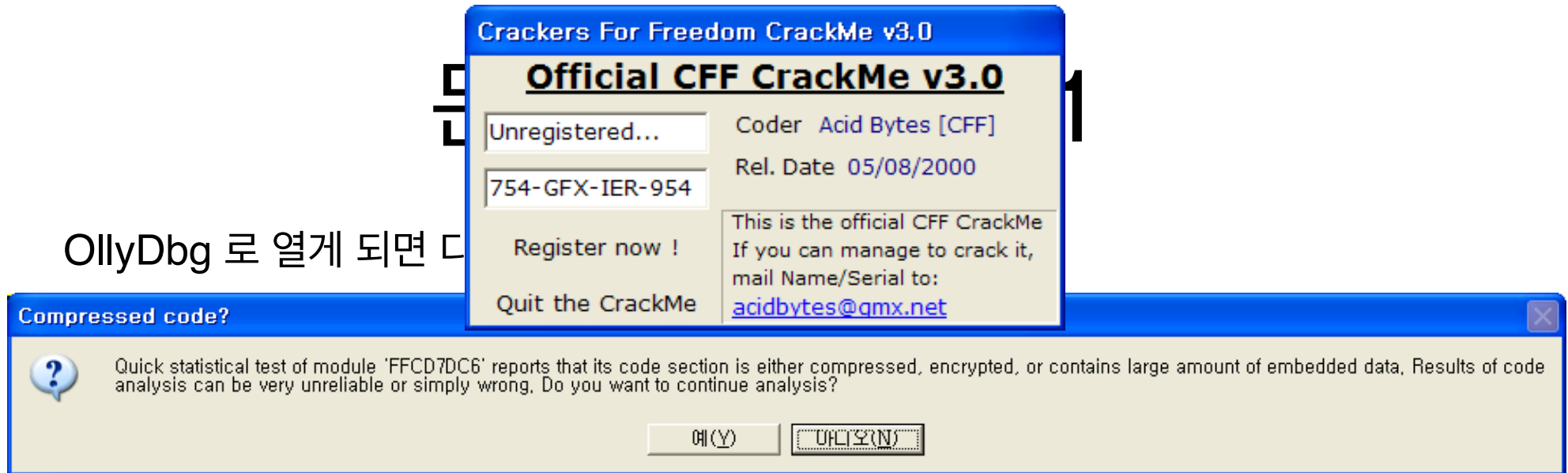


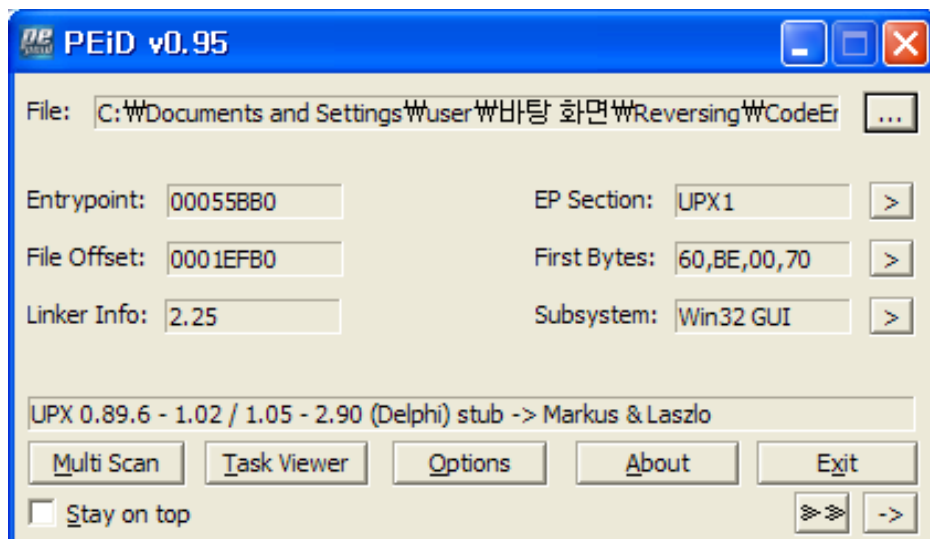
# CODE ENGN level5

문제 풀이

OllyDbg 로 열게 되면



실행 압축이 되어있어 역어셈시 잘못된 결과를 초래할 수 도 있는 것인데,  
계속 진행하기 위해서 예를 눌러줬습니다.

