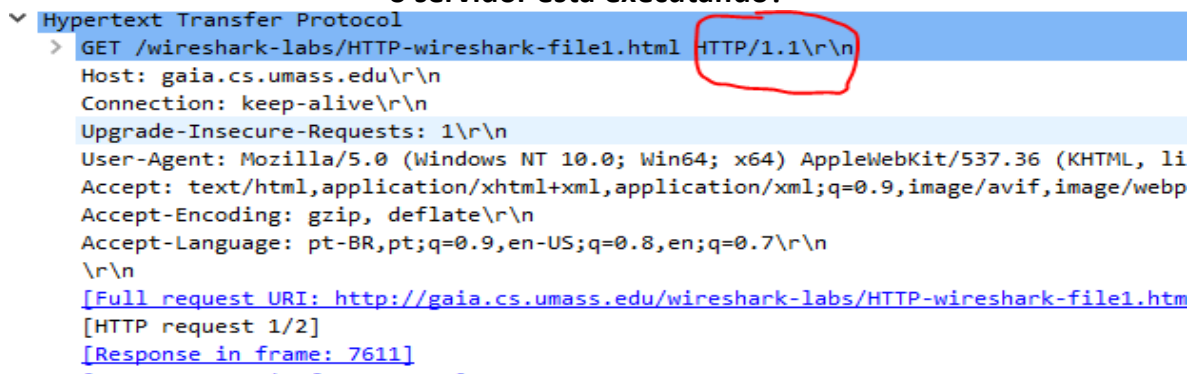


Atividade 3

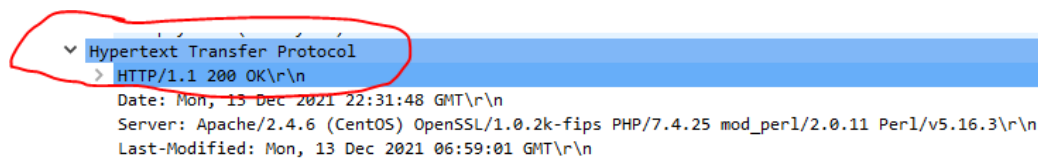
Protocolo HTTP

1. Seu navegador está executando HTTP versão 1.0, 1.1, 2 ou 3? Qual versão de HTTP o servidor está executando?



```
▼ 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, li
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
    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.htm
    [HTTP request 1/2]
    [Response in frame: 7611]
```

Figura 1: Versão HTTP

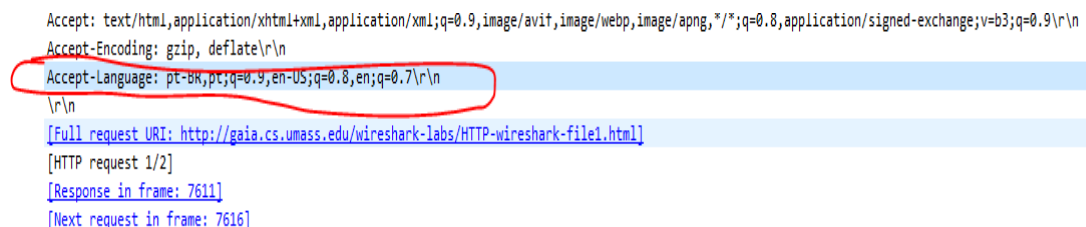


```
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Mon, 13 Dec 2021 22:31:48 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Mon, 13 Dec 2021 06:59:01 GMT\r\n
```

Figura 2: Versão HTTP servidor

R = Meu navegador está executando HTTP versão 1.1 e o do servidor está executando na 1.1 também.

2. Quais idiomas (se houver) seu navegador indica que pode aceitar para o servidor?

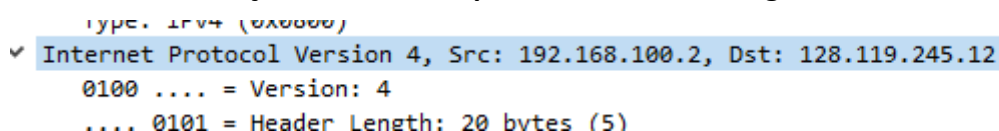


```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: pt-br,pt;q=0.9,en-US;q=0.8,en;q=0.7\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
[HTTP request 1/2]
[Response in frame: 7611]
[Next request in frame: 7616]
```

Figura 3: Idiomas

R = Português brasileiro (pt-br), português (pt), inglês americano (en-US) e inglês (en).

3. Qual é o endereço IP do seu computador? Do servidor gaia.cs.umass.edu?



```
type: IPv4 (0x00000000)
▼ Internet Protocol Version 4, Src: 192.168.100.2, Dst: 128.119.245.12
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
```

Figura 4: Endereço IP do meu computador e do servidor

R = O endereço IP do meu computador é 192.168.100.2 e o do servidor gaia.cs.umass.edu é 128.119.245.12

4. Qual é o código de status retornado do servidor para o seu navegador?

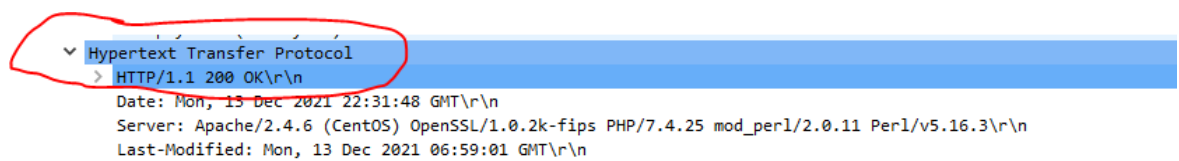


Figura 5: Código Status

R = Código 200 Ok, que foi bem sucedido a requisição.

5. Quando o arquivo HTML que você está recuperando foi modificado pela última vez no servidor?

Last-Modified: Mon, 13 Dec 2021 06:59:01 GMT\r\n

Figura 6: Last Modified

R = Foi modificado 13/12/2021 às 06:59.

6. Quantos bytes de conteúdo estão sendo retornados ao seu navegador?

```
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: 0.160927000 seconds]
[Request in frame: 7597]
[Next request in frame: 7616]
[Next response in frame: 7638]
```

Figura 7: Bytes de Conteúdo

R = 128 bytes de conteúdo.

7. Ao inspecionar os dados brutos na janela de conteúdo do pacote, você vê algum cabeçalho nos dados que não são exibidos na janela de listagem de pacotes? Se sim, escreva um.

R = Não há.

Congratulations again! Now you've downloaded the file lab2-2.html.
This file's last modification date will not change.

Thus if you download this multiple times on your browser, a complete copy
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE
field in your browser's HTTP GET request to the server.

Figura 8: Limpando cache, abrindo Wireshark e acessando site denovo igual o tutorial.

No.	Time	Source	Destination	Protocol	Length	Info
2119	20:25:19,207647	192.168.100.2	128.119.245.12	HTTP	550	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2124	20:25:19,369533	128.119.245.12	192.168.100.2	HTTP	784	HTTP/1.1 200 OK (text/html)
2321	20:26:59,988856	192.168.100.2	128.119.245.12	HTTP	662	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2324	20:27:00,155542	128.119.245.12	192.168.100.2	HTTP	294	HTTP/1.1 304 Not Modified
2337	20:27:02,542288	192.168.100.2	128.119.245.12	HTTP	662	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2338	20:27:02,709161	128.119.245.12	192.168.100.2	HTTP	293	HTTP/1.1 304 Not Modified
2340	20:27:03,722184	192.168.100.2	128.119.245.12	HTTP	662	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2341	20:27:03,888740	128.119.245.12	192.168.100.2	HTTP	293	HTTP/1.1 304 Not Modified

Figura 9: Refresh no site gaia e stop no Wireshark e filtro no http.

8. Inspeção o conteúdo da primeira solicitação HTTP GET de seu navegador para o servidor. Você vê uma linha "IF-MODIFIED-SINCE" no HTTP GET?

```
▼ 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/96.0.4664.93 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: 2124]
```

Figura 10: Resultado

R = Não há a linha IF-MODIFIED-SINCE.

9. Inspeção o conteúdo da resposta do servidor. O servidor retornou explicitamente o conteúdo do arquivo? Como você sabe?

```
✓ 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
  \n
  01a0 74 6d 6c 3e 0a 0a 43 6f 6e 67 72 61 74 75 6c 61 tml>..Co ngratula
  01b0 74 69 6f 6e 73 20 61 67 61 69 6e 21 20 20 4e 6f tions ag ain! No
  01c0 77 20 79 6f 75 27 76 65 20 64 6f 77 6e 6c 6f 61 w you've downloa
  01d0 64 65 64 20 74 68 65 20 66 69 6c 65 20 6c 61 62 ded the file lab
  01e0 32 2d 32 2e 68 74 6d 6c 2e 20 3c 62 72 3e 0a 54 2-2.html . <br>T
  01f0 68 69 73 20 66 69 6c 65 27 73 20 6c 61 73 74 20 his file 's last
  0200 6d 6f 64 69 66 69 63 61 74 69 6f 6e 20 64 61 74 modifica tion dat
  0210 65 20 77 69 6c 6c 20 6e 6f 74 20 63 68 61 6e 67 e will n ot chang
  0220 65 2e 20 20 3c 70 3e 0a 54 68 75 73 20 20 69 66 e. <p>.. Thus if
```

Figura 11: Resposta do servidor

R = Sim, foi retornado corretamente o acesso ao site gaia pelo texto da mensagem e também código 200 de ok, content header diferente de 0 o que significa que o conteúdo foi devolvido.

10. Agora inspeção o conteúdo da segunda solicitação HTTP GET de seu navegador para o servidor. Você vê uma linha "IF-MODIFIED-SINCE:" no HTTP GET? Em caso afirmativo, quais informações seguem o cabeçalho "IF-MODIFIED-SINCE:"?

```
If-None-Match: "173-5d3019b90653e"\r\n
If-Modified-Since: Mon, 13 Dec 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 1/3]
[Response in frame: 2324]
[Next request in frame: 2337]
  ac 75 1d f7 6a 0c 74 27 ea 72 c0 2f 08 00 45 00 .u..j..t' ..r/..E-
  02 88 3b 91 40 00 80 06 22 b0 c0 a8 64 02 80 77 ..;.@... "...d..w
  f5 0c ff d3 00 50 a3 b7 a4 0b 1a 65 fc 35 50 18 ....P... ..e.SP-
  04 01 1d a8 00 00 47 45 54 20 2f 77 69 72 65 73 .....GE T /wires
  68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-lab s/HTTP-w
  69 72 65 73 68 61 72 6b 2d 66 69 6c 65 32 2e 68 ireshark -file2.h
  74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1..Ho
  73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 st: gaia .cs.umas
  73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f s.edu..C onnectio
```

Figura 12: IF-MODIFIED-SINCE

R = Sim, contém a informação do dia e horário, 13/12/2021 às 06:59, Segunda Feira.

11. Qual é o código de status HTTP e a frase retornada do servidor em resposta a este segundo HTTP GET? O servidor retornou explicitamente o conteúdo do arquivo? Explique.

2321	20:26:59,988856	192.168.100.2	128.119.245.12	HTTP	662	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2324	20:27:00,155542	128.119.245.12	192.168.100.2	HTTP	294	HTTP/1.1 304 Not Modified

Figura 13: Mensagem retornada segundo HTTP GET

```

Hypertext Transfer Protocol
> HTTP/1.1 304 Not Modified\r\n
  Date: Mon, 13 Dec 2021 23:26:59 GMT\r\n

```

Figura 14: Mensagem Not Modified código 304

```

Date: Mon, 13 Dec 2021 23:26:59 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 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: "173-5d3019b90653e"\r\n
\r\n
[HTTP response 1/3]
[Time since request: 0.166686000 seconds]
[Request in frame: 2321]
[Next request in frame: 2337]
[Next response in frame: 2338]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

```

Figura 15: Infos da mensagem

R = Código 304 e a mensagem é a Not Modified. Não há a linha de content length e não há conteúdo, o texto não foi retornado pela mensagem HTTP e isso pode ser observado pela quebra de linha \r\n, sendo assim, o servidor não retornou arquivo, a requisição o navegador obteve pelo cache.

Executando parte 3 do tutorial.

THE BILL OF RIGHTS
Amendments 1-10 of the Constitution

The Conventions of a number of the States having, at the time of adopting the Constitution, expressed a desire, in order to prevent misconstruction or abuse of its powers, that further declaratory and restrictive clauses should be added, and as extending the ground of public confidence in the Government will best insure the beneficent ends of its institution;

Resolved, by the Senate and House of Representatives of the United States of America, in Congress assembled, two-thirds of both Houses concurring, that the following articles be proposed to the Legislatures of the several States, as amendments to the Constitution of the United States; all or any of which articles, when ratified by three-fourths of the said Legislatures, to be valid to all intents and purposes as part of the said Constitution, namely:

Amendment I

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

Amendment II

A well regulated militia, being necessary to the security of a free state, the right of the people to keep and bear arms, shall not be infringed.

