实现 DOS 自动登录文件过程的方法

铁道部第一设计院 郭永华

摘要：本文提出并实现一种 *DOS* 自动登录文件过程的方法，它扩充了 *DOS* 系统管理功能，使其能够监视运行文件，并自动记录下文件各及运行起止时间。

1.引言

众所周知，目前较为流行的 UNIX 和 XENIX 操作系统具有将所有用户上机的日期、用时及使用过的文件资料和过程记录下来的功能，而我们熟悉的 DOS 操作系统却缺乏这种功能。这对于系统管理，特别是公用机房微机的使用管理无疑是非常遗憾的。为此，笔者通过对 DOS 系统功能及文件过程的分析，提出并实现一种自动登录文件过程的方法，它具有类似 UNIX 操作系统 C-shell 的 history 命令的功能，凡是在机上运行的文件，它都能将其路径、文件各及执行时间记录下来。此方法既不影响使用操作，又扩充了 DOS 系统管理功能，具有一定的实用价值。

2.实现原理

在 DOS 环境下可运行的主要有。COM 文件和。EXE 文件。当我们在系统提示符下键入一个可执行文件各进，DOS 是利用命令合理解释程序调用 EXEC 过程将其加载并执行之。本文设计一个中断处理扩充程序，通过修改 DOS 系统功能来实现对文件过程的自动登录。为了实现这一功能，必须将该程序常驻内存，使之成为 INT21H 的一部分，而 DOS 系统本身为我们提供了程序驻留内存的中断和功能调用，即用 INT21H 的 35H(取中断向量)、25H(置中断向量)和 INT27H(驻留内存并退出)。程序驻留内存后便可以监视 DOS 执行的所有文件了。

3.具体实现

程序设计旨在 DOS 执行文件的同时，将运行起始时间及结束时间连同文件名(含路径、驱动器)登录下来，并保存在 C:盘根目录下的一个命令历史记录文件 HISTORY。DOC 中。

在具体实现中，运行文件各的获取是技术关键。由于 DOS 可以用 PATH 命令建一张目录搜字表，而命令合理行键入的文件各并不一定在录前目录下。再者，运行文件各的后缀一般都省缺了。显然，我们不可能从命令行获得完整的文件名。但是，我们知道 DOS 对所有文件的执行都是利用 INT21H 中断 4 BH 号功能进行加载的。此时，DS: DX 正指向当前加载的文件名和路径。由此，我们对 INT21H 中断进行修改，截获 4 BH 号功能调用的入口参数，就得到了被加载文件名。接着调用 2 CH 号功能提取当前系统时间填入记录缓冲区“开始时间”，然后再转去执行原功能。

为了获取运行结束时间，我们修改 INT20H 中断和 INT21H 中断的 φH、4 CH 子功能，插入一段测时程序，在运行文件执行终止回 DOD 时，再次调用 2 CH 功能。

程序中，缓冲区 execname 用于存放一个命令历史记录文件的记录，它对应于当前被加载运行的文件。其格式为：驱动器、路径、文件名＜开始时间--结束时间＞”。

源程序 HIXT。ADM(附后)经过 MASM 编译，用 LINK 连接后，再彤 EXEZBIN 转换成 HIST · COM。将其放在 AUTOEXEC · BAT 文件中，系统启动后一次加载，驻留内存即可。

本程序在 AST386、286 及 IBM PC / XT 等机上使用，效果很好。

```
1 ;*;文件名:  HIST。ASM
2 ;code        segment
3 ;            assume cs:code,ds:code
4 ;            org   100h
5 ;start;      jmp   init
6 ;oid20h      dd    ?                    ;保存原 INT 20H 中断向量
7 ;oid21h      dd    ?                    ;保存原 INT 21H 中断向量
8 ;exechame    db 57 dup(?),3cd           ;存放被加载程序名
9 ;hourl       db    0,0,':'              ;小时的十位数
10;minutel     db 0,0,':'                 ;分的十位数
11;secondl     db 0,0,'-'                 ;秒的十位数
12;hour2       db 0,0,':'                 ;小时的十位数
13;minute2     db 0,0,':'                 ;分的十位数
14;second2     db 0,0,3eh,0ah,0dh         ;秒的十位数
15;count       equ $-execname             ;每次写入字节数
16;fname       db 'c:history。doc',0,0
17;doscall     macro function             ;宏定义调用DOS 功能

18;            mov   ah,function
19;            int   21h
20;            endm
21;hex-bcd     macro hex,buf              ;宏定义将(1 字节的)16进制转换为
22;            mov   al,hex               ;二位数的10进制字符
23;            xor   ah,ah
24;            mov   cl,10
25;            div   cl
26;            add   al,'0'
27;            mov   cs:buf,al
28;            add   ah,'0'
29;            mov   cs:buf+1,ah
30;            endm
31;gettime     macro hour,minute,second   ;宏定义取系统时间
32;            doscall 2ch
33;            push cx
34;            hex-bcd cl,minute
35;            pop cx
36;            hex-bcd cl,minute
37;            hex-bcd dh,second
38;            endm
39;gs-vect     macro intno,oldint,nteint; ;宏定义取/置中断向量
40;            mov al,intno
41;            doscall 35h
42;            mov word ptr oldint,bx
43;            mov word ptr oldint+2,es
44;            mov dx,offset nteint
45;            doscall 25h
46;            endm
```

```
47: new21h      proc far                          ;新INT 21H 中断处理程序
48:             cmp  ax,0ff00h
49:             jne  aa1
50:             mov  al,0feh                      ;设置安装标志
51:             iret                              ;中断返回
52: aa1:        push ds                           ;保存原寄存器
53:             push es
54:             push ax
55:             push bx
56:             push cx
57:             push dx
58:             push si
59:             push di
60:             pushf
61:             cmp  ah,4dh                       ;是加载程序功能调用吗?
62:             jne  aa3
63:             xor  bx,bx
64:             mov  si,dx
65:             cld
66: loop1:      lodsb                             ;取被加载程序名(含驱动器,路径)
67:             cmp  al,33
68:             jb loop2
69:             cmp  al,127
70:             ja loop2
71:             mov  cs:execname[bx],al
72:             inc  bx
73:             jmp  short  loop1
74: loop2:      cmp  bx,count-24                  ;在程序名后补空格符
75:             ja aa2
76:             mov  cs:execname[bx],20h
77:             inc  bx
78:             jmp  short  loop2
79: aa2:        gettime  hour1,minute1,second1;   ;作一次时间测试
80:             jmp  short  aa4
81: aa3:        cmp  ah,4ch                       ;是终止进程功能调用吗?
82:             jne  aa4
83:             call w reco                       ;调子程填写运行记录
84: aa4:        popf
85:             pop  di                           ;恢复寄存器
86:             pop  si
87:             pop  dx
88:             pop  cx
89:             pop  bx
90:             pop  ax
91:             pop  es
92:             pop  ds
93:             assume ds:nothing
```

```
94:                jmp  cs:old21h                    ;转到原INT 21H 中断处理
95: new21h         endp
96: new20h         proc far                          ;新INT 20H 中断处理程序
97:                pushf
98:                call w-reco                       ;调子程填写运行记录
99:                popf
100:               assume ds:nothing
101:               jmp  cs:old20h                    ;转到原 INT 20H 中断处理
102: new20h        endp
103: exist:        mov  bx,ax                        ;填写动物记录子程序
104:               push cs
105:               pop  ds
106:               gettime  hour2,,minute2,second2;  ;再作一次时间测试
107:               movdx,offset fname
108:               mov  al,1
109:               doscall  3dh                      ;打开文件
110:               jnc  exist
111:               mov  cx,20h
112:               doscal 3ch                        ;建立一个新文件
113: exist:        mov  bx,ax
114:               xor  dx,dx
115:               mov  cx,dx
116:               mov  al,2
117:               dosacll  42h                      ;指针移到文件尾
118:               mov  cx,count
119:               mov  dx,offset execname
120:               doscall  40h                      ;写文件
121:               doscall  3eh                      ;关闭文件
122:               ret
123: w reco        endp
124: init:         mov  ax,0ff00h                    ;测试安装标志
125:               int  21h
126:               cmp  al,0feh
127:               jne  next                         ;第一次安装,转显示已装入信息
128:               mov  dx,offset masg
129:               doscall  9h
130:               int  20h
131: next:         gs-vect  21h,old21h,new21h;       ;取/置 INT21H中断向量
132:               gs-vect  20h,old20h,new20h        ;取/置 INT20H 中断向量
133:               mov  dx,offset init
134:               int  27h                          ;驻留退出
135: masg          db '<HIST> has been installed!',0ah,0dh,07,'$'
136: code          ends
137:               end  start
```