

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

O cliente está usando a versão 1.1 do protocolo HTTP.

```
> Frame 316: 551 bytes on wire (4408 bits), 551 bytes captured (4408 bits) on interface \Device\NPF_{974E1BD6-0849-479E-B9AA-4DC9F63482A4}, id 0
> Ethernet II, Src: Inventus_5f:e7:34 (a4:63:a1:5f:e7:34), Dst: Kaonmedi_00:06:8b (98:77:e7:00:06:8b)
> Internet Protocol Version 4, Src: 192.168.0.26, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 64260, Dst Port: 80, Seq: 1, Ack: 1, Len: 497
< Hypertext Transfer Protocol
  < GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.67 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: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 321]
```

O servidor também usa essa versão.

```
> Frame 321: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{974E1BD6-0849-479E-B9AA-4DC9F63482A4}, id 0
> Ethernet II, Src: Kaonmedi_00:06:8b (98:77:e7:00:06:8b), Dst: Inventus_5f:e7:34 (a4:63:a1:5f:e7:34)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.26
> Transmission Control Protocol, Src Port: 80, Dst Port: 64260, Seq: 1, Ack: 498, Len: 486
< Hypertext Transfer Protocol
  < HTTP/1.1 200 OK\r\n
    Date: Mon, 23 May 2022 12:23:25 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.28 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Mon, 23 May 2022 05:59:01 GMT\r\n
    ETag: "80-5dfa7896e6f8c"\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: 0.155094000 seconds]
```

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

As línguas aceitas são: português e inglês.

```
> Frame 316: 551 bytes on wire (4408 bits), 551 bytes captured (4408 bits) on interface \Device\NPF_{974E1BD6-0849-479E-B9AA-4DC9F63482A4}, id 0
> Ethernet II, Src: Inventus_5f:e7:34 (a4:63:a1:5f:e7:34), Dst: Kaonmedi_00:06:8b (98:77:e7:00:06:8b)
> Internet Protocol Version 4, Src: 192.168.0.26, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 64260, Dst Port: 80, Seq: 1, Ack: 1, Len: 497
< Hypertext Transfer Protocol
  < GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.67 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: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 321]
```

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

O endereço IP do computador é: 192.168.0.26

```
> Ethernet II, Src: Inventus_5f:e7:34 (a4:63:a1:5f:e7:34), Dst: Kaonmedi_00:06:8b (98:77:e7:00:06:8b)
> Internet Protocol Version 4, Src: 192.168.0.26, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 537
    Identification: 0x15ba (5562)
    > Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0xacde [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.26
    Destination Address: 128.119.245.12
> Transmission Control Protocol, Src Port: 64260, Dst Port: 80, Seq: 1, Ack: 1, Len: 497
> Hypertext Transfer Protocol
```

O endereço de gaia.cs.umass.edu server é 128.119.245.12

```
> Ethernet II, Src: Inventus_5f:e7:34 (a4:63:a1:5f:e7:34), Dst: Kaonmedi_00:06:8b (98:77:e7:00:06:8b)
> Internet Protocol Version 4, Src: 192.168.0.26, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 537
    Identification: 0x15ba (5562)
    > Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0xacde [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.26
    Destination Address: 128.119.245.12
> Transmission Control Protocol, Src Port: 64260, Dst Port: 80, Seq: 1, Ack: 1, Len: 497
> Hypertext Transfer Protocol
```

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

O código de status devolvido pelo servidor é 200.

```
> Frame 321: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{974E1BD6-0B49-479E-B9AA-4DC9F63482A4}, id 0
> Ethernet II, Src: Kaonmedi_00:06:8b (98:77:e7:00:06:8b), Dst: Inventus_5f:e7:34 (a4:63:a1:5f:e7:34)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.26
> Transmission Control Protocol, Src Port: 80, Dst Port: 64260, Seq: 1, Ack: 498, Len: 486
> Hypertext Transfer Protocol
    > HTTP/1.1 200 OK\r\n
    Date: Mon, 23 May 2022 12:23:25 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.28 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Mon, 23 May 2022 05:59:01 GMT\r\n
    ETag: "80-5dfa7896e6f8c"\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: 0.155094000 seconds]
```

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

O documento foi modificado pela última vez em 23 de maio de 2022.

```
> Frame 321: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{974E1BD6-0849-479E-B9AA-4DC9F63482A4}, id 0
> Ethernet II, Src: Kaonmedi_00:06:8b (98:77:e7:00:06:8b), Dst: Inventus_5f:e7:34 (a4:63:a1:5f:e7:34)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.26
> Transmission Control Protocol, Src Port: 80, Dst Port: 64260, Seq: 1, Ack: 498, Len: 486
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Mon, 23 May 2022 12:23:25 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.28 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Mon, 23 May 2022 05:59:01 GMT\r\n
    ETag: "80-5dfa7896e6f8c"\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: 0.155094000 seconds]
```

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

128 bytes de conteúdo estão sendo retornados para o browser.

```
> Frame 321: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{974E1BD6-0849-479E-B9AA-4DC9F63482A4}, id 0
> Ethernet II, Src: Kaonmedi_00:06:8b (98:77:e7:00:06:8b), Dst: Inventus_5f:e7:34 (a4:63:a1:5f:e7:34)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.26
> Transmission Control Protocol, Src Port: 80, Dst Port: 64260, Seq: 1, Ack: 498, Len: 486
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Mon, 23 May 2022 12:23:25 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.28 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Mon, 23 May 2022 05:59:01 GMT\r\n
    ETag: "80-5dfa7896e6f8c"\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: 0.155094000 seconds]
```

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.

Não, todos os headers são apresentados.

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 há nenhum IF-MODIFIED-SINCE no primeiro GET.

```
> Frame 76: 551 bytes on wire (4408 bits), 551 bytes captured (4408 bits) on interface \Device\NPF_{974E1BD6-0849-479E-B9AA-4DC9F63482A4}, id 0
> Ethernet II, Src: Inventus_5f:e7:34 (a4:63:a1:5f:e7:34), Dst: Kaonmedi_00:06:8b (98:77:e7:00:06:8b)
> Internet Protocol Version 4, Src: 192.168.0.26, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 64724, Dst Port: 80, Seq: 1, Ack: 1, Len: 497
▼ 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/101.0.4951.67 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: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7\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: 79]
```

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

O servidor retorna o texto do arquivo.

```
\r\n
[HTTP response 1/1]
[Time since request: 0.169049000 seconds]
[Request in frame: 76]
[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)
\r\n
<html>\r\n
\r\n
Congratulations again! Now you've downloaded the file lab2-2.html. <br>\r\n
This file's last modification date will not change. <p>\r\n
Thus if you download this multiple times on your browser, a complete copy <br>\r\n
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\r\n
field in your browser's HTTP GET request to the server.\r\n
\r\n
</html>\r\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?

Há o IF-MODIFIED-SINCE nesse request e é seguido pela data e horário da modificação.

```
> Transmission Control Protocol, Src Port: 64725, Dst Port: 80, Seq: 1, Ack: 1, Len: 609
▼ 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/101.0.4951.67 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: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7\r\n
If-None-Match: "173-5dfa7896e67bc"\r\n
If-Modified-Since: Mon, 23 May 2022 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: 140]
```

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 retorno é 304 e o servidor alerta que não houve modificação no arquivo. Portanto, o seu conteúdo não é retornado.

```
▼ 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, 23 May 2022 13:05:34 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.28 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: "173-5dfa7896e67bc"\r\n
      \r\n
      [HTTP response 1/1]
      [Time since request: 0.151629000 seconds]
      [Request in frame: 138]
      [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 enviado 1 HTTP GET request message. E o pacote com a mensagem GET é o 53.

No.	Time	Source	Destination	Protocol	Length	Info
53	7.005825	192.168.0.26	128.119.245.12	HTTP	551	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
58	7.164088	128.119.245.12	192.168.0.26	HTTP	535	HTTP/1.1 200 OK (text/html)

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

O pacote com a resposta para o HTTP GET request é o 58.

```
No.    Time    Source        Destination    Protocol  Length  Info
--
53 7.005825 192.168.0.26  128.119.245.12 HTTP      551    GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
58 7.164088 128.119.245.12 192.168.0.26  HTTP      535    HTTP/1.1 200 OK (text/html)

> Frame 58: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{974E1BD6-0849-479E-B9AA-4DC9F63482A4}, id 0
> Ethernet II, Src: Kaonmedi_00:06:8b (98:77:e7:00:06:8b), Dst: Inventus_5f:e7:34 (a4:63:a1:5f:e7:34)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.26
> Transmission Control Protocol, Src Port: 80, Dst Port: 64898, Seq: 4381, Ack: 498, Len: 481
> [2 Reassembled TCP Segments (4861 bytes): #57(4380), #58(481)]
▼ 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: Mon, 23 May 2022 13:33:14 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.28 mod_perl/2.0.11 Perl/v5.16.3\r\n
      Last-Modified: Mon, 23 May 2022 05:59:01 GMT\r\n
```

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

O status é 200 e a resposta OK.

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

Foram necessários dois segmentos TCP.

No.	Time	Source	Destination	Protocol	Length	Info
53	7.005825	192.168.0.26	128.119.245.12	HTTP	551	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
58	7.164088	128.119.245.12	192.168.0.26	HTTP	535	HTTP/1.1 200 OK (text/html)

> Frame 58: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{974E18D6-0849-479E-B9AA-4DC9F63482A4}, id 0
 > Ethernet II, Src: Kaonmedi_00:06:8b (98:77:e7:00:06:8b), Dst: Inventus_5f:e7:34 (a4:63:a1:5f:e7:34)
 > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.26
 > Transmission Control Protocol, Src Port: 80, Dst Port: 64898, Seq: 4381, Ack: 498, Len: 481
 > [2 Reassembled TCP Segments (4861 bytes): #57(4380), #58(481)]
 [Frame: 57, payload: 0-4379 (4380 bytes)]
 [Frame: 58, payload: 4380-4860 (481 bytes)]
 [Segment count: 2]
 [Reassembled TCP length: 4861]
 [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a204d6f6e2c203233204d61792032_-]
 > Hypertext Transfer Protocol
 > Line-based text data: text/html (98 lines)

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

Foram enviadas 3 HTTP GET request message. O pacote 255 foi enviado para o endereço 128.119.245.12. O pacote 261 foi enviado para o endereço 128.119.245.12. E o pacote 280 foi enviado para o endereço 178.79.137.164.

No.	Time	Source	Destination	Protocol	Length	Info
255	43.140962	192.168.0.26	128.119.245.12	HTTP	551	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
260	43.296426	128.119.245.12	192.168.0.26	HTTP	1355	HTTP/1.1 200 OK (text/html)
261	43.316880	192.168.0.26	128.119.245.12	HTTP	497	GET /pearson.png HTTP/1.1
267	43.472263	128.119.245.12	192.168.0.26	HTTP	745	HTTP/1.1 200 OK (PNG)
280	44.165613	192.168.0.26	178.79.137.164	HTTP	464	GET /8E_cover_small.jpg HTTP/1.1
284	44.449036	178.79.137.164	192.168.0.26	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.

Paralelo. Observa-se que o request para as imagens foram feitos pelos pacotes 261 e 280, enquanto que a resposta 200 OK está no pacote 255. Portanto, a solicitação pelas imagens foi feita depois da do pacote 255.

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

O primeiro HTTP GET request está no pacote 32 e sua resposta está no 35 com o código 401 Unathorized.

No.	Time	Source	Destination	Protocol	Length	Info
32	2.181733	192.168.0.26	128.119.245.12	HTTP	567	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
35	2.356543	128.119.245.12	192.168.0.26	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
208	25.752568	192.168.0.26	128.119.245.12	HTTP	652	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
212	25.919155	128.119.245.12	192.168.0.26	HTTP	544	HTTP/1.1 200 OK (text/html)

> Frame 35: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{974E1BD6-0849-479E-B9AA-4DC9F63482A4}, id 0

> Ethernet II, Src: Kaonmedi_00:06:8b (98:77:e7:00:06:8b), Dst: Inventus_Sf:e7:34 (a4:63:a1:5f:e7:34)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.26

> Transmission Control Protocol, Src Port: 80, Dst Port: 65375, Seq: 1, Ack: 514, Len: 717

▼ Hypertext Transfer Protocol

> HTTP/1.1 401 Unauthorized\r\n

Date: Mon, 23 May 2022 14:36:46 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.28 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

[Content length: 381]

Keep-Alive: timeout=5, max=100\r\n

Connection: Keep-Alive\r\n

Content-Type: text/html; charset=iso-8859-1\r\n

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

É inserido o campo Authorization: Basic ...

No.	Time	Source	Destination	Protocol	Length	Info
32	2.181733	192.168.0.26	128.119.245.12	HTTP	567	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
35	2.356543	128.119.245.12	192.168.0.26	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
208	25.752568	192.168.0.26	128.119.245.12	HTTP	652	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
212	25.919155	128.119.245.12	192.168.0.26	HTTP	544	HTTP/1.1 200 OK (text/html)

> Frame 208: 652 bytes on wire (5216 bits), 652 bytes captured (5216 bits) on interface \Device\NPF_{974E1BD6-0849-479E-B9AA-4DC9F63482A4}, id 0

> Ethernet II, Src: Inventus_Sf:e7:34 (a4:63:a1:5f:e7:34), Dst: Kaonmedi_00:06:8b (98:77:e7:00:06:8b)

> Internet Protocol Version 4, Src: 192.168.0.26, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 65376, Dst Port: 80, Seq: 1, Ack: 1, Len: 598

▼ 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 d2lyZXNoYXJrLXN0dWRLbnRzOm5ldHdvcm0=\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) Chrome/101.0.4951.67 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