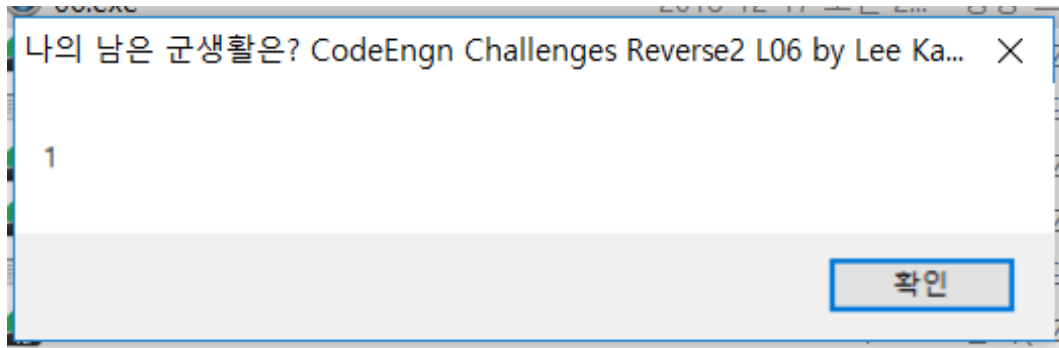
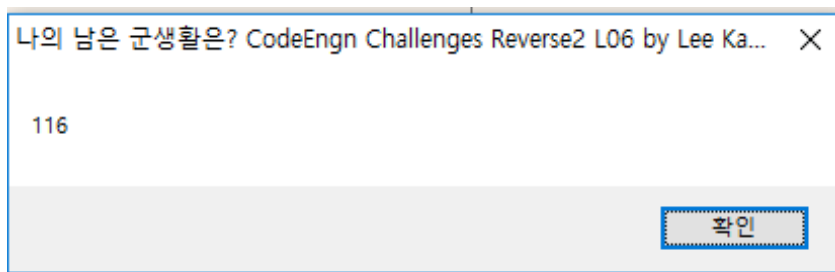


### 19.3.18 CodeEngn Advance 06

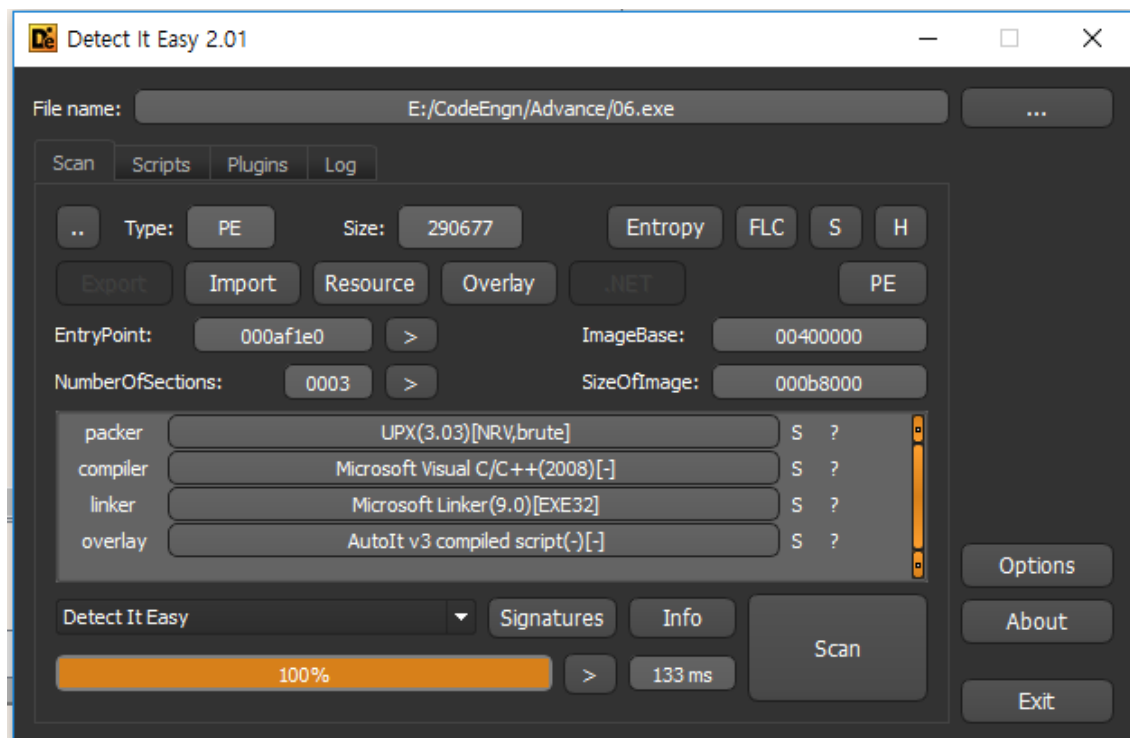
Tree to Tree



확인 누르면 숫자가 계속 올라간다.



UPX패킹 되어있다.



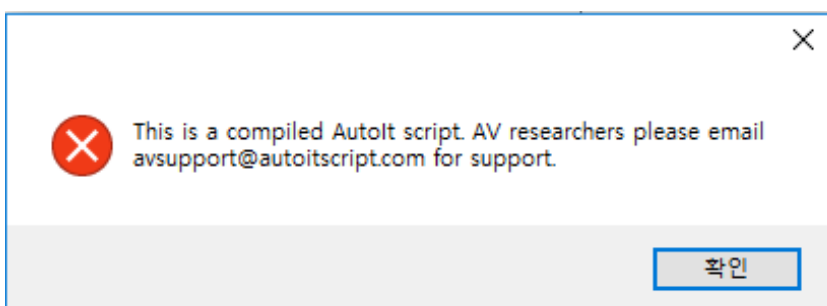
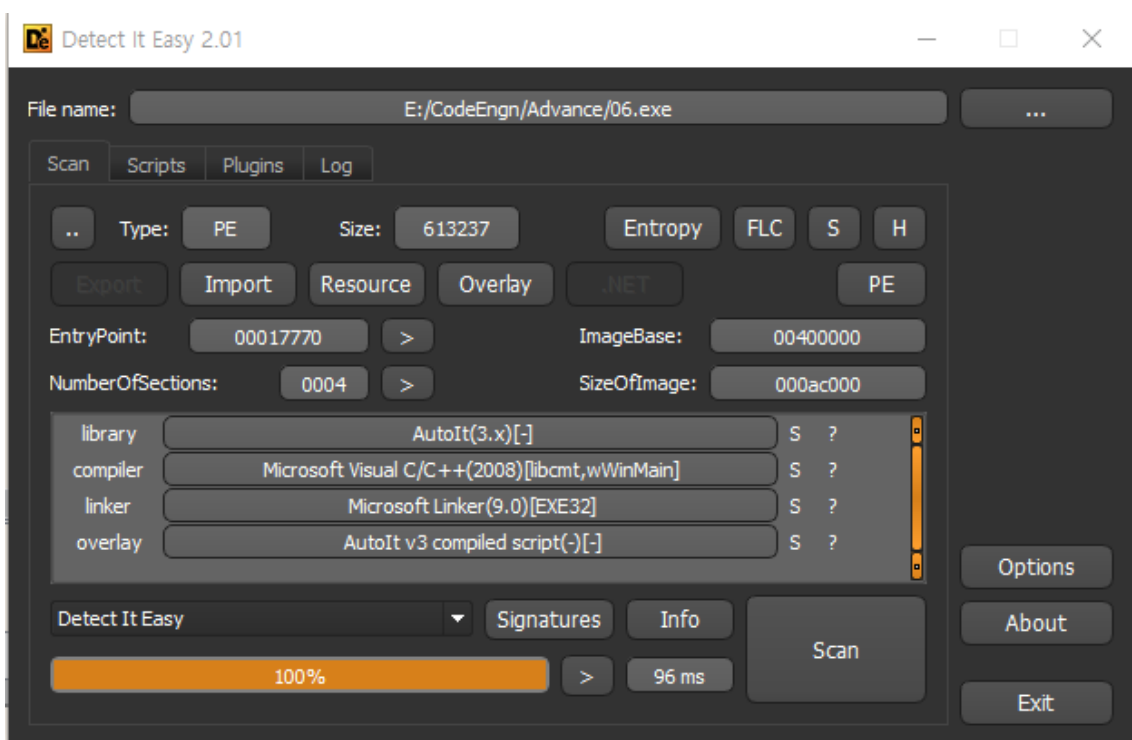
```
Microsoft Windows [Version 10.0.17134.590]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\kwlee>C:\Users\kwlee\OneDrive\upx.exe -d E:\CodeEngn\Advance\06.exe
      Ultimate Packer for executables
      Copyright (C) 1996 - 2018
UPX 3.95w      Markus Oberhumer, Laszlo Molnar & John Reiser   Aug 26th 2018

-----
File size      Ratio      Format      Name
-----
613237 <-    290677    47.40%    win32/pe    06.exe

Unpacked 1 file.
