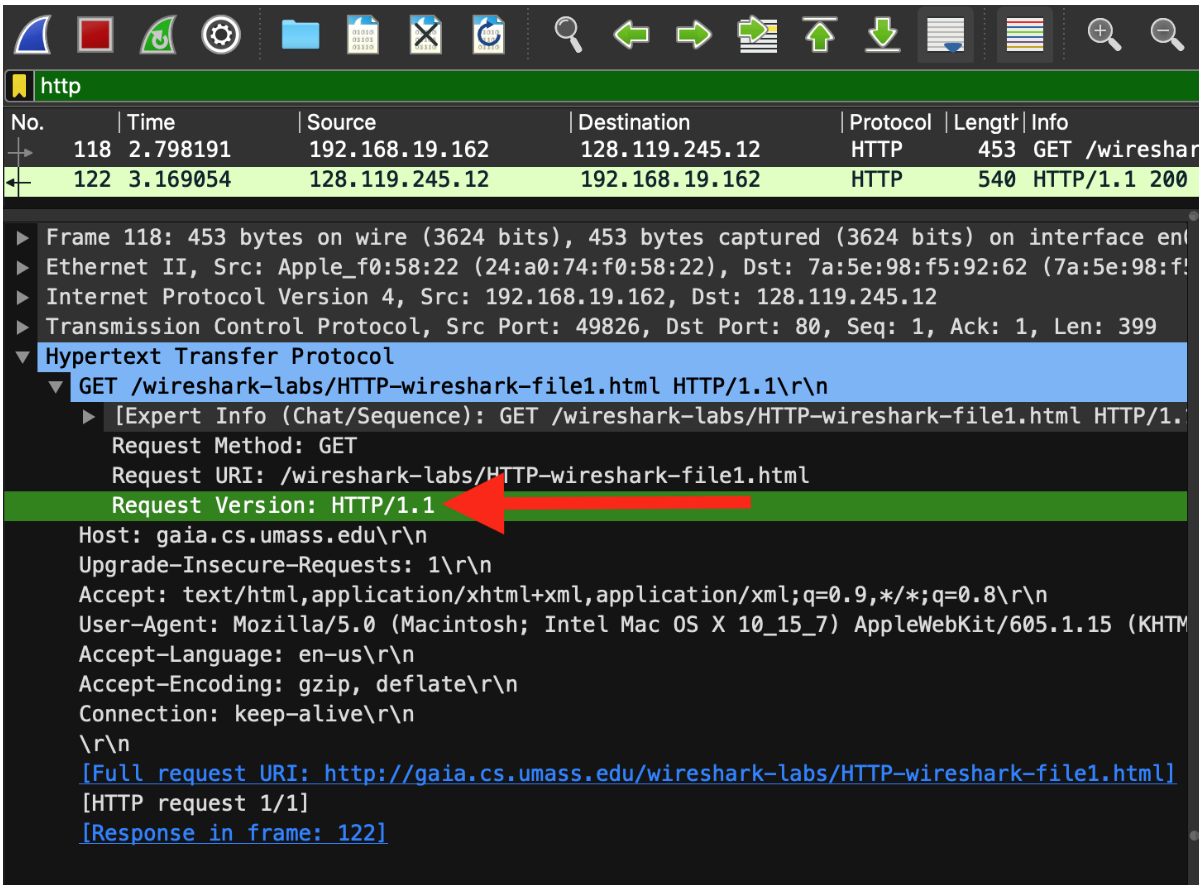
For
gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

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

Browser is running HTTP version 1.1.

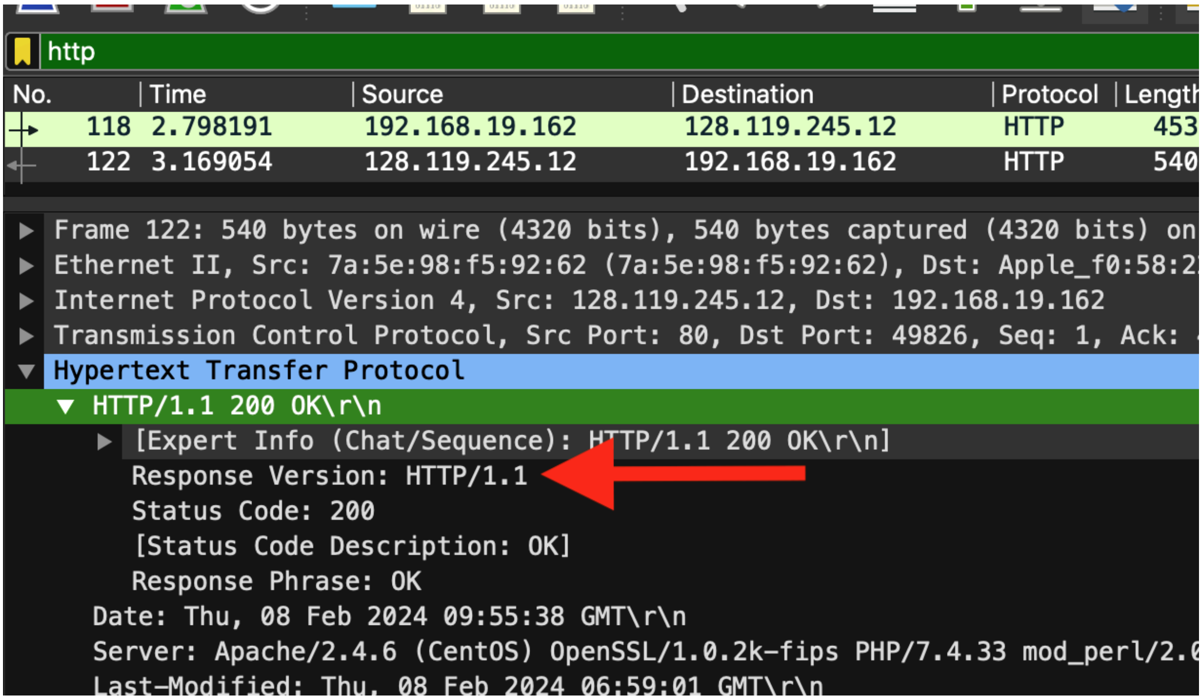


```
http
```

```
No.     Time        Source           Destination      Protocol  Length Info
  118   2.798191    192.168.19.162   128.119.245.12   HTTP      453    GET /wireshar
  122   3.169054    128.119.245.12   192.168.19.162   HTTP      540    HTTP/1.1 200
```

```
▶ Frame 118: 453 bytes on wire (3624 bits), 453 bytes captured (3624 bits) on interface en
▶ Ethernet II, Src: Apple_f0:58:22 (24:a0:74:f0:58:22), Dst: 7a:5e:98:f5:92:62 (7a:5e:98:f
▶ Internet Protocol Version 4, Src: 192.168.19.162, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 49826, Dst Port: 80, Seq: 1, Ack: 1, Len: 399
▼ Hypertext Transfer Protocol
  ▼ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    ▶ [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTM
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 122]
```

