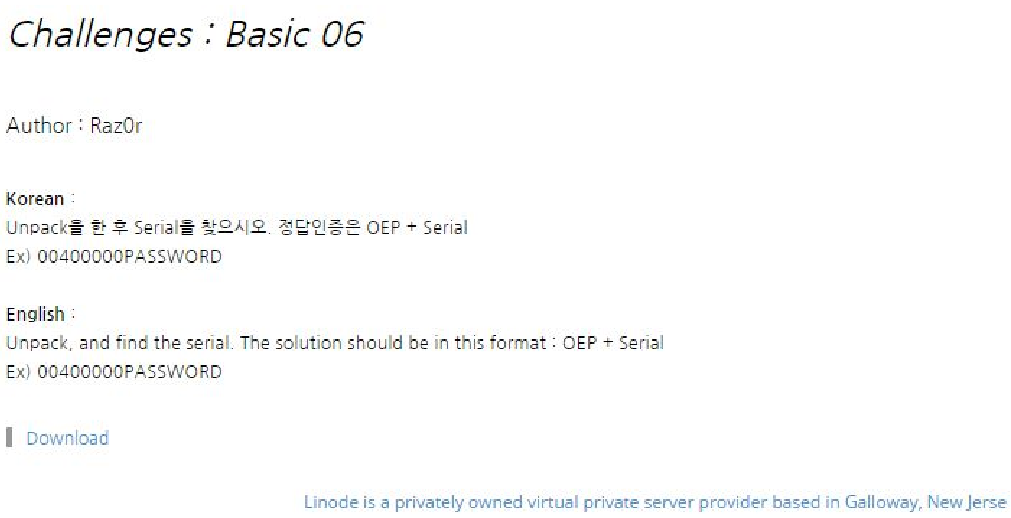
CodeEngn

Solving problems

basic level6

Nick : C y __ h
Email : h61cker@gmail.com



Challenges : Basic 06

Author : Raz0r

Korean :
Unpack을 한 후 Serial을 찾으시오. 정답인증은 OEP + Serial
Ex) 00400000PASSWORD

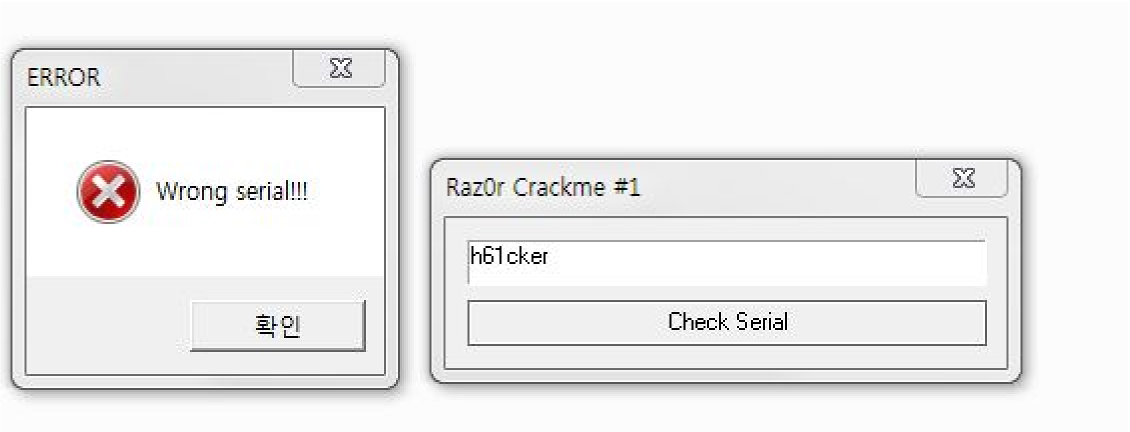
English :
Unpack, and find the serial. The solution should be in this format : OEP + Serial
Ex) 00400000PASSWORD

Download

풀이 순서를 추측하자면

Unpacking - > Find Serial key -> OEP = OEP + SERIAL

이 정도 순서로 하면 인증키가 나올 것 같습니다.



