Lab
2

BÁO CÁO BÀI THỰC HÀNH SỐ 1
PHÂN TÍCH GÓI TIN HTTP VỚI WIRESHARK

Môn học: Nhập môn mạng máy tính

Sinh viên thực hiện	Trần Thanh Hùng (23520580)
Thời gian thực hiện	27/03/2024 – 03/04/2024
Số câu đã hoàn thành	5/5

TRẢ LỜI CÁC CÂU HỎI

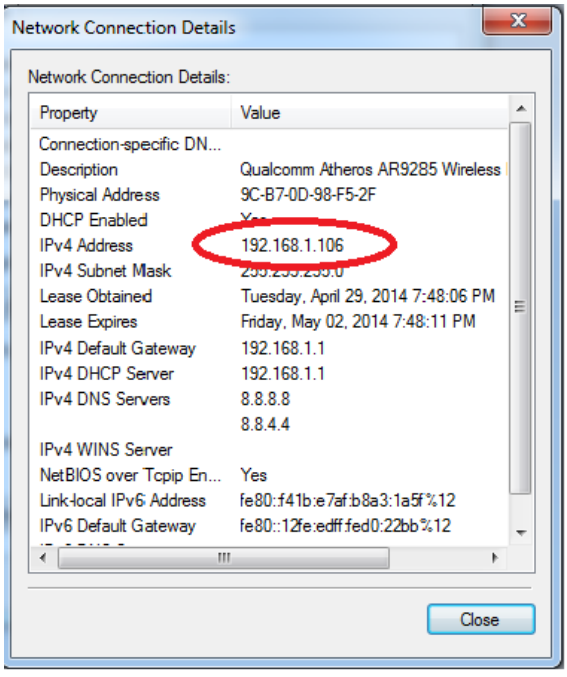
Gợi ý: *Trả lời câu hỏi đúng, đầy đủ, cần giải thích lý do tại sao có được đáp án, có các hình ảnh, bằng chứng để chứng minh tính đúng đắn*.

Ví dụ:

Câu 1. Địa chỉ IP máy tính của bạn là gì?

Trả lời: *192.168.1.106*

Để xem địa chỉ IP của máy tính trên Windows, mở **Control Panel** và chọn **View network status and tasks.** Chọn mạng tương ứng đang sử dụng để kết nối Internet, chọn **Details** trong cửa sổ trạng thái. Xem địa chỉ IP trong Ipv4 Address



1. Trình duyệt đang sử dụng phiên bản HTTP 1.0 hay 1.1? Phiên bản HTTP server đang sử dụng là bao nhiêu?

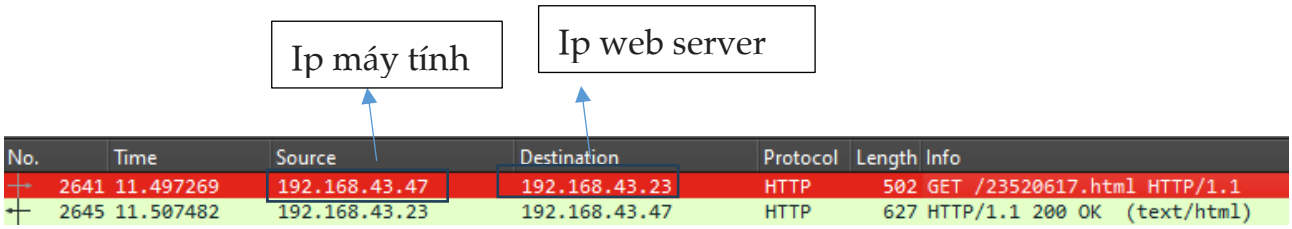
   Trình duyệt đang sử dụng phiên bản HTTP 1.1

   Sever đang sử dụng phiên bản HTTP 1.1

2. Địa chỉ IP của máy tính bạn là bao nhiêu? Của web server là bao nhiêu?

