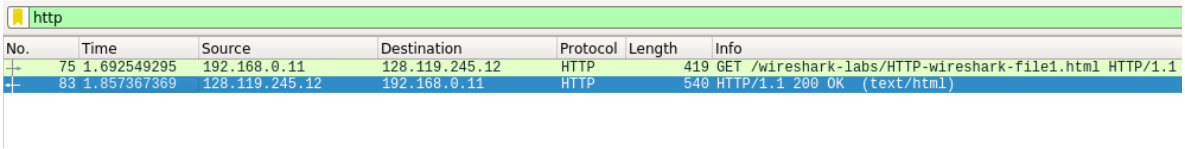
Wireshark Lab: HTTP

Nome: Vinícius Gonzaga Rocha
Matrícula: 11511BCC019
Descrição: Atividade realizada para o aprofundamento do conhecimento do protocolo HTTP. Foram desenvolvidas 5 partes, cada uma com um foco diferente. Cada seção representa uma parte e dentro de cada uma existem capturas de telas para as respostas da questões levantadas nas seções. Nem todo o conteúdo exibido na tela do Wireshark foi documentado, apenas o conteúdo pertinente as respostas.

---

1. The Basic HTTP GET/response interaction

Mensagens capturadas:



GET:

```
▼ 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]
        [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:61.0) Gecko/20100101 Firefox/61.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-GB,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\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: 83]
```

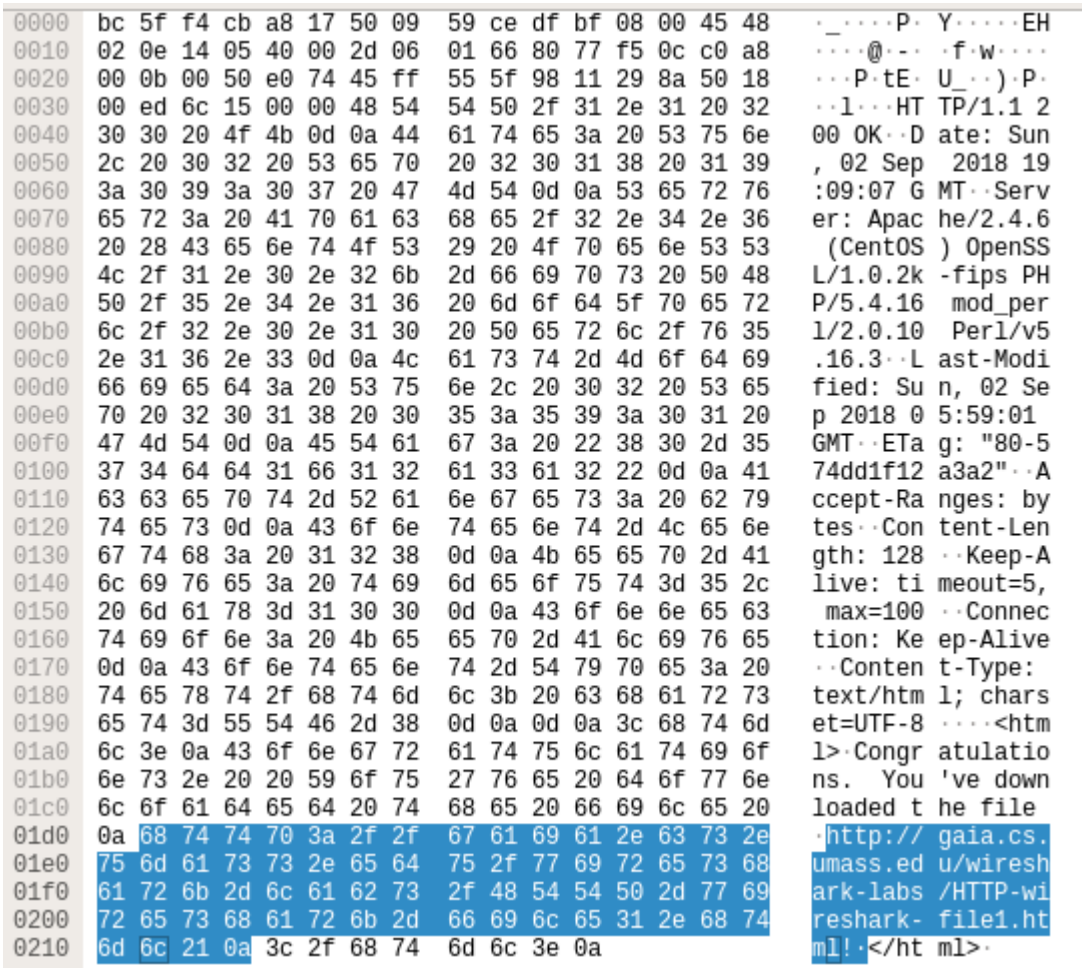
Response:

```
▼ 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: Sun, 02 Sep 2018 19:09:07 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Sun, 02 Sep 2018 05:59:01 GMT\r\n
    ETag: "80-574dd1f12a3a2"\r\n
    Accept-Ranges: bytes\r\n
  ▼ Content-Length: 128\r\n
      [Content length: 128]
    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: 0.164818074 seconds]
    [Request in frame: 75]
    File Data: 128 bytes
▼ Line-based text data: text/html (4 lines)
    <html>\n
    Congratulations.  You've downloaded the file \n
    http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
    </html>\n
```

