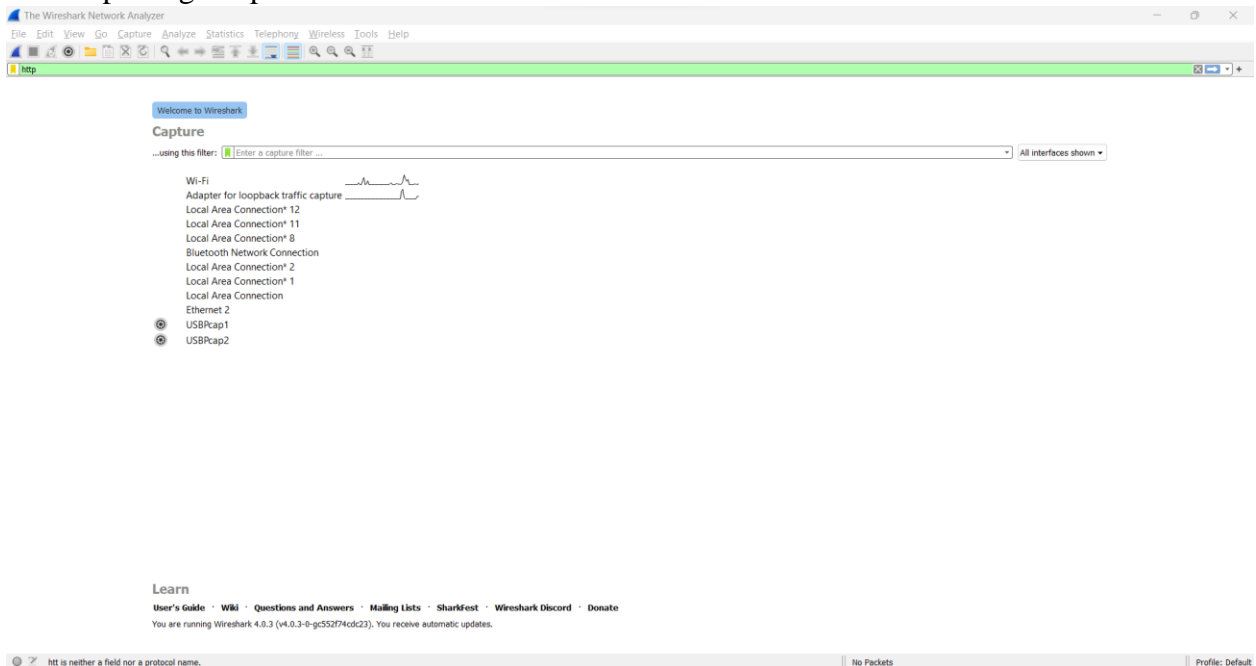


CSCE-5580 Computer Network

Lab-2 HTTP

1. Start up the Wireshark packet sniffer, as described in the introductory lab (but don't yet start packet capture).
2. Enter "http" (just the letters, not the quotation marks) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window. (We're only interested in the HTTP protocol here, and don't want to see the clutter of all captured packets).
3. Start capturing the packets.



NOTE: Take and attach screenshots for all the questions in work documents (Use the snipper tool).

- A. Answer the following question after running the following link in the browser

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>

1. What is the version of HTTP on the server and your browser with Screenshots? What is the language accepted by your browser?

The version of HTTP on the server is HTTP/1.1. The version of HTTP in the browser is also HTTP/1.1. The accepted language by the browser is English (United States en-us) and English (United Kingdom en-gb), as indicated by the "Accept-Language" header in the HTTP request.

```

Wireshark - Packet 211 - ass2Q1.pcapng
> Frame 211: 623 bytes on wire (4984 bits), 623 bytes captured (4984 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
> Ethernet II, Src: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53), Dst: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
> Internet Protocol Version 4, Src: 192.168.1.127, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60809, Dst Port: 80, Seq: 1, Ack: 1, Len: 569
< 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/1.1\r\n]
      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
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 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-GB,en-US;q=0.9,en;q=0.8\r\n
      If-None-Match: "80-5f72663f7728d"\r\n
      If-Modified-Since: Sat, 18 Mar 2023 05:59:01 GMT\r\n
      \r\n
      [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
      [HTTP request 1/2]
      [Response in frame: 230]
      [Next request in frame: 232]

