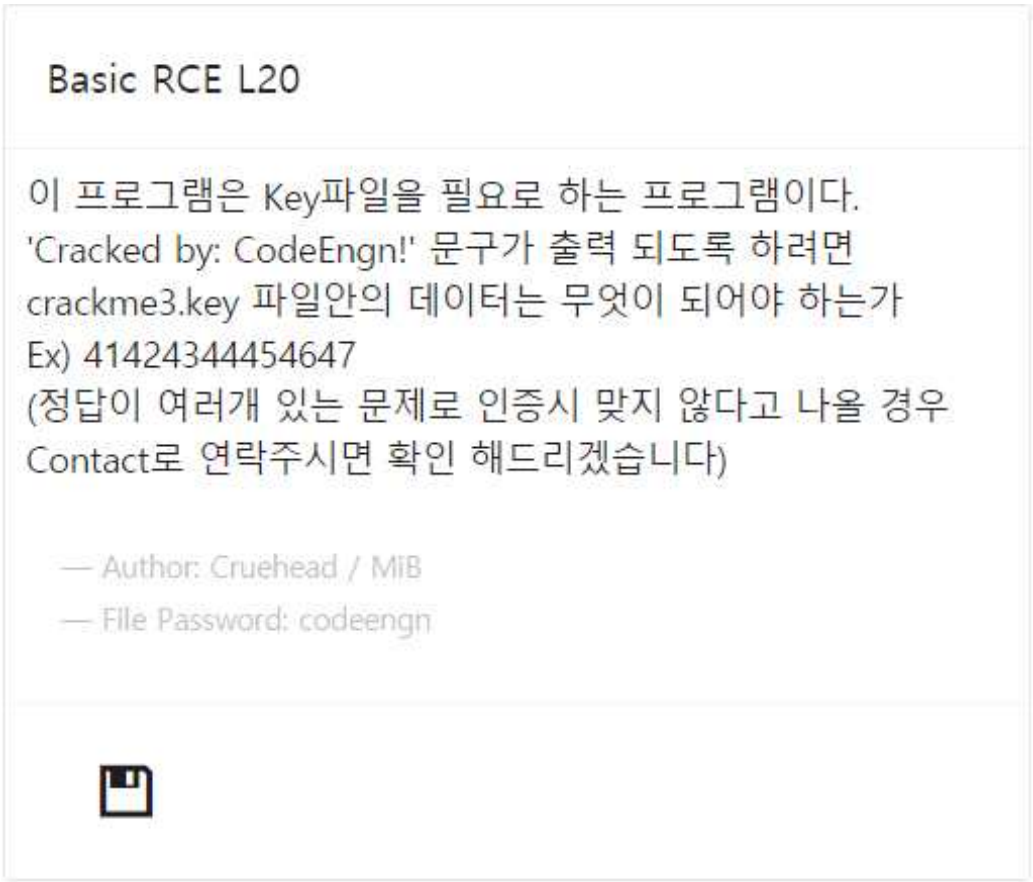
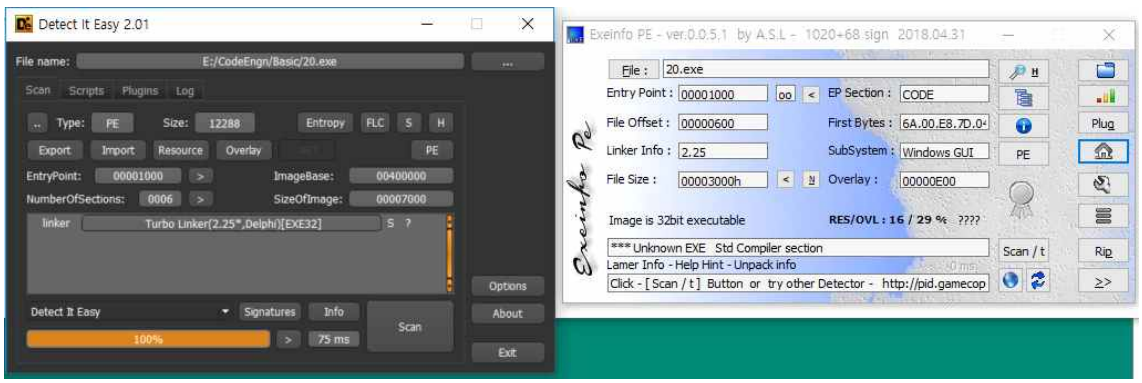
2019.02.21. CodeEngn Basic 20

