Họ tên: Phạm Tùng Dương

MSSV: 20225825

**Bài 1. Cài đặt các máy tính kết nối với nhau trong mạng**

**Sinh viên tiến hành cài đặt 3 máy tính kết nối với nhau trong một mạng. Sinh viên có thể sử dụng máy ảo (cài VirtualBox) hoặc máy thật. Hệ điều hành sử dụng là Ubuntu. Gọi 3 máy đó là A, B, và C.**

thực hiện:

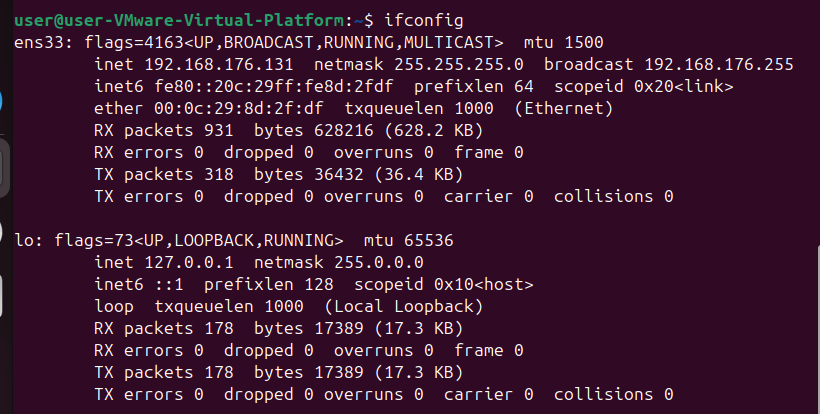
* cài đặt cả 3 máy là máy ảo chạy trên VMware. sử dụng os ubuntu 24.04.3 desktop

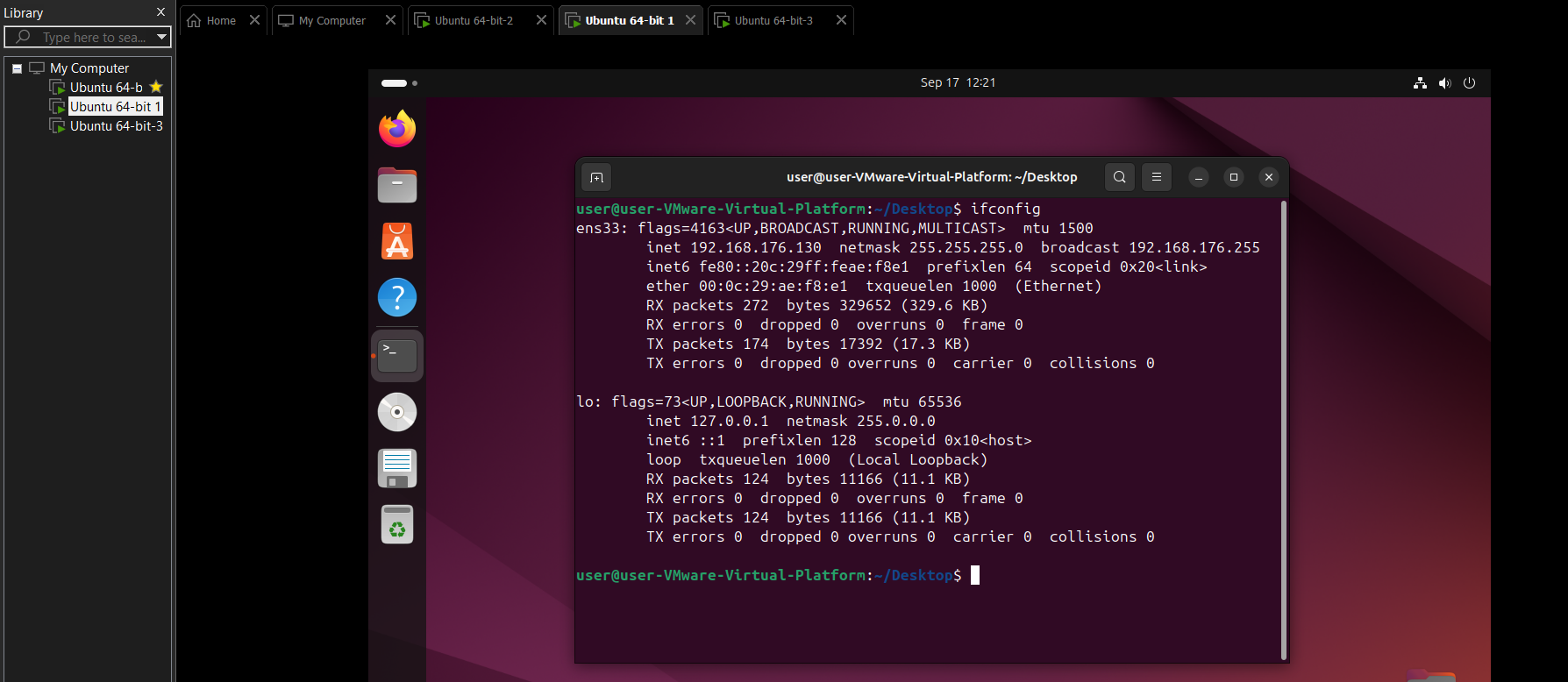
**Bài 2. Cấu hình mạng cho các máy**

**Câu hỏi 1: Trình bày các bước (các lệnh) để thực hiện quá trình cấu hình mạng sao cho các máy nằm trong cùng một mạng đó.**

* setting network cho cả 3 máy là NAT

**Câu hỏi 2: Em thực hiện lệnh nào để biết các máy đã được kết nối trong cùng một mạng?**

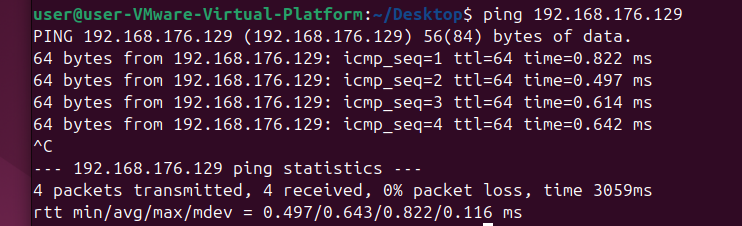
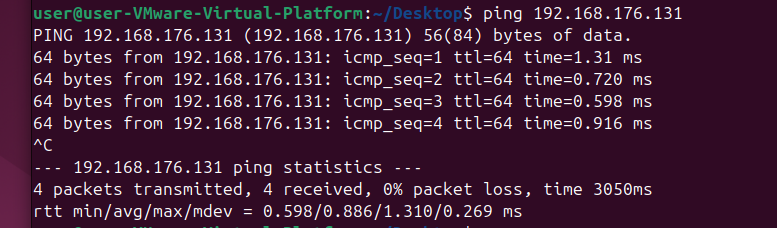
* sử dụng lệnh ifconfig để xem địa chỉ ip của từng máy
* (nếu chưa có ifconfig) thì tải bằng lệnh sudo apt install net-tools
* khi gõ thành công ifconfig 3 máy sẽ hiện như sau:
* máy 3
* máy 2



* máy 1:

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

Nội dung do AI tạo ra có thể không chính xác.

* ping để kiểm tra kết nối giữa các máy:  
  + máy 1 ping 2  
    
  + máy 1 ping máy 3  
  

**Bài 3. Cài đặt wireshark cho máy A. Thử kết nối giữa các máy. Quan sát màn hình**

**wireshark của máy A khi được B và C thực hiện lệnh ping.**

**Thực hiện bắt các gói tin với wireshark:**

**- Ấn vào nút Capture**

**- Lựa chọn giao diện mạng (interface) phù hợp (chú ý: phải chọn đúng giao diện**

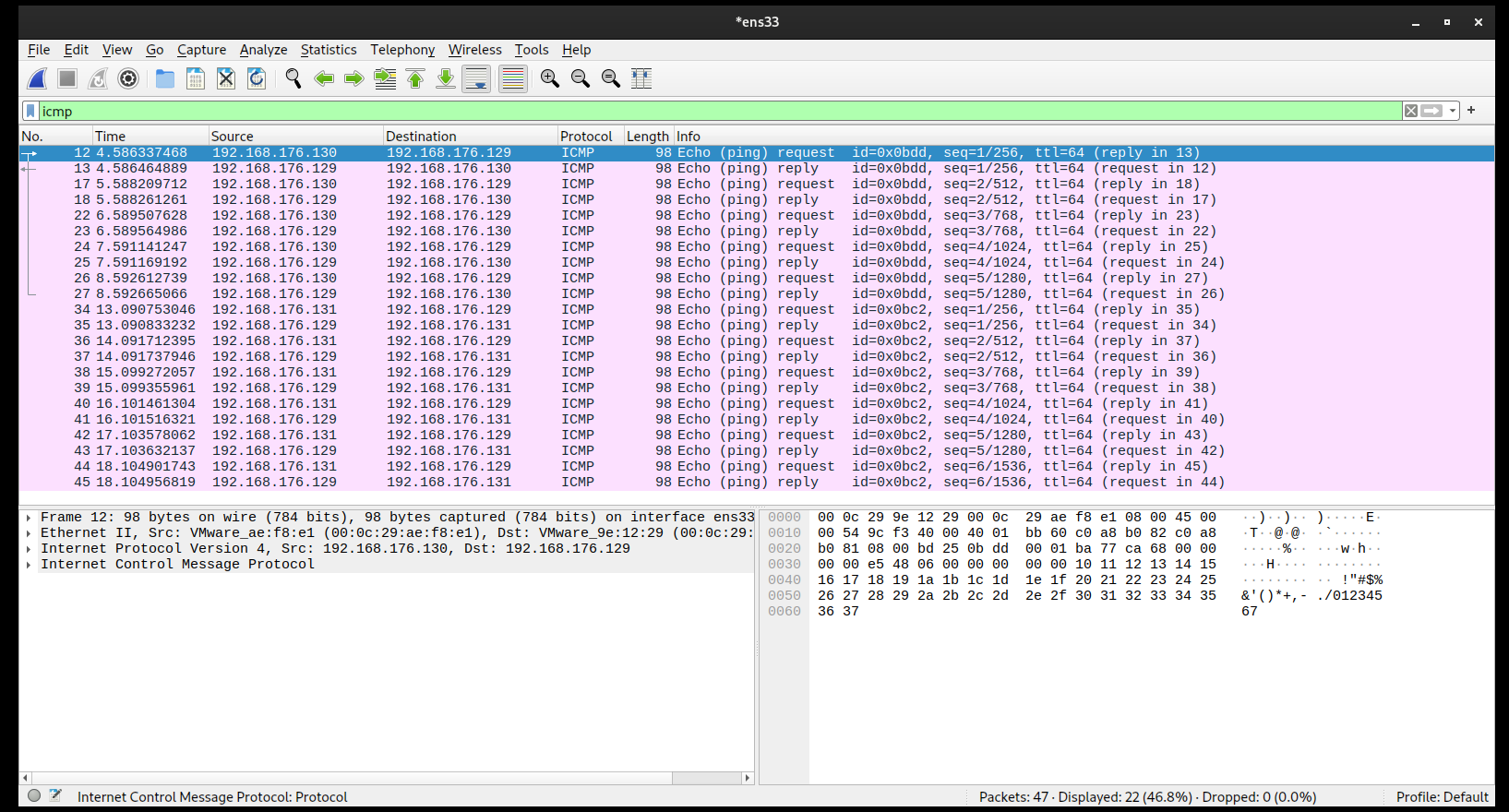
**đang có kết nối giữa các máy)**

**Câu hỏi 3: Thực hiện lệnh ping giữa các máy. Những dòng thông tin nào trên cửa sổ**

**wireshark cho thấy thông tin của lệnh ping đó?**

Trả lời:

* thực hiện cài đặt wireshark trên máy 2 và dùng máy 1 và máy 2 để ping.
* Những dòng thông tin nào trên cửa sổ wireshark cho thấy thông tin của lệnh ping đó là:
* protocol: ICMP
* Info: Echo (ping) request/reply
* source: ip của máy gửi
* destination: ip của máy nhận

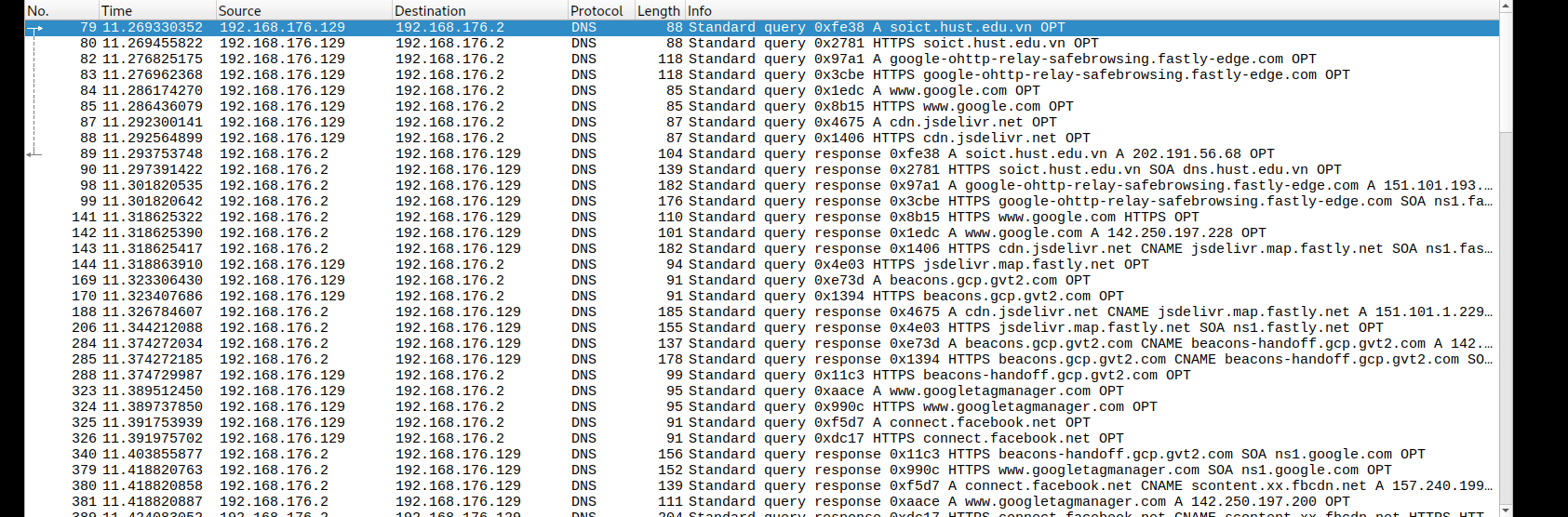


**Câu hỏi 4: Dùng trình duyệt của máy đang chạy wireshark truy cập vào các trang web**

**khác nhau. Những dòng thông tin nào trên cửa sổ wireshark cho thấy thông tin của quá trình duyệt web đó (các gói tin liên quan HTTP/HTTPS traffic).**

trả lời:

* ta có thấy các gói tin của trong web đó bằng các thông tin như:
* tên miền trang web. vd: [soict.hust.edu.vn](http://soict.hust.edu.vn)
* ip ở source hoặc destination
* giao thức http/https
* các phương thức như Get Post



**Thực hiện phân tích các luồng dữ liệu TCP và UDP với wireshark:**

**- Đối với UDP:**

**o Ở máy server, sử dụng công cụ netcat để chạy lệnh: nc -u -l 9999**

**o Ở máy client: echo "Test UDP traffic" | nc -u 127.0.0.1 9999**

**o Sau khi chạy được một lúc, dừng wireshark lại và nhập “udp” vào thanh**

**filter để lọc ra các thông điệp UDP**

**Ở bảng giữa sẽ có các thông tin chi tiết về cấu trúc gói:**

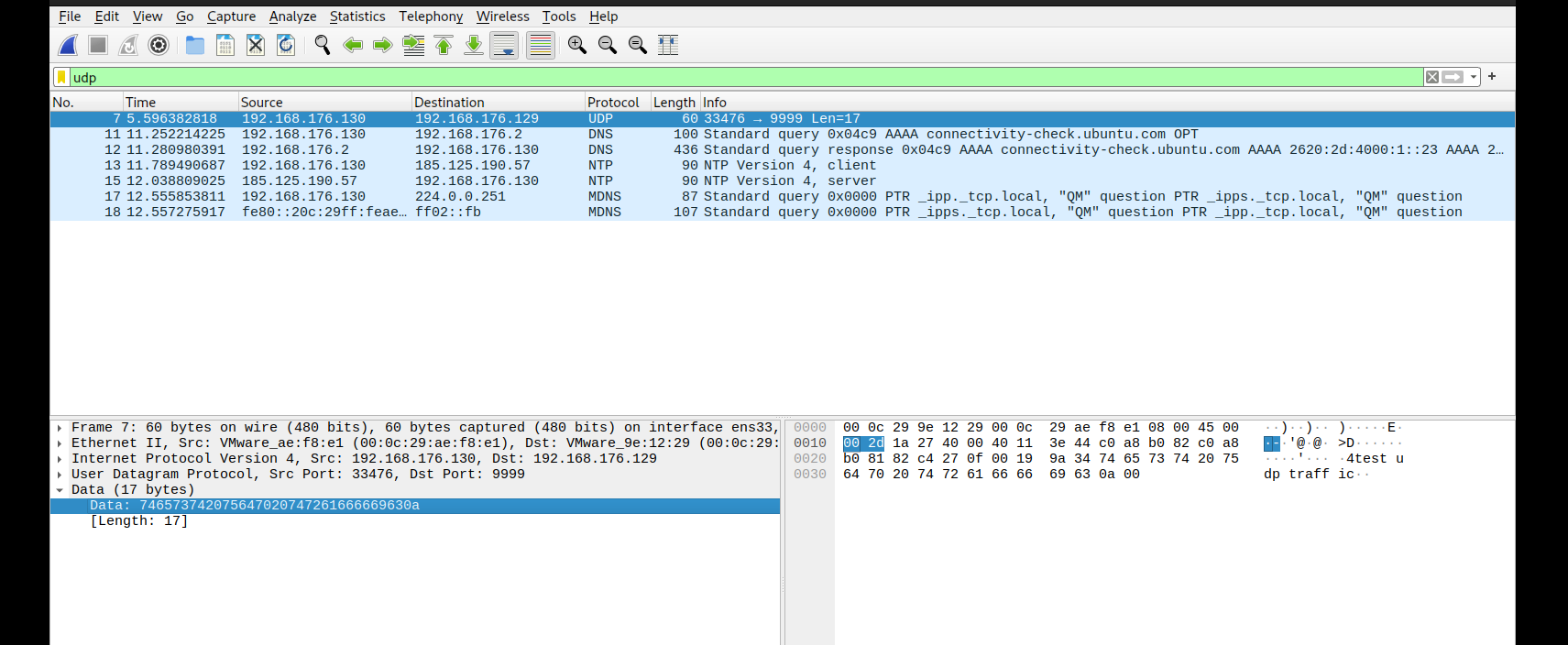
**- Frame: Thông tin chung về gói (kích thước, thời gian, v.v.).**

