

CPSC 471-01 Project 1

Team: Luc Dang (solo)

Part 1 - Python Programming Web Server

```
#import socket module
from socket import *
import sys # In order to terminate the program
serverSocket = socket(AF_INET, SOCK_STREAM)
#Prepare a sever socket

# TASK 1
#Fill in start
serverSocket.bind(('localhost', 45678))
serverSocket.listen()
#Fill in end

while True:
    #Establish the connection
    print('Ready to serve...')

    # TASK 2
    connectionSocket, addr = serverSocket.accept() #Fill in start #Fill in
end

    try:

        # TASK 3
        message = connectionSocket.recv(1024) #Fill in start #Fill in end

        filename = message.split()[1]
        f = open(filename[1:])

        # TASK 4
        outputdata = f.read() #Fill in start #Fill in end

        # TASK 5
        #Send one HTTP header line into socket
        #Fill in start
        header = 'HTTP/1.1 200 OK\r\n'
        connectionSocket.send(header.encode('utf-8'))
        #Fill in end

        #Send the content of the requested file to the client
        for i in range(0, len(outputdata)):
            connectionSocket.send(outputdata[i].encode('utf-8'))
        connectionSocket.send("\r\n".encode('utf-8'))
        connectionSocket.close()
```

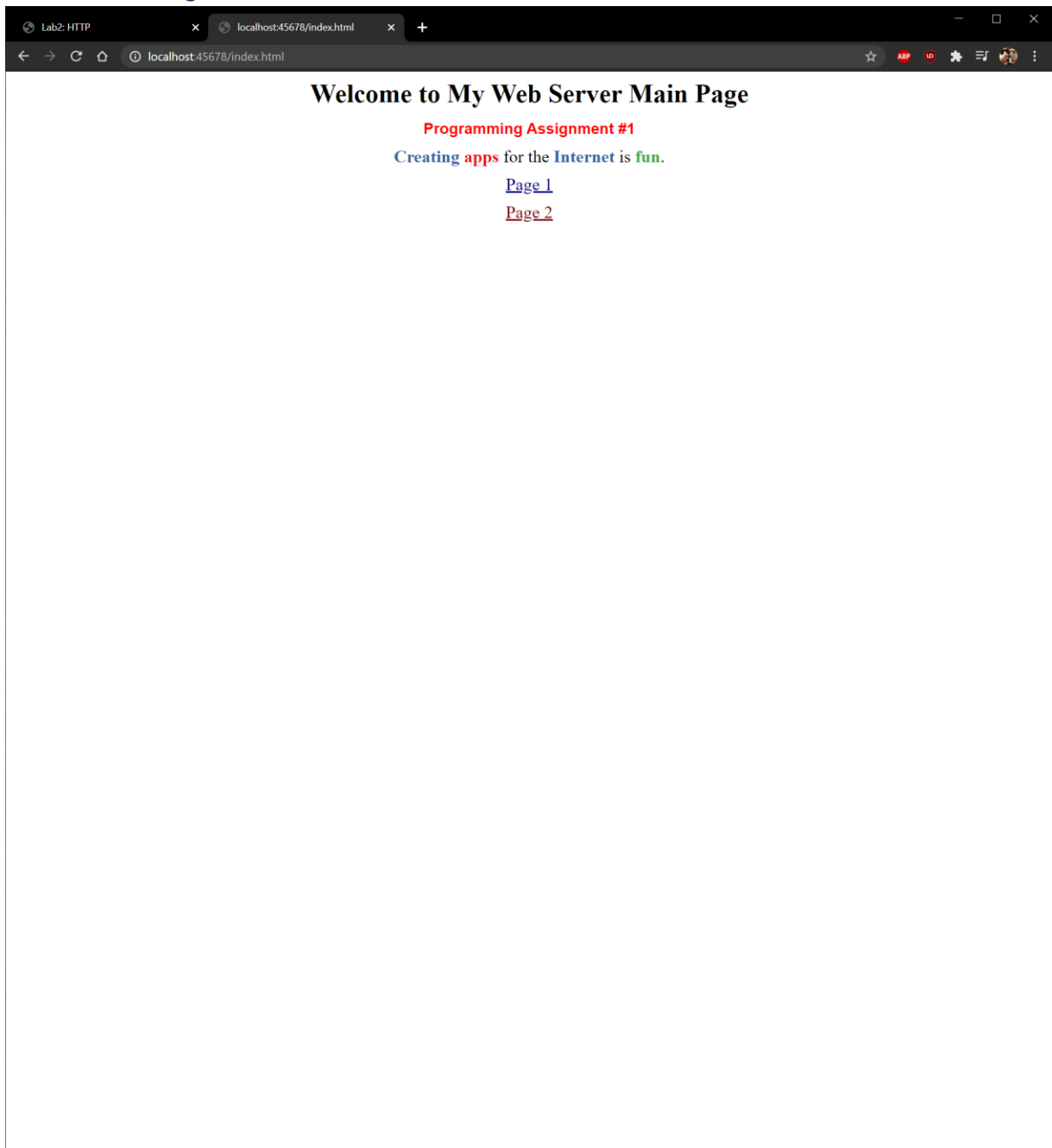
```
except IOError:
    # TASK 6
    #Send response message for file not found
    #Fill in start
    notFound = 'HTTP/1.1 404 Not Found\r\n'
    connectionSocket.send(notFound.encode('utf-8'))
    #Fill in end

    # TASK 7
    #Close client socket
    #Fill in start
    connectionSocket.close()
    #Fill in end

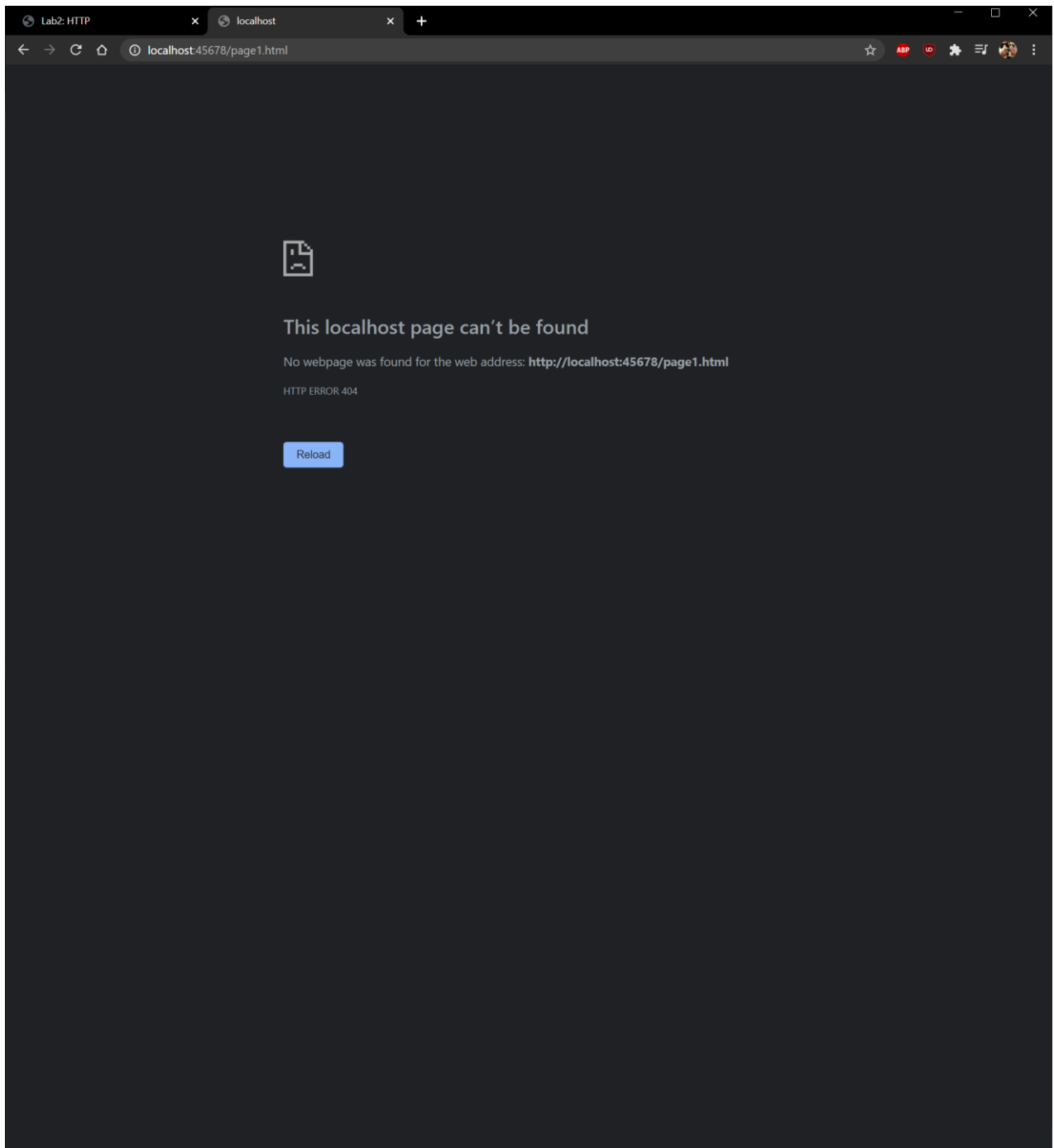
serverSocket.close()
sys.exit()#Terminate the program after sending the corresponding data
```

