# Reverse Engineering

## OllyDbg로 쉽게 디버깅하기 - Back to User 모드

이름: 김 연재 ( http://hisjournal.net/blog )
소속: CERT-IS ( http://www.cert-is.com )

Table of Contents

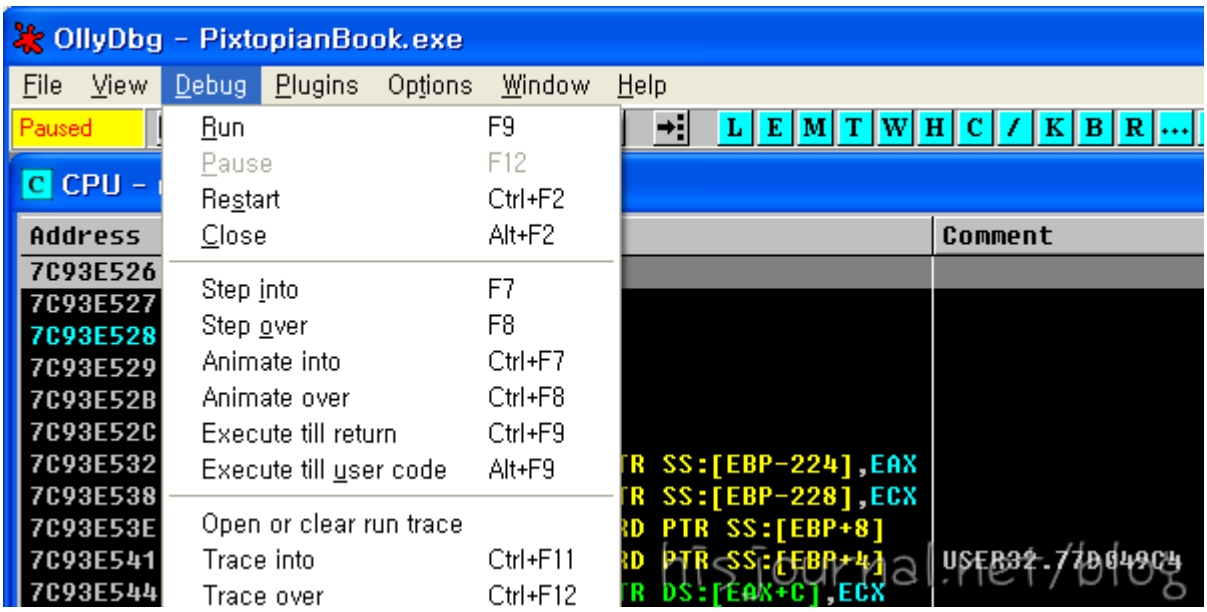
OllyDbg는 Back to User 모드라는 기능을 지원하고 있습니다. 소스가 만 줄짜리인 프로그램을 처음부터 끝까지 맨땅에 헤딩하듯이 분석하기란 너무나 고달프기에, 이 Back to User 모드를 사용합니다. 이 기능을 사용하면 처음부터 분석할 필요 없이 디버깅을 하고 싶은 부분만 쉽게 찾아갈 수 있습니다.

## Back to User 모드

예를 들여서 설명하죠.

