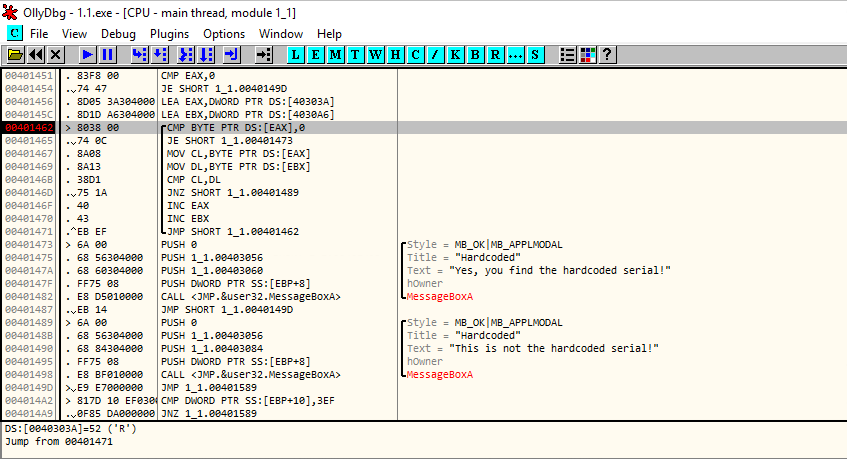
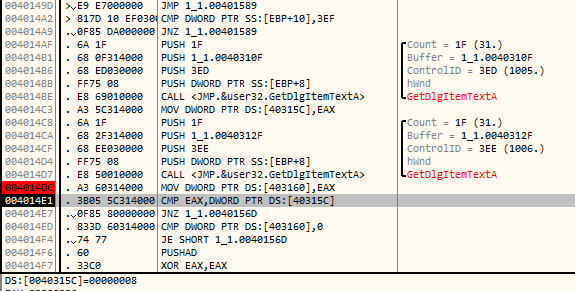
1. CrackMe 1.1
2. Phần Hardcoded:



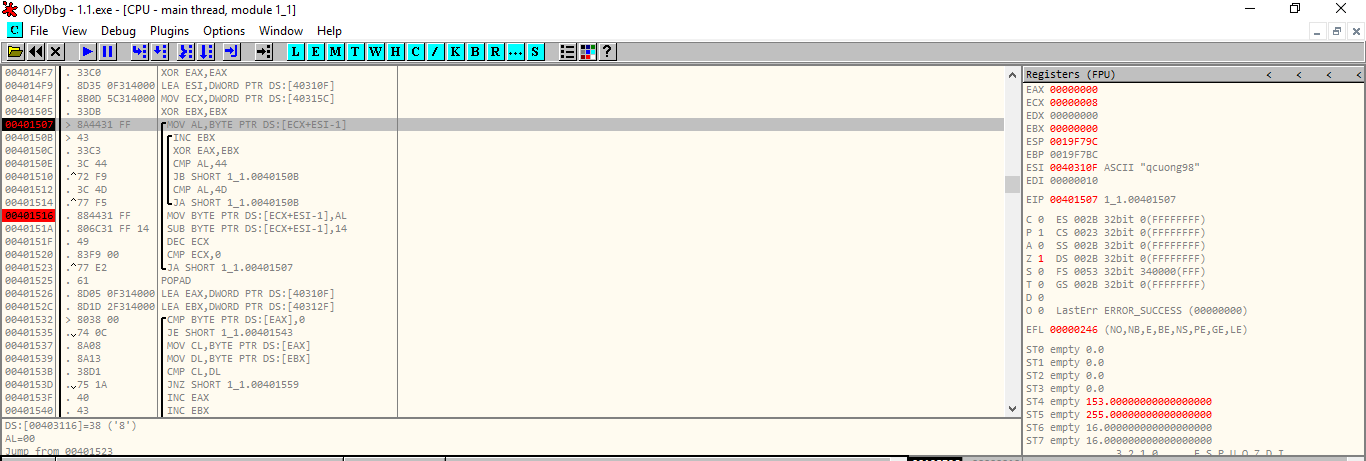
* Để chương trình vào được phần Good Boy thì EAX và EBX phải giữ giá trị giống nhau (có cùng độ dài, mỗi ký tự ở vị trí tương ứng của EAX và EBX giống nhau) dựa vào đoạn vòng lặp từ dòng 00401462 đến dòng 00401471
* EBX chính là giá trị ta nhập vào ở phần Hardcoded
* EAX mang giá trị là “Reversing raises knowledge!”
* Vậy phần Hardcoded sẽ là: “Reversing raises knowledge!”

1. Phần Name và Serial

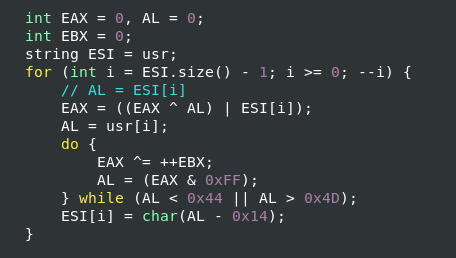
* Sau khi đã nhập đúng hardcoded thì ta tiến hành chạy code



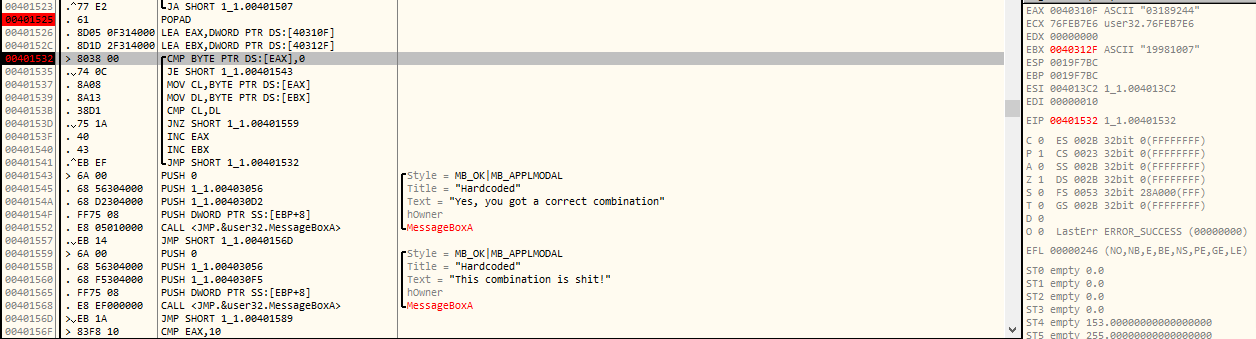
* Name và Serial phải có độ dài bằng nhau



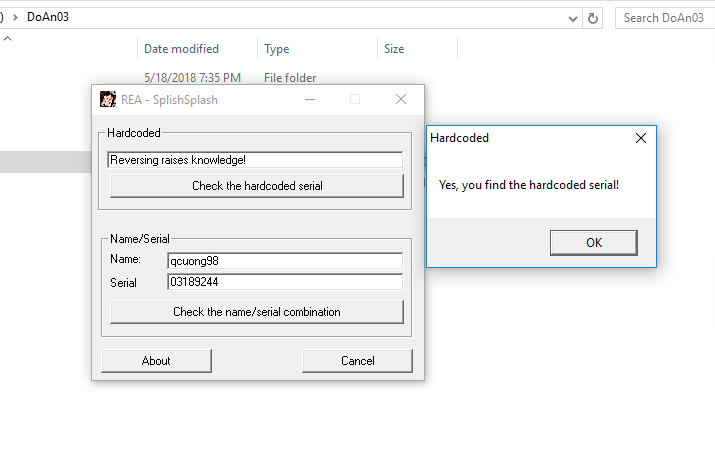
* ESI đang lưu giá trị Name
* Ta chuyển code vòng lặp từ dòng 00401507 đến 00401516 ra C++

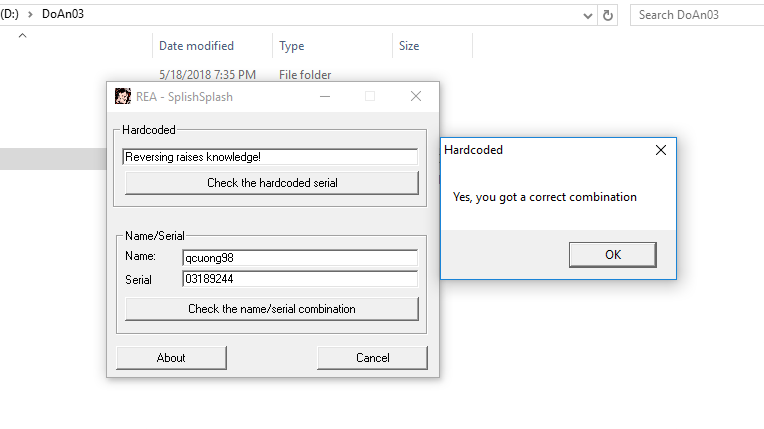


* Sau đó EAX = ESI mới và EBX = Serial ta vừa nhập

- Nếu EAX = EBX thì ta sẽ vào được Good Boy

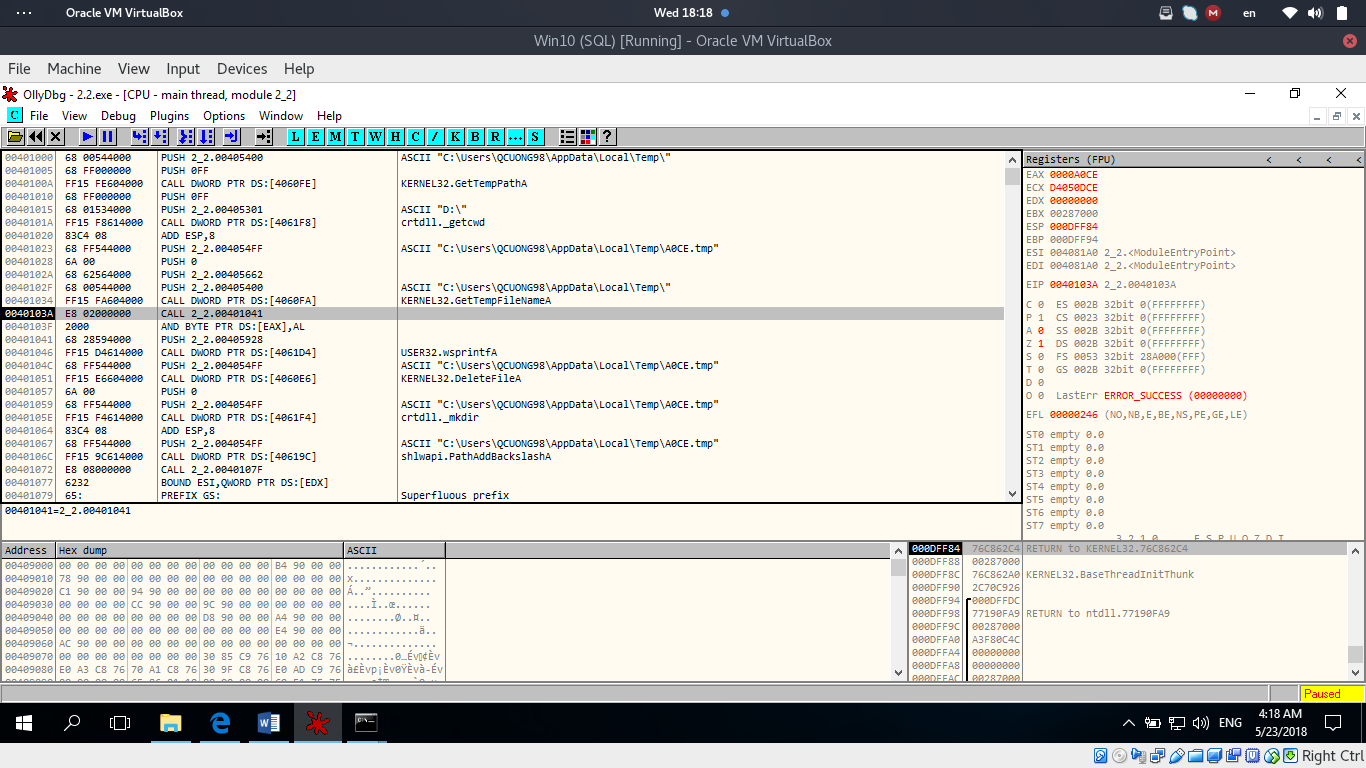
=> Ta có đoạn code sinh từ Name -> Serial



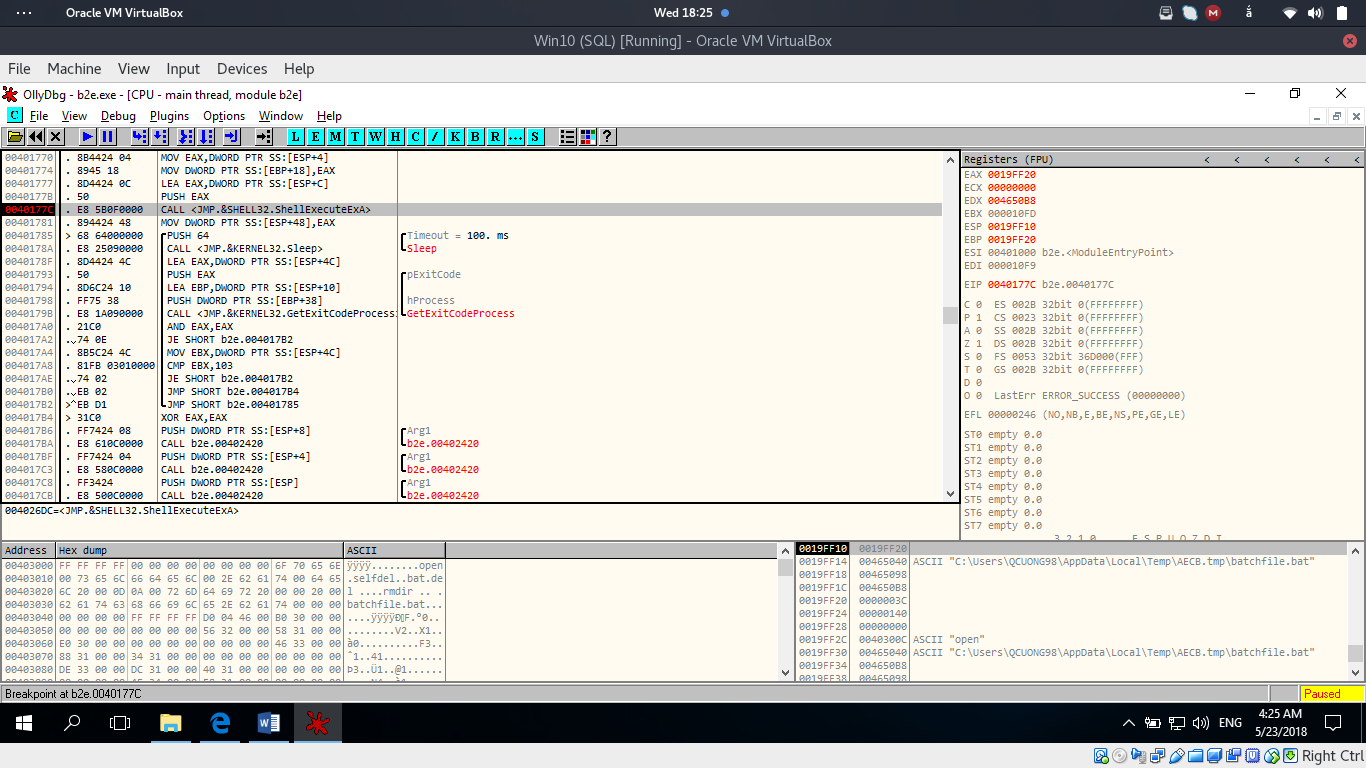


1. CrackMe 2.2

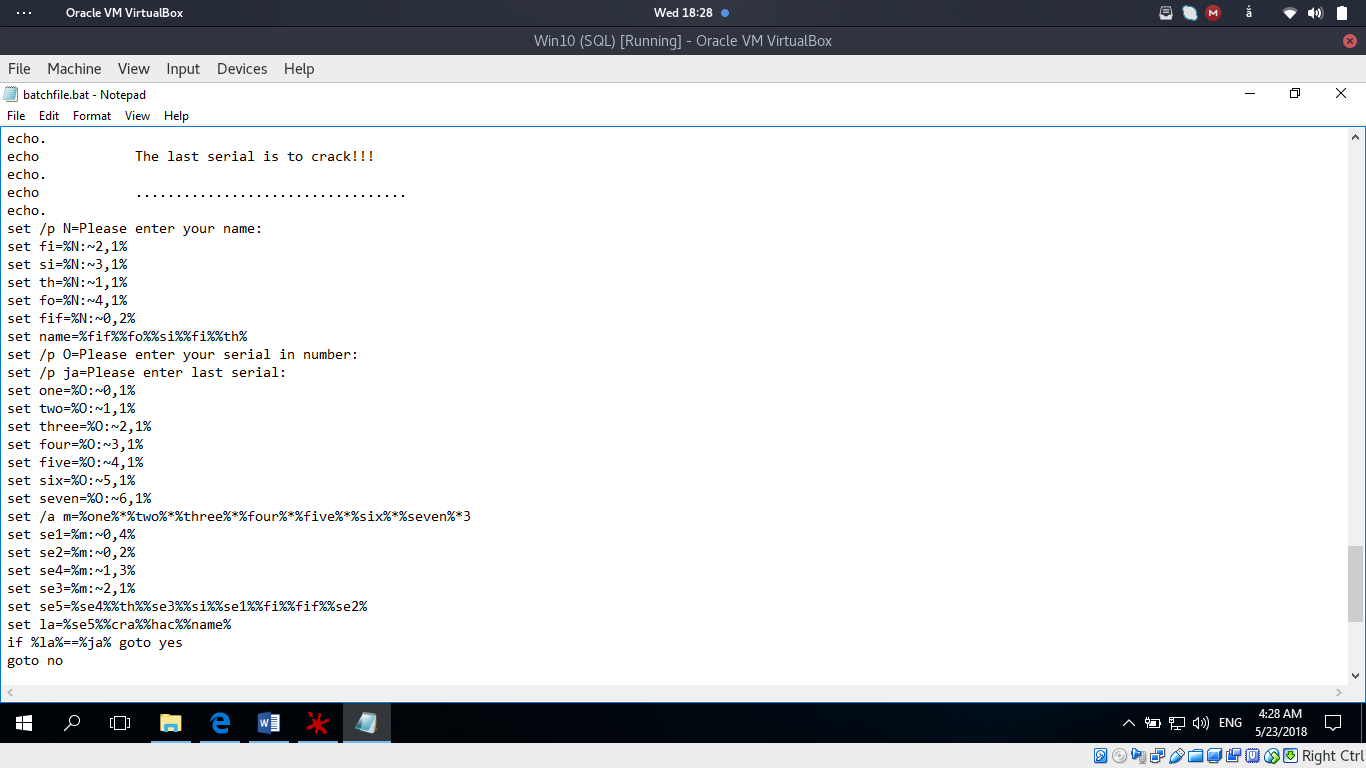
* Bản thân đoạn code trong 2.2 khi xuất hiện phần code để nhập Name/Serial/LastSerial -> Dự đoán 2.2 tạo ra một file thực thi khác



* Mỗi lần chương trình chạy sẽ tạo ra một file b2e.exe tại C:\Users\XXX\AppData\Local\Temp\ABCD.temp. Với A, B, C, D có thể là ký tự in hoa hoặc số
* Ta copy file b2e ra một thư mục khác để chạy OllyDebugger



* File b2e.exe tạo ra file batchfile.bat trong thư mục Temp.
* Ta copy file batchfile.bat ra để xem



* File batchfile.bat chính là file thực thi cuối cùng ta chuyến code sang C++ để có được keygen