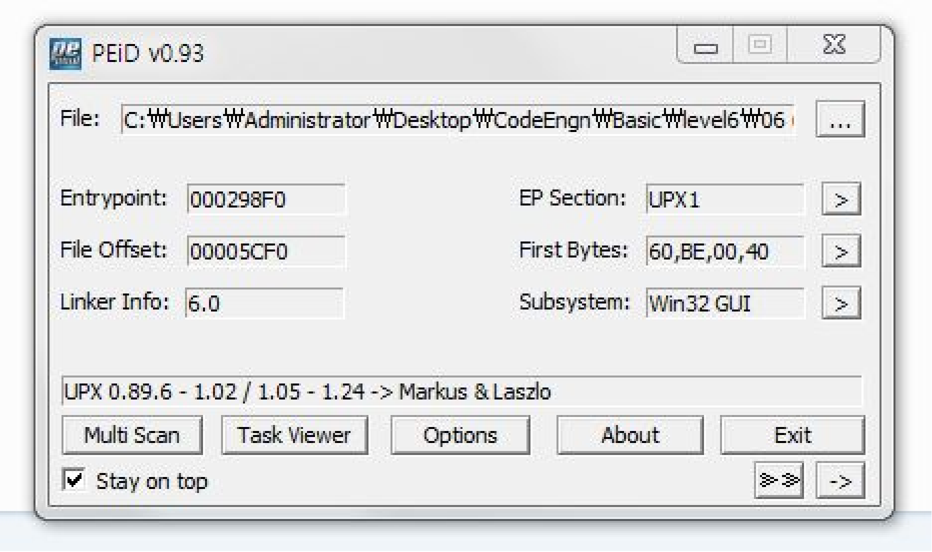
ERROR

Wrong serial!!!

Raz0r Crackme #1

h61cker

정답 시리얼 키를 입력하면 성공 메세지가 뜰 것 같습니다.



File: C:₩Users₩Administrator₩Desktop₩CodeEngn₩Basic₩level6₩06

Entrypoint: 000298F0

EP Section: UPX1

File Offset: 00005CF0

First Bytes: 60,BE,00,40

Linker Info: 6.0

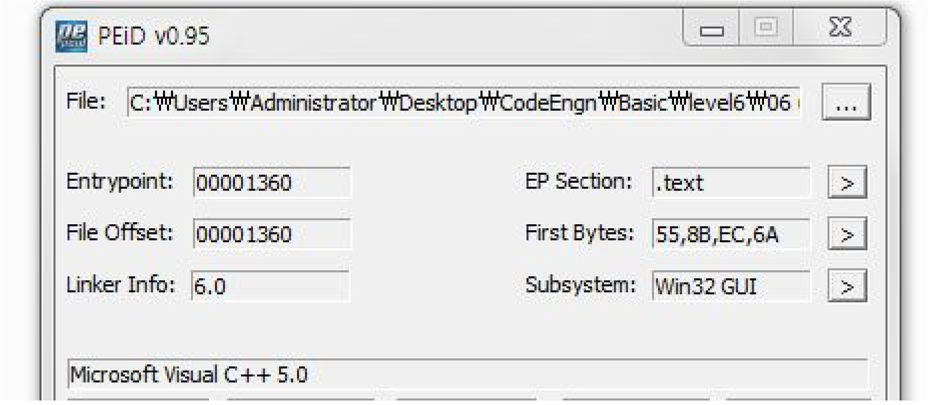
Subsystem: Win32 GUI

UPX 0.89.6 - 1.02 / 1.05 - 1.24 -> Markus & Laszlo

☑ Stay on top

upx 으로 되어있습니다.

언패킹 하겠습니다.



