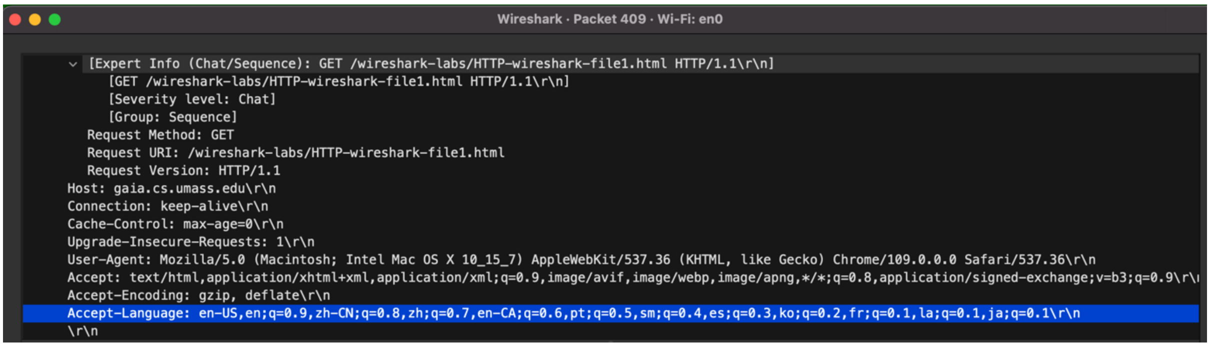
Lab 2 HTTP

Lab Report

Guanlin Jiang (21093962D)

Q2: What languages (if any) does your browser indicate that it can accept to the server?

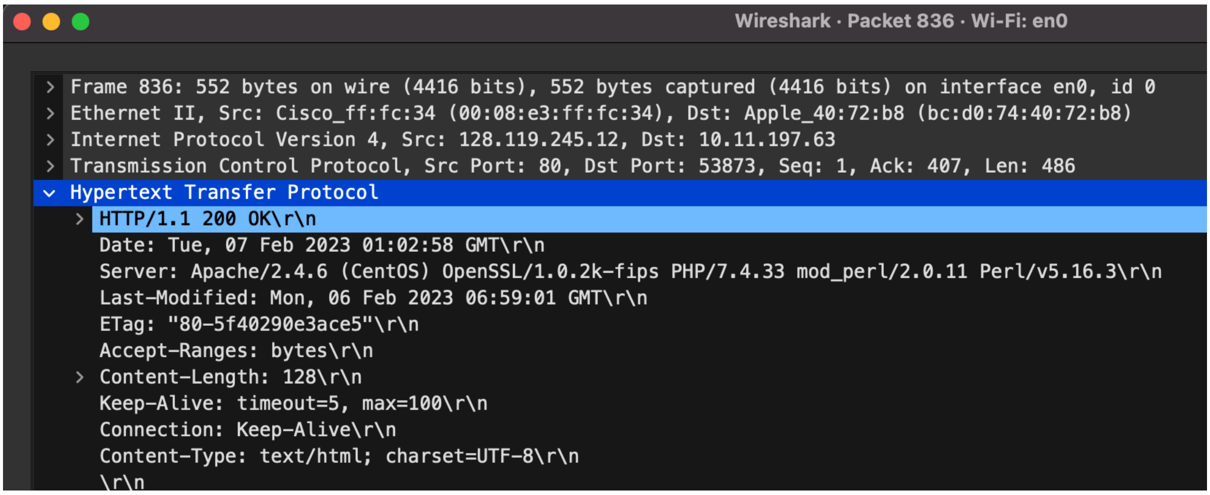
Answer: The languages browser indicate are en-US, zh-CN, zh, en-CA, zh, pt, sm, es, ko, fr, la, ja.



```
    v [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
          [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
          [Severity level: Chat]
          [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 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=0.9\r\
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7,en-CA;q=0.6,pt;q=0.5,sm;q=0.4,es;q=0.3,ko;q=0.2,fr;q=0.1,la;q=0.1,ja;q=0.1\r\n
    \r\n
```

Q4: What is the status code returned from the server to your browser?

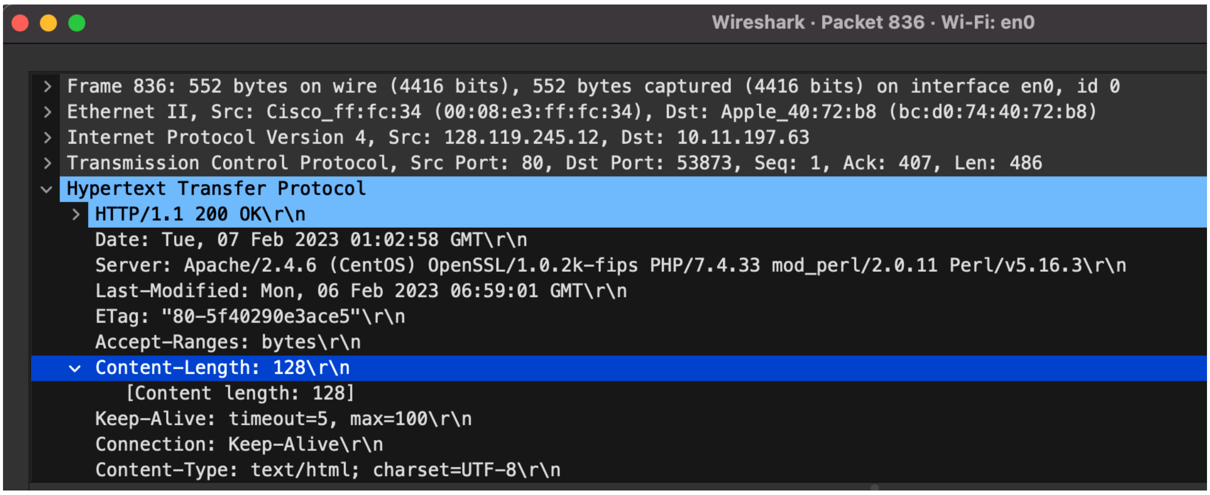
Answer: The status code is 200.



```
> Frame 836: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface en0, id 0
> Ethernet II, Src: Cisco_ff:fc:34 (00:08:e3:ff:fc:34), Dst: Apple_40:72:b8 (bc:d0:74:40:72:b8)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.11.197.63
> Transmission Control Protocol, Src Port: 80, Dst Port: 53873, Seq: 1, Ack: 407, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Tue, 07 Feb 2023 01:02:58 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, 06 Feb 2023 06:59:01 GMT\r\n
    ETag: "80-5f40290e3ace5"\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
```

Q6: How many bytes of content are being returned to your browser?

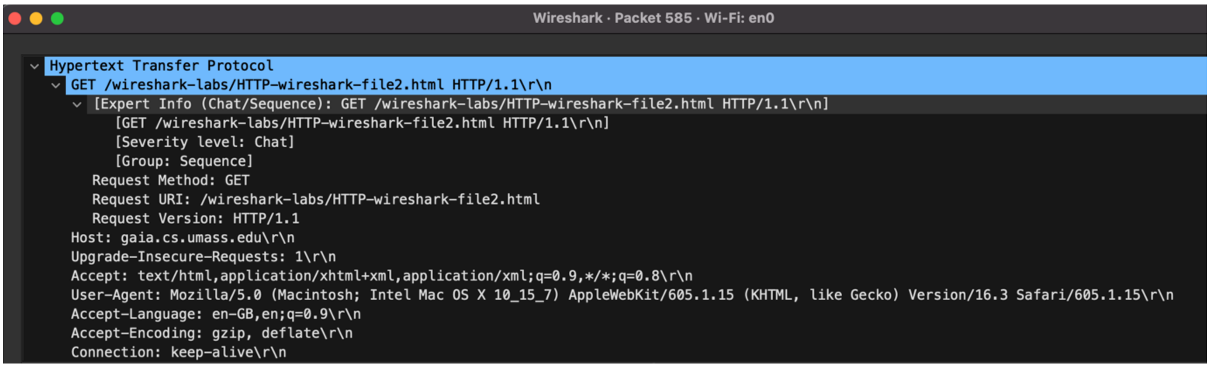
Answer: The content are being returned is 128 bytes.



```
> Frame 836: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface en0, id 0
> Ethernet II, Src: Cisco_ff:fc:34 (00:08:e3:ff:fc:34), Dst: Apple_40:72:b8 (bc:d0:74:40:72:b8)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.11.197.63
> Transmission Control Protocol, Src Port: 80, Dst Port: 53873, Seq: 1, Ack: 407, Len: 486
⌄ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Tue, 07 Feb 2023 01:02:58 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, 06 Feb 2023 06:59:01 GMT\r\n
    ETag: "80-5f40290e3ace5"\r\n
    Accept-Ranges: bytes\r\n
  ⌄ 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
```

Q8: 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?

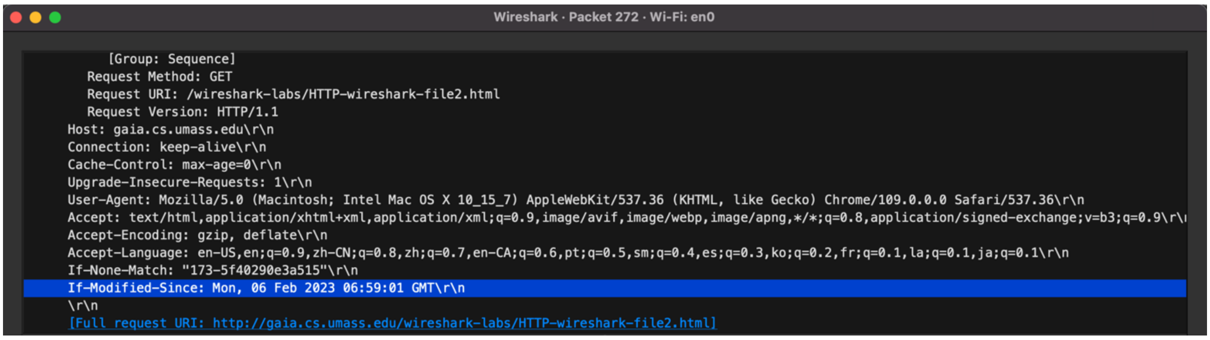
Answer: In the GET message, there is no IF-MODIFIED-SINCE line.



```
⌄ Hypertext Transfer Protocol
  ⌄ GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    ⌄ [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
        [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file2.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 (KHTML, like Gecko) Version/16.3 Safari/605.1.15\r\n
    Accept-Language: en-GB,en;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
```

Q10: 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 “IFMODIFIED-SINCE:” header?

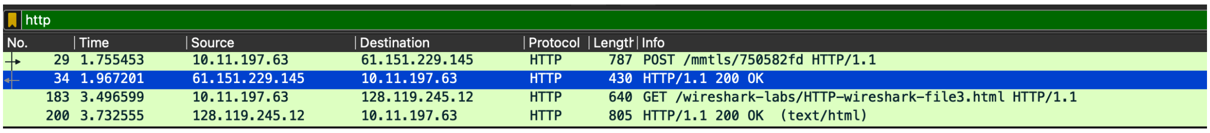
Answer: Yes, I saw the “IF-MODIFIED-SINCE:” line in the HTTP GET, the IFMODIFIED-SINCE: Mon, 06 Feb 2023 06:59:01 GMT\r\n (Those information about time and date).



```
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file2.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 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=0.9\r\
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7,en-CA;q=0.6,pt;q=0.5,sm;q=0.4,es;q=0.3,ko;q=0.2,fr;q=0.1,la;q=0.1,ja;q=0.1\r\n
    If-None-Match: "173-5f40290e3a515"\r\n
    If-Modified-Since: Mon, 06 Feb 2023 06:59:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

Q12: 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?

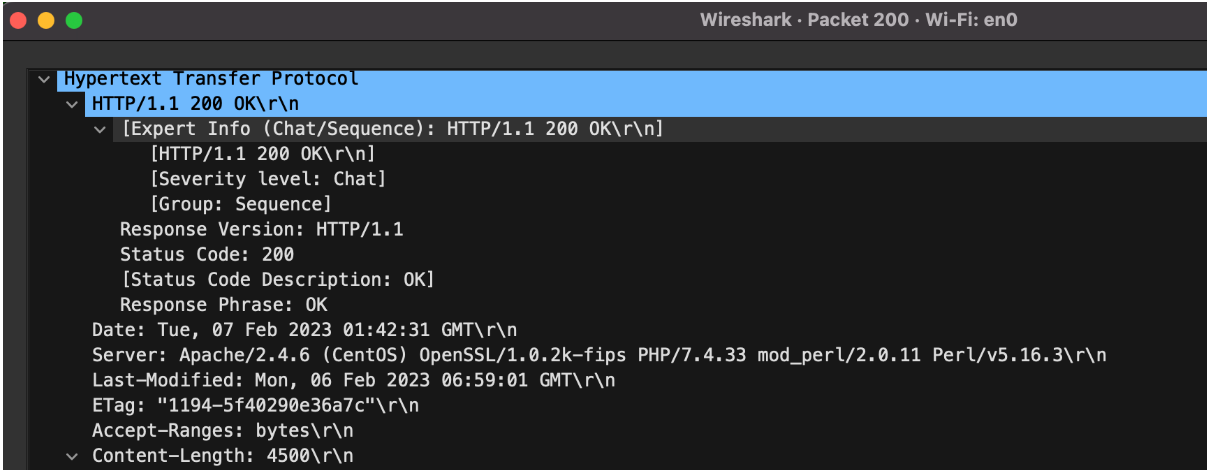
Answer: There have 1 HTTP GET request message, the packet number is 183.



No.	Time	Source	Destination	Protocol	Length	Info
29	1.755453	10.11.197.63	61.151.229.145	HTTP	787	POST /mmtls/750582fd HTTP/1.1
34	1.967201	61.151.229.145	10.11.197.63	HTTP	430	HTTP/1.1 200 OK
183	3.496599	10.11.197.63	128.119.245.12	HTTP	640	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
200	3.732555	128.119.245.12	10.11.197.63	HTTP	805	HTTP/1.1 200 OK (text/html)

Q14: What is the status code and phrase in the response?

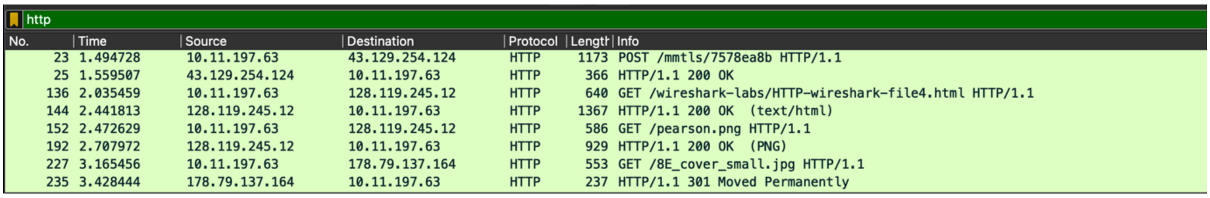
Answer: The status code is 200, and the phrase in the response is OK.



```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      [HTTP/1.1 200 OK\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
  Date: Tue, 07 Feb 2023 01:42:31 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, 06 Feb 2023 06:59:01 GMT\r\n
  ETag: "1194-5f40290e36a7c"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 4500\r\n
```

Q16: How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

Answer: There have 3 HTTP GET request messages. The GET requests sent to ip: 128.119.245.12 and 178.79.137.164.



No.	Time	Source	Destination	Protocol	Length	Info
23	1.494728	10.11.197.63	43.129.254.124	HTTP	1173	POST /mmtls/7578ea8b HTTP/1.1
25	1.559507	43.129.254.124	10.11.197.63	HTTP	366	HTTP/1.1 200 OK
136	2.035459	10.11.197.63	128.119.245.12	HTTP	640	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
144	2.441813	128.119.245.12	10.11.197.63	HTTP	1367	HTTP/1.1 200 OK (text/html)
152	2.472629	10.11.197.63	128.119.245.12	HTTP	586	GET /pearson.png HTTP/1.1
192	2.707972	128.119.245.12	10.11.197.63	HTTP	929	HTTP/1.1 200 OK (PNG)
227	3.165456	10.11.197.63	178.79.137.164	HTTP	553	GET /8E_cover_small.jpg HTTP/1.1
235	3.428444	178.79.137.164	10.11.197.63	HTTP	237	HTTP/1.1 301 Moved Permanently