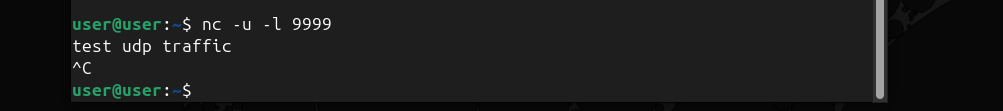
**- Ethernet: Địa chỉ MAC nguồn và đích.**

**- IP: Địa chỉ IP nguồn và đích.**

**- UDP: Cổng nguồn và đích, độ dài và checksum.**

Trả lời:





* t có thể thấy khi máy chủ mở cổng 9999 và nhận được thông điệp cho máy khách gửi

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

Nội dung do AI tạo ra có thể không chính xác.

**Câu hỏi 5: Quan sát UDP packet trên wireshark, phân tích về tính đơn giản của UDP. Gợi ý: không có kết nối, do đó không có cờ (flags) để thiết lập hoặc hủy kết nối.**

trả lời:

Phân tích khi quan sát wireshark:

* ta có thể thấy chỉ có một gói UDP đơn lẻ được gửi đi, từ đó suy ra UDP không có các cơ chế phức tạp như là thiết lập, hủy kết nối hay kiểm tra kết nối như TCP
* cũng không có flags để quản lý trạng thái
* vì vậy UDP được coi là không đáng tin cậy vì không thể phát hiện gói tin khi bị mất và không gửi lại gói tin

