



Lab 2

BÁO CÁO BÀI THỰC HÀNH SỐ 2

Môn học: Nhập môn Mạng máy tính

Sinh viên thực hiện	Đoàn Phương Nam (22520908)
Thời gian thực hiện	11/10/2023 – 14/10/2023
Tự chấm điểm	10/10

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.

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 1.1 . Phiên bản HTTP server đang sử dụng bản 1.1.

Length Info

```
539 GET /22520844.html HTTP/1.1
639 HTTP/1.1 200 OK (text/html)
```

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

Địa chỉ IP của máy tính là 192.168.222.83

Địa chỉ IP của server là 192.168.222.240

No.	Time	Source	Destination	Protocol	Length	Info
340	5.005413	192.168.222.83	192.168.222.240	HTTP	539	GET /22520844.html HTTP/1.1

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

Các mã trạng thái trả về từ server là 200 OK, 301 move permanently và 404: Các tài nguyên hiện tại không được tìm thấy nhưng có thể có trong tương lai. Các request tiếp theo của Client được chấp nhận

```
GET /22520844.html HTTP/1.1
HTTP/1.1 200 OK (text/html)
GET /Styles/profi/images/logo186x150.png
HTTP/1.1 301 Moved Permanently (text/html)
GET /favicon.ico HTTP/1.1
HTTP/1.1 404 Not Found (text/html)
```

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

Trả về 1245 bytes

Lab 1: Làm quen với Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
340	5.005413	192.168.222.83	192.168.222.240	HTTP	539	GET /22520844.html HTTP/1.1
344	5.008450	192.168.222.240	192.168.222.83	HTTP	639	HTTP/1.1 200 OK (text/html)
352	5.027710	192.168.222.83	192.168.20.88	HTTP	496	GET /Styles/profi/images/logo186x150.png HTTP/1.1
353	5.030641	192.168.20.88	192.168.222.83	HTTP	493	HTTP/1.1 301 Moved Permanently (text/html)
397	5.089804	192.168.222.83	192.168.222.240	HTTP	483	GET /favicon.ico HTTP/1.1
398	5.093955	192.168.222.240	192.168.222.83	HTTP	1437	HTTP/1.1 404 Not Found (text/html)

```
> Frame 398: 1437 bytes on wire (11496 bits), 1437 bytes captured (11496 bits) on interface \Device\NPF_{0F2390A0-CB67-4FA6-B044-9A6E4CC7A7A4}, id 0
> Ethernet II, Src: CompalIn_51:e4:cd (08:8f:c3:51:e4:cd), Dst: CompalIn_e6:91:93 (08:97:98:e6:91:93)
> Internet Protocol Version 4, Src: 192.168.222.240, Dst: 192.168.222.83
> Transmission Control Protocol, Src Port: 80, Dst Port: 52591, Seq: 586, Ack: 915, Len: 1383
> Hypertext Transfer Protocol
  > HTTP/1.1 404 Not Found\r\n
    Content-Type: text/html\r\n
    Server: Microsoft-IIS/10.0\r\n
    Date: Wed, 11 Oct 2023 08:29:54 GMT\r\n
  > Content-Length: 1245\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.004151000 seconds]
    [Prev request in frame: 340]
    [Prev response in frame: 344]
    [Request in frame: 397]
    [Request URI: http://192.168.222.240/favicon.ico]
    File Data: 1245 bytes
> Line-based text data: text/html (29 lines)
```

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

Xem xét nội dung của HTTP GET đầu tiên, không thấy dòng “IF-MODIFIED-SINCE”.

The screenshot shows the Wireshark interface with packet 340 selected. The packet list on the left shows the first four packets of the capture. The packet details pane on the right shows the structure of the selected packet. The packet is an HTTP GET request for /22520844.html. The details pane shows the request line, host, connection, upgrade-insecure-requests, user-agent, accept, accept-encoding, and accept-language headers. The packet bytes pane on the right shows the raw data of the packet in hexadecimal and ASCII.

