

# 리버스 엔지니어링 (3)

발표자: 양유진

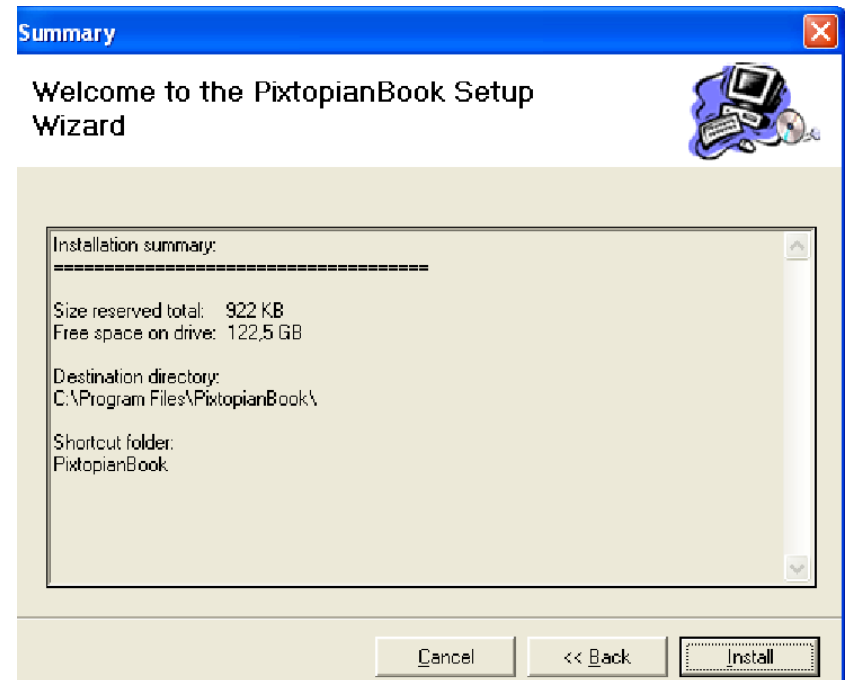
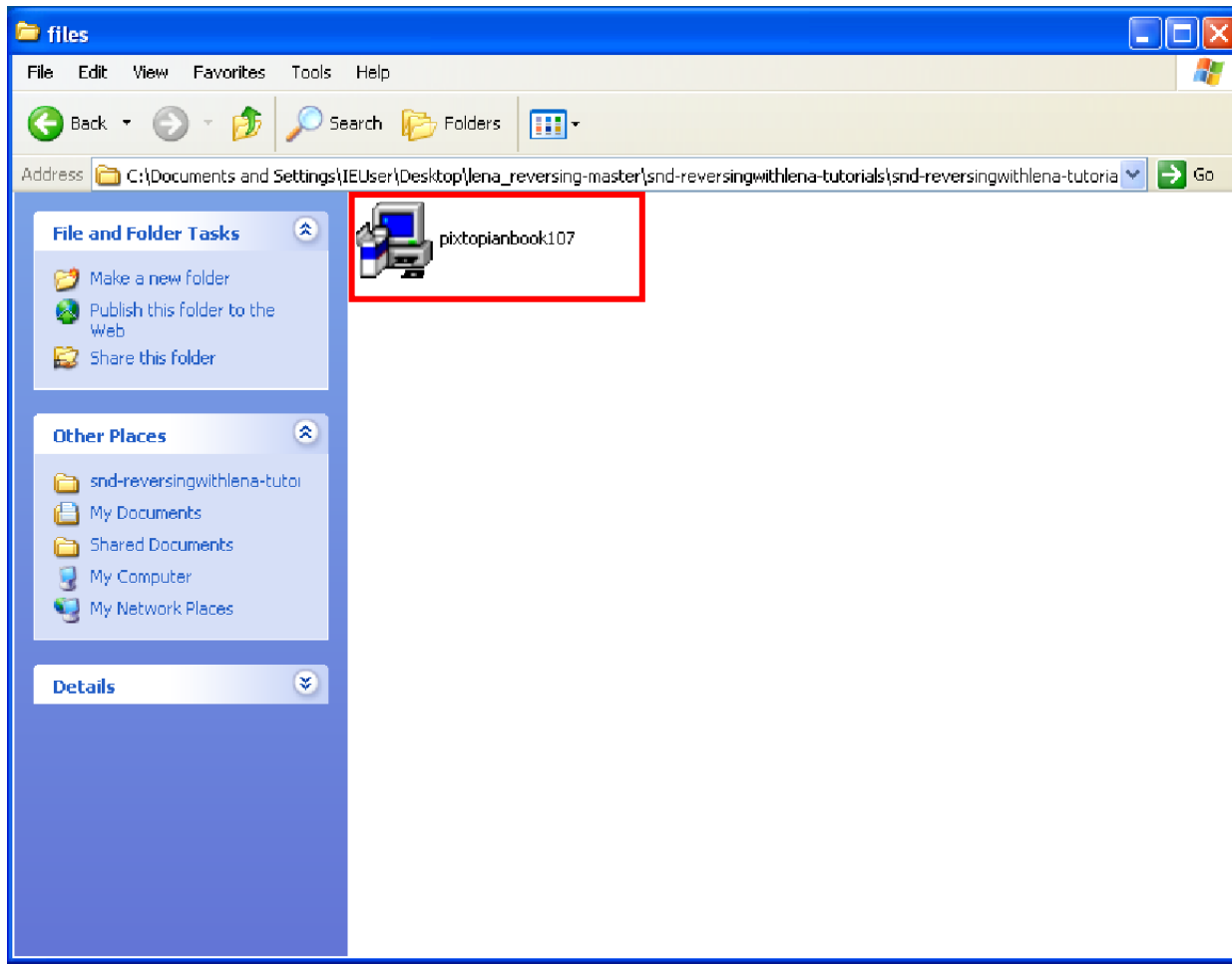
링크: <https://youtu.be/1SFIPMg0D0E>

## 실습 목적

제약사항 패치하여 체험판 프로그램 크랙하기

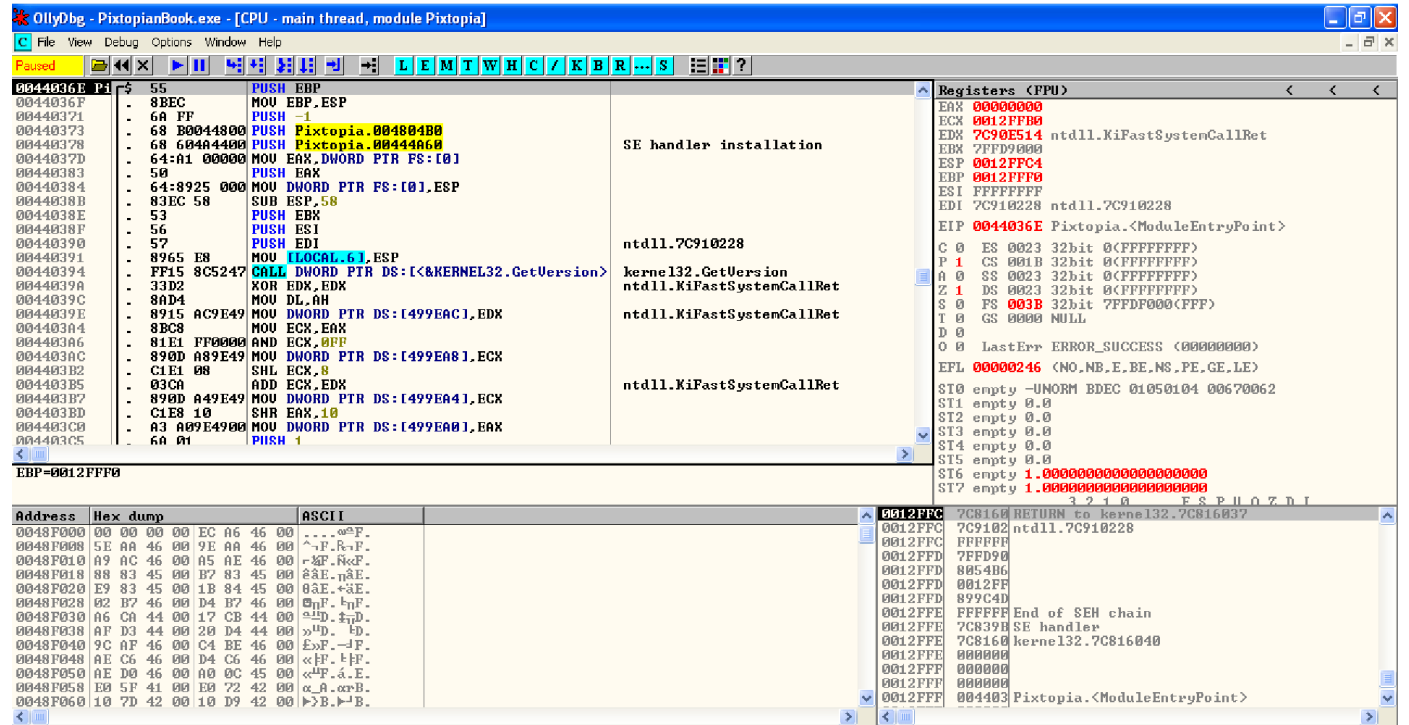
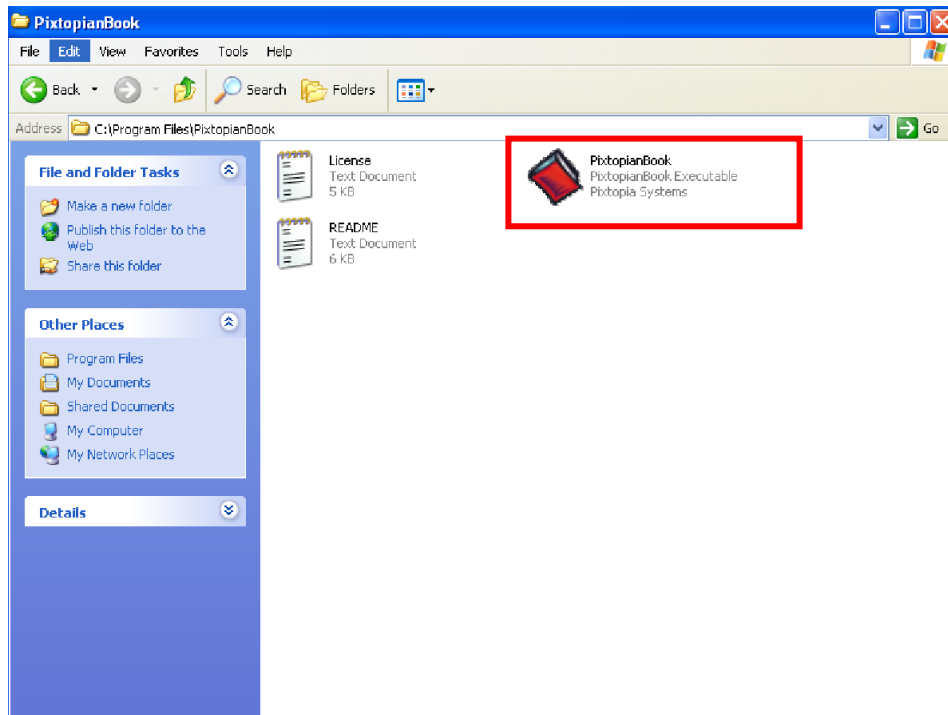
# 1. 프로그램 설치

lena\_reversing-master\snd-reversingwithlena-tutorials\snd-reversingwithlena-tutorial04.tutorial\files



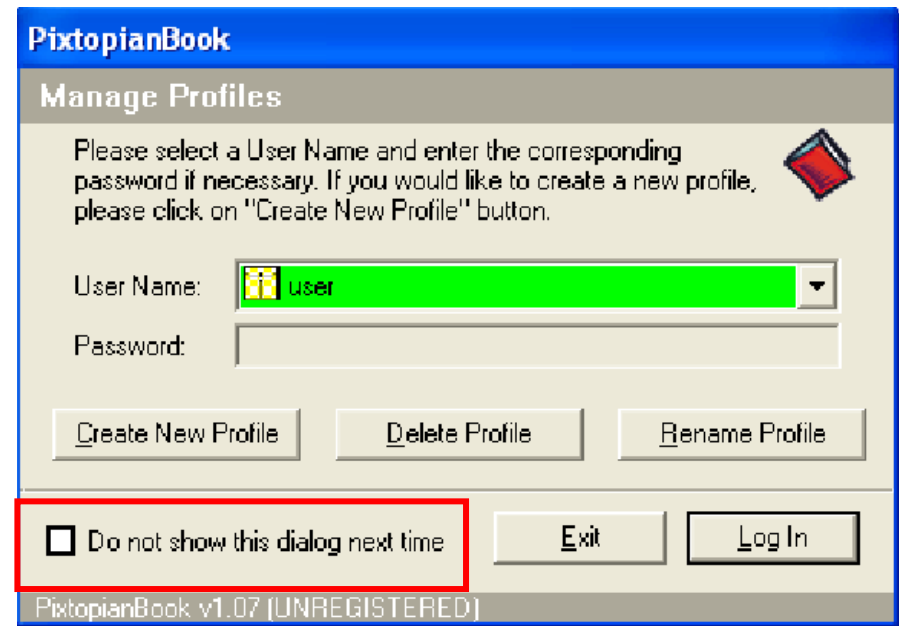
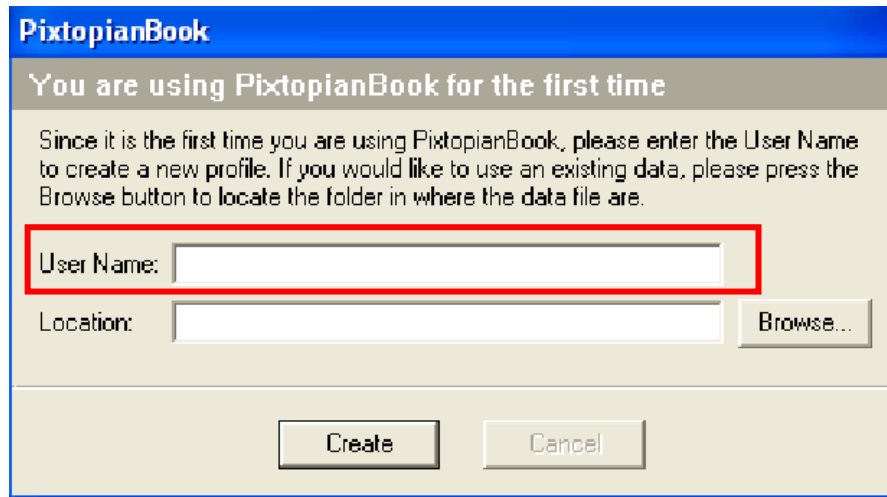
## 2. OllyDbg로 실행파일 열기

C:\Program Files\PixtopianBook



### 3. 실행

아무거나 적어도 됨



체크하면 이 창이 다시 뜨지 않음

### 3. 문제 (1) 프로그램 실행 안 됨

실행 도중 예외 처리 오류가 발생하여 실행이 안 됨

OllyDbg - PixtopianBook.exe - [CPU - main thread, module kernel32]

File View Debug Options Window Help

Paused

Registers (FPU)

EAX 0012E984  
ECX 00000000  
EDX 00980608  
EBX 00000000  
ESP 0012E980  
EBP 0012E9D4  
ESI 0012EA14  
EDI 0012EA14  
EIP 7C812FD3 kernel32.7C812FD3

C 0 ES 0023 32bit 0<FFFFFFFF>  
P 1 CS 001B 32bit 0<FFFFFFFF>  
A 0 SS 0023 32bit 0<FFFFFFFF>  
Z 0 DS 0023 32bit 0<FFFFFFFF>  
S 0 FS 003B 32bit 7FFDF000<FFF>  
T 0 GS 0000 NULL  
D 0  
O 0 LastErr ERROR\_SXS\_KEY\_NOT\_FOUND (000036B7)  
EFL 00000206 <NO.NB.NE.A.NS.PE.GE.G>

Stack [0012E980]=004804E8 (Pixtopia.004804E8)  
ESI=0012EA14

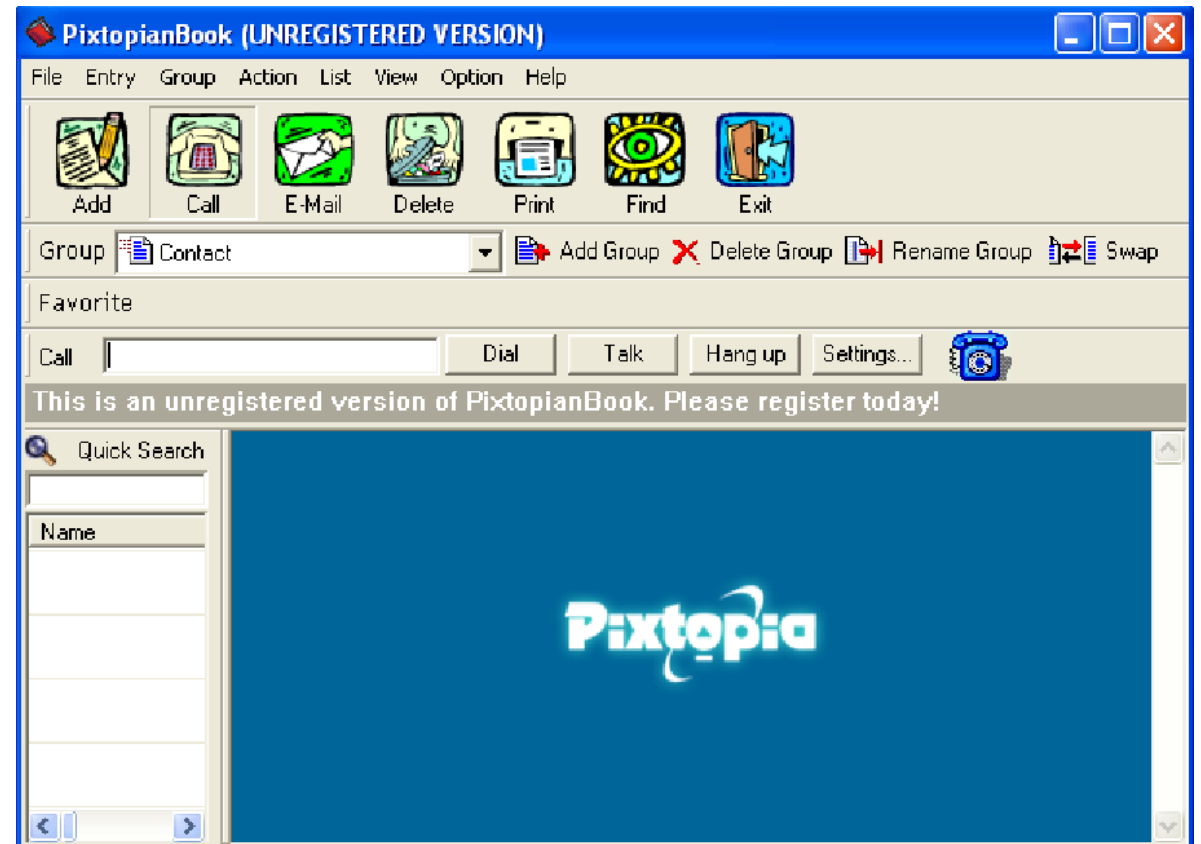
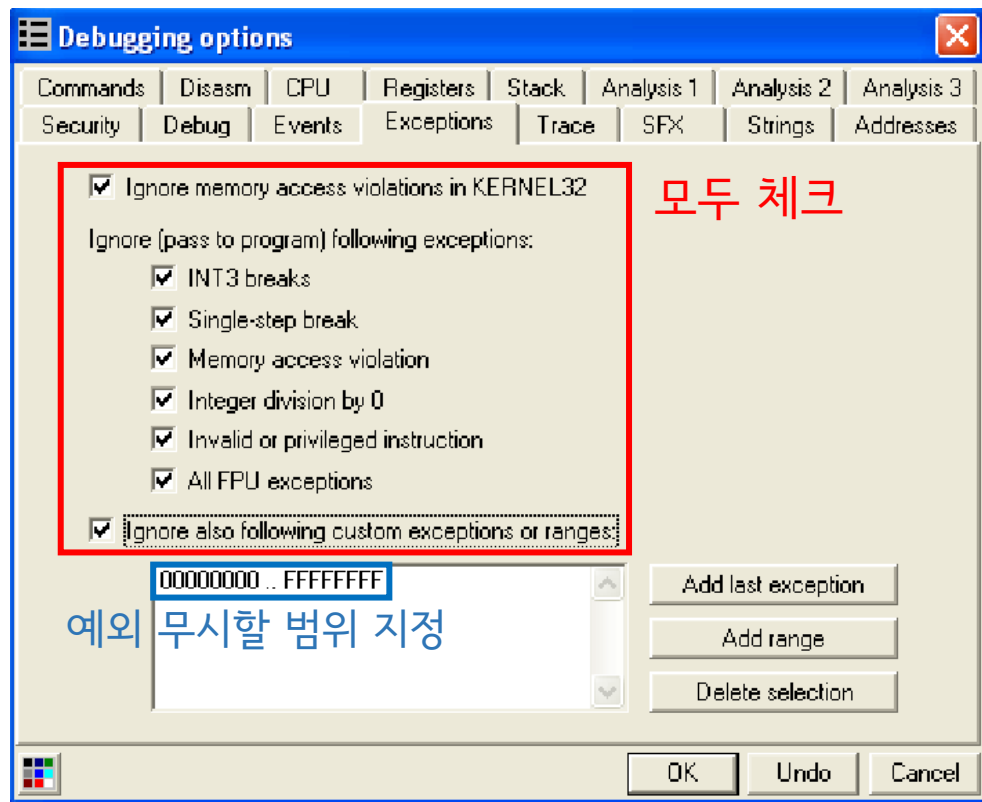
Address Hex dump ASCII

0048F000 00 00 00 00 EC A6 46 00 . . . .  
0048F008 5E AA 46 00 9E AA 46 00 ^ . F . R . F .  
0048F010 A9 AC 46 00 A5 AE 46 00 r . F . N c F .  
0048F018 88 83 45 00 B7 83 45 00 â . E . n â E .  
0048F020 E9 83 45 00 1B 84 45 00 0 â E . + â E .  
0048F028 02 B7 46 00 D4 B7 46 00 0 n F . t n F .  
0048F030 A6 CA 44 00 17 CB 44 00 a . D . \$ . i D .  
0048F038 AF D3 44 00 20 D4 44 00 > n D . t D .  
0048F040 9C AF 46 00 C4 BE 46 00 E . F . - d F .  
0048F048 AE C6 46 00 D4 C6 46 00 < [ F . t [ F .  
0048F050 AE D0 46 00 A0 0C 45 00 < n F . â . E .  
0048F058 E0 5F 41 00 E0 72 42 00 a . a . c c r B .  
0048F060 10 7D 42 00 10 D9 42 00 t > B . t > B .

