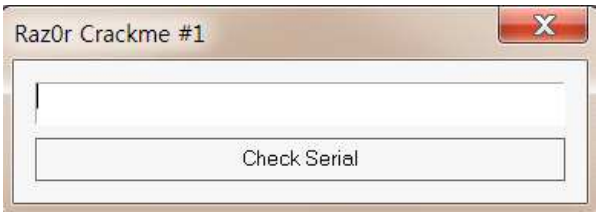
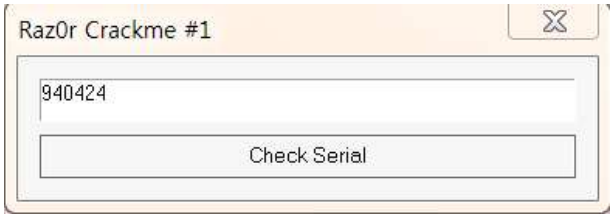
코드 엔진 Challenges: Basic 06

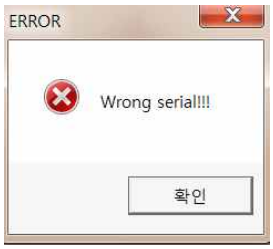
Author: Raz0r
Korean: Unpack을 한 후 Serial을 찾으시오.
정답 인증은 OEP+Serial
Ex)00400000PASSWARD

문제를 확인했으니 파일을 다운로드 받아서 실행해보자.

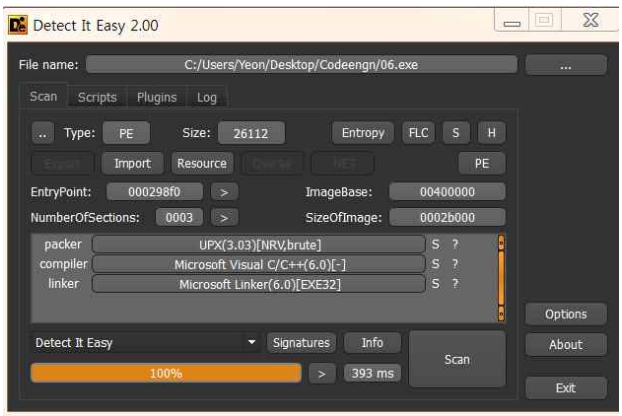


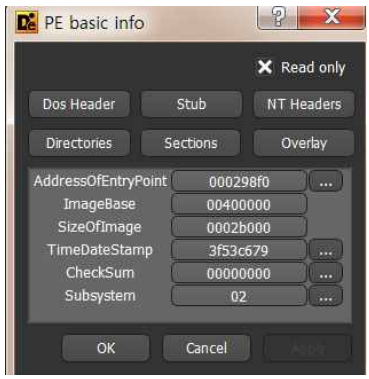
파일을 실행하자 다음과 같이 일반적인 시리얼 인증 프로그램과 같은 형태를 띄는 화면이 뜬다. 임의의 값을 입력하고 Check Serial을 누르자 "Wrong Sereal!"이라는 메시지가 뜨면서 에러를 발생시킨다.





프로그램을 실행해서 살펴보았으니 프로그램을 분석해보자.
먼저 문제에 Unpack이라는 단어가 나오니 프로그램이 Pack되어있다는 것을 알 수 있다.
이를 먼저 DE를 통해 분석해보자.





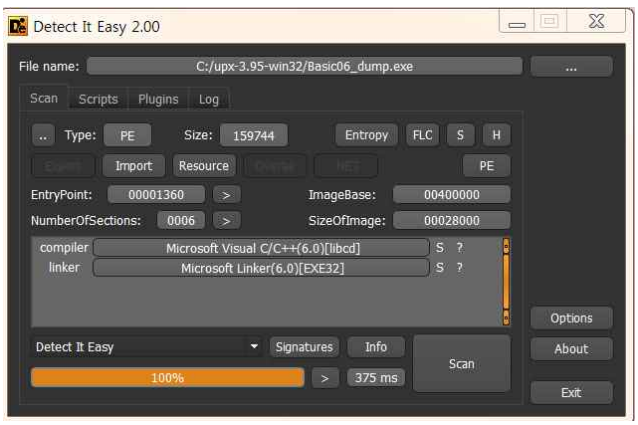
이 프로그램은 UPX로 패킹되어있으며 패킹된 프로그램의 엔트리포인트는 004298f0이다.
저번에는 올리덤프를 이용해 언패킹 했지만 UPX를 간단하고 빠르게 언패킹해주는 도구를 이용해보자.

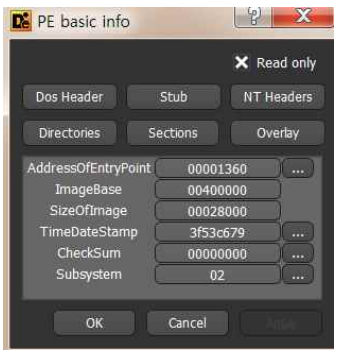
```
C:₩upx-3.95-win32>upx -d -o Basic06_dump.exe 06.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2018
UPX 3.95w       Markus Oberhumer, Laszlo Molnar & John Reiser   Aug 26th 2018

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
    159744 <-     26112   16.35%    win32/pe     Basic06_dump.exe

Unpacked 1 file.
```

UPX를 통해 파일을 언팩하였다.
우리는 파일을 언팩하는 것이니 –d 옵션을 사용하여 06.exe를 언팩하여 Basic06_dump.exe 파일을 만들었다.



