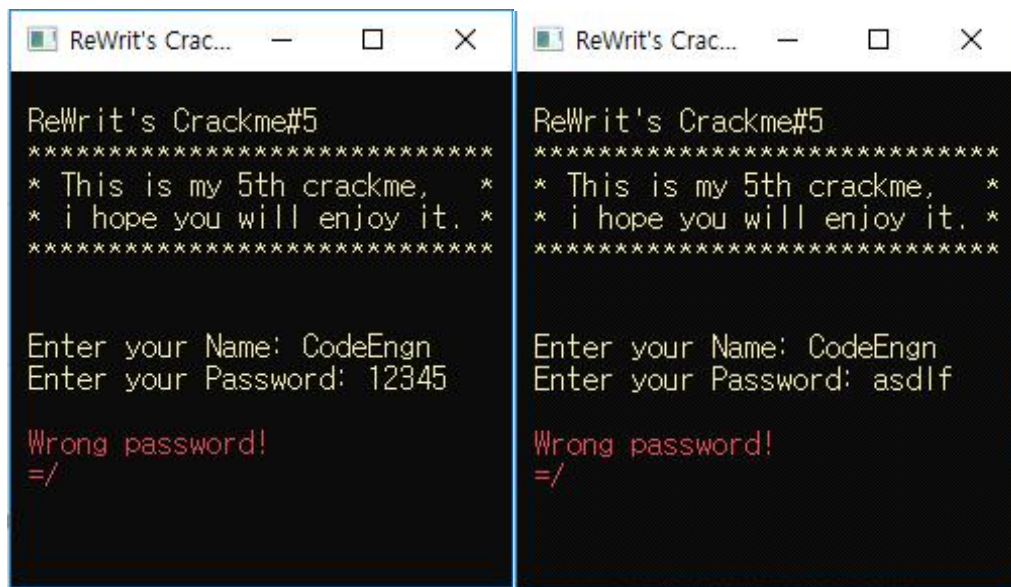


2019.02.20. CodeEngn Basic 16

Tree to Tree

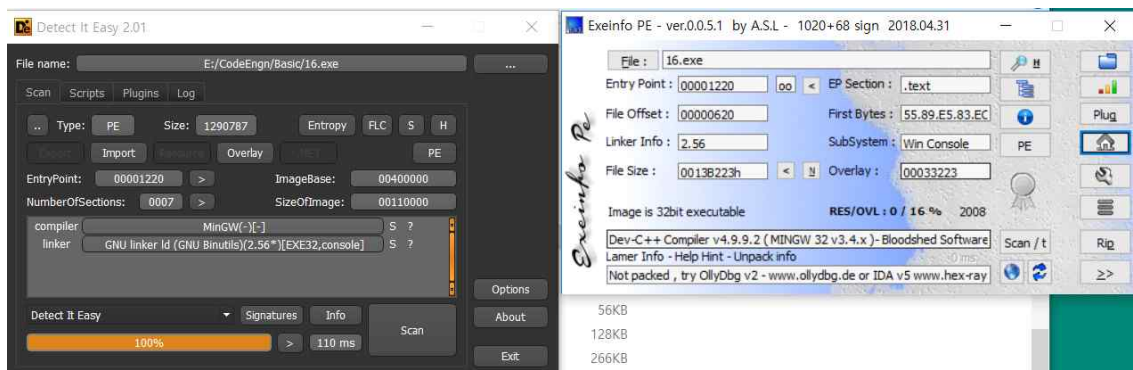


Serial문제!



