030  fa f0 7c 8c 00 00 02 04  05 b4 01 03 03 08 01 01   ··|····· ········
0040  04 02                                              ··

Source Port (tcp.srcport), 2 bytes    Packets: 245 · Displayed: 206 (84.1%) · Dropped: 0 (0.0%)
```

2. What is the TCP port number used by gaia.cs.umass.edu to communicate with your computer?
80



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

tcp

```
No.  Time             Source          Destination     Protocol Length Info
  19 17:05:41.823534 10.2.1.101      10.8.20.105     SMB2     258 Ioctl Response FSCTL_DFS_GET_REFERRALS
  20 17:05:41.870113 10.8.20.105     10.2.1.101      TCP       54 58193 → 445 [ACK] Seq=3946 Ack=1131 Win=524288 Len=0
  26 17:05:42.999244 204.79.197.222  10.8.20.105     TCP       60 443 → 58167 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  28 17:05:43.954092 13.107.21.200   10.8.20.105     TCP       60 443 → 58162 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  35 17:05:45.538782 208.77.137.27   10.8.20.105     TLSv1.2   85 Encrypted Alert
  36 17:05:45.538783 208.77.137.27   10.8.20.105     TCP       60 443 → 58182 [FIN, ACK] Seq=32 Ack=1 Win=60 Len=0
  37 17:05:45.538995 10.8.20.105     208.77.137.27   TCP       54 58182 → 443 [ACK] Seq=1 Ack=33 Win=255 Len=0
  39 17:05:46.540327 10.8.20.105     128.119.245.12  TCP       54 58181 → 80 [FIN, ACK] Seq=1 Ack=1 Win=256 Len=0
  40 17:05:46.540977 10.8.20.105     128.119.245.12  TCP       66 58194 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  41 17:05:46.556035 128.119.245.12  10.8.20.105     TCP       66 80 → 58194 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1380 SACK_PERM=1 WS=128
  42 17:05:46.556157 10.8.20.105     128.119.245.12  TCP       54 58194 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
```

```
> Frame 41: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Cisco_59:ec:bf (00:2c:c8:59:ec:bf), Dst: Dell_16:a0:16 (14:b3:1f:16:a0:16)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.8.20.105
v Transmission Control Protocol, Src Port: 80, Dst Port: 58194, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 58194
    [Stream index: 6]
    [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)
```

