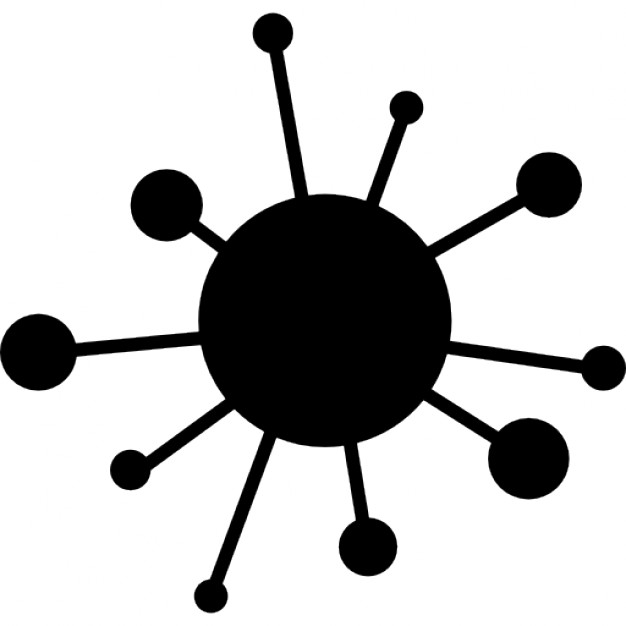
# 计算机病毒学

实验1硬盘引导记录分析



学号：0x091395

姓名：uknowho

实验目的

1、掌握主引导记录数据的数据与文本获取方式。

2、掌握工具软件debug32.exe的使用技巧。

3、掌握主引导记录数据分析方法。

4、掌握主引导记录代码分析方法。

实验原理

请参考教材第8章第1节的内容。

实验步骤

1、打开磁盘与文件分析软件diskhex.exe，选取待分析的物理驱动器。

2、选取物理驱动器的物理0号扇区，分别以数据和文本方式导出到指定文件夹中。

3、打开指定文件夹中以文本方式导出的主引导记录数据，分析主引导记录的基本结构。

4、打开工具软件debug32.exe，使用？命令，浏览常用debug指令的功能、格式。

5、利用debug32.exe打开指定文件夹中导出的主引导记录的数据文件。

6、将当前段偏移量0100h处长度为200h字节的主引导记录代码，移动到搬家前的执行空间0000:7C00。例如：m 0100 L200 0000:7C00。

7、利用反汇编命令U，获得搬家前执行的代码。例如：u 0:7C00。

8、根据需要，利用命令窗口的“编辑”下的“标记”功能，把需要保存的反编译结果复制后保存到指定文档中。

9、将当前段偏移量0100h处长度为200h字节的主引导记录代码，移动到搬家后的执行空间0000:0600。例如：m 0100 L200 0000:0600。

10、利用反汇编命令U，获得搬家后执行的代码。例如：u 0:061B。

11、根据需要，利用命令窗口的“编辑”下的“标记”功能，把需要保存的反编译结果复制后保存到指定文档中。

12、整理获得的数据及代码，参考附录的范例，整理成实验报告。

附录1 本机磁盘分析结果

**主引导记录读入内存后数据映像**

0ADD:7C00 33 C0 8E D0 BC 00 7C FB-50 07 50 1F FC BE 1B 7C 3.....|.P.P....|

0ADD:7C10 BF 1B 06 50 57 B9 E5 01-F3 A4 CB BD BE 07 B1 04 ...PW...........

0ADD:7C20 38 6E 00 7C 09 75 13 83-C5 10 E2 F4 CD 18 8B F5 8n.|.u..........

0ADD:7C30 83 C6 10 49 74 19 38 2C-74 F6 A0 B5 07 B4 07 8B ...It.8,t.......

0ADD:7C40 F0 AC 3C 00 74 FC BB 07-00 B4 0E CD 10 EB F2 88 ..<.t...........

0ADD:7C50 4E 10 E8 46 00 73 2A FE-46 10 80 7E 04 0B 74 0B N..F.s\*.F..~..t.

0ADD:7C60 80 7E 04 0C 74 05 A0 B6-07 75 D2 80 46 02 06 83 .~..t....u..F...

