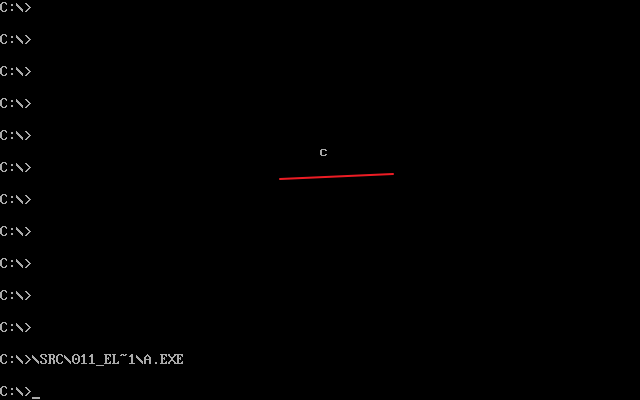
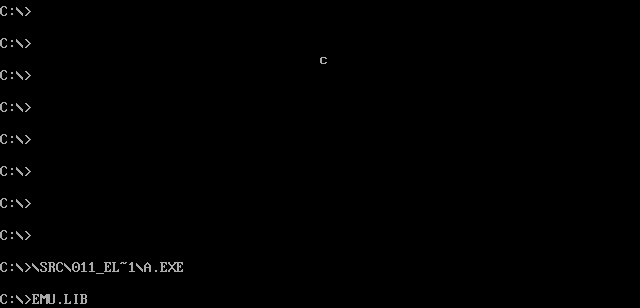
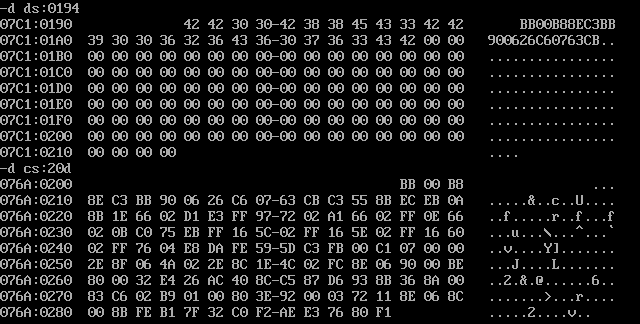
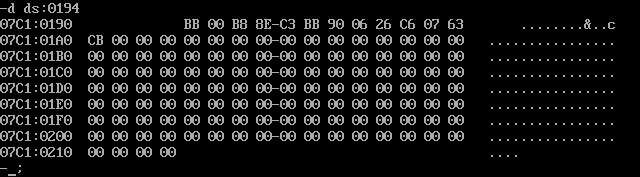
# C语言综合研究与高强度程序设计训练11

在定义数组a的语句中加入相关的内容使得下面的程序可以在屏幕中间打印一个字符 “c”

char a[200] = {'c'};  
main() { ((void(far \*)())(long)a)(); }

* 根据以前学过的操作显存中数据来显示字符可以写出以下程序
* main() { \*(char far \*)(0xb8000000 + 160 \* 10 + 80) = 'c'; }
  + 运行结果
  + 
* 根据书中所给代码可以看到a为函数指针，返回值为空，参数为空，所以可以写一个函数功能为在屏幕中打印c。
* void f();  
  main() {  
   f();  
  }  
  void f() { \*(char far \*)(0xb8000000 + 160 \* 10 + 80) = 'c'; }
  + 运行结果
  + 
* 然后修改程序查看汇编代码
* char a[200] = "0";  
  void far f();  
  main() {  
   f();  
   ((void(far \*)())(long)a)();  
  }  
  void far f() { \*(char far \*)(0xb8000000 + 160 \* 10 + 80) = 'c'; }
  + 汇编代码
  + 
  + 从中可以看到((void(far \*)())(long)a)();对应的汇编代码转换成了函数从1fff->20b据此可以推测如果将数组a中的值改为函数f()对应 的机器码的话就可以正确打印了。
* 修改程序
* char a[200] = "BB00B88EC3BB900626C60763CB";  
  void far f();  
  void(far \*b)();  
  main() {  
   f();  
   ((void(far \*)())(long)a)();  
  }  
  void far f() { \*(char far \*)(0xb8000000 + 160 \* 10 + 80) = 'c'; }
  + 然后再debug中卡到赋值失败，然后修改赋值方式
  + 
* 修改程序
* char a[200] = {0xBB, 0x00, 0xB8, 0x8E, 0xC3, 0xBB, 0x90,  
   0x06, 0x26, 0xC6, 0x07, 0x63, 0xCB};  
  void far f();  
  main() {  
   ((void(far \*)())(long)a)();  
  }  
  void far f() { \*(char far \*)(0xb8000000 + 160 \* 10 + 80) = 'c'; }
  + 运行结果
    - 可以看到数据复制成功
    - 
    - 接程运行一下可以看到打印出c
    - 