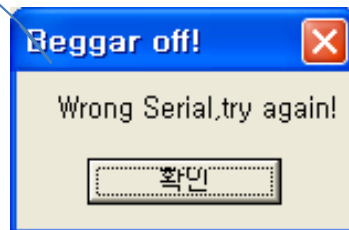


그리고 PEiD를 통해 확인을 해보니,  
UPX 로 압축되어 있는것을 확인할수  
있었습니다.



다음과 같은 코드가 뜨는 것 을 볼 수 있습니다.

보이는 것과 같이 Unregistered... 상태입니다.



이상 상태에서 Register now ! 버튼을 눌렀을때의 상황입니다. 잘못된 Serial 이라고 말해주네요.

그리고 이 메시지 박스역시  
Back to user mode를 이용해서  
리턴되는 순간을 포착하게되면  
다음과 같다.

0043D143	40	DB 40	CHAR '@'
0043D144	24	DB 24	CHAR 'z'
0043D145	50	DB 50	CHAR 'p'
0043D146	88	DB 88	
0043D147	33	DB 33	CHAR '1'
0043D148	FC	DB FC	
0043D149	FF	DB FF	
0043D14A	F8	DB F8	
0043D14B	33	DB 33	CHAR 'E'
0043D14C	50	DB 50	CHAR '3'
0043D14D	59	DB 59	CHAR '2'
0043D14E	59	DB 59	CHAR 'v'
0043D14F	59	DB 59	CHAR 'v'
0043D150	59	DB 59	CHAR 'd'
0043D151	59	DB 59	
0043D152	59	DB 59	
0043D153	59	DB 59	
0043D154	59	DB 59	
0043D155	59	DB 59	
0043D156	59	DB 59	
0043D157	59	DB 59	
0043D158	59	DB 59	
0043D159	59	DB 59	
0043D15A	59	DB 59	
0043D15B	59	DB 59	
0043D15C	59	DB 59	
0043D15D	59	DB 59	
0043D15E	59	DB 59	
0043D15F	59	DB 59	
0043D160	59	DB 59	
0043D161	59	DB 59	
0043D162	59	DB 59	
0043D163	59	DB 59	
0043D164	59	DB 59	
0043D165	59	DB 59	
0043D166	59	DB 59	
0043D167	59	DB 59	
0043D168	59	DB 59	
0043D169	59	DB 59	
0043D16A	59	DB 59	
0043D16B	59	DB 59	
0043D16C	59	DB 59	
0043D16D	59	DB 59	
0043D16E	59	DB 59	
0043D16F	59	DB 59	
0043D170	59	DB 59	
0043D171	59	DB 59	
0043D172	59	DB 59	
0043D173	59	DB 59	
0043D174	59	DB 59	
0043D175	59	DB 59	
0043D176	59	DB 59	
0043D177	59	DB 59	
0043D178	59	DB 59	
0043D179	59	DB 59	
0043D17A	59	DB 59	
0043D17B	59	DB 59	
0043D17C	59	DB 59	
0043D17D	59	DB 59	
0043D17E	59	DB 59	
0043D17F	59	DB 59	
0043D180	59	DB 59	
0043D181	59	DB 59	
0043D182	59	DB 59	
0043D183	59	DB 59	
0043D184	59	DB 59	
0043D185	59	DB 59	
0043D186	59	DB 59	
0043D187	59	DB 59	
0043D188	59	DB 59	
0043D189	59	DB 59	
0043D18A	59	DB 59	
0043D18B	59	DB 59	
0043D18C	59	DB 59	
0043D18D	59	DB 59	
0043D18E	59	DB 59	
0043D18F	59	DB 59	
0043D190	59	DB 59	
0043D191	59	DB 59	
0043D192	59	DB 59	
0043D193	59	DB 59	
0043D194	59	DB 59	
0043D195	59	DB 59	
0043D196	59	DB 59	
0043D197	59	DB 59	
