

정상동작하면 정상만이 찍힌다.

디버거로 실행!

0040840B	- E8 00690000	CALL 04.0040ED10	
00408410	- FF15 70B14300	CALL DWORD PTR DS:[<&KERNEL32.GetCommandLineA>]	[GetCommandLineA
00408416	- A3 E4A24300	MOV DWORD PTR DS:[43A2E4],EAX	
0040841B	- E8 D0660000	CALL 04.0040EAF0	
00408420	- A3 FC884300	MOV DWORD PTR DS:[4388FC],EAX	
00408425	- E8 B6610000	CALL 04.0040E5E0	
0040842A	- E8 61600000	CALL 04.0040E490	
0040842F	- E8 7C430000	CALL 04.0040C7B0	
00408434	- 8B0D 48894300	MOV ECX,DWORD PTR DS:[438948]	
0040843A	- 890D 4C894300	MOV DWORD PTR DS:[43894C],ECX	
00408440	- 8B15 48894300	MOV EDX,DWORD PTR DS:[438948]	
00408446	- 52	PUSH EDX	
00408447	- A1 40894300	MOV EAX,DWORD PTR DS:[438940]	
0040844C	- 50	PUSH EAX	
0040844D	- 8B0D 3C894300	MOV ECX,DWORD PTR DS:[43893C]	
00408453	- 51	PUSH ECX	
00408454	- E8 B68BF0FF	CALL 04.0040100F	
00408459	- 83C4 0C	ADD ESP,0C	
0040845C	- 8945 E4	MOV DWORD PTR SS:[EBP-1C],EAX	
0040845F	- 8B55 E4	MOV EDX,DWORD PTR SS:[EBP-1C]	
00408462	- 52	PUSH EDX	
00408463	- E8 88430000	CALL 04.0040C7F0	
00408468	- 8B45 EC	MOV EAX,DWORD PTR SS:[EBP-14]	
0040846D	- 8B45 EC	MOV ECX,DWORD PTR SS:[EBP-14]	

BP절어둔부분을 F8로 지나치자 디버깅당함! 떴다

그래서 BP걸고 들어가보았다.

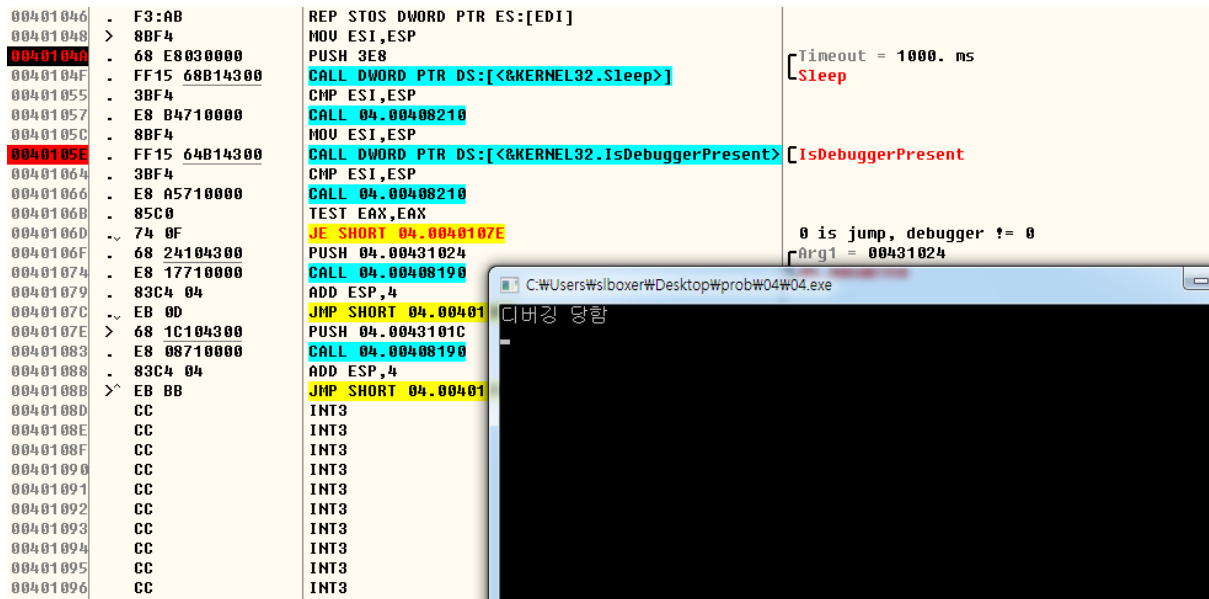
00401037	- 8B7D 00	MOV EDI,DWORD PTR SS:[EBP-40]	
0040103C	- B9 10000000	MOV ECX,10	
00401041	- B8 CCCCCCCC	MOV EAX,CCCCCCCC	
00401046	- F3:AB	REP STOS DWORD PTR ES:[EDI]	
00401048	> 8BF4	MOV ESI,ESP	
00401049	- 68 E8030000	PUSH 3E8	[Timeout = 1000. ms
0040104F	- FF15 68B14300	CALL DWORD PTR DS:[<&KERNEL32.Sleep>]	[Sleep
00401055	- 3BF4	CMP ESI,ESP	
00401057	- E8 B4710000	CALL 04.00408210	
0040105C	- 8BF4	MOV ESI,ESP	
0040105E	- FF15 64B14300	CALL DWORD PTR DS:[<&KERNEL32.IsDebuggerPresent>]	[IsDebuggerPresent
00401064	- 3BF4	CMP ESI,ESP	
00401066	- E8 A5710000	CALL 04.00408210	
0040106B	- 85C0	TEST EAX,EAX	
0040106D	~ 74 0F	JE SHORT 04.0040107E	
0040106F	- 68 24104300	PUSH 04.00431024	[Arg1 = 00431024
00401074	- E8 17710000	CALL 04.00408190	[04.00408190
00401079	- 83C4 04	ADD ESP,4	
0040107C	~ EB 0D	JMP SHORT 04.0040108B	
0040107E	> 68 1C104300	PUSH 04.0043101C	[Arg1 = 0043101C
00401083	- E8 08710000	CALL 04.00408190	[04.00408190
00401088	- 83C4 04	ADD ESP,4	
0040108B	> EB BB	JMP SHORT 04.00401048	
0040108D	CC	INT3	
0040108E	CC	INT3	

위쪽 잘린부분은 스택에 공간만들어주는 작업이니 무시하고

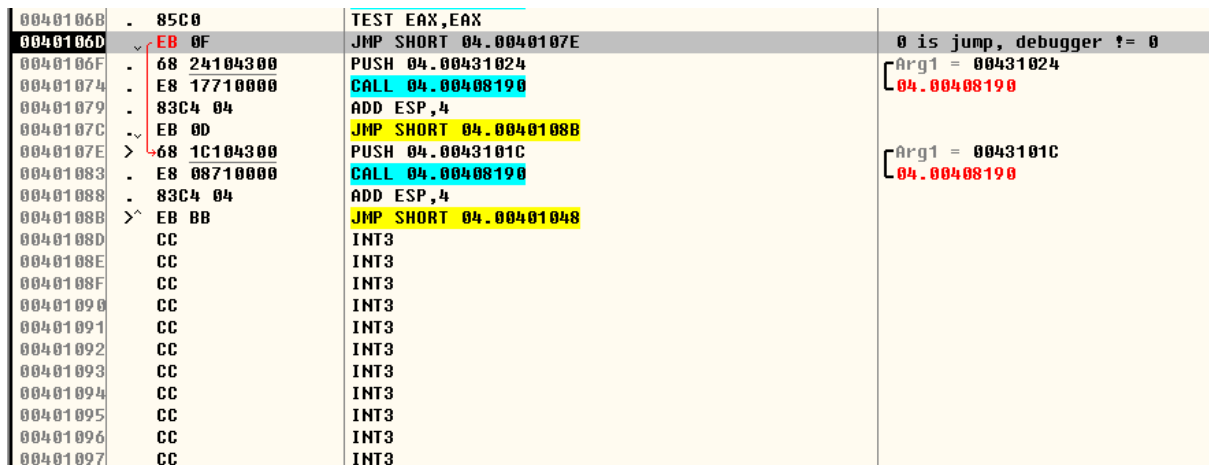
1000ms씩 쉬는 함수가 있다(sleep) 동작할때 보면 1초마다 글씨 찍히는걸 볼수있다.

그리고 아래에 IsDebuggerPresent로 디버거가 있는지 알아본다.

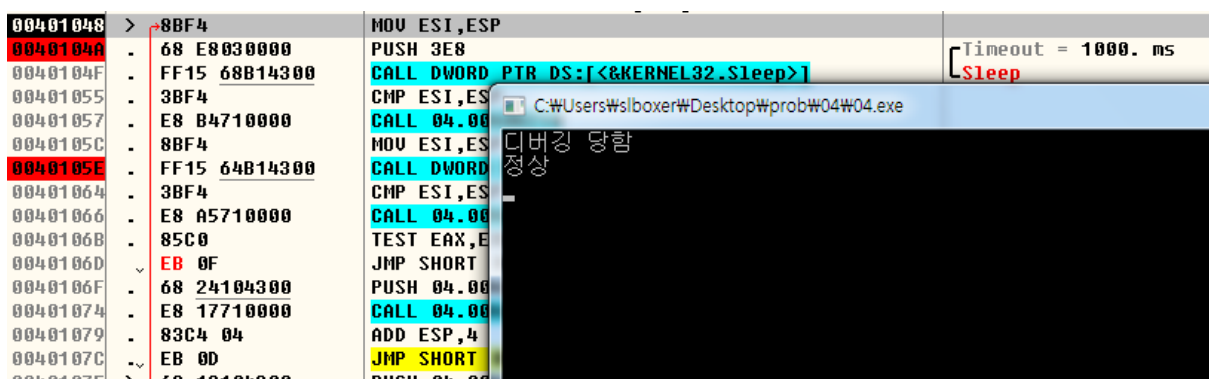
TEST EAX, EAX가 0이면 점프하는데 IsDebuggerPresent에서 EAX가 0이 아니었는지 점프하지 않고 push 00431024를 진행하였다.



그대로 진행했더니 이렇게 디버깅당함이 떴다.



디버거 탐지 함수는 찾았지만 난 이 프로그램을 속일것이다. JE를 JMP로 바꿨다.



속이기까지 성공했다.

따라서 디버거 탐지함수는 IsDebuggerPresent