2

Lab

**BÁO CÁO BÀI THỰC HÀNH SỐ 1**

**Phân tích gói tin HTTP với Wireshark**

(Sniffing HTTP Traffic with Wireshark)

**Môn học: Nhập môn Mạng máy tính**

|  |  |
| --- | --- |
| **Giảng viên hướng dẫn** | ThS. Đỗ Thị Hương Lan |
| **Sinh viên thực hiện** | Nguyễn Duy Khang (22520619) |
| **Mức độ hoàn thành** | Hoàn thành |
| **Thời gian thực hiện** | 22/09/2019 – 29/09/2019 |
| **Tự chấm điểm** | 9.5/10 |

* 1. **CÁC BƯỚC THỰC HÀNH**

**Gợi ý:** *Ghi rõ từng bước thực hành, chụp hình ảnh screenshot để báo cáo thêm trực quan*

* 1. **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.*

**Ví dụ:**

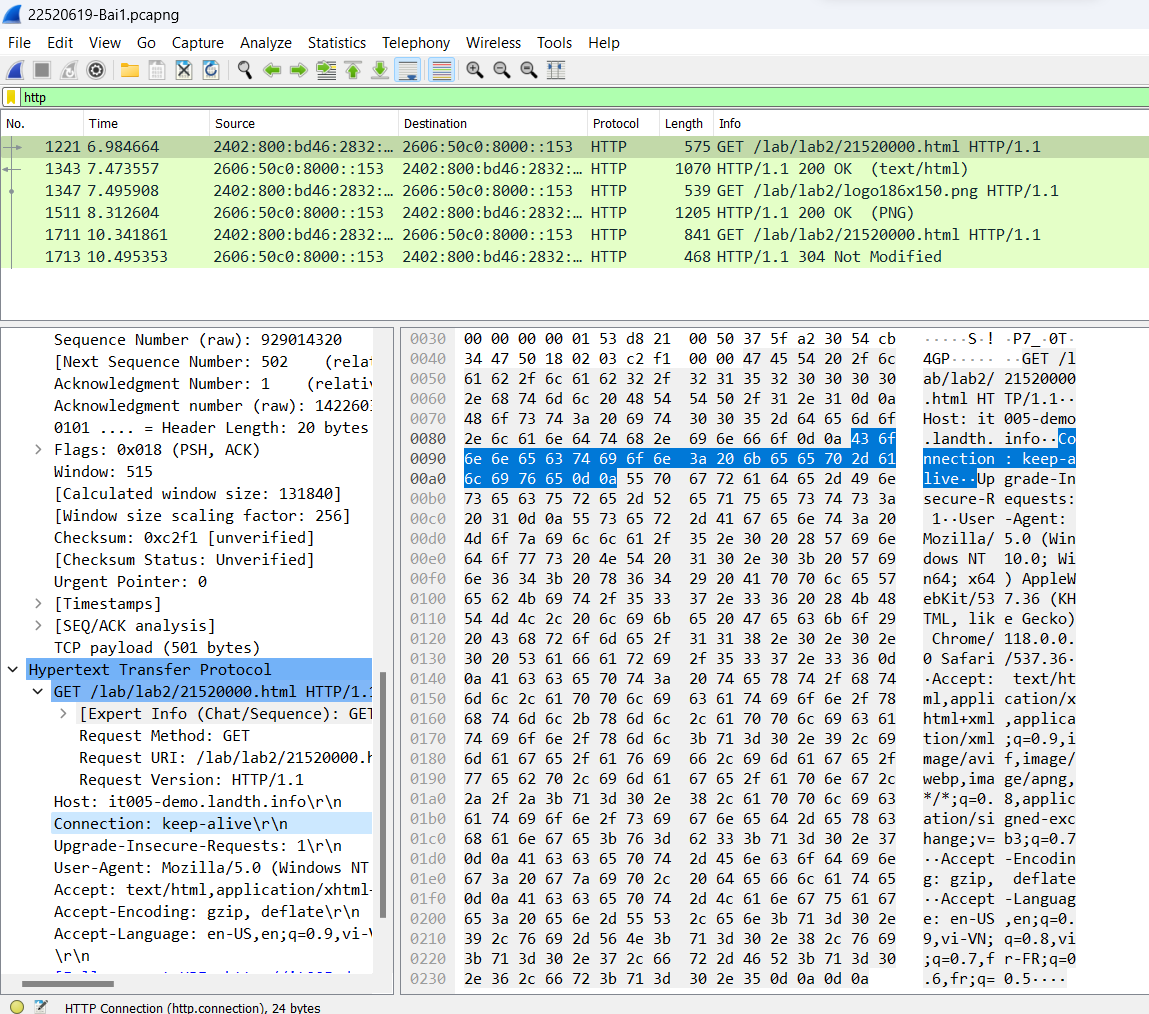
*Câu 1. Địa chỉ IP máy tính của bạn là gì?*

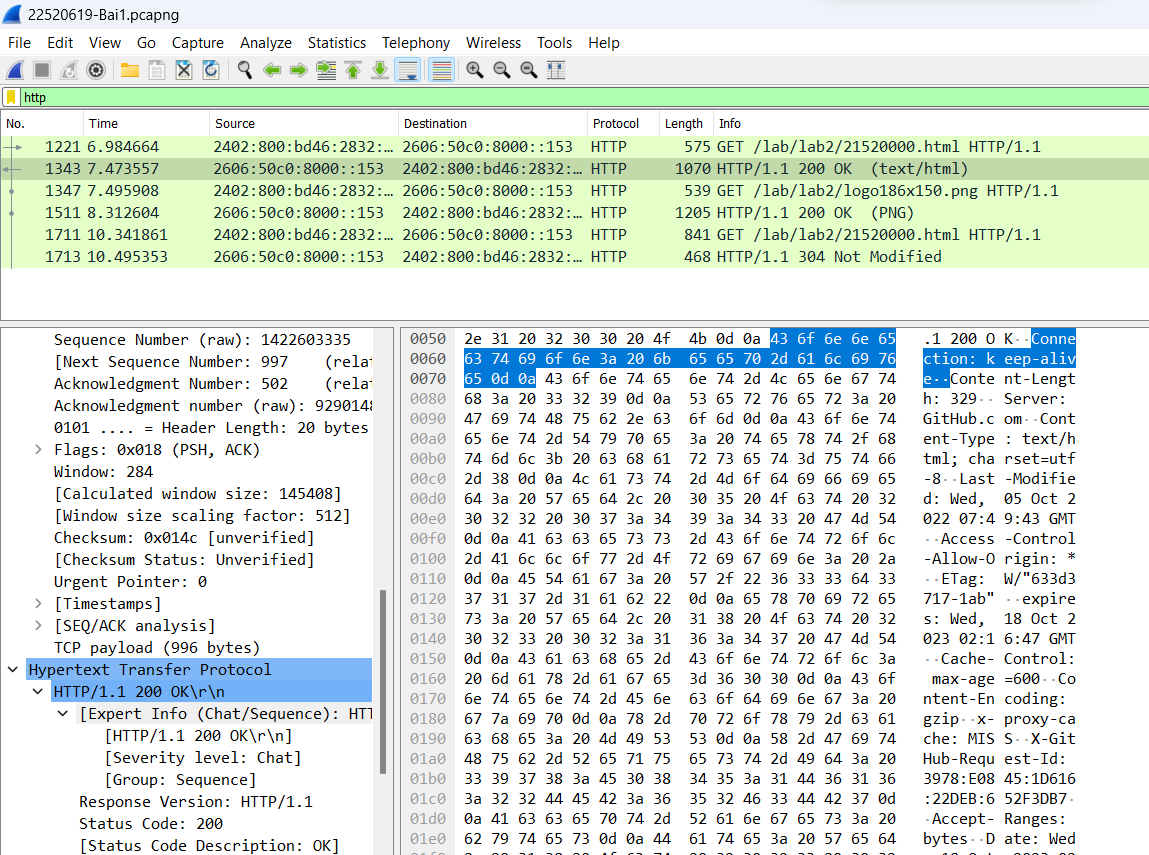
***Trả lời:*** *192.168.1.106*

Để xem địa chỉ IP của máy tính trên Windows, mở **Control Panel** và chọn **View network status and tasks.** Chọn mạng tương ứng đang sử dụng để kết nối Internet, chọn **Details** trong cửa sổ trạng thái. Xem địa chỉ IP trong Ipv4 Address

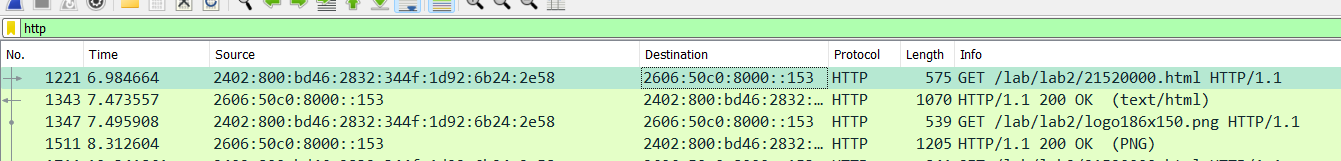


1. HTTP có điều kiện
2. Trình duyệt đang sử dụng phiên bản HTTP 1.0 hay 1.1? Phiên bản HTTP server đang sử dụng là bao nhiêu?



* 1. Trình duyệt đang sử dụng phiên bản HTTP 1.1, có thể quan sát được ở mục Hypertext Transfer Protocol -> Request Version: HTTP/1.1
  2. Phiên bản HTTP server đang sử dụng là HTTP/1.1 200 OK\r\n , có thể quan sát được như sau
  3. 

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



* 1. Thông qua phần Destination của gói tin 1221, ta thấy đây là điểm đến web được gửi từ máy tính, nên 2606:50c0:8000::153 là IP version 6 của web
  2. Địa chỉ IP của máy dự đoán sẽ nằm ở phần Source, chính là nguồn gởi gói tin đến điểm đến, nguồn gởi ở đây là máy tính, vậy địa chỉ IP version 6 của máy đang sử dụng là 2402:800:bd46:2832:344f:1d92:6b24:2e58

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

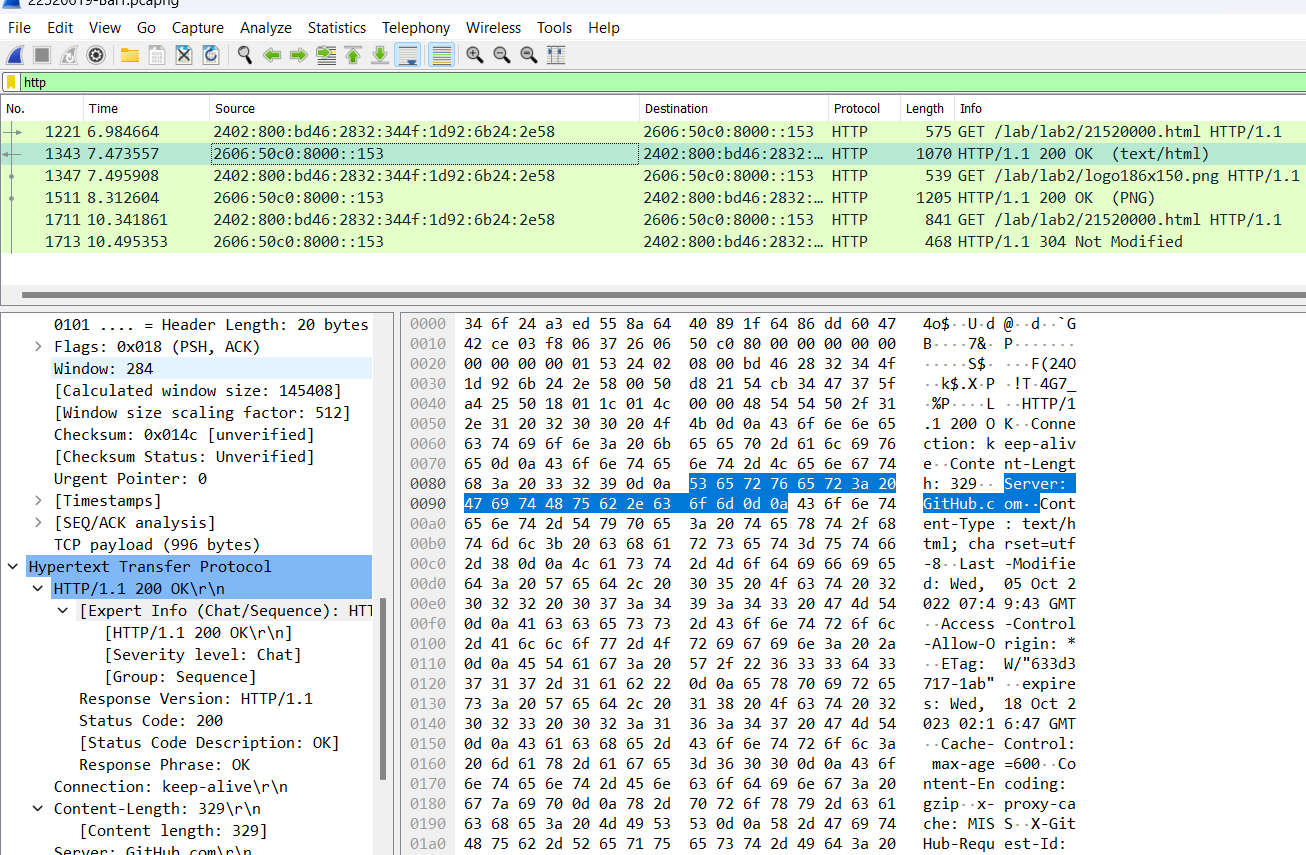
A screenshot of a computer

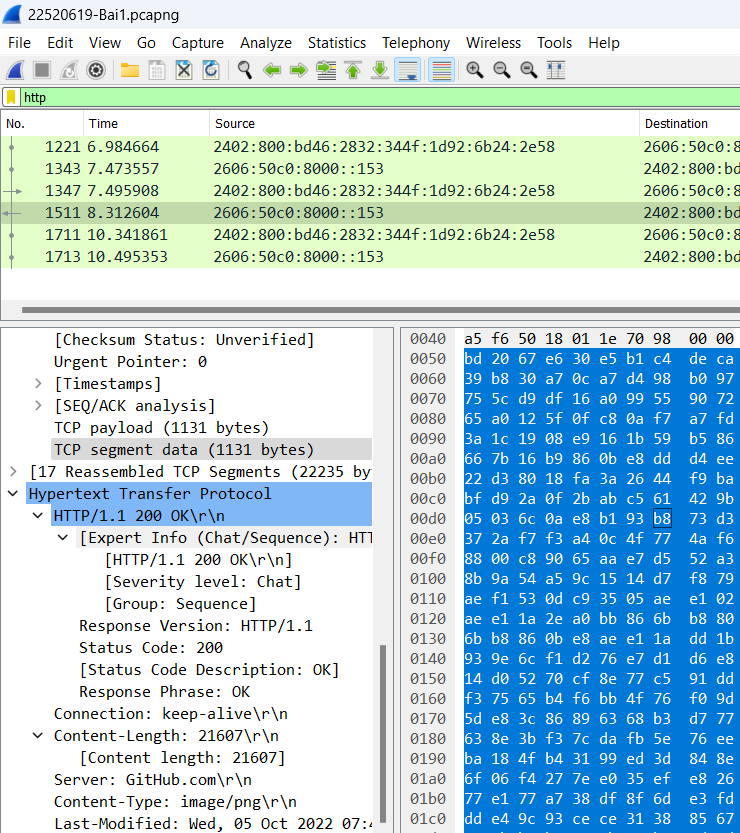
Description automatically generated



* 1. Quan sát gói tin phản hồi trả về, là gói tin thứ 1343, ở mục Status Code :200 , vậy mã trạng thái sever trả về là 200

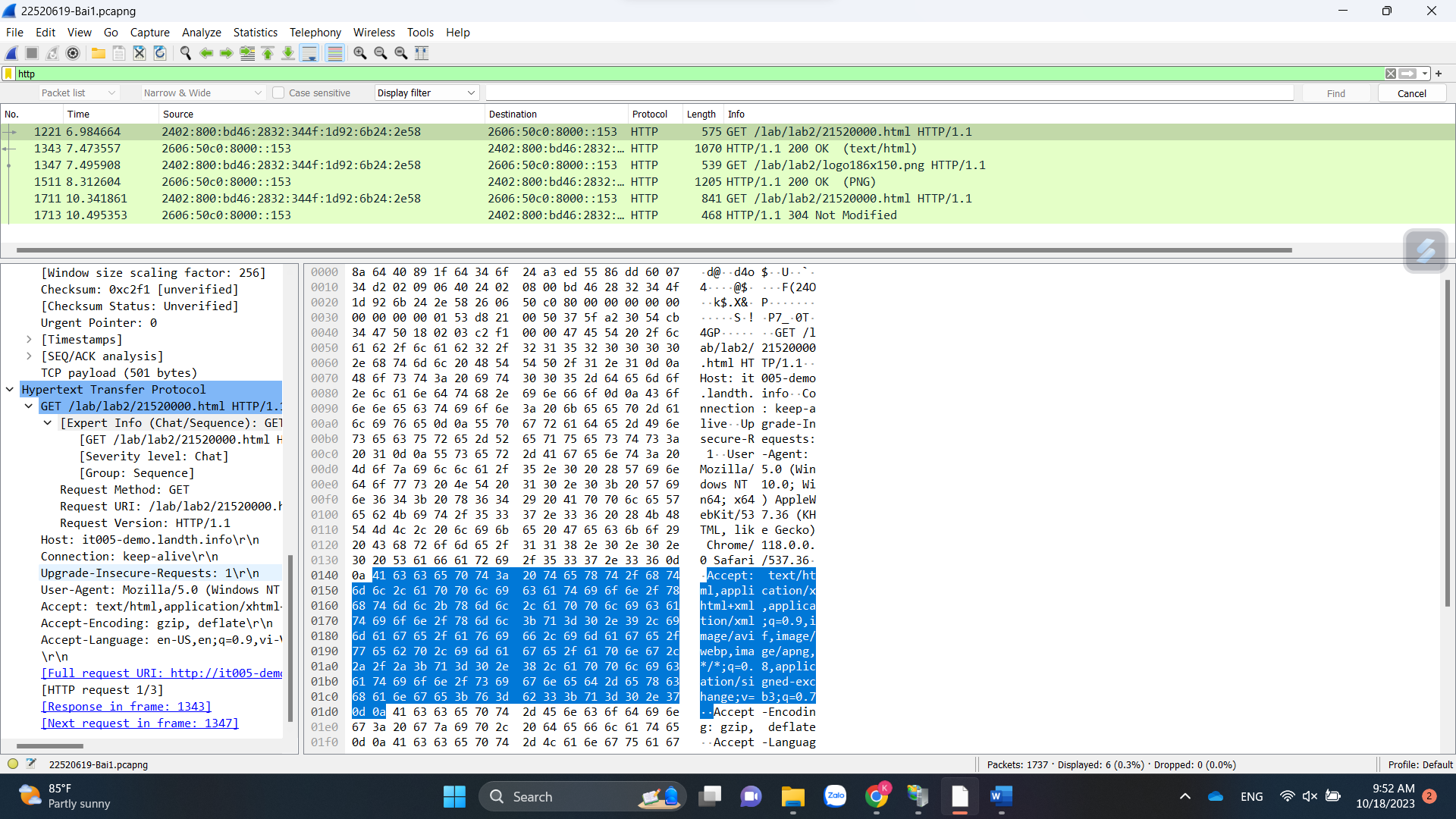
1. Server đã trả về cho trình duyệt tổng cộng bao nhiêu bytes nội dung?





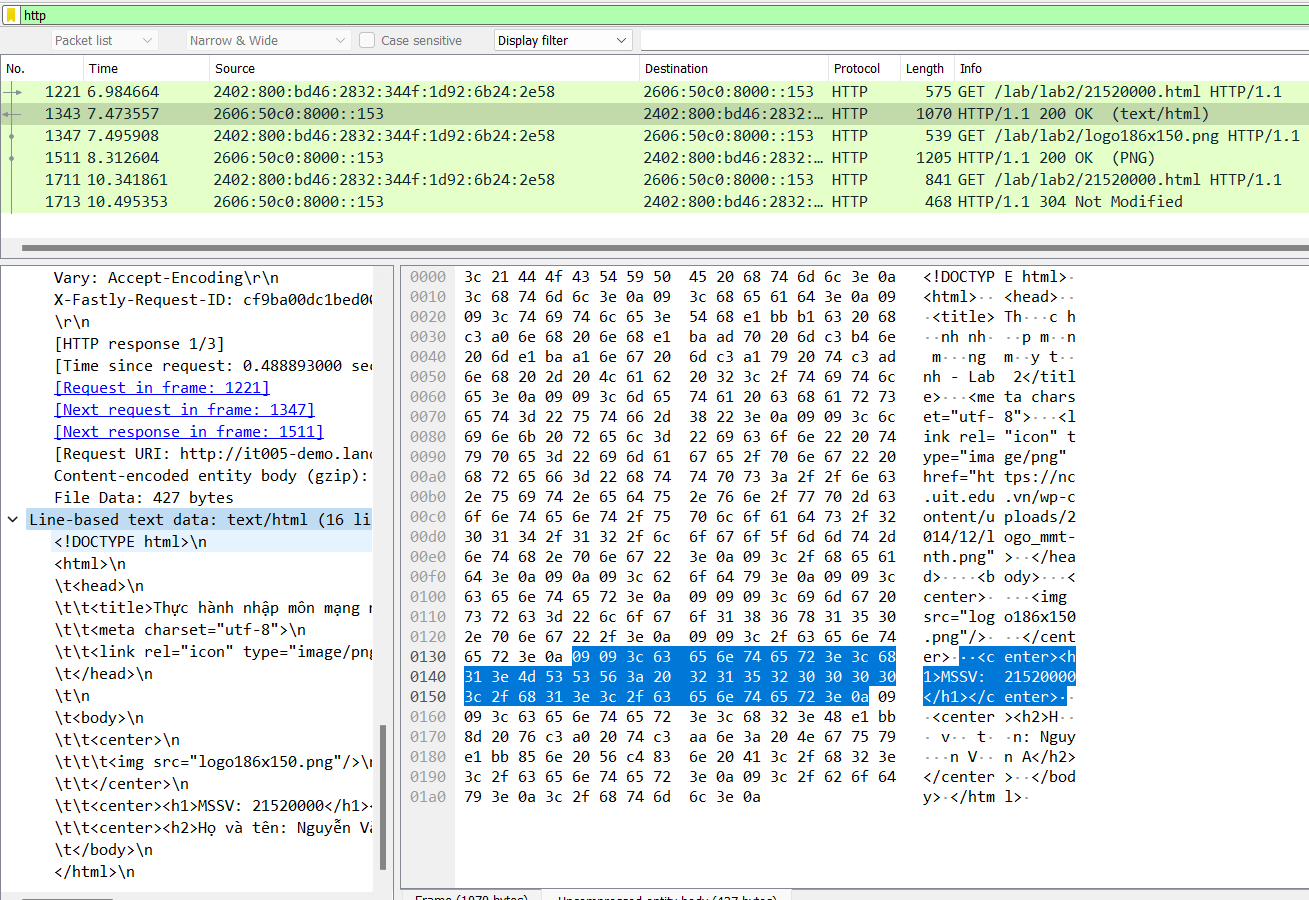
* 1. Tổng Content length chương trình trả về là 329 + 21607 = 21936 bytes nội dung

1. Xem xét nội dung của **HTTP GET** đầu tiên. Bạn có thấy dòng **“IF-MODIFIED-SINCE”** hay không?  
   *Gợi ý:****HTTP GET đầu tiên****là gói tin đầu tiên yêu cầu đến URL đang truy cập. Bỏ qua các gói tin không liên quan khác*



