

**TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA CÔNG NGHỆ THÔNG TIN**



**MÔN HỌC: MẠNG MÁY TÍNH
LỚP CỬ NHÂN TÀI NĂNG 2017**

BÁO CÁO ĐỒ ÁN THỰC HÀNH 1 PHÂN TÍCH GÓI TIN

GIẢNG VIÊN:

Đỗ Hoàng Cường
Lê Quốc Hòa
Nguyễn Thành Long
Lê Hà Minh

NHÓM THỰC HIỆN:

1712152 | Nguyễn Thị Mai Thanh
1712228 | Phạm Việt Nga
1712807 | Nguyễn Thị Minh Thùy

BÀI 1: GÓI TIN TRUY CẬP WEB

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

Internet Protocol Version 4, Src: 216.58.199.99, Dst: 172.29.51.16

- IP nguồn: 216.58.199.99
- IP đích: 172.29.51.16

Ethernet II, Src: IntelCor_8c:5e:ba (00:1c:c0:8c:5e:ba), Dst: Dell_e7:b3:9f (20:47:47:e7:b3:9f)

- MAC nguồn: 00:1c:c0:8c:5e:ba
- MAC đích: 20:47:47:e7:b3:9f

2. Cho biết thông tin port nguồn, port đích của gói tin?

Transmission Control Protocol, Src Port: 443, Dst Port: 54102, Seq: 47, Ack: 414, Len: 74

Source Port: 443

Destination Port: 54102

- Port nguồn: 443
- Port đích: 54102

3. Gói tin trên sử dụng giao thức gì ở tầng Application?

Secure Sockets Layer

> TLSv1.2 Record Layer: Application Data Protocol: http-over-tls

- Gói tin sử dụng giao thức TLSv1.2 ở tầng Application.

4. Cho biết giao thức được sử dụng ở tầng Transportation?

- Giao thức TCP được sử dụng ở tầng Transportation.

Flags: 0x00

Fragment offset: 0

Time to live: 54

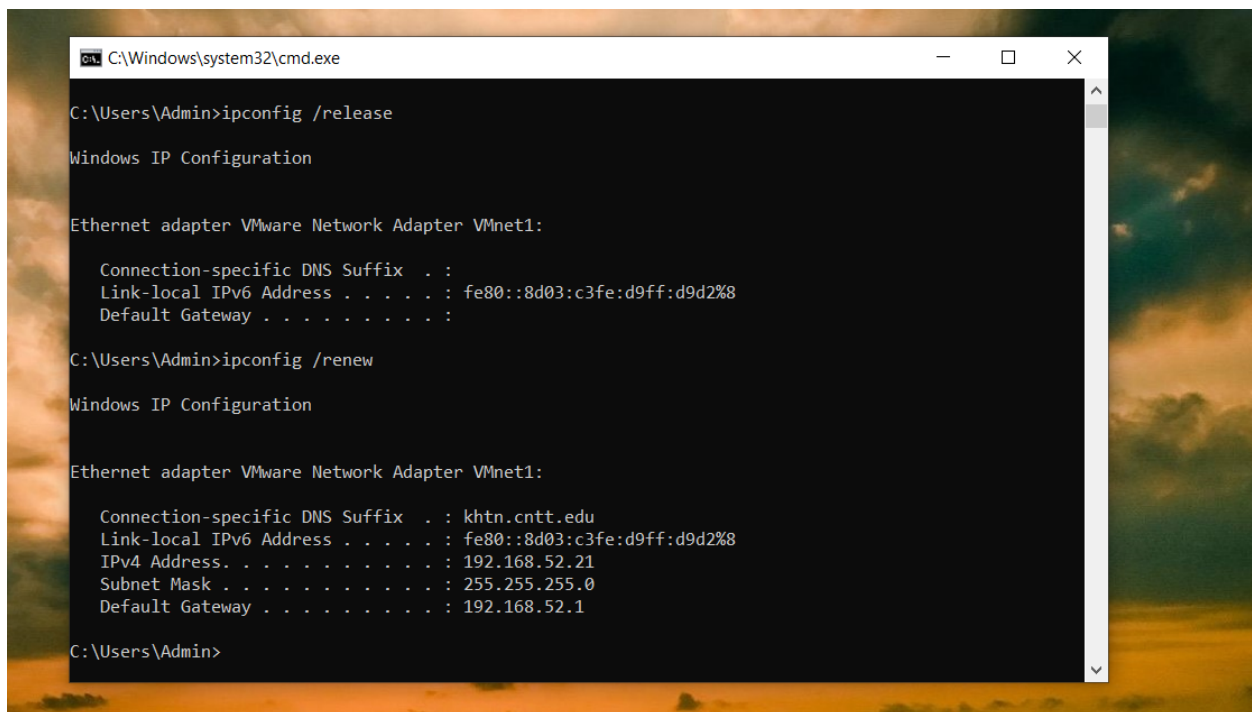
Protocol: TCP (6)