Amendment III

No soldier shall, in time of peace be quartered in any house, without the consent of the owner, nor in time of war, but in a manner to be prescribed by law.

Amendment IV

Figura 16: Execução parte 3

No.	Time	Source	Destination	Protocol	Length	Info
23	21:01:26,157400	192.168.100.2	128.119.245.12	HTTP	550	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
32	21:01:26,315835	128.119.245.12	192.168.100.2	HTTP	679	HTTP/1.1 200 OK (text/html)

> Frame 32: 679 bytes on wire (5432 bits), 679 bytes captured (5432 bits) on interface \Device\NPF_{00EA2AF1-DFF6-4FB3-9DF2-FE83EEC0FAB7}, id 0
 > Ethernet II, Src: HuaweiTe_f7:6a:0c (ac:75:1d:f7:6a:0c), Dst: Elitegro_72:c0:2f (74:27:ea:72:c0:2f)
 > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.100.2
 > Transmission Control Protocol, Src Port: 80, Dst Port: 49979, Seq: 4237, Ack: 497, Len: 625
 > [4 Reassembled TCP Segments (4861 bytes): #28(1412), #29(1412), #30(1412), #32(625)]
 > Hypertext Transfer Protocol
 > Line-based text data: text/html (98 lines)

0000	74 27 ea 72 c0 2f ac 75 1d f7 6a 0c 08 00 45 00	t'r /u ··j··E·
0010	02 99 74 bd 40 00 2c 06 3d 73 80 77 f5 0c c0 a8	·t @, · =s w···
0020	64 02 00 50 c3 3b f1 d1 fa fa c8 7f 2c b9 50 18	d·P ; ······P·
0030	00 ed 9a 46 00 00 67 3e 3c 68 33 3e 41 6d 65 6e	···F·g> <h3>Amen
0040	64 6d 65 6e 74 20 56 49 49 49 3c 2f 68 33 3e 3c	dment VI II</h3><
0050	2f 73 74 72 6f 6e 67 3e 3c 2f 61 3e 0a 0a 3c 70	/strong> ··<p
0060	3e 3c 2f 70 3e 3c 70 3e 45 78 63 65 73 73 69 76	></p><p> Excessiv
0070	65 20 62 61 69 6c 20 73 68 61 6c 6c 20 6e 6f 74	e bail s hall not

Figura 17: Execução parte 3, file3 do site gaia

12. Quantas mensagens de solicitação HTTP GET seu navegador enviou? Qual número de pacote no rastreamento contém a mensagem GET para a Declaração de Direitos (Bill of Rights)?

R = 1 mensagem de solicitação HTTP GET. O número do pacote correspondente a mensagem GET é o 23 como na figura 17 acima.

13. Qual número de pacote no rastreamento contém o código de status e a frase associada à resposta à solicitação HTTP GET?

R = Número 32 do pacote, como na figura 17 anteriormente.

14. Qual é o código de status e a frase na resposta?

```

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: Tue, 14 Dec 2021 00:01:25 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Mon, 13 Dec 2021 06:59:01 GMT\r\n
    ETag: "1194-5d3019b90171d"\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
  
```

Figura 18: Código e frase.

R = Código 200 de status e a frase é "OK".

15. Quantos segmentos TCP contendo dados foram necessários para transportar a única resposta HTTP e o texto da Declaração de Direitos?

```

[4 Reassembled TCP Segments (4861 bytes): #28(1412), #29(1412), #30(1412), #32(625)]
  [Frame: 28, payload: 0-1411 (1412 bytes)]
  [Frame: 29, payload: 1412-2823 (1412 bytes)]
  [Frame: 30, payload: 2824-4235 (1412 bytes)]
  [Frame: 32, payload: 4236-4860 (625 bytes)]
  [Segment count: 4]
  [Reassembled TCP length: 4861]
  [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a205475652c203134204465632032...]
  
```

Figura 19: Código e frase.

R = 4 segmentos TCP foram necessários para transportar, frames 28, 29, 30 e 32.

Limpado cache, aberto wireshark e aberto site do file 4.html conforme o roteiro 4.

o.	Time	Source	Destination	Protocol	Length	Info
34	22:37:30,452211	192.168.100.2	128.119.245.12	HTTP	550	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
40	22:37:30,608713	128.119.245.12	192.168.100.2	HTTP	1355	HTTP/1.1 200 OK (text/html)
41	22:37:30,637316	192.168.100.2	128.119.245.12	HTTP	496	GET /pearson.png HTTP/1.1
47	22:37:30,792543	128.119.245.12	192.168.100.2	HTTP	841	HTTP/1.1 200 OK (PNG)
55	22:37:31,456947	192.168.100.2	178.79.137.164	HTTP	463	GET /8E_cover_small.jpg HTTP/1.1
59	22:37:31,675784	178.79.137.164	192.168.100.2	HTTP	225	HTTP/1.1 301 Moved Permanently

Frame 34: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits) on interface \Device\NPF_{0DEA2AF1-DFF6-4FB3-9DF2-FE83EEC0FAB7}, id		
Ethernet II, Src: Elitegro_72:c0:2f (74:27:ea:72:c0:2f), Dst: HuaweiTe_f7:6a:0c (ac:75:1d:f7:6a:0c)		
Internet Protocol Version 4, Src: 192.168.100.2, Dst: 128.119.245.12		
Transmission Control Protocol, Src Port: 51046, Dst Port: 80, Seq: 1, Ack: 1, Len: 496		
Hypertext Transfer Protocol		

000	ac 75 1d f7 6a 0c 74 27	ea 72 c0 2f 08 00 45 00	..u..j..t'..r../..E..
010	02 18 3b ab 40 00 80 06	23 06 c0 a8 64 02 80 77	..;@...#...d..w..
020	f5 0c c7 66 00 50 48 91	1b f3 36 bf 8f 3e 50 18	...f..PH...6...>P..
030	04 01 49 9f 00 00 47 45	54 20 2f 77 69 72 65 73	...I...GE T /wires
040	68 61 72 6b 2d 6c 61 62	73 2f 48 54 54 50 2d 77	hark-lab s/HTTP-w
050	69 72 65 73 68 61 72 6b	2d 66 69 6c 65 34 2e 68	reshark -file4.h
060	74 6d 6d 20 48 54 54 50	2f 31 2e 31 0d 0a 48 6f	tml HTTP /1.1..Ho
070	73 74 3a 20 67 61 69 61	2e 63 73 2e 75 6d 61 73	st: gaia .cs.umas
080	73 2e 65 64 75 0d 0a 43	6f 6e 6e 65 63 74 69 6f	s.edu..C onnectio

Figura 20: Execução file 4 do site gaia

16. Quantas mensagens de solicitação HTTP GET seu navegador enviou? Para quais endereços de Internet essas solicitações GET foram enviadas?

R = 3 mensagens de solicitação HTTP GET conforme a imagem 20 acima. Os endereços foram: primeira mensagem get do pacote número 34 para o endereço 128.119.245.12, segunda mensagem get do pacote número 41 para o endereço 128.119.245.12 e a terceira mensagem get do pacote número 55 para o endereço 178.79.137.164

17. Você pode dizer se o seu navegador baixou as duas imagens em série ou se elas foram baixadas dos dois sites em paralelo? Explique.

R = As imagens foram baixadas em série, o primeiro get ocorre no pacote 41 e o OK no 47 e a segunda imagem começa no 55 o get ou seja a primeira termina antes da segunda ser requisitada.

This page is password protected! If you're seeing this, you've downloaded the page correctly
Congratulations!

Figura 21: Execução file 5 do site gaia após digitar senha e usuário.

No.	Time	Source	Destination	Protocol	Length	Info
20	23:03:39,071388	192.168.100.2	128.119.245.12	HTTP	566	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
22	23:03:39,228899	128.119.245.12	192.168.100.2	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
49	23:03:56,264293	192.168.100.2	128.119.245.12	HTTP	651	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
53	23:03:56,422079	128.119.245.12	192.168.100.2	HTTP	544	HTTP/1.1 200 OK (text/html)
55	23:03:57,050945	192.168.100.2	128.119.245.12	HTTP	512	GET /favicon.ico HTTP/1.1
56	23:03:57,207622	128.119.245.12	192.168.100.2	HTTP	538	HTTP/1.1 404 Not Found (text/html)
1...	23:04:29,438852	192.168.100.2	72.246.130.58	HTTP	281	GET / HTTP/1.1
1...	23:04:29,451316	72.246.130.58	192.168.100.2	HTTP	317	HTTP/1.1 304 Not Modified
1...	23:04:29,487225	192.168.100.2	8.241.239.254	HTTP	335	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?ed937f87709aece4 HTTP/1.1
1...	23:04:29,506539	8.241.239.254	192.168.100.2	HTTP	391	HTTP/1.1 304 Not Modified

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/96.0.4664.93 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/protected_pages/HTTP-wireshark-file5.html]	
[HTTP request 1/1]	
[Response in frame: 22]	
0000	ac 75 1d f7 6a 0c 74 27 ea 72 c0 2f 08 00 45 00
0010	02 28 3b bb 40 00 80 06 22 e6 c0 a8 64 02 80 77
0020	f5 0c c9 61 00 50 fd 53 15 ce d1 f3 34 71 50 18
0030	04 01 ef 88 00 00 47 45 54 20 2f 77 69 72 65 73

Figura 22: Stop no Wireshark após acesso do file 5 do site gaia, que era protegido com senha e usuário. Foi digitado conforme o passo a passo da seção 5

18. Qual é a resposta do servidor (código de status e frase) em resposta à mensagem HTTP GET inicial do seu navegador?

TCP payload (/1/ bytes)	
Hypertext Transfer Protocol	
HTTP/1.1 401 Unauthorized\r\n	
Date: Tue, 14 Dec 2021 02:03:38 GMT\r\n	
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 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	
0000	74 27 ea 72 c0 2f ac 75 1d f7 6a 0c 08 00 45 00
0010	02 f5 b6 a2 40 00 2e 06 f9 31 80 77 f5 0c c0 a8
0020	64 02 00 50 c9 61 d1 f3 34 71 fd 53 17 ce 50 18
0030	00 ed 8d 01 00 00 48 54 54 50 2f 31 2e 31 20 34

Figura 23: Código de status e frase

R = O código de status foi o 401 e a mensagem foi “Unauthorized”, não autorizado.

19. Quando o seu navegador envia a mensagem HTTP GET pela segunda vez, qual novo campo é incluído na mensagem HTTP GET?

No.	Time	Source	Destination	Protocol	Length	Info
20	23:03:39,071388	192.168.100.2	128.119.245.12	HTTP	566	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
22	23:03:39,228899	128.119.245.12	192.168.100.2	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
49	23:03:56,264293	192.168.100.2	128.119.245.12	HTTP	651	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
53	23:03:56,422079	128.119.245.12	192.168.100.2	HTTP	544	HTTP/1.1 200 OK (text/html)
55	23:03:57,050945	192.168.100.2	128.119.245.12	HTTP	512	GET /favicon.ico HTTP/1.1
56	23:03:57,207622	128.119.245.12	192.168.100.2	HTTP	538	HTTP/1.1 404 Not Found (text/html)
1...	23:04:29,438852	192.168.100.2	72.246.130.58	HTTP	281	GET / HTTP/1.1
1...	23:04:29,451316	72.246.130.58	192.168.100.2	HTTP	317	HTTP/1.1 304 Not Modified
1...	23:04:29,487225	192.168.100.2	8.241.239.254	HTTP	335	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?ed937f87709aece4 HTTP/1.1
1...	23:04:29,506539	8.241.239.254	192.168.100.2	HTTP	391	HTTP/1.1 304 Not Modified

Transmission Control Protocol, Src Port: 51554, Dst Port: 80, Seq: 1, Ack: 1, Len: 597	
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 d2lyZXNoYXJrLXN0dWRIbnRzM05ldHdvcm0=\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/96.0.4664.93 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	
\r\n	
0000	ac 75 1d f7 6a 0c 74 27 ea 72 c0 2f 08 00 45 00
0010	02 7d 3b c0 40 00 80 06 22 8c c0 a8 64 02 80 77
0020	f5 0c c9 62 00 50 51 e7 12 86 41 1a 01 49 50 18
0030	04 01 29 cf 00 00 47 45 54 20 2f 77 69 72 65 73

Figura 24: segunda mensagem GET campos credenciais e authorization

R = É incluído o campo “Authorization”, autorização, Basic
d2lyZXnoYXJrLXN0dWRlbnRzOm5ldHdvcm5=\r\n e o campo Credentials: wireshark-
students: network. Esse campo foi o usuário e senha informado no acesso ao site gaia.