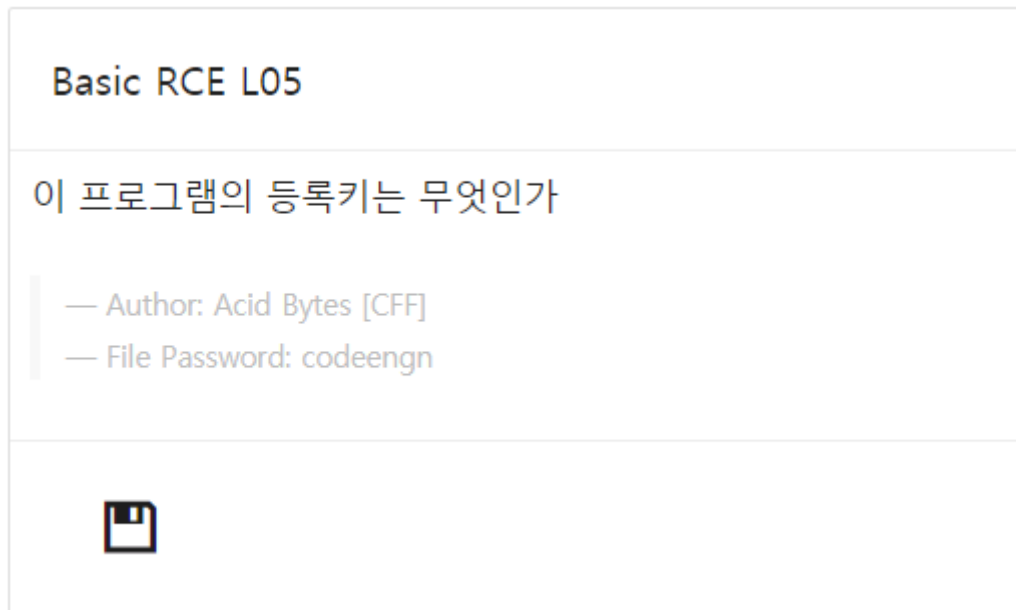
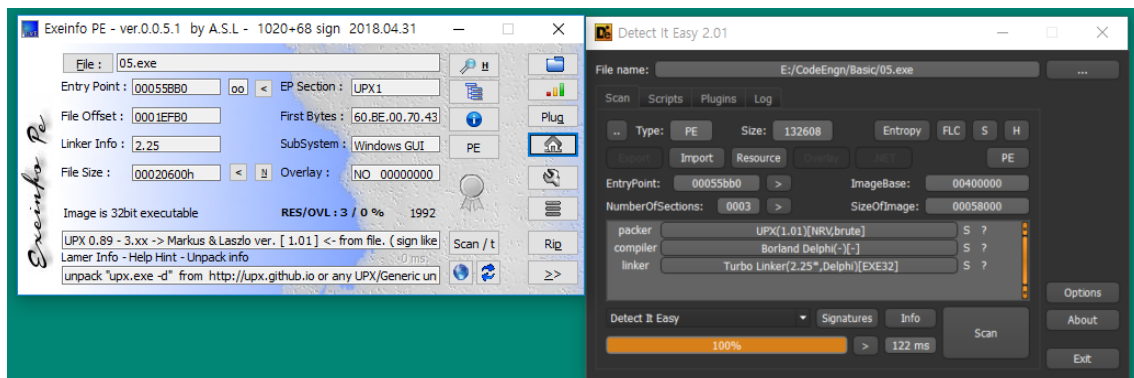


2019.02.12. CodeEngn Basic RCE L05

Tree to Tree



먼저 PE 분석기로 돌려보니 UPX패킹이 되어있다.






