**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP HCM**

**KHOA CÔNG NGHỆ THÔNG TIN**

**Môn: Thực Hành Phân Tích Mã Độc**

**------------------------------------------------------------------**

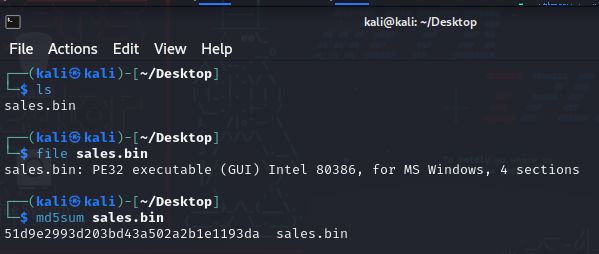
**Họ Và Tên: Trần Hân Nhi**

**MSSV: 2011770131**

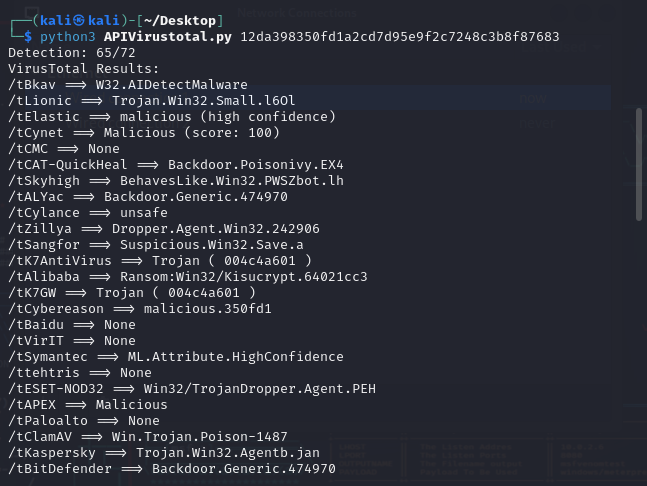
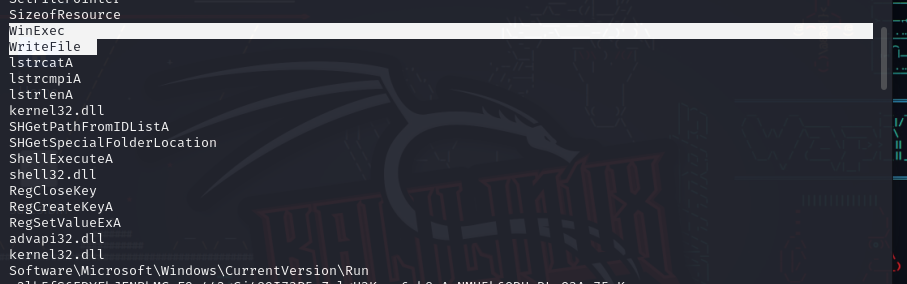
**Lớp: 20DATA1**

**Báo Cáo Tuần 2**

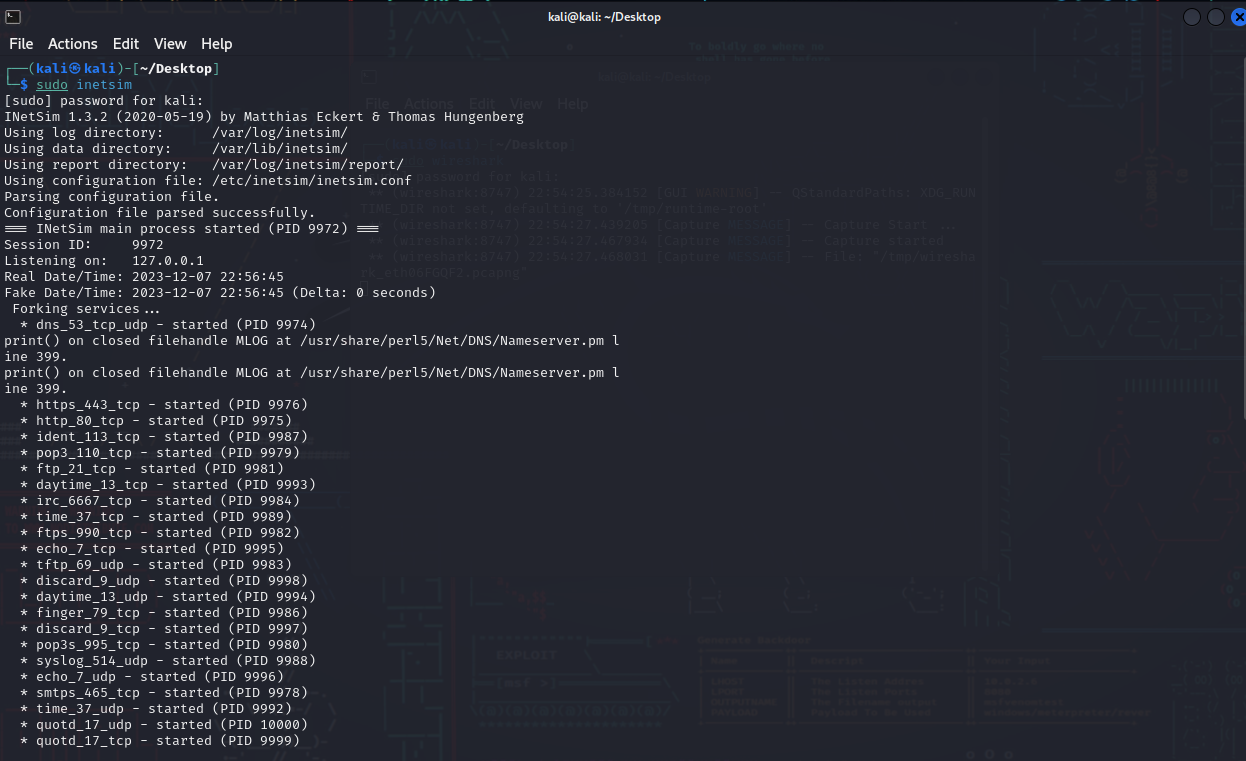
* Thực hiện phân tích tĩnh để kiểm tra mẫu mã độc, dùng md5sum xác định giá trị hàm băm của file sales.bin