```

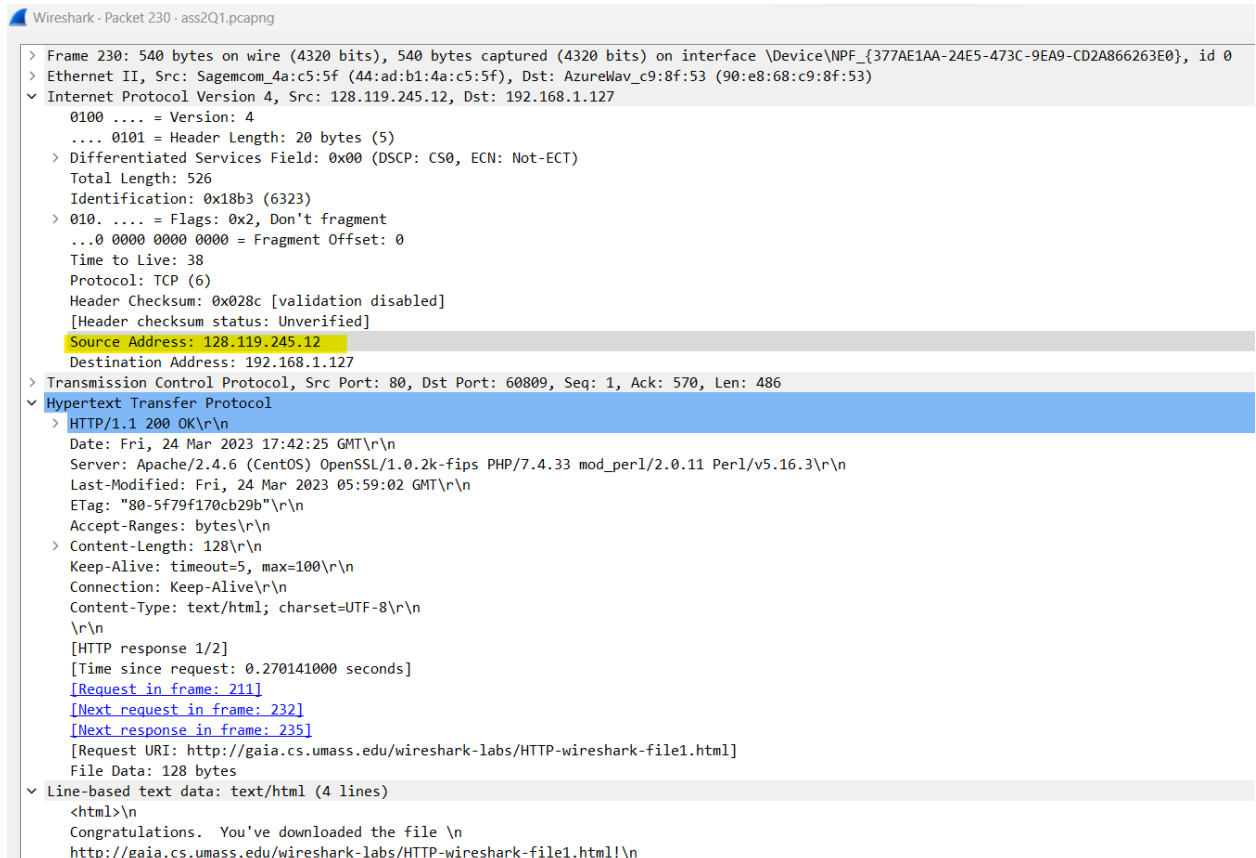
Language:

```

Wireshark - Packet 211 - ass2Q1.pcapng
> Frame 211: 623 bytes on wire (4984 bits), 623 bytes captured (4984 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
> Ethernet II, Src: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53), Dst: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
> Internet Protocol Version 4, Src: 192.168.1.127, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60809, Dst Port: 80, Seq: 1, Ack: 1, Len: 569
< 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/1.1\r\n]
      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
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 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-GB,en-US;q=0.9,en;q=0.8\r\n
      If-None-Match: "80-5f72663f7728d"\r\n
      If-Modified-Since: Sat, 18 Mar 2023 05:59:01 GMT\r\n
      \r\n
      [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
      [HTTP request 1/2]
      [Response in frame: 230]
      [Next request in frame: 232]

```

2. What is the source IP address of the response that you received after sending the GET request?



Wireshark - Packet 230 - ass2Q1.pcapng

```

> Frame 230: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
> Ethernet II, Src: Sagemcom_4a:c5:5f (44:ad:b1:4a:c5:5f), Dst: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
  > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.127
    > 0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 526
      Identification: 0x18b3 (6323)
    > 010. .... = Flags: 0x2, Don't fragment
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 38
      Protocol: TCP (6)
      Header Checksum: 0x028c [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 128.119.245.12
      Destination Address: 192.168.1.127
    > Transmission Control Protocol, Src Port: 80, Dst Port: 60809, Seq: 1, Ack: 570, Len: 486
  > Hypertext Transfer Protocol
    > HTTP/1.1 200 OK\r\n
      Date: Fri, 24 Mar 2023 17:42:25 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: Fri, 24 Mar 2023 05:59:02 GMT\r\n
      ETag: "80-5f79f170cb29b"\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 1/2]
      [Time since request: 0.270141000 seconds]
      [Request in frame: 211]
      [Next request in frame: 232]
      [Next response in frame: 235]
      [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
      File Data: 128 bytes
    > Line-based text data: text/html (4 lines)
      <html>\n
      Congratulations. You've downloaded the file \n
      http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n

```

- What is the status code that you received in the response? Write about any two-status code.

The status code received in the response is 200. Two other common HTTP status codes are 304 NOT MODIFIED and 404 NOT FOUND. HTTP 200 OK status code indicates that the request has succeeded, and the response contains the requested data. HTTP 404 NOT FOUND status code indicates that the requested resource was not found on the server. HTTP 304 NOT MODIFIED status code indicates that the requested resource has not been modified since the last request.

```

Wireshark - Packet 230 - ass2Q1.pcapng

> Frame 230: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
> Ethernet II, Src: Sagemcom_4a:c5:5f (44:ad:b1:4a:c5:5f), Dst: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.127
> Transmission Control Protocol, Src Port: 80, Dst Port: 60809, Seq: 1, Ack: 570, Len: 486
> 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: Fri, 24 Mar 2023 17:42:25 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: Fri, 24 Mar 2023 05:59:02 GMT\r\n
      ETag: "80-5f79f170cb29b"\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 1/2]
      [Time since request: 0.270141000 seconds]
      [Request in frame: 211]
      [Next request in frame: 232]
      [Next response in frame: 235]
      [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
      File Data: 128 bytes
  > Line-based text data: text/html (4 lines)
    <html>\n
    Congratulations. You've downloaded the file \n
    http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
    </html>\n
  
```

4. What is the last modified date with the time of the file that you've received in the response with a screenshot?

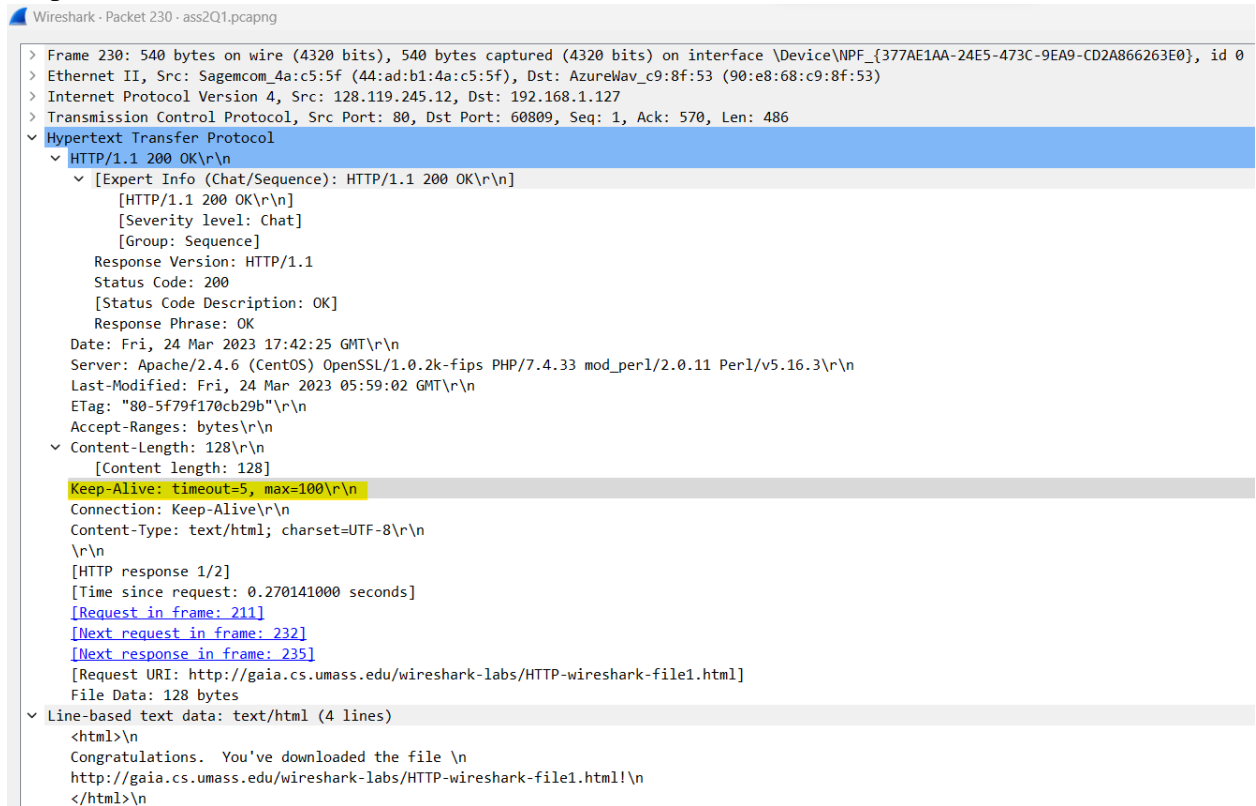
The last modified date and time of the file that was received in the response are Fri, 24 Mar 2023 05:59:02 GMT. You can find this information in the "Last-Modified" header of the server response. Here's a screenshot that highlights the Last-Modified field:

```

Wireshark - Packet 230 - ass2Q1.pcapng

> Frame 230: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
> Ethernet II, Src: Sagemcom_4a:c5:5f (44:ad:b1:4a:c5:5f), Dst: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.127
> Transmission Control Protocol, Src Port: 80, Dst Port: 60809, Seq: 1, Ack: 570, Len: 486
> 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: Fri, 24 Mar 2023 17:42:25 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: Fri, 24 Mar 2023 05:59:02 GMT\r\n
      ETag: "80-5f79f170cb29b"\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 1/2]
      [Time since request: 0.270141000 seconds]
      [Request in frame: 211]
      [Next request in frame: 232]
      [Next response in frame: 235]
      [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
      File Data: 128 bytes
  > Line-based text data: text/html (4 lines)
    <html>\n
    Congratulations. You've downloaded the file \n
    http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
    </html>\n
  
```

5. What are timeout and max field values? (Hint: you can find this in the keepalive field)
 The "Keep-Alive" field in the response header contains the "timeout" and "max" values. The "timeout" field specifies the maximum number of seconds the server should keep the connection open if there are no new requests from the client. In this case, it is set to 5 seconds. The "max" field specifies the maximum requests the client can send during the keep-alive connection. In this case, it is set to 100 submissions.



```

Wireshark · Packet 230 · ass2Q1.pcapng
> Frame 230: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
> Ethernet II, Src: Sagemcom_4a:c5:5f (44:ad:b1:4a:c5:5f), Dst: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.127
> Transmission Control Protocol, Src Port: 80, Dst Port: 60809, Seq: 1, Ack: 570, Len: 486
▼ 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: Fri, 24 Mar 2023 17:42:25 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: Fri, 24 Mar 2023 05:59:02 GMT\r\n
      ETag: "80-5f79f170cb29b"\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
      \r\n
      [HTTP response 1/2]
      [Time since request: 0.270141000 seconds]
      [Request in frame: 211]
      [Next request in frame: 232]
      [Next response in frame: 235]
      [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
      File Data: 128 bytes
    ▼ Line-based text data: text/html (4 lines)
      <html>\n
      Congratulations. You've downloaded the file \n
      http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
      </html>\n
  
```

- B. Answer the following question after running the following link in the browser

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>

1. What is the length of the response packet after running the above link in your browser?
 The Total Length field in the IP header gives the correct packet length for the IP packet, which includes both the IP header and the encapsulated TCP segment with its payload data. In this case, the Total Length field value is **770 bytes**. The length of the payload data carried in the HTTP response, then the Content-Length header value of **371 bytes** would be more relevant. The frame length 784 refers to the size of the captured packet that Wireshark reports. The TCP payload field 730 indicates the size of the data that is being transmitted in the packet.

Wireshark - Packet 16674 - ass2Q2.pcapng

```

> Frame 16674: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
> Ethernet II, Src: JuniperN_da:eb:c0 (54:1e:56:da:eb:c0), Dst: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
  > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.125.157.174
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 770
      Identification: 0x4318 (17176)
    > 010. .... = Flags: 0x2, Don't fragment
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 43
      Protocol: TCP (6)
      Header Checksum: 0xec2e [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 128.119.245.12
      Destination Address: 10.125.157.174
  > Transmission Control Protocol, Src Port: 80, Dst Port: 64647, Seq: 1, Ack: 473, Len: 730
    > 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: Fri, 24 Mar 2023 19:54:56 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: Fri, 24 Mar 2023 05:59:02 GMT\r\n
          ETag: "173-5f79f170caacb"\r\n
          Accept-Ranges: bytes\r\n
          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
          [HTTP response 1/1]
          [Time since request: 0.102680000 seconds]
          [Request in frame: 15914]
          [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
          File Data: 371 bytes

```

2. What is the difference between the length of the response packets? (1st Response and 2nd response)

Difference = Length of the response packets 1 - Length of the response packet 2

$$= 770 - 280$$

$$= 49$$

First Response:

```

Wireshark · Packet 16674 · ass2Q2.pcapng

> Frame 16674: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
> Ethernet II, Src: JuniperN_da:eb:c0 (54:1e:56:da:eb:c0), Dst: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.125.157.174
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 770
    Identification: 0x4318 (17176)
  > 010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 43
  Protocol: TCP (6)
  Header Checksum: 0xec2e [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 128.119.245.12
  Destination Address: 10.125.157.174
> Transmission Control Protocol, Src Port: 80, Dst Port: 64647, Seq: 1, Ack: 473, Len: 730
> 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: Fri, 24 Mar 2023 19:54:56 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: Fri, 24 Mar 2023 05:59:02 GMT\r\n
      ETag: "173-5f79f170caacb"\r\n
      Accept-Ranges: bytes\r\n
      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
      [HTTP response 1/1]
      [Time since request: 0.102680000 seconds]
      [Request in frame: 15914]
      [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
      File Data: 371 bytes

```

Second Response:

```

Wireshark · Packet 32701 · ass2Q2.pcapng

> Frame 32701: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
> Ethernet II, Src: JuniperN_da:eb:c0 (54:1e:56:da:eb:c0), Dst: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.125.157.174
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 280
    Identification: 0xe435 (58421)
  > 010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 42
  Protocol: TCP (6)
  Header Checksum: 0x4dfb [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 128.119.245.12
  Destination Address: 10.125.157.174
> Transmission Control Protocol, Src Port: 80, Dst Port: 64695, Seq: 1, Ack: 597, Len: 240
> Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
      [HTTP/1.1 304 Not Modified\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
      Date: Fri, 24 Mar 2023 19:56:03 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
      Connection: Keep-Alive\r\n
      Keep-Alive: timeout=5, max=100\r\n
      ETag: "173-5f79f170caacb"\r\n
      \r\n
      [HTTP response 1/1]
      [Time since request: 0.041876000 seconds]
      [Request in frame: 32699]
      [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

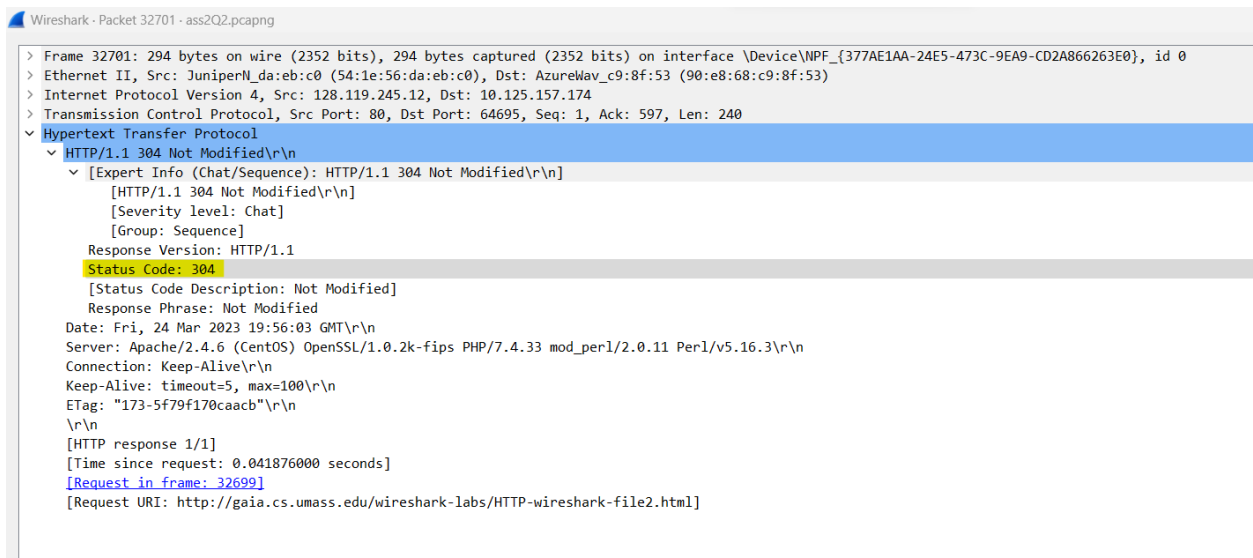
```

C. Enter the following link again then answer the questions.

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>

1. What is the status code for the response?

The status code for the response is "304 Not Modified" because we are just reloading the file again, that was just loaded few minutes ago. It is an HTTP response status code that indicates that the requested resource has not been modified since the last time it was accessed by the client, which means that the client's cached version of the requested resource is still valid, and the server did not send the complete content of the requested file.