0043D198	59	DB 59	
0043D199	59	DB 59	
0043D19A	59	DB 59	
0043D19B	59	DB 59	
0043D19C	59	DB 59	
0043D19D	59	DB 59	
0043D19E	59	DB 59	
0043D19F	59	DB 59	
0043D1A0	59	DB 59	
0043D1A1	59	DB 59	
0043D1A2	59	DB 59	
0043D1A3	59	DB 59	
0043D1A4	59	DB 59	
0043D1A5	59	DB 59	
0043D1A6	59	DB 59	
0043D1A7	59	DB 59	
0043D1A8	59	DB 59	
0043D1A9	59	DB 59	
0043D1AA	59	DB 59	
0043D1AB	59	DB 59	
0043D1AC	59	DB 59	
0043D1AD	59	DB 59	
0043D1AE	59	DB 59	
0043D1AF	59	DB 59	
0043D1B0	59	DB 59	
0043D1B1	59	DB 59	
0043D1B2	59	DB 59	
0043D1B3	59	DB 59	
0043D1B4	59	DB 59	
0043D1B5	59	DB 59	
0043D1B6	59	DB 59	
0043D1B7	59	DB 59	
0043D1B8	59	DB 59	
0043D1B9	59	DB 59	
0043D1BA	59	DB 59	
0043D1BB	59	DB 59	
0043D1BC	59	DB 59	
0043D1BD	59	DB 59	
0043D1BE	59	DB 59	
0043D1BF	59	DB 59	
0043D1C0	59	DB 59	
0043D1C1	59	DB 59	
0043D1C2	59	DB 59	
0043D1C3	59	DB 59	
0043D1C4	59	DB 59	
0043D1C5	59	DB 59	
0043D1C6	59	DB 59	
0043D1C7	59	DB 59	
0043D1C8	59	DB 59	
0043D1C9	59	DB 59	
0043D1CA	59	DB 59	
0043D1CB	59	DB 59	
0043D1CC	59	DB 59	
0043D1CD	59	DB 59	
0043D1CE	59	DB 59	
0043D1CF	59	DB 59	
0043D1D0	59	DB 59	
0043D1D1	59	DB 59	
0043D1D2	59	DB 59	
0043D1D3	59	DB 59	
0043D1D4	59	DB 59	
0043D1D5	59	DB 59	
0043D1D6	59	DB 59	
0043D1D7	59	DB 59	
0043D1D8	59	DB 59	
0043D1D9	59	DB 59	
0043D1DA	59	DB 59	
0043D1DB	59	DB 59	
0043D1DC	59	DB 59	
0043D1DD	59	DB 59	
0043D1DE	59	DB 59	
0043D1DF	59	DB 59	
0043D1E0	59	DB 59	
0043D1E1	59	DB 59	
0043D1E2	59	DB 59	
0043D1E3	59	DB 59	
0043D1E4	59	DB 59	
0043D1E5	59	DB 59	
0043D1E6	59	DB 59	
0043D1E7	59	DB 59	
0043D1E8	59	DB 59	
0043D1E9	59	DB 59	
0043D1EA	59	DB 59	
0043D1EB	59	DB 59	
0043D1EC	59	DB 59	
0043D1ED	59	DB 59	
0043D1EE	59	DB 59	
0043D1EF	59	DB 59	
0043D1F0	59	DB 59	
0043D1F1	59	DB 59	
0043D1F2	59	DB 59	
0043D1F3	59	DB 59	
0043D1F4	59	DB 59	
0043D1F5	59	DB 59	
0043D1F6	59	DB 59	
0043D1F7	59	DB 59	
0043D1F8	59	DB 59	
0043D1F9	59	DB 59	
0043D1FA	59	DB 59	
0043D1FB	59	DB 59	
0043D1FC	59	DB 59	
0043D1FD	59	DB 59	
0043D1FE	59	DB 59	
0043D1FF	59	DB 59	



하지만 스택을 따라가는 것은 시간이 더 많이 걸리고 따라서  
역추적으로 이 함수를 호출한곳을 찾아가보겠습니다.

```

74 06 JE SHORT FFC07DC6.0043012E
81CB 00001000 OR EBX,100000
3407 XOR EBX,ESI
55 PUSH EBP
68 ADD14300 PUSH FFC07DC6.004301A0
64:FF31 PUSH DWORD PTR FS:[ECX]
64:8921 MOV DWORD PTR FS:[ECX],ESP
53
57
56
8B45 FC
8B40 24
50
E8 3191FCFF
8945 F8
33C0
5A
59
59
64:8910
68 B4D14300
> 8B45 EC
3B45 E8

```

이런  
하지  
Working...에서는 무조건  
이된다.  
따라서 이전 proc를 확인해봐야 합니다.

0012F928	0012F99C	Pointer to next SEH record
0012F92C	0043D1AD	SE handler
0012F930	0012F990	
0012F934	00000000	
0012F938	00A18AA8	
0012F93C	00A12608	
0012F940	00A19414	
0012F944	0000001C	
0012F948	004023C5	RETURN to FFC07DC6.004023C5 from FFC07DC6.00401DF4
0012F94C	0012F99C	
0012F950	FFC07DC6.004023EE	
0012F954	FFC07DC6.004023F5	
0012F958	00A1943C	ASCII "Unregistered..."

스택을 확인해보면  
이 함수를 호출한 위치를 알 수 있습니다.

6A 00 B9 C80F4400 BA D80F4400 A1 442C4400 8B00 E8 76C1FFFF 8D55 FC 8B83 C8020000 E8 20FFFDFF 837D FC 00 75 18 6A 00 B9 E80F4400 BA FC0F4400 A1 442C4400 8B00 E8 4AC1FFFF 8D55 FC 8B83 C4020000 E8 F4FEFDFF 8B45 FC BA 14104400 E8 F32BFCFF 75 51 8D55 FC 8B83 C8020000 E8 D7FEFDFF 8B45 FC BA 2C104400 E8 D62BFCFF 75 1A 6A 00 B9 3C104400 BA 5C104400 A1 442C4400 8B00 E8 F8C0FFFF EB 32 6A 00 B9 80104400 BA 8C104400 A1 442C4400 8B00 E8 DEC0FFFF EB 18 6A 00 B9 80104400 BA 8C104400 A1 442C4400 8B00 E8 C4C0FFFF 33C6	 PUSH 0 MOV ECX,FFCD7DC6.00440FC8 MOV EDX,FFCD7DC6.00440FD8 MOV EAX,DWORD PTR DS:[442C44] MOV EAX,DWORD PTR DS:[EAX] CALL FFCD7DC6.0043D068 LEA EDX,[LOCAL.1] MOV EAX,DWORD PTR DS:[EBX+2C8] CALL FFCD7DC6.00420E20 CMP [LOCAL.1],0 JNZ SHORT FFCD7DC6.00440F1E PUSH 0 MOV ECX,FFCD7DC6.00440FE8 MOV EDX,FFCD7DC6.00440FFC MOV EAX,DWORD PTR DS:[442C44] MOV EAX,DWORD PTR DS:[EAX] CALL FFCD7DC6.0043D068 LEA EDX,[LOCAL.1] MOV EAX,DWORD PTR DS:[EBX+2C4] CALL FFCD7DC6.00420E20 MOV EAX,[LOCAL.1] MOV EDX,FFCD7DC6.00441014 CALL FFCD7DC6.00403B2C JNZ SHORT FFCD7DC6.00440F8C LEA EDX,[LOCAL.1] MOV EAX,DWORD PTR DS:[EBX+2C8] CALL FFCD7DC6.00420E20 MOV EAX,[LOCAL.1] MOV EDX,FFCD7DC6.0044102C CALL FFCD7DC6.00403B2C JNZ SHORT FFCD7DC6.00440F72 PUSH 0 MOV ECX,FFCD7DC6.0044103C MOV EDX,FFCD7DC6.0044105C MOV EAX,DWORD PTR DS:[442C44] MOV EAX,DWORD PTR DS:[EAX] CALL FFCD7DC6.0043D068 JMP SHORT FFCD7DC6.00440FA4 PUSH 0 MOV ECX,FFCD7DC6.00441080 MOV EDX,FFCD7DC6.0044108C MOV EAX,DWORD PTR DS:[442C44] MOV EAX,DWORD PTR DS:[EAX] CALL FFCD7DC6.0043D068 JMP SHORT FFCD7DC6.00440FA4 PUSH 0 MOV ECX,FFCD7DC6.00441080 MOV EDX,FFCD7DC6.0044108C MOV EAX,DWORD PTR DS:[442C44] MOV EAX,DWORD PTR DS:[EAX] CALL FFCD7DC6.0043D068 VBB ENQ ENQ	 ASCII "No Name entered" ASCII "Enter a Name!"          ASCII "No Serial entered" ASCII "Enter a Serial!"       ASCII "Registered User"       ASCII "GFX-754-IER-954"       ASCII "CrackMe cracked successfully" ASCII "Congrats! You cracked this CrackMe!"       ASCII "Beggar off!" ASCII "Wrong Serial,try again!"       ASCII "Beggar off!" ASCII "Wrong Serial,try again!"
---	---	---

그리고 이러한 코드를 확인할 수 있습니다.

분기문으써 점프하면  
잘못된 코드라는 MessageBox를  
볼 수 있다.

따라서 분기문을 만나기 전에 호출하는 함수가 문자열 비교함수임을  
알 수 있고 그전에 넣어주는것인 이름과 시리얼 값임을 알 수 있습니다.

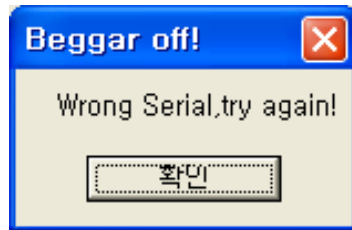
# 검증



앞서  
따라

00455BB0	> 50	PUSHAD	
00455BB1	. BE 00704300	MOV ESI,FFCD7DC6.00437000	
00455BB6	. 8DBE 00A0FCFF	LEA EDI,DWORD PTR DS:[ESI+FFFC0000]	
00455BBC	. C787 00240400 71	MOV DWORD PTR DS:[EDI+42400],689C0471	
00455BC6	. 57	PUSH EDI	
00455BC7	. 83CD FF	OR EBP,FFFFFFFF	ntdll.7C940228
00455BCA	~ EB 0E	JMP SHORT FFCD7DC6.00455BDA	
00455BCC	. 90	NOP	
00455BCD	. 90	NOP	
00455BCE	. 90	NOP	
00455BCF	. 90	NOP	
00455BD0	> 8A06	MOV AL,BYTE PTR DS:[ESI]	
00455BD2	. 46	INC ESI	
00455BD3	. 8807	MOV BYTE PTR DS:[EDI],AL	
00455BD5	. 47	INC EDI	ntdll.7C940228
00455BD6	> 01DB	ADD EBX,EBX	
00455BD8	~ 75 07	JNZ SHORT FFCD7DC6.00455BE1	
00455BDA	> 8B1E	MOV EBX,DWORD PTR DS:[ESI]	
00455BDC	. 83EE FC	SUB ESI,-4	
00455BDF	. 110B	ADC EBX,EBX	
00455BE1	> 72 ED	JB SHORT FFCD7DC6.00455BD0	
00455BE3	. B8 01000000	MOV EAX,1	
00455BE8	> 01DB	ADD EBX,EBX	
00455BEA	~ 75 07	JNZ SHORT FFCD7DC6.00455BF3	
00455BEC	. 8B1E	MOV EBX,DWORD PTR DS:[ESI]	
00455BEE	. 83EE FC	SUB ESI,-4	
00455BF1	. 110B	ADC EBX,EBX	
00455BF3	> 11C0	ADC EAX,EAX	
00455BF5	. 010B	ADD EBX,EBX	
00455BF7	~ 73 EF	JNB SHORT FFCD7DC6.00455BE8	
00455BF9	~ 75 09	JNZ SHORT FFCD7DC6.00455C04	
00455BFB	. 8B1E	MOV EBX,DWORD PTR DS:[ESI]	
00455BFD	. 83EE FC	SUB ESI,-4	
00455C00	. 110B	ADC EBX,EBX	
00455C02	~ 73 E4	JNB SHORT FFCD7DC6.00455BE8	
00455C04	> 31C9	XOR ECX,ECX	
00455C06	. 83E8 03	SUB EAX,3	
00455C09	~ 72 00	JB SHORT FFCD7DC6.00455C18	
00455C0B	. C1E0 08	SHL EAX,8	
00455C0E	. 8A06	MOV AL,BYTE PTR DS:[ESI]	
00455C10	. 46	INC ESI	
00455C11	. 83F0 FF	XOR EAX,FFFFFFFF	
00455C14	~ 74 74	JE SHORT FFCD7DC6.00455C8A	
00455C16	. 89C5	MOV EBP,EAX	
