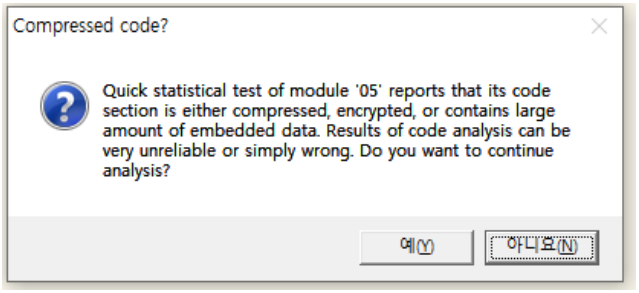
문제: 이 프로그램의 등록키는 무엇인가

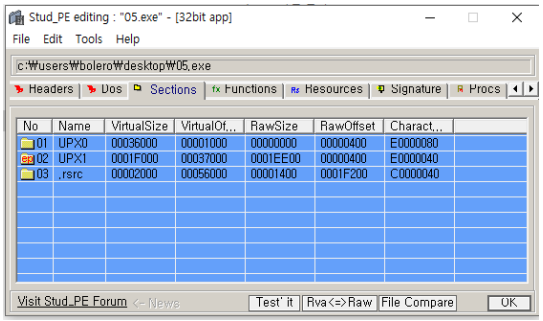
일단 그냥 실행하면

이렇게 뜸. 변경도 가능

디버거로 열어보자



이런 문구가 뜬다. 구글에서 찾아보니까 UPX 패킹 뭐라하는데 STUD-PE로 까보았다



대충 UPX0, UPX1 이런 거 있는 거 보니 패킹되어있는 듯...

언패킹 할려면? 팩 과정을 찾아내서 그 부분에 BP를 걸고 디버깅을 한다.

1. **PUSHAD 과정 찾기**
2. **중간을 넘어서, POPAD 과정 찾기**(AD를 PUSH와 POP 한다는 것인가 보다.)

1. PUSHAD 과정을 찾는다.

- 여기서 PUSHAD 란 PACKING 과정을 위해 모든 Register 들을 Stack 에 PUSH 하는 과정을 의미합니다.

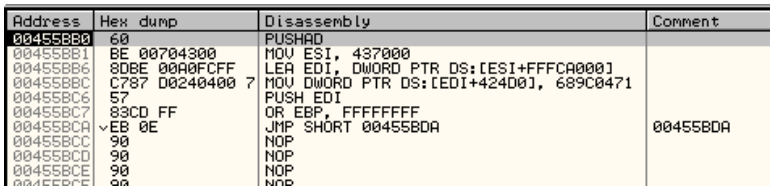
2. 중간을 넘어서, POPAD 과정을 찾는다.

- 여기서 POPAD 란 PACKING 과정이 모두 끝난 후에,
OEP 위치 직전에서 프로그램 실행을 위해 다시 모든 Register 위치에 원래대로 값을 복원시키는 것을 말합니다.

출처: 내 블로그 ㅎㅎ

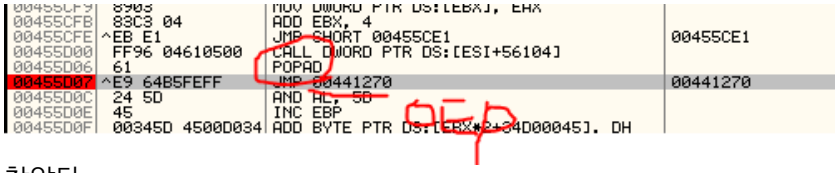
n1094.tistory.com

일단 무조건 UPX 패킹된 PE 파일을 디버거로 오픈하면 PUSHAD를 볼 수 있다.