```

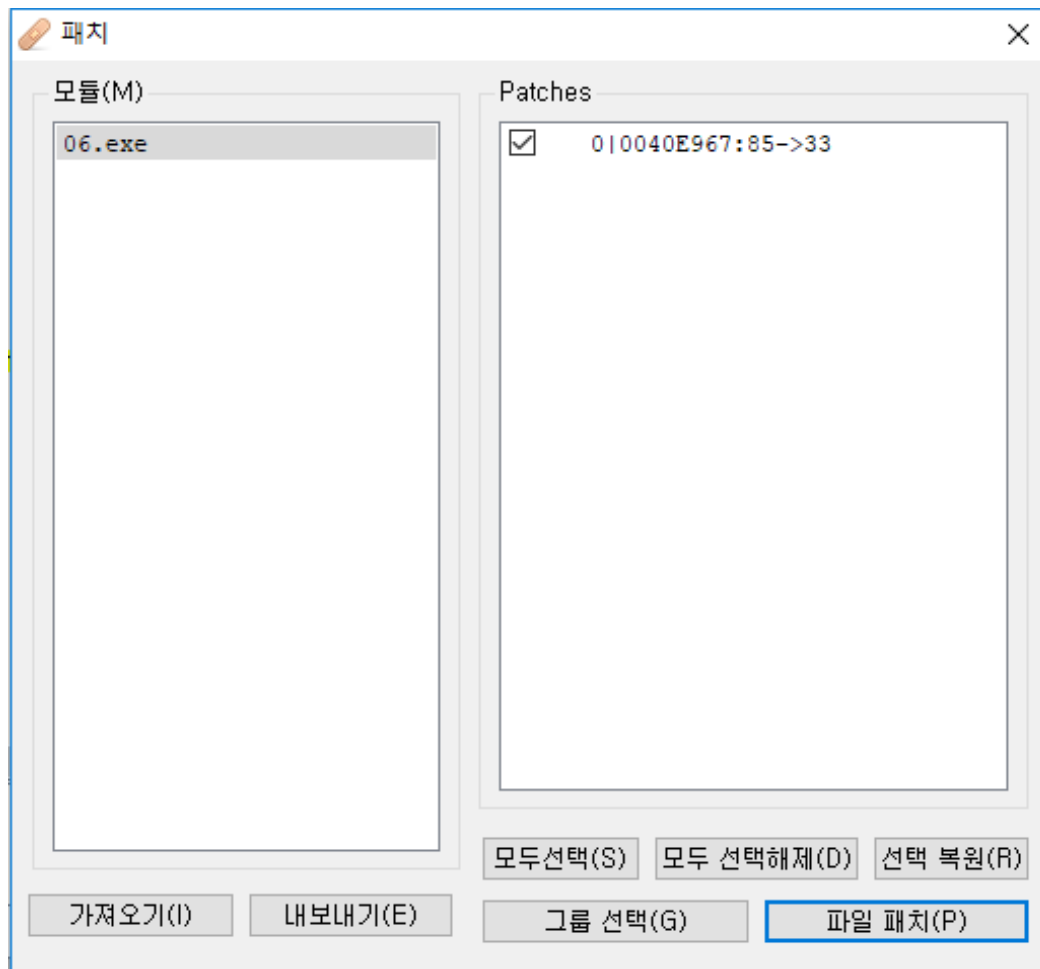
언팩 후 다시 올려보니 AutoIt를 이용해서 만든 프로그램



안티디버깅 되어있다.

