Lab

2

Phân tích gói tin HTTP với Wireshark

Sniffing HTTP Traffic with Wireshark

Môn học: Nhập môn Mạng máy tính

1. HTTP GET/response có điều kiện

Dừng bắt gói tin và nhập "http" vào cửa sổ display-filter để hiển thị các thông điệp HTTP.

Trả lời các câu hỏi sau kèm theo hình ảnh minh chứng kết quả từ Wireshark:

1. Trình duyệt đang sử dụng phiên bản HTTP 1.0 hay 1.1? Phiên bản HTTP server đang sử dụng là bao nhiêu?
2. Địa chỉ IP của máy tính bạn là bao nhiêu? Của web server là bao nhiêu?
3. Mã trạng thái (status code) trả về từ server là gì?
4. Server đã trả về cho trình duyệt bao nhiêu bytes nội dung?
5. Xem xét nội dung của HTTP GET đầu tiên. Bạn có thấy dòng "IF-MODIFIED-SINCE" hay không?
6. Xem xét nội dung phản hồi từ server. Server có thật sự trả về nội dung của fileHTML hay không? Tại sao?
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?
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? Giảithích.
9. Trình duyệt đã gửi bao nhiêu HTTP GET? Đến những địa chỉ IP nào?

Trả lời:

1. Mở wireshark và tiến hành bắt gói tin, ta có:

```
2024-03-21 02:23:38.908229  192.168.217.57   192.168.217.137  192.168.217.137          HTTP    520 GET /23520027.html HTTP/1.1                192.168.217.57
2024-03-21 02:23:42.063048  192.168.217.137  192.168.217.57                            HTTP   1514 HTTP/1.1 200 OK  (text/html)       192.168.217.137
2024-03-21 02:23:44.648535  192.168.217.137  192.168.217.57                            HTTP   1201 Continuation                       192.168.217.137
2024-03-21 02:23:57.647697  192.168.217.57   192.168.217.137  192.168.217.137          HTTP    632 GET /23520027.html HTTP/1.1        192.168.217.57
2024-03-21 02:23:58.795210  192.168.217.137  192.168.217.57                            HTTP    197 HTTP/1.1 304 Not Modified          192.168.217.137
2024-03-21 02:24:28.387736  192.168.217.57   192.168.217.137  192.168.217.137          HTTP    632 GET /23520027.html HTTP/1.1        192.168.217.57
2024-03-21 02:24:33.649452  192.168.217.137  192.168.217.57                            HTTP    197 HTTP/1.1 304 Not Modified          192.168.217.137
```

-Ta có thể thấy rằng ở lần request đầu tiên:

```
520 GET /23520027.html HTTP/1.1
```

Trình duyệt đã sử dụng HTTP 1.1

-Ở lần request từ sever:

```
1514 HTTP/1.1 200 OK  (text/html)
```

Phiên bản HTTP server đang sử dụng là HTTP 1.1

2. Ta tiến hành phân tích sâu hơn:

```
2024-03-21 02:23:38.908229  192.168.217.57   192.168.217.137  192.168.217.137          HTTP    520 GET /23520027.html HTTP/1.1                192.168.217.57
2024-03-21 02:23:42.063048  192.168.217.137  192.168.217.57                            HTTP   1514 HTTP/1.1 200 OK  (text/html)             192.168.217.137
2024-03-21 02:23:44.648535  192.168.217.137  192.168.217.57                            HTTP   1201 Continuation                              192.168.217.137
2024-03-21 02:23:57.647697  192.168.217.57   192.168.217.137  192.168.217.137          HTTP    632 GET /23520027.html HTTP/1.1                192.168.217.57
2024-03-21 02:23:58.795210  192.168.217.137  192.168.217.57                            HTTP    197 HTTP/1.1 304 Not Modified                  192.168.217.137
2024-03-21 02:24:28.387736  192.168.217.57   192.168.217.137  192.168.217.137          HTTP    632 GET /23520027.html HTTP/1.1                192.168.217.57
2024-03-21 02:24:33.649452  192.168.217.137  192.168.217.57                            HTTP    197 HTTP/1.1 304 Not Modified                  192.168.217.137
```

-Từ thông tin trên, ta có thể thấy rằng:
+Địa chỉ IP của máy tính là: 192.168.212.57
+Địa chỉ IP của web sever là: 192.168.212.137