Packet Content (GET):

```
0000  50 09 59 ce df bf bc 5f  f4 cb a8 17 08 00 45 00   P·Y····_ ·····E·
0010  01 95 39 7a 40 00 40 06  c9 b1 c0 a8 00 0b 80 77   ··9z@·@· ·······w
0020  f5 0c e0 74 00 50 98 11  28 1d 45 ff 55 5f 50 18   ···t·P·· (·E·U_P·
0030  00 e5 16 29 00 00 47 45  54 20 2f 77 69 72 65 73   ···)··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 55  73 65 72 2d 41 67 65 6e   s.edu··U ser-Agen
0090  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
00a0  58 31 31 3b 20 55 62 75  6e 74 75 3b 20 4c 69 6e   X11; Ubu ntu; Lin
00b0  75 78 20 78 38 36 5f 36  34 3b 20 72 76 3a 36 31   ux x86_6 4; rv:61
00c0  2e 30 29 20 47 65 63 6b  6f 2f 32 30 31 30 30 31   .0) Geck o/201001
00d0  30 31 20 46 69 72 65 66  6f 78 2f 36 31 2e 30 0d   01 Firef ox/61.0·
00e0  0a 41 63 63 65 70 74 3a  20 74 65 78 74 2f 68 74   ·Accept:  text/ht
00f0  6d 6c 2c 61 70 70 6c 69  63 61 74 69 6f 6e 2f 78   ml,appli cation/x
0100  68 74 6d 6c 2b 78 6d 6c  2c 61 70 70 6c 69 63 61   html+xml ,applica
0110  74 69 6f 6e 2f 78 6d 6c  3b 71 3d 30 2e 39 2c 2a   tion/xml ;q=0.9,*
0120  2f 2a 3b 71 3d 30 2e 38  0d 0a 41 63 63 65 70 74   /*;q=0.8 ··Accept
0130  2d 4c 61 6e 67 75 61 67  65 3a 20 65 6e 2d 47 42   -Languag e: en-GB
0140  2c 65 6e 3b 71 3d 30 2e  35 0d 0a 41 63 63 65 70   ,en;q=0. 5··Accep
0150  74 2d 45 6e 63 6f 64 69  6e 67 3a 20 67 7a 69 70   t-Encodi ng: gzip
0160  2c 20 64 65 66 6c 61 74  65 0d 0a 43 6f 6e 6e 65   , deflat e··Conne
0170  63 74 69 6f 6e 3a 20 6b  65 65 70 2d 61 6c 69 76   ction: k eep-aliv
0180  65 0d 0a 55 70 67 72 61  64 65 2d 49 6e 73 65 63   e··Upgra de-Insec
0190  75 72 65 2d 52 65 71 75  65 73 74 73 3a 20 31 0d   ure-Requ ests: 1·
01a0  0a 0d 0a                                          ···
```