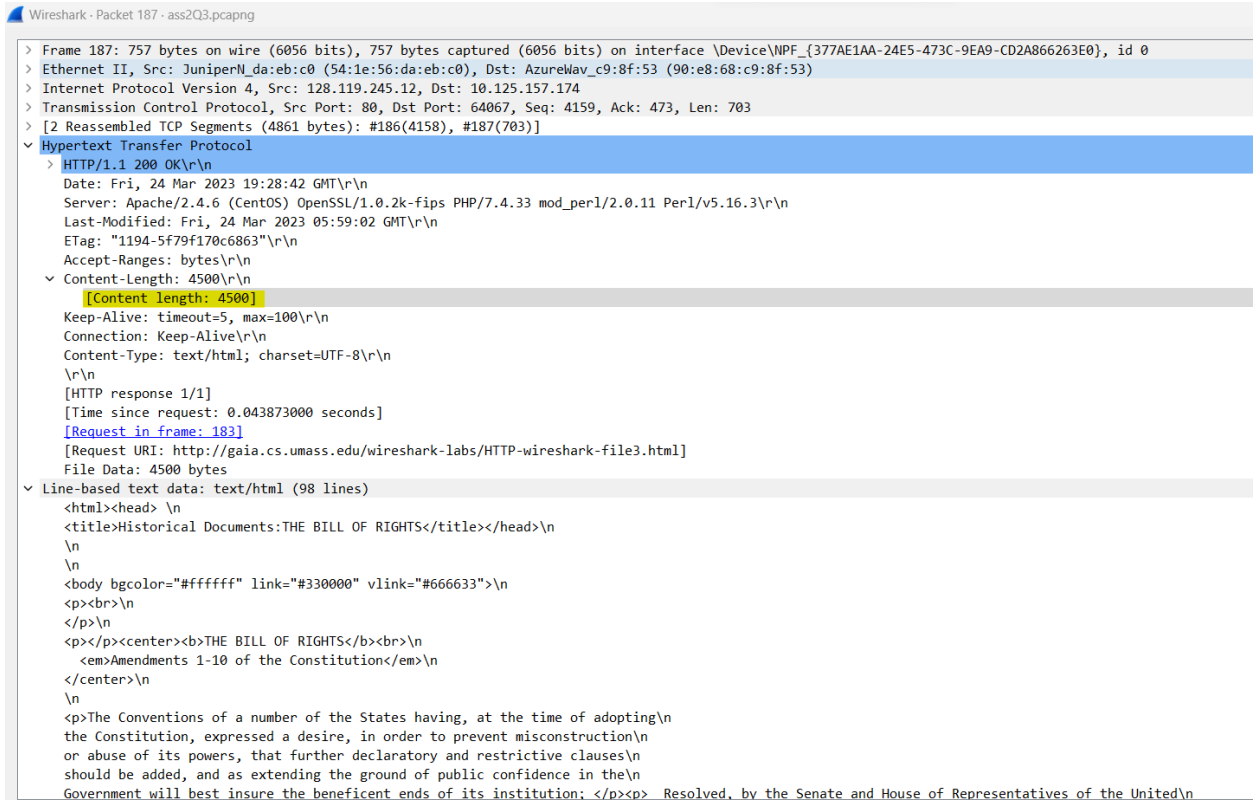


D. Answer the following question after running the following link in the browser.

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>

1. What is the file length after running the above link in your browser?

The file length is 4500. This indicates that the file being transmitted in this capture is 4500 bytes in length.



```

Wireshark - Packet 187 - ass2Q3.pcapng
> Frame 187: 757 bytes on wire (6056 bits), 757 bytes captured (6056 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
> Ethernet II, Src: JuniperN_da:eb:c0 (54:1e:56:da:eb:c0), Dst: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.125.157.174
> Transmission Control Protocol, Src Port: 80, Dst Port: 64067, Seq: 4159, Ack: 473, Len: 703
> [2 Reassembled TCP Segments (4861 bytes): #186(4158), #187(703)]
< Hypertext Transfer Protocol
  < HTTP/1.1 200 OK\r\n
    Date: Fri, 24 Mar 2023 19:28:42 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: Fri, 24 Mar 2023 05:59:02 GMT\r\n
    ETag: "1194-5f79f170c6863"\r\n
    Accept-Ranges: bytes\r\n
    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
    [HTTP response 1/1]
    [Time since request: 0.043873000 seconds]
    [Request in frame: 183]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    File Data: 4500 bytes
  < Line-based text data: text/html (98 lines)
    <html><head> \n
    <title>Historical Documents:THE BILL OF RIGHTS</title></head>\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
    </center>\n
    \n
    <p>The Conventions of a number of the States having, at the time of adopting\n
    the Constitution, expressed a desire, in order to prevent misconstruction\n
    or abuse of its powers, that further declaratory and restrictive clauses\n
    should be added, and as extending the ground of public confidence in the\n
    Government will best insure the beneficent ends of its institution: </p><p> Resolved, by the Senate and House of Representatives of the United\n
  
```

2. What is the background(bgcolor) color mentioned in the HTML document?

The HTML response from the server does not contain any "background" attribute, so it is not possible to determine the background color of the HTML page from this packet capture. The background(bgcolor) color mentioned in the HTML document is "#FFFFFF", which represents white.

Wireshark - Packet 187 - ass2Q3.pcapng

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
</center>\n
\n
<p>The Conventions of a number of the States having, at the time of adopting\n
the Constitution, expressed a desire, in order to prevent misconstruction\n
or abuse of its powers, that further declaratory and restrictive clauses\n
should be added, and as extending the ground of public confidence in the\n
Government will best insure the beneficent ends of its institution; <p><p> Resolved, by the Senate and House of Representatives of the United\n
States of America, in Congress assembled, two-thirds of both Houses concurring,\n
that the following articles be proposed to the Legislatures of the several\n
States, as amendments to the Constitution of the United States; all or any\n
of which articles, when ratified by three-fourths of the said Legislatures,\n
to be valid to all intents and purposes as part of the said Constitution,\n
namely: </p><p><a name="1"><strong><h3>Amendment I</h3></strong></a>\n
\n
<p></p><p><p>Congress shall make no law respecting an establishment of\n
religion, or prohibiting the free exercise thereof; or\n
abridging the freedom of speech, or of the press; or the\n
right of the people peaceably to assemble, and to petition\n
the government for a redress of grievances.\n
\n
</p><p><a name="2"><strong><h3>Amendment II</h3></strong></a>\n
\n
<p></p><p><p>A well regulated militia, being necessary to the security\n
of a free state, the right of the people to keep and bear\n
arms, shall not be infringed.\n
\n
</p><p><a name="3"><strong><h3>Amendment III</h3></strong></a>\n
\n
<p></p><p><p>No soldier shall, in time of peace be quartered in any house,\n
without the consent of the owner, nor in time of war, but\n

```

Nls: 187 - Time: 20.614602 - Source: 128.119.245.12 - Destination: 10.125.157.174 - Protocol: HTTP - Length: 757 - Info: HTTP/1.1 200 OK (text/html)

3. How many GET request was sent to receive The Bill of Rights HTML file from the server?

Only one Get Request was sent to receive The Bill of Rights HTML file from the server.

Wireshark - Packet 183 - ass2Q3.pcapng

> Frame 183: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0

> Ethernet II, Src: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53), Dst: JuniperN_da:eb:c0 (54:1e:56:da:eb:c0)

> Internet Protocol Version 4, Src: 10.125.157.174, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 64067, Dst Port: 80, Seq: 1, Ack: 1, Len: 472

> Hypertext Transfer Protocol

> GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n

> [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]

> [GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]

> [Severity level: Chat]

> [Group: Sequence]

> Request Method: GET

> Request URI: /wireshark-labs/HTTP-wireshark-file3.html

> Request Version: HTTP/1.1

> 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/111.0.0.0 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-GB,en;q=0.9\r\n

> \r\n

> [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]

> [HTTP request 1/1]

> [Response in frame: 187]

183	20.570729	10.125.157.174	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
187	20.614602	128.119.245.12	10.125.157.174	HTTP	757	HTTP/1.1 200 OK (text/html)

- E. Answer the following question after running the following link in the browser.

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>

1. What is the content-type of the file that was received in the response after the first GET Request? How many GET requests were sent to retrieve the whole page?

There were three GET requests sent to retrieve the whole page.

599	19.432208	192.168.1.127	128.119.245.12	HTTP	538 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
616	19.516204	128.119.245.12	192.168.1.127	HTTP	1355 HTTP/1.1 200 OK (text/html)
629	19.572503	192.168.1.127	128.119.245.12	HTTP	484 GET /pearson.png HTTP/1.1
644	19.671062	128.119.245.12	192.168.1.127	HTTP	801 HTTP/1.1 200 OK (PNG)
694	20.239933	192.168.1.127	178.79.137.164	HTTP	451 GET /8E_cover_small.jpg HTTP/1.1
705	20.536022	178.79.137.164	192.168.1.127	HTTP	240 HTTP/1.1 302 Found

First GET Request: to load the webpage as text/html.

