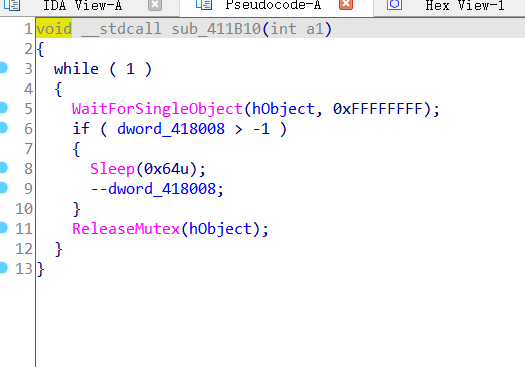


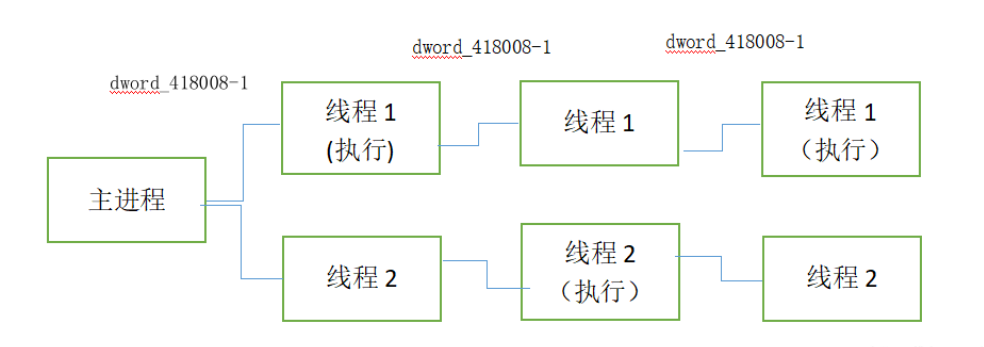
第一个线程h0bject会执行StartAddress函数，第二个线程v4执行sub\_41119f函数,然后挨个分析打开StartAddress函数

关键：

**两个线程同时工作的，所以要交替处理数据**

**当时我自己写exp的时候就只看了第一个处理输入字符串的线程进行算法逆向，逆出来不对，后来看wp恍然大悟，第二线程看似没有处理输入字符串，但它把第一个线程中用于索引字符串的索引改变了**

故线程2只是占着线程的计算器，每次运行dword\_418008减1，现在理一下思路，线程1改变了字符串，而线程2没有改变，也就是说**奇数改变偶数不改变**，直到dword\_418008减为0 ，线程结束，主进程也跟着结束



逆向得到

**ThisisthreadofwindowshahaIsES**

**但实际上还缺少了最后一位，需要爆破为E**