Basic

# RCE_04 문제풀이

name : 조 성환
nickname : Lum4n
@Lum4n, namul10@mail.com
문제 : http://codeengn.com/

**Reverse L05 Start**

Author : Acid Bytes [CFF]

**Korea** :

이 프로그램의 등록키는 무엇인가

**English** :

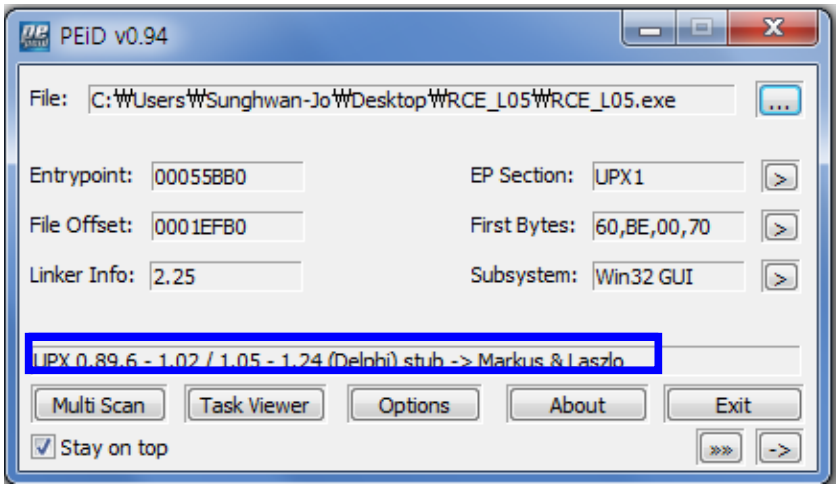
The registration key of this program is?

Down

총 85 분이 이 문제를 푸셨습니다. / 85 people solved this problem.

히힛 5번이네요~우선 프로그램을 실행시켜볼겠습니다.


음 네임을 입력받고 시리얼키를 입력받은후 'Register now !' 를 클릭해서 이름과 시리얼이 맞는지 검사하는 프로그램이군요 PEiD로 열어보겠습니다.




Pack 되어있는 파일이군요~. UPX 를 이용해서 언팩을 하겠습니다.

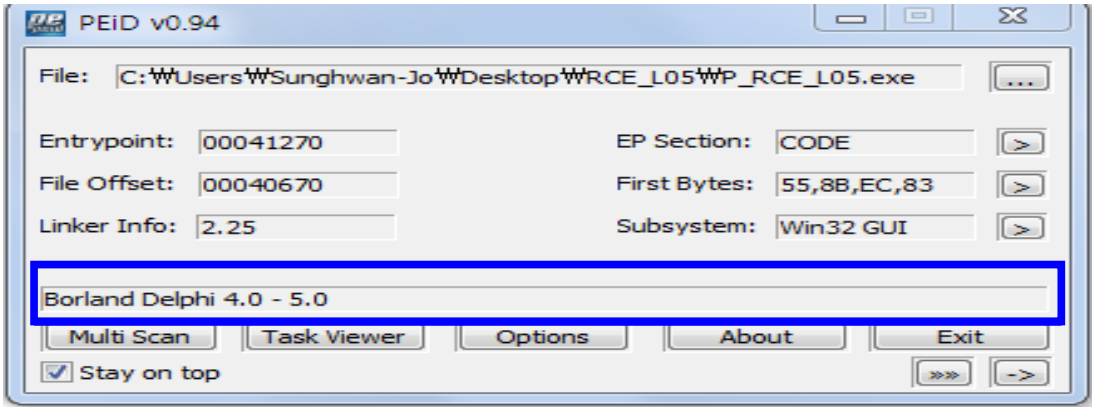
```
C:₩Users₩Sunghwan-Jo₩Desktop₩RCE_L05>UPX -d P_RCE_L05.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996, 1997, 1998, 1999, 2000, 2001
UPX 1.20w        Markus F.X.J. Oberhumer & Laszlo Molnar        May 23rd 2001

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
    315392 <-    132608   42.04%    win32/pe      P_RCE_L05.exe

Unpacked 1 file.

C:₩Users₩Sunghwan-Jo₩Desktop₩RCE_L05>
```

언팩 완료~ : )



