리버스 엔지니어링(3)

발표자: 양유진

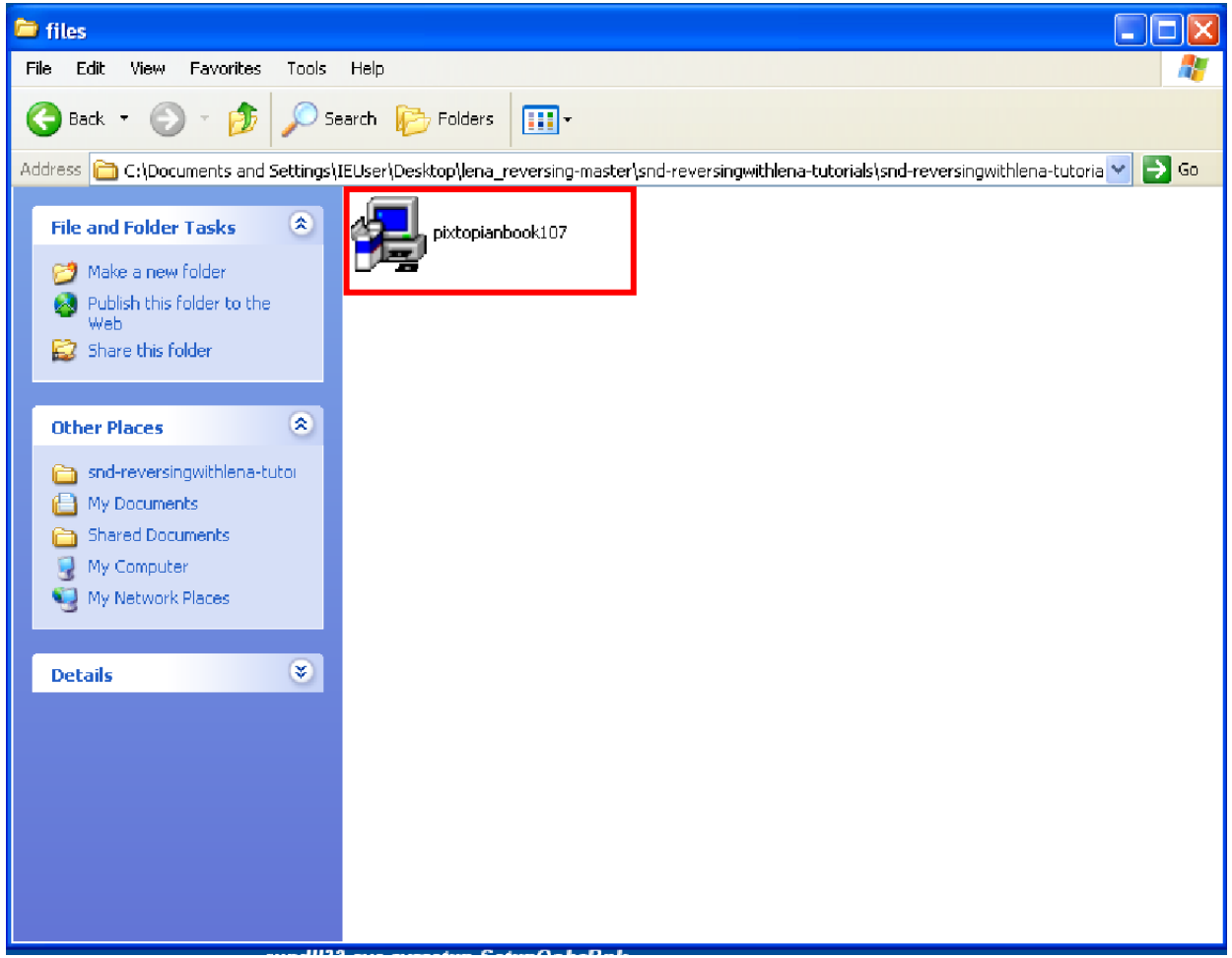
링크: https://youtu.be/1SFIPMg0D0E

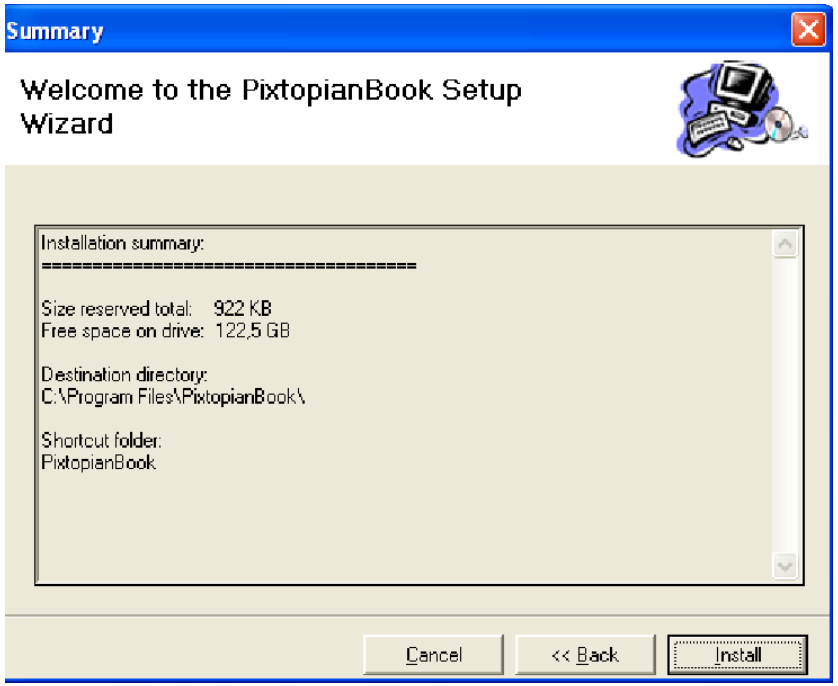
실습 목적

제약사항 패치하여 체험판 프로그램 크랙하기

1. 프로그램 설치

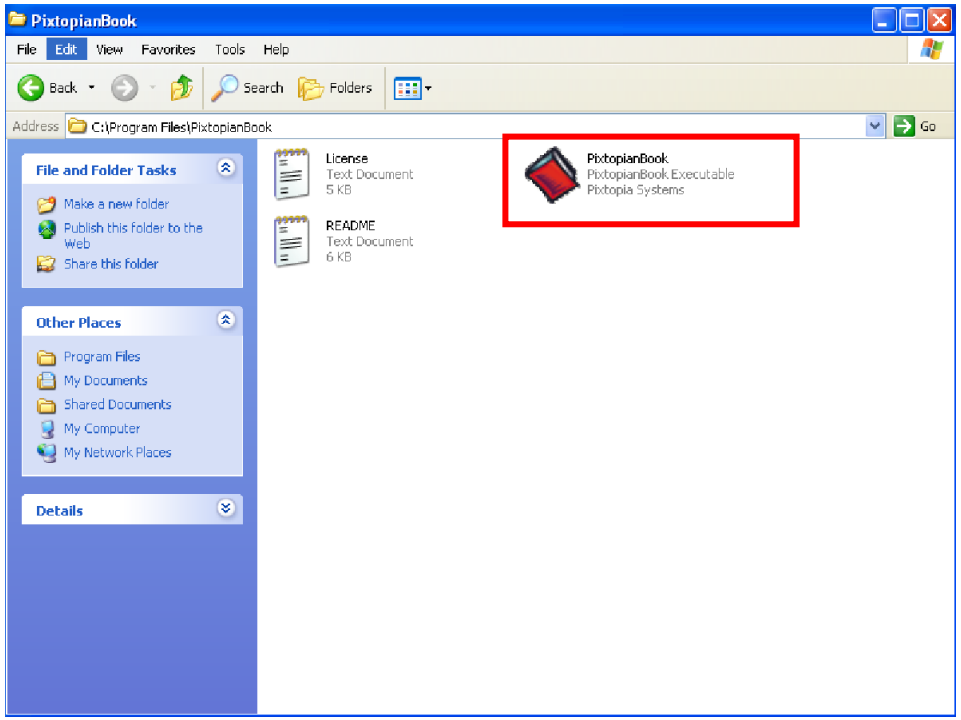
lena_reversing-master\snd-reversingwithlena-tutorials\snd-reversingwithlena-tutorial04.tutorial\files

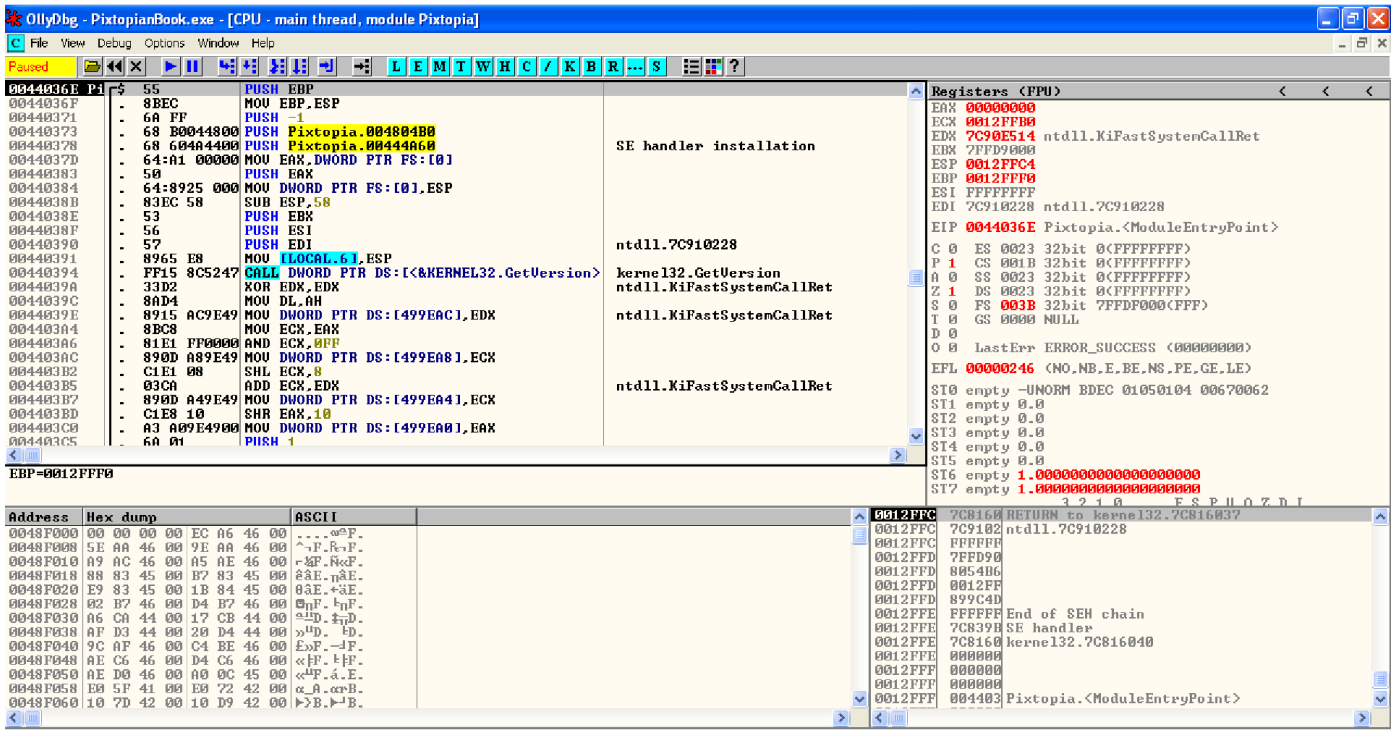




2. OllyDbg로 실행파일 열기

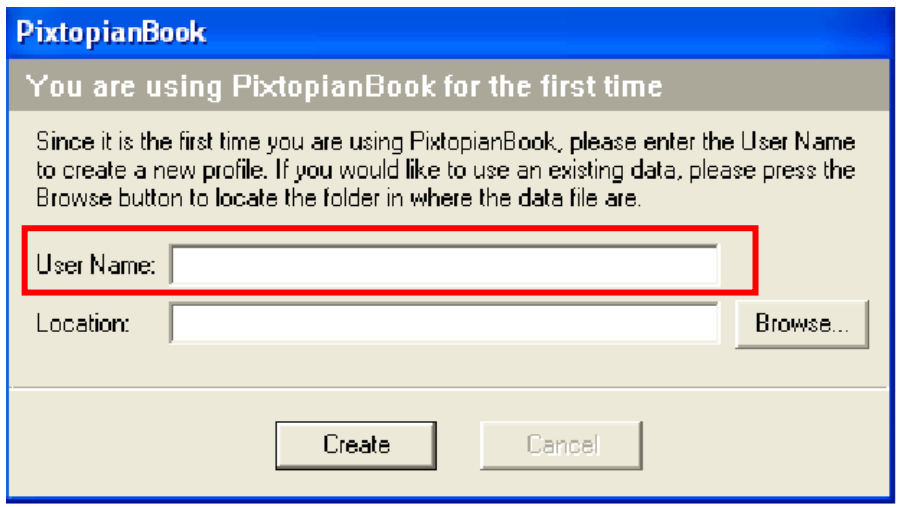
C:\Program Files\PixtopianBook

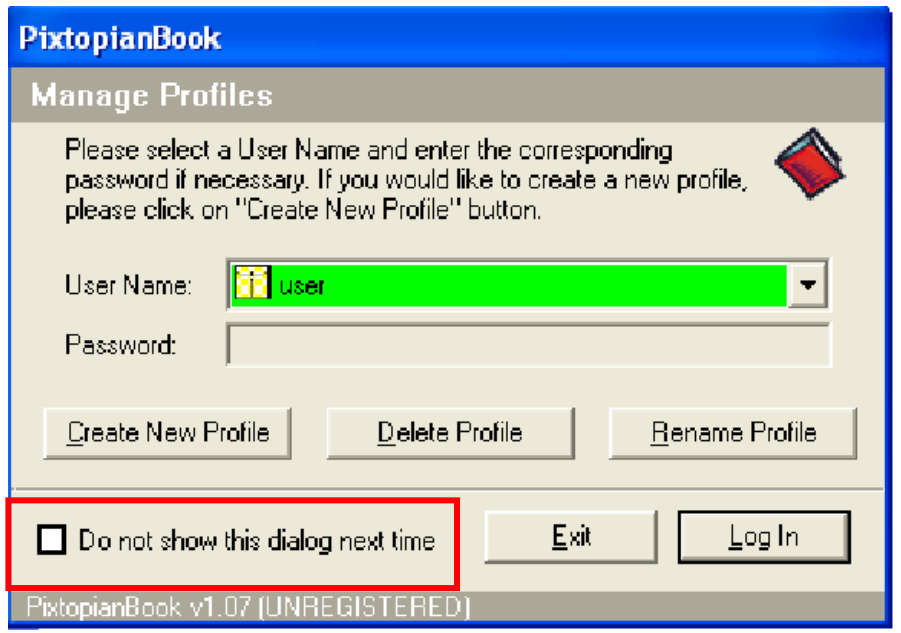




3. 실행

아무거나 적어도 됨

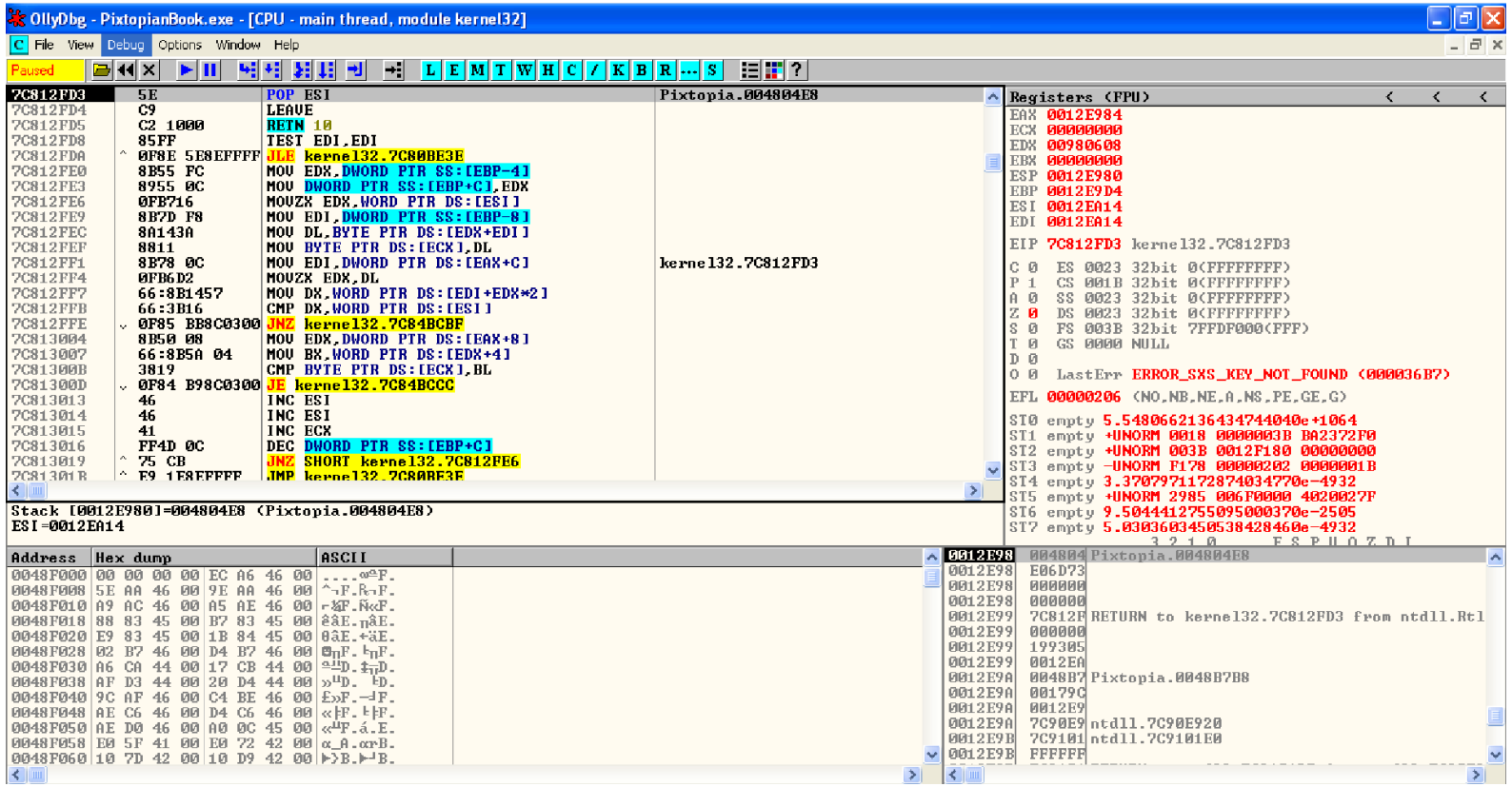




체크하면 이 창이 다시 뜨지 않음

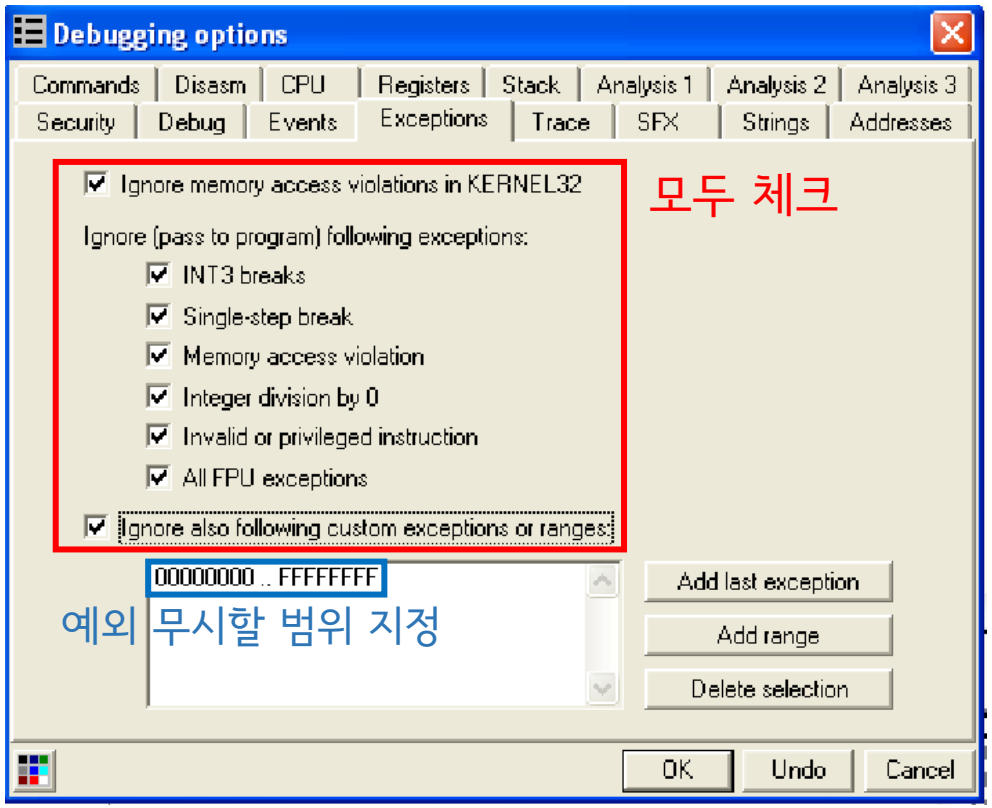
3. 문제 (1) 프로그램 실행 안 됨

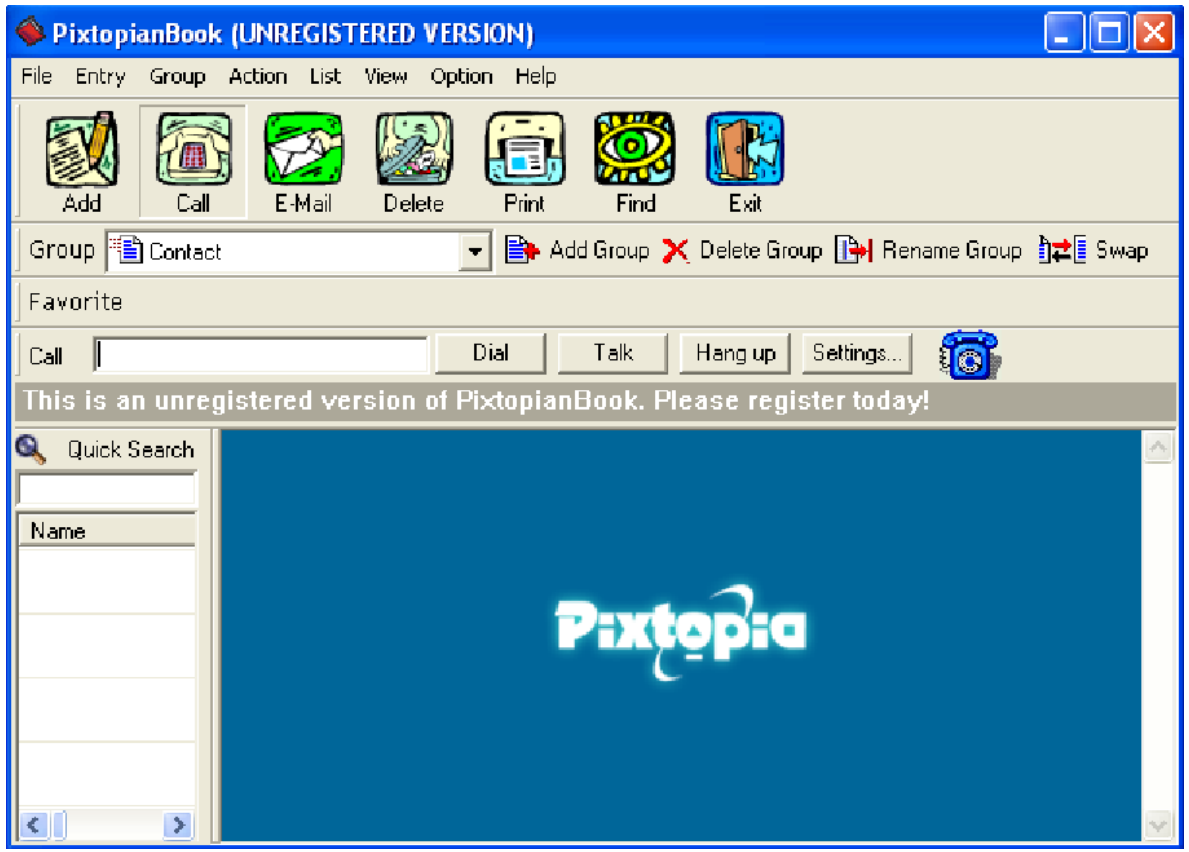
실행 도중 예외 처리 오류가 발생하여 실행이 안 됨



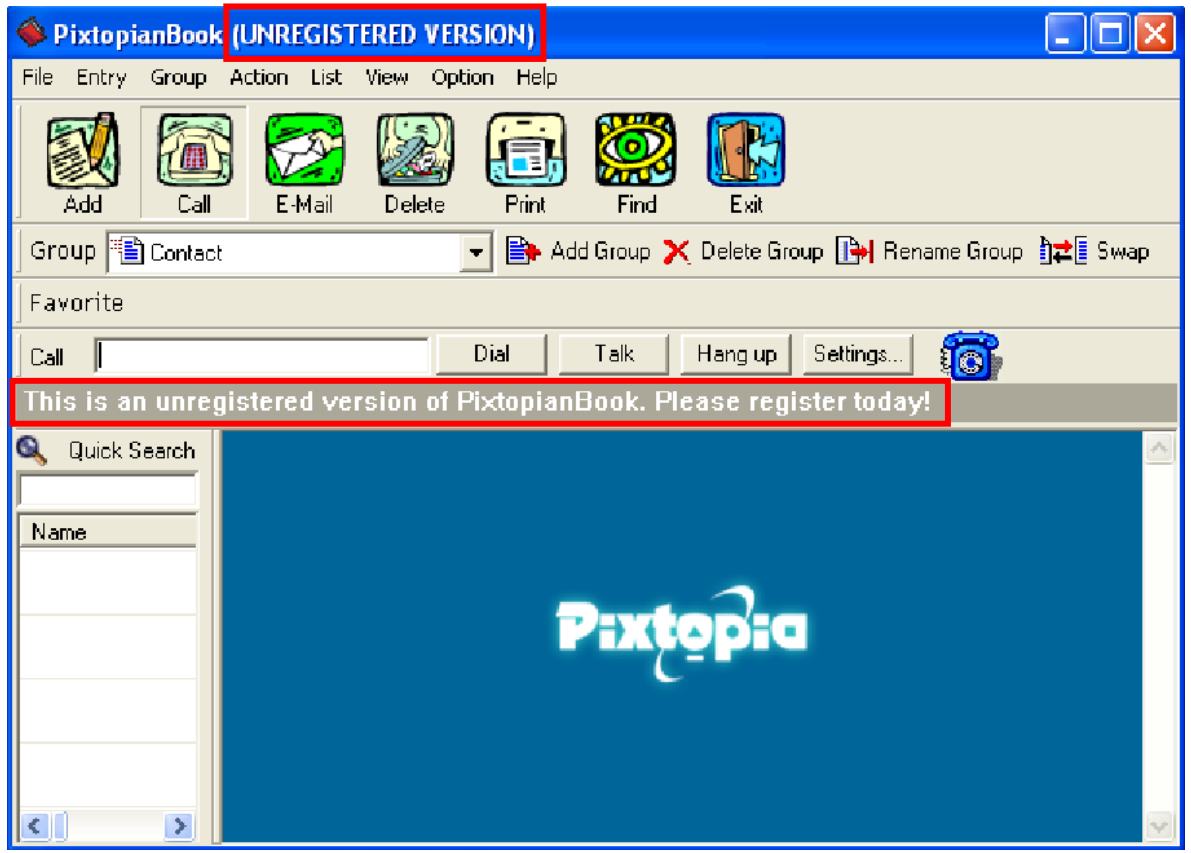
3. 문제 (1)의 솔루션 - 예외 처리 무시

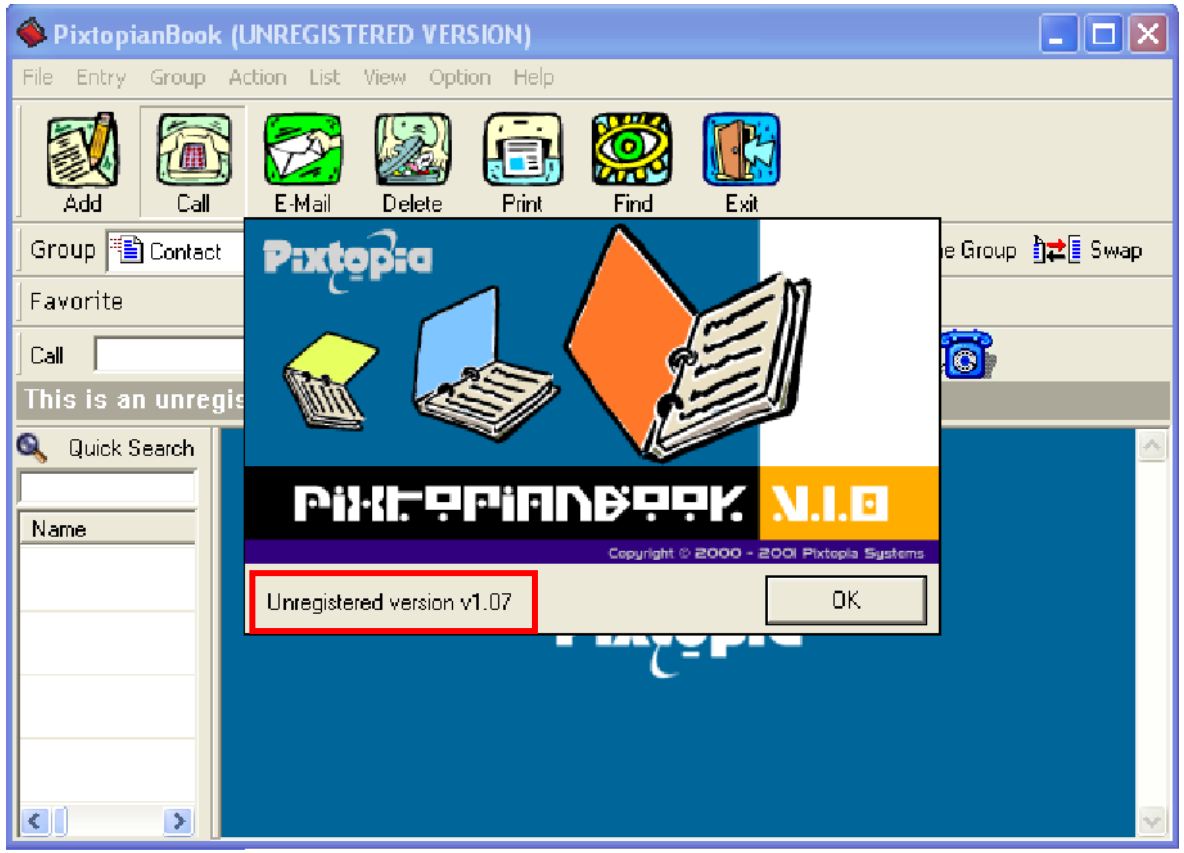
Options > Debugging options > Exceptions





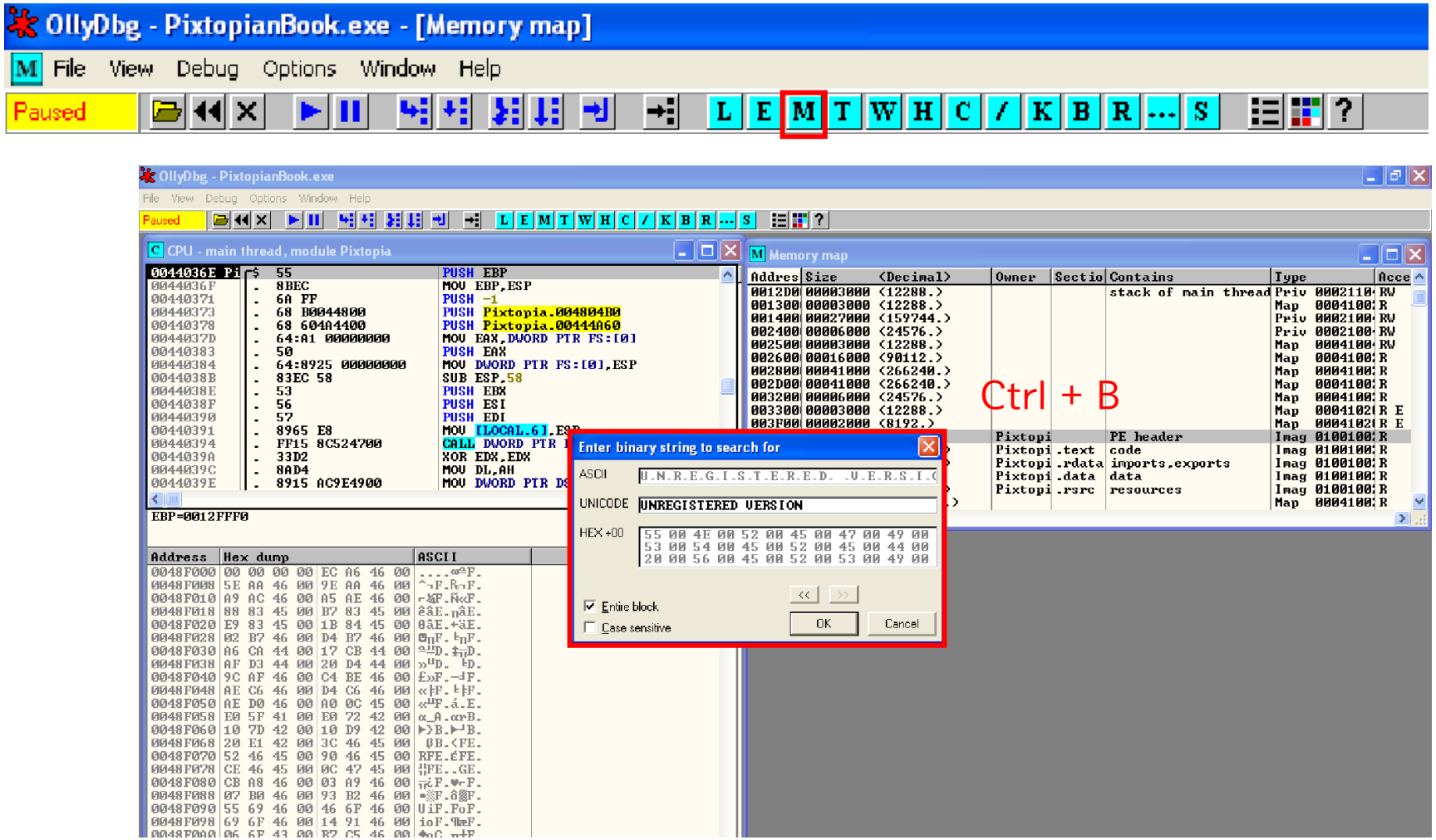
3. 문제 (2) Unregistered



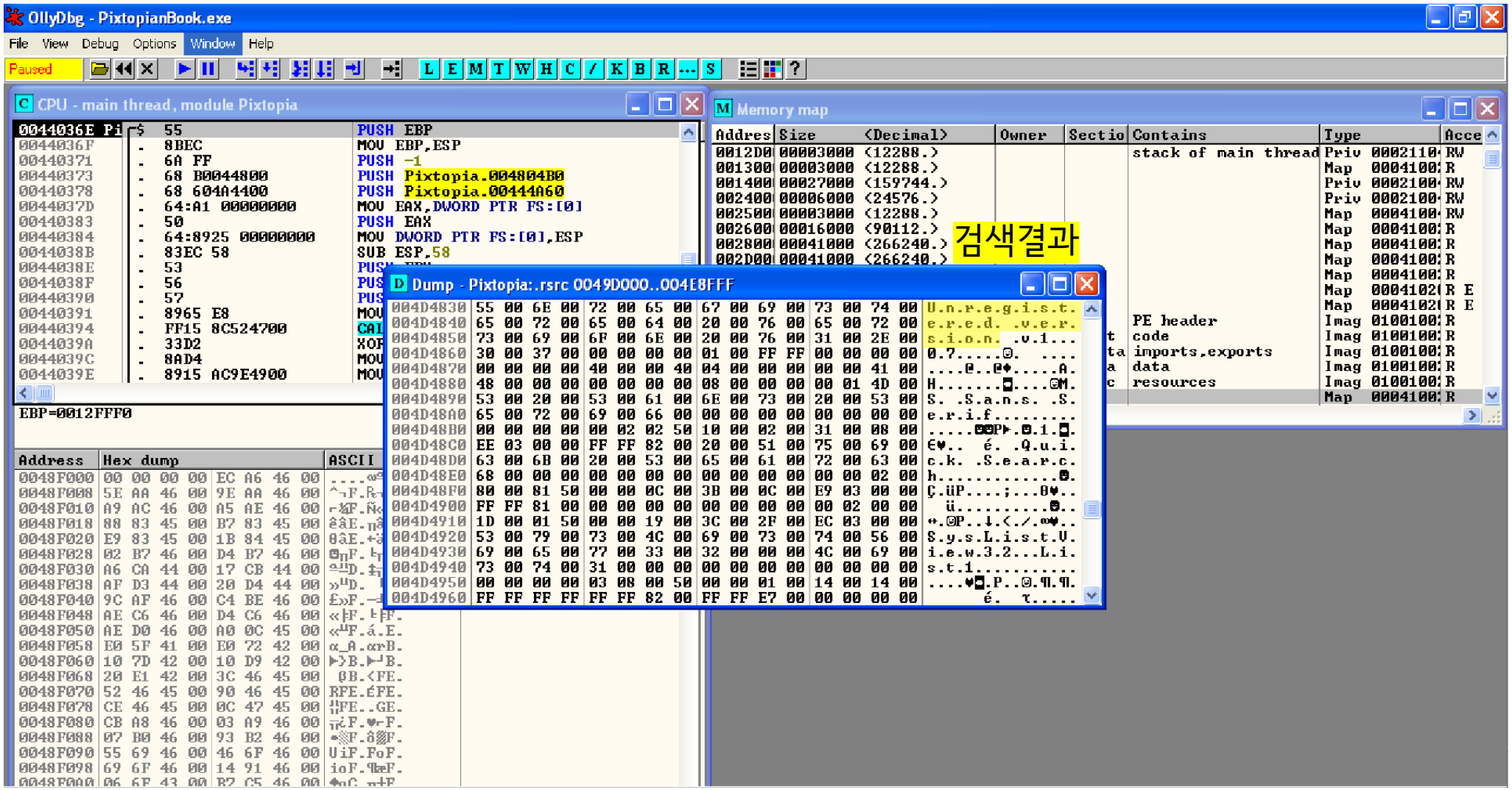


3. 문제 (2)의 솔루션 - 문자열 변경

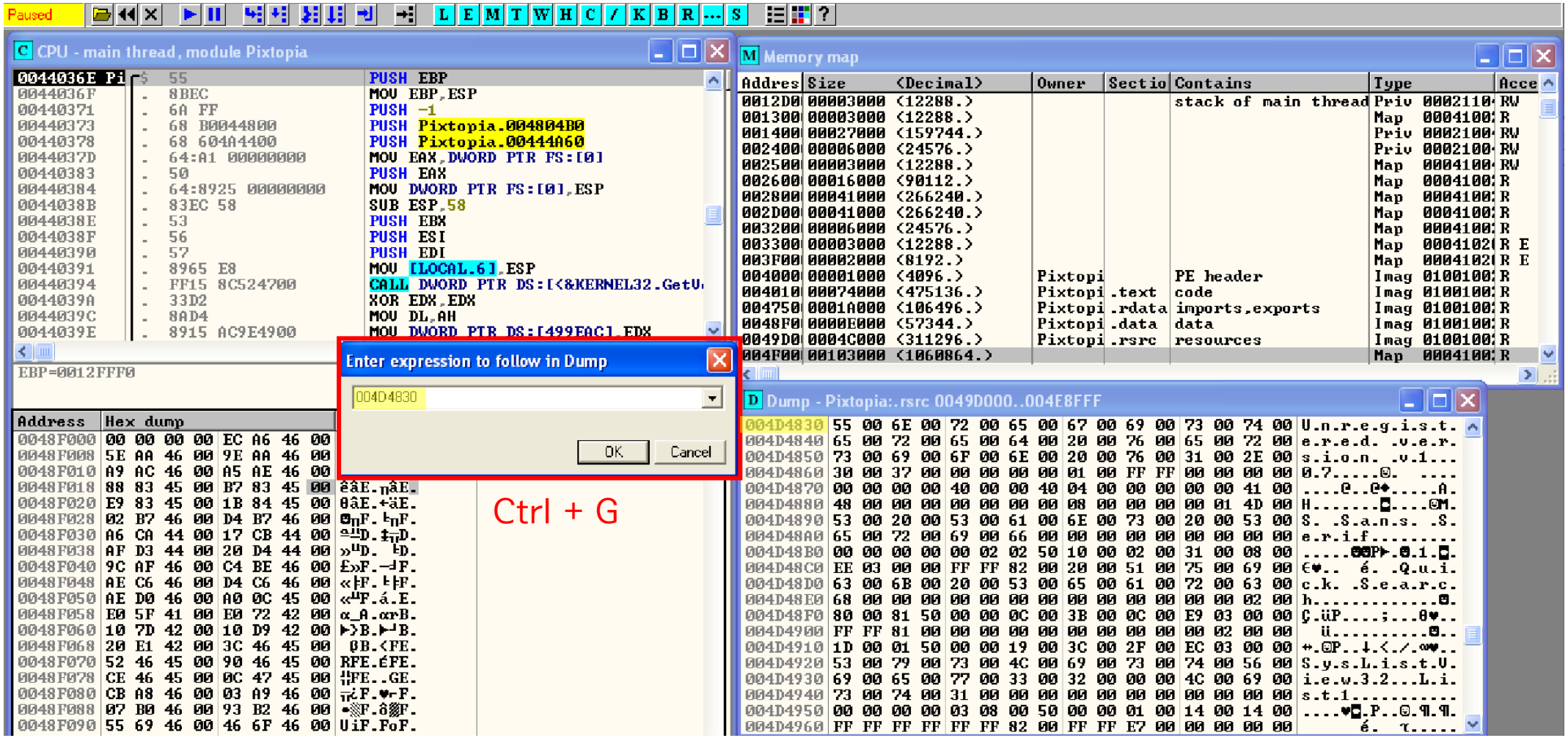
Memory map 클릭



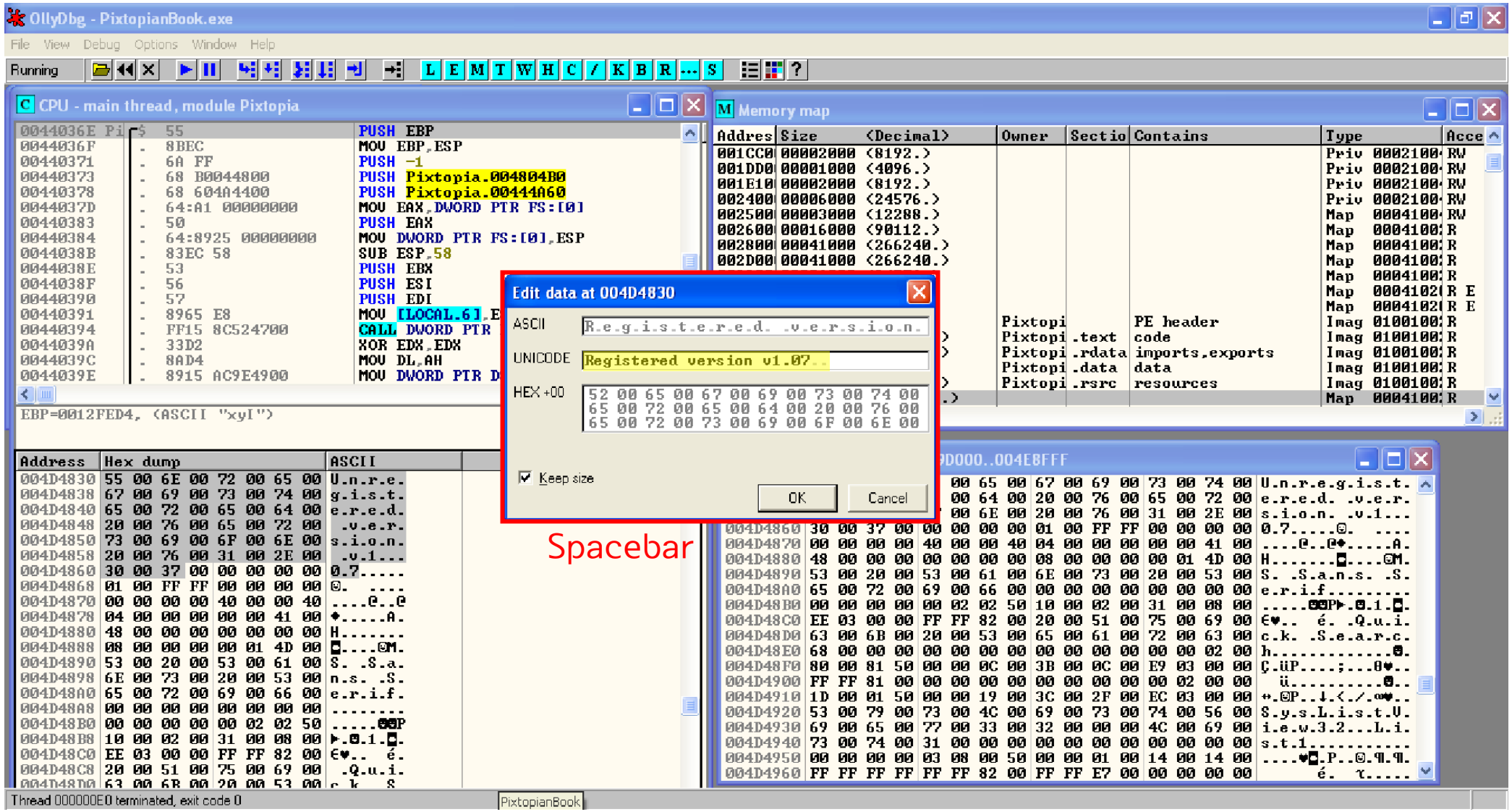
3. 문제 (2)의 솔루션 - 문자열 변경



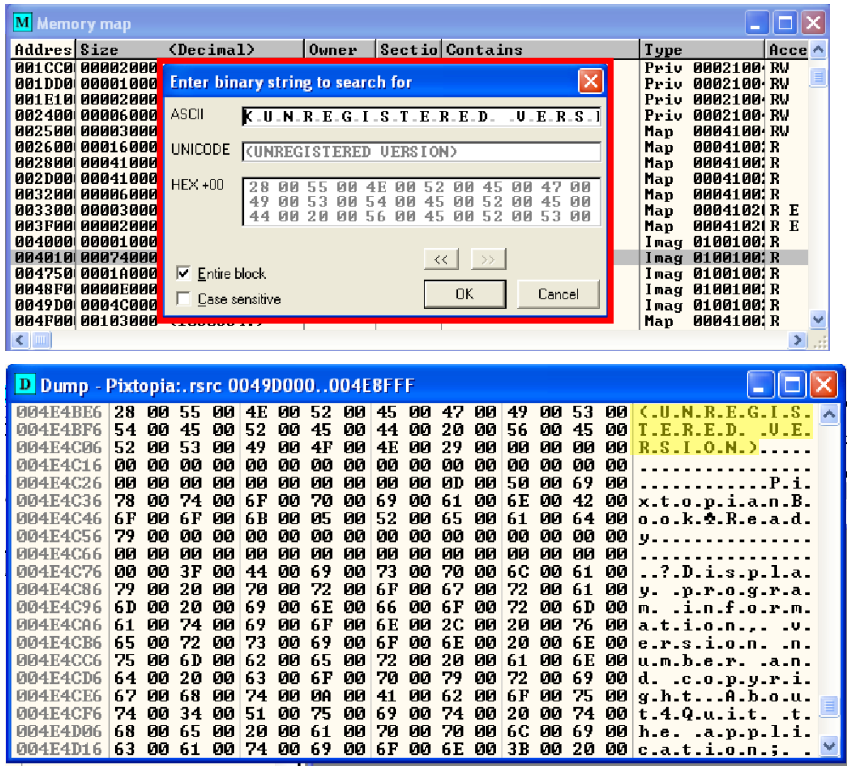
3. 문제 (2)의 솔루션 - 문자열 변경

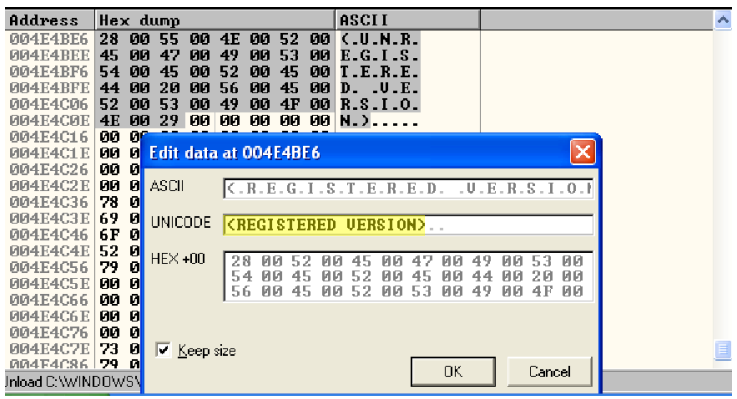


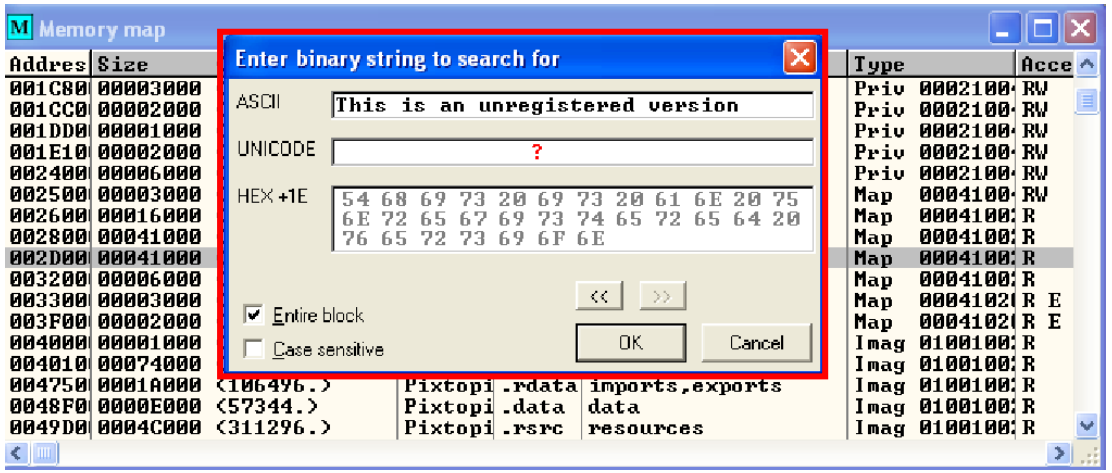
3. 문제 (2)의 솔루션 - 문자열 변경

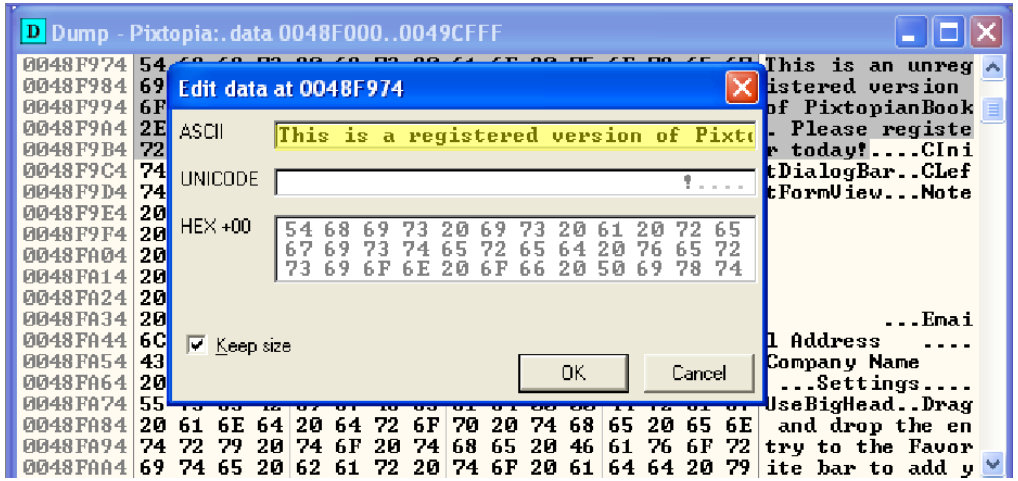


3. 문제 (2)의 솔루션 - 문자열 변경

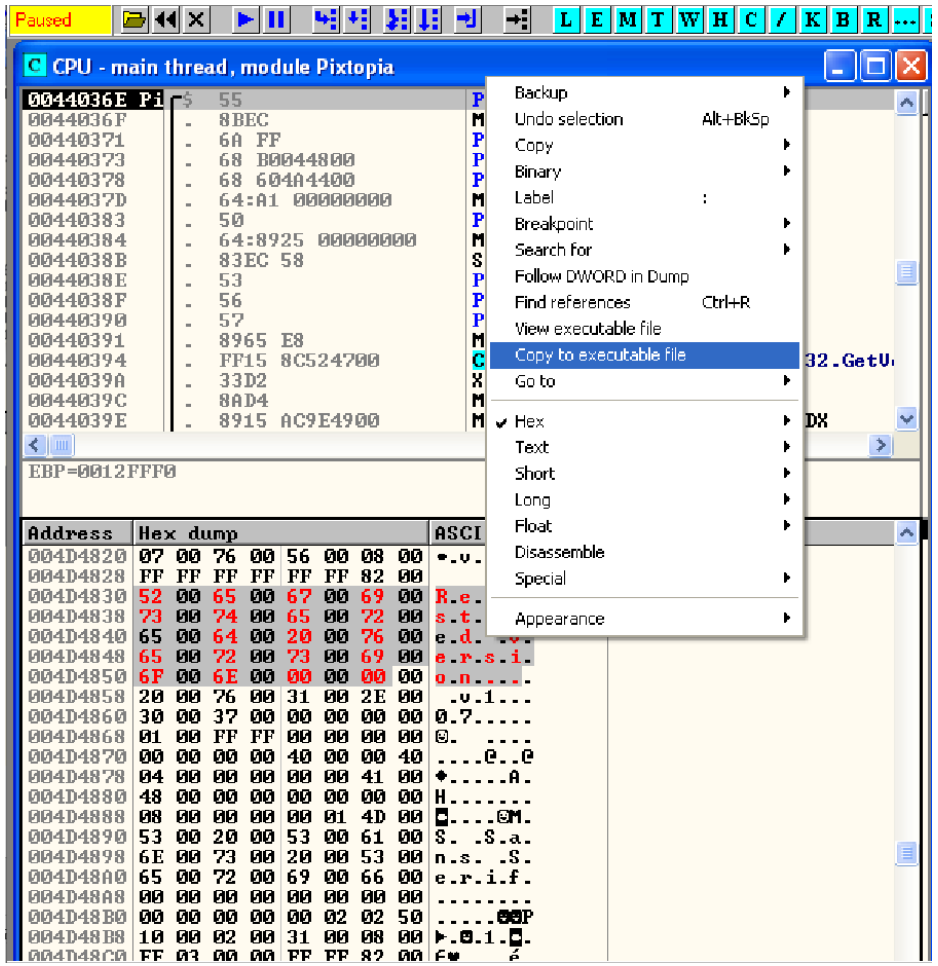


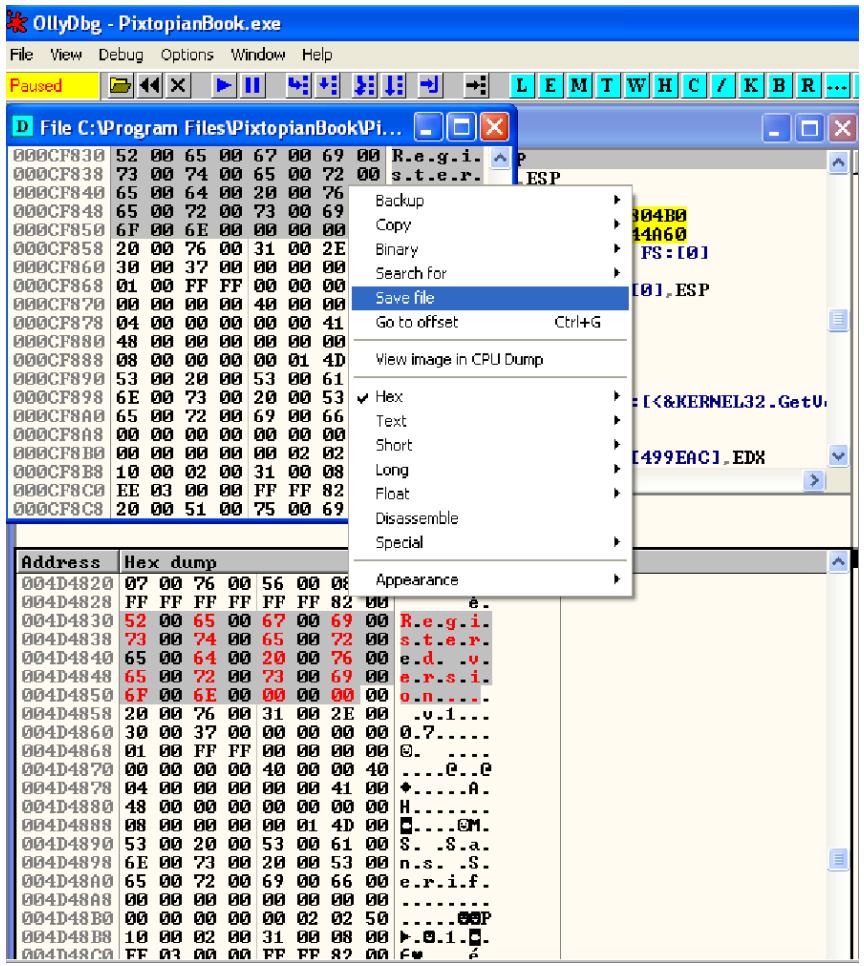


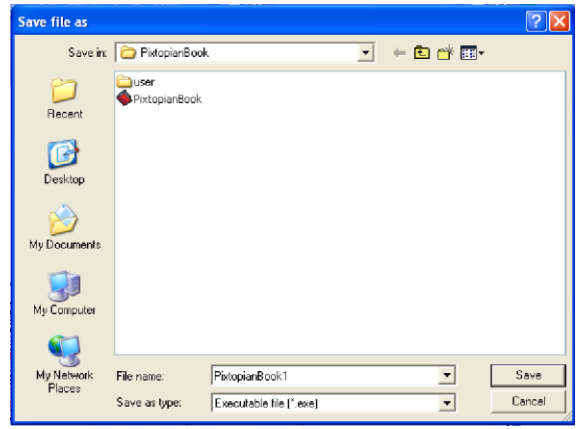




3. 문제 (2)의 솔루션 - 문자열 변경

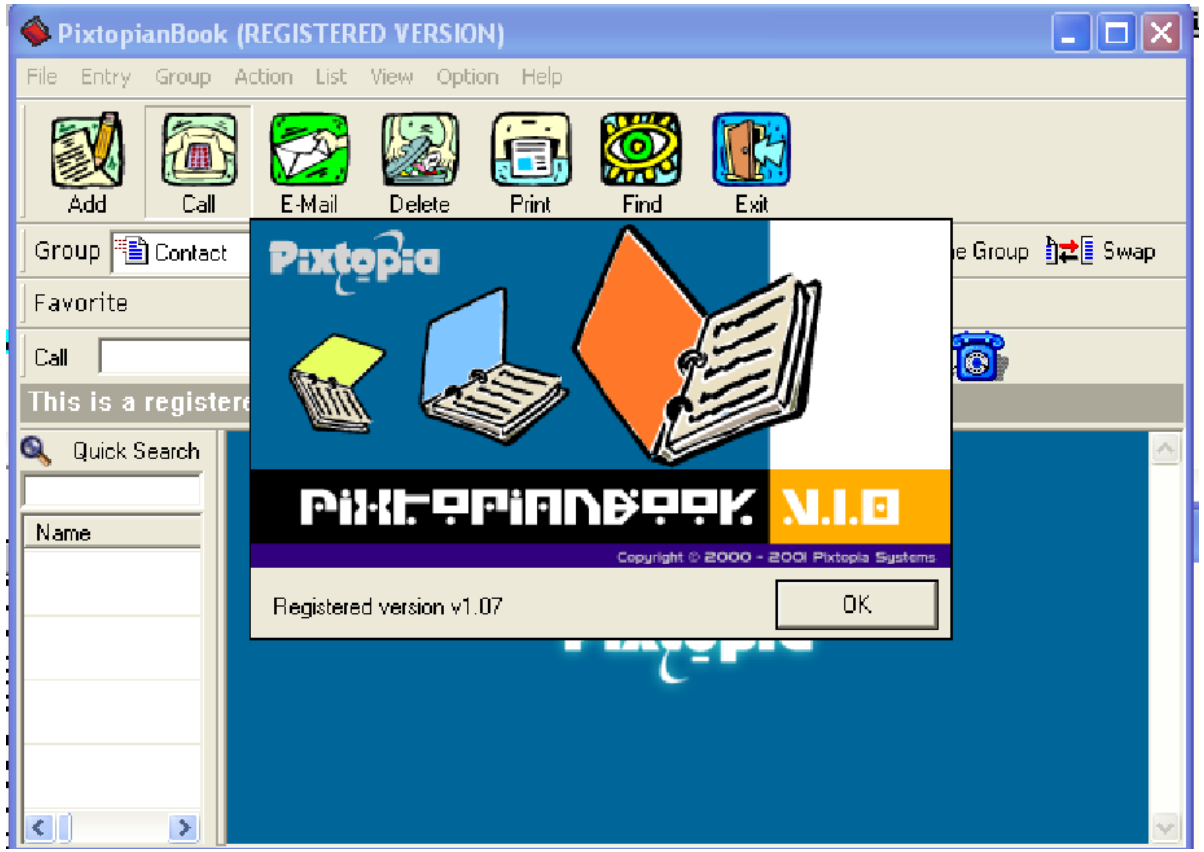






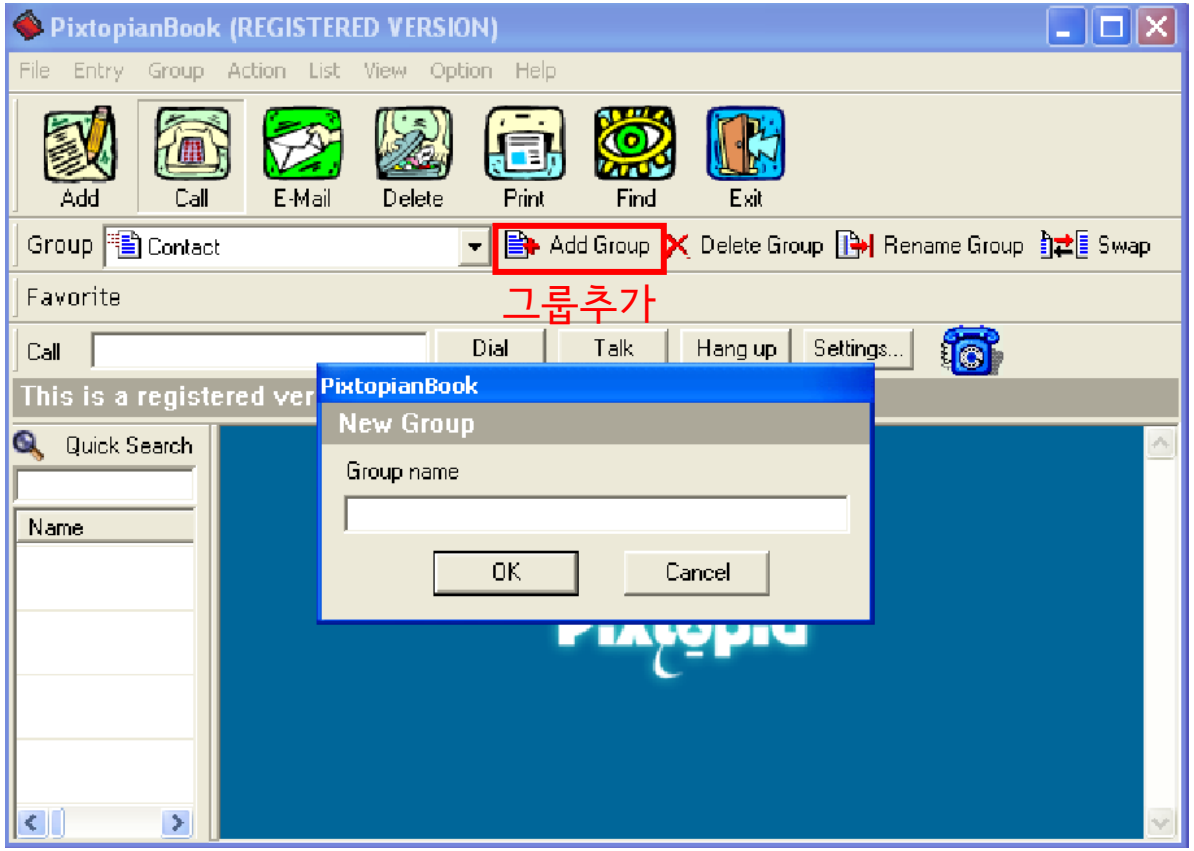
PixtopianBook1로 저장

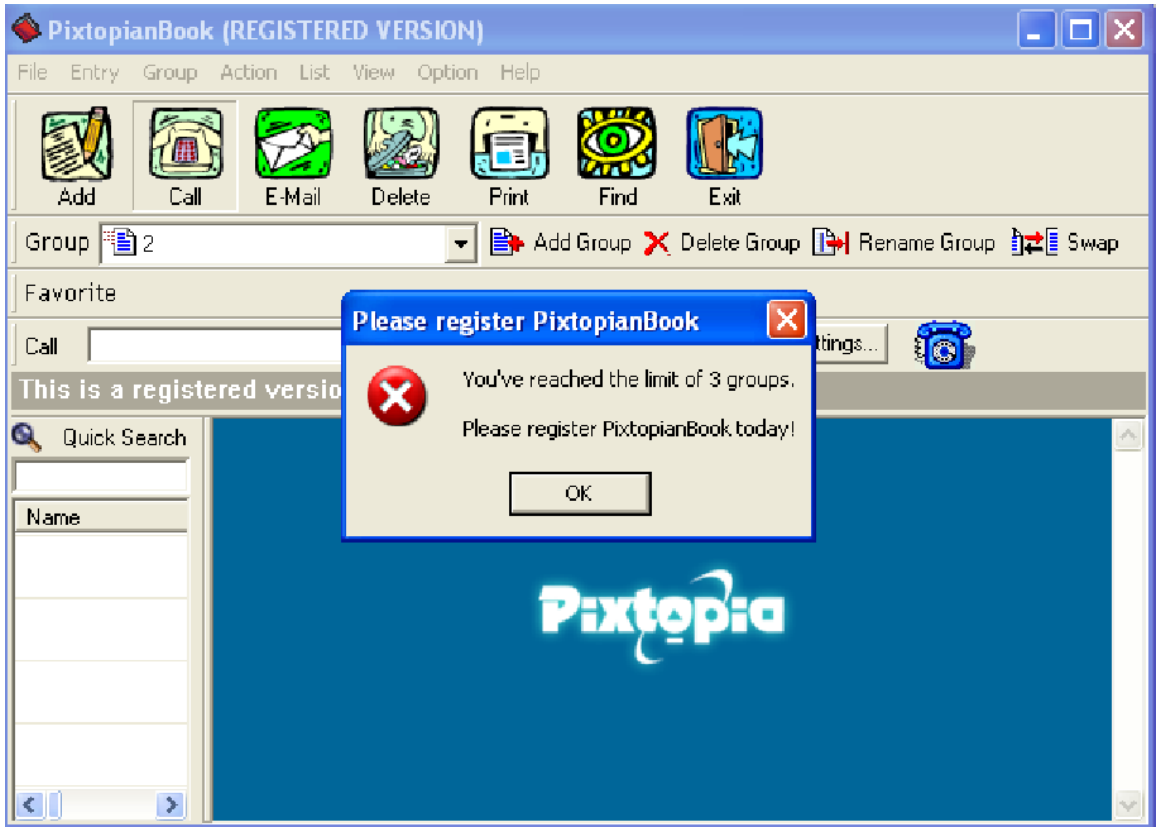
3. 문제 (2)의 솔루션 - 문자열 변경 (결과)



3. 문제 (3) 그룹 생성 제한

최대 3개까지만 그룹 생성 가능





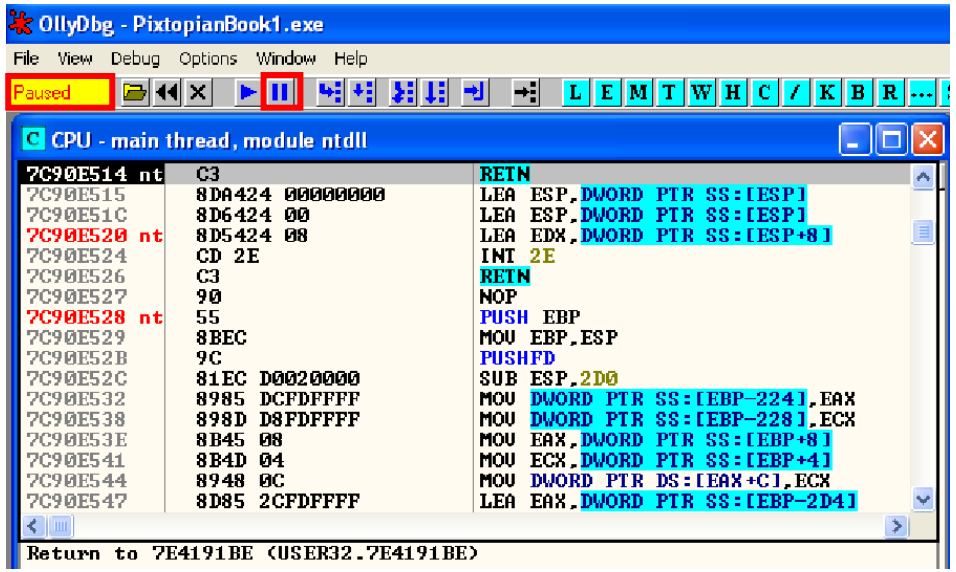
3. 문제 (3)의 솔루션 - 우회 (Back to user mode 이용)

Back to user mode

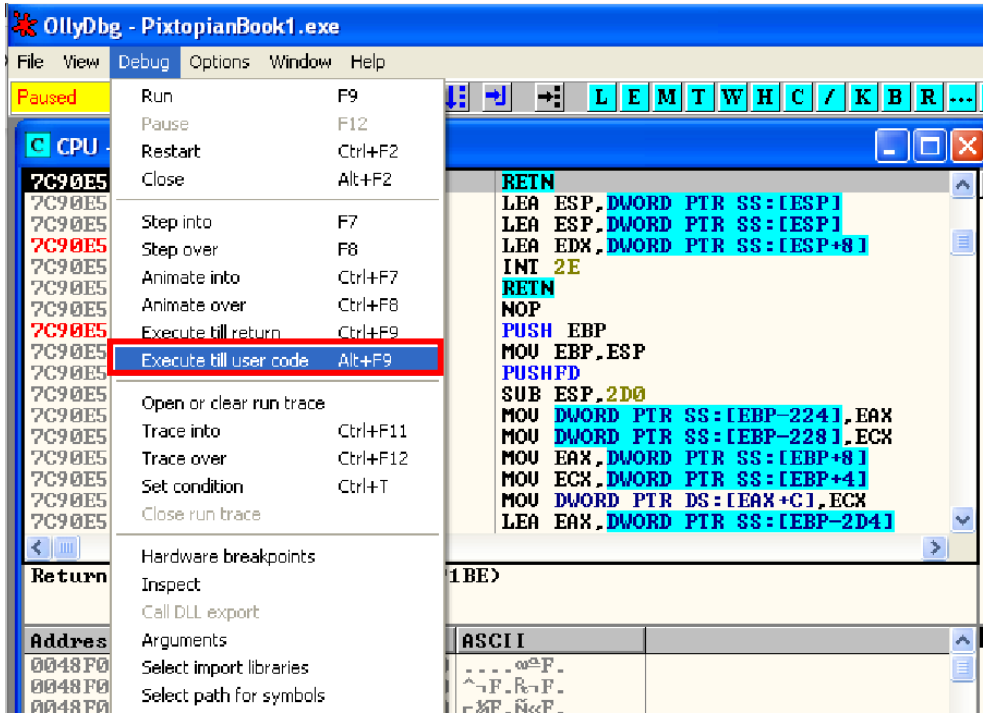
- 특정 이벤트를 발생하기 전에 설정해두고 call 명령이 일어난 바로 다음 주소로 이동해주는 모드
- call 명령이 일어난 바로 다음의 위치를 잡을 수 있음. (함수 호출부를 찾는데 유용함)

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

