什么是控件输入call

当我们想要在游戏里进行喊话和聊天的时候，需要在游戏内置的控件里输入相应的内容，这个往控件输入内容的call就叫控件输入call。

定位控件输入call

以游戏的账号密码输入框为例，来找这样一个控件输入框。当我们在输入字符的时候，这个call会在内部改变当前的字符长度，字符长度就可以作为一个突破口。

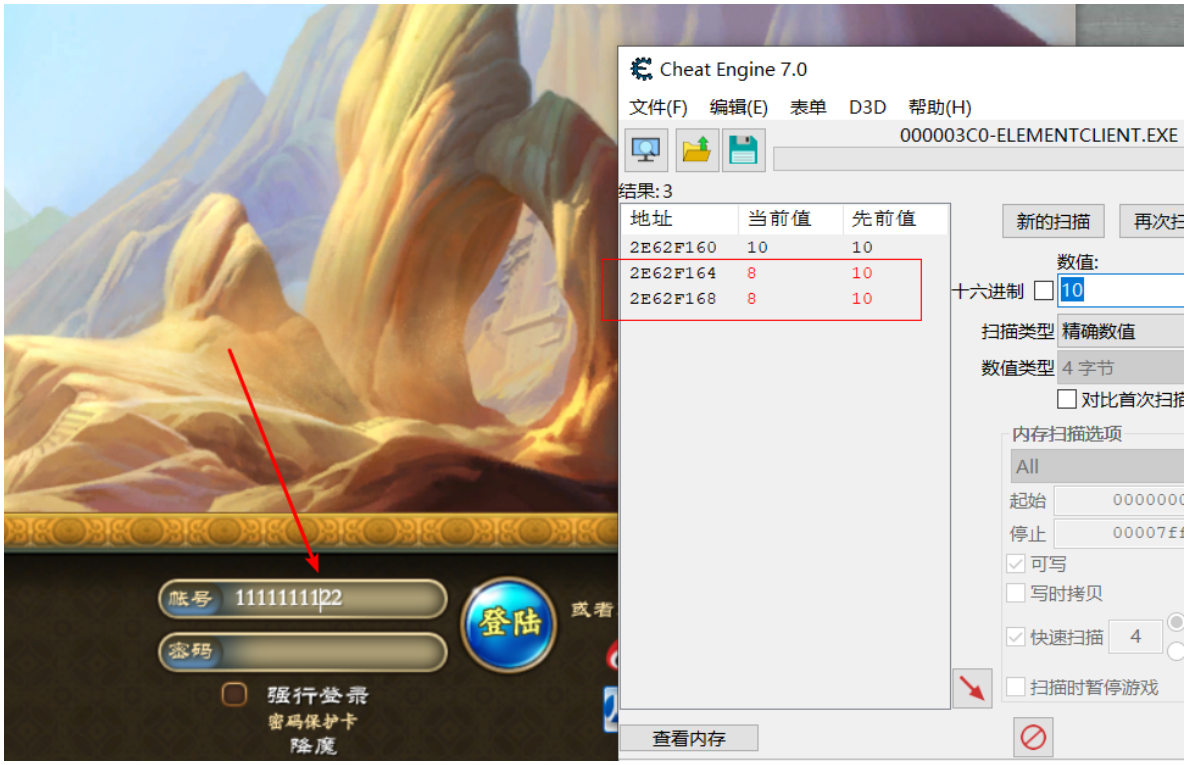
所以利用这个内存访问关系，只要在当前的字符长度下断，就可以找到这个控件输入call

