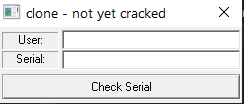
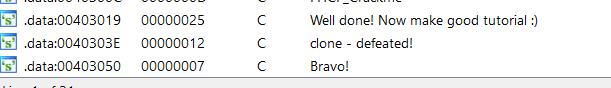
**Clone**

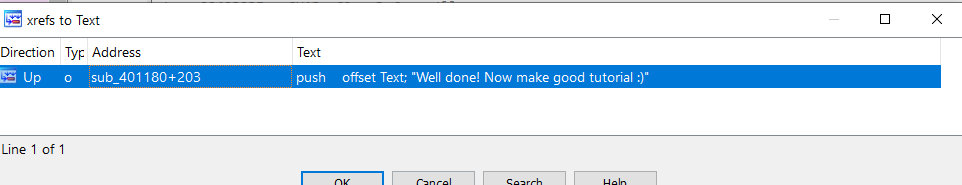
Chạy thử chương trình:

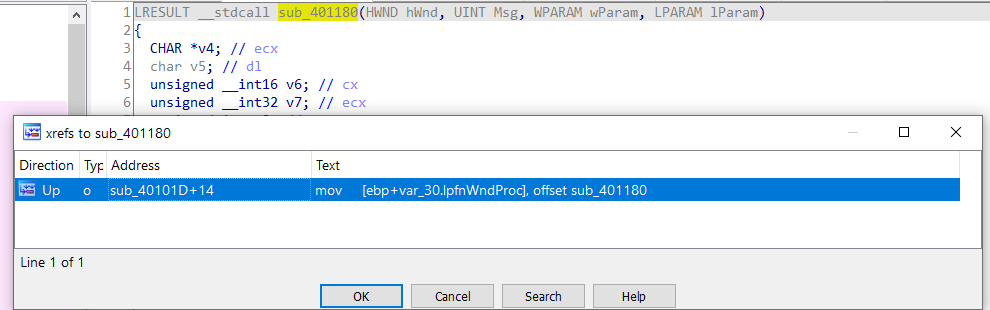


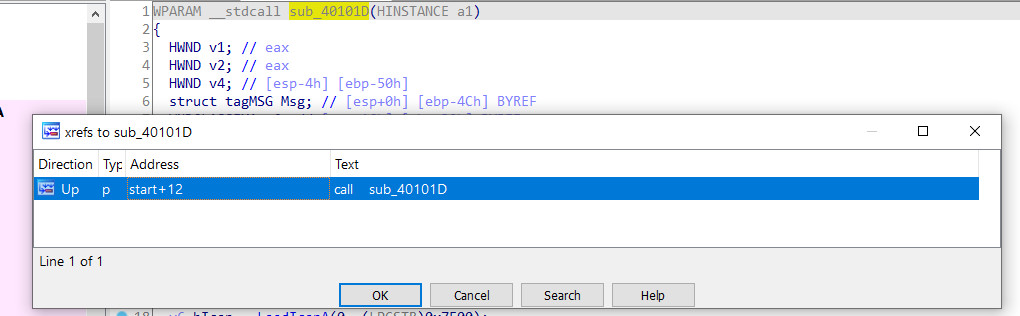
Shift F12 để xem chuỗi có trong chương trình



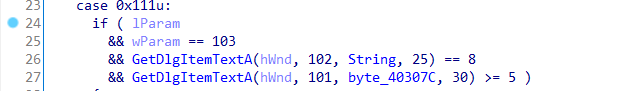
Đi đến nơi gọi chuỗi



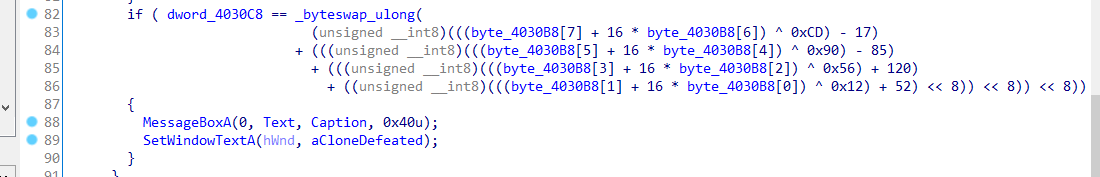
Ta thấy hàm sub\_401180 gọi chuỗi ta mong muốn và hàm sub\_40101D gọi hàm sub\_401180 