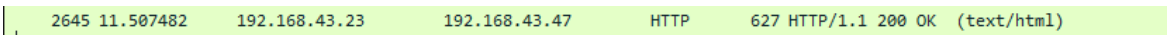
   IP của máy tính là: 192.168.43.47

   IP của web sever là: 192.168.43.23

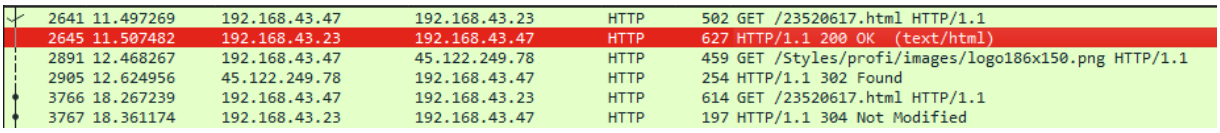


3. Các mã trạng thái (status code) trả về từ server là gì?

   Các mã trạng thái (status code) trả về từ sever là: 200



4. Server đã trả về cho trình duyệt tổng cộng bao nhiêu bytes nội dung?



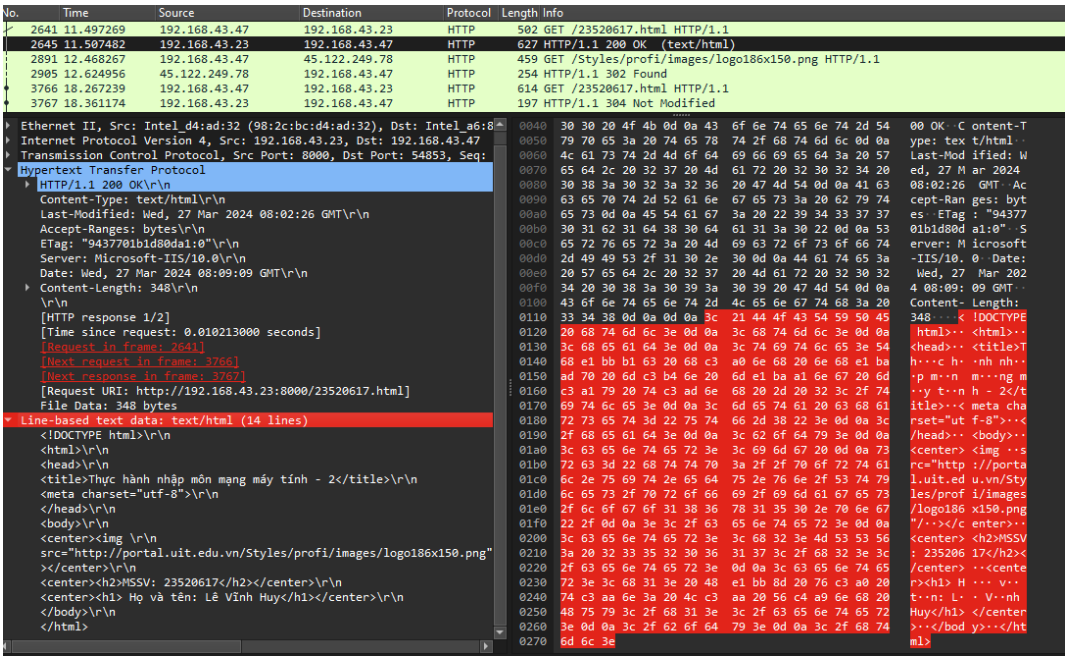
   Server trả về trình duyệt 627 byte nội dung

5. Xem xét nội dung của HTTP GET đầu tiên. Bạn có thấy dòng "IF-MODIFIEDSINCE" hay không?

   Nội dung của HTTP GET đầu tiên không có dòng "IF-MODIFIEDSINCE"

6. Xem xét nội dung phản hồi từ server đối với HTTP GET đầu tiên. Server có trả về nội dung của file HTML hay không? Mã trạng thái đi kèm là gì? Giải thích ý nghĩa.

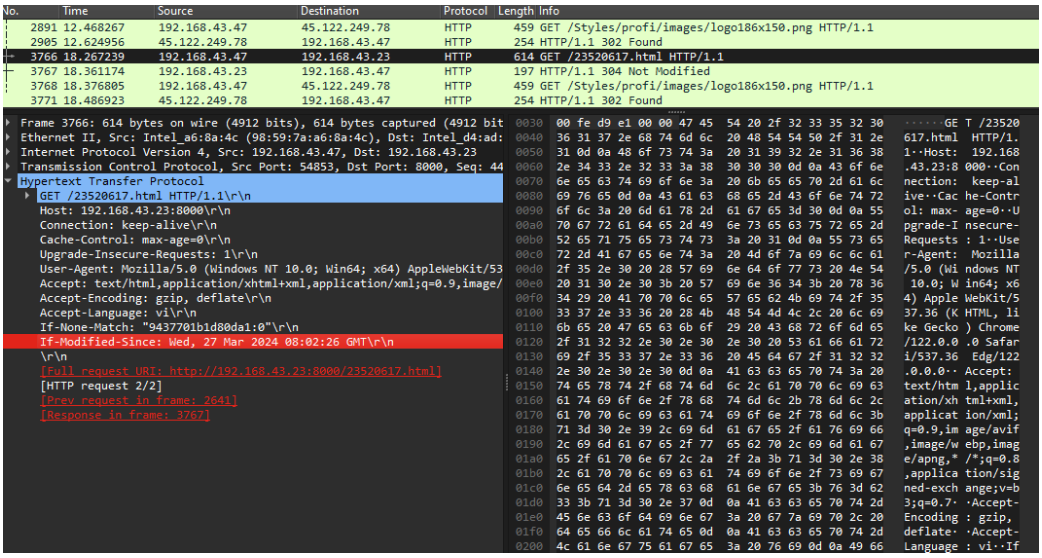
   Từ nội dung phản hồi từ server đối với HTTP Get đầu tiên, server có trả về nội dung file HTML kèm với mã trạng thái 200 OK.



   Mã trạng thái 200 OK được trả về khi máy chủ đáp ứng yêu cầu thành công. Cụ thể, khi máy khách gửi yêu cầu tới máy chủ, nếu máy chủ xử lý yêu cầu thành công và trả về dữ liệu yêu cầu, nó sẽ gửi lại phản hồi với mã trạng thái 200 để cho biết yêu cầu đã được hoàn thành thành công và dữ liệu được trả về đúng như yêu cầu

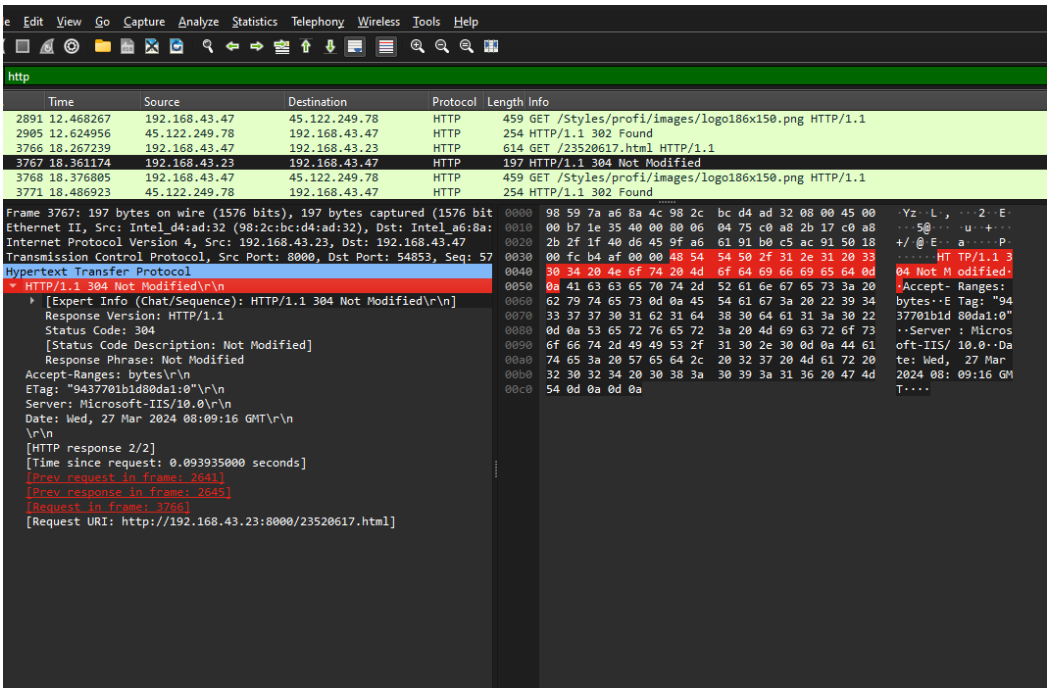
7. Xem xét nội dung của HTTP GET thứ 2. Bạn có thấy dòng "IF-MODIFIEDSINCE" hay không? Nếu có, giá trị của IF-MODIFIED-SINCE là gì?