定位字符长度

首先在控件里输入8个1，在CE里搜索8

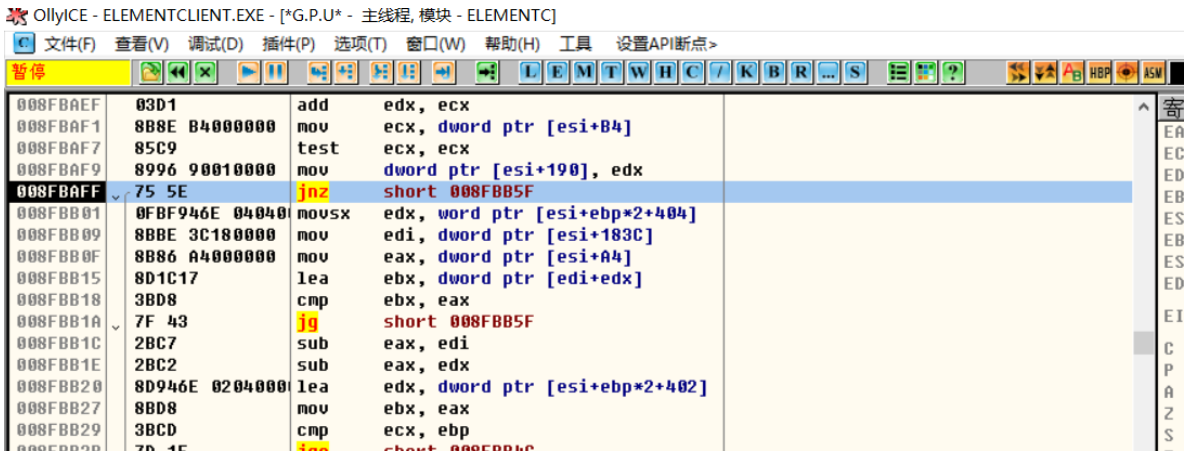
然后不断去修改字符长度，很容易就能筛出控件的字符长度。

最后还剩下三个值，然后我们把鼠标挪到1111的位置，再来看一下三个值的变化

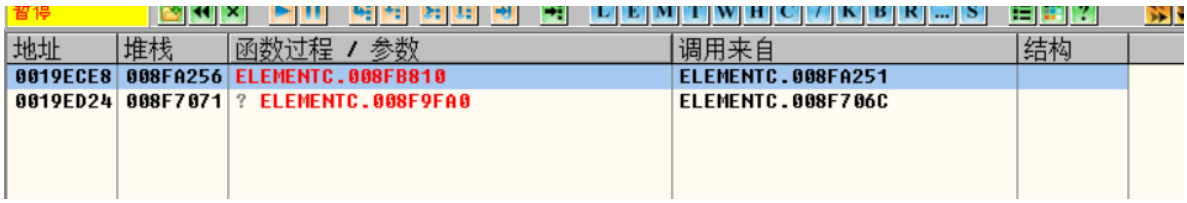


注意看光标的位置和CE里的数值。有两个值发生了变化，这两个值表示的是当前光标所在的字符的位置，剩下的那个才是真正的字符长度

通过字符长度定位控件输入call

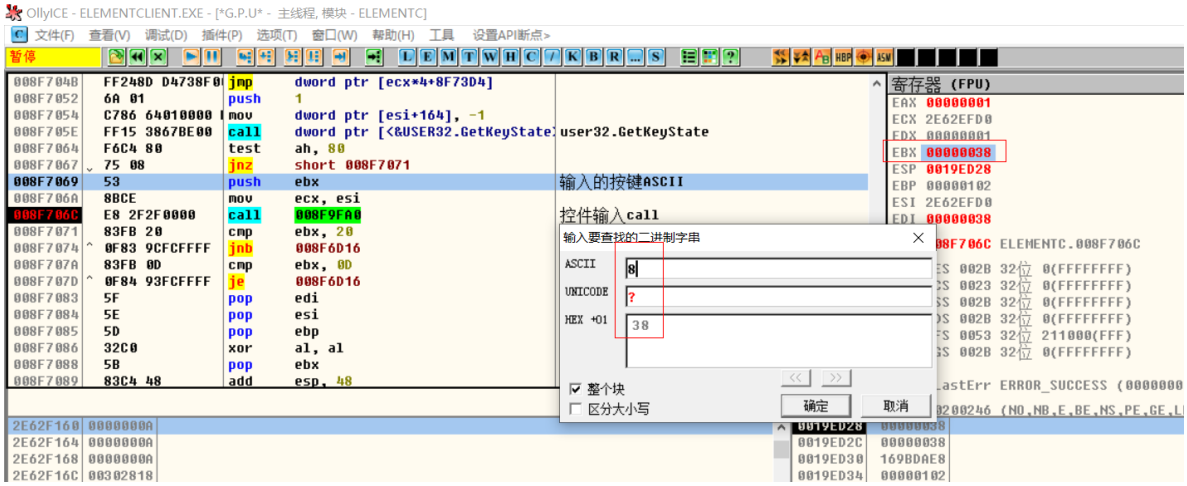


接着我们在字符长度下硬件写入断点，随便输入一个值，让程序断下

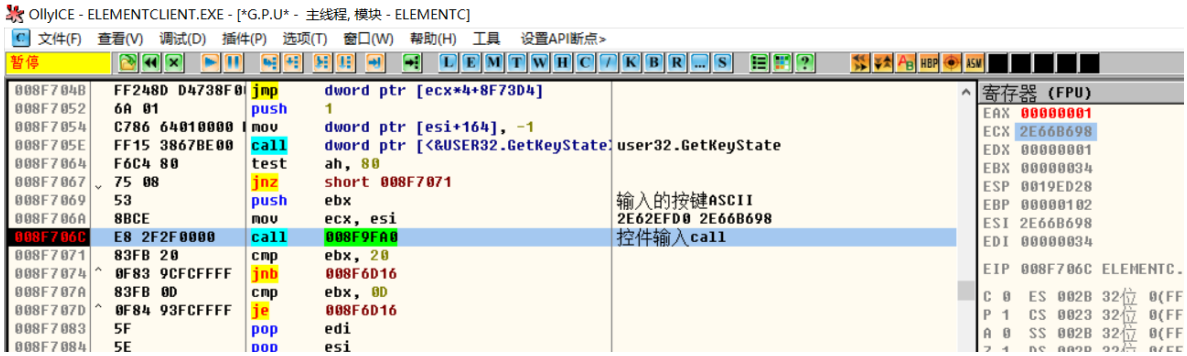


打开调用堆栈，找到第二个call，显示调用，这个就是我们要的控件输入call

接下来分析参数，我们先输入一个8，看看当前的寄存器状态



ebx的值是38，也就是数字8的ASCII值，所以这个参数的含义是输入的按键ASCII值



再看ecx，这个寄存器的值在输入按键和密码的时候分别出现了两次，那么可以猜到这个参数应该就是控件ID。

往上追ecx的来源可以找到一个二叉树的结构，我们这里不进行深究。

相关工具：

https://github.com/TonyChen56/GameReverseNote