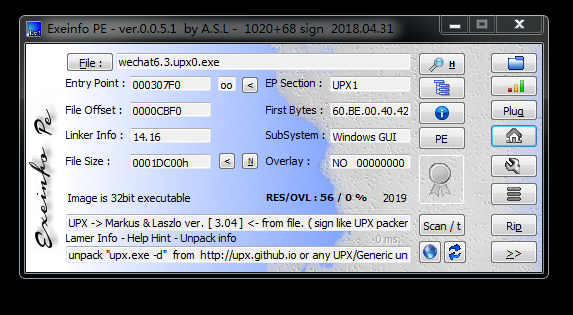
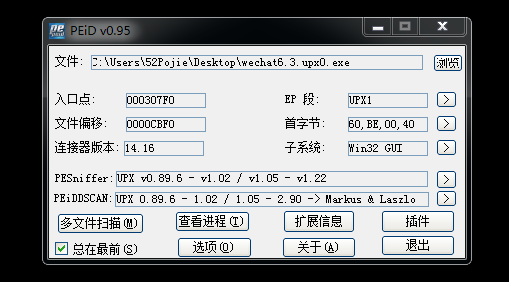
逆向分析

第一步：

查壳：

工具有PEID， EXEINFOPE 等多个 推荐使用Exeinfo PE ，最近更新2019.9.27；当然查壳软件需要多个，防止误查。





可以看到是一个UPX的壳

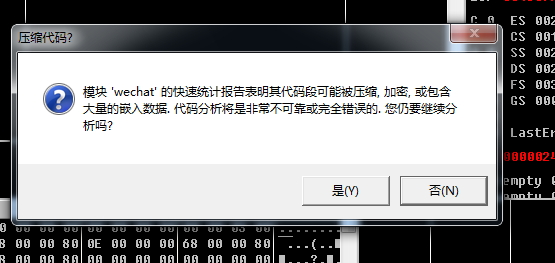
第二步：

脱壳：

直接用脱壳工具脱壳，注意脱壳软件适用的版本

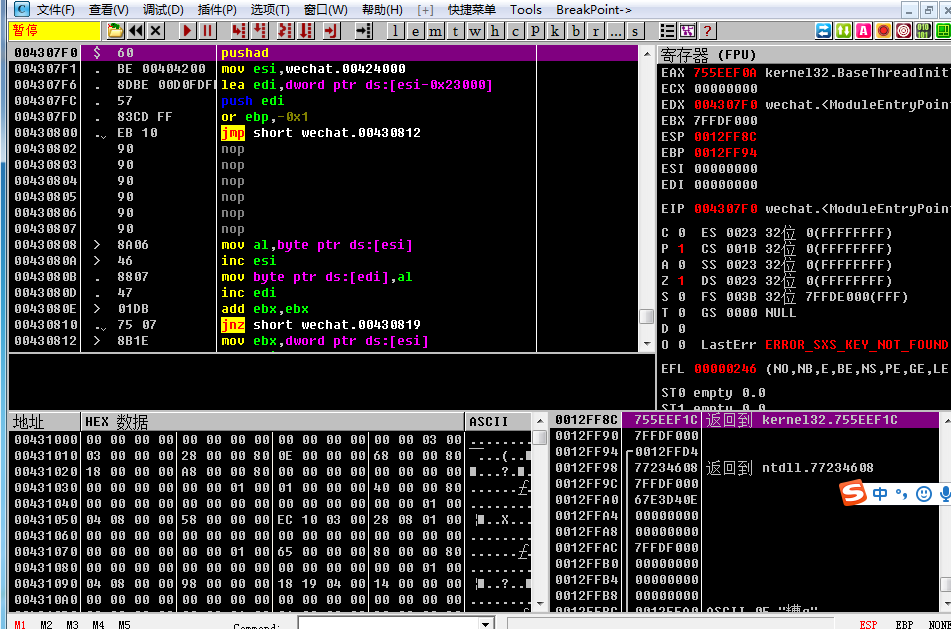
也可以手动脱壳，下面演示一下手动脱壳

使用OD 载入 目标文件，会出现下列提示



