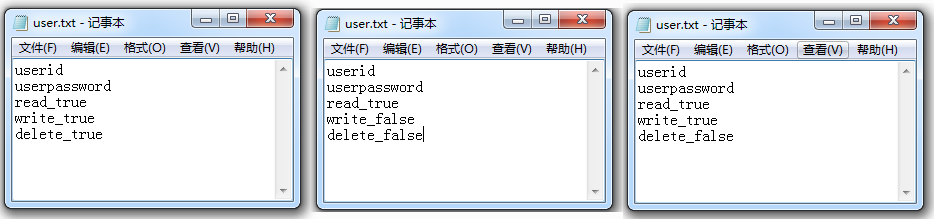
**（2016级）操作系统大作业（12选1）**

在网上先搜索和调研，按小组独立完成。

1（90分）、编写一个驱动程序D、相应的应用程序A和动态链接库L（可选）。驱动程序D（和可选的L）的核心功能是可以对特定的目录(譬如d:\OS)或文件(譬如d:\OS\homework.doc)进行保护。假定在c:\user.txt中已经事先记录有当前用户的ID、密码和权限：例如文件有这样5行：userid usrpassword read\_true/read\_false write\_true/write\_false delete\_true/delete\_false。其中后3行的内容任取“/”前后的一个词，表示该用户的读、写、删除的权限。那么当前用户对指定目录和文件的操作权限仅限于c:\user.txt文件所示。如果越权操作（例如无写的权限，如果用户进行写，即保存文件就是越权操作）就自动使该操作无效并给出提示。应用程序A的功能是安装和卸载该驱动。（提示：支持widows7环境，编写文件过滤驱动。）



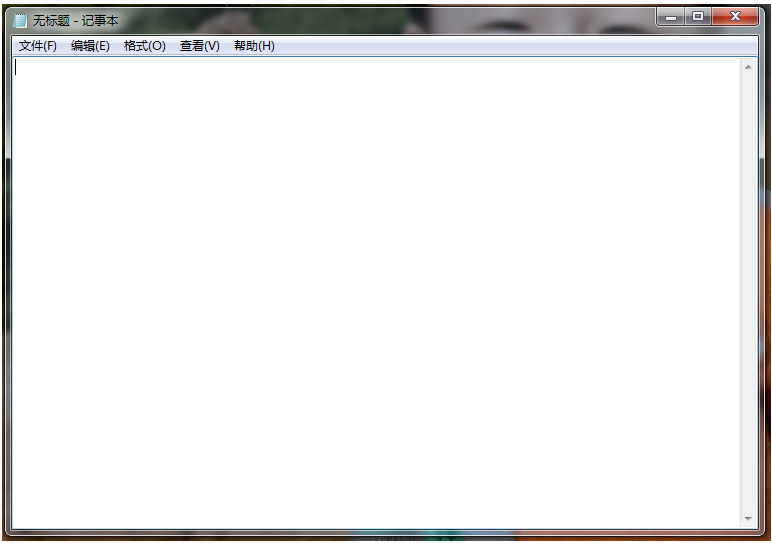
2（60分）、试述windows中PE文件的作用，格式，并结合一个C程序实例验证之。C程序自己写，要求程序中有2个全局变量（1个已初始化，1个未初始化），2个自定义函数（一个带参数，1个不带参数），每个函数都有2个局部变量。都有返回值。

3、（80分）试述Linux中elf文件的作用，格式，并结合一个C程序实例验证之。C程序自己写，要求程序中有2个全局变量（1个已初始化，1个未初始化），2个自定义函数（一个带参数，1个不带参数），每个函数都有2个局部变量。都有返回值。

4、（60分）阅读linux0.11的源代码，把它加载用户应用程序的过程描述出来（用户在控制台上输入程序名然后回车，linux即开始执行对应的应用程序，从此时开始描述）。要求：首先要找到linux0.11源码，定位到它的shell代码，看它如何执行用户输入的命令（/或运行应用程序）的。要跟踪linux0.11 中全代码执行过程，把每个函数的调用过程用图或流程图的方式描述清楚。

5、（60分）阅读linux2.6的源代码，把它加载用户应用程序的过程描述出来（用户在控制台上输入程序名然后回车，linux即开始执行对应的应用程序，从此时开始描述）。要求：首先要找到linux2.6源码，定位到它的shell代码，看它如何执行用户输入的命令（/或运行应用程序）的。要跟踪linux2.6中全代码执行过程，把每个函数的调用过程用图或流程图的方式描述清楚。

6、（90分）在windows **XP（如有时间可以尝试win7或win8）**下修改一个现有的exe可执行程序（显然没有源代码！譬如nodepad.exe或其他任何自己编写的可执行程序）。让该程序运行后先执行一个特别的附加功能（附加功能是：弹出一个对话框，要求用户输入用户名和口令，正确即可继续运行该程序，否则程序结束）。注意：附加功能嵌入到了原来的程序中，不是一个独立程序！要求了解pe文件格式，另外建议使用汇编编程。



7、（90分）在Linux中下修改一个现有的elf可执行程序（显然没有源代码！譬如vi或其他任何自己编写的可执行程序）。让该程序运行后先执行一个特别的附件功能（附加功能是：创建或打开一个指定文件写入helloworld的字符串）后再继续运行该程序，否则程序结束。注意：附加功能嵌入到了原来的程序中，不是一个独立程序！要求了解elf文件格式，另外建议使用汇编编程。

8、（60分）结合intel结构CPU的相关规范深入了解汇编程序的编写和编译过程。特别搞清楚这些问题：org指令的这用，（程序员编程时不明确指明的情况下的）各个段寄存器和相关寄存器的缺省值是多少？堆栈的地址和大小如何设置？上述所有问题的解释都需要**结合程序实例**做说明。

9、（70分）试调研linux内核的各个主要版本的差异：从liunx0.11开始到最新版本。包括进程管理，进程调度，内存管理，文件系统，设备管理，shell，源代码的规模（要具体数据：代码行数，目录夹文件的数量）等多个方面的比较。要求至少包括5个版本：其中0.11，2.4，2.6，2.8，3.0。

10、（70分）了解微软的WRK。WRK的全称是“Windows Research Kernel”，它是微软为高校操作系统课程提供的可修改和跟踪的操作系统教学平台。它给出了Windows这个成功的商业操作系统的内核大部分代码，可以对其进行修改、编译，并且可以用这个内核启动Windows操作系统。要求：（1）请尝试安装虚拟机，把WRK配置好并能运行起来，让用户和系统进行交互，用户能编写和编译程序，在WRK中运行和测试。（2）研究和跟踪WRK源代码，搞清楚进程是如何创建的。结合createproccess函数，跟踪其流程，把其中每个函数的调用过程用图或流程图的方式描述清楚。WRK介绍性的网址：

<http://baike.baidu.com/link?url=pR0ktso9X4V5IxvjjY_LzAXi1kpbnINXiVrNu26loq-u6znG1AfJdUx0q6NGh1zxu_DjLMngO-KjDksyea8aaq>

11. （80分）比较32位操作系统和64位操作系统的差异。如何开发64位的应用，如何建立相应的开发环境，并给出2-3个63位的应用程序的变成实例？

12. （90分）开发一个虚拟串口驱动程序（安装后，系统出现新的“串口”，例如COM3），分别开发出win 7 32位和64位的两个版本，并比较他们的在位数宽度上的差别。