

Lab 03

The screenshot shows a Windows PC with two windows open. The left window is a Command Prompt displaying network configuration for three adapters: Wireless LAN adapter Local Area Connection* 1, Wireless LAN adapter Local Area Connection* 2, and Wireless LAN adapter Wi-Fi. The Wi-Fi adapter is connected to the network. The right window is Wireshark, showing a packet capture on the 'eth0' interface. The packet list shows a series of TCP packets from 10.0.0.13 to 128.119.245.12. The packet details pane shows the selected packet (No. 227) as a Transmission Control Protocol (TCP) packet with Source Port: 80 and Destination Port: 60086. The packet bytes pane shows the raw data of the packet.

My IP address: 10. 0. 0. 13

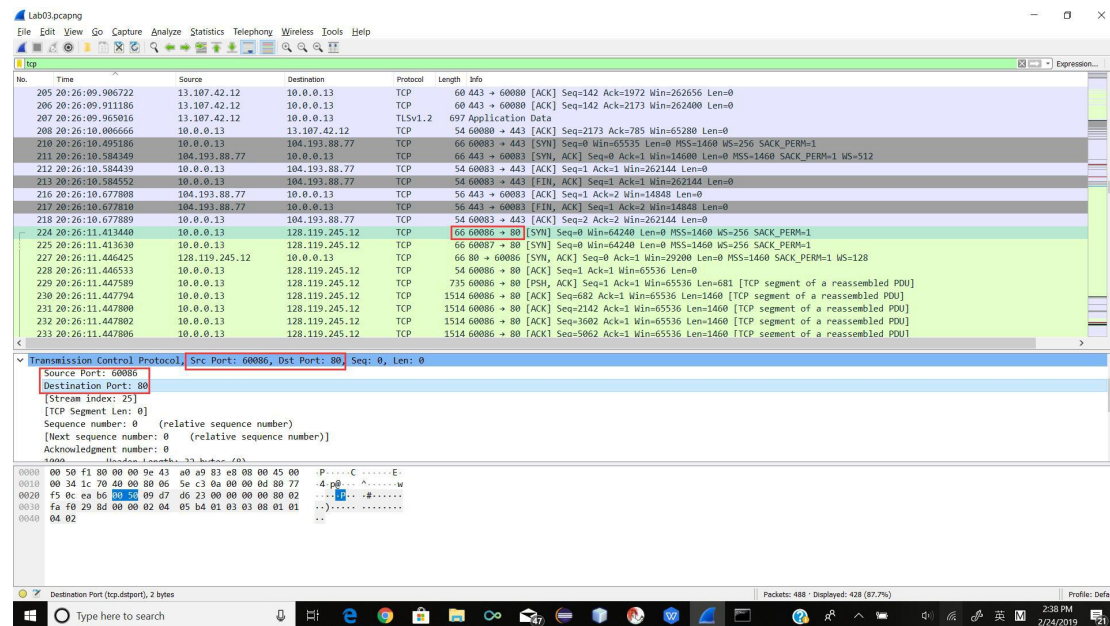
1. What is the TCP port number used by your computer to communicate with gaia.cs.umass.edu?

The screenshot shows the Wireshark interface with a packet capture on the 'eth0' interface. The packet list shows a series of TCP packets from 10.0.0.13 to 128.119.245.12. The packet details pane shows the selected packet (No. 227) as a Transmission Control Protocol (TCP) packet with Source Port: 80 and Destination Port: 60086. The packet bytes pane shows the raw data of the packet.

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.

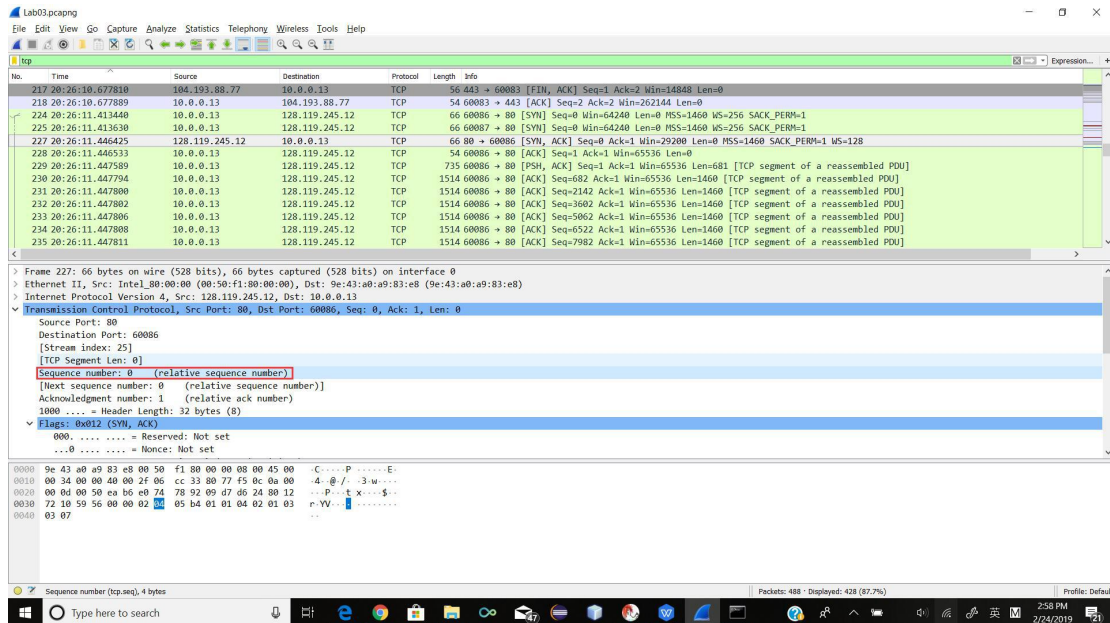
3. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between your computer and `gaia.cs.umass.edu`? What is it in the segment that identifies the segment as a SYN segment?

The image displays two screenshots of the Wireshark network protocol analyzer. The top screenshot shows a list of captured packets, with packet 224 selected. The details pane for this packet shows the 'Transmission Control Protocol' section, where the 'Sequence number' is 0 and the 'Flags' field is 0x002 (SYN). The bottom screenshot shows the expanded 'Flags' field, highlighting the 'S' bit (SYN) as set. The packet data section shows the raw bytes of the packet, including the Ethernet II header, Internet Protocol header, and the TCP segment.

Sequence number is 0 and Flag 0x002 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.

Lab03.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
360	20:26:11.563033	10.0.0.13	128.119.245.12	TCP	1514	60086 → 80 [ACK] Seq=145222 Ack=1 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
361	20:26:11.563035	10.0.0.13	128.119.245.12	TCP	1514	60086 → 80 [PSH, ACK] Seq=146682 Ack=1 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
362	20:26:11.563037	10.0.0.13	128.119.245.12	TCP	1514	60086 → 80 [ACK] Seq=148142 Ack=1 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
363	20:26:11.563256	128.119.245.12	10.0.0.13	TCP	60	80 → 60086 [ACK] Seq=1 Ack=72222 Win=173696 Len=0
364	20:26:11.563288	10.0.0.13	128.119.245.12	TCP	1514	60086 → 80 [ACK] Seq=149602 Ack=1 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
365	20:26:11.563292	10.0.0.13	128.119.245.12	TCP	1514	60086 → 80 [ACK] Seq=151062 Ack=1 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
366	20:26:11.563294	10.0.0.13	128.119.245.12	HTTP	535	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
367	20:26:11.566516	128.119.245.12	10.0.0.13	TCP	60	80 → 60086 [ACK] Seq=1 Ack=76682 Win=181632 Len=0
368	20:26:11.569258	128.119.245.12	10.0.0.13	TCP	60	80 → 60086 [ACK] Seq=1 Ack=80982 Win=181632 Len=0
369	20:26:11.570906	128.119.245.12	10.0.0.13	TCP	60	80 → 60086 [ACK] Seq=1 Ack=83982 Win=182528 Len=0
370	20:26:11.570907	128.119.245.12	10.0.0.13	TCP	60	80 → 60086 [ACK] Seq=1 Ack=85362 Win=181632 Len=0
371	20:26:11.571856	128.119.245.12	10.0.0.13	TCP	60	80 → 60086 [ACK] Seq=1 Ack=88282 Win=189056 Len=0
372	20:26:11.575682	128.119.245.12	10.0.0.13	TCP	60	80 → 60086 [ACK] Seq=1 Ack=92662 Win=197888 Len=0

< Frame 366: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface 0

> Ethernet II, Src: 9e:43:a0:a9:83:e8 (9e:43:a0:a9:83:e8), Dst: Intel_80:00:00 (80:50:f1:80:00:00)

> Internet Protocol Version 4, Src: 10.0.0.13, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 60086, Dst Port: 80, Seq: 152522, Ack: 1, Len: 481

Source Port: 60086

Destination Port: 80

[Stream index: 25]

[TCP Segment Len: 481]

Sequence number: 152522 (relative sequence number)

[Next sequence number: 153003] (relative sequence number)

Acknowledgment number: 1 (relative ack number)

0101 = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)

0000 = Reserved: Not set

0020 f5 0c ea b6 00 50 00 d0 22 c1 e0 74 78 93 50 18P.....tx-P-

0030 01 00 8a 11 00 00 61 72 73 2c 20 74 68 65 20 73or s, the s

0040 69 6d 70 6c 65 20 61 6e 64 0d 0a 6c 6f 76 69 6e imple an d lovin

0050 67 20 68 65 61 72 74 20 6f 66 20 68 65 72 20 63 g heart of her c

0060 68 69 6c 64 68 6f 6f 64 3e 20 20 61 6e 64 20 68 hillhood : and h

0070 6f 77 20 73 68 65 20 77 6f 75 6c 64 20 67 61 74 ow she w ould gat

0080 68 65 72 20 61 62 6f 75 74 0d 0a 68 65 72 20 6f her abou t her o

0090 74 68 65 72 20 6c 69 74 74 6c 65 20 63 68 69 6c then lit tle chil

00a0 64 72 65 6c 2c 20 61 6e 64 20 6d 61 6b 65 20 54 dren, an d make T

Frame 366 (535 bytes) Reassembled TCP (153003 bytes)

Transmission Control Protocol: Protocol

Packets: 488 · Displayed: 428 (87.7%)

Profile: Default

○ Type here to search

3:07 PM 2/24/2019

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_{87ECDFD9-CA2E-4423-8880-E5CB87989374})
Interface name: \Device\NPF_{87ECDFD9-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\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
```