# IDA Pro에서 코드 패치 하기

- DS

일반적으로 IDA pro에서는 바이너리의 수정이 불가능하다. 그 이유는 IDA pro는 코드 바이너리의 이해를 돕기 위하여 설계가 되었기 때문이다. 하지만 메뉴 중 File > Patch Program 이나 File > Produce File > Create EXE File?는 왜 있는 건일까?

## 1. Edit > Patch Program

IDA를 실행시키고 Edit 메뉴를 훑어 본 사람이라면 위에서 언급한 Patch Program이 없다는 것을 의아하게 생각할 것이다. Patch Program은 숨겨진 메뉴이기 때문에 설정 파일을 조작해야 한다.

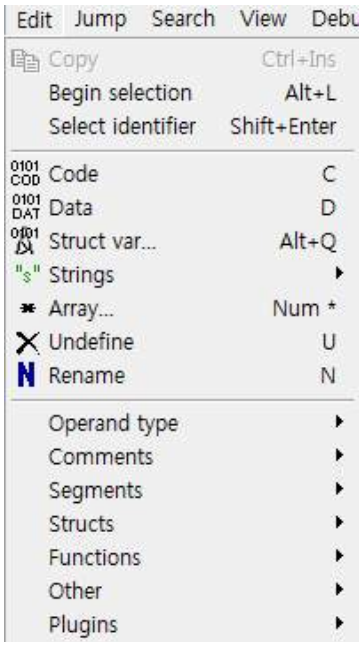


그림 1 기본적인 EDIT 메뉴

설정파일을 조작하기 위해서 IDA pro가 설치된 폴더에 cfg에 있는 idagui.cfg 파일을 텍스트 에디터로 열어보자.

수많은 환경 설정이 보인다. 이에 관한 내용은 IDA pro book[1]의 Chapter 11을

1) C. Eagle, The IDA pro book, No starch press, 2008

참고하기 바란다.

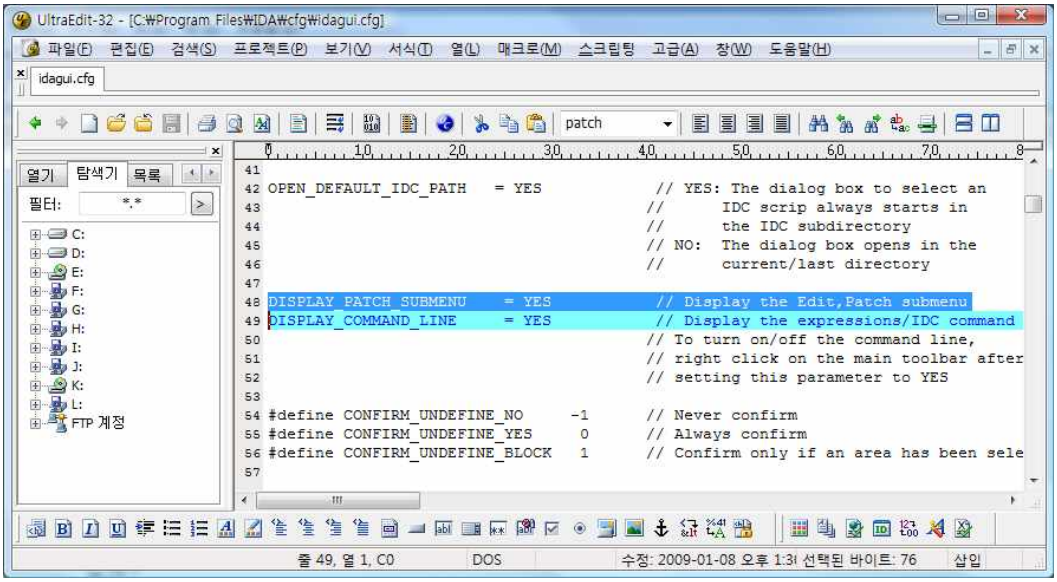


그림 2 idagui.cfg 파일

이중에서 DISPLAY_PATCH_SUBMENU를 YES로 바꿔 주고 IDA pro를 다시 실행해 보면 EDIT 메뉴에 'Patch Program' 메뉴가 생긴 것을 확인 할 수 있다.

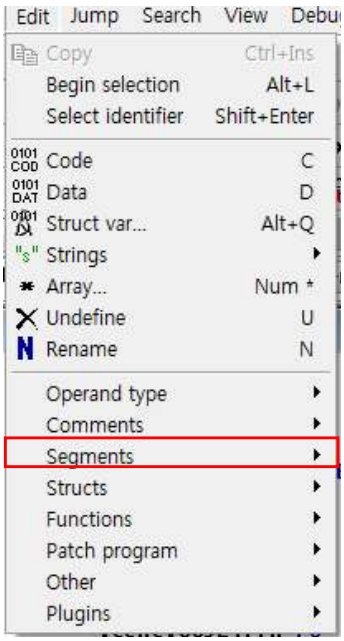


그림 4 설정 변경 후 EDIT 메뉴

Patch Program에는 세 개의 하위 메뉴가 있으며 각 메뉴에 대한 설명은 다음과 같다.

- Change Bytes

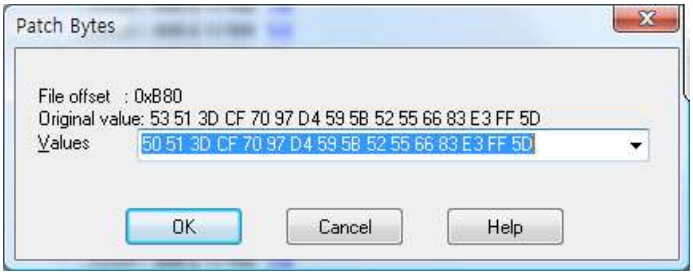


그림 5 Patch Bytes Dialog

커서의 위치부터 16 바이트의 값을 읽어와 출력해 주며 수정 할 수 있게 해준다.

- Change Word


그림 6 Patch Word Dialog

상대적으로 덜 유용한 Change Word 메뉴는 Word 값을 변경 할 수 있게 해준다.

- Assemble

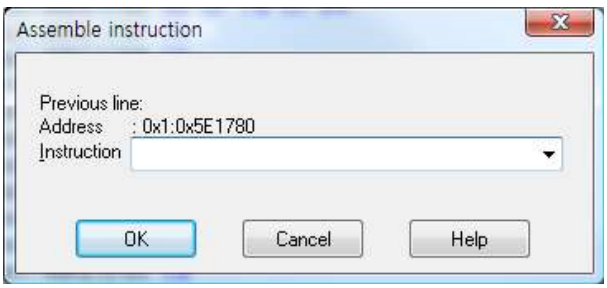


그림 7 Patch Assemble Dialog

마지막으로 가장 유용하다고 볼 수 있는 Assemble은 Assemble 명령을 입력하여 코드패칭을 할 수 있다. 하지만 모든 프로세서에 가능한 것이 아니기 때문에 불가능한 프로세서인 경우 “Sorry, this processor module doesn't support the assembler." 라는 메시지를 출력한다.