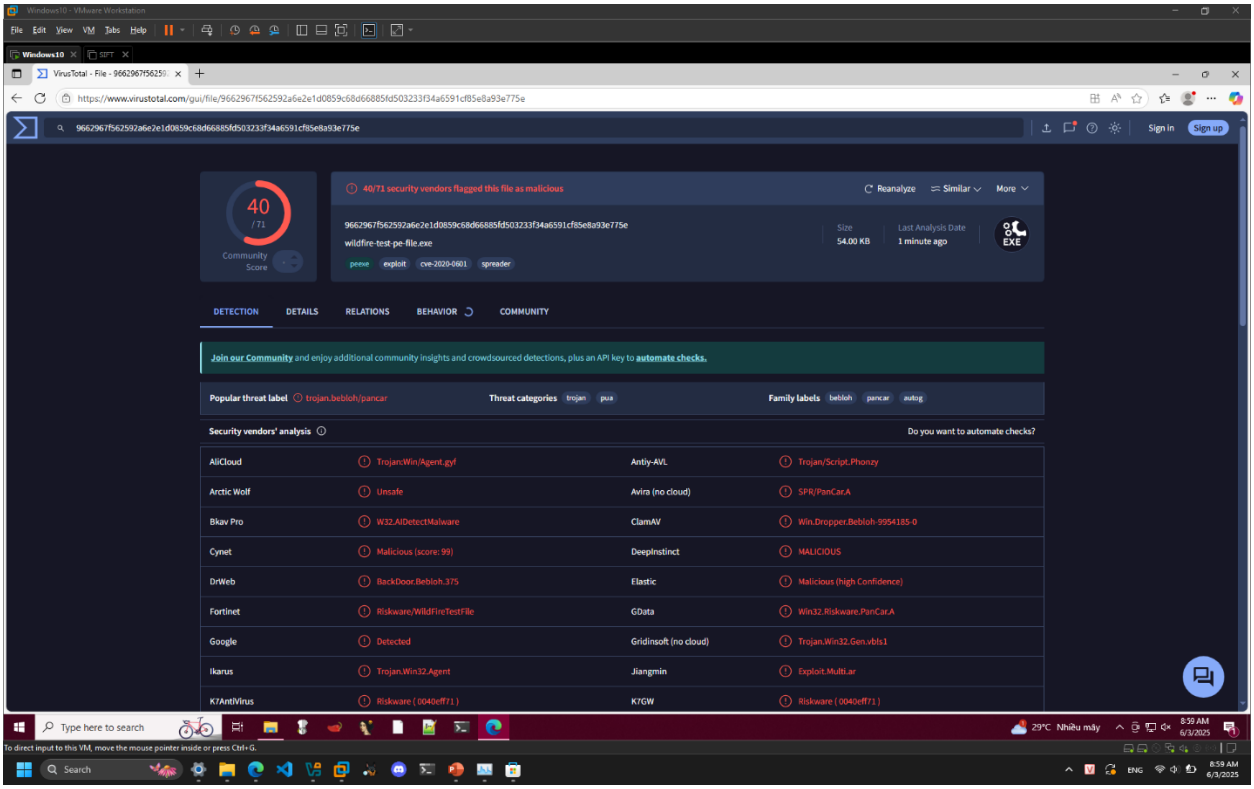
Họ và tên: Trần Trí Dũng

MSSV: HE190680

