Lab 2

BÁO CÁO BÀI THỰC HÀNH SỐ 2

Phân tích gói tin HTTP với Wireshark

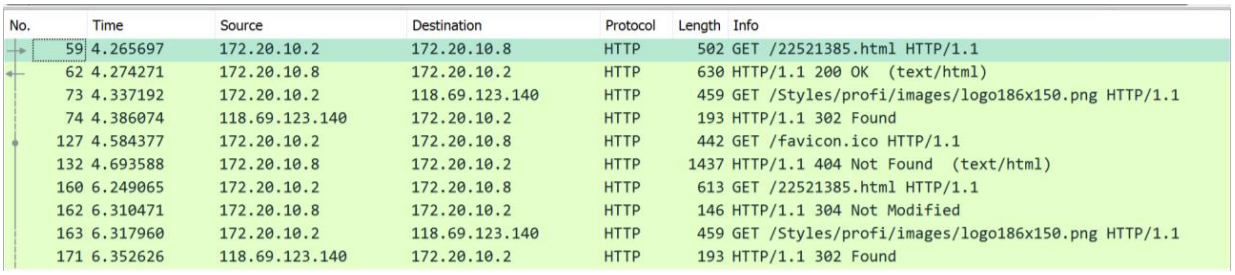
Sniffing HTTP Traffic with Wireshark

Môn học: Nhập môn Mạng máy tính

Sinh viên thực hiện	Đặng Đức Tài (22521270)
Thời gian thực hiện	15/11/2023 – 20/11/2023
Tự chấm điểm	10/10

B. THỰC HÀNH

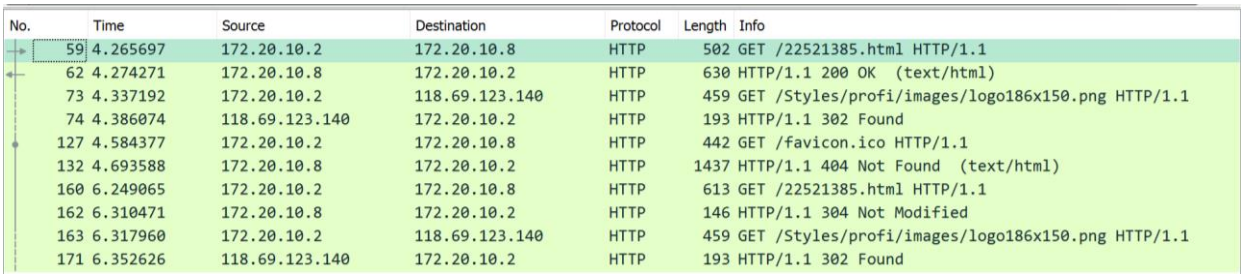
1. *Trình duyệt đang sử dụng phiên bản HTTP 1.0 hay 1.1? Phiên bản HTTP server đang sử dụng là bao nhiêu?*



No.	Time	Source	Destination	Protocol	Length	Info
59	4.265697	172.20.10.2	172.20.10.8	HTTP	502	GET /22521385.html HTTP/1.1
62	4.274271	172.20.10.8	172.20.10.2	HTTP	630	HTTP/1.1 200 OK (text/html)
73	4.337192	172.20.10.2	118.69.123.140	HTTP	459	GET /Styles/profi/images/logo186x150.png HTTP/1.1
74	4.386074	118.69.123.140	172.20.10.2	HTTP	193	HTTP/1.1 302 Found
127	4.584377	172.20.10.2	172.20.10.8	HTTP	442	GET /favicon.ico HTTP/1.1
132	4.693588	172.20.10.8	172.20.10.2	HTTP	1437	HTTP/1.1 404 Not Found (text/html)
160	6.249065	172.20.10.2	172.20.10.8	HTTP	613	GET /22521385.html HTTP/1.1
162	6.310471	172.20.10.8	172.20.10.2	HTTP	146	HTTP/1.1 304 Not Modified
163	6.317960	172.20.10.2	118.69.123.140	HTTP	459	GET /Styles/profi/images/logo186x150.png HTTP/1.1
171	6.352626	118.69.123.140	172.20.10.2	HTTP	193	HTTP/1.1 302 Found

