

Họ và tên: Lê Hoài Nam

MSSV: 18120468

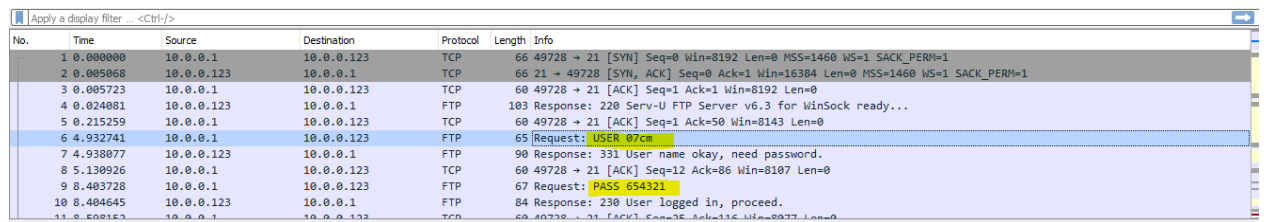
Lớp: 18CTT4

Bài tập thực hành Wireshark

Câu 1:

a. Username và password của người dùng là gì?

- User name: 07cm
- Password: 654321

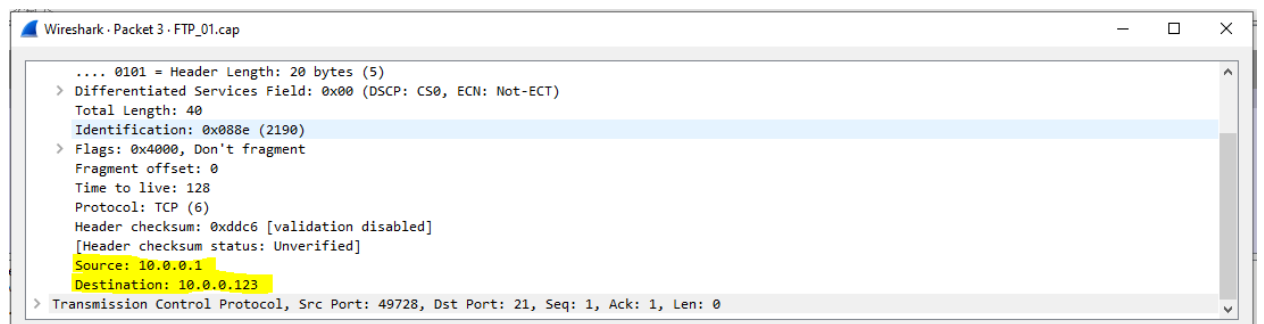


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.1	10.0.0.123	TCP	66	49728 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=1 SACK_PERM=1
2	0.005068	10.0.0.123	10.0.0.1	TCP	66	21 → 49728 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=1 SACK_PERM=1
3	0.005723	10.0.0.1	10.0.0.123	TCP	60	49728 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
4	0.024081	10.0.0.123	10.0.0.1	FTP	103	Response: 220 Serv-U FTP Server v6.3 for WinSock ready...
5	0.215259	10.0.0.1	10.0.0.123	TCP	60	49728 → 21 [ACK] Seq=1 Ack=50 Win=8143 Len=0
6	4.932741	10.0.0.1	10.0.0.123	FTP	65	Request: USER 07cm
7	4.938077	10.0.0.123	10.0.0.1	FTP	90	Response: 331 User name okay, need password.
8	5.130926	10.0.0.1	10.0.0.123	TCP	60	49728 → 21 [ACK] Seq=12 Ack=86 Win=8107 Len=0
9	8.403728	10.0.0.1	10.0.0.123	FTP	67	Request: PASS 654321
10	8.404645	10.0.0.123	10.0.0.1	FTP	84	Response: 230 User logged in, proceed.
11	8.600353	10.0.0.1	10.0.0.123	TCP	60	49728 → 21 [ACK] Seq=12 Ack=116 Win=8077 Len=0

Ghi chú: Hình ảnh sever nhận và kiểm tra user name và password

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

- Địa chỉ IP máy Client: 10.0.0.1
- Địa chỉ TP máy Sever: 10.0.0.123

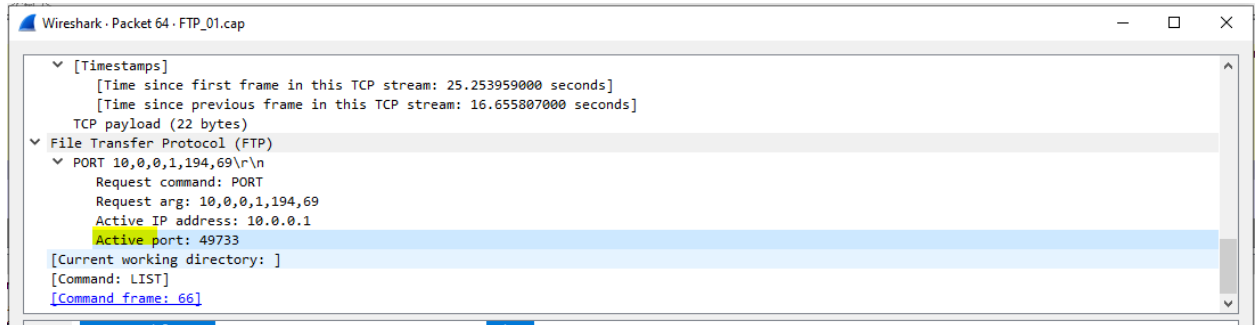


Wireshark · Packet 3 · FTP_01.cap
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x088e (2190)
> Flags: 0x4000, Don't fragment
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0xddc6 [validation disabled]
[Header checksum status: Unverified]
Source: 10.0.0.1
Destination: 10.0.0.123
> Transmission Control Protocol, Src Port: 49728, Dst Port: 21, Seq: 1, Ack: 1, Len: 0

