|  |
| --- |
| BAN CƠ YẾU CHÍNH PHỦ  **HỌC VIỆN KỸ THUẬT MẬT MÃ**  ¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯ |
| HỌC PHẦN  **ĐÁNH GIÁ VÀ KIỂM ĐỊNH**  **AN TOÀN HỆ THỐNG THÔNG TIN** |
| BÀI THỰC HÀNH  **KHÁM PHÁ MẠNG** |
| **Sinh viên thực hiện: HOÀNG NGUYÊN THÁI - AT14C** |
| **Hà Nội, 2021** |

MỤC LỤC

[*Phần 1. Sử dụng các câu lệnh kiểm tra và khám phá mạng* 3](#_Toc75791040)

[Giới thiệu 3](#_Toc75791041)

[Chuẩn bị 3](#_Toc75791042)

[Các bước thực hiện 3](#_Toc75791043)

[*Phần 2. Sử dụng Advanced IP Scanner để khám phá mạng chủ động* 18](#_Toc75791051)

[*Phần 3. Sử dụng Wireshark để khám phá mạng tự động* 19](#_Toc75791052)

# *Sử dụng các câu lệnh kiểm tra và khám phá mạng*

## Giới thiệu

Có rất nhiều các lệnh trong Command Line của Windows hoặc Terminal của Linux hỗ trợ cho việc kiểm tra và khám phá mạng. Các lệnh thường sử dụng như: ping, telnet, tracert, nslookup, ipconfig, arp, netstat cho phép người kiểm thử khám phá mạng thu thập các thông tin liên quan. Bài thực hành này với mục đích giúp sinh viên hiểu và có thể sử dụng các câu lệnh này để kiểm tra khám phá mạng.

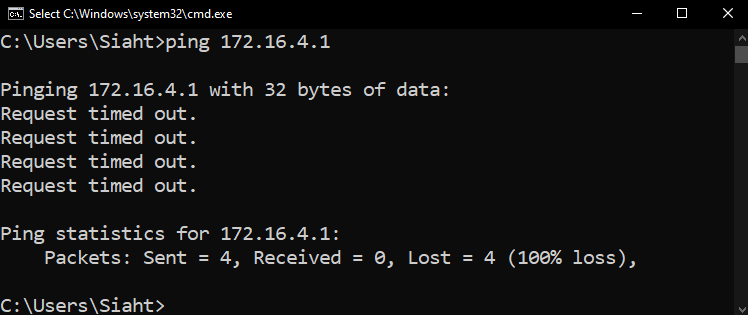
## Chuẩn bị

* Máy tính chạy hệ điều hành Windows với công cụ Command Line
* Máy tính có kết nối mạng

## Các bước thực hiện

### Ping

* **Request timed out** là dòng lệnh thông báo khi không kết nối được đến máy đích và không có phản hồi trả về. Nguyên nhân của lỗi này là do các thiết bị định tuyến router bị tắt hoặc địa chỉ máy đích không có thật, bị tắt hay cấm ping (chặn giao thức ICMP).



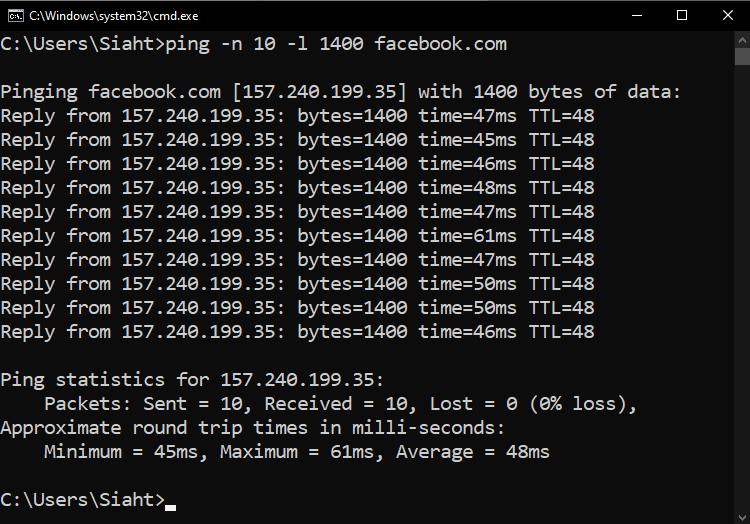
* Ping facebook.com



* Ping –n 10 –l 1400 facebook.com

Kiểm tra các tham số

* ping /?
* -n count: Number of echo requests to send.(Số request gửi là 10)
* -l size: Send buffer size. (Kích thước bộ đệm gửi bytes = 1400)

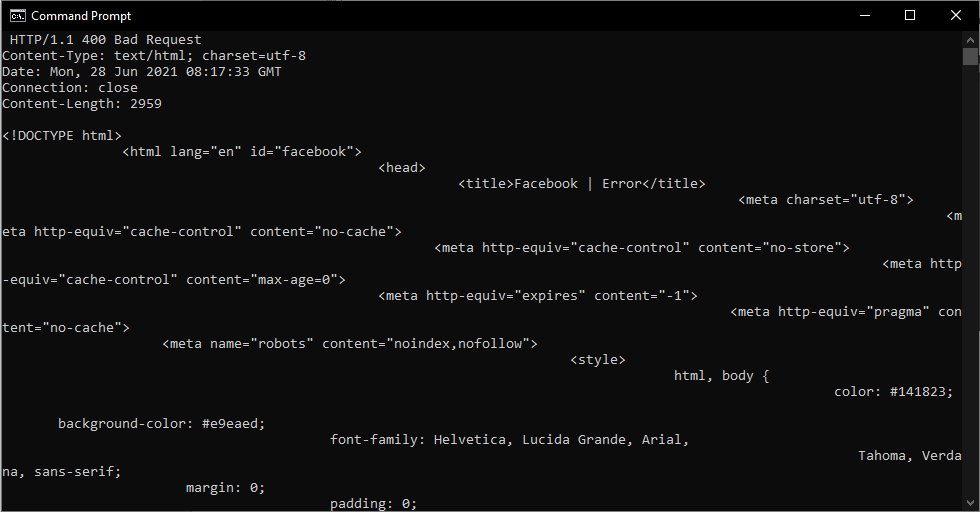


* Ping –n 100 –l 1500 facebook.com

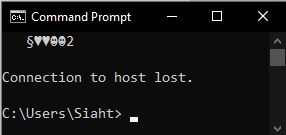


### Telnet

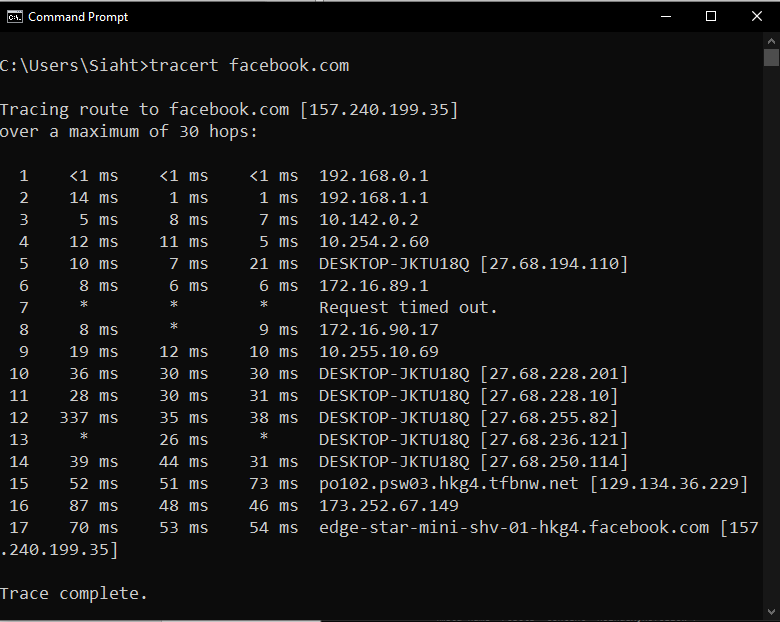
* telnet facebook.com 80

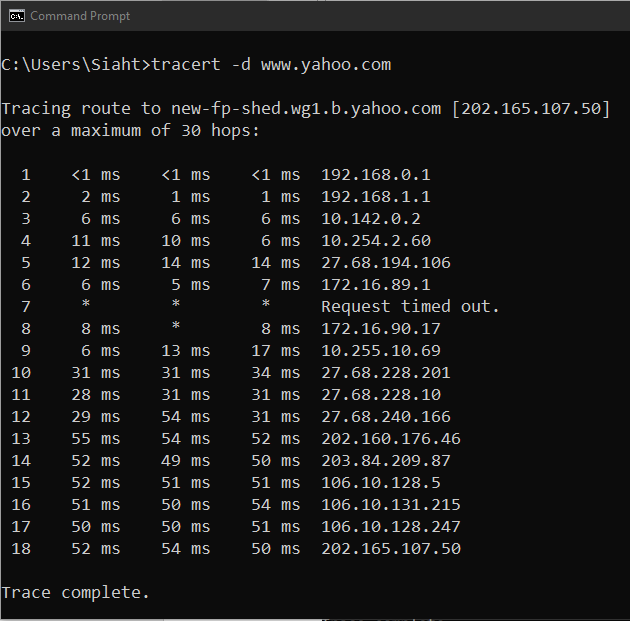


* telnet facebook.com 443

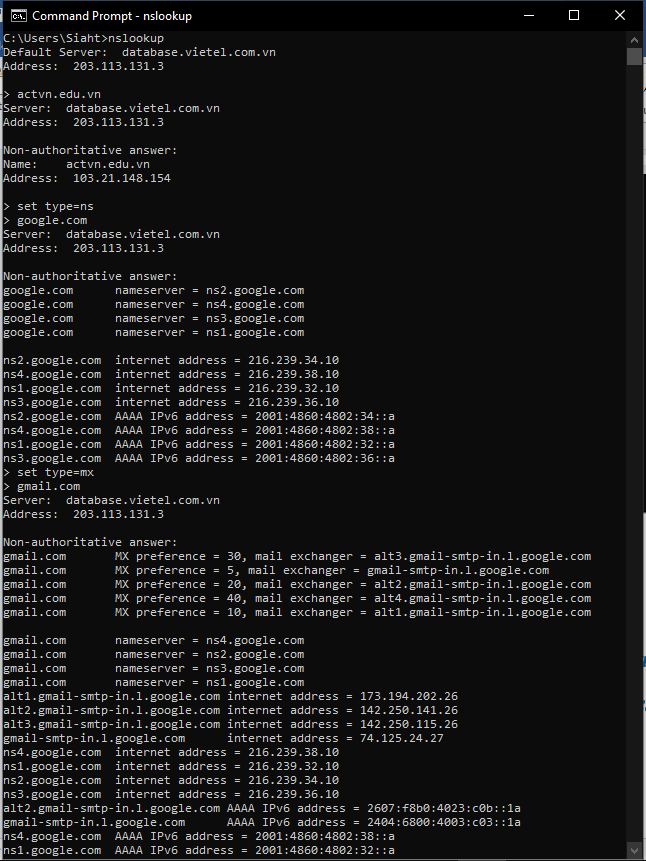


* Tracert: Mỗi khi đi qua 1 router sẽ bị trừ đi 1 hops cho tới khi đến đích với tối đa 30 hops



