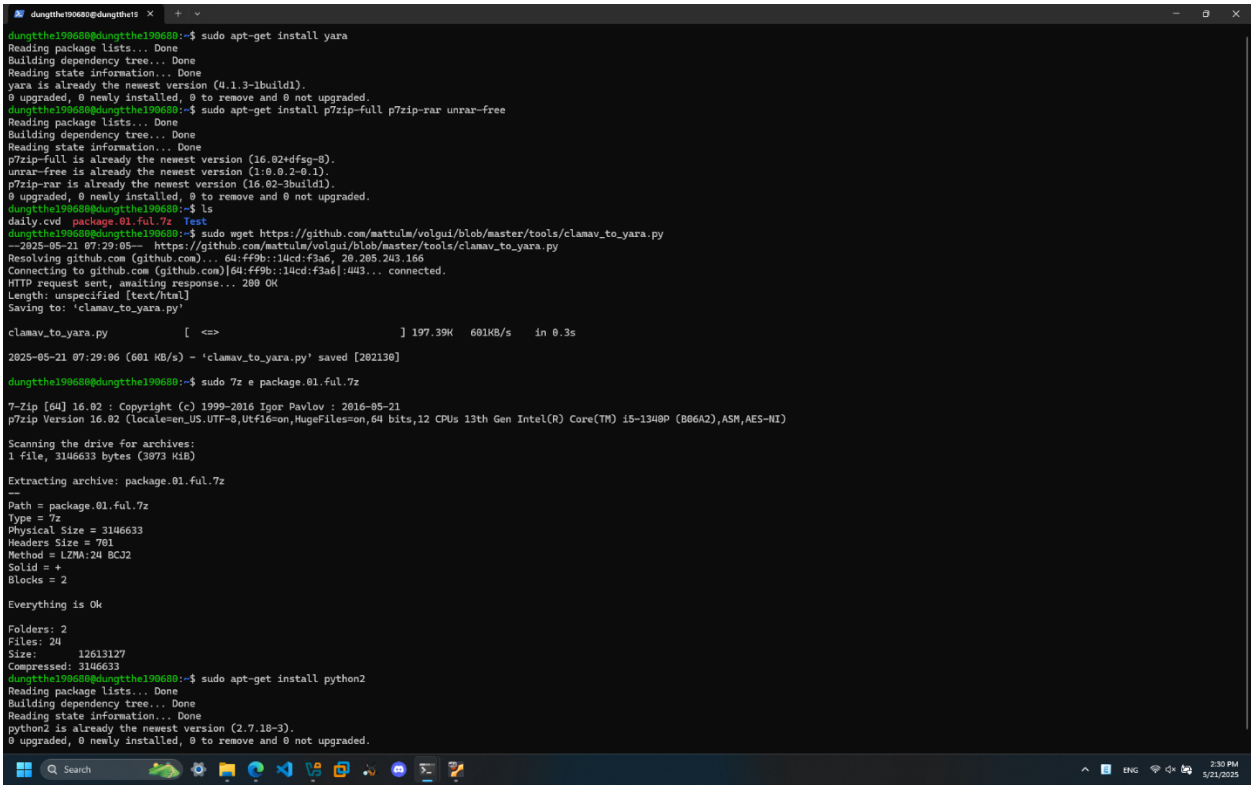
Họ và tên: Trần Trí Dũng

Mã số sinh viên: HE190680

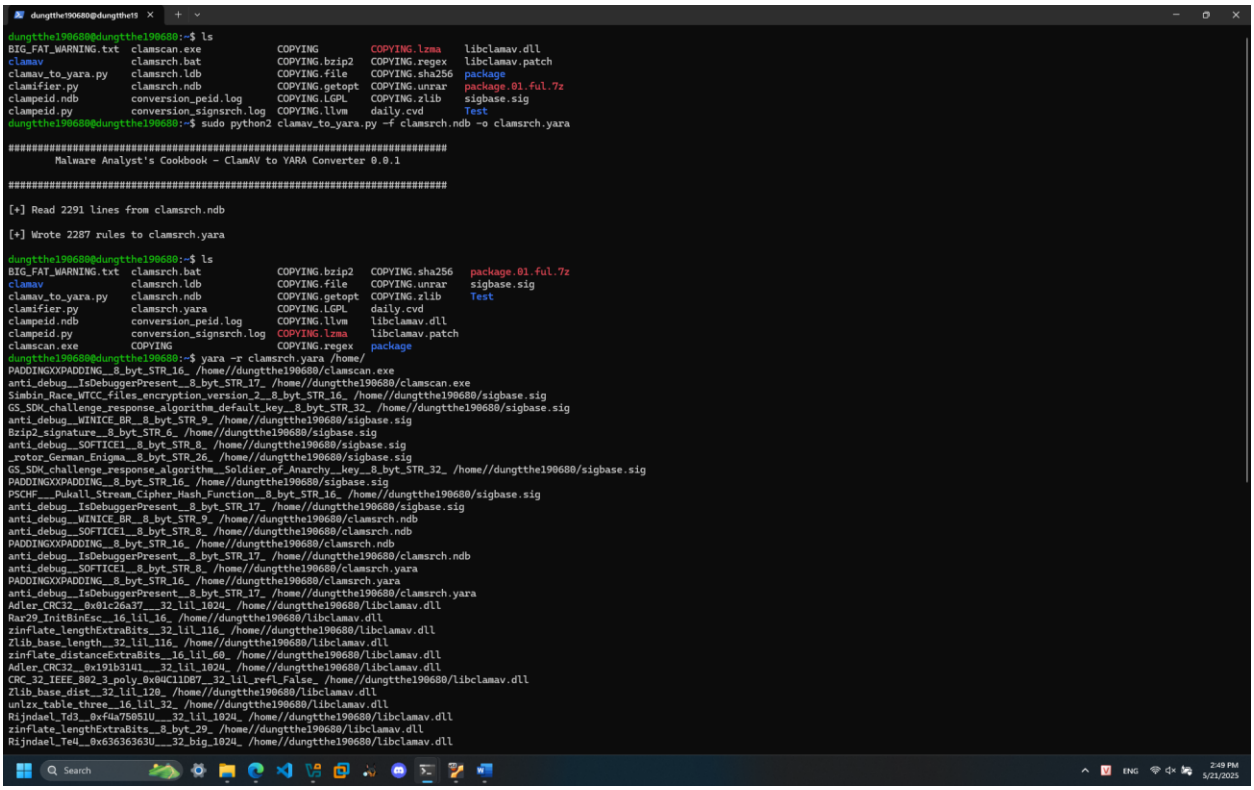
Lớp: IA1901

Lab 4:

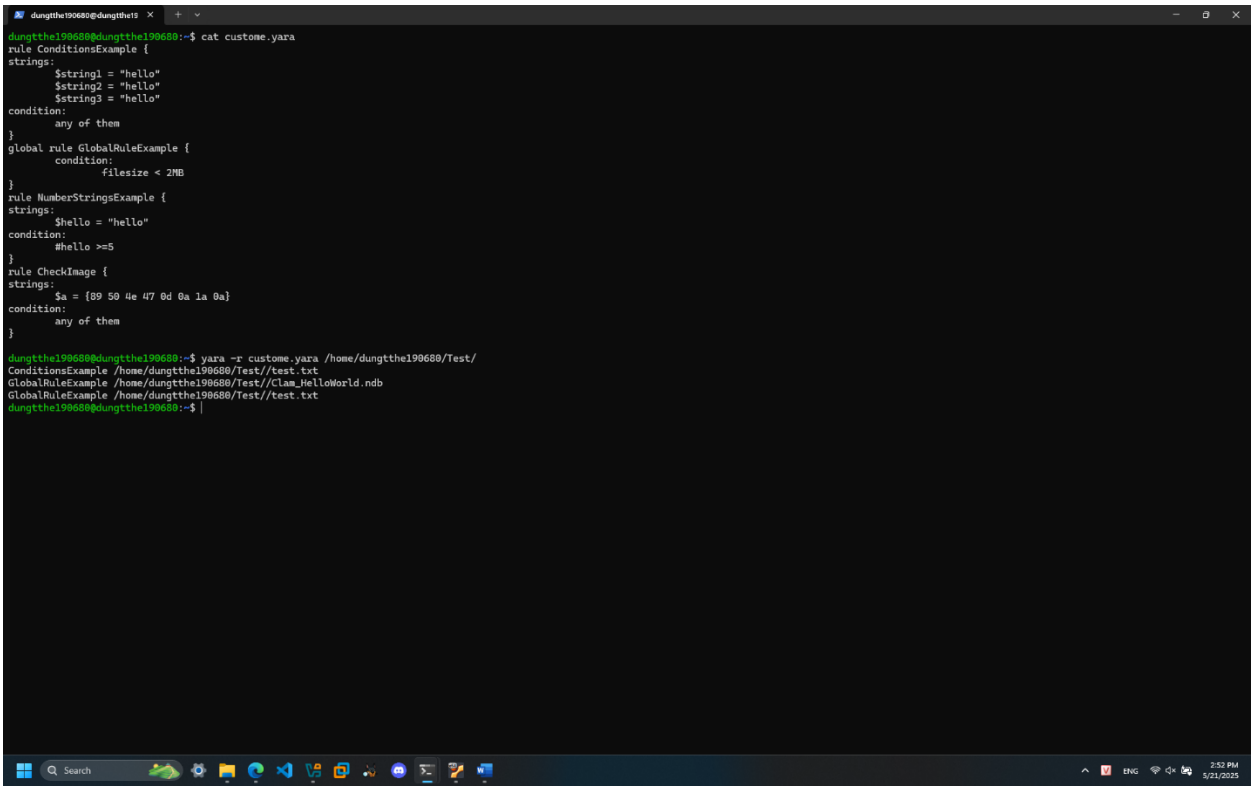
Install YARA -> Install p7zip-full -> Download package.01.ful.7z -> Download file clam_to_yara.py -> Install python2



Convert file clamav to yara -> Start scanning with the yara:

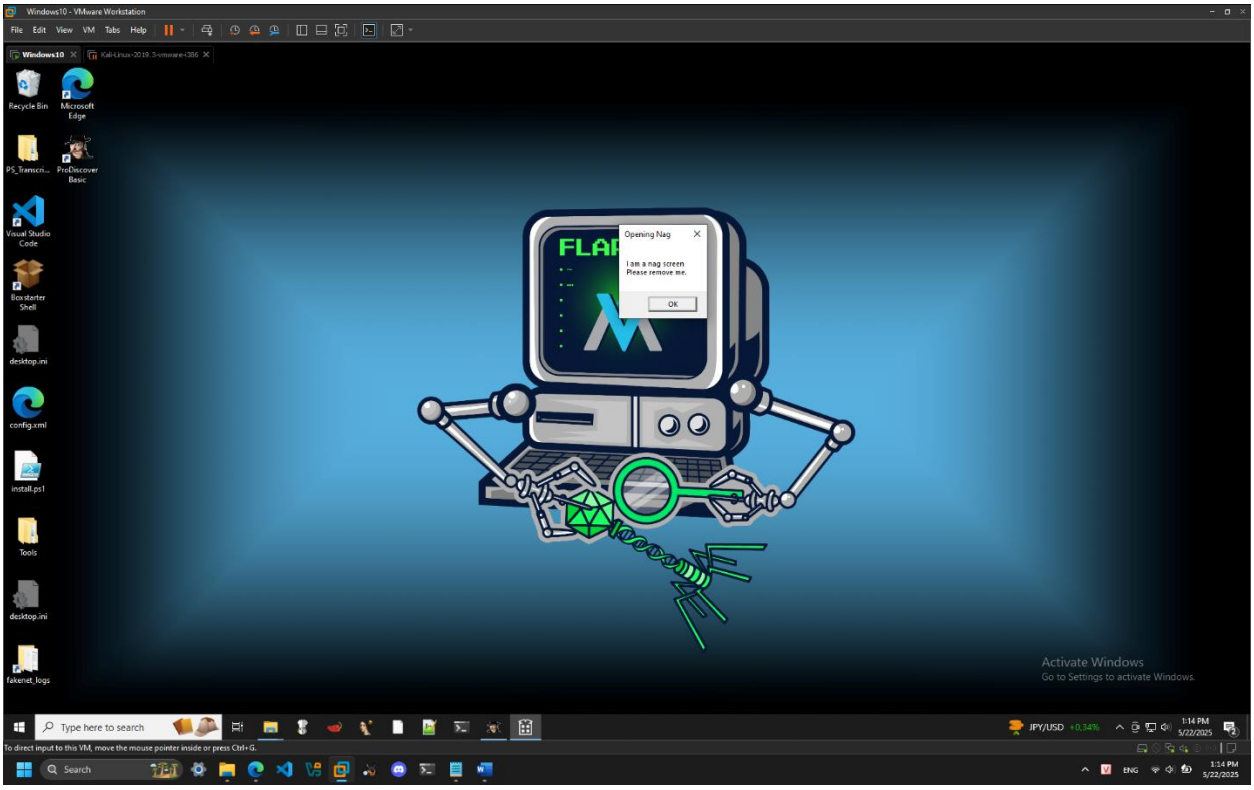


Create a new rule file called custome.yara -> Test yara rules:

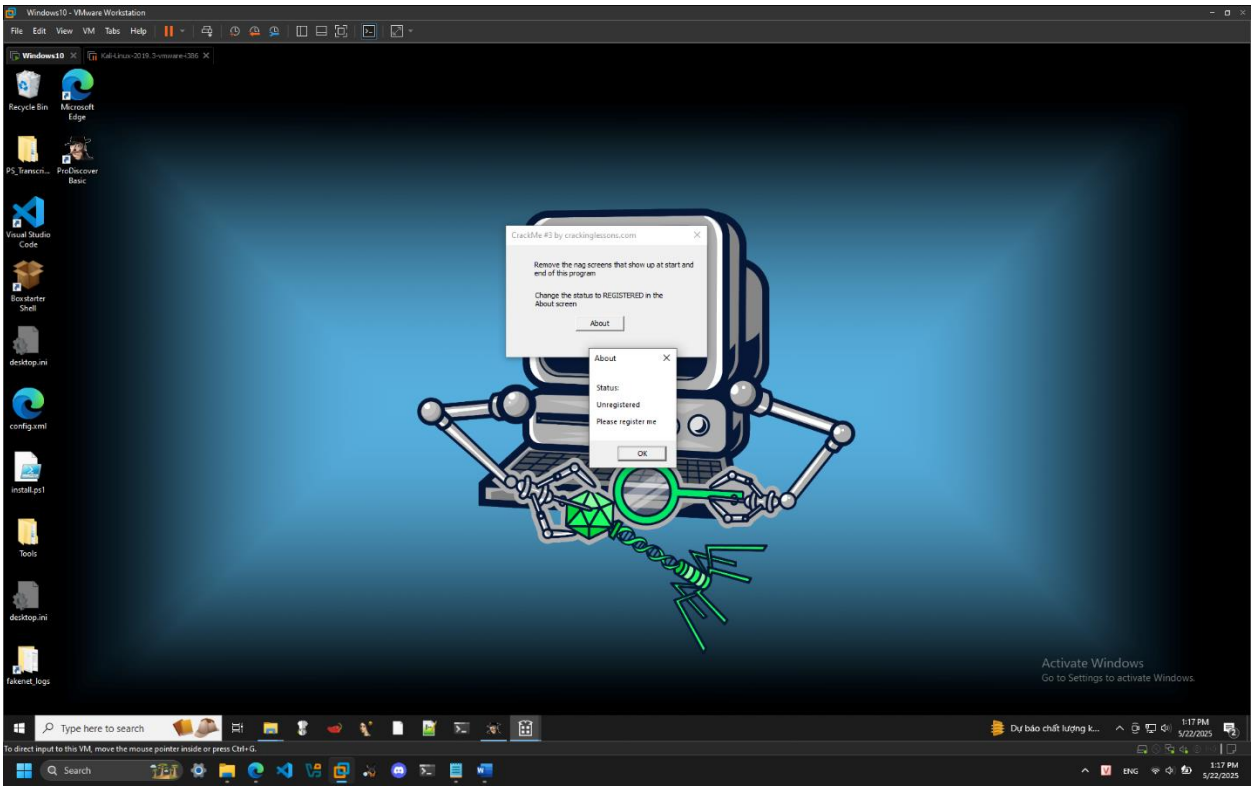


CrackMe #3:

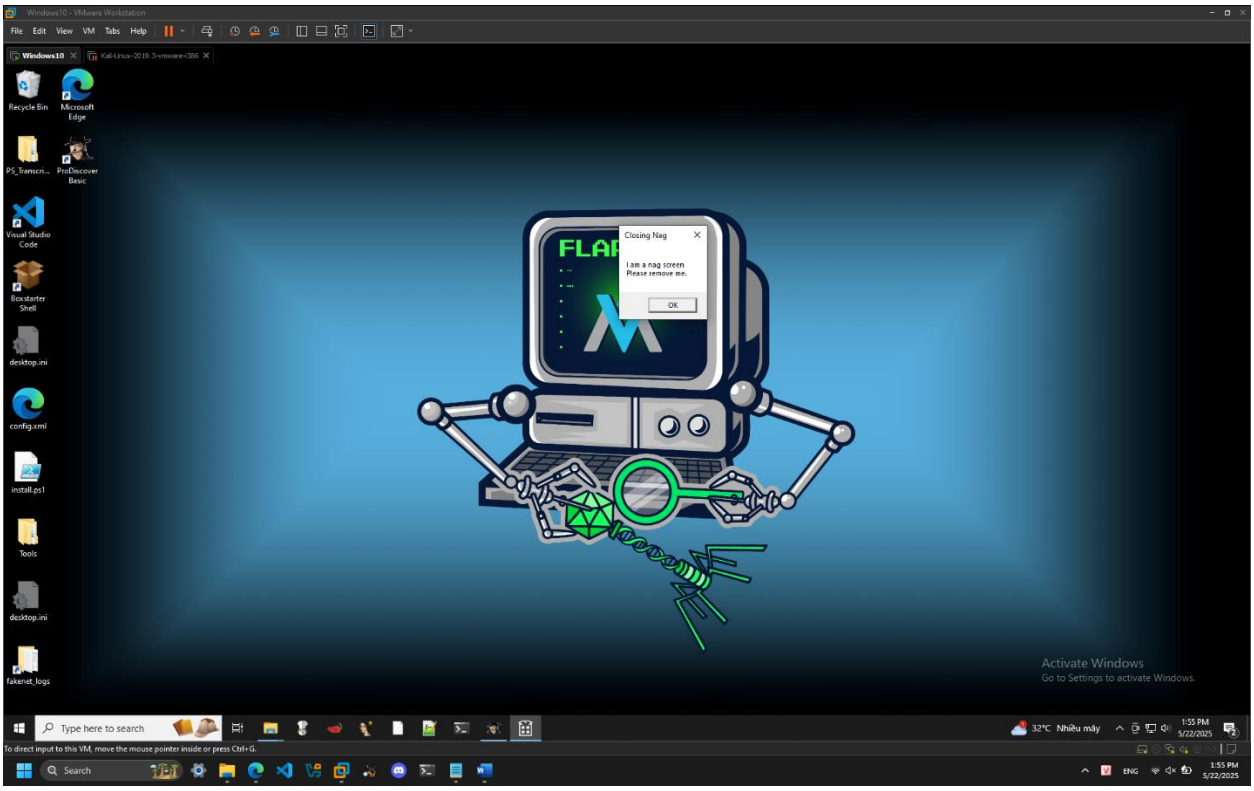
Đầu tiên em thử chạy chương trình và nhận được thông báo có từ khóa “Opening”:



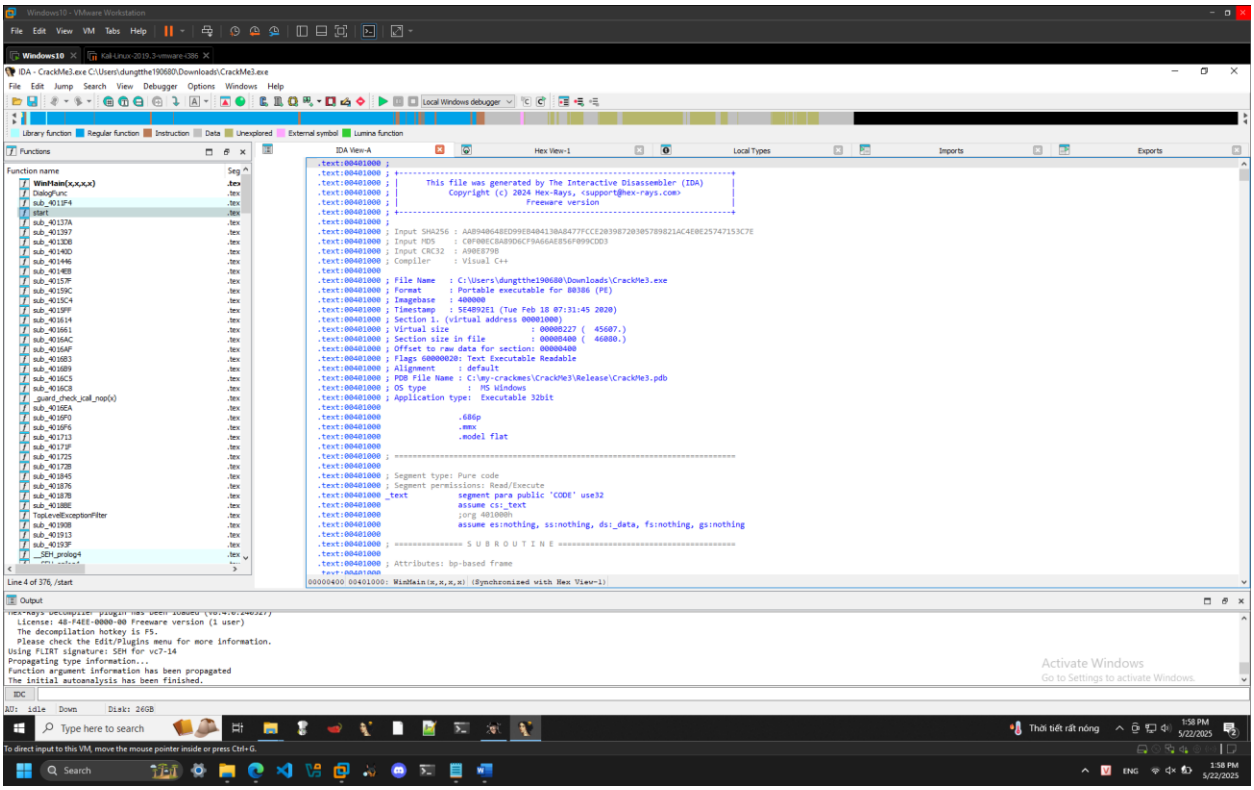
Sau khi tắt thông báo đầu tiên, em nhận được thông báo tiếp theo có từ khóa “Unregistered”:



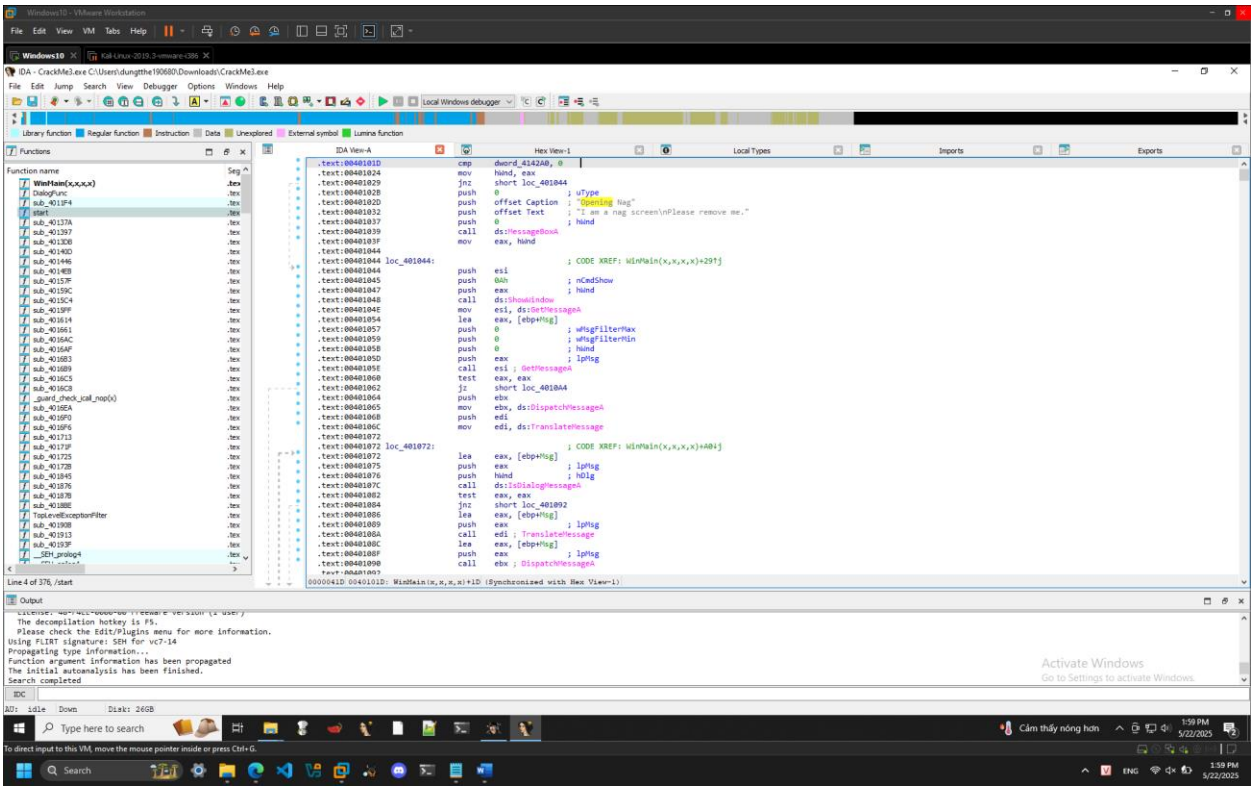
Sau khi tắt thông báo thứ hai, em nhận được thông báo cuối cùng có từ khóa “Closing”:



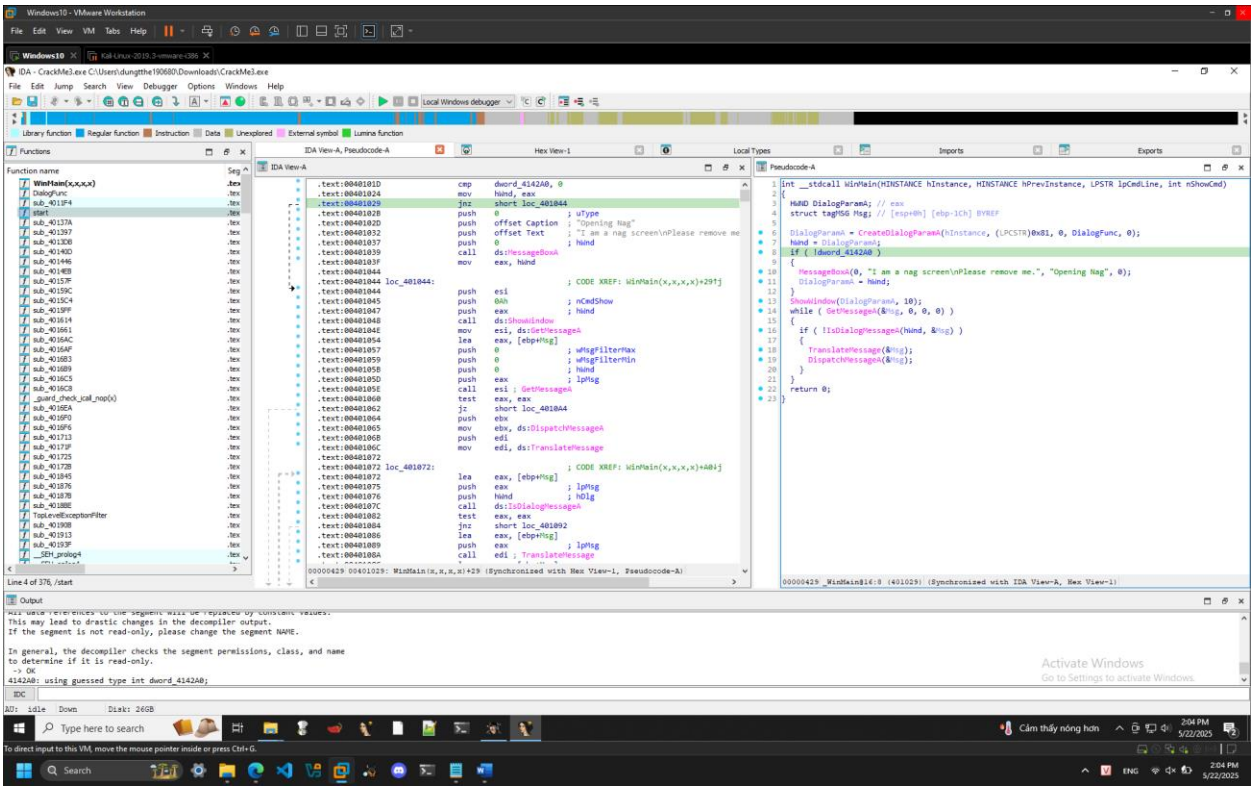
Em mở phần mềm IDA và tiến hành dịch ngược file:



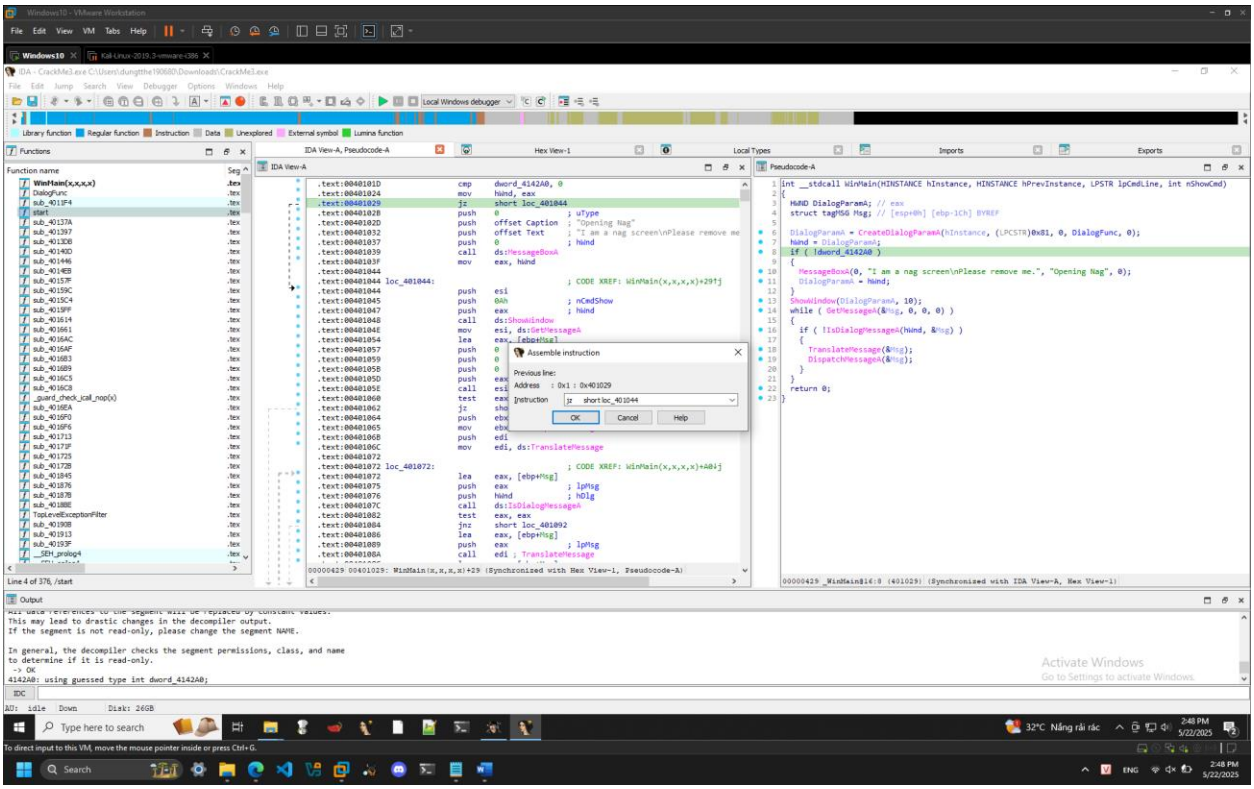
Em search từ khóa “Opening” và được điều hướng đến đoạn code này:



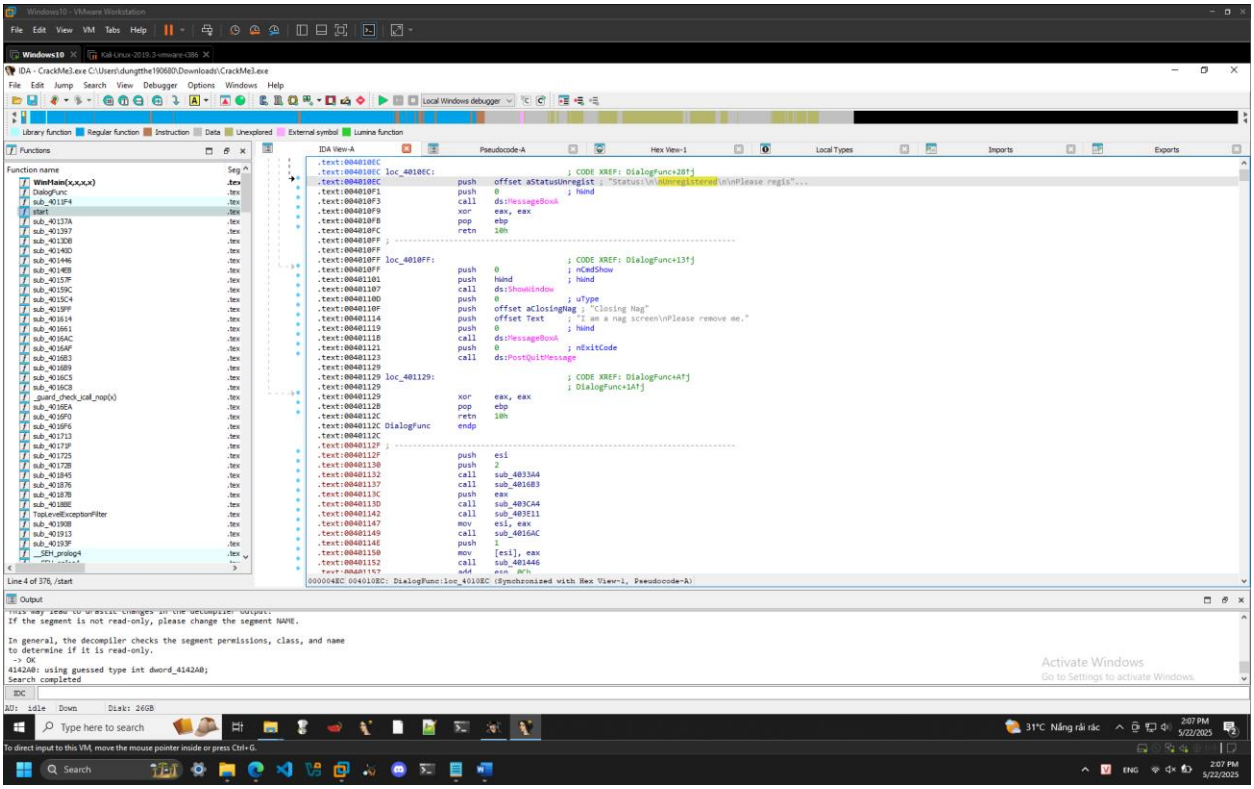
Em bôi đen đoạn code và decompile sang pseudocode thì nhận được đoạn code này:



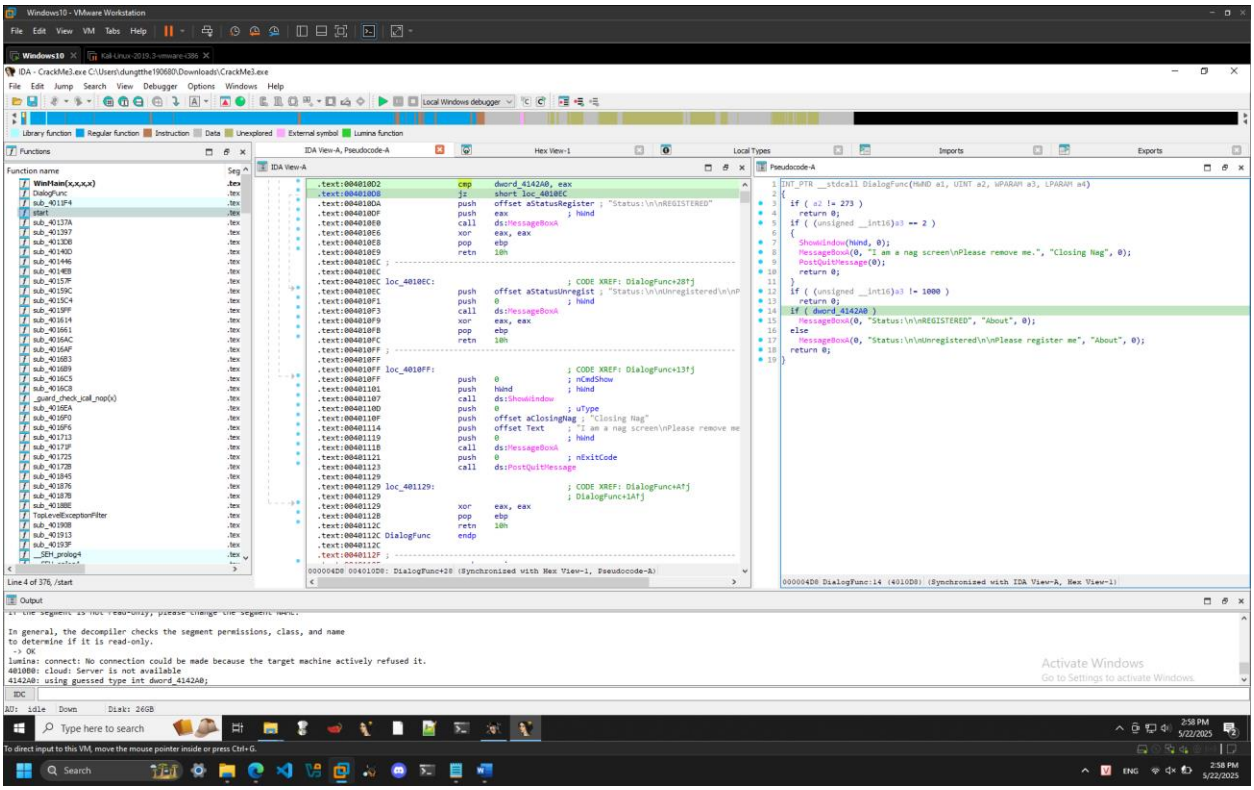
Có thể thấy thông báo đầu tiên được hiển thị nếu giá trị của biến “dword_4142A0” bằng 0. Vì vậy để ngăn thông báo hiển thị em đảo ngược logic đoạn code bằng cách sửa “jnz” thành “jz”:



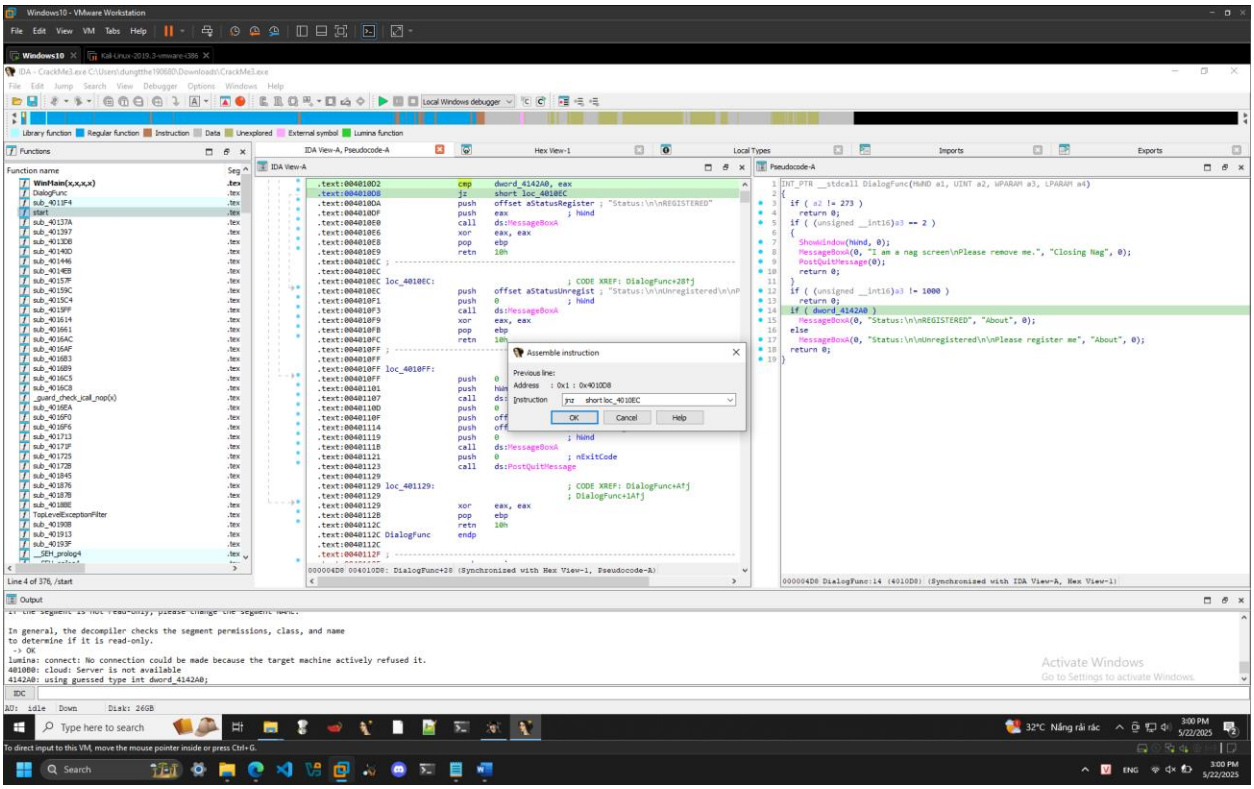
Tiếp theo em search từ khóa “Unregistered” và được điều hướng đến đoạn code này:



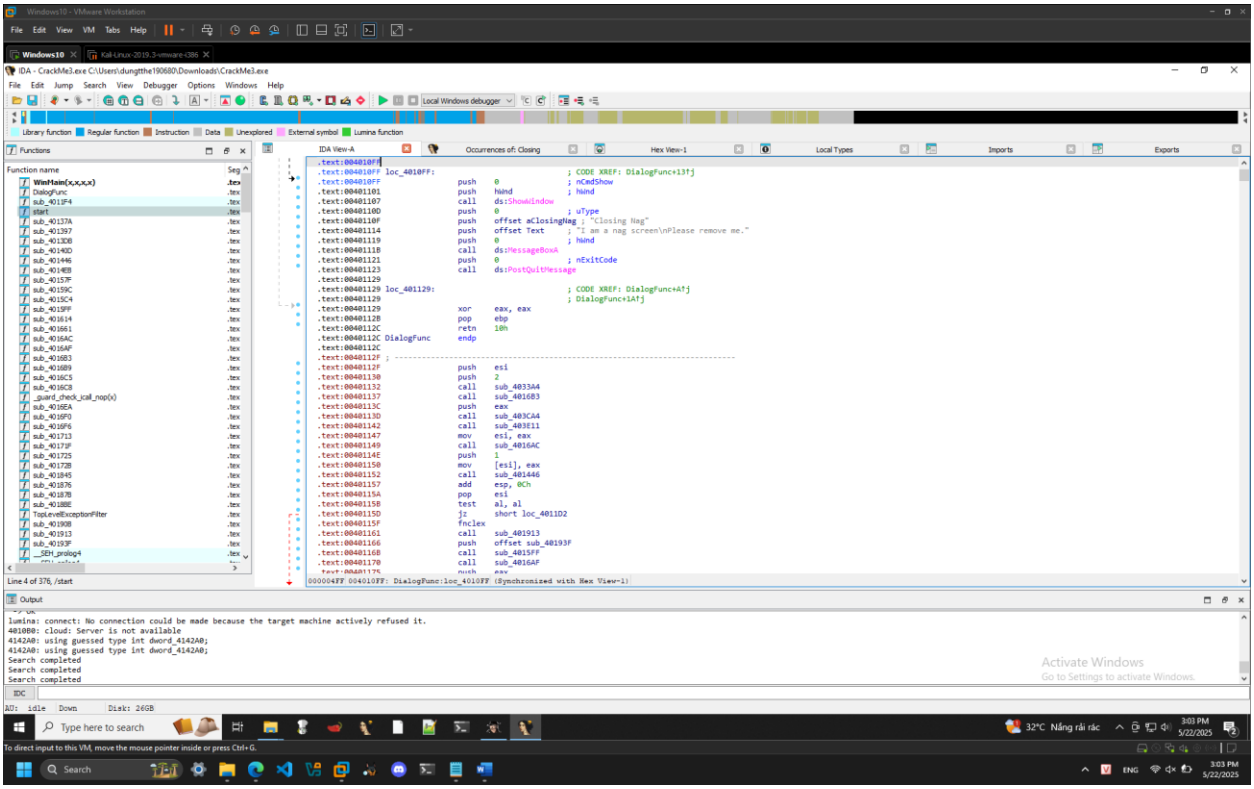
Em bôi đen đoạn code và decompile sang pseudocode thì nhận được đoạn code này:



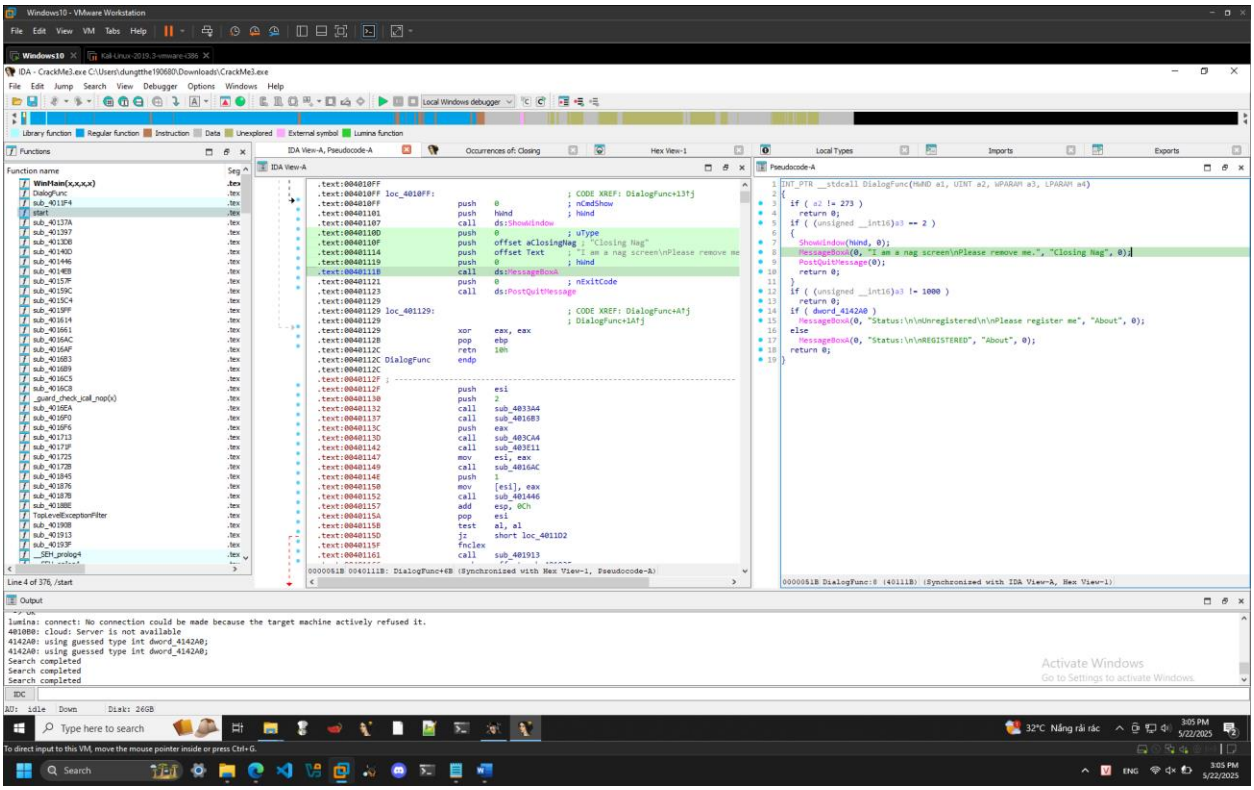
Có thể thấy thông báo chưa đăng ký được hiển thị nếu giá trị của biến “dword_4142A0” bằng 0. Vì vậy để hiển thị thông báo đã đăng ký em đảo ngược logic đoạn code bằng cách sửa “jz” thành “jnz”:



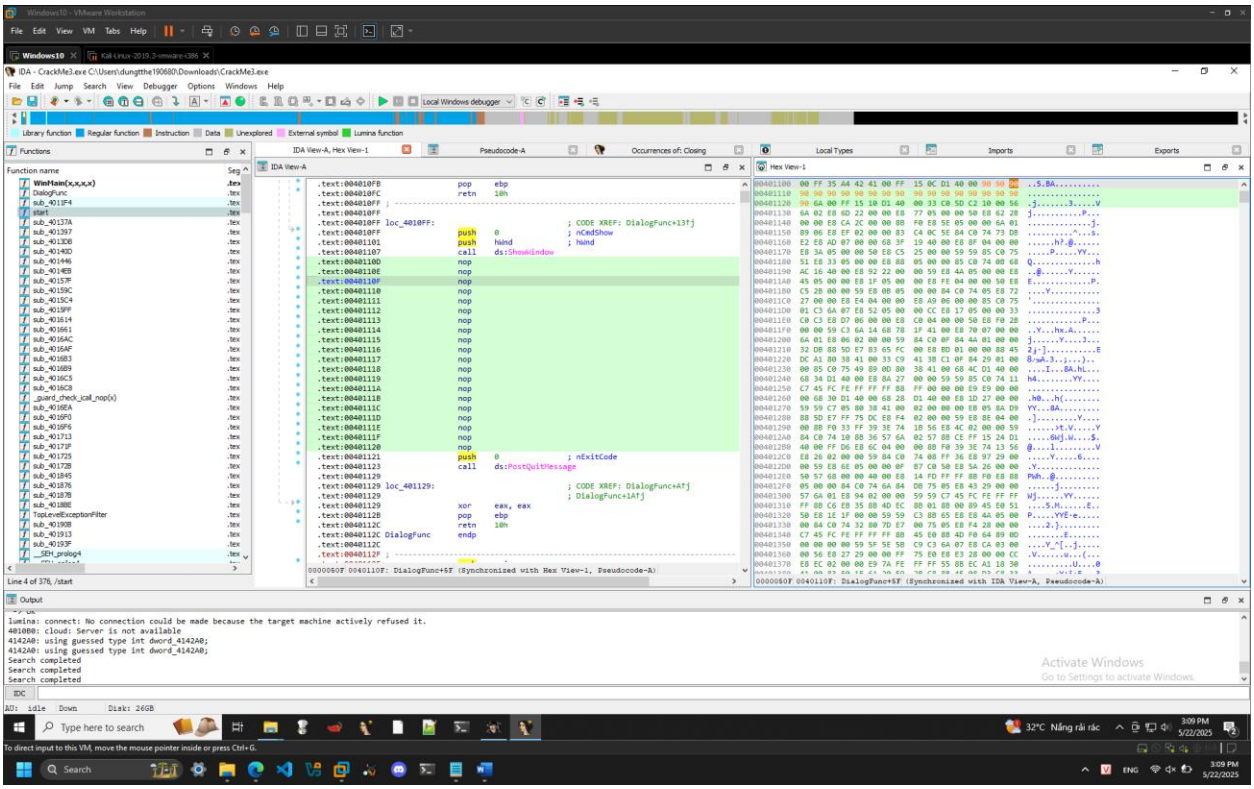
Cuối cùng em search từ khóa “Closing” và được điều hướng đến đoạn code này:



Em bôi đen đoạn code và decompile sang pseudocode thì nhận được đoạn code này:



Có thể thấy thông báo được hiển thị nếu điều kiện của hàm if bằng True, nhưng vì trong hàm if còn gọi các hàm liên quan đến chức năng khác của chương trình nên không thể sửa logic của cả hàm if được. Vì vậy để ngăn thông báo hiển thị em xóa đoạn code gọi hàm hiển thị bằng cách sửa mã hex của chúng thành 90 (nop):



Lưu lại và chạy chương trình sẽ nhận được thông báo đã đăng ký và thông báo khi bắt đầu và kết thúc chương trình sẽ không hiển thị: