**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**CƠ SỞ TẠI THÀNH PHỐ HỒ CHÍ MINH**



**LAB 3:**

***Wireshark DNS***

**Môn :** KỸ THUẬT THEO DÕI, GIÁM SÁT AN TOÀN MẠNG

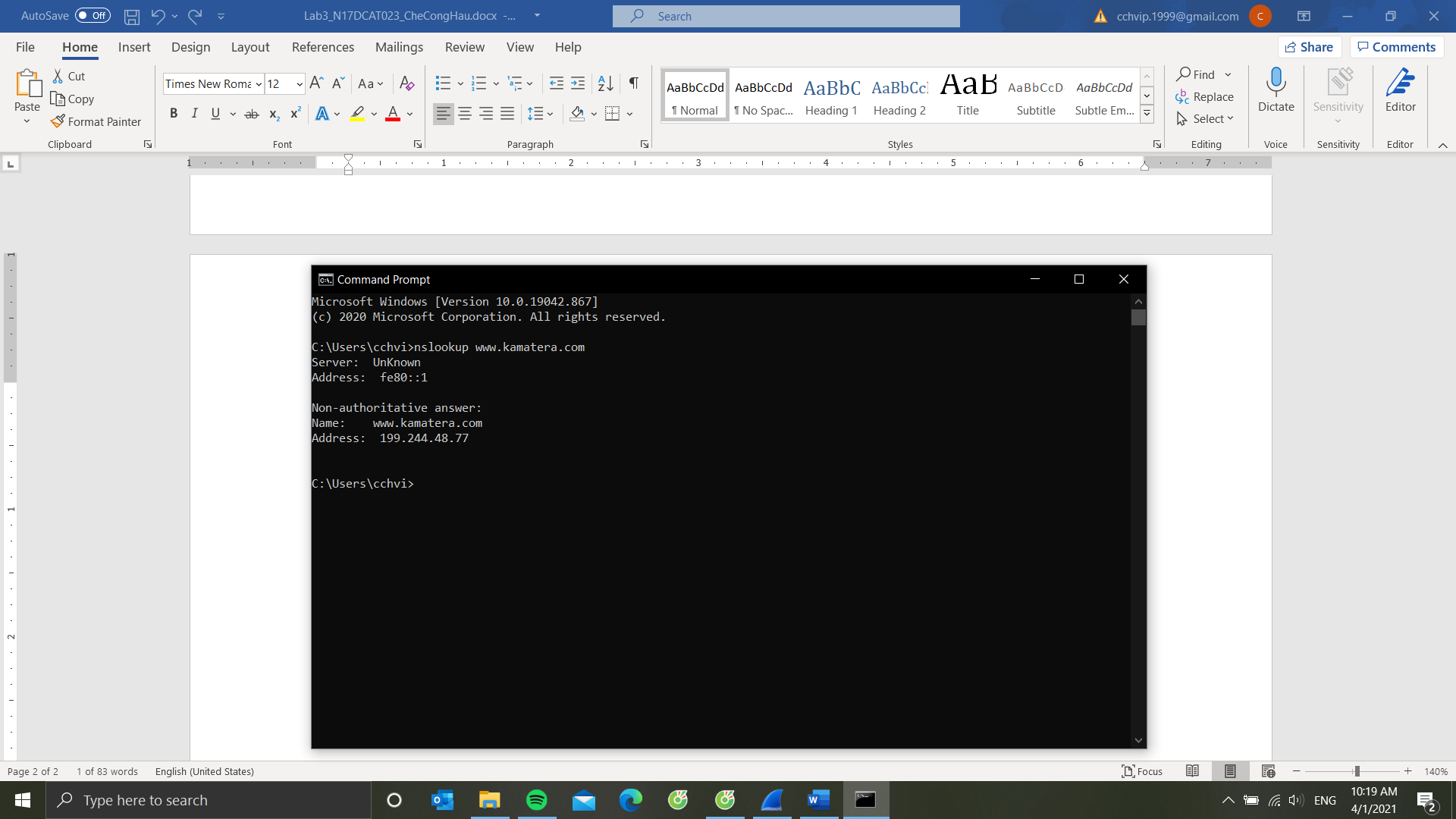
Giảng viên: Sam Nguyen Xuan

Họ tên: Chế Công Hậu – N17DCAT023

*Ngày 1 tháng 4 năm 2021*

