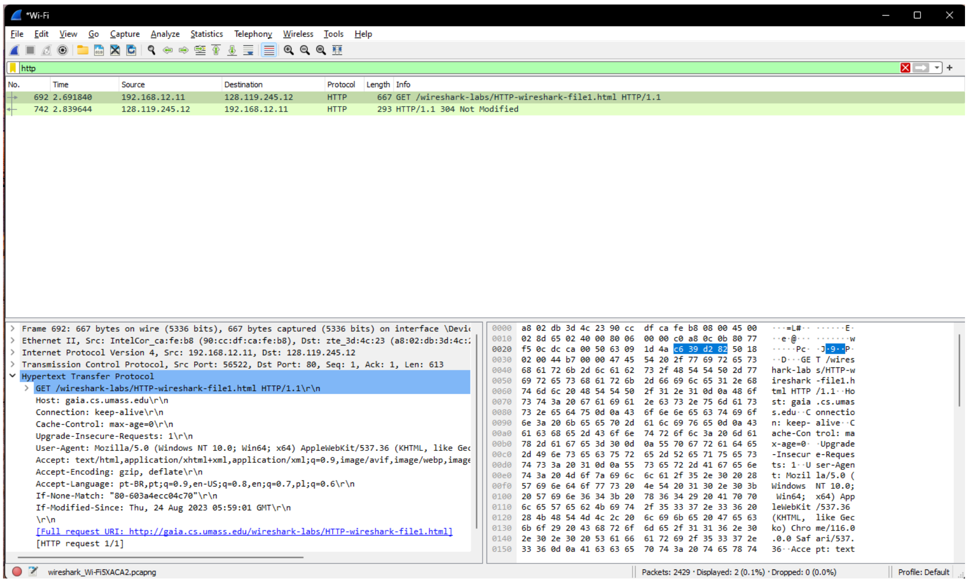
WireShark Lab 02 - HTTP v7.0

Igor Augusto Reis Gomes – 12011BSI290 – igor.augusto@ufu.br

Heitor Guimarães Da Fonseca Filho – 12011BSI203 – heitor.filho@ufu.br

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

Está rodando a versão 1.1: GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time       Source          Destination     Protocol Length Info
  692 2.691840   192.168.12.11   128.119.245.12  HTTP      667 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  742 2.839644   128.119.245.12  192.168.12.11   HTTP      293 HTTP/1.1 304 Not Modified
```

```
> Frame 692: 667 bytes on wire (5336 bits), 667 bytes captured (5336 bits) on interface \Devi
> Ethernet II, Src: IntelCor_ca:fe:b8 (90:cc:df:ca:fe:b8), Dst: zte_3d:4c:23 (a8:02:db:3d:4c:
> Internet Protocol Version 4, Src: 192.168.12.11, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 56522, Dst Port: 80, Seq: 1, Ack: 1, Len: 613
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    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 Gec
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7,pl;q=0.6\r\n
    If-None-Match: "80-603a4ecc04c70"\r\n
    If-Modified-Since: Thu, 24 Aug 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 1/1]
```

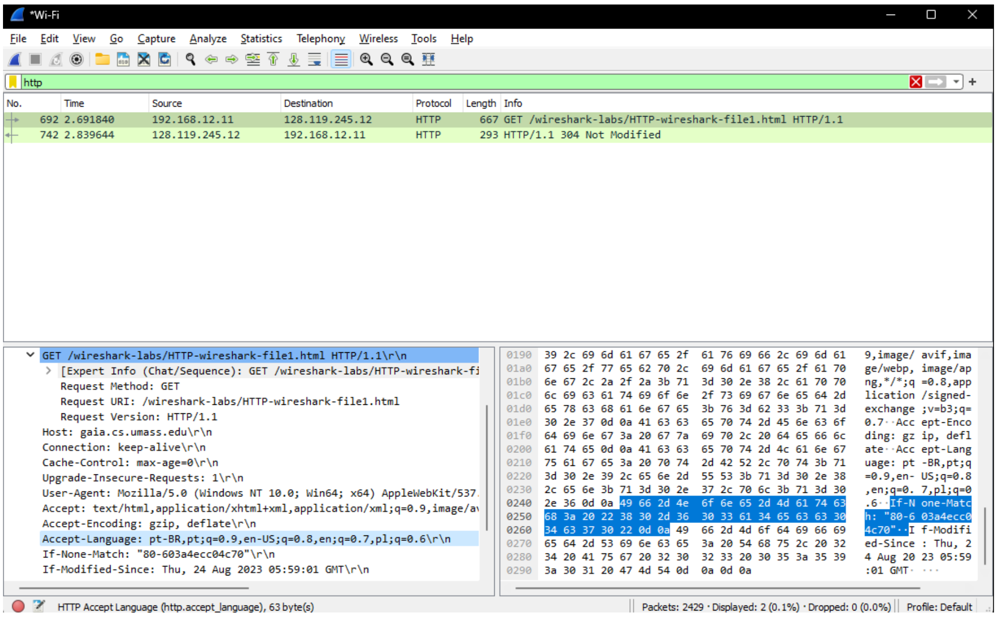
```
0000  a8 02 db 3d 4c 23 90 cc  df ca fe b8 08 00 45 00   ···=L#·· ······E·
0010  02 8d 65 02 40 00 80 06  00 00 c0 a8 0c 0b 80 77   ··e·@··· ·······w
0020  f5 0c dc ca 00 50 63 09  1d 4a c6 39 d2 82 50 18   ·····Pc· ·J·9··P·
0030  02 00 44 b7 00 00 47 45  54 20 2f 77 69 72 65 73   ··D···GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 31 2e 68   ireshark -file1.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 43   n: keep- alive··C
00a0  61 63 68 65 2d 43 6f 6e  74 72 6f 6c 3a 20 6d 61   ache-Con trol: ma
00b0  78 2d 61 67 65 3d 30 0d  0a 55 70 67 72 61 64 65   x-age=0· ·Upgrade
00c0  2d 49 6e 73 65 63 75 72  65 2d 52 65 71 75 65 73   -Insecur e-Reques
00d0  74 73 3a 20 31 0d 0a 55  73 65 72 2d 41 67 65 6e   ts: 1··U ser-Agen
00e0  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
00f0  57 69 6e 64 6f 77 73 20  4e 54 20 31 30 2e 30 3b   Windows  NT 10.0;
0100  20 57 69 6e 36 34 3b 20  78 36 34 29 20 41 70 70    Win64;  x64) App
0110  6c 65 57 65 62 4b 69 74  2f 35 33 37 2e 33 36 20   leWebKit /537.36
0120  28 4b 48 54 4d 4c 2c 20  6c 69 6b 65 20 47 65 63   (KHTML,  like Gec
0130  6b 6f 29 20 43 68 72 6f  6d 65 2f 31 31 36 2e 30   ko) Chro me/116.0
0140  2e 30 2e 30 20 53 61 66  61 72 69 2f 35 33 37 2e   .0.0 Saf ari/537.
0150  33 36 0d 0a 41 63 63 65  70 74 3a 20 74 65 78 74   36··Acce pt: text
```

wireshark_Wi-Fi5XACA2.pcapng | Packets: 2429 · Displayed: 2 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

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

As linguagens aceitas em ordem de preferência (indicado pelo valor “q”) são português(Brasil), inglês (Estados Unidos) e polonês

Accept-Language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7,pl;q=0.6\r\n


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time       Source          Destination     Protocol Length Info
  692 2.691840   192.168.12.11   128.119.245.12  HTTP      667 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  742 2.839644   128.119.245.12  192.168.12.11   HTTP      293 HTTP/1.1 304 Not Modified
```

```
  v GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-fi
      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
    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.
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/av
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7,pl;q=0.6\r\n
    If-None-Match: "80-603a4ecc04c70"\r\n
    If-Modified-Since: Thu, 24 Aug 2023 05:59:01 GMT\r\n
```

```
0190  39 2c 69 6d 61 67 65 2f  61 76 69 66 2c 69 6d 61   9,image/ avif,ima
01a0  67 65 2f 77 65 62 70 2c  69 6d 61 67 65 2f 61 70   ge/webp, image/ap
01b0  6e 67 2c 2a 2f 2a 3b 71  3d 30 2e 38 2c 61 70 70   ng,*/*;q =0.8,app
01c0  6c 69 63 61 74 69 6f 6e  2f 73 69 67 6e 65 64 2d   lication /signed-
01d0  65 78 63 68 61 6e 67 65  3b 76 3d 62 33 3b 71 3d   exchange ;v=b3;q=
01e0  30 2e 37 0d 0a 41 63 63  65 70 74 2d 45 6e 63 6f   0.7··Acc ept-Enco
01f0  64 69 6e 67 3a 20 67 7a  69 70 2c 20 64 65 66 6c   ding: gz ip, defl
0200  61 74 65 0d 0a 41 63 63  65 70 74 2d 4c 61 6e 67   ate··Acc ept-Lang
0210  75 61 67 65 3a 20 70 74  2d 42 52 2c 70 74 3b 71   uage: pt -BR,pt;q
0220  3d 30 2e 39 2c 65 6e 2d  55 53 3b 71 3d 30 2e 38   =0.9,en- US;q=0.8
0230  2c 65 6e 3b 71 3d 30 2e  37 2c 70 6c 3b 71 3d 30   ,en;q=0. 7,pl;q=0
0240  2e 36 0d 0a 49 66 2d 4e  6f 6e 65 2d 4d 61 74 63   .6··If-N one-Matc
0250  68 3a 20 22 38 30 2d 36  30 33 61 34 65 63 63 30   h: "80-6 03a4ecc0
0260  34 63 37 30 22 0d 0a 49  66 2d 4d 6f 64 69 66 69   4c70"··I f-Modifi
0270  65 64 2d 53 69 6e 63 65  3a 20 54 68 75 2c 20 32   ed-Since : Thu, 2
0280  34 20 41 75 67 20 32 30  32 33 20 30 35 3a 35 39   4 Aug 20 23 05:59
0290  3a 30 31 20 47 4d 54 0d  0a 0d 0a                  :01 GMT· ···
```

