

REPORT:

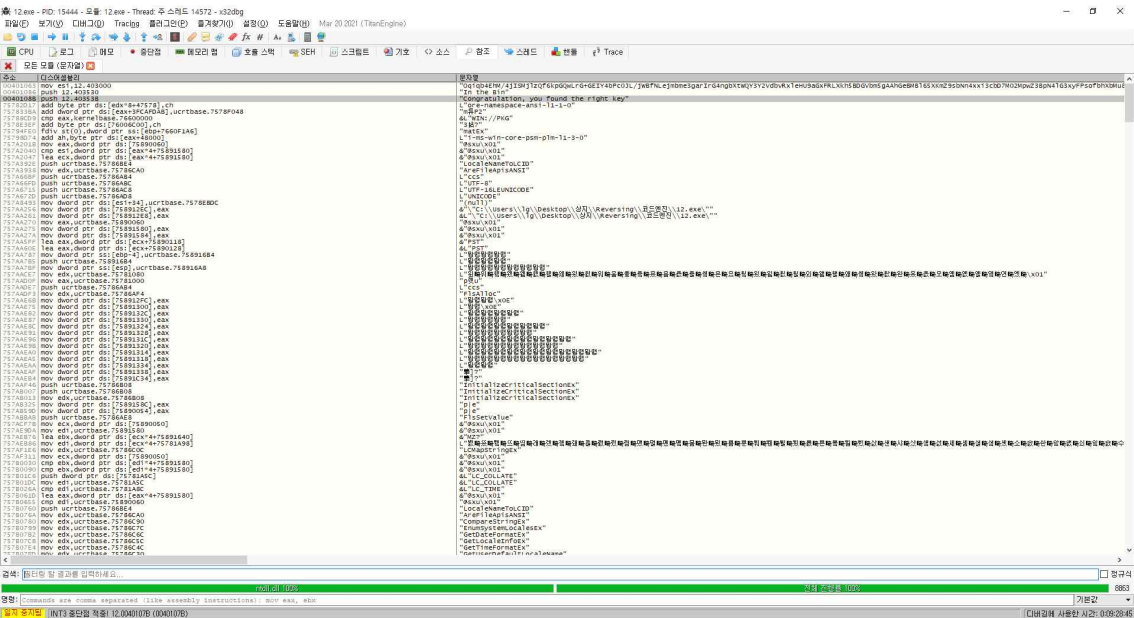
코드엔진 Basic

RCE 12 Writeup

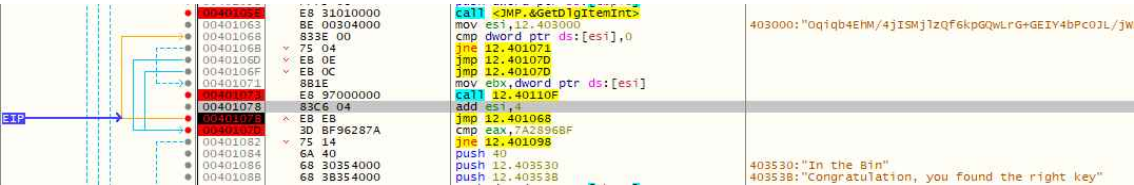
COLONY
1824275 정상지

2021.07.24

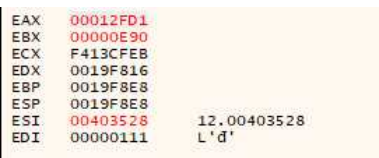
Key값과 + 주소영역을 찾으시오



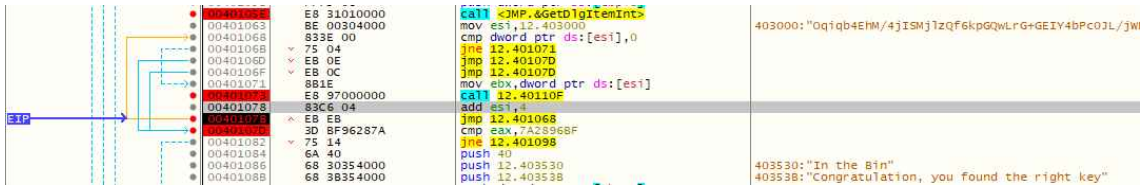
문자열 참조를 통해 해당 위치 확인후



분기문 이전의 코드에서 일어나는 일을 알아보기 위해 중단점 설정



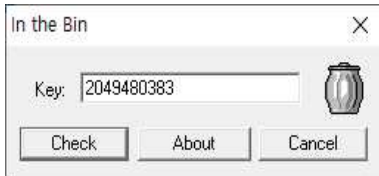
해당 디버깅 시 dec값을 hex값으로 변경하는 것을 알 수 있다



분기문에서는 eax의 값과 7A2896BF와 비교하는 구문이 있는데 해당 값이 되기위한 dec값을 계산기를 통해 구해보면



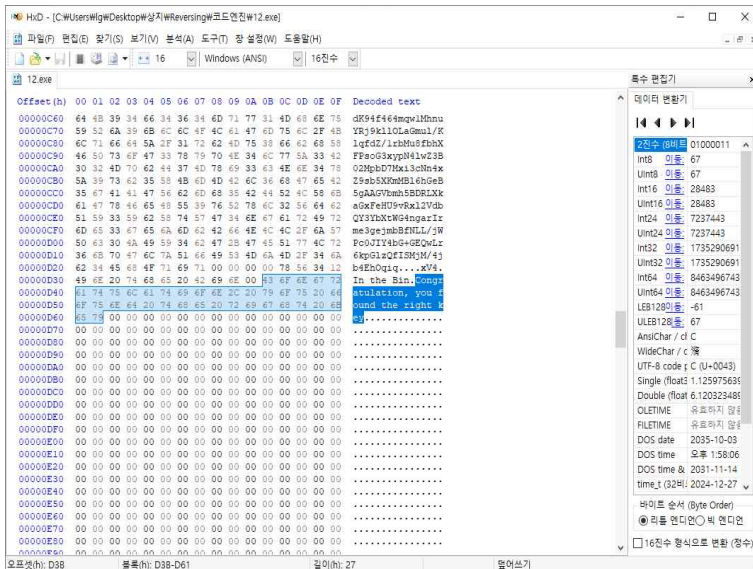
2049480383이다



해당 값을 넣고 실행시키면



메시지 박스가 나온 것을 볼 수 있다



HxD에서 프로그램을 열어 메시지 박스 내의 내용을 수정한다

00000D30	49 6E 20 74 68 65 20 42 69 6E 00 32 30 34 39 34	In the Bin.20494
00000D40	38 30 33 38 33 00 00 00 00 00 00 00 00 00 00	80383.....
00000D50	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000D60	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000D70	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000D80	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000D90	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

해당 주소 값은 0x0D3B~0x0D61이다

따라서 답은 20494803830D3B0D61 이다