0040E94F	50	push eax
0040E950	68 04010000	push 104
0040E955	FF15 24D34700	call dword ptr ds:[<&GetCurrentDirectoryW>]
0040E958	57	push edi
0040E95C	E8 1FDFFFFFFF	call 06.40C880
0040E961	FF15 20D34700	call dword ptr ds:[<&IsDebuggerPresent>]
0040E967	85C0	test eax, eax
0040E969	0F85 6F4F0200	jnz 06.43380E
0040E96F	8B4424 0F	mov byte ptr ss:[esp+F], al
0040E973	8E 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

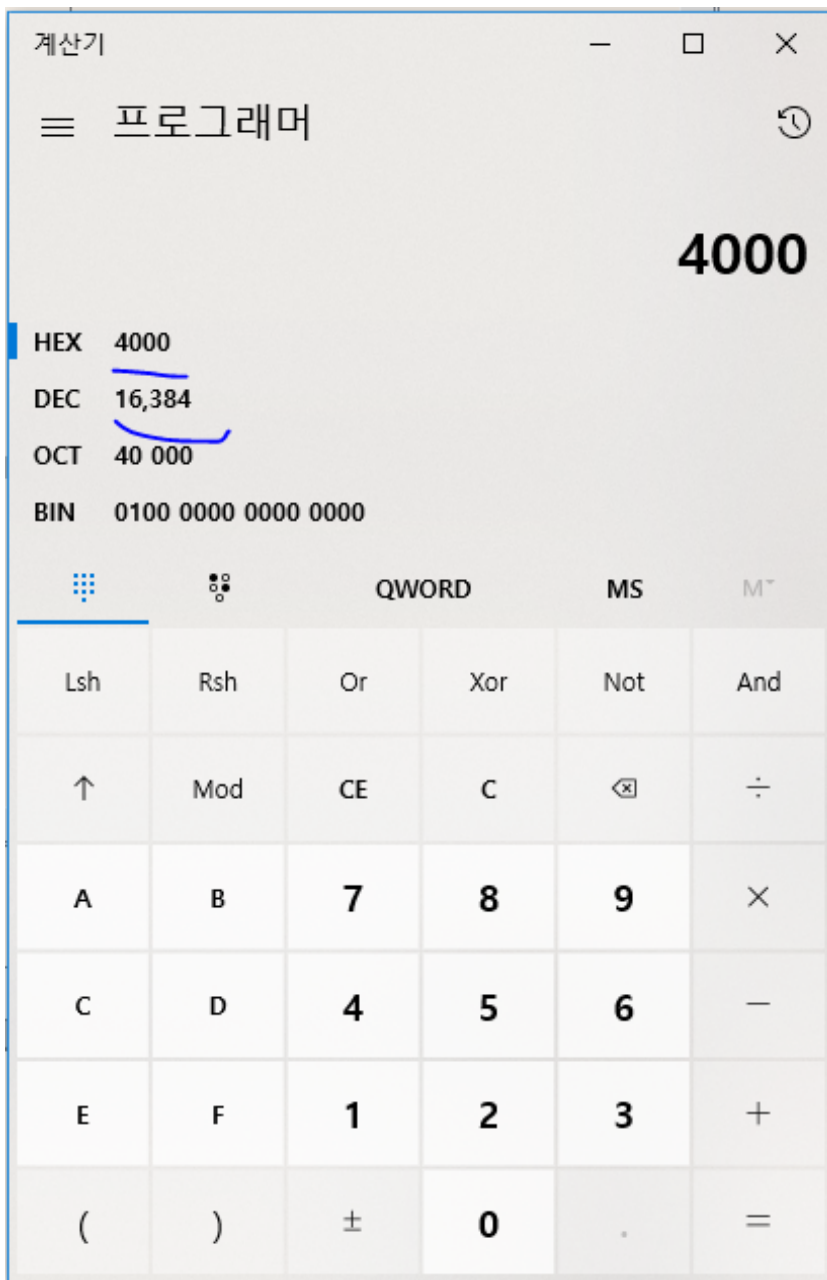
IsDebuggerPresent ! 아래 test를 XOR로 바꾼후 패치



```

cmp eax, 8
je 06patch.43080C
cmp eax, A
je 06patch.430831
cmp eax, 5
je 06patch.430846
cmp eax, 8
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 590EF8FF	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

```

je 06patch.40B28A
push edx
call dword ptr ds:[<&VariantClear>]
mov ecx,dword ptr 06patch.0040B28A A: '\n'
mov edx,dword ptr 06patch.0040B28A A: '\n'
push edx
je 06patch.430831
