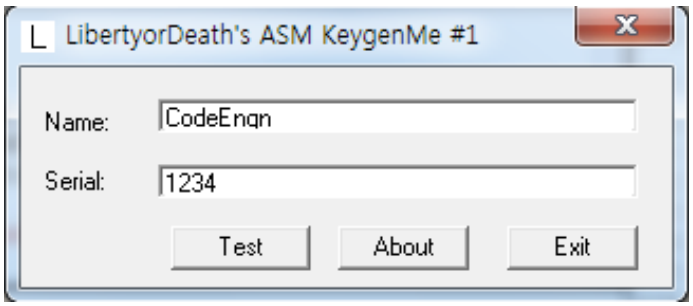
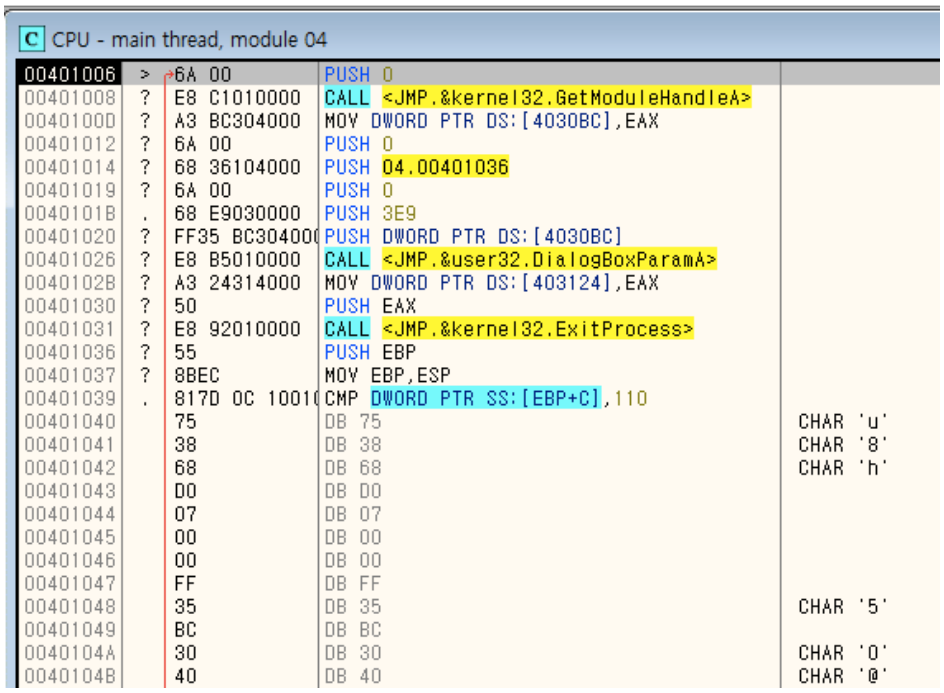
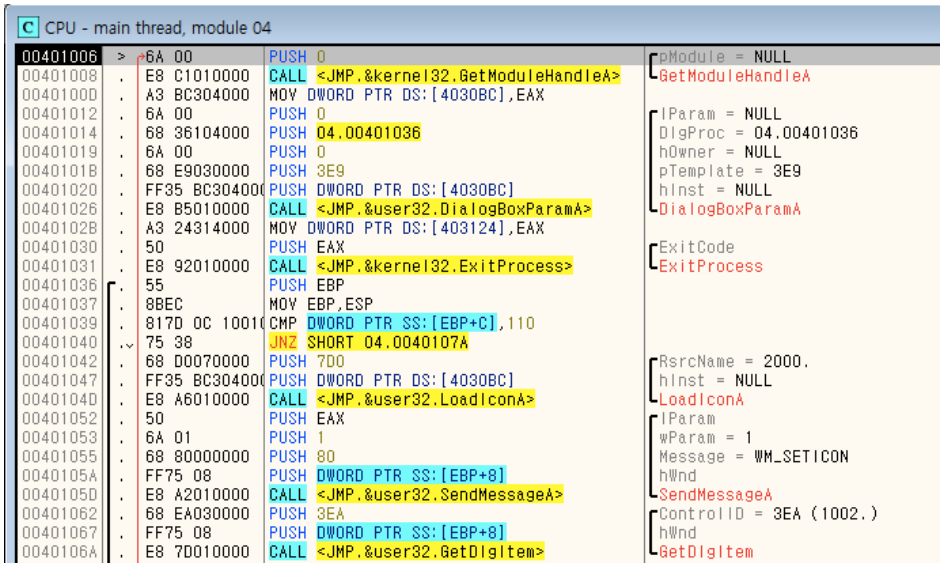


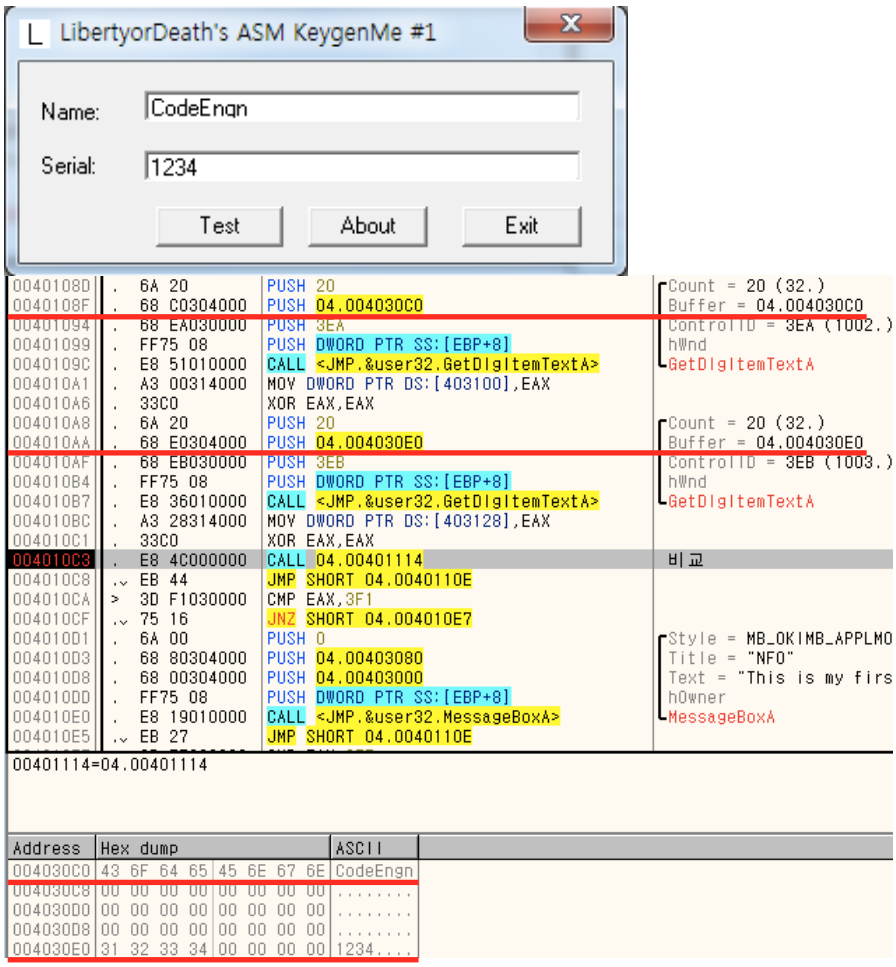
여태까지의 문제처럼 이름과 시리얼을 입력하고 이를 인증하는 프로그램입니다.



처음 프로그램을 실행하고 진행하다 보면 이렇게 나오는데 이는 Ctrl + A를 통해 해결할 수 있습니다.



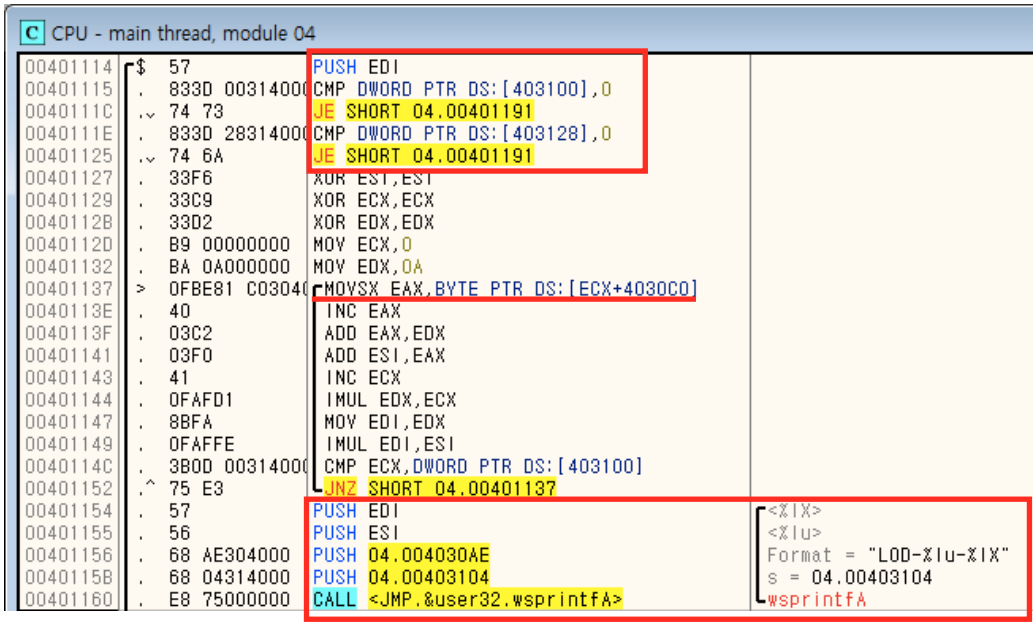
이제 분석을 시작하도록 하겠습니다.



GetDigItemText함수를 통해 이름과 시리얼을 버퍼에 저장했습니다.

그 후 주석에 비교라고 되어있는 함수콜이 보입니다.

이름을 이용해서 시리얼을 만들고 입력한 값과 비교하는 함수인데 분석해보도록 하겠습니다.



위의 네모의 부분은 이름과 시리얼이 빈칸인지 아닌지 체크하는 부분입니다.

빈칸이면 루틴을 실행하지 않고 넘어갑니다.

그 밑으로 XOR을 이용해서 초기화 하는 부분을 볼 수 있고 ECX와 EDX에 값을 집어넣습니다.

ECX는 카운팅을 위해 0을 넣고 EDX는 알고리즘에 사용하기 위해 0x0A의 값을 넣습니다.

밑줄 친 부분은 본격적인 알고리즘의 시작으로 EAX에 입력한 이름의 HEX값을 한 글자씩 넣는 부분입니다.

HEX값에 + 1을 하고 EDX와 더한 뒤 그 결과를 ESI에 저장합니다.

EDX와 ECX는 서로 곱하고 그 값을 EDI에 집어넣습니다. 최종적으로 EDI와 ESI를 곱하게 됩니다.

입력한 문자가 모두 해당 알고리즘을 지난 뒤 wsprintf를 통해 시리얼을 만듭니다.

입력값은 EDI와 ESI 두 개인데 EDI는 HEX값(%x) 그대로, ESI는 10진수(%u)로 변환되어 만들어집니다.

입력한 값과 만들어진 시리얼을 비교하고 분기하게 됩니다.