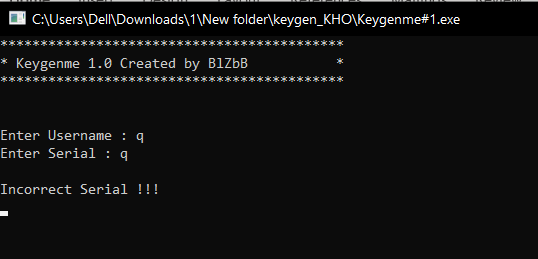
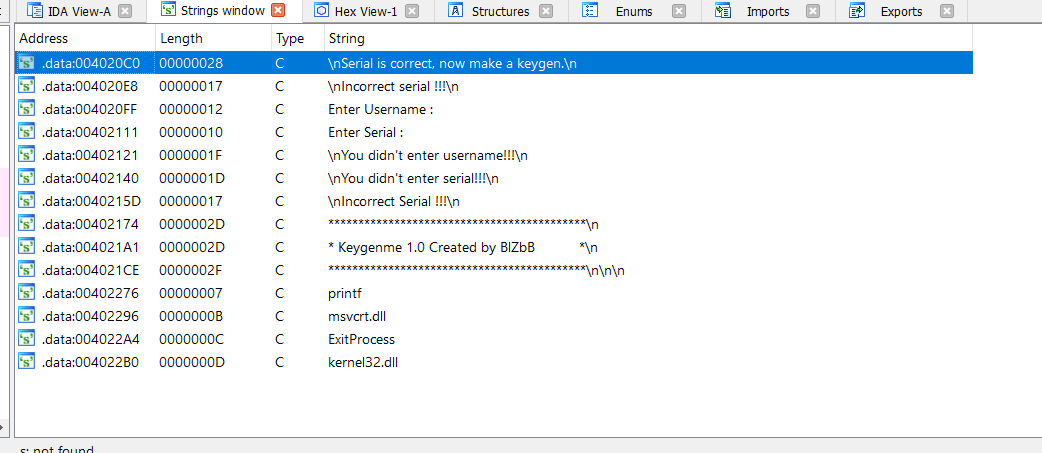
**Keygen**

