Ariel Salazar

IT 520 – Lab3

February 18th, 2019

Instructions:

• Start up your web browser. Go the http://gaia.cs.umass.edu/wiresharklabs/alice.txt and retrieve an ASCII copy of Alice in Wonderland. Save this file somewhere on your computer.

• Next go to http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html.

• Use the Browse button in this form to enter the name of the file (full path name) on your computer containing Alice in Wonderland (or do so manually). Don't yet press the "Upload alice.txt file" button.

• Now start up Wireshark and begin packet capture (Capture->Start) and then press OK on the Wireshark Packet Capture Options screen (we'll not need to select any options here).

• Returning to your browser, press the "Upload alice.txt file" button to upload the file to the gaia.cs.umass.edu server. Once the file has been uploaded, a short congratulations message will be displayed in your browser window.

• Stop Wireshark packet capture and filter tcp packets.

• (For each of these questions, take a screenshot of Wireshark, and attach it to your answer) - Questions without Full Screenshot will not be graded. A lab submission template is available on canvas. Your screenshot should indicate the time and date on your computer.

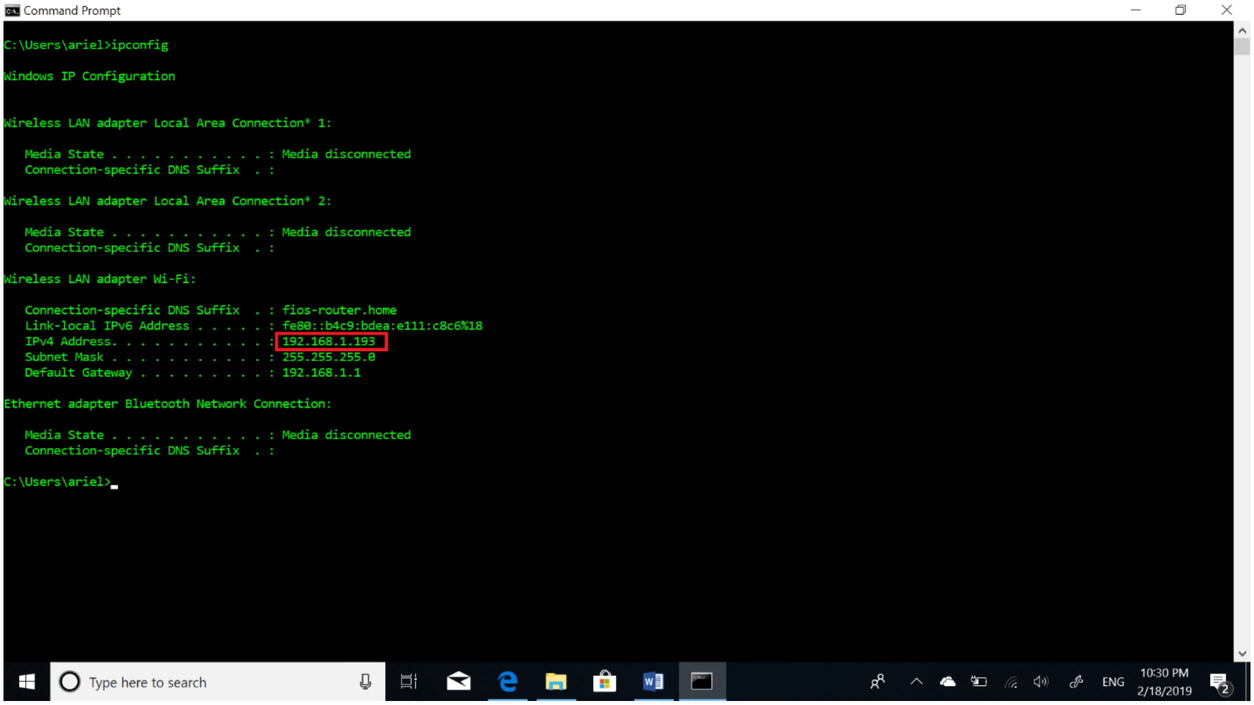
• Include a terminal screenshot showing computer IP address on the front page before Question 1, and a full PRINT of the HTTP OK message as the last page.

Lab will NOT be graded if either of these two is missing.

Questions:

Terminal Screenshot with the IP address of my computer:

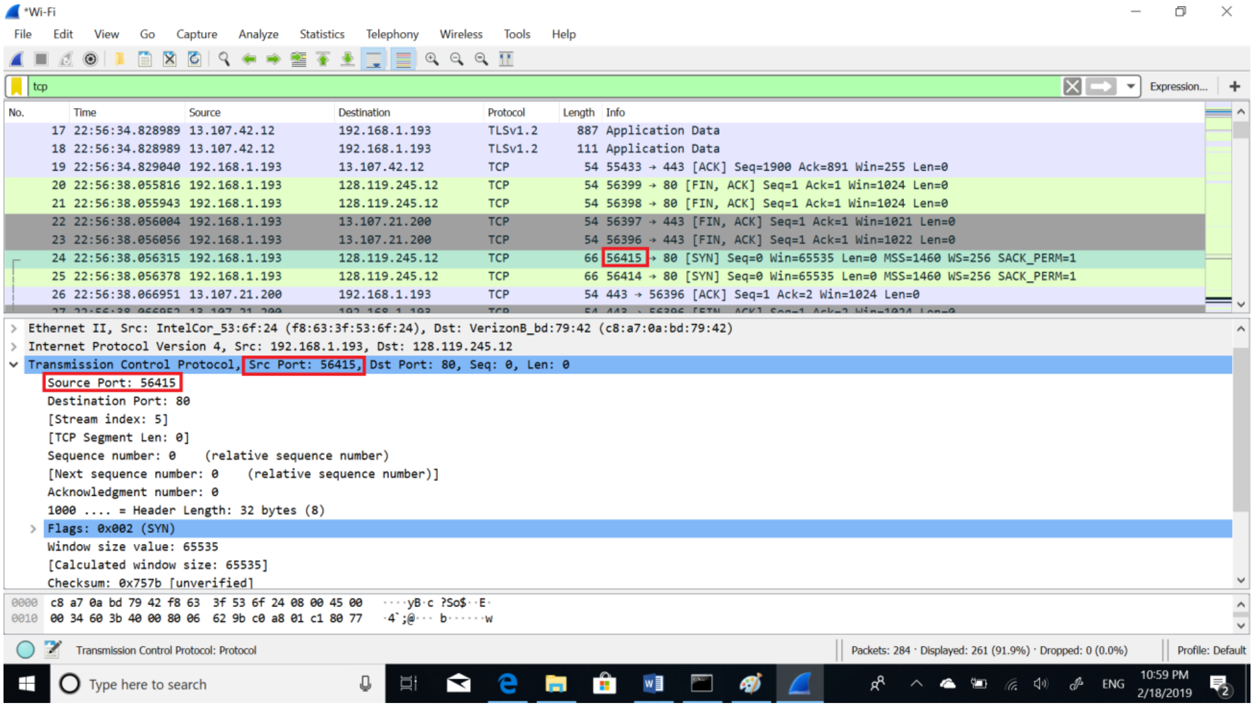
IP Address: 192.168.1.193



```
C:\Users\ariel>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

   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::b4c9:bdea:e111:c8c6%18
   IPv4 Address. . . . . . . . . . . : 192.168.1.193
   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  . :

C:\Users\ariel>_
```

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

The Port Number used by my computer is: 56415


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
Expression…
Transmission Control Protocol: Protocol
Packets: 284 · Displayed: 261 (91.9%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
ENG
10:59 PM
2/18/2019

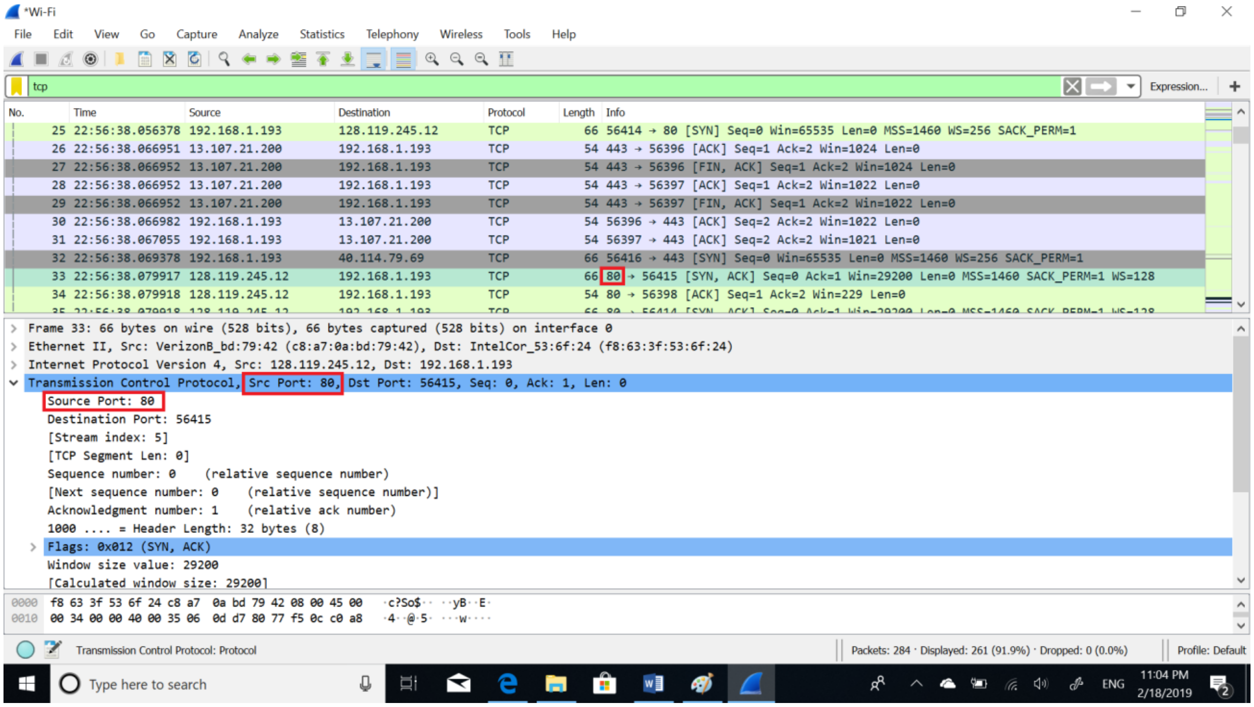
```
No.   Time            Source         Destination    Protocol Length Info
   17 22:56:34.828989 13.107.42.12   192.168.1.193  TLSv1.2   887 Application Data
   18 22:56:34.828989 13.107.42.12   192.168.1.193  TLSv1.2   111 Application Data
   19 22:56:34.829040 192.168.1.193  13.107.42.12   TCP        54 55433 → 443 [ACK] Seq=1900 Ack=891 Win=255 Len=0
   20 22:56:38.055816 192.168.1.193  128.119.245.12 TCP        54 56399 → 80 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
   21 22:56:38.055943 192.168.1.193  128.119.245.12 TCP        54 56398 → 80 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
   22 22:56:38.056004 192.168.1.193  13.107.21.200  TCP        54 56397 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1021 Len=0
   23 22:56:38.056056 192.168.1.193  13.107.21.200  TCP        54 56396 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1022 Len=0
   24 22:56:38.056315 192.168.1.193  128.119.245.12 TCP        66 56415 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
   25 22:56:38.056378 192.168.1.193  128.119.245.12 TCP        66 56414 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
   26 22:56:38.066951 13.107.21.200  192.168.1.193  TCP        54 443 → 56396 [ACK] Seq=1 Ack=2 Win=1024 Len=0
```

```
> Ethernet II, Src: IntelCor_53:6f:24 (f8:63:3f:53:6f:24), Dst: VerizonB_bd:79:42 (c8:a7:0a:bd:79:42)
> Internet Protocol Version 4, Src: 192.168.1.193, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 56415, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 56415
    Destination Port: 80
    [Stream index: 5]
    [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)
    Window size value: 65535
    [Calculated window size: 65535]
    Checksum: 0x757b [unverified]
```

```
0000  c8 a7 0a bd 79 42 f8 63  3f 53 6f 24 08 00 45 00   ····yB·c ?So$··E·
0010  00 34 60 3b 40 00 80 06  62 9b c0 a8 01 c1 80 77   ·4`;@··· b······w
```

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

The TCP port number used by gaia.cs.umass.edu is: 80


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
Expression…
Transmission Control Protocol: Protocol
Packets: 284 · Displayed: 261 (91.9%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
ENG
11:04 PM
2/18/2019