22520908-Ba1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
340	5.005413	192.168.222.83	192.168.222.240	HTTP	539	GET /22520844.html HTTP/1.1
352	5.027710	192.168.222.83	192.168.20.88	HTTP	496	GET /Styles/profi/images/logo186x150.png HTTP/1.1
397	5.089804	192.168.222.83	192.168.222.240	HTTP	483	GET /favicon.ico HTTP/1.1
344	5.008450	192.168.222.240	192.168.222.83	HTTP	639	HTTP/1.1 200 OK (text/html)
353	5.030641	192.168.20.88	192.168.222.83	HTTP	493	HTTP/1.1 301 Moved Permanently (text/html)
398	5.093955	192.168.222.240	192.168.222.83	HTTP	1437	HTTP/1.1 404 Not Found (text/html)

> Frame 340: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits) on interface \Device\NPF_{0F2390A0-CB67-4FA6-B044-9A6E4CC7A7A4}, id 0

> Ethernet II, Src: CompalIn_e6:91:93 (08:97:98:e6:91:93), Dst: CompalIn_51:e4:cd (08:8f:c3:51:e4:cd)

> Internet Protocol Version 4, Src: 192.168.222.83, Dst: 192.168.222.240

> Transmission Control Protocol, Src Port: 52591, Dst Port: 80, Seq: 1, Ack: 1, Len: 485

> Hypertext Transfer Protocol

> GET /22520844.html HTTP/1.1\r\n

Host: 192.168.222.240\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) Chrome/118.0.0.0 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=0.7\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Language: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5\r\n

\r\n

[Full request URI: http://192.168.222.240/22520844.html]

[HTTP request 1/2]

[Response in frame: 344]

[Next request in frame: 397]

0000 08 8f c3 51 e4 cd 08 97 98 e6 91 93 08 00 45

0010 02 0d bc b9 40 00 80 06 00 00 c0 a8 de 53 c0

0020 de f0 cd 6f 00 50 e8 21 13 75 ba e0 5a b2 50

0030 01 00 40 95 00 00 47 45 54 20 2f 32 32 35 32

0040 38 34 34 2e 68 74 6d 6c 20 48 54 54 50 2f 31

0050 31 0d 0a 48 6f 73 74 3a 20 31 39 32 2e 31 36

0060 2e 32 32 32 2e 32 34 30 0d 0a 43 6f 6e 6e 65

0070 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76

0080 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63

0090 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d

00a0 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a

00b0 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77

00c0 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 34

00d0 20 78 36 34 29 20 41 70 70 6c 65 57 65 62 4b

00e0 74 2f 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c

00f0 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20 43 68

0100 6f 6d 65 2f 31 31 38 2e 30 2e 30 2e 30 20 53

0110 66 61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 63

0120 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c

0130 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d

0140 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f

0150 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67

0160 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 62

0170 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f 2a

0180 71 3d 30 2e 38 2c 61 70 70 6c 69 63 61 74 69

0190 6a 6e 77 69 67 6e 6e 6a 74 6e 70 6c 69 61 6e

Hypertext Transfer Protocol: Protocol

Packets: 650 · Displayed: 6 (0.9%)