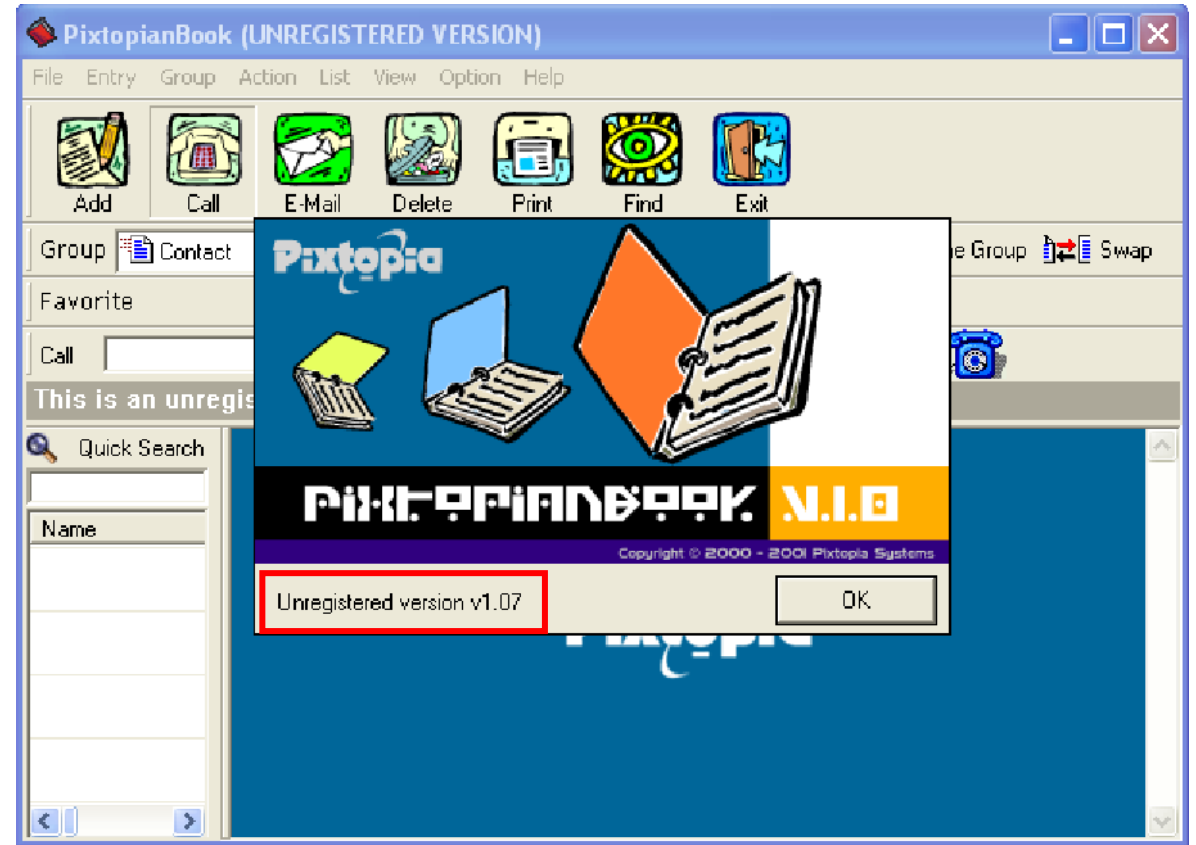
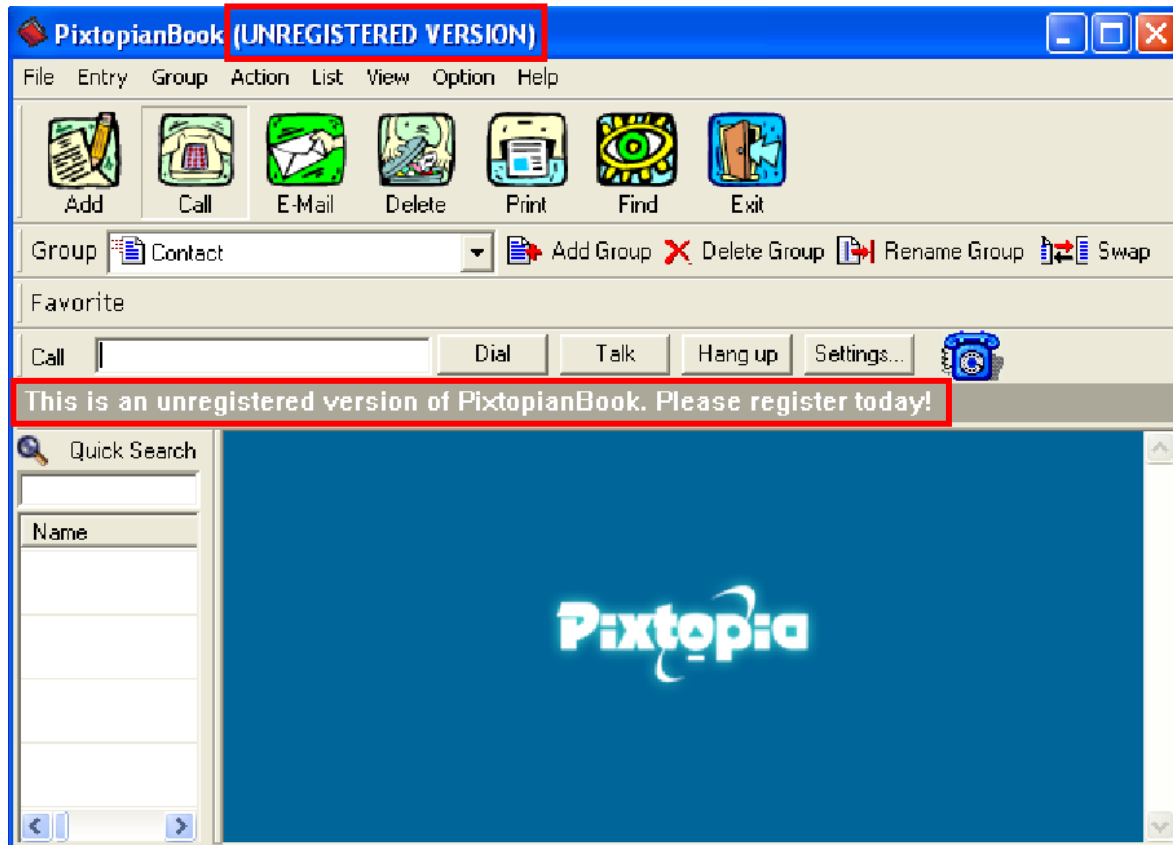
0012E98 Pixtopia.004804E8  
0012E98 E06D73  
0012E98 00000000  
0012E98 00000000  
0012E99 7C812F RETURN to kernel32.7C812FD3 from ntdll.Rtl  
0012E99 00000000  
0012E99 199305  
0012E99 0012EA  
0012E9A 0048B7 Pixtopia.0048B7B8  
0012E9A 00179C  
0012E9A 0012E9  
0012E9A 7C90E9 ntdll.7C90E920  
0012E9B 7C9101 ntdll.7C9101E0  
0012E9B FFFFFFFF

### 3. 문제 (1)의 솔루션 - 예외 처리 무시

Options > Debugging options > Exceptions



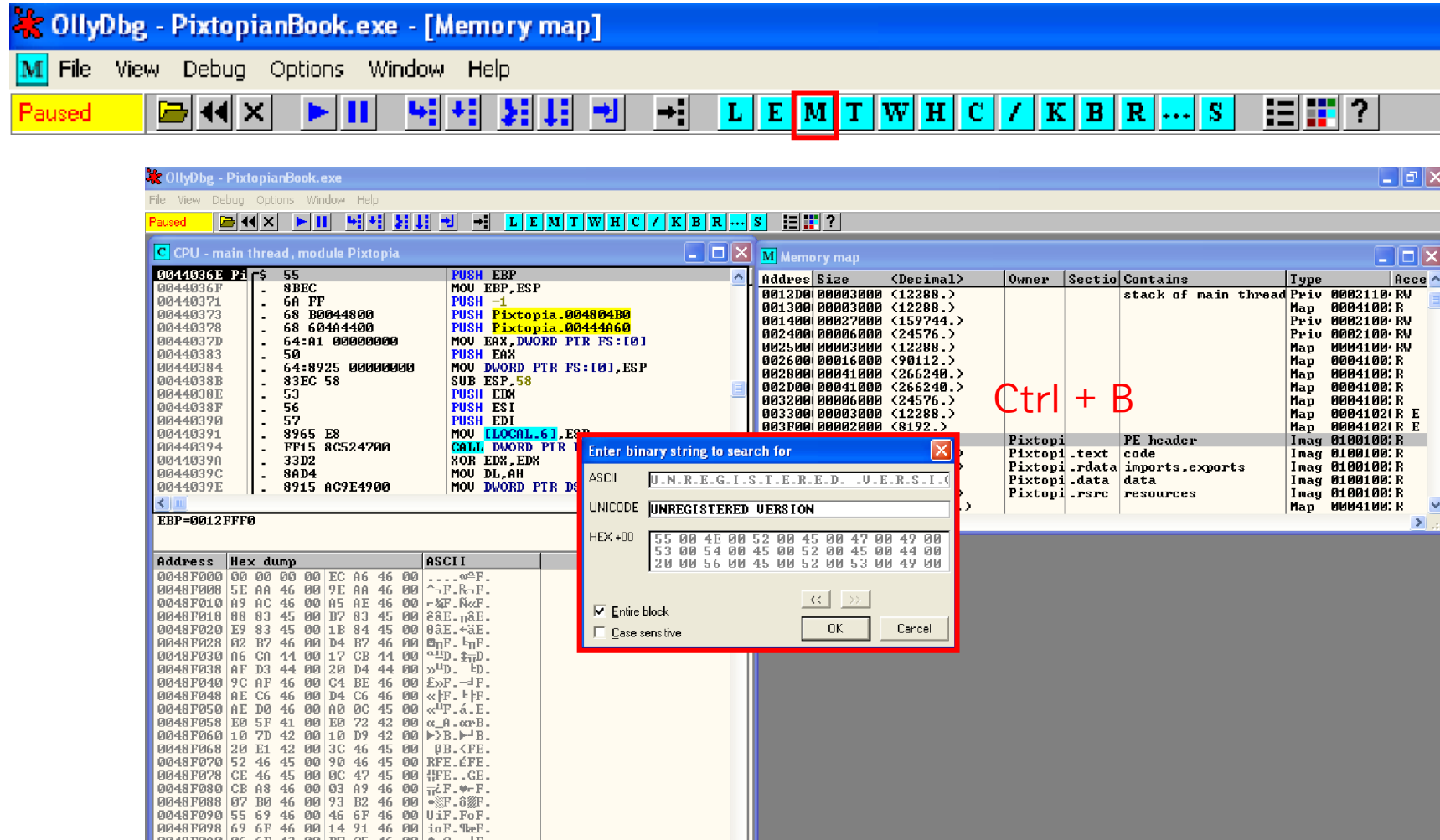
### 3. 문제 (2) Unregistered





### 3. 문제 (2)의 솔루션 - 문자열 변경

Memory map 클릭



### 3. 문제 (2)의 솔루션 - 문자열 변경

OllyDbg - PixtopianBook.exe

File View Debug Options Window Help

Paused

CPU - main thread, module Pixtopia

0044036E Pi 55 PUSH EBP  
0044036F 8BEC MOV EBP,ESP  
00440371 6A FF PUSH -1  
00440373 68 B0044800 PUSH Pixtopia.004804B0  
00440378 68 604A4400 PUSH Pixtopia.0044A60  
0044037D 64:A1 00000000 MOV EAX,DWORD PTR FS:[0]  
00440383 50 PUSH EAX  
00440384 64:8925 00000000 MOV DWORD PTR FS:[0],ESP  
0044038B 83EC 58 SUB ESP,58  
0044038E 53 PUSH EBX  
0044038F 56 PUSH ESI  
00440390 57 PUSH EDI  
00440391 8965 E8 MOV EAX,EAX  
00440394 FF15 8C524700 CALL 8C524700  
0044039A 33D2 XOR EAX,EAX  
0044039C 8AD4 MOV ECX,EDX  
0044039E 8915 AC9E4900 MOV ECX,EDX

EBP=0012FFF0

Address Hex dump ASCII  
0048F000 00 00 00 00 EC A6 46 00 .....  
0048F008 5E AA 46 00 9E AA 46 00 ^~F.R.  
0048F010 A9 AC 46 00 A5 AE 46 00 -&F.N.  
0048F018 88 83 45 00 B7 83 45 00 2&E.n.  
0048F020 E9 83 45 00 1B 84 45 00 0&E.+  
0048F028 02 B7 46 00 D4 B7 46 00 0F.F. b  
0048F030 A6 CA 44 00 17 CB 44 00 2D.D. t  
0048F038 AF D3 44 00 20 D4 44 00 >UD.  
0048F040 9C AF 46 00 C4 BE 46 00 E>F.-  
0048F048 AE C6 46 00 D4 C6 46 00 <<F. bF.  
0048F050 AE D0 46 00 A0 0C 45 00 <<F.á.E.  
0048F058 E0 5F 41 00 E0 72 42 00 α.A.αrB.  
0048F060 10 7D 42 00 10 D9 42 00 >>B.~B.  
0048F068 20 E1 42 00 3C 46 45 00 0B.<FE.  
0048F070 52 46 45 00 90 46 45 00 RFE.éFE.  
0048F078 CE 46 45 00 0C 47 45 00 tFE..GE.  
0048F080 CB A8 46 00 03 A9 46 00 r&F.~F.  
0048F088 07 B0 46 00 93 B2 46 00 \*F.âF.  
0048F090 55 69 46 00 46 6F 46 00 U iF.FoF.  
0048F098 69 6F 46 00 14 91 46 00 ioF.~F.  
0048F0A0 06 6F 43 00 B7 C5 46 00 \*nC. n+F.

Memory map

Address	Size	(Decimal)	Owner	Section	Contains	Type	Access
0012D0	00003000	<12288.>			stack of main thread	Priv	0002110: RW
001300	00003000	<12288.>				Map	0004100: R
001400	00027000	<159744.>				Priv	0002100: RW
002400	00006000	<24576.>				Priv	0002100: RW
002500	00003000	<12288.>				Map	0004100: RW
002600	00016000	<90112.>				Map	0004100: R
002800	00041000	<266240.>				Map	0004100: R
002D00	00041000	<266240.>				Map	0004100: R

Dump - Pixtopia: .rsrc 0049D000..004E8FFF

Address	Hex dump	ASCII
004D4830	55 00 6E 00 72 00 65 00 67 00 69 00 73 00 74 00	U.n.r.e.g.i.s.t.
004D4840	65 00 72 00 65 00 64 00 20 00 76 00 65 00 72 00	e.r.e.d..v.e.r.
004D4850	73 00 69 00 6F 00 6E 00 20 00 76 00 31 00 2E 00	s.i.o.n..v.i...
004D4860	30 00 37 00 00 00 00 00 01 00 FF FF 00 00 00 00	0.7.....@.
004D4870	00 00 00 00 40 00 00 00 40 04 00 00 00 00 41 00	....@+....A.
004D4880	48 00 00 00 00 00 00 00 08 00 00 00 00 01 4D 00	H.....CM.
004D4890	53 00 20 00 53 00 61 00 6E 00 73 00 20 00 53 00	S..S.a.n.s..S.
004D48A0	65 00 72 00 69 00 66 00 00 00 00 00 00 00 00 00	e.r.i.f.....
004D48B0	00 00 00 00 00 02 02 50 10 00 02 00 31 00 08 00	.....00P..0.1.
004D48C0	EE 03 00 00 FF FF 82 00 20 00 51 00 75 00 69 00	E.. é..Q.u.i.
004D48D0	63 00 60 00 20 00 53 00 65 00 61 00 72 00 63 00	c.k..S.e.a.r.c.
004D48E0	68 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00	h.....@.
004D48F0	80 00 81 50 00 00 0C 00 3B 00 0C 00 E9 03 00 00	Ç.üP.....0v..
004D4900	FF FF 81 00 00 00 00 00 00 00 00 00 00 02 00 00	ü.....@.
004D4910	1D 00 01 50 00 00 19 00 3C 00 2F 00 EC 03 00 00	+.@P..1.<./..w..
004D4920	53 00 79 00 73 00 4C 00 69 00 73 00 74 00 56 00	S.y.s.L.i.s.t.U.
004D4930	69 00 65 00 77 00 33 00 32 00 00 00 4C 00 69 00	i.e.w.3.2...L.i.
004D4940	73 00 74 00 31 00 00 00 00 00 00 00 00 00 00 00	s.t.1.....
004D4950	00 00 00 00 03 08 00 50 00 00 01 00 14 00 14 00	....P..@.q.q.
004D4960	FF FF FF FF FF FF 82 00 FF FF E7 00 00 00 00 00	é. r.....

검색결과

PE header  
code  
imports, exports  
data  
resources

### 3. 문제 (2)의 솔루션 - 문자열 변경

Paused

CPU - main thread, module Pixtopia

Memory map

Enter expression to follow in Dump

004D4830

Ctrl + G

Dump - Pixtopia:.rsrc 0049D000..004EBFFF

004D4830 55 00 6E 00 72 00 65 00 67 00 69 00 73 00 74 00 U.n.r.e.g.i.s.t.  
004D4840 65 00 72 00 65 00 64 00 20 00 76 00 65 00 72 00 e.r.e.d. v.e.r.  
004D4850 73 00 69 00 6F 00 6E 00 20 00 76 00 31 00 2E 00 s.i.o.n. v.i...  
004D4860 30 00 37 00 00 00 00 00 01 00 FF FF 00 00 00 00 0.7.....@.  
004D4870 00 00 00 00 40 00 00 00 04 00 00 00 00 41 00 ....@...+.....A.  
004D4880 48 00 00 00 00 00 00 00 00 00 00 00 01 4D 00 H.....@.....@M.  
004D4890 53 00 20 00 53 00 61 00 6E 00 73 00 20 00 53 00 S. .S.a.n.s. .S.  
004D48A0 65 00 72 00 69 00 66 00 00 00 00 00 00 00 00 00 e.r.i.f.....  
004D48B0 00 00 00 00 02 02 50 10 00 02 00 31 00 08 00 .....@P>..@.1.□  
004D48C0 EE 03 00 00 FF FF 82 00 20 00 51 00 75 00 69 00 €... é. .Q.u.i.  
004D48D0 63 00 6B 00 20 00 53 00 65 00 61 00 72 00 63 00 c.k. .S.e.a.r.c.  
004D48E0 68 00 00 00 00 00 00 00 00 00 00 00 02 00 h.....@.....@.  
004D48F0 80 00 81 50 00 00 0C 00 3B 00 0C 00 E9 03 00 00 Ç.üP.....;...@v..  
004D4900 FF FF 81 00 00 00 00 00 00 00 00 00 02 00 00 ü.....@.....@.  
004D4910 1D 00 01 50 00 00 19 00 3C 00 2F 00 EC 03 00 00 +.GP.↓.<./..@v..  
004D4920 53 00 79 00 73 00 4C 00 69 00 73 00 74 00 56 00 S.y.s.L.i.s.t.U.  
004D4930 69 00 65 00 77 00 33 00 32 00 00 00 4C 00 69 00 i.e.w.3.2...L.i.  
004D4940 73 00 74 00 31 00 00 00 00 00 00 00 00 00 00 s.t.1.....@.....@.  
004D4950 00 00 00 00 03 08 00 50 00 00 01 00 14 00 14 00 .....@P..@.q.¶.  
004D4960 FF FF FF FF FF FF 82 00 FF FF E7 00 00 00 00 00 é. .r.....

### 3. 문제 (2)의 솔루션 - 문자열 변경

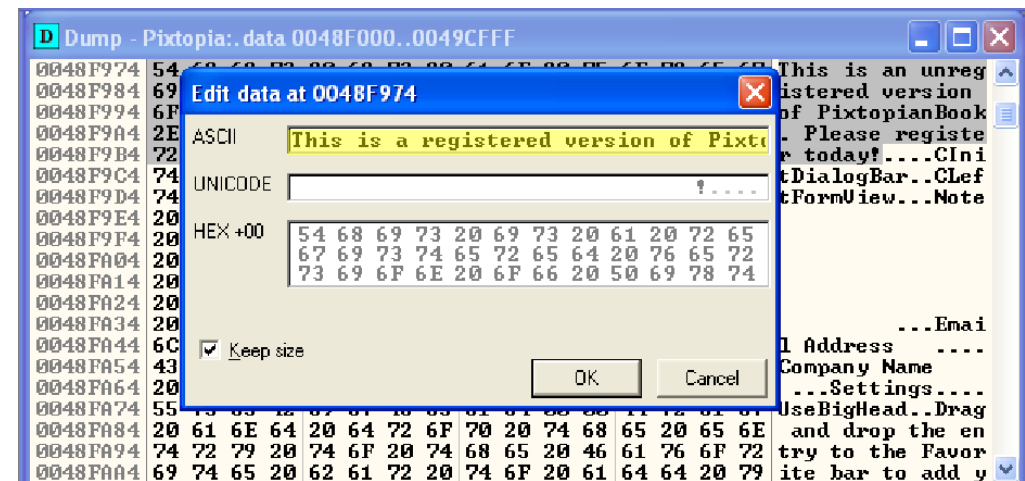
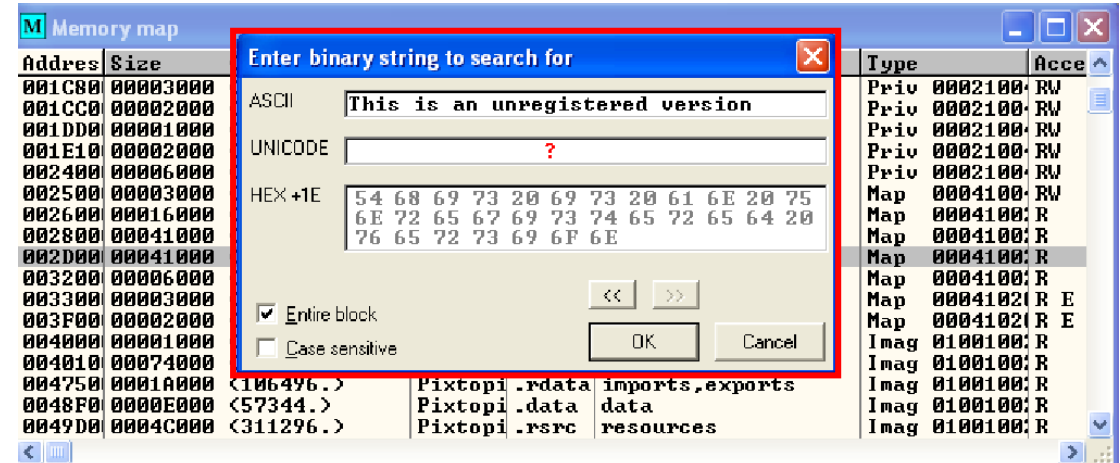
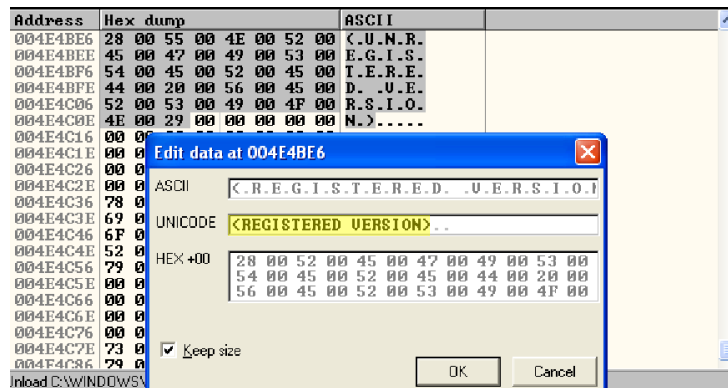
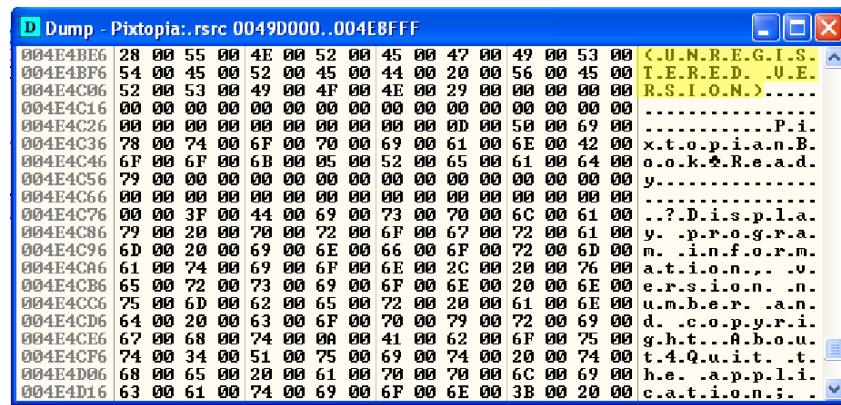
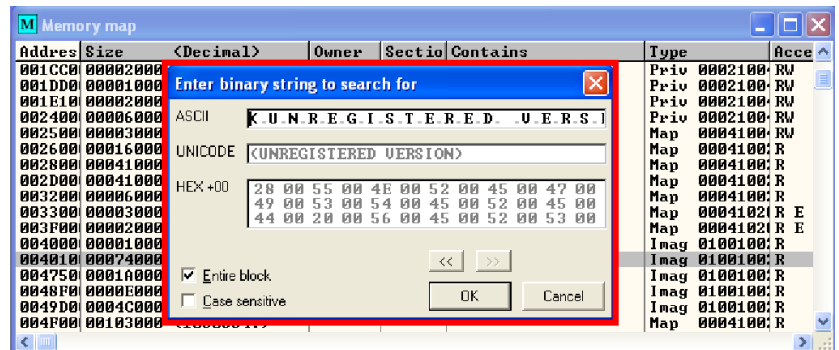
The screenshot shows the OllyDbg interface with the following components:

- Disassembly:** Shows assembly instructions for the main thread of Pixtopia.exe. The instruction at address 00440394 is highlighted: `CALL DWORD PTR [LOCAL.6], EBP`.
- Memory map:** Displays the memory layout of the module, including sections like .text, .rdata, .data, and .rsrc.
- Memory dump:** Shows the hex dump and ASCII representation of the memory at address 004D4830. The ASCII string is "Registered version v1.07".
- Edit data dialog:** A dialog box titled "Edit data at 004D4830" is open, showing the ASCII string "Registered version v1.07" and the hex dump. The "Keep size" checkbox is checked.

The memory dump shows the following data:

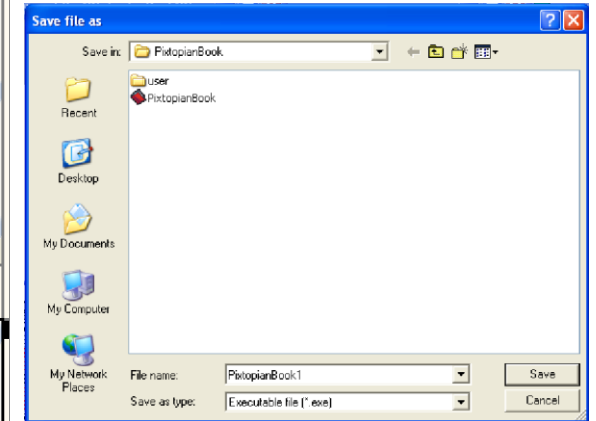
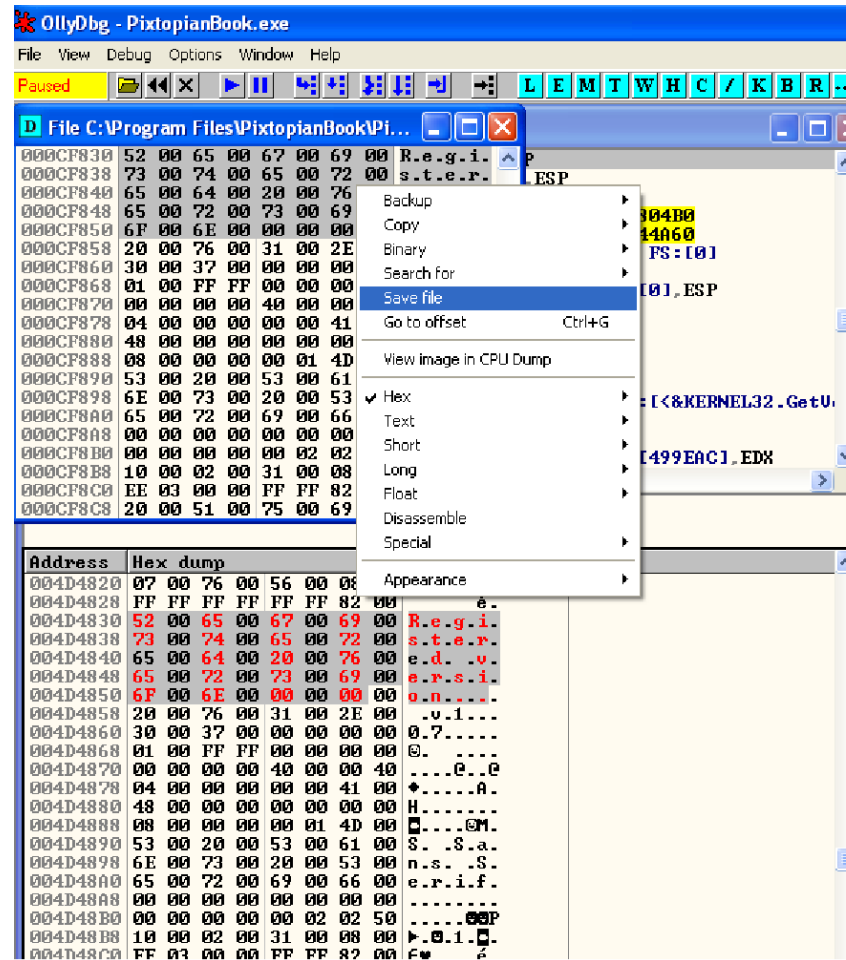
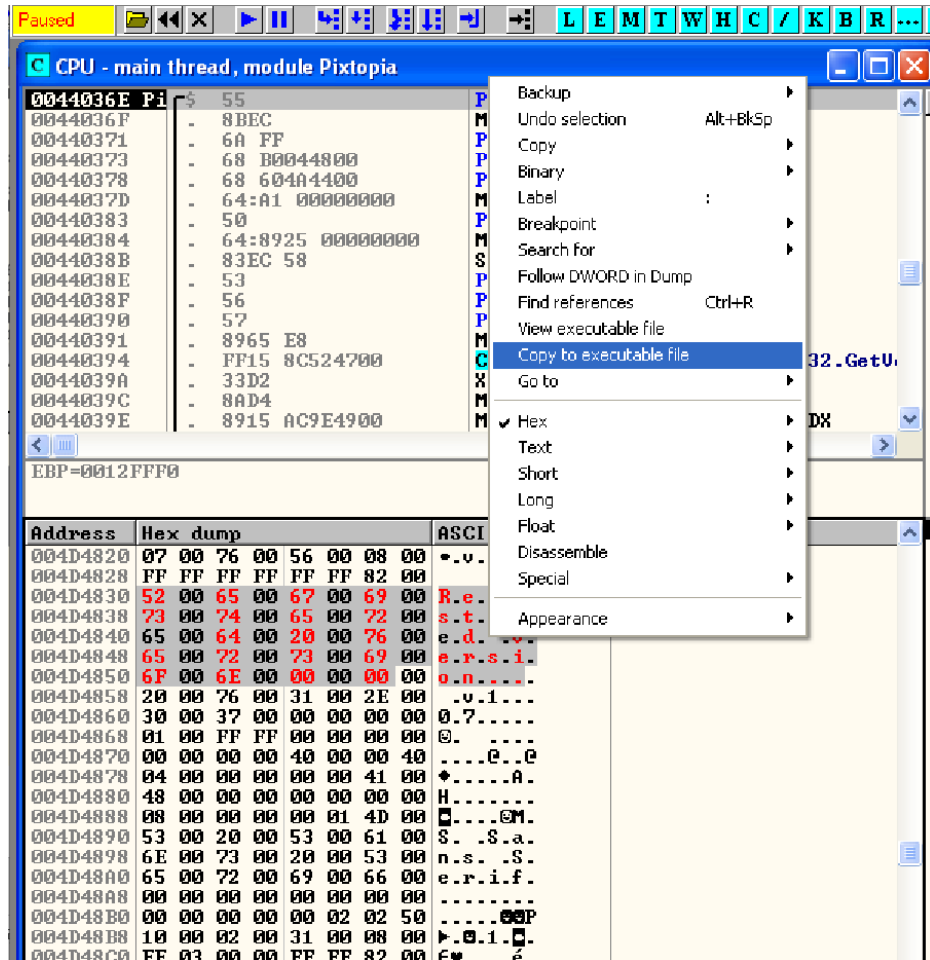
Address	Hex dump	ASCII
004D4830	55 00 6E 00 72 00 65 00	U.n.r.e.
004D4838	67 00 69 00 73 00 74 00	g.i.s.t.
004D4840	65 00 72 00 65 00 64 00	e.r.e.d.
004D4848	20 00 76 00 65 00 72 00	.v.e.r.
004D4850	73 00 69 00 6F 00 6E 00	s.i.o.n.
004D4858	20 00 76 00 31 00 2E 00	.v.i...
004D4860	30 00 37 00 00 00 00 00	0.7....
004D4868	01 00 FF FF 00 00 00 00	@.....
004D4870	00 00 00 00 40 00 00 40	....e..e
004D4878	04 00 00 00 00 00 41 00	.....A.
004D4880	48 00 00 00 00 00 00 00	H.....
004D4888	08 00 00 00 00 01 4D 00	.....CM.
004D4890	53 00 20 00 53 00 61 00	S...S.a.
004D4898	6E 00 73 00 20 00 53 00	n.s...S.
004D48A0	65 00 72 00 69 00 66 00	e.r.i.f.
004D48A8	00 00 00 00 00 00 00 00	.....
004D48B0	00 00 00 00 00 02 02 50	.....ESP
004D48B8	10 00 02 00 31 00 08 00	.....i..
004D48C0	EE 03 00 00 FF FF 82 00	.....é.
004D48C8	20 00 51 00 75 00 69 00	.....Q.u.i.
004D48D0	63 00 6B 00 70 00 53 00	.....c.k.

### 3. 문제 (2)의 솔루션 - 문자열 변경



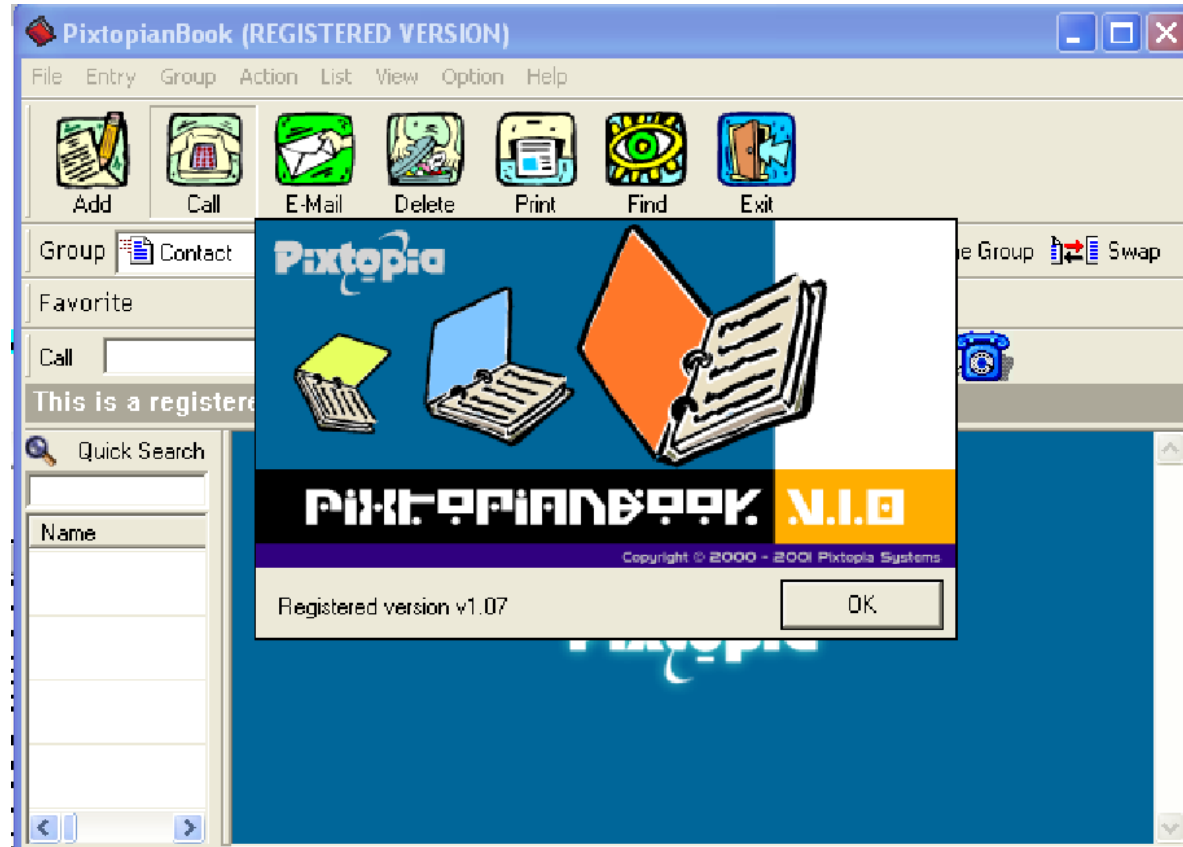


### 3. 문제 (2)의 솔루션 - 문자열 변경



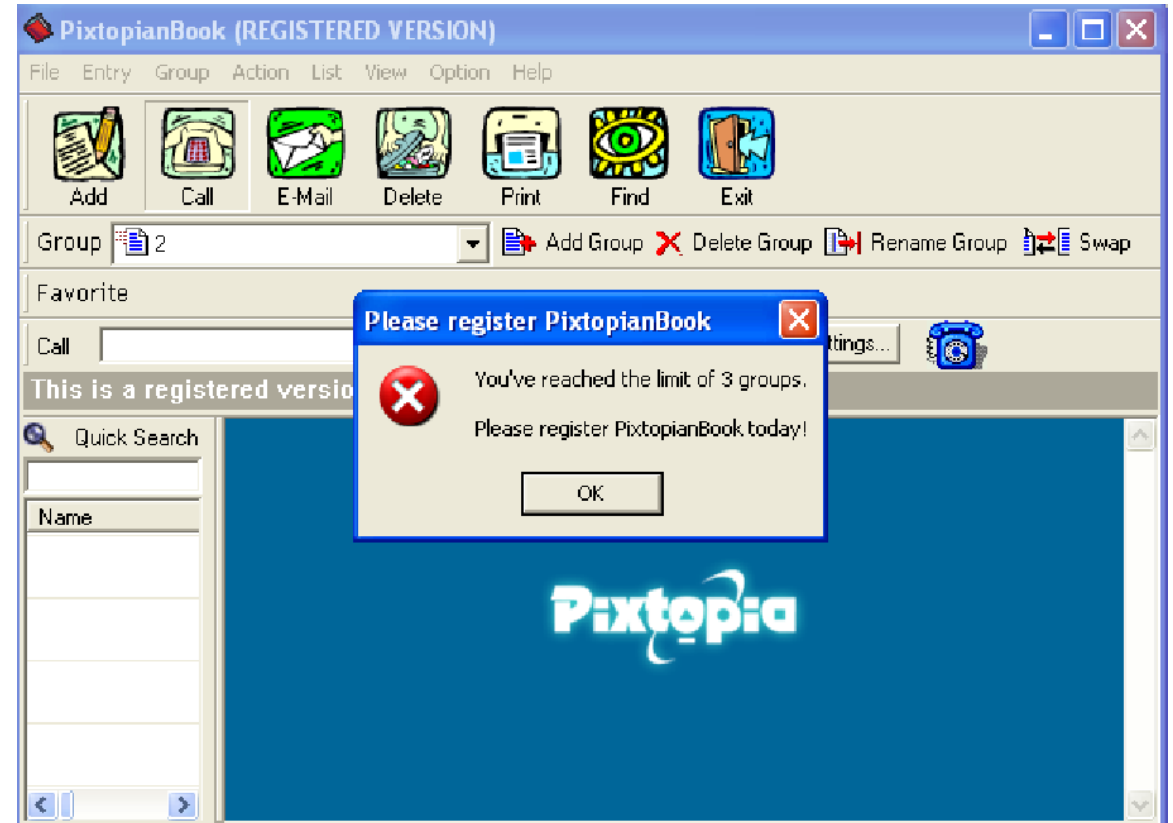
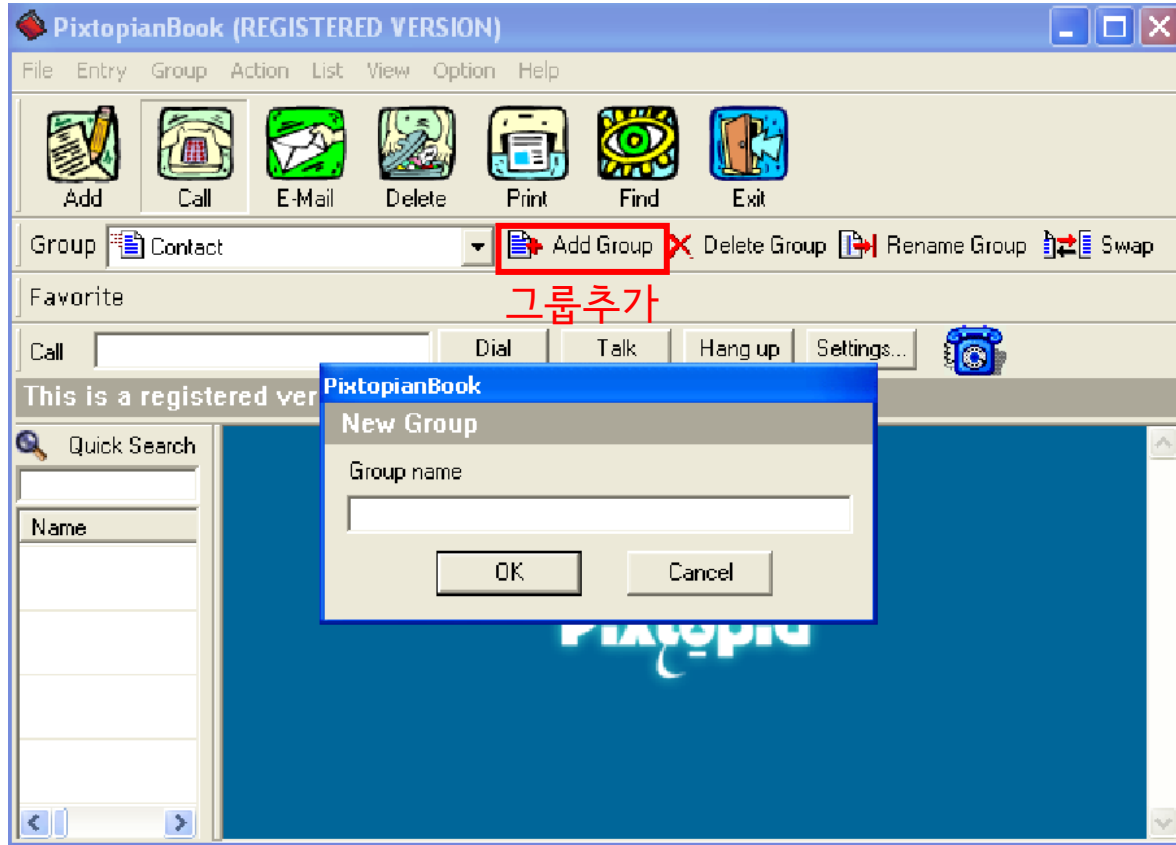
PixtopianBook1로 저장

### 3. 문제 (2)의 솔루션 - 문자열 변경 (결과)



### 3. 문제 (3) 그룹 생성 제한

최대 3개까지만 그룹 생성 가능





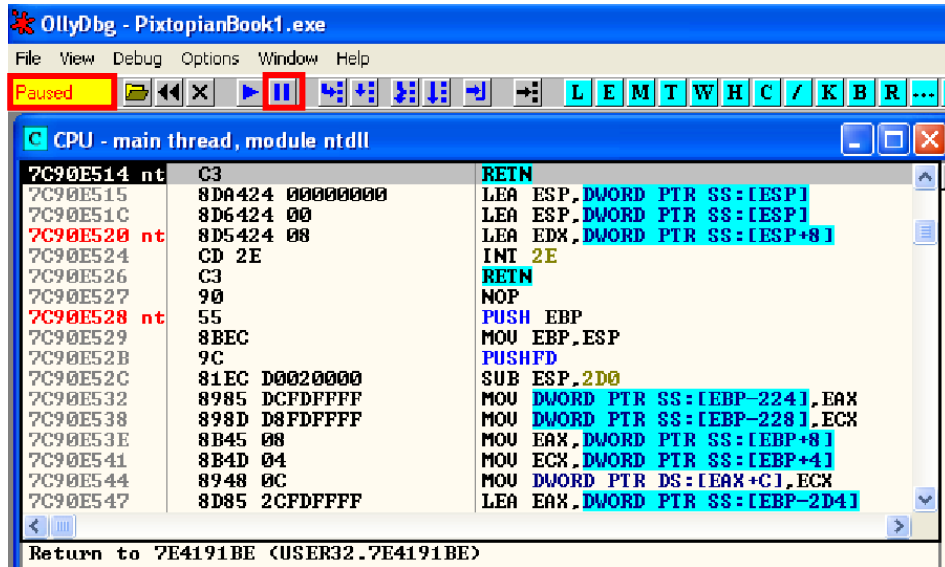
### 3. 문제 (3)의 솔루션 - 우회 (Back to user mode 이용)

## Back to user mode

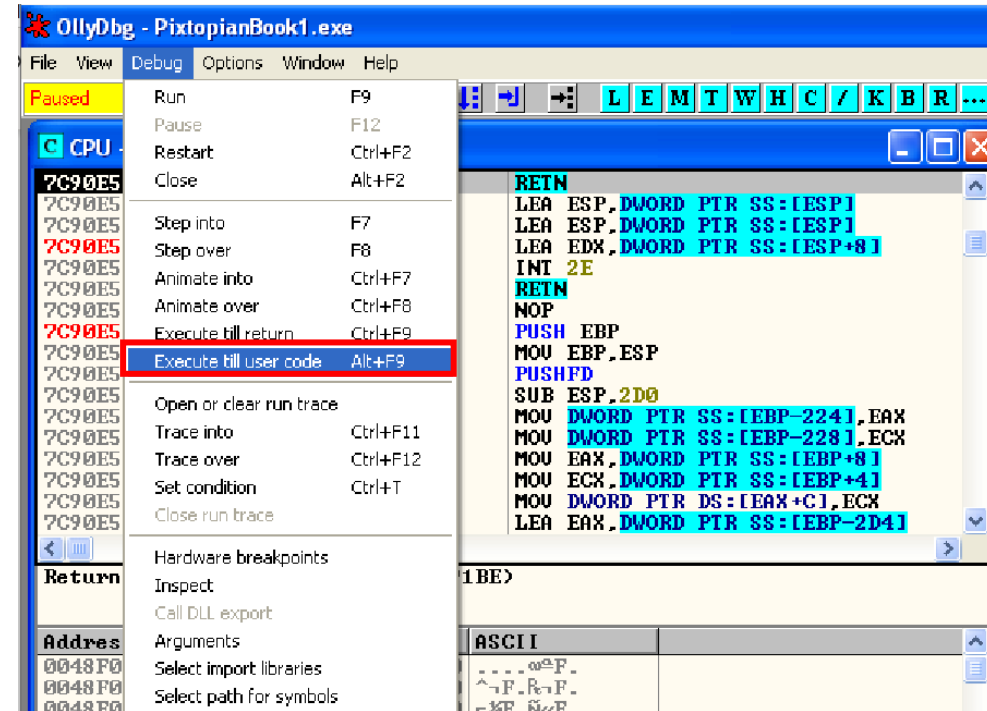
- 특정 이벤트를 발생하기 전에 설정해두고 call 명령이 일어난 바로 다음 주소로 이동해주는 모드
- call 명령이 일어난 바로 다음의 위치를 잡을 수 있음. (함수 호출부를 찾는데 유용함)

### 3. 문제 (3)의 솔루션 - 우회 (Back to user mode 이용)

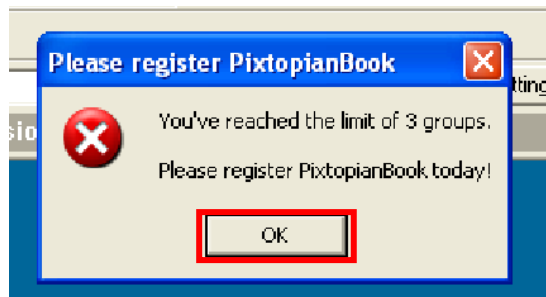
#### 1. 실행중지



#### 2. Debug > Execute till user code



#### 3. 확인 버튼 누르기



### 3. 문제 (3)의 솔루션 - 우회 (MessageBoxA)

The screenshot shows a debugger window with the following assembly code and comments:

Address	Disassembly	Comment
004562E5	MOV ECX, EAX	
004562E7	JMP SHORT Pixtopia.004562DA	
004562E9	MOV EAX, ESI	
004562EB	POP ESI	Pixtopia.004761E8
004562EC	RETN	
004562ED	MOV EAX, DWORD PTR SS:[ESP+8]	Pixtopia.0048F6B4
004562F1	PUSH ESI	
004562F2	TEST EAX, EAX	
004562F4	MOV ESI, ECX	ntdll.7C91005D
004562F6	JNZ SHORT Pixtopia.00456300	
004562F8	CALL Pixtopia.0046AEC6	
004562FD	MOV EAX, DWORD PTR DS:[EAX+10]	
00456300	TEST ESI, ESI	
00456302	JNZ SHORT Pixtopia.00456308	
00456304	XOR ECX, ECX	ntdll.7C91005D
00456306	JMP SHORT Pixtopia.0045630B	
00456308	MOV ECX, DWORD PTR DS:[ESI+1C]	
0045630B	PUSH DWORD PTR SS:[ESP+10]	
0045630F	PUSH EAX	
00456310	PUSH DWORD PTR SS:[ESP+10]	
00456314	PUSH ECX	
00456315	CALL DWORD PTR DS:[<USER32.MessageBoxA>]	[Style = MB_OK;MB_ICONHAND;MB_APPLMODAL Title = 00000001 ??? Text = 00000010 ??? hOwner = 7C91005D MessageBoxA Pixtopia.004761E8]
0045631B	POP ESI	
0045631C	RETN 0C	
0045631F	PUSH EBP	
00456320	MOV ERP, ESP	

메시지 박스(시스템) 호출

(Windows System API) user32.dll / kernel32.dll

### 3. 문제 (3)의 솔루션 - 우회 (SendMessageA)

Group Contact Add Group Delete Group Rename Group Swap

Paused

```
00408ADE - 64:8925 00000000 MOV DWORD PTR FS:[0],ESP
00408AE5 - 81EC 34010000 SUB ESP,134
00408AEB - 53 PUSH EBX
00408AEC - 8BD9 MOV EBX,ECX
00408AEE - 56 PUSH ESI
00408AEF - 6A 00 PUSH 0
00408AF1 - 8B83 A4000000 MOV EAX,DWORD PTR DS:[EBX+4]
00408AF7 - 6A 00 PUSH 0
00408AF9 - 68 46010000 PUSH 146
00408AFE - 50 PUSH EAX
00408AFF - FF15 D0564700 CALL DWORD PTR DS:[470056D0],SendMessage0
00408B05 - 83F8 03 CMP EAX,3
00408B08 - 7C 2A 30 JLT SHORT Pixtopia.00408B34
00408B0A - 6A 10 PUSH 10
00408B0C - 68 00F74800 PUSH Pixtopia.0048F700
00408B11 - 68 B4F64800 PUSH Pixtopia.0048F6B4
00408B16 - 8BCB MOV ECX,EBX
00408B18 - E8 D0D70400 CALL Pixtopia.004562ED
00408B1D - 5E POP ESI
00408B1E - 5B POP EBX
00408B1F - 8B8C24 34010000 MOV ECX,DWORD PTR SS:[ESP+134]
00408B26 - 64:890D 00000000 MOV DWORD PTR FS:[0],ECX
00408B2D - 81C4 40010000 ADD ESP,140
00408B33 - C3 RETN
00408B34 - 6A 00 PUSH 0
00408B36 - 8D4C24 24 LEA ECX,DWORD PTR SS:[ESP+24]
```

메시지 창으로 메시지 보내기

ESI에 축박지 주소 저장

콤보 상자의 목록 상자에 있는 항목 수를 가져오는 함수

SendMessageA

hWnd 메시지 수신할 창의 핸들번호

Message 보낼 메시지

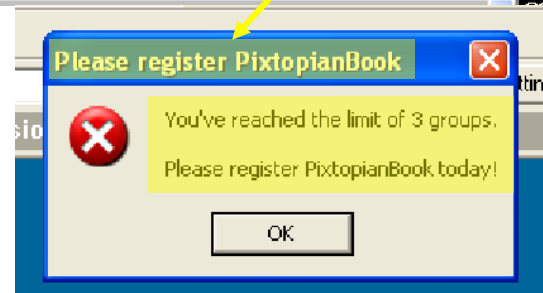
wParam 추가 메시지 관련 정보

lParam 반환값: 메시지 처리 결과

함수 반환 결과(EAX)

3이상이면 점프X

Stack [0012F790]=004761E8 (Pixtopia.004761E8), ASCII "piG"  
ESI=004761E8 (Pixtopia.004761E8), ASCII "piG"