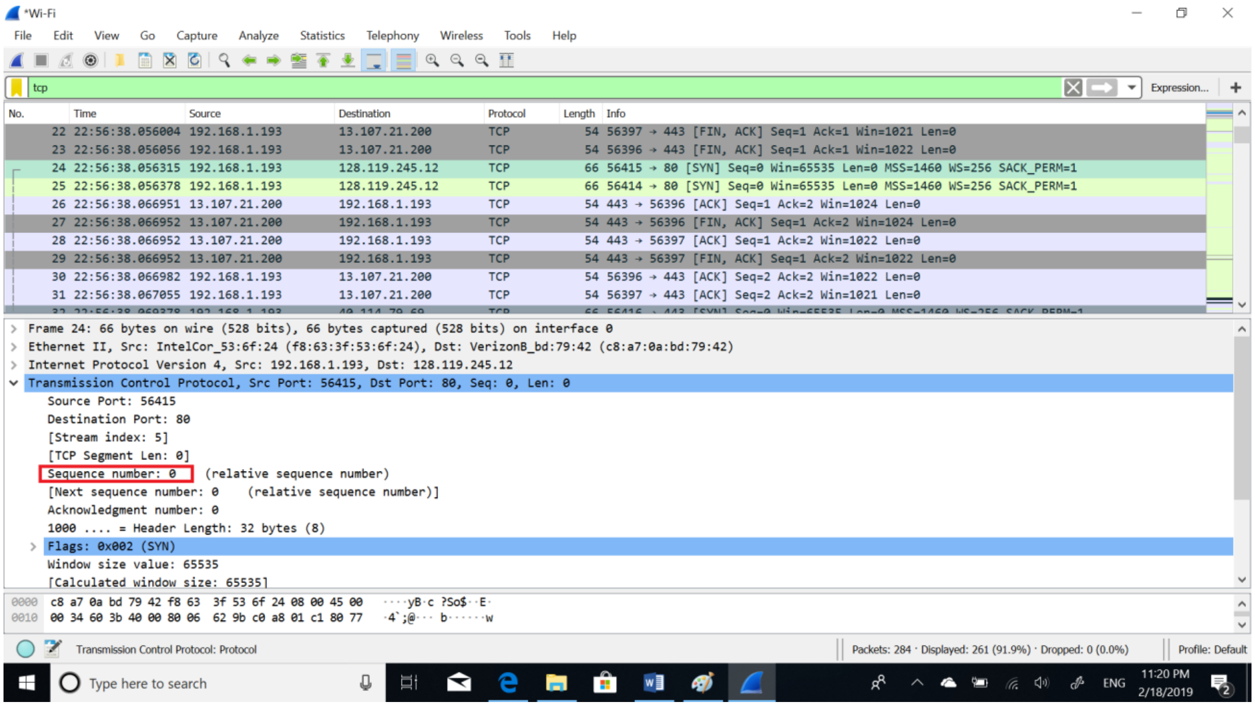
```
No.   Time            Source         Destination    Protocol Length Info
   25 22:56:38.056378 192.168.1.193  128.119.245.12 TCP        66 56414 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
   26 22:56:38.066951 13.107.21.200  192.168.1.193  TCP        54 443 → 56396 [ACK] Seq=1 Ack=2 Win=1024 Len=0
   27 22:56:38.066952 13.107.21.200  192.168.1.193  TCP        54 443 → 56396 [FIN, ACK] Seq=1 Ack=2 Win=1024 Len=0
   28 22:56:38.066952 13.107.21.200  192.168.1.193  TCP        54 443 → 56397 [ACK] Seq=1 Ack=2 Win=1022 Len=0
   29 22:56:38.066952 13.107.21.200  192.168.1.193  TCP        54 443 → 56397 [FIN, ACK] Seq=1 Ack=2 Win=1022 Len=0
   30 22:56:38.066982 192.168.1.193  13.107.21.200  TCP        54 56396 → 443 [ACK] Seq=2 Ack=2 Win=1022 Len=0
   31 22:56:38.067055 192.168.1.193  13.107.21.200  TCP        54 56397 → 443 [ACK] Seq=2 Ack=2 Win=1021 Len=0
   32 22:56:38.069378 192.168.1.193  40.114.79.69   TCP        66 56416 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
   33 22:56:38.079917 128.119.245.12 192.168.1.193  TCP        66 80 → 56415 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
   34 22:56:38.079918 128.119.245.12 192.168.1.193  TCP        54 80 → 56398 [ACK] Seq=1 Ack=2 Win=229 Len=0
```

```
> Frame 33: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: VerizonB_bd:79:42 (c8:a7:0a:bd:79:42), Dst: IntelCor_53:6f:24 (f8:63:3f:53:6f:24)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.193
v Transmission Control Protocol, Src Port: 80, Dst Port: 56415, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 56415
    [Stream index: 5]
    [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]
```

```
0000  f8 63 3f 53 6f 24 c8 a7  0a bd 79 42 08 00 45 00   ·c?So$·· ··yB··E·
0010  00 34 00 00 40 00 35 06  0d d7 80 77 f5 0c c0 a8   ·4··@·5· ···w····
```