   Ở nội dung GET thứ 2, có dòng "IF-MODIFIEDSINCE"



8. Mã trạng thái HTTP được trả về từ server tương ứng với HTTP GET thứ 2 là gì? Ý nghĩa nó là gì? Server có thật sự gửi về nội dung của file hay không? Giải thích.

- Mã trạng thái HTTP được trả về từ server tương ứng với HTTP GET thứ 2 là 304 Not Modified.

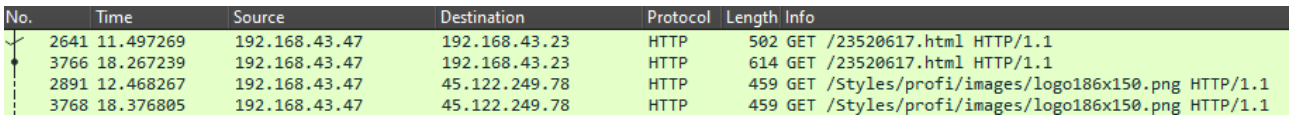


- 304 Not Modified cho biết rằng tài nguyên được yêu cầu chưa được sửa đổi kể từ lần cuối cùng nó được tải, và không cần phải truyền lại

- Server không gửi nội dung của file HTML mà trình duyệt sẽ lấy nội dung từ cache để hiển thị cho người dung.

9. Trình duyệt đã gửi bao nhiêu HTTP GET? Đến những địa chỉ IP nào?

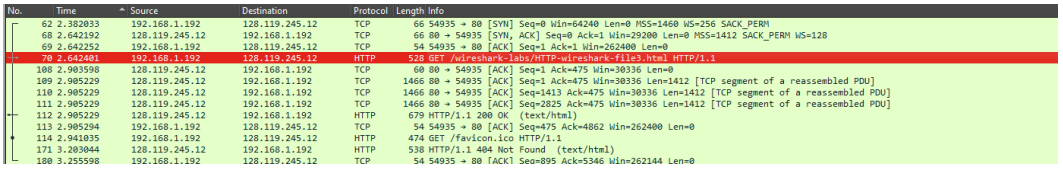
Trình duyệt đã gửi 4 HTTP GET đến server (cả sau khi refresh, mỗi lần 2 gói tin HTTP GET) đến những địa chỉ IP: 192.168.43.23 và 45.122.249.78



No.	Time	Source	Destination	Protocol	Length	Info
2641	11.497269	192.168.43.47	192.168.43.23	HTTP	502	GET /23520617.html HTTP/1.1
3766	18.267239	192.168.43.47	192.168.43.23	HTTP	614	GET /23520617.html HTTP/1.1
2891	12.468267	192.168.43.47	45.122.249.78	HTTP	459	GET /Styles/profi/images/logo186x150.png HTTP/1.1
3768	18.376805	192.168.43.47	45.122.249.78	HTTP	459	GET /Styles/profi/images/logo186x150.png HTTP/1.1

10. Trình duyệt đã gửi bao nhiêu HTTP GET?

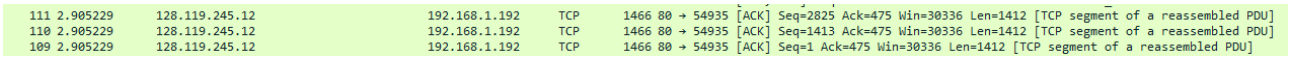
    Trình duyệt đã gửi 2 file HTTP GET, gói tin thứ 70 (yêu cầu file HTML) và gói tin 114 (yêu cầu favico.ico/ biểu tượng trang web)



