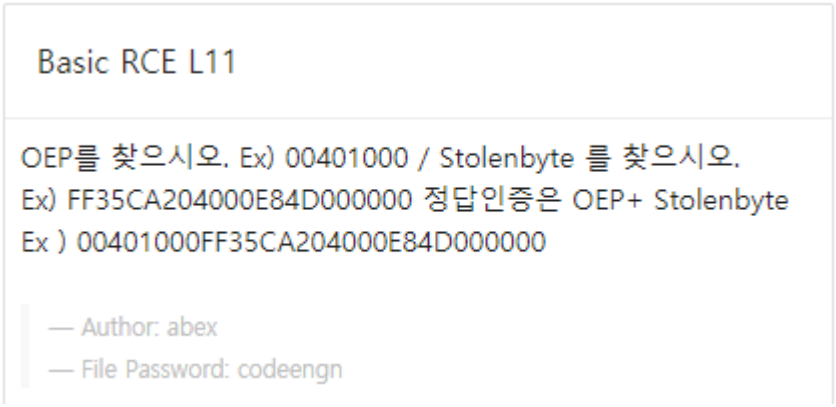
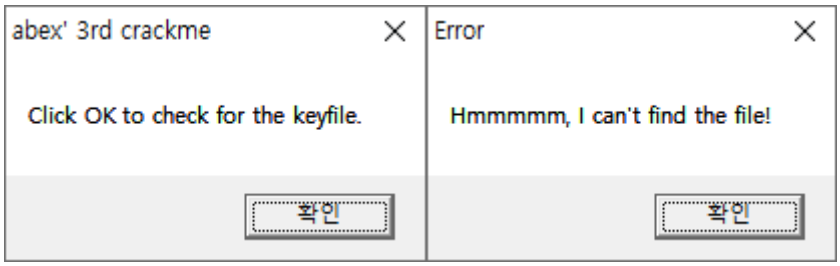
CodeEngn Basic RCE

11. Level 11

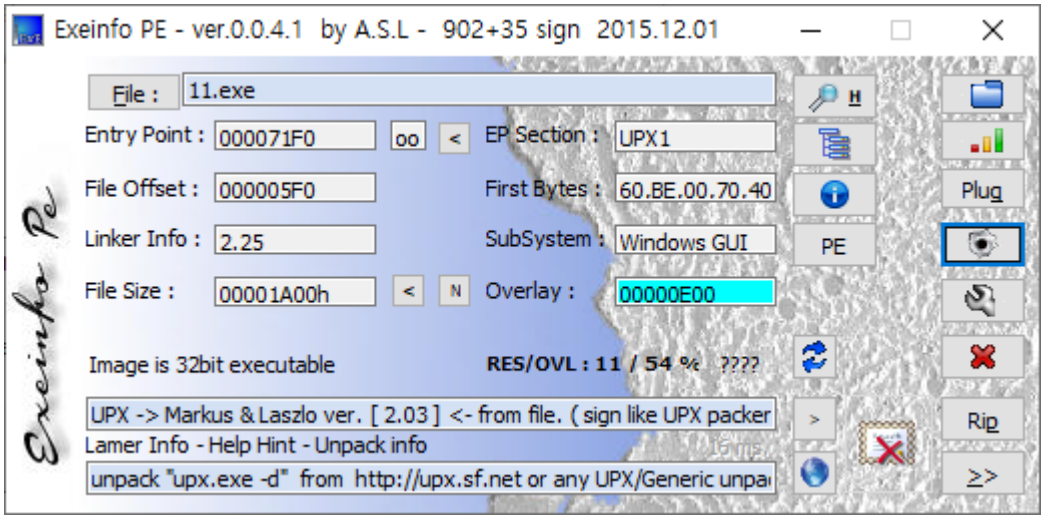


OEP : 시작지점

Stolenbyte : 이동된 코드

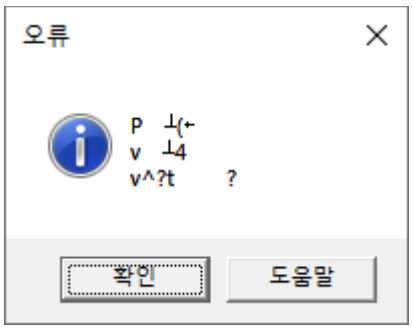


먼저 exeinfo로 패킹확인을 하자.



upx1로 패킹되어있는것이 보인다.

언패킹 후 파일을 실행하면 Click OK to check for the keyfile. 부분이 오류가 뜨는 것을 확인할 수 있다.



x64dbg로 까보자.

```
00401000    90          nop                                     EntryPoint
00401001    90          nop
00401002    90          nop
00401003    90          nop
00401004    90          nop
00401005    90          nop
00401006    90          nop
00401007    90          nop
00401008    90          nop
00401009    90          nop
0040100A    90          nop
0040100B    90          nop
```

EntryPoint가 nop으로 채워져있다.

일단 언패킹한 파일을 깐 것만으로 OEP가 401000인 것을 확인할 수 있다.

패킹하기 전 파일을 x64dbg로 봐보자.

```
004071F0    60          pushad                                  EntryPoint
004071F1    BE 00704000 mov esi,11 (2).407000                   esi:EntryPoint
004071F6    8DBE 00A0FFFF lea edi,dword ptr ds:[esi-6000]       edi:EntryPoint
004071FC    57          push edi                                edi:EntryPoint
004071FD    83CD FF     or ebp,FFFFFFFF
00407200    EB 10       jmp 11 (2).407212
00407202    90          nop
00407203    90          nop
00407204    90          nop
00407205    90          nop
00407206    90          nop
00407207    90          nop
```

pushad 명령어로 push all되는 값이 있다.

그럼 이 구간의 pushad와 짝인 popad를 찾자.

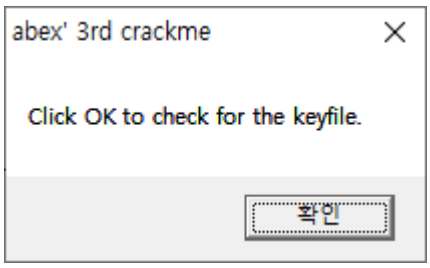
```
0040736D    61          popad
0040736E    6A 00       push 0
00407370    68 00204000 push 11 (2).402000
00407375    68 12204000 push 11 (2).402012
0040737A    8D4424 80   lea eax,dword ptr ss:[esp-80]
0040737E    6A 00       push 0
00407380    39C4        cmp esp,eax
00407382    75 FA       jne 11 (2).40737E
00407384    83EC 80     sub esp,FFFFFF80
00407387    E9 809CFFFF jmp 11 (2).40100C
```

push하는 값이 "Click OK to check for the keyfile." 이 맞는지 확인하기 위해 BP를 걸고 실행한다.

```
0040736D    61          popad
0040736E    6A 00       push 0
00407370    68 00204000 push 11.402000                  402000:"abex' 3rd crackme"
00407375    68 12204000 push 11.402012                  402012:"Click OK to check for the keyfile."
0040737A    8D4424 80   lea eax,dword ptr ss:[esp-80]
0040737E    6A 00       push 0
00407380    39C4        cmp esp,eax
00407382    75 FA       jne 11.40737E
00407384    83EC 80     sub esp,FFFFFF80
00407387    E9 809CFFFF jmp 11.40100C
```

정확하다.

그리고 마지막에 있는 jmp구문을 실행하니



메시지 박스가 출력된다.

그럼 Stolenbyte는

```
0040736E    6A 00       push 0
00407370    68 00204000 push 11.402000                  402000:"abex' 3rd crackme"
00407375    68 12204000 push 11.402012                  402012:"Click OK to check for the keyfile."
```

이 부분일 것 같다.

6A006800204000681220400O