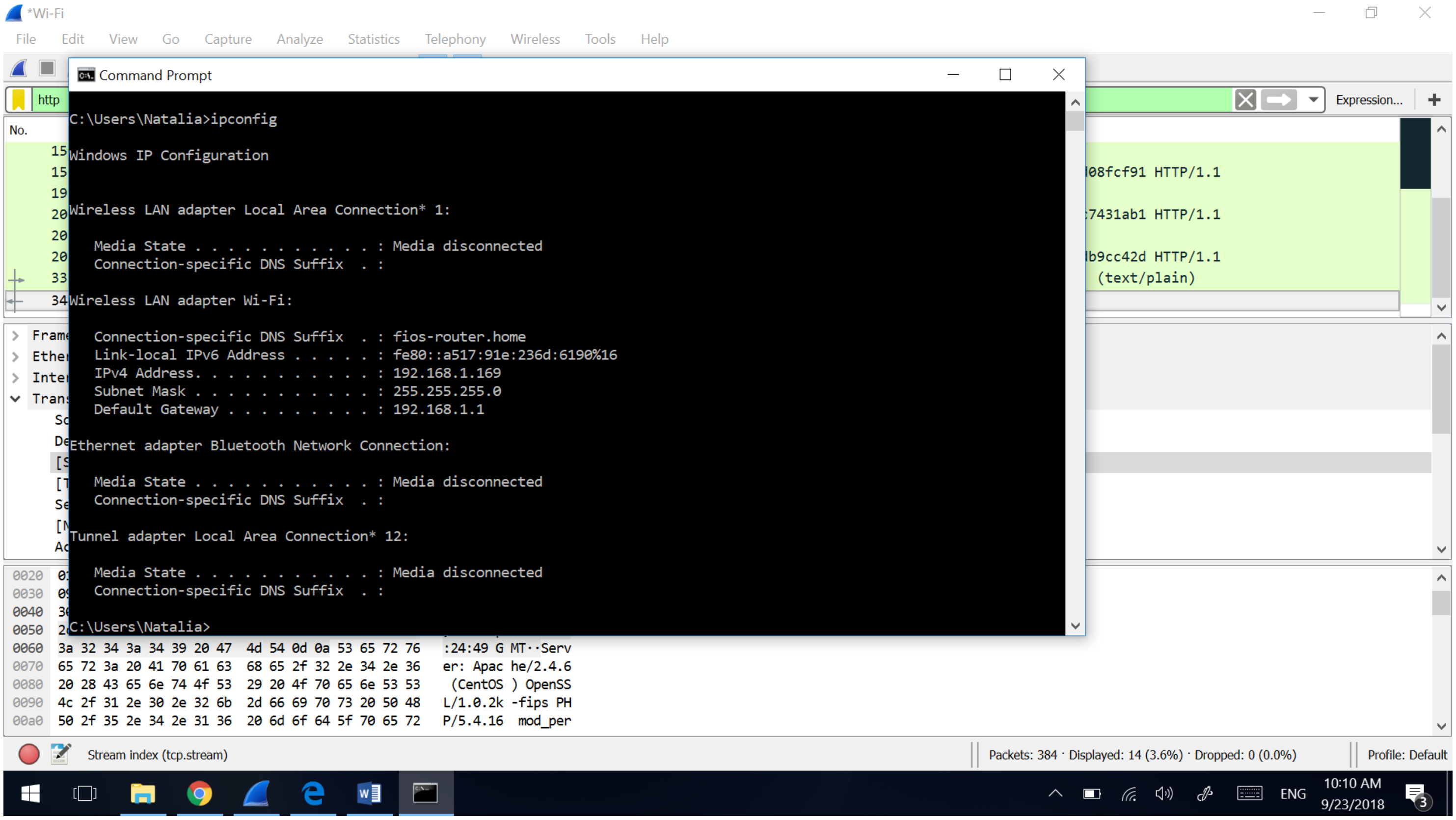

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
Command Prompt
Stream index (tcp.stream)
Packets: 384 · Displayed: 14 (3.6%) · Dropped: 0 (0.0%)
Profile: Default
ENG
10:10 AM
9/23/2018

```
C:\Users\Natalia>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : fios-router.home
   Link-local IPv6 Address . . . . . : fe80::a517:91e:236d:6190%16
   IPv4 Address. . . . . . . . . . . : 192.168.1.169
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

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

Tunnel adapter Local Area Connection* 12:

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

C:\Users\Natalia>
```

```
)08fcf91 HTTP/1.1
:7431ab1 HTTP/1.1
)b9cc42d HTTP/1.1
 (text/plain)
```

```
0060  3a 32 34 3a 34 39 20 47  4d 54 0d 0a 53 65 72 76   :24:49 G MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apac he/2.4.6
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentOS ) OpenSS
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73 20 50 48   L/1.0.2k -fips PH
00a0  50 2f 35 2e 34 2e 31 36  20 6d 6f 64 5f 70 65 72   P/5.4.16  mod_per
```

