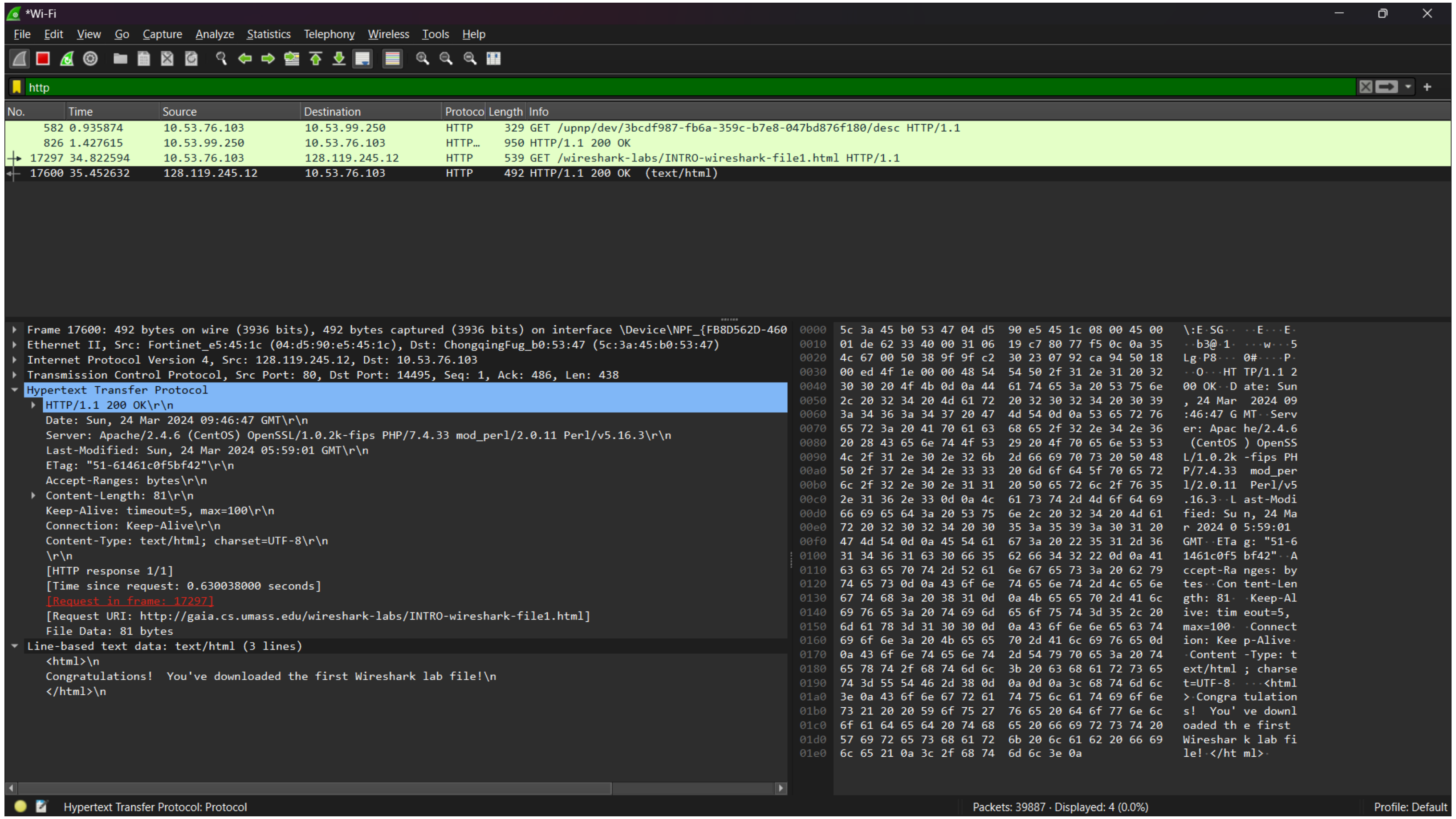
Intro

Yogesh P
201EE138



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

```
http
```

```
No.    Time       Source          Destination     Protoco Length Info
   582 0.935874   10.53.76.103    10.53.99.250    HTTP     329 GET /upnp/dev/3bcdf987-fb6a-359c-b7e8-047bd876f180/desc HTTP/1.1
   826 1.427615   10.53.99.250    10.53.76.103    HTTP…    950 HTTP/1.1 200 OK
 17297 34.822594  10.53.76.103    128.119.245.12  HTTP     539 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
 17600 35.452632  128.119.245.12  10.53.76.103    HTTP     492 HTTP/1.1 200 OK  (text/html)
```

```
Frame 17600: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{FB8D562D-460
Ethernet II, Src: Fortinet_e5:45:1c (04:d5:90:e5:45:1c), Dst: ChongqingFug_b0:53:47 (5c:3a:45:b0:53:47)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.53.76.103
Transmission Control Protocol, Src Port: 80, Dst Port: 14495, Seq: 1, Ack: 486, Len: 438
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Sun, 24 Mar 2024 09:46:47 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Last-Modified: Sun, 24 Mar 2024 05:59:01 GMT\r\n
  ETag: "51-61461c0f5bf42"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 81\r\n
  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: 0.630038000 seconds]
  [Request in frame: 17297]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
  File Data: 81 bytes
Line-based text data: text/html (3 lines)
  <html>\n
  Congratulations!  You've downloaded the first Wireshark lab file!\n
  </html>\n
```

```
0000  5c 3a 45 b0 53 47 04 d5  90 e5 45 1c 08 00 45 00   \:E·SG·· ··E···E·
0010  01 de 62 33 40 00 31 06  19 c7 80 77 f5 0c 0a 35   ··b3@·1· ···w···5
0020  4c 67 00 50 38 9f 9f c2  30 23 07 92 ca 94 50 18   Lg·P8··· 0#····P·
0030  00 ed 4f 1e 00 00 48 54  54 50 2f 31 2e 31 20 32   ··O···HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 53 75 6e   00 OK··D ate: Sun
0050  2c 20 32 34 20 4d 61 72  20 32 30 32 34 20 30 39   , 24 Mar  2024 09
0060  3a 34 36 3a 34 37 20 47  4d 54 0d 0a 53 65 72 76   :46:47 G MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apac he/2.4.6
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentOS ) OpenSS
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73 20 50 48   L/1.0.2k -fips PH
00a0  50 2f 37 2e 34 2e 33 33  20 6d 6f 64 5f 70 65 72   P/7.4.33  mod_per
00b0  6c 2f 32 2e 30 2e 31 31  20 50 65 72 6c 2f 76 35   l/2.0.11  Perl/v5
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3··L ast-Modi
00d0  66 69 65 64 3a 20 53 75  6e 2c 20 32 34 20 4d 61   fied: Su n, 24 Ma
00e0  72 20 32 30 32 34 20 30  35 3a 35 39 3a 30 31 20   r 2024 0 5:59:01 
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 35 31 2d 36   GMT··ETa g: "51-6
0100  31 34 36 31 63 30 66 35  62 66 34 32 22 0d 0a 41   1461c0f5 bf42"··A
0110  63 63 65 70 74 2d 52 61  6e 67 65 73 3a 20 62 79   ccept-Ra nges: by
0120  74 65 73 0d 0a 43 6f 6e  74 65 6e 74 2d 4c 65 6e   tes··Con tent-Len
0130  67 74 68 3a 20 38 31 0d  0a 4b 65 65 70 2d 41 6c   gth: 81· ·Keep-Al
0140  69 76 65 3a 20 74 69 6d  65 6f 75 74 3d 35 2c 20   ive: tim eout=5, 
0150  6d 61 78 3d 31 30 30 0d  0a 43 6f 6e 6e 65 63 74   max=100· ·Connect
0160  69 6f 6e 3a 20 4b 65 65  70 2d 41 6c 69 76 65 0d   ion: Kee p-Alive·
0170  0a 43 6f 6e 74 65 6e 74  2d 54 79 70 65 3a 20 74   ·Content -Type: t
0180  65 78 74 2f 68 74 6d 6c  3b 20 63 68 61 72 73 65   ext/html ; charse
0190  74 3d 55 54 46 2d 38 0d  0a 0d 0a 3c 68 74 6d 6c   t=UTF-8· ···<html
01a0  3e 0a 43 6f 6e 67 72 61  74 75 6c 61 74 69 6f 6e   >·Congra tulation
01b0  73 21 20 20 59 6f 75 27  76 65 20 64 6f 77 6e 6c   s!  You' ve downl
01c0  6f 61 64 65 64 20 74 68  65 20 66 69 72 73 74 20   oaded th e first 
01d0  57 69 72 65 73 68 61 72  6b 20 6c 61 62 20 66 69   Wireshar k lab fi
01e0  6c 65 21 0a 3c 2f 68 74  6d 6c 3e 0a               le!·</ht ml>·
```

```
Hypertext Transfer Protocol: Protocol          Packets: 39887 · Displayed: 4 (0.0%)          Profile: Default
```

1. Which of the following protocols are shown as appearing (i.e., are listed in the Wireshark “protocol” column) in your trace file: TCP, QUIC, HTTP, DNS, UDP, TLSv1.2?

A: All of them

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?

A: 0.63s

3. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer or (if you are using the trace file) the computer that sent the HTTP GET message?

A: 128.119.245.12,   10.53.76.103

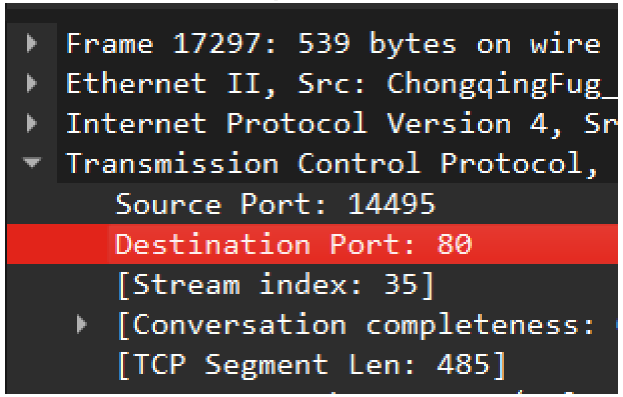
4. Expand the information on the HTTP message in the Wireshark “Details of selected packet” window (see Figure 3 above) so you can see the fields in the HTTP GET request message. What type of Web browser issued the HTTP request? The answer is shown at the right end of the information following the “User-Agent:” field in the expanded HTTP message display. [This field value in the HTTP message is how a web server learns what type of browser you are using.] Firefox, Safari, Microsoft Internet Edge, Other

A: User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36\r\n

Chrome

5. Expand the information on the Transmission Control Protocol for this packet in the Wireshark “Details of selected packet” window (see Figure 3 in the lab writeup) so you can see the fields in the TCP segment carrying the HTTP message. What is the destination port number (the number following “Dest Port:” for the TCP segment containing the HTTP request) to which this HTTP request is being sent?

