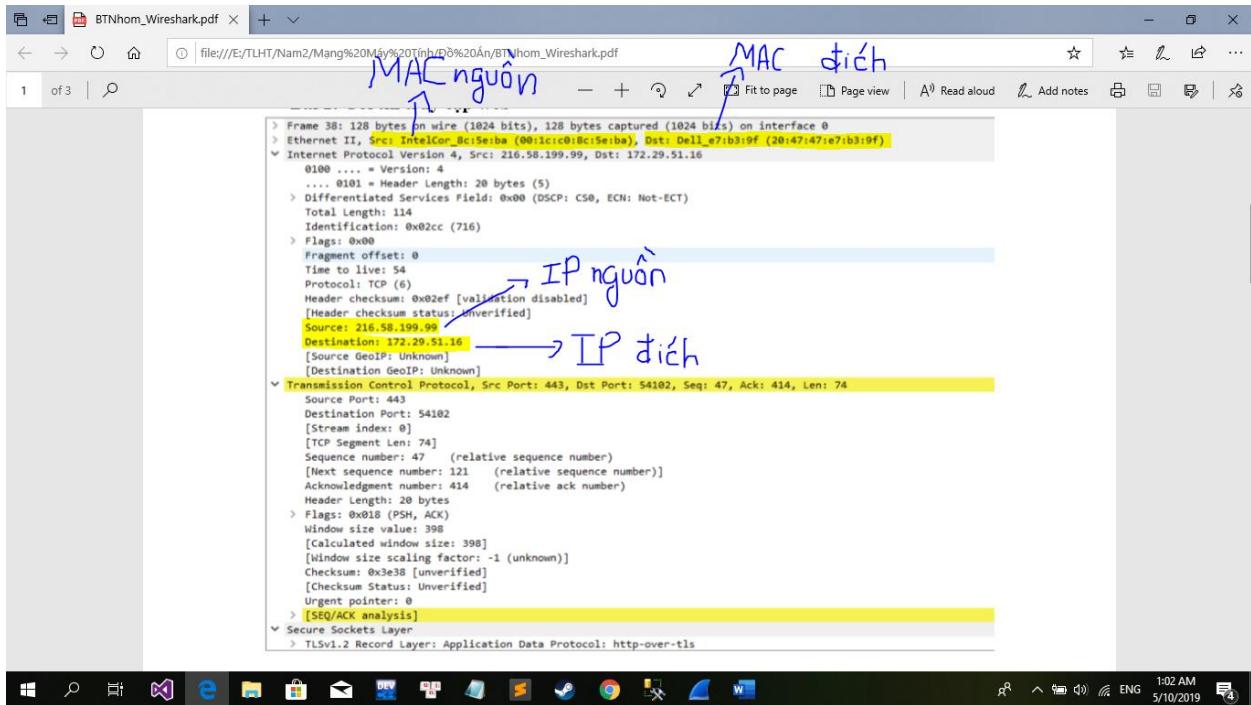


ĐỒ ÁN THỰC HÀNH 1 – PHÂN TÍCH GÓI TIN

MÔN MẠNG MÁY TÍNH

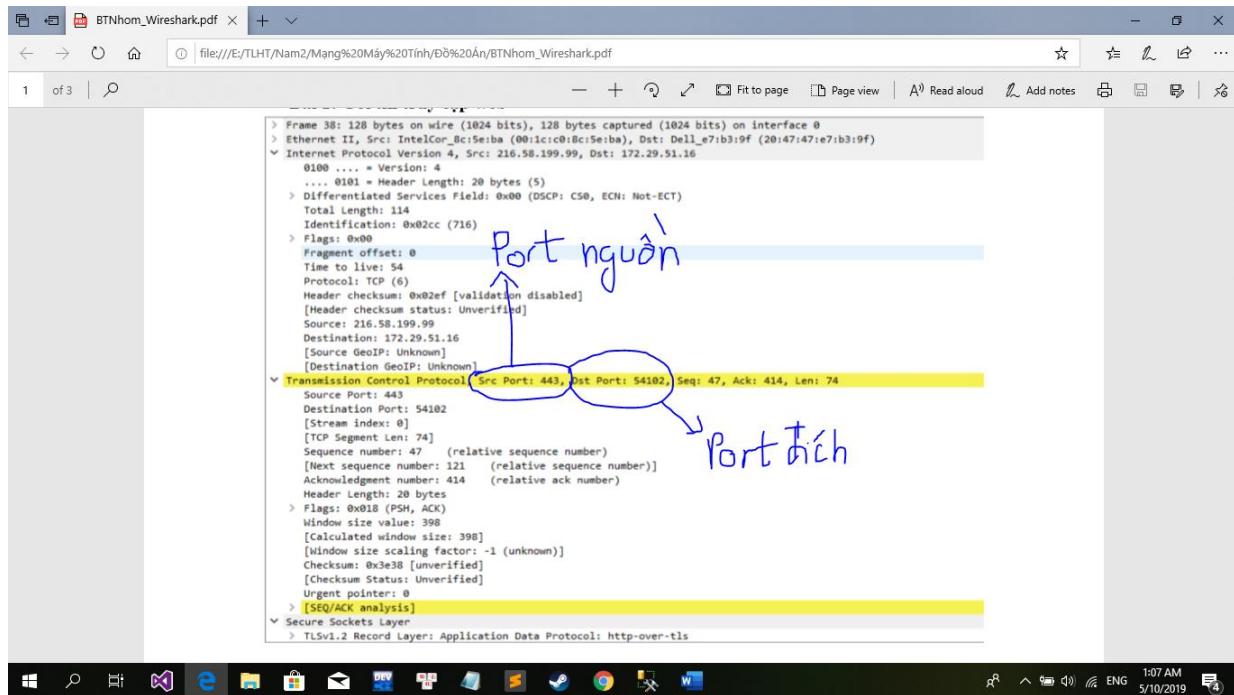
Bài 1: Gói Tập Tin Truy Cập Web:

Câu 1.1: Cho biết địa chỉ IP nguồn, IP đích, MAC nguồn, MAC đích của gói tin trên?



- IP nguồn (IP Src): 216.58.199.99
- IP đích (IP Dst): 172.29.51.16
- MAC nguồn : IntelCor_8c:5e:ba (00:1c:c0:8c:5e:ba)
- MAC đích : Dell_e7:b3:9f (20:47:47:e7:b3:9f)

Câu 1.2: Cho biết thông tin port nguồn, port đích của gói tin trên?

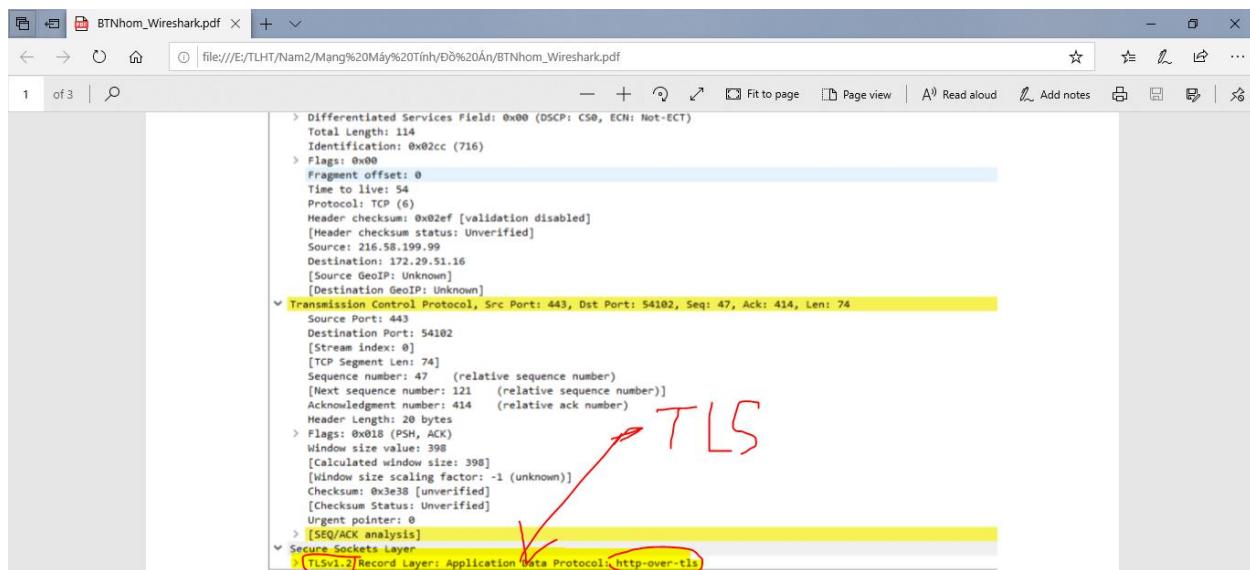


Port nguồn :443
Port đích :54102

Port nguồn (Port Src) :443

Port đích (Port Dst) : 54102

Câu 1.3: Gói tin trên sử dụng giao thức gì ở tầng Application?