call 06patch.411299
add esp,4
je 06patch.430846
jmp 06patch.40B28A
mov ecx,dword ptr 06patch.430854
cmp ecx,edi
je 06patch.40B28A
je 06patch.43087A
push ecx
mov eax,dword ptr ss:[esp+14]
call 06patch.441299
push eax
jmp 06patch.40B28A
mov eax,dword ptr 06patch.441299
mov dword ptr ds:[eax+8],1
mov dword ptr ds:[eax],edi
call 06patch.401299
call 06patch.412949
jmp 06patch.40B28A
mov eax,dword ptr 06patch.441299
add esp,4
mov ecx,dword ptr 06patch.441299
inc eax
mov edx,dword ptr 06patch.441299
mov eax,dword ptr ss:[esp+20],eax
push edx
cmp eax,dword ptr ss:[esp+40]
call 06patch.411299
jb 06patch.40B240
mov eax,dword ptr 06patch.441299
mov ecx,dword ptr ds:[eax]

```

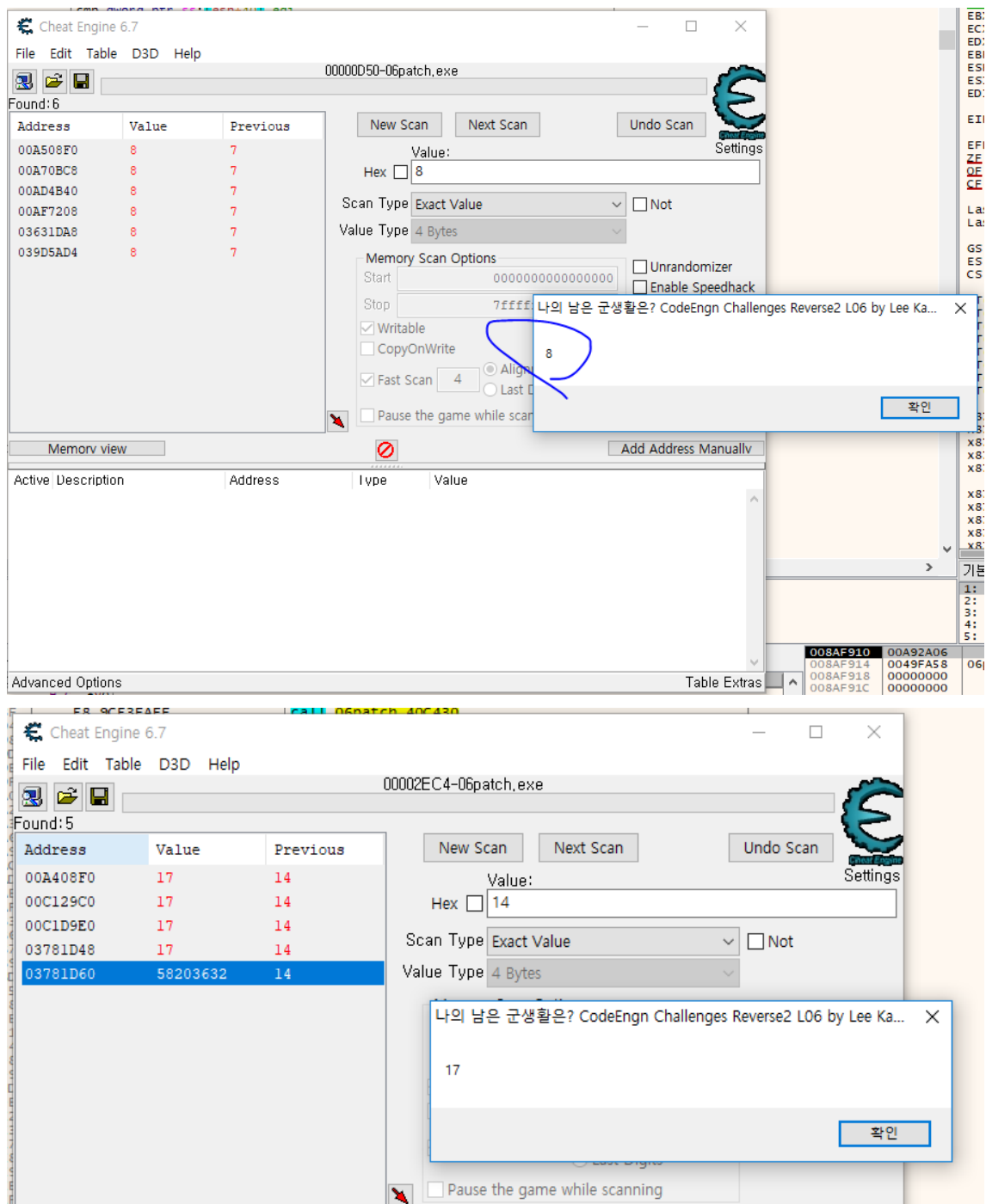
01A2EB70	00 00 00 00	00 00 00 00	E8 2D 59 4D	4F BD 00 18	.....è-
01A2EB80	31 00 36 00	00 00 AD BA	0D F0 AD BA	0D F0 AD BA	1.6....°.ð
01A2EB90	AB AB AB AB	AB AB AB AB	00 00 00 00	00 00 00 00	««««««««..