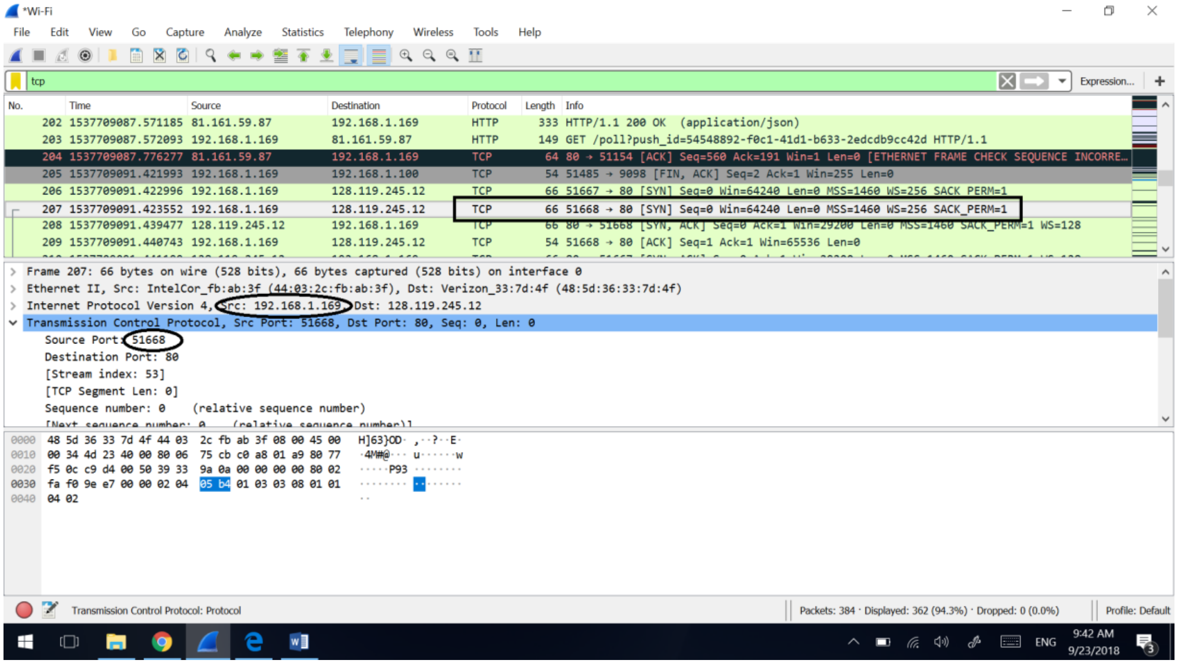
1. What is the TCP port number used by your computer to communicate with gaia.cs.umass.edu?

Answer:

TCP SYN

IP address: 192.168.1.169

TCP port number: 51668


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

```
No.  Time               Source          Destination     Protocol  Length  Info
202  1537709087.571185  81.161.59.87    192.168.1.169   HTTP      333  HTTP/1.1 200 OK  (application/json)
203  1537709087.572093  192.168.1.169   81.161.59.87    HTTP      149  GET /poll?push_id=54548892-f0c1-41d1-b633-2edcdb9cc42d HTTP/1.1
204  1537709087.776277  81.161.59.87    192.168.1.169   TCP        64  80 → 51154 [ACK] Seq=560 Ack=191 Win=1 Len=0 [ETHERNET FRAME CHECK SEQUENCE INCORRE…
205  1537709091.421993  192.168.1.169   192.168.1.100   TCP        54  51485 → 9098 [FIN, ACK] Seq=2 Ack=1 Win=255 Len=0
206  1537709091.422996  192.168.1.169   128.119.245.12  TCP        66  51667 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
207  1537709091.423552  192.168.1.169   128.119.245.12  TCP        66  51668 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
208  1537709091.439477  128.119.245.12  192.168.1.169   TCP        66  80 → 51668 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
209  1537709091.440743  192.168.1.169   128.119.245.12  TCP        54  51668 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
```

```
> Frame 207: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: IntelCor_fb:ab:3f (44:03:2c:fb:ab:3f), Dst: Verizon_33:7d:4f (48:5d:36:33:7d:4f)
> Internet Protocol Version 4, Src: 192.168.1.169, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 51668, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 51668
    Destination Port: 80
    [Stream index: 53]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
```

```
0000  48 5d 36 33 7d 4f 44 03  2c fb ab 3f 08 00 45 00   H]63}OD· ,··?··E·
0010  00 34 4d 23 40 00 80 06  75 cb c0 a8 01 a9 80 77   ·4M#@··· u······w
0020  f5 0c c9 d4 00 50 39 33  9a 0a 00 00 00 00 80 02   ·····P93 ········
0030  fa f0 9e e7 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··
```

Transmission Control Protocol: Protocol
Packets: 384 · Displayed: 362 (94.3%) · Dropped: 0 (0.0%)
Profile: Default
ENG
9:42 AM
9/23/2018

