HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

BÁO CÁO

Bài 8: Bắt dữ liệu mạng

Giảng viên hướng dẫn: Vũ Minh Mạnh

Sinh viên thực hiện: Nguyễn Quốc Vượng

Mã sinh viên: B21DCAT227

Lớp: D21CQAT03-B

Hà Nội, 2023

Môn học Thực tập cơ sở Bài 8: Bắt dữ liệu mạng

1 Mục đích

Bài thực hành này giúp sinh viên nắm được công cụ và cách thức bắt dữ liệu mạng, bao gồm:

1. Sử dụng tcpdump để bắt gói tin mạng
2. Sử dụng được Wireshark để bắt và phân tích gói tin mạng (HTTP/HTTPS/FTP / TCP/IP)
3. Sử dụng Network Miner để bắt và phân tích gói tin mạng

2 Nội dung thực hành

2.1 Tìm hiểu lý thuyết ○ Tìm hiểu về tính năng và hoạt động của một số công cụ bắt dữ liệu mạng như: tcpdump, Wireshark, Network Miner…

1. Tcpdump:

- **Tính năng**: Tcpdump là một tiện ích dòng lệnh được sử dụng để bắt và phân tích gói tin trên mạng. Nó cho phép người dùng xem và ghi lại gói tin mạng trên một giao diện mạng cụ thể hoặc trên tất cả các giao diện mạng.
- **Hoạt động**: Tcpdump hoạt động bằng cách lắng nghe và ghi lại các gói tin mạng đi qua một giao diện mạng. Người dùng có thể chỉ định các điều kiện lọc để chỉ hiển thị hoặc ghi lại các gói tin mạng cụ thể dựa trên địa chỉ IP, cổng, giao thức, v.v.

2. Wireshark:

- **Tính năng**: Wireshark là một công cụ phân tích gói tin mạng mạnh mẽ và dễ sử dụng, cung cấp một giao diện đồ họa để xem, phân tích và phân loại các gói tin mạng.

- **Hoạt động**: Wireshark hoạt động bằng cách lắng nghe và ghi lại các gói tin mạng từ một hoặc nhiều giao diện mạng. Sau đó, nó hiển thị các gói tin này dưới dạng danh sách chi tiết, cho phép người dùng xem, lọc, và phân tích chúng theo nhiều cách khác nhau.

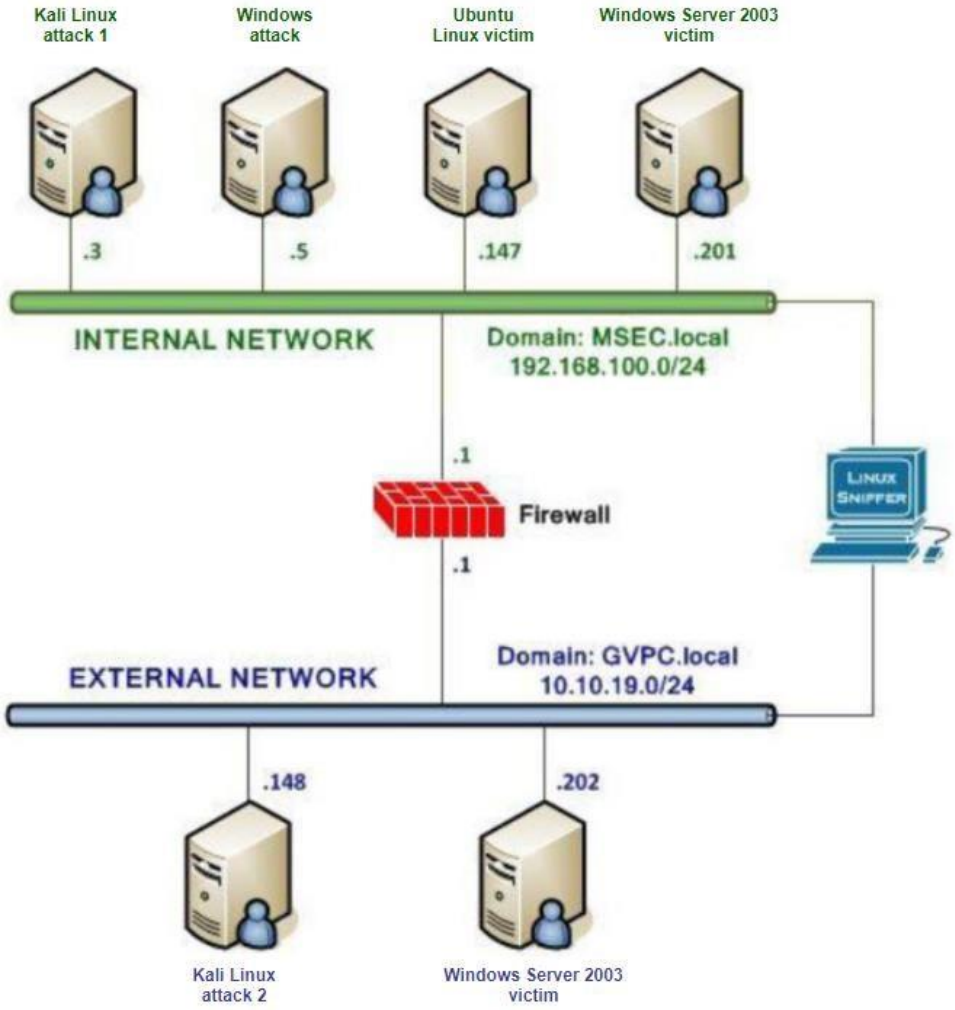
3. NetworkMiner:

- **Tính năng**: NetworkMiner là một công cụ phân tích mạng tự động được thiết kế để thu thập thông tin từ các gói tin mạng và phân tích dữ liệu đó để trích xuất thông tin quan trọng như tên người dùng, mật khẩu, URL, v.v.
- **Hoạt động**: NetworkMiner hoạt động bằng cách tự động phân tích gói tin mạng và trích xuất thông tin từ chúng. Nó cũng cung cấp các tính năng như tái lắp các tệp tin được truyền qua mạng và xác định các máy chủ mạng và các dịch vụ đang chạy.

