作业1

**1.1 一个C程序可以编译成目标文件或可执行文件。目标文件和可执行文件通常包含text、data、bss、rodata段，程序执行时也会用到堆（heap）和栈（stack）。**

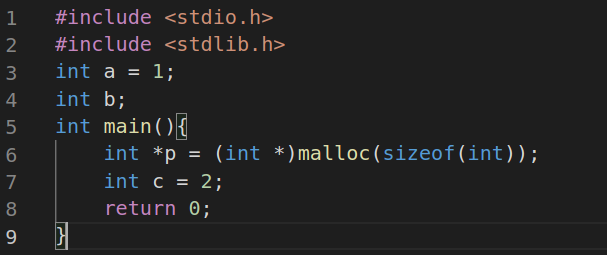
**（1）请写一个C程序，使其包含data段和bss段，并在运行时包含堆的使用。请说明所写程序中哪些变量在data段、bss段和堆上。**

**（2）请了解readelf、objdump命令的使用，用这些命令查看（1）中所写程序的data和bss段，截图展示。**

**（3）请说明（1）中所写程序是否用到了栈。**

**提交内容：所写C程序、问题解答、截图等。**

（1）所写C程序如下图所示。

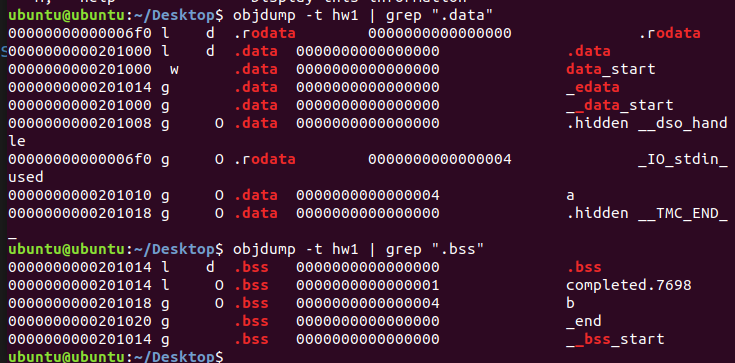


a为初始化的全局变量，位于.data段。

b为未初始化的全局变量，位于.bss段。

malloc分配的内存空间位于堆中，即指针p所指内容位于堆。

1. 使用objdump命令，截取.data段和.bss段如下图所示。



由图可知，初始化的全局变量a，位于.data段；未初始化的全局变量b，位于.bss段。

（3）用到了栈。main函数的调用、函数内的局部变量c均使用到了栈。c保存在main函数的函数栈中。

**1.2 Linux 下常见的3种系统调用方法包括有：**

**（1）通过glibc提供的库函数**

**（2）使用syscall函数直接调用相应的系统调用**

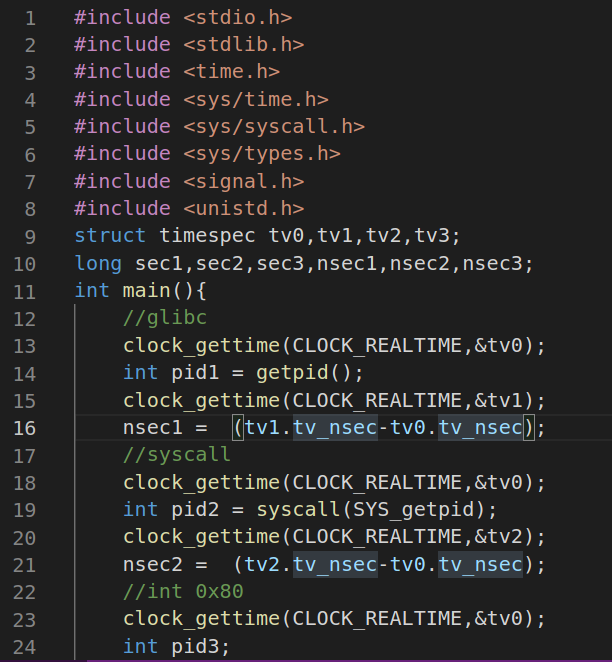
**（3）通过int 80指令（32位系统）或者syscall指令（64位系统）的内联汇编调用**

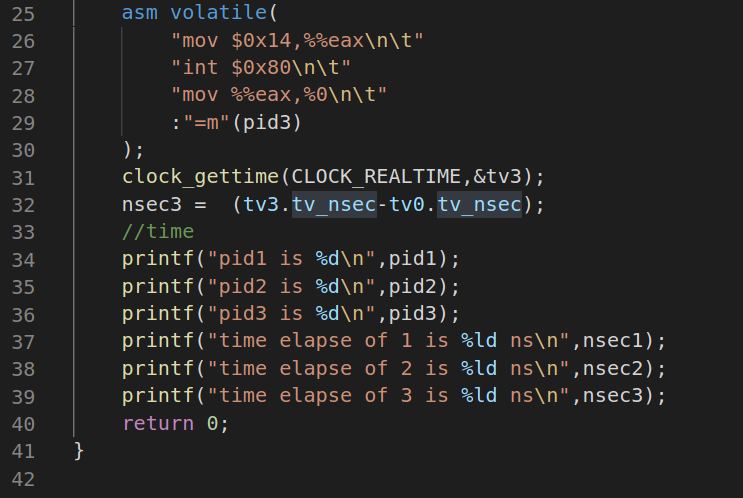
**请研究Linux(kernel>=2.6.24) getpid这一系统调用的用法，使用上述3种系统调用方法来执行，并记录和对比3种方法的运行时间，并尝试解释时间差异结果。**

**提示：gettimeofday和clock\_gettime是Linux下用来测量耗时的常用函数，请调研这两个函数，选择合适函数来测量一次系统调用的时间开销。**

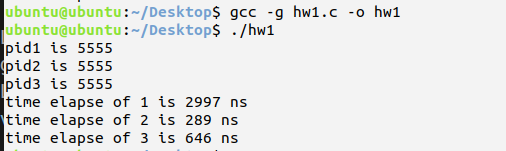
**提交内容：所写程序、执行结果、结果分析、系统环境（uname -a)等。**

代码如下：





运行比对结果如下：



结果分析：

glibc进行系统调用耗时最长，syscall耗时最短。glibc有函数封装调用，理应更耗时，与预期相符。

理论上内联式汇编应当最快，因为省去了函数封装，直接在汇编层面进行系统调用，与预期不是很相符。猜测是编译环境和编译器优化的问题。

系统环境：

985ee9a31ea79385ef4e4821d19e554