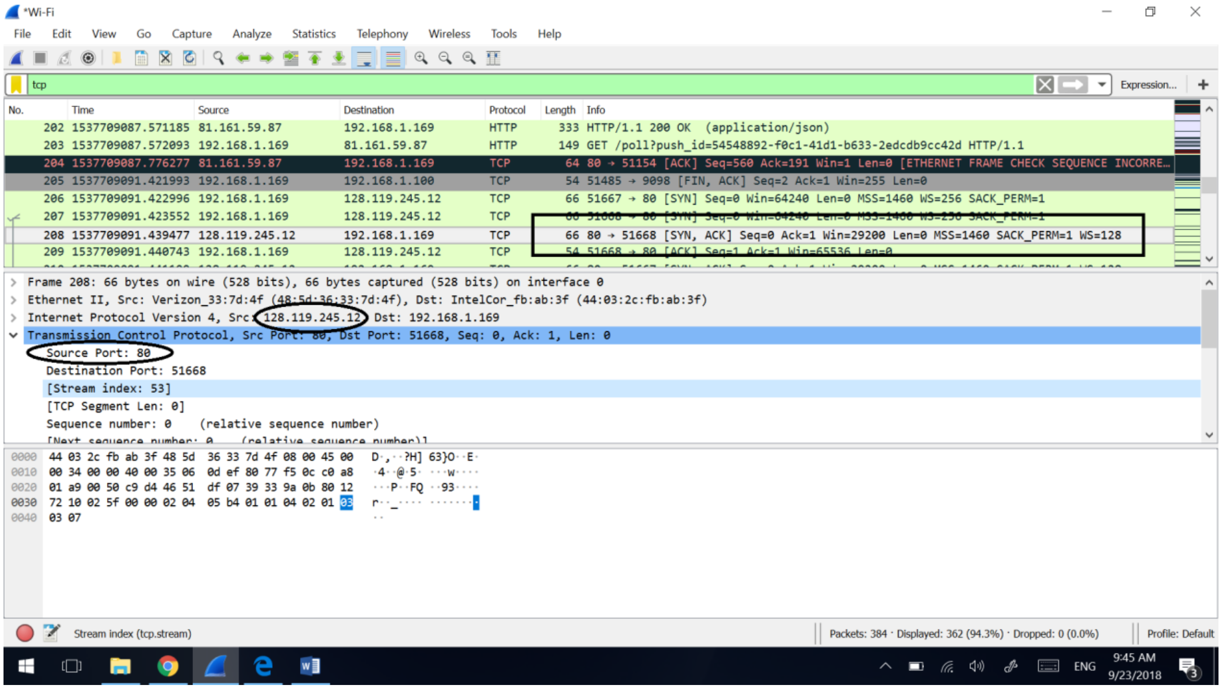
2. What is the TCP port number used by gaia.cs.umass.edu to communicate with your computer?

Answer:

TCP SYN, ACK

IP address: 128.119.245.12

TCP port number: 80


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
9:45 AM
9/23/2018
ENG

tcp

```
No.  Time               Source          Destination     Protocol Length Info
 202 1537709087.571185 81.161.59.87    192.168.1.169   HTTP     333 HTTP/1.1 200 OK  (application/json)
 203 1537709087.572093 192.168.1.169   81.161.59.87    HTTP     149 GET /poll?push_id=54548892-f0c1-41d1-b633-2edcdb9cc42d HTTP/1.1
 204 1537709087.776277 81.161.59.87    192.168.1.169   TCP       64 80 → 51154 [ACK] Seq=560 Ack=191 Win=1 Len=0 [ETHERNET FRAME CHECK SEQUENCE INCORRE…
 205 1537709091.421993 192.168.1.169   192.168.1.100   TCP       54 51485 → 9098 [FIN, ACK] Seq=2 Ack=1 Win=255 Len=0
 206 1537709091.422996 192.168.1.169   128.119.245.12  TCP       66 51667 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 207 1537709091.423552 192.168.1.169   128.119.245.12  TCP       66 51668 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 208 1537709091.439477 128.119.245.12  192.168.1.169   TCP       66 80 → 51668 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
 209 1537709091.440743 192.168.1.169   128.119.245.12  TCP       54 51668 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
```