- Một số tài liệu tham khảo:
- Chương 4, Bài giảng Kỹ thuật theo dõi giám sát an toàn mạng, HVCN BCVT 2021 ○ https://www.tcpdump.org/index.html#documentation ○ https://www.wireshark.org/docs/wsug_html/ ○ https://docs.securityonion.net/en/2.3/networkminer.html#

2.2 Chuẩn bị môi trường ○ Phần mềm VMWare Workstation(hoặc các phần mềm hỗ trợ ảo hóa khác). ○ Các file máy ảo VMware và hệ thống mạng đã cài đặt trong bài thực hành 5 trước đó: máy trạm, máy Kali Linux, máy chủ Windows và Linux. Chú ý: chỉ cần bật các máy cần sử dụng trong bài lab.

- Topo mạng như đã cấu hình trong bài 5.

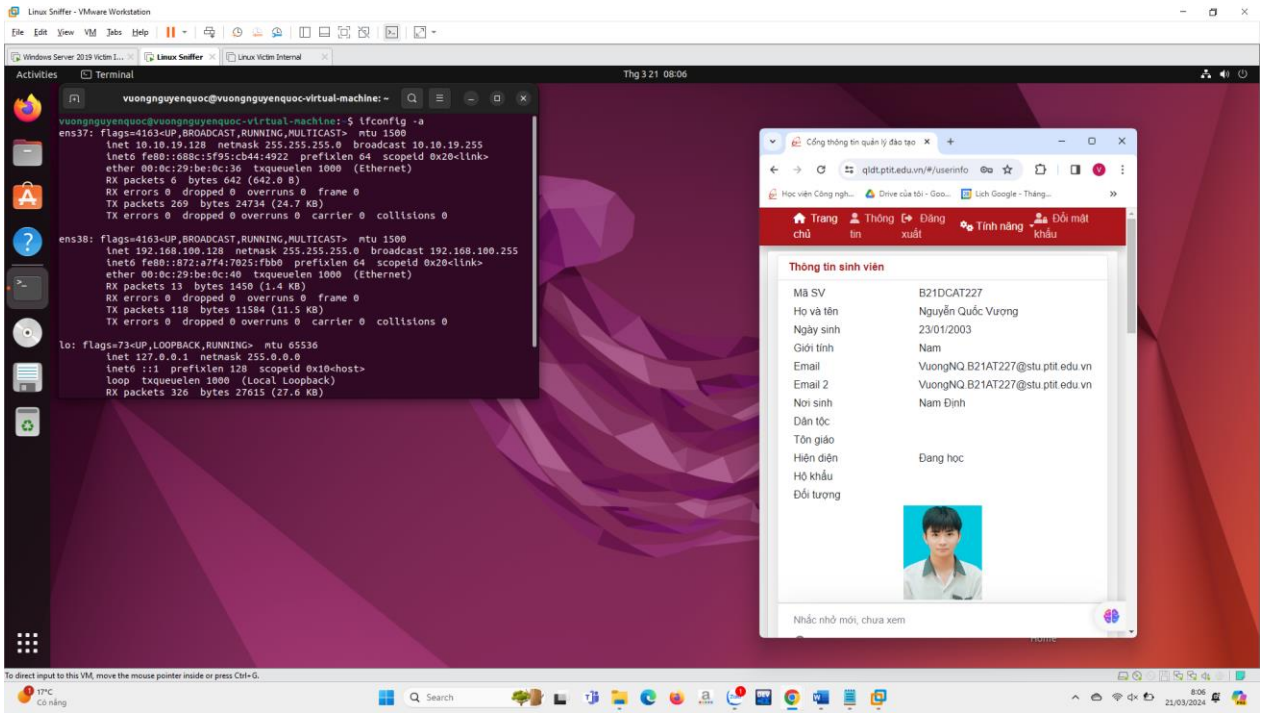


2.3 Các bước thực hiện và kết quả cần đạt

2.3.1 Sử dụng tcpdump

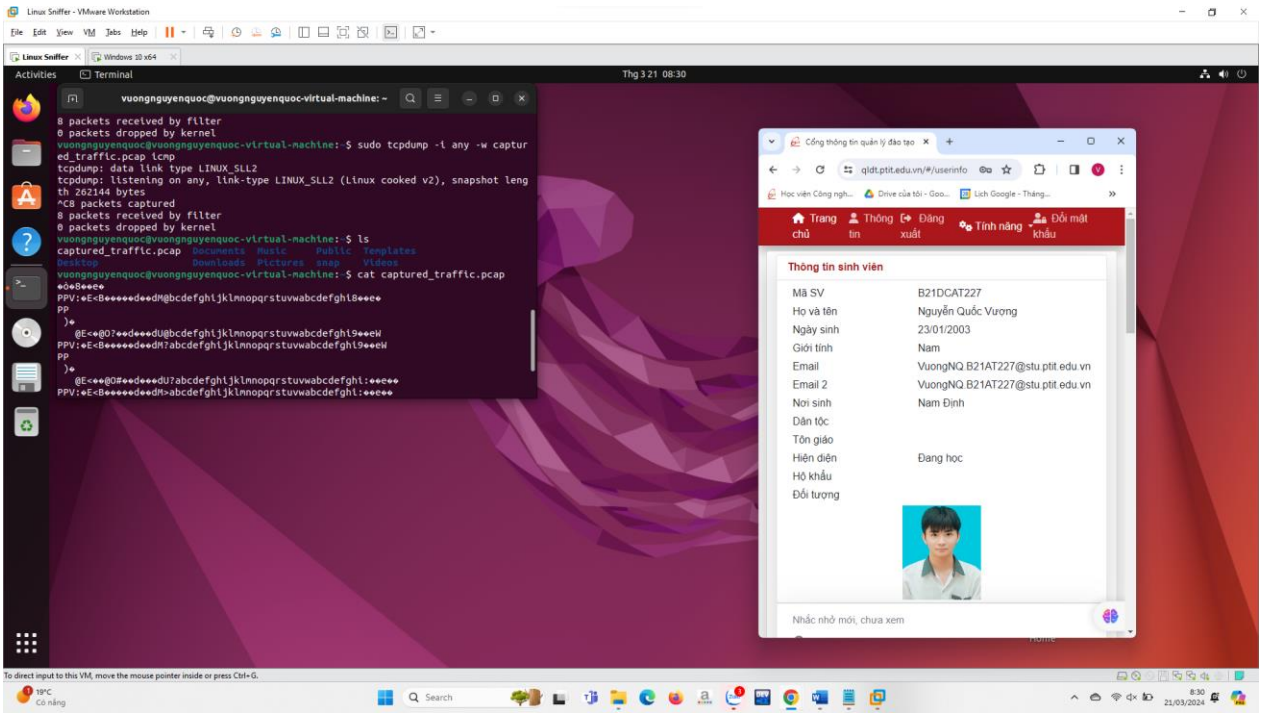
a) Các bước thực hiện

- Trong mạng Internal, đăng nhập Linux Sniffer và xem tất cả các interfaces trong hệ thống (root@bt:~#**ifconfig -a**)

