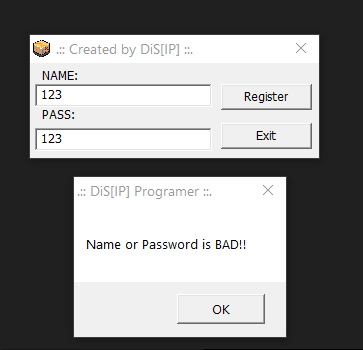
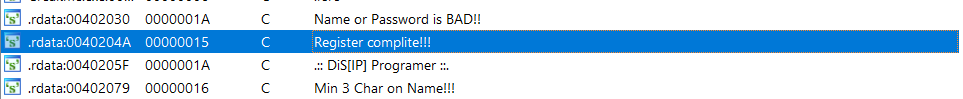
**Crack\_001**

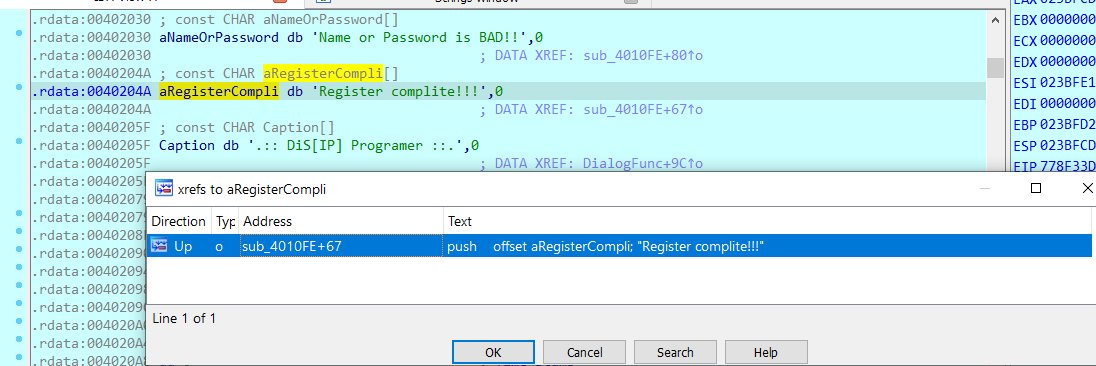
Chạy thử chương trình ta thấy chương trình yêu cầu nhập name, pass, sau đó thực hiện kiểm tra và in ra chuỗi thông báo

****

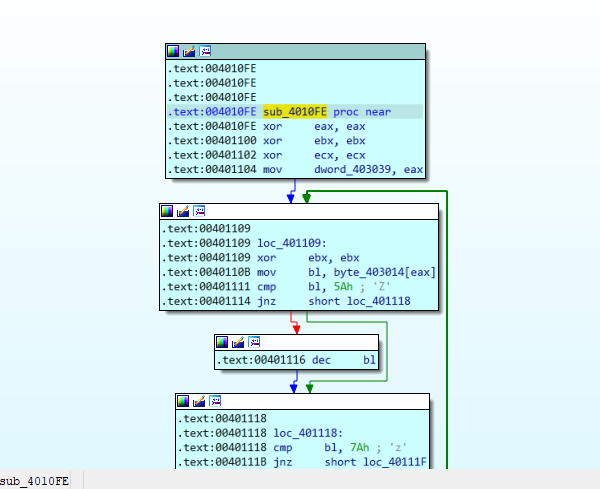
Shift +F12 để tìm kiếm chuỗi trong chương trình