주소	Hex	ASCII
03D50068	EE FE EE FE EE FE EE FE EE FE EE FE EE FE EE FE EE FE	ïïïïïïïïïïïïïïïï
03D50078	EE FE EE FE EE FE EE FE EE FE EE FE EE FE EE FE EE FE	ïïïïïïïïïïïïïïïï
03D50088	EE FE EE FE EE FE EE FE EE FE E8 2D 59 4D 40 BD 01 18	ïïïïïïïïïïïïïïïï
03D50098	10 00 00 00 0D F0 AD BA 01 00 00 00 58 EB A2 01	.....ð. ....Xec.
03D500A8	AB AB AB AB AB AB AB AB 00 00 00 00 00 00 00 00	««««««««««««««««
03D500B8	EE 2D 59 4E 4F BD 01 1C F5 FF FF FF F0 0D D5 03	ë-YNO%...öyyyo.ð.
03D500C8	00 00 00 00 08 00 00 00 18 01 D5 03 AB AB AB AB	.....ð. ....««««
03D500D8	AB AB AB AB EE FE EE FE 00 00 00 00 00 00 00 00	««««ïïïï

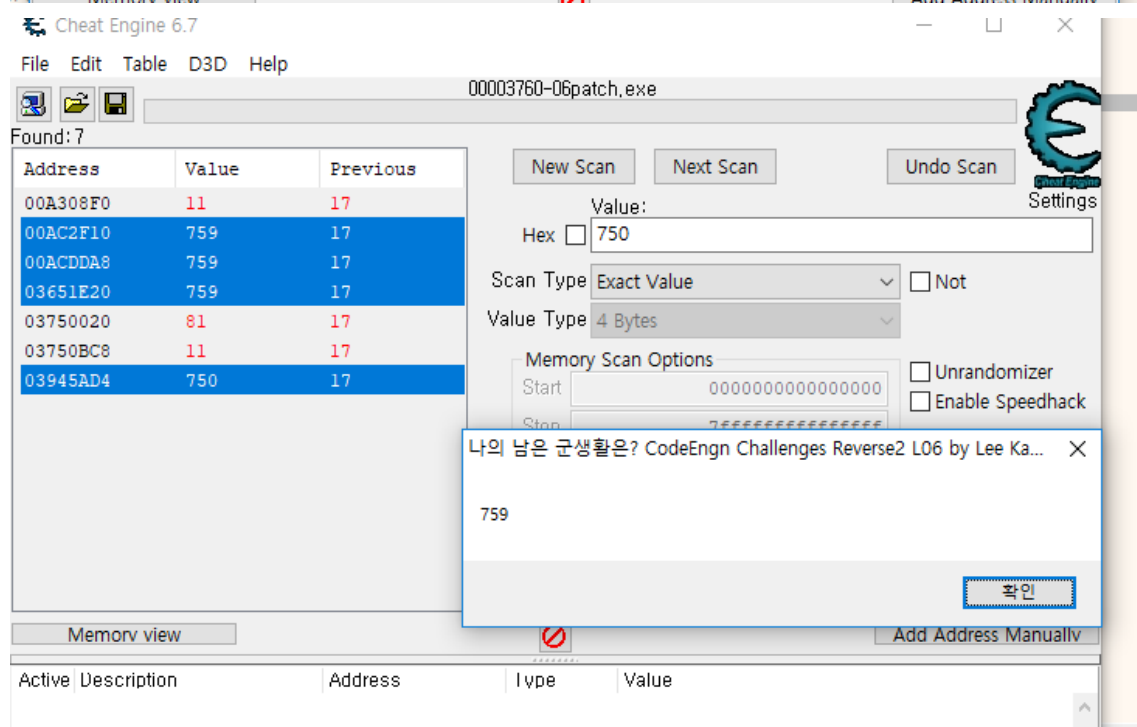
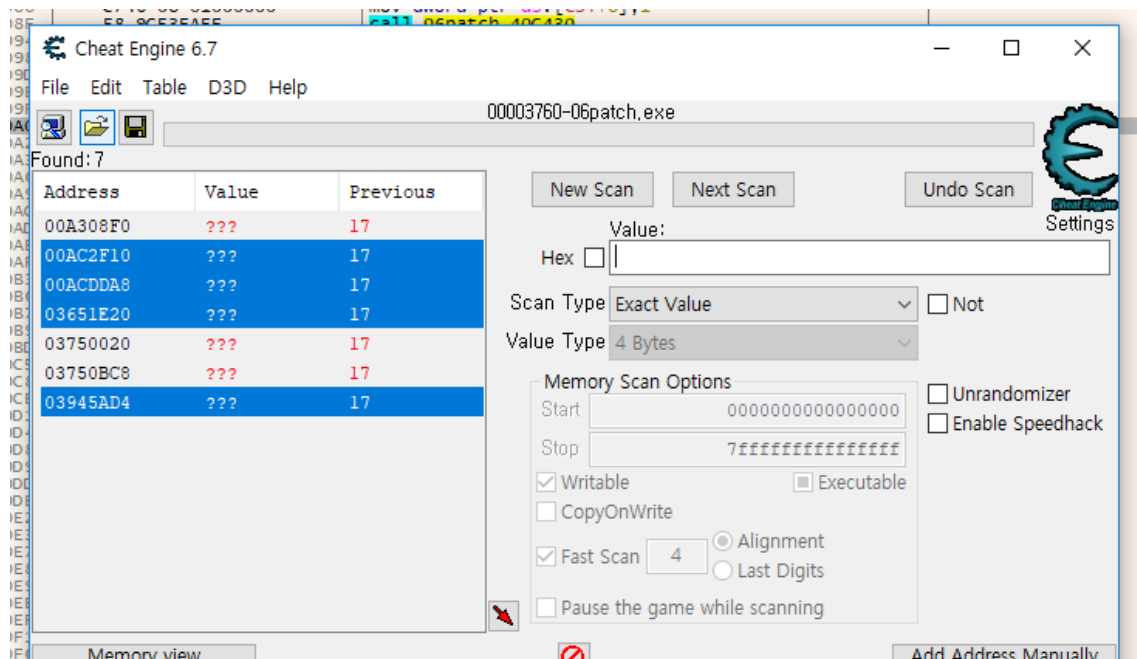
0040B248	8B41 0C	mov eax,dword ptr ds:[ecx+C]	eax:&"16", [ecx+C]:&"16"
0040B24E	894C24 14	mov dword ptr ss:[esp+14],ecx	
0040B252	3BC7	cmp eax,edi	eax:&"16"
0040B254	74 28	jle 06patch.40B27E	
0040B256	8B48 0C	mov ecx,dword ptr ds:[ecx+C]	
0040B259	FF09	dec dword ptr ds:[ecx]	
0040B25B	894424 18	mov dword ptr ss:[esp+18],eax	
0040B25F	8B40 0C	mov eax,dword ptr ds:[ecx+C]	eax:&"16"
0040B262	3938	cmp dword ptr ds:[eax],edi	[eax]:&"16"
0040B264	0F84 7E550200	jle 06patch.4307E8	
0040B26A	8B5424 18	mov edx,dword ptr ss:[esp+18]	
0040B26E	52	push edx	
0040B26F	E8 D5760000	call 06patch.412949	
0040B274	8B4C24 18	mov ecx,dword ptr ss:[esp+18]	
0040B278	83C4 04	add esp,4	
0040B27B	8979 0C	mov dword ptr ds:[ecx+C],edi	[ecx+C]:&"16"
0040B27E	8B41 08	mov eax,dword ptr ds:[ecx+8]	eax:&"16"
0040B281	83F8 08	cmp eax,8	eax:&"16"
0040B284	0F84 82550200	jle 06patch.43080C	
0040B28A	83F8 0A	cmp eax,A	eax:&"16", A: '\n'
0040B28D	0F84 9E550200	jle 06patch.430831	
0040B293	83F8 05	cmp eax,5	eax:&"16"
0040B296	0F84 AA550200	jle 06patch.430846	
0040B29C	83F8 0B	cmp eax,8	eax:&"16", B: '\v'
