ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH

**TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN**

Ảnh có chứa văn bản, Phông chữ, biểu tượng, Đồ họa

Mô tả được tạo tự động

BÁO CÁO ĐỒ ÁN WIRESHARK

MÔN HỌC: MẠNG MÁY TÍNH

|  |  |  |
| --- | --- | --- |
| Lớp: | 23CTT1 |  |
| Thành viên: | 23120030 | Trần Thanh Đạt |
|  | 23120048 | Phan Hoàng Quốc Huy |
|  | 23120051 | Nguyễn Duy Khánh |

Đánh giá mức độ hoàn thành:

|  |  |  |  |
| --- | --- | --- | --- |
| **Bài** | **Câu** | **Ghi chú** | **Đánh giá** |
| 1 |  |  |  |
|  | 1 | Xác định được tên miền và cho biết địa chỉ IPs | 100% |
|  | 2 | Xác định được số lượng gói tin | 100% |
|  | 3 | Xác định được trang web có dùng gzip hay không, có ghi cookie hay không | 100% |
|  | 4 | Xác định được mục đích của gói 26, 27 và giải thích | 100% |
|  | 5 | Xác định được mục đích khi client hỏi địa chỉ IP của của domain us.i1.yimg.com | 100% |
|  | 6 | Xác định được mục đích khi hệ thống không cần một yêu cầu DNS khác trước câu lệnh get thứ hai | 100% |
|  | 7 | Xác định số lượng HTTP request client gửi đi  Xác định IP của client  Xác định loại HTTP connections  Vẽ hình được | 100% |
| 2 |  |  |  |
|  | 1 | Đã lọc thành công | 100% |
|  | 2 | Xác định giao thức gói tin DHCP sử dụng tại tầng Transport | 100% |
|  | 3 | Xác định địa chỉ tại tầng Link của host được cấp IP | 100% |
|  | 4 | Xác định thông tin IP nguồn, Port nguồn và IP đích, Port đích của 4 gói tin | 100% |
|  | 5 | Chỉ ra điểm khác biệt giữa các giá trị trong gói tin DHCP Discover và DHCP Request | 100% |
|  | 6 | Xác định giá trị Transaction-ID của 4 gói tin đợt cấp 1, giá trị Transaction-ID của 2 gói tin (Request/ACK) đợt cấp hai  Mục đích sử dụng của transaction-ID | 100% |
|  | 7 | Ý nghĩa trường thông tin lease-time, giá trị của trường này trong gói tin bắt được | 100% |
|  | 8 | Chỉ ra trường giá trị cho biết có thông tin DHCP relay agent hay không | 100% |
| 3 |  |  |  |
|  | 1 | Mối quan hệ giữa MSS và MTU | 100% |
|  | 2 | Cho biết MTU trên card mạng kết nối Internet của máy | 100% |
|  | 3 | Kích thước của các phần của gói ICMP tại tầng mạng cơ bản | 100% |
|  | 4 | Kích thước của các phần của gói ICMP tại tầng Data Link cơ bản | 100% |
|  | 5 | Xác định lượng data trong ICMP và TTL | 100% |
|  | 6 | Xác định lượng data trong ICMP | 100% |
|  | 7 | Xác định lượng data trong ICMP, sự khác biệt với câu 6 và giải thích | 100% |
|  | 8 | Xác định vấn đề và giải thích | 100% |
| Tổng kết |  | Hoàn thành đầy đủ nội dung đồ án yêu cầu |  |

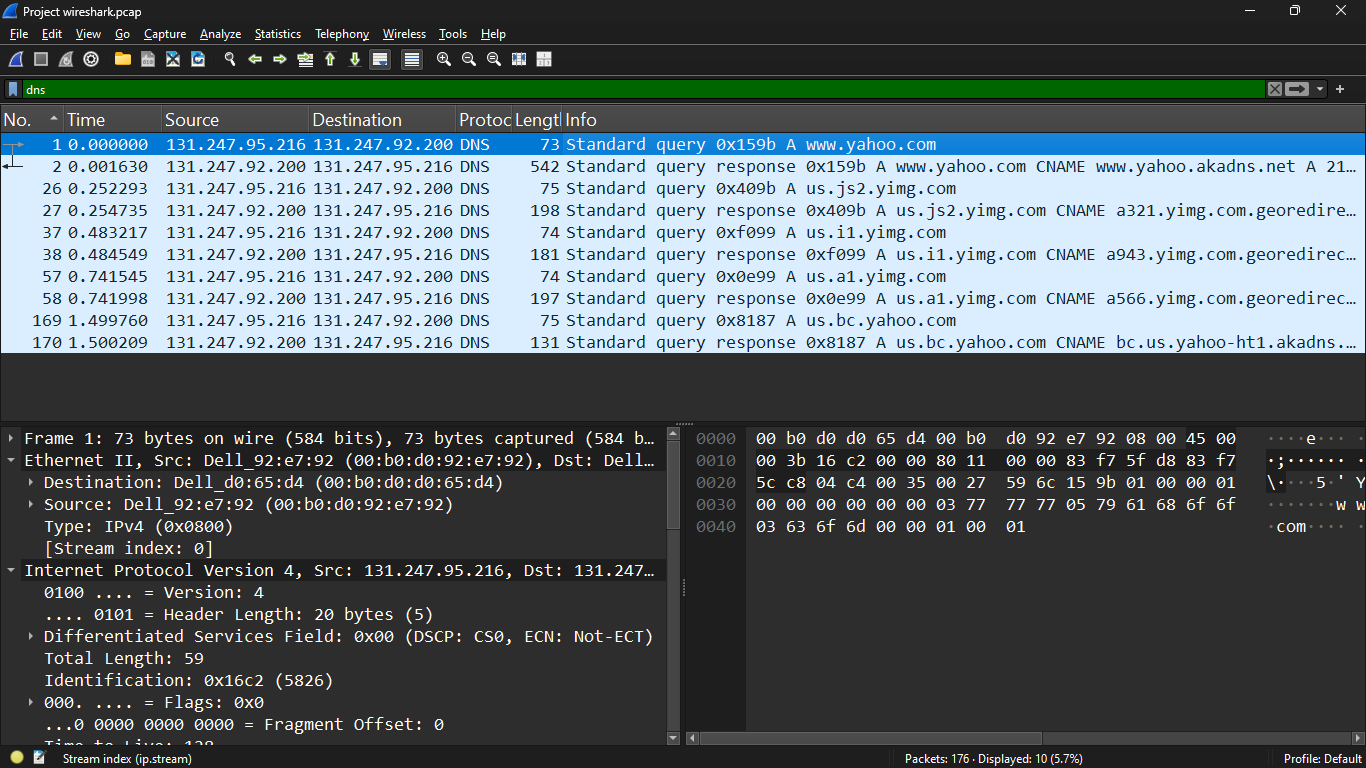
Bảng phân công công việc:

|  |  |  |
| --- | --- | --- |
| Thành viên | Nhiệm vụ | Đánh giá |
| Trần Thanh Đạt | Làm bài 2 | Hoàn thành tốt |
| Phan Hoàng Quốc Huy | Làm bài 3 và viết báo cáo | Hoàn thành tốt |
| Nguyễn Duy Khánh | Làm bài 1 | Hoàn thành tốt |

**Bài 01: HTTP**

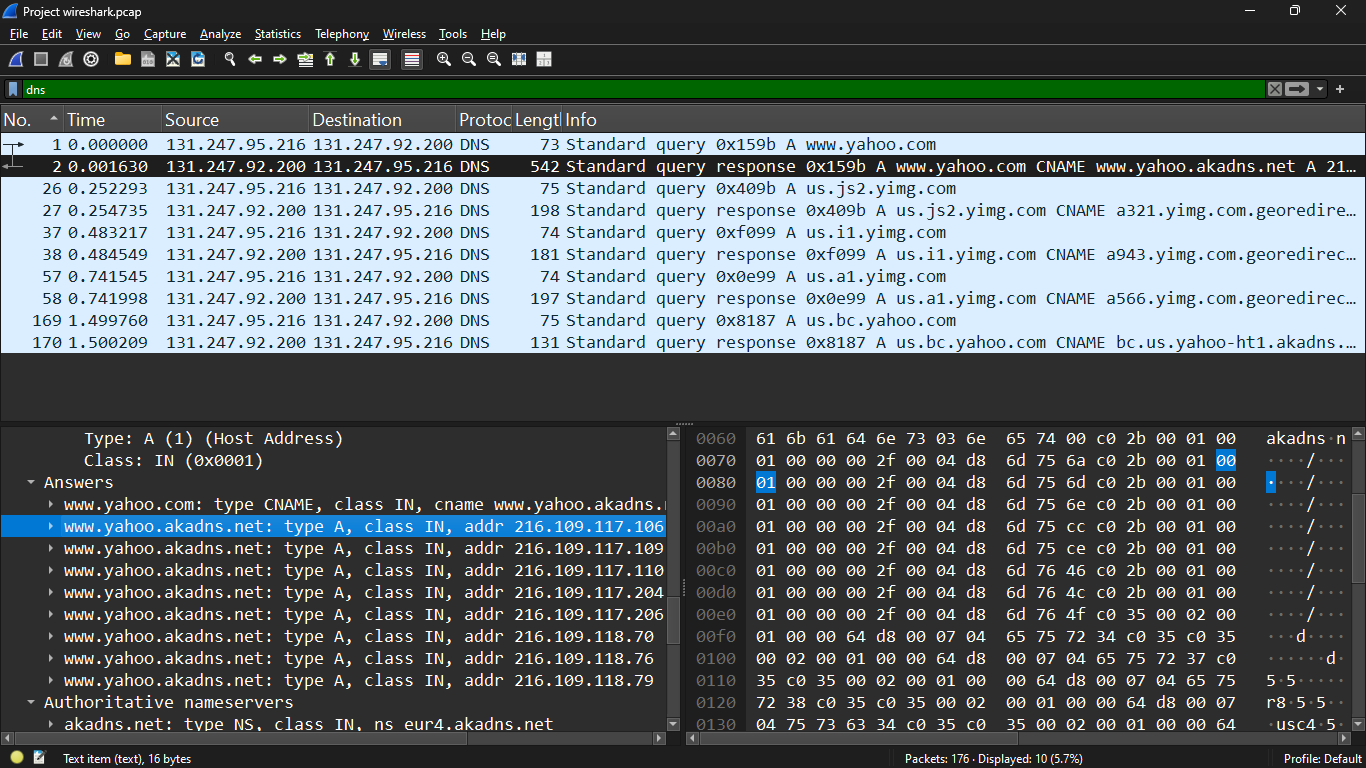
1. **Nhìn vào những gói đầu tiên, máy client đang truy vấn IP của một tên miền. Cho biết tên miền của website là gì? Cho biết hai địa chỉ IPs của website này?**

Tên miền của website: [www.yahoo.com](http://www.yahoo.com)

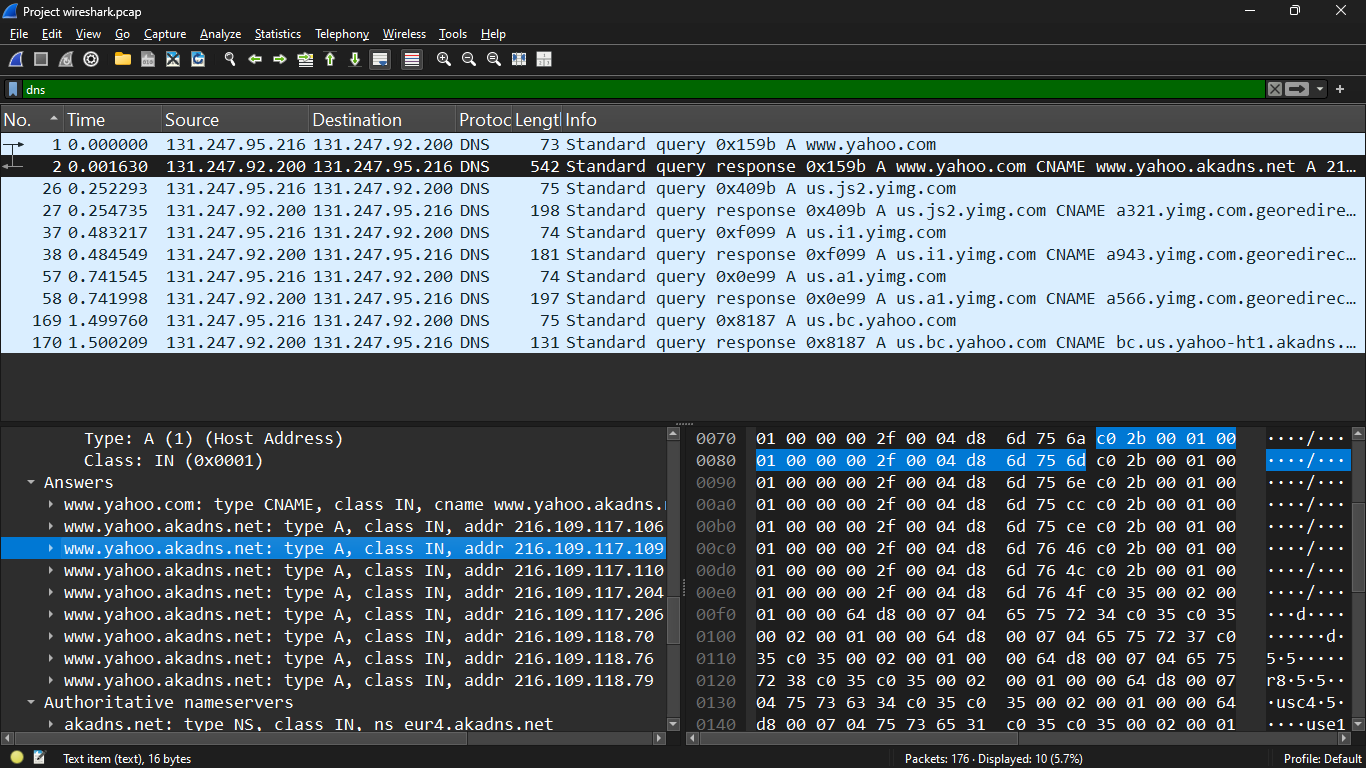


Hai địa chỉ IPs của website:

216.109.117.106



216.109.117.109



1. **Có bao nhiêu gói tin (packets) mà Server đã gửi cho máy client tính từ lúc bắt đầu đến khi nhận được trang web (chỉ tính kết quả của yêu cầu HTTP GET đầu tiên)?**

11 gói

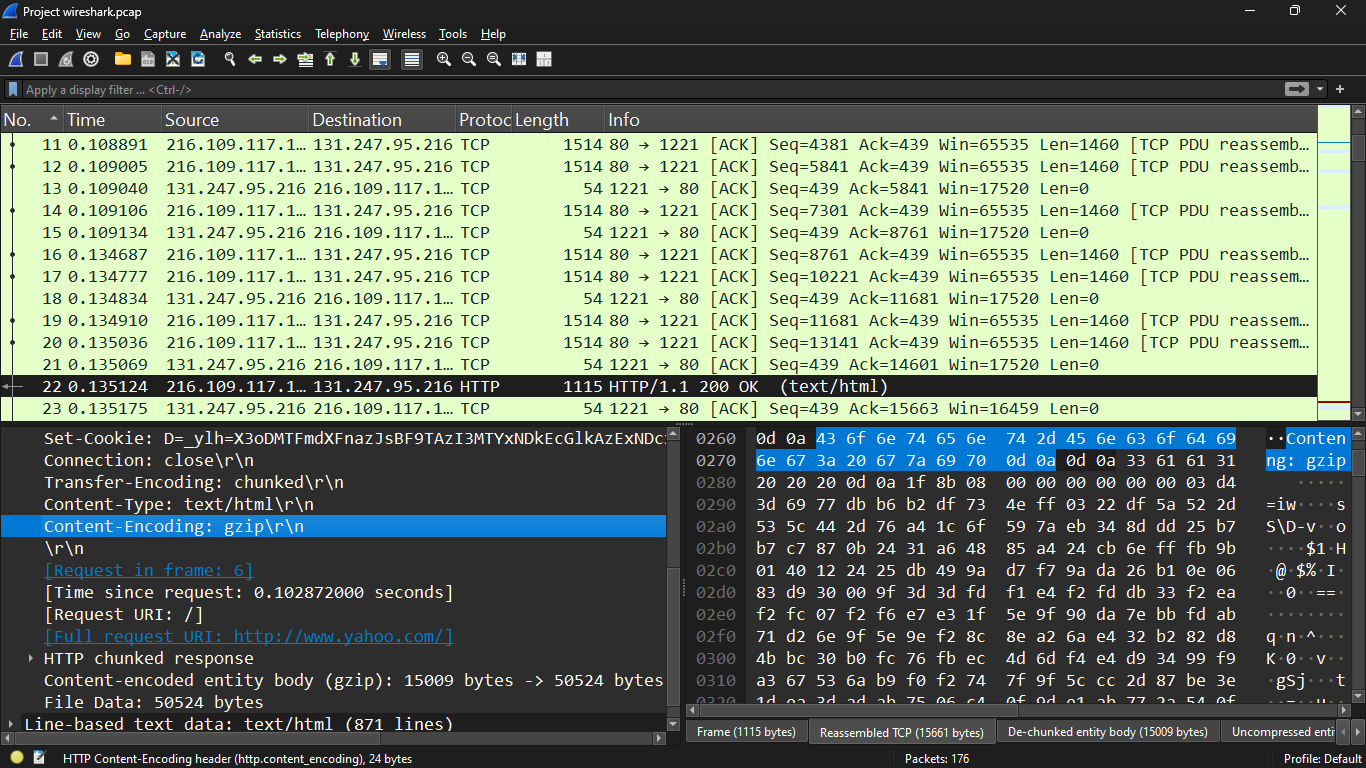
Là các gói có số 7, 8, 10, 11, 12, 14, 16, 17, 19, 20, 22

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

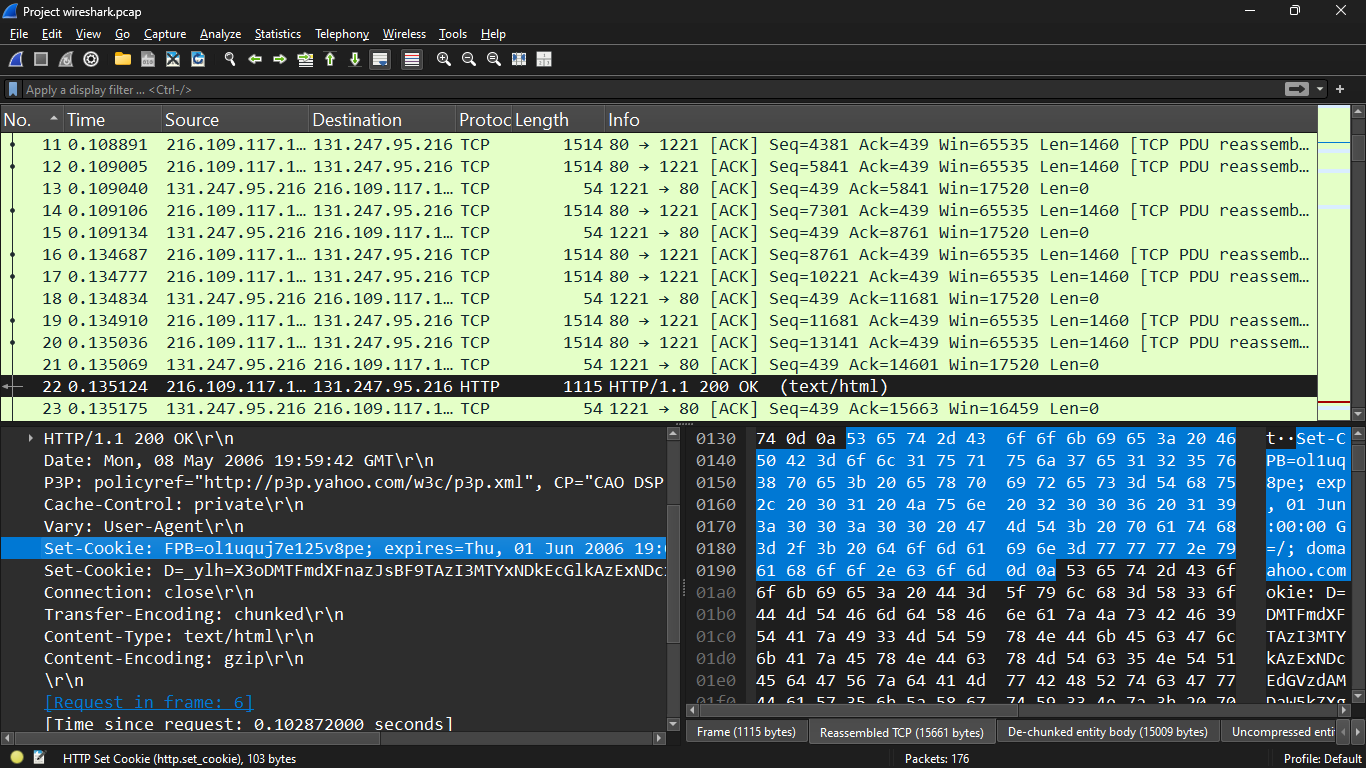
Mô tả được tạo tự động

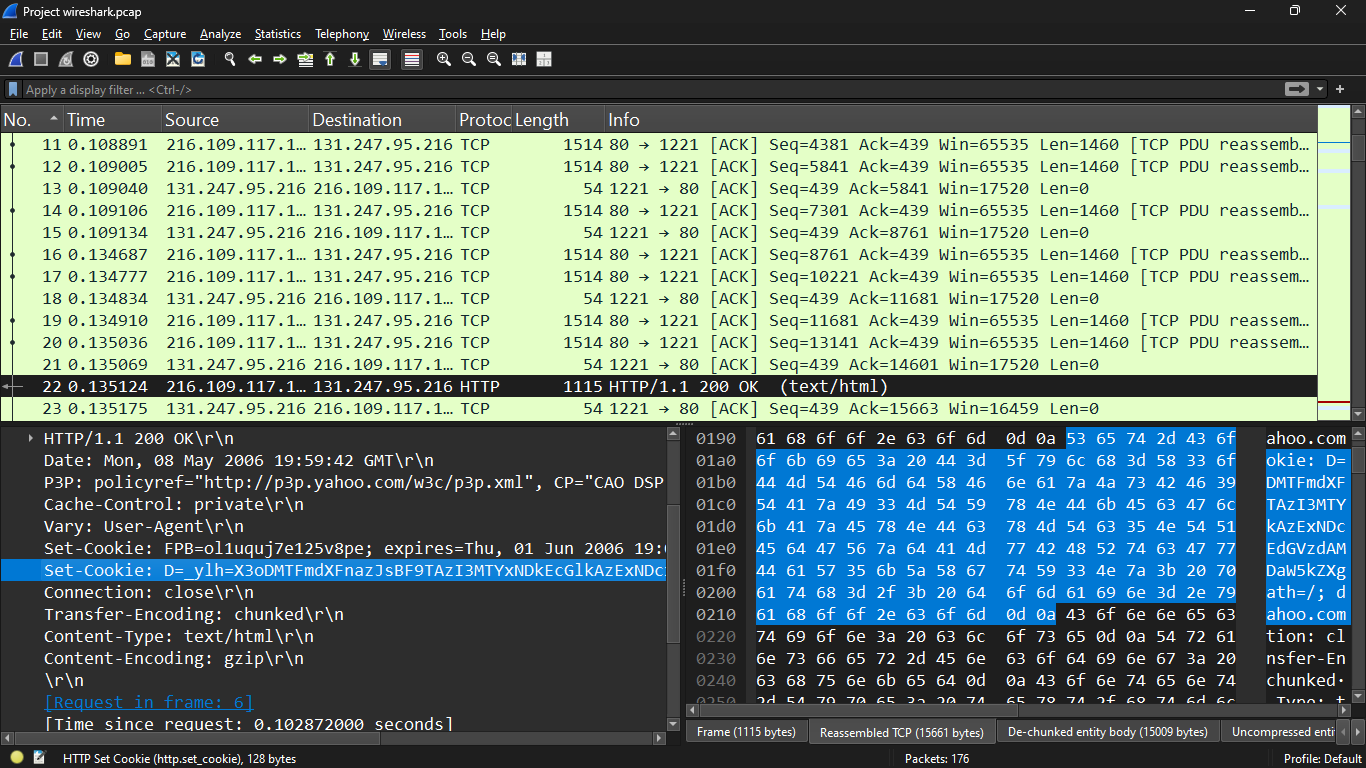
1. **Trang web này (server) có sử dụng gzip để nén dữ liệu khi gửi đi không? Nó có ghi cookie không? Để trả lời câu hỏi này, bạn cần xem phần header của gói dữ liệu được tái tạo lại. Nó là gói cuối cùng từ câu hỏi số 2 ở trên. Kiểm tra xem nó có “Content-Encoding” được đặt là gzip không, còn có ghi cookie không, thì các bạn tự tìm hiểu.**

Có sử dụng gzip để nén dữ liệu khi gửi đi



Có ghi 2 cookies





1. **Gói tin số 26 và 27 đang muốn làm gì? Theo bạn, tại sao lại phát sinh gói 26 và 27?**