Hàm start gọi hàm sub\_40101D 

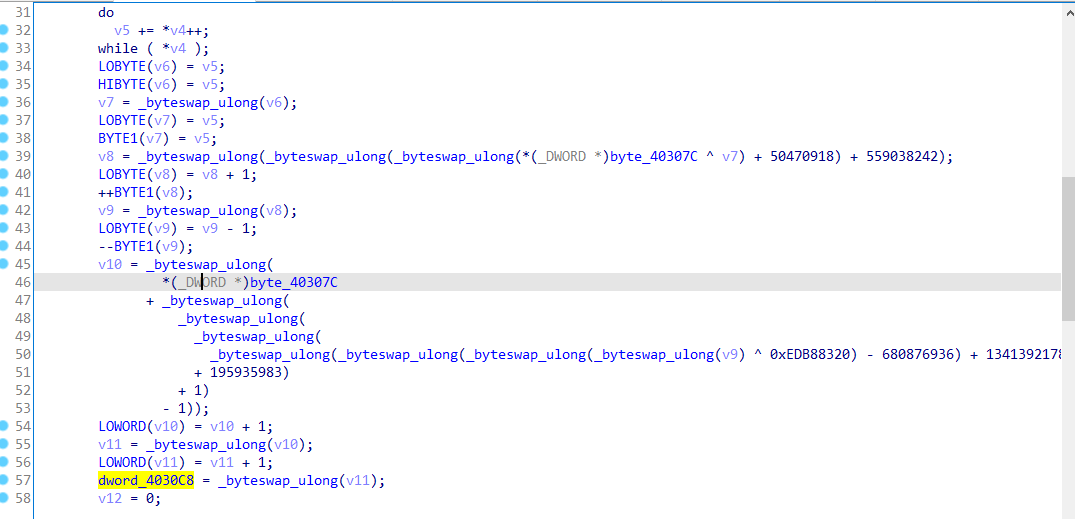
Trong hàm sub\_401180 username sẽ được nhập vào byte\_40307 có ít nhất 5 kí tự, còn serial được nhập vào String phải có 8 kí tự. (debug để biết nào username, serial )



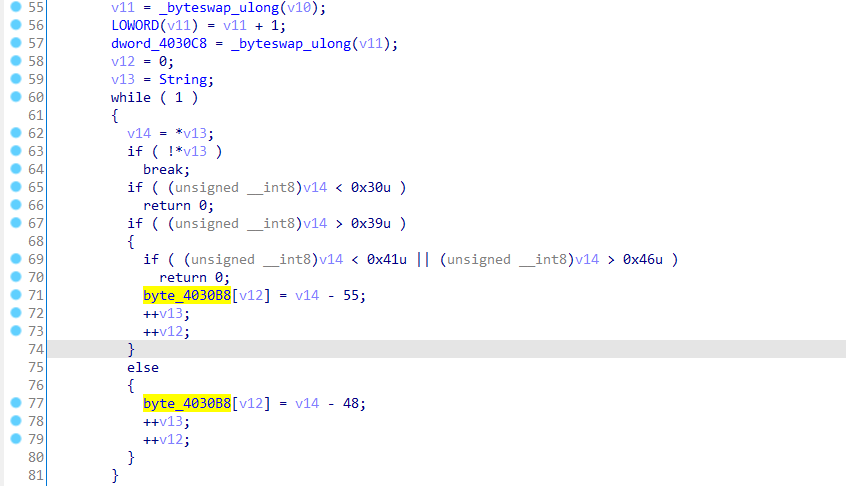
Mục tiêu của ta là thực hiện được câu lệnh bên trong if, vì vậy cần tìm cách để điều kiện if đúng.



Ta thấy dword\_4030C8 được tính toán ở đoạn code sau, ta chỉ cần debug để thấy kết quả

Nhập username là quynh thì dword\_4030C8 mang giá trị là 0x969BB6F5

Đoạn code tiếp theo trả về giá trị hex thật lưu ở byte\_4030B8 của các kí tự trong serial nếu chúng thuộc { 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F}



Ta thấy dword\_4030C8(sau khi đảo bit – byteswap\_ulong) được so sánh lần lượt 2 kí tự với lần lượt 2 kí tự được biến đổi từ byte\_4030B8 tạo ra , vậy serial cần thỏa:

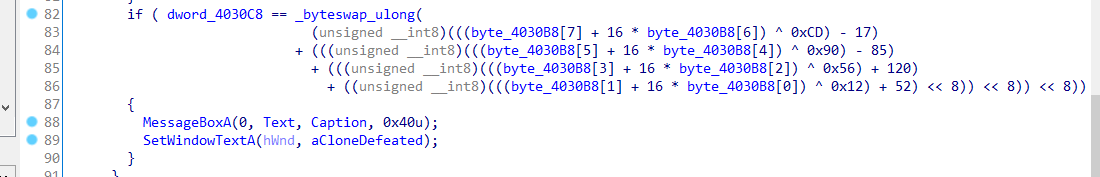
((serial[7] + 16 \* serial[6]) ^ 0xCD) - 17 = 0x96 => serial[6,7] = 6a

((serial[5] + 16 \* serial[4]) ^ 0x90) - 85 = 0x9B => serial[4,5] = 60

((serial[3] + 16 \* serial[2]) ^ 0x56) + 120 = 0xB6 => serial[2,3] = 68

((serial[1] + 16 \* serial[0]) ^ 0x12) + 52 = 0XF5 => serial[0,1] = d3

Vậy serial thỏa là: D368606A



Kiểm tra:

