BÀI TẬP THỰC HÀNH WIRESHARK

MSSV : **18120113** Lớp : **18CTT1**
Họ và Tên : **Nguyễn Chánh Đại**

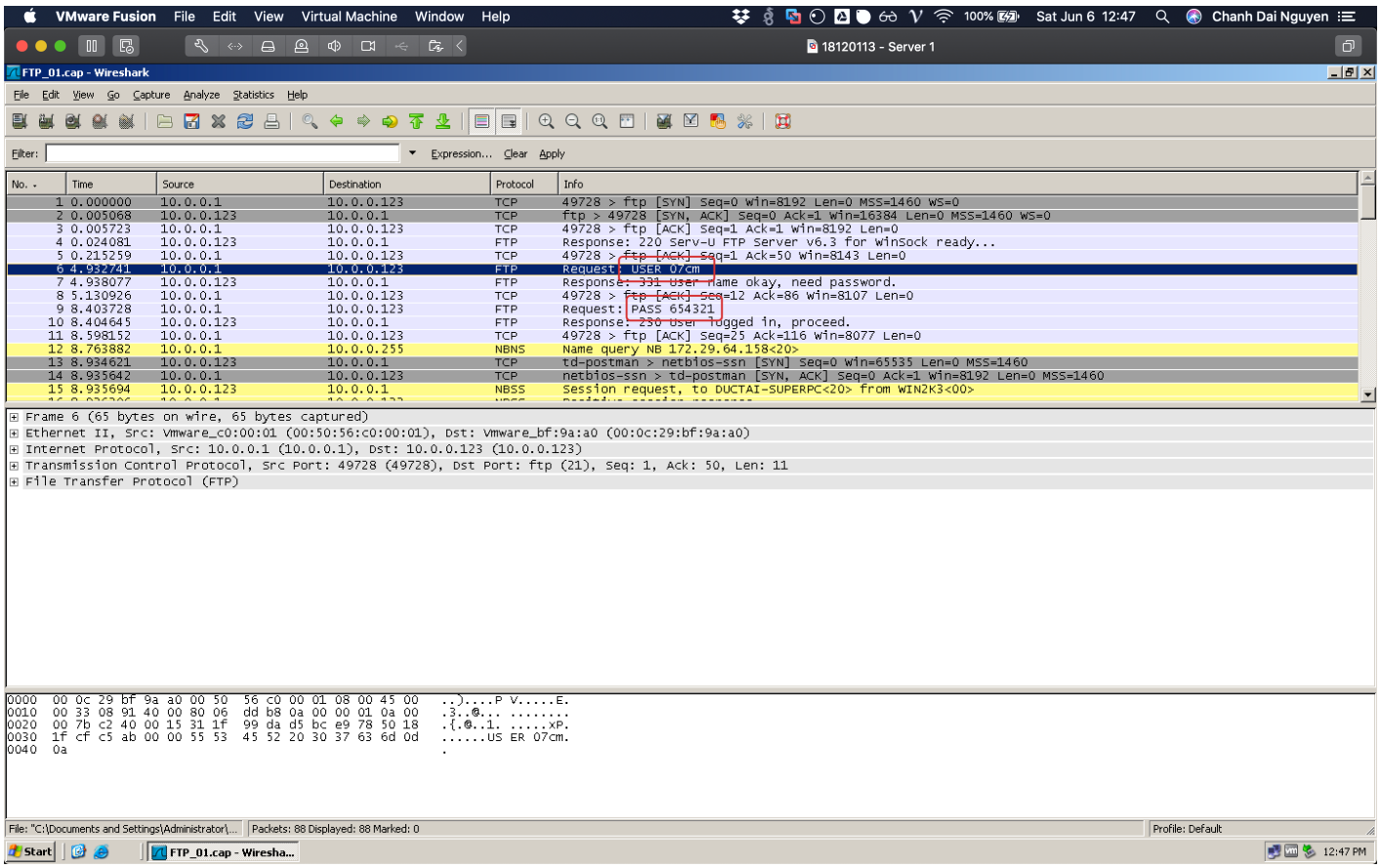
Lưu ý :

- Bài tập cá nhân.
- Sinh viên làm bài trên đề bài sau.
- Cần chụp hình và ghi chú rõ ràng cho các câu trả lời.
- Nộp bài với file **MSSV_BTTH02.zip**, bao gồm file báo cáo **MSSV_BTTH02.pdf** và các files lưu thông tin các gói tin được bắt bởi Wireshark **MSSV_DHCP.pcap** (Câu 3), **MSSV_ICMP.pcap** (Câu 4).
- Các bài làm giống nhau sẽ nhận điểm 0.
- Chỉ nhận bài tập tại phần nộp bài của Website môn học, không nhận bài theo hình thức khác.

Câu 1. Cho tập tin FTP_01.cap, đọc tập tin này bằng Wireshark và trả lời các câu hỏi sau :

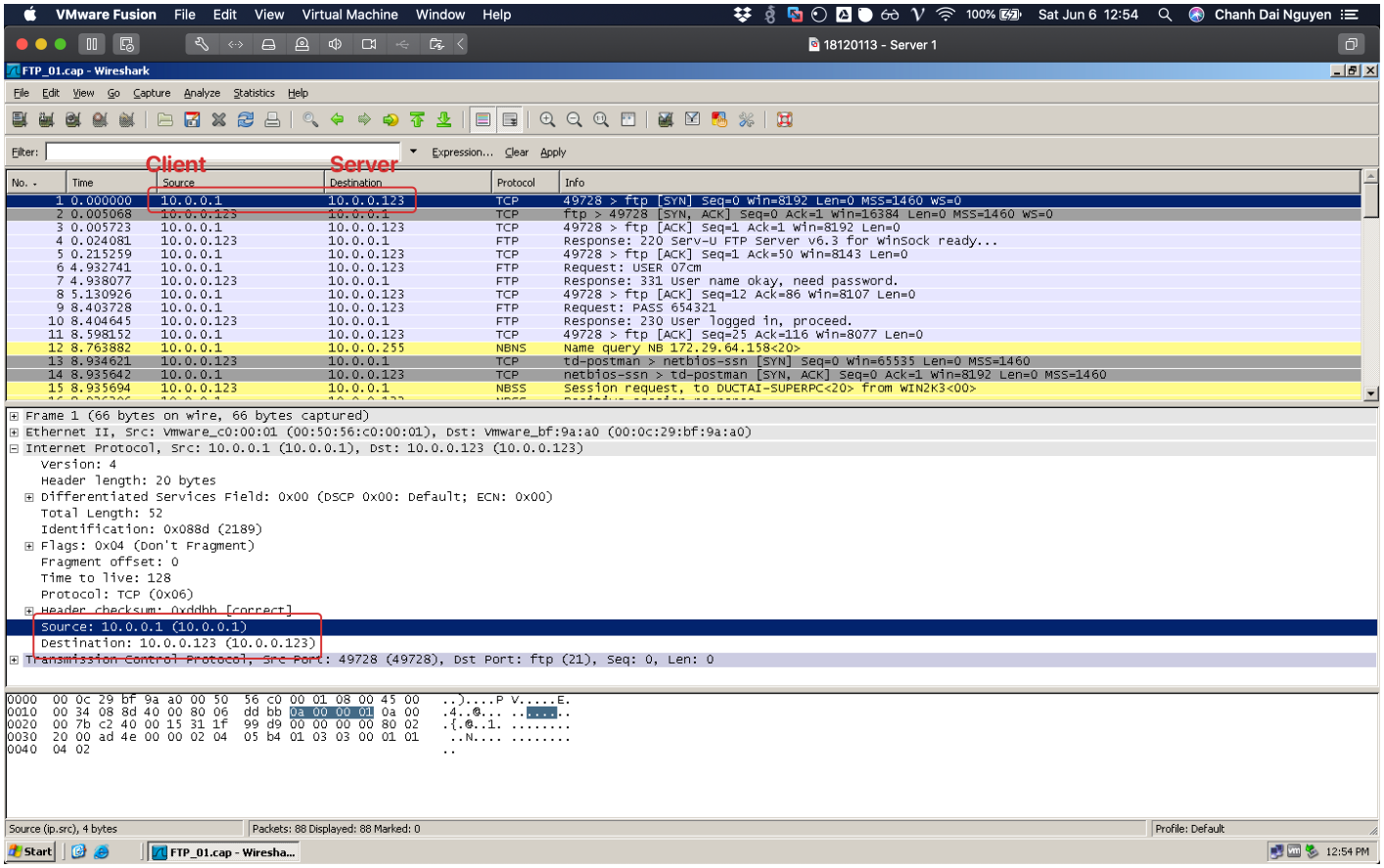
1 a. Username và Password của người dùng là gì ?

Username	Password
07cm	654321



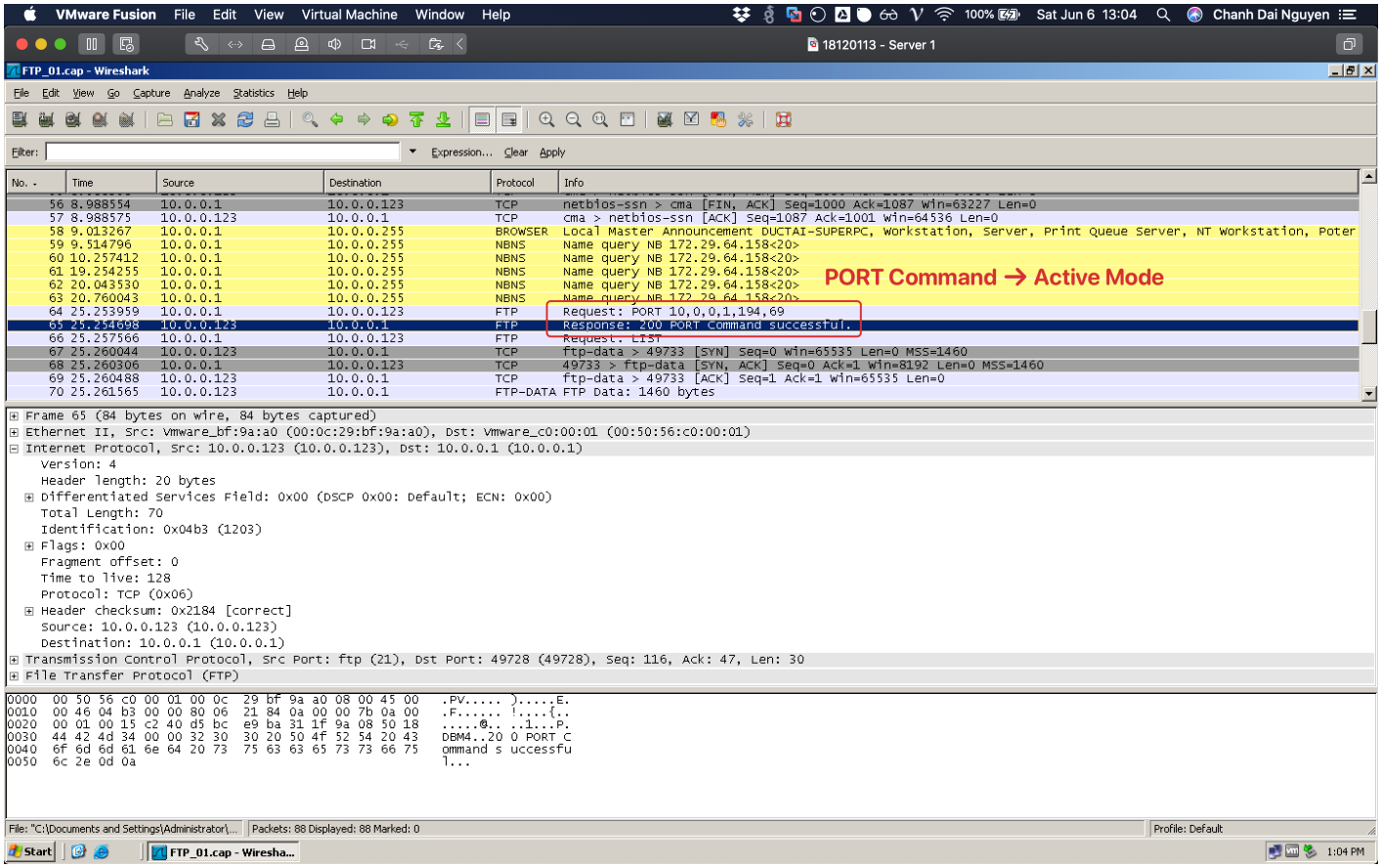
1 b. Địa chỉ IP máy Client và máy Server là gì ?

IP Máy Client	IP Máy Server
10.0.0.1	10.0.0.123



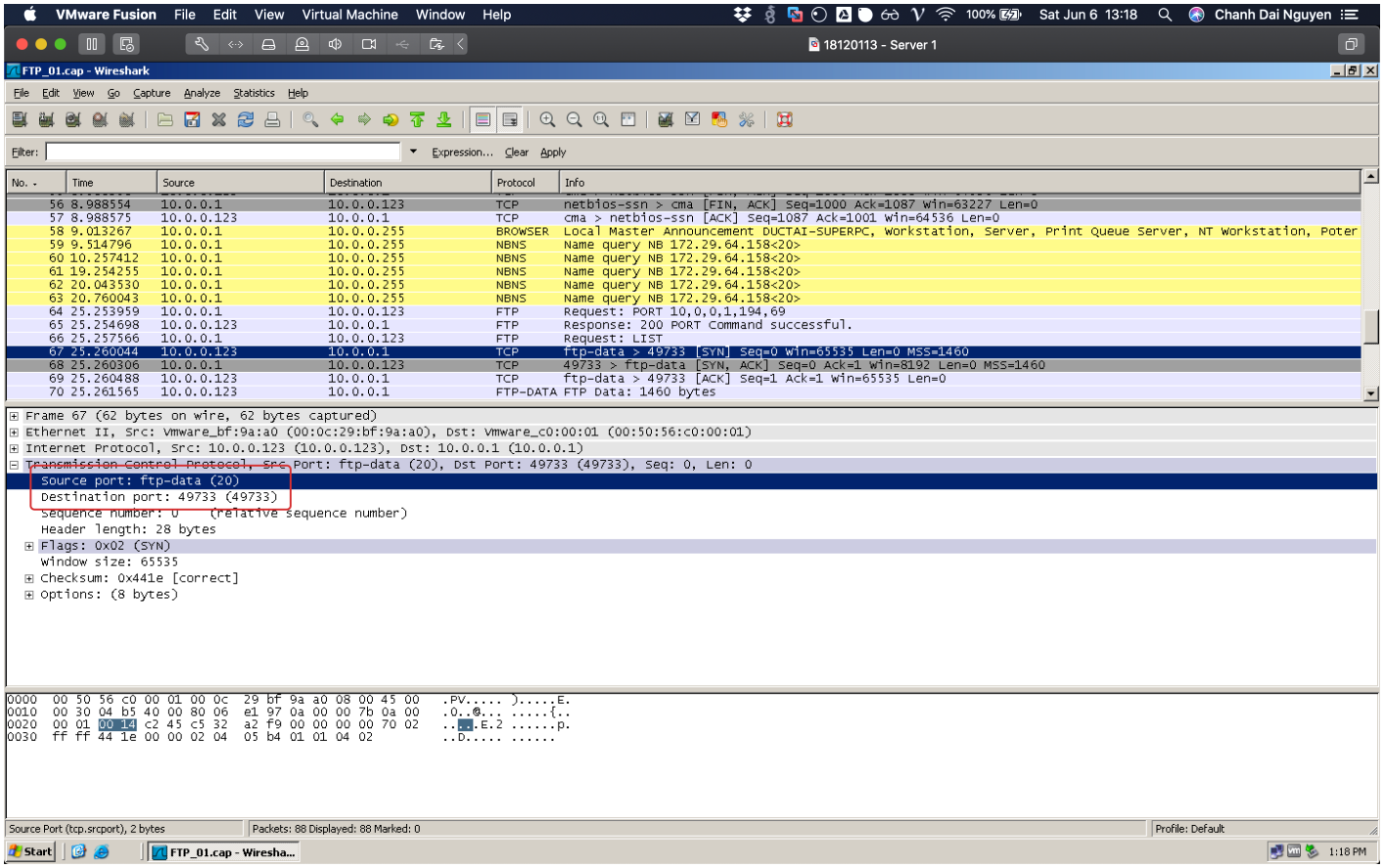
1 c. Client truy xuất lên Server theo mode nào: Active hay Passive ?