File: C:₩Users₩Administrator₩Desktop₩CodeEngn₩Basic₩level6₩06

Entrypoint: 00001360

EP Section: .text

File Offset: 00001360

First Bytes: 55,8B,EC,6A

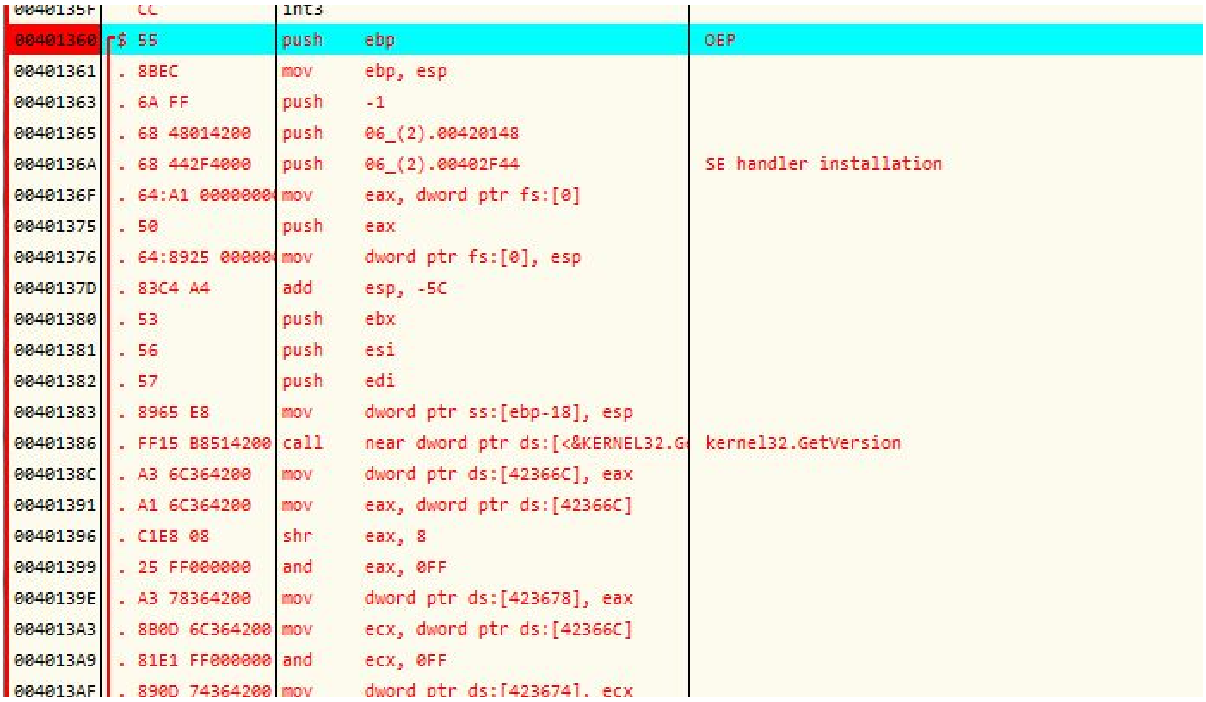
Linker Info: 6.0

Subsystem: Win32 GUI

Microsoft Visual C++ 5.0

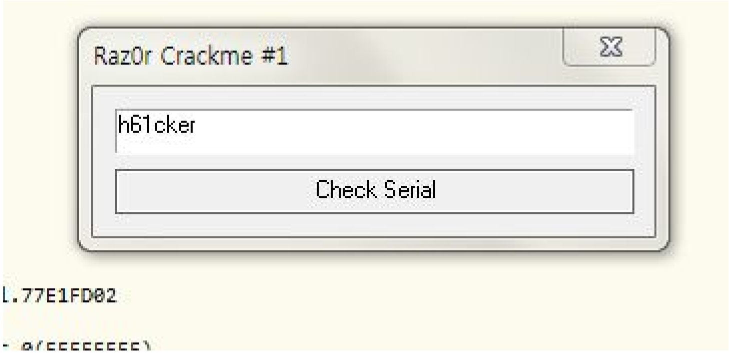
언패킹 완료.

분석해보도록 하겠습니다.



```
0040135F    CC            int3
00401360  r$ 55           push    ebp                                   OEP
00401361  . 8BEC          mov     ebp, esp
00401363  . 6A FF         push    -1
00401365  . 68 48014200   push    06_(2).00420148
0040136A  . 68 442F4000   push    06_(2).00402F44                       SE handler installation
0040136F  . 64:A1 0000000 mov     eax, dword ptr fs:[0]
00401375  . 50            push    eax
00401376  . 64:8925 00000 mov     dword ptr fs:[0], esp
0040137D  . 83C4 A4       add     esp, -5C
00401380  . 53            push    ebx
00401381  . 56            push    esi
00401382  . 57            push    edi
00401383  . 8965 E8       mov     dword ptr ss:[ebp-18], esp
00401386  . FF15 B8514200 call    near dword ptr ds:[<&KERNEL32.G       kernel32.GetVersion
0040138C  . A3 6C364200   mov     dword ptr ds:[42366C], eax
00401391  . A1 6C364200   mov     eax, dword ptr ds:[42366C]
00401396  . C1E8 08       shr     eax, 8
00401399  . 25 FF000000   and     eax, 0FF
0040139E  . A3 78364200   mov     dword ptr ds:[423678], eax
004013A3  . 8B0D 6C364200 mov     ecx, dword ptr ds:[42366C]
004013A9  . 81E1 FF000000 and     ecx, 0FF
004013AF  . 890D 74364200 mov     dword ptr ds:[423674], ecx
```

