虚拟机win32密码：VistaAsteria!

第二周（20150914）笔记：

驱动框架

变量必须初始化

用mallloc分配的内存后，不能再让此变量指向静态只读区，

全局变量g\_ 常量c\_ c++类成员变量 m\_ 静态变量 s\_

驱动架框：

应用层的API全部封装在kernel.dll和user32.dll中，kernel.dll/user32.dll进一步封装在ntdll.dll中（此时还是在应用层），从R3进入R0 -> sysenter/int2e进入内核，进入上下文，进入一个IO管理器中通过IRP包来进行从上往下一层层的处理，如果是文件包发给ntfs.sys,处理完成后，再下发disk.sys 分发函数就是用来处理R3的函数

KiFastSystemCallRet()->可以hook它，来监控应用层的所有函数

2:49

WinObj.exe（GLOBAL??）可查看本地计算机中所有的盘符所对应的链接名，而底层就是通过些和R3联系的