经典
游戏工具软件

- 详细介绍常用图形、图像工具软件
- 图形、图像工具软件使用方法及实用技巧
- 图文并茂

888

电脑报888工具软件系列丛书

曹国钧 主编

西南交通大学出版社

电脑报 888 工具软件系列丛书

1. 流行压缩工具软件	9.80 元
2. Norton 6.0～8.0 实用小工具集	9.80 元
3. 最新多媒体实用工具	9.80 元
4. Windows 3.x 工具软件	9.80 元
5. Windows 95 工具软件	9.80 元
6. 经典游戏工具软件	9.80 元
7. 常用图形图象工具软件	9.80 元
8. 超级便携工具软件	9.80 元

ISBN 7-81022-889-7

ISBN 7—81022—889—7/T・166

套价：78.40 元(本册定价：9.80 元)

9 787810 228893 >

作者介绍

曹国钧，高级工程师，1991 年毕业于重庆大学，硕士。现从事计算机应用开发工作。

作为中国计算机界自由撰稿人、栏目主持人、计算机专业作家，他曾在多家权威计算机报纸、杂志（如《计算机世界月刊》、《中国计算机用户》、《Modern Computing》、《电脑报》、《软件报》等）上发表 200 多篇文章。他还是清华大学出版社等中国十余家著名出版社的特约作家。曹国钧目前已经或正在出版的计算机专业著作数十本，包括 MS－DOS、Windows 及应用程序、Windows 95、WPS、CCED、汉字系统（UCDOS、天汇、2.13 等）、硬盘、多媒体方面。现在是《电脑报》明星栏目《专家坐堂》栏目主持人，《新潮电子》杂志的特约撰稿人。

电脑报 888 工具软件系列丛书

经典游戏工具软件

曹国钧 著

- 游戏巫师 Game Wizard
- GameTools
- GB4
- FPE（整人专家）
- 解拆大全 CM386

西南交通大学出版社

内容提要

在这个繁荣的电脑时代里，游戏成为人们消遣娱乐的一种方式，随之而来的游戏破关与解密也就诞生了。

目前出现了许多用于修改游戏的软件，例如，GB (Game Buster) 、DGB (Disk Game Baster) 、SGB (Super Game Buster) 、GW (Game Wizaed) 、GTS (Game Tools) 、FPE (Fix People Expert) 、CM386 (Crack Mate) 等。

本书将介绍这些游戏工具的各种不同的使用方法和技巧，使游戏的破关、解密变得较为容易。

本书内容全面，深入浅出，通俗易懂。

本书适用于计算机爱好者、游戏发烧友。

电脑报 888 工具软件系列丛书

（经典游戏工具软件）

曹国钧　主编

*

西南交通大学出版社出版发行

（成都二环路北一段 610031）

全国新华书店经销

重庆日报社印刷厂印刷

*

开本：150×260 1/20 印张：5.7

字数：140 千字　印数：1—10000 册

1996 年 8 月第 1 版

1996 年 8 月第 1 次印刷

ISBN 7—81022—889—7/T・166

套价：78.40 元　本册定价：9.80 元

目　录

导　引

您曾经为了游戏不能破关而烦恼吗？

您曾经为了游戏不能解除密码（口令）而无法感到不知所措吗？

目前出现了许多用于修改游戏的软件，例如，GB（Game Buster）、DGB（Disk Game Buster）、SGB（Super Game Blaster）、GW（Game Wizaed）、GTS（Game Tools）、FPE（Fix People Expert）、CM386（Crack Mate）等。这些游戏工具提供了各种不同的方法和技巧，使游戏的破关、解除密码变得十分容易。即使您对汇编语言一点也不懂，也能轻松地使用这些游戏工具完成您想要做的事情。

我们在本书中将详细地介绍这些游戏工具的主要功能、特点、使用方法与技巧，并给出详细的实例分析。

为了使读者对游戏工具有一个初步的了解，我们将列出游戏克星 3.0/4.0（Game Blaster）、游戏巫师（Game Wizard）、游戏工具（Game Tools）、整人专家（Fix People Expert）、解拆大王（CM386）等流行游戏工具的比较表。