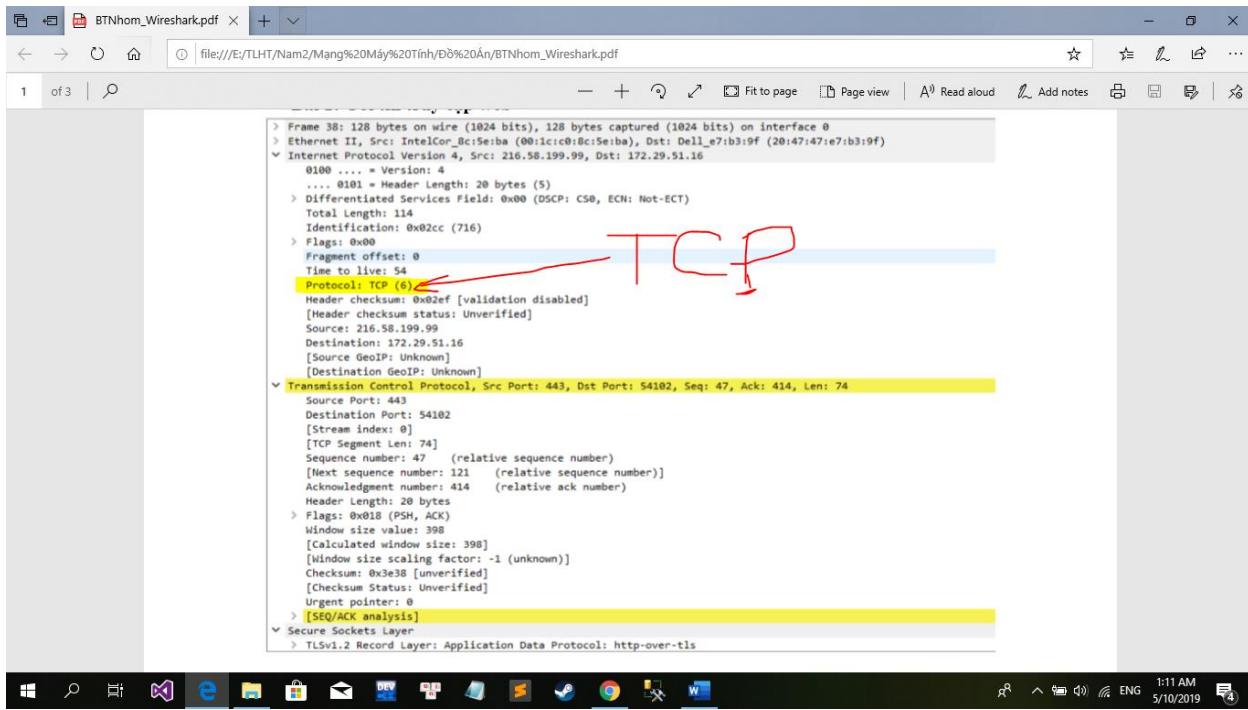
TLS

1. Cho biết địa chỉ IP nguồn, IP đích, MAC nguồn, MAC đích của gói tin trên?



Gói tin trên sử dụng giao thức TLS/SSL ở tầng Application.

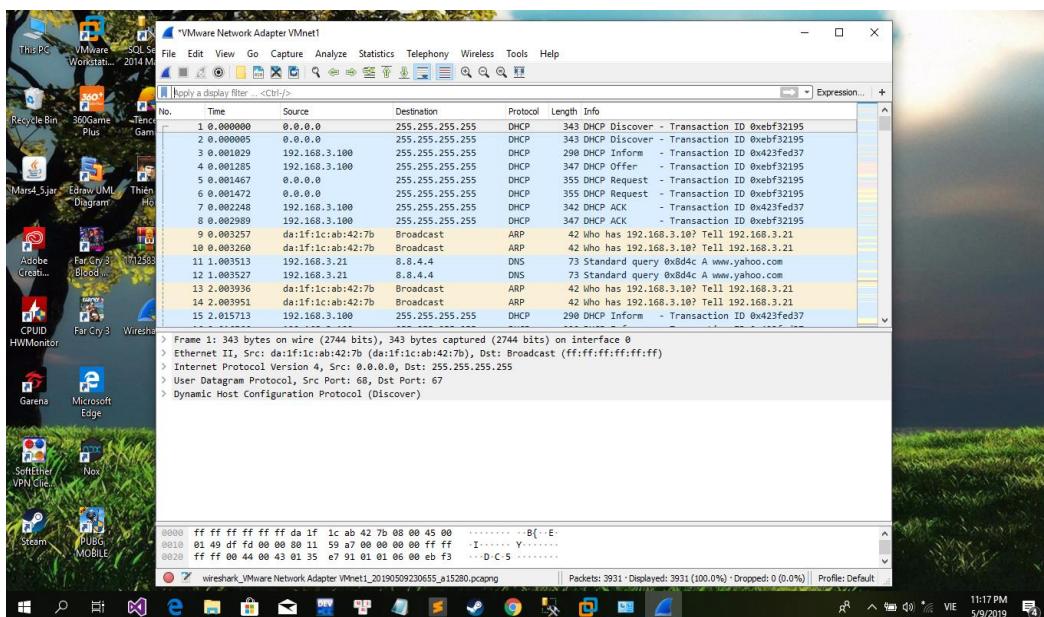
Câu 1.4: Hãy cho biết giao thức sử dụng ở tầng transportation trong gói tin?



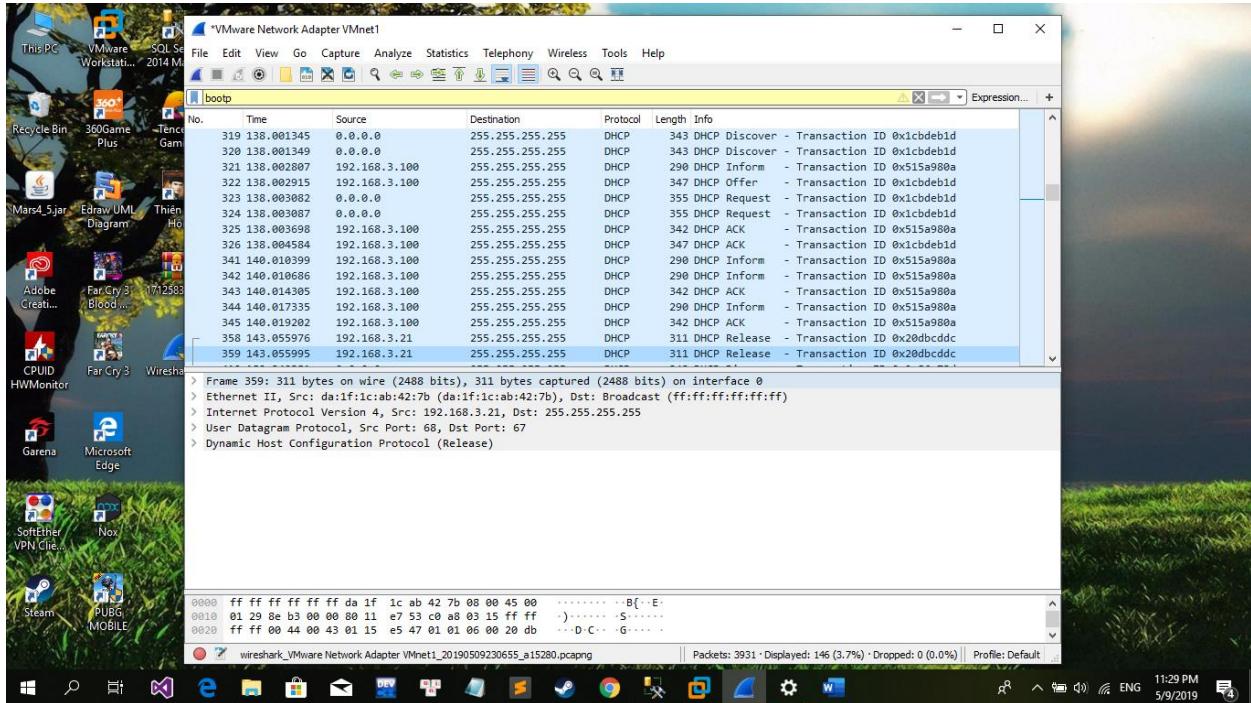
Giao thức sử dụng ở tầng transportation trong gói tin là TCP (Transmission Control Protocol)

Bài 2:DHCP

- Với mọi IP trong bài này thì $X = 03$
 - Sử dụng phần mềm Wireshark bắt gói tin :



- Dùng bộ lọc (Filter) lọc các gói tin sử dụng giao thức DHCP . DHCP sử dụng giao thức BOOTP nên ta lọc theo BOOTP.

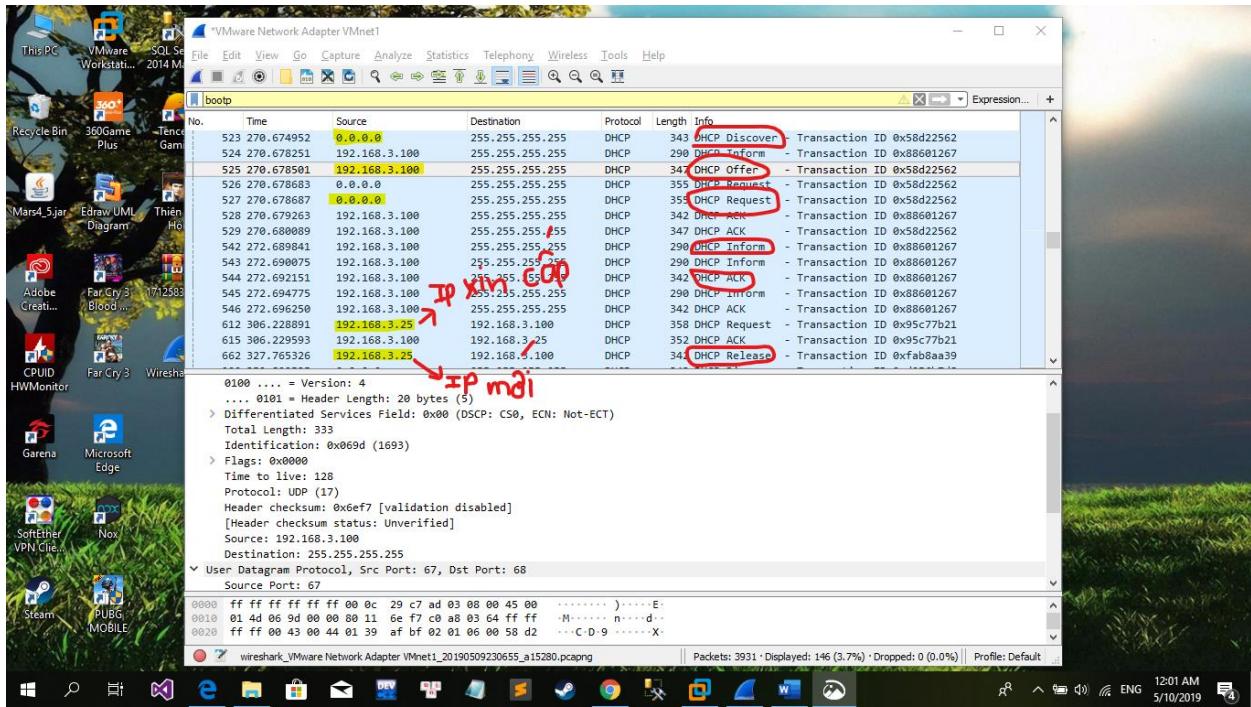
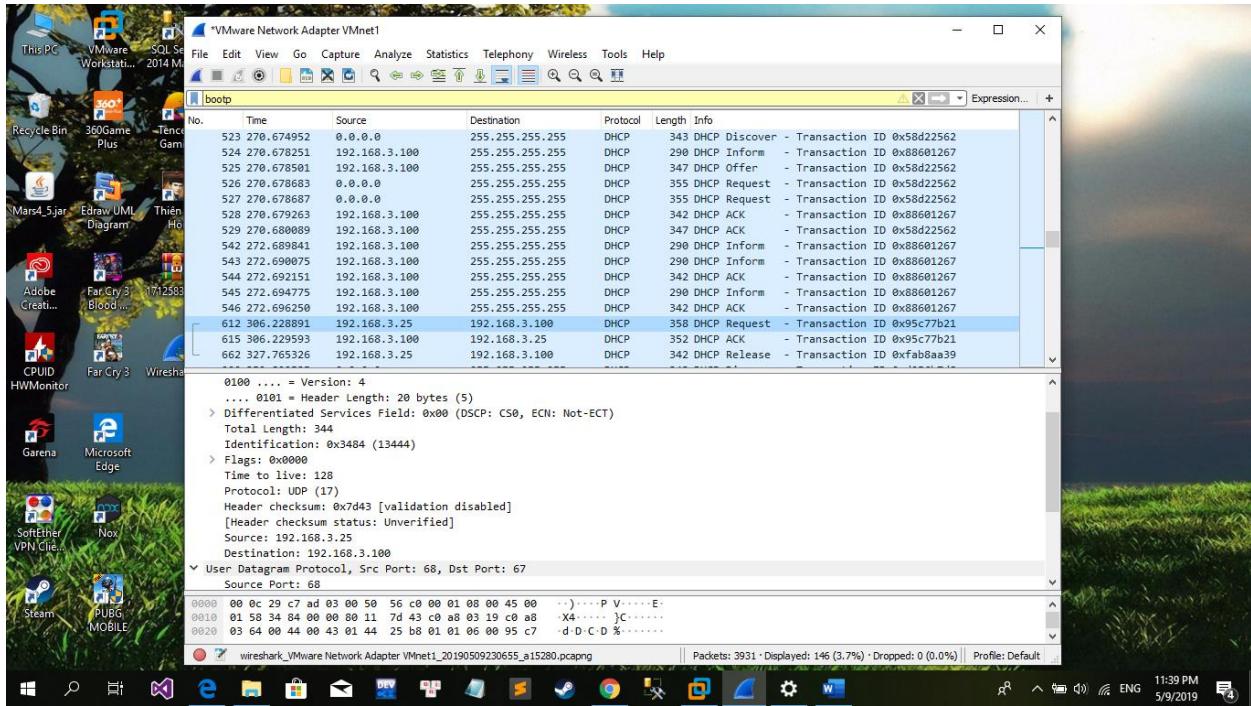


Câu 2.1: Liệt kê tên các gói tin DHCP bắt được trong quá trình xin cấp mới địa chỉ IP?

Trong quá trình xin cấp mới IP từ Server: (Renew)

WireShark đã bắt được các gói tin như: **DHCP Discover** (Khởi động với địa chỉ IP rỗng như trong hình dưới là 0.0.0.0, gửi 1 thông điệp chứa địa chỉ MAC, tên máy tính đến Server, gửi liên tục cho đến khi nhận được phản hồi), **DHCP Inform** (Người dùng đã tự cấu hình địa chỉ IP như dưới là 192.168.3.100 và muốn có thêm thông tin từ DHCP Server), **DHCP Offer** (Server nhận được thông điệp từ Client và chuẩn bị địa chỉ IP cho client. Sau đó nếu client phù hợp với cấu hình thì Server sẽ chuẩn bị thông điệp đề nghị chứa MAC, IP để nghị, Subnet mask, IP Server, Rental period), **DHCP Request** (Khi Client nhận được đề nghị và chấp nhận một trong các địa chỉ IP, Client sẽ phát tán thông điệp này để khẳng định nó đã chấp nhận IP này từ Server), **DHCP ACK** (Sau khi Client thuê được IP đó thì Server sẽ tự động rút các đơn chào hàng về địa chỉ IP đó) và **DHCP Release** (Client nhận được IP mới và sử dụng).

Rental period), **DHCP Request** (Khi Client nhận được đề nghị và chấp nhận một trong các địa chỉ IP , Client sẽ phát tán thông điệp này để khẳng định nó đã chấp nhận IP này từ Server), **DHCP ACK** (Sau khi Client thuê được IP đó thì Server sẽ tự động rút các đơn chào hàng về địa chỉ IP đó) và **DHCP Release** (Client nhận được IP mới và sử dụng).

