

BÁO CÁO LAB02

BÀI 2:

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 sử dụng phiên bản HTTP 1.1

Server: 1.1

```
529 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
784 HTTP/1.1 200 OK (text/html)
```

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

IP máy: 192.168.0.103

IP server: 128.119.245.12

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

```
HTTP/1.1 200 OK\r\n
```

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

```
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
File Data: 371 bytes
```

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

Không thấy.

6. Xem xét nội dung phản hồi từ server. Server có thật sự trả về nội dung của file HTML hay không? Tại sao?

Có trả về nội dung.

Vì ta request lên server và phản hồi lại thành công HTTP/1.1 200 OK. Một phản hồi 200 có thể lưu vào bộ nhớ cache theo mặc định.

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?

Có thấy IF-MODIFIED SINCE.

If-Modified-Since: Thu, 14 Oct 2021 05:59:01 GMT\r\n

Nếu đối tượng không thay đổi trước mốc If-Modified-Since thì yêu cầu lấy trong cache và phản hồi HTTP/1.0 304 Not Modified, còn nếu thay đổi trước mốc đó thì phản hồi HTTP/1.1 200 OK

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.

```
641 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
293 HTTP/1.1 304 Not Modified
```

Ý nghĩa : 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 gửi về nội dung file vì đã file đã lưu trong cache nên chỉ lấy từ trong cache ra.

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

No.	Time	Source	Destination	Protocol	Length	Info
1226	7.175934	192.168.0.103	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1280	7.434631	128.119.245.12	192.168.0.103	HTTP	784	HTTP/1.1 200 OK (text/html)
1297	7.524786	192.168.0.103	128.119.245.12	HTTP	475	GET /favicon.ico HTTP/1.1
1359	7.783555	128.119.245.12	192.168.0.103	HTTP	538	HTTP/1.1 404 Not Found (text/html)
1623	9.213322	192.168.0.103	128.119.245.12	HTTP	641	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1680	9.474924	128.119.245.12	192.168.0.103	HTTP	293	HTTP/1.1 304 Not Modified

Trình duyệt gửi HTTP GET :

1226	7.175934	192.168.0.103	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1623	9.213322	192.168.0.103	128.119.245.12	HTTP	641	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

BÀI 3:

10. Trình duyệt đã gửi bao nhiêu HTTP GET? Dòng “THE BILL OF RIGHTS” được chứa trong gói tin phản hồi thứ mấy?

No.	Time	Source	Destination	Protocol	Length	Info
-	895.8.257833	192.168.0.103	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1

Dòng “THE BILL OF RIGHTS” được chứa trong gói tin phản hồi :

No.	Time	Source	Destination	Protocol	Length	Info
+	895.8.257833	192.168.0.103	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
-	908.8.525968	128.119.245.12	192.168.0.103	HTTP	679	HTTP/1.1 200 OK (text/html)

>	Transmission Control Protocol, Src Port: 80, Dst Port: 65445, Seq: 4237, Ack: 476, Len: 625
>	[4 Reassembled TCP Segments (4861 bytes): #904(1412), #905(1412), #906(1412), #908(625)]
>	Hypertext Transfer Protocol
▼	Line-based text data: text/html (98 lines)
	<html><head> \n
	<title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
	\n
	\n
	<body bgcolor="#ffffff" link="#330000" vlink="#666633">\n
	<p> \n
	</p>\n
	<p><p><center>THE BILL OF RIGHTS \n

0070	00 67 00 50 ff a5 0a 0c d6 c4 d2 08 40 16 50 18	..P.....@..B..
------	---	----------------

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

>	[4 Reassembled TCP Segments (4861 bytes): #904(1412), #905(1412), #906(1412), #908(625)]
---	--

BÀI 4:

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

113	4.043069	192.168.1.102	128.119.245.12	HTTP	545	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html	HTTP/1.1
122	4.320647	128.119.245.12	192.168.1.102	HTTP	771	HTTP/1.1 401 Unauthorized	(text/html)

401 Unauthorized : status code khi web bạn đang truy cập không thể được tải cho đến khi đăng nhập lần đầu bằng một ID(username) và mật khẩu hợp lệ.

13. 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, server phản hồi thành công với status code 200.

```
630 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
544 HTTP/1.1 200 OK (text/html)
```

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

Tìm username, password:

No.	Time	Source	Destination	Protocol	Length	Info
113	4.043069	192.168.1.102	128.119.245.12	HTTP	545	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
122	4.320647	128.119.245.12	192.168.1.102	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
1126	45.479983	192.168.1.102	128.119.245.12	HTTP	630	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
1141	45.743512	128.119.245.12	192.168.1.102	HTTP	544	HTTP/1.1 200 OK (text/html)

> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 62260, Dst Port: 80, Seq: 1, Ack: 1, Len: 576
✓ 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 d2lyZXNoYXJrLXN0dWRlbnRzM5ldHdvcms=\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/94.0.4606.81 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=0.9\r\n
Accept-Encoding: gzip, deflate\r\n

Connection: keep-alive\r\n

Cache-Control: max-age=0\r\n

✓ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzM5ldHdvcms=\r\n

Credentials: wireshark-students:network

Upgrade-Insecure-Requests: 1\r\n