Ghi chú: Hình ảnh giao tiếp giữa Sever và Client

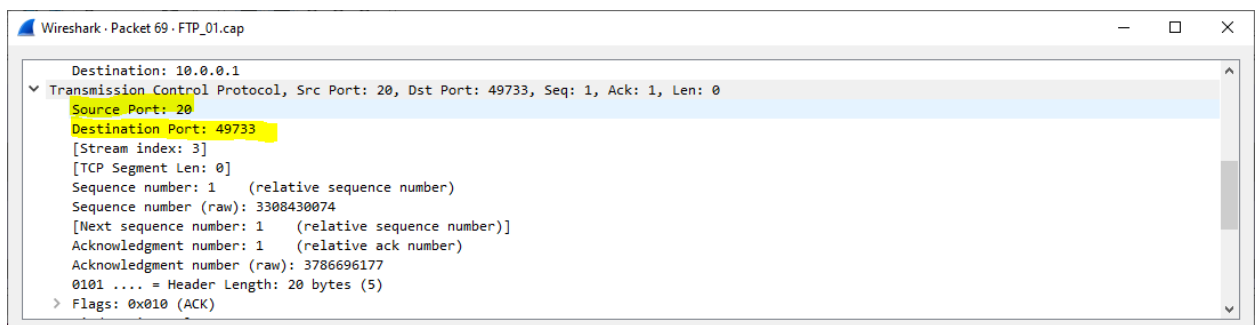
c. Client truy xuất lên Server theo mode nào: active hay passive?

- Client truy xuất lên Server theo mode : active



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

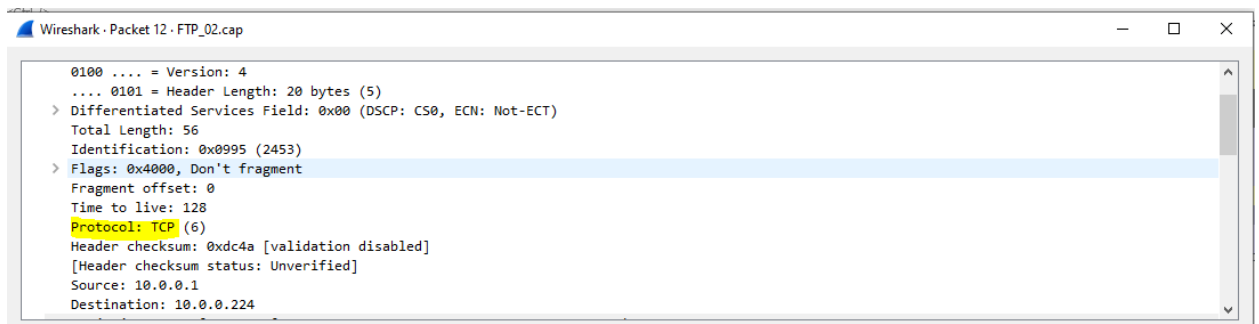
- Port truyền dữ liệu của FTP Server: 20
- Port truyền dữ liệu của FTP Client: 49733



Câu 2:

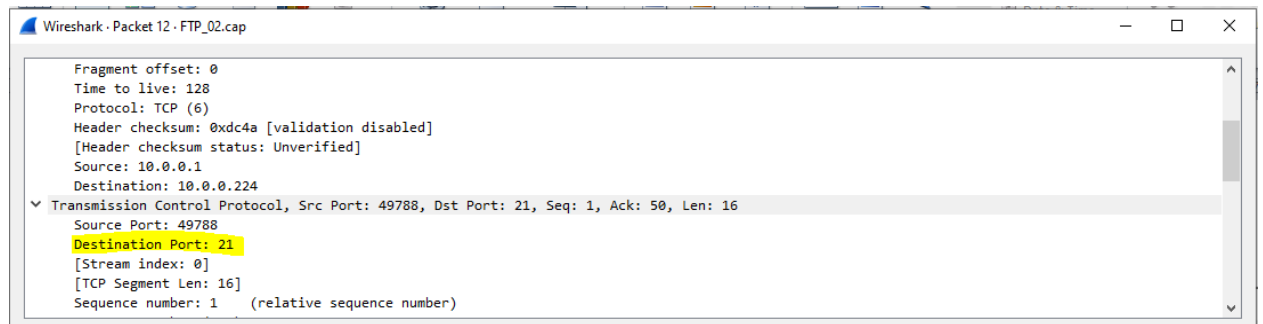
a. FTP sử dụng giao thức nào UDP hay TCP?

- FTP sử dụng giao thức TCP



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

- Port mặc định của FTP Server là: 21



c. Username và password của người dùng là gì?

- Username: cm07
- Password: 123654

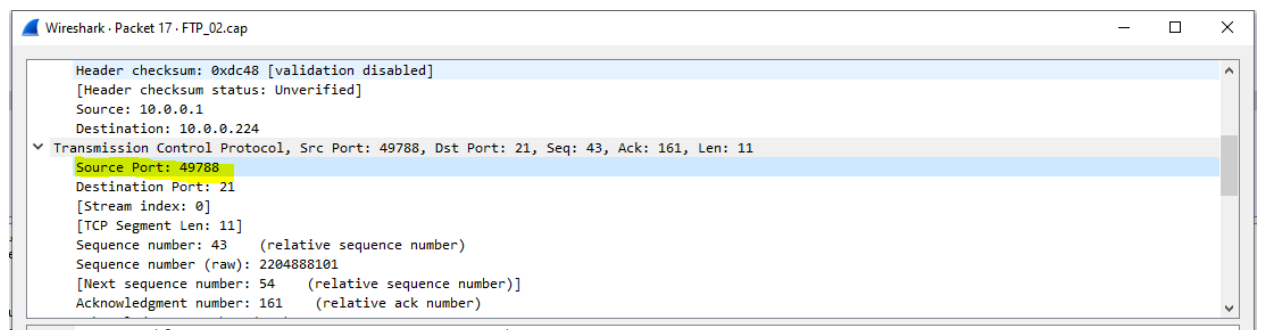
No.	Time	Source	Destination	Protocol	Length	Info
12	12.730270	10.0.0.1	10.0.0.224	FTP	70	Request: USER anonymous
13	12.731818	10.0.0.224	10.0.0.1	FTP	124	Response: 331 User name okay, please send complete E-mail address as password.
14	12.848222	10.0.0.1	10.0.0.224	FTP	80	Request: PASS mozilla@example.com
15	12.849323	10.0.0.224	10.0.0.1	FTP	95	Response: 530 Sorry, no ANONYMOUS access allowed.
16	13.077727	10.0.0.1	10.0.0.224	TCP	60	49788 → 21 [ACK] Seq=43 Ack=161 Win=65540 Len=0
17	21.836141	10.0.0.1	10.0.0.224	FTP	65	Request: USER cm07
18	21.837661	10.0.0.224	10.0.0.1	FTP	90	Response: 331 User name okay, need password.
19	21.905232	10.0.0.1	10.0.0.224	FTP	67	Request: PASS 123654
20	21.906163	10.0.0.224	10.0.0.1	FTP	84	Response: 230 User logged in, proceed.
21	21.935646	10.0.0.1	10.0.0.224	FTP	60	Request: SYST
22	21.936326	10.0.0.224	10.0.0.1	FTP	72	Response: 215 UNIX Type: L8