HTTP Accept Language (http.accept_language), 63 byte(s) | Packets: 2429 · Displayed: 2 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

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

O endereço IP do meu computador é: 192.168.12.11

O do servidor gaia.cs.umass.edu é: 128.119.245.12

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

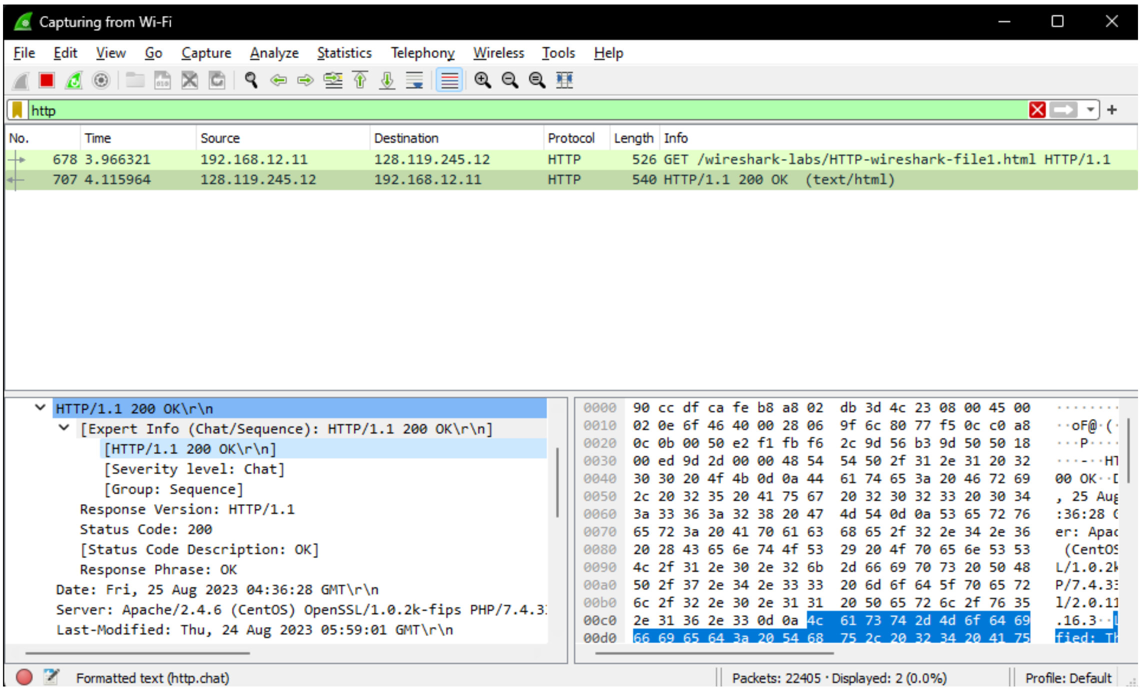
Está retornando o código de status 200:

Status Code: 200

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

Foi modificado pela última vez em:

Last-Modified: Thu, 24 Aug 2023 05:59:01 GMT\r\n


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
```

```
No.   Time      Source          Destination     Protocol Length Info
  678 3.966321  192.168.12.11   128.119.245.12  HTTP      526 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  707 4.115964  128.119.245.12  192.168.12.11   HTTP      540 HTTP/1.1 200 OK  (text/html)
```

```
v HTTP/1.1 200 OK\r\n
    v [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, 25 Aug 2023 04:36:28 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.3
  Last-Modified: Thu, 24 Aug 2023 05:59:01 GMT\r\n
```

```
0000  90 cc df ca fe b8 a8 02  db 3d 4c 23 08 00 45 00   ········
0010  02 0e 6f 46 40 00 28 06  9f 6c 80 77 f5 0c c0 a8   ··oF@·(·
0020  0c 0b 00 50 e2 f1 fb f6  2c 9d 56 b3 9d 50 50 18   ···P····
0030  00 ed 9d 2d 00 00 48 54  54 50 2f 31 2e 31 20 32   ···-··HT
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 46 72 69   00 OK··D
0050  2c 20 32 35 20 41 75 67  20 32 30 32 33 20 30 34   , 25 Aug
0060  3a 33 36 3a 32 38 20 47  4d 54 0d 0a 53 65 72 76   :36:28 G
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apac
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentOS
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73 20 50 48   L/1.0.2k
00a0  50 2f 37 2e 34 2e 33 33  20 6d 6f 64 5f 70 65 72   P/7.4.33
00b0  6c 2f 32 2e 30 2e 31 31  20 50 65 72 6c 2f 76 35   l/2.0.11
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3··L
00d0  66 69 65 64 3a 20 54 68  75 2c 20 32 34 20 41 75   fied: Th
```

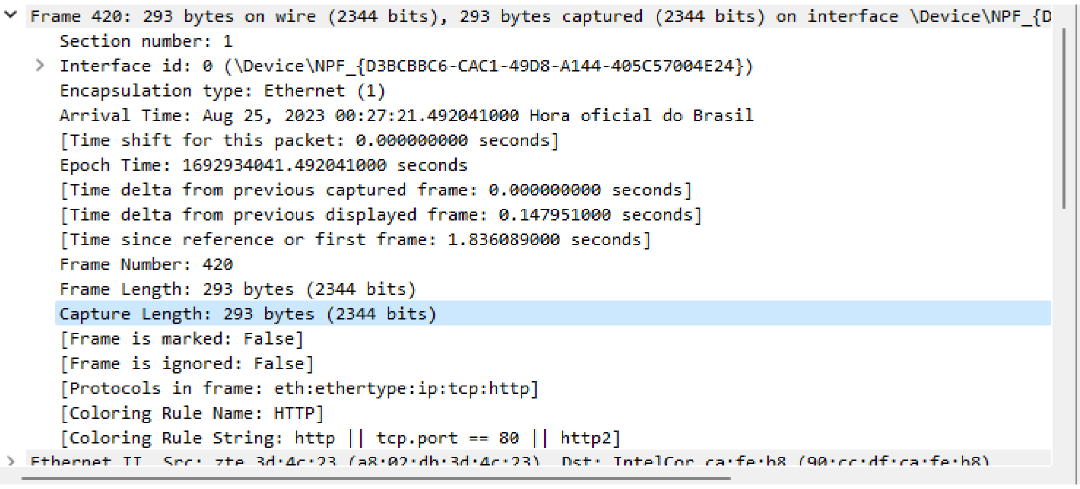
Formatted text (http.chat)

Packets: 22405 · Displayed: 2 (0.0%)

Profile: Default

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

São retornados 293 bytes ao meu navegador



