计算机实用软件技术系列丛书

IBMPC实用技术高级专题

计算机病毒的预防与消除

朱华编著

学苑出版社

计算机实用软件技术系列丛书

IBM PC 实用技术高级专题

计算机病毒的预防与消除

朱　毕　　编著

熊可宜　　审校

学苑出版社

1994

(京)新登字 151 号

内 容 简 介

本手册共分十五章介绍了计算机病毒的预防和消除。第一章简述了 DOS 技术基础，第二章至第十三章介绍了小球病毒、扬基病毒、1701 病毒、Jerusalen 病毒、1575 病毒、X.X 病毒、Stoned 病毒、I/O 端口病毒、Brain 病毒、Vienna 病毒、音乐病毒、Amiga 病毒。

本书中的程序编译后生成的程序 KILL1 能消除目前国内所有的 BOOT 型病毒。了解了计算机病毒的预防和消除，使每一个计算机用户都能有效地使用和维护计算机。

欲购本书的用户，请直接与北京 8721 信箱联系，邮编：100080，电话：2562329。

计算机实用软件技术系列丛书

计算机病毒的预防与消除

编　　著： 朱　毕
审　　校： 熊可宜
责任编辑： 甄国宪
出版发行： 学苑出版社　　**邮政编码：**100036
社　　址： 北京市海淀区万寿路西街 11 号
印　　刷： 施园印刷厂
开　　本： 787×1092　1/16
印　　张： 31　　**字数：** 722 千字
印　　数： 1～5000
版　　次： 1994 年 1 月北京第 1 版第 1 次
ISBN $_{7}$-5077-0876-4/TP・25
本册定价：25.00 元

目　录

第一章 DOS 技术基础

攻击 PC 机的病毒程序通常都巧妙地利用了磁盘操作系统(DOS)的各种强大功能,以实现其传染、隐藏、破坏等目的,有的病毒程序水平非常高,因此分析和解消计算机病毒时要求我们对 DOS 系统有足够的了解,本章就六个大的方面对 DOS 系统作了较详细的介绍,这些方面包括了病毒经常使用的各种技术,对于我们搞清楚计算机病毒的原理和机制、消除和免疫是很有帮助的,有兴趣的读者不妨仔细阅读一遍本章的内容,相信你们会有不小的收获。对那些已经比较了解 DOS 系统的读者来说,本章有些内容就显得过于浅显了,因此可以挑选某些节次,比如第二节 DOS 是如何启动的等等加以阅读。

本章包括以下六节内容:

1) DOS 系统概述
2) DOS 是如何启动的
3) DOS 是如何加载文件的
4) DOS 中断系统
5) DOS 的文件管理系统
6) DOS 内存分配

1.1 DOS 系统概述

1.1.1 DOS 系统的发展过程

自 1980 年 IBM 公司为其设计的个人计算机系统定 Microsoft 公司出品的 PC－DOS1.0 作为标准操作系统以来,DOS 的发展历程已经过了十余年时间。在这期间,几乎是连续不断地有 DOS 的新版本推出,这些新版本通常与比其版本号低一些的 DOS 系统完全兼容,并且每一个新版本推出都增加了一些以前没有的新功能。操作系统的一步步发展是为了适应 PC 机家族逐渐扩充的需要的,自从基本型 PC 机后,IBM 公司又相继推出了 IBM PC/XT,IBM PC/AT(286),以及 IBM 386 等功能越来越多的新机型,因此 DOS 操作系统也相应地有着与此几乎相同的发展轨迹。

下表统计了 DOS 系统从 1981～1988 年期间的发展过程

版本号	时间	特点
DOS1.0	1981.10	PC 机的第一个操作系统,仅支持单面软盘
DOS1.1	1982.10	这是广泛用于 PC 兼容机的操作系统,可支持双面软盘
DOS2.0	1983.3	PC/XT 所用操作系统,支持硬盘
DOS3.0	1984.8	PC/AT(286)所用操作系统,支持 1.2MB 软盘和大容量硬盘

DOS3.1	1984.11	支持 Microsoft 网络服务系统
DOS3.2	1986.3	支持 3.5 英寸软盘，且驱动器中固化了盘格式化程序
DOS3.3	1987	支持虚拟盘，支持硬盘分区且可支持 PS/2 系统
DOS4.0	1988.6	支持大于 32M 的单一分区及许多强大功能

1.1.2 DOS 常用命令分析

DOS 经启动进驻内存后会出现提示符“>”，此时 DOS 等待用户键入一个 DOS 命令或一个应用程序的命令行。前者是 DOS 提供给用户的各种功能，这些功能妥为两类，分别为 DOS 内部命令和 DOS 外部命令。

执行 DOS 命令时必须遵守以下规范

1）内部命令在 DOS 常驻内存后的任何时刻均可执行。外部命令包含在扩展名为 COM 或 EXE 的文件中，只有这些文件存在于指定驱动器中时才可执行。

2）有的命令在揭示符“>”后发出，用 RETURN 键确认，若没有出现错误信息，则表示该命令执行成功。

3）有的命令后面可跟一个或多个参数，系统按指定的参数执行相应的 DOS 功能，若未键入参数，则按缺省值处理。多个参数之间通常用空格或逗号、分号等隔开。

4）DOS 提供某些键或键的组合来完成一些特殊功能。

下表列出了所有的 DOS 内部命令(3.0 以上)

命令	解释
CD	改变当前目录
CLS	清屏
COPY	拷贝磁盘文件
CTTY	改变主控制台
DATE	修改系统日期
DEL	删除磁盘文件
DIR	列文件清单
ERASR	删除磁盘文件
MKDIR	建立子目录
PATH	建立搜寻目录
PROMPT	定义系统揭示符
REN	修改文件名
RD	删除空目录
SET	设置运行环境
TIME	修改系统时间
TYRE	显示文件内容
VER	显示 DOS 版本号
VERIFY	验证写盘数据
VOL	显示磁盘卷标
ECHO	显示字符串
FOR	循环执行命令

GOTO	控制跳转命令
IF	条件执行命令
PAUSE	暂停命令
REM	显示注释信息
SHIFT	移位替换参数
BREAK	中断 DOS 开关
BUFFERS	置 DOS 缓冲区
COUNTRY	指定国家名称
DEUICE	安装设备驱动程序
FCBS	置打开的 FCB 数
FILES	置打开文件数
LASTDRIVE	置最后驱动器号
SHELL	定义外壳程序

注:上表中自 BREAK 以后为系统配置命令。

下表列出了所有的 DOS 外部命令:

命令字	解释
ASSIGN	分派驱动器请求
ATTRIB	置文件只读属性
BACKUP	磁盘文件转储
CHKDSK	磁盘状态检验
COMMAND	加载命令处理程序
COMP	磁盘文件比较
DEBUG	DOS 调试程序
EISCOPY	复制整张软盘
EDLIN	行编辑程序
EXEIBIN	EXE 文件转换成 COM 文件
FDISK	硬盘格式化
FIND	输出指定字符串
FORMAT	磁盘格式化
GRAFTABL	装入附加图符表
GRAPHICS	拷贝屏幕图形
JOIN	将驱动器连接目录
KEYBYY	装入键盘替换程序
LABEL	设置磁盘卷标
LINK	DOS 连接程序
MODE	设置设备操作方式
MORE	屏幕显示过滤
PRINT	假脱要打印文件
RECOVER	恢复磁盘文件
RESTORE	磁盘文件复原
SELECT	选择国别代码
SHARE	装入文件共享程序

SORT	文件排序过滤
SUBST	驱动器替换路经
SYS	传送系统隐含文件
TREE	显示树型目录

下表列出了所有的 DOS 专用键：

键组合	解释
Ctrl+Alt+Del	系统热启动
Ctrl+BreaK(或 Ctrl+C)	中止命令运行
Shift+Prtsc	当前屏幕打印
Ctrl+P	打印机联机开关
Ctrl+Numlock(或 Ctrl+S)	暂停命令执行开关
F1 或→	从最后一行起一个一个显示字符
F2	显示最后一行中指定字符前所有字符
F3	显示最后一行
F4	跳过最后一行指定字符前的字符
F5	存储当前行
F6	给出文件结束符 Ctrl+z

下面我们介绍一些常用 DOS 命令：

1.1.2.1 DIR 命令

格式：DIR[d:][Path][filename][/p][/w]

解释：列文件清单命令，被文件型病毒感染的系统中用此命令查看文件长度，可发现某些文件变长了，该文件有可能就是染有病毒的文件。

[d:] 表示驱动器号
[path] 表示路径名
[filename] 表示文件名
[/p] 表示逐屏显示
[/W] 表示多列显示

【举例】：

```
A>DIR C:\SAFE\*.*
Volume in drive C has no label
Directory of      C:\SAFE

.              <DIR>    2-05-91      4:05p
..             <DIR>    2-05         4:05p
```

```
SCAN     EXE      46912   12-17-89    12:52p
KILL     EXE       8256   1-01-80     12:04a
SCAN63   EXE      46535   6-02-90     6:06p
        3File(s).        335028 bytes free
```

1.1.2.2 COMP 命令

格式:[d:][Path]COMP [d:][Path][filename]
[d:][Path][filename]

解释:磁盘文件比较命令。这是一个DOS外部命令,最前面的[d:][Path]指名了COMP文件所在的驱动器号及路径名。之后的两个[d:][Path][filename]分别表示两个待比较的文件,前一个称为主文件,后一个称为次文件,在内存中驻留有某些病毒时,我们用DIR命令看不到文件长度的增加(如4096病毒),但如果我们用COMP命令比较一个正确的文件和一个被感染过的文件(必须是两个长度一样的文件)时,就有可能发现病毒。

【举例】:

```
A>COMP A:A1.EXE B:A2.EXE
Compare error at offset 156
File1=MZ
File2=ND
1 Mismatches ending compare
```

1.1.2.3 FDISK 命令

格式:FDISK

解释:硬盘分区命令。这是一个外部命令,只对硬盘操作。在硬盘物理格式化后用此命令建立分区,然后运行格式化命令,在这几个步骤完成之后,硬盘才真正可以使用。

用法:在A>号下键入FDISK

屏幕上会出现FDISK的菜单如下:

1. Create DOS Partiton
2. Change Active Partition
3. Delete DOS Partition
4. Display Partiton Data

若系统配置了两个硬盘,则还有:

5. Select Next Fixed Disk Dive

这些功能分别是建立DOS分区、改变活动分区、删除DOS分区、显示分区信息和选择下一个硬盘。

具体用法在一般的DOS手册上有详细介绍,此处不再讲述。

1.1.2.4 FORMAT 命令

格式:[d:][Path]FORMAT[d:][/s][/1][/8][/v][/8][/4]

解释:磁盘格式化命令,这是一个外部命令。当发生病毒的交叉感染等情况后磁盘数据变得无法挽回了,我们需要对其重新格式化。

最前面的[d:][Path]指明了 FORMAT 文件所在处的驱动器及路径。

[/s]参数表示格式化后立即传送三个系统文件,使之成为可以启动的系统盘。

[/1]参数表示将软盘格式化成单面的。

[/8]参数表示软盘采用每道 8 扇区的格式,否则采用每道 9 或 15 扇区的格式(缺省值)。

[/v]参数表示要求用户给出一个卷标。

[/B]参数表示为目标软盘格式化每道 8 扇区的格式,同时分配空间准备存放 DOS 两个隐含文件。用 SYS 命令可将任何 DOS 版本的系统文件传送到 FORMAT/B 格式化的软盘上。若未用/B,则只有 2.X 版的 DOS 才能用相应的 SYS 命令传送系统,该参数不能与/8 和/V 同时使用。

[/4]表示在高密驱动器上对双面双密软盘进行格式化。

1.1.2.5 系统配置命令

FILES 命令

设置同时打开的文件句柄数。最大值为 20,其中包括 DOS 为标准 I/O 设备预留的 5 个文件句柄:标准输入(0),标准输出(1),标准错误(2),辅助输入输出(3)和标准打印(4)。用于用户程序的文件句柄数为 5.19,所以应用程序一次打开的文件不能超过 15 个。

格式:FILES=X;X 是 8.255 中任一个数,缺省值是 8。

FCBS 命令

设置同时打开的文件控制块数。在网络系统中,当装入文件共享支持软件 SHARE 后,本命令设置允许 DOS 一次同时打开的文件控制块数以及打开的 FCB 中不允许 DOS 自动关闭的文件控制块数。

格式:FCBS=m,n

m 指一次能打开的 FCB 数目,取值 1.255,缺省值为 4。

n 指打开的 FCB 中不能由 DOS 自动关闭的文件数目,取值范围为 0.255,缺省值为 0。

m 必须大于 n

BUFFERS 命令

分配磁缓冲区数量命令。磁盘缓冲区是 DOS 用于存放从磁盘读取或写入磁盘的数据的一块内存。每区容量为 528 个字节。

格式:BUFFERS=X,X 是 1.99 中任一数,缺省值为 2。

DEVICE 命令

安装设备驱动程序命令。在 DOS 启动中,本命令将指定的设备驱动程序装入内存并常驻。

设备驱动程序为.SYS 文件或.BIN 文件,由设备头,策略过程和中断过程三部分组成,包含设备运行行的全部代码。

格式:DEVICE=[d:][path][fileneame]

[d:][Path]分别指明了设备驱动程序所在的驱动器号和路径;

[filename]表示该设备驱动程序的文件名。

所有的系统配置命令均应写在 CONFIG.SYS 文件中,当系统启动时进行加载。

1.2 DOS 是如何启动的

1.2.1 DOS 的构成

DOS 由几个主要部分组成，每一部分对应用程序提供特定支持，这些部分分别称为 DOS Bios 模块，DOS Kernel 模块和 DOS Shell 模块。在三个模块分别对应三个文件，其文件名为 IO. SYS、MSDOS. SYS 和 COMMAND. COM，在 PC. DOS 中则为 IBMBIO. COM、IBMDOS. COM 和 COMMAND. COM。其中前两个文件为系统兼隐含型，用 DIR 命令看不到，但用 PC-TOOLS 等软件可以看到。

1.2.1.1 IBMBIO. COM 文件

这个文件完成 DOS 的基本输入输出管理功能。它是 DOS 中最依赖于硬件的部分，不仅提供所有标准驱动程序而且支持装载和初始化系统。

该文件由两部分组成，分别是系统初始化程序 SYSINT 和标准设备驱动程序。

SYSINT 程序完成系统启动过程中的初始化工作，其中包括确定内存容量、定位 IBMDOS. COM 解释 CONFIG. SYS 并设置系统运行环境等。

标准设备驱动程序由 11 个驱动程序的设备链组成。这 11 个驱动程序为 6 类，它们分别是：

1)标准输入输出设备驱动程序，支持显示器和键盘，名为 CON。

2)标准制表设备驱动程序，支持打印机，名为 PRN，LPTI，LPT2，LPT3。

3)辅助输入输出设备驱动程序，支持异步串行通信接口，名为 AUX，COMI，COM2。

4)时钟设备驱动程序，支持时间和日期的服务，名为 CLOCKS。

5)块设备驱动程序，支持软盘和硬盘的操作，无设备名。

6)空设备驱动程序，支持应用程序的模块操作，其名为 NUL。

这些设备驱动程序由 IBMDOS 通过设备请求头调用。设备请求头是一个有定义的数据结构，含有请求操作的命令码。返回的状态字、传送的内存地址及扇区或字节计数器。设备驱动程序解释这些请求并将其转化为不同硬件设备控制器相应的控制命令。

固化在 ROM 中的硬件驱动程序是独立的，它不仅可由 IBMBIO. COM 调用，而且也可以由应用程序调用。但由于 ROM——BIOS 依赖于硬件，所以直接调用 ROM—BIOS 功能的程序是无法在其它兼容机上运行的。

总之，IBMBIO. COM 是 DOS 内核与 ROM—BIOS 之间的接口，基于 IBMIO. COM 的编程可运行于硬件不完全相同的兼容机。

1.2.1.2 IBMDOS. COM 文件

这个文件完成 DOS 的文件管理和系统调用功能，它是 DOS 的核心。它也由两部分组成，它们分别是内核初始化程序和系统功能调用程序。

前者完成 DOS 内部的初始化工作。包括设置 DOS 中断向量人口，检查常驻的设备驱动链，建立磁盘参数表、设置缺省的磁盘扇区缓冲区等。

后者主要由系统功能调用 INT 21H 构成。该程序向用户提供了一套由 0—63H 子程序号

组成的系统功能调用。这些调用都脱离于具体硬件，具有很好的兼容性。

这此功能分别是：

1）字符设备输入输出功能。

2）磁盘控制功能。

3）动态存储管理功能。

4）目录管理功能。

5）文件管理功能。

6）其它系统功能。

1.2.1.3 COMMAND.COM 文件

这个文件是DOS命令的解释程序，它是操作系统和用户的接口。该文件由三部分组成，它们分别是常驻部分，暂驻部分和Shell初始化程序。

常驻部分 由IBMBIO.COM加载到内存低端位于DOS内核和可安装的设备驱动程序之上。它包括中断22H，27H(控制暂存应用程序的退出或驻留)，23H(Ctrl—C处理)和24H(严重错误处理)以及重新装入暂驻部分的加载程序等。

暂驻部分 由IBMBIO.COM加载到内存高端。它包括命令解程序、内部命令程序、批处理程序等。该部分占据的存储空间有可能被应用程序覆盖。当应用程序退出时，常驻部分检查暂驻部分是否仍然存在，若不存在则要重新加载暂驻部分。

初始化部分 在启动后退出内存。

1.2.2 DOS的软盘启动过程

1.2.2.1 软盘的DOS引导记录

引导记录由三部分组成；它们分别是软盘基数表、软盘I/O参数表、引导记录块。

(1)软盘I/O参数表

该表占19个字节，从偏移0BH处开始，具体内容如下表所示：

字节位移	含义	双面软盘	高密软盘
0—1	每扇区字节数	512	512
H2	每族扇区数	2	1
3—4	保留扇区数	1	1
5	FAT表数	2	2
6—7	根目录项数	112	224
8—9	总扇区数	2DOH	960H
0AH	磁盘标志	FDH	F9H
0BH—0CH	每个FAT表所占扇区数	2	7
0DH—0EH	每道扇区数	9	15

0FH－10H	磁头数	2	2
11H－12H	隐含扇区数	0	0

(2) 软盘基数表

该表占 11 个字节，从偏移 21H 开始，下表描述了其详细参数：

位移	含义	双面软盘	高密软盘
0	高 4 位为步进速率，低 4 位为磁头缺载时间	DFH	EFH
1	高 7 位为磁头加载时间，低 1 位为非 DMA 方式	02H	1AH
2	马达等待时间	25H	25H
3	每扇区数字节数	2	2
4	每道区扇数	9	15
5	扇区间隔字节数	2AH	2AH
6	每区字节数	FFH	FFH
7	格式化时扇区间隔的填充字节	50H	50H
8	格式化时扇区数据的填充字节	F6H	F6H
9	寻找后磁头的稳定时间	15	0
OAH	命令等待时间	2	2

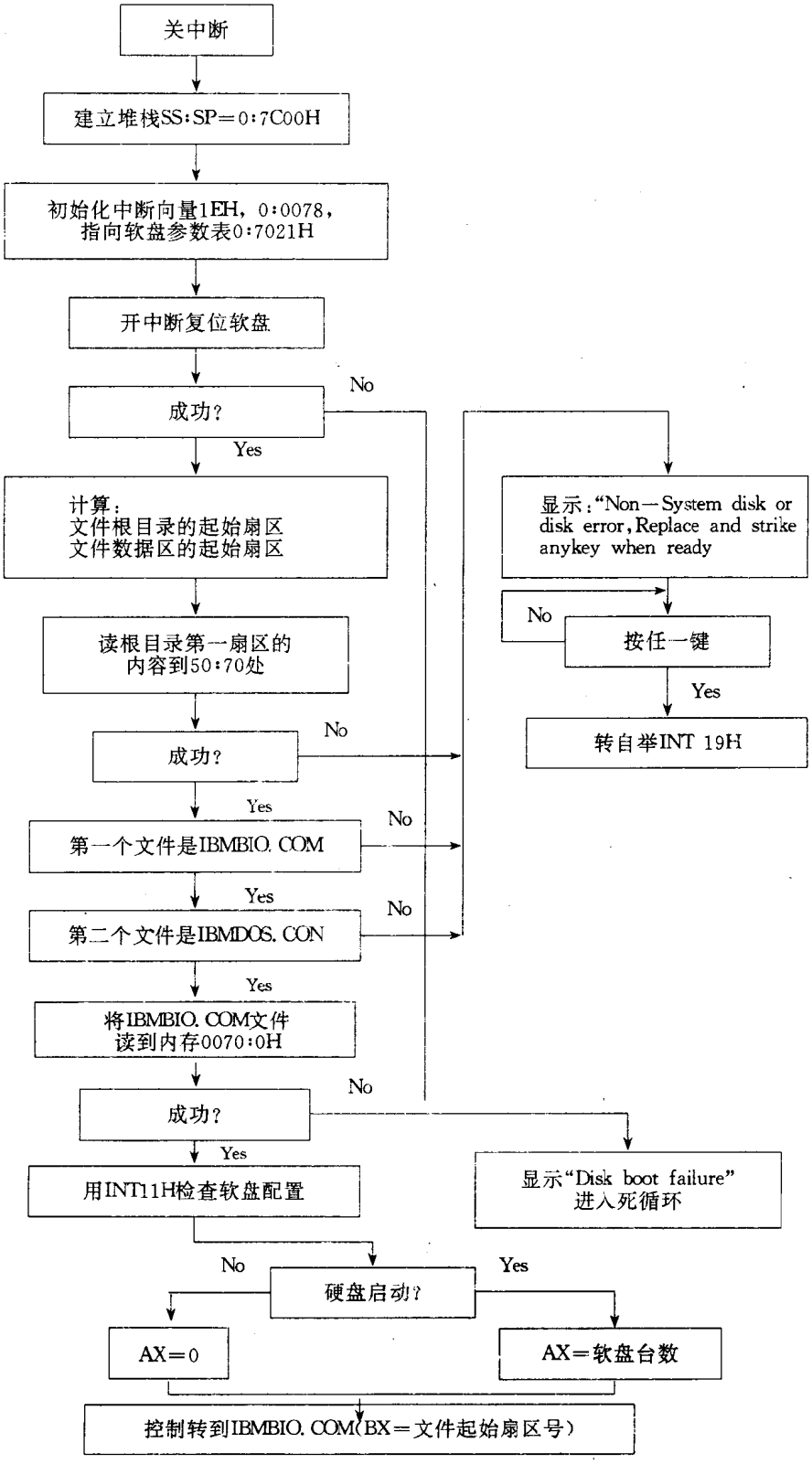
(3) 引导记录块

引导记录块的作用是检查软盘根目录下是否存在两个隐含的系统文件。若存在，则将 IBMIO.COM 读至指定区域，并将控制权交给它。否则，会显示相应出错信息。

下页是引导记录块的流程图：

以下是用 DOS3.3 格式化的软盘的引导记录

```
C>debug
-1100 0 0 1
-d 100 2ff
28CC:0100  EB 34 90  49 42  4D 4D  53-33  2E 33  00 02  02 01 00  .4.IBMMS3.3…
28CC:0110  02 70 00  D0 02  FD 02  00-09  00 02  00 00  00 00 00  .p……
28CC:0120  00 00 00  00 00  00 00  00-00  00 00  00 00  00 00 12  ……
28CC:0130  00 00 00  00 01  00 FA  33-C0  8E D0  BC 00  7C 16 07  …3…|…
28CC:0140  BB 78 00  36 C5  37 1E  56-16  53 BF  2B 7C  B9 0B 00  .X.6.7.V.S.+|…
28CC:0150  FC AC 26  80 3D  00 74  03-26  8A 05  AA 8A  C4 E2 F1  ..&..=.t.&…
28CC:0160  06 1F 89  47 02  C7 07  2B-7C  FB CD  13 72  67 A0 10  …G…+|…rg…
28CC:0170  7C 98 F7  26 16  7C 03  06-1C  7C 03  06 0E  7C A3 3F  |..&.|…|…|.?
28CC:0180  7C A3 37  7C B8  20 00  F7-26  11 7C  8B 1E  0B 7C 03  |.7|. ..&.|…|.
28CC:0190  C3 48 F7  F3 01  06 37  7C-BB  00 05  A1 3F  7C E8 9F  .H…7|…?|..
28CC:01A0  00 B8 01  02 E8  B3 00  72-19  8B FB  B9 0B  00 BE D6  …r…
28CC:01B0  7D F3 A6  75 0D  8D 7F  20-BE  E1 7D  B9 0B  00 F3 A6  }..u…..}…
```


关中断
建立堆栈SS:SP=0:7C00H
初始化中断向量1EH，0:0078，
指向软盘参数表0:7021H
开中断复位软盘
成功？
No
Yes
计算：
文件根目录的起始扇区
文件数据区的起始扇区
读根目录第一扇区的
内容到50:70处
成功？
No
Yes
第一个文件是IBMBIO. COM
No
Yes
第二个文件是IBMDOS. CON
No
Yes
将IBMBIO. COM文件
读到内存0070:0H
成功？
No
Yes
用INT11H检查软盘配置
显示"Non—System disk or
disk error，Replace and strike
anykey when ready
No
按任一键
Yes
转自举INT 19H
显示"Disk boot failure"
进入死循环
No
硬盘启动？
Yes
AX=0
AX=软盘台数
控制转到IBMBIO. COM(BX=文件起始扇区号)

```
28CC:01C0  74 18 BE  77 7D  E8 6A  00-32  E4 CD  16 5E  1F 8F 04  t..w}.j.2…^ …
28CC:01D0  8F 44 02  CD 19  BE C0  7D-EB  EB A1  1C 05  33 D2 F7  .D…}…3..
28CC:01E0  36 0B 7C  FE C0  A2 3C  7C-A1  37 7C  A3 3D  7C BB 00  6.|…<|.7|.=|..
28CC:01F0  07 A1 37  7C E8  49 00  A1-18  7C 2A  06 3B  7C 40 38  ..7|.I…|*.;|@8
28CC:0200  06 3C 7C  73 03  A0 3C  7C-50  E8 4E  00 58  72 C6 28  .<|s..<|P.N.Xr.(
28CC:0210  06 3C 7C  74 0C  01 06  37-7C  F7 26  0B 7C  03 D8 EB  .<|t…7|.&.|…
28CC:0220  D0 8A 2E  15 7C  8A 16  FD-7D  8B 1E  3D 7C  EA 00 00  …|…}..=|…
28CC:0230  70 00 AC  0A C0  74 22  B4-0E  BB 07  00 CD  10 EB F2  p…t"……
28CC:0240  33 D2 F7  36 18  7C FE  C2-88  16 3B  7C 33  D2 F7 36  3…6.|…;|3..6
28CC:0250  1A 7C 88  16 A2  7C A3  39-7C  C3 B4  02 8B  16 39 7C  .|..*|.9|…9|
28CC:0260  B1 06 D2  E6 0A  36 3B  7C-8B  CA 86  E9 8A  16 FD 7D  …6;|…}
28CC:0270  8A 36 2A  7C CD  13 C3  0D-0A  4E 6F  6E 2D  53 79 73  .6*|…Non-Sys
28CC:0280  74 65 6D  20 64  69 73  6B-20  6F 72  20 64  69 73 6B  tem disk or disk
28CC:0290  20 65 72  72 6F  72 0D  0A-52  65 70  6C 61  63 65 20  error..Replace
28CC:02A0  61 6E 64  20 73  74 72  69-6B  65 20  61 6E  79 20 6B  and strike any k
28CC:02B0  65 79 20  77 68  65 6E  20-72  65 61  64 79  0D 0A 00  ey when ready…
28CC:02C0  0D 0A 44  69 73  6B 20  42-6F  6F 74  20 66  61 69 6C  ..Disk Boot fail
28CC:02D0  75 72 65  0D 0A  00 49  42-4D  42 49  4F 20  20 43 4F  ure…IBMBIO CO
28CC:02E0  4D 49 42  4D 44  4F 53  20-20  43 4F  4D 00  00 00 00  MIBMDOSCOM…
28CC:02F0  00 00 00  00 00  00 00  00-00  00 00  00 00  00 55 AA  ……U.
-q
```

以下是用Debug的U命令反汇编的引导记录程序清单：

```
5E49:7C00   JMP +      7C36
5E49:7C02   NOP
5E49:7C03   DB         'IBMMS33'
5E49:7C0B   DW         0200
5E49:7C0D   DB         02
5E49:7C0E   DW         0001
5E49:7C10   DB         02
5E49:7C11   DW         0070
5E49:7C13   DW         02D0
5E49:7C15   DB         FD
5E49:7C16   DW         0002
5E49:7C18   DW         0009
5E49:7C1A   DW         0002
5E49:7C1C   DW         0000
5E49:7C1E   DB         00
5E49:7C1F   DB         00
5E49:7C20   DB         00
5E49:7C21   DB         00,00,00,00,00,00,00,00,00,00
5E49:7C2B   DB         00,00,00,00,12,00,00,00,00,01,00
5E49:7C36   CLI
5E49:7C37   XOR        AX,AX
```