Client truy xuất lên Server theo Active Mode.



1 d. Port truyền dữ liệu của FTP Server và Client là bao nhiêu ?

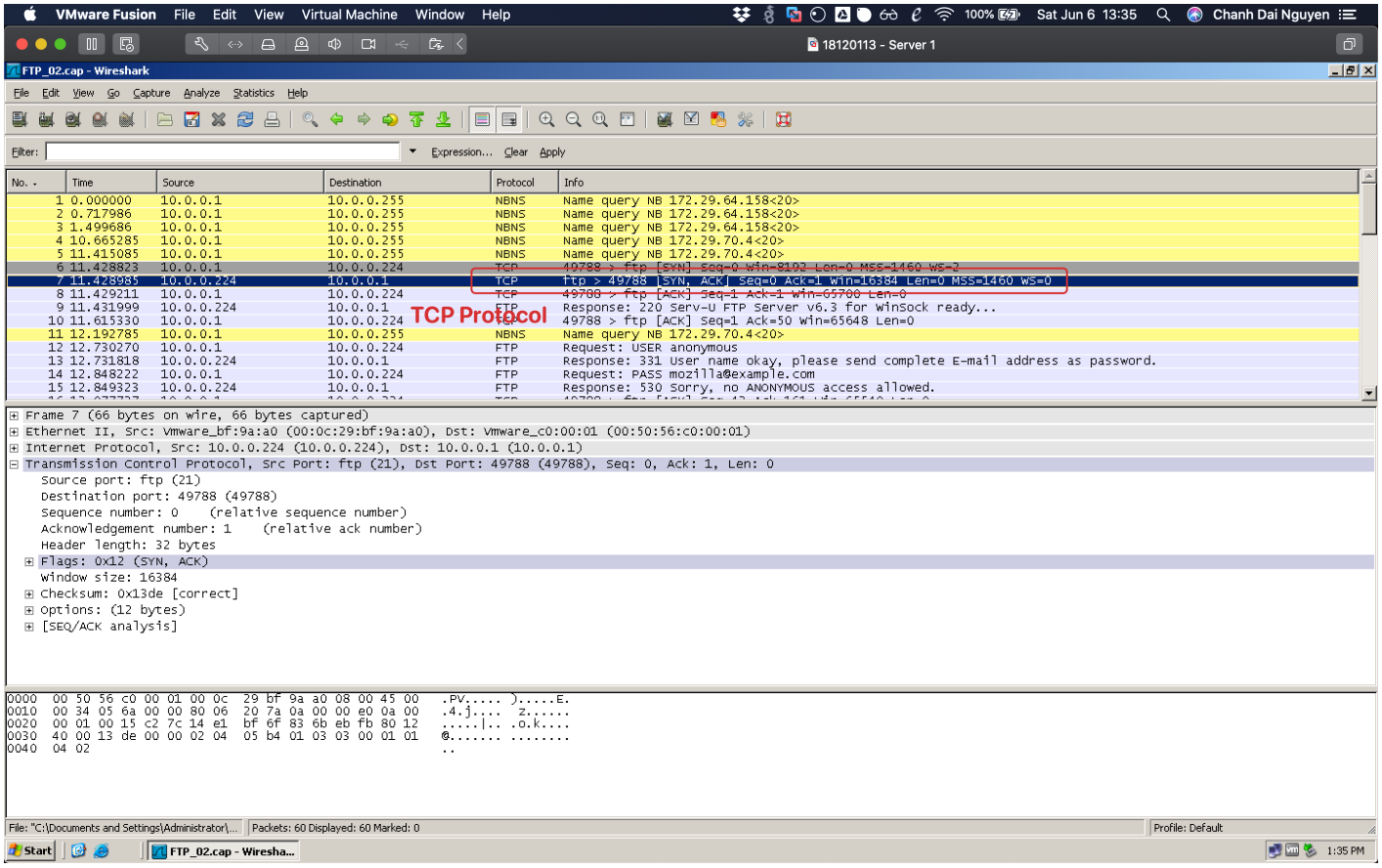
Port FTP Server	Port Client
20	49733



Câu 2. Cho tập tin FTP_02.cap, đọc tập tin này bằng Wireshark và trả lời các câu hỏi sau :

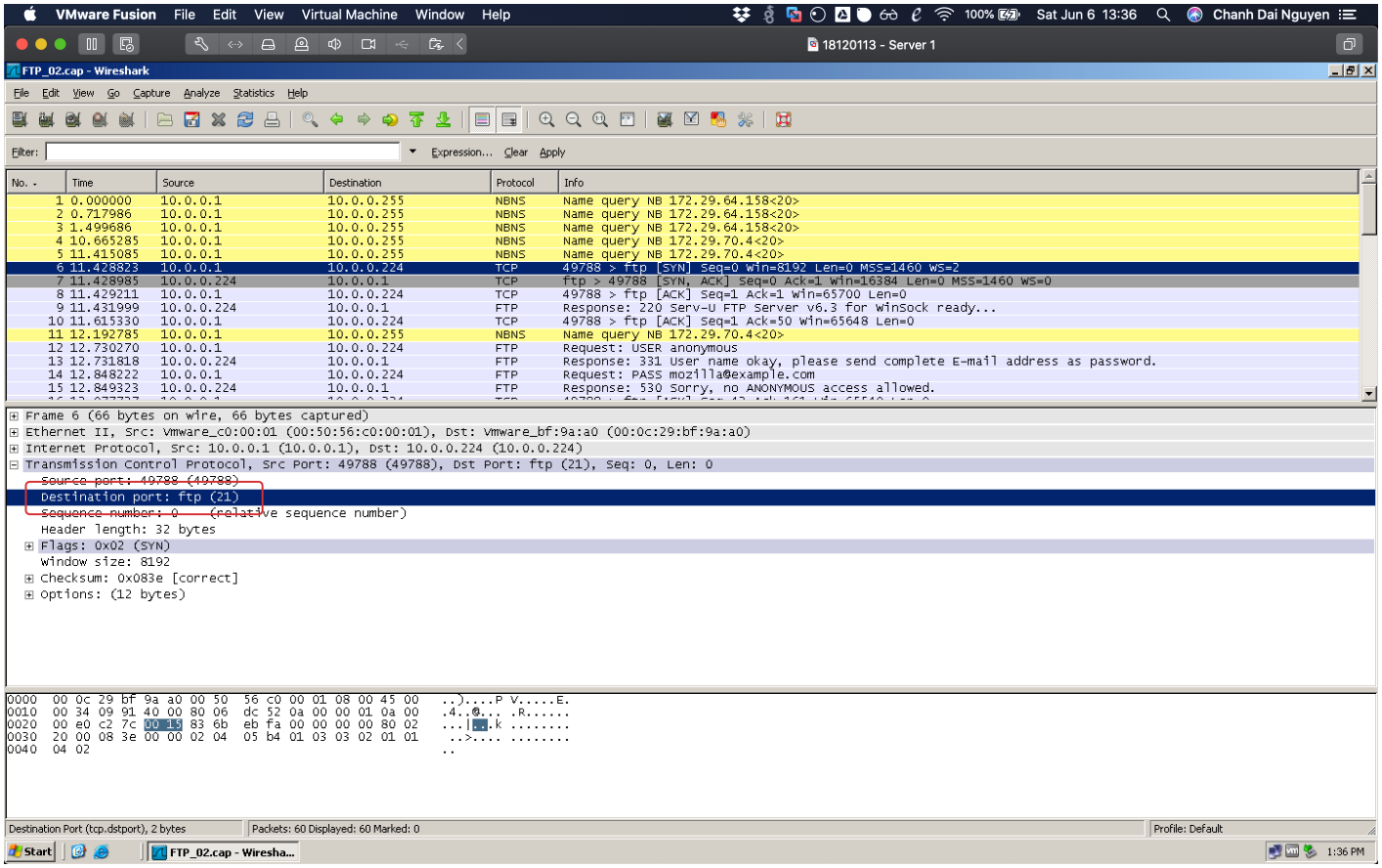
2 a. FTP sử dụng giao thức nào UDP hay TCP ?

FTP sử dụng giao thức TCP.



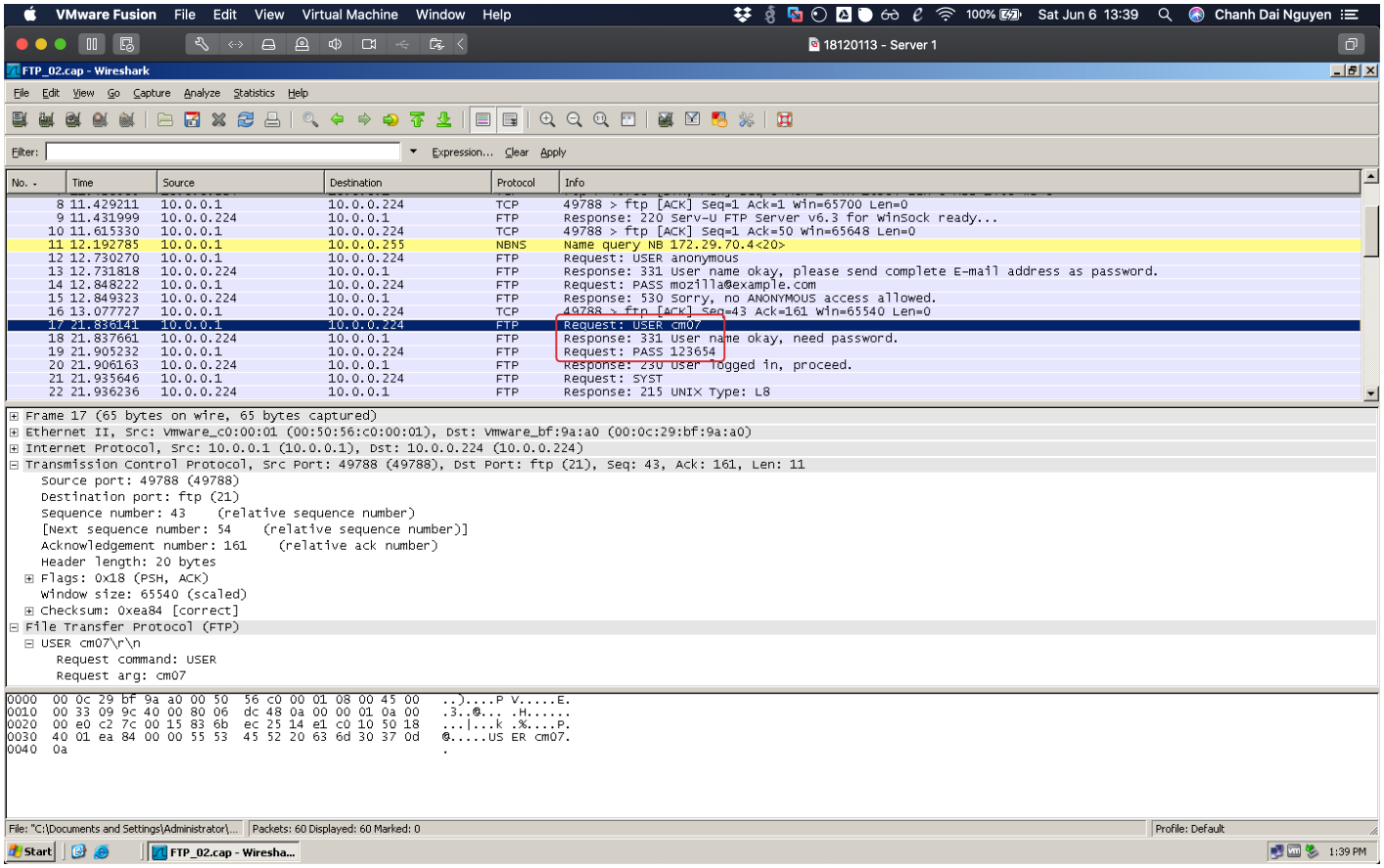
2 b. Port mặc định của FTP Server để nhận kết nối là bao nhiêu ?

FTP Server nhận kết nối ở Port mặc định : 21



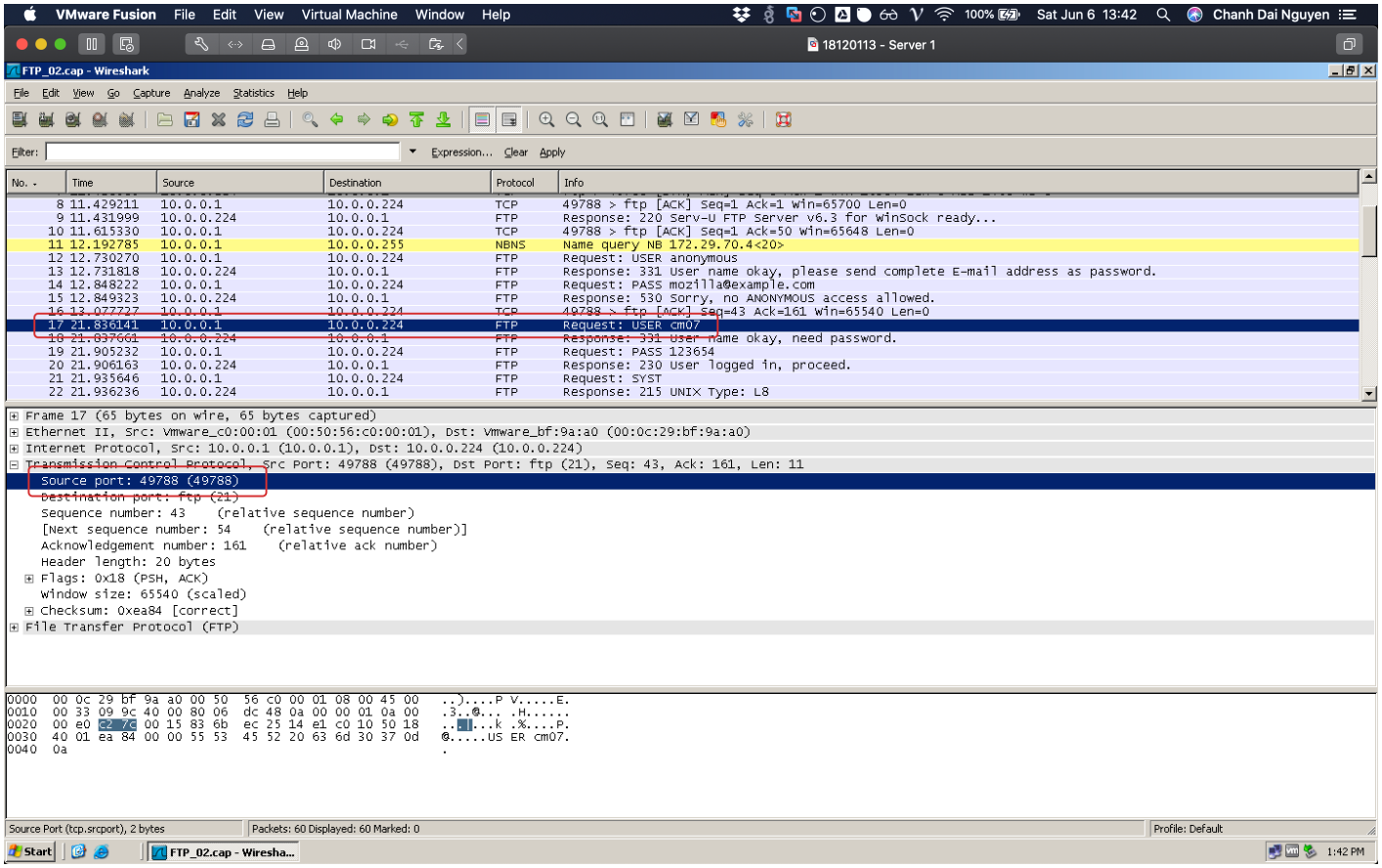
2 c. Username và Password của người dùng là gì ?

Username	Password
cm07	123654



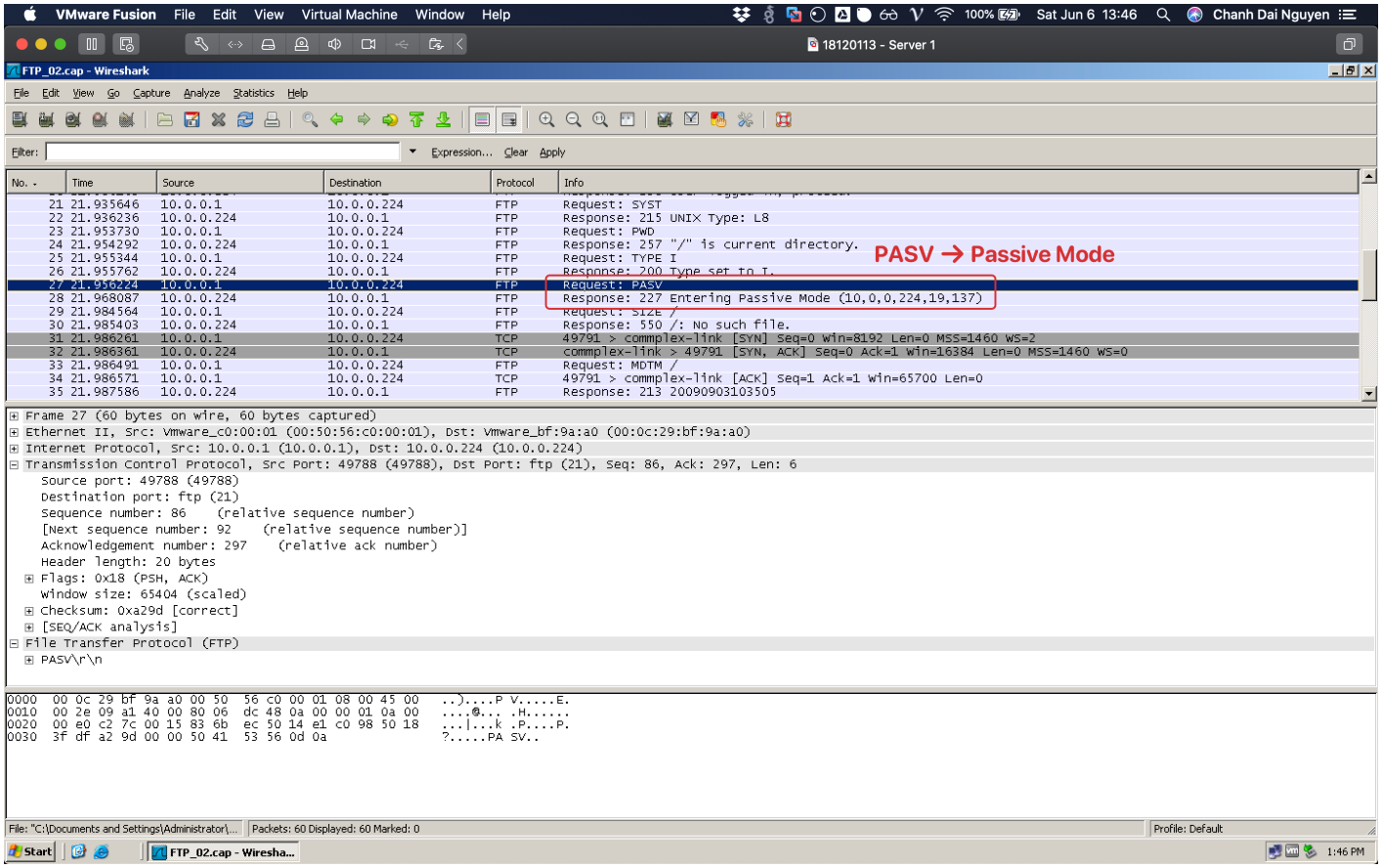
2 d. Port truyền lệnh của Client là bao nhiêu ?

Port truyền lệnh của Client là 49788.

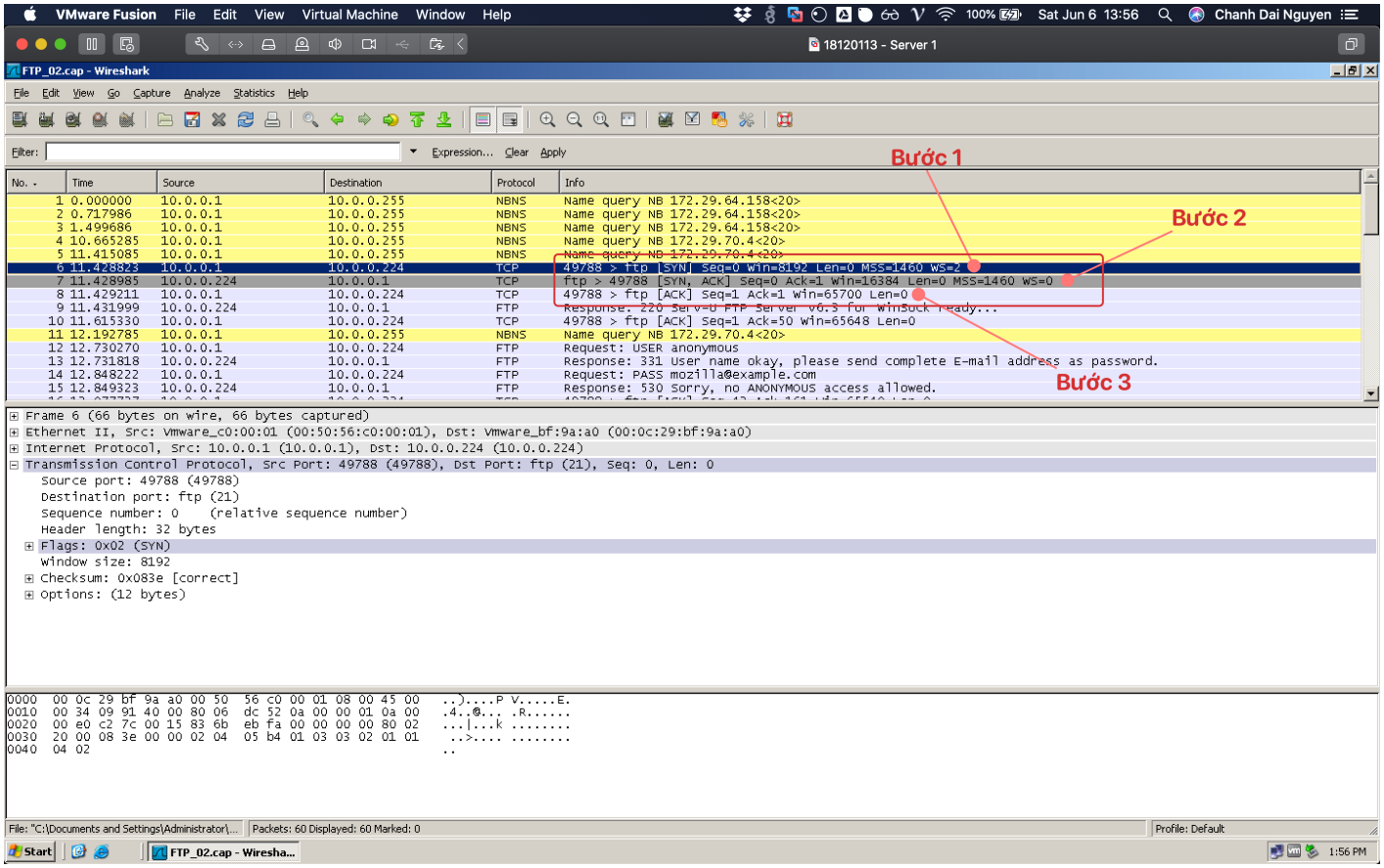


2 e. Client truy xuất lên Server theo mode nào: Active hay Passive ?

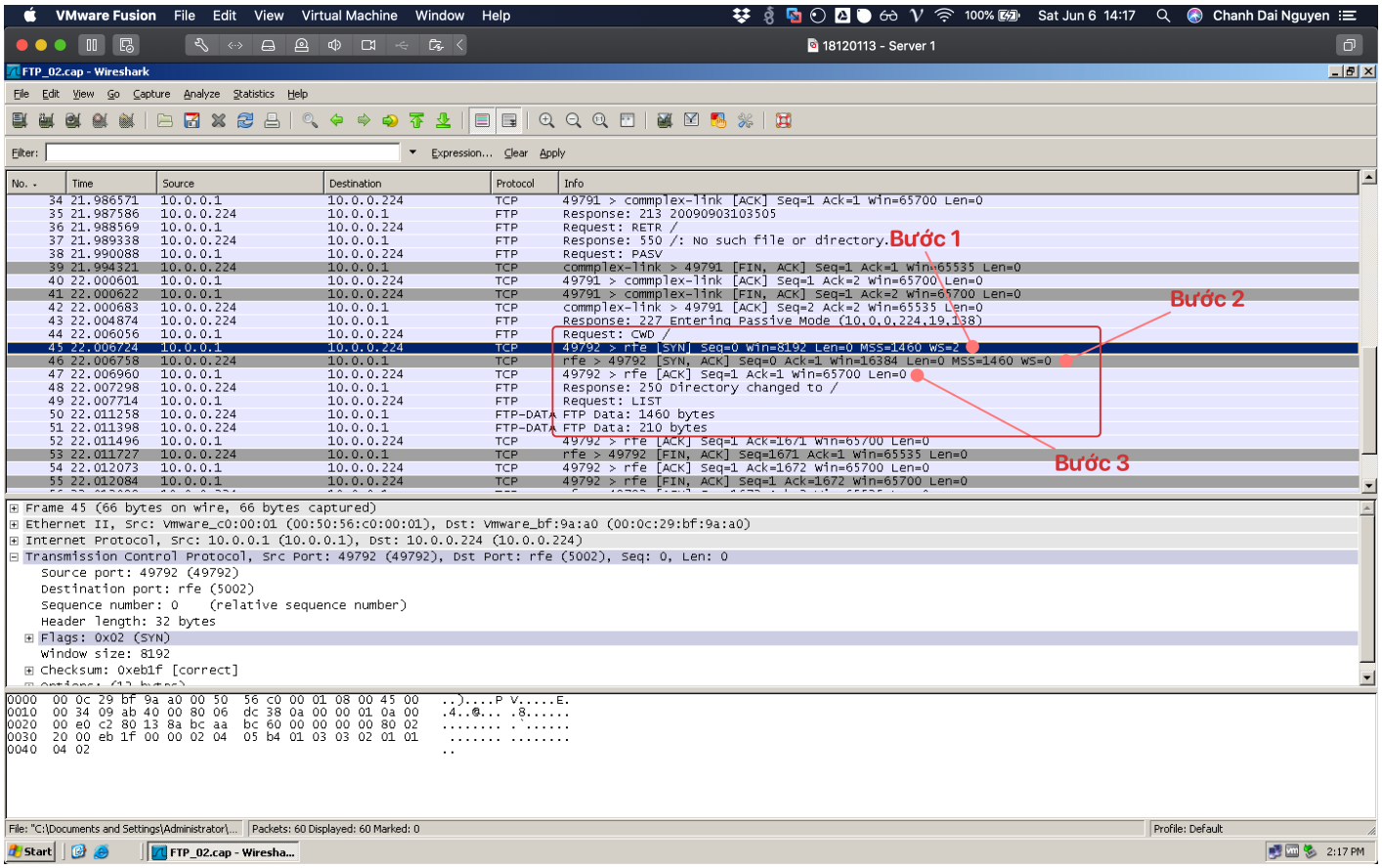
Client truy xuất lên Server theo Passive Mode.



2 f. Chỉ ra quá trình bắt tay 3 bước của Client và Server để tạo kết nối ban đầu khi thực hiện truyền Username và Password.

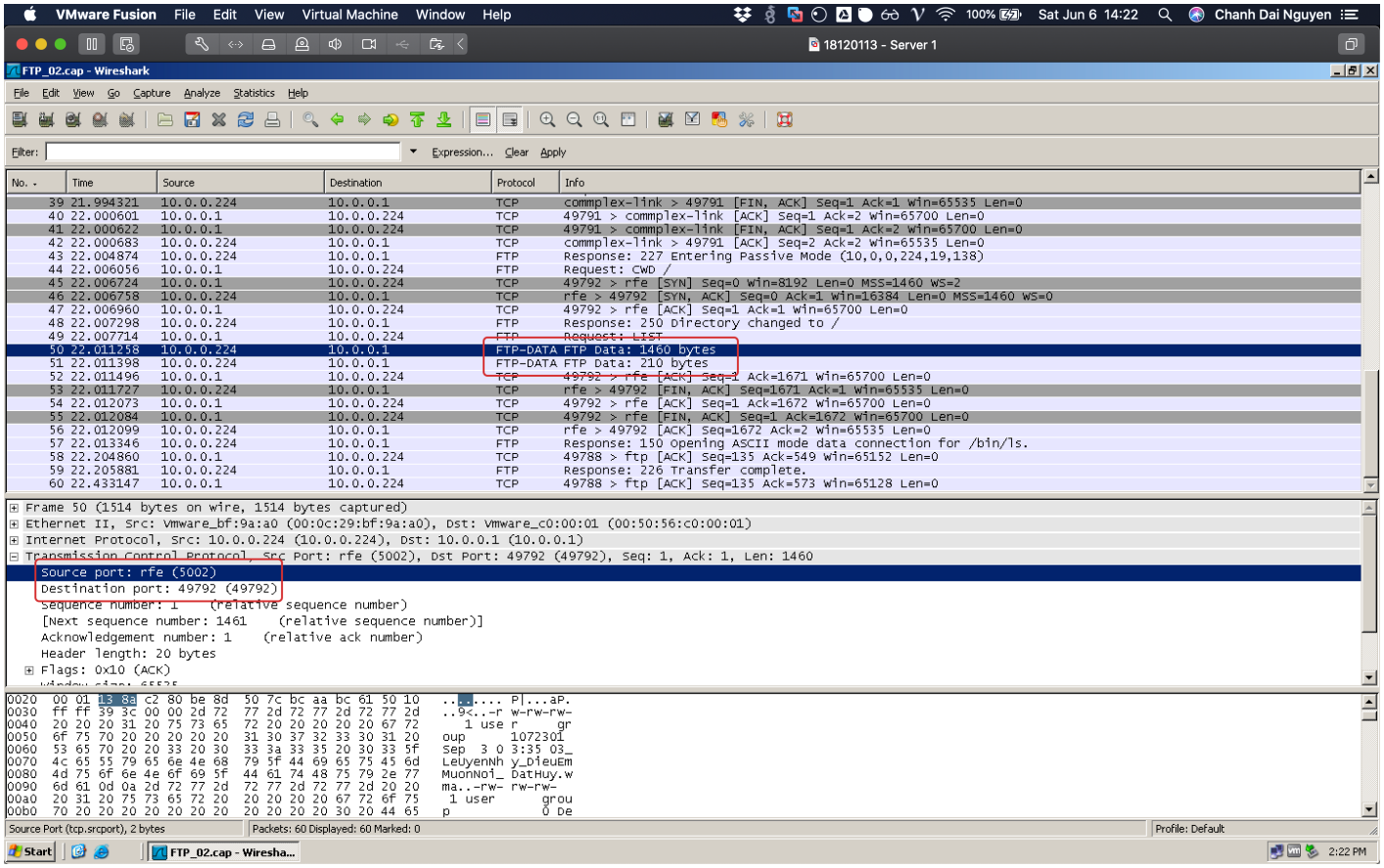


2 g. Chỉ ra quá trình bắt tay 3 bước của Client và Server để tạo kết nối truyền dữ liệu.



