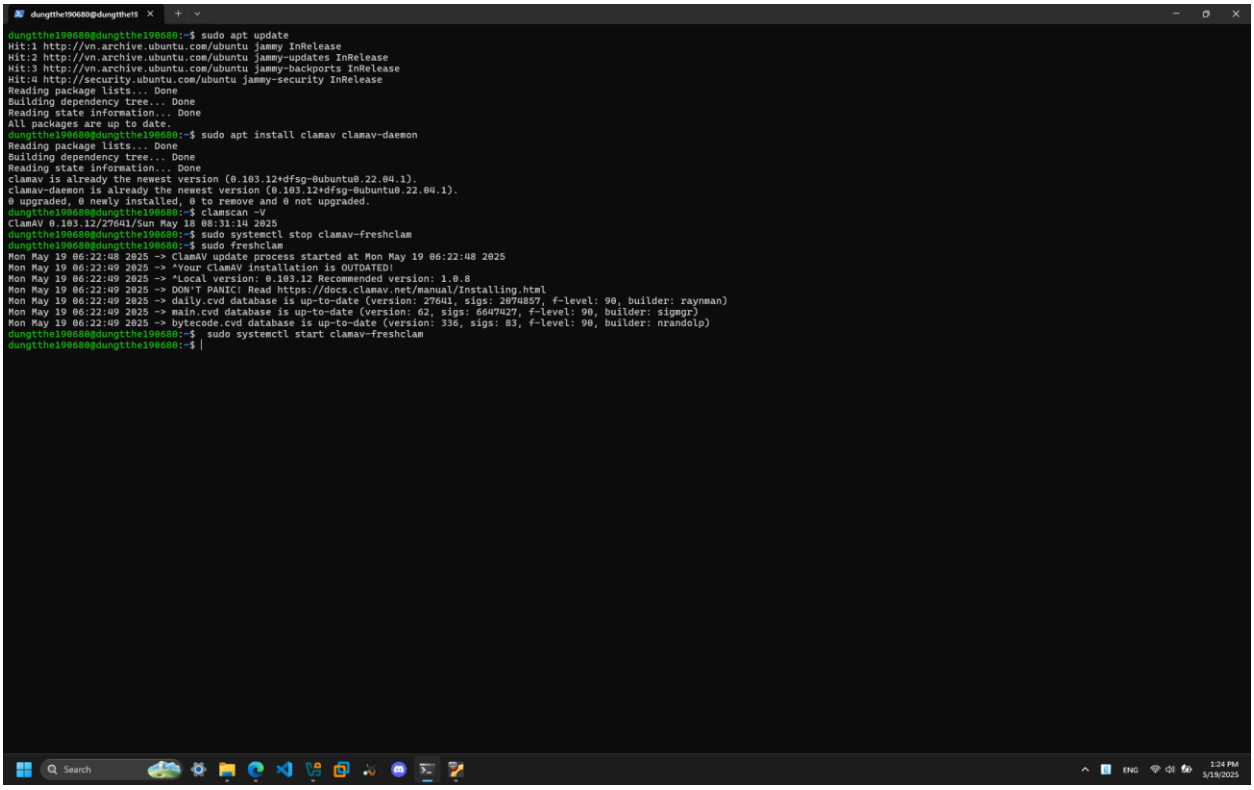
Họ và tên: Trần Trí Dũng

Mã số sinh viên: HE190680

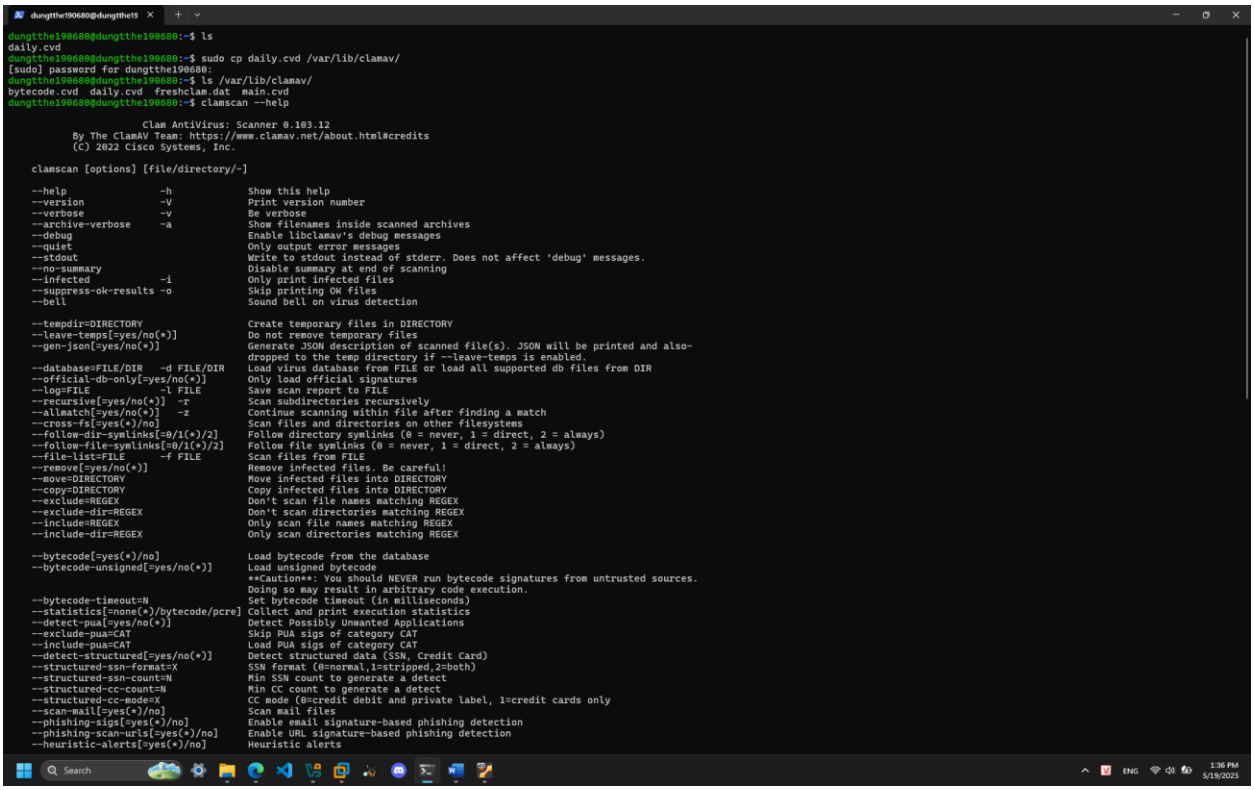
Lớp: IA1901

Lab 2:

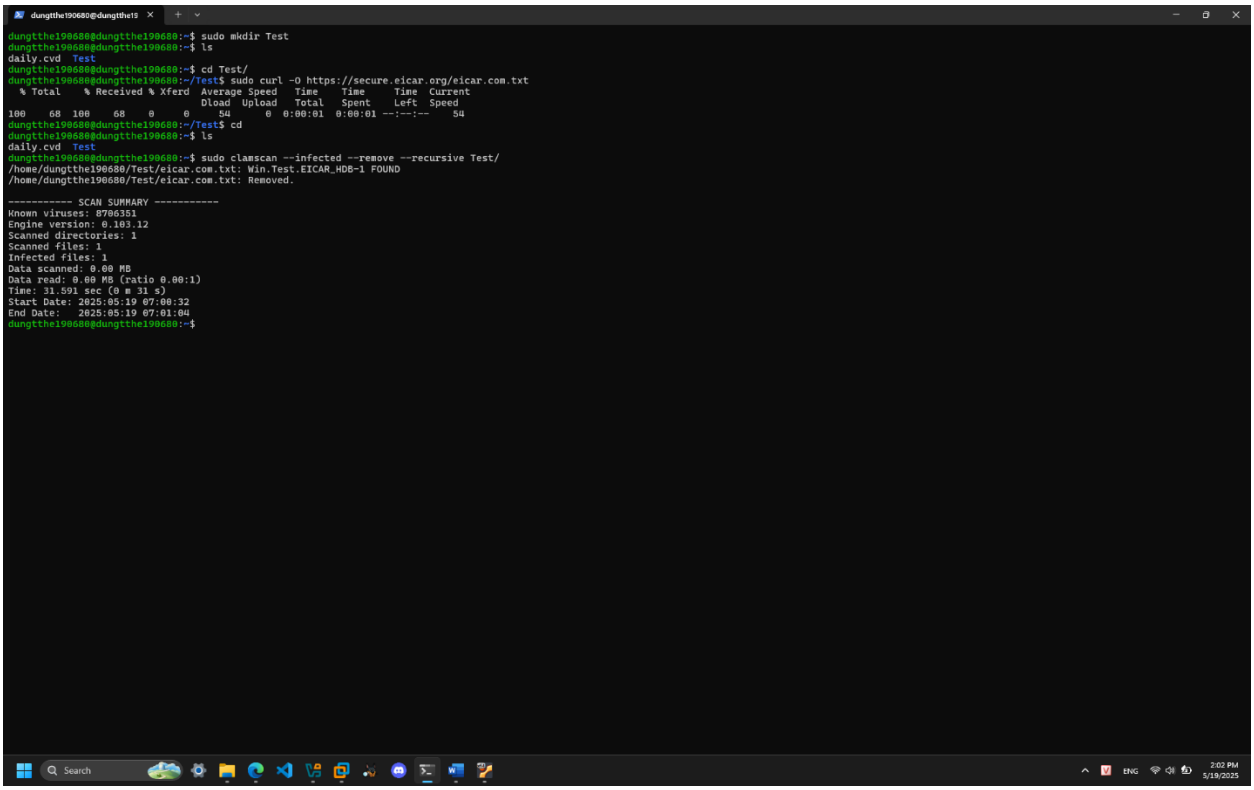
Update the Repository -> Install ClamAV -> Verify ClamAV -> Download Updates Using freshclam:

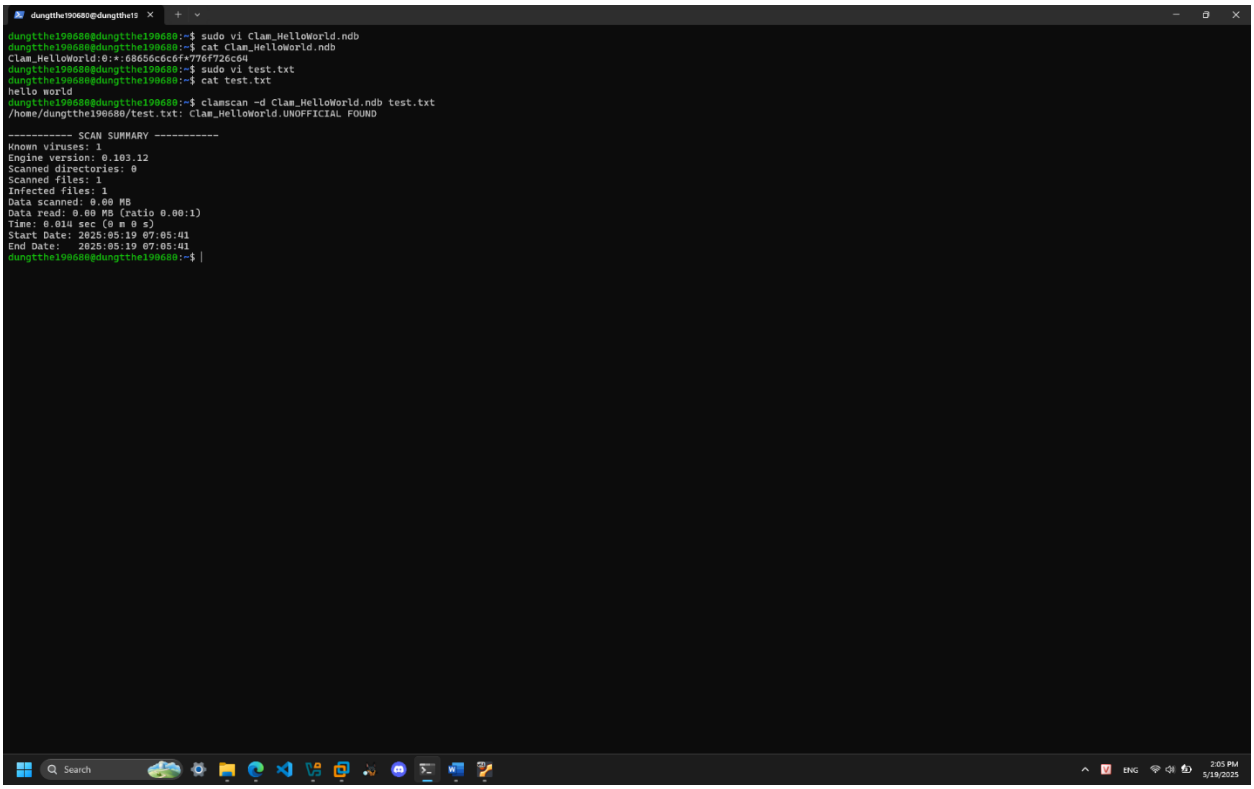


Download Updates Using Official Website:



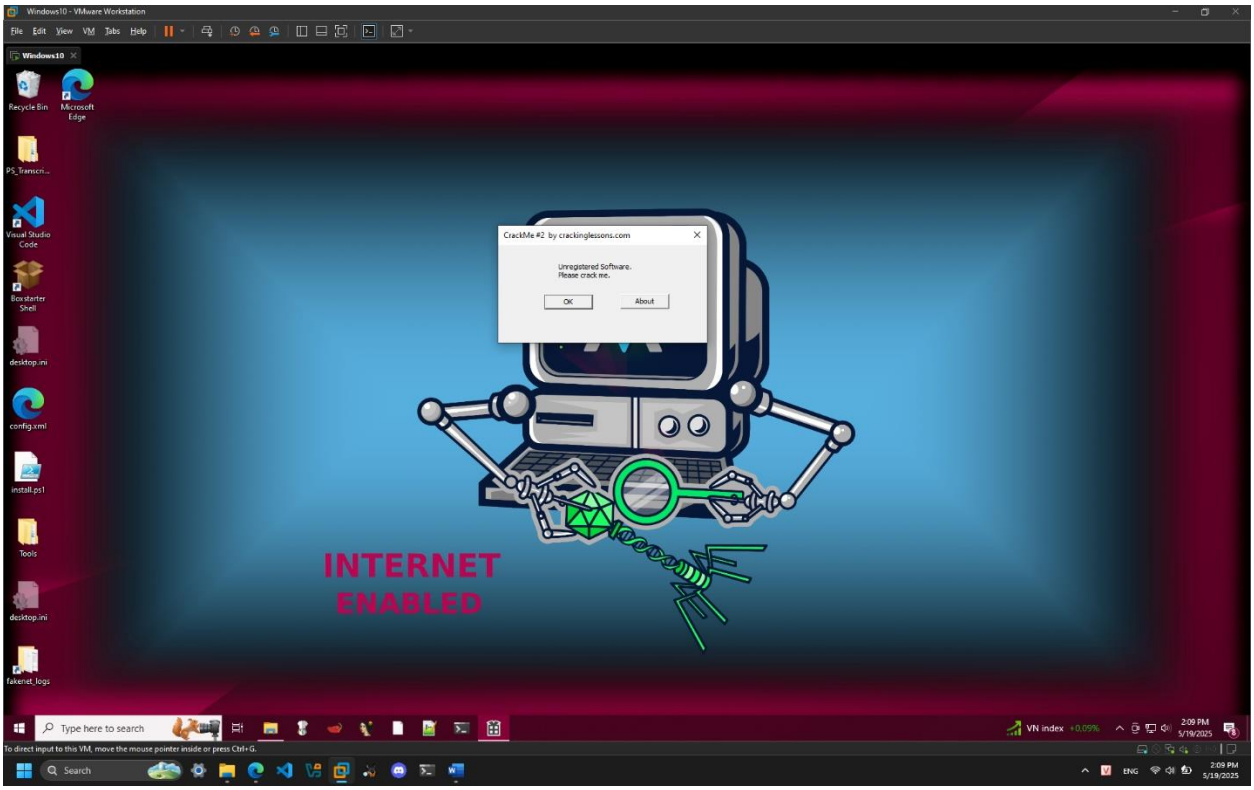
Scan a Directory:



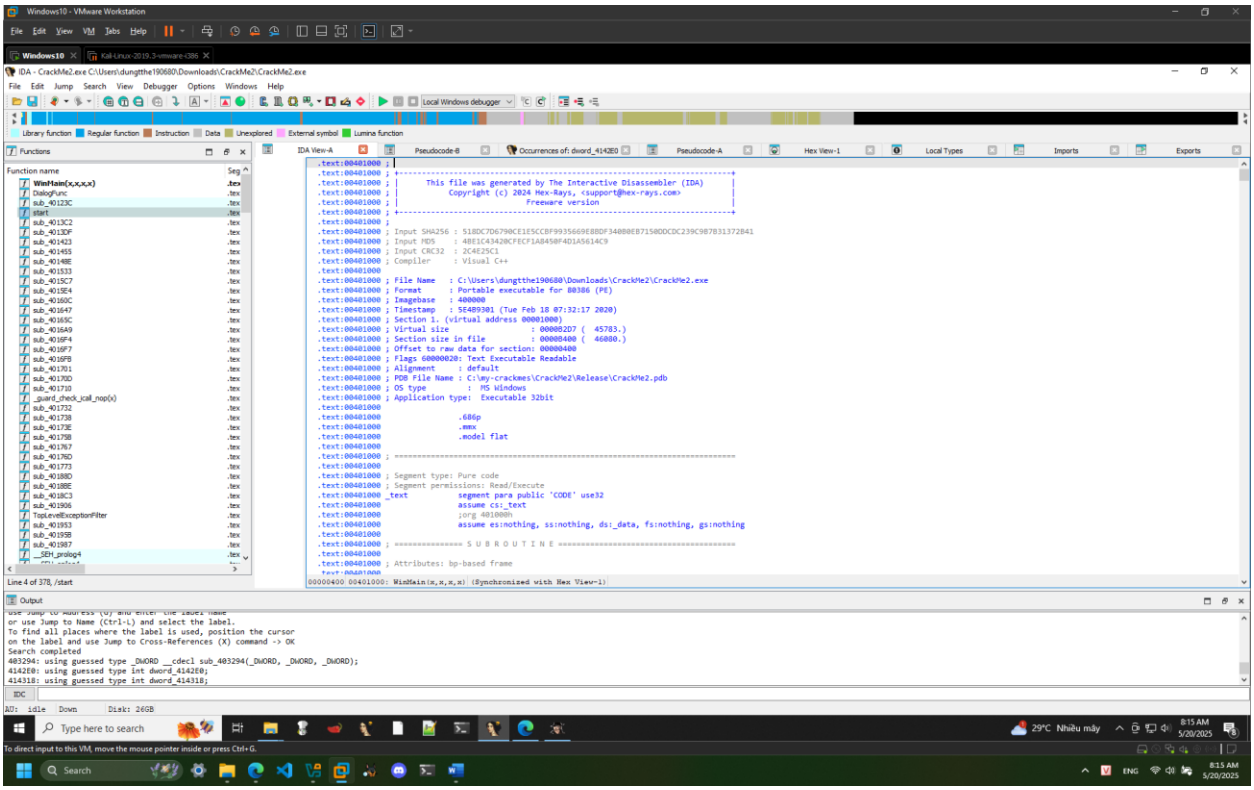


CrackMe #2

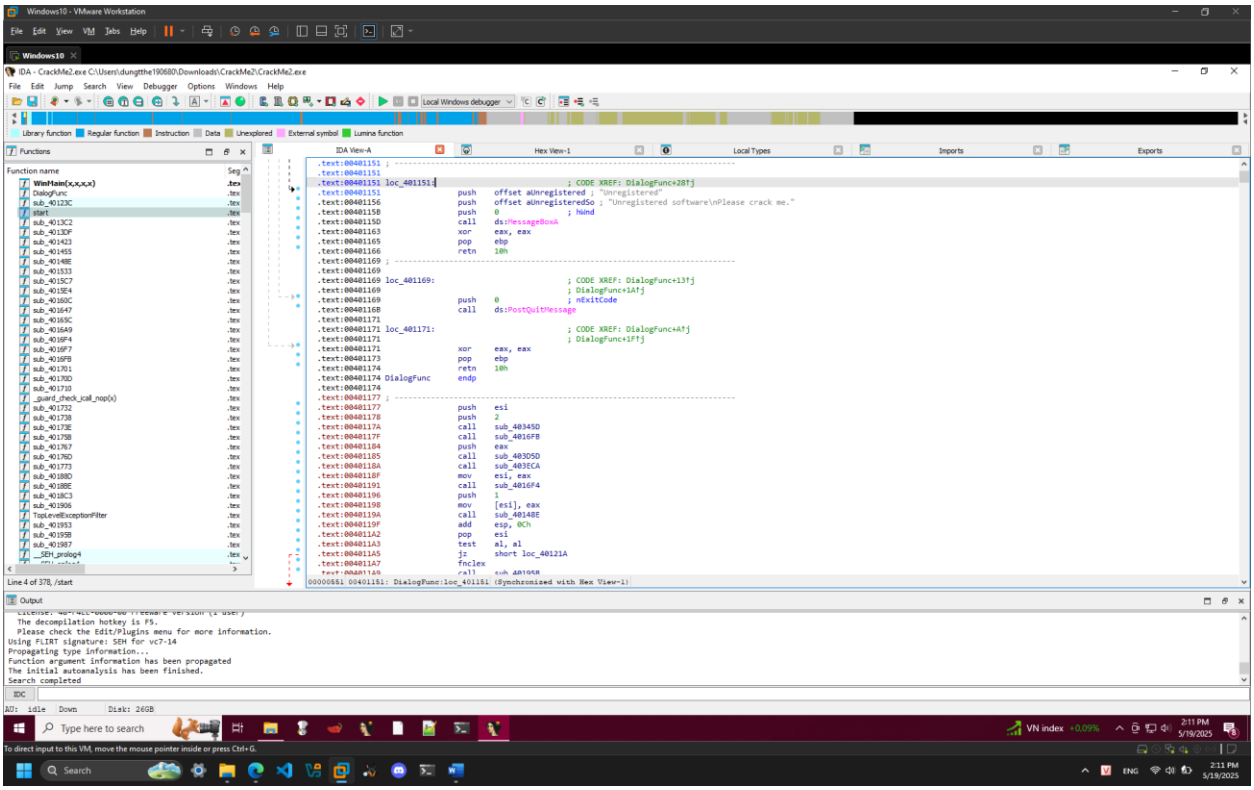
Đầu tiên em thử chạy chương trình và nhận được thông báo có từ khóa “Unregistered”:



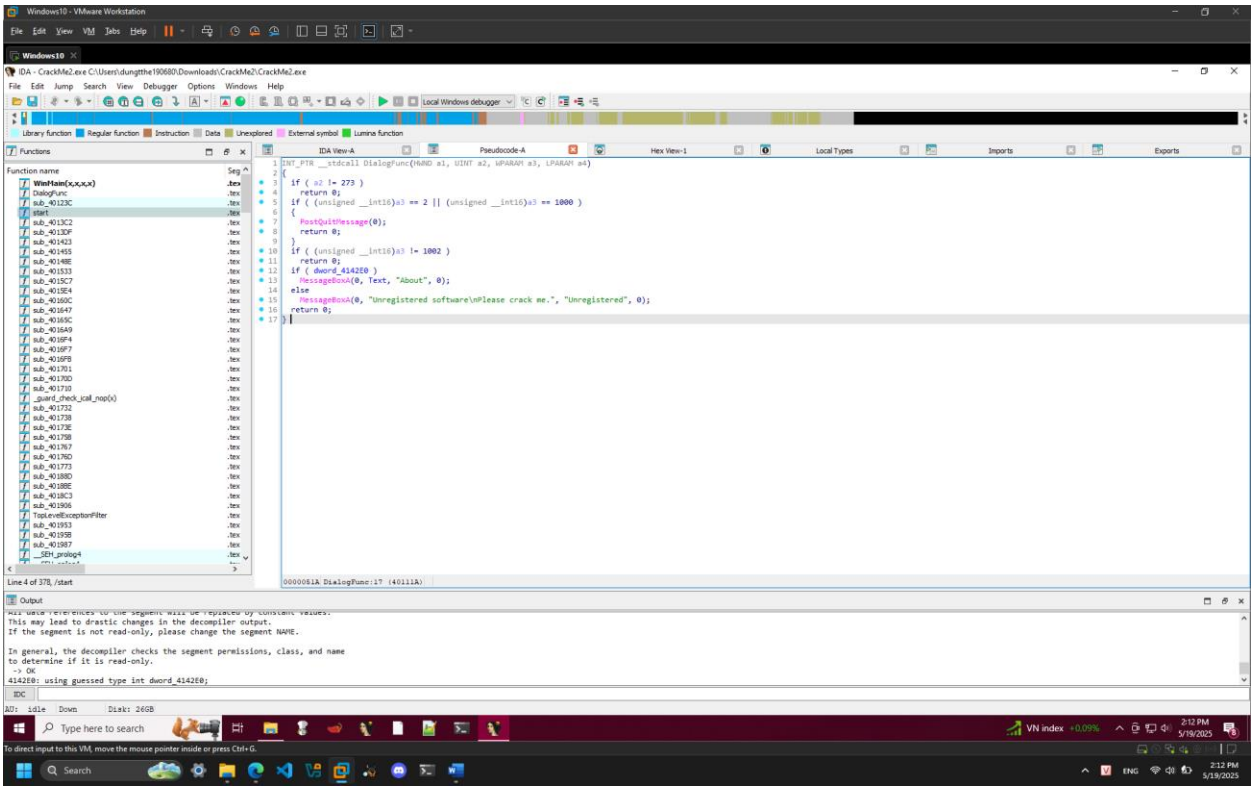
Sau đó em mở phần mềm IDA và tiến hành dịch ngược file:



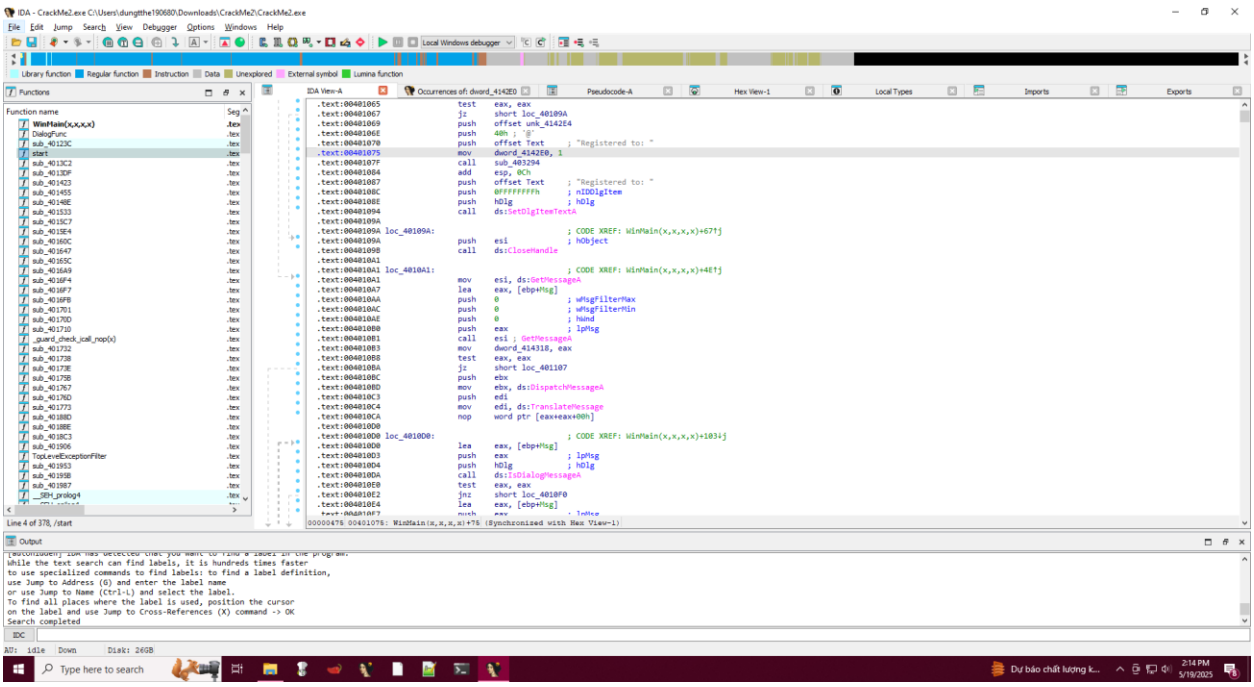
Em search từ khóa “Unregistered” và được điều hướng đến đoạn code này:



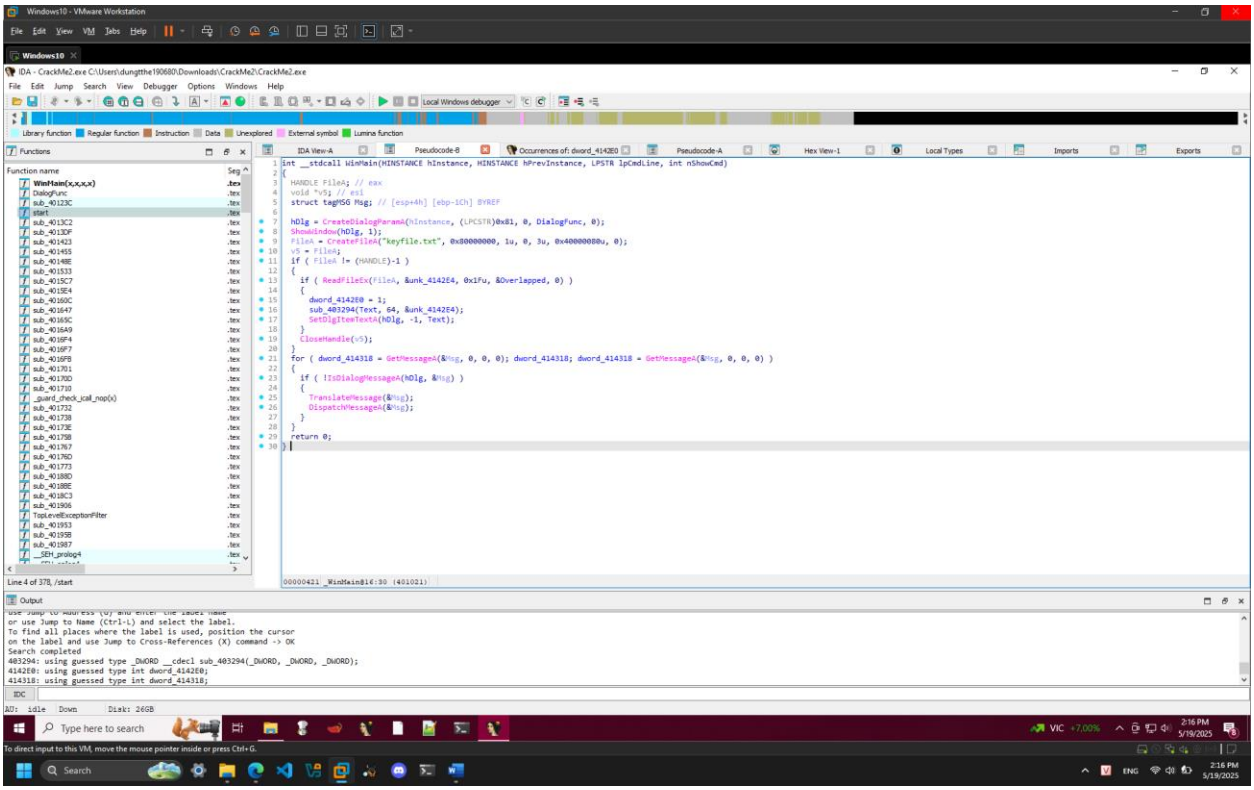
Em bôi đen đoạn code và decompile sang pseudocode thì nhận được đoạn code này:



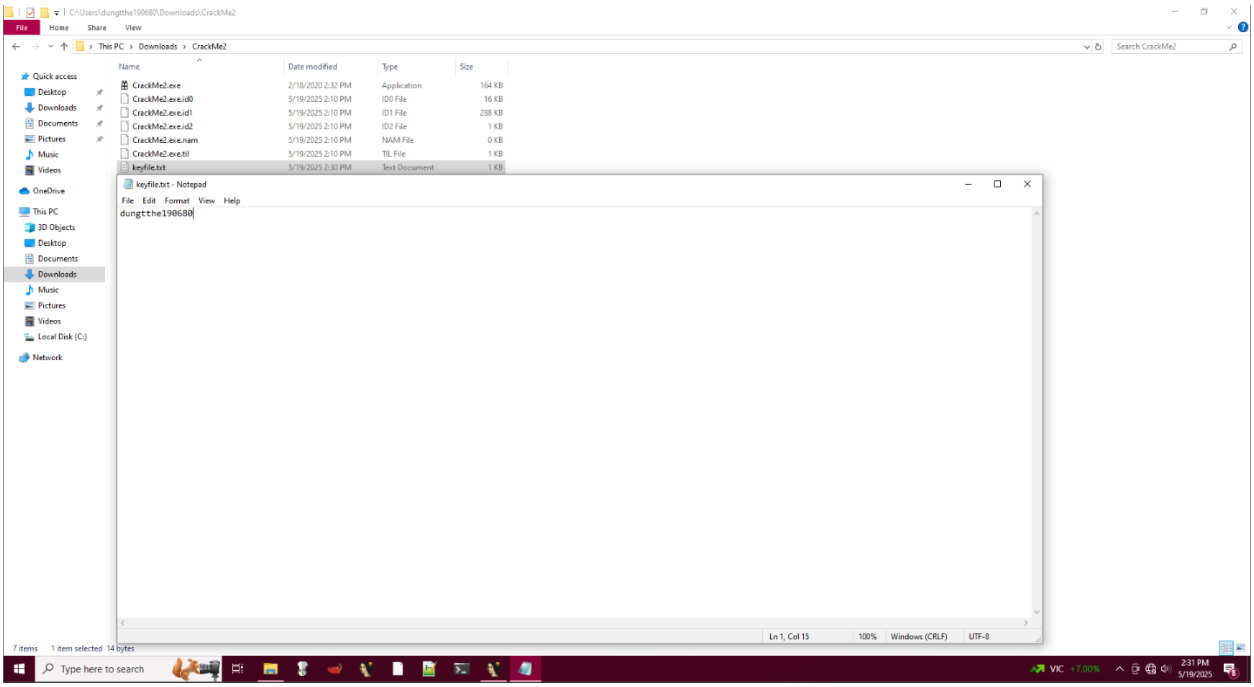
Có thể thấy nội dung được hiển thị trong thông báo nằm trong một hàm if được quyết định bởi giá trị của biến “dword_4142E0”. Vì vậy em tiếp tục search từ khóa “dword_4142E0” và được điều hướng đến đoạn code này:



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



Từ đoạn code trên suy ra giá trị của biến “dword_4142E0” được xác định bởi việc có thể đọc được dữ liệu từ file “keyfile.txt” hay không và giá trị đọc được trả về biến “Text”. Vì vậy để hiển thị tên người đăng ký là “dungtthe190680”, em tạo file “keyfile.txt” trong cùng thư mục với chương trình:



Chạy lại chương trình sẽ nhận được kết quả đã đăng ký thành công: