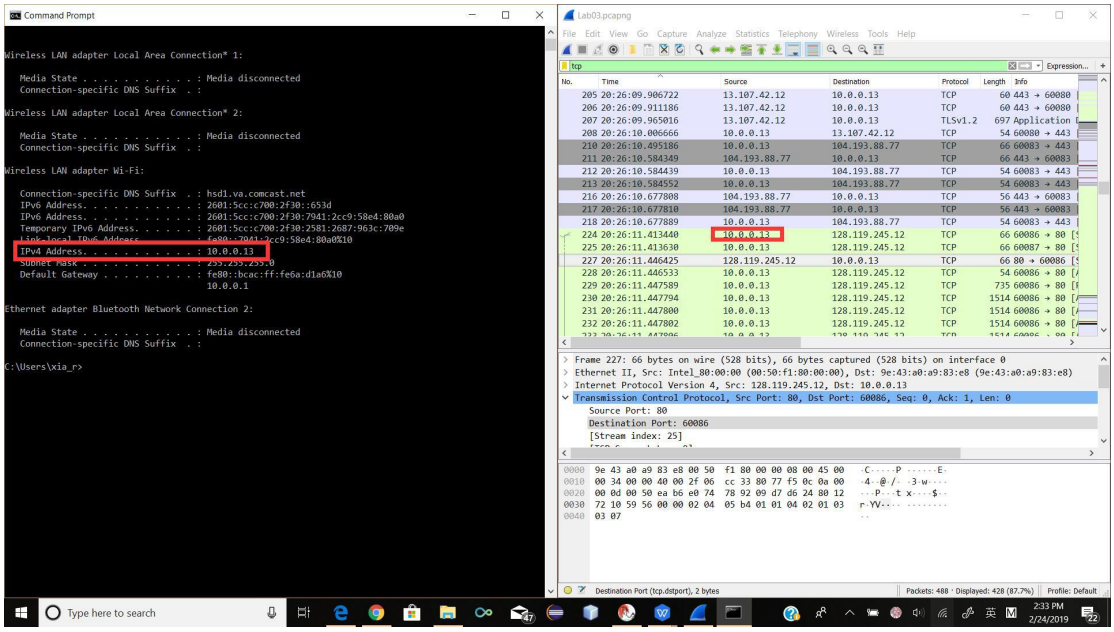
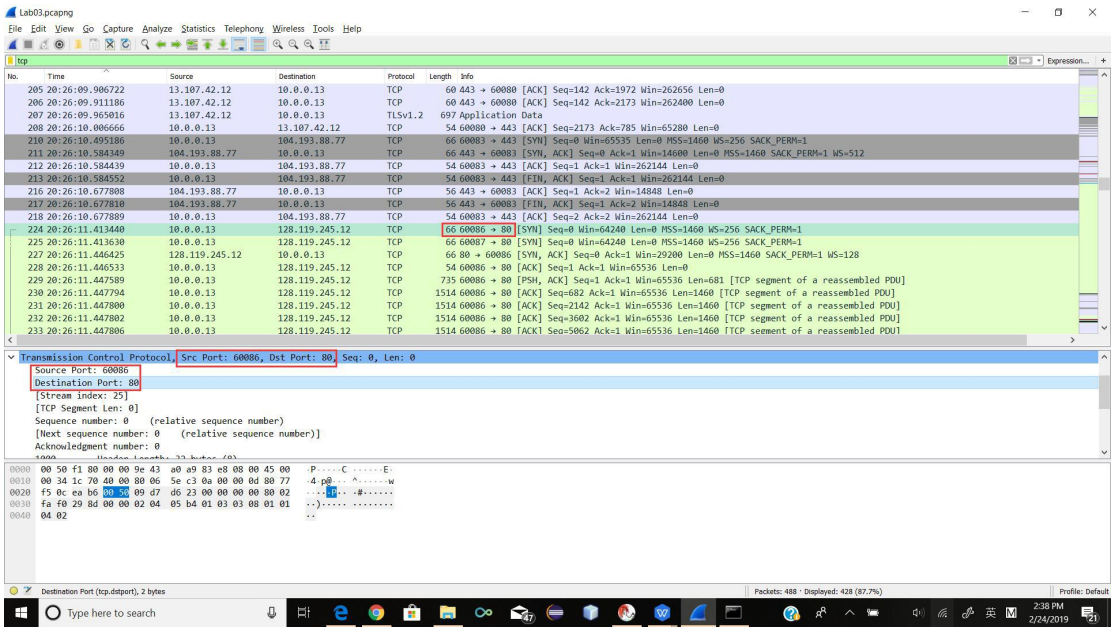
Lab 03



My IP address: 10. 0. 0. 13

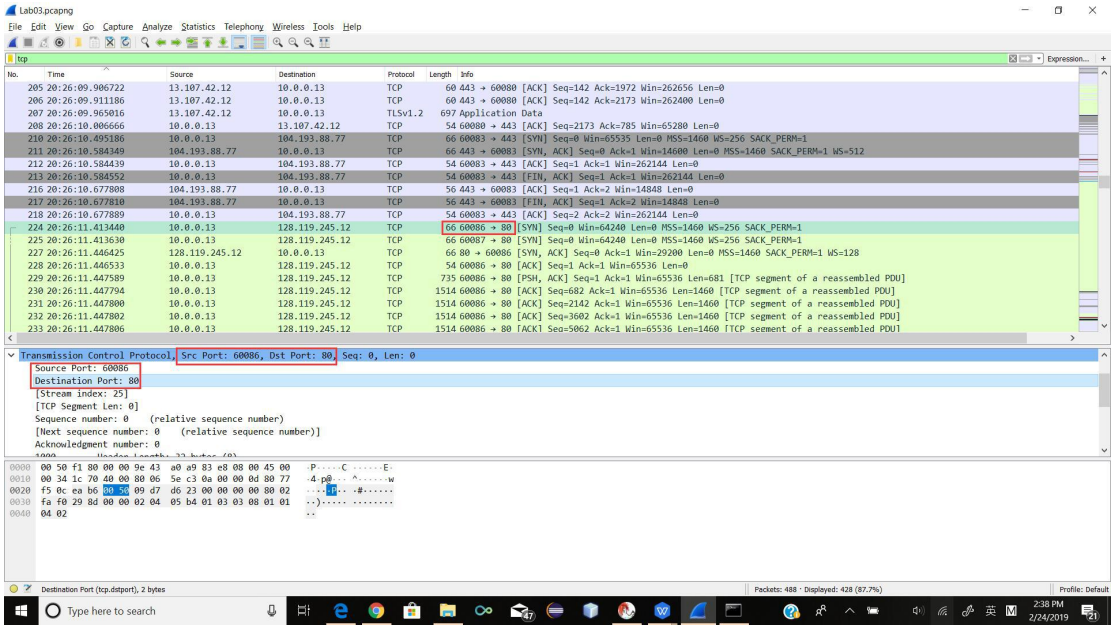
1. What is the TCP port number used by your computer to communicate with gaia.cs.umass.edu?



Port 80 is used to communicate with web server, and port 60086 is used

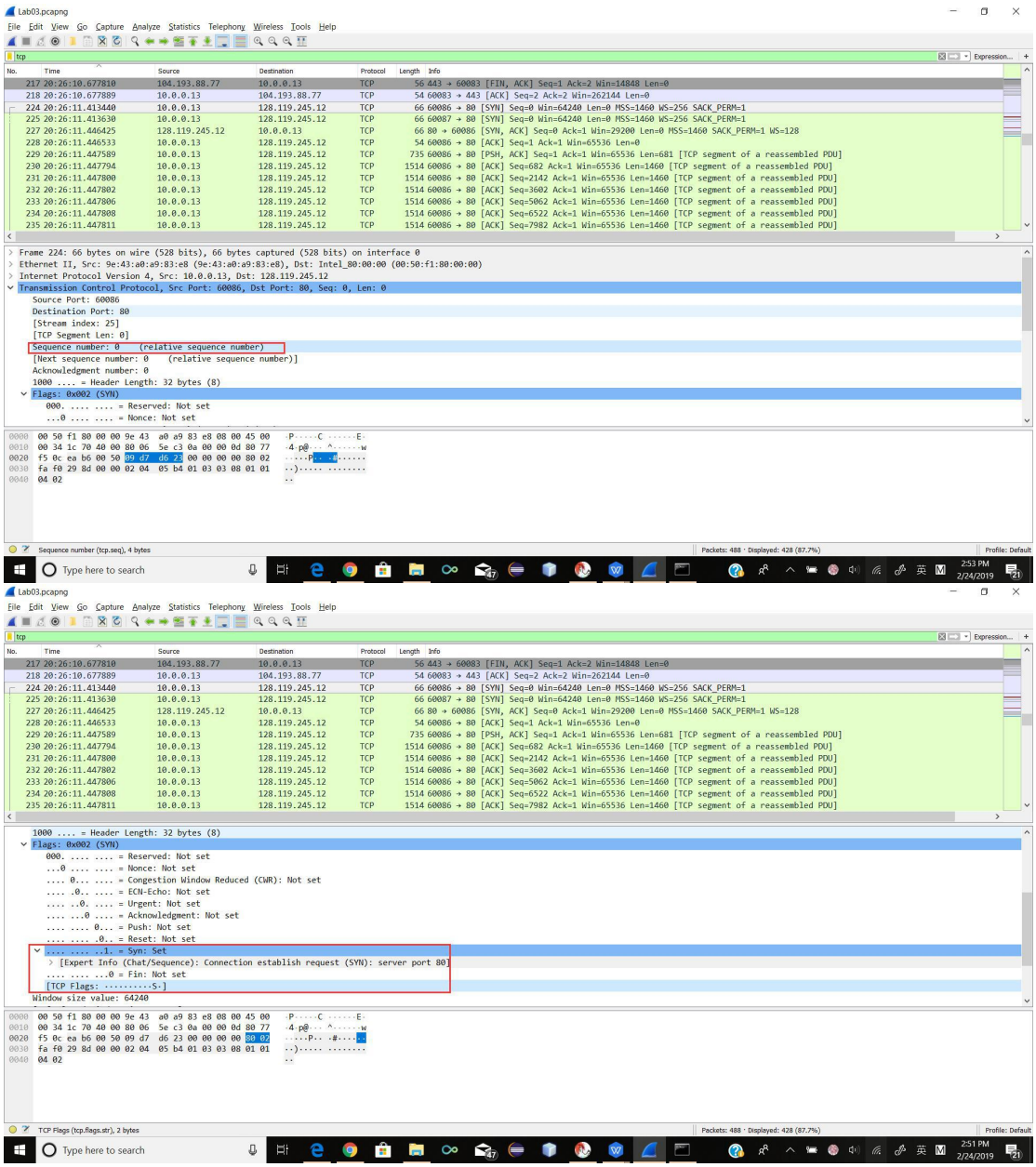
by the web server to identify and reply to my computer.

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



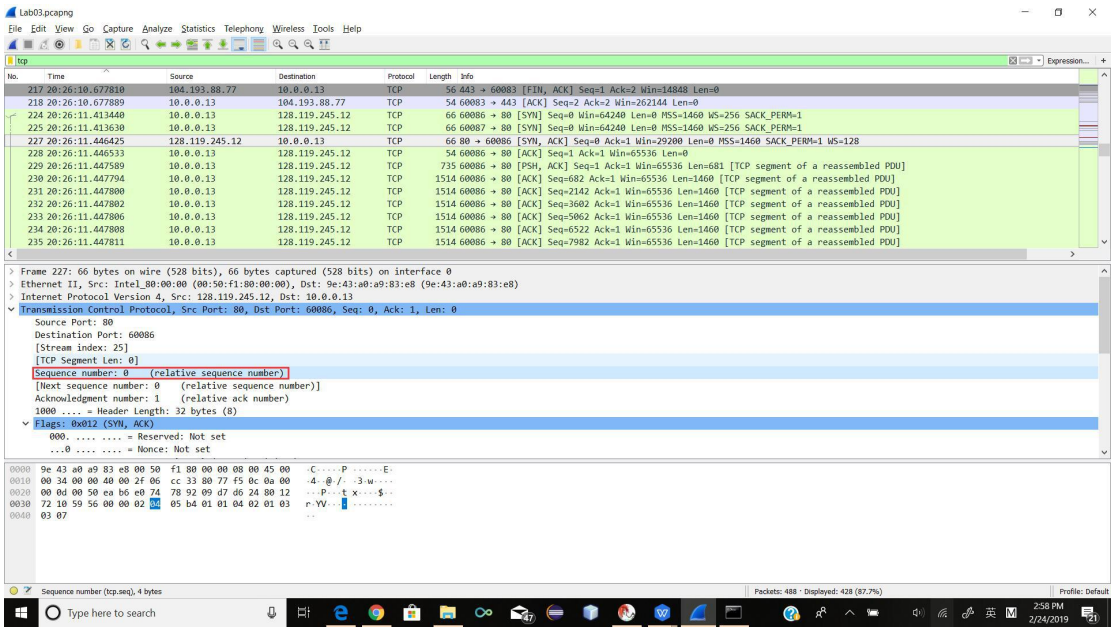
Port 80 is used to communicate with web server, and port 60086 is used by the web server to identify and reply to my computer.

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?



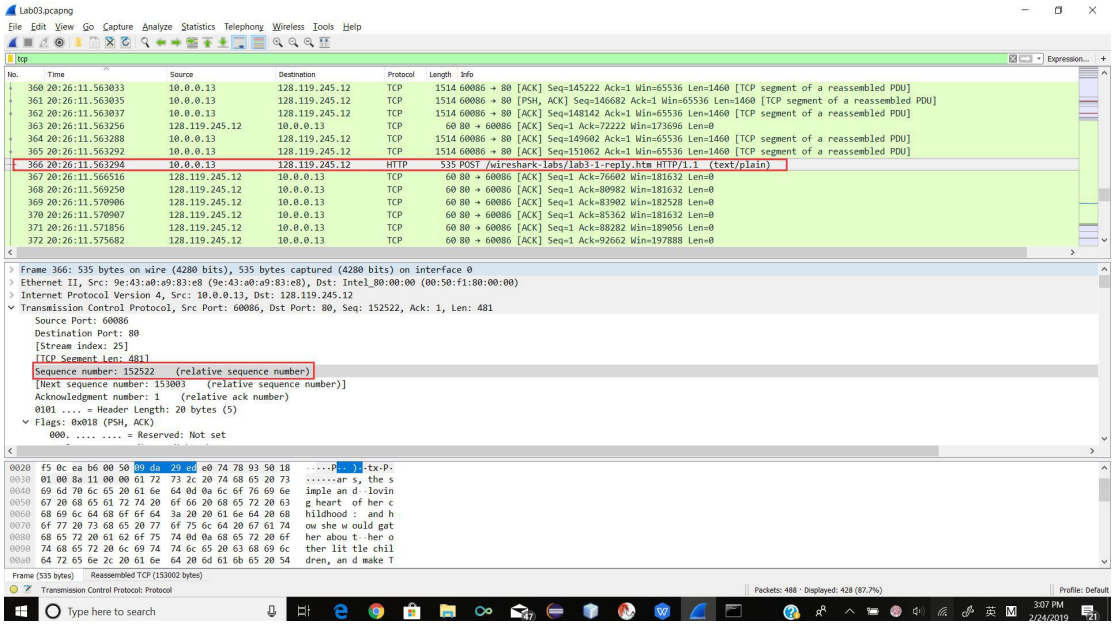
Sequence number is 0 and Flag 0x002 identifies the segment as a SYN segment.

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 of the SYNACK segment is 0. Acknowledge number is 1.

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 is 152522.

```
No.     Time               Source                Destination           Protocol Length Info
    402 20:26:11.637881    128.119.245.12        10.0.0.13             HTTP     831    HTTP/1.1 200 OK  (text/html)
Frame 402: 831 bytes on wire (6648 bits), 831 bytes captured (6648 bits) on interface 0
    Interface id: 0 (\Device\NPF_{87ECFDF9-CA2E-4423-8880-E5CB87989374})
        Interface name: \Device\NPF_{87ECFDF9-CA2E-4423-8880-E5CB87989374}
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 16, 2019 20:26:11.637881000 Eastern Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1550366771.637881000 seconds
    [Time delta from previous captured frame: 0.000201000 seconds]
    [Time delta from previous displayed frame: 0.074587000 seconds]
    [Time since reference or first frame: 11.946602000 seconds]
    Frame Number: 402
    Frame Length: 831 bytes (6648 bits)
    Capture Length: 831 bytes (6648 bits)
    [Frame is marked: True]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Intel_80:00:00 (00:50:f1:80:00:00), Dst: 9e:43:a0:a9:83:e8 (9e:43:a0:a9:83:e8)
    Destination: 9e:43:a0:a9:83:e8 (9e:43:a0:a9:83:e8)
        Address: 9e:43:a0:a9:83:e8 (9e:43:a0:a9:83:e8)
        .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Intel_80:00:00 (00:50:f1:80:00:00)
        Address: Intel_80:00:00 (00:50:f1:80:00:00)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.13
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 817
    Identification: 0x048c (1164)
    Flags: 0x4000, Don't fragment
        0... .... .... .... = Reserved bit: Not set
        .1.. .... .... .... = Don't fragment: Set
        ..0. .... .... .... = More fragments: Not set
        ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 47
    Protocol: TCP (6)
    Header checksum: 0xc4aa [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.119.245.12
    Destination: 10.0.0.13
Transmission Control Protocol, Src Port: 80, Dst Port: 60086, Seq: 1, Ack: 153003, Len: 777
    Source Port: 80
    Destination Port: 60086
    [Stream index: 25]
    [TCP Segment Len: 777]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 778    (relative sequence number)]
    Acknowledgment number: 153003    (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: 2054
    [Calculated window size: 262912]
    [Window size scaling factor: 128]
    Checksum: 0x1445 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
        [iRTT: 0.033093000 seconds]
        [Bytes in flight: 777]
        [Bytes sent since last PSH flag: 777]
    [Timestamps]
        [Time since first frame in this TCP stream: 0.224441000 seconds]
        [Time since previous frame in this TCP stream: 0.000201000 seconds]
    TCP payload (777 bytes)
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
```

```
            [HTTP/1.1 200 OK\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Sun, 17 Feb 2019 01:26:11 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
        [Content length: 418]
    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: 0.074587000 seconds]
    [Request in frame: 366]
    File Data: 418 bytes
Line-based text data: text/html (11 lines)
    <TITLE>Upload page for TCP Ethereal Lab</TITLE>\n
    <body bgcolor="#FFFFFF">\n
    <p><font face="Arial, Helvetica, sans-serif" size="4"> Congratulations! <br> </font>\n
    \n
    <P><font face="Arial, Helvetica, sans-serif"> You've now transferred a copy of alice.txt ffrom\n
    your computer to \n
    gaia.cs.umass.edu.  You should now stop Wireshark packet capture. It's time to start analyzing the captured Wireshark packets! </font>\n
    \n
    </FORM>\n
    \n
    \n
```