Ghi chú:

- Ban đầu client nhập username: anonymous và password: mozilla@example.com nhưng sever báo đăng nhập lỗi. Sau đó client gửi lại lần thứ 2 username: cm07 và pass 123654 thì thành công đăng nhập.

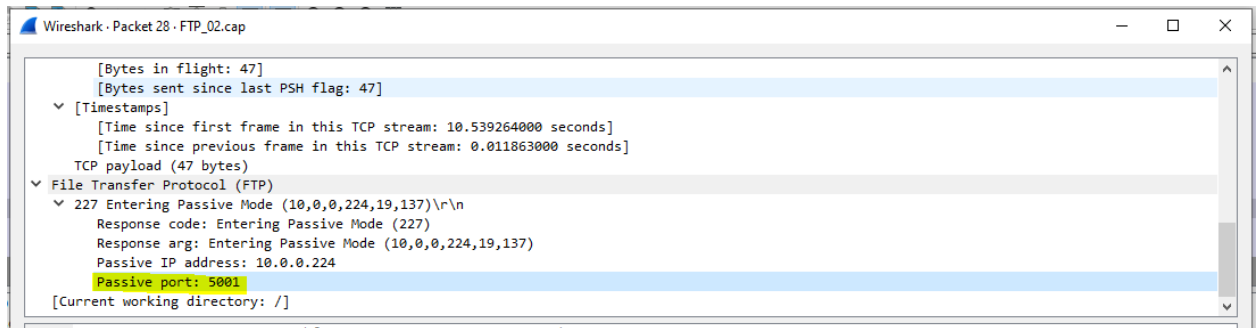
d. Port truyền lệnh của Client là bao nhiêu?

- Port truyền lệnh của Client là: 49788



e. Client truy xuất lên Server theo mode nào: active hay passive?

- Client truy xuất lên Server theo mode : passive



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.

- Bước 1: Client gửi username
- Bước 2: Sever phản hồi kết quả chấp nhận username mà Client đã gửi hay không. Nếu user name không hợp lệ thì quay lại bước 1. Nếu user name hợp lệ thì sever yêu cầu thêm password.
- Bước 3: Client gửi mật khẩu, Sever kiểm tra mật khẩu. Nếu password hợp lệ thì thông báo đăng nhập thành công. Nếu không hợp lệ thì quay lại bước 1.

The image shows a Wireshark packet capture window titled 'Apply a display filter ... <Ctrl-/>'. The packet list pane shows the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
12	12.730270	10.0.0.1	10.0.0.224	FTP	70	Request: USER anonymous
13	12.731818	10.0.0.224	10.0.0.1	FTP	124	Response: 331 User name okay, please send complete E-mail address as password.
14	12.848222	10.0.0.1	10.0.0.224	FTP	80	Request: PASS mozilla@example.com
15	12.849323	10.0.0.224	10.0.0.1	FTP	95	Response: 530 Sorry, no ANONYMOUS access allowed.
16	13.077727	10.0.0.1	10.0.0.224	TCP	60	49788 → 21 [ACK] Seq=43 Ack=161 Win=65540 Len=0
17	21.836141	10.0.0.1	10.0.0.224	FTP	65	Request: USER cm07
18	21.837661	10.0.0.224	10.0.0.1	FTP	90	Response: 331 User name okay, need password.
19	21.905232	10.0.0.1	10.0.0.224	FTP	67	Request: PASS 123654
20	21.906163	10.0.0.224	10.0.0.1	FTP	84	Response: 230 User logged in, proceed.
21	21.935646	10.0.0.1	10.0.0.224	FTP	60	Request: SYST
22	21.935646	10.0.0.224	10.0.0.1	FTP	72	Response: 215 UNIX Type: L8

Ghi chú:

- Hình ảnh trên ghi lại quá trình client gửi username và password lên sever.
- Ban đầu client nhập username: anonymous và password: mozilla@example.com nhưng sever báo đăng nhập lỗi. Sau đó client gửi lại lần thứ 2 username: cm07 và pass 123654 thì thành công đăng nhập.

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

- Bước 1: Client gửi một gói tin SYN đến Sever
- Bước 2: Sever nhận gói tin SYN, rồi gửi lại gói SYS-ACK cho Client
- Bước 3: Client nhận gói SYS-ACK, rồi sau đó gửi lại gói ACK thông báo đồng ý tạo kết nối.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.1	10.0.0.255	NBNS	92	Name query NB 172.29.64.158<20>
2	0.717986	10.0.0.1	10.0.0.255	NBNS	92	Name query NB 172.29.64.158<20>
3	1.499686	10.0.0.1	10.0.0.255	NBNS	92	Name query NB 172.29.64.158<20>
4	10.665285	10.0.0.1	10.0.0.255	NBNS	92	Name query NB 172.29.70.4<20>
5	11.415885	10.0.0.1	10.0.0.255	NBNS	92	Name query NB 172.29.70.4<20>
6	11.428823	10.0.0.1	10.0.0.224	TCP	66	49788 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
7	11.428985	10.0.0.224	10.0.0.1	TCP	66	21 → 49788 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=1 SACK_PERM=1
8	11.429211	10.0.0.1	10.0.0.224	TCP	60	49788 → 21 [ACK] Seq=1 Ack=1 Win=65700 Len=0
9	11.431999	10.0.0.224	10.0.0.1	FTP	103	Response: 220 Serv-U FTP Server v6.3 for WinSock ready...
10	11.615330	10.0.0.1	10.0.0.224	TCP	60	49788 → 21 [ACK] Seq=1 Ack=50 Win=65648 Len=0
11	12.103285	10.0.0.1	10.0.0.255	NBNS	92	Name query NB 172.29.70.4<20>

- Ghi chú: Hình ảnh giao tiếp giữa Client và Sever

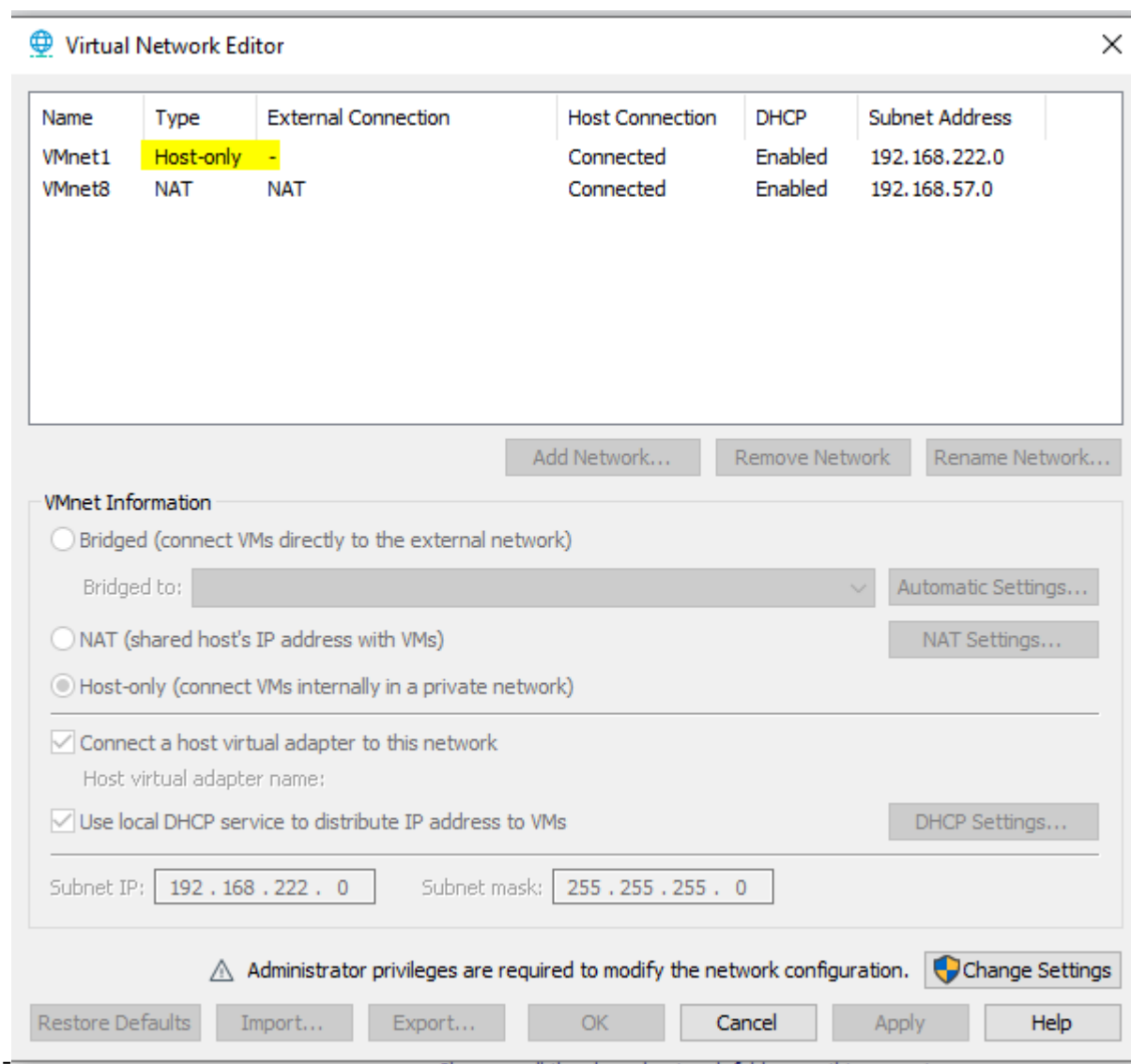
h. Port truyền dữ liệu của FTP Server và Client là bao nhiêu?