```
0000  14 b3 1f 16 a0 16 00 2c  c8 59 ec bf 08 00 45 00   ·······, ·Y····E·
0010  00 34 00 00 40 00 33 06  b3 cf 80 77 f5 0c 0a 08   ·4··@·3· ···w····
0020  14 69 00 50 e3 52 7c 26  89 eb 82 4d fd ae 80 12   ·i·P·R|& ···M····
0030  72 10 ff 9a 00 00 02 04  05 64 01 01 04 02 01 03   r······· ·d······
0040  03 07                                              ··
```

Source Port (tcp.srcport), 2 bytes

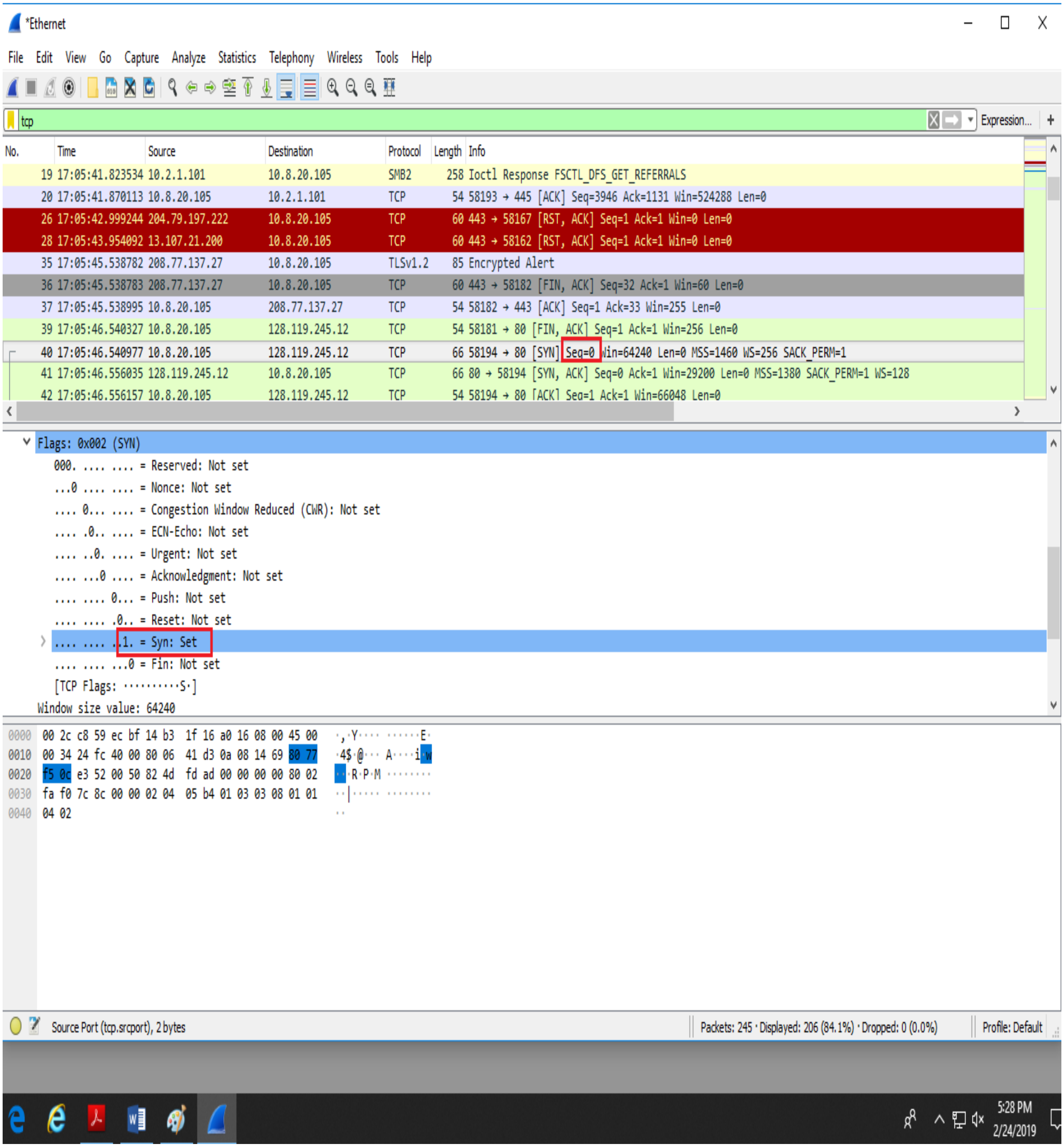
Packets: 245 · Displayed: 206 (84.1%) · Dropped: 0 (0.0%)

Profile: Default

5:20 PM
2/24/2019

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

Sequence number: 0 segment :1



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
Expression...
+

