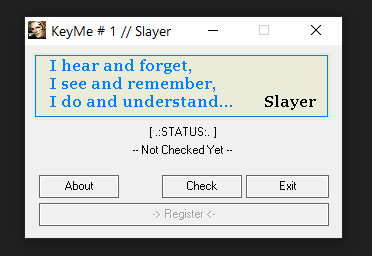
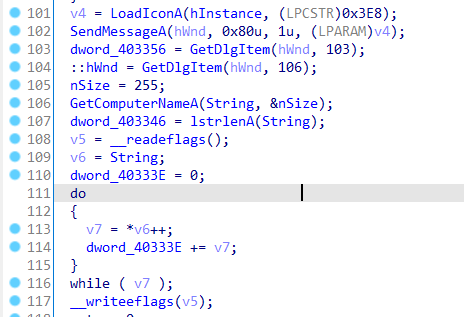
**S\_Crackme1**

Chạy thử chương trình



Trong hàm start có nhắc đến hàm DialogFunc, ta vào xem hàm này:



Quan sát đoạn code trên ta thấy chương trình sẽ lấy chuỗi tên computer lưu vào String, gán dword\_403346 bằng độ dài String, gán v6 bằng String. Sau đó từ dòng 111 đến 116 gán tên máy tính vào dword\_40333E.

Tiếp đến là đoạn code khi chúng ta nhấn check:

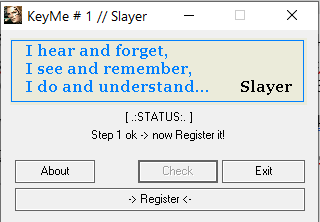


Để chạy được vào else ở dòng 51 để EnableWindown điều kiện if ở dòng 46 phải sai, tức dword\_403342 =0. Nhìn lên các dòng code phía trên, ta thấy ban đầu v13 chứa nội dung của Clipboard, sau đó gán dword\_403233 = v13, dword\_403342 = dword\_40333E (tên máy tính).

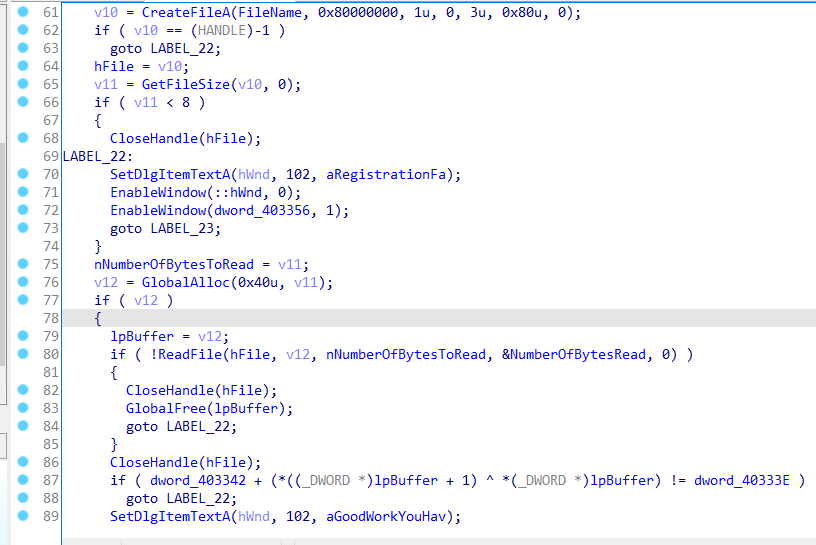
Quan sát vòng lặp do while, dword\_403342 được tính lại dựa trên dword\_403233 , ta thấy để

dword\_403342 =0, dword\_403233 cần giống dword\_403342, tức là ta cần coppy tên máy vào clipboard trước khi nhấn check.





Pass step 1 , tiếp theo xem hàm khi nhấn Register:



Chương trình mở một file có tên là “reg.key” (hàm CreateFileA)



Chương trình kiểm tra điều kiện file phải có ít nhất 8 kí tự và lưu nội dung của file vào biến v12.

Để không đi đến LABEL 22, vì phía trên dword\_403342 =0 nên chỉ cần thỏa điều kiện lpBuffer[0,3] ^ lpBuffer[4,7] = tên máy tính (giá trị tương ứng máy mình sau debug là: 0x418)

Vậy ta tạo 1 file với tên là reg.key cùng thư mục với file KeyMe.exe với nội dung là PLHHHHHH.