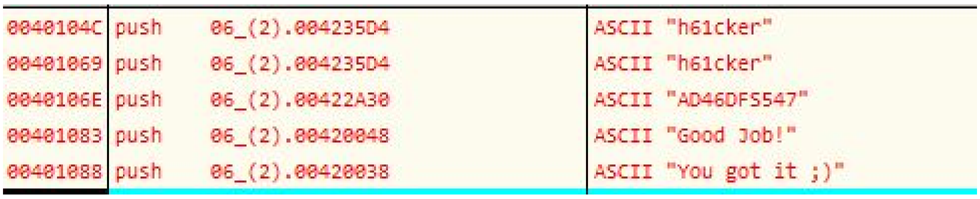
프로그램의 진짜 실행 위치 == OEP 는 00401360 입니다.



Raz0r Crackme #1

h61cker

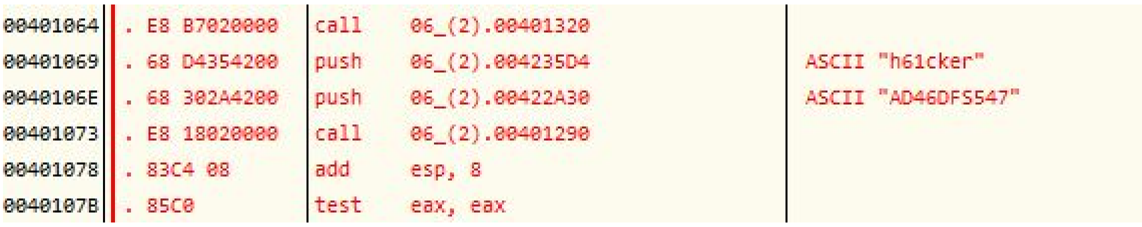
디버깅 도중에 api 가 호출되어서 입력했습니다.



```
0040104C push    06_(2).004235D4        ASCII "h61cker"
00401069 push    06_(2).004235D4        ASCII "h61cker"
0040106E push    06_(2).00422A30        ASCII "AD46DFS547"
00401083 push    06_(2).00420048        ASCII "Good Job!"
00401088 push    06_(2).00420038        ASCII "You got it ;)"
```

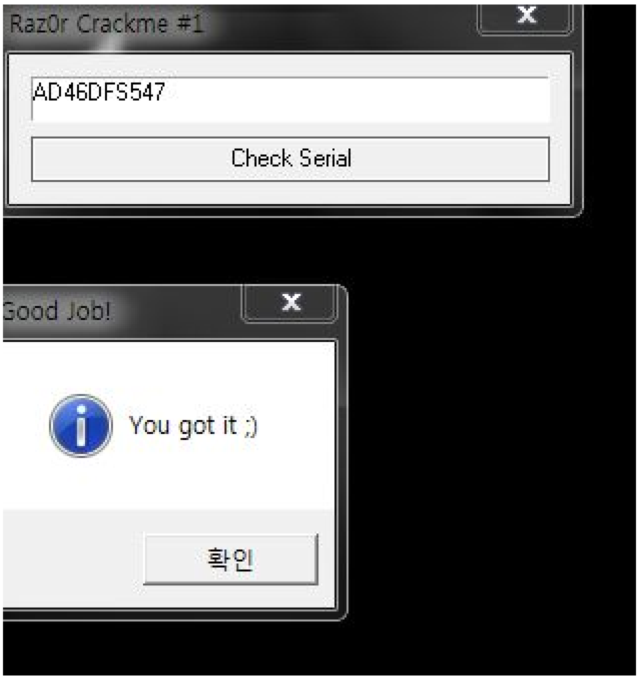
문자열들을 검색해서 봤는데

제가 입력한 h61cker 과 AD46DFS547 이라는 문자열이 붙어있네요



```
00401064  . E8 B7020000   call    06_(2).00401320
00401069  . 68 D4354200   push    06_(2).004235D4          ASCII "h61cker"
0040106E  . 68 302A4200   push    06_(2).00422A30          ASCII "AD46DFS547"
00401073  . E8 18020000   call    06_(2).00401290
00401078  . 83C4 08       add     esp, 8
0040107B  . 85C0          test    eax, eax
```

h61cker 과 AD46DFS547 문자열을 비교하고 있습니다.



Raz0r Crackme #1

AD46DFS547

Good Job!

You got it ;)

key flag : 00401360AD46DFS547