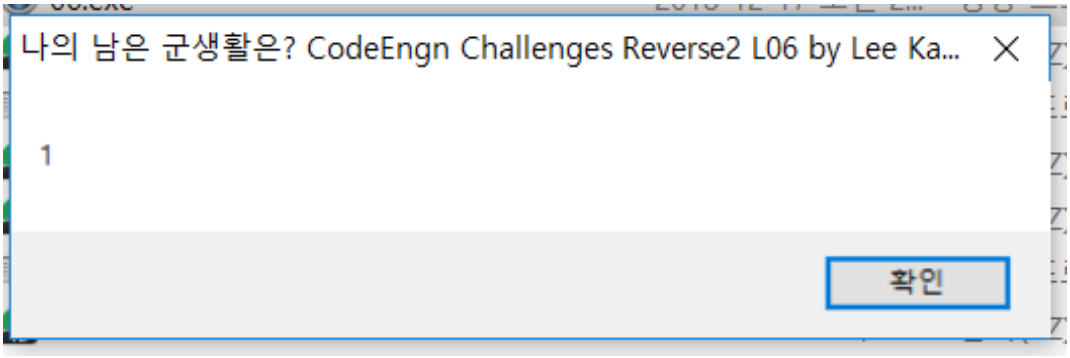
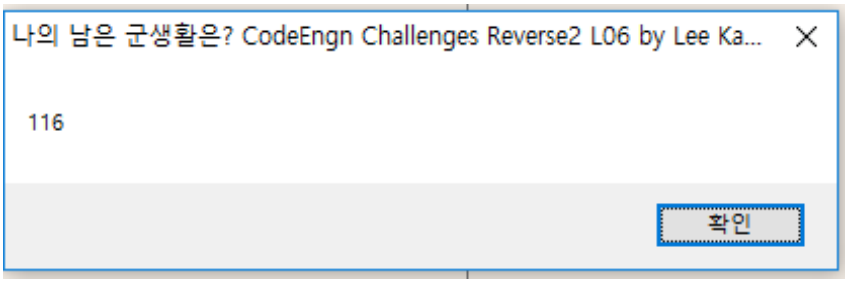
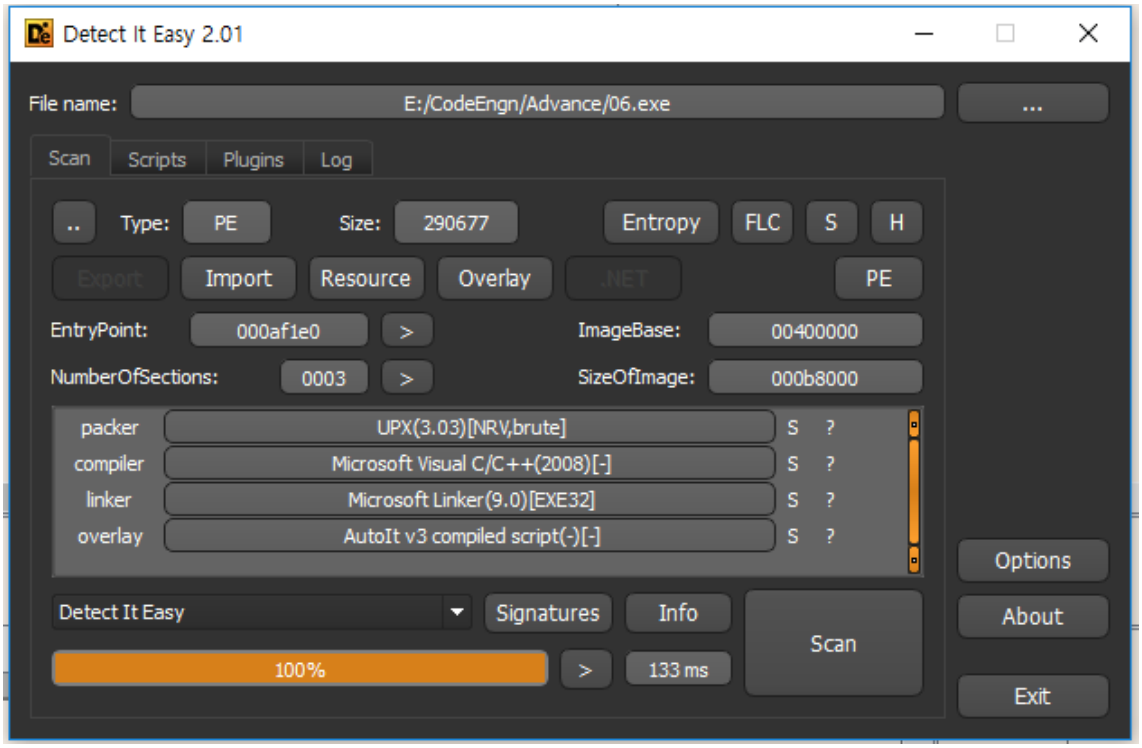
19.3.18 CodeEngn Advance 06
Tree to Tree

