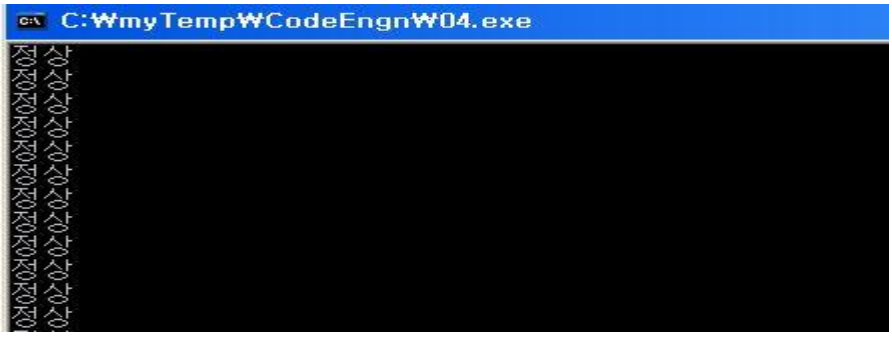
Basic 04 풀이

[문제]
이 프로그램은 디버거 프로그램을 탐지하는 기능을 갖고 있다. 디버거를 탐지하는 함수의 이름은 무엇인가

1. 프로그램 실행하여 기능 확인

04.exe를 실행시키면 아래와 같이 나온다.

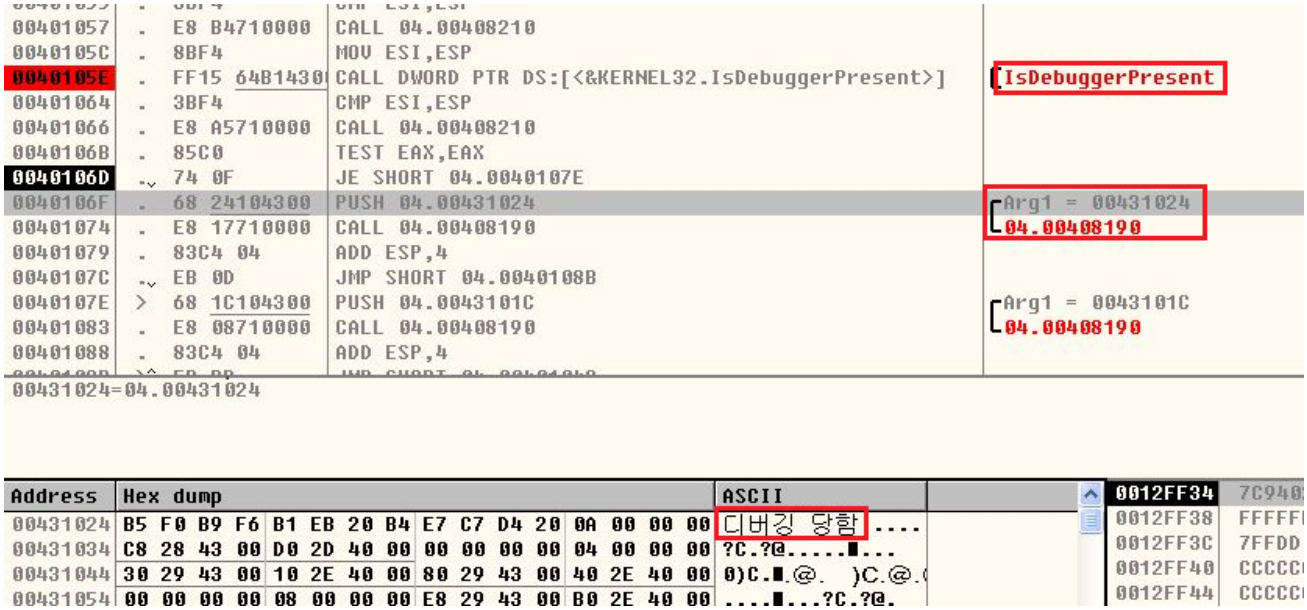


하지만 OllyDbg를 통해서 실행시키면 아래와 같이 '디버깅 당함'이라고 나온다. 프로그램이 디버깅을 당하고 있는지 탐지하는 기능을 가지고 있다.

2. Step by Step

프로그램을 순차적으로 진행해 나가면서 특정 함수를 호출후 '정상' 또는 '디버깅 당함' 문자열을 출력하는 분기점을 발견하였다.

아래 그림에서 IsDebuggerPresent 함수 호출후 출력문의 분기가 이루어 지는 것을 확인할 수 있다.



따라서 이번 문제의 답은 IsDebuggerPresent 이다.

- End -