Anti_Baek

주어진 프로그램을 실행하면

다음과 같은 버튼이 나온다 'NO'를 누르면 프로그램이 종료되고 YES를 누르면

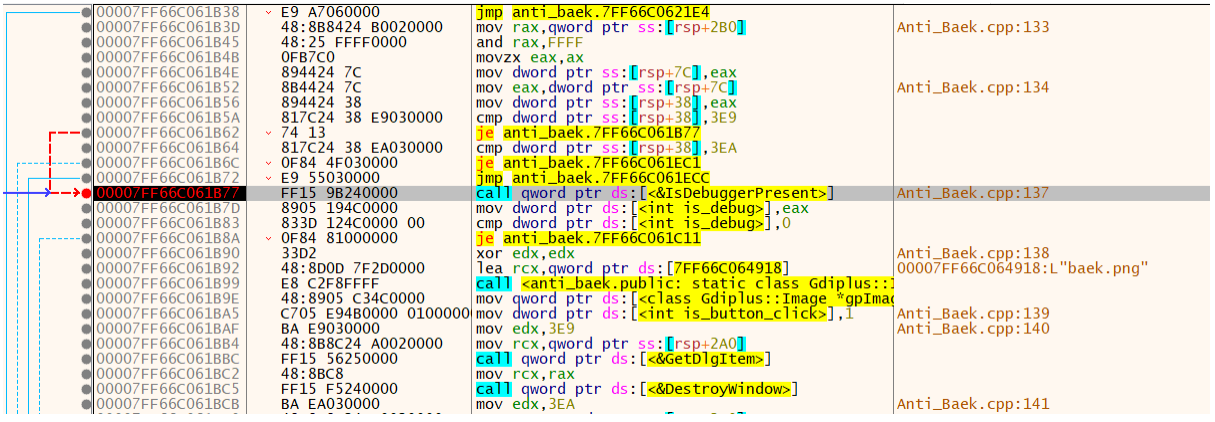
합격이라는 사진이 등장한다.

이제 디버거로 실행을 해서 YES를 누르면

영역을 전개한 백종원이 나온다. 우리는 영역에 당한것이다...

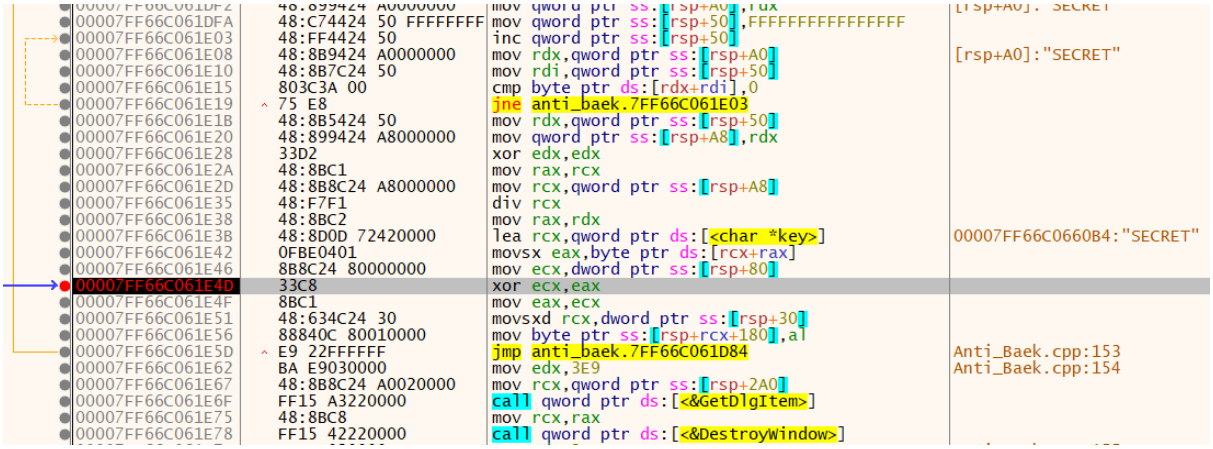
디버거로 실행하면 다른 사진이 등장하므로 안티 디버깅 기법이 있다는 것을 알 수 있다.

힌트로 주어진 IsDebuggerPresent 함수를 찾아보면

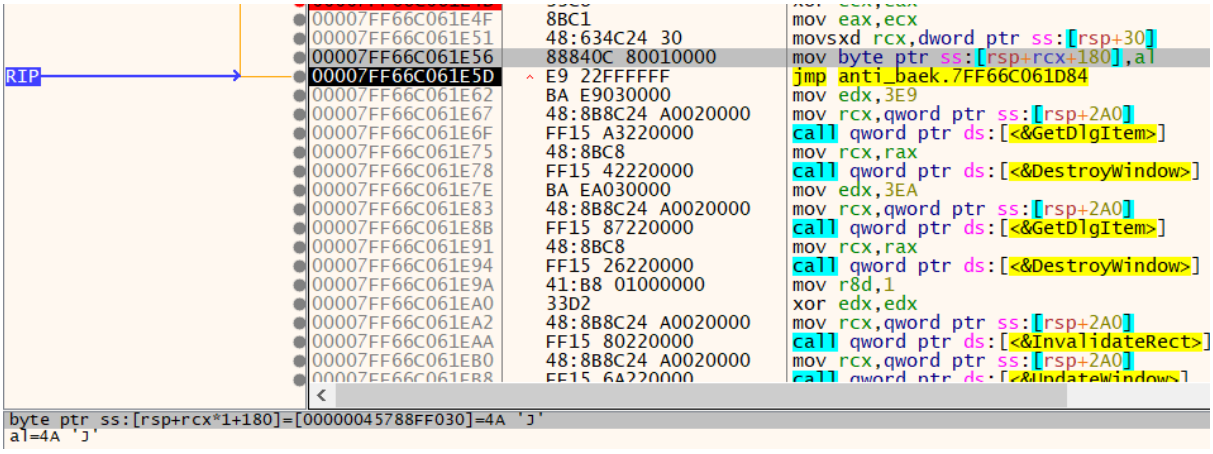


해당 위치에 존재하고 이 결과값(eax)을 1 → 0으로 바꿔주면 안티디버깅이 우회가 된다.

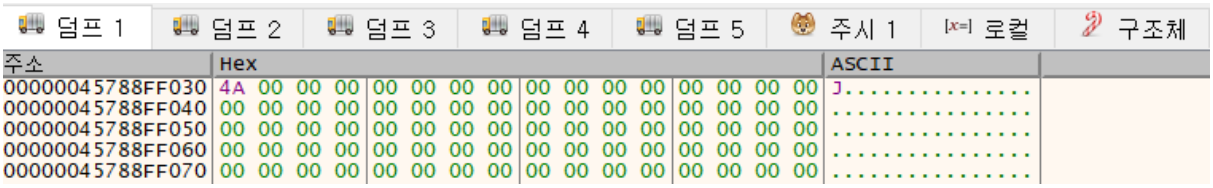
이후 그대로 실행을 해보면



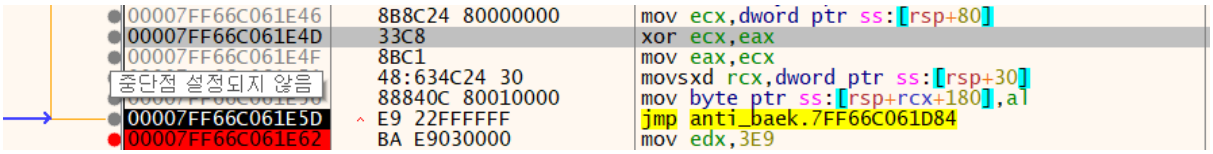
SECRET이라는 문자열과 xor을 하는 부분이 보이고



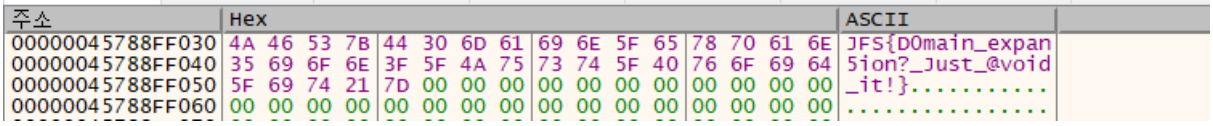
그 값을 특정 메모리에 저장을 한다.



이 메모리 위치를 보면 xor 결과인 J가 들어있으므로 반복 루틴이 끝나는 지점에 break point를 걸고



실행 결과인 메모리를 확인해보면 FLAG를 얻을 수 있다.




```
FLAG : JFS{D0main_expan5ion?_Just_@void_it!}
```