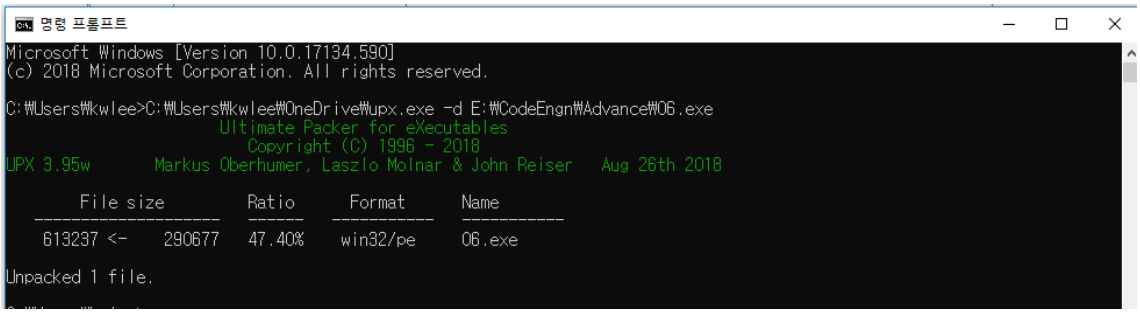


확인 누르면 숫자가 계속 올라간다.

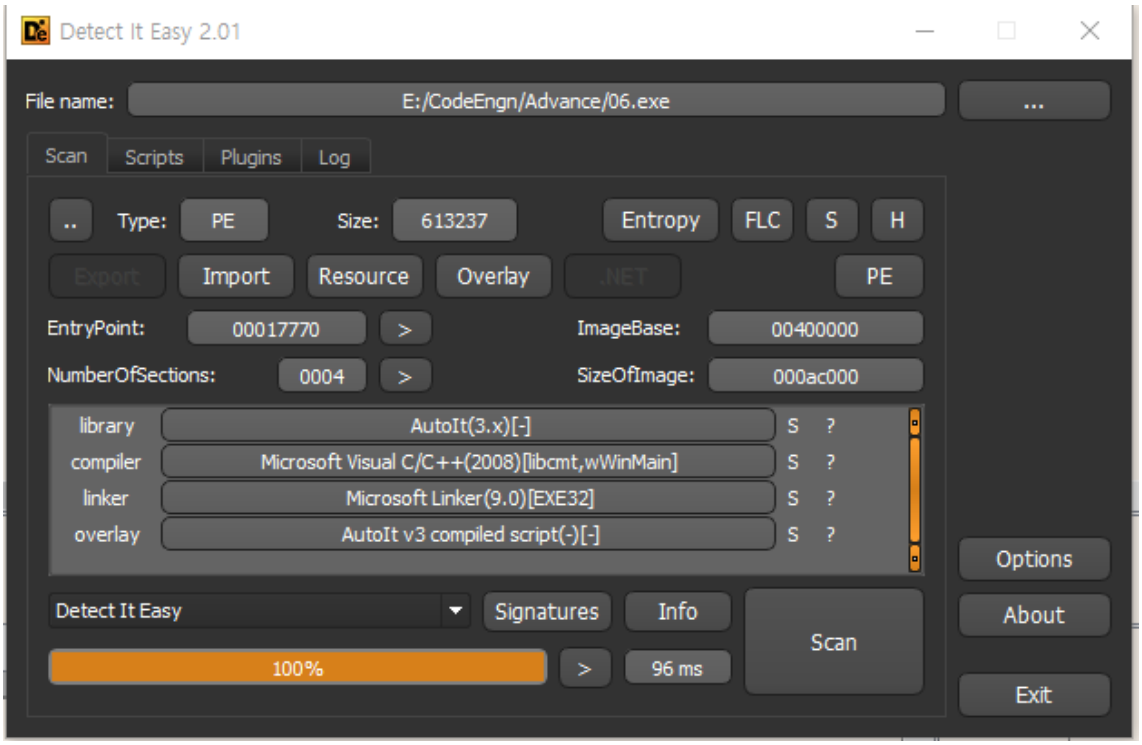


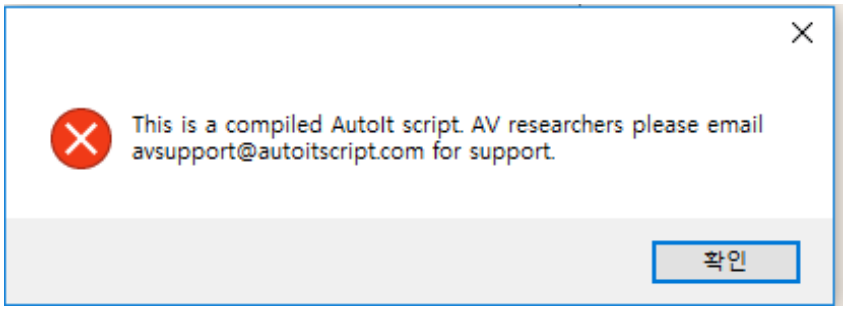
UPX패킹 되어있다.





언팩 후 다시 올려보니 AutoIt를 이용해서 만든 프로그램

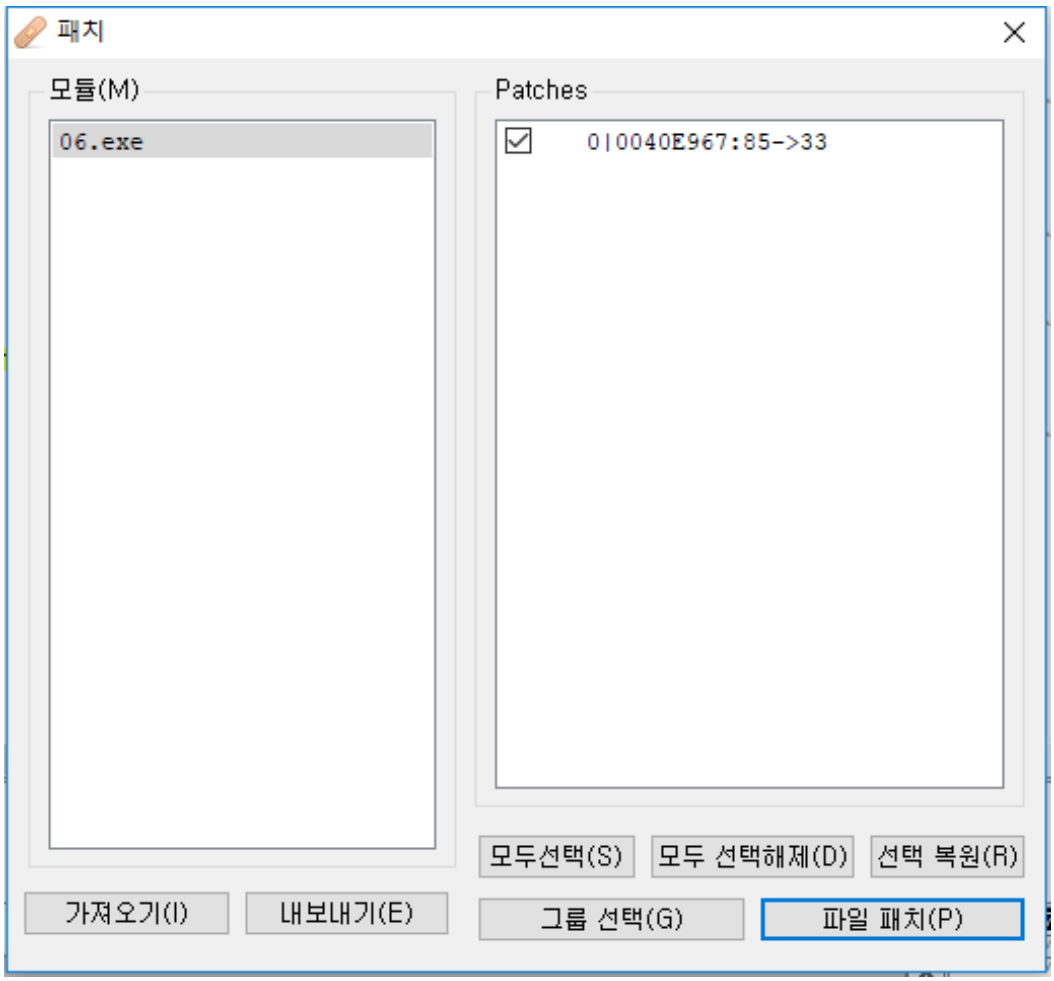




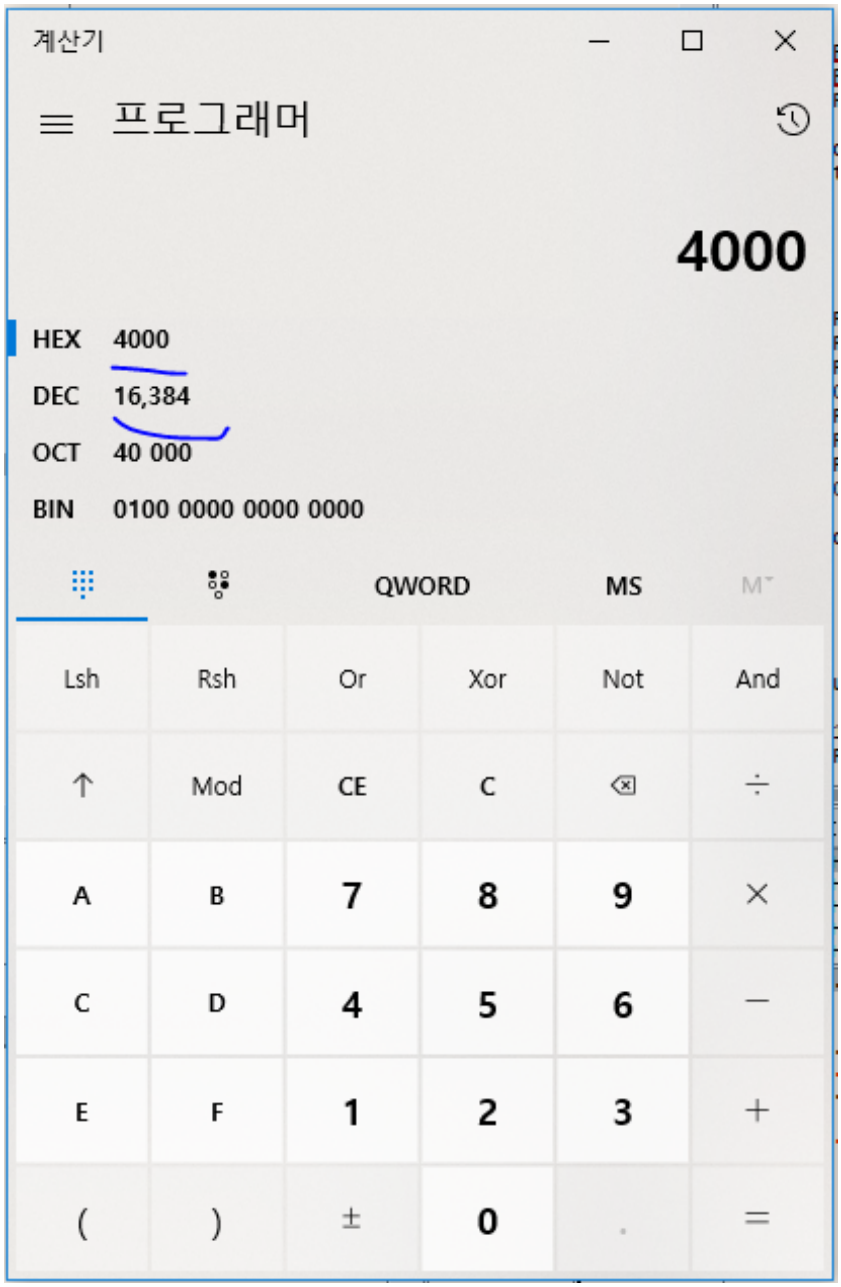
안티디버깅 되어있다.

```
0040E94F    50              push eax
0040E950    68 04010000     push 104
0040E955    FF15 24D34700   call dword ptr ds:[<&GetCurrentDirectoryW>]
0040E95B    57              push edi
0040E95C    E8 1FDFFFFF     call 06.40C880
0040E961    FF15 20D34700   call dword ptr ds:[<&IsDebuggerPresent>]
