

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH ĐẠI
HỌC KHOA HỌC TỰ NHIÊN
KHOA CÔNG NGHỆ THÔNG TIN
BỘ MÔN MẠNG MÁY TÍNH



BÁO CÁO BÀI TẬP
THỰC HÀNH
WIRESHARK

Lớp: Mạng máy tính - CQ2018/1
Họ tên sinh viên: Lê Nhật Nam
MSSV: 18120061

Bài tập thực hành Wireshark

MSSV: 18120061

Họ và tên: Lê Nhựt Nam

Lớp: 18CTT1

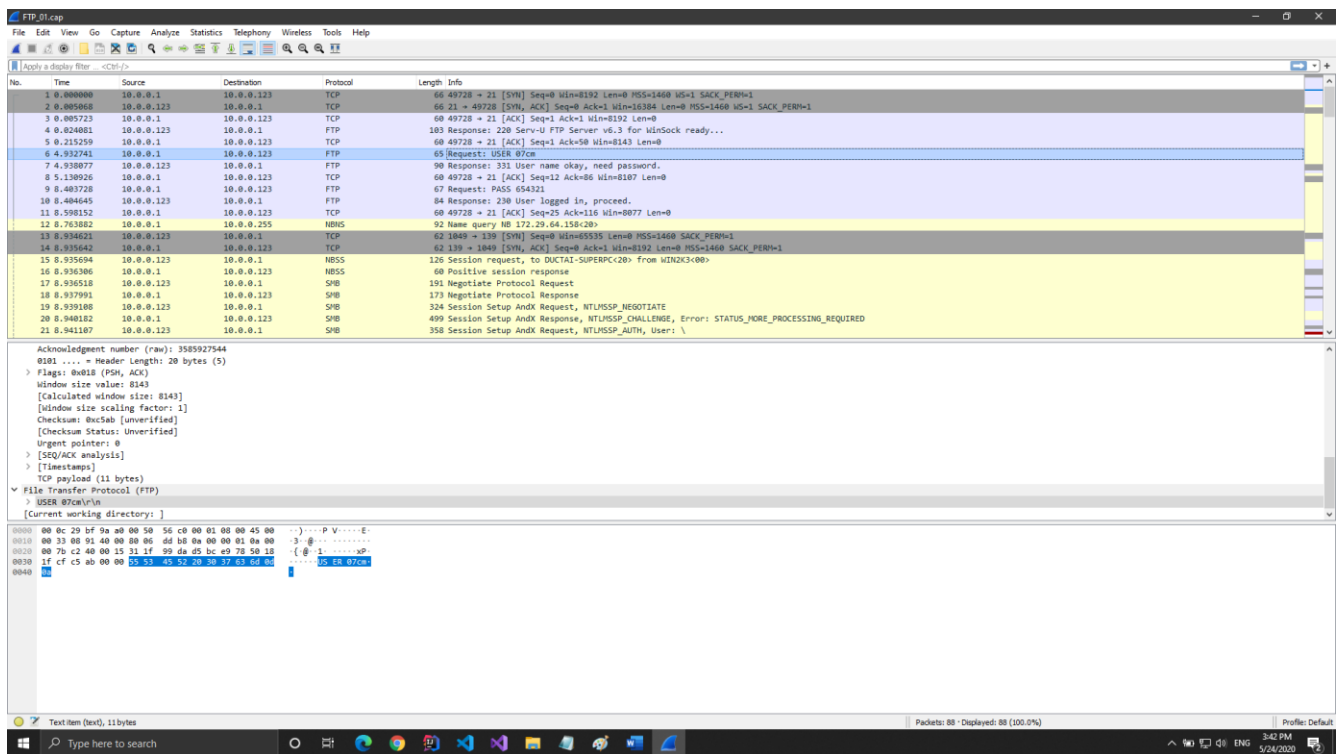
Lưu ý:

- 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:

- a. Username và password của người dùng là gì?
- b. Địa chỉ IP máy Client và máy Server là gì?
- c. Client truy xuất lên Server theo mode nào: active hay passive?
- d. Port truyền dữ liệu của FTP Server và Client là bao nhiêu?

[Trả lời]



a) Username và password của người dùng

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.

File Transfer Protocol (FTP)

USER 07cm\r\n

Request command: USER

Request arg: 07cm

[Current working directory:]

```

0000  00 0c 29 bf 9a a0 00 50 56 c0 00 01 08 00 45 00  ..)....P V....E.
0010  00 33 08 91 40 00 80 06 dd b8 0a 00 00 01 0a 00  3..@.....
0020  00 7b c2 40 00 15 31 1f 99 da d5 bc e9 78 50 18  .{..@..1.....xP.
0030  1f cf c5 ab 00 00 55 53 45 52 20 30 37 63 6d 0d  ....US ER 07cm.
0040  0a
  
```

Vậy -> Username: 07cm

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.

```

File Transfer Protocol (FTP)
  PASS 654321\r\n
    Request command: PASS
    Request arg: 654321
  [Current working directory: ]

```

0000	00 0c 29 bf 9a a0 00 50	56 c0 00 01 08 00 45 00	..)....P V....E.
0010	00 35 08 93 40 00 80 06	dd b4 0a 00 00 01 0a 00	5..@...
0020	00 7b c2 40 00 15 31 1f	99 e5 d5 bc e9 9c 50 18	{..@..1.P.
0030	1f ab c7 a6 00 00 50 41	53 53 20 36 35 34 33 32PA SS 65432
0040	31 0d 0a		1..

Vậy -> Password: 654321

b) Địa chỉ IP máy Client và máy Server

```

Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.123
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 52
  Identification: 0x088d (2189)
  > Flags: 0x4000, Don't fragment
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (6)
  Header checksum: 0xddbb [validation disabled]
  [Header checksum status: Unverified]
  Source: 10.0.0.1

```

0000	00 0c 29 bf 9a a0 00 50	56 c0 00 01 08 00 45 00	..)....P V....E.
0010	00 34 08 8d 40 00 80 06	dd bb 0a 00 00 01 0a 00	4..@...
0020	00 7b c2 40 00 15 31 1f	99 d9 00 00 00 00 80 02	{..@..1.
0030	20 00 ad 4e 00 00 02 04	05 b4 01 03 03 00 01 01	..N....
0040	04 02		..

Địa chỉ IP máy Client (Client IP Address): 10.0.0.1

Địa chỉ IP máy Server (Server IP Address): 10.0.0.123

c) Client truy xuất lên Server theo mode: Active

64	25.253959	10.0.0.1	10.0.0.123	FTP	76 Request: PORT 10,0,0,1,194,69
65	25.254698	10.0.0.123	10.0.0.1	FTP	84 Response: 200 PORT Command successful.
66	25.257566	10.0.0.1	10.0.0.123	FTP	60 Request: LIST
67	25.260044	10.0.0.123	10.0.0.1	TCP	62 20 → 49733 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
68	25.260306	10.0.0.1	10.0.0.123	TCP	62 49733 → 20 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1

Client lắng nghe tại port 49728 và cmd tới port 21 của FTP Sever

FTP Sever từ port 21 gửi ACK đến port 49728 của Client

➔ Nên Client đang truy xuất lên Server theo mode active

d) Port truyền dữ liệu của FTP Server và Client

64	25.253959	10.0.0.1	10.0.0.123	FTP	76 Request: PORT 10,0,0,1,194,69
65	25.254698	10.0.0.123	10.0.0.1	FTP	84 Response: 200 PORT Command successful.
66	25.257566	10.0.0.1	10.0.0.123	FTP	60 Request: LIST

File Transfer Protocol (FTP)

PORT 10,0,0,1,194,69\r\n

Request command: PORT

Request arg: 10,0,0,1,194,69

Active IP address: 10.0.0.1

Active port: 49733

[Current working directory:]

[Command: LIST]

[Command frame: 66]

0000	00 0c 29 bf 9a a0 00 50 56 c0 00 01 08 00 45 00	..)....P V.....E.
0010	00 3e 08 b5 40 00 80 06 dd 89 0a 00 00 01 0a 00	.>...@...
0020	00 7b c2 40 00 15 31 1f 99 f2 d5 bc e9 ba 50 18	.{. @...1.P.
0030	1f 8d 01 a1 00 00 50 4f 52 54 20 31 30 2c 30 2cPO RT 10,0,
0040	30 2c 31 2c 31 39 34 2c 36 39 0d 0a	0,1,194, 69...

File Transfer Protocol (FTP)

200 PORT Command successful.\r\n

Response code: Command okay (200)

Response arg: PORT Command successful.

[Current working directory:]

0000	00 50 56 c0 00 01 00 0c 29 bf 9a a0 08 00 45 00	.PV.....).....E.
0010	00 46 04 b3 00 00 80 06 21 84 0a 00 00 7b 0a 00	.F..... !.....{..
0020	00 01 00 15 c2 40 d5 bc e9 ba 31 1f 9a 08 50 18@... ..1...P.
0030	44 42 4d 34 00 00 32 30 30 20 50 4f 52 54 20 43	DBM4...20 0 PORT C
0040	6f 6d 6d 61 6e 64 20 73 75 63 63 65 73 73 66 75	ommand s successfu
0050	6c 2e 0d 0a	l...

Port truyền dữ liệu của FTP Server: 20

Port truyền dữ liệu của Client: 49733

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

- FTP sử dụng giao thức nào UDP hay TCP?
- Port mặc định của FTP Server để nhận kết nối là bao nhiêu?
- Username và password của người dùng là gì?
- Port truyền lệnh của Client là bao nhiêu?
- Client truy xuất lên Server theo mode nào: active hay passive?
- 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.
- Chỉ ra quá trình bắt tay 3 bước của Client và Server để tạo kết nối truyền dữ liệu.

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

[Trả lời]

The image shows a Wireshark packet capture of an FTP session. The packet list on the left shows several Name Query (NB) packets from 10.0.0.1 to 10.0.0.255, followed by a TCP Reset (RST) packet from 10.0.0.255 to 10.0.0.1. The packet details pane on the right shows the structure of the captured packets, including Ethernet II, Internet Protocol Version 4, and User Datagram Protocol. The packet bytes pane at the bottom shows the raw data of the captured packets, including the Ethernet II header and the User Datagram Protocol header.

FTP_02.cap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl>F

No.	Time	Source	Destination	Protocol	Length	Info
1	0.800000	10.0.0.1	10.0.0.255	NBNS	92	Name query NB 172.29.64.158(20)
2	0.717906	10.0.0.1	10.0.0.255	NBNS	92	Name query NB 172.29.64.158(20)
3	1.499606	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	11.415805	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	10.0.0.255	TCP	60	49788 → 21 [SYN] Seq=0 Win=0 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=65780 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	12.192785	10.0.0.1	10.0.0.255	NBNS	92	Name query NB 172.29.70.4(20)
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 mcilla@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	21.836143	10.0.0.1	10.0.0.224	FTP	65	Request: USER cm87
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

Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
Ethernet II, Src: VMware_c8:00:01:00:50:56(c8:00:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Address: Broadcast (ff:ff:ff:ff:ff:ff)
...1. = 1G bit: Locally administered address (this is NOT the factory default)
...1. = 2G bit: Group address (multicast/broadcast)
Source: VMware_c8:00:01:00:50:56(c8:00:01)
Address: VMware_c8:00:01:00:50:56(c8:00:01)
...0. = 1G bit: Globally unique address (factory default)
...0. = 2G bit: Individual address (unicast)
Type: IPv4 (0x0000)
Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.255
User Datagram Protocol, Src Port: 1337, Dst Port: 137
NetBIOS Name Service

0000 ff ff ff ff ff 00 56 c8 00 01 00 00 45 00P.V....E-
0010 00 4e 09 8a 00 00 11 1c 16 0a 00 00 01 0a 00N.....
0020 00 ff 00 09 00 09 0a 40 72 83 85 01 10 00 01I.....
0030 00 00 00 00 00 20 44 42 44 48 44 43 43 4f 44D.BOHDCOD
0040 43 44 4a 43 4f 44 47 44 45 43 4f 44 42 44 44CDXCDDD ECDORPD
0050 40 43 41 43 41 43 00 00 20 00 01ZCAGCA

Packets: 60 · Displayed: 60 (100.0%) Profile: Default

4:32 PM 5/24/2020

a) FTP sử dụng TCP

Internet Protocol Version 4, Src: 10.0.0.224, Dst: 10.0.0.1
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 89
 Identification: 0x0570 (1392)
 > Flags: 0x0000
 Fragment offset: 0
 Time to live: 128
 Protocol: TCP (6)
 Header checksum: 0x204f [validation disabled]
 [Header checksum status: Unverified]
 Source: 10.0.0.224
 Destination: 10.0.0.1
 > Transmission Control Protocol, Src Port: 21, Dst Port: 49788, Seq: 1, Ack: 1, Len: 49
 > File Transfer Protocol (FTP)
 [Current working directory:]

0000	00 50 56 c0 00 01 00 0c	29 bf 9a a0 08 00 45 00	·PV·····)·····E·
0010	00 59 05 70 00 00 80 06	20 4f 0a 00 00 e0 0a 00	·Y·p·····O·····
0020	00 01 00 15 c2 7c 14 e1	bf 70 83 6b eb fb 50 18	····· ···p·k··P·
0030	44 70 52 30 00 00 32 32	30 20 53 65 72 76 2d 55	DpR0··22 0 Serv-U
0040	20 46 54 50 20 53 65 72	76 65 72 20 76 36 2e 33	FTP Ser ver v6.3
0050	20 66 6f 72 20 57 69 6e	53 6f 63 6b 20 72 65 61	for Win Sock rea
0060	64 79 2e 2e 2e 0d 0a		dy·····

b) Port mặc định của FTP Server: 21

Transmission Control Protocol, Src Port: 49788, Dst Port: 21, Seq: 0, Len: 0
 Source Port: 49788
 Destination Port: 21

c) Username và password của người dùng

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.

File Transfer Protocol (FTP)
 USER cm07\r\n
 Request command: USER
 Request arg: cm07
 [Current working directory:]

0000	00 0c 29 bf 9a a0 00 50	56 c0 00 01 08 00 45 00	··)·····P V·····E·
0010	00 33 09 9c 40 00 80 06	dc 48 0a 00 00 01 0a 00	·3··@····H·····
0020	00 e0 c2 7c 00 15 83 6b	ec 25 14 e1 c0 10 50 18	··· ···k·%·····P·
0030	40 01 ea 84 00 00 55 53	45 52 20 63 6d 30 37 0d	@·····US ER cm07·
0040	0a		·

Username: cm07

```

File Transfer Protocol (FTP)
  PASS 123654\r\n
    Request command: PASS
    Request arg: 123654
  [Current working directory: ]

```

0000	00 0c 29 bf 9a a0 00 50 56 c0 00 01 08 00 45 00	..)....P V.....E.
0010	00 35 09 9d 40 00 80 06 dc 45 0a 00 00 01 0a 00	.5..@... .E.....
0020	00 e0 c2 7c 00 15 83 6b ec 30 14 e1 c0 34 50 18k .0...4P.
0030	3f f8 e9 67 00 00 50 41 53 53 20 31 32 33 36 35	?..g..PA SS 12365
0040	34 0d 0a	4..

Password: 123654

d) Port truyền lệnh của Client: 49788

```

Transmission Control Protocol, Src Port: 49788, Dst Port: 21, Seq: 0, Len: 0
  Source Port: 49788
  Destination Port: 21
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  Sequence number (raw): 2204888058
  [Next sequence number: 1 (relative sequence number)]
  Acknowledgment number: 0
  Acknowledgment number (raw): 0
  1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window size value: 8192
    [Calculated window size: 8192]
    Checksum: 0x083e [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale,
    > TCP Option - Maximum segment size: 1460 bytes
    > TCP Option - No-Operation (NOP)

```

0000	00 0c 29 bf 9a a0 00 50 56 c0 00 01 08 00 45 00	..)....P V.....E.
0010	00 34 09 91 40 00 80 06 dc 52 0a 00 00 01 0a 00	.4..@... .R.....
0020	00 e0 c2 7c 00 15 83 6b eb fa 00 00 00 00 80 02k
0030	20 00 08 3e 00 00 02 04 05 b4 01 03 03 02 01 01	..>.....
0040	04 02	..

e) Client truy xuất lên Server theo mode: passive

28	21.968087	10.0.0.224	10.0.0.1	FTP	101 Response: 227 Entering Passive Mode (10,0,0,224,19,137)
29	21.984564	10.0.0.1	10.0.0.224	FTP	62 Request: SIZE /
30	21.985403	10.0.0.224	10.0.0.1	FTP	76 Response: 550 /: No such file.
31	21.986261	10.0.0.1	10.0.0.224	TCP	66 49791 → 5001 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
32	21.986361	10.0.0.224	10.0.0.1	TCP	66 5001 → 49791 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=1 SACK_PERM=1
33	21.986491	10.0.0.1	10.0.0.224	FTP	62 Request: MDTM /
34	21.986571	10.0.0.1	10.0.0.224	TCP	60 49791 → 5001 [ACK] Seq=1 Ack=1 Win=65700 Len=0
35	21.987586	10.0.0.224	10.0.0.1	FTP	74 Response: 213 20090903103505
36	21.988569	10.0.0.1	10.0.0.224	FTP	62 Request: RETR /
37	21.989338	10.0.0.224	10.0.0.1	FTP	89 Response: 550 /: No such file or directory.
38	21.990088	10.0.0.1	10.0.0.224	FTP	60 Request: PASV
39	21.994321	10.0.0.224	10.0.0.1	TCP	54 5001 → 49791 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
40	22.000601	10.0.0.1	10.0.0.224	TCP	60 49791 → 5001 [ACK] Seq=1 Ack=2 Win=65700 Len=0
41	22.000622	10.0.0.1	10.0.0.224	TCP	60 49791 → 5001 [FIN, ACK] Seq=1 Ack=2 Win=65700 Len=0
42	22.000683	10.0.0.224	10.0.0.1	TCP	54 5001 → 49791 [ACK] Seq=2 Ack=2 Win=65535 Len=0

f)

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	11.415085	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	12.192785	10.0.0.1	10.0.0.255	NBNS	92 Name query NB 172.29.70.4<20>

g) Quá trình bắt tay truyền dữ liệu giữa FTP Server và Client

44	22.006056	10.0.0.1	10.0.0.224	FTP	61 Request: CMD /
45	22.006724	10.0.0.1	10.0.0.224	TCP	66 49792 → 5002 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
46	22.006758	10.0.0.224	10.0.0.1	TCP	66 5002 → 49792 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=1 SACK_PERM=1
47	22.006960	10.0.0.1	10.0.0.224	TCP	60 49792 → 5002 [ACK] Seq=1 Ack=1 Win=65700 Len=0
48	22.007298	10.0.0.224	10.0.0.1	FTP	82 Response: 250 Directory changed to /

h)

Port truyền dữ liệu của FTP Server: 5002

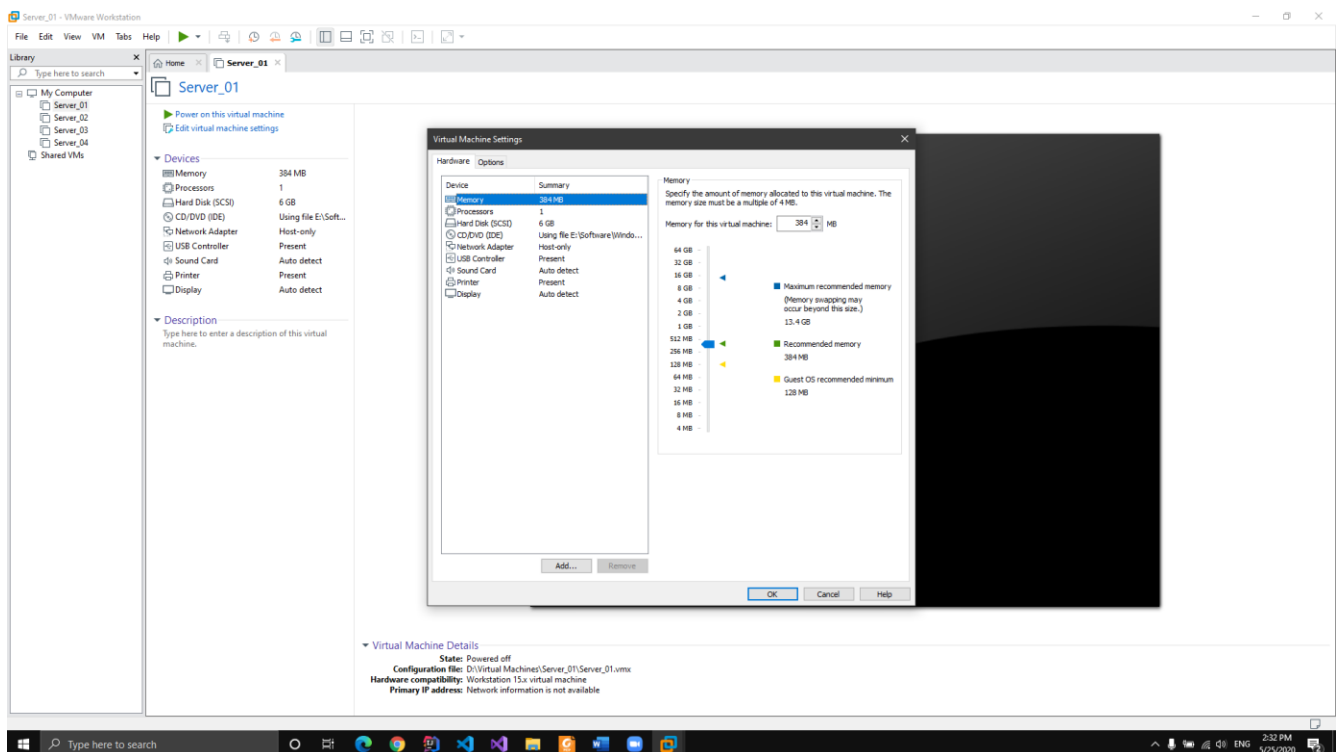
Port truyền dữ liệu của FTP Client: 49792

45	22.006724	10.0.0.1	10.0.0.224	TCP	66 49792 → 5002 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
46	22.006758	10.0.0.224	10.0.0.1	TCP	66 5002 → 49792 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=1 SACK_PERM=1
47	22.006960	10.0.0.1	10.0.0.224	TCP	60 49792 → 5002 [ACK] Seq=1 Ack=1 Win=65700 Len=0

