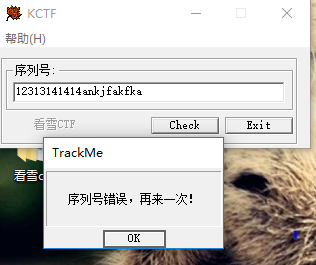
看雪ctf2018——第一题

0x01

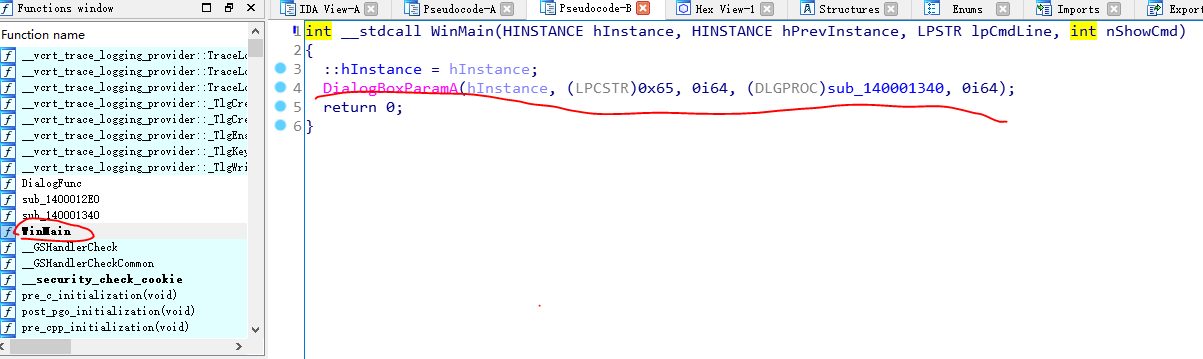
拿到程序，首先运行一下



可以看出，是一个输入字符串，检测序列号的正确性的程序，根据以往经验可知，这个程序调用了getdlgitemtexta之类的函数，用于获得窗口内容，然后计算校验，流程大体这样。

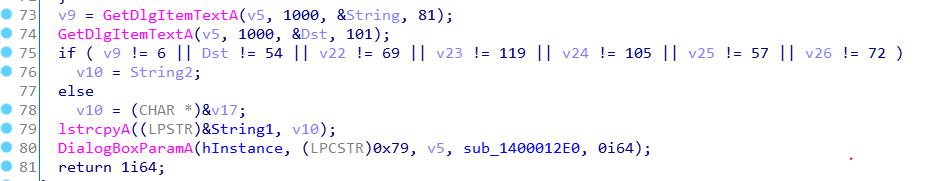
0x02

将程序拖入IDA，找到入口函数或者程序入口点



dialogboxparama是弹出对话框，重点在sub\_140001340这是检测输入的函数

查看函数内容



有关GetDlgItemTextA的用法介绍

<https://docs.microsoft.com/zh-cn/windows/desktop/api/winuser/nf-winuser-getdlgitemtexta>

分析：根据用法，v9是输入的字符串的长度，检测一下是不是输入字符串长度为6，剩下的dst，v22等，在前面的没有赋值的，是程序运行后输入的值。所以输入的话，肯定不是将这几个数5469119.。。。。。拼起来，而是常用的ascii码，转换一下，得到6Ewi9H