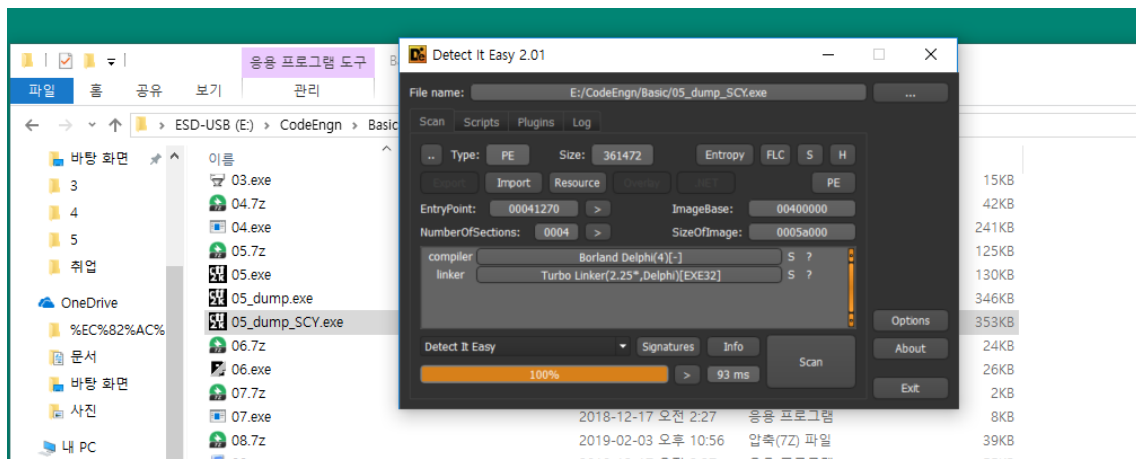
사실 따로 언팩할 필요까지는 없었다.

언팩을 덤프하는 원리는 먼저 OEP를 찾는다.

찾아낼 때에는 pushad, popad를 찾을 때까지 트레이싱을 해도 되고 명령어 검색을 통해 pushad와 popad를 찾아 breakpoint를 걸어주는 방법 이 있다.

OEP를 찾을때까지 실행했다면 패킹된 code값들이 원래 자리에 적재되어있는데 그값들을 덤프하여 ep를 설정해주면 언팩 했다고 말할 수 있다.

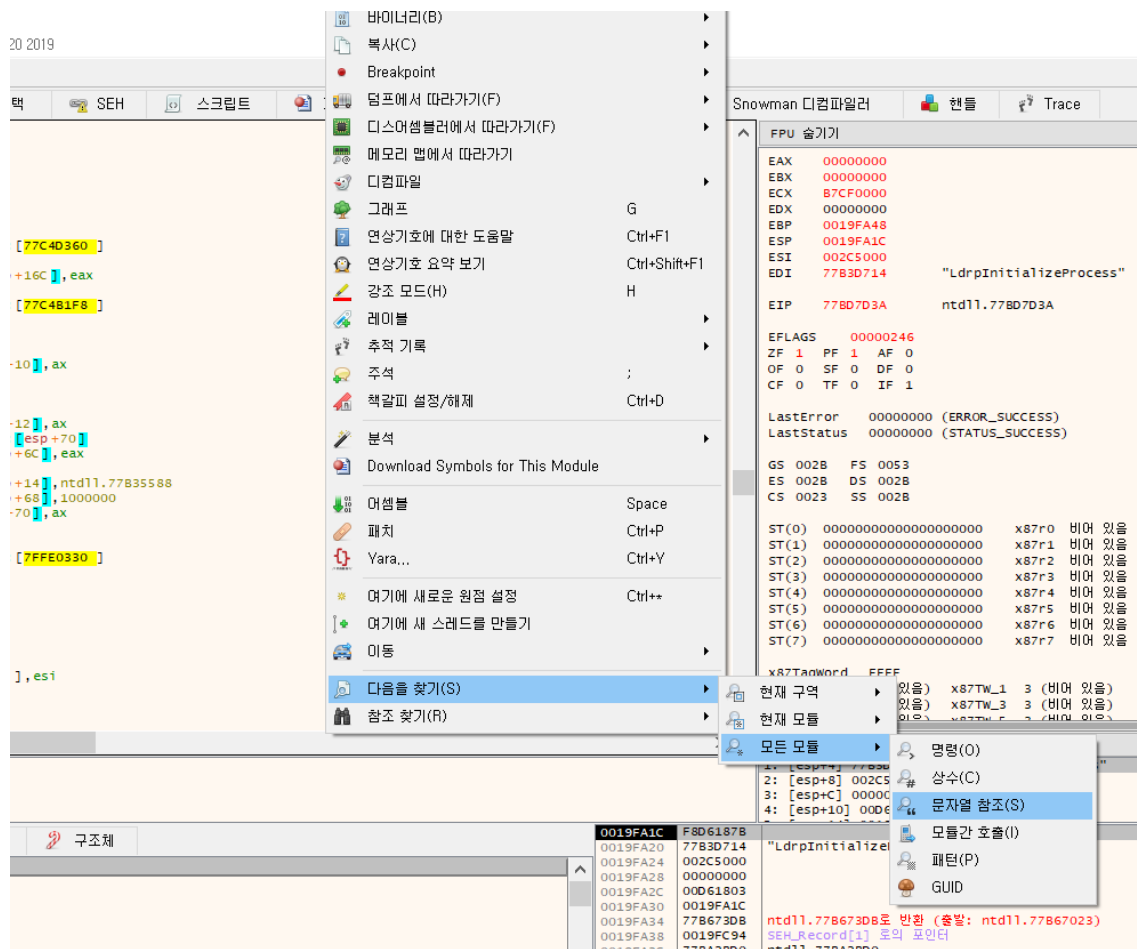
 05.exe	2018-12-17 오전 2:27	응용 프로그램	130KB
 05_dump.exe	2019-02-12 오후 3:06	응용 프로그램	346KB
 05_dump_SCY.exe	2019-02-12 오후 3:06	응용 프로그램	353KB



