UFU 45 ANOS

Prática 2 – Wireshark LAB - HTTP

Redes de Comunicações I

Gabriel Resende Soares

11721ECP011

Leonardo Vecchi Meirelles

12011ECP002

Setembro 2023

Sumário

The Basic HTTP GET/response interaction

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

R : HTTP/1.1

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

R : Accept-Language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7

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

R :

Source Address: 192.168.15.27

Destination Address: 128.119.245.12

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

R : Como eu já havia baixado o .html, a resposta foi 304: “Not Modified”.

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

R : Last-Modified: Mon, 25 Sep 2023 05:59:02 GMT\r\n

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

R : 128 bytes.

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.

R : 0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Identification: 0x0f20 (3872)

010. .... = Flags: 0x2, Don't fragment

0... .... = Reserved bit: Not set

.1.. .... = Don't fragment: Set

..0. .... = More fragments: Not set

...0 0000 0000 0000 = Fragment Offset: 0

```
No.     Time              Source                Destination           Protocol Length Info
   8361 01:49:07,078749    192.168.15.27         128.119.245.12        HTTP     526    GET /wireshark-labs/HTTP-wireshark-file1.html
HTTP/1.1
Frame 8361: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface \Device\NPF_{E42C0A5B-9D1B-4333-A144-
E0870EB91F6A}, id 0
Ethernet II, Src: Micro-St_d4:02:c8 (d8:cb:8a:d4:02:c8), Dst: MitraSta_d2:c2:11 (ac:c6:62:d2:c2:11)
Internet Protocol Version 4, Src: 192.168.15.27, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 53069, Dst Port: 80, Seq: 1, Ack: 1, Len: 472
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/117.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: pt-BR,pt;q=0.9\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: 8363]
No.     Time              Source                Destination           Protocol Length Info
   8363 01:49:07,239087    128.119.245.12        192.168.15.27         HTTP     540    HTTP/1.1 200 OK  (text/html)
Frame 8363: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{E42C0A5B-9D1B-4333-A144-
E0870EB91F6A}, id 0
Ethernet II, Src: MitraSta_d2:c2:11 (ac:c6:62:d2:c2:11), Dst: Micro-St_d4:02:c8 (d8:cb:8a:d4:02:c8)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.15.27
Transmission Control Protocol, Src Port: 80, Dst Port: 53069, Seq: 1, Ack: 473, Len: 486
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Tue, 26 Sep 2023 04:49:09 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Mon, 25 Sep 2023 05:59:02 GMT\r\n
    ETag: "80-60628a7b13b32"\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: 0.160338000 seconds]
    [Request in frame: 8361]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    File Data: 128 bytes
Line-based text data: text/html (4 lines)
```

The HTTP CONDITIONAL GET/response interaction

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?

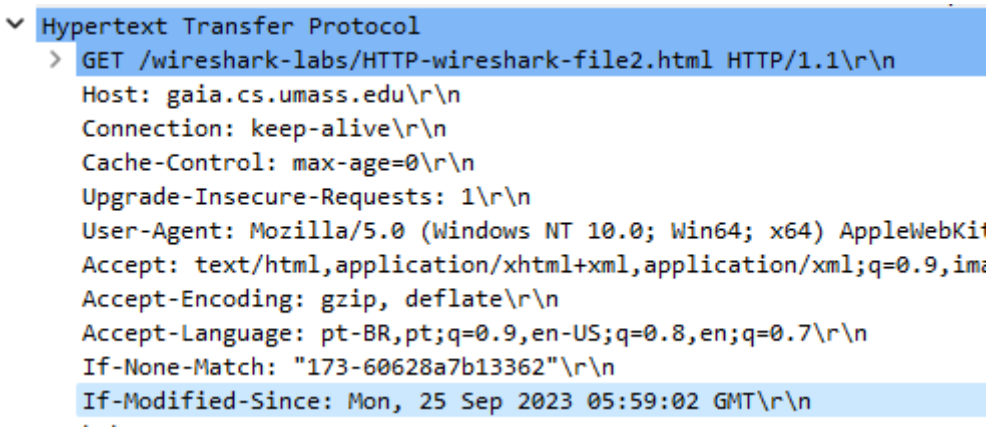
Não, tal mensagem não foi encontrada.

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

Sim, o conteúdo é apresentado ao final.

```
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
```

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?



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 code é 304, frase retornada: Not Modified. O servidor não retornou o conteúdo do arquivo, pois ele não foi modificado desde a última requisição, portanto não houve a necessidade de reenvio, pois o conteúdo estava armazenado na cache do navegador.

```
No.     Time              Source                Destination           Protocol Length Info
    123 01:51:29,917573    192.168.15.27         128.119.245.12        HTTP     526    GET /wireshark-labs/HTTP-wireshark-file2.html
HTTP/1.1
Frame 123: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface \Device\NPF_{E42C0A5B-9D1B-4333-A144-
E0870EB91F6A}, id 0
Ethernet II, Src: Micro-St_d4:02:c8 (d8:cb:8a:d4:02:c8), Dst: MitraSta_d2:c2:11 (ac:c6:62:d2:c2:11)
Internet Protocol Version 4, Src: 192.168.15.27, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 53077, Dst Port: 80, Seq: 1, Ack: 1, Len: 472
    Source Port: 53077
    Destination Port: 80
    [Stream index: 3]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 472]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3353064729
    [Next Sequence Number: 473    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2268760332
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 1029
    [Calculated window size: 263424]
    [Window size scaling factor: 256]
    Checksum: 0x473a [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (472 bytes)
Hypertext Transfer Protocol
No.     Time              Source                Destination           Protocol Length Info
    126 01:51:30,070328    128.119.245.12        192.168.15.27         HTTP     784    HTTP/1.1 200 OK  (text/html)
Frame 126: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{E42C0A5B-9D1B-4333-A144-
E0870EB91F6A}, id 0
Ethernet II, Src: MitraSta_d2:c2:11 (ac:c6:62:d2:c2:11), Dst: Micro-St_d4:02:c8 (d8:cb:8a:d4:02:c8)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.15.27
Transmission Control Protocol, Src Port: 80, Dst Port: 53077, Seq: 1, Ack: 473, Len: 730
    Source Port: 80
    Destination Port: 53077
    [Stream index: 3]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 730]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2268760332
    [Next Sequence Number: 731    (relative sequence number)]
    Acknowledgment Number: 473    (relative ack number)
    Acknowledgment number (raw): 3353065201
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0xdf21 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (730 bytes)
Hypertext Transfer Protocol
Line-based text data: text/html (10 lines)
```

Retrieving Long Documents

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?

R : O navegador enviou apenas uma mensagem de requisição.

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

R : O packet de número 149, O status code é 200 e a frase associada é “OK”.

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

R : O status code é 200 e a frase associada é “OK”.

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

R: [4 Reassembled TCP Segments (4861 bytes): #146(1440), #147(1440), #148(1440), #149(541)]

```
No.     Time               Source                Destination           Protocol Length Info
    144 01:51:36,625749    192.168.15.27         128.119.245.12        HTTP     526    GET /wireshark-labs/HTTP-wireshark-file3.html
HTTP/1.1
Frame 144: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface \Device\NPF_{E42C0A5B-9D1B-4333-A144-
E0870EB91F6A}, id 0
Ethernet II, Src: Micro-St_d4:02:c8 (d8:cb:8a:d4:02:c8), Dst: MitraSta_d2:c2:11 (ac:c6:62:d2:c2:11)
Internet Protocol Version 4, Src: 192.168.15.27, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 53078, Dst Port: 80, Seq: 1, Ack: 1, Len: 472
    Source Port: 53078
    Destination Port: 80
    [Stream index: 6]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 472]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2398928580
    [Next Sequence Number: 473    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 746322540
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 1029
    [Calculated window size: 263424]
    [Window size scaling factor: 256]
    Checksum: 0x473a [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (472 bytes)
Hypertext Transfer Protocol
No.     Time               Source                Destination           Protocol Length Info
    149 01:51:36,802727    128.119.245.12        192.168.15.27         HTTP     595    HTTP/1.1 200 OK  (text/html)
Frame 149: 595 bytes on wire (4760 bits), 595 bytes captured (4760 bits) on interface \Device\NPF_{E42C0A5B-9D1B-4333-A144-
E0870EB91F6A}, id 0
Ethernet II, Src: MitraSta_d2:c2:11 (ac:c6:62:d2:c2:11), Dst: Micro-St_d4:02:c8 (d8:cb:8a:d4:02:c8)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.15.27
Transmission Control Protocol, Src Port: 80, Dst Port: 53078, Seq: 4321, Ack: 473, Len: 541
    Source Port: 80
    Destination Port: 53078
    [Stream index: 6]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 541]
    Sequence Number: 4321    (relative sequence number)
    Sequence Number (raw): 746326860
    [Next Sequence Number: 4862    (relative sequence number)]
    Acknowledgment Number: 473    (relative ack number)
    Acknowledgment number (raw): 2398929052
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0x0544 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (541 bytes)
    TCP segment data (541 bytes)
[4 Reassembled TCP Segments (4861 bytes): #146(1440), #147(1440), #148(1440), #149(541)]
    [Frame: 146, payload: 0-1439 (1440 bytes)]
    [Frame: 147, payload: 1440-2879 (1440 bytes)]
    [Frame: 148, payload: 2880-4319 (1440 bytes)]
    [Frame: 149, payload: 4320-4860 (541 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 48545502f312e3120323030204f4b0d0a446174653a205475652c203236205365702032…]
Hypertext Transfer Protocol
Line-based text data: text/html (98 lines)
```

HTML Documents with Embedded Objects

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

R : Foram 3 GETs :

226	01:51:44,589753	192.168.15.27	128.119.245.12	HTTP	526 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
229	01:51:44,762872	128.119.245.12	192.168.15.27	HTTP	1355 HTTP/1.1 200 OK (text/html)
230	01:51:44,772784	192.168.15.27	128.119.245.12	HTTP	472 GET /pearson.png HTTP/1.1
235	01:51:44,943161	128.119.245.12	192.168.15.27	HTTP	785 HTTP/1.1 200 OK (PNG)
242	01:51:45,728024	192.168.15.27	178.79.137.164	HTTP	439 GET /8E_cover_small.jpg HTTP/1.1
246	01:51:45,962657	178.79.137.164	192.168.15.27	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.

R : Meu navegador baixou as duas imagens em série, como é possível perceber na imagem anterior.

```
No.     Time              Source                Destination           Protocol Length Info
    226 01:51:44,589753   192.168.15.27         128.119.245.12        HTTP     526    GET /wireshark-labs/HTTP-wireshark-file4.html
HTTP/1.1
Frame 226: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface \Device\NPF_{E42C0A5B-9D1B-4333-A144-
E0870EB91F6A}, id 0
Ethernet II, Src: Micro-St_d4:02:c8 (d8:cb:8a:d4:02:c8), Dst: MitraSta_d2:c2:11 (ac:c6:62:d2:c2:11)
Internet Protocol Version 4, Src: 192.168.15.27, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 53080, Dst Port: 80, Seq: 1, Ack: 1, Len: 472
    Source Port: 53080
    Destination Port: 80
    [Stream index: 9]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 472]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 4291175945
    [Next Sequence Number: 473    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1114936597
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 1029
    [Calculated window size: 263424]
    [Window size scaling factor: 256]
    Checksum: 0x473a [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (472 bytes)
Hypertext Transfer Protocol
No.     Time              Source                Destination           Protocol Length Info
    229 01:51:44,762872   128.119.245.12        192.168.15.27         HTTP     1355   HTTP/1.1 200 OK  (text/html)
Frame 229: 1355 bytes on wire (10840 bits), 1355 bytes captured (10840 bits) on interface \Device\NPF_{E42C0A5B-9D1B-4333-A144-
E0870EB91F6A}, id 0
Ethernet II, Src: MitraSta_d2:c2:11 (ac:c6:62:d2:c2:11), Dst: Micro-St_d4:02:c8 (d8:cb:8a:d4:02:c8)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.15.27
Transmission Control Protocol, Src Port: 80, Dst Port: 53080, Seq: 1, Ack: 473, Len: 1301
    Source Port: 80
    Destination Port: 53080
    [Stream index: 9]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 1301]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1114936597
    [Next Sequence Number: 1302    (relative sequence number)]
    Acknowledgment Number: 473    (relative ack number)
    Acknowledgment number (raw): 4291176417
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0xee39 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (1301 bytes)
Hypertext Transfer Protocol
Line-based text data: text/html (23 lines)
No.     Time              Source                Destination           Protocol Length Info
    230 01:51:44,772784   192.168.15.27         128.119.245.12        HTTP     472    GET /pearson.png HTTP/1.1
Frame 230: 472 bytes on wire (3776 bits), 472 bytes captured (3776 bits) on interface \Device\NPF_{E42C0A5B-9D1B-4333-A144-
E0870EB91F6A}, id 0
Ethernet II, Src: Micro-St_d4:02:c8 (d8:cb:8a:d4:02:c8), Dst: MitraSta_d2:c2:11 (ac:c6:62:d2:c2:11)
Internet Protocol Version 4, Src: 192.168.15.27, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 53080, Dst Port: 80, Seq: 473, Ack: 1302, Len: 418
    Source Port: 53080
    Destination Port: 80
    [Stream index: 9]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 418]
    Sequence Number: 473    (relative sequence number)
    Sequence Number (raw): 4291176417
    [Next Sequence Number: 891    (relative sequence number)]
    Acknowledgment Number: 1302    (relative ack number)
    Acknowledgment number (raw): 1114937898
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 1024
    [Calculated window size: 262144]
    [Window size scaling factor: 256]
    Checksum: 0x4704 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
```

```
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (418 bytes)
Hypertext Transfer Protocol
No.     Time              Source                Destination           Protocol Length Info
    235 01:51:44,943161   128.119.245.12        192.168.15.27         HTTP     785    HTTP/1.1 200 OK  (PNG)
Frame 235: 785 bytes on wire (6280 bits), 785 bytes captured (6280 bits) on interface \Device\NPF_{E42C0A5B-9D1B-4333-A144-
E0870EB91F6A}, id 0
Ethernet II, Src: MitraSta_d2:c2:11 (ac:c6:62:d2:c2:11), Dst: Micro-St_d4:02:c8 (d8:cb:8a:d4:02:c8)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.15.27
Transmission Control Protocol, Src Port: 80, Dst Port: 53080, Seq: 4182, Ack: 891, Len: 731
    Source Port: 80
    Destination Port: 53080
    [Stream index: 9]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 731]
    Sequence Number: 4182    (relative sequence number)
    Sequence Number (raw): 1114940778
    [Next Sequence Number: 4913    (relative sequence number)]
    Acknowledgment Number: 891    (relative ack number)
    Acknowledgment number (raw): 4291176835
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 245
    [Calculated window size: 31360]
    [Window size scaling factor: 128]
    Checksum: 0x9fd6 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (731 bytes)
    TCP segment data (731 bytes)
[3 Reassembled TCP Segments (3611 bytes): #233(1440), #234(1440), #235(731)]
    [Frame: 233, payload: 0-1439 (1440 bytes)]
    [Frame: 234, payload: 1440-2879 (1440 bytes)]
    [Frame: 235, payload: 2880-3610 (731 bytes)]
    [Segment count: 3]
    [Reassembled TCP length: 3611]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a205475652c203236205365702032…]
Hypertext Transfer Protocol
Portable Network Graphics
No.     Time              Source                Destination           Protocol Length Info
    242 01:51:45,728024   192.168.15.27         178.79.137.164        HTTP     439    GET /8E_cover_small.jpg HTTP/1.1
Frame 242: 439 bytes on wire (3512 bits), 439 bytes captured (3512 bits) on interface \Device\NPF_{E42C0A5B-9D1B-4333-A144-
E0870EB91F6A}, id 0
Ethernet II, Src: Micro-St_d4:02:c8 (d8:cb:8a:d4:02:c8), Dst: MitraSta_d2:c2:11 (ac:c6:62:d2:c2:11)
Internet Protocol Version 4, Src: 192.168.15.27, Dst: 178.79.137.164
Transmission Control Protocol, Src Port: 53081, Dst Port: 80, Seq: 1, Ack: 1, Len: 385
    Source Port: 53081
    Destination Port: 80
    [Stream index: 10]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 385]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 514593204
    [Next Sequence Number: 386    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2228553978
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 1029
    [Calculated window size: 263424]
    [Window size scaling factor: 256]
    Checksum: 0x0d53 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (385 bytes)
Hypertext Transfer Protocol
No.     Time              Source                Destination           Protocol Length Info
    246 01:51:45,962657   178.79.137.164        192.168.15.27         HTTP     225    HTTP/1.1 301 Moved Permanently
Frame 246: 225 bytes on wire (1800 bits), 225 bytes captured (1800 bits) on interface \Device\NPF_{E42C0A5B-9D1B-4333-A144-
E0870EB91F6A}, id 0
Ethernet II, Src: MitraSta_d2:c2:11 (ac:c6:62:d2:c2:11), Dst: Micro-St_d4:02:c8 (d8:cb:8a:d4:02:c8)
Internet Protocol Version 4, Src: 178.79.137.164, Dst: 192.168.15.27
Transmission Control Protocol, Src Port: 80, Dst Port: 53081, Seq: 1, Ack: 386, Len: 171
    Source Port: 80
    Destination Port: 53081
    [Stream index: 10]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 171]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2228553978
```

```
   [Next Sequence Number: 172    (relative sequence number)]
   Acknowledgment Number: 386    (relative ack number)
   Acknowledgment number (raw): 514593589
   0101 .... = Header Length: 20 bytes (5)
   Flags: 0x018 (PSH, ACK)
   Window: 501
   [Calculated window size: 64128]
   [Window size scaling factor: 128]
   Checksum: 0x1876 [unverified]
   [Checksum Status: Unverified]
   Urgent Pointer: 0
   [Timestamps]
   [SEQ/ACK analysis]
   TCP payload (171 bytes)
Hypertext Transfer Protocol
```

HTTP Authentication

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

R : O status code foi 401, frase "Unauthorized"

```
678 01:51:49,572886    192.168.15.27     128.119.245.12    HTTP    542 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
679 01:51:49,743219    128.119.245.12    192.168.15.27     HTTP    770 HTTP/1.1 401 Unauthorized  (text/html)
```

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

R : Foi incluído o campo de "Authorization"

```
Hypertext Transfer Protocol
  GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.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
  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/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: pt-BR,pt;q=0.9\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: 838]
```

```
No.     Time               Source                Destination           Protocol Length Info
    678 01:51:49,572886    192.168.15.27         128.119.245.12        HTTP     542    GET /wireshark-labs/protected_pages/HTTP-
wireshark-file5.html HTTP/1.1
Frame 678: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface \Device\NPF_{E42C0A5B-9D1B-4333-A144-
E0870EB91F6A}, id 0
Ethernet II, Src: Micro-St_d4:02:c8 (d8:cb:8a:d4:02:c8), Dst: MitraSta_d2:c2:11 (ac:c6:62:d2:c2:11)
Internet Protocol Version 4, Src: 192.168.15.27, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 53080, Dst Port: 80, Seq: 891, Ack: 4913, Len: 488
Hypertext Transfer Protocol
    GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
        Request Method: GET
        Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: pt-BR,pt;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    [HTTP request 3/3]
    [Prev request in frame: 230]
    [Response in frame: 679]
No.     Time               Source                Destination           Protocol Length Info
    679 01:51:49,743219    128.119.245.12        192.168.15.27         HTTP     770    HTTP/1.1 401 Unauthorized  (text/html)
Frame 679: 770 bytes on wire (6160 bits), 770 bytes captured (6160 bits) on interface \Device\NPF_{E42C0A5B-9D1B-4333-A144-
E0870EB91F6A}, id 0
Ethernet II, Src: MitraSta_d2:c2:11 (ac:c6:62:d2:c2:11), Dst: Micro-St_d4:02:c8 (d8:cb:8a:d4:02:c8)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.15.27
Transmission Control Protocol, Src Port: 80, Dst Port: 53080, Seq: 4913, Ack: 1379, Len: 716
Hypertext Transfer Protocol
    HTTP/1.1 401 Unauthorized\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
        Response Version: HTTP/1.1
        Status Code: 401
        [Status Code Description: Unauthorized]
        Response Phrase: Unauthorized
    Date: Tue, 26 Sep 2023 04:51:51 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    WWW-Authenticate: Basic realm="wireshark-students only"\r\n
    Content-Length: 381\r\n
    Keep-Alive: timeout=5, max=98\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 3/3]
    [Time since request: 0.170333000 seconds]
    [Prev request in frame: 230]
    [Prev response in frame: 235]
    [Request in frame: 678]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    File Data: 381 bytes
Line-based text data: text/html (12 lines)
No.     Time               Source                Destination           Protocol Length Info
    836 01:52:33,228644    192.168.15.27         128.119.245.12        HTTP     627    GET /wireshark-labs/protected_pages/HTTP-
wireshark-file5.html HTTP/1.1
Frame 836: 627 bytes on wire (5016 bits), 627 bytes captured (5016 bits) on interface \Device\NPF_{E42C0A5B-9D1B-4333-A144-
E0870EB91F6A}, id 0
Ethernet II, Src: Micro-St_d4:02:c8 (d8:cb:8a:d4:02:c8), Dst: MitraSta_d2:c2:11 (ac:c6:62:d2:c2:11)
Internet Protocol Version 4, Src: 192.168.15.27, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 53085, Dst Port: 80, Seq: 1, Ack: 1, Len: 573
Hypertext Transfer Protocol
    GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
        Request Method: GET
        Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.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
    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/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: pt-BR,pt;q=0.9\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: 838]
No.     Time                Source                Destination           Protocol Length Info
    838 01:52:33,390661     128.119.245.12        192.168.15.27         HTTP     544    HTTP/1.1 200 OK  (text/html)
Frame 838: 544 bytes on wire (4352 bits), 544 bytes captured (4352 bits) on interface \Device\NPF_{E42C0A58-9D1B-4333-A144-
E0870EB91F6A}, id 0
Ethernet II, Src: MitraSta_d2:c2:11 (ac:c6:62:d2:c2:11), Dst: Micro-St_d4:02:c8 (d8:cb:8a:d4:02:c8)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.15.27
Transmission Control Protocol, Src Port: 80, Dst Port: 53085, Seq: 1, Ack: 574, Len: 490
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, 26 Sep 2023 04:52:35 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Mon, 25 Sep 2023 05:59:02 GMT\r\n
    ETag: "84-60628a7b14ad3"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 132\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: 0.162017000 seconds]
    [Request in frame: 836]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    File Data: 132 bytes
Line-based text data: text/html (6 lines)
```