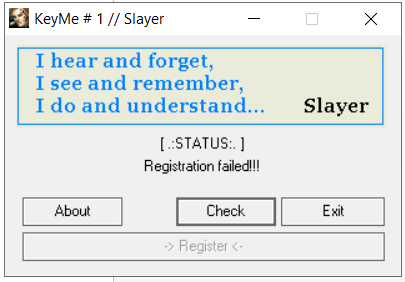
**LẬP TRÌNH HỆ THỐNG– LỚP NT209.L21.ANTN**

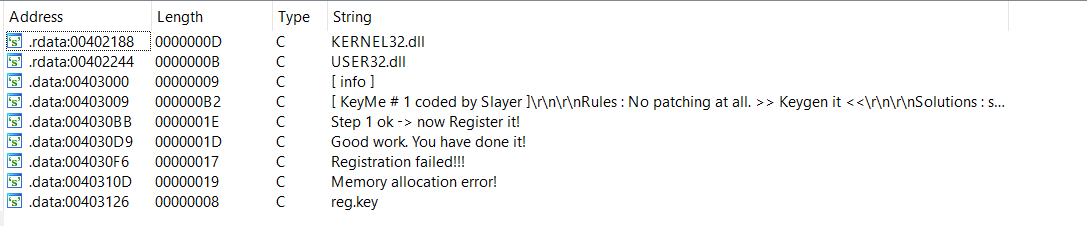
**RE CHALLENGES: S\_CRACKME1**

|  |  |  |  |
| --- | --- | --- | --- |
| **Giảng viên hướng dẫn** | **Phạm Văn Hậu** | | **ĐIỂM** |
| **Sinh viên thực hiện 1** | **Trần Đức Lương** | **19521815** |  |

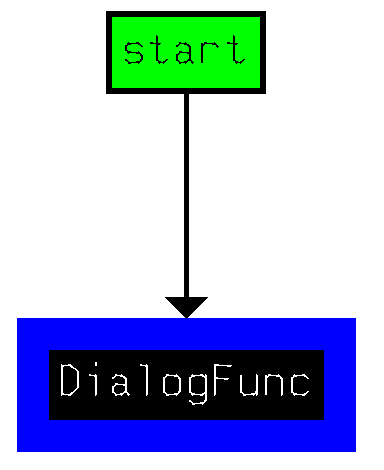
Thử chạy chương trình và ấn nút check thì báo không thành công. Nhìn vào giao diện có thể đoán được là để thực hiện đăng nhập thành công vào chương trình này cần 2 bước, cụ thể sau khi ấn nút check thì mới enable được nút register, sau đó thực hiện một số thao tác để đăng nhập thành công.



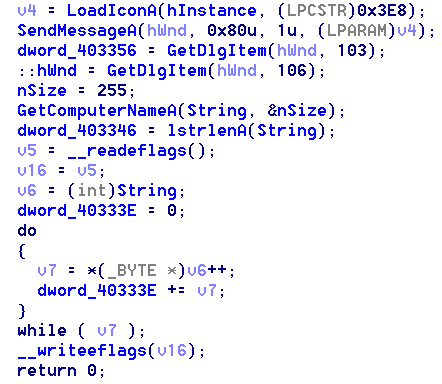
Mở chương trình bằng IDA Pro, xem strings có trong chương trình. Để ý có 2 strings là “Step 1 ok …” và “Good work ..”, điều này có nghĩa là chương trình sẽ có đúng 2 bước như dự đoán.



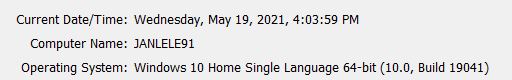
Thực hiện xem sơ đồ hoạt động của chương trình. Chương trình chỉ có đúng 2 hàm, hàm start gọi hàm DialogFunc 1 lần rồi cho ra kết quả.



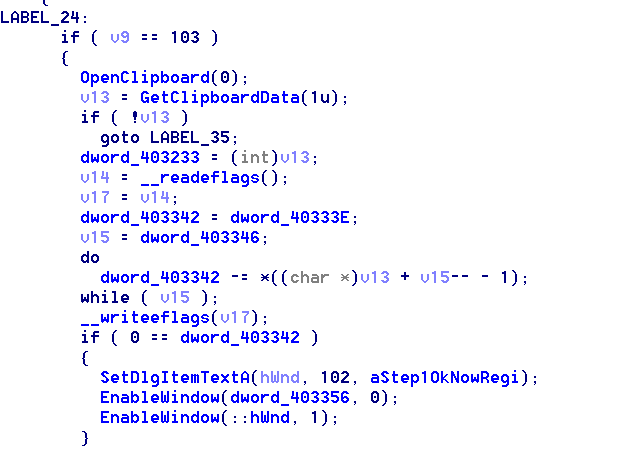
Xem mã giả của hàm DialogFunc trên, chương trình thực hiện lấy tên của máy tính mình đang sử dụng bằng hàm GetComputerNameA lưu vào biến String và trả về cả độ dài của String đó. Tiếp theo sau đó biến dword\_403346 sẽ lưu độ dài của String còn dword\_40333E lưu String đó dưới dạng hex của tổng các kí tự có trong String.