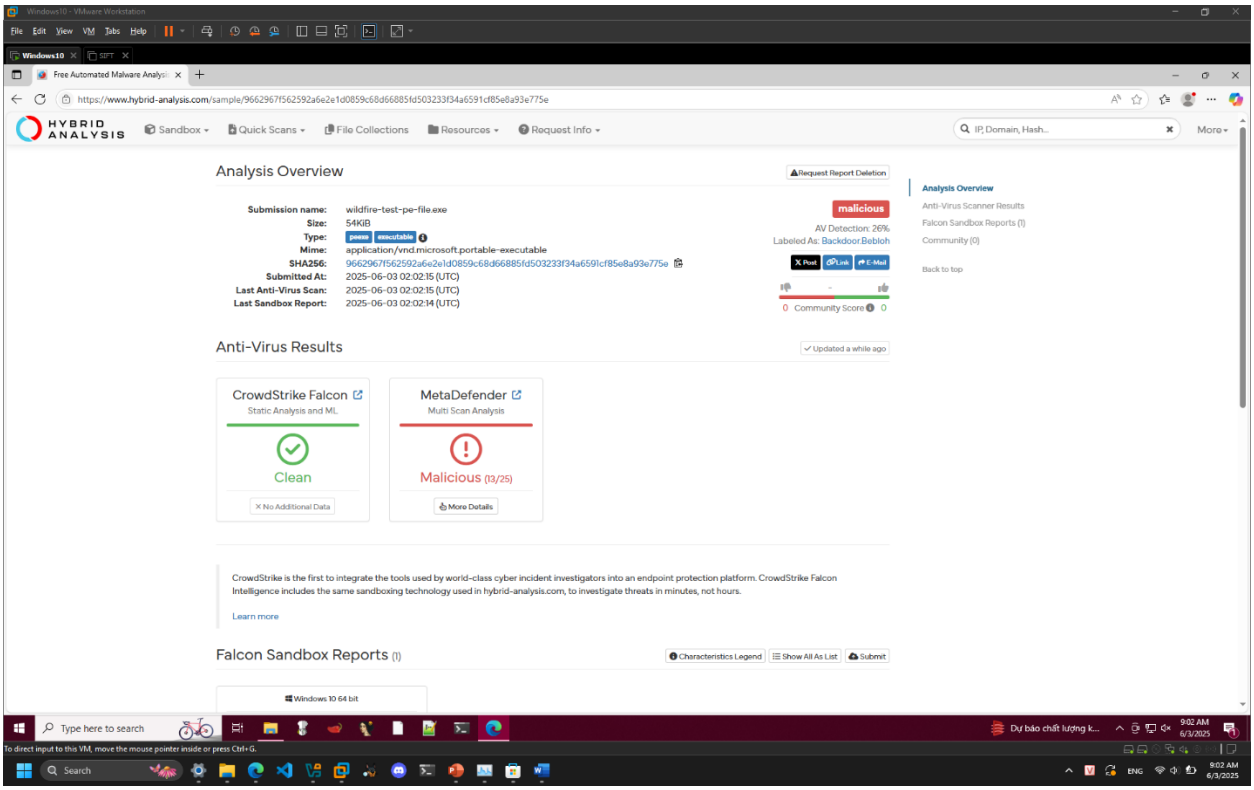
Lớp: IA1901

Lab 6:

Upload VirusTotal:

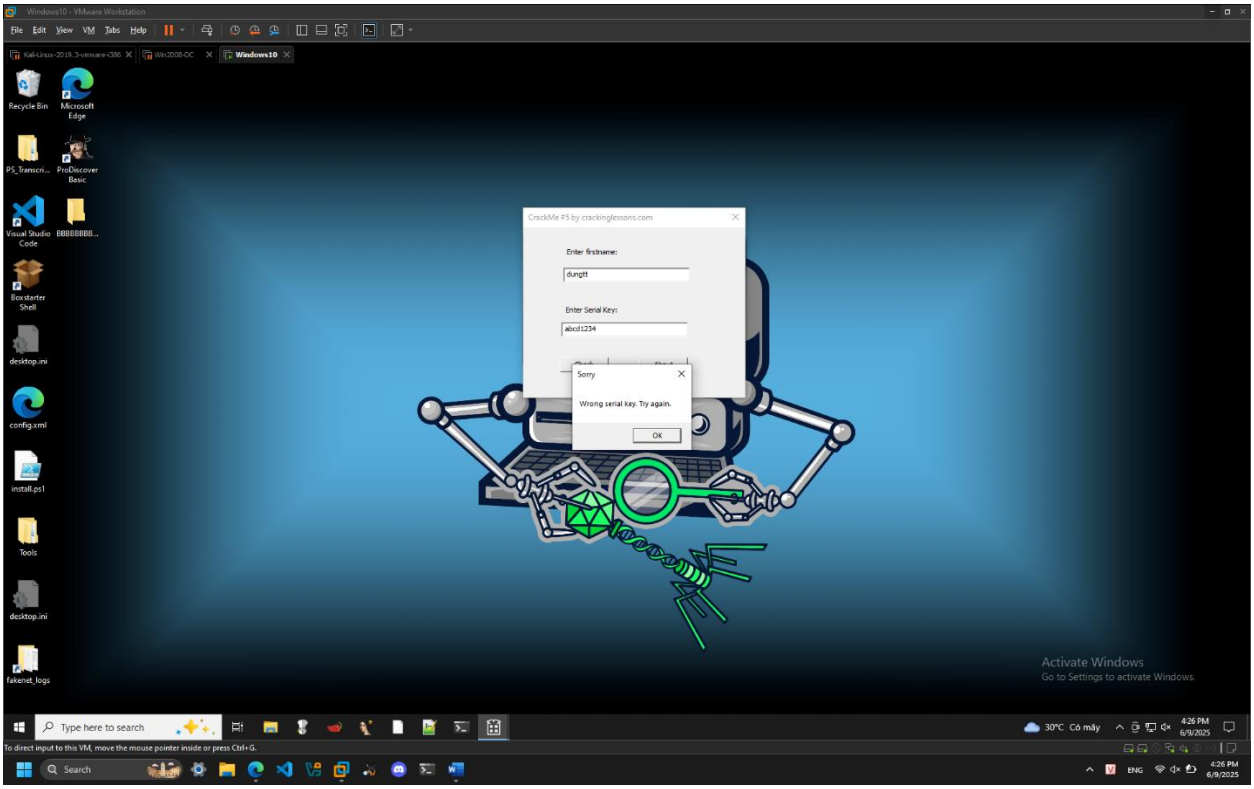


Upload hybrid-analysis:

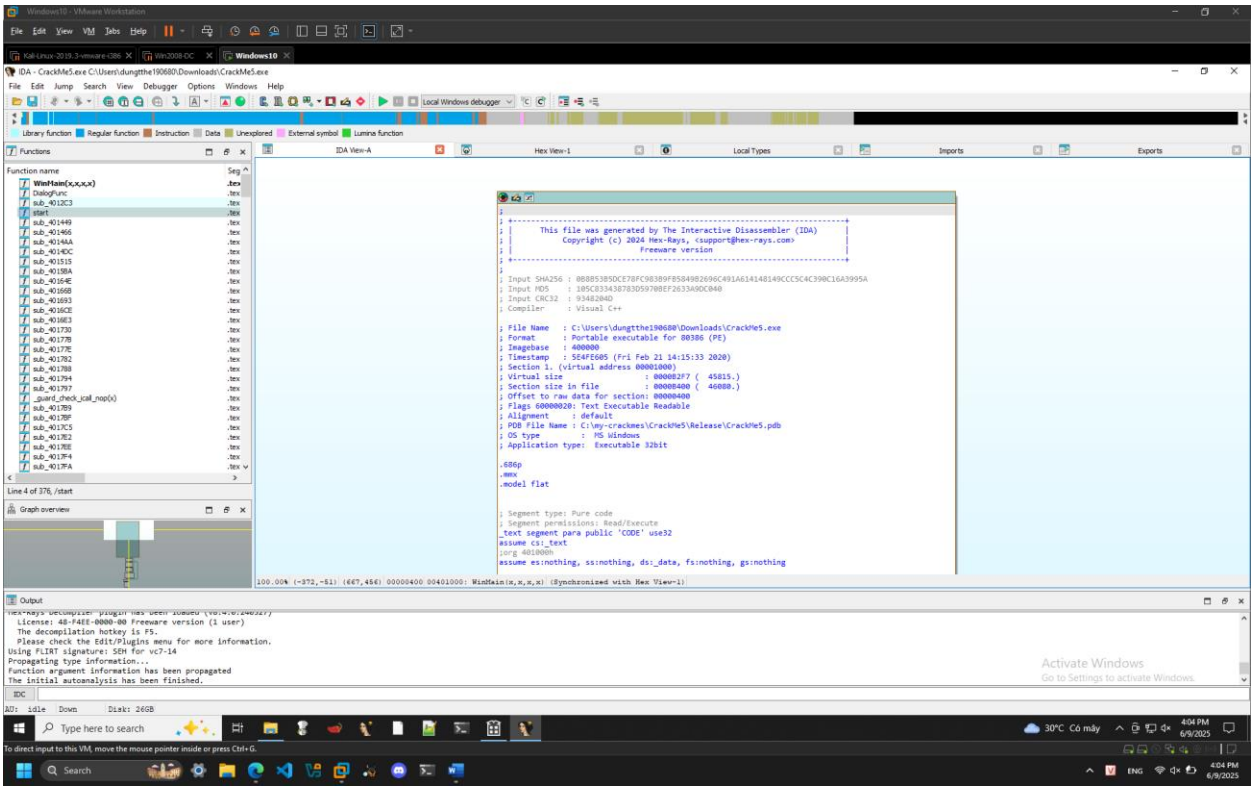


CrackMe #5:

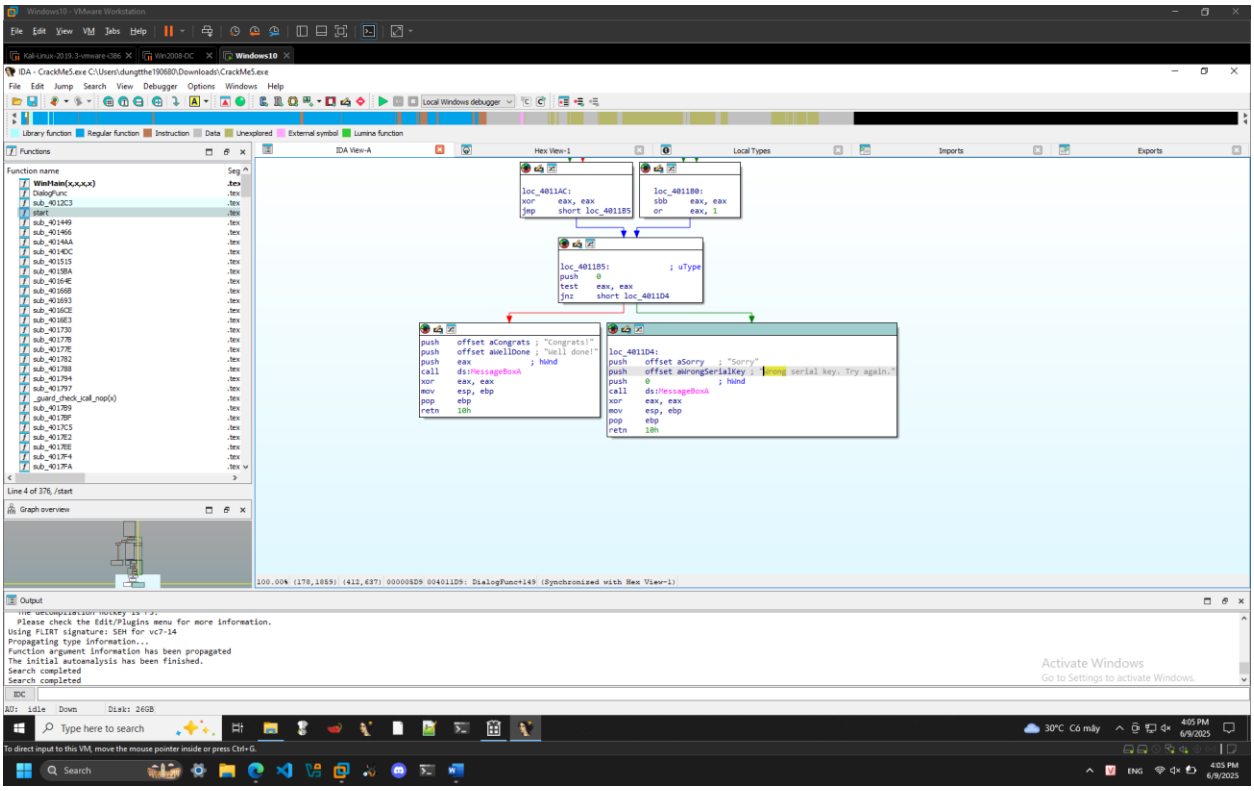
Đầu tiên em thử chạy chương trình và nhận được thông báo có từ khóa “Wrong”:



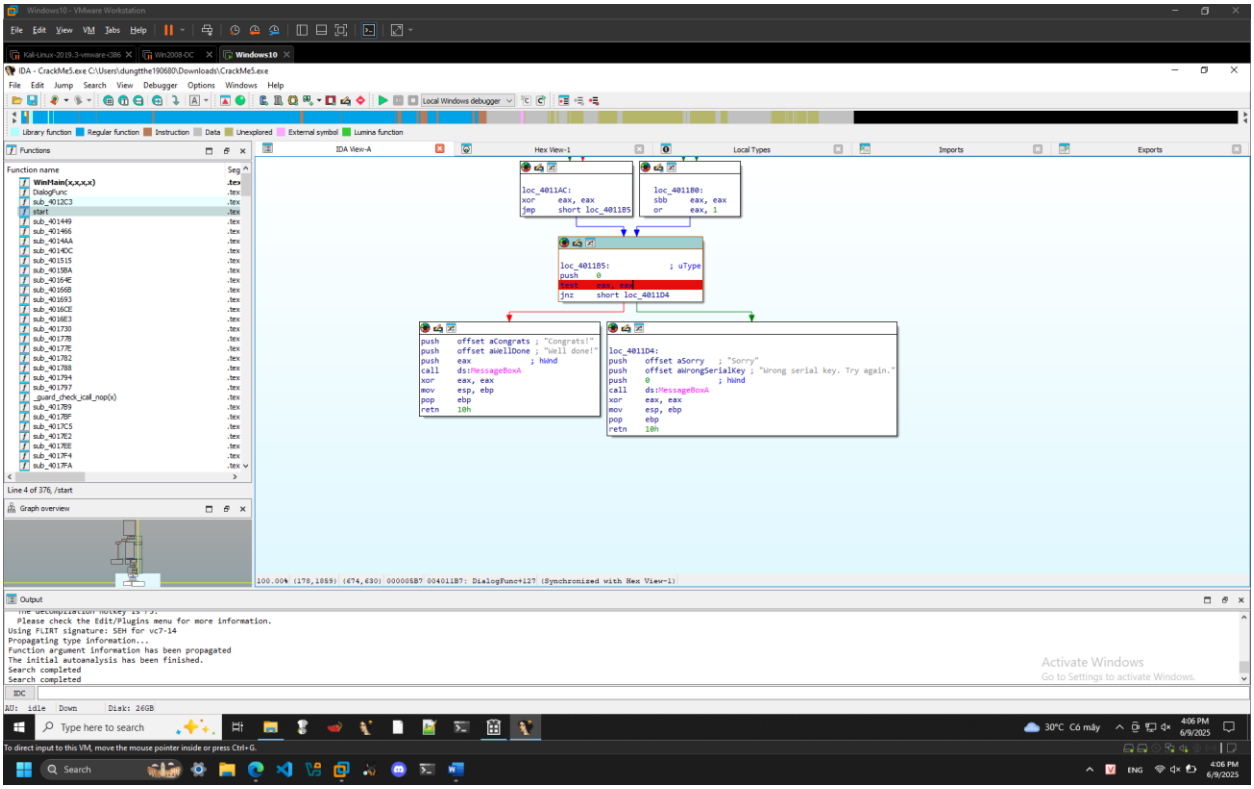
Sau đó em mở phần mềm IDA và tiến hành dịch ngược file:



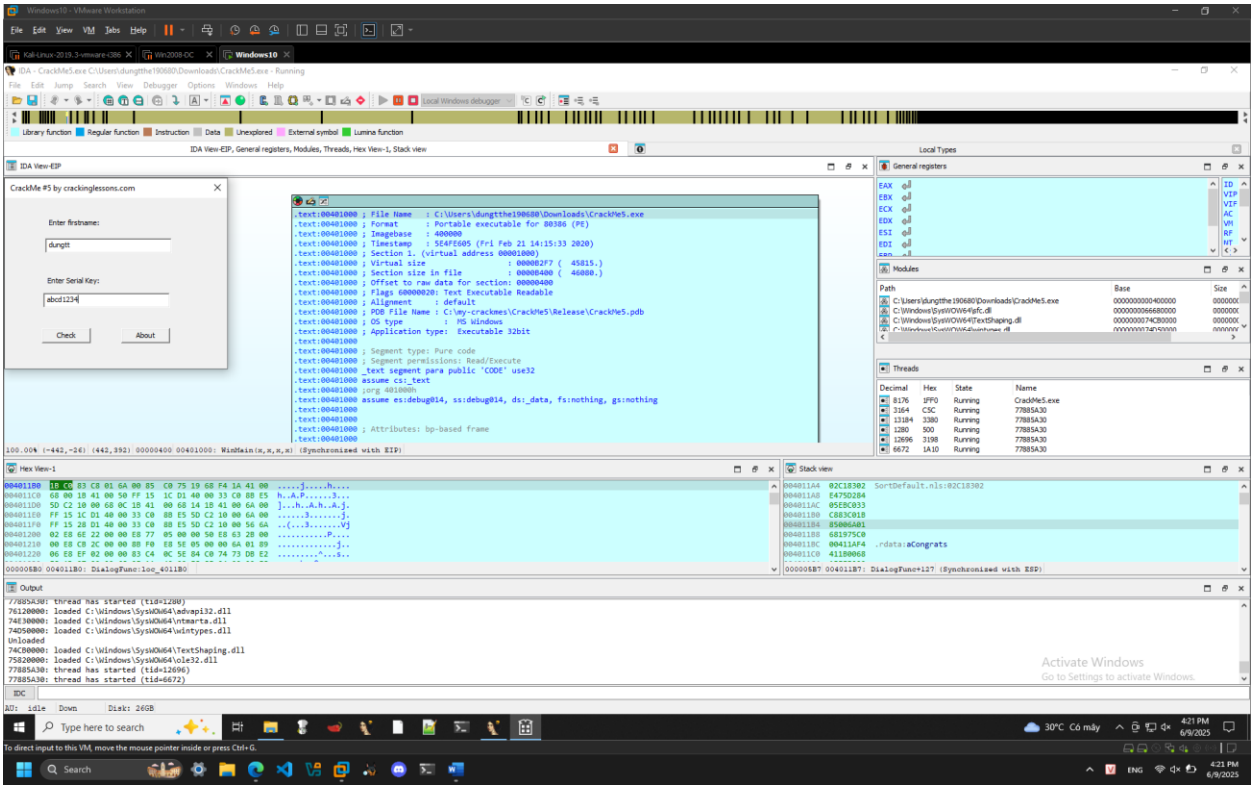
Em search từ khóa “Wrong” và được điều hướng đến đoạn code này:



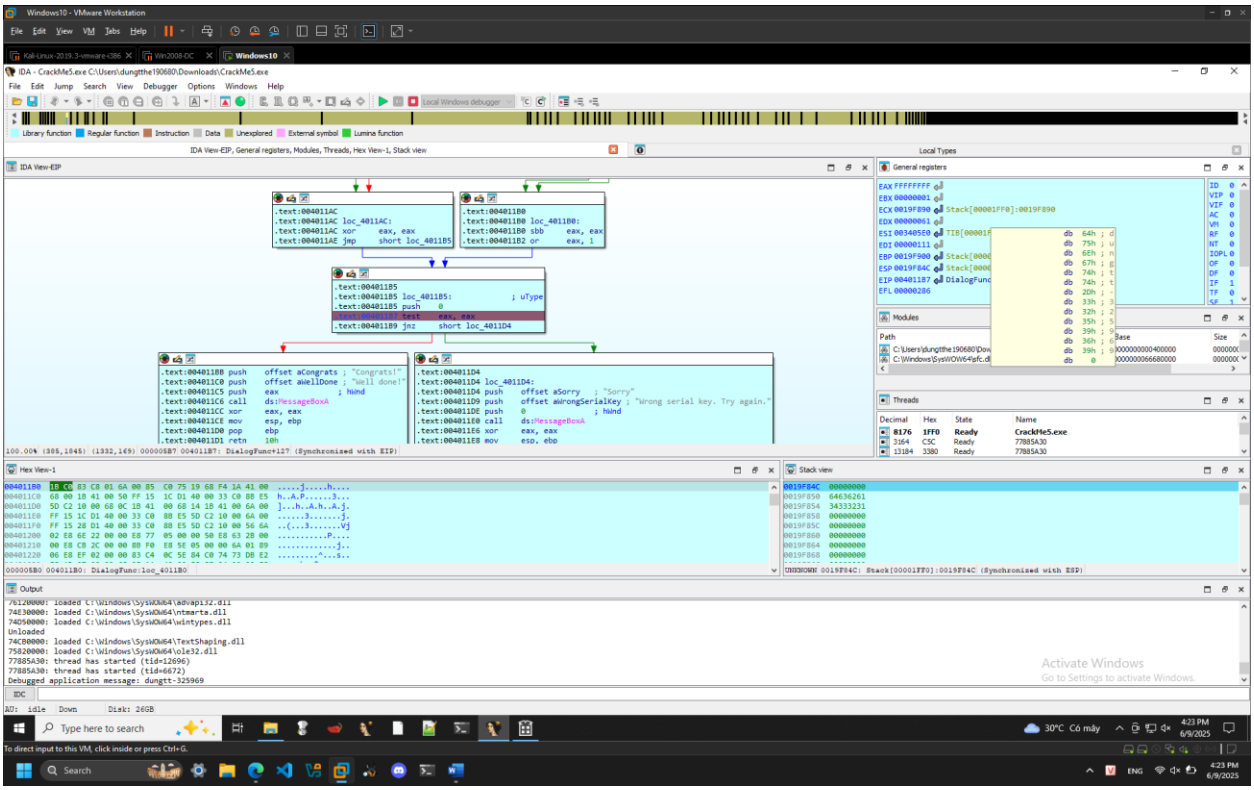
Có thể thấy logic so sánh tính đúng sai của input nằm trong đoạn code loc_4011B5, vì vậy để xem mật khẩu đúng, em đặt một breakpoint trong đoạn code này:



Sau đó em mở debugger và tiến hành debug chương trình:



Kiểm tra giá trị trong thanh ghi thì em tìm được mật khẩu chính xác của người dùng “dungtt”:



Em chạy lại chương trình, nhập mật khẩu vừa tìm được và nhận được thông báo chính xác: