# ICMP

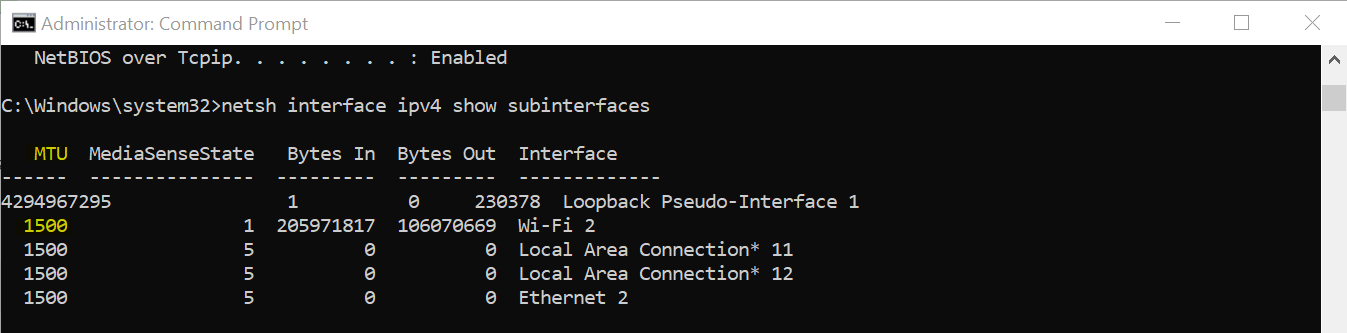
1. Cho biết MSS (maximum segment size) là gì? có liên quan gì đến MTU (maximum transmission unit)?

* MTU (Maximum Transmission Unit) là kích thước gói tin lớn nhất có thể được gửi trong một mạng. Giao thức kiểm soát truyền dẫn (TCP) trên Internet sử dụng MTU để xác định kích thước tối đa của mỗi gói tin trong bất kỳ quá trình truyền dữ liệu nào.
* MSS (Maximum Segment Size) là độ dài tối đa của một phân đoạn (segment) được truyền tải trên một kết nối TCP (Transmission Control Protocol). MSS không bao gồm tiêu đề TCP hoặc tiêu đề IP, mà chỉ quy định kích thước tối đa của phần dữ liệu trong gói tin. Do đó, MSS được xác định bởi giá trị MTU (Maximum Transmission Unit) của mạng trừ đi độ dài các tiêu đề TCP và IP.

<https://www.imperva.com/learn/application-security/what-is-mtu-mss/>

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

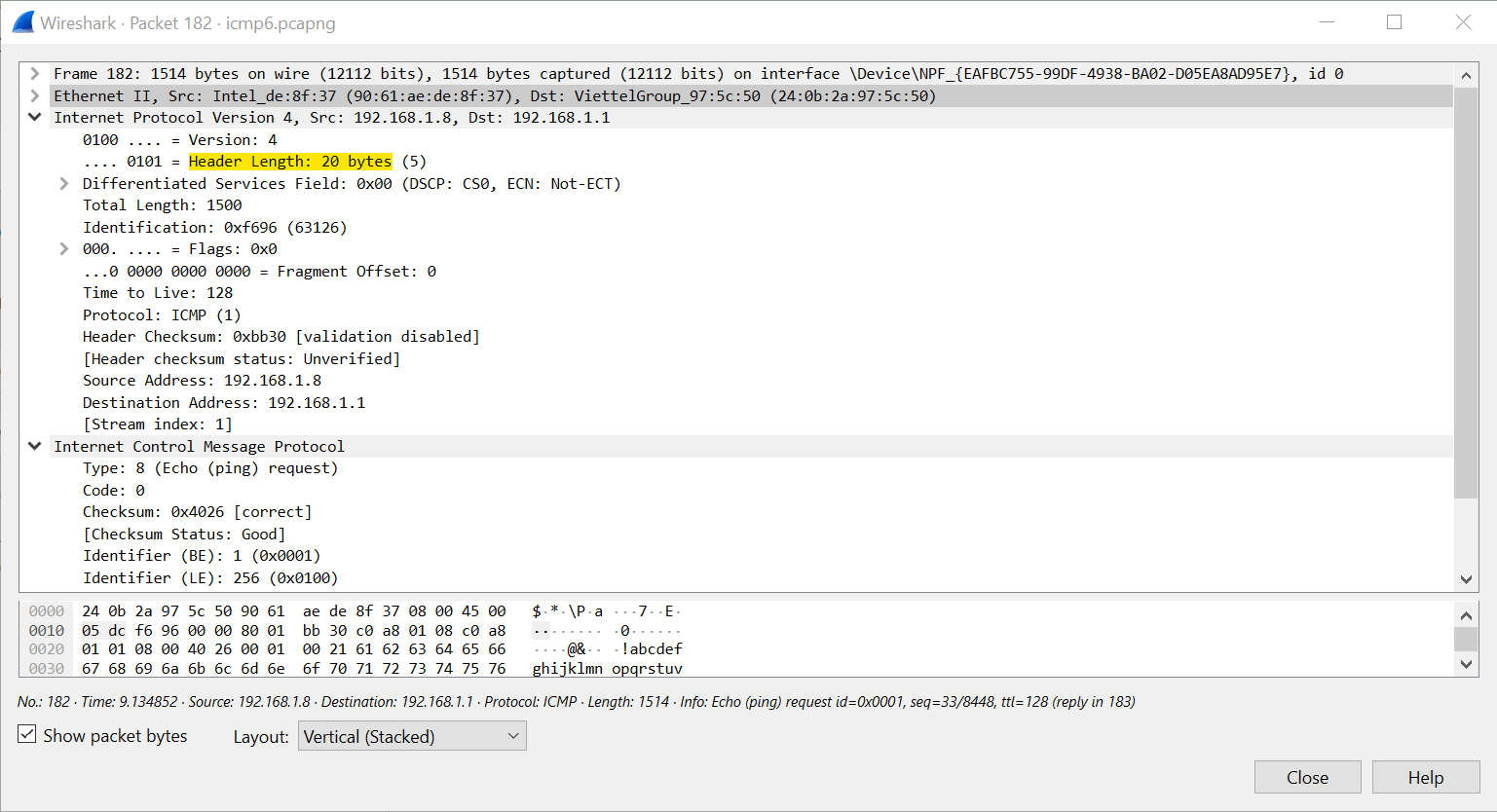
* MTU trên card mạng có kết nối internet của máy là 1500 bytes.



1. 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)

* Gói ICMP tại tầng Network bao gồm các phần:

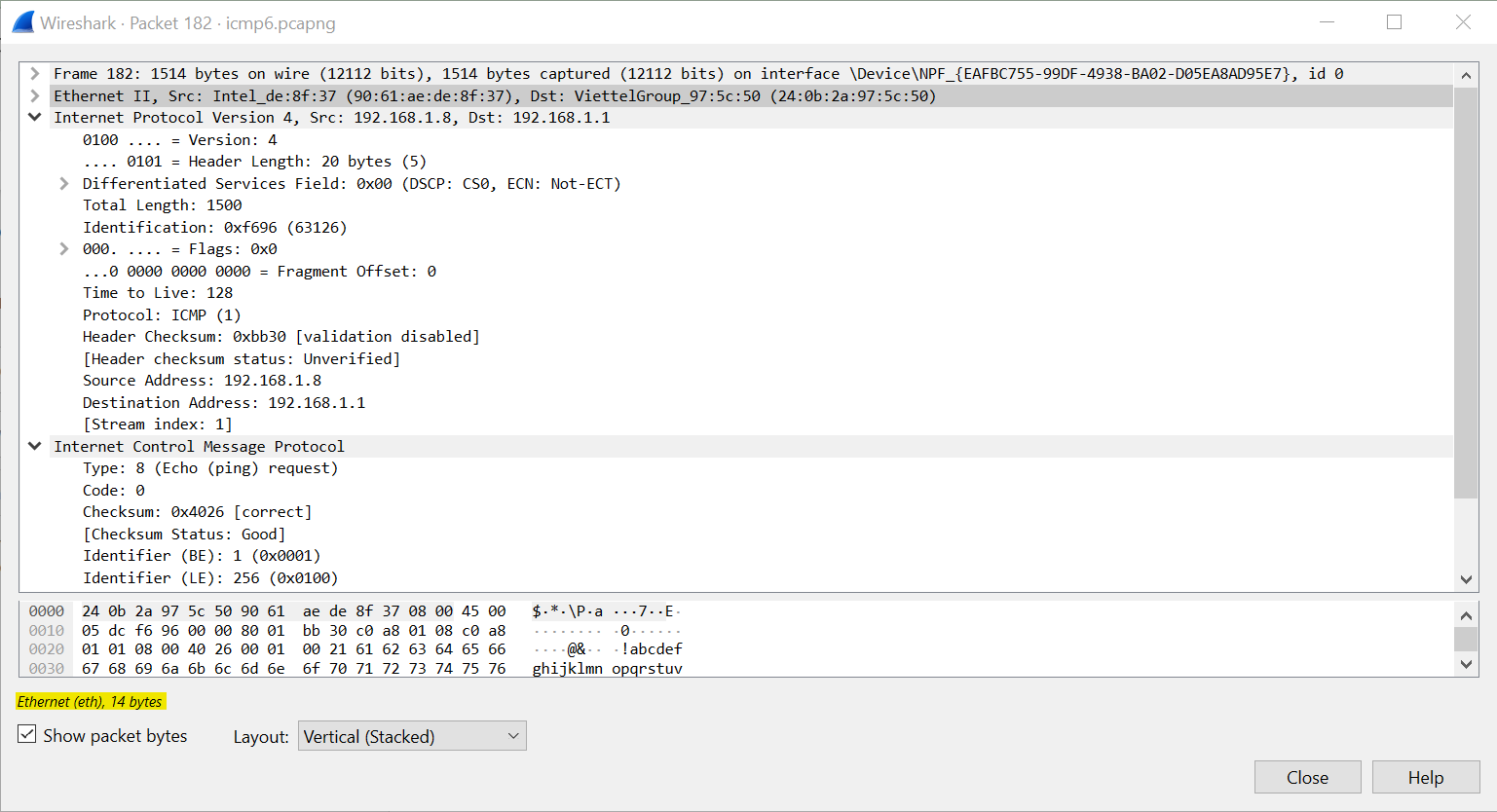
+ IP Header: 20 byte (đối với IPv4)



+ ICMP Header: 8 + ICMP payload byte

=> Đáp án: 28 + ICMP payload.

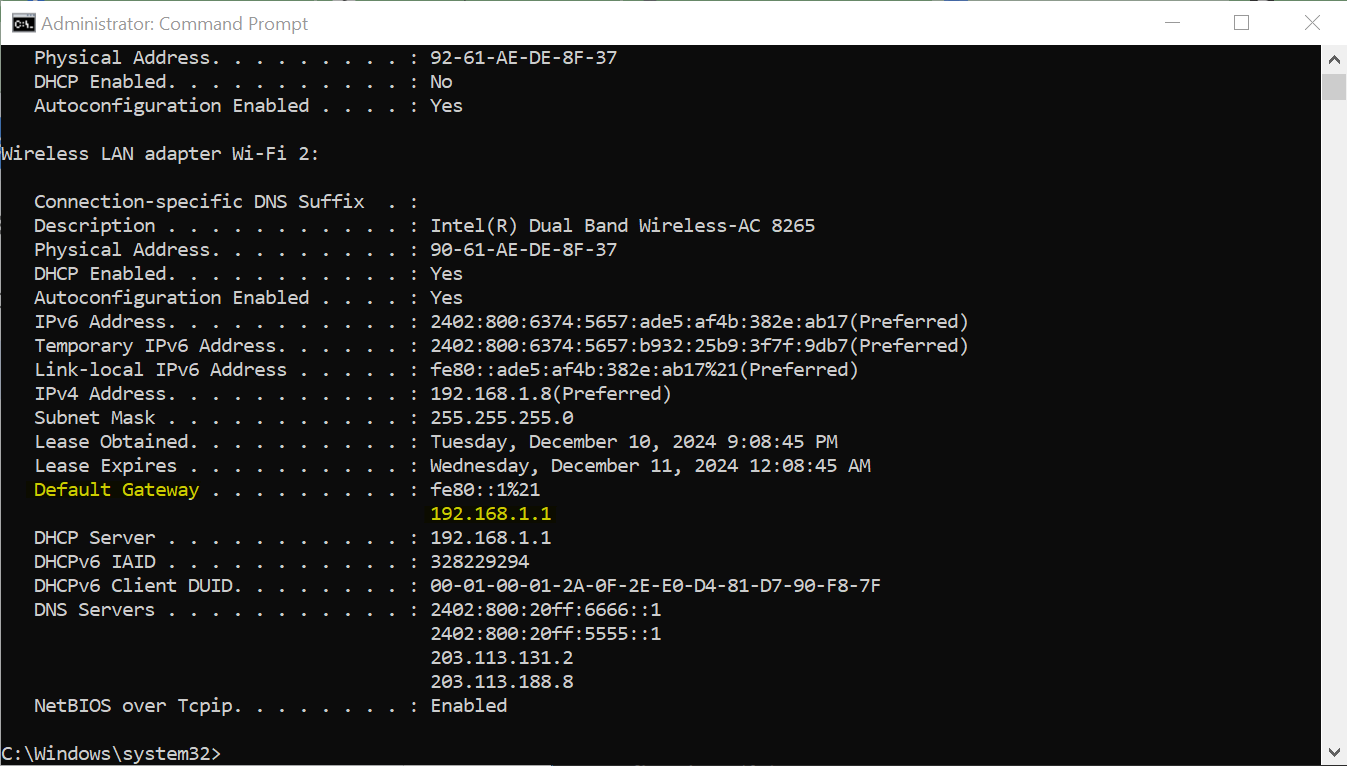
1. Kích thước MTU là 1500, cho biết kích thước của các phần của gói ICMP tại tầng Data Link cơ bản là bao nhiêu? (cho biết cách tính toán của bạn để có kết quả của từng phần)



* Tương tự câu trên, nhưng có thêm phần Ethernet Header: 14 byte

=> Đáp án: 42 + ICMP payload.

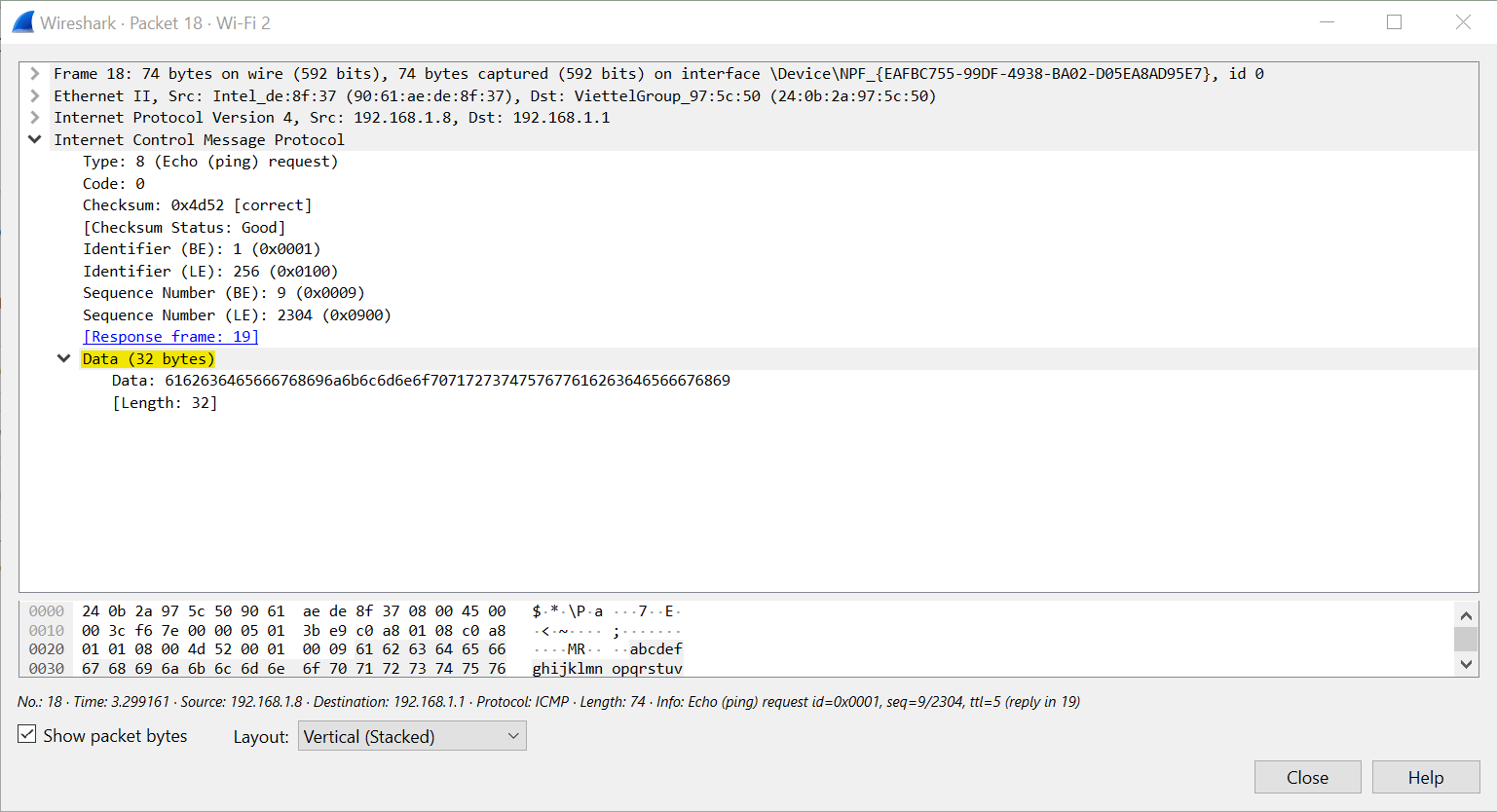
Chuẩn bị:



5.1

"> ping -i 5 <ip của default gateway>". Vd: ping -i 5 192.168.1.1 và bắt gói tin lưu lại với tên file "icmp5\_1.pcap". Cho biết lượng data trong ICMP (ICMP payload) là bao nhiêu? TTL (Time to live) là bao nhiêu?

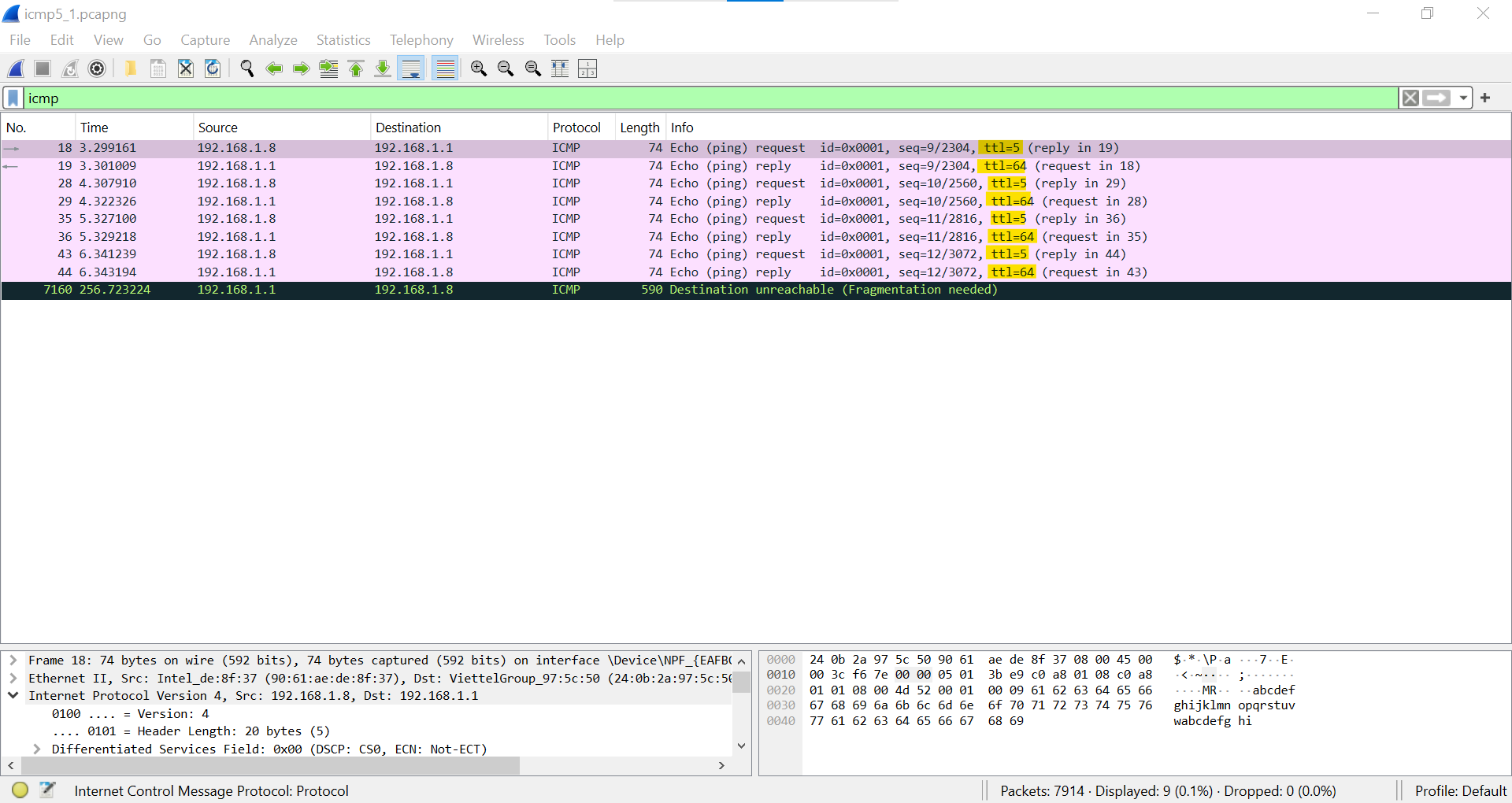
* Dựa vào trường “Data” trong phần tiêu đề ICMP của các gói tin, ta quan sát được ICMP payload là 32 byte.



* Dựa vào trường “Time to Live” trong phần tiêu đề IPv4 của các gói tin, ta quan sát được:

+ Các gói ICMP request có TTL = 5 giây (Sử dụng lệnh ping -i 5 <ip của default gateway> sẽ thay đổi khoảng thời gian giữa các gói ICMP request thành 5 giây)

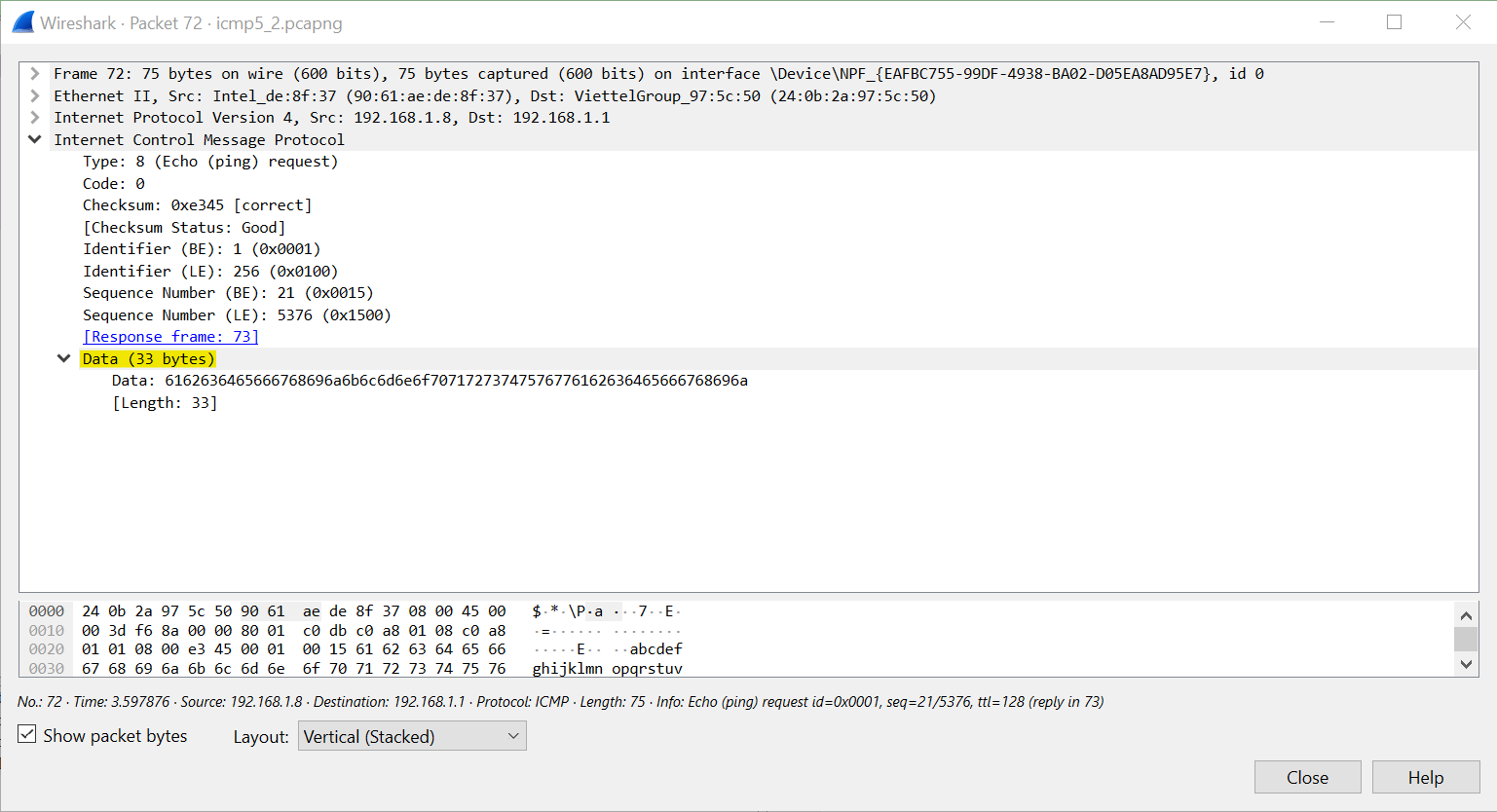
+ Các gói ICMP reply có TTL = 64 giây



5.2

"> ping -l 33 <ip của default gateway>" . Vd: ping -l 33 5 192.168.1.1 và bắt gói tin lưu lại với tên file "icmp5\_2.pcap". Cho biết lượng data trong ICMP (ICMP payload) là bao nhiêu? TTL (Time to live) là bao nhiêu?

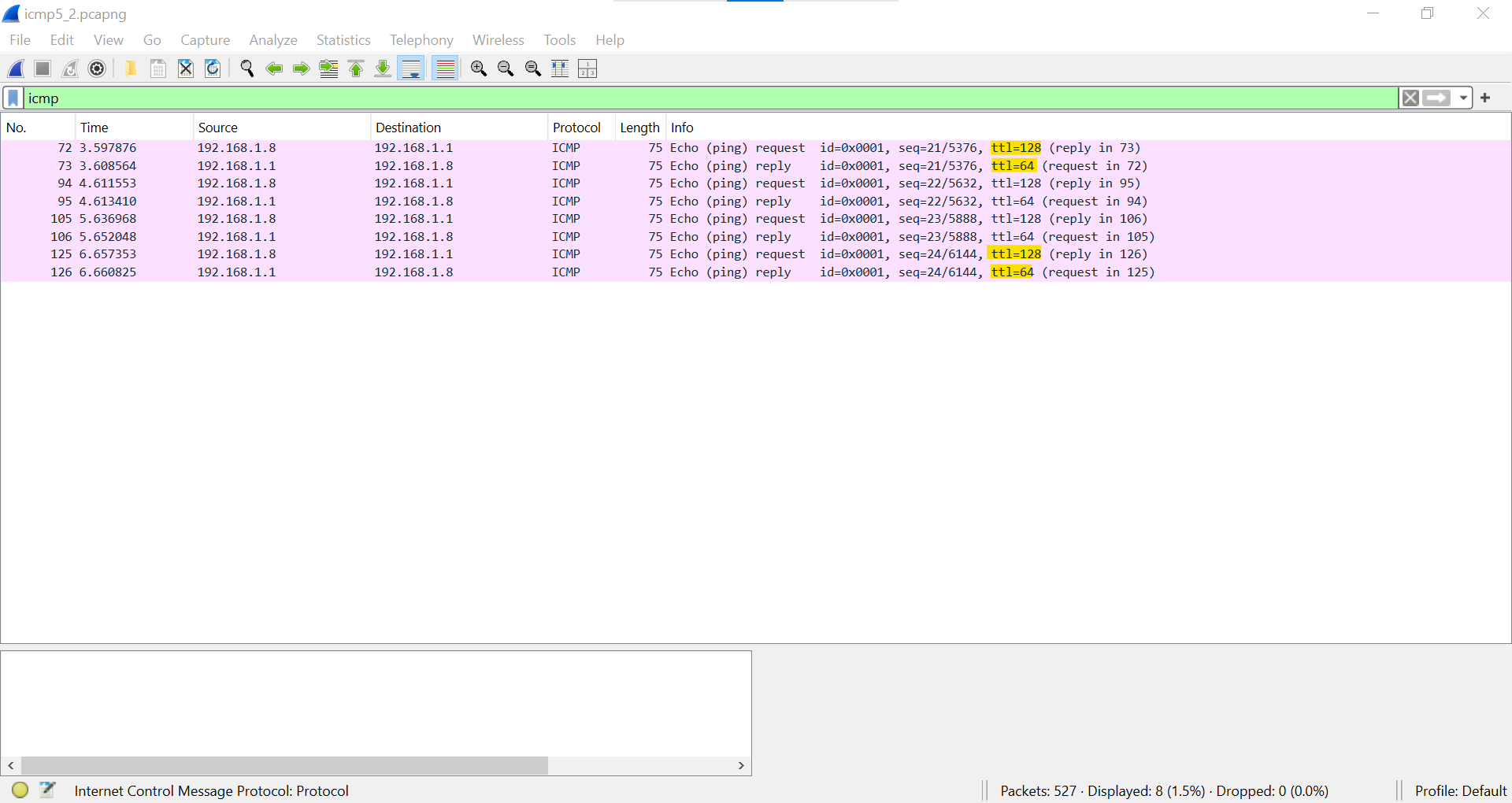
* Dựa vào trường “Data” trong phần tiêu đề ICMP của các gói tin, ta quan sát được ICMP payload là 33 byte. (lệnh "> ping -l 33 <ip của default gateway>" sẽ cài đặt ICMP payload thành 33 byte)



* Dựa vào trường “Time to Live” trong phần tiêu đề IPv4 của các gói tin, ta quan sát được:

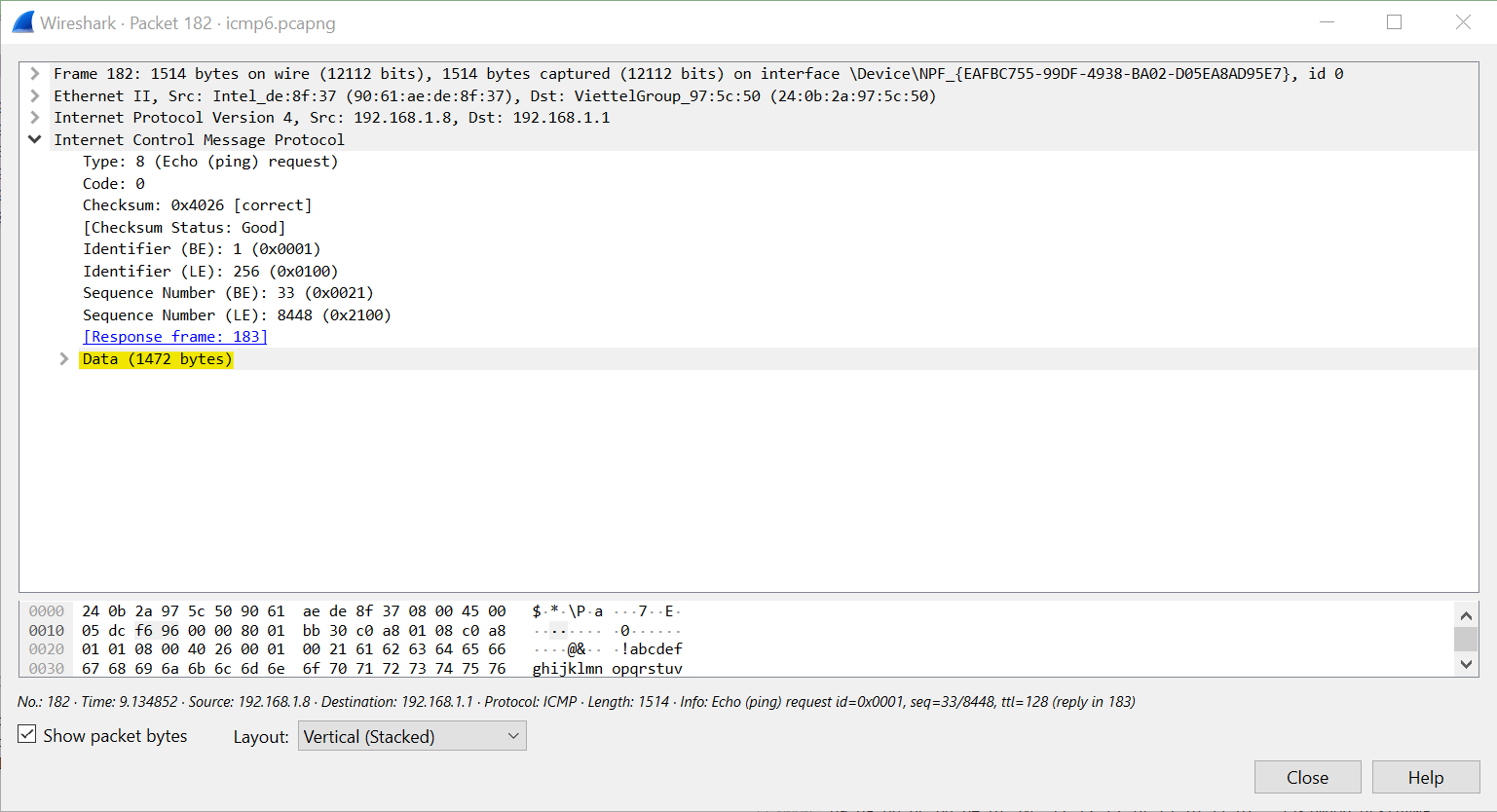
+ Các gói ICMP request có TTL = 128 giây

