**BÁO CÁO THỰC HÀNH TUẦN 1**

**MÔN: THỰC HÀNH LẬP TRÌNH MẠNG**

**Sinh viên: Đinh Huy Dương**

**MSSV: 20215020**

**Bài 1-2:**

Câu hỏi 1:

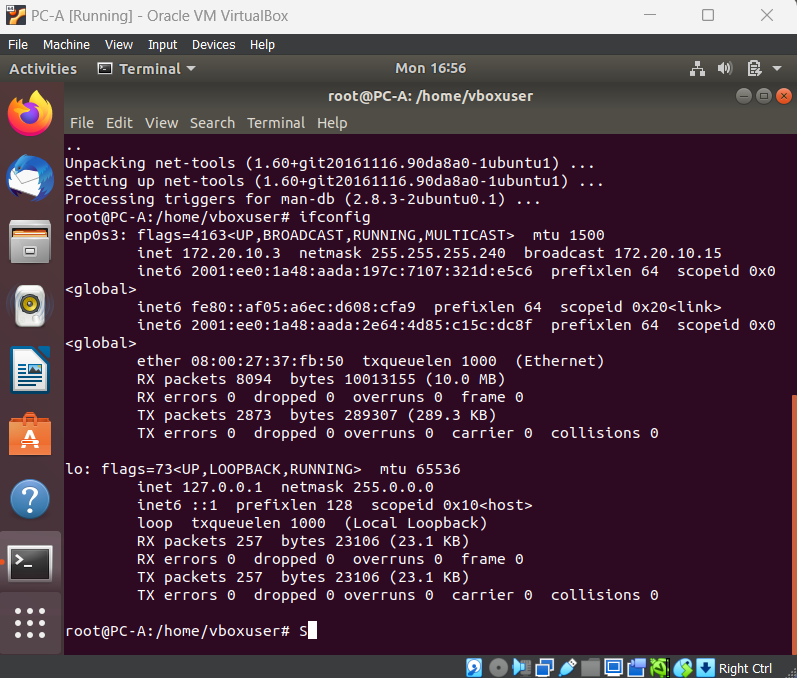
Cấu hình 3 máy ảo sử dụng Bridge Adapter cho chung với Adapter của máy thật A computer screen shot of a network

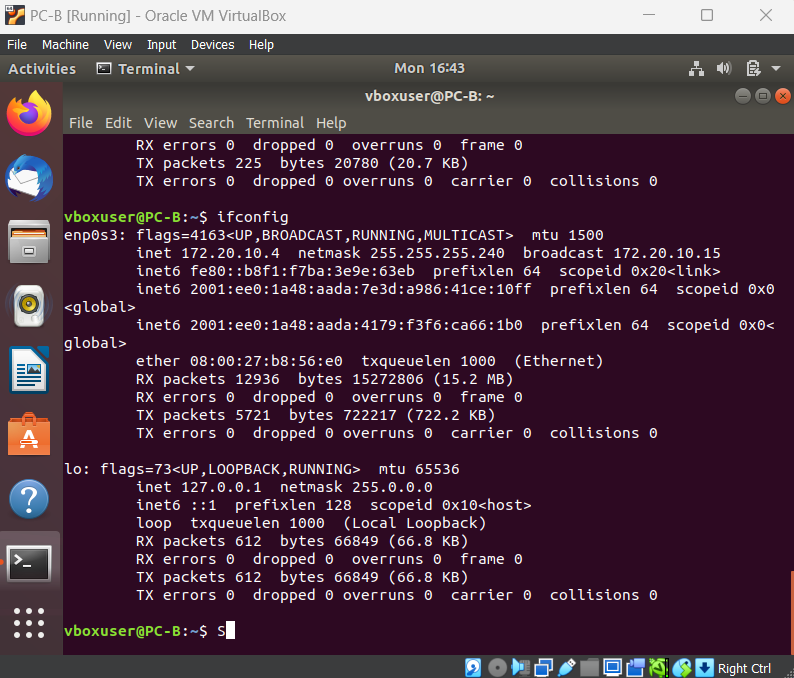
Description automatically generated

Như này các máy ảo sẽ sử dụng chung cùng một mạng

Kết quả chạy lệnh “ifconfig” của 3 máy

Máy A:



Máy B:

Máy C:

A screenshot of a computer

Description automatically generated

Ta kết nối 3 máy tính A, B, C cùng một mạng.

Câu hỏi 2:

Cụ thể:

* Máy A có địa chỉ IPv4: 172.20.10.3, mặt nạ 255.255.255.240
* Máy B có địa chỉ IPv4: 172.20.10.4, mặt nạ 255.255.255.240
* Máy C có địa chỉ IPv4: 172.20.10.2, mặt nạ 255.255.255.240

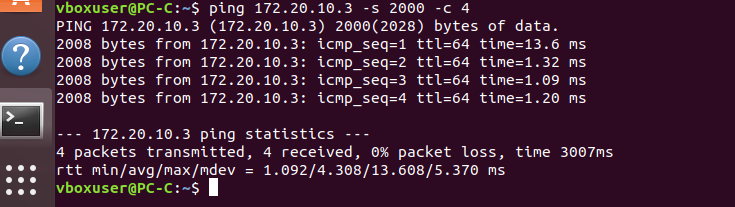
Dễ dạng nhận ra, mặt nạ mạng của 3 mạng này chuyển sang dạng nhị phân có 24 số 1, tương ứng với số lượng bit của NetworkID là 24 bit.

Sử dụng phép AND của 3 địa chỉ IP qua mặt nạ sẽ cho ra được 24 bit đầu giống nhau, và cho ra địa chỉ mạng chung của 3 mạng này: 172.20.10.0

**Bài 3:**

Thực hiện lệnh ping lần lượt từ máy C, B đến máy A có địa chỉ IP: 172.20.10.3

Máy C:



Máy B:

A computer screen with white text

Description automatically generated

Câu hỏi 3: Wireshark của máy A trên Network Interface enp0s3:A screenshot of a computer

Description automatically generated A screenshot of a computer

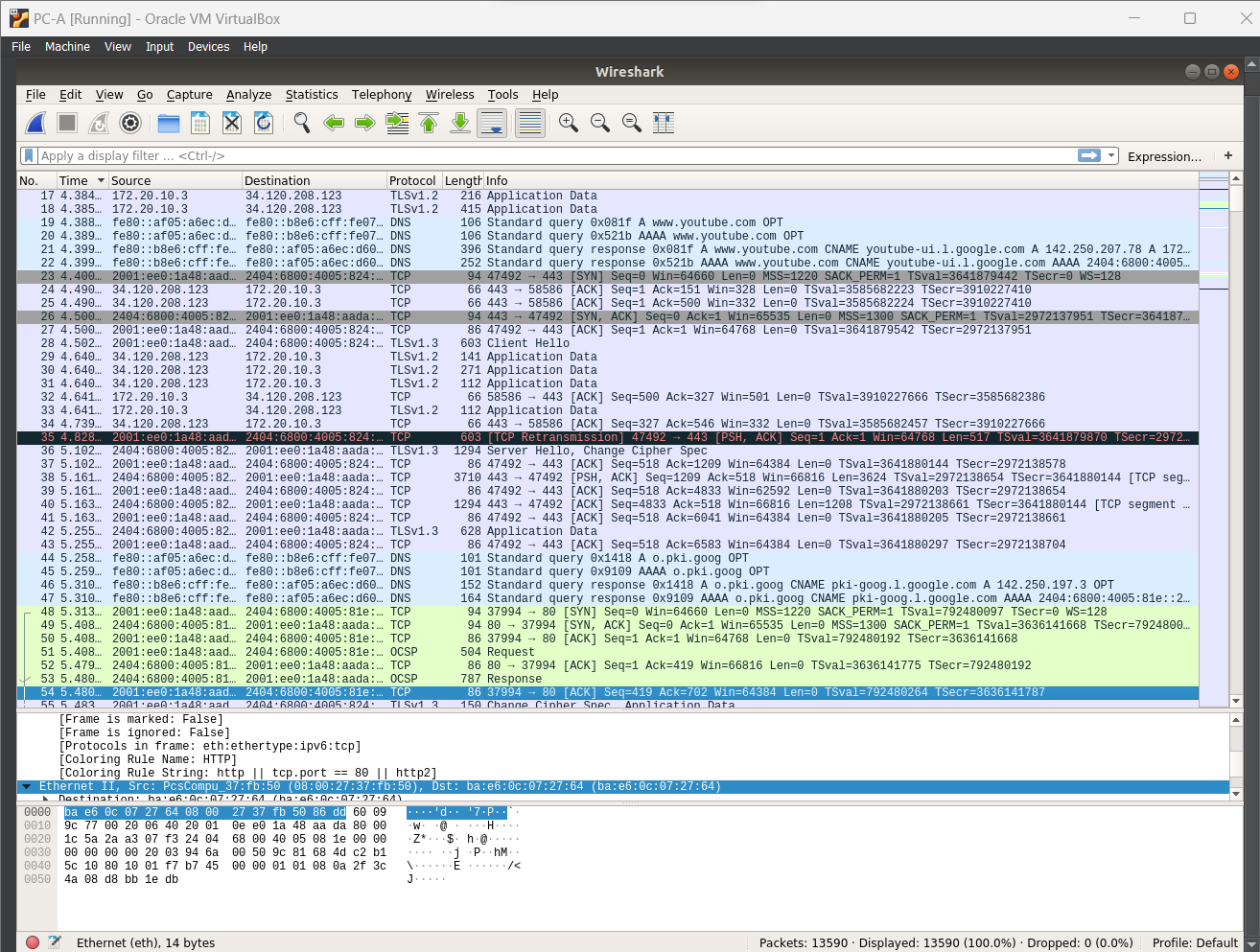
Description automatically generated

Ta có thể thấy các máy C (172.20.10.2) đã ping đến máy A (172.20.10.3) trước, sau đó máy B (172.20.10.4) ping đến thành công

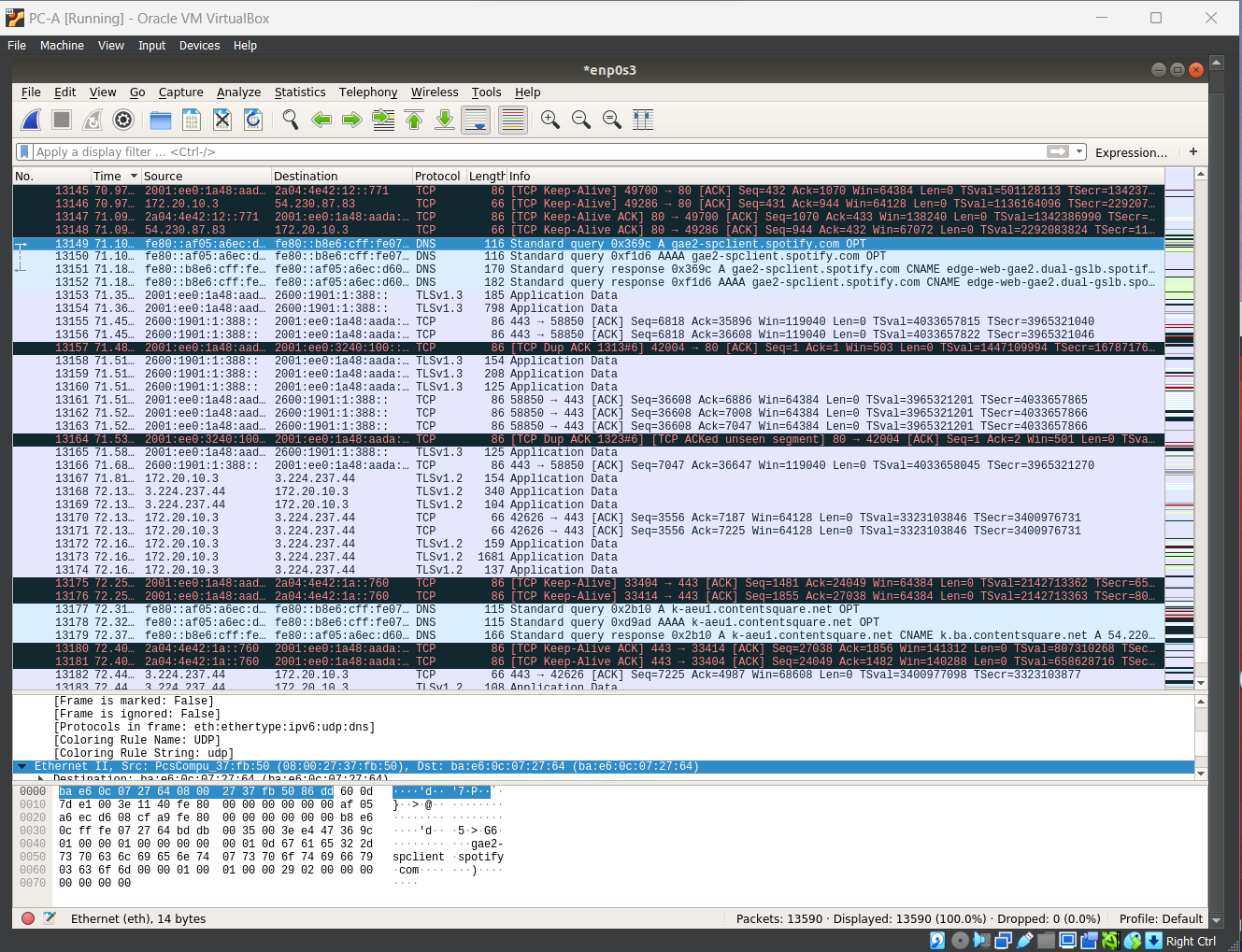
Những dòng có chứa địa chỉ đích (Destination) và nguồn (Source) là các địa chỉ của các máy thể hiện lệnh ping

Câu hỏi 4:

* Tại máy A, ta truy cập vào trang web youtube.com và spotify.com. Kết quả hiện ra ở wireshark và các dòng có gói tin của HTTP:

youtube.com, từ dòng 19:  


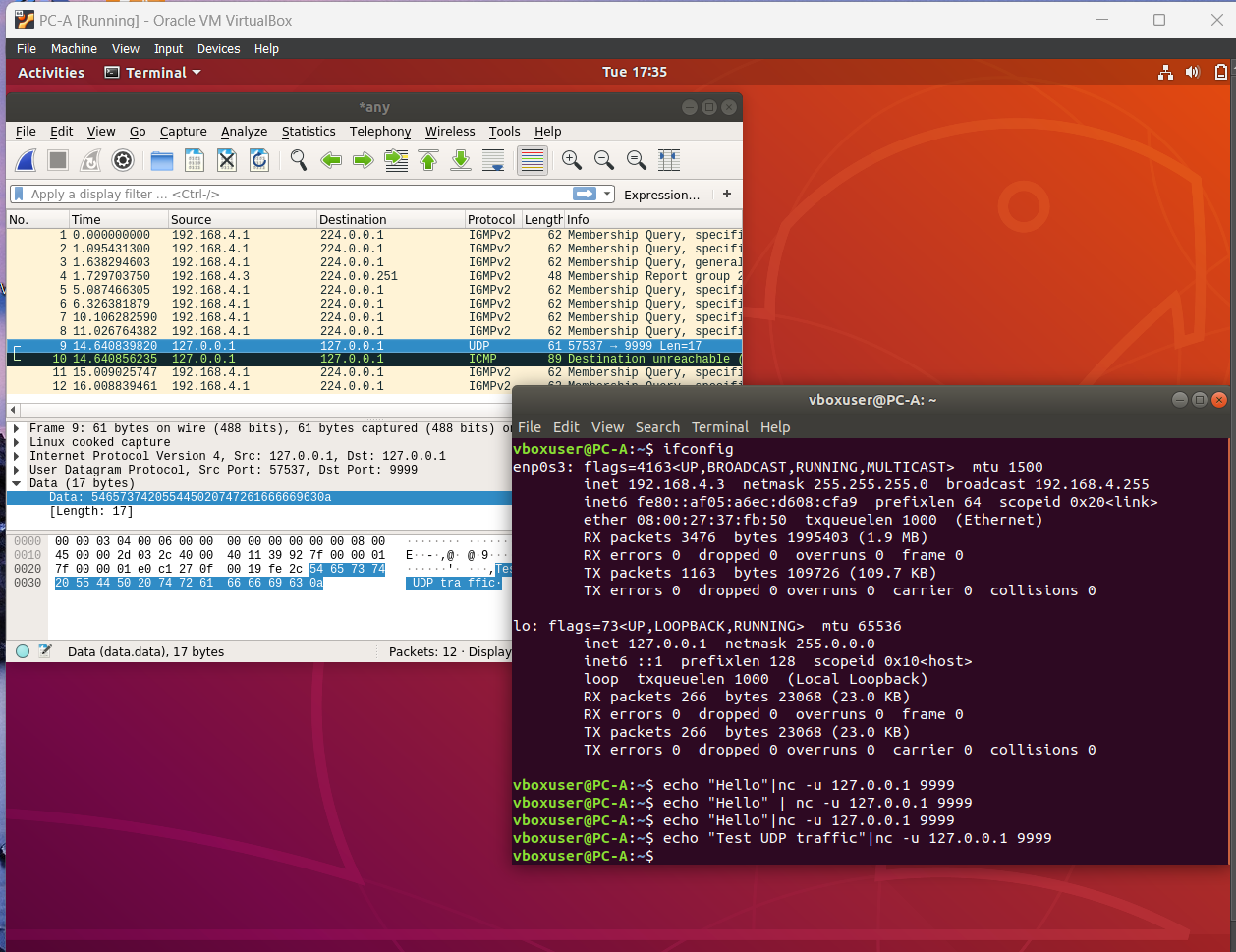
spotify.com: Bắt đầu từ dòng 13149



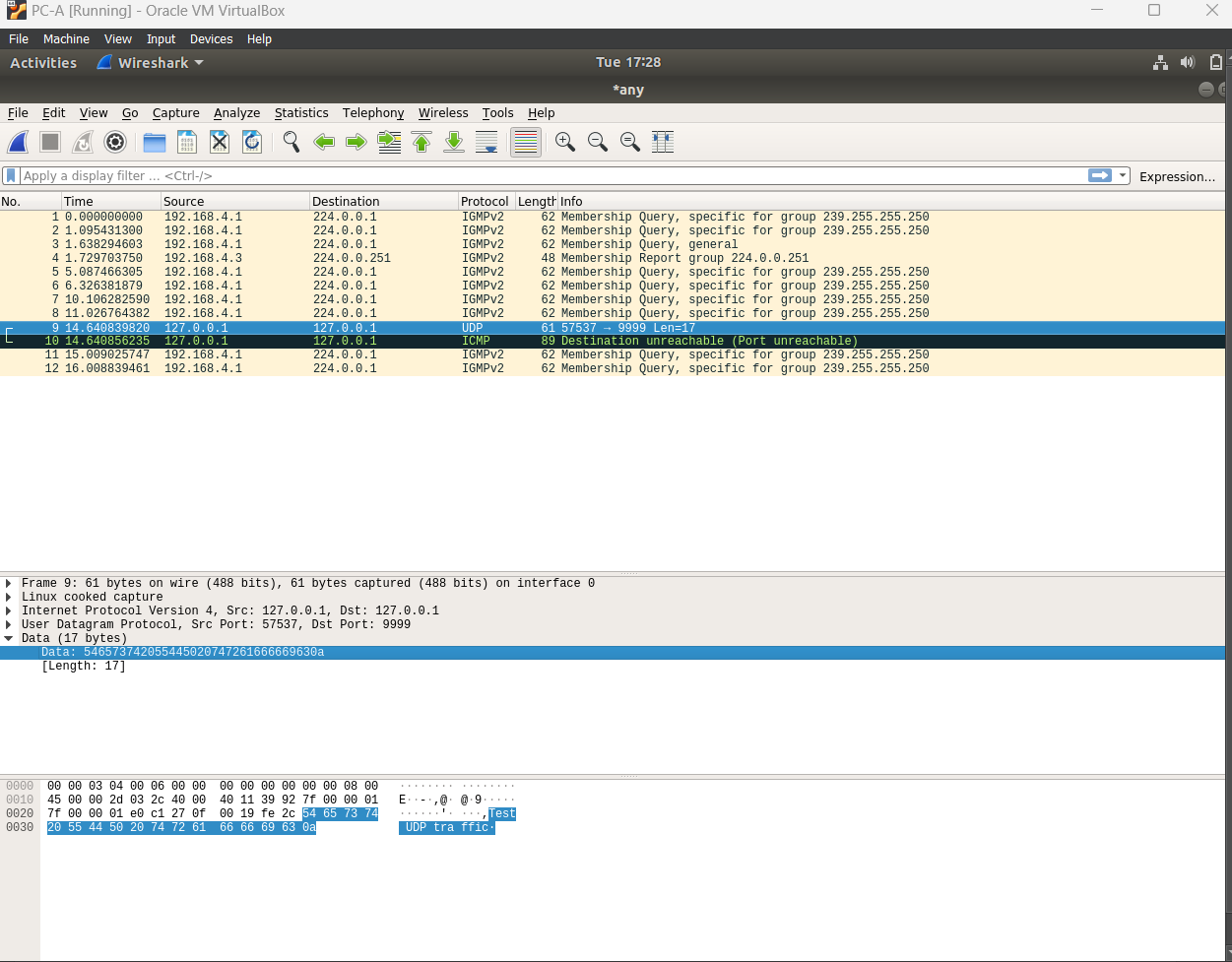
Câu hỏi 5:

Phân tích luồng dữ liệu TCP và UDP

Ta thực hiện trên máy A, giờ có địa chỉ IP 192.168.4.3:

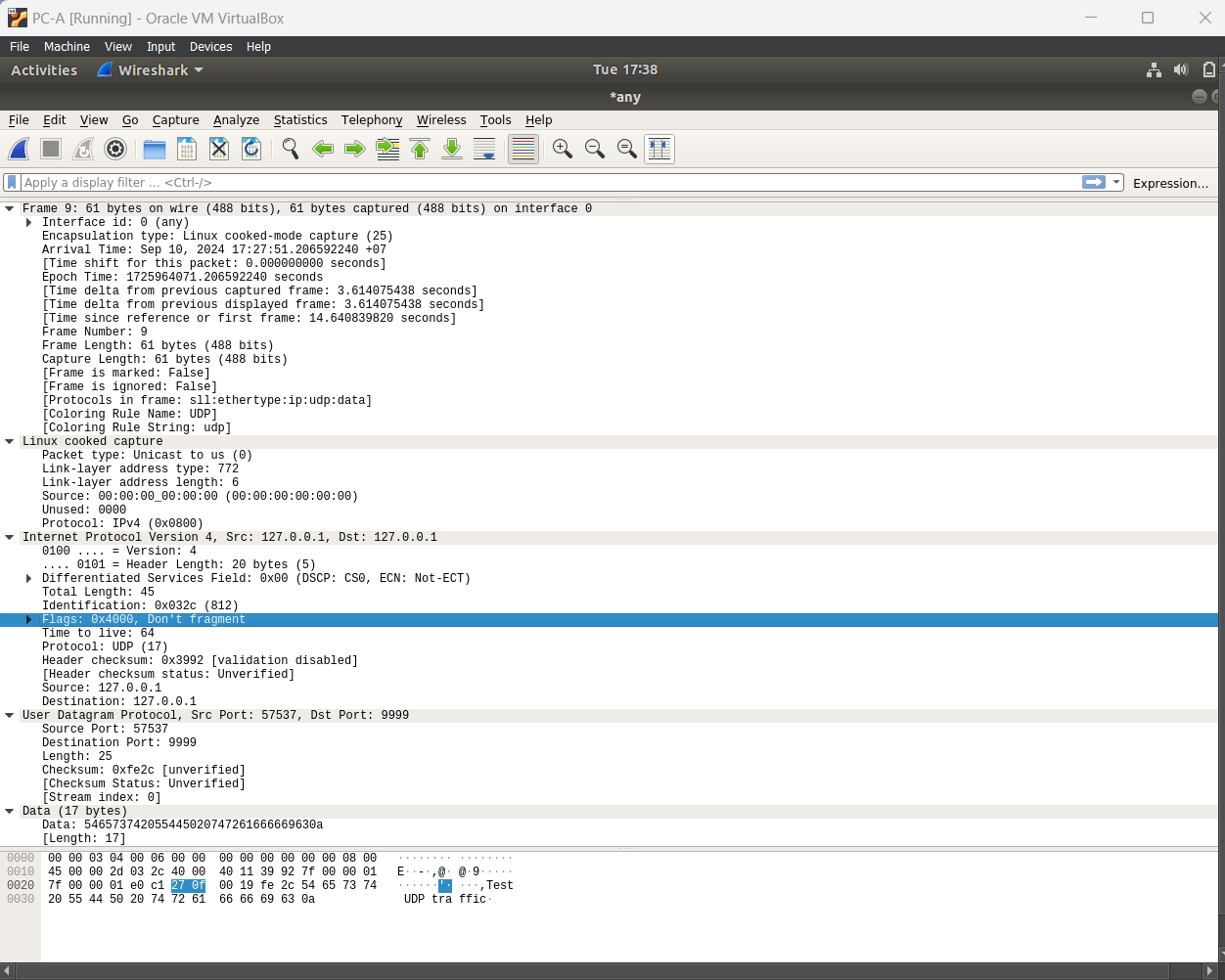


* UDP:



Thực hiện lệnh netcat trên máy A tới địa chỉ loopback 127.0.0.1 để bắt được gói tin UDP, nhìn ở bảng cuối ta có thể thấy thông điệp được echo “Test UDP traffic”

Chi tiết:



Dễ dàng nhận thấy do UDP được thiết kế theo hướng không kết nối, nên trong cấu trúc của một gói tin chỉ có các thông tin cơ bản như địa chỉ đích, nguồn, payload, checksum, độ dài; mà không cần các flag để thiết lập hoặc đóng liên kết hay điều khiển luồng.

-TCP:

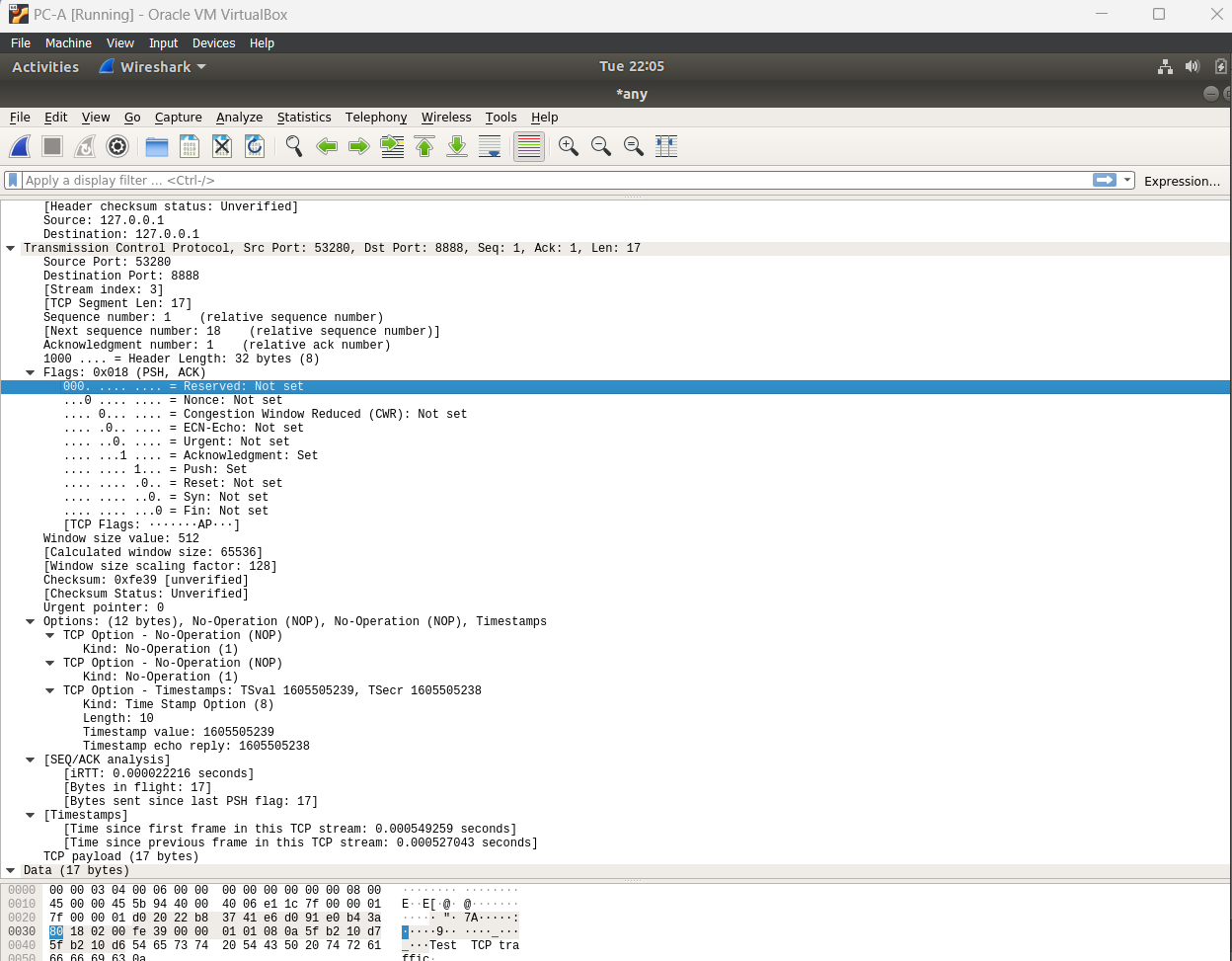


A screenshot of a computer

Description automatically generated

Ở bảng dưới tại dòng có cờ PSH, ACK ta đã thấy được thông điệp ta echo “Test TCP traffic”

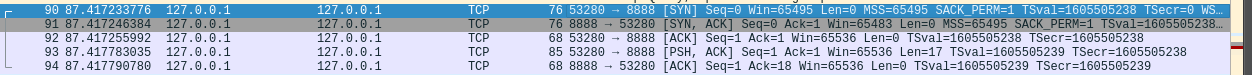
Câu hỏi 6:

* Một số trường được mở rộng so với gói tin UDP: 
  + Sequence Number: Đảm bảo thứ tự của gói tin
  + Ack Number: Đảm bảo dữ liệu được nhận đầy đủ
  + Offset (Header length): Báo hiệu nơi bắt đầu của payload trong packet
  + Flag: Điều khiển trạng thái kết nối, đây đảm bảo tính tin cậy của TCP
  + Window size: Chỉ rõ cửa sổ thông tin người nhận để kiểm soát luồng gửi
  + Urgent pointer: Trỏ đến cờ Urgent để tín hiệu khẩn
  + Option: Tính năng phụ

Các trường này đảm bảo TCP tin cậy và là một giao thức so với UDP (không tin cậy, không kết nối)

Câu hỏi 7: Bắt tay 3 bước

* SYN: Client đưa cho Server số hiệu Seq của mình và cho Server đồng bộ (Synchronize)
* SYN/ACK: Server chấp nhận số Seq của client và đưa cho Client số Seq của mình (Ack Server mới = Seq Client + 1)
* ACK: Client chấp nhận số Seq của Server (Ack Client mới = Seq Client cũ + Seq Client cũ, Seq Client mới = Seq Client cũ +1)



Giao thức đảm bảo độ tin cậy, độ chính xác (Đúng thứ tự) và liên kết có kết nối của TCP

**Bài 4:**

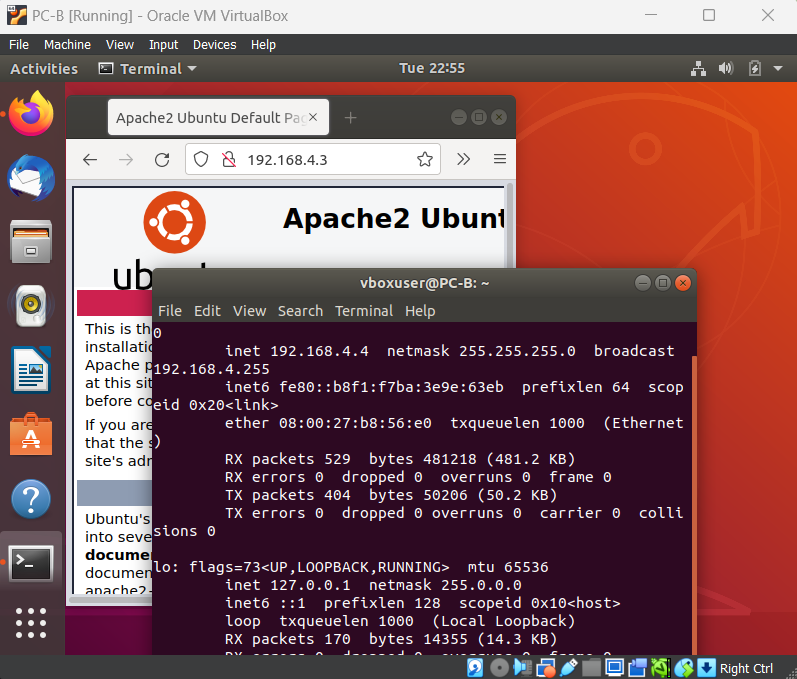
Câu hỏi 8:

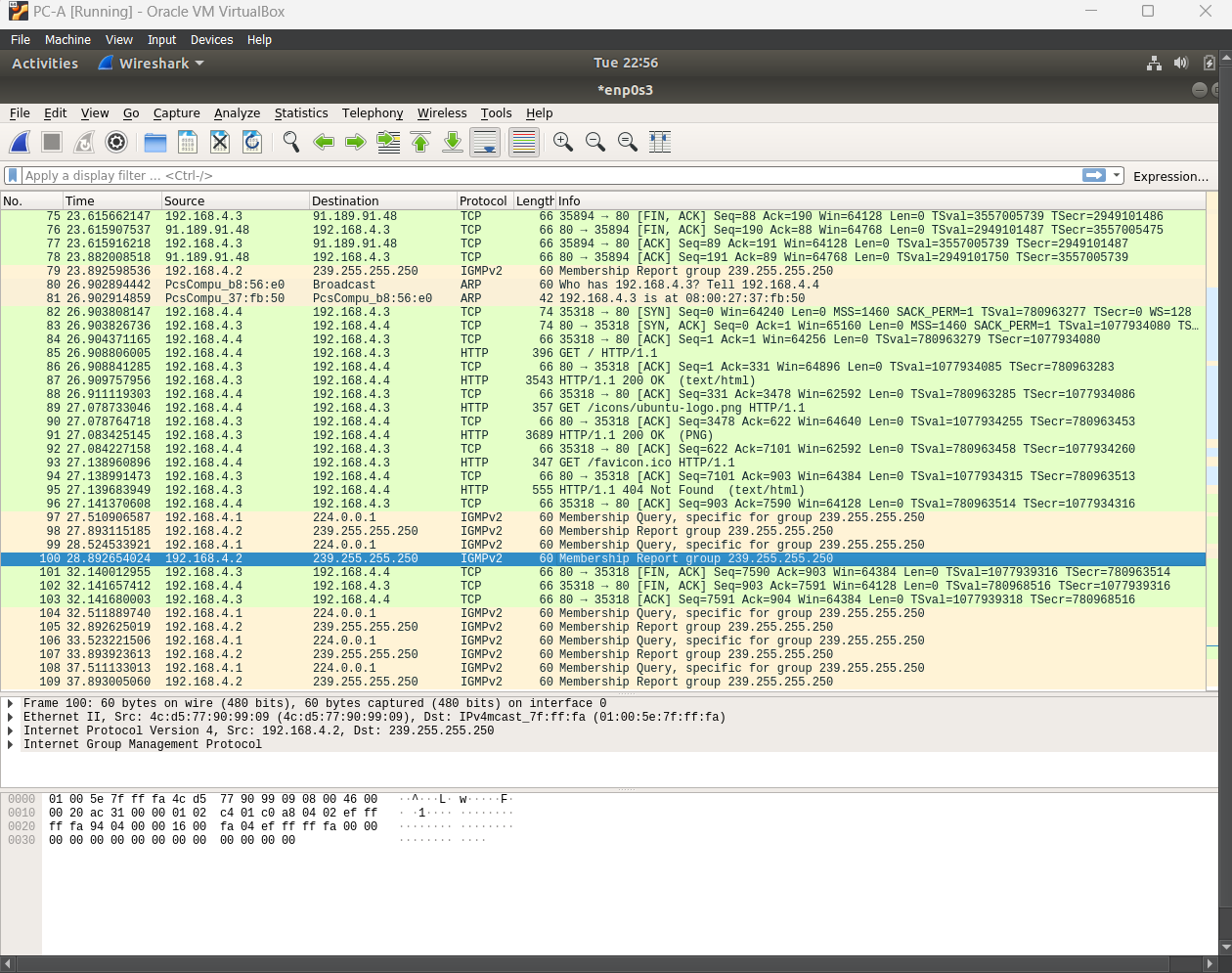
Máy A được cài đặt Apache webserver trên, có địa chỉ 192.168.4.3

A screenshot of a computer

Description automatically generated

Máy B truy cập vào trang web, có địa chỉ 192.168.4.4:



Kết quả hiển thị trên Wireshark:  


Từ dòng 82 ta có thể thấy máy B gửi gói tin TCP đến máy A để thiết lập bắt tay 3 bước