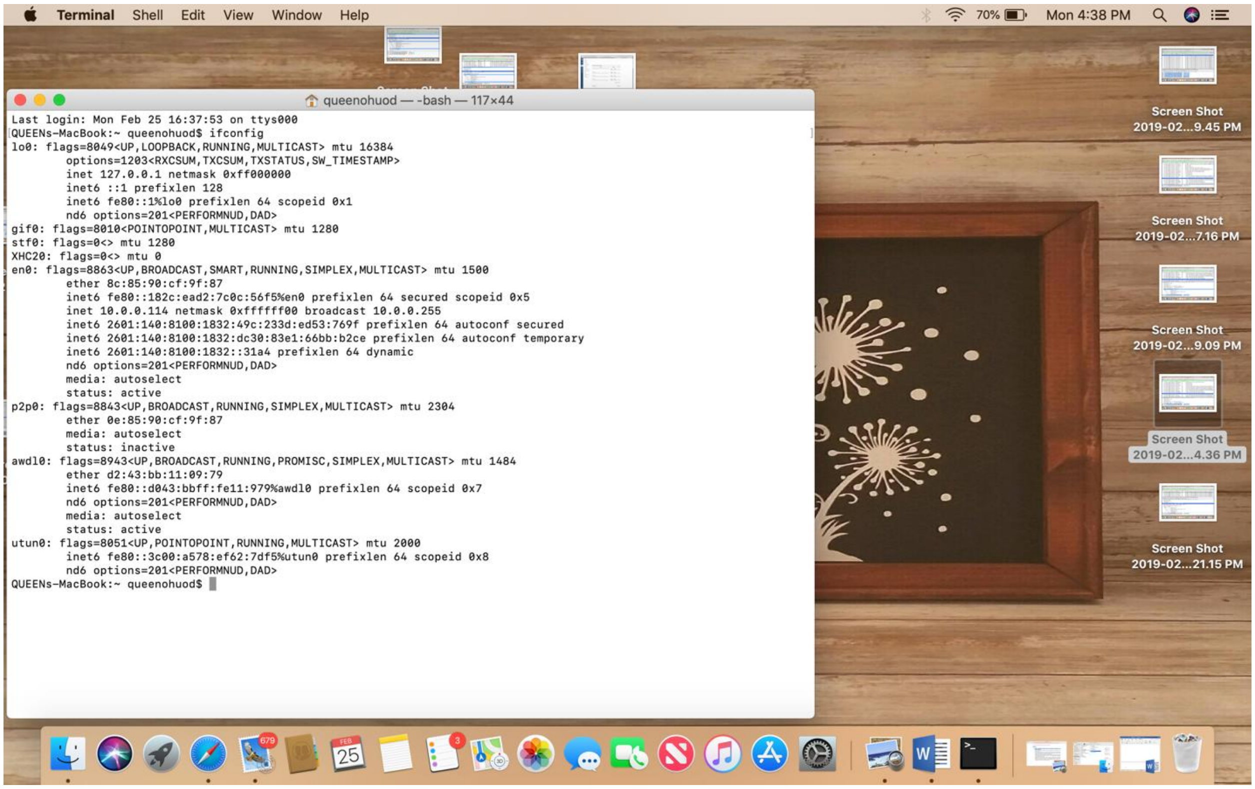
Enterprise Infrastructure & Networks

IT 520

LAB#3

OHUOD ALTHIYABI


Terminal
Shell
Edit
View
Window
Help
70%
Mon 4:38 PM
queenohuod — -bash — 117×44
Screen Shot 2019-02...9.45 PM
Screen Shot 2019-02...7.16 PM
Screen Shot 2019-02...9.09 PM
Screen Shot 2019-02...4.36 PM
Screen Shot 2019-02...21.15 PM

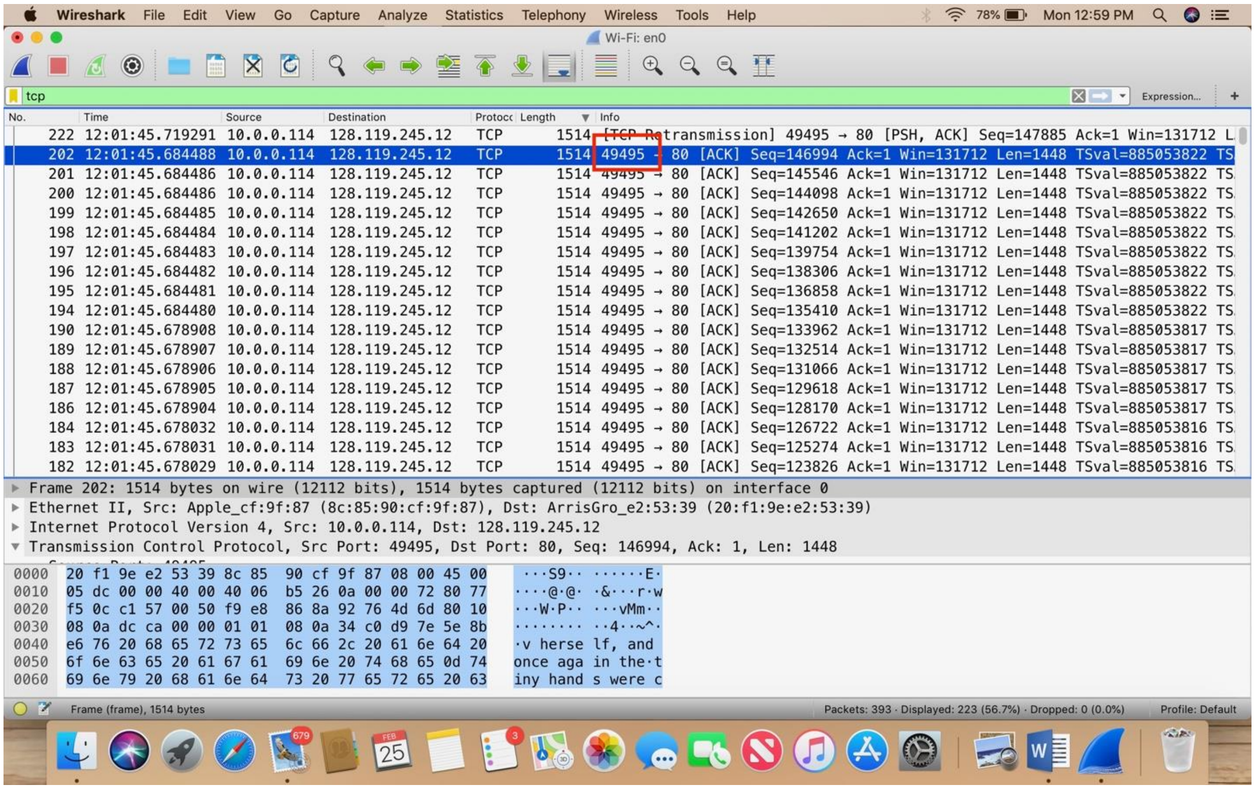
```
Last login: Mon Feb 25 16:37:53 on ttys000
QUEENs-MacBook:~ queenohuod$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
XHC20: flags=0<> mtu 0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 8c:85:90:cf:9f:87
        inet6 fe80::182c:ead2:7c0c:56f5%en0 prefixlen 64 secured scopeid 0x5
        inet 10.0.0.114 netmask 0xffffff00 broadcast 10.0.0.255
        inet6 2601:140:8100:1832:49c:233d:ed53:769f prefixlen 64 autoconf secured
        inet6 2601:140:8100:1832:dc30:83e1:66bb:b2ce prefixlen 64 autoconf temporary
        inet6 2601:140:8100:1832::31a4 prefixlen 64 dynamic
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
        ether 0e:85:90:cf:9f:87
        media: autoselect
        status: inactive
awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1484
        ether d2:43:bb:11:09:79
        inet6 fe80::d043:bbff:fe11:979%awdl0 prefixlen 64 scopeid 0x7
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
        inet6 fe80::3c00:a578:ef62:7df5%utun0 prefixlen 64 scopeid 0x8
        nd6 options=201<PERFORMNUD,DAD>
QUEENs-MacBook:~ queenohuod$ 
```

10.0.0.114

Questions:

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

49495


Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
78% Mon 12:59 PM
Wi-Fi: en0
Expression...
+

```
tcp
```

```
No.   Time            Source      Destination     Protocol Length  Info
  222 12:01:45.719291 10.0.0.114  128.119.245.12  TCP      1514 [TCP Retransmission] 49495 → 80 [PSH, ACK] Seq=147885 Ack=1 Win=131712 L
  202 12:01:45.684488 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=146994 Ack=1 Win=131712 Len=1448 TSval=885053822 TS
  201 12:01:45.684486 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=145546 Ack=1 Win=131712 Len=1448 TSval=885053822 TS
  200 12:01:45.684486 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=144098 Ack=1 Win=131712 Len=1448 TSval=885053822 TS
  199 12:01:45.684485 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=142650 Ack=1 Win=131712 Len=1448 TSval=885053822 TS
  198 12:01:45.684484 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=141202 Ack=1 Win=131712 Len=1448 TSval=885053822 TS
  197 12:01:45.684483 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=139754 Ack=1 Win=131712 Len=1448 TSval=885053822 TS
  196 12:01:45.684482 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=138306 Ack=1 Win=131712 Len=1448 TSval=885053822 TS
  195 12:01:45.684481 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=136858 Ack=1 Win=131712 Len=1448 TSval=885053822 TS
  194 12:01:45.684480 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=135410 Ack=1 Win=131712 Len=1448 TSval=885053822 TS
  190 12:01:45.678908 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=133962 Ack=1 Win=131712 Len=1448 TSval=885053817 TS
  189 12:01:45.678907 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=132514 Ack=1 Win=131712 Len=1448 TSval=885053817 TS
  188 12:01:45.678906 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=131066 Ack=1 Win=131712 Len=1448 TSval=885053817 TS
  187 12:01:45.678905 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=129618 Ack=1 Win=131712 Len=1448 TSval=885053817 TS
  186 12:01:45.678904 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=128170 Ack=1 Win=131712 Len=1448 TSval=885053817 TS
  184 12:01:45.678032 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=126722 Ack=1 Win=131712 Len=1448 TSval=885053816 TS
  183 12:01:45.678031 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=125274 Ack=1 Win=131712 Len=1448 TSval=885053816 TS
  182 12:01:45.678029 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=123826 Ack=1 Win=131712 Len=1448 TSval=885053816 TS
```

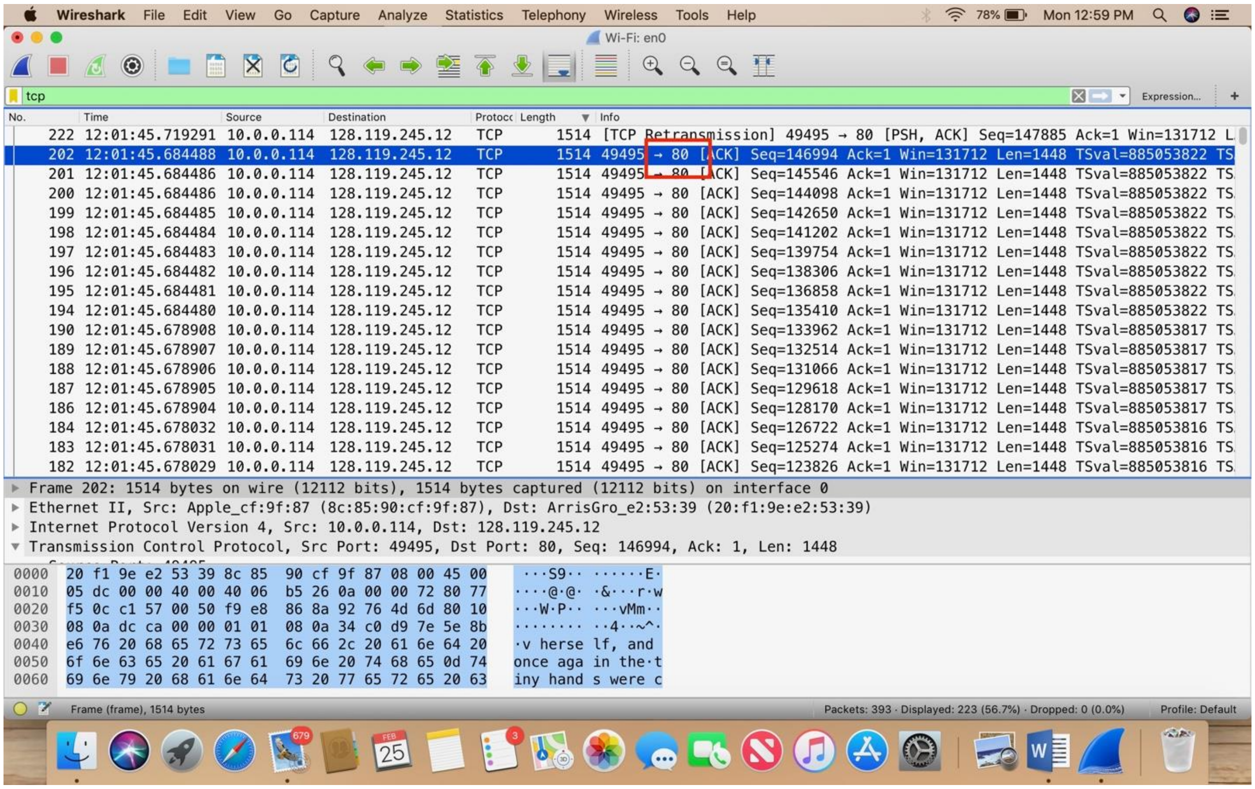
```
▶ Frame 202: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▶ Ethernet II, Src: Apple_cf:9f:87 (8c:85:90:cf:9f:87), Dst: ArrisGro_e2:53:39 (20:f1:9e:e2:53:39)
▶ Internet Protocol Version 4, Src: 10.0.0.114, Dst: 128.119.245.12
▼ Transmission Control Protocol, Src Port: 49495, Dst Port: 80, Seq: 146994, Ack: 1, Len: 1448
```

```
0000  20 f1 9e e2 53 39 8c 85  90 cf 9f 87 08 00 45 00    ···S9·· ······E·
0010  05 dc 00 00 40 00 40 06  b5 26 0a 00 00 72 80 77   ····@·@· ·&···r·w
0020  f5 0c c1 57 00 50 f9 e8  86 8a 92 76 4d 6d 80 10   ···W·P·· ···vMm··
0030  08 0a dc ca 00 00 01 01  08 0a 34 c0 d9 7e 5e 8b   ········ ··4··~^·
0040  e6 76 20 68 65 72 73 65  6c 66 2c 20 61 6e 64 20   ·v herse lf, and 
0050  6f 6e 63 65 20 61 67 61  69 6e 20 74 68 65 0d 74   once aga in the·t
0060  69 6e 79 20 68 61 6e 64  73 20 77 65 72 65 20 63   iny hand s were c
```

```
Frame (frame), 1514 bytes          Packets: 393 · Displayed: 223 (56.7%) · Dropped: 0 (0.0%)          Profile: Default
```

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

80



tcp

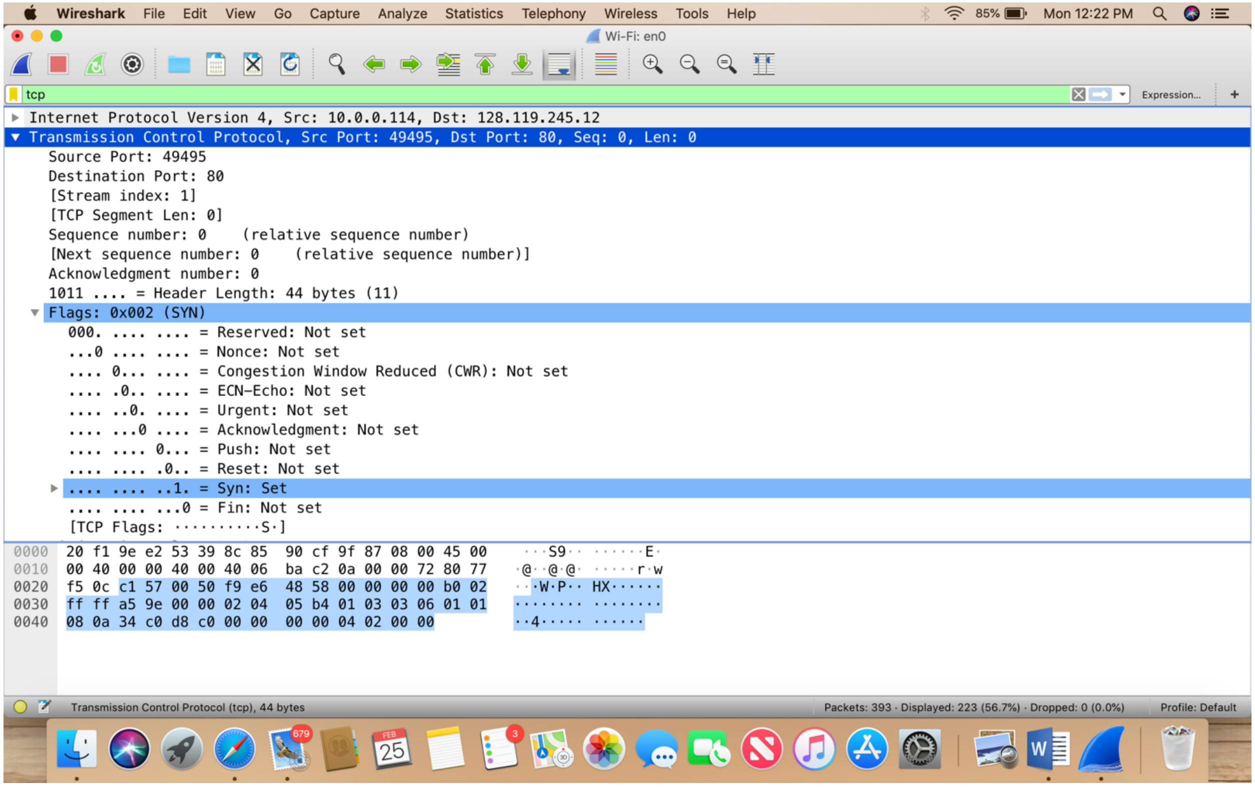
```
No.   Time             Source      Destination     Protocol Length Info
  222 12:01:45.719291 10.0.0.114  128.119.245.12  TCP      1514 [TCP Retransmission] 49495 → 80 [PSH, ACK] Seq=147885 Ack=1 Win=131712 L
  202 12:01:45.684488 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=146994 Ack=1 Win=131712 Len=1448 TSval=885053822 TS
  201 12:01:45.684486 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=145546 Ack=1 Win=131712 Len=1448 TSval=885053822 TS
  200 12:01:45.684486 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=144098 Ack=1 Win=131712 Len=1448 TSval=885053822 TS
  199 12:01:45.684485 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=142650 Ack=1 Win=131712 Len=1448 TSval=885053822 TS
  198 12:01:45.684484 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=141202 Ack=1 Win=131712 Len=1448 TSval=885053822 TS
  197 12:01:45.684483 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=139754 Ack=1 Win=131712 Len=1448 TSval=885053822 TS
  196 12:01:45.684482 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=138306 Ack=1 Win=131712 Len=1448 TSval=885053822 TS
  195 12:01:45.684481 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=136858 Ack=1 Win=131712 Len=1448 TSval=885053822 TS
  194 12:01:45.684480 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=135410 Ack=1 Win=131712 Len=1448 TSval=885053822 TS
  190 12:01:45.678908 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=133962 Ack=1 Win=131712 Len=1448 TSval=885053817 TS
  189 12:01:45.678907 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=132514 Ack=1 Win=131712 Len=1448 TSval=885053817 TS
  188 12:01:45.678906 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=131066 Ack=1 Win=131712 Len=1448 TSval=885053817 TS
  187 12:01:45.678905 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=129618 Ack=1 Win=131712 Len=1448 TSval=885053817 TS
  186 12:01:45.678904 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=128170 Ack=1 Win=131712 Len=1448 TSval=885053817 TS
  184 12:01:45.678032 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=126722 Ack=1 Win=131712 Len=1448 TSval=885053816 TS
  183 12:01:45.678031 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=125274 Ack=1 Win=131712 Len=1448 TSval=885053816 TS
  182 12:01:45.678029 10.0.0.114  128.119.245.12  TCP      1514 49495 → 80 [ACK] Seq=123826 Ack=1 Win=131712 Len=1448 TSval=885053816 TS
```

```
▶ Frame 202: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▶ Ethernet II, Src: Apple_cf:9f:87 (8c:85:90:cf:9f:87), Dst: ArrisGro_e2:53:39 (20:f1:9e:e2:53:39)
▶ Internet Protocol Version 4, Src: 10.0.0.114, Dst: 128.119.245.12
▼ Transmission Control Protocol, Src Port: 49495, Dst Port: 80, Seq: 146994, Ack: 1, Len: 1448
```

```
0000  20 f1 9e e2 53 39 8c 85  90 cf 9f 87 08 00 45 00    ···S9·· ······E·
0010  05 dc 00 00 40 00 40 06  b5 26 0a 00 00 72 80 77   ····@·@· ·&···r·w
0020  f5 0c c1 57 00 50 f9 e8  86 8a 92 76 4d 6d 80 10   ···W·P·· ···vMm··
0030  08 0a dc ca 00 00 01 01  08 0a 34 c0 d9 7e 5e 8b   ········ ··4··~^·
0040  e6 76 20 68 65 72 73 65  6c 66 2c 20 61 6e 64 20   ·v herse lf, and
0050  6f 6e 63 65 20 61 67 61  69 6e 20 74 68 65 0d 74   once aga in the·t
0060  69 6e 79 20 68 61 6e 64  73 20 77 65 72 65 20 63   iny hand s were c
```

Frame (frame), 1514 bytes   Packets: 393 · Displayed: 223 (56.7%) · 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? What is it in the segment that identifies the segment as a SYN segment?



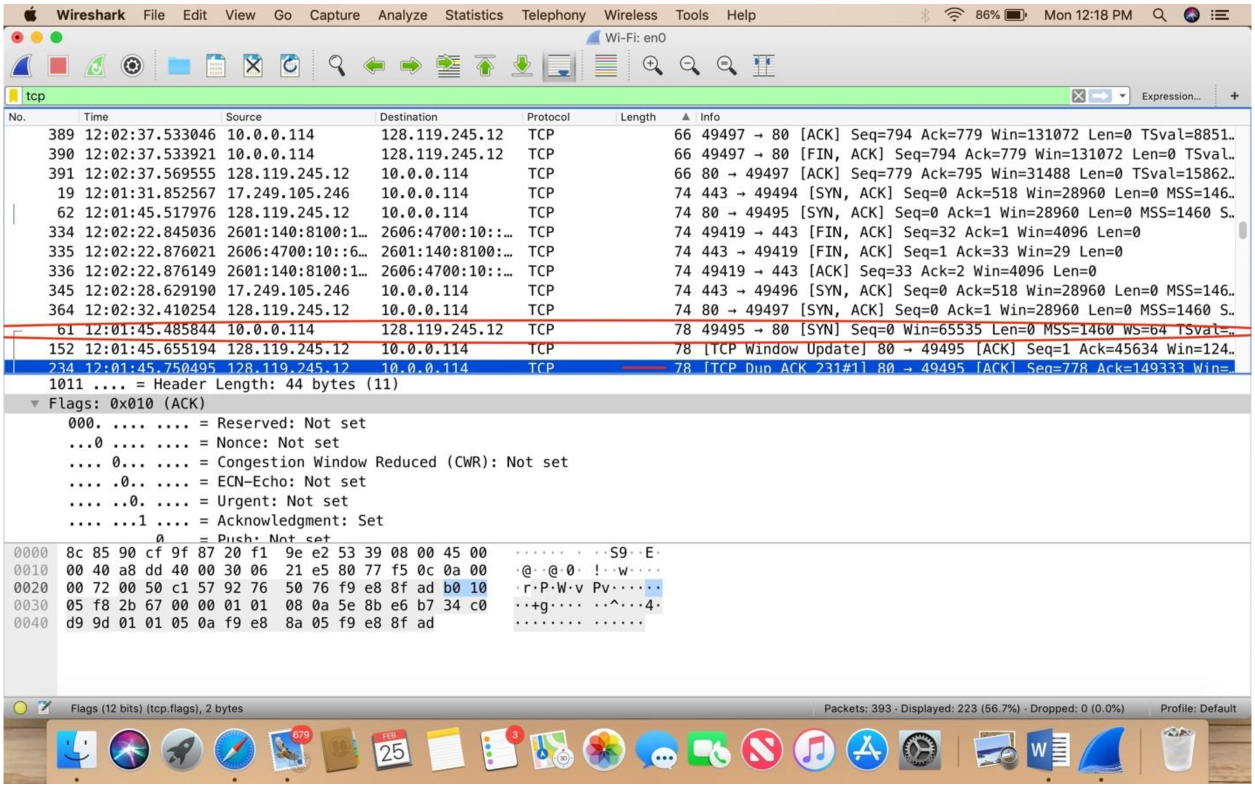
```
▶ Internet Protocol Version 4, Src: 10.0.0.114, Dst: 128.119.245.12
▼ Transmission Control Protocol, Src Port: 49495, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 49495
    Destination Port: 80
    [Stream index: 1]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    1011 .... = Header Length: 44 bytes (11)
  ▼ 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·]
```

```
0000  20 f1 9e e2 53 39 8c 85  90 cf 9f 87 08 00 45 00    ···S9·· ······E·
0010  00 40 00 00 40 00 40 06  ba c2 0a 00 00 72 80 77    ·@··@·@· ·····r·w
0020  f5 0c c1 57 00 50 f9 e6  48 58 00 00 00 00 b0 02    ···W·P·· HX······
0030  ff ff a5 9e 00 00 02 04  05 b4 01 03 03 06 01 01    ········ ········
0040  08 0a 34 c0 d8 c0 00 00  00 00 04 02 00 00          ··4····· ······
```

Transmission Control Protocol (tcp), 44 bytes

Packets: 393 · Displayed: 223 (56.7%) · Dropped: 0 (0.0%)

Profile: Default



```
tcp

No.   Time             Source            Destination       Protocol   Length ▲ Info
  389 12:02:37.533046 10.0.0.114        128.119.245.12    TCP        66 49497 → 80 [ACK] Seq=794 Ack=779 Win=131072 Len=0 TSval=8851…
  390 12:02:37.533921 10.0.0.114        128.119.245.12    TCP        66 49497 → 80 [FIN, ACK] Seq=794 Ack=779 Win=131072 Len=0 TSval…
  391 12:02:37.569555 128.119.245.12    10.0.0.114        TCP        66 80 → 49497 [ACK] Seq=779 Ack=795 Win=31488 Len=0 TSval=15862…
   19 12:01:31.852567 17.249.105.246    10.0.0.114        TCP        74 443 → 49494 [SYN, ACK] Seq=0 Ack=518 Win=28960 Len=0 MSS=146…
   62 12:01:45.517976 128.119.245.12    10.0.0.114        TCP        74 80 → 49495 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 S…
  334 12:02:22.845036 2601:140:8100:1…  2606:4700:10::…   TCP        74 49419 → 443 [FIN, ACK] Seq=32 Ack=1 Win=4096 Len=0
  335 12:02:22.876021 2606:4700:10::6…  2601:140:8100:…   TCP        74 443 → 49419 [FIN, ACK] Seq=1 Ack=33 Win=29 Len=0
  336 12:02:22.876149 2601:140:8100:1…  2606:4700:10::…   TCP        74 49419 → 443 [ACK] Seq=33 Ack=2 Win=4096 Len=0
  345 12:02:28.629190 17.249.105.246    10.0.0.114        TCP        74 443 → 49496 [SYN, ACK] Seq=0 Ack=518 Win=28960 Len=0 MSS=146…
  364 12:02:32.410254 128.119.245.12    10.0.0.114        TCP        74 80 → 49497 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 S…
   61 12:01:45.485844 10.0.0.114        128.119.245.12    TCP        78 49495 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=…
  152 12:01:45.655194 128.119.245.12    10.0.0.114        TCP        78 [TCP Window Update] 80 → 49495 [ACK] Seq=1 Ack=45634 Win=124…
  234 12:01:45.750495 128.119.245.12    10.0.0.114        TCP        78 [TCP Dup ACK 231#1] 80 → 49495 [ACK] Seq=778 Ack=149333 Win=…

    1011 .... = Header Length: 44 bytes (11)
  ▼ Flags: 0x010 (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
      .... .... 0... = Push: Not set

0000  8c 85 90 cf 9f 87 20 f1  9e e2 53 39 08 00 45 00   ·······  ··S9··E·
0010  00 40 a8 dd 40 00 30 06  21 e5 80 77 f5 0c 0a 00   ·@··@·0·  !··w····
0020  00 72 00 50 c1 57 92 76  50 76 f9 e8 8f ad b0 10   ·r·P·W·v  Pv······
0030  05 f8 2b 67 00 00 01 01  08 0a 5e 8b e6 b7 34 c0   ··+g····  ··^···4·
0040  d9 9d 01 01 05 0a f9 e8  8a 05 f9 e8 8f ad         ········  ······

Flags (12 bits) (tcp.flags), 2 bytes          Packets: 393 · Displayed: 223 (56.7%) · Dropped: 0 (0.0%)     Profile: Default
```