```
v Frame 420: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{D
    Section number: 1
  > Interface id: 0 (\Device\NPF_{D3BCBBC6-CAC1-49D8-A144-405C57004E24})
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 25, 2023 00:27:21.492041000 Hora oficial do Brasil
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1692934041.492041000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.147951000 seconds]
    [Time since reference or first frame: 1.836089000 seconds]
    Frame Number: 420
    Frame Length: 293 bytes (2344 bits)
    Capture Length: 293 bytes (2344 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: zte_3d:4c:23 (a8:02:db:3d:4c:23), Dst: IntelCor_ca:fe:b8 (90:cc:df:ca:fe:b8)
```

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

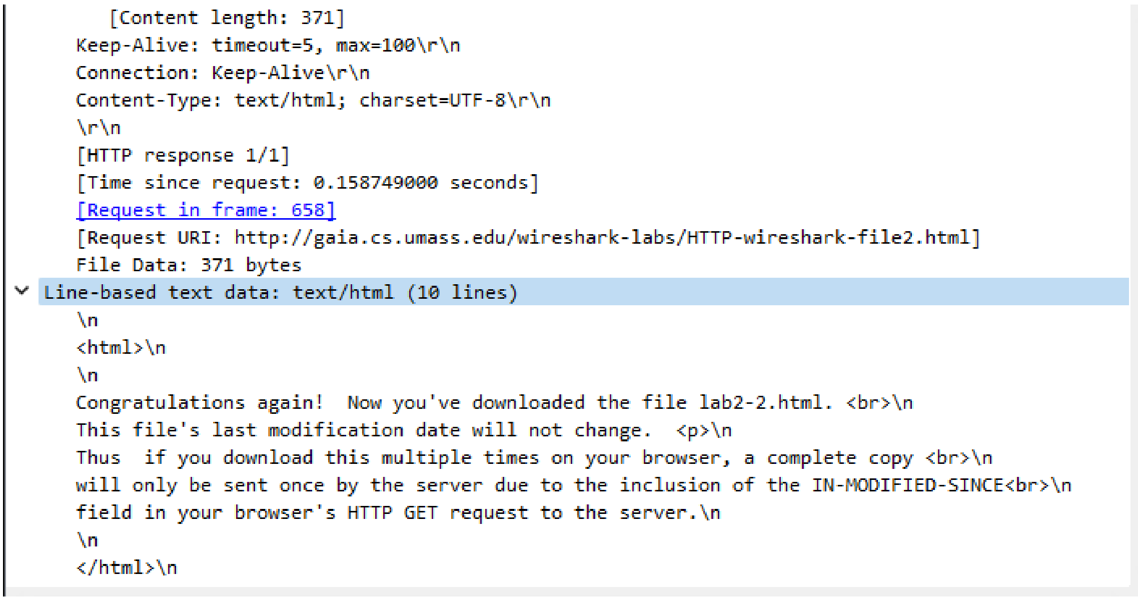
Nenhum dado é mostrado na Http Message

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

Não, apenas: Last-Modified: Thu, 24 Aug 2023 05:59:01 GMT\r\n

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

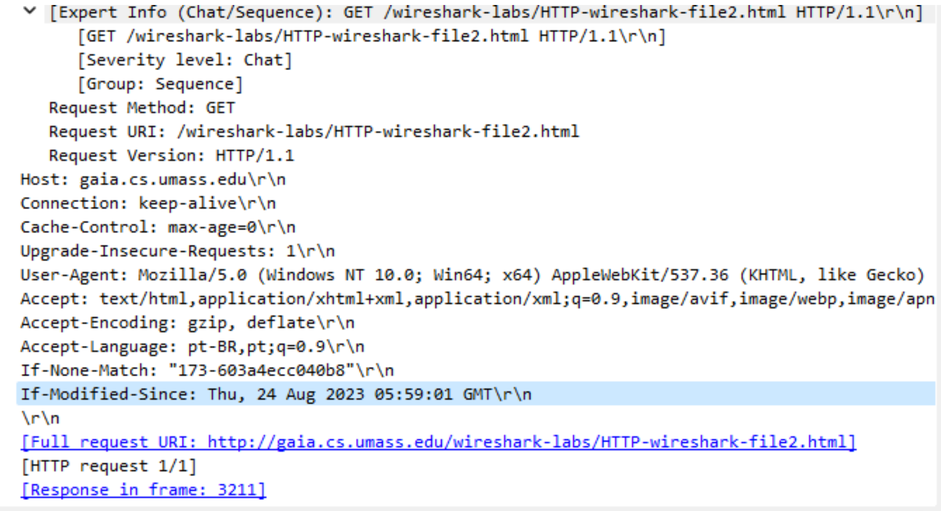
Segue abaixo, o conteúdo retornado explicitamente pelo servidor:



```
        [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: 0.158749000 seconds]
     [Request in frame: 658]
     [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 IN-MODIFIED-SINCE<br>\n
     field in your browser's HTTP GET request to the server.\n
     \n
     </html>\n
```

10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?

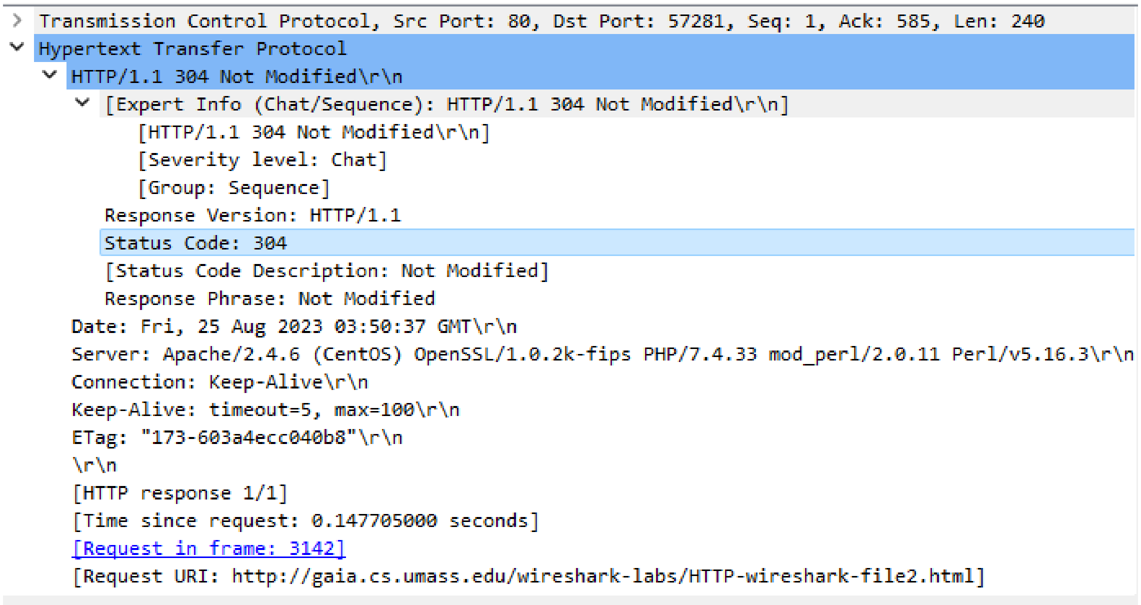
Sim, após o Segundo GET, aparece o IF-MODIFIED-SINCE: If-Modified-Since: Thu, 24 Aug 2023 05:59:01 GMT\r\n



```
  ˅ [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
       [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
       [Severity level: Chat]
       [Group: Sequence]
    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
 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)
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
 Accept-Encoding: gzip, deflate\r\n
 Accept-Language: pt-BR,pt;q=0.9\r\n
 If-None-Match: "173-603a4ecc040b8"\r\n
 If-Modified-Since: Thu, 24 Aug 2023 05:59:01 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: 3211]
```

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

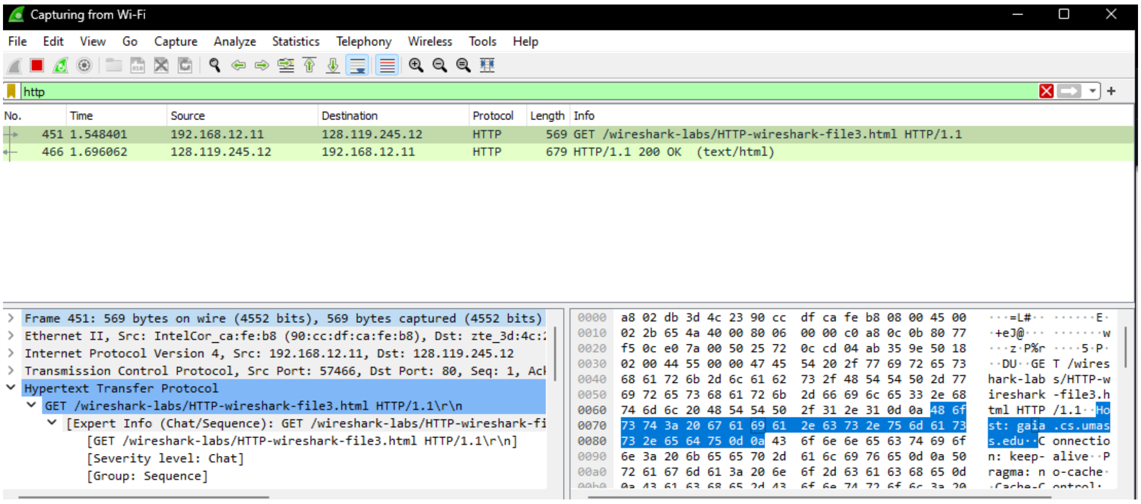
O código de status retornado é 304 Not Modified. Dado que o arquivo não foi modificado, o arquivo de texto não é retornado explicitamente pelo servidor na mensagem HTTP.



