

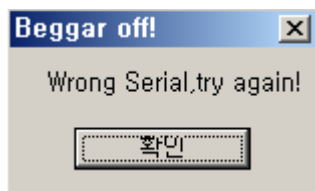
문제 : 문제 : 이 프로그램의 등록키는?

해당 프로그램을 실행 시켜보면

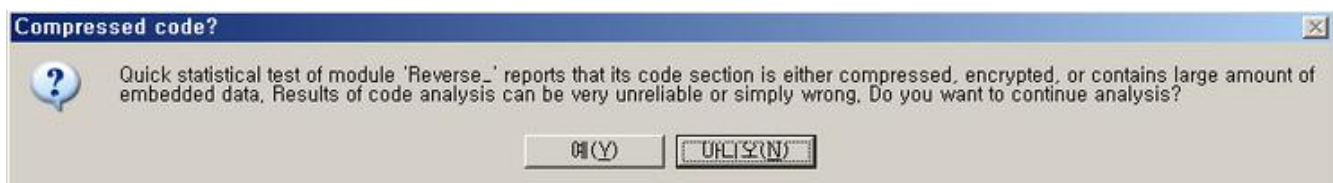


위와 같은 창이 나타납니다.

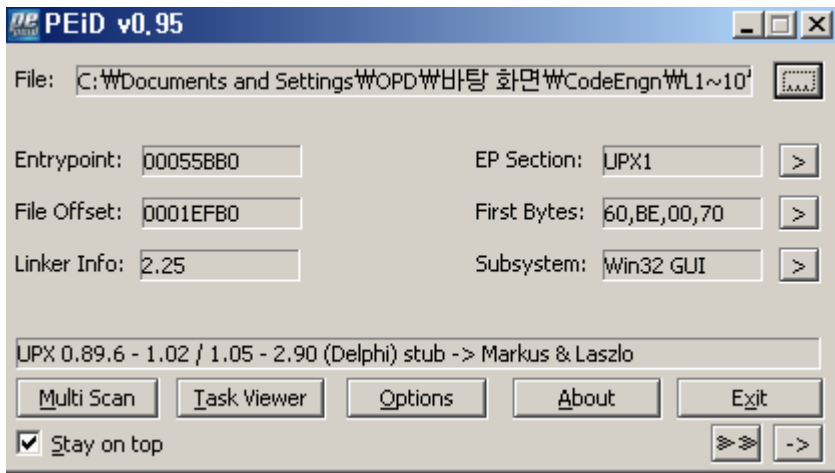
Name 과 Serial 이 입력되어 있어 등록 버튼을 눌렀더니 오류 창이 나타났습니다.



OlllyDBG 로 열어서 프로그램을 확인해 보면



이런 오류 창이 뜨게 되며 프로그램이 패킹 되어있다는 것을 알 수 있었습니다.



확인해 보니 UPX 방식으로 패킹 되어있는 것을 확인할 수 있었습니다..

```
00455CFE | ^ EB E1 | JMP SHORT Reverse_.00455CE1
00455D00 | > FF96 0461050 | CALL DWORD PTR DS:[ESI+56104]
00455D06 | > 61 | POPAD
00455D07 | ^ E9 64B5FEFF | JMP Reverse_.00441270
```

POPAD 다음에 나오는 OEP 로 점프하는 점프문에서 브레이크 포인트를 걸어 실행 시켜

OEP 까지 진행 시키면 패킹된 데이터가 실행 상태로 복원되어 메모리에 로딩되는데.

```
00441270 | > 55 | PUSH EBP
00441271 | . 8BEC | MOV EBP,ESP
00441273 | ? 83C4 F4 | ADD ESP,-0C
00441276 | . B8 60114400 | MOV EAX,Reverse_.00441160
0044127B | . E8 E848FCFF | CALL Reverse_.00405B68
00441280 | ? A1 442C4400 | MOV EAX,DWORD PTR DS:[442C44]
00441285 | ? 8B00 | MOV EAX,DWORD PTR DS:[EAX]
00441287 | ? E8 ECBBFFFF | CALL Reverse_.0043CE78
0044128C | ? A1 442C4400 | MOV EAX,DWORD PTR DS:[442C44]
00441291 | ? 8B00 | MOV EAX,DWORD PTR DS:[EAX]
00441293 | . BA D0124400 | MOV EDX,Reverse_.004412D0
00441298 | . E8 17B8FFFF | CALL Reverse_.0043CAB4
0044129D | ? 8B00 102D4400 | MOV ECX,DWORD PTR DS:[442D10]
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]
004412B0 | ? 8B15 5C0C4400 | MOV EDX,DWORD PTR DS:[440C5C]
```

ASCII "Crackers For Freedom CrackMe v3.0"
Reverse_.00443830
Reverse_.00440CA8

이 상태에서 Dump 시킨 후 확인해 보면 패킹이 풀린 것을 확인할 수 있습니다.

이를 가지고 실행 상태에서 에러 창을 띄우고 Back to user mode 로 실행 위치를 찾아가면

```
0043D13C | . 53 | PUSH EBX
0043D13D | . 57 | PUSH EDI
0043D13E | . 56 | PUSH ESI
0043D13F | . 8B45 FC | MOV EAX,DWORD PTR SS:[EBP-4]
0043D142 | . 8B40 24 | MOV EAX,DWORD PTR DS:[EAX+24]
0043D145 | . 50 | PUSH EAX
0043D146 | . E8 3191FCFF | CALL Unpack_R.0040627C
0043D14B | . 8945 F8 | MOV DWORD PTR SS:[EBP-8],EAX
```

Style
Title
Text
hOwner
MessageBoxA

메시지 창을 호출하는 API 에서 멈추게 되는데.

이 근처에서는 암호에 대한 힌트를 찾을 수 없었으며 메시지 창은 서브루틴을 따로 호출해 실행 하기 때문입니다.

이 서브루틴의 시작 점에 브레이크 포인트를 걸어 어느 위치에서 호출하는지 알아내서 호출 위치로 거슬러 올라가면

00440F49	. 8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
00440F4C	. BA 2C104400	MOV EDX,Unpack_R.0044102C	ASCII "GFX-754-IER-954"
00440F51	. E8 D62BFCFF	CALL Unpack_R.00403B2C	
00440F56	. 75 1A	JNZ SHORT Unpack_R.00440F72	
00440F58	. 6A 00	PUSH 0	
00440F5A	. B9 3C104400	MOV ECX,Unpack_R.0044103C	ASCII "CrackMe cracked successfully"
00440F5F	. BA 5C104400	MOV EDX,Unpack_R.0044105C	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 Unpack_R.0043D068	
00440F70	. EB 32	JMP SHORT Unpack_R.00440FA4	
00440F72	. 6A 00	PUSH 0	
00440F74	. B9 80104400	MOV ECX,Unpack_R.00441080	ASCII "Beggar off!"
00440F79	. BA 8C104400	MOV EDX,Unpack_R.0044108C	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 Unpack_R.0043D068	
00440F8A	. EB 18	JMP SHORT Unpack_R.00440FA4	
00440F8C	. 6A 00	PUSH 0	
00440F8E	. B9 80104400	MOV ECX,Unpack_R.00441080	ASCII "Beggar off!"
00440F93	. BA 8C104400	MOV EDX,Unpack_R.0044108C	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 Unpack_R.0043D068	
00440FA4	. 33C0	XOR EAX,EAX	

이 프로그램의 등록 키와 아이디를 얻을 수 있었습니다.



답 : 이 프로그램을 등록 하기 위해서는 Registered User 라는 이름과 GFX-754-IER-954라는 시리얼 넘버가 있어야 됩니다.