2

Lab 22222222222222222222 22222

BÁO CÁO BÀI THỰC HÀNH SỐ 2

Phân tích gói tin HTTP với Wireshark

Sniffing HTTP Traffic with Wireshark

Môn học: Nhập môn Mạng máy tính

|  |  |
| --- | --- |
| Sinh viên thực hiện | Mai Nguyễn Nam Phương (22521164) |
| Thời gian thực hiện | 15/10/2023 – 22/10/2023 |
| Tự chấm điểm | 10/10 |

TRẢ LỜI CÁC CÂU HỎI

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?

**Trả lời**: Trình duyệt đang sử dụng phiên bản HTTP 1.1, phiên bản của HTTP server là 1.1 Ảnh có chứa văn bản, Phông chữ, số, phần mềm

Mô tả được tạo tự động



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

**Trả lời**: Địa chỉ IP của máy tính là 172.20.10.2, của web server là 172.20.10.3

Ảnh có chứa văn bản, Phông chữ, số, phần mềm

Mô tả được tạo tự động



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

Bao gồm các mã 200 OK, 304 Not Modified, 302 Found

Ảnh có chứa văn bản, Phông chữ, số, phần mềm

Mô tả được tạo tự động



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

**Trả lời**: Server đã trả về 352 bytes nội dung

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, phần mềm

Mô tả được tạo tự động



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

**Trả lời**: Không có

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.

**Trả lời**: Quá trình cơ bản diễn ra như sau:

- Máy tính yêu cầu file (lệnh get)

- Máy chủ nhận được yêu cầu sẽ đi tìm kiếm xem file ở đâu.

+ Nếu như file cần tìm đã có sẵn ở bộ nhớ đệm cache thì sẽ lấy từ cache trả về.

+ Nếu file yêu cầu thực sự chưa có ở cache thì thực hiện tiếp.

- Sau đó, máy chủ tìm thấy file và trả về lại máy.

- Máy tải file và hiển thị cho người dung => Do đó, Server có trả về nội dung của file HTML.Vì trước khi truy cập trang web ta đã xóa cache nên khi ta chạy GET Request đầu tiên cho máy chủ, file chưa hề lưu trong bộ nhớ cache nên máy chủ sẽ tải trực tiếp file về

- Mã trạng thái đi kèm là 200 OK: Yêu cầu đã thành công.

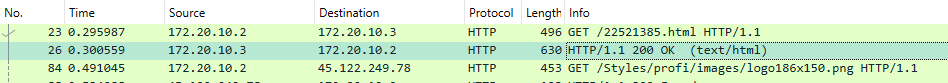
Ý nghĩa của thành công còn phụ thuộc vào phương thức HTTP là gì:

+ GET: Tài nguyên đã được tìm nạp và được truyền trong nội dung thông điệp.

+ HEAD: Các header thực thể nằm trong nội dung thông điệp.

+ PUT hoặc POST: Tài nguyên mô tả kết quả của hành động được truyền trong nội dung thông điệp.

+ TRACE: Nội dung thông điệp chứa thông báo yêu cầu khi máy chủ nhận được. => Ta chỉ xét phương thức GET cho bài này, do đó ý nghĩa của mã 200 ở đây là: Tài nguyên đã được tìm nạp và được truyền trong nội dung thông điệp.





Câu 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?

**Trả lời**: Ta có thấy dòng IF-MODIFIED-SINCEẢnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, phần mềm

Mô tả được tạo tự động



Giá trị của If-Modified-Since: Wed, 15 Nov 2023 07:05:31 GMT

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

**Trả lời**: - Mã trạng thái HTTP được trả về từ Server tương ứng với lần GET thứ 2 là: 304 Not Modified.

- 304 Not Modified: Code này được sử dụng cho mục đích caching. Nó 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 thực sự gởi về nội dung của file. Giải thích:

+ Ở lần GET đầu tiên: file chúng ta Request không có sẵn trong cache nên phải lên trực tiếp máy chủ để lấy về và khi đó máy chủ phản hồi lại nội dung mà ta cần, đồng thời lưu vào cache của trình duyệt đó.

+ Ở lần GET thứ 2 ta lại gửi một Request trùng ở lần GET đầu tiên và vì nó đã được lưu trong cache ở trình duyệt. Nên ta có thể thấy được 2 Request trùng nhau thông qua dòng If-modified-since, nó sẽ trả về nội dung giống như ở lần GET đầu tiên.

* Nên lúc này ta chỉ nhận file được lấy tại Cache mà không cần lên Máy chủ để lấy => Server không trả về nội dung đó nữa và phản hồi với mã trạng thái 304.

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Mô tả được tạo tự động



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

**Trả lời**: Trình duyệt đã gửi 4 HTTP GET, đến 2 địa chỉ IP  
172.20.10.3 và 45.122.249.78

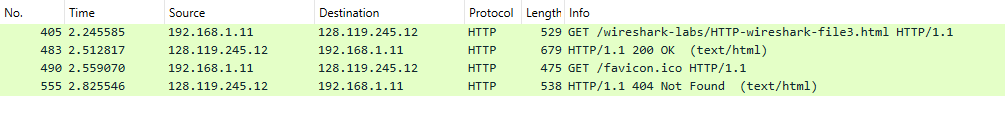
Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Mô tả được tạo tự động



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

**Trả lời**: Trình duyệt đã gửi 2 HTTP GET





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

**Trả lời**:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, Trang web

Mô tả được tạo tự động



Dựa trên hình ảnh trên ta sẽ thấy cần 4 TCP segments để chứa hết response và nội dung của The Bill of Rights

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

**Trả lời**:

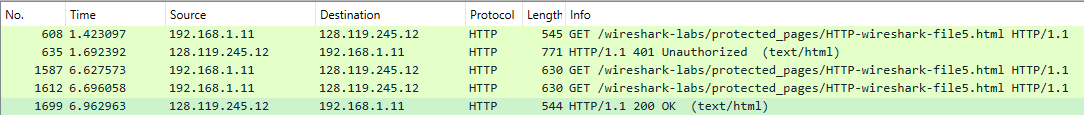
Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, phần mềm

Mô tả được tạo tự động



Được chứa trong gói tin phản hồi thứ nhất

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



Mã trạng thái được trả về là 401 Unauthorized

Ý nghĩa: là một phản hồi từ máy chủ web cho biết người dùng hoặc máy ứng dụng không có quyền truy cập tài nguyên được yêu cầu. Mã này thông báo rằng yêu cầu không được chấp nhận vì người dùng chưa xác thực hoặc xác thực không thành công. Ví dụ: cấm truy cập 1 file trong thư mục nào đó trong hosting đối với người dùng dù có được link

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

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, phần mềm

Mô tả được tạo tự động



Trường dữ liệu mới xuất hiện là trường Authoriration