Họ và tên: Lê Trung Sơn

MSSV: 1810482

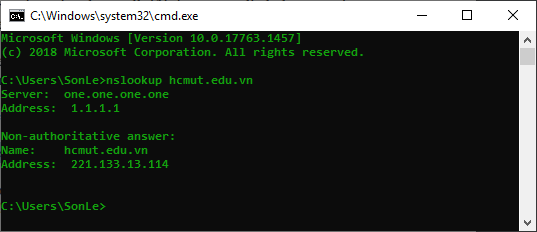
LAB 2

**I. nslookup**

**1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?**

- Vhọn website là hcmut.edu.vn

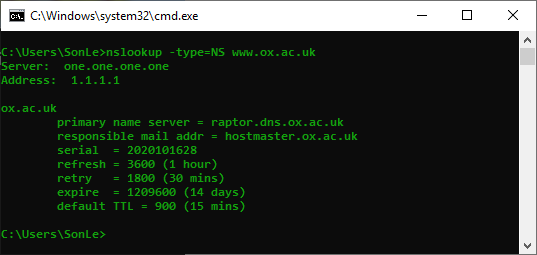
- IP của server là 221.133.13.114



2. Run nslookup to determine the authoritative DNS servers for a university in Europe.

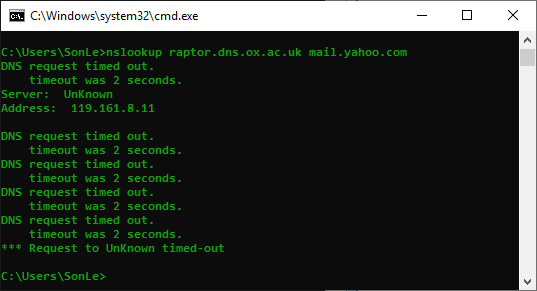
- Chọn trường đại học Oxford

- Máy chủ DNS có thẩm quyền cho Oxford là raptor.dns.ox.ac.uk



3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

- IP là 119.161.8.11

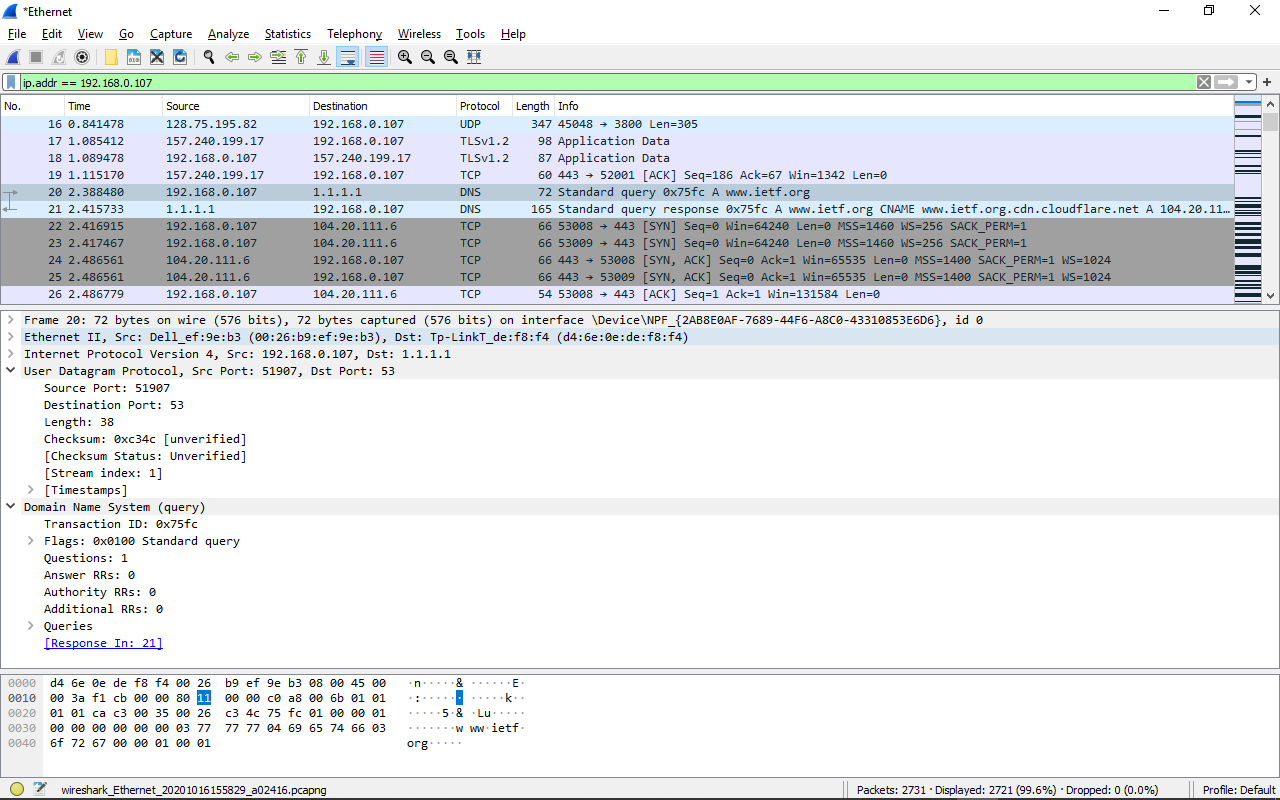


**II. ipconfig**

**III. Tracing DNS with Wireshark**

4. Locate the DNS query and response messages. Are then sent over UDP or TCP?

- Các truy vấn và phản hồi thông qua UDP (packet 20)



5. What is the destination port for the DNS query message? What is the source port of DNS response message?

- Destination port của DNS query message là 53

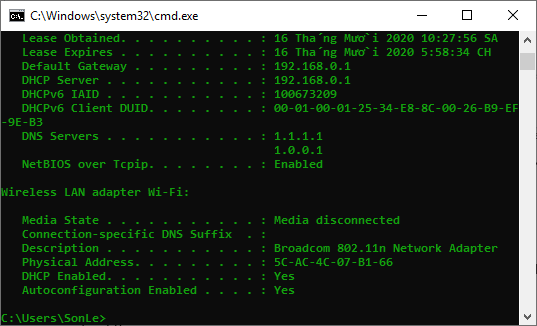
- Source port DNS response message cũng là 53

