linux下的OllyDbg --- EDB

1、安装：

sudo apt-get install cmake build-essential libboost-dev \

libqt5xmlpatterns5-dev qtbase5-dev qt5-default \

libqt5svg5-dev libgraphviz-dev libcapstone-dev xterm

sudo apt install git

sudo git clone --recursive https://github.com/eteran/edb-debugger.git

cd edb-debugger

sudo mkdir build

cd build

sudo cmake .. 如出错 sudo apt-get install --reinstall pkg-config cmake-data

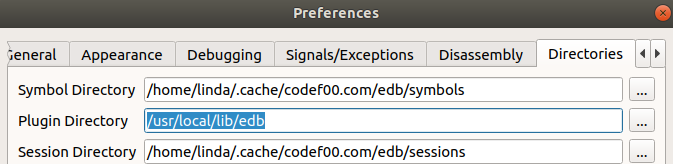
sudo make

这种方法安装的版本比较新目前1.3

sudo apt install edb-debugger安装的版本旧1.0

2、设定

edb参数设定（安装后的默认值）：



/usr/local/lib/edb

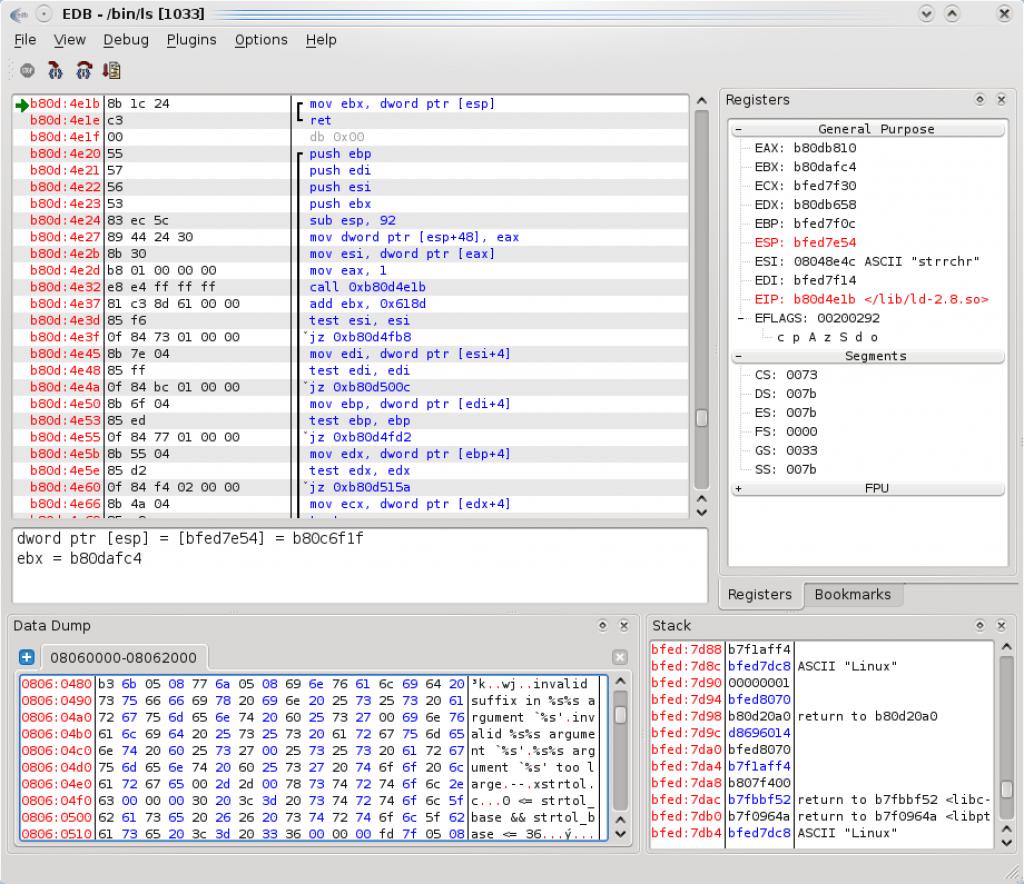
3、使用

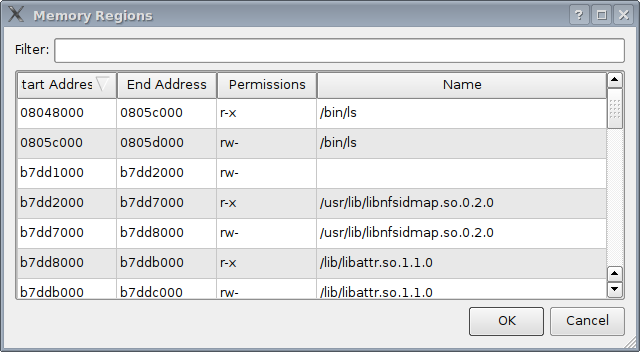
在windows下做过反汇编的人，估计都认识ollydbg这样软件。没错，ollydbg是window下做破解软件和反汇编软件人士的利器。现在介绍一个和ollydbg一样的软件，但它是在linux下运行的 --- EDG。

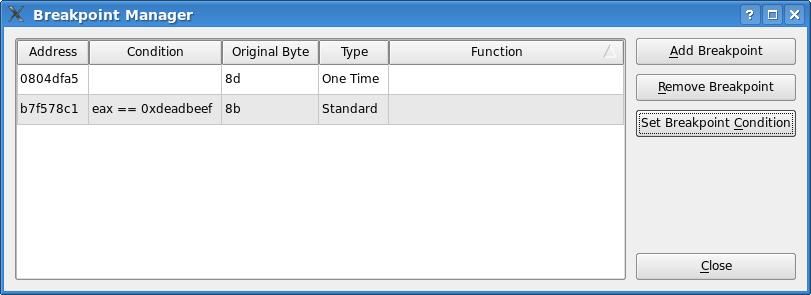
这个软件的作者本来是个软件反汇编人士，在windows下经常反汇编各种没有开源的软件。但是苦于在linux没有这方面类似的软件（这就是linux下的好处，因为大多软件都开源了，所以也没什么人需要去反汇编这些软件，哈哈），作者就自己亲自写了一个，并且还开了源。

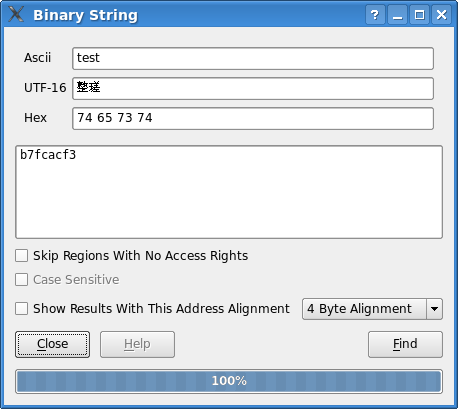
软件使用了QT4.5以上和boost1.35以上版本来编译。

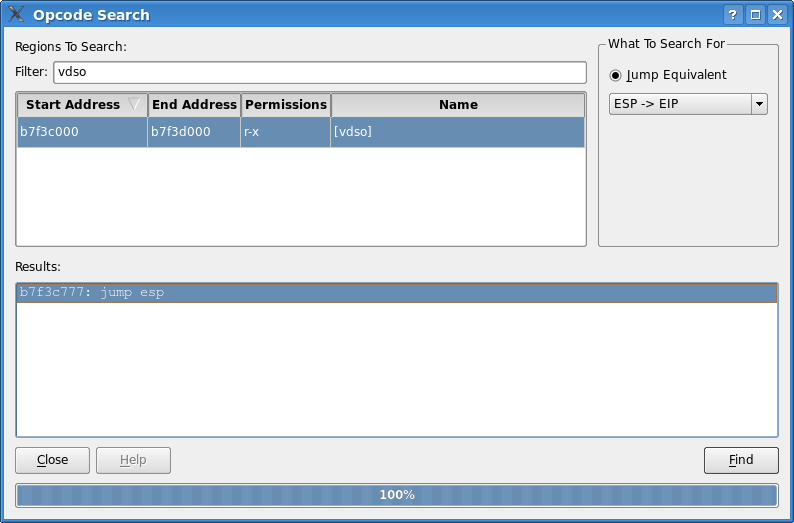
现在来看下这个软件的几个截图：











想要做linux下的反汇编程序的就用得上这个软件了，但是，我觉得这个软件的最大好处就是开源，那么你就可以知道别人是怎么制作这款反汇编的程序的，毕竟linux下那么多软件都是开源的，反汇编就显得不是那么必须。