```
Wireshark - Packet 599 - ass2Q4.pcapng
> Frame 599: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
> Ethernet II, Src: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53), Dst: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
> Internet Protocol Version 4, Src: 192.168.1.127, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 59195, Dst Port: 80, Seq: 1, Ack: 1, Len: 484
v Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n
  > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n]
  Request Method: GET
  Request URI: /wireshark-labs/HTTP-wireshark-file4.html
  Request Version: HTTP/1.1
  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/111.0.0.0 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-GB,en-US;q=0.9,en;q=0.8\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
  [HTTP request 1/2]
  [Response in frame: 616]
  [Next request in frame: 629]
```

Second GET Request: to get the PNG image.

```
Wireshark - Packet 629 - ass2Q4.pcapng
> Frame 629: 484 bytes on wire (3872 bits), 484 bytes captured (3872 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
> Ethernet II, Src: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53), Dst: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
> Internet Protocol Version 4, Src: 192.168.1.127, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 59195, Dst Port: 80, Seq: 485, Ack: 1302, Len: 430
v Hypertext Transfer Protocol
  GET /pearson.png HTTP/1.1\r\n
  > [Expert Info (Chat/Sequence): GET /pearson.png HTTP/1.1\r\n]
  Request Method: GET
  Request URI: /pearson.png
  Request Version: HTTP/1.1
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36\r\n
  Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
  Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/pearson.png]
  [HTTP request 2/2]
  [Prev request in frame: 599]
  [Response in frame: 644]
```

Third GET Request: to get the JPG image.

```

Wireshark - Packet 694 - ass2Q4.pcapng
> Frame 694: 451 bytes on wire (3608 bits), 451 bytes captured (3608 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
> Ethernet II, Src: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53), Dst: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
> Internet Protocol Version 4, Src: 192.168.1.127, Dst: 178.79.137.164
> Transmission Control Protocol, Src Port: 59203, Dst Port: 80, Seq: 1, Ack: 1, Len: 397
< Hypertext Transfer Protocol
  < GET /8E_cover_small.jpg HTTP/1.1\r\n
    < [Expert Info (Chat/Sequence): GET /8E_cover_small.jpg HTTP/1.1\r\n]
      < [GET /8E_cover_small.jpg HTTP/1.1\r\n]
      < [Severity level: Chat]
      < [Group: Sequence]
      < Request Method: GET
      < Request URI: /8E_cover_small.jpg
      < Request Version: HTTP/1.1
      < Host: kurose.cslash.net\r\n
      < Connection: keep-alive\r\n
      < User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36\r\n
      < Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
      < Referer: http://gaia.cs.umass.edu/\r\n
      < Accept-Encoding: gzip, deflate\r\n
      < Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
      < \r\n
      < [Full request URI: http://kurose.cslash.net/8E_cover_small.jpg]
      < [HTTP request 1/1]
      < [Response in frame: 705]

```

The content type of the file received in response to the first GET request (/wireshark-labs/HTTP-wireshark-file4.html) is "text/html".

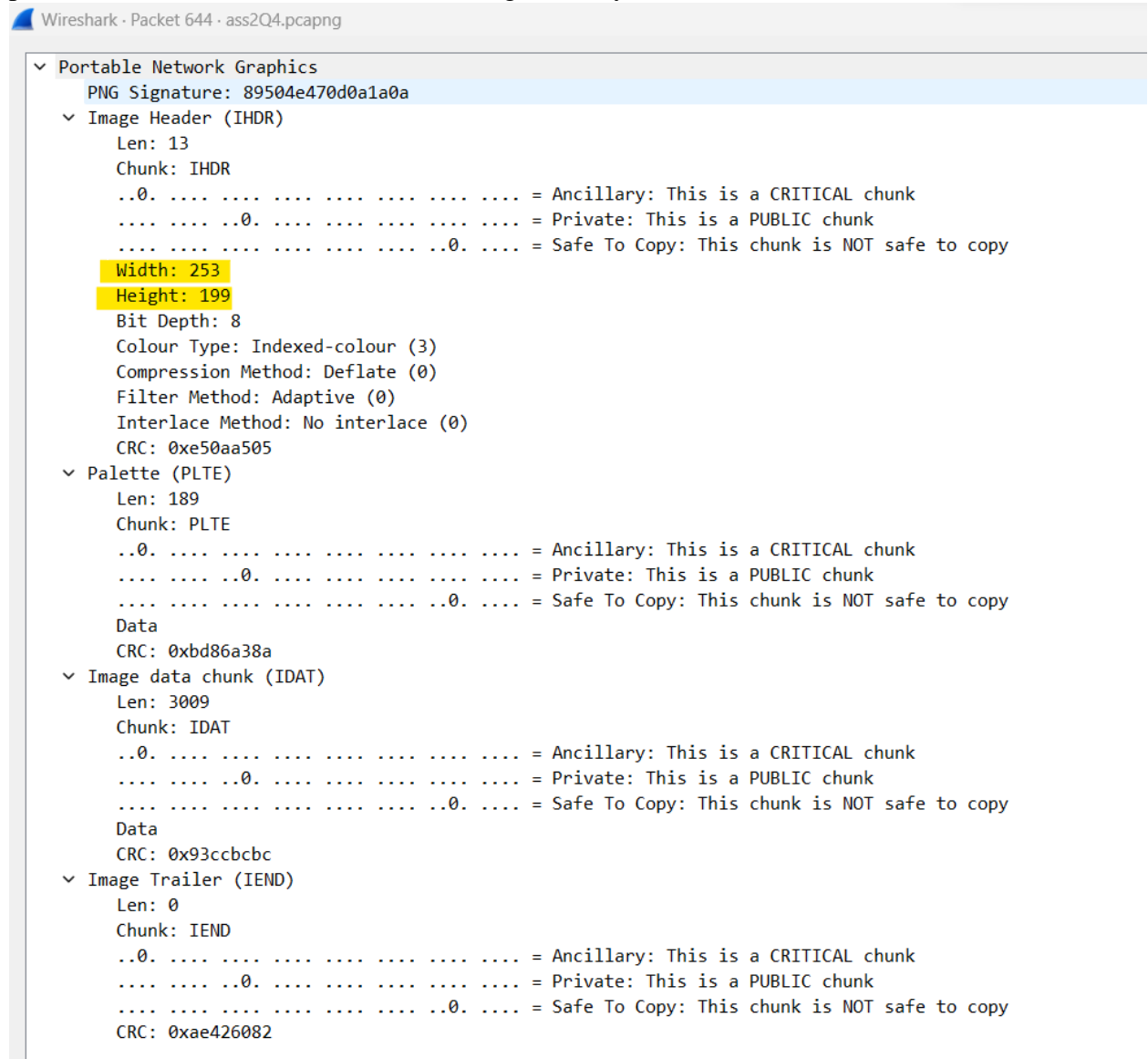
```