00455C18	> 01DB	ADD EBX,EBX	
00455C1A	~ 75 07	JNZ SHORT FFCD7DC6.00455C23	
00455C1C	. 8B1E	MOV EBX,DWORD PTR DS:[ESI]	
00455C1E	. 83EE FC	SUB ESI,-4	
00455C21	. 110B	ADC EBX,EBX	
00455C23	> 11C9	ADC ECX,ECX	
00455C25	. 01DB	ADD EBX,EBX	
00455C27	~ 75 07	JNZ SHORT FFCD7DC6.00455C30	
00455C29	. 8B1E	MOV EBX,DWORD PTR DS:[ESI]	
00455C2B	. 83EE FC	SUB ESI,-4	
00455C2E	. 110B	ADC EBX,EBX	
00455C30	> 11C9	ADC ECX,ECX	
00455C32	~ 75 20	JNZ SHORT FFCD7DC6.00455C54	
00455C34	. 41	INC ECX	
00455C35	> 01DB	ADD EBX,EBX	
00455C37	~ 75 07	JNZ SHORT FFCD7DC6.00455C40	
00455C39	. 8B1E	MOV EBX,DWORD PTR DS:[ESI]	
00455C3B	. 83EE FC	SUB ESI,-4	
00455C3E	. 110B	ADC EBX,EBX	
00455C40	> 11C9	ADC ECX,ECX	
00455C42	. 01DB	ADD EBX,EBX	
00455C44	~ 73 EF	JNB SHORT FFCD7DC6.00455C35	
00455C46	~ 75 09	JNZ SHORT FFCD7DC6.00455C51	





이제 팩킹이 풀렸으므로 간단히 문자열을 검색해보게되면

00440E9C DD FFC07DC6.00440CA8	ASCII "4wB"
00440EA7 ASCII "Unit1"	
00440EDC MOV ECX,FFC07DC6.00440FC8	ASCII "No Name entered"
00440EE1 MOV EDX,FFC07DC6.00440FD8	ASCII "Enter a Name!"
00440F08 MOV ECX,FFC07DC6.00440FE8	ASCII "No Serial entered"
00440F0D MOV EDX,FFC07DC6.00440FFC	ASCII "Enter a Serial!"
00440F2F MOV EDX,FFC07DC6.00441014	ASCII "Registered User"
00440F4C MOV EDX,FFC07DC6.0044102C	ASCII "GFX-754-IER-954"
00440F5A MOV ECX,FFC07DC6.0044103C	ASCII "CrackMe cracked successfully"
00440F5F MOV EDX,FFC07DC6.0044105C	ASCII "Congrats! You cracked this CrackMe!"
00440F74 MOV ECX,FFC07DC6.00441080	ASCII "Beggar off!"
00440F79 MOV EDX,FFC07DC6.0044108C	ASCII "Wrong Serial,try again!"
00440F8E MOV ECX,FFC07DC6.00441080	ASCII "Beggar off!"
00440F93 MOV EDX,FFC07DC6.0044108C	ASCII "Wrong Serial,try again!"
00440FC8 ASCII "No Name entered",0	
00440FD8 ASCII "Enter a Name!".0	

이렇게 이름과 serial 키가 보이는것을 확인할 수 있습니다.