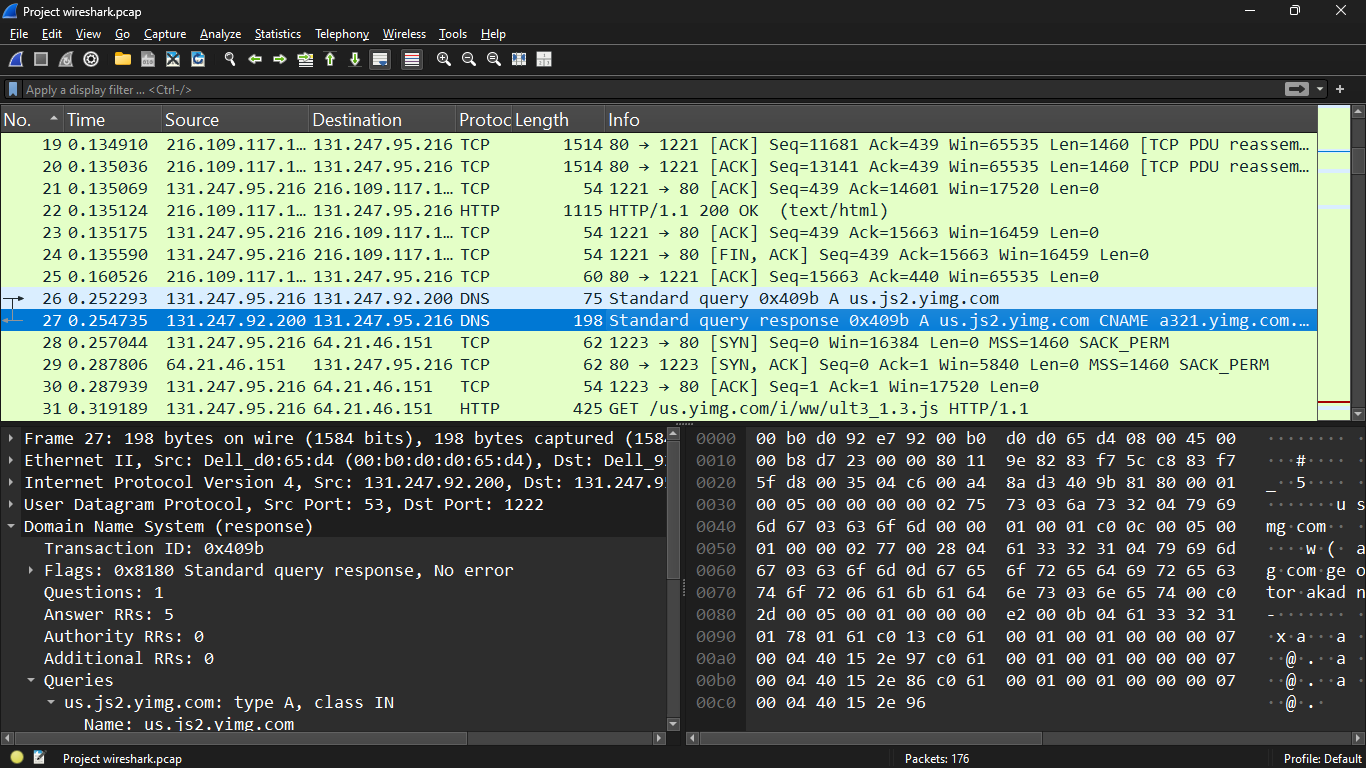
- Gói 26 là yêu cầu của client để tìm địa chỉ IP của us.js2.yimg.com, do trang web hoặc ứng dụng cần tải tài nguyên từ máy chủ này.  
- Gói 27 là phản hồi từ máy chủ DNS, trả về bản ghi CNAME trỏ đến a321.x.a.yimg.com và các IP thực tế của us.js2.yimg.com: 64.21.46.151, 64.21.46.134, và 64.21.46.150.  
- Nguyên nhân: Trang web chứa tài nguyên từ us.js2.yimg.com (hình ảnh, quảng cáo…), nên client phải truy vấn DNS để lấy địa chỉ IP sau khi tải trang chính.

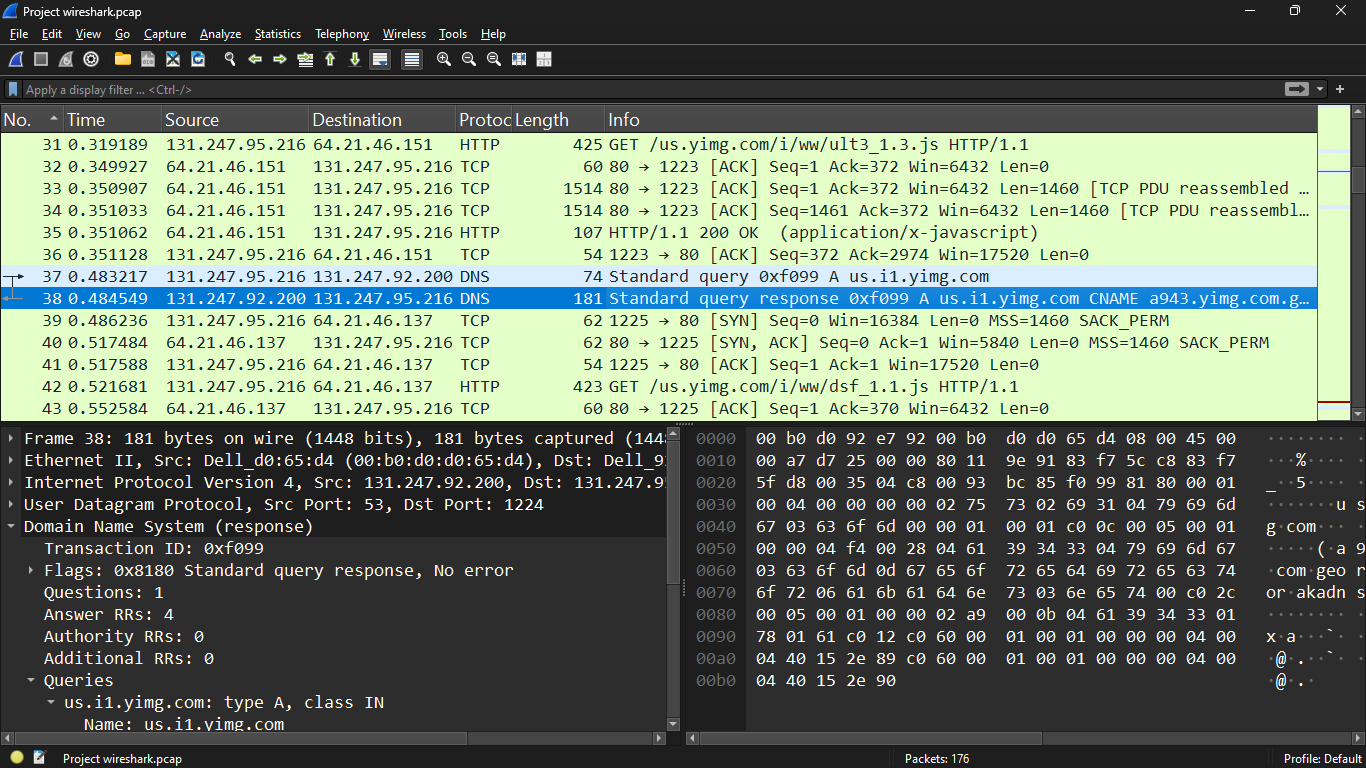
1. **Tại sao gói tin thứ 37 là một gói tin DNS query khác, cho domain là us.i1.yimg.com. Tại sao client lại cần hỏi địa chỉ IP cho domain này? Trong khi gói tin số 26 đã làm việc này rồi phải không?**

- Trang web client truy cập sử dụng tài nguyên từ nhiều domain. Sau khi tải xong tài nguyên từ us.js2.yimg.com (gói 26 và 27), client tiếp tục yêu cầu tài nguyên từ us.i1.yimg.com (hình ảnh, script, hoặc nội dung khác).

- Các domain như us.js2.yimg.com và us.i1.yimg.com thuộc các máy chủ khác nhau, được Yahoo dùng để phân phối tải. Vì vậy, client cần truy vấn DNS cho từng domain để tải đủ nội dung.

- Nếu domain có bản ghi CNAME (như gói 27 và 38), client phải truy vấn DNS tiếp theo để lấy IP của domain đích mà CNAME chỉ đến.



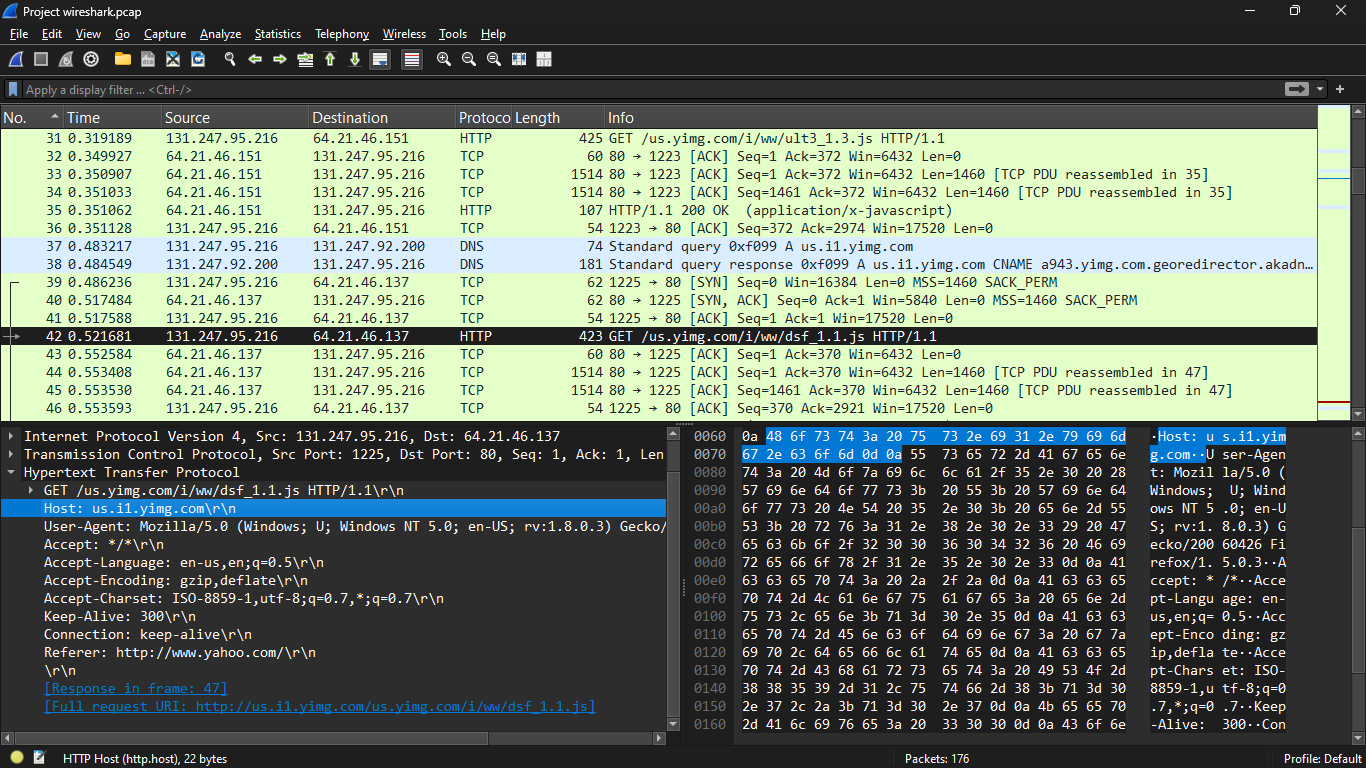


1. **Tại gói 42, bạn sẽ thấy một câu lệnh HTTP “Get”, và trong gói 48 là một câu lệnh HTTP “Get” mới. Tại sao hệ thống không cần một yêu cầu DNS khác trước câu lệnh get thứ hai? (Nhấp vào gói 42 và nhìn vào cửa sổ giữa. Mở rộng dòng có tiêu đề “Hypertext Transfer Protocol” và đọc dòng “Host:”. So sánh dòng đó với dòng “Host:” của gói 48)**

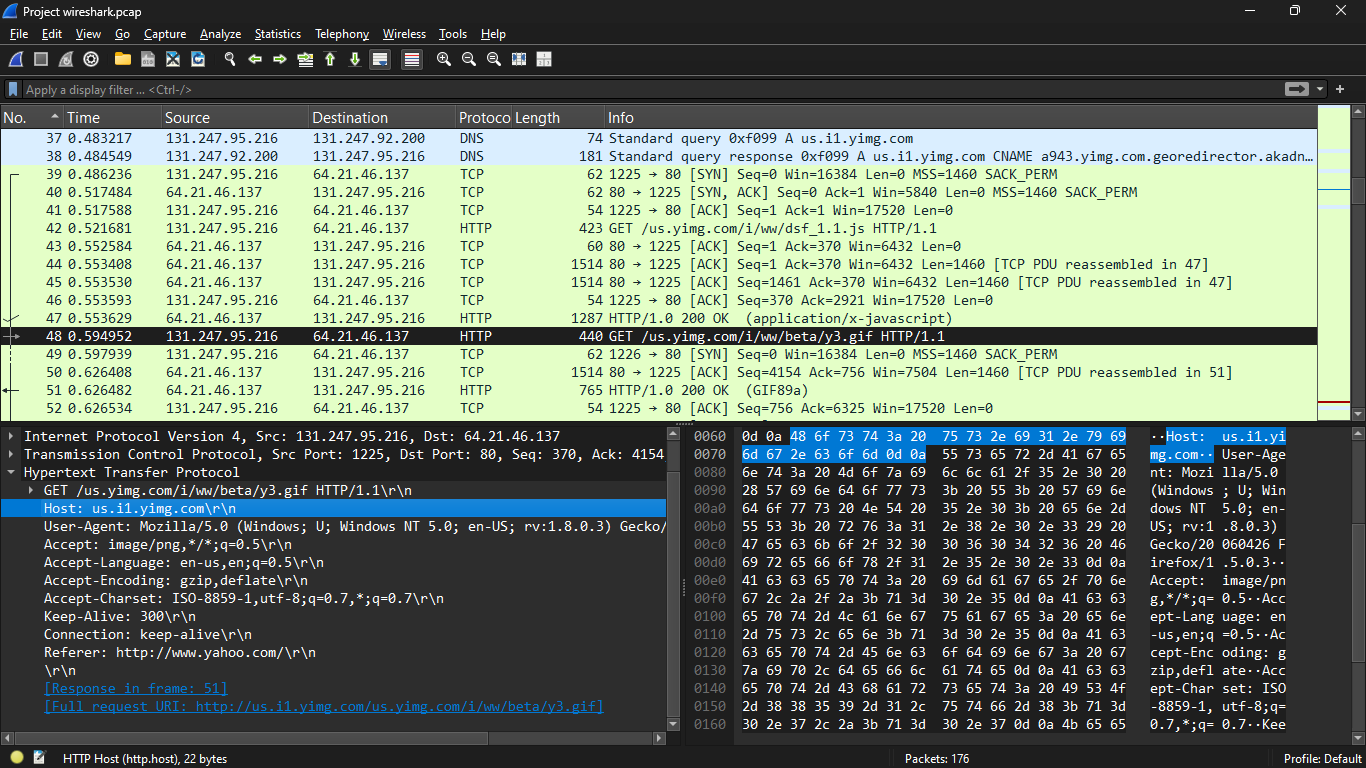
- DNS Cache: Sau khi client thực hiện một yêu cầu DNS cho us.i1.yimg.com(gói tin số 37 và 38), kết quả DNS được lưu trong cache. Khi client gửi các yêu cầu HTTP sau này đến us.i1.yimg.com, nó sẽ sử dụng địa chỉ IP đã lưu mà không cần truy vấn DNS lại.

- HTTP Requests và Domain: Gói tin số 42 và 48 đều yêu cầu tài nguyên từ us.i1.yimg.com.Vì thông tin DNS đã được client lưu trữ, nó có thể trực tiếp gửi yêu cầu HTTP đến IP đã biết mà không cần truy vấn DNS lại.

- Tóm lại: Hệ thống không cần truy vấn DNS mới cho gói tin số 48 vì thông tin DNS đã được lưu trong cache sau lần truy vấn DNS trước đó (gói tin số 37 và 38). Do đó, client có thể gửi các yêu cầu HTTP mà không cần truy vấn DNS lại cho cùng một domain.



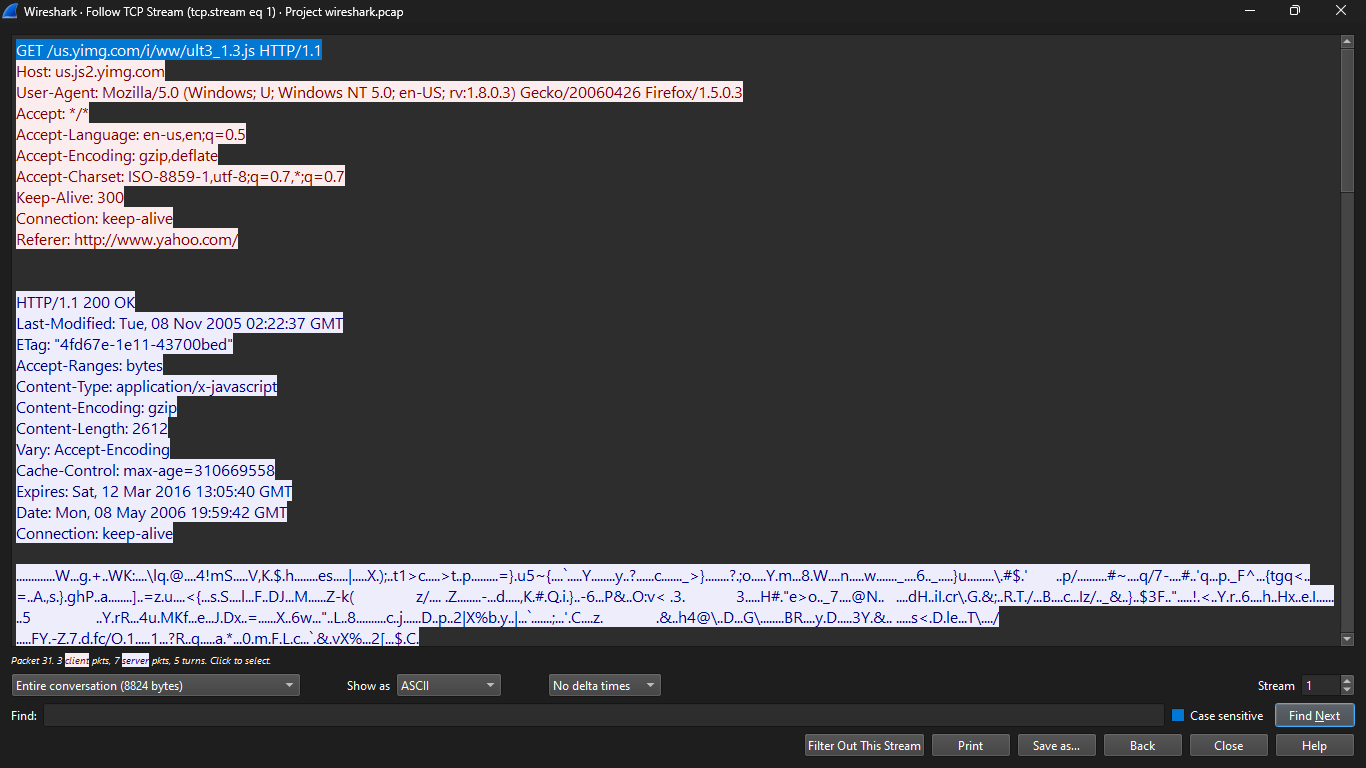
Host của gói 42 là us.i1.yimg.com



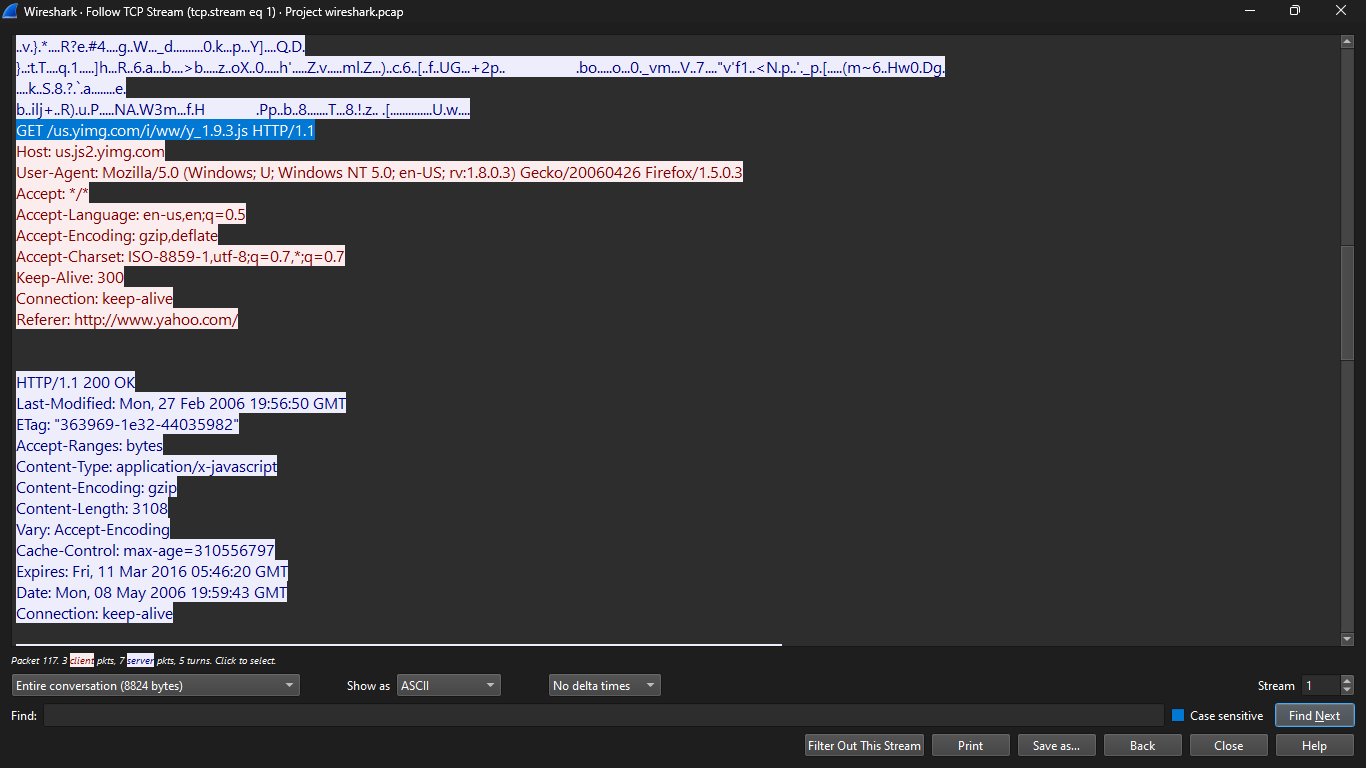
Host của gói 48 là us.i1.yimg.com

1. **Nhấp chuột phải lên gói tin thứ 31 => Follow => TCP Stream.**
2. **Cho biết có bao nhiêu HTTP request từ client gửi đi?**

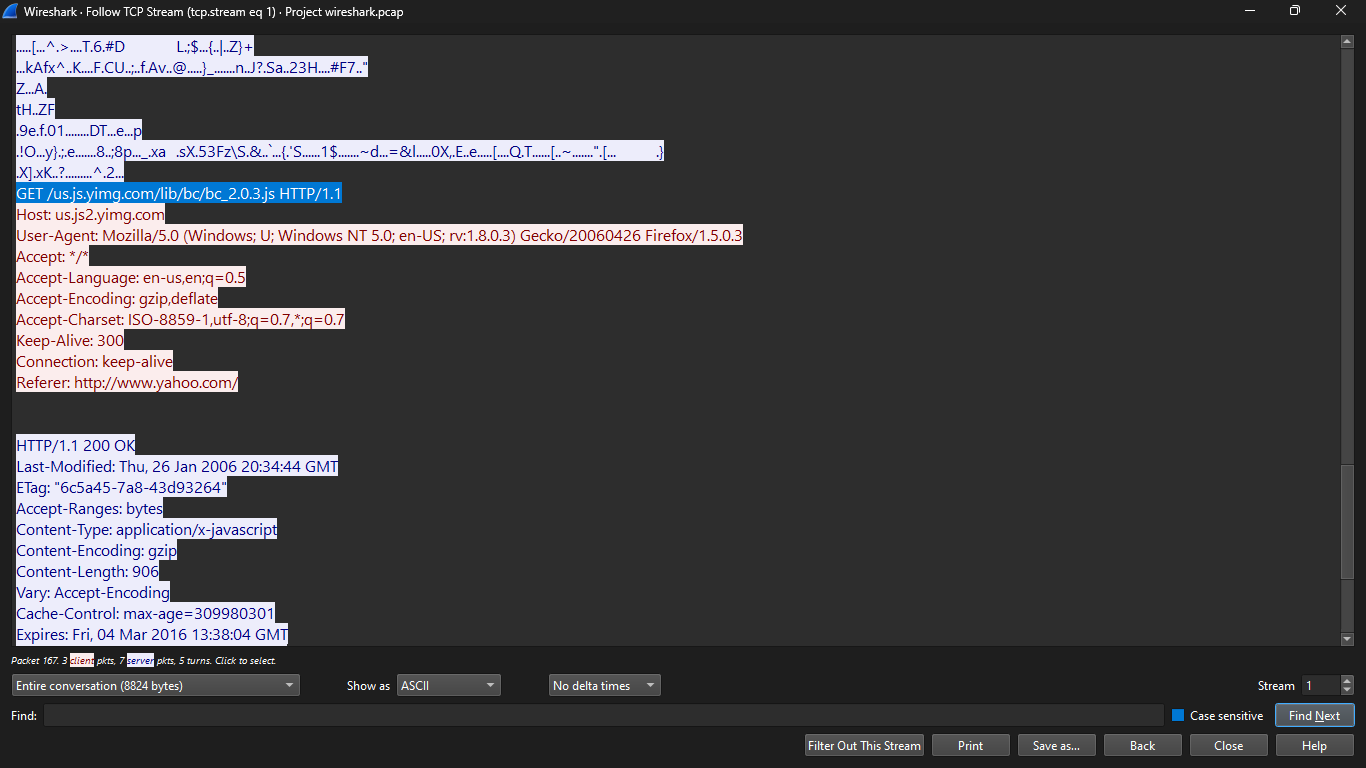
Có 3 HTTP request từ client gửi đi  
Request 1:



Request 2:

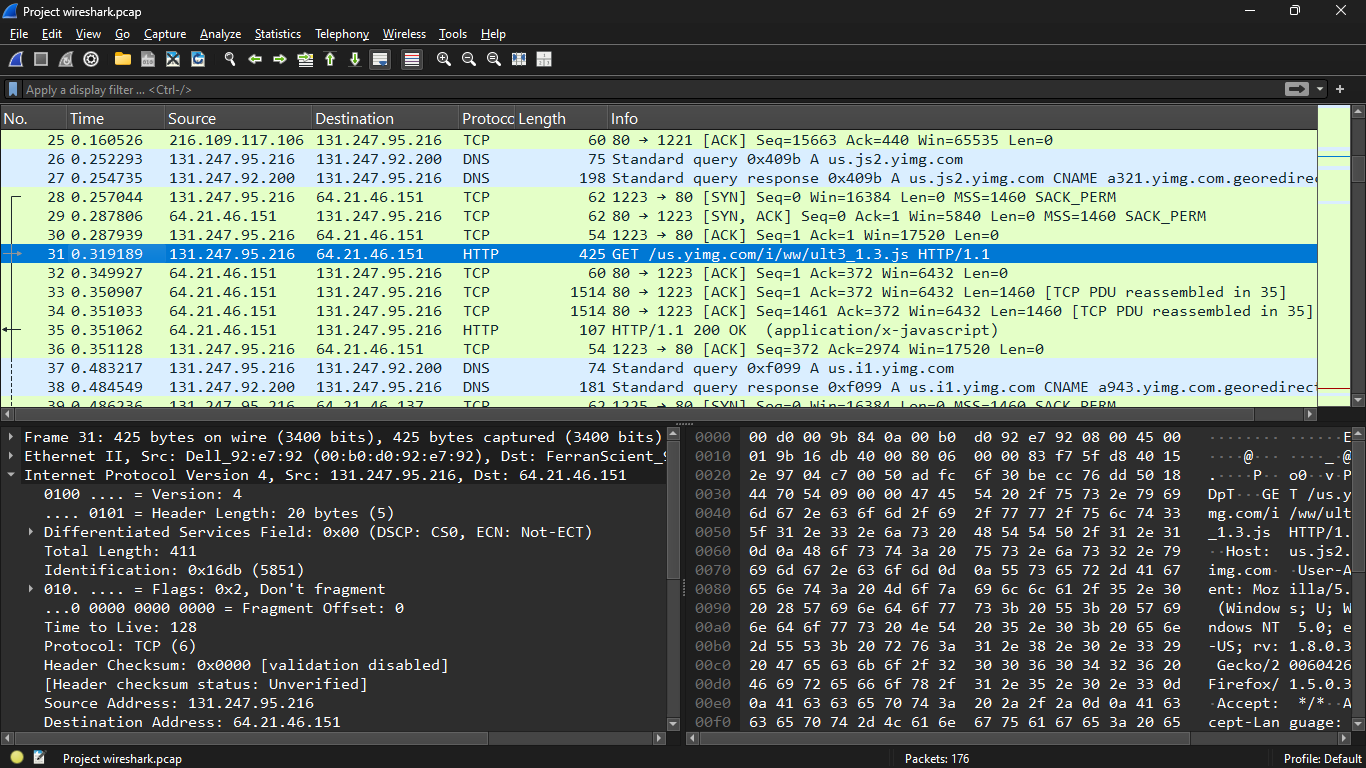


Request 3:



1. **Cho biết IP của máy client?**

IP của máy client là: 131.247.95.216



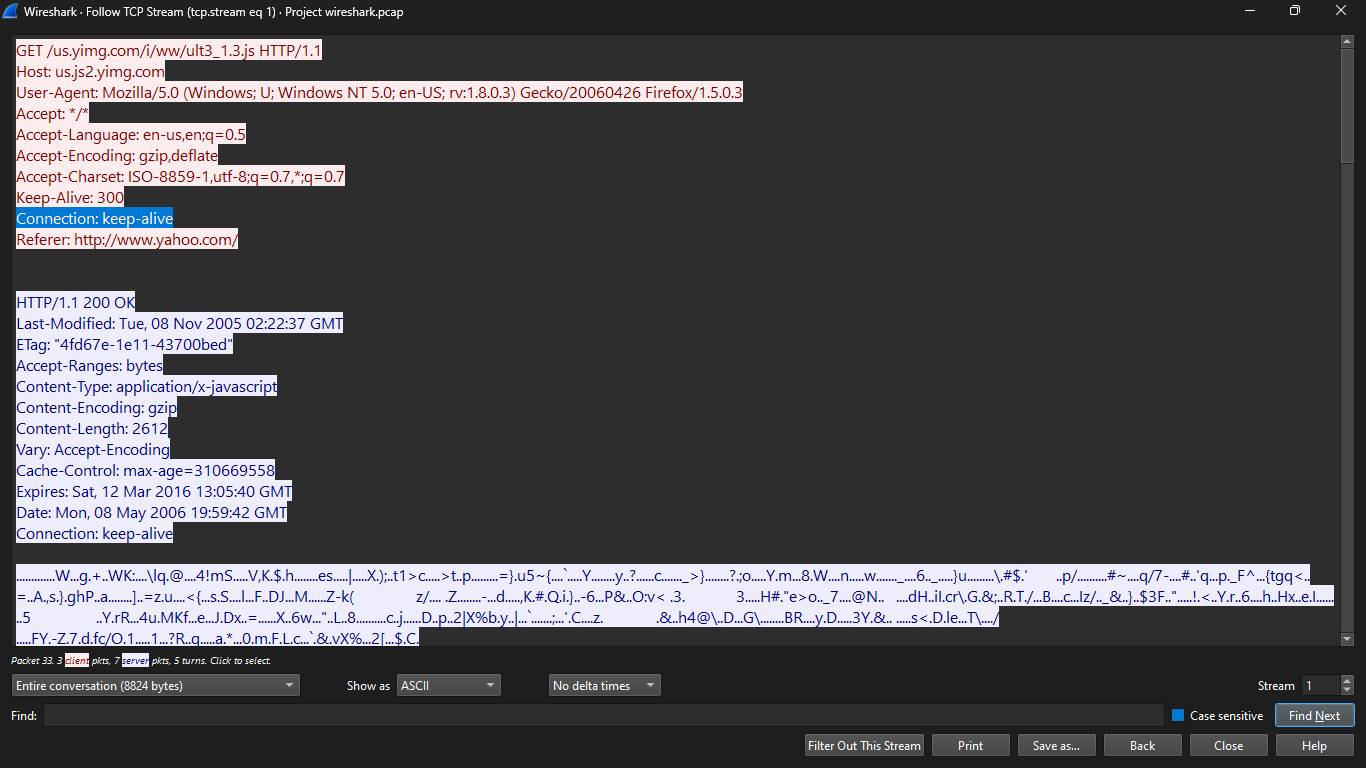
Vì đây là gói mà client gửi cho server nên ở cột source là IP của client.

1. **Cho biết loại HTTP connections là gì? (Non-persistent HTTP hay Persistent HTTP), tại sao?**

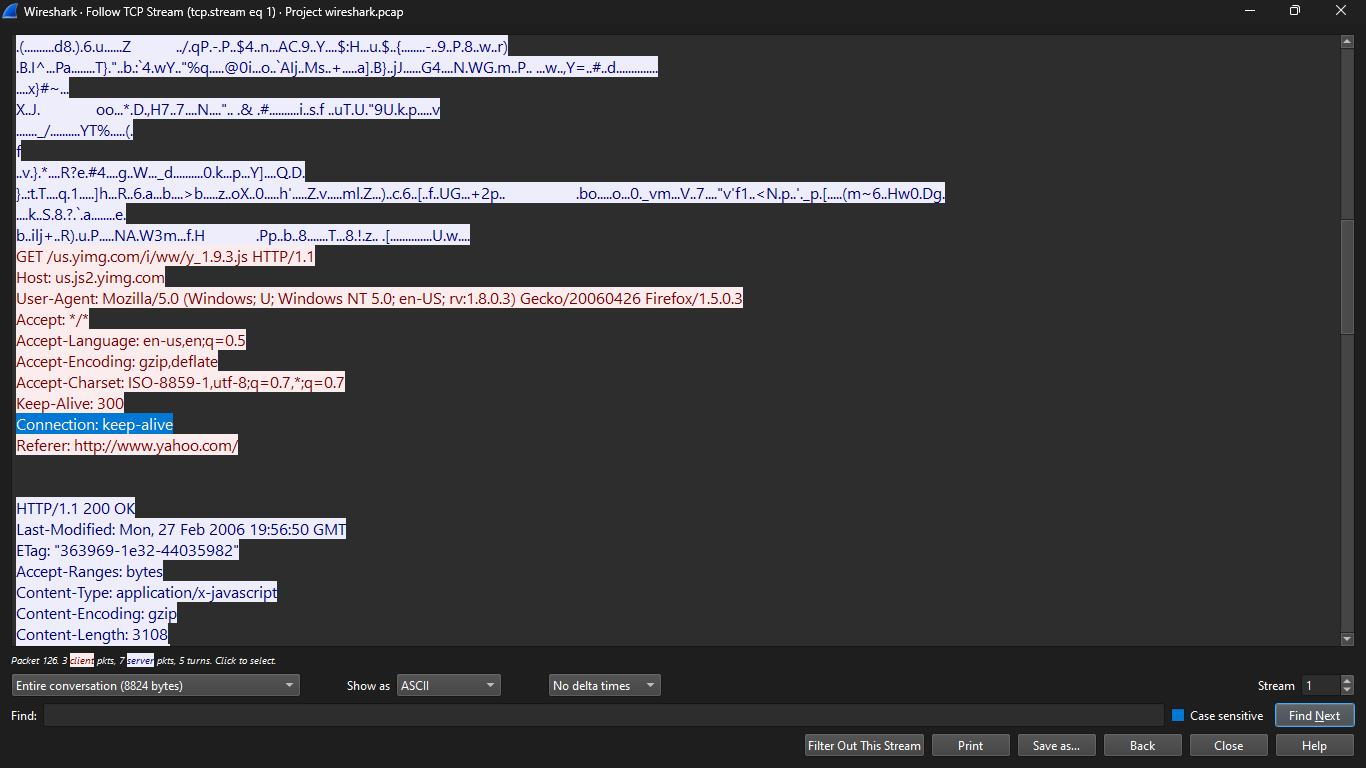
- Loại HTTP connections là: Persistent HTTP

- Bởi vì: Tất cả các yêu cầu đều chứa header Connection: keep-alive, cho phép giữ kết nối TCP mở sau mỗi yêu cầu, tránh việc thiết lập lại kết nối mới.

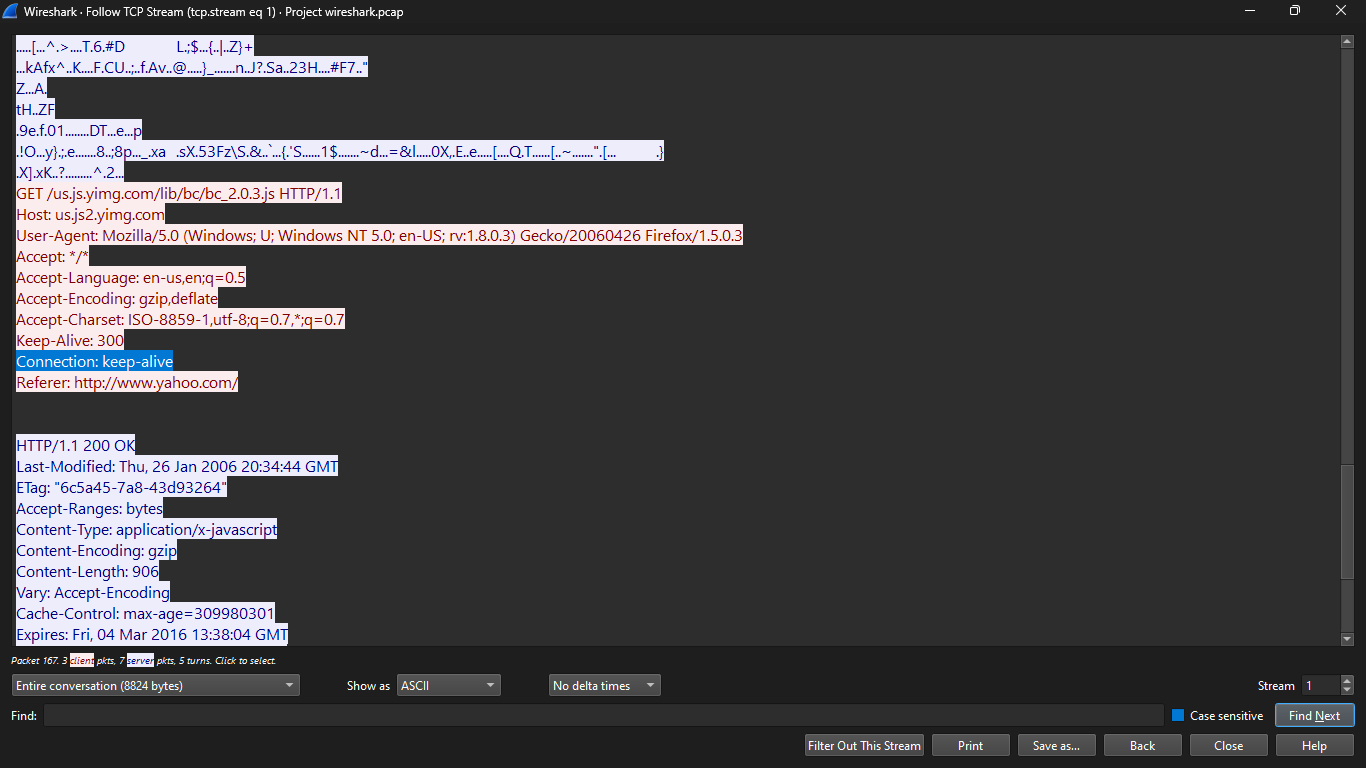
Request 1:



Request 2:



Request 3:



1. **Vẽ hình quá trình trao đổi gói tin giữa client và máy chủ bắt đầu từ gói tin TCP SYN đến khi kết thúc tcp stream filter. Hình vẽ thể hiện được seq number, SYN, ACK, ack number, lượng data (bytes) gửi đi .... (không sử dụng chức năng Statistics/Flow Graph của Wireshark)**

Ảnh có chứa văn bản, biên lai, Phông chữ, chữ viết tay

Mô tả được tạo tự động

**Bài 02: DHCP**

**1. Lọc các gói tin theo giao thức DHCP**

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

Mô tả được tạo tự động

**2. Gói tin DHCP sử dụng giao thức nào tại tầng transport**

UDP

**3. Hãy cho biết địa chỉ tại tầng link của host được cấp IP**

Client MAC address: MicroStarINT\_89:5d:91 (d8:bb:c1:89:5d:91)

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

Mô tả được tạo tự động

**4. Cho biết thông tin IP nguồn, Port nguồn và IP đích, Port đích của 4 gói tin (Discover/Offer/Request/ACK) trong đợt xin cấp IP đầu tiên**

Gói Discover:

IP nguồn: 0.0.0.0

PORT nguồn: 68

IP đích: 255.255.255.255

PORT đích: 67

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

Mô tả được tạo tự động

Gói Offer:

IP nguồn:192.168.100.1

PORT nguồn: 67

IP đích: 192.168.100.145

PORT đích: 68

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

Mô tả được tạo tự động

Gói Request:

IP nguồn: 0.0.0.0

PORT nguồn: 68

IP đích: 255.255.255.255

PORT đích: 67

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

Mô tả được tạo tự động

Gói ACK:

IP nguồn:192.168.100.1

PORT nguồn: 67

IP đích: 192.168.100.145

PORT đích: 68

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

Mô tả được tạo tự động

**5. Chỉ ra điểm khác biệt giữa các giá trị trong gói tin DHCP Discover và DHCP Request**

Về cơ bản thì cả 2 gói tin có các giá trị giống nhau.

Nhưng ở trường Message type có sự khác nhau, ở gói DHCP Discover có message type là Discover, ở gói DHCP Request có message type là Request.

Gói DHCP Request có trường Option: (54) DHCP Server Identifier còn gói DHCP Discover không có trường này.Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự độngẢnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự độngẢnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động

**6. Cho biết giá trị Transaction-ID của 4 gói tin (Discover/Offer/Request/ACK) trong đợt xin cấp IP đầu tiên, giá trị Transaction-ID của 2 gói tin (Request/ACK) trong đợt xin cấp IP lần hai.**

**Mục đích sử dụng của transaction-ID là gì?**

Transaction-ID đợt xin cấp IP 1: **0xb7e0a583**

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

Mô tả được tạo tự động

Transaction-ID 2 gói Request và ACK đợt xin cấp IP 2: **0x71106dfa**

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

Mô tả được tạo tự động

**Mục đích của việc dùng Transaction-ID: dùng để phân biệt các giao dịch DHCP của các thiết bị khác nhau trên cùng một mạng**

**7. Cho biết ý nghĩa trường thông tin lease-time, giá trị của trường này trong gói tin bắt được là bao nhiêu?**

**Ý nghĩa: Thời gian thuê IP mà DHCP server cấp phát cho clien**t

Giá trị trường này nằm trong gói Offer hoặc gói ACK, cả 4 gói trong 2 đợt cấp đều có giá trị là: **12 hours (43200)**  
Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự độngẢnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự độngẢnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự độngẢnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động

**8. Trong gói tin DHCP bắt được, hãy chỉ ra trường giá trị cho biết có thông tin DHCP relay agent hay không? Nếu có hãy cho biết IP của DHCP relay agent.**

Không có thông tin DHCP relay agent do

Relay agent IP address: 0.0.0.0

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động

**Bài 03: ICMP**

**1. Cho biết MSS (maximum segment size) là gì? Có liên quan gì đến MTU (maximum transmission unit)?**

- MSS (Maximum Segment Size) là tham số TCP xác định kích thước tối đa của một segment dữ liệu mà máy tính có thể gửi trong một lần trao đổi qua mạng. MSS được chỉ định trong tiêu đề TCP để thông báo kích thước tối đa dữ liệu cho các máy khác.

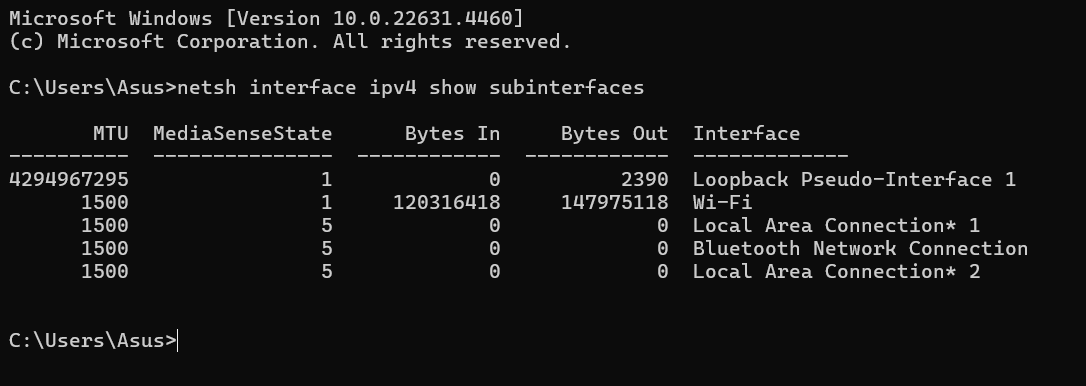
- MSS thường được đặt trong các tiêu đề TCP để hướng dẫn các máy tính khác

về kích thước tối đa của các phần dữ liệu mà chúng nên gửi.

- MSS giới hạn kích thước tối đa của dữ liệu trong mỗi segment TCP. Dữ liệu từ lớp ứng dụng sẽ được chia nhỏ để không vượt quá MSS trước khi truyền qua TCP.

- Khi xuống lớp liên kết (như Ethernet), dữ liệu tiếp tục được chia nhỏ theo MTU (Maximum Transmission Unit) để đảm bảo phù hợp với giới hạn liên kết và không cần cắt nhỏ thêm khi truyền qua mạng.

**2. Cho biết MTU trên card mạng kết nối internet của máy bạn là bao nhiêu (có chụp hình)?**

****

MTU:1500

**3. Kích thước MTU là 1500, cho biết kích thước của các phần của gói ICMP tại tầng mạng cơ bản (network) là bao nhiêu? (cho biết cách tính toán của bạn để có kết quả của từng phần)**

MTU: 1500 bytes

IP Header: 20 bytes (IPv4)

ICMP Header: 8 bytes  
ICMP Payload = MTU – IP Header – ICMP Header = 1500 – 20 – 8 = 1472 bytes

**4. Kích thước MTU là 1500, cho biết kích thước của các phần của gói ICMP tại tầng Data Link cơ bản là bao nhiêu? (cho biết cách tính toán của bạn để có kết quả của từng phần)**

MTU: 1500 bytes

Ethernet Header: 14 bytes

IP Header: 20 bytes (IPv4)

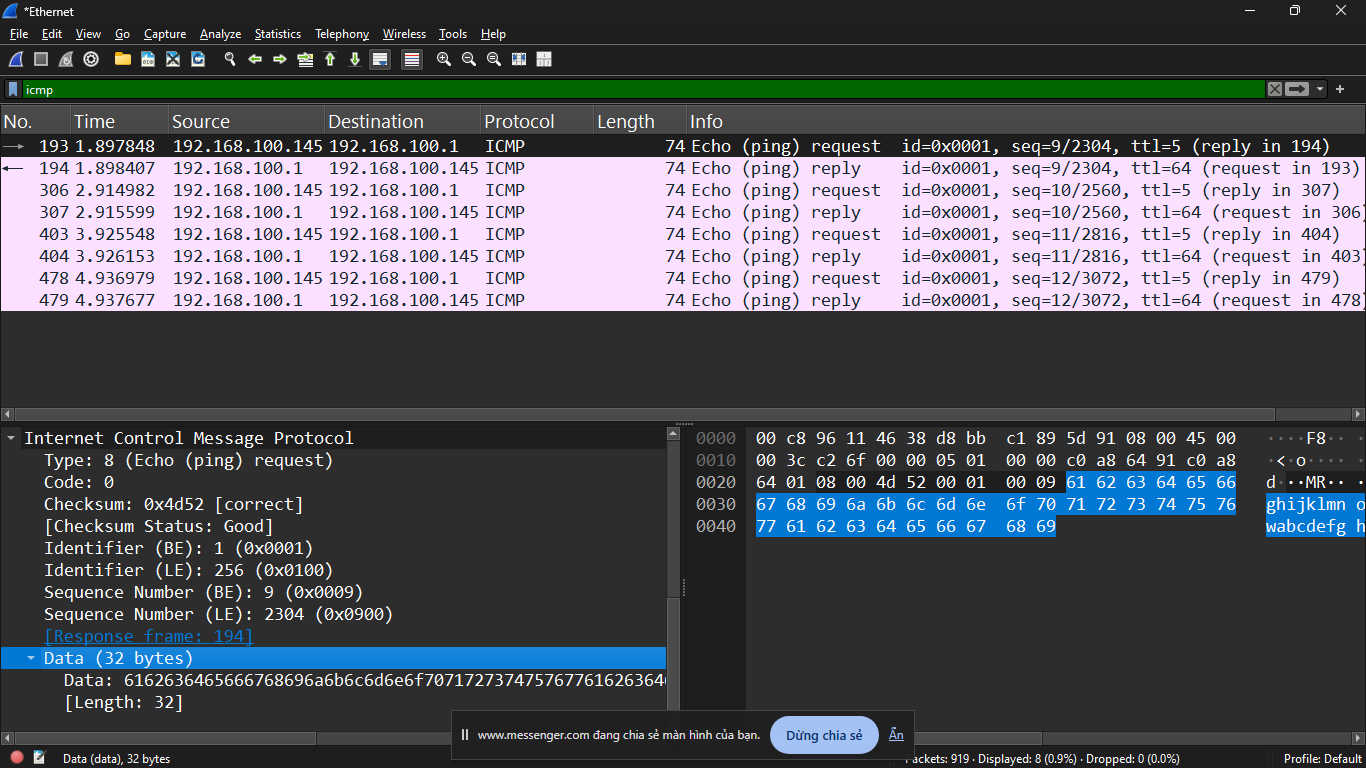
ICMP Header: 8 bytes

ICMP Payload = MTU – Ethernet Header – IP Header – ICMP Header = 1500 – 14 – 20 – 8 = 1458 bytes

**5.**

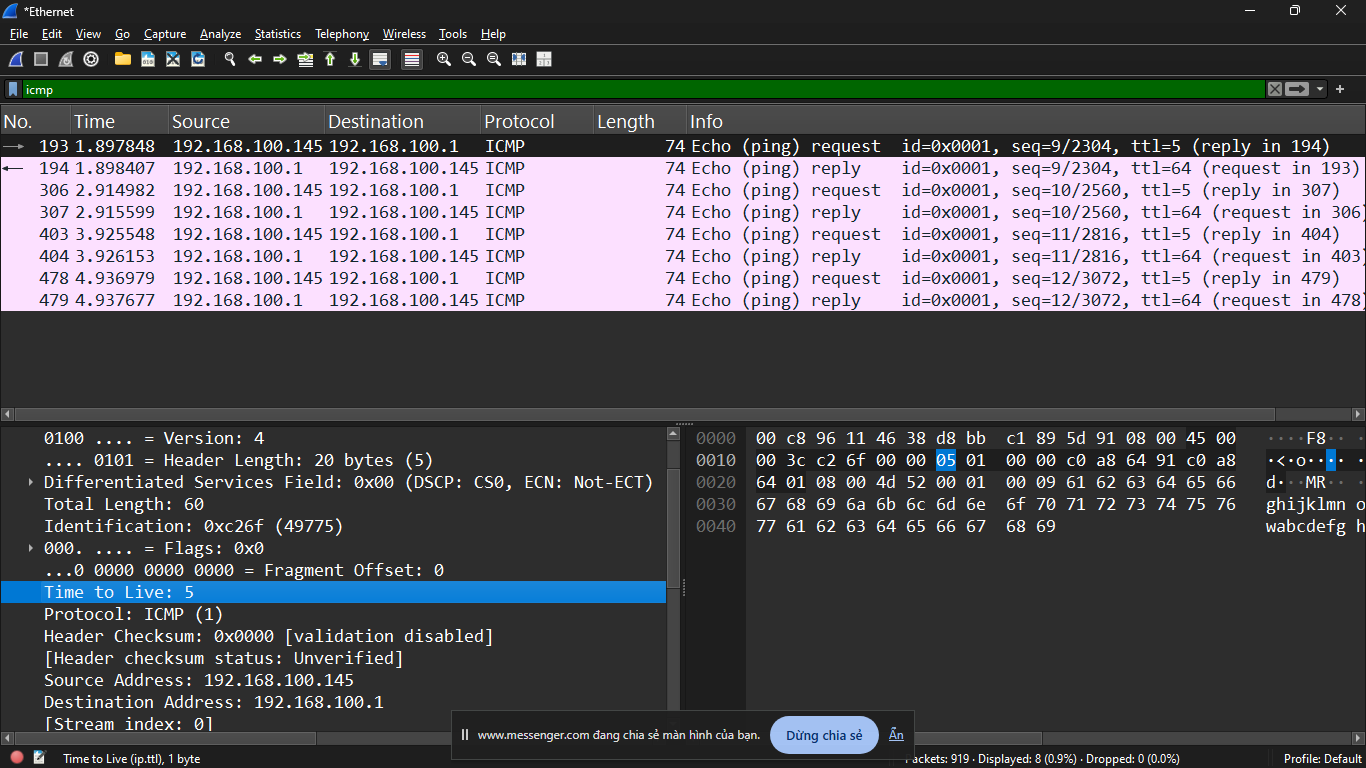
**5.1 "> ping -i 5 <ip của default gateway>"**

