《操作系统原理实验》

实验报告

（实验一）

学 院 名 称：	数据科学与计算机学院
专业（班级）：	16 计科 2 班
学 生 姓 名：	朱志儒
学 号：	16337341
时 间：	2018 年 3 月 11 日

实 验 一 ： 接管裸机的控制权

一.实验目的

1、 搭建和应用实验环境

2、 接管裸机的控制权

二.实验要求

1、 搭建和应用实验环境

虚拟机安装，生成一个基本配置的虚拟机XXXPC和多个1.44MB容量的虚拟软盘，将其中一个虚拟软盘用DOS格式化为DOS引导盘，用WinHex工具将其中一个虚拟软盘的首扇区填满你的个人信息。

2、 接管裸机的控制权

设计IBM_PC的一个引导扇区程序，程序功能是：用字符‘A’从屏幕左边某行位置45度角下斜射出，保持一个可观察的适当速度直线运动，碰到屏幕的边后产生反射，改变方向运动，如此类推，不断运动；在此基础上，增加你的个性扩展，如同时控制两个运动的轨迹，或炫酷动态变色，个性画面，如此等等，自由不限。还要在屏幕某个区域特别的方式显示你的学号姓名等个人信息。将这个程序的机器码放进放进第三张虚拟软盘的首扇区，并用此软盘引导你的XXXPC，直到成功。

三. 实验方案

1、 虚拟机配置方法

使用Vmware Workstation配置虚拟机，虚拟机的配置：核心数为1的处理器、4MB的内存、10MB的磁盘、1.44MB的软盘。

2、 软件工具与作用

Notepad++：编写程序时使用的编辑器；

16位编辑器WinHex：可以以16进制的方式打开并编辑任意文件；

NAMS汇编工具：可以将汇编代码编译成对应的二进制代码；

WinImage：可以创建虚拟软盘。

3、 相关原理

（1）显示器：将那些内容以视觉可见的方式呈现在屏幕上；

（2）显示卡：

为显示器提供内容，并控制显示器的显示模式和状态：

图形方式：最小可控制单位为像素，VGA：640 X 400；

文本方式：最小可控制单位为字符，VGA：25 X 80；

显示卡内存：存放像素或文字及相关属性；

（3）字符方式现存地址空间：B8000~BFFFF共32KB

（4）访问显存使用逻辑地址：

采用“段地址：偏移地址”的形式；

显存段地址B800；

（5）屏幕上字符的显示属性：

R	G	B	背景色	前景色	
			K=0 时不闪烁，K=1 时闪烁	I=0	I=1
0	0	0	黑	黑	灰
0	0	1	蓝	蓝	浅蓝
0	1	0	绿	绿	浅绿
0	1	1	青	青	浅青
1	0	0	红	红	浅红
1	0	1	品（洋）红	品（洋）红	浅品（洋）红
1	1	0	棕	棕	黄
1	1	1	白	白	亮白

4、 算法

字符出现的位置为（X，Y），则内存地址的偏移量为（X x 80 + Y）X 2

5、 部分代码解释

```
mov ax,07C0H
mov ds,ax            ；在DS寄存器中载入数据段地址

mov cx, word[namelen]          ;显示名字
mov si, myname
mov di, 2
dis:
mov al, byte[ds:si]
inc si
mov ah, 07h
mov word [gs:di],ax
add di,2
loop dis
```

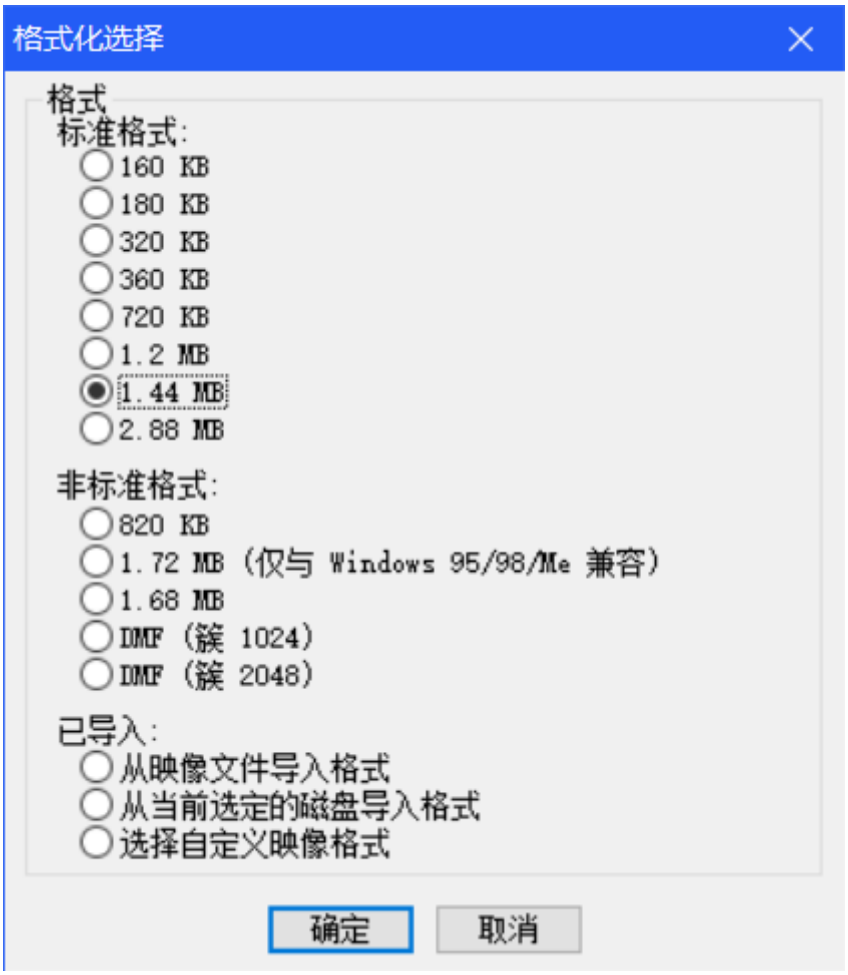
四. 实验过程和结果

1、 配置虚拟机

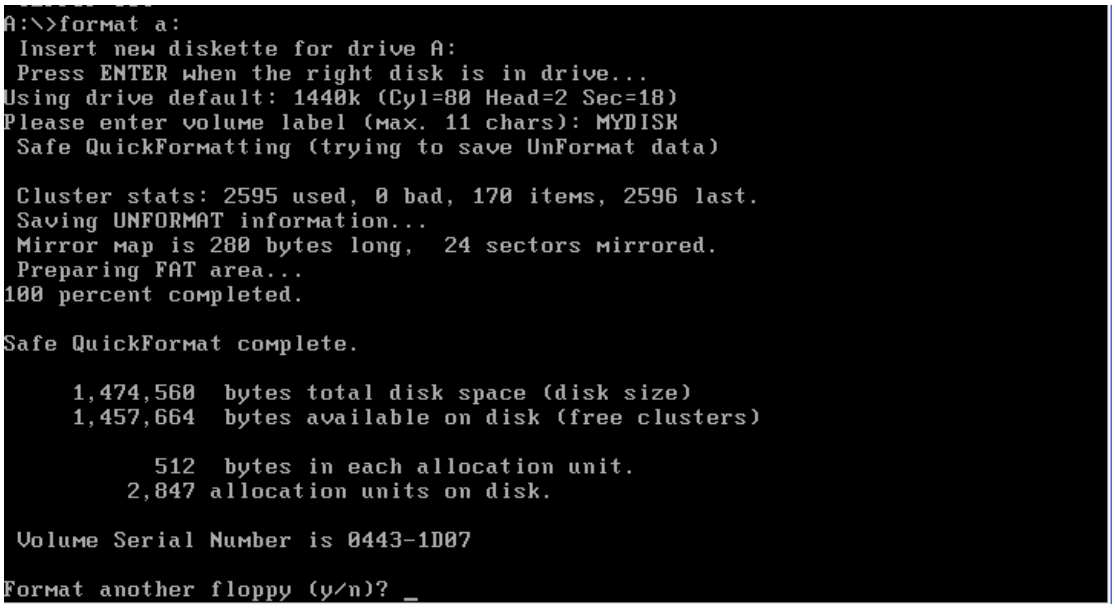
在VMware Workstation主界面中选择：文件→新建虚拟机→自定义→稍后安装操作系统→版本选择MS-DOS→处理器数目1、处理器核心数1→内存4M→磁盘10M，然后将得到一个符合要求的虚拟机，如图所示。

2、 创建虚拟软盘镜像文件并格式化软盘

在WinImage中选择：文件→新建→标准格式：1.44MB→保存，在保存时选择 .ima 保存类型，文件名改为stone.img，创建过程如图所示。



以同样的方式创建软盘镜像format_example.img，然后使用DOS格式化为DOS引导盘，如图所示。



3、 在首扇区填充个人信息

使用WinImage以上述方式创建一个名为personal_info.img的虚拟软盘镜像文件，在WinHex中选择：文件→打开→选择personal_info.img文件，在首扇区填充个人信息，如图所示。

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
00000010	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
00000020	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
00000030	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
00000040	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
00000050	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
00000060	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
00000070	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
00000080	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
00000090	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
000000A0	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
000000B0	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
000000C0	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
000000D0	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
000000E0	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
000000F0	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
00000100	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
00000110	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
00000120	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
00000130	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
00000140	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
00000150	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
00000160	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
00000170	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
00000180	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
00000190	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
000001A0	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
000001B0	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
000001C0	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
000001D0	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
000001E0	31	36	33	33	37	33	34	31	5A	68	75	5A	68	69	72	75	16337341ZhuZhiru
000001F0	31	36	33	33	37	33	34	31	5A	20	5A	20	52	20	55	AA	16337341Z Z R U?
00000200	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

4、 编写程序并将其载入软盘

在Notepad++中编写名为stone.asm的汇编代码，使用NASM将stone.asm编译成对应的stone.com文件，再在WinHex中分别打开stone.com和stone.img，手动将stone.com中的程序载入stone.img中，如图所示。

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	31	36	33	33	37	33	34	31	20	5A	68	75	5A	68	69	72	16337341 ZhuZhir
00000010	75	00	00	00	B8	C0	07	8E	D8	8C	C8	8E	C0	B8	00	B8	u...咐.庁屓幫??
00000020	8E	E8	C6	06	EB	01	41	C6	06	E1	01	0F	C7	06	DF	01	庤??A??.??
00000030	00	00	C7	06	DD	01	11	00	FF	0E	E2	01	75	FA	C7	06	..??.. .?u .
00000040	E2	01	50	C3	FF	0E	E4	01	75	EE	C7	06	E2	01	50	C3	?P?.?u钄.?P?
00000050	C7	06	E4	01	44	02	B0	01	3A	06	E6	01	74	1C	B0	02	??D.?:.?t.?
00000060	3A	06	E6	01	74	5B	B0	03	3A	06	E6	01	0F	84	98	00	:.?t[?:.?.赍.
00000070	B0	04	3A	06	E6	01	0F	84	D2	00	FF	06	E7	01	FF	06	?:.?.勫. .? .
00000080	E9	01	8B	1E	E7	01	B8	19	00	29	D8	74	0E	8B	1E	E9	????.)豺.??
00000090	01	B8	50	00	29	D8	74	16	E9	F5	00	C7	06	E7	01	17	.寤.)豺.轷.??.
000000A0	00	C6	06	E6	01	02	C6	06	E1	01	E0	E9	E2	00	C7	06	.??.??嚅??
000000B0	E9	01	4E	00	C6	06	E6	01	04	C6	06	E1	01	0F	E9	CF	?N.??.??.橄
000000C0	00	FF	0E	E7	01	FF	06	E9	01	8B	1E	E9	01	B8	50	00	. .? .???寤.
000000D0	29	D8	74	0E	8B	1E	E7	01	B8	FF	FF	29	D8	74	16	E9	)豺.???)豺.?
000000E0	AE	00	C7	06	E9	01	4E	00	C6	06	E6	01	03	C6	06	E1	???N.??.??
000000F0	01	E0	E9	9B	00	C7	06	E7	01	01	00	C6	06	E6	01	01	.嚅???..??.
00000100	C6	06	E1	01	0F	E9	88	00	FF	0E	E7	01	FF	0E	E9	01	??.闡. .? .?
00000110	8B	1E	E7	01	B8	FF	FF	29	D8	74	0D	8B	1E	E9	01	B8	???)豺.???
00000120	FF	FF	29	D8	74	14	EB	68	C7	06	E7	01	01	00	C6	06	)豺.雋??..?
00000130	E6	01	04	C6	06	E1	01	E0	EB	56	C7	06	E9	01	01	00	?.??曜V??..
00000140	C6	06	E6	01	02	C6	06	E1	01	0F	EB	44	FF	06	E7	01	??.??.陸 .?
00000150	FF	0E	E9	01	8B	1E	E9	01	B8	FF	FF	29	D8	74	0D	8B	.????)豺.?
00000160	1E	E7	01	B8	19	00	29	D8	74	14	EB	24	C7	06	E9	01	.??.)豺.???
00000170	01	00	C6	06	E6	01	01	C6	06	E1	01	E0	EB	12	C7	06	..??.??曜.?
00000180	E7	01	17	00	C6	06	E6	01	03	C6	06	E1	01	0F	EB	00	?..??.??.?
00000190	A1	DF	01	89	C5	B4	07	B0	20	65	89	46	00	31	C0	A1	∵.龑??e墩.1馈
000001A0	E7	01	BB	50	00	F7	E3	03	06	E9	01	BB	02	00	F7	E3	?藪.縻..??.縻
000001B0	89	C5	A3	DF	01	8A	26	E1	01	A0	EB	01	65	89	46	00	龑__.??狒.e墩.
000001C0	8B	0E	DD	01	BE	00	00	BF	02	00	3E	8A	04	46	B4	07	???.?.>?F?
000001D0	65	89	05	83	C7	02	E2	F2	E9	5D	FE	EB	FE	11	00	00	e?込.怛閉 ?..
000001E0	00	0F	50	C3	44	02	04	07	00	00	00	41	00	00	00	00	..P肇.....A....
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA	..............U?

5、 展示‘A’的45度飞行

在VMware Workstation的虚拟机DOS中选择：编辑虚拟设置→添加→选择软盘驱动器→使用软盘映像→选择stone.img文件→开启此虚拟机，然后将会看到第一行显示着我的个人信息，字符‘A’从屏幕左边45度角下斜射出，保持一个可观察的适当速度直线运动，碰到屏幕的边后，字符‘A’颜色发生变化并反射，改变方向运动，如此类推，不断运动。如图所示。

五.实验总结

这次实验充满挑战，我们需要在一个没有操作系统的虚拟机上跑一个程序，这我之前从没有做过的事。

通过在网上查阅资料，我明白如何使用WinImage创建新的软盘映像文件，如何使用DOS的format指令格式化软盘。

对于这次实验，我借鉴了老师给的代码，经过一些修改后，才使得字符‘A’从屏幕左边45度角下斜射出，保持一个可观察的适当速度直线运动，碰到屏幕的边后，字符‘A’反射，改变方向运动，如此类推，不断运动。

老师的代码会让字符‘A’的运动轨迹保留下来，而我将其稍作修改，使得字符‘A’在运动过程中不会保留轨迹，并在碰到屏幕边缘后会改变颜色。

显示个人信息的汇编代码编译后在虚拟机上运行时，我发现在第一行原本应该显示我的名字的地方，却显示了乱码。经过查阅资料后，我了解到主引导扇区数据为512字节，处理器会将这些数据加载到0x000:0x7c00逻辑地址中，接着检验最后两个字节是否为0x55和0xAA，如果存在，说明主引导扇区有效，跳到该位置

执行。所以在裸机上，程序的指令和数据会被载入到0x7c00的位置，所以只有在DS赋值为07C0h时，才能访问到正确的数据，不然就是乱码。

最具有挑战的是，编译后的代码不能超过512字节，这就需要使用更少的代码实现这些功能。

感言：这次实验只是实现一个小小的功能，而我却花费了差不多一周的时间，这说明我还有很多地方学习和提升，所以在以后的日子里，我将广泛阅读有关操作系统原理的书籍，打好基础，为以后的操作系统原理实验做准备。

建议：希望以后老师能够在课堂上讲详细一些，如果老师讲的不详细的话，我将需要花大量时间补习我的知识漏洞。

六. 参考文献

1、 Dos格式化命令FORMAT使用教程

https://wenku.baidu.com/view/9bae7b6048d7c1c708a145d4

2、 WinImage_制作_大IMG软盘镜像

https://wenku.baidu.com/view/95c15cefbb4cf7ec4bfed01b.html

3、 NASM汇编笔记

http://blog.csdn.net/zhuichao001/article/details/5618206

4、 NASM的ORG 0100h的实际含义

http://blog.csdn.net/ruyanhai/article/details/7177904