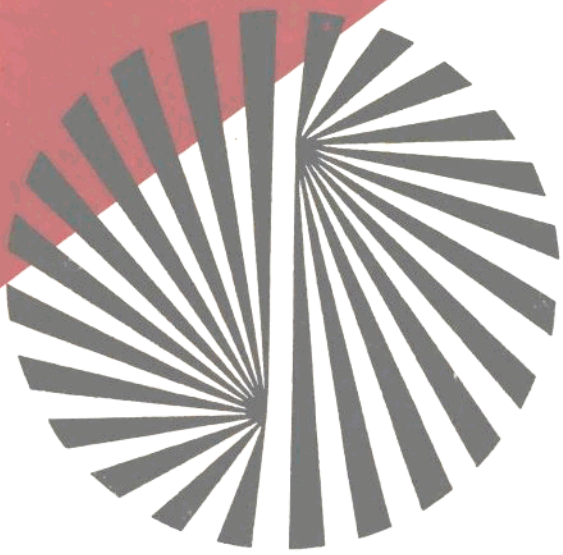
电脑步步高丛书·9·



朱 彤 编著

常用动态调试软件

中山大学出版社

电脑步步高丛书(9)

常用动态调试软件

朱彤 编著

中山大学出版社

·广州·

(粤)新登字 11 号

版权所有　不得翻印

图书在版编目(CIP)数据

常用动态调试软件/朱 彤编著. —广州:中山大学出版社,1994

(电脑步步高丛书(9))
ISBN7—306—00897—8

Ⅰ 书名
Ⅱ 朱 彤
Ⅲ ①计算机 ②动态调试
Ⅳ TP3

责任编辑:张亚拉
责任技编:黄少伟　　封面设计:朱震华

*

中山大学出版社出版发行
(广州市新港西路135号)
广东省新华书店经销
中山大学出版社印刷厂印刷

*

787×1092 毫米　16 开本　8 印张　17 万字
1994 年 6 月第 1 版　1994 年 6 月第 1 次印刷
印数:1—5000 册　　定价:7.80 元

《电脑步步高丛书》

序

电脑技术在现代社会中的重要性随着电脑应用的普及而变得越来越明显。技术的现代化，生产与管理的自动化，信息处理与交换的网络化，领导决策的科学化，教育与娱乐的影视化，乃至于物业与家庭理财方式和个人就业基础的变化等，都与电脑技术有着密切的联系。越来越多的人认识到学习电脑的重要性，领导人号召“电脑的普及要从娃娃抓起”。《电脑步步高丛书》就是为了给普及电脑开路。丛书从选题到选材都处处为广大电脑用户着想，试图给他们提供一套既简明扼要又系统实用的电脑技术资料。

电脑技术本身也在日新月异地发展着。硬件技术不断出现革命性的进步。多样性、多功能、多版本的系统软件与应用软件层出不穷，已有的系统和软件尚未摸透，新版的系统和软件又已流行开来，电脑技术的发展永无尽头。知识更新的速度是如此之快，以至于不奋起直追就跟不上潮流。时势造英雄，勇于开拓进取的人方有可能成为时代的弄潮儿。《电脑步步高丛书》就是这些弄潮儿发表自己的经验、体会和成果的天地。

中山大学出版社计算机图书编辑室

1994年3月

前　言

随着计算机的广泛应用和日益普及，它越来越深入到人们日常生活的各个领域。同时，与之相应的应用软件也以越来越快的速度开发出来和升级更新。由于软件产品是一种特殊的产品，生产难度大，成本高，又极易被复制，所以生产厂家出于商业上或技术上的考虑，往往会对其软件产品进行加密。另一方面，用户常常企图破译应用软件的密码，以便修改程序的某一部分来满足自己的实际需要，这就是所谓解密。

为了对软件进行解密或者调试一个程序，那就免不了要对其进行动态跟踪。最好的、功能最强的动态跟踪工具当然首推动态调试卡，但是，对于广大的微机使用者来说，这种专业性质的硬件设备过于昂贵，他们更感兴趣的是动态调试软件。