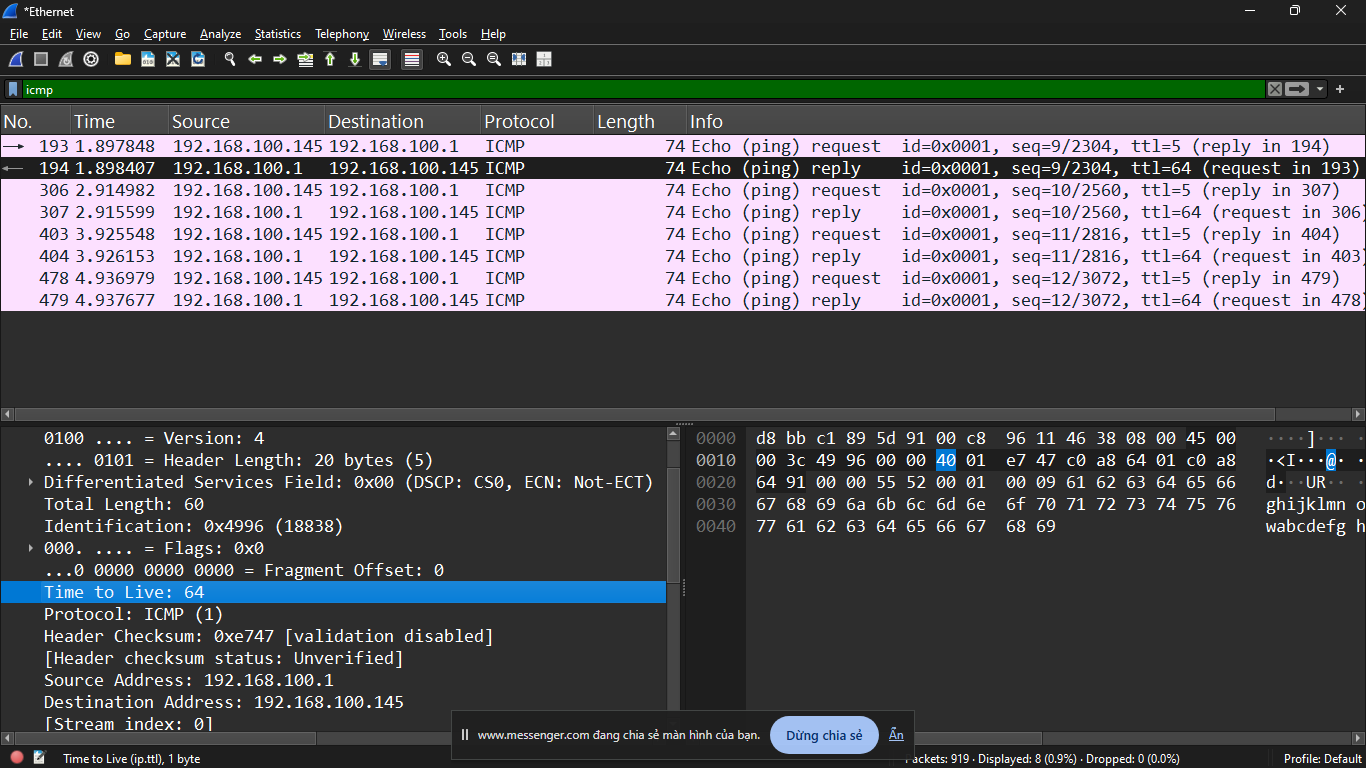
**Data trong ICMP (ICMP payload): 32 bytes**



**TTL của gói request là 5**

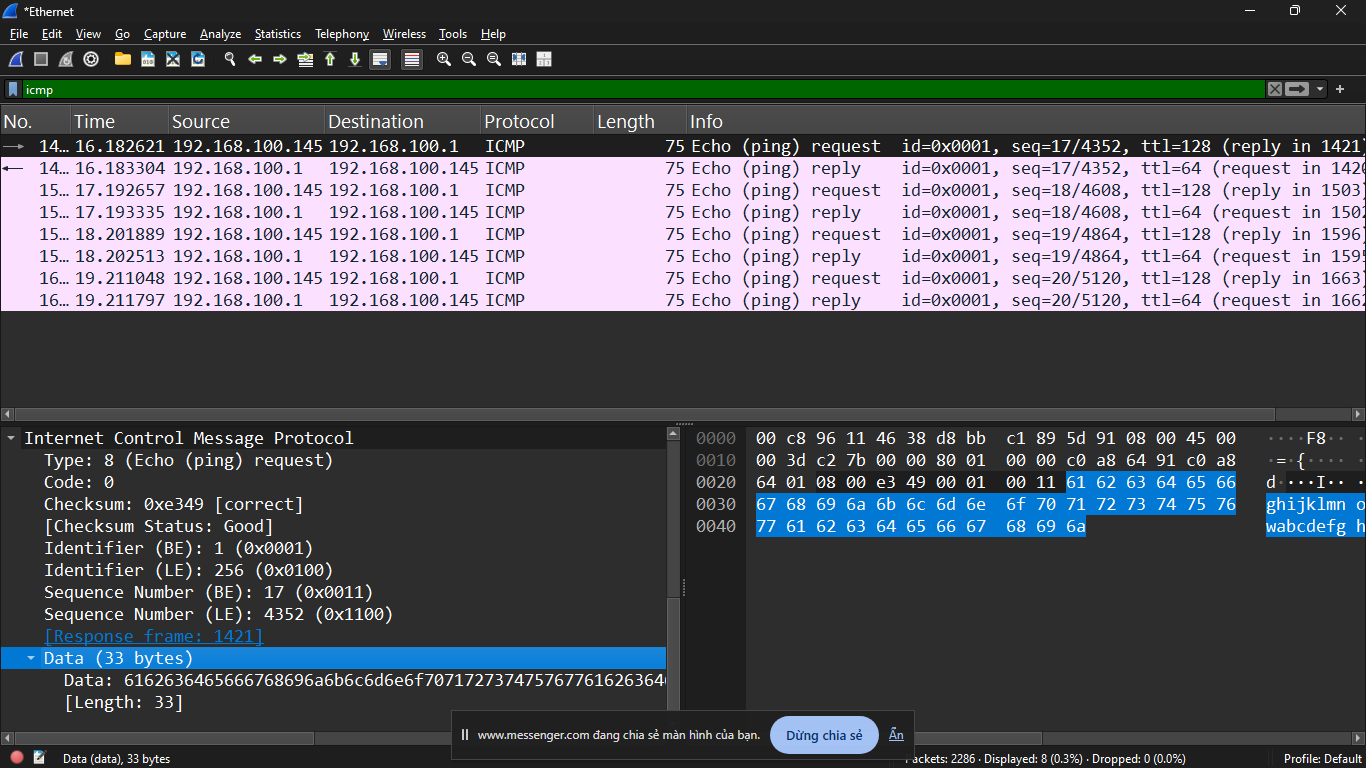
**của gói reply là 64**

****

****

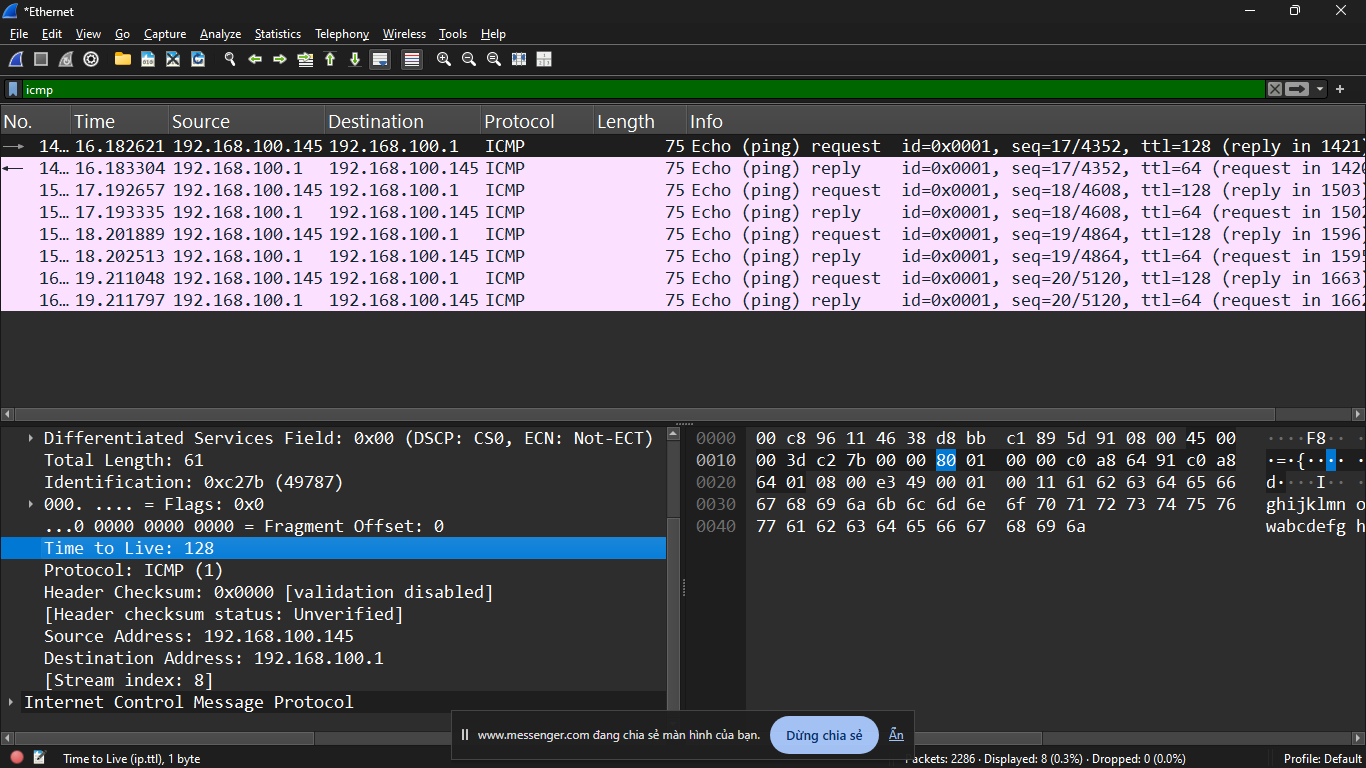
**5.2 "> ping -l 33 <ip của default gateway>"**

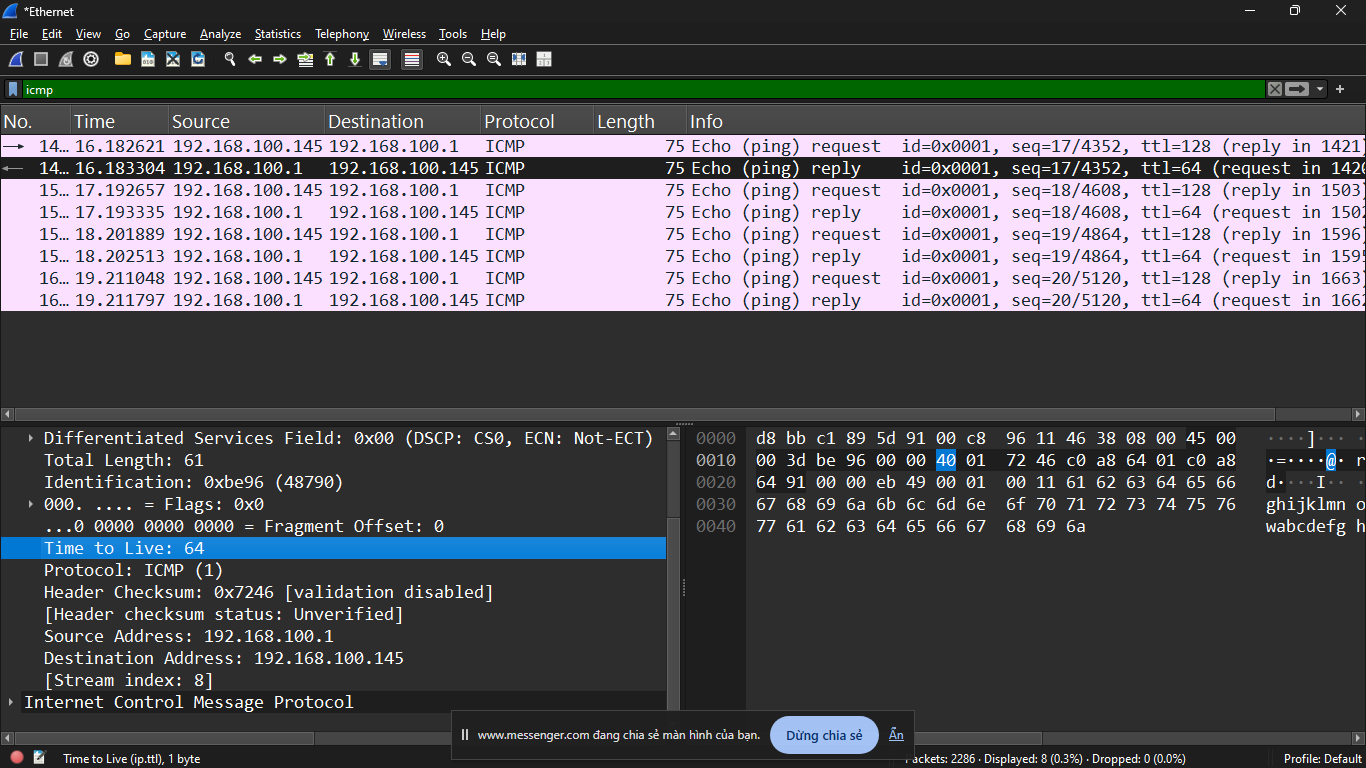
**Data trong ICMP (ICMP payload): 33 bytes**