3. Mã trạng thái (status code) trả về từ server là: **200 OK**

4. Sever đã trả về cho client:

```
HTTP   1514 HTTP/1.1 200 OK  (text/html)
```

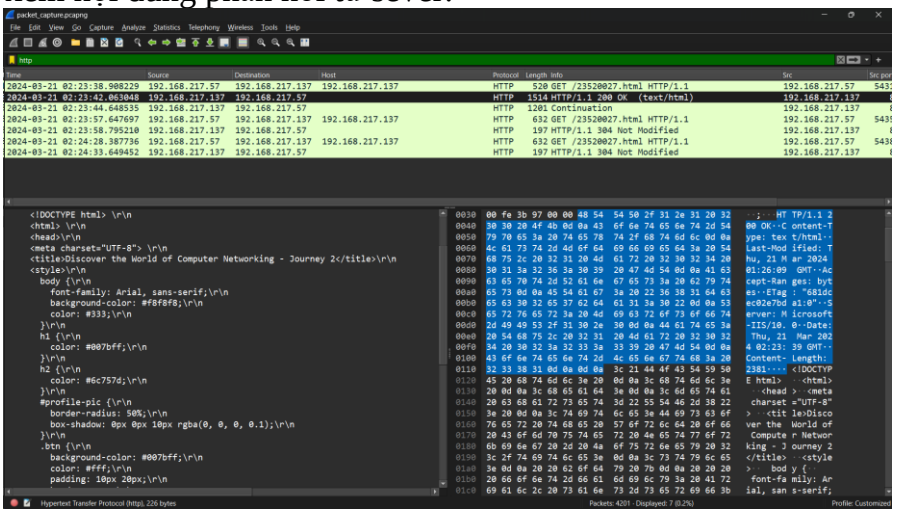
Dựa vào thông tin trên, server đã trả về cho trình duyệt 1514 bytes nội dung.

5. Ta tiến hành xem nội dung của HTTP GET đầu tiên:

```
Hypertext Transfer Protocol
  GET /23520027.html HTTP/1.1\r\n
  Host: 192.168.217.137\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,
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9,vi;q=0.8\r\n
  \r\n
  [Full request URI: http://192.168.217.137/23520027.html]
  [HTTP request 1/1]
  [Response in frame: 897]
```

Dựa vào thông tin trên, **không có** dòng "IF-MODIFIED-SINCE"

6. Ta tiến hành xem nội dung phản hồi từ sever:

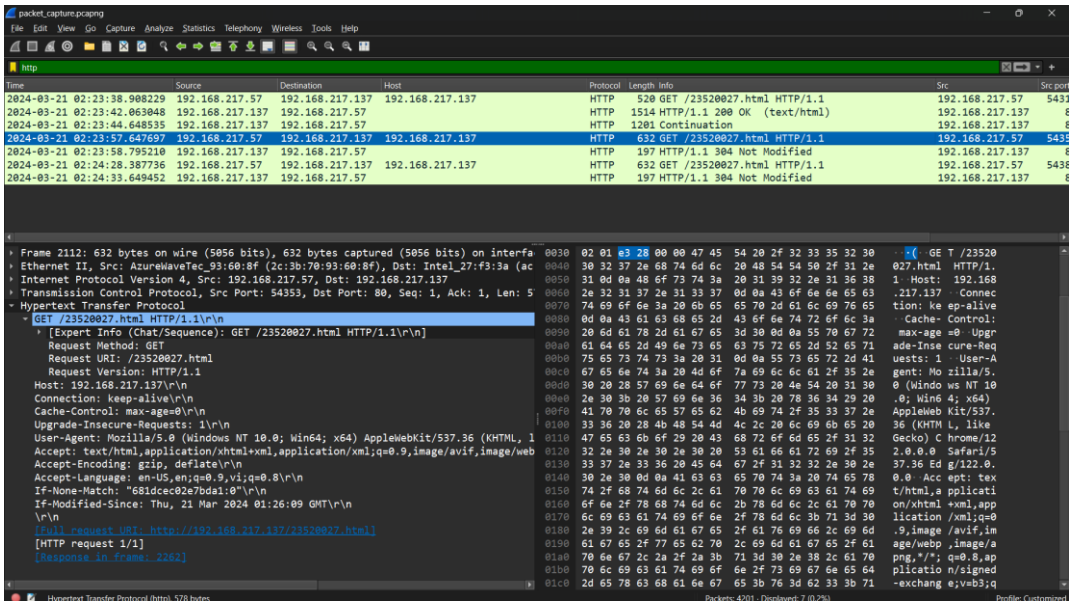


Xem xét nội dung phản hồi từ server. Server **trả về** nội dung của fileHTML

Lý do:

Vì ban đầu trước khi bắt gói tin, ta đã xóa cache rồi. Do đó, khi người dùng gửi request lên server, server sẽ kiểm tra xem trong cache có nội dung đó chưa. Nếu chưa thì server sẽ trả về nội dung của file đó cho người dùng. Ngược lại thì không. Vì trước khi bắt gói tin, ta đã xóa bộ nhớ cache rồi, nên server sẽ không tìm thấy file đó. Do đó, nội dung của file đó sẽ được trả về cho người dùng.

7. Tiến hành xem nội dung ở HTTP GET lần thứ 2:




```
If-Modified-Since: Thu, 21 Mar 2024 01:26:09 GMT\r\n
```

Ta có thể thấy rõ rằng có dòng "IF-MODIFIED- SINCE"

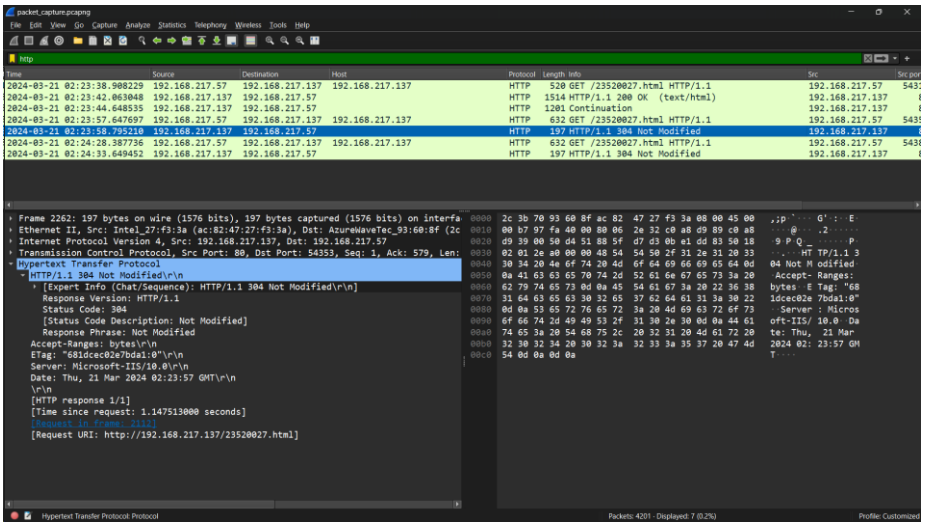
Giá trị của IF-MODIFIED-SINCE là: **Thu, 21 Mar 2024 01:26:09 GMT\r\n**

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

```
HTTP    197 HTTP/1.1 304 Not Modified
```

*Ý nghĩa nó là: Mã phản hồi HTTP 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.

*Ở lần bắt gói tin thứ 2:



Trong hình trên, ta thấy phần thông tin của gói tin đó không có chỗ nào hiển thị cho ta về nội dung của trang web như lần GET đầu tiên.

Giải thích: Vì lúc này, trong bộ nhớ cache của ta đã có nội dung của file đó ở lần gửi request đầu tiên (được minh chứng thông qua trạng thái 304 NOT MODIFIED được trả về), do đó, lúc này, server sẽ không gửi lại nội dung đó cho người dùng nữa.

9. Trình duyệt đã gửi 2 HTTP GET, và đến địa chỉ **192.168.212.137**.

Time	Source	Destination	Host	Protocol	Length	Info
2024-03-21 02:23:38.908229	192.168.217.57	192.168.217.137	192.168.217.137	HTTP	520	GET /23520027.html HTTP/1.1
2024-03-21 02:23:42.063048	192.168.217.137	192.168.217.57		HTTP	1514	HTTP/1.1 200 OK (text/html)
2024-03-21 02:23:44.648535	192.168.217.137	192.168.217.57		HTTP	1201	Continuation
2024-03-21 02:23:57.647697	192.168.217.57	192.168.217.137	192.168.217.137	HTTP	632	GET /23520027.html HTTP/1.1
2024-03-21 02:23:58.795210	192.168.217.137	192.168.217.57		HTTP	197	HTTP/1.1 304 Not Modified

