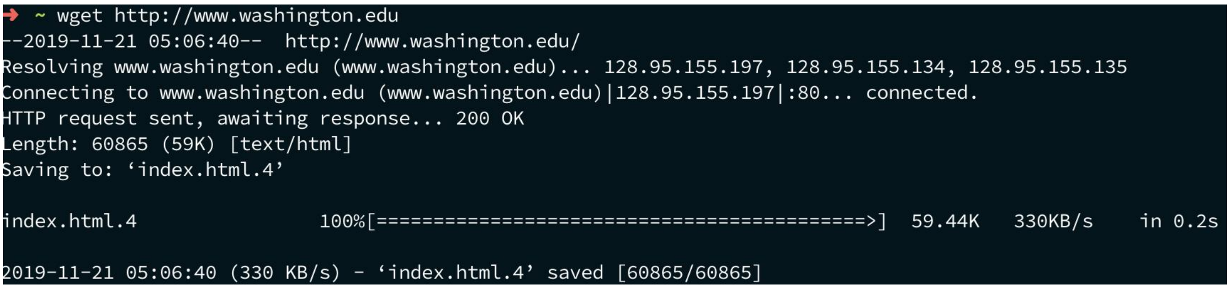
Lab 6 – Yuanjie Yue 11/20/2019

Step 1. Capture a trace

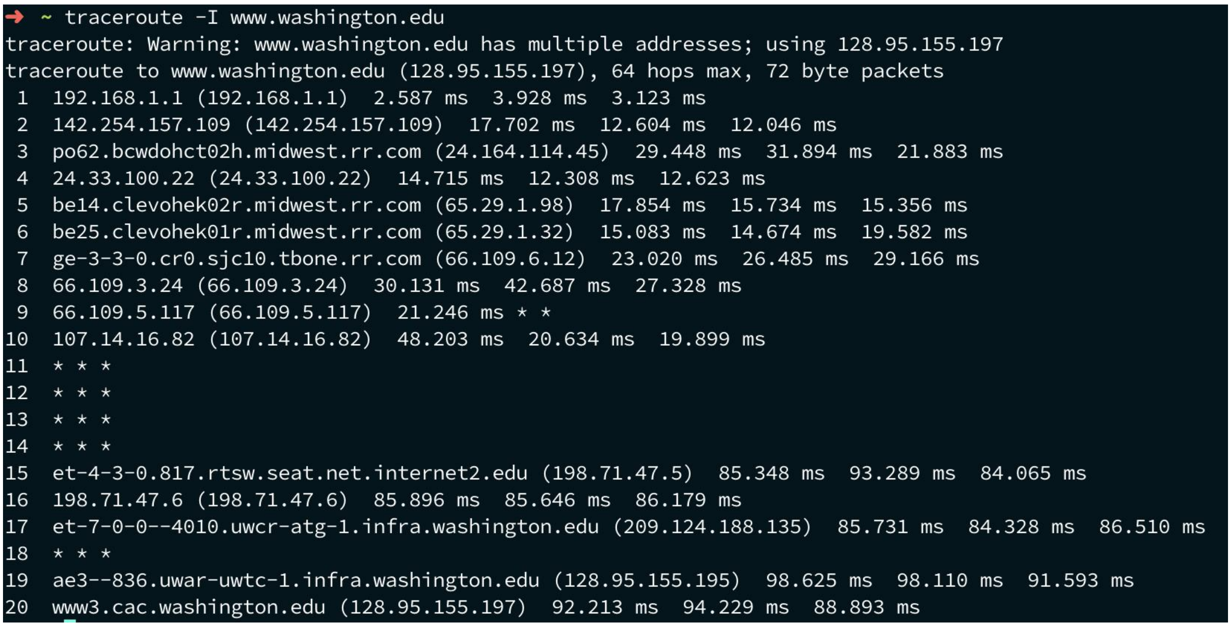
1) Find a URL, I am using this one, http://www.washington.edu

2) Fetch the URL with wget command.



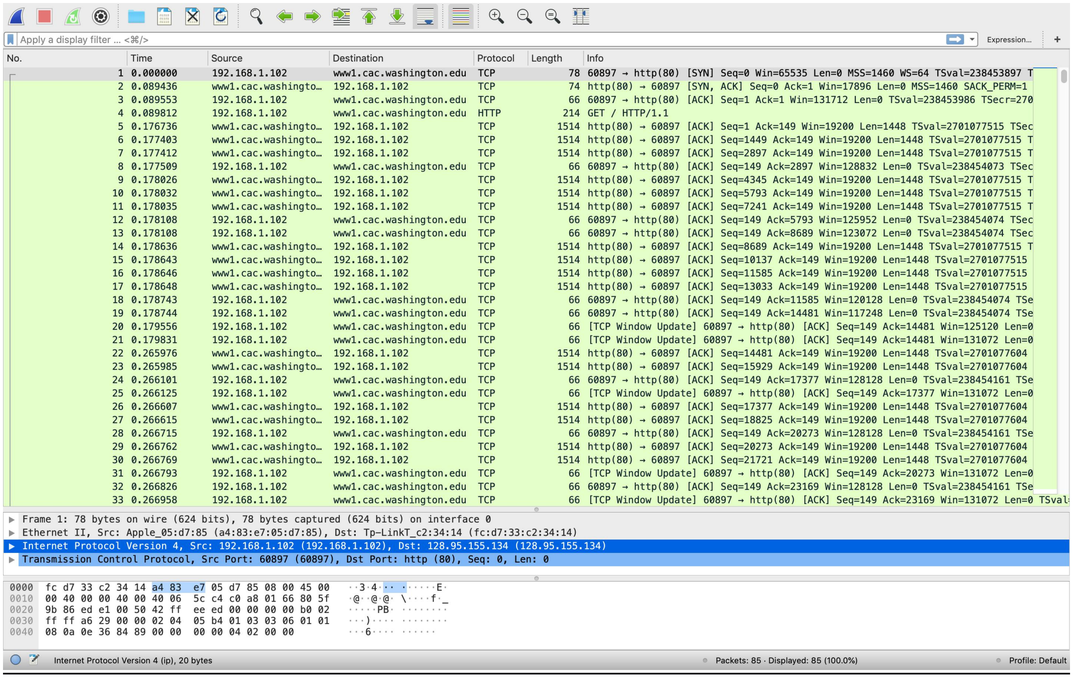
```
➜ ~ wget http://www.washington.edu
--2019-11-21 05:06:40--  http://www.washington.edu/
Resolving www.washington.edu (www.washington.edu)... 128.95.155.197, 128.95.155.134, 128.95.155.135
Connecting to www.washington.edu (www.washington.edu)|128.95.155.197|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 60865 (59K) [text/html]
Saving to: ‘index.html.4’

index.html.4             100%[=========================================>]  59.44K   330KB/s    in 0.2s

2019-11-21 05:06:40 (330 KB/s) - ‘index.html.4’ saved [60865/60865]
```