BÀI 2: DHCP

** Ghi chú: lấy $X = 52$.

- DHCP – DNS server có địa chỉ IP 192.168.X.100 ~ 192.168.52.100
- Card mạng VMnet1 được cấp địa chỉ IP 192.168.52.21 từ DHCP – DNS server cấu hình trên máy ảo.

1. Tên các gói tin DHCP bắt được trong quá trình xin cấp mới địa chỉ IP?



```
C:\Windows\system32\cmd.exe

C:\Users\Admin>ipconfig /release

Windows IP Configuration

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::8d03:c3fe:d9ff:d9d2%8
    Default Gateway . . . . . : 

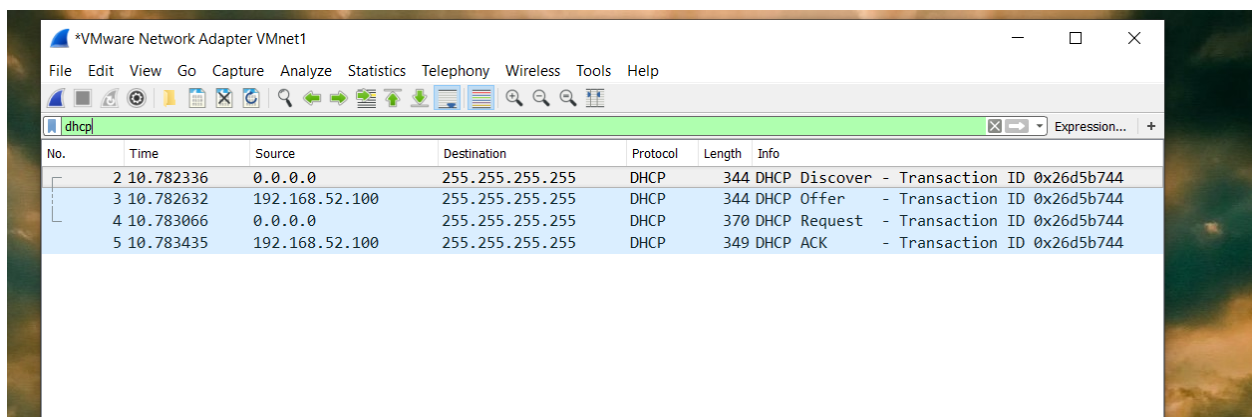
C:\Users\Admin>ipconfig /renew

Windows IP Configuration

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . : khtn.cntt.edu
    Link-local IPv6 Address . . . . . : fe80::8d03:c3fe:d9ff:d9d2%8
    IPv4 Address. . . . . : 192.168.52.21
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.52.1

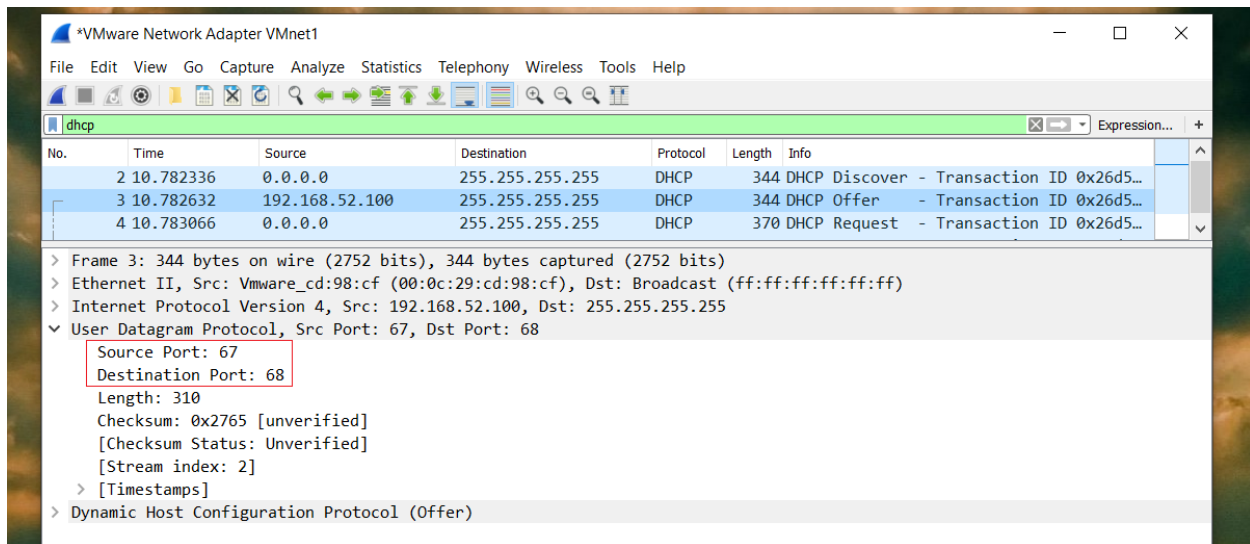
C:\Users\Admin>
```



