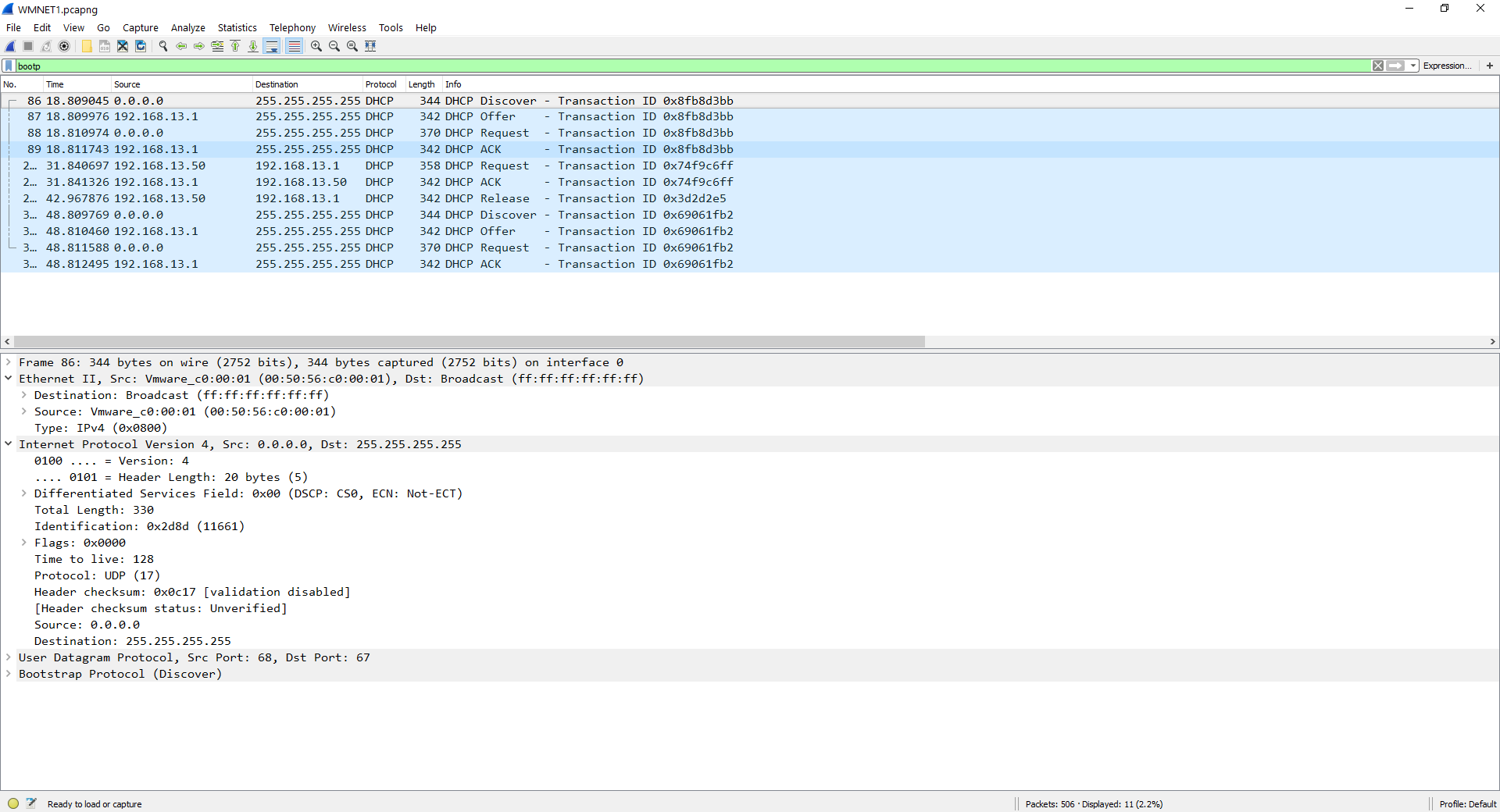
Phần 1:

1. Kiểm tra với các gói tin bắt được bằng Wireshark, ta thấy ở mục Internet Protocal sử dụng UDP.



1. Biểu đồ thời gian minh họa sự trao đổi giữa 4 gói đầu tiên (Discover/Offer/Request/ACK) DHCP của máy client và server:

DHCP ACK

DHCP REQUEST

DHCP OFFER

DHCP DISCOVER

Port 68

Port 68

Port 68

Port 68

Port 67

Port 67

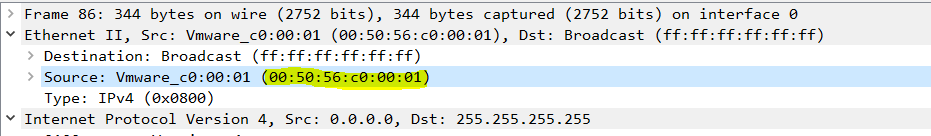
Port 67

Port 67

Server – IP: 192.168.13.1

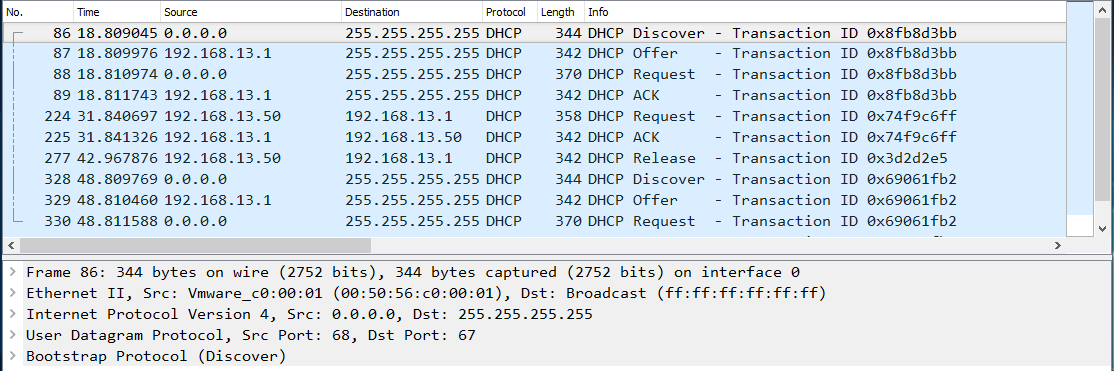
Client

1. Địa chỉ MAC của máy host là: 00:50:56:c0:00:01

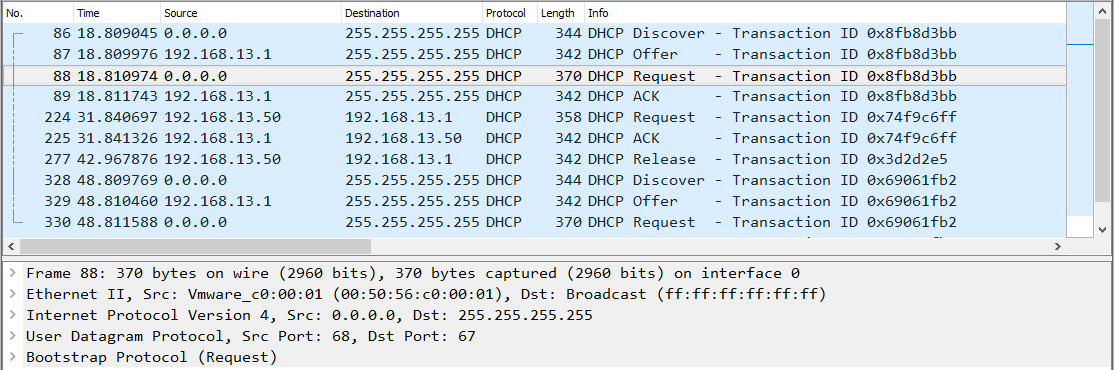


1. Điểm khác nhau giữa DHCP DISCOVER và DHCP REQUEST là:

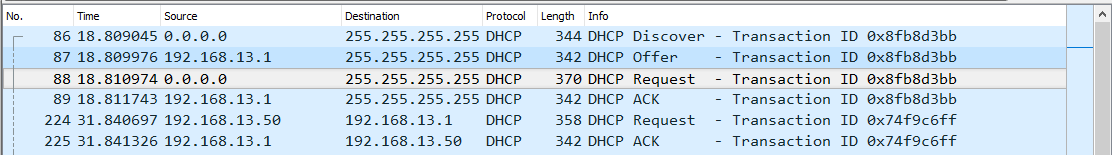
* Kiểu tin nhắn gửi đi DHCP
* Yêu cầu bao gồm trường định danh máy chủ
* Frame
* DHCP DISCOVER:



* DHCP REQUEST:

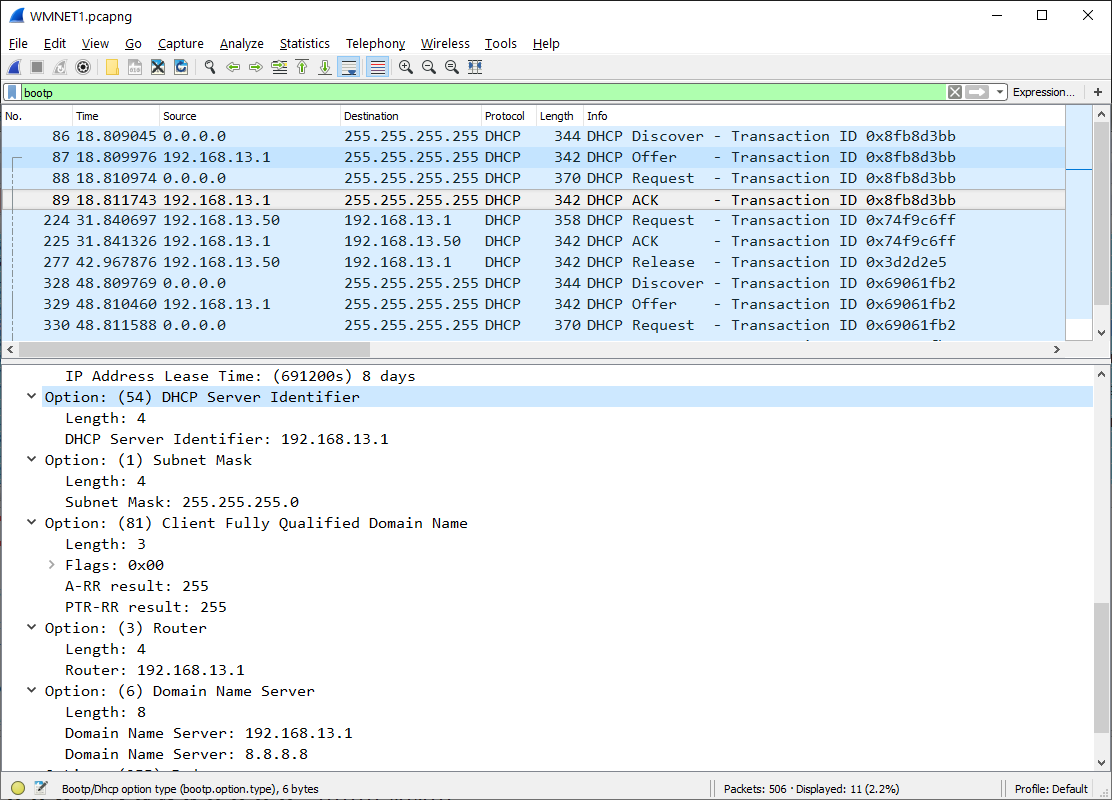


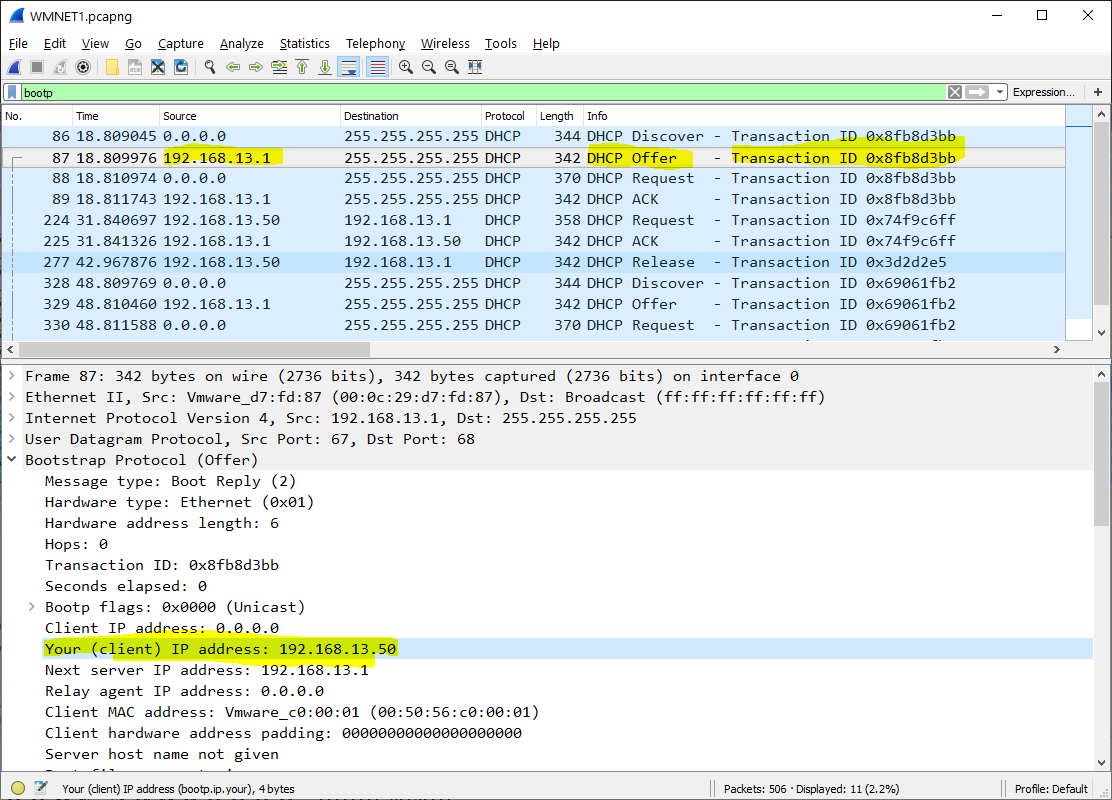
* Giá trị của Transaction-ID trong 4 gói tin đầu là: 0x8fb8d3bb
* Giá trị của Transaction-ID trong 2 gói tin sau(DHCP REQUEST/ACK) là: 0x74f9c6ff



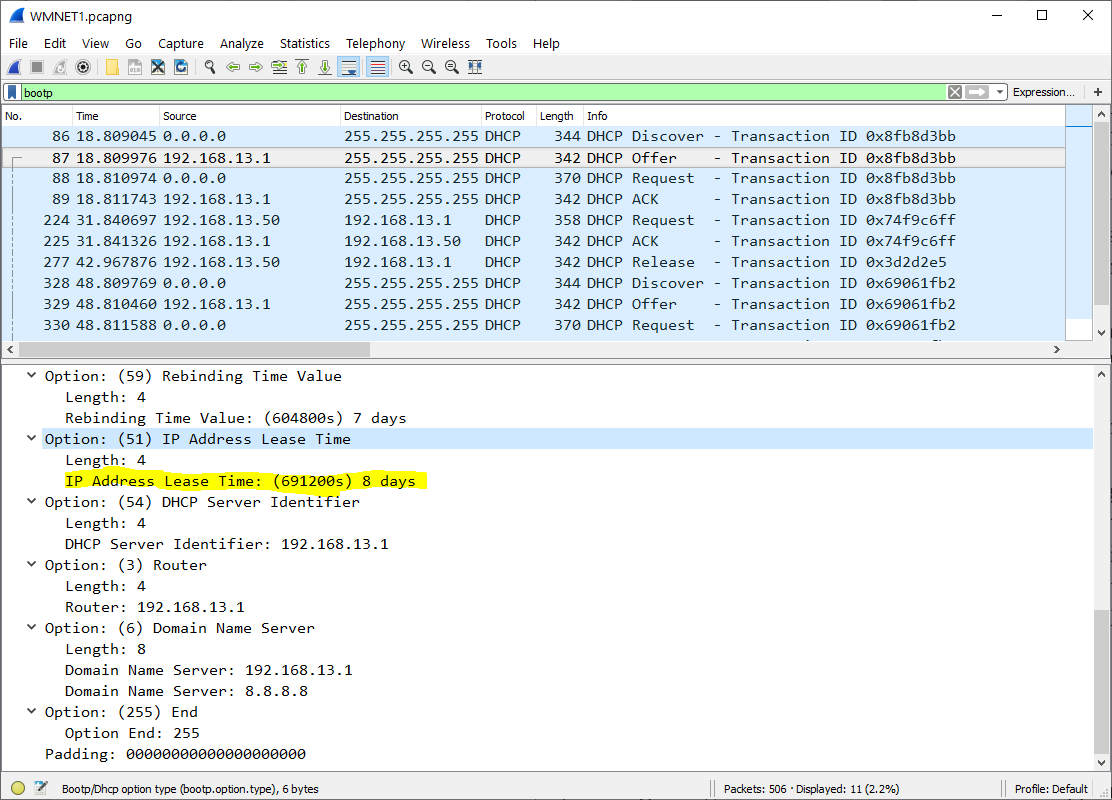
* Mục đích của Transaction-ID là: transaction-id là khác nhau để máy chủ có thể phân biệt được các yêu cầu khác nhau được thực hiện bởi người dùng.
* Discover: 0.0.0.0 / 255.255.255.255
* Offer: 192.168.13.1 / 255.255.255.255
* Request: 0.0.0.0 / 255.255.255.255
* ACK: 192.168.13.1 / 255.255.255.255

1. Địa chỉ IP của DHCP server là: 192.168.13.1

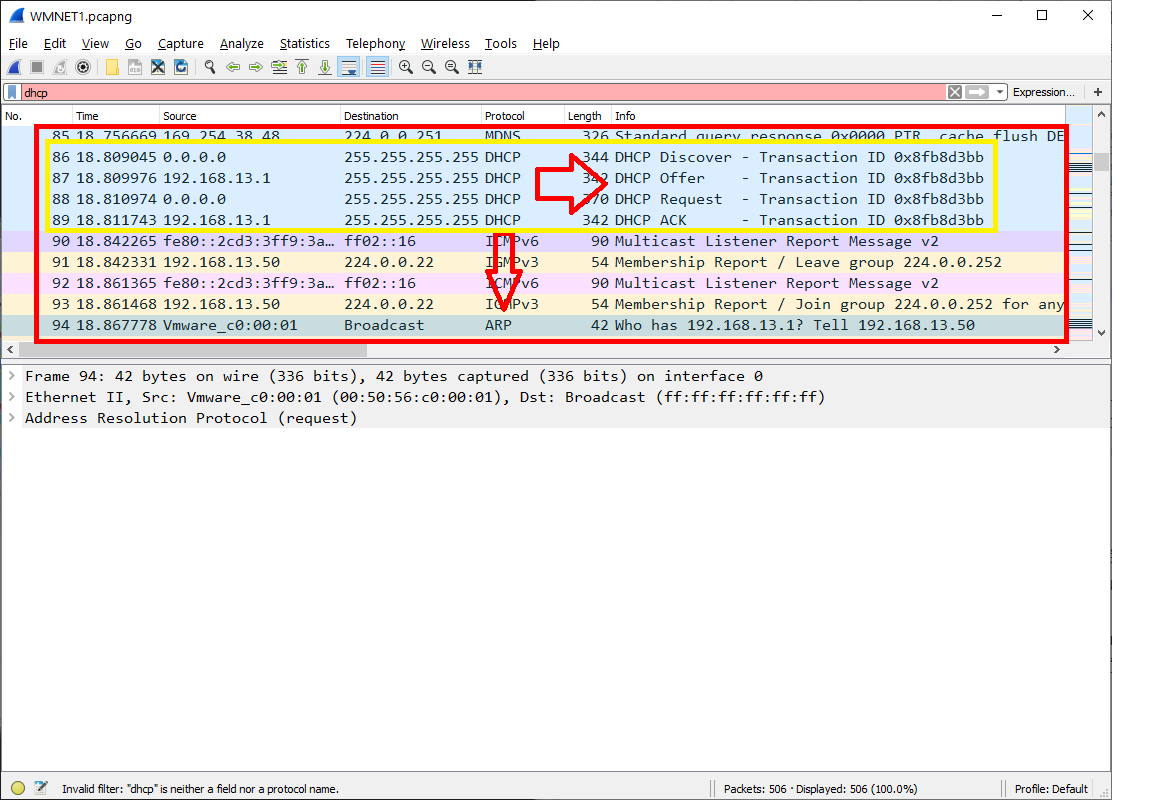


1. 