目前，有多种多样的动态调试软件。常见的有DOS系统的外部命令DEBUG，Windows系统的符号调试工具SYMDEB，Microsoft公司生产的CODEVIEW和全屏幕调试工具FSD(Full Screen Debug)，Borland公司出品的Turbo Debugger，以及Nu－Mega技术公司的Soft－ICE等。Soft－ICE的动态调试功能特别强大，并随着386微机的普及而拥有越来越多的用户。

本书对上述动态调试软件都作了介绍，但重点介绍的是Soft－ICE (2.5版)。结合作者的使用经验，本书第6章介绍了一些常用的反动态跟踪技术，以便于读者进行动态调试时，能正确地判断和克服应用程序中设置的反跟踪障碍，使调试得以顺利进行下去。在本书附录中有重要端口和数据区的资料。在进行动态跟踪时，这些资料有时候是必不可少的。

本书的第五章由彭悦浩编著，特此表示感谢。

编　者

1994－5 于广州

试读结束：需要全本请在线购买：　www.ertongbook.com

目 录

1 概述

1.1 使用 Soft－ICE 的最大好处

当你调试或跟踪一个程序时，如果你使用的是 DOS 的 DEBUG 或 Turbo Debug 等其它一些动态调试工具，有时你会遇到这样一些情况：

最使你感兴趣的部分如果不在程序的开头，而是在中间，一大堆初始化代码之后，你不得不从开头进入，并艰难地越过这些对你来说毫无意义的代码以后，才能达到你感兴趣的部分；或者，你正在跟踪一个有加密措施的程序的执行过程时，在关键代码部分出现之前，该程序的自我保护指令关闭了显示屏，甚至屏蔽了键盘，使你试图分析其加密措施的希望成为泡影……。

在你束手无策或被一大堆只起除始化作用的非关键部分代码搞得心烦意乱时，你可能会希望：要是有一个功能强大的，并且能在任何时候随时进入的调试器，那么，一切将会变得顺手多了。

Soft－ICE 正是你所希望拥有的这种强大武器。

1.2 Soft－ICE 的描述

Soft－ICE 是一个优秀的动态调试工具，它提供硬件级的动态调试。具有强大的动态调试功能。

Soft－ICE 使用分页、I/O 特权级别、断点寄存器等 80386 保护方式的特性，在虚拟机上运行 DOS，以增加硬件级断点。

Soft－ICE 的这些特性，对于实时处理、硬件级中断、内存保护、中断服务等方面的程序的调试和跟踪显得特别方便。如果你还不熟悉 Soft－ICE，只使用过 CODEVIEW 或其它调试软件，由于 Soft－ICE 能与其它现有的调试程序一起工作，所以，你大可不必了解一个全新的动态调试程序就能得到一个取长补短的强有力的动态调试组合工具。

而且 Soft－ICE 具有良好的窗口界面，在线帮助等，使你能很方便的使用。Soft－ICE 还具有远程调试、双监视器等强大功能。

1.3 Soft－ICE 的特性

1）通过热键可随时弹出调式程序或返回应用程序。

2) 可在内存读写、口读写、内存指令执行、中断时方便地设置断点。
3) 在符号及源程序级上进行的动态调试。
4) 回溯过去的跟踪。
5) 与其它调试程序一起工作。
6) 支持 EMM4.0 协定。
7) 以 80386 保护方式工作。
8) 良好的窗口界面。
9) 充分利用内存资源。
10) 可调试设备驱动程序、中断服务程序、引导程序等 DEBUG 不便于调试的程序。
11) 灵活的热键及功能键设置功能。
12) 支持双监视器。

1.4 系统配置

Soft－ICE 只能工作在 386 或 386 以上的机型。又因为 Soft－ICE 不使用 DOS 的功能调用和 ROM BIOS 中断作为其屏幕显示及键盘输入，而是直接对硬件端口操作，所以，显示卡必须与 MDA、HERCULES、CGA、EGA、或 VGA 完全兼容。

1.5 磁盘文件

Soft－ICE 装在 5″ 或 3″ 磁盘上，包含以下文件：

S－ICE.EXE	Soft－ICE 主程序文件
S－ICE.DAT	包含初始化命令的文本文件
LDR.EXE	源程序和符号文件以及可执行文件的装入程序
MSYM.EXE	符号文件生成程序
UPTIME.EXE	设置时钟的程序
README.SI	包含有没出现在操作手册上的有关 Soft－ICE 最新信息的文本文件
SAMPLE.EXE	一个用作示范的短程序
SAMPLE.ASM	用作示范的汇编语言源程序
SAMPLE.SYM	示范程序的符号文件
IOSIM.ASM	一个受用户限制的断点的汇编语言源程序文件的例子
IOSIM.EXE	一个受用户限制的断点的例子

试读结束：需要全本请在线购买： www.ertongbook.com

2 Soft－ICE 命令

2.1 安装

Soft－ICE 既可作为一个可安装的设备驱动程序在 CONFIG.SYS 中装入，也可在 DOS 提示符下直接安装。

2.1.1 在 DOS 提示符下安装

假如你所用的计算机上没有扩展内存，则只能这样安装。在 DOS 提示符下，象普通外部命令一样，敲入：

S－ICE

Soft－ICE 将装入内存高端，并对 DOS 为不可见，以后 DOS 在进行内存管理时将认为此处内存是不存在的，并且不能再分配给其它程序使用。因此，建议在其它内存驻留程序(TSR)或控制程序之前装入 Soft－ICE。

2.1.2 在 CONFIG.SYS 中作为设备驱动程序装入

如果你所使用的计算机上有扩展内存，那么最好把 S－ICE.EXE 作为设备驱动程序装入 CONFIG.SYS 中，这样才能充分发挥 Soft－ICE 的优越性能：

1) 与其它使用扩展内存的程序一起共享扩展内存，如 VDISK.SYS、SMARTDRV.SYS、PC－CACHE.EXE 等。

2) 使用 EMM4.0 的各种性能。

3) 在符号或源程序级上进行动态调试。

4) 回溯过去的跟踪。

5) 与其它调试程序共同工作。

Soft－ICE 将为主程序体以及相关保留部分定位一定的扩展内存，但 S－ICE.EXE 必须在 CONFIG.SYS 中的任何其它定位在扩展内存的设备驱动程序（如 VDISK.SYS)之前装入。建议在初次使用 Soft－ICE 时，把 S－ICE.EXE 作为第一个设备驱动程序写入 CONFIG.SYS 中：

DEVICE＝DRIVER:\PATH\S－ICE.EXE

而且为了更好的使用 Soft－ICE，应把 Soft－ICE 所在的路径写入 AUTOEXEC.BAT；另外，在符号或源程序级上进行调试时，为了搜索源文件路径，可设置环境变量 SRC：

SET SRC=PATH1;PATH2;……

其中 PATH1,PATH2,…… 为源文件所在目录,当要装入源文件时,将顺序搜索上述路径。

当然,也可在 DOS 提示符下直接运行 S－ICE.EXE。使用这种方法时,S－ICE.EXE 将自动安装在扩展内存顶端,几乎不占用常规内存。如果,扩展内存顶端已被其它程序占用,S－ICE.EXE 将覆盖它。所以只有能确定在此之前,没有任何其它程序装在扩展内存高端时,才能这样装入,且 Soft－ICE 的许多优良性能在此环境下才能充分发挥。

2.2 开始使用 Soft－ICE

本书使用说明:按 CTRL＋D 指先按下 CTRL 键不放,再按下 D 键;输入 WIN,指依次键入 W、I、N,然后按回车键,其余类似。所有介绍均以 Soft－ICE 2.5 版本为准。

2.2.1 激活

当安装好 Soft－ICE 后,可在任何时侯通过热键序列来随时激活 Soft－ICE。如果没有在 S－ICE.DAT 中作特殊的初始化处理,改变热键序列,那么,缺省的热键序列为 CTRL＋D。

按 CTRL＋D 激活 Soft－ICE,这时,你可以看到如下图所示的窗口。

如果路径设置不正确的话,搜索不到 S－ICE.DAT 初始化文件,窗口可能只有部分显现,若是小窗口,则可输入窗口命令 WIN,使其扩展为大窗口。

最上面一层为寄存器窗口,显示 AX、BX、CX、DX、SP、BP、SI、DI、DS、ES、SS、CS、IP 和标志 FLAGS 的值,标志置位以大写的高亮度字符表示。

第二层为数据窗口,左边为地址,中间是十六进制数据,右边是对应的 ASCII 码。

第三层为代码窗口,左边为地址或行号,中间是机器代码,右边是反汇编指令或源程序行。

第四层为命令窗口,输入各种控制命令。

底层是命令提示行,显示在线提示帮助。

```
AX=0100  BX=0003  CX=00F9  DX=007F  SP=0A8C  BP=0000  SI=010D  DI=01FB
DS=0123  ES=0123  SS=0123  CS=0123  IP=1111  o  d  I  s  z  a  p c
-------------------------------------------------------------------
0000:0000 8A 10 1C 01 F4 06 70 00-16 00 77 0F B2 07 6A 02  ......p...w...j.
0000:0010 F4 06 70 00 B0 04 D8 17-43 EB 00 F0 EB EA 00 F0  ..p.....c.......
0000:0020 3C 00 77 0F B3 02 39 11-57 00 77 0F 6F 00 77 0F  <.w...9.W.w.o.w.
0000:0030 87 00 77 0F 9F 00 77 0F-B7 00 77 0F F4 06 70 00  ..w...w...w...p.
-------------------------------------------------------------------
FDC8:A680 C3              RET
FDC8:A681 26C43E3400      LES     DI,ES:[0034]                ES:0034=0018
FDC8:A686 03FB            ADD     DI,BX
FDC8:A688 C3              RET
FDC8:A689 E8E0FF          CALL    A66C
FDC8:A68C 72FA            JB      A688
FDC8:A68E 26803DFF        CMP     BYTE PTR ES:[DI],FF
FDC8:A692 7504            JNZ     A698
-------------------------------------------------------------------
:BC *
:EC
:PRN LPT2
:RS
:BPX
:     Enter A Command or ? For Help
```

2.2.2 退出

再按 CTRL＋D，或输入命令 X，退回到应用程序界面状态。

2.2.3 窗口操作

1）改变大小

ALT＋↓　　使窗口变矮

ALT＋↑　　使窗口变高

窗口高度可在 8 行到 25 行之间调整。

改变窗口宽度用 WIN 命令，当 WIN 命令不带参数时，将使窗口宽度在全屏幕宽和 46 个字符宽之间反复切换。

2）移动

当采用小窗口模式时，通过移动窗口，使你看到 Soft－ICE 窗口后面由应用程序所显示的屏幕信息，这对于调试需要观察屏幕输出的程序显得特别方便。

CTRL＋↓　　把整个窗口向下移动一行

CTRL＋↑	把整个窗口向上移动一行
CTRL＋←	把整个窗口向左移动一列
CTRL＋→	把整个窗口向右移动一列

2.2.4 行编辑操作

通过行编辑键，可以编辑以前的输入，而且每个键的意义都相当直观、方便，并有类似于 DOSKEY 的功能，可以回溯以前输入的命令。

↓	显示下一条命令
↑	显示上一条命令
←	向左移动光标
→	向右移动光标
PgUp	向上滚动一页
PgDn	向下滚动一页
SHIFT＋↓	向下滚动一行
SHIFT＋↑	向上滚动一行
INS	切换插入/改写方式
DEL	删除当前字符
HOME	光标移至行首
END	光标移至行尾
BACKSPACE	删除光标左边的字符，并退一格。
ESC	取消当前命令

注意，当光标在命令窗口时，↑、↓ 键起类似于 DOSKEY 的作用，当光标在代码窗口或数据窗口中时，与 SHIFT＋↑、SHIFT＋↓ 相同，使窗口屏幕上滚或下滚一行。

2.2.5 语法

在 Soft－ICE 中，命令的语法规则为：

命令　　参数

命令长度为一至六个字符，参数可有多个，以空格分开，参数必须是 ASCII 串或表达式。

1）ASCII 串

ASCII 串是以单引号或双引号括起来的 ASCII 字符串。

2）表达式

表达式是由地址参数、数字、数字参数，以及寄存器组成，并且可由 ＋、－、*、/ 四种运算符连接。

（1）数字一般是十六进制数的形式。

（2）数字参数可分为字节参数、字参数、双字参数三种：

0F	字节参数
23CE	字参数
B000:8000	双字参数

双字参数是由用分号隔开的两个字参数组成。

(3) 寄存器

可用于表达式的寄存器有:AL、AH、AX、BL、BH、BX、CL、CH、CX、DL、DH、DX、SI、DI、BP、SP、IP、CS、DS、ES、SS、FLAGS。

(4) 地址参数

地址参数可以是双字参数,也可以是段址:偏移量的形式(如 DS:SI)。

另外,还可以用一些特殊符号来表示相应的地址:

$	当前的 CS:IP
@地址	间接地址
.NUMBER	源程序行号
.	当前指令

注意:@ 可多级嵌套。举几个例子如下:

U CS:IP-0A

反汇编从当前指令以前十字节处开始的指令。

U $-0A

同上。

U.10 (注:此处为十进制)

从源程序的第十行开始反汇编。

G @SS:SP

如果当前 IP 在中断服务或子程序的第一条指令处,这条指令将在调用处的下一条指令处设置断点,并连续执行完中断服务或子程序,返回调用处。

2.2.6 帮助信息

如果你对 Soft-ICE 的某条命令的使用方法不是很熟悉,那么,你可以在 Soft-ICE 窗口下用 ? 或 H 命令来获得及时的帮助。

?	显示所有命令的简短描述。
? 命令	显示某一特定命令的较详细帮助及其使用举例
? 表达式	求表达式的值,并依次以十六进制,十进制和 ASCII 码三种方式显示结果。

用 H 代替上述的 ？，结果完全一样。

2.2.7 一个简单例子

以下以 Soft－ICE 自带的一个简单汇编程序 SAMPLE 为例，介绍如何用 Soft－ICE 来调试程序。

在 CONFIG.SYS 的第一行安装 Soft－ICE：

```
DEVICE=DRIVE:\PATH\S-ICE.EXE /SYM 50
```

参数 /SYM 50 表示为符号及源程序保留 50K 的扩展内存。若没有扩展内存，可在 DOS 提示符下直接运行 S－ICE. EXE，但不能在符号及源程序级进行调试。另外，在 AUTOEXEC.BAT 中，写明 Soft－ICE 的搜索路径。然后重新启动系统，初始化屏幕如下：

```
                Soft－ICE
Kelvin Ishigo
Elite High Technology Inc.
Registration #SI011753

Copr. (c) Nu－Mega Technologies 1987, 1990
All Rights Reserved
Soft－ICE Version 2.50
Soft－ICE is loaded from 00227000H up to 00260000H
50K of symbol space reserved
10K of back trace space reserved
1180K of extended memory avaiable
```

第一行至第八行是版权及版本信息，第九行告诉你 Soft－ICE 及其相关部分所占用内存的确定区域，第十行显示有多少符号和源程序所用的符号空间被保留，第十一行显示有多少内存为回溯跟踪缓冲区所保留(默认为 10K)，第十二行显示还有多少扩展内存剩下。

首先用 CTRL＋D 激活 Soft－ICE。

接着，用 WIN 命令，在小窗口模式和全屏幕方式之间切换，若是小窗口，用 CTRL＋↑、CTRL＋↓、CTRL＋←、CTRL＋→，可使窗口分别向上、下、左、右移动；用 ALT＋↑、ALT＋↓，可使窗口变高、变矮；用 SHIFT＋↑、SHIFT＋↓，可使当前窗口信息上滚、下滚一行；而 PGUP、PGDN，可使当前窗口信息向上翻页或向下翻页。

WR 命令可使寄存器窗口打开或关闭。

MAP 命令显示系统内存的映象，当前指令指针(CS:IP)所在区域是用高亮度表示的。

VER 命令显示版本号。

RS 命令将暂时显示应用程序屏幕，待按任一键后，返回 Soft－ICE 窗口，这对于监视应用程序的输出十分有用。

CLS 命令可清除命令窗口。

X 命令退出 Soft－ICE 窗口。

现在，我们已经知道了几个最常用的 Soft－ICE 控制命令，接下来我们将会试着调试

试读结束：需要全本请在线购买： www.ertongbook.com