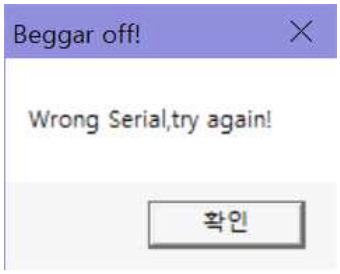
CodeEngn Basic RCE L05
: 이 프로그램의 등록키는 무엇인가



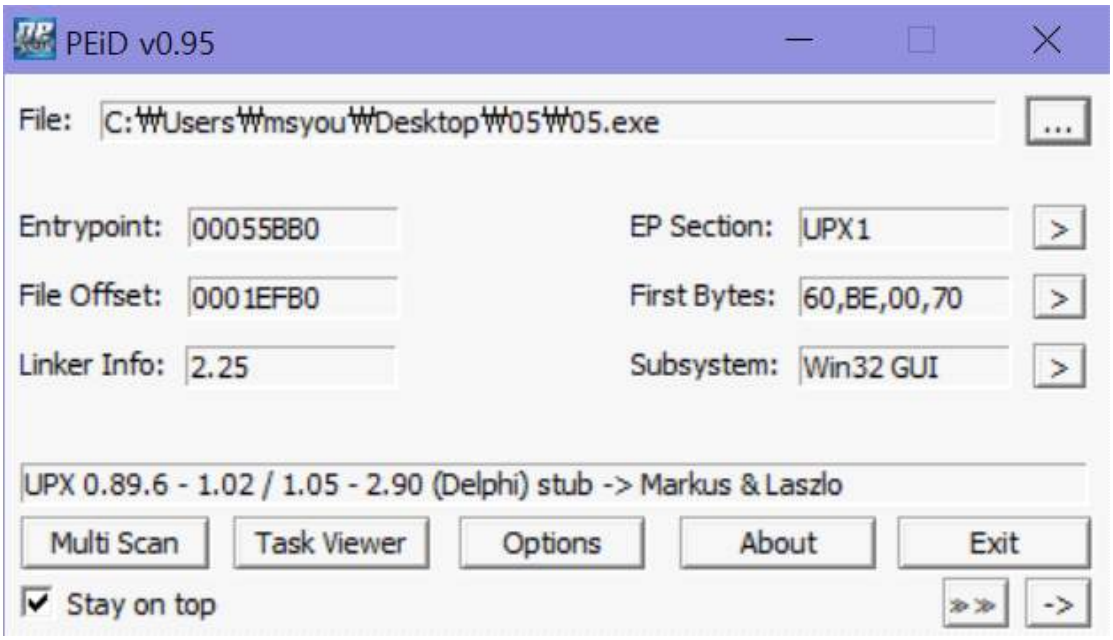
5번 실행파일을 실행하면 crackme 라는 제목의 창이 보여지고, Unregistered에 아무거나 입력하고 Register now!를 누르면, 시리얼을 찾으라고 나온다.