Profile: Default

234 CH

14/10/2023

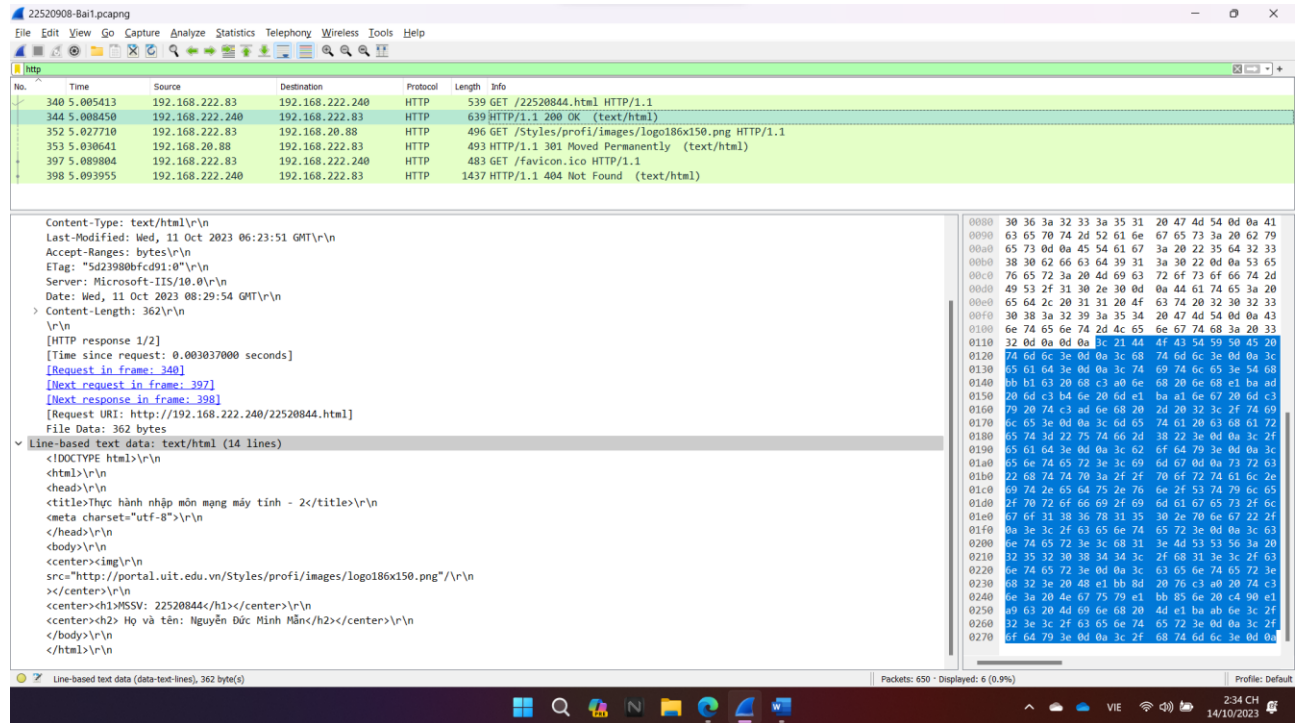
Lab 1: Làm quen với Wireshark

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 file HTML.

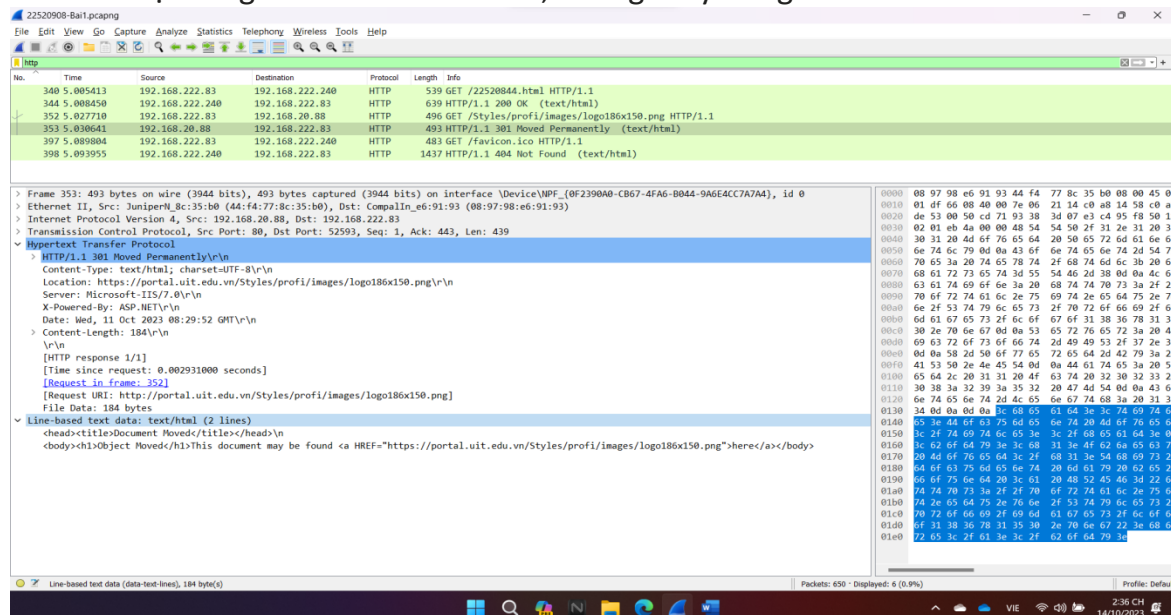
Mã trạng thái đi kèm là 200 OK.

Ý nghĩa: Request đã được tiếp nhận và xử lý thành công.



Câu 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?

Xem xét nội dung của HTTP GET thứ 2, không thấy dòng “IF-MODIFIED-SINCE”.



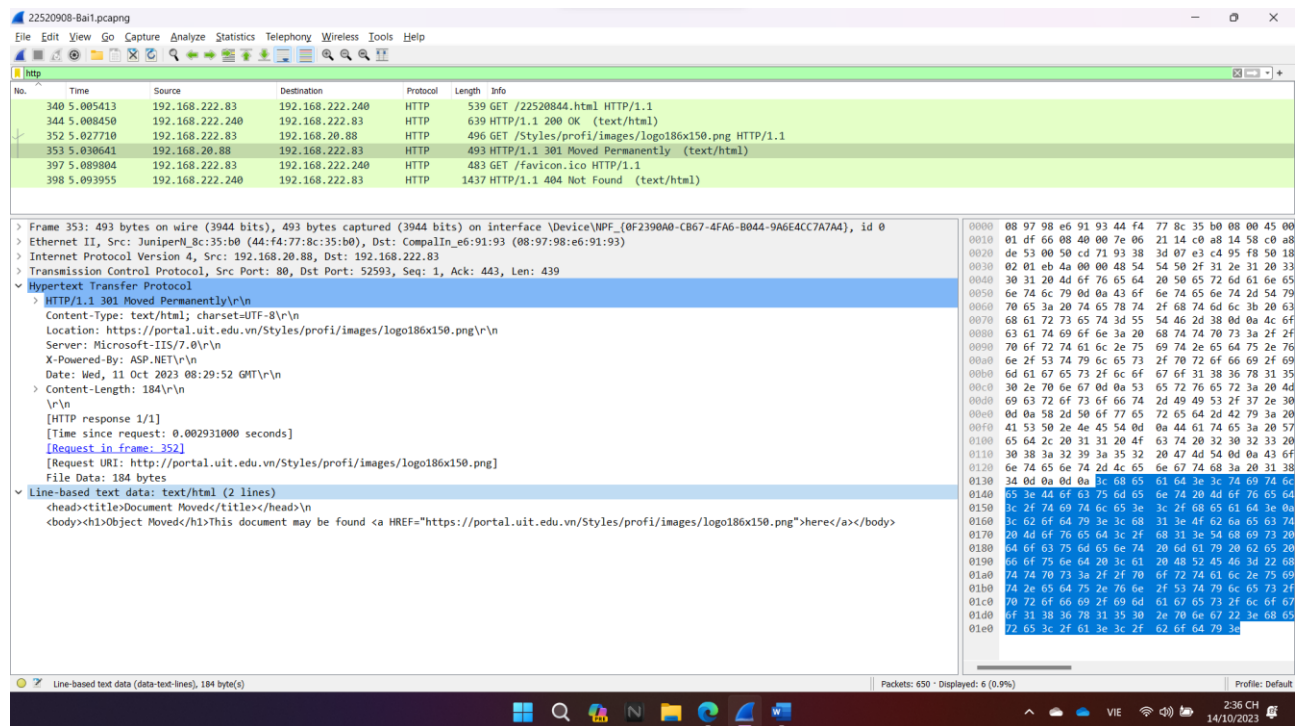
Câu 8. Mã trạng thái HTTP được trả về từ server tương ứng với HTTP GET thứ 2 là gì? Ý nghĩa nó là gì? Server có thật sự gửi về nội dung của file hay không? Giải thích.

Server có trả về nội dung file HTML.

Mã trạng thái đi kèm là 301 move permanently.

Ý nghĩa: thông báo rằng các trang web hoặc URL đã chuyển hướng vĩnh viễn sang một trang web hoặc URL khác, có nghĩa là tất cả những giá trị của trang web hoặc URL gốc sẽ chuyển hết sang URL mới.

Server đã thực sự gửi về nội dung file.



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

Trình duyệt đã gửi 3 HTTP GET.

Đến :

- 192.168.222.240 – 2 HTTP GET
- 192.168.20.88 – 1 HTTP GET

Destination	Protocol	Length	Info
192.168.222.240	HTTP	539	GET /22520844.html HTTP/1.1
192.168.222.83	HTTP	639	HTTP/1.1 200 OK (text/html)
192.168.20.88	HTTP	496	GET /Styles/profi/images/logo186x150.png HTTP/1.1
192.168.222.83	HTTP	493	HTTP/1.1 301 Moved Permanently (text/html)
192.168.222.240	HTTP	483	GET /favicon.ico HTTP/1.1
192.168.222.83	HTTP	1437	HTTP/1.1 404 Not Found (text/html)

3. Truy cập các trang HTTP dài

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

Trình duyệt đã gửi 2 HTTP GET

No.	Time	Source	Destination	Protocol	Length	Info
279	4.669341	192.168.222.83	128.119.245.12	HTTP	568	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
288	4.942202	128.119.245.12	192.168.222.83	HTTP	559	HTTP/1.1 200 OK (text/html)
293	4.975700	192.168.222.83	128.119.245.12	HTTP	514	GET /favicon.ico HTTP/1.1
296	5.241684	128.119.245.12	192.168.222.83	HTTP	538	HTTP/1.1 404 Not Found (text/html)

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

Cần 4 TCP segment để chứa hết HTTP response

> Transmission Control Protocol, Src Port: 80, Dst Port: 57915, Seq: 4357, Ack: 515, Len: 505

✓ [4 Reassembled TCP Segments (4861 bytes): #284(1452), #285(1452), #287(1452), #288(505)]

[Frame: 284, payload: 0-1451 (1452 bytes)]

[Frame: 285, payload: 1452-2903 (1452 bytes)]

[Frame: 287, payload: 2904-4355 (1452 bytes)]

[Frame: 288, payload: 4356-4860 (505 bytes)]

[Segment count: 4]

[Reassembled TCP length: 4861]

[Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a4461746553a205765642c203131204f63742032...]

> Hypertext Transfer Protocol

No.	Time	Source	Destination	Protocol	Length	Info
279	4.669341	192.168.222.83	128.119.245.12	HTTP	568	GET /wireshark-labs/HTTP-wireshark-f
288	4.942202	128.119.245.12	192.168.222.83	HTTP	559	HTTP/1.1 200 OK (text/html)
293	4.975700	192.168.222.83	128.119.245.12	HTTP	514	GET /favicon.ico HTTP/1.1
296	5.241684	128.119.245.12	192.168.222.83	HTTP	538	HTTP/1.1 404 Not Found (text/html)

> Frame 288: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{0F2390A0-CB67-...}

> Ethernet II, Src: JuniperN_8c:35:b0 (44:f4:77:8c:35:b0), Dst: CompalIn_e6:91:93 (08:97:98:e6:91:93)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.222.83

> Transmission Control Protocol, Src Port: 80, Dst Port: 57915, Seq: 4357, Ack: 515, Len: 505

> [4 Reassembled TCP Segments (4861 bytes): #284(1452), #285(1452), #287(1452), #288(505)]

> Hypertext Transfer Protocol

✓ Line-based text data: text/html (98 lines)

```
<html><head> \n
<title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
...
```

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

Lab 1: Làm quen với Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
279	4.669341	192.168.222.83	128.119.245.12	HTTP	568	GET /wireshark-labs/HTTP-wireshark-f
288	4.942202	128.119.245.12	192.168.222.83	HTTP	559	HTTP/1.1 200 OK (text/html)
293	4.975700	192.168.222.83	128.119.245.12	HTTP	514	GET /favicon.ico HTTP/1.1
296	5.241684	128.119.245.12	192.168.222.83	HTTP	538	HTTP/1.1 404 Not Found (text/html)

> Frame 288: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{0F2390A0-CB67-4FA6-B044-9A6E4CC7A7A4}, id 0
> Ethernet II, Src: JuniperN_8c:35:b0 (44:f4:77:8c:35:b0), Dst: CompalIn_e6:91:93 (08:97:98:e6:91:93)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.222.83
> Transmission Control Protocol, Src Port: 80, Dst Port: 57915, Seq: 4357, Ack: 515, Len: 505
> [4 Reassembled TCP Segments (4861 bytes): #284(1452), #285(1452), #287(1452), #288(505)]
> Hypertext Transfer Protocol
Line-based text data: text/html (98 lines)
 <html><head> \n
 <title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
 ...

Nội dung THE BILL OF RIGHTS xuất hiện trong gói tin số 288

4. Chứng thực HTTP

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

Mã trạng thái 401 Unauthorized

Ý nghĩa: thông báo website vẫn tồn tại, hoạt động nhưng người dùng không thể truy cập vào do không được cấp quyền truy cập hay sở hữu quyền truy cập (bao gồm tài khoản mật khẩu không hợp lệ).