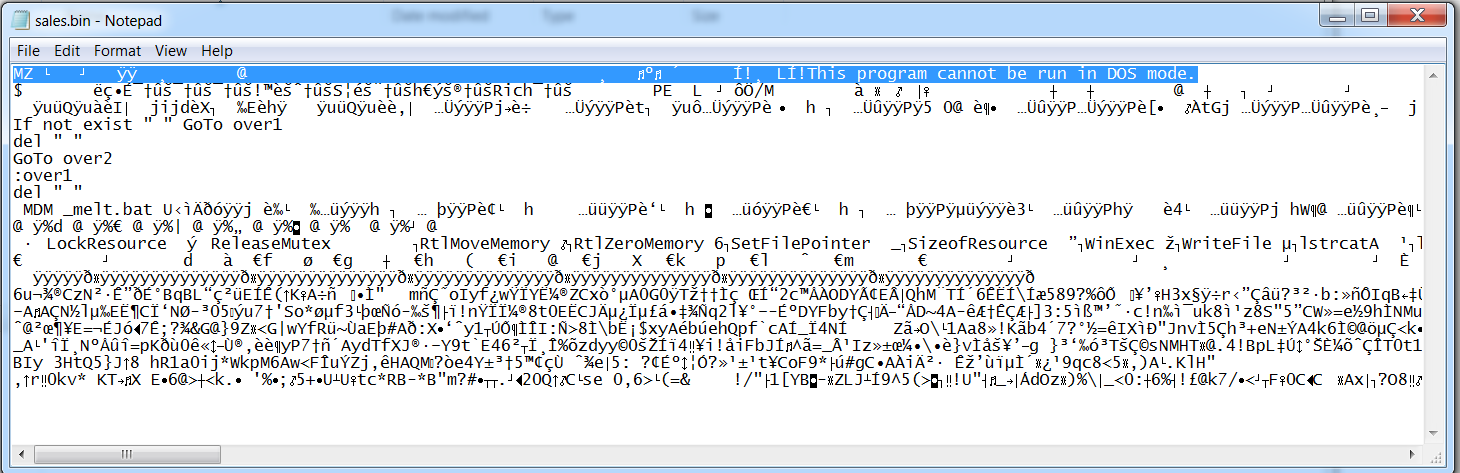
* Dùng strings kiểm tra



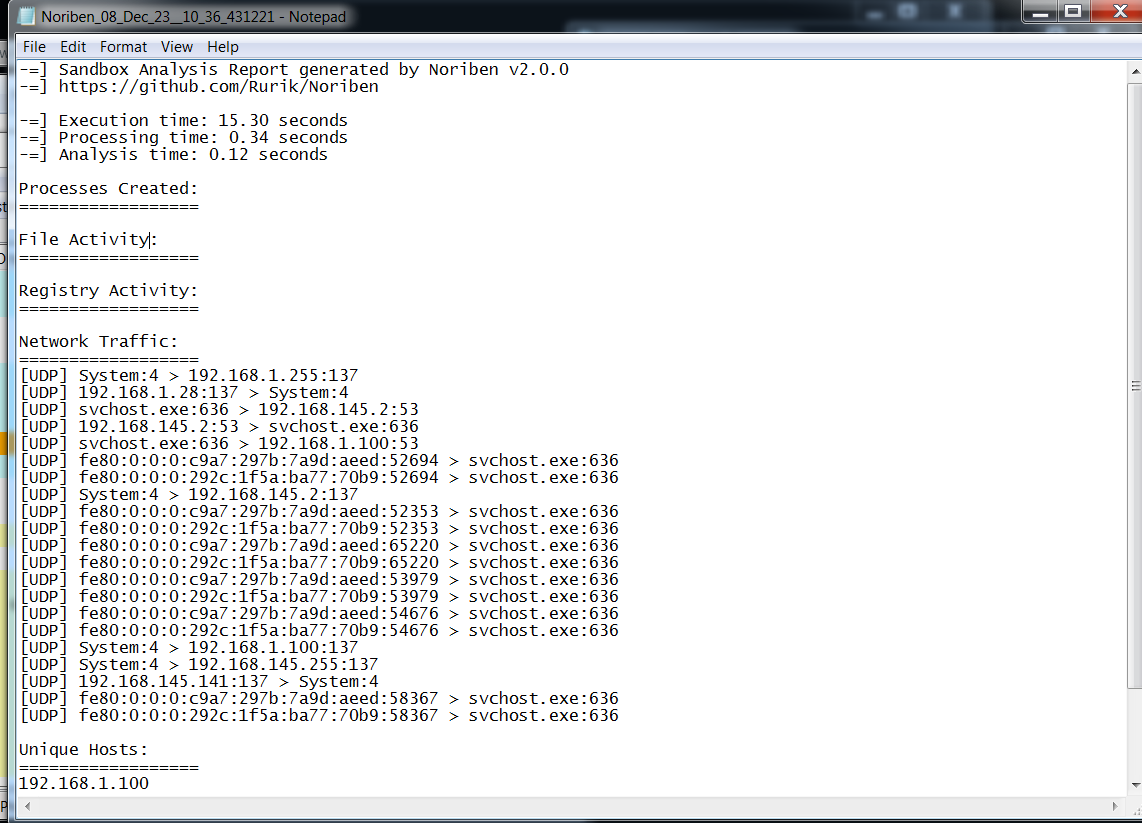
* Dùng inetsim mô phỏng port đánh lạc hướng mã độc.

