

CENG 435 - Data Communications and Networking

2023-1

Wireshark Assignment 2

Anıl Eren Göçer
e2448397@ceng.metu.edu.tr

October 26, 2023

1. My Browser: HTTP 1.1

The server: HTTP 1.1

```
> Frame 183: 514 bytes on wire (4112 bits), 514 bytes captured (4112 bits) on interface \Device\NPF_{C8CA7682-5C7F-429D-9DE7-0BB02CB24562}, id 0
> Ethernet II, Src: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4), Dst: IntelCor_d2:46:ed (00:1b:21:d2:46:ed)
> Internet Protocol Version 4, Src: 144.122.41.179, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 55755, Dst Port: 80, Seq: 1, Ack: 1, Len: 460
▼ 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/118.0.0.0 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: tr\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: 197]
      [Next request in frame: 202]
```

Figure 1: My Browser's HTTP version

```
> Frame 197: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{C8CA7682-5C7F-429D-9DE7-0BB02CB24562}, id 0
> Ethernet II, Src: IntelCor_d2:46:ed (00:1b:21:d2:46:ed), Dst: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 144.122.41.179
> Transmission Control Protocol, Src Port: 80, Dst Port: 55755, Seq: 1, Ack: 461, 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, 20 Oct 2023 18:09:48 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, 20 Oct 2023 05:59:02 GMT\r\n
      0000 3c f0 11 e1 a6 f4 00 1b 21 d2 46 ed 08 00 45 00 <.....!F...E-
      0010 02 0e c8 aa 40 00 27 06 59 8e 80 77 f5 0c 90 7a ...@..Y..w...z
      0020 29 b3 00 50 d9 cb 64 cb e1 3a 4a d5 9c f8 50 18 )..P..d...:J...P-
      0030 00 ed df 81 00 00 48 54 54 50 2f 31 2e 31 20 32 .....HT TP/1.1 2
      0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 46 72 69 00 OK...D ate: Fri
      0050 2c 20 32 30 20 4f 63 74 20 32 30 32 33 20 31 38 , 20 Oct 2023 18
      0060 3a 30 39 3a 34 38 20 47 4d 54 0d 0a 53 65 72 76 :09:48 G MT..Serv
      0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 3a 2e 36 er: Apac he/2.4.6
      0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 (CentOS ) OpenSS
      0090 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 L/1.0.2k -fips PH
      00a0 50 2f 37 2e 34 2e 33 33 20 6d 6f 64 5f 70 65 72 P/7.4.33 mod_per
      00b0 6c 2f 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76 35 l/2.0.11 Perl/v5
      00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3..L ast-Modi
      00d0 66 69 65 64 3a 20 46 72 69 2c 20 32 30 20 4f 63 fied: Fr i, 20 Oc
      00e0 74 20 32 30 32 33 20 30 35 3a 35 39 3a 30 32 20 t 2023 0 5:59:02
      00f0 47 4d 54 0d 0a 45 54 61 67 3a 20 22 38 30 2d 36 GMT..ETa g: "00-6
      0100 30 38 31 66 39 31 62 62 65 32 39 37 22 0d 0a 41 081f91bb e297"-A
      0110 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 ccept-Ra nges: by
```

Figure 2: Server's HTTP version

2. It accepts **Turkish** which is represented by **tr**.

```
> Frame 183: 514 bytes on wire (4112 bits), 514 bytes captured (4112 bits) on interface \Device\NPF_{C8CA7682-5C7F-429D-9DE7-0BB02CB24562}, id 0
> Ethernet II, Src: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4), Dst: IntelCor_d2:46:ed (00:1b:21:d2:46:ed)
> Internet Protocol Version 4, Src: 144.122.41.179, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 55755, Dst Port: 80, Seq: 1, Ack: 1, Len: 460
▼ 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/118.0.0.0 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: tr\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: 197]
  [Next request in frame: 202]
```

Figure 3: Accepted languages by my browser

3.

4. My computer's IP address = 144.122.41.179

The server's IP address = 128.119.245.12

No.	Time	Source	Destination	Protocol	Length	Info
183	2.373439	144.122.41.179	128.119.245.12	HTTP	514	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
197	2.590133	128.119.245.12	144.122.41.179	HTTP	540	HTTP/1.1 200 OK (text/html)

Figure 4: My computer's IP address

No.	Time	Source	Destination	Protocol	Length	Info
183	2.373439	144.122.41.179	128.119.245.12	HTTP	514	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
197	2.590133	128.119.245.12	144.122.41.179	HTTP	540	HTTP/1.1 200 OK (text/html)

Figure 5: The server's IP address

5.

6. Status code = 200

Response Phrase = OK

```
> Frame 197: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{C8CA7682-5C7F-429D-9DE7-0BB02CB24562}, id 0
> Ethernet II, Src: IntelCor_d2:46:ed (00:1b:21:d2:46:ed), Dst: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 144.122.41.179
> Transmission Control Protocol, Src Port: 80, Dst Port: 55755, Seq: 1, Ack: 461, 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, 20 Oct 2023 18:09:48 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, 20 Oct 2023 05:59:02 GMT\r\n
    ETag: "80-6081f91bbe297"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 128\r\n
  Keep-Alive: timeout=5, max=100\r\n
  ^
```

Figure 6: Status code

7.

8. Last modification is when = Friday, 20 October 2023, 05:59:02 GMT

```
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 144.122.41.179
> Transmission Control Protocol, Src Port: 80, Dst Port: 55755, Seq: 1, Ack: 461, 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, 20 Oct 2023 18:09:48 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, 20 Oct 2023 05:59:02 GMT\r\n
        ETag: "80-6081f91bbe297"\r\n
        Accept-Ranges: bytes\r\n
```

Figure 7: Last modification time-date

9. 128 bytes are returned.

```
> Transmission Control Protocol, Src Port: 80, Dst Port: 55755, Seq: 1, Ack: 461, 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, 20 Oct 2023 18:09:48 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, 20 Oct 2023 05:59:02 GMT\r\n
        ETag: "80-6081f91bbe297"\r\n
        Accept-Ranges: bytes\r\n
    > Content-Length: 128\r\n
      [Content length: 128]
    Keep-Alive: timeout=5, max=100\r\n
```

Figure 8: Number of bytes returned

10. No, there is not such header. All the headers in the raw data are also displayed in the packet details windows. You can see corresponding raw data part to each header below.

```
> Frame 197: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_
> Ethernet II, Src: IntelCor_d2:46:ed (00:1b:21:d2:46:ed), Dst: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 144.122.41.179
> Transmission Control Protocol, Src Port: 80, Dst Port: 55755, Seq: 1, Ack: 461, Len: 486
  > Hypertext Transfer Protocol
    > HTTP/1.1 200 OK\r\n
      Date: Fri, 20 Oct 2023 18:09:48 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, 20 Oct 2023 05:59:02 GMT\r\n
      ETag: "80-6081f91bbe297"\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: 0.216694000 seconds]
    [Request in frame: 183]
    [Next request in frame: 202]
    [Next response in frame: 210]
```

0040	30 30 20 4f 4b 0d 0a 44	61 74 65 3a 20 46 72 69	00 OK--D ate: Fri
0050	2c 20 32 30 20 4f 63 74	20 32 30 32 33 20 31 38	, 20 Oct 2023 18
0060	3a 30 39 3a 34 38 20 47	4d 54 0d 0a 53 65 72 76	09:48 GMT..Serv
0070	65 72 3a 20 41 70 61 63	68 65 2f 32 2e 34 2e 36	er: Apac he/2.4.6
0080	20 28 43 65 6e 74 4f 53	29 20 4f 70 65 6e 53 53	(CentOS) OpenSS
0090	4c 2f 31 2e 30 2e 32 6b	2d 66 69 70 73 20 50 48	L/1.0.2k -fips PH
00a0	50 2f 37 2e 34 2e 33 33	20 6d 6f 64 5f 70 65 72	P/7.4.33 mod_per
00b0	6c 2f 32 2e 30 2e 31 31	20 50 65 72 6c 2f 76 35	l/2.0.11 Perl/v5
00c0	2e 31 36 2e 33 0d 0a 4c	61 73 74 2d 4d 6f 64 69	.16.3--L ast-Modi
00d0	66 69 65 64 3a 20 46 72	69 2c 20 32 30 20 4f 63	fied: Fr i, 20 Oc
00e0	74 20 32 30 32 33 20 30	35 3a 35 39 3a 30 32 20	t 2023 0 5:59:02
00f0	47 4d 54 0d 0a 45 54 61	67 3a 20 22 38 30 2d 36	GMT--ETa g: "80-6
0100	30 38 31 66 39 31 62 62	65 32 39 37 22 0d 0a 41	081f91bb e297"--A

Figure 9: Date

```
> Frame 197: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_
> Ethernet II, Src: IntelCor_d2:46:ed (00:1b:21:d2:46:ed), Dst: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 144.122.41.179
> Transmission Control Protocol, Src Port: 80, Dst Port: 55755, Seq: 1, Ack: 461, Len: 486
Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Fri, 20 Oct 2023 18:09:48 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, 20 Oct 2023 05:59:02 GMT\r\n
    ETag: "80-6081f91bbe297"\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: 0.216694000 seconds]
    [Request in frame: 183]
    [Next request in frame: 202]
    [Next response in frame: 210]
```

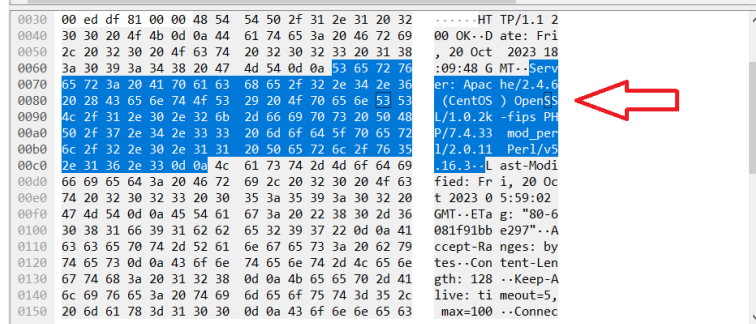


Figure 10: Server

```
> Frame 197: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_
> Ethernet II, Src: IntelCor_d2:46:ed (00:1b:21:d2:46:ed), Dst: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 144.122.41.179
> Transmission Control Protocol, Src Port: 80, Dst Port: 55755, Seq: 1, Ack: 461, Len: 486
Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Fri, 20 Oct 2023 18:09:48 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, 20 Oct 2023 05:59:02 GMT\r\n
    ETag: "80-6081f91bbe297"\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: 0.216694000 seconds]
    [Request in frame: 183]
    [Next request in frame: 202]
    [Next response in frame: 210]
```

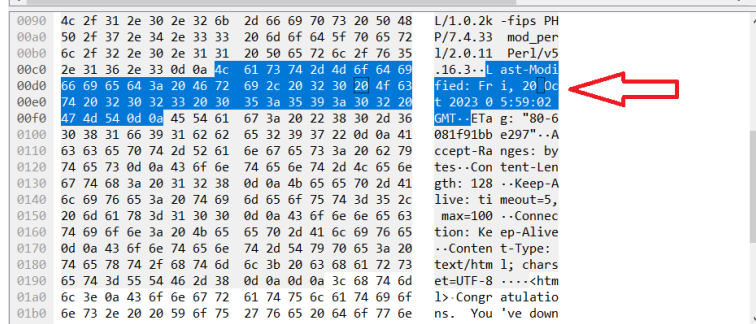


Figure 11: Last-Modified

```

> Frame 197: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_
> Ethernet II, Src: IntelCor_d2:46:ed (00:1b:21:d2:46:ed), Dst: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 144.122.41.179
> Transmission Control Protocol, Src Port: 80, Dst Port: 55755, Seq: 1, Ack: 461, Len: 486
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Fri, 20 Oct 2023 18:09:48 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, 20 Oct 2023 05:59:02 GMT\r\n
    ETag: "80-6081f91bbe297"\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: 0.216694000 seconds]
  [Request in frame: 183]
  [Next request in frame: 202]
  [Next response in frame: 210]

```

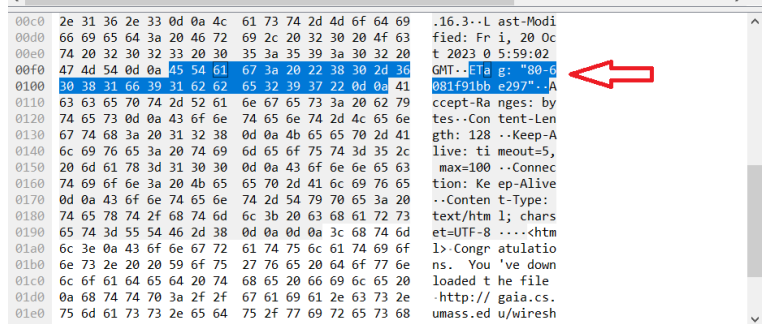


Figure 12: ETag

```

> Frame 197: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_
> Ethernet II, Src: IntelCor_d2:46:ed (00:1b:21:d2:46:ed), Dst: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 144.122.41.179
> Transmission Control Protocol, Src Port: 80, Dst Port: 55755, Seq: 1, Ack: 461, Len: 486
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Fri, 20 Oct 2023 18:09:48 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, 20 Oct 2023 05:59:02 GMT\r\n
    ETag: "80-6081f91bbe297"\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: 0.216694000 seconds]
  [Request in frame: 183]
  [Next request in frame: 202]
  [Next response in frame: 210]

```

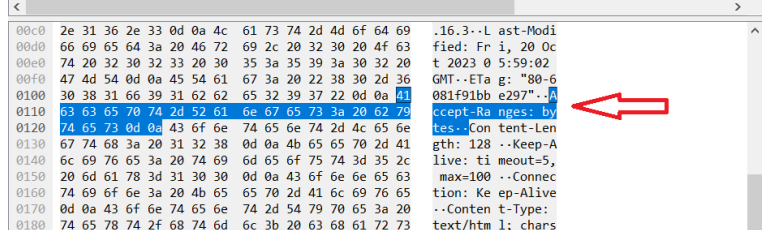


Figure 13: Accept-Ranges



```

> Frame 197: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: IntelCor_d2:46:ed (00:1b:21:d2:46:ed), Dst: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 144.122.41.179
> Transmission Control Protocol, Src Port: 80, Dst Port: 55755, Seq: 1, Ack: 461, Len: 486
Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Fri, 20 Oct 2023 18:09:48 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, 20 Oct 2023 05:59:02 GMT\r\n
    ETag: "80-6081f91bbe297"\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: 0.216694000 seconds]
    [Request in frame: 183]
    [Next request in frame: 202]
    [Next response in frame: 210]
  <
  00f0 47 4d 54 0d 0a 45 54 61 67 3a 20 22 38 30 2d 36 GMT--Etag: "80-6
  0100 30 38 31 66 39 31 62 62 65 32 39 37 22 0d 0a 41 081f91bb e297"--A
  0110 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 ccept-Ra nges: by
  0120 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e tes--Con nges: by
  0130 67 74 68 3a 20 31 32 38 0d 0a 4b 65 65 70 2d 41 gth: 128 --Keep-A
  0140 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c live: ti meout=5,
  0150 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 max=100 --Connec
  0160 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 tion: Ke ep-Alive
  0170 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 --.Content t-type:
  0180 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 78 text/htm l; chaps
  0190 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 6d et=UTF-8 --<htm
  01a0 6c 3e 0a 43 6f 6e 67 72 61 74 75 6c 61 74 69 6f l>-Congratulatio
  01b0 6e 73 2e 20 20 59 6f 75 27 76 65 20 64 6f 77 6e ns. You 've down

```

Figure 17: Content-Type

11. No, there is not “IF-MODIFIED-SINCE” line.

```

> Frame 525: 514 bytes on wire (4112 bits), 514 bytes captured (4112 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4), Dst: IntelCor_d2:46:ed (00:1b:21:d2:46:ed)
> Internet Protocol Version 4, Src: 144.122.41.179, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 59509, Dst Port: 80, Seq: 1, Ack: 1, Len: 460
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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 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\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: tr\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: 544]

```

Figure 18: Not existence of IF-MODIFIED-SINCE

12. Yes, the server explicitly returned the contents of the file. I can tell this because the HTML content is available under **Line-based text data** part.

```

> Frame 544: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: IntelCor_d2:46:ed (00:1b:21:d2:46:ed), Dst: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 144.122.41.179
> Transmission Control Protocol, Src Port: 80, Dst Port: 59509, Seq: 1, Ack: 461, Len: 730
Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Fri, 20 Oct 2023 20:02:54 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, 20 Oct 2023 05:59:02 GMT\r\n
    ETag: "173-6081f91bbdac7"\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: 0.229696000 seconds]
    [Request in frame: 525]
    [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)
    \n
    <html>\n
    \n
    Congratulations again! Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change. <p>\n
    Thus if you download this multiple times on your browser, a complete copy <br>\n
    will only be sent once by the server due to the inclusion of the IF-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n

```

Figure 19: Line-based text data

- 13.
14. Yes, I see "IF-MODIFIED-SINCE" line. It includes the information of the last modification time-data on the response content and it is Fri, 20 October 2023, 05:59:02 GMT.

```
> Frame 1825: 626 bytes on wire (5008 bits), 626 bytes captured (5008 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4), Dst: IntelCor_d2:46:ed (00:1b:21:d2:46:ed)
> Internet Protocol Version 4, Src: 144.122.41.179, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 59526, Dst Port: 80, Seq: 1, Ack: 1, Len: 572
v 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/116.0.0.0 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\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: tr\r\n
    If-None-Match: "173-6081f91bbdac7"\r\n
    If-Modified-Since: Fri, 20 Oct 2023 05:59:02 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: 1829]
```

Figure 20: IF-MODIFIED-SINCE

15. Status code = 304

Response Phrase = Not Modified

```
> Frame 1829: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF_{C8CA7682-5C7F-429D-9DE7-0B802CB24562}, id 0
> Ethernet II, Src: IntelCor_d2:46:ed (00:1b:21:d2:46:ed), Dst: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 144.122.41.179
> Transmission Control Protocol, Src Port: 80, Dst Port: 59526, Seq: 1, Ack: 573, Len: 240
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: Fri, 20 Oct 2023 20:03:04 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: "173-6081f91bbdac7"\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.142112000 seconds]
  [Request in frame: 1825]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

Figure 21: Status code, Response Phrase, Explicit content existence

No, it did not return the content of the file explicitly because browser cached it and it is the same as the content on the server since no further modification is done. This can be understood by looking at the packet bytes and packet details windows which do **not** include **Line-based text data** part.

16.

17. My browser sent 1 HTTP GET request and its packet number is 418.

No.	Time	Source	Destination	Protocol	Length	Info
418	4.616047	144.122.41.179	128.119.245.12	HTTP	514	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
432	4.761473	128.119.245.12	144.122.41.179	HTTP	1057	HTTP/1.1 200 OK (text/html)

Figure 22: HTTP GET Request count and packet number

18. The response's packet number is 432 and it includes status code and response phrase as shown below in two figures.

No.	Time	Source	Destination	Protocol	Length	Info
418	4.616047	144.122.41.179	128.119.245.12	HTTP	514	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
432	4.761473	128.119.245.12	144.122.41.179	HTTP	1057	HTTP/1.1 200 OK (text/html)

Figure 23: The response's packet number

```
> Frame 432: 1057 bytes on wire (8456 bits), 1057 bytes captured (8456 bits) on interface \Device\NPF_
> Ethernet II, Src: IntelCor_d2:46:ed (00:1b:21:d2:46:ed), Dst: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 144.122.41.179
> Transmission Control Protocol, Src Port: 80, Dst Port: 61078, Seq: 3859, Ack: 461, Len: 1003
> [2 Reassembled TCP Segments (4861 bytes): #430(3858), #432(1003)]
✓ 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, 20 Oct 2023 21:08:03 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
    Last-Modified: Fri, 20 Oct 2023 05:59:02 GMT\r\n
    ETag: "1194-6081f91bb985f"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 4500\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: 0.145426000 seconds]
    [Request in frame: 418]
    [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)
```

Figure 24: Existence of status code and response phrase in response

- 19.
20. Status code = 200

Response phrase = OK

```
> Frame 432: 1057 bytes on wire (8456 bits), 1057 bytes captured (8456 bits) on interface \Device\NPF_
> Ethernet II, Src: IntelCor_d2:46:ed (00:1b:21:d2:46:ed), Dst: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 144.122.41.179
> Transmission Control Protocol, Src Port: 80, Dst Port: 61078, Seq: 3859, Ack: 461, Len: 1003
> [2 Reassembled TCP Segments (4861 bytes): #430(3858), #432(1003)]
< 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, 20 Oct 2023 21:08:03 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
    Last-Modified: Fri, 20 Oct 2023 05:59:02 GMT\r\n
    ETag: "1194-6081f91bb985f"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 4500\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: 0.145426000 seconds]
    [Request in frame: 418]
    [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)
```

Figure 25: Status code and response phrase

21. 2 TCP segments are needed.

```
> Frame 432: 1057 bytes on wire (8456 bits), 1057 bytes captured (8456 bits) on interface \Device\NPF_
> Ethernet II, Src: IntelCor_d2:46:ed (00:1b:21:d2:46:ed), Dst: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 144.122.41.179
> Transmission Control Protocol, Src Port: 80, Dst Port: 61078, Seq: 3859, Ack: 461, Len: 1003
< [2 Reassembled TCP Segments (4861 bytes): #430(3858), #432(1003)]
  [Frame: 430, payload: 0-3857 (3858 bytes)]
  [Frame: 432, payload: 3858-4860 (1003 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 4861]
  [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a204672692c203230204f63742032...]
> Hypertext Transfer Protocol
> Line-based text data: text/html (98 lines)
```

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 46 72 69 2c 20 32 30 20 4f	-Date: Fri, 20 Oct 2023 21:08:03
0020	63 74 20 32 30 32 33 20 32 31 3a 30 38 3a 30 33	ct 2023 21:08:03
0030	20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70	GMT-Server: 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) OpenSSL/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_perl/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-Modified:
00a0	46 72 69 2c 20 32 30 20 4f 63 74 20 32 30 32 33	Fri, 20 Oct 2023
00b0	20 30 35 3a 35 39 3a 30 32 20 47 4d 54 0d 0a 45	05:59:02 GMT-E
00c0	54 61 67 3a 20 22 31 31 39 34 2d 36 30 38 31 66	Tag: "11 94-6081f
00d0	39 31 62 62 39 38 35 66 22 0d 0a 41 63 63 65 70	91bb985f "-Accp
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
0150	74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d	t/html; charset=
0160	55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 6d 6c 3e 3c	UTF-8- -<html><
0170	68 65 61 64 3e 20 0a 3c 74 69 74 6c 65 3e 48 69	head> -< title>Hi
0180	73 74 6f 72 69 63 61 6c 20 44 6f 63 75 6d 65 6e	storical Documen
0190	74 73 3a 54 48 45 20 42 49 4c 4c 20 4f 46 20 52	ts:THE B ILL OF R

Figure 26: Number of required TCP segments

22. This question is cancelled.

23.

24. My browser sent 4 HTTP GET requests.

3 of them (with packet numbers 120, 134, 475) are sent to **128.119.245.12**

1 of them (with packet number 145 is sent to **178.79.137.164**

No.	Time	Source	Destination	Protocol	Length	Info
120	3.329916	144.122.41.179	128.119.245.12	HTTP	514	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
131	3.474232	128.119.245.12	144.122.41.179	HTTP	69	HTTP/1.1 200 OK (text/html)
134	3.489501	144.122.41.179	128.119.245.12	HTTP	460	GET /pearson.png HTTP/1.1
145	3.563739	144.122.41.179	178.79.137.164	HTTP	427	GET /8E_cover_small.jpg HTTP/1.1
148	3.623661	178.79.137.164	144.122.41.179	HTTP	225	HTTP/1.1 301 Moved Permanently
155	3.631949	128.119.245.12	144.122.41.179	HTTP	1093	HTTP/1.1 200 OK (PNG)
475	5.967248	144.122.41.179	128.119.245.12	HTTP	460	GET /favicon.ico HTTP/1.1
483	6.110638	128.119.245.12	144.122.41.179	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Figure 27: HTTP GET requests that are sent

25. My browser downloaded them **in parallel**.

Packet number of request for pearson image = 134

Packet number of response for pearson image = 155

Packet number of request for cover image = 145

Packet number of response for cover image = 148

$$t_{134} = 3.489501, t_{155} = 3.631949$$

$$t_{145} = 3.563739, t_{148} = 3.623661$$

The intervals (134-155) and (145-148) intersect in time. Therefore, I inferred that they are downloaded **in parallel**.

No.	Time	Source	Destination	Protocol	Length	Info
120	3.329916	144.122.41.179	128.119.245.12	HTTP	514	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
131	3.474232	128.119.245.12	144.122.41.179	HTTP	69	HTTP/1.1 200 OK (text/html)
134	3.489501	144.122.41.179	128.119.245.12	HTTP	460	GET /pearson.png HTTP/1.1
145	3.563739	144.122.41.179	178.79.137.164	HTTP	427	GET /8E_cover_small.jpg HTTP/1.1
148	3.623661	178.79.137.164	144.122.41.179	HTTP	225	HTTP/1.1 301 Moved Permanently
155	3.631949	128.119.245.12	144.122.41.179	HTTP	1093	HTTP/1.1 200 OK (PNG)
475	5.967248	144.122.41.179	128.119.245.12	HTTP	460	GET /favicon.ico HTTP/1.1
483	6.110638	128.119.245.12	144.122.41.179	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Figure 28: Request and response times for two images

26. Packet of number of the packet containing initial HTTP GET request is 205.

No.	Time	Source	Destination	Protocol	Length	Info
205	3.821602	144.122.41.179	128.119.245.12	HTTP	530	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
212	3.968025	128.119.245.12	144.122.41.179	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
713	15.218970	144.122.41.179	128.119.245.12	HTTP	615	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
724	15.363223	128.119.245.12	144.122.41.179	HTTP	544	HTTP/1.1 200 OK (text/html)

Figure 29: Initial HTTP GET request's packet number

27. The first response's packet number is 212.

Status code = 401

Response phrase = Unauthorized

```
> Frame 212: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{C
> Ethernet II, Src: IntelCor_d2:46:ed (00:1b:21:d2:46:ed), Dst: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 144.122.41.179
> Transmission Control Protocol, Src Port: 80, Dst Port: 61964, Seq: 1, Ack: 477, 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: Fri, 20 Oct 2023 22:15:23 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
      WWW-Authenticate: Basic realm="wireshark-students only"\r\n
    > Content-Length: 381\r\n
      Keep-Alive: timeout=5, max=100\r\n
      Connection: Keep-Alive\r\n
      Content-Type: text/html; charset=iso-8859-1\r\n
      \r\n
      [HTTP response 1/1]
      [Time since request: 0.146423000 seconds]
      [Request in frame: 205]
      [Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
      File Data: 381 bytes
    > Line-based text data: text/html (12 lines)
```

Figure 30: The first response's status code and response phrase

28. A new field, **Authorization**, is included in the second HTTP GET request.

```
> Frame 713: 615 bytes on wire (4920 bits), 615 bytes captured (4920 bits) on interface \Device\NPF_{C
> Ethernet II, Src: IntelCor_e1:a6:f4 (3c:f0:11:e1:a6:f4), Dst: IntelCor_d2:46:ed (00:1b:21:d2:46:ed)
> Internet Protocol Version 4, Src: 144.122.41.179, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 61965, Dst Port: 80, Seq: 1, Ack: 1, Len: 561
✓ Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.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
  ✓ Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcm5=\r\n
    Credentials: wireshark-students:network
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chro
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: tr\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.h
    [HTTP request 1/1]
    [Response in frame: 724]
```

Figure 31: A new field, Authorization, in the second HTTP GET request