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

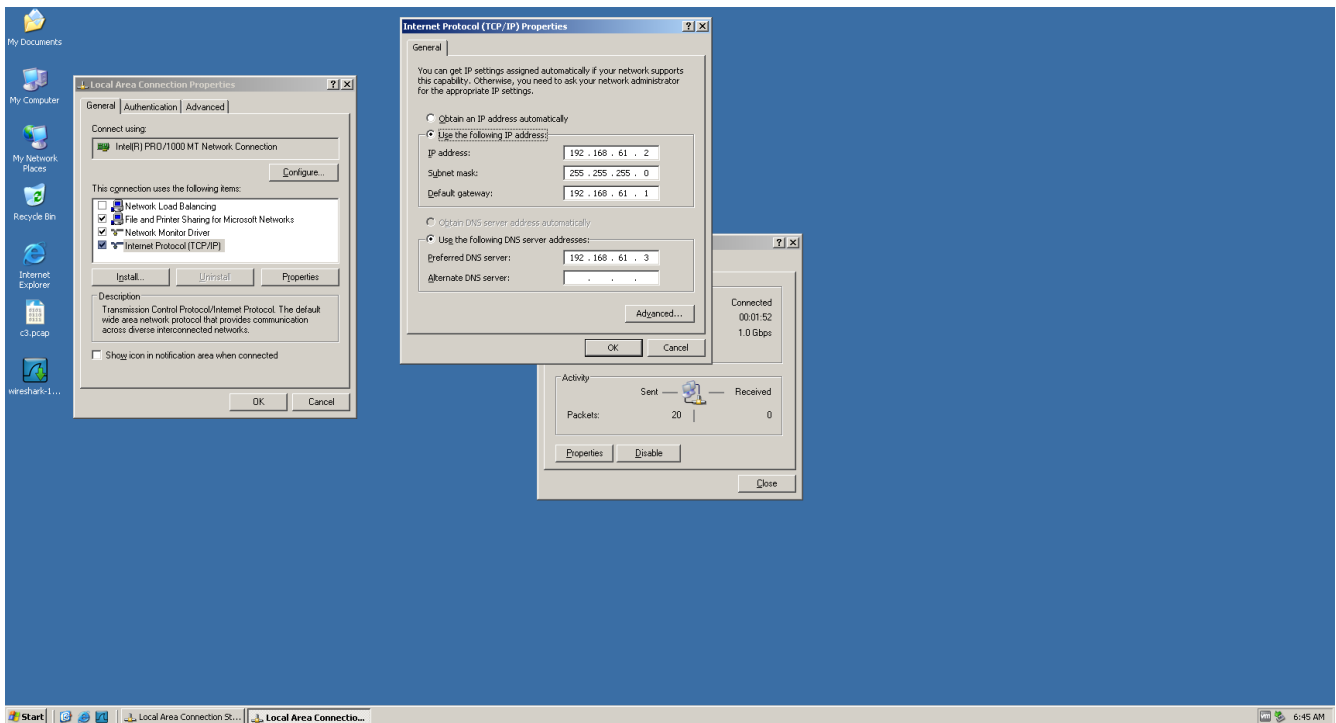
- Sử dụng máy ảo MS Windows Server 2003/2008/2012 để làm DHCP server. Thiết lập card mạng của máy ảo là Host-Only.

[Trả lời]

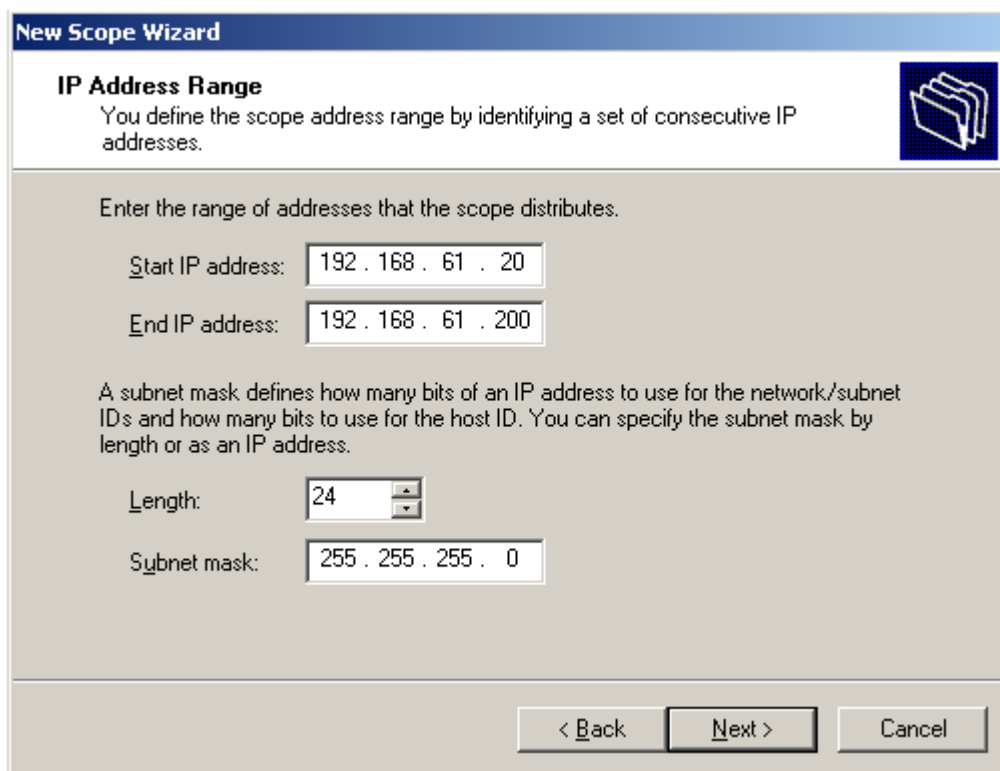


Sử dụng máy ảo Server_01 làm DHCP Server với thiết lập card mạng máy ảo Host – Only, thông số phần cứng ảo như hình chụp

- 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.



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



- d. Khoảng địa chỉ IP dành riêng (reservation): 192.168.X.50/24 – 192.168.X.60/24

[Trả lời]

The screenshot shows a Windows-style dialog box titled "New Scope Wizard". The current step is "Add Exclusions", which includes a brief explanation: "Exclusions are addresses or a range of addresses that are not distributed by the server." Below this, instructions state: "Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only." There are two input fields: "Start IP address:" containing "192 . 168 . 61 . 50" and "End IP address:" containing "192 . 168 . 61 . 60". An "Add" button is to the right of the "End IP address" field. Below these fields is a section labeled "Excluded address range:" with a large empty text box and a "Remove" button to its right. At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

New Scope Wizard

Add Exclusions

Exclusions are addresses or a range of addresses that are not distributed by the server.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: 192 . 168 . 61 . 50 End IP address: 192 . 168 . 61 . 60 Add

Excluded address range:

Remove

< Back Next > Cancel

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

[Trả lời]

New Scope Wizard

Router (Default Gateway)
 You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:

<input type="text" value=" . . ."/>	Add
192.168.61.1	Remove
	Up
	Down

< Back Next > Cancel

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

New Scope Wizard

Domain Name and DNS Servers
 The Domain Name System (DNS) maps and translates domain names used by clients on your network.

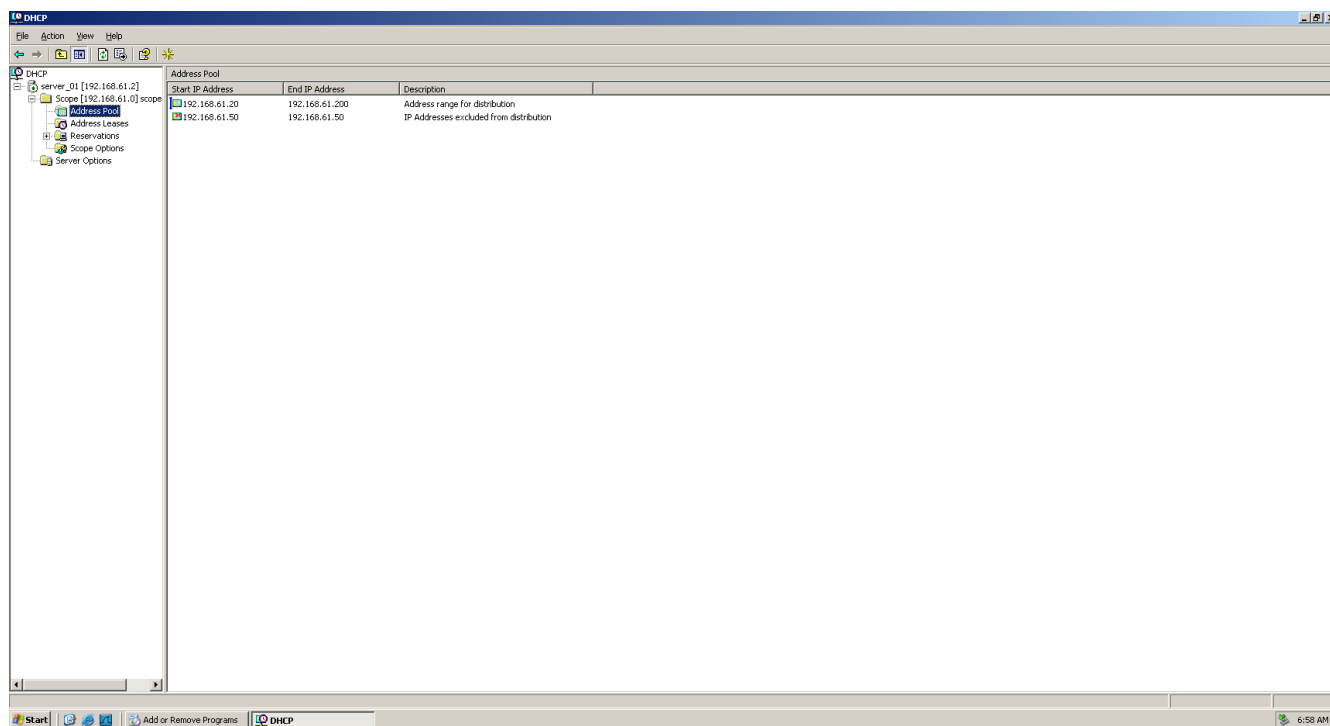
You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

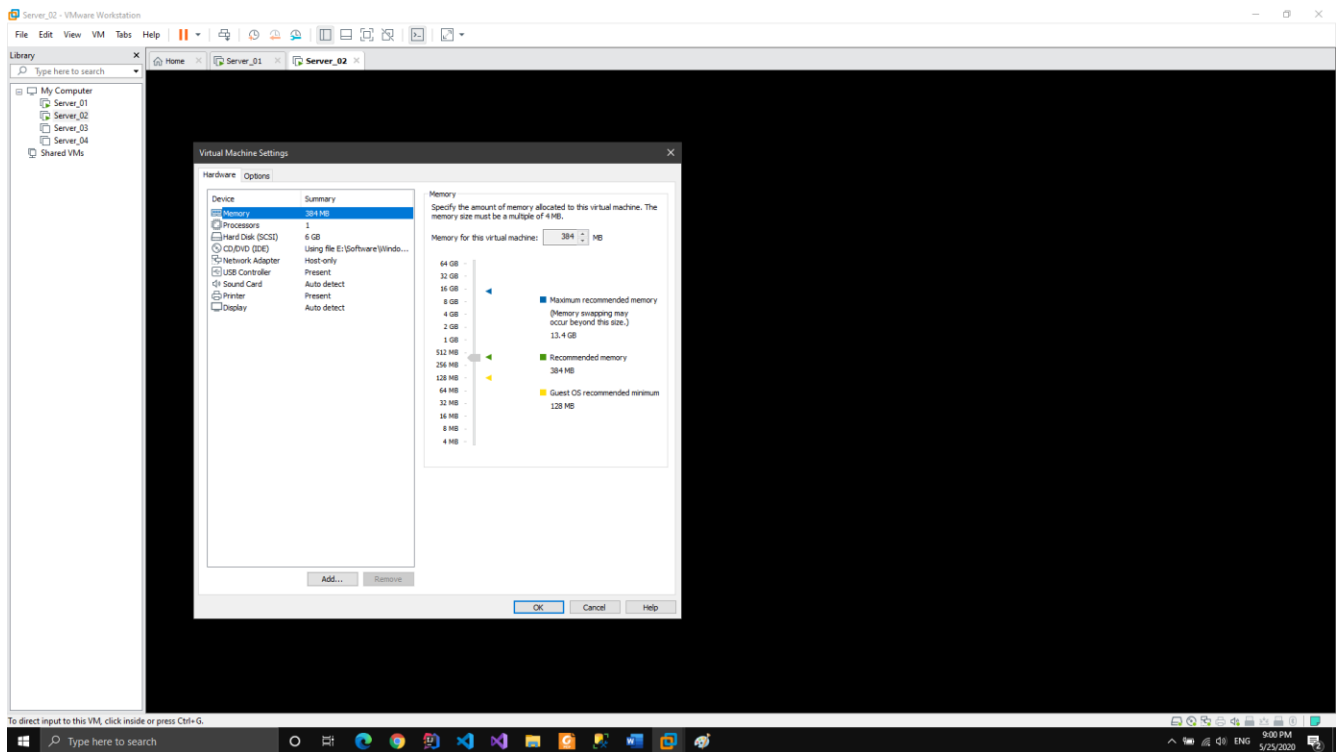
Server name:	IP address:	
<input type="text"/>	192 . 168 . 61 . 3	Add
Resolve		Remove
		Up
		Down

< Back Next > Cancel

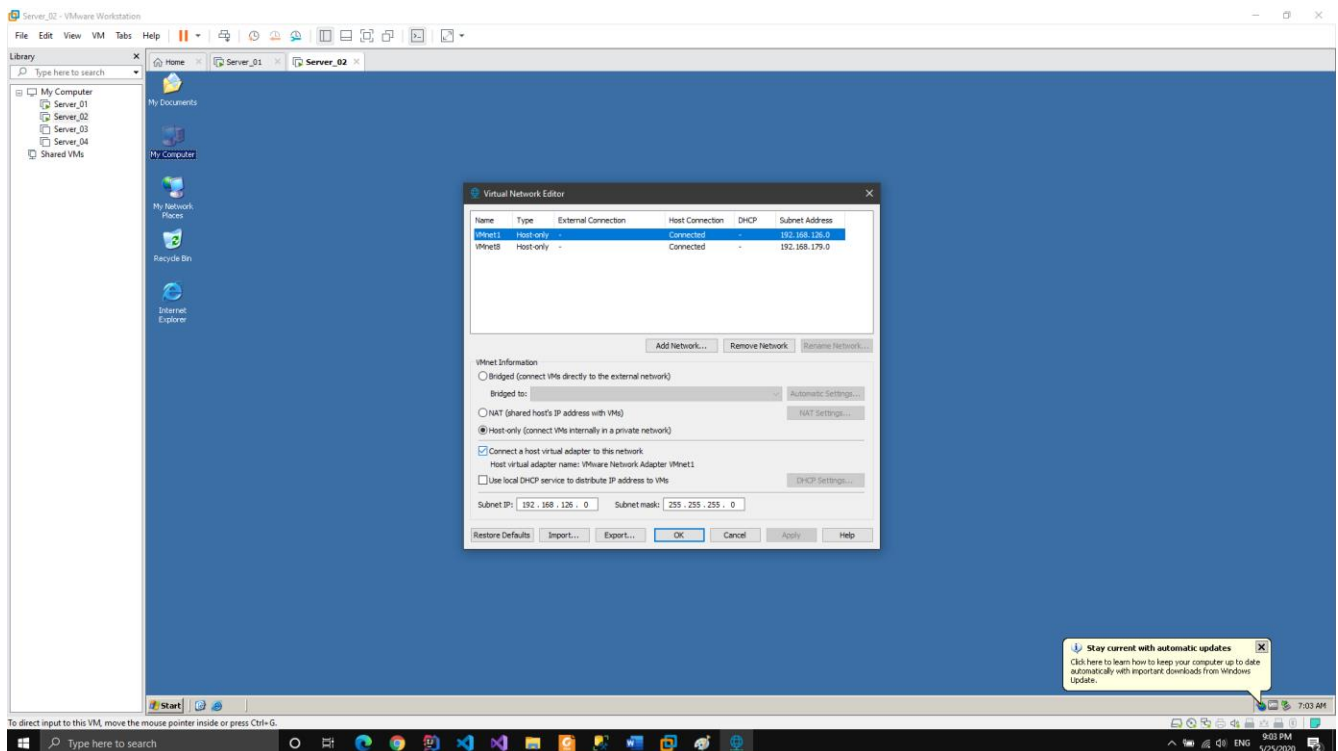


- g. Cấu hình một máy ảo khác (ví dụ: Windows 7, Windows Server 2003...) làm DHCP client.
Thiết lập card mạng của máy ảo này là Host-Only.

[Trả lời]



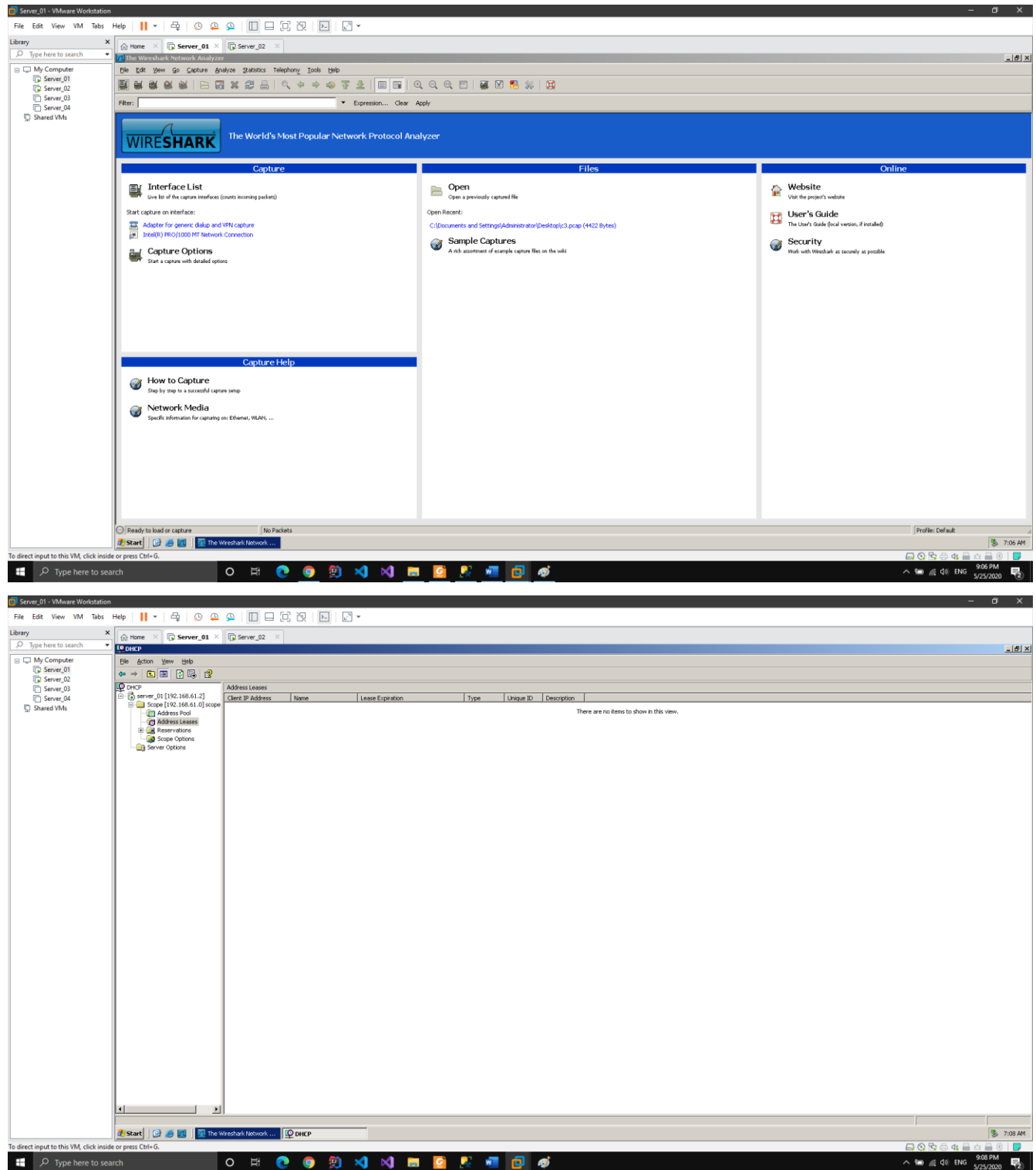
- h. Tắt tính năng DHCP của phần mềm VMWare (Trên VMWare Player/Workstation > Chọn menu Edit > Virtual Network Editor > Chọn card mạng VMNet1 > Bỏ chọn “Use local DHCP service to distribute IP addresses to VMs”).



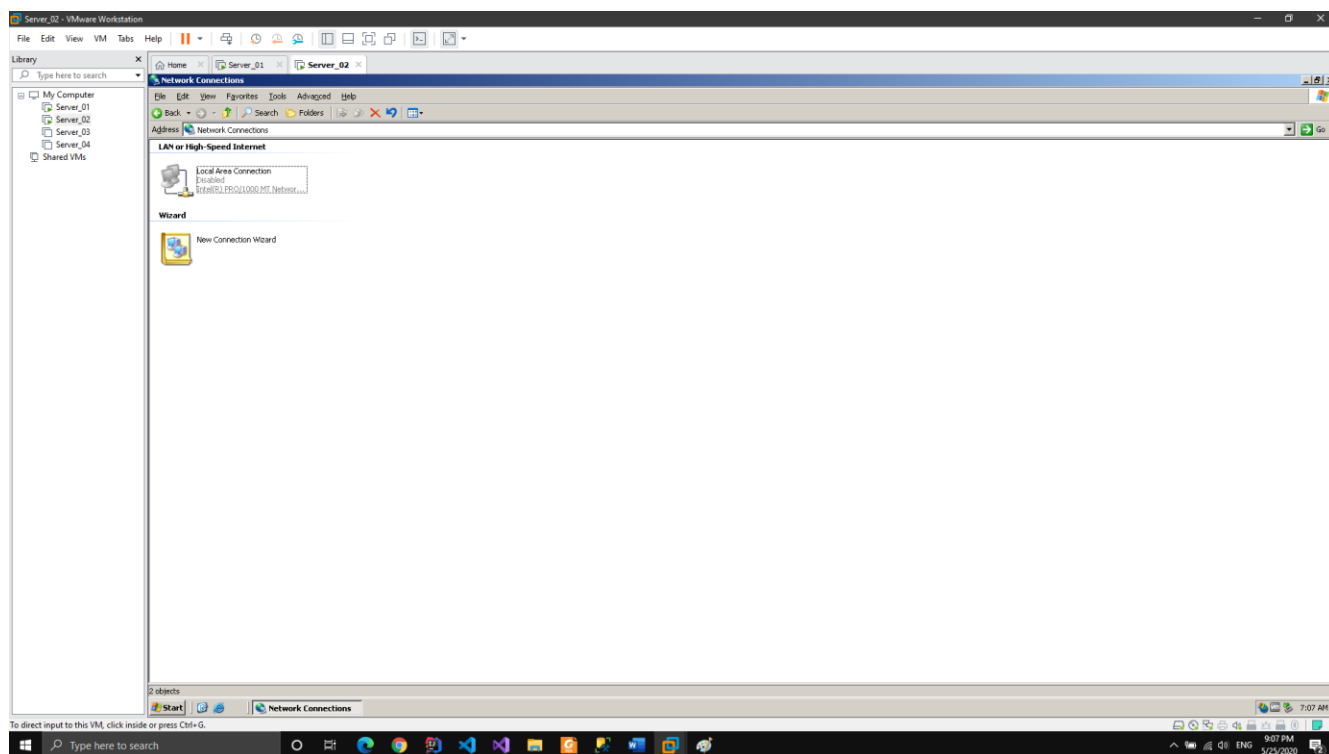
- i. Thực hiện xin cấp phát địa chỉ IP từ client đến DHCP server và dùng Wireshark để bắt gói tin của quá trình này.