6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

- IP mà DNS query gửi đến là 1.1.1.1

- Sử dụng lệnh ipconfig /all để xác định IP của local DNS server

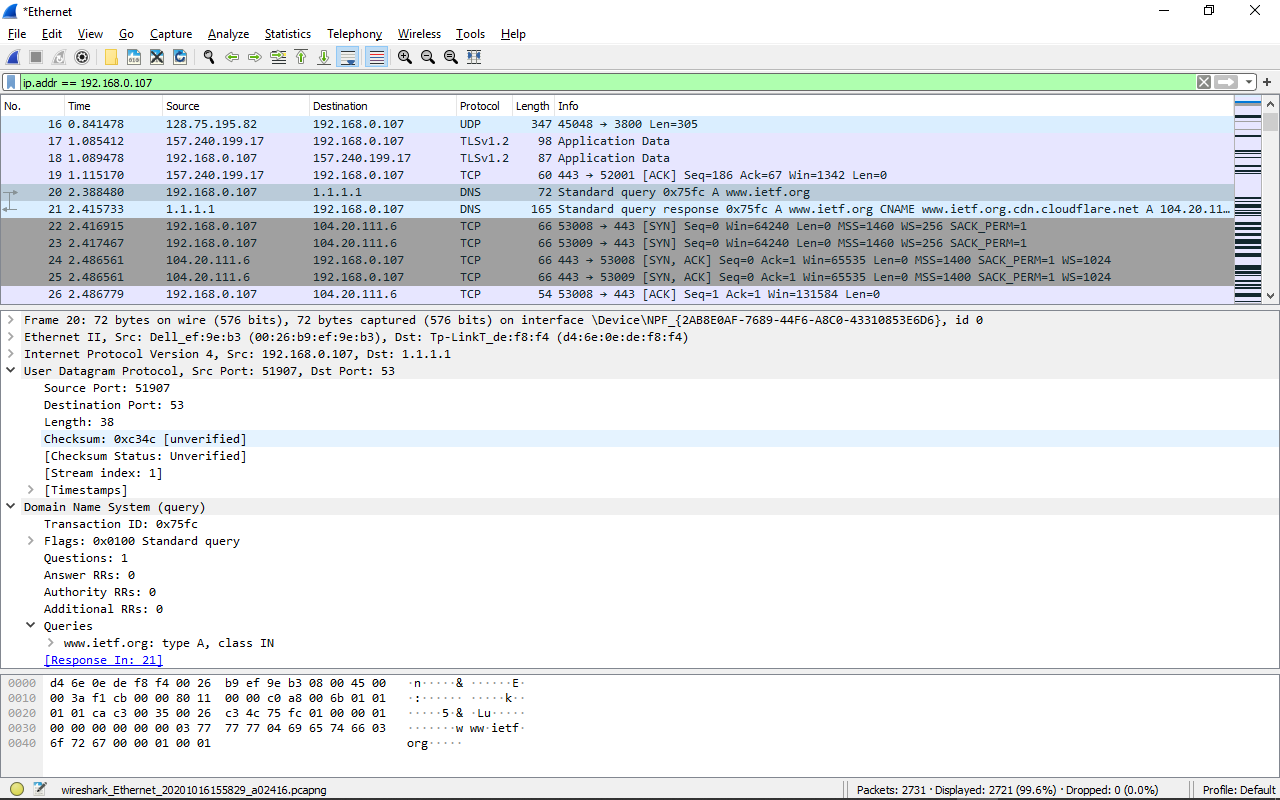
- 2 địa chỉ IP trên là giống nhau



7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

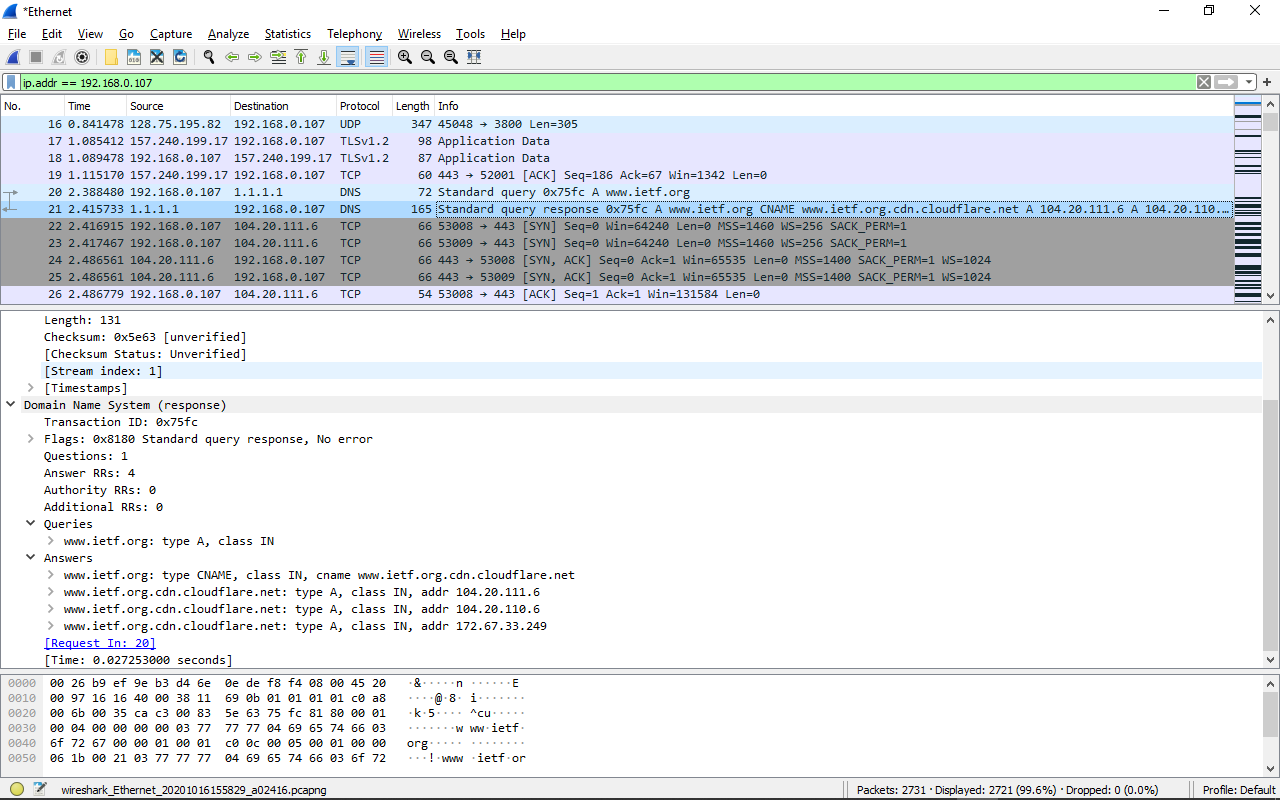
- Type của DNS là type A

- Không có “answers”



8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

- Có 1 “answer” trong bảng. Nó bao gồm các địa chỉ IP của trang web



9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

- Địa chỉ IP đích của SYN là 104.20.111.6 tương ứng với địa chỉ cung cấp bởi DNS response, đây cũng là địa chỉ type A của trang web

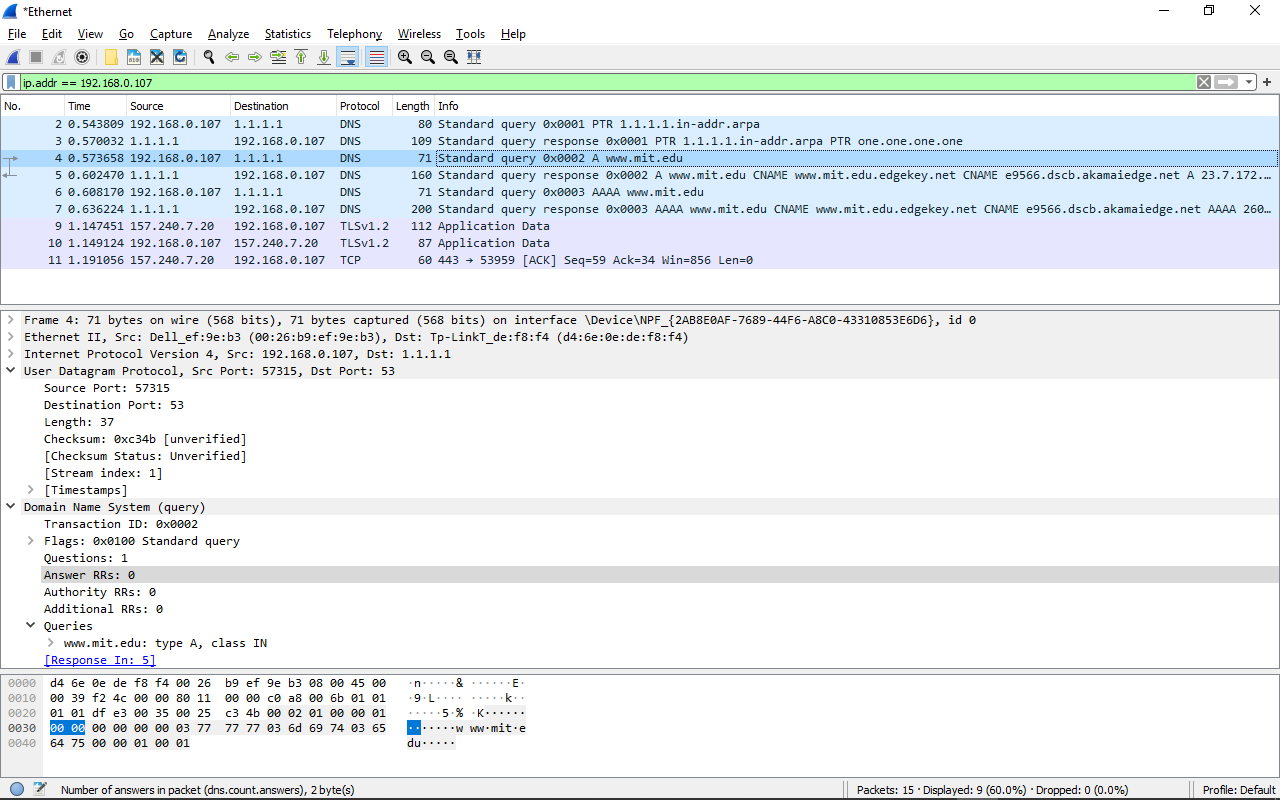
10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

- Không cần truy vấn DNS cho mỗi hình ảnh vì tất cả hình đều được load từ website xuống

11. What is the destination port for the DNS query message? What is the source port of DNS response message?

- Destination port của DNS query message là 53

- Source port DNS response message cũng là 53



12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

- IP mà DNS query message gửi đến chính là địa chỉ local DNS server 1.1.1.1 của máy

13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

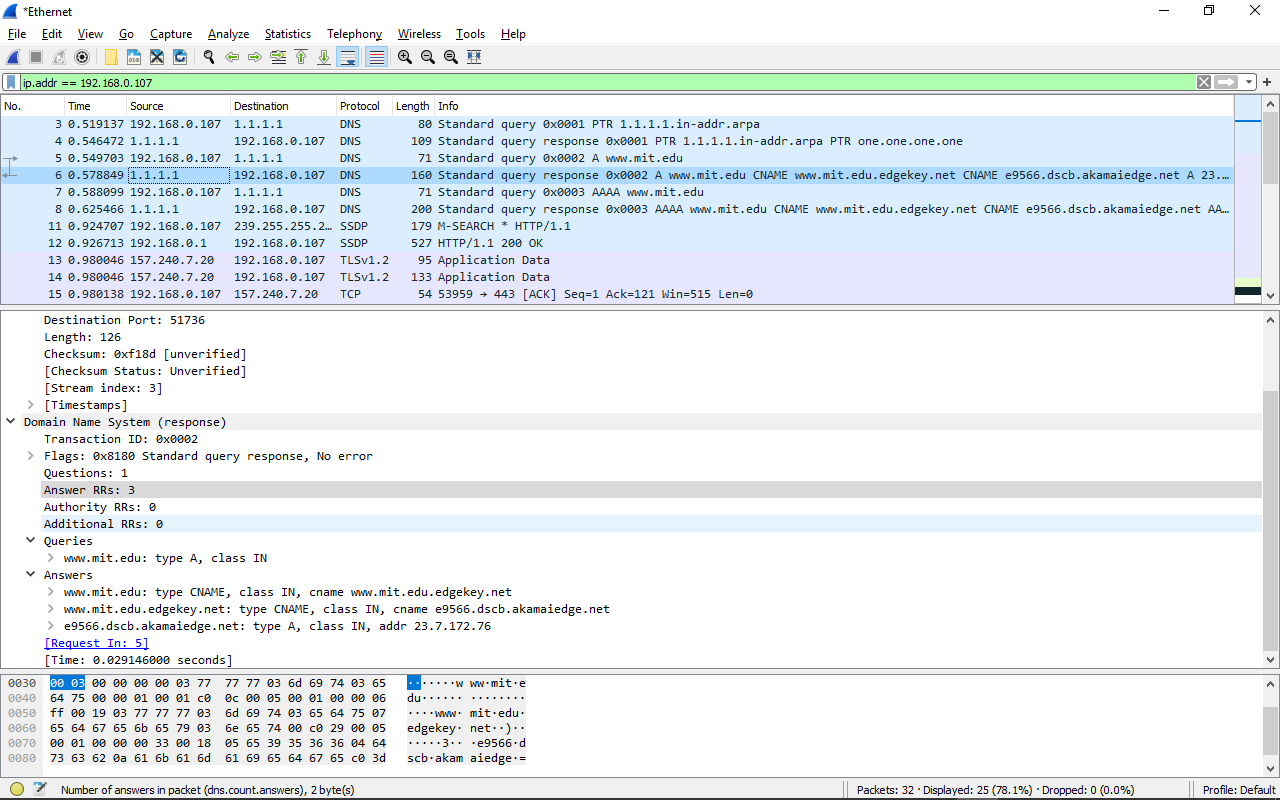
- Type là A và không có answers nào trong bảng

14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

- Nó có 1 answer bao gồm 3 thông tin máy chủ

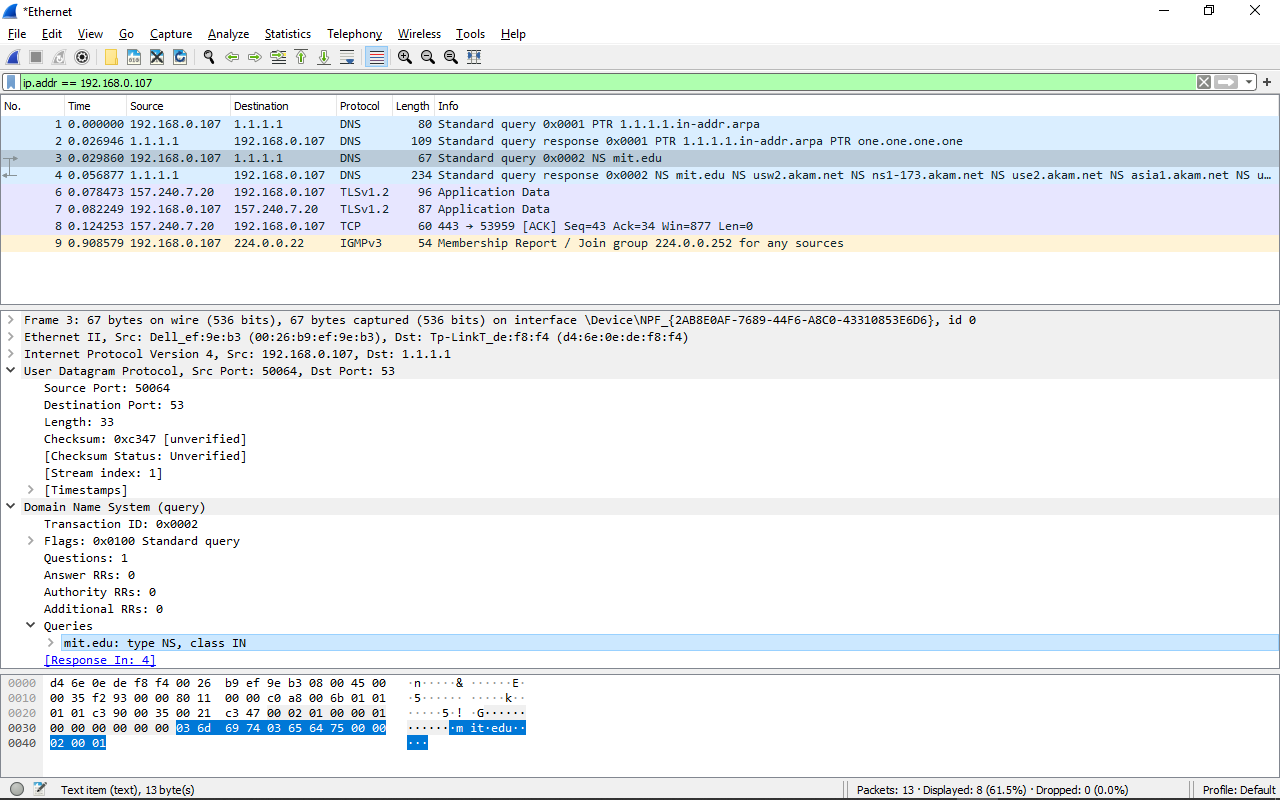
15. Provide a screenshot.

- Hình ở trên



16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

- IP mà DNS query message gửi đến chính là địa chỉ local DNS server 1.1.1.1 của máy



17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

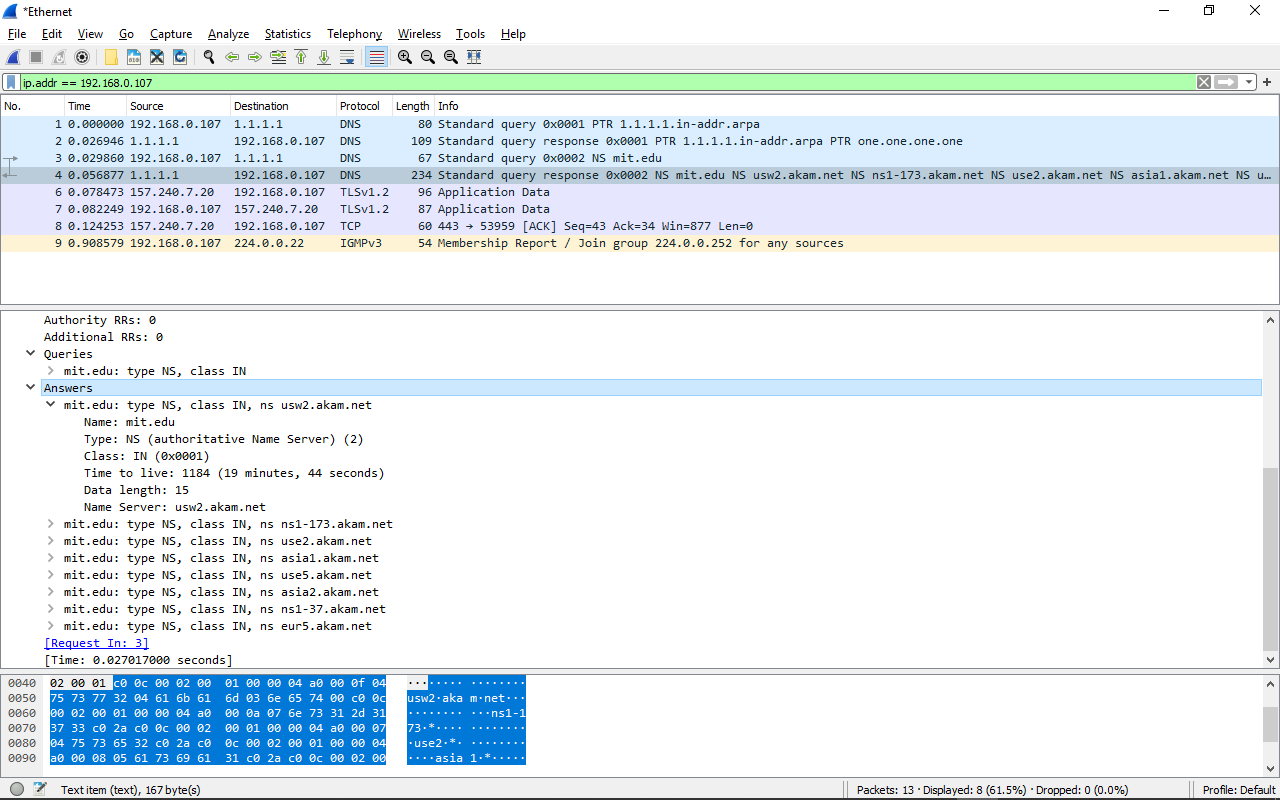
- Type của DNS query là NS và không có answers nào trong bảng

18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?