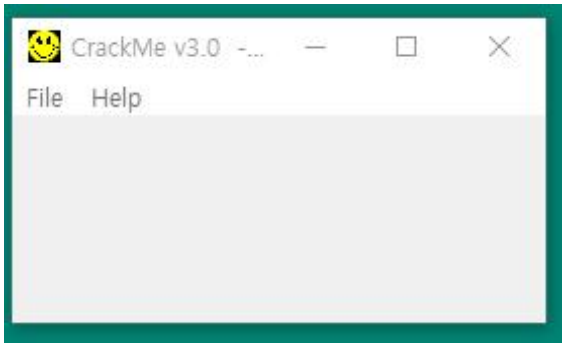
Tree to Tree



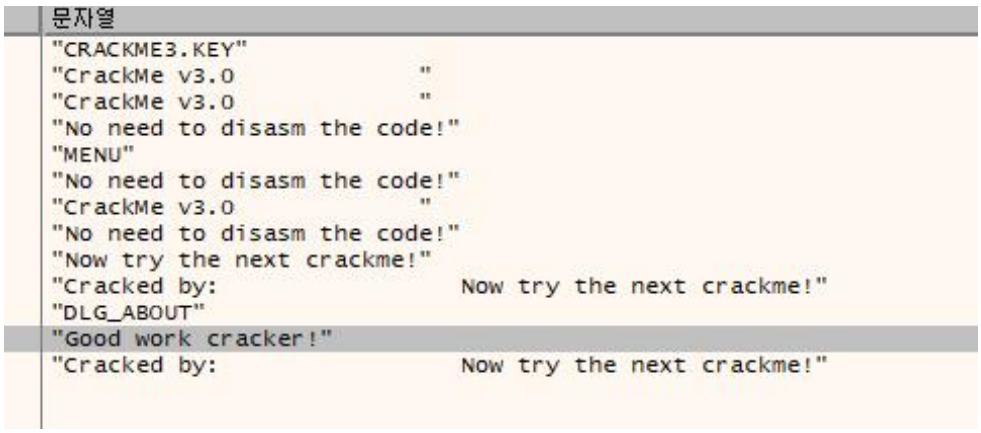
Basic 마지막 문제 패킹이 되어있지 않음



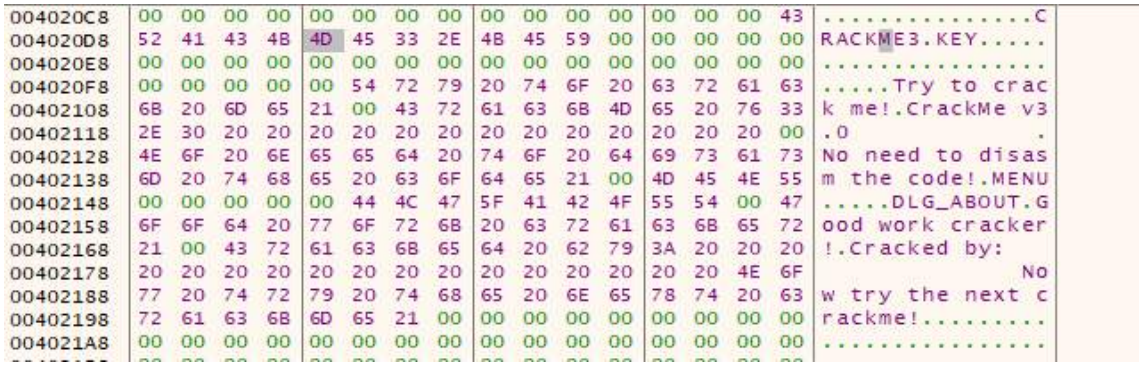
그냥실행시켰을 때 파일을 오픈하고 그런건 없음 자동실행이라고 예상



우선 문자열을 찾아보고



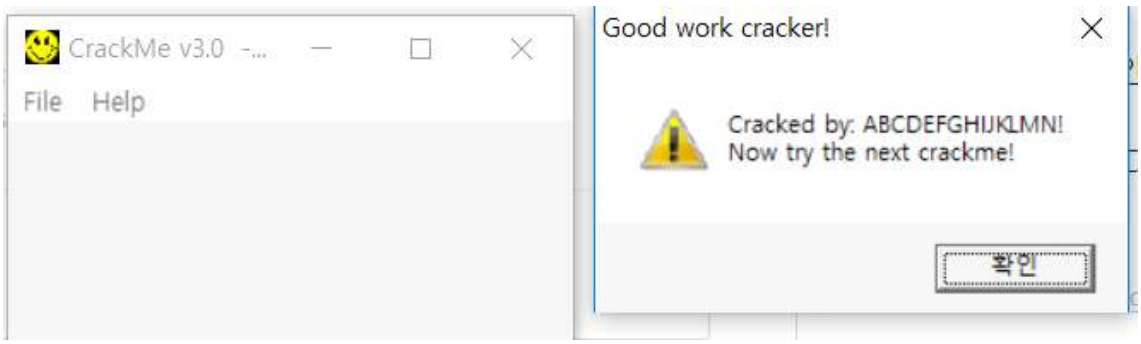
따라가다보니 파일이름은 CRACKME3.KEY



계속 트레이싱 하다보니 조건문 3개만 넘기면 창을 띄울 수 있다.

문자열 출력 방식을 알기위해 조건문을 간단한 우회로 넘기고 출력해보니

```
00401058   FF35 F5204000      push dword ptr ds:[4020F5]
00401061   E8 30040000        call <JMP.&ReadFile>
00401066   833D A0214000 12   cmp dword ptr ds:[4021A0],12
0040106D   74 C8              je 20.401037
0040106F   68 08204000        push 20.402008                    402008:"ABCDEFGHIJKLMN"
00401074   E8 98020000        call 20.401311
00401079   8135 F9204000 7856341 xor dword ptr ds:[4020F9],12345678
00401083   83C4 04            add esp,4
00401086   68 08204000        push 20.402008                    402008:"ABCDEFGHIJKLMN"
0040108B   E8 AC020000        call 20.40133C
00401090   83C4 04            add esp,4
00401093   3B05 F9204000      cmp eax,dword ptr ds:[4020F9]
00401099   0F94C0             sete al
0040109C   50                 push eax
0040109D   84C0               test al,al
0040109F   74 96              je 20.401037
004010A1   68 0E214000        push 20.40210E                    40210E:"CrackMe v3.0
004010A6   E8 9B020000        call 20.401346
```