```
No.  Time            Source          Destination     Protocol Length Info
  19 17:05:41.823534 10.2.1.101      10.8.20.105     SMB2     258 Ioctl Response FSCTL_DFS_GET_REFERRALS
  20 17:05:41.870113 10.8.20.105     10.2.1.101      TCP       54 58193 → 445 [ACK] Seq=3946 Ack=1131 Win=524288 Len=0
  26 17:05:42.999244 204.79.197.222  10.8.20.105     TCP       60 443 → 58167 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  28 17:05:43.954092 13.107.21.200   10.8.20.105     TCP       60 443 → 58162 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  35 17:05:45.538782 208.77.137.27   10.8.20.105     TLSv1.2   85 Encrypted Alert
  36 17:05:45.538783 208.77.137.27   10.8.20.105     TCP       60 443 → 58182 [FIN, ACK] Seq=32 Ack=1 Win=60 Len=0
  37 17:05:45.538995 10.8.20.105     208.77.137.27   TCP       54 58182 → 443 [ACK] Seq=1 Ack=33 Win=255 Len=0
  39 17:05:46.540327 10.8.20.105     128.119.245.12  TCP       54 58181 → 80 [FIN, ACK] Seq=1 Ack=1 Win=256 Len=0
  40 17:05:46.540977 10.8.20.105     128.119.245.12  TCP       66 58194 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  41 17:05:46.556035 128.119.245.12  10.8.20.105     TCP       66 80 → 58194 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1380 SACK_PERM=1 WS=128
  42 17:05:46.556157 10.8.20.105     128.119.245.12  TCP       54 58194 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
```

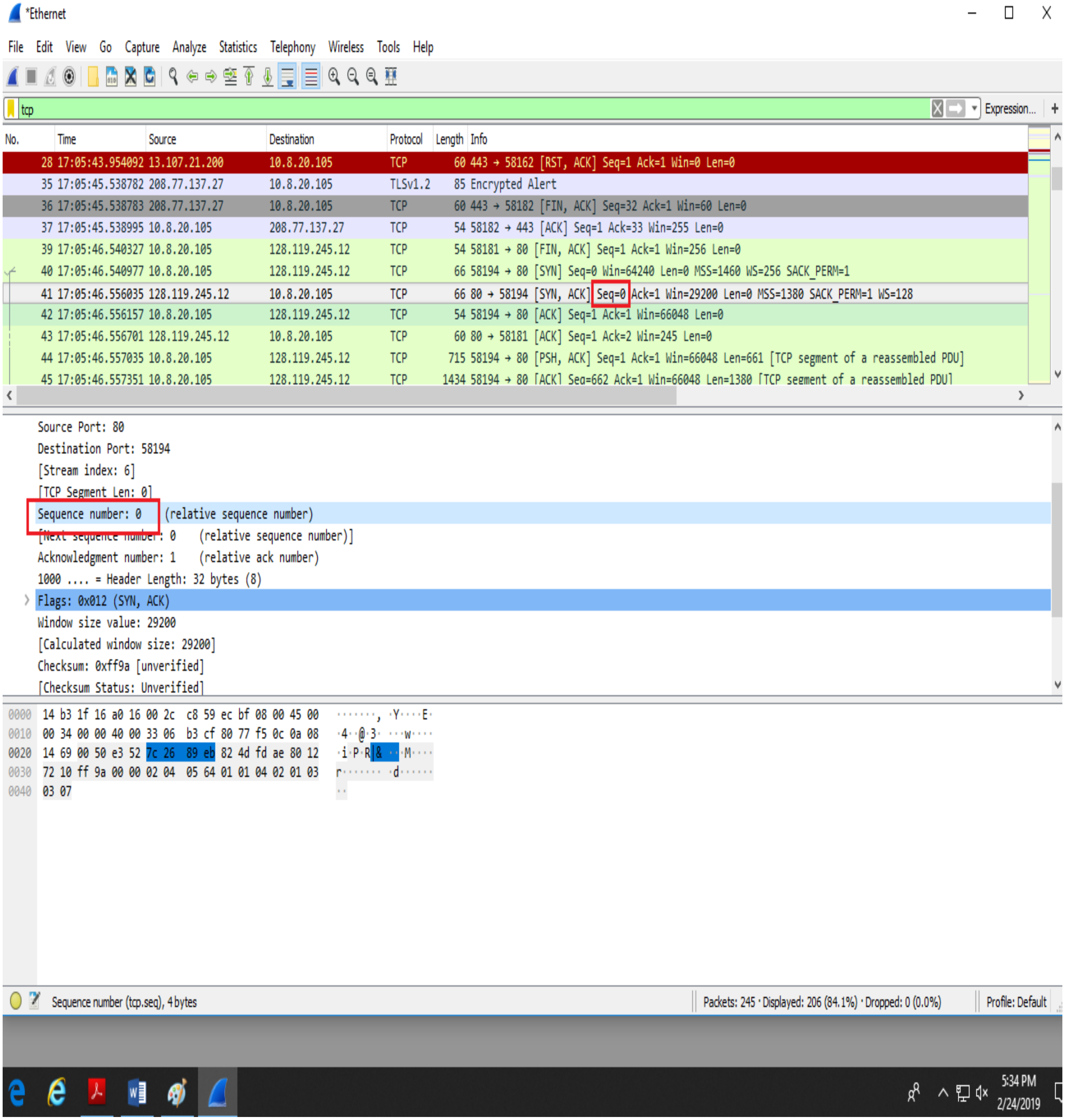
```
v Flags: 0x002 (SYN)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...0 .... = Acknowledgment: Not set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
  > .... .... ..1. = Syn: Set
    .... .... ...0 = Fin: Not set
    [TCP Flags: ··········S·]
  Window size value: 64240
```

```
0000  00 2c c8 59 ec bf 14 b3  1f 16 a0 16 08 00 45 00   ·,·Y···· ······E·
0010  00 34 24 fc 40 00 80 06  41 d3 0a 08 14 69 80 77   ·4$·@··· A····i·w
0020  f5 0c e3 52 00 50 82 4d  fd ad 00 00 00 00 80 02   ···R·P·M ········
0030  fa f0 7c 8c 00 00 02 04  05 b4 01 03 03 08 01 01   ··|····· ········
0040  04 02                                              ··
```

Source Port (tcp.srcport), 2 bytes | Packets: 245 · Displayed: 206 (84.1%) · Dropped: 0 (0.0%) | Profile: Default

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.

Sequence number is 0


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

tcp

```
No.  Time            Source          Destination     Protocol Length Info
  28 17:05:43.954092 13.107.21.200   10.8.20.105     TCP        60 443 → 58162 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  35 17:05:45.538782 208.77.137.27   10.8.20.105     TLSv1.2    85 Encrypted Alert
  36 17:05:45.538783 208.77.137.27   10.8.20.105     TCP        60 443 → 58182 [FIN, ACK] Seq=32 Ack=1 Win=60 Len=0
  37 17:05:45.538995 10.8.20.105     208.77.137.27   TCP        54 58182 → 443 [ACK] Seq=1 Ack=33 Win=255 Len=0
  39 17:05:46.540327 10.8.20.105     128.119.245.12  TCP        54 58181 → 80 [FIN, ACK] Seq=1 Ack=1 Win=256 Len=0
  40 17:05:46.540977 10.8.20.105     128.119.245.12  TCP        66 58194 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  41 17:05:46.556035 128.119.245.12  10.8.20.105     TCP        66 80 → 58194 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1380 SACK_PERM=1 WS=128
  42 17:05:46.556157 10.8.20.105     128.119.245.12  TCP        54 58194 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
  43 17:05:46.556701 128.119.245.12  10.8.20.105     TCP        60 80 → 58181 [ACK] Seq=1 Ack=2 Win=245 Len=0
  44 17:05:46.557035 10.8.20.105     128.119.245.12  TCP       715 58194 → 80 [PSH, ACK] Seq=1 Ack=1 Win=66048 Len=661 [TCP segment of a reassembled PDU]
  45 17:05:46.557351 10.8.20.105     128.119.245.12  TCP      1434 58194 → 80 [ACK] Seq=662 Ack=1 Win=66048 Len=1380 [TCP segment of a reassembled PDU]
```

```
    Source Port: 80
    Destination Port: 58194
    [Stream index: 6]
    [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)
    Window size value: 29200
    [Calculated window size: 29200]
    Checksum: 0xff9a [unverified]
    [Checksum Status: Unverified]
```

```
0000  14 b3 1f 16 a0 16 00 2c  c8 59 ec bf 08 00 45 00   ·······, ·Y····E·
0010  00 34 00 00 40 00 33 06  b3 cf 80 77 f5 0c 0a 08   ·4··@·3· ···w····
0020  14 69 00 50 e3 52 7c 26  89 eb 82 4d fd ae 80 12   ·i·P·R|& ···M····
0030  72 10 ff 9a 00 00 02 04  05 64 01 01 04 02 01 03   r······· ·d······
0040  03 07                                              ··
```

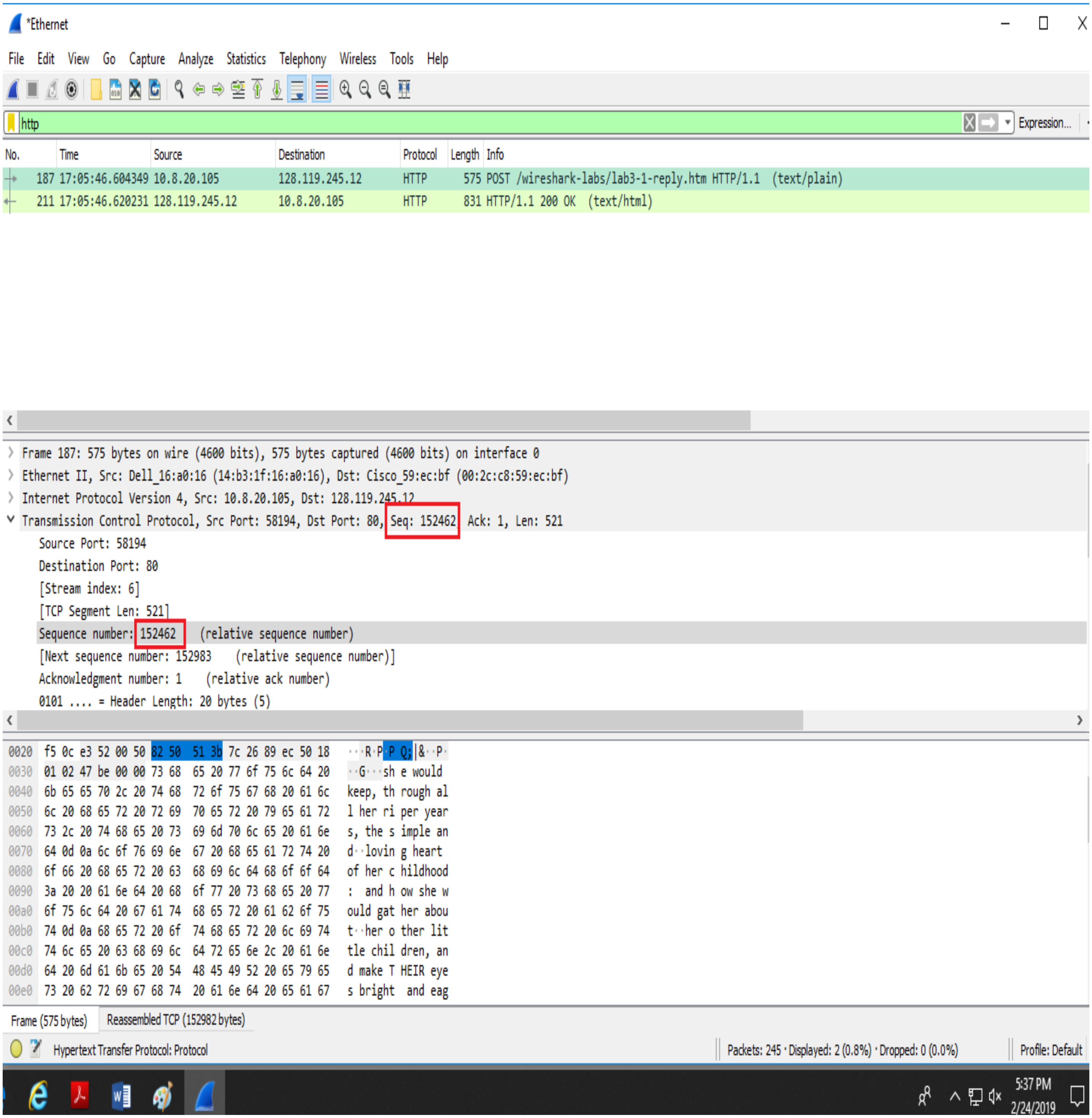
Sequence number (tcp.seq), 4 bytes

Packets: 245 · Displayed: 206 (84.1%) · Dropped: 0 (0.0%)

Profile: Default

5. What is the sequence number of the TCP segment containing the HTTP POST command? Note: that to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

Sequence number: 152462



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...

