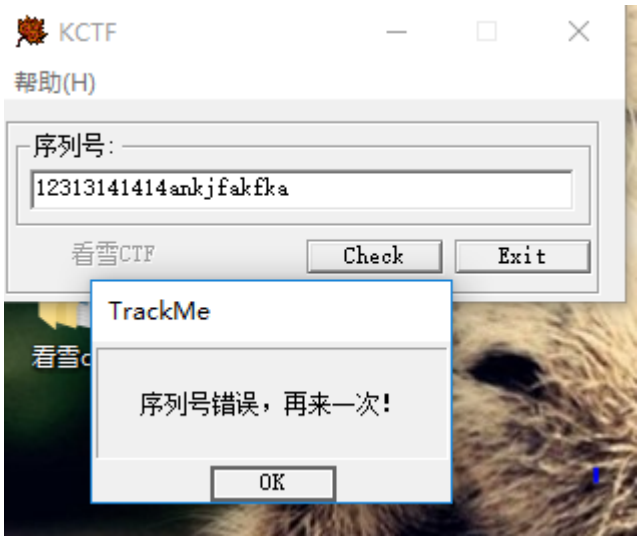
看雪 ctf2018——第一题

0x01

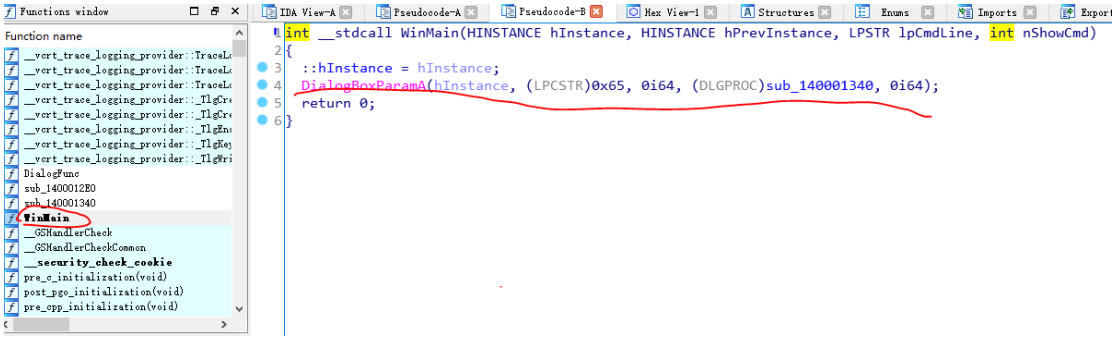
拿到程序，首先运行一下



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

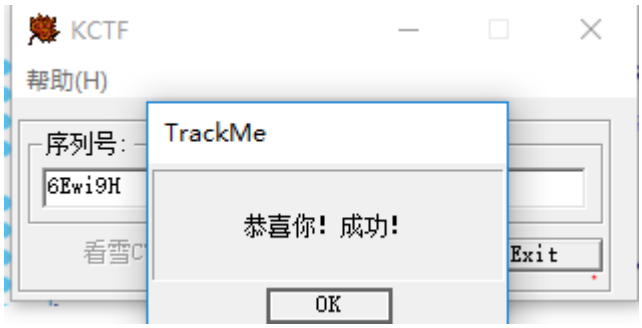
查看函数内容

```
v9 = GetDlgItemTextA(v5, 1000, &String, 81);
GetDlgItemTextA(v5, 1000, &Dst, 101);
if ( v9 != 6 || Dst != 54 || v22 != 69 || v23 != 119 || v24 != 105 || v25 != 57 || v26 != 72 )
  v10 = String2;
else
  v10 = (CHAR *)&v17;
lstrcpyA((LPSTR)&String1, v10);
DialogBoxParamA(hInstance, (LPCSTR)0x79, v5, sub_1400012E0, 0i64);
return 1i64;
```

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


KCTF
帮助(H)
序列号:
6Ewi9H
Exit
TrackMe
恭喜你！成功！
OK