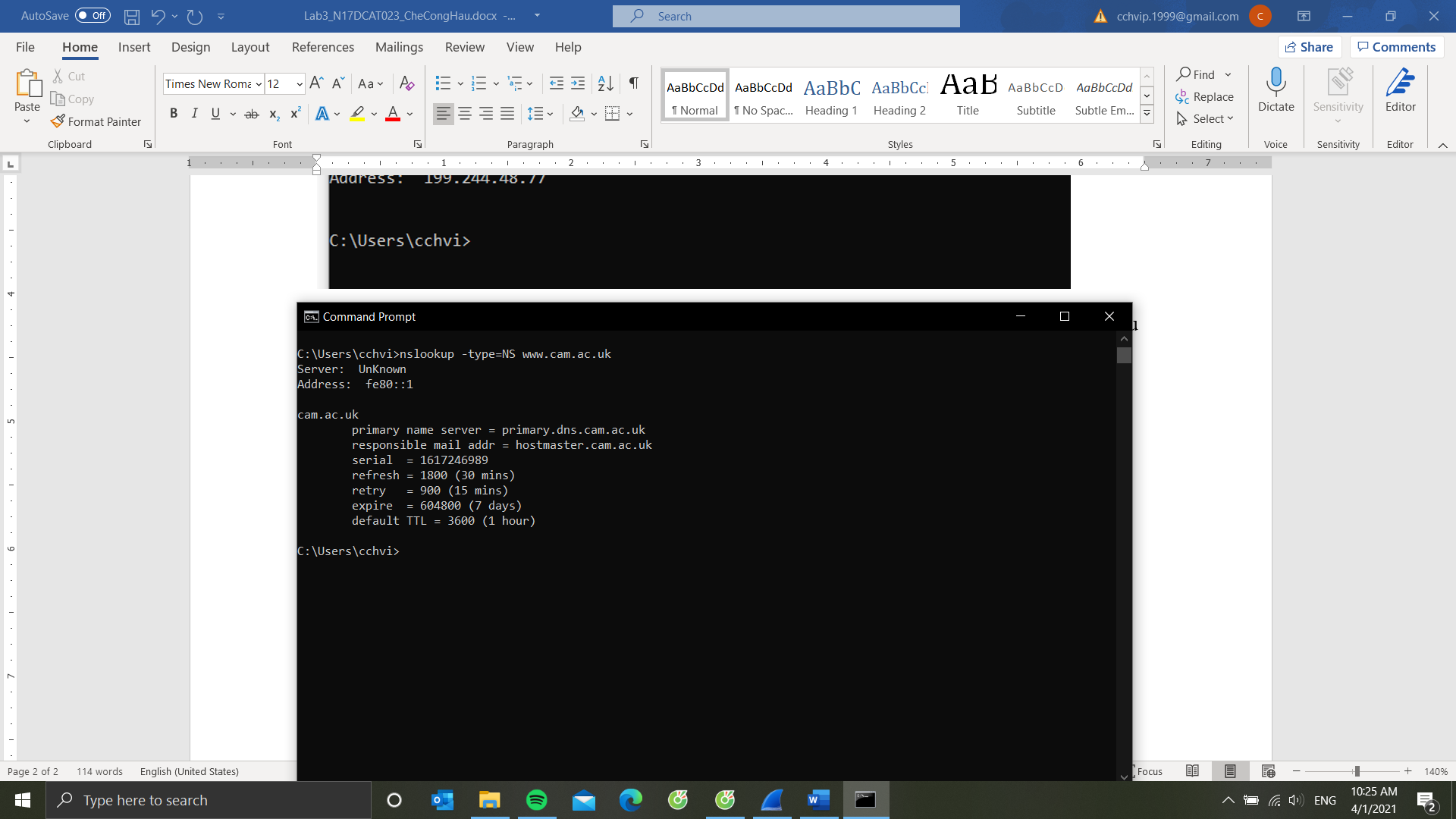
1. **nslookup**
2. Chạy nslookup để lấy địa chỉ IP của Web Server ở Châu Á. Địa chỉ IP của máy chủ đó là gì?

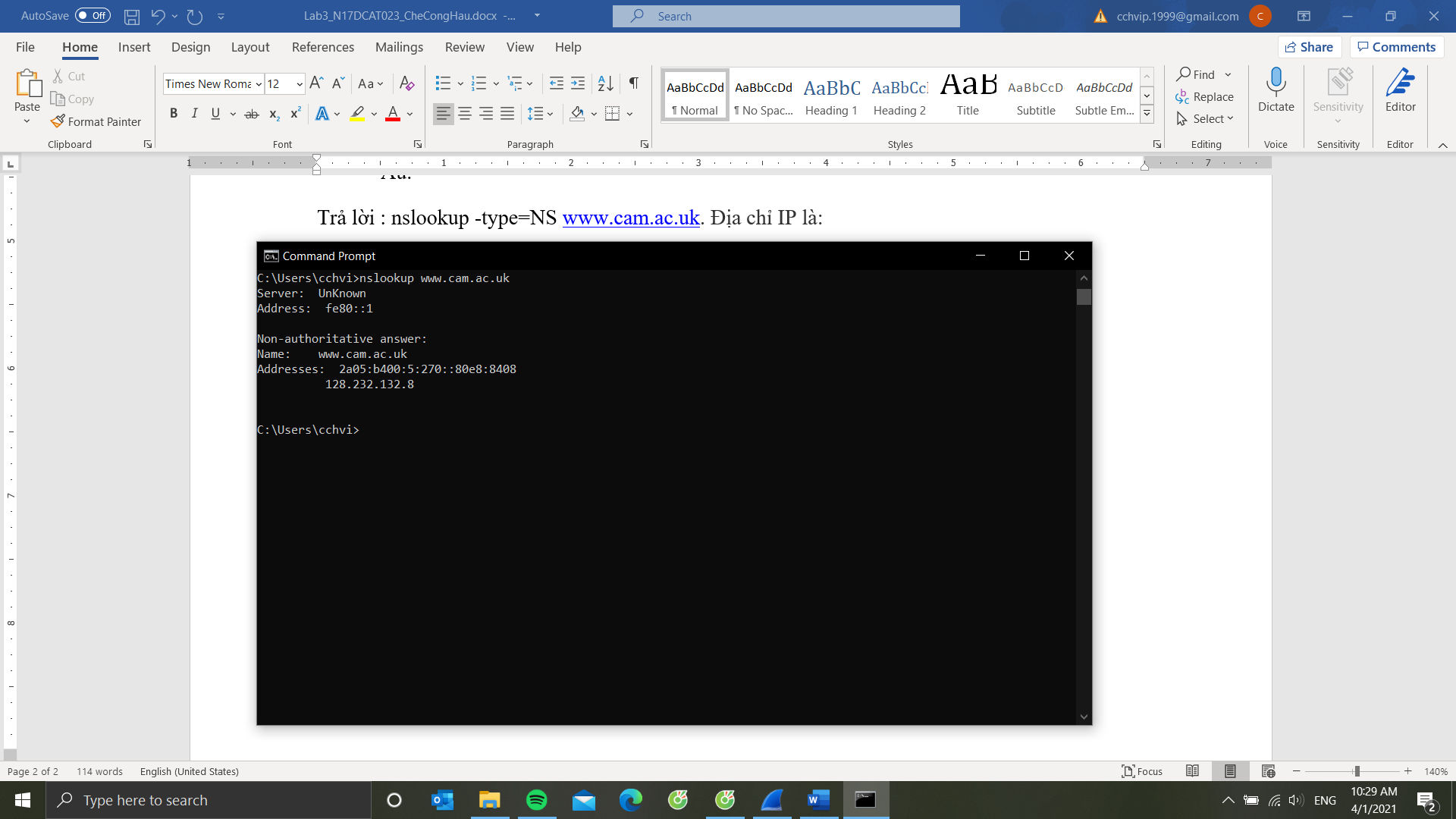
Trả lời : nslookup [www.kamatera.com/](http://www.kamatera.com/). Địa chỉ IP là : 199.244.48.77



