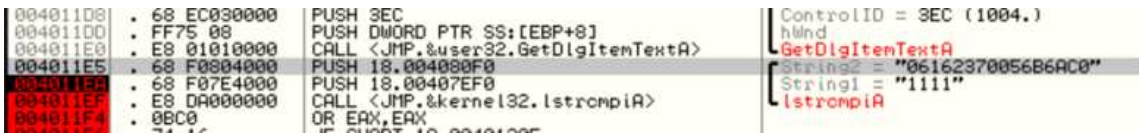
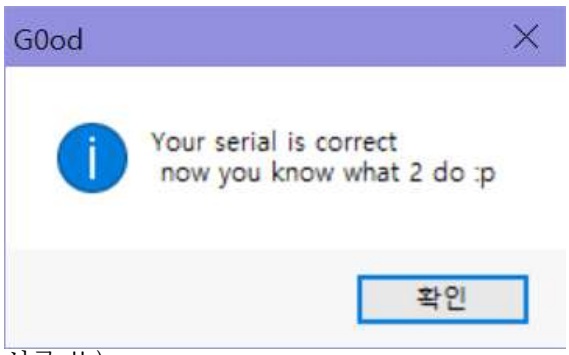
CodeEngn Basic RCE L18
: Name이 CodeEngn일때 Serial은 무엇인가

16번 문제와 비슷하게 시리얼을 찾는 문제이다.
올리디버거에 올려 all text strings 찾아서 성공메세지/오류메세지 찾아 이동하였다.

오류메세지가 성공메세지보다 위쪽에 있는 걸로 보니 성공메세지로 점프하는 명령이 있을거라고 판단을 했고, 004011F6에 JE SHORT 0040120E로 이동하는 (성공메세지) 어셈블리어가 있다. 바로 위에 있는 함수를 보니 strcmp로, 문자열을 비교하는 함수이다.



인자값이 2개가 들어가는 것이 보이는데, 1111은 실행 시 내가 넣어준 임의의 값이고, string2에는 06162370056B6AC0 문자열이 들어가고 있다. 시리얼을 비교하는 것으로 보아 0616 ~~~ 이것이 이름이 CodeEngn일 때 시리얼 넘버라는 것을 추측할 수 있다.



성공 !!:)