No.	Time	Source	Destination	Protocol	Length	Info
62	2.382033	192.168.1.192	128.119.245.12	TCP	66	54935 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
68	2.642192	128.119.245.12	192.168.1.192	TCP	66	80 → 54935 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412 SACK_PERM WS=128
69	2.642252	192.168.1.192	128.119.245.12	TCP	54	54935 → 80 [ACK] Seq=1 Ack=1 Win=262400 Len=0
70	2.642401	192.168.1.192	128.119.245.12	HTTP	528	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
108	2.903598	128.119.245.12	192.168.1.192	TCP	60	80 → 54935 [ACK] Seq=1 Ack=475 Win=30336 Len=0
109	2.905229	128.119.245.12	192.168.1.192	TCP	1466	80 → 54935 [ACK] Seq=1 Ack=475 Win=30336 Len=1412 [TCP segment of a reassembled PDU]
110	2.905229	128.119.245.12	192.168.1.192	TCP	1466	80 → 54935 [ACK] Seq=1413 Ack=475 Win=30336 Len=1412 [TCP segment of a reassembled PDU]
111	2.905229	128.119.245.12	192.168.1.192	TCP	1466	80 → 54935 [ACK] Seq=2825 Ack=475 Win=30336 Len=1412 [TCP segment of a reassembled PDU]
112	2.905229	128.119.245.12	192.168.1.192	HTTP	679	HTTP/1.1 200 OK (text/html)
113	2.905294	192.168.1.192	128.119.245.12	TCP	54	54935 → 80 [ACK] Seq=475 Ack=4862 Win=262400 Len=0
114	2.941035	192.168.1.192	128.119.245.12	HTTP	474	GET /favicon.ico HTTP/1.1
171	3.203044	128.119.245.12	192.168.1.192	HTTP	538	HTTP/1.1 404 Not Found (text/html)
180	3.255598	192.168.1.192	128.119.245.12	TCP	54	54935 → 80 [ACK] Seq=895 Ack=5346 Win=262144 Len=0

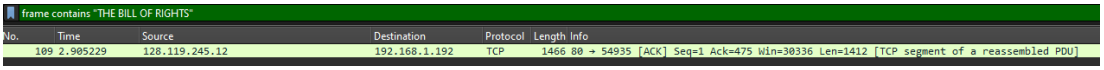
11. Cần bao nhiêu TCP segments để chứa hết HTTP response và nội dung của The Bill of Rights?

    Có 3 TCP segments để chứa hết HTTP response và nội dung của The Bill of Rights



111	2.905229	128.119.245.12	192.168.1.192	TCP	1466	80 → 54935 [ACK] Seq=2825 Ack=475 Win=30336 Len=1412 [TCP segment of a reassembled PDU]
110	2.905229	128.119.245.12	192.168.1.192	TCP	1466	80 → 54935 [ACK] Seq=1413 Ack=475 Win=30336 Len=1412 [TCP segment of a reassembled PDU]
109	2.905229	128.119.245.12	192.168.1.192	TCP	1466	80 → 54935 [ACK] Seq=1 Ack=475 Win=30336 Len=1412 [TCP segment of a reassembled PDU]

12. Dòng chữ "THE BILL OF RIGHTS" được chứa trong gói tin phản hồi thứ mấy?

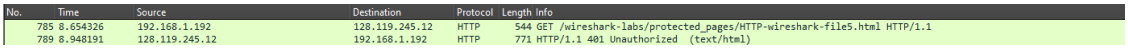


frame contains "THE BILL OF RIGHTS"

No.	Time	Source	Destination	Protocol	Length	Info
109	2.905229	128.119.245.12	192.168.1.192	TCP	1466	80 → 54935 [ACK] Seq=1 Ack=475 Win=30336 Len=1412 [TCP segment of a reassembled PDU]

Gói tin thứ 109 chứa dòng chữ "THE BILL OF RIGHTS"