0ADD:7C70 46 08 06 83 56 0A 00 E8-21 00 73 05 A0 B6 07 EB F...V...!.s.....

0ADD:7C80 BC 81 3E FE 7D 55 AA 74-0B 80 7E 10 00 74 C8 A0 ..>.}U.t..~..t..

0ADD:7C90 B7 07 EB A9 8B FC 1E 57-8B F5 CB BF 05 00 8A 56 .......W.......V

0ADD:7CA0 00 B4 08 CD 13 72 23 8A-C1 24 3F 98 8A DE 8A FC .....r#..$?.....

0ADD:7CB0 43 F7 E3 8B D1 86 D6 B1-06 D2 EE 42 F7 E2 39 56 C..........B..9V

0ADD:7CC0 0A 77 23 72 05 39 46 08-73 1C B8 01 02 BB 00 7C .w#r.9F.s......|

0ADD:7CD0 8B 4E 02 8B 56 00 CD 13-73 51 4F 74 4E 32 E4 8A .N..V...sQOtN2..

0ADD:7CE0 56 00 CD 13 EB E4 8A 56-00 60 BB AA 55 B4 41 CD V......V.`..U.A.

0ADD:7CF0 13 72 36 81 FB 55 AA 75-30 F6 C1 01 74 2B 61 60 .r6..U.u0...t+a`

0ADD:7D00 6A 00 6A 00 FF 76 0A FF-76 08 6A 00 68 00 7C 6A j.j..v..v.j.h.|j

0ADD:7D10 01 6A 10 B4 42 8B F4 CD-13 61 61 73 0E 4F 74 0B .j..B....aas.Ot.

0ADD:7D20 32 E4 8A 56 00 CD 13 EB-D6 61 F9 C3 49 6E 76 61 2..V.....a..Inva

0ADD:7D30 6C 69 64 20 70 61 72 74-69 74 69 6F 6E 20 74 61 lid partitionta

0ADD:7D40 62 6C 65 00 45 72 72 6F-72 20 6C 6F 61 64 69 6E ble.Error loadin

0ADD:7D50 67 20 6F 70 65 72 61 74-69 6E 67 20 73 79 73 74 g operating syst

0ADD:7D60 65 6D 00 4D 69 73 73 69-6E 67 20 6F 70 65 72 61 em.Missing opera

0ADD:7D70 74 69 6E 67 20 73 79 73-74 65 6D 00 00 00 00 00 ting system.....

0ADD:7D80 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................

0ADD:7D90 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................

0ADD:7DA0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................

0ADD:7DB0 00 00 00 00 00 2C 44 63-0F AD 0F AD 00 00 80 01 .....,Dc........

0ADD:7DC0 01 00 07 FE FF FF 3F 00-00 00 4C B1 BF 03 00 00 ......?...L.....

0ADD:7DD0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................

0ADD:7DE0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................

0ADD:7DF0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 55 AA ..............U.

**移位后主引导记录在内存中的映像**

0ADD:0600 33 C0 8E D0 BC 00 7C FB-50 07 50 1F FC BE 1B 7C 3.....|.P.P....|

0ADD:0610 BF 1B 06 50 57 B9 E5 01-F3 A4 CB BD BE 07 B1 04 ...PW...........

0ADD:0620 38 6E 00 7C 09 75 13 83-C5 10 E2 F4 CD 18 8B F5 8n.|.u..........

0ADD:0630 83 C6 10 49 74 19 38 2C-74 F6 A0 B5 07 B4 07 8B ...It.8,t.......

0ADD:0640 F0 AC 3C 00 74 FC BB 07-00 B4 0E CD 10 EB F2 88 ..<.t...........

0ADD:0650 4E 10 E8 46 00 73 2A FE-46 10 80 7E 04 0B 74 0B N..F.s\*.F..~..t.

0ADD:0660 80 7E 04 0C 74 05 A0 B6-07 75 D2 80 46 02 06 83 .~..t....u..F...

0ADD:0670 46 08 06 83 56 0A 00 E8-21 00 73 05 A0 B6 07 EB F...V...!.s.....

