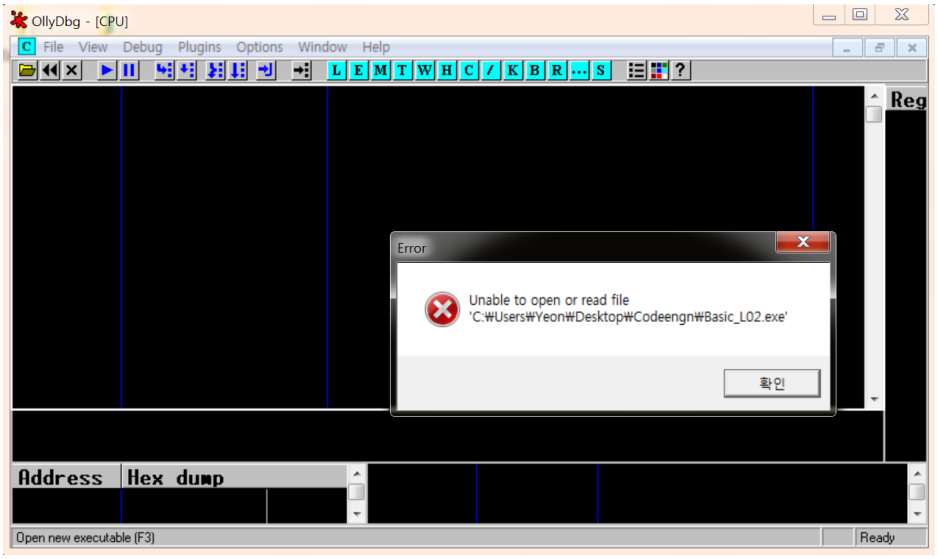
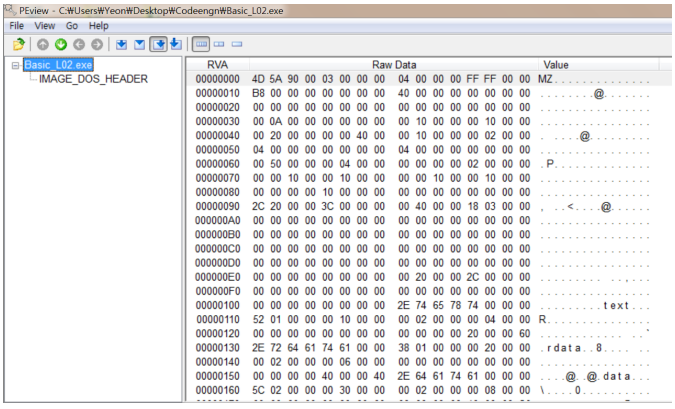
코드 엔진 Challenges: Basic 02

Author: ArturDents
Korean: 패스워드로 인증하는 실행파일이 손상되어 실행이 안되는 문제가 생겼다 패스워드가 무엇인지 분석하시오.

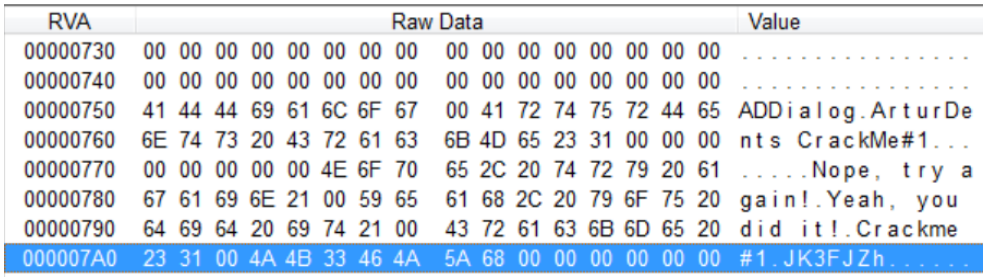
문제를 확인했으니 파일을 다운로드 받아서 실행해보자.



프로그램 실행결과 화면에 아무것도 뜨지 않고 실행이 안되는 것을 볼 수 있다. PE File format이 손상된 것이라고 생각 할 수 있다. 이를 확인하기 위해서 PEview 프로그램을 이용해보자.



정상적인 PE File Format이 아닌 IMAGE_DOS_HEADER 구조체만 가지고 있다.



RVA	Raw Data																Value
00000730	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000740	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000750	41	44	44	69	61	6C	6F	67	00	41	72	74	75	72	44	65	ADDialog.ArturDe
00000760	6E	74	73	20	43	72	61	63	6B	4D	65	23	31	00	00	00	nts CrackMe#1...
00000770	00	00	00	00	00	4E	6F	70	65	2C	20	74	72	79	20	61	.....Nope, try a
00000780	67	61	69	6E	21	00	59	65	61	68	2C	20	79	6F	75	20	gain!.Yeah, you
00000790	64	69	64	20	69	74	21	00	43	72	61	63	6B	6D	65	20	did it!.Crackme
000007A0	23	31	00	4A	4B	33	46	4A	5A	68	00	00	00	00	00	00	#1.JK3FJZh......

PEView를 이용해서 IMAGE_DOS_HEADER의 Raw_data 값을 보면 위와 같이 ASCII 코드값을 볼 수 있고 프로그램내에 패스워드가 있는 것을 볼 수 있다.
이렇게 PE구조안에 Raw_data 값을 통해서 패스워드를 알 수 있는 이유는 이프로그램이 패스워드를 컴파일 되기전부터 소스내에 선언된 정적 변수에 저장한것이기 때문이다. 이렇게 저장된 변수들(전역,정적)들은 Winodows 실행파일에 PE구조에 .data 섹션에 저장되는 규칙이있다.

비밀번호는 JK3FjZh이다.