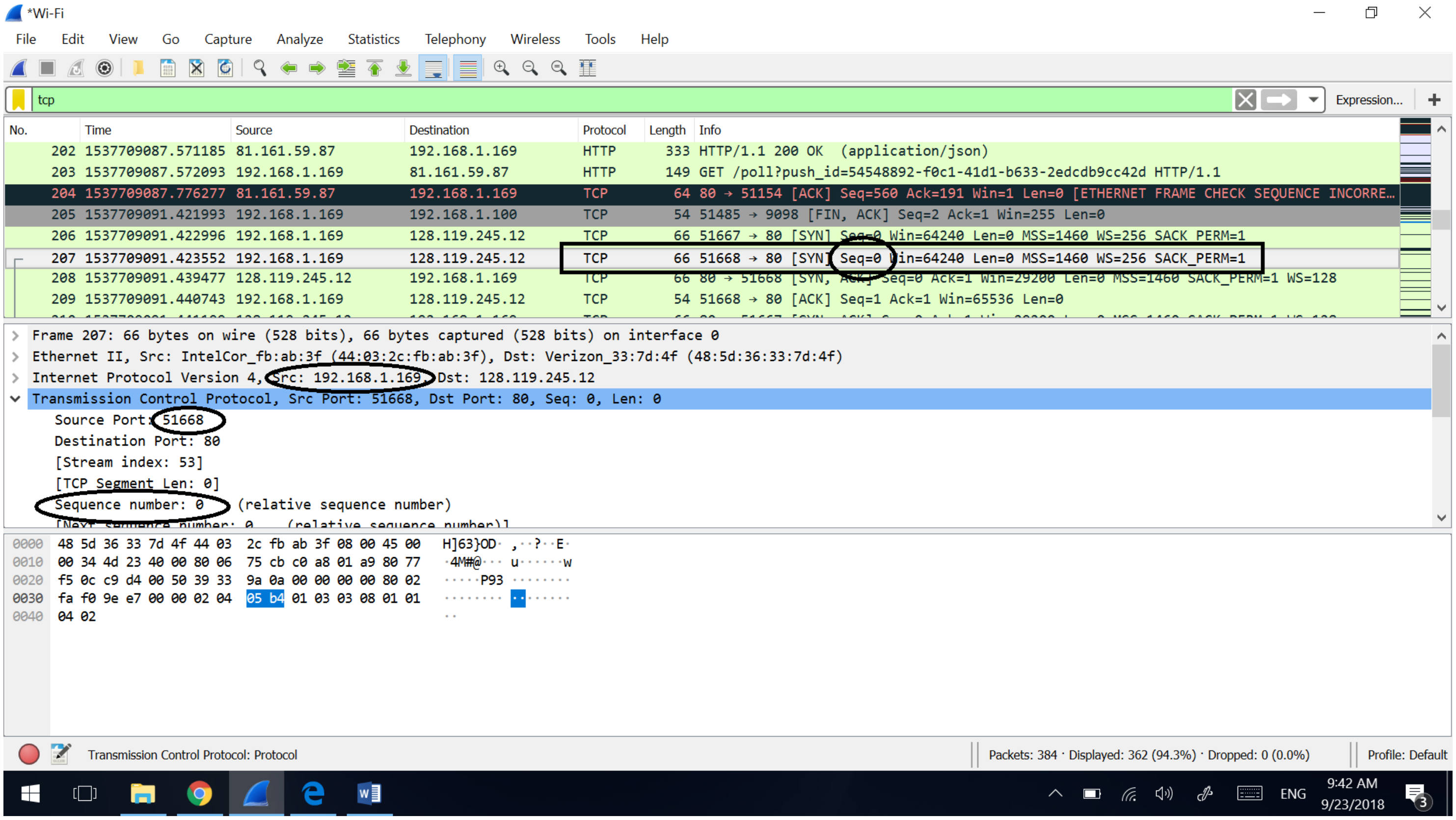
```
> Frame 208: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Verizon_33:7d:4f (48:5d:36:33:7d:4f), Dst: IntelCor_fb:ab:3f (44:03:2c:fb:ab:3f)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.169
v Transmission Control Protocol, Src Port: 80, Dst Port: 51668, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 51668
    [Stream index: 53]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
```

```
0000  44 03 2c fb ab 3f 48 5d  36 33 7d 4f 08 00 45 00   D·,··?H] 63}O··E·
0010  00 34 00 00 40 00 35 06  0d ef 80 77 f5 0c c0 a8   ·4··@·5· ···w····
0020  01 a9 00 50 c9 d4 46 51  df 07 39 33 9a 0b 80 12   ···P··FQ ··93····
0030  72 10 02 5f 00 00 02 04  05 b4 01 01 04 02 01 03   r··_···· ········
0040  03 07                                              ··
```

Stream index (tcp.stream)   Packets: 384 · Displayed: 362 (94.3%) · Dropped: 0 (0.0%)   Profile: Default

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?

