目录

简介

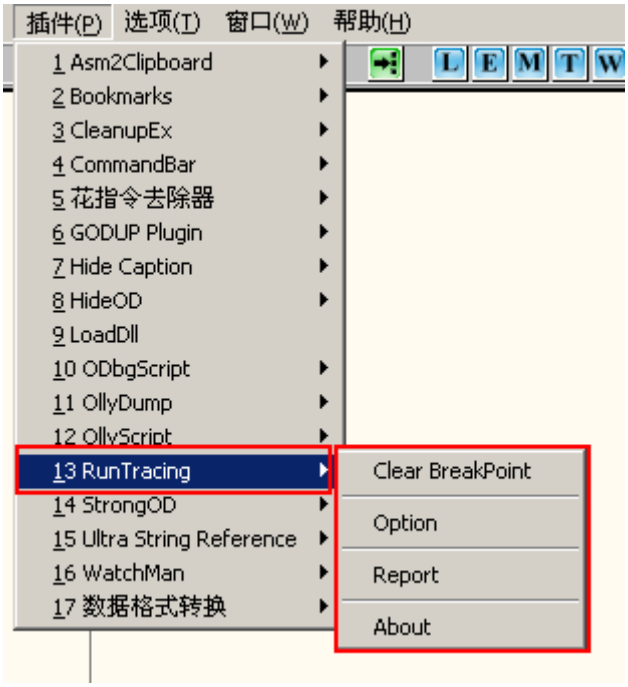
欢迎使用 **程序运行分析器** 。 程序运行分析器可以记录用户设定的地址范围内函数的调用情况。

要学习软件的具体使用方法，请详细阅读后面的章节。

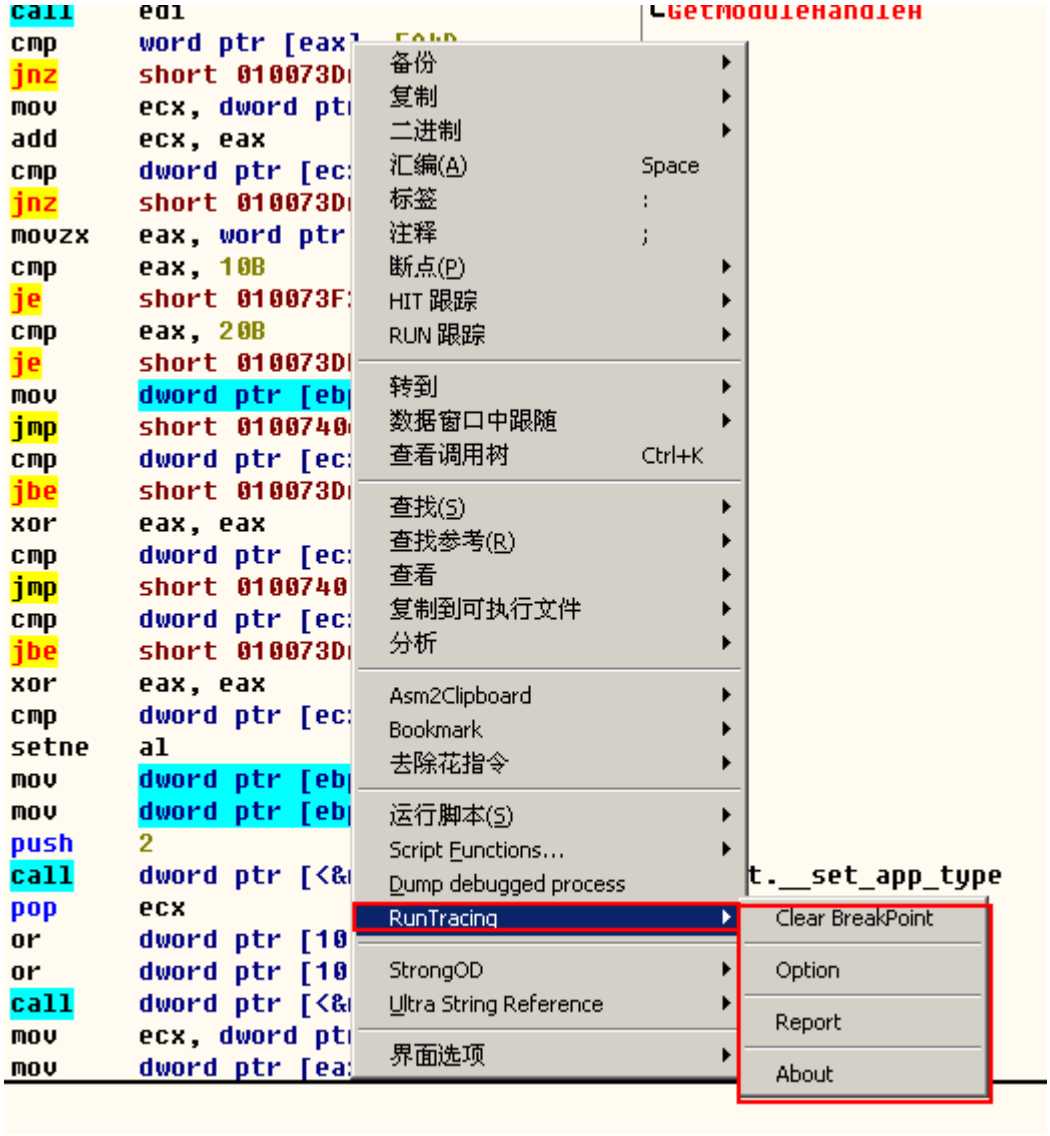
安装

将 runTracing.dll 文件放置 OD 插件目录（plugin）内即可。

当 od 加载插件之后，在插件菜单项中会多一项 RunTracing。



在反汇编窗口中右键也会有相应的菜单项



功能介绍

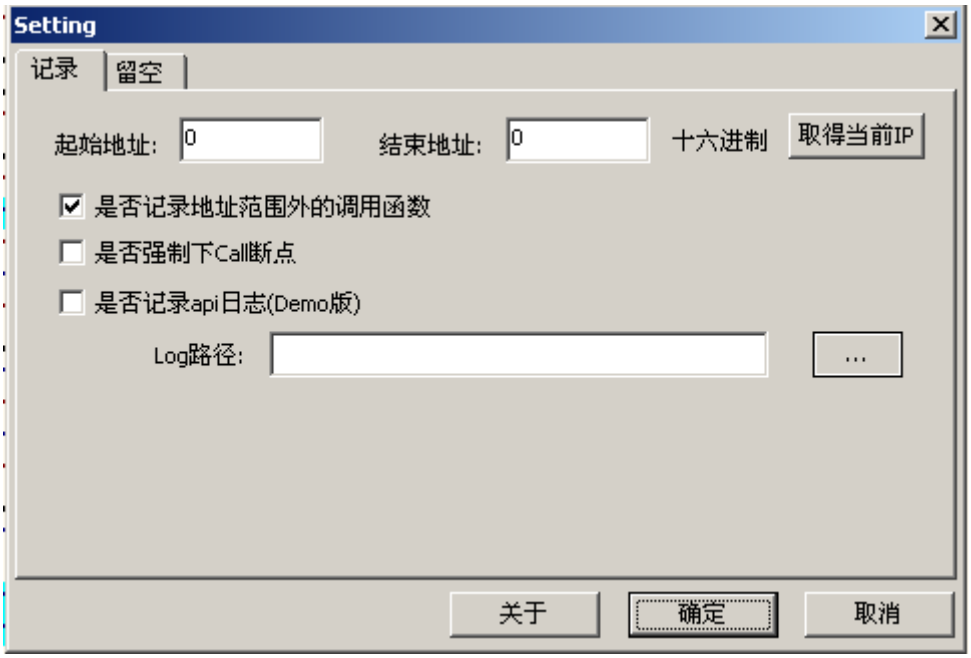
软件主要具有如下功能：

Clear BreakPoint：清除程序内所有的断点功能。

注：这个功能原本是内部功能，为了不让原来程序的断点影响程序运行分析器的功能。因为 od 的断点虽然可以一次全部禁止，但是不能一次全部删除，所以将此接口作为功能公开了。

Option: 程序运行分析器选项设置。

记录选项卡:



起始地址和结束地址：监控的地址。并不是程序的所有调用函数我们都感兴趣，所以可以在这里设置监控的地址范围，但是也并不是在地址范围内所有的 call 都会下断点，而是在起始地址开始到**所处的函数结束**或者到了**结束地址**内的 call 才会记录。而且对于调用地址外，再调用地址内的这样调用如果不开启记录地址范围外的调用函数是无法记录完整的流程。

取得当前 IP: 取得当前 EIP 的值，填入起始地址中。通过当前已选择 CPU 窗口的线程标识符去取得 EIP 的值。

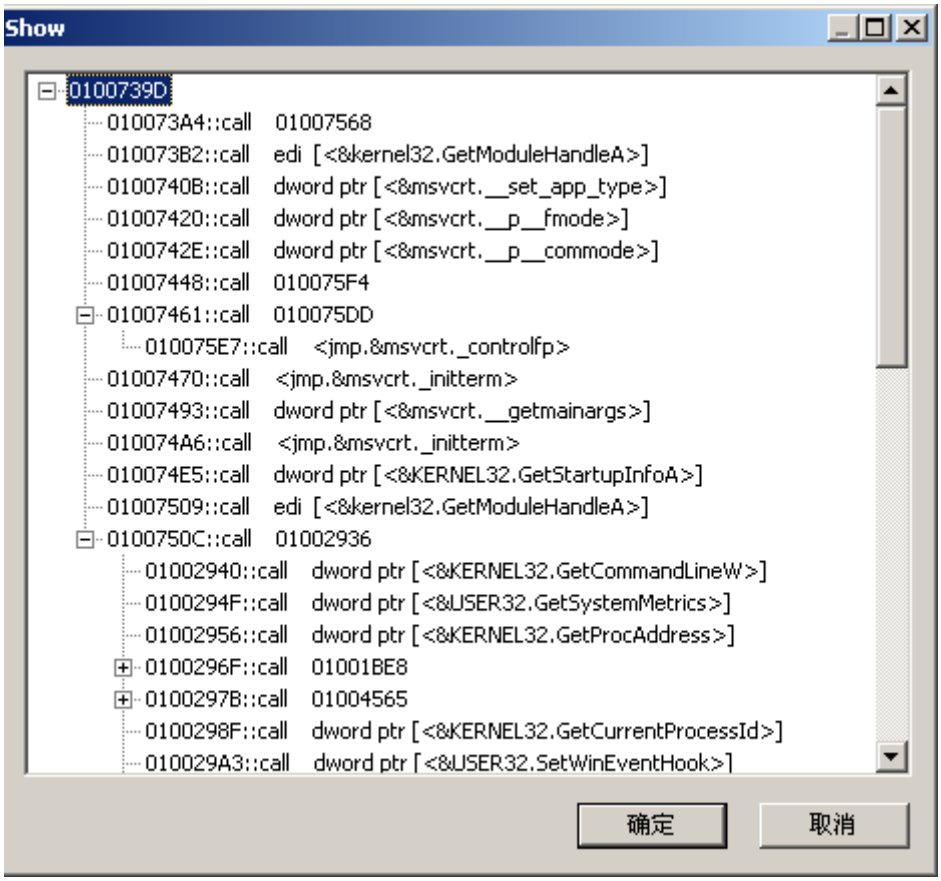
是否记录地址范围外的调用函数： 有时我们只是想知道，在某次调用中，都调用了哪些函数，而不用知道他完整的调用，就可以把此钩给去掉。否则可以钩上此项。

是否强制下 Call 断点: 因为本程序是作为 od 插件形式开发的，使用的都是 od 的一些接口。对于一些 od 无法识别的函数，本程序也无法做判断，为了程序能够正确执行，对于无法识别的函数不作处理，将选择权交给用户，用户根据实际情况来选择是否需要强制下断点。**建议钩上此项**。

是否记录 API 日志: 以后扩展功能。

原定是这里实现一个小型的词法解析，可以根据一些头文件的定义，去读相关的参数内容，记录下来。

信息展示:



以树状形式展示程序执行顺序。

跳转:

选中某一项，单击右键，可以将汇编窗口跳去那条指令处。

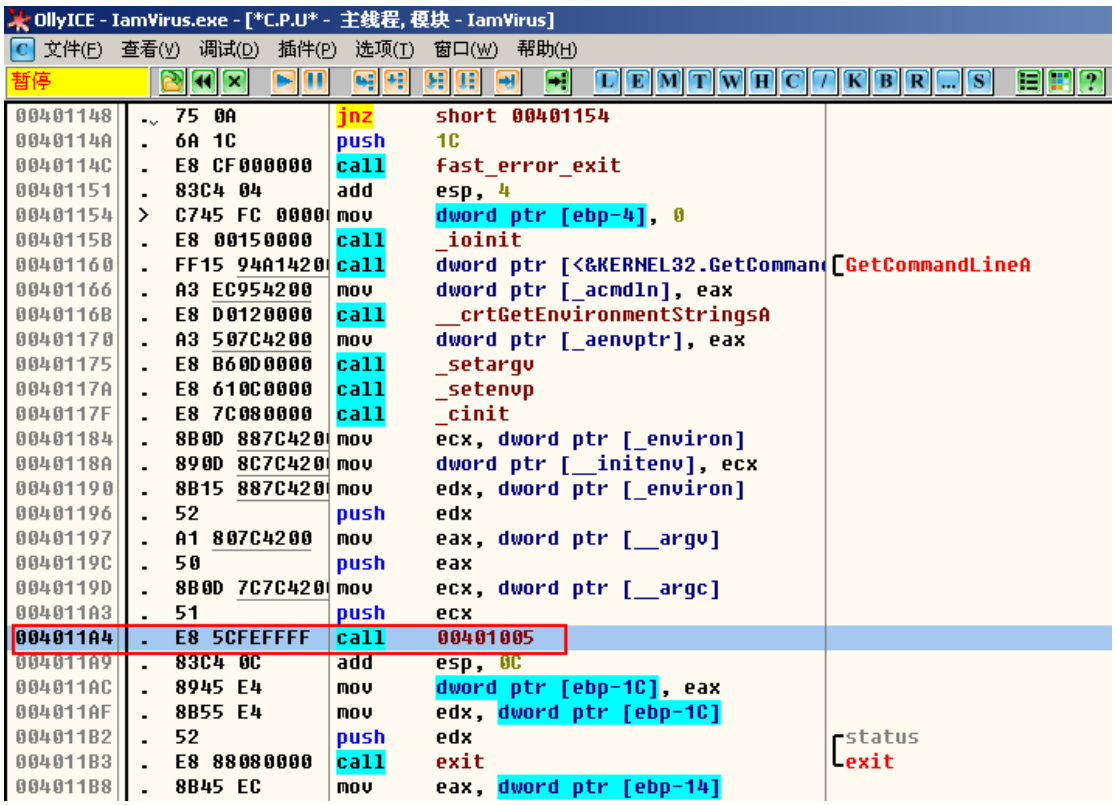
软件运行平台

操作系统: 凡是可以正常运行 OD,且 OD 加载此程序不出错。(有些改版的 OD 加载此 DLL 时会异常退出)。

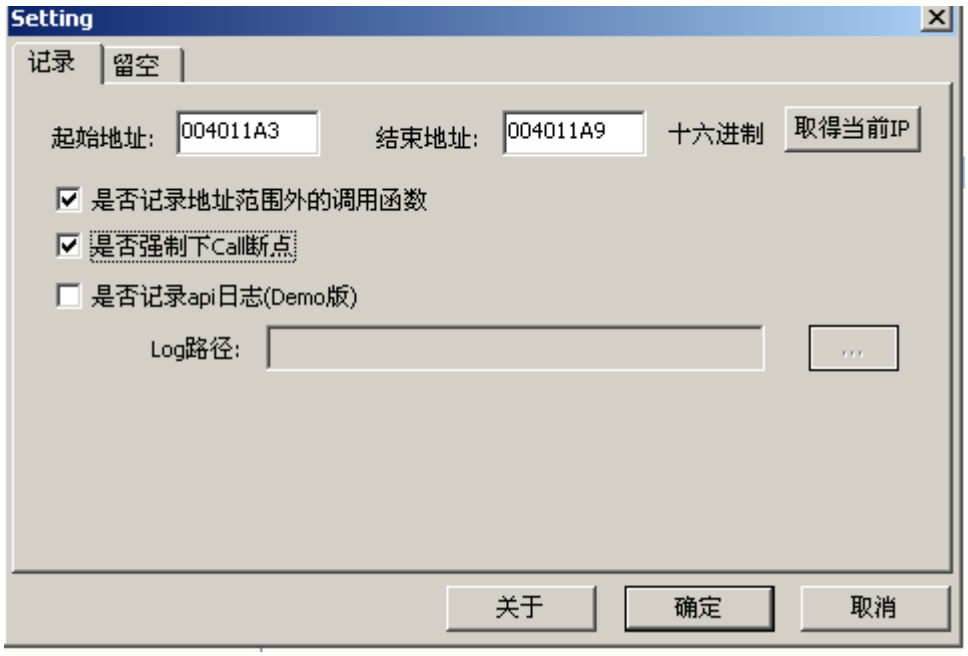
硬件配置：Intel 486DX with 64MB RAM(推荐 128MB 以上内存)

磁盘空间：10MB 以上的自由磁盘空间

使用示例



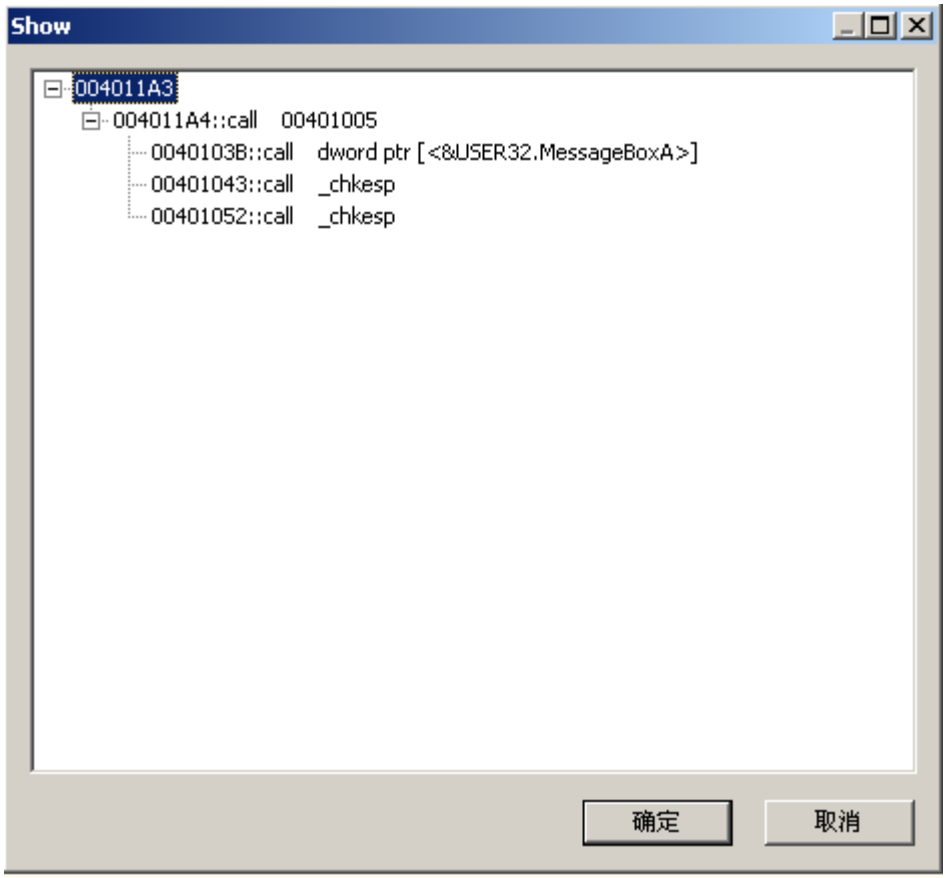
对于如上程序，我们只关心在 4011A4 里面程序做了什么，于是我们可以设置地址为 4011A4-4011a9，结束地址也可以是长度，**当结束地址小于 0x10000 的时候，程序是将结束地址当成长度来处理的。**所以上面结束地址输入 5 也是可以的。



对于起始地址，我们也可以按 F4 执行到 004011A3 处，然后点击取得当前 IP。

再按 F9 开始执行。

在程序运行中或者程序退出后，可以点击 Report 查看结果。



选中某一项，单击右键，可以将汇编窗口跳去那条指令处。