13. Mã trạng thái và ý nghĩa nó trong HTTP response tương ứng với HTTP GET đầu tiên là gì?



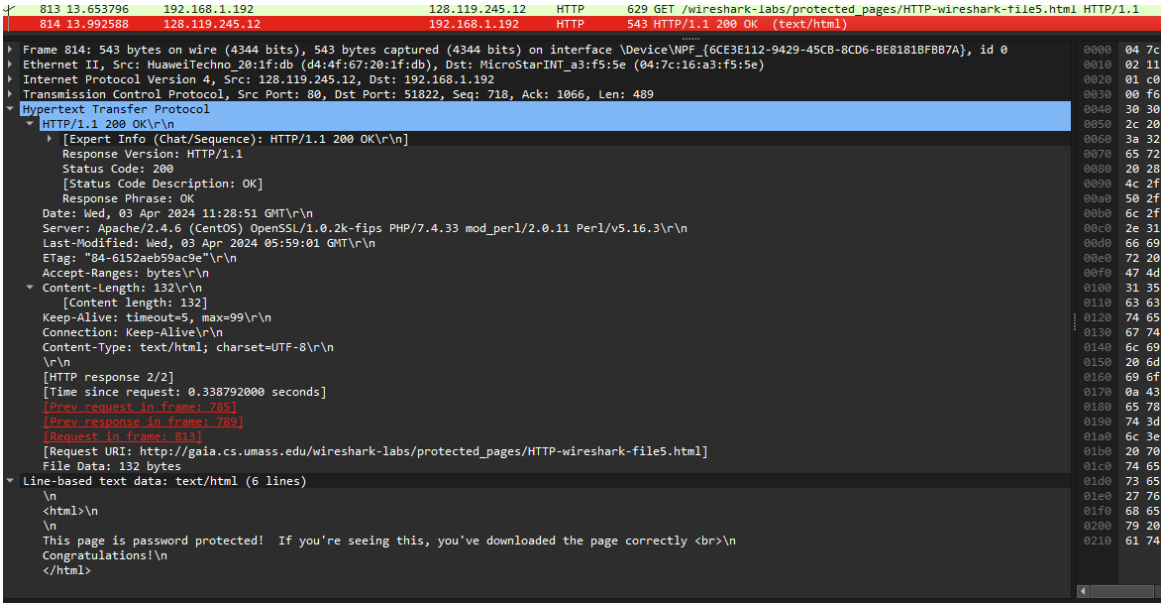
No.	Time	Source	Destination	Protocol	Length	Info
785	8.654326	192.168.1.192	128.119.245.12	HTTP	544	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
789	8.948191	128.119.245.12	192.168.1.192	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)

Mã trạng thái HTTP response tương ứng với HTTP GET đầu tiên là 401 Unauthorized.

Ý nghĩa 401 unauthorized được trả về bởi máy chủ web để cho biết rằng truy cập vào tài nguyên được yêu cầu bị từ chối do không có thông tin xác thực hợp lệ

14. Khi trình duyệt gửi HTTP GET lần thứ 2, trường dữ liệu nào mới nào xuất hiện trong HTTP GET?

Khi trình duyệt gửi HTTP GET lần thứ 2, trường dữ liệu mới kèm status code 200 OK kèm theo nội dụng trang web



```
813 13.653796   192.168.1.192   128.119.245.12   HTTP   629 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
814 13.992588   128.119.245.12  192.168.1.192    HTTP   543 HTTP/1.1 200 OK  (text/html)

Frame 814: 543 bytes on wire (4344 bits), 543 bytes captured (4344 bits) on interface \Device\NPF_{6CE3E112-9429-45CB-8CD6-BE8181BFBB7A}, id 0
Ethernet II, Src: HuaweiTechno_20:1f:db (d4:4f:67:20:1f:db), Dst: MicroStarINT_a3:f5:5e (04:7c:16:a3:f5:5e)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.192
Transmission Control Protocol, Src Port: 80, Dst Port: 51822, Seq: 718, Ack: 1066, Len: 489
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: Wed, 03 Apr 2024 11:28:51 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
  Last-Modified: Wed, 03 Apr 2024 05:59:01 GMT\r\n
  ETag: "84-6152aeb59ac9e"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 132\r\n
    [Content length: 132]
  Keep-Alive: timeout=5, max=99\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [HTTP response 2/2]
  [Time since request: 0.338792000 seconds]
  [Prev request in frame: 785]
  [Prev response in frame: 789]
  [Request in frame: 813]
  [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)
  \n
  <html>\n
  \n
  This page is password protected!  If you're seeing this, you've downloaded the page correctly <br>\n
  Congratulations!\n
  </html>

0000  04 7c 16 a3 f5 5e d4 4f 67 20 1f db 08 00 45 00
0010  02 11 ...
0020  01 c0 ...
0030  00 f6 ...
0040  30 30 ...
0050  2c 20 ...
0060  3a 32 ...
0070  65 72 ...
0080  20 28 ...
0090  4c 2f ...
00a0  50 2f ...
00b0  6c 2f ...
00c0  2e 31 ...
00d0  66 69 ...
00e0  72 20 ...
00f0  47 4d ...
0100  31 35 ...
0110  63 63 ...
0120  74 65 ...
0130  67 74 ...
0140  6c 69 ...
0150  20 6d ...
0160  69 6f ...
0170  0a 43 ...
0180  65 78 ...
0190  74 3d ...
01a0  6c 3e ...
01b0  20 70 ...
01c0  74 65 ...
01d0  73 65 ...
01e0  27 76 ...
01f0  68 65 ...
0200  79 20 ...
0210  61 74 ...
```