****

**TTL của gói request là 128**

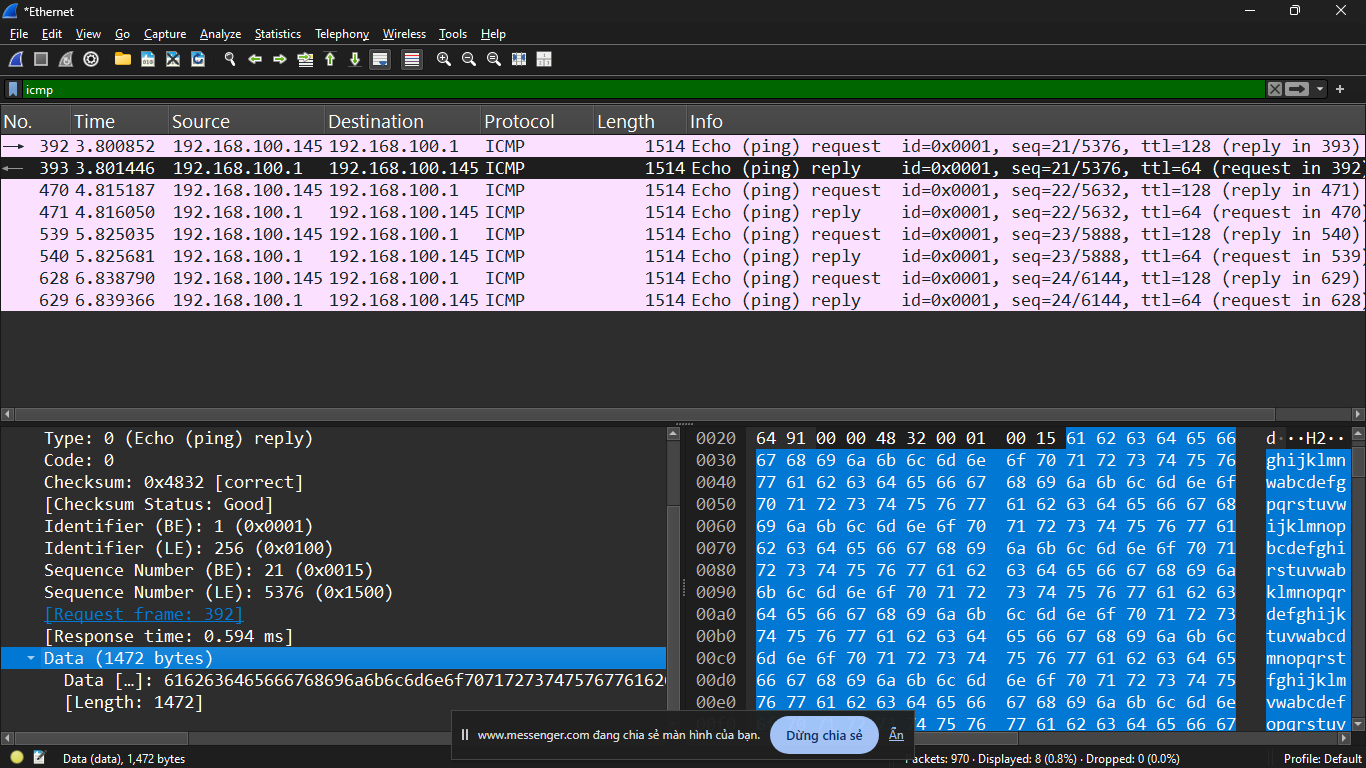
**của gói reply là 64**

****

****

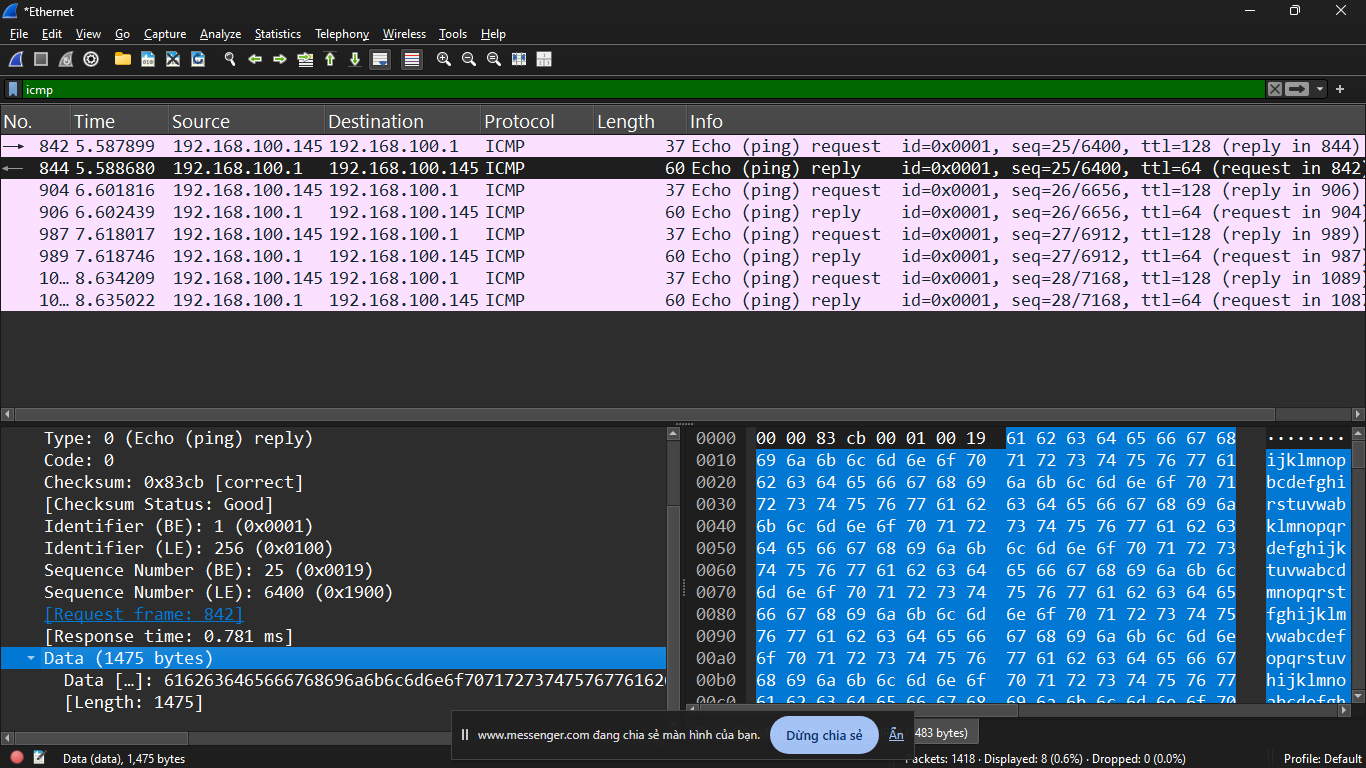
**6. "> ping -l 1472 <ip của default gateway>"**

**Data trong ICMP (ICMP payload): 1472 bytes**



**7. "> ping -l 1475 <ip của default gateway>"**

**Data trong ICMP (ICMP payload): 1475 bytes**

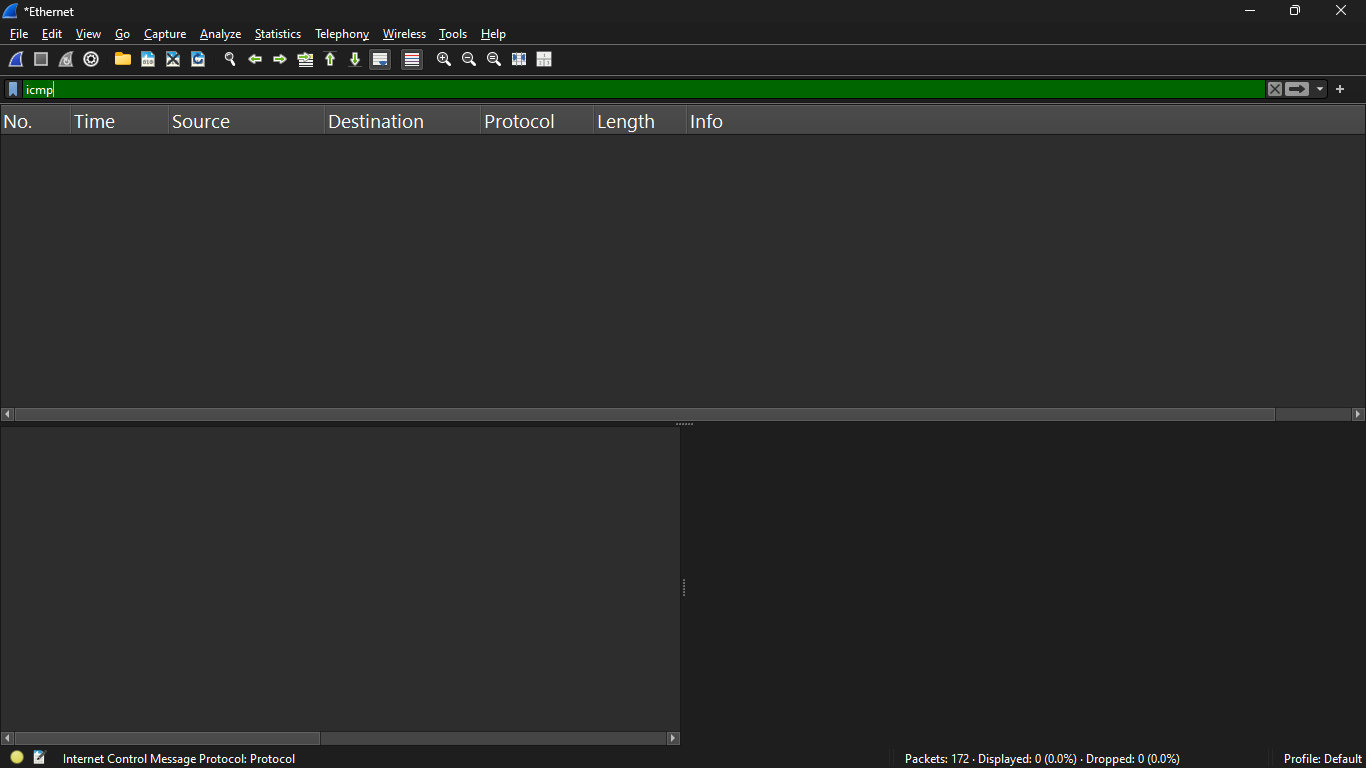


Gói tin đã bị phân mảnh do vượt quá giới hạn MTU vì 20 bytes (IP Header) + 8 bytes (ICMP Header) + 1475 bytes (ICMP Payload) = 1503 bytes > 1500 bytes

****

**8."> ping -f -l 1475 <ip của default gateway>"**

Không có gói tin ICMP Echo Reply



Bởi vì: Lệnh ping -f yêu cầu gửi các gói tin ICMP Echo Request liên tục mà không chờ phản hồi.

Lệnh -l 1475 yêu cầu mỗi gói tin có kích thước payload là 1475 bytes.

Vấn đề chính là kích thước gói tin vượt quá MTU (1500 bytes) của mạng, mà DF (Don't Fragment) flag được bật. Điều này có nghĩa là:

Gói tin không thể bị chia nhỏ khi vượt quá MTU.

Các router sẽ không chấp nhận gói tin vượt quá MTU và trả về thông báo ICMP lỗi "Destination Unreachable, Fragmentation needed".

Do đó, không có gói ICMP Echo Reply được gửi lại từ máy đích vì gói tin không thể đến được do giới hạn MTU của mạng.