操作系统课程设计实验报告

实验名称：　　内存和进程地址空间实时显示

姓名/学号：　　卜梦煜/1120192419

一、　实验目的

熟悉 Windows 系统存储器管理内存管理的虚拟页式存储器机制，包括系统主存地址空间的组织与分配方式，虚拟内存的管理，查看物理内存的使用情况，查看正在运行进程的虚拟地址详细情况与工作集信息。

二、　实验内容

设计一个内存监视器，能实时地显示当前系统中内存的使用情况，包括系统地址空间的布局，物理内存的使用情况；能实时显示某个进程的虚拟地址空间布局和工作集信息等。

相关的系统调用：GetSystemInfo(), VirtualQueryEx(), GetPerformanceInfo(), GlobalMemoryStatusEx() …

三、　实验环境

1. 硬件环境

2. 软件环境

Visual Studio Community 2019　16.11.3

四、 原理分析

本任务可分为三个子任务：查询系统信息、查询所有在运行进程、查询某个在运行进程的详细信息。

1. 查询系统信息

与查询系统信息相关的系统调用 API 包括：GlobalMemoryStatusEx()、GetSystemInfo()、GetPerformanceInfo()，分别查询系统的内存信息、基本信息、性能信息。

（1）GlobalMemoryStatusEx()函数

该函数原型为：

BOOL GlobalMemoryStatusEx(LPMEMORYSTATUSEX lpBuffer)

用于获取当前系统物理内存与虚拟内存的信息，并保存在 MEMORYSTATUSEX 结构体中。MEMORYSTATUSEX 结构体中重要参数如下：

1）dwMemoryLoad，以 B 为单位，反映当前物理内存的使用率。

2）ullTotalPhys，以 B 为单位，反映物理内存的总大小，即内存条容量。

3）ullAvailPhys，以 B 为单位，反映物理内存可用大小，等于总大小×(1-使用率)。

4）ullTotalPageFile，以 B 为单位，反映总交换文件大小，与 Windows 文件交换区有关。

5）ullAvailPageFile，以 B 为单位，反映可用交换文件大小。

6）ullTotalVirtual，以 B 为单位，反映总虚拟内存大小，与硬件设计相关。

7）ullAvailVirtual，以 B 为单位，反映当前可用虚拟内存大小。

8）ullAvailExtendedVirtual，以 B 为单位，反映扩展内存大小。

（2）GetSystemInfo()函数

该函数原型为：

VOID GetSystemInfo(LPSYSTEM_INFO lpSystemInfo)

用于获取系统基本信息，并保存在 SYSTEM_INFO 结构体中。SYSTEM_INFO 结构体重要参数如下：

1）dwPageSize，反映系统页面大小，一般为 4KB。

2）lpMinimumApplicationAddress，反映进程私有地址空间可访问的最小内存地址。

3）lpMaximumApplicationAddress，反映进程私有地址空间可访问的最大内存地址。

4）dwAllocationGranularity，反映系统分配粒度。这是 Windows 为解决碎片问题提出的分配方案，即当请求分配的内存大小小于分配粒度时，按分配粒度分配内存。系统粒度一般固化在硬件上，一般为 64KB。

（3）GetPerformanceInfo()函数

该函数原型为：

BOOL GetPerformanceInfo

(PPERFORMANCE_INFORMATION pPerformanceInformation, DWORD cb)

用于获取系统性能信息，存在 PERFORMANCE_INFORMATION 结构体中。结构体主要参数如下：

1）PhysicalTotal，以页为单位，反映物理内存总大小。

2）PhysicalAvailable，以页为单位，反映物理内存的总大小。

3）SystemCache，以页为单位，反映系统缓存 cache 大小。

4）PageSize，以 B 为单位，反映页的大小。

5）HandleCount，反映当前打开的句柄数。

6）ProcessCount，反映当前正在运行的进程数。

7）ThreadCount，反映当前正在运行的线程数。

2. 查询所有在运行进程

相关的系统调用 API 有：CreateToolhelp32Snapshot()、Process32First()、Process32Next()、OpenProcess()、GetProcessMemoryInfo()。

CreateToolhelp32Snapshot()用于获取系统进程快照的句柄；Process32First()、Process32Next()用于按句柄遍历进程，并将快照进程信息保存在 PROCESSENTRY32 结构体中；OpenProcess()、GetProcessMemoryInfo()用于按照进程 id 打开和提取进程信息，保存在 PROCESS_MEMORY_COUNTERS 结构体中。

3. 查询某个在运行进程的详细信息

相关的系统调用 API 有：GetSystemInfo()、VirtualQueryEx()、GetModuleFileName()。

GetSystemInfo()获取系统信息，VirtualQueryEx()获得进程虚拟空间信息。利

用 lpMinimumApplicationAddress、lpMaximumApplicationAddress 得到进程虚拟地址起止范围，利用 RegionSize 得到进程内存块大小，即可按块遍历进程内存空间。

五、 程序设计与实现

（1）CheckSystemMemory()模块

该模块调用 GlobalMemoryStatusEx() 获取系统内存信息，保存在 MEMORYSTATUSEX 结构体中查询。

（2）CheckSystemInfo()模块

该模块调用 GetSystemInfo()获取系统基本信息，保存在 SYSTEM_INFO 结构体中查询。

（3）CheckSystemPerformance()模块

该模块调用 GetPerformanceInfo ()获取系统性能信息，保存在 PERFORMANCE_INFORMATION 结构体中查询。

（4）CheckProcessInfo()模块

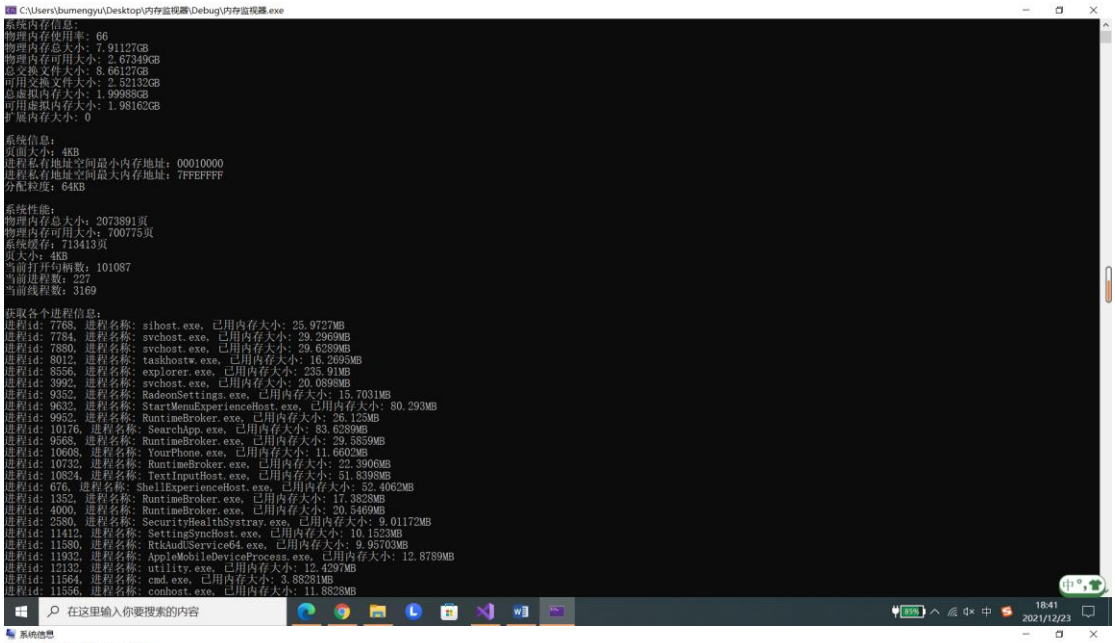
该进程调用 CreateToolhelp32Snapshot()、Process32First()、Process32Next()、OpenProcess()、GetProcessMemoryInfo()获取当前正在运行的进程的信息。

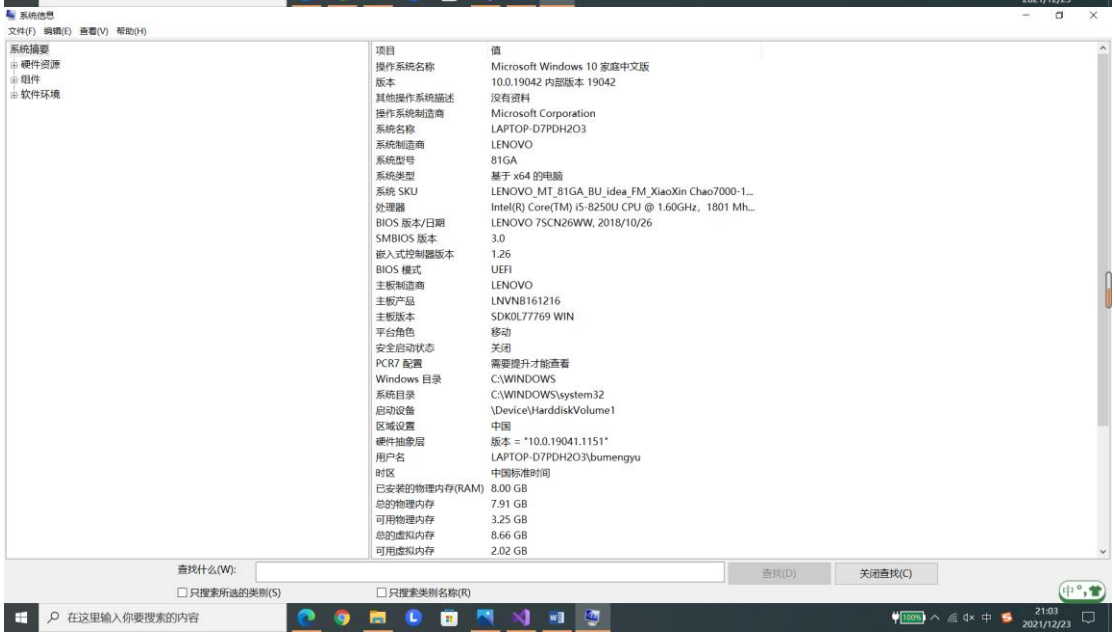
（5）WalkVM()模块

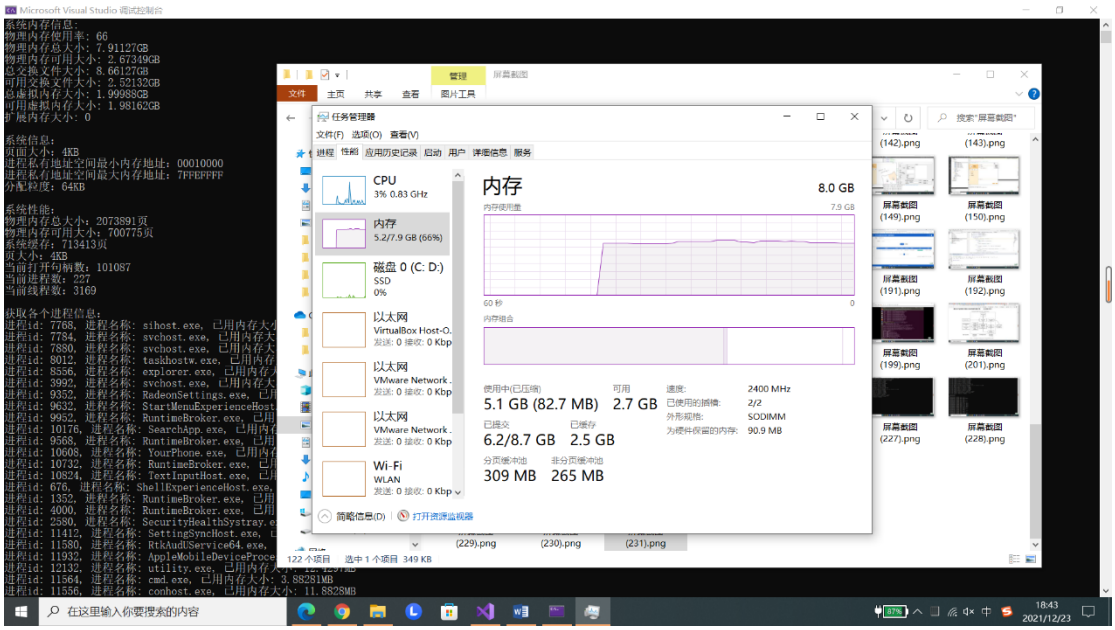
该模块调用 GetSystemInfo()、VirtualQueryEx()、GetModuleFileName()，按照进程 id 获取对应进程的详细的地址空间使用情况，包括块的内存范围、块的状态、块的显示类型、块的名称。

六、 运行结果与分析

（1）CheckSystemMemory()模块、CheckSystemInfo()模块、CheckSystemPerformance()模块


C:\Users\bumengyu\Desktop\内存监视器\Debug\内存监视器.exe
系统内存信息：
物理内存使用率：66
物理内存总大小：7.91127GB
物理内存可用大小：2.67349GB
总交换文件大小：8.66127GB
可用交换文件大小：2.52132GB
总虚拟内存大小：1.99988GB
可用虚拟内存大小：1.98162GB
扩展内存大小：0
系统信息：
页面大小：4KB
进程私有地址空间最小内存地址：00010000
进程私有地址空间最大内存地址：7FFEFFFF
分配粒度：64KB
系统性能：
物理内存总大小：2073891页
物理内存可用大小：700775页
系统缓存：713413页
页大小：4KB
当前打开句柄数：101087
当前进程数：227
当前线程数：3169
获取各个进程信息：
进程id：7768，进程名称：sihost.exe，已用内存大小：25.9727MB
进程id：7784，进程名称：svchost.exe，已用内存大小：29.2969MB
进程id：7880，进程名称：svchost.exe，已用内存大小：29.6289MB
进程id：8012，进程名称：taskhostw.exe，已用内存大小：16.2695MB
进程id：8556，进程名称：explorer.exe，已用内存大小：235.91MB
进程id：3992，进程名称：svchost.exe，已用内存大小：20.0898MB
进程id：9352，进程名称：RadeonSettings.exe，已用内存大小：15.7031MB
进程id：9632，进程名称：StartMenuExperienceHost.exe，已用内存大小：80.293MB
进程id：9952，进程名称：RuntimeBroker.exe，已用内存大小：26.125MB
进程id：10176，进程名称：SearchApp.exe，已用内存大小：83.6289MB
进程id：9568，进程名称：RuntimeBroker.exe，已用内存大小：29.5859MB
进程id：10608，进程名称：YourPhone.exe，已用内存大小：11.6602MB
进程id：10732，进程名称：RuntimeBroker.exe，已用内存大小：22.3906MB
进程id：10824，进程名称：TextInputHost.exe，已用内存大小：51.8398MB
进程id：676，进程名称：ShellExperienceHost.exe，已用内存大小：52.4062MB
进程id：1352，进程名称：RuntimeBroker.exe，已用内存大小：17.3828MB
进程id：4000，进程名称：RuntimeBroker.exe，已用内存大小：20.5469MB
进程id：2580，进程名称：SecurityHealthSystray.exe，已用内存大小：9.01172MB
进程id：11412，进程名称：SettingSyncHost.exe，已用内存大小：10.1523MB
进程id：11580，进程名称：RtkAudUService64.exe，已用内存大小：9.95703MB
进程id：11932，进程名称：AppleMobileDeviceProcess.exe，已用内存大小：12.8789MB
进程id：12132，进程名称：utility.exe，已用内存大小：12.4297MB
进程id：11564，进程名称：cmd.exe，已用内存大小：3.88281MB
进程id：11556，进程名称：conhost.exe，已用内存大小：11.8828MB
在这里输入你要搜索的内容
18:41
2021/12/23


系统信息
文件(F) 编辑(E) 查看(V) 帮助(H)
系统摘要
硬件资源
组件
软件环境
项目 值
操作系统名称 Microsoft Windows 10 家庭中文版
版本 10.0.19042 内部版本 19042
其他操作系统描述 没有资料
操作系统制造商 Microsoft Corporation
系统名称 LAPTOP-D7PDH2O3
系统制造商 LENOVO
系统型号 81GA
系统类型 基于 x64 的电脑
系统 SKU LENOVO_MT_81GA_BU_idea_FM_XiaoXin Chao7000-1...
处理器 Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz，1801 Mh...
BIOS 版本/日期 LENOVO 7SCN26WW, 2018/10/26
SMBIOS 版本 3.0
嵌入式控制器版本 1.26
BIOS 模式 UEFI
主板制造商 LENOVO
主板产品 LNVNB161216
主板版本 SDK0L77769 WIN
平台角色 移动
安全启动状态 关闭
PCR7 配置 需要提升才能查看
Windows 目录 C:\WINDOWS
系统目录 C:\WINDOWS\system32
启动设备 \Device\HarddiskVolume1
区域设置 中国
硬件抽象层 版本 = "10.0.19041.1151"
用户名 LAPTOP-D7PDH2O3\bumengyu
时区 中国标准时间
已安装的物理内存(RAM) 8.00 GB
总的物理内存 7.91 GB
可用物理内存 3.25 GB
总的虚拟内存 8.66 GB
可用虚拟内存 2.02 GB
查找什么(W):
查找(D)
关闭查找(C)
只搜索所选的类别(S)
只搜索类别名称(R)
在这里输入你要搜索的内容
21:03
2021/12/23

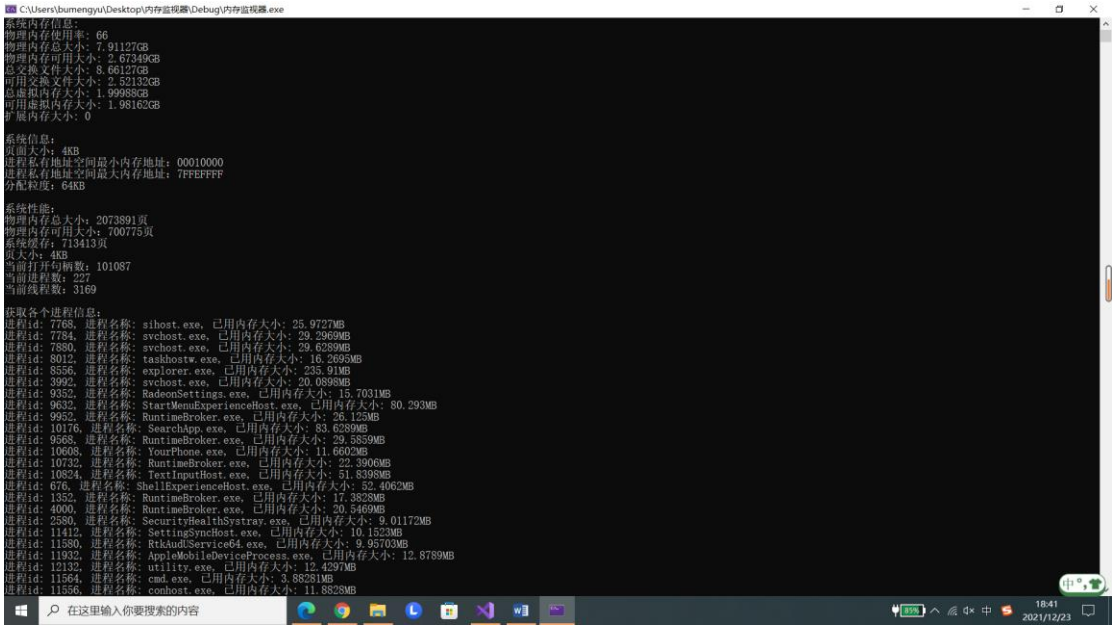


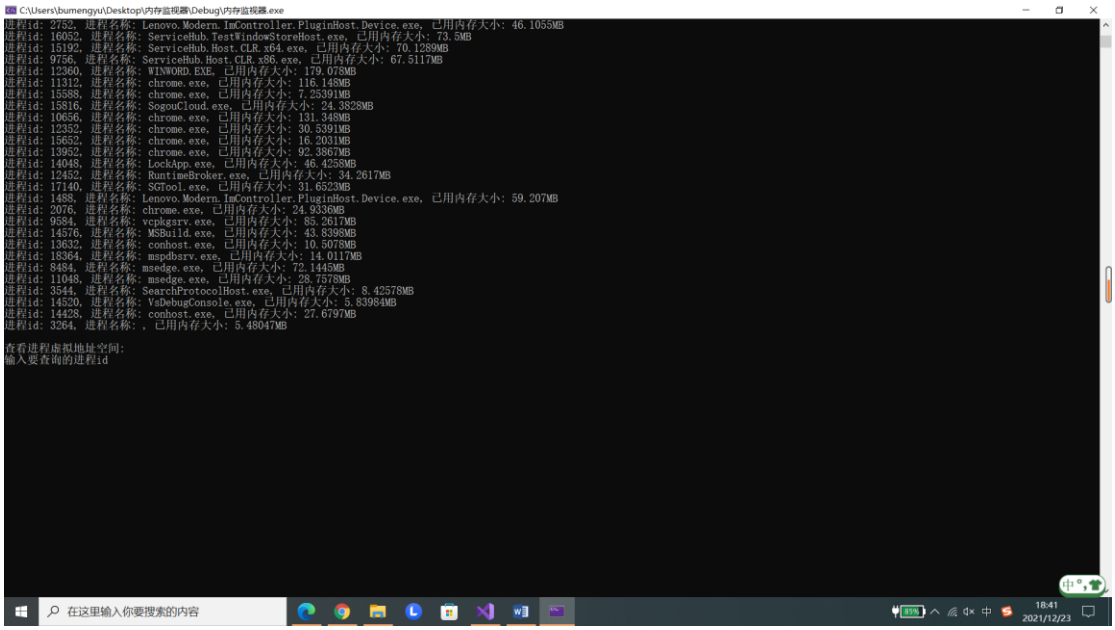
1）CheckSystemMemory()模块，物理内存总大小、可用内存总大小等信息均与系统硬件信息符合。

2）CheckSystemInfo()模块，页面大小、系统分配粒度均与系统硬件符合。进程私有空间总大小为 2GB，与 Windows 文件系统分配的每个进程的虚拟内存中私有内存空间大小符合。对进程私有空间，有 64KB 的禁入区，这是由 ntfs 文件卷定义的。

3）CheckSystemPerformance()模块，物理内存总大小、可用大小、页大小与CheckSystemMemory()模块、CheckSystemInfo()模块结果相同。打开的句柄数、当前进程数、当前线程数与任务管理器结果相同。

（2）CheckProcessInfo()模块

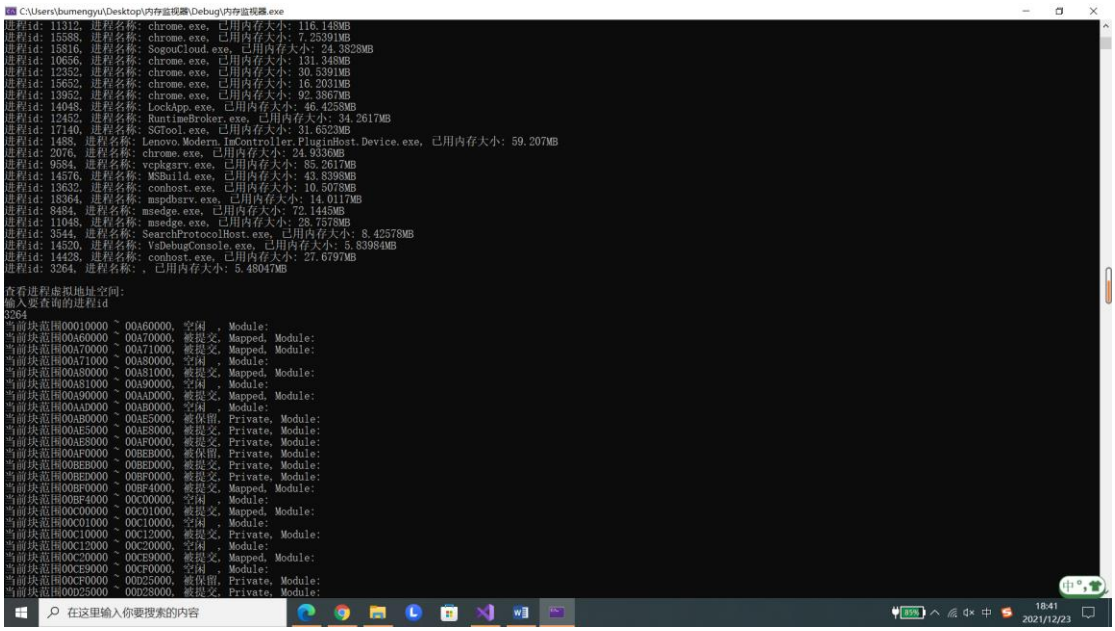


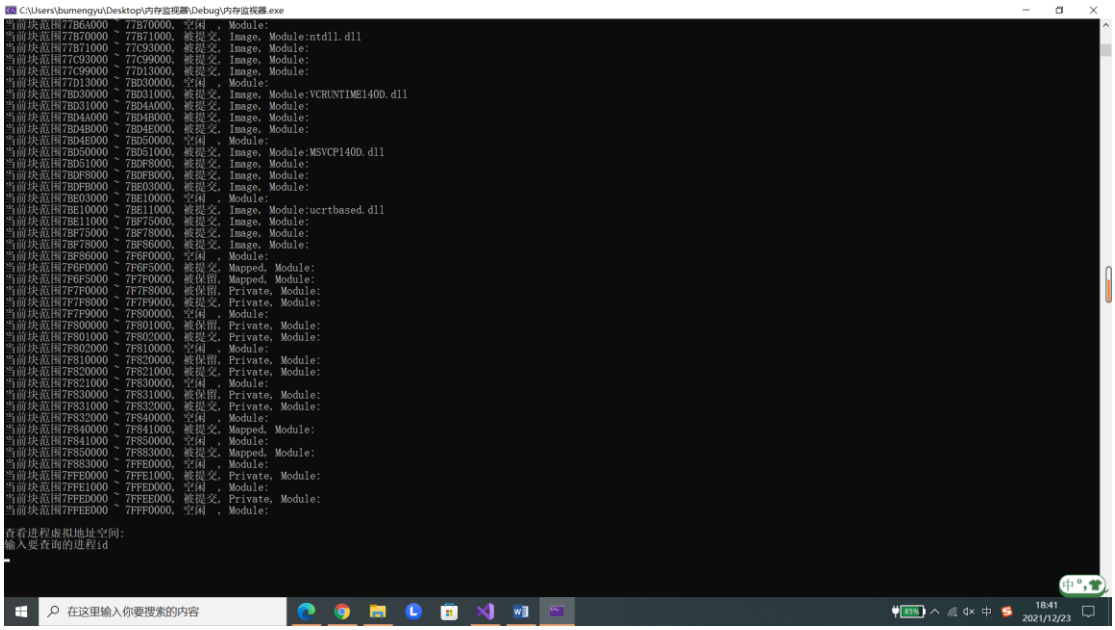


可以看到系统中正在运行的进程的简略信息，包括进程 id、进程名称、进程已用内存大小。

（3）WalkVM()模块

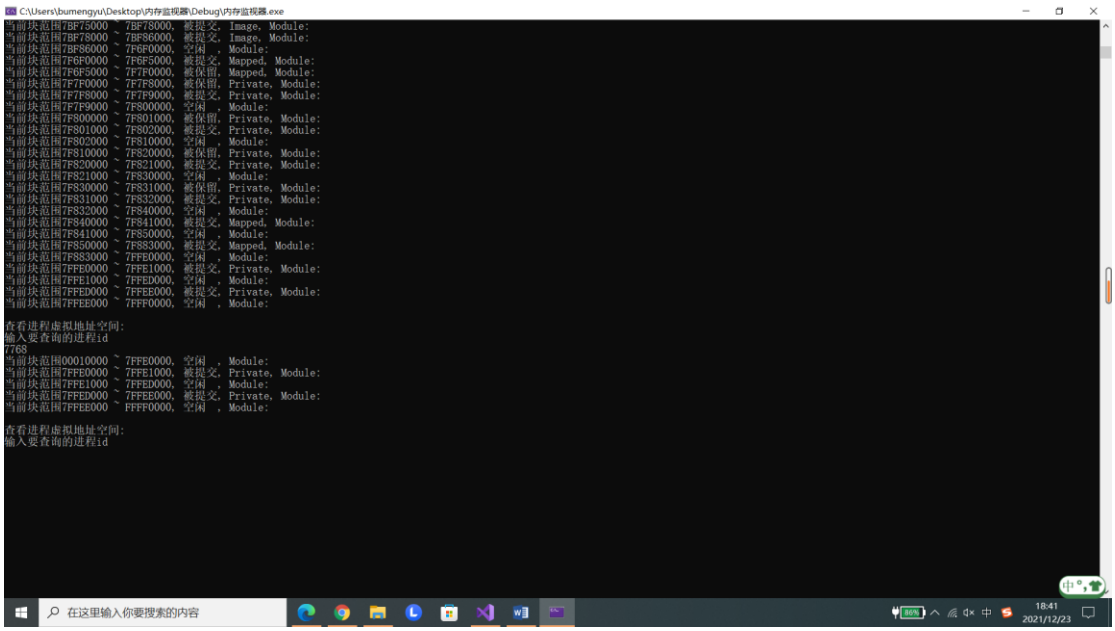
1）查询当前程序（内存管理器）的内存使用情况如下：





分析可知，分配的块大小是与系统粒度相符合的，即最小的块大小为 64KB。对于具体某个块，只有块的状态为“已提交”、块的显示类型为“Image”的块才有名称。

2）查询系统进程的内存分配如下：



相比用户自定义程序的进程，系统进程的内存从高地址开始使用，分配更加连续整齐。

七、 实验收获与体会

本实验的关键在于掌握 Windows 进程管理相关的系统 API，在程序中调用即可很方便地得到主存、进程等的信息。通过实验，我掌握了与系统存储、进程信息访问相关的函数，如 GlobalMemoryStatusEx()、GetSystemInfo()、

GetPerformanceInfo() 、 CreateToolhelp32Snapshot() 、 Process32First() 、 Process32Next() 、 OpenProcess() 、 GetProcessMemoryInfo() 、 GetSystemInfo() 、 VirtualQueryEx()、GetModuleFileName()等，也知道了各个函数的输入输出的含义、信息保存的结构等。

通过实验，我将实验中内存、进程的概念与实际的电脑硬件信息、任务管理器信息等联系了起来，得到了印证，也加深了对 Windows 存储管理的理解。