Lab 1

BÁO CÁO BÀI THỰC HÀNH SỐ 1

Làm quen với Wireshark

Wireshark Getting Started

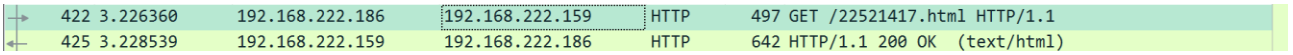
Môn học: Nhập môn Mạng máy tính

Sinh viên thực hiện	Dương Thuận Trí (22521517)
Thời gian thực hiện	11/10/2023- 18/10/2023
Tự chấm điểm	10/10

TRẢ LỜI CÁC CÂU HỎI

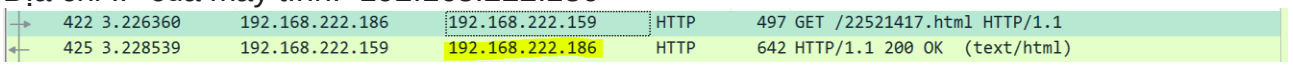
Câu 1: Trình duyệt đang sử dụng phiên bản HTTP 1.0 hay 1.1? Phiên bản HTTP server đang sử dụng là bao nhiêu?

- Trình duyệt đang sử dụng phiên bản HTTP 1.1
- Phiên bản HTTP sever đang sử dụng là 1.1

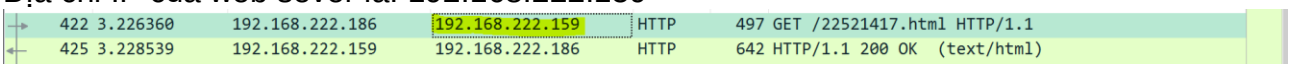


Câu 2: Địa chỉ IP của máy tính bạn là bao nhiêu? Của web server là bao nhiêu?

- Địa chỉ IP của máy tính: 192.168.222.186

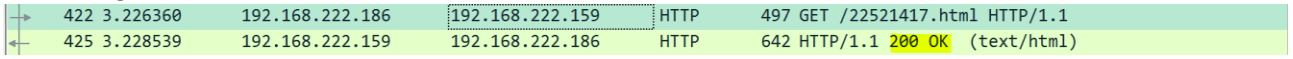


- Địa chỉ IP của web sever là: 192.168.222.159



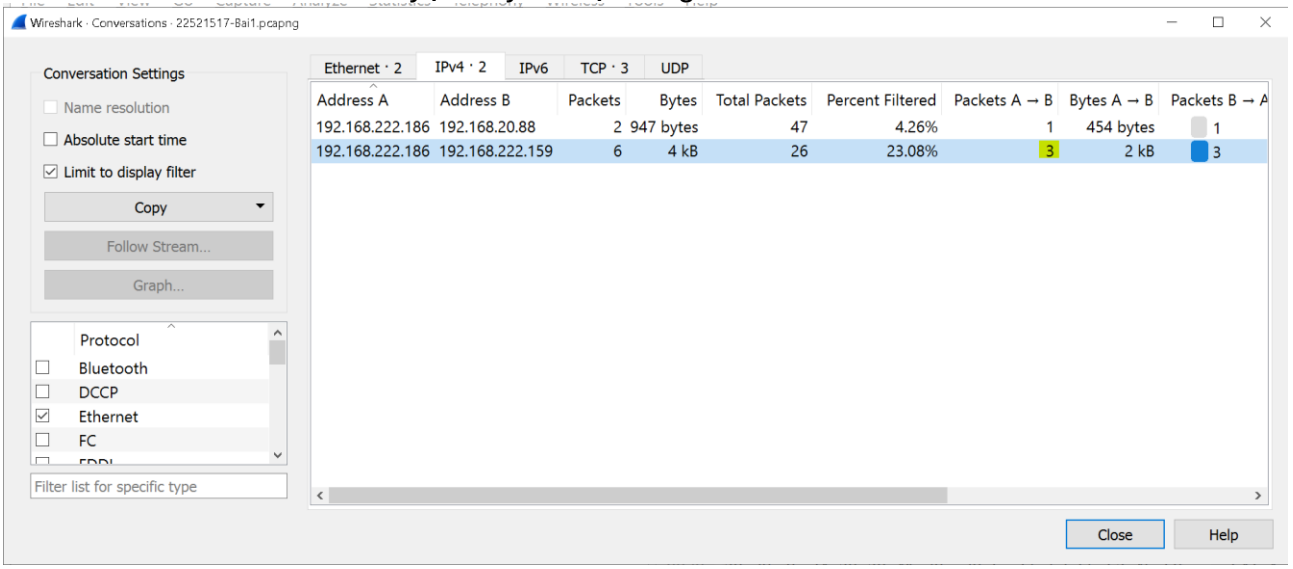
Câu 3: Các mã trạng thái (status code) trả về từ server là gì?

