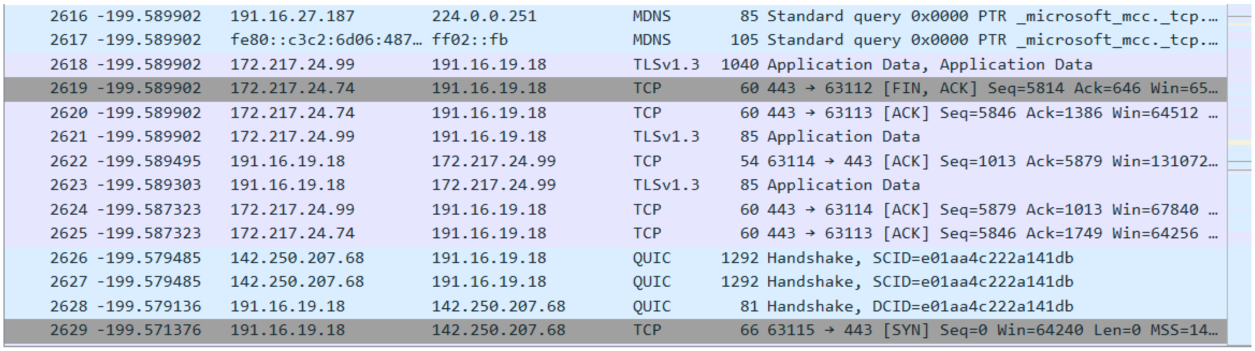
Name: Nguyen Minh Hieu

Class: CC01

Lab1a: Introduction to Wireshark Packet Sniffer Tool

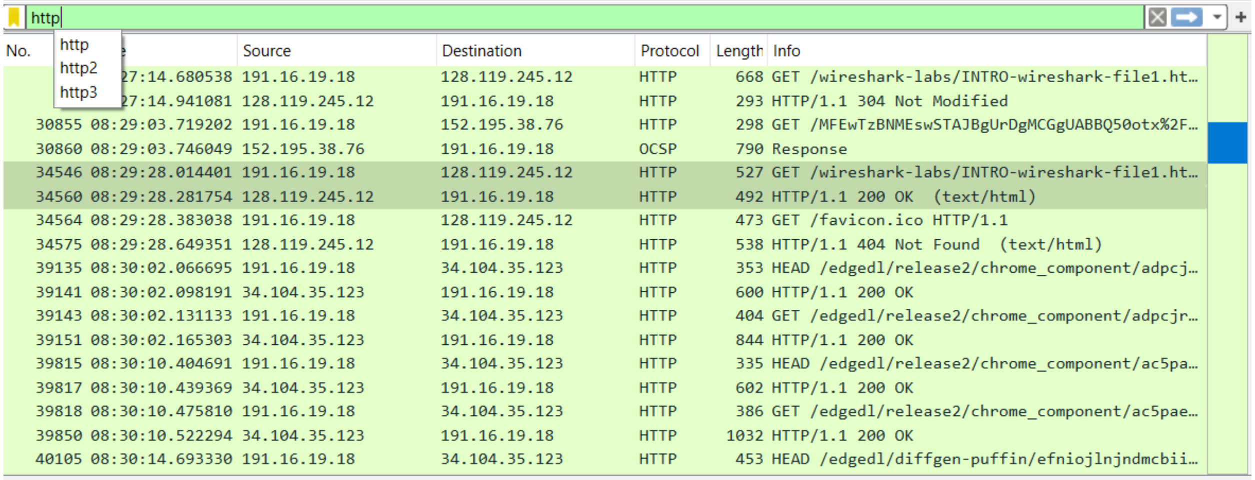
Q.1: List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.



```
2616 -199.589902  191.16.27.187     224.0.0.251      MDNS      85 Standard query 0x0000 PTR _microsoft_mcc._tcp.…
2617 -199.589902  fe80::c3c2:6d06:487… ff02::fb     MDNS     105 Standard query 0x0000 PTR _microsoft_mcc._tcp.…
2618 -199.589902  172.217.24.99     191.16.19.18     TLSv1.3 1040 Application Data, Application Data
2619 -199.589902  172.217.24.74     191.16.19.18     TCP       60 443 → 63112 [FIN, ACK] Seq=5814 Ack=646 Win=65…
2620 -199.589902  172.217.24.74     191.16.19.18     TCP       60 443 → 63113 [ACK] Seq=5846 Ack=1386 Win=64512 …
2621 -199.589902  172.217.24.99     191.16.19.18     TLSv1.3   85 Application Data
2622 -199.589495  191.16.19.18      172.217.24.74    TCP       54 63114 → 443 [ACK] Seq=1013 Ack=5879 Win=131072…
2623 -199.589303  191.16.19.18      172.217.24.99    TLSv1.3   85 Application Data
2624 -199.587323  172.217.24.99     191.16.19.18     TCP       60 443 → 63114 [ACK] Seq=5879 Ack=1013 Win=67840 …
2625 -199.587323  172.217.24.74     191.16.19.18     TCP       60 443 → 63113 [ACK] Seq=5846 Ack=1749 Win=64256 …
2626 -199.579485  142.250.207.68    191.16.19.18     QUIC    1292 Handshake, SCID=e01aa4c222a141db
2627 -199.579485  142.250.207.68    191.16.19.18     QUIC    1292 Handshake, SCID=e01aa4c222a141db
2628 -199.579136  191.16.19.18      142.250.207.68   QUIC      81 Handshake, DCID=e01aa4c222a141db
2629 -199.571376  191.16.19.18      142.250.207.68   TCP       66 63115 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=14…
```