```
> Transmission Control Protocol, Src Port: 80, Dst Port: 57281, Seq: 1, Ack: 585, Len: 240
v Hypertext Transfer Protocol
  v HTTP/1.1 304 Not Modified\r\n
    v [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, 25 Aug 2023 03:50:37 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "173-603a4ecc040b8"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.147705000 seconds]
    [Request in frame: 3142]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

Foi feito apenas 1 uma requisição GET pelo navegador. O pacote tem nº 451



```
No.   Time        Source          Destination     Protocol Length Info
  451 1.548401    192.168.12.11   128.119.245.12  HTTP      569 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  466 1.696062    128.119.245.12  192.168.12.11   HTTP      679 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 451: 569 bytes on wire (4552 bits), 569 bytes captured (4552 bits)
> Ethernet II, Src: IntelCor_ca:fe:b8 (90:cc:df:ca:fe:b8), Dst: zte_3d:4c:
> Internet Protocol Version 4, Src: 192.168.12.11, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 57466, Dst Port: 80, Seq: 1, Ack
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-fi
        [GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
```

```
0000  a8 02 db 3d 4c 23 90 cc  df ca fe b8 08 00 45 00   ···=L#·· ······E·
0010  02 2b 65 4a 40 00 80 06  00 00 c0 a8 0c 0b 80 77   ·+eJ@··· ·······w
0020  f5 0c e0 7a 00 50 25 72  0c cd 04 ab 35 9e 50 18   ···z·P%r ····5·P·
0030  02 00 44 55 00 00 47 45  54 20 2f 77 69 72 65 73   ··DU··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 33 2e 68   ireshark -file3.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 50   n: keep- alive··P
00a0  72 61 67 6d 61 3a 20 6e  6f 2d 63 61 63 68 65 0d   ragma: n o-cache·
00b0  0a 43 61 63 68 65 2d 43  6f 6e 74 72 6f 6c 3a 20   ·Cache-C ontrol:
```

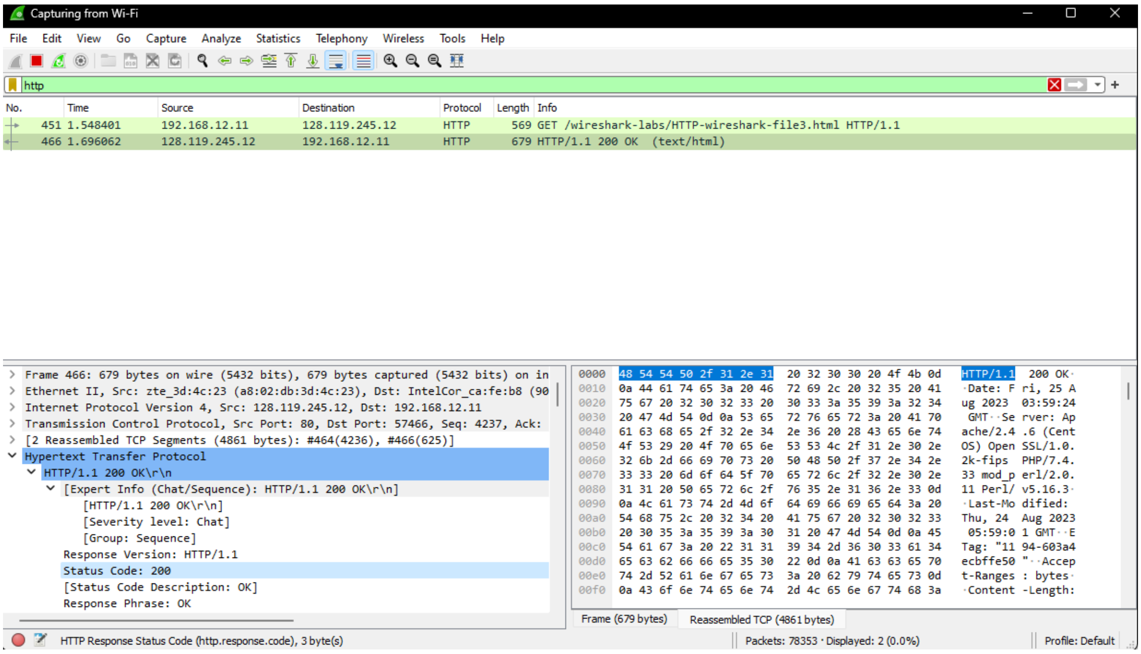
13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

O número de pacote do response associado ao GET é: 466

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

O código de status da resposta é:

HTTP/1.1 200 OK\r\n



Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.  Time      Source          Destination     Protocol Length Info
 451 1.548401  192.168.12.11   128.119.245.12  HTTP      569 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
 466 1.696062  128.119.245.12  192.168.12.11   HTTP      679 HTTP/1.1 200 OK  (text/html)
```

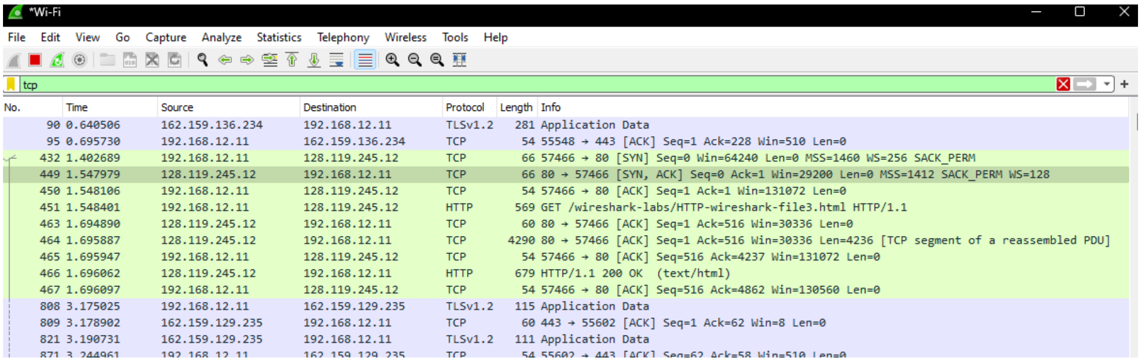
```
> Frame 466: 679 bytes on wire (5432 bits), 679 bytes captured (5432 bits) on in
> Ethernet II, Src: zte_3d:4c:23 (a8:02:db:3d:4c:23), Dst: IntelCor_ca:fe:b8 (90
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.12.11
> Transmission Control Protocol, Src Port: 80, Dst Port: 57466, Seq: 4237, Ack:
> [2 Reassembled TCP Segments (4861 bytes): #464(4236), #466(625)]
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    v [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
```

```
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 35 20 41   ·Date: F ri, 25 A
0020  75 67 20 32 30 32 33 20  30 33 3a 35 39 3a 32 34   ug 2023  03:59:24
0030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
0040  61 63 68 65 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0050  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
0060  32 6b 2d 66 69 70 73 20  50 48 50 2f 37 2e 34 2e   2k-fips  PHP/7.4.
0070  33 33 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   33 mod_p erl/2.0.
0080  31 31 20 50 65 72 6c 2f  76 35 2e 31 36 2e 33 0d   11 Perl/ v5.16.3·
0090  0a 4c 61 73 74 2d 4d 6f  64 69 66 69 65 64 3a 20   ·Last-Mo dified:
00a0  54 68 75 2c 20 32 34 20  41 75 67 20 32 30 32 33   Thu, 24  Aug 2023
00b0  20 30 35 3a 35 39 3a 30  31 20 47 4d 54 0d 0a 45    05:59:0 1 GMT··E
00c0  54 61 67 3a 20 22 31 31  39 34 2d 36 30 33 61 34   Tag: "11 94-603a4
00d0  65 63 62 66 66 65 35 30  22 0d 0a 41 63 63 65 70   ecbffe50 "··Accep
00e0  74 2d 52 61 6e 67 65 73  3a 20 62 79 74 65 73 0d   t-Ranges : bytes·
00f0  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   ·Content -Length:
```

HTTP Response Status Code (http.response.code), 3 byte(s) | Packets: 78353 · Displayed: 2 (0.0%) | Profile: Default

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

Há um pacote, o pacote 449, como é possível observar abaixo:



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

```
No.  Time      Source           Destination      Protocol Length Info
  90 0.640506  162.159.136.234  192.168.12.11    TLSv1.2   281 Application Data
  95 0.695730  192.168.12.11    162.159.136.234  TCP        54 55548 → 443 [ACK] Seq=1 Ack=228 Win=510 Len=0
 432 1.402689  192.168.12.11    128.119.245.12   TCP        66 57466 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 449 1.547979  128.119.245.12   192.168.12.11    TCP        66 80 → 57466 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412 SACK_PERM WS=128
 450 1.548106  192.168.12.11    128.119.245.12   TCP        54 57466 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
 451 1.548401  192.168.12.11    128.119.245.12   HTTP      569 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
 463 1.694890  128.119.245.12   192.168.12.11    TCP        60 80 → 57466 [ACK] Seq=1 Ack=516 Win=30336 Len=0
 464 1.695887  128.119.245.12   192.168.12.11    TCP      4290 80 → 57466 [ACK] Seq=1 Ack=516 Win=30336 Len=4236 [TCP segment of a reassembled PDU]
 465 1.695947  192.168.12.11    128.119.245.12   TCP        54 57466 → 80 [ACK] Seq=516 Ack=4237 Win=131072 Len=0
 466 1.696062  128.119.245.12   192.168.12.11    HTTP      679 HTTP/1.1 200 OK  (text/html)
 467 1.696097  192.168.12.11    128.119.245.12   TCP        54 57466 → 80 [ACK] Seq=516 Ack=4862 Win=130560 Len=0
 808 3.175025  192.168.12.11    162.159.129.235  TLSv1.2   115 Application Data
 809 3.178902  162.159.129.235  192.168.12.11    TCP        60 443 → 55602 [ACK] Seq=1 Ack=62 Win=8 Len=0
 821 3.190731  162.159.129.235  192.168.12.11    TLSv1.2   111 Application Data
 871 3.244961  192.168.12.11    162.159.129.235  TCP        54 55602 → 443 [ACK] Seq=62 Ack=58 Win=510 Len=0
```

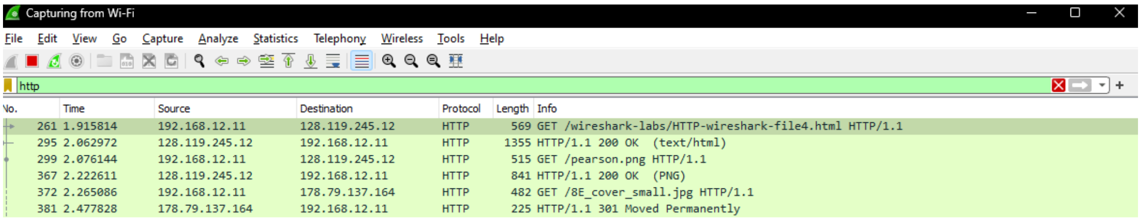
16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

Foram feitas 3 requisições GET pelo navegador. Foram enviadas para os seguintes endereços:

261 - 192.168.12.11 - 128.119.245.12 - HTTP - GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1

299 - 192.168.12.11 - 128.119.245.12 - HTTP - GET /pearson.png HTTP/1.1

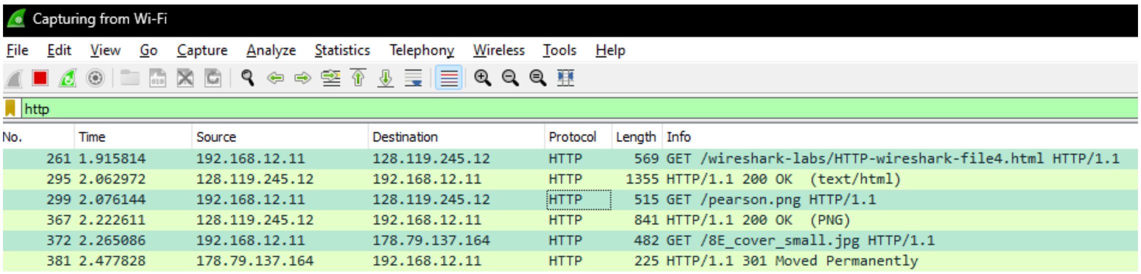
372 - 192.168.12.11 - 178.79.137.164 - HTTP - GET /8E_cover_small.jpg HTTP/1.1


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.    Time       Source           Destination      Protocol  Length  Info
  261 1.915814    192.168.12.11    128.119.245.12   HTTP      569 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
  295 2.062972    128.119.245.12   192.168.12.11    HTTP     1355 HTTP/1.1 200 OK  (text/html)
  299 2.076144    192.168.12.11    128.119.245.12   HTTP      515 GET /pearson.png HTTP/1.1
  367 2.222611    128.119.245.12   192.168.12.11    HTTP      841 HTTP/1.1 200 OK  (PNG)
  372 2.265086    192.168.12.11    178.79.137.164   HTTP      482 GET /8E_cover_small.jpg HTTP/1.1
  381 2.477828    178.79.137.164   192.168.12.11    HTTP      225 HTTP/1.1 301 Moved Permanently
```

