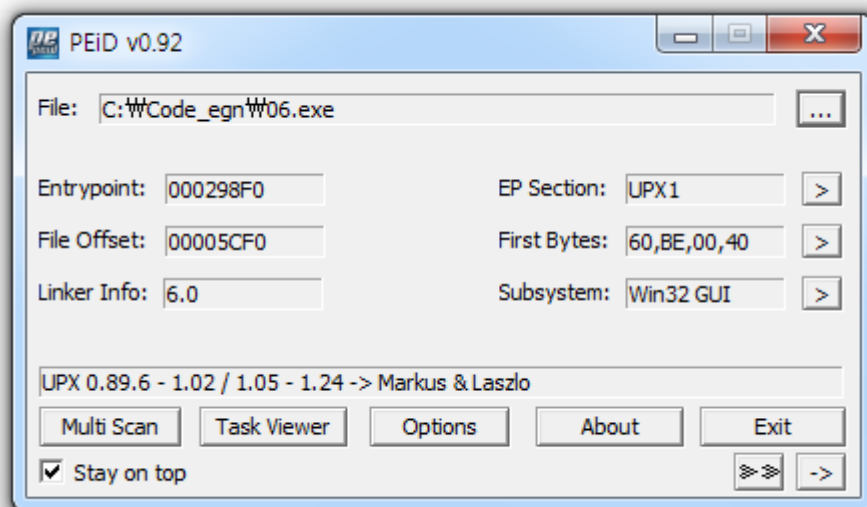
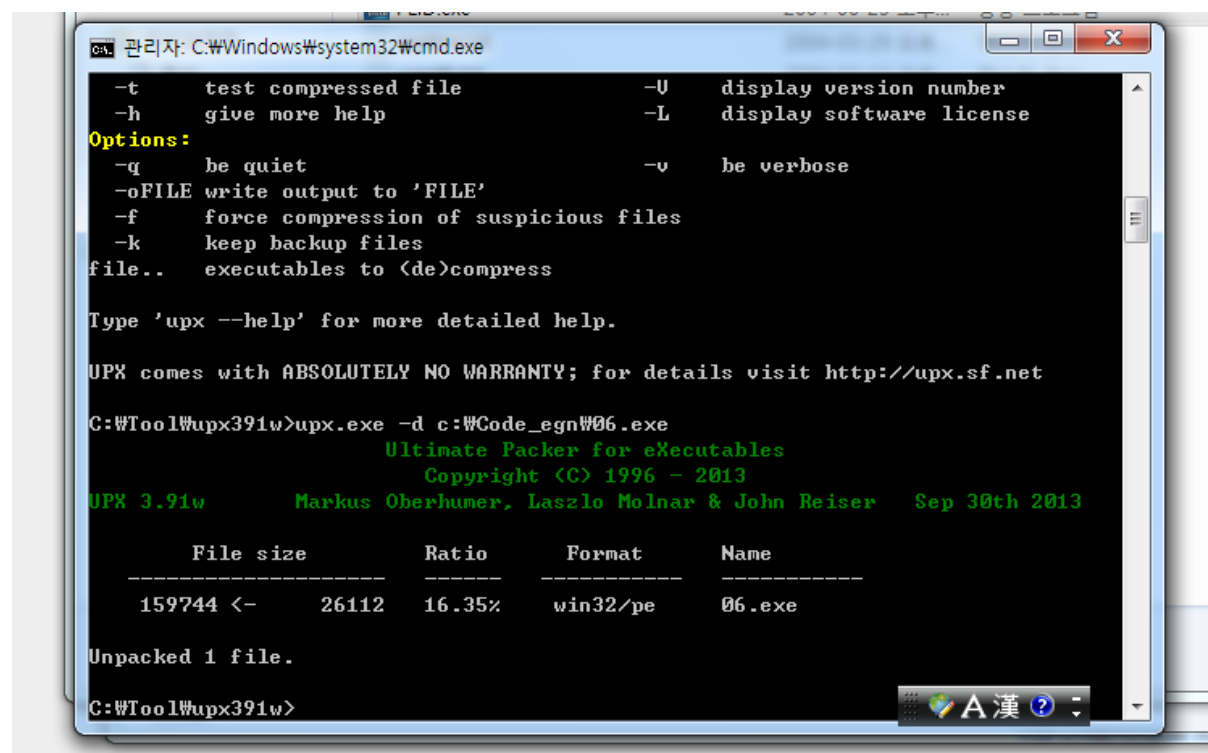


Code Engn Basic 6

4.Z320



PEiD로 확인 시 UPX 패키징이 되어 있는것을 확인할 수 있습니다.