Screen Captures

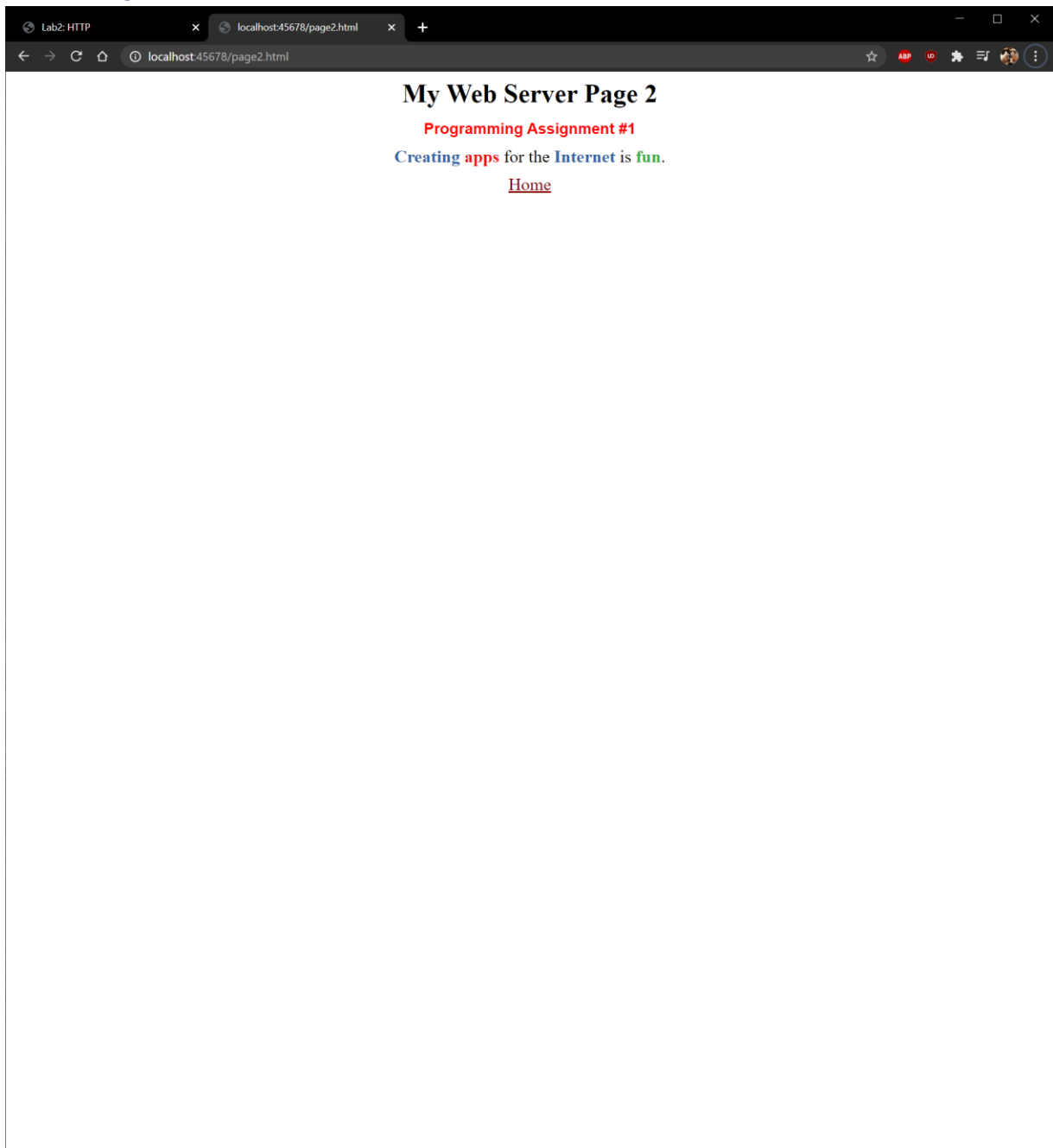
1. The Main Page



2. The 404 Not Found



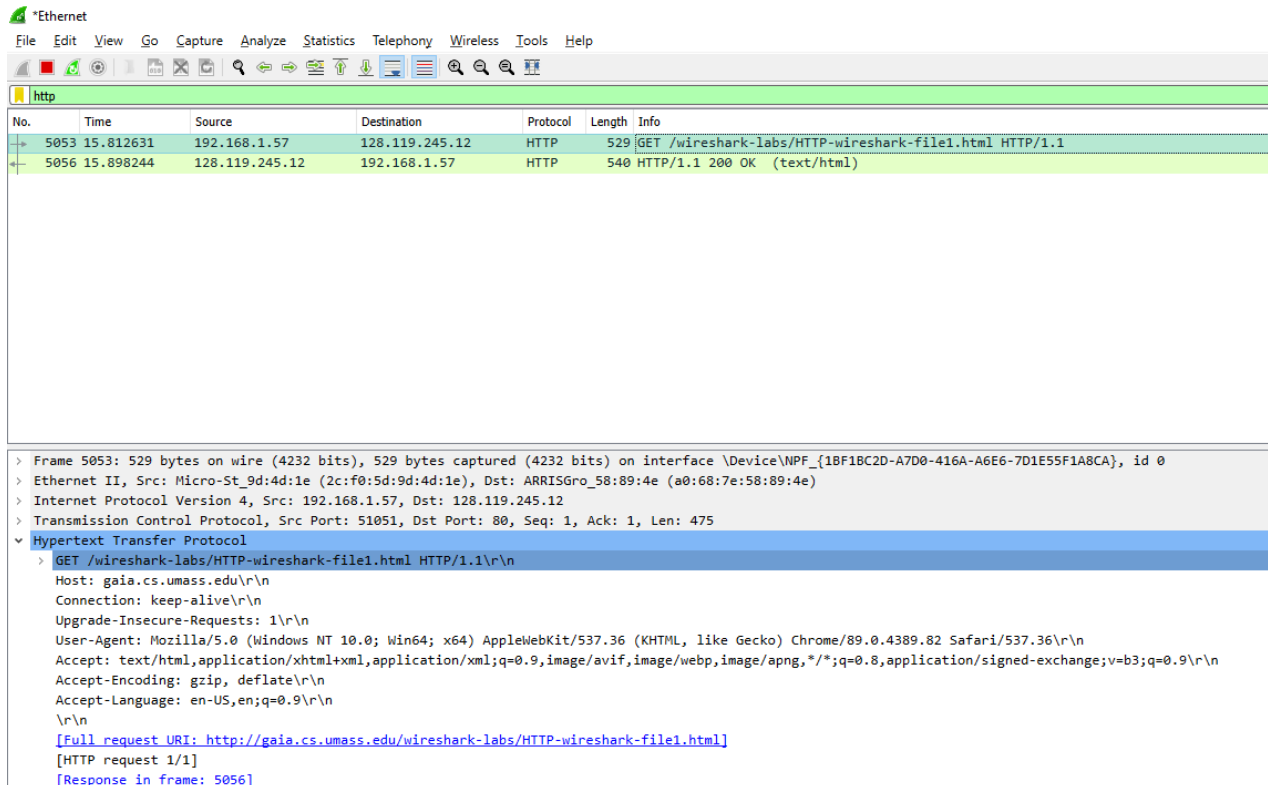
3. The Page 2



Part 2 – Analyzing HTTP messages using Wireshark

THE BASIC HTTP GET/RESPONSE INTERACTION

1.



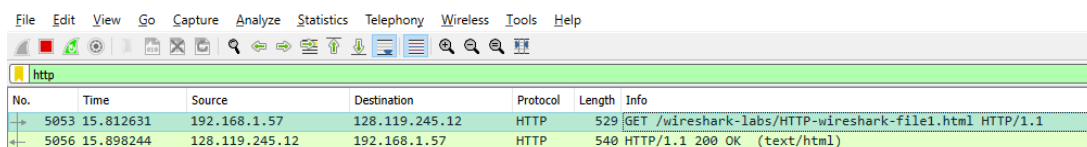
My browser is running HTTP version 1.1 as seen by the GET request. The Server is running version 1.1 as well as seen with “HTTP/1.1 200 OK”.

2.



My browser indicates that it accepts the English language as seen at the bottom of the screenshot with “en-US,en;”

3.



From the GET request we can from the source that my IP address is “192.168.1.57” and the address of the server is the destination at “128.119.245.12”

4.

```
> Frame 5056: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{18F1BC2D-A7D0-416A-A6E6-7D1E55F1A8CA}, id 0
> Ethernet II, Src: ARRISGro_58:89:4e (a0:68:7e:58:89:4e), Dst: Micro-St_d:4d:1e (2c:f0:5d:9d:4d:1e)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.57
> Transmission Control Protocol, Src Port: 80, Dst Port: 51051, Seq: 1, Ack: 476, 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
```

The status code is 200 as seen in the highlighted section of the screenshot.

5.

```
> Transmission Control Protocol, Src Port: 80, Dst Port: 51051, Seq: 1, Ack: 476, 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: Mon, 15 Mar 2021 04:10:24 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
      Last-Modified: Sun, 14 Mar 2021 06:59:01 GMT\r\n
      ETag: "80-5bd79ab0783da"\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
```

The HTML file was last modified “Sun, 14 Mar 2021 06:59:01 GMT” as seen in the highlighted section of the screenshot

6.

```
Date: Mon, 15 Mar 2021 04:10:24 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Sun, 14 Mar 2021 06:59:01 GMT\r\n
ETag: "80-5bd79ab0783da"\r\n
Accept-Ranges: bytes\r\n
> Content-Length: 128\r\n
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.085613000 seconds]
  [Request in frame: 5053]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
  File Data: 128 bytes
```

From the screen shot we see that “Content-Length: 128” and “File Data: 128 bytes” so we know 128 bytes are being returned to the browser.

7.

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
5053	15.812631	192.168.1.57	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
5056	15.898244	128.119.245.12	192.168.1.57	HTTP	540	HTTP/1.1 200 OK (text/html)
7806	158.629725	2603:8000:63f:f0be::...	2606:2800:11f:85d:1::...	HTTP	361	GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?88cfb2e47adfa1b HTTP/1.1
7808	158.649576	2606:2800:11f:85d:1::...	2603:8000:63f:f0be::...	HTTP	366	HTTP/1.1 304 Not Modified
7809	158.653326	2603:8000:63f:f0be::...	2606:2800:11f:85d:1::...	HTTP	356	GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?b5c992abe8255e43 HTTP/1.1
7810	158.676722	2606:2800:11f:85d:1::...	2603:8000:63f:f0be::...	HTTP	403	HTTP/1.1 304 Not Modified
7897	179.736817	2603:8000:63f:f0be::...	2606:2800:11f:85d:1::...	HTTP	361	GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?c71d30dbda2917ee HTTP/1.1
7899	179.752810	2606:2800:11f:85d:1::...	2603:8000:63f:f0be::...	HTTP	366	HTTP/1.1 304 Not Modified
7900	179.756621	2603:8000:63f:f0be::...	2606:2800:11f:85d:1::...	HTTP	356	GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?7feec28952f03c2c HTTP/1.1
7901	179.773074	2606:2800:11f:85d:1::...	2603:8000:63f:f0be::...	HTTP	403	HTTP/1.1 304 Not Modified
10713	575.230396	192.168.1.130	192.168.1.57	HTTP/X...	1192	POST /5e707e06-8beb-4910-a8da-5c6b207c61c5 HTTP/1.1
10714	575.230865	192.168.1.57	192.168.1.130	HTTP	213	HTTP/1.1 202
10725	575.384804	fe80::18a9:d5cf:997::...	fe80::190e:bea1:322::...	HTTP/X...	807	POST /b8d6b5fa-7d14-4f92-8510-a845ee8596cf/ HTTP/1.1
10728	575.385397	fe80::190e:bea1:322::...	fe80::18a9:d5cf:997::...	HTTP/X...	975	HTTP/1.1 200
10737	575.501060	192.168.1.130	192.168.1.57	HTTP/X...	1192	POST /5e707e06-8beb-4910-a8da-5c6b207c61c5 HTTP/1.1
10738	575.501338	192.168.1.57	192.168.1.130	HTTP	213	HTTP/1.1 202

[Checksum Status: Unverified]
 Urgent Pointer: 0
 > [SEQ/ACK analysis]
 > [Timestamps]
 TCP payload (486 bytes)

▼ Hypertext Transfer Protocol

> HTTP/1.1 200 OK\r\n

Date: Mon, 15 Mar 2021 04:10:24 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n

Last-Modified: Sun, 14 Mar 2021 06:59:01 GMT\r\n

ETag: "80-5bd79ab0783da"\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

In the packet listing window, only the status code is seen, so headers like “Content-Length” and “Keep-Alive” are only displayed in the packet content window.

The HTTP CONDITIONAL GET/RESPONSE INTERACTION

8.

The screenshot shows the Wireshark interface with the 'http' filter applied. The packet list pane displays four packets, with packet 17 selected. The packet details pane shows the expanded 'GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1' request. The request includes headers for Host, Connection, Upgrade-Insecure-Requests, User-Agent, Accept, Accept-Encoding, and Accept-Language. The full request URI is highlighted in blue.

No.	Time	Source	Destination	Protocol	Length	Info
15	6.414256	192.168.1.57	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
17	6.503133	128.119.245.12	192.168.1.57	HTTP	784	HTTP/1.1 200 OK (text/html)
94	20.590708	192.168.1.57	128.119.245.12	HTTP	641	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
97	20.675693	128.119.245.12	192.168.1.57	HTTP	294	HTTP/1.1 304 Not Modified

```
> 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]
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
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.82 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\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/HTTP-wireshark-file2.html]
[HTTP request 1/1]
[Response in frame: 17]
```

There is no “If-Modified-Since” in the first HTTP GET request.

9.

The screenshot shows the Wireshark interface with the 'http' filter applied. The packet list pane displays four packets, with packet 17 selected. The packet details pane shows the expanded 'HTTP response 1/1' for the first request. The response includes headers for Date, Server, Last-Modified, ETag, Accept-Ranges, Content-Length, Keep-Alive, Connection, Content-Type, and Content-Disposition. The full response URI is highlighted in blue.

No.	Time	Source	Destination	Protocol	Length	Info
15	6.414256	192.168.1.57	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
17	6.503133	128.119.245.12	192.168.1.57	HTTP	784	HTTP/1.1 200 OK (text/html)
94	20.590708	192.168.1.57	128.119.245.12	HTTP	641	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
97	20.675693	128.119.245.12	192.168.1.57	HTTP	294	HTTP/1.1 304 Not Modified

```
Date: Mon, 15 Mar 2021 04:31:24 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Sun, 14 Mar 2021 06:59:01 GMT\r\n
ETag: "173-5bd79ab077c0a"\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 1/1]
[Time since request: 0.088877000 seconds]
[Request in frame: 15]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
File Data: 371 bytes
> Line-based text data: text/html (10 lines)
```

From the server response, we can see that the server explicitly returns 371 bytes of file data, or 10 lines of “text/html” data from the screenshot highlight.

10.

The screenshot shows a Wireshark capture of an HTTP GET request. The packet list pane displays four packets, with packet 94 selected. The packet details pane shows the Hypertext Transfer Protocol section expanded, displaying the full request URI and other headers.

No.	Time	Source	Destination	Protocol	Length	Info
15	6.414256	192.168.1.57	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
17	6.503133	128.119.245.12	192.168.1.57	HTTP	784	HTTP/1.1 200 OK (text/html)
94	20.590708	192.168.1.57	128.119.245.12	HTTP	641	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
97	20.675693	128.119.245.12	192.168.1.57	HTTP	294	HTTP/1.1 304 Not Modified

Hypertext Transfer Protocol

- GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
- 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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.82 Safari/537.36\r\n
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
- Accept-Encoding: gzip, deflate\r\n
- Accept-Language: en-US,en;q=0.9\r\n
- If-None-Match: "173-5bd79ab077c0a"\r\n
- If-Modified-Since: Sun, 14 Mar 2021 06:59:01 GMT\r\n
- \r\n
- [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
- [HTTP request 1/1]
- [Response in frame: 97]

There is an “If-Modified-Since” and the information following it is the exact time and data that it was sent from the server.

11.

The screenshot shows a Wireshark capture of an HTTP 304 Not Modified response. The packet list pane displays four packets, with packet 97 selected. The packet details pane shows the Hypertext Transfer Protocol section expanded, displaying the response status code and other headers.

No.	Time	Source	Destination	Protocol	Length	Info
15	6.414256	192.168.1.57	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
17	6.503133	128.119.245.12	192.168.1.57	HTTP	784	HTTP/1.1 200 OK (text/html)
94	20.590708	192.168.1.57	128.119.245.12	HTTP	641	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
97	20.675693	128.119.245.12	192.168.1.57	HTTP	294	HTTP/1.1 304 Not Modified

Transmission Control Protocol, Src Port: 80, Dst Port: 51575, Seq: 1, Ack: 588, Len: 240

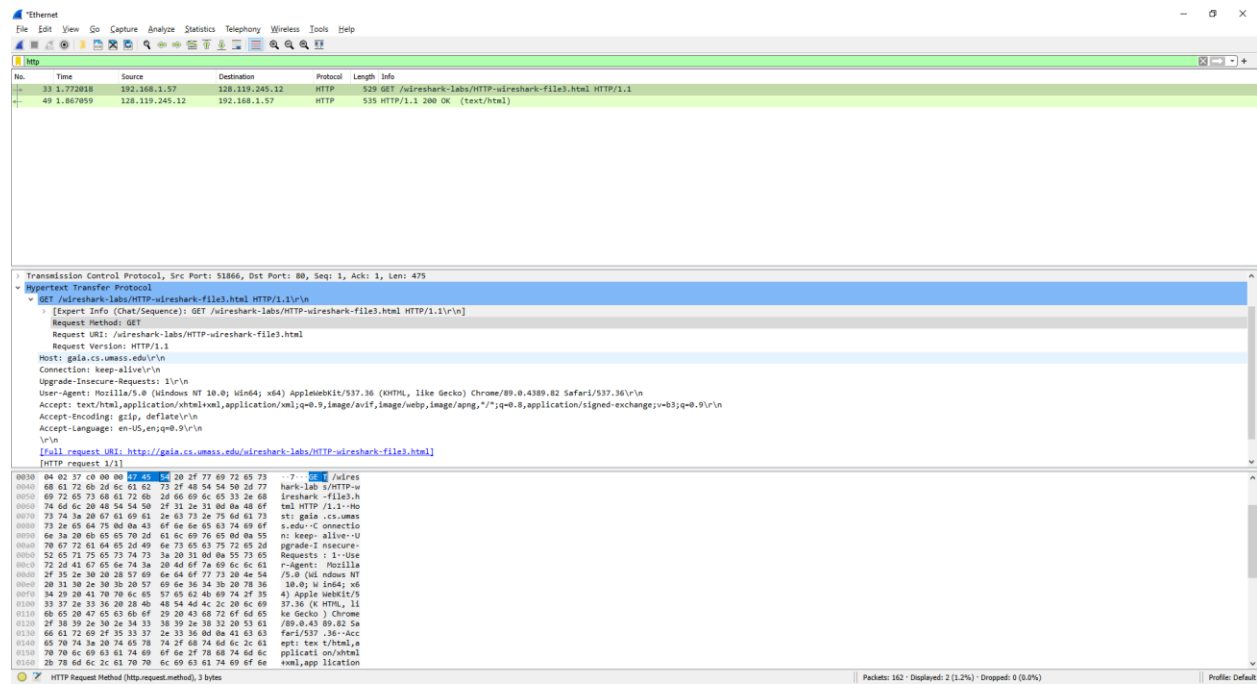
Hypertext Transfer Protocol

- HTTP/1.1 304 Not Modified\r\n
- [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
- Response Version: HTTP/1.1
- Status Code: 304
- [Status Code Description: Not Modified]
- Response Phrase: Not Modified
- Date: Mon, 15 Mar 2021 04:31:39 GMT\r\n
- Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 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: "173-5bd79ab077c0a"\r\n
- \r\n
- [HTTP response 1/1]
- [Time since request: 0.084985000 seconds]
- [Request in frame: 94]

The HTTP status code from the second server response was 304 Not Modified. This time, the server didn’t explicitly return the contents of the file because there is no “Content-Length” header or raw text data sent in this response unlike the first server response.

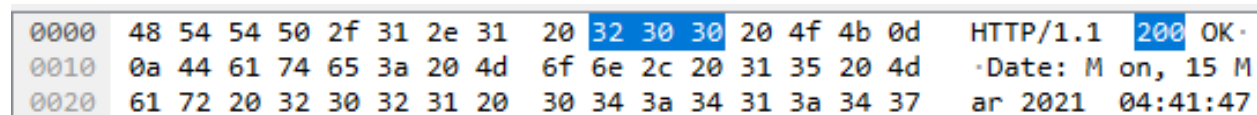
RETRIEVING LONG DOCUMENTS

12.



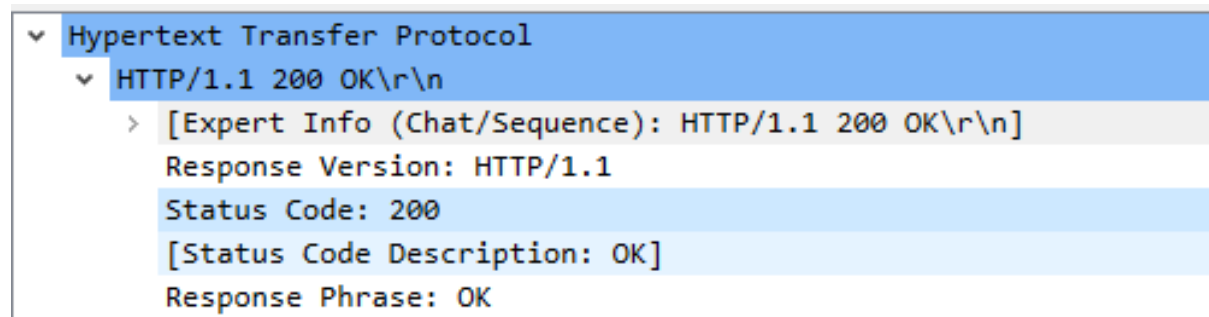
The browser only sent one HTTP GET request message as seen in “[HTTP request 1/1]”. The packet number corresponding to the GET message was “47 54 54” in hexadecimal as seen in the highlighted portions.

13.



The packet number corresponding to the status code 200 in the server response was “32 30 30” in hexadecimal.

14.



The status code was 200 and the response phrase was OK.

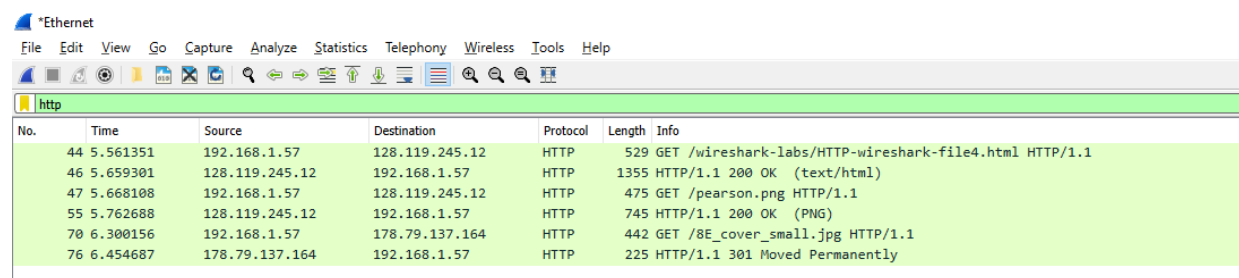
15.

```
▼ [4 Reassembled TCP Segments (4861 bytes): #45(1460), #46(1460), #48(1460), #49(481)]
[Frame: 45, payload: 0-1459 (1460 bytes)]
[Frame: 46, payload: 1460-2919 (1460 bytes)]
[Frame: 48, payload: 2920-4379 (1460 bytes)]
[Frame: 49, payload: 4380-4860 (481 bytes)]
[Segment count: 4]
[Reassembled TCP length: 4861]
[Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a204d6f6e2c203135204d61722032...]
```

There were 4 TCP segments that were needed to carry the HTTP response and the text.

HTML DOCUMENTS WITH EMBEDDED OBJECTS

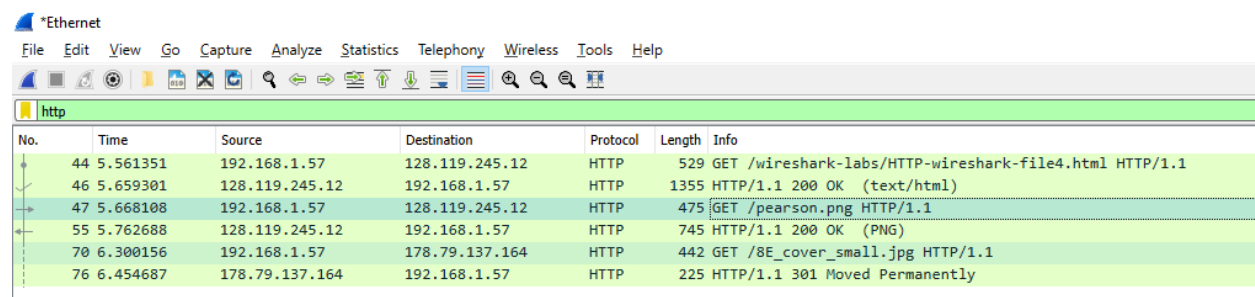
16.



No.	Time	Source	Destination	Protocol	Length	Info
44	5.561351	192.168.1.57	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
46	5.659301	128.119.245.12	192.168.1.57	HTTP	1355	HTTP/1.1 200 OK (text/html)
47	5.668108	192.168.1.57	128.119.245.12	HTTP	475	GET /pearson.png HTTP/1.1
55	5.762688	128.119.245.12	192.168.1.57	HTTP	745	HTTP/1.1 200 OK (PNG)
70	6.300156	192.168.1.57	178.79.137.164	HTTP	442	GET /8E_cover_small.jpg HTTP/1.1
76	6.454687	178.79.137.164	192.168.1.57	HTTP	225	HTTP/1.1 301 Moved Permanently

There were 3 total GET requests from the browser, where the first 2 were sent to IP address [128.119.245.12](#) and the last was sent to IP address [178.79.137.164](#).

17.



No.	Time	Source	Destination	Protocol	Length	Info
44	5.561351	192.168.1.57	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
46	5.659301	128.119.245.12	192.168.1.57	HTTP	1355	HTTP/1.1 200 OK (text/html)
47	5.668108	192.168.1.57	128.119.245.12	HTTP	475	GET /pearson.png HTTP/1.1
55	5.762688	128.119.245.12	192.168.1.57	HTTP	745	HTTP/1.1 200 OK (PNG)
70	6.300156	192.168.1.57	178.79.137.164	HTTP	442	GET /8E_cover_small.jpg HTTP/1.1
76	6.454687	178.79.137.164	192.168.1.57	HTTP	225	HTTP/1.1 301 Moved Permanently

We can tell that these two images were downloaded at different times due to the [Time](#) column in the packet listing window. The second GET request was done after the first one got its response, so we can say that the images were downloaded serially.

HTTP AUTHENTICATION

18.

The screenshot shows a Wireshark capture of an HTTP 401 Unauthorized response. The packet list pane shows four packets: a GET request (10), a 401 response (12), another GET request (90), and a 200 OK response (93). The packet details pane for packet 12 is expanded, showing the Hypertext Transfer Protocol section with the status code 401 and the phrase 'Unauthorized'.

No.	Time	Source	Destination	Protocol	Length	Info
10	1.304839	192.168.1.57	128.119.245.12	HTTP	545	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
12	1.394693	128.119.245.12	192.168.1.57	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
90	10.943362	192.168.1.57	128.119.245.12	HTTP	630	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
93	11.033062	128.119.245.12	192.168.1.57	HTTP	544	HTTP/1.1 200 OK (text/html)

Frame 12: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{1BF1BC2D-A7D0-416A-A6E6-7D1E55F1A8CA}, id 0
> Ethernet II, Src: ARRISGro_58:89:4e (a0:68:7e:58:89:4e), Dst: Micro-St_9d:4d:1e (2c:f0:5d:9d:4d:1e)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.57
> Transmission Control Protocol, Src Port: 80, Dst Port: 52336, Seq: 1, Ack: 492, Len: 717
> Hypertext Transfer Protocol
 > HTTP/1.1 401 Unauthorized\r\n
 > [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
 Response Version: HTTP/1.1
 Status Code: 401
 [Status Code Description: Unauthorized]
 Response Phrase: Unauthorized
 Date: Mon, 15 Mar 2021 05:00:46 GMT\r\n

The server's initial response the HTTP GET message was **401 Unauthorized**

19.

The screenshot shows a Wireshark capture of an HTTP GET request. The packet list pane shows four packets: a GET request (10), a 401 response (12), a second GET request (90), and a 200 OK response (93). The packet details pane for packet 90 is expanded, showing the Hypertext Transfer Protocol section with the request method GET, the URI /wireshark-labs/protected_pages/HTTP-wireshark-file5.html, and the Authorization header: Basic d2lyZXNoYXJrLXN0dWRIbnRzOm5ldHdvcm0=.

No.	Time	Source	Destination	Protocol	Length	Info
10	1.304839	192.168.1.57	128.119.245.12	HTTP	545	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
12	1.394693	128.119.245.12	192.168.1.57	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
90	10.943362	192.168.1.57	128.119.245.12	HTTP	630	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
93	11.033062	128.119.245.12	192.168.1.57	HTTP	544	HTTP/1.1 200 OK (text/html)

Frame 90: 630 bytes on wire (5040 bits), 630 bytes captured (5040 bits) on interface \Device\NPF_{1BF1BC2D-A7D0-416A-A6E6-7D1E55F1A8CA}, id 0
> Ethernet II, Src: Micro-St_9d:4d:1e (2c:f0:5d:9d:4d:1e), Dst: ARRISGro_58:89:4e (a0:68:7e:58:89:4e)
> Internet Protocol Version 4, Src: 192.168.1.57, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 52340, Dst Port: 80, Seq: 1, Ack: 1, Len: 576
> Hypertext Transfer Protocol
 > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
 > [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
 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 d2lyZXNoYXJrLXN0dWRIbnRzOm5ldHdvcm0=\r\n
 Upgrade-Insecure-Requests: 1\r\n

The new field included in the second HTTP GET message is **“Authorization”**