17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

As duas mensagens GET das imagens foram baixadas em paralelo, sendo elas as de pacote de números 299 e 372:

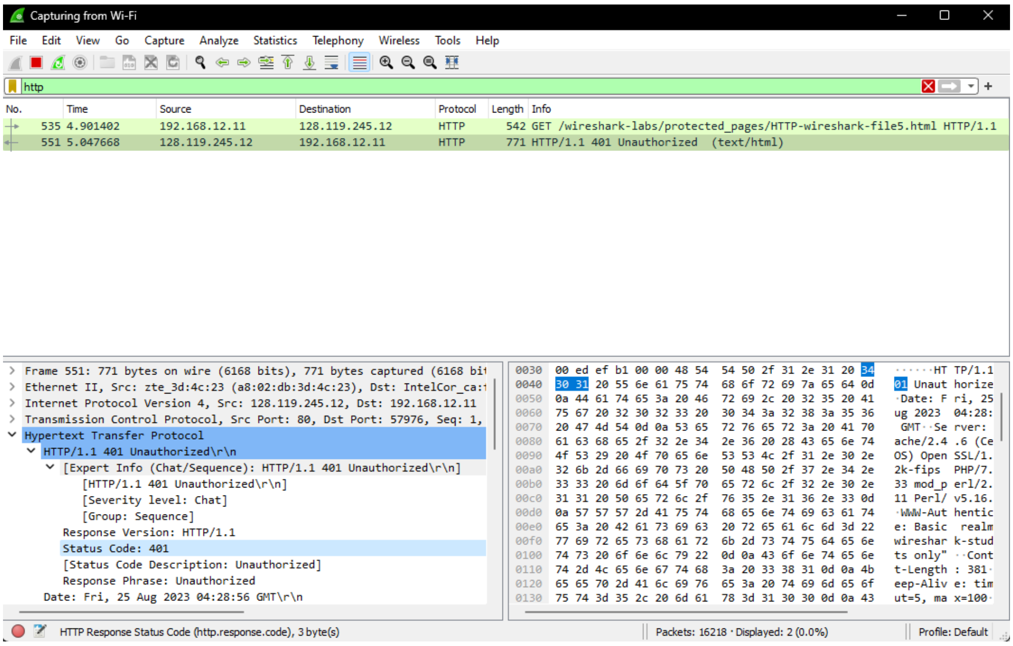

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.    Time       Source           Destination      Protocol  Length  Info
  261 1.915814    192.168.12.11    128.119.245.12   HTTP      569 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
  295 2.062972    128.119.245.12   192.168.12.11    HTTP     1355 HTTP/1.1 200 OK  (text/html)
  299 2.076144    192.168.12.11    128.119.245.12   HTTP      515 GET /pearson.png HTTP/1.1
  367 2.222611    128.119.245.12   192.168.12.11    HTTP      841 HTTP/1.1 200 OK  (PNG)
  372 2.265086    192.168.12.11    178.79.137.164   HTTP      482 GET /8E_cover_small.jpg HTTP/1.1
  381 2.477828    178.79.137.164   192.168.12.11    HTTP      225 HTTP/1.1 301 Moved Permanently
```

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

O Código de status do servidor na resposta foi 401 Unauthorized:

HTTP/1.1 401 Unauthorized\r\n


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.    Time       Source           Destination      Protocol  Length  Info
  535 4.901402    192.168.12.11    128.119.245.12   HTTP      542 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
  551 5.047668    128.119.245.12   192.168.12.11    HTTP      771 HTTP/1.1 401 Unauthorized  (text/html)
```

