

**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**  
**TRƯỜNG ĐẠI HỌC BÁCH KHOA**  
**KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH**



**MẠNG MÁY TÍNH TN (CO3094)**  
**BÀI TẬP LAB 1A – NETWORK DEVICES**  
**LỚP: L09**  
**GVHD: Bùi Xuân Giang**

**Sinh viên thực hiện**

Nguyễn Tấn Tài : 2212990

Thành phố Hồ Chí Minh, tháng 9 năm 2024

## Lab 2a: Wireshark HTTP

### 1. The Basic HTTP GET/response interaction

#### Các bước thực hiện

1. Mở trình duyệt web của bạn.
2. Khởi động Wireshark packet sniffer, như đã được mô tả trong phòng thực hành giới thiệu (nhưng đừng bắt gói tin ngay). Nhập “http” (chỉ nhập các ký tự, không nhập dấu ngoặc kép) vào cửa sổ chỉ định bộ lọc hiển thị, để chỉ những tin nhắn HTTP đã bắt được mới được hiển thị sau này trong cửa sổ danh sách gói tin. (Chúng ta chỉ quan tâm đến giao thức HTTP ở đây và không muốn xem lẫn lộn với tất cả các gói tin đã bắt được).
3. Chờ khoảng một phút (chúng ta sẽ thấy lý do ngay sau đây), sau đó bắt đầu bắt gói tin bằng Wireshark.
4. Nhập địa chỉ sau vào trình duyệt của bạn: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html> Trình duyệt của bạn sẽ hiển thị một tệp HTML rất đơn giản, chỉ có một dòng.
5. Dừng bắt gói tin của Wireshark.

**Ghi chú:** Bạn nên bỏ qua bất kỳ thông điệp HTTP GET và phản hồi nào dành cho **favicon.ico**. Nếu bạn thấy tham chiếu đến tệp này, đó là do trình duyệt của bạn tự động yêu cầu máy chủ xem liệu nó (máy chủ) có tệp biểu tượng nhỏ nên được hiển thị bên cạnh URL hiển thị trong trình duyệt của bạn hay không. Chúng ta sẽ bỏ qua các tham chiếu đến tệp phức tạp này trong bài thực hành này.

#### Trả lời các câu hỏi

1. Trình duyệt của bạn đang chạy HTTP phiên bản 1.0 hay 1.1? Phiên bản HTTP mà máy chủ đang chạy là gì?

Trong Wireshark, khi tìm thấy thông điệp HTTP GET, xem chi tiết của gói tin trong cửa sổ phân tích chi tiết, ta thấy phiên bản HTTP ở đó. Để tìm phiên bản của máy chủ, hãy kiểm tra phản hồi HTTP từ máy chủ (thông thường là một gói có mã trạng thái **200 OK**). Phiên bản HTTP của máy chủ cũng sẽ được hiển thị trong dòng tương tự.

```
HTTP/1.1 200 OK\r\n
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
```

2. Những ngôn ngữ nào (nếu có) mà trình duyệt của bạn chỉ ra rằng nó có thể chấp nhận từ máy chủ?

```
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
If-Modified-Since: Sat, 05 Oct 2024 05:59:02 GMT\r\n
```

Điều này có nghĩa là trình duyệt của bạn có thể chấp nhận nội dung bằng tiếng Anh (en-US).

3. Địa chỉ IP của máy tính của bạn là gì? Địa chỉ IP của máy chủ **gaia.cs.umass.edu** là gì?

```
C:\Users\DELL>nslookup gaia.cs.umass.edu
Server: Unknown
Address: fe80::b0e5:f9ff:fe11:4564

Non-authoritative answer:
Name:   gaia.cs.umass.edu
Address: 128.119.245.12
```

```
Wireless LAN adapter Wi-Fi 2:

Connection-specific DNS Suffix  . : 
IPv6 Address. . . . . : 2401:d800:291f:b3dd:b58f:f732:7a06:6055
Temporary IPv6 Address. . . . . : 2401:d800:291f:b3dd:c409:8031:c6a8:ccf1
Link-local IPv6 Address . . . . . : fe80::1613:46e5:c0a9:5240%21
IPv4 Address. . . . . : 172.20.10.3
Subnet Mask . . . . . : 255.255.255.240
Default Gateway . . . . . : fe80::b0e5:f9ff:fe11:4564%21
                          172.20.10.1
```

IP của máy tính: 172.10.10.3

IP của máy chủ **gaia.cs.umass.edu**: 128.119.245.12

4. Mã trạng thái nào được trả về từ máy chủ đến trình duyệt của bạn?

No.	Time	Source	Destination	Protocol	Length	Info
134	16:31:51.377195	128.119.245.12	172.20.10.3	HTTP	784	HTTP/1.1 200 OK (text/html)

Mã trả về: 200 OK.

