기본적인 OllyDbg의 사용법은 이미 인터넷에 많이 나와있기 때문에 따로 알려드리지 않겠습니다.

Challenges : Basic 05

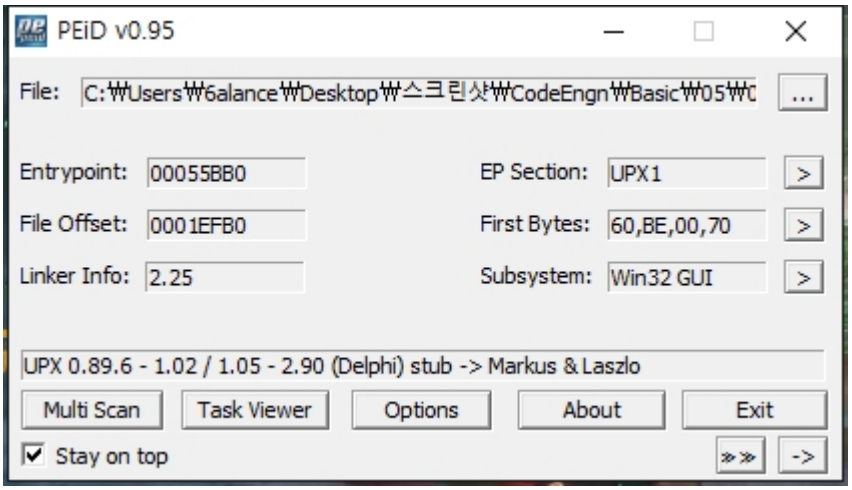
Author : Acid Bytes [CFF]

Korean :
이 프로그램의 등록키는 무엇인가

English :
The registration key of this program is?

Download

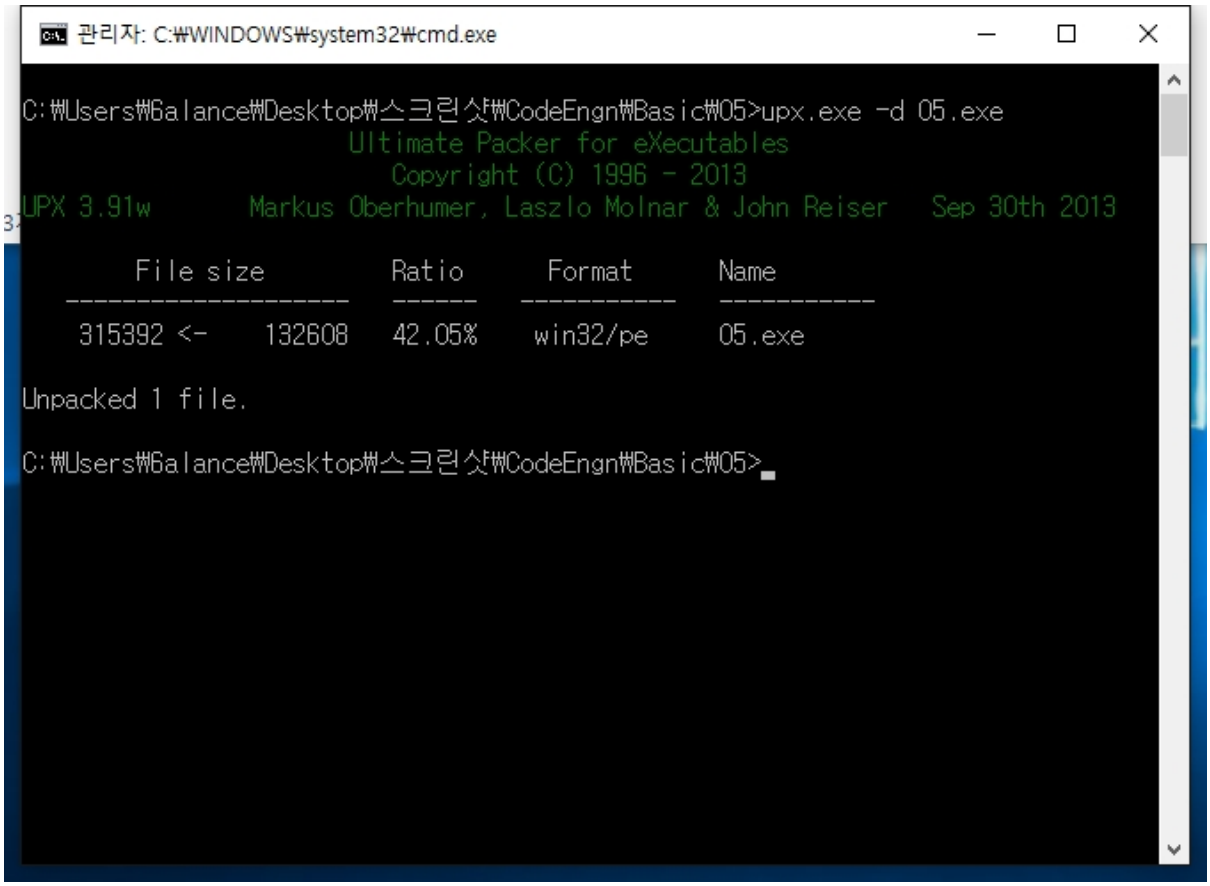
<문제>
등록키가 무엇인지 알아내는 문제인데..



PEiD로 열어본 결과 UPX로 패킹되어있다는 것을 확인할 수 있었다.
UPX는 가볍에 언패킹할 수 있는데

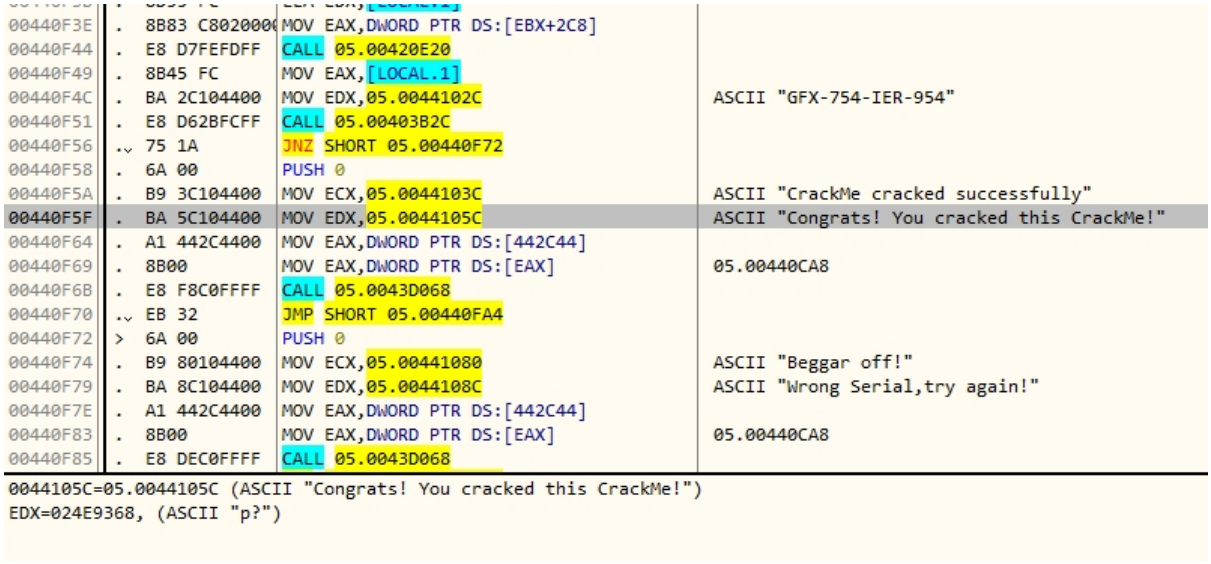
1. UPX 프로그램을 이용한 언패킹
2. ESP Trick을 이용한 언패킹
3. 기타등등

ESP Trick을 이용한 언패킹은 아직 Basic 과정이니까 좀 더 익숙해지면
그때 자세히 포스팅하겠다.



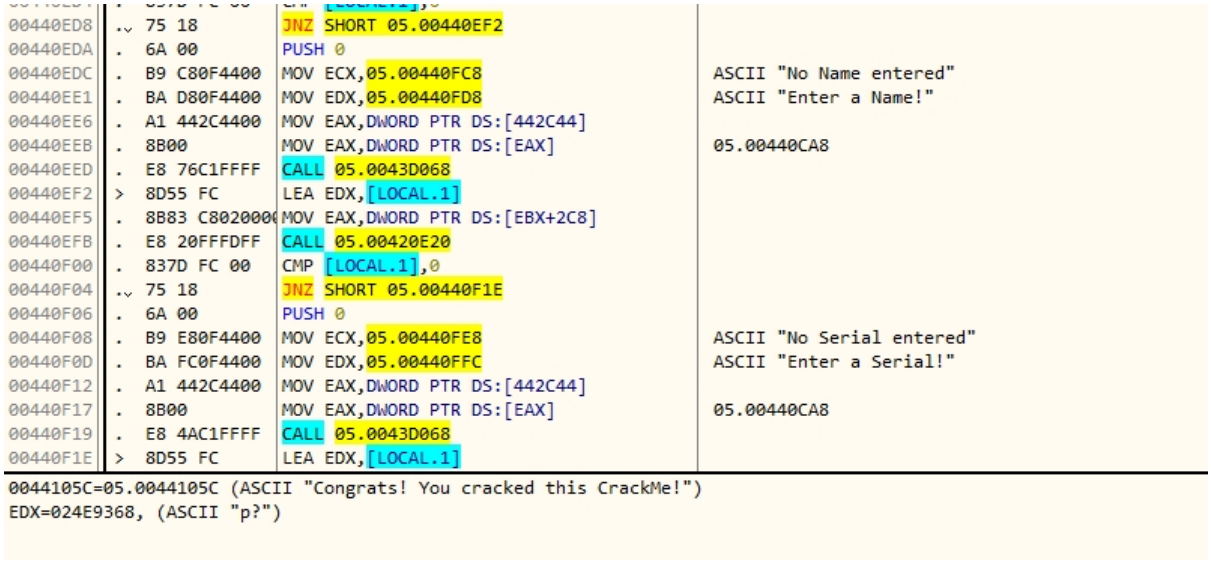
우선 UPX 프로그램을 통해 언패킹을 한다.

언패킹한 프로그램을 올리디버거로 연 후 문자열을 검색해보면
위 사진처럼 “CrackMe를 크랙한 것을 축하해!!” 라는 문자를 볼 수 있다.
위 문자열을 더블클릭해 어셈블리창으로 들어가보자.



위 사진처럼 해당 어셈블리로 이동하게된다.

위쪽을 잘 살펴보면



이름과 시리얼이 입력되었는지 확인하는 함수들이 있고,
또 밑으로 내려보면

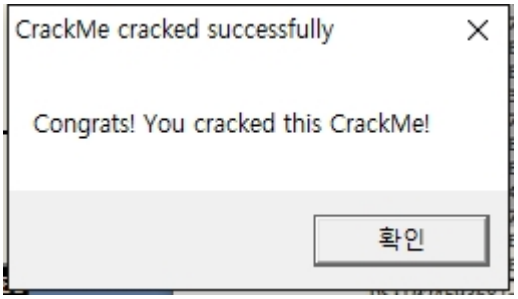
```
00440F0D  .  BA FC0F4400   MOV EDX,05.00440FFC                ASCII "Enter a Serial!"
00440F12  .  A1 442C4400   MOV EAX,DWORD PTR DS:[442C44]
00440F17  .  8B00          MOV EAX,DWORD PTR DS:[EAX]        05.00440CA8
00440F19  .  E8 4AC1FFFF   CALL 05.0043D068
00440F1E  >  8D55 FC       LEA EDX,[LOCAL.1]
00440F21  .  8B83 C402000( MOV EAX,DWORD PTR DS:[EBX+2C4]
00440F27  .  E8 F4FEFDFF   CALL 05.00420E20
00440F2C  .  8B45 FC       MOV EAX,[LOCAL.1]
00440F2F  .  BA 14104400   MOV EDX,05.00441014               ASCII "Registered User"
00440F34  .  E8 F32BFCFF   CALL 05.00403B2C
00440F39  .v 75 51         JNZ SHORT 05.00440F8C
00440F3B  .  8D55 FC       LEA EDX,[LOCAL.1]
00440F3E  .  8B83 C802000( MOV EAX,DWORD PTR DS:[EBX+2C8]
00440F44  .  E8 D7FEFDFF   CALL 05.00420E20
00440F49  .  8B45 FC       MOV EAX,[LOCAL.1]
00440F4C  .  BA 2C104400   MOV EDX,05.0044102C               ASCII "GFX-754-IER-954"
00440F51  .  E8 D62BFCFF   CALL 05.00403B2C
00440F56  .v 75 1A         JNZ SHORT 05.00440F72
00440F58  .  6A 00         PUSH 0
00441014=05.00441014 (ASCII "Registered User")
EDX=024E9368, (ASCII "p?")
```

Registered User라는 문자열로 어떤 짓거리를 하는 함수를 발견할 수 있다.
저 함수 내부로 들어가보면

```
00403B4F  >  52            PUSH EDX
00403B50  .  C1EA 02       SHR EDX,2
00403B53  .v 74 26         JE SHORT 05.00403B7B
00403B55  > ┌8B0E        ┌MOV ECX,DWORD PTR DS:[ESI]        05.0043EB70
00403B57  . │8B1F        │MOV EBX,DWORD PTR DS:[EDI]
00403B59  . │39D9        │CMP ECX,EBX
00403B5B  .v│75 58       │JNZ SHORT 05.00403BB5
00403B5D  . │4A          │DEC EDX
00403B5E  .v│74 15       │JE SHORT 05.00403B75
00403B60  . │8B4E 04     │MOV ECX,DWORD PTR DS:[ESI+4]
00403B63  . │8B5F 04     │MOV EBX,DWORD PTR DS:[EDI+4]
00403B66  . │39D9        │CMP ECX,EBX
00403B68  .v│75 4B       │JNZ SHORT 05.00403BB5
00403B6A  . │83C6 08     │ADD ESI,8
00403B6D  . │83C7 08     │ADD EDI,8
00403B70  . │4A          │DEC EDX
00403B71  .^└75 E2       └JNZ SHORT 05.00403B55
00403B73  .v EB 06         JMP SHORT 05.00403B7B
00403B75  >  83C6 04       ADD ESI,4
DS:[024E9368]=0043EB70 (05.0043EB70)
ECX=573A21BC
Jump from 00403B71
```

이 반복문을 통해 Registered User와 어떤 문자열을 비교하고,
시리얼을 비교한다.

그 두개를 잘 캐치해서 두개의 TextBox에 적절하게 옮긴 후 버튼을 누르게되면



이 창을 볼 수 있게 된다.

문제를 하나하나 다 설명하면서 포스팅하려니 갈수록 양도 많아지고
공부에 전혀 도움이 되지 않을 것 같더라구요.
그래서 이제부턴 문제를 푸는데 필요한 배경지식과 힌트들 위주로

작성할 생각입니당
그럼 모두들 화이또!