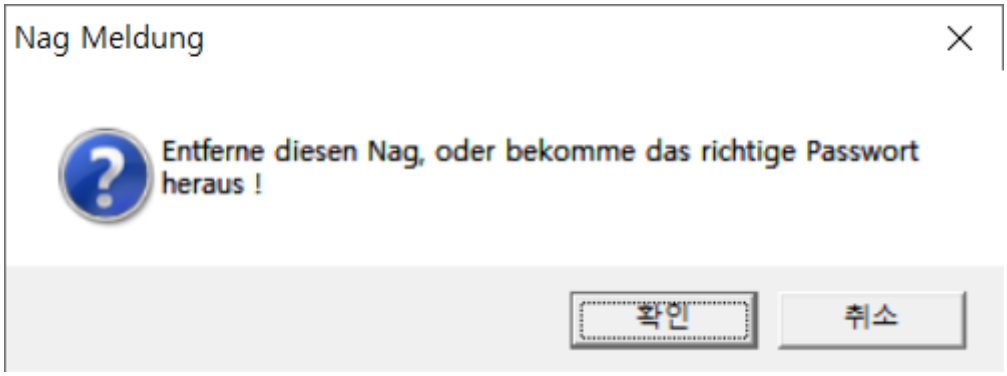
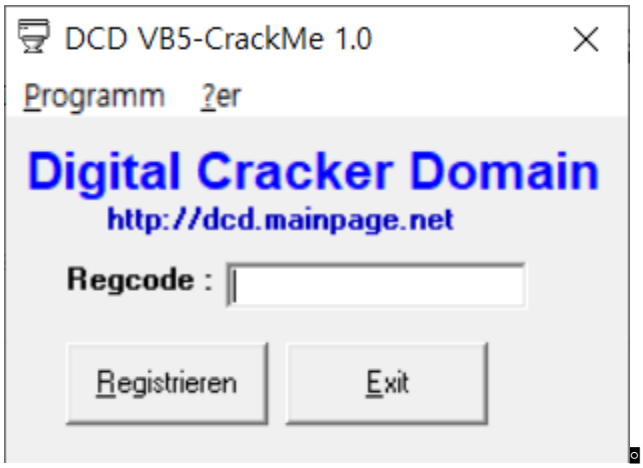
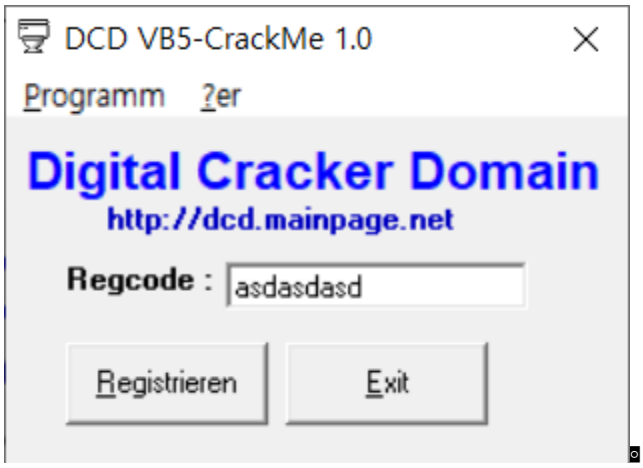
03.exe - 비주얼베이직에서 스트링 비교함수 이름은?

