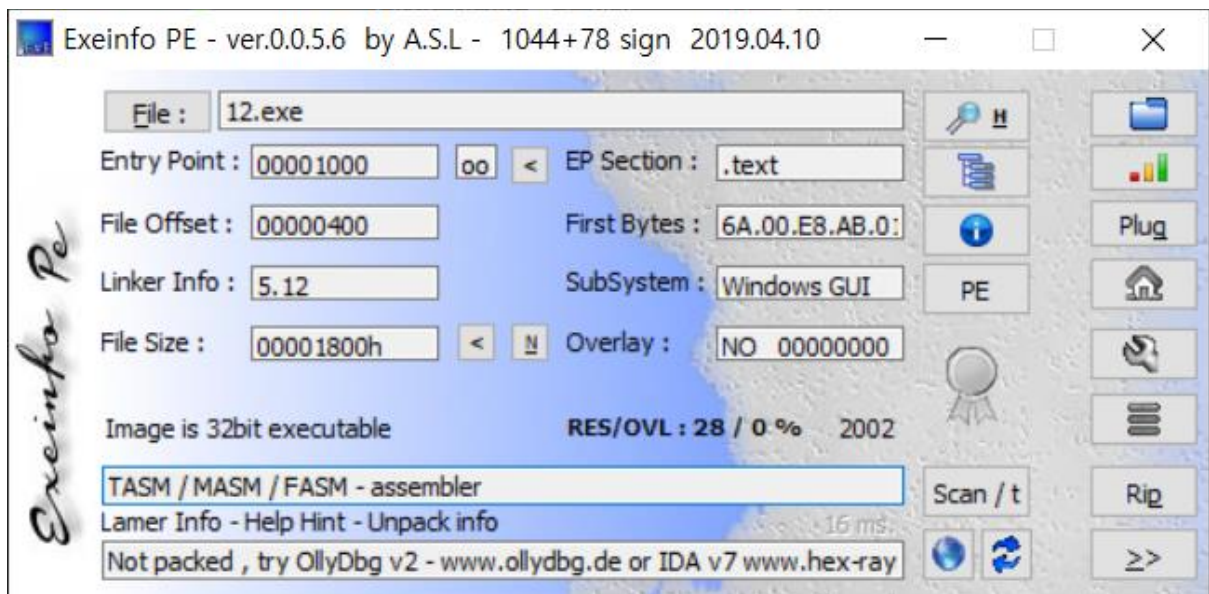


12.exe - Key를 구한 후 입력하게 되면 성공메시지를 볼 수 있다

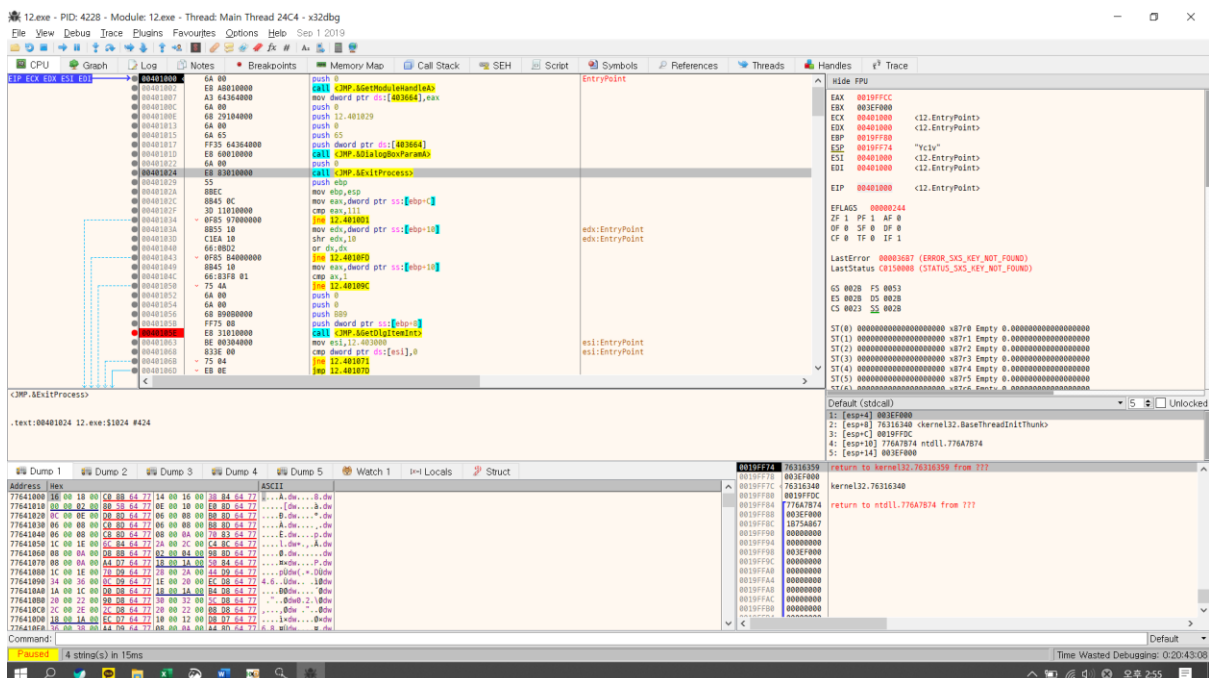
이때 성공메시지 대신 Key 값이 MessageBox에 출력 되도록 하려면 파일을 HexEdit로 오픈 한 다음 0x???? ~ 0x???? 영역에 Key 값을 overwrite 하면 된다.

문제 : Key값과 + 주소영역을 찾으시오 Ex) 77777777????????



PE 분석을 통해 Packing이 되지 않았다는 것을 확인할 수 있다.

이제 X32DBG를 통해 분석을 해본다.



이제 여기서 문자열 검색을 통해 분석을 해본다.

Address	Disassembly	String
00401086	push 12.403530	"In the Bin"
00401088	push 12.403538	"Congratulation, you found the right key"
00404455	add byte ptr ds:[edx+eax+400100],bh	"e!"
00404599	add byte ptr ds:[edx+eax+400100],bh	"e!"

검색을 통해 성공 메시지를 발견했다. 이때 메시지 주소로 들어가 분석을 해본다.

0040104C	66:83F8 01	cmp ax,1	
00401050	75 4A	jne 12.40109C	
00401052	6A 00	push 0	
00401054	6A 00	push 0	
00401056	68 B9080000	push 889	
00401058	FF75 08	push dword ptr ss:[ebp+8]	
0040105E	E8 31010000	call <JMP.&GetDlgItemInt>	
00401063	BE 00304000	mov esi,12.403000	
00401068	833E 00	cmp dword ptr ds:[esi],0	
0040106B	75 04	jne 12.401071	
0040106D	EB 0E	jmp 12.40107D	
0040106F	EB 0C	jmp 12.40107D	
00401071	8B1E	mov ebx,dword ptr ds:[esi]	
00401073	E8 97000000	call 12.40106F	
00401075	83C6 04	add esi,4	
0040107B	EB EB	jmp 12.401068	
0040107D	3D BF96287A	cmp eax,7A2896BF	
00401082	75 14	jne 12.401098	
00401084	6A 40	push 40	
00401086	68 30354000	push 12.403530	403530:"In the Bin"
00401088	68 38354000	push 12.403538	403538:"Congratulation, you found the right key"
00401090	FF75 08	push dword ptr ss:[ebp+8]	
00401093	E8 02010000	call <JMP.&MessageBoxA>	
00401098	EB 6C	jmp 12.401106	
0040109A	EB 61	jmp 12.4010FD	
0040109C	66:83F8 02	cmp ax,2	
004010A0	75 10	jne 12.4010B2	
004010A2	6A 00	push 0	
004010A4	6A 00	push 0	
004010A6	6A 10	push 10	
004010A8	FF75 08	push dword ptr ss:[ebp+8]	

Jne를 통해 성공 메시지를 출력 하는지에 대해 분기점이 갈리고 있는데 이때 위의 cmp eax,7A2896BF를 통해 비교 하여 키 값을 체크 하고 있는 것을 볼 수가 있다.

0040107B	EB EB	jmp 12.401068	
0040107D	3D BF96287A	cmp eax,7A2896BF	
00401082	75 14	jne 12.401098	
00401084	6A 40	push 40	

이때 EAX의 값을 확인해본다.

Edit

Expression: 000004D2

Bytes: D2040000

Signed: 1234

Unsigned: 1234

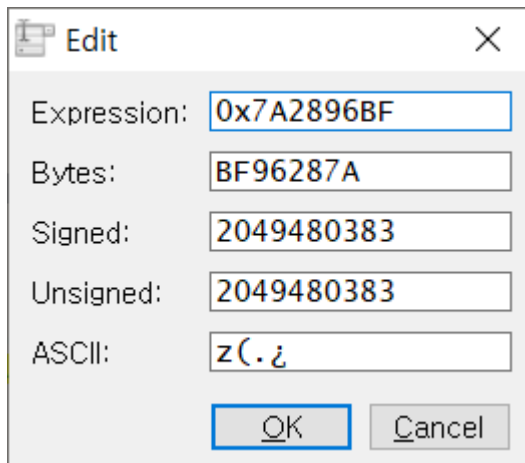
ASCII: ...0

OK

Cancel

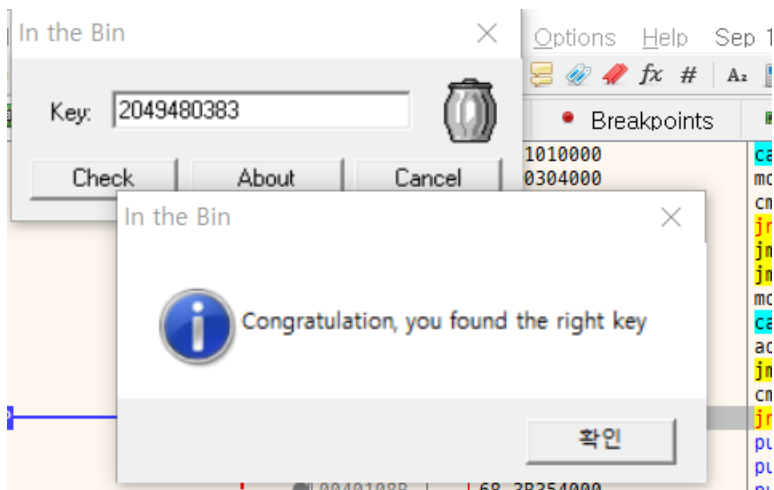
테스트를 위해 입력한 키 값인 1234가 16진수로 인코딩 되어 저장되어 있는 것을 알 수가 있다.

이때 cmp를 하는 7A2896BF를 10진수로 바꾸어 확인해 본다.



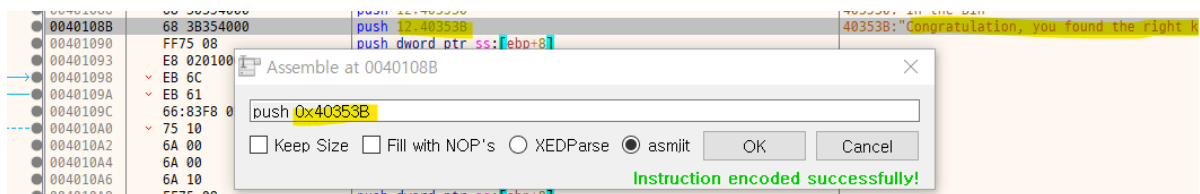
이때 키 값은 2049480383라는 것을 알 수가 있다.

이제 이 찾은 키 값이 정확한지 체크를 해본다.



그 결과 정확한 키 값을 찾았다는 것을 확인할 수가 있다.

이제 문제로 돌아와 성공 메시지 부분에 키 값을 넣어서 수정을 해본다.



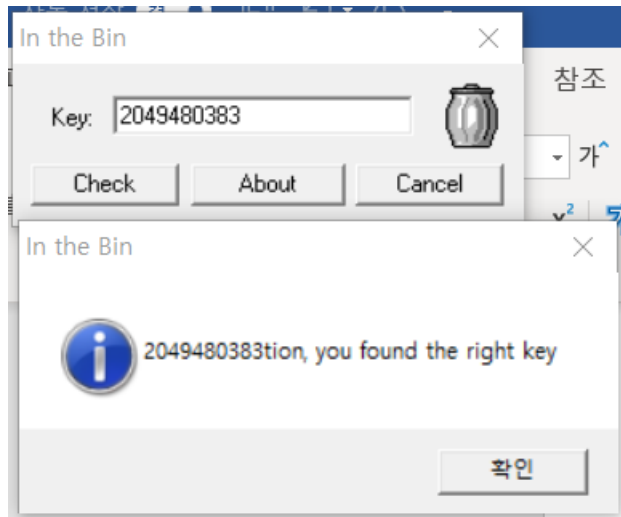
문자열을 PUSH 하는 주소를 확인하여 성공 메시지를 참조하는 주소를 확인하고

Address	Hex	ASCII
0040353B	43 6F 6E 67 72 61 74 75 6C 61 74 69 6F 6E 2C 20	Congratulation,
0040354B	79 6F 75 20 66 6F 75 6E 64 20 74 68 65 20 72 69	you found the ri
0040355B	67 68 74 20 6B 65 79 00 00 00 00 00 00 00 00	ght key.....
0040356B	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040357B	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040358B	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040359B	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

덤프를 확인하여 offset 주소를 구하여 수정을 진행해본다.

00000D00	50 63 30 4A 49 59 34 62 47 2B 47 45 51 77 4C 72	Pc0JIY4bG+GEQwLr
00000D10	36 6B 70 47 6C 7A 51 66 49 53 4D 6A 4D 2F 34 6A	6kpG1zQfISMjM/4j
00000D20	62 34 45 68 4F 71 69 71 00 00 00 00 78 56 34 12	b4EhOqiq....xV4.
00000D30	49 6E 20 74 68 65 20 42 69 6E 00 32 30 34 39 34	In the Bin.20494
00000D40	38 30 33 38 33 00 00 00 00 00 00 00 00 00 00 00	80383.....
00000D50	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000D60	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Offset 주소를 가지고 수정을 하여 성공 시리얼 키 값을 삽입한다.



수정한 파일을 실행해서 정상적을 동작하는 것을 확인할 수가 있다.

정답: 20494803830D3B0D45