**- Đối với TCP:**

**o Ở máy server, sử dụng công cụ netcat để chạy lệnh: nc -l 8888**

**o Ở máy client: echo "Test TCP traffic" | nc 127.0.0.1 8888**

**o Sau khi chạy được một lúc, dừng wireshark lại và nhập “tcp” vào thanh filter để lọc ra các thông điệp TCP**

**Quan sát thông tin 1 TCP packet, chúng ta sẽ thấy các thông tin sau:**

**Frame: Chi tiết chung về gói tin.**

**Ethernet: Địa chỉ MAC.**

**IP: Thông tin địa chỉ IP**.

**Câu hỏi 6: Ấn vào trường thông tin TCP, quan sát sẽ thấy nhiều trường hơn so với UDP.**

**Đó là những trường nào? Ý nghĩa của từng trường là gì?**

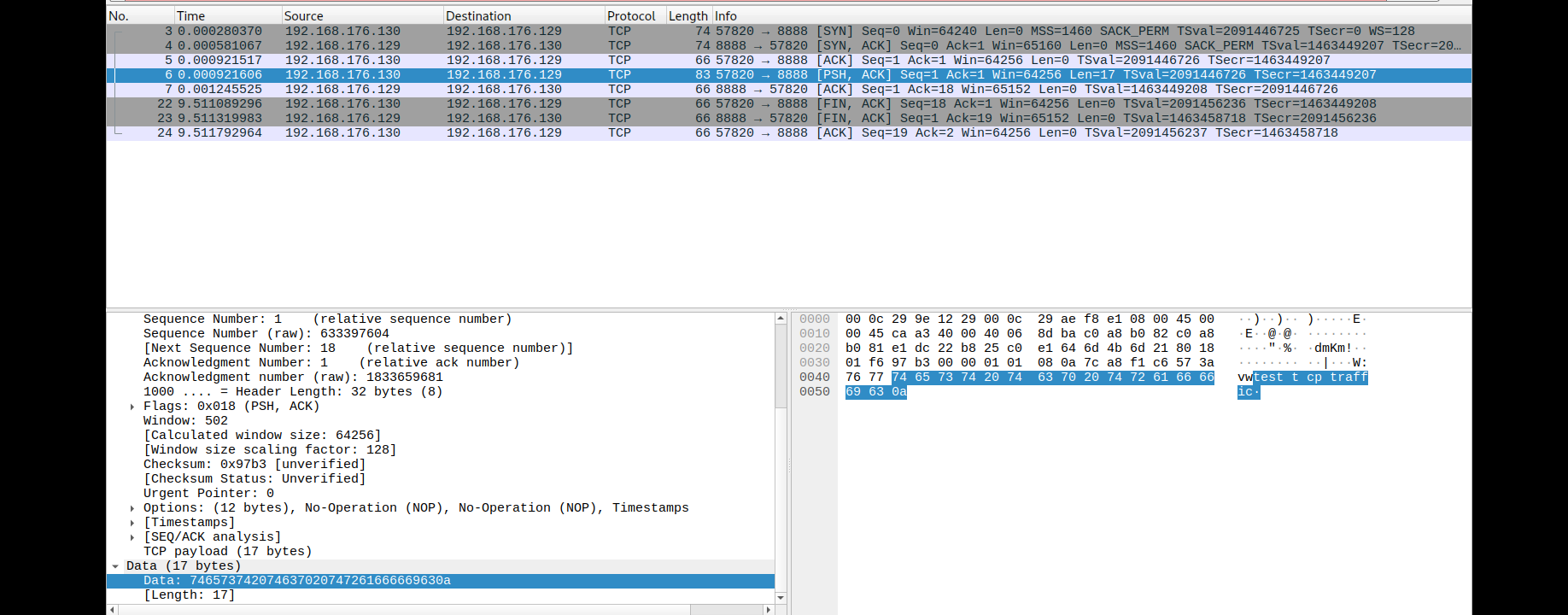
Trả lời:

* khi quan sát gói TCP ta có thế thấy sự khác biệt so với UDP như sau:

+flags: [SYN], [SYN,ACK], [ACK] dùng để kiểm tra kết nối và luồng của các tệp tin

+ ack là số xác nhận, dùng để báo cho bên gửi biết là dữ liệu đã được chuyền đến đâu. vd gói đầu có ack = 1, sau khi nhận được một gói có ack = 1 và len = 17 thì gói tiếp theo có ack = 18

+ seq là số thứ tự của byte dữ liệu trong luồng



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

Nội dung do AI tạo ra có thể không chính xác.



Câu 7:

Dùng nslookup

Dòng adddress sẽ hiển thị địa chỉ IP

Câu 8:Lí do

* DNS load balancing / round-robin: tên miền có nhiều A records; resolver trả về lần lượt các IP.
* CDN (Content Delivery Network): DNS trả IP của edge server khác nhau tùy vị trí/geo/latency/health.
* Caching / TTL: các resolver trung gian cache khác nhau; khi TTL thay đổi, bạn có thể nhận IP khác.
* DNS-based failover / health checks: nếu một server down, DNS trả IP khác.
* Sử dụng nhiều DNS resolver (ISP, public DNS): mỗi resolver có cache khác nhau.
* Anycast: IP giống nhưng route tới node khác — kết quả “khác” về mặt traceroute nhưng IP giống.

Câu 9: Ý nghĩa từng cột

Cột 1: số hop.

Cột 2: hostname/IP.

3 cột ms: RTT cho 3 probe.

Câu 10:khác biệt

Số hop nhiều hơn: đi qua ISP và nhiều router trung gian → số hop lớn hơn so với LAN (thường 1–2 hop).

Thời gian (latency) lớn hơn: RTT cao hơn, biến thiên lớn hơn.

Firewall / ICMP filtering: nhiều router trên Internet chặn trả ICMP Time Exceeded hoặc chặn probe