UPX를 이용, 디컴프레스 합니다.

Address	Disassembly	Comment
00401360	55	PUSH EBP
00401361	8BEC	MOV EBP,ESP
00401363	6A FF	PUSH -1
00401365	68 48014200	PUSH 06.00420148
0040136A	68 442F4000	PUSH 06.00402F44
0040136F	64:A1 00000000	MOV EAX,DWORD PTR FS:[0]
00401375	50	PUSH EAX
00401376	64:8925 0000	MOV DWORD PTR FS:[0],ESP
0040137D	83C4 A4	ADD ESP,-5C
00401380	53	PUSH EBX
00401381	56	PUSH ESI
00401382	57	PUSH EDI
00401383	8965 E8	MOV DWORD PTR SS:[EBP-18],ESP
00401386	FF15 B8514200	CALL DWORD PTR DS:[<&KERNEL32.GetVersion
0040138C	A3 6C364200	MOV DWORD PTR DS:[42366C],EAX
00401391	A1 6C364200	MOV EAX,DWORD PTR DS:[42366C]
00401396	C1E8 08	SHR EAX,8
00401399	25 FF000000	AND EAX,0FF
0040139E	A3 78364200	MOV DWORD PTR DS:[423678],EAX
004013A3	8B00 6C364200	MOV ECX,DWORD PTR DS:[42366C]
004013A9	81E1 FF000000	AND ECX,0FF
004013AF	8900 74364200	MOV DWORD PTR DS:[423674],ECX
004013B5	8B15 74364200	MOV EDX,DWORD PTR DS:[423674]
004013BB	C1E2 08	SHL EDX,8
004013BE	0315 78364200	ADD EDX,DWORD PTR DS:[423678]
004013C4	8915 78364200	MOV DWORD PTR DS:[423670],EDX
004013CA	A1 6C364200	MOV EAX,DWORD PTR DS:[42366C]
004013CF	C1E8 10	SHR EAX,10
004013D2	25 FFFF0000	AND EAX,0FFFF
004013D7	A3 6C364200	MOV DWORD PTR DS:[42366C],EAX
004013DC	6A 00	PUSH 0
004013DE	E8 7D190000	CALL 06.00402D60
004013E3	83C4 04	ADD ESP,4
004013E6	85C0	TEST EAX,EAX
004013E8	75 0A	JNZ SHORT 06.004013F4
004013EA	6A 1C	PUSH 1C
004013EC	E8 FF000000	CALL 06.004014F0
004013F1	83C4 04	ADD ESP,4
004013F4	C745 FC 0000	MOV DWORD PTR SS:[EBP-4],0
004013FB	E8 F0150000	CALL 06.004029F0
00401400	FF15 B4514200	CALL DWORD PTR DS:[<&KERNEL32.GetCommand
00401406	A3 CC4F4200	MOV DWORD PTR DS:[424FCC],EAX
0040140B	E8 C0130000	CALL 06.004027D0
00401410	A3 50364200	MOV DWORD PTR DS:[423650],EAX
00401415	E8 A60E0000	CALL 06.004022C0
0040141A	E8 510D0000	CALL 06.00402170
0040141F	E8 AC080000	CALL 06.00401CD0
00401424	C745 D0 0000	MOV DWORD PTR SS:[EBP-30],0
0040142B	8B4D 04	MOV ECX,DWORD PTR SS:[EBP-FC]

여기서 OEP가 00401360임을 확인할 수 있습니다.

00401030	> 55	PUSH EBP	
00401031	8BEC	MOV EBP,ESP	
00401033	83EC 40	SUB ESP,40	
00401036	53	PUSH EBX	
00401037	56	PUSH ESI	
00401038	57	PUSH EDI	
00401039	8D7D C0	LEA EDI,DWORD PTR SS:[EBP-40]	
0040103C	B9 10000000	MOV ECX,10	
00401041	B8 CCCCCCCC	MOV EAX,CCCCCCCC	
00401046	F3:AB	REP STOS DWORD PTR ES:[EDI]	
00401048	8BF4	MOV ESI,ESP	
0040104A	6A 64	PUSH 64	
0040104C	68 D4354200	PUSH 06.004235D4	Count = 64 (100.)
00401051	68 E8030000	PUSH 3E8	Buffer = 06.004235D4
00401056	A1 38364200	MOV EAX,DWORD PTR DS:[423638]	ControlID = 3E8 (1000.)
0040105B	50	PUSH EAX	hWnd => NULL
0040105C	FF15 B0524200	CALL DWORD PTR DS:[<&USER32.GetDlgItemTextA]	GetDlgItemTextA
00401062	3BF4	CMP ESI,ESP	
00401064	E8 B7020000	CALL 06.00401320	
00401069	68 D4354200	PUSH 06.004235D4	
0040106E	68 302A4200	PUSH 06.00422A30	
00401073	E8 18020000	CALL 06.00401290	ASCII "AD46DFS547"
00401078	83C4 08	ADD ESP,8	
0040107B	85C0	TEST EAX,EAX	
0040107D	75 24	JNZ SHORT 06.004010A3	
0040107F	3BF4	MOV ESI,ESP	
00401081	6A 40	PUSH 40	
00401083	68 48004200	PUSH 06.00420048	Style = MB_OK!MB_ICONASTERISK!MB_APPLMODAL
00401088	68 38004200	PUSH 06.00420038	Title = "Good Job!"
0040108D	8B0D 38364200	MOV ECX,DWORD PTR DS:[423638]	Text = "You got it ;)"
00401093	51	PUSH ECX	hOwner => NULL
00401094	FF15 B4524200	CALL DWORD PTR DS:[<&USER32.MessageBoxA]	MessageBoxA
0040109A	3BF4	CMP ESI,ESP	
0040109C	E8 7F020000	CALL 06.00401320	
004010A1	EB 22	JMP SHORT 06.004010C5	
004010A3	> 8BF4	MOV ESI,ESP	
004010A5	6A 10	PUSH 10	
004010A7	68 30004200	PUSH 06.00420030	Style = MB_OK!MB_ICONHAND!MB_APPLMODAL
004010AC	68 1C004200	PUSH 06.0042001C	Title = "ERROR"
004010B1	8B15 38364200	MOV EDX,DWORD PTR DS:[423638]	Text = "Wrong serial!!!"
004010B7	52	PUSH EDX	hOwner => NULL
004010B8	FF15 B4524200	CALL DWORD PTR DS:[<&USER32.MessageBoxA]	MessageBoxA
004010BE	3BF4	CMP ESI,ESP	
004010C0	E8 5B020000	CALL 06.00401320	
004010C5	> 33C0	XOR EAX,EAX	
004010C7	5F	POP EDI	
004010C8	5E	POP ESI	
004010C9	5B	POP EBX	
004010CA	83C4 40	ADD ESP,40	
004010CD	3BEC	CMP EBP,ESP	
004010CF	E8 4C020000	CALL 06.00401320	
004010D4	8BE5	MOV ESP,EBP	
004010D6	5D	POP EBP	
004010D7	C3	RETN	
004010D8	CC	INT3	

문자열을 입력받은 후 메시지 박스를 출력하는 함수가 보입니다.

그리고 무언가 정해진 ASCII값과 사용자가 입력한 ASCII값을 PUSH 후 함수를 호출함을 볼 수 있습니다.

그리고 아래에는 Good Job이라는 제목과 ERROR이라는 제목을 가진 메시지 박스가 나오는것으로 보아 TEST명령의 결과에 따라 성공과 실패가 나뉘지는것을 확인할 수 있습니다.

0040120E	CC	INT3	
0040120F	CC	INT3	
00401290	\$ 8B5424 04	MOV EDX,DWORD PTR SS:[ESP+4]	06.00422A30
00401294	. 8B4C24 08	MOV ECX,DWORD PTR SS:[ESP+8]	
00401298	. F7C2 03000000	TEST EDX,3	
0040129E	. 75 3C	JNZ SHORT 06.004012DC	
004012A0	> 8B02	MOV EAX,DWORD PTR DS:[EDX]	
004012A2	. 3A01	CMP AL,BYTE PTR DS:[ECX]	
004012A4	. 75 2E	JNZ SHORT 06.004012D4	
004012A6	. 0AC0	OR AL,AL	
004012A8	. 74 26	JE SHORT 06.004012D0	
004012AA	. 3A61 01	CMP AH,BYTE PTR DS:[ECX+1]	
004012AD	. 75 25	JNZ SHORT 06.004012D4	
004012AF	. 0AE4	OR AH,AH	
004012B1	. 74 1D	JE SHORT 06.004012D0	
004012B3	. C1E8 10	SHR EAX,10	
004012B6	. 3A41 02	CMP AL,BYTE PTR DS:[ECX+2]	
004012B9	. 75 19	JNZ SHORT 06.004012D4	
004012BB	. 0AC0	OR AL,AL	
004012BD	. 74 11	JE SHORT 06.004012D0	
004012BF	. 3A61 03	CMP AH,BYTE PTR DS:[ECX+3]	
004012C2	. 75 10	JNZ SHORT 06.004012D4	
004012C4	. 83C1 04	ADD ECX,4	
004012C7	. 83C2 04	ADD EDX,4	
004012CA	. 0AE4	OR AH,AH	
004012CC	. 75 D2	JNZ SHORT 06.004012A0	
004012CE	. 8BFF	MOV EDI,EDI	
004012D0	> 33C0	XOR EAX,EAX	
004012D2	. C3	RETN	
004012D3	. 90	NOP	
004012D4	> 1BC0	SBB EAX,EAX	
004012D6	. D1E0	SHL EAX,1	
004012D8	. 40	INC EAX	
004012D9	. C3	RETN	
004012DA	. 8BFF	MOV EDI,EDI	
004012DC	> F7C2 01000000	TEST EDX,1	
004012E2	. 74 14	JE SHORT 06.004012F8	
004012E4	. 8A02	MOV AL,BYTE PTR DS:[EDX]	
004012E6	. 42	INC EDX	
004012E7	. 3A01	CMP AL,BYTE PTR DS:[ECX]	
004012E9	. 75 E9	JNZ SHORT 06.004012D4	
004012EB	. 41	INC ECX	
004012EC	. 0AC0	OR AL,AL	
004012EE	. 74 E0	JE SHORT 06.004012D0	
004012F0	. F7C2 02000000	TEST EDX,2	
004012F6	. 74 A8	JE SHORT 06.004012A0	
004012F8	> 66:8B02	MOV AX,WORD PTR DS:[EDX]	
004012FB	. 83C2 02	ADD EDX,2	
004012FE	. 3A01	CMP AL,BYTE PTR DS:[ECX]	
00401300	. 75 D2	JNZ SHORT 06.004012D4	
00401302	. 0AC0	OR AL,AL	
00401304	. 74 CA	JE SHORT 06.004012D0	
00401306	. 3A61 01	CMP AH,BYTE PTR DS:[ECX+1]	
00401309	. 75 C9	JNZ SHORT 06.004012D4	
0040130B	. 0AE4	OR AH,AH	
0040130D	. 74 C1	JE SHORT 06.004012D0	
0040130F	. 83C1 02	ADD ECX,2	
00401312	. EB 8C	JMP SHORT 06.004012A0	
00401314	CC	INT3	
00401315	CC	INT3	

EDX에 프로그램 내에 있던 값을, ECX에는 사용자가 입력한 값을 넣은 뒤 루프문 안으로 들어갑니다.

EAX에 문자열 4byte를 넣은 뒤 사용자가 입력한 값 한글자 한글자와 서로 비교를 하기 시작합니다. 그리고 비교하여 값이 다를 경우에는 004012D4로 점프, EAX값을 1로 만든 뒤에 리턴 함을 확인할 수 있습니다. 이때 위에서 TEST EAX EAX의 결과값에 따라 메시징박스의 내용이 달라짐으로 보아 004012D4는 실패의 메시지를 띄우게 하기 위한 주소값임을 알 수 있습니다.

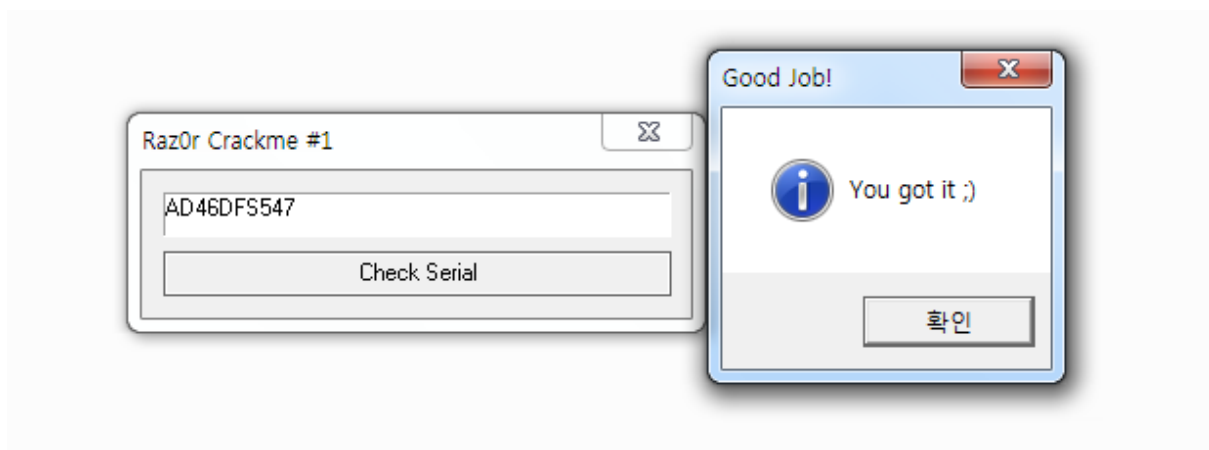
004012C4	. 83C1 04	ADD ECX,4	
004012C7	. 83C2 04	ADD EDX,4	
004012CA	. 0AE4	OR AH,AH	
004012CC	. 75 D2	JNZ SHORT 06.004012A0	
004012CE	. 8BFF	MOV EDI,EDI	
004012D0	> 33C0	XOR EAX,EAX	
004012D2	. C3	RETN	
004012D3	. 90	NOP	
004012D4	> 1BC0	SBB EAX,EAX	
004012D6	. D1E0	SHL EAX,1	
004012D8	. 40	INC EAX	
004012D9	. C3	RETN	
004012DA	. 8BFF	MOV EDI,EDI	
004012DC	> F7C2 01000000	TEST EDX,1	

비교를 계속하다 널 문자열을 만나게 되면 OR AL(AH) AL(AH) 구문에서 ZF가 설정되므로 004012D0로 빠져나오게 되며 EAX값이 0으로 셋팅된 채로 RETN하게 됩니다.

00401069	. 68 D4354200	PUSH 06.004235D4	ASCII "AAAAAAAAAA"
0040106E	. 68 302A4200	PUSH 06.00422A30	ASCII "AD46DFS547"
00401073	. E8 18020000	CALL 06.00401290	
00401078	. 83C4 08	ADD ESP,8	
0040107B	. 85C0	TEST EAX,EAX	
0040107D	. 75 24	JNZ SHORT 06.004010A3	
0040107F	. 8BF4	MOV ESI,ESP	
00401081	. 6A 40	PUSH 40	
00401083	. 68 48004200	PUSH 06.00420048	Style = MB_OK!MB_ICONASTERISK!MB_APPLMODAL
00401088	. 68 38004200	PUSH 06.00420038	Title = "Good Job!"
0040108D	. 8B00 38364200	MOV ECX,DWORD PTR DS:[423638]	Text = "You got it ;)"
00401093	. 51	PUSH ECX	hOwner => 00060638 ('Raz0r Crackme #1',class='#32770')
00401094	. FF15 B4524200	CALL DWORD PTR DS:[<&USER32.MessageBoxA	MessageBoxA
0040109A	. 3BF4	CMPL ESI,ESP	
0040109C	. E8 7F020000	CALL 06.00401320	
004010A1	. 75 22	JMP SHORT 06.004010C5	

그리고 TEST문에서 ZF가 설정되지 않으므로 Good Job 부분으로 갈 수가 있게 됩니다.

즉 프로그램 내에 있는 문자열 값이 키값이라 볼 수 있는 것입니다.



그리고 이를 입력하게 되면 맞는 답임을 알리는 메세지 박스가 나오는 것을 확인할 수 있습니다.
따라서 6번 문제의 답은 OEP인 00401360과 키 값인 AD46DFS547를 합한 00401360AD46DFS547가 되게 됩니다.