5. Tập HTML mà bạn đang tải về đã được chỉnh sửa lần cuối tại máy chủ vào thời điểm nào?

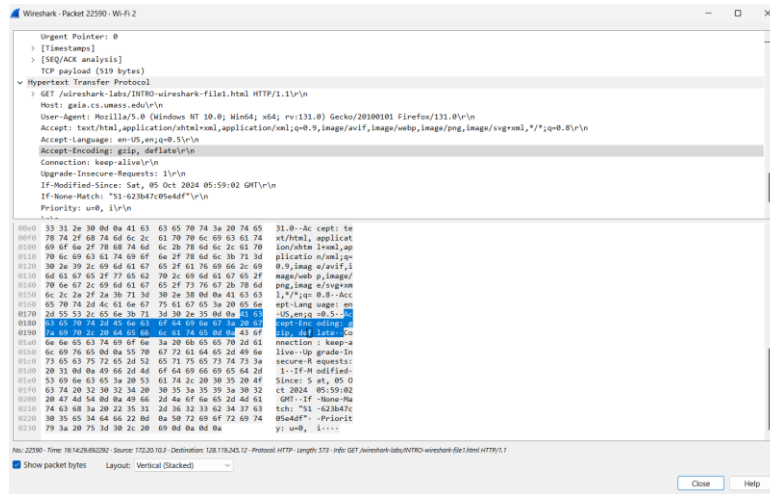
```
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
If-Modified-Since: Sat, 05 Oct 2024 05:59:02 GMT\r\n
```

Thay đổi lần cuối vào: 2h 59p 05, thứ 7, ngày 5, tháng 10, năm 2024.

6. Có bao nhiêu byte nội dung đang được trả về trình duyệt của bạn? → 371 bytes.

```
Content-Length: 371\r\n
```

7. Bằng cách kiểm tra dữ liệu thô trong cửa sổ nội dung gói tin, bạn có thấy bất kỳ tiêu đề nào bên trong dữ liệu mà không được hiển thị trong cửa sổ danh sách gói tin không? Nếu có, hãy nêu tên.



The image shows a Wireshark packet capture window for packet 22590. The packet is an HTTP GET request for a file named 'virefresh-file.html'. The packet structure is shown in the 'Packet Details' pane, and the raw data is shown in the 'Packet Bytes' pane. The raw data is displayed in hexadecimal and ASCII format. The packet structure is as follows:

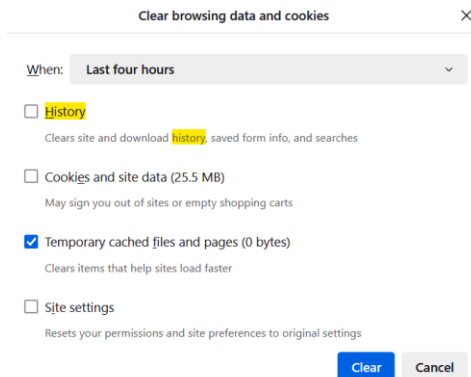
- Frame 22590: 1814 bytes on wire (14512 bits) captured (14512 bits) on interface 0
- Ethernet II, Src: Intel(R) Ethernet Controller (P0-P3), Dst: Intel(R) Ethernet Controller (P0-P3)
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.15
- TCP, Src Port: 54444, Dst Port: 80, Seq: 3110111111, Win: 65535, Len: 0
- Hypertext Transfer Protocol
  - Host: gaia.cs.umass.edu
  - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
  - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,\*/\*;q=0.8
  - Accept-Encoding: gzip, deflate
  - Connection: keep-alive
  - Upgrade-Insecure-Requests: 1
  - If-Modified-Since: Sat, 05 Oct 2024 05:59:02 GMT
  - If-None-Match: "51-623b47c05d4d"
  - Priority: u=0, l=1

Bằng cách di chuyển chuột theo từng khối của dữ liệu thô (ở dưới) và nhấn vào, em ko thấy dữ liệu nào không hiện thị nếu ta mở rộng tất cả nội dung ở trên bằng cách mở cách nút mũi tên.

## 2. The HTTP CONDITIONAL GET/response interaction

### Các bước thực hiện

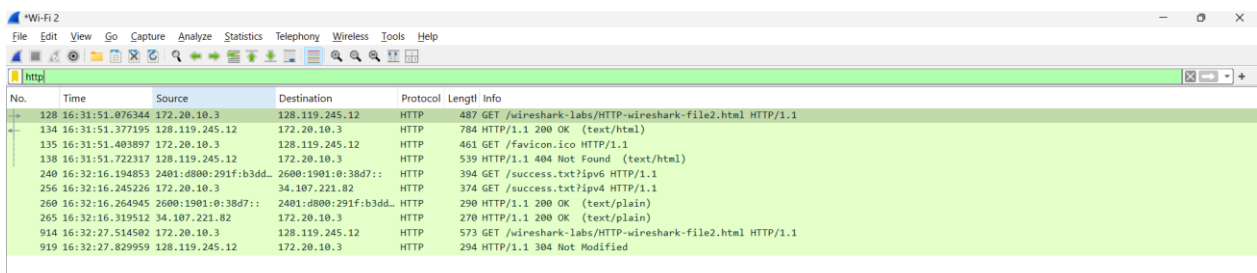
1. Mở trình duyệt web của bạn và đảm bảo rằng bộ nhớ cache của trình duyệt đã được xóa, như đã thảo luận ở trên (xóa cache).



2. Khởi động phần mềm Wireshark để bắt gói tin.
3. Nhập URL sau vào trình duyệt của bạn: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>. Trình duyệt của bạn sẽ hiển thị một tệp HTML rất đơn giản gồm 5 dòng.

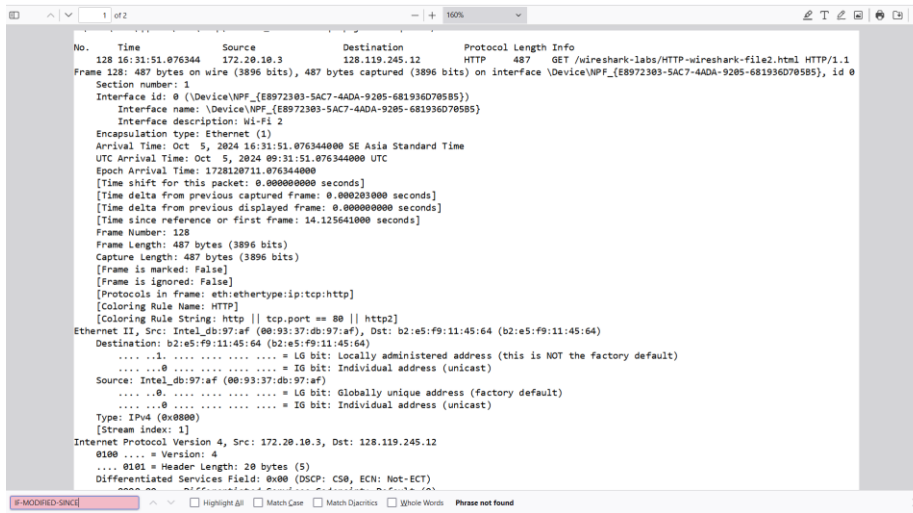


4. Nhanh chóng nhập lại cùng một URL vào trình duyệt của bạn (hoặc chỉ cần chọn nút làm mới trên trình duyệt của bạn).
5. Dừng việc bắt gói tin trên Wireshark và nhập "http" vào trong cửa sổ chỉ định bộ lọc hiển thị, để chỉ những thông điệp HTTP đã được bắt sẽ hiển thị trong cửa sổ danh sách gói tin.



## Trả lời câu hỏi

8. Kiểm tra nội dung của yêu cầu HTTP GET đầu tiên từ trình duyệt của bạn tới máy chủ. Bạn có thấy dòng IF-MODIFIED-SINCE trong yêu cầu HTTP GET không?