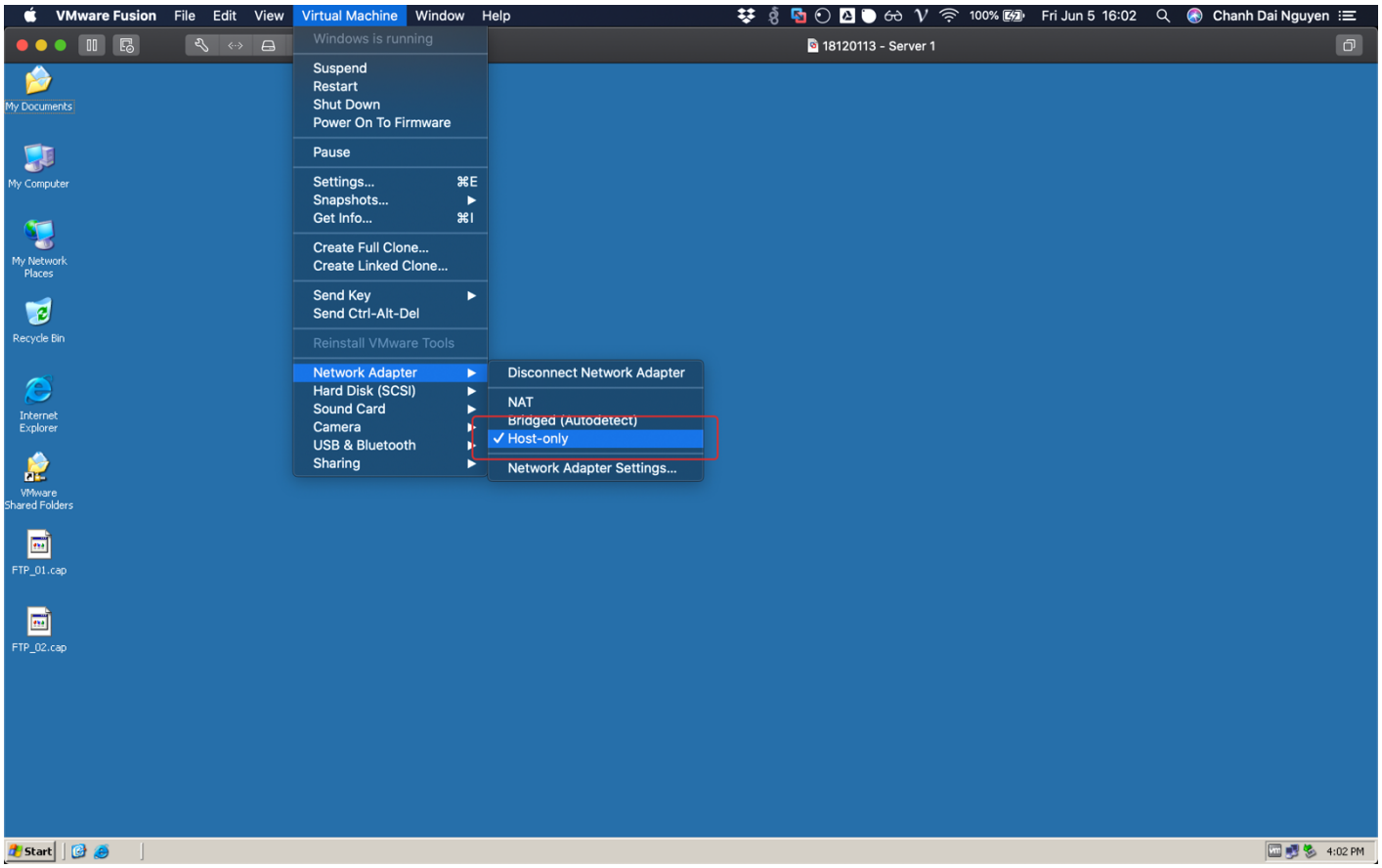
2 h. Port truyền dữ liệu của FTP Server và Client là bao nhiêu ?

Port FTP Server	Port Client
5002	49792



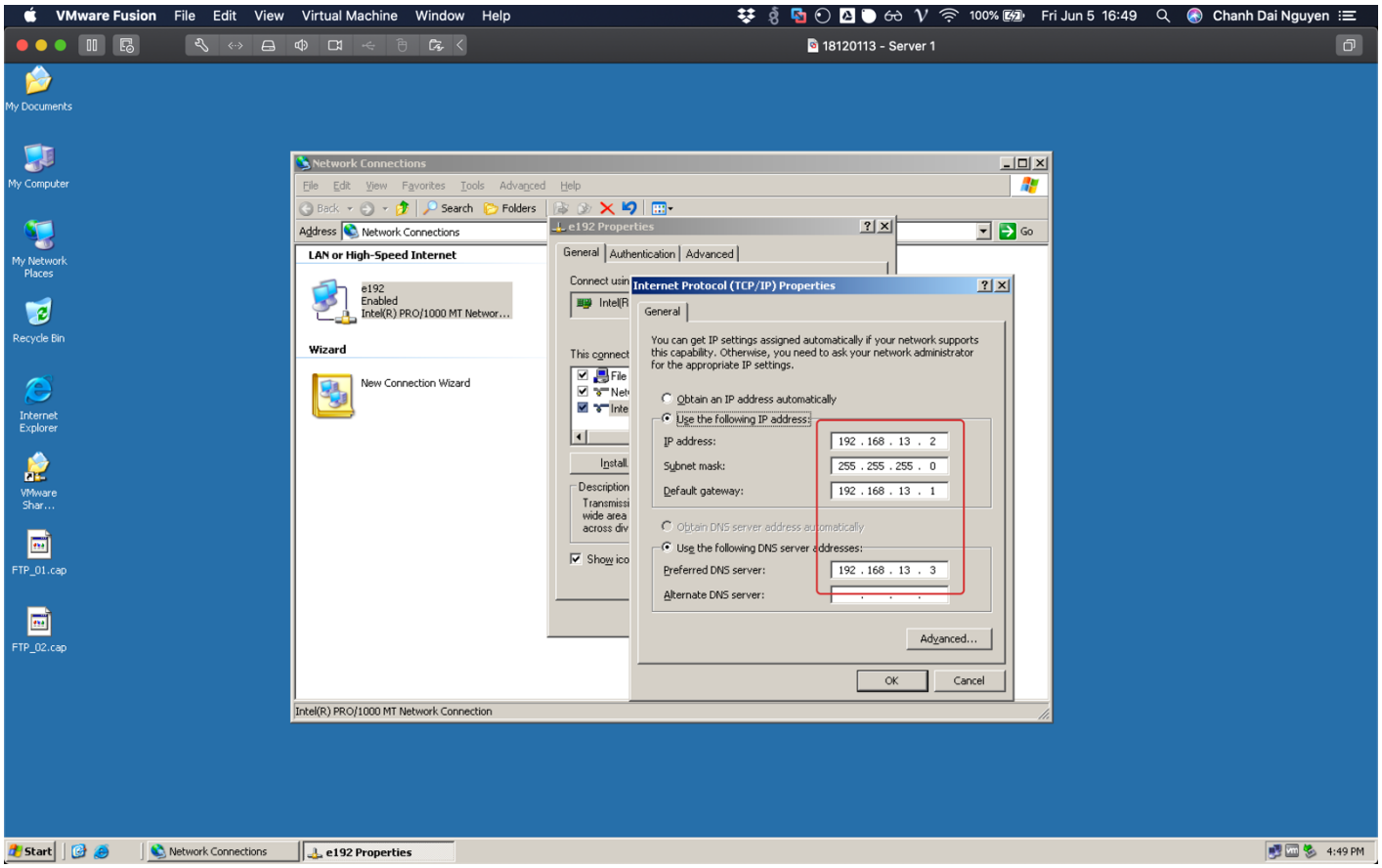
Câu 3. Cấu hình dịch vụ DHCP với các thông tin sau :

3 a. Sử dụng máy ảo MS Windows Server 2003/2008/2012 để làm DHCP Server. Thiết lập Card Mạng của máy ảo là Host-Only.



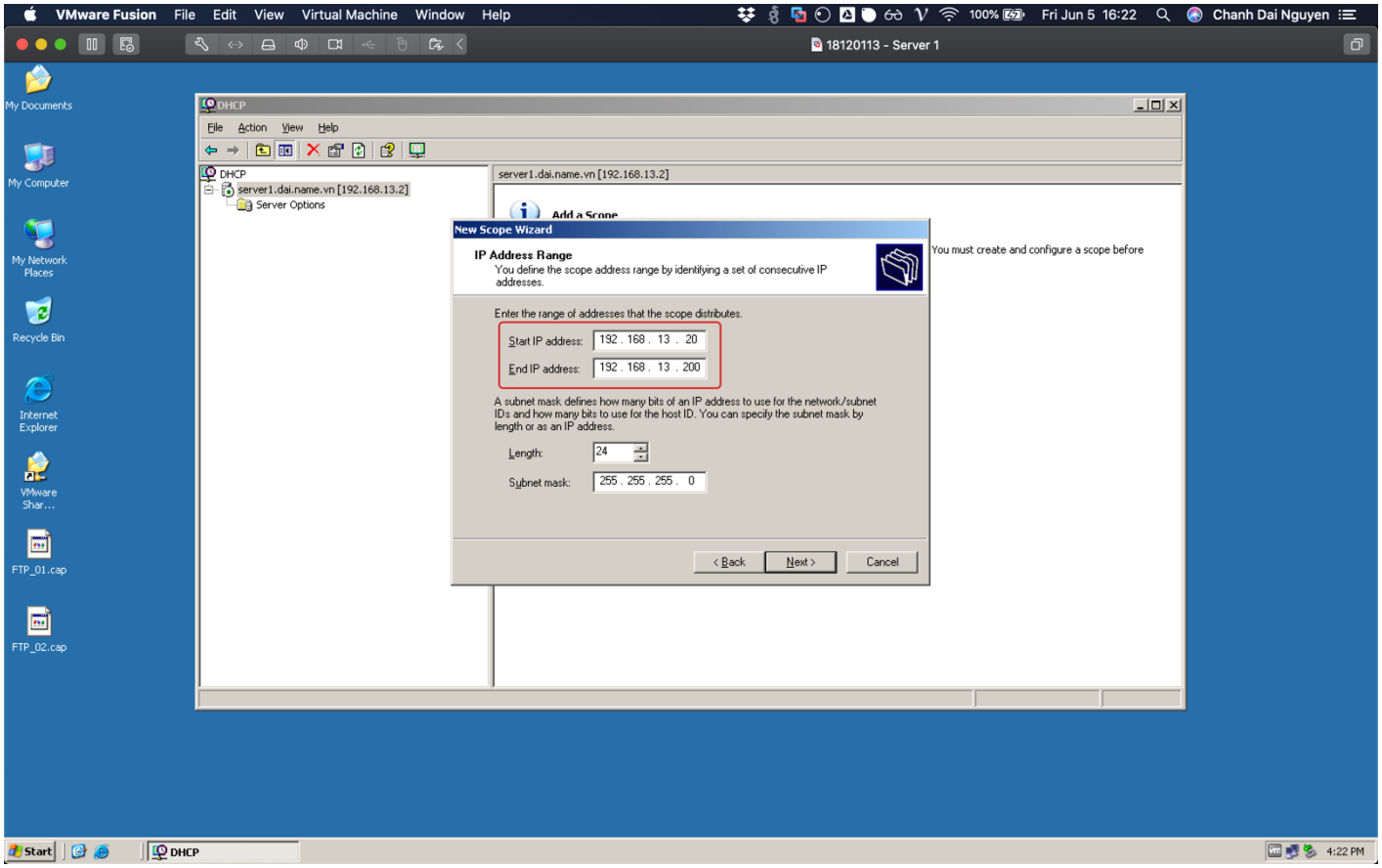
3 b. Cấu hình địa chỉ IP tĩnh cho máy làm DHCP Server này là : 192.168.X.2/24, với X là 2 chữ số cuối của MSSV.

MSSV = 1812113 → X = 13 → 192.168.13.2



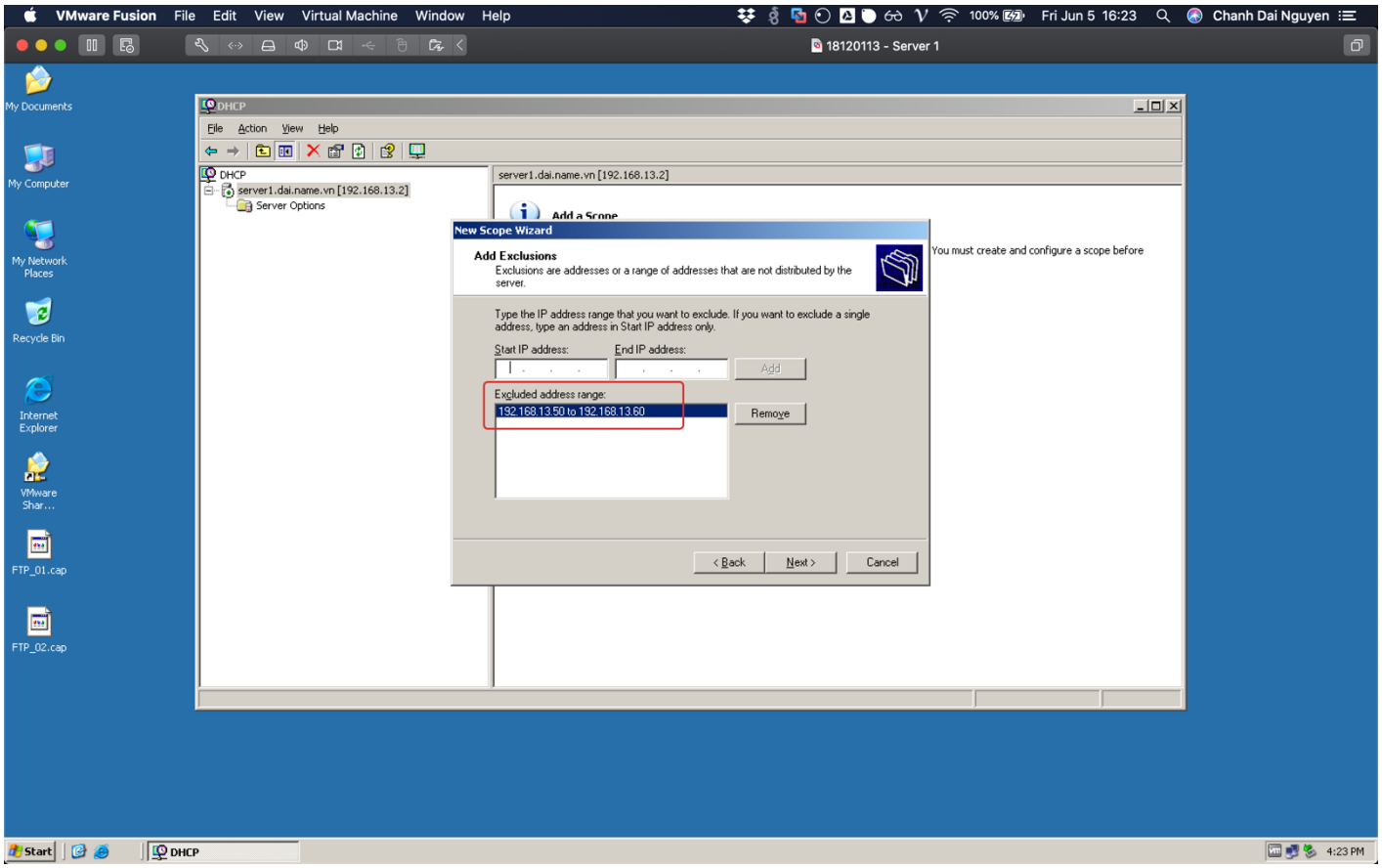
3 c. Khoảng địa chỉ IP cấp cho các Clients là : 192.168.X.20/24 – 192.168.X.200/24