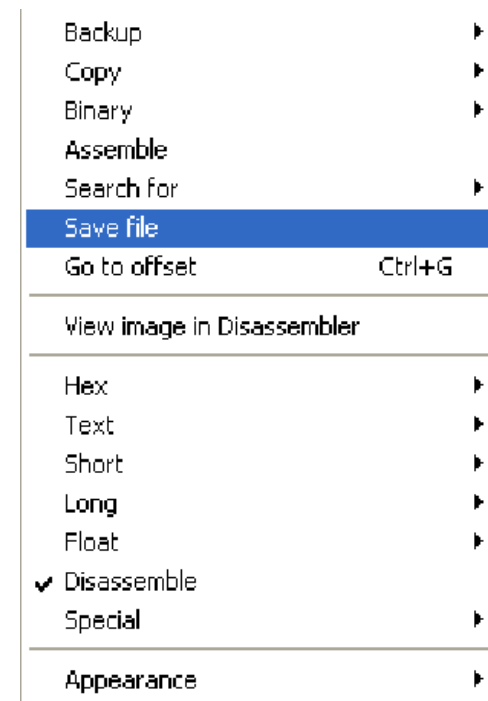
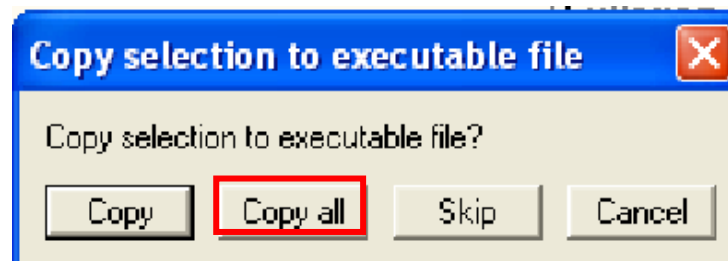
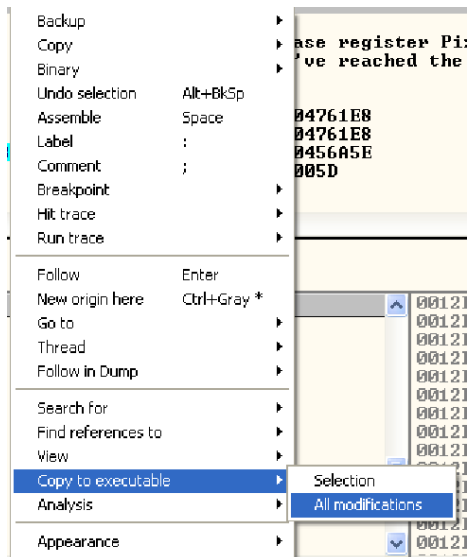
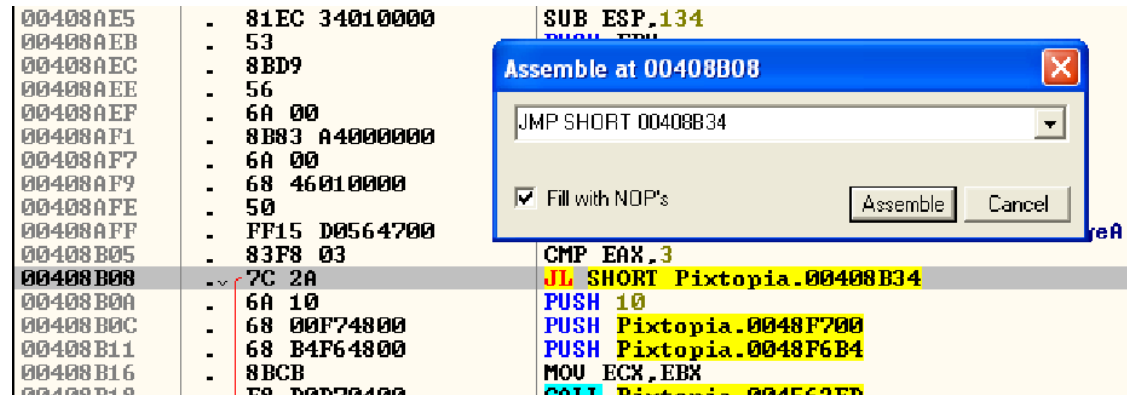
### 3. 문제 (3)의 솔루션 - 우회 (명령어 수정)

00408AFF	. FF15 D0564700	CALL DWORD PTR DS:[&USER32.SendMessageA]
00408B05	. 83F8 03	CMP EAX,3
00408B08	. 7C 2A	JL SHORT Pixtopia.00408B34

방법1) CMP 명령어의 두번째 operand를 3보다 더 큰 숫자로 변경 → 임시적인 방법

방법2) 분기하지 않도록 JL 명령어를 JMP 명령어로 변경 → 영구적인 방법 (숫자와 관계 없어짐)

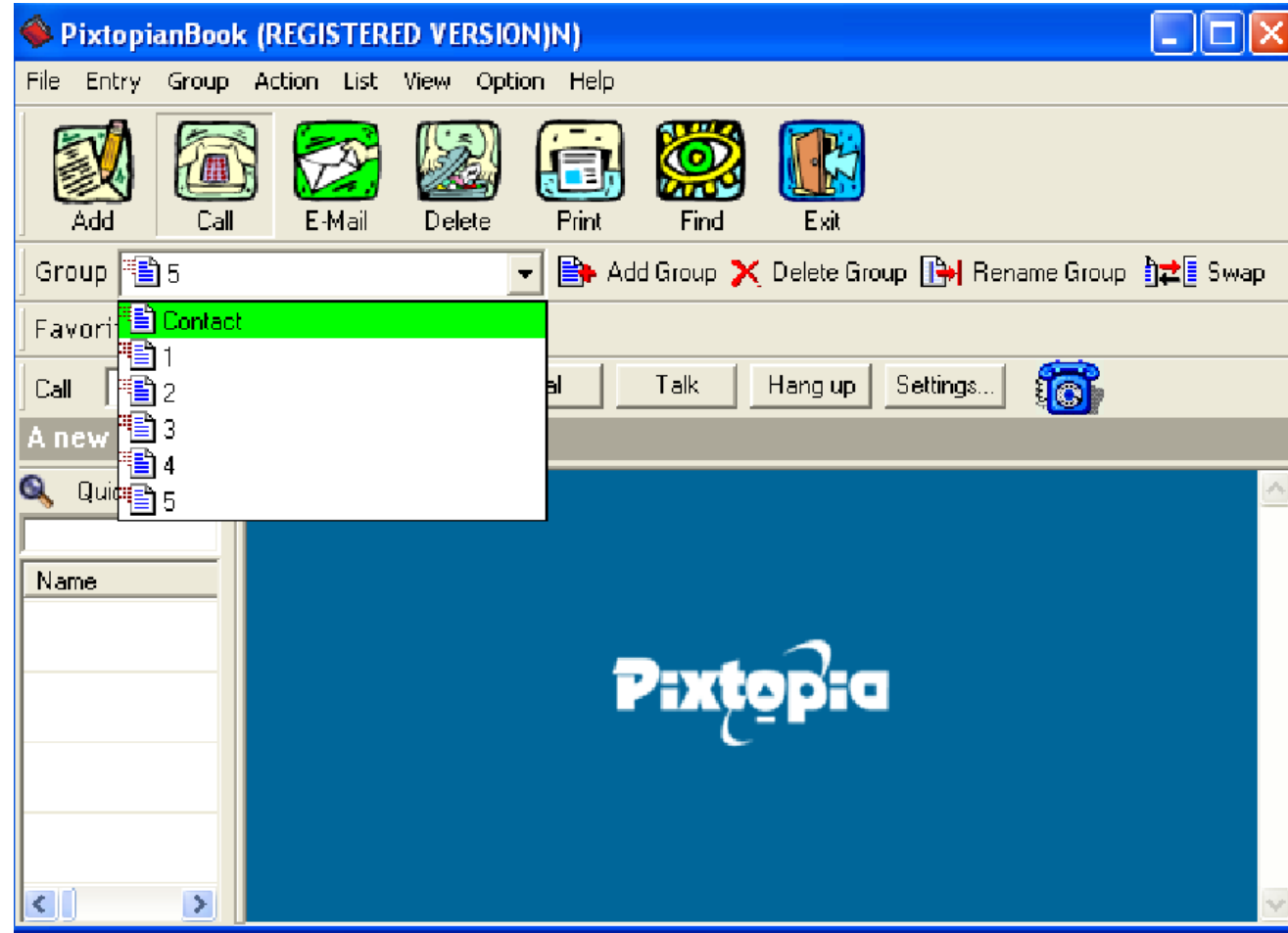
### 3. 문제 (3)의 솔루션 - 우회 (변경부분 저장)



PixtopianBook2로 저장

### 3. 문제 (3)의 솔루션 - 우회 (결과)

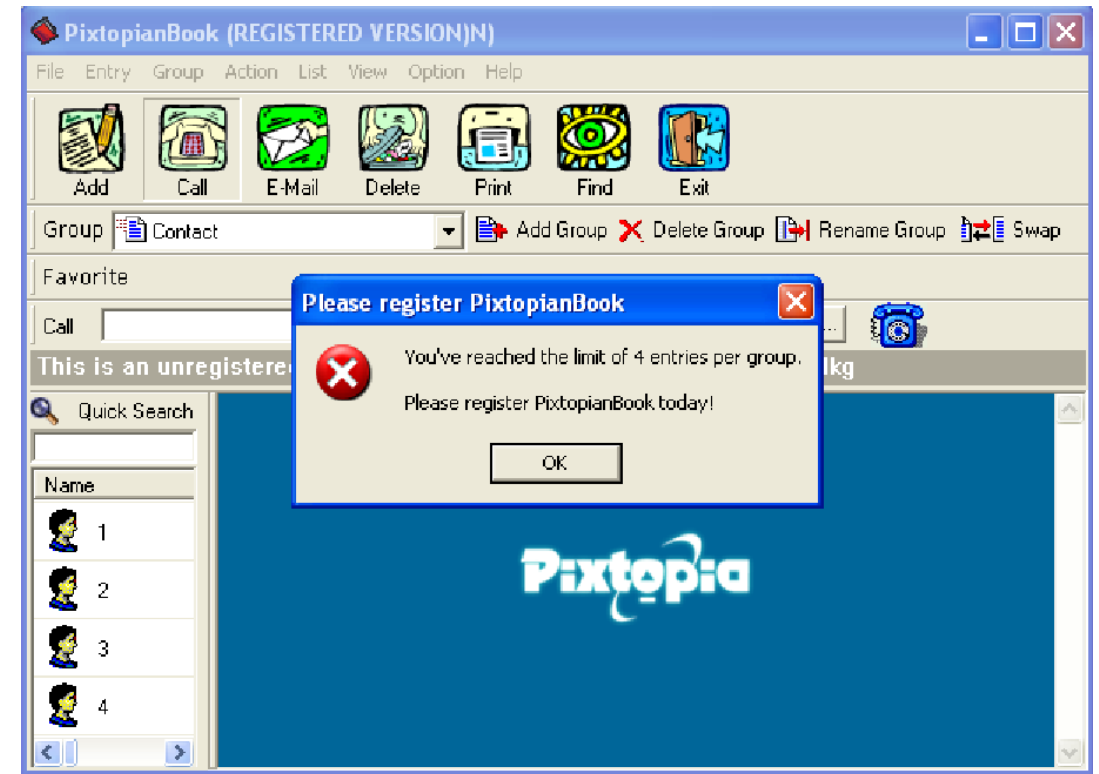
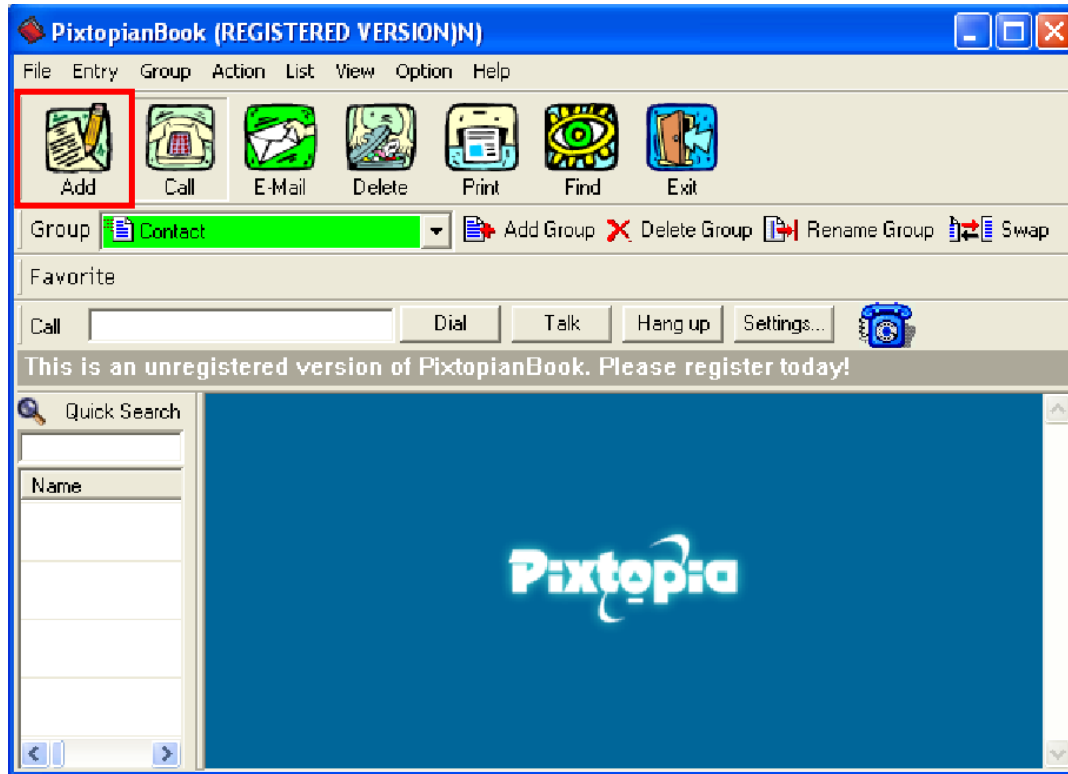
4개 이상 추가 가능해짐