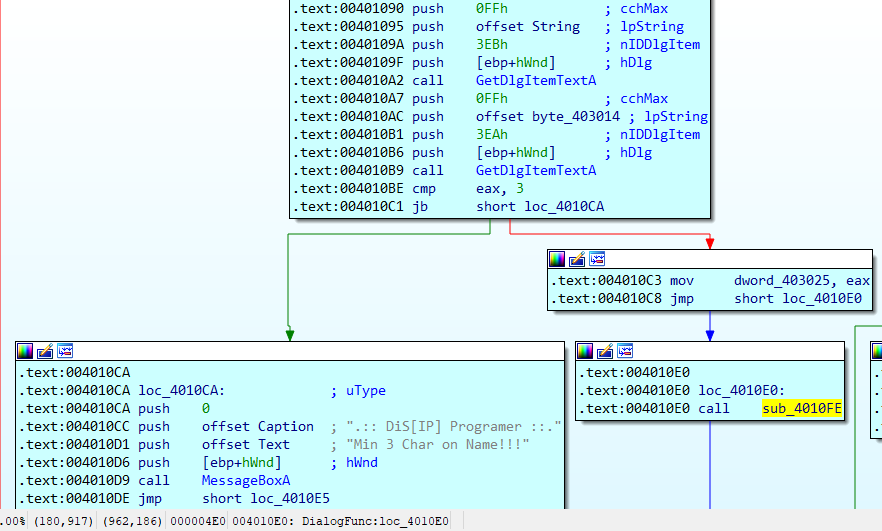


Nhấp vào chuỗi Register complete!!! (thông báo thành công) để đi tới vùng data chuỗi đó, tiếp tục nhấn X để xem nơi nào gọi chuỗi, chọn ok.





Kéo dần lên trên bấm X vào sub\_4010FE để xem nơi nào gọi nó 

Ta đến được đây. Ở đây ta thấy chương trình so sánh nếu eax <3 in ra “Min 3 Char on Name!!!” , suy ra chương trình đọc input Name (tối thiểu 3 kí tự) lưu vào địa chỉ 403014 và pass lưu vào địa chỉ gán thẻ String.

Nếu input thỏa yêu cầu chương trình nhảy đến khối bên phải , lưu độ dài Name vào vùng nhớ địa chỉ 403025, sau đó nhảy đến 004010E0 và gọi hàm sub\_4010FE(enter vào xem hàm)

Các giá trị khởi tạo ban đầu: eax, ebx, ecx, [dword\_403039]=0

Ta có thể debug ban đầu để hình dung tổng thể các đoạn code tiếp theo như sau: xét lần lượt từng kí tự từ đầu đến cuối trong chuỗi Name, eax sẽ đếm số kí tự đã được xét trong chuỗi Name, bl giữ giá trị của kí tự trong chuỗi Name đang xét. Nếu trường hợp kí tự trong chuỗi Name đang xét bằng ‘Z’ hoặc ‘z’ hoặc ‘9’ thì giữ nguyên bl; ngược lại thì tăng bl lên 1; bh được gán giá trị ban đầu là ‘a’ và tăng lên 1 sau mỗi lần xét 1 kí tự. cx được gán giá trị của 2 byte liên tiếp bắt đầu từ địa chỉ String[eax\*2] (gán lên thanh ghi với thứ tự ngược lại). Thực hiện so sánh bx và cx.

Tóm lại, chương trình sẽ duyệt qua chuỗi Name, với mỗi kí tự trong Name sẽ tạo ra 2 kí tự trong chuỗi pass.Trong đó:

+ Kí tự đầu được tính như sau: nếu trường hợp kí tự trong chuỗi Name đang xét bằng ‘Z’ hoặc ‘z’ hoặc ‘9’ thì kí tự đầu bằng kí tự đang xét của Name; ngược lại thì kí tự đầu bằng kí tự kế tiếp trong bảng mã ASCII của kí tự đang xét của Name.

+ Kí tự sau: bằng ‘a’ đối với kí tự đầu tiên của Name và tăng dần lên ‘b’, ‘c’, ‘d’,…. Với các kí tự kế tiếp của Name.

Vậy sẽ có rất nhiều trường hợp thỏa mãn. Chọn Name là Zz9ad và pass là Zazb9cbdee

Kiểm tra :