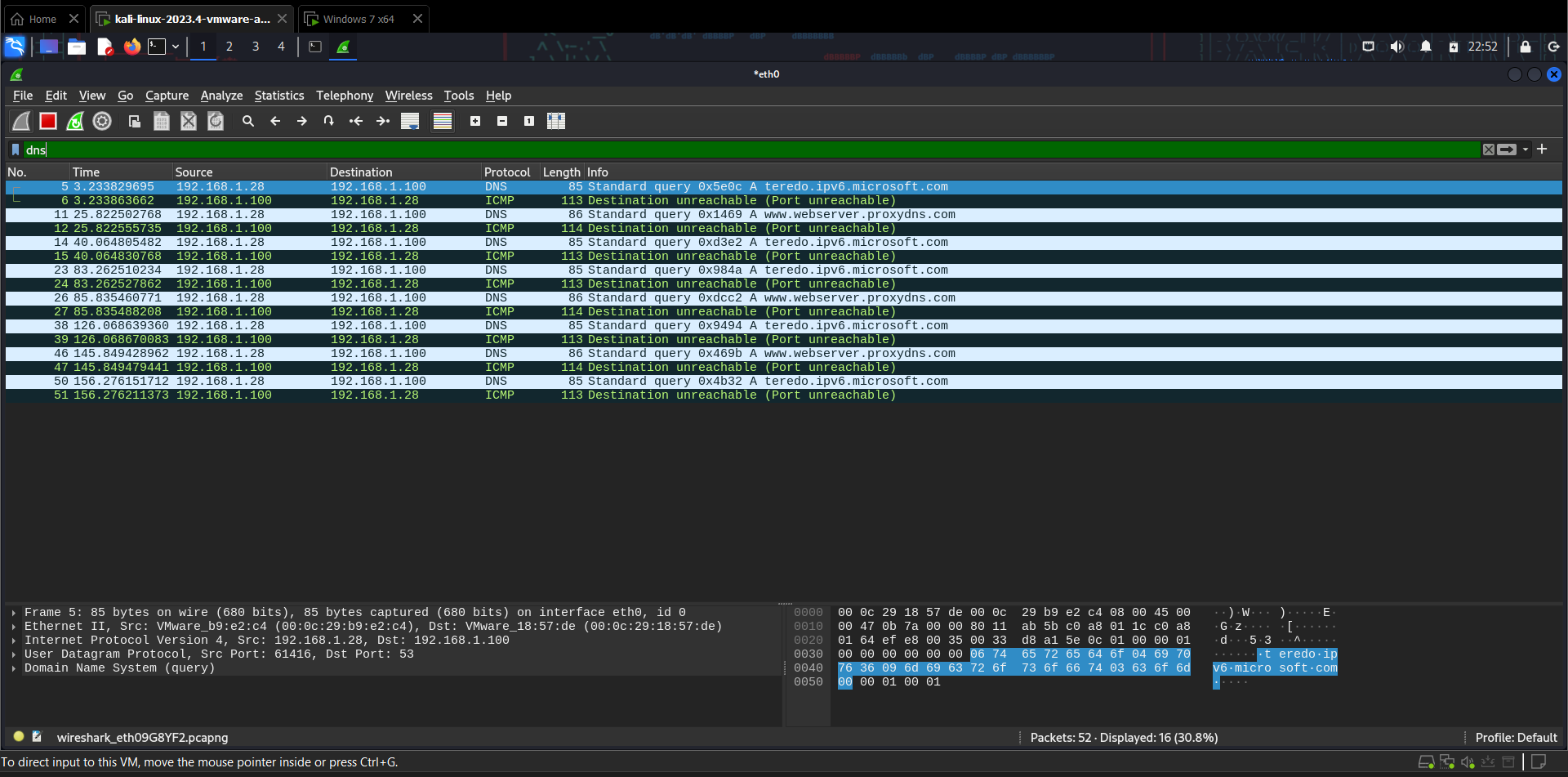
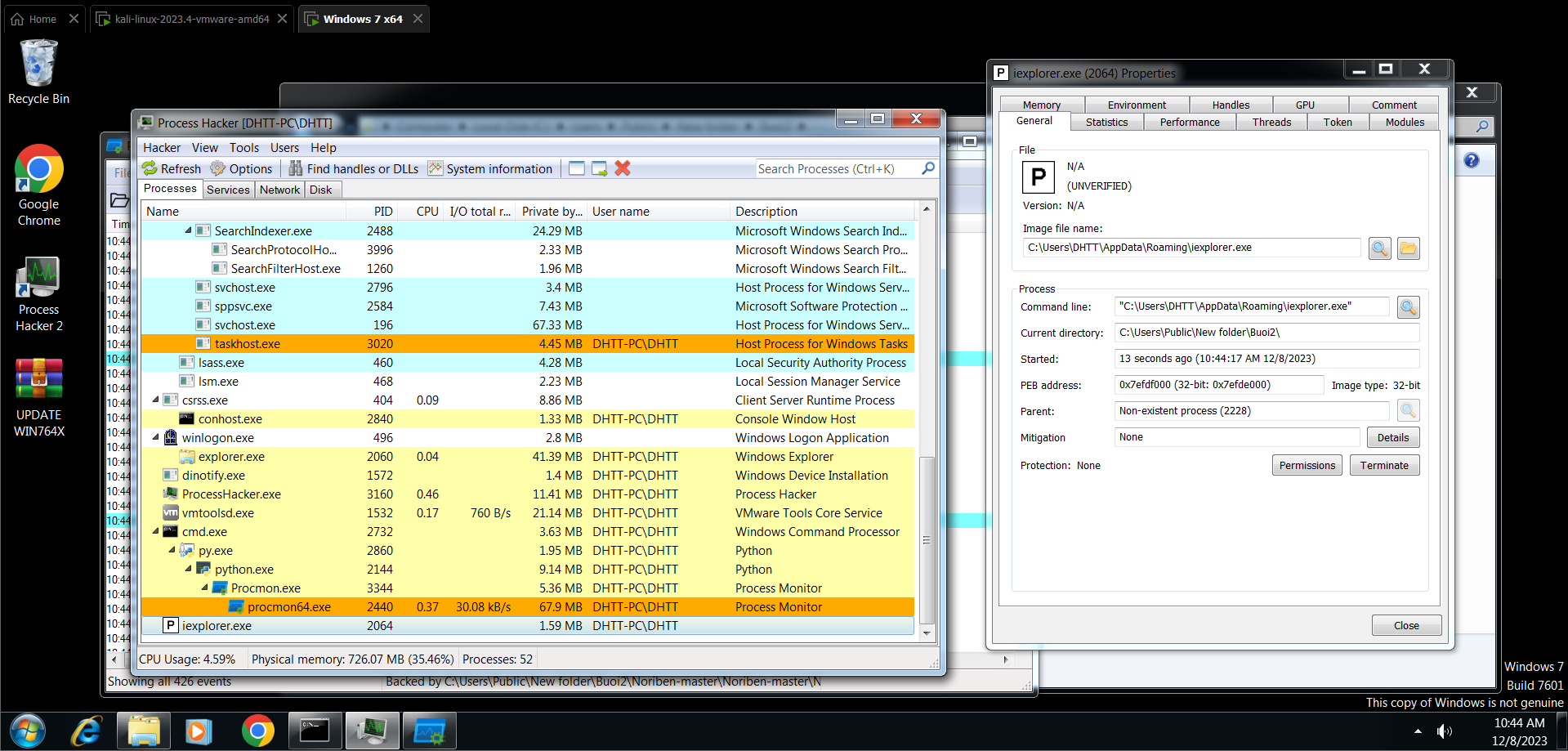


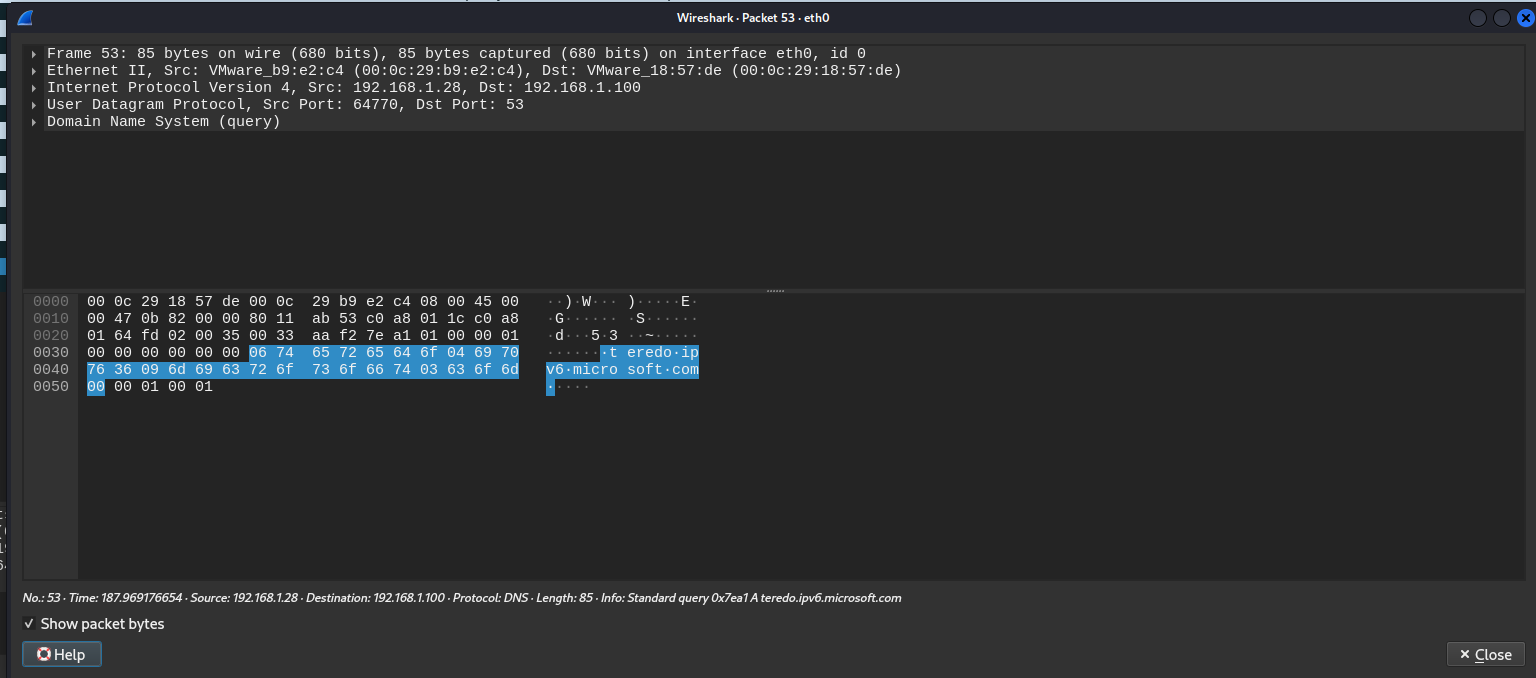
* Xác định tệp thực thi bằng notepad. File hiện dòng MZ, ta xác định được đây là tệp thực thi EXE PE.



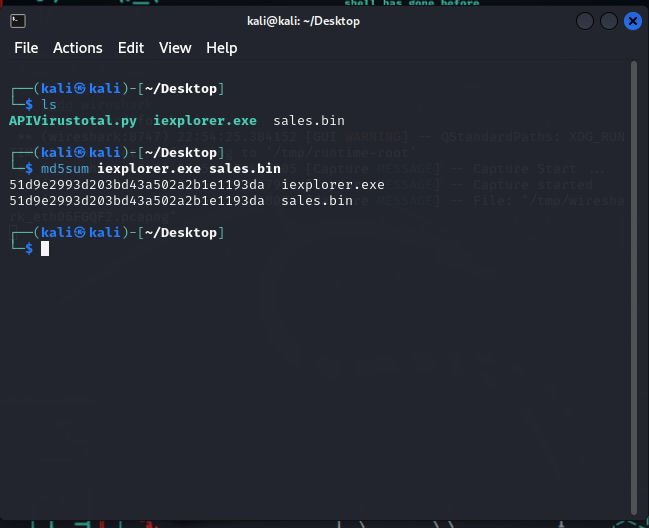
* Chạy Noriben khởi động Process Monitor. Khi hoàn tất giám sát, lưu kết quả vào một tệp văn bản (.txt) và tệp CSV (.csv) trong cùng thư mục.



- Khi thực thi file mã độc, Process Hacker hiện 1 tiến trình lạ. Ta tiến hành kiểm tra thông tin của chương trình lạ.



* So sánh giá trị băm md5 của file mã độc và tiến trình lạ.



* File iexplorer.exe không cần triển khai chức năng xoá file trong mã nguồn. Nó chỉ cần nhập và gọi hàm DeleteFile.