Packet Content (Response):



```
0000  bc 5f f4 cb a8 17 50 09  59 ce df bf 08 00 45 48   ·_····P· Y·····EH
0010  02 0e 14 05 40 00 2d 06  01 66 80 77 f5 0c c0 a8   ····@·-· ·f·w····
0020  00 0b 00 50 e0 74 45 ff  55 5f 98 11 29 8a 50 18   ···P·tE· U_··)·P·
0030  00 ed 6c 15 00 00 48 54  54 50 2f 31 2e 31 20 32   ··l···HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 53 75 6e   00 OK··D ate: Sun
0050  2c 20 30 32 20 53 65 70  20 32 30 31 38 20 31 39   , 02 Sep  2018 19
0060  3a 30 39 3a 30 37 20 47  4d 54 0d 0a 53 65 72 76   :09:07 G MT··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 35 2e 34 2e 31 36  20 6d 6f 64 5f 70 65 72   P/5.4.16  mod_per
00b0  6c 2f 32 2e 30 2e 31 30  20 50 65 72 6c 2f 76 35   l/2.0.10  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 53 75  6e 2c 20 30 32 20 53 65   fied: Su n, 02 Se
00e0  70 20 32 30 31 38 20 30  35 3a 35 39 3a 30 31 20   p 2018 0 5:59:01
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 38 30 2d 35   GMT··ETa g: "80-5
0100  37 34 64 64 31 66 31 32  61 33 61 32 22 0d 0a 41   74dd1f12 a3a2"··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 tent-Len
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   ··Conten t-Type:
0180  74 65 78 74 2f 68 74 6d  6c 3b 20 63 68 61 72 73   text/htm l; chars
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>·Congr atulatio
01b0  6e 73 2e 20 20 59 6f 75  27 76 65 20 64 6f 77 6e   ns.  You 've down
01c0  6c 6f 61 64 65 64 20 74  68 65 20 66 69 6c 65 20   loaded t he file
01d0  0a 68 74 74 70 3a 2f 2f  67 61 69 61 2e 63 73 2e   ·http:// gaia.cs.
01e0  75 6d 61 73 73 2e 65 64  75 2f 77 69 72 65 73 68   umass.ed u/wiresh
01f0  61 72 6b 2d 6c 61 62 73  2f 48 54 54 50 2d 77 69   ark-labs /HTTP-wi
0200  72 65 73 68 61 72 6b 2d  66 69 6c 65 31 2e 68 74   reshark- file1.ht
0210  6d 6c 21 0a 3c 2f 68 74  6d 6c 3e 0a               ml!·</ht ml>·
```

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

Tanto o browser cliente quanto o servidor rodam a versão 1.1 do protocolo. Isso pode ser verificado nos itens Request Version e Response Version.

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

En-GB é aceito, conforme o item Accept-Language.

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

Conforme as colunas Source e Destination:

- Minha máquina: 192.168.0.11

- Servidor: 128.119.245.12

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

200 Ok, conforme o item Status Code.

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

Em 2 de Setembro de 2018 às 05:59:01, conforme o item Last-Modified.

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

128 bytes, conforme o item File Data.

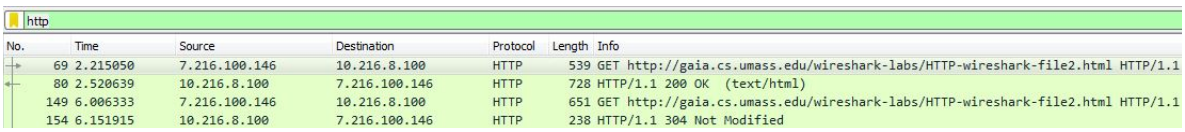
7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

Não.

---

2. The HTTP CONDITIONAL GET/response interaction

Mensagens capturadas:



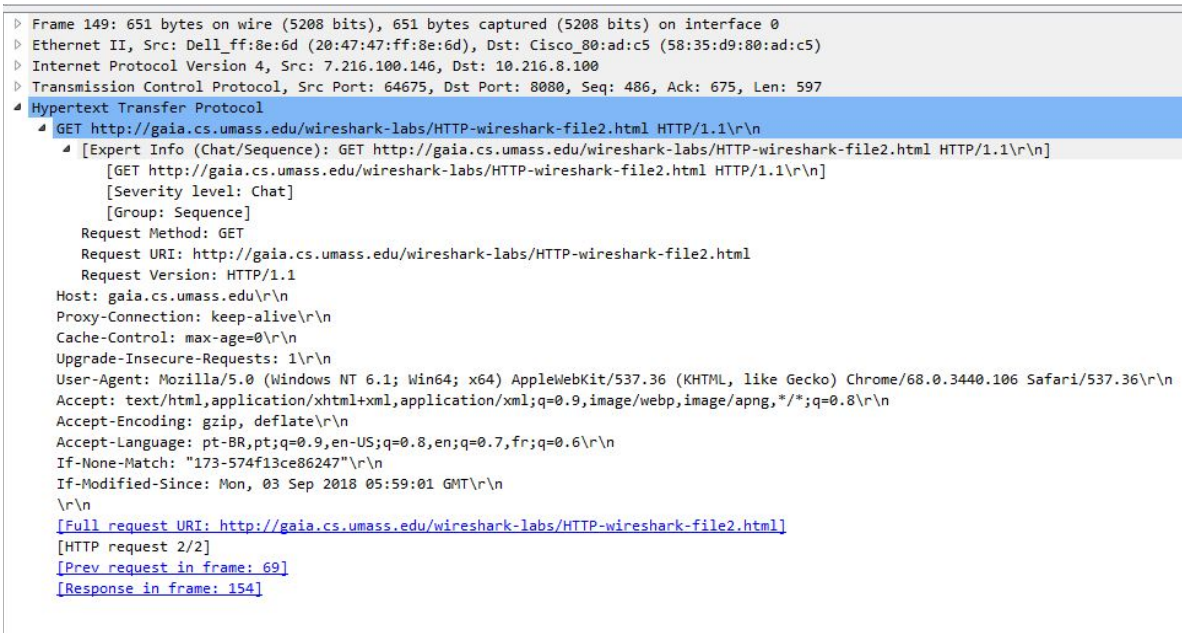
GET 1:

```
Frame 69: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits) on interface 0
Ethernet II, Src: Dell_ff:8e:6d (20:47:47:ff:8e:6d), Dst: Cisco_80:ad:c5 (58:35:d9:80:ad:c5)
Internet Protocol Version 4, Src: 7.216.100.146, Dst: 10.216.8.100
Transmission Control Protocol, Src Port: 64675, Dst Port: 8080, Seq: 1, Ack: 1, Len: 485
Hypertext Transfer Protocol
  GET http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
       [GET http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
       [Severity level: Chat]
       [Group: Sequence]
     Request Method: GET
     Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html
     Request Version: HTTP/1.1
  Host: gaia.cs.umass.edu\r\n
  Proxy-Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\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,fr;q=0.6\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: 80]
```

Response 1:

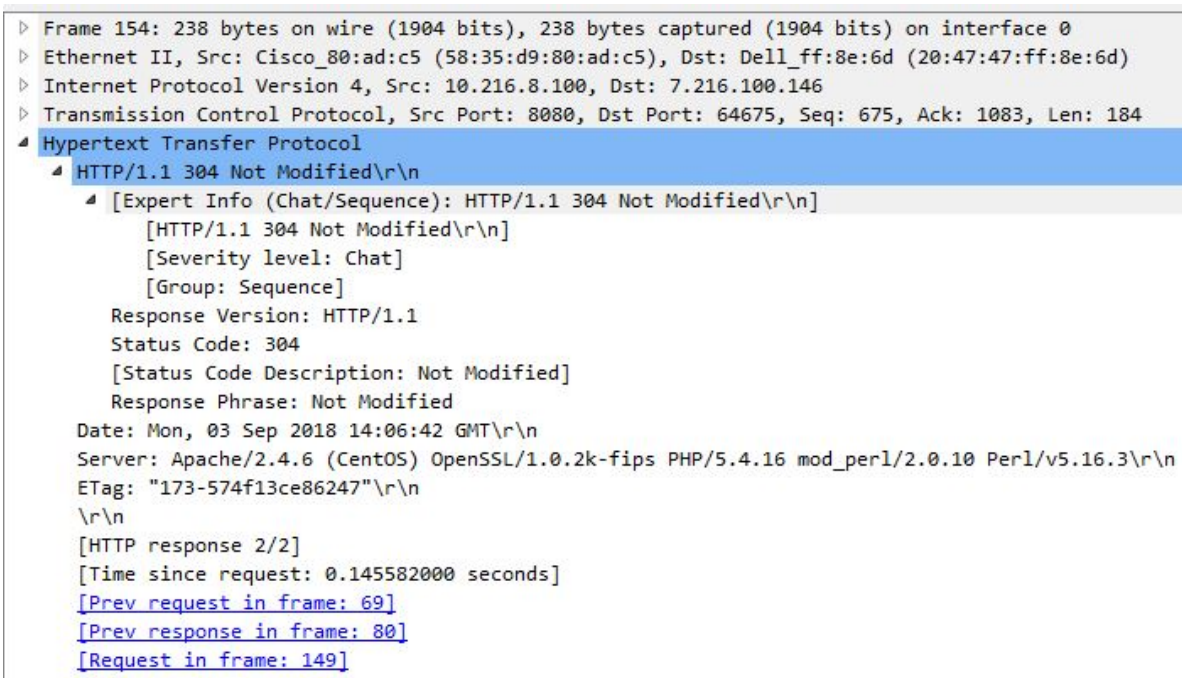
```
Frame 80: 728 bytes on wire (5824 bits), 728 bytes captured (5824 bits) on interface 0
Ethernet II, Src: Cisco_80:ad:c5 (58:35:d9:80:ad:c5), Dst: Dell_ff:8e:6d (20:47:47:ff:8e:6d)
Internet Protocol Version 4, Src: 10.216.8.100, Dst: 7.216.100.146
Transmission Control Protocol, Src Port: 8080, Dst Port: 64675, Seq: 1, Ack: 486, Len: 674
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, 03 Sep 2018 14:06:38 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
  Last-Modified: Mon, 03 Sep 2018 05:59:01 GMT\r\n
  ETag: "173-574f13ce86247"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 371\r\n
     [Content length: 371]
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [HTTP response 1/2]
  [Time since request: 0.305589000 seconds]
  [Request in frame: 69]
  [Next request in frame: 149]
  [Next response in frame: 154]
  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
```

GET 2:



```
Frame 149: 651 bytes on wire (5208 bits), 651 bytes captured (5208 bits) on interface 0
Ethernet II, Src: Dell_ff:8e:6d (20:47:47:ff:8e:6d), Dst: Cisco_80:ad:c5 (58:35:d9:80:ad:c5)
Internet Protocol Version 4, Src: 7.216.100.146, Dst: 10.216.8.100
Transmission Control Protocol, Src Port: 64675, Dst Port: 8080, Seq: 486, Ack: 675, Len: 597
Hypertext Transfer Protocol
  GET http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
        [GET http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html
      Request Version: HTTP/1.1
  Host: gaia.cs.umass.edu\r\n
  Proxy-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 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\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,fr;q=0.6\r\n
  If-None-Match: "173-574f13ce86247"\r\n
  If-Modified-Since: Mon, 03 Sep 2018 05:59:01 GMT\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  [HTTP request 2/2]
  [Prev request in frame: 69]
  [Response in frame: 154]
```

Response 2:



```
Frame 154: 238 bytes on wire (1904 bits), 238 bytes captured (1904 bits) on interface 0
Ethernet II, Src: Cisco_80:ad:c5 (58:35:d9:80:ad:c5), Dst: Dell_ff:8e:6d (20:47:47:ff:8e:6d)
Internet Protocol Version 4, Src: 10.216.8.100, Dst: 7.216.100.146
Transmission Control Protocol, Src Port: 8080, Dst Port: 64675, Seq: 675, Ack: 1083, Len: 184
Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
    [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: Mon, 03 Sep 2018 14:06:42 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
  ETag: "173-574f13ce86247"\r\n
  \r\n
  [HTTP response 2/2]
  [Time since request: 0.145582000 seconds]
  [Prev request in frame: 69]
  [Prev response in frame: 80]
  [Request in frame: 149]
```

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?

Esta linha não existe no primeiro GET.

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

Sim, pois é possível expandir o item Line-based text data: text/html (10 lines) e obter o conteúdo da página.

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, o contéudo deste item é: Mon, 03 Sep 2018 05:59:01 GMT.

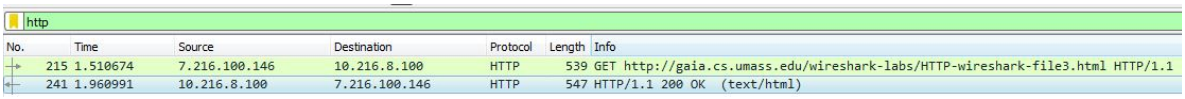
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

O status retornado é o 304 - Not Modified. O servidor não retornou o conteúdo novamente. Este fato ocorre pois o conteúdo da página não foi modificado desde o último carregamento. Isso faz com que seja desnecessário reenviar os conteúdos novamente, uma vez que o browser já está exibindo o conteúdo presente no servidor. Isso otimiza e descongestiona a rede, uma vez que conteúdos redundantes não são reenviados desnecessariamente.

---

3. Retrieving Long Documents

Mensagens capturadas:



GET:

```
Transmission Control Protocol, Src Port: 56377, Dst Port: 8080, Seq: 1, Ack: 1, Len: 485
Hypertext Transfer Protocol
  GET http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
        [GET http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html
      Request Version: HTTP/1.1
  Host: gaia.cs.umass.edu\r\n
  Proxy-Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\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,fr;q=0.6\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
  [HTTP request 1/1]
  [Response in frame: 241]
```

Response e TCP segments:

```
[4 Reassembled TCP Segments (4805 bytes): #237(1392), #238(1460), #240(1460), #241(493)]
    [Frame: 237, payload: 0-1391 (1392 bytes)]
    [Frame: 238, payload: 1392-2851 (1460 bytes)]
    [Frame: 240, payload: 2852-4311 (1460 bytes)]
    [Frame: 241, payload: 4312-4804 (493 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4805]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a204d...]
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, 03 Sep 2018 14:34:07 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
  Last-Modified: Mon, 03 Sep 2018 05:59:01 GMT\r\n
  ETag: "1194-574f13ce8103f"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 4500\r\n
      [Content length: 4500]
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.450317000 seconds]
  [Request in frame: 215]
  File Data: 4500 bytes
Line-based text data: text/html (98 lines)
```

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

Apenas 1 GET foi enviado. O pacote 215, conforme item [Request in frame: 215]

13. Which packet number in the trace contains the status code and phrase

associated with the response to the HTTP GET request?

O pacote 215, conforme item [Request in frame: 215]

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

200 - OK, conforme itens Status Code: 200 e Response Phrase: OK.

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

4 segmentos foram necessários, conforme item Segment count.

---

4. HTML Documents with Embedded Objects

Mensagens capturadas:

No.	Time	Source	Destination	Protocol	Length	Info
71	1.671366	7.216.100.146	10.216.8.100	HTTP	539	GET http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
78	1.962494	10.216.8.100	7.216.100.146	HTTP	1071	HTTP/1.1 200 OK (text/html)
81	1.999151	7.216.100.146	10.216.8.100	HTTP	510	GET http://gaia.cs.umass.edu/pearson.png HTTP/1.1
89	2.026699	7.216.100.146	10.216.8.100	HTTP	525	GET http://manic.cs.umass.edu/~kurose/cover_5th_ed.jpg HTTP/1.1
96	2.146213	10.216.8.100	7.216.100.146	HTTP	757	HTTP/1.1 200 OK (PNG)
110	2.332595	10.216.8.100	7.216.100.146	HTTP	491	HTTP/1.1 302 Found (text/html)
122	2.494113	7.216.100.146	10.216.8.100	HTTP	525	GET http://caite.cs.umass.edu/~kurose/cover_5th_ed.jpg HTTP/1.1
253	3.428390	10.216.8.100	7.216.100.146	HTTP	1354	HTTP/1.1 200 OK (JPEG JFIF image)

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

4 requisições GET foram enviadas. O endereço foi 10.216.8.100

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.

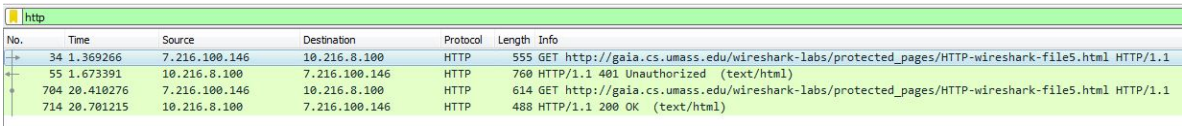
Analisando os tempos, é possível perceber que os downloads foram em paralelo, pois o download da primeira imagem foi solicitado no tempo 1.999151 e finalizado no tempo 2.146213. Enquanto isso, o download da segunda imagem foi solicitado no tempo 2.026699 e finalizado no tempo 3.428390, pois a segunda imagem mudou de localização e por isso foi feito um quarto GET para o real endereço da

imagem, uma vez que o terceiro retornou a nova localização desta.