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

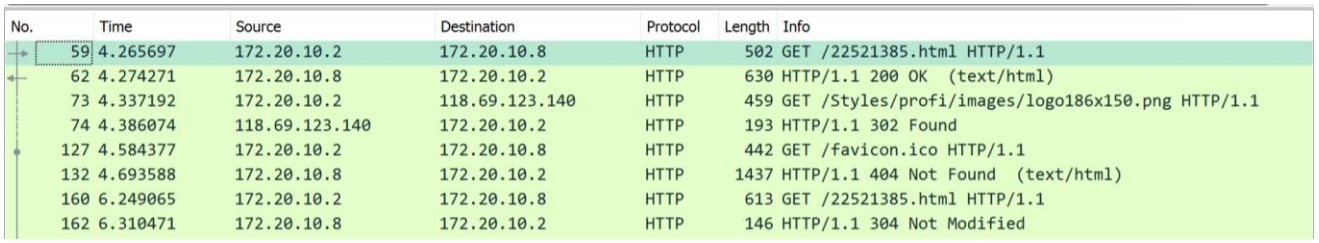
2. *Địa chỉ IP của máy tính bạn là bao nhiêu? Của web server là bao nhiêu?*



No.	Time	Source	Destination	Protocol	Length	Info
59	4.265697	172.20.10.2	172.20.10.8	HTTP	502	GET /22521385.html HTTP/1.1
62	4.274271	172.20.10.8	172.20.10.2	HTTP	630	HTTP/1.1 200 OK (text/html)
73	4.337192	172.20.10.2	118.69.123.140	HTTP	459	GET /Styles/profi/images/logo186x150.png HTTP/1.1
74	4.386074	118.69.123.140	172.20.10.2	HTTP	193	HTTP/1.1 302 Found
127	4.584377	172.20.10.2	172.20.10.8	HTTP	442	GET /favicon.ico HTTP/1.1
132	4.693588	172.20.10.8	172.20.10.2	HTTP	1437	HTTP/1.1 404 Not Found (text/html)
160	6.249065	172.20.10.2	172.20.10.8	HTTP	613	GET /22521385.html HTTP/1.1
162	6.310471	172.20.10.8	172.20.10.2	HTTP	146	HTTP/1.1 304 Not Modified
163	6.317960	172.20.10.2	118.69.123.140	HTTP	459	GET /Styles/profi/images/logo186x150.png HTTP/1.1
171	6.352626	118.69.123.140	172.20.10.2	HTTP	193	HTTP/1.1 302 Found

- Địa chỉ IP của máy tính là: 172.20.10.2
- Địa chỉ IP của Web Server là: 172.20.10.8

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



No.	Time	Source	Destination	Protocol	Length	Info
59	4.265697	172.20.10.2	172.20.10.8	HTTP	502	GET /22521385.html HTTP/1.1
62	4.274271	172.20.10.8	172.20.10.2	HTTP	630	HTTP/1.1 200 OK (text/html)
73	4.337192	172.20.10.2	118.69.123.140	HTTP	459	GET /Styles/profi/images/logo186x150.png HTTP/1.1
74	4.386074	118.69.123.140	172.20.10.2	HTTP	193	HTTP/1.1 302 Found
127	4.584377	172.20.10.2	172.20.10.8	HTTP	442	GET /favicon.ico HTTP/1.1
132	4.693588	172.20.10.8	172.20.10.2	HTTP	1437	HTTP/1.1 404 Not Found (text/html)
160	6.249065	172.20.10.2	172.20.10.8	HTTP	613	GET /22521385.html HTTP/1.1
162	6.310471	172.20.10.8	172.20.10.2	HTTP	146	HTTP/1.1 304 Not Modified

- Các mã trạng thái (status code) trả về từ Server là: 200 OK, 302 Found, 404 Not Found, 304 Not Modified, 302 Found.