2. Truy cập các trang HTTP dài

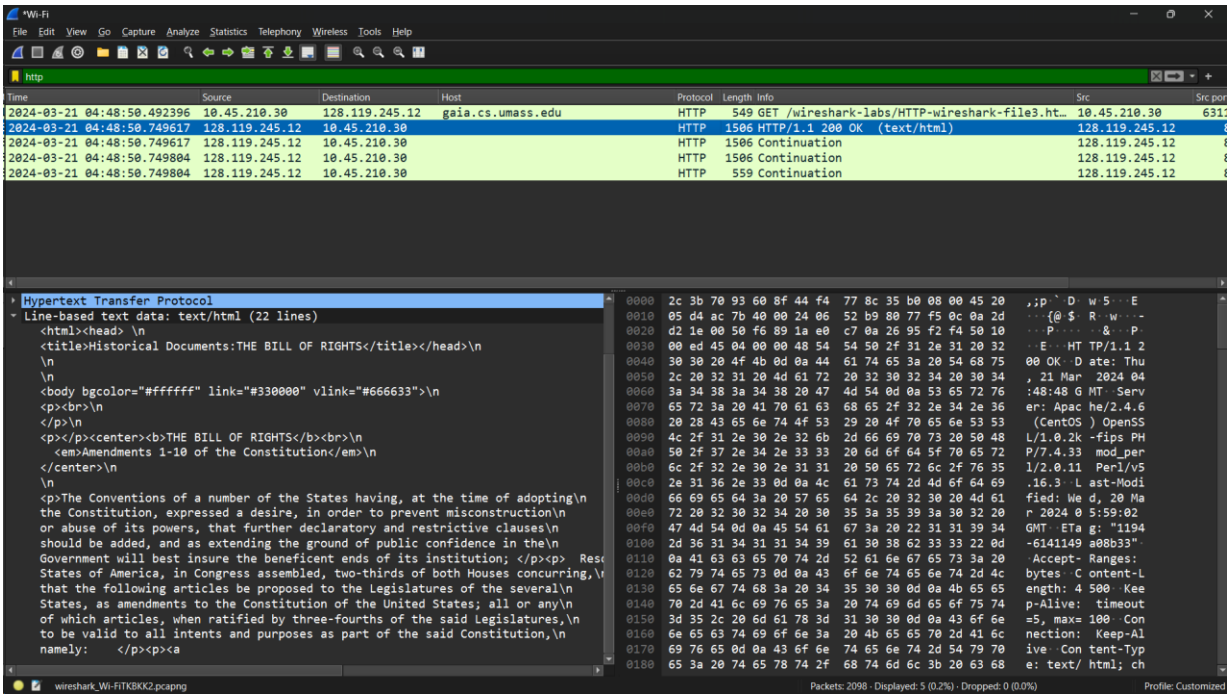
10. Trình duyệt đã gửi bao nhiêu HTTP GET? Dòng "**THE BILL OF RIGHTS**"được chứa trong gói tin phản hồi thứ mấy?
11. Cần bao nhiêu TCP segments để chứa hết HTTP response và nội dung của The Bill of Rights?

Trả lời:

10. Trình duyệt đã gửi 1 HTTP GET:

Time	Source	Destination	Host	Protocol	Length	Info
2024-03-21 04:48:50.492396	10.45.210.30	128.119.245.12	gaia.cs.umass.edu	HTTP	549	GET /wireshark-labs/HTTP-wireshark-file3.ht…
2024-03-21 04:48:50.749617	128.119.245.12	10.45.210.30		HTTP	1506	HTTP/1.1 200 OK (text/html)
2024-03-21 04:48:50.749617	128.119.245.12	10.45.210.30		HTTP	1506	Continuation
2024-03-21 04:48:50.749804	128.119.245.12	10.45.210.30		HTTP	1506	Continuation
2024-03-21 04:48:50.749804	128.119.245.12	10.45.210.30		HTTP	559	Continuation

Dòng "**THE BILL OF RIGHTS**"được chứa trong gói tin phản hồi đầu tiên:



11. Ta có thể thấy rằng cần **4** TCP segments để chứa hết HTTP response và nội dung của The Bill of Rights

```
2024-03-21 04:48:50.492396  10.45.210.30     128.119.245.12   gaia.cs.umass.edu              HTTP    549 GET /wireshark-labs/HTTP-wireshark-file3.ht…
2024-03-21 04:48:50.749617  128.119.245.12   10.45.210.30                                    HTTP   1506 HTTP/1.1 200 OK  (text/html)
2024-03-21 04:48:50.749617  128.119.245.12   10.45.210.30                                    HTTP   1506 Continuation
2024-03-21 04:48:50.749804  128.119.245.12   10.45.210.30                                    HTTP   1506 Continuation
2024-03-21 04:48:50.749804  128.119.245.12   10.45.210.30                                    HTTP    559 Continuation
```

3. Chứng thực HTTP:

12. Mã trạng thái và ý nghĩa nó trong HTTP response tương ứng với HTTP GET đầu tiên là gì?
13. Khi trình duyệt gửi HTTP GET lần thứ 2, trường dữ liệu nào mới nào xuất hiện trong HTTP GET?

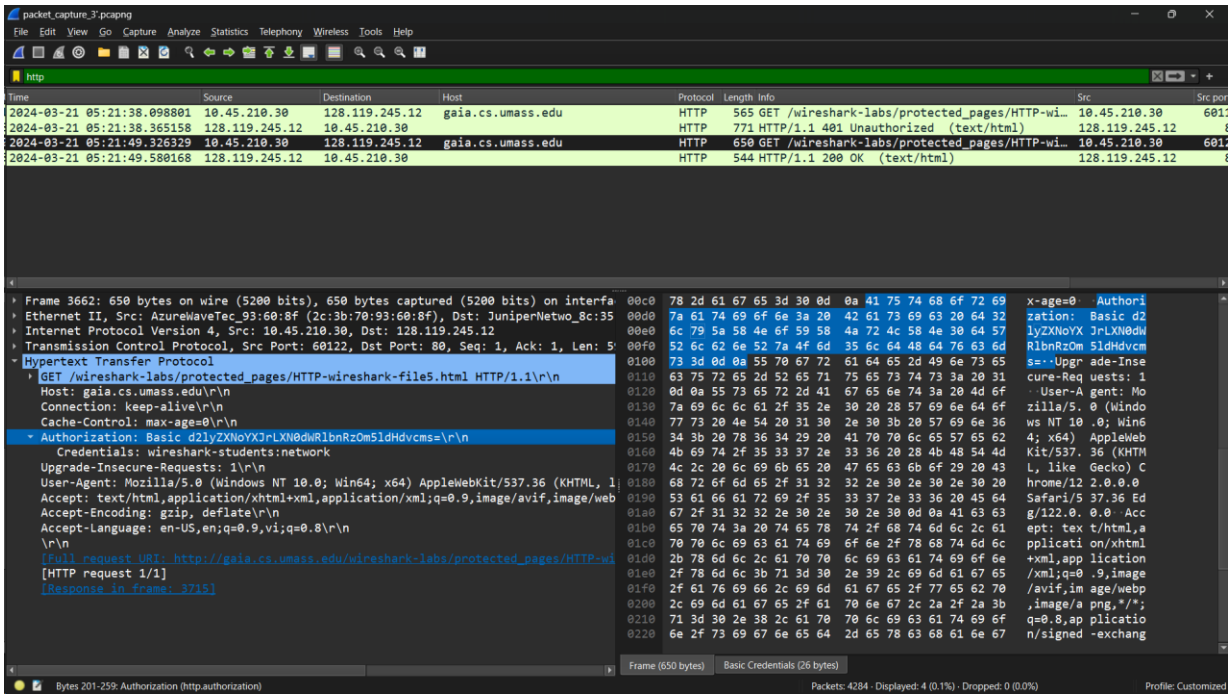
Trả lời:

12. Mã trạng thái trong HTTP GET đầu tiên là: **401 Unauthorized**

```
HTTP    565 GET /wireshark-labs/protected_pages/HTTP-wi…
HTTP    771 HTTP/1.1 401 Unauthorized  (text/html)
```

Ý nghĩa: Mã trạng thái 401 Unauthorized cho ta biết trang web đó yêu cầu thông tin đăng nhập của người dùng. Do đó, response trên trả về 401 Unauthorized vì ban đầu ta chưa nhập username và password tương ứng.

13. Trường dữ liệu mới xuất hiện là: **Authorization.**



Điểm đặc biệt là có thể thấy Username và Password để đăng nhập vào website.

*Ở HTTP GET lần thứ nhất, không có mục trên vì chưa đăng nhập.