流行游戏工具比较表

比较项目		游戏克星	游戏巫师	游戏工具	整人专家	解拆大王
版本		V3.0/4.0	V2.30	V3.22	V4.0	V2.0
出版时间		1992	1994	1993	1994	1992
占用内存（KB）	常规	110	0	11	0	10
	EMS	190	10	0	76	0
系统最低要求	CPU	8086	80286	80386	80286	80386
	RAM	640KB	1MB	1MB	1MB	1MB
支持显示卡类型	CGA EGA VGA SVGA	VGA SVGA	VGA SVGA	VGA SVGA	VGA SVGA	VGA SVGA
内存卸载		不可	可	可	可	可
扫描范围		0－640KB	0－16MB	0－640KB	0－4MB	0－640KB
扫描方式种类		2	3	2	2	2
需扫描次数		较多较少	一般	最少	一般	
最大扫描次数		10	20	20	256	20
按字扫描		不可	可	可	可	可
表格中地址数		8	10	9	12	10
表格中数据锁定		可	可	可	可	可
表格存储、重载		可	可	可	可	可
游戏存储、重载		可	可	可	可	可
支持语音卡		一般	好	好	好	一般
速度调整		可	可	可	可	可
保护模式游戏		不支持	支持	不支持	不支持	不支持

DOS/V 游戏	不支持	不支持	不支持	支持	不支持
改变中断设置	可	可	可	不可	可
鼠标器模拟键盘	可	不可	不可	不可	不可
内存修改	可	可	可	可	可
鼠标器激活	不可	不可	不可	可	不可
内置 Debugger	没有	有	没有	没有	有
文本阅读	不可	可	不可	可	不可
精确查找	可	可	可	可	不可
调整游戏进度	可	可	可	可	不可
保存游戏地址表	可	可	不可	可	不可
装入地址表时自动调整地址	不可	不可	不可	可	不可
可输入 10 进制数	可	可	可	可	不可
中止并退出游戏	可	可	可	可	不可
退出驻留	不可	可	可	可	不可
定义热键	不可	可	不可	可	不可
老板屏幕	不可	可	不可	可	不可
抓图	不可	不可	不可	可	不可
转到 DOS 外壳	不可	可	可	不可	不可
支持 EMS/XMS	可	可	可	可	不可
装入高端	不可	可	可	可	不可
外部调试器	不可	不可	可	不可	不可
中断监控	不可	不可	可	不可	不可
自动屏幕保护	不可	可	不可	不可	不可
同时查看文件	不可	可	不可	不可	不可

通过这个表，读者就可以根据自己的需要选择合适的游戏工具软件。

第一章 游戏克星 GAME BUSTER 4.0

GAME BUSTER 4.0(又称为 GB4) 是游戏软件中使用最多的分析工具。为了使读者对 GB4 有一个深刻的了解,本章将详细地介绍 GB4 使用、分析与实例。

1.1 GAME BUSTER 4.0 软件介绍

1.1.1 基本配置

[1] IBM PC/XT/AT/386/486/Pentinm;最少 640KB 内存;
[2] 单色、CGA、EGA、VGA 显示器;
[3] DOS 3.3 或以上版本。
推荐存储器容量:
[1] 190KB 左右扩充内存(EMS)
[2] 250KB 左右扩展内存(XMS)
[3] 以硬盘空间来模拟内存 (载入 GB 之前先执行 EXTDISK.EXE)
GB4 软件包括如下文件:

[1] GB.EXE	游戏克星 4 的主程序
[2] GBINST.EXE	游戏克星硬盘安装程序
[3] GBUNINST.EXE	游戏克星的硬盘反安装程序
[4] EXTDISK.EXE	硬盘空间模拟扩展存储器程序
[5] SEEGA—CO.EXE	单显模拟 CGA 彩显程序
[6] SEEGA—LD.EXE	特殊大容量格式化磁盘读写程序
[7] GB4.BAT	执行游戏克星 4 的批处理文件

1.1.2 安装工作及使用注意事项

1. 使用软盘

使用 DOS 开机后,将 GAME BUSTER 4.0 磁片放入 A 软盘中,执行"GB.EXE"文件便可将 GAME BUSTER 4.0 载入内存之中。另外因为游戏克星 4 是一套极为专业化的商品工具软件包,故在安装及使用的过程中需注意到很多方面,以保证游戏克星 4 的正常运行及其本身安全。

2. 使用硬盘

[1] 某些防病毒系统的使用者应特别注意:在您完成了硬盘的安装或反安装程序之后,请您马上执行防病毒系统保存 BOOT 信息程序,否则下次执行时防病毒系统将报告硬盘分区表受到改变,最好不要使用防病毒系统。

[2] 在执行硬盘安装及反安装过程中,您的硬盘 C 及原版软盘不要设定为写保护。

[3] 若您在执行安装程序时,出现"ERROR :STANDARED FORMAT

OF HARD DISK C"，则说明您的硬盘格式不能为 GB4 接受，这时您只能在软盘上执行游戏克星。

[4] 在游戏克星原版软盘上，不要再写入任何资料，否则，原版软盘有可能受到毁灭性的破坏。

[5] 若您的硬盘在安装 GB4.0 之后，受到病毒感染或者破坏，请不要再使用硬盘中的 GB.EXE 程序(因执行时可能死机)。此时，您应该执行游戏克星 4 的硬盘反安装程序，将其复原回原版软盘里。若这样做成功了，请记住清除病毒之后再执行 GB4 的硬盘安装程序，重新安装 GB4.0。

