

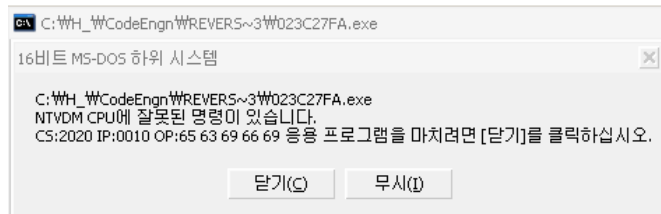
Reverse L02

2009년 12월 22일 화요일
오후 4:26

파일 확인



프로그램 실행



파일을 실행 시키면, **16비트 MS-DOS 하위 시스템**이라고 하면서 오류가 뜬다.

- 32비트 체계인 Window XP 에서 16비트 프로그램이 실행 될 시 나타나는 오류 이다.

Olydbg 로 실행



파일을 읽을 수 없다고 나온다.

With WinHex

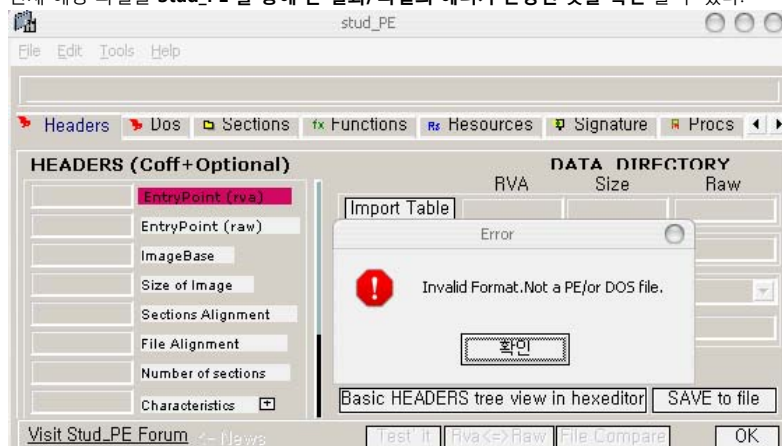
문제에서 **파일**이 손상 되었다고 언급 하였으니, Win Hex 를 통해서 파일을 열어 보았다.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
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	61Nope, 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

- 아래로 내려 보면. "Yeah, you did it!. Crackme#1 뒤에 **JK3FJZh** 라는 문자열이 있다.

보충 설명

현재 해당 파일을 Stud_PE 를 통해 본 결과, 파일의 헤더가 손상된 것을 확인 할 수 있다.



- PE Signature 도 없을 뿐더러, 크기도 전혀 맞지 않기 때문에 WinHex 를 이용하여 복구 시켰다.

기존 Header

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZyy..
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	02	00	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	00text...

복구한 Header

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZyy..
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	00	00	00	00	00	00	00	00	00	00	00	C0	00	00	00A...
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..e...'.í! .Lí!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000060	74	20	62	65	20	72	75	6E	28	69	6E	20	44	4F	53	20	t be run in DOS
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode....\$......
00000080	E3	E2	11	DB	A7	83	7F	88	A7	83	7F	88	A7	83	7F	88	ãã.Û\$!!!\$!!!\$!!!
00000090	A7	83	7F	88	A9	83	7F	88	5B	A3	6D	88	A6	83	7F	88	\$!!!@!!![£m! !!!
000000A0	60	85	79	88	A6	83	7F	88	52	69	63	68	A7	83	7F	88	`!y! !!!Rich\$!!!
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000C0	50	45	00	00	4C	01	04	00	15	D3	E6	39	00	00	00	00	PE .L....Óæ9....
000000D0	00	00	00	00	E0	00	0F	01	0B	01	05	0C	00	02	00	00	...à.....
000000E0	00	0A	00	00	00	00	00	00	00	10	00	00	00	10	00	00
000000F0	00	20	00	00	00	00	40	00	00	10	00	00	00	02	00	00@.....
00000100	04	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00
00000110	00	50	00	00	00	04	00	00	00	00	00	00	02	00	00	00	.P.....
00000120	00	00	10	00	00	10	00	00	00	00	10	00	00	10	00	00
00000130	00	00	00	00	10	00	00	00	00	00	00	00	00	00	00	00
00000140	2C	20	00	00	3C	00	00	00	00	40	00	00	18	03	00	00	, ..<....@.....
00000150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000190	00	00	00	00	00	00	00	00	00	20	00	00	2C	00	00	00
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001B0	00	00	00	00	00	00	00	00	2E	74	65	78	74	00	00	00text...

복구 후 파일 실행



Check It! 버튼을 눌러도 아무런 동작이 일어나지 않는다.

Ollydbg 로 확인

004010BA	. E8 6F000000	CALL <JMP.&USER32.GetDlgItemTextA>	LGetDlgItemTextA			
004010BF	. B8 5C304000	MOV EAX,Recover_.0040305C	ASCII "1234"			
004010C4	. B8 1E304000	MOV EBX,Recover_.0040301E				
004010C9	. B9 07000000	MOV ECX,7				
004010CE	> 8A13	MOV DL,BYTE PTR DS:[EBX]				
0040305C=Recover_.0040305C (ASCII "1234")						
Address	Hex dump				ASCII	
00403000	41 44 44 69	61 6C 6F 67	00 41 72 74	75 72 44 65	ADDIALOG.ArturDe	
00403010	6E 74 73 20	43 72 61 63	6B 4D 65 23	31 00 00 00	nts CrackMe#1..	
00403020	00 00 00 00	00 4E 6F 70	65 2C 20 74	72 79 20 61Nope, try a	
00403030	67 61 69 6E	21 00 59 65	61 68 2C 20	79 6F 75 20	gain!.Yeah, you	
00403040	64 69 64 20	69 74 21 00	43 72 61 63	6B 6D 65 20	did it!.Crackme	
00403050	23 31 00 4A	00 00 40 00	5A 68 00 00	31 32 33 34	#1..J..@.Zh. 1234	

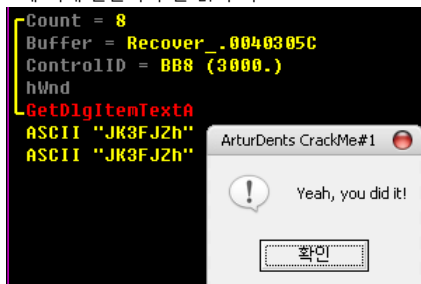
0040305C 부분 부터 사용자가 입력한 값이 들어가고, 0040301E 의 값을 참조하여 7자리 비교 하는 Code 이다.

- a. 현재 해당 코드는 Key 값이 올바르게 들어가지 않았으므로, 코드가 원하는 0040301E 자리에 JK3FJZh 문자열을 넣는다.

004010AB	. 6A 07	PUSH 7	Count = 7
004010AD	. 68 5C304000	PUSH Recover_.0040305C	Buffer = Recover_.0040305C
004010B2	. 68 B80B0000	PUSH 0BB8	ControlID = BB8 (3000.)
004010B7	. FF75 08	PUSH DWORD PTR SS:[EBP+8]	hWnd
004010BA	. E8 6F000000	CALL <JMP.&USER32.GetDlgItemTextA>	GetDlgItemTextA
004010BF	. B8 5C304000	MOV EAX,Recover_.0040305C	ASCII "JK3FJZ"
004010C4	. B8 1E304000	MOV EBX,Recover_.0040301E	ASCII "JK3FJZh"
004010C9	. B9 07000000	MOV ECX,7	
004010CE	> 8A13	MOV DL,BYTE PTR DS:[EBX]	
004010D0	. 3810	CMP BYTE PTR DS:[EAX],DL	
004010D2	. 75 18	JNZ SHORT Recover_.004010EC	
004010D4	. 40	INC EAX	
004010D5	. 43	INC EBX	
004010D6	. ^E2 F6	LOOPD SHORT Recover_.004010CE	

Address	Hex dump	ASCII
00403000	41 44 44 69 61 6C 6F 67 00 41 72 74 75 72 44 65	ADDIALOG.ArturDe
00403010	6E 74 73 20 43 72 61 63 6B 4D 65 23 31 00 4A 4B	nts CrackMe#1 JK
00403020	33 46 4A 5A 68 00 4E 6F 70 65 2C 74 72 79 20 61	3FJZh. Nope, try a
00403030	67 61 69 6E 21 00 59 65 61 68 2C 20 79 6F 75 20	gain!.Yeah, you
00403040	64 69 64 20 69 74 21 00 43 72 61 63 6B 6D 65 20	did it!.Crackme
00403050	23 31 00 00 00 00 40 00 00 00 00 00 4A 4B 33 46	#1....@....JK3F
00403060	4A 5A 00 00 00 00 00 00 00 00 00 00 00 00 00 00	JZ.....

- i. Push 7 에 의해 한글자가 덜 읽혀 지므로 004010AB : PUSH 7 -> PUSH 8 로, 004010C9 : MOV ECX 7 -> MOV ECX 8 로 변환 후 실행



- a) 올바른 값이 들어가게 되고, 004010CE ~ 004010D6 의 Loop 조건을 만족하여 검사하였기에 성공 MessageBox 출력된다.

답
JK3FJZh