* DHCP mà server cấp cho DHCP OFFER là 192.168.13.50
* Tin nhắn cung cấp chứa địa chỉ DHCP được cung cấp bởi máy chủ

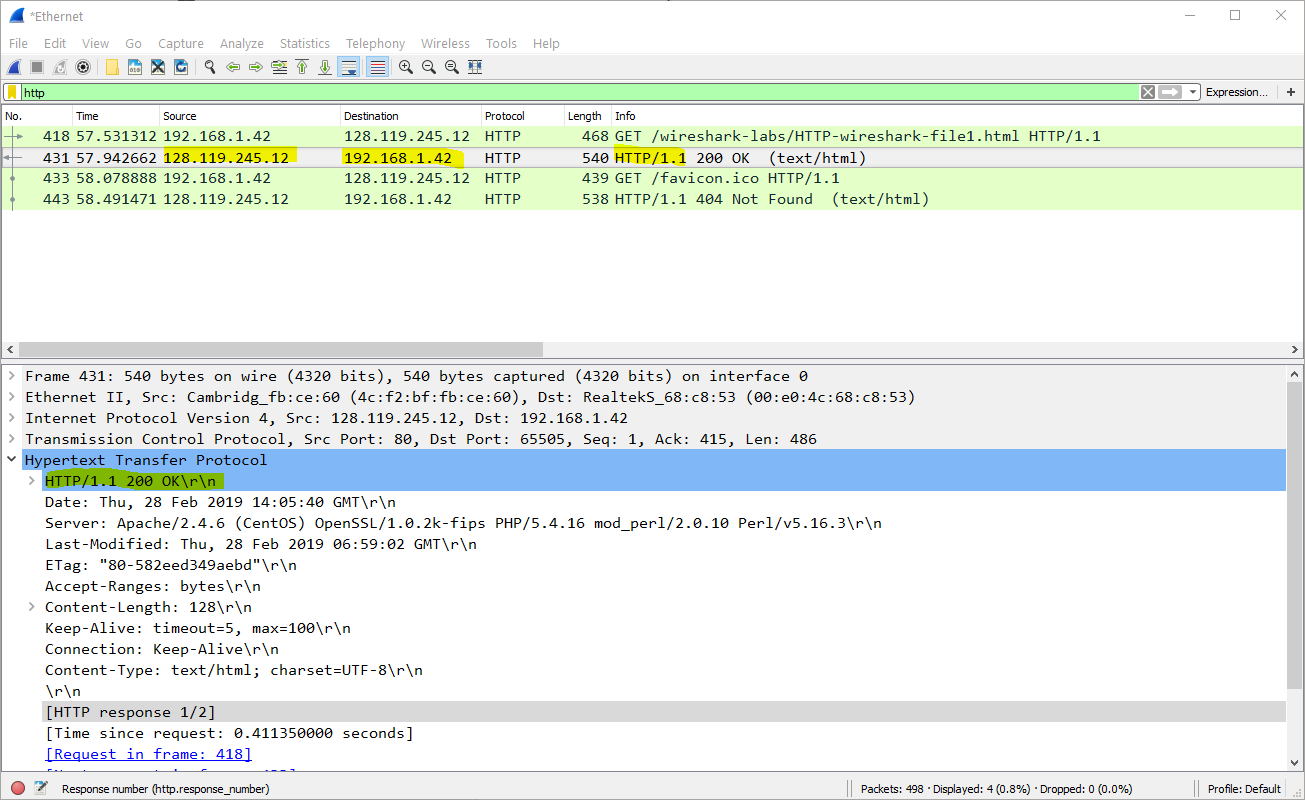
1. 

* Lease time(thời gian cho thuê): tức là một thiết bị được gán địa chỉ IP trong thời gian, sau thời gian đó, nó được gia hạn thời gian thuê và được cấp địa chỉ IP mới hoặc là địa chỉ IP đó sẽ được chuyển cho người khác nếu bạn không gia hạn thêm thời gian thuê.
* Mục đích của lease time là đem cho người dùng thuê và quản lý số lượng thiết bị sử dụng bởi vì nỗi lo hết địa chỉ IP do quá nhiều thiết bị sử dụng (thu hồi lại địa chỉ IP không được gia hạn).
* Không có bất kì xác nhận nào cho việc yêu cầu địa chỉ IP của máy chủ.
* Nếu như tin nhắn của DHCP REQUEST bị mất, máy của client sẽ giải phóng địa chỉ IP, nhưng máy chủ sẽ không xác nhận được rằng IP của clients đã giải phóng mà cho tới khi thời gian cho thuê hết thì máy chủ sẽ không gán IP đó cho bất kì thiết bị nào cho đến khi hết hạn.

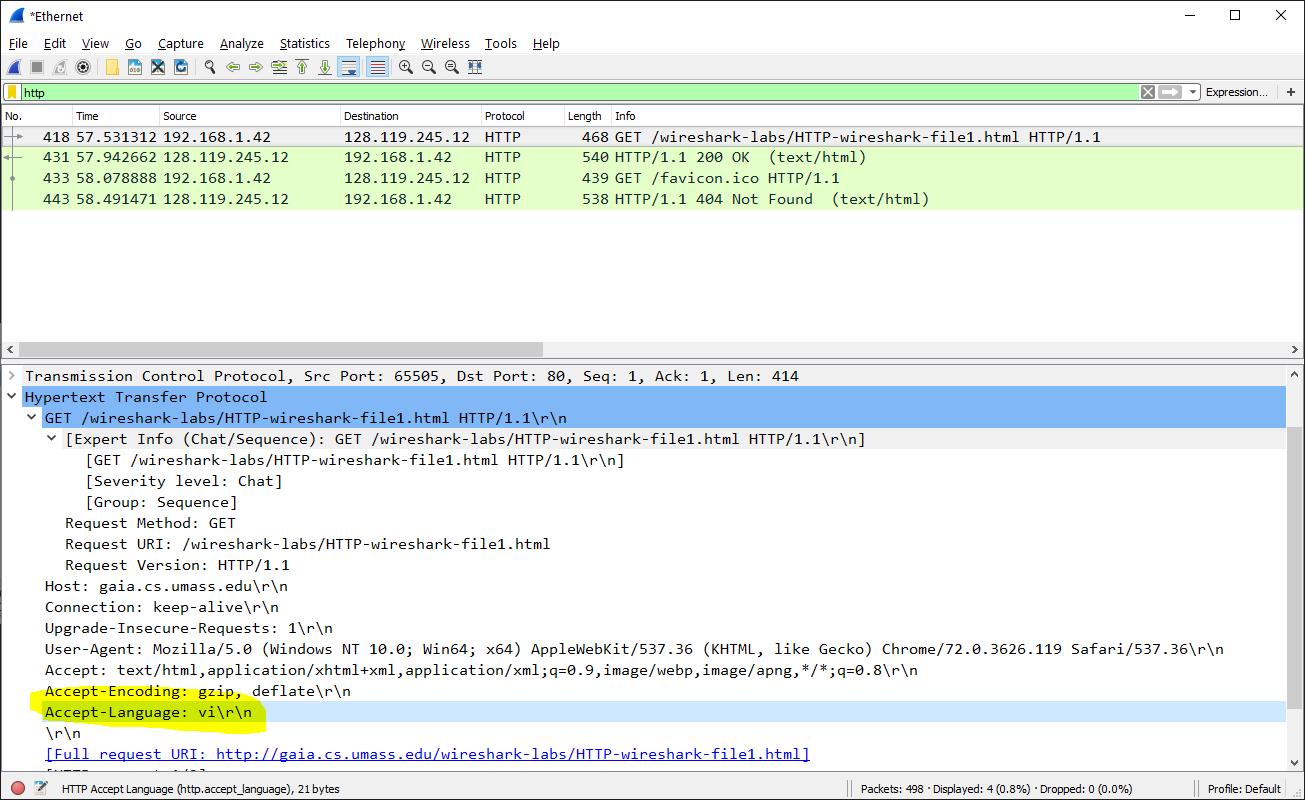
1. 

* Có xuất hiện các gói tin ARP, chúng dường như là các chương trình phát sóng được gửi bởi networks để xây dựng các địa chỉ IP đã biết bởi mạng của clients.

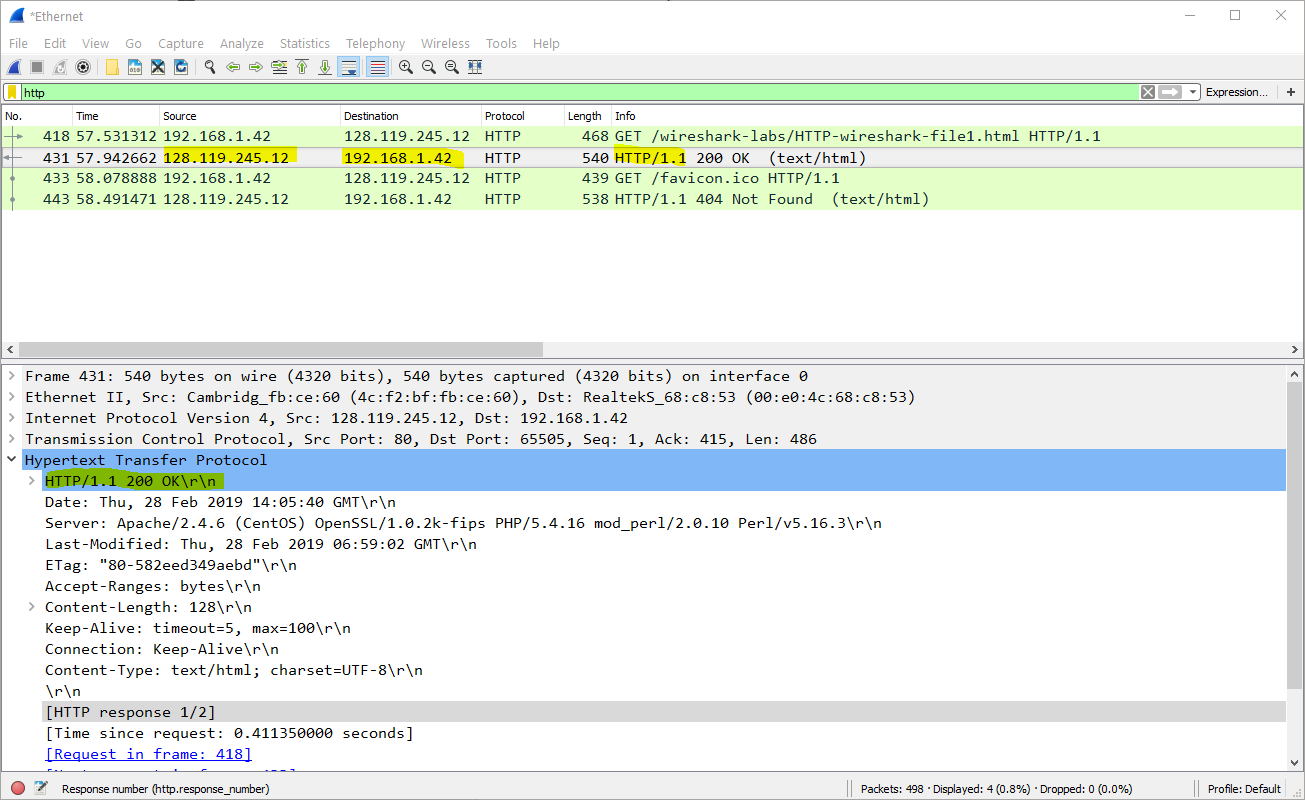
HTTP

1. The Basic HTTP GET/response interaction
2. 

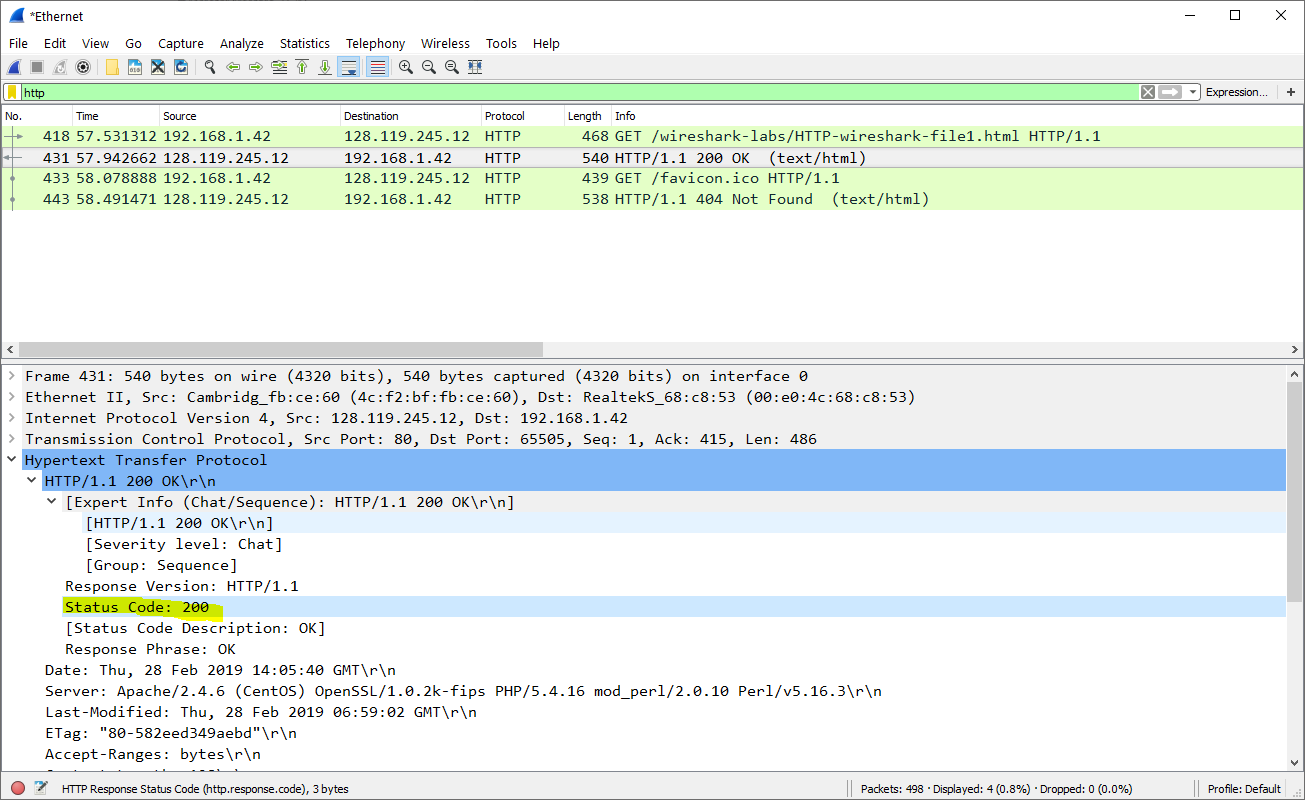
* Qua hình cho thấy cả trên trình duyệt web của em lẫn như cả trên server đều chạy HTTP version 1.1

1. 

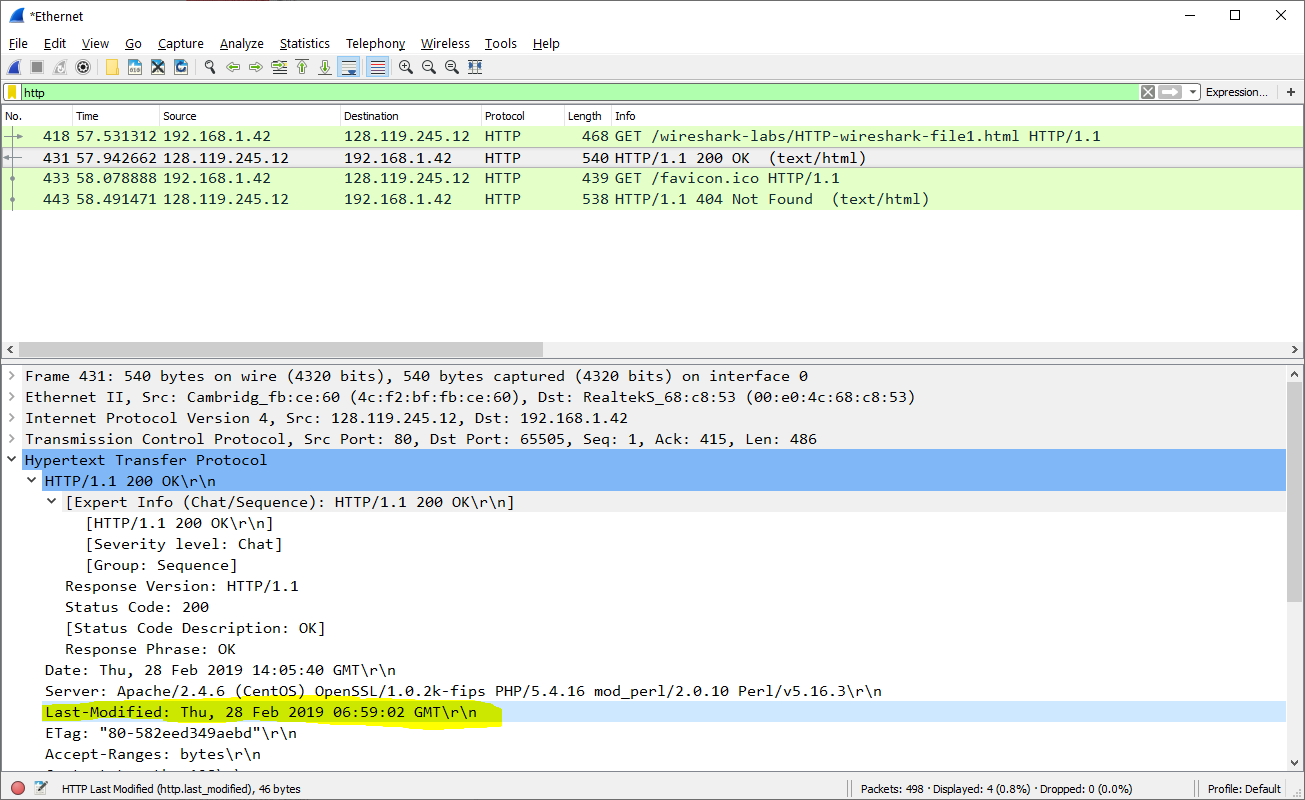
* Ngôn ngữ được chấp nhận là: vi(Tiếng Việt).

1. 

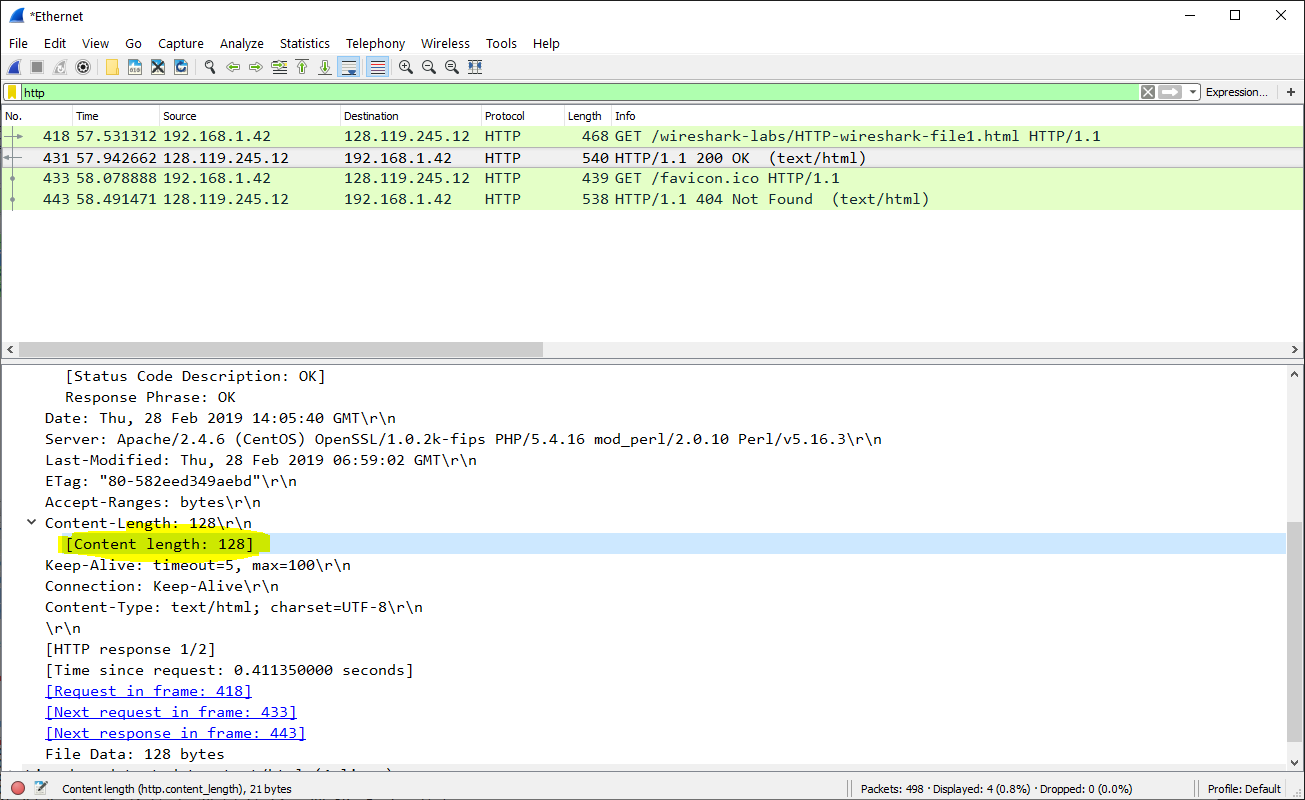
* Địa chỉ IP máy em là: 192.168.1.42
* Địa chỉ IP máy chủ server là: 128.119.245.12

1. 