3) Trace the route using traceroute command



```
➜ ~ traceroute -I www.washington.edu
traceroute: Warning: www.washington.edu has multiple addresses; using 128.95.155.197
traceroute to www.washington.edu (128.95.155.197), 64 hops max, 72 byte packets
 1  192.168.1.1 (192.168.1.1)  2.587 ms  3.928 ms  3.123 ms
 2  142.254.157.109 (142.254.157.109)  17.702 ms  12.604 ms  12.046 ms
 3  po62.bcwdohct02h.midwest.rr.com (24.164.114.45)  29.448 ms  31.894 ms  21.883 ms
 4  24.33.100.22 (24.33.100.22)  14.715 ms  12.308 ms  12.623 ms
 5  be14.clevohek02r.midwest.rr.com (65.29.1.98)  17.854 ms  15.734 ms  15.356 ms
 6  be25.clevohek01r.midwest.rr.com (65.29.1.32)  15.083 ms  14.674 ms  19.582 ms
 7  ge-3-3-0.cr0.sjc10.tbone.rr.com (66.109.6.12)  23.020 ms  26.485 ms  29.166 ms
 8  66.109.3.24 (66.109.3.24)  30.131 ms  42.687 ms  27.328 ms
 9  66.109.5.117 (66.109.5.117)  21.246 ms * *
10  107.14.16.82 (107.14.16.82)  48.203 ms  20.634 ms  19.899 ms
11  * * *
12  * * *
13  * * *
14  * * *
15  et-4-3-0.817.rtsw.seat.net.internet2.edu (198.71.47.5)  85.348 ms  93.289 ms  84.065 ms
16  198.71.47.6 (198.71.47.6)  85.896 ms  85.646 ms  86.179 ms
17  et-7-0-0--4010.uwcr-atg-1.infra.washington.edu (209.124.188.135)  85.731 ms  84.328 ms  86.510 ms
18  * * *
19  ae3--836.uwar-uwtc-1.infra.washington.edu (128.95.155.195)  98.625 ms  98.110 ms  91.593 ms
20  www3.cac.washington.edu (128.95.155.197)  92.213 ms  94.229 ms  88.893 ms
```

4) Set up the filter to be ‘tcp port 80’, then repeat the wget command in 2) step.



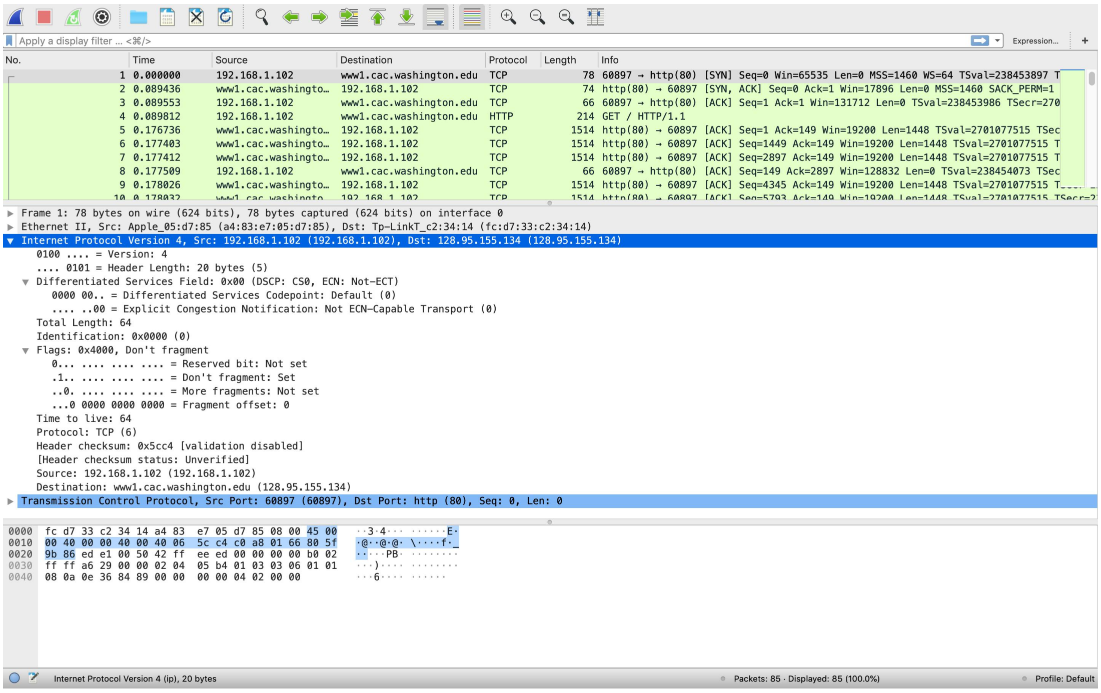
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	www1.cac.washington.edu	TCP	78	60897 → http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=238453897 T
2	0.089436	www1.cac.washingto…	192.168.1.102	TCP	74	http(80) → 60897 [SYN, ACK] Seq=0 Ack=1 Win=17896 Len=0 MSS=1460 SACK_PERM=1
3	0.089553	192.168.1.102	www1.cac.washington.edu	TCP	66	60897 → http(80) [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=238453986 TSecr=270
4	0.089812	192.168.1.102	www1.cac.washington.edu	HTTP	214	GET / HTTP/1.1
5	0.176736	www1.cac.washingto…	192.168.1.102	TCP	1514	http(80) → 60897 [ACK] Seq=1 Ack=149 Win=19200 Len=1448 TSval=2701077515 TSec
6	0.177403	www1.cac.washingto…	192.168.1.102	TCP	1514	http(80) → 60897 [ACK] Seq=1449 Ack=149 Win=19200 Len=1448 TSval=2701077515 T
7	0.177412	www1.cac.washingto…	192.168.1.102	TCP	1514	http(80) → 60897 [ACK] Seq=2897 Ack=149 Win=19200 Len=1448 TSval=2701077515 T
8	0.177509	192.168.1.102	www1.cac.washington.edu	TCP	66	60897 → http(80) [ACK] Seq=149 Ack=2897 Win=128832 Len=0 TSval=238454073 TSec
9	0.178026	www1.cac.washingto…	192.168.1.102	TCP	1514	http(80) → 60897 [ACK] Seq=4345 Ack=149 Win=19200 Len=1448 TSval=2701077515 T
10	0.178032	www1.cac.washingto…	192.168.1.102	TCP	1514	http(80) → 60897 [ACK] Seq=5793 Ack=149 Win=19200 Len=1448 TSval=2701077515 T
11	0.178035	www1.cac.washingto…	192.168.1.102	TCP	1514	http(80) → 60897 [ACK] Seq=7241 Ack=149 Win=19200 Len=1448 TSval=2701077515 T
12	0.178108	192.168.1.102	www1.cac.washington.edu	TCP	66	60897 → http(80) [ACK] Seq=149 Ack=5793 Win=125952 Len=0 TSval=238454074 TSec
13	0.178108	192.168.1.102	www1.cac.washington.edu	TCP	66	60897 → http(80) [ACK] Seq=149 Ack=8689 Win=123072 Len=0 TSval=238454074 TSec
14	0.178636	www1.cac.washingto…	192.168.1.102	TCP	1514	http(80) → 60897 [ACK] Seq=8689 Ack=149 Win=19200 Len=1448 TSval=2701077515 T
15	0.178643	www1.cac.washingto…	192.168.1.102	TCP	1514	http(80) → 60897 [ACK] Seq=10137 Ack=149 Win=19200 Len=1448 TSval=2701077515
16	0.178646	www1.cac.washingto…	192.168.1.102	TCP	1514	http(80) → 60897 [ACK] Seq=11585 Ack=149 Win=19200 Len=1448 TSval=2701077515
17	0.178648	www1.cac.washingto…	192.168.1.102	TCP	1514	http(80) → 60897 [ACK] Seq=13033 Ack=149 Win=19200 Len=1448 TSval=2701077515
18	0.178743	192.168.1.102	www1.cac.washington.edu	TCP	66	60897 → http(80) [ACK] Seq=149 Ack=11585 Win=120128 Len=0 TSval=238454074 TSe
19	0.178744	192.168.1.102	www1.cac.washington.edu	TCP	66	60897 → http(80) [ACK] Seq=149 Ack=14481 Win=117248 Len=0 TSval=238454074 TSe
20	0.179556	192.168.1.102	www1.cac.washington.edu	TCP	66	[TCP Window Update] 60897 → http(80) [ACK] Seq=149 Ack=14481 Win=125120 Len=0
21	0.179831	192.168.1.102	www1.cac.washington.edu	TCP	66	[TCP Window Update] 60897 → http(80) [ACK] Seq=149 Ack=14481 Win=131072 Len=0
22	0.265976	www1.cac.washingto…	192.168.1.102	TCP	1514	http(80) → 60897 [ACK] Seq=14481 Ack=149 Win=19200 Len=1448 TSval=2701077604
23	0.265985	www1.cac.washingto…	192.168.1.102	TCP	1514	http(80) → 60897 [ACK] Seq=15929 Ack=149 Win=19200 Len=1448 TSval=2701077604
24	0.266101	192.168.1.102	www1.cac.washington.edu	TCP	66	60897 → http(80) [ACK] Seq=149 Ack=17377 Win=128128 Len=0 TSval=238454161 TSe
25	0.266125	192.168.1.102	www1.cac.washington.edu	TCP	66	[TCP Window Update] 60897 → http(80) [ACK] Seq=149 Ack=17377 Win=131072 Len=0
26	0.266607	www1.cac.washingto…	192.168.1.102	TCP	1514	http(80) → 60897 [ACK] Seq=17377 Ack=149 Win=19200 Len=1448 TSval=2701077604
27	0.266615	www1.cac.washingto…	192.168.1.102	TCP	1514	http(80) → 60897 [ACK] Seq=18825 Ack=149 Win=19200 Len=1448 TSval=2701077604
28	0.266715	192.168.1.102	www1.cac.washington.edu	TCP	66	60897 → http(80) [ACK] Seq=149 Ack=20273 Win=128128 Len=0 TSval=238454161 TSe
29	0.266762	www1.cac.washingto…	192.168.1.102	TCP	1514	http(80) → 60897 [ACK] Seq=20273 Ack=149 Win=19200 Len=1448 TSval=2701077604
30	0.266769	www1.cac.washingto…	192.168.1.102	TCP	1514	http(80) → 60897 [ACK] Seq=21721 Ack=149 Win=19200 Len=1448 TSval=2701077604
31	0.266793	192.168.1.102	www1.cac.washington.edu	TCP	66	[TCP Window Update] 60897 → http(80) [ACK] Seq=149 Ack=20273 Win=131072 Len=0
32	0.266826	192.168.1.102	www1.cac.washington.edu	TCP	66	60897 → http(80) [ACK] Seq=149 Ack=23169 Win=128128 Len=0 TSval=238454161 TSe
33	0.266958	192.168.1.102	www1.cac.washington.edu	TCP	66	[TCP Window Update] 60897 → http(80) [ACK] Seq=149 Ack=23169 Win=131072 Len=0 TSval

```
▶ Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
▶ Ethernet II, Src: Apple_05:d7:85 (a4:83:e7:05:d7:85), Dst: Tp-LinkT_c2:34:14 (fc:d7:33:c2:34:14)
▶ Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 128.95.155.134 (128.95.155.134)
▶ Transmission Control Protocol, Src Port: 60897 (60897), Dst Port: http (80), Seq: 0, Len: 0
```

```
0000  fc d7 33 c2 34 14 a4 83  e7 05 d7 85 08 00 45 00   ··3·4··· ······E·
0010  00 40 00 00 40 00 40 06  5c c4 c0 a8 01 66 80 5f   ·@··@·@· \····f·_
0020  9b 86 ed e1 00 50 42 ff  ee ed 00 00 00 00 b0 02   ·····PB· ········
0030  ff ff a6 29 00 00 02 04  05 b4 01 03 03 06 01 01   ···)···· ········
0040  08 0a 0e 36 84 89 00 00  00 00 04 02 00 00         ···6···· ······
```

Internet Protocol Version 4 (ip), 20 bytes
Packets: 85 · Displayed: 85 (100.0%)
Profile: Default

Step 2. Inspect the Trace

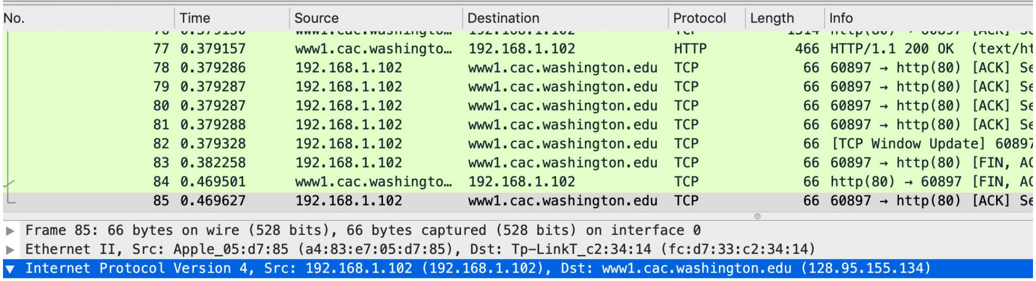


```
No.   Time       Source                Destination            Protocol  Length  Info
    1 0.000000   192.168.1.102         www1.cac.washington.edu TCP       78     60897 → http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=238453897 T
    2 0.089436   www1.cac.washingto…   192.168.1.102          TCP       74     http(80) → 60897 [SYN, ACK] Seq=0 Ack=1 Win=17896 Len=0 MSS=1460 SACK_PERM=1
    3 0.089553   192.168.1.102         www1.cac.washington.edu TCP       66     60897 → http(80) [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=238453986 TSecr=270
    4 0.089812   192.168.1.102         www1.cac.washington.edu HTTP      214    GET / HTTP/1.1
    5 0.176736   www1.cac.washingto…   192.168.1.102          TCP       1514   http(80) → 60897 [ACK] Seq=1 Ack=149 Win=19200 Len=1448 TSval=2701077515 TSec
    6 0.177403   www1.cac.washingto…   192.168.1.102          TCP       1514   http(80) → 60897 [ACK] Seq=1449 Ack=149 Win=19200 Len=1448 TSval=2701077515 T
    7 0.177412   www1.cac.washingto…   192.168.1.102          TCP       1514   http(80) → 60897 [ACK] Seq=2897 Ack=149 Win=19200 Len=1448 TSval=2701077515 T
    8 0.177509   192.168.1.102         www1.cac.washington.edu TCP       66     60897 → http(80) [ACK] Seq=149 Ack=2897 Win=128832 Len=0 TSval=238454073 TSec
    9 0.178026   www1.cac.washingto…   192.168.1.102          TCP       1514   http(80) → 60897 [ACK] Seq=4345 Ack=149 Win=19200 Len=1448 TSval=2701077515 T
   10 0.178032   www1.cac.washingto…   192.168.1.102          TCP       1514   http(80) → 60897 [ACK] Seq=5793 Ack=149 Win=19200 Len=1448 TSval=2701077515 TSecr=2

▶ Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
▶ Ethernet II, Src: Apple_05:d7:85 (a4:83:e7:05:d7:85), Dst: Tp-LinkT_c2:34:14 (fc:d7:33:c2:34:14)
▼ Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 128.95.155.134 (128.95.155.134)
    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: 64
    Identification: 0x0000 (0)
  ▼ 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: 64
    Protocol: TCP (6)
    Header checksum: 0x5cc4 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102 (192.168.1.102)
    Destination: www1.cac.washington.edu (128.95.155.134)
▶ Transmission Control Protocol, Src Port: 60897 (60897), Dst Port: http (80), Seq: 0, Len: 0

0000  fc d7 33 c2 34 14 a4 83  e7 05 d7 85 08 00 45 00   ··3·4··· ······E·
0010  00 40 00 00 40 00 40 06  5c c4 c0 a8 01 66 80 5f   ·@··@·@· \····f·_
0020  9b 86 ed e1 00 50 42 ff  ee ed 00 00 00 00 b0 02   ·····PB· ········
0030  ff ff a6 29 00 00 02 04  05 b4 01 03 03 06 01 01   ···)···· ········
0040  08 0a 0e 36 84 89 00 00  00 00 04 02 00 00         ···6···· ······

Internet Protocol Version 4 (ip), 20 bytes          Packets: 85 · Displayed: 85 (100.0%)          Profile: Default
```

Step 3. IP Packet Structure

1. What are the IP addresses of your computer and the remote server?

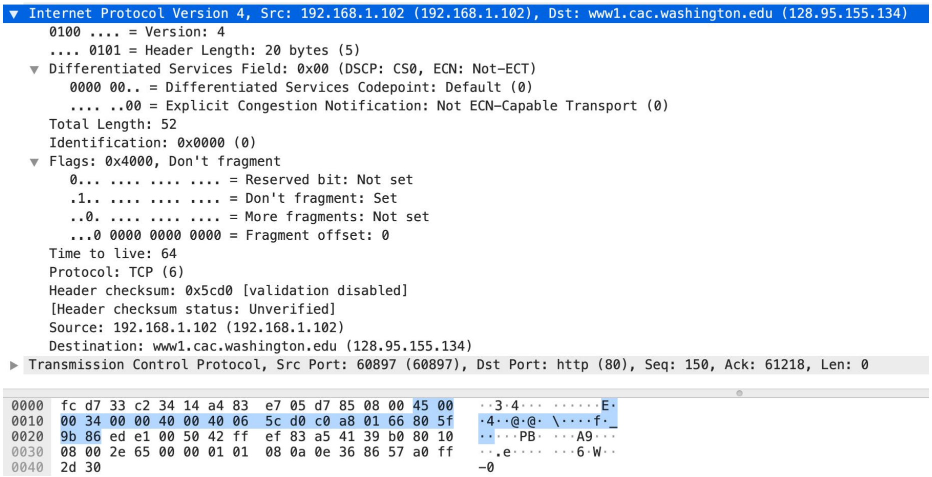
My IP is 192.168.1.102, and the remote server is 128.95.155.134



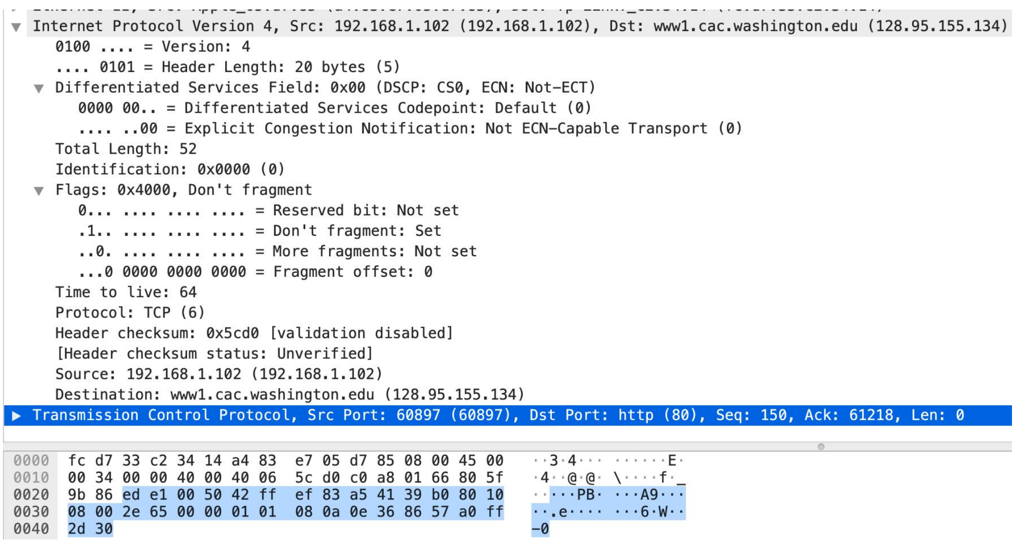
```
No.   Time       Source                Destination              Protocol  Length  Info
   77 0.379157   www1.cac.washingto…   192.168.1.102            HTTP      466     HTTP/1.1 200 OK  (text/ht
   78 0.379286   192.168.1.102         www1.cac.washington.edu  TCP       66      60897 → http(80) [ACK] Se
   79 0.379287   192.168.1.102         www1.cac.washington.edu  TCP       66      60897 → http(80) [ACK] Se
   80 0.379287   192.168.1.102         www1.cac.washington.edu  TCP       66      60897 → http(80) [ACK] Se
   81 0.379288   192.168.1.102         www1.cac.washington.edu  TCP       66      60897 → http(80) [ACK] Se
   82 0.379328   192.168.1.102         www1.cac.washington.edu  TCP       66      [TCP Window Update] 60897
   83 0.382258   192.168.1.102         www1.cac.washington.edu  TCP       66      60897 → http(80) [FIN, AC
   84 0.469501   www1.cac.washingto…   192.168.1.102            TCP       66      http(80) → 60897 [FIN, AC
   85 0.469627   192.168.1.102         www1.cac.washington.edu  TCP       66      60897 → http(80) [ACK] Se

▶ Frame 85: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▶ Ethernet II, Src: Apple_05:d7:85 (a4:83:e7:05:d7:85), Dst: Tp-LinkT_c2:34:14 (fc:d7:33:c2:34:14)
▼ Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: www1.cac.washington.edu (128.95.155.134)
```

2. Does the Total Length field include the IP header plus IP payload, or just the IP payload?

The Total Length field include IP header plus IP payload, as we could see that the current Total Length is 52, which is the sum of the Header Length 20 and payload length 32.



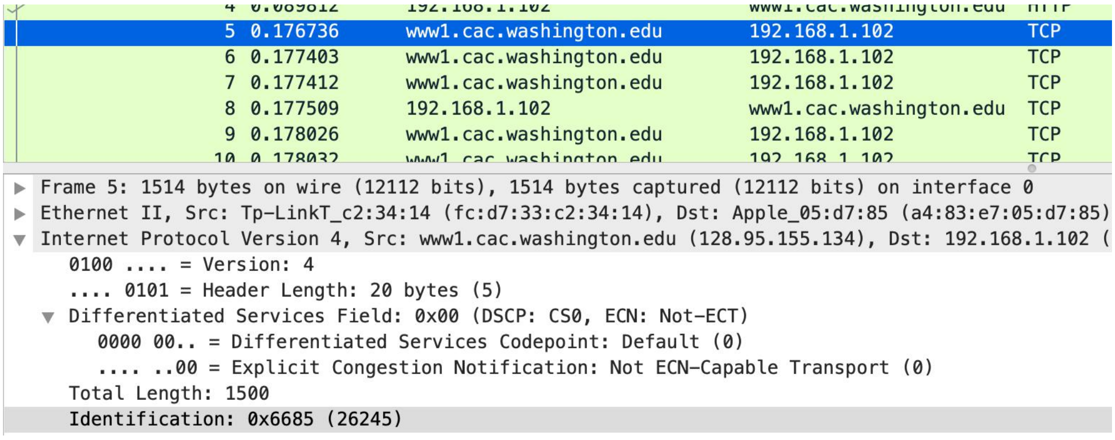
```
▼ Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: www1.cac.washington.edu (128.95.155.134)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 52
    Identification: 0x0000 (0)
  ▼ 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: 64
    Protocol: TCP (6)
    Header checksum: 0x5cd0 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102 (192.168.1.102)
    Destination: www1.cac.washington.edu (128.95.155.134)
▶ Transmission Control Protocol, Src Port: 60897 (60897), Dst Port: http (80), Seq: 150, Ack: 61218, Len: 0

0000  fc d7 33 c2 34 14 a4 83  e7 05 d7 85 08 00 45 00   ··3·4··· ······E·
0010  00 34 00 00 40 00 40 06  5c d0 c0 a8 01 66 80 5f   ·4··@·@· \····f·_
0020  9b 86 ed e1 00 50 42 ff  ef 83 a5 41 39 b0 80 10   ·····PB· ···A9···
0030  08 00 2e 65 00 00 01 01  08 0a 0e 36 86 57 a0 ff   ···.e···· ···6·W··
0040  2d 30                                              -0
```



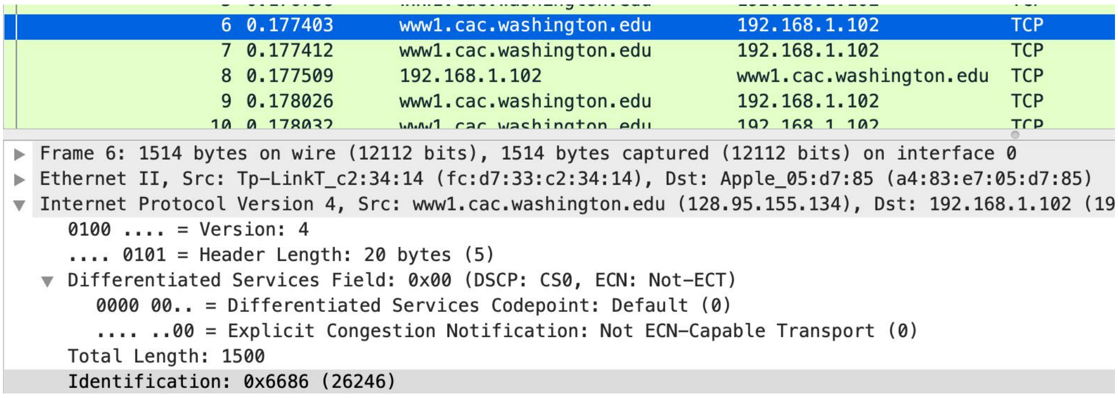
```
▼ Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: www1.cac.washington.edu (128.95.155.134)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 52
    Identification: 0x0000 (0)
  ▼ 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: 64
    Protocol: TCP (6)
    Header checksum: 0x5cd0 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102 (192.168.1.102)
    Destination: www1.cac.washington.edu (128.95.155.134)
▶ Transmission Control Protocol, Src Port: 60897 (60897), Dst Port: http (80), Seq: 150, Ack: 61218, Len: 0

0000  fc d7 33 c2 34 14 a4 83  e7 05 d7 85 08 00 45 00   ··3·4··· ······E·
0010  00 34 00 00 40 00 40 06  5c d0 c0 a8 01 66 80 5f   ·4··@·@· \····f·_
0020  9b 86 ed e1 00 50 42 ff  ef 83 a5 41 39 b0 80 10   ·····PB· ···A9···
0030  08 00 2e 65 00 00 01 01  08 0a 0e 36 86 57 a0 ff   ···e···· ···6·W··
0040  2d 30                                              -0
```

3. How does the value of the Identification field change or stay the same for different packets? For instance, does it hold the same value for all packets in a TCP connection or does it differ for each packet? Is it the same in both directions? Can you see any pattern if the value does change?

Every packet has a different value, and it increase with each ICMP request. We could see that it increase by 1 when new request comes.



```
  4 0.089812  192.168.1.102            www1.cac.washington.edu  HTTP
  5 0.176736  www1.cac.washington.edu  192.168.1.102            TCP
  6 0.177403  www1.cac.washington.edu  192.168.1.102            TCP
  7 0.177412  www1.cac.washington.edu  192.168.1.102            TCP
  8 0.177509  192.168.1.102            www1.cac.washington.edu  TCP
  9 0.178026  www1.cac.washington.edu  192.168.1.102            TCP
 10 0.178032  www1.cac.washington.edu  192.168.1.102            TCP

▶ Frame 5: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▶ Ethernet II, Src: Tp-LinkT_c2:34:14 (fc:d7:33:c2:34:14), Dst: Apple_05:d7:85 (a4:83:e7:05:d7:85)
▼ Internet Protocol Version 4, Src: www1.cac.washington.edu (128.95.155.134), Dst: 192.168.1.102 (
    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: 1500
    Identification: 0x6685 (26245)
```

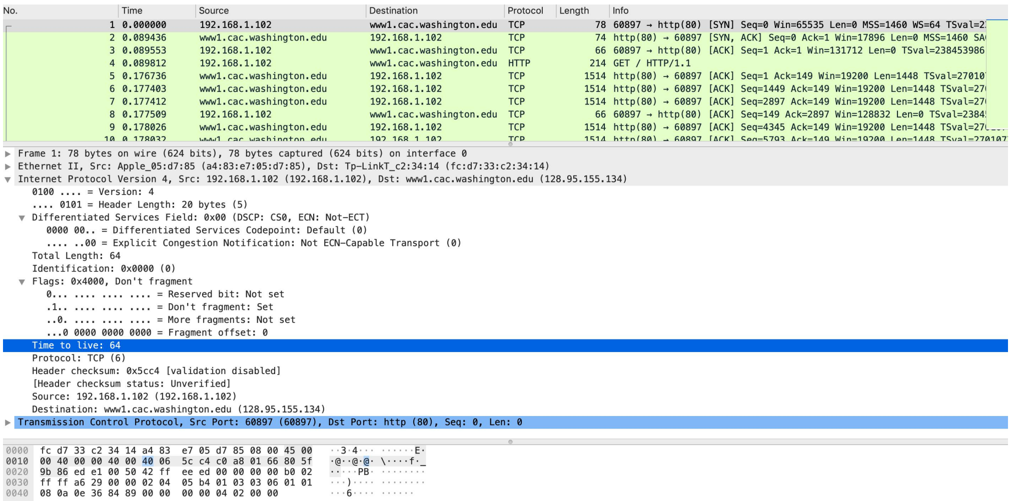


```
  6 0.177403  www1.cac.washington.edu  192.168.1.102            TCP
  7 0.177412  www1.cac.washington.edu  192.168.1.102            TCP
  8 0.177509  192.168.1.102            www1.cac.washington.edu  TCP
  9 0.178026  www1.cac.washington.edu  192.168.1.102            TCP
 10 0.178032  www1.cac.washington.edu  192.168.1.102            TCP

▶ Frame 6: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▶ Ethernet II, Src: Tp-LinkT_c2:34:14 (fc:d7:33:c2:34:14), Dst: Apple_05:d7:85 (a4:83:e7:05:d7:85)
▼ Internet Protocol Version 4, Src: www1.cac.washington.edu (128.95.155.134), Dst: 192.168.1.102 (19
    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: 1500
    Identification: 0x6686 (26246)
```

4. What is the initial value of the TTL field for packets sent from your computer? Is it the maximum possible value, or some lower value?

The initial TTL field for packets sent from my computer is 64.

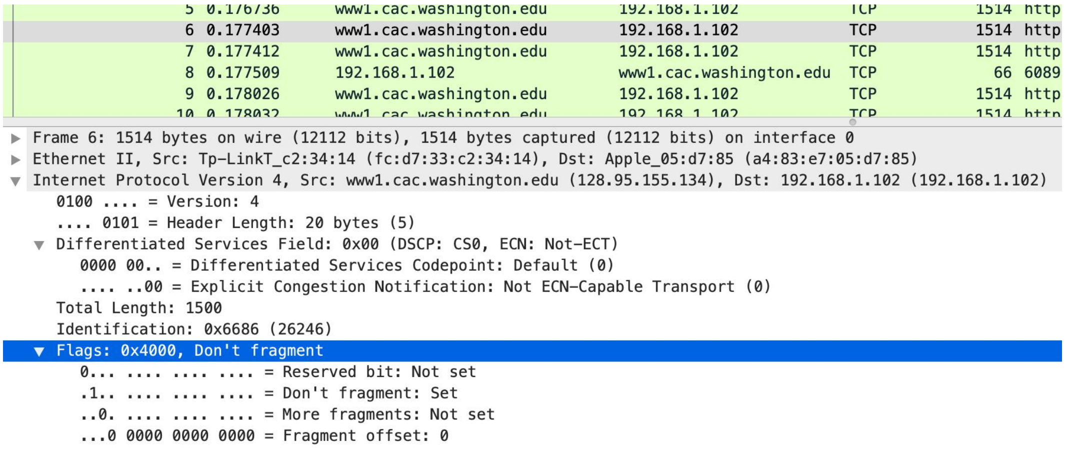
It is a lower value, because we know that the TTL field is of 8 bit long, so its maximum could be 255.



```
No.         Time        Source                    Destination               Protocol  Length  Info
          1 0.000000    192.168.1.102             www1.cac.washington.edu   TCP           78  60897 → http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2
          2 0.089436    www1.cac.washington.edu   192.168.1.102             TCP           74  http(80) → 60897 [SYN, ACK] Seq=0 Ack=1 Win=17896 Len=0 MSS=1460 SA
          3 0.089553    192.168.1.102             www1.cac.washington.edu   TCP           66  60897 → http(80) [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=238453986
          4 0.089812    192.168.1.102             www1.cac.washington.edu   HTTP         214  GET / HTTP/1.1
          5 0.176736    www1.cac.washington.edu   192.168.1.102             TCP         1514  http(80) → 60897 [ACK] Seq=1 Ack=149 Win=19200 Len=1448 TSval=27010
          6 0.177403    www1.cac.washington.edu   192.168.1.102             TCP         1514  http(80) → 60897 [ACK] Seq=1449 Ack=149 Win=19200 Len=1448 TSval=27
          7 0.177412    www1.cac.washington.edu   192.168.1.102             TCP         1514  http(80) → 60897 [ACK] Seq=2897 Ack=149 Win=19200 Len=1448 TSval=27
          8 0.177509    192.168.1.102             www1.cac.washington.edu   TCP           66  60897 → http(80) [ACK] Seq=149 Ack=2897 Win=128832 Len=0 TSval=2384
          9 0.178026    www1.cac.washington.edu   192.168.1.102             TCP         1514  http(80) → 60897 [ACK] Seq=4345 Ack=149 Win=19200 Len=1448 TSval=27
         10 0.178032    www1.cac.washington.edu   192.168.1.102             TCP         1514  http(80) → 60897 [ACK] Seq=5793 Ack=149 Win=19200 Len=1448 TSval=270107

▶ Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
▶ Ethernet II, Src: Apple_05:d7:85 (a4:83:e7:05:d7:85), Dst: Tp-LinkT_c2:34:14 (fc:d7:33:c2:34:14)
▼ Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: www1.cac.washington.edu (128.95.155.134)
    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: 64
    Identification: 0x0000 (0)
  ▼ 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: 64
    Protocol: TCP (6)
    Header checksum: 0x5cc4 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102 (192.168.1.102)
    Destination: www1.cac.washington.edu (128.95.155.134)
▶ Transmission Control Protocol, Src Port: 60897 (60897), Dst Port: http (80), Seq: 0, Len: 0

0000  fc d7 33 c2 34 14 a4 83  e7 05 d7 85 08 00 45 00   ··3·4··· ······E·
0010  00 40 00 00 40 00 40 06  5c c4 c0 a8 01 66 80 5f   ·@··@·@· \····f·_
0020  9b 86 ed e1 00 50 42 ff  ee ed 00 00 00 00 b0 02   ·····PB· ········
0030  ff ff a6 29 00 00 02 04  05 b4 01 03 03 06 01 01   ···)···· ········
0040  08 0a 0e 36 84 89 00 00  00 00 04 02 00 00         ···6···· ······
```

5. How can you tell from looking at a packet that it has not been fragmented? Most often IP packets in normal operation are not fragmented. But the receiver must have a way to be sure. Hint: you may need to read your text to confirm a guess.

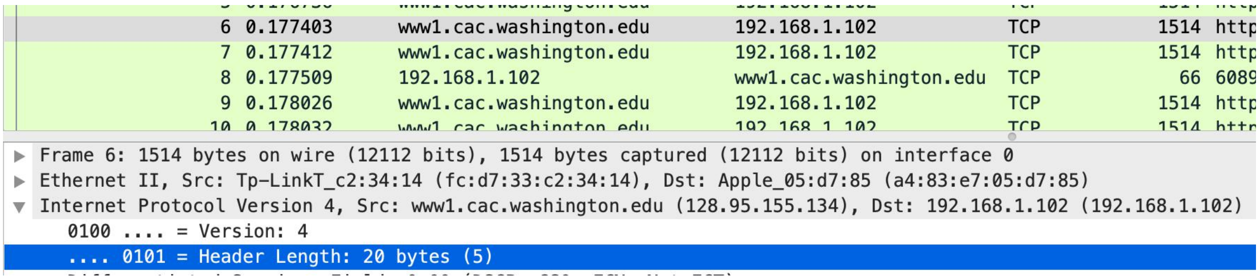
The 2 bytes flags has the fragmented or not information, the receiver could check if the Don't fragment bit is set, and further check the value Fragment offset to be sure whether a packet is fragmented or not



```
  5 0.176736    www1.cac.washington.edu   192.168.1.102             TCP    1514  http
  6 0.177403    www1.cac.washington.edu   192.168.1.102             TCP    1514  http
  7 0.177412    www1.cac.washington.edu   192.168.1.102             TCP    1514  http
  8 0.177509    192.168.1.102             www1.cac.washington.edu   TCP      66  6089
  9 0.178026    www1.cac.washington.edu   192.168.1.102             TCP    1514  http
 10 0.178032    www1.cac.washington.edu   192.168.1.102             TCP    1514  http

▶ Frame 6: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▶ Ethernet II, Src: Tp-LinkT_c2:34:14 (fc:d7:33:c2:34:14), Dst: Apple_05:d7:85 (a4:83:e7:05:d7:85)
▼ Internet Protocol Version 4, Src: www1.cac.washington.edu (128.95.155.134), Dst: 192.168.1.102 (192.168.1.102)
    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: 1500
    Identification: 0x6686 (26246)
  ▼ 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
```

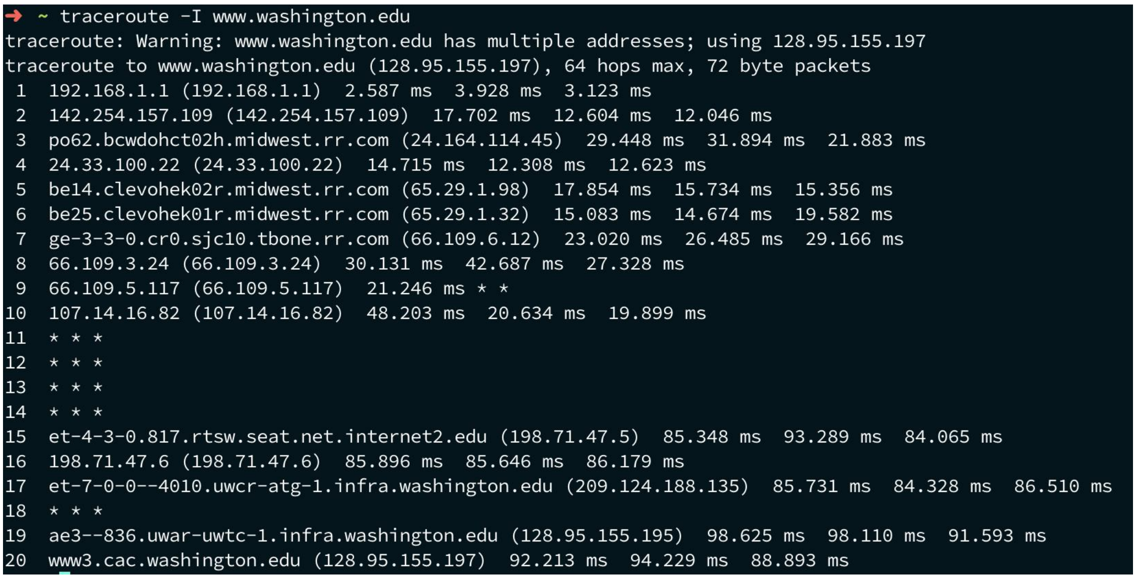
6. What is the length of the IP Header and how is this encoded in the header length field? Hint: notice that only 4 bits are used for this field, as the version takes up the other 4 bits of the byte. You may guess and check your text.

IP Header is 20 bytes long. It is encoded with the IP version into one single bytes, with upper 4 bits stands for the IP version and lower 4 bits stands for the header length.



```
  6 0.177403    www1.cac.washington.edu   192.168.1.102             TCP    1514  http
  7 0.177412    www1.cac.washington.edu   192.168.1.102             TCP    1514  http
  8 0.177509    192.168.1.102             www1.cac.washington.edu   TCP      66  6089
  9 0.178026    www1.cac.washington.edu   192.168.1.102             TCP    1514  http
 10 0.178032    www1.cac.washington.edu   192.168.1.102             TCP    1514  http

▶ Frame 6: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▶ Ethernet II, Src: Tp-LinkT_c2:34:14 (fc:d7:33:c2:34:14), Dst: Apple_05:d7:85 (a4:83:e7:05:d7:85)
▼ Internet Protocol Version 4, Src: www1.cac.washington.edu (128.95.155.134), Dst: 192.168.1.102 (192.168.1.102)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
```

Step 4: Internet Paths



```
➜ ~ traceroute -I www.washington.edu
traceroute: Warning: www.washington.edu has multiple addresses; using 128.95.155.197
traceroute to www.washington.edu (128.95.155.197), 64 hops max, 72 byte packets
 1  192.168.1.1 (192.168.1.1)  2.587 ms  3.928 ms  3.123 ms
 2  142.254.157.109 (142.254.157.109)  17.702 ms  12.604 ms  12.046 ms
 3  po62.bcwdohct02h.midwest.rr.com (24.164.114.45)  29.448 ms  31.894 ms  21.883 ms
 4  24.33.100.22 (24.33.100.22)  14.715 ms  12.308 ms  12.623 ms
 5  be14.clevohek02r.midwest.rr.com (65.29.1.98)  17.854 ms  15.734 ms  15.356 ms
 6  be25.clevohek01r.midwest.rr.com (65.29.1.32)  15.083 ms  14.674 ms  19.582 ms
 7  ge-3-3-0.cr0.sjc10.tbone.rr.com (66.109.6.12)  23.020 ms  26.485 ms  29.166 ms
 8  66.109.3.24 (66.109.3.24)  30.131 ms  42.687 ms  27.328 ms
 9  66.109.5.117 (66.109.5.117)  21.246 ms * *
10  107.14.16.82 (107.14.16.82)  48.203 ms  20.634 ms  19.899 ms
11  * * *
12  * * *
13  * * *
14  * * *
15  et-4-3-0.817.rtsw.seat.net.internet2.edu (198.71.47.5)  85.348 ms  93.289 ms  84.065 ms
16  198.71.47.6 (198.71.47.6)  85.896 ms  85.646 ms  86.179 ms
17  et-7-0-0--4010.uwcr-atg-1.infra.washington.edu (209.124.188.135)  85.731 ms  84.328 ms  86.510 ms
18  * * *
19  ae3--836.uwar-uwtc-1.infra.washington.edu (128.95.155.195)  98.625 ms  98.110 ms  91.593 ms
20  www3.cac.washington.edu (128.95.155.197)  92.213 ms  94.229 ms  88.893 ms
```

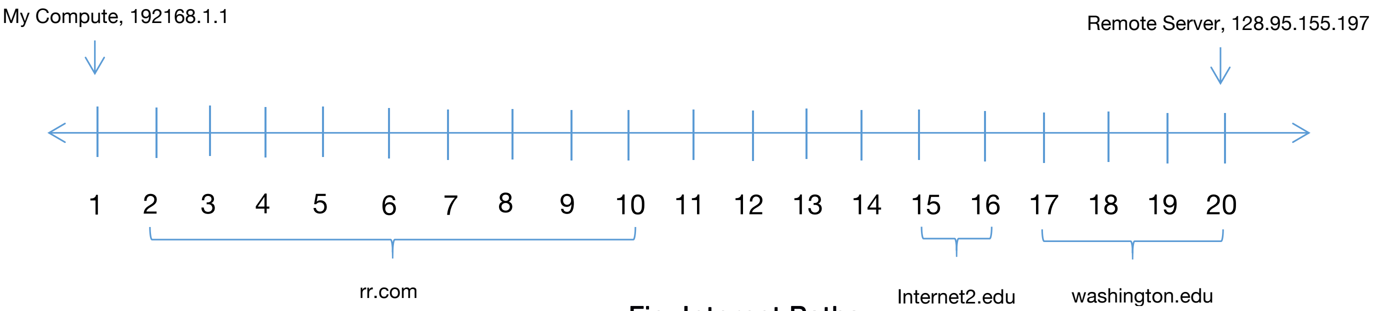
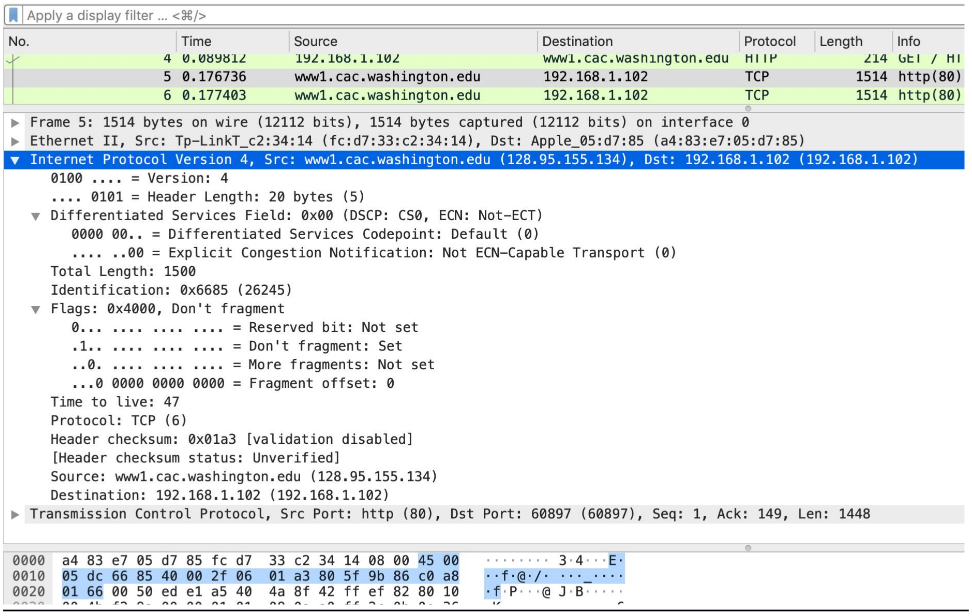


Fig. Internet Paths

Step 5: IP Header Checksum



```
Apply a display filter ... <⌘/>
No.          Time        Source                   Destination              Protocol  Length  Info
          4  0.089812    192.168.1.102            www1.cac.washington.edu  HTTP         214  GET / HT
          5  0.176736    www1.cac.washington.edu  192.168.1.102            TCP         1514  http(80)
          6  0.177403    www1.cac.washington.edu  192.168.1.102            TCP         1514  http(80)

▶ Frame 5: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▶ Ethernet II, Src: Tp-LinkT_c2:34:14 (fc:d7:33:c2:34:14), Dst: Apple_05:d7:85 (a4:83:e7:05:d7:85)
▼ Internet Protocol Version 4, Src: www1.cac.washington.edu (128.95.155.134), Dst: 192.168.1.102 (192.168.1.102)
    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: 1500
    Identification: 0x6685 (26245)
  ▼ 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: 0x01a3 [validation disabled]
    [Header checksum status: Unverified]
    Source: www1.cac.washington.edu (128.95.155.134)
    Destination: 192.168.1.102 (192.168.1.102)
▶ Transmission Control Protocol, Src Port: http (80), Dst Port: 60897 (60897), Seq: 1, Ack: 149, Len: 1448

0000  a4 83 e7 05 d7 85 fc d7  33 c2 34 14 08 00 45 00   ········ 3·4···E·
0010  05 dc 66 85 40 00 2f 06  01 a3 80 5f 9b 86 c0 a8   ··f·@·/· ···_····
0020  01 66 00 50 ed e1 a5 40  4a 8f 42 ff ef 82 80 10   ·f·P···@ J·B·····
```

As we could see, the IP header in hexadecimal format is 4500 05dc 6685 4000 2f06 01a3 805f 9b86 c0a8 0166

Word meaning:

4500 -> IP version and Header Length (45) + Differentiated Service Field (00)
05dc -> Total Length

6685 -> Identification
4000 -> Fragment Flags
2f06 -> Time to live (2f) + Protocol (06)
01a3 -> Header Checksum
805f -> Source IP (upper part)
9b86 -> Source IP (lower part)
c0a8 -> Destination IP (upper part)
0166 -> Destination IP (lower part)

We could do the following calculation:

4500 + 05dc = 4ADC
4ADC + 6685 = B161
B161 + 4000 = F161
F161 + 2f06 = 12067
12067 + 01a3 = 1220A
1220A + 805f = 1A269
1A269 + 9b86 = 23DEF
23DEF + c0a8 = 2FE97
2FE97 + 0166 = 2FFFD
FFFD + 2 = FFFF
The sum is 0xffff, which means the sum is correct.