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

No.	Time	Source	Destination	Protocol	Length	Info
59	4.265697	172.20.10.2	172.20.10.8	HTTP	502	GET /22521385.html HTTP/1.1
62	4.274271	172.20.10.8	172.20.10.2	HTTP	630	HTTP/1.1 200 OK (text/html)
73	4.337192	172.20.10.2	118.69.123.140	HTTP	459	GET /Styles/profi/images/logo186x150.png HTTP/1.1
74	4.386074	118.69.123.140	172.20.10.2	HTTP	193	HTTP/1.1 302 Found
127	4.584377	172.20.10.2	172.20.10.8	HTTP	442	GET /favicon.ico HTTP/1.1
132	4.693588	172.20.10.8	172.20.10.2	HTTP	1437	HTTP/1.1 404 Not Found (text/html)
160	6.249065	172.20.10.2	172.20.10.8	HTTP	613	GET /22521385.html HTTP/1.1
162	6.310471	172.20.10.8	172.20.10.2	HTTP	146	HTTP/1.1 304 Not Modified

- Server đã trả về cho trình duyệt tổng cộng 630 + 193 + 1437 + 146 = ***2406 bytes***.

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

```
Hypertext Transfer Protocol
  GET /22521385.html HTTP/1.1\r\n
  Host: 172.20.10.8\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) Chr
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: vi,en-US;q=0.9,en;q=0.8\r\n
```

- Không có dòng "IF-MODIFIED-SINCE".

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.***

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Content-Type: text/html\r\n
  Last-Modified: Wed, 15 Nov 2023 07:05:31 GMT\r\n
  Accept-Ranges: bytes\r\n
  ETag: "575ba1f9217da1:0"\r\n
  Server: Microsoft-IIS/10.0\r\n
  Date: Wed, 15 Nov 2023 08:40:52 GMT\r\n
```

- Server có trả về nội dung của file HTML.

- Mã trạng thái đi kèm là 200 OK: Request đã được tiếp nhận và Web Server đã trả về tất cả nội dung được client yêu cầu

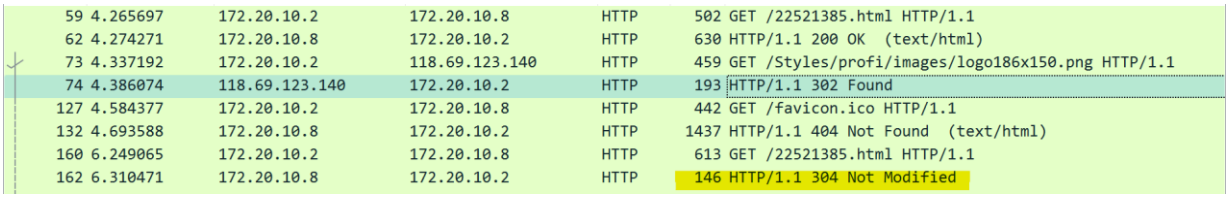
7. ***Xem xét nội dung của HTTP GET thứ 2. Bạn có thấy dòng "IF-MODIFIEDSINCE" hay không? Nếu có, giá trị của IF-MODIFIED-SINCE là gì?***