3. 硬盘安装

开机后，将 GAME BUSTER 4.0 的原版软盘放入 A 驱动器中，并执行 GBINST.EXE 安装程序。在执行完之后，请在您的硬盘的根目录下建立一个叫"GB4" 的子目录，把 A 盘中的所有文件以 COPY 命令拷贝到 GB4 子目录下，以后在硬盘的 GB4 的子目录 GH 下直接敲 GB4 执行文件就可以了，此时，就可运行 GB4 了。

4. 硬盘反安装

若您要将 GAME BUSTER 4.0 带到别的电脑上执行或者您要重新

格式化您的硬盘 C:，或者更新硬盘 C:，或者更新主机板，您都必须先将 GAM

E BUSTER 4.0 反安装回您的 GB4 原版软盘上。

首先将 GAME BUSTER 4.0 的原版软盘放入 A 驱动器中，再执行

GBUNINST.EXE，执行完毕后，反安装的工作就完成了，而此时您的硬盘里的 GAME BUSTER 4.0 程序便无法再继续执行。当您的更改工作完成后，请再把 GAME BUSTER 4.0 用前述的硬盘安装步骤重新安装回硬盘 C，这样，GB4 就可再次正常使用了。

5. 解密版的 GB4 的安装

目前流行的 GB4 大多数是解密版的，只有一个文件 GB4.EXE。该文件只要拷贝到硬盘中就可使用。在软盘也能正常使用。

另外，请用户注意：若您使用"STACKER"软件倍容您的硬盘，安装后请把"GB.

EXE" 拷贝至没有被"STACKER"压缩过的标准硬盘上。GB4 可以在 DBLSPA

CE 压缩的硬盘上正常使用。

1.1.3 装载方式

当键入"GB" 执行 GB4，显示一段版权信息后，GB4 程序便以常驻方式存于内存之中。

此外您也可加入参数执行，可使用的参数如下：

(1) 显示卡参数

当 GAME BUSTER 4.0 载入时会自动判断您使用的图形界面卡，若 GB4 判断错误

时，您可加入以下参数执行：

.GB/H ：GB4 单色版本。

.GB/C ：GB4CGA 版本。

.GB/E ：GB4EGA 版本。

.GB/V ：GB4VGA 版本。

.GB/V=？：执行 GB4 Super VGA 版本。

？=0 代表　标准 VGA CARD

？=1 代表　ET3000 SVGA CARD

？=2 代表　ET4000 SVGA CARD

？=3 代表　TTRIDENT SVGA CARD

？=4 代表　ATI SVGA CARD

？=5 代表　EXVEREX SVGA CARD

？=6 代表　PARADISE SVGA CARD

？=7 代表　VIDEO SVGA CARD

？=8 代表　TSENG 640＊480 MODE

？=9 代表　CHIPS & TECH SVGA CARD

？=A 代表　GENOA SVGA CARD

(2) 其他参数

如果装入 GB4 之后，电脑死机或是无法呼叫出 GB4，您可试着使用下列参数：

.GB/I?：改变 GB4 所使用的中断位置，? 值为 1－9；

. GB/NI：不重设电脑的中断控制器，此一参数会使得 GB4 的拦截能力减弱，使得在某些 GAME 下无法叫出 GB4，若您的电脑使用了 EMM386. SYS 程序，GB4 也会自动执行此一参数。

＊［注 1］：如果您使用了 EMM386. SYS，GB4 将会自动启动/NI 的参数，此/NI 能数会使得 GB4 的拦截能力减弱，而造成在某些 GAME 之下无法呼叫出 GB4。为防此种情况发生，您应避免载入 EMM386. SYS ，或者改用 QEMM 及 386MAX 程序取代之。

＊［注 2］：如果您使用了 GB/NI 的参数，或使用了 EMM386. SYS (GB4 在这种情况下将会自动启动 /NI 的参数)，可能使得某些使用“声霸卡”语音合成功能的 GAME 死机。如果有这种情况发生，可将此游戏设定为使用“魔奇音效卡”发声，或者将 /NI 参数除去以及避免载入 EMM386. SYS (可以用 QEMM 或 386MAX 程序取代之)。

1.1.4 内存需求

GB4 会自动侦测电脑上是否有扩展内存 (EXTENTED MEMORY)，以便增大主内存的剩余空间。故有 1024K 或以上内存的 AT 及 386/486 机器应避免载入虚拟内存 VDISK 程序 或其它占用全部扩展内存的程序。您最好留 190K 左右的扩展内存给 GB4 使用，若您的扩展内存为 XMS 的规格 (如使用 DOS 5.0 的 HIMEM. SYS)，则 GB4 需要使用 250K 左右的扩展内存空间。