The server is running HTTP version 1.1

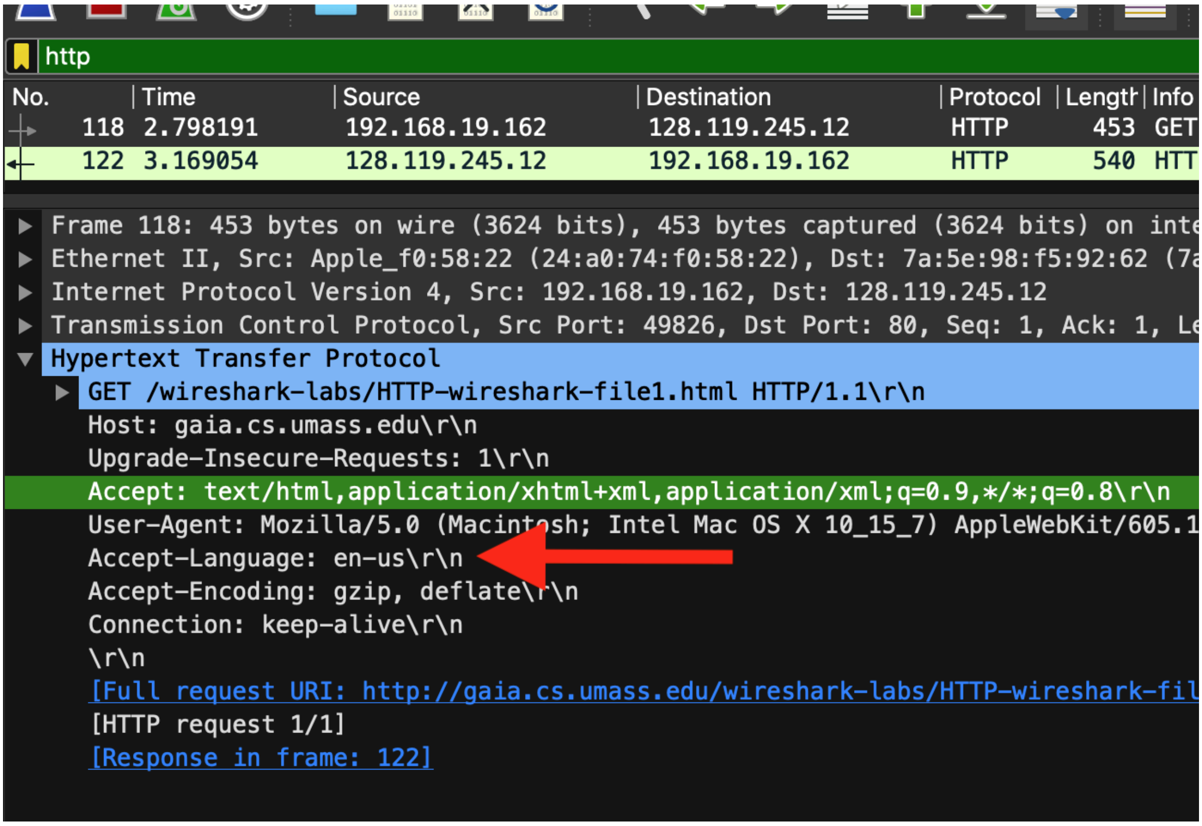


```
http
No.      Time       Source           Destination      Protocol  Length
  118  2.798191   192.168.19.162   128.119.245.12   HTTP       453
  122  3.169054   128.119.245.12   192.168.19.162   HTTP       540

▶ Frame 122: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on
▶ Ethernet II, Src: 7a:5e:98:f5:92:62 (7a:5e:98:f5:92:62), Dst: Apple_f0:58:2
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.19.162
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 49826, Seq: 1, Ack:
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 200 OK\r\n
    ▶ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Thu, 08 Feb 2024 09:55:38 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0
    Last-Modified: Thu, 08 Feb 2024 06:59:01 GMT\r\n
```

2. What languages (if any) does your browser indicate that it can accept to the server? In the captured session, what other information (if any) does the browser provide the server with regarding the user/browser?

It can accept US-english. It also shows my browser,its version and my operating system and other information related to my device.

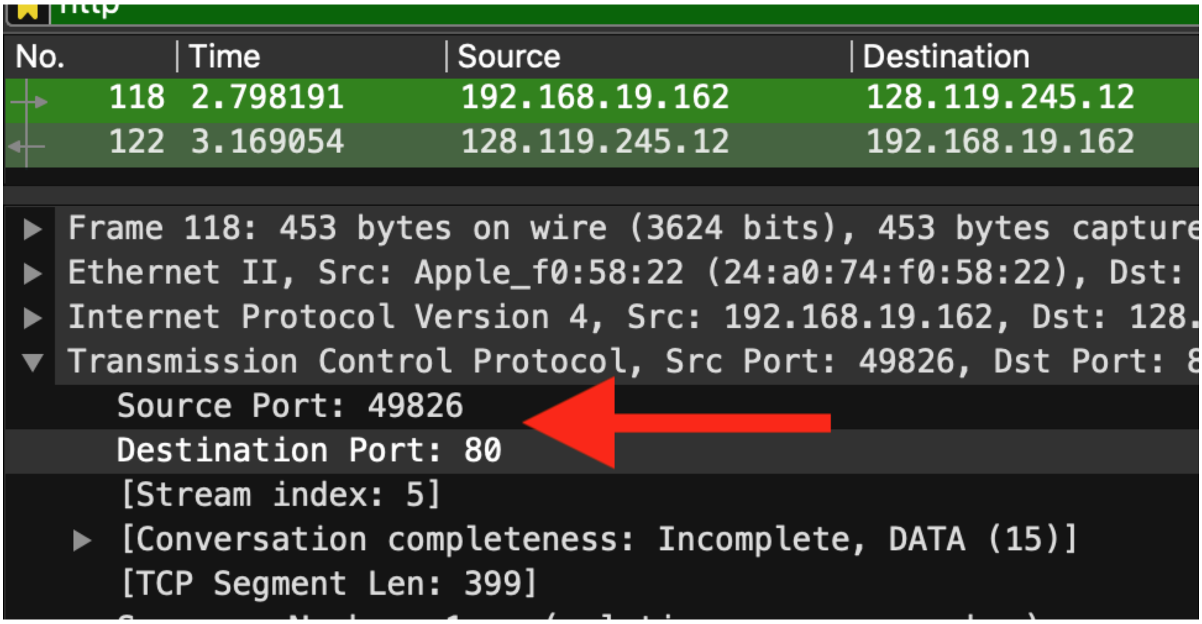


```
http
No.      Time      Source           Destination      Protocol  Length Info
    118  2.798191  192.168.19.162   128.119.245.12   HTTP       453  GET
    122  3.169054  128.119.245.12   192.168.19.162   HTTP       540  HTT

▶ Frame 118: 453 bytes on wire (3624 bits), 453 bytes captured (3624 bits) on inte
▶ Ethernet II, Src: Apple_f0:58:22 (24:a0:74:f0:58:22), Dst: 7a:5e:98:f5:92:62 (7a
▶ Internet Protocol Version 4, Src: 192.168.19.162, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 49826, Dst Port: 80, Seq: 1, Ack: 1, Le
▼ Hypertext Transfer Protocol
  ▶ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-fil
    [HTTP request 1/1]
    [Response in frame: 122]
```

3. What is the IP address and port number of your computer? Of the server?

My IP address and port: 192.168.19.162:49826
Server IP address and port: 128.119.245.12:80

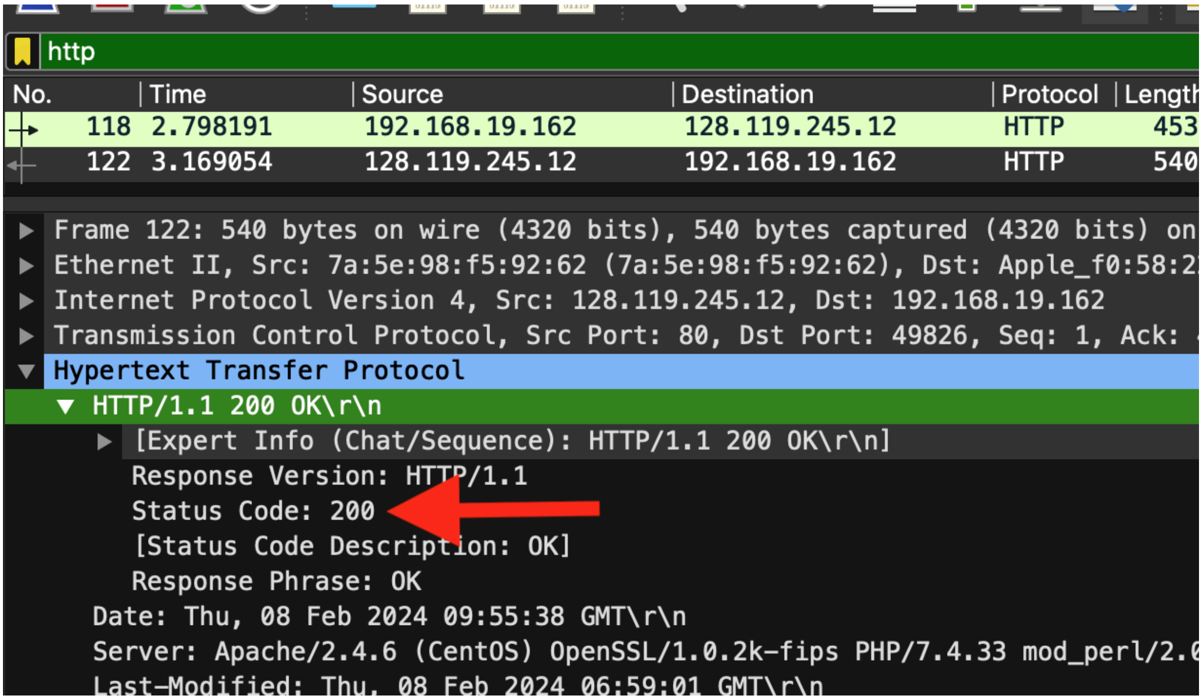


```
No.      Time      Source           Destination
    118  2.798191  192.168.19.162   128.119.245.12
    122  3.169054  128.119.245.12   192.168.19.162

▶ Frame 118: 453 bytes on wire (3624 bits), 453 bytes capture
▶ Ethernet II, Src: Apple_f0:58:22 (24:a0:74:f0:58:22), Dst:
▶ Internet Protocol Version 4, Src: 192.168.19.162, Dst: 128.
▼ Transmission Control Protocol, Src Port: 49826, Dst Port: 8
    Source Port: 49826
    Destination Port: 80
    [Stream index: 5]
  ▶ [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 399]
```

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

The status code returned was 200.

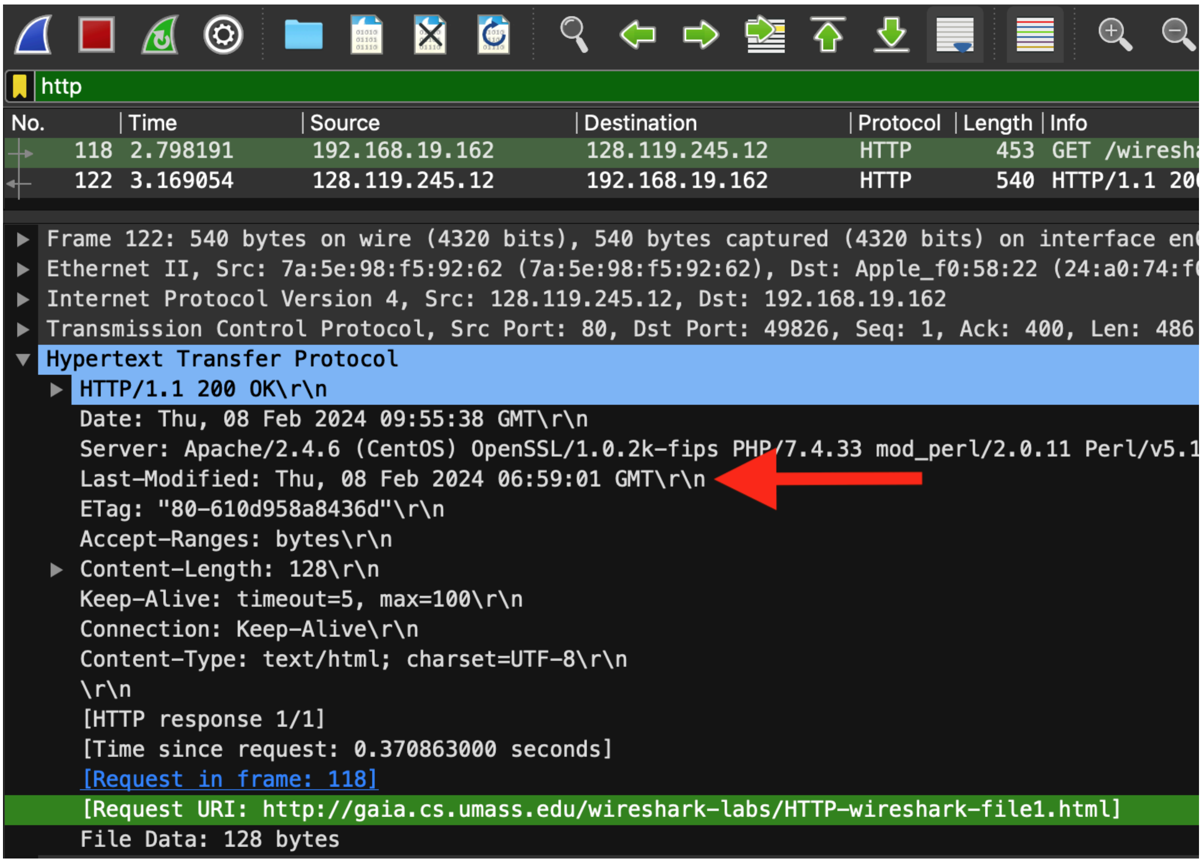


```
http
No.    Time         Source            Destination       Protocol  Length
118    2.798191     192.168.19.162    128.119.245.12    HTTP      453
122    3.169054     128.119.245.12    192.168.19.162    HTTP      540

▶ Frame 122: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on
▶ Ethernet II, Src: 7a:5e:98:f5:92:62 (7a:5e:98:f5:92:62), Dst: Apple_f0:58:2
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.19.162
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 49826, Seq: 1, Ack:
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 200 OK\r\n
    ▶ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
  Date: Thu, 08 Feb 2024 09:55:38 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0
  Last-Modified: Thu, 08 Feb 2024 06:59:01 GMT\r\n
```

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

It was at this time.

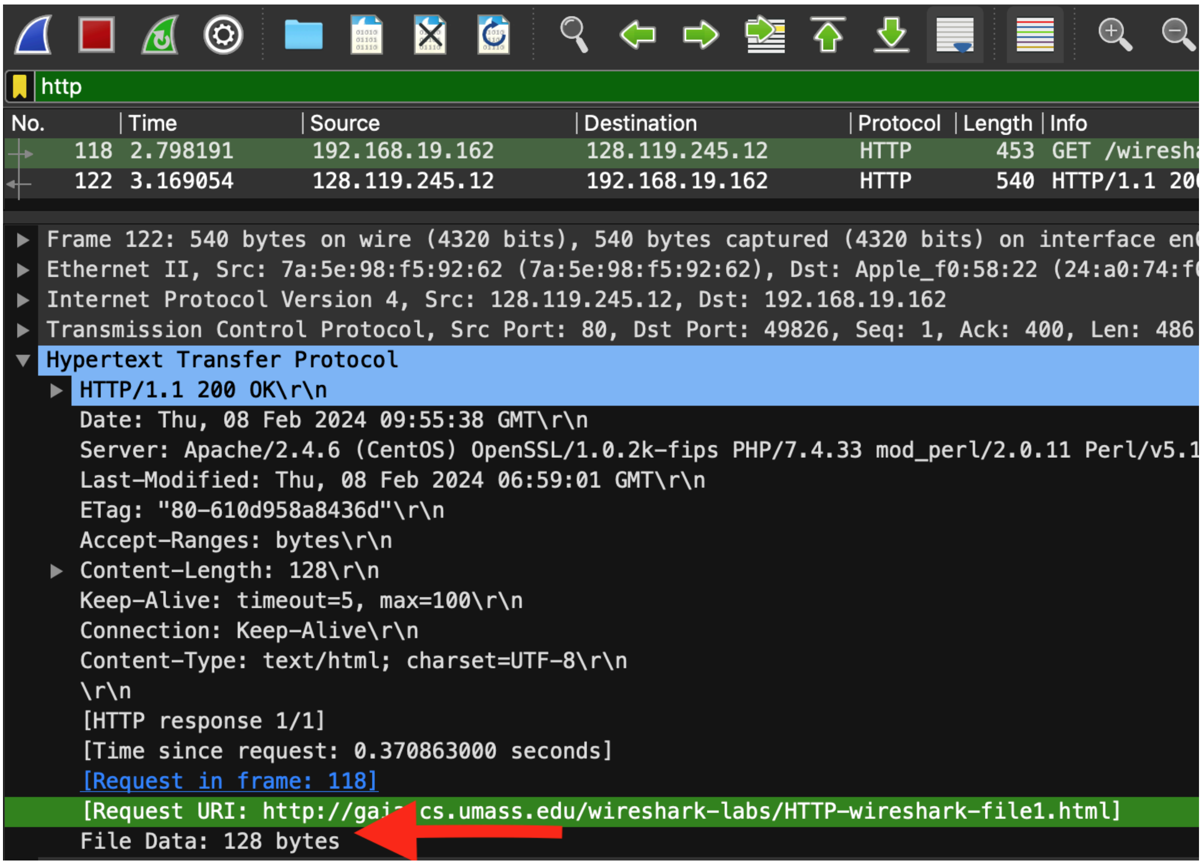


```
No.   Time      Source           Destination      Protocol Length Info
 118  2.798191  192.168.19.162   128.119.245.12   HTTP        453 GET /wiresha
 122  3.169054  128.119.245.12   192.168.19.162   HTTP        540 HTTP/1.1 20

▶ Frame 122: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface en
▶ Ethernet II, Src: 7a:5e:98:f5:92:62 (7a:5e:98:f5:92:62), Dst: Apple_f0:58:22 (24:a0:74:f
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.19.162
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 49826, Seq: 1, Ack: 400, Len: 486
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Date: Thu, 08 Feb 2024 09:55:38 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.1
    Last-Modified: Thu, 08 Feb 2024 06:59:01 GMT\r\n
    ETag: "80-610d958a8436d"\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
    [HTTP response 1/1]
    [Time since request: 0.370863000 seconds]
    [Request in frame: 118]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    File Data: 128 bytes
```

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

It returned 128 bytes of data.



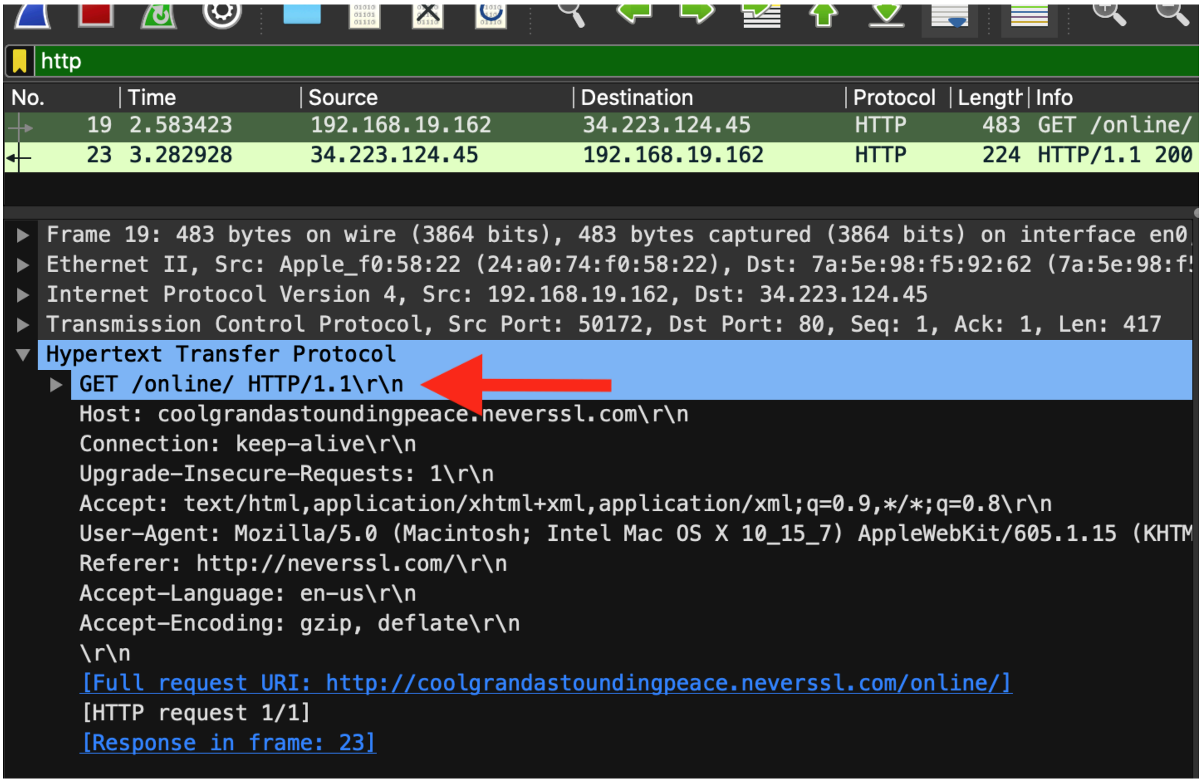
```
http
No.      Time        Source            Destination       Protocol  Length  Info
    118  2.798191    192.168.19.162    128.119.245.12    HTTP         453  GET /wiresha
    122  3.169054    128.119.245.12    192.168.19.162    HTTP         540  HTTP/1.1 20

▶ Frame 122: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface en
▶ Ethernet II, Src: 7a:5e:98:f5:92:62 (7a:5e:98:f5:92:62), Dst: Apple_f0:58:22 (24:a0:74:f
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.19.162
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 49826, Seq: 1, Ack: 400, Len: 486
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Date: Thu, 08 Feb 2024 09:55:38 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.1
    Last-Modified: Thu, 08 Feb 2024 06:59:01 GMT\r\n
    ETag: "80-610d958a8436d"\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
    [HTTP response 1/1]
    [Time since request: 0.370863000 seconds]
    [Request in frame: 118]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    File Data: 128 bytes
```

For http://coolgrandastoundingpeace.neverssl.com/online/

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

Browser is running HTTP version 1.1.

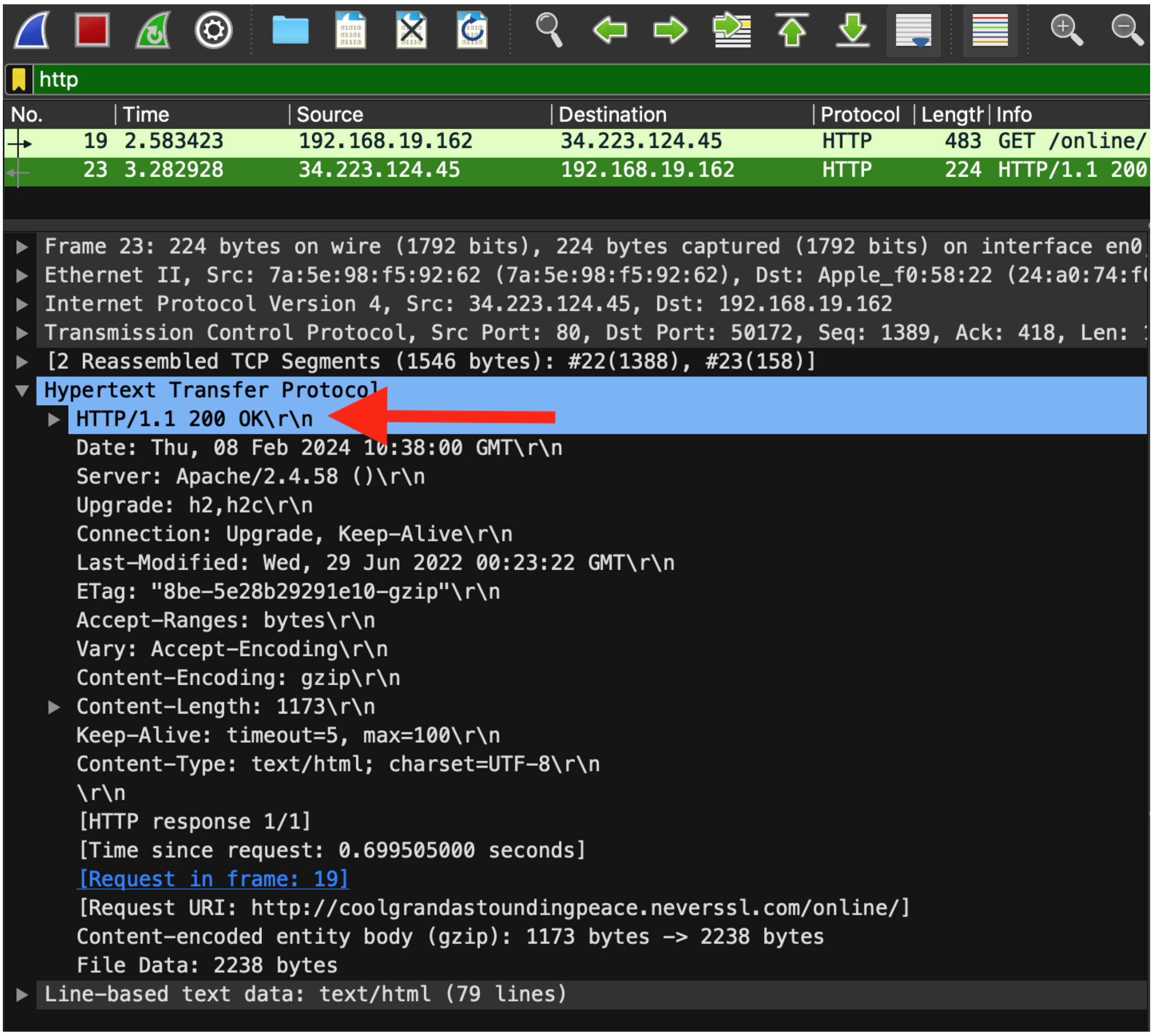


```
http

No.   Time       Source          Destination     Protocol  Lengtł Info
   19 2.583423   192.168.19.162  34.223.124.45   HTTP      483  GET /online/
   23 3.282928   34.223.124.45   192.168.19.162  HTTP      224  HTTP/1.1 200

▶ Frame 19: 483 bytes on wire (3864 bits), 483 bytes captured (3864 bits) on interface en0
▶ Ethernet II, Src: Apple_f0:58:22 (24:a0:74:f0:58:22), Dst: 7a:5e:98:f5:92:62 (7a:5e:98:f!
▶ Internet Protocol Version 4, Src: 192.168.19.162, Dst: 34.223.124.45
▶ Transmission Control Protocol, Src Port: 50172, Dst Port: 80, Seq: 1, Ack: 1, Len: 417
▼ Hypertext Transfer Protocol
  ▶ GET /online/ HTTP/1.1\r\n
    Host: coolgrandastoundingpeace.neverssl.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTM
    Referer: http://neverssl.com/\r\n
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
    \r\n
    [Full request URI: http://coolgrandastoundingpeace.neverssl.com/online/]
    [HTTP request 1/1]
    [Response in frame: 23]
```

The server is running HTTP version 1.1

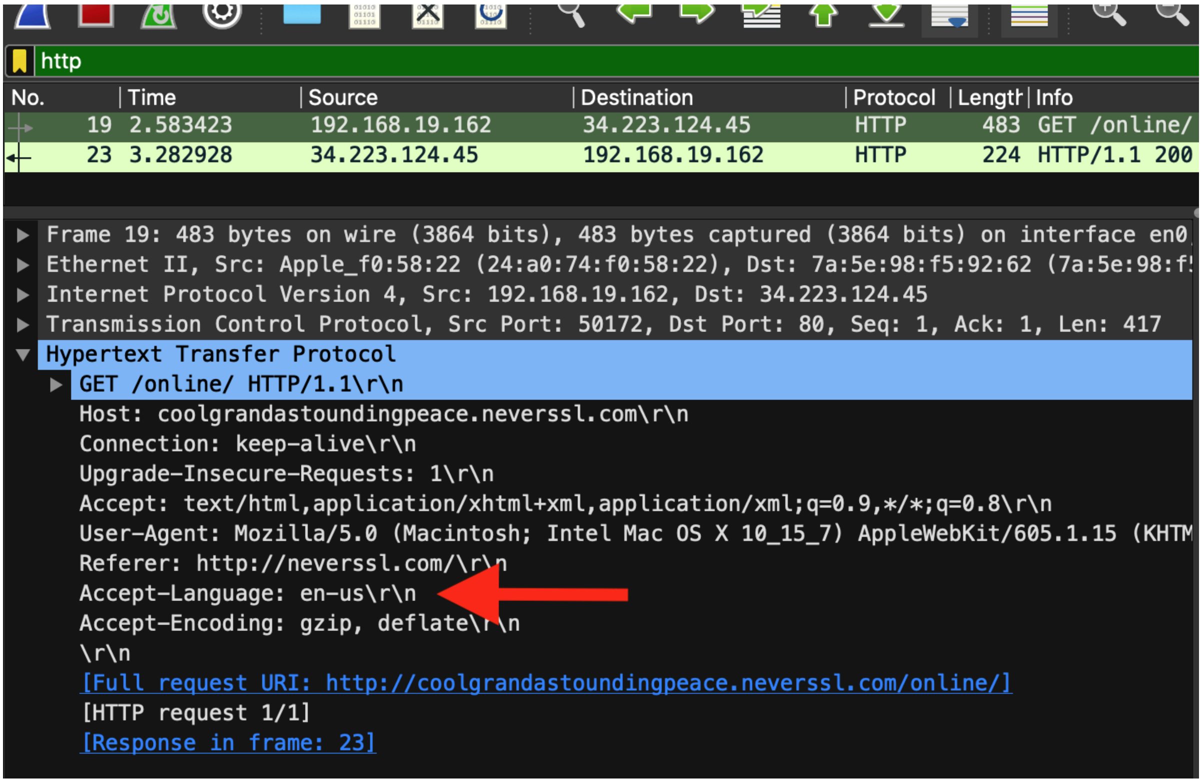


```
http
No.   | Time      | Source         | Destination    | Protocol | Length | Info
   19  2.583423    192.168.19.162   34.223.124.45    HTTP        483  GET /online/
   23  3.282928    34.223.124.45    192.168.19.162   HTTP        224  HTTP/1.1 200

▶ Frame 23: 224 bytes on wire (1792 bits), 224 bytes captured (1792 bits) on interface en0
▶ Ethernet II, Src: 7a:5e:98:f5:92:62 (7a:5e:98:f5:92:62), Dst: Apple_f0:58:22 (24:a0:74:f
▶ Internet Protocol Version 4, Src: 34.223.124.45, Dst: 192.168.19.162
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 50172, Seq: 1389, Ack: 418, Len:
▶ [2 Reassembled TCP Segments (1546 bytes): #22(1388), #23(158)]
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Date: Thu, 08 Feb 2024 10:38:00 GMT\r\n
    Server: Apache/2.4.58 ()\r\n
    Upgrade: h2,h2c\r\n
    Connection: Upgrade, Keep-Alive\r\n
    Last-Modified: Wed, 29 Jun 2022 00:23:22 GMT\r\n
    ETag: "8be-5e28b29291e10-gzip"\r\n
    Accept-Ranges: bytes\r\n
    Vary: Accept-Encoding\r\n
    Content-Encoding: gzip\r\n
  ▶ Content-Length: 1173\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.699505000 seconds]
    [Request in frame: 19]
    [Request URI: http://coolgrandastoundingpeace.neverssl.com/online/]
    Content-encoded entity body (gzip): 1173 bytes -> 2238 bytes
    File Data: 2238 bytes
▶ Line-based text data: text/html (79 lines)
```

2. What languages (if any) does your browser indicate that it can accept to the server? In the captured session, what other information (if any) does the browser provide the server with regarding the user/browser?

It can accept US-english. It also shows my browser,its version and my operating system and other information related to my device.

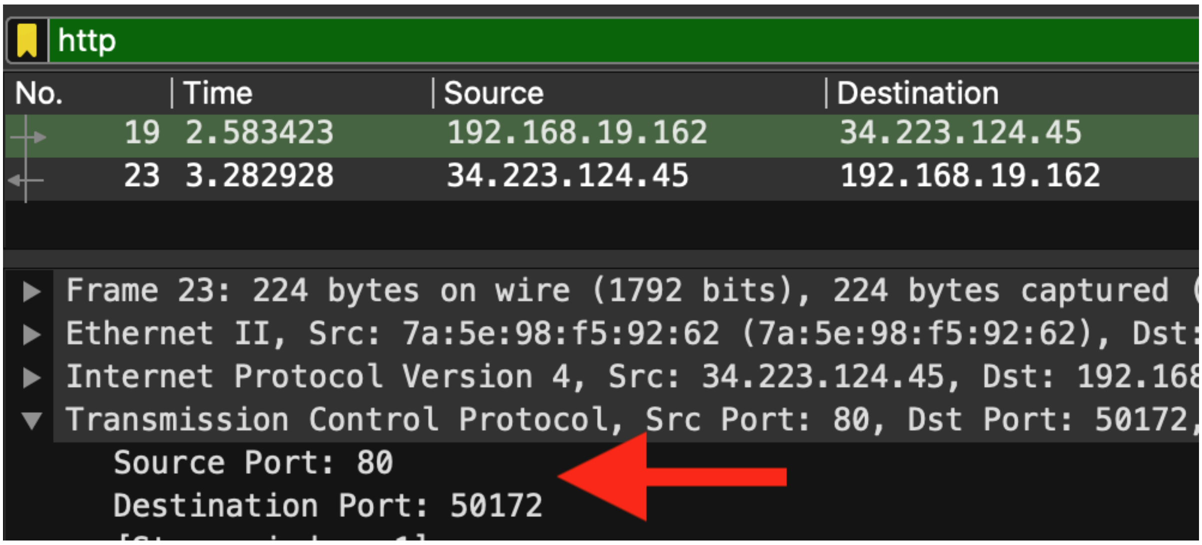


```
http
No.    Time        Source           Destination      Protocol  Lengtł Info
    19 2.583423    192.168.19.162   34.223.124.45    HTTP       483  GET /online/
    23 3.282928    34.223.124.45    192.168.19.162   HTTP       224  HTTP/1.1 200

▶ Frame 19: 483 bytes on wire (3864 bits), 483 bytes captured (3864 bits) on interface en0
▶ Ethernet II, Src: Apple_f0:58:22 (24:a0:74:f0:58:22), Dst: 7a:5e:98:f5:92:62 (7a:5e:98:f!
▶ Internet Protocol Version 4, Src: 192.168.19.162, Dst: 34.223.124.45
▶ Transmission Control Protocol, Src Port: 50172, Dst Port: 80, Seq: 1, Ack: 1, Len: 417
▼ Hypertext Transfer Protocol
  ▶ GET /online/ HTTP/1.1\r\n
    Host: coolgrandastoundingpeace.neverssl.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTM
    Referer: http://neverssl.com/\r\n
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
    \r\n
    [Full request URI: http://coolgrandastoundingpeace.neverssl.com/online/]
    [HTTP request 1/1]
    [Response in frame: 23]
```

3. What is the IP address and port number of your computer? Of the server?

My IP address and port: 192.168.19.162:50172
Server IP address and port: 34.223.124.45:80

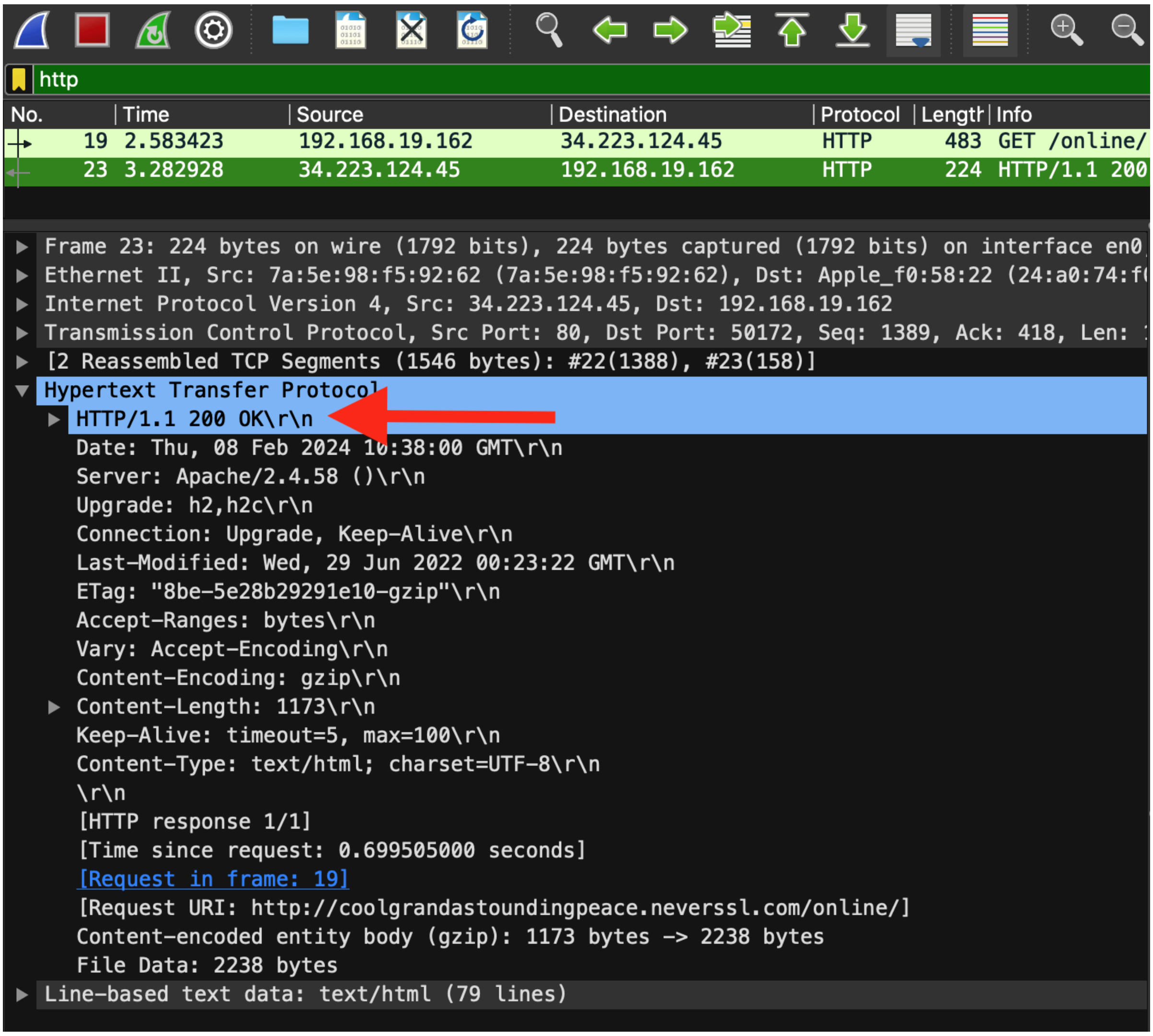


```
http
No.    Time        Source           Destination
    19 2.583423    192.168.19.162   34.223.124.45
    23 3.282928    34.223.124.45    192.168.19.162

▶ Frame 23: 224 bytes on wire (1792 bits), 224 bytes captured (
▶ Ethernet II, Src: 7a:5e:98:f5:92:62 (7a:5e:98:f5:92:62), Dst:
▶ Internet Protocol Version 4, Src: 34.223.124.45, Dst: 192.168
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 50172,
    Source Port: 80
    Destination Port: 50172
```

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

The status code returned was 200.

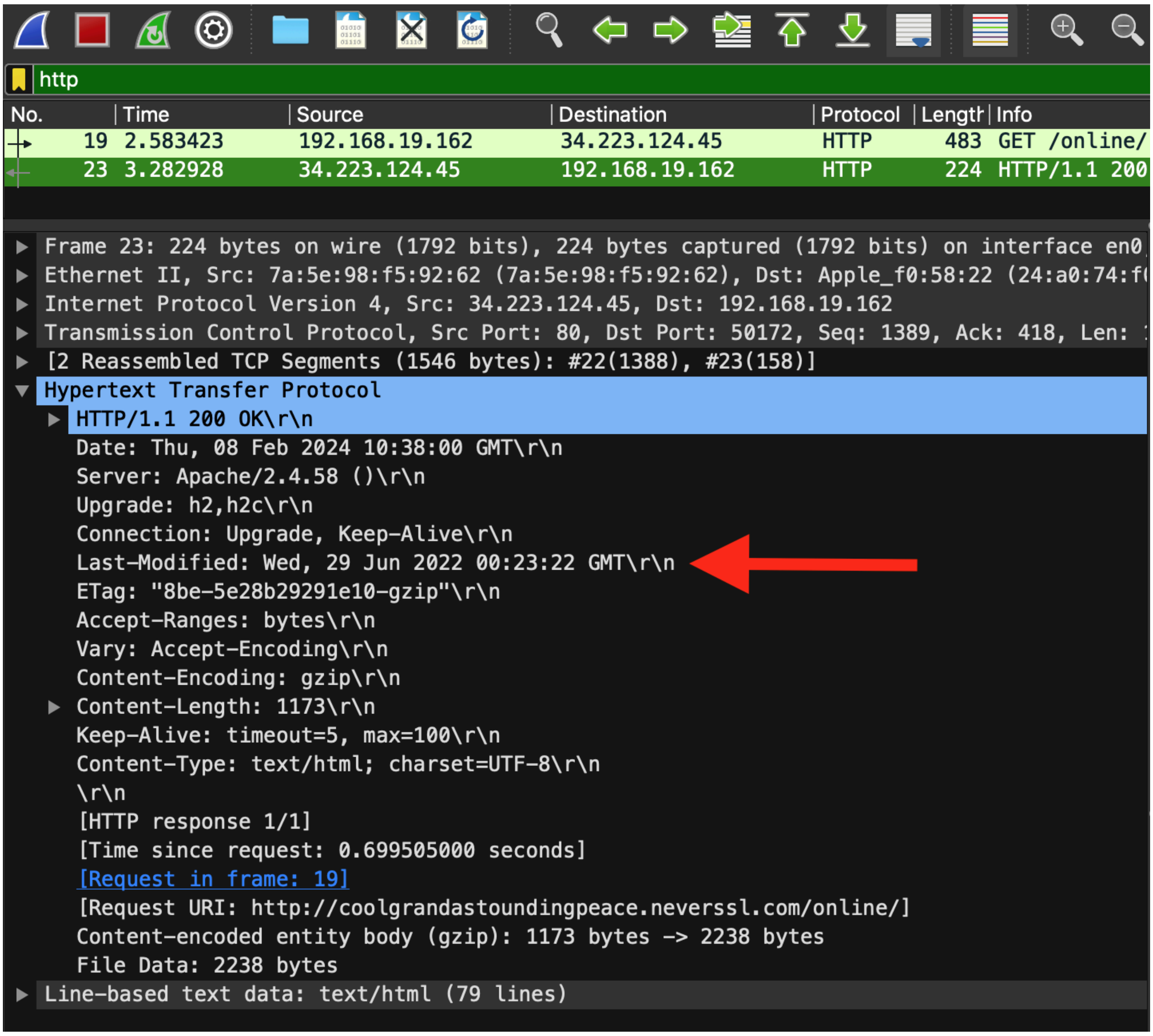


```
No.   Time       Source           Destination      Protocol Length Info
  19  2.583423   192.168.19.162   34.223.124.45    HTTP     483  GET /online/
  23  3.282928   34.223.124.45    192.168.19.162   HTTP     224  HTTP/1.1 200

▶ Frame 23: 224 bytes on wire (1792 bits), 224 bytes captured (1792 bits) on interface en0,
▶ Ethernet II, Src: 7a:5e:98:f5:92:62 (7a:5e:98:f5:92:62), Dst: Apple_f0:58:22 (24:a0:74:f
▶ Internet Protocol Version 4, Src: 34.223.124.45, Dst: 192.168.19.162
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 50172, Seq: 1389, Ack: 418, Len:
▶ [2 Reassembled TCP Segments (1546 bytes): #22(1388), #23(158)]
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Date: Thu, 08 Feb 2024 10:38:00 GMT\r\n
    Server: Apache/2.4.58 ()\r\n
    Upgrade: h2,h2c\r\n
    Connection: Upgrade, Keep-Alive\r\n
    Last-Modified: Wed, 29 Jun 2022 00:23:22 GMT\r\n
    ETag: "8be-5e28b29291e10-gzip"\r\n
    Accept-Ranges: bytes\r\n
    Vary: Accept-Encoding\r\n
    Content-Encoding: gzip\r\n
  ▶ Content-Length: 1173\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.699505000 seconds]
    [Request in frame: 19]
    [Request URI: http://coolgrandastoundingpeace.neverssl.com/online/]
    Content-encoded entity body (gzip): 1173 bytes -> 2238 bytes
    File Data: 2238 bytes
▶ Line-based text data: text/html (79 lines)
```

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

It was at this time.

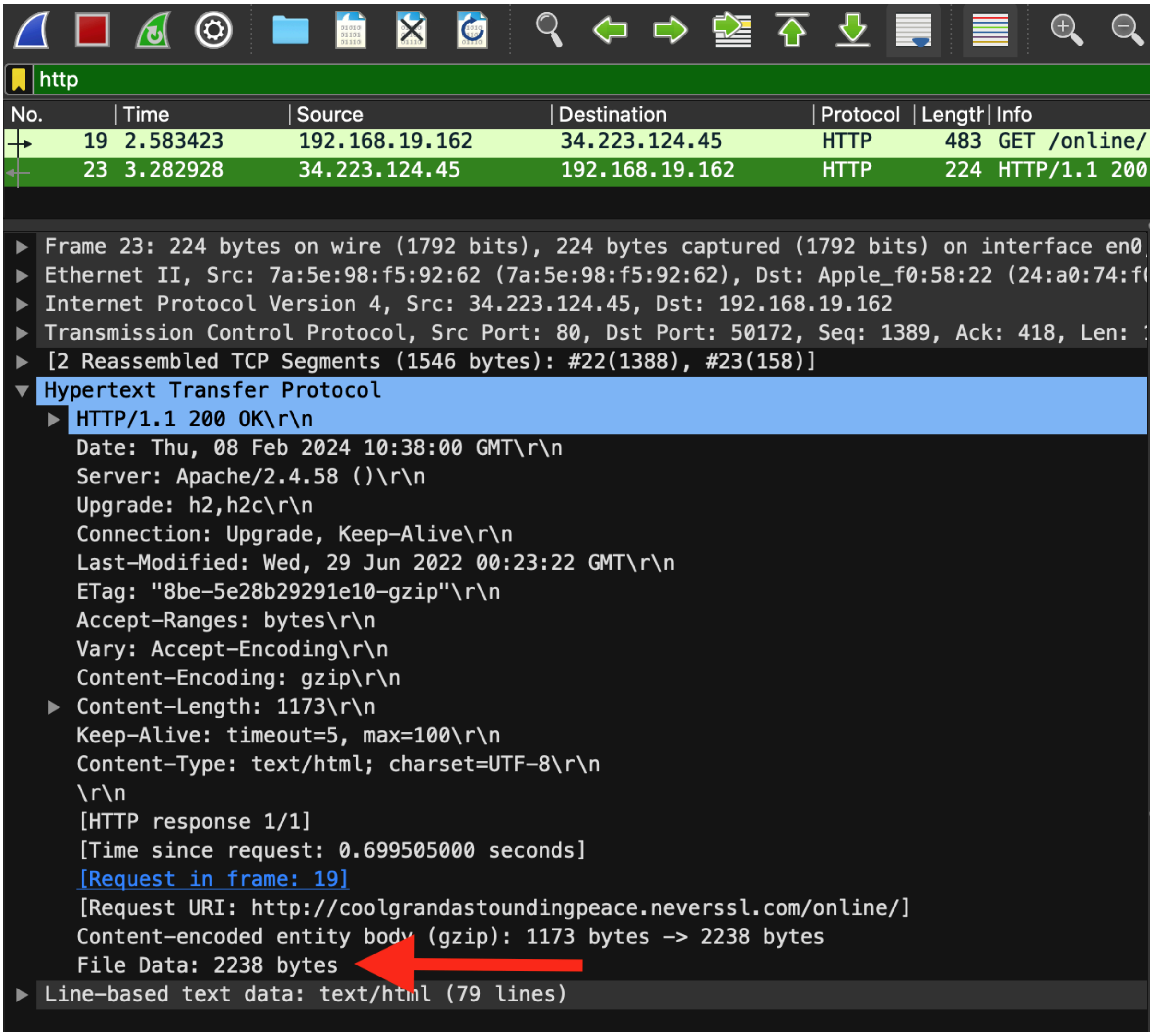


```
http
No.   |Time      |Source          |Destination     |Protocol |Length|Info
   19  2.583423   192.168.19.162   34.223.124.45    HTTP        483  GET /online/
   23  3.282928   34.223.124.45    192.168.19.162   HTTP        224  HTTP/1.1 200

▶ Frame 23: 224 bytes on wire (1792 bits), 224 bytes captured (1792 bits) on interface en0
▶ Ethernet II, Src: 7a:5e:98:f5:92:62 (7a:5e:98:f5:92:62), Dst: Apple_f0:58:22 (24:a0:74:f
▶ Internet Protocol Version 4, Src: 34.223.124.45, Dst: 192.168.19.162
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 50172, Seq: 1389, Ack: 418, Len:
▶ [2 Reassembled TCP Segments (1546 bytes): #22(1388), #23(158)]
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Date: Thu, 08 Feb 2024 10:38:00 GMT\r\n
    Server: Apache/2.4.58 ()\r\n
    Upgrade: h2,h2c\r\n
    Connection: Upgrade, Keep-Alive\r\n
    Last-Modified: Wed, 29 Jun 2022 00:23:22 GMT\r\n
    ETag: "8be-5e28b29291e10-gzip"\r\n
    Accept-Ranges: bytes\r\n
    Vary: Accept-Encoding\r\n
    Content-Encoding: gzip\r\n
  ▶ Content-Length: 1173\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.699505000 seconds]
    [Request in frame: 19]
    [Request URI: http://coolgrandastoundingpeace.neverssl.com/online/]
    Content-encoded entity body (gzip): 1173 bytes -> 2238 bytes
    File Data: 2238 bytes
▶ Line-based text data: text/html (79 lines)
```

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

It returned 2238 bytes of data.



http

```
No.    | Time       | Source           | Destination      | Protocol | Length | Info
    19  2.583423    192.168.19.162     34.223.124.45      HTTP       483  GET /online/
    23  3.282928    34.223.124.45      192.168.19.162     HTTP       224  HTTP/1.1 200
```

```
▶ Frame 23: 224 bytes on wire (1792 bits), 224 bytes captured (1792 bits) on interface en0,
▶ Ethernet II, Src: 7a:5e:98:f5:92:62 (7a:5e:98:f5:92:62), Dst: Apple_f0:58:22 (24:a0:74:f(
▶ Internet Protocol Version 4, Src: 34.223.124.45, Dst: 192.168.19.162
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 50172, Seq: 1389, Ack: 418, Len: 1
▶ [2 Reassembled TCP Segments (1546 bytes): #22(1388), #23(158)]
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Date: Thu, 08 Feb 2024 10:38:00 GMT\r\n
    Server: Apache/2.4.58 ()\r\n
    Upgrade: h2,h2c\r\n
    Connection: Upgrade, Keep-Alive\r\n
    Last-Modified: Wed, 29 Jun 2022 00:23:22 GMT\r\n
    ETag: "8be-5e28b29291e10-gzip"\r\n
    Accept-Ranges: bytes\r\n
    Vary: Accept-Encoding\r\n
    Content-Encoding: gzip\r\n
  ▶ Content-Length: 1173\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.699505000 seconds]
    [Request in frame: 19]
    [Request URI: http://coolgrandastoundingpeace.neverssl.com/online/]
    Content-encoded entity body (gzip): 1173 bytes -> 2238 bytes
    File Data: 2238 bytes
▶ Line-based text data: text/html (79 lines)
```