### 3. 문제 (4) 등록 인원수 제한

최대 4명까지만 사용자 추가 가능

사용자 추가





### 3. 문제 (4)의 솔루션 - 우회 (Back to user mode 이용)

```
Paused
004562E9 > 8BC6 MOV EAX,ESI
004562EB - 5E POP ESI
004562EC - C3 RETN
004562ED $ 8B4424 08 MOV EAX,DWORD PTR SS:[ESP+8]
004562F1 - 56 PUSH ESI
004562F2 - 85C0 TEST EAX,EAX
004562F4 - 8BF1 MOV ESI,ECX
004562F6 - 75 08 JNZ SHORT Pixtopia.00456300
004562F8 - E8 C94B0100 CALL Pixtopia.0046AEC6
004562FD - 8B40 10 MOV EAX,DWORD PTR DS:[EAX+10]
00456300 > 85F6 TEST ESI,ESI
00456302 - 75 04 JNZ SHORT Pixtopia.00456308
00456304 - 33C9 XOR ECX,ECX
00456306 - EB 03 JMP SHORT Pixtopia.0045630B
00456308 > 8B4E 1C MOV ECX,DWORD PTR DS:[ESI+1C]
0045630B > FF7424 10 PUSH DWORD PTR SS:[ESP+10]
0045630F - 50 PUSH EAX
00456310 - FF7424 10 PUSH DWORD PTR SS:[ESP+10]
00456314 - 51 PUSH ECX
00456315 - FF15 04564700 CALL DWORD PTR DS:[&USER32.MessageBoxA]
0045631B - 5E POP ESI
0045631C - C2 0C00 RETN 0C
0045631F $ 55 PUSH EBP
00456320 - 8BEC MOV EBP,ESP
00456322 - 56 PUSH ESI
00456323 - 57 PUSH EDI
```

00984A58  
Pixtopia.0048FC68  
ntdll.7C91005D  
ntdll.7C91005D  
[Style = MB\_OK;MB\_ICONHAND;MB\_APPLMODAL  
Title = 00000001 ???  
Text = 00000010 ???  
hOwner = 7C91005D  
MessageBoxA  
00984A58

### 3. 문제 (4)의 솔루션 - 우회 (SendMessageA)

Paused			L E M T W H C / K B R ... S															
00412D98	-	50	PUSH EAX															
00412D99	-	68 786A4700	PUSH Pixtopia.00476A78															
00412D9E	-	E8 25670400	CALL Pixtopia.004594C8															
00412DA3	-	83C4 08	ADD ESP,8															
00412DA6	-	8BD8	MOV EBX,EAX															
00412DA8	-	8B86 14030000	MOV EAX,DWORD PTR DS:[ESI+314]															
00412DAE	-	6A 00	PUSH 0															
00412DB0	-	6A 00	PUSH 0															
00412DB2	-	68 47010000	PUSH 147															
00412DB7	-	50	PUSH EAX															
00412DB8	-	FF15 D0564700	CALL DWORD PTR DS:[<USER32.SendMessageA>]															
00412DBE	-	8B8E BC010000	MOV ECX,DWORD PTR DS:[ESI+1BC]															
00412DC4	-	8BF8	MOV EDI,EAX															
00412DC6	-	8B04F9	MOV EAX,DWORD PTR DS:[ECX+EDI*8]															
00412DC9	-	8D2CFD 00000000	LEA EBP,DWORD PTR DS:[EDI*8]															
00412DD0	-	83F8 04 4이상이면 점프X	CMP EAX,4															
00412DD3	-	7C 1A	JL SHORT Pixtopia.00412DEF															
00412DD5	-	8B4C24 10	MOV ECX,DWORD PTR SS:[ESP+10]															
00412DD9	-	6A 10	PUSH 10															
00412DDB	-	68 00F74800	PUSH Pixtopia.0048F700															
00412DE0	-	68 68FC4800	PUSH Pixtopia.0048FC68															
00412DE5	-	E8 03350400	CALL Pixtopia.004562ED															
00412DEA	-	E9 DD000000	JMP Pixtopia.00412ECC															
00412DEF	>	8D4C24 14	LEA ECX,DWORD PTR SS:[ESP+14]															
00412DF3	-	E8 38610100	CALL Pixtopia.00428F30															
00412DF8	-	68 D8784900	PUSH Pixtopia.004978D8															

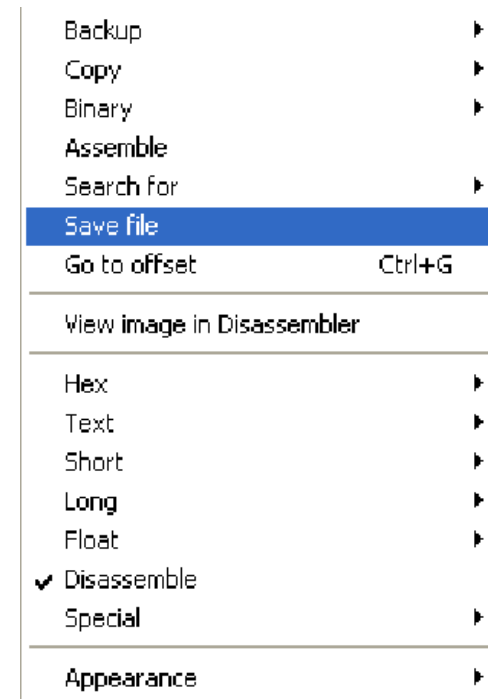
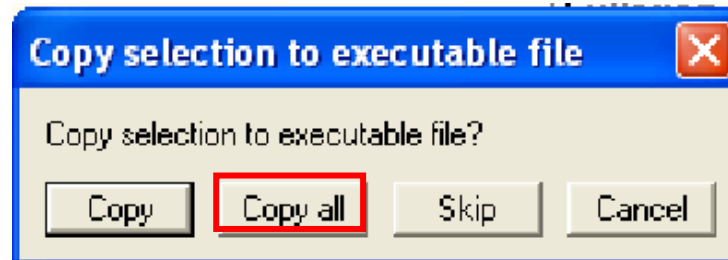
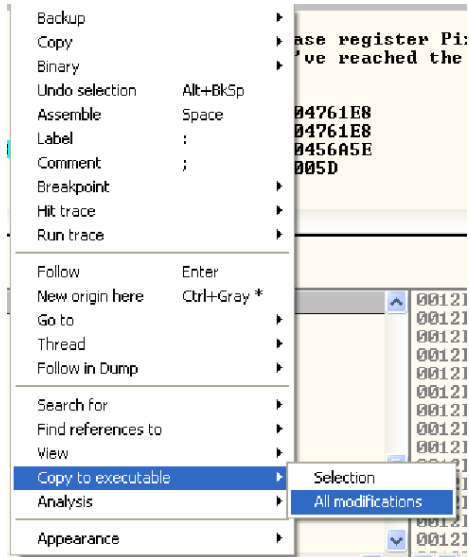
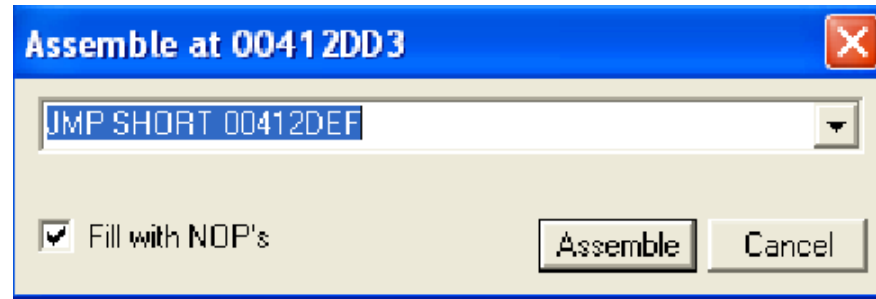
메시지 창으로 메시지 보내기

콤보 상자의 목록 상자에서 현재 선택한 항목의 인덱스를 가져오는 함수

```
lParam = 0
wParam = 0
Message = CB_GETCURREL
hWnd = 1
SendMessageA
```

ASCII "Please register F  
ASCII "You've reached th

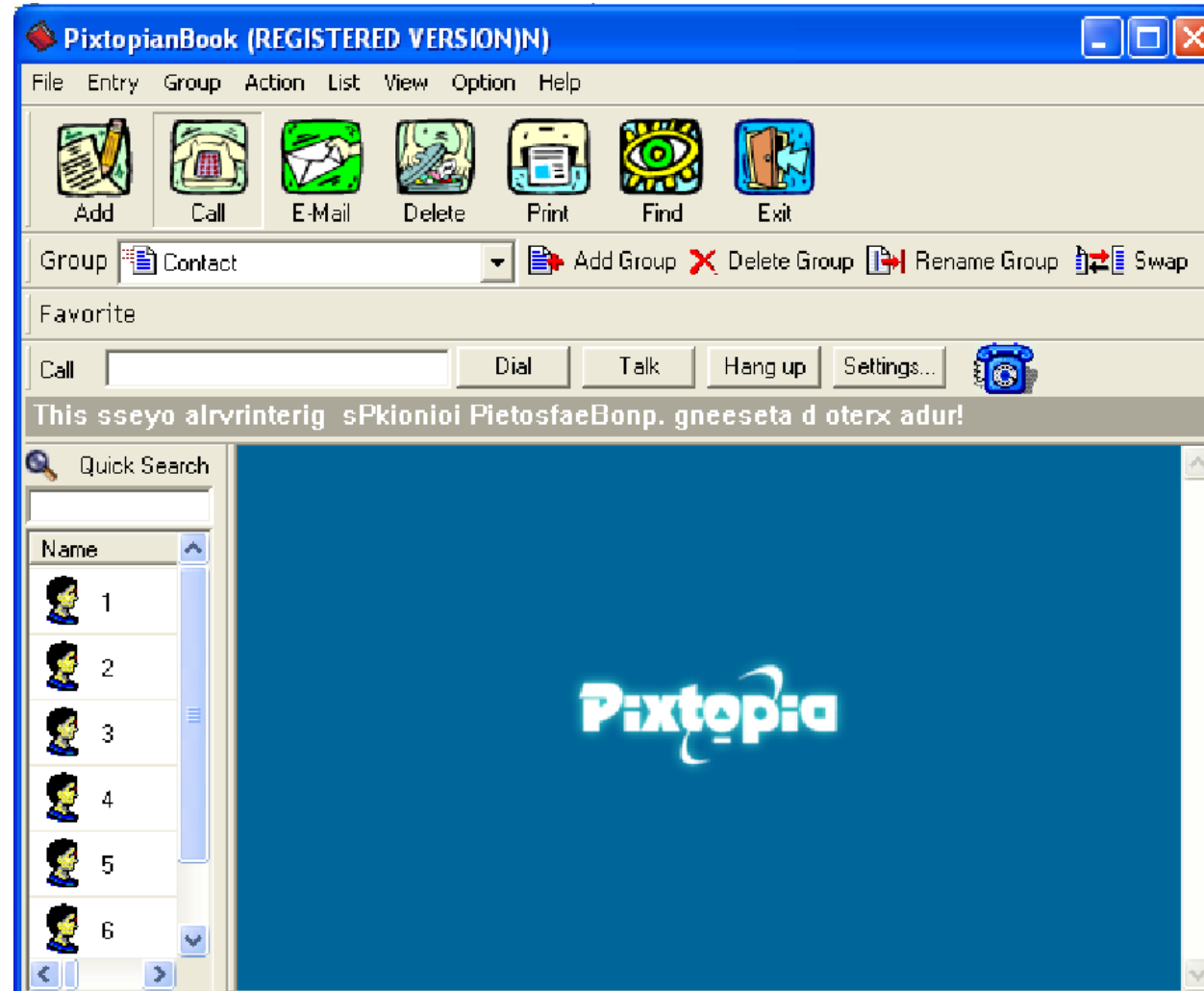
### 3. 문제 (4)의 솔루션 - 우회 (명령어 수정 및 변경 사항 저장)



PixtopianBook3으로 저장

### 3. 문제 (4)의 솔루션 - 우회 (결과)

5명 이상 추가 가능해짐



감사합니다