1. Chạy nslookup để xác định máy chủ DNS có thẩm quyền cho một trường đại học ở Châu Âu.

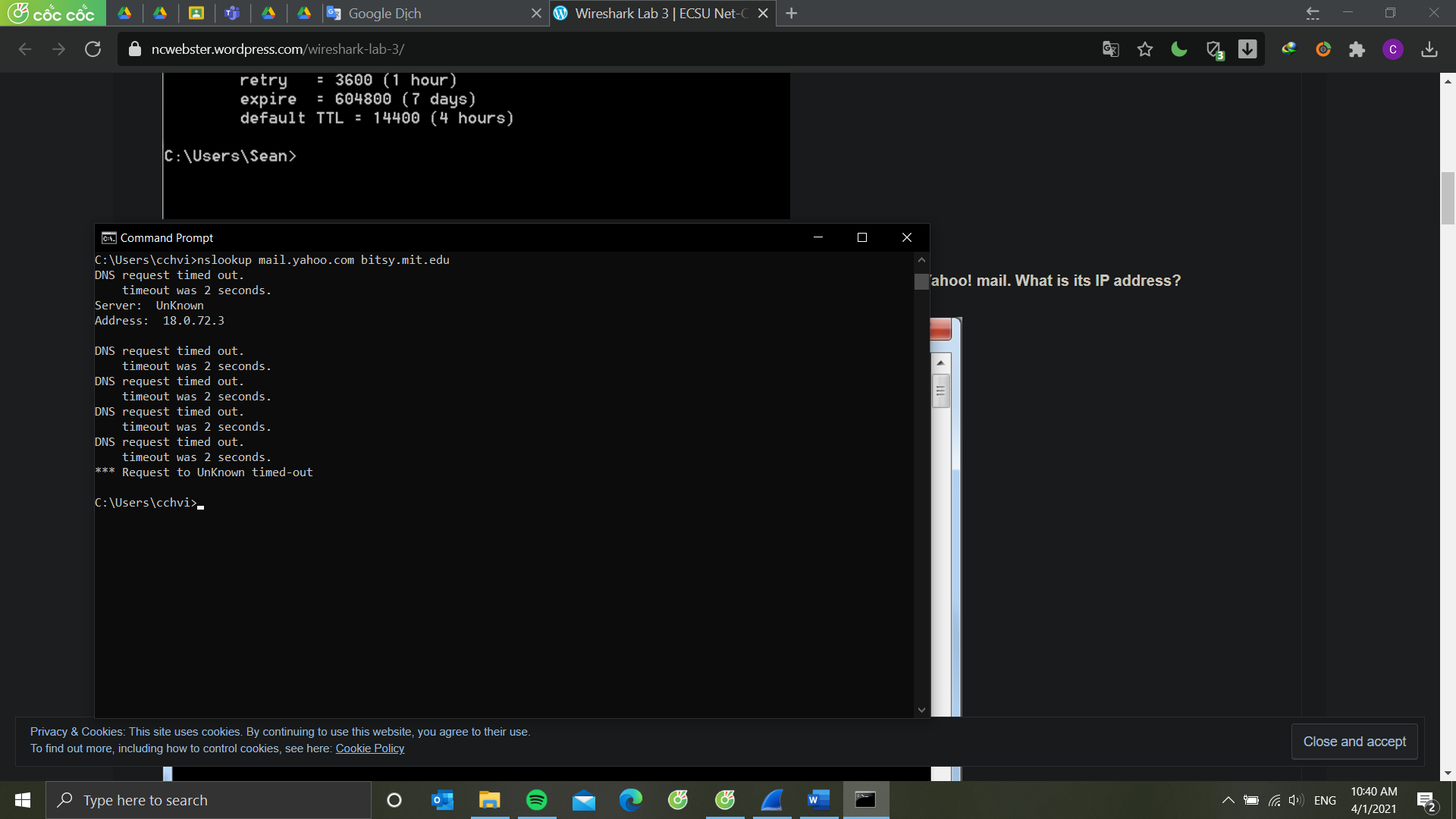
Trả lời : nslookup -type=NS [www.cam.ac.uk](http://www.cam.ac.uk). Địa chỉ IP là: 128.232.132.8





1. Chạy nslookup để một trong các máy chủ DNS được truy vấn cho các mail server như Yahoo. Địa chỉ IP của nó là gì?

Trả lời : nslookup mail.yahoo.com bitsy.mit.edu. Địa chỉ IP là : 18.0.72.3

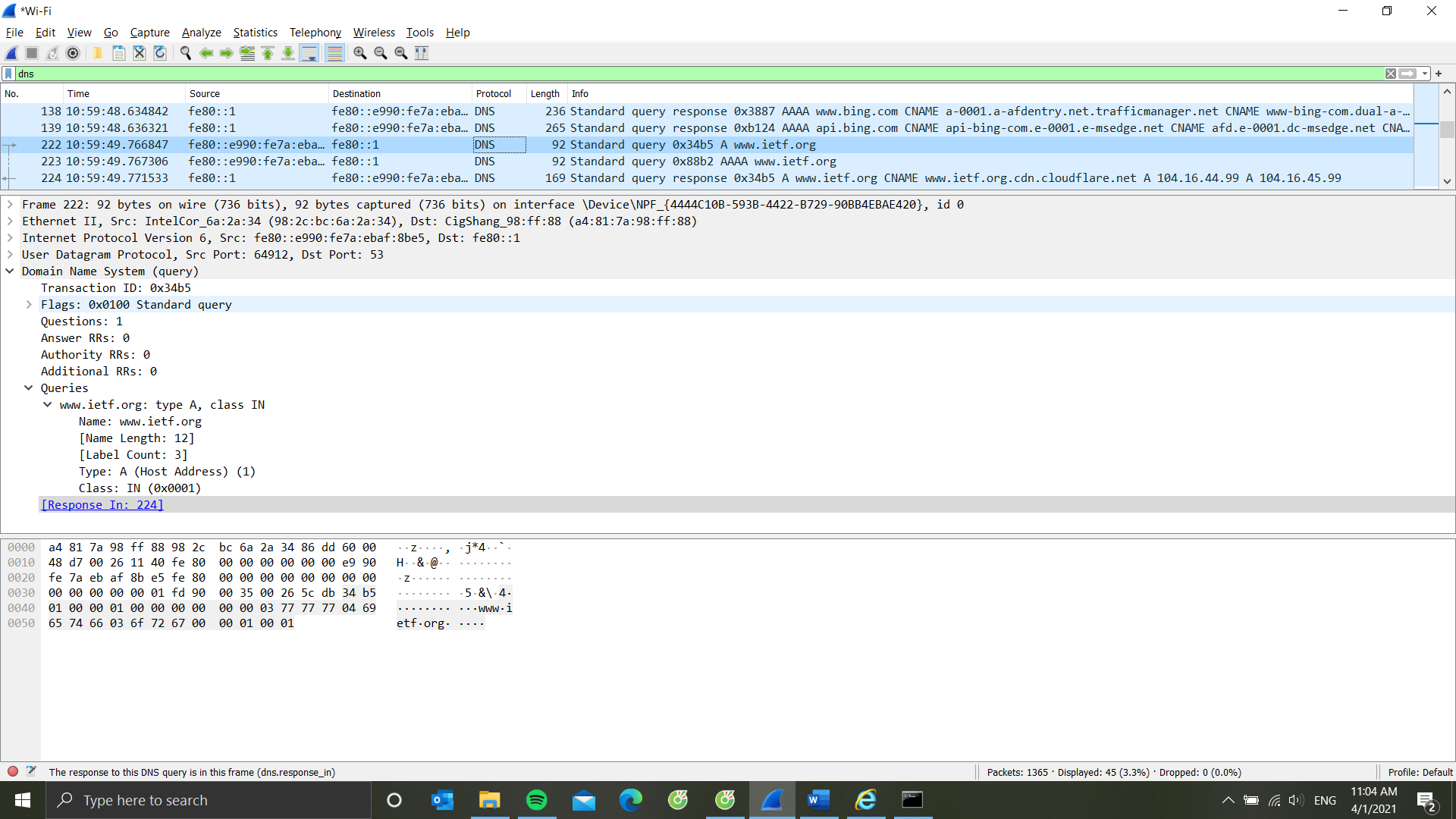


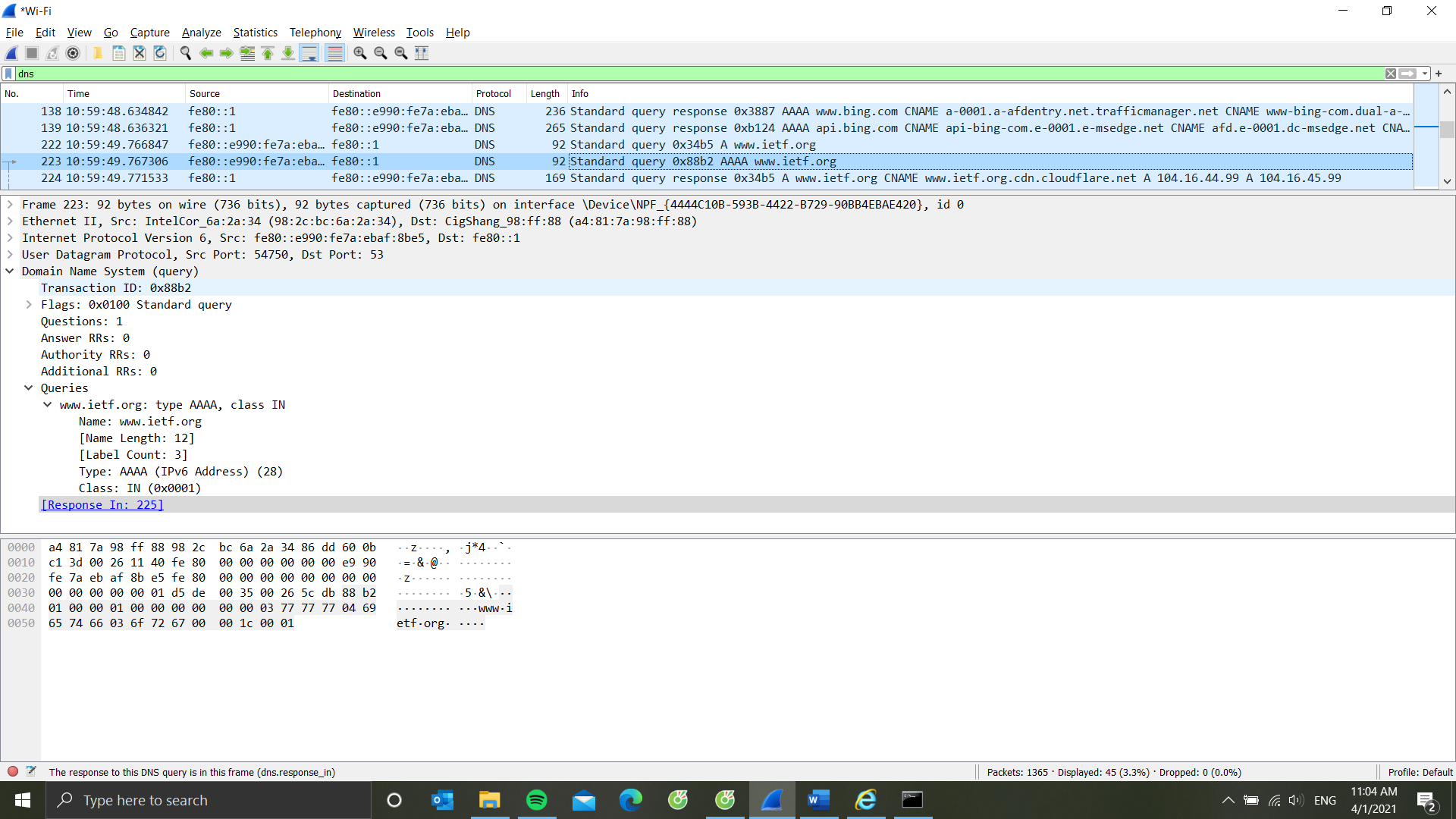
1. **Ipconfig**
2. **Tracing DNS with Wireshark**

* Nhập lệnh ipconfig /flushdns vào cmd để xóa bộ nhớ đệm của DNS.
* Xóa bộ nhớ đệm (cache) của trình duyệt sắp sử dụng.
* Mở Wireshark và nhập “ip.addr == your\_IP\_address”(192.168.1.44) vào phần filter và bắt đầu bắt gói
* Truy cập <http://www.ietf.org>.

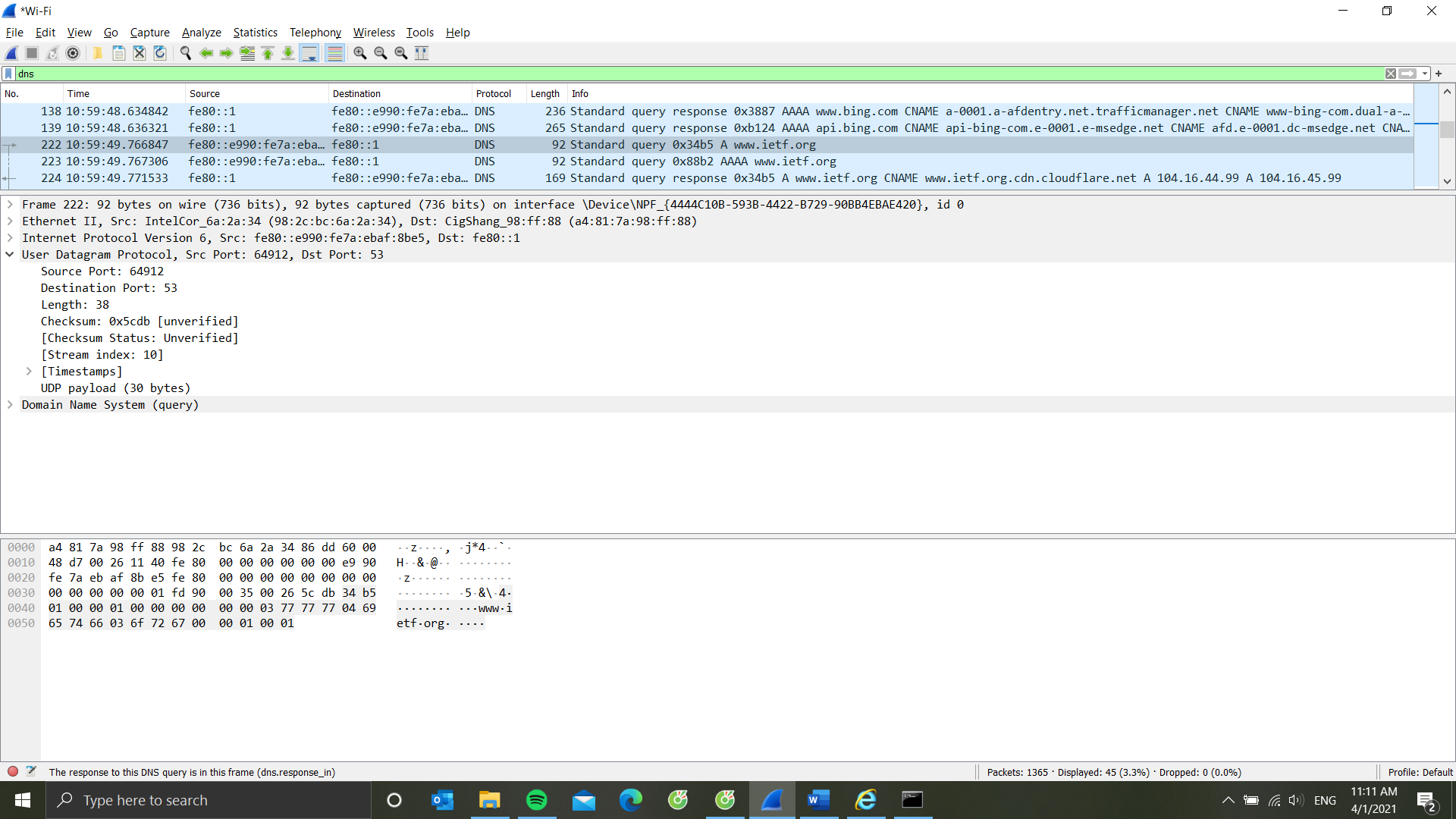
1. Xác định vị trí DNS query và thông báo phản hồi. Sau đó có được gửi qua UDP hoặc TCP không?