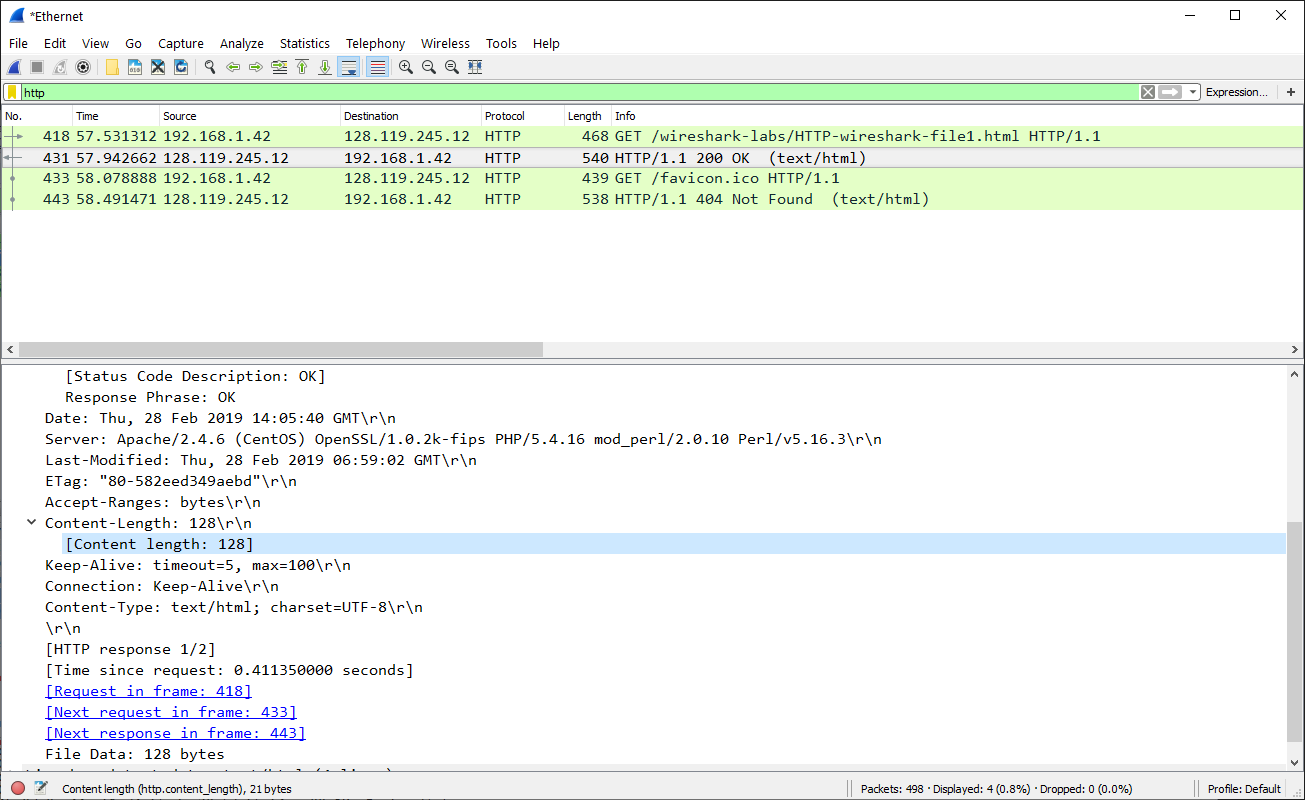
* Status code được máy chủ server gửi về là : 200

1. 

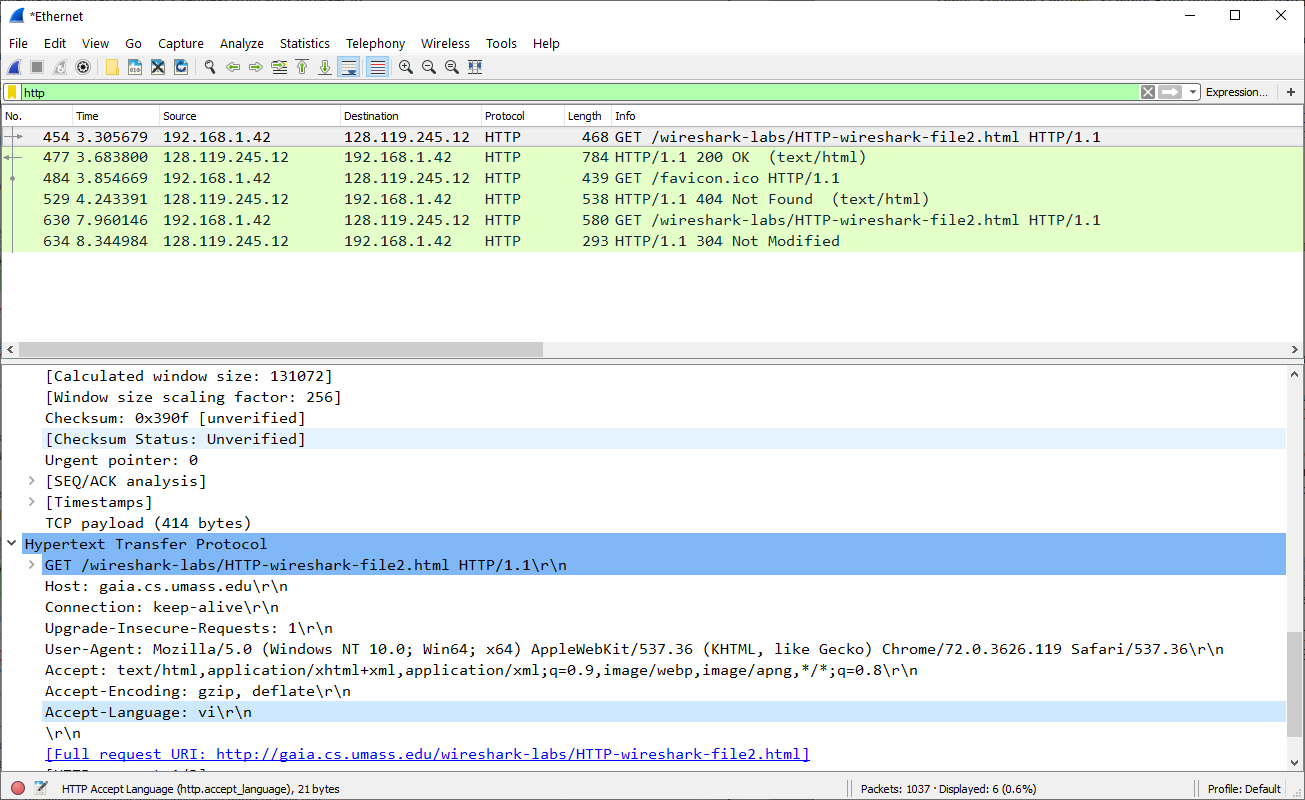
* Tệp tin HTML được sửa đổi lần cuối vào: Thu, 28 Feb 2019 06:59:02 GMT

1. 

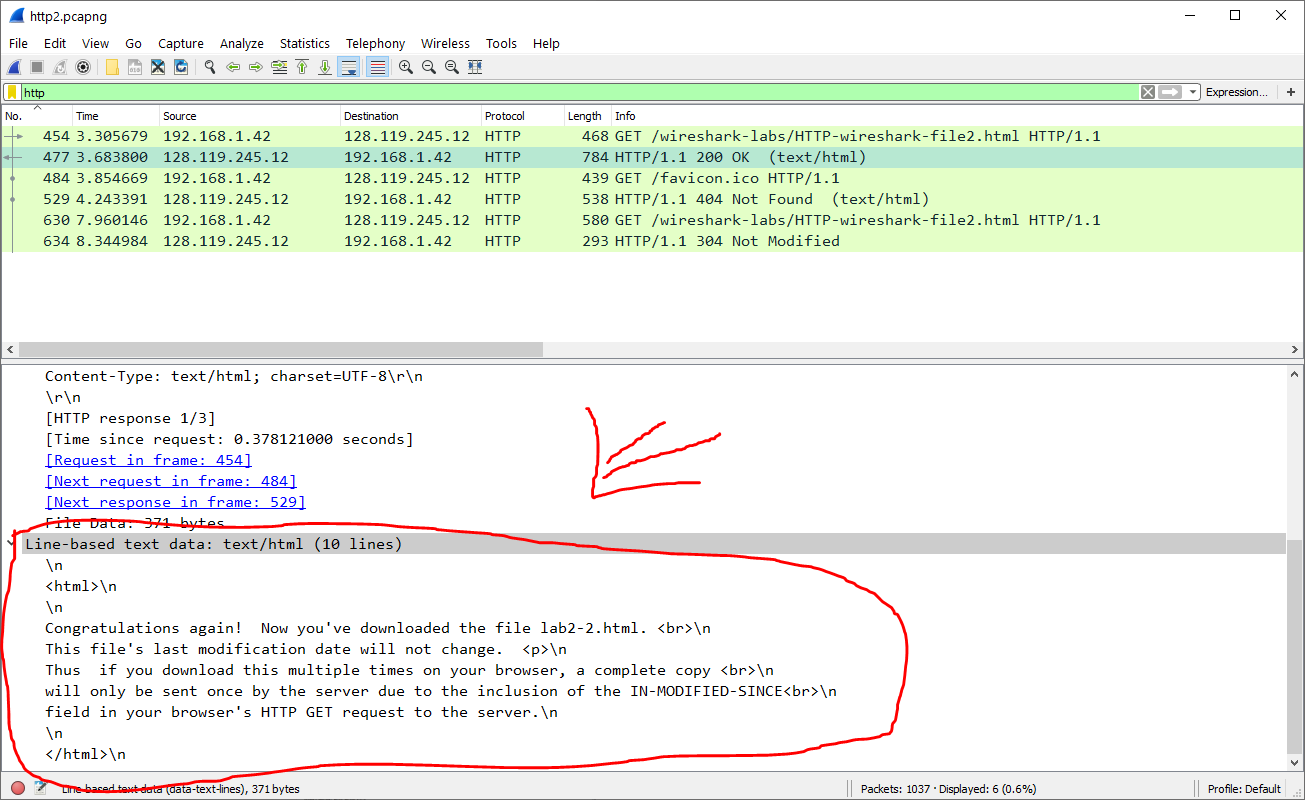
* Số bytes nội dung mà được trả về trình duyệt là: 128

1. 

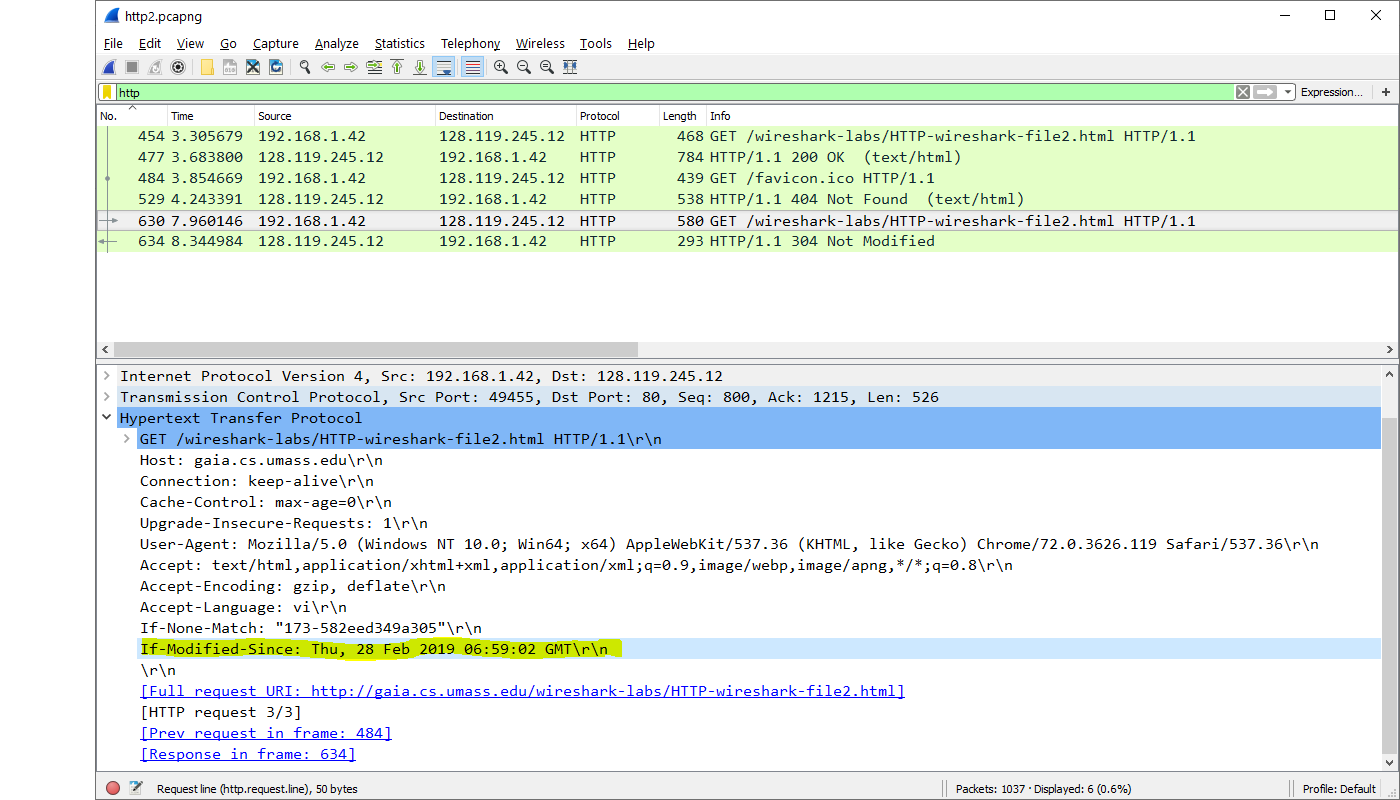
* Không có thấy phần headers .

1. The HTTP CONDITIONAL GET/response interaction
2. 

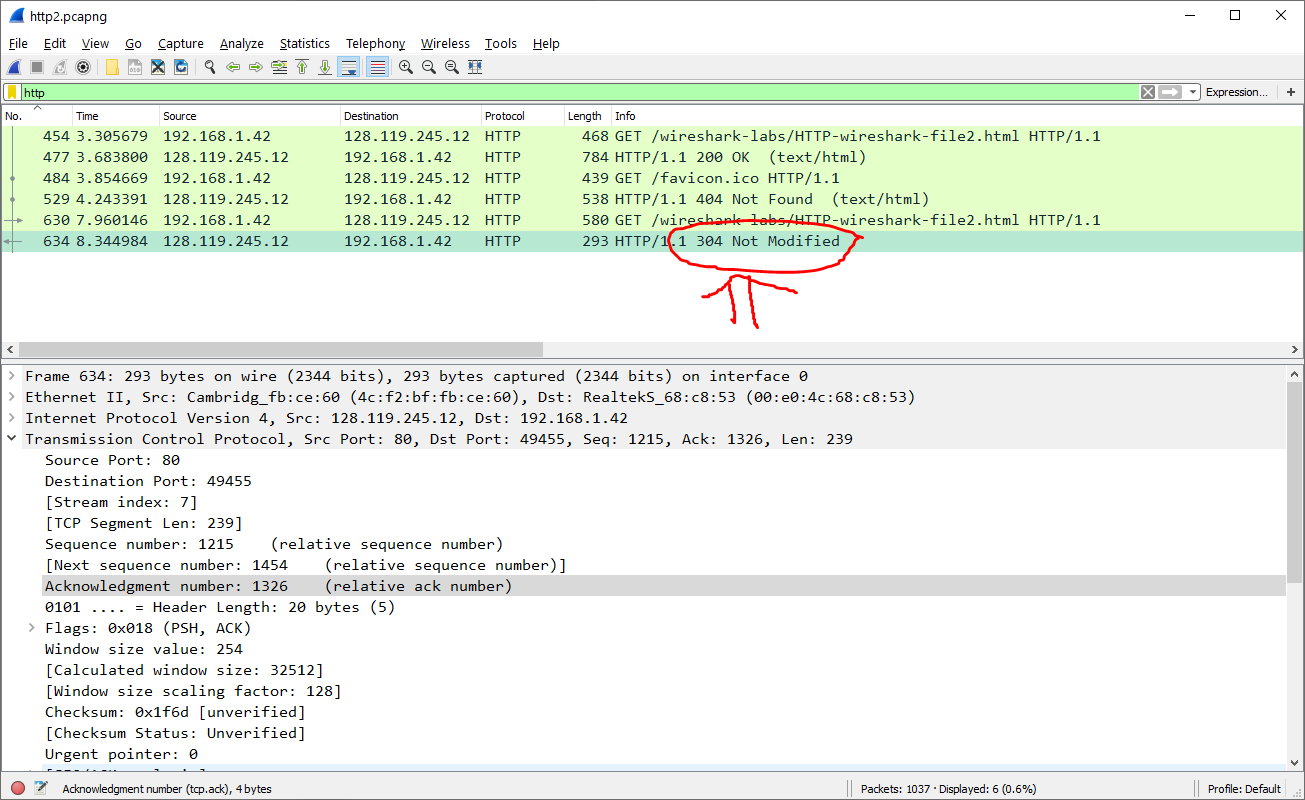
* Không thấy có dòng “IF-MODIFIED-SINCE” trong dòng HTTP GET

1. 

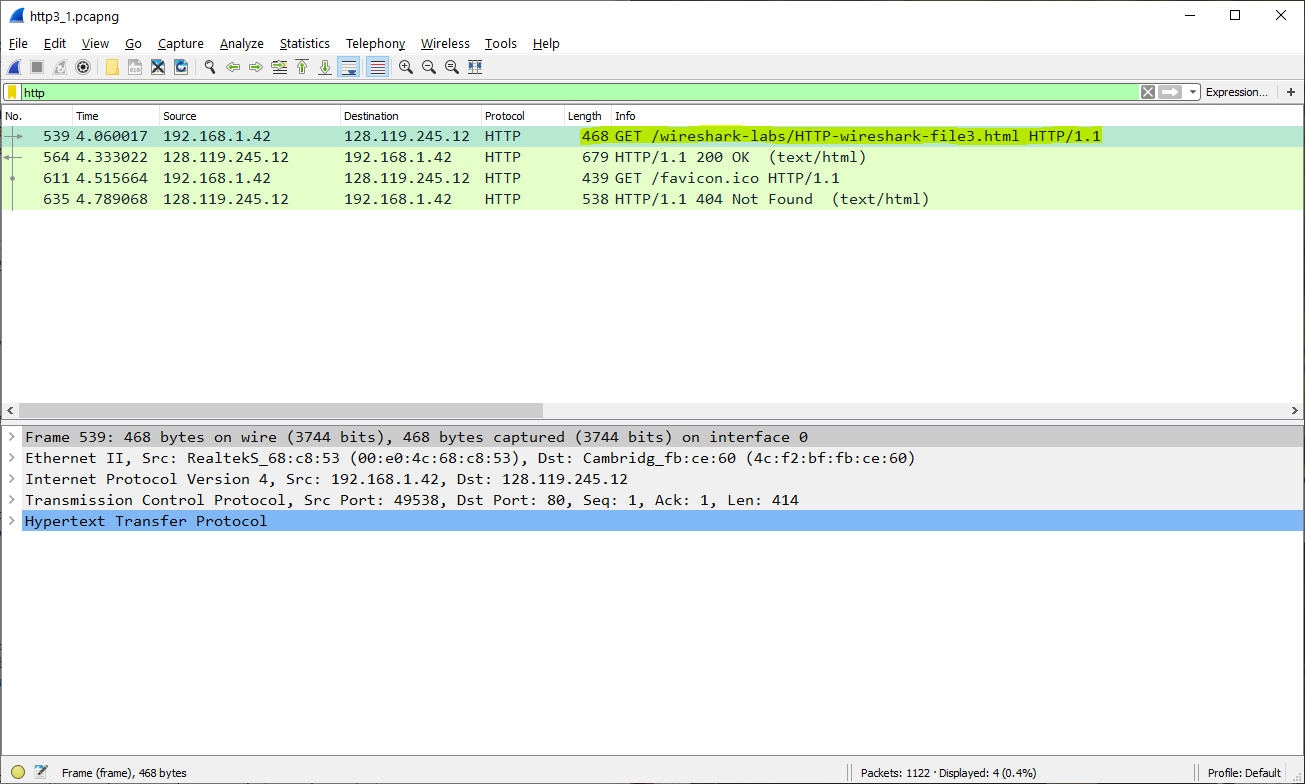
* Nội dung được máy chủ phản hồi đã bao gồm luôn cả nội dung hiển thị trên trang web, trong phần Line-based text data, nội dung được hiển trị trong wireshark là phần ngôn ngữ HTML với phần nội dung text là nội dung hiển thi trên web.

1. 

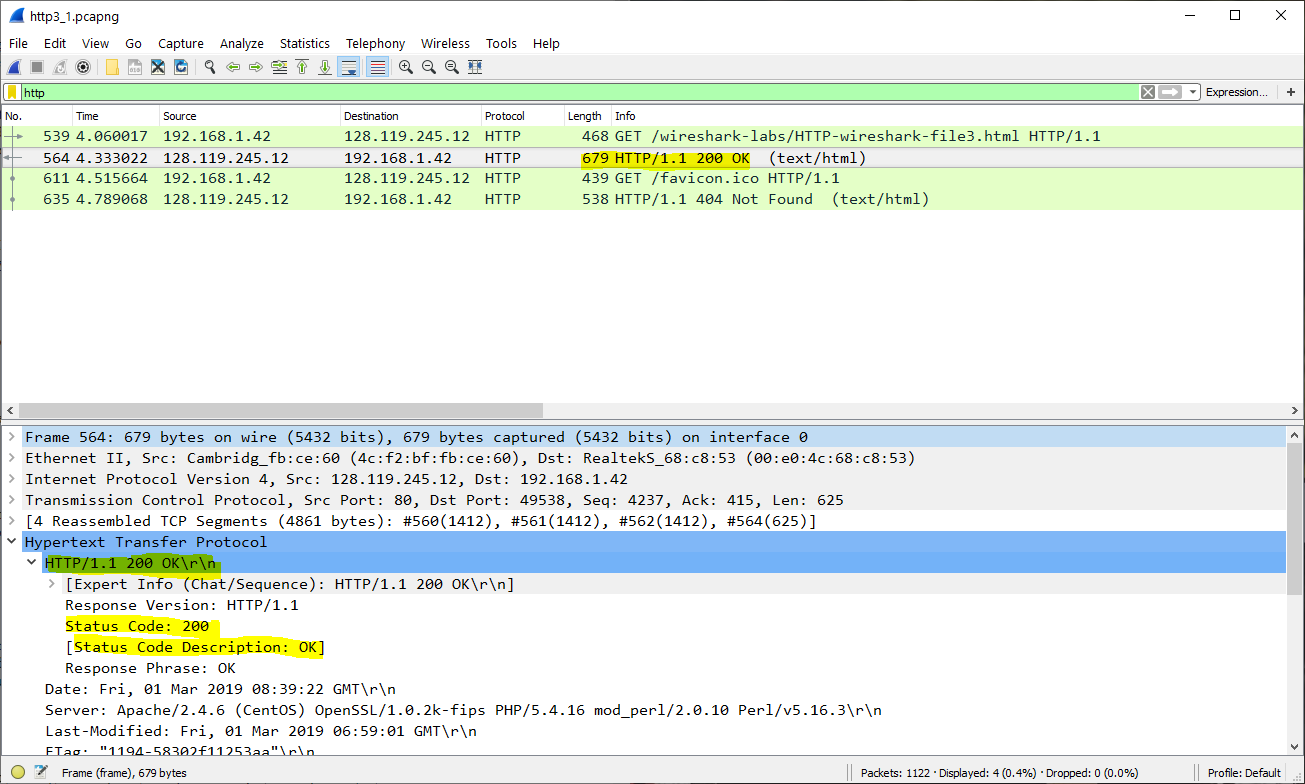
* Bây giờ thì đã có dòng IF-MODIFIED-SINCE. Nội dung hiển thị ở trong dòng này là thời gian mà truy cập vào trang web hay cũng như là thời gian mà tệp tin HTML được chỉnh sửa lần cuối là: Thu, 28 Feb 2019 06:59:02 GMT

1. 

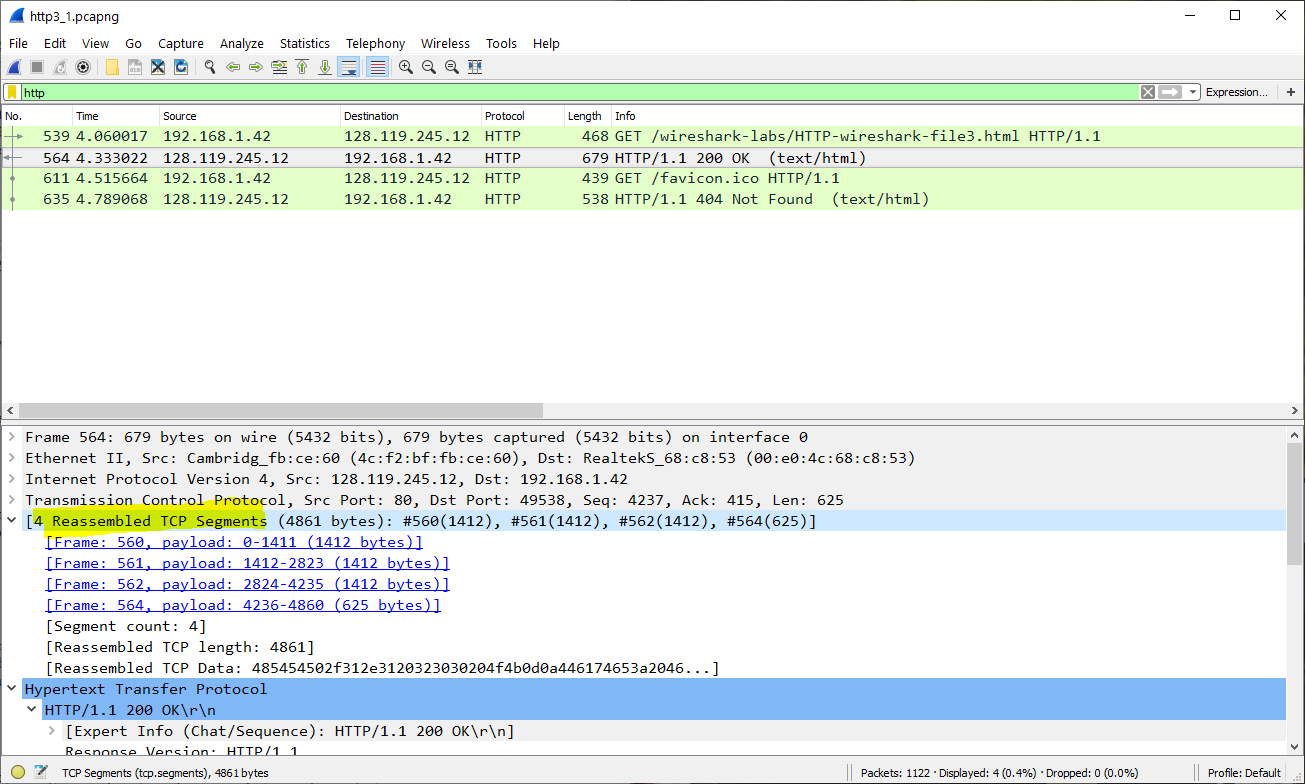
* Mã trạng thái(status code) mà máy chủ trả về là: 304 Not Modified
* Máy chủ không trả về nội dung của tệp vì trình duyệt chỉ cần truy xuất nội dung từ bộ đệm. Nếu tệp đã được sửa đổi kể từ lần truy cập cuối cùng, nó sẽ trả về nội dung của tệp, thay vào đó, nó chỉ đơn giản là bảo trình duyệt của tôi truy xuất tệp cũ từ bộ nhớ được lưu trong bộ nhớ cache.

1. Retrieving Long Documents
2. 

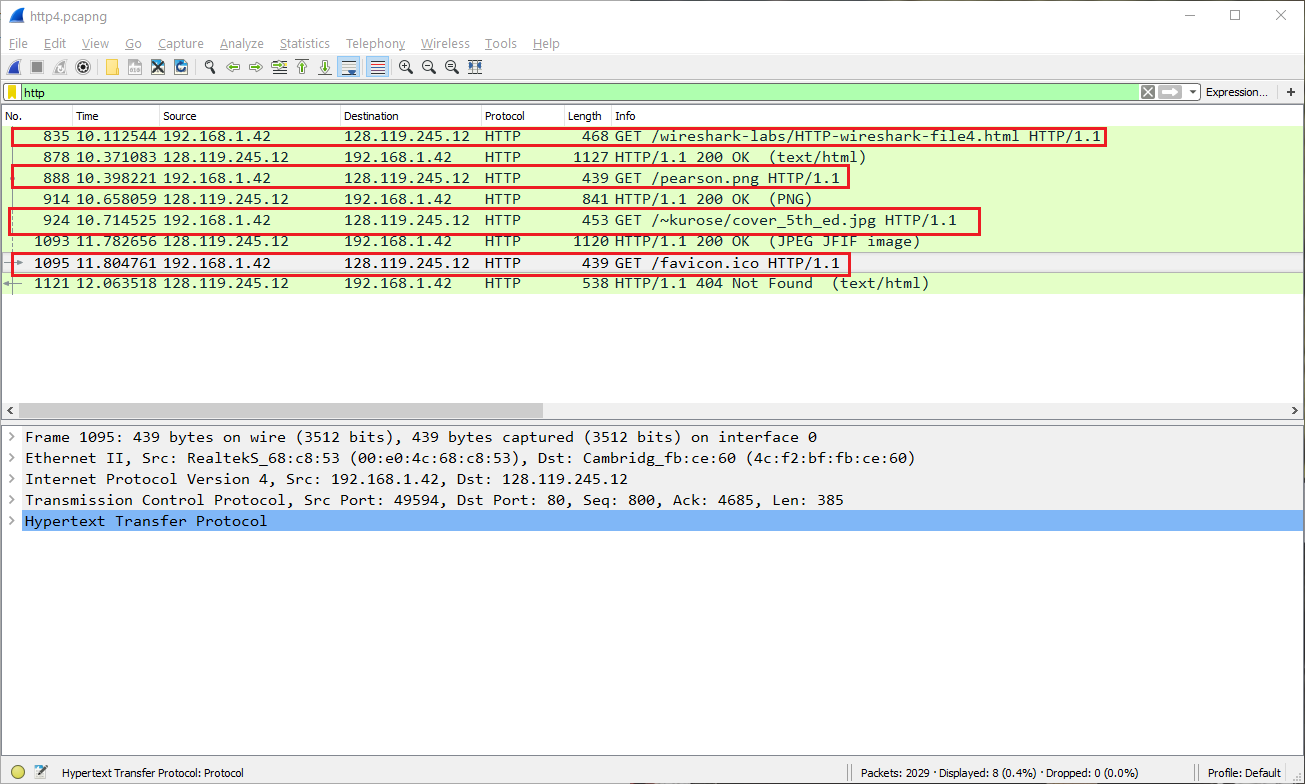
* Trình duyệt chỉ gửi một yêu cầu HTTP GET đến server. Gói tin đó đứa tin nhắn GET số hiệu 539

1. 

* Gói tin chứa phản hồi HTTP GET của server mang số hiệu là 764
* Mã trạng thái: 200 (OK)

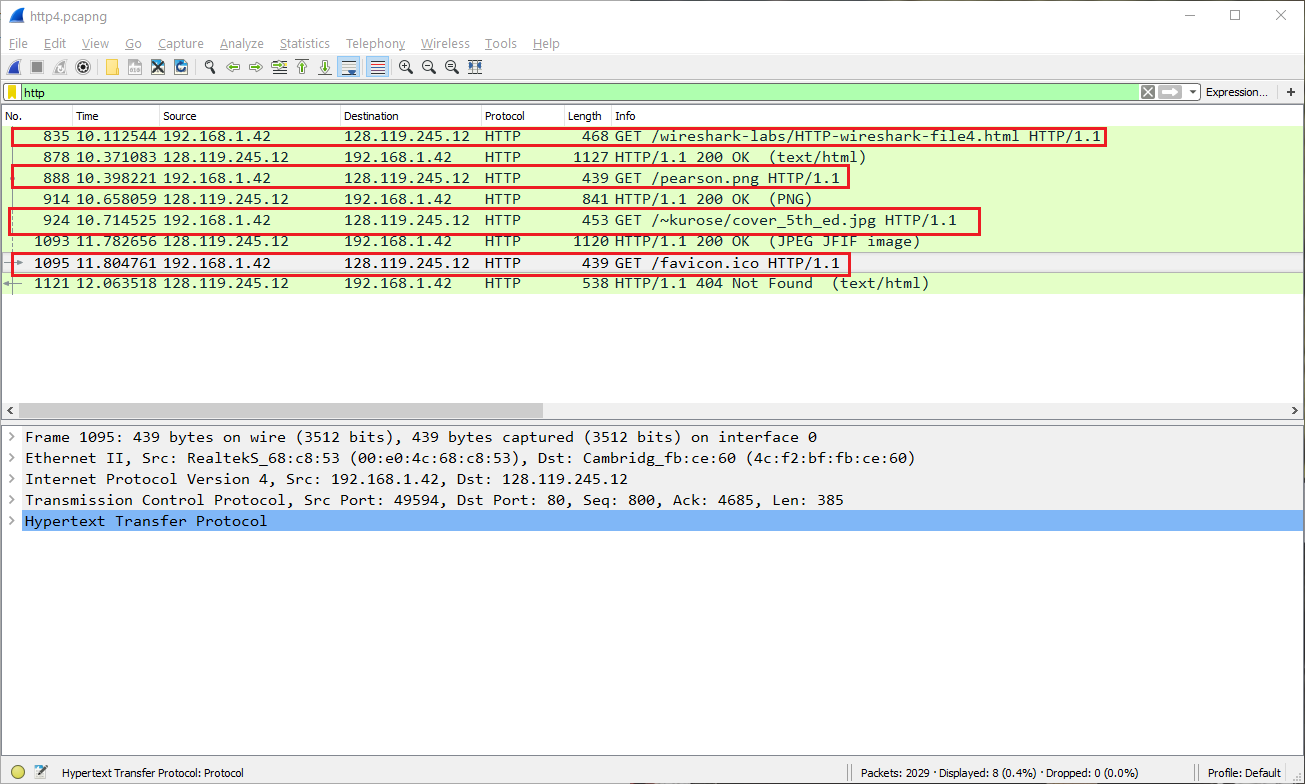
1. 

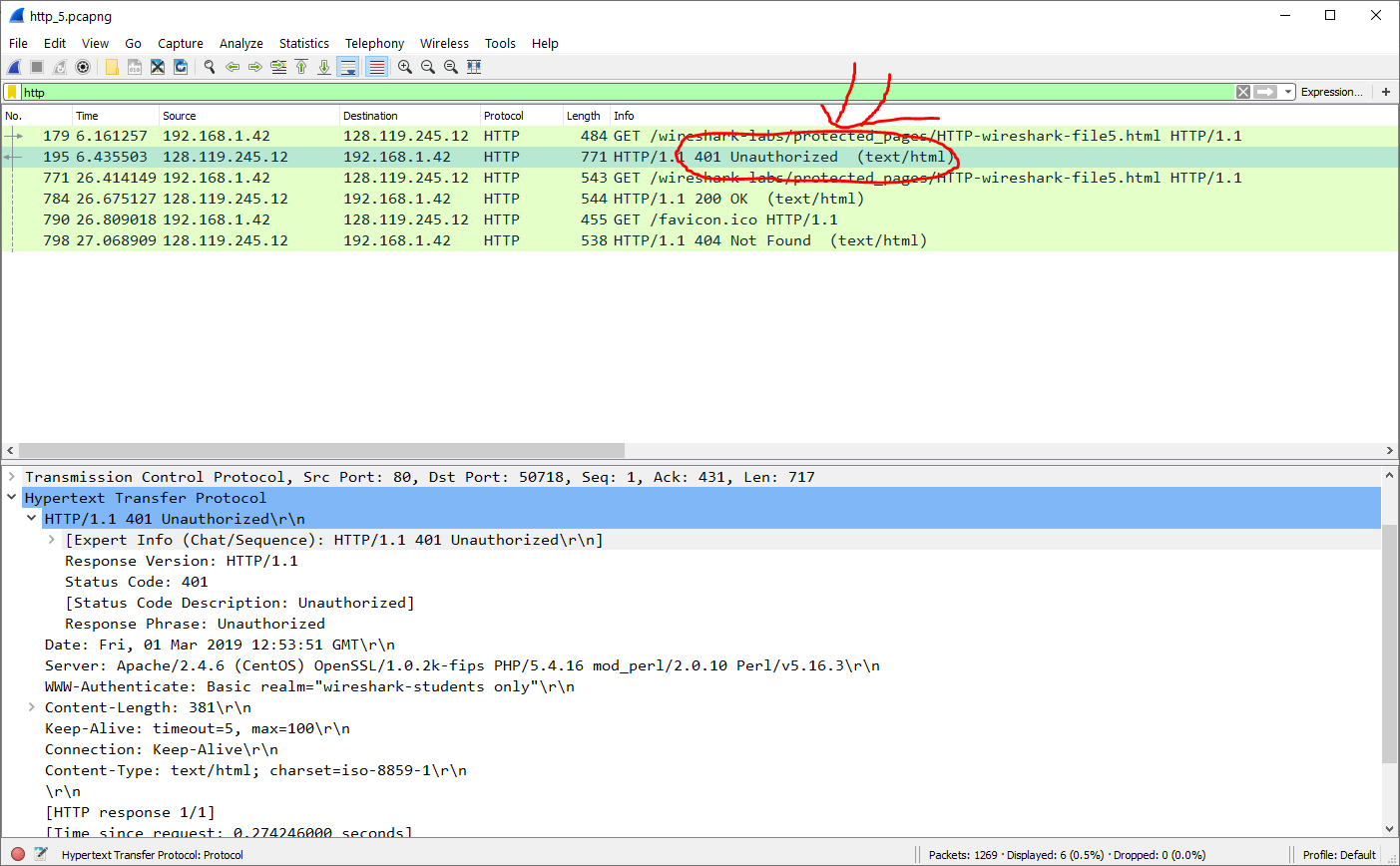
* Có tất cả 4 reassembled TCP segment

1. HTML Documents with Embedded Objects
2. 

* Có tất cả 4 tin nhắn yêu cầu GET.
  + Trang ban đầu
  + Logo Pearson
  + Hình ảnh cuốn sách Pearson 5th Edition
  + Logo của page hiển thị trên tab trình duyệt
* Địa chỉ IP của page: 128.119.245.12
* Địa chỉ logo Pearson: 128.119.245.12
* Địa chỉ hình cuốn sách Pearson 5th Edition: 128.119.245.12
* Địa chỉ logo page hiển thị trên tab trình duyệt: 128.119.245.12

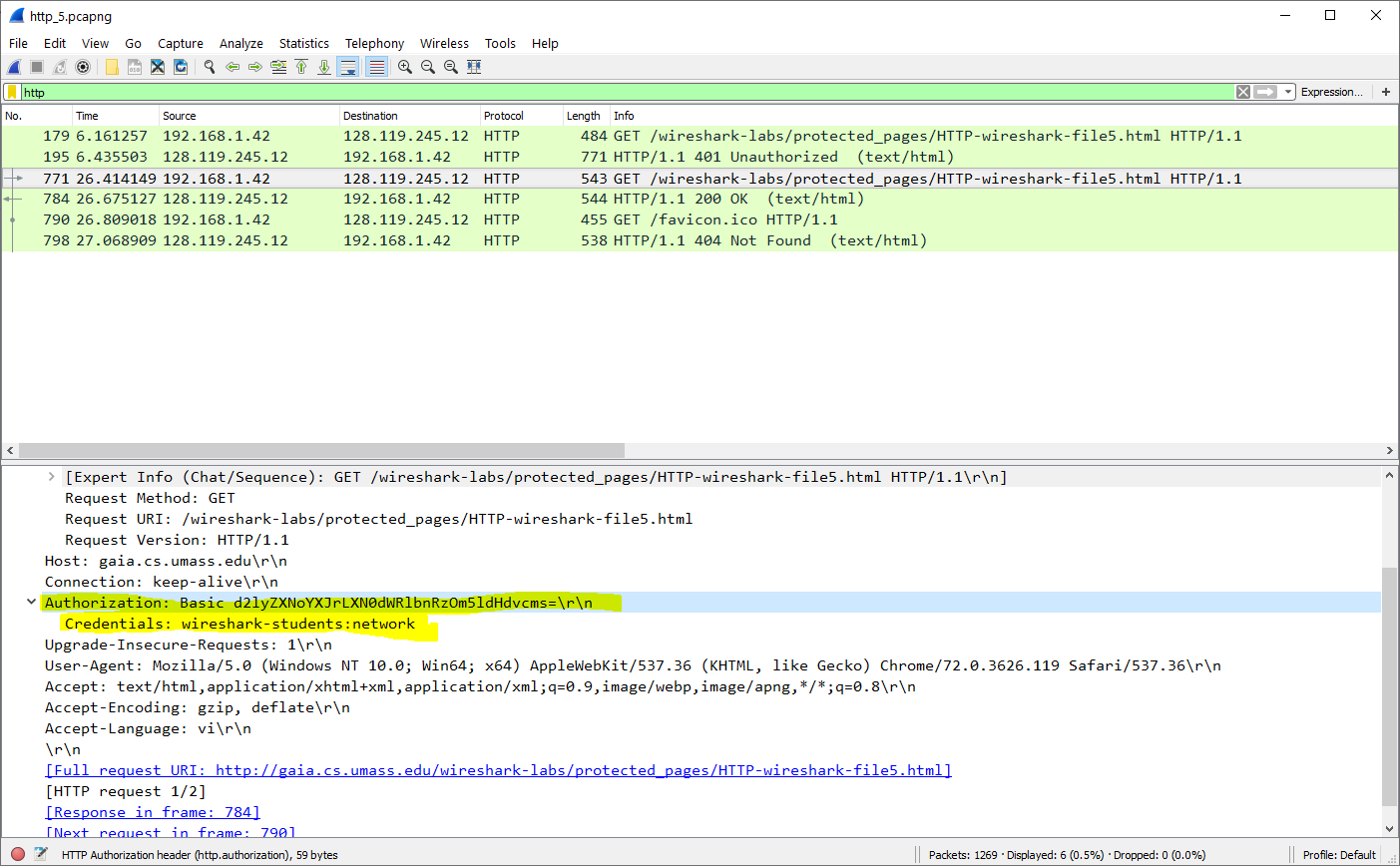
Trình duyệt sẽ tải những tấm ảnh về một cách tuần tự. Bởi vì khi page load, nội dung của page sẽ hiện từ trên xuống dưới. Cùng với đó, khi check lại tuần tự request/respond bằng wireshark thì tuần tự của nội dung page được máy chủ nhận yêu cầu và phản hồi rồi mới thực hiện tiếp tục các nội dung khác.



1. HTTP Authentication
2. 

* Sau khi gửi request đầu tiên thì server gửi về thông báo với mã code là :

401 Unauthorized(không được phép truy cập, phải đăng nhập)

1. 

* Một mục mới xuất hiện sau khi HTTP GET thứ 2 được gửi đi là mục Authorization. Nội dung này được kèm theo bởi vì chúng ta vừa thực hiện một việc đó là cung cấp cho server username và password để server kiểm tra và cấp cho chúng ta quyền truy cập vào page.
* Nội dung của mục này gồm username và password chúng ta cung cấp dưới dạng text utf-8 và 1 dòng được decode dưới dạng base-64
* Dạng base-64 là: d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=

