湖南科技大学计算机科学与工程学院

操作系统 课程设计报告

**专业班级：** 21计科七班

**姓 名：** 罗玉婷

**学 号：** 2101020326

**指导教师：** 肖小聪

**时 间**： 17、18周

**地 点**： 逸夫楼416

|  |
| --- |
| **指导教师评语：**  **成绩： 等级：**  **签名：**  **年 月 日** |

1. **实验题目（四号宋体，加粗，以下标题的字体格式与此相同）**

**实验一 Windows进程管理**

**二、实验目的**

（1）学会使用 VC 编写基本的 Win32 Consol Application（控制台应用程序)。

（2）通过创建进程、观察正在运行的进程和终止进程的程序设计和调试操作，进一步熟悉操作系统的进程概念，理解 Windows 进程的“一生”。

（3）通过阅读和分析实验程序，学习创建进程、观察进程、终止进程以及父子进程同步的基本程序设计方法。

1. **实验内容（实验原理/运用的理论知识、算法/程序流程图、步骤和方法、关键代码）**

**（1）编写基本的 Win32 Consol Application**

**步骤 1**：登录进入 Windows 系统，启动 VC++ 6.0。

**步骤 2**：在“FILE”菜单中单击“NEW”子菜单，在“projects”选项卡中选择“Win32 Consol Application”,然后在“Project name”处输入工程名，“Location” 处输入工程目录。创建一个新的控制台应用程序工程。

**步骤 3**：在“FILE”菜单中单击“NEW”子菜单，在“Files”选项卡中选择“C++ Source File”, 然后在“File”处输入 C/C++源程序的文件名。

**步骤 4**：将清单 2-1 所示的程序清单复制到新创建的 C/C++源程序中。编译成可执行文件。

**步骤 5**：在“开始”菜单中单击“程序”-“附件”-“命令提示符”命令，进入 Windows“命令提示符”窗口，然后进入工程目录中的 debug 子目录，执行编译好的可执行程序，列出运行结果 (如果运行不成功，则可能的原因是什么？)

**（2） 创建进程**

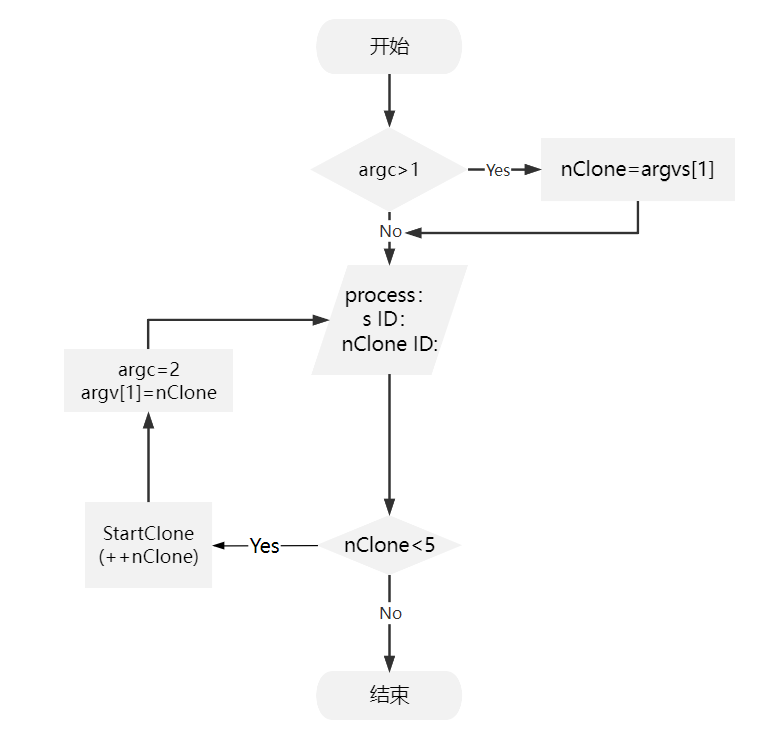
本实验显示了创建子进程的基本框架。该程序只是再一次地启动自身，显示它的系统进程 ID和它在进程列表中的位置。

**步骤 1**：创建一个“Win32 Consol Application”工程，然后拷贝清单 2-2 中的程序，编译成可执行4文件。

**步骤 2**：在“命令提示符”窗口运行步骤 1 中生成的可执行文件，列出运行结果。按下 ctrl+alt+del，调用 windows 的任务管理器，记录进程相关的行为属性。

**步骤 3**：在“命令提示符”窗口加入参数重新运行生成的可执行文件，列出运行结果。按下ctrl+alt+del，调用 windows 的任务管理器，记录进程相关的行为属性。

**步骤 4**：修改清单 2-2 中的程序，将 nClone 的定义和初始化方法按程序注释中的修改方法进行修改，编译成可执行文件（执行前请先保存已经完成的工作）。再按步骤 2 中的方式运行，看看结果会有什么不一样。列出行结果。从中你可以得出什么结论？说明 nClone 的作用。 变量的定义和初始化方法（位置）对程序的执行结果有影响吗？为什么？



**（3） 父子进程的简单通信及终止进程**

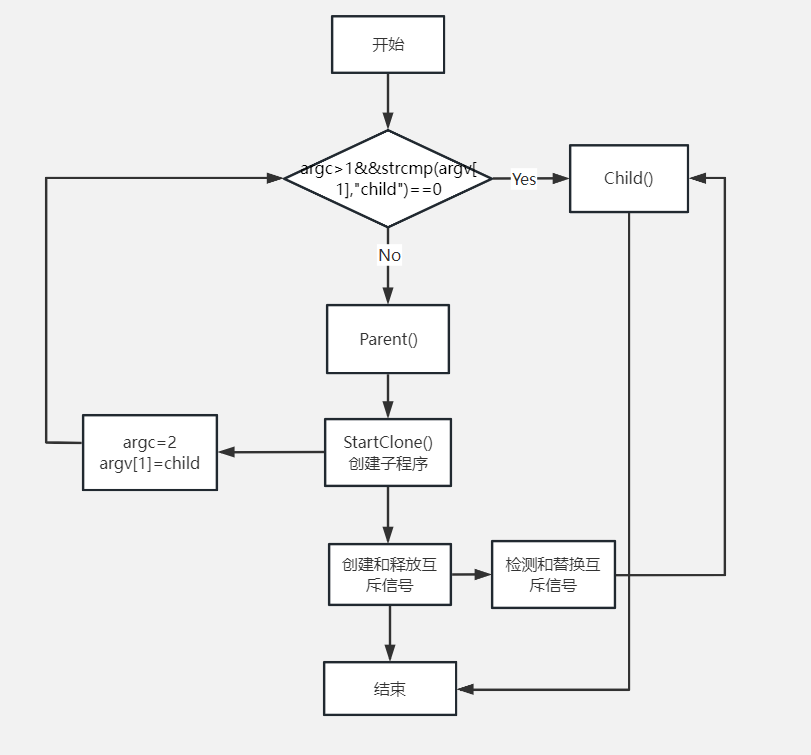
**步骤 1：**创建一个“Win32 Consol Application”工程，然后拷贝清单 2-3 中的程序，编译成可执行文件。

**步骤 2：**在 VC 的工具栏单击“Execute Program”(执行程序) 按钮，或者按 Ctrl + F5 键，或者在“命令提示符”窗口运行步骤 1 中生成的可执行文件，列出运行结果。

**步骤 3：**按源程序中注释中的提示，修改源程序 2-3，编译执行（执行前请先保存已经完成的工 作），列出运行结果。在程序中加入跟踪语句，或调试运行程序，同时参考 MSDN 中的帮助文件 CreateProcess()的使用方法，理解父子进程如何传递参数。给出程序执行过程的大概描述。

**步骤 4：**按源程序中注释中的提示，修改源程序 2-3，编译执行，列出运行结果。

**步骤 5：**参考 MSDN 中 的 帮 助 文 件 CreateMutex() 、 OpenMutex() 、 ReleaseMutex() 和WaitForSingleObject()的使用方法，理解父子进程如何利用互斥体进行同步的。给出父子进程同步过程的一个大概描述。

--3程序执行的大概描述：

从main()函数开始，首先判断argc的值（argc初始值默认为1），决定进行父进程还是子进程，因为argc不满足大于1，所以调用parent()函数，在执行parent（）函数过程中调用StartClone() ;然后通过sprintf(szCmdLine, “”%s\"child\" , szFilename)将argv[1]赋值child，后面满足条件后调用child()函数；由于设置了互斥信号，则只允许一个进程进行，所以只有当父进程释放互斥信号hMutexSuicide时，子进程检测获得才结束进程。

--4父子进程同步的大概描述：

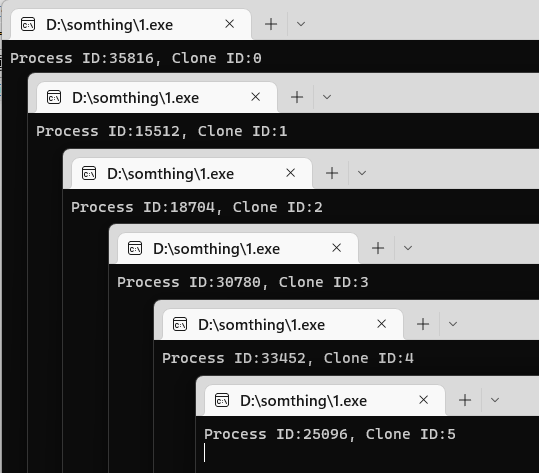
CreateMutex() 创建互斥体hMutexSuicide信号、 OpenMutex()打开互斥体、 ReleaseMutex()释放互斥体、WaitForSingleObject()检测Hhandle信号状态，通过这些只允许有一个状态被创建或者使用也就是信号量唯一，实现进程同步。

1. **实验结果与分析**

**（1）**在将void改为int后编译执行

****

1. 未修改运行

****

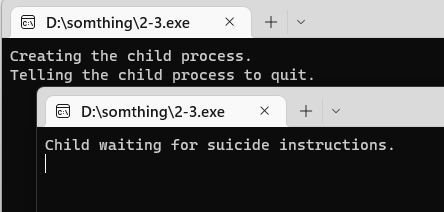
****

修改后运行：（由于关机了并未保存截图）

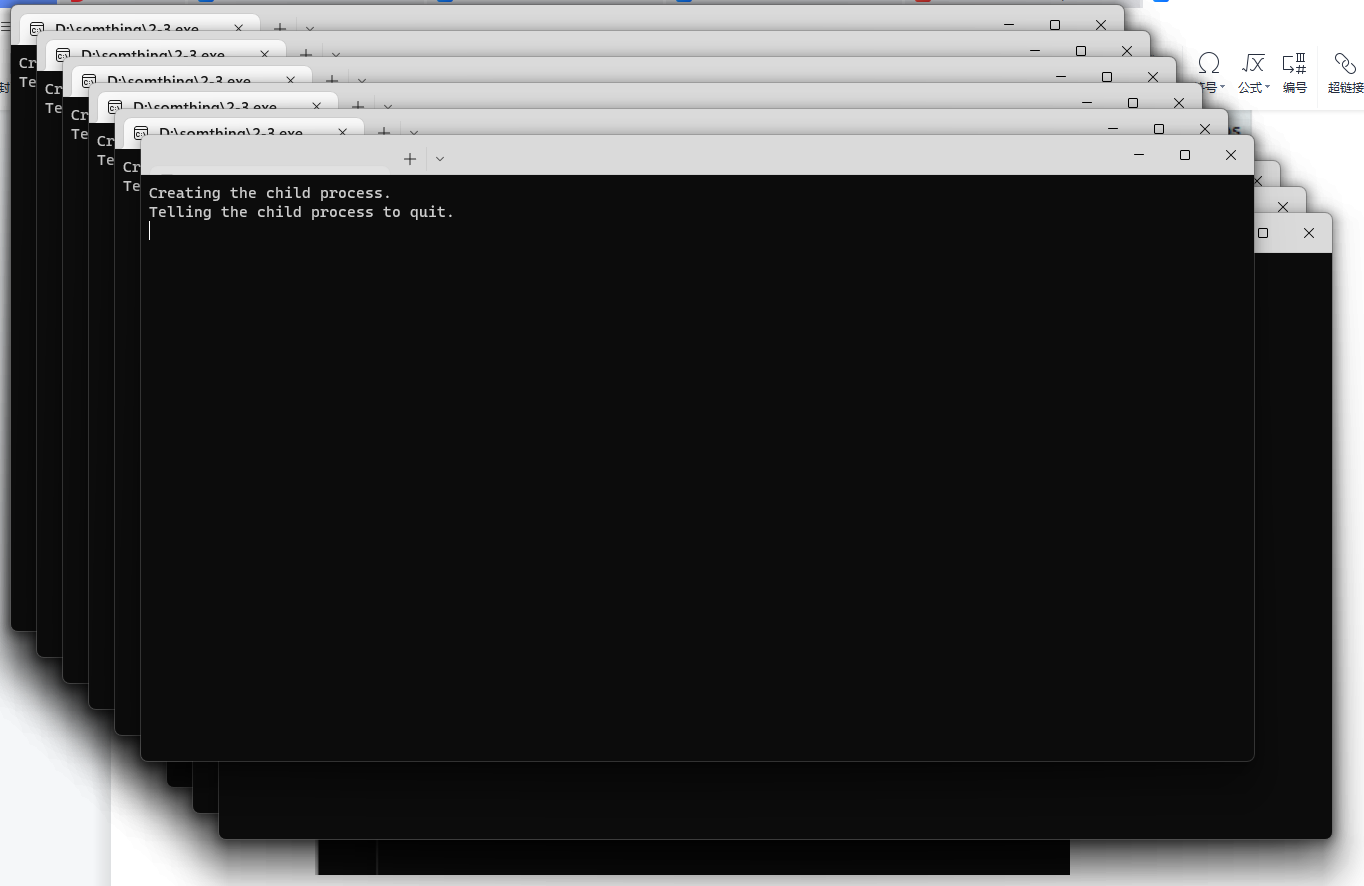
会一直创建进程，直到CPU利用率达到100%

nClone的作用是控制执行过程；未修改前，当nClone>5跳出循环，创建子进程就会结束；修改后，每次nClone会被重置为0，所以会陷入死循环，一直创建子进程

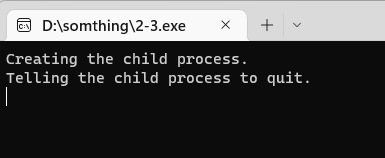
1. 未修改前运行：



修改后运行（1）：



修改后（2）：



**五、小结与心得体会**

1.加深了对操作系统进程概念的理解，Windows 所创建的每个进程都从调用 CreateProcess() API 函数开始，都以调用ExitProcess() 或TerminateProcess() API函数终止。可利用CreateMutex()API可创建互斥体，放弃共享资源时可调用ReleaseMute()API。

2. 修改为sscanf\_s出现了编译错误 

原因是sscanf\_s函数是C11标准中新增的函数，因此不是所有的编译器都支持它。我使用的是旧版本的编译器，无法使用sscanf\_s函数。

sscanf-s与sscanf函数的功能基本相同，但是sscanf\_s函数增加了一些安全检查。具体来说，sscanf\_s函数在解析字符串时会进行缓冲区边界检查，以防止缓冲区溢出。sscanf\_s函数还要求在format字符串中指定每个可变参数的最大长度，以便进行安全检查。

**一、实验题目**

**实验二 Linux 进程控制**

**二、实验目的**

通过进程的创建、撤销和运行加深对进程概念和进程并发执行的理解，明确进程和程序之间的区别。

**三、实验内容**

**（1）任务一：进程的创建**

**任务要求**：编写一段程序，使用系统调用 fork（）创建一个子进程。当此程序运行时，在系统中有一个父进程和一个子进程活动。让每一个进程在屏幕上分别显示字符：父进程显示字符“b”；子进程显示字符“a”，另外父子进程都显示字符“c”。

**步骤 1：**使用 vi 或 gedit 新建一个 fork\_demo.c 程序，然后拷贝清单 3-1 中的程序，使用 cc 或者gcc 编译成可执行文件 fork\_demo。例如，可以使用 gcc –o fork\_demo fork\_demo.c 完成编译。

**步骤 2：**在命令行输入./fork\_demo 运行该程序。

**步骤 3：**多次运行程序，观察屏幕上的显示结果，并分析多次运行为什么会出现不同的结果。

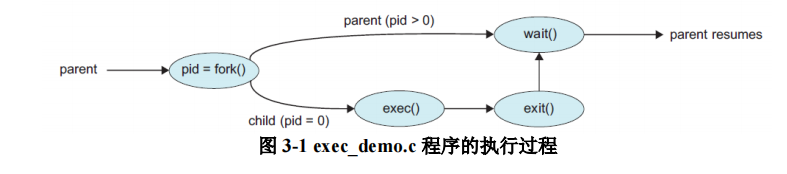
**（2）任务二：子进程执行新任务**

**任务要求：**编写一段程序，使用系统调用 fork（）创建一个子进程。子进程通过系统调用 exec更换自己原有的执行代码，转去执行 Linux 命令/bin/ls (显示当前目录的列表)，然后调用 exit（）函数结束。父进程则调用 waitpid()等待子进程结束，并在子进程结束后显示子进程的标识符，然后正常结束。程序执行过程如图 3-1 所示。

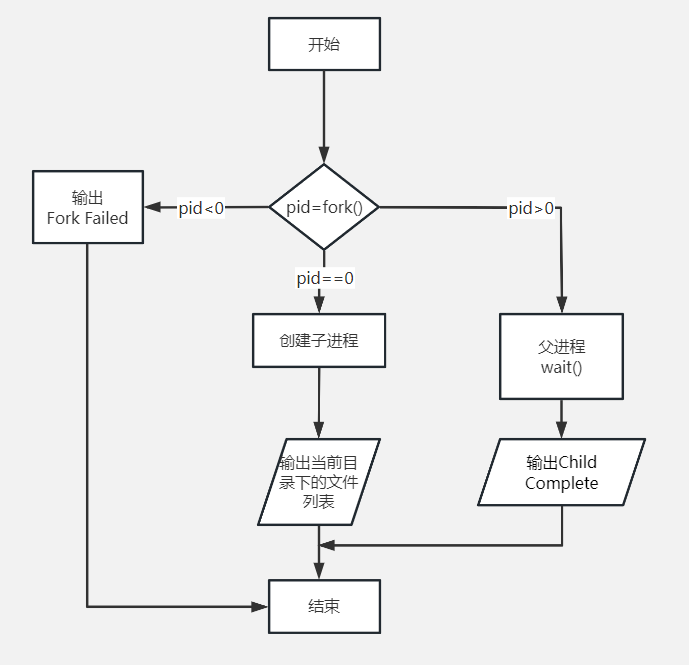
**步骤 1**：使用 vi 或 gedit 新建一个 exec\_demo.c 程序，然后拷贝清单 3-2 中的程序（该程序的执行如图 3-1 所示），使用cc或者 gcc 编译成可执行文件exec\_demo。例如，可以使用 gcc –o exec\_demo exec\_demo.c 完成编译。

**步骤 2：**在命令行输入./exec\_demo 运行该程序。

**步骤 3：**观察该程序在屏幕上的显示结果，并分析。

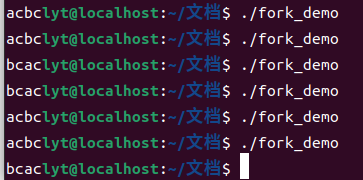
****

流程图：

****

**四、实验结果与分析**

**（1）**在main前加int后可编译运行

****

这是一个使用 fork() 函数创建进程的 C 语言程序，它会创建两个进程并打印出字符 "a" 和 "b"，最后打印一个字符 "c"。

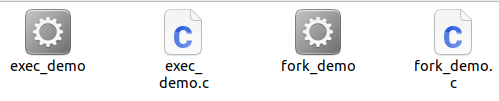
使用 srand() 函数初始化随机数种子，以便在后面的程序中使用 rand() 函数生成不同的随机数。在一个 while 循环中调用 fork() 函数创建子进程，如果 fork() 函数返回值为 -1，则表示创建进程失败，继续等待创建进程直到成功。

如果 fork() 函数返回值为 0，则表示当前进程为子进程，调用 sleep() 函数等待一个随机时间后输出字符 "a"。如果 fork() 函数返回值不为 0，则表示当前进程为父进程，调用 sleep() 函数等待一个随机时间后输出字符 "b"。最后，父进程和子进程都输出字符 "c"。

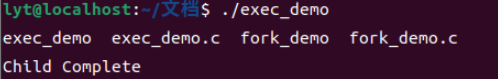
由于父进程和子进程同时运行，因此输出的字母顺序可能会不同，例如会输出 "acbc" 或 "bcac" 不同的顺序。

**（2）**

该目录下的文件列表：



编译执行结果：



调用fork()函数创建一个子进程，如果返回值小于 0，则表示创建进程失败，输出错误信息并退出程序。如果返回值等于 0，则表示当前进程为子进程，在子进程中通过调用 execlp() 函数来执行 /bin/ls 命令，显示当前目录下的文件列表。其中，第一个参数 "/bin/ls" 是要执行的命令，第二个参数 "ls" 是命令的名称，NULL 表示命令参数列表结束。如果返回值大于 0，则表示当前进程为父进程，在父进程中调用 wait() 函数来等待子进程的执行，直到子进程运行完毕后输出 "Child Complete"。

**五、小结与心得体会**

加深了我对Linux操作系统的进程概念的了解，也学会了在Linux基本运行，也使我明白了在Linux系统中子进程的创建，以及父子进程的运行过程，加深了对进程运行的理解。在Linux中利用fork建立一个子进程，父进程继续运行，子进程在同样的位置执行同样的程序。对于父进程，fork()返回子进程的 pid, 对于子进程，fork()返回 0，出错时返回-1,while((x=fork())==-1)这句话是用来判断子进程是否能创建成功，而且当x=0时运行子进程，当x>0时父进程执行，而x<0时，则进程创建不成功，通过代码确定父子进程的先后执行顺序。

**一、实验题目**

**实验三 Linux 进程间通信**

**二、实验目的**

Linux 系统的进程通信机构（IPC）允许在任意进程间大批量地交换数据，通过本实验，理解熟悉 Linux 支持的消息通信机制。

**三、实验内容**

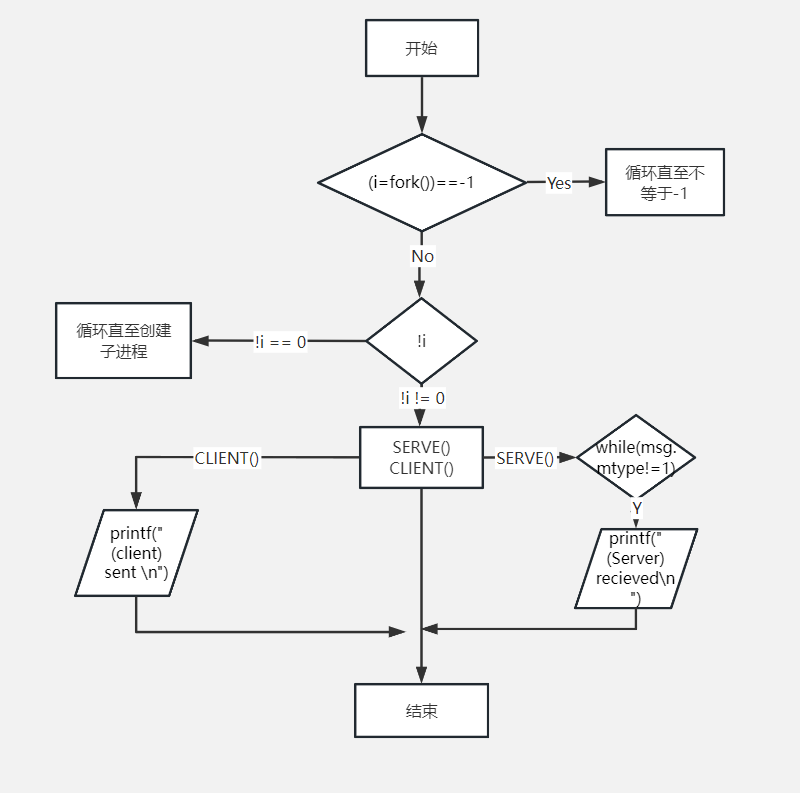
**消息的创建、发送和接收的程序设计**

（1） 为了便于操作和观察结果，用一个程序作为“引子”，先后 fork()两个子进程 SERVER和 CLIENT，进行通信。

（2） SERVER 端建立一个 key 为 75 的消息队列，等待其他进程发来的消息。当遇到类型为 1 的消息，则作为结束信号，取消该队列，并退出 SERVER。SERVER 每接收到一个消息后显示一句“（server） received”。

（3） CLIENT 端使用 key 为 75 的消息队列，先后发送类型从 10 到 1 的消息，然后退出。最后的一个消息，即是 SERVER 端需要的结束信号。CLIENT 每发送一条消息后显示一句“(client)sent”。

（4） 父进程在 SERVER 和 CLIENT 均退出后结束。



**四、实验结果与分析**

****

**（1）**控制消息队列系统调用 msgctl()在此起的作用

msgctl()系统调用在SERVER函数中被调用，用于删除消息队列。具体来说，当SERVER函数接收到mtype为1的消息时，它调用msgctl()函数将消息队列从系统中删除，以便释放系统资源。在使用完消息队列之后，需要通过调用msgctl()函数将其从系统中删除，否则它将一直存在于系统中，占用系统资源。

删除消息队列可能会导致正在等待该消息队列的进程无法继续进行，因此在删除消息队列之前需要确保所有进程都已经完成对该消息队列的操作。这个程序中使用了wait()函数等待子进程退出，以确保在删除消息队列之前所有进程都已经完成对消息队列的操作。

**（2）**从理论上说，上述程序应当是每当 client 发送一条消息后，server 接收该消息，client 再发送下一条，也即是应该交替出现“（client）sent”和“（server）received”，但实际结果大多不是这样，会出现几个“（client）sent”连续后再几个“（server）received”，请分析原因。

在这个程序中，客户端进程和服务器进程都是并发运行的，它们之间的通信是通过共享的消息队列来实现的。由于进程的调度是由操作系统决定的，因此进程的执行顺序是不确定的。这导致在实际运行中，客户端发送的多条消息和服务器接收的多条消息可能不是交替出现的，而是在一段时间内连续出现，这是很正常的行为。另外，由于消息队列是一个共享的资源，多个进程都可以对它进行操作，因此在实际运行中可能会出现一些竞争条件。例如，当客户端进程和服务器进程同时试图从空队列中读取消息时，服务器进程可能会阻塞等待，直到有消息到达为止。同样地，当客户端进程试图向满队列中发送消息时，它可能会阻塞等待，直到有空闲空间为止。这些情况都可能导致程序的行为与预期不同。因此，在编写使用消息队列进行进程间通信的程序时，需要考虑这些竞争条件，并采取相应的措施来避免它们。

**五、小结与心得体会**

加深了我对Linux操作系统的进程进程间消息通信机制的了解，也能更加熟练的使用fork()函数，也学会了系统调用函数的使用以及相关命令的运用。值得注意的是多个进程是并发运行时，通信是通过共享的消息队列来实现，调度是由操作系统来决定，因此进程执行顺序是不确定的。

**一、实验题目**

**实验四 Windows 线程的互斥与同步**

**二、实验目的**

(1) 回顾操作系统进程、线程的有关概念，加深对 Windows 线程的理解。

(2) 了解互斥体对象，利用互斥与同步操作编写生产者-消费者问题的并发程序，加深对 P (即semWait)、V(即semSignal)原语以及利用 P、V 原语进行进程间同步与互斥操作的理解。

**三、实验内容**

**生产者消费者问题**

步骤 1：创建一个“Win32 Consol Application”工程，然后拷贝清单 5-1 中的程序，编译成可执行文件。

步骤 2：在“命令提示符”窗口运行步骤 1 中生成的可执行文件，列出运行结果。

步骤 3：仔细阅读源程序，找出创建线程的 WINDOWS API 函数，回答下列问题：线程的第一个执行函数是什么（从哪里开始执行）？它位于创建线程的 API 函数的第几个参数中？

步骤 4：修改清单 5-1 中的程序，调整生产者线程和消费者线程的个数，使得消费者数目大于生产者，看看结果有何不同。察看运行结果，从中你可以得出什么结论？

步骤 5：修改清单 5-1 中的程序，按程序注释中的说明修改信号量 EmptySemaphore 的初始化方法，看看结果有何不同。

步骤 6：根据步骤 4 的结果，并查看 MSDN，回答下列问题：

1）CreateMutex 中有几个参数，各代表什么含义。

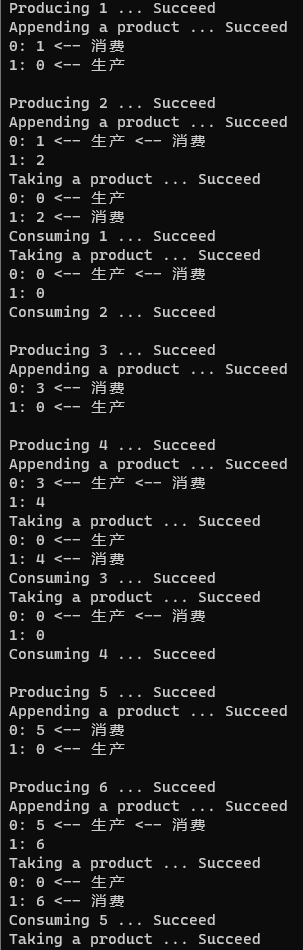
2）CreateSemaphore 中有几个参数，各代表什么含义，信号量的初值在第几个参数中。

3）程序中 P、V 原语所对应的实际 Windows API 函数是什么，写出这几条语句。

4）CreateMutex 能用 CreateSemaphore 替代吗？尝试修改程序 5-1，将信号量 Mutex 完全用CreateSemaphore 及相关函数实现。写出要修改的语句。

1. **实验结果与分析**

**（1）步骤2：**

****

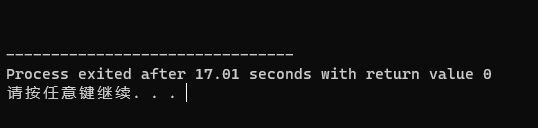
**（2）步骤3**：

创建线程的 WINDOWS API 函数是CreateThread函数，线程的第一个执行函数是Produce()，它位于CreateThread的第三个参数中。这个参数是一个指向线程函数的指针，当线程被创建时，它将从这个函数开始执行。

**（3）步骤4：**

当生产者个数多于消费者个数时，生产速度快，生产者经常等待消费者；反之，消费者经常等待

**（4）步骤5：**



结果为空，因为在信号量被创建时，缓冲区中没有空闲位置可用，即初始状态下缓冲区是满的。

1. **步骤6：**
2. CreateMutex 中有几个参数，各代表什么含义。

三个

第一个参数是一个指向 SECURITY\_ATTRIBUTES 结构体的指针，用于指定互斥量的安全属性，通常可以设为 NULL，表示使用默认安全属性。

第二个参数指定互斥量的初始拥有者。 FALSE表示互斥量没有初始拥有者。

第三个参数指定互斥量对象的名称，通常可以设为 NULL，表示互斥量对象没有名称。

1. CreateSemaphore 中有几个参数，各代表什么含义，信号量的初值在第几个参数中。

四个

第一个参数是一个指向 SECURITY\_ATTRIBUTES 结构体的指针，用于指定信号量的安全属性，通常可以设为 NULL，表示使用默认安全属性。

第二个参数指定信号量的初始计数器值。当参数的值为 SIZE\_OF\_BUFFER，即缓冲区的大小，表示在信号量被创建时，缓冲区中有 SIZE\_OF\_BUFFER 个空闲位置可用。

第三个参数指定信号量的最大计数器值。参数的值为 SIZE\_OF\_BUFFER，表示信号量的计数器最大值与缓冲区的大小相等。

第四个参数指定信号量对象的名称，通常可以设为 NULL，表示信号量对象没有名称。

1. 程序中 P、V 原语所对应的实际 Windows API 函数是什么，写出这几条语句。

P(full)：WaitForSingleObject(FullSemaphore,INFINITE)

V(full)：ReleaseSemaphore(FullSemaphore,1,NULL)

P(mutex)：WaitForSingleObject(Mutex,INFINITE)

V(mutex)：ReleaseMutex(Mutex)

p(empty)：WaitForSingleObject(EmptySemaphore,INFINITE)

V(empty)：ReleaseSemaphore(EmptySemaphore,1,NULL)

4）CreateMutex 能用 CreateSemaphore 替代吗？尝试修改程序 5-1，将信号量 Mutex 完全用CreateSemaphore 及相关函数实现。写出要修改的语句。

可以

Mutex = CreateMutex(NULL,FALSE,NULL)修改为Mutex =CreateSemaphore(NULL,FA

LSE,FALSE,NULL);生产者、消费者体内：ReleaseMutex(Mutex)修改为ReleaseSemaphore(Mutex,1,NULL)。

**五、小结与心得体会**

加深了我对Windows线程的了解，了解互斥体对象，基本掌握了互斥与同步操作编写生产者-消费者问题的并发程序，加深对 P (即semWait)、V(即 semSignal)原语以及利用 P、V 原语进行进程间同步与互斥操作的理解。

**一、实验题目**

**实验五 内存管理**

**二、实验目的**

了解 Windows 的内存结构和虚拟内存的管理，理解进程的虚拟内存空间和物理内存的映射关系。加深对操作系统内存管理、虚拟存储管理等理论知识的理解。

**三、实验内容**

了解和检测进程的虚拟内存空间。

**步骤 1：**创建一个“Win32 Consol Application”工程，然后拷贝清单 6-1 中的程序，编译成可执行文件。

**步骤 2：**在 VC 的工具栏单击“Execute Program”(执行程序) 按钮，或者按 Ctrl + F5 键，或者在“命令提示符”窗口运行步骤 1 中生成的可执行文件。

**步骤 3**：根据运行结果，回答下列问题

虚拟内存每页容量为：\_\_\_\_\_4.00 KB\_\_\_\_\_ 最小应用地址：\_\_\_0x00010000\_\_\_\_

最大应用地址：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_0x7ffffffeffff\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

当前可供应用程序使用的内存空间为：\_\_\_\_\_\_\_\_\_\_\_\_\_\_3.99 GB\_\_\_\_\_\_\_\_\_\_\_\_\_\_

当前计算机的实际内存大小为：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_32G\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

理论上每个 Windows 应用程序可以独占的最大存储空间是：\_\_\_\_\_\_4GB\_\_\_\_\_\_\_

|  |
| --- |
| **提示**：可供应用程序使用的内存空间实际上已经减去了开头与结尾两个 64KB 的保护区。虚拟内存空间中的64KB保护区是防止编程错误的一种 Windows 方式。任何对内存中这一区域 的访问 (读、写、执行) 都将引发一个错误陷阱，从而导致错误并终止程序的执行。 |

按 committed、reserved、free 等三种虚拟地址空间分别记录实验数据。其中“描述”是指对该组数据的简单描述，例如，对下列一组数据：

00010000 – 00012000 <8.00KB> Committed, READWRITE, Private

可描述为：具有 READWRITE 权限的已调配私有内存区。

将系统当前的自由区 (free) 虚拟地址空间按表 6-3 格式记录

表 6-3 实验记录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 地址 | 大小 | 虚拟地址  空间类型 | 访问权限 | 描述 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 00023000-00030000 | (52.0KB) | Free | NOACCESS | 拒绝访问 |
| 0004f000-00050000 | (4.00KB) | Free | NOACCESS | 拒绝访问 |
| 00054000-00060000 | (48.0KB) | Free | NOACCESS | 拒绝访问 |
| 00062000-00070000 | (56.0KB) | Free | NOACCESS | 拒绝访问 |
| 000a1000-000b0000 | (60.0KB) | Free | NOACCESS | 拒绝访问 |
| 000b3000-000c0000 | (52.0KB) | Free | NOACCESS | 拒绝访问 |
| 00122000-00130000 | (56.0KB) | Free | NOACCESS | 拒绝访问 |
| 001fe000-00200000 | (8.00KB) | Free | NOACCESS | 拒绝访问 |
| 0041e000-00420000 | (8.00KB) | Free | NOACCESS | 拒绝访问 |
| 00651000-00660000 | (60.0KB) | Free | NOACCESS | 拒绝访问 |
| 00661000-00670000 | (60.0KB) | Free | NOACCESS | 拒绝访问 |
| 00671000-00680000 | (60.0KB) | Free | NOACCESS | 拒绝访问 |
| 00681000-00690000 | (60.0KB) | Free | NOACCESS | 拒绝访问 |
| 006f2000-00700000 | (56.0KB) | Free | NOACCESS | 拒绝访问 |
| 00708000-00710000 | (32.0KB) | Free | NOACCESS | 拒绝访问 |
| 00719000-00740000 | (156KB) | Free | NOACCESS | 拒绝访问 |
| 00750000-007a0000 | (320KB) | Free | NOACCESS | 拒绝访问 |
| 01221000-01230000 | (60.0KB) | Free | NOACCESS | 拒绝访问 |
| 02631000-02640000 | (60.0KB) | Free | NOACCESS | 拒绝访问 |
| 02740000-61440000 | (1.48GB) | Free | NOACCESS | 拒绝访问 |
| 6145a000-64940000 | (52.8MB) | Free | NOACCESS | 拒绝访问 |
| 64955000-6fc40000 | (178MB) | Free | NOACCESS | 拒绝访问 |
| 6fda3000-7ffe0000 | (258MB) | Free | NOACCESS | 拒绝访问 |
| 7ffe1000-7ffe4000 | (12.0KB) | Free | NOACCESS | 拒绝访问 |
| 7ffe5000-7ff4fdec0000 | (1.96GB) | Free | NOACCESS | 拒绝访问 |
| 7ff5fffe1000-7ff5ffff0000 | (60.0KB) | Free | NOACCESS | 拒绝访问 |
| 7ff5ffff1000-7ffdd9cc0000 | (3.40GB) | Free | NOACCESS | 拒绝访问 |
| 7ffdd9dc0000-7ffddc740000 | (41.5MB) | Free | NOACCESS | 拒绝访问 |
| 7ffddc7d7000-7ffddf6f0000 | (47.0MB) | Free | NOACCESS | 拒绝访问 |
| 7ffddf801000-7ffddf810000 | (60.0KB) | Free | NOACCESS | 拒绝访问 |
| 7ffddf8aa000-7ffddf8b0000 | (24.0KB) | Free | NOACCESS | 拒绝访问 |
| 7ffddfc53000-7ffddfd90000 | (1.23MB) | Free | NOACCESS | 拒绝访问 |
| 7ffddfea8000-7ffddfeb0000 | (32.0KB) | Free | NOACCESS | 拒绝访问 |
| 7ffddfed6000-7ffde00b0000 | (1.85MB) | Free | NOACCESS | 拒绝访问 |
| 7ffde00e1000-7ffde00f0000 | (60.0KB) | Free | NOACCESS | 拒绝访问 |
| 7ffde014e000-7ffde09d0000 | (8.50MB) | Free | NOACCESS | 拒绝访问 |
| 7ffde0d59000-7ffde0f10000 | (1.71MB) | Free | NOACCESS | 拒绝访问 |
| 7ffde0fb7000-7ffde0fc0000 | (36.0KB) | Free | NOACCESS | 拒绝访问 |
| 7ffde10b1000-7ffde1260000 | (1.68MB) | Free | NOACCESS | 拒绝访问 |
| 7ffde1322000-7ffde13d0000 | (696KB) | Free | NOACCESS | 拒绝访问 |
| 7ffde157b000-7ffde17f0000 | (2.45MB) | Free | NOACCESS | 拒绝访问 |
| 7ffde1819000-7ffde20f0000 | (8.83MB) | Free | NOACCESS | 拒绝访问 |
| 7ffde2207000-7ffde2250000 | (292KB) | Free | NOACCESS | 拒绝访问 |
| 7ffde2464000-7fffffff0000 | (475MB) | Free | NOACCESS | 拒绝访问 |

|  |
| --- |
| **提示：**详细记录实验数据在实验活动中是必要的，但想想是否可以简化记录的办法？ |

解决：可以通过将数据复制到电子表格中，然后进行数据的分列，数据合并。

将系统当前的已调配区 (committed) 虚拟地址空间按表 6-4 格式记录

表 6-4 实验记录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 地址 | 大小 | 虚拟地址  空间类型 | 访问权限 | 描述 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 00010000-00020000 | (64.0KB) | Committed | READWRITE | Mapped |
| 00020000-00023000 | (12.0KB) | Committed | READONLY | Mapped |
| 00030000-0004f000 | (124KB) | Committed | READONLY | Mapped |
| 00050000-00054000 | (16.0KB) | Committed | READONLY | Mapped |
| 00060000-00062000 | (8.00KB) | Committed | READWRITE | Private |
| 00070000-000a1000 | (196KB) | Committed | READONLY | Mapped |
| 000b0000-000b3000 | (12.0KB) | Committed | READONLY | Mapped |
| 000c0000-000c2000 | (8.00KB) | Committed | READWRITE | Private |
| 00130000-001fe000 | (824KB) | Committed | READONLY | Mapped |
| 003f7000-00400000 | (36.0KB) | Committed | READWRITE | Private |
| 00400000-00401000 | (4.00KB) | Committed | READONLY | Image |
| 00401000-00404000 | (12.0KB) | Committed | EXECUTE\_READ | Image |
| 00404000-00405000 | (4.00KB) | Committed | READWRITE | Image |
| 00405000-00408000 | (12.0KB) | Committed | READONLY | Image |
| 00408000-0040a000 | (8.00KB) | Committed | READWRITE | Image |
| 0040a000-0040c000 | (8.00KB) | Committed | WRITECOPY | Image |
| 0040c000-0041e000 | (72.0KB) | Committed | READONLY | Image |
| 00619000-0061c000 | (12.0KB) | Committed | GUARD | READWRITE |
| 0061c000-00620000 | (16.0KB) | Committed | READWRITE | Private |
| 00620000-00651000 | (196KB) | Committed | READONLY | Mapped |
| 00660000-00661000 | (4.00KB) | Committed | READONLY | Mapped |
| 00670000-00671000 | (4.00KB) | Committed | READONLY | Mapped |
| 00680000-00681000 | (4.00KB) | Committed | READONLY | Mapped |
| 00690000-00691000 | (4.00KB) | Committed | READWRITE | Private |
| 00700000-00704000 | (16.0KB) | Committed | READONLY | Mapped |
| 00710000-00719000 | (36.0KB) | Committed | READONLY | Mapped |
| 00740000-00747000 | (28.0KB) | Committed | READWRITE | Private |
| 007a0000-007c6000 | (152KB) | Committed | READWRITE | Private |
| 00a99000-00a9c000 | (12.0KB) | Committed | GUARD | READWRITE |
| 00a9c000-00aa0000 | (16.0KB) | Committed | READWRITE | Private |
| 00c9b000-00c9e000 | (12.0KB) | Committed | GUARD | READWRITE |
| 00c9e000-00ca0000 | (8.00KB) | Committed | READWRITE | Private |
| 00e9b000-00e9e000 | (12.0KB) | Committed | GUARD | READWRITE |
| 00e9e000-00ea0000 | (8.00KB) | Committed | READWRITE | Private |
| 00ea0000-00f1b000 | (492KB) | Committed | READONLY | Mapped |
| 010a0000-01221000 | (1.50MB) | Committed | READONLY | Mapped |
| 01230000-015d1000 | (3.62MB) | Committed | READONLY | Mapped |
| 02640000-02654000 | (80.0KB) | Committed | READWRITE | Private |
| 61440000-61441000 | (4.00KB) | Committed | READONLY | Image |
| 61441000-61450000 | (60.0KB) | Committed | EXECUTE\_READ | Image |
| 61450000-61451000 | (4.00KB) | Committed | READWRITE | Image |
| 61451000-61454000 | (12.0KB) | Committed | READONLY | Image |
| 61454000-61455000 | (4.00KB) | Committed | READWRITE | Image |
| 61455000-61456000 | (4.00KB) | Committed | READONLY | Image |
| 61456000-61457000 | (4.00KB) | Committed | READWRITE | Image |
| 61457000-61459000 | (8.00KB) | Committed | WRITECOPY | Image |
| 61459000-6145a000 | (4.00KB) | Committed | READONLY | Image |
| 64940000-64941000 | (4.00KB) | Committed | READONLY | Image |
| 64941000-64949000 | (32.0KB) | Committed | EXECUTE\_READ | Image |
| 64949000-6494a000 | (4.00KB) | Committed | READWRITE | Image |
| 6494a000-6494d000 | (12.0KB) | Committed | READONLY | Image |
| 6494d000-6494e000 | (4.00KB) | Committed | READWRITE | Image |
| 6494e000-64950000 | (8.00KB) | Committed | READONLY | Image |
| 64950000-64951000 | (4.00KB) | Committed | READWRITE | Image |
| 64951000-64954000 | (12.0KB) | Committed | WRITECOPY | Image |
| 64954000-64955000 | (4.00KB) | Committed | READONLY | Image |
| 6fc40000-6fc41000 | (4.00KB) | Committed | READONLY | Image |
| 6fc41000-6fd08000 | (796KB) | Committed | EXECUTE\_READ | Image |
| 6fd08000-6fd0c000 | (16.0KB) | Committed | READWRITE | Image |
| 6fd0c000-6fd43000 | (220KB) | Committed | READONLY | Image |
| 6fd43000-6fd45000 | (8.00KB) | Committed | READWRITE | Image |
| 6fd45000-6fd9d000 | (352KB) | Committed | READONLY | Image |
| 6fd9d000-6fd9e000 | (4.00KB) | Committed | READWRITE | Image |
| 6fd9e000-6fda1000 | (12.0KB) | Committed | WRITECOPY | Image |
| 6fda1000-6fda3000 | (8.00KB) | Committed | READONLY | Image |
| 7ffe0000-7ffe1000 | (4.00KB) | Committed | READONLY | Private |
| 7ffe4000-7ffe5000 | (4.00KB) | Committed | READONLY | Private |
| 7ff4fdec0000-7ff4fdec5000 | (20.0KB) | Committed | READONLY | Mapped |
| 7ff5fffe0000-7ff5fffe1000 | (4.00KB) | Committed | READWRITE | Private |
| 7ff5ffff0000-7ff5ffff1000 | (4.00KB) | Committed | READONLY | Mapped |
| 7ffdd9cc0000-7ffdd9cc1000 | (4.00KB) | Committed | READONLY | Image |
| 7ffdd9cc1000-7ffdd9d69000 | (672KB) | Committed | EXECUTE\_READ | Image |
| 7ffdd9d69000-7ffdd9dad000 | (272KB) | Committed | READONLY | Image |
| 7ffdd9dad000-7ffdd9daf000 | (8.00KB) | Committed | READWRITE | Image |
| 7ffdd9daf000-7ffdd9dc0000 | (68.0KB) | Committed | READONLY | Image |
| 7ffddc740000-7ffddc741000 | (4.00KB) | Committed | READONLY | Image |
| 7ffddc741000-7ffddc793000 | (328KB) | Committed | EXECUTE\_READ | Image |
| 7ffddc793000-7ffddc7b7000 | (144KB) | Committed | READONLY | Image |
| 7ffddc7b7000-7ffddc7ba000 | (12.0KB) | Committed | READWRITE | Image |
| 7ffddc7ba000-7ffddc7d7000 | (116KB) | Committed | READONLY | Image |

将系统当前的保留区 (reserved) 虚拟地址空间按表 6-5 格式记录。

表 6-5 实验记录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 地址 | 大小 | 虚拟地址  空间类型 | 访问权限 | 描述 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 000c2000-00122000 | (384KB) | Reserved | READONLY | Private |
| 00200000-003f7000 | (1.96MB) | Reserved | READONLY | Private |
| 00420000-00619000 | (1.97MB) | Reserved | READONLY | Private |
| 00691000-006f2000 | (388KB) | Reserved | READONLY | Private |
| 00704000-00708000 | (16.0KB) | Reserved | READONLY | Mapped |
| 00747000-00750000 | (36.0KB) | Reserved | READONLY | Private |
| 007c6000-008a0000 | (872KB) | Reserved | READONLY | Private |
| 008a0000-00a99000 | (1.97MB) | Reserved | READONLY | Private |
| 00aa0000-00c9b000 | (1.98MB) | Reserved | READONLY | Private |
| 00ca0000-00e9b000 | (1.98MB) | Reserved | READONLY | Private |
| 00f1b000-010a0000 | (1.51MB) | Reserved | READONLY | Mapped |
| 015d1000-02631000 | (16.3MB) | Reserved | READONLY | Mapped |
| 02654000-02740000 | (944KB) | Reserved | READONLY | Private |
| 7ff4fdec5000-7ff4fdfc0000 | (0.98MB) | Reserved | READONLY | Mapped |
| 7ff4fdfc0000-7ff5fdfe0000 | (128KB) | Reserved | READONLY | Private |
| 7ff5fdfe0000-7ff5fffe0000 | (32.0MB) | Reserved | READONLY | Private |

1. **实验结果与分析**

**（1）报错：**

问题1：将void改为int

问题2：error: cast from 'LPCVOID' {aka 'const void\*'} to 'DWORD' {aka 'long unsigned int'} loses precision [-fpermissive]|

解决：将(DWORD)改为(DWORD64)

问题3：显示StrFormatByteSize()不可以用

解决：没有链接库，右击项目名称—>build options—>link settings—>other linker options—>添加lshlwapi

**（2）**该程序从主函数Main()出发，调用void WalkVM(HANDLE hProcess)函数，void WalkVM(HANDLEhProcess)函数获得系统信息，分配应用程序内存地址空间。然后开始做循环，从函数运行开始每次获得下一个虚拟程序内存块的信息，之后计算块的结尾及大小，然后再显示块的大小与位置，状态，显示保护方式(void ShowProtection(DWORD dwTarget))，将文件名显示出来，移动块指针获得下一块，依次这样循环下去，直至结束。

**五、小结与心得体会**

了解了内存结构和虚拟内存的管理，理解了进程的虚拟内存空间和物理内存的映射关系。了解了Virtual QueryEX() API 等虚拟内存API的作用及使用方法

**设计类实验的正文格式如下：**

**一、实验题目（四号宋体，加粗，以下标题的字体格式与此相同）**

**二、实验目的**

例如：掌握使用银行家算法避免死锁问题。（小四号宋体，以下段内字体格式与此相同）

**三、总体设计（含背景知识或基本原理与算法、或模块介绍、设计步骤等）**

**四、详细设计（含主要的数据结构、程序流程图、关键代码等）**

（正文小四号宋体，关键源代码五号字体）

**五、实验结果与分析**

**六、小结与心得体会**