- Port truyền dữ liệu của FTP Server: 21
- Port truyền dữ liệu của FTP Client: 49788

Wireshark · Packet 58 · FTP_02.cap	
Header checksum: 0xdc3e [validation disabled] [Header checksum status: Unverified] Source: 10.0.0.1 Destination: 10.0.0.224	
Transmission Control Protocol, Src Port: 49788, Dst Port: 21, Seq: 135, Ack: 549, Len: 0	
Source Port: 49788 Destination Port: 21 [Stream index: 0] [TCP Segment Len: 0] Sequence number: 135 (relative sequence number) Sequence number (raw): 2204888193 [Next sequence number: 135 (relative sequence number)] Acknowledgment number: 549 (relative ack number)	

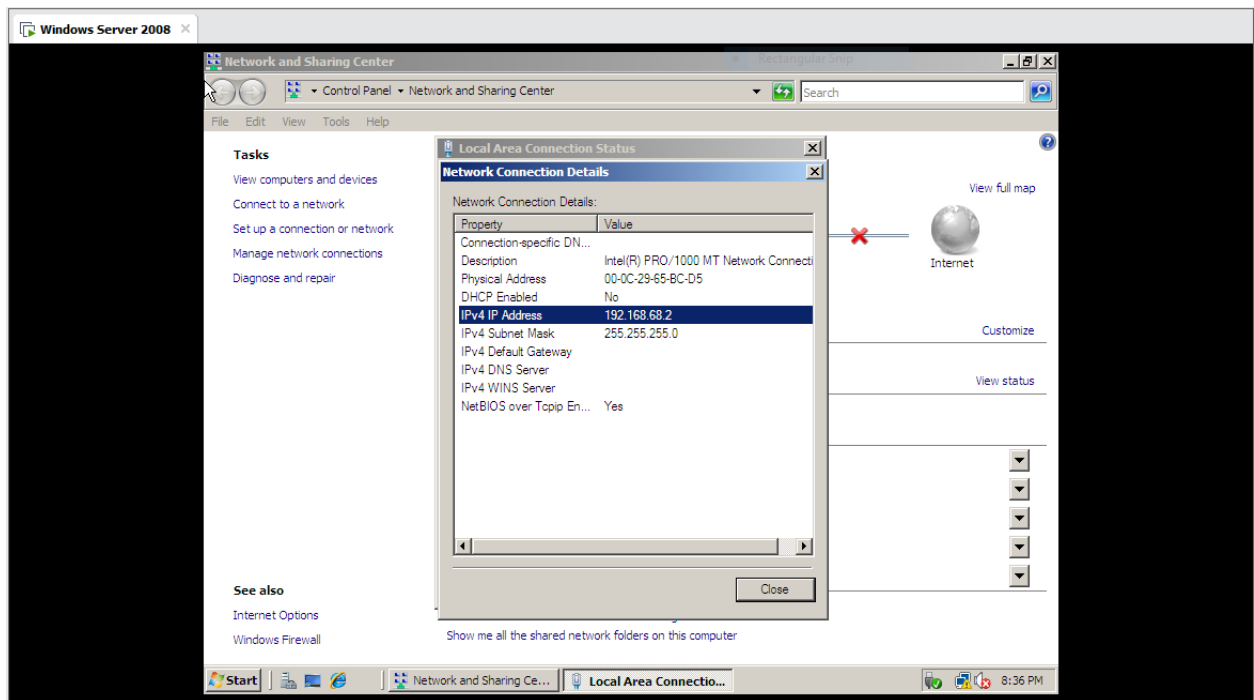
Câu 3:

- 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.



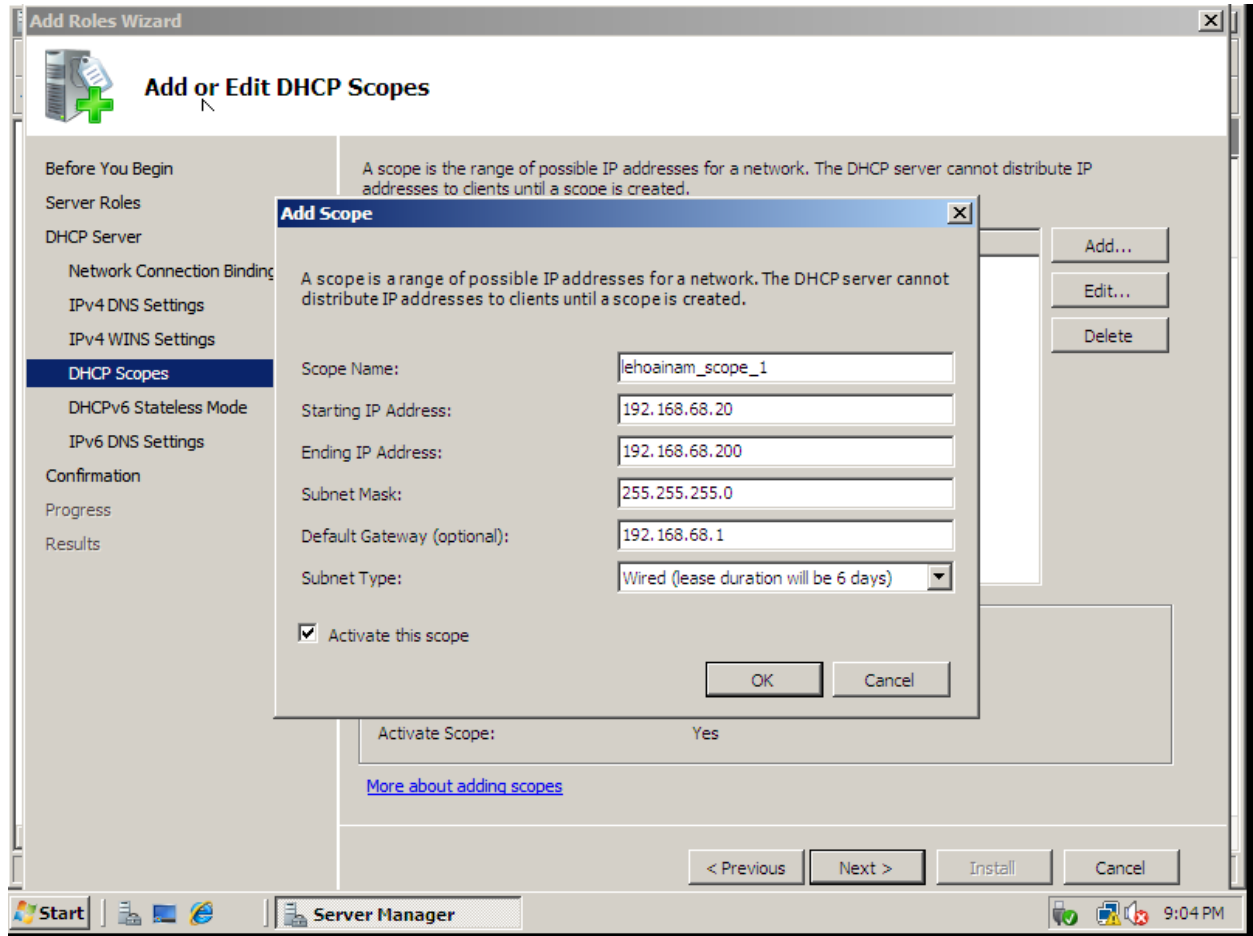
Ghi chú: Hình ảnh thể hiện đã thiết lập card mạng của máy ảo là host only

- 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. Ví dụ: MSSV = 1812123 \rightarrow X = 23.



