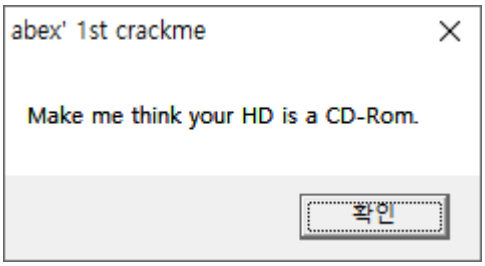
CodeEngn Basic RCE

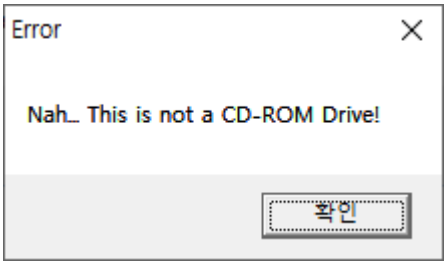
1. Level 01

Basic RCE L01

HDD를 CD-Rom으로 인식시키기 위해서는 GetDriveTypeA의 리턴값이 무엇이 되어야 하는가



"너의 HD 를 나의 CD-ROM 으로 생각하게 만들어라"



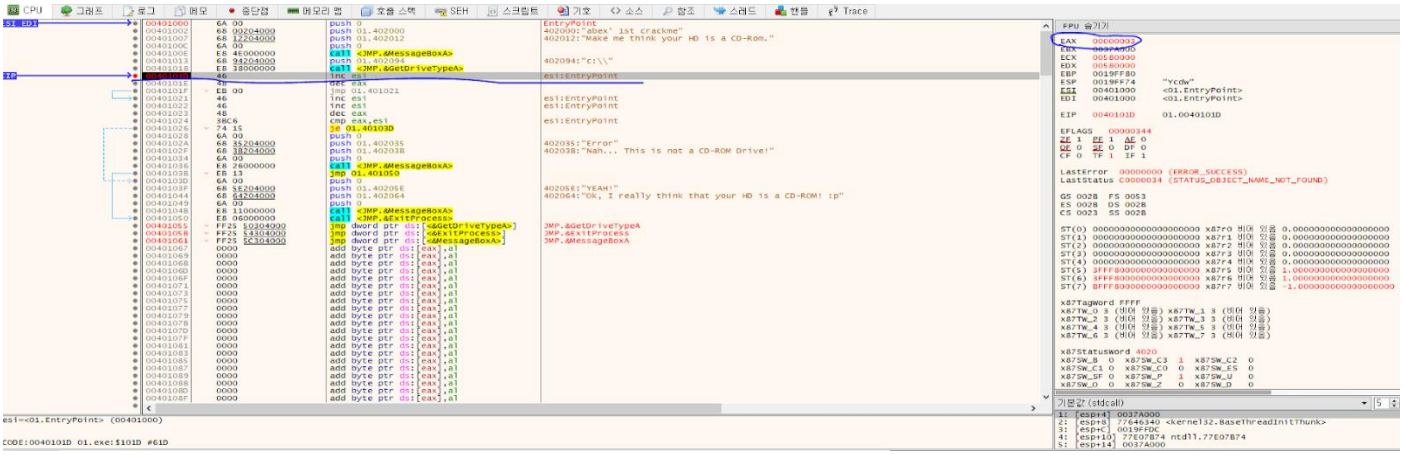
"어쨌든... 이건 CD-ROM 이 아니다!"

```
00401000   6A 00          push 0                  EntryPoint
00401002   68 00204000    push 01.402000          402000:"abex' 1st crackme"
00401007   68 12204000    push 01.402012          402012:"Make me think your HD is a CD-Rom."
0040100C   6A 00          push 0
0040100E   E8 4E000000    call <JMP.&MessageBoxA>
```

Entrypoint 후 프로그램에 "Make me think yout HD is a CD-Rom" text 와 "abex' 1st crackme" caption 인자를 전달함. WIN API MessageBoxA 함수 호출.

```
00401013   68 94204000    push 01.402094          402094:"C:\\"
00401018   E8 38000000    call <JMP.&GetDriveTypeA>
```

push 01.402094 부분은 함수호출을 위해 인자(C:₩₩)를 전달해준거고 그 다음 GetDriveTypeA 라는 WIN API 함수가 호출됨. 이 함수의 리턴값은 eax 레지스터에 저장됨.



GetDriveTypeA 함수를 호출한 다음구문에 BreakPoint 를 걸고 실행을 해보면 EAX 레지스터에 GetDriveTypeA 의 반환값이 들어있음.

```
ESI   00401000
```

inc esi 는 피연산자에 1 을 더함. 이 구문이 실행되고 나서 피연산자는 esi 가 되고 1 을 증가시키면 00401001.

```
0040101E    48          dec eax
```

dec 옵코드는 inc 와 반대로 피연산자에서 1 을 뺌. 위에서 eax 의 값이 3 인걸 확인했으니 이 구문이 실행되면 eax 의 값은 2 가 됨.

```
0040101F    EB 00       jmp 01.401021
00401021    46          inc esi          esi:EntryPoint
00401022    46          inc esi          esi:EntryPoint
00401023    48          dec eax
00401024    3BC6        cmp eax,esi      esi:EntryPoint
```

jmp 는 피연산자 위치로 이동. 01.401021 의 위치는 다음구문인 inc esi 임.