点击 是

来到壳的入口



下面我们使用ESP定律来脱壳

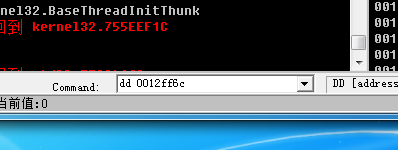
简单说下ESP定律：

ESP定律的原理是：堆栈平衡原理

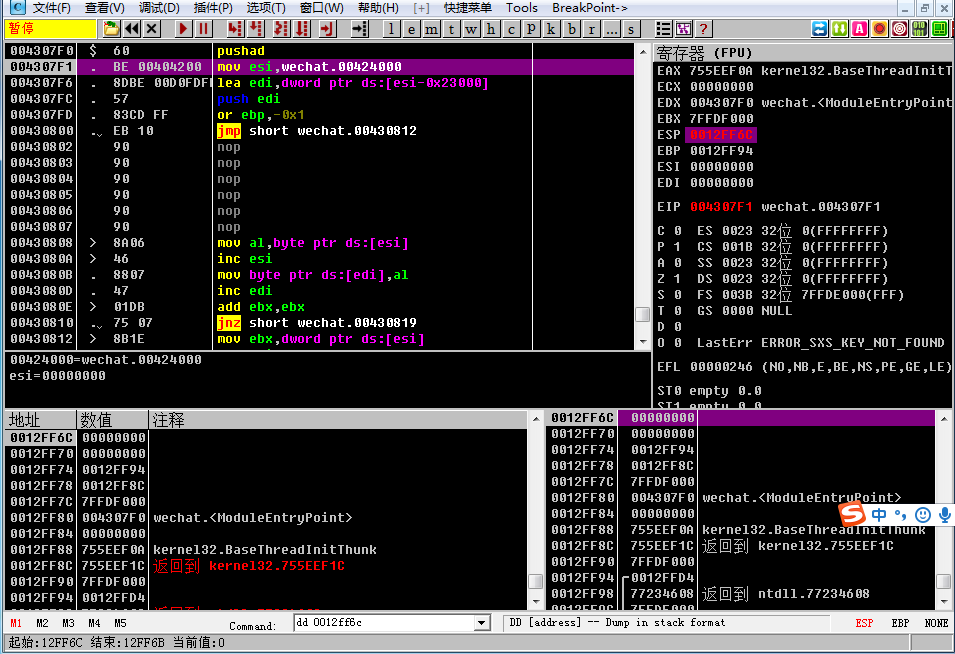
ESP定律使用的范围：几乎全部的压缩壳，部分加密壳

注意此时 寄存器窗口（FPU）的显示，单步F8，当FPU窗口中有且只有ESP和EIP变为红色的时候，右键点击FPU窗口中的ESP ，然后点击 “数据窗口跟随”。

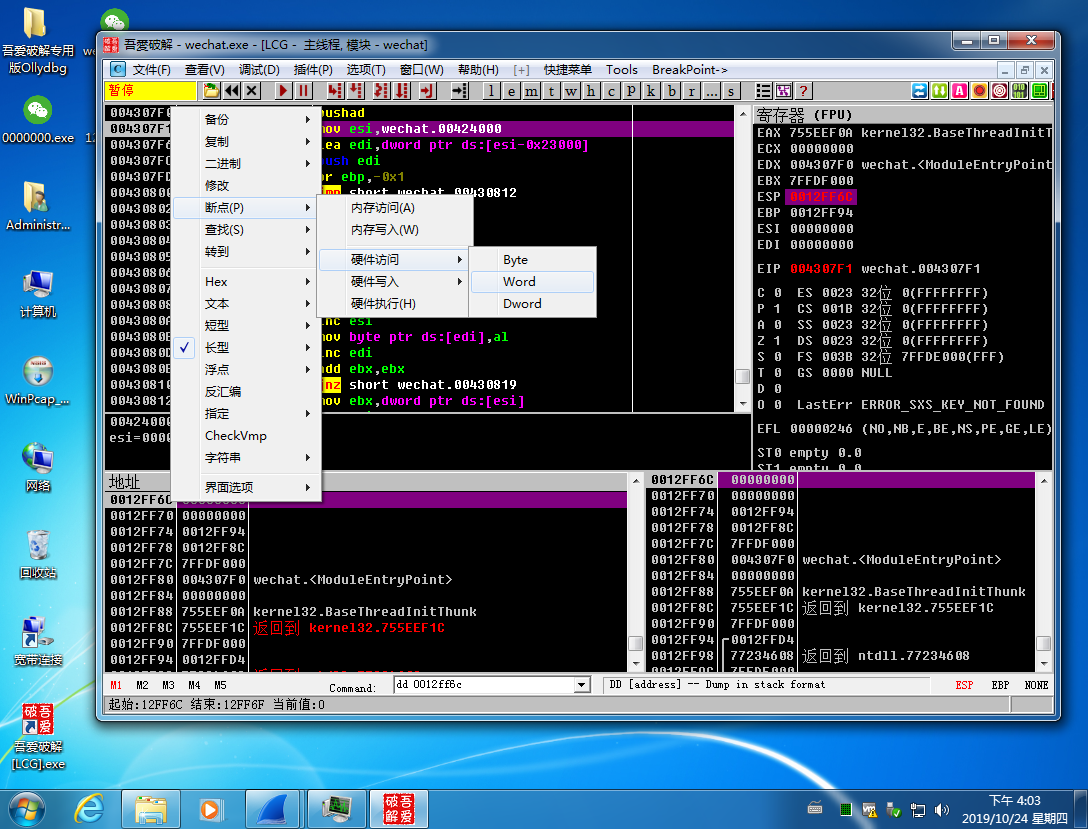
或者 下方command窗口中输入 DD ESP的值，如此次分析就是 DD 0012FF6C，敲击回车键



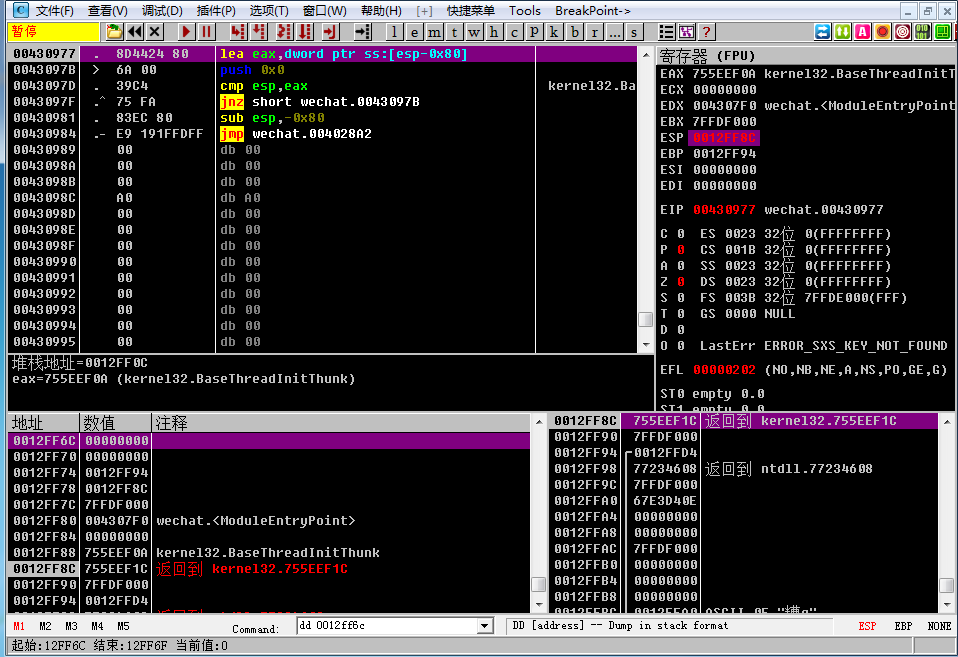
这两种方法都是来到数据窗口中的 0012FF6C 地址



在数据窗口中 0012FF6C 的数值栏中右键 下硬件访问断点

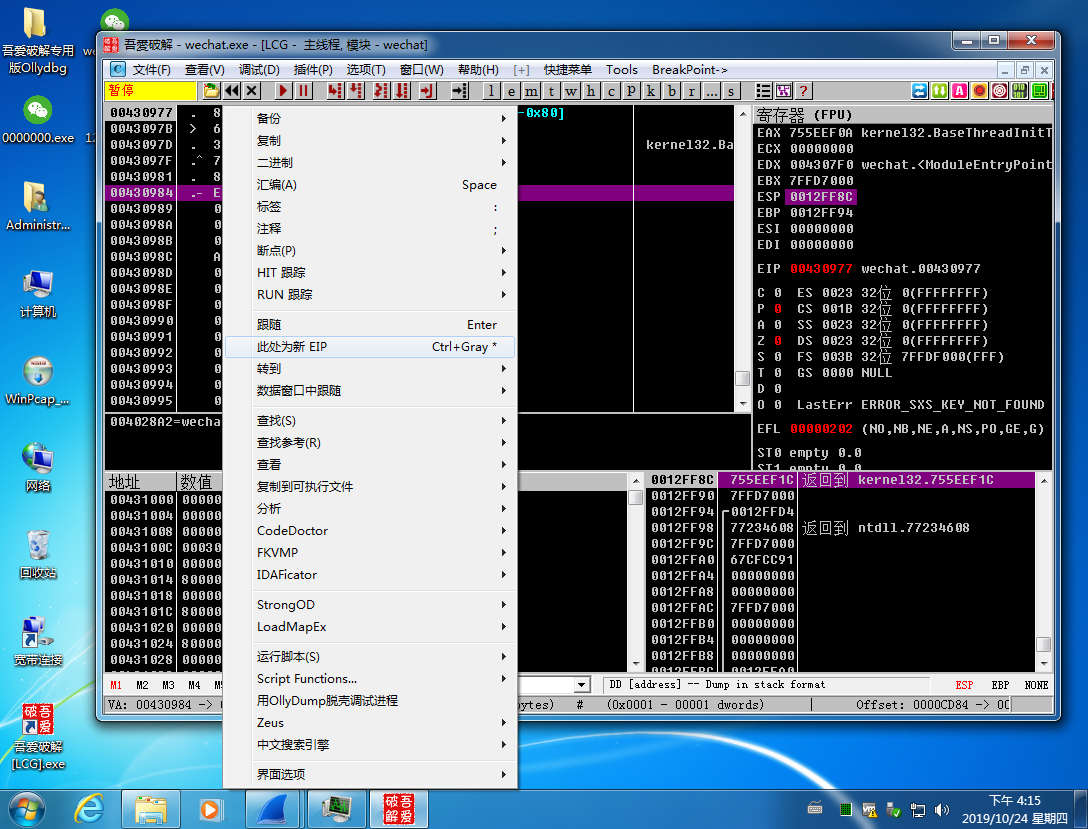


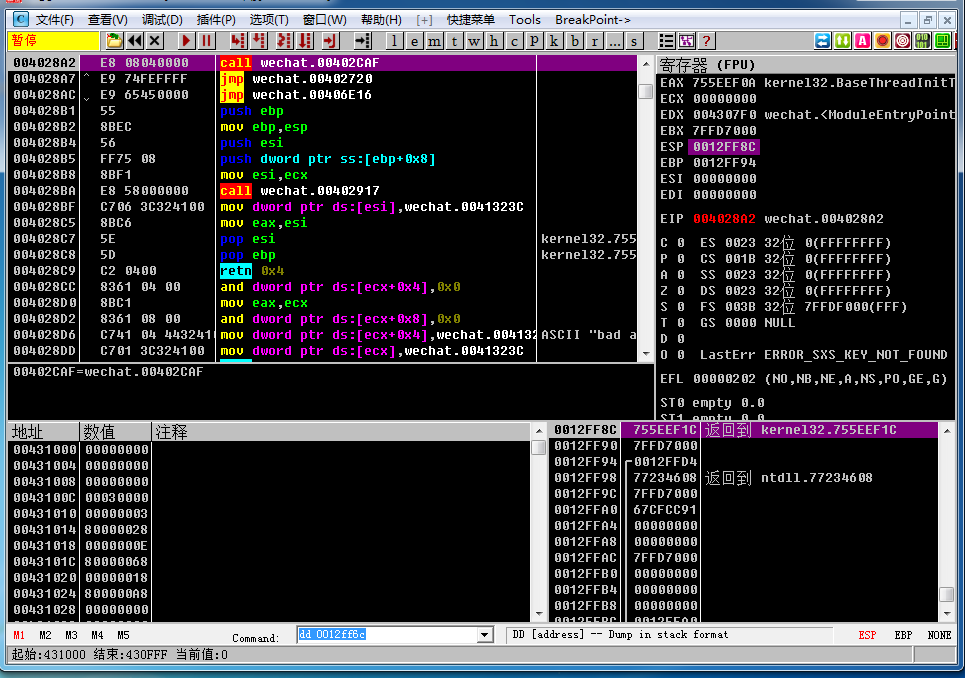
这个操作也可以在command窗口输入 HR 0012FFA4 回车后完成，然后我们按F9运行程序，此时程序会暂停在我们设置的断点位置



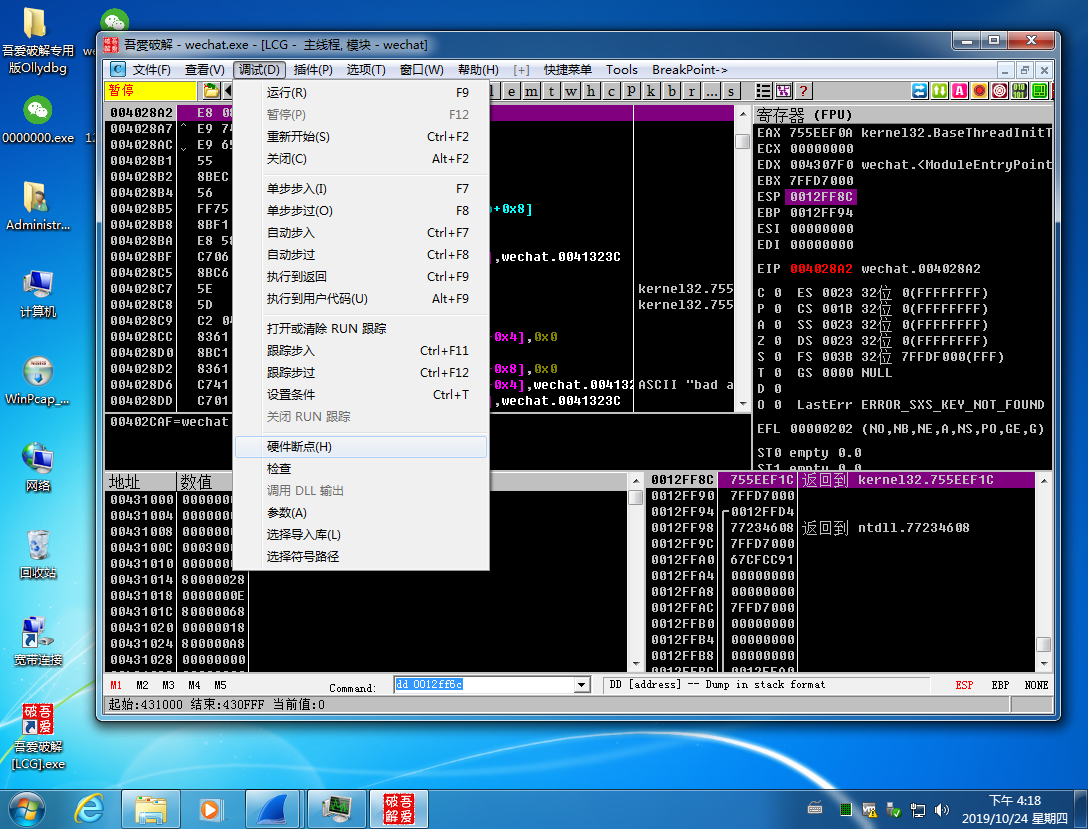
这个时候我们可以看到程序下面有一个非常显眼的大跳转，jmp wechat.004028A2就是我们需要的程序OEP