pFile	Raw Data	Value
00000300	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000310	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000320	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000330	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000340	00 00 0A 00 24 49 6E 66 6F 3A 20 54 68 69 73 20	....$Info: This
00000350	66 69 6C 65 20 69 73 20 70 61 63 6B 65 64 20 77	file is packed w
00000360	69 74 68 20 74 68 65 20 55 50 58 20 65 78 65 63	ith the UPX exec
00000370	75 74 61 62 6C 65 20 70 61 63 6B 65 72 20 68 74	utable packer ht
00000380	74 70 3A 2F 2F 75 70 78 2E 74 73 78 2E 6F 72 67	tp://upx.tsx.org
00000390	20 24 0A 00 24 49 64 3A 20 55 50 58 20 31 2E 30	$..$Id: UPX 1.0
000003A0	31 20 43 6F 70 79 72 69 67 68 74 20 28 43 29 20	1 Copyright (C)
000003B0	31 39 39 36 2D 32 30 30 30 20 74 68 65 20 55 50	1996-2000 the UP
000003C0	58 20 54 65 61 6D 2E 20 41 6C 6C 20 52 69 67 68	X Team. All Righ
000003D0	74 73 20 52 65 73 65 72 76 65 64 2E 20 24 0A 00	ts Reserved. $..
000003E0	55 50 58 21 0C 09 02 0A 49 31 4E DE 5F 2D CA 96	UPX!....I1N._-..
000003F0	33 37 05 00 B0 EB 01 00 00 D0 04 00 26 15 00 EB	37..........&...
00000400	2E 66 FE FF 04 10 40 00 03 07 42 6F 6F 6C 65 61	.f....@...Boolea
00000410	6E 01 00 04 15 FB DD F6 FF 05 46 61 6C 73 65 04	n.........False.
00000420	54 72 75 65 8D 0D 2C 11 02 04 43 68 61 72 1F EE	True..,...Char..
00000430	7F B7 1B FF 03 90 40 13 01 07 49 6E 74 65 67 65	......@...Intege
00000440	72 04 11 65 E5 EF DB 80 FF 00 7F 8B C0 58 17 04	r..e.......X..
00000450	42 79 2B D3 8C FC D8 6C 13 57 6F 72 64 03 FF 80	By+....l.Word...
00000460	37 C8 DC 7F 0A 06 53 74 72 69 6E 67 D4 0B 00 1F	7.....String....
00000470	9A 6E F9 BD 62 0B 10 2E 1C 03 20 24 B7 CD B2 69	.n..b..... $...i
00000480	18 B4 2B C8 10 2C 0B 07 54 96 0D 33 FF 4F 62 6A	..+..,..T..3.Obj

PEVIEW로 파일을 연 모습인데, 쭉쭉 내리다 보면 "This file is packed with the UPX executable packer ~~" 라고 나온다.

UPX로 실행 압축되어 있을거라고 추측할 수 있고, [PEiD]를 이용해 EP Section을 보면 upx로 패킹되어 있음을 확인할 수 있다.

↓

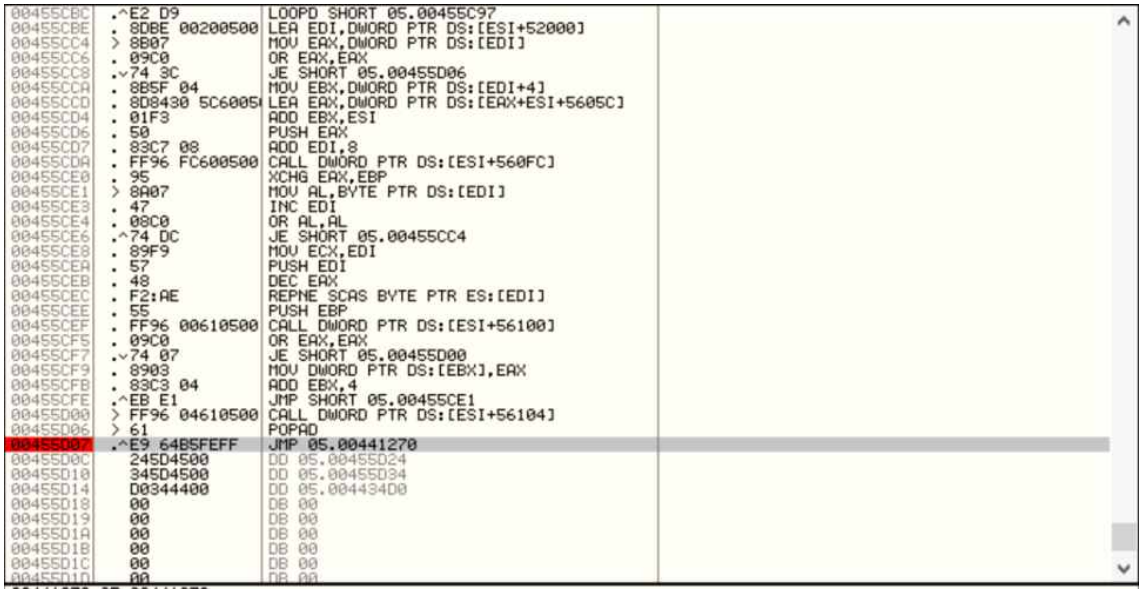


UPX는 실행 파일 압축 프로그램이고, 05.exe는 압축되어 있다는 것을 알 수 있다.
따라서 unpacking을 해주어야 한다.