프로그램을 시작하면 이러한 알림창이 뜨게 되고





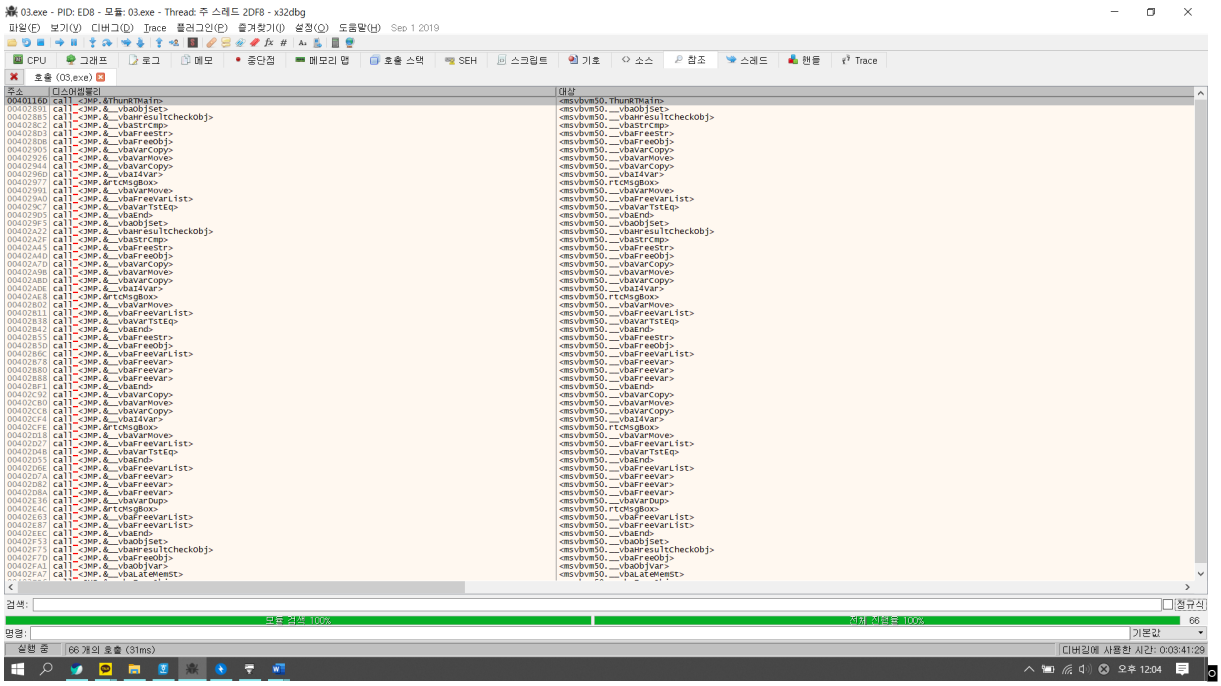
이러한 화면을 통해 Regcode에 비밀번호를 입력하여 문제에서 요구하는 “비주얼베이직에서 스트링 비교함수”를 이용하여 비밀번호가 맞는지 체크를 하여 작동하는 형식이다. 이때 X32DBG를 이용하여서 비밀번호를 입력시 발생하는 인터럽트를 체크 하여 확인 하면 된다.



아무 키값을 입력한다음 Regisrieren 버튼을 눌러 “비주얼베이직에서 스트링 비교함수”를 실행하여 인터럽트를 발생 시킨다.

위와 같은 화면이 뜨게 되고 STRING 비교를 하게 된 것을 확인 할수 있다.

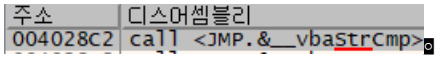
이때 X32DBG에서 인터럽트를 검색을 하여 어떤 호출이 발생했는지 검색을 한다.



다양한 인터럽트가 검색이 되어진다.

이때 String 비교함수를 찾아야 한다. 그렇기 때문에 str, string 등과 같은 키워드를 통해 검색을 해본다.

