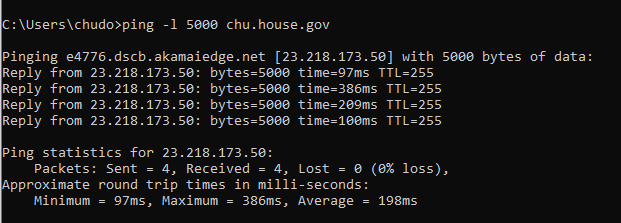
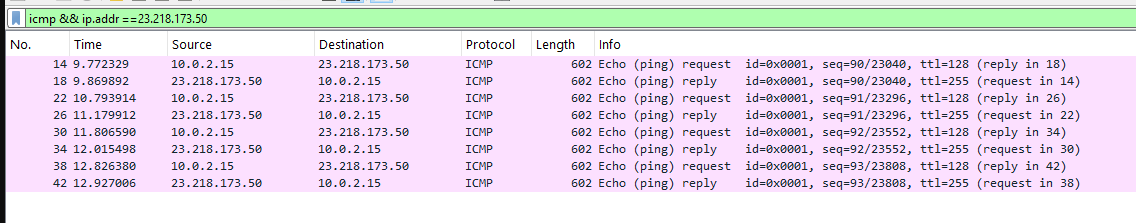
chọn trang web có tên miền dễ nhận dạng với họ, hoặc họ tên viết tắt

ở đây tôi chọn trang web: [https://chu.com.au](https://chu.com.au/)

1. Phân tích lưu lượng bằng ping



hình 1 - sử dụng ping trên terminal



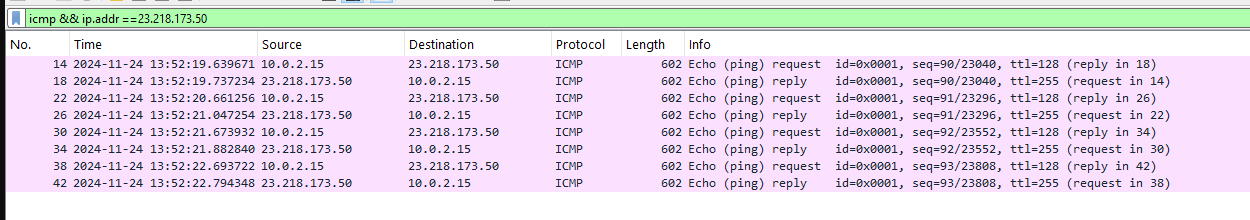
hình 2 - Lưu lượng tiện ích Ping trên Wireshark

Tại hình 2 chúng ta lọc lấy các protocol ICMP và lọc cụ thể IP đang muốn bắt.

* Phân tích bảng:

Cột No. : Số thứ tự gói tin

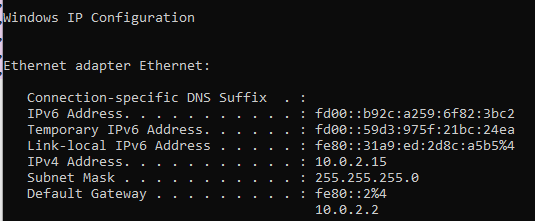
Cột Time: là thời gian, chúng ta có thể thay đổi định dạng để dễ nhìn hơn băng cách: tại menu chọn view -> time display format -> mục đầu tiên



xét dòng 1, tức No.14

Cột source: chính là source ip trên máy tính:

Ta xem ip của máy tính bằng câu lệnh ipconfig



Cột Destination: là địa chỉ mà chúng ta vừa ping

Cột protocol: ICMP: là protocol sử dụng cho lệnh ping của chúng ta.

Cột length: độ dài gói tin

Cột info: Chứa thông tin, các kiểu dữ liệu

Ví dụ request là kiểu dữ liệu ,

id : seq: 90/2340: là gói tin 90 trong tổng số gói tin 2340

ttl = 128: time to live

reply in 18: nếu như muốn xem thông tin reply, thì coi gói tin thứ 18. tức là No.18

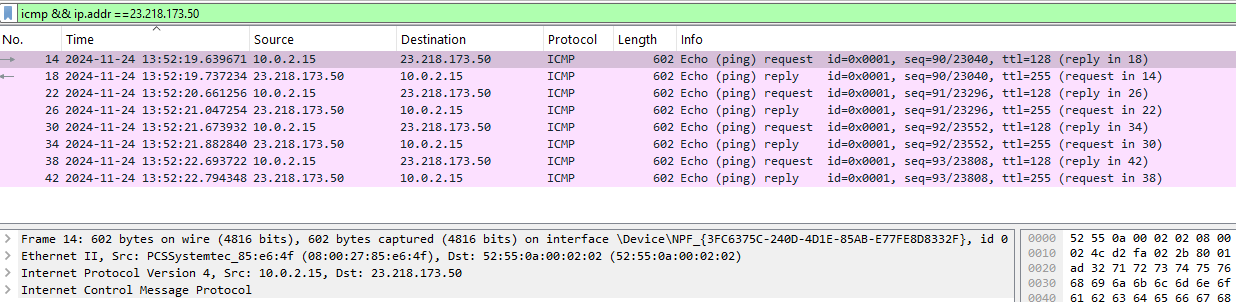
vậy nghĩa là gói tin 18 trả lời cho gói tin 14

xét No.18, cột info: mục request in 14: cho ta biết gói tin request là gói 14

sau khi thực hiện xong request và reply thì nó ms trả về 

(khi ta ping trên terminal)

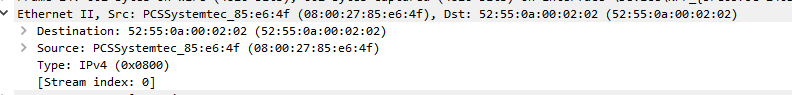
Tiếp tục chúng ta xem xét tiếp, ta click vào dòng No.14



Hiển thị ở dưới chính tà biểu thị cho 4 tầng giao thức TCP

Tầng Frame: Là tầng 1 (Physical Layer) : làm việc với các bit nhị phân.

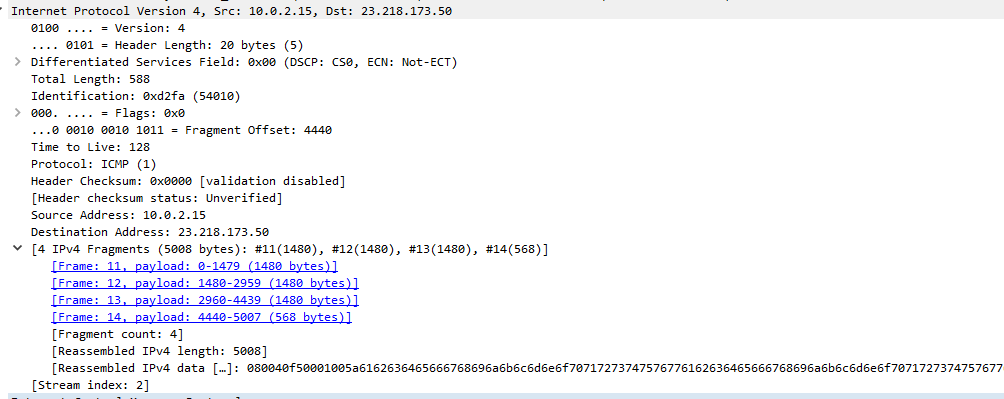
Tầng Ethernet: Là tầng 2: Cho biết nó sử dụng công nghệ Ethernet, ở đây nó cho ta biết đc source và destination, và ip đang chạy là ip version nào.



ở mục source nhờ vào 24 bit đầu tiên nó sẽ test ra chúng ta đang dùng máy nào (máy ảo nào hoặc máy thật)

mục desti cũng vậy

Tại tầng Internet: Tầng 3:



ở đây nó sẽ cho ta biết rõ hơn về các thông tin

như ở đây đang sử dụng IPv4

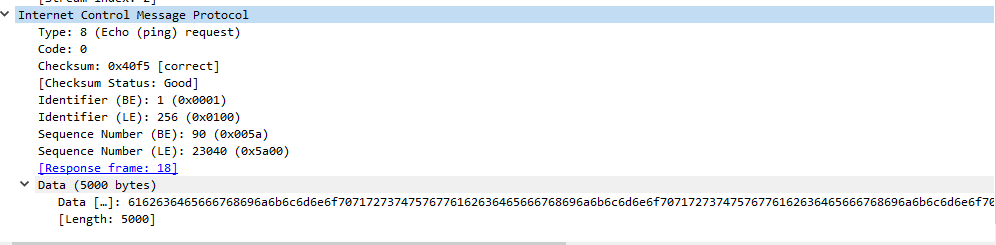
Và cũng ghi rõ source IP của máy và IP chúng ta đang ping

Giao thức đang dùng là ICMP và protocol id ở đây là = 1

Tổng độ dài total length: 588

Time to live: 128

Tầng 4: Cho biết nó đang sử dụng protocol j.



Như chúng ta thấy nó đang được sử dụng ICMP (internet control message protocol)

dòng type: Ta biết đc kiểu request, và máy tính sẽ hiểu request là số 8, còn số 0 là reply

Trả lời cho các câu hỏi

1. Gói tin gốc có bị phân mảnh không, trường nào cho biết điều này?

Các bước thực hiện:

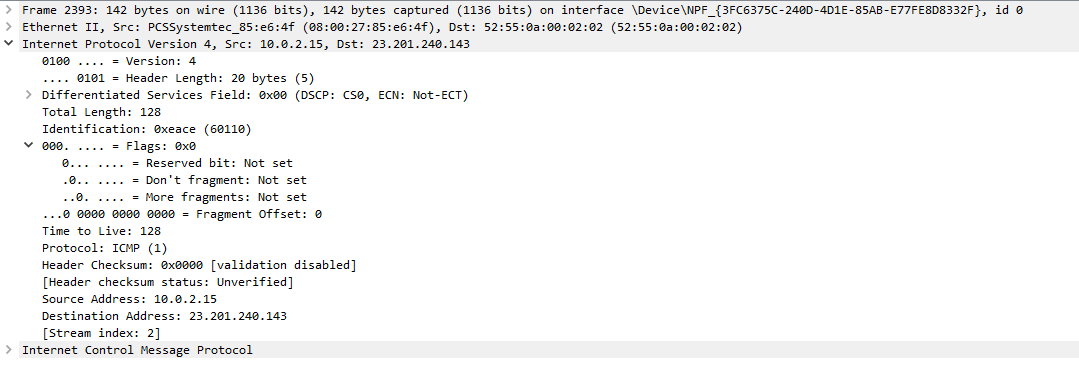
Kiểm tra trường IP Flags và Fragment Offset:

**Chọn một gói tin** từ danh sách.

Trong cửa sổ chi tiết gói tin (Packet Details Pane), mở phần Internet Protocol Version 4 (IPv4)

Tìm các trường sau:

* **Flags (Cờ)**:
  + Trường này chứa các bit điều khiển cho phân mảnh.
  + Ba bit Flags thường gặp:
    - **Bit DF (Don't Fragment)**: Nếu giá trị là 1, không được phép phân mảnh.
    - **Bit MF (More Fragments)**: Nếu giá trị là 1, đây là gói bị phân mảnh và vẫn còn các phân mảnh tiếp theo.
    - **Bit Reserved**: Thường bằng 0 (không sử dụng).
* **Fragment Offset**:
  + Trường này xác định vị trí của phân mảnh trong gói tin ban đầu.
  + Nếu giá trị là 0, đây là phân mảnh đầu tiên hoặc gói tin không bị phân mảnh.



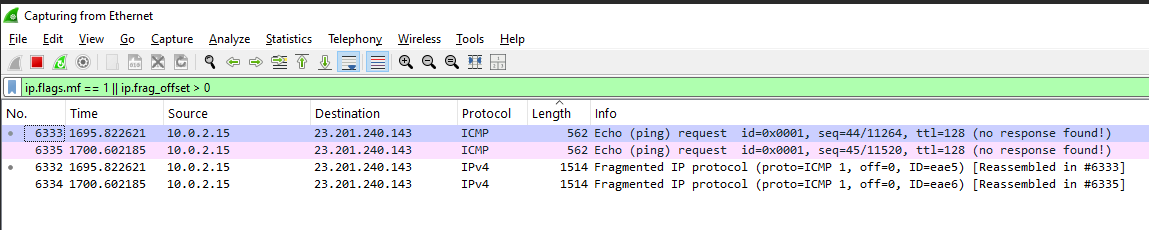
giá trị trong trường **Flags** và **Fragment Offset** có các ý nghĩa như sau:

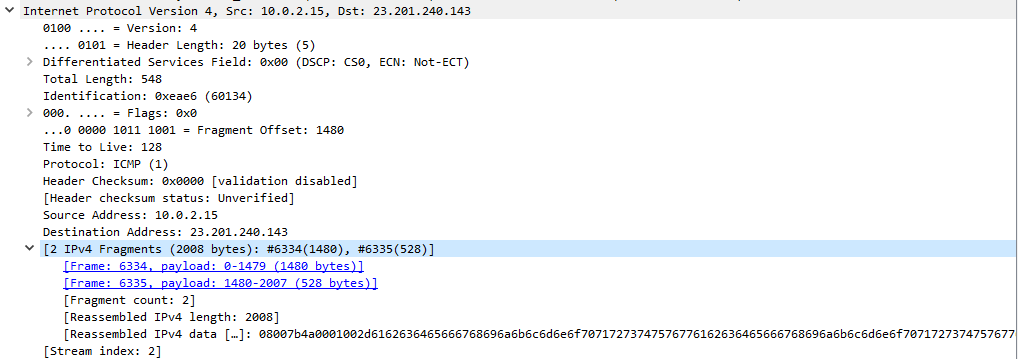
### **Phân tích giá trị**

1. **Flags (0x0)**:
   * **Reserved bit**: Not set (bằng 0).
   * **Don't Fragment**: Not set (bằng 0).
   * **More Fragments**: Not set (bằng 0).
   * **Giá trị tổng**: 0x0, có nghĩa là:
     + Gói tin này không bị phân mảnh.
     + Không có yêu cầu rằng gói tin phải "không được phân mảnh" (DF = 0).
     + Đây là gói tin hoàn chỉnh, không cần thêm bất kỳ phân mảnh nào.
2. **Fragment Offset (0)**:
   * Giá trị này là 0, cho biết rằng:
     + Đây không phải là một phân mảnh.
     + Nếu gói tin này là một phần của quá trình phân mảnh, Fragment Offset sẽ chứa giá trị khác 0 (ví dụ: vị trí của phân mảnh trong gói ban đầu).

Trả lời cho câu hỏi: Không, không xảy ra phân mảnh. Các trường xác nhận điều này là Flags (0x0) và Fragment Offset (0).)

Dò tìm các gói tin bị phân mảnh: ip.flags.mf == 1 || ip.frag\_offset > 0





2. Thông tin nào cho biết một phân đoạn gói là cuối cùng hay trung gian?