Three different protocols are: MDNS, TCP, QUIC

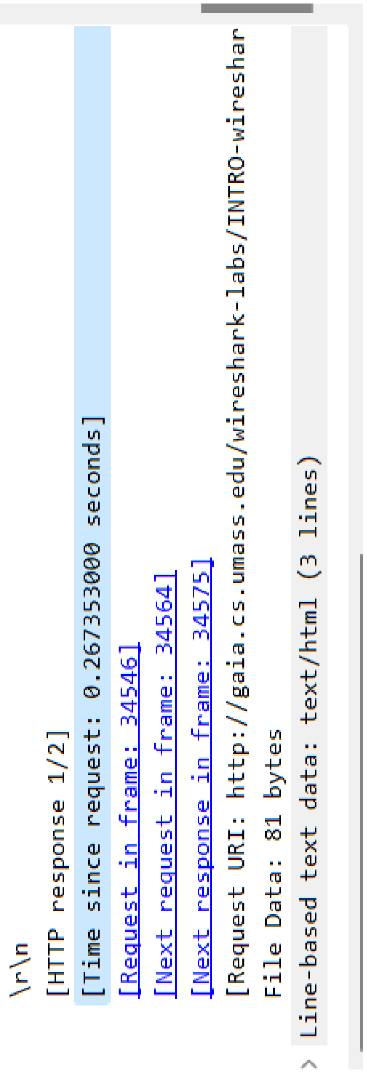
Q.2: How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet□listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the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



```
No.   e                Source          Destination      Protocol Length Info
      27:14.680538 191.16.19.18    128.119.245.12   HTTP      668 GET /wireshark-labs/INTRO-wireshark-file1.ht…
      27:14.941081 128.119.245.12  191.16.19.18     HTTP      293 HTTP/1.1 304 Not Modified
30855 08:29:03.719202 191.16.19.18    152.195.38.76    HTTP      298 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2F…
30860 08:29:03.746049 152.195.38.76   191.16.19.18     OCSP      790 Response
34546 08:29:28.014401 191.16.19.18    128.119.245.12   HTTP      527 GET /wireshark-labs/INTRO-wireshark-file1.ht…
34560 08:29:28.281754 128.119.245.12  191.16.19.18     HTTP      492 HTTP/1.1 200 OK  (text/html)
34564 08:29:28.383038 191.16.19.18    128.119.245.12   HTTP      473 GET /favicon.ico HTTP/1.1
34575 08:29:28.649351 128.119.245.12  191.16.19.18     HTTP      538 HTTP/1.1 404 Not Found  (text/html)
39135 08:30:02.066695 191.16.19.18    34.104.35.123    HTTP      353 HEAD /edgedl/release2/chrome_component/adpcj…
39141 08:30:02.098191 34.104.35.123   191.16.19.18     HTTP      600 HTTP/1.1 200 OK
39143 08:30:02.131133 191.16.19.18    34.104.35.123    HTTP      404 GET /edgedl/release2/chrome_component/adpcjr…
39151 08:30:02.165303 34.104.35.123   191.16.19.18     HTTP      844 HTTP/1.1 200 OK
39815 08:30:10.404691 191.16.19.18    34.104.35.123    HTTP      335 HEAD /edgedl/release2/chrome_component/ac5pa…
39817 08:30:10.439369 34.104.35.123   191.16.19.18     HTTP      602 HTTP/1.1 200 OK
39818 08:30:10.475810 191.16.19.18    34.104.35.123    HTTP      386 GET /edgedl/release2/chrome_component/ac5pae…
39850 08:30:10.522294 34.104.35.123   191.16.19.18     HTTP     1032 HTTP/1.1 200 OK
40105 08:30:14.693330 191.16.19.18    34.104.35.123    HTTP      453 HEAD /edgedl/diffgen-puffin/efniojlnjndmcbii…
```

Amount of time for the HTTP GET message was sent until the HTTP OK reply was received:

From 8:29:28.014401 to 8:29:28.281754: 0.267353 s



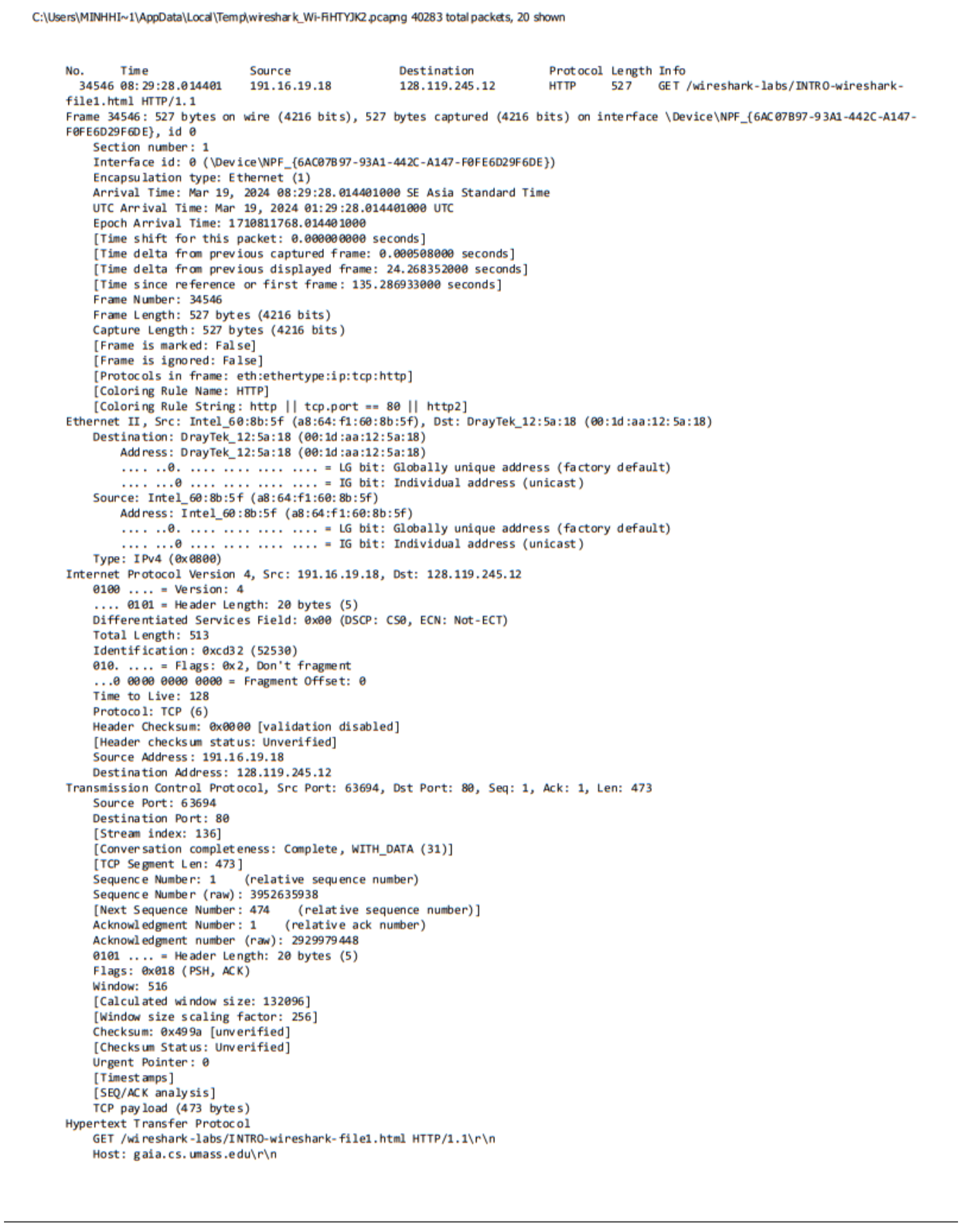
```
\r\n
[HTTP response 1/2]
[Time since request: 0.267353000 seconds]
[Request in frame: 34546]
[Next request in frame: 34564]
[Next response in frame: 34575]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshar
File Data: 81 bytes
```

Q.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?

Internet address of the gaia.cs.umass.edu: 128.119.245.1

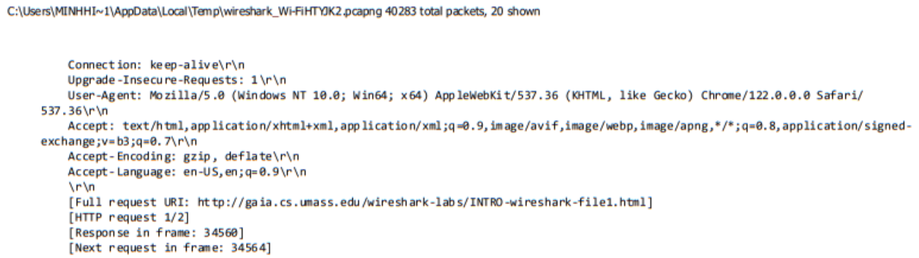
Internet address of my computer: 191.16.19.18

Q.4: 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.



C:\Users\MINHHI~1\AppData\Local\Temp\wireshark_Wi-FiHTYJK2.pcapng 40283 total packets, 20 shown

```
No.     Time               Source                Destination           Protocol Length Info
  34546 08:29:28.014401    191.16.19.18          128.119.245.12        HTTP     527    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 34546: 527 bytes on wire (4216 bits), 527 bytes captured (4216 bits) on interface \Device\NPF_{6AC07B97-93A1-442C-A147-
F0FE6D29F6DE}, id 0
    Section number: 1
    Interface id: 0 (\Device\NPF_{6AC07B97-93A1-442C-A147-F0FE6D29F6DE})
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 19, 2024 08:29:28.014401000 SE Asia Standard Time
    UTC Arrival Time: Mar 19, 2024 01:29:28.014401000 UTC
    Epoch Arrival Time: 1710811768.014401000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000508000 seconds]
    [Time delta from previous displayed frame: 24.268352000 seconds]
    [Time since reference or first frame: 135.286933000 seconds]
    Frame Number: 34546
    Frame Length: 527 bytes (4216 bits)
    Capture Length: 527 bytes (4216 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Intel_60:8b:5f (a8:64:f1:60:8b:5f), Dst: DrayTek_12:5a:18 (00:1d:aa:12:5a:18)
    Destination: DrayTek_12:5a:18 (00:1d:aa:12:5a:18)
        Address: DrayTek_12:5a:18 (00:1d:aa:12:5a:18)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Intel_60:8b:5f (a8:64:f1:60:8b:5f)
        Address: Intel_60:8b:5f (a8:64:f1:60:8b:5f)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 191.16.19.18, 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: 513
    Identification: 0xcd32 (52530)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 191.16.19.18
    Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port: 63694, Dst Port: 80, Seq: 1, Ack: 1, Len: 473
    Source Port: 63694
    Destination Port: 80
    [Stream index: 136]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 473]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3952635938
    [Next Sequence Number: 474    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2929979448
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 516
    [Calculated window size: 132096]
    [Window size scaling factor: 256]
    Checksum: 0x499a [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (473 bytes)
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
```



```
C:\Users\MINHHI~1\AppData\Local\Temp\wireshark_Wi-FiHTYJK2.pcapng 40283 total packets, 20 shown

        Connection: keep-alive\r\n
        Upgrade-Insecure-Requests: 1\r\n
        User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/
    537.36\r\n
        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
    exchange;v=b3;q=0.7\r\n
        Accept-Encoding: gzip, deflate\r\n
        Accept-Language: en-US,en;q=0.9\r\n
        \r\n
        [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
        [HTTP request 1/2]
        [Response in frame: 34560]
        [Next request in frame: 34564]
```

GET message

```
No.     Time               Source                Destination           Protocol Length Info
  34560 08:29:28.281754    128.119.245.12        191.16.19.18          HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 34560: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{6AC07B97-93A1-442C-A147-F0FE6D29F6DE}, id
0
    Section number: 1
    Interface id: 0 (\Device\NPF_{6AC07B97-93A1-442C-A147-F0FE6D29F6DE})
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 19, 2024 08:29:28.281754000 SE Asia Standard Time
    UTC Arrival Time: Mar 19, 2024 01:29:28.281754000 UTC
    Epoch Arrival Time: 1710811768.281754000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000918000 seconds]
    [Time delta from previous displayed frame: 0.267353000 seconds]
    [Time since reference or first frame: 135.554286000 seconds]
    Frame Number: 34560
    Frame Length: 492 bytes (3936 bits)
    Capture Length: 492 bytes (3936 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: DrayTek_12:5a:18 (00:1d:aa:12:5a:18), Dst: Intel_60:8b:5f (a8:64:f1:60:8b:5f)
    Destination: Intel_60:8b:5f (a8:64:f1:60:8b:5f)
        Address: Intel_60:8b:5f (a8:64:f1:60:8b:5f)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: DrayTek_12:5a:18 (00:1d:aa:12:5a:18)
        Address: DrayTek_12:5a:18 (00:1d:aa:12:5a:18)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 191.16.19.18
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
    Total Length: 478
    Identification: 0xc4ca (50378)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 39
    Protocol: TCP (6)
    Header Checksum: 0x4589 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.119.245.12
    Destination Address: 191.16.19.18
Transmission Control Protocol, Src Port: 80, Dst Port: 63694, Seq: 1, Ack: 474, Len: 438
    Source Port: 80
    Destination Port: 63694
    [Stream index: 136]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 438]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2929979448
    [Next Sequence Number: 439    (relative sequence number)]
    Acknowledgment Number: 474    (relative ack number)
    Acknowledgment number (raw): 3952636411
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0xc3b0 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (438 bytes)
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Tue, 19 Mar 2024 01:29:28 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, 18 Mar 2024 05:59:01 GMT\r\n
    ETag: "51-613e90de41caa"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
```

```
    [Time since request: 0.267353000 seconds]
    [Request in frame: 34546]
    [Next request in frame: 34564]
    [Next response in frame: 34575]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
```

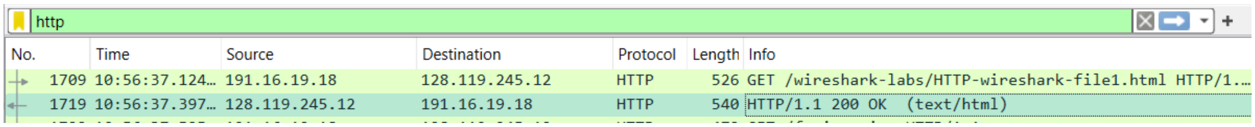
OK message

LAB2a: Visit this link to download: [LabMMT/2152555_NguyenMinhHieu_Lab2a.pkt at main · ngynmhieu/LabMMT (github.com)]

LAB3a: Wireshark Lab: HTTP

Q1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the

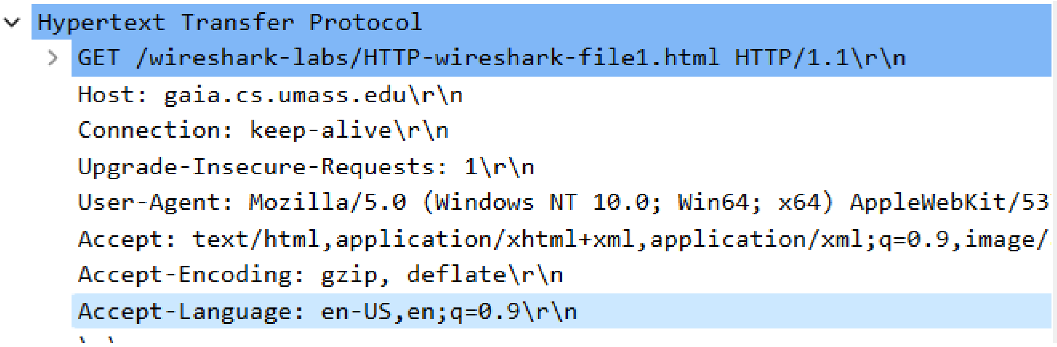
server running?



```
http
No.  Time                Source          Destination     Protocol  Length  Info
1709 10:56:37.124…       191.16.19.18    128.119.245.12  HTTP      526     GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.…
1719 10:56:37.397…       128.119.245.12  191.16.19.18    HTTP      540     HTTP/1.1 200 OK  (text/html)
```

Version 1.1

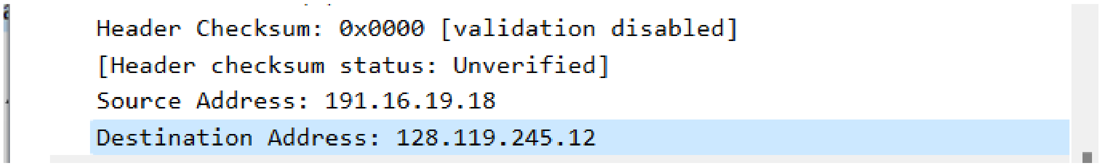
Q2. What languages (if any) does your browser indicate that it can accept to the server?



```
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/53
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
```

Accept language” en-US, en

Q3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

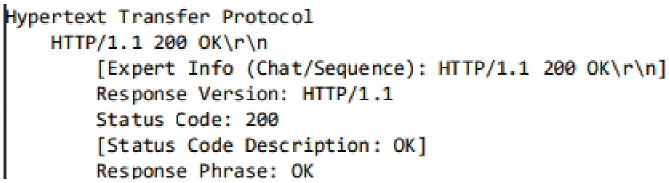


```
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 191.16.19.18
Destination Address: 128.119.245.12
```

IP address of my computer: 191.16.19.18

IP address of gaia.cs.umass.edu server: 128.119.245.12

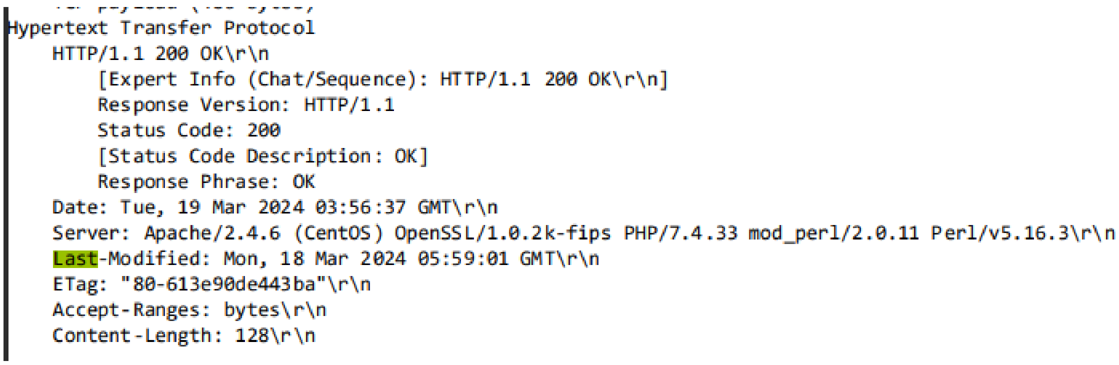
4. What is the status code returned from the server to your browser?



```
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
```