```
Hypertext Transfer Protocol
  GET /22521385.html HTTP/1.1\r\n
  Host: 172.20.10.8\r\n
  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 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chr
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: vi,en-US;q=0.9,en;q=0.8\r\n
  If-None-Match: "575ba1f9217da1:0"\r\n
  If-Modified-Since: Wed, 15 Nov 2023 07:05:31 GMT\r\n
```

- Có thấy "IF-MODIFIEDSINCE".

- Giá trị của IF-MODIFIEDSINCE: Wed, 15 Nov 2023 07:05:31 GMT\r\n

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.*



59	4.265697	172.20.10.2	172.20.10.8	HTTP	502 GET /22521385.html HTTP/1.1
62	4.274271	172.20.10.8	172.20.10.2	HTTP	630 HTTP/1.1 200 OK (text/html)
73	4.337192	172.20.10.2	118.69.123.140	HTTP	459 GET /Styles/profi/images/logo186x150.png HTTP/1.1
74	4.386074	118.69.123.140	172.20.10.2	HTTP	193 HTTP/1.1 302 Found
127	4.584377	172.20.10.2	172.20.10.8	HTTP	442 GET /favicon.ico HTTP/1.1
132	4.693588	172.20.10.8	172.20.10.2	HTTP	1437 HTTP/1.1 404 Not Found (text/html)
160	6.249065	172.20.10.2	172.20.10.8	HTTP	613 GET /22521385.html HTTP/1.1
162	6.310471	172.20.10.8	172.20.10.2	HTTP	146 HTTP/1.1 304 Not Modified

- Mã trạng thái HTTP được trả về từ web server tương ứng với HTTP GET thứ 2 là: 304 Not Modified.
- Ý nghĩa: Code này được sử dụng cho mục đích caching. Nó cho client biết rằng phản hồi chưa được điều chỉnh, nên client có thể tiếp tục sử dụng cùng phiên bản phản hồi trong bộ nhớ cache.
- Server không thực sự gửi về nội dung của file0.
- Giải thích: Đối tượng mà client yêu cầu ở GET thứ 2 (file html) không có bất kỳ sự thay đổi nào nên server trả về mã trạng thái 304: sử dụng lại nội dung được trả về trước đó được lưu trong cache

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

Trình duyệt đã gửi 5 HTTP GET đến các địa chỉ IP sau:

- 172.20.10.8
- 118.69.123.140

No.	Time	Source	Destination	Protocol	Length	Info
59	4.265697	172.20.10.2	172.20.10.8	HTTP	502	GET /22521385.html HTTP/1.1
62	4.274271	172.20.10.8	172.20.10.2	HTTP	630	HTTP/1.1 200 OK (text/html)
73	4.337192	172.20.10.2	118.69.123.140	HTTP	459	GET /Styles/profi/images/logo186x150.png HTTP/1.1
74	4.386074	118.69.123.140	172.20.10.2	HTTP	193	HTTP/1.1 302 Found
127	4.584377	172.20.10.2	172.20.10.8	HTTP	442	GET /favicon.ico HTTP/1.1
132	4.693588	172.20.10.8	172.20.10.2	HTTP	1437	HTTP/1.1 404 Not Found (text/html)
160	6.249065	172.20.10.2	172.20.10.8	HTTP	613	GET /22521385.html HTTP/1.1
162	6.310471	172.20.10.8	172.20.10.2	HTTP	146	HTTP/1.1 304 Not Modified
163	6.317960	172.20.10.2	118.69.123.140	HTTP	459	GET /Styles/profi/images/logo186x150.png HTTP/1.1
171	6.352626	118.69.123.140	172.20.10.2	HTTP	193	HTTP/1.1 302 Found

10. Trình duyệt đã gửi bao nhiêu HTTP GET?

- Trình duyệt đã gửi 2 gói tin HTTP GET.

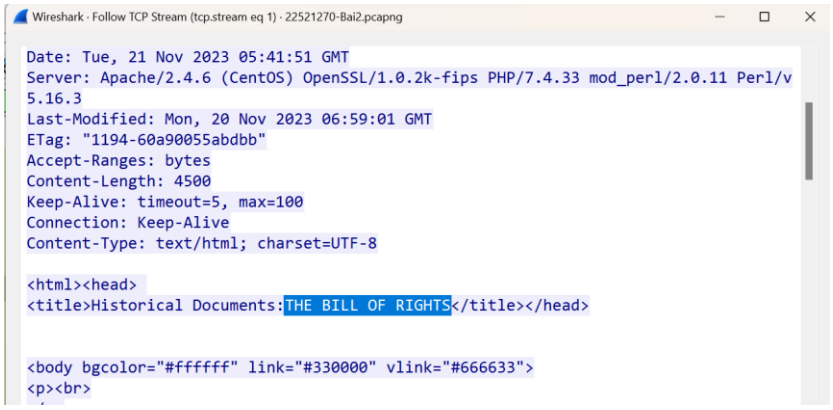
No.	Time	Source	Destination	Protocol	Length	Info
129	2.384838	172.30.189.3	128.119.245.12	HTTP	535	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
156	2.644326	128.119.245.12	172.30.189.3	HTTP	559	HTTP/1.1 200 OK (text/html)
164	2.678486	172.30.189.3	128.119.245.12	HTTP	481	GET /favicon.ico HTTP/1.1
169	2.937642	128.119.245.12	172.30.189.3	HTTP	538	HTTP/1.1 404 Not Found (text/html)

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