→ 192.168.**13**.20/24 – 192.168.**13**.200/24



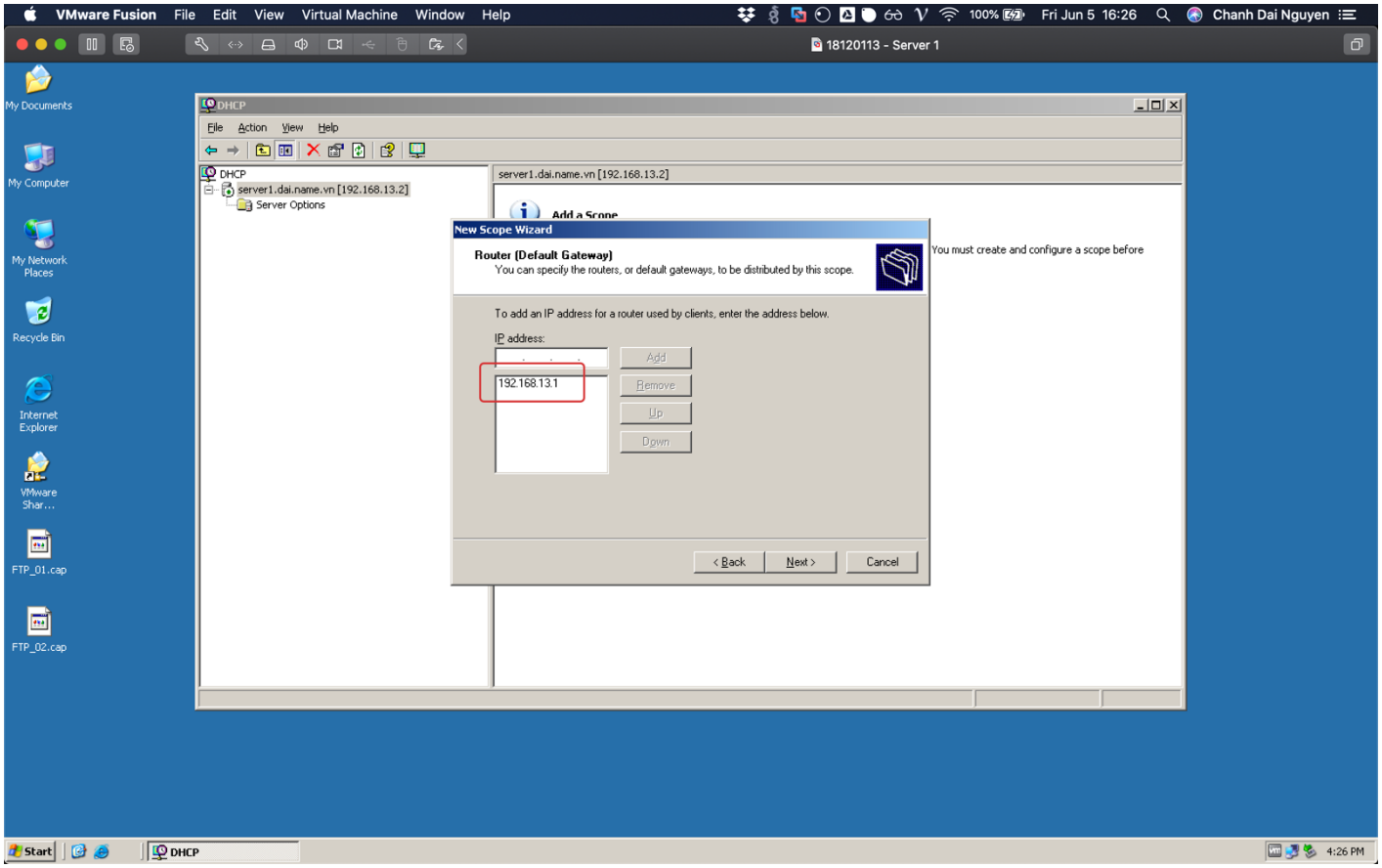
3 d. Khoảng địa chỉ IP không được cấp tự động (Exclusion) : 192.168.X.50/24 – 192.168.X.60/24

→ 192.168.**13**.50/24 – 192.168.**13**.60/24



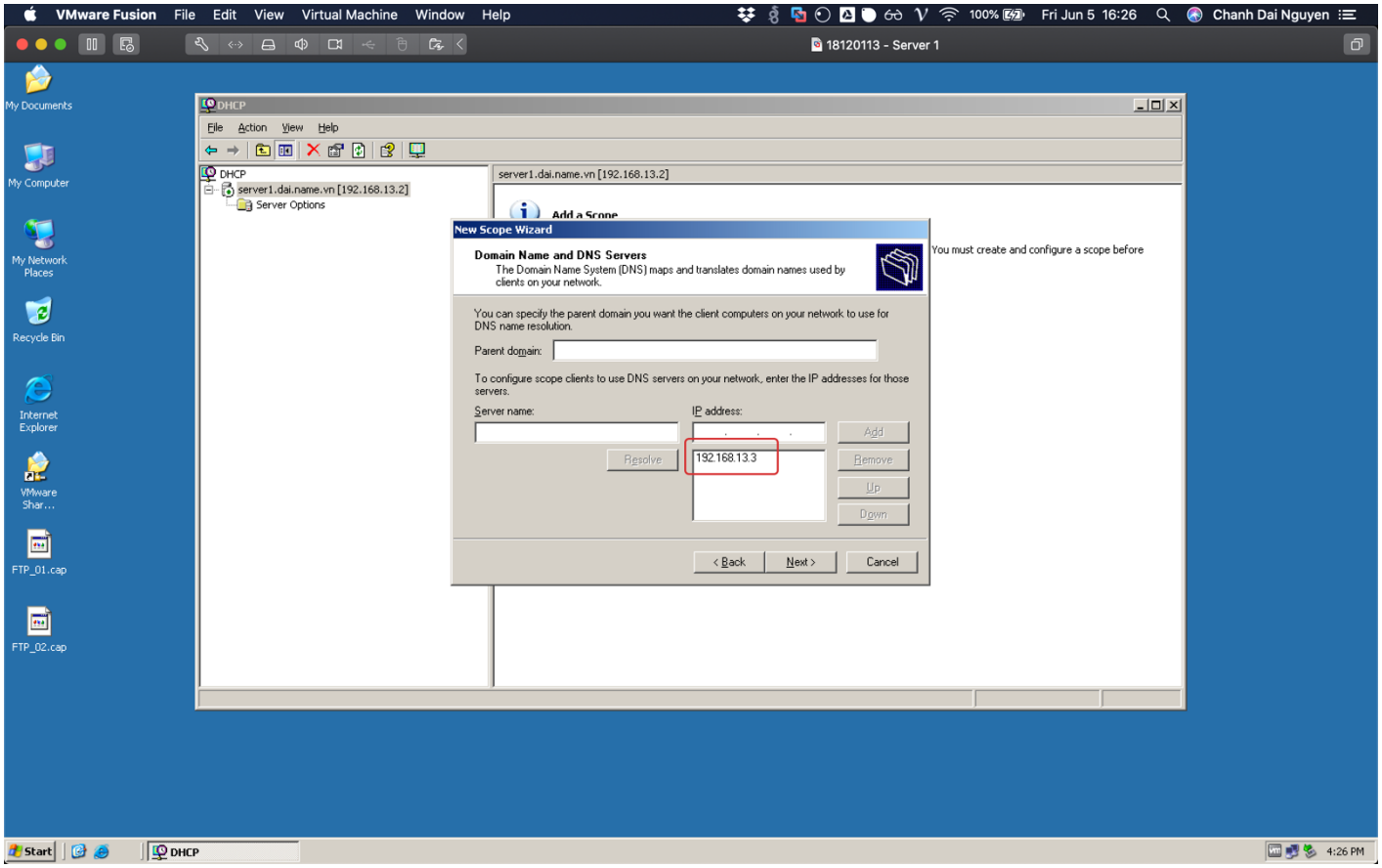
3 e. Default Gateway cung cấp cho các Clients : 192.168.X.1

→ 192.168.**13**.1

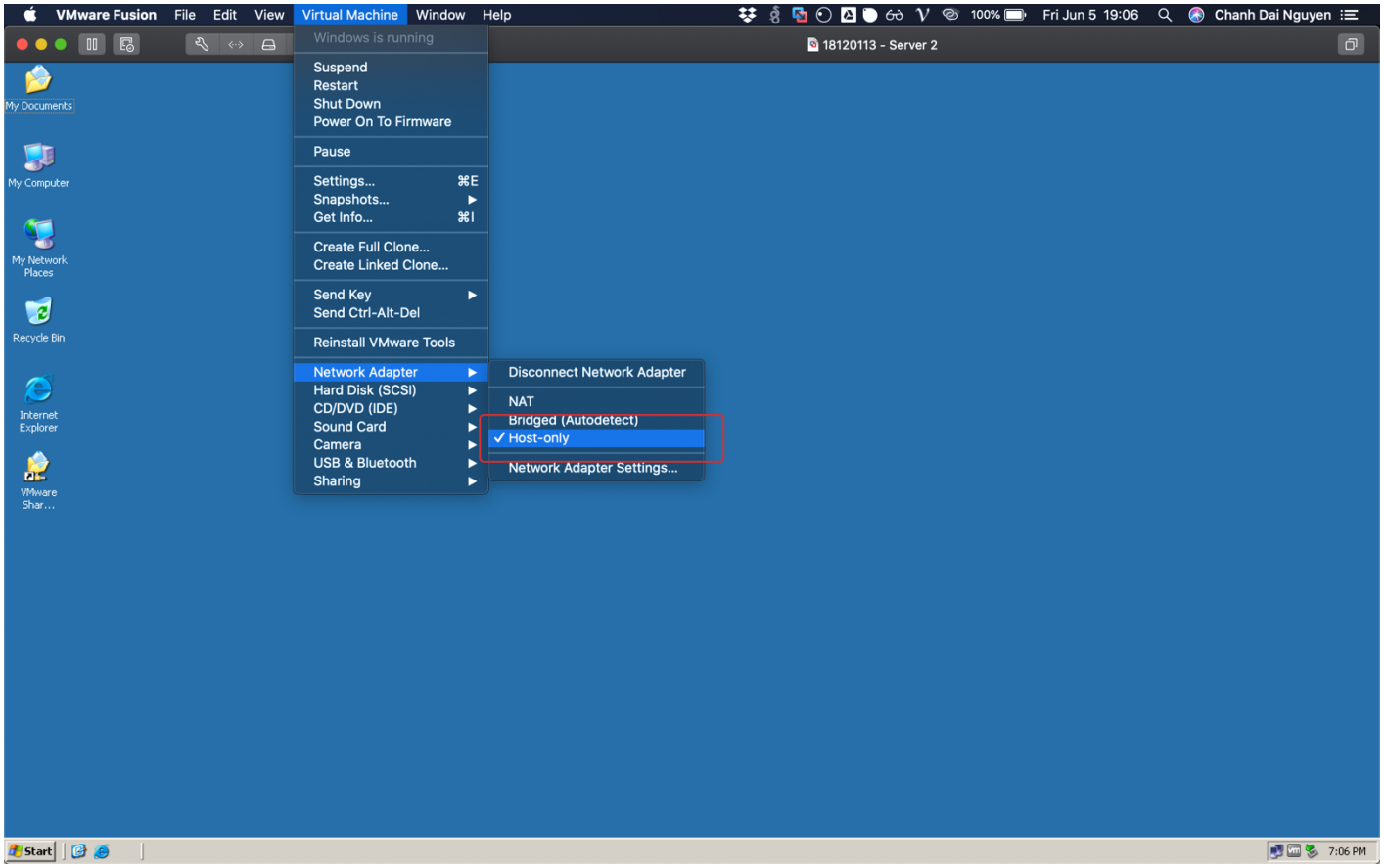


3 f. DNS Server cung cấp cho các Clients: 192.168.X.3

→ 192.168.**13**.3

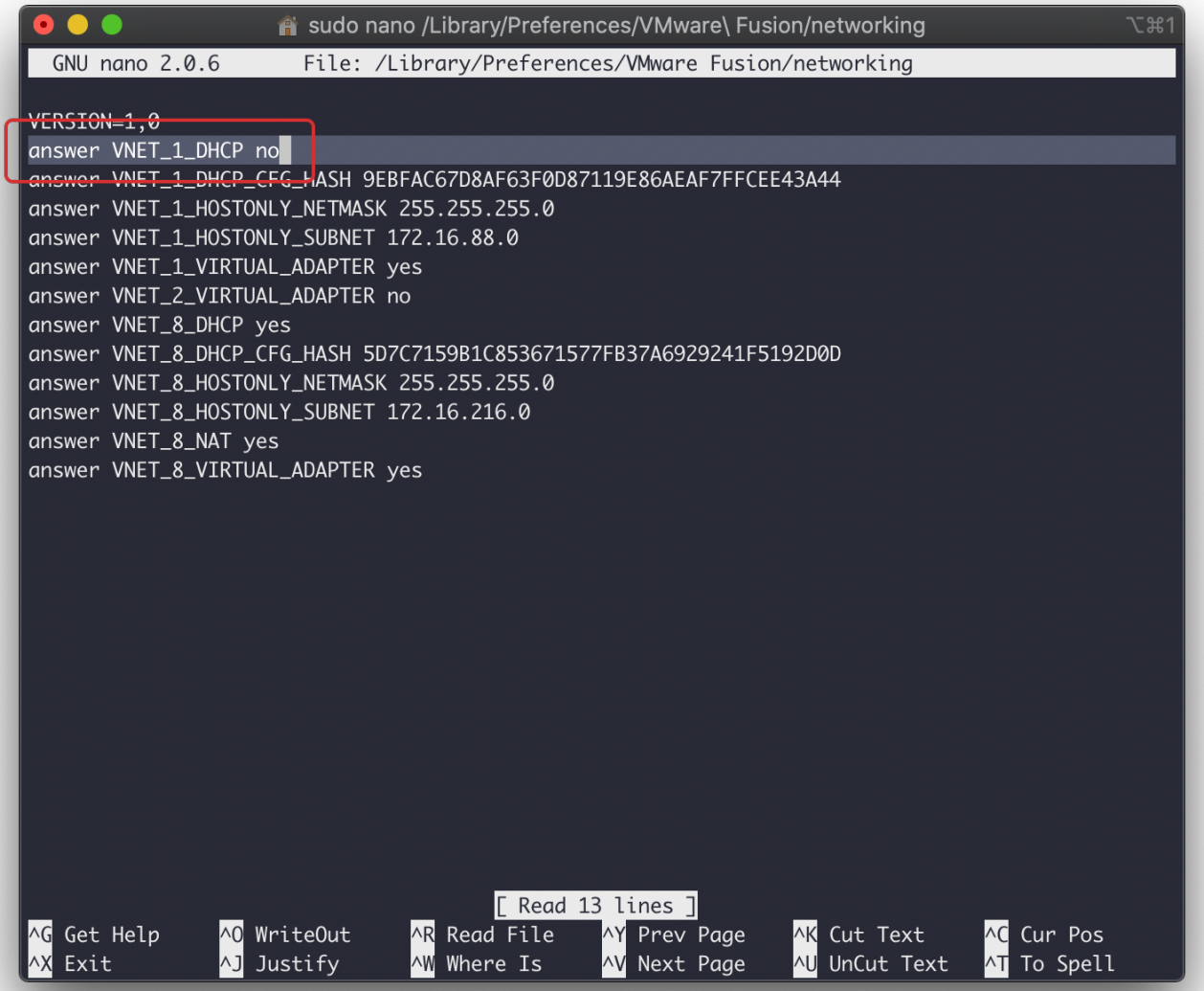


3 g. Cấu hình một máy ảo khác (Windows 7, Windows Server 2003, …) làm DHCP Client. Thiết lập Card Mạng của máy ảo này là Host-Only.