这时候在 jmp wechar.004028A2 上右键，选择 此处为新的EIP ，然后，F8 单步过，来到程序的领空

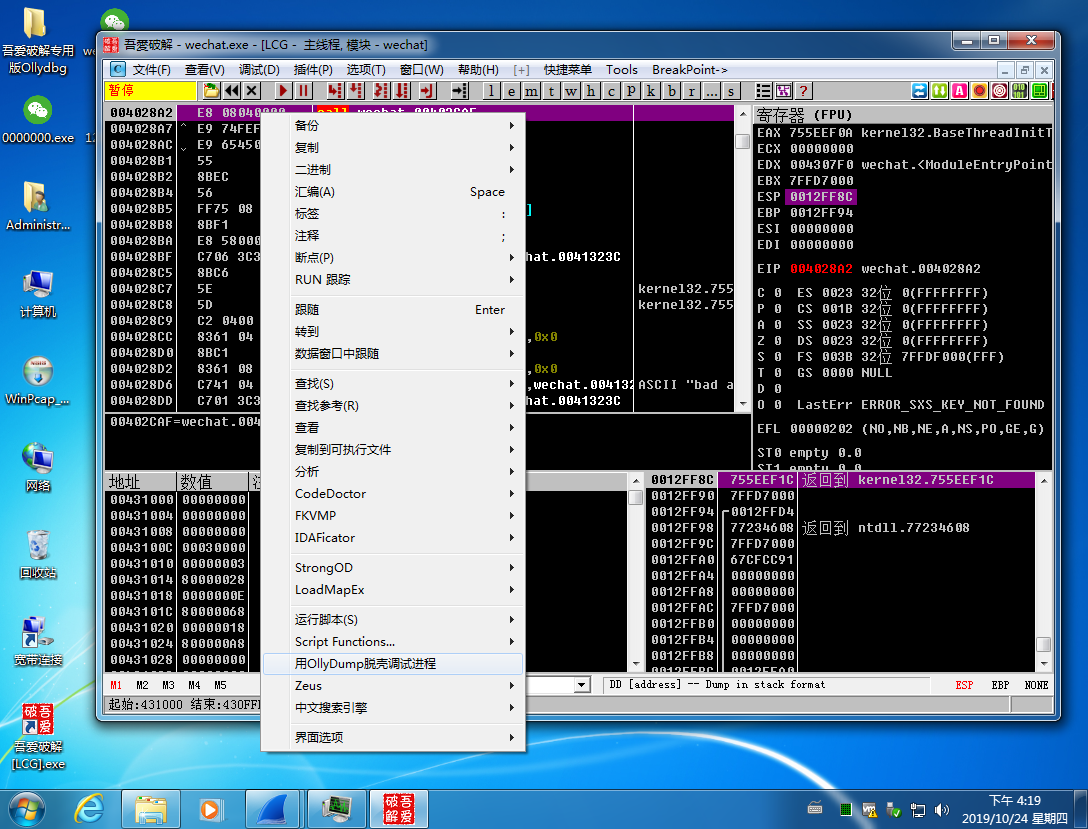




然后我们就可以脱壳了 ，脱壳前先把断点去掉 调试-硬件断点-删除



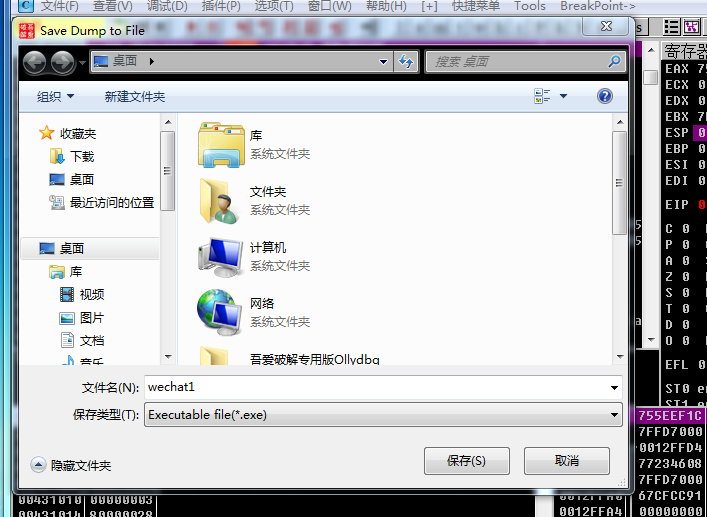
然后右击程序当前位置第一行代码，选择OllyDump脱壳调试进程



在弹出的窗口中点击脱壳

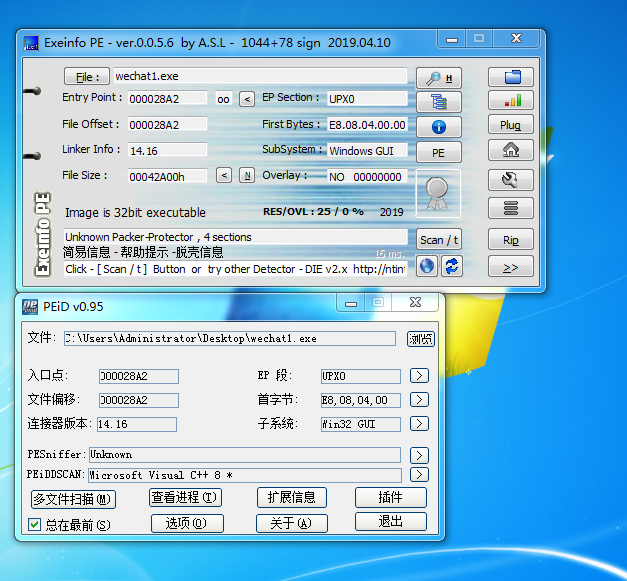


保存文件



此时我们已经完成了脱壳

使用查壳软件查看



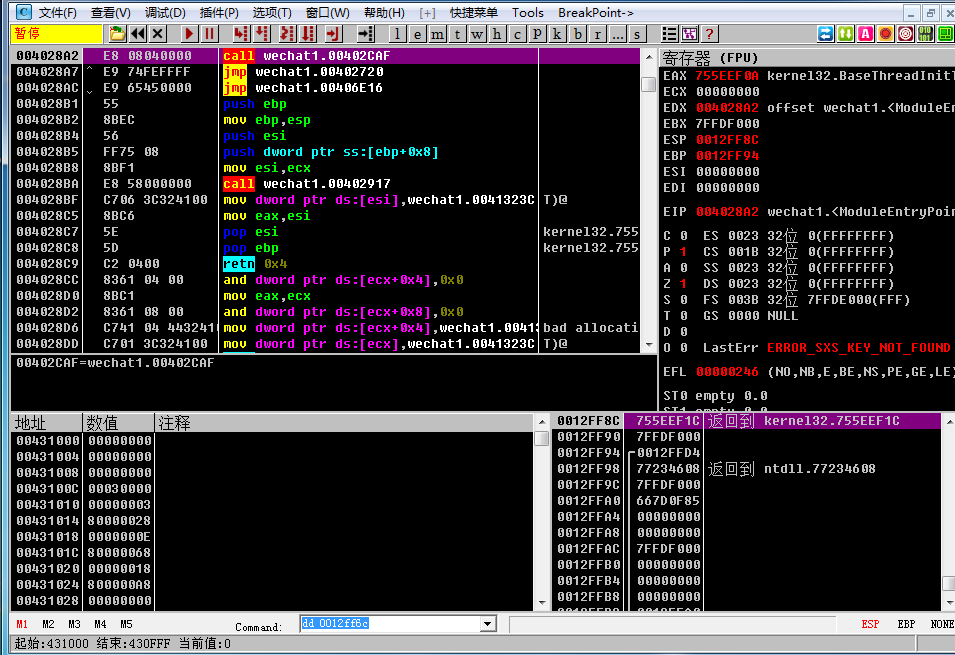
这个目标的壳只是简单的UPX壳，也没有资源修复之类的，如果遇见需要修复重定位和资源的话，可以参考其他教程

、

第三步：

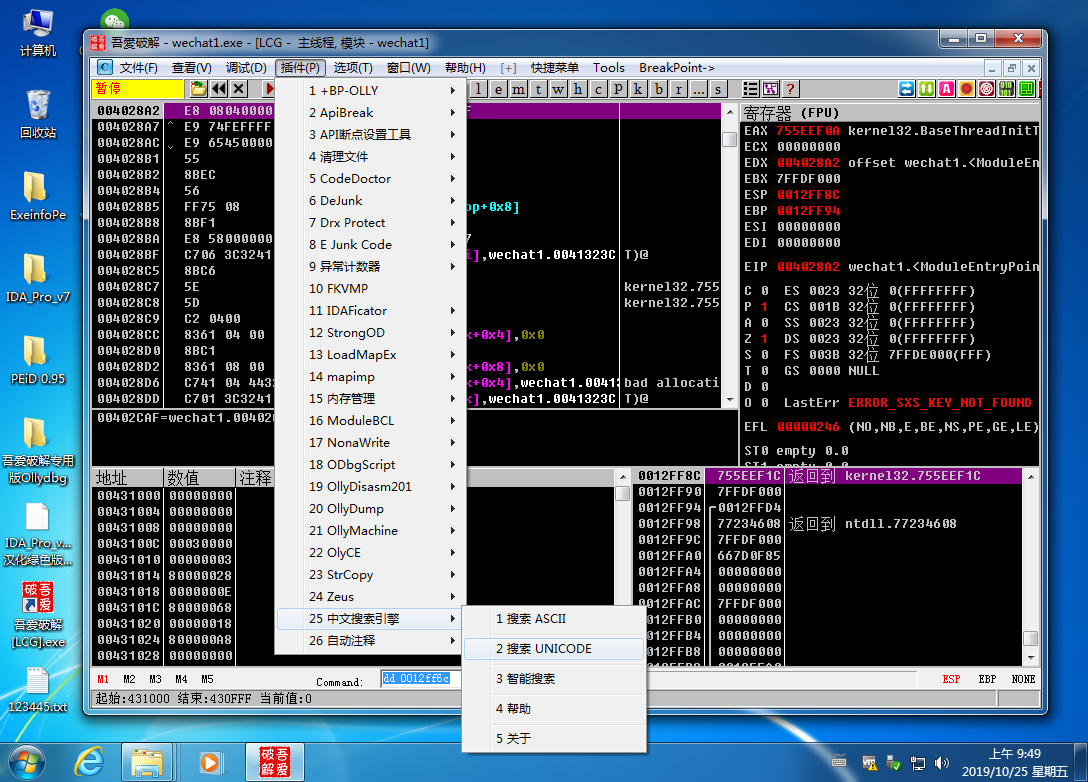
分析：

将dump出来的程序拖进OD里面，这次打开没有加密提示了。

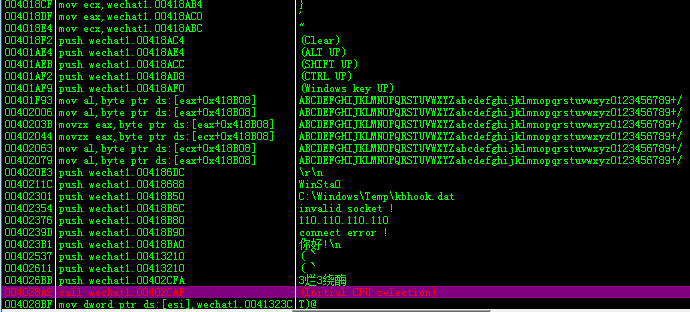


我们可以使用一些插件来帮助我们完成一系列的工作。

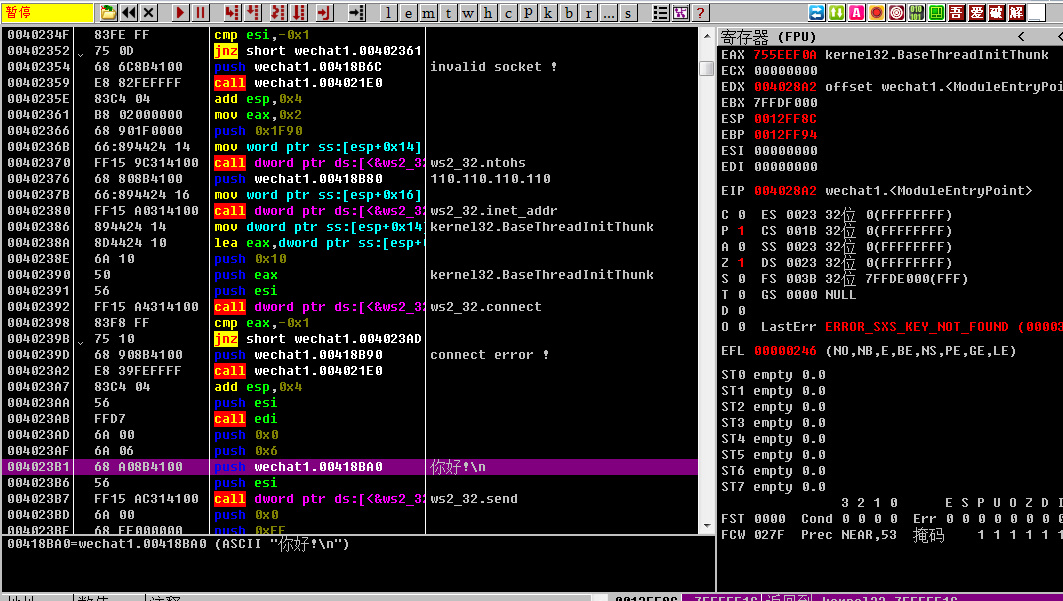
比如使用中文搜索插件



点击只能搜索， 我们先来看看有没有 非常显眼的字符串，如果是加壳程序，插件分析是不起作用的，所以，只有脱过壳的程序才能使用。

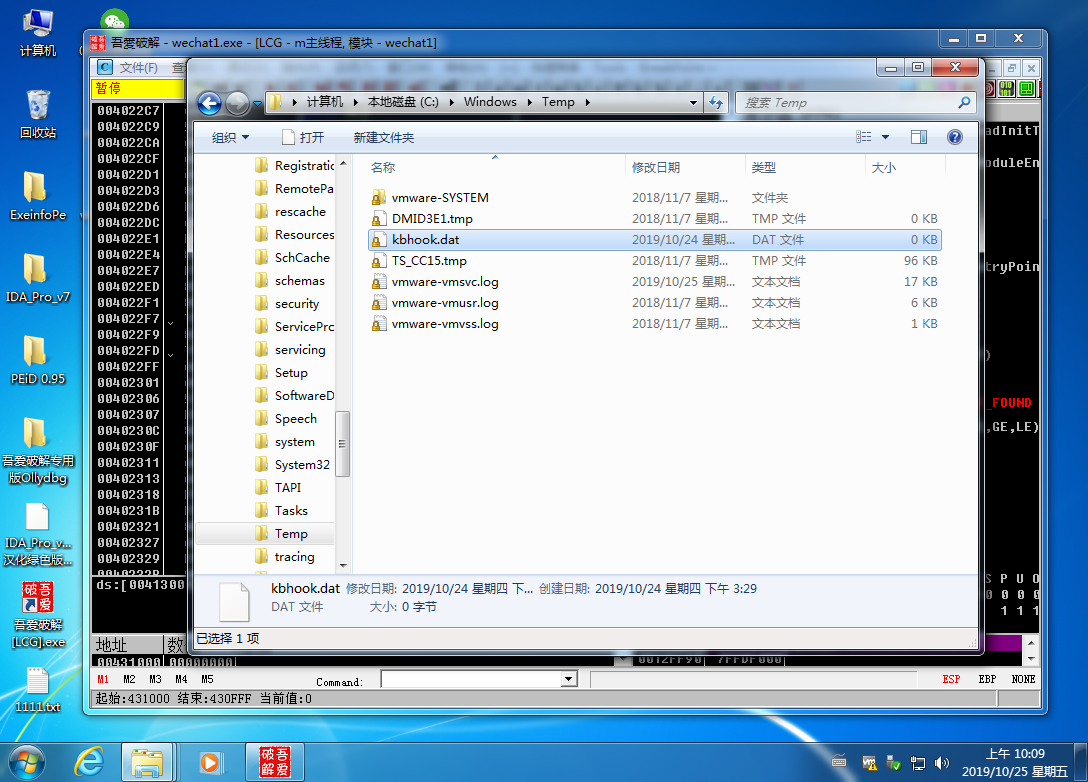


非常的幸运，我们第一眼就看到了关键的字符串， 图中的110.110.110.110 像是木马回链的IP地址，C：\windwos\Temp\kbhook.dat 路径从名字来看是一个hook相关的文件，还有相关的汉字“你好”。我们就先从“你好”分析，鼠标双击 你好， 进入程序主界面



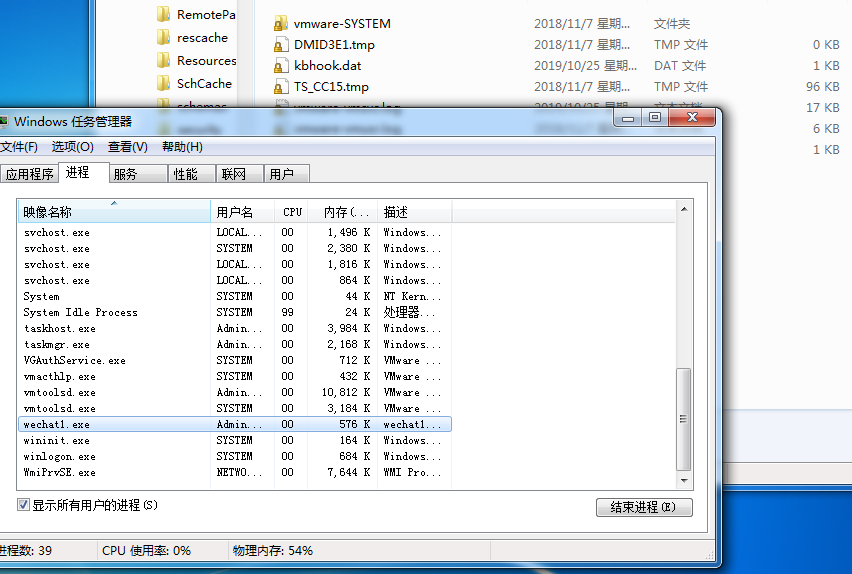
可以看到，这是向110.110.110.100服务器发送“你好”字符。

我们再来看看这个 kbhook.dat 是什么东西 ，打开路径

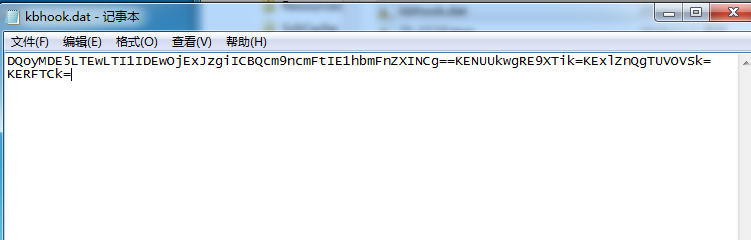


发现是0KB ，里面一片空白，这时候我们需要关闭OD ，让程序真正的执行一下。

调用任务管理器查看一下程序的进程



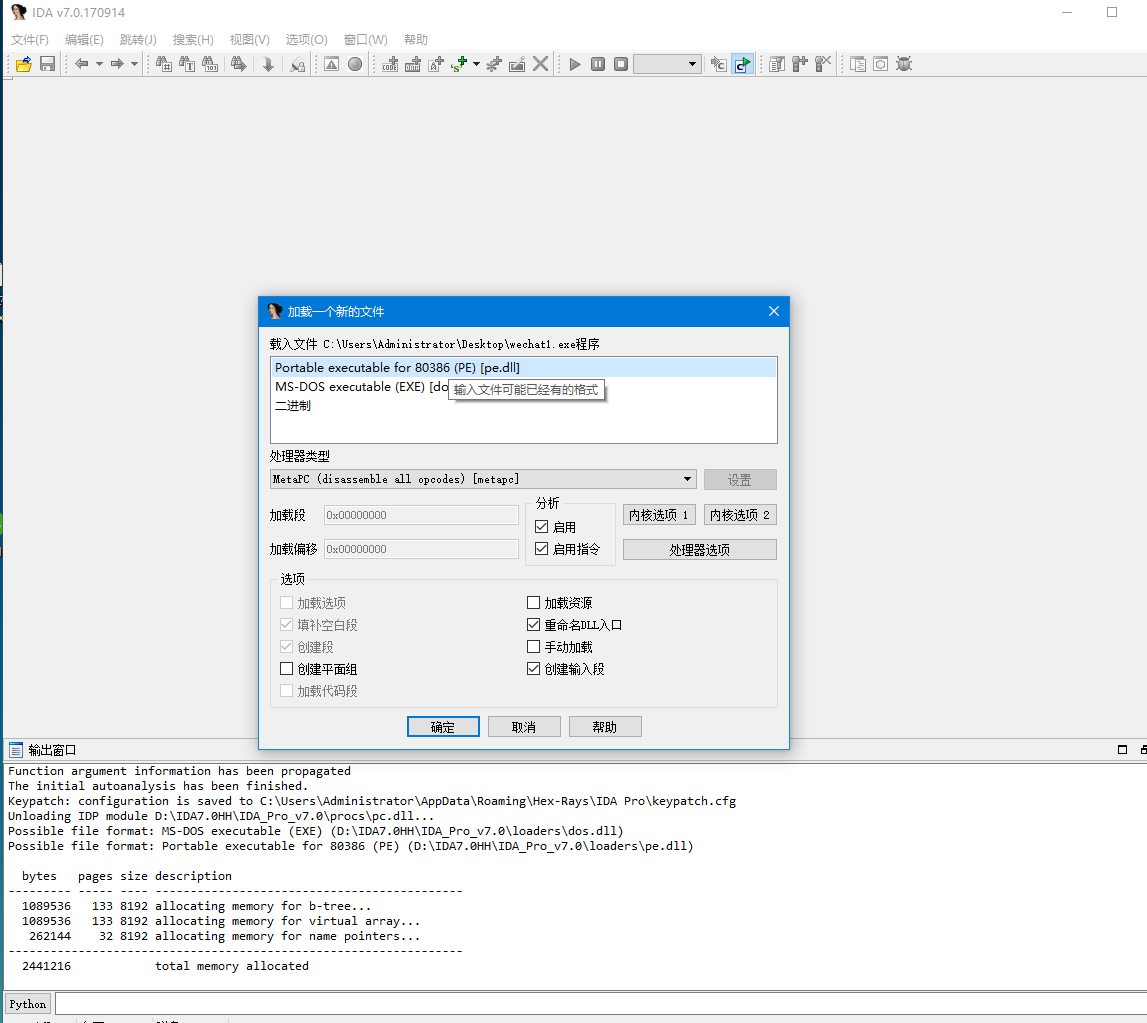
这时候发现kbhook.dat已经变大了 ，猜测是键盘记录 我们打开kbhook，发现被目标占用，先结束进程，再打开文件



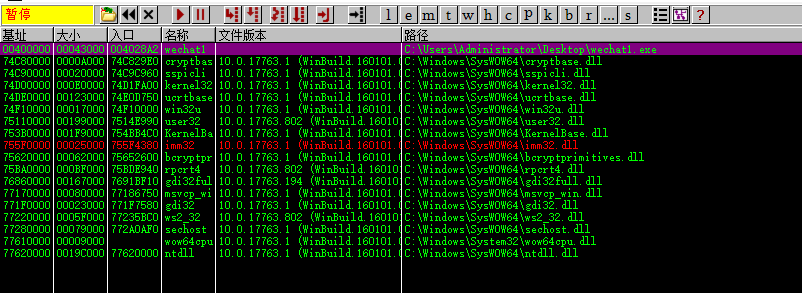
经对照，是经过base64编码的 解码后 是记录的键盘操作，分析完成。

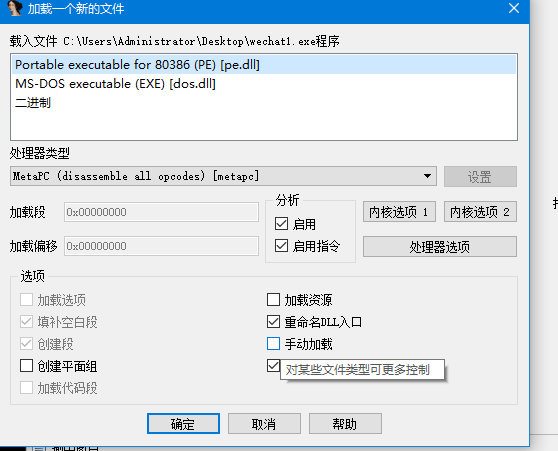
我们也可以使用IDA进行分析， 首先将目标程序拖进OD ，并F8单步过，一直到程序运行起来， 记录下程序在哪一个CALL 上面直接运行起来的。

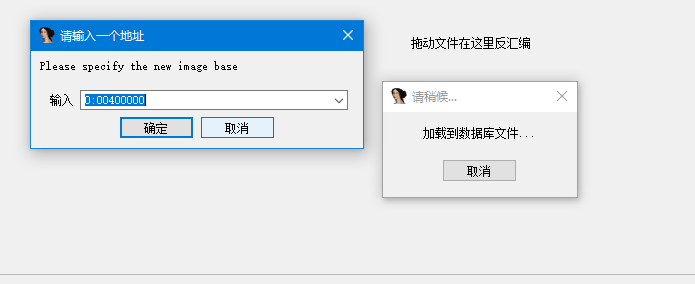
经过单步，我们发现程序是在 call wechat1.00402220这个地址上直接运行起来的。我们记录下这个地址， 打开IDA，将目标拖入IDA



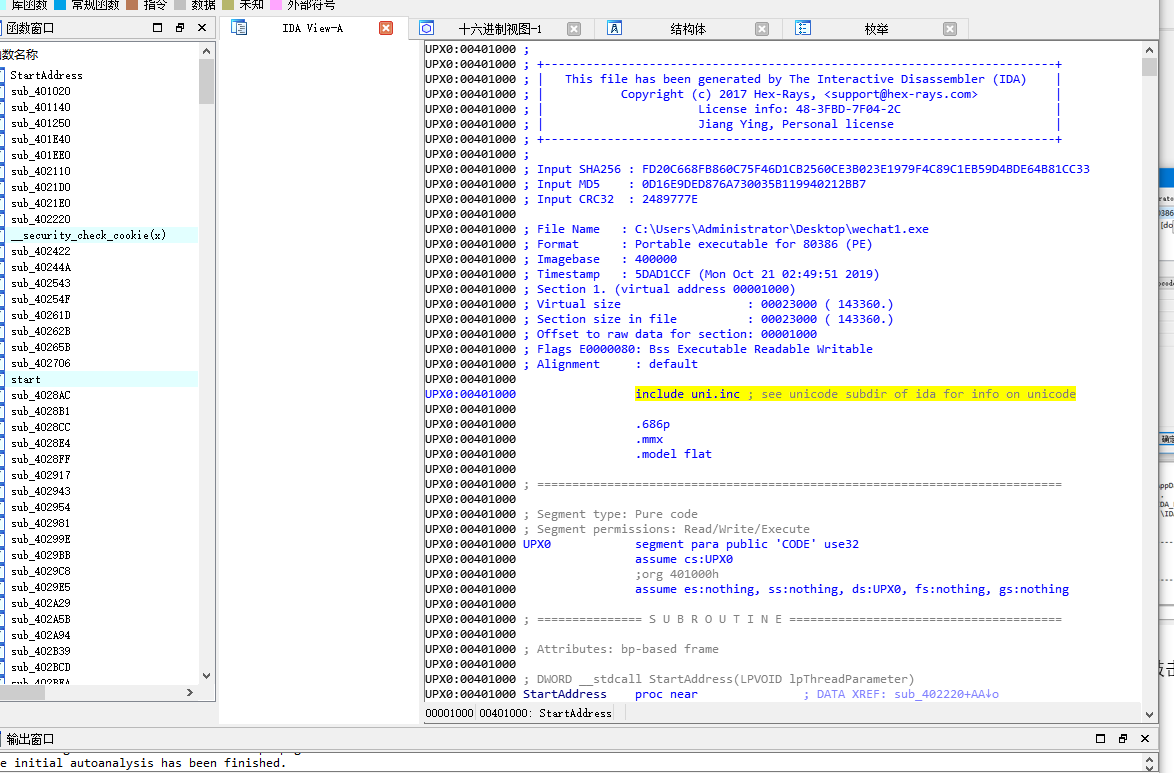
点击 确定加载程序，因为没有重定位，所以地址一样，如果是有重定位，需要勾选 IDA“手动加载”，然后将OD中的中的基地址（按alt+E调出OD窗口）填进去，这样两个程序的地址就能对应起来



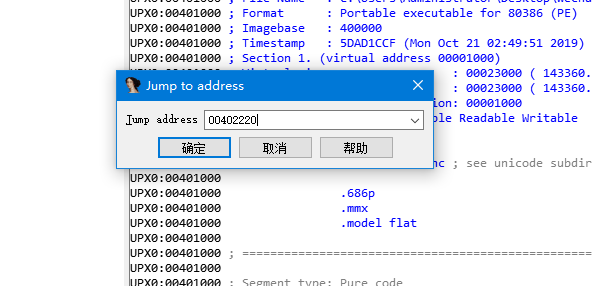




我们进入IDA的概览模式，敲击空格键 切换到反汇编



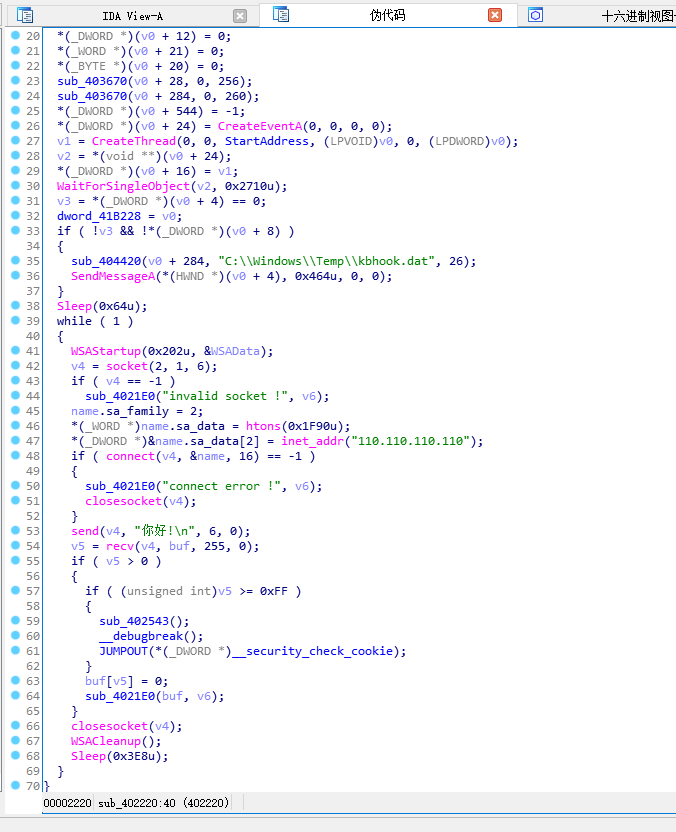
我们来搜索一下记录的地址， 快捷键G 是地址搜索



点击确定



来到了函数00402220 ，这时候我们使用F5插件 进行代码的伪C查看



可以看到，程序的流程一目了然。