```
[2 Reassembled TCP Segments (4861 bytes): #155(4356), #156(505)]
    [Frame: 155, payload: 0-4355 (4356 bytes)]
    [Frame: 156, payload: 4356-4860 (505 bytes)]
```

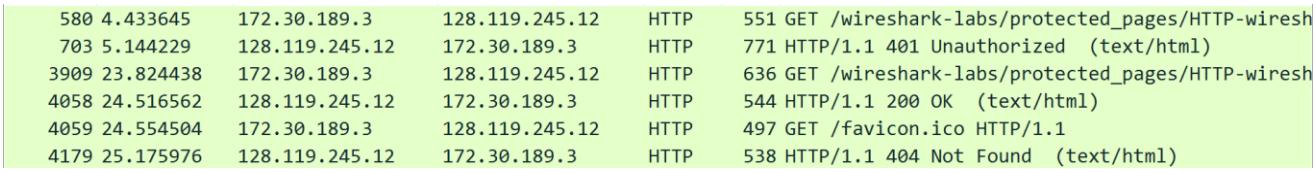
- Cần 2 TCP segments để chứa hết HTTP response và nội dung của The Bill of Rights.

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



- Dòng "THE BILL OF RIGHTS" được chứa trong gói tin phản hồi thứ nhất.

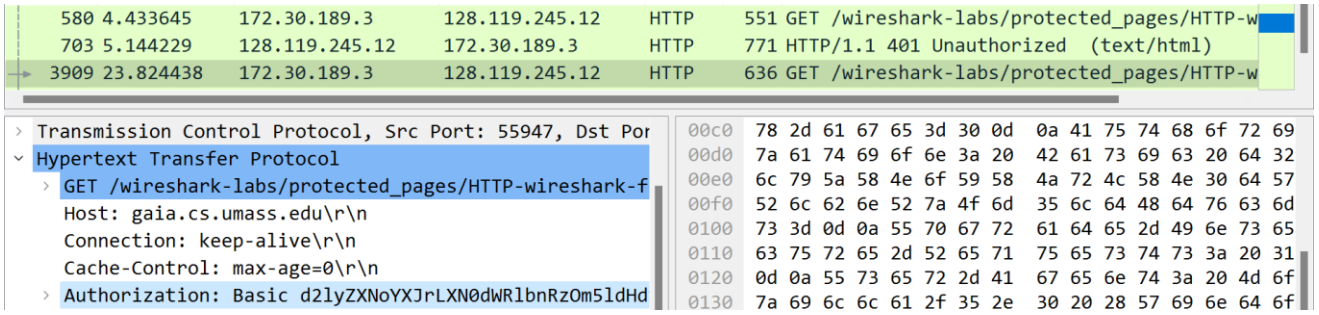
13. Mã trạng thái và ý nghĩa nó trong HTTP response tương ứng với HTTP GET đầu tiên là gì?



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

- Ý nghĩa: website đang tồn tại nhưng người truy cập không thể vào do không sở hữu quyền truy cập. Quyền truy cập có thể là ID người dùng kèm theo mật khẩu 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, xuất hiện một trường dữ liệu mới là trường Authorization trong HTTP GET.