Không , yêu cầu đầu tiên thông thường sẽ không có tiêu đề IF-MODIFIED-SINCE.

9. Kiểm tra nội dung phản hồi của máy chủ. Máy chủ có trả lại nội dung của tệp không? Làm thế nào bạn biết được điều này?

Có, vì ta nhận được các tiêu đề phổ biến trong các gói tin phản hồi.

Time	Source	Destination	Protocol	Length	Info
134 16:31:51.377195	128.119.245.12	172.20.10.3	HTTP	784	HTTP/1.1 200 OK (text/html)

```
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
Priority: u=0, i\r\n
```

10. Bây giờ kiểm tra nội dung của yêu cầu HTTP GET thứ hai từ trình duyệt của bạn tới máy chủ. Bạn có thấy dòng IF-MODIFIED-SINCE trong yêu cầu HTTP GET không? Nếu có, thông tin nào theo sau tiêu đề IF-MODIFIED-SINCE?

```
Upgrade-Insecure-Requests: 1\r\n
If-Modified-Since: Sat, 05 Oct 2024 05:59:02 GMT\r\n
If-None-Match: "173-623b47c060037"\r\n
```

Có, thông tin đi kèm là thời gian lần cuối mà máy chủ báo cáo tệp được sửa đổi.

11. Mã trạng thái HTTP và cụm từ trả về từ máy chủ trong phản hồi đối với yêu cầu HTTP GET thứ hai là gì? Máy chủ có trả lại nội dung của tệp không? Giải thích.

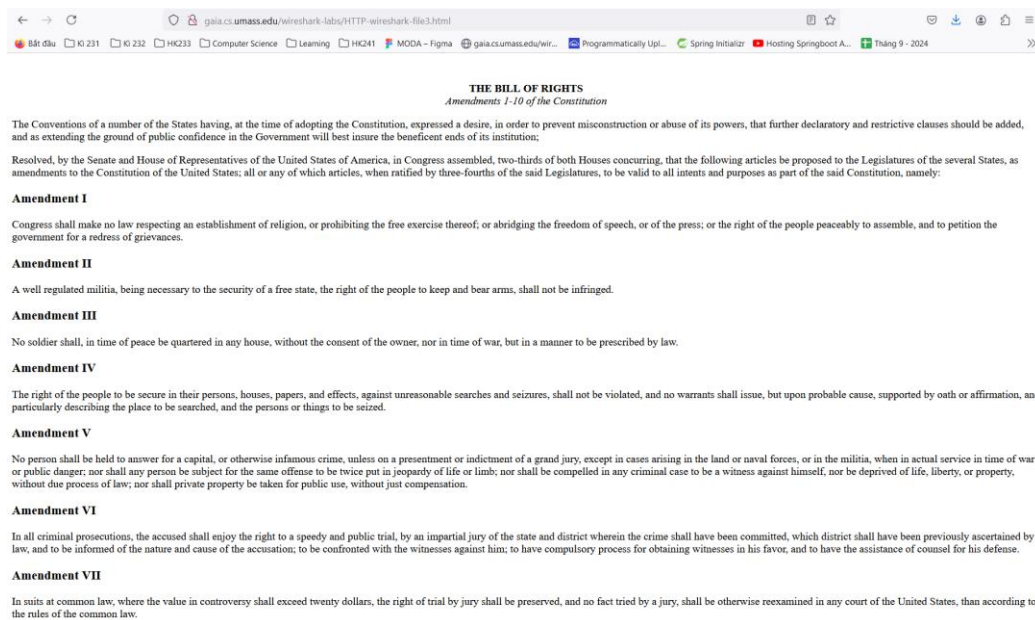
No.	Time	Source	Destination	Protocol	Length	Info
919	16:32:27.829959	128.119.245.12	172.20.10.3	HTTP	294	HTTP/1.1 304 Not Modified

Nếu tệp không thay đổi kể từ yêu cầu trước đó, mã trạng thái sẽ là 304 Not Modified. Điều này có nghĩa là máy chủ không gửi lại nội dung của tệp vì tệp không có thay đổi nào.

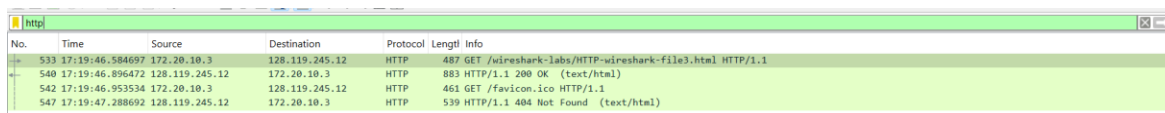
### 3. Retrieving Long Documents

#### Các bước thực hiện

1. Mở trình duyệt web của bạn và đảm bảo rằng bộ nhớ cache của trình duyệt đã được xóa, như đã thảo luận ở trên.
2. Khởi động phần mềm Wireshark để bắt gói tin.
3. Nhập URL sau vào trình duyệt của bạn: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html> Trình duyệt của bạn sẽ hiển thị văn bản **US Bill of Rights** khá dài.



4. Dừng bắt gói tin Wireshark và nhập "http" vào trong cửa sổ chỉ định bộ lọc hiển thị, để chỉ những thông điệp HTTP đã được bắt sẽ hiển thị.



No.	Time	Source	Destination	Protocol	Length	Info
533	17:19:46.584697	172.20.10.3	128.119.245.12	HTTP	487	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
540	17:19:46.896472	128.119.245.12	172.20.10.3	HTTP	883	HTTP/1.1 200 OK (text/html)
542	17:19:46.953534	172.20.10.3	128.119.245.12	HTTP	461	GET /favicon.ico HTTP/1.1
547	17:19:47.288692	128.119.245.12	172.20.10.3	HTTP	539	HTTP/1.1 404 Not Found (text/html)



## Trả lời câu hỏi

12. Có bao nhiêu thông điệp yêu cầu HTTP GET mà trình duyệt của bạn đã gửi? Số gói tin nào trong tệp theo dõi chứa thông điệp GET cho Bill of Rights?

No.	Time	Source	Destination	Protocol	Length	Info
533	17:19:46.584697	172.20.10.3	128.119.245.12	HTTP	487	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
540	17:19:46.896472	128.119.245.12	172.20.10.3	HTTP	883	HTTP/1.1 200 OK (text/html)
542	17:19:46.953534	172.20.10.3	128.119.245.12	HTTP	461	GET /favicon.ico HTTP/1.1
547	17:19:47.288692	128.119.245.12	172.20.10.3	HTTP	539	HTTP/1.1 404 Not Found (text/html)

Nếu không tính yêu cầu GET cho favicon, tổng cộng có 3 yêu cầu mà trình duyệt đã gửi. Để xác định số gói tin chứa thông điệp GET cho Bill of Rights, kiểm tra cột Info để thấy thông tin yêu cầu GET /wireshark-labs/HTTP-wireshark-file3.html, như vậy tổng cộng có 1 gói tin chứa thông điệp GET cho Bill of Rights.

13. Số gói tin nào trong tệp theo dõi chứa mã trạng thái và cụm từ liên kết với phản hồi đối với yêu cầu HTTP GET?

Từ hình ở trên, có 2 gói tin chứa mã trạng thái và cụm từ liên kết với phản hồi đối với yêu cầu HTTP GET, thứ 2 và thứ 4.

14. Mã trạng thái và cụm từ nào được trả về trong phản hồi?

Info

HTTP/1.1 200 OK (text/html)

Info

HTTP/1.1 404 Not Found

15. Có bao nhiêu phân đoạn TCP chứa dữ liệu đã cần thiết để truyền tải toàn bộ phản hồi HTTP và văn bản của Bill of Rights?

Phản hồi này là một tệp HTML dài và không thể chứa trong một gói TCP duy nhất. Trong Wireshark, ta sẽ thấy nhiều gói tin có phần thông tin như TCP segment of a reassembled PDU. Mỗi gói tin này là một phân đoạn của phản hồi. → 2 gói tin đầu tiên.

TCP payload (829 bytes)


TCP segment data (829 bytes)

TCP payload (433 bytes)

## 4. HTML Documents with Embedded Objects


### Các bước thực hiện

1. Mở trình duyệt web của bạn và đảm bảo rằng bộ nhớ cache của trình duyệt đã được xóa, như đã thảo luận ở trên.
2. Khởi động phần mềm Wireshark để bắt gói tin.
3. Nhập URL sau vào trình duyệt của bạn: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>. Trình duyệt của bạn sẽ hiển thị một tệp HTML gắn với hai hình ảnh. Hai hình ảnh này được tham chiếu trong tệp HTML gốc. Tức là, bản thân hình ảnh không được chứa trong tệp HTML mà thay vào đó là các URL cho hình ảnh này được chứa trong tệp HTML đã tải xuống. Như đã thảo luận trong sách giáo khoa, trình duyệt của bạn sẽ phải tải những logo này từ các trang web được chỉ định. Logo của nhà xuất bản của chúng tôi được tải từ trang web [gaia.cs.umass.edu](http://gaia.cs.umass.edu). Hình ảnh của bìa sách phiên bản thứ 5 của chúng tôi (một trong những bìa sách yêu thích của chúng tôi) được lưu trữ tại máy chủ [caite.cs.umass.edu](http://caite.cs.umass.edu). (Đây là hai máy chủ web khác nhau bên trong [cs.umass.edu](http://cs.umass.edu)).



Pearson

This little HTML file is being served by [gaia.cs.umass.edu](http://gaia.cs.umass.edu). It contains two embedded images. The image above, also served from the [gaia.cs.umass.edu](http://gaia.cs.umass.edu) web site, is the logo of our publisher, Pearson. The image of our 8th edition book cover below is stored at, and served from, a WWW server [kurose.cslash.net](http://kurose.cslash.net) in France:



James F. Kurose | Keith W. Ross

COMPUTER NETWORKING  
A TOP-DOWN APPROACH

And while we have your attention, you might want to take time to check out the available open resources for this book at [http://gaia.cs.umass.edu/kurose\\_ross](http://gaia.cs.umass.edu/kurose_ross).

4. Dừng bắt gói tin Wireshark và nhập "http" vào trong cửa sổ chỉ định bộ lọc hiển thị, để chỉ những thông điệp HTTP đã được bắt sẽ hiển thị.

No.	Time	Source	Destination	Protocol	Length	Info
618	17:36:01.982570	172.20.10.3	128.119.245.12	HTTP	487	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
624	17:36:02.279385	128.119.245.12	172.20.10.3	HTTP	1355	HTTP/1.1 200 OK (text/html)
638	17:36:02.300046	172.20.10.3	128.119.245.12	HTTP	464	GET /pearson.png HTTP/1.1
730	17:36:02.679670	128.119.245.12	172.20.10.3	HTTP	978	HTTP/1.1 200 OK (PNG)
751	17:36:03.224734	172.20.10.3	178.79.137.164	HTTP	431	GET /8E_cover_small.jpg HTTP/1.1
755	17:36:03.503559	178.79.137.164	172.20.10.3	HTTP	225	HTTP/1.1 301 Moved Permanently
796	17:36:04.125195	2401:d800:291f:b3dd::	2402:800:6353:1::7d::	OCSP	515	Request
812	17:36:04.345152	2401:d800:291f:b3dd::	2402:800:6353:1::7d::	OCSP	515	Request
815	17:36:04.389410	2402:800:6353:1::7d::	2401:d800:291f:b3dd::	OCSP	964	Response
839	17:36:04.849753	2402:800:6353:1::7d::	2401:d800:291f:b3dd::	OCSP	964	Response

**Trả lời câu hỏi**

16. Trình duyệt của bạn đã gửi bao nhiêu thông điệp yêu cầu HTTP GET? Các yêu cầu GET này đã được gửi tới các địa chỉ Internet nào?

Trình duyệt của tôi gửi đi 9 yêu cầu.

Các yêu cầu được gửi đi tới 2 địa chỉ Internet: gửi đến máy chủ **gaia.cs.umass.edu** để tải tệp HTML và logo; gửi đến máy chủ **caite.cs.umass.edu** để tải bìa sách.

Destination
128.119.245.12

Destination
128.119.245.12

17. Bạn có thể cho biết liệu trình duyệt của bạn đã tải về hai hình ảnh một cách tuần tự hay chúng được tải về từ hai trang web cùng lúc không? Giải thích.

Time
17:36:01.982570
17:36:02.279385
17:36:02.300046
17:36:02.679670
17:36:03.224734
17:36:03.503559
17:36:04.125195
17:36:04.345152
17:36:04.389410
17:36:04.849753

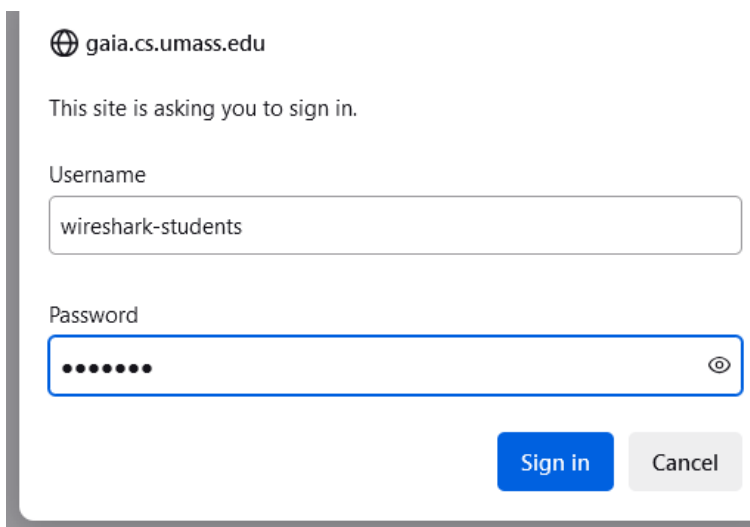
Nếu hai yêu cầu GET được gửi ngay lập tức hoặc rất gần nhau (trong khoảng thời gian nhỏ), điều đó có nghĩa là trình duyệt đã tải hình ảnh **song song** (tức là cùng lúc từ hai máy chủ).

Quan sát cột Time, ta thấy có sự chênh lệch nhưng rất gần nhau, tức là trình duyệt đã tải hình ảnh **song song**.

## 5. HTTP Authentication

### Các bước thực hiện

1. Đảm bảo rằng bộ nhớ cache của trình duyệt đã được xóa, như đã thảo luận ở trên, và đóng trình duyệt của bạn. Sau đó, mở lại trình duyệt của bạn.
2. Khởi động phần mềm Wireshark để bắt gói tin.
3. Nhập URL sau vào trình duyệt của bạn: [http://gaia.cs.umass.edu/wireshark-labs/protected\\_pages/HTTP-wireshark-file5.html](http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html).
4. Nhập tên người dùng và mật khẩu yêu cầu vào hộp bật lên.



gaia.cs.umass.edu

This site is asking you to sign in.

Username

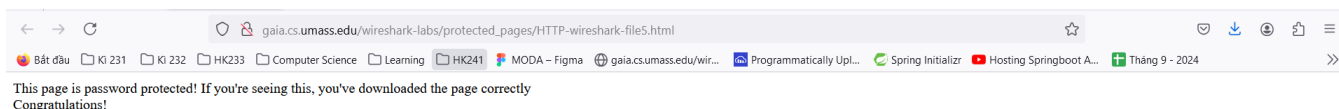
wireshark-students

Password

••••••••

Sign in Cancel

5. Dừng bắt gói tin Wireshark và nhập "http" vào trong cửa sổ chỉ định bộ lọc hiển thị, để chỉ những thông điệp HTTP đã được bắt sẽ hiển thị.



### Trả lời câu hỏi

18. Mã phản hồi của máy chủ (mã trạng thái và cụm từ) đối với thông điệp HTTP GET ban đầu từ trình duyệt của bạn là gì?

### Info

**HTTP/1.1 401 Unauthorized**

Trước khi nhập tên người dùng và mật khẩu, máy chủ sẽ gửi một phản hồi yêu cầu xác thực từ trình duyệt. ➔ 404 Unauthorized.

19. Khi trình duyệt của bạn gửi thông điệp HTTP GET lần thứ hai, trường mới nào được thêm vào trong thông điệp HTTP GET?

```
HTTP/1.1 200 OK (text/html)
Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcm0=\r\n
Credentials: wireshark-students:network
```

Trường mới được thêm vào trong thông điệp HTTP GET thứ hai là **Authorization: Basic**. Trường này chứa thông tin xác thực được mã hóa bằng Base64.