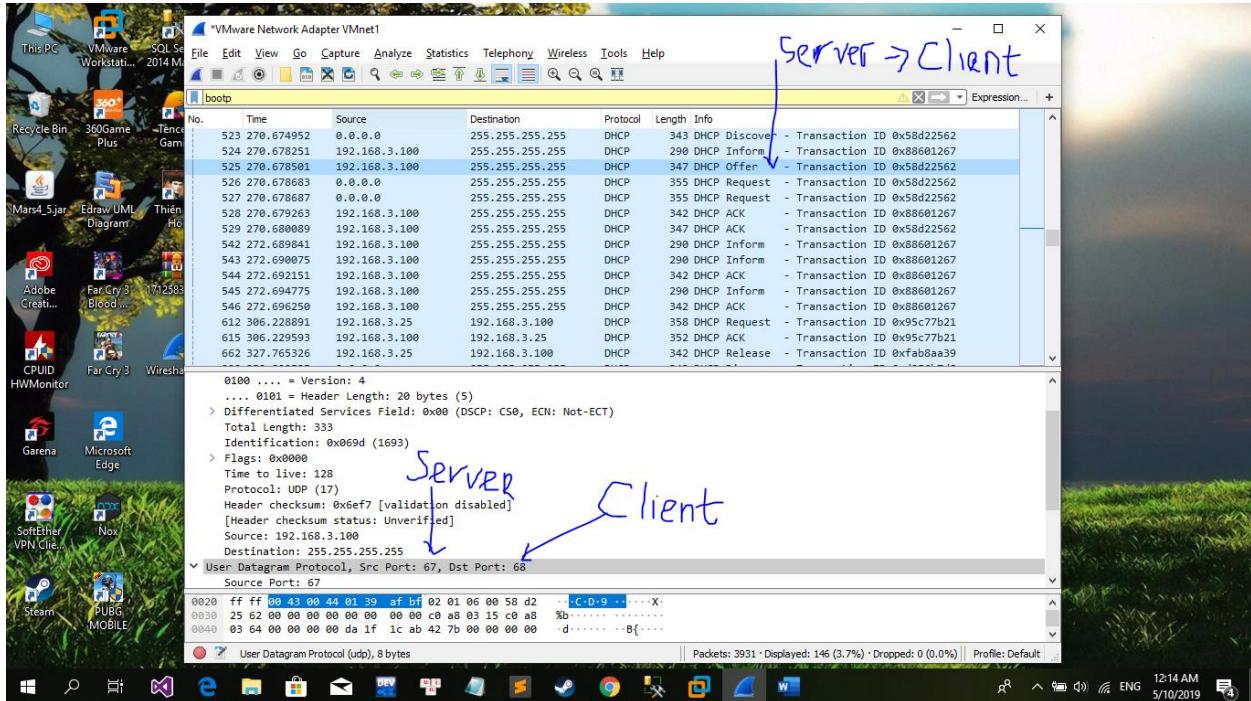
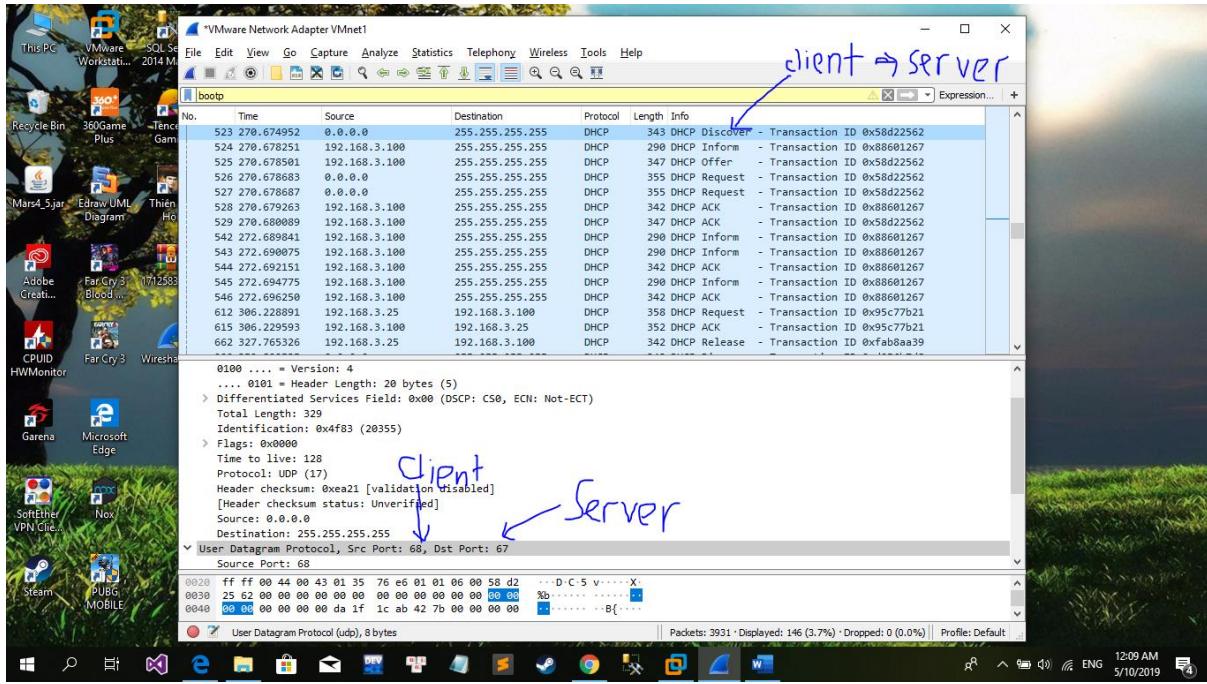


Câu 2.2: Dịch vụ DHCP sử dụng port ở server và client là bao nhiêu?

Dịch vụ DHCP sử dụng port ở server : 67

Dịch vụ DHCP sử dụng port ở client : 68

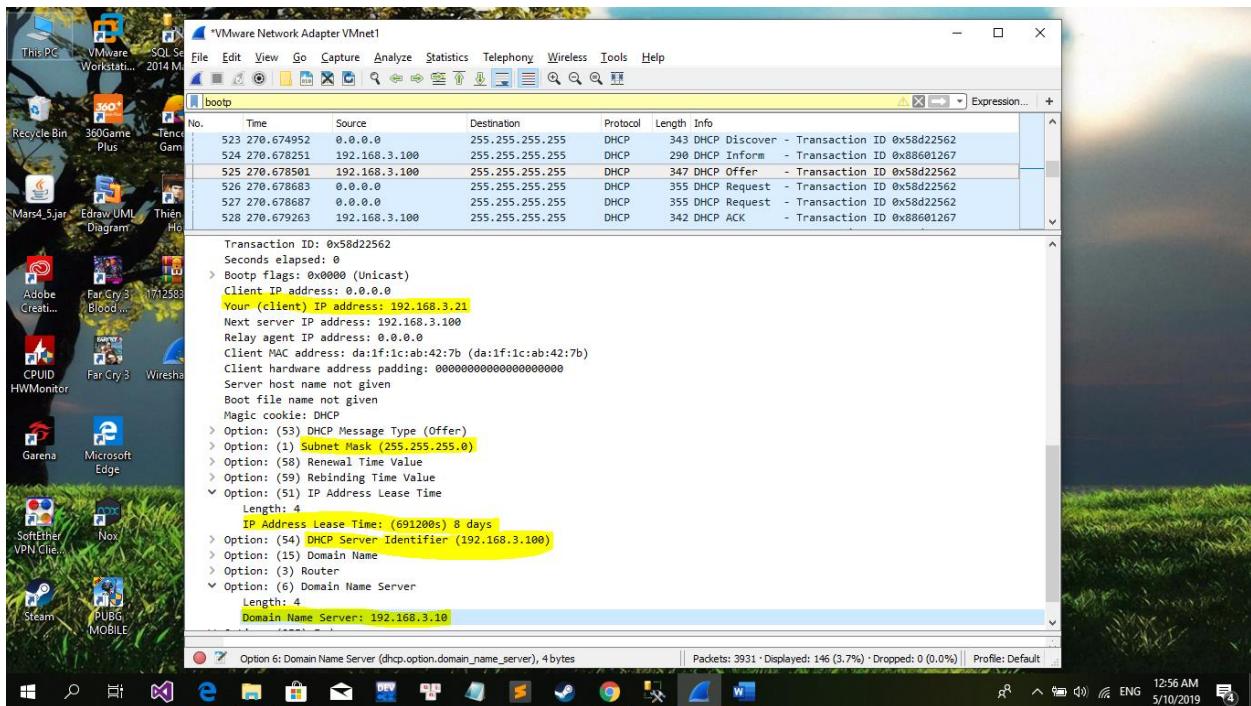
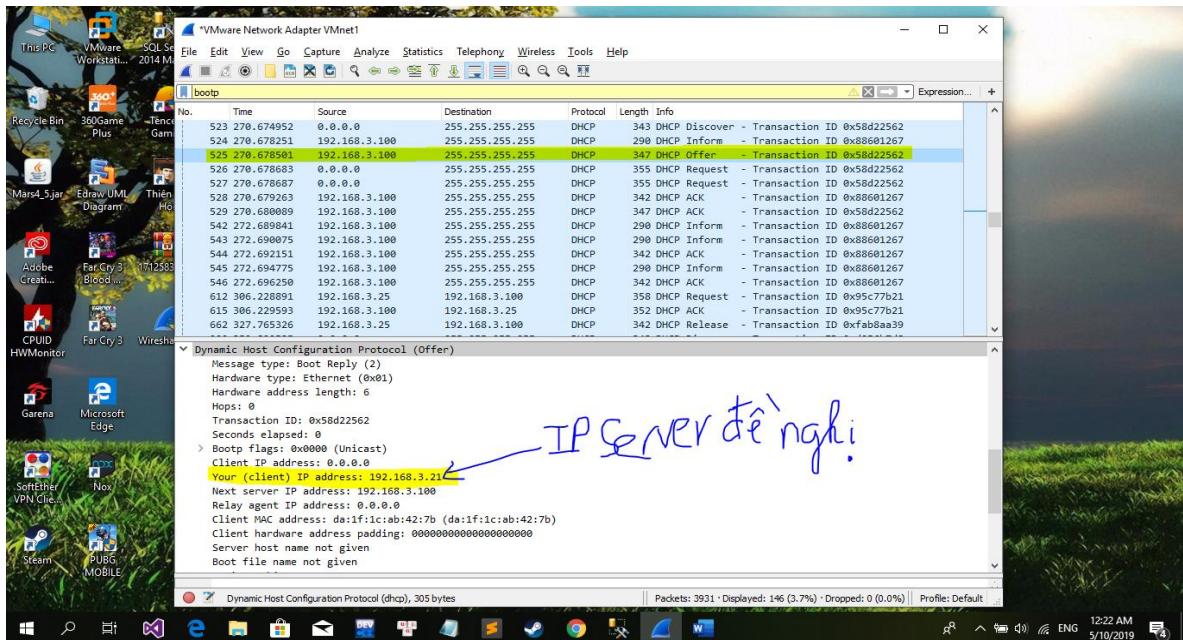
Hình dưới : Client gửi thông điệp đến Server nên Port Src là của Client và Port Dst là của Server



Hình trên là Server chuẩn bị gửi cho Client về Offer IP nên Port Src là của Server và Port Dst là của Client.

Câu 2.3: Địa chỉ IP mà DHCP server đề nghị cấp cho client được gửi từ gói tin nào?

Địa chỉ IP mà DHCP Server đề nghị cấp cho Client được gửi từ gói tin DHCP Offer như hình dưới. Nhưng IP mà DHCP Server đề nghị (192.168.3.21) không đáp ứng được Client nên sau cùng Client đã nhận được một IP khác(192.168.3.25) và chấp nhận IP này để sử dụng.



Gói tin trên chứa một số thông tin cơ bản như sau :

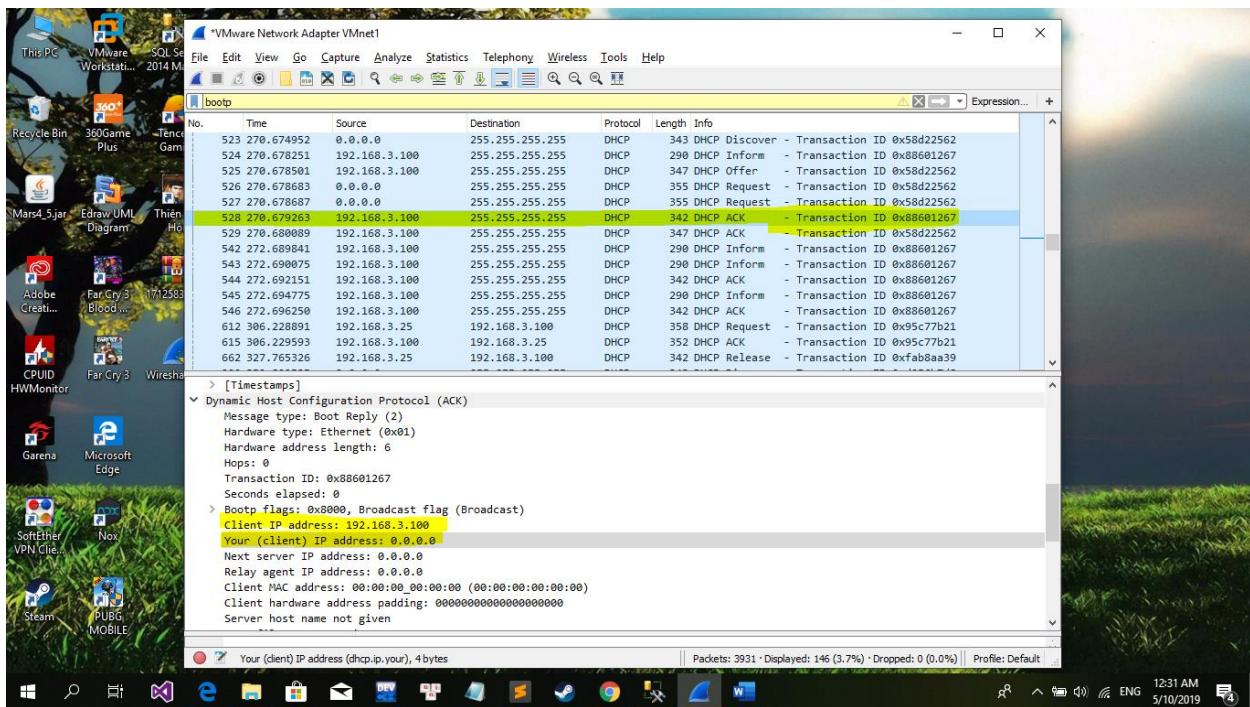
- Địa chỉ IP Client: 192.168.3.21
- Subnet Mask: 255.255.255.0
- DHCP Server: 192.168.3.100
- DNS Server: 192.168.3.10
- Lease Time: 8 days
-

Câu 2.4: Hãy cho biết sự khác biệt giữa 2 trường thông tin: Your IP address và Client IP Address trong gói tin DHCP ACK?

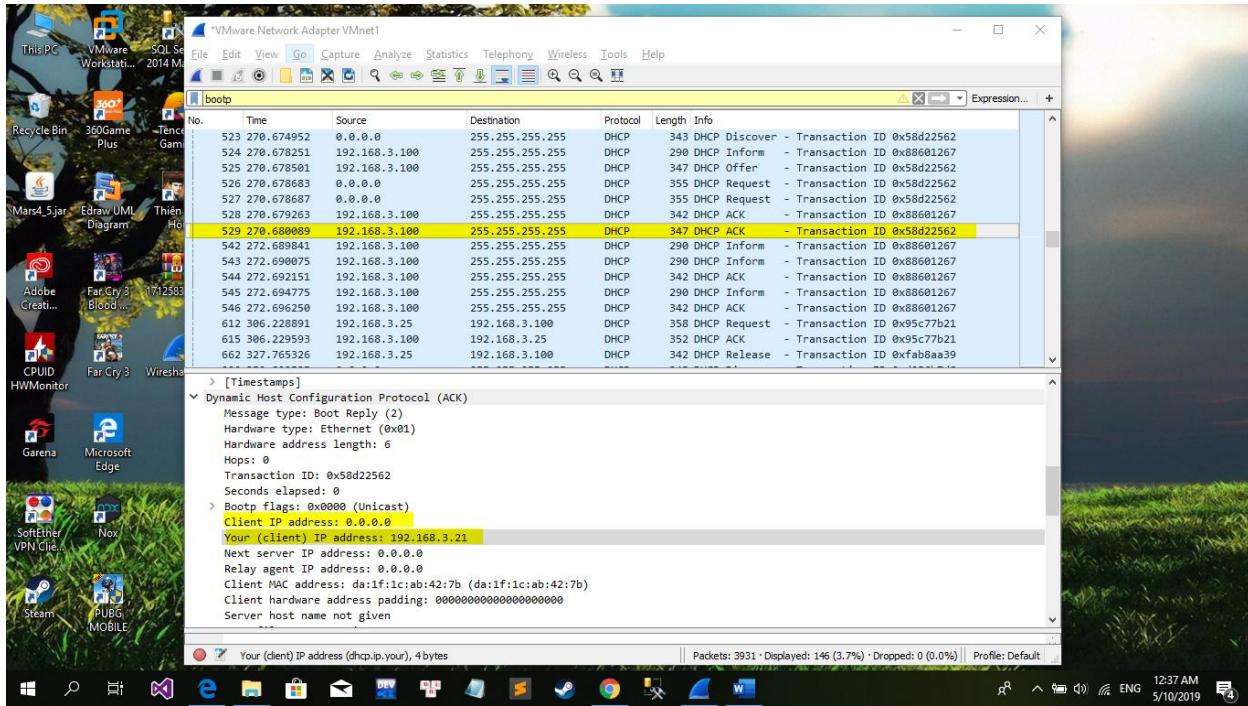
Sự khác biệt giữa 2 trường thông tin trên như sau:

Your IP Address (YID) : IP này được cấp bởi Server để đăng ký cho Client.

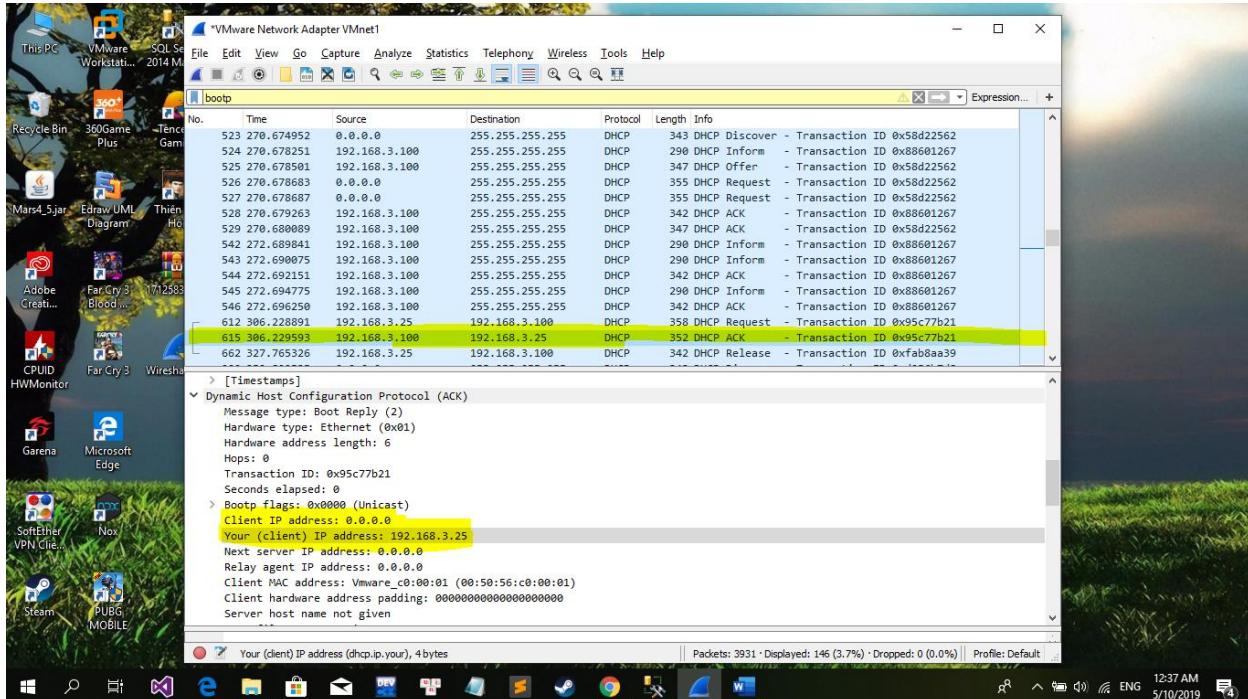
Client IP Address (CIA) : Client sẽ đặt IP của mình trong trường này nếu và chỉ nếu nó đang có IP hay đang xin cấp lại IP, còn nếu không sẽ mặc định là 0.0.0.0.



⇒ Hình trên Client IP Address là **192.168.3.100** (Lúc này Client có địa chỉ IP của nó là 192.168.3.100) và Your IP Address là **0.0.0.0** (Vì lúc này Server chưa cung cấp cho Client 1 IP nào cả nên mặc định là 0.0.0.0)



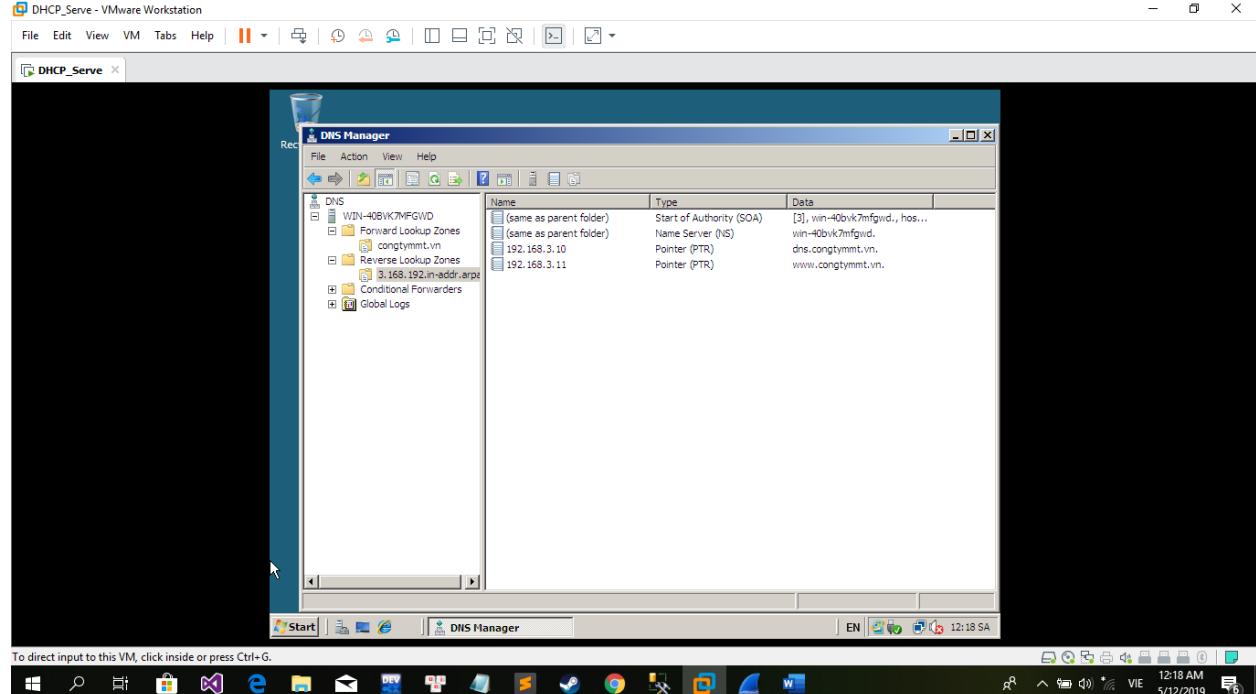
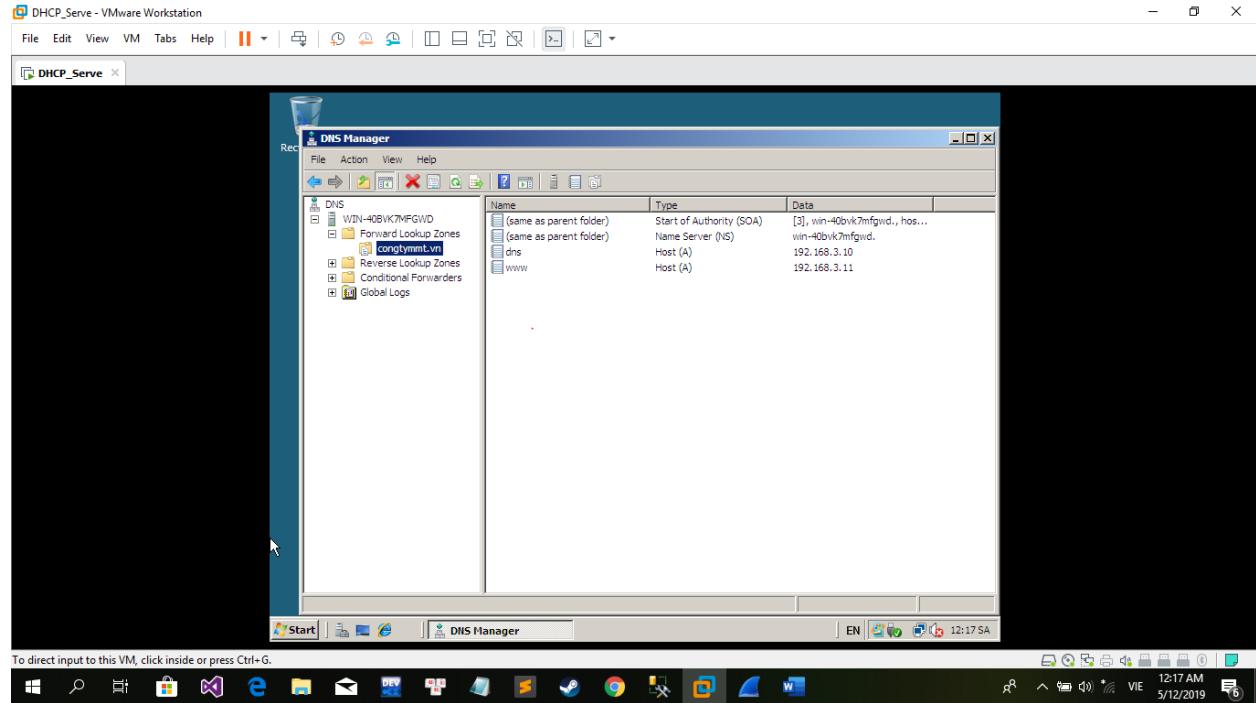
⇒ Hình trên Your IP Address là **192.168.3.21** (Lúc này Server cấp cho Client một địa chỉ IP mới là 192.168.3.21) và Client IP Address là **0.0.0.0** (IP của Client được cấp mới từ DHCP ACK trước)



=>Hình trên Your IP Address là **192.168.3.25** (Lúc này Server cấp lại cho Client 1 IP mới)và Client IP Address là **0.0.0.0** (Lúc này Client vẫn chưa nhận được IP từ Server).

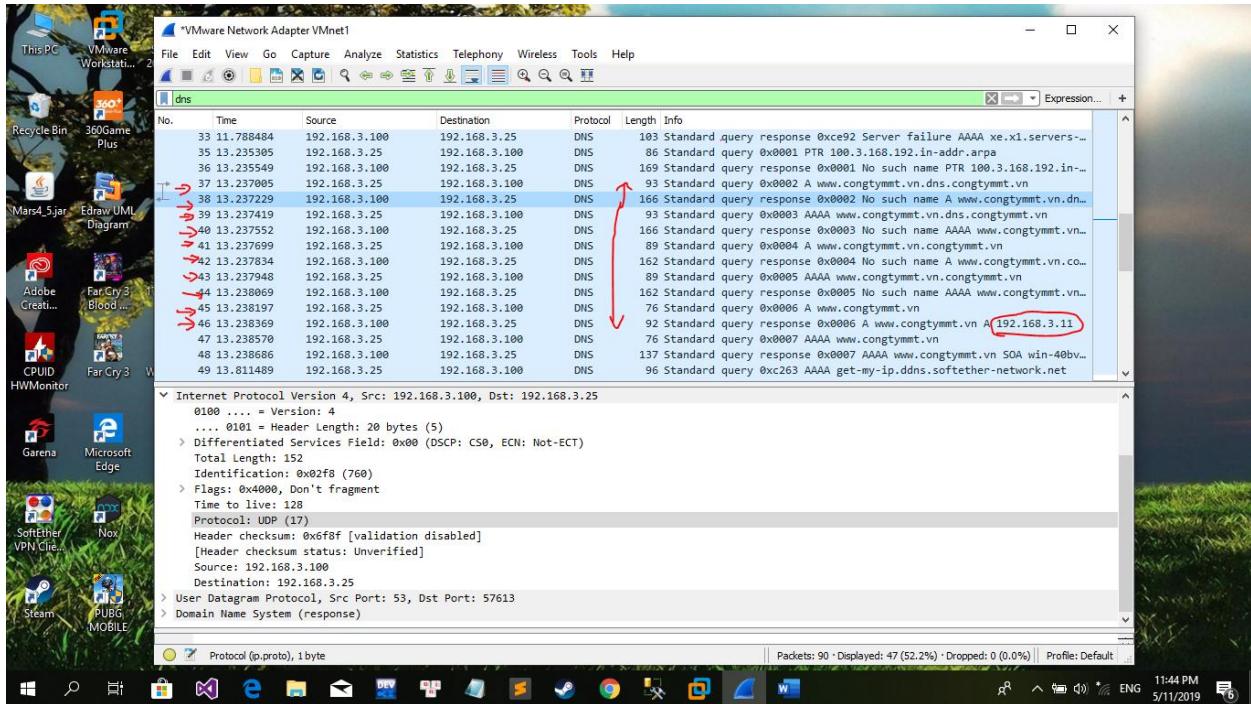
Câu 3:DNS

- Với mọi IP trong bài này thì $X = 03$



Câu 3.1: Có bao nhiêu gói tin được truyền và nhận trong quá trình truy vấn?

Có tổng cộng 10 gói tin được truyền đi và nhận về trong quá trình truy vấn. Client phải gửi thông tin yêu cầu IP của địa chỉ www.congtymmt.vn 5 lần thì Server mới phản hồi lại địa chỉ IP của www.congtymmt.vn ở lần phản hồi thứ 10. Tương đương với STT trong hình từ 37 đến 46.

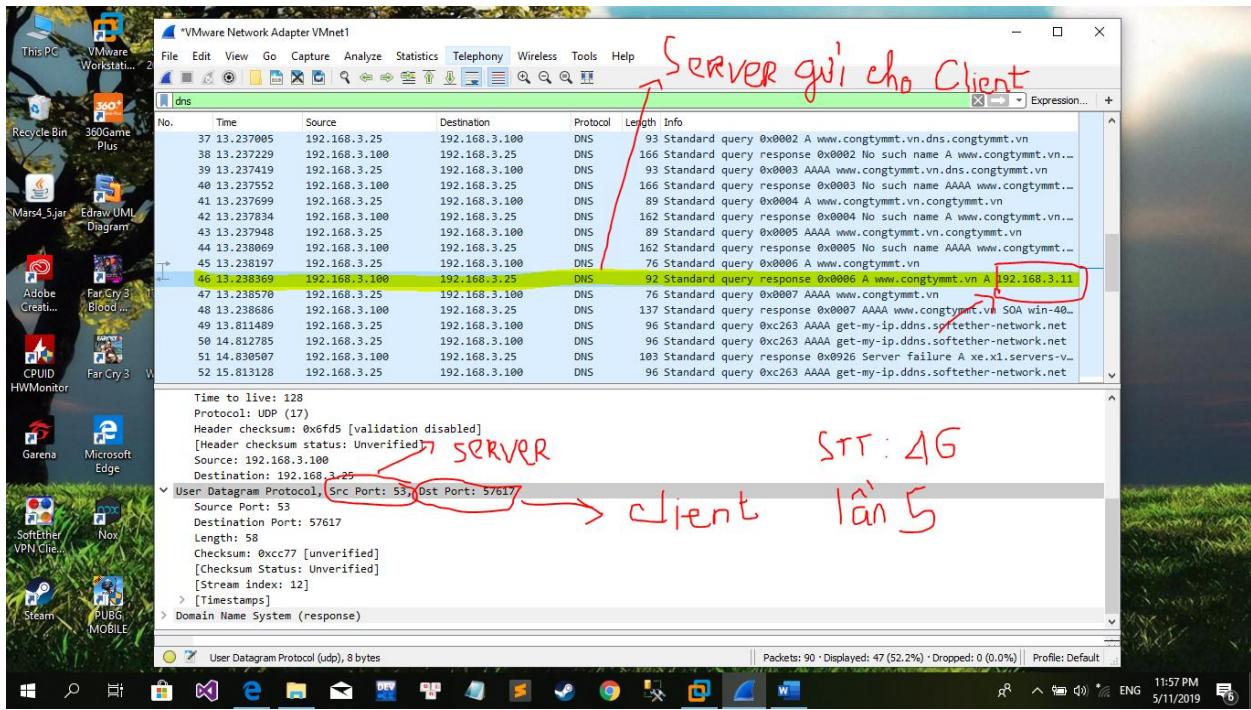
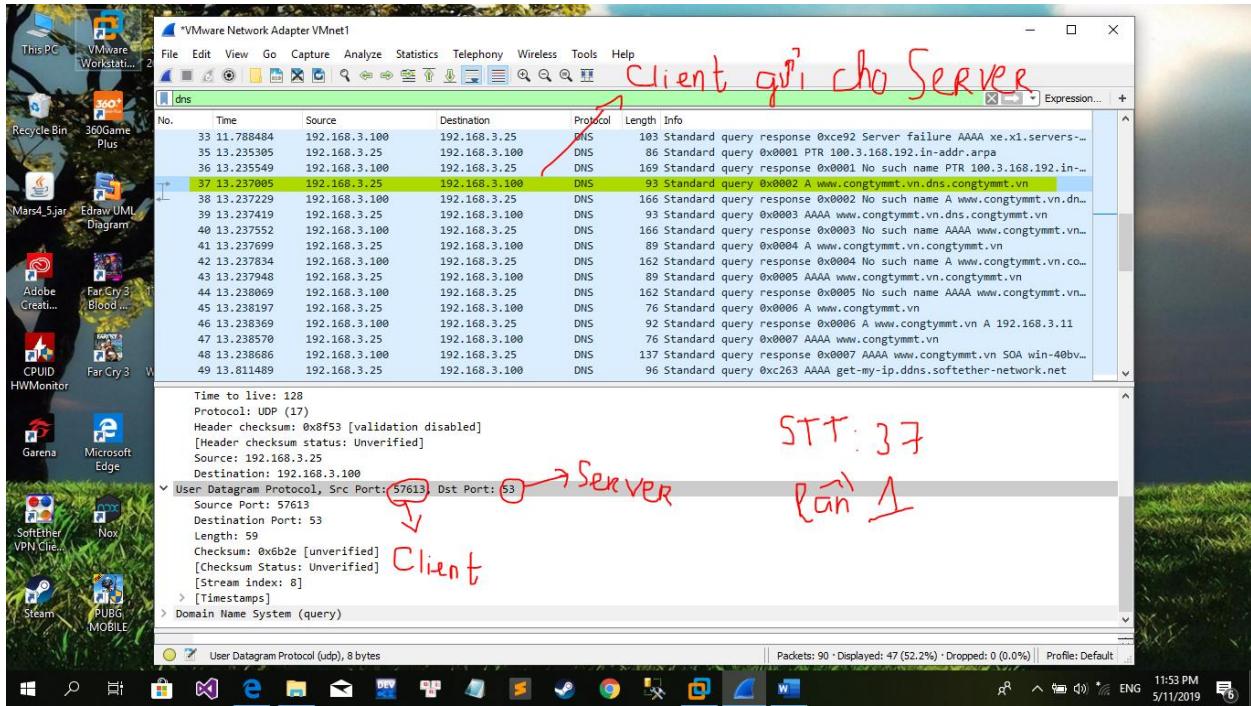