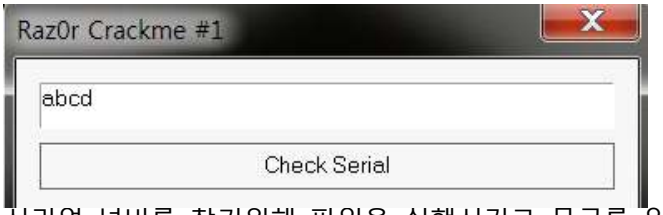


언팩한 파일을 분석해보니 파일은 제대로 언패킹되었고 OEP는 00401360인걸 알 수 있다.

그럼 이제 올리디버거로 원본 파일을 열어 시리얼을 찾아보자.

```
00401360  ┌$ 55              PUSH EBP
00401361  |. 8BEC            MOV EBP,ESP
00401363  |. 6A FF           PUSH -1
00401365  |. 68 48014200     PUSH Basic06_.00420148
0040136A  |. 68 442F4000     PUSH Basic06_.00402F44                SE handler installation
0040136F  |. 64:A1 00000000  MOV EAX,DWORD PTR FS:[0]
00401375  |. 50              PUSH EAX
00401376  |. 64:8925 000000  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 DWORD PTR DS:[<&KERNEL32.GetVersion  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
```

정확하게 언팩이되어있어 OEP를 쉽게 찾을 수 있다. 이제 시리얼 주소를 찾아보도록하자.



시리얼 넘버를 찾기위해 파일을 실행시키고 문구를 입력했다.

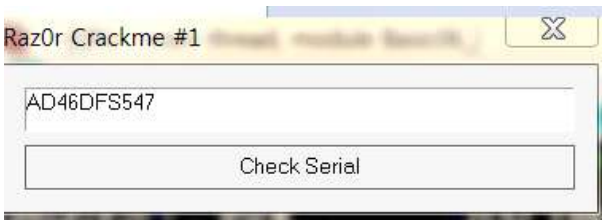
그리고 search for all text strings를 이용해 아까 보았던 오류 문구를 찾았다.

```
0040104C PUSH Basic06_.004235D4          ASCII "abcd"
00401069 PUSH Basic06_.004235D4          ASCII "abcd"
0040106E PUSH Basic06_.00422A30          ASCII "AD46DFS547"
00401083 PUSH Basic06_.00420048          ASCII "Good Job!"
00401088 PUSH Basic06_.00420038          ASCII "You got it ;)"
004010A7 PUSH Basic06_.00420030          ASCII "ERROR"
004010AC PUSH Basic06_.0042001C          ASCII "Wrong serial!!!"
004010B7 PUSH EDX                        (Initial CPU selection)
0040132E PUSH Basic06_.00420068          ASCII "The value of ESP was not properly saved across a function
0040133A PUSH Basic06_.00420054          ASCII "i386\chkesp.c"
004016CC PUSH Basic06_.00420220          ASCII "user32.dll"
```

창을 보다시피 "abcd"와 함께 "AD460DFS547"이라는 아스키 코드가 보이는데 수상한 것 같다. 오류 문구를 눌러 해당 코드 영역으로 이동해보자.

```
00401062  . 3BF4          CMP ESI,ESP
00401064  . E8 B7020000   CALL Basic06_.00401320
00401069  . 68 D4354200   PUSH Basic06_.004235D4          ASCII "abcd"
0040106E  . 68 302A4200   PUSH Basic06_.00422A30          ASCII "AD46DFS547"
00401073  . E8 18020000   CALL Basic06_.00401290
00401078  . 83C4 08       ADD ESP,8
0040107B  . 85C0          TEST EAX,EAX
0040107D  . 75 24         JNZ SHORT Basic06_.004010A3
0040107F  . 8BF4          MOV ESI,ESP
00401081  . 6A 40         PUSH 40                        Style = MB_OK|MB_ICONASTERISK|MB_APPLMOD
00401083  . 68 48004200   PUSH Basic06_.00420048         Title = "Good Job!"
00401088  . 68 38004200   PUSH Basic06_.00420038         Text = "You got it ;)"
0040108D  . 8B0D 38364200 MOV ECX,DWORD PTR DS:[423638]
00401093  . 51            PUSH ECX                       hOwner => 009202E8 ('Raz0r Crackme #1',c
00401094  . FF15 B4524200 CALL DWORD PTR DS:[<&USER32.MessageBoxA> MessageBoxA
0040109A  . 3BF4          CMP ESI,ESP
0040109C  . E8 7F020000   CALL Basic06_.00401320
004010A1  . EB 22         JMP SHORT Basic06_.004010C5
004010A3  > 8BF4          MOV ESI,ESP
004010A5  . 6A 10         PUSH 10                        Style = MB_OK|MB_ICONHAND|MB_APPLMODAL
004010A7  . 68 30004200   PUSH Basic06_.00420030        Title = "ERROR"
004010AC  . 68 1C004200   PUSH Basic06_.0042001C        Text = "Wrong serial!!!"
004010B1  . 8B15 38364200 MOV EDX,DWORD PTR DS:[423638]
004010B7  . 52            PUSH EDX                       hOwner = 009202E8 ('Raz0r Crackme #1',cl
004010B8  . FF15 B4524200 CALL DWORD PTR DS:[<&USER32.MessageBoxA> MessageBoxA
004010BE  . 3BF4          CMP ESI,ESP
004010C0  . E8 5B020000   CALL Basic06_.00401320
```

해당 문구로 이동하자 주변에 abcd를 푸시하고 AD46DFS547를 푸시한후 00401290(비교관련) 함수를 호출 하는 것이 보인다. AD46DFS547를 입력해 확인해보자.



인증에 성공하는 것을 확인할 수 있다.

문제의 답은 00401360AD46DFS547