* 1. Không quan sát được dòng **“IF-MODIFIED-SINCE”**  của HTTP GET đầu tiên

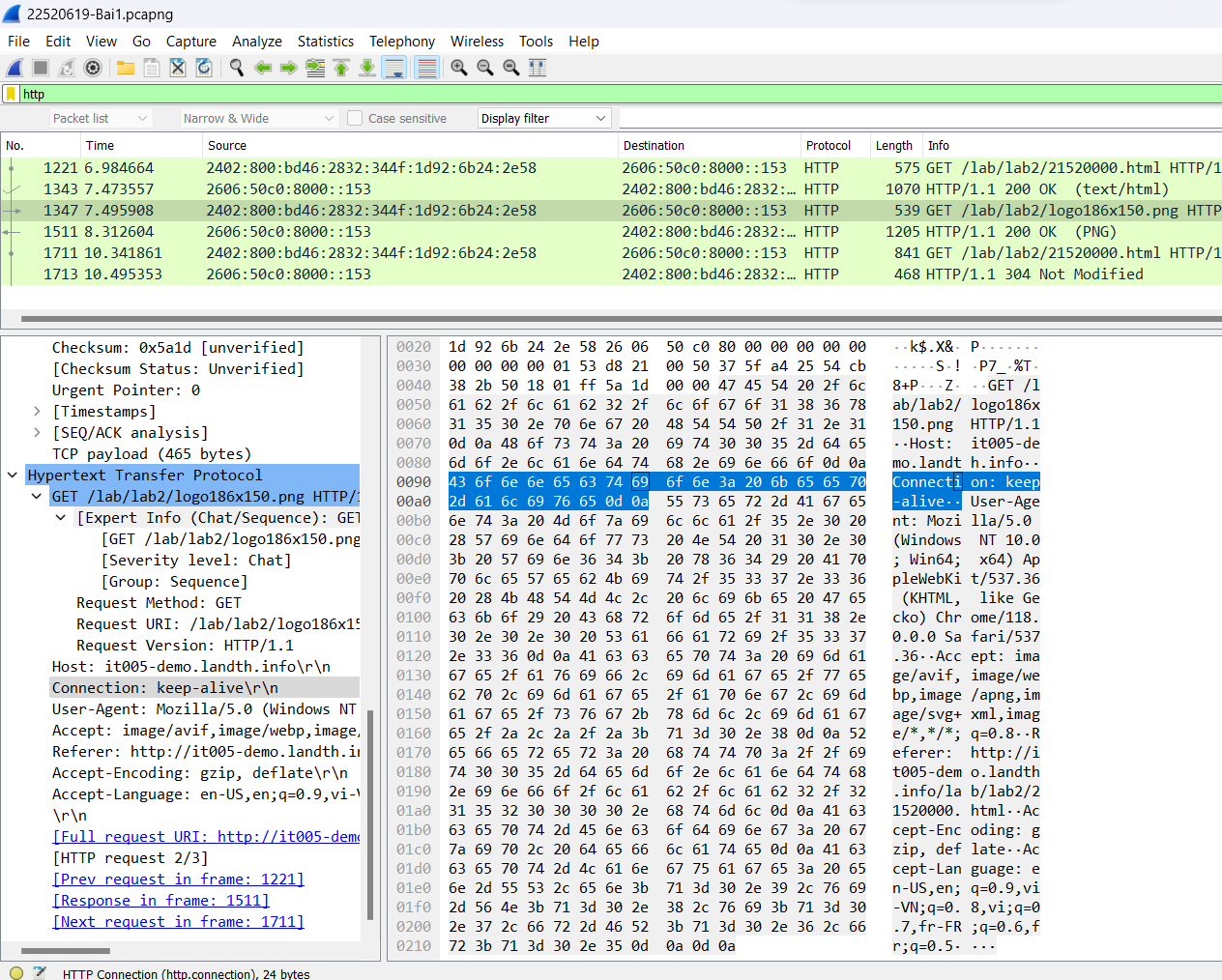
1. Xem xét nội dung phản hồi từ server đối với HTTP GET đầu tiên. Server có trả về nội dung của file HTML hay không? Mã trạng thái đi kèm là gì? Giải thích ý nghĩa



* 1. Sever có trả về nội dung ở dòng Line-based text data, status code trả về là 200 ở vị trí được khoanh đỏ, ý nghĩa của mã trạng thái này là mã trạng thái thành công được trả về khi yêu cầu được xử lý thành công và trang web trả về dữ liệu yêu cầu.

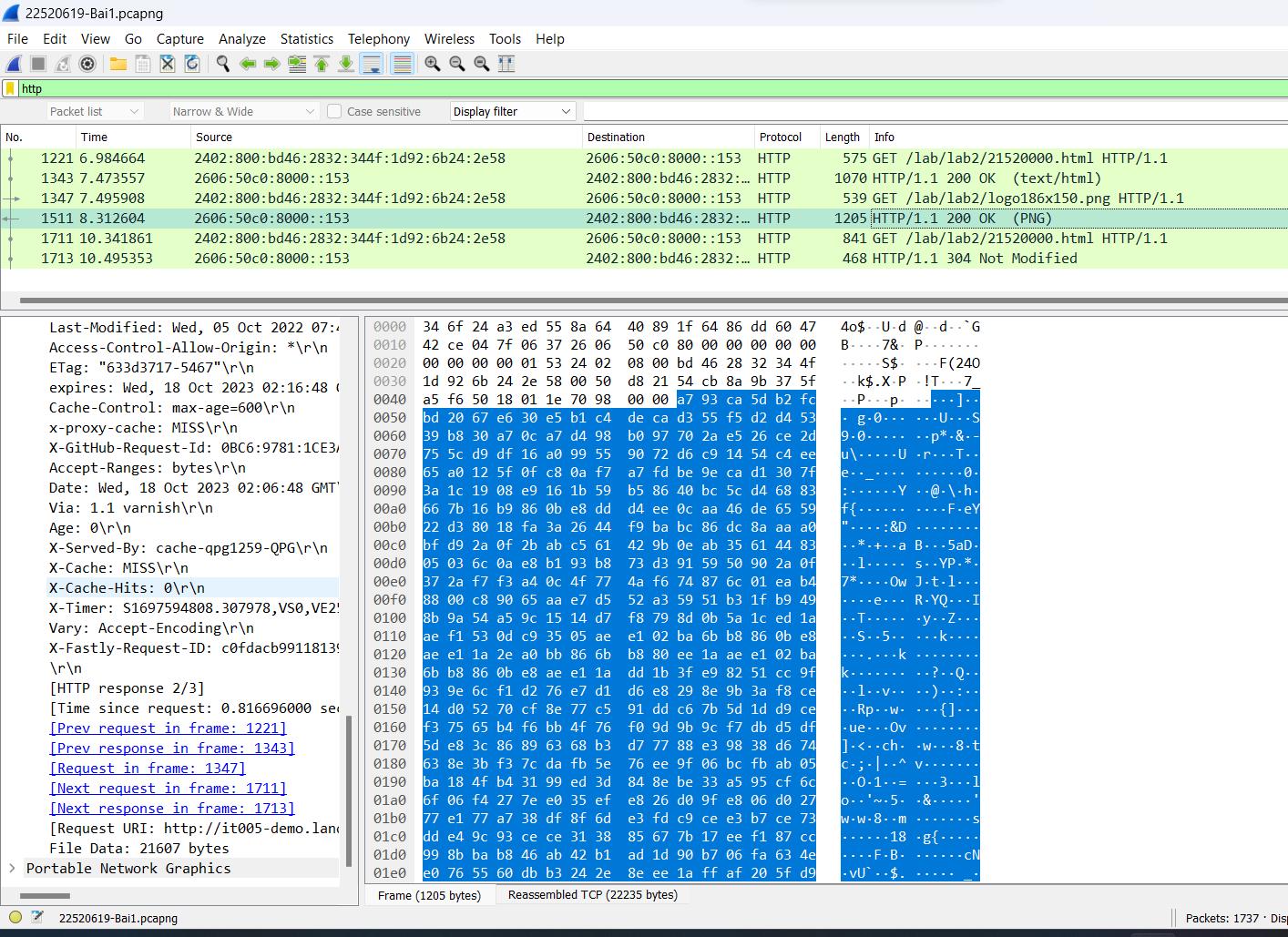
1. Xem xét nội dung của **HTTP GET** thứ 2. Bạn có thấy dòng **“IF-MODIFIED-SINCE”** hay không? Nếu có, giá trị của **IF-MODIFIED-SINCE** là gì?

*Gợi ý:****HTTP GET thứ 2****là gói tin thứ 2 yêu cầu đến URL đang truy cập. Bỏ qua các gói tin không liên quan khác*



* 1. Không quan sát được dòng **“IF-MODIFIED-SINCE”**  của HTTP GET thứ 2

1. 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
   1. Mã trạng thái HTTP được trả về từ server tương ứng với **HTTP GET** thứ 2 là: 200, có thể quan sát được ở vị trí được khoanh đỏ, ý nghĩa của mã trạng thái này là mã trạng thái thành công được trả về khi yêu cầu được xử lý thành công và trang web trả về dữ liệu yêu cầu.
   2. Không quan sát được nội dung của file gửi về vì không có mục Line-based text data



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

* Trình duyệt đã gửi 3 HTTP GET đến cùng 1 địa chỉ IP là 2606:50c0:8000::153, có thể quan sát được ở mục destination ở các HTTP GET này

A screenshot of a computer

Description automatically generated

1. Truy cập các trang HTTP dài
2. Trình duyệt đã gửi bao nhiêu HTTP GET?

* Trình duyệt đã gửi tổng cộng 2 HTTP GET, có thể quan sát được ở ảnh bên dưới

A screenshot of a computer

Description automatically generated

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

* Thông qua chi tiết gói tin, cần 2 TCP segments để chứa hết HTTP response và nội dung của The Bill of Rights

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated

* Dòng chữ “THE BILL OF RIGHTS” được chứa trong gói tin phản hồi đầu tiên, ở chi tiết gói tin

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

A screenshot of a computer

Description automatically generated

* Mã trạng thái trong HTTP response tương ứng với HTTP GET đầu tiên là: 401
* Ý nghĩa của status code 401: Header yêu cầu không chứa mã xác thực cần thiết và client bị từ chối truy cập.

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

A screenshot of a computer

Description automatically generated

* Browser gửi HTTP GET lần 2 sau khi nhập user name và password để gửi lên server, field mới xuất hiện trong HTTP GET: Authorization: BasicZXRoLXN0dWRlbnRzOm5ldHdvcmtz \r\n