---

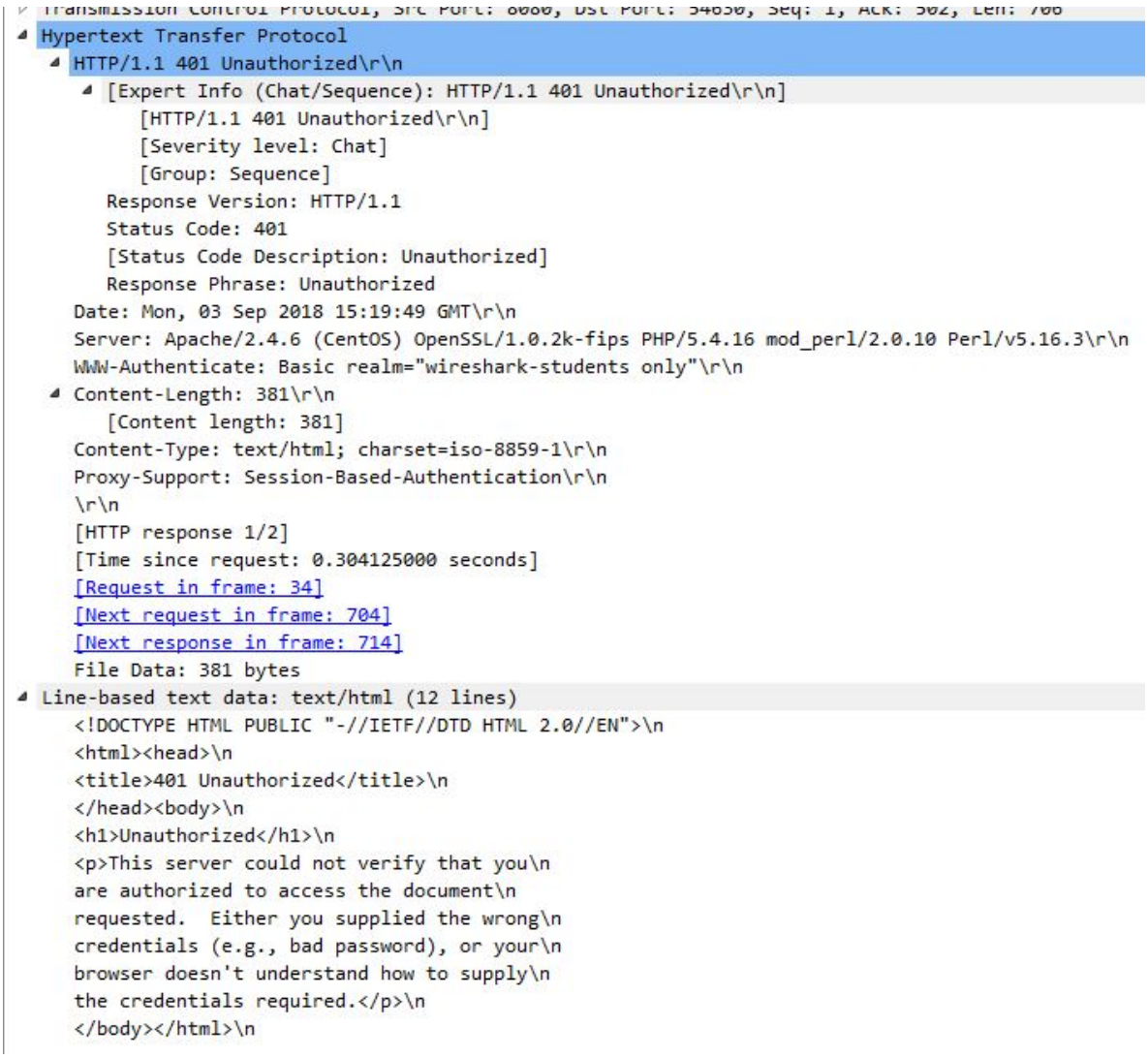
5 HTTP Authentication

Mensagens capturadas:



No.	Time	Source	Destination	Protocol	Length	Info
34	1.369266	7.216.100.146	10.216.8.100	HTTP	555	GET http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
55	1.673391	10.216.8.100	7.216.100.146	HTTP	760	HTTP/1.1 401 Unauthorized (text/html)
704	20.410276	7.216.100.146	10.216.8.100	HTTP	614	GET http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
714	20.701215	10.216.8.100	7.216.100.146	HTTP	488	HTTP/1.1 200 OK (text/html)

Response 1:



```
▸ Transmission Control Protocol, Src Port: 8080, Dst Port: 54630, Seq: 1, Ack: 502, Len: 706
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 401 Unauthorized\r\n
    ▾ [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: Mon, 03 Sep 2018 15:19:49 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    WWW-Authenticate: Basic realm="wireshark-students only"\r\n
  ▾ Content-Length: 381\r\n
      [Content length: 381]
    Content-Type: text/html; charset=iso-8859-1\r\n
    Proxy-Support: Session-Based-Authentication\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.304125000 seconds]
    [Request in frame: 34]
    [Next request in frame: 704]
    [Next response in frame: 714]
    File Data: 381 bytes
▾ Line-based text data: text/html (12 lines)
    <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
    <html><head>\n
    <title>401 Unauthorized</title>\n
    </head><body>\n
    <h1>Unauthorized</h1>\n
    <p>This server could not verify that you\n
    are authorized to access the document\n
    requested.  Either you supplied the wrong\n
    credentials (e.g., bad password), or your\n
    browser doesn't understand how to supply\n
    the credentials required.</p>\n
    </body></html>\n
```

GET 2:

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

401 - Unauthorized, conforme os itens Status Code e Status Response.

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 novo campo incluído é o Authorization, que contém as credenciais de autenticação.
