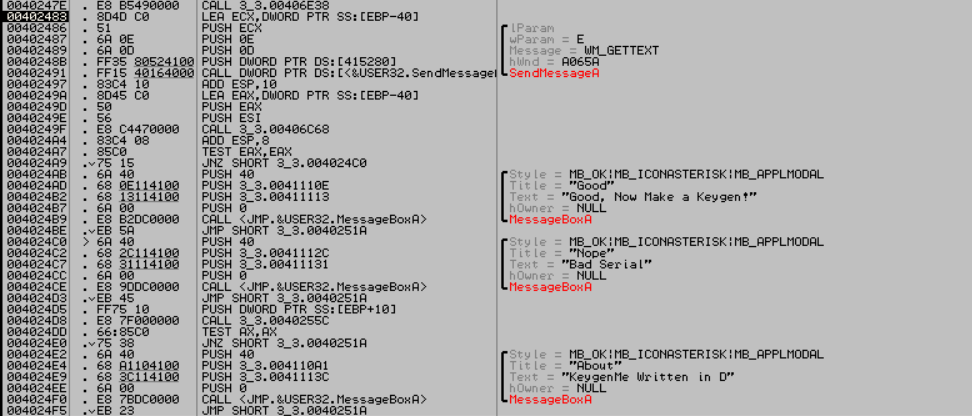
3\_3.exe

1. Tìm GOOD, BAD BOY

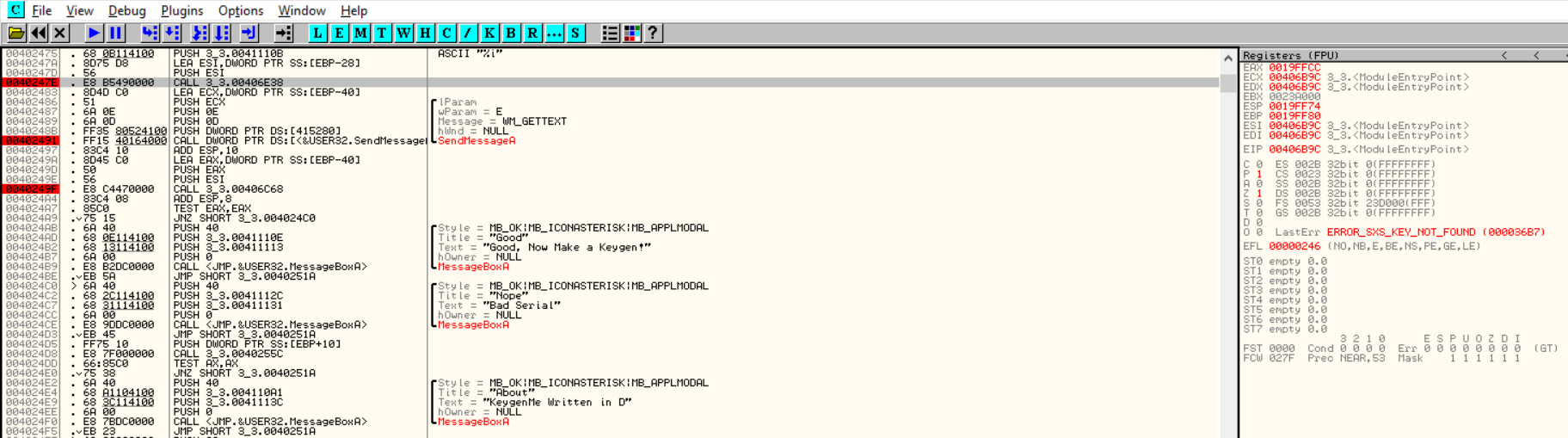


* Sử dụng chức năng tìm kiếm chuỗi để tìm GOOD BOY, BAD BOY

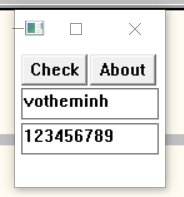


* Đi đến đoạn code liên quan

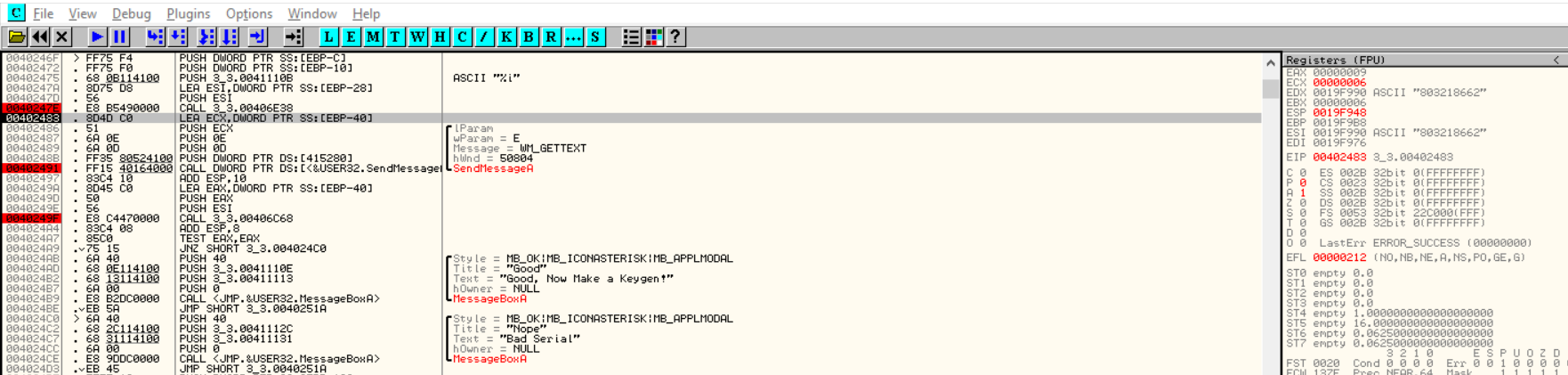
1. Phân tích code



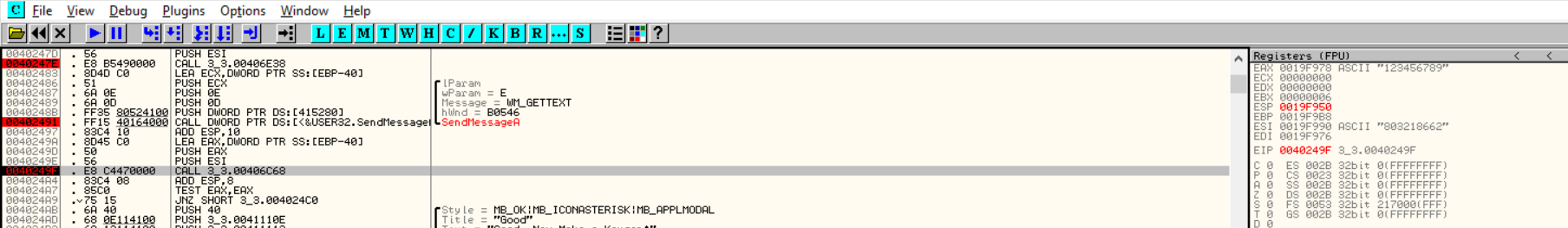
* Đặt breakpoint tại những điểm quan trọng và bắt đầu Debug, chú ý giá trị của các thanh ghi



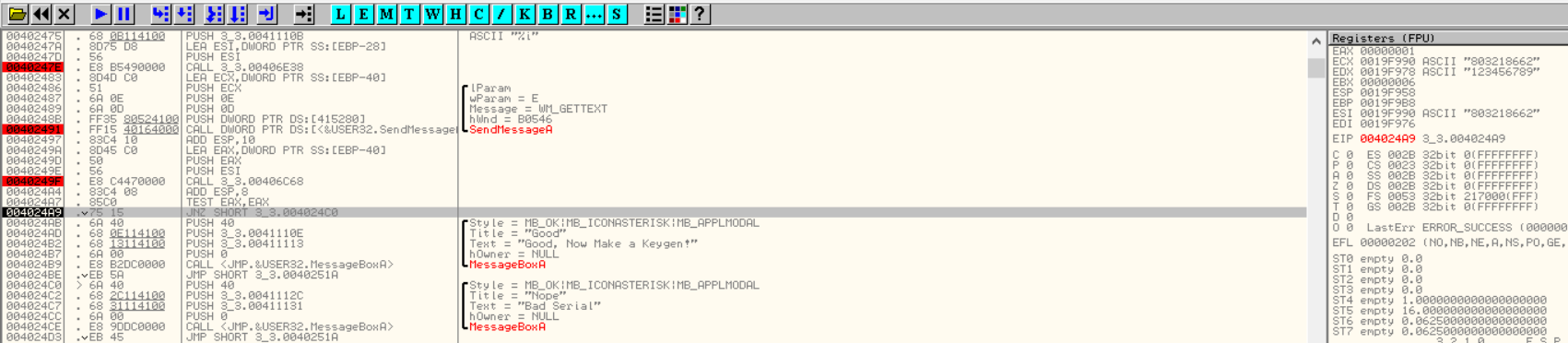
* Nhập thử Username: “votheminh”, Password: “123456789”



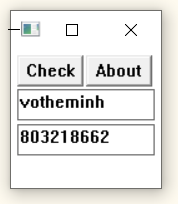
* Sau khi chạy qua lệnh CALL 3\_3.00406E38, ta thấy giá trị khả nghi trong thanh ghi EDX, ESI = “803218662”



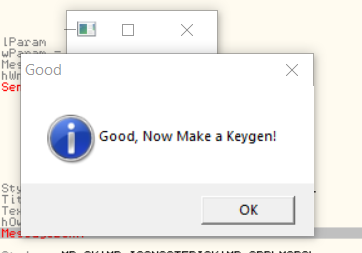
* EAX lúc này lưu chiều dài chuỗi tên ta nhập vào “votheminh”, ESI = “803218662”



* Tới lệnh JNZ 3\_3.004024C0 là lệnh nhảy đến GOODBOY nên ta có thể đoán là lệnh TEST EAX, EAX là kiểm tra điều kiện chuỗi ta nhập vào
* CALL 3\_3.004024C0 là lệnh so sánh giá trị trong EDX “123456789” với giá trị trong thành ghi ECX = “803218662” nếu đúng thì EAX = 0, nếu sai thì EAX = 1
* Chạy tiếp tục tiếp theo chắc chắn sẽ chạy vào BAD BOY



* Chạy thử với trường hợp Username: “votheminh”, Serial: “803218662”



* Đã đúng GOOD BOY nên với Username: “vothem%n” thì Serial: “803218662”