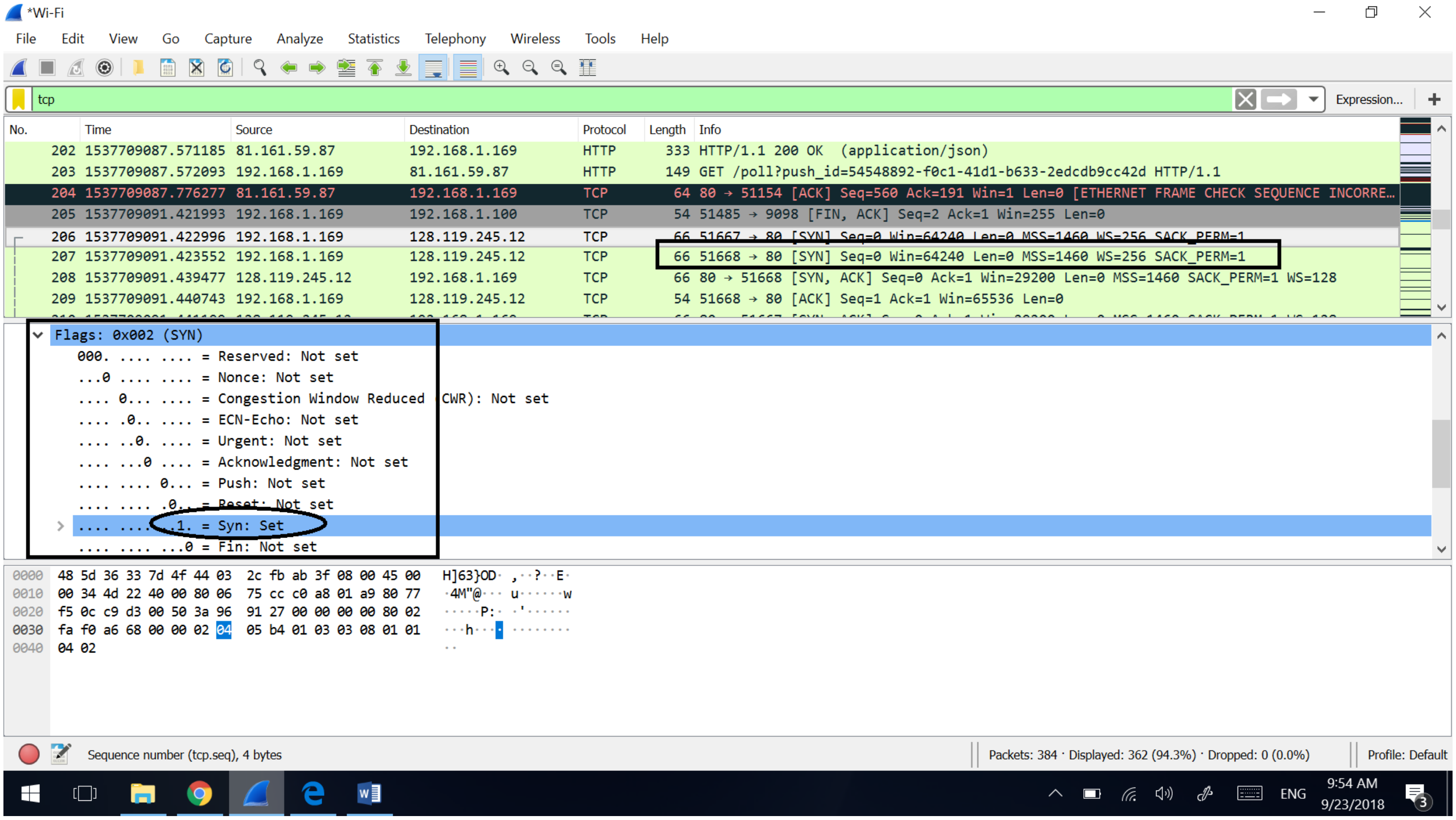
Answer: 0



```
tcp

No.  Time               Source          Destination     Protocol Length Info
 202 1537709087.571185 81.161.59.87    192.168.1.169   HTTP     333 HTTP/1.1 200 OK  (application/json)
 203 1537709087.572093 192.168.1.169   81.161.59.87    HTTP     149 GET /poll?push_id=54548892-f0c1-41d1-b633-2edcdb9cc42d HTTP/1.1
 204 1537709087.776277 81.161.59.87    192.168.1.169   TCP       64 80 → 51154 [ACK] Seq=560 Ack=191 Win=1 Len=0 [ETHERNET FRAME CHECK SEQUENCE INCORRE…
 205 1537709091.421993 192.168.1.169   192.168.1.100   TCP       54 51485 → 9098 [FIN, ACK] Seq=2 Ack=1 Win=255 Len=0
 206 1537709091.422996 192.168.1.169   128.119.245.12  TCP       66 51667 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 207 1537709091.423552 192.168.1.169   128.119.245.12  TCP       66 51668 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 208 1537709091.439477 128.119.245.12  192.168.1.169   TCP       66 80 → 51668 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
 209 1537709091.440743 192.168.1.169   128.119.245.12  TCP       54 51668 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0

> Frame 207: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: IntelCor_fb:ab:3f (44:03:2c:fb:ab:3f), Dst: Verizon_33:7d:4f (48:5d:36:33:7d:4f)
> Internet Protocol Version 4, Src: 192.168.1.169, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 51668, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 51668
    Destination Port: 80
    [Stream index: 53]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]

0000  48 5d 36 33 7d 4f 44 03  2c fb ab 3f 08 00 45 00   H]63}OD· ,··?··E·
0010  00 34 4d 23 40 00 80 06  75 cb c0 a8 01 a9 80 77   ·4M#@··· u······w
0020  f5 0c c9 d4 00 50 39 33  9a 0a 00 00 00 00 80 02   ·····P93 ········
0030  fa f0 9e e7 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··

Transmission Control Protocol: Protocol    Packets: 384 · Displayed: 362 (94.3%) · Dropped: 0 (0.0%)    Profile: Default
```

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

Answer: Flags indicates 1 for SYN, which results that the segment is SYN.


