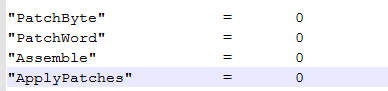
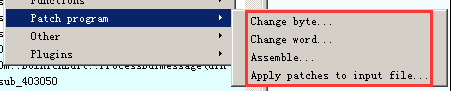
# 1.功能选项

Edit->Patch Program菜单是GUI版本的IDA的一项隐藏功能，用户需要编辑idagui.cfg配置文件才能激活该菜单。

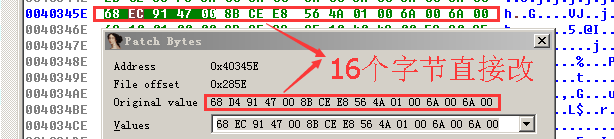


可用选项如图所示



# Change byte

用于编辑IDA数据库中的字节值。相关的字节编辑对话框如图所示 。



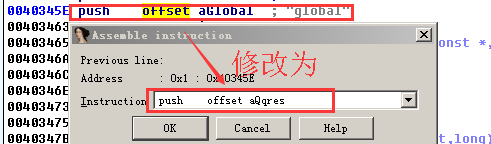
这个对话框显示了从光标所在位置开始的16个字节的值。你可以更改显示的部分或全部字节。   
同时,Address表示了虚拟地址，File offset表示了文件偏移量。实际上，Hex View可以直接改字节，右键Edit即可。

# Change word

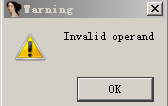
功能更有限，感觉没必要介绍了。

# Assemble

利用“汇编”选项可以输入使用一个内部汇编器汇编的汇编语言语句。然后，IDA会将得到的指令字节写入当前的屏幕位置。



但不如人愿：



点击最右边的Help，我们可以找到答案：

This command allows you to assemble instructions. Currently, only the IBM PC processors provide an assembler, nonetheless, plugin writers can extend or totally replace the built-in assembler by writing their own.

The assembler requires to enclose all memory references into square brackets. For example:

mov ax, [counter]

Also, the keyword 'offset' must not be used. Instead of

mov eax, offset name

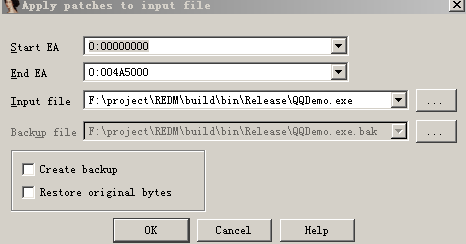
you must write

mov eax, name

所以写成push aQqres就OK了。

# Apply patches to input file

把改动更新到二进制文件中



# DIF显示被修改的地方

Produce file▶Create DIF file

DIF文件是一个纯文本文件，其中列出了一个IDA数据库中所有被修改的字节。

这个文件的第一行是注释，第一行是最初的二进制文件的名称，随后则是文件中被修改的字节列表。每一行都指出被修改的字节的**文件偏移量**（而非虚拟地址）、**字节的原始值**以及字节在数据库中的**当前值。**