- Mã trạng thái trả về từ sever là: 200



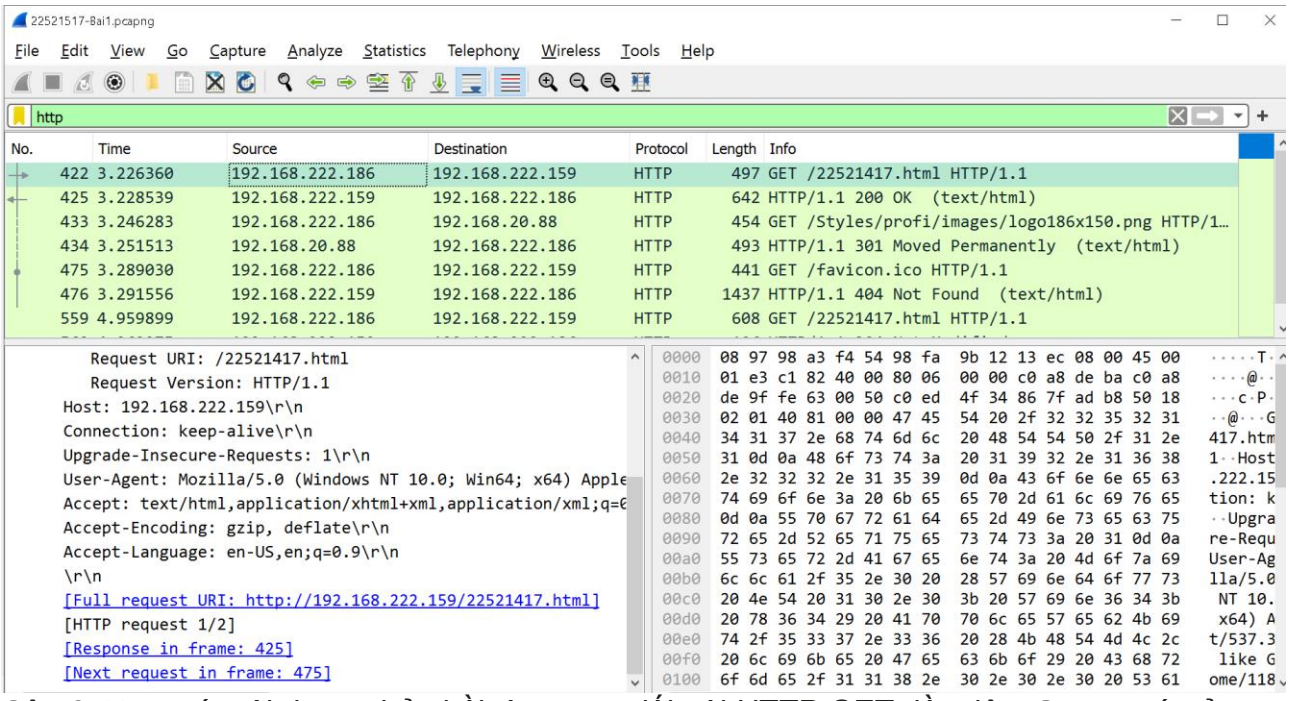
Câu 4: Server đã trả về cho trình duyệt tổng cộng bao nhiêu bytes nội dung?

- Server đã trả về cho trình duyệt 3 bytes nội dung



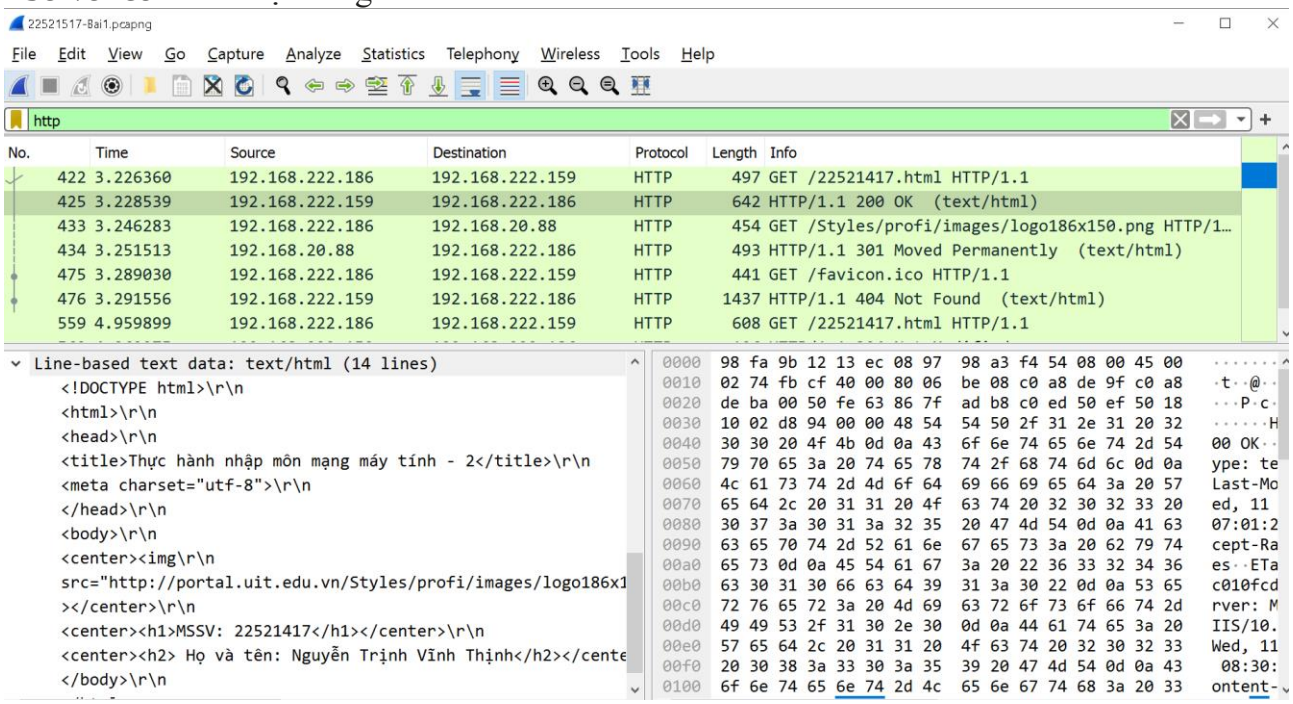
Câu 5: Xem xét nội dung của HTTP GET đầu tiên. Bạn có thấy dòng "IF-MODIFIED-SINCE" hay không?

- Dòng "IF-MODIFIED-SINCE" không có trong nội dung của HTTP GET đầu tiên.



Câu 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.

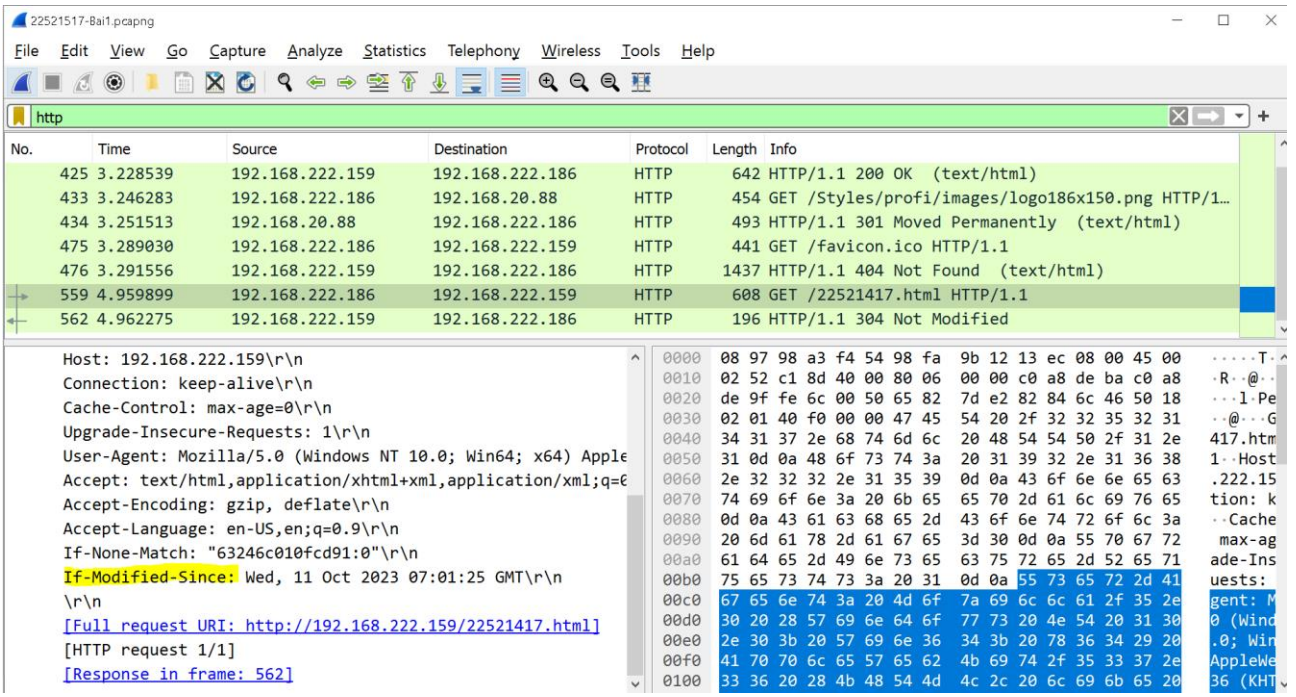
- Server có trả về nội dung của file HTML.



- Mã trạng thái đi kèm là: 200 (mô tả mã trạng thái: OK)
- Ý nghĩa: phản hồi tiêu chuẩn cho các yêu cầu HTTP thành công.

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

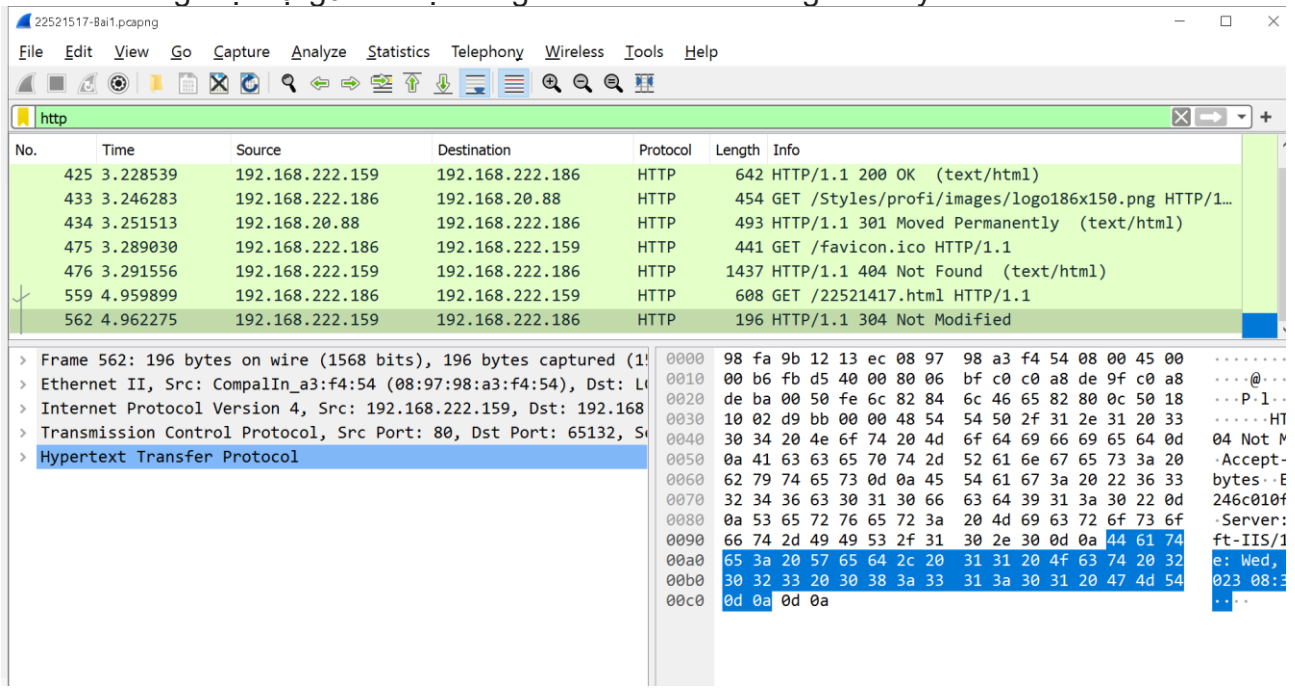
- HTTP GET thứ 2 có dòng “IF-MODIFIED-SINCE”



- Giá trị của IF-MODIFIED-SINCE là: Wed, 11 Oct 2023 07:01:25 GMT\r\n

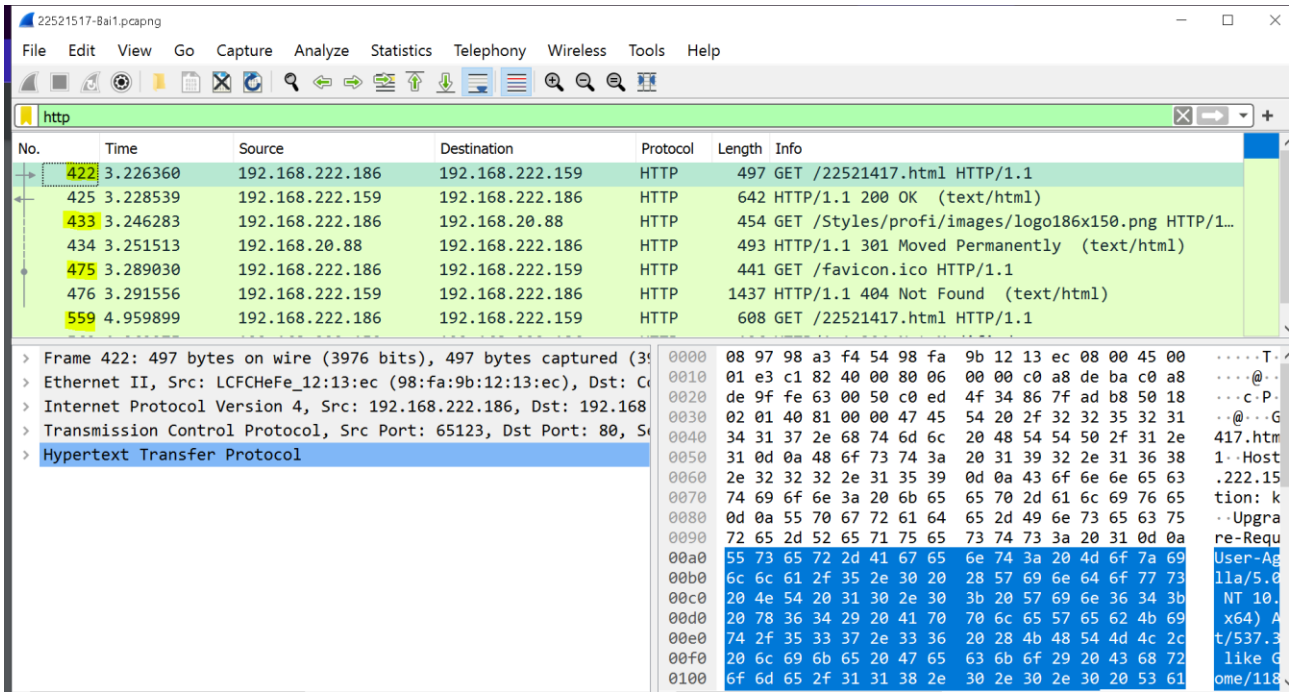
Câu 8: Mã trạng thái HTTP được trả về từ server tương ứng với HTTP GET thứ 2 là gì? Ý nghĩa nó là gì? Server có thật sự gửi về nội dung của file hay không? Giải thích.

- Mã trạng thái: 304 (mô tả mã trạng thái: Not Modified)
- Ý nghĩa: Nếu header yêu cầu bao gồm tham số 'if modified since', mã trạng thái này sẽ được trả về, trong trường hợp file không thay đổi kể từ ngày đó.
- Server không thật sự gửi về nội dung của file vì file không có thay đổi nào.



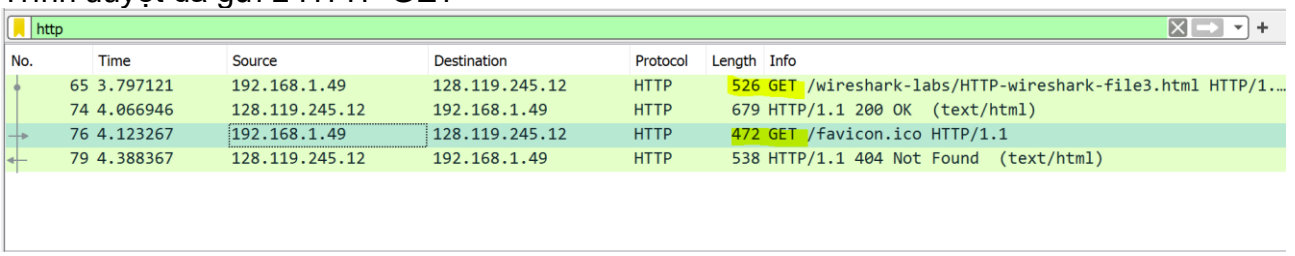
Câu 9: Trình duyệt đã gửi bao nhiêu HTTP GET? Đến những địa chỉ IP nào?

- Trình duyệt đã gửi 4 HTTP GET
- Đến những địa chỉ: 192.168.222.159, 192.168.20.88.



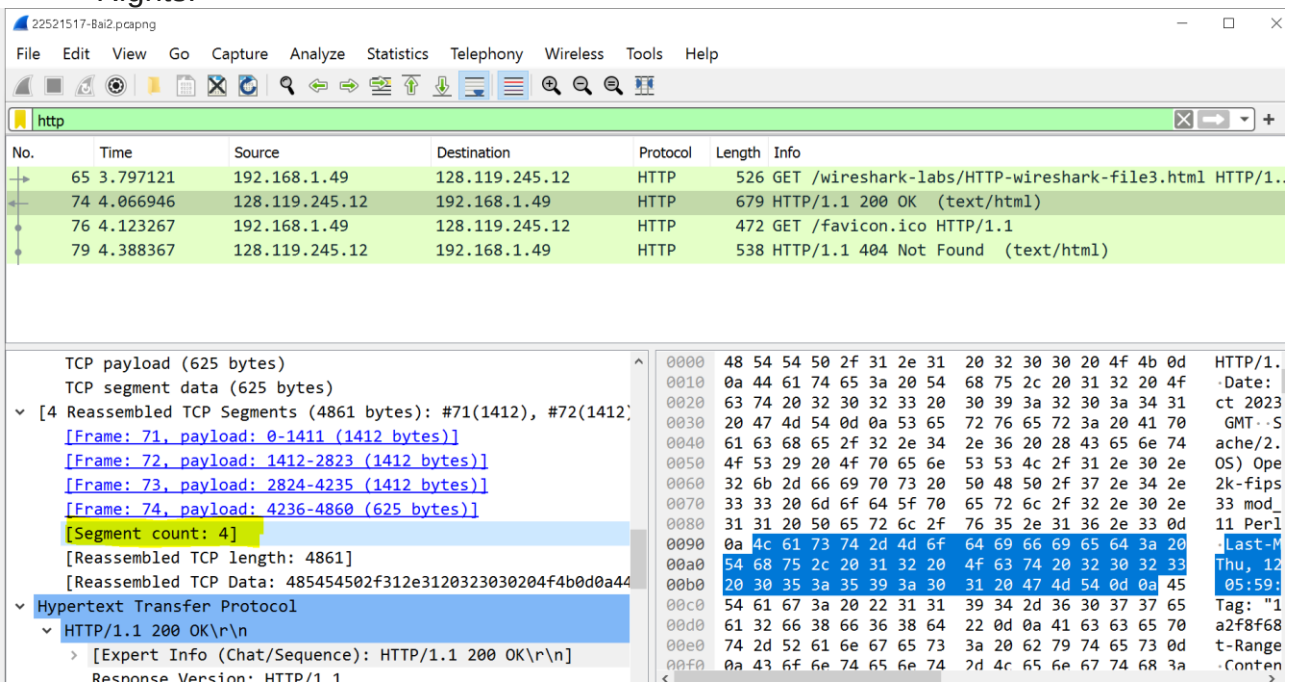
Câu 10: Trình duyệt đã gửi bao nhiêu HTTP GET?

- Trình duyệt đã gửi 2 HTTP GET



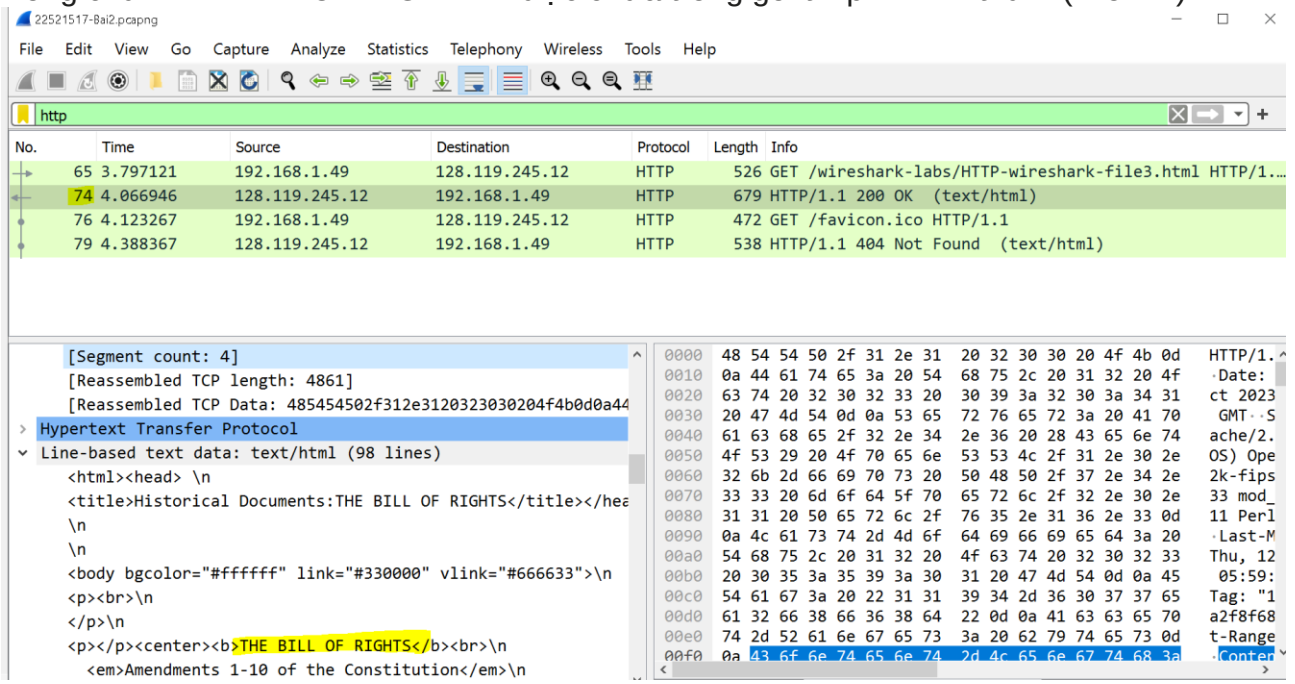
Câu 11: Cần bao nhiêu TCP segments để chứa hết HTTP response và nội dung của The Bill of Rights?

- Cần 4 TCP segments để chứa hết HTTP response và nội dung của The Bill of Rights.



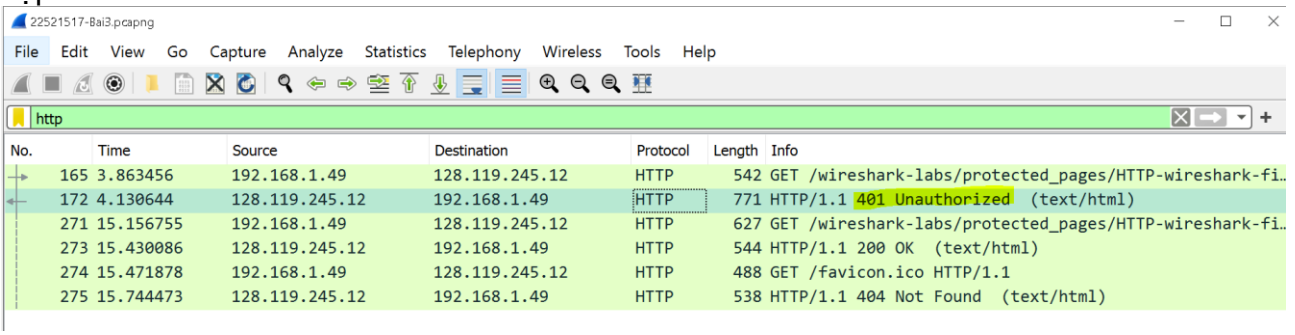
Câu 12: Dòng chữ “THE BILL OF RIGHTS” được chứa trong gói tin phản hồi thứ mấy?

- Dòng chữ “THE BILL OF RIGHTS” được chứa trong gói tin phản hồi thứ 1 (No. 74)