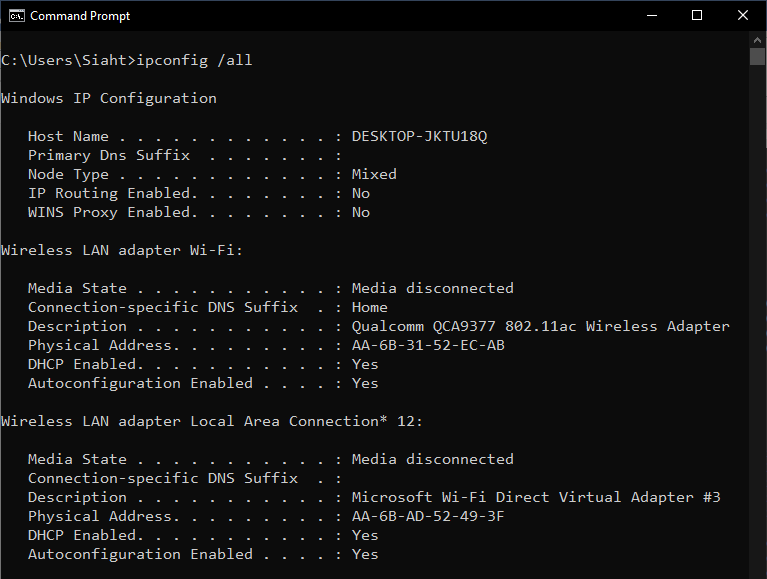


* Nslookup: Ở đây ta có kết quả nslookup với ns là bản ghi name server và mx là mail



### Ipconfig

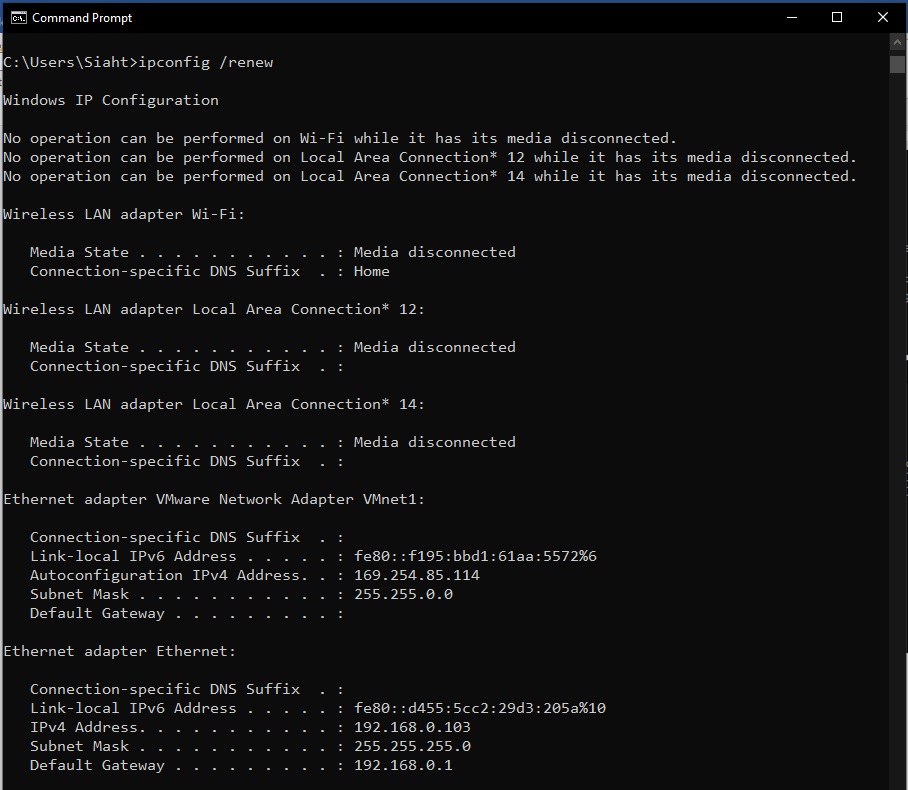
* ipconfig /all: Hiển thị tất cả thông tin cấu hình.



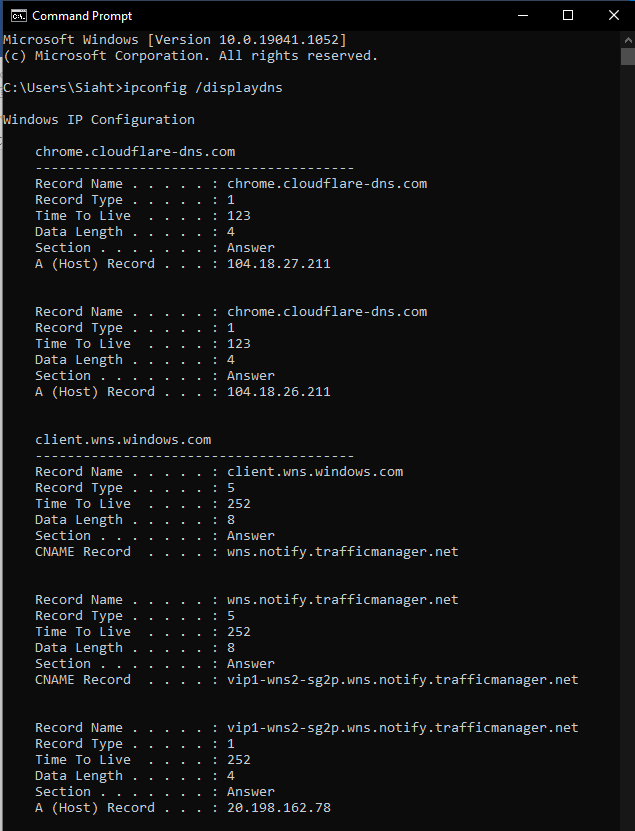
* ipconfig /release: Giải phóng địa chỉ IPv4 cho adapter cụ thể.



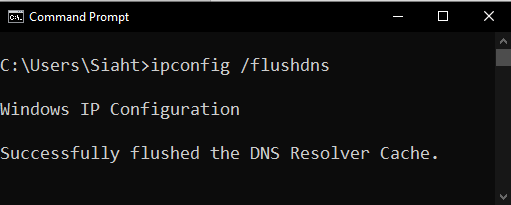
* ipconfig /renew: Cấp mới địa chỉ IPv4 cho adapter cụ thể



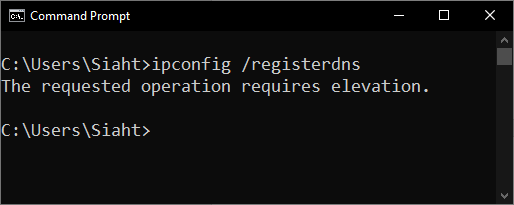
* ipconfig /displaydns: Hiển thị nội dung của bộ nhớ cache DNS (Lưu trữ các trang web công khai đã truy cập)



* ipconfig /flushdns: Xóa bộ nhớ đệm DNS Resolver và tạo mới

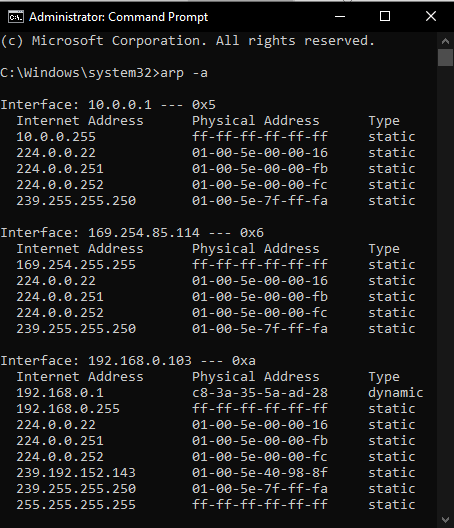


* ipconfig /registerdns: Tùy chọn này cho phép bạn cập nhật các thiết lập DNS. Nếu DNS không thể đăng ký một tên miền hoặc không thể kết nối với máy chủ DHCP, câu lệnh này có thể giúp xử lý vấn đề bằng cách đăng ký lại DNS

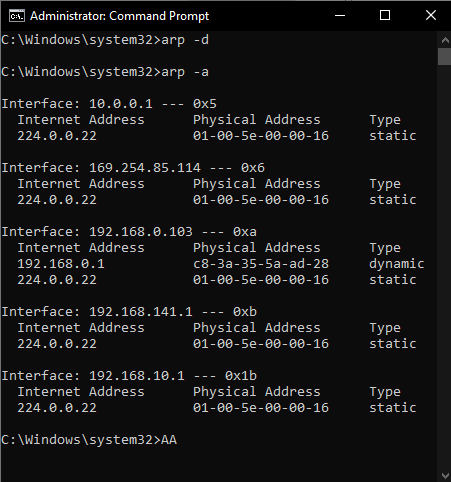


### Arp

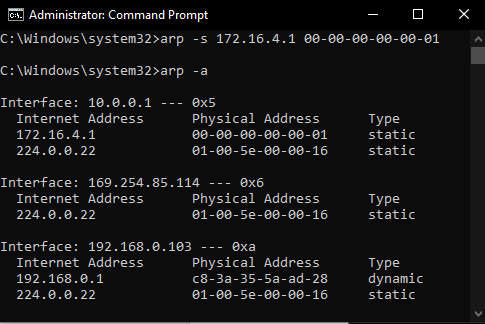
* arp –a: Ta sẽ xem được các entry có trong ARP Cache bao gồm địa chỉ IP, MAC và loại (dynamic/static)



* arp –d > arp –a: Xóa cache ARP (Run cmd as administrator)

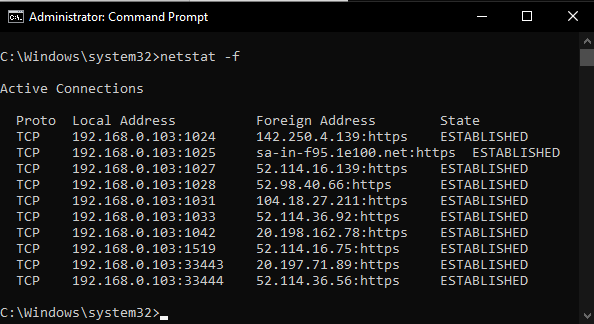


* arp -s 172.16.4.1 00-00-00-00-00-01 (Add một entry ARP static vào ARP cache)

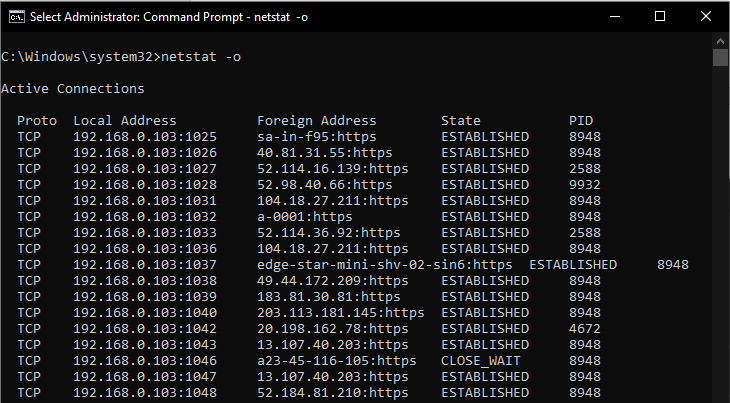


### Netstat

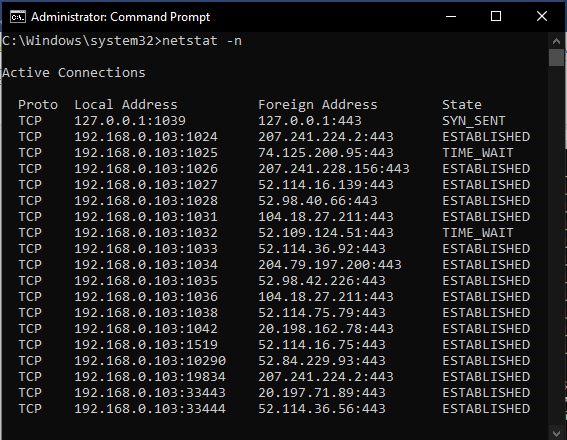
* netstat –f



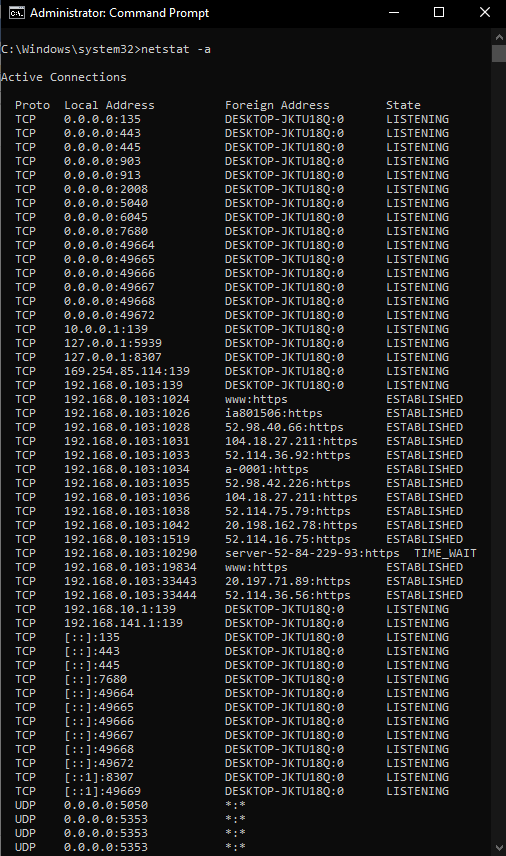
* netstat –o: Hiển thị những kết nối TCP đang hoạt động và bao gồm cả ID tiến trình cho mỗi kết nối. Người dùng có thể tìm kiếm ứng dụng bằng cách tra cứu PID trên tab Processes trong Windows Task Manager. Tham số -o có thể được kết hợp với -a, -p và -n.



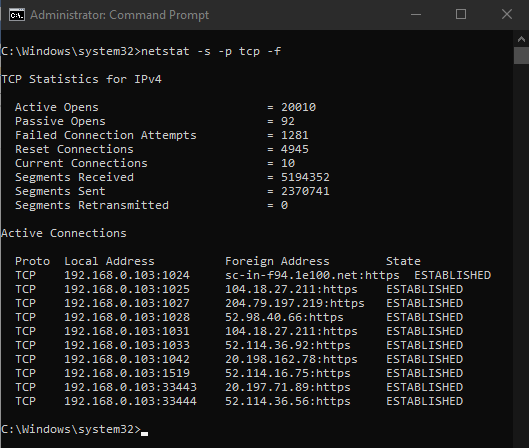
* netstat –n: Hiển thị những kết nối TCP đang hoạt động, tuy nhiên các địa chỉ và số cổng được biểu diễn dưới dạng số chứ không thể xác định một cái tên cụ thể.



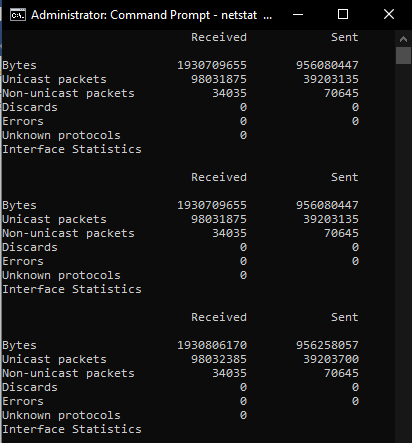
* netstat –a: Hiển thị toàn bộ các kết nối TCP đang hoạt động và các cổng TCP cũng như UDP mà trên đó máy tính đang nghe.



* netstat –s –p tcp –f

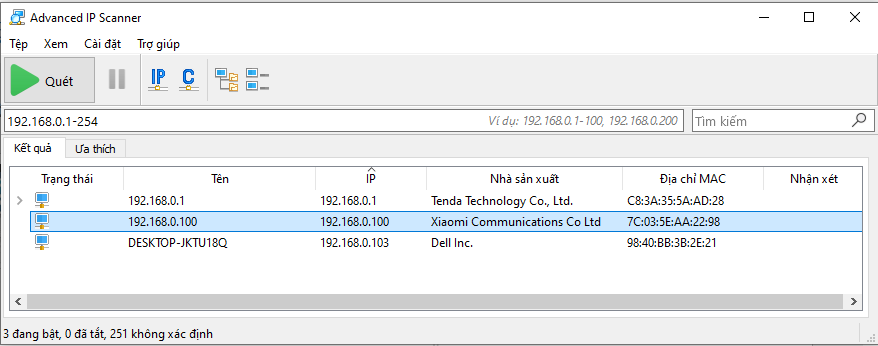


* netstat –e –t 5

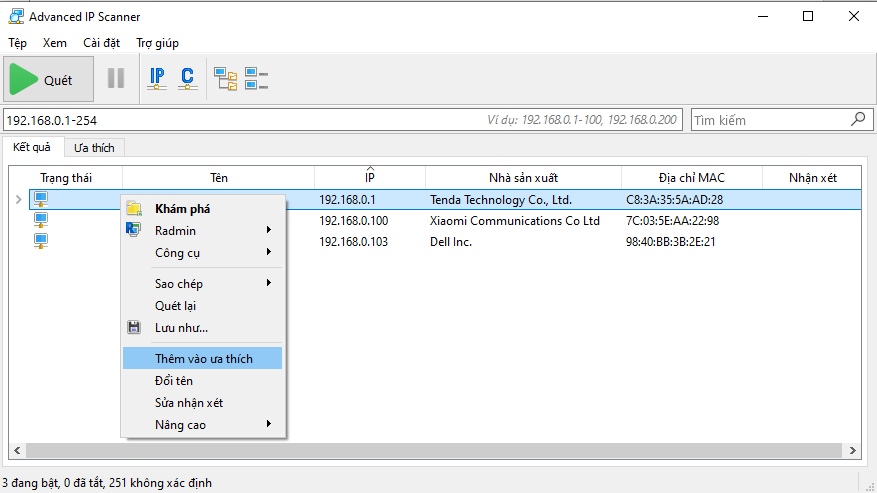


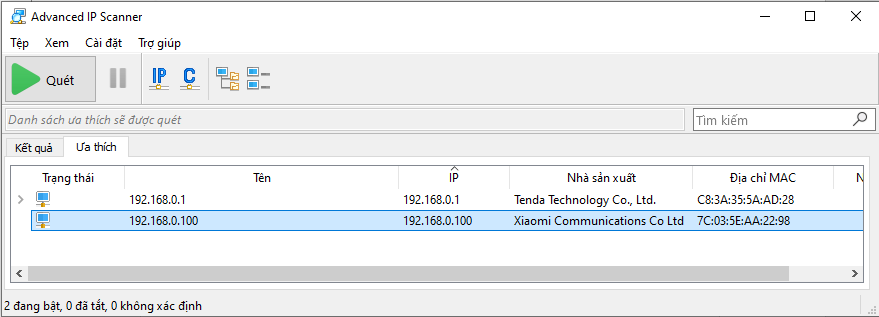
# *Sử dụng Advanced IP Scanner để khám phá mạng chủ động*

* Tiến hành quét mạng



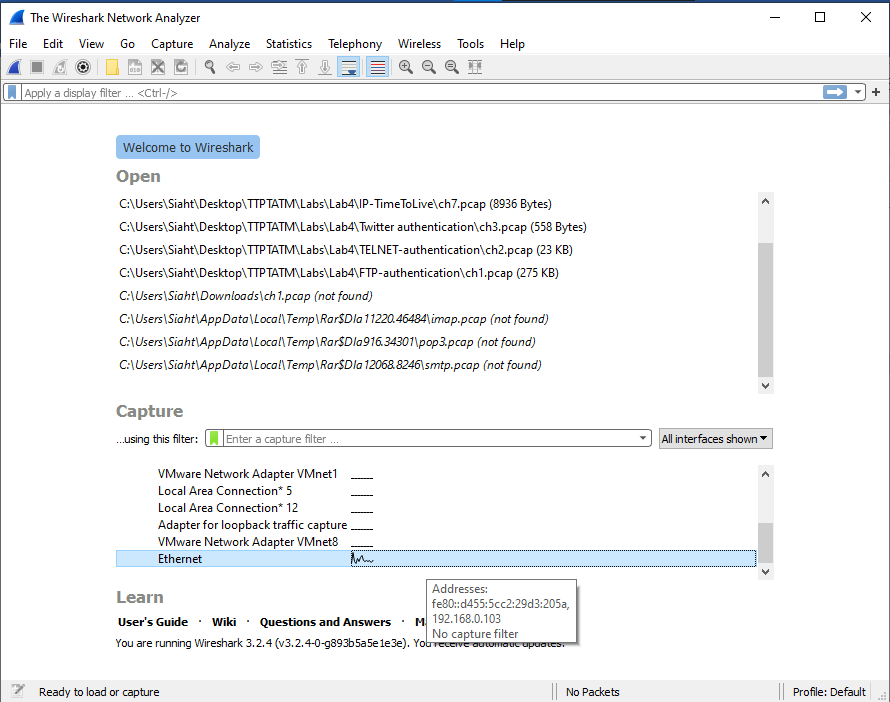
* Thêm các máy cần lưu ý vào mục ưa thích