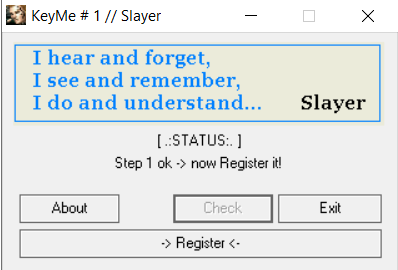
Ở đây máy tính em đang sử dụng có Computer Name là JANLELE91 thì dword\_40333E == 0x265 và dword\_403346 == 9.



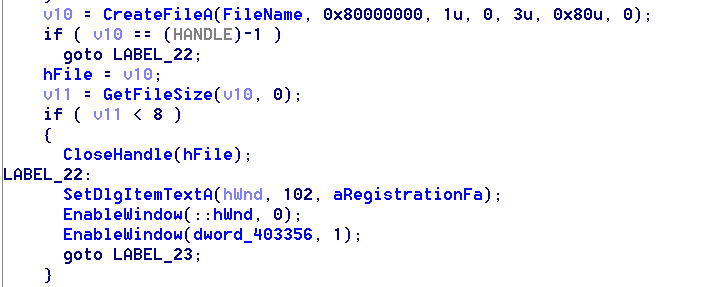
Dưới đây block để vượt qua step 1. Để ý hàm có dòng chữ Clipboard (khay lưu tạm) và để thỏa mãn các điều kiện thì Clipboard phải đang lưu Computer Name của mình là “JANLELE91”. Khi đó trước khi dòng thông báo của aStep10kNowRegi được thực thi thì phải ấn copy JANLELE91 rồi ấn vào Check.



Sau khi ấn vào Check có thể thấy đã xong Step 1 và nút Register đã được enabled.



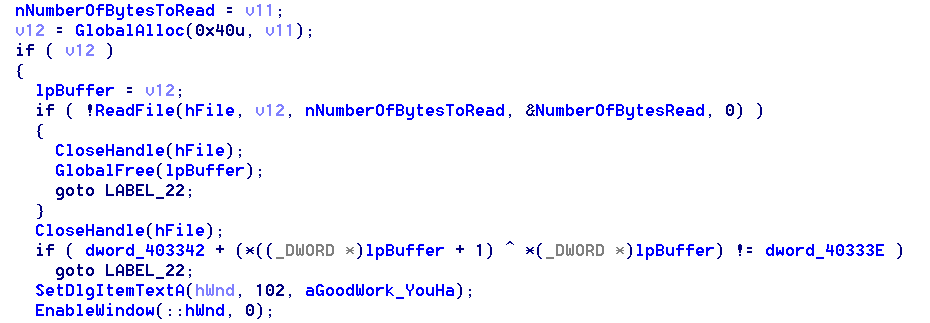
Tiếp theo, chúng ta phải tạo một file có tên được lưu ở biến FileName (hàm CreateFileA).



Thực hiện truy xuất FileName thì thấy ta phải tạo một file có tên “reg.key” cùng folder với chương trình với nội dung là một chuỗi có độ dài tối thiểu là 8. Ta sẽ tối ưu bằng cách lưu một chuỗi có 8 kí tự.



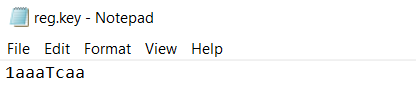
Tiếp theo để biết cần lưu chuỗi gì trong file reg.key, chúng ta đọc block dưới đây. Chương trình thực hiện so sánh dword\_403342 + hex(4 kí tự cuối) ^ hex(4 kí tự đầu) với dword\_40333E.



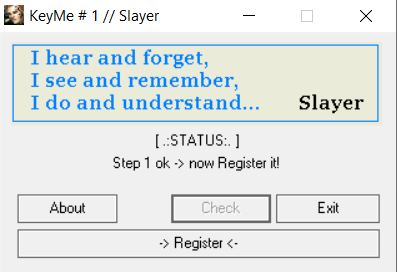
Cụ thể để thành công ta cần hex(4 kí tự cuối) ^ hex(4 kí tự đầu) == dword\_40333E (do dword\_403342 == 0 sau step 1).

Khi đó: hex(4 kí tự cuối) ^ hex(4 kí tự đầu) == 0x265 ()

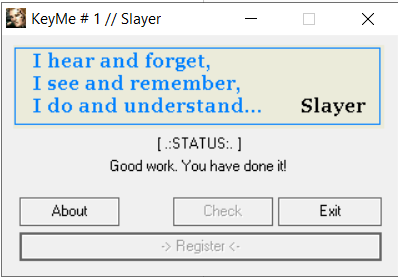
Chú ý ở đây chương trình dùng phương thức Little Endian để lưu trữ dữ liệu. Thực hiện lấy thử một chuỗi 4 ký tự làm 4 kí tự đầu, đó là s1 = “1aaa” khi đó hex(s1) == 0x61616131. Để tìm 4 ký tự sau, ta lấy 0x61616131 ^ 0x265 = 0x61616354 tương đương với chuỗi s2 = “Tcaa”.

Thực hiện ghi chuỗi “1aaaTcaa” vào file reg.key. 

Chạy lại chương trình, copy Computer Name là JANLELE91 rồi ấn nút Check



Tiếp tục ấn nút Register ta được:



Vậy ta đã register thành công.