Status code: 200

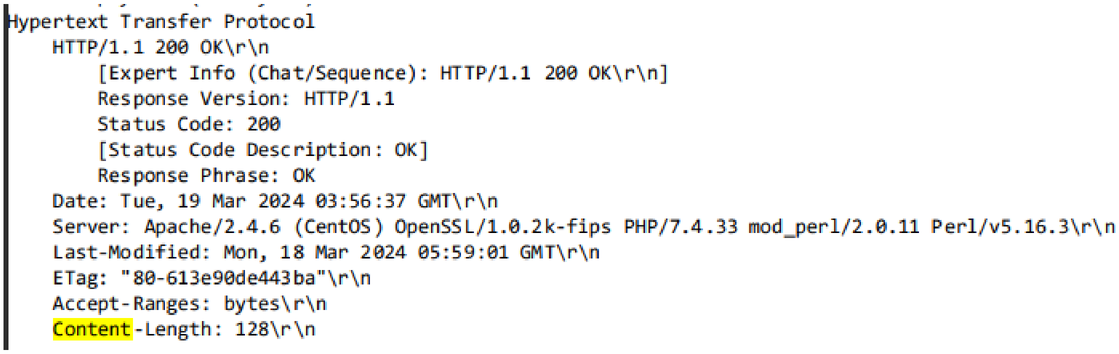
5. When was the HTML file that you are retrieving last modified at the server?



```
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: Tue, 19 Mar 2024 03:56:37 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, 18 Mar 2024 05:59:01 GMT\r\n
    ETag: "80-613e90de443ba"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 128\r\n
```

Last modified: Monday, 18 March 2024 5:59:01 GMT

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



```
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: Tue, 19 Mar 2024 03:56:37 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, 18 Mar 2024 05:59:01 GMT\r\n
    ETag: "80-613e90de443ba"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 128\r\n
```

128 bytes

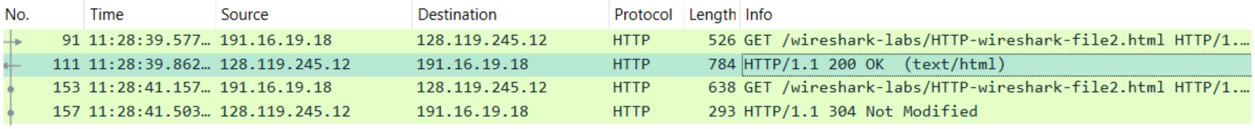
7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one

According to the packet data given in the prior discussion, there are no headers present in the data that are not shown in the packet-listing window.

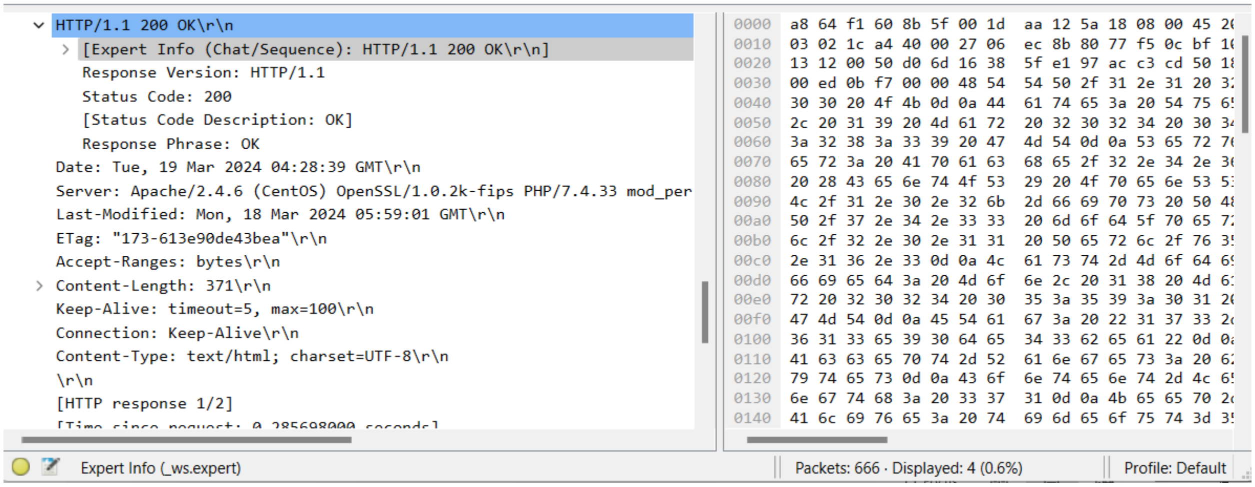
8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?

No, there isn't exist this parameter

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



```
No.   Time           Source          Destination      Protocol  Length  Info
  91 11:28:39.577… 191.16.19.18    128.119.245.12   HTTP        526 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.…
 111 11:28:39.862… 128.119.245.12  191.16.19.18     HTTP        784 HTTP/1.1 200 OK  (text/html)
 153 11:28:41.157… 191.16.19.18    128.119.245.12   HTTP        638 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.…
 157 11:28:41.503… 128.119.245.12  191.16.19.18     HTTP        293 HTTP/1.1 304 Not Modified
```



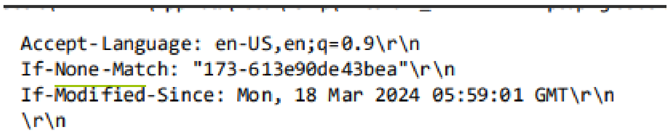
```
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Tue, 19 Mar 2024 04:28:39 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_per
    Last-Modified: Mon, 18 Mar 2024 05:59:01 GMT\r\n
    ETag: "173-613e90de43bea"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 371\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 1/2]
    [Time since request: 0.285698000 seconds]
```

```
0000  a8 64 f1 60 8b 5f 00 1d  aa 12 5a 18 08 00 45 2
0010  03 02 1c a4 40 00 27 06  ec 8b 80 77 f5 0c bf 1
0020  13 12 00 50 d0 6d 16 38  5f e1 97 ac c3 cd 50 1
0030  00 ed 0b f7 00 00 48 54  54 50 2f 31 2e 31 20 3
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 54 75 6
0050  2c 20 31 39 20 4d 61 72  20 32 30 32 34 20 30 3
0060  3a 32 38 3a 33 39 20 47  4d 54 0d 0a 53 65 72 7
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 3
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 5
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73 20 50 4
00a0  50 2f 37 2e 34 2e 33 33  20 6d 6f 64 5f 70 65 7
00b0  6c 2f 32 2e 30 2e 31 31  20 50 65 72 6c 2f 76 3
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 6
00d0  66 69 65 64 3a 20 4d 6f  6e 2c 20 31 38 20 4d 6
00e0  72 20 32 30 32 34 20 30  35 3a 35 39 3a 30 31 2
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 31 37 33 2
0100  36 31 33 65 39 30 64 65  34 33 62 65 61 22 0d 0
0110  41 63 63 65 70 74 2d 52  61 6e 67 65 73 3a 20 6
0120  79 74 65 73 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 6
0130  6e 67 74 68 3a 20 33 37  31 0d 0a 4b 65 65 70 2
0140  41 6c 69 76 65 3a 20 74  69 6d 65 6f 75 74 3d 3
```

Expert Info (_ws.expert)   Packets: 666 · Displayed: 4 (0.6%)   Profile: Default

Indeed, the server did purposefully send back the file’s contents. This is evident from the HTTP response status “200 OK”, signifying that the server has successfully handled the request and is now transmitting the data.

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?

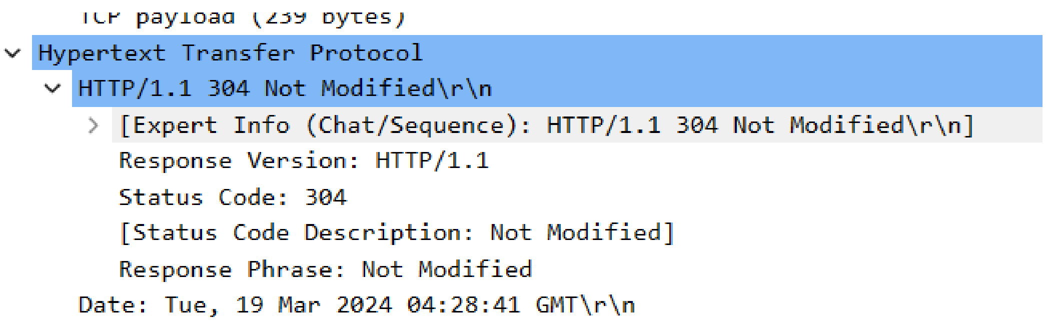


```
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "173-613e90de43bea"\r\n
If-Modified-Since: Mon, 18 Mar 2024 05:59:01 GMT\r\n
\r\n
```

If-Modified-Since: Mon, 18 Mar 2024 05:59:01 GMT\r\n

The server utilizes this data to ascertain if the browser’s cached file version is the most recent one. If there have been no modifications to the file on the server since that time, the server responds with a “304 Not Modified” status code, as demonstrated in the response you supplied.

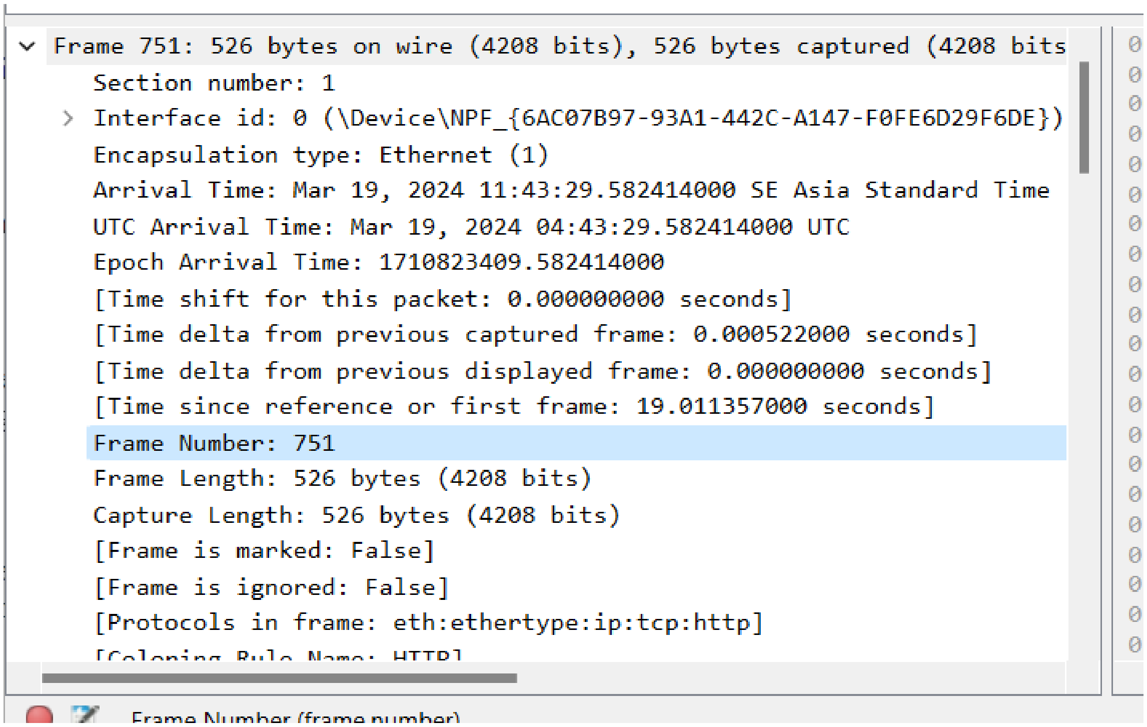
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.



```
      TCP payload (239 bytes)
v Hypertext Transfer Protocol
  v HTTP/1.1 304 Not Modified\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
    Date: Tue, 19 Mar 2024 04:28:41 GMT\r\n
```

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?