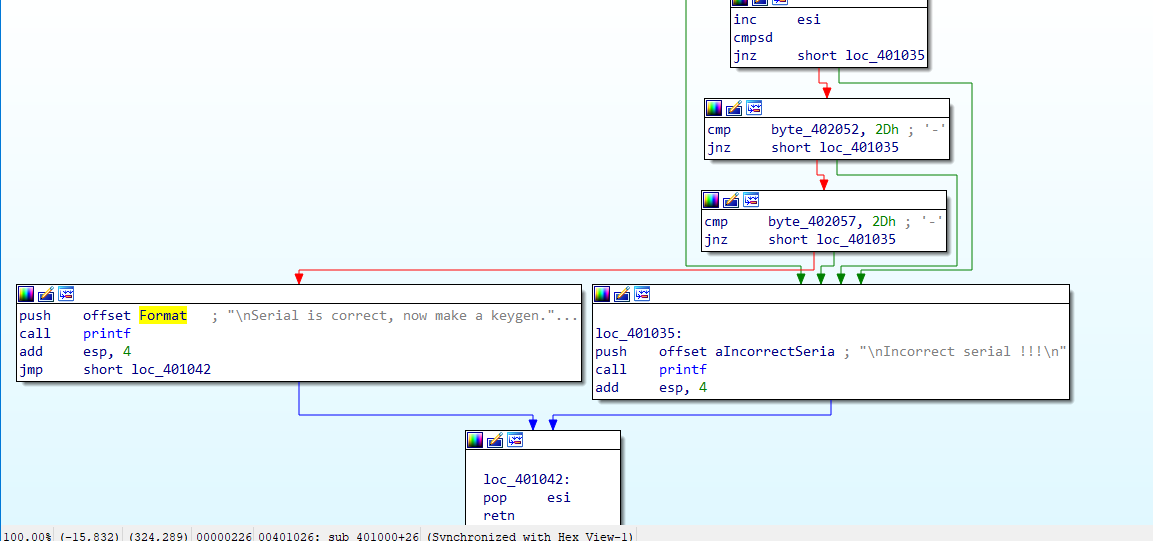
Chạy thử chương trình



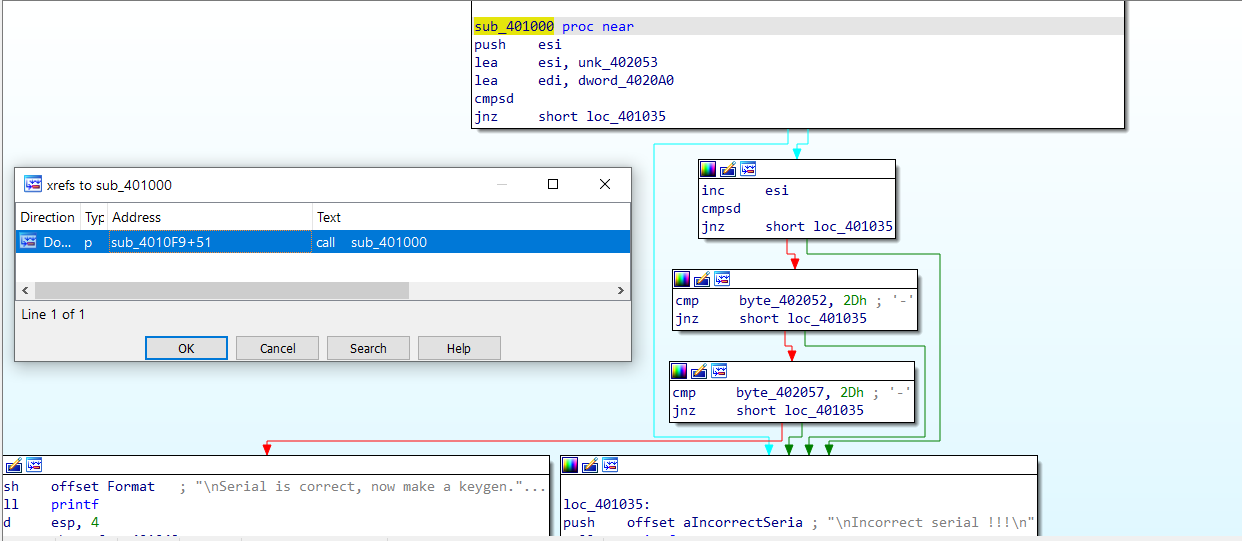
Shift F12 để xem chuỗi

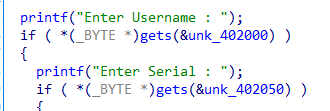
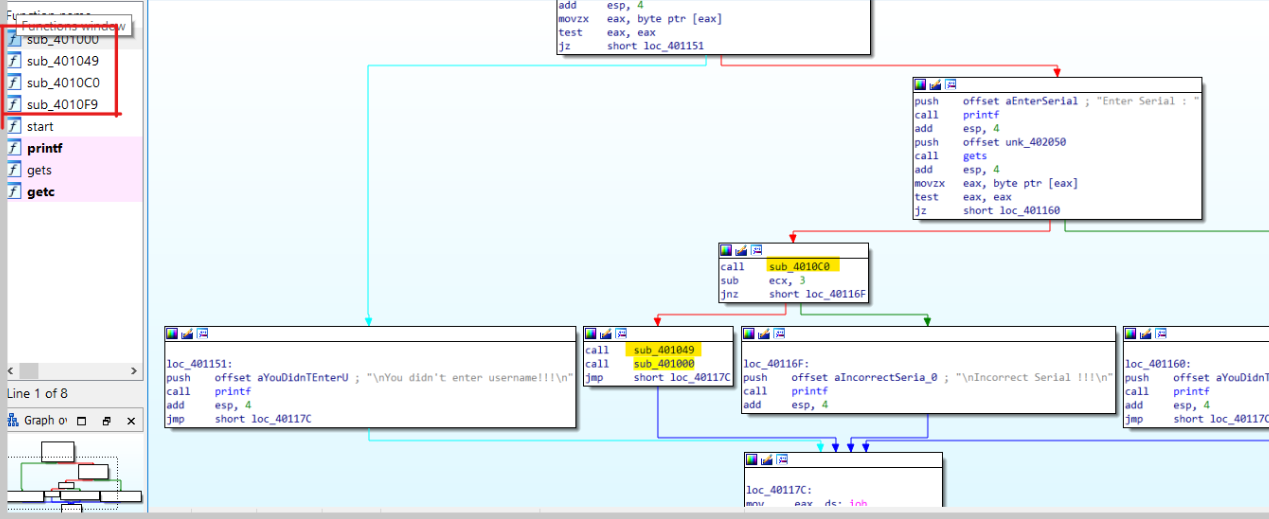


Đi đến nơi gọi chuỗi “Serial is correct, now make a keygen.”



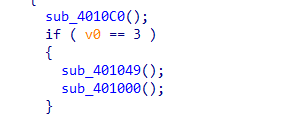
Kéo lên trên đi đến nơi gọi sub\_401000

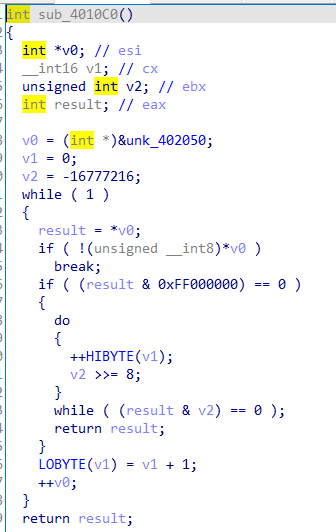


Sau khi nhấp OK ta đến được đây. Ta thấy ở đây có nhập input và có gọi các hàm ở cửa sổ Function. Ta sẽ bắt đầu phân tích tại đây.

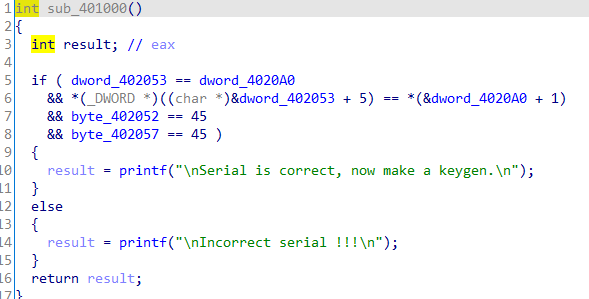
Username nhập vào lưu tại địa chỉ 402000 và serial lưu tại địa chỉ 402050.

Nhìn vào graph ta thấy sau khi đã nhập đủ username, serial chương trình sẽ gọi sub\_4010C0, sau đó so sánh v0 với 3 để gọi tiếp hai hàm mà có chuỗi thành công. Vì vậy , i giá trị sau khi thực hiện hàm sub\_4010C0() của v0 //ecx phải là 3





Gán v0 = địa chỉ của vùng nhớ unk\_402050. Trong hàm while ta thấy để tăng v1 thì ta thấy để v1 = 3 thì phải lặp 3 lần, từ đây có thể suy ra chuỗi serial phải có 12 kí tự và các giá trị serial[0], [4], [8] != 0 và serial[12] = 0

****

serial[3,4,5,6] = giá trị tại ô nhớ từ 4020A0 đến 4020A3; serial[8,9,10,11] = giá trị tại ô nhớ từ 4020A4 đến 4020A7; serial[2, 7] = 45

debug để thấy giá trị



Kiem tra

