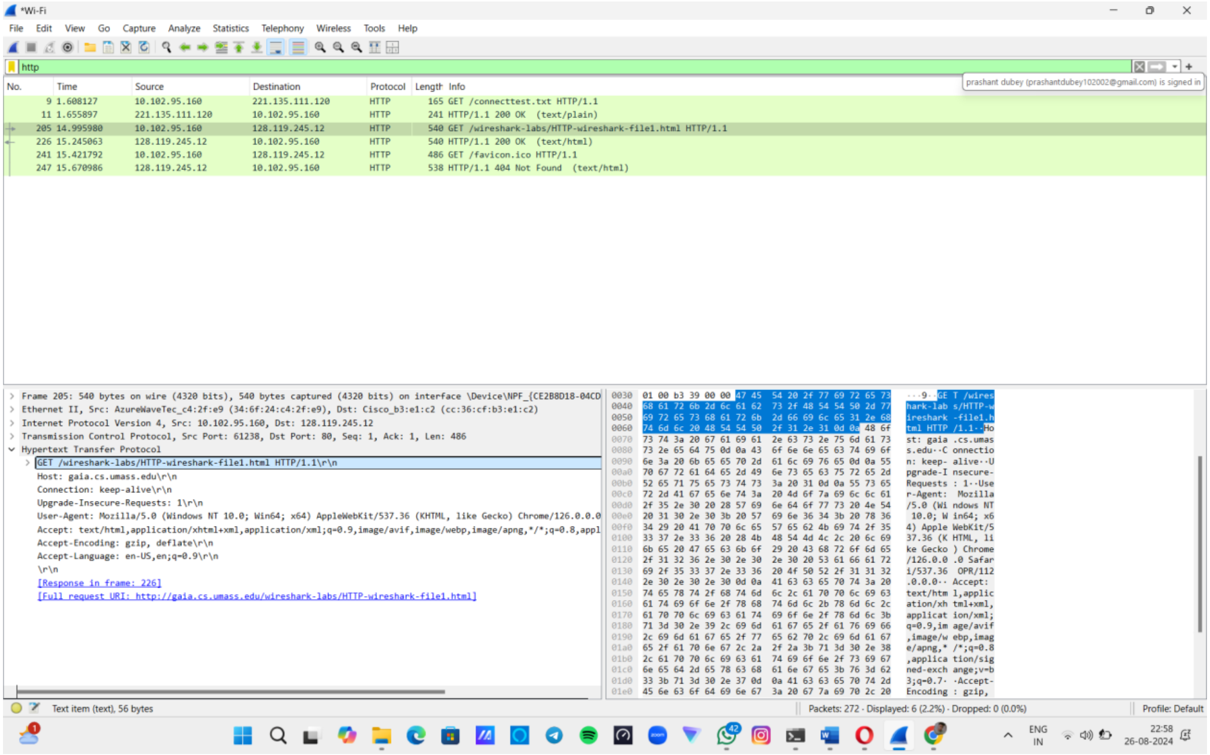
Computer Network: Wireshark HTTP

Assignment 2

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

Answer:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
prashant dubey (prashantdubey102002@gmail.com) is signed in
Text item (text), 56 bytes
Profile: Default
ENG IN
22:58
26-08-2024

```
No.   Time        Source            Destination       Protocol Length Info
    9 1.608127    10.102.95.160     221.135.111.120   HTTP     165 GET /connecttest.txt HTTP/1.1
   11 1.655897    221.135.111.120   10.102.95.160     HTTP     241 HTTP/1.1 200 OK  (text/plain)
  205 14.995980   10.102.95.160     128.119.245.12    HTTP     540 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  226 15.245063   128.119.245.12    10.102.95.160     HTTP     540 HTTP/1.1 200 OK  (text/html)
  241 15.421792   10.102.95.160     128.119.245.12    HTTP     486 GET /favicon.ico HTTP/1.1
  247 15.670986   128.119.245.12    10.102.95.160     HTTP     538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 205: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{CE2B8D18-04CD
> Ethernet II, Src: AzureWaveTec_c4:2f:e9 (34:6f:24:c4:2f:e9), Dst: Cisco_b3:e1:c2 (cc:36:cf:b3:e1:c2)
> Internet Protocol Version 4, Src: 10.102.95.160, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 61238, Dst Port: 80, Seq: 1, Ack: 1, Len: 486
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-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/126.0.0.0
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Response in frame: 226]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
```

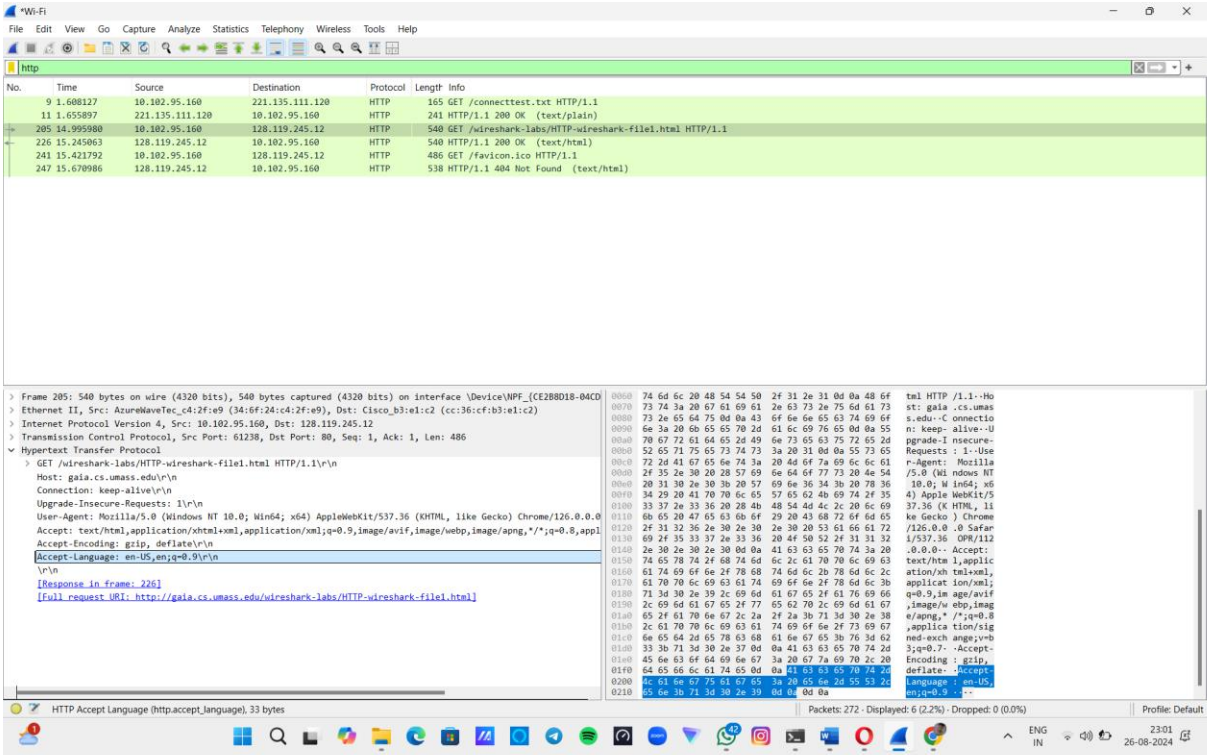
```
0030  01 00 b3 39 00 00 47 45  54 20 2f 77 69 72 65 73   ···9··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 31 2e 68   ireshark -file1.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep- alive··U
00a0  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I nsecure-
00b0  52 65 71 75 65 73 74 73  3a 20 31 0d 0a 55 73 65   Requests : 1··Use
00c0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
00d0  2f 35 2e 30 20 28 57 69  6e 64 6f 77 73 20 4e 54   /5.0 (Wi ndows NT
00e0  20 31 30 2e 30 3b 20 57  69 6e 36 34 3b 20 78 36    10.0; W in64; x6
00f0  34 29 20 41 70 70 6c 65  57 65 62 4b 69 74 2f 35   4) Apple WebKit/5
0100  33 37 2e 33 36 20 28 4b  48 54 4d 4c 2c 20 6c 69   37.36 (K HTML, li
0110  6b 65 20 47 65 63 6b 6f  29 20 43 68 72 6f 6d 65   ke Gecko ) Chrome
0120  2f 31 32 36 2e 30 2e 30  2e 30 20 53 61 66 61 72   /126.0.0 .0 Safar
0130  69 2f 35 33 37 2e 33 36  20 4f 50 52 2f 31 31 32   i/537.36  OPR/112
0140  2e 30 2e 30 2e 30 0d 0a  41 63 63 65 70 74 3a 20   .0.0.0·· Accept: 
0150  74 65 78 74 2f 68 74 6d  6c 2c 61 70 70 6c 69 63   text/htm l,applic
0160  61 74 69 6f 6e 2f 78 68  74 6d 6c 2b 78 6d 6c 2c   ation/xh tml+xml,
0170  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 6d 6c 3b   applicat ion/xml;
0180  71 3d 30 2e 39 2c 69 6d  61 67 65 2f 61 76 69 66   q=0.9,im age/avif
0190  2c 69 6d 61 67 65 2f 77  65 62 70 2c 69 6d 61 67   ,image/w ebp,imag
01a0  65 2f 61 70 6e 67 2c 2a  2f 2a 3b 71 3d 30 2e 38   e/apng,* /*;q=0.8
01b0  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2f 73 69 67   ,applica tion/sig
01c0  6e 65 64 2d 65 78 63 68  61 6e 67 65 3b 76 3d 62   ned-exch ange;v=b
01d0  33 3b 71 3d 30 2e 37 0d  0a 41 63 63 65 70 74 2d   3;q=0.7· ·Accept-
01e0  45 6e 63 6f 64 69 6e 67  3a 20 67 7a 69 70 2c 20   Encoding : gzip, 
```

Packets: 272 · Displayed: 6 (2.2%) · Dropped: 0 (0.0%)

HTTP Version 1.1

2. What languages (if any) does your browser indicate that it can accept to the server?

Answer:



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

http

```
No.   Time       Source            Destination       Protocol Length Info
    9 1.608127   10.102.95.160     221.135.111.120   HTTP      165 GET /connecttest.txt HTTP/1.1
   11 1.655897   221.135.111.120   10.102.95.160     HTTP      241 HTTP/1.1 200 OK  (text/plain)
  205 14.995980  10.102.95.160     128.119.245.12    HTTP      540 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  226 15.245063  128.119.245.12    10.102.95.160     HTTP      540 HTTP/1.1 200 OK  (text/html)
  241 15.421792  10.102.95.160     128.119.245.12    HTTP      486 GET /favicon.ico HTTP/1.1
  247 15.670986  128.119.245.12    10.102.95.160     HTTP      538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 205: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{CE2B8D18-04CD
> Ethernet II, Src: AzureWaveTec_c4:2f:e9 (34:6f:24:c4:2f:e9), Dst: Cisco_b3:e1:c2 (cc:36:cf:b3:e1:c2)
> Internet Protocol Version 4, Src: 10.102.95.160, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 61238, Dst Port: 80, Seq: 1, Ack: 1, Len: 486
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-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/126.0.0.0
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Response in frame: 226]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
```

```
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep- alive··U
00a0  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I nsecure-
00b0  52 65 71 75 65 73 74 73  3a 20 31 0d 0a 55 73 65   Requests : 1··Use
00c0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
00d0  2f 35 2e 30 20 28 57 69  6e 64 6f 77 73 20 4e 54   /5.0 (Wi ndows NT
00e0  20 31 30 2e 30 3b 20 57  69 6e 36 34 3b 20 78 36    10.0; W in64; x6
00f0  34 29 20 41 70 70 6c 65  57 65 62 4b 69 74 2f 35   4) Apple WebKit/5
0100  33 37 2e 33 36 20 28 4b  48 54 4d 4c 2c 20 6c 69   37.36 (K HTML, li
0110  6b 65 20 47 65 63 6b 6f  29 20 43 68 72 6f 6d 65   ke Gecko ) Chrome
0120  2f 31 32 36 2e 30 2e 30  2e 30 20 53 61 66 61 72   /126.0.0 .0 Safar
0130  69 2f 35 33 37 2e 33 36  20 4f 50 52 2f 31 31 32   i/537.36  OPR/112
0140  2e 30 2e 30 2e 30 0d 0a  41 63 63 65 70 74 3a 20   .0.0.0·· Accept: 
0150  74 65 78 74 2f 68 74 6d  6c 2c 61 70 70 6c 69 63   text/htm l,applic
0160  61 74 69 6f 6e 2f 78 68  74 6d 6c 2b 78 6d 6c 2c   ation/xh tml+xml,
0170  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 6d 6c 3b   applicat ion/xml;
0180  71 3d 30 2e 39 2c 69 6d  61 67 65 2f 61 76 69 66   q=0.9,im age/avif
0190  2c 69 6d 61 67 65 2f 77  65 62 70 2c 69 6d 61 67   ,image/w ebp,imag
01a0  65 2f 61 70 6e 67 2c 2a  2f 2a 3b 71 3d 30 2e 38   e/apng,* /*;q=0.8
01b0  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2f 73 69 67   ,applica tion/sig
01c0  6e 65 64 2d 65 78 63 68  61 6e 67 65 3b 76 3d 62   ned-exch ange;v=b
01d0  33 3b 71 3d 30 2e 37 0d  0a 41 63 63 65 70 74 2d   3;q=0.7· ·Accept-
01e0  45 6e 63 6f 64 69 6e 67  3a 20 67 7a 69 70 2c 20   Encoding : gzip, 
01f0  64 65 66 6c 61 74 65 0d  0a 41 63 63 65 70 74 2d   deflate· ·Accept-
0200  4c 61 6e 67 75 61 67 65  3a 20 65 6e 2d 55 53 2c   Language : en-US,
0210  65 6e 3b 71 3d 30 2e 39  0d 0a 0d 0a               en;q=0.9 ····
```