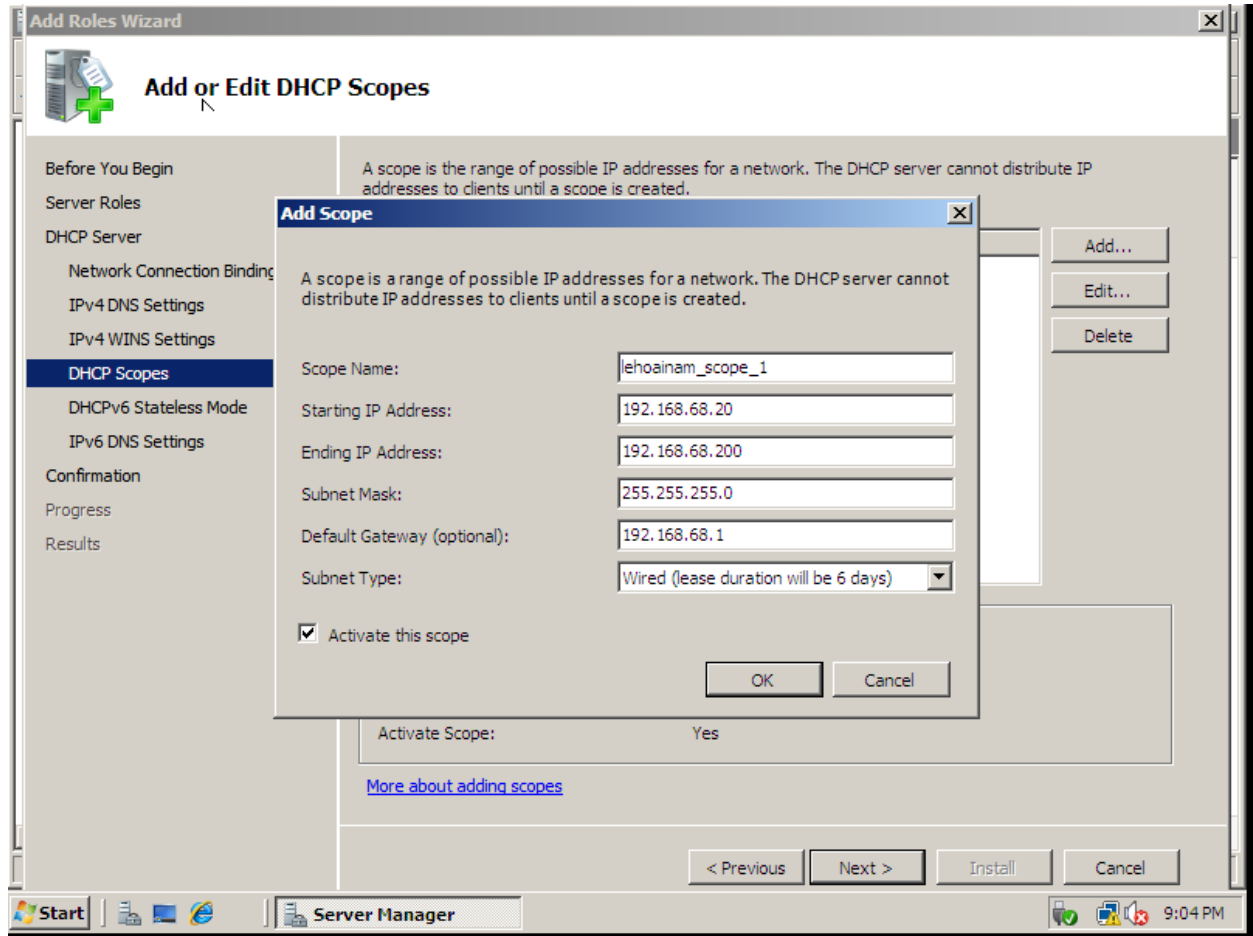
Ghi chú: Hình ảnh về cấu hình mạng của máy ảo làm DHCP Sever

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



Ghi chú: Hình ảnh các khoảng địa chỉ IP cung cấp cho các Client

e. Default gateway cung cấp cho các clients: 192.168.X.1



Ghi chú: Default Gateway cung cấp cho các Client

f. DNS server cung cấp cho các clients: 192.168.X.3

Add Roles Wizard

Specify IPv4 DNS Server Settings

When clients obtain an IP address from the DHCP server, they can be given DHCP options such as the IP addresses of DNS servers and the parent domain name. The settings you provide here will be applied to clients using IPv4.

Specify the name of the parent domain that clients will use for name resolution. This domain will be used for all scopes you create on this DHCP server.

Parent Domain:

Specify the IP addresses of the DNS servers that clients will use for name resolution. These DNS servers will be used for all scopes you create on this DHCP server.