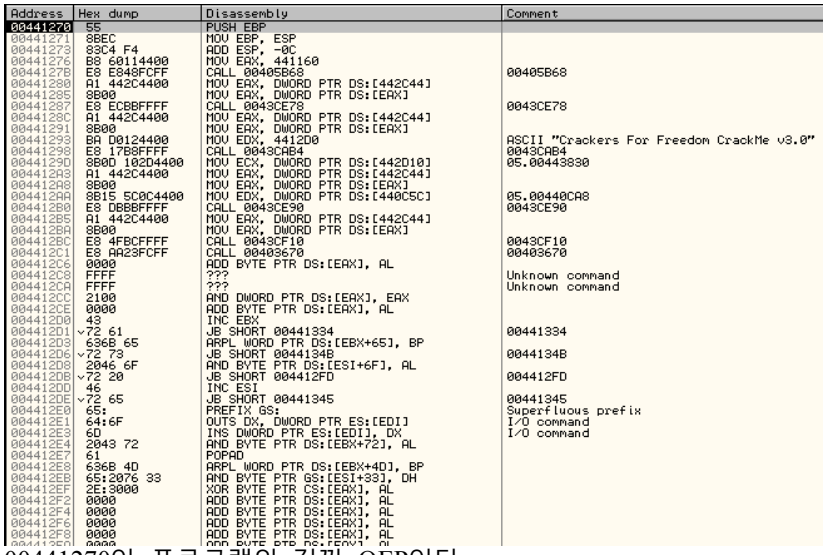
Address	Hex dump	Disassembly	Comment
00455BB0	60	PUSHAD	
00455BB1	BE 00704300	MOV ESI, 437000	
00455BB6	8DBE 00A0FCFF	LEA EDI, DWORD PTR DS:[ESI+FFFCA000]	
00455BBC	C787 D0240400 7	MOV DWORD PTR DS:[EDI+424D0], 689C0471	
00455BC6	57	PUSH EDI	
00455BC7	83CD FF	OR EBP, FFFFFFFF	
00455BCA	EB 0E	JMP SHORT 00455BDA	00455BDA
00455BCC	90	NOP	
00455BCD	90	NOP	
00455BCE	90	NOP	

PUSHAD 이후부터 POPAD 까지 있는 모든 소스는 UPX 패킹을 위한 것이므로, 뛰어넘는다.
스크롤 다운 해보면 POPAD를 무조건 찾을 수 있을 것으로 생각한다.



00455CF9	8903	MOV DWORD PTR DS:[EBX], EAX	
00455CFB	83C3 04	ADD EBX, 4	
00455CFE	EB E1	JMP SHORT 00455CE1	00455CE1
00455D00	FF96 04610500	CALL DWORD PTR DS:[ESI+56104]	
00455D06	61	POPAD	
00455D07	E9 64B5FEFF	JMP 00441270	00441270
00455D0C	24 5D	AND AL, 5D	
00455D0E	45	INC EBP	
00455D0F	00345D 4500D034	ADD BYTE PTR DS:[EBX*2+34D00045], DH	

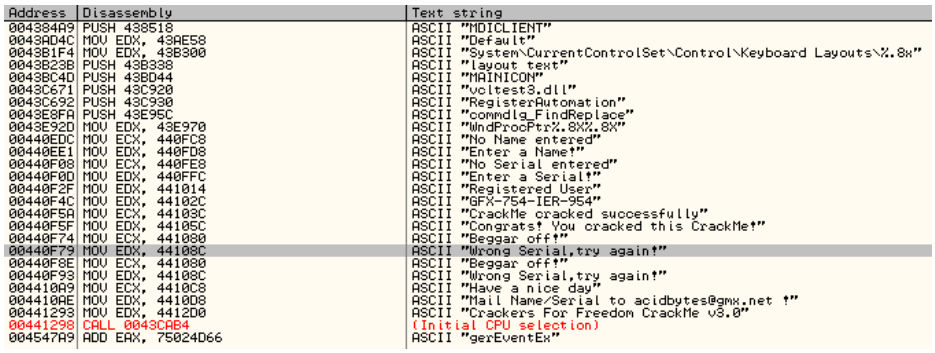
찾았다.
그러면 JMP 부분에 BP를 걸고 F9로 실행. BP에서 멈추면 F7로 step into하기!



Address	Hex dump	Disassembly	Comment
00441270	55	PUSH EBP	
00441271	8BEC	MOV EBP, ESP	
00441273	83C4 F4	ADD ESP, -0C	
00441276	B8 60114400	MOV EAX, 441160	
0044127B	E8 E548FCFF	CALL 00405B68	00405B68
00441280	A1 442C4400	MOV EAX, DWORD PTR DS:[442C44]	
00441285	8B00	MOV EAX, DWORD PTR DS:[EAX]	
00441287	E8 ECBBFFFF	CALL 0043CE78	0043CE78
0044128C	A1 442C4400	MOV EAX, DWORD PTR DS:[442C44]	
00441291	8B00	MOV EAX, DWORD PTR DS:[EAX]	
00441293	BA D0124400	MOV EDX, 4412D0	ASCII "Crackers For Freedom CrackMe v3.0"
00441298	E8 17B8FFFF	CALL 0043CAB4	0043CAB4
0044129D	8B0D 102D4400	MOV ECX, DWORD PTR DS:[442D10]	05.00443830
004412A3	A1 442C4400	MOV EAX, DWORD PTR DS:[442C44]	
004412A8	8B00	MOV EAX, DWORD PTR DS:[EAX]	
004412AA	8B15 5C0C4400	MOV EDX, DWORD PTR DS:[440C5C]	05.00440CA8
004412B0	E8 DBBBFFFF	CALL 0043CE90	0043CE90
004412B5	A1 442C4400	MOV EAX, DWORD PTR DS:[442C44]	
004412BA	8B00	MOV EAX, DWORD PTR DS:[EAX]	
004412BC	E8 4FBCFFFF	CALL 0043CF10	0043CF10
004412C1	E8 AA29FCFF	CALL 00403670	00403670
004412C6	0000	ADD BYTE PTR DS:[EAX], AL	
004412C8	FFFF	???	Unknown command
004412CA	FFFF	???	Unknown command
004412CC	2100	AND DWORD PTR DS:[EAX], EAX	
004412CE	0000	ADD BYTE PTR DS:[EAX], AL	
004412D0	43	INC EBX	
004412D1	72 61	JB SHORT 00441334	00441334
004412D3	636B 65	ARPL WORD PTR DS:[EBX+65], BP	
004412D6	72 73	JB SHORT 0044134B	0044134B
004412D8	2046 6F	AND BYTE PTR DS:[ESI+6F], AL	
004412DB	72 20	JB SHORT 004412FD	004412FD
004412DD	46	INC ESI	
004412DE	72 65	JB SHORT 00441345	00441345
004412E0	65:	PREFIX GS:	Superfluous prefix
004412E1	64:6F	OUTS DX, DWORD PTR ES:[EDI]	I/O command
004412E3	6D	INS DWORD PTR ES:[EDI], DX	I/O command
004412E4	2043 72	AND BYTE PTR DS:[EBX+72], AL	
004412E7	61	POPAD	
004412E8	636B 4D	ARPL WORD PTR DS:[EBX+4D], BP	
004412EB	65:2076 33	AND BYTE PTR GS:[ESI+33], DH	
004412EF	2E:3000	XOR BYTE PTR CS:[EAX], AL	
004412F2	0000	ADD BYTE PTR DS:[EAX], AL	
004412F4	0000	ADD BYTE PTR DS:[EAX], AL	
004412F6	0000	ADD BYTE PTR DS:[EAX], AL	
004412F8	0000	ADD BYTE PTR DS:[EAX], AL	

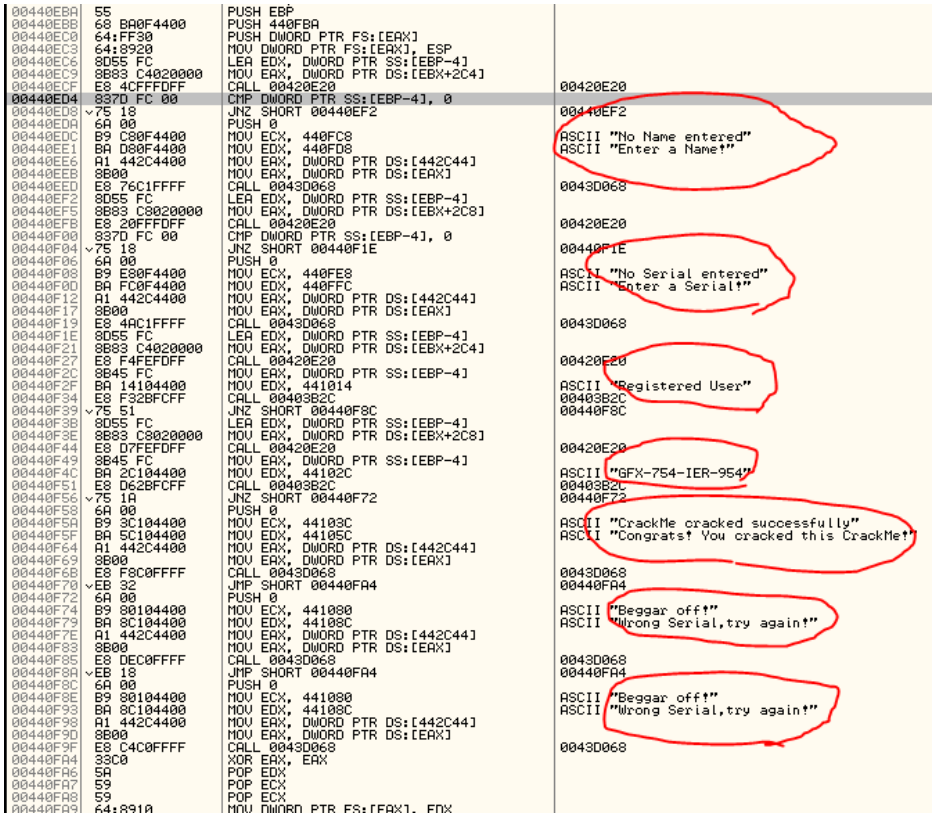
00441270이 프로그램의 진짜 OEP이다.
그럼 일단 프로그램을 실행시켜 보자.

Wrong Serial,try again! 문자열 확인 -> Search for -> All referenced text strings 로 해당 문자열 검색하기.



```
Address   Disassembly              Text string
004384A9  PUSH 438518              ASCII "MDICLIENT"
0043AD4C  MOV EDX, 43AE58          ASCII "Default"
0043B1F4  MOV EDX, 43B300          ASCII "System\CurrentControlSet\Control\Keyboard Layouts\%.8x"
0043B23B  PUSH 43B338              ASCII "layout text"
0043BC4D  PUSH 43BD44              ASCII "MAINICON"
0043C671  PUSH 43C920              ASCII "voltest3.dll"
0043C692  PUSH 43C930              ASCII "RegisterAutomation"
0043E8FA  PUSH 43E95C              ASCII "commdlg_FindReplace"
0043E92D  MOV EDX, 43E970          ASCII "WndProcPtr%.8X%.8X"
00440EDC  MOV ECX, 440FC8          ASCII "No Name entered"
00440EE1  MOV EDX, 440FD8          ASCII "Enter a Name!"
00440F08  MOV ECX, 440FE8          ASCII "No Serial entered"
00440F0D  MOV EDX, 440FFC          ASCII "Enter a Serial!"
00440F2F  MOV EDX, 441014          ASCII "Registered User"
00440F4C  MOV EDX, 44102C          ASCII "GFX-754-IER-954"
00440F5A  MOV ECX, 44103C          ASCII "CrackMe cracked successfully"
00440F5F  MOV EDX, 44105C          ASCII "Congrats! You cracked this CrackMe!"
00440F74  MOV ECX, 441080          ASCII "Beggar off!"
00440F79  MOV EDX, 44108C          ASCII "Wrong Serial,try again!"
00440F8E  MOV ECX, 441090          ASCII "Beggar off!"
00440F93  MOV EDX, 44108C          ASCII "Wrong Serial,try again!"
004410A9  MOV ECX, 4410C8          ASCII "Have a nice day"
004410AE  MOV EDX, 4410D8          ASCII "Mail Name/Serial to acidbytes@gmx.net !"
00441293  MOV EDX, 4412D0          ASCII "Crackers For Freedom CrackMe v3.0"
00441298  CALL 0043CAB4            (Initial CPU selection)
004547A9  ADD EAX, 75024D66        ASCII "gerEventEx"
```

있다... 더블클릭해서 이동!



```
00440EBA  55                 PUSH EBP
00440EBB  68 BA0F4400        PUSH 440FBA
00440EC0  64:FF30            PUSH DWORD PTR FS:[EAX]
00440EC3  64:8920            MOV DWORD PTR FS:[EAX], ESP
00440EC6  8D55 FC            LEA EDX, DWORD PTR SS:[EBP-4]
00440EC9  8B83 C4020000      MOV EAX, DWORD PTR DS:[EBX+2C4]
00440ECF  E8 4CFFFDFF        CALL 00420E20                          00420E20
00440ED4  837D FC 00         CMP DWORD PTR SS:[EBP-4], 0
00440ED8  75 18              JNZ SHORT 00440EF2                     00440EF2
00440EDA  6A 00              PUSH 0
00440EDC  B9 C80F4400        MOV ECX, 440FC8                        ASCII "No Name entered"
00440EE1  BA D80F4400        MOV EDX, 440FD8                        ASCII "Enter a Name!"
00440EE6  A1 442C4400        MOV EAX, DWORD PTR DS:[442C44]
00440EEB  8B00               MOV EAX, DWORD PTR DS:[EAX]
00440EED  E8 76C1FFFF        CALL 0043D068                          0043D068
00440EF2  8D55 FC            LEA EDX, DWORD PTR SS:[EBP-4]
00440EF5  8B83 C8020000      MOV EAX, DWORD PTR DS:[EBX+2C8]
00440EFB  E8 20FFFDFF        CALL 00420E20                          00420E20
00440F00  837D FC 00         CMP DWORD PTR SS:[EBP-4], 0
00440F04  75 18              JNZ SHORT 00440F1E                     00440F1E
00440F06  6A 00              PUSH 0
00440F08  B9 E80F4400        MOV ECX, 440FE8                        ASCII "No Serial entered"
00440F0D  BA FC0F4400        MOV EDX, 440FFC                        ASCII "Enter a Serial!"
00440F12  A1 442C4400        MOV EAX, DWORD PTR DS:[442C44]
00440F17  8B00               MOV EAX, DWORD PTR DS:[EAX]
00440F19  E8 4AC1FFFF        CALL 0043D068                          0043D068
00440F1E  8D55 FC            LEA EDX, DWORD PTR SS:[EBP-4]
00440F21  8B83 C4020000      MOV EAX, DWORD PTR DS:[EBX+2C4]
00440F27  E8 F4FEFDFF        CALL 00420E20                          00420E20
00440F2C  8B45 FC            MOV EAX, DWORD PTR SS:[EBP-4]
00440F2F  BA 14104400        MOV EDX, 441014                        ASCII "Registered User"
00440F34  E8 F32BFCFF        CALL 00403B2C                          00403B2C
00440F39  75 51              JNZ SHORT 00440F8C                     00440F8C
00440F3B  8D55 FC            LEA EDX, DWORD PTR SS:[EBP-4]
00440F3E  8B83 C8020000      MOV EAX, DWORD PTR DS:[EBX+2C8]
00440F44  E8 D7FEFDFF        CALL 00420E20                          00420E20
00440F49  8B45 FC            MOV EAX, DWORD PTR SS:[EBP-4]
00440F4C  BA 2C104400        MOV EDX, 44102C                        ASCII "GFX-754-IER-954"
00440F51  E8 D62BFCFF        CALL 00403B2C                          00403B2C
00440F56  75 1A              JNZ SHORT 00440F72                     00440F72
00440F58  6A 00              PUSH 0
00440F5A  B9 3C104400        MOV ECX, 44103C                        ASCII "CrackMe cracked successfully"
00440F5F  BA 5C104400        MOV EDX, 44105C                        ASCII "Congrats! You cracked this CrackMe!"
00440F64  A1 442C4400        MOV EAX, DWORD PTR DS:[442C44]
00440F69  8B00               MOV EAX, DWORD PTR DS:[EAX]
00440F6B  E8 F8C0FFFF        CALL 0043D068                          0043D068
00440F70  EB 32              JMP SHORT 00440FA4                     00440FA4
00440F72  6A 00              PUSH 0
00440F74  B9 80104400        MOV ECX, 441080                        ASCII "Beggar off!"
00440F79  BA 8C104400        MOV EDX, 44108C                        ASCII "Wrong Serial,try again!"
00440F7E  A1 442C4400        MOV EAX, DWORD PTR DS:[442C44]
00440F83  8B00               MOV EAX, DWORD PTR DS:[EAX]
00440F85  E8 DEC0FFFF        CALL 0043D068                          0043D068
00440F8A  EB 18              JMP SHORT 00440FA4                     00440FA4
00440F8C  6A 00              PUSH 0
00440F8E  B9 80104400        MOV ECX, 441080                        ASCII "Beggar off!"
00440F93  BA 8C104400        MOV EDX, 44108C                        ASCII "Wrong Serial,try again!"
00440F98  A1 442C4400        MOV EAX, DWORD PTR DS:[442C44]
00440F9D  8B00               MOV EAX, DWORD PTR DS:[EAX]
00440F9F  E8 C4C0FFFF        CALL 0043D068                          0043D068
00440FA4  33C0               XOR EAX, EAX
00440FA6  5A                 POP EDX
00440FA7  59                 POP ECX
00440FA8  59                 POP ECX
00440FA9  64:8910            MOV DWORD PTR FS:[EAX], EDX
```

중요한 부분만 가져왔다. (원래 push ebp 와 mov ebp, esp로 이루어져 있는 함수의 prologue 부분을 찾고 싶었는데 찾지 못함...)