0040E967    85C0            test eax,eax
0040E969    0F85 6F4F0200   jne 06.4338DE
0040E96F    884424 0F       mov byte ptr ss:[esp+F],al
0040E973    BE 30044A00     mov esi,06.4A0430
0040E978    3905 3CF44900   cmp dword ptr ds:[49F43C],eax
0040E97E    0F84 734F0200   je 06.4338F7
0040E984    68 3CF44900     push 06.49F43C
```

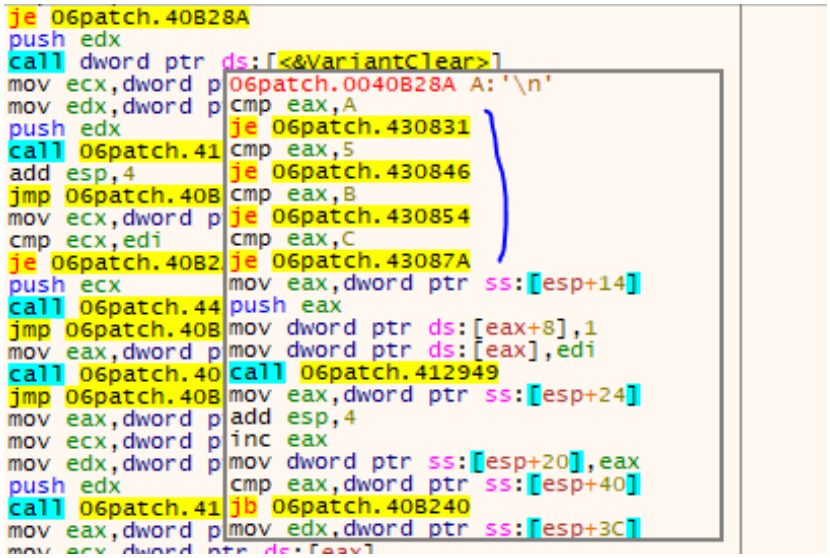
IsDebuggerPresent ! 아래 test를 XOR로 바꾼후 패치

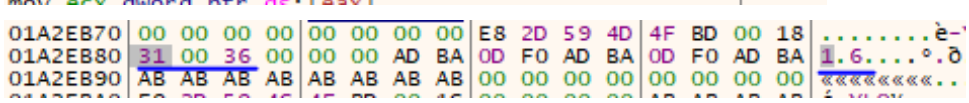


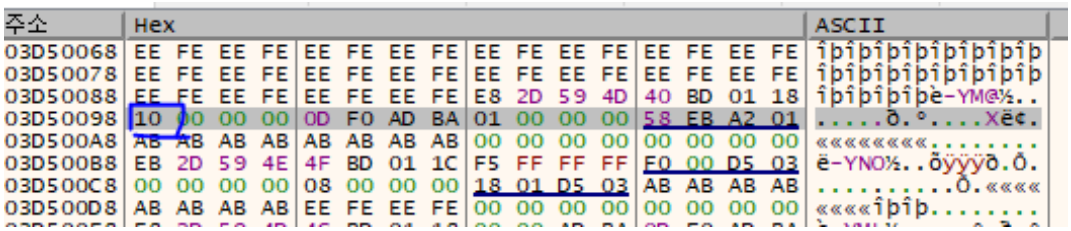

```
cmp eax,8
je 06patch.43080C
cmp eax,A
je 06patch.430831
cmp eax,5
je 06patch.430846
cmp eax,B
je 06patch.430854
cmp eax,C
je 06patch.43087A
mov eax,dword ptr ss:[esp+14]
push eax
```

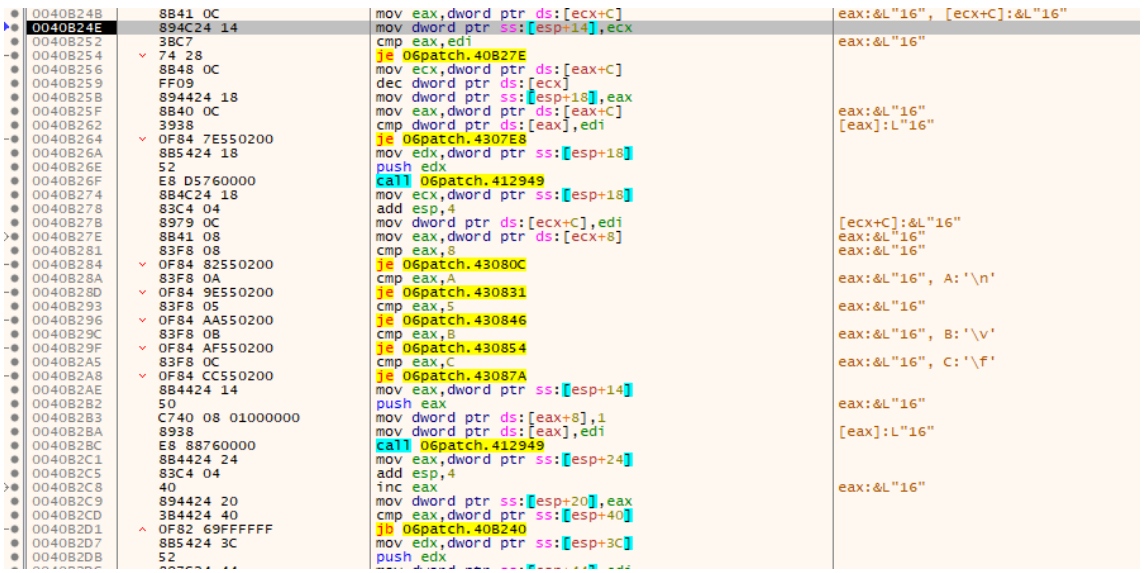



```
0045DFBA   83C1 58          add ecx,58
0045DFBD   51               push ecx
0045DFBE   8D7424 34        lea esi,dword ptr ss:[esp+34]
0045DFC2   E8 590EFBFF      call 06patch.40EE20
0045DFC7   8B7424 48        mov esi,dword ptr ss:[esp+48]
0045DFCB   817C24 24 00400000 cmp dword ptr ss:[esp+24],4000
0045DFD3   76 16            jbe 06patch.45DFEB
0045DFD5   68 00400000      push 4000
0045DFDA   8D5424 24        lea edx,dword ptr ss:[esp+24]
0045DFDE   52               push edx
0045DFDF   83C8 FF          or eax,FFFFFFFF
0045DFE2   E8 F933FAFF      call 06patch.4013E0
```



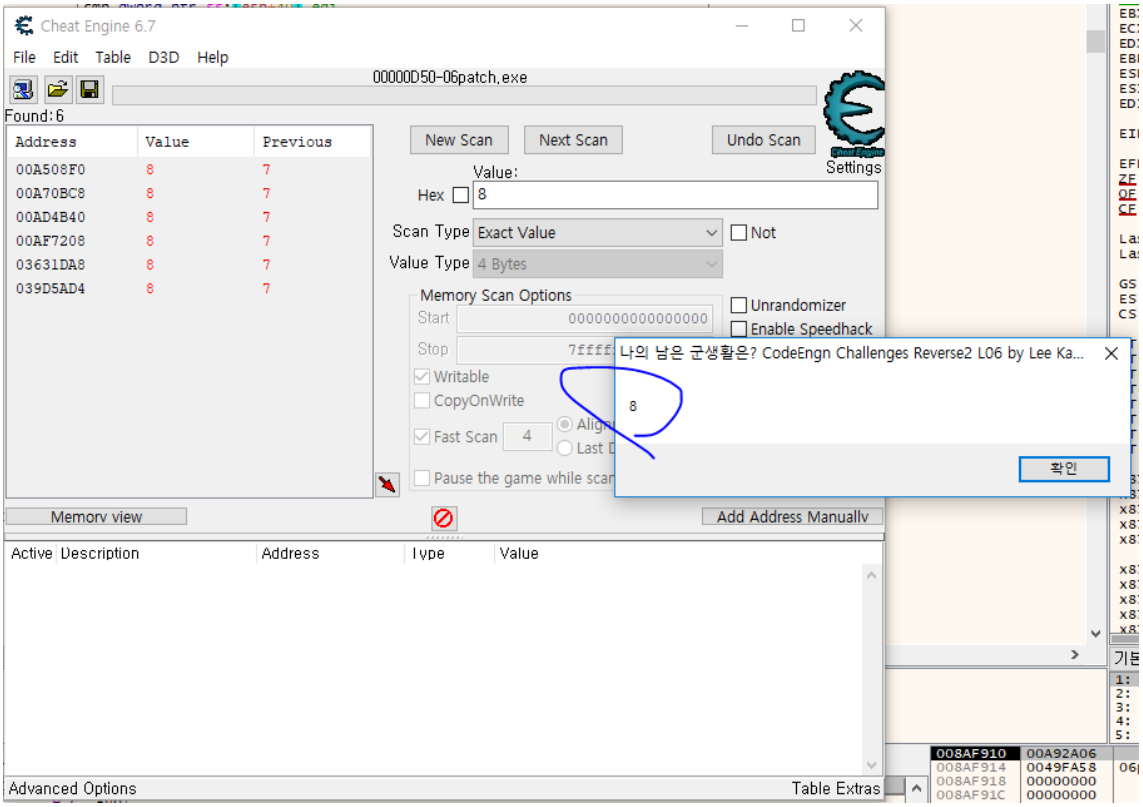


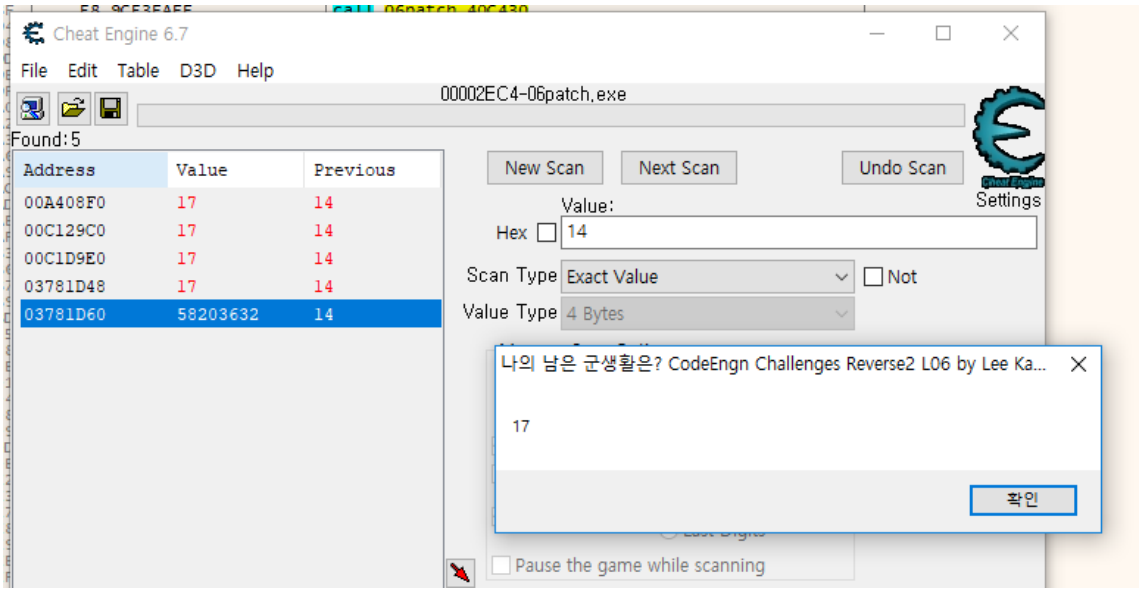




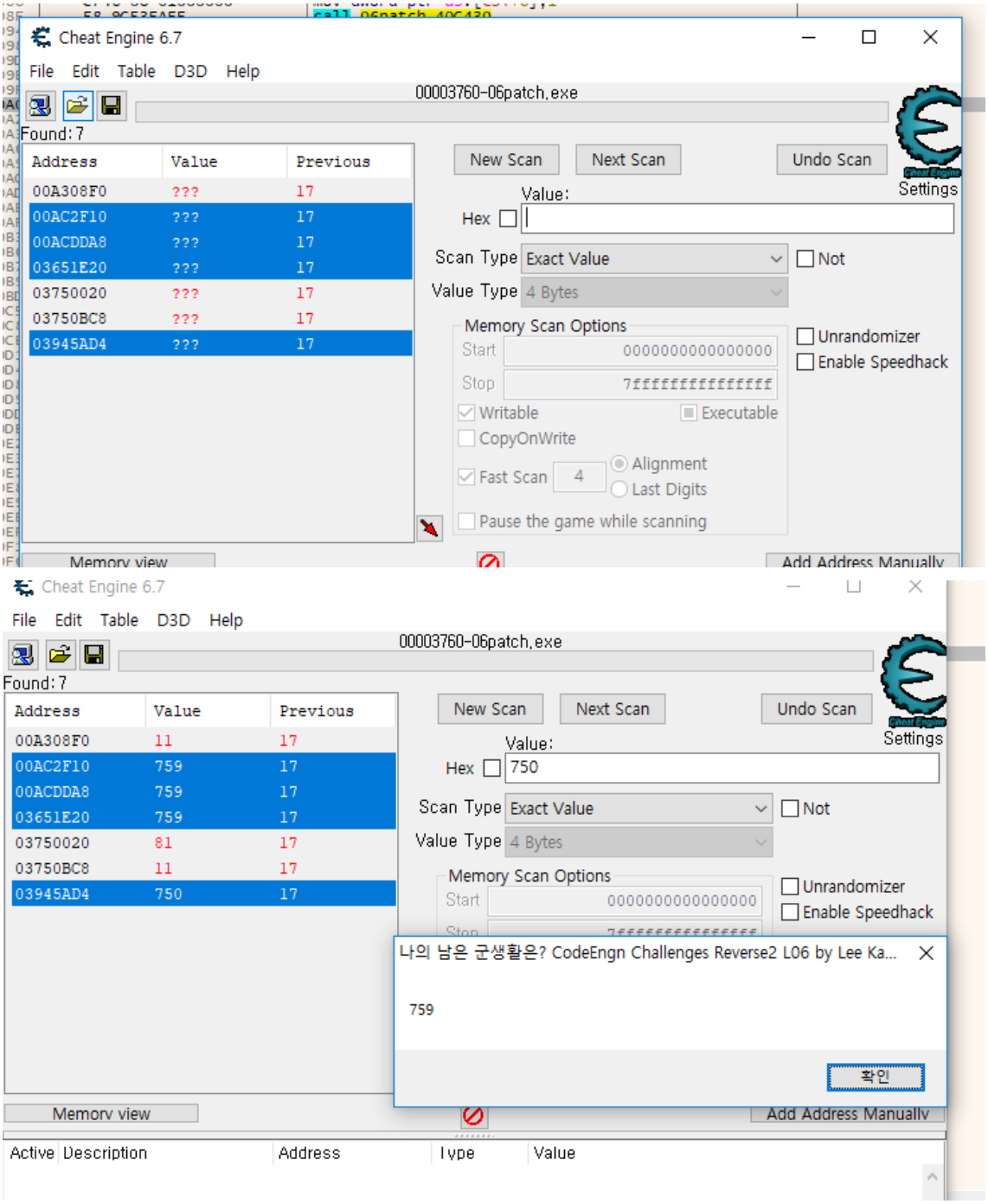
계속 트레이싱하는데 위치를 단서가 될만한게 없어서 다른방법을 생각했다.