0ADD:0680 BC 81 3E FE 7D 55 AA 74-0B 80 7E 10 00 74 C8 A0 ..>.}U.t..~..t..

0ADD:0690 B7 07 EB A9 8B FC 1E 57-8B F5 CB BF 05 00 8A 56 .......W.......V

0ADD:06A0 00 B4 08 CD 13 72 23 8A-C1 24 3F 98 8A DE 8A FC .....r#..$?.....

0ADD:06B0 43 F7 E3 8B D1 86 D6 B1-06 D2 EE 42 F7 E2 39 56 C..........B..9V

0ADD:06C0 0A 77 23 72 05 39 46 08-73 1C B8 01 02 BB 00 7C .w#r.9F.s......|

0ADD:06D0 8B 4E 02 8B 56 00 CD 13-73 51 4F 74 4E 32 E4 8A .N..V...sQOtN2..

0ADD:06E0 56 00 CD 13 EB E4 8A 56-00 60 BB AA 55 B4 41 CD V......V.`..U.A.

0ADD:06F0 13 72 36 81 FB 55 AA 75-30 F6 C1 01 74 2B 61 60 .r6..U.u0...t+a`

0ADD:0700 6A 00 6A 00 FF 76 0A FF-76 08 6A 00 68 00 7C 6A j.j..v..v.j.h.|j

0ADD:0710 01 6A 10 B4 42 8B F4 CD-13 61 61 73 0E 4F 74 0B .j..B....aas.Ot.

0ADD:0720 32 E4 8A 56 00 CD 13 EB-D6 61 F9 C3 49 6E 76 61 2..V.....a..Inva

0ADD:0730 6C 69 64 20 70 61 72 74-69 74 69 6F 6E 20 74 61 lid partitionta

0ADD:0740 62 6C 65 00 45 72 72 6F-72 20 6C 6F 61 64 69 6E ble.Error loadin

0ADD:0750 67 20 6F 70 65 72 61 74-69 6E 67 20 73 79 73 74 g operating syst

0ADD:0760 65 6D 00 4D 69 73 73 69-6E 67 20 6F 70 65 72 61 em.Missing opera

0ADD:0770 74 69 6E 67 20 73 79 73-74 65 6D 00 00 00 00 00 ting system.....

0ADD:0780 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................

0ADD:0790 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................

0ADD:07A0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................

0ADD:07B0 00 00 00 00 00 2C 44 63-0F AD 0F AD 00 00 80 01 .....,Dc........

0ADD:07C0 01 00 07 FE FF FF 3F 00-00 00 4C B1 BF 03 00 00 ......?...L.....

0ADD:07D0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................

0ADD:07E0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................

0ADD:07F0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 55 AA ..............U.

**主引导记录数据按照功能分段**

1. 代码段

0ADD:0600 33 C0 8E D0 BC 00 7C FB-50 07 50 1F FC BE 1B 7C 3.....|.P.P....|

0ADD:0610 BF 1B 06 50 57 B9 E5 01-F3 A4 CB BD BE 07 B1 04 ...PW...........

0ADD:0620 38 6E 00 7C 09 75 13 83-C5 10 E2 F4 CD 18 8B F5 8n.|.u..........

0ADD:0630 83 C6 10 49 74 19 38 2C-74 F6 A0 B5 07 B4 07 8B ...It.8,t.......

0ADD:0640 F0 AC 3C 00 74 FC BB 07-00 B4 0E CD 10 EB F2 88 ..<.t...........

0ADD:0650 4E 10 E8 46 00 73 2A FE-46 10 80 7E 04 0B 74 0B N..F.s\*.F..~..t.

0ADD:0660 80 7E 04 0C 74 05 A0 B6-07 75 D2 80 46 02 06 83 .~..t....u..F...

0ADD:0670 46 08 06 83 56 0A 00 E8-21 00 73 05 A0 B6 07 EB F...V...!.s.....

0ADD:0680 BC 81 3E FE 7D 55 AA 74-0B 80 7E 10 00 74 C8 A0 ..>.}U.t..~..t..

0ADD:0690 B7 07 EB A9 8B FC 1E 57-8B F5 CB BF 05 00 8A 56 .......W.......V

0ADD:06A0 00 B4 08 CD 13 72 23 8A-C1 24 3F 98 8A DE 8A FC .....r#..$?.....

0ADD:06B0 43 F7 E3 8B D1 86 D6 B1-06 D2 EE 42 F7 E2 39 56 C..........B..9V

0ADD:06C0 0A 77 23 72 05 39 46 08-73 1C B8 01 02 BB 00 7C .w#r.9F.s......|

0ADD:06D0 8B 4E 02 8B 56 00 CD 13-73 51 4F 74 4E 32 E4 8A .N..V...sQOtN2..

0ADD:06E0 56 00 CD 13 EB E4 8A 56-00 60 BB AA 55 B4 41 CD V......V.`..U.A.

0ADD:06F0 13 72 36 81 FB 55 AA 75-30 F6 C1 01 74 2B 61 60 .r6..U.u0...t+a`

0ADD:0700 6A 00 6A 00 FF 76 0A FF-76 08 6A 00 68 00 7C 6A j.j..v..v.j.h.|j

0ADD:0710 01 6A 10 B4 42 8B F4 CD-13 61 61 73 0E 4F 74 0B .j..B....aas.Ot.

0ADD:0720 32 E4 8A 56 00 CD 13 EB-D6 61 F9 C3

===搬家代码(L=1BH)

1. 出错提示信息数据段

0ADD:0720 49 6E 76 61 2..V.....a..Inva

0ADD:0730 6C 69 64 20 70 61 72 74-69 74 69 6F 6E 20 74 61 lid partitionta

0ADD:0740 62 6C 65 00 45 72 72 6F-72 20 6C 6F 61 64 69 6E ble.Error loadin

0ADD:0750 67 20 6F 70 65 72 61 74-69 6E 67 20 73 79 73 74 g operating syst

0ADD:0760 65 6D 00 4D 69 73 73 69-6E 67 20 6F 70 65 72 61 em.Missing opera

0ADD:0770 74 69 6E 67 20 73 79 73-74 65 6D 00 00 00 00 00 ting system.....

0ADD:0780 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................

0ADD:0790 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................

0ADD:07A0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................

0ADD:07B0 00 00 00 00 00

1. 出错提示信息起始位置低字节

0ADD:07B5 2C 44 63

1. 保留数据

0ADD:07B8 -0F AD 0F AD 00 00

1. 分区表数据

0ADD:07BE 80 01 .....,Dc........

0ADD:07C0 01 00 07 FE FF FF 3F 00-00 00 4C B1 BF 03 00 00 ......?...L.....

0ADD:07D0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................

0ADD:07E0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................

0ADD:07F0 00 00 00 00 00 00 00 00-00 00 00 00 00 00

1. 系统块标志值

0ADD:07FE 55 AA ..............U.

**主引导记录使用的内存空间分布**

表1-1 主引导记录使用的内存空间

|  |  |  |  |
| --- | --- | --- | --- |
| 项目 | 起始地址 | 长度 | 用途 |
| 栈空间 | 0000:7BFF | 动态变化 | 栈空间（栈底指针为0000:7C00H） |
| 临时主引导区 | 0000:7C00 | 0200H(512) | 暂时存放主引导记录数据 |
| 主引导区 | 0000:061B | 01E5H(485)  061B+1E5=800  072B-61B=111 | 存放主引导记录数据 |
| 出错提示信息串 | 0000:072C | 0050H  0089H | 出错提示信息数据 |
| 出错提示信息首地址 | 0000:07B5 | 0003H | 出错提示信息起始位置的低字节 |
| 保留数据 | 0000:07B8 | 0006H | ???????what the heck. |
| 分区表数据 | 0000:07BE | 0040H(64) | 分区表 |
| 块结束标志 | 0000:07FE | 0020H | 结束标志 |

**主引导记录工作流程**

1. 设置数据空间

**0ADD:7C00 33C0 XOR AX,AX ;**AX清零

**0ADD:7C02 8ED0 MOV SS,AX**

**0ADD:7C04 BC007C MOV SP,7C00 ;**设置栈底地址0000:7C00

**0ADD:7C07 FB STI ;**开启响应软中断的功能

**0ADD:7C08 50 PUSH AX ;**不明白

**0ADD:7C09 07 POP ES ;**不明白

**0ADD:7C0A 50 PUSH AX ;**不明白

**0ADD:7C0B 1F POP DS ;**不明白

1. 搬家到0：061B，让激活分区引导记录使用0:7C00

; 清方向标志位，使SI，DI在对其操作后自动增1。

**0ADD:7C0C FC CLD**

**0ADD:7C0D BE1B7C MOV SI,7C1B ;**原地址起始位置

**0ADD:7C10 BF1B06 MOV DI,061B ;**目的地址起始位置

**0ADD:7C13 50 PUSH AX**

**0ADD:7C14 57 PUSH DI**

**0ADD:7C15 B9E501 MOV CX,01E5 ;**复制长度

**0ADD:7C18 F3 REPZ ;**不明白

**0ADD:7C19 A4 MOVSB ;**从DS:SI复制到ES:DI，长度01E5

**0ADD:7C1A CB RETF ;**跳转到0:061b继续执行

1. 检查分区表，查找激活分区表项

0ADD:061B BDBE07 MOV BP,07BE ;BP指向第一个分区表

0ADD:061E B104 MOV CL,04 ;检查四个分区表项

0ADD:0620 386E00 CMP [BP+00],CH ;分区类型

0ADD:0623 7C09 JL 062E ;80H符号位为1，为激活分区

0ADD:0625 7513 JNZ 063A ;为非激活分区，跳转到063A

0ADD:0627 83C510 ADD BP,+10 ;未找到激活分区(80H)BP指向下一个分区标识

0ADD:062A E2F4 LOOP 0620 ;继续寻找激活分区

0ADD:062C CD18 INT 18 ;未找到激活分区(均为00H)调用ROM BASIC

; 找到第一个激活分区时跳转到这里。找到激活分区后继续检查剩余分区项，在没有出错的情况下跳转去读引导记录，若出现有多个激活分区，或者有激活标志既非80H又非00H的错误，则去显示输出错误提示信息。

0ADD:062E 8BF5 MOV SI,BP ;SI保存了当前分区项的首地址

0ADD:0630 83C610 ADD SI,+10 ;指向下一个分区项

0ADD:0633 49 DEC CX ;待检查分区项-1

; 4个分区项是否检查完毕，是则跳转至064FH，读取引导记录。

0ADD:0634 7419 JZ 064F

0ADD:0636 382C CMP [SI],CH ;继续检查，判断是否是非激活分区(CH=00H)

;不明白非激活分区则去检查下一个分区项不正常分区或又一个激活分区则出错提示，激活标志既不是80H也不是00H，或有超过1个的激活分区时，跳转至这里，显示输出分区表出错提示信息，然后死机，进入死循环。

0ADD:0638 74F6 JZ 0630

;获得出错提示信息入口地址，先取低字给AL，再取高字，在显示出模块中给AH，显示”Invalid partition table”

0ADD:063A A0B507 MOV AL,[07B5] ;[07B5]=2C

1. 显示出错提示信息

根据执行到这里的AL参数显示对应出错提示字符信息，AL的值可以为02CH、044H或者063H。对应的提示信息分别是，“Invalid partition table”、“Error loading operating system”和“Missing operating system”。

0ADD:063D B407 MOV AH,07 AH=07,AX=072C,0744，0763

0ADD:063F 8BF0 MOV SI,AX

0ADD:0641 AC LODSB ;读取错误信息

0ADD:0642 3C00 CMP AL,00 ;判断字符串结尾00

0ADD:0644 74FC JZ 0642 ;错误信息显示完，跳转，死循环

;调用INT 10H 0E号功能显示字符，显示字符后光标前移。

入口参数:

AL=字符

BH=页号

BL=前景色

出口参数:

无

; 设置显示方式为0007H且光标前移，显示AL中的数据即出错提示信息字符串。

0ADD:0646 BB0700 MOV BX,0007z` ;提示信息未打印完则继续显示

0ADD:0649 B40E MOV AH,0E

0ADD:064B CD10 INT 10

0ADD:064D EBF2 JMP 0641 ;读下一个个字符

1. 读引导记录

0ADD:064F 884E10 MOV [BP+10],CL ;指向引导记录位置

; 调用069B模块子程序读取引导记录数据。

0ADD:0652 E84600 CALL 069B

0ADD:0655 732A JNB 0681 ;读取成功，跳转到0681

; 读盘失败则顺序执行下面的操作。首先置分区备份引导记录的读取状态为”已读过”，这里只是改了状态标志值，实质上还未读过。

0ADD:0657 FE4610 INC BYTE PTR [BP+10]

; 根据当前分区类型是否是FAT32来判断是否要读备份引导记录。当前分区的类型若是FAT32则去读备份引导记录，否则跳转去显示出错提示信息。程序根据分区类型标志值来判断当前分区的分区类型，其中0BH或者0CH代表FAT32，06H或者OEH代表FAT16。

0ADD:065A 807E040B CMP BYTE PTR [BP+04],0B

0ADD:065E 740B JZ 066B ;等于0B 跳转066B

0ADD:0660 807E040C CMP BYTE PTR [BP+04],0C

0ADD:0664 7405 JZ 066B ;等于0C 跳转066B

0ADD:0666 A0B607 MOV AL,[07B6] ;分区类型不是FAT32时出错提示

; 跳转显示 “Error loading operating system”。

0ADD:0669 75D2 JNZ 063D

; 分区类型是FAT32时的进一步处理，尝试读一次备份引导记录数据。备份引导记录存放在引导记录后面相隔06H个扇区的位置，因此备份引导记录的起始扇区，数要在引导记录的起始扇区数基础上加06H。同理，备份引导记录的前总扇区数比引导记录的前总扇区数要多06H个扇区，因此备份引导记录的前总扇区数要在引导记录前总扇区数基础上加06H。

0ADD:066B 80460206 ADD BYTE PTR [BP+02],06

0ADD:066F 83460806 ADD WORD PTR [BP+08],+06

0ADD:0673 83560A00 ADC WORD PTR [BP+0A],+00 ;放进位

; 调用069B模块子程序读取备份引导记录数据。

0ADD:0677 E82100 CALL 069B

; 读备份引导记录成功则跳转至0681

0ADD:067A 7305 JNB 0681

; 读备份引导记录失败则直接给出出错提示信息入口地址的低字节。

0ADD:067C A0B607 MOV AL,[07B6]

; 跳转显示 “Error loading operating system”。

; 读成功后跳转到这里来执行。主引导向引导转交控制权前的处理过程:判断系统块标志值是否为0AA55H，系统块标志值是0AA55H，则系统就承认读取到的引导记录，然后就转交控制权给引导。系统块标志值不是0AA55H，则系统就否认读取到的引导记录的有效性，系统就要根据备份引导记录的读取状态来进一步决定是去读备份引导记录还是出错处理。

0000:0681 813EFE7D55AA CMP Word Ptr [7DFE]，0AA55h;比较系统块标志和0AA55H

; 系统块标志值是0AA55H则跳转至0694H， 准备转交控制权。不是0AA55H则进一步判断是再次读盘还是出错处理。

0ADD:067F EBBC JMP 063D

0ADD:0681 813EFE7D55AA CMP WORD PTR [7DFE],AA55

0ADD:0687 740B JZ 0694

0ADD:0689 807E1000 CMP BYTE PTR [BP+10],00 ;判断备份引导是否读过

; 没有读过则跳转至0657H去读备份引导记录数据。

0ADD:068D 74C8 JZ 0657 ;已经读过了则出错提示

0ADD:068F A0B707 MOV AL,[07B7]

; 无条件跳转去显示出错提示信息 ”Missing operating system”。

0ADD:0692 EBA9 JMP 063D

1. 转让控制权给激活分区的引导记录

0ADD:0694 8BFC MOV DI,SP ;栈顶指针SP指向7C00

0ADD:0696 1E PUSH DS ;两次进栈操作为RETF指令准备新的CS:IP

0ADD:0697 57 PUSH DI

0ADD:0698 8BF5 MOV SI,BP ;BP中记录了激活分区项的首地址

0ADD:069A CB RETF- ;控制权转到 0000:7C00H