CodeEngn Basic Level 5 풀이 보고서

Name : GiGaGs

E-Mail : violetstair@gmail.com

Blog : violetstair.tistory.com

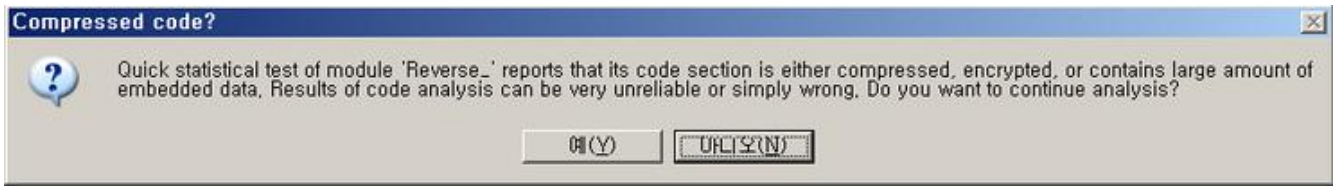
문제 : 문제 : 이 프로그램의 등록키는?

해당 프로그램을 실행 시켜보면

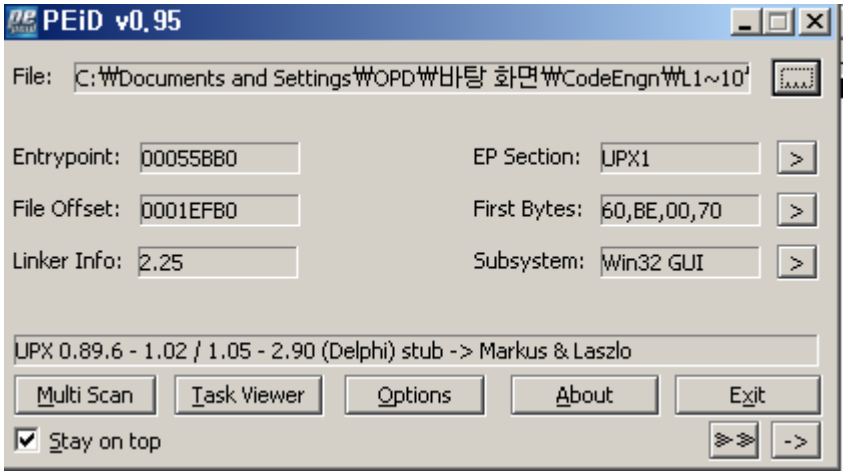
위와 같은 창이 나타납니다.

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

OllyDBG 로 열어서 프로그램을 확인해 보면



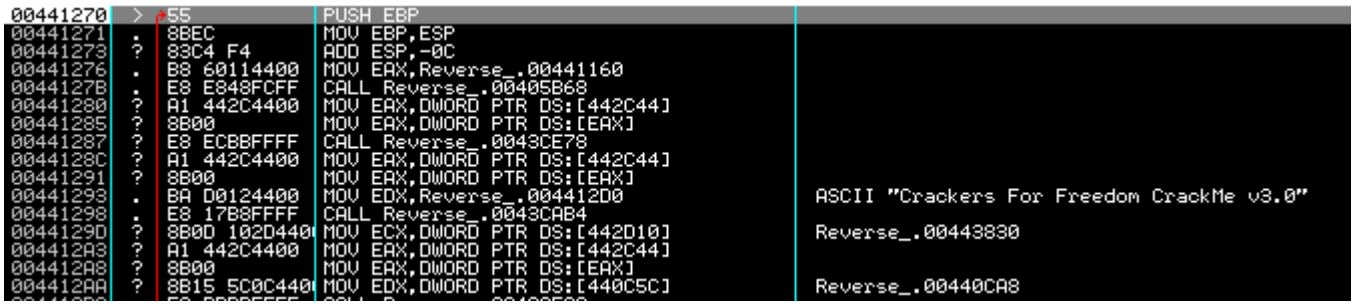
이런 오류 창이 뜨게 되며 프로그램이 패킹 되어있다는 것을 알 수 있었습니다.



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

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

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



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

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  .v 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  .v 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  .v 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.