이번엔 문자인지 숫자인지 모름

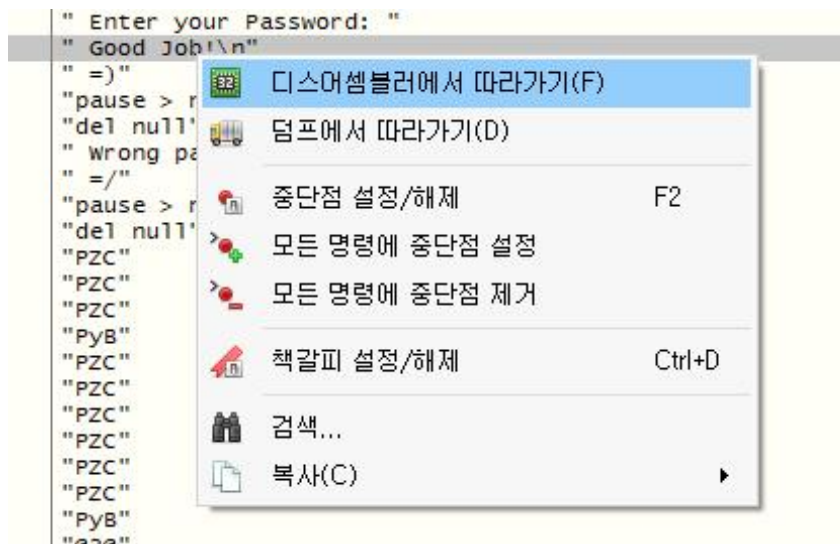
분석기 돌려보니 패킹되어있지 않음



main부분에서 현재모듈 문자열 검색하니 성공문자열 나옴

```
"Title ReWrit's Crackme #5"
"mode con: Cols=31 Lines=16"
" ReWrit's Crackme#5\n"
" *****\n"
" * This is my 5th crackme, *\n"
" * i hope you will enjoy it. *\n"
" *****\n"
"\n\n"
" Enter your Name: "
" Enter your Password: "
" Good Job!\n"
" =)"
"pause > null"
"del null"
" Wrong password!\n"
" =/"
"pause > null"
"del null"
"PZC"
```

디스어셈블리어에서 따라가기



비교문에서 breakpoint후 실행 참고로 password는 12345로 입력했다.

004015A2	0F 85 94 00 00 00	jne 16.40163C	
004015A8	C7 04 24 F5 FF FF FF	mov dword ptr ss:[esp],FFFFFFFF	
004015AF	E8 8C F6 00 00	call <JMP.&GetStdHandle>	
004015B4	83 EC 04	sub esp,4	
004015B7	C7 44 24 04 0A 00 00 00	mov dword ptr ss:[esp+4],A	A: '\n'
004015BF	89 04 24	mov dword ptr ss:[esp],eax	
004015C2	E8 89 F6 00 00	call <JMP.&SetConsoleTextAttribute>	
004015C7	83 EC 08	sub esp,8	
004015CA	C7 44 24 04 A8 B1 43 00	mov dword ptr ss:[esp+4],16.43B1A8	
004015D2	C7 04 24 C0 33 44 00	mov dword ptr ss:[esp],16.4433C0	
004015D9	E8 52 8D 02 00	call 16.42A330	
004015DE	C7 44 24 04 D9 00 44 00	mov dword ptr ss:[esp+4],16.4400D9	4400D9: " Good Job!\n"
004015E6	C7 04 24 C0 33 44 00	mov dword ptr ss:[esp],16.4433C0	
004015ED	E8 E6 AD 03 00	call 16.43C3D8	
004015F2	C7 44 24 04 E5 00 44 00	mov dword ptr ss:[esp+4],16.4400E5	4400E5: " =)"
004015FA	C7 04 24 C0 33 44 00	mov dword ptr ss:[esp],16.4433C0	
00401601	E8 D2 AD 03 00	call 16.43C3D8	
00401606	C7 04 24 E9 00 44 00	mov dword ptr ss:[esp],16.4400E9	4400E9: "pause > null"
0040160D	E8 BE F3 00 00	call <JMP.&system>	
00401612	C7 04 24 F6 00 44 00	mov dword ptr ss:[esp],16.4400F6	4400F6: "del null"
00401619	E8 82 F3 00 00	call <JMP.&system>	
0040161E	8D 45 C8	lea eax,dword ptr ss:[ebp-38]	
00401621	89 04 24	mov dword ptr ss:[esp],eax	
00401624	C7 45 90 FF FF FF FF	mov dword ptr ss:[ebp-70],FFFFFFFF	
00401628	E8 50 D8 02 00	call 16.42EE80	
00401630	C7 45 88 00 00 00 00	mov dword ptr ss:[ebp-78],0	
00401637	E9 EA 00 00 00	jmp 16.401726	
0040163C	C7 04 24 F5 FF FF FF	mov dword ptr ss:[ebp-7C],FFFFFFFF	

EAX에는 12345가 수로 바뀌여서 0x3039로 저장된 모습을 볼 수 있다.

아마 답은 숫자일꺼라고 예상

0070FEFC	97 0D C6 E4	6C 16 75 00	D4 70 27 77	E9 7E 29 77
0070FF0C	A0 15 75 00	F0 4E 7C 00	F9 70 29 77	08 00 00 00
0070FF1C	[0070FEFC] = E4C6D97 (사용자 데이터)			00 00 00 00
0070FF2C	00 00 00 00	00 00 00 00	FF 70 00 00	
0070FF3C	E7 11 40 00	01 00 00 00	C0 15 75 00	78 18 75 00
0070FF4C	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00

EAX	00003039	
EBX	00004000	
ECX	00000000	
EDX	E4B8D80	
EBP	0070FF38	
ESP	0070FE80	" 4D "
ESI	00401220	<16. EntryPoint>
EDI	00401220	<16. EntryPoint>

ebp-3C부분에 저장되어있던 dword만큼의 데이터를
십진수로 변환해보니
3838184855



3838184855 입력



Clear