Preferred DNS Server IPv4 Address:

Alternate DNS Server IPv4 Address:

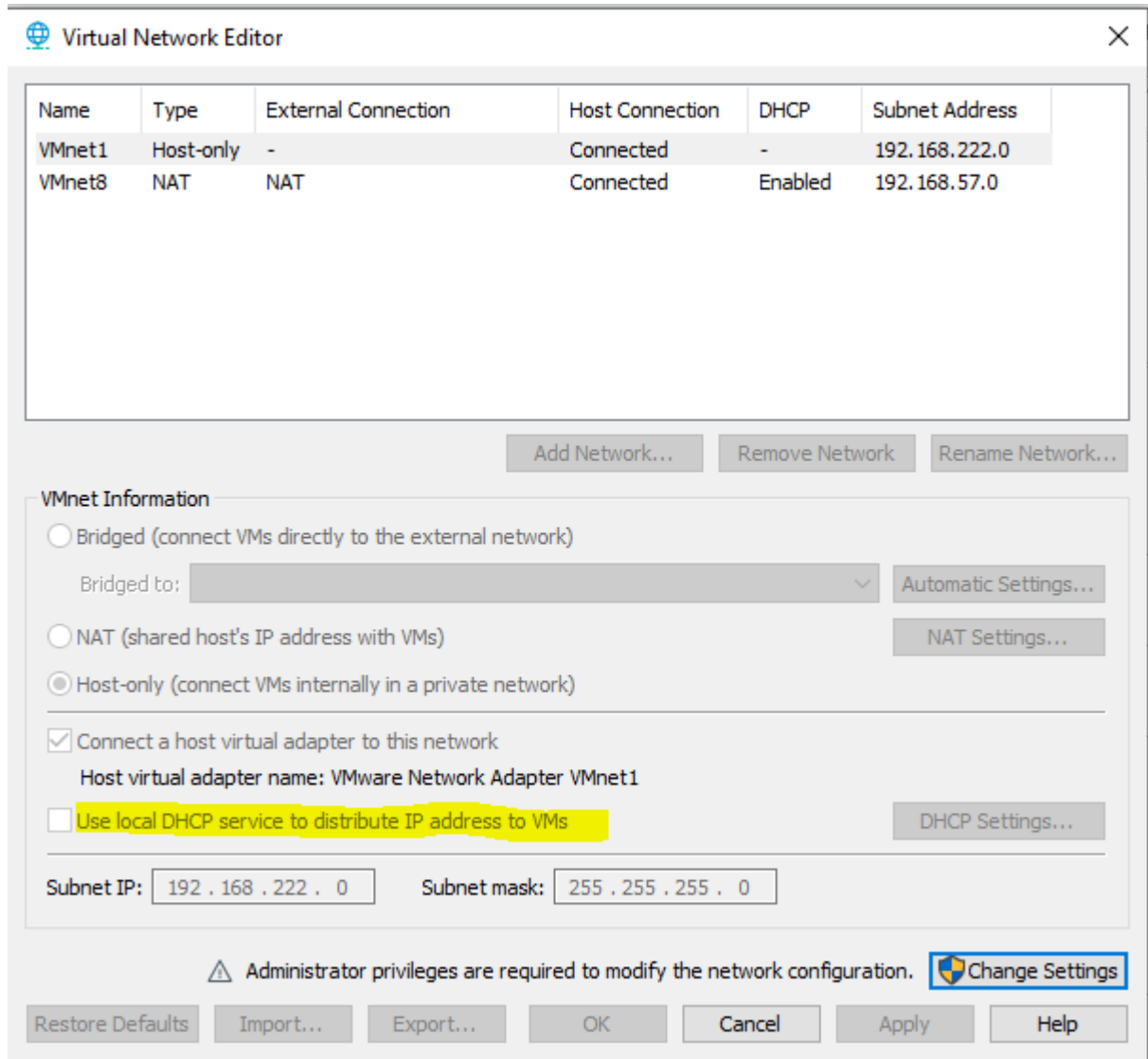
[More about DNS server settings](#)

< Previous Next > Install Cancel

Start Server Manager 8:57 PM

Ghi chú: DSN Sever

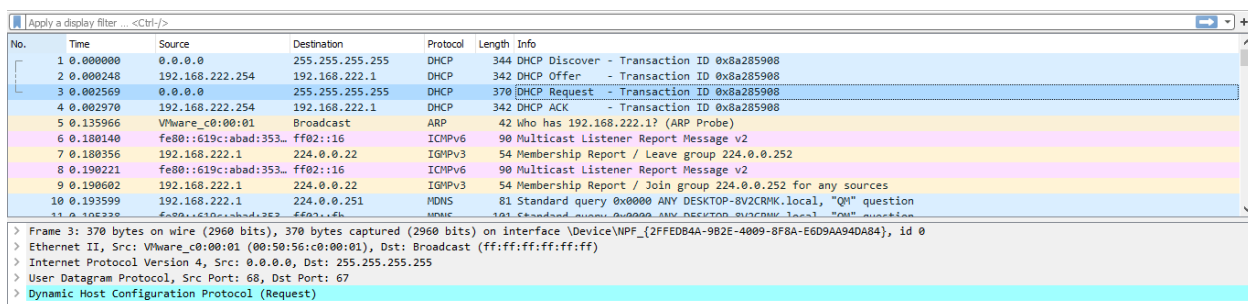
h, Tắt tính năng DHCP của phần mềm VMWare



Ghi chú: Hình ảnh thể hiện tắt tính năng DHCP của phần mềm VMWare

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

- 4 gói tin (discover, offer, request, ACK)

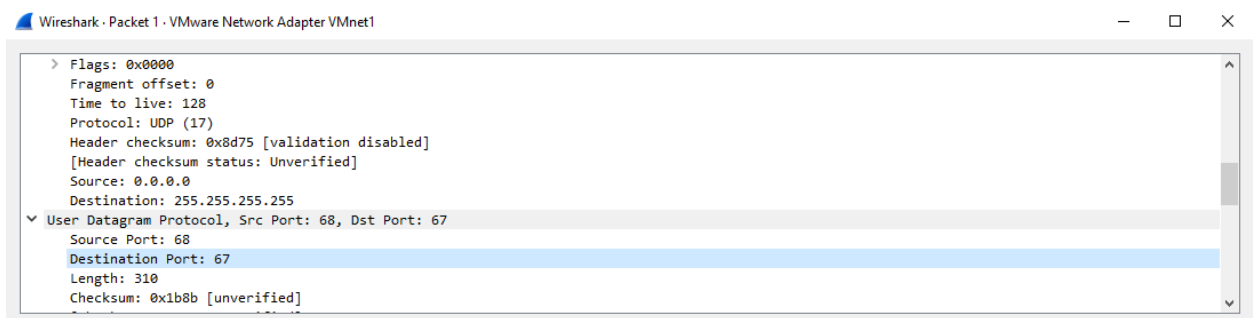


Ghi chú: Hình ảnh wireshark bắt được

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?

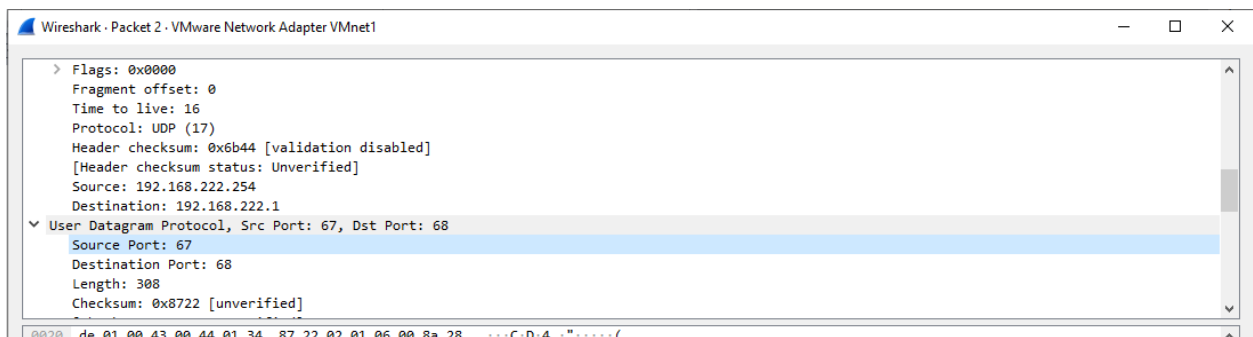
Gồm 4 gói tin:

- Gói tin discover:
 - + IP nguồn: 0.0.0.0
 - + IP đích: 255.255.255.255
 - + MAC nguồn:
 - + MAC đích:
 - + Port nguồn: 68
 - + Port đích: 67



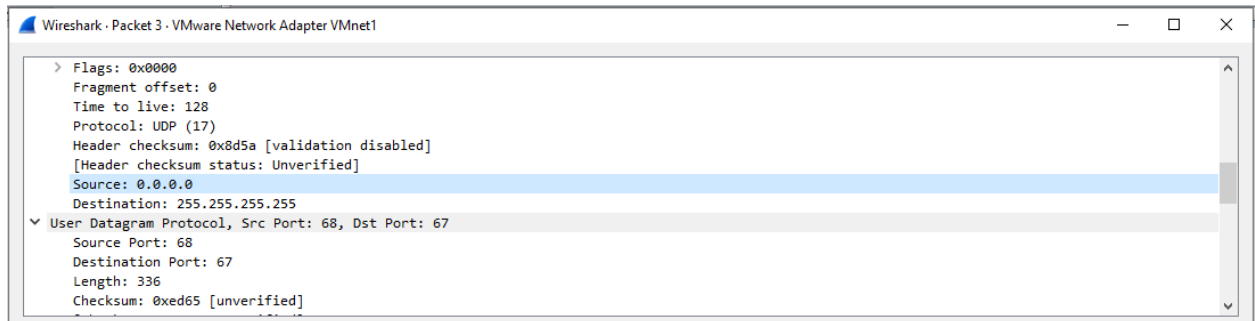
Ghi chú: Hình ảnh bắt gói tin discover

- Gói tin Offer:
 - + IP nguồn: 192.168.222.254
 - + IP đích: 192.168.222.1
 - + MAC nguồn:
 - + MAC đích:
 - + Port nguồn: 67
 - + Port đích: 68



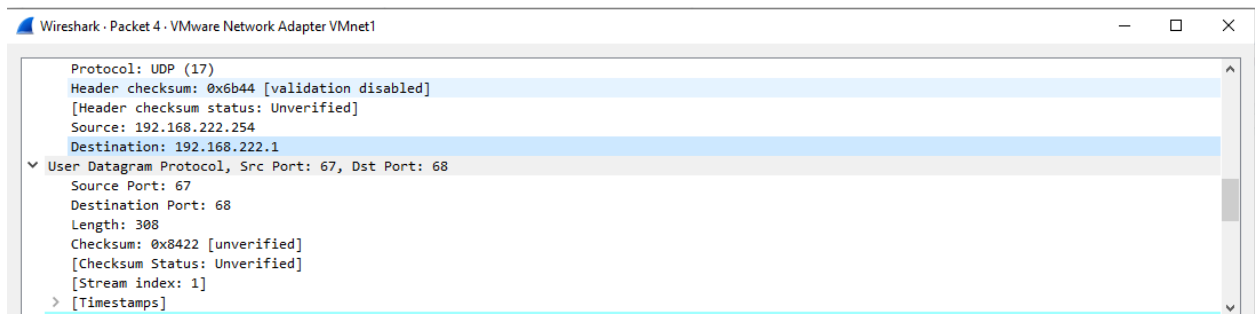
Ghi chú: Hình ảnh bắt gói tin offer

- Gói tin request:
 - + IP nguồn: 0.0.0.0
 - + IP đích: 255.255.255.255
 - + MAC nguồn:
 - + MAC đích:
 - + Port nguồn: 68
 - + Port đích: 67



Ghi chú: Hình ảnh bắt gói tin request

- Gói tin ACK:
 - + IP nguồn: 192.168.222.254
 - + IP đích: 192.168.222.1
 - + MAC nguồn:
 - + MAC đích:
 - + Port nguồn: 67
 - + Port đích: 68



Ghi chú: Hình ảnh bắt gói tin ACK