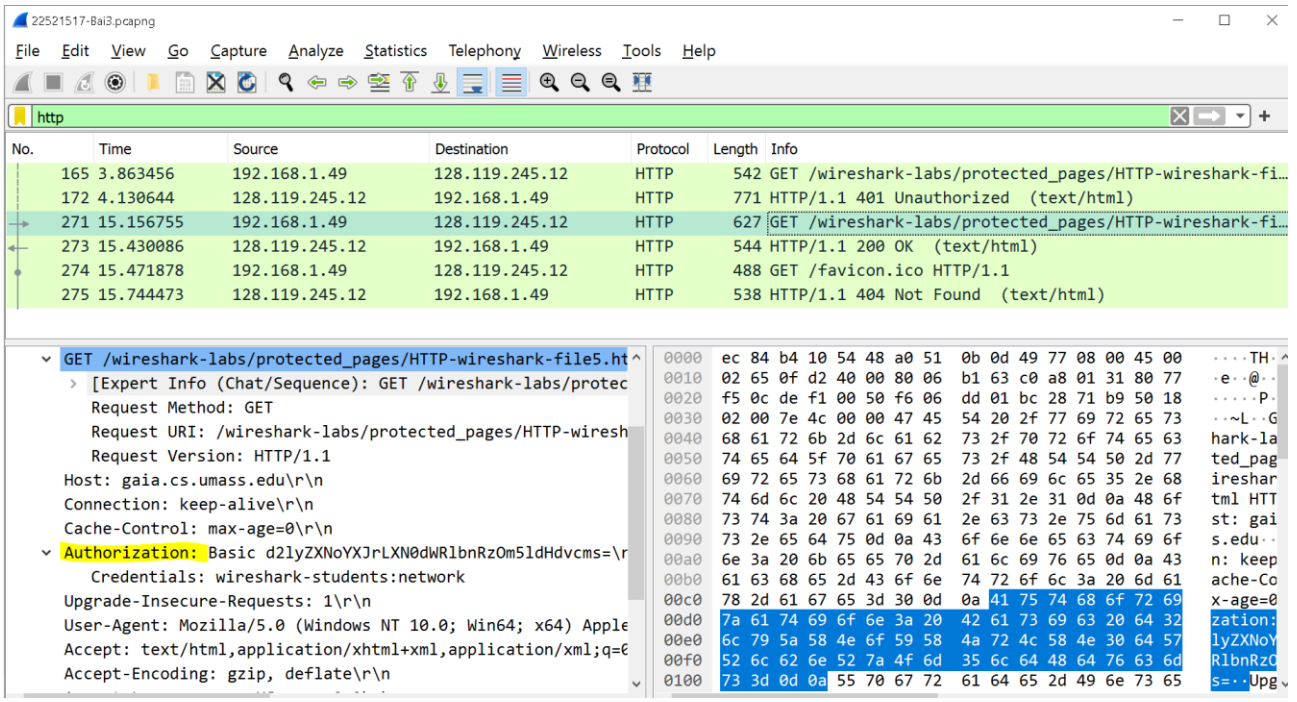
Câu 13: Mã trạng thái và ý nghĩa nó trong HTTP response tương ứng với HTTP GET đầu tiên là gì?

- Mã trạng thái: 401
- Mô tả mã trạng thái: Unauthorized
- Ý nghĩa: Header yêu cầu không chứa mã xác thực cần thiết và client bị từ chối truy cập.



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

- Khi trình duyệt gửi HTTP GET lần thứ 2, trường dữ liệu Authorization xuất hiện, vì lúc này những thông tin xác thực đã được cấp (username, password).


22521517-Bai3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
165 3.863456 192.168.1.49 128.119.245.12 HTTP 542 GET /wireshark-labs/protected_pages/HTTP-wireshark-fi…
172 4.130644 128.119.245.12 192.168.1.49 HTTP 771 HTTP/1.1 401 Unauthorized (text/html)
271 15.156755 192.168.1.49 128.119.245.12 HTTP 627 GET /wireshark-labs/protected_pages/HTTP-wireshark-fi…
273 15.430086 128.119.245.12 192.168.1.49 HTTP 544 HTTP/1.1 200 OK (text/html)
274 15.471878 192.168.1.49 128.119.245.12 HTTP 488 GET /favicon.ico HTTP/1.1
275 15.744473 128.119.245.12 192.168.1.49 HTTP 538 HTTP/1.1 404 Not Found (text/html)
GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.ht
[Expert Info (Chat/Sequence): GET /wireshark-labs/protec
Request Method: GET
Request URI: /wireshark-labs/protected_pages/HTTP-wiresh
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
Credentials: wireshark-students:network
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Apple
Accept: text/html,application/xhtml+xml,application/xml;q=0
Accept-Encoding: gzip, deflate\r\n
0000 ec 84 b4 10 54 48 a0 51 0b 0d 49 77 08 00 45 00
0010 02 65 0f d2 40 00 80 06 b1 63 c0 a8 01 31 80 77
0020 f5 0c de f1 00 50 f6 06 dd 01 bc 28 71 b9 50 18
0030 02 00 7e 4c 00 00 47 45 54 20 2f 77 69 72 65 73
0040 68 61 72 6b 2d 6c 61 62 73 2f 70 72 6f 74 65 63
0050 74 65 64 5f 70 61 67 65 73 2f 48 54 54 50 2d 77
0060 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 35 2e 68
0070 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f
0080 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73
0090 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f
00a0 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43
00b0 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61
00c0 78 2d 61 67 65 3d 30 0d 0a 41 75 74 68 6f 72 69
00d0 7a 61 74 69 6f 6e 3a 20 42 61 73 69 63 20 64 32
00e0 6c 79 5a 58 4e 6f 59 58 4a 72 4c 58 4e 30 64 57
00f0 52 6c 62 6e 52 7a 4f 6d 35 6c 64 48 64 76 63 6d
0100 73 3d 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65