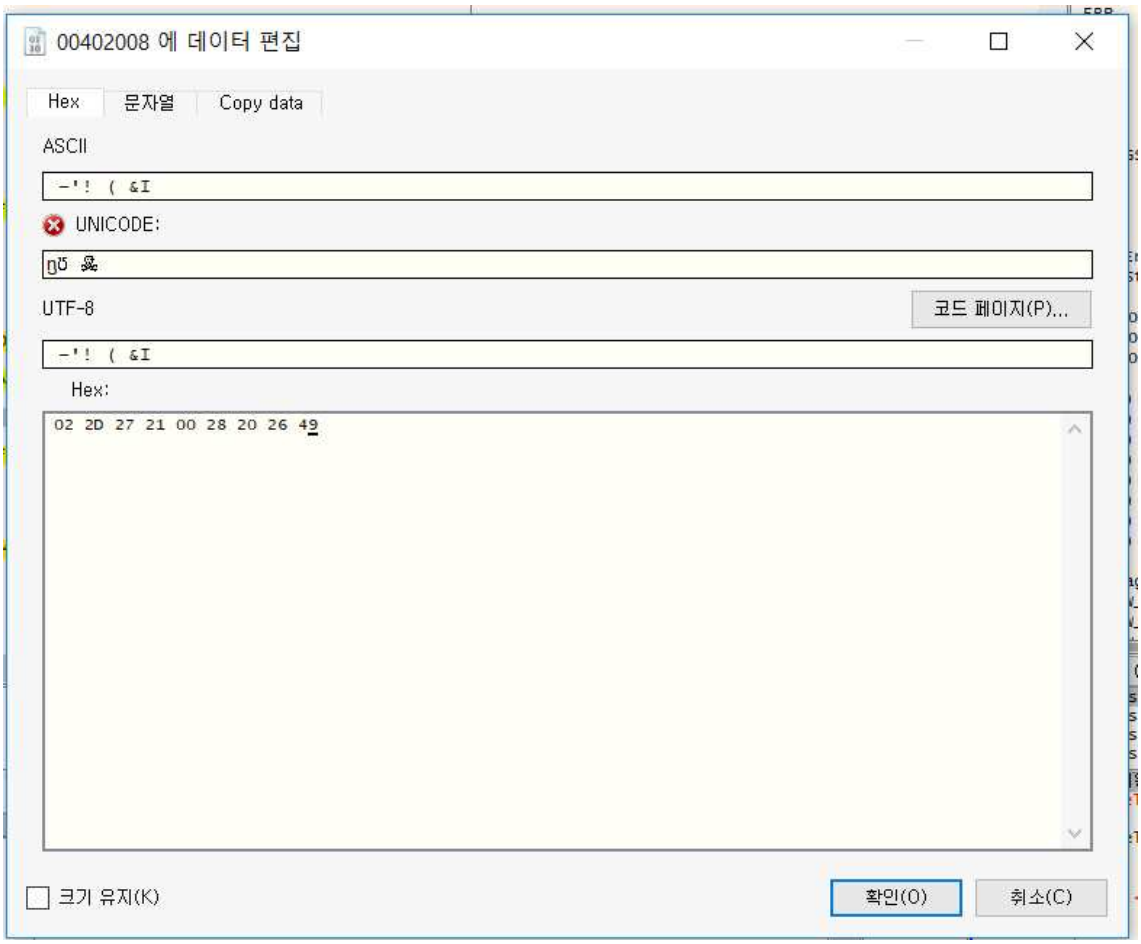


A~M까지 출력된다.

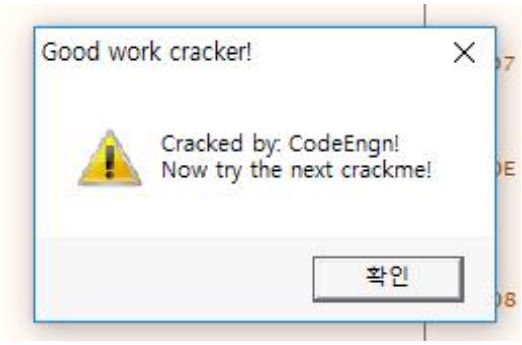
내부로 들어가보자

```
33C9                 xor ecx,ecx
33C0                 xor eax,eax
8B7424 04            mov esi,dword ptr ss:[esp+4]
B3 41                mov bl,41                                 41:'A'
8A06                 mov al,byte ptr ds:[esi]
32C3                 xor al,bl
8806                 mov byte ptr ds:[esi],al
46                   inc esi
FEC3                 inc bl
0105 F9204000        add dword ptr ds:[4020F9],eax
3C 00                cmp al,0
74 07                je 20.401335
FEC1                 inc cl
80FB 4F              cmp bl,4F                                 4F:'O'
75 E6                jne 20.401318
890D 49214000        mov dword ptr ds:[402149],ecx
C3                   ret
8B7424 04            mov esi,dword ptr ss:[esp+4]
83C6 0E              add esi,E
8B06                 mov eax,dword ptr ds:[esi]
C3                   ret
8B7424 04            mov esi,dword ptr ss:[esp+4]
83C6 0D              add esi,D
C706 202D2043        mov dword ptr ds:[esi],43202D20
C746 04 726163 6B    mov dword ptr ds:[esi+4],6B636172
C746 08 65642121     mov dword ptr ds:[esi+8],21216465
C3                   ret
8B0D 49214000        mov ecx,dword ptr ds:[402149]
8B7424 04            mov esi,dword ptr ss:[esp+4]
8B7C24 08            mov edi,dword ptr ss:[esp+8]              edi:EntryPoint
83C7 0C              add edi,C                                 edi:EntryPoint
F3:A4                rep movsb
```

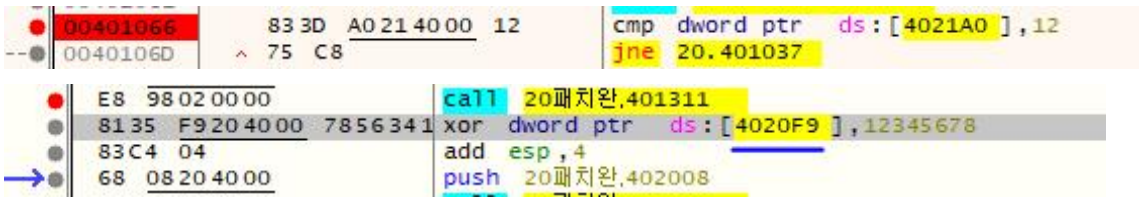
내부로 들어가서 조건을 보니 null을 만날때까지 문자 xor A++ 그리고 그 문자의 아스키코드를 중첩해서 더한다. 더한 값은 따로 저장



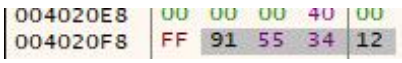
계산해보니022D272100282026 49까지하면 딱 CodeEngn이 생성됨

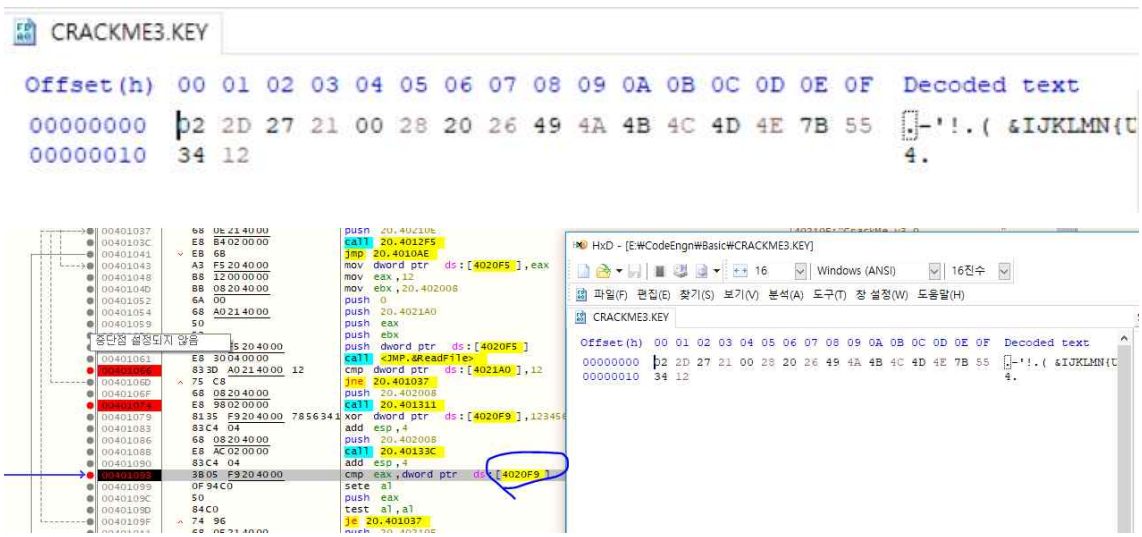


이제 CRACKME3.KEY파일을 만들어서 해보니 조건문에 걸린다.
우선 파일크기가 18byte필요 지금까지 필요한값은 9byte
9byte가 더필요하다.

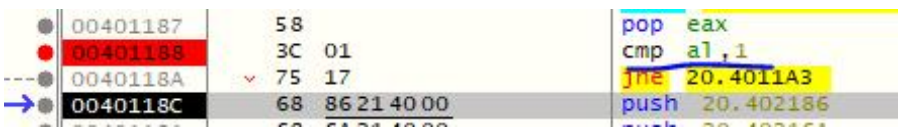


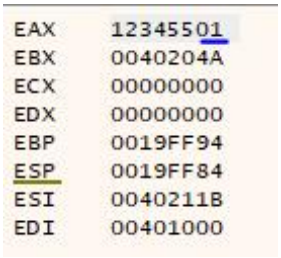
또 뒤에 4byte와 4020F9 (문자열을 만들며 헥사 값을 더한 값이 있는주소에 xor 123456788 한 값)를 비교함





004020F9 78 55 34 12





마지막에 한번 더 비교해주고 메시지창을 띄워준다.
022D27210028202649 + 잉여5byte + 7B553412
Clear