Trả lời : hai hình dưới. Được gửi qua UDP.

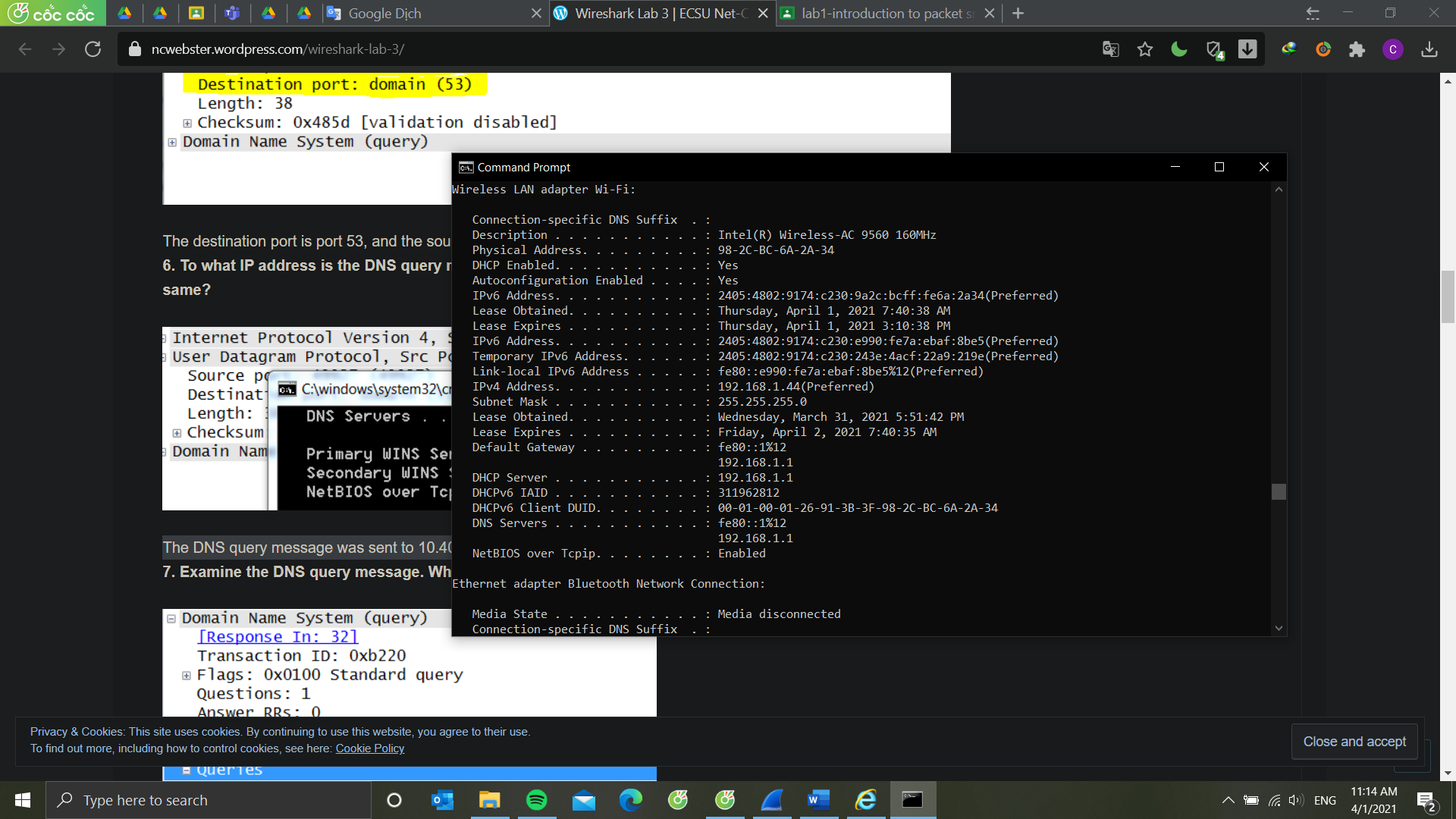




1. Destination port cho thông báo DNS query là 53 và source port của thông báo phản hồi DNS là 64912.

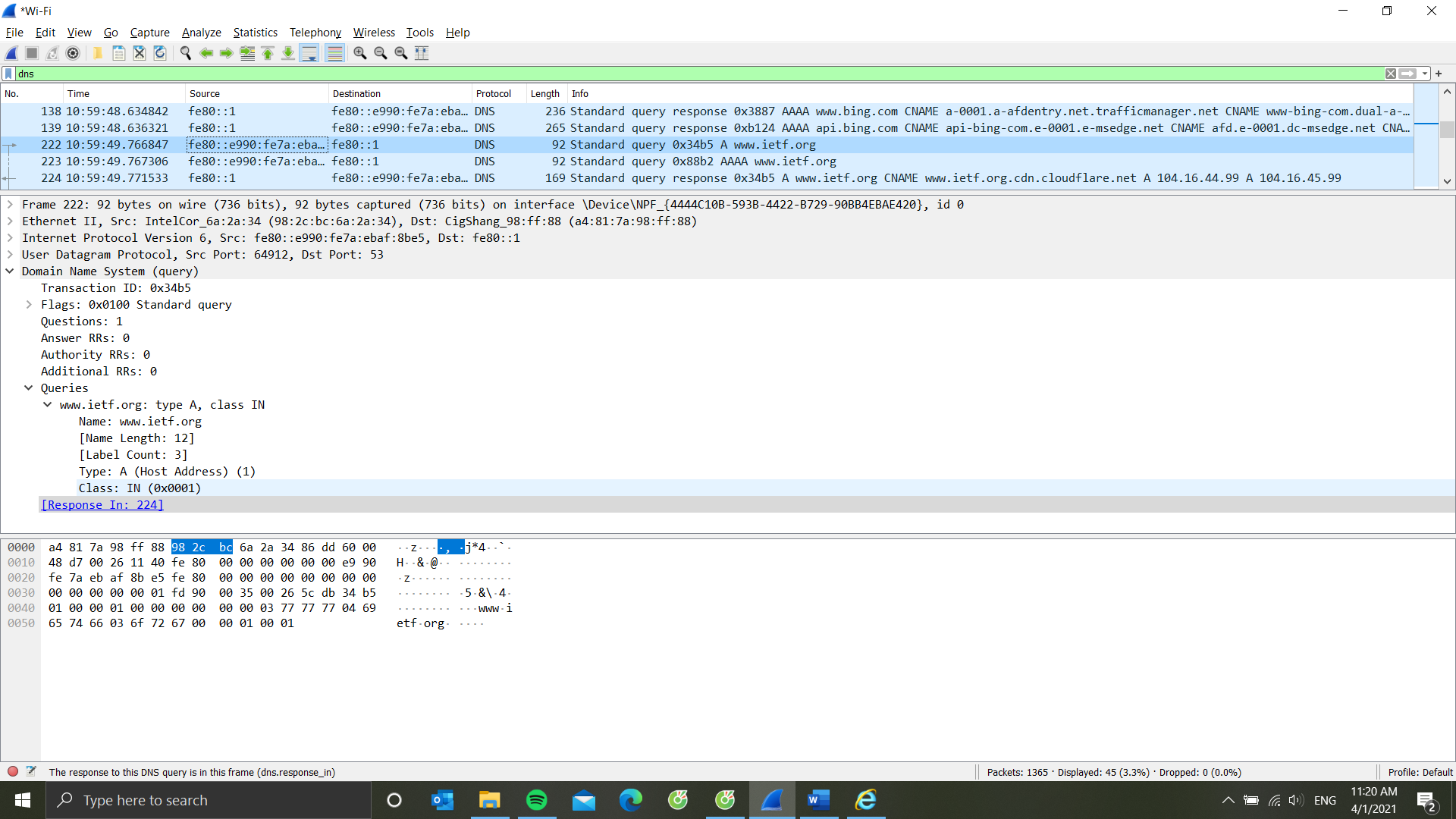


1. Thông báo truy vấn DNS được gửi đến địa chỉ IP nào? Sử dụng ipconfig để xác định địa chỉ IP của máy chủ DNS cục bộ của bạn. Hai địa chỉ IP này có giống nhau không?

Trả lời : Thông báo DNS query được gửi đến 192.168.1.1 hoặc là fe80::1%12. Đây là địa chỉ IP giống như địa chỉ máy chủ DNS cục bộ.

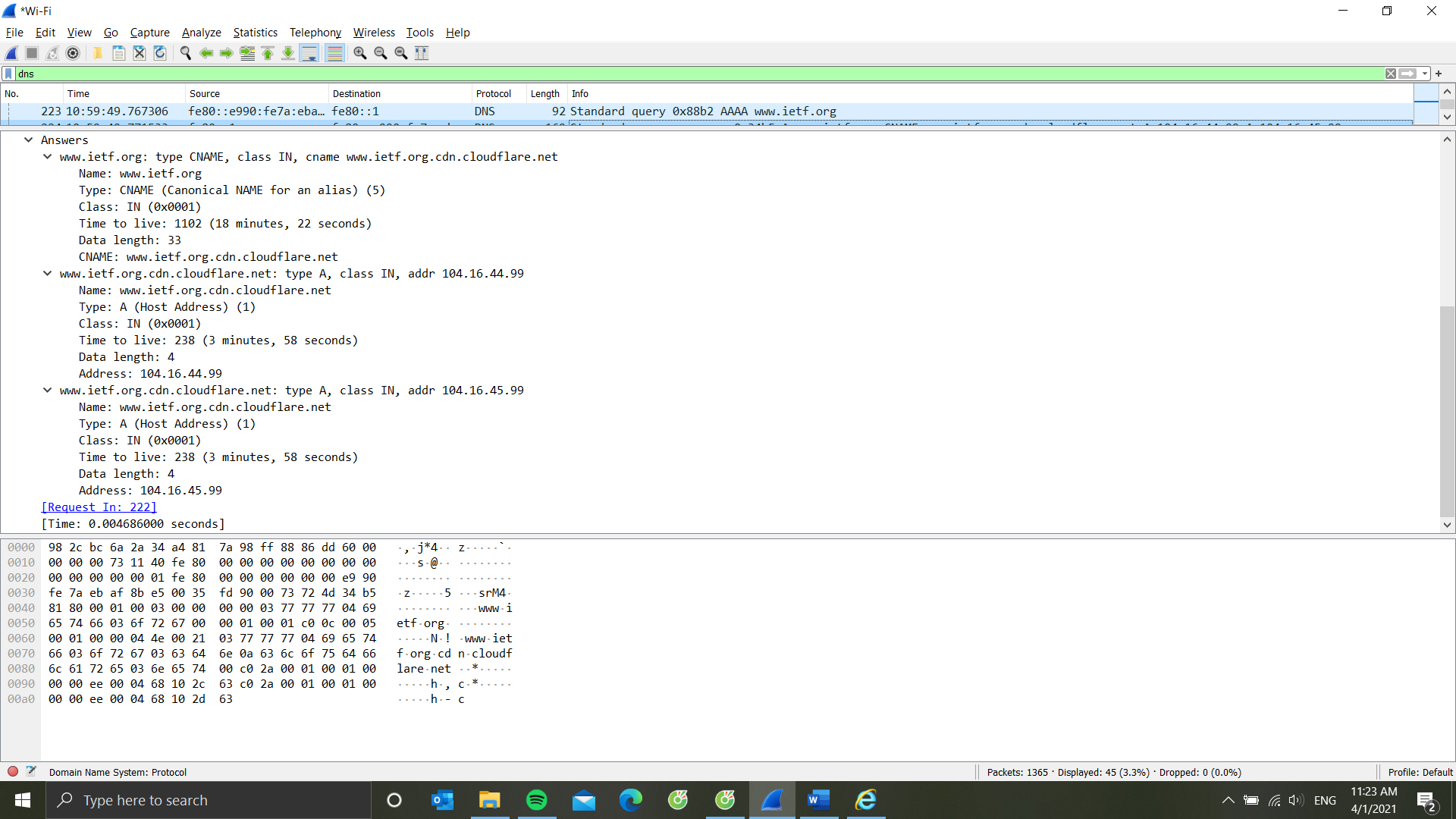
1. Kiểm tra thông báo truy vấn DNS. “Type” truy vấn DNS là gì? Thông báo truy vấn có chứa bất kỳ “answers” nào không?