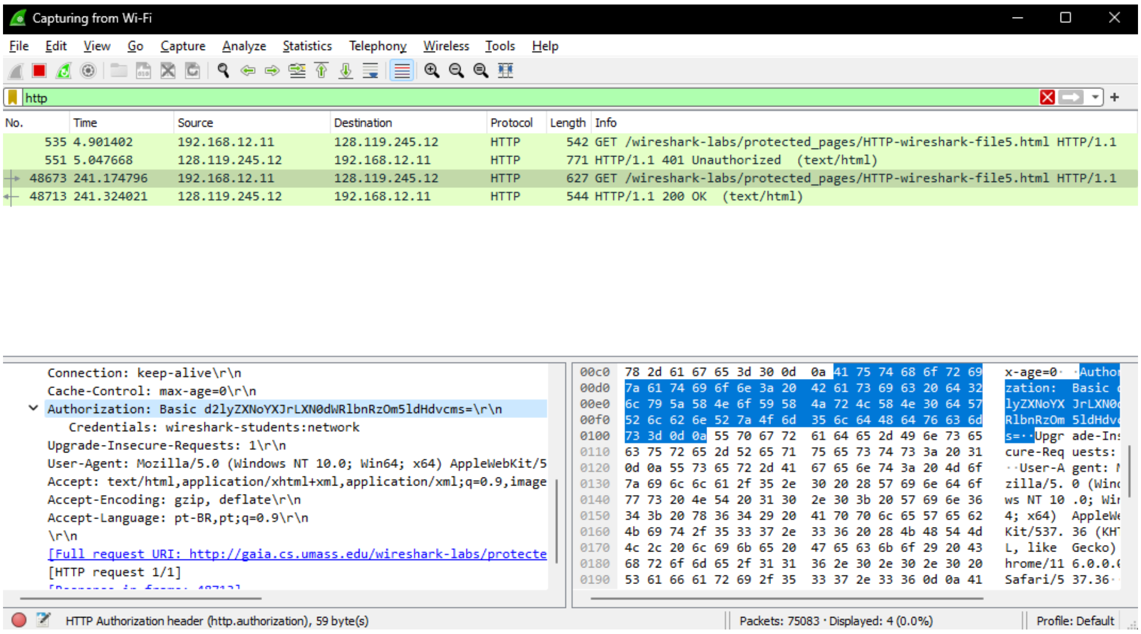
```
> Frame 551: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bi
> Ethernet II, Src: zte_3d:4c:23 (a8:02:db:3d:4c:23), Dst: IntelCor_ca:
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.12.11
> Transmission Control Protocol, Src Port: 80, Dst Port: 57976, Seq: 1,
v Hypertext Transfer Protocol
  v HTTP/1.1 401 Unauthorized\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
        [HTTP/1.1 401 Unauthorized\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 401
      [Status Code Description: Unauthorized]
      Response Phrase: Unauthorized
    Date: Fri, 25 Aug 2023 04:28:56 GMT\r\n
```

```
0030  00 ed ef b1 00 00 48 54  54 50 2f 31 2e 31 20 34   ······HT TP/1.1 4
0040  30 31 20 55 6e 61 75 74  68 6f 72 69 7a 65 64 0d   01 Unaut horize
0050  0a 44 61 74 65 3a 20 46  72 69 2c 20 32 35 20 41   ·Date: F ri, 25
0060  75 67 20 32 30 32 33 20  30 34 3a 32 38 3a 35 36   ug 2023  04:28:
0070  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver:
0080  61 63 68 65 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Ce
0090  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.
00a0  32 6b 2d 66 69 70 73 20  50 48 50 2f 37 2e 34 2e   2k-fips  PHP/7.
00b0  33 33 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   33 mod_p erl/2.
00c0  31 31 20 50 65 72 6c 2f  76 35 2e 31 36 2e 33 0d   11 Perl/ v5.16.
00d0  0a 57 57 57 2d 41 75 74  68 65 6e 74 69 63 61 74   ·WWW-Aut hentic
00e0  65 3a 20 42 61 73 69 63  20 72 65 61 6c 6d 3d 22   e: Basic  realm
00f0  77 69 72 65 73 68 61 72  6b 2d 73 74 75 64 65 6e   wireshar k-stud
0100  74 73 20 6f 6e 6c 79 22  0d 0a 43 6f 6e 74 65 6e   ts only" ··Cont
0110  74 2d 4c 65 6e 67 74 68  3a 20 33 38 31 0d 0a 4b   t-Length : 381·
0120  65 65 70 2d 41 6c 69 76  65 3a 20 74 69 6d 65 6f   eep-Aliv e: tim
0130  75 74 3d 35 2c 20 6d 61  78 3d 31 30 30 0d 0a 43   ut=5, ma x=100·
```

HTTP Response Status Code (http.response.code), 3 byte(s) | Packets: 16218 · Displayed: 2 (0.0%) | Profile: Default

19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

O HTTP GET inclui o novo campo Authorization:


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.     Time        Source          Destination     Protocol Length Info
    535 4.901402    192.168.12.11   128.119.245.12  HTTP      542 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
    551 5.047668    128.119.245.12  192.168.12.11   HTTP      771 HTTP/1.1 401 Unauthorized  (text/html)
  48673 241.174796  192.168.12.11   128.119.245.12  HTTP      627 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
  48713 241.324021  128.119.245.12  192.168.12.11   HTTP      544 HTTP/1.1 200 OK  (text/html)
```

```
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
  ⌄ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
       Credentials: wireshark-students:network
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/5
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: pt-BR,pt;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protecte
    [HTTP request 1/1]
```

```
00c0  78 2d 61 67 65 3d 30 0d  0a 41 75 74 68 6f 72 69   x-age=0· ·Author
00d0  7a 61 74 69 6f 6e 3a 20  42 61 73 69 63 20 64 32   zation:  Basic d
00e0  6c 79 5a 58 4e 6f 59 58  4a 72 4c 58 4e 30 64 57   lyZXNoYX JrLXN0d
00f0  52 6c 62 6e 52 7a 4f 6d  35 6c 64 48 64 76 63 6d   RlbnRzOm 5ldHdvc
0100  73 3d 0d 0a 55 70 67 72  61 64 65 2d 49 6e 73 65   s=··Upgr ade-Ins
0110  63 75 72 65 2d 52 65 71  75 65 73 74 73 3a 20 31   cure-Req uests: 
0120  0d 0a 55 73 65 72 2d 41  67 65 6e 74 3a 20 4d 6f   ··User-A gent: M
0130  7a 69 6c 6c 61 2f 35 2e  30 20 28 57 69 6e 64 6f   zilla/5. 0 (Wind
0140  77 73 20 4e 54 20 31 30  2e 30 3b 20 57 69 6e 36   ws NT 10 .0; Win
0150  34 3b 20 78 36 34 29 20  41 70 70 6c 65 57 65 62   4; x64)  AppleWe
0160  4b 69 74 2f 35 33 37 2e  33 36 20 28 4b 48 54 4d   Kit/537. 36 (KHT
0170  4c 2c 20 6c 69 6b 65 20  47 65 63 6b 6f 29 20 43   L, like  Gecko) 
0180  68 72 6f 6d 65 2f 31 31  36 2e 30 2e 30 2e 30 20   hrome/11 6.0.0.0
0190  53 61 66 61 72 69 2f 35  33 37 2e 33 36 0d 0a 41   Safari/5 37.36··
```

HTTP Authorization header (http.authorization), 59 byte(s)

Packets: 75083 · Displayed: 4 (0.0%)

Profile: Default