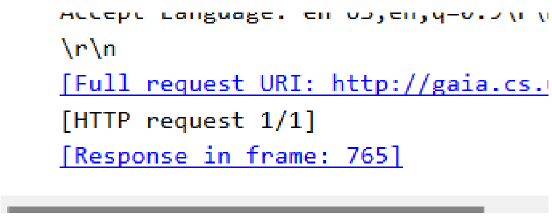
Only one: Frame 751



```
v Frame 751: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits
      Section number: 1
    > Interface id: 0 (\Device\NPF_{6AC07B97-93A1-442C-A147-F0FE6D29F6DE})
      Encapsulation type: Ethernet (1)
      Arrival Time: Mar 19, 2024 11:43:29.582414000 SE Asia Standard Time
      UTC Arrival Time: Mar 19, 2024 04:43:29.582414000 UTC
      Epoch Arrival Time: 1710823409.582414000
      [Time shift for this packet: 0.000000000 seconds]
      [Time delta from previous captured frame: 0.000522000 seconds]
      [Time delta from previous displayed frame: 0.000000000 seconds]
      [Time since reference or first frame: 19.011357000 seconds]
      Frame Number: 751
      Frame Length: 526 bytes (4208 bits)
      Capture Length: 526 bytes (4208 bits)
      [Frame is marked: False]
      [Frame is ignored: False]
      [Protocols in frame: eth:ethertype:ip:tcp:http]
      [Coloring Rule Name: HTTP]

Frame Number (frame.number)
```

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



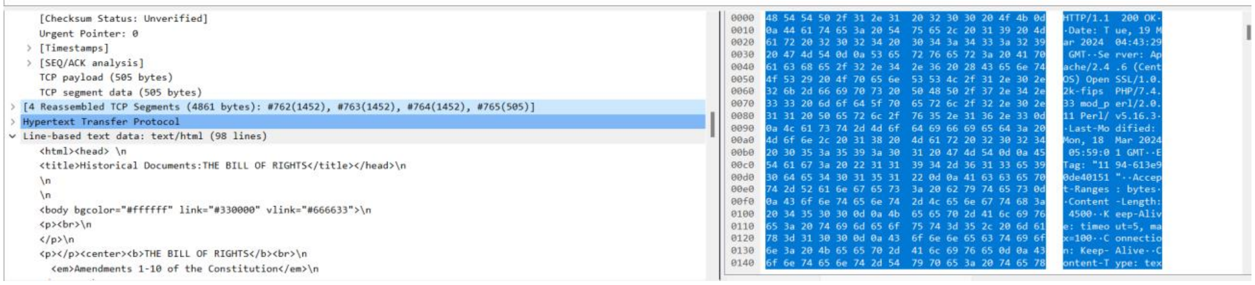
```
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.u
    [HTTP request 1/1]
    [Response in frame: 765]
```

Frame: 765

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

The code and phrase in the response was 200 OK

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

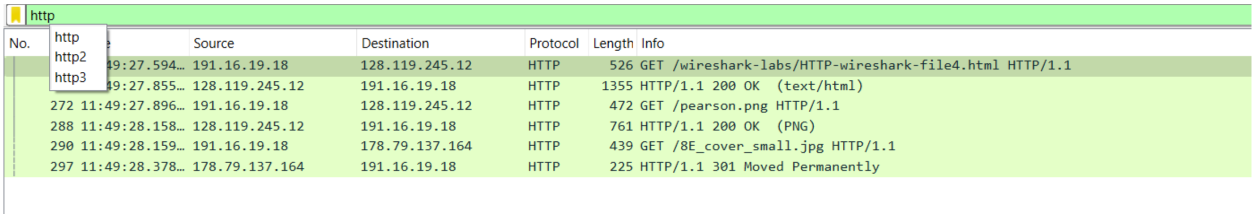


```
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (505 bytes)
    TCP segment data (505 bytes)
> [4 Reassembled TCP Segments (4861 bytes): #762(1452), #763(1452), #764(1452), #765(505)]
> Hypertext Transfer Protocol
v Line-based text data: text/html (98 lines)
    <html><head> \n
    <title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
    \n
    \n
    <body bgcolor="#ffffff" link="#330000" vlink="#666633">\n
    <p><br>\n
    </p>\n
    <p></p><center><b>THE BILL OF RIGHTS</b><br>\n
      <em>Amendments 1-10 of the Constitution</em>\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 54  75 65 2c 20 31 39 20 4d   ·Date: T ue, 19 M
0020  61 72 20 32 30 32 34 20  30 34 3a 34 33 3a 32 39   ar 2024  04:43:29
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 31 38 20  4d 61 72 20 32 30 32 34   Mon, 18  Mar 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 31 33 65 39   Tag: "11 94-613e9
00d0  30 64 65 34 30 31 35 31  22 0d 0a 41 63 63 65 70   0de40151 "··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
```

There are 4 reassembled TCP segments.

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



```
http
No.   http      Source          Destination     Protocol  Length Info
      http2
      http3
      49:27.594… 191.16.19.18   128.119.245.12  HTTP       526 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
      49:27.855… 128.119.245.12 191.16.19.18    HTTP      1355 HTTP/1.1 200 OK  (text/html)
  272 11:49:27.896… 191.16.19.18   128.119.245.12  HTTP       472 GET /pearson.png HTTP/1.1
  288 11:49:28.158… 128.119.245.12 191.16.19.18    HTTP       761 HTTP/1.1 200 OK  (PNG)
  290 11:49:28.159… 191.16.19.18   178.79.137.164  HTTP       439 GET /8E_cover_small.jpg HTTP/1.1
  297 11:49:28.378… 178.79.137.164 191.16.19.18    HTTP       225 HTTP/1.1 301 Moved Permanently
```

My Brower send 3 requests:

- The initial page : 128.119.245.12

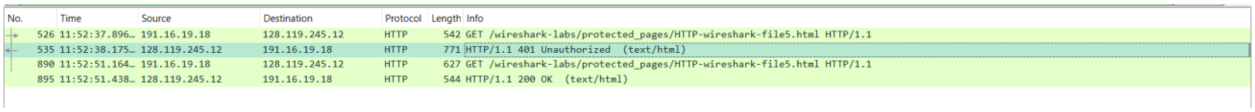
Pearson logo: 128.119.245.12

Pearson book : 178.79.137.164

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

It’s observable that the second request was dispatched following the completion of the first one. Therefore, I’m under the impression that these files were downloaded in a sequential manner.