```
No.   Time             Source          Destination     Protocol Length Info
  187 17:05:46.604349 10.8.20.105     128.119.245.12  HTTP       575 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1  (text/plain)
  211 17:05:46.620231 128.119.245.12  10.8.20.105     HTTP       831 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 187: 575 bytes on wire (4600 bits), 575 bytes captured (4600 bits) on interface 0
> Ethernet II, Src: Dell_16:a0:16 (14:b3:1f:16:a0:16), Dst: Cisco_59:ec:bf (00:2c:c8:59:ec:bf)
> Internet Protocol Version 4, Src: 10.8.20.105, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 58194, Dst Port: 80, Seq: 152462  Ack: 1, Len: 521
    Source Port: 58194
    Destination Port: 80
    [Stream index: 6]
    [TCP Segment Len: 521]
    Sequence number: 152462    (relative sequence number)
    [Next sequence number: 152983    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
```

```
0020  f5 0c e3 52 00 50 82 50  51 3b 7c 26 89 ec 50 18   ···R·P·P Q;|&··P·
0030  01 02 47 be 00 00 73 68  65 20 77 6f 75 6c 64 20   ··G···sh e would 
0040  6b 65 65 70 2c 20 74 68  72 6f 75 67 68 20 61 6c   keep, th rough al
0050  6c 20 68 65 72 20 72 69  70 65 72 20 79 65 61 72   l her ri per year
0060  73 2c 20 74 68 65 20 73  69 6d 70 6c 65 20 61 6e   s, the s imple an
0070  64 0d 0a 6c 6f 76 69 6e  67 20 68 65 61 72 74 20   d··lovin g heart 
0080  6f 66 20 68 65 72 20 63  68 69 6c 64 68 6f 6f 64   of her c hildhood
0090  3a 20 20 61 6e 64 20 68  6f 77 20 73 68 65 20 77   :  and h ow she w
00a0  6f 75 6c 64 20 67 61 74  68 65 72 20 61 62 6f 75   ould gat her abou
00b0  74 0d 0a 68 65 72 20 6f  74 68 65 72 20 6c 69 74   t··her o ther lit
00c0  74 6c 65 20 63 68 69 6c  64 72 65 6e 2c 20 61 6e   tle chil dren, an
00d0  64 20 6d 61 6b 65 20 54  48 45 49 52 20 65 79 65   d make T HEIR eye
00e0  73 20 62 72 69 67 68 74  20 61 6e 64 20 65 61 67   s bright  and eag
```

Frame (575 bytes)
Reassembled TCP (152982 bytes)
Hypertext Transfer Protocol: Protocol
Packets: 245 · Displayed: 2 (0.8%) · Dropped: 0 (0.0%)
Profile: Default
5:37 PM
2/24/2019

```
C :\U sers\S aints\A ppD ata\Local\Temp\w ireshark_23890EB4-B5B3-4545-A 889-D A 70B712816F
_20190224170541_a10952.pcapng 245 total packets, 2 show n

211 17:05:46.620231 128.119.245.12 10.8.20.105 HTTP 831 HTTP/1.1 200 OK (text/html)

Frame 211: 831 bytes on wire (6648 bits), 831 bytes captured (6648 bits) on interface 0

Ethernet II, Src: Cisco_59:ec:bf (00:2c:c8:59:ec:bf), Dst: Dell_16:a0:16 (14:b3:1f:16:a0:16)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.8.20.105

Transmission Control Protocol, Src Port: 80, Dst Port: 58194, Seq: 1, Ack: 152983, Len: 777

Source Port: 80

Destination Port: 58194

[Stream index: 6]

[TCP Segment Len: 777]

Sequence number: 1 (relative sequence number)

[Next sequence number: 778 (relative sequence number)]

Acknowledgment number: 152983 (relative ack number)

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

Flags: 0x018 (PSH, ACK)

Window size value: 1432

[Calculated window size: 183296]

[Window size scaling factor: 128]

Checksum: 0xb7ba [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

[SEQ/ACK analysis]

[Timestamps]

TCP payload (777 bytes)

Hypertext Transfer Protocol

Line-based text data: text/html (11 lines)
```