No.	Time	Source	Destination	Protocol	Length	Info
2	10.782336	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x26d5b744
3	10.782632	192.168.52.100	255.255.255.255	DHCP	344	DHCP Offer - Transaction ID 0x26d5b744
4	10.783066	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x26d5b744
5	10.783435	192.168.52.100	255.255.255.255	DHCP	349	DHCP ACK - Transaction ID 0x26d5b744

- Có 4 gói tin DHCP bắt được trong quá trình xin cấp mới địa chỉ IP.
 - **DHCP Discover:** gói tin từ client khi mới bắt đầu tham gia vào hệ thống mạng, nội dung gói tin yêu cầu thông tin địa chỉ IP từ DHCP server. Có thể thấy địa chỉ IP nguồn (của client) là 0.0.0.0 bởi lúc này client chưa có địa chỉ IP.
 - **DHCP Offer:** gói tin server gửi phản hồi lại client về địa chỉ IP mà server mong muốn cấp cho client.
 - **DHCP Request:** gói tin client gửi lại server để xác nhận việc nó muốn nhận địa chỉ IP nào sau khi nhận được gói tin DHCP Offer từ server.
 - **DHCP ACK:** gói tin server gửi cho client để kiểm tra và xác nhận lại các thông tin đã thỏa thuận giữa server và client trong suốt quá trình trao đổi. Client có thể tham gia trên mạng TCP/IP và hoàn thành hệ thống khởi động.

2. Dịch vụ DHCP sử dụng port ở server và client là bao nhiêu?



- Port ở server: 67
- Port ở client: 68

3. Địa chỉ IP mà DHCP server đề nghị cấp cho client được gửi từ gói tin nào?

No.	Time	Source	Destination	Protocol	Length	Info
20	8.542561	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x5b4741a3
21	8.542846	192.168.52.100	255.255.255.255	DHCP	344	DHCP Offer - Transaction ID 0x5b4741a3
22	8.543260	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x5b4741a3
23	8.543603	192.168.52.100	255.255.255.255	DHCP	349	DHCP ACK - Transaction ID 0x5b4741a3
224	32.495270	192.168.52.21	192.168.52.100	DHCP	358	DHCP Request - Transaction ID 0xe811d764
225	32.496957	192.168.52.100	192.168.52.21	DHCP	349	DHCP ACK - Transaction ID 0xe811d764

> Frame 225: 349 bytes on wire (2792 bits), 349 bytes captured (2792 bits)

> Ethernet II, Src: Vmware_ae:7a:66 (00:0c:29:ae:7a:66), Dst: Vmware_c0:00:01 (00:50:56:c0:00:01)

> Internet Protocol Version 4, Src: 192.168.52.100, Dst: 192.168.52.21

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 335

Identification: 0x026d (621)

> Flags: 0x0000

Time to live: 128

Protocol: UDP (17)

Header checksum: 0xd67 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.52.100

Destination: 192.168.52.21

> User Datagram Protocol, Src Port: 67, Dst Port: 68

> Dynamic Host Configuration Protocol (ACK)

wireshark_VMware Network Adapter VMnet1_20190411180031_a01996.pcap | Packets: 313 · Displayed: 6 (1.9%) · Dropped: 0 (0.0%) | Profile: Default

- Được gửi từ gói tin cuối cùng DHCP ACK.

4. Nêu sự khác biệt giữa hai trường thông tin: Your IP address và Client IP Address trong gói tin DHCP ACK?

- Your IP address: là địa chỉ được cấp bởi server để đăng ký cho client. Là địa chỉ IP mà VMnet1 được cấp từ DHCP server cấu hình trên VMWare.
 - > Bootp flags: 0x0000 (Unicast)
 - Client IP address: 0.0.0.0
 - Your (client) IP address: 192.168.52.21
- Client IP address: Nếu client đang có IP hay đang xin cấp lại IP thì client sẽ tự đặt IP của mình trong trường này. Nếu không nằm trong hai điều kiện trên thì mặc định là 0.0.0.0 và trong trường hợp trên, client không có IP và được nhận IP động từ phía server nên **client IP address: 0.0.0.0**

BÀI 3: DNS

Thực hiện truy vấn DNS tại máy thật địa chỉ www.congtymmt.vn

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.437]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Admin>nslookup www.congtymmt.vn
Server: UnKnown
Address: 192.168.52.100

Name: www.congtymmt.vn
Address: 192.168.52.11

C:\Users\Admin>
```

Từ việc truy vấn trên, ta có địa chỉ của www.congtymmt.vn là: 192.168.52.11 đúng như ban đầu cấu hình PTR record.

1. Có bao nhiêu gói tin được truyền và nhận trong quá trình truy vấn?

The screenshot shows a Wireshark capture of network traffic on the VMnet1 interface. The DNS filter is applied, showing six packets. The first four packets are queries from the client (192.168.52.21) to the server (192.168.52.100), and the last two are responses from the server back to the client.

No.	Time	Source	Destination	Protocol	Length	Info
2	0.688593	192.168.52.21	192.168.52.100	DNS	87	Standard query 0x0001 PTR 100.52.168.192.in-addr.arpa
3	0.688823	192.168.52.100	192.168.52.21	DNS	163	Standard query response 0x0001 No such name PTR 100.52.168.192.in-addr.arpa SOA quochoa
4	0.689713	192.168.52.21	192.168.52.100	DNS	76	Standard query 0x0002 A www.congtymmt.vn
5	0.689914	192.168.52.100	192.168.52.21	DNS	92	Standard query response 0x0002 A www.congtymmt.vn A 192.168.52.11
6	0.690206	192.168.52.21	192.168.52.100	DNS	76	Standard query 0x0003 AAAA www.congtymmt.vn
7	0.690379	192.168.52.100	192.168.52.21	DNS	125	Standard query response 0x0003 AAAA www.congtymmt.vn SOA may

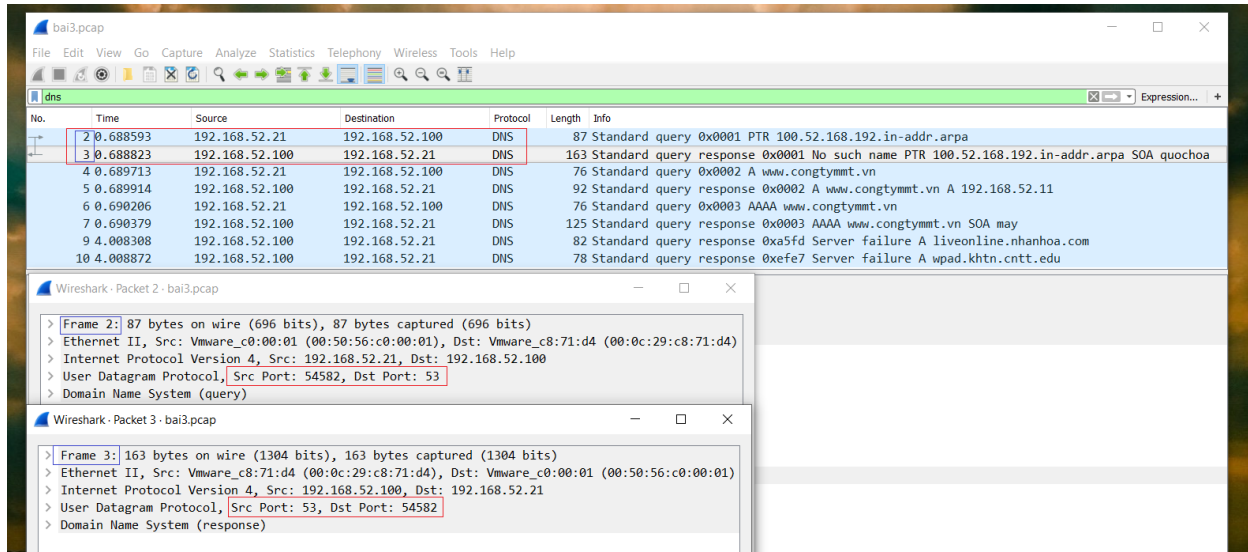
Below the Wireshark window, a command prompt window shows the output of the nslookup command, confirming the IP address 192.168.52.11 for www.congtymmt.vn.

- Có 6 gói tin được truyền và nhận trong quá trình truy vấn (trong đó, 4 gói tin được truyền đi từ server tới client và 2 gói tin server nhận lại từ client).

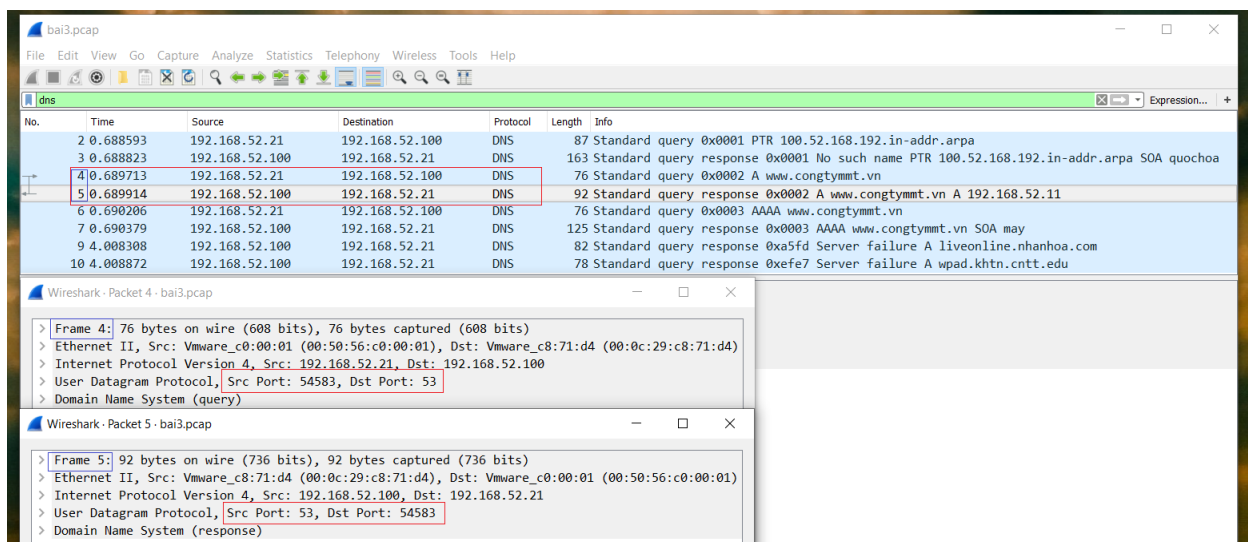
- 2 gói tin cuối cùng không phải truy vấn địa chỉ www.congtymmt.vn

2. DNS sử dụng port ở server và client là bao nhiêu?

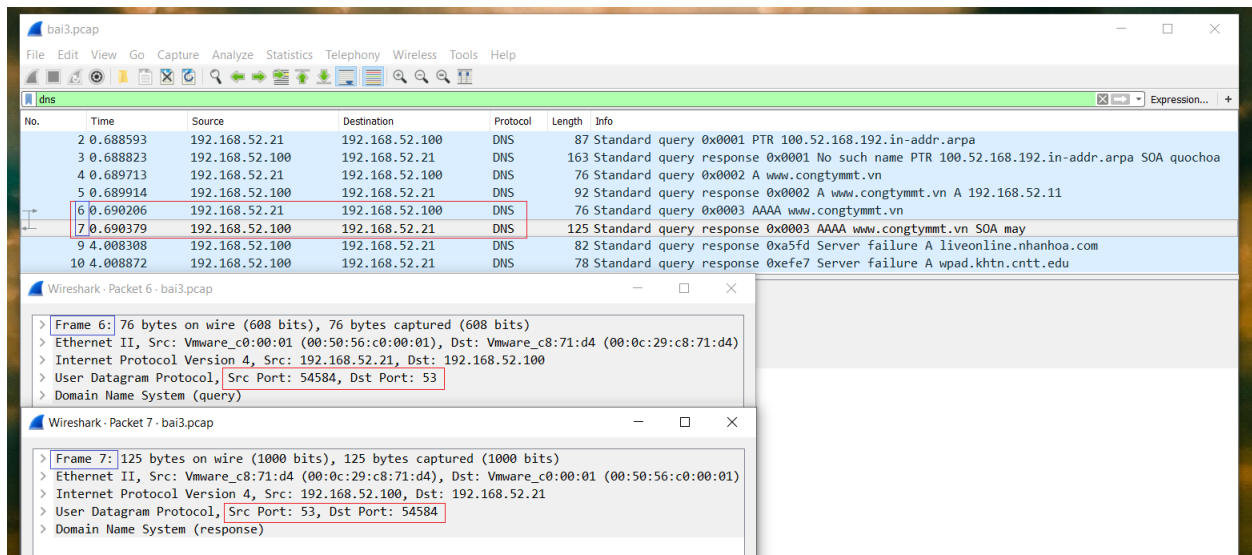
- Port ở server: 53
- Port ở client:
 - 2 gói đầu: 54582



- 2 gói tiếp: 54583

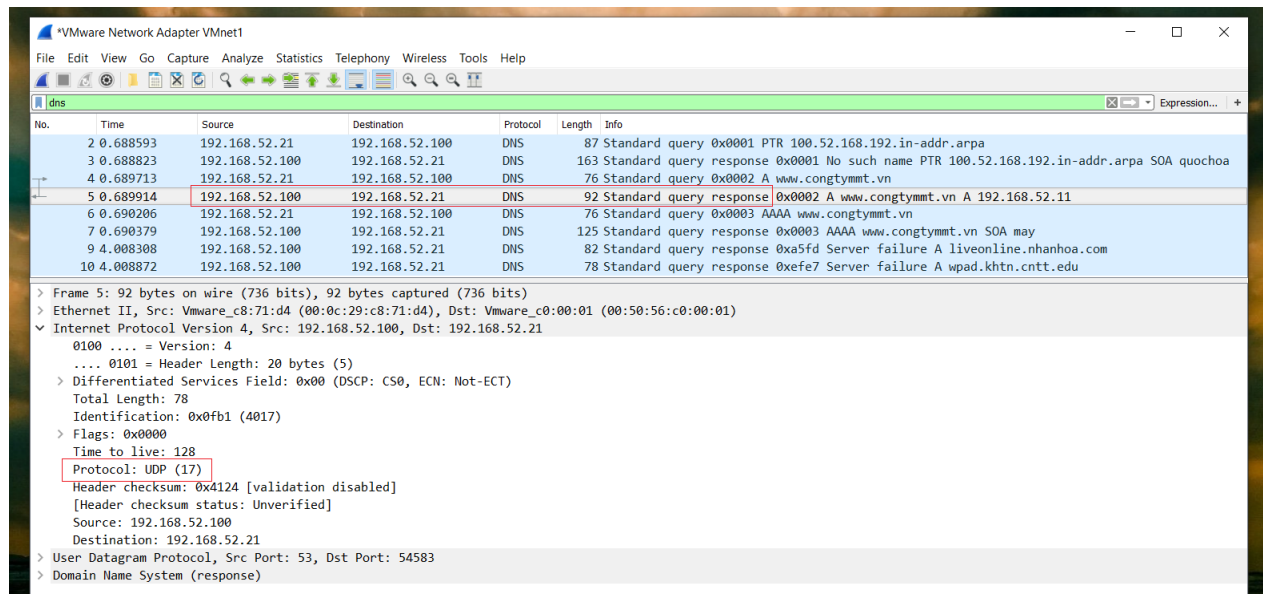


- 2 gói cuối: 54584



**** Chú thích hình ảnh:** đóng khung màu đỏ (gói tin và port tương ứng), đóng khung màu xanh (ánh xạ vị trí gói tin bắt được với thông tin chi tiết của gói tin).

3. Giao thức sử dụng ở tầng transportation của gói tin DNS responses?



- Giao thức UDP được sử dụng ở tầng transportation của gói tin DNS responses.

4. Cho biết thông tin Name Server quản lý zone congtymmt.vn?