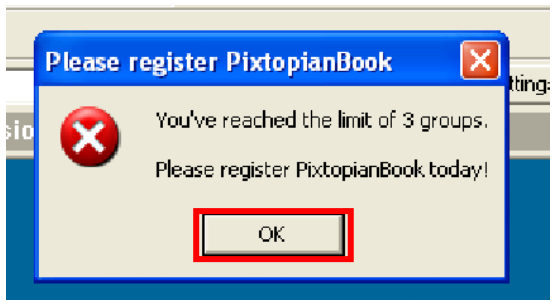
1. 실행중지



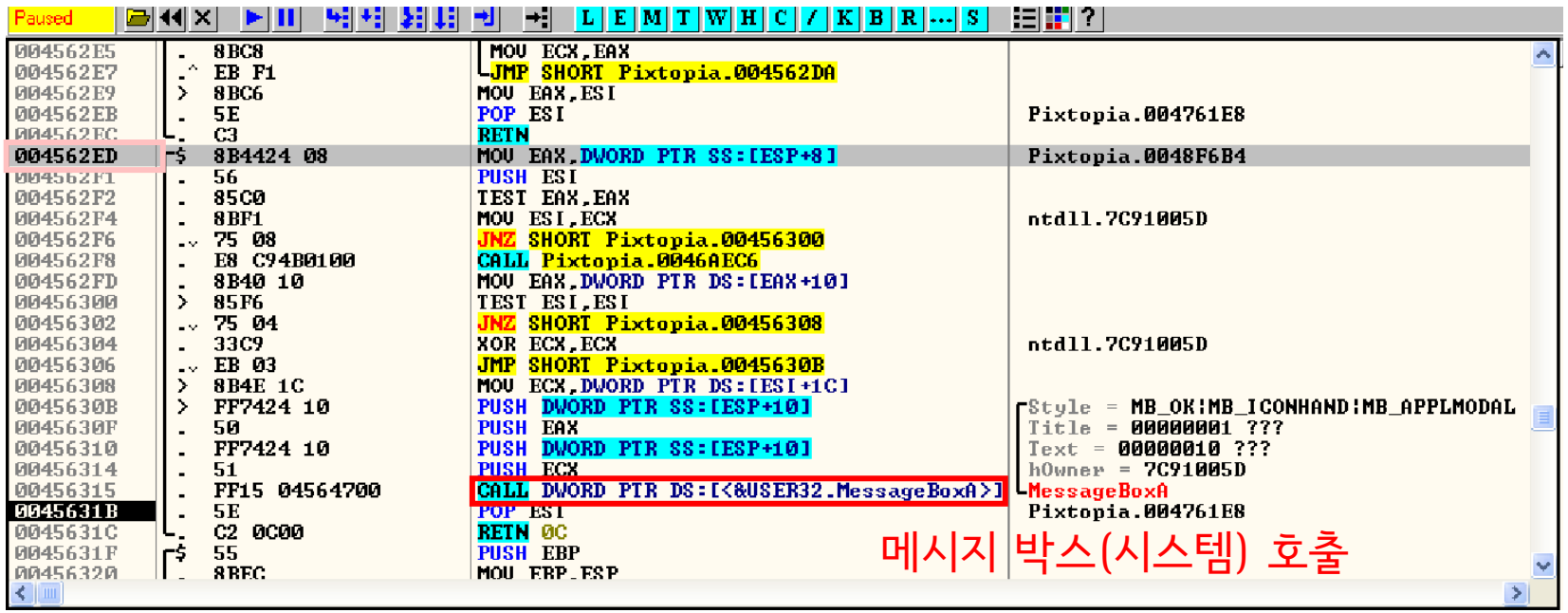
2. Debug > Execute till user code



3. 확인 버튼 누르기



3. 문제 (3)의 솔루션 - 우회 (MessageBoxA)



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

3. 문제 (3)의 솔루션 - 우회 (SendMessageA)

메시지 창으로 메시지 보내기

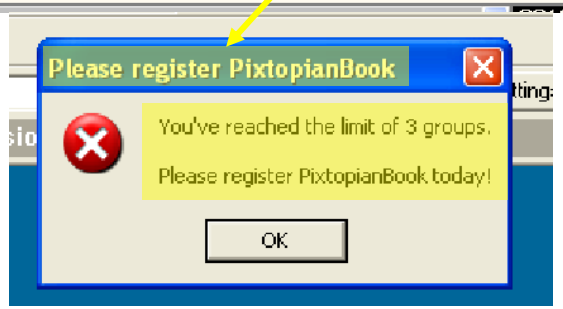
콤보 상자의 목록 상자에 있는 항목 수를 가져오는 함수

SendMessageA

hWnd	메시지 수신할 창의 핸들번호
Message	보낼 메시지
wParam lParam	추가 메시지 관련 정보

반환값: 메시지 처리 결과

```
00408ADE   .  64:8925 00000000   MOV DWORD PTR FS:[0],ESP          ntdll.7C91005D
00408AE5   .  81EC 34010000      SUB ESP,134                      Pixtopia.004761E8
00408AEB   .  53                 PUSH EBX
00408AEC   .  8BD9               MOV EBX,ECX
00408AEE   .  56                 PUSH ESI    ESI에 출발지 주소 저장
00408AEF   .  6A 00              PUSH 0                           lParam = 0
00408AF1   .  8B83 A4000000      MOV EAX,DWORD PTR DS:[EBX+A4]
00408AF7   .  6A 00              PUSH 0                           wParam = 0
00408AF9   .  68 46010000        PUSH 146                         Message = CB_GETCOUNT
00408AFE   .  50                 PUSH EAX                         hWnd = 1
