电子科技大学 计算机（网安）学院

标 准 实 验 报 告

（实验）课程名称 计算机操作系统

电子科技大学教务处制表

电 子 科 技 大 学

实 验 报 告

学生姓名：黄鑫　　学号：　2021050901013　指导教师：丁旭阳

实验地点：　主楼 A2-412　　实验时间：2023.12.9

一、实验室名称：主楼 A2-412

二、实验项目名称：虚拟内存综合实验

三、实验学时：4

四、实验原理：

1. 理解 X86 计算机的寻址机制，包括逻辑地址、线性地址、物理地址、虚拟地址的概念。

2. 编写示例程序，其中包含一个整数变量，通过查看寄存器和相关数据结构，计算变量的线性地址。

3. 使用 Bochs 虚拟机，查看寄存器信息，了解全局描述符表（GDT）、局部描述符表（LDT）等数据结构。

4. 根据段选择符、GDT 或 LDT 等信息，计算变量的线性地址。

5. 了解 CPU 的页式内存管理机制，使用 creg 查看寄存器信息。

6. 基于页式地址转换，计算变量的物理地址。

7. 实验预备知识包括物理地址、逻辑地址、线性地址、虚拟地址等概念，以及 CPU 的段式内存管理和页式内存管理原理。

8. 使用 Bochs 的常用命令，如`c`启动 Linux、`sreg`查看段寄存器值、`creg`查看控制寄存器值等。通过这些步骤，实验者能够深入理解计算机内存管理的机制。

五、实验目的：

理解内存管理机制： 通过实验，学习和理解计算机系统中的段页式内存管理机制，深入掌握逻辑地址、线性地址、物理地址和虚拟地址之间的关系。

熟悉实验环境： 在 Linux 内核（0.11）和 Bochs 虚拟机的环境下，学生将获得对实验操作所需的基本环境和工具的熟悉。

加强编程和调试技能： 通过编写示例程序，学生将了解如何通过手工查看系统内存、修改特定物理内存的值，实现对程序运行的控制。同时，熟悉使用 Bochs 调试工具进行寄存器查看和程序执行的监测。

六、实验内容：

通过手工查看系统内存，并修改特定物理内存的值，实现控制程序运行的目的。

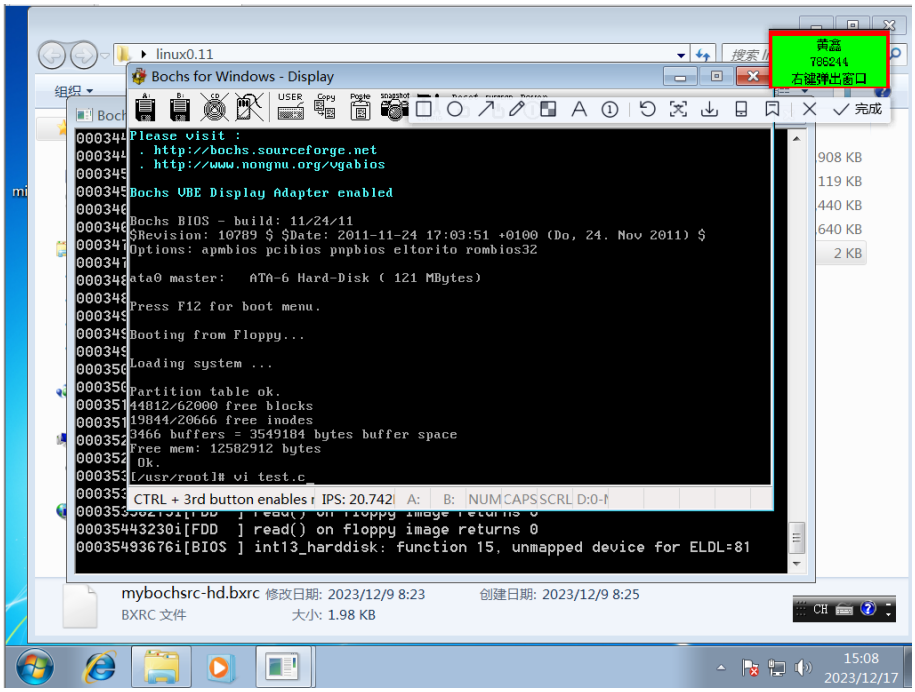
七、实验器材（设备、元器件）：

Linux 内核（0.11）+ Bochs

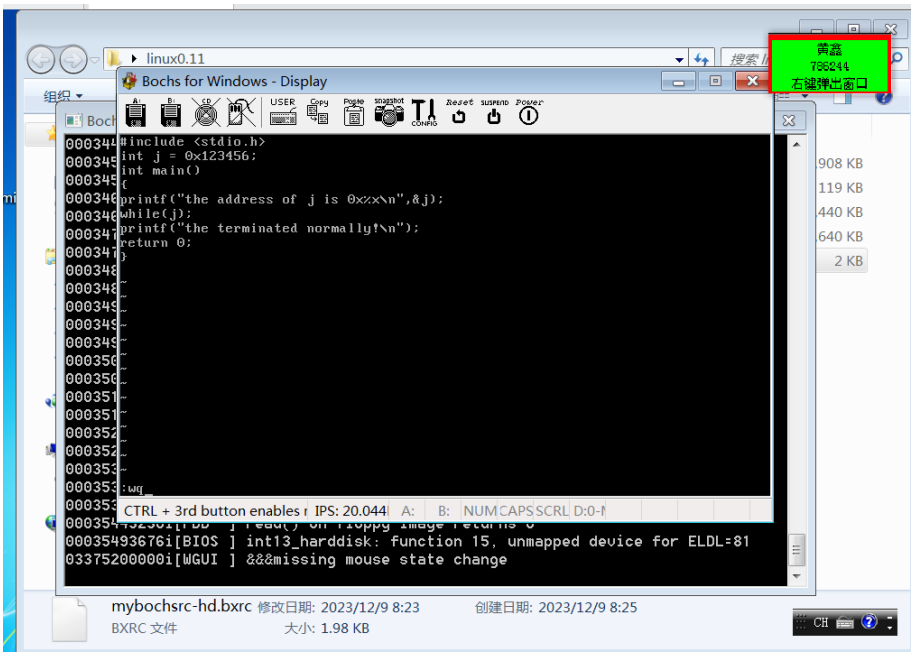
一台 PC

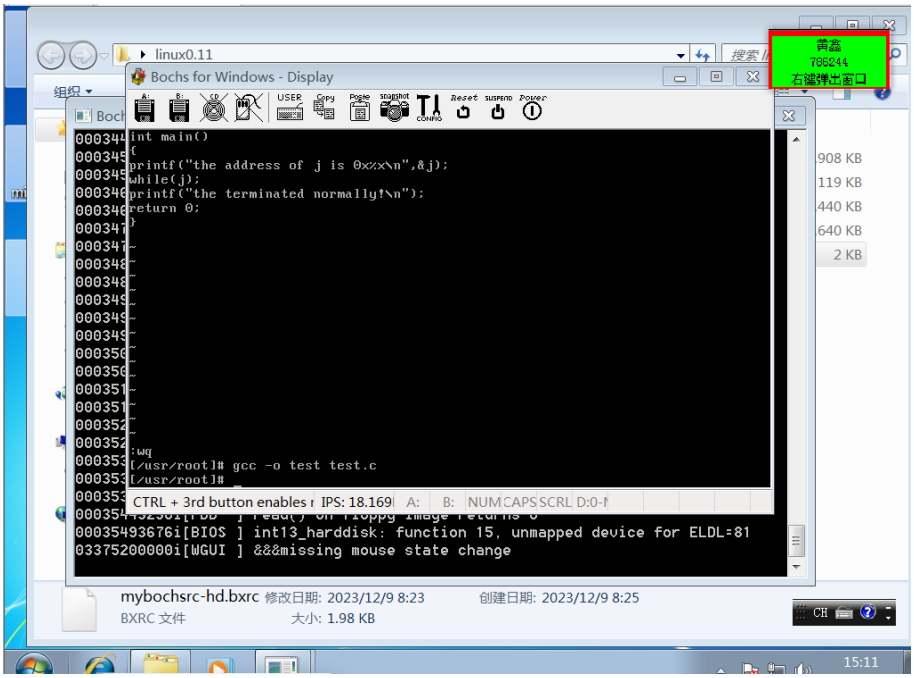
八、实验步骤：

1. 在根目录新建文件夹，并新建 test.c 文件，使用“vi test.c”命令对 test.c 文件进行编辑

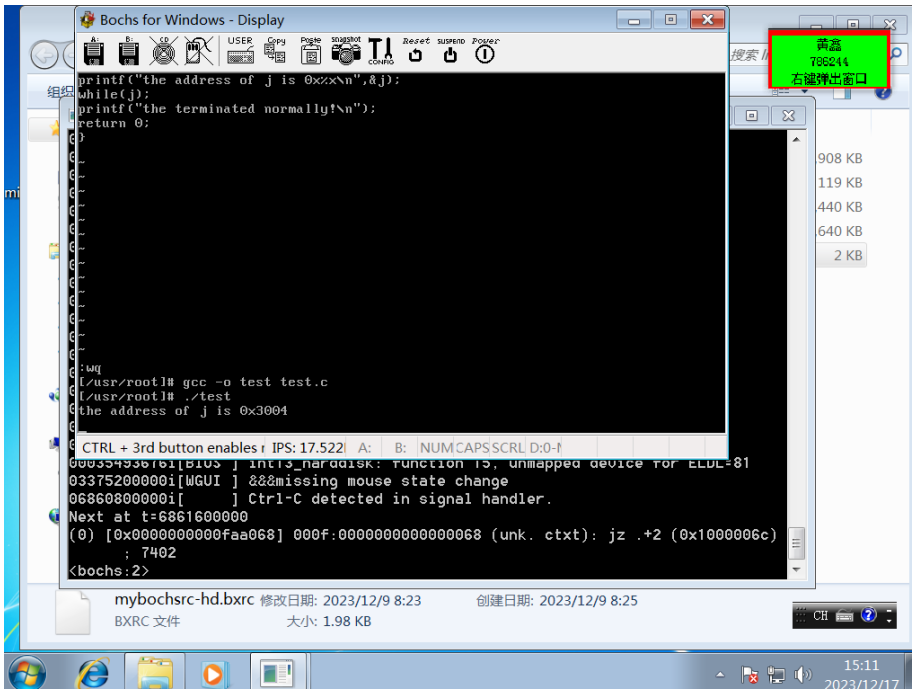


2. 输入实验指导书中的示例代码，按下 esc 键，并输入“:wq”保存文件。接着在该目录下使用 gcc 命令进行 C 语言程序的编译，输入“gcc -o test test.c”命令生成可执行文件 test。



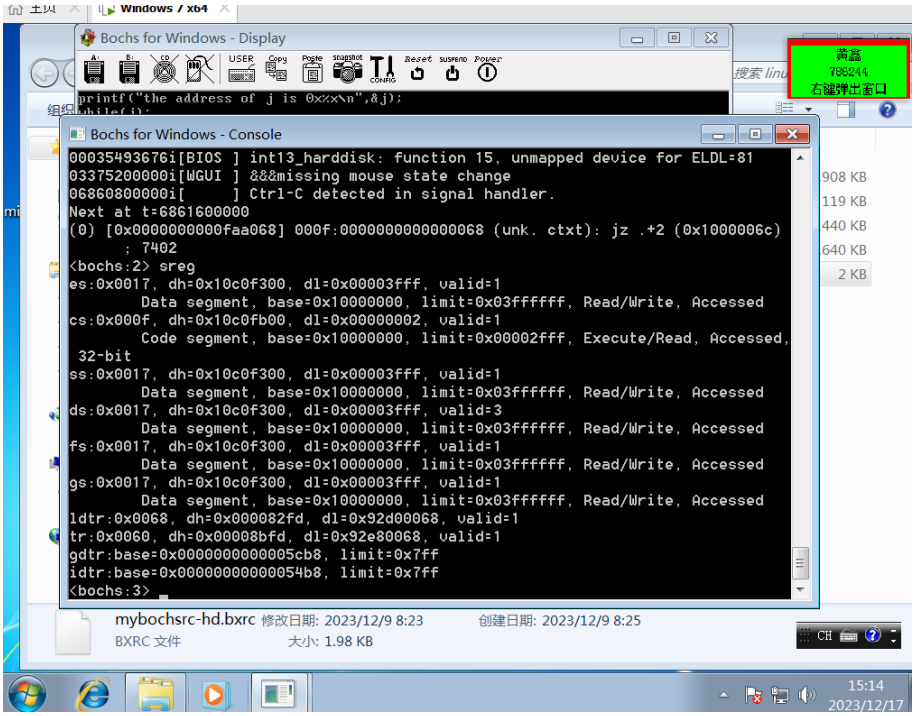


3. 输入 ls 命令查看当前目录下文件，并输入“./test”命令执行程序在控制台按 ctrl+c 暂停进行调试。

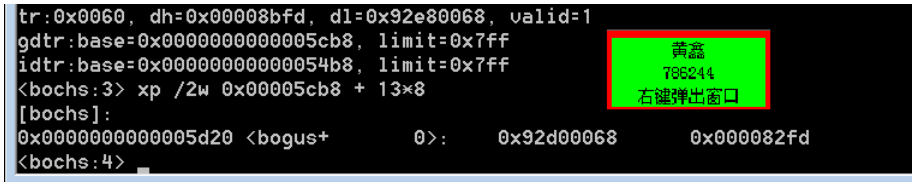


4. 逻辑地址由两部份组成，[段标识符：段内偏移量]。执行程序后可以看到变量 j 的逻辑地址为:0x3004，即 0011 0000 0000 0100，根据段标识符中 T1 位为 1 代表在 LDT 选择。

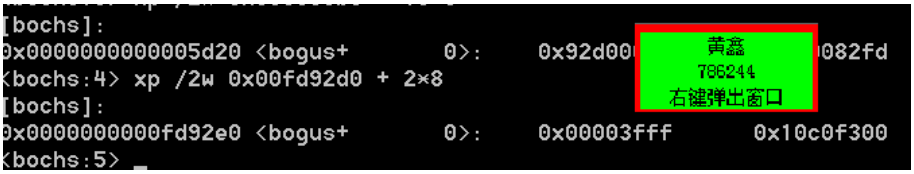
5. 通过 sreg 命令显示段寄存器的内容



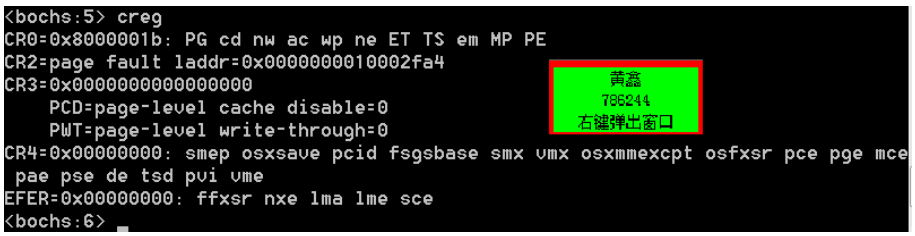
6.LDT 的描述符放在 GDT 中，这个表描述符也会有一个段选择子，ldtr 装载的就是这个选择子，GDT 的基址保存在 gdtr 中。ldtr 段选择子为 0x0068 => 0000 0000 0110 1000 b，可知索引为 1101b 即 13，TI 位为 0，即 GDT 中的第 13 项为 LDT 的段描述符，每个段描述符 64bit => 8byte：



7.得到的 LDT 段描述符（与 sreg 指令得到的 ldtr 中的 dl、dh 相同），从而我们可以得到 LDT 的基址为 0x00f9c2d0。数据段寄存器 ds 的段描述符可以通过 sreg 命令看到 ds 段选择子为 0x0017 => 0000 0000 0001 0111 b，可知索引为 10b 即 2，TI 位为 1，即 LDT 中的第 2 项为 ds 的段描述符，每个段描述符 64bit => 8byte。得到的 ds 段描述符，从而我们可以得到 ds 的基址为 0x10000000



8. 逻辑地址为 0x3004 的变量 j 对应的线性地 0x10000000+0x3004=0x10003004 由线性地址计数出物理地址线性地址 0x10003004 => 0001 0000 0000 0000 0011 0000 0000 0100 b，可知页目录号为 1000000b 即 64，页表为 11b 即 3，页内偏移为 100b 即 4 页目录表的基址存放于 CR3 中：



9、获取目录项（ CR3 起始地址为 0，此处计算时省略不写）

页目录项中高 20 位用来指向相应的页表，低 12 位是一些标志或保留位，

可得页表起始地址为 0x00fa6000。

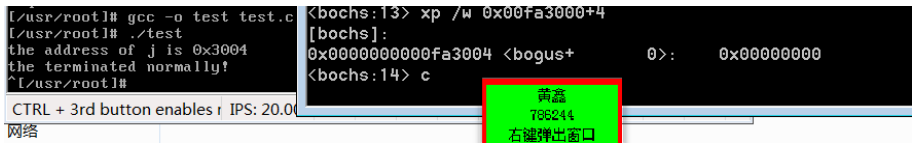
10、获取页表项

页表项中高 20 位用来指向相应的物理页，低 12 位是一些标志或保留位，可知物理页起始地址为：0x00fa3000

11、可以看到 test.c 中变量 j 的值

12、将 test.c 中 j 的值改为 0

13、成功跳出循环，程序结束



九、实验数据及结果分析：

在实验过程中，我成功运行了编写的示例程序，并通过输出的地址信息验证了对变量的地址计算。通过 Bochs 工具，我查看了寄存器的状态，确保了相关寄存器的值与预期一致。此外，通过 Bochs 的命令，我还查看了内存内容，进一步确认了物理地址的计算结果。

十、实验结论：

通过这次实验，我更深入地理解了段页式内存管理、寻址机制和地址转换的原理。我能够准确计算变量的线性地址，并使用页式内存管理机制计算物理地址。实验结论进一步巩固了我对计算机内存管理的知识。

十一、总结及心得体会：

这次实验让我感受到了实际操作的重要性。通过亲自编写程序、查看寄存器状态和使用调试工具，我不仅理论上了解了计算机内存管理的原理，还深入体验了这些概念在实际运行中的表现。在解决实验中遇到的问题的过程中，我的调试

和分析能力得到了提升。

十二、对本实验过程及方法、手段的改进建议：

在实验中，我认为更详细的实验指导和更直观的实验环境演示可能会对学生更有帮助。此外，提供更多关于 Bochs 工具的使用技巧和命令解释也可以提高学生在实验中的自信心。

总的来说，通过这次实验，我不仅学到了更多关于计算机内存管理的知识，而且加强了实际操作和问题解决的能力，这对我的学习和将来的实践都具有重要的意义。

报告评分：

指导教师签字：