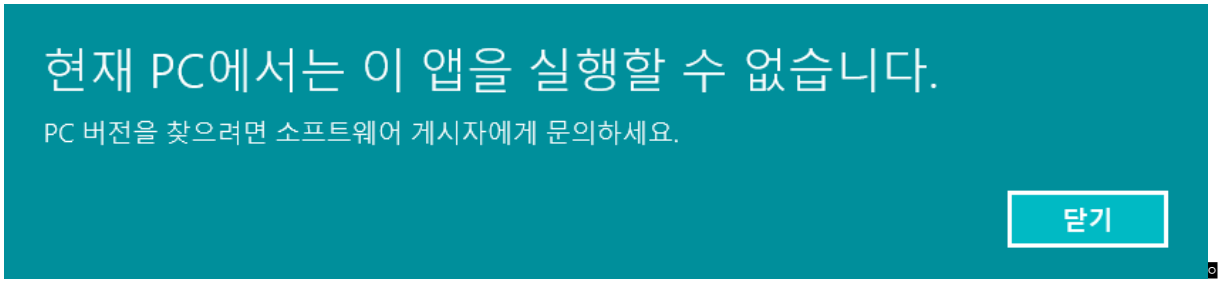
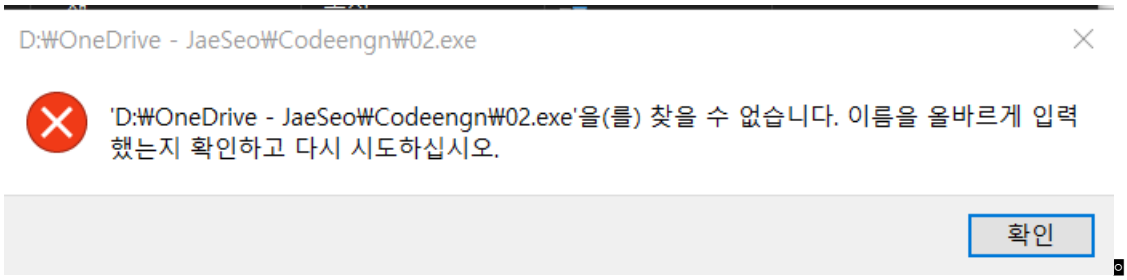
02.EXE - 패스워드로 인증하는 실행파일이 손상되어 실행이 안되는 문제가 생겼다. 패스워드가 무엇인지 분석하시오

일단 프로그램을 실행 해본다.

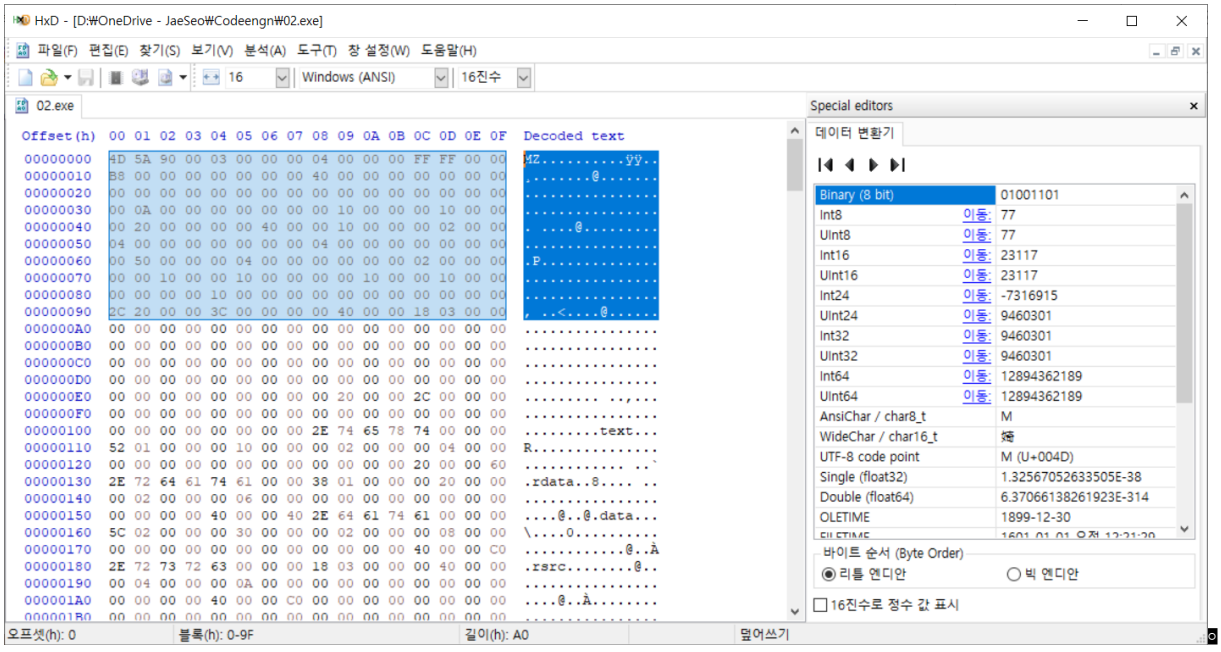


관리자 권한으로도 실행 해본다.