[Trả lời]

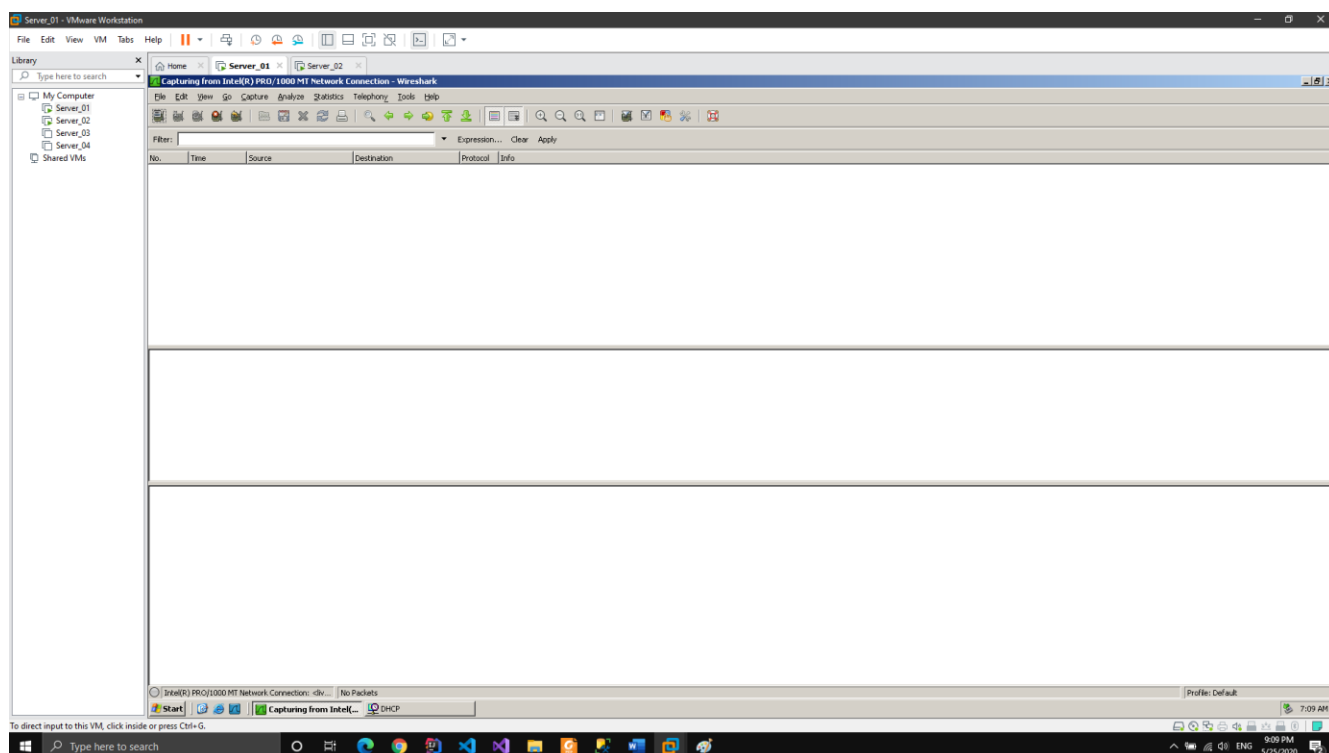
Chuẩn bị Wireshark ở Server_01, giả sử đây là Server



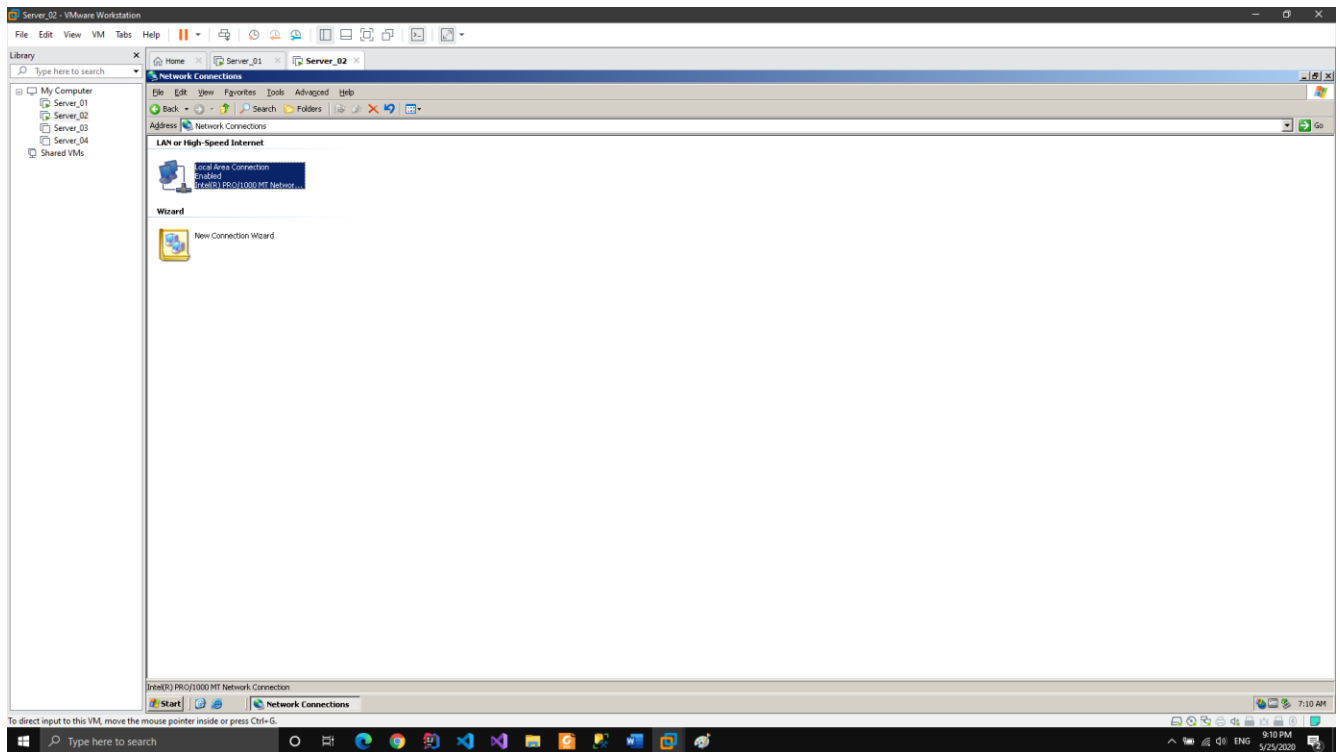
Chuẩn bị kết nối ở Server_02, giả sử đây là Client



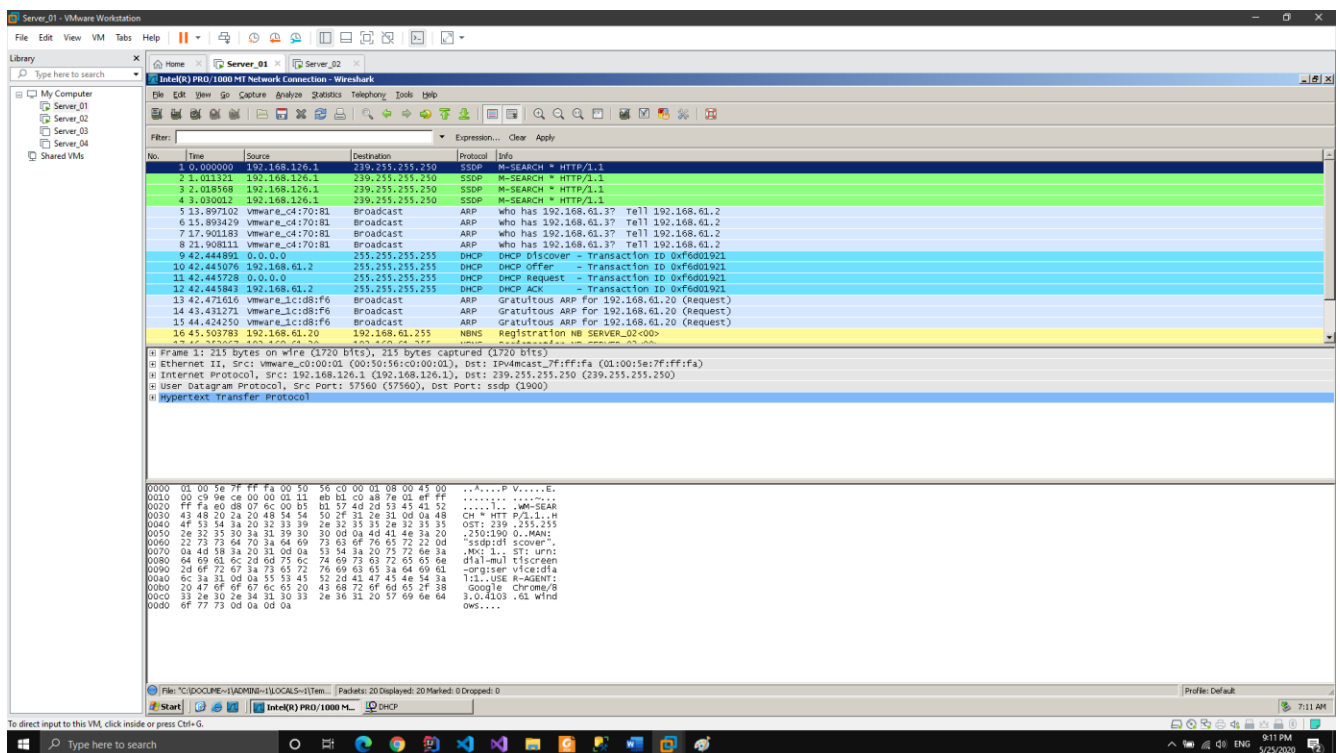
Bật Wireshark Capturing ở Server



Enable Connection ở Client



Kết quả hiển thị trên Wireshark



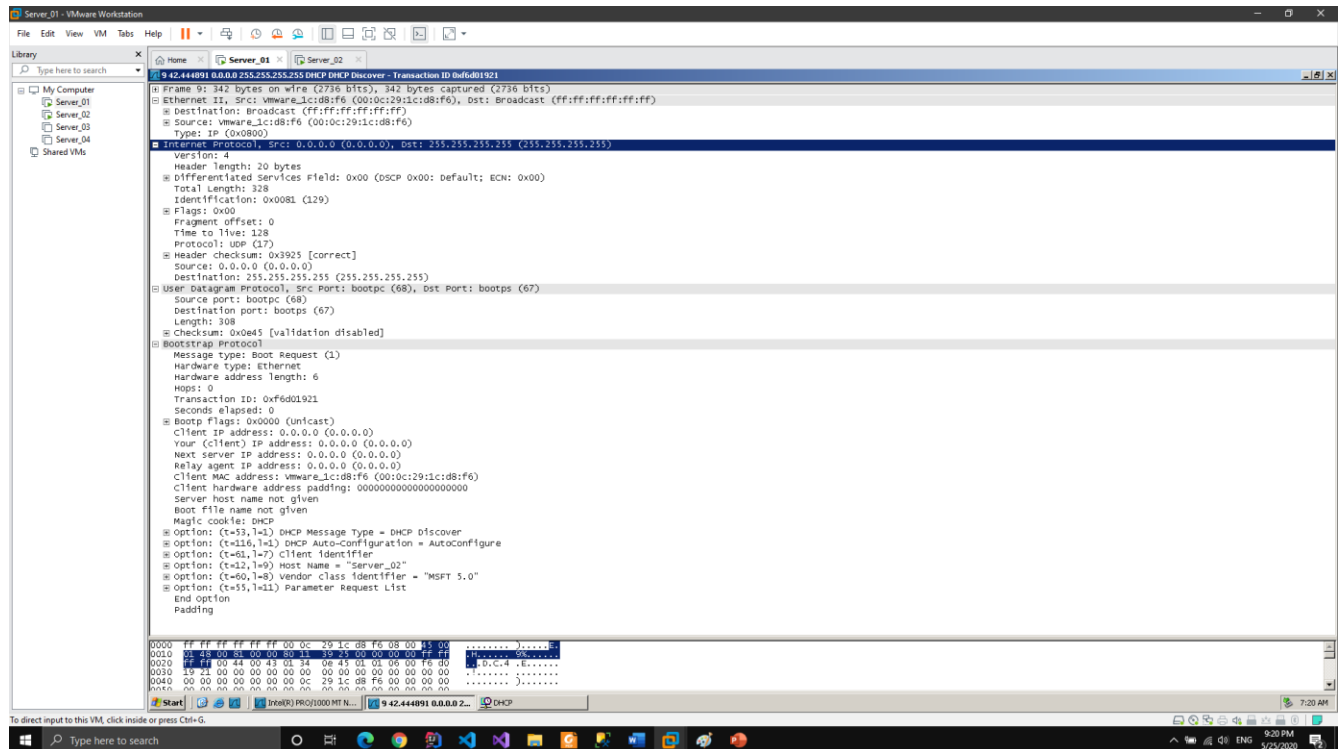
j. Cho biết có bao nhiêu gói tin được truyền và nhận trong quá trình cấp phát địa chỉ IP?

Có 4 gói tin được truyền và nhận trong quá trình cấp phát địa chỉ IP với protocol là DHCP

- 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?

[Trả lời]

Gói Discover: Client tìm Server



IP nguồn: 0.0.0.0

IP đích: 255.255.255.255

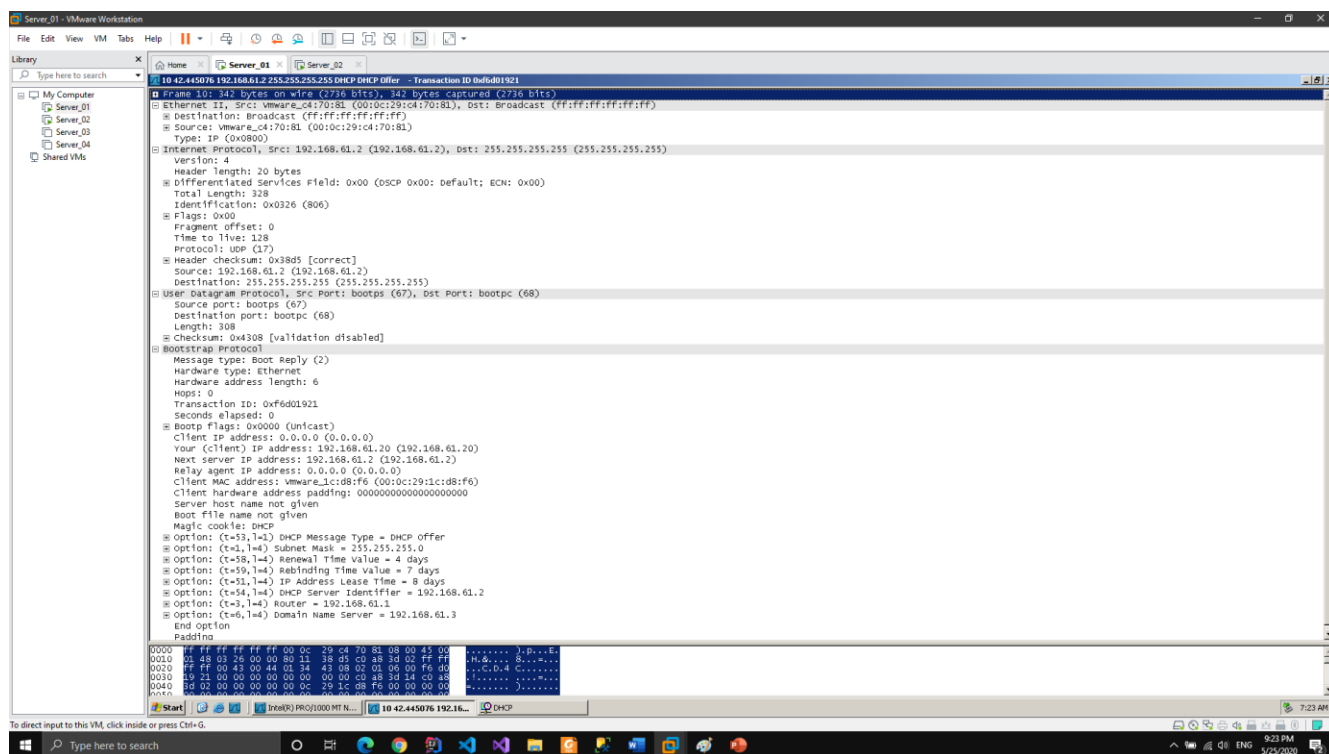
MAC nguồn: 00:0c:29:1c:d8:f6

MAC đích: ff:ff:ff:ff:ff:ff

Port nguồn: 68

Port đích: 67

Gói Offer: DHCP gợi ý một địa chỉ IP



IP nguồn: 192.168.61.2

IP đích: 255.255.255.255

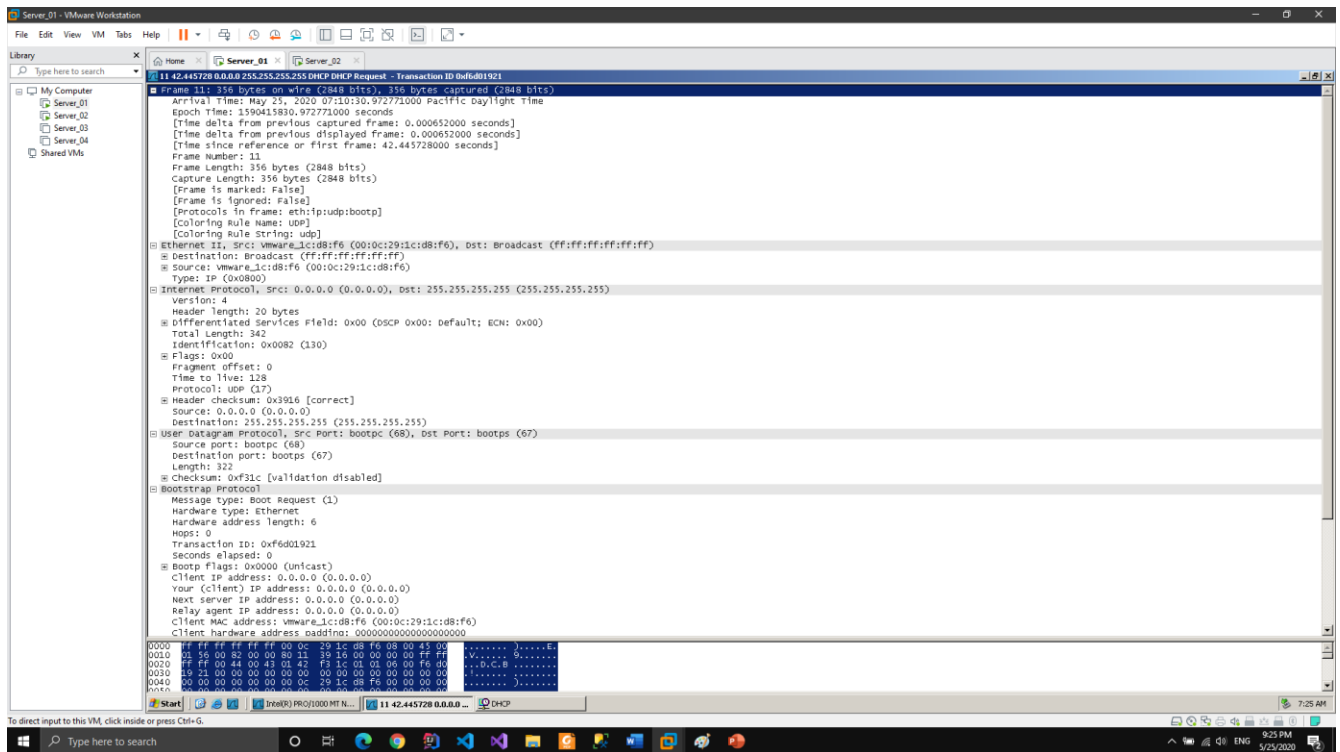
MAC nguồn: 00:0c:29:c4:70:81

MAC đích: ff:ff:ff:ff:ff:ff

Port nguồn: 67

Port đích: 68

Gói Request: Client yêu cầu cấp 1 địa chỉ IP



IP nguồn: 0.0.0.

IP đích: 255.255.255.255

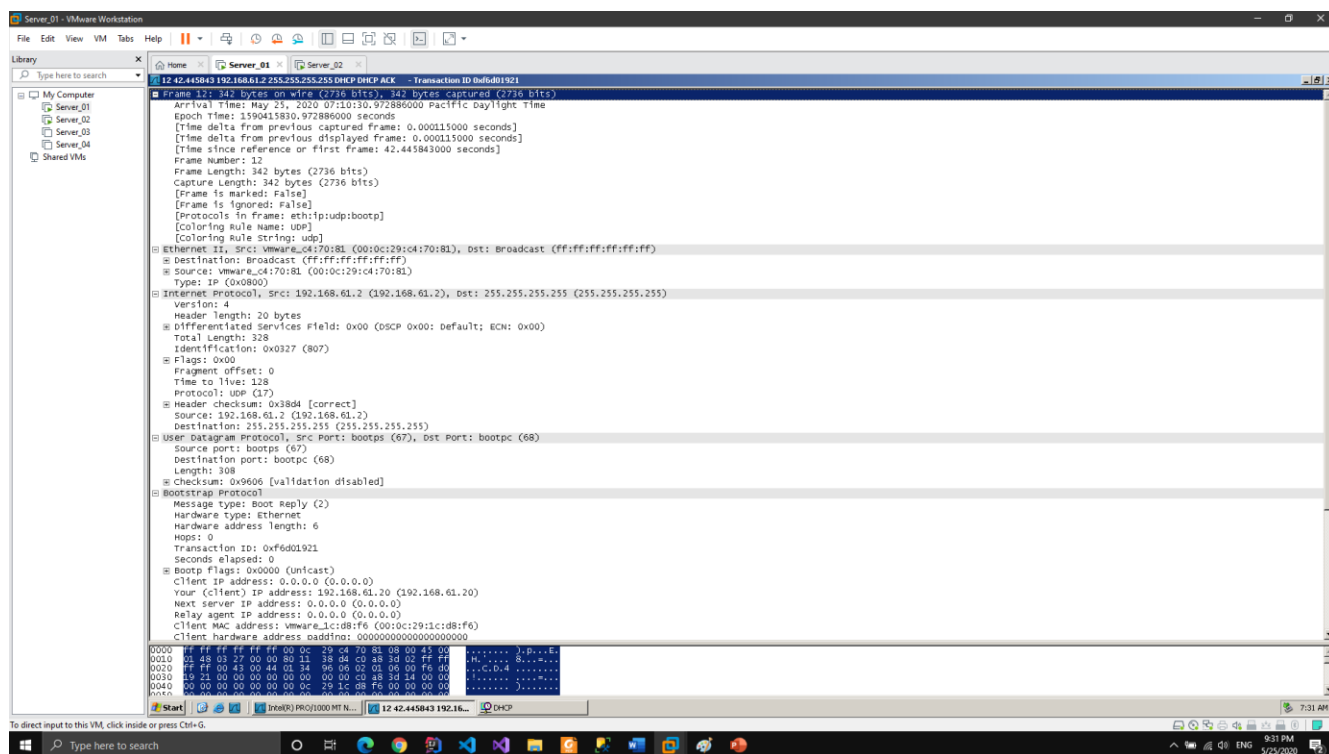
MAC nguồn: 00:0c:29:1c:d8:f6

MAC đích: ff:ff:ff:ff:ff:ff

Port nguồn: 68

Port đích: 67

Gói Ack



IP nguồn: 192.168.61.2

IP đích: 255.255.255.255

MAC nguồn: 00:0c:29:c4:70:81

MAC đích: ff:ff:ff:ff:ff:ff

Port nguồn: 67

Port đích: 68

1. Thông tin default gateway và DNS server nằm trong gói tin nào?

Thông tin default gateway và DNS server nằm ở gói tin Ack

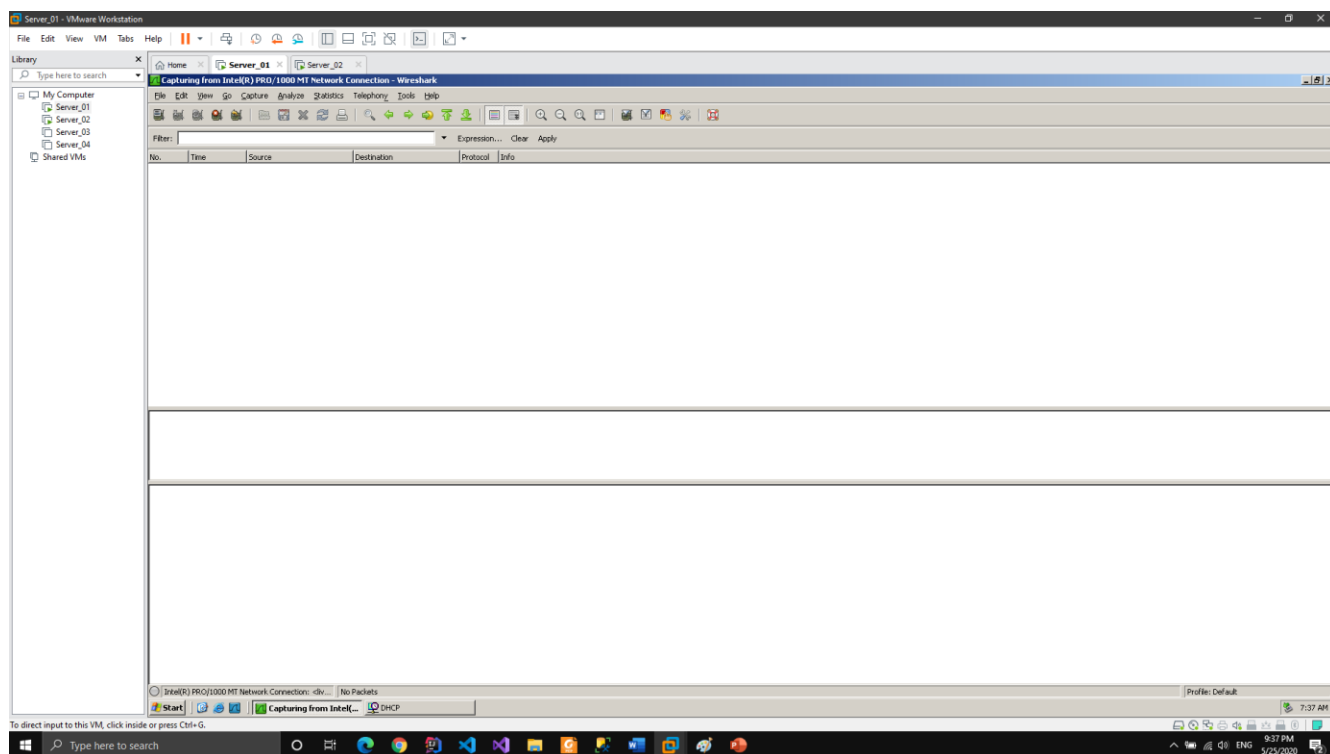
```
Bootstrap Protocol
  Message type: Boot Reply (2)
  Hardware type: Ethernet
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xf6d01921
  Seconds elapsed: 0
  Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0 (0.0.0.0)
  Your (client) IP address: 192.168.61.20 (192.168.61.20)
  Next server IP address: 0.0.0.0 (0.0.0.0)
  Relay agent IP address: 0.0.0.0 (0.0.0.0)
  Client MAC address: vmware_1c:d8:f6 (00:0c:29:1c:d8:f6)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  Option: (t=53,l=1) DHCP Message Type = DHCP ACK
  Option: (t=58,l=4) Renewal Time Value = 4 days
  Option: (t=59,l=4) Rebinding Time Value = 7 days
  Option: (t=51,l=4) IP Address Lease Time = 8 days
  Option: (t=54,l=4) DHCP Server Identifier = 192.168.61.2
  Option: (t=1,l=4) Subnet Mask = 255.255.255.0
  Option: (t=81,l=3) Client Fully Qualified Domain Name
  Option: (t=3,l=4) Router = 192.168.61.1
  Option: (t=6,l=4) Domain Name Server = 192.168.61.3
  End option
  Padding
```

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:

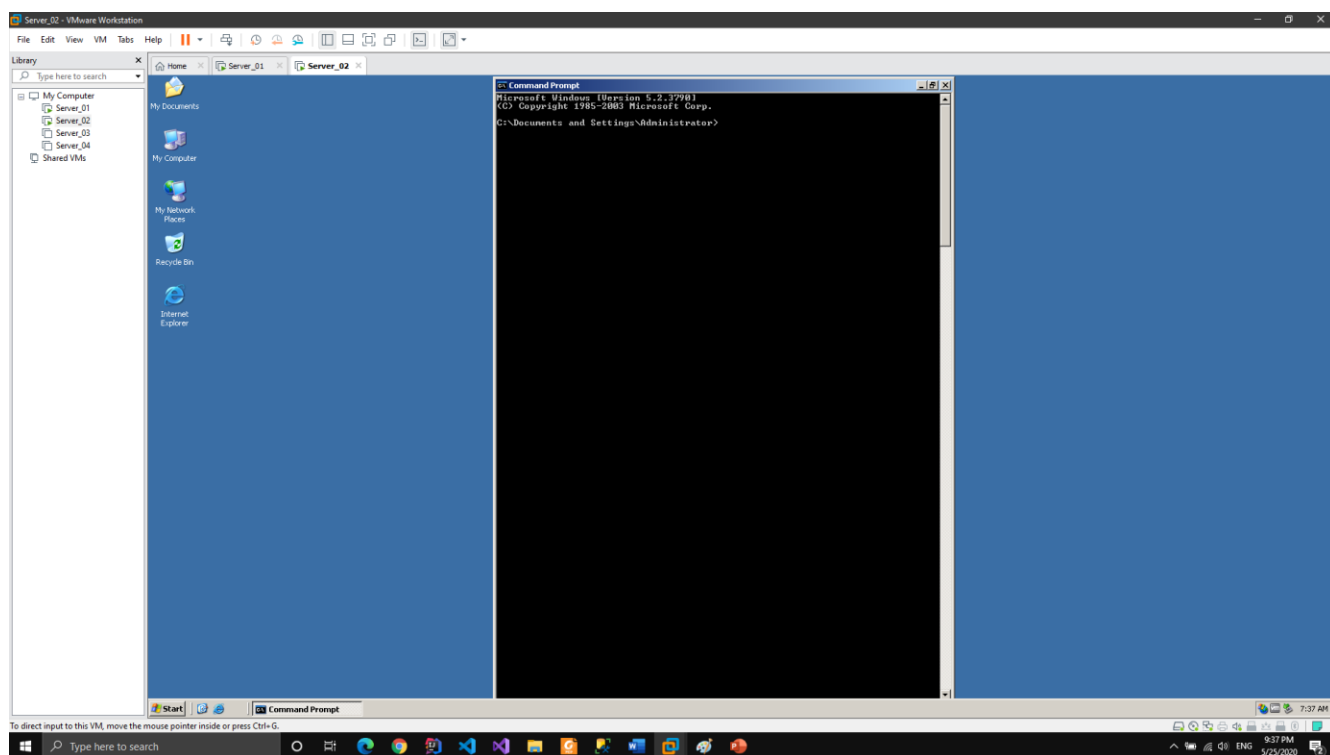
- a. Thực hiện lệnh ping từ client đến server và dùng Wireshark để bắt các gói tin tương ứng.

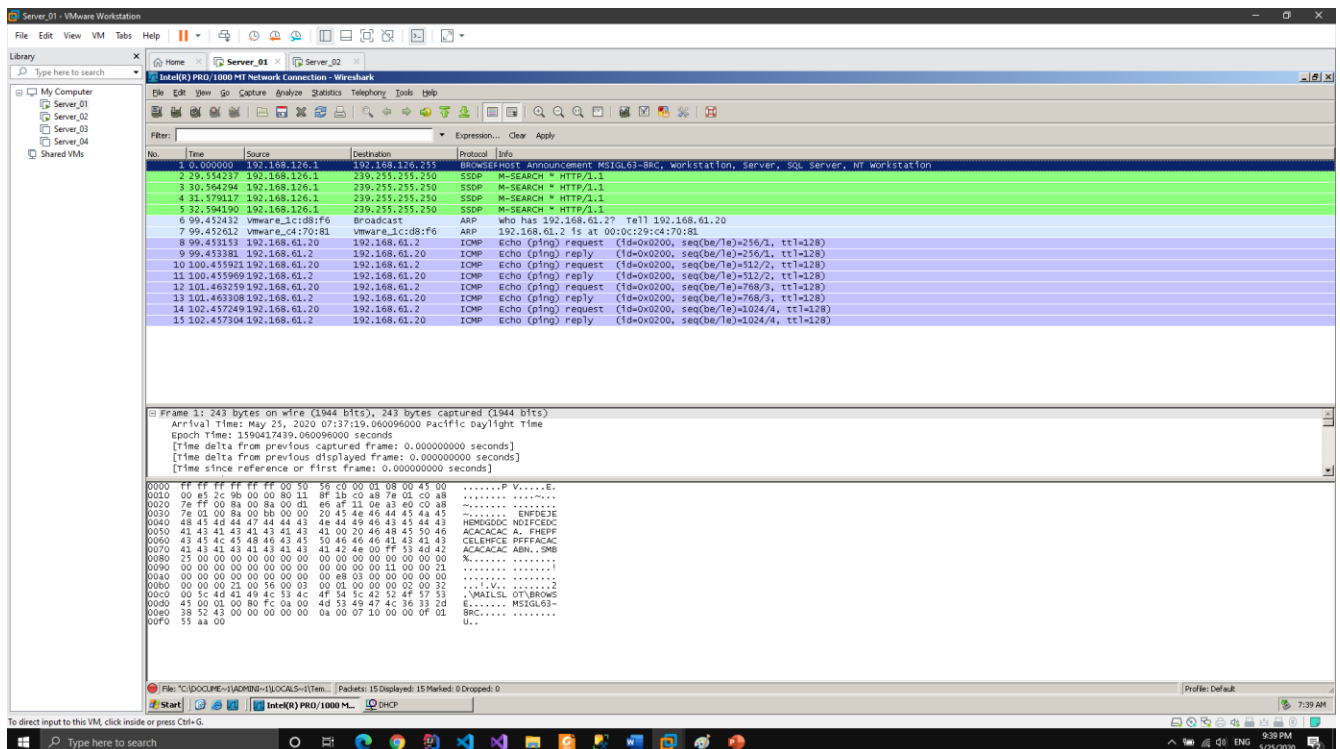
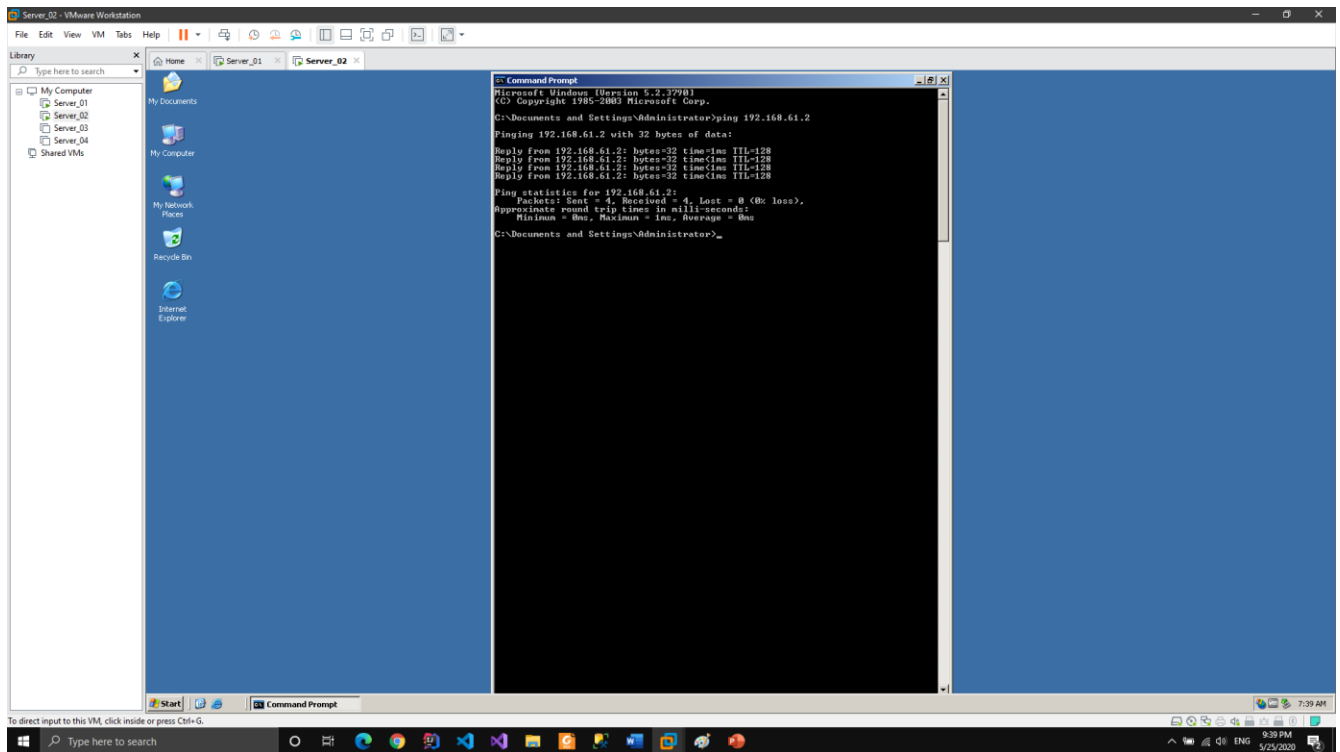
[Trả lời]

Bật capturing ở Server



Bật Command Prompt ở client, chuẩn bị ping lên Server





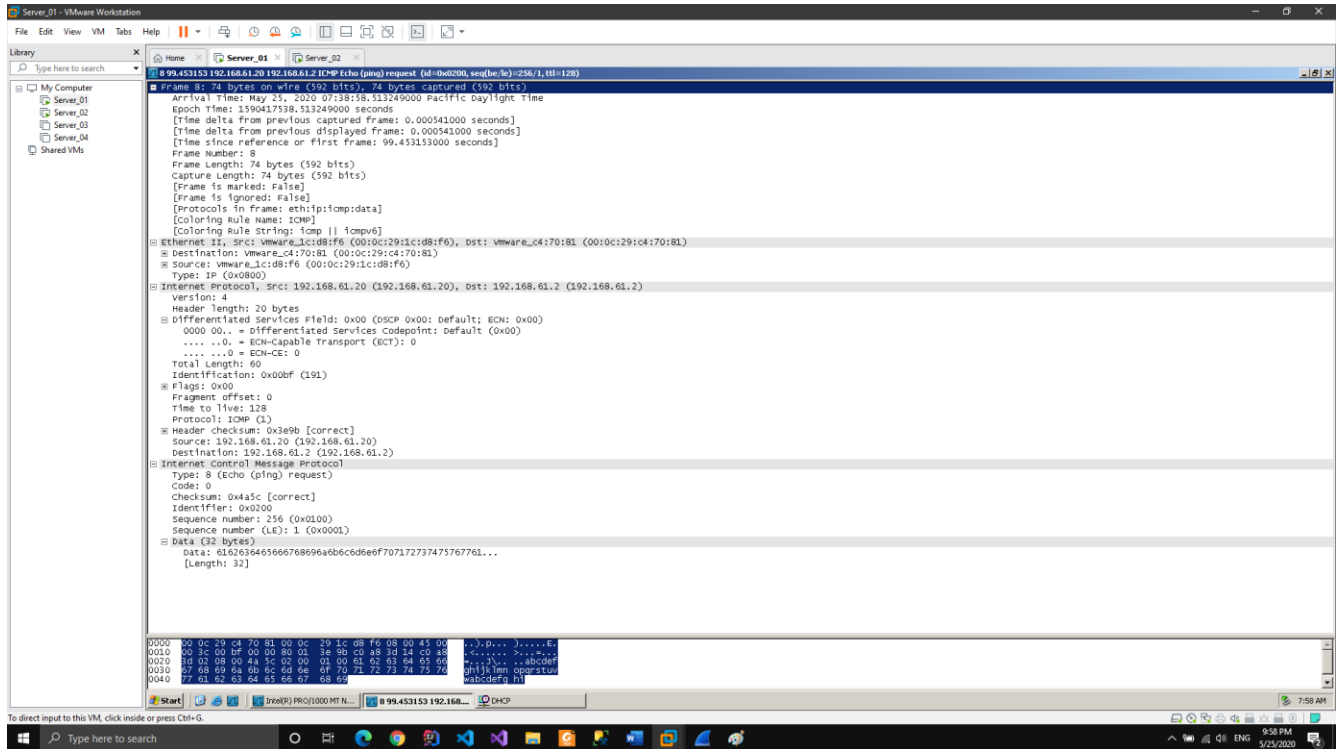
b. Cho biết có bao nhiêu gói tin của quá trình thực hiện lệnh ping?

[Trả lời]

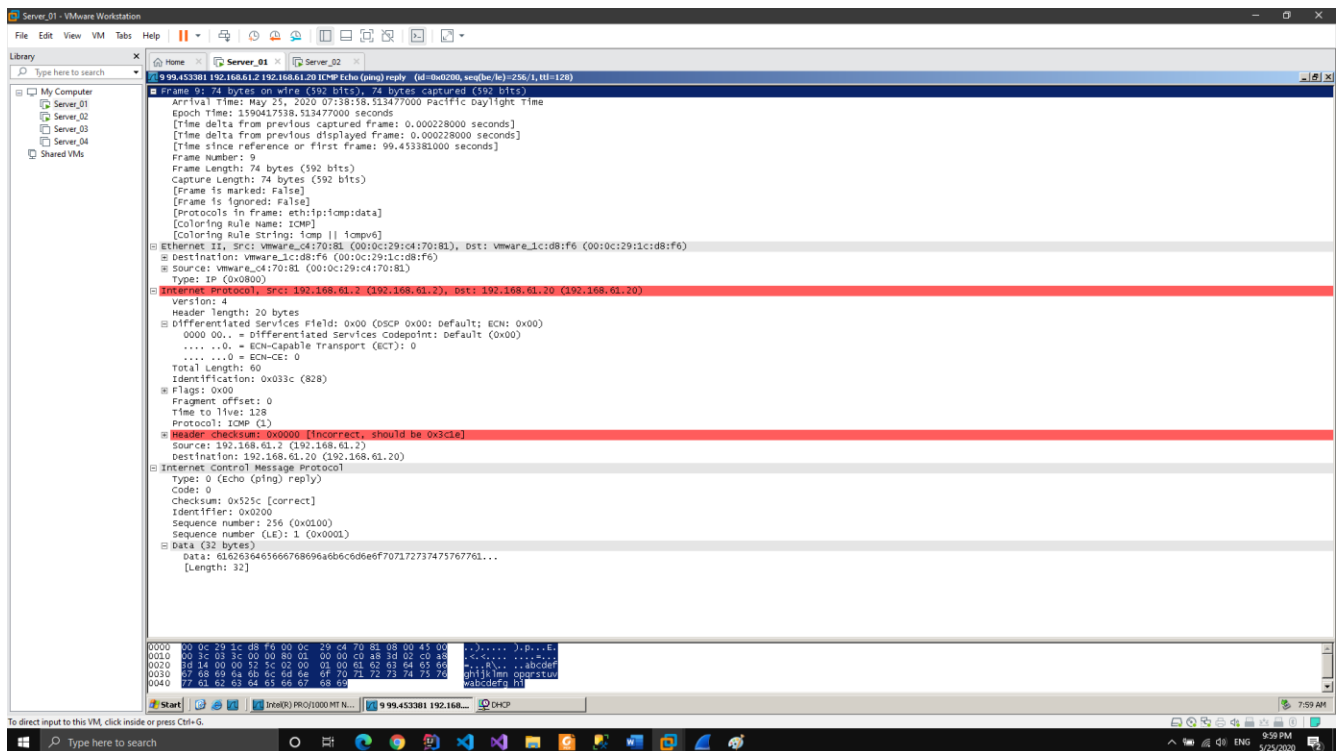
Có tất cả 8 gói tin của quá trình thực hiện lệnh ping theo giao thức ICMP

Hai loại gói

- Gói request



- Gói reply



c. Địa chỉ MAC nguồn, MAC đích là gì?

[Trả lời]

Gói chức năng request

MAC nguồn: 00:0c:29:1c:d8:f6

MAC đích: 00:0c:29:c4:70:81

Gói gói chức năng reply

MAC nguồn: 00:0c:29:c4:70:81

MAC đích: 00:0c:29:1c:d8:f6

d. Địa chỉ IP nguồn, IP đích là gì?

Gói chức năng request

IP nguồn: 192.168.61.20

IP đích: 192.168.61.2

Gói gói chức năng reply

IP nguồn: 192.168.61.2

IP đích: 192.168.61.20

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

abcdefghijklmn oqprstuvwabcdefg hi