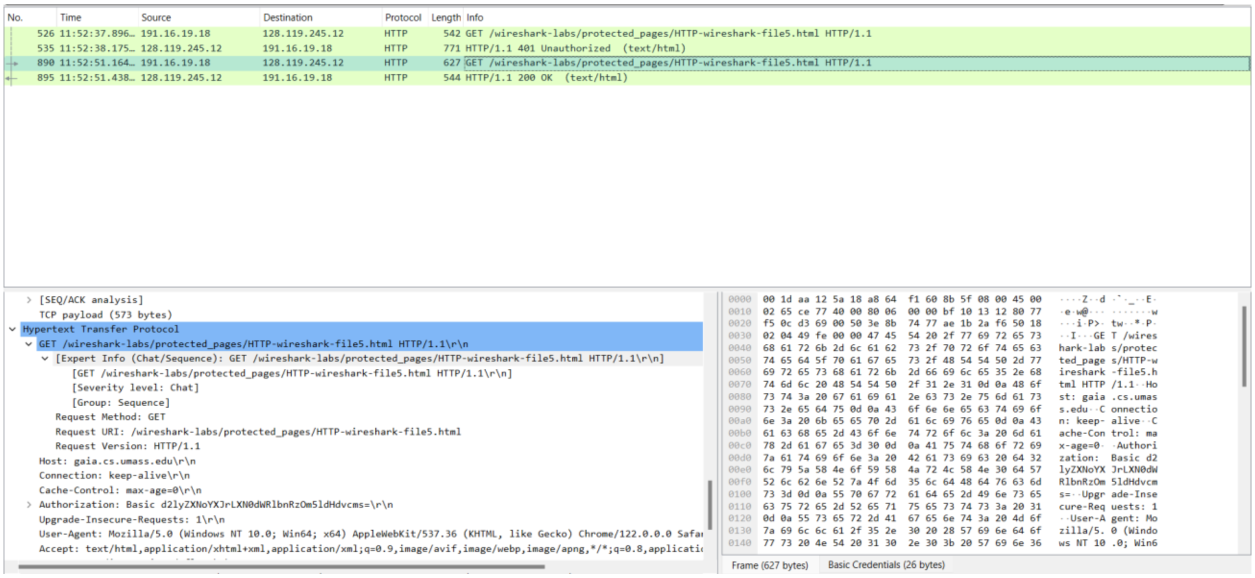
18. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?



```
No.  Time           Source          Destination     Protocol Length Info
 526 11:52:37.896… 191.16.19.18    128.119.245.12  HTTP      542 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
 535 11:52:38.175… 128.119.245.12  191.16.19.18    HTTP      771 HTTP/1.1 401 Unauthorized  (text/html)
 890 11:52:51.164… 191.16.19.18    128.119.245.12  HTTP      627 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
 895 11:52:51.438… 128.119.245.12  191.16.19.18    HTTP      544 HTTP/1.1 200 OK  (text/html)
```

The first respond was 401 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?



```
No.   Time             Source           Destination      Protocol  Length  Info
  526 11:52:37.896…    191.16.19.18     128.119.245.12   HTTP       542    GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
  535 11:52:38.175…    128.119.245.12   191.16.19.18     HTTP       771    HTTP/1.1 401 Unauthorized  (text/html)
  890 11:52:51.164…    191.16.19.18     128.119.245.12   HTTP       627    GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
  895 11:52:51.438…    128.119.245.12   191.16.19.18     HTTP       544    HTTP/1.1 200 OK  (text/html)
```

```
  > [SEQ/ACK analysis]
    TCP payload (573 bytes)
v Hypertext Transfer Protocol
  v GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
        [GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.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
  > Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safa
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicati
```

```
0000  00 1d aa 12 5a 18 a8 64  f1 60 8b 5f 08 00 45 00   ····Z··d ·`·_··E·
0010  02 65 ce 77 40 00 80 06  00 00 bf 10 13 12 80 77   ·e·w@··· ·······w
0020  f5 0c d3 69 00 50 3e 8b  74 77 ae 1b 2a f6 50 18   ···i·P>· tw··*·P·
0030  02 04 49 fe 00 00 47 45  54 20 2f 77 69 72 65 73   ··I···GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 70 72 6f 74 65 63   hark-lab s/protec
0050  74 65 64 5f 70 61 67 65  73 2f 48 54 54 50 2d 77   ted_page s/HTTP-w
0060  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 35 2e 68   ireshark -file5.h
0070  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0080  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0090  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
00a0  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 43   n: keep- alive··C
00b0  61 63 68 65 2d 43 6f 6e  74 72 6f 6c 3a 20 6d 61   ache-Con trol: ma
00c0  78 2d 61 67 65 3d 30 0d  0a 41 75 74 68 6f 72 69   x-age=0· ·Authori
00d0  7a 61 74 69 6f 6e 3a 20  42 61 73 69 63 20 64 32   zation:  Basic d2
00e0  6c 79 5a 58 4e 6f 59 58  4a 72 4c 58 4e 30 64 57   lyZXNoYX JrLXN0dW
00f0  52 6c 62 6e 52 7a 4f 6d  35 6c 64 48 64 76 63 6d   RlbnRzOm 5ldHdvcm
0100  73 3d 0d 0a 55 70 67 72  61 64 65 2d 49 6e 73 65   s=··Upgr ade-Inse
0110  63 75 72 65 2d 52 65 71  75 65 73 74 73 3a 20 31   cure-Req uests: 1
0120  0d 0a 55 73 65 72 2d 41  67 65 6e 74 3a 20 4d 6f   ··User-A gent: Mo
0130  7a 69 6c 6c 61 2f 35 2e  30 20 28 57 69 6e 64 6f   zilla/5. 0 (Windo
0140  77 73 20 4e 54 20 31 30  2e 30 3b 20 57 69 6e 36   ws NT 10 .0; Win6
```

It is Authorization