str키워드로 검색을 했을 때 이와 같이 5가지의 결과가 나오게 되는데



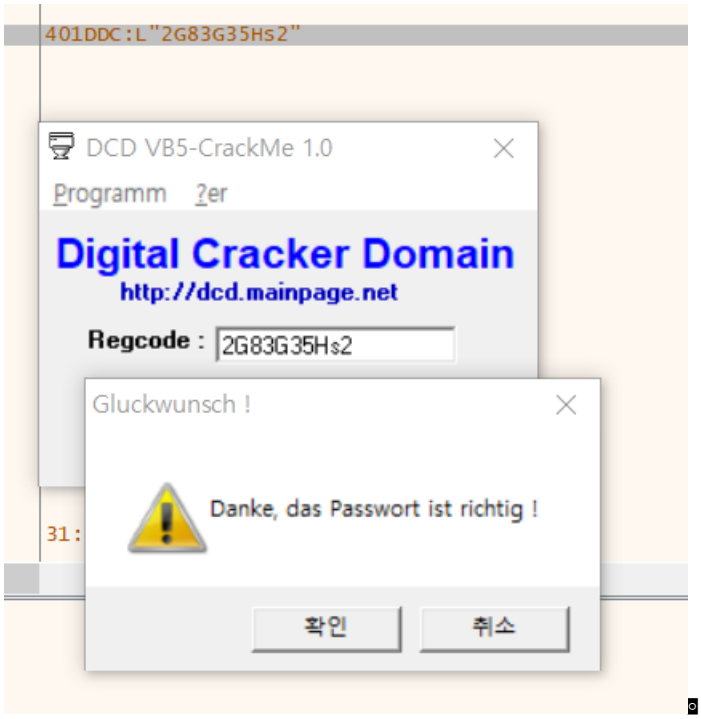
처음에 있는 vbaStrCmp가 visual basic String Compare의 약어로 추측이 된다.

들어가서 확인을 해본다.

```
0040289C    57              push edi
0040289D    8B07            mov eax,dword ptr ds:[edi]
0040289F    FF90 A0000000   call dword ptr ds:[eax+A0]
004028A5    3BC6            cmp eax,esi
004028A7    7D 11           jge 03.4028BA
004028A9    68 A0000000     push A0
004028AE    68 F41D4000     push 03.401DF4
004028B3    57              push edi
004028B4    50              push eax
004028B5    E8 84E8FFFF     call <JMP.&__vbaHresultCheckObj>
004028BA    FF75 A8         push dword ptr ss:[ebp-58]
004028BD    68 DC1D4000     push 03.401DDC                  401DDC:L"2G83G35Hs2"
004028C2    E8 83E8FFFF     call <JMP.&__vbaStrCmp>
004028C7    8BF8            mov edi,eax
004028C9    8D4D A8         lea ecx,dword ptr ss:[ebp-58]
004028CC    F7DF            neg edi
004028CE    1BFF            sbb edi,edi
004028D0    47              inc edi
004028D1    F7DF            neg edi
004028D3    E8 60E8FFFF     call <JMP.&__vbaFreeStr>
004028D8    8D4D A4         lea ecx,dword ptr ss:[ebp-5C]
004028DB    E8 52E8FFFF     call <JMP.&__vbaFreeObj>
004028E0    66:3BFE         cmp di,si
004028E3    0F84 F3000000   je 03.4029DC
004028E9    6A 08           push 8
004028EB    8D95 74FFFFFF   lea edx,dword ptr ss:[ebp-8C]
004028F1    5E              pop esi
004028F2    8D4D AC         lea ecx,dword ptr ss:[ebp-54]
004028F5    C785 7CFFFFFF 081E400 mov dword ptr ss:[ebp-84],03.401E08   401E08:L"Danke, das Passwort ist richtig !"
004028FF    89B5 74FFFFFF   mov dword ptr ss:[ebp-8C],esi
00402905    E8 22E8FFFF     call <JMP.&__vbaVarCopy>
0040290A    6A 03           push 3
0040290C    8D95 74FFFFFF   lea edx,dword ptr ss:[ebp-8C]
00402912    5B              pop ebx
00402913    8D4D DC         lea ecx,dword ptr ss:[ebp-24]
00402916    C785 7CFFFFFF 3100000 mov dword ptr ss:[ebp-84],31   31:'1'
00402920    899D 74FFFFFF   mov dword ptr ss:[ebp-8C],ebx
```

들어가 보면 위와 같이 암호로 추정이 되는 문자를 PUSH 한다음 vbaStrCmp를 Call 하고 있는 것을 볼수 있다.

이때 위에 있는 암호를 입력하여 예상이 맞는지 확인 해본다.



실제로 정확하게 동작을 하였고 비주얼베이직에서 스트링 비교함수 이름은 “vbaStrCmp”이라는 것이라는 것을 알수 있다.

정답 : vbaStrCmp