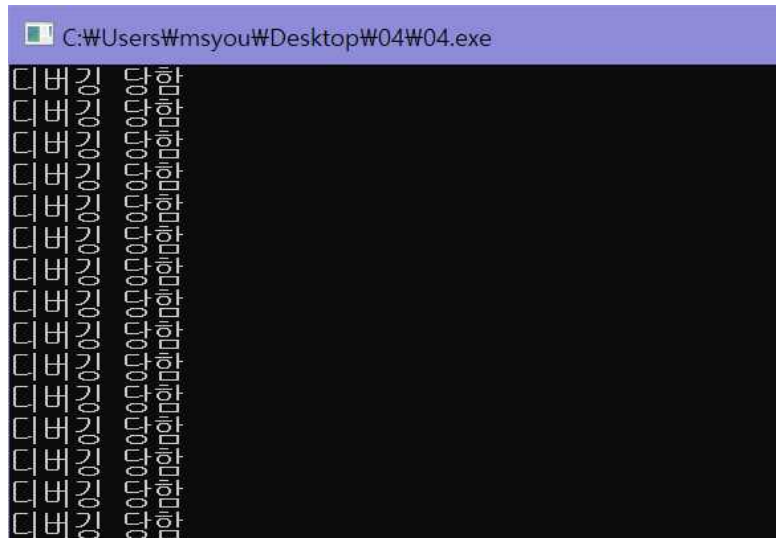
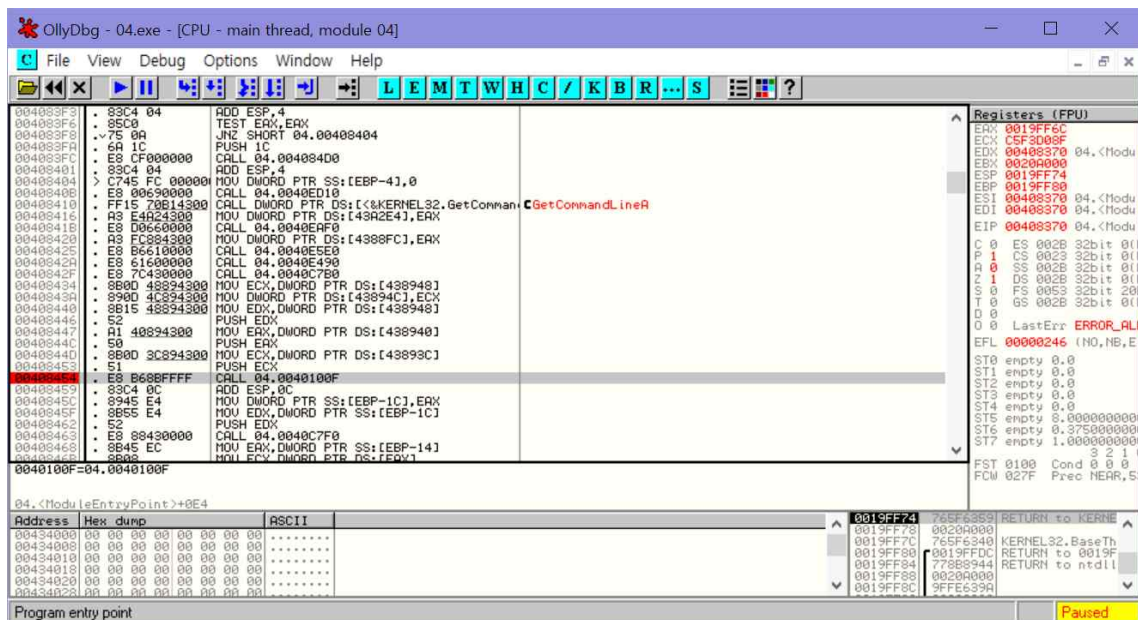


## CodeEngn Basic RCE L04

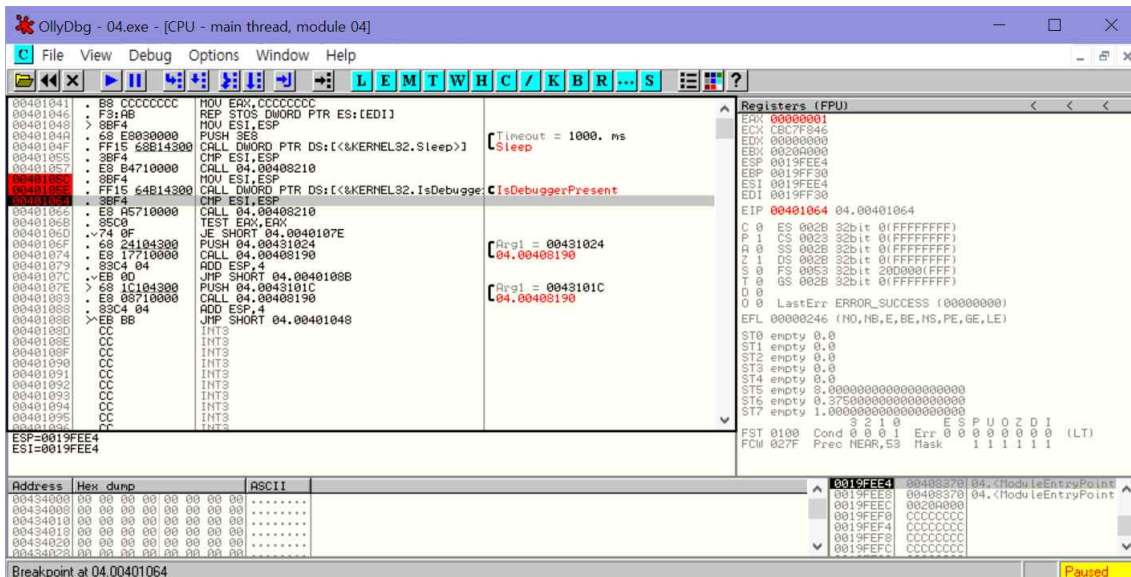
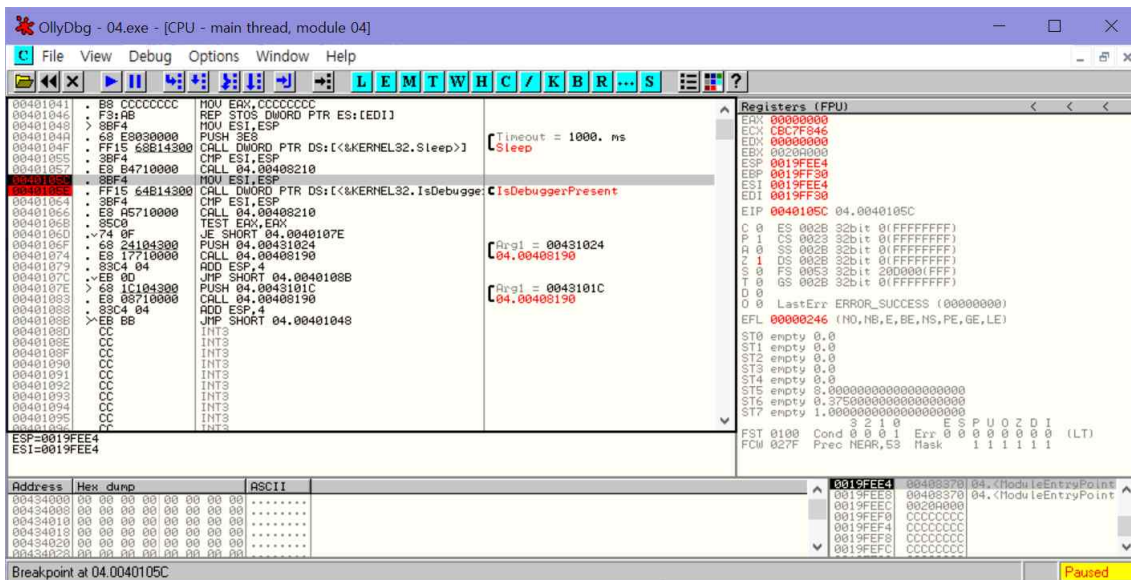
: 이 프로그램은 디버거 프로그램을 탐지하는 기능을 갖고 있다. 디버거를 탐지하는 함수의 이름은 무엇인가



올리디버거를 열어서 ctrl+f8눌러서 실행하면 디버깅 당함이라고 나오고,



멈춘 주소에 f2를 눌러 break point를 걸어주고 엔터를 눌러서 들어간다.



내리다 보면 isDebuggerPresent라는 디버거 함수가 보인다. 디버거를 탐지하는 함수로, 탐지하면 0이 아닌 값을 리턴, 탐지하지 못하면 0을 반환한다. 전후로 bp를 걸어주고 실행시키면 EAX의 값이 0->1로 바뀌는 것을 볼 수 있다. 따라서 바뀐 EAX를 0으로 설정하여준다.



다음과 같이 디버깅 당함이 아니라 정상으로 출력되는 것을 볼 수 있다.