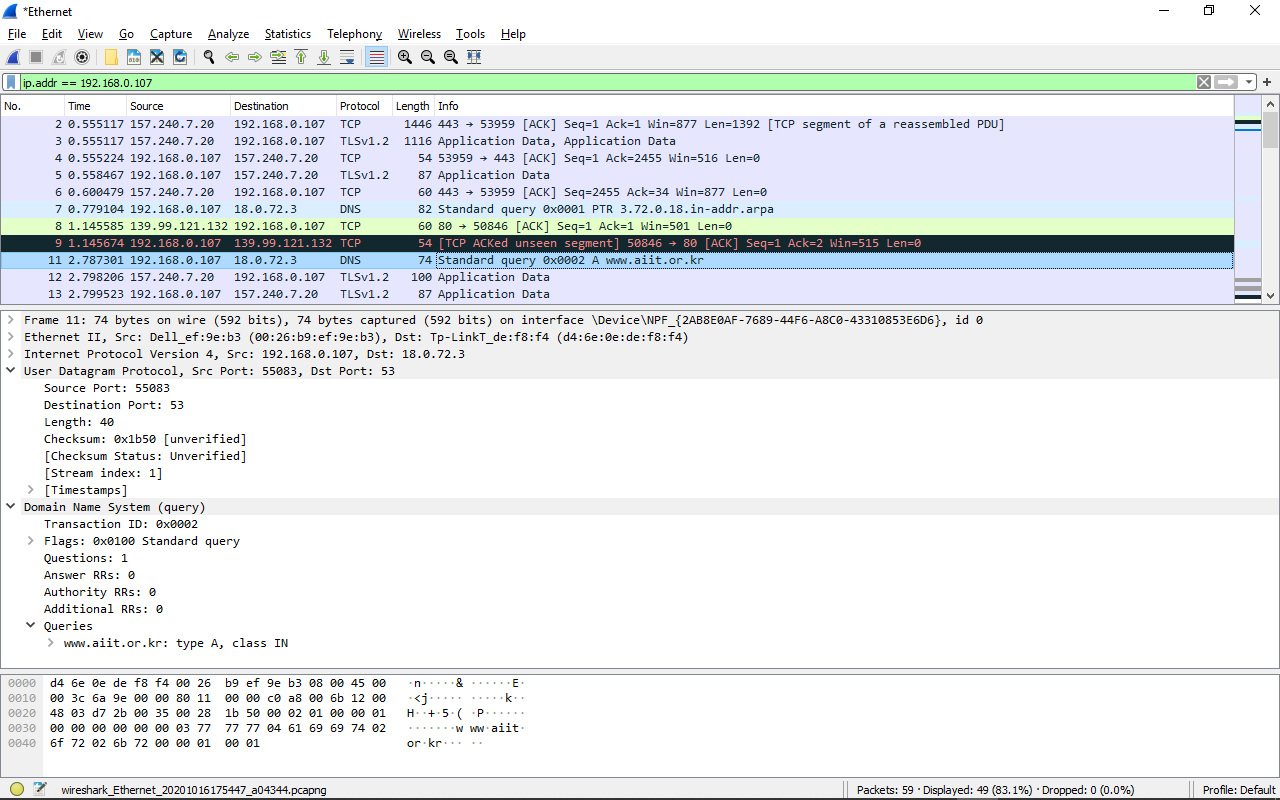
- Có 8 MIT nameservers là usw2.akam.net, ns1-173.akam.net, use2.akam.net, asia1.akam.net, use5.akam.net, asia2.akam.net, ns1-37.akam.net, eur5.akam.net không bao gồm địa chỉ IP

19. Provide a screenshot.

- Hình ở trên



20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

- IP mà DNS query message gửi tới là 18.0.72.3, đây không phải DNS server , mà nó là địa chỉ tương ứng của website bitsy.mit.edu 

21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

- Type của DNS query là A và nó không có answers

22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

- Không có DNS response message

23. Provide a screenshot.

- Hình ở trên