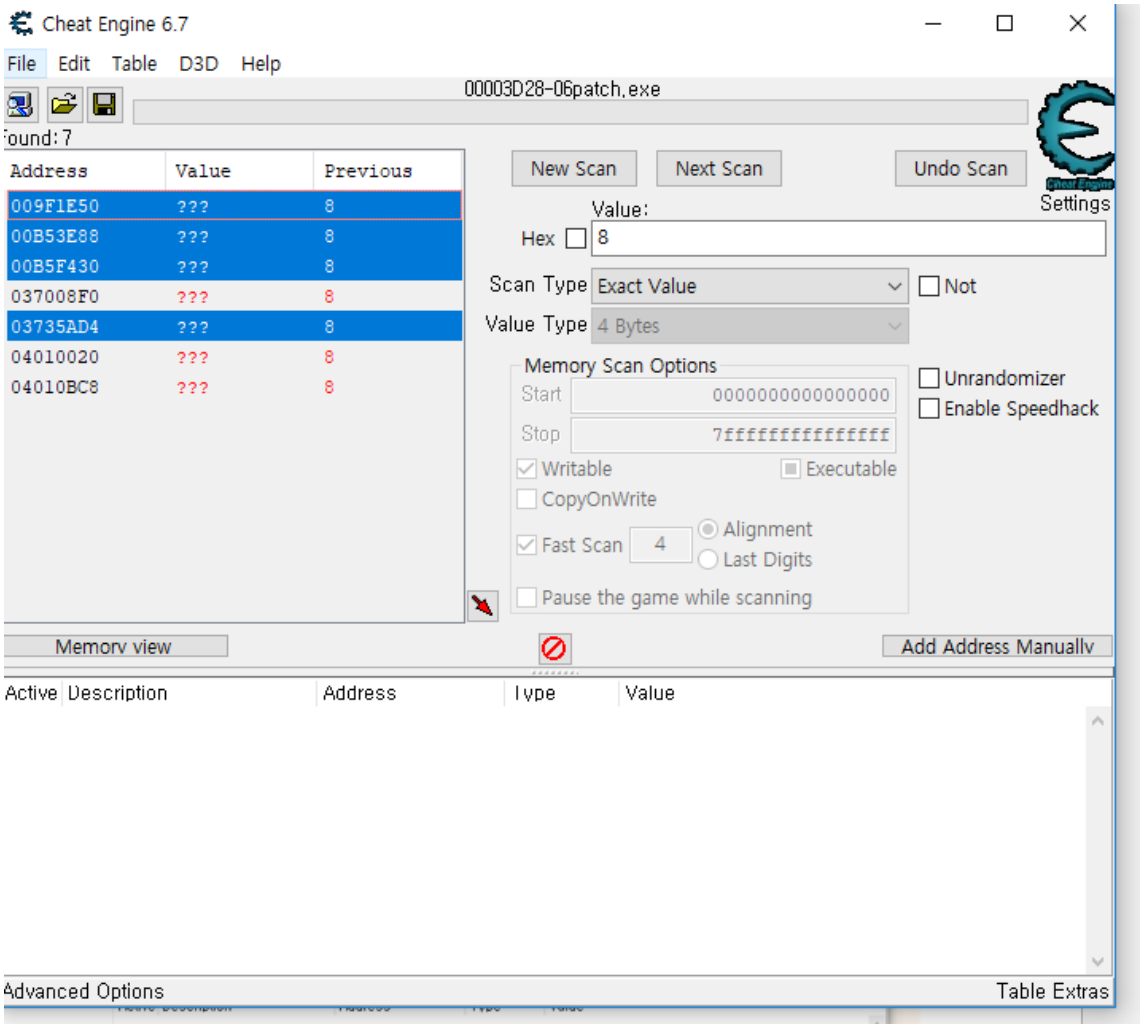
Cheat Engine을 이용하여 날짜 범위를 줄인다.





먼저 일수에 해당하는 주소값들을 추린뒤에 99999를 넣어보니 그냥 종료된다.
아마 값 비교해서 더 크면 그냥 종료되는 프로그램이라고 유추
다음으로 1000을 넣어보니 또 종료 이번에는 되는 값으로
300넣어보니 301을 띄워주는 메시지창이 뜬다.


Cheat Engine 6.7
File Edit Table D3D Help
00003760-06patch.exe
Found: 7
Address Value Previous
00A308F0 ??? 17
00AC2F10 ??? 17
00ACDDA8 ??? 17
03651E20 ??? 17
03750020 ??? 17
03750BC8 ??? 17
03945AD4 ??? 17
New Scan
Next Scan
Undo Scan
Settings
Value:
Hex
Scan Type Exact Value
Not
Value Type 4 Bytes
Memory Scan Options
Start 0000000000000000
Stop 7fffffffffffffff
Writable
Executable
CopyOnWrite
Fast Scan 4
Alignment
Last Digits
Pause the game while scanning
Unrandomizer
Enable Speedhack
Memory view
Add Address Manually
Cheat Engine 6.7
File Edit Table D3D Help
00003760-06patch.exe
Found: 7
Address Value Previous
00A308F0 11 17
00AC2F10 759 17
00ACDDA8 759 17
03651E20 759 17
03750020 81 17
03750BC8 11 17
03945AD4 750 17
New Scan
Next Scan
Undo Scan
Settings
Value:
Hex
750
Scan Type Exact Value
Not
Value Type 4 Bytes
Memory Scan Options
Start 0000000000000000
Unrandomizer
Enable Speedhack
나의 남은 군생활은? CodeEngn Challenges Reverse2 L06 by Lee Ka...
759
확인
Memory view
Add Address Manually
Active Description Address Type Value



점점 줄여나가는 식으로 유추해보니 790에서 값들이 ???로 변하며 종료된다.

여기 MD5 해시하고자하는 텍스트를 붙여 넣습니다

790

MD5 해시를 생성!

당신의 MD5 메시지 여기에서 소화 복사합니다.

2DACE78F80BC92E6D7493423D729448E

Clear