보면 문자열이 크게 7개가 있다. (빨간색 동그라미)

1. No Name entered! Enter a Name! : 아마 username을 치는 dialog box 안에 문자열이 없는 경우 출력하는 오류 메시지로 추정됨.

2. No Serial entered! Enter a Serial! : 1번처럼 Serial number를 치는 dialog box 안에 문자열이 없는 경우 출력하는 오류 메시지로 추정.

3. Registered User : 아마 정답 사용자겠죠?

```
MOV EAX, DWORD PTR SS:[EBP-4]
MOV EDX, 441014                          ASCII "Registered User"
CALL 00403B2C                            00403B2C
JNZ SHORT 00440F8C                       00440F8C
```

이유를 알기 위해 4줄만 캡쳐해옴.
일단 MOV EAX, DWORD PTR SS:[EBP-4]
더블워드 크기의 포인터 EBP-4 위치의 값을 EAX로 옮김
MOV EDX, 441014 이건 441014 위치의 값을 EDX로 옮김
comment처럼 00441014 위치에는 "Registered User" 문자열이 있을 것으로 추정됨.
그리고 00403B2C 함수를 호출 -> 아마 EAX, EDX를 인자로 받아서 두 개를 비교하는 함수로 예상할 수 있다.

확인해보고 싶다.

```
Address   Hex dump          Disassembly              Comment
00403B2C  53                PUSH EBX
00403B2D  56                PUSH ESI
00403B2E  57                PUSH EDI
00403B2F  89C6              MOV ESI, EAX
00403B31  89D7              MOV EDI, EDX
00403B33  39D0              CMP EAX, EDX
00403B35  0F84 8F000000     JE 00403BCA              00403BCA
```

함수 호출 전에 EBX, ESI, EDI에서 사용중인 값은 방해받으면 안되니까 일단 PUSH 함.
예상대로다. EAX랑 EDX랑 같으면 00403BCA로 이동

```
Address   Hex dump   Disassembly
00403BCA  5F         POP EDI
00403BCB  5E         POP ESI
00403BCC  5B         POP EBX
00403BCD  C3         RETN
```

00403BCA에는 다시 역순으로 EDI, ESI, EBX 순서로 값을 POP하고 RETN 하는 코드가 있음.

다시 main으로 돌아와서 Jump Not Zero면(JNZ) 00440F8C로 이동

```
00440F8C  6A 00              PUSH 0
00440F8E  B9 80104400        MOV ECX, 441080          ASCII "Beggar off!"
00440F93  BA 8C104400        MOV EDX, 44108C          ASCII "Wrong Serial,try again!"
00440F98  A1 442C4400        MOV EAX, DWORD PTR DS:[442C44]
00440F9D  8B00               MOV EAX, DWORD PTR DS:[EAX]
00440F9F  E8 C4C0FFFF        CALL 0043D068            0043D068
```

00440F8C에는 Wrong Serial,try again! 오류 메시지를 출력하는 코드가 있다.
그러므로...프로그램의 username 값은 Registered User가 답이 됨.

4. GFX-754-IER-954 : 정답 시리얼 번호라고 추측
Registered User 때처럼 똑같이 EAX, EDX로 옮기고 00403B2C 함수를 호출함.
그리고 또 CMP EAX, EDX를 하고 JE(정답)이면 정상리턴.
그러므로 프로그램의 Serial number 값은 GFX-754-IER-954가 된다.

위까지 모두 순조롭게 진행 되었으면 Error Message 부분으로 점프하지 않고 순차적으로 진행하여
5. CrackMe cracked successfully! Congrats1 You cracked this CrackMe!
문자열을 출력함을 알 수 있다.

진짜 정답인지 테스트 해보자

이렇게 입력해주고 Registered now!를 누르면

1. username 박스에 문자열이 있는가?
2. Serial number 박스에 문자열이 있는가?
3. username 값이 Registered User와 같은가?
4. Serial number 값이 GFX-754-IER-954와 같은가?

순서로 검사할 것이다.

정답!
만약 입력한 username이 Registered User가 아니라면?

틀렸다고 출력한다. (사실 저 오류 메시지는 틀리고 원래는 Wrong username이 되야하지 않나...)