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?**

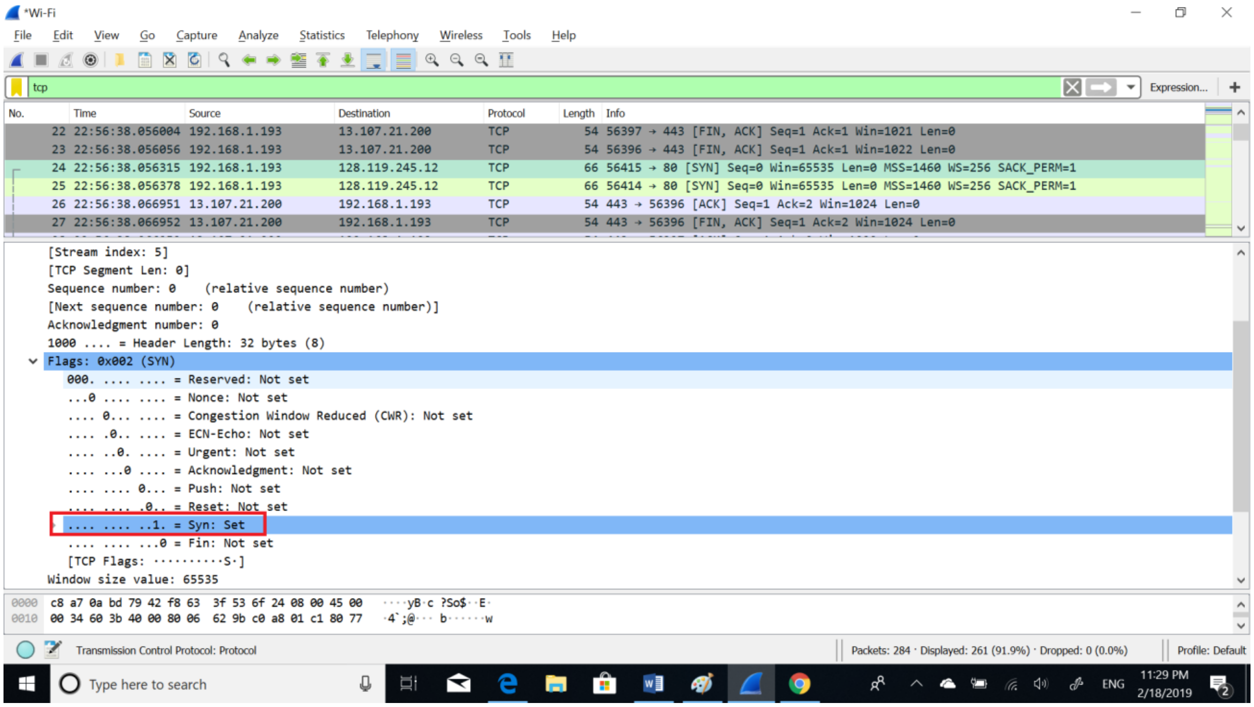
   The sequence number of the TCP SYN segment that is used to initiate the TCP connection between my computer and the gaia.cs.umass.edu is: 0 (for this segment)



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

```
No.   Time             Source         Destination     Protocol Length Info
   22 22:56:38.056004 192.168.1.193  13.107.21.200   TCP      54 56397 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1021 Len=0
   23 22:56:38.056056 192.168.1.193  13.107.21.200   TCP      54 56396 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1022 Len=0
   24 22:56:38.056315 192.168.1.193  128.119.245.12  TCP      66 56415 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
   25 22:56:38.056378 192.168.1.193  128.119.245.12  TCP      66 56414 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
   26 22:56:38.066951 13.107.21.200  192.168.1.193   TCP      54 443 → 56396 [ACK] Seq=1 Ack=2 Win=1024 Len=0
   27 22:56:38.066952 13.107.21.200  192.168.1.193   TCP      54 443 → 56396 [FIN, ACK] Seq=1 Ack=2 Win=1024 Len=0
   28 22:56:38.066952 13.107.21.200  192.168.1.193   TCP      54 443 → 56397 [ACK] Seq=1 Ack=2 Win=1022 Len=0
   29 22:56:38.066952 13.107.21.200  192.168.1.193   TCP      54 443 → 56397 [FIN, ACK] Seq=1 Ack=2 Win=1022 Len=0
   30 22:56:38.066982 192.168.1.193  13.107.21.200   TCP      54 56396 → 443 [ACK] Seq=2 Ack=2 Win=1022 Len=0
   31 22:56:38.067055 192.168.1.193  13.107.21.200   TCP      54 56397 → 443 [ACK] Seq=2 Ack=2 Win=1021 Len=0
   32 22:56:38.069378 192.168.1.193  40.114.79.69    TCP      66 56416 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1

> Frame 24: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: IntelCor_53:6f:24 (f8:63:3f:53:6f:24), Dst: VerizonB_bd:79:42 (c8:a7:0a:bd:79:42)
> Internet Protocol Version 4, Src: 192.168.1.193, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 56415, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 56415
    Destination Port: 80
    [Stream index: 5]
    [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)
    Window size value: 65535
    [Calculated window size: 65535]

0000  c8 a7 0a bd 79 42 f8 63  3f 53 6f 24 08 00 45 00   ····yB·c ?So$··E·
0010  00 34 60 3b 40 00 80 06  62 9b c0 a8 01 c1 80 77   ·4`;@··· b······w

Transmission Control Protocol: Protocol    Packets: 284 · Displayed: 261 (91.9%) · Dropped: 0 (0.0%)    Profile: Default
```

   In the segment there is a Syn flag that is set to 1 and indicates that this segment is a SYN segment.

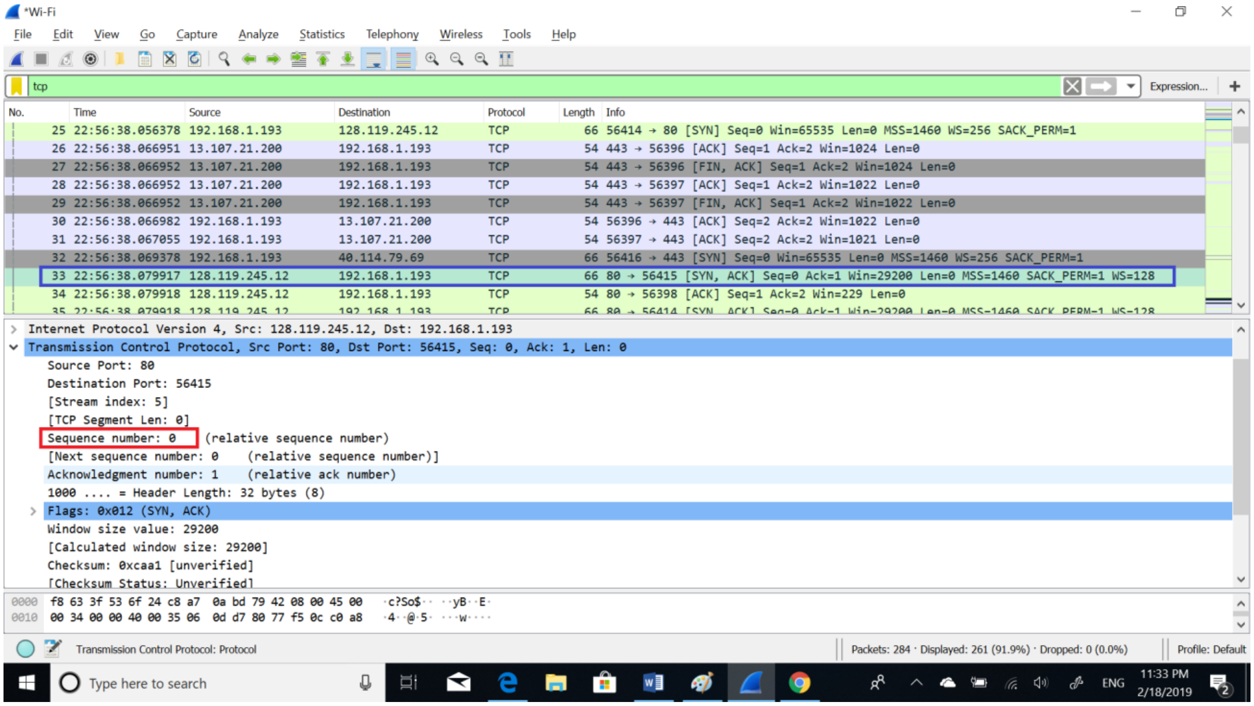


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
Expression...

```
No.   Time             Source         Destination     Protocol Length Info
   22 22:56:38.056004 192.168.1.193  13.107.21.200   TCP      54 56397 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1021 Len=0
   23 22:56:38.056056 192.168.1.193  13.107.21.200   TCP      54 56396 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1022 Len=0
   24 22:56:38.056315 192.168.1.193  128.119.245.12  TCP      66 56415 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
   25 22:56:38.056378 192.168.1.193  128.119.245.12  TCP      66 56414 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
   26 22:56:38.066951 13.107.21.200  192.168.1.193   TCP      54 443 → 56396 [ACK] Seq=1 Ack=2 Win=1024 Len=0
   27 22:56:38.066952 13.107.21.200  192.168.1.193   TCP      54 443 → 56396 [FIN, ACK] Seq=1 Ack=2 Win=1024 Len=0

    [Stream index: 5]
    [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)
  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: 65535

0000  c8 a7 0a bd 79 42 f8 63  3f 53 6f 24 08 00 45 00   ····yB·c ?So$··E·
0010  00 34 60 3b 40 00 80 06  62 9b c0 a8 01 c1 80 77   ·4`;@··· b······w

Transmission Control Protocol: Protocol    Packets: 284 · Displayed: 261 (91.9%) · 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.**

   The sequence number of the SYNACK segment sent by gaia.cs.umass.edu to my computer in reply to the SYN is: 0 (for this segment)



```
No.  Time               Source          Destination     Protocol  Length Info
  25 22:56:38.056378 192.168.1.193   128.119.245.12  TCP         66 56414 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
  26 22:56:38.066951 13.107.21.200   192.168.1.193   TCP         54 443 → 56396 [ACK] Seq=1 Ack=2 Win=1024 Len=0
  27 22:56:38.066952 13.107.21.200   192.168.1.193   TCP         54 443 → 56396 [FIN, ACK] Seq=1 Ack=2 Win=1024 Len=0
  28 22:56:38.066952 13.107.21.200   192.168.1.193   TCP         54 443 → 56397 [ACK] Seq=1 Ack=2 Win=1022 Len=0
  29 22:56:38.066952 13.107.21.200   192.168.1.193   TCP         54 443 → 56397 [FIN, ACK] Seq=1 Ack=2 Win=1022 Len=0
  30 22:56:38.066982 192.168.1.193   13.107.21.200   TCP         54 56396 → 443 [ACK] Seq=2 Ack=2 Win=1022 Len=0
  31 22:56:38.067055 192.168.1.193   13.107.21.200   TCP         54 56397 → 443 [ACK] Seq=2 Ack=2 Win=1021 Len=0
  32 22:56:38.069378 192.168.1.193   40.114.79.69    TCP         66 56416 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
  33 22:56:38.079917 128.119.245.12  192.168.1.193   TCP         66 80 → 56415 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
  34 22:56:38.079918 128.119.245.12  192.168.1.193   TCP         54 80 → 56398 [ACK] Seq=1 Ack=2 Win=229 Len=0
  35 22:56:38.079918 128.119.245.12  192.168.1.193   TCP         66 80 → 56414 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
```

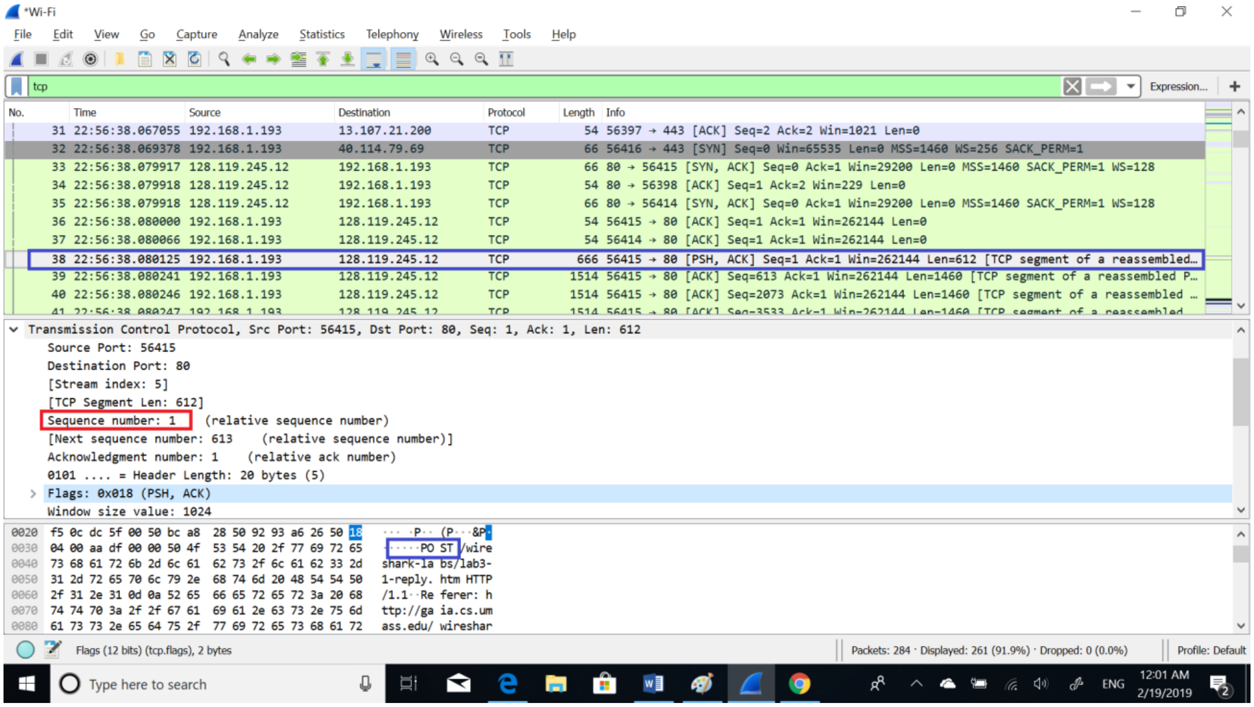
```
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.193
v Transmission Control Protocol, Src Port: 80, Dst Port: 56415, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 56415
    [Stream index: 5]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence 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: 0xcaa1 [unverified]
    [Checksum Status: Unverified]
```

```
0000  f8 63 3f 53 6f 24 c8 a7  0a bd 79 42 08 00 45 00   ·c?So$·· ··yB··E·
0010  00 34 00 00 40 00 35 06  0d d7 80 77 f5 0c c0 a8   ·4··@·5· ···w····
```

Transmission Control Protocol: Protocol | Packets: 284 · Displayed: 261 (91.9%) · 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.**

   The sequence number of the TCP segment containing the HTTP POST command is: 1



```
No.  Time               Source          Destination     Protocol  Length Info
  31 22:56:38.067055 192.168.1.193   13.107.21.200   TCP         54 56397 → 443 [ACK] Seq=2 Ack=2 Win=1021 Len=0
  32 22:56:38.069378 192.168.1.193   40.114.79.69    TCP         66 56416 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
  33 22:56:38.079917 128.119.245.12  192.168.1.193   TCP         66 80 → 56415 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
  34 22:56:38.079918 128.119.245.12  192.168.1.193   TCP         54 80 → 56398 [ACK] Seq=1 Ack=2 Win=229 Len=0
  35 22:56:38.079918 128.119.245.12  192.168.1.193   TCP         66 80 → 56414 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
  36 22:56:38.080000 192.168.1.193   128.119.245.12  TCP         54 56415 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
  37 22:56:38.080066 192.168.1.193   128.119.245.12  TCP         54 56414 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
  38 22:56:38.080125 192.168.1.193   128.119.245.12  TCP        666 56415 → 80 [PSH, ACK] Seq=1 Ack=1 Win=262144 Len=612 [TCP segment of a reassembled…
  39 22:56:38.080241 192.168.1.193   128.119.245.12  TCP       1514 56415 → 80 [ACK] Seq=613 Ack=1 Win=262144 Len=1460 [TCP segment of a reassembled P…
  40 22:56:38.080246 192.168.1.193   128.119.245.12  TCP       1514 56415 → 80 [ACK] Seq=2073 Ack=1 Win=262144 Len=1460 [TCP segment of a reassembled …
  41 22:56:38.080247 192.168.1.193   128.119.245.12  TCP       1514 56415 → 80 [ACK] Seq=3533 Ack=1 Win=262144 Len=1460 [TCP segment of a reassembled
```

```
v Transmission Control Protocol, Src Port: 56415, Dst Port: 80, Seq: 1, Ack: 1, Len: 612
    Source Port: 56415
    Destination Port: 80
    [Stream index: 5]
    [TCP Segment Len: 612]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 613    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 1024
```

```
0020  f5 0c dc 5f 00 50 bc a8  28 50 92 93 a6 26 50 18   ···_·P·· (P···&P·
0030  04 00 aa df 00 00 50 4f  53 54 20 2f 77 69 72 65   ······PO ST /wire
0040  73 68 61 72 6b 2d 6c 61  62 73 2f 6c 61 62 33 2d   shark-la bs/lab3-
0050  31 2d 72 65 70 6c 79 2e  68 74 6d 20 48 54 54 50   1-reply. htm HTTP
0060  2f 31 2e 31 0d 0a 52 65  66 65 72 65 72 3a 20 68   /1.1··Re ferer: h
0070  74 74 70 3a 2f 2f 67 61  69 61 2e 63 73 2e 75 6d   ttp://ga ia.cs.um
0080  61 73 73 2e 65 64 75 2f  77 69 72 65 73 68 61 72   ass.edu/ wireshar
```

Flags (12 bits) (tcp.flags), 2 bytes | Packets: 284 · Displayed: 261 (91.9%) · Dropped: 0 (0.0%) | Profile: Default