22520908-Bai3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
611	1.281132	192.168.222.83	209.197.3.8	HTTP	500	GET /filestreamingservice/files/02d94459-38b6-4c1e-9cbe-46fb4f626087?P1=1697022188&P2=404&P3=28P4=HfbQvzSw01mG0m1fWBg3d1bnBHLZz599j...
641	1.300545	192.168.222.83	209.197.3.8	HTTP	500	GET /filestreamingservice/files/02d94459-38b6-4c1e-9cbe-46fb4f626087?P1=1697022188&P2=404&P3=28P4=HfbQvzSw01mG0m1fWBg3d1bnBHLZz599j...
615	5.843793	192.168.222.83	128.119.245.12	HTTP	584	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
619	9.106892	128.119.245.12	192.168.222.83	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
683	9.563458	209.197.3.8	192.168.222.83	HTTP	201	HTTP/1.1 503 Service Unavailable
802	12.676105	192.168.222.83	128.119.245.12	HTTP	669	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
806	12.954520	128.119.245.12	192.168.222.83	HTTP	544	HTTP/1.1 200 OK (text/html)
807	12.996065	192.168.222.83	128.119.245.12	HTTP	530	GET /favicon.ico HTTP/1.1
819	13.272686	128.119.245.12	192.168.222.83	HTTP	538	HTTP/1.1 404 Not Found (text/html)

> Frame 619: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{0F2390A0-CB67-4FA6-B044-9A6E4CC7A7A4}, id 0
> Ethernet II, Src: JuniperN_8c:35:b0 (44:f4:77:8c:35:b0), Dst: CompalIn_e6:91:93 (08:97:98:e6:91:93)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.222.83
> Transmission Control Protocol, Src Port: 80, Dst Port: 58006, Seq: 1, Ack: 531, Len: 717
> Hypertext Transfer Protocol
 HTTP/1.1 401 Unauthorized\r\n
 Date: Wed, 11 Oct 2023 08:50:17 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
 WWW-Authenticate: Basic realm="wireshark-students only"\r\n
 Content-Length: 381\r\n
 Keep-Alive: timeout=5, max=100\r\n
 Connection: Keep-Alive\r\n
 Content-Type: text/html; charset=iso-8859-1\r\n
 \r\n
 [HTTP response 1/1]
 [Time since request: 0.262389000 seconds]
 [Request in frame: 615]
 [Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]

0000 08 97 98 e6 91 93 44 f4 77 8c 35 b0 08 00 45
0010 02 f5 7b c3 40 00 21 06 c6 9f 80 77 f5 0c c0
0020 de 53 00 50 e2 96 b4 18 f0 65 4a 3d 40 69 50
0030 00 ed 69 b9 00 00 48 54 54 50 2f 31 2e 31 20
0040 30 31 20 55 6e 61 75 74 68 6f 72 69 7a 65 64
0050 0a 44 61 74 65 3a 20 57 65 64 2c 20 31 31 20
0060 63 74 20 32 30 32 33 20 30 38 3a 35 30 3a 31
0070 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41
0080 61 63 68 05 2f 32 2e 34 2e 36 20 28 43 65 6e
0090 4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 30
00a0 32 6b 2d 66 69 70 73 20 50 48 50 2f 32 2e 34
00b0 33 33 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e 30
00c0 31 31 20 50 65 72 6c 2f 76 35 2e 31 36 2e 33
00d0 0a 57 57 57 2d 41 75 74 68 65 6e 74 69 63 61
00e0 65 3a 20 42 61 73 69 63 20 72 65 61 6c 6d 3d
00f0 77 69 72 65 73 68 61 72 6b 2d 73 74 75 64 65
0100 74 73 20 6f 6e 6c 79 22 0d 0a 43 6f 6e 74 65
0110 74 2d 4c 65 6e 67 74 68 3a 20 33 38 31 0d 0a
0120 ee ee 70 7d 81 e6 60 7c ee 7a 7a 7a e0 ee ee

Packets: 1032 - Displayed: 9 (0.9%) Profile: Default

Lab 1: Làm quen với Wireshark

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

Khi trình duyệt gửi HTTP GET lần thứ 2, trường dữ liệu mới xuất hiện là Authorization và Credentials (chứa tài khoản và mật khẩu để truy cập vào web)