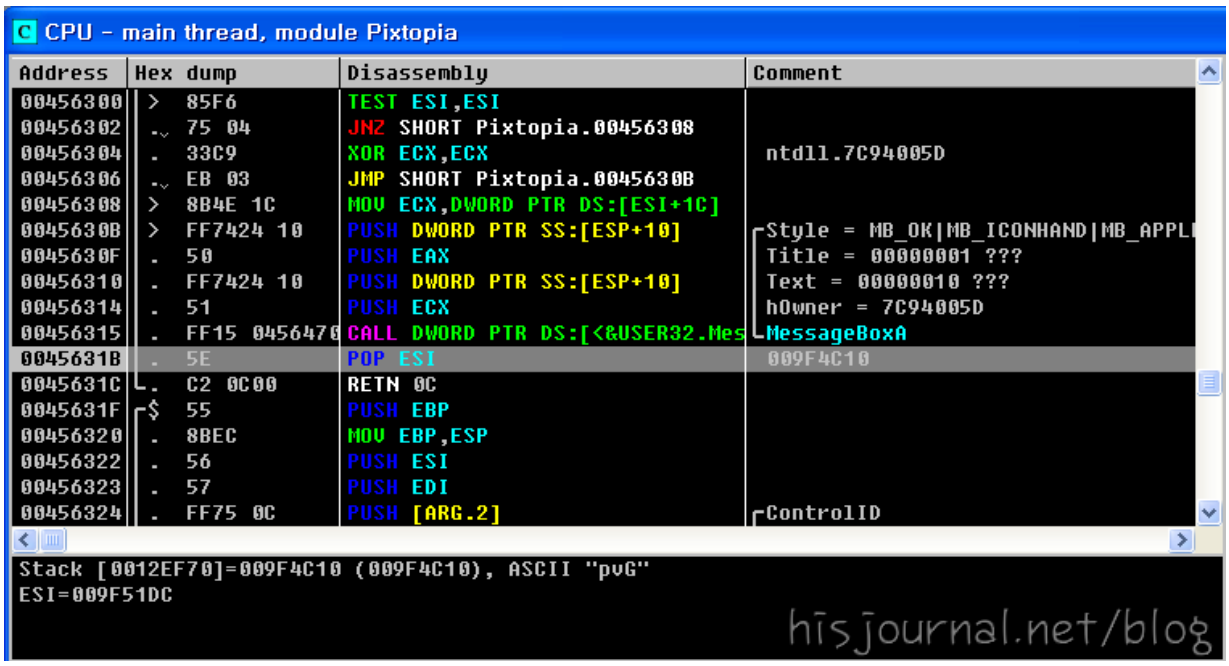

Lenas Reversing for Newbies 강좌의 4번 째 문제 파일입니다. 등록되지 않은 사용자는 하나의 그룹당 4명의 정보까지만 저장할 수 있는 제약이 있죠. 하지만 Back to User 모드를 이용하여 쉽게 우회할 수 있습니다.

우 선, OllyDbg로 프로그램을 불러온 다음 실행(F9)시킵니다. 그리고 위 그림처럼 디버깅하고 싶은 부분에서 프로세스가 멈추어져 있는 상태를 만듭니다. 메시지창을 띄운다던지, 사용자의 입력을 기다리던지 등으로요. 프로세스가 멈추어져 있지 않은 상태라면 Back to user 모드로 넘어가지 않고 단순히 Step over를 수행합니다. **꼭 프로세스가 멈추어져 있는 상태!!**




이제 디버깅을 일시정지(F12)합니다. 그러면 상태창에 Paused 라고 나오는데 이 상태에서 Execute till user code(Alt+F9)를 눌러 Back to user 모드로 들어갑니다. 성공하였으면 Back to user 라고 상태창에 나옵니다. 실패했으면? 그대로 Paused 이거나 Terminated 라고 나옵니다.

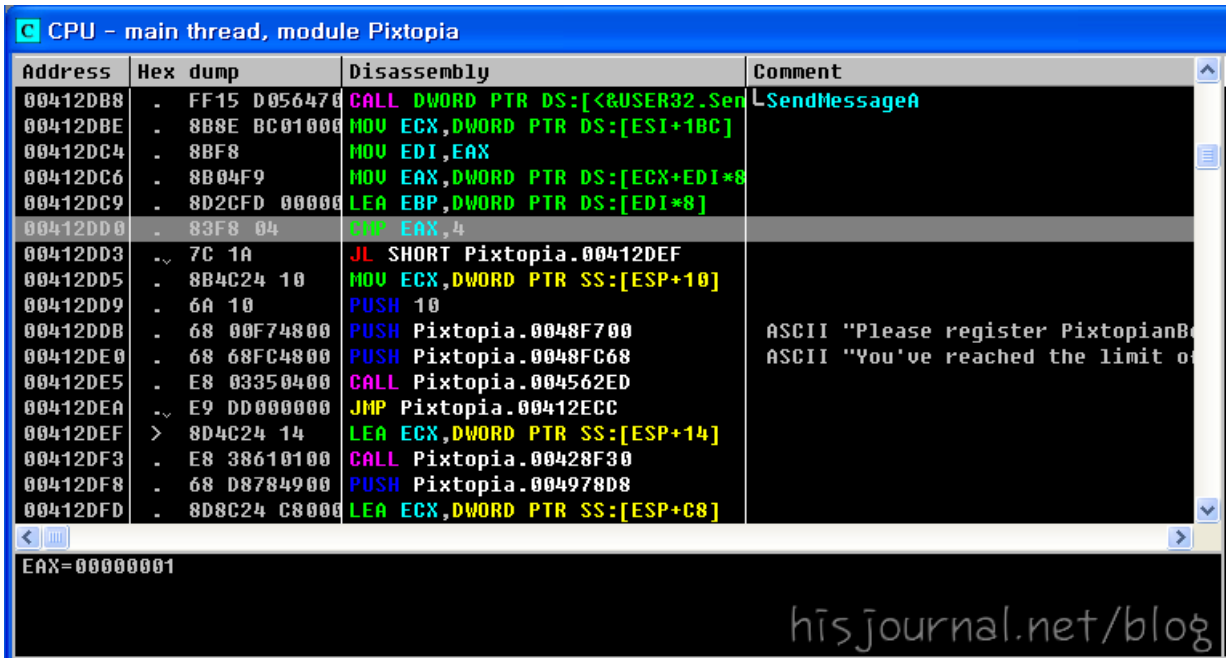
## 루틴 분석




Back to User 모드로 들어갔으면 아까의 메시지창에서 "확인" 버튼을 누릅니다. 그러면 OllyDbg가 알아서 마지막 함수의 call 이 끝난 지점을 찾아갑니다. 위 그림에서라면, MessageBoxA 함수가 call 되고 나서 그 다음 명령이죠. 즉, 이 지점 근처 어딘가에 등록 여부를 확인하거나 4명의 정보가 이미 저장되었는지 아닌지를 확인하는 어떤 루틴이 존재할

것이고, 우리가 원하지 않은 경우라면 MessageBoxA 함수를 call 한다는 것을 가정할 수 있습니다.

실제로 위 그림에서 *0045631C* 주소의 RETN 명령을 따라 가면, 아래 그림과 같은 루틴을 찾을 수 있습니다.




*00412DD0* 주소에서 어떤 변수와 4를 비교하는 것을 알 수 있는데, 이 부분이 이미 4명의 정보가 저장되었는지를 확인하는 루틴입니다. 우리는 여기서 우회를 함으로써 등록되지 않았지만 계속 정보를 추가할 수 있죠.

## 또 다른 예

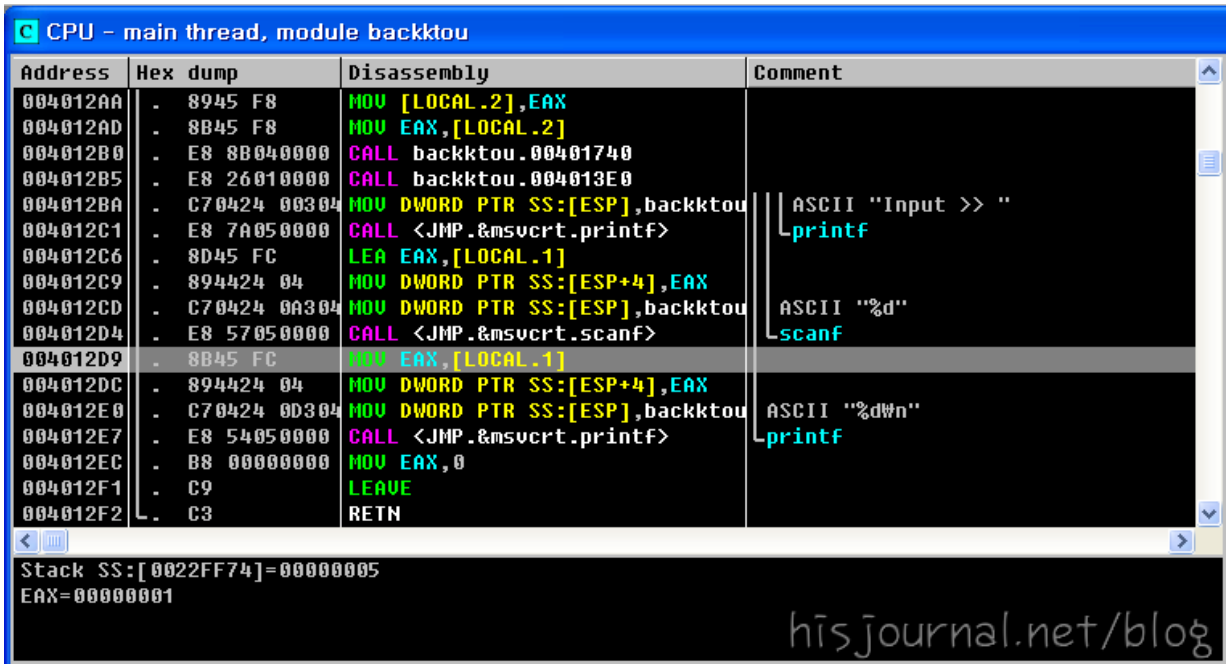
또 다른 예를 보겠습니다.

```
#include <stdio.h>
int main (void)
{
    int input;

    printf ("Input >> ");
    scanf ("%d", &input);
    printf ("%d\n", input);
```

```
    return 0;
}
```

이런 프로그램을 만들어보죠. 콘솔의 경우에는 메시지창이 안 뜰테니 사용자의 입력을 받기 위해 프로세스가 멈추어져 있는 상태를 만들어야 합니다. scanf() 함수가 대표적이죠.




이 프로그램의 사용자 입력 부분에서 Back to User 모드로 들어가면 위 그림처럼 루틴이 나옵니다. 역시 sacnf() 함수가 call 되고나서 다음 명령을 가리키고 있습니다.

이 처럼 Back to User 모드를 이용하면 디버깅을 하고 싶은 부분의 루틴을 쉽게 찾아갈 수 있습니다. 너무나 좋은 기능이죠. 하지만, 아쉽게도 프로세스가 멈추는 시점이 있어야 한다는 단점이 있어서 만능은 아닙니다. 그래도 왠만해서는 에러(혹은 경고) 메시지가 뜨는 경우가 많은니 충분히 유용할 겁니다. 잊어서는 안 될 것은, Back to User 모드를 이용하려면 프로세스가 멈춘 상태이어야 한다는 것! 꼭 기억하세요!