

Thực hành Nhập Môn Mạng Máy Tính

Lab2

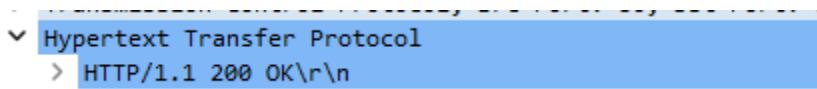
GVHD: Ngô Khánh Khoa

MSSV: 23520362

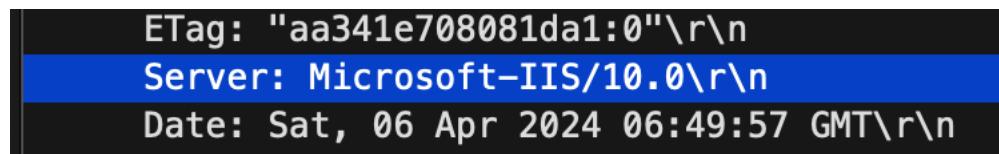
Họ và tên: Đỗ Phương Duy

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 bản HTTP 1.1



Phiên bản HTTP Server: Microsoft-IIS/10.0



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

Địa chỉ IP máy là: 192.168.43.63

Địa chỉ của web server là: 192.168.43.69

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---------------|---------------|----------|--------|---|
| 40 | 1.374871 | 192.168.43.69 | 192.168.43.63 | HTTP | 599 | GET /23521436.html?fbclid=IwAR0zzxOjNjDGo_An78s6q2fk-8roXHXRPR62FXBdqR724GMhpyhbmcQ24M HTTP/1.1 |
| 41 | 1.508767 | 192.168.43.63 | 192.168.43.69 | HTTP | 643 | HTTP/1.1 200 OK (text/html) |
| 65 | 3.390293 | 192.168.43.69 | 192.168.43.63 | HTTP | 711 | GET /23521436.html?fbclid=IwAR0zzxOjNjDGo_An78s6q2fk-8roXHXRPR62FXBdqR724GMhpyhbmcQ24M HTTP/1.1 |
| 66 | 3.397262 | 192.168.43.63 | 192.168.43.69 | HTTP | 197 | HTTP/1.1 304 Not Modified |
| 83 | 4.829213 | 192.168.43.69 | 192.168.43.63 | HTTP | 711 | GET /23521436.html?fbclid=IwAR0zzxOjNjDGo_An78s6q2fk-8roXHXRPR62FXBdqR724GMhpyhbmcQ24M HTTP/1.1 |
| 85 | 4.841057 | 192.168.43.63 | 192.168.43.69 | HTTP | 197 | HTTP/1.1 304 Not Modified |

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

Status: 200 OK

| | | | | | | |
|----|----------|---------------|---------------|------|-----|-----------------------------|
| 41 | 1.508767 | 192.168.43.63 | 192.168.43.69 | HTTP | 643 | HTTP/1.1 200 OK (text/html) |
|----|----------|---------------|---------------|------|-----|-----------------------------|

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

Server đã trả về 364 bytes nội dung

```
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Content-Type: text/html\r\n
    Last-Modified: Fri, 29 Mar 2024 02:25:59 GMT\r\n
    Accept-Ranges: bytes\r\n
    ETag: "aa341e708081da1:0"\r\n
    Server: Microsoft-IIS/10.0\r\n
    Date: Sat, 06 Apr 2024 06:49:57 GMT\r\n
  > Content-Length: 364\r\n
    \r\n
    [HTTP response 1/3]
    [Time since request: 0.133896000 seconds]
    [Request in frame: 40]
    [Next request in frame: 65]
    [Next response in frame: 66]
    [Request URI: http://192.168.43.63/23521436.html?fbclid=IwAR0zzxOjNjDGo_An78s6
      File Data: 364 bytes
  ▼ Line-based text data: text/html (14 lines)
    . . .
```

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

Nội dung HTTP GET đầu tiên không có dòng “IF-MODIFIEDSINCE”

23520362.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

| No. | http | Source | Destination | Protocol | Length | Info |
|--------|----------|---------------|---------------|----------|--------|---|
| 74871 | http2 | 192.168.43.69 | 192.168.43.63 | HTTP | 599 | GET /23521436.html?fbclid=IwAR0zzxOjNjDGo_A |
| 808767 | http3 | 192.168.43.63 | 192.168.43.69 | HTTP | 643 | HTTP/1.1 |
| 65 | 3.390293 | 192.168.43.69 | 192.168.43.63 | HTTP | 711 | GET /23521436.html?fbclid=IwAR0zzxOjNjDGo_A |
| 66 | 3.397262 | 192.168.43.63 | 192.168.43.69 | HTTP | 197 | HTTP/1.1 |
| 83 | 4.829213 | 192.168.43.69 | 192.168.43.63 | HTTP | 711 | GET /23521436.html?fbclid=IwAR0zzxOjNjDGo_A |
| 85 | 4.841057 | 192.168.43.63 | 192.168.43.69 | HTTP | 197 | HTTP/1.1 |

```

> Ethernet II, Src: CloudNetwork_7c:e8:f9 (f0:a6:54:7c:e8:f9), Dst: ChongqingFug_bg (08:00:27:00:00:00)
> Internet Protocol Version 4, Src: 192.168.43.69, Dst: 192.168.43.63
> Transmission Control Protocol, Src Port: 65021, Dst Port: 80, Seq: 1, Ack: 1, Len: 599
< Hypertext Transfer Protocol
  > GET /23521436.html?fbclid=IwAR0zzxOjNjDGo_A
    Host: 192.168.43.63\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/91.0.4453.114 Safari/537.36
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
    Referer: https://l.messenger.com/\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
  \r\n
  [Full request URI: http://192.168.43.63/23521436.html?fbclid=IwAR0zzxOjNjDGo_A]
  [HTTP request 1/3]
  [Response in frame: 41]
  [Next request in frame: 65]
```

HyperText Transfer Protocol

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

Server đã trả về nội dung của file HTML vì Status code = 200 OK

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---------------|---------------|----------|--------|---------|
| 40 | 1.374871 | 192.168.43.69 | 192.168.43.63 | HTTP | 599 | GET /23 |
| 41 | 1.508767 | 192.168.43.63 | 192.168.43.69 | HTTP | 643 | HTTP/1. |
| 65 | 3.390293 | 192.168.43.69 | 192.168.43.63 | HTTP | 711 | GET /23 |
| 66 | 3.397262 | 192.168.43.63 | 192.168.43.69 | HTTP | 197 | HTTP/1. |
| 83 | 4.829213 | 192.168.43.69 | 192.168.43.63 | HTTP | 711 | GET /23 |
| 85 | 4.841057 | 192.168.43.63 | 192.168.43.69 | HTTP | 197 | HTTP/1. |

```

> Internet Protocol Version 4, Src: 192.168.43.63, Dst: 192.168.43.69
> Transmission Control Protocol, Src Port: 80, Dst Port: 65021, Seq: 1, Ack: 546, L
> Hypertext Transfer Protocol
▼ Line-based text data: text/html (14 lines)
  <!DOCTYPE html>\\r\\n
  <html>\\r\\n
    <meta charset = "UTF-8">\\r\\n
  <head>\\r\\n
    <title>Thực hành nhập môn mạng máy tính - 2</title>\\r\\n
  </head>\\r\\n
  <body>\\r\\n
    <center><img\\r\\n
    src="http://portal.uit.edu.vn/Styles/profi/images/logo186x150.png"/\\r\\n
  ></center>\\r\\n
  <center><h1>MSSV: 23521436</h1></center>\\r\\n
  <center><h2> Họ và tên: Bùi Ngọc Thiên Thành</h2></center>\\r\\n
  </body>\\r\\n
  </html>

```

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?

- Nội dung của HTTP GET thứ 2 có xuất hiện dòng “IF-MODIFIEDSINCE”
- Giá trị của “IF-MODIFIEDSINCE” là Fri, 29 Mar 2024 02:25:59 GMT

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---------------|---------------|----------|--------|---|
| 40 | 1.374871 | 192.168.43.69 | 192.168.43.63 | HTTP | 599 | GET /23521436.html?fbclid=IwAR0zzx0jNjDGo_A |
| 41 | 1.508767 | 192.168.43.63 | 192.168.43.69 | HTTP | 643 | HTTP/1.1 |
| 65 | 3.390293 | 192.168.43.69 | 192.168.43.63 | HTTP | 711 | GET /23521436.html?fbclid=IwAR0zzx0jNjDGo_A |
| 66 | 3.397262 | 192.168.43.63 | 192.168.43.69 | HTTP | 197 | HTTP/1.1 |
| 83 | 4.829213 | 192.168.43.69 | 192.168.43.63 | HTTP | 711 | GET /23521436.html?fbclid=IwAR0zzx0jNjDGo_A |
| 85 | 4.841057 | 192.168.43.63 | 192.168.43.69 | HTTP | 197 | HTTP/1.1 |


```

> Internet Protocol Version 4, Src: 192.168.43.69, Dst: 192.168.43.63
> Transmission Control Protocol, Src Port: 65021, Dst Port: 80, Seq: 546, Ack: 590,
` Hypertext Transfer Protocol
  > GET /23521436.html?fbclid=IwAR0zzx0jNjDGo_A
    Host: 192.168.43.63\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
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
      Referer: https://l.messenger.com/\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: en-US,en;q=0.9\r\n
      If-None-Match: "aa341e708081da1:0"\r\n
      If-Modified-Since: Fri, 29 Mar 2024 02:25:59 GMT\r\n
    \r\n
    [Full request URI: http://192.168.43.63/23521436.html?fbclid=IwAR0zzx0jNjDGo_A
    [HTTP request 2/3]
  
```

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 HTTP được trả về từ server tương ứng với HTTP GET thứ 2 là 304 Not Modified.

Ý nghĩa: Mã này chỉ ra rằng không cần phải truyền lại các tài nguyên được yêu cầu. Nó là một sự chuyển hướng ngầm đến một tài nguyên được lưu trong bộ nhớ cache.

Server không gửi nội dung HTML đầy đủ mà thông báo rằng nội dung cũ vẫn còn hiệu lực.

Giải thích: tại vì nội dung của tài nguyên được yêu cầu chưa bị thay đổi kể từ lần truy cập trước.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---------------|---------------|----------|--------|--|
| 40 | 1.374871 | 192.168.43.69 | 192.168.43.63 | HTTP | 599 | GET /23521436.html?fbclid=IwAR0zzxOjNjDGo_An78s6q2fk-8 |
| 41 | 1.508767 | 192.168.43.63 | 192.168.43.69 | HTTP | 643 | HTTP/1.1 200 OK (text/html) |
| 65 | 3.390293 | 192.168.43.69 | 192.168.43.63 | HTTP | 711 | GET /23521436.html?fbclid=IwAR0zzxOjNjDGo_An78s6q2fk-8 |
| 66 | 3.397262 | 192.168.43.63 | 192.168.43.69 | HTTP | 197 | HTTP/1.1 304 Not Modified |
| 83 | 4.829213 | 192.168.43.69 | 192.168.43.63 | HTTP | 711 | GET /23521436.html?fbclid=IwAR0zzxOjNjDGo_An78s6q2fk-8 |
| 85 | 4.841057 | 192.168.43.63 | 192.168.43.69 | HTTP | 197 | HTTP/1.1 304 Not Modified |


```

> Frame 66: 197 bytes on wire (1576 bits), 197 bytes captured (1576 bits) on interface
> Ethernet II, Src: ChongqingFug_b9:68:1d (b4:b5:b6:b9:68:1d), Dst: CloudNetwork_7c
> Internet Protocol Version 4, Src: 192.168.43.63, Dst: 192.168.43.69
> Transmission Control Protocol, Src Port: 80, Dst Port: 65021, Seq: 590, Ack: 1203
└ Hypertext Transfer Protocol
  └ HTTP/1.1 304 Not Modified\r\n
    Accept-Ranges: bytes\r\n
    ETag: "aa341e708081da1:0"\r\n
    Server: Microsoft-IIS/10.0\r\n
    Date: Sat, 06 Apr 2024 06:49:59 GMT\r\n
    \r\n
    [HTTP response 2/3]
    [Time since request: 0.006969000 seconds]
    [Prev request in frame: 40]
    [Prev response in frame: 41]
    [Request in frame: 65]
    [Next request in frame: 83]
    [Next response in frame: 85]
  
```

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

Trình duyệt đã gửi 3 HTTP GET, đến địa chỉ IP 192.168.43.63

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---------------|---------------|----------|--------|--|
| 40 | 1.374871 | 192.168.43.69 | 192.168.43.63 | HTTP | 599 | GET /23521436.html?fbclid=IwAR0zzxOjNjDGo_An78s6q2fk-8 |
| 41 | 1.508767 | 192.168.43.63 | 192.168.43.69 | HTTP | 643 | HTTP/1.1 200 OK (text/html) |
| 65 | 3.390293 | 192.168.43.69 | 192.168.43.63 | HTTP | 711 | GET /23521436.html?fbclid=IwAR0zzxOjNjDGo_An78s6q2fk-8 |
| 66 | 3.397262 | 192.168.43.63 | 192.168.43.69 | HTTP | 197 | HTTP/1.1 304 Not Modified |
| 83 | 4.829213 | 192.168.43.69 | 192.168.43.63 | HTTP | 711 | GET /23521436.html?fbclid=IwAR0zzxOjNjDGo_An78s6q2fk-8 |
| 85 | 4.841057 | 192.168.43.63 | 192.168.43.69 | HTTP | 197 | HTTP/1.1 304 Not Modified |

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

Trình duyệt đã gửi 2 HTTP GET

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|--|
| 760 | 3.942528 | 10.45.125.162 | 128.119.245.12 | HTTP | 583 | GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1 |
| 782 | 4.192237 | 128.119.245.12 | 10.45.125.162 | HTTP | 559 | HTTP/1.1 200 OK (text/html) |
| 799 | 4.375508 | 10.45.125.162 | 128.119.245.12 | HTTP | 529 | GET /favicon.ico HTTP/1.1 |
| 847 | 4.929781 | 128.119.245.12 | 10.45.125.162 | HTTP | 538 | HTTP/1.1 404 Not Found (text/html) |

Dòng “THE BILL OF RIGHTS” được chứa trong gói tin phản hồi thứ nhất.

The screenshot shows the Wireshark interface with the 'http' protocol selected. The packet list pane shows four frames, with the first frame (760) highlighted. The details pane displays the raw HTTP response, which includes the header and the content of the 'index.html' file. The content pane shows the decoded HTML code, including the title 'Historical Documents: THE BILL OF RIGHTS' and the text of the Bill of Rights document.

```

Connection: keep-alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.249709000 seconds]
[Request in frame: 760]
[Next request in frame: 799]
[Next response in frame: 847]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-
File Data: 4500 bytes
Line-based text data: text/html (98 lines)
<html><head> \n
<title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
\n
<body background="#fffff# 1in#:#300000# v1in#:#666633#\">\n

```

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

The screenshot shows the Wireshark interface with the 'http' protocol selected. The packet list pane shows four frames, with the first frame (760) highlighted. The details pane displays the raw HTTP response, which includes the header and the content of the 'index.html' file. The content pane shows the decoded HTML code, including the title 'Historical Documents: THE BILL OF RIGHTS' and the text of the Bill of Rights document. The status bar at the bottom indicates that there are 4 reassembled TCP segments in total.

```

> Frame 782: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits)
> Ethernet II, Src: JuniperNetwo_8c:35:b0 (44:f4:77:8c:35:b0), Dst: Apple
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.45.125.162
> Transmission Control Protocol, Src Port: 80, Dst Port: 51585, Seq: 4357
> [4 Reassembled TCP Segments (4861 bytes): #779(1452), #780(1452), #781(
    [Frame: 779, payload: 0-1451 (1452 bytes)]
    [Frame: 780, payload: 1452-2903 (1452 bytes)]
    [Frame: 781, payload: 2904-4355 (1452 bytes)]
    [Frame: 782, payload: 4356-4860 (505 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data [truncated]: 485454502f312e3120323030204f4b0d0;
> Hypertext Transfer Protocol
> Line-based text data: text/html (98 lines)

```

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

Status code: 401 Unauthorized

| | | | | |
|----------------|----------------|----------------|------|--|
| + 121 1.507233 | 10.45.125.162 | 128.119.245.12 | HTTP | 599 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1 |
| + 176 1.844842 | 128.119.245.12 | 10.45.125.162 | HTTP | 771 HTTP/1.1 401 Unauthorized (text/html) |

Ý nghĩa: để cho biết rằng truy cập vào tài nguyên được yêu cầu bị từ chối do không có thông tin xác thực hợp lệ. Nghĩa là người dùng đã cố gắng truy cập vào một trang web hoặc tài nguyên mà họ không có quyền truy cập

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

- Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdv cms=

The screenshot shows a Wireshark capture window with two frames selected:

- Frame 121: A successful HTTP GET request to "HTTP-wireshark-file5.html" with a status of 599.
- Frame 176: An immediate response from the server with a status of 771, indicating "HTTP/1.1 401 Unauthorized (text/html)".

The details pane displays the raw HTTP request and response. The request includes the URL and the Authorization header set to "Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdv cms=". The response includes the status line and the "text/html" content type.

The screenshot shows a Wireshark capture window with four frames selected:

- Frame 3520: A successful HTTP GET request to "HTTP-wireshark-file5.html" with a status of 684.
- Frame 3613: An immediate response from the server with a status of 544.

The details pane displays the raw HTTP request and response. The request includes the URL and the Authorization header set to "Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdv cms=". The response includes the status line and the "text/html" content type.