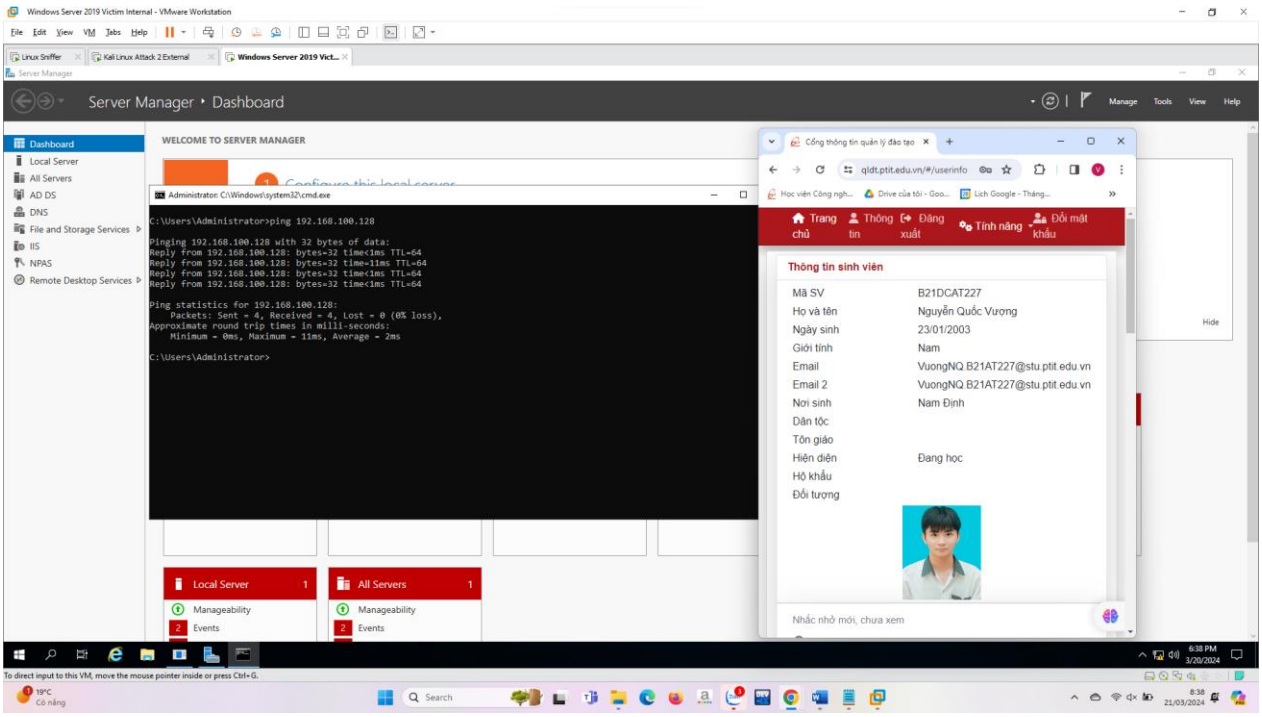


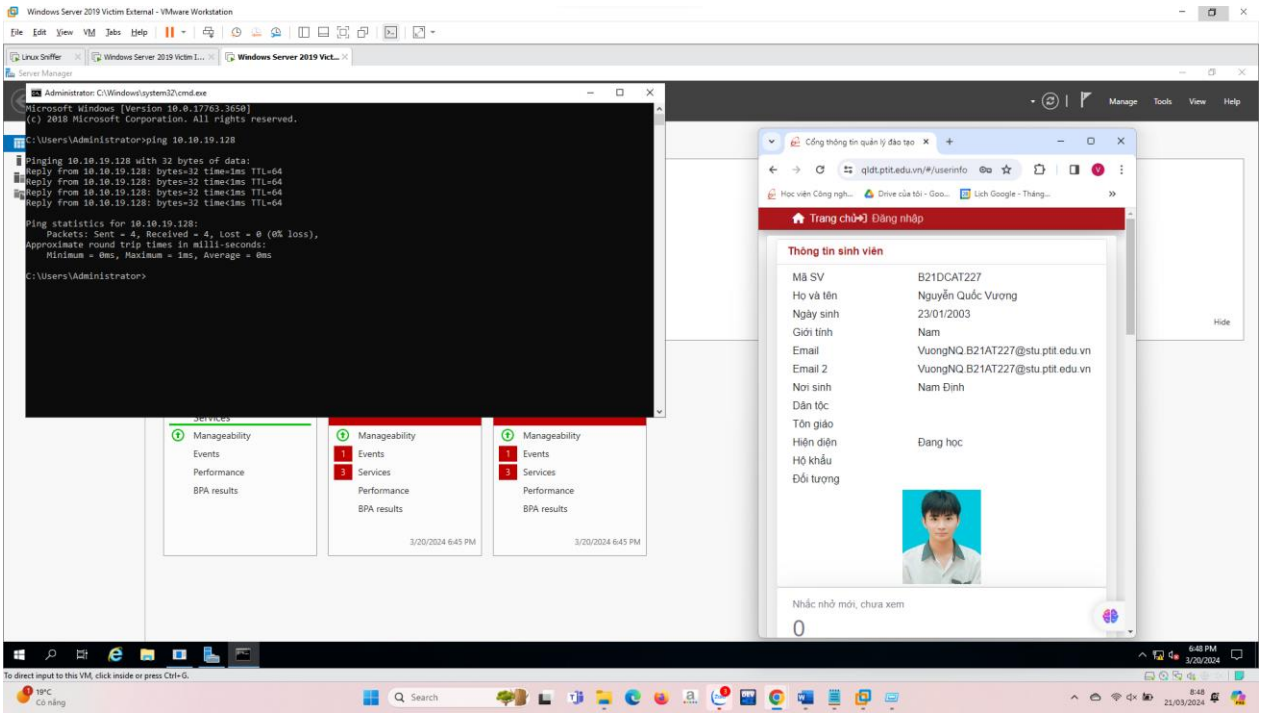
- Kích hoạt các interfaces(eth0, eth1) hoạt động ở chế độ hỗn hợp, sau đó khởi động tcpdump. Bắt gói tin trên

dải mạng 192.168.100.0/24 và gửi vào một file(thời gian chờ dữ liệu trong khoảng 5 phút).

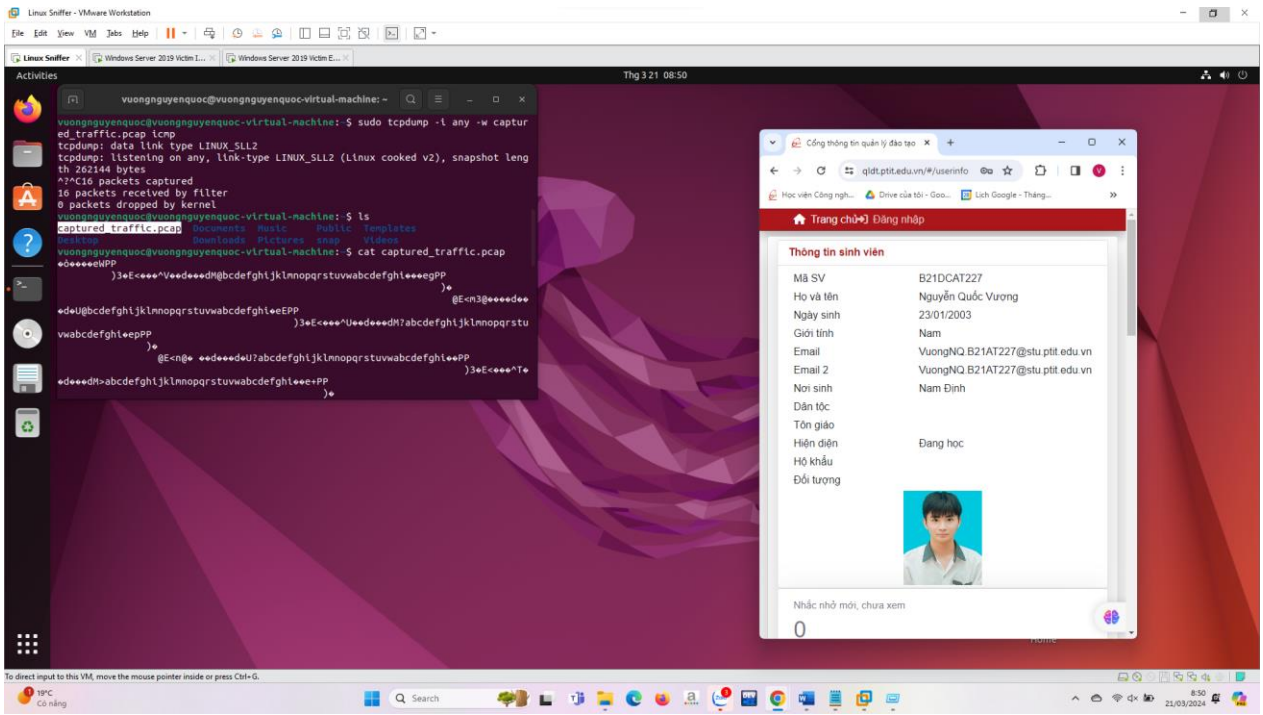


- Trên máy Window Server 2003 và tiến hành ping đến dải mạng internal và dải mạng external





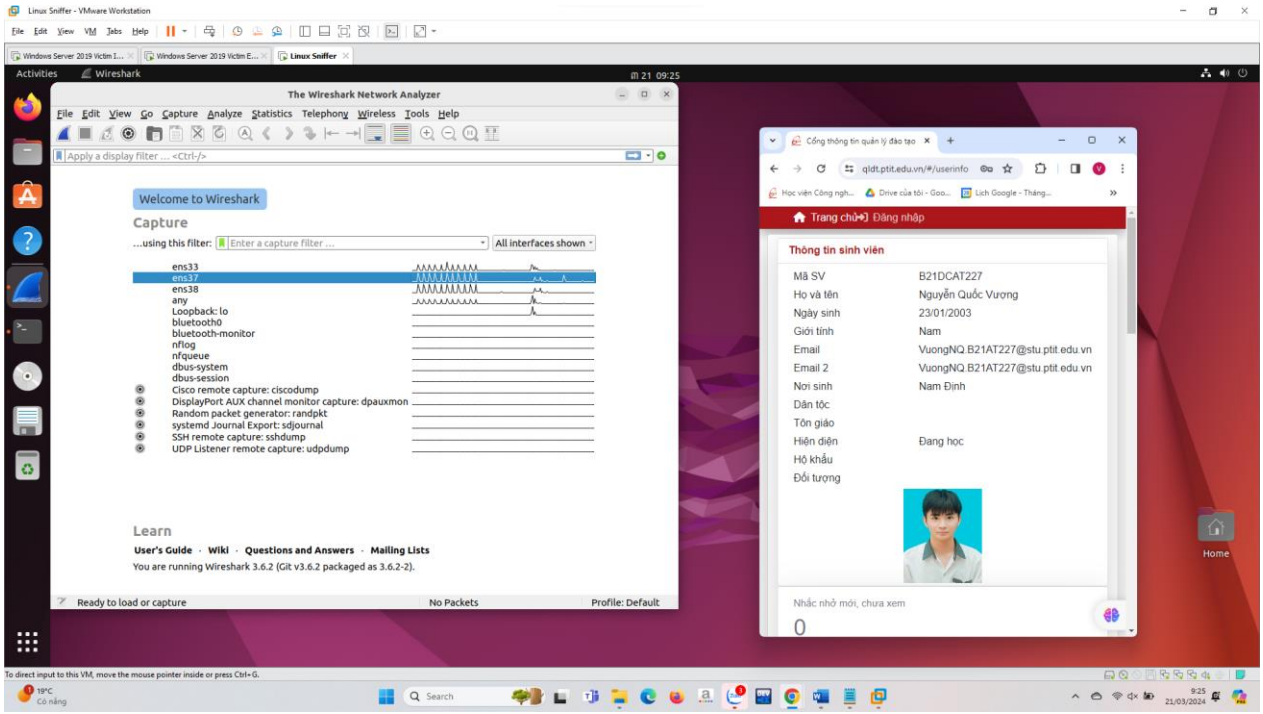
- Trên máy Linux Sniffer, tiến hành bắt gói tin bằng tcpdump, và lưu dữ liệu vào file pcap.



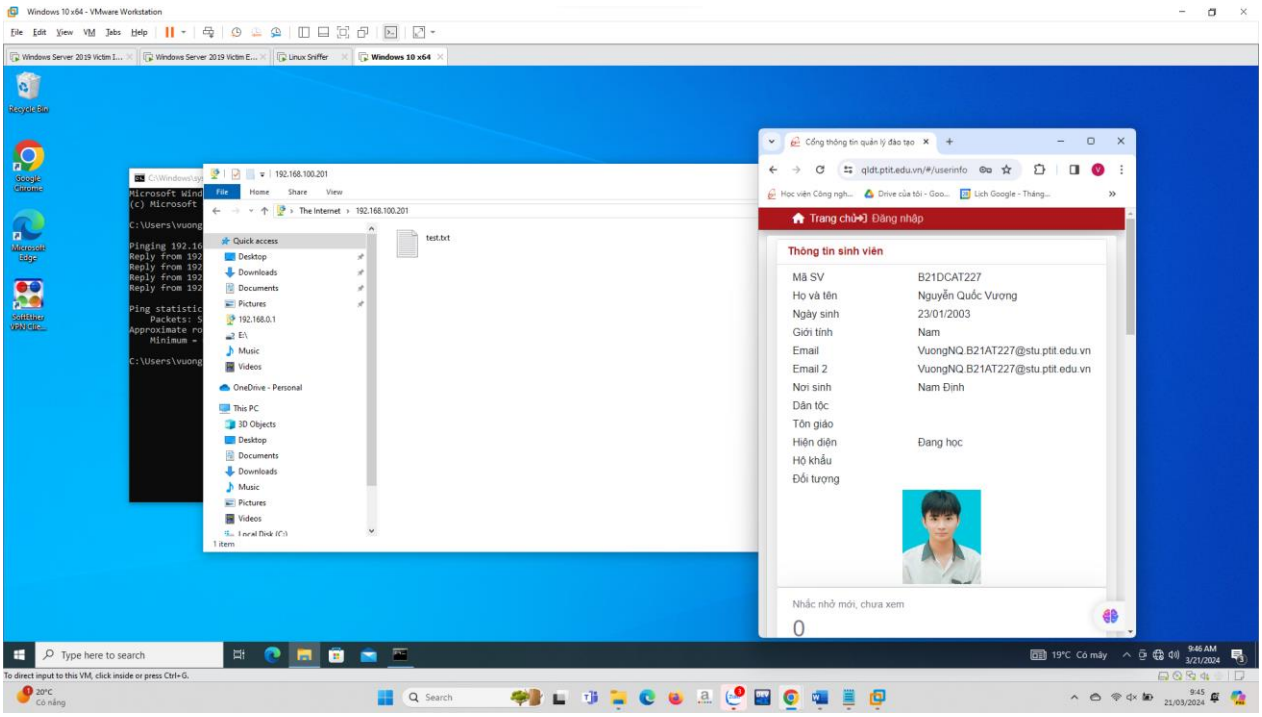
2.3.2 Sử dụng Wireshark để bắt và phân tích các gói tin

a) Các bước thực hiện

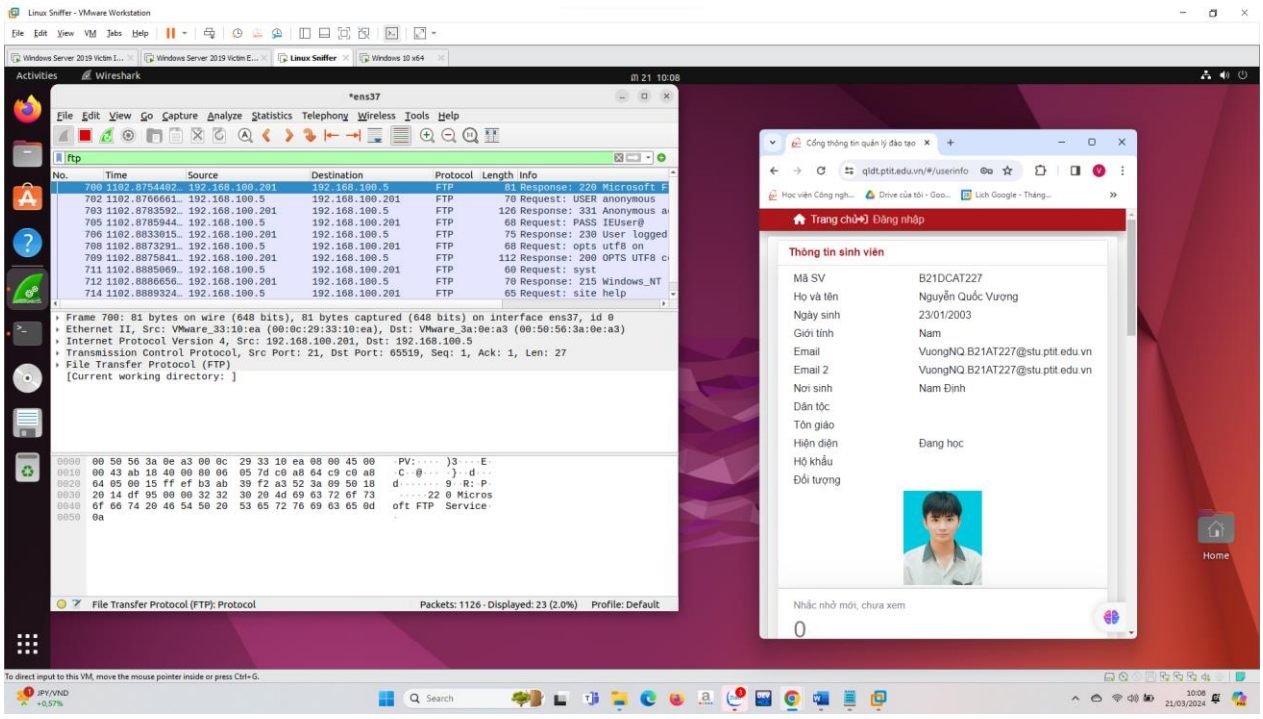
- Có thể tải Wireshark ở đây: http://www.wireshark.org/download.html
- Trên máy Windows attack, bật các interfaces eth0, eth1 và khởi động Wireshark. Trong **Capture Interfaces** chọn Start ở dòng eth0 để bắt gói tin trên dải mạng 192.168.100.0



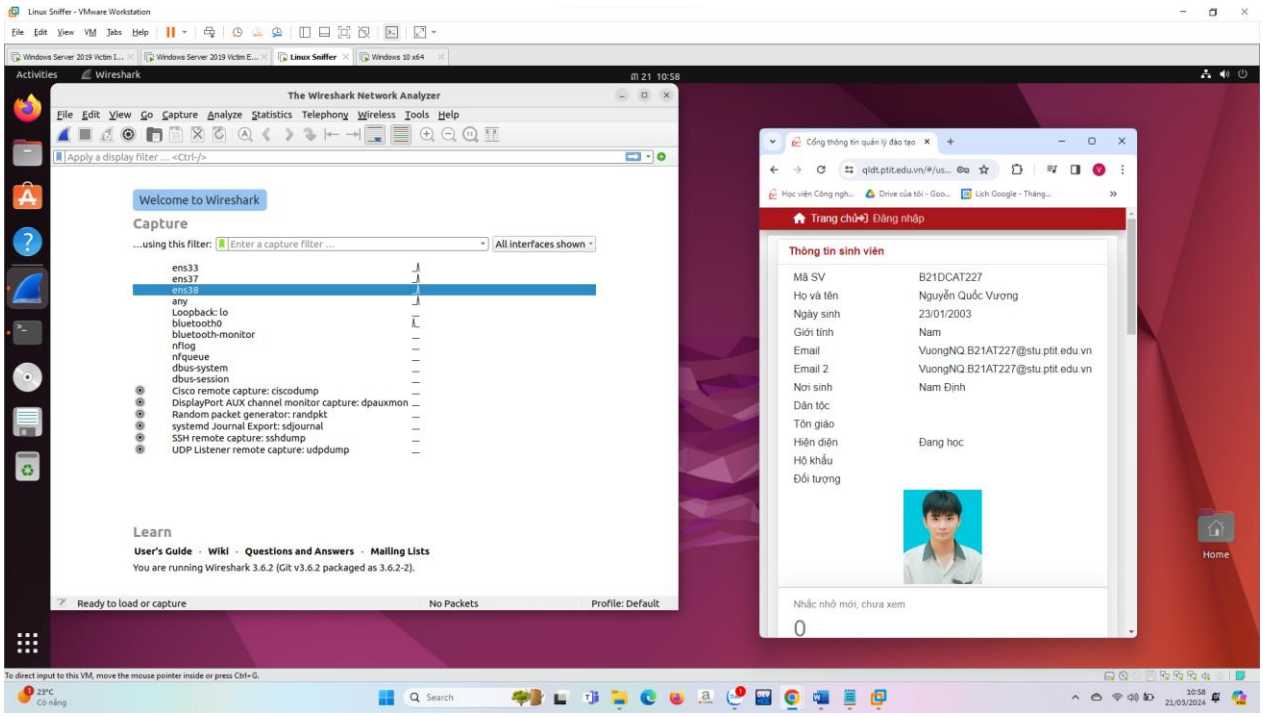
- Trên máy Windows 7 victim kết nối tới ftp server (C:**ftp 192.168.100.201)**



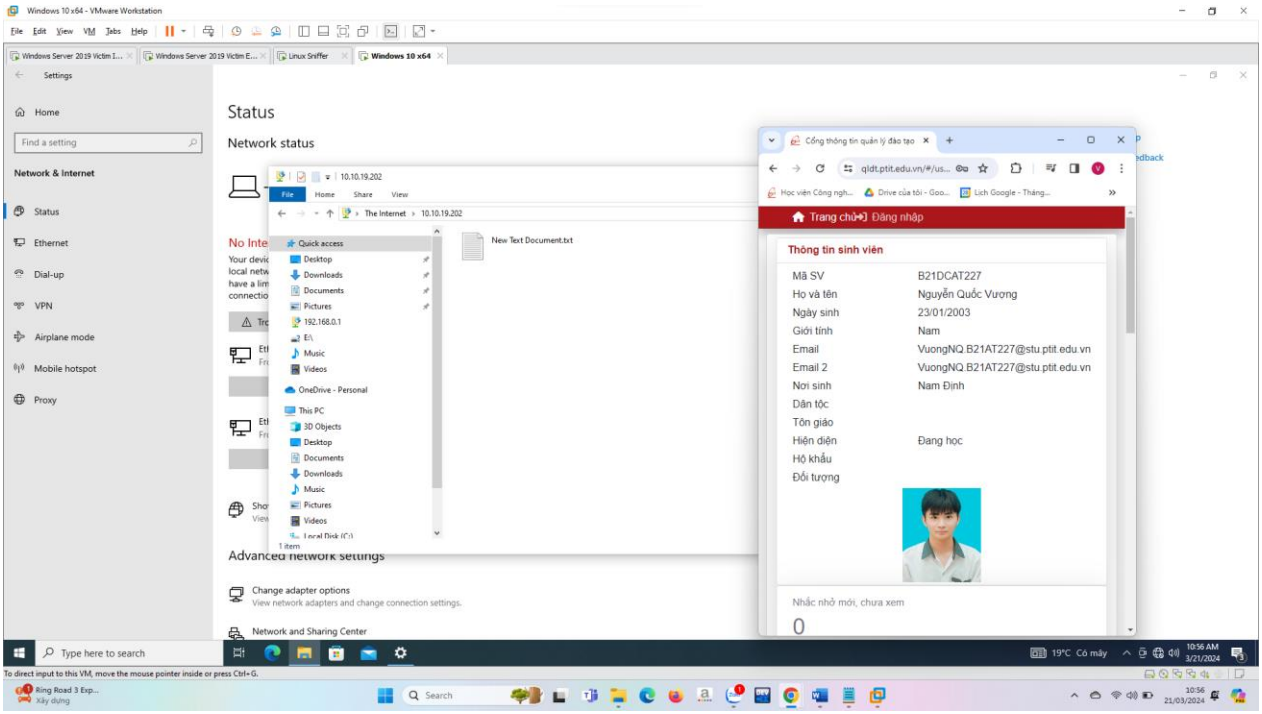
o Trên Linux Sniffer dừng quá trình bắt gói tin và tiến hành lọc gói tin theo giao thức ftp



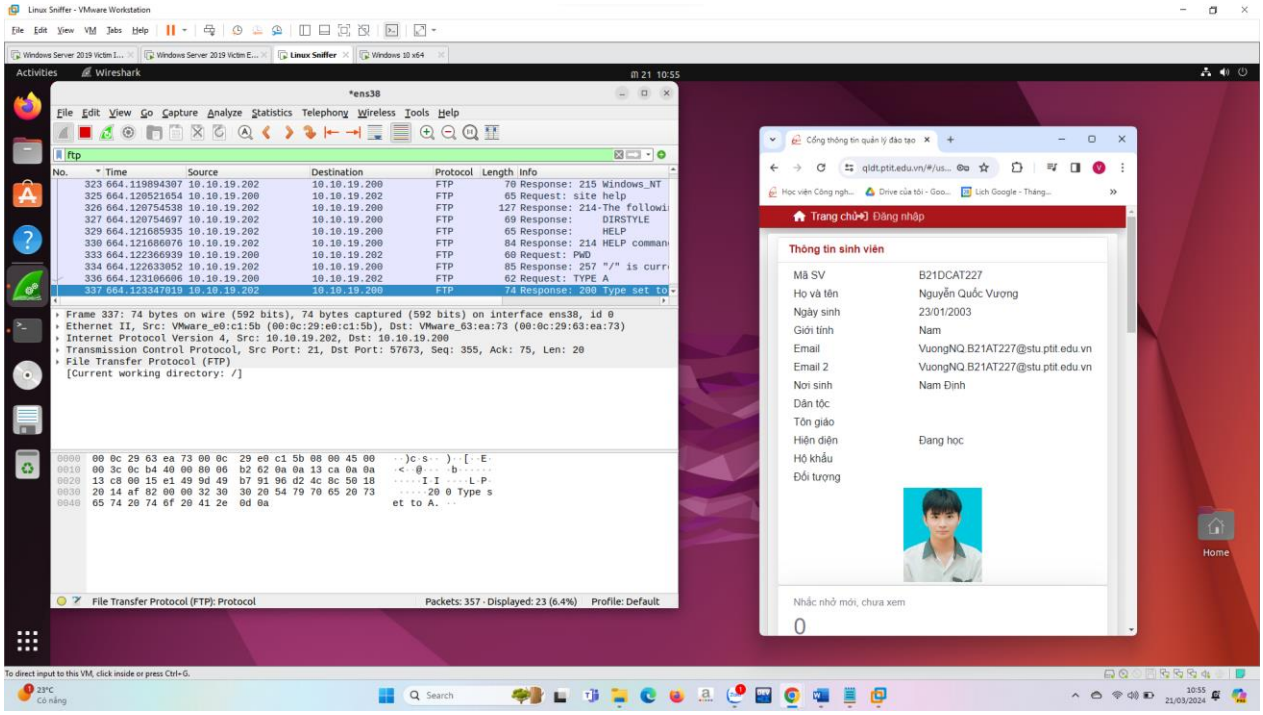
o Trên máy Linux Sniffer, trong **Capture Interfaces** chọn Start ở dòng eth1 để bắt gói tin trên dải mạng 10.10.19.0



- Trên máy Windows 7 victim, kết nối với ftp server(root@bt:~#**ftp 10.10.19.202)**



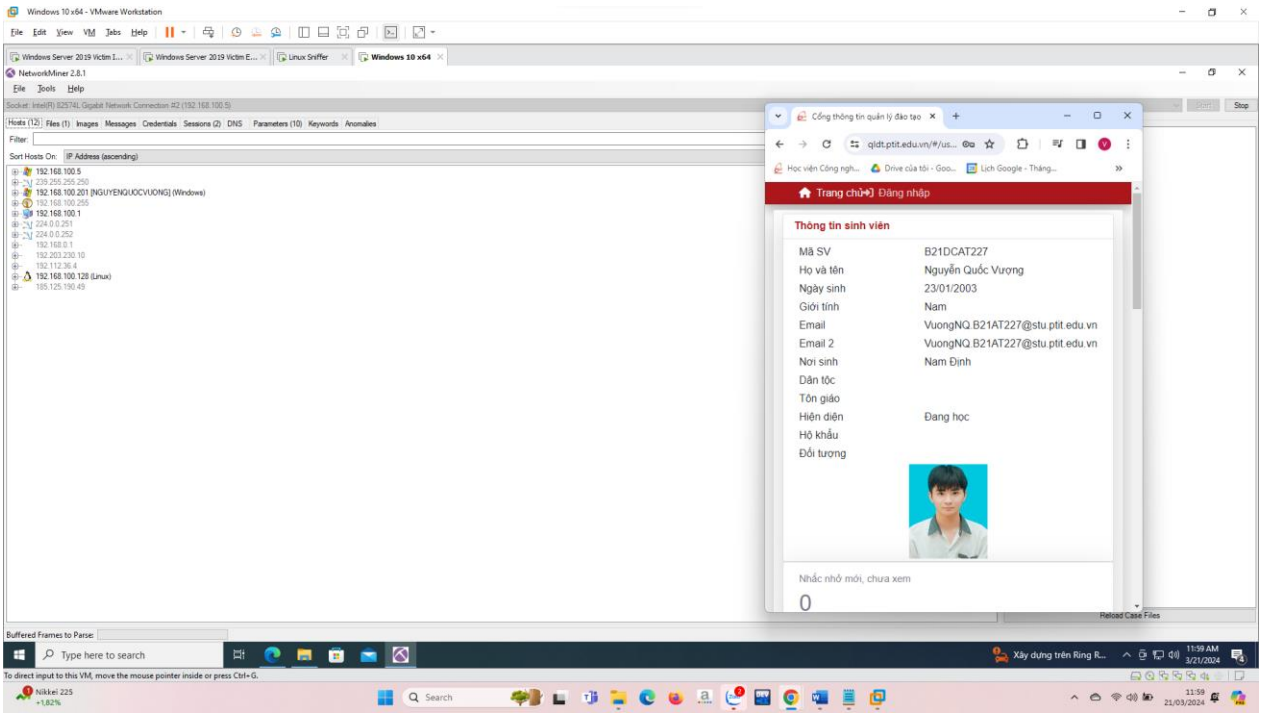
o Trên Linux Sniffer dừng quá trình bắt gói tin và tiến hành lọc gói tin theo giao thức ftp



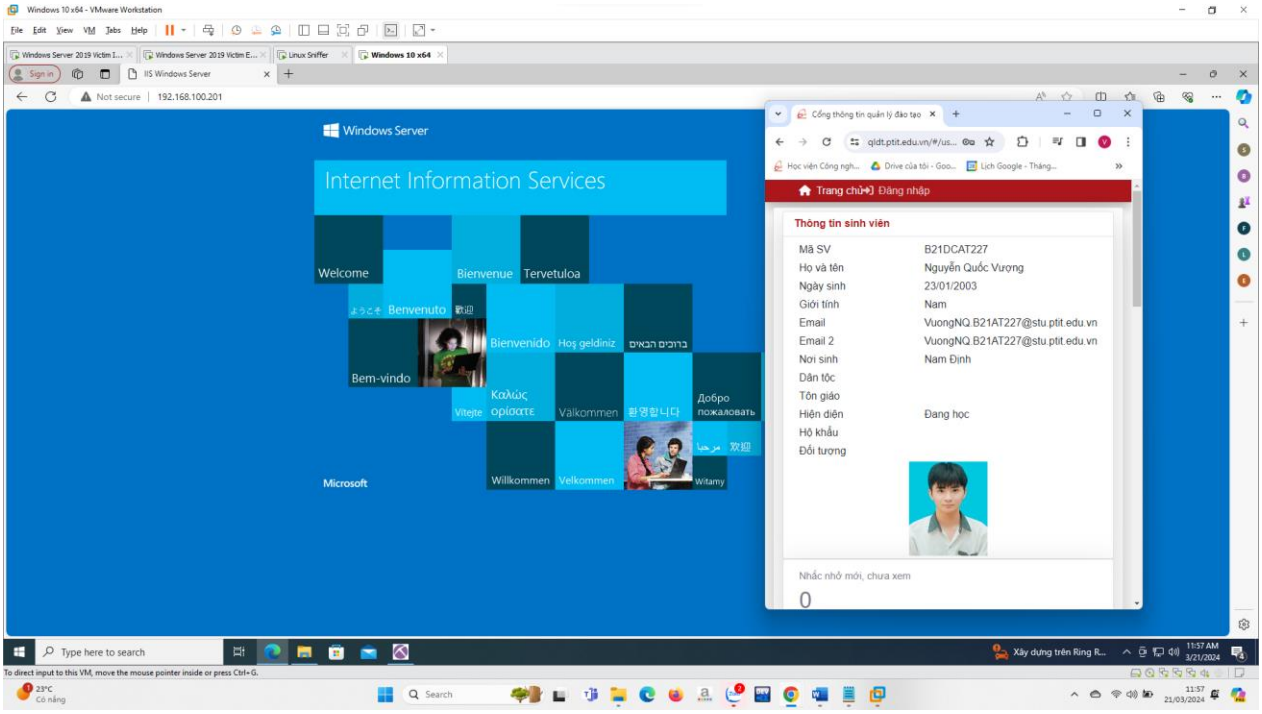
2.3.3 Sử dụng Network Miner để bắt và phân tích các gói tin

a) Các bước thực hiện

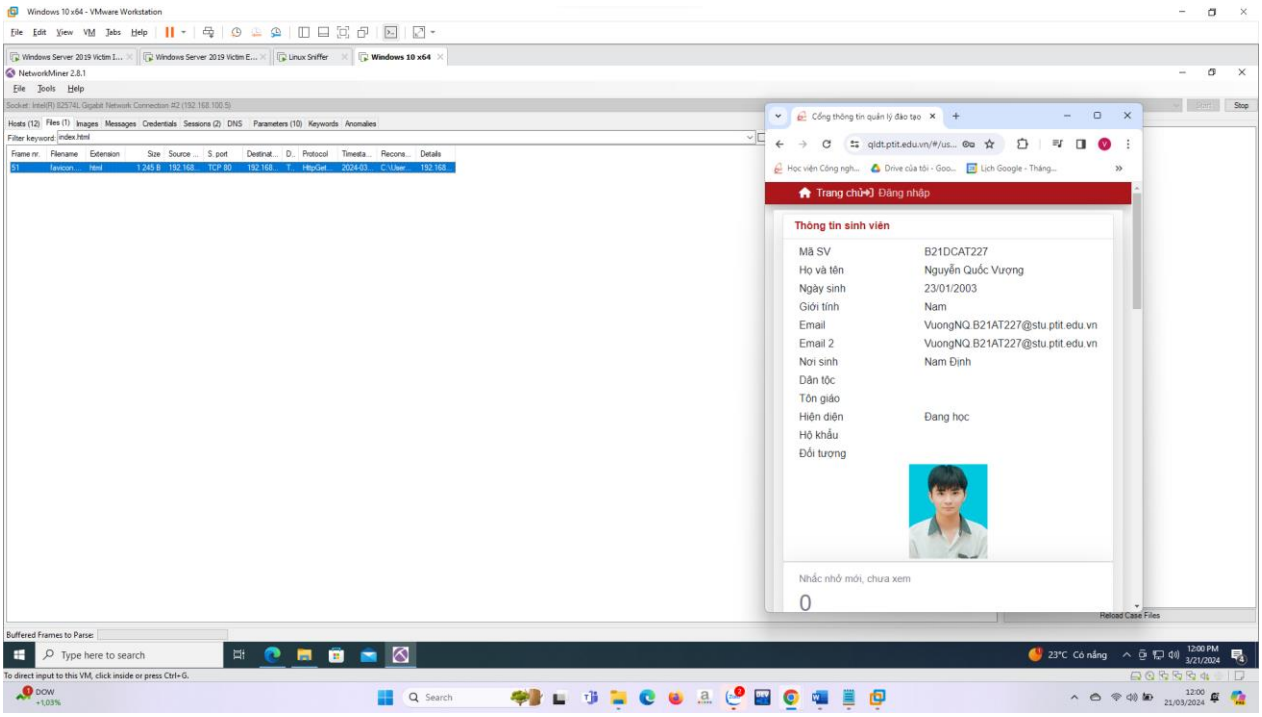
o Trên máy Windows 7 Internal Attack khởi động Network Miner và chọn **Socket: Intel® PRO/1000MT Network Connection(192.168.100.5)** và bắt đầu bắt gói tin.



Sử dụng Internet Explorer để kết nối đến trang web của Windows 2003 Server Internal Victim: http://192.168.100.201/. Sau đó dừng quá trình bắt gói tin.



o Trong Network Miner, chọn File/ index.html để xem dữ liệu gói tin vừa bắt được.


Windows 10 x64 - VMware Workstation
NetworkMiner 2.8.1
Cổng thông tin quản lý đào tạo
Trang chủ
Đăng nhập
Thông tin sinh viên
Mã SV B21DCAT227
Họ và tên Nguyễn Quốc Vượng
Ngày sinh 23/01/2003
Giới tính Nam
Email VuongNQ.B21AT227@stu.ptit.edu.vn
Email 2 VuongNQ.B21AT227@stu.ptit.edu.vn
Nơi sinh Nam Định
Dân tộc
Tôn giáo
Hiện diện Đang học
Hộ khẩu
Đối tượng
Nhắc nhở mới, chưa xem
0
Type here to search
23°C Có nắng
Search