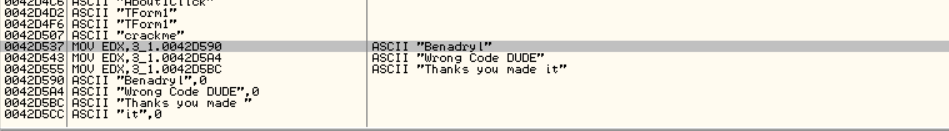
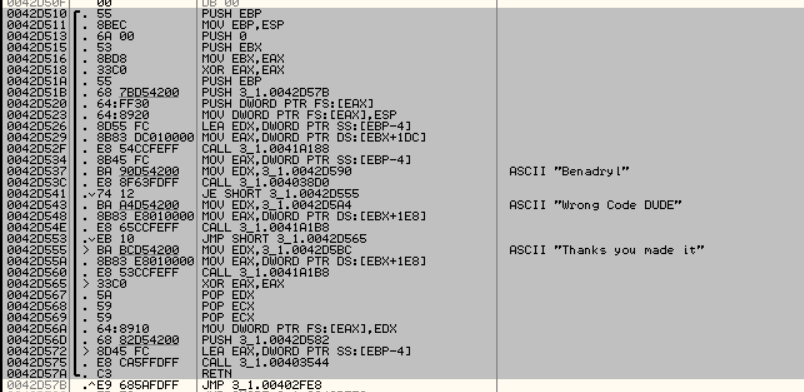
Đề 3

3\_1.exe

1. Tìm GOOD BOY, BAD BOY

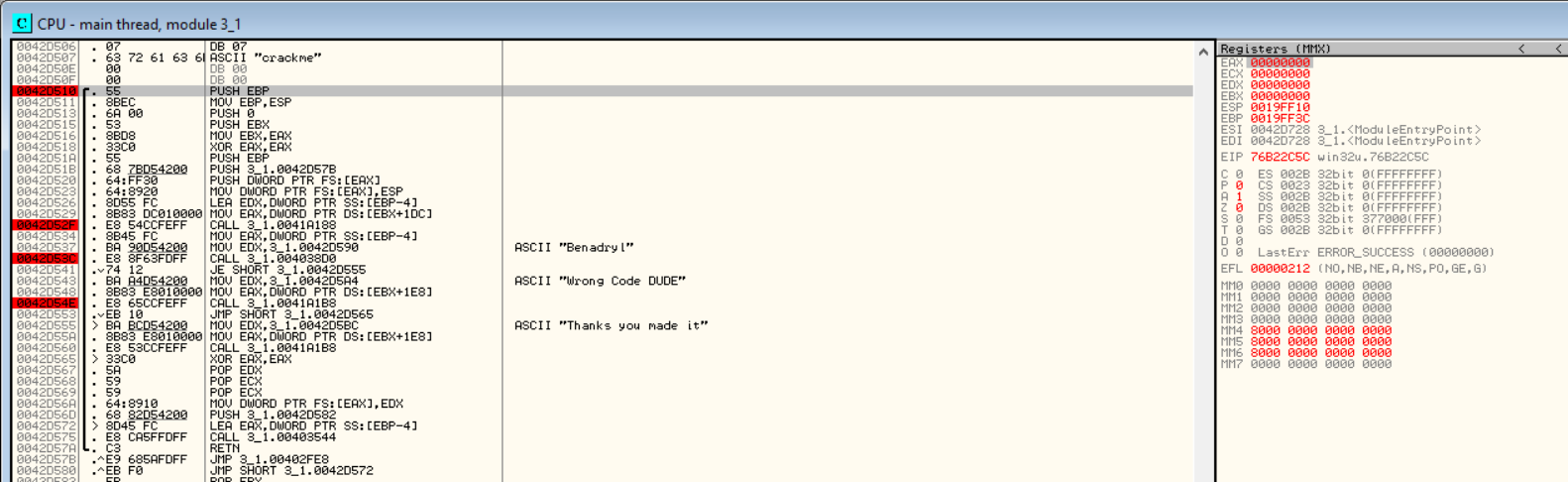


* Sử dụng chức năng tìm kiếm chuỗi trong OllyDbg tìm GOOD BOY và BAD BOY trong đoạn code

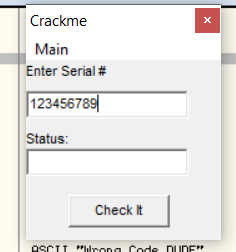


* Đi đến đoạn code chứa thông tin về GOOD BOY, BAD BOY

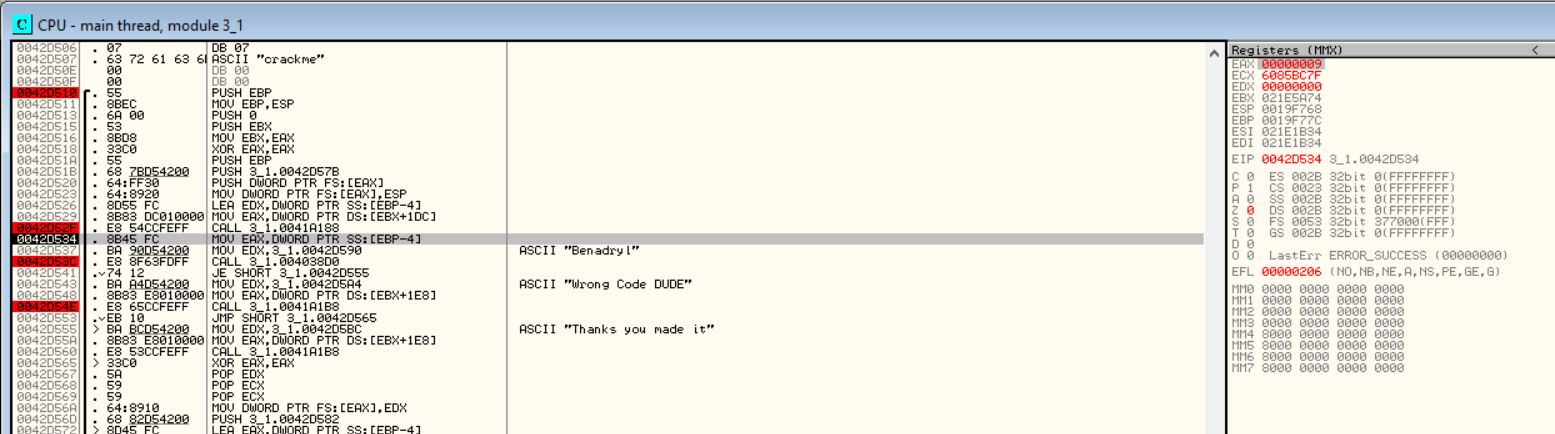
1. Phân tích code



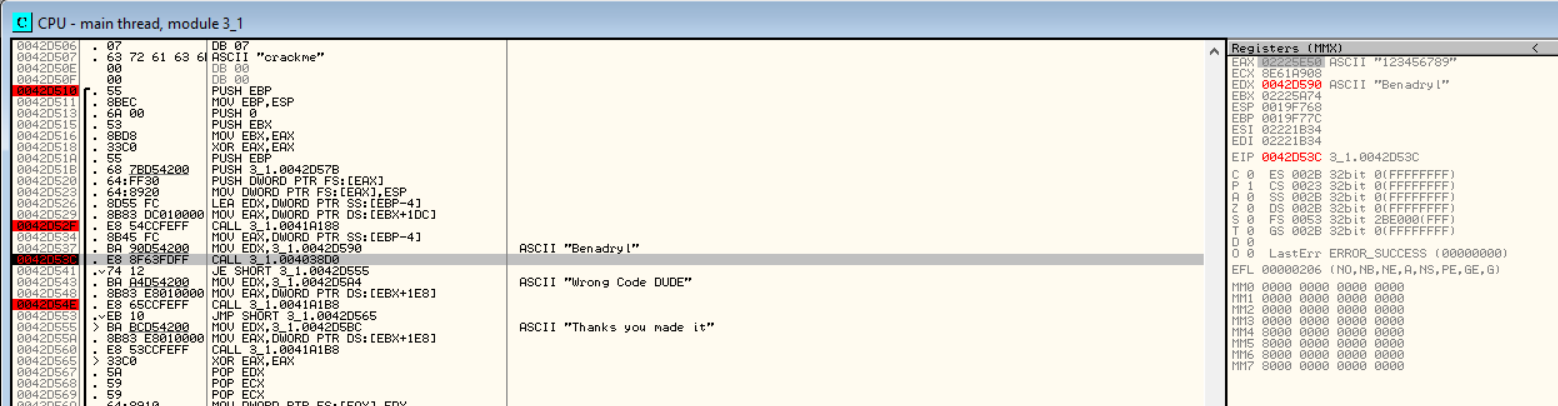
* Đặt bookmark và tiến hành chạy từng lệnh một, chúng ta sẽ dừng ở những lệnh quan trọng, chú ý giá trị của các thanh ghi



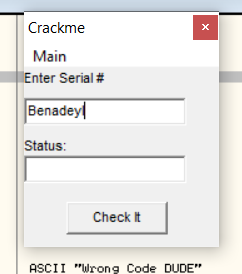
* Nhập thử giá trị cho Serial và nhấn Check It



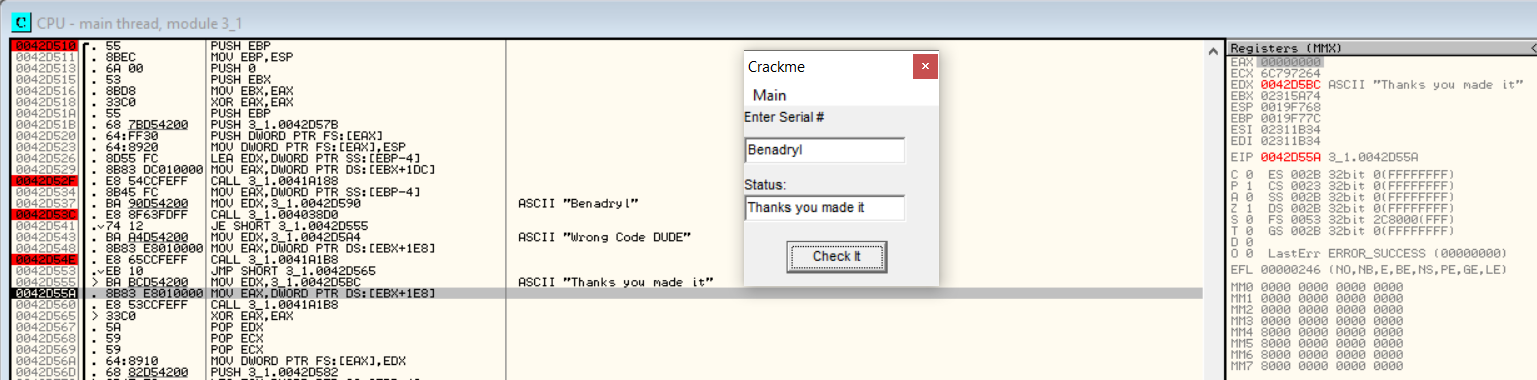
* Thực hiện xong lệnh CALL 3\_1.0041A188 ta thấy EAX lưu giá trị là số ký tự chuỗi ta nhập vào (không quan trọng lắm)



* Thực hiện tiếp 2 lệnh tiếp theo ta thấy giá trị của thanh ghi EAX lúc này là chuỗi kí tự ta nhập vào, EDX là một chuỗi khả nghi chứa chuỗi “Benadryl”
* 2 lệnh tiếp theo là lệnh CALL 3\_1.004038D0 và lệnh JE SHORT 3\_1.0042D555, điều đặc biệt là 3\_1.0042D555 là địa chỉ của dòng lệnh dẫn đến GOOD BOY ta có thể nghi ngờ rằng lệnh CALL 3\_1.004038D0 dùng để gọi hàm so sánh chuỗi ta nhập vào với KEY và “Benadryl” bị nghi ngờ là KEY, lệnh nếu kết quả đúng thì JE SHORT 3\_1.0042D55 sẽ đưa ta đến GOOD BOY
* Tiếp tục chạy tất nhiên sẽ tới BADBOY và kết thúc chương trình



* Chạy lại chương trình và thử Serial với “Benadryl”



* Kết quả đúng là KEY 3\_1.exe = Benadryl