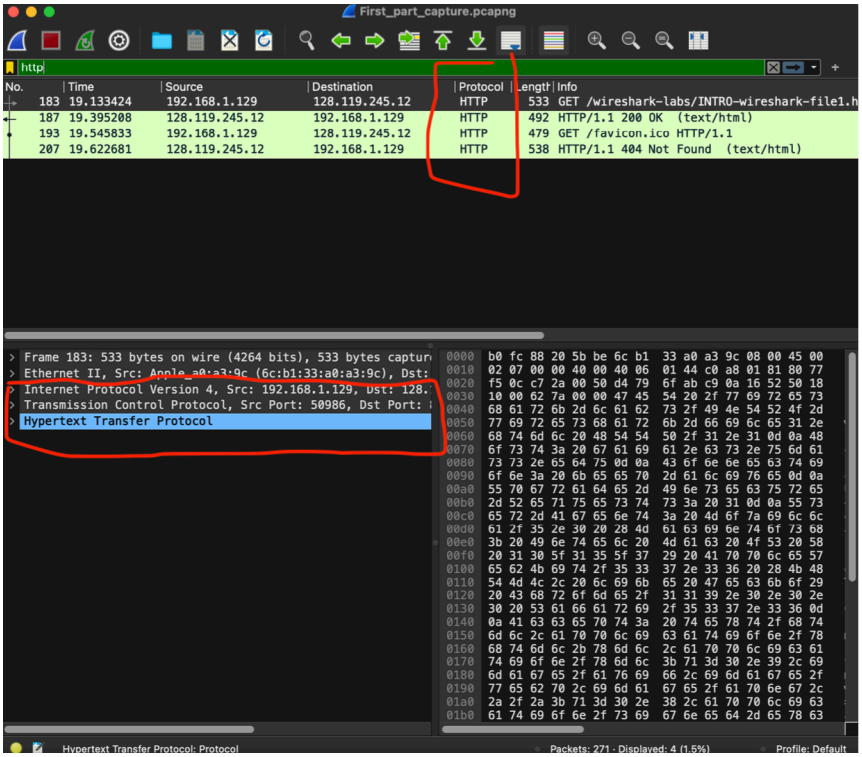
Part 1

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?

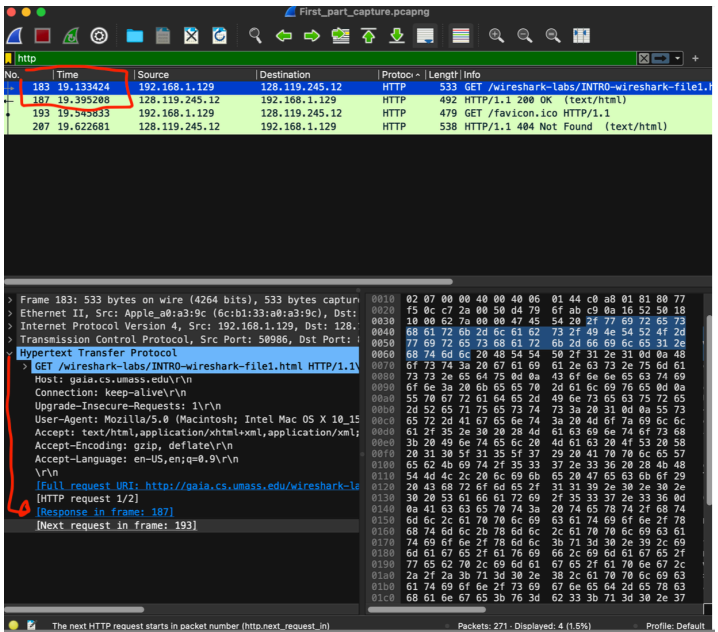
- In the Wireshark capture screenshot, the "Protocol" column shows instances of HTTP and TCP protocols within the network traffic data. The screenshot does not display the QUIC, DNS, UDP, or TLSv1.2 protocols.



2) How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. (If you want to display the Time field in time-of-day format, select the Wireshark *View* pull down menu, then select Time *Display Format*, then select *Time-of-day*.)

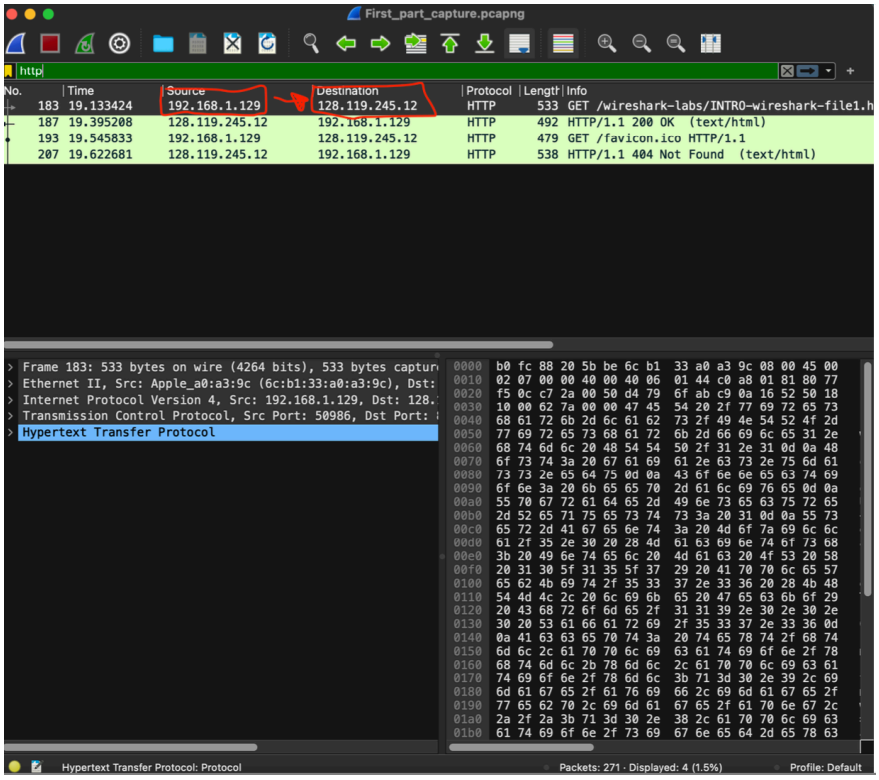
-

Time difference=Time of HTTP OK reply − Time of HTTP GET request
Time difference=19.395208 − 19.133248
Time difference=0.261960 seconds



3)What is the Internet address of the gaia.cs.umass.edu (also known as www-net.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

- The Internet address of gaia.cs.umass.edu at the time of the capture was 128.119.245.12.
- The Internet address of my computer that sent the HTTP GET message was 192.168.1.129.
-

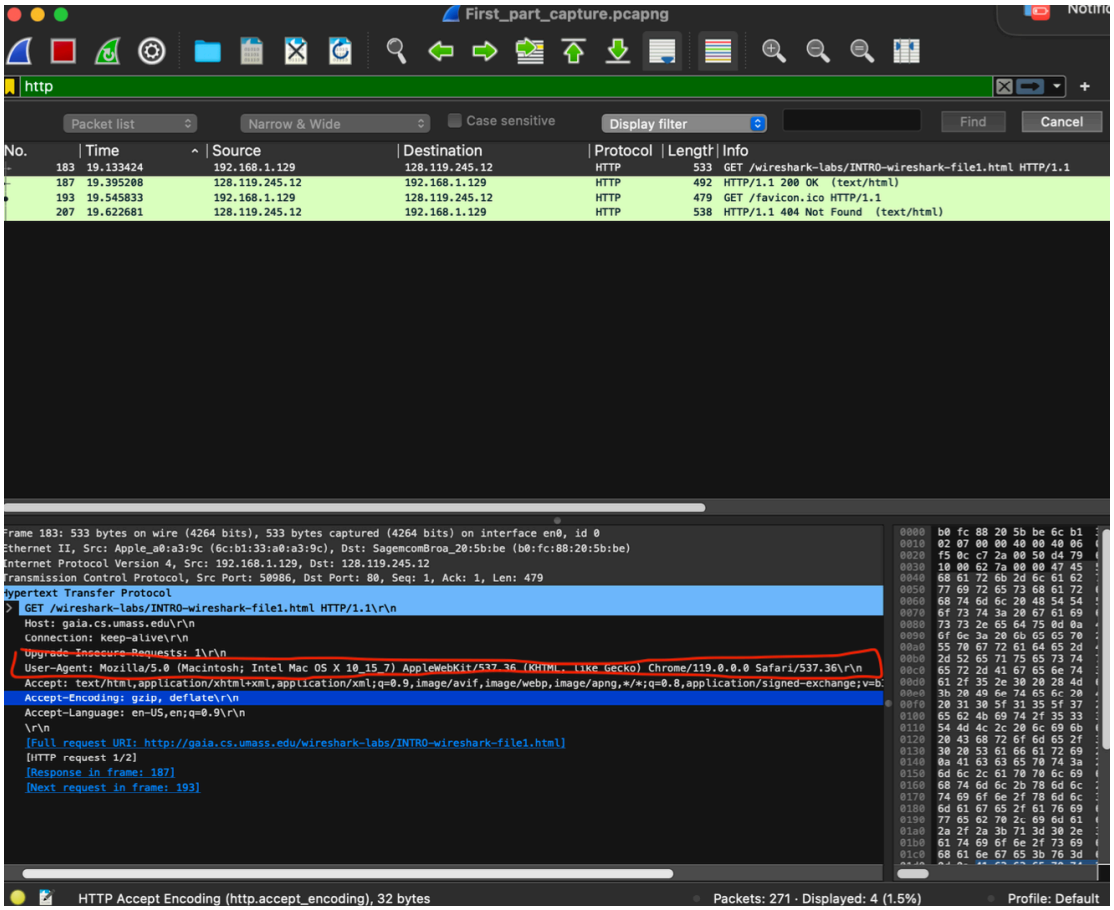


4) Expand the information on the HTTP message in the Wireshark "Details of selected packet" window (see Figure 3 above) so you can see the fields in the HTTP GET request message. What type of Web browser issued the HTTP request? The answer is shown at the right end of the information following the "User-Agent:" 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

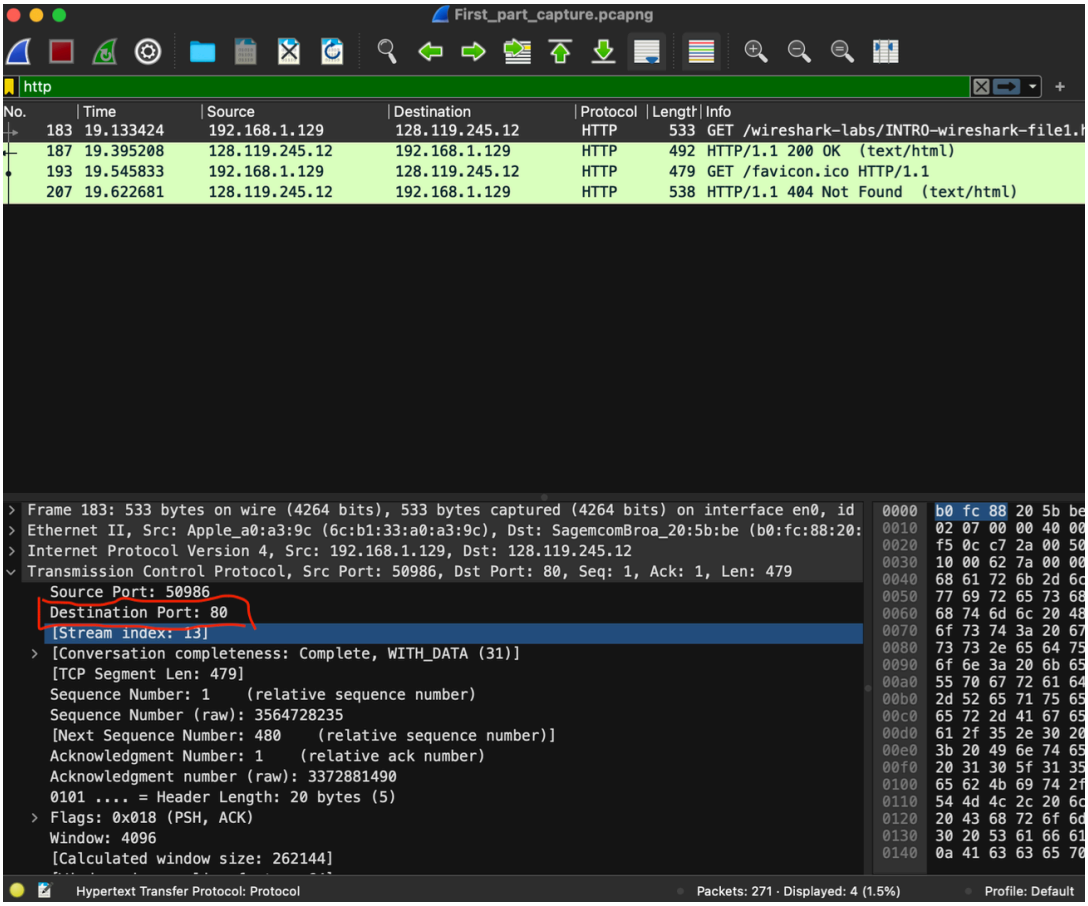
- User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36\r\n

- Mozilla/5.0 is a general token that used to indicate compatibility with the Mozilla rendering engine.
- (Macintosh; Intel Mac OS X 10_15_7) specifies that the operating system of the device using the browser is macOS version 10.15.7.
- AppleWebKit/537.36 specifies the rendering engine used by Chrome.
- (KHTML, like Gecko) is another token used for compatibility.
- Chrome/119.0.0.0 indicates the browser version.
- Safari/537.36 is included for historical reasons and refers to the WebKit-based rendering engine.



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?

- The destination port number for the TCP segment carrying the HTTP request is 80.



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.

/Users/alexgarza/Desktop/Mac-Home/School/UT Fall 2023/CS 326E/Labs/Lab02/First_part_capture.pcapng 271 total packets, 4 shown

```
No.     Time           Source                Destination           Protocol Length Info
    183 19.133424      192.168.1.129         128.119.245.12        HTTP     533    GET /wireshark-
labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 183: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits) on interface en0, id 0
Ethernet II, Src: Apple_a0:a3:9c (6c:b1:33:a0:a3:9c), Dst: SagemcomBroa_20:5b:be (b0:fc:
88:20:5b:be)
Internet Protocol Version 4, Src: 192.168.1.129, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50986, Dst Port: 80, Seq: 1, Ack: 1, Len: 479
    Source Port: 50986
    Destination Port: 80
    [Stream index: 13]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 479]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3564728235
    [Next Sequence Number: 480    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3372881490
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 4096
    [Calculated window size: 262144]
    [Window size scaling factor: 64]
    Checksum: 0x627a [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (479 bytes)
Hypertext Transfer Protocol
```

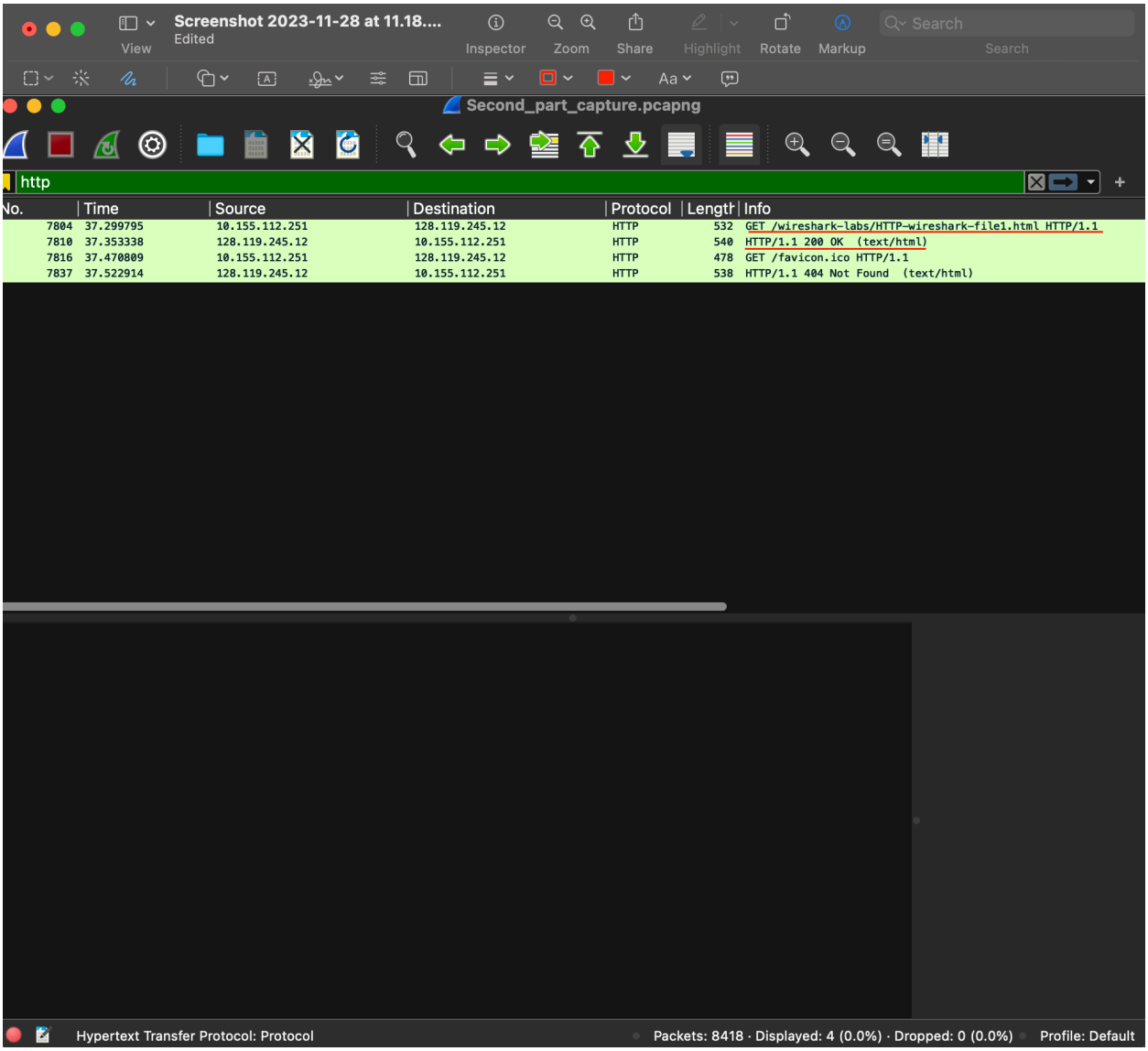
/Users/alexgarza/Desktop/Mac-Home/School/UT Fall 2023/CS 326E/Labs/Lab02/First_part_capture.pcapng 271 total packets, 4 shown

```
No.     Time           Source                Destination           Protocol Length Info
    187 19.395208      128.119.245.12        192.168.1.129         HTTP     492    HTTP/1.1 200 OK
(text/html)
Frame 187: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface en0, id 0
Ethernet II, Src: SagemcomBroa_20:5b:be (b0:fc:88:20:5b:be), Dst: Apple_a0:a3:9c
(6c:b1:33:a0:a3:9c)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.129
Transmission Control Protocol, Src Port: 80, Dst Port: 50986, Seq: 1, Ack: 480, Len: 438
    Source Port: 80
    Destination Port: 50986
    [Stream index: 13]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 438]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3372881490
    [Next Sequence Number: 439    (relative sequence number)]
    Acknowledgment Number: 480    (relative ack number)
    Acknowledgment number (raw): 3564728714
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0xf478 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (438 bytes)
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)
```

Part2

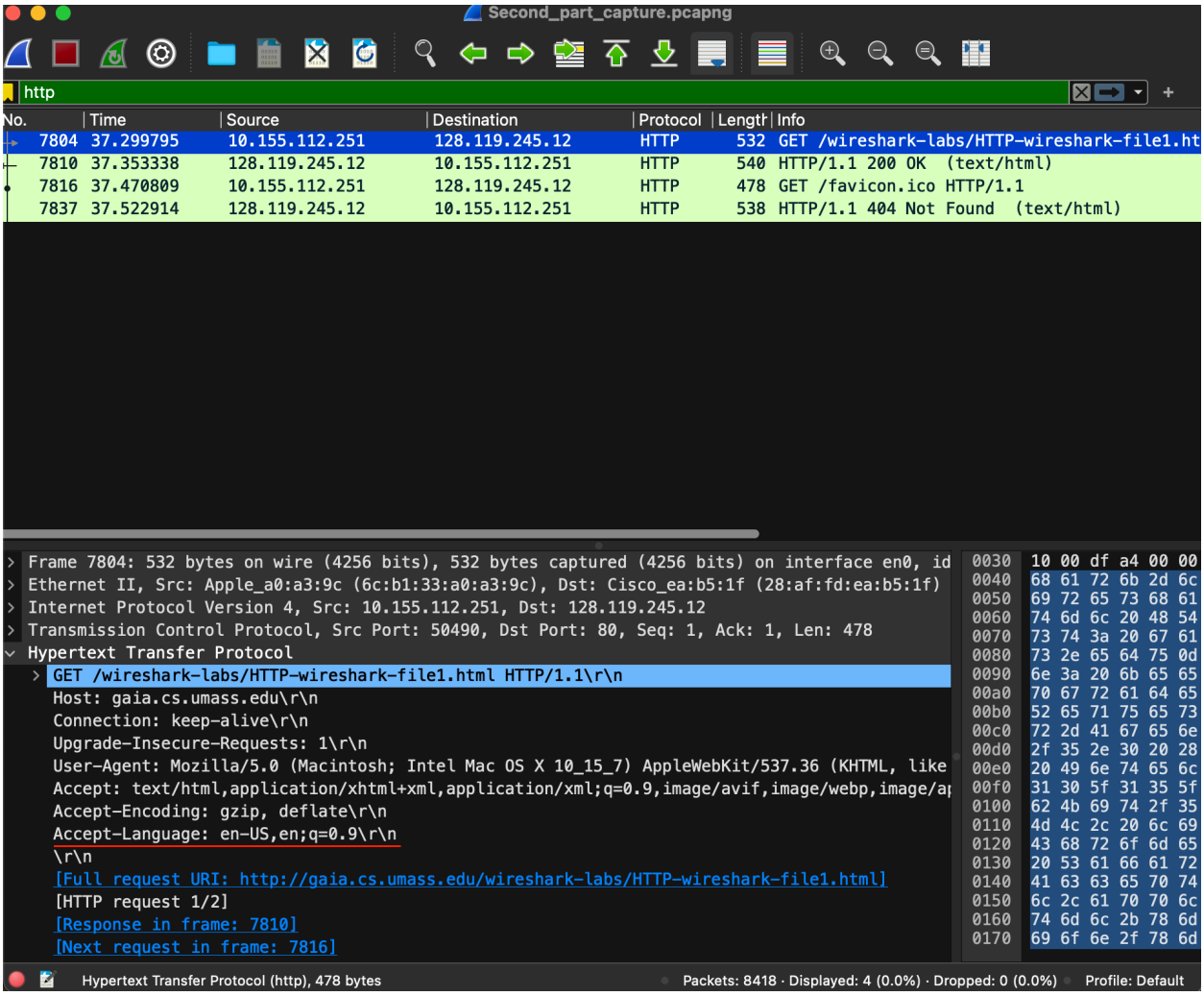
1) Is your browser running HTTP version 1.0, 1.1, or 2? What version of HTTP is the server running?

- The browser is running HTTP 1.1, which can be inferred from the GET request packet that includes "HTTP/1.1" in the Info column next to the GET method.The server is also running HTTP 1.1, as seen by the response packet with "HTTP/1.1 200 OK" in the Info column, which is the server's response to the GET request.



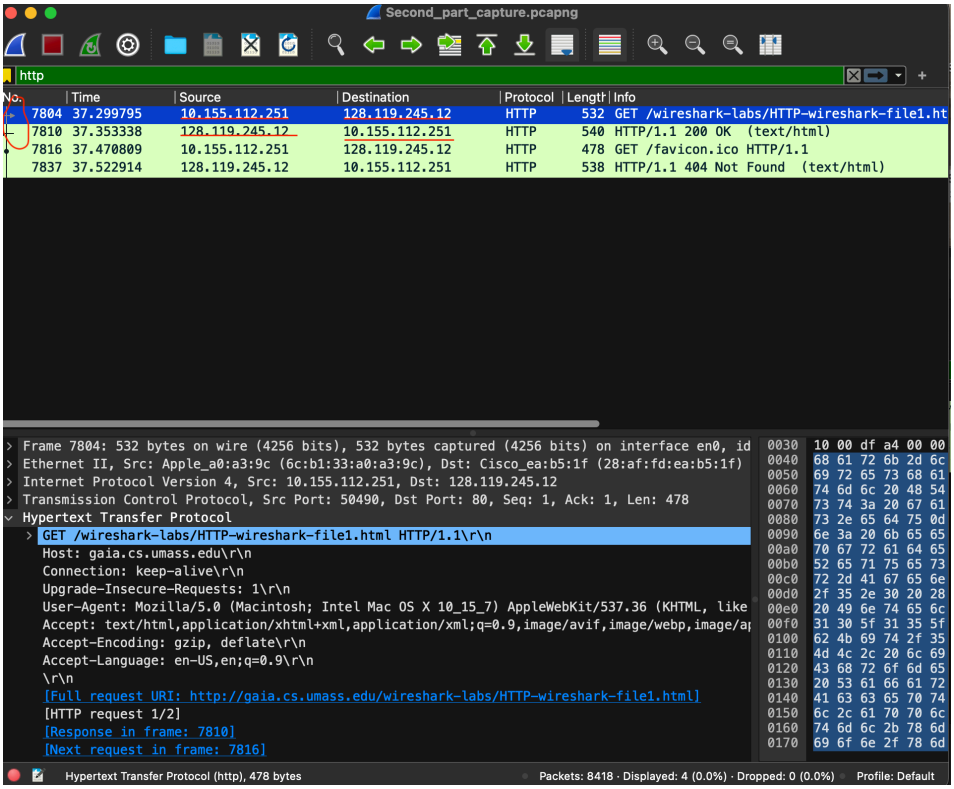
2) What languages (if any) does your browser indicate that it can accept to the server?

- en-US: The browser prefers American English.



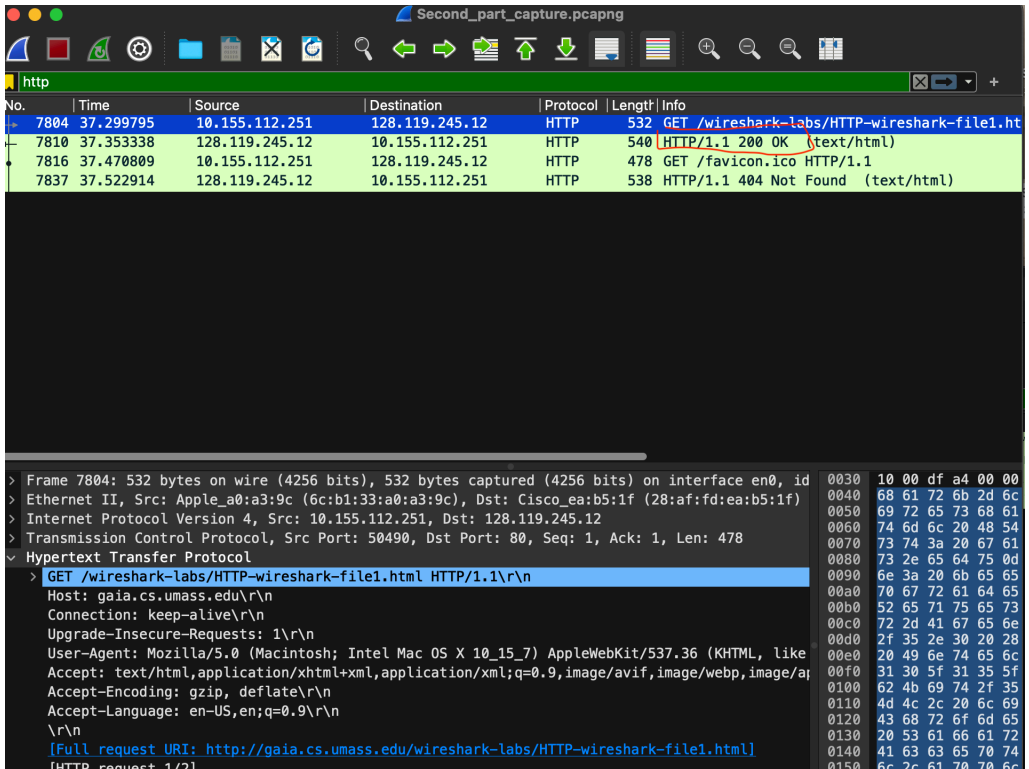
3)What is the IP address of your computer? What is the IP address of the gaia.cs.umass.edu server?

- My IP address of your computer is 10.155.112.251.
- The IP address of the gaia.cs.umass.edu server is 128.119.245.12.



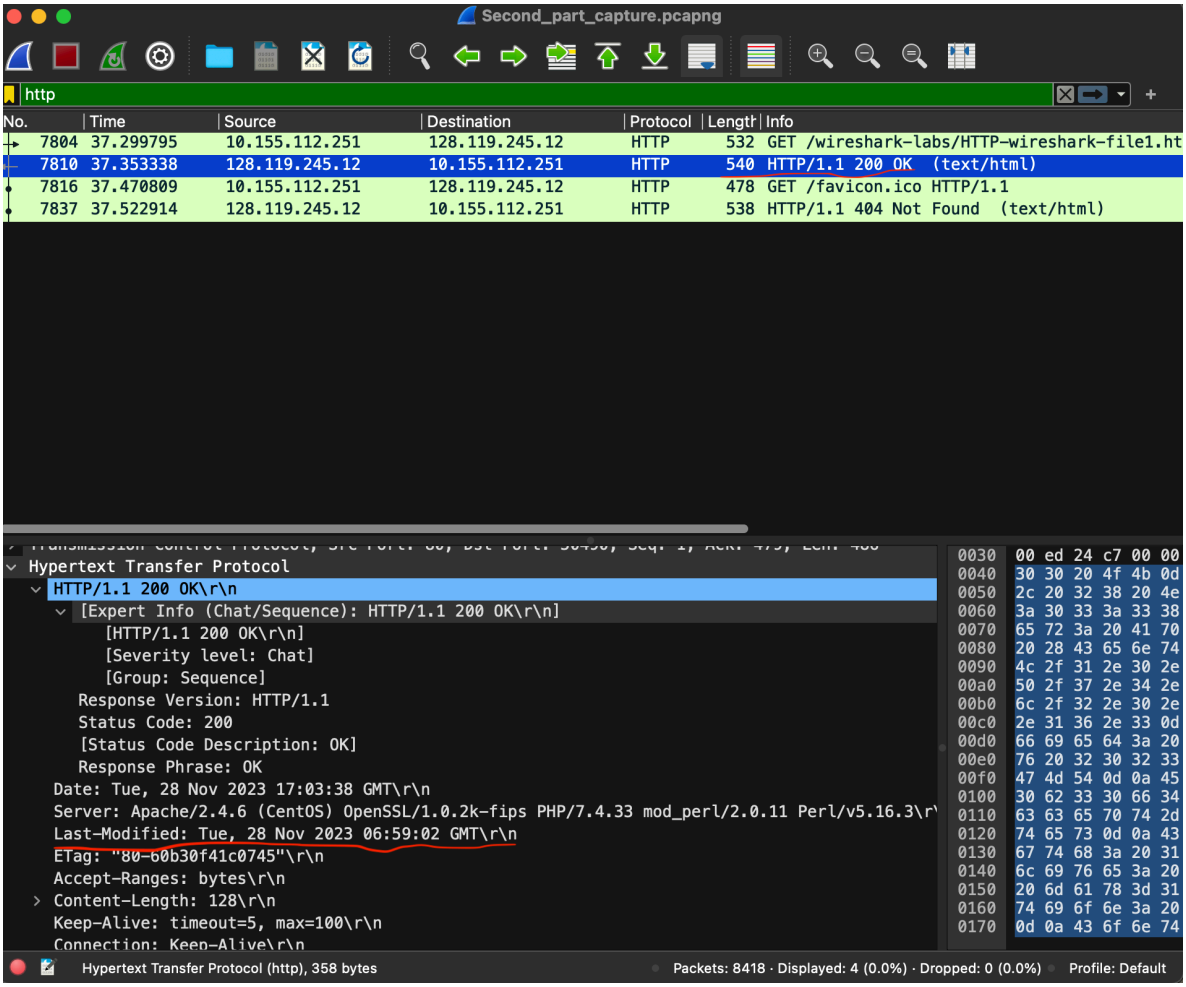
4) What is the status code returned from the server to your browser?

- The status code returned from the server to the browser is 200, as seen in the packet with the HTTP response. This is indicated in the Info column with the text "HTTP/1.1 200 OK.
- "A 200 OK status code is a standard response in HTTP, indicating that the request was successfully received, understood, and processed by the server."



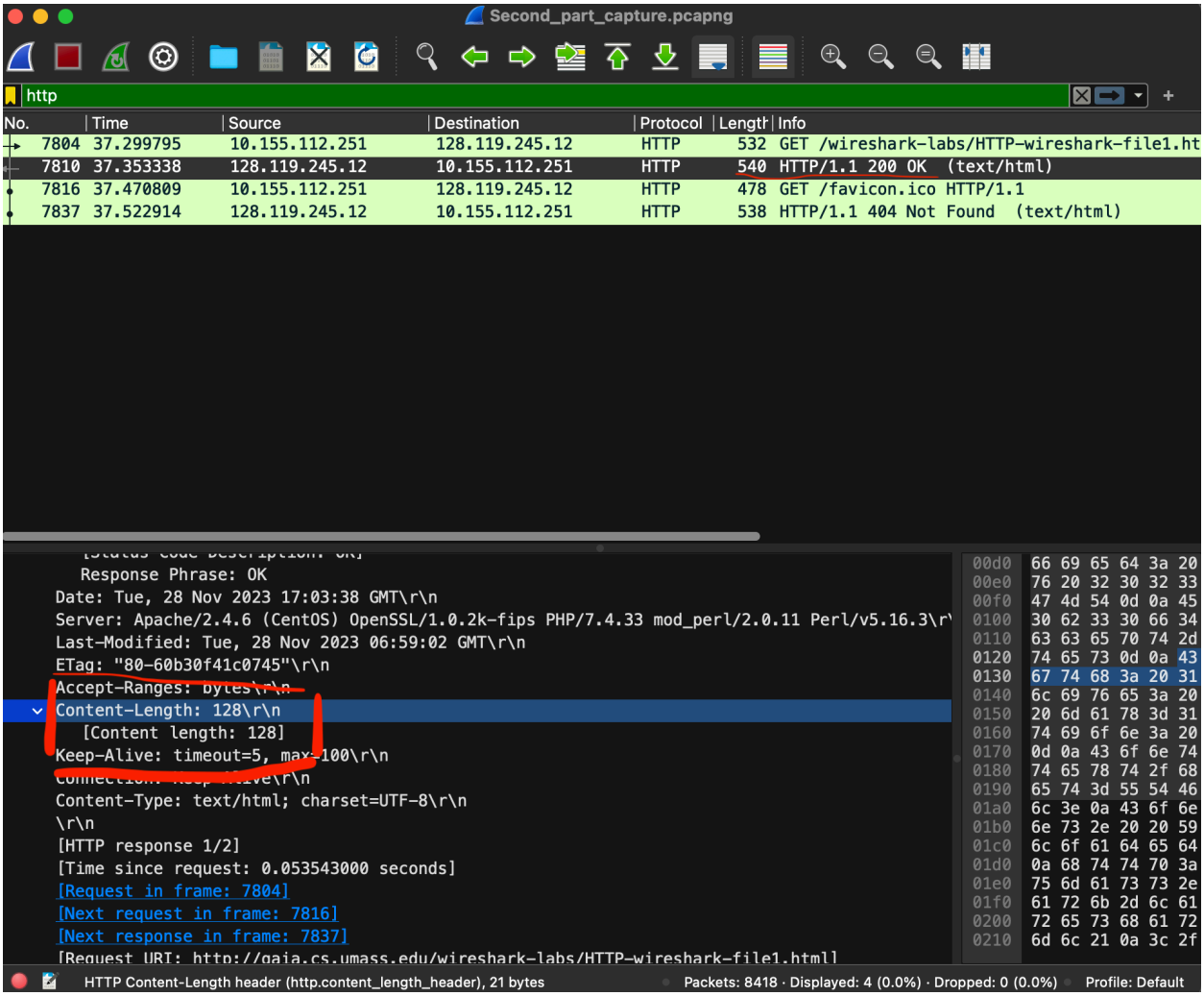
5) When was the HTML file that you are retrieving last modified at the server?

- Last modified at the server on "Tue, 28 Nov 2023 06:59:02 GMT",



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

- The HTTP response indicates that the content length being returned to the browser is "128" bytes.



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.

- I do not believe so.

Host: gaia.cs.umass.edu
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
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
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

These are header-name:values. There is not one that Isee that is not found already in the packet-listing window based on this packet.