Wireshark - Packet 616 - ass2Q4.pcapng
> Frame 616: 1355 bytes on wire (10840 bits), 1355 bytes captured (10840 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
> Ethernet II, Src: Sagemcom_4a:c5:5f (44:ad:b1:4a:c5:5f), Dst: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.127
> Transmission Control Protocol, Src Port: 80, Dst Port: 59195, Seq: 1, Ack: 485, Len: 1301
< 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: Sat, 18 Mar 2023 22:29:11 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: Sat, 18 Mar 2023 05:59:01 GMT\r\n
      < ETag: "3ae-5f72663f762ed"\r\n
      < Accept-Ranges: bytes\r\n
      < Content-Length: 942\r\n
      < [Content length: 942]
      < 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: 0.083996000 seconds]
      < [Request in frame: 599]
      < [Next request in frame: 629]
      < [Next response in frame: 644]
      < [Request URI: http://gaia.cs.umass.edu/pearson.png]
      < File Data: 942 bytes
  < Line-based text data: text/html (23 lines)
    < <html>\n
    < <head>\n
    < <title>Lab2-4 file: Embedded URLs</title>\n
    < <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">\n
    < </head>\n
    < \n
    < <body bgcolor="#FFFFFF" text="#000000">\n
    < \n
    < <p>\n
    <  </p>\n

```

2. What is the width and height of the file received in response (PNG - Portable Network Graphics)? Include File Data as well?

The file received in response is a PNG file with a width of 253 pixels and a height of 199 pixels. The file data starts with the PNG signature bytes: 89 50 4E 47 0D 0A 1A 0A.



File Data:

Wireshark - Packet 644 · ass2Q4.pcapng

```

> Frame 644: 801 bytes on wire (6408 bits), 801 bytes captured (6408 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
> Ethernet II, Src: Sagemcom_4a:c5:5f (44:ad:b1:4a:c5:5f), Dst: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.127
> Transmission Control Protocol, Src Port: 80, Dst Port: 59195, Seq: 4166, Ack: 915, Len: 747
> [3 Reassembled TCP Segments (3611 bytes): #640(1432), #643(1432), #644(747)]
< Hypertext Transfer Protocol
  < HTTP/1.1 200 OK\r\n
    Date: Sat, 18 Mar 2023 22:29:11 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: Sat, 06 Aug 2016 10:08:14 GMT\r\n
    ETag: "cc3-539645c7f1ee7"\r\n
    Accept-Ranges: bytes\r\n
  < Content-Length: 3267\r\n
    Keep-Alive: timeout=5, max=99\r\n
    Connection: Keep-Alive\r\n
    Content-Type: image/png\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.098559000 seconds]
    [Prev request in frame: 599]
    [Prev response in frame: 616]
    [Request in frame: 629]
    [Request URI: http://gaia.cs.umass.edu/pearson.png]
    File Data: 3267 bytes
  < Portable Network Graphics
    PNG Signature: 89504e470d0a1a0a
    < Image Header (IHDR)
      Len: 13
      Chunk: IHDR
      ..0. .... = Ancillary: This is a CRITICAL chunk
      .... ..0. .... = Private: This is a PUBLIC chunk
      .... ....0. .... = Safe To Copy: This chunk is NOT safe to copy
      Width: 253
      Height: 199
      Bit Depth: 8
      Colour Type: Indexed-colour (3)
      Compression Method: Deflate (0)
      Filter Method: Adaptive (0)
      Interlace Method: No interlace (0)
      CRC: 0xe50aa505

```

Wireshark - Follow TCP Stream (tcp.stream eq 62) · ass2Q4.pcapng

Host: gaia.cs.umass.edu
 Connection: keep-alive
 Upgrade-Insecure-Requests: 1
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 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-GB,en-US;q=0.9,en;q=0.8

HTTP/1.1 200 OK
 Date: Sat, 18 Mar 2023 22:29:11 GMT
 Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3
 Last-Modified: Sat, 18 Mar 2023 05:59:01 GMT
 ETag: "3ae-5f726b3f762ed"
 Accept-Ranges: bytes
 Content-Length: 942
 Keep-Alive: timeout=5, max=100
 Connection: Keep-Alive
 Content-Type: text/html; charset=UTF-8

```

<html>
<head>
<title>Lab2-4 file: Embedded URLs</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
</head>

<body bgcolor="#FFFFFF" text="#000000">

<p>
 </p>
<p>This little HTML file is being served by gaia.cs.umass.edu.
It contains two embedded images. The image above, also served from the
gaia.cs.umass.edu web site, is the logo of our publisher, Pearson.
The image of our 8th edition book cover below is stored at, and served from,
a WWW server kurose.cslash.net in France:<p>
<p align="left"></p>
And while we have your attention, you might want to take time to check out the
available open resources for this book at
<a href="http://gaia.cs.umass.edu/kurose_ross"> http://gaia.cs.umass.edu/kurose_ross</a>.

</body>
</html>

```

2 client files, 4 server files, 3 turns
 Entire conversation (5826 bytes) Show data as: ASCII Stream: 62

Find: Filter Out This Stream Print Save as... Back Close Help

```

GET /pearson.png HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

HTTP/1.1 200 OK
Date: Sat, 18 Mar 2023 22:29:11 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3
Last-Modified: Sat, 06 Aug 2016 10:08:14 GMT
ETag: "cc3-539645c7f1ee7"
Accept-Ranges: bytes
Content-Length: 3267
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: image/png

.PNG
...
IHDR.....
PLTE.....
tRNL.....
IDATx.....
IEND B

```

3. What is the host of the GET request of /8E_cover_small.jpg?

The host of the GET request for /8E_cover_small.jpg is:

Host: kurose.cslash.net\r\n

```

> Frame 694: 451 bytes on wire (3608 bits), 451 bytes captured (3608 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
> Ethernet II, Src: AzureNw_c9:8f:53 (90:e8:68:c9:8f:53), Dst: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
> Internet Protocol Version 4, Src: 192.168.1.127, Dst: 178.79.137.164
> Transmission Control Protocol, Src Port: 59203, Dst Port: 80, Seq: 1, Ack: 1, Len: 397
Hypertext Transfer Protocol
  GET /8E_cover_small.jpg HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /8E_cover_small.jpg HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /8E_cover_small.jpg
    Request Version: HTTP/1.1
    Host: kurose.cslash.net\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36\r\n
    Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
    Referer: http://gaia.cs.umass.edu/\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
    \r\n
    [Full request URI: http://kurose.cslash.net/8E_cover_small.jpg]
    [HTTP request 1/1]
    [Response in frame: 705]

```

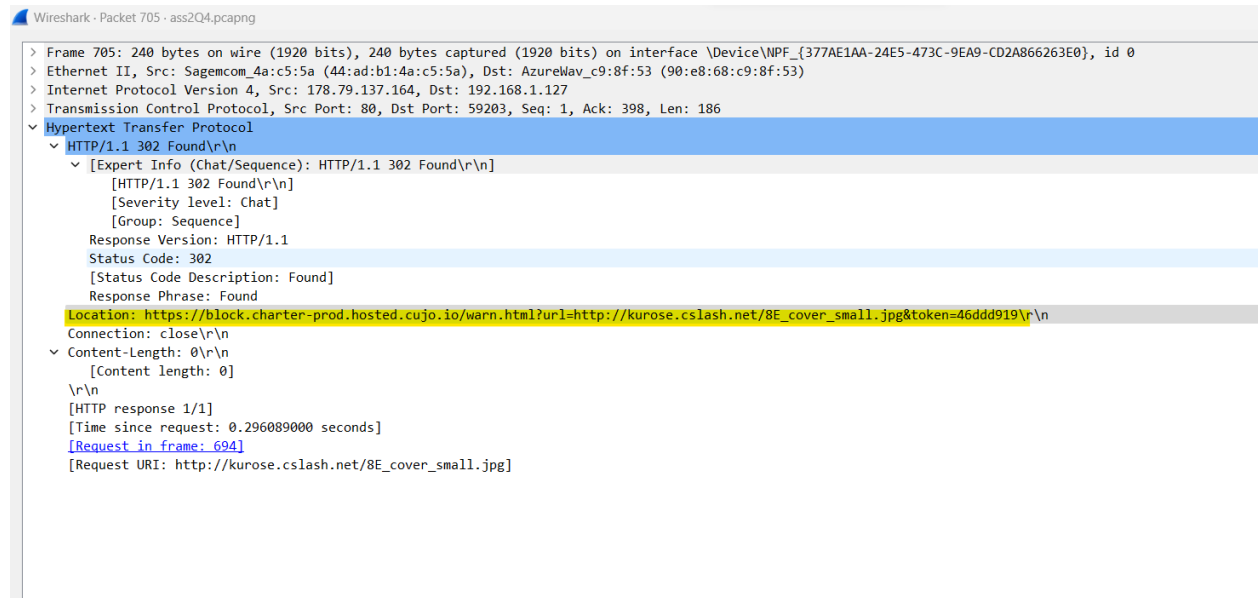
4. What is the location of /8E_cover_small.jpg file in response 302 found?

The location of the /8E_cover_small.jpg file in the HTTP response 302 Found is:

Location: [https://block.charter-](https://block.charter-prod.hosted.cujo.io/warn.html?url=http://kurose.cslash.net/8E_cover_small.jpg&token=46ddd919)

[prod.hosted.cujo.io/warn.html?url=http://kurose.cslash.net/8E_cover_small.jpg&token=46ddd919](https://block.charter-prod.hosted.cujo.io/warn.html?url=http://kurose.cslash.net/8E_cover_small.jpg&token=46ddd919)

It is specified in the "Location" header of the HTTP response.



```
Wireshark · Packet 705 · ass2Q4.pcapng
> Frame 705: 240 bytes on wire (1920 bits), 240 bytes captured (1920 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
> Ethernet II, Src: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a), Dst: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
> Internet Protocol Version 4, Src: 178.79.137.164, Dst: 192.168.1.127
> Transmission Control Protocol, Src Port: 80, Dst Port: 59203, Seq: 1, Ack: 398, Len: 186
v Hypertext Transfer Protocol
  v HTTP/1.1 302 Found\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 302 Found\r\n]
      [HTTP/1.1 302 Found\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 302
      [Status Code Description: Found]
      Response Phrase: Found
      Location: https://block.charter-prod.hosted.cujo.io/warn.html?url=http://kurose.cslash.net/8E_cover_small.jpg&token=46ddd919\r\n
    Connection: close\r\n
  v Content-Length: 0\r\n
    [Content length: 0]
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.296089000 seconds]
  [Request in frame: 694]
  [Request URI: http://kurose.cslash.net/8E_cover_small.jpg]
```