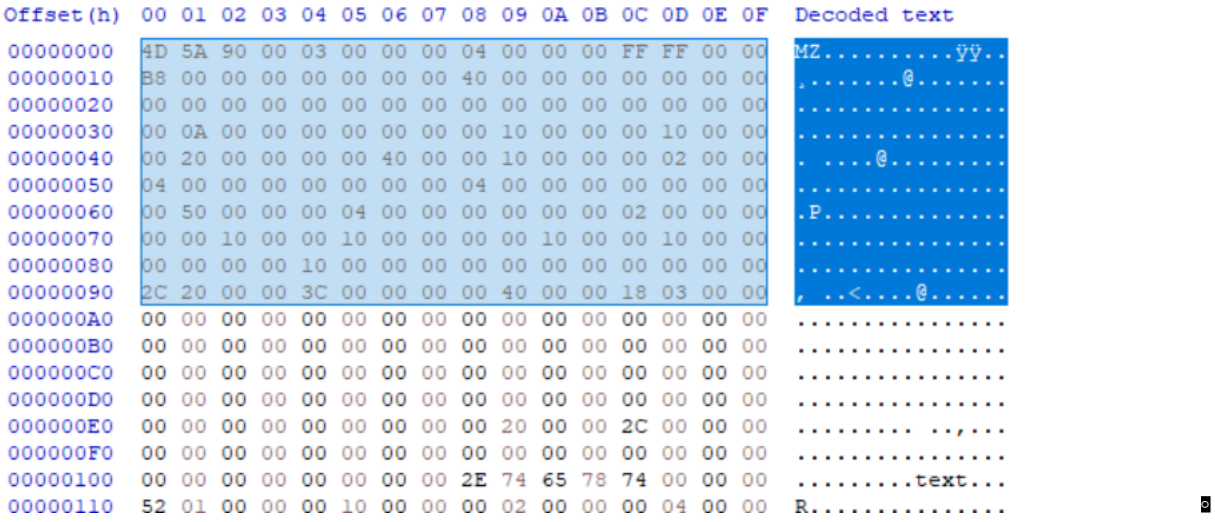


위와 같은 내용으로 프로그램이 손상이 되어 디버깅도 불가능 하다는 것을 알게되었다.

그렇기 때문에 HEXEDITER로 열어서 분석을 한다.



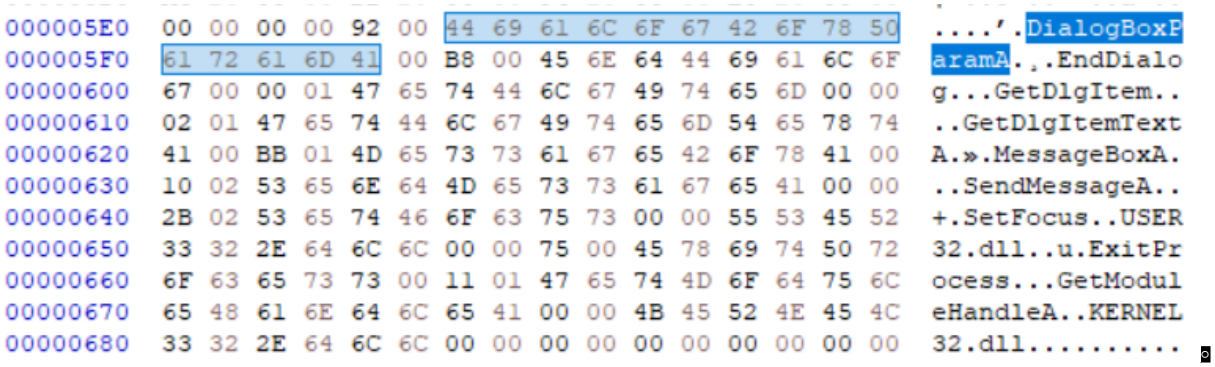
일단 시작을 보면 PE header 부분이 보이게 된다.



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ.....ÿÿ..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	¸.......@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000030	00	0A	00	00	00	00	00	00	00	10	00	00	00	10	00	00	....
00000040	00	20	00	00	00	00	40	00	00	10	00	00	00	02	00	00	. ....@.........
00000050	04	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00	....
00000060	00	50	00	00	00	04	00	00	00	00	00	00	02	00	00	00	.P..............
00000070	00	00	10	00	00	10	00	00	00	00	10	00	00	10	00	00	....
00000080	00	00	00	00	10	00	00	00	00	00	00	00	00	00	00	00	....
00000090	2C	20	00	00	3C	00	00	00	00	40	00	00	18	03	00	00	, ..<....@......
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
000000E0	00	00	00	00	00	00	00	00	00	20	00	00	2C	00	00	00	....,...
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000100	00	00	00	00	00	00	00	00	2E	74	65	78	74	00	00	00	.........text...
00000110	52	01	00	00	00	10	00	00	00	02	00	00	00	04	00	00	R...............

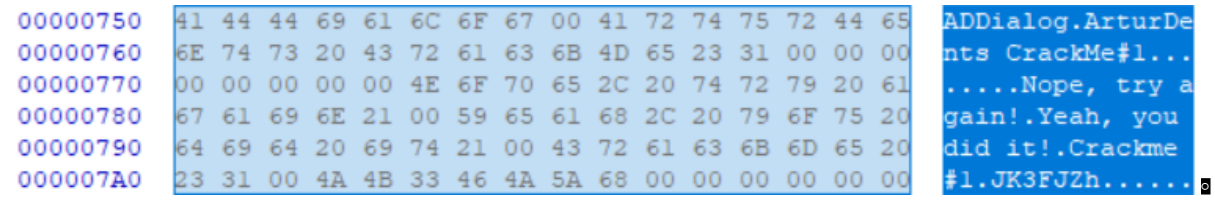
대략 이정도 부분이 PE Header 부분으로 보인다.

이제 PE Header, section Header 부분을 지나 section Data 부분을 분석 해본다.



000005E0	00	00	00	00	92	00	44	69	61	6C	6F	67	42	6F	78	50	....'.DialogBoxP
000005F0	61	72	61	6D	41	00	B8	00	45	6E	64	44	69	61	6C	6F	aramA.¸.EndDialo
00000600	67	00	00	01	47	65	74	44	6C	67	49	74	65	6D	00	00	g...GetDlgItem..
00000610	02	01	47	65	74	44	6C	67	49	74	65	6D	54	65	78	74	..GetDlgItemText
00000620	41	00	BB	01	4D	65	73	73	61	67	65	42	6F	78	41	00	A.».MessageBoxA.
00000630	10	02	53	65	6E	64	4D	65	73	73	61	67	65	41	00	00	..SendMessageA..
00000640	2B	02	53	65	74	46	6F	63	75	73	00	00	55	53	45	52	+.SetFocus..USER
00000650	33	32	2E	64	6C	6C	00	00	75	00	45	78	69	74	50	72	32.dll..u.ExitPr
00000660	6F	63	65	73	73	00	11	01	47	65	74	4D	6F	64	75	6C	ocess...GetModul
00000670	65	48	61	6E	64	6C	65	41	00	00	4B	45	52	4E	45	4C	eHandleA..KERNEL
00000680	33	32	2E	64	6C	6C	00	00	00	00	00	00	00	00	00	00	32.dll..........

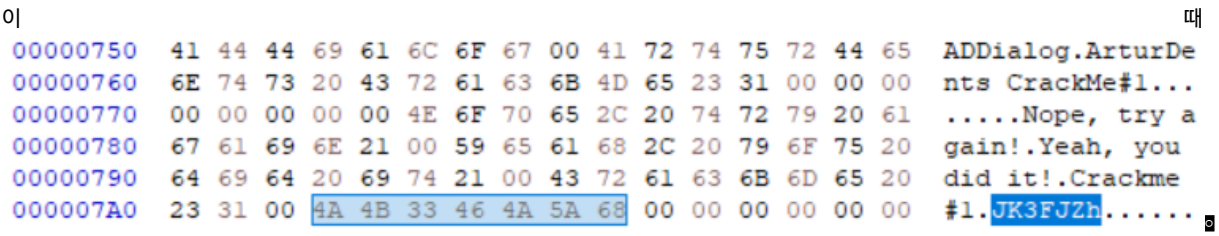
이쪽을 보면 DialogBox를 실행하고 MessageBox를 시행 SendMessage등과 같이 다양한 작업을 수행을 한다는 것을 알 수 있다.



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......

좀더 내려 보다 보면 ADDialog와 관련된 메시지를 확인 할수 있는데

이 때



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......

이러한 부분에 문자열을 발견할수 있다. 이러한 문자가 암호로 의심이 되는데 CodeEgne 사이트에 제출을 한다.

Level	Comment	Point	Report Point	Upload Report
Basic L02	코드엔진! 사랑해요!!! CodeEngn!! CodeEngn!!	3	0	x

정답 인 것을 확인 했다.

정답 : JK3FJZh