HTTP Accept Language (http.accept_language), 33 bytes

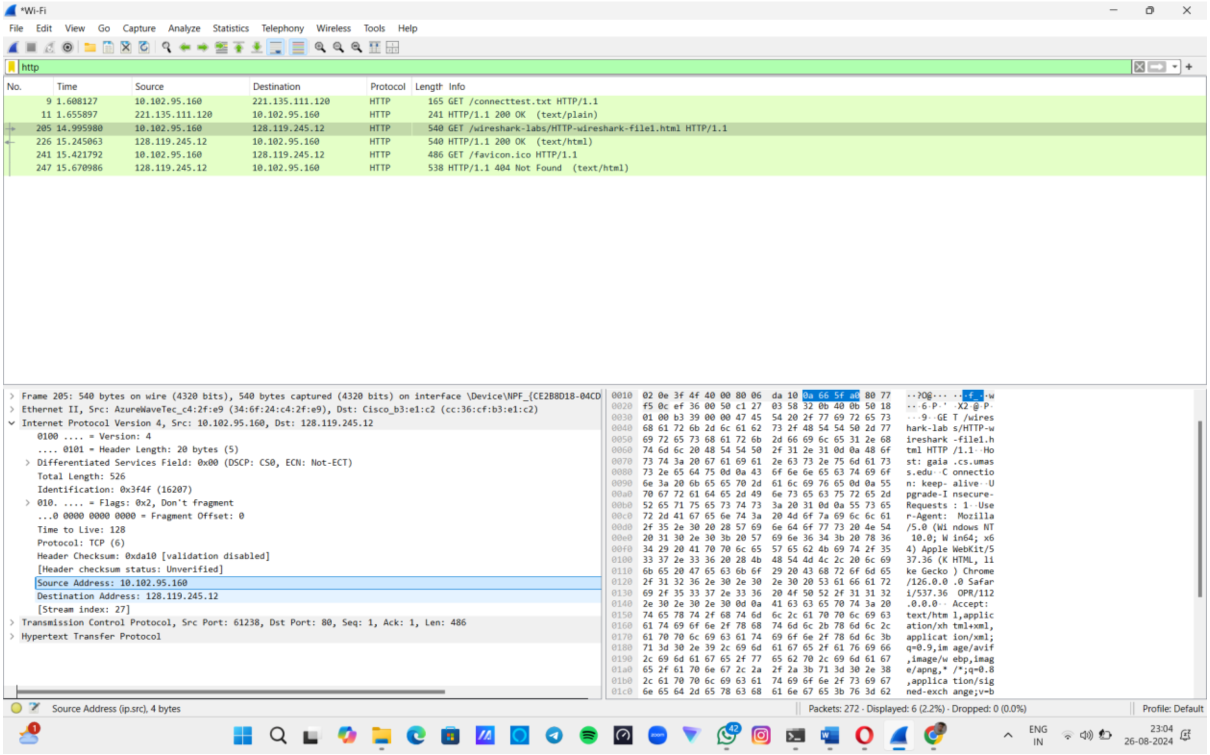
Packets: 272 · Displayed: 6 (2.2%) · Dropped: 0 (0.0%)

Profile: Default

The browser indicate that it can accept en-US , en to the server

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

Answer:


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

http

```
No.   Time       Source           Destination      Protocol Length Info
    9 1.608127   10.102.95.160    221.135.111.120  HTTP     165 GET /connecttest.txt HTTP/1.1
   11 1.655897   221.135.111.120  10.102.95.160    HTTP     241 HTTP/1.1 200 OK  (text/plain)
  205 14.995980  10.102.95.160    128.119.245.12   HTTP     540 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  226 15.245063  128.119.245.12   10.102.95.160    HTTP     540 HTTP/1.1 200 OK  (text/html)
  241 15.421792  10.102.95.160    128.119.245.12   HTTP     486 GET /favicon.ico HTTP/1.1
  247 15.670986  128.119.245.12   10.102.95.160    HTTP     538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 205: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{CE2B8D18-04CD
> Ethernet II, Src: AzureWaveTec_c4:2f:e9 (34:6f:24:c4:2f:e9), Dst: Cisco_b3:e1:c2 (cc:36:cf:b3:e1:c2)
v Internet Protocol Version 4, Src: 10.102.95.160, 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: 526
    Identification: 0x3f4f (16207)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0xda10 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.102.95.160
    Destination Address: 128.119.245.12
    [Stream index: 27]
> Transmission Control Protocol, Src Port: 61238, Dst Port: 80, Seq: 1, Ack: 1, Len: 486
> Hypertext Transfer Protocol
```

```
0010  02 0e 3f 4f 40 00 80 06  da 10 0a 66 5f a0 80 77   ··?O@··· ···f_··w
0020  f5 0c ef 36 00 50 c1 27  03 58 32 0b 40 0b 50 18   ···6·P·' ·X2·@·P·
0030  01 00 b3 39 00 00 47 45  54 20 2f 77 69 72 65 73   ···9··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 31 2e 68   ireshark -file1.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep- alive··U
00a0  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I nsecure-
00b0  52 65 71 75 65 73 74 73  3a 20 31 0d 0a 55 73 65   Requests : 1··Use
00c0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
00d0  2f 35 2e 30 20 28 57 69  6e 64 6f 77 73 20 4e 54   /5.0 (Wi ndows NT
00e0  20 31 30 2e 30 3b 20 57  69 6e 36 34 3b 20 78 36    10.0; W in64; x6
00f0  34 29 20 41 70 70 6c 65  57 65 62 4b 69 74 2f 35   4) Apple WebKit/5
0100  33 37 2e 33 36 20 28 4b  48 54 4d 4c 2c 20 6c 69   37.36 (K HTML, li
0110  6b 65 20 47 65 63 6b 6f  29 20 43 68 72 6f 6d 65   ke Gecko ) Chrome
0120  2f 31 32 36 2e 30 2e 30  2e 30 20 53 61 66 61 72   /126.0.0 .0 Safar
0130  69 2f 35 33 37 2e 33 36  20 4f 50 52 2f 31 31 32   i/537.36  OPR/112
0140  2e 30 2e 30 2e 30 0d 0a  41 63 63 65 70 74 3a 20   .0.0.0·· Accept: 
0150  74 65 78 74 2f 68 74 6d  6c 2c 61 70 70 6c 69 63   text/htm l,applic
0160  61 74 69 6f 6e 2f 78 68  74 6d 6c 2b 78 6d 6c 2c   ation/xh tml+xml,
0170  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 6d 6c 3b   applicat ion/xml;
0180  71 3d 30 2e 39 2c 69 6d  61 67 65 2f 61 76 69 66   q=0.9,im age/avif
0190  2c 69 6d 61 67 65 2f 77  65 62 70 2c 69 6d 61 67   ,image/w ebp,imag
01a0  65 2f 61 70 6e 67 2c 2a  2f 2a 3b 71 3d 30 2e 38   e/apng,* /*;q=0.8
01b0  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2f 73 69 67   ,applica tion/sig
01c0  6e 65 64 2d 65 78 63 68  61 6e 67 65 3b 76 3d 62   ned-exch ange;v=b
```

Source Address (ip.src), 4 bytes

Packets: 272 · Displayed: 6 (2.2%) · Dropped: 0 (0.0%)

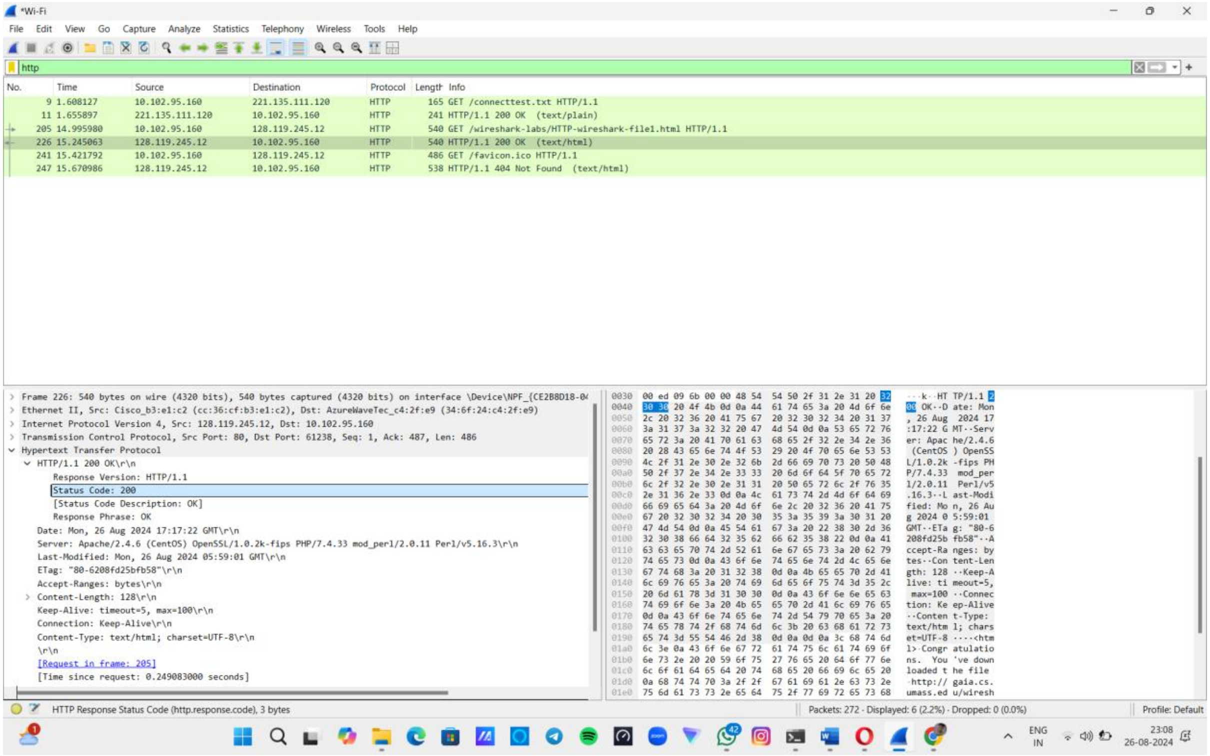
Profile: Default

My IP Address: 10.102.95.160

IP Address of gaia.cs.umass.edu server is 128.119.245.12

4. What is the status code returned from the server to your browser?

Answer:



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

```
No.   Time        Source            Destination       Protocol  Length Info
    9 1.608127    10.102.95.160     221.135.111.120   HTTP      165 GET /connecttest.txt HTTP/1.1
   11 1.655897    221.135.111.120   10.102.95.160     HTTP      241 HTTP/1.1 200 OK  (text/plain)
  205 14.995980   10.102.95.160     128.119.245.12    HTTP      540 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  226 15.245063   128.119.245.12    10.102.95.160     HTTP      540 HTTP/1.1 200 OK  (text/html)
  241 15.421792   10.102.95.160     128.119.245.12    HTTP      486 GET /favicon.ico HTTP/1.1
  247 15.670986   128.119.245.12    10.102.95.160     HTTP      538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 226: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{CE2B8D18-0
> Ethernet II, Src: Cisco_b3:e1:c2 (cc:36:cf:b3:e1:c2), Dst: AzureWaveTec_c4:2f:e9 (34:6f:24:c4:2f:e9)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.102.95.160
> Transmission Control Protocol, Src Port: 80, Dst Port: 61238, Seq: 1, Ack: 487, Len: 486
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Mon, 26 Aug 2024 17:17:22 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: Mon, 26 Aug 2024 05:59:01 GMT\r\n
    ETag: "80-6208fd25bfb58"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 128\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
    [Request in frame: 205]
    [Time since request: 0.249083000 seconds]
```

```
0030  00 ed 09 6b 00 00 48 54  54 50 2f 31 2e 31 20 32   ···k··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 4d 6f 6e   00 OK··D ate: Mon
0050  2c 20 32 36 20 41 75 67  20 32 30 32 34 20 31 37   , 26 Aug  2024 17
0060  3a 31 37 3a 32 32 20 47  4d 54 0d 0a 53 65 72 76   :17:22 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 4d 6f  6e 2c 20 32 36 20 41 75   fied: Mo n, 26 Au
00e0  67 20 32 30 32 34 20 30  35 3a 35 39 3a 30 31 20   g 2024 0 5:59:01
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 38 30 2d 36   GMT··ETa g: "80-6
0100  32 30 38 66 64 32 35 62  66 62 35 38 22 0d 0a 41   208fd25b fb58"··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 31 32 38  0d 0a 4b 65 65 70 2d 41   gth: 128 ··Keep-A
0140  6c 69 76 65 3a 20 74 69  6d 65 6f 75 74 3d 35 2c   live: ti meout=5,
0150  20 6d 61 78 3d 31 30 30  0d 0a 43 6f 6e 6e 65 63    max=100 ··Connec
0160  74 69 6f 6e 3a 20 4b 65  65 70 2d 41 6c 69 76 65   tion: Ke ep-Alive
0170  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ··Conten t-Type:
0180  74 65 78 74 2f 68 74 6d  6c 3b 20 63 68 61 72 73   text/htm l; chars
0190  65 74 3d 55 54 46 2d 38  0d 0a 0d 0a 3c 68 74 6d   et=UTF-8 ····<htm
01a0  6c 3e 0a 43 6f 6e 67 72  61 74 75 6c 61 74 69 6f   l>·Congr atulatio
01b0  6e 73 2e 20 20 59 6f 75  27 76 65 20 64 6f 77 6e   ns.  You 've down
01c0  6c 6f 61 64 65 64 20 74  68 65 20 66 69 6c 65 20   loaded t he file
01d0  0a 68 74 74 70 3a 2f 2f  67 61 69 61 2e 63 73 2e   ·http:// gaia.cs.
01e0  75 6d 61 73 73 2e 65 64  75 2f 77 69 72 65 73 68   umass.ed u/wiresh
```

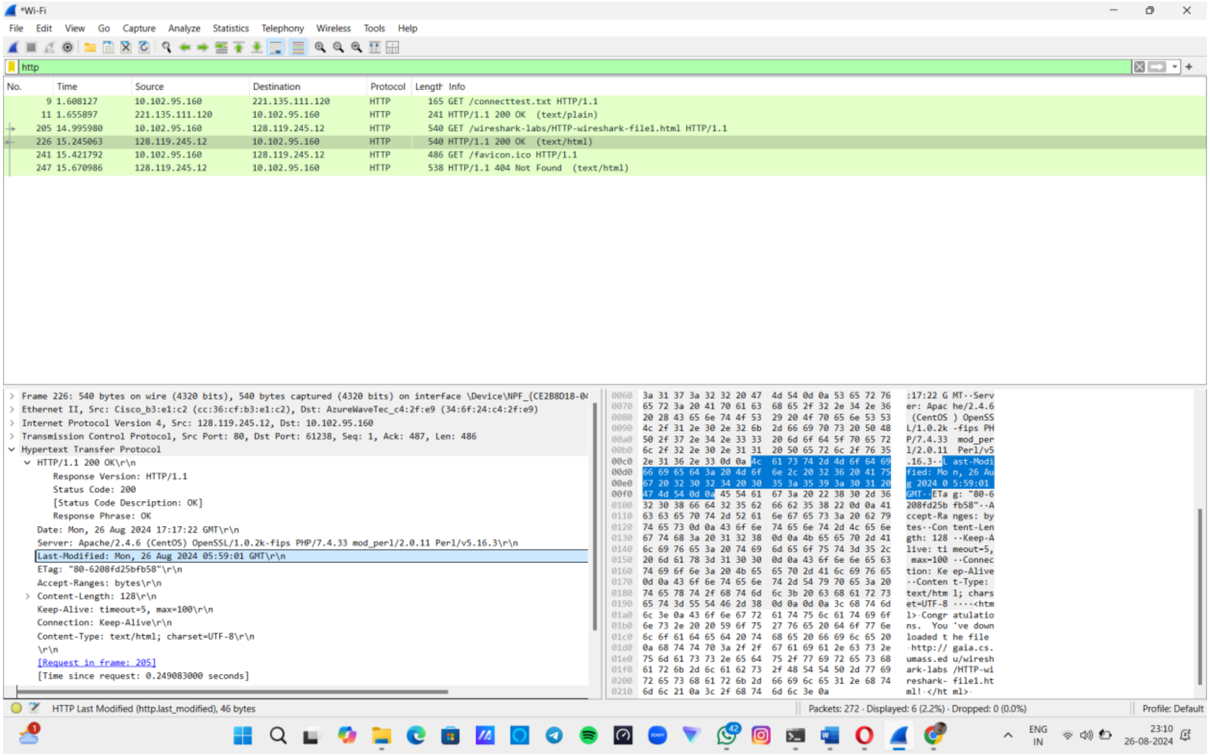
HTTP Response Status Code (http.response.code), 3 bytes

Packets: 272 · Displayed: 6 (2.2%) · Dropped: 0 (0.0%)

Status code is 200

5. When was the HTML file that you are retrieving last modified at the server?

Answer:



```
http
```

```
No.    Time        Source            Destination       Protocol  Length  Info
     9 1.608127    10.102.95.160     221.135.111.120   HTTP       165 GET /connecttest.txt HTTP/1.1
    11 1.655897    221.135.111.120   10.102.95.160     HTTP       241 HTTP/1.1 200 OK  (text/plain)
   205 14.995980   10.102.95.160     128.119.245.12    HTTP       540 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   226 15.245063   128.119.245.12    10.102.95.160     HTTP       540 HTTP/1.1 200 OK  (text/html)
   241 15.421792   10.102.95.160     128.119.245.12    HTTP       486 GET /favicon.ico HTTP/1.1
   247 15.670986   128.119.245.12    10.102.95.160     HTTP       538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 226: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{CE2B8D18-04
> Ethernet II, Src: Cisco_b3:e1:c2 (cc:36:cf:b3:e1:c2), Dst: AzureWaveTec_c4:2f:e9 (34:6f:24:c4:2f:e9)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.102.95.160
> Transmission Control Protocol, Src Port: 80, Dst Port: 61238, Seq: 1, Ack: 487, Len: 486
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Mon, 26 Aug 2024 17:17:22 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: Mon, 26 Aug 2024 05:59:01 GMT\r\n
    ETag: "80-6208fd25bfb58"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 128\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
    [Request in frame: 205]
    [Time since request: 0.249083000 seconds]
```

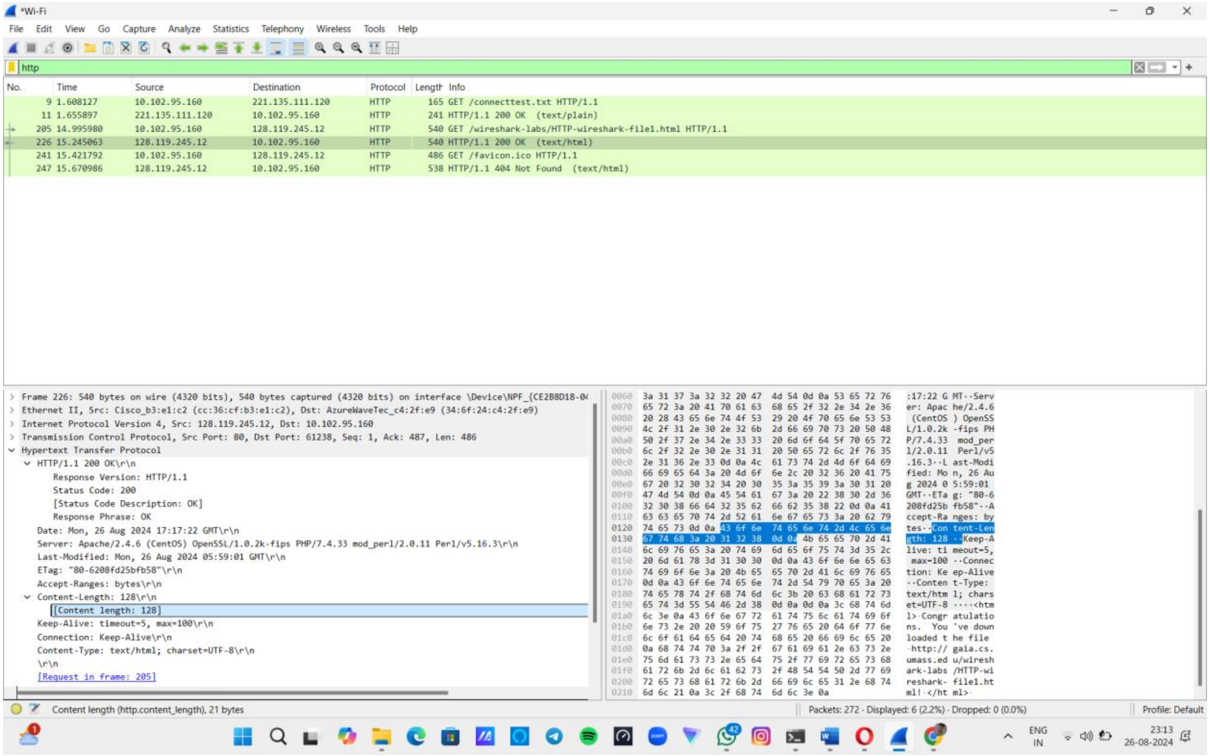
```
0060  3a 31 37 3a 32 32 20 47  4d 54 0d 0a 53 65 72 76   :17:22 G MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apac he/2.4.6
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentOS ) OpenSS
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73 20 50 48   L/1.0.2k -fips 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 4d 6f  6e 2c 20 32 36 20 41 75   fied: Mo n, 26 Au
00e0  67 20 32 30 32 34 20 30  35 3a 35 39 3a 30 31 20   g 2024 0 5:59:01 
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 38 30 2d 36   GMT··ETa g: "80-6
0100  32 30 38 66 64 32 35 62  66 62 35 38 22 0d 0a 41   208fd25b fb58"··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 31 32 38  0d 0a 4b 65 65 70 2d 41   gth: 128 ··Keep-A
0140  6c 69 76 65 3a 20 74 69  6d 65 6f 75 74 3d 35 2c   live: ti meout=5,
0150  20 6d 61 78 3d 31 30 30  0d 0a 43 6f 6e 6e 65 63    max=100 ··Connec
0160  74 69 6f 6e 3a 20 4b 65  65 70 2d 41 6c 69 76 65   tion: Ke ep-Alive
0170  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ··Conten t-Type: 
0180  74 65 78 74 2f 68 74 6d  6c 3b 20 63 68 61 72 73   text/htm l; chars
0190  65 74 3d 55 54 46 2d 38  0d 0a 0d 0a 3c 68 74 6d   et=UTF-8 ····<htm
01a0  6c 3e 0a 43 6f 6e 67 72  61 74 75 6c 61 74 69 6f   l>·Congr atulatio
01b0  6e 73 2e 20 20 59 6f 75  27 76 65 20 64 6f 77 6e   ns.  You 've down
01c0  6c 6f 61 64 65 64 20 74  68 65 20 66 69 6c 65 20   loaded t he file 
01d0  0a 68 74 74 70 3a 2f 2f  67 61 69 61 2e 63 73 2e   ·http:// gaia.cs.
01e0  75 6d 61 73 73 2e 65 64  75 2f 77 69 72 65 73 68   umass.ed u/wiresh
01f0  61 72 6b 2d 6c 61 62 73  2f 48 54 54 50 2d 77 69   ark-labs /HTTP-wi
0200  72 65 73 68 61 72 6b 2d  66 69 6c 65 31 2e 68 74   reshark- file1.ht
0210  6d 6c 21 0a 3c 2f 68 74  6d 6c 3e 0a               ml!·</ht ml>·
```

```
HTTP Last Modified (http.last_modified), 46 bytes    Packets: 272 · Displayed: 6 (2.2%) · Dropped: 0 (0.0%)    Profile: Default
```

Last Modified:Mon,26 Aug,2024

6. How many bytes of content are being returned to your browser?

Answer:


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

```
No.   Time        Source           Destination      Protocol Length Info
    9 1.608127    10.102.95.160    221.135.111.120  HTTP      165 GET /connecttest.txt HTTP/1.1
   11 1.655897    221.135.111.120  10.102.95.160    HTTP      241 HTTP/1.1 200 OK  (text/plain)
  205 14.995980   10.102.95.160    128.119.245.12   HTTP      540 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  226 15.245063   128.119.245.12   10.102.95.160    HTTP      540 HTTP/1.1 200 OK  (text/html)
  241 15.421792   10.102.95.160    128.119.245.12   HTTP      486 GET /favicon.ico HTTP/1.1
  247 15.670986   128.119.245.12   10.102.95.160    HTTP      538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 226: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{CE2B8D18-0
> Ethernet II, Src: Cisco_b3:e1:c2 (cc:36:cf:b3:e1:c2), Dst: AzureWaveTec_c4:2f:e9 (34:6f:24:c4:2f:e9)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.102.95.160
> Transmission Control Protocol, Src Port: 80, Dst Port: 61238, Seq: 1, Ack: 487, Len: 486
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Mon, 26 Aug 2024 17:17:22 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: Mon, 26 Aug 2024 05:59:01 GMT\r\n
    ETag: "80-6208fd25bfb58"\r\n
    Accept-Ranges: bytes\r\n
  v Content-Length: 128\r\n
        [Content length: 128]
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [Request in frame: 205]
```

```
0060  3a 31 37 3a 32 32 20 47  4d 54 0d 0a 53 65 72 76   :17:22 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 4d 6f  6e 2c 20 32 36 20 41 75   fied: Mo n, 26 Au
00e0  67 20 32 30 32 34 20 30  35 3a 35 39 3a 30 31 20   g 2024 0 5:59:01 
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 38 30 2d 36   GMT··ETa g: "80-6
0100  32 30 38 66 64 32 35 62  66 62 35 38 22 0d 0a 41   208fd25b fb58"··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 31 32 38  0d 0a 4b 65 65 70 2d 41   gth: 128 ··Keep-A
0140  6c 69 76 65 3a 20 74 69  6d 65 6f 75 74 3d 35 2c   live: ti meout=5,
0150  20 6d 61 78 3d 31 30 30  0d 0a 43 6f 6e 6e 65 63    max=100 ··Connec
0160  74 69 6f 6e 3a 20 4b 65  65 70 2d 41 6c 69 76 65   tion: Ke ep-Alive
0170  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ··Conten t-Type: 
0180  74 65 78 74 2f 68 74 6d  6c 3b 20 63 68 61 72 73   text/htm l; chars
0190  65 74 3d 55 54 46 2d 38  0d 0a 0d 0a 3c 68 74 6d   et=UTF-8 ····<htm
01a0  6c 3e 0a 43 6f 6e 67 72  61 74 75 6c 61 74 69 6f   l>·Congr atulatio
01b0  6e 73 2e 20 20 59 6f 75  27 76 65 20 64 6f 77 6e   ns.  You 've down
01c0  6c 6f 61 64 65 64 20 74  68 65 20 66 69 6c 65 20   loaded t he file 
01d0  0a 68 74 74 70 3a 2f 2f  67 61 69 61 2e 63 73 2e   ·http:// gaia.cs.
01e0  75 6d 61 73 73 2e 65 64  75 2f 77 69 72 65 73 68   umass.ed u/wiresh
01f0  61 72 6b 2d 6c 61 62 73  2f 48 54 54 50 2d 77 69   ark-labs /HTTP-wi
0200  72 65 73 68 61 72 6b 2d  66 69 6c 65 31 2e 68 74   reshark- file1.ht
0210  6d 6c 21 0a 3c 2f 68 74  6d 6c 3e 0a               ml!·</ht ml>·
```

Content length (http.content_length), 21 bytes

Packets: 272 · Displayed: 6 (2.2%) · Dropped: 0 (0.0%)

Profile: Default

Content Length – 128

7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

Answer:

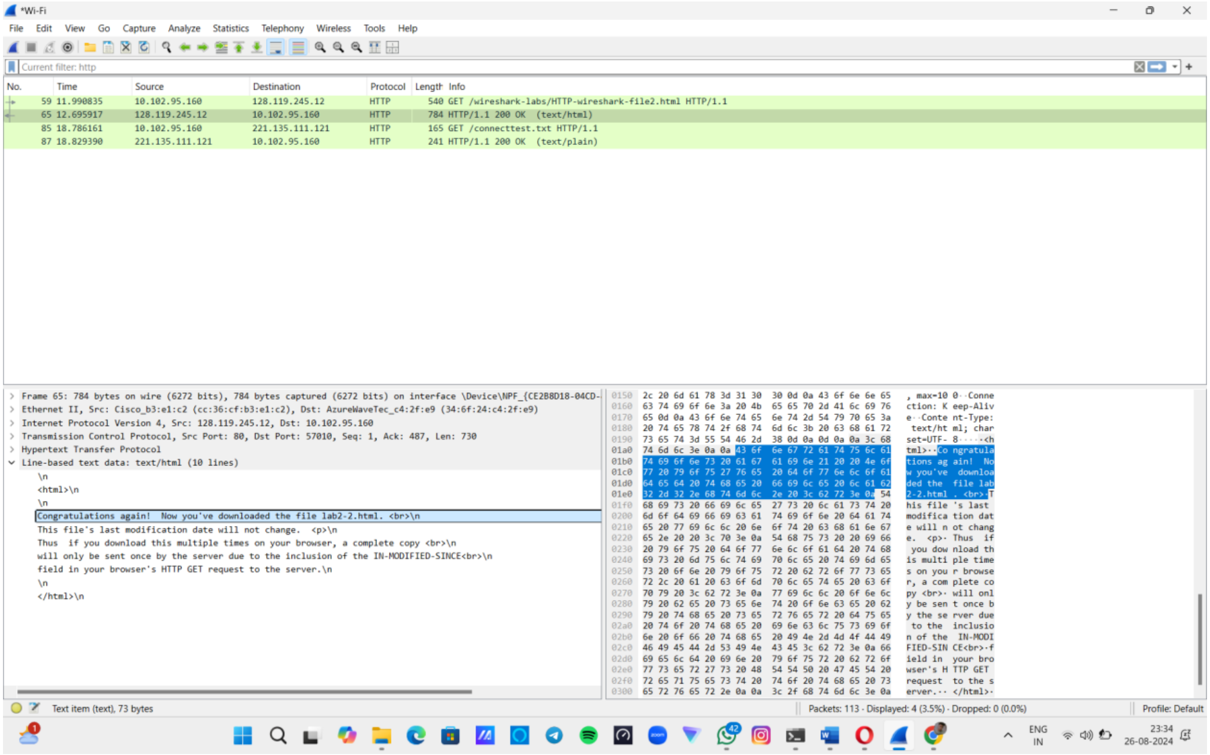
NO

8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

NO

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Answer:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Current filter: http

```
No.   Time        Source           Destination      Protocol  Length  Info
   59 11.990835   10.102.95.160    128.119.245.12   HTTP       540 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   65 12.695917   128.119.245.12   10.102.95.160    HTTP       784 HTTP/1.1 200 OK  (text/html)
   85 18.786161   10.102.95.160    221.135.111.121  HTTP       165 GET /connecttest.txt HTTP/1.1
   87 18.829390   221.135.111.121  10.102.95.160    HTTP       241 HTTP/1.1 200 OK  (text/plain)
```

```
> Frame 65: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{CE2B8D18-04CD-
> Ethernet II, Src: Cisco_b3:e1:c2 (cc:36:cf:b3:e1:c2), Dst: AzureWaveTec_c4:2f:e9 (34:6f:24:c4:2f:e9)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.102.95.160
> Transmission Control Protocol, Src Port: 80, Dst Port: 57010, Seq: 1, Ack: 487, Len: 730
> Hypertext Transfer Protocol
v Line-based text data: text/html (10 lines)
     \n
     <html>\n
     \n
     Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
     This file's last modification date will not change.  <p>\n
     Thus  if you download this multiple times on your browser, a complete copy <br>\n
     will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
     field in your browser's HTTP GET request to the server.\n
     \n
     </html>\n
```

```
0150  2c 20 6d 61 78 3d 31 30  30 0d 0a 43 6f 6e 6e 65   , max=10 0··Conne
0160  63 74 69 6f 6e 3a 20 4b  65 65 70 2d 41 6c 69 76   ction: K eep-Aliv
0170  65 0d 0a 43 6f 6e 74 65  6e 74 2d 54 79 70 65 3a   e··Conte nt-Type:
0180  20 74 65 78 74 2f 68 74  6d 6c 3b 20 63 68 61 72    text/ht ml; char
0190  73 65 74 3d 55 54 46 2d  38 0d 0a 0d 0a 0a 3c 68   set=UTF- 8·····<h
01a0  74 6d 6c 3e 0a 0a 43 6f  6e 67 72 61 74 75 6c 61   tml>··Co ngratula
01b0  74 69 6f 6e 73 20 61 67  61 69 6e 21 20 20 4e 6f   tions ag ain!  No
01c0  77 20 79 6f 75 27 76 65  20 64 6f 77 6e 6c 6f 61   w you've  downloa
01d0  64 65 64 20 74 68 65 20  66 69 6c 65 20 6c 61 62   ded the  file lab
01e0  32 2d 32 2e 68 74 6d 6c  2e 20 3c 62 72 3e 0a 54   2-2.html . <br>·T
01f0  68 69 73 20 66 69 6c 65  27 73 20 6c 61 73 74 20   his file 's last 
0200  6d 6f 64 69 66 69 63 61  74 69 6f 6e 20 64 61 74   modifica tion dat
0210  65 20 77 69 6c 6c 20 6e  6f 74 20 63 68 61 6e 67   e will n ot chang
0220  65 2e 20 20 3c 70 3e 0a  54 68 75 73 20 20 69 66   e.  <p>· Thus  if
0230  20 79 6f 75 20 64 6f 77  6e 6c 6f 61 64 20 74 68    you dow nload th
0240  69 73 20 6d 75 6c 74 69  70 6c 65 20 74 69 6d 65   is multi ple time
0250  73 20 6f 6e 20 79 6f 75  72 20 62 72 6f 77 73 65   s on you r browse
0260  72 2c 20 61 20 63 6f 6d  70 6c 65 74 65 20 63 6f   r, a com plete co
0270  70 79 20 3c 62 72 3e 0a  77 69 6c 6c 20 6f 6e 6c   py <br>· will onl
0280  79 20 62 65 20 73 65 6e  74 20 6f 6e 63 65 20 62   y be sen t once b
0290  79 20 74 68 65 20 73 65  72 76 65 72 20 64 75 65   y the se rver due
02a0  20 74 6f 20 74 68 65 20  69 6e 63 6c 75 73 69 6f    to the  inclusio
02b0  6e 20 6f 66 20 74 68 65  20 49 4e 2d 4d 4f 44 49   n of the  IN-MODI
02c0  46 49 45 44 2d 53 49 4e  43 45 3c 62 72 3e 0a 66   FIED-SIN CE<br>·f
02d0  69 65 6c 64 20 69 6e 20  79 6f 75 72 20 62 72 6f   ield in  your bro
02e0  77 73 65 72 27 73 20 48  54 54 50 20 47 45 54 20   wser's H TTP GET 
02f0  72 65 71 75 65 73 74 20  74 6f 20 74 68 65 20 73   request  to the s
0300  65 72 76 65 72 2e 0a 0a  3c 2f 68 74 6d 6c 3e 0a   erver.·· </html>·
```

Text item (text), 73 bytes

Packets: 113 · Displayed: 4 (3.5%) · Dropped: 0 (0.0%)

Profile: Default

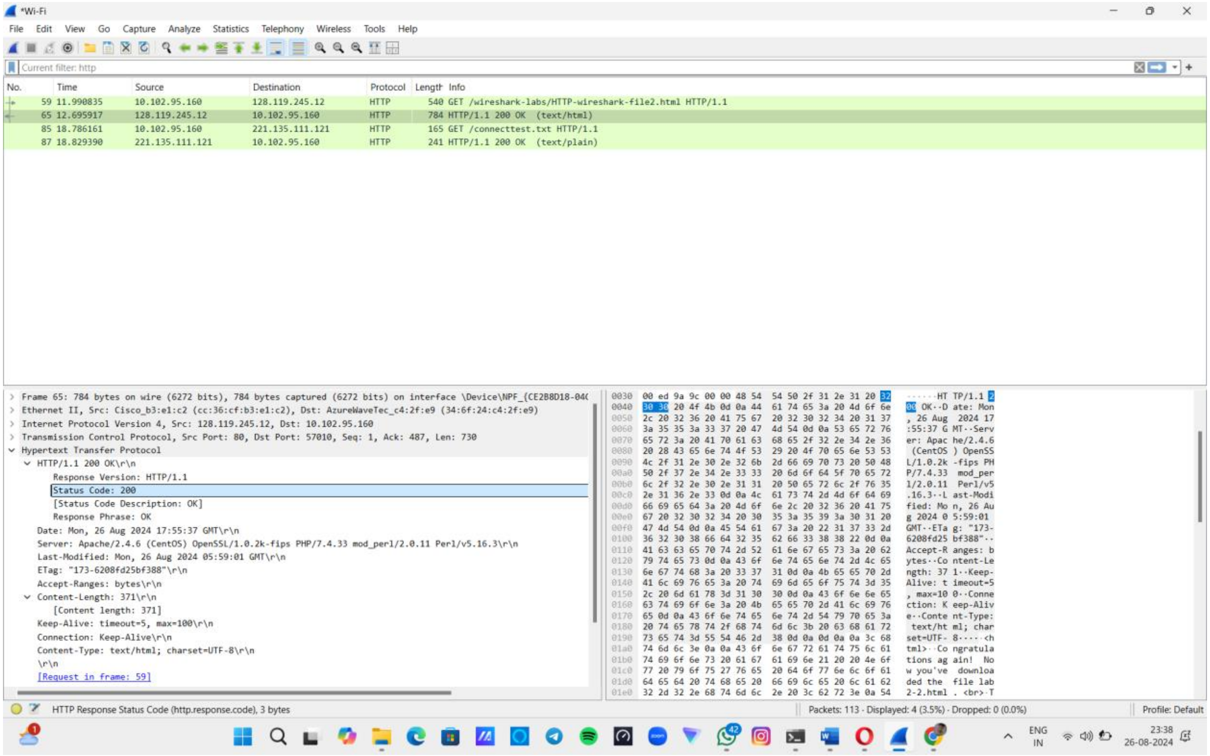
10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Answer:

NO

11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

Answer:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Current filter: http

```
No.   Time        Source            Destination       Protocol  Length Info
   59 11.990835   10.102.95.160     128.119.245.12    HTTP       540 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   65 12.695917   128.119.245.12    10.102.95.160     HTTP       784 HTTP/1.1 200 OK  (text/html)
   85 18.786161   10.102.95.160     221.135.111.121   HTTP       165 GET /connecttest.txt HTTP/1.1
   87 18.829390   221.135.111.121   10.102.95.160     HTTP       241 HTTP/1.1 200 OK  (text/plain)
```

```
> Frame 65: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{CE2B8D18-04(
> Ethernet II, Src: Cisco_b3:e1:c2 (cc:36:cf:b3:e1:c2), Dst: AzureWaveTec_c4:2f:e9 (34:6f:24:c4:2f:e9)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.102.95.160
> Transmission Control Protocol, Src Port: 80, Dst Port: 57010, Seq: 1, Ack: 487, Len: 730
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Mon, 26 Aug 2024 17:55:37 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: Mon, 26 Aug 2024 05:59:01 GMT\r\n
    ETag: "173-6208fd25bf388"\r\n
    Accept-Ranges: bytes\r\n
  v Content-Length: 371\r\n
      [Content length: 371]
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [Request in frame: 59]
```

```
0030  00 ed 9a 9c 00 00 48 54  54 50 2f 31 2e 31 20 32   ······HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 4d 6f 6e   00 OK··D ate: Mon
0050  2c 20 32 36 20 41 75 67  20 32 30 32 34 20 31 37   , 26 Aug  2024 17
0060  3a 35 35 3a 33 37 20 47  4d 54 0d 0a 53 65 72 76   :55:37 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 4d 6f  6e 2c 20 32 36 20 41 75   fied: Mo n, 26 Au
00e0  67 20 32 30 32 34 20 30  35 3a 35 39 3a 30 31 20   g 2024 0 5:59:01 
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 31 37 33 2d   GMT··ETa g: "173-
0100  36 32 30 38 66 64 32 35  62 66 33 38 38 22 0d 0a   6208fd25 bf388"··
0110  41 63 63 65 70 74 2d 52  61 6e 67 65 73 3a 20 62   Accept-R anges: b
0120  79 74 65 73 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   ytes··Co ntent-Le
0130  6e 67 74 68 3a 20 33 37  31 0d 0a 4b 65 65 70 2d   ngth: 37 1··Keep-
0140  41 6c 69 76 65 3a 20 74  69 6d 65 6f 75 74 3d 35   Alive: t imeout=5
0150  2c 20 6d 61 78 3d 31 30  30 0d 0a 43 6f 6e 6e 65   , max=10 0··Conne
0160  63 74 69 6f 6e 3a 20 4b  65 65 70 2d 41 6c 69 76   ction: K eep-Aliv
0170  65 0d 0a 43 6f 6e 74 65  6e 74 2d 54 79 70 65 3a   e··Conte nt-Type:
0180  20 74 65 78 74 2f 68 74  6d 6c 3b 20 63 68 61 72    text/ht ml; char
0190  73 65 74 3d 55 54 46 2d  38 0d 0a 0d 0a 0a 3c 68   set=UTF- 8·····<h
01a0  74 6d 6c 3e 0a 0a 43 6f  6e 67 72 61 74 75 6c 61   tml>··Co ngratula
01b0  74 69 6f 6e 73 20 61 67  61 69 6e 21 20 20 4e 6f   tions ag ain!  No
01c0  77 20 79 6f 75 27 76 65  20 64 6f 77 6e 6c 6f 61   w you've  downloa
01d0  64 65 64 20 74 68 65 20  66 69 6c 65 20 6c 61 62   ded the  file lab
01e0  32 2d 32 2e 68 74 6d 6c  2e 20 3c 62 72 3e 0a 54   2-2.html . <br>·T
```

HTTP Response Status Code (http.response.code), 3 bytes

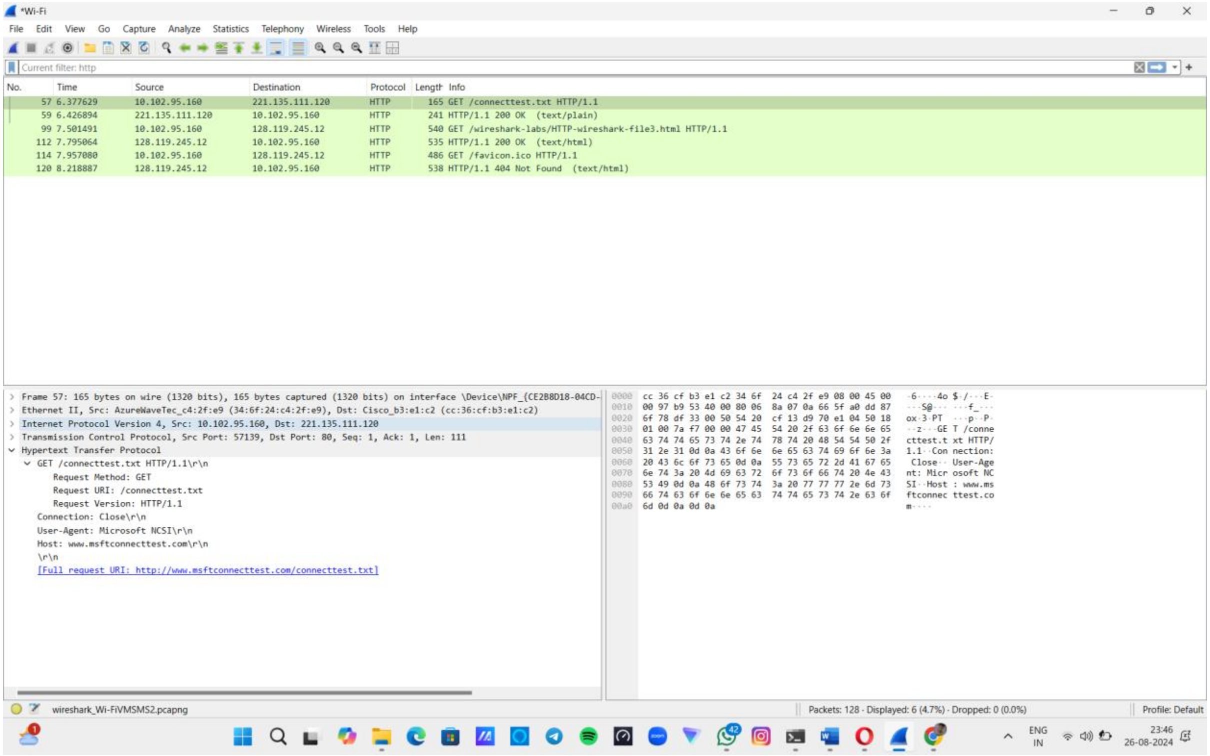
Packets: 113 · Displayed: 4 (3.5%) · Dropped: 0 (0.0%)

Profile: Default

Status Code-200,Phase:OK

12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

Answer:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Current filter: http

```
No.   Time      Source           Destination      Protocol Length Info
   57 6.377629  10.102.95.160    221.135.111.120  HTTP     165 GET /connecttest.txt HTTP/1.1
   59 6.426894  221.135.111.120  10.102.95.160    HTTP     241 HTTP/1.1 200 OK  (text/plain)
   99 7.501491  10.102.95.160    128.119.245.12   HTTP     540 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  112 7.795064  128.119.245.12   10.102.95.160    HTTP     535 HTTP/1.1 200 OK  (text/html)
  114 7.957080  10.102.95.160    128.119.245.12   HTTP     486 GET /favicon.ico HTTP/1.1
  120 8.218887  128.119.245.12   10.102.95.160    HTTP     538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 57: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface \Device\NPF_{CE2B8D18-04CD-
> Ethernet II, Src: AzureWaveTec_c4:2f:e9 (34:6f:24:c4:2f:e9), Dst: Cisco_b3:e1:c2 (cc:36:cf:b3:e1:c2)
> Internet Protocol Version 4, Src: 10.102.95.160, Dst: 221.135.111.120
> Transmission Control Protocol, Src Port: 57139, Dst Port: 80, Seq: 1, Ack: 1, Len: 111
v Hypertext Transfer Protocol
  v GET /connecttest.txt HTTP/1.1\r\n
      Request Method: GET
      Request URI: /connecttest.txt
      Request Version: HTTP/1.1
    Connection: Close\r\n
    User-Agent: Microsoft NCSI\r\n
    Host: www.msftconnecttest.com\r\n
    \r\n
    [Full request URI: http://www.msftconnecttest.com/connecttest.txt]
```

```
0000  cc 36 cf b3 e1 c2 34 6f  24 c4 2f e9 08 00 45 00   ·6····4o $·/···E·
0010  00 97 b9 53 40 00 80 06  8a 07 0a 66 5f a0 dd 87   ···S@··· ···f_···
0020  6f 78 df 33 00 50 54 20  cf 13 d9 70 e1 04 50 18   ox·3·PT  ···p··P·
0030  01 00 7a f7 00 00 47 45  54 20 2f 63 6f 6e 6e 65   ··z···GE T /conne
0040  63 74 74 65 73 74 2e 74  78 74 20 48 54 54 50 2f   cttest.t xt HTTP/
0050  31 2e 31 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a   1.1··Con nection:
0060  20 43 6c 6f 73 65 0d 0a  55 73 65 72 2d 41 67 65    Close·· User-Age
0070  6e 74 3a 20 4d 69 63 72  6f 73 6f 66 74 20 4e 43   nt: Micr osoft NC
0080  53 49 0d 0a 48 6f 73 74  3a 20 77 77 77 2e 6d 73   SI··Host : www.ms
0090  66 74 63 6f 6e 6e 65 63  74 74 65 73 74 2e 63 6f   ftconnec ttest.co
00a0  6d 0d 0a 0d 0a                                     m····
```

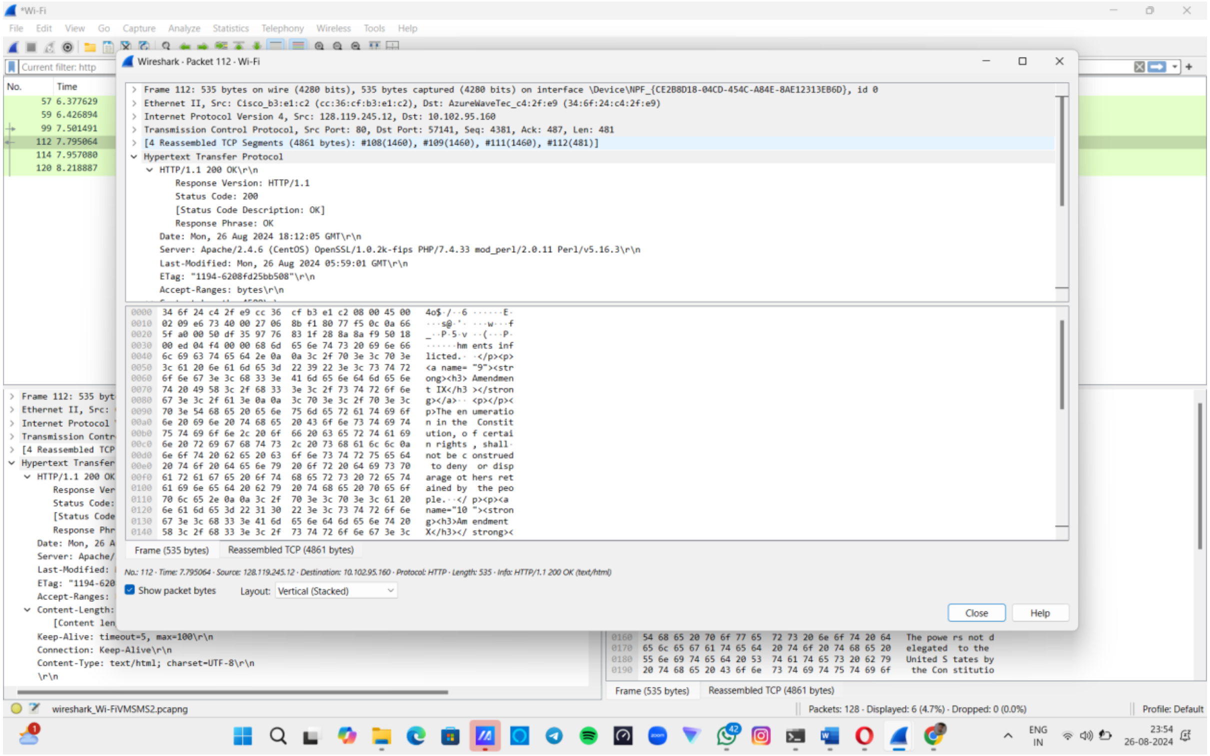
```
wireshark_Wi-FiVMSMS2.pcapng    Packets: 128 · Displayed: 6 (4.7%) · Dropped: 0 (0.0%)    Profile: Default
```

The Browser sent 3 HTTP requests.

Packet number 99

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Answer:



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Current filter: http
Wireshark · Packet 112 · Wi-Fi

```
No.   Time
 57 6.377629
 59 6.426894
 99 7.501491
112 7.795064
114 7.957080
120 8.218887
```

```
> Frame 112: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{CE2B8D18-04CD-454C-A84E-8AE12313EB6D}, id 0
> Ethernet II, Src: Cisco_b3:e1:c2 (cc:36:cf:b3:e1:c2), Dst: AzureWaveTec_c4:2f:e9 (34:6f:24:c4:2f:e9)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.102.95.160
> Transmission Control Protocol, Src Port: 80, Dst Port: 57141, Seq: 4381, Ack: 487, Len: 481
> [4 Reassembled TCP Segments (4861 bytes): #108(1460), #109(1460), #111(1460), #112(481)]
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Mon, 26 Aug 2024 18:12:05 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: Mon, 26 Aug 2024 05:59:01 GMT\r\n
    ETag: "1194-6208fd25bb508"\r\n
    Accept-Ranges: bytes\r\n
```

```
0000  34 6f 24 c4 2f e9 cc 36  cf b3 e1 c2 08 00 45 00   4o$·/··6 ······E·
0010  02 09 e6 73 40 00 27 06  8b f1 80 77 f5 0c 0a 66   ···s@·'· ···w···f
0020  5f a0 00 50 df 35 97 76  83 1f 28 8a 8a f9 50 18   _··P·5·v ··(···P·
0030  00 ed 04 f4 00 00 68 6d  65 6e 74 73 20 69 6e 66   ······hm ents inf
0040  6c 69 63 74 65 64 2e 0a  0a 3c 2f 70 3e 3c 70 3e   licted.· ·</p><p>
0050  3c 61 20 6e 61 6d 65 3d  22 39 22 3e 3c 73 74 72   <a name= "9"><str
0060  6f 6e 67 3e 3c 68 33 3e  41 6d 65 6e 64 6d 65 6e   ong><h3> Amendmen
0070  74 20 49 58 3c 2f 68 33  3e 3c 2f 73 74 72 6f 6e   t IX</h3 ></stron
0080  67 3e 3c 2f 61 3e 0a 0a  3c 70 3e 3c 2f 70 3e 3c   g></a>·· <p></p><
0090  70 3e 54 68 65 20 65 6e  75 6d 65 72 61 74 69 6f   p>The en umeratio
00a0  6e 20 69 6e 20 74 68 65  20 43 6f 6e 73 74 69 74   n in the  Constit
00b0  75 74 69 6f 6e 2c 20 6f  66 20 63 65 72 74 61 69   ution, o f certai
00c0  6e 20 72 69 67 68 74 73  2c 20 73 68 61 6c 6c 0a   n rights , shall·
00d0  6e 6f 74 20 62 65 20 63  6f 6e 73 74 72 75 65 64   not be c onstrued
00e0  20 74 6f 20 64 65 6e 79  20 6f 72 20 64 69 73 70    to deny  or disp
00f0  61 72 61 67 65 20 6f 74  68 65 72 73 20 72 65 74   arage ot hers ret
0100  61 69 6e 65 64 20 62 79  20 74 68 65 20 70 65 6f   ained by  the peo
0110  70 6c 65 2e 0a 0a 3c 2f  70 3e 3c 70 3e 3c 61 20   ple.··</ p><p><a 
0120  6e 61 6d 65 3d 22 31 30  22 3e 3c 73 74 72 6f 6e   name="10 "><stron
0130  67 3e 3c 68 33 3e 41 6d  65 6e 64 6d 65 6e 74 20   g><h3>Am endment 
0140  58 3c 2f 68 33 3e 3c 2f  73 74 72 6f 6e 67 3e 3c   X</h3></ strong><
```

No.: 112 · Time: 7.795064 · Source: 128.119.245.12 · Destination: 10.102.95.160 · Protocol: HTTP · Length: 535 · Info: HTTP/1.1 200 OK (text/html)

☑ Show packet bytes   Layout: Vertical (Stacked)

```
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
```

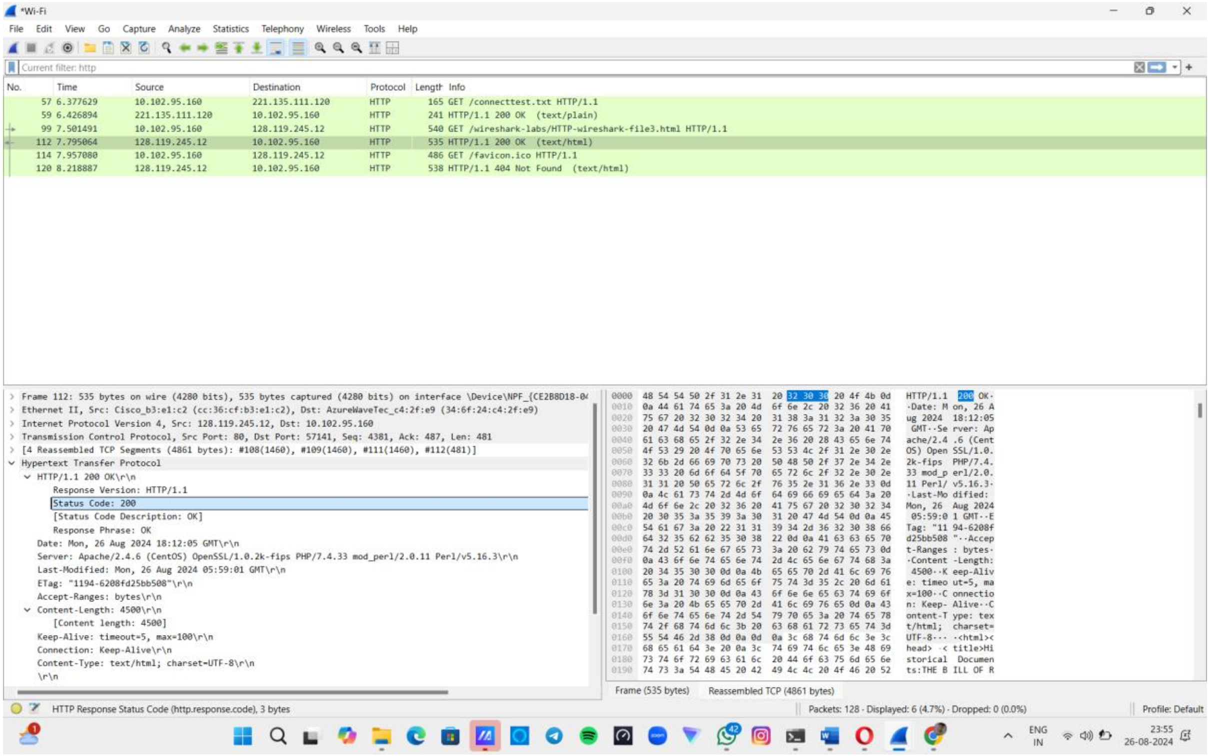
```
0160  54 68 65 20 70 6f 77 65  72 73 20 6e 6f 74 20 64   The powe rs not d
0170  65 6c 65 67 61 74 65 64  20 74 6f 20 74 68 65 20   elegated  to the 
0180  55 6e 69 74 65 64 20 53  74 61 74 65 73 20 62 79   United S tates by
0190  20 74 68 65 20 43 6f 6e  73 74 69 74 75 74 69 6f    the Con stitutio
```

wireshark_Wi-FiVMSMS2.pcapng
Packets: 128 · Displayed: 6 (4.7%) · Dropped: 0 (0.0%)
Profile: Default
ENG
IN
23:54
26-08-2024

Packet number 112 contains the given data

14. What is the status code and phrase in the response?

Answer:



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

Current filter: http

```
No.   Time        Source            Destination       Protocol  Length Info
   57 6.377629    10.102.95.160     221.135.111.120   HTTP       165 GET /connecttest.txt HTTP/1.1
   59 6.426894    221.135.111.120   10.102.95.160     HTTP       241 HTTP/1.1 200 OK  (text/plain)
   99 7.501491    10.102.95.160     128.119.245.12    HTTP       540 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  112 7.795064    128.119.245.12    10.102.95.160     HTTP       535 HTTP/1.1 200 OK  (text/html)
  114 7.957080    10.102.95.160     128.119.245.12    HTTP       486 GET /favicon.ico HTTP/1.1
  120 8.218887    128.119.245.12    10.102.95.160     HTTP       538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 112: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{CE2B8D18-0
> Ethernet II, Src: Cisco_b3:e1:c2 (cc:36:cf:b3:e1:c2), Dst: AzureWaveTec_c4:2f:e9 (34:6f:24:c4:2f:e9)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.102.95.160
> Transmission Control Protocol, Src Port: 80, Dst Port: 57141, Seq: 4381, Ack: 487, Len: 481
> [4 Reassembled TCP Segments (4861 bytes): #108(1460), #109(1460), #111(1460), #112(481)]
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Mon, 26 Aug 2024 18:12:05 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: Mon, 26 Aug 2024 05:59:01 GMT\r\n
    ETag: "1194-6208fd25bb508"\r\n
    Accept-Ranges: bytes\r\n
  v Content-Length: 4500\r\n
      [Content length: 4500]
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
```

```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK·
0010  0a 44 61 74 65 3a 20 4d  6f 6e 2c 20 32 36 20 41   ·Date: M on, 26 A
0020  75 67 20 32 30 32 34 20  31 38 3a 31 32 3a 30 35   ug 2024  18:12:05
0030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
0040  61 63 68 65 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0050  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
0060  32 6b 2d 66 69 70 73 20  50 48 50 2f 37 2e 34 2e   2k-fips  PHP/7.4.
0070  33 33 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   33 mod_p erl/2.0.
0080  31 31 20 50 65 72 6c 2f  76 35 2e 31 36 2e 33 0d   11 Perl/ v5.16.3·
0090  0a 4c 61 73 74 2d 4d 6f  64 69 66 69 65 64 3a 20   ·Last-Mo dified: 
00a0  4d 6f 6e 2c 20 32 36 20  41 75 67 20 32 30 32 34   Mon, 26  Aug 2024
00b0  20 30 35 3a 35 39 3a 30  31 20 47 4d 54 0d 0a 45    05:59:0 1 GMT··E
00c0  54 61 67 3a 20 22 31 31  39 34 2d 36 32 30 38 66   Tag: "11 94-6208f
00d0  64 32 35 62 62 35 30 38  22 0d 0a 41 63 63 65 70   d25bb508 "··Accep
00e0  74 2d 52 61 6e 67 65 73  3a 20 62 79 74 65 73 0d   t-Ranges : bytes·
00f0  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   ·Content -Length:
0100  20 34 35 30 30 0d 0a 4b  65 65 70 2d 41 6c 69 76    4500··K eep-Aliv
0110  65 3a 20 74 69 6d 65 6f  75 74 3d 35 2c 20 6d 61   e: timeo ut=5, ma
0120  78 3d 31 30 30 0d 0a 43  6f 6e 6e 65 63 74 69 6f   x=100··C onnectio
0130  6e 3a 20 4b 65 65 70 2d  41 6c 69 76 65 0d 0a 43   n: Keep- Alive··C
0140  6f 6e 74 65 6e 74 2d 54  79 70 65 3a 20 74 65 78   ontent-T ype: tex
0150  74 2f 68 74 6d 6c 3b 20  63 68 61 72 73 65 74 3d   t/html;  charset=
0160  55 54 46 2d 38 0d 0a 0d  0a 3c 68 74 6d 6c 3e 3c   UTF-8··· ·<html><
0170  68 65 61 64 3e 20 0a 3c  74 69 74 6c 65 3e 48 69   head> ·< title>Hi
0180  73 74 6f 72 69 63 61 6c  20 44 6f 63 75 6d 65 6e   storical  Documen
0190  74 73 3a 54 48 45 20 42  49 4c 4c 20 4f 46 20 52   ts:THE B ILL OF R
```

Frame (535 bytes) Reassembled TCP (4861 bytes)

HTTP Response Status Code (http.response.code), 3 bytes

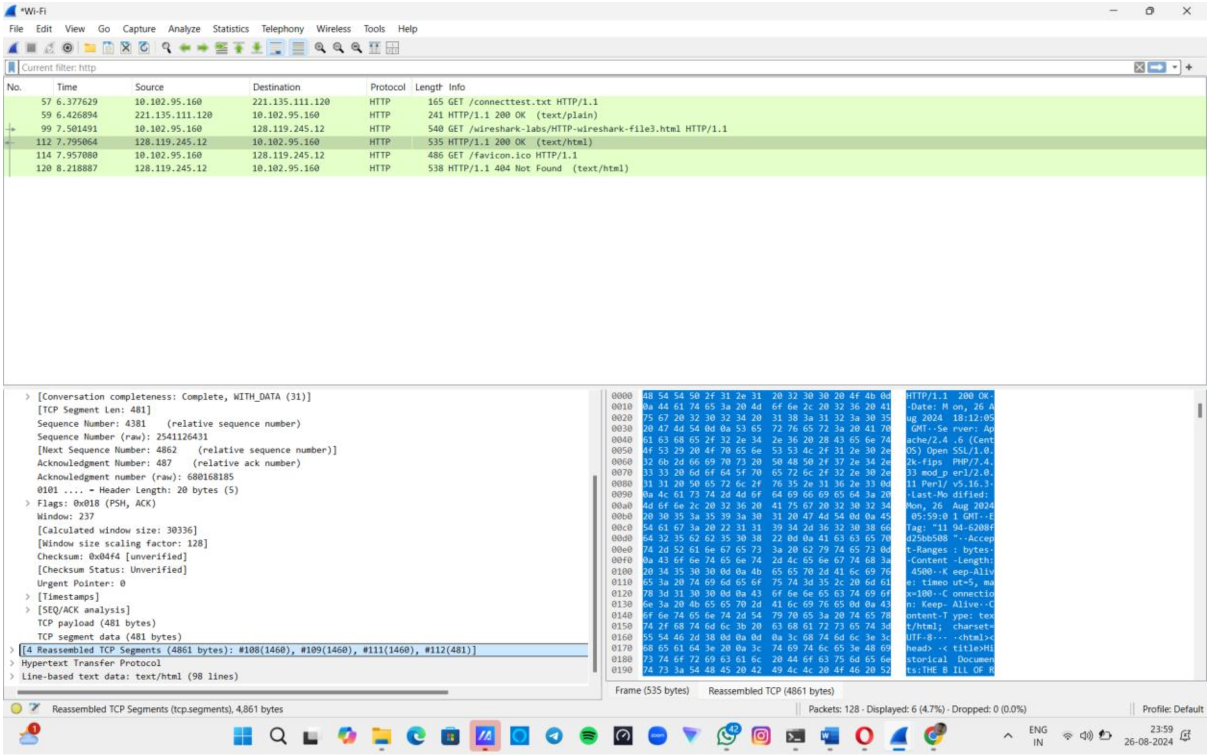
Packets: 128 · Displayed: 6 (4.7%) · Dropped: 0 (0.0%)

Profile: Default

Status code-200,the phase is OK

15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

Answer:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ENG IN
23:59
26-08-2024

Current filter: http

```
No.     Time        Source            Destination       Protocol  Length Info
     57 6.377629    10.102.95.160     221.135.111.120   HTTP       165 GET /connecttest.txt HTTP/1.1
     59 6.426894    221.135.111.120   10.102.95.160     HTTP       241 HTTP/1.1 200 OK  (text/plain)
     99 7.501491    10.102.95.160     128.119.245.12    HTTP       540 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
    112 7.795064    128.119.245.12    10.102.95.160     HTTP       535 HTTP/1.1 200 OK  (text/html)
    114 7.957080    10.102.95.160     128.119.245.12    HTTP       486 GET /favicon.ico HTTP/1.1
    120 8.218887    128.119.245.12    10.102.95.160     HTTP       538 HTTP/1.1 404 Not Found  (text/html)
```

```
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 481]
    Sequence Number: 4381    (relative sequence number)
    Sequence Number (raw): 2541126431
    [Next Sequence Number: 4862    (relative sequence number)]
    Acknowledgment Number: 487    (relative ack number)
    Acknowledgment number (raw): 680168185
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0x04f4 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (481 bytes)
    TCP segment data (481 bytes)
> [4 Reassembled TCP Segments (4861 bytes): #108(1460), #109(1460), #111(1460), #112(481)]
> Hypertext Transfer Protocol
> Line-based text data: text/html (98 lines)
```

```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK·
0010  0a 44 61 74 65 3a 20 4d  6f 6e 2c 20 32 36 20 41   ·Date: M on, 26 A
0020  75 67 20 32 30 32 34 20  31 38 3a 31 32 3a 30 35   ug 2024  18:12:05
0030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
0040  61 63 68 65 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0050  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
0060  32 6b 2d 66 69 70 73 20  50 48 50 2f 37 2e 34 2e   2k-fips  PHP/7.4.
0070  33 33 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   33 mod_p erl/2.0.
0080  31 31 20 50 65 72 6c 2f  76 35 2e 31 36 2e 33 0d   11 Perl/ v5.16.3·
0090  0a 4c 61 73 74 2d 4d 6f  64 69 66 69 65 64 3a 20   ·Last-Mo dified: 
00a0  4d 6f 6e 2c 20 32 36 20  41 75 67 20 32 30 32 34   Mon, 26  Aug 2024
00b0  20 30 35 3a 35 39 3a 30  31 20 47 4d 54 0d 0a 45    05:59:0 1 GMT··E
00c0  54 61 67 3a 20 22 31 31  39 34 2d 36 32 30 38 66   Tag: "11 94-6208f
00d0  64 32 35 62 62 35 30 38  22 0d 0a 41 63 63 65 70   d25bb508 "··Accep
00e0  74 2d 52 61 6e 67 65 73  3a 20 62 79 74 65 73 0d   t-Ranges : bytes·
00f0  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   ·Content -Length:
0100  20 34 35 30 30 0d 0a 4b  65 65 70 2d 41 6c 69 76    4500··K eep-Aliv
0110  65 3a 20 74 69 6d 65 6f  75 74 3d 35 2c 20 6d 61   e: timeo ut=5, ma
0120  78 3d 31 30 30 0d 0a 43  6f 6e 6e 65 63 74 69 6f   x=100··C onnectio
0130  6e 3a 20 4b 65 65 70 2d  41 6c 69 76 65 0d 0a 43   n: Keep- Alive··C
0140  6f 6e 74 65 6e 74 2d 54  79 70 65 3a 20 74 65 78   ontent-T ype: tex
0150  74 2f 68 74 6d 6c 3b 20  63 68 61 72 73 65 74 3d   t/html;  charset=
0160  55 54 46 2d 38 0d 0a 0d  0a 3c 68 74 6d 6c 3e 3c   UTF-8··· ·<html><
0170  68 65 61 64 3e 20 0a 3c  74 69 74 6c 65 3e 48 69   head> ·< title>Hi
0180  73 74 6f 72 69 63 61 6c  20 44 6f 63 75 6d 65 6e   storical  Documen
0190  74 73 3a 54 48 45 20 42  49 4c 4c 20 4f 46 20 52   ts:THE B ILL OF R
```

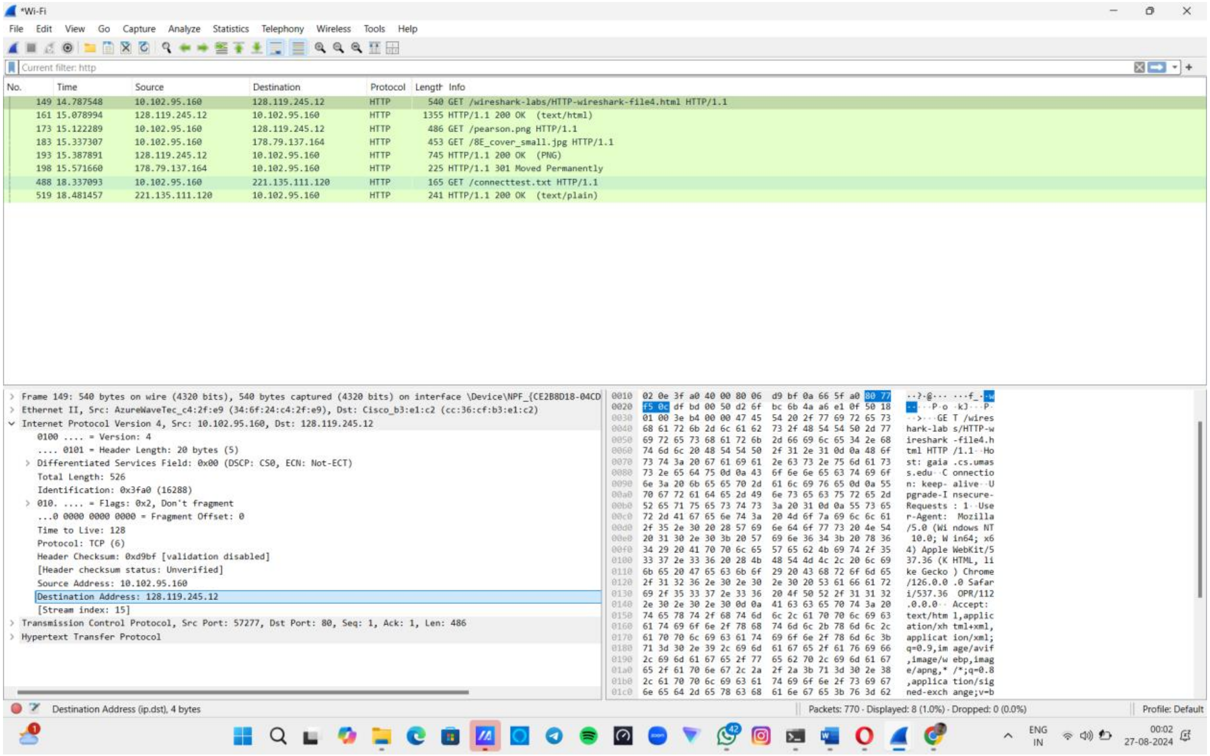
Frame (535 bytes)   Reassembled TCP (4861 bytes)

Reassembled TCP Segments (tcp.segments), 4,861 bytes   Packets: 128 · Displayed: 6 (4.7%) · Dropped: 0 (0.0%)   Profile: Default

4 TCP Segments.

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

Answer:



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

Current filter: http

```
No.   Time        Source           Destination      Protocol Length Info
  149 14.787548   10.102.95.160    128.119.245.12   HTTP      540 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
  161 15.078994   128.119.245.12   10.102.95.160    HTTP     1355 HTTP/1.1 200 OK  (text/html)
  173 15.122289   10.102.95.160    128.119.245.12   HTTP      486 GET /pearson.png HTTP/1.1
  183 15.337307   10.102.95.160    178.79.137.164   HTTP      453 GET /8E_cover_small.jpg HTTP/1.1
  193 15.387891   128.119.245.12   10.102.95.160    HTTP      745 HTTP/1.1 200 OK  (PNG)
  198 15.571660   178.79.137.164   10.102.95.160    HTTP      225 HTTP/1.1 301 Moved Permanently
  488 18.337093   10.102.95.160    221.135.111.120  HTTP      165 GET /connecttest.txt HTTP/1.1
  519 18.481457   221.135.111.120  10.102.95.160    HTTP      241 HTTP/1.1 200 OK  (text/plain)
```

```
> Frame 149: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{CE2B8D18-04CD
> Ethernet II, Src: AzureWaveTec_c4:2f:e9 (34:6f:24:c4:2f:e9), Dst: Cisco_b3:e1:c2 (cc:36:cf:b3:e1:c2)
v Internet Protocol Version 4, Src: 10.102.95.160, 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: 526
    Identification: 0x3fa0 (16288)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0xd9bf [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.102.95.160
    Destination Address: 128.119.245.12
    [Stream index: 15]
> Transmission Control Protocol, Src Port: 57277, Dst Port: 80, Seq: 1, Ack: 1, Len: 486
> Hypertext Transfer Protocol
```

```
0010  02 0e 3f a0 40 00 80 06  d9 bf 0a 66 5f a0 80 77   ··?·@··· ···f_··w
0020  f5 0c df bd 00 50 d2 6f  bc 6b 4a a6 e1 0f 50 18   ·····P·o ·kJ···P·
0030  01 00 3e b4 00 00 47 45  54 20 2f 77 69 72 65 73   ··>···GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 34 2e 68   ireshark -file4.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep- alive··U
00a0  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I nsecure-
00b0  52 65 71 75 65 73 74 73  3a 20 31 0d 0a 55 73 65   Requests : 1··Use
00c0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
00d0  2f 35 2e 30 20 28 57 69  6e 64 6f 77 73 20 4e 54   /5.0 (Wi ndows NT
00e0  20 31 30 2e 30 3b 20 57  69 6e 36 34 3b 20 78 36    10.0; W in64; x6
00f0  34 29 20 41 70 70 6c 65  57 65 62 4b 69 74 2f 35   4) Apple WebKit/5
0100  33 37 2e 33 36 20 28 4b  48 54 4d 4c 2c 20 6c 69   37.36 (K HTML, li
0110  6b 65 20 47 65 63 6b 6f  29 20 43 68 72 6f 6d 65   ke Gecko ) Chrome
0120  2f 31 32 36 2e 30 2e 30  2e 30 20 53 61 66 61 72   /126.0.0 .0 Safar
0130  69 2f 35 33 37 2e 33 36  20 4f 50 52 2f 31 31 32   i/537.36  OPR/112
0140  2e 30 2e 30 2e 30 0d 0a  41 63 63 65 70 74 3a 20   .0.0.0·· Accept: 
0150  74 65 78 74 2f 68 74 6d  6c 2c 61 70 70 6c 69 63   text/htm l,applic
0160  61 74 69 6f 6e 2f 78 68  74 6d 6c 2b 78 6d 6c 2c   ation/xh tml+xml,
0170  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 6d 6c 3b   applicat ion/xml;
0180  71 3d 30 2e 39 2c 69 6d  61 67 65 2f 61 76 69 66   q=0.9,im age/avif
0190  2c 69 6d 61 67 65 2f 77  65 62 70 2c 69 6d 61 67   ,image/w ebp,imag
01a0  65 2f 61 70 6e 67 2c 2a  2f 2a 3b 71 3d 30 2e 38   e/apng,* /*;q=0.8
01b0  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2f 73 69 67   ,applica tion/sig
01c0  6e 65 64 2d 65 78 63 68  61 6e 67 65 3b 76 3d 62   ned-exch ange;v=b
```

Destination Address (ip.dst), 4 bytes

Packets: 770 · Displayed: 8 (1.0%) · Dropped: 0 (0.0%)

Profile: Default

In total 4 HTTP GET request message were sent.

They were sent to:

Twice were sent to - 128.119.145.12

One were sent to - 178.79.137.164

One were sent to - 221.135.111.120

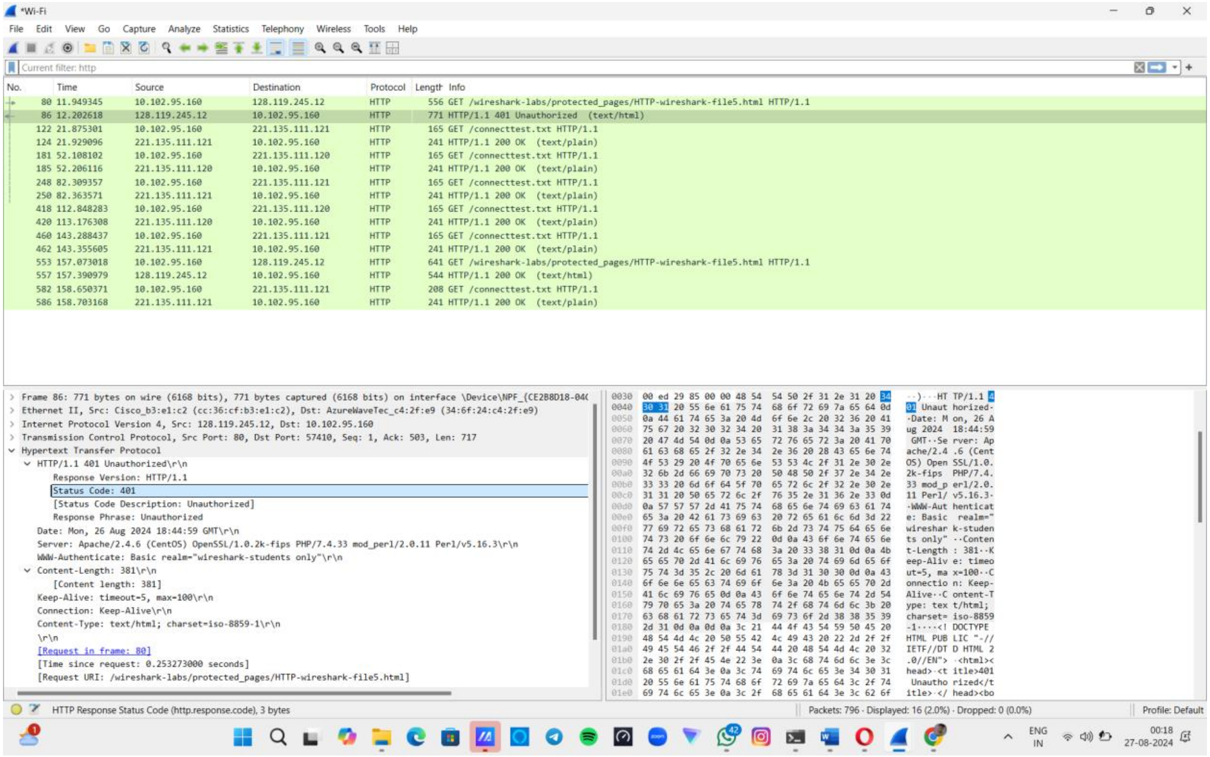
17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

Answer:

Yes the Two images were downloaded serially as it can be observed from the time stamps

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

Answer:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Current filter: http
Profile: Default
ENG
IN
00:18
27-08-2024

```
No.    Time         Source            Destination       Protocol  Length Info
    80 11.949345    10.102.95.160     128.119.245.12    HTTP      556 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
    86 12.202618    128.119.245.12    10.102.95.160     HTTP      771 HTTP/1.1 401 Unauthorized  (text/html)
   122 21.875301    10.102.95.160     221.135.111.121   HTTP      165 GET /connecttest.txt HTTP/1.1
   124 21.929096    221.135.111.121   10.102.95.160     HTTP      241 HTTP/1.1 200 OK  (text/plain)
   181 52.108102    10.102.95.160     221.135.111.120   HTTP      165 GET /connecttest.txt HTTP/1.1
   185 52.206116    221.135.111.120   10.102.95.160     HTTP      241 HTTP/1.1 200 OK  (text/plain)
   248 82.309357    10.102.95.160     221.135.111.121   HTTP      165 GET /connecttest.txt HTTP/1.1
   250 82.363571    221.135.111.121   10.102.95.160     HTTP      241 HTTP/1.1 200 OK  (text/plain)
   418 112.848283   10.102.95.160     221.135.111.120   HTTP      165 GET /connecttest.txt HTTP/1.1
   420 113.176308   221.135.111.120   10.102.95.160     HTTP      241 HTTP/1.1 200 OK  (text/plain)
   460 143.288437   10.102.95.160     221.135.111.121   HTTP      165 GET /connecttest.txt HTTP/1.1
   462 143.355605   221.135.111.121   10.102.95.160     HTTP      241 HTTP/1.1 200 OK  (text/plain)
   553 157.073018   10.102.95.160     128.119.245.12    HTTP      641 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
   557 157.390979   128.119.245.12    10.102.95.160     HTTP      544 HTTP/1.1 200 OK  (text/html)
   582 158.650371   10.102.95.160     221.135.111.121   HTTP      208 GET /connecttest.txt HTTP/1.1
   586 158.703168   221.135.111.121   10.102.95.160     HTTP      241 HTTP/1.1 200 OK  (text/plain)
```

```
> Frame 86: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{CE2B8D18-04(
> Ethernet II, Src: Cisco_b3:e1:c2 (cc:36:cf:b3:e1:c2), Dst: AzureWaveTec_c4:2f:e9 (34:6f:24:c4:2f:e9)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.102.95.160
> Transmission Control Protocol, Src Port: 80, Dst Port: 57410, Seq: 1, Ack: 503, Len: 717
v Hypertext Transfer Protocol
  v HTTP/1.1 401 Unauthorized\r\n
      Response Version: HTTP/1.1
      Status Code: 401
      [Status Code Description: Unauthorized]
      Response Phrase: Unauthorized
    Date: Mon, 26 Aug 2024 18:44:59 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
    WWW-Authenticate: Basic realm="wireshark-students only"\r\n
  v Content-Length: 381\r\n
      [Content length: 381]
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [Request in frame: 80]
    [Time since request: 0.253273000 seconds]
    [Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
```

```
0030  00 ed 29 85 00 00 48 54  54 50 2f 31 2e 31 20 34   ··)···HT TP/1.1 4
0040  30 31 20 55 6e 61 75 74  68 6f 72 69 7a 65 64 0d   01 Unaut horized·
0050  0a 44 61 74 65 3a 20 4d  6f 6e 2c 20 32 36 20 41   ·Date: M on, 26 A
0060  75 67 20 32 30 32 34 20  31 38 3a 34 34 3a 35 39   ug 2024  18:44:59
0070  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
0080  61 63 68 65 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0090  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
00a0  32 6b 2d 66 69 70 73 20  50 48 50 2f 37 2e 34 2e   2k-fips  PHP/7.4.
00b0  33 33 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   33 mod_p erl/2.0.
00c0  31 31 20 50 65 72 6c 2f  76 35 2e 31 36 2e 33 0d   11 Perl/ v5.16.3·
00d0  0a 57 57 57 2d 41 75 74  68 65 6e 74 69 63 61 74   ·WWW-Aut henticat
00e0  65 3a 20 42 61 73 69 63  20 72 65 61 6c 6d 3d 22   e: Basic  realm="
00f0  77 69 72 65 73 68 61 72  6b 2d 73 74 75 64 65 6e   wireshar k-studen
0100  74 73 20 6f 6e 6c 79 22  0d 0a 43 6f 6e 74 65 6e   ts only" ··Conten
0110  74 2d 4c 65 6e 67 74 68  3a 20 33 38 31 0d 0a 4b   t-Length : 381··K
0120  65 65 70 2d 41 6c 69 76  65 3a 20 74 69 6d 65 6f   eep-Aliv e: timeo
0130  75 74 3d 35 2c 20 6d 61  78 3d 31 30 30 0d 0a 43   ut=5, ma x=100··C
0140  6f 6e 6e 65 63 74 69 6f  6e 3a 20 4b 65 65 70 2d   onnectio n: Keep-
0150  41 6c 69 76 65 0d 0a 43  6f 6e 74 65 6e 74 2d 54   Alive··C ontent-T
0160  79 70 65 3a 20 74 65 78  74 2f 68 74 6d 6c 3b 20   ype: tex t/html; 
0170  63 68 61 72 73 65 74 3d  69 73 6f 2d 38 38 35 39   charset= iso-8859
0180  2d 31 0d 0a 0d 0a 3c 21  44 4f 43 54 59 50 45 20   -1····<! DOCTYPE 
0190  48 54 4d 4c 20 50 55 42  4c 49 43 20 22 2d 2f 2f   HTML PUB LIC "-//
01a0  49 45 54 46 2f 2f 44 54  44 20 48 54 4d 4c 20 32   IETF//DT D HTML 2
01b0  2e 30 2f 2f 45 4e 22 3e  0a 3c 68 74 6d 6c 3e 3c   .0//EN"> ·<html><
01c0  68 65 61 64 3e 0a 3c 74  69 74 6c 65 3e 34 30 31   head>·<t itle>401
01d0  20 55 6e 61 75 74 68 6f  72 69 7a 65 64 3c 2f 74    Unautho rized</t
01e0  69 74 6c 65 3e 0a 3c 2f  68 65 61 64 3e 3c 62 6f   itle>·</ head><bo
```

HTTP Response Status Code (http.response.code), 3 bytes

Packets: 796 · Displayed: 16 (2.0%) · Dropped: 0 (0.0%)

To the initial HTTP GET request from browser the response had the response had Status code-401 and Phrase-Unauthorized

19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Answer:

The HTTP GET includes the Authorization :Basic:field.

And in the response it show status code 200