00408AFF   .  FF15 D0564700      CALL DWORD PTR DS:[<&USER32.SendMessageA>] SendMessageA
00408B05   .  83F8 03            CMP EAX,3                        함수 반환 결과(EAX)
00408B08   .  7C 2A              JL SHORT Pixtopia.00408B34       3이상이면 점프X
00408B0A   .  6A 10              PUSH 10
00408B0C   .  68 00F74800        PUSH Pixtopia.0048F700           ASCII "Please register PixtopianBook"
00408B11   .  68 B4F64800        PUSH Pixtopia.0048F6B4           ASCII "You've reached the limit of 3 gr
00408B16   .  8BCB               MOV ECX,EBX
00408B18   .  E8 D0D70400        CALL Pixtopia.004562ED
00408B1D   .  5E                 POP ESI                          Pixtopia.004761E8
00408B1E   .  5B                 POP EBX                          Pixtopia.004761E8
00408B1F   .  8B8C24 34010000    MOV ECX,DWORD PTR SS:[ESP+134]   Pixtopia.00456A52
00408B26   .  64:890D 00000000   MOV DWORD PTR FS:[0],ECX         ntdll.7C91005D
00408B2D   .  81C4 40010000      ADD ESP,140
00408B33   .  C3                 RETN
00408B34   >  6A 00              PUSH 0
00408B36   .  8D4C24 24          LEA ECX,DWORD PTR SS:[ESP+24]
Stack [0012F790]=004761E8 (Pixtopia.004761E8), ASCII "piG"
ESI=004761E8 (Pixtopia.004761E8), ASCII "piG"
```



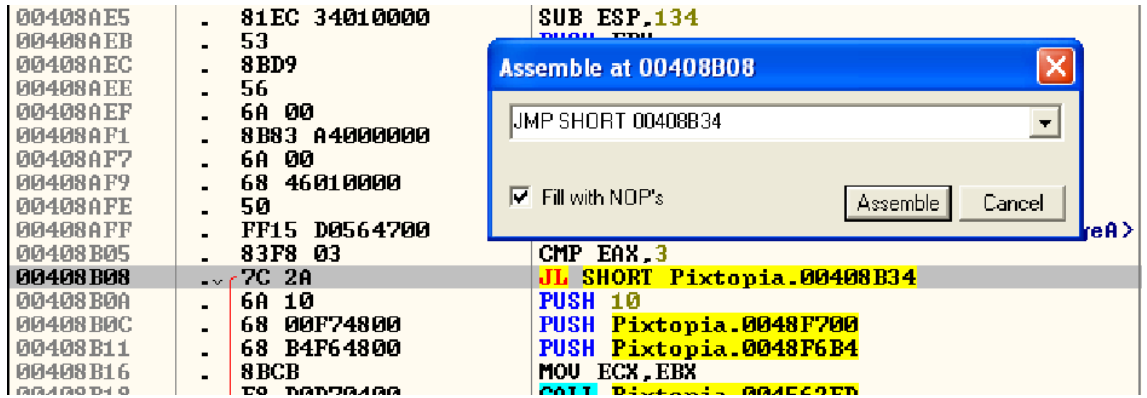
3. 문제 (3)의 솔루션 - 우회 (명령어 수정)

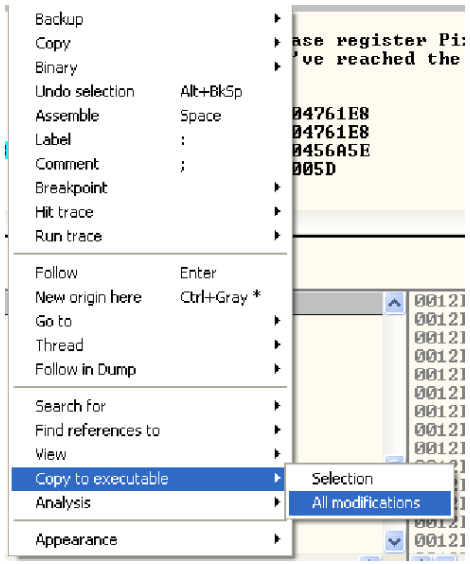
```
00408AFF    .   FF15 D0564700       CALL DWORD PTR DS:[<&USER32.SendMessageA>
00408B05    .   83F8 03             CMP EAX,3
00408B08    .v  7C 2A               JL SHORT Pixtopia.00408B34
```

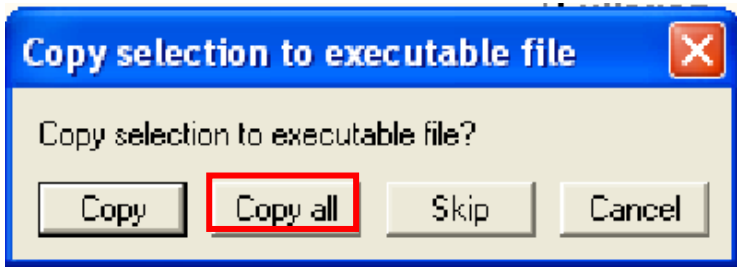
방법1) CMP 명령어의 두번째 operand를 3보다 더 큰 숫자로 변경 → 임시적인 방법

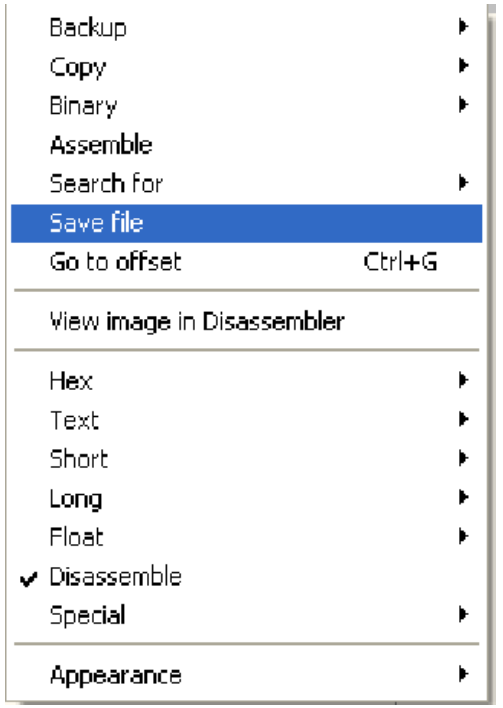
방법2) 분기하지 않도록 JL 명령어를 JMP 명령어로 변경 → 영구적인 방법 (숫자와 관계 없어짐)

3. 문제 (3)의 솔루션 - 우회 (변경부분 저장)





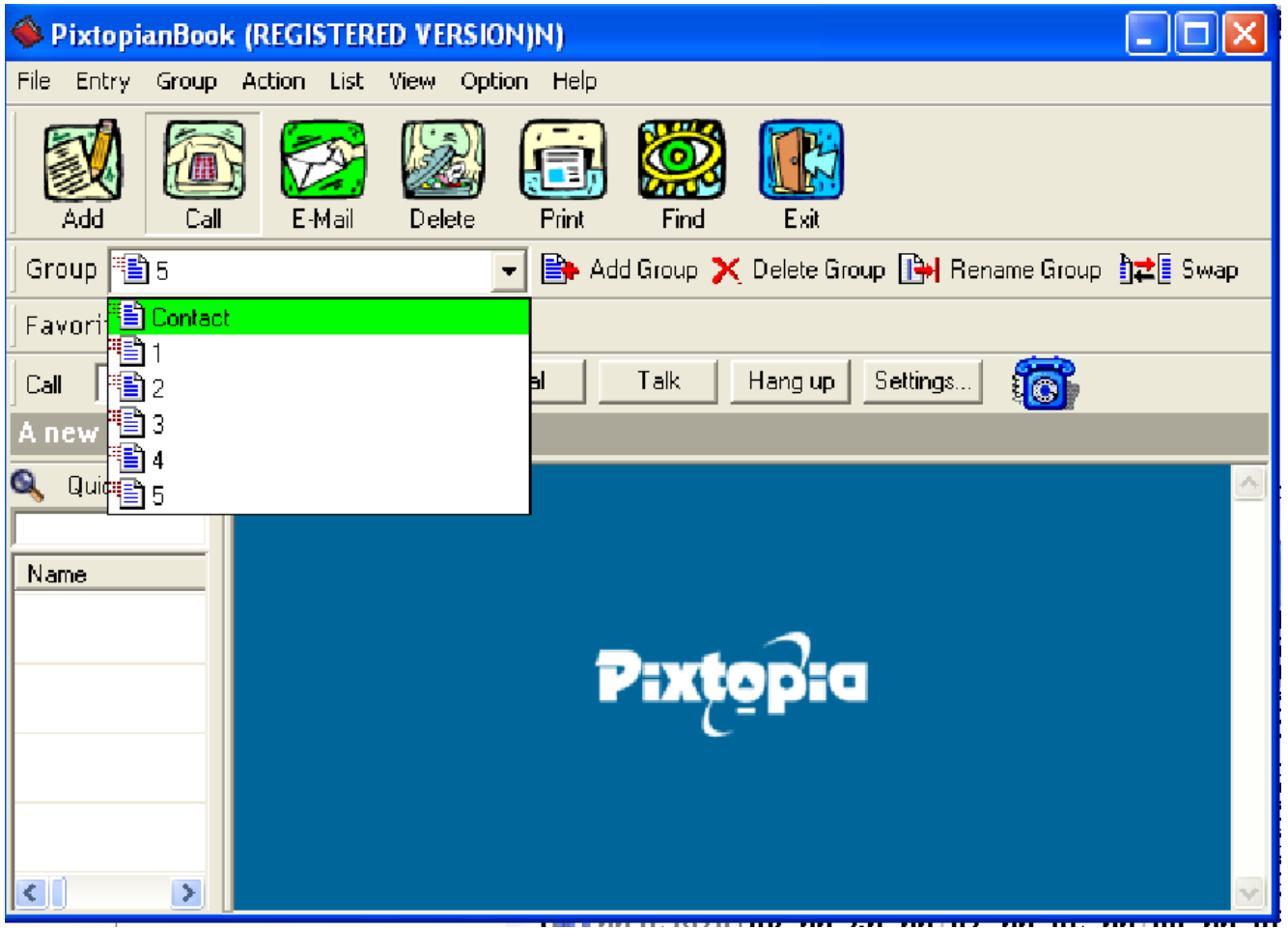




PixtopianBook2로 저장

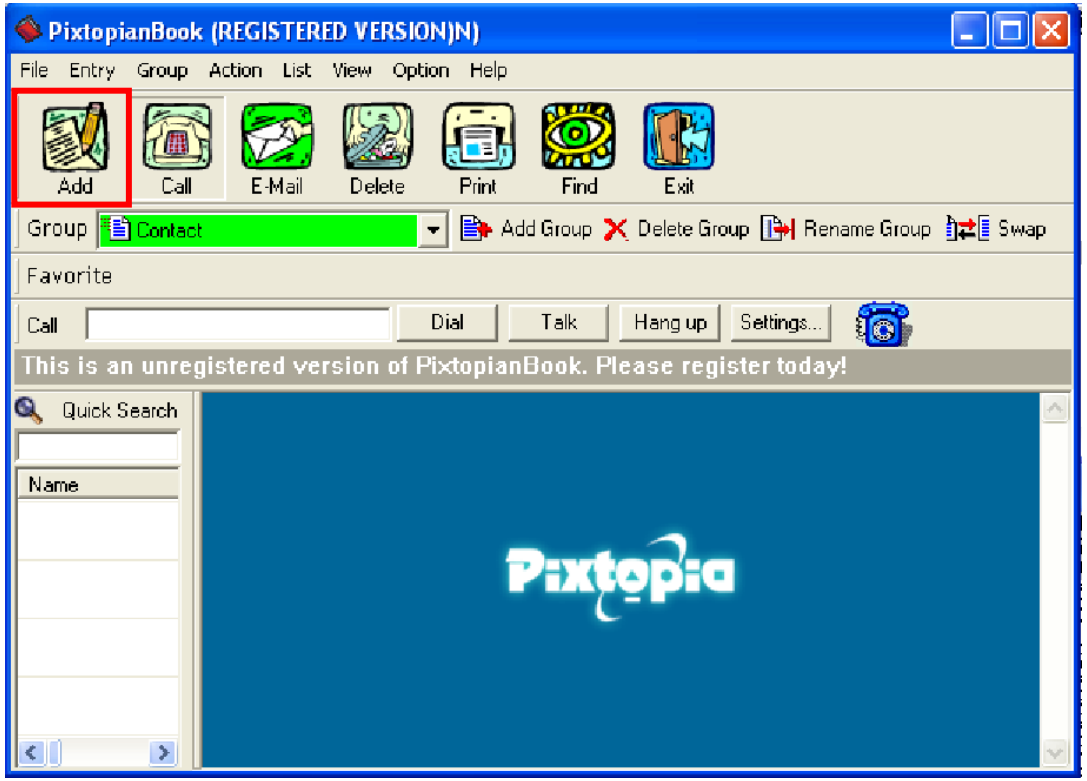
3. 문제 (3)의 솔루션 - 우회 (결과)

4개 이상 추가 가능해짐



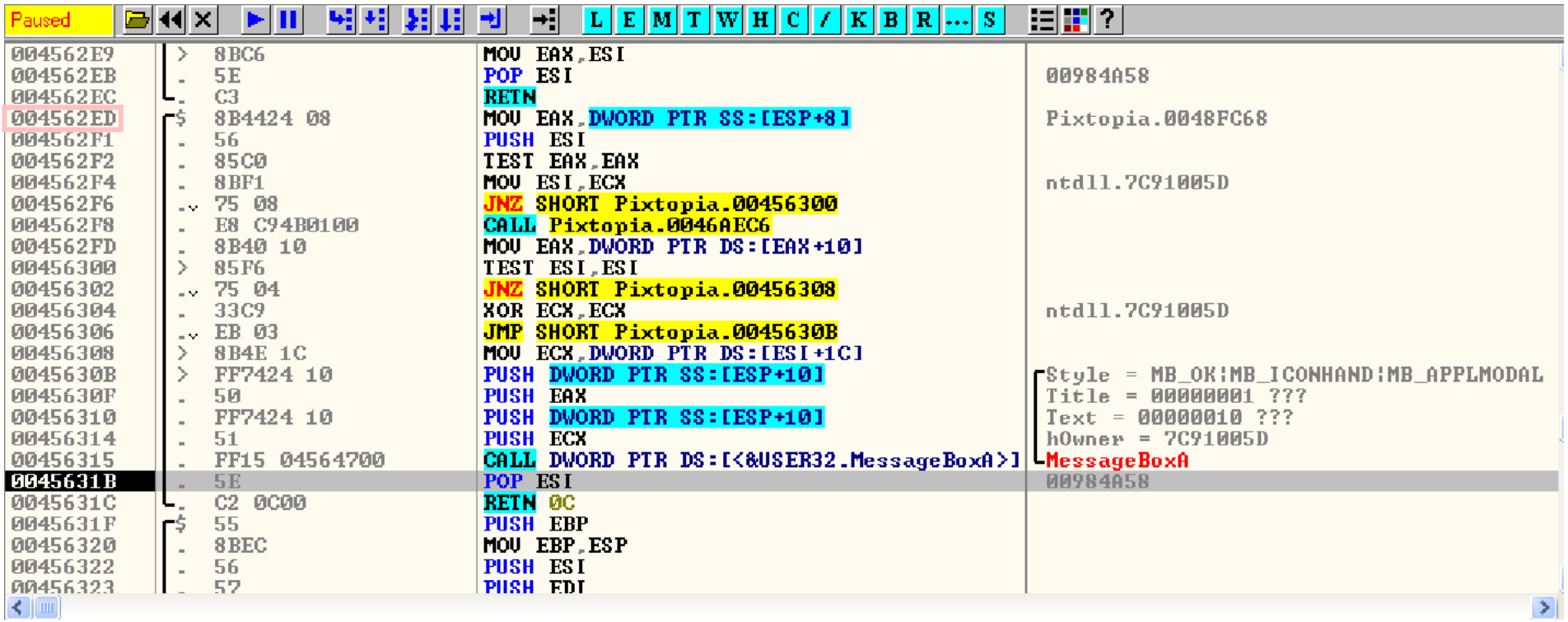
3. 문제 (4) 등록 인원수 제한

사용자 추가

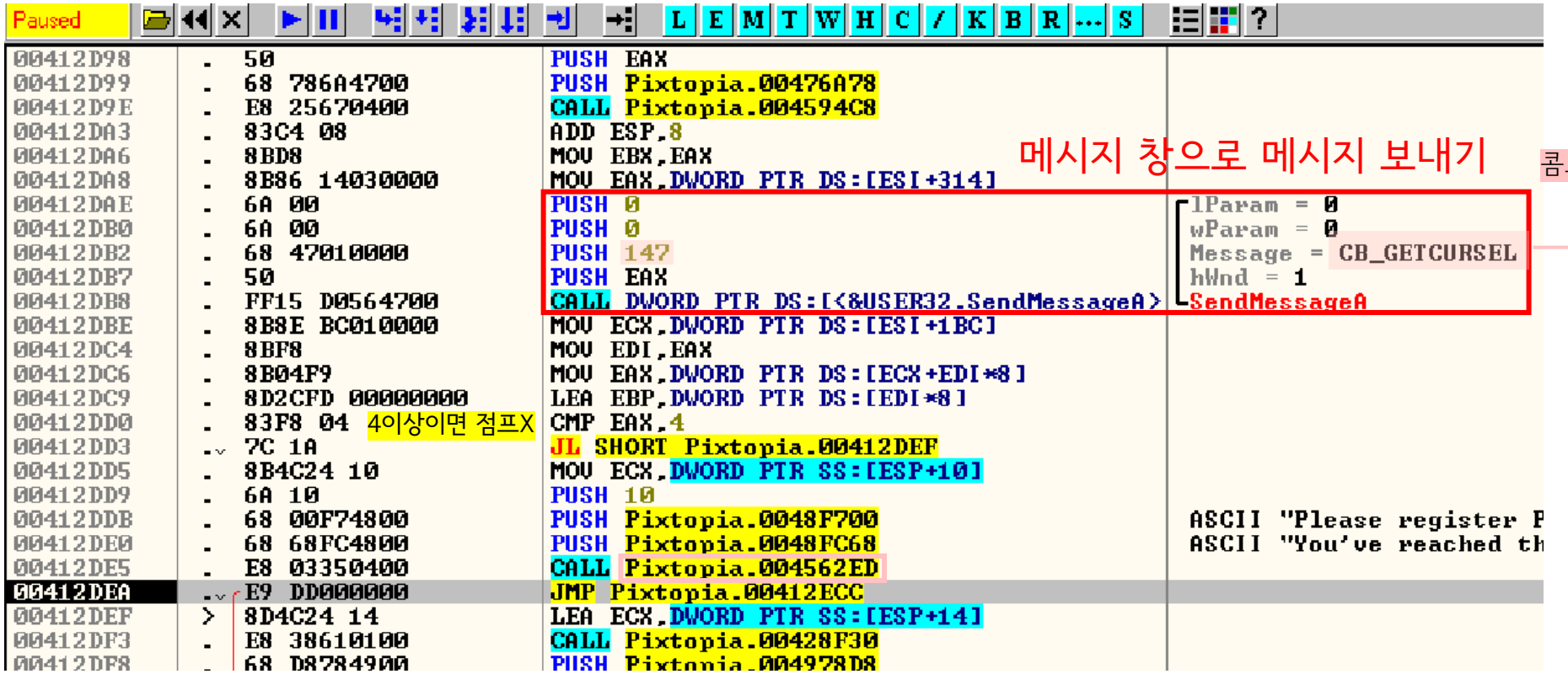


최대 4명까지만 사용자 추가 가능

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

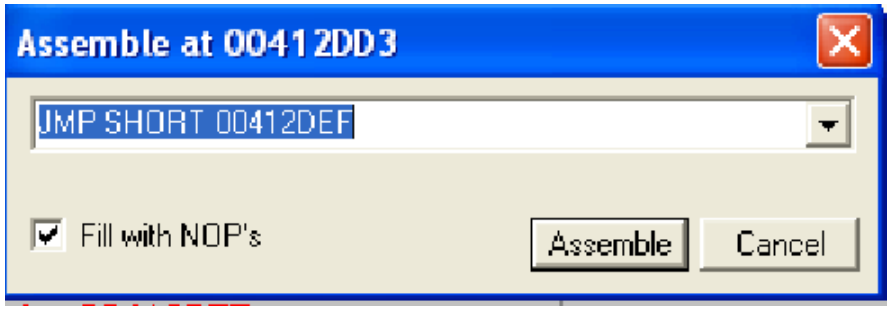


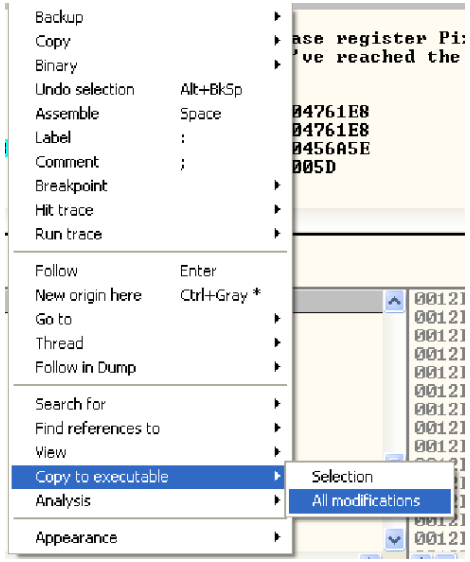
3. 문제 (4)의 솔루션 - 우회 (SendMessageA)

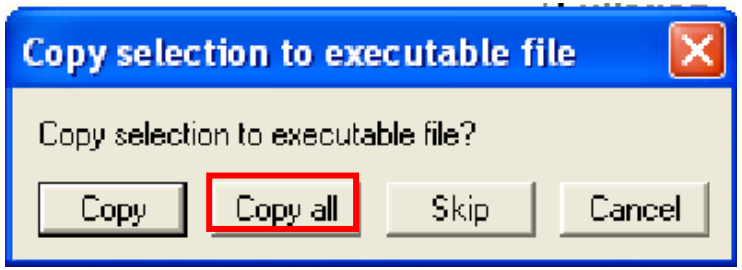


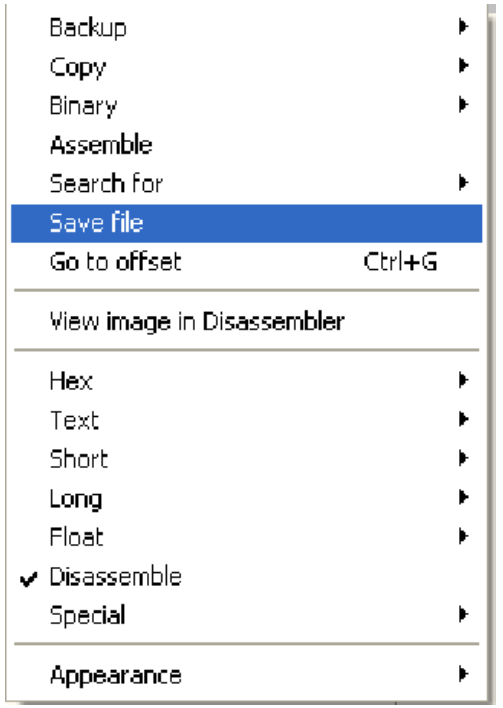
콤보 상자의 목록 상자에서 현재 선택한 항목의 인덱스를 가져오는 함수

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





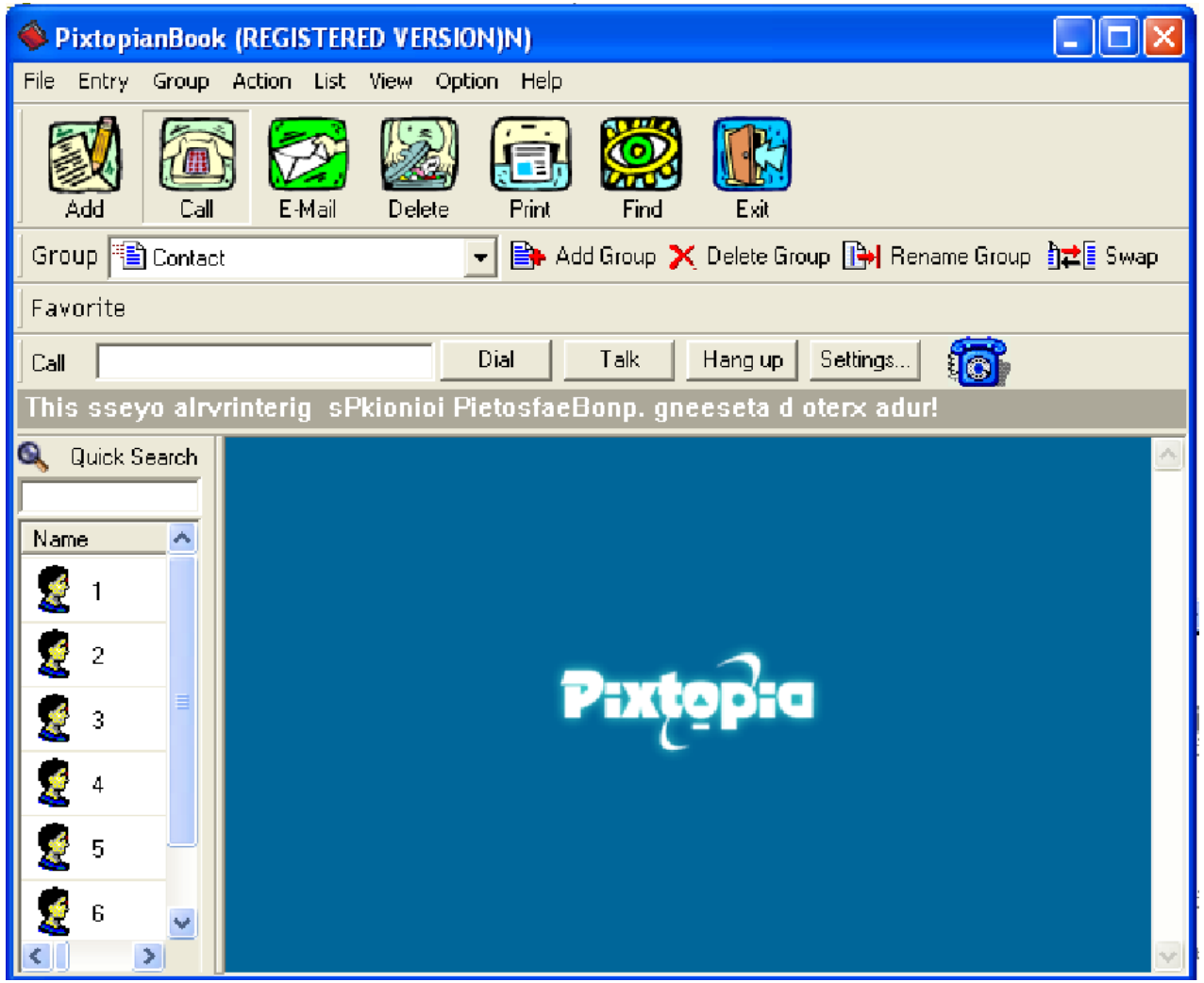




PixtopianBook3으로 저장

3. 문제 (4)의 솔루션 - 우회 (결과)

5명 이상 추가 가능해짐



감사합니다