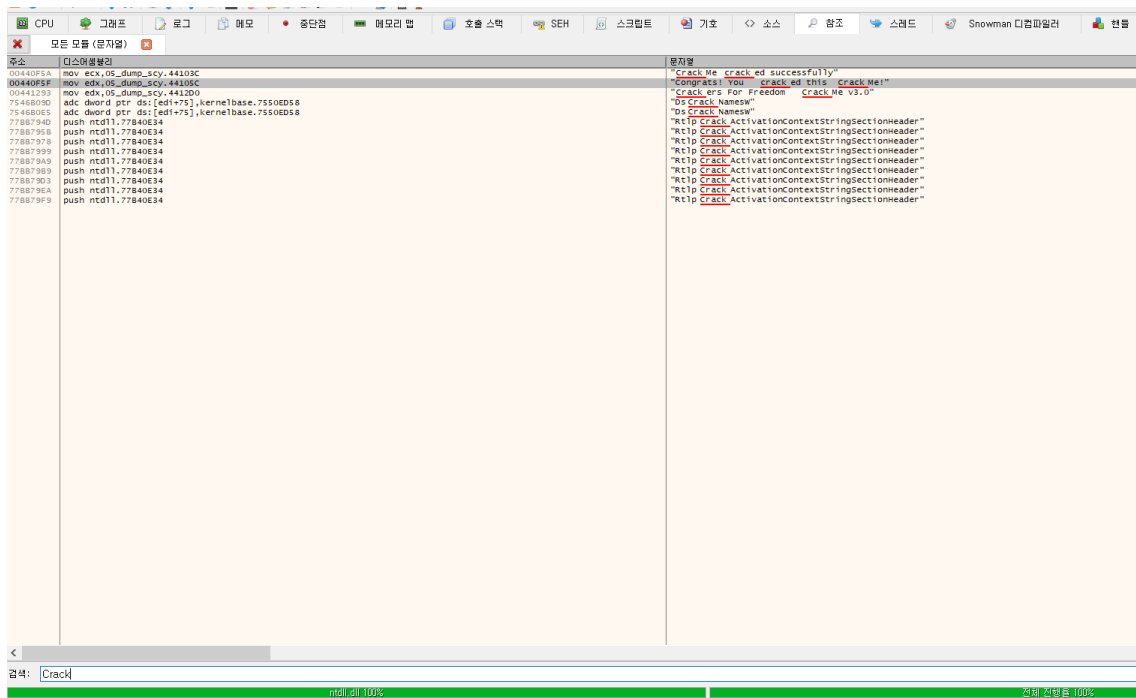
언팩 완료

05_dump_SCY.exe

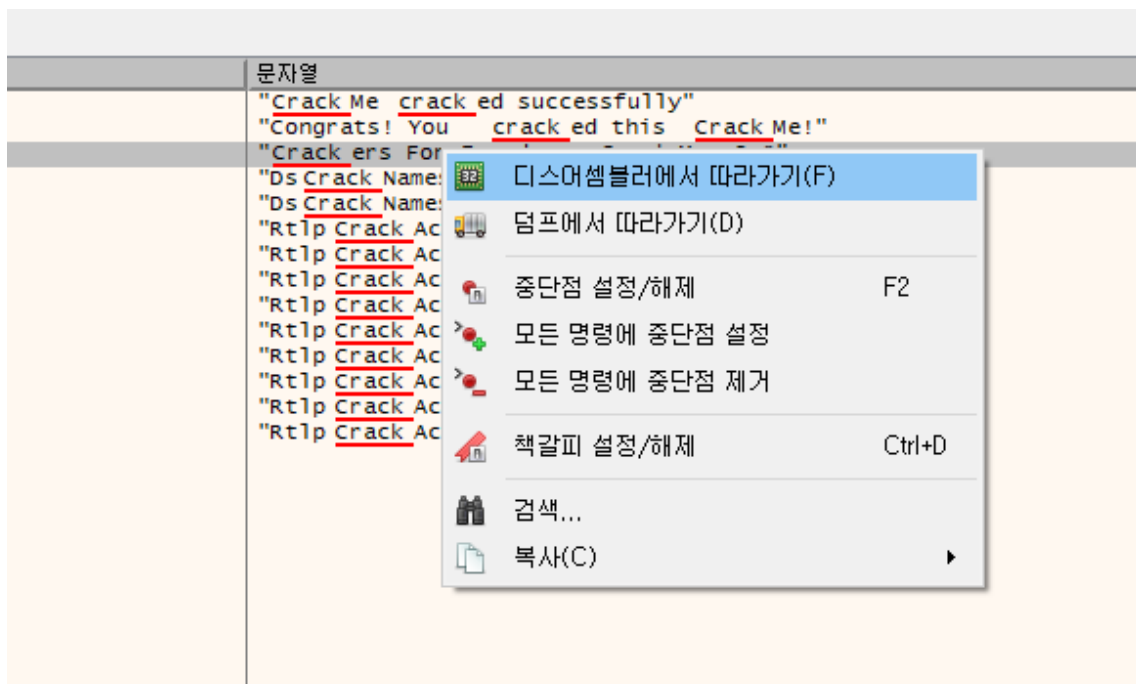
문제를 풀기위해서 시리얼 넘버를 찾아야되는데 문자열 검색을 먼저 진행했다.



Crack이라는 문자열로 검색을 진행했고 성공했다는 문자열을 가진 아이를 발견



마우스 오른쪽 클릭을 통하여 덤프해서 따라가기 클릭



다행히 문자열들 사이로 키 값 같이 보이는 문자열들을 발견

넣어보자.

00440FEA	20	53	65	72	69	61	6C	20	65	6E	74	65	72	65	64	00	Serial entered.
00440FFA	00	00	45	6E	74	65	72	20	61	20	53	65	72	69	61	6C	..Enter a Serial
0044100A	21	00	FF	FF	FF	FF	0F	00	00	00	52	65	67	69	73	74	!.yyyy....Regist
0044101A	65	72	65	64	20	55	73	65	72	00	FF	FF	FF	FF	0F	00	ered User.yyyy..
0044102A	00	00	47	46	58	2D	37	35	34	2D	49	45	52	2D	39	35	..GFX-754-IER-95
0044103A	34	00	43	72	61	63	68	4D	65	20	63	72	61	63	68	65	4.CrackMe cracke
0044104A	64	20	73	75	63	63	65	73	73	66	75	6C	6C	79	00	00	d successfully..