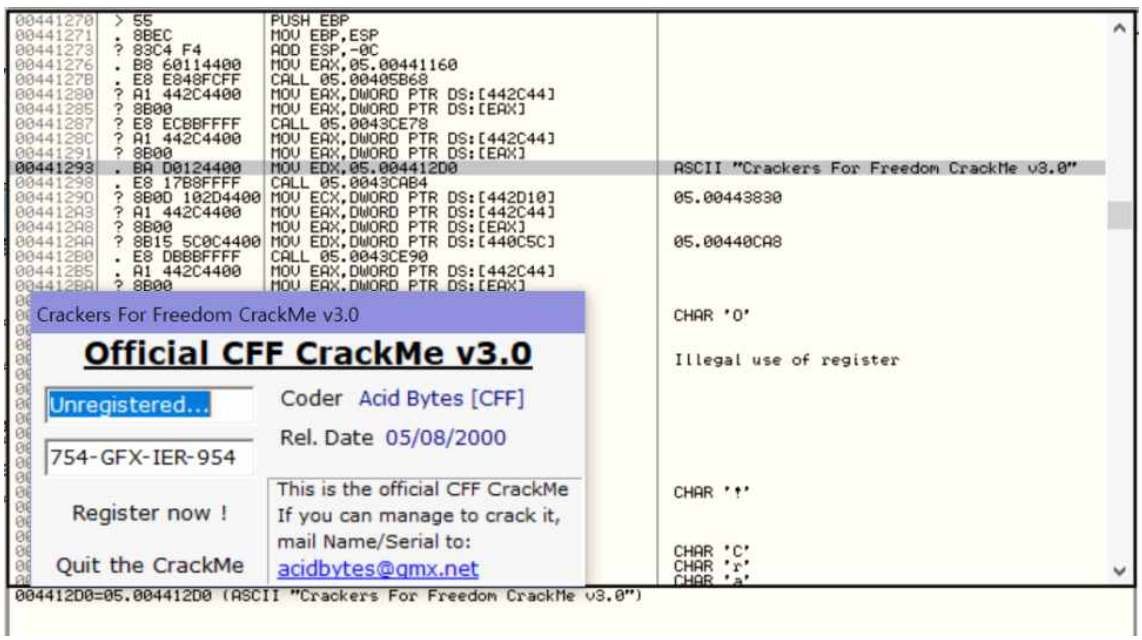
<Unpacking 과정>

1. 압축되어 있는 데이터를 읽어와서 압축 해제 후 메모리에 기록한다.
2. 압축 해제가 완료되면 CALL이나 JMP 주소를 복원한다.
3. IAT를 복구한다.
4. OEP로 이동한다.

올리디버거로 실행시켜보면, PUSHAD에서 멈추는데, 여기서 쭉 내리다보면 POPAD가 보인다. POPAD 바로 밑에 있는 JMP 명령어가 OEP로 가는 코드이다!

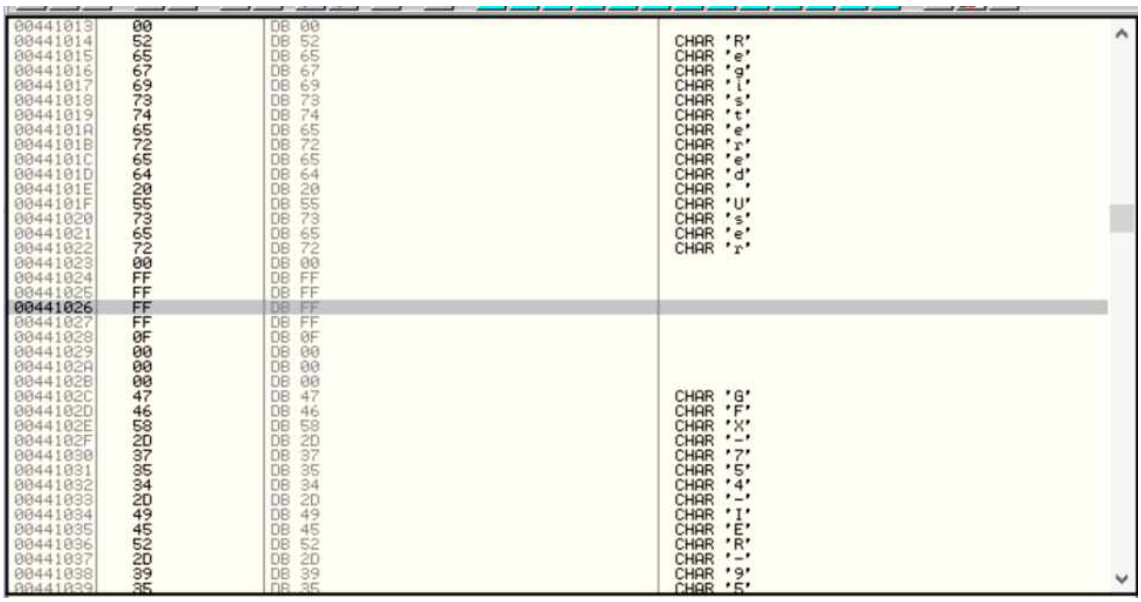


F2로 BP를 걸고 실행시킨 다음, Enter로 들어가 보면,

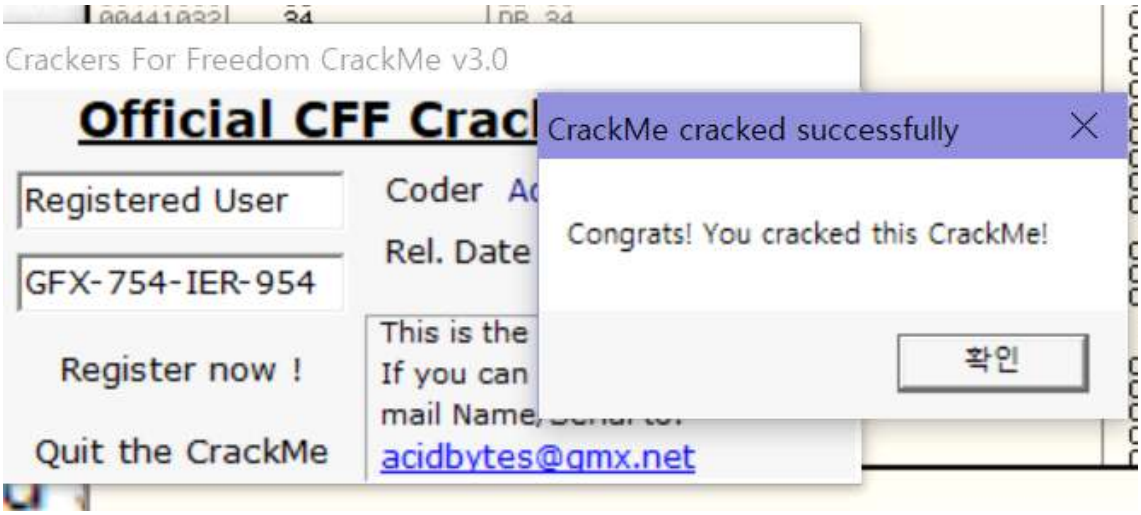


압축이 되지 않은 어셈블리어들을 볼 수가 있다.
exe파일의 제목과 같은 아스키문자열도 보인다.

이제 프로그램 등록키를 찾아야 하는데, 오른쪽 마우스 -> search for -> binary string -> ASCII 값에 처음 부분에서 에러메시지로 떴던 wrong을 입력해주었다.



이동된 주소 전후로 살펴보면 GFX-754 등등의 비슷한 키가 나오고, 위에 Registered User이란 스트링도 보인다. 해당 값을 답이라고 추측하고 exe 파일을 실행하여 값을 넣어보았다.



congrats!라고 나오며 성공메시지가 뜬다.