Trả lời : Type A và không có chứa “answers”.

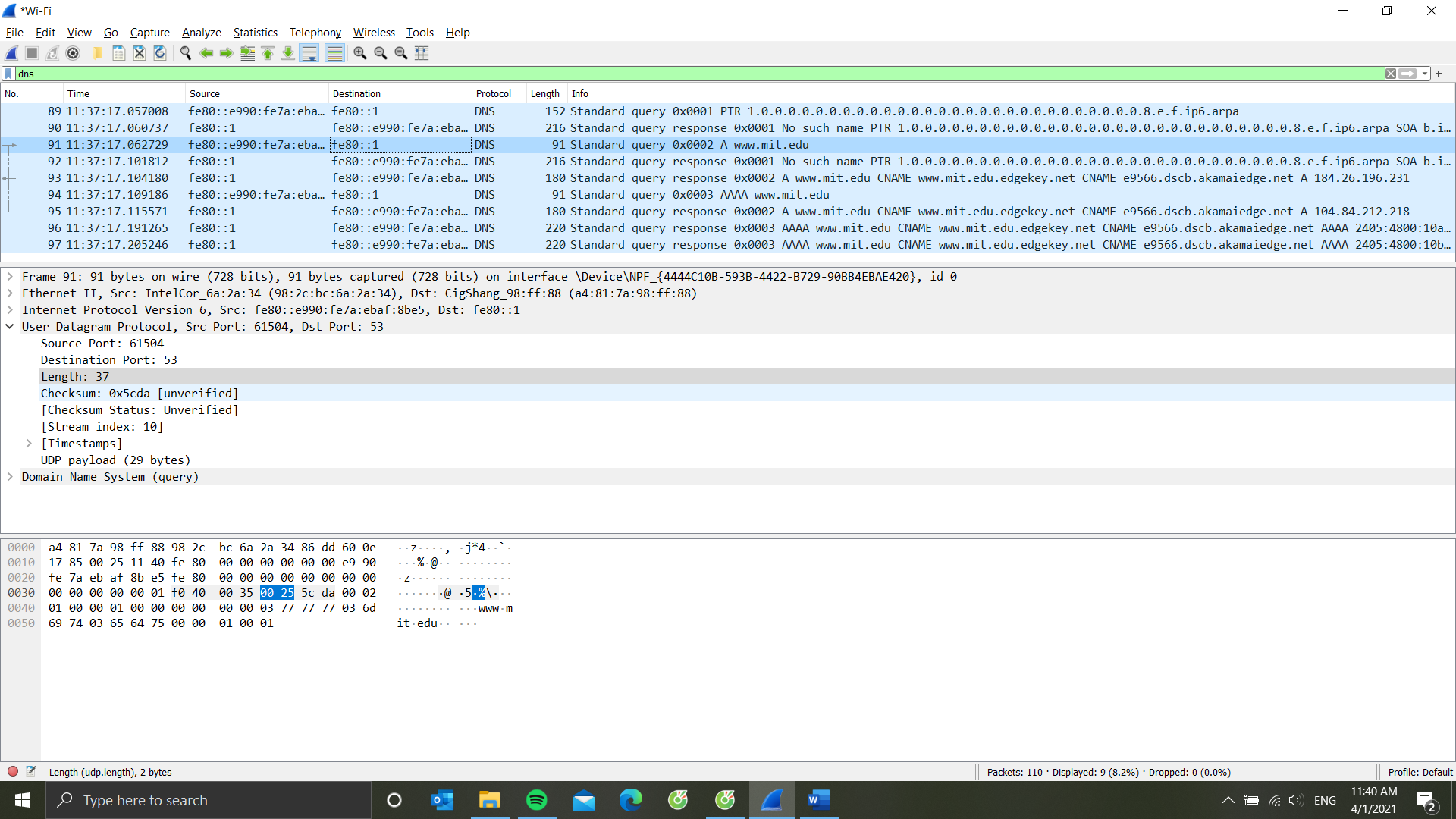


1. Kiểm tra thông báo phản hồi DNS. Có bao nhiêu "answers" được cung cấp? Mỗi câu trả lời này chứa những gì?

Trả lời : Có ba “answers” và chứa thông tin về tên của host, loại địa chỉ, class, TTL, độ dài dữ liệu và địa chỉ IP.



1. Địa chỉ IP đích đầu tiên của gói SYN tương ứng với địa chỉ được cung cấp bởi DNS response 104.16.44.99.
2. Trang web này chứa hình ảnh. Trước khi truy xuất từng hình ảnh, máy chủ không có đưa ra các truy vấn DNS mới.
3. Destination port cho thông báo truy vấn DNS là cổng 53. Source port của thông báo phản hồi DNS cũng là cổng 53.



1. Thông báo DNS query được gửi đến 192.168.1.1 hoặc là fe80::1%12. Đây là cùng một địa chỉ IP của máy chủ DNS cục bộ.
2. Type : PTR, không chứa answers.

