进程的定义和CreateProcess函数的解释计算机等级考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/645/2021_2022__E8_BF_9B_E7_A8_8B_E7_9A_84_E5_c97_645908.htm 进程通常被定义为一个正在运行的程序的实例，它由两个部分组成：一个是操作系统用来管理进程的内核对象。内核对象也是系统用来存放关于进程的统计信息的地方。另一个是地址空间，它包含所有可执行模块或D L L 模块的代码和数据。它还包含动态内存分配的空间。如线程堆栈和堆分配空间。 BOOL CreateProcess(PCTSTR pszApplicationName, //pszApplicationName指定要创建进程的应用程序名，如在此设置需要全名PTSTR pszCommandLine, //需要创建进程的命令行参数，一般第一个字符用来存储应用程序名，不需要全地址PSECURITY_ATTRIBUTES psaProcess, //描述进程的可继承特征，为SECURITY_ATTRIBUTES结构体PSECURITY_ATTRIBUTES psaThread, //描述主线程的可继承性 BOOL bInheritHandles, //被创建的进程是否继承当前进程的内核操作权限 DWORD fdwCreate, //规定如何创建进程 PVOID pvEnvironment, //pvEnvironment参数用于指向包含新进程将要使用的环境字符串的内存块。 //在大多数情况下，为该参数传递N U L L，使子进程能够继承它的父进程正在使用的一组环境字符串。 PCTSTR pszCurDir, // pszCurDir允许父进程设置子进程的当前驱动器和目录。 //如果本参数是N U L L，则新进程的工作目录将与生成新进程的应用程序的目录相同。 PSTARTUPINFO psiStartInfo, //位置窗口标题显示名称光标等信息，包含了控制台模式和窗体模式，但我并不关心

//一般使用默认值但是需要初始化长度
PPROCESS_INFORMATION ppiProcInfo). 当一个线程调用CreateProcess时，系统就会创建一个进程内核对象，其初始使用计数是1。该进程内核对象不是进程本身，而是操作系统管理进程时使用的一个较小的数据结构。可以将进程内核对象视为由进程的统计信息组成的一个较小的数据结构。然后，系统为新进程创建一个虚拟地址空间，并将可执行文件或任何必要的D L L 文件的代码和数据加载到该进程的地址空间中。 Code
/**//*** ** Module name: Inherit.c Notices:Copyright(c)2000 Jeffrey Richter ***/
#include 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com