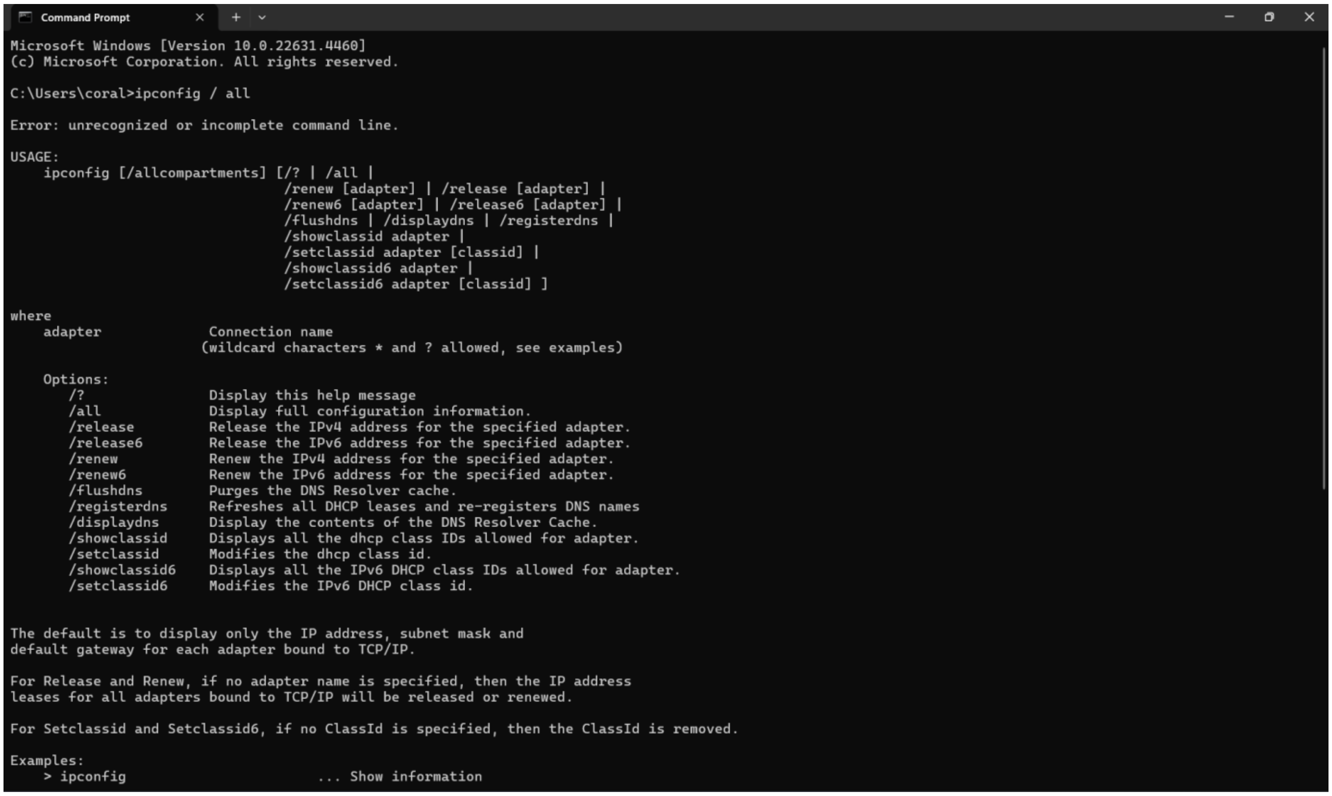
Polytechnic University of Puerto Rico
Electrical and Computer Engineering & Computer Science Department
COE 4330, Section 80 – Computer Networks

Homework 4

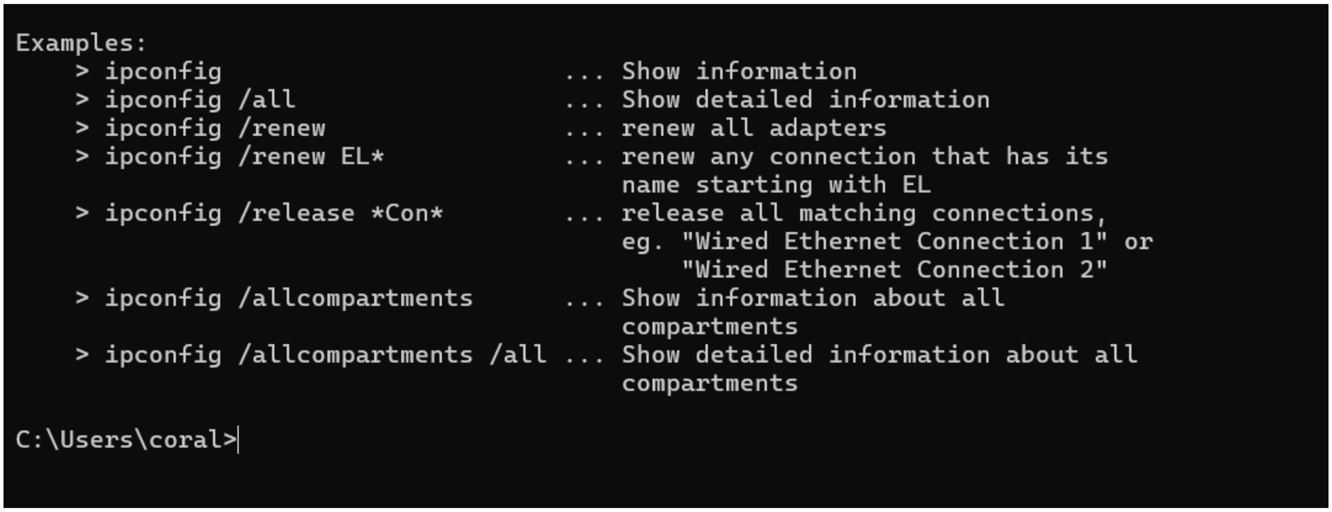
Name: **Coral S. Schmidt Montilla** **ID#:** **148830**

Completely answer all of the following questions.

1. Open Windows' Command Prompt and type ipconfig /all (in Linux/Unix/Mac type ifconfig). Provide a screenshot that shows the result of executing the command for the network interface in use during the exercise. This screenshot will show your computer's IP address, default gateway, and local DNS servers.



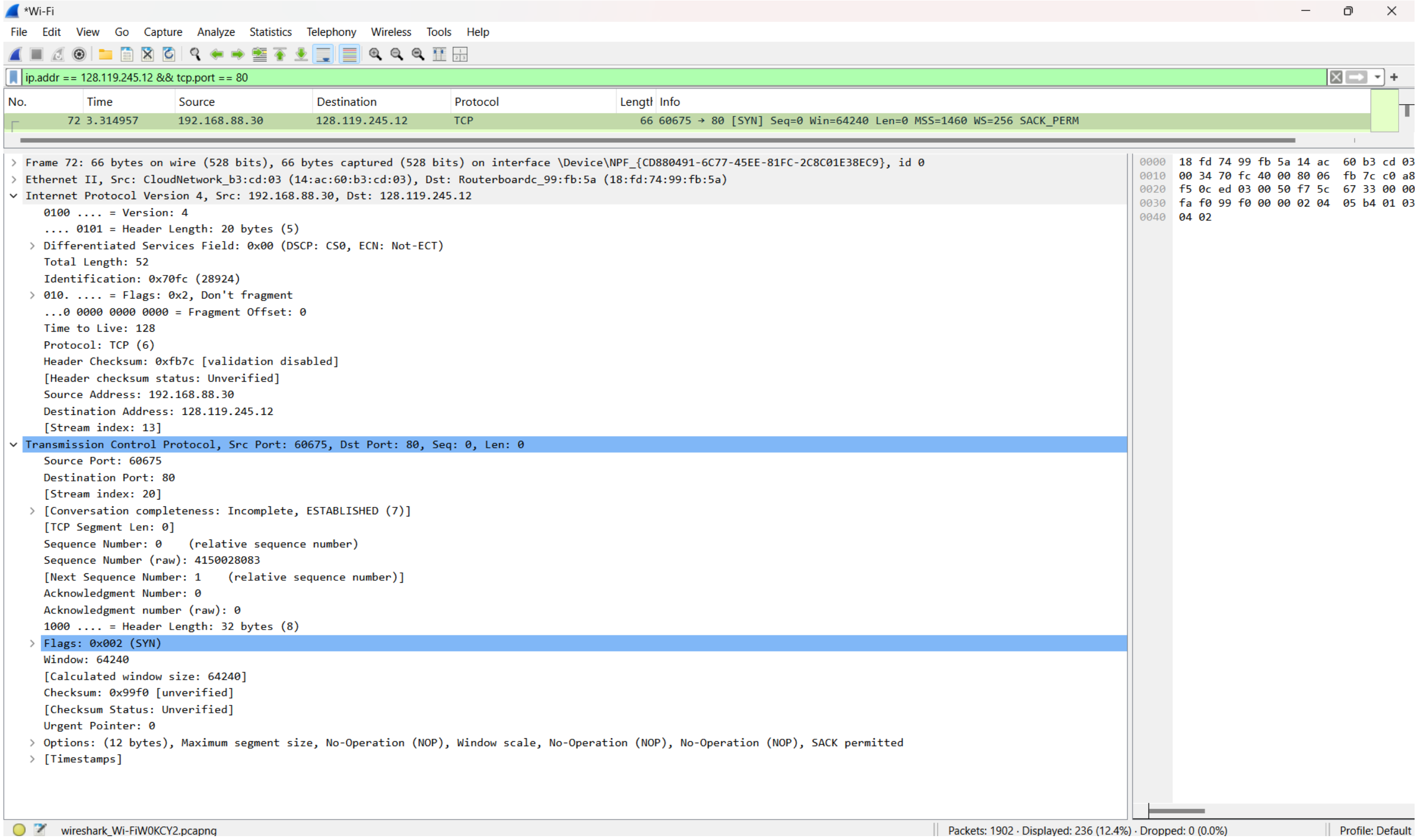
```
Microsoft Windows [Version 10.0.22631.4460]
(c) Microsoft Corporation. All rights reserved.

C:\Users\coral>ipconfig / all

Error: unrecognized or incomplete command line.

USAGE:
    ipconfig [/allcompartments] [/? | /all |
                                 /renew [adapter] | /release [adapter] |
                                 /renew6 [adapter] | /release6 [adapter] |
                                 /flushdns | /displaydns | /registerdns |
                                 /showclassid adapter |
                                 /setclassid adapter [classid] |
                                 /showclassid6 adapter |
                                 /setclassid6 adapter [classid] ]

where
    adapter             Connection name
                       (wildcard characters * and ? allowed, see examples)

    Options:
       /?               Display this help message
       /all             Display full configuration information.
       /release         Release the IPv4 address for the specified adapter.
       /release6        Release the IPv6 address for the specified adapter.
       /renew           Renew the IPv4 address for the specified adapter.
       /renew6          Renew the IPv6 address for the specified adapter.
       /flushdns        Purges the DNS Resolver cache.
       /registerdns     Refreshes all DHCP leases and re-registers DNS names
       /displaydns      Display the contents of the DNS Resolver Cache.
       /showclassid     Displays all the dhcp class IDs allowed for adapter.
       /setclassid      Modifies the dhcp class id.
       /showclassid6    Displays all the IPv6 DHCP class IDs allowed for adapter.
       /setclassid6     Modifies the IPv6 DHCP class id.


The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is removed.

Examples:
    > ipconfig                       ... Show information
```



```
Examples:
    > ipconfig                       ... Show information
    > ipconfig /all                  ... Show detailed information
    > ipconfig /renew                ... renew all adapters
    > ipconfig /renew EL*            ... renew any connection that has its
                                         name starting with EL
    > ipconfig /release *Con*        ... release all matching connections,
                                         eg. "Wired Ethernet Connection 1" or
                                             "Wired Ethernet Connection 2"
    > ipconfig /allcompartments      ... Show information about all
                                         compartments
    > ipconfig /allcompartments /all ... Show detailed information about all
                                         compartments

C:\Users\coral>
```

2. What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu? Include a Wireshark screenshot to justify your answers. *2 points*

   As shown in the Wireshark screenshot below, the IP address of my client computer is **192.168.88.30**, and the TCP port number used is **60675**. These values are found in the packet details under the **Internet Protocol Version 4** section (Source field) and the **Transmission Control Protocol** section (Source Port field). The server's IP address is **128.119.245.12**, and it is communicating on port **80** (Destination Port).



ip.addr == 128.119.245.12 && tcp.port == 80

```
No.     Time        Source          Destination      Protocol   Lengtl Info
     72 3.314957    192.168.88.30   128.119.245.12   TCP            66 60675 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
```

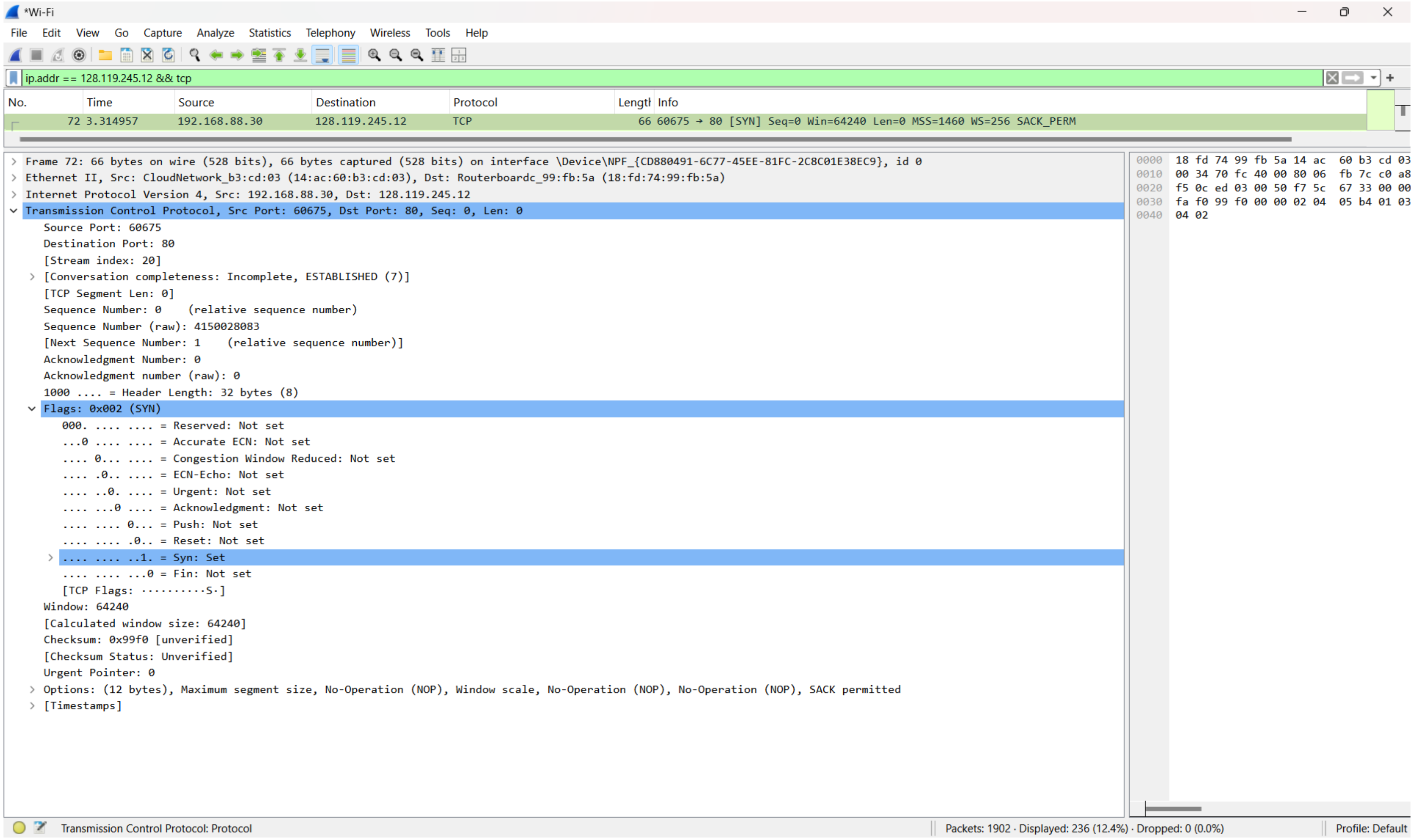
```
> Frame 72: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{CD880491-6C77-45EE-81FC-2C8C01E38EC9}, id 0
> Ethernet II, Src: CloudNetwork_b3:cd:03 (14:ac:60:b3:cd:03), Dst: Routerboardc_99:fb:5a (18:fd:74:99:fb:5a)
v Internet Protocol Version 4, Src: 192.168.88.30, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x70fc (28924)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0xfb7c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.88.30
    Destination Address: 128.119.245.12
    [Stream index: 13]
v Transmission Control Protocol, Src Port: 60675, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 60675
    Destination Port: 80
    [Stream index: 20]
  > [Conversation completeness: Incomplete, ESTABLISHED (7)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 4150028083
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0x99f0 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
  > [Timestamps]
```

```
0000  18 fd 74 99 fb 5a 14 ac  60 b3 cd 03
0010  00 34 70 fc 40 00 80 06  fb 7c c0 a8
0020  f5 0c ed 03 00 50 f7 5c  67 33 00 00
0030  fa f0 99 f0 00 00 02 04  05 b4 01 03
0040  04 02
```

wireshark_Wi-FiW0KCY2.pcapng | Packets: 1902 · Displayed: 236 (12.4%) · Dropped: 0 (0.0%) | Profile: Default

3. What is the real sequence number, in hex, of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment? Include a Wireshark screenshot to justify your answers. *2 points*

As shown in the Wireshark screenshot below, the real sequence number of the TCP SYN segment used to initiate the connection is **0x415028083**. This value is found in the "Sequence Number (raw)" field under the **Transmission Control Protocol** section in the packet details.
The SYN segment is identified by the Flags field, where the SYN flag is set to **1**. This is further indicated by the "Flags: 0x002 (SYN)" field in the packet details.


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

ip.addr == 128.119.245.12 && tcp

```
No.    Time         Source          Destination       Protocol  Lengtl Info
    72 3.314957     192.168.88.30   128.119.245.12    TCP           66 60675 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
```

```
> Frame 72: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{CD880491-6C77-45EE-81FC-2C8C01E38EC9}, id 0
> Ethernet II, Src: CloudNetwork_b3:cd:03 (14:ac:60:b3:cd:03), Dst: Routerboardc_99:fb:5a (18:fd:74:99:fb:5a)
> Internet Protocol Version 4, Src: 192.168.88.30, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 60675, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 60675
    Destination Port: 80
    [Stream index: 20]
  > [Conversation completeness: Incomplete, ESTABLISHED (7)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 4150028083
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  v Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Accurate ECN: Not set
      .... 0... .... = Congestion Window Reduced: 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: 64240
    [Calculated window size: 64240]
    Checksum: 0x99f0 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
  > [Timestamps]
```

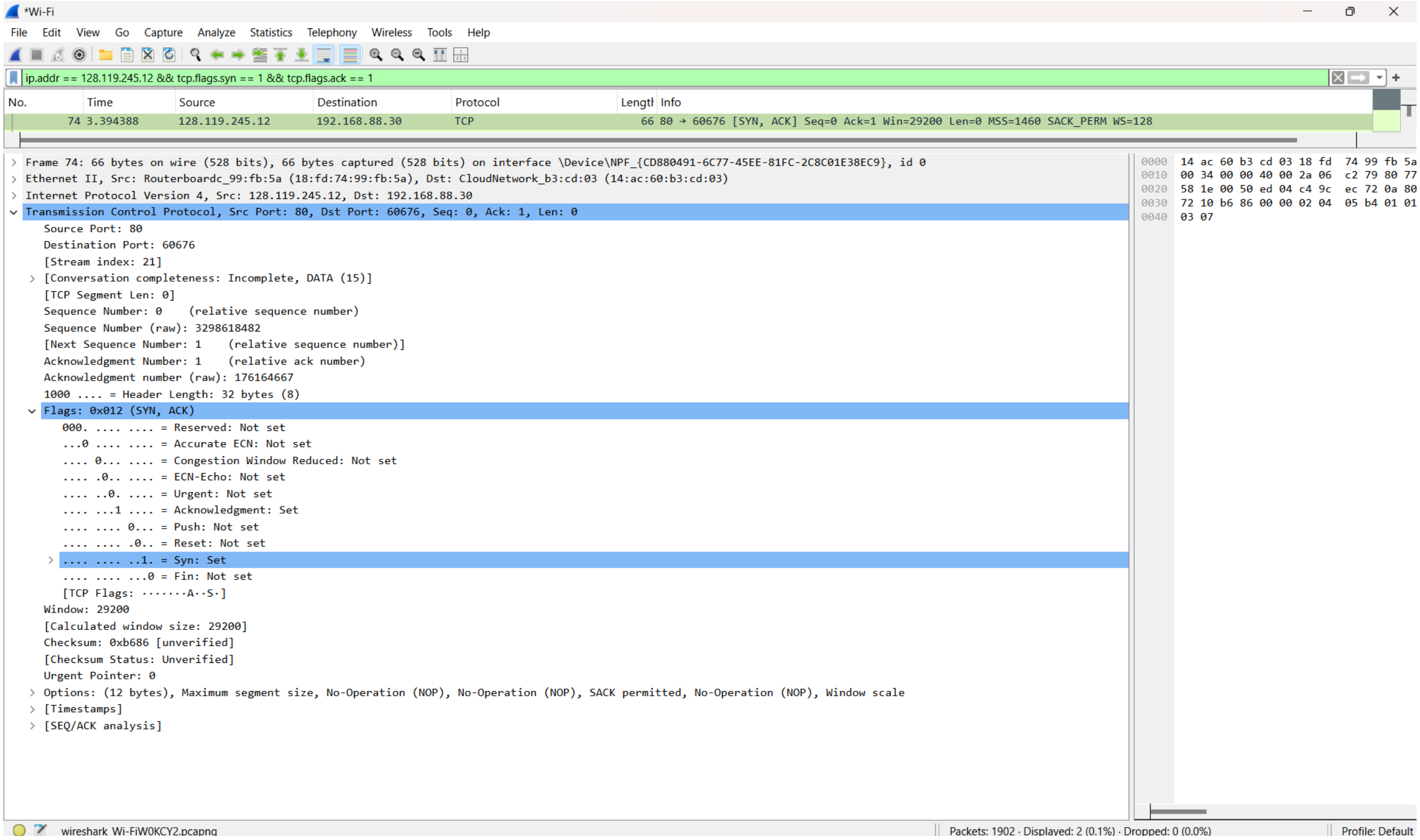
```
0000  18 fd 74 99 fb 5a 14 ac  60 b3 cd 03
0010  00 34 70 fc 40 00 80 06  fb 7c c0 a8
0020  f5 0c ed 03 00 50 f7 5c  67 33 00 00
0030  fa f0 99 f0 00 00 02 04  05 b4 01 03
0040  04 02
```

Transmission Control Protocol: Protocol | Packets: 1902 · Displayed: 236 (12.4%) · Dropped: 0 (0.0%) | Profile: Default

4. What is the real sequence number, in hex, of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the real value, in hex, of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment? Include Wireshark screenshot(s) to justify your answers. *4 points*

As shown in the Wireshark screenshot below, the real sequence number of the SYN-ACK segment sent by the server is **0xc43216b2**. The real value of the Acknowledgment field is **0x415028084**, which is calculated as the client's initial sequence number (**0x415028083**) plus 1.

The SYN-ACK segment is identified by the **Flags** field, where both SYN and ACK flags are set (0x012). These values are highlighted in the Wireshark screenshot below.


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

```
ip.addr == 128.119.245.12 && tcp.flags.syn == 1 && tcp.flags.ack == 1
```

```
No.   Time       Source          Destination    Protocol  Lengtl Info
   74 3.394388   128.119.245.12  192.168.88.30  TCP          66 80 → 60676 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
```

```
> Frame 74: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{CD880491-6C77-45EE-81FC-2C8C01E38EC9}, id 0
> Ethernet II, Src: Routerboardc_99:fb:5a (18:fd:74:99:fb:5a), Dst: CloudNetwork_b3:cd:03 (14:ac:60:b3:cd:03)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.88.30
v Transmission Control Protocol, Src Port: 80, Dst Port: 60676, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 60676
    [Stream index: 21]
  > [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 3298618482
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 176164667
    1000 .... = Header Length: 32 bytes (8)
  v Flags: 0x012 (SYN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Accurate ECN: Not set
      .... 0... .... = Congestion Window Reduced: Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    > .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······A··S·]
    Window: 29200
    [Calculated window size: 29200]
    Checksum: 0xb686 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale
  > [Timestamps]
  > [SEQ/ACK analysis]
```

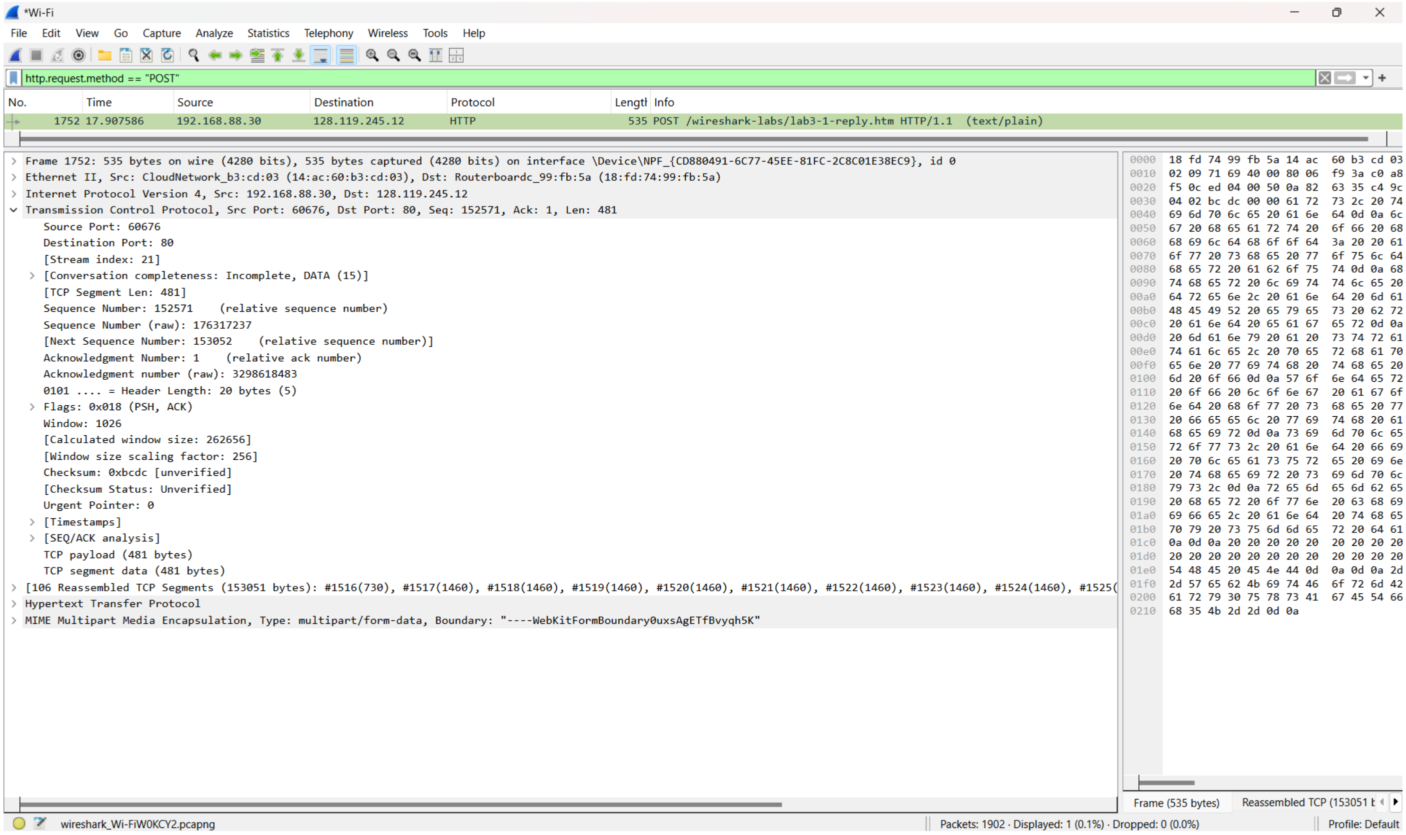
```
0000  14 ac 60 b3 cd 03 18 fd  74 99 fb 5a
0010  00 34 00 00 40 00 2a 06  c2 79 80 77
0020  58 1e 00 50 ed 04 c4 9c  ec 72 0a 80
0030  72 10 b6 86 00 00 02 04  05 b4 01 01
0040  03 07
```

```
wireshark_Wi-FiW0KCY2.pcapng    Packets: 1902 · Displayed: 2 (0.1%) · Dropped: 0 (0.0%)    Profile: Default
```

5. What is the real sequence number, in hex, of the TCP segment containing the HTTP POST command? Note that in order 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. Include Wireshark screenshot(s) to justify your answers. *1 point*

   As shown in the Wireshark screenshot below, the real sequence number of the TCP segment containing the HTTP POST command is **0x253f3**. This value is found in the **Sequence Number (raw)** field under the **Transmission Control Protocol** section.

   The content of the packet is verified in the **Packet Bytes** pane, where the ASCII representation includes the "POST" command. These details confirm that this segment contains the HTTP POST command.



http.request.method == "POST"

```
No.    Time         Source          Destination      Protocol   Lengtl Info
  1752 17.907586    192.168.88.30   128.119.245.12   HTTP          535 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1  (text/plain)
```

```
> Frame 1752: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{CD880491-6C77-45EE-81FC-2C8C01E38EC9}, id 0
> Ethernet II, Src: CloudNetwork_b3:cd:03 (14:ac:60:b3:cd:03), Dst: Routerboardc_99:fb:5a (18:fd:74:99:fb:5a)
> Internet Protocol Version 4, Src: 192.168.88.30, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 60676, Dst Port: 80, Seq: 152571, Ack: 1, Len: 481
    Source Port: 60676
    Destination Port: 80
    [Stream index: 21]
  > [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 481]
    Sequence Number: 152571    (relative sequence number)
    Sequence Number (raw): 176317237
    [Next Sequence Number: 153052    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3298618483
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 1026
    [Calculated window size: 262656]
    [Window size scaling factor: 256]
    Checksum: 0xbcdc [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (481 bytes)
    TCP segment data (481 bytes)
> [106 Reassembled TCP Segments (153051 bytes): #1516(730), #1517(1460), #1518(1460), #1519(1460), #1520(1460), #1521(1460), #1522(1460), #1523(1460), #1524(1460), #1525(
> Hypertext Transfer Protocol
> MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "----WebKitFormBoundary0uxsAgETfBvyqh5K"
```

```
0000  18 fd 74 99 fb 5a 14 ac  60 b3 cd 03
0010  02 09 71 69 40 00 80 06  f9 3a c0 a8
0020  f5 0c ed 04 00 50 0a 82  63 35 c4 9c
0030  04 02 bc dc 00 00 61 72  73 2c 20 74
0040  69 6d 70 6c 65 20 61 6e  64 0d 0a 6c
0050  67 20 68 65 61 72 74 20  6f 66 20 68
0060  68 69 6c 64 68 6f 6f 64  3a 20 20 61
0070  6f 77 20 73 68 65 20 77  6f 75 6c 64
0080  68 65 72 20 61 62 6f 75  74 0d 0a 68
0090  74 68 65 72 20 6c 69 74  74 6c 65 20
00a0  64 72 65 6e 2c 20 61 6e  64 20 6d 61
00b0  48 45 49 52 20 65 79 65  73 20 62 72
00c0  20 61 6e 64 20 65 61 67  65 72 0d 0a
00d0  20 6d 61 6e 79 20 61 20  73 74 72 61
00e0  74 61 6c 65 2c 20 70 65  72 68 61 70
00f0  65 6e 20 77 69 74 68 20  74 68 65 20
0100  6d 20 6f 66 0d 0a 57 6f  6e 64 65 72
0110  20 6f 66 20 6c 6f 6e 67  20 61 67 6f
0120  6e 64 20 68 6f 77 20 73  68 65 20 77
0130  20 66 65 65 6c 20 77 69  74 68 20 61
0140  68 65 69 72 0d 0a 73 69  6d 70 6c 65
0150  72 6f 77 73 2c 20 61 6e  64 20 66 69
0160  20 70 6c 65 61 73 75 72  65 20 69 6e
0170  20 74 68 65 69 72 20 73  69 6d 70 6c
0180  79 73 2c 0d 0a 72 65 6d  65 6d 62 65
0190  20 68 65 72 20 6f 77 6e  20 63 68 69
01a0  69 66 65 2c 20 61 6e 64  20 74 68 65
01b0  70 79 20 73 75 6d 6d 65  72 20 64 61
01c0  0a 0d 0a 20 20 20 20 20  20 20 20 20
01d0  20 20 20 20 20 20 20 20  20 20 20 20
01e0  54 48 45 20 45 4e 44 0d  0a 0d 0a 2d
01f0  2d 57 65 62 4b 69 74 46  6f 72 6d 42
0200  61 72 79 30 75 78 73 41  67 45 54 66
0210  68 35 4b 2d 2d 0d 0a
```

wireshark_Wi-FiW0KCY2.pcapng

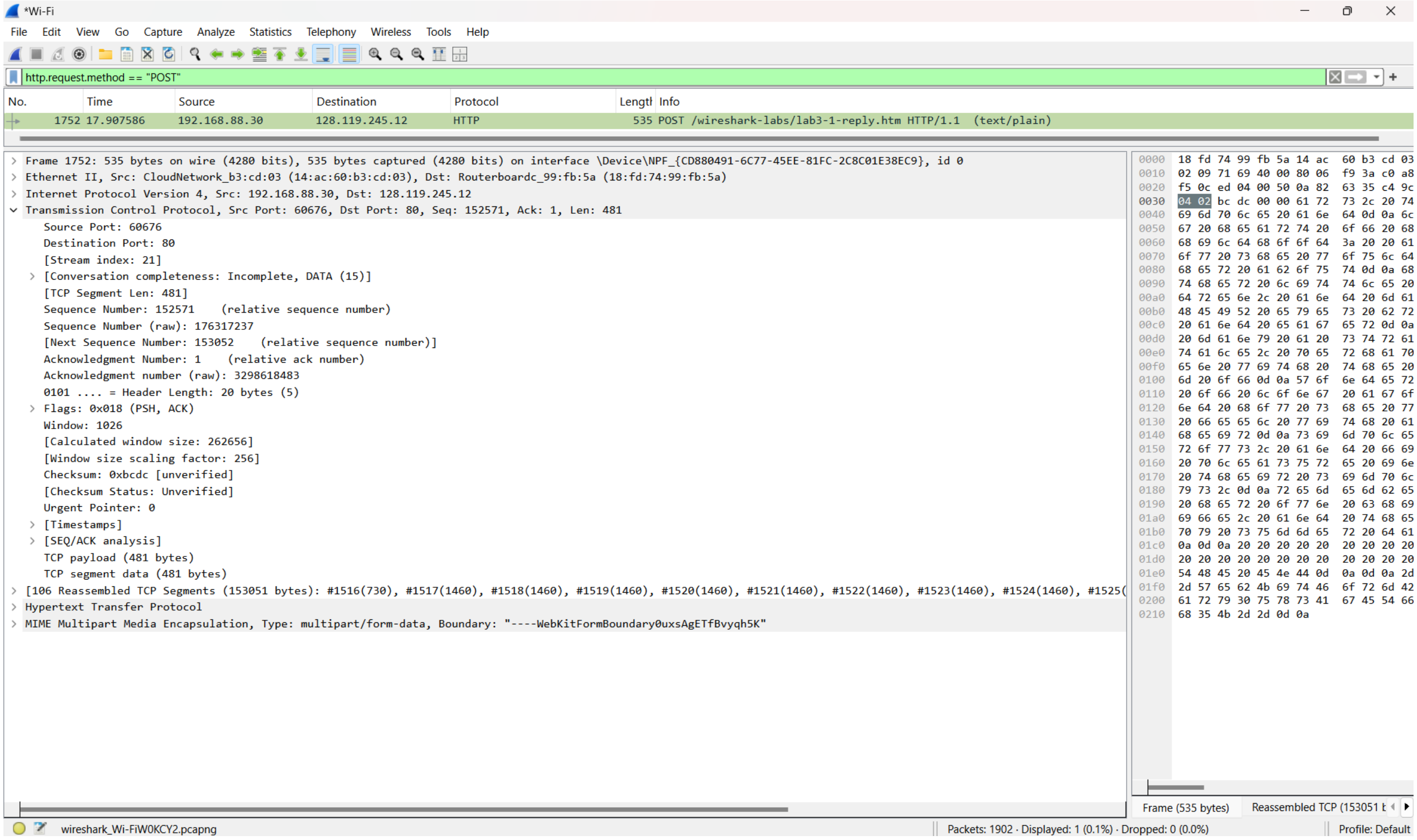
Packets: 1902 · Displayed: 1 (0.1%) · Dropped: 0 (0.0%)

Profile: Default

6. What is the length, in bytes, of the TCP segment containing the HTTP POST command? Include Wireshark screenshot(s) to justify your answers. *1 point*

   As shown in the Wireshark screenshot below, the length of the TCP segment containing the HTTP POST command is **481 bytes**. This value is found in the **TCP payload (481 bytes)** field under the **Transmission Control Protocol** section.

   The length is also confirmed by the raw data displayed in the **Packet Bytes** pane, which corresponds to the payload size. These details highlight the size of the TCP segment carrying the HTTP POST command.


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

```
http.request.method == "POST"
```

```
No.        Time         Source          Destination      Protocol    Lengtl Info
    1752 17.907586    192.168.88.30    128.119.245.12   HTTP          535 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1  (text/plain)
```

```
> Frame 1752: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{CD880491-6C77-45EE-81FC-2C8C01E38EC9}, id 0
> Ethernet II, Src: CloudNetwork_b3:cd:03 (14:ac:60:b3:cd:03), Dst: Routerboardc_99:fb:5a (18:fd:74:99:fb:5a)
> Internet Protocol Version 4, Src: 192.168.88.30, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 60676, Dst Port: 80, Seq: 152571, Ack: 1, Len: 481
     Source Port: 60676
     Destination Port: 80
     [Stream index: 21]
   > [Conversation completeness: Incomplete, DATA (15)]
     [TCP Segment Len: 481]
     Sequence Number: 152571    (relative sequence number)
     Sequence Number (raw): 176317237
     [Next Sequence Number: 153052    (relative sequence number)]
     Acknowledgment Number: 1    (relative ack number)
     Acknowledgment number (raw): 3298618483
     0101 .... = Header Length: 20 bytes (5)
   > Flags: 0x018 (PSH, ACK)
     Window: 1026
     [Calculated window size: 262656]
     [Window size scaling factor: 256]
     Checksum: 0xbcdc [unverified]
     [Checksum Status: Unverified]
     Urgent Pointer: 0
   > [Timestamps]
   > [SEQ/ACK analysis]
     TCP payload (481 bytes)
     TCP segment data (481 bytes)
> [106 Reassembled TCP Segments (153051 bytes): #1516(730), #1517(1460), #1518(1460), #1519(1460), #1520(1460), #1521(1460), #1522(1460), #1523(1460), #1524(1460), #1525(
> Hypertext Transfer Protocol
> MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "----WebKitFormBoundary0uxsAgETfBvyqh5K"
```

```
0000  18 fd 74 99 fb 5a 14 ac  60 b3 cd 03
0010  02 09 71 69 40 00 80 06  f9 3a c0 a8
0020  f5 0c ed 04 00 50 0a 82  63 35 c4 9c
0030  04 02 bc dc 00 00 61 72  73 2c 20 74
0040  69 6d 70 6c 65 20 61 6e  64 0d 0a 6c
0050  67 20 68 65 61 72 74 20  6f 66 20 68
0060  68 69 6c 64 68 6f 6f 64  3a 20 20 61
0070  6f 77 20 73 68 65 20 77  6f 75 6c 64
0080  68 65 72 20 61 62 6f 75  74 0d 0a 68
0090  74 68 65 72 20 6c 69 74  74 6c 65 20
00a0  64 72 65 6e 2c 20 61 6e  64 20 6d 61
00b0  48 45 49 52 20 65 79 65  73 20 62 72
00c0  20 61 6e 64 20 65 61 67  65 72 0d 0a
00d0  20 6d 61 6e 79 20 61 20  73 74 72 61
00e0  74 61 6c 65 2c 20 70 65  72 68 61 70
00f0  65 6e 20 77 69 74 68 20  74 68 65 20
0100  6d 20 6f 66 0d 0a 57 6f  6e 64 65 72
0110  20 6f 66 20 6c 6f 6e 67  20 61 67 6f
0120  6e 64 20 68 6f 77 20 73  68 65 20 77
0130  20 66 65 65 6c 20 77 69  74 68 20 61
0140  68 65 69 72 0d 0a 73 69  6d 70 6c 65
0150  72 6f 77 73 2c 20 61 6e  64 20 66 69
0160  20 70 6c 65 61 73 75 72  65 20 69 6e
0170  20 74 68 65 69 72 20 73  69 6d 70 6c
0180  79 73 2c 0d 0a 72 65 6d  65 6d 62 65
0190  20 68 65 72 20 6f 77 6e  20 63 68 69
01a0  69 66 65 2c 20 61 6e 64  20 74 68 65
01b0  70 79 20 73 75 6d 6d 65  72 20 64 61
01c0  0a 0d 0a 20 20 20 20 20  20 20 20 20
01d0  20 20 20 20 20 20 20 20  20 20 20 20
01e0  54 48 45 20 45 4e 44 0d  0a 0d 0a 2d
01f0  2d 57 65 62 4b 69 74 46  6f 72 6d 42
0200  61 72 79 30 75 78 73 41  67 45 54 66
0210  68 35 4b 2d 2d 0d 0a
```

```
wireshark_Wi-FiW0KCY2.pcapng    Packets: 1902 · Displayed: 1 (0.1%) · Dropped: 0 (0.0%)    Profile: Default
```