0044105A	00	00	43	6F	6E	67	72	61	74	73	21	20	59	6F	75	20	..Congrats! You
0044106A	63	72	61	63	68	65	64	20	74	68	69	73	20	43	72	61	cracked this Cra
0044107A	63	68	4D	65	21	00	42	65	67	67	61	72	20	6F	66	66	ckMe!.Beggan off
0044108A	21	00	4B	05	44	10	CE	(사용자 코드)	72	69	61	6C	2C	74			!.Wrong Serial,t
0044109A	72	79	20	61	67	61	69	6E	21	00	53	88	D8	6A	00	89	ry again!.S.0j.'
004410AA	C8	10	44	00	BA	D8	10	44	00	A1	44	2C	44	00	88	00	E.D.*0.D.iD.D...
004410BA	E8	A9	BF	FF	FF	8B	C3	E8	3E	8D	FF	FF	58	C3	48	61	e@yy,Aes.yy[Aha
004410CA	76	65	20	61	20	6E	69	63	65	20	64	61	79	00	40	61	ve a nice day,Wa
004410DA	69	6C	20	4E	61	6D	65	2F	53	65	72	69	61	6C	20	74	!! Name/Serial t
004410EA	6F	20	61	63	69	64	62	79	74	65	73	40	67	6D	78	2E	o acidbytes@gmx.

성공!