+ Các gói ICMP reply có TTL = 64 giây



6. "> ping -l 1472 <ip của default gateway>". Vd: ping -l 1472 5 192.168.1.1 và bắt gói tin lưu lại với tên file "icmp6.pcap". Cho biết lượng data trong ICMP (ICMP payload) là bao nhiêu?

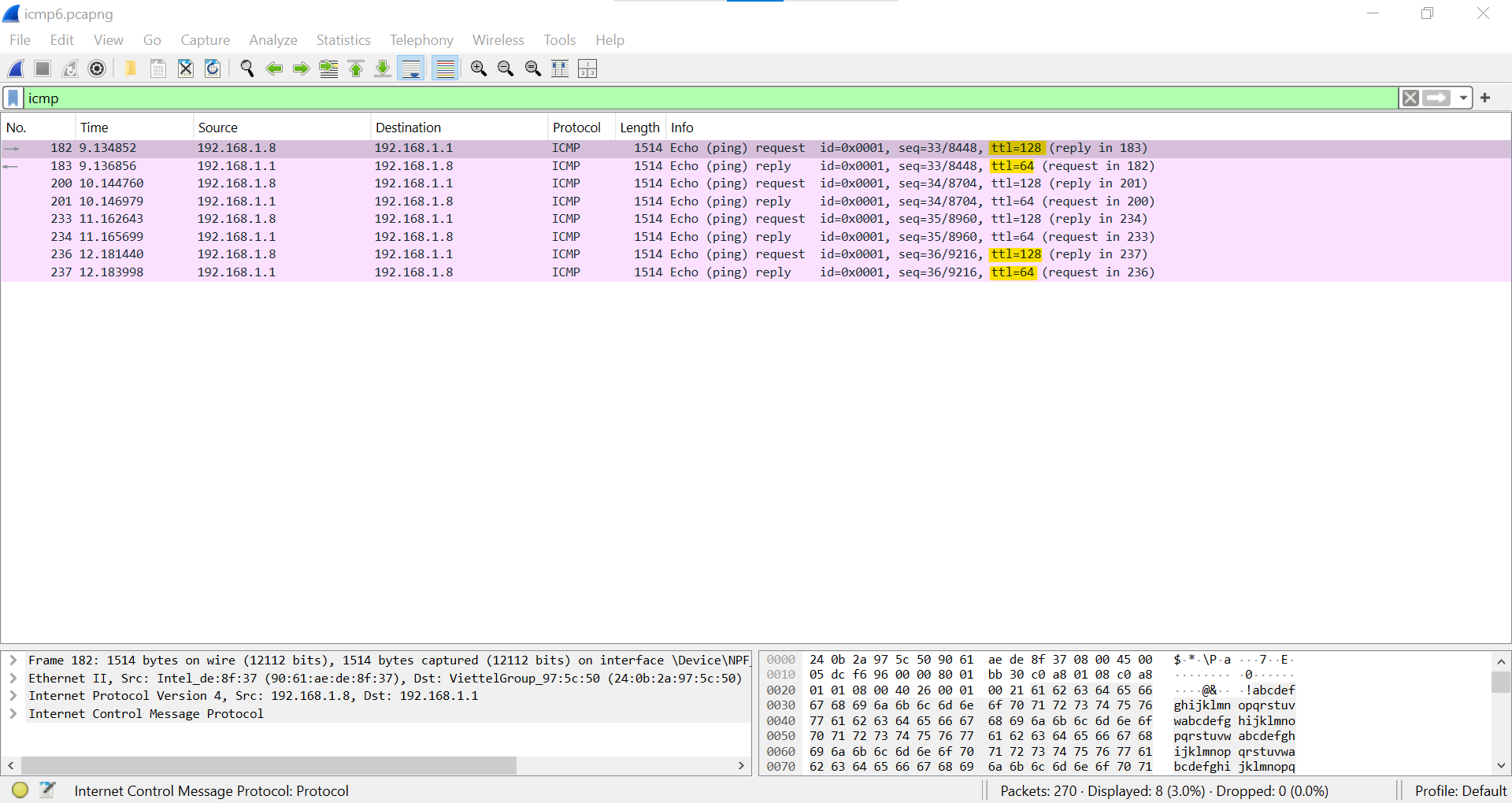
* Dựa vào trường “Data” trong phần tiêu đề ICMP của các gói tin, ta quan sát được ICMP payload là 1472 byte. (lệnh "> ping -l 1472 <ip của default gateway>" sẽ cài đặt ICMP payload thành 1472 byte)



* Dựa vào trường “Time to Live” trong phần tiêu đề IPv4 của các gói tin, ta quan sát được:

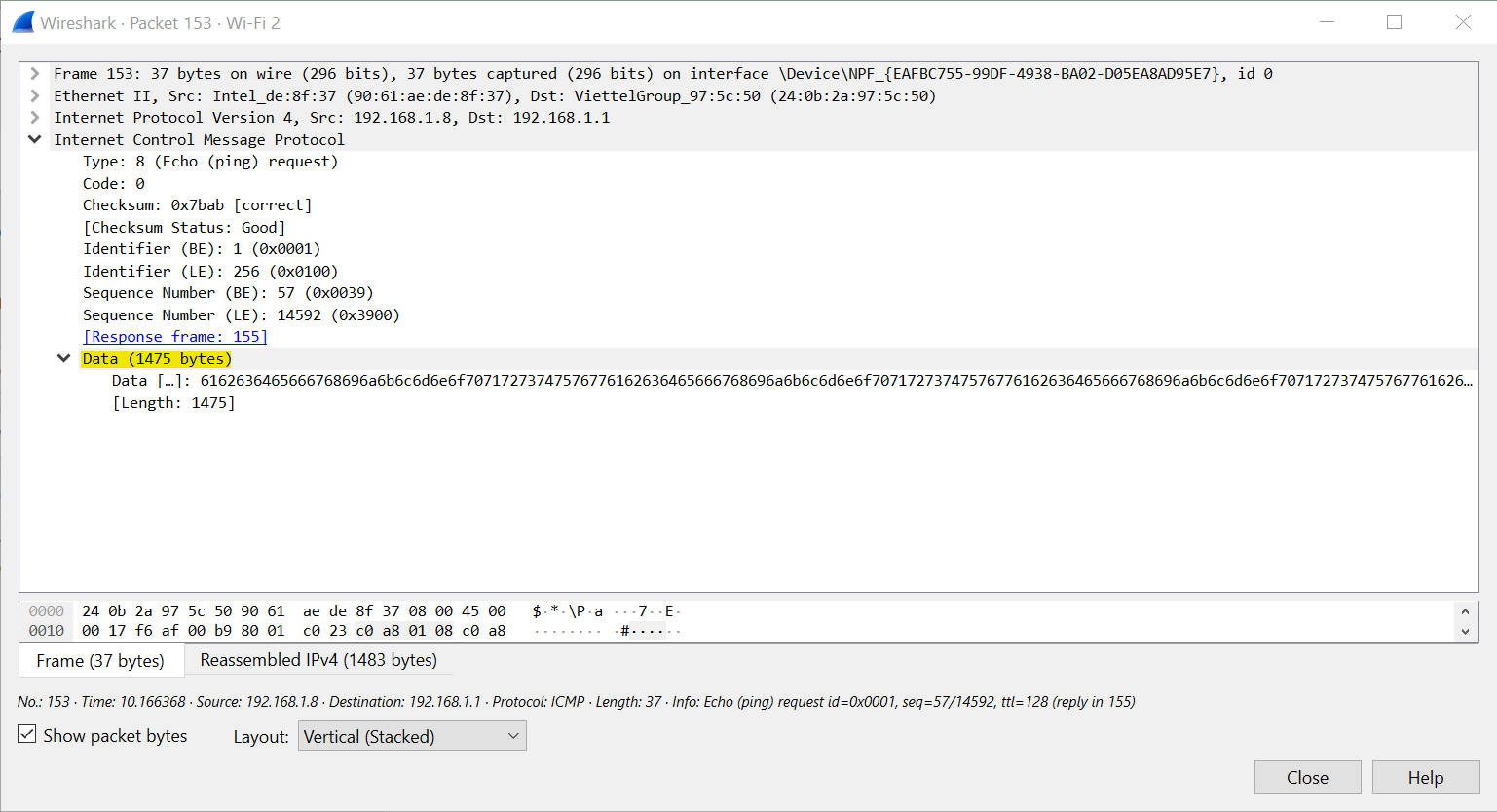
+ Các gói ICMP request có TTL = 128 giây

+ Các gói ICMP reply có TTL = 64 giây

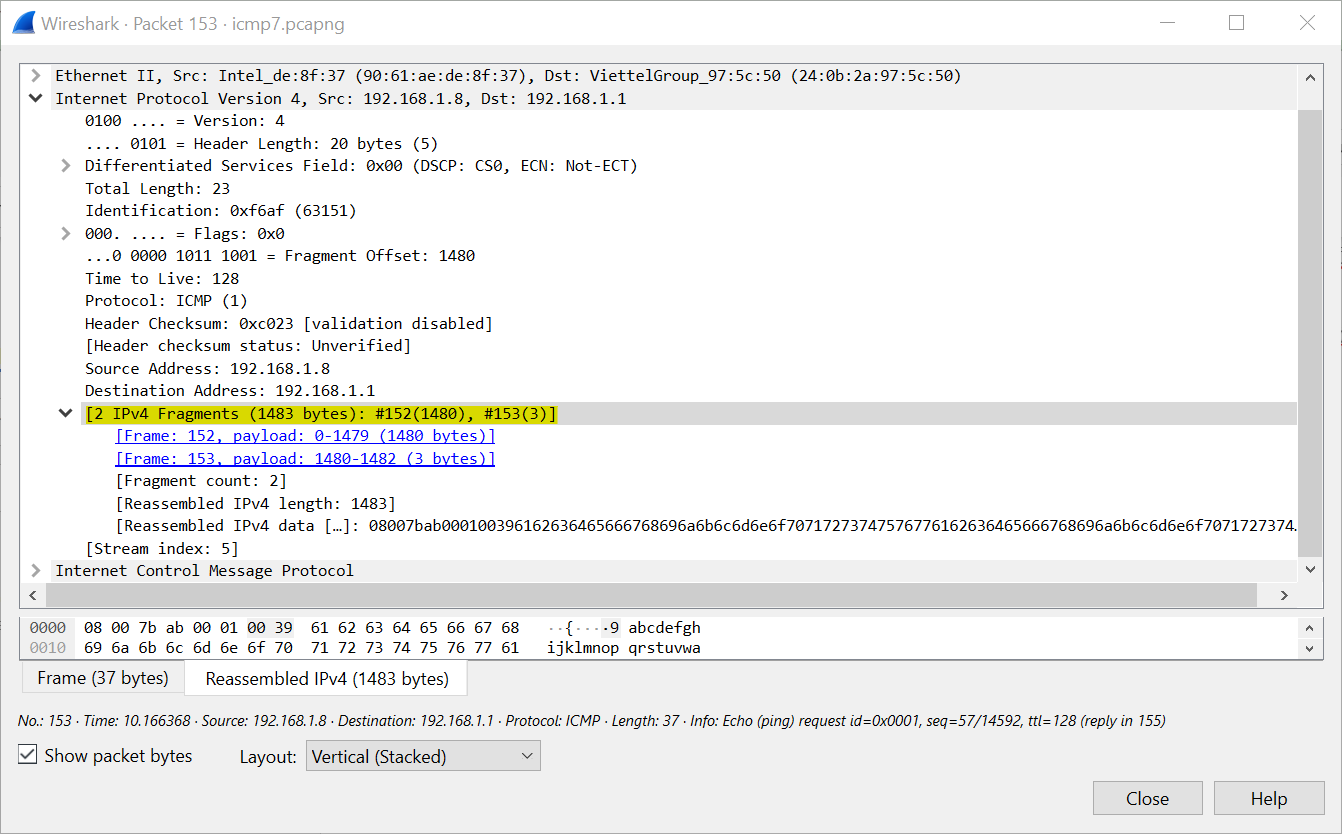


7. "> ping -l 1475 <ip của default gateway>". Vd: ping -l 1475 5 192.168.1.1 và bắt gói tin lưu lại với tên file "icmp7.pcap". Cho biết lượng data trong ICMP (ICMP payload) là bao nhiêu? Gói tin khác gì so với câu 6 bạn đã bắt ở trên và giải thích sự khác nhau đó?

* Dựa vào trường “Data” trong phần tiêu đề ICMP của các gói tin, ta quan sát được ICMP payload là 1475 byte. (lệnh "> ping -l 1475 <ip của default gateway>" sẽ cài đặt ICMP payload thành 1475 byte)

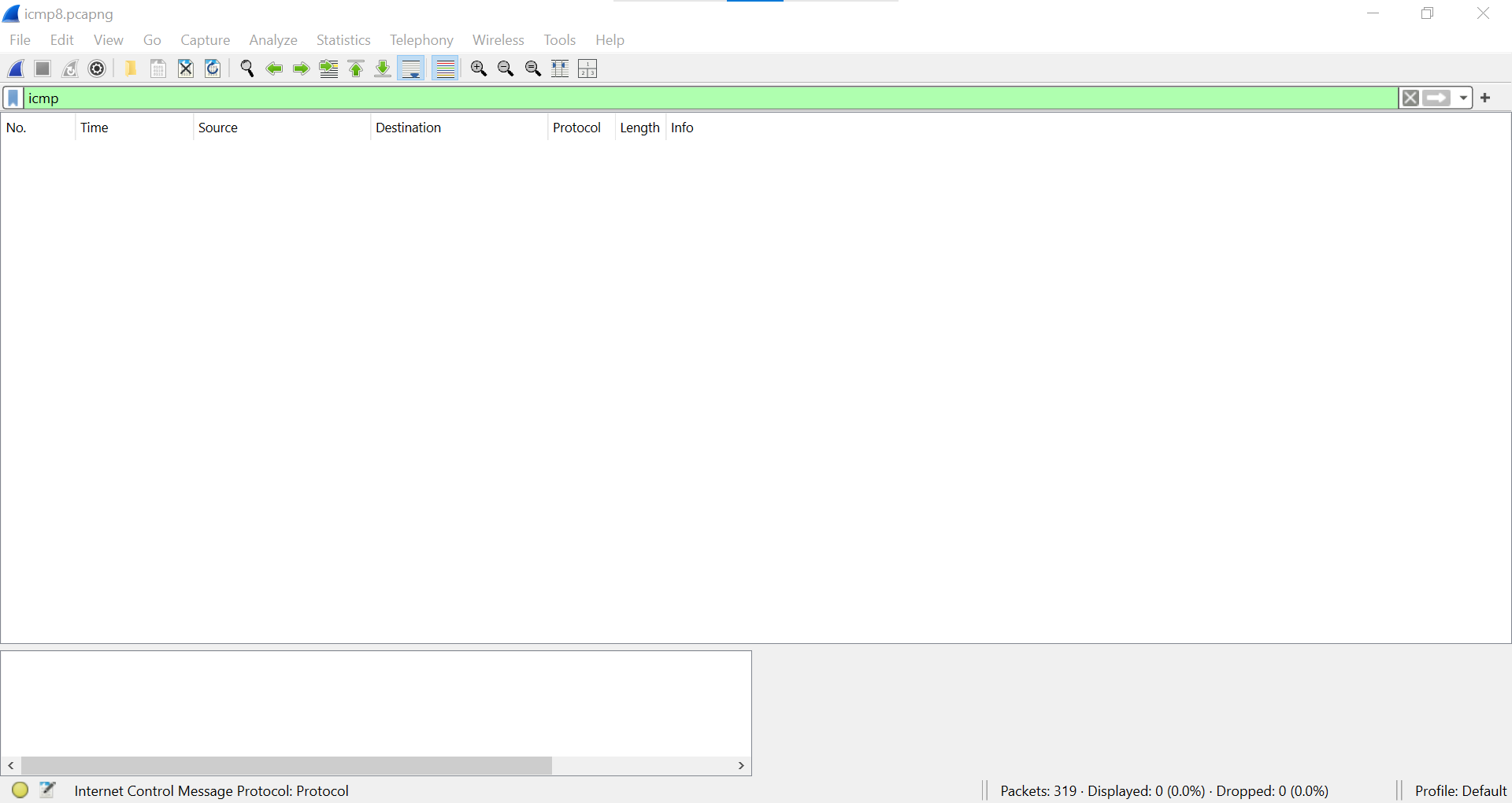


* Quan sát tiêu đề IP của 2 gói tin ICMP Request từ 2 bài 6 và 7, ta nhận thấy sự khác biệt: gói tin ở bài 7 có trường [2 IPv4 Fragments (1483 bytes): #152(1480), #153(3)], trong khi gói tin ở bài 6 không có trường này.
* Điều đó có nghĩa là gói tin ICMP ở bài này đã được phân thành 2 mảnh (fragments).
* Nguyên nhân là do MTU = 1500 byte. Nhưng gói tin ICMP được gửi đi có kích thước = 1475 (payload) + 20 byte (IP Header) + 8 byte (ICMP Header) = 1503 byte > MTU. Nên bắt buộc phải phân mảnh gói tin.



8. "> ping -f -l 1475 <ip của default gateway>". Vd: ping -f -l 1475 5 192.168.1.1 và bắt gói tin lưu lại với tên file "icmp8.pcap". Sau khi bắt gói tin bạn thấy vấn đề gì và giải thích kết quả mà bạn có được?

- Thực hiện ping như trên, gói tin ICMP sẽ không được gửi đi thành công. Lọc các gói tin ICMP trên wireshark không thu được kết quả.



- Tương tự như câu 7, kích thước của gói tin ICMP lúc này vượt quá MTU. Nên buộc phải phân mảnh gói tin để có thể ping thành công. Nhưng lệnh ping lúc này có tham số -f, có nghĩa cờ DF (Don’t Fragment) được bật, buộc gói tin không thể phân mảnh. Dẫn đến gói tin ICMP không thể gửi thành công.