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

```
No.  Time               Source          Destination     Protocol  Length  Info
 202 1537709087.571185  81.161.59.87    192.168.1.169   HTTP       333 HTTP/1.1 200 OK  (application/json)
 203 1537709087.572093  192.168.1.169   81.161.59.87    HTTP       149 GET /poll?push_id=54548892-f0c1-41d1-b633-2edcdb9cc42d HTTP/1.1
 204 1537709087.776277  81.161.59.87    192.168.1.169   TCP         64 80 → 51154 [ACK] Seq=560 Ack=191 Win=1 Len=0 [ETHERNET FRAME CHECK SEQUENCE INCORRE…
 205 1537709091.421993  192.168.1.169   192.168.1.100   TCP         54 51485 → 9098 [FIN, ACK] Seq=2 Ack=1 Win=255 Len=0
 206 1537709091.422996  192.168.1.169   128.119.245.12  TCP         66 51667 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 207 1537709091.423552  192.168.1.169   128.119.245.12  TCP         66 51668 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 208 1537709091.439477  128.119.245.12  192.168.1.169   TCP         66 80 → 51668 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
 209 1537709091.440743  192.168.1.169   128.119.245.12  TCP         54 51668 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
```

```
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
```

```
0000  48 5d 36 33 7d 4f 44 03  2c fb ab 3f 08 00 45 00   H]63}OD· ,··?··E·
0010  00 34 4d 22 40 00 80 06  75 cc c0 a8 01 a9 80 77   ·4M"@··· u······w
0020  f5 0c c9 d3 00 50 3a 96  91 27 00 00 00 00 80 02   ·····P:· ·'······
0030  fa f0 a6 68 00 00 02 04  05 b4 01 03 03 08 01 01   ···h···· ········
0040  04 02                                              ··
```

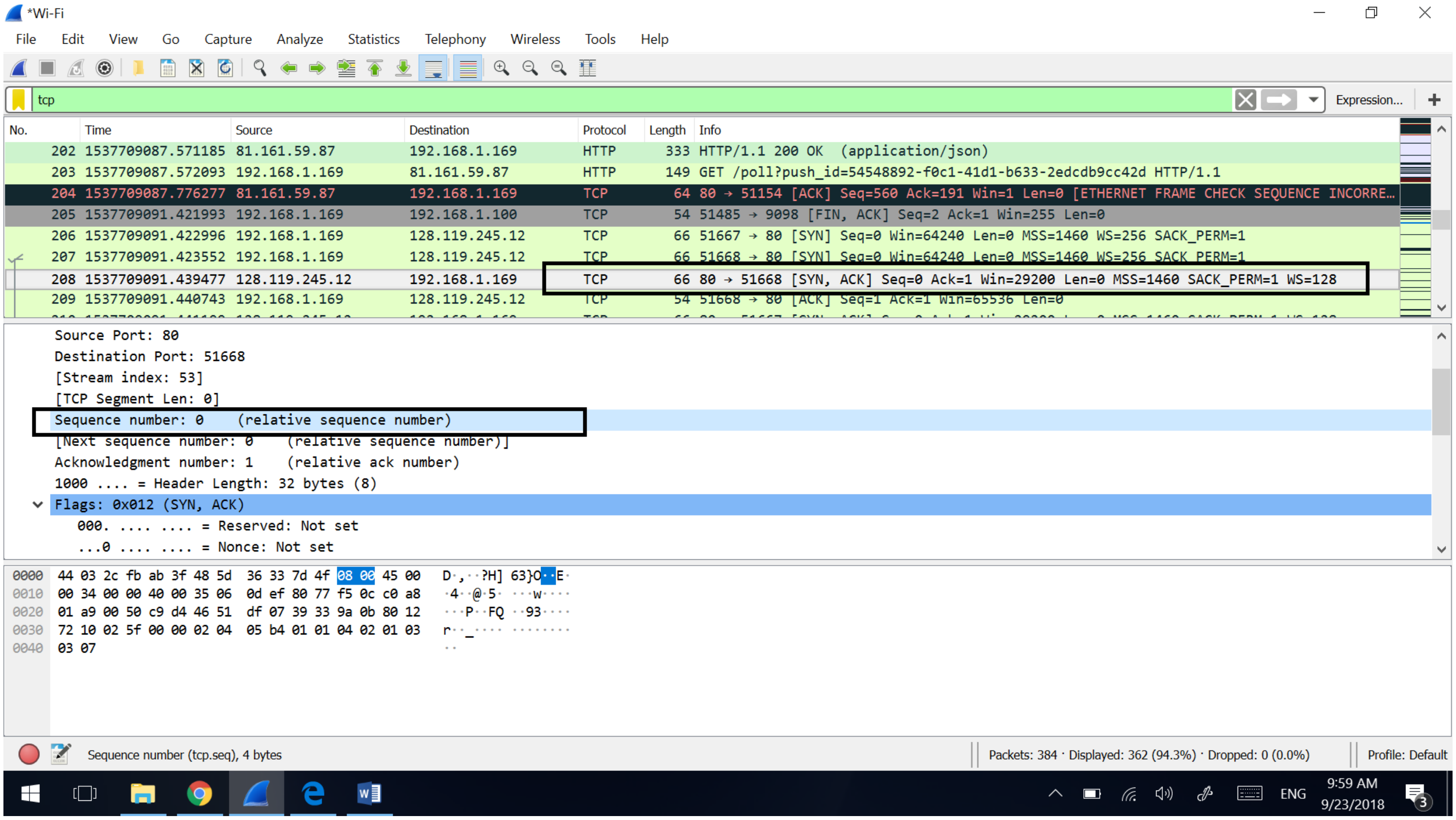
Sequence number (tcp.seq), 4 bytes

Packets: 384 · Displayed: 362 (94.3%) · 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?

Answer: We are looking at SYN ACK segment, and the sequence number is 0.



tcp

```
No.   Time              Source          Destination     Protocol Length Info
  202 1537709087.571185 81.161.59.87    192.168.1.169   HTTP     333 HTTP/1.1 200 OK  (application/json)
  203 1537709087.572093 192.168.1.169   81.161.59.87    HTTP     149 GET /poll?push_id=54548892-f0c1-41d1-b633-2edcdb9cc42d HTTP/1.1
  204 1537709087.776277 81.161.59.87    192.168.1.169   TCP       64 80 → 51154 [ACK] Seq=560 Ack=191 Win=1 Len=0 [ETHERNET FRAME CHECK SEQUENCE INCORRE…
  205 1537709091.421993 192.168.1.169   192.168.1.100   TCP       54 51485 → 9098 [FIN, ACK] Seq=2 Ack=1 Win=255 Len=0
  206 1537709091.422996 192.168.1.169   128.119.245.12  TCP       66 51667 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  207 1537709091.423552 192.168.1.169   128.119.245.12  TCP       66 51668 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  208 1537709091.439477 128.119.245.12  192.168.1.169   TCP       66 80 → 51668 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
  209 1537709091.440743 192.168.1.169   128.119.245.12  TCP       54 51668 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
```

```
    Source Port: 80
    Destination Port: 51668
    [Stream index: 53]
    [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
```

```
0000  44 03 2c fb ab 3f 48 5d  36 33 7d 4f 08 00 45 00   D·,··?H] 63}O··E·
0010  00 34 00 00 40 00 35 06  0d ef 80 77 f5 0c c0 a8   ·4··@·5· ···w····
0020  01 a9 00 50 c9 d4 46 51  df 07 39 33 9a 0b 80 12   ···P··FQ ··93····
0030  72 10 02 5f 00 00 02 04  05 b4 01 01 04 02 01 03   r··_···· ········
0040  03 07                                              ··
```

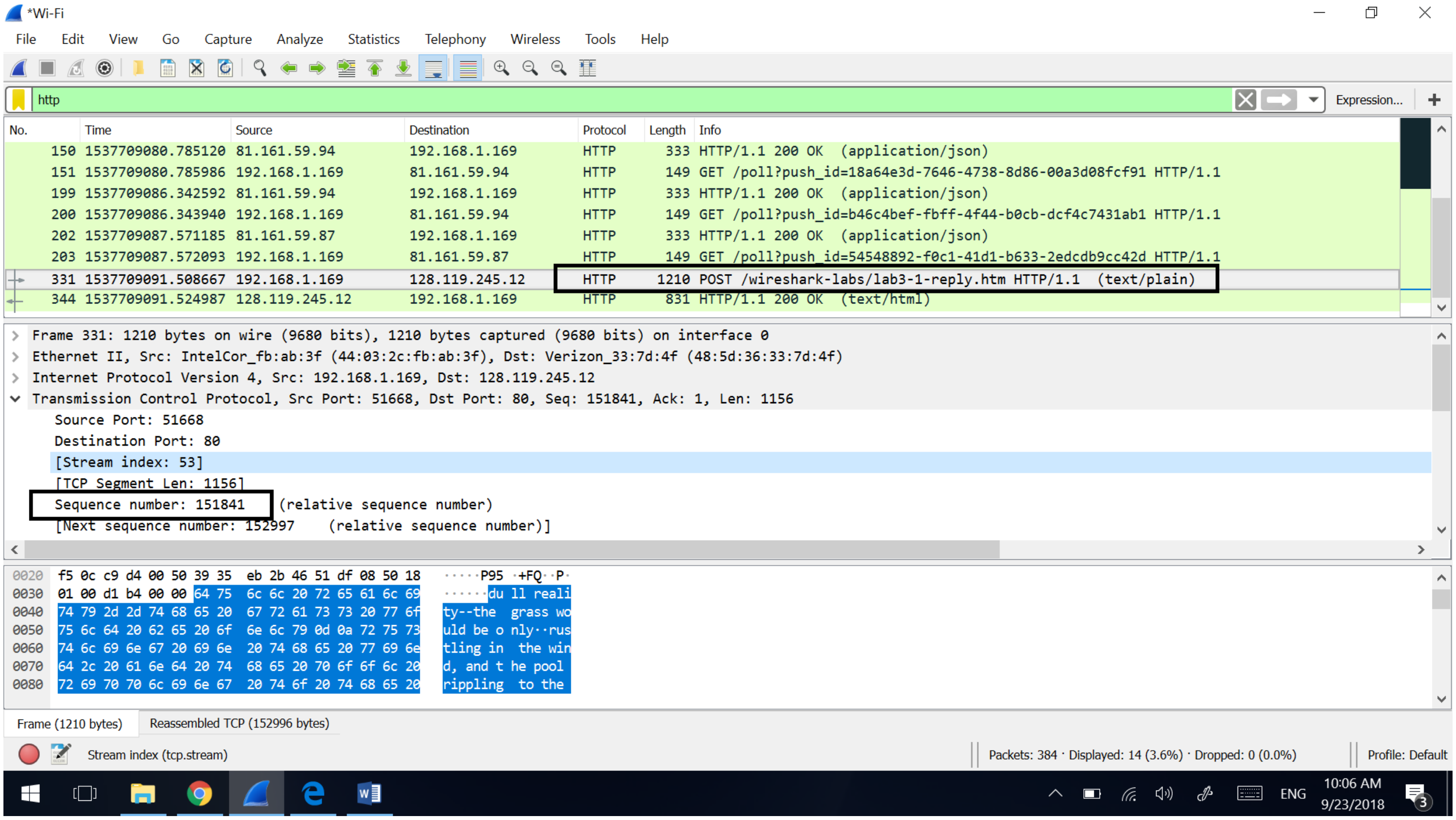
Sequence number (tcp.seq), 4 bytes

Packets: 384 · Displayed: 362 (94.3%) · Dropped: 0 (0.0%)

Profile: Default

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

Answer: HTTP => POST => Trans Prot Control => Sequence number: 151841


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

```
No.  Time               Source          Destination     Protocol Length Info
 150 1537709080.785120 81.161.59.94    192.168.1.169   HTTP      333 HTTP/1.1 200 OK  (application/json)
 151 1537709080.785986 192.168.1.169   81.161.59.94    HTTP      149 GET /poll?push_id=18a64e3d-7646-4738-8d86-00a3d08fcf91 HTTP/1.1
 199 1537709086.342592 81.161.59.94    192.168.1.169   HTTP      333 HTTP/1.1 200 OK  (application/json)
 200 1537709086.343940 192.168.1.169   81.161.59.94    HTTP      149 GET /poll?push_id=b46c4bef-fbff-4f44-b0cb-dcf4c7431ab1 HTTP/1.1
 202 1537709087.571185 81.161.59.87    192.168.1.169   HTTP      333 HTTP/1.1 200 OK  (application/json)
 203 1537709087.572093 192.168.1.169   81.161.59.87    HTTP      149 GET /poll?push_id=54548892-f0c1-41d1-b633-2edcdb9cc42d HTTP/1.1
 331 1537709091.508667 192.168.1.169   128.119.245.12  HTTP     1210 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1  (text/plain)
 344 1537709091.524987 128.119.245.12  192.168.1.169   HTTP      831 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 331: 1210 bytes on wire (9680 bits), 1210 bytes captured (9680 bits) on interface 0
> Ethernet II, Src: IntelCor_fb:ab:3f (44:03:2c:fb:ab:3f), Dst: Verizon_33:7d:4f (48:5d:36:33:7d:4f)
> Internet Protocol Version 4, Src: 192.168.1.169, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 51668, Dst Port: 80, Seq: 151841, Ack: 1, Len: 1156
    Source Port: 51668
    Destination Port: 80
    [Stream index: 53]
    [TCP Segment Len: 1156]
    Sequence number: 151841    (relative sequence number)
    [Next sequence number: 152997    (relative sequence number)]
```

```
0020  f5 0c c9 d4 00 50 39 35  eb 2b 46 51 df 08 50 18   ·····P95 ·+FQ··P·
0030  01 00 d1 b4 00 00 64 75  6c 6c 20 72 65 61 6c 69   ······du ll reali
0040  74 79 2d 2d 74 68 65 20  67 72 61 73 73 20 77 6f   ty--the  grass wo
0050  75 6c 64 20 62 65 20 6f  6e 6c 79 0d 0a 72 75 73   uld be o nly··rus
0060  74 6c 69 6e 67 20 69 6e  20 74 68 65 20 77 69 6e   tling in  the win
0070  64 2c 20 61 6e 64 20 74  68 65 20 70 6f 6f 6c 20   d, and t he pool 
0080  72 69 70 70 6c 69 6e 67  20 74 6f 20 74 68 65 20   rippling  to the 
```

Frame (1210 bytes)
Reassembled TCP (152996 bytes)
Stream index (tcp.stream)
Packets: 384 · Displayed: 14 (3.6%) · Dropped: 0 (0.0%)
Profile: Default
ENG
10:06 AM
9/23/2018