

**汇编语言程序设计大作业实验报告防护部分**

|  |  |
| --- | --- |
| 姓 名： | 马承乾 金为轩 李葳骏  李聪 李亚轩 连国鑫 |
| 学 号： | (按照姓名一栏顺序填写)  22920212204180 22920212204112  22920212204134 22920212204124  22920212204135 22920212204142 |
| 年 级： | 2021级 |
| 指导教师： | 林颖 |
| 课程名 ： | 汇编语言程序设计 |

2023年 6 月

1. **实验目的**

1、对学生汇编语言程序实验课编程能力整体考查

2、考查学生团队合作编程的效率和团队学习能力

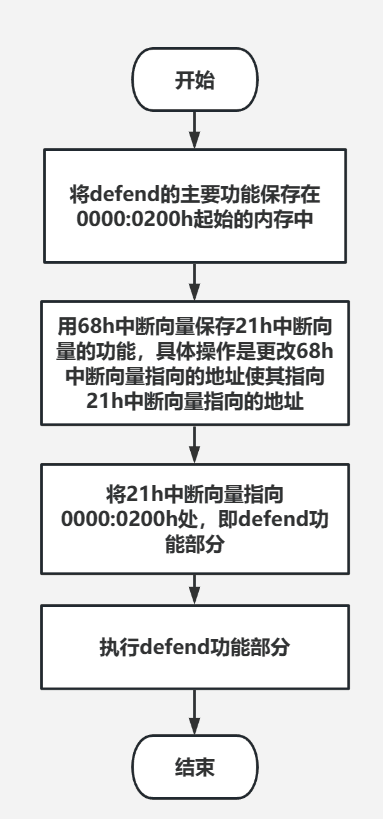
3、让学生完成具有一定的挑战性的任务

1. **实验内容**

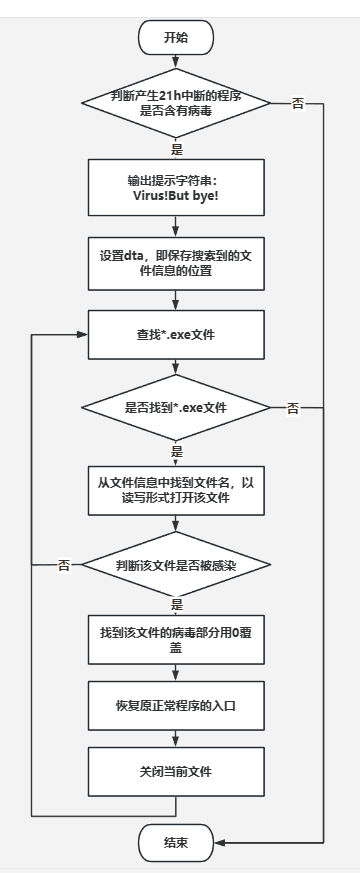
编写一个防病毒程序defend.exe，运行 defend.exe后再运行virus.exe或感染病毒的EXE文件，报警并自动杀毒。无毒文件正常运行。

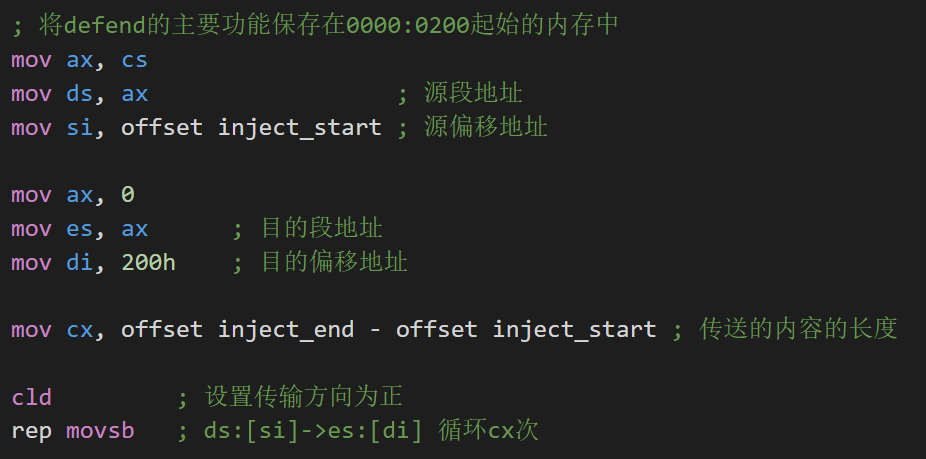
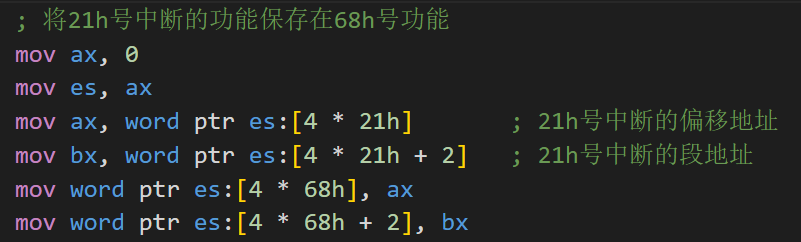
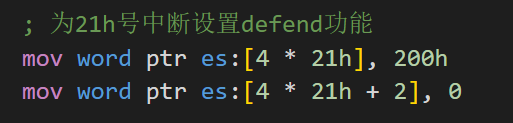
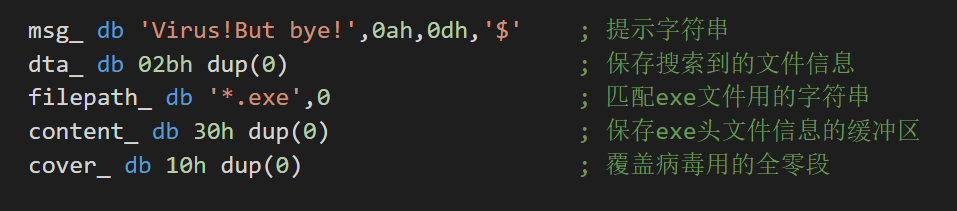
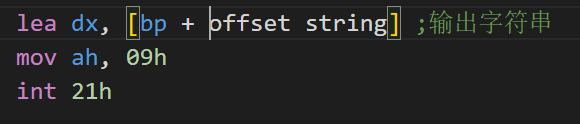
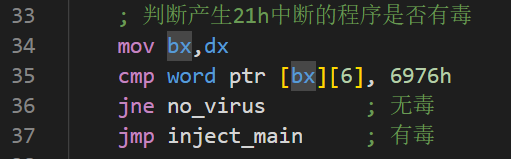
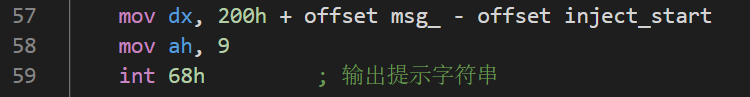
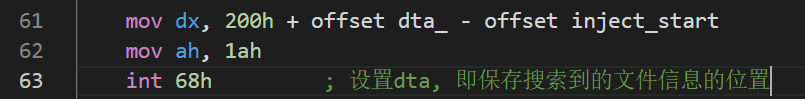
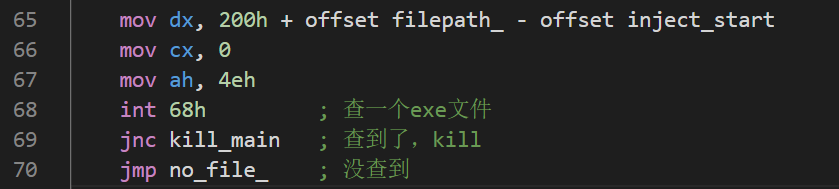
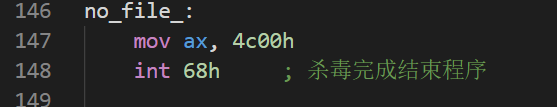
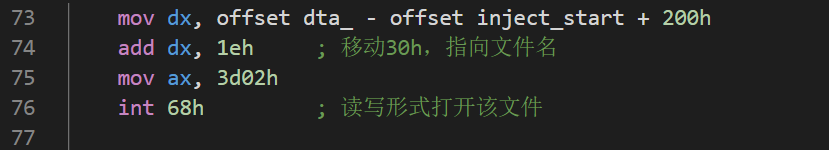
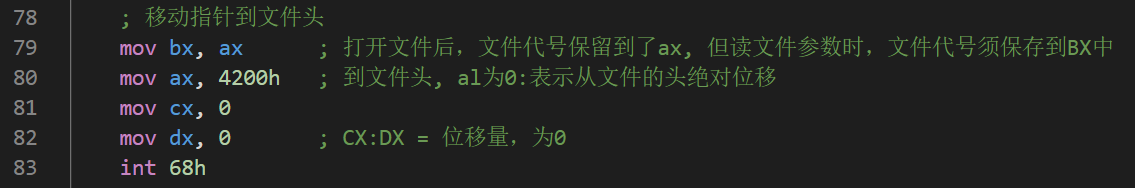
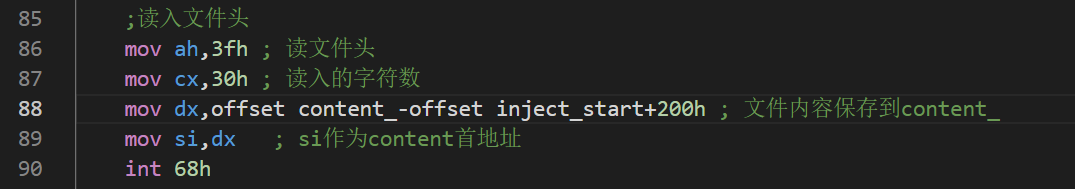
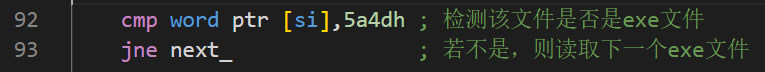
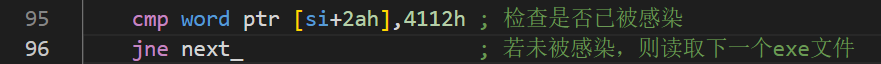
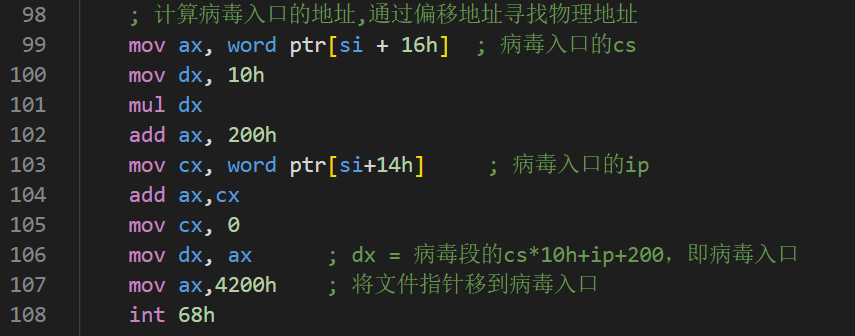
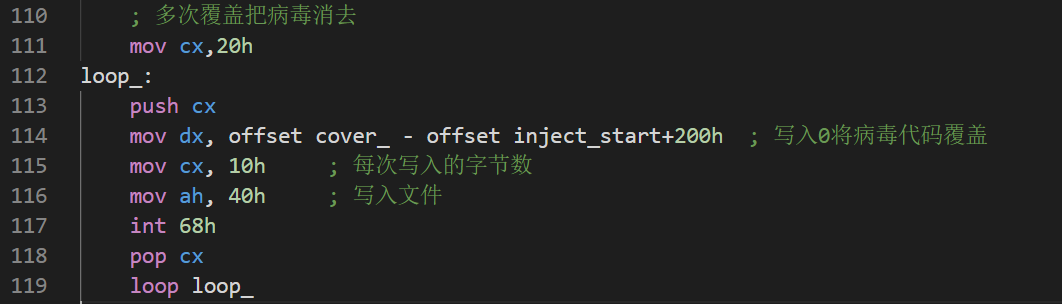
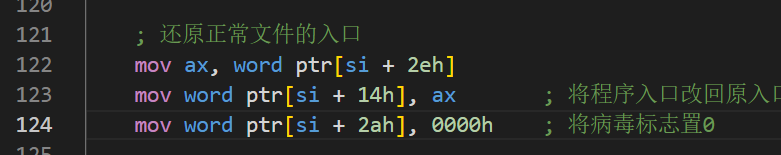
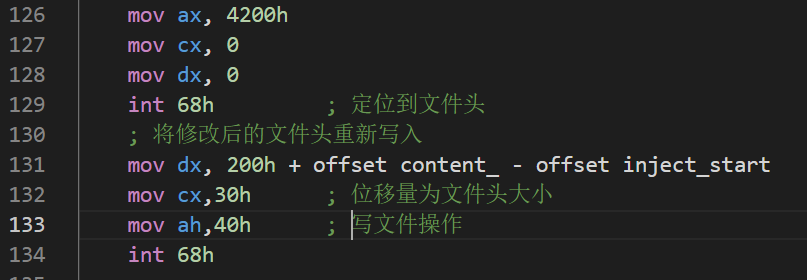
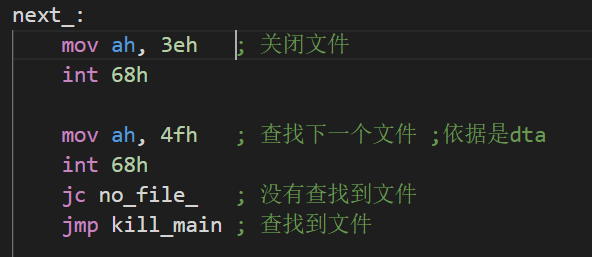
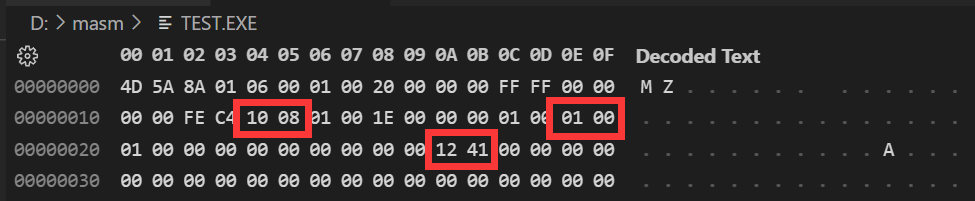
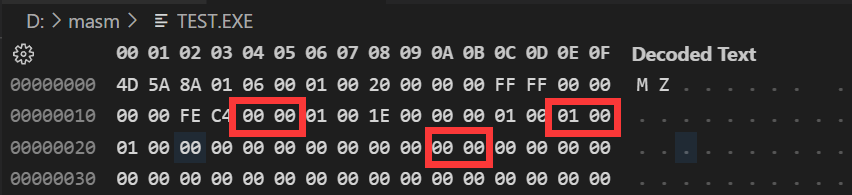
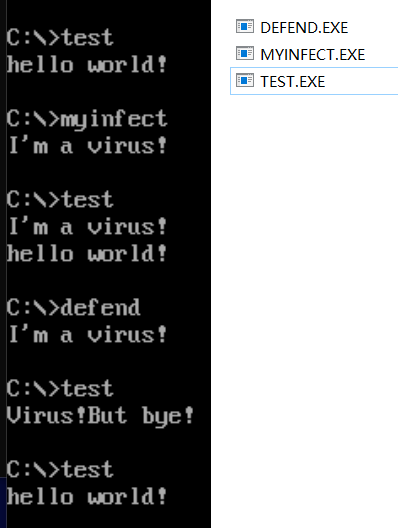
1. **实验步骤及结果**
2. 实验流程图：

以下为程序总体流程：



以下为defend具体功能部分流程图：



1. 实验思路：被病毒感染的程序，一定会使用INT 21h指令，所以可以通过更改21h号中断，使得它能对感染的程序进行杀毒，但又不影响正常程序的运行。
2. defend.asm的主要代码：
   1. 更改21h号中断：用保留的68h号中断，保存21h号中断的功能，然后将21h号中断的功能改成我们自己设定的defend功能。  
        
      中断向量表中保存了每个中断的地址，即低16为保存偏移地址，高16为保存段地址，所以可以通过更改68h号中断的地址，以此保存21h号功能。  
        
      同理可以为21h号功能指定新的defend的功能的位置，即0000:0200。  
      
   2. defend功能的实现部分  
      主要用到的存储数据的部分：  
        
      在含有病毒的文件中都有下面这一段代码，输出提示字符串I'm a virus!  
        
        
      所以可以通过判断某次执行INT 21h指令时，ds: dx对应的字符串是不是I'm a virus!，为了方便起见我们只检测第7个和第8个字符vi，v、i分别对应的ASCII是76h、69h，载入后低在低、高在高，所以是6976h。  
        
      若该程序无毒，执行no\_virus部分，正常执行原21h中断的功能，即调用指令INT 68h。  
        
      若程序有毒，执行inject\_main部分。  
      注意所有需要调用21h号中断的指令，都应该改成INT 68h。  
      输出提示字符串，表示程序有毒，用dos的09号功能：  
        
      设置dta，保存文件信息的位置：  
        
      搜索exe文件：  
        
      若没有搜索到文件，则说明没有感染病毒的文件，直接结束程序：  
        
      若搜索到文件，则执行kill\_main部分：  
      从文件信息dta中读取搜索到的文件的名字，并以读写的形式打开该文件，即ah=3dh(打开文件)，al=02h（读写方式）:  
        
        
        
        
        
      计算病毒入口的地址，并将文件指针移到病毒入口。  
        
      用零将病毒的代码部分覆盖掉，达到杀毒的效果  
        
      si中保存的是content的偏移地址，即保存文件头的位置，修改其中的程序入口信息。  
        
      移动文件指针到文件头，将修改后的文件头重新写入文件。  
        
      该文件杀毒完成，关闭当前文件，并搜索下一个文件。  
      
3. **实验结果与分析**Defend前被感染的test  
     
   Defend后被感染的test（显然已经消毒）  
     
   运行结果：  
   
4. **实验总结**

通过本次实验，我对内存驻留技术、文件操作技术、中断修改技术有了深刻认识，汇编语言编程能力有了长足进步，并且学会了通过查看二进制文件的方式判断功能是否实现，知道了如何方便地查看文件头以及文件头内容对应的意义；在这次大作业过程中，debug的过程让我对汇编语言的认识一点点加深，分工合作的过程也让我明白了良好的交流以及编程过程中注释的重要作用，编程能力和工程能力同时有了提升。