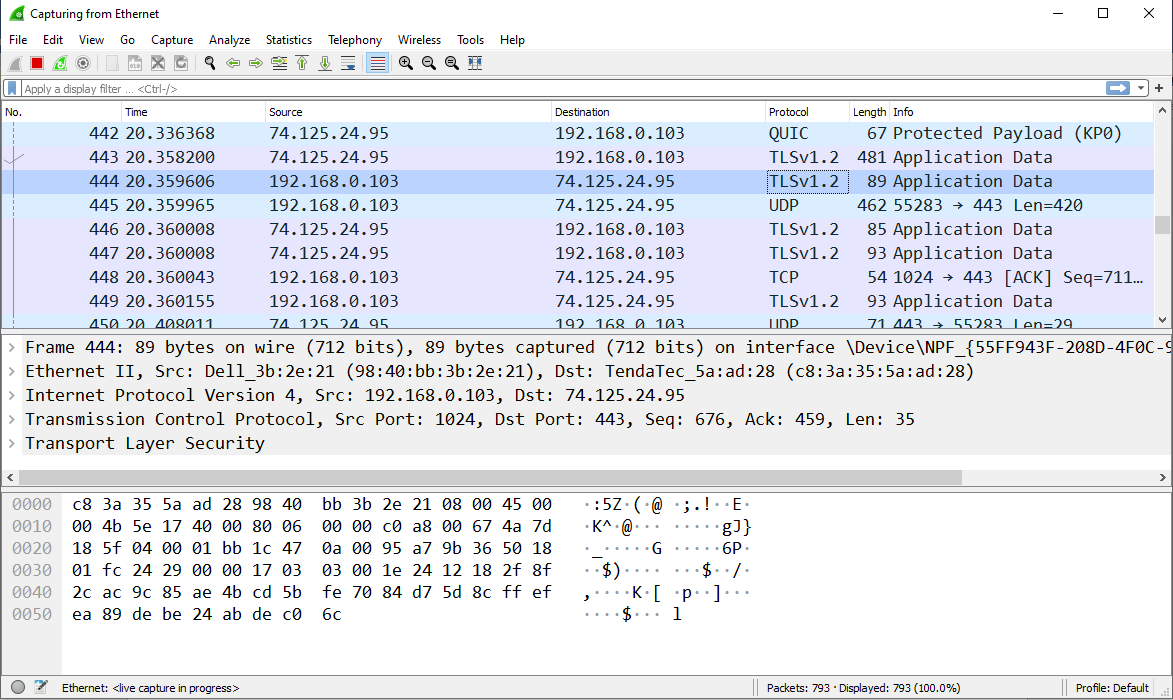


# *Sử dụng Wireshark để khám phá mạng tự động*

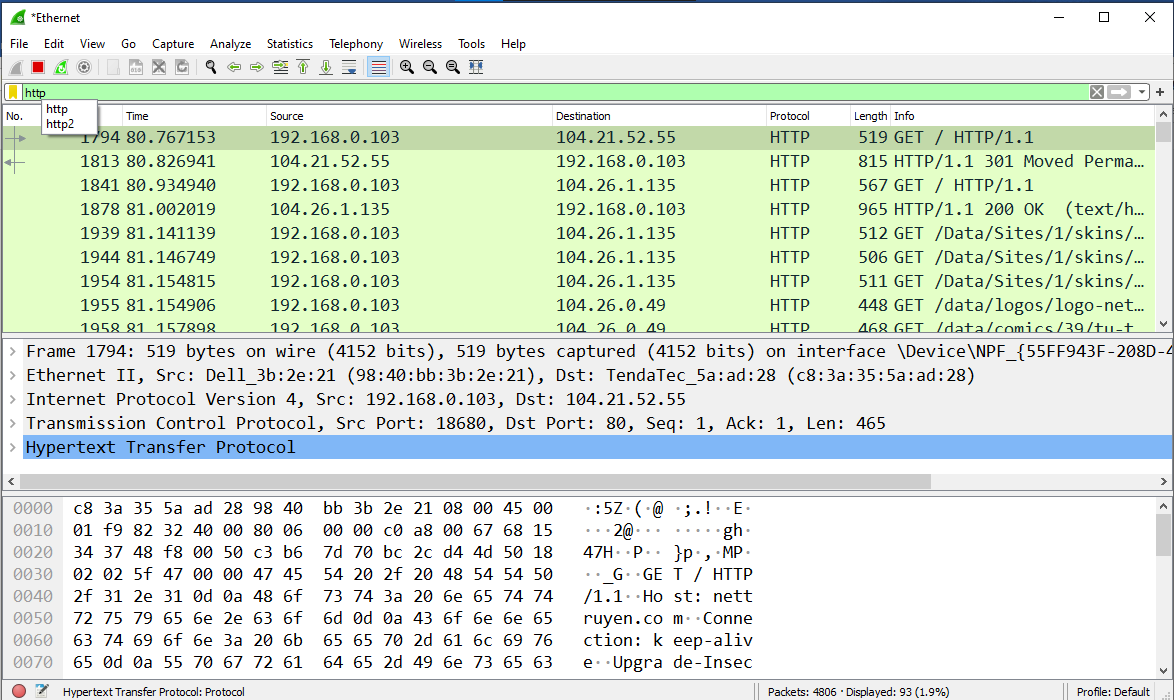
* Chọn giao diện card mạng để lắng nghe



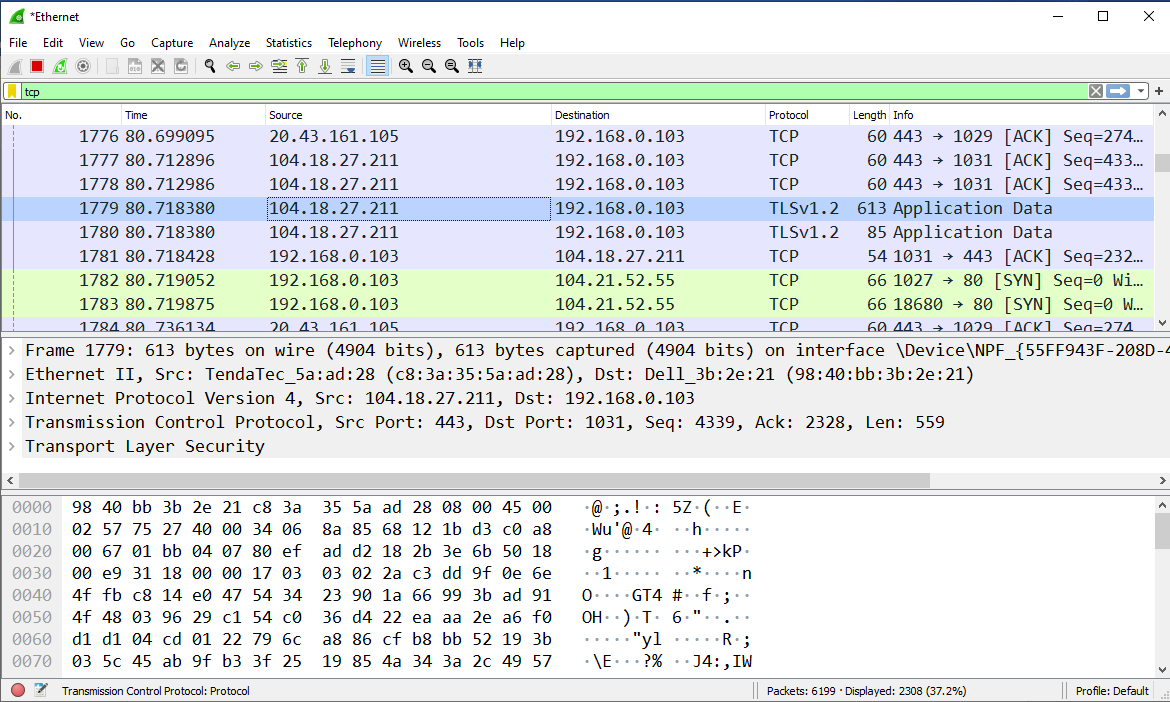
* Sử dụng Wireshark để lắng nghe mạng



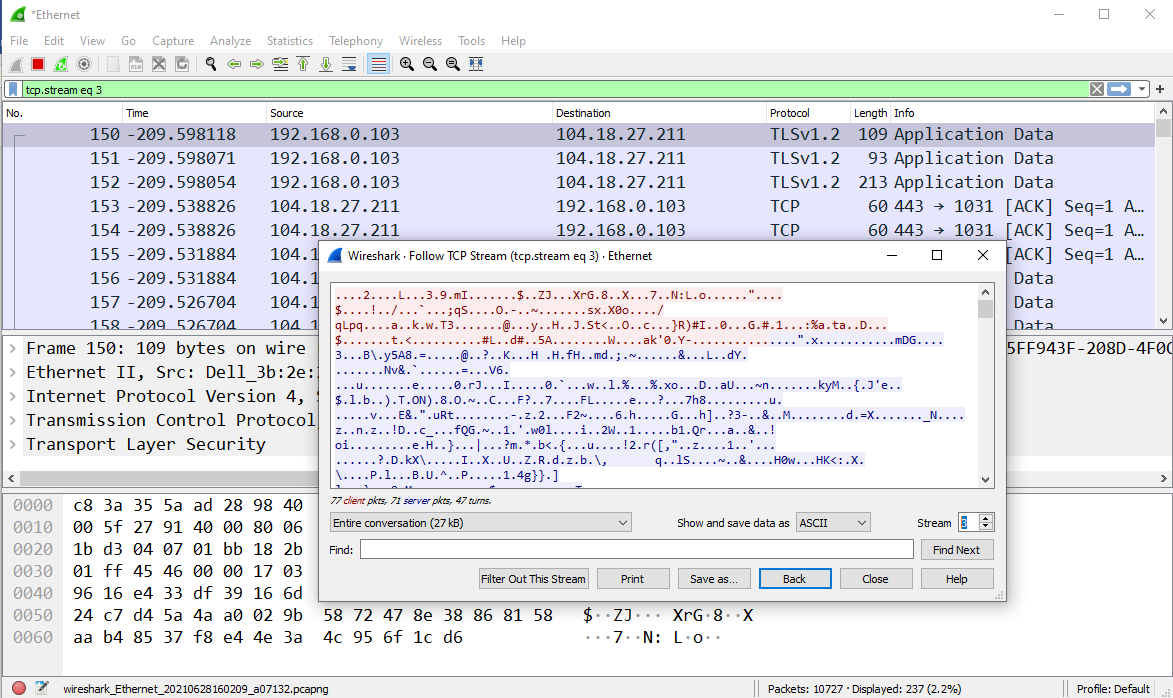
* Lọc các giao thức HTTP



* Lọc các giao thức TCP



* Lọc các gói tin theo luồng TCP Stream



* Kiểm tra một gói tin cụ thể