0040B2A5	0F84 AF550200	jle 06patch.430854	
0040B2A8	83F8 0C	cmp eax,C	eax:&"16", C: '\f'
0040B2AE	0F84 CC550200	jle 06patch.43087A	
0040B2B2	8B4424 14	mov eax,dword ptr ss:[esp+14]	
0040B2B8	50	push eax	eax:&"16"
0040B2B3	C740 08 01000000	mov dword ptr ds:[eax+8],1	
0040B2BA	8938	mov dword ptr ds:[eax],edi	[eax]:&"16"
0040B2BC	E8 88760000	call 06patch.412949	
0040B2C1	8B4424 24	mov eax,dword ptr ss:[esp+24]	
0040B2C5	83C4 04	add esp,4	
0040B2C8	40	inc eax	eax:&"16"
0040B2C9	894424 20	mov dword ptr ss:[esp+20],eax	
0040B2CD	3B4424 40	cmp eax,dword ptr ss:[esp+40]	
0040B2D1	0F82 69FFFFF	jbe 06patch.40B240	
0040B2D7	8B5424 3C	mov edx,dword ptr ss:[esp+3C]	
0040B2DB	52	push edx	

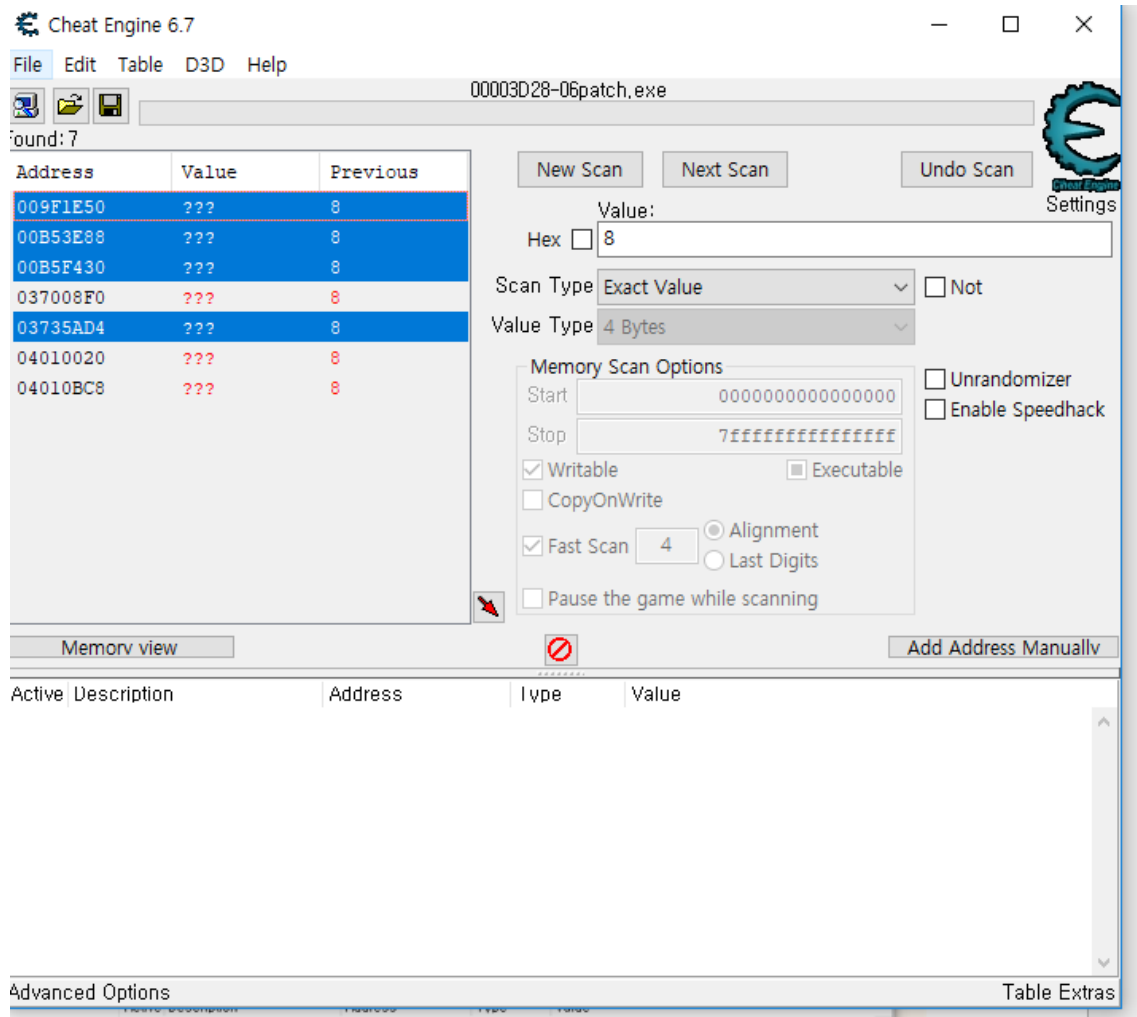
계속 트레이닝하는데 위치를 단서가 될만한게 없어서 다른방법을 생각했다.

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.





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