3 h. Tắt tính năng DHCP của phần mềm VMWare

Tắt tính năng DHCP của phần mềm VMWare Fusion 11.5.0 trên macOS 10.15.5

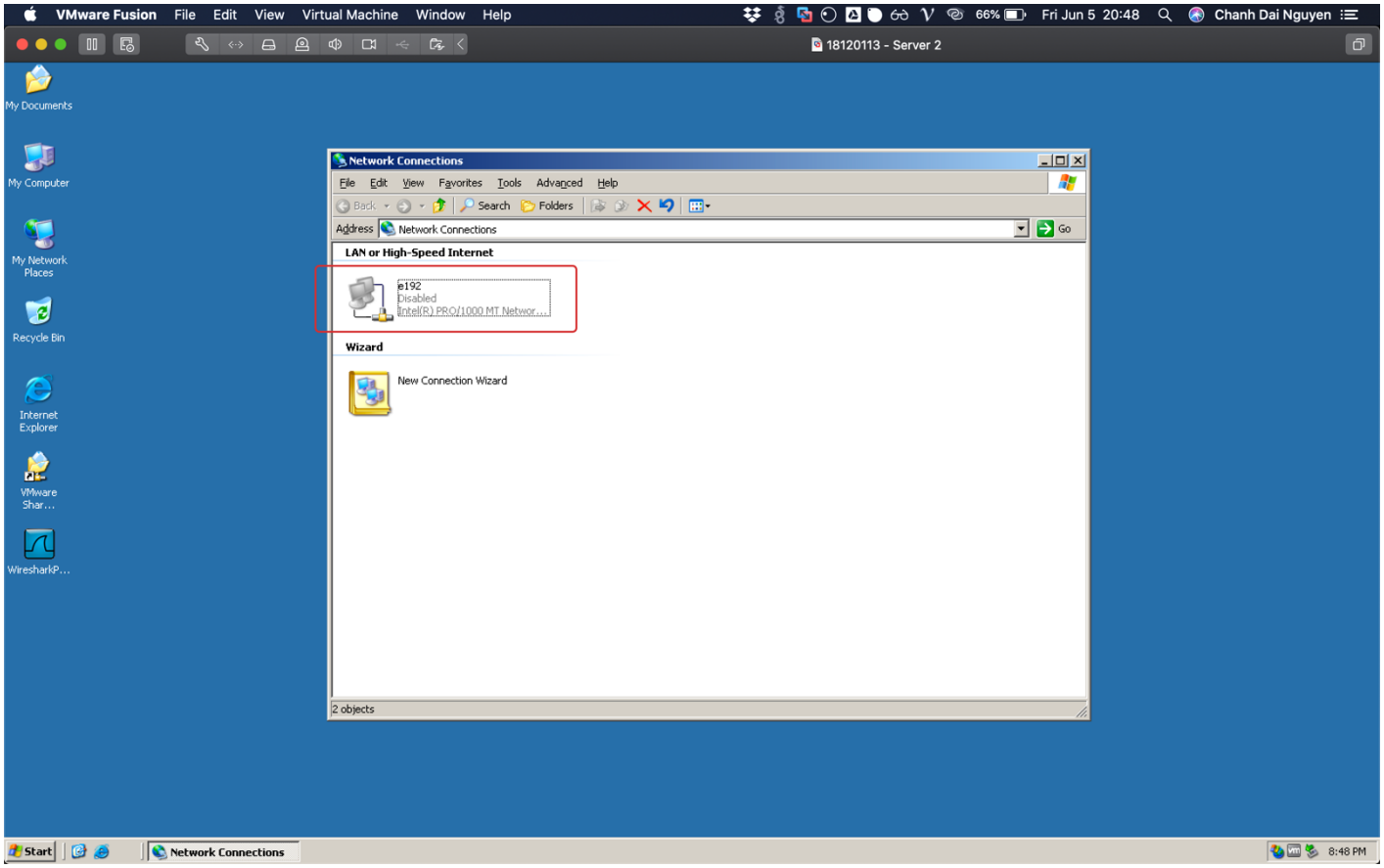


3 i. Thực hiện xin cấp phát địa chỉ IP từ client đến DHCP server và dùng Wireshark để bắt gói tin của quá trình này.

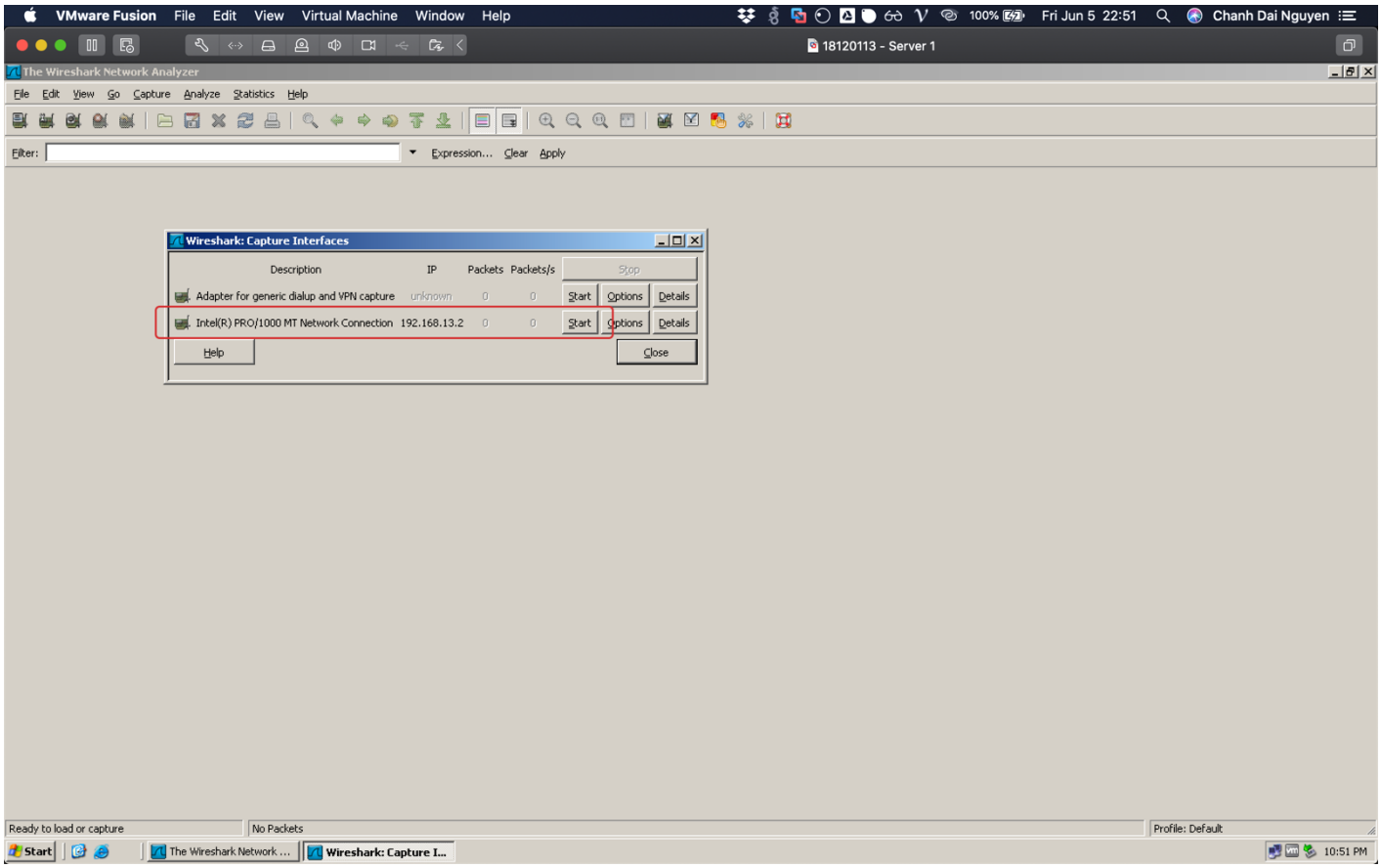
- Video quá trình thực hiện : https://youtu.be/K6uOl8auPIA

- Mô tả quá trình thực hiện :

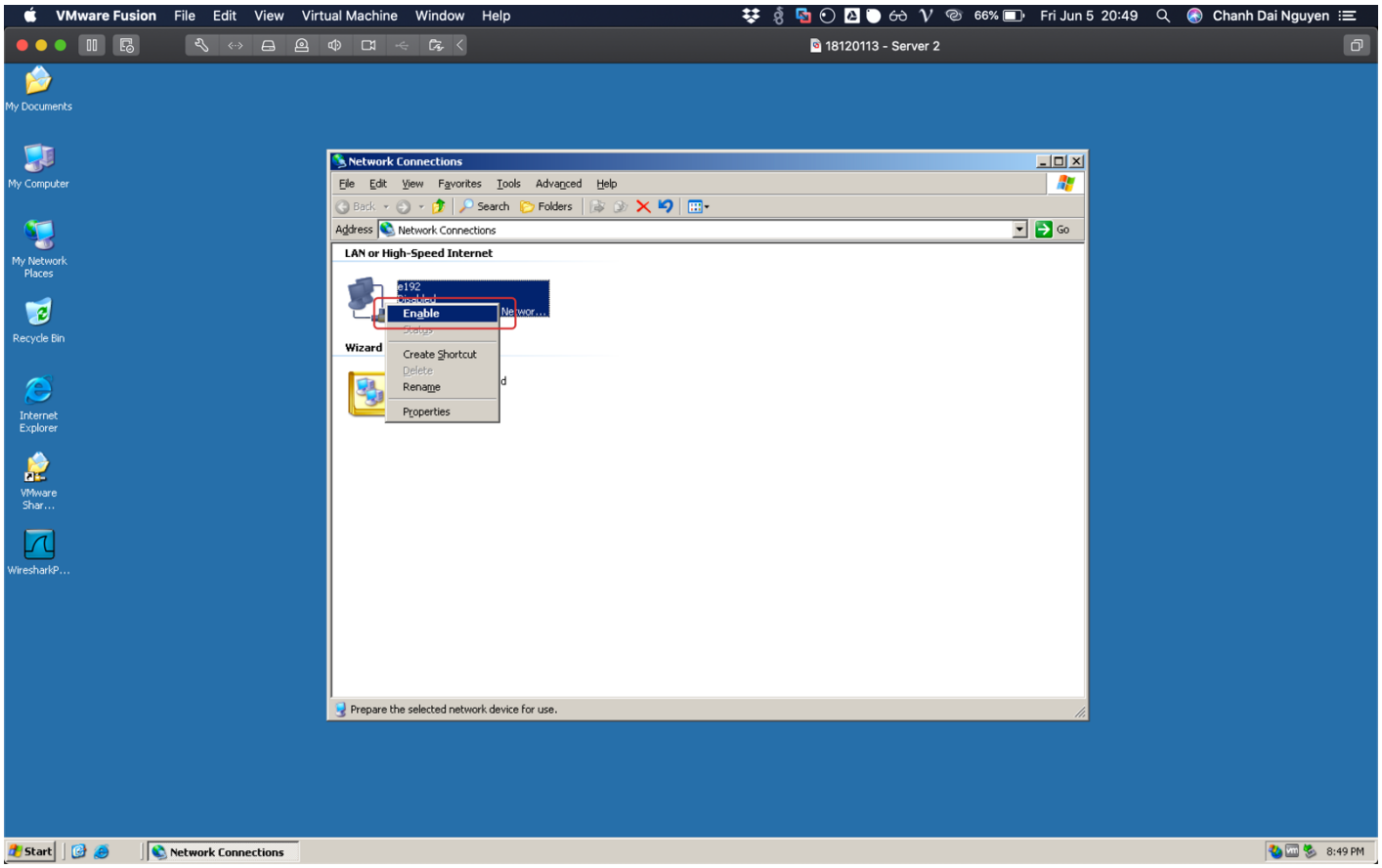
Bước 1. Tại DHCP Client (Server 2), Disable Card Mạng.



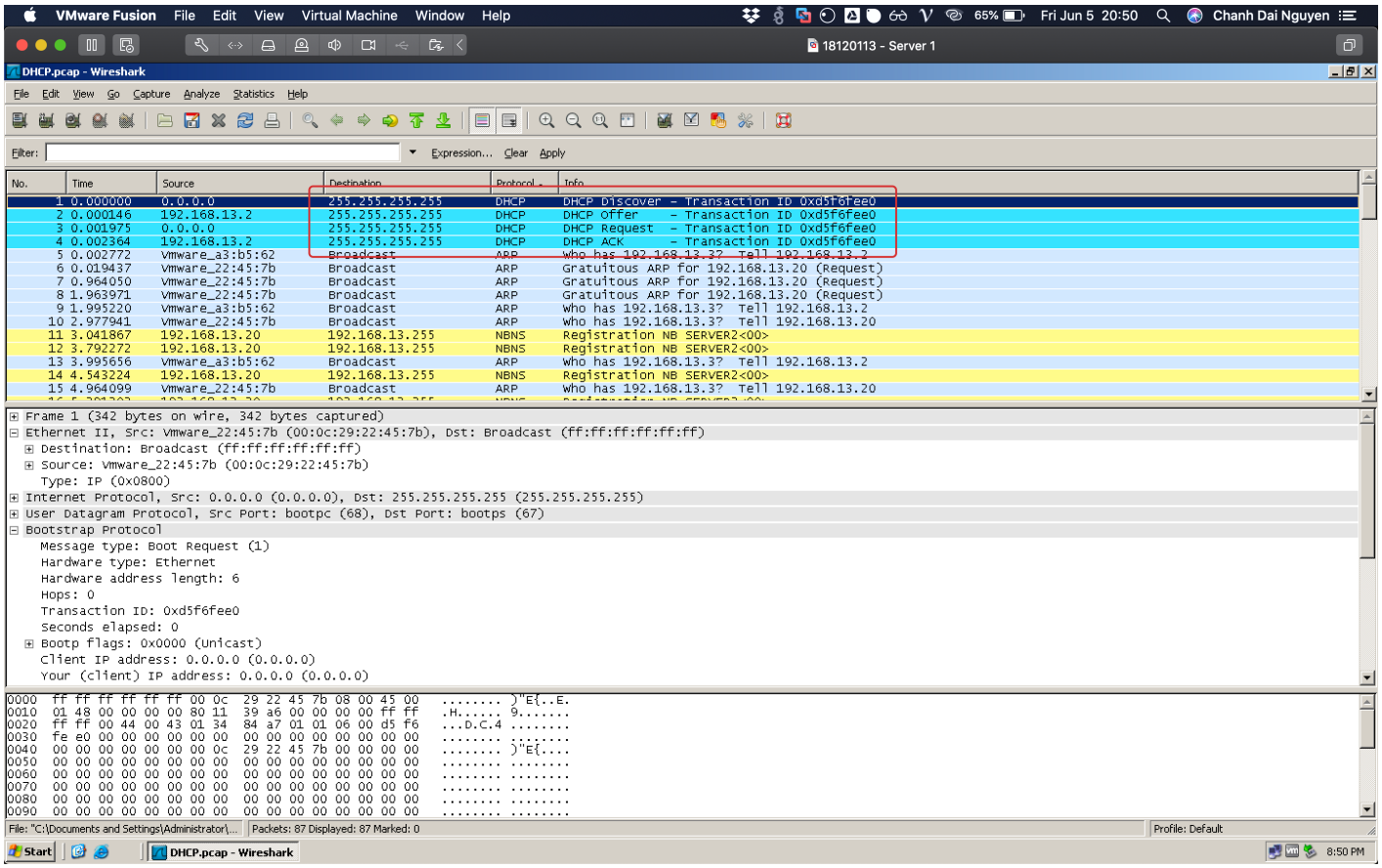
Bước 2. Tại DHCP Server (Server 1), Start Capture.



Bước 3. Tại DHCP Client (Server 2), Enable lại Card Mạng để xin cấp phát địa chỉ IP.

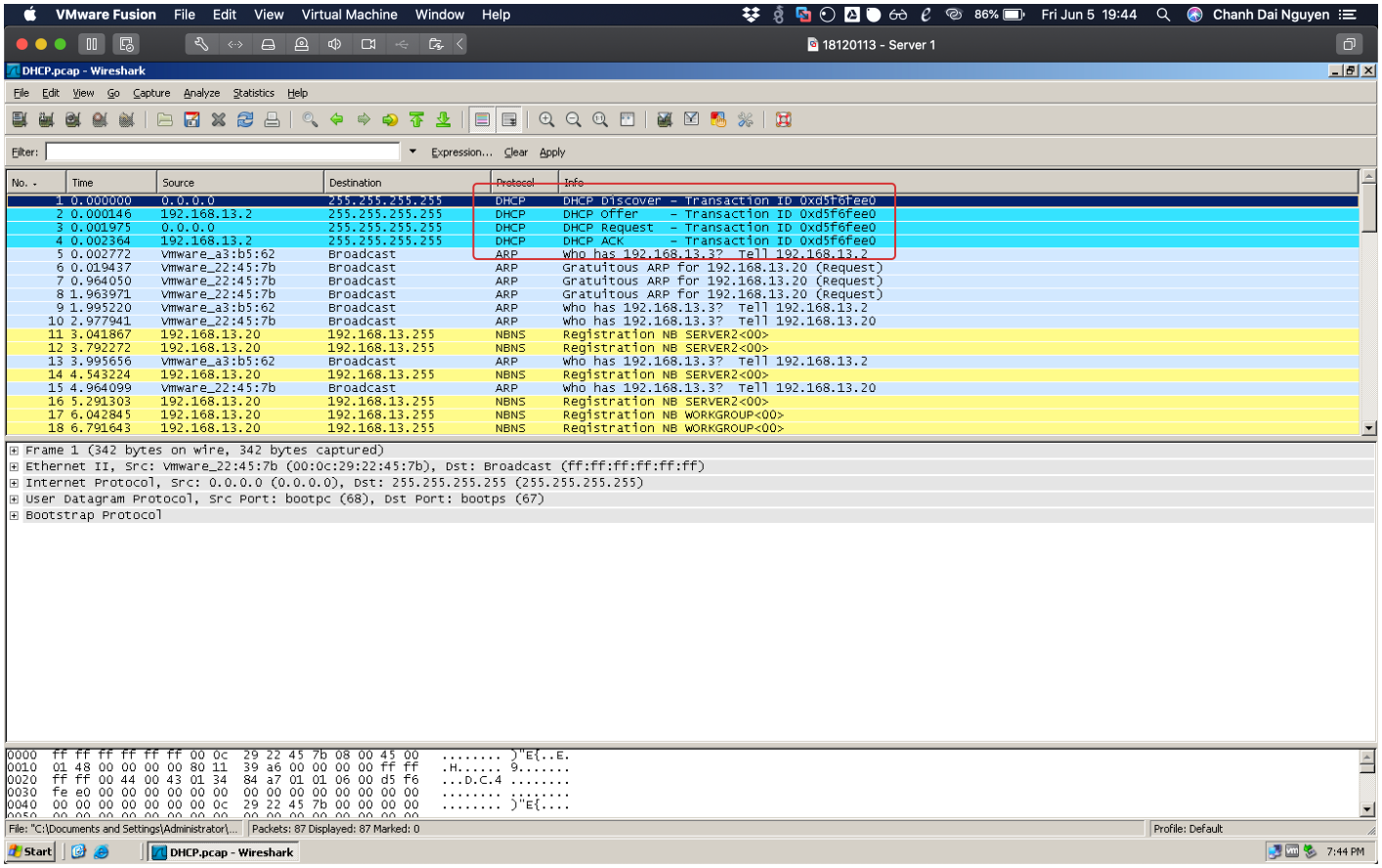


Bước 4. Tại DHCP Server (Server 1), Stop Capture và Xem kết quả.



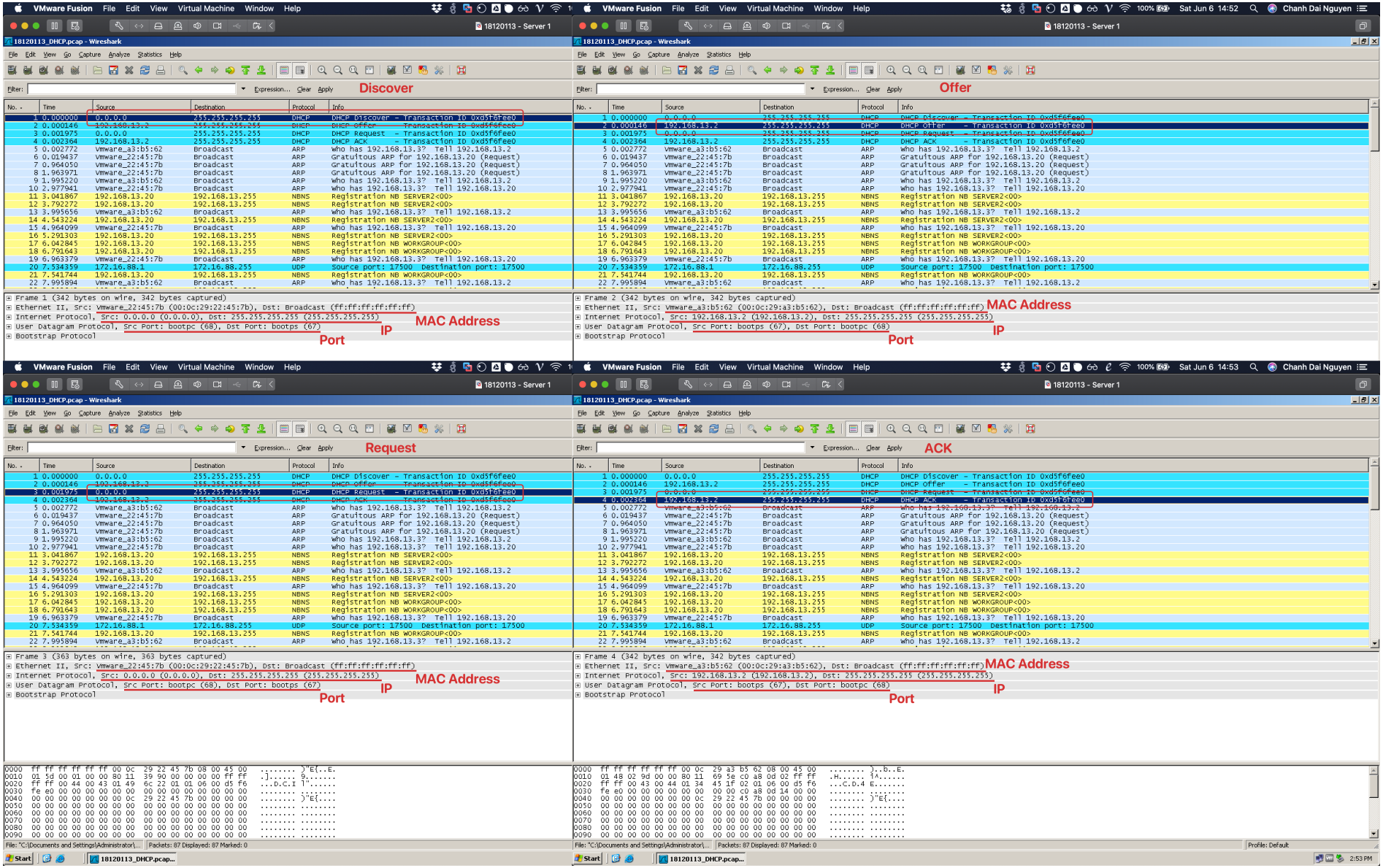
3 j. Cho biết có bao nhiêu gói tin được truyền và nhận trong quá trình cấp phát địa chỉ IP ?

Có 4 gói tin được truyền và nhận trong quá trình cấp phát địa chỉ IP : *Discover, Offer, Request, ACK.*



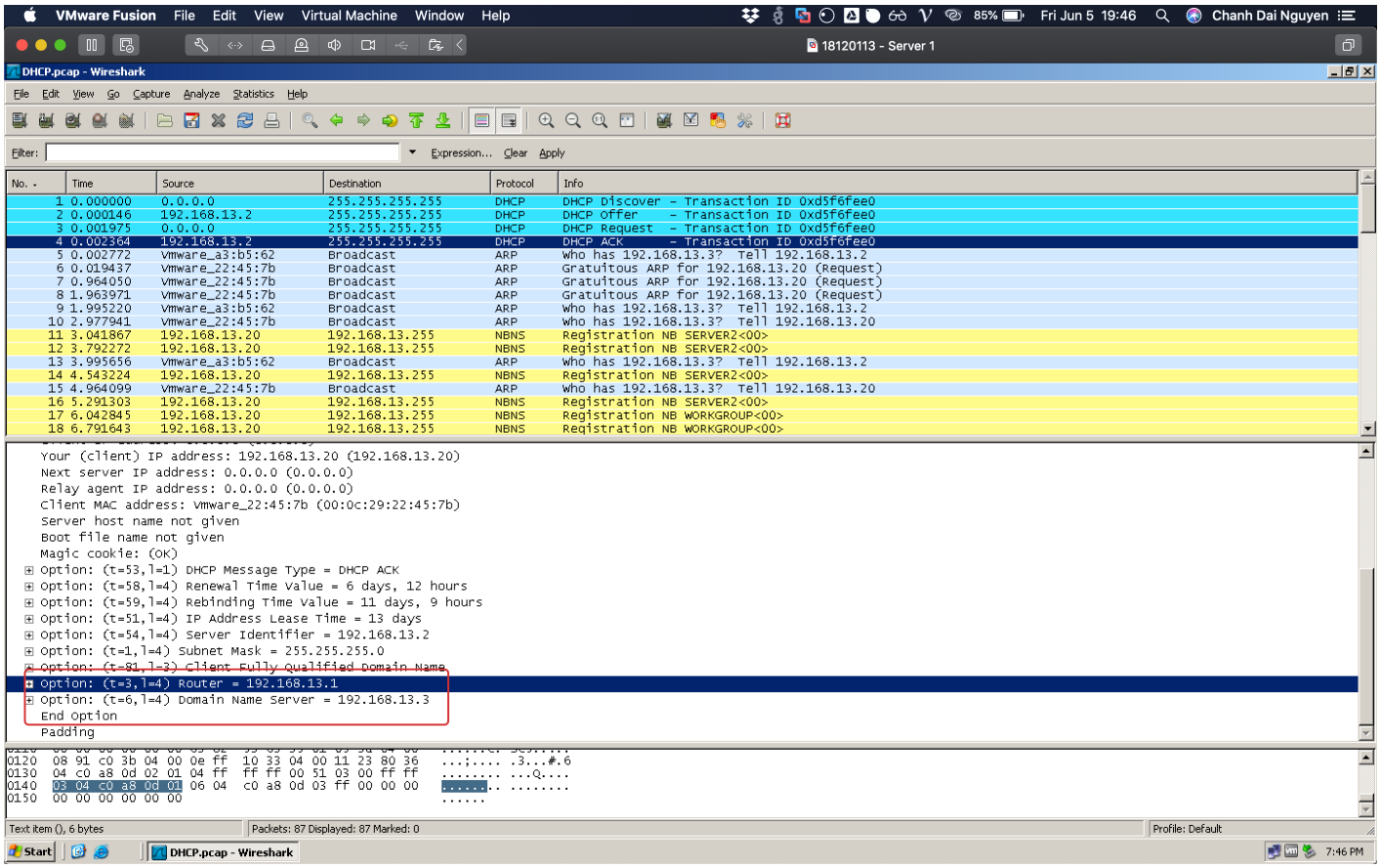
3 k. Gồm những gói tin nào, giải thích mục đích của mỗi gói ? Với mỗi gói cho biết : IP Nguồn, IP Đích, MAC Nguồn, MAC Đích, Port Nguồn, Port Đích ?

Gói tin	Mục đích	IP Nguồn	IP Đích	MAC Nguồn	MAC Đích	Port Nguồn	Port Đích
Discover	Client tìm DHCP Server	0.0.0.0	255.255.255.255	00:0c:29:22:45:7b	ff:ff:ff:ff:ff:ff	68	67
Offer	DHCP gợi ý một địa chỉ IP	192.168.13.2	255.255.255.255	00:0c:29:a3:b5:62	ff:ff:ff:ff:ff:ff	67	68
Request	Client yêu cầu cấp 1 địa chỉ IP	0.0.0.0	255.255.255.255	00:0c:29:22:45:7b	ff:ff:ff:ff:ff:ff	68	67
ACK	Server xác nhận đồng ý và giải phóng địa chỉ IP	192.168.13.2	255.255.255.255	00:0c:29:a3:b5:62	ff:ff:ff:ff:ff:ff	67	68


Discover
Offer
Request
ACK
MAC Address
IP
Port

3 l. Thông tin Default Gateway và DNS Server nằm trong gói tin nào ?

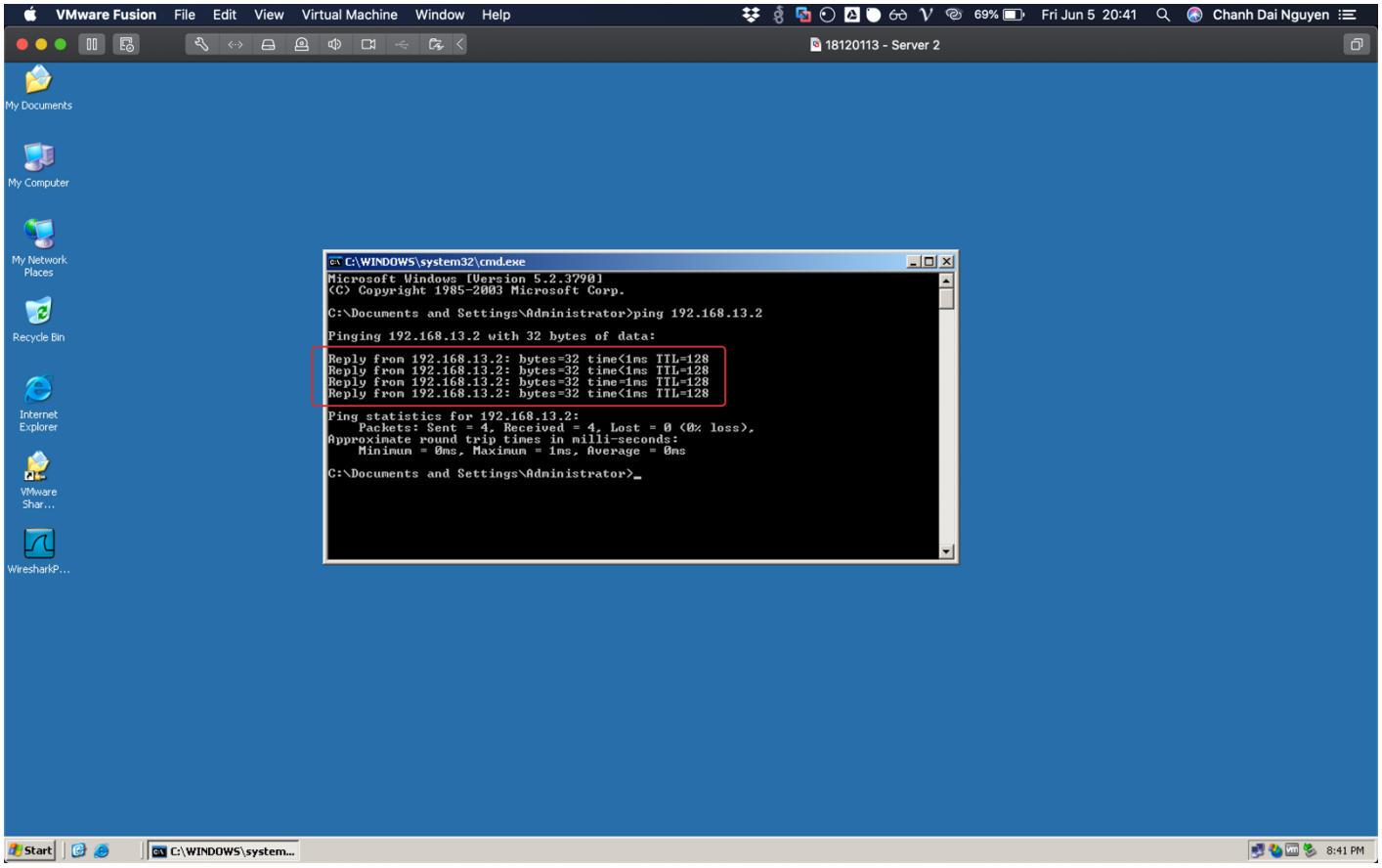
Thông tin Default Gateway và DNS Server nằm trong gói tin Offer và ACK.



Câu 4. Sử dụng 2 máy tính của bài tập 3, sau khi client đã có được thông tin TCP/IP được cấp phát với DHCP server, thực hiện các yêu cầu sau :

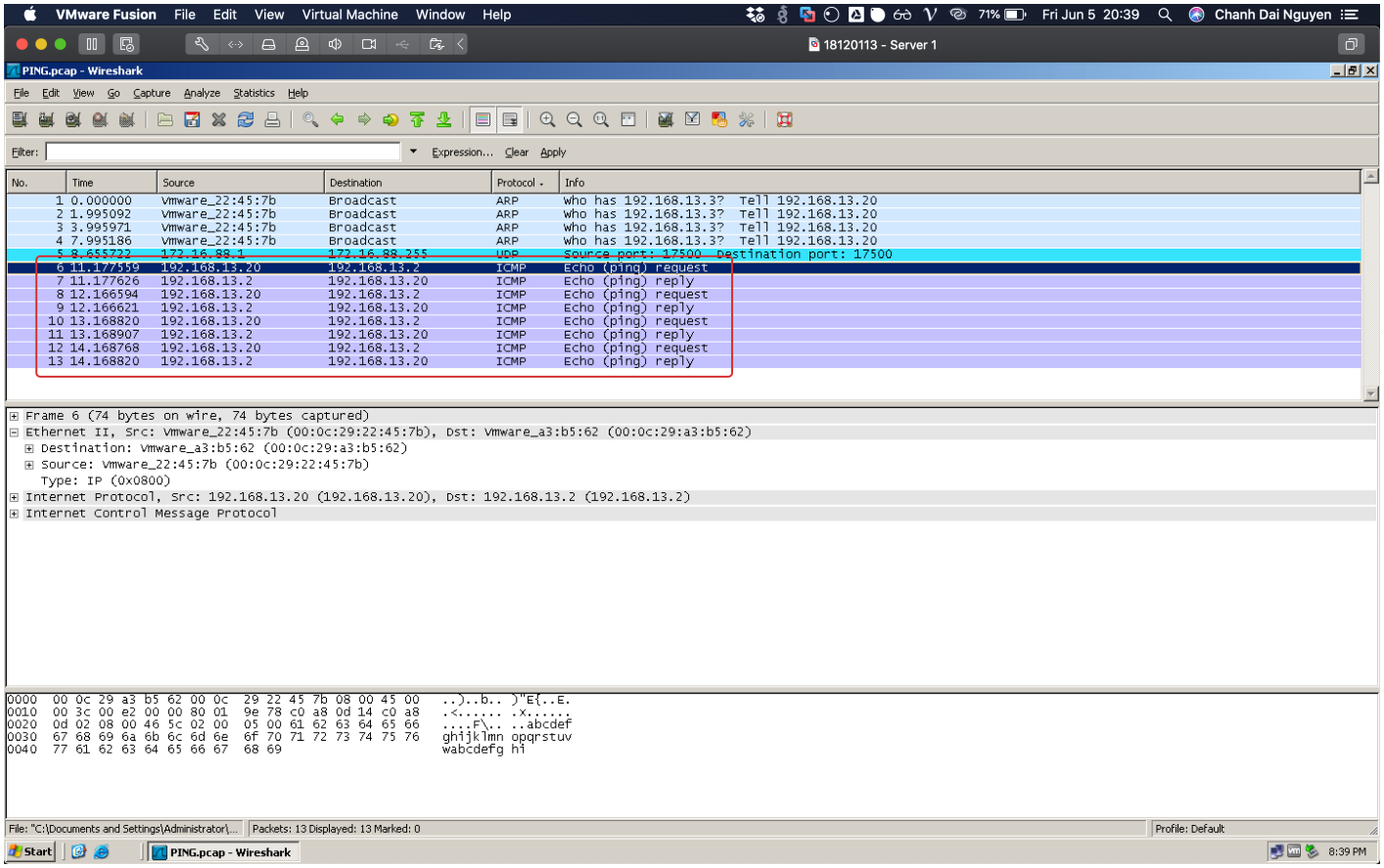
4 a. Thực hiện lệnh ping từ Client đến Server và dùng Wireshark để bắt các gói tin tương ứng.

Video quá trình thực hiện : https://youtu.be/XVpPsWX879w



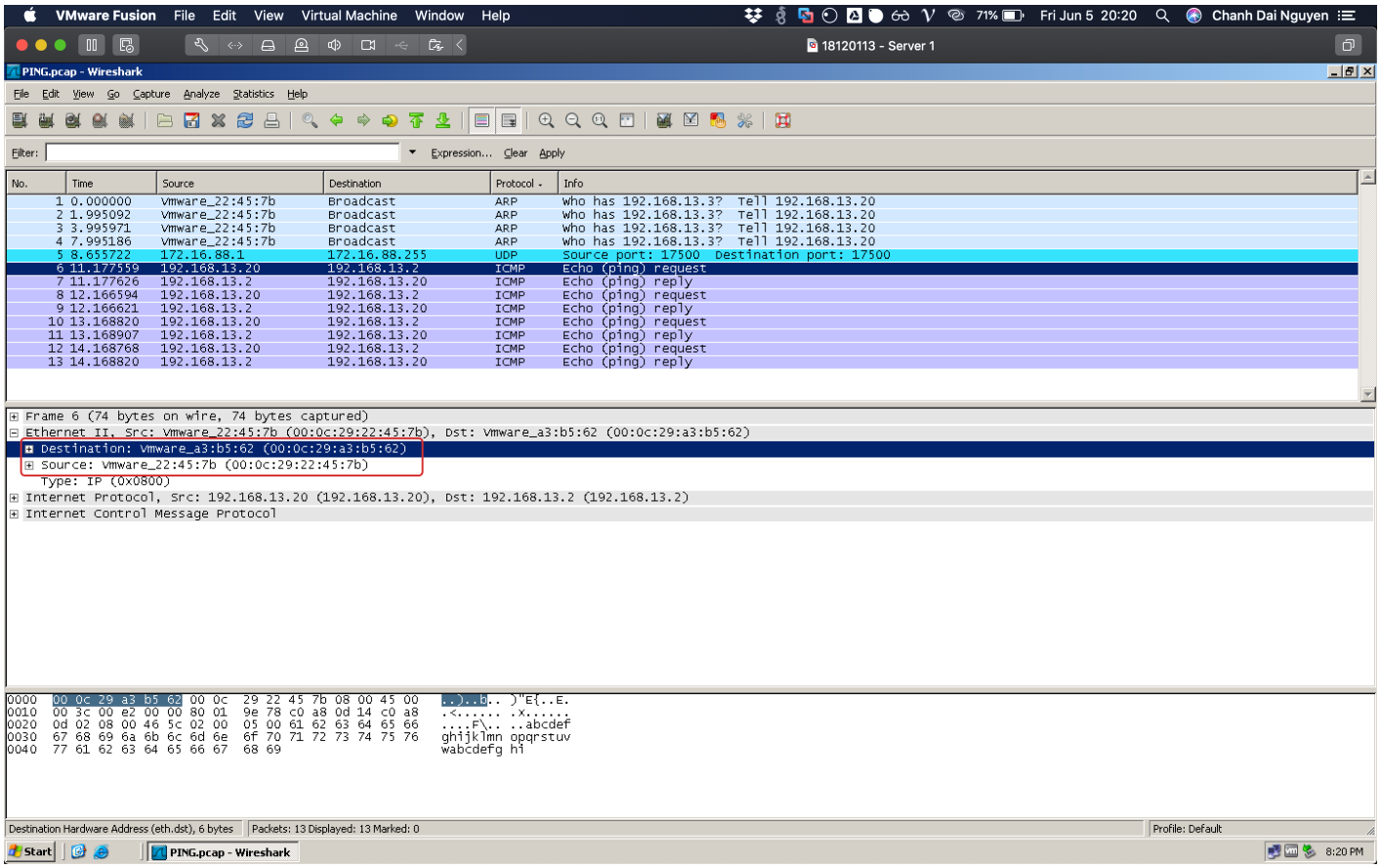
4 b. Cho biết có bao nhiêu gói tin của quá trình thực hiện lệnh ping ?

Có 8 gói tin của quá trình thực hiện lệnh ping.



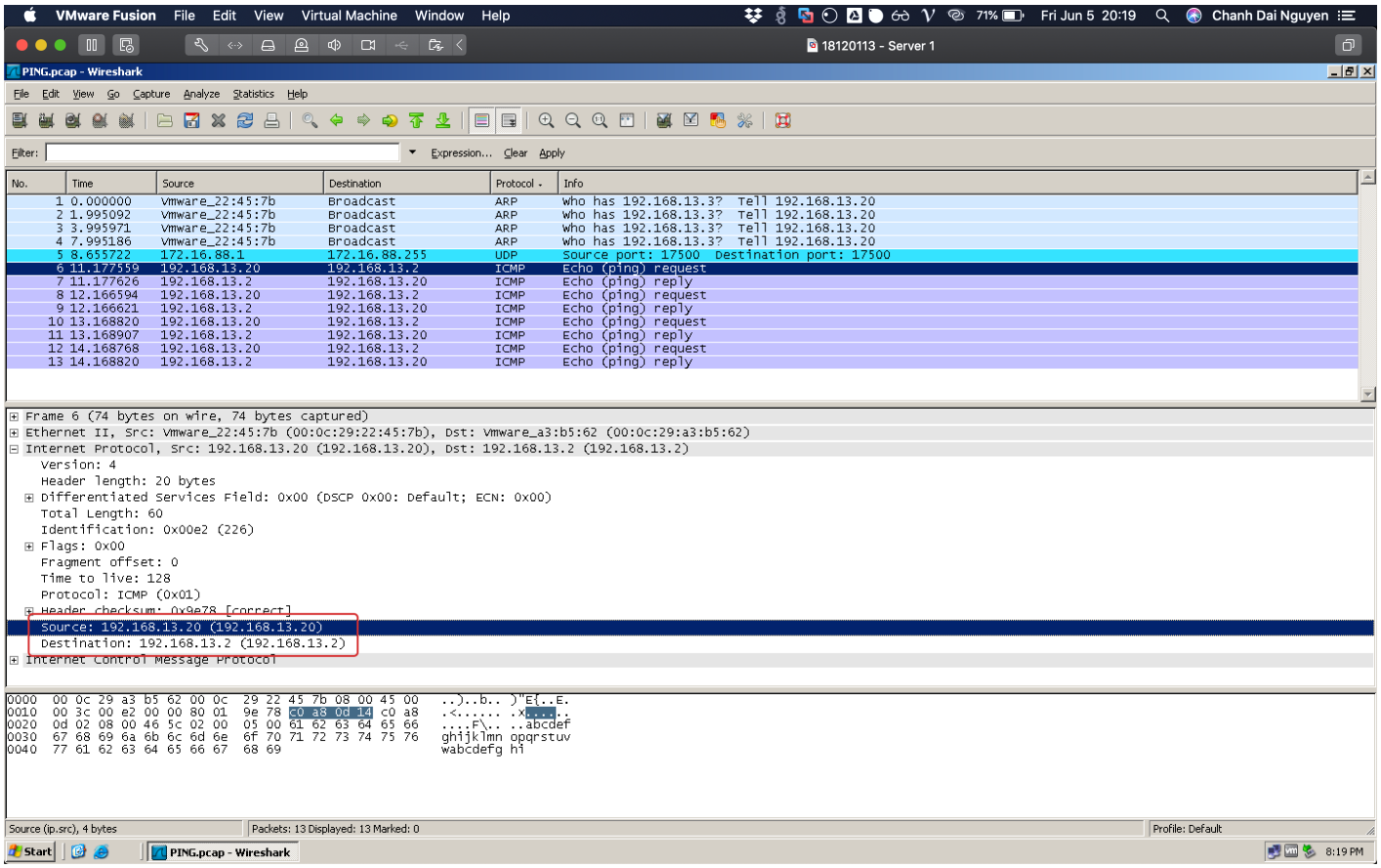
4 c. Địa chỉ MAC Nguồn, MAC Đích là gì ?

MAC Nguồn	MAC Đích
00:0c:29:22:45:7b	00:0c:29:a3:b5:62



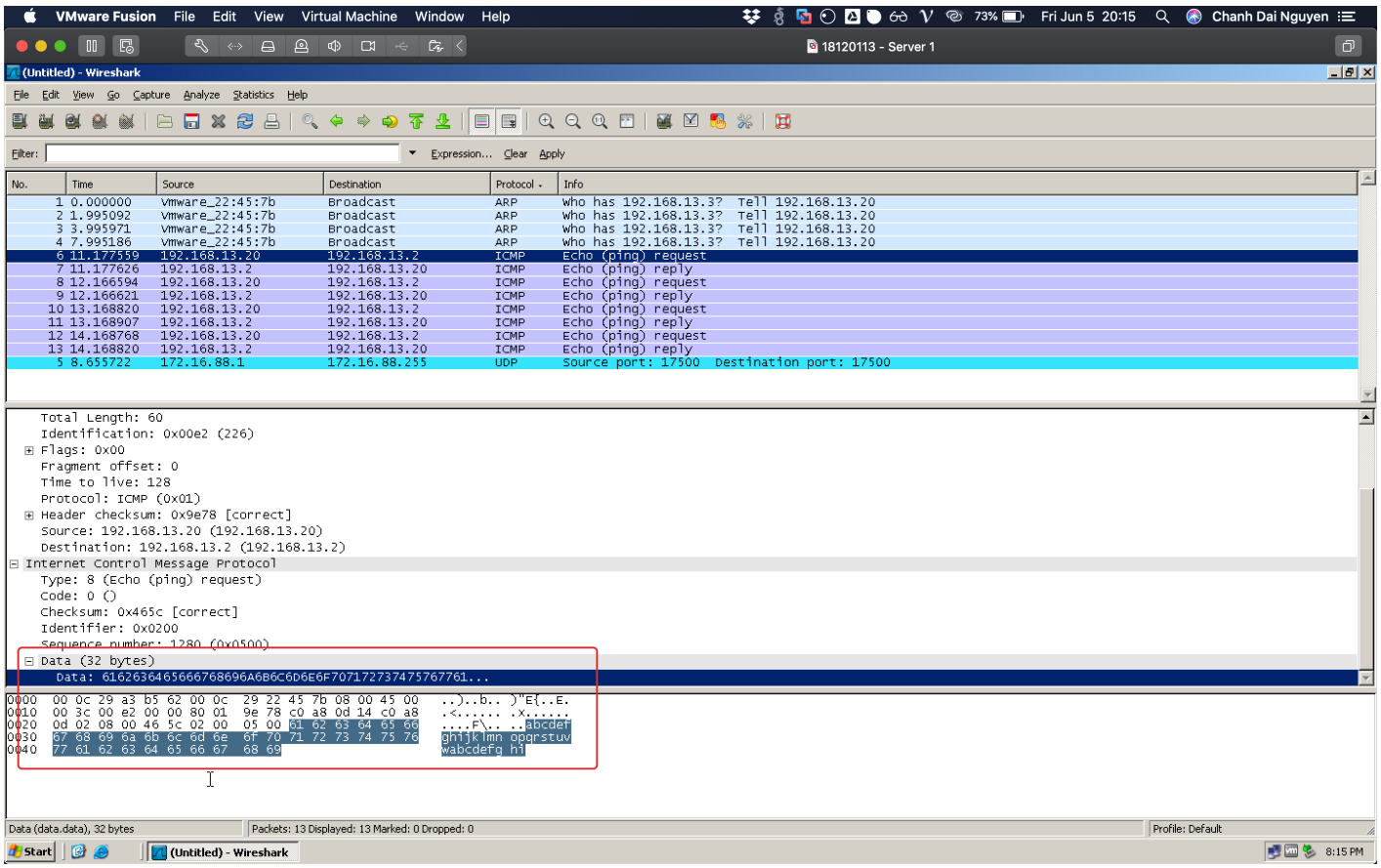
4 d. Địa chỉ IP Nguồn, IP Đích là gì ?

IP Nguồn	IP Đích
192.168.13.20	192.168.13.2



4 e. Nội dung phần data của gói tin ICMP là gì ?

Data của gói tin ICMP : 61626364656667686 96A6B6C6D6E6F707172737475767761...



--- Hết ---