inc esi 에서는 00401001 에서 1 을 더해준 값인 00401002. 마지막 구문은 똑같아서 esi 의 값은 00401003 이 됨.

```
ESI   00401003    &"abex' 1st crackme"
```

```
00401023    48          dec eax
00401024    3BC6        cmp eax,esi      esi:&"abex' 1st crackme"
00401026    74 15       je 01.40103D
```

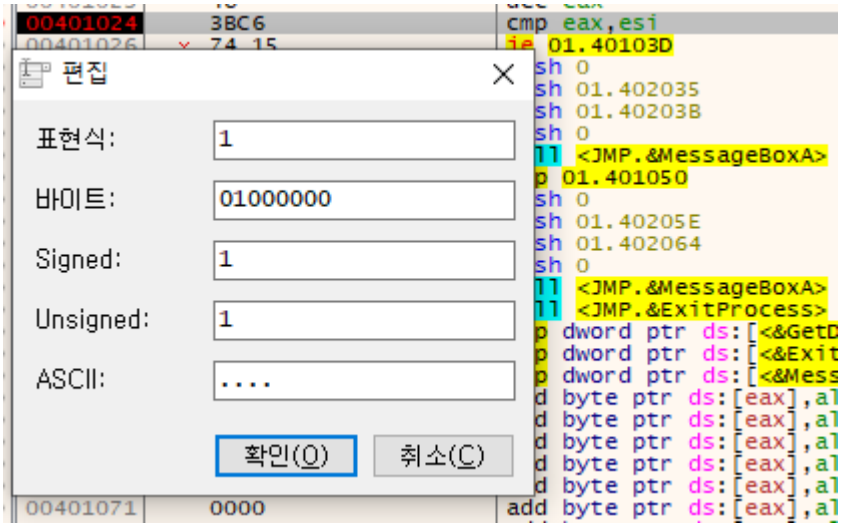
dec eax 구문실행으로 eax 의 값은 1.

그 다음 cmp 라는 옵코드(opcode)는 두 개의 피연산자의 값이 같으면 아래의 구문, je 를 통해 01.40103D 로 이동.

참이라면 01.40103D 로 이동하고 성공했다는 내용을 담고있는 WIN API MessageBoxA 함수가 호출됨.

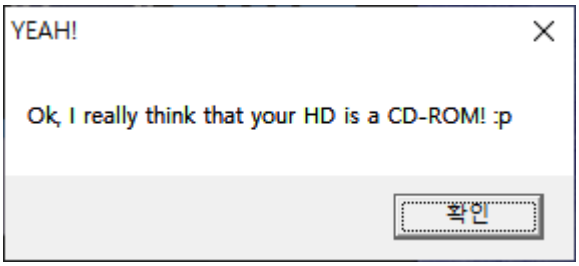
거짓이라면 실패했다는 내용을 담고있는 WIN API MessageBoxA 함수를 호출함.

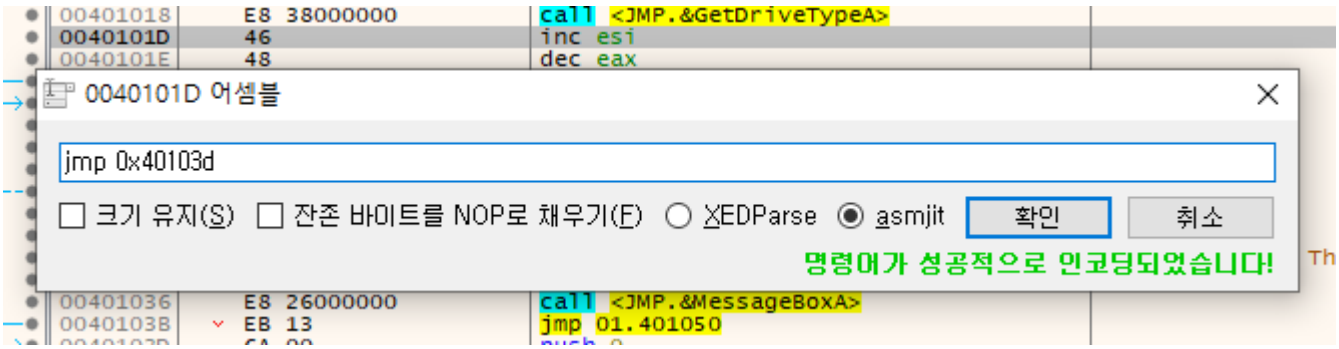
그렇기 때문에 cmp eax,esi 구문에서 거짓이 아닌 참이 되게 만들어줘야함.



두 개의 피연산자를 비교하는 구문에 BreakPoint 를 걸어두고 ESI 값과 EAX 값이 동일하게 바꿈.

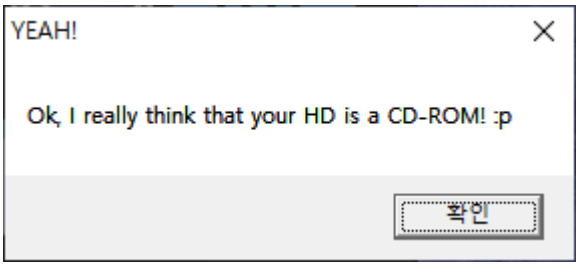
실행.





inc esi 구문 실행 전에 구문을 성공했다는 의미의 메시지박스를 출력하는 위치 이동.

inc esi 구문을 더블클릭해 jmp 0x40103d 로 이동할 위치를 써주고 확인 후 실행.



GetDriveTypeA 의 리턴값 eax = 5