A: 80

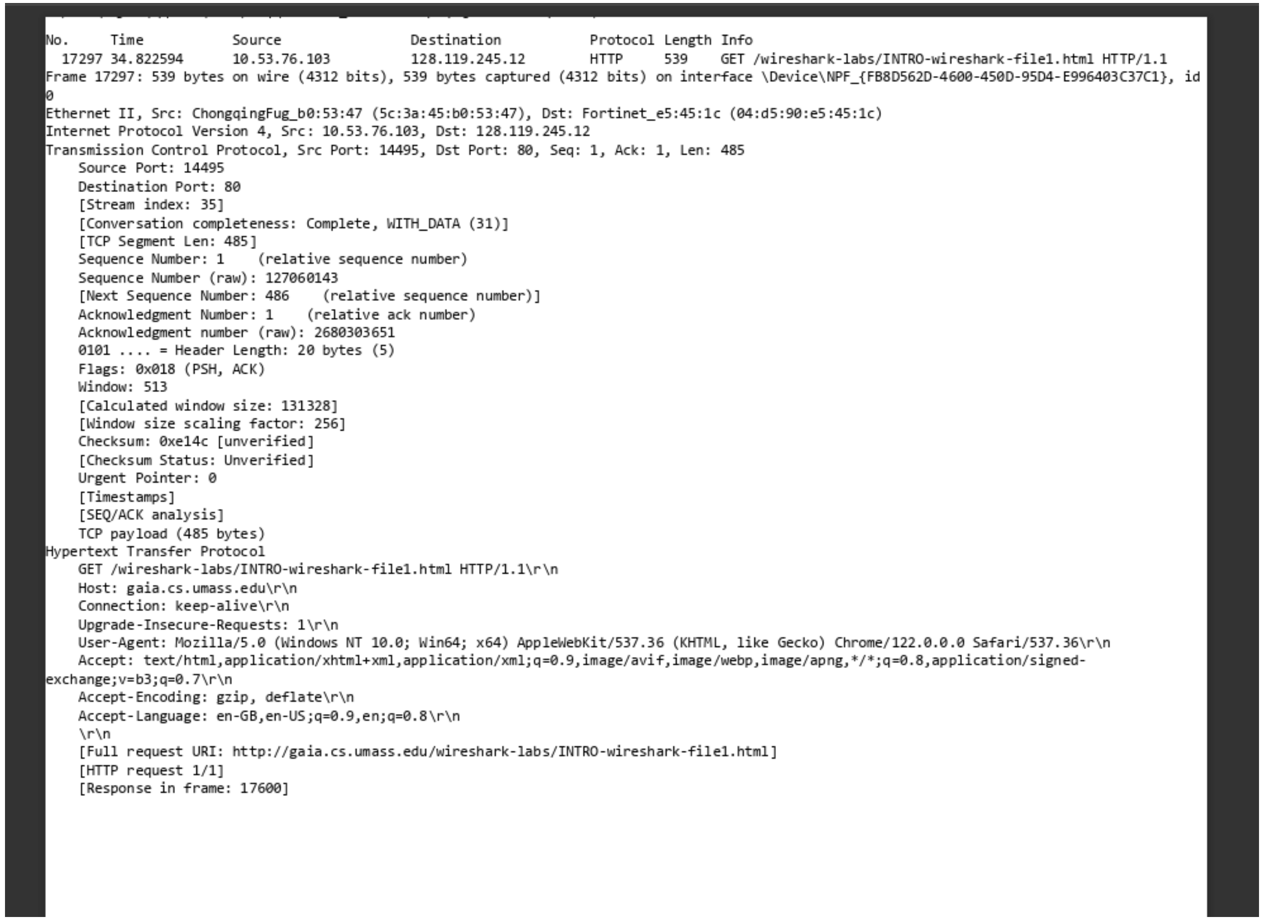


```
▸ Frame 17297: 539 bytes on wire
▸ Ethernet II, Src: ChongqingFug_
▸ Internet Protocol Version 4, Sr
▾ Transmission Control Protocol,
      Source Port: 14495
      Destination Port: 80
      [Stream index: 35]
    ▸ [Conversation completeness:
      [TCP Segment Len: 485]
```

6. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the “Selected Packet Only” and “Print as displayed” radial buttons, and then click OK.

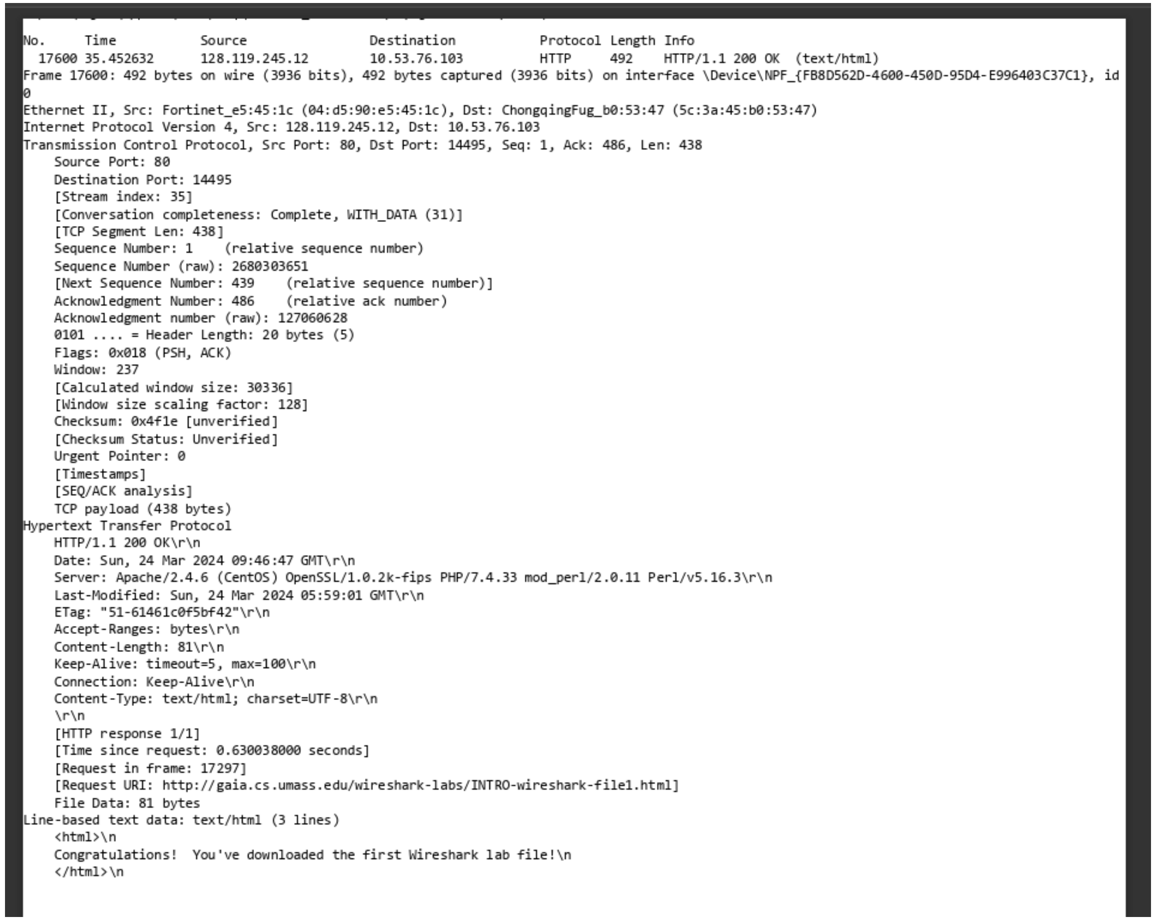
A: next slides

get



```
No.     Time           Source                Destination           Protocol Length Info
  17297 34.822594      10.53.76.103          128.119.245.12        HTTP     539    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 17297: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits) on interface \Device\NPF_{FB8D562D-4600-450D-95D4-E996403C37C1}, id
0
Ethernet II, Src: ChongqingFug_b0:53:47 (5c:3a:45:b0:53:47), Dst: Fortinet_e5:45:1c (04:d5:90:e5:45:1c)
Internet Protocol Version 4, Src: 10.53.76.103, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 14495, Dst Port: 80, Seq: 1, Ack: 1, Len: 485
    Source Port: 14495
    Destination Port: 80
    [Stream index: 35]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 485]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 127060143
    [Next Sequence Number: 486    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2680303651
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 513
    [Calculated window size: 131328]
    [Window size scaling factor: 256]
    Checksum: 0xe14c [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (485 bytes)
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 17600]
```

response



```
No.     Time           Source                Destination           Protocol Length Info
  17600 35.452632      128.119.245.12        10.53.76.103          HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 17600: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{FB8D562D-4600-450D-95D4-E996403C37C1}, id
0
Ethernet II, Src: Fortinet_e5:45:1c (04:d5:90:e5:45:1c), Dst: ChongqingFug_b0:53:47 (5c:3a:45:b0:53:47)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.53.76.103
Transmission Control Protocol, Src Port: 80, Dst Port: 14495, Seq: 1, Ack: 486, Len: 438
    Source Port: 80
    Destination Port: 14495
    [Stream index: 35]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 438]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2680303651
    [Next Sequence Number: 439    (relative sequence number)]
    Acknowledgment Number: 486    (relative ack number)
    Acknowledgment number (raw): 127060628
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0x4f1e [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (438 bytes)
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Sun, 24 Mar 2024 09:46:47 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sun, 24 Mar 2024 05:59:01 GMT\r\n
    ETag: "51-61461c0f5bf42"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\r\n
    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: 0.630038000 seconds]
    [Request in frame: 17297]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
    <html>\n
    Congratulations!  You've downloaded the first Wireshark lab file!\n
    </html>\n
```