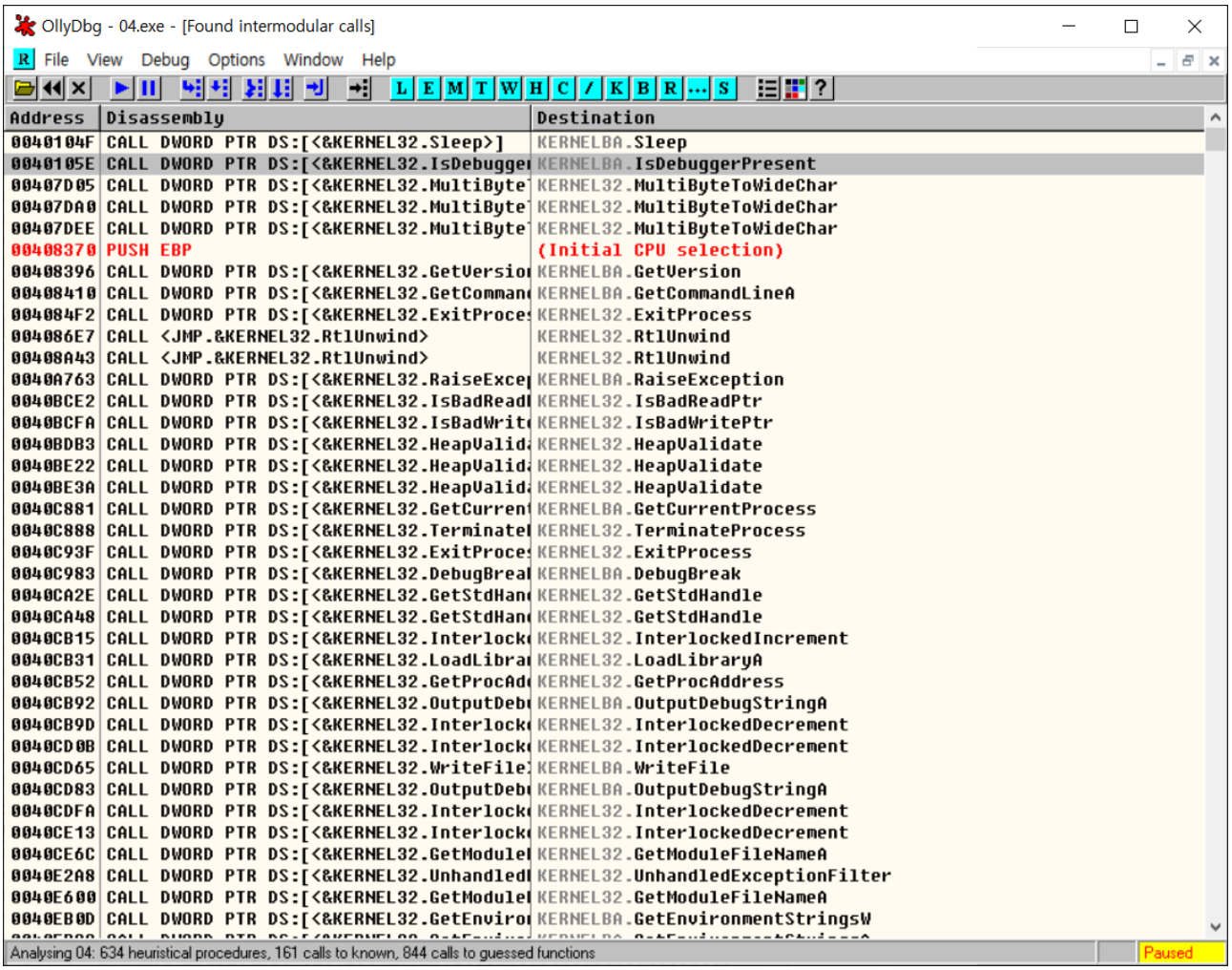
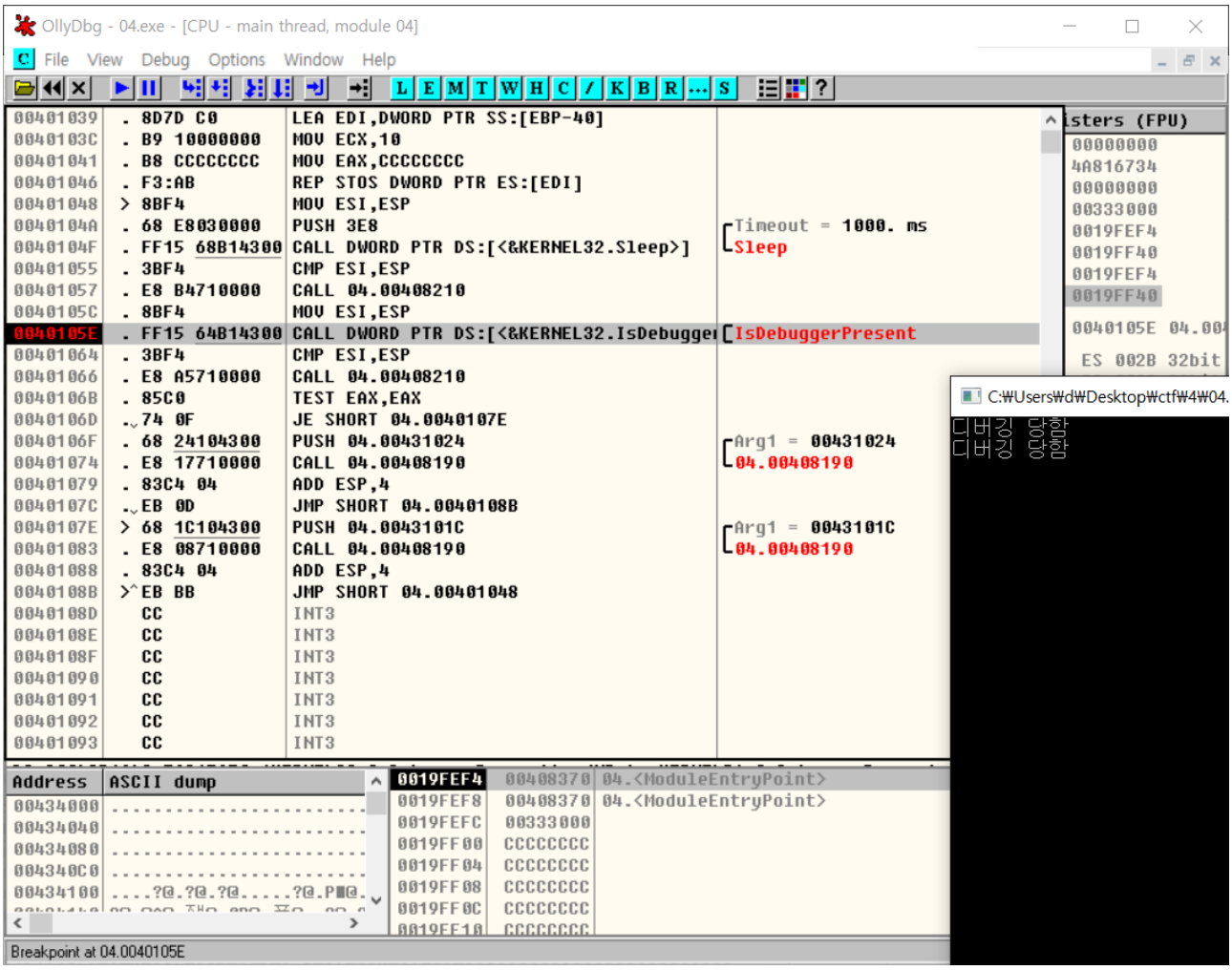
[CodeEngn]

Basic RCE L04



? 가 디버거를 탐지하는 함수라고 한다.

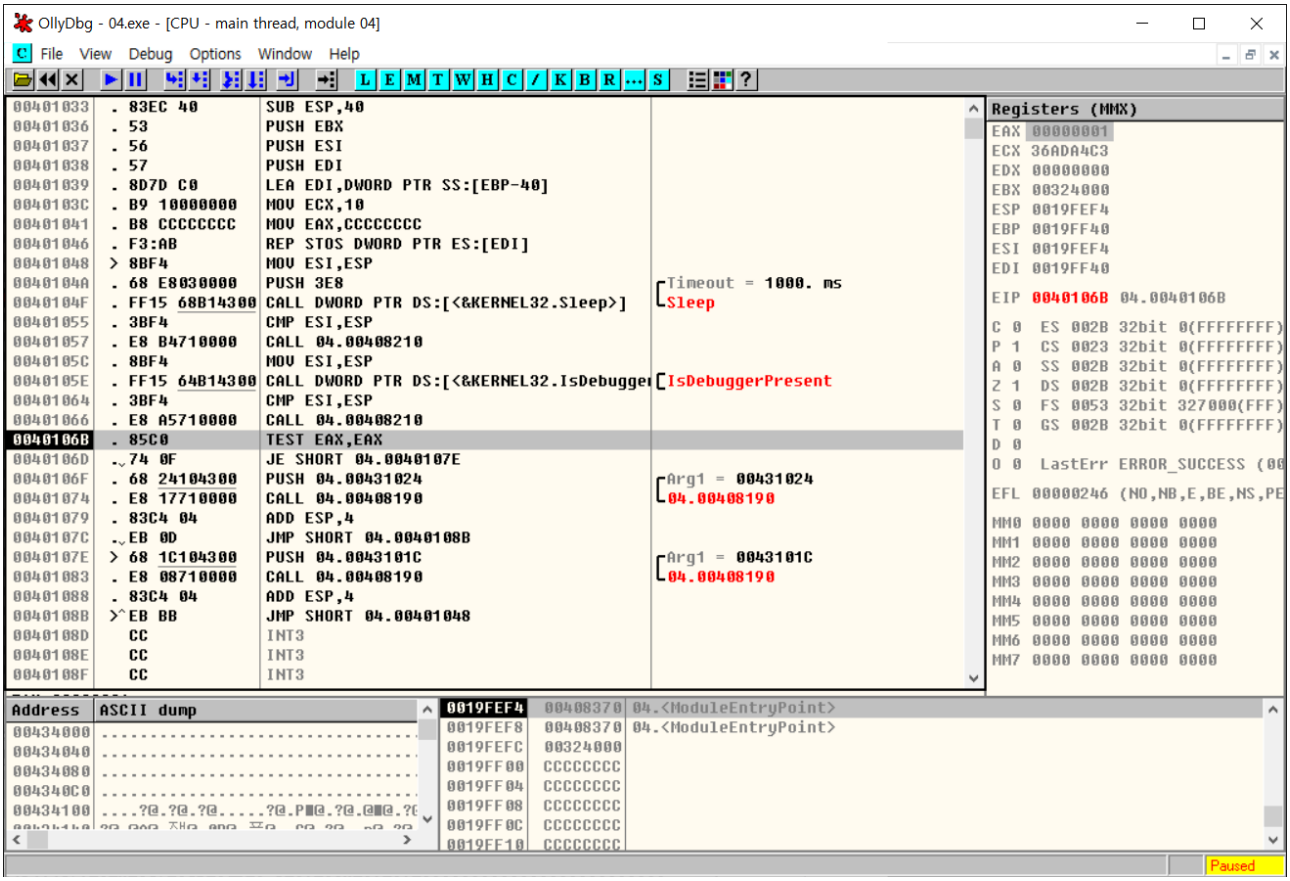
== 번외편 ==



40105E 에 break 를 걸어서 테스트를 해보았다.

자동 실행 버튼을 누를때마다 디버깅당함이라는 텍스트가 나왔다.

이 IsDebuggerPresent() 는 디버거 당할때는 반환값 1, 아닐 경우에는 리턴값 0 을 반환해준다.



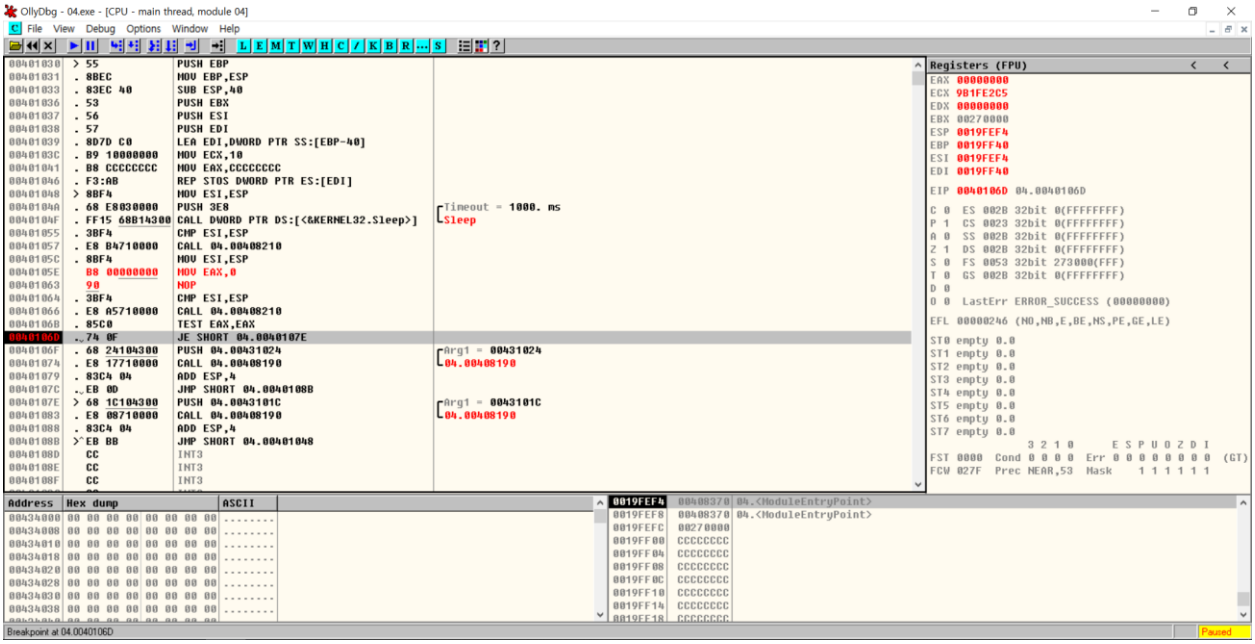
현재 디버거를 실행한 상태여서, EAX 에 1 이 들어간 것을 확인할 수 있다.

그리고 TEST EAX, EAX 가 있는데,

EAX + EAX 해서 나온 결과 값이 2 이다, 그리고 ZF 는 0 set 이 되고,

JE 조건이 맞지 않기 때문에, 40106D 로 가게 된다.

그러면, 디버깅당함이라는 문자열이 나오게 된다.

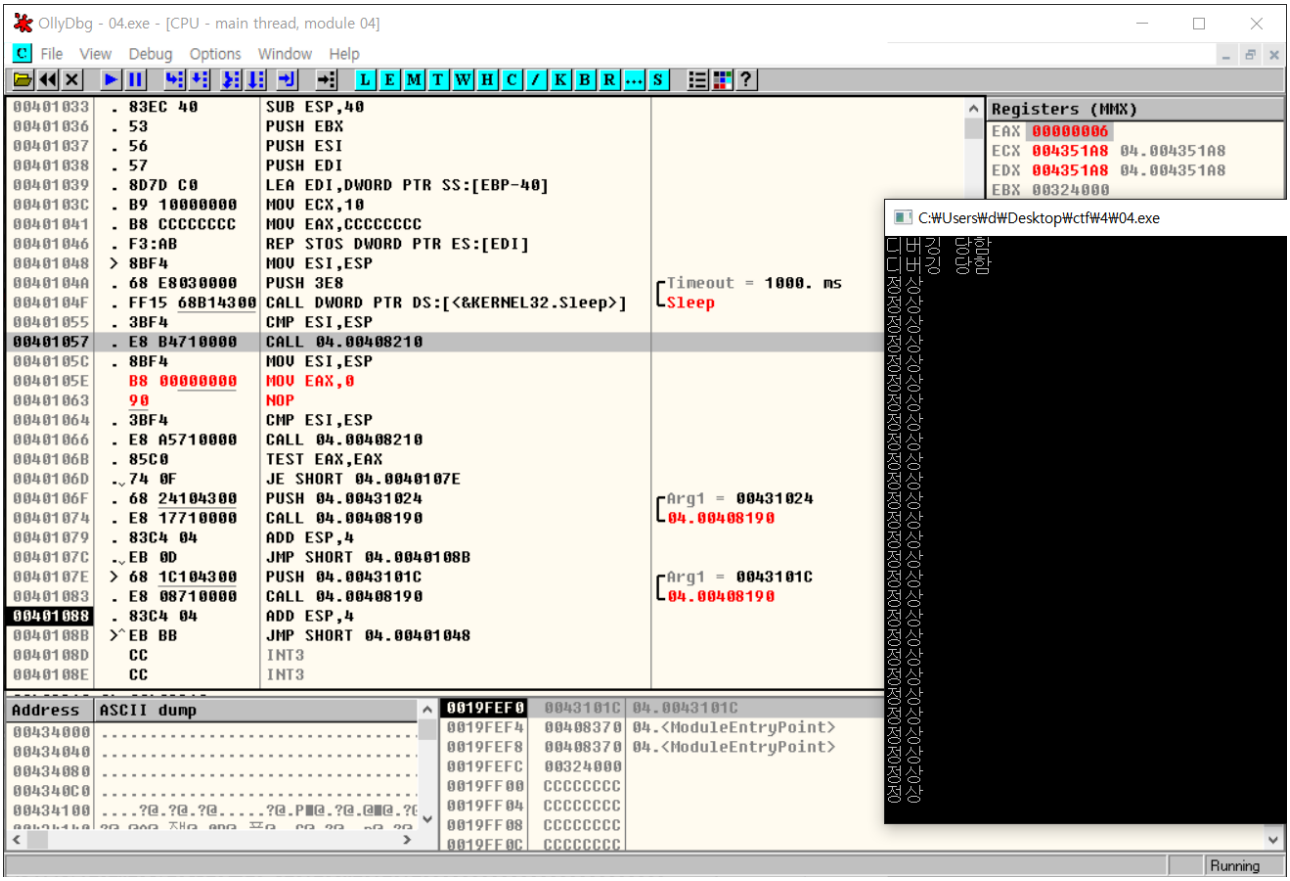


IsDebuggerPresent()에 반환값을 강제로 0 으로 설정하고 난 뒤에 결과이다.

TEST EAX, EAX 에 결과는 0 이다.

즉, ZF 가 1 set 이 되고,

때문에, 40107E 로 점프하게 되고, “정상” 이라는 문자열이 나타나게 된다.



IsDebuggerPresent() 우회 성공이다.