Câu 3.2 : DNS sử dụng port ở server và client là bao nhiêu?

DNS sử dụng port ở server là: 53

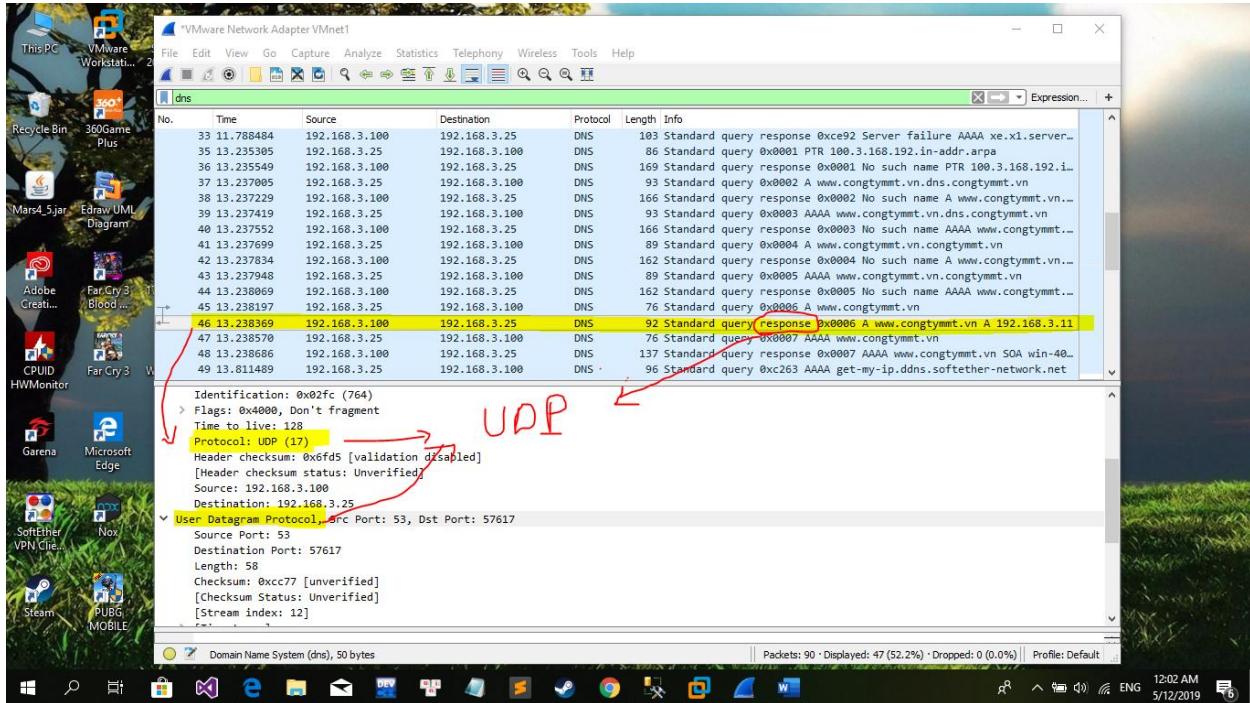
DNS sử dụng port ở client là: trong 5 lần gửi yêu cầu cho server thì port của client thay đổi từ 57613 đến 57617. (Lần 1: 57613, lần 2: 57614, lần 3: 57615, lần 4: 57616, lần 5: 57617).

Cuối cùng khi yêu cầu từ client và server phản hồi lại IP thì lúc này port của Server là 53 và port của Client là 57617.



Câu 3.3: Giao thức sử dụng ở tầng transportation của gói tin DNS responses?

Giao thức UDP (User Datagram Protocol) được sử dụng ở tầng Transportation của gói tin DNS responses.



Câu 3.4: Cho biết thông tin Name Server quản lý zone congtymmt.vn?

- Thông tin Name Server quản lý zone congtymmt.vn :
 - Tên Server: Unknown
 - Địa chỉ IP : 192.168.3.100
- Thông tin về www.congtymmt.vn :
 - Type: A
 - Class : IN
 - IP Address: 192.168.3.11

Windows Command Prompt window showing DNS lookup results:

```

C:\> nslookup www.congtymt.vn
Server: Unknown
Address: 192.168.3.100

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
Name: www.congtymt.vn
Address: 192.168.3.11

```

Handwritten annotation: "Name Server" with arrows pointing to the server address and the name.

Taskbar status: ENG 12:13 AM 5/12/2019

Wireshark capture showing DNS traffic:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|---------------|---------------|----------|--------|---|
| 33 | 11.788484 | 192.168.3.100 | 192.168.3.25 | DNS | 103 | Standard query response 0xce92 Server failure AAAA xe.x1.server.. |
| 35 | 13.235305 | 192.168.3.25 | 192.168.3.100 | DNS | 86 | Standard query 0x0001 PTR 100.3.168.192.in-addr.arpa |
| 36 | 13.235549 | 192.168.3.100 | 192.168.3.25 | DNS | 169 | Standard query response 0x0001 No such name PTR 100.3.168.192.i.. |
| 37 | 13.237085 | 192.168.3.25 | 192.168.3.100 | DNS | 93 | Standard query 0x0002 A www.congtymt.vn.dns.congtymt.vn |
| 38 | 13.237229 | 192.168.3.100 | 192.168.3.25 | DNS | 166 | Standard query response 0x0002 No such name A www.congtymt.vn.. |
| 39 | 13.237419 | 192.168.3.25 | 192.168.3.100 | DNS | 93 | Standard query 0x0003 AAAA www.congtymt.vn.dns.congtymt.vn |
| 40 | 13.237552 | 192.168.3.100 | 192.168.3.25 | DNS | 166 | Standard query response 0x0003 No such name AAAA www.congtymt.. |
| 41 | 13.237699 | 192.168.3.25 | 192.168.3.100 | DNS | 89 | Standard query 0x0004 A www.congtymt.vn.congtymt.vn |
| 42 | 13.237834 | 192.168.3.100 | 192.168.3.25 | DNS | 162 | Standard query response 0x0004 No such name A www.congtymt.vn.. |
| 43 | 13.237948 | 192.168.3.25 | 192.168.3.100 | DNS | 89 | Standard query 0x0005 AAAA www.congtymt.vn.congtymt.vn |
| 44 | 13.238069 | 192.168.3.100 | 192.168.3.25 | DNS | 162 | Standard query response 0x0005 No such name AAAA www.congtymt.. |
| 45 | 13.238197 | 192.168.3.25 | 192.168.3.100 | DNS | 76 | Standard query 0x0006 A www.congtymt.vn |
| 46 | 13.238369 | 192.168.3.100 | 192.168.3.25 | DNS | 92 | Standard query response 0x0006 A www.congtymt.vn A 192.168.3.11 |
| 47 | 13.238570 | 192.168.3.25 | 192.168.3.100 | DNS | 76 | Standard query 0x0007 AAAA www.congtymt.vn |
| 48 | 13.238686 | 192.168.3.100 | 192.168.3.25 | DNS | 137 | Standard query response 0x0007 AAAA www.congtymt.vn SOA win-40.. |
| 49 | 13.811489 | 192.168.3.25 | 192.168.3.100 | DNS | 96 | Standard query 0xc263 AAAA get-my-ip.ddns.softether-network.net |

Handwritten annotation: "Queries" and "Answers" with arrows pointing to specific sections in the Wireshark capture.

Taskbar status: ENG 12:15 AM 5/12/2019