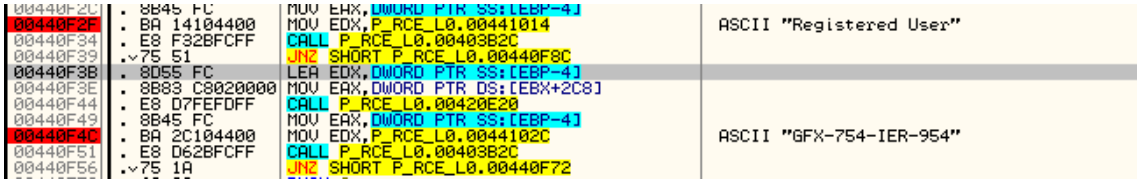

델파이로 만들어진 프로그램 이군요~ 분석을 위해 올리로 열어보겠습니다.,

```
00440EDC| MOV ECX,P_RCE_L0.00440FC8          | ASCII "No Name entered"
00440EE1| MOV EDX,P_RCE_L0.00440FD8          | ASCII "Enter a Name!"
00440F08| MOV ECX,P_RCE_L0.00440FE8          | ASCII "No Serial entered"
00440F0D| MOV EDX,P_RCE_L0.00440FFC          | ASCII "Enter a Serial!"
00440F2F| MOV EDX,P_RCE_L0.00441014          | ASCII "Registered User"
00440F4C| MOV EDX,P_RCE_L0.0044102C          | ASCII "GFX-754-IER-954"
00440F5A| MOV ECX,P_RCE_L0.0044103C          | ASCII "CrackMe cracked successfully"
00440F5F| MOV EDX,P_RCE_L0.0044105C          | ASCII "Congrats! You cracked this CrackMe!"
00440F74| MOV ECX,P_RCE_L0.00441080          | ASCII "Beggar off!"
00440F79| MOV EDX,P_RCE_L0.0044108C          | ASCII "Wrong Serial,try again!"
00440F8E| MOV ECX,P_RCE_L0.00441080          | ASCII "Beggar off!"
00440F93| MOV EDX,P_RCE_L0.0044108C          | ASCII "Wrong Serial,try again!"
```

올리디버거로 연후에 프로그램에 사용된 문자열들만 보던 중 올바른 name과 serial을 입력할 경우 출력될 것으로 추측되는 문자열이 보이네요. 저 문자열이 사용된 곳을 살펴보겠습니다.

```
00440EE6  . A1 442C4400     MOV EAX,DWORD PTR DS:[442C44]
00440EEB  . 8B00            MOV EAX,DWORD PTR DS:[EAX]
00440EED  . E8 76C1FFFF     CALL P_RCE_L0.0043D068
00440EF2  > 8D55 FC         LEA EDX,DWORD PTR SS:[EBP-4]
00440EF5  . 8B83 C8020000   MOV EAX,DWORD PTR DS:[EBX+2C8]
00440EFB  . E8 20FFFDFF     CALL P_RCE_L0.00420E20
00440F00  . 837D FC 00      CMP DWORD PTR SS:[EBP-4],0
00440F04  .v75 18           JNZ SHORT P_RCE_L0.00440F1E
00440F06  . 6A 00           PUSH 0
00440F08  . B9 E80F4400     MOV ECX,P_RCE_L0.00440FE8       ASCII "No Serial entered"
00440F0D  . BA FC0F4400     MOV EDX,P_RCE_L0.00440FFC       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 P_RCE_L0.0043D068
00440F1E  > 8D55 FC         LEA EDX,DWORD PTR SS:[EBP-4]
00440F21  . 8B83 C4020000   MOV EAX,DWORD PTR DS:[EBX+2C4]
00440F27  . E8 F4FEFDFF     CALL P_RCE_L0.00420E20
00440F2C  . 8B45 FC         MOV EAX,DWORD PTR SS:[EBP-4]
00440F2F  . BA 14104400     MOV EDX,P_RCE_L0.00441014       ASCII "Registered User"
00440F34  . E8 F32BFCFF     CALL P_RCE_L0.00403B2C
00440F39  .v75 51           JNZ SHORT P_RCE_L0.00440F8C
00440F3B  . 8D55 FC         LEA EDX,DWORD PTR SS:[EBP-4]
00440F3E  . 8B83 C8020000   MOV EAX,DWORD PTR DS:[EBX+2C8]
00440F44  . E8 D7FEFDFF     CALL P_RCE_L0.00420E20
00440F49  . 8B45 FC         MOV EAX,DWORD PTR SS:[EBP-4]
```

0044103C의 함수 첫부분인데요 분기점이 많이 보입니다. 좀더 아래를 살펴보니~~




이런 부분이 보이는데 너무 적나라하게 나와잇네요. . . .

00440F2C에서 EAX에 제가 입력한 NAME이들어가고 00440F49에서는 EAX에 제가넣은 PASSWORD가 들어가는 것으로 보아 데이터 두 개를 매개변수로 그아래 00403B2C함수를 실행해서 검사를 하는 것 같습니다.

**그래서 결국 답은 GFX-754-IER-954 입니다 . : )**