如果您的主机没有扩展内存或剩余空间不足，则 GB4 将占用 118K 左

右的主内存空间，从而使得某些需要大容量内存的游戏无法执行。为解决这个问题，GB4 提供了一个崭新的以硬盘空间来模拟扩展内存的程序 EXTDISK.EXE。您可在载入 GB 之前，先执行此程序，则您的 GB4 将只占用 11K 内存空间！

若您的扩展内存被其它程序占用，例如 DISK CACHE、SHADOW RAM，使得其剩余空间小于 GB4 的需求，而您又无法或不愿取消这些程序，您同样可以执行 EXTDISK.EXE 程序来让 GB4 正常运行。

* [注 1]：若您使用了 EXTDISK.EXE 程序，执行 GB.EXE 时请勿加 /? 的参数，以免导致程序不能正常执行。

* [注 2]：若您使用了 EXTDISK.EXE 程序，则游戏克星的 SAVE/LOAD GAME 功能不能保证可以正常执行。

* [注 3]：若您的电脑上扩展内存的规格为 XMS（例如用 DOS 5.0 或 HIMEM.SYS），但没有足够的剩余空间（250K 左右）给 GB4 使用，则游戏克星的 SAVE/LOAD GAME 功能未必可以正常执行。

1.1.5 程序载入顺序

一般来说驱动程序及一般常驻程序（例如鼠标的驱动程序或抓图程序）应先载入内存中，然后才载入 GB4。而供单色显示器使用的模拟 CGA 转换程序应在 GB4 之后才执行，但若是使用具有放大功能的 CGA 转换程序，则应在载入转换程序之后，以 GB/H 的方式执行 GB4。

1.1.6 程序相容性

若您使用了 EMM386.SYS（或是 EMM386.EXE），游戏克星会减低它的键盘拦截能力，会导致在一些游戏之下呼叫不出 GB4，或是使用跟踪功能时无法发生效力，且如果游戏程序也使用了 EMS 就可能会造成死机（例如 WIND COMMANDER Ⅰ），故您最好使用 QEMM 程序来取代 EMM386.SYS。

1.1.7 准备工作磁盘

当 GB4 使用低级分析功能及储存游戏进度时，需要用到额外的空白磁碟片。低级分析需使用 640K 的硬盘空间或两张 360K 磁盘；而储存单色、CGA、EGA、VGA 游戏则需使用 1.2M 的硬盘空间或三张 360K 磁盘。将低级分析需使用到的空白磁盘（已格式化）分别标上编号。例如将 360K 磁盘，作为工作盘，则需标上 WORKDISK 1 — 2，储存游戏则需标上 SAVE GAME DISK 1 — 3。

1.2 功能说明

在游戏进行中连续按二次[CTRL]键便可呼叫出 GB4 主菜单，此时可用

方向键或数字键选择项目，使用完毕后可用 [ESC]键跳出主菜单。主菜单如下：

```
0. Game Table
1. Address Analysis
2. List Address
3. Modify Memory
4. Trace
5. MouseKey
6. Other Options
7. Load/Save Game
```

1.2.1 GAME TABLE（地址记录表）

该菜单找出游戏中储存资料的地址之后，便可将您所选定的地址及其注解填入表内，以便以后使用。

例：

01－BALL	3000:6B5A	02
02－LEVEL	3000:6BC4	04
03	0000:0000	5B
04	0000:0000	5B

* [注 1]：按 [ALT]+<1>—<8> 便可将选定的地址及其注解填入表格中。

* [注 2]：按 <1>—<8> 则能把数值写入该项选定的地址位中。

* [注 3]：按 [SHIFT]+<1>—<8> 锁定该地址的内容，使得该地址的数值保持不变，再按一次便可解除锁定。

* [注 4]：[S] 键可将表格存入磁盘中；[L] 键则从磁盘上载入表格。

* [注 5]：在输入地址表格文件名时不必加扩展名.

* [注 6]：填入地址栏时，若键入"＊＋1"则为选定地址的下一个地址。

* [注 7]：填入地址栏时，若键入"＊－1"则为选定地址的上一个地址。

* [注 8]：若您欲使用上次所储存的记录表格，请使用与上次执行游戏时相同的 CONFIG. SYS 以及 AUTOEXEC. BAT 文件（或其它的常驻程序），这样游戏程序载入内存中的位置才会与上次相同，才能避免表格内的地址因变动而失效。

1.2.2 ADDRESS ANALYSIS（地址分析）

此菜单让使用者输入欲寻找地址的数值，以便让 GB4 跟据这些分析值来展开寻找的工作。在第一次选择这项功能时，屏幕上会询问您是要进行高级分析或低级分析"LEVEL (H/L)?"，若您要寻找的变数是可以确切得知的数值，如现存的球数、人数、关数等，您便可键入 [H]；也就是要选择高级分析；如果要寻找的数据是以图形方式来表示，而不知道其确切的数值（例如游戏中能源的长度、主角的体力等等），我们便可键入 [L]，也就是选择低级分析的工作方式。

当选择完分析方式之后，游戏克星便会问您："ANALYSIS VALUE 01:?"，也就是第一个分析的数值是多少，您就要输入当时游戏中您所要寻找的变数数值。若您所选择的是低级分析的工作方式，不能确定其具体数值，您可自行估计一个大约的数值代替。随着游戏的进行，您要输入几次分析值，这样一来，GB4 便可依照您所提供的数据，找到内存中变数的地址。

若您要重新分析新的数据，可在输入分析值的时候输入英文字母"X"，此时 BG4 的分析功能会重新回到初始状态，您便可以进行下一个变数的分析。

* [注 1]：游戏克星的输入系统为十六进制，故您所填入的数值范围应为 00－FF。若您要输入的数值为十进制，则数值的范围应为 0－255，并请在数值前加一"/"号，游戏克星便会自动将其转换为十六进制数值。

* [注 2]：低级分析的原则为：变数越大，则输入的分析值也要越大；变数越小，则输入的分析值也要越小；变数不变时，其间输入的分析值是一样的。

* [注 3]：低级分析的原则依据是分析值间的大小关系，而分析值间大小的比例则不予考虑。

1.2.3 LIST ADDRESS（列出符合分析条件的地址）

当您使用功能 [1] 输入三个以上的分析值之后，便可利用此功能列出您所要寻找的变数地址。如果所列出的地址太多时，表示使用者进行分析的次数不够，此时应再使用功能 [1]，多输入几个分析值，便可滤去许多不相干的地址。等到列出的地址减少到 4 个以下时，便会出现一个以亮度表示的光标，让使用者选定最有可能的地址，被选定的地址前会出现一个"＊"号，而在输入地址时便可用"＊"号来代替选定的地址。

例：

2000:31A9	02	01	01	00	03
2000:4529	02	01	00	00	04
3000:1928	02	01	01	00	03

1.2.4 MODIFY MEMORY（修改内存）

此功能可让您读出或修改目前内存的内容。

* [注 1]：按 [R] 键表示要读出内存的内容；

* [注 2]：按 [W] 键表示要修改内存的内容；

* [注 3]：选择完读取或是修改项目以后，便要输入内存地址。此时若您事先

在功能 [2] 中选定地址的话，会出现一个"＊"号，直接按 [ENTER] 便可输入；

* [注 4]：输入地址之后，您便可读取或填入数值。

* [注 5]：填入地址时若键入"＊＋1"，则为选定地址的下一个地址；

* [注 6]：填入地址时若键入"＊－1"，则为选定地址的上一个地址；

* [注 7]：游戏克星的输入系统为十六进制，故您所填入的数值范围应为 00－FF；

若您用十进制，则输入范围应为 0－255，并要在数值前面加一个“/”号，游戏克

星便会自动将其转换为十六进制数值。

1.2.5 TRACE（指令跟踪功能）

此功能可找出“改变某一内存地址内容”的指令，并加以除掉，以达成使此内存内容保持不变的目的。例如我们可以找出《打砖块》游戏程序中，负责把“球数减掉一个”的指令，然后除掉它，以后不论球掉下多少个，球数还是不变，甚至会不断增加！

举例来说，如果您已找到了“打砖块”游戏中球数的地址，便可使用此功能。首先进行指令追踪，然后键入球数的地址，按 [ESC] 跳出 GB4 后，便会发现游戏速度明显下降。此时故意让球掉下，只要球的个数一变动，GB4 便能找出减少球数的指令，将其显示在屏幕上，并询问是否加以除掉。若回答“YES”，则此减少球数的指令便被自动清除，以后游戏便天下无敌了。

＊ [注]：若您使用了 EMM386.SYS 或 EMM386.EXE，指令跟踪功能功能在某些游戏下可能无法生效（即跟踪时画面速度不会减慢），此时应避免载入 EMM386 或用 QEMM 取代之。

1.2.6 MOUSEKEY（鼠标模拟键盘）

此菜单功能让您用鼠标来代替键盘操纵游戏，并且可与键盘配合同时使用。进入此有此功能后，画面便会出现以下四个选项：

[1]：ENABLE MOUSEKEY [启动鼠标控制功能] ——— 选择此项按回车键，启动鼠标控制功能。

[2]：DISABLE MOUSEKEY [取消鼠标控制功能] ——— 选择此项按回车键，取消鼠标控制功能。

[3]：DEFINE MOUSE [定义鼠标控制功能] ——— 此项让您设定鼠标的移动方向和按钮分别要代表键盘上的哪一些按键。例如：游戏中控制主角动作的按键分别为：往上 [Q]，往下 [A]，往左 [O]，往右 [P]，发射 [SPACE]，跳跃 [ENTER]。您便可在按 [ENTER] 键进入鼠标定义表之后，依次序键入 [Q]、[A]、[O]、[P]、[SPACE] 及 [ENTER] 键即可完成设定。

[4]：PARAMETER [设定鼠标的特殊参数] ——— 此项目让您设定控制鼠标的一些参数，请用光标选择参数项目之后，用 [ENTER] 键及左右方向键来设定参数。

[A]：设定鼠标左边按钮为连发及其连发速率。

＊ [ENTER] 键：设定/取消 连发

＊ 左右方向键：设定连发速率

[B]：设定鼠标右边按钮为连发及其连发速率。

＊ [ENTER] 键：设定/取消 连发

＊ 左右方向键：设定连发速率

[C]:SENSITIVITY：设定鼠标灵敏度。

* 左右方向键:设定鼠标灵敏度,灵敏度的数值越小则鼠标越灵敏。

* 左右方向键:设定临界值

[D]:SUSTAIN LIMIT:设定鼠标的临界值。

* [说明]:在某些游戏中,主角一直往左或往右走,此时若您的鼠标也一直跟着移动,恐怕就要移出界了。现在只要您的鼠标持续往一个方向移动一段时间,便会自动设定为持续移动。也就是当停下鼠标之后,也还是往原来的方向移动,而这段时间便是持续移动的临界值。临界值越大,则鼠标要往同一方向移动较长的时间,才能够变成持续(自动)移动,临界值越小,则只要移动一下便等于一直移动了。

[E]:DIRECTION [移动方向] ——— 本功能可设定鼠标为八方向或四方向移动。若您设定为八方向,则当鼠标往右上方移动时,程序会同时送出往上及往右两个方向按键的讯号;若设定为四方向。则只会送出上、下、左、右键其中的一个讯号。一般来说设定为八个方向较为灵活,而当游戏中的主角本身无法往斜方向移动(如某些走方格子的 RPG),则设定为四方向较佳。

* [注 1]:连发的方式为按一次鼠标钮为开始连发,再按一次鼠标钮为关闭连发,而并非一直按着为连发。您可用《氚星异形 2》来试试连发的威力。

* [注 2]:有些游戏的方向键并非控制移动,例如往上是跳跃,往下是蹲下,此时您可把这些键设定在鼠标上,以免因鼠标左右移动时,产生往上或往下的偏移,而造成误判。

* [注 3]:使用鼠标时可配合键盘一起使用,例如鼠标负责移动,键盘负责发射或者跳跃。

* [注 4]:若游戏程序中也使用了鼠标来控制的话,请避免使用此功能,以免造成控制上的混乱。

* [注 5]:欲使用本功能,必须在游戏克星本身执行之前首先载入鼠标的驱动程序。

1.2.7 OTHER OPTIONS (其它功能选项)

进入此选项之后,便出现以下几个附属功能的选项:

(1). DEFINE KEYBOARD (重新定义键盘)——— 此功能可以让您重新设定游戏的控制键。例如原先游戏的发射是按 [SPACE] 键,而您欲将其改为使用 [ALT]键,则请在进入键盘定义表后,首先按 [ALT] 键,接着再按 [SPACE] 键,最后按 [ESC]键跳出即可。若您要清除原先的设定,只要在进入键盘定义表后,不设定任何按键,而直接按 [ESC] 键跳出即可。

* [注]:此功能应在游戏开始进行之后再使用。

(2). GAME SPEED (调整游戏的速度) ——— 此功能可加快或减慢游戏的进行速度。请把游标移至选项之后,以左右方向键来设定速度。

* [注 1]:由于有些游戏开始时会先设定速度,故此功能应在游戏进行中使用。

* [注 2]:加速功能可能在某些游戏中无法生效,如有此情形发生的话,请把速度调回"00",再进行游戏。

(3). MAGIC WINDOW (电视墙)——— 此功能可以使您的电脑屏幕有如电视墙的特技效果。请把游标移至此选项后,按 [ENTER] 键便可启动电视墙效果,再按一次 [ENTER] 键便可解除电视墙效果。在您设定电视墙后,可以用左右方向键来设定三种电视墙的显视模式:

. MODE1:四个分割画面

. MODE2:左右两个分割画面

. MODE3:上下两个分割画面

* [注 1]:您必须有 VGA 卡才能使用此功能。若您使用的是标准 VGA 卡,您可以调用 EGA 显示模式之下的电视墙功能;若您拥有 SUPER VGA 卡,则能使用电视墙的全部功能。

* [注 2]:有些使用了 VGA 特殊模式的游戏,只能有 MODE 3 的效果。

(4). QUIT TO DOS (跳回 DOS) ——— 把光标移至此选项之下,按回车键两次,便可不必重新开机而跳回 DOS,令您可随意操纵您的电脑。

* [注 3]:如果游戏中使用了"声音卡"的语音合成功能,请使用游戏程序所提供的正常退出方式,以免下一个也使用"声音卡"游戏的语音合成功能的失效

1.2.8 SAVE/LOAD GAME (储存/载入游戏)

由于有些游戏内容太长,不是短时间内能够完成;或是难度太高,经常有"一失足成千古恨"的情形发生,在紧要关头时,便可利用此一功能将游戏进度储存在磁盘上,等到不小心阵亡或下次重新开机时,再载回您所储存的游戏进度,而不必从头开始。

* [注 1]:在输入游戏进度文件名时,不必输入扩展名。

* [注 2]:如欲载回先前所储存的游戏进度时,请维持与先前储存游戏时相同的开机程序,即相同的 CONFIG. SYS、AUTOEXEC. BAT 文件,以维持游戏克星在内存中的位置与上次存档时相同,以免出现"ALLOC ATIONERROR"的错误讯息,而无法顺利载入游戏进度。

* [注 3]:重新开机之后,若在 DOS 状态下载入上次的游戏记录,可能使您的音效卡无法发出声音,此时您应以正常的方式执行此游戏程序,等到游戏开始了,也就是游戏程序已经设定完音效卡的参数后,您再叫出游戏克星,并载入上次的游戏记录。

* [注 4]:由于游戏记录文件并没有储存扩充内存(EMS)的资料,故重新开机后,如欲载入使用了 EMS 的游戏程序的进度档案,请以正常方式执行此游戏程序,等到游戏开始后,也就是游戏程序将 EMS 填入原有的资料后,您再呼叫出游戏克星 4,并载入上次的游戏记录,这样才能保证游戏能接着上一次的进度继续运行。

* [注 5]:若您使用的是 EGA 图形卡,应以正常的方式执行此游戏程序,等到游戏开始后,也就是游戏程序已经设定完 EGA 画面的颜色之后,您再呼叫出游戏克星,并载入上次的游戏记录。

* [注 6]:使用者在执行过 COMPRESS DISK 等改变文件在游戏上的位置的程序后,请勿再使用先前所储存的游戏进度。

* [注 7]:若您使用了"EXTDISK.EXE"程序,GB4 的 SAVE/LOAD GAME 功能不能保证可以正常执行。

* [注 8]:若您的扩展内存为 XMS 规格,(如使用 DOS 5.0 或 HIMEM.SYS),但没有足够的剩余空间 (250KB 左右) 给 GB4 使用,则 GB4 中的 LOAD/SAVEGAME 未必能正常使用。

* [注 9]:注意:若使用了"STACKER"软件压缩您的硬盘,则 LOAD/SAVEGAME 功能无法正常使用。

1.3 无敌拷贝功能

GB4 可以说是目前世界上最为强劲的万能拷贝工具,任何加密方式对它来说,都不放在眼下!以前有一套叫"GB3"的游戏工具箱及一套叫"RCOPY 02"的工具系统,也有类似的拷贝功能。但"GB3"占用系统内存太大(78K);然而"RCOPY 02"最多只支持 EGA 640 * 400 的显示器,而绝大多数新推出的游戏都只支持 VGA256 色显示器,且需要大容量的系统内存空间(有的甚至需要使用到 EMS),故以上两种工具系统对新游戏都无能为力了!

但最新推出的 GB4 则克服了以上所有的缺点,支持所有的显示模式,而最厉害的是:虽然 GB4 拥有这么多强劲的功能,但只占用系统内存 11K 的空间!这样一来,以上所有的问题都迎刃而解了。如果您的电脑使用 DOS5.0 操作系统,并且使用了 Device HIMEM.SYSB,则系统内存空间可达 637KB。就算运行了 GB4,还有 626KB 的系统内存,连运行条件最苛刻的"鹰式战机 3.0"(需用到 618KB 系统内存)都可顺利执行。

无敌拷贝制作方法如下:

以"街头霸王 I"为例,在运行前须在 A 驱插入"KeyDisk",程序在运行时会自动检测 A 盘上的加密指纹,当一切正常时才继续往下执行,否则将会自动退出游戏程序,回到 DOS 状态。以下就是利用 GB4 来制作"街头霸王 I"的拷贝副本:

(1) 启动电脑;

(2) 运行 GB4;

(3) 运行"街头霸王 I";当通过密码检测,去到游戏主菜单时,把游戏克星 4 呼叫出来;

(4) 选择 GB4 的第七项储存/载入游戏功能,按"S",跟着输入文件名(任意),然后按回车键,即自动生成通过密码检测的"街霸 I"工作副本,接着就可以把该副本录到磁盘上保存起来。这样,您就拥有一套全解密且不需钥匙盘的"街霸 II"了!

(5) 如果以后想玩游戏,则只需进入 GB4,选择第七项,按"L",输入文件名(必须是"街霸 II"副本的文件名)后按回车,就可去到"街霸 II"主菜单,继续玩游戏了。

1.4 控制键说明

游戏克星热键：游戏进行中按键盘左下方的［CTRL］键两次，便可呼叫出游戏克星的主菜单，按［ESC］键便可跳出游戏克星回到游戏中。

以下的控制键均在GB4的主菜单下使用：

＊［CTRL］－［P］切换显示页 ——— 如果使用者呼叫出GB4后，却看不到游戏克星4主菜单的画面时，请连续按此切换键，直至GB4主菜单出现。如要跳出GB4，请再次使用此功能，切换回原先所显示的游戏画面，并按下［ESC］跳回游戏中。

＊［CTRL］－［S］显示完整画面 ——— 此功能可配合抓图程序使用，当按下［CTRL－［S］后GB4会把主菜单隐藏起来，此时屏幕上所出现的是完整的游戏画面，便可将屏幕的图形用先前驻留的抓图程序抓下来，完成后再按［ESC］键回到主目录。

＊［注］：抓图程序须在游戏克星程序之前预先载入。

＊［CTRL］－［H］改变GB4召唤键 ——— 由于游戏克星是以连续两次［CTRL］呼叫出来的，有些游戏也使用了［CTRL］键，为了避免冲突，此功能可将召唤键由［CTRL］改成［TAB］键。下次欲叫出游戏克星，便应改按［TAB］两次。

＊［CTRL］－［Q］回到DOS ——— 如想中途跳出游戏时，按［CTRL］－［Q］便可结束游戏，回到DOS状态下。

＊将按键固定 ——— 如果游戏中的某些按键要一直按住，例如“太空小蜜蜂－92”的发射键［SHIFT键］，或者是其它射击游戏中的射击键，您可以让GB4代替您一直按住这些键。

具体做法如下：

按住您所要固定的按键并连按［CTRL］键两次，呼叫出GB4，等主菜单出现之后再放开这个键，接着退回游戏状态。如此一来，游戏程序便认为这个按键被一直按住了。如果您想解除这项功能的话，只要在游戏中再按一次这个键便可。

1.5 在GB4中使用QEMM6.0

若您使用了QEMM6.0版，请注意下列事项：

1.在执行游戏克星的硬盘安装及反安装过程之前，您的QEMM参数行中若有ST:M或ST:F的参数，请先加以去除。

2.欲顺利执行游戏克星，请调整您QEMM参数行列：

(1)若您的参数行中有ST:M，请在其后再加上XST=F000。(或改用ST:F)

(2)若您的参数行中有ST:M，则游戏克星无法判断您使用的SVGA卡，故请在执行游戏克星时加上/V=？的参数，？的数值请看前面介绍。

(3)经过上列的参数修正，使用游戏克星还是有死机的情形的话，请将QEMM参数行中的ST:M及ST:F去除。

1.6 GB4 的锦囊妙计

除了前面介绍的 GB4 的充当死机克星、保存现场、为软件添加鼠标器等基本功能外，它还有许多的用处。下面是笔者在实践过程中摸索出的几条 GB4 使用技巧。

1.6.1 简化地址分析

GB4 在分析游戏地址时，至少要输入分析值三次以上。

实际上，在作准确分析(或称为高级分析－High Anaylysis)时，只要输入一至二个值即可找到，这时，后一次或后二次不需要等数值发生变化就可再次分析。

1.6.2 修改物品表

在很多游戏中，主角都有一张长长的物品表。GB4 可以把物品改出来，当然还得看游戏程序设计中的物品存储方式是不是链表形式。

例如，《武状元－黄飞鸿》有两个表，一个武功表，另一个是物品表。这两个表的修改方法是一样的，若修改武功表的话，先拿佛山无影脚分析。佛山无影脚后面跟着数值 40，表示可使用 40 次佛山无影脚。用第一个技巧，找出次数 40 的地址，把该地址减 2 就是武功代号的地址，其内容应该是 04(即佛山无影脚大代号是 04)。若用不同的值填入新地址，就会有不同的功夫出现，是不是很简单？有耐心的话，从 00 填到 FF(实际上用不了那么长，因为没有那么多的物品，大约到 55 就可整理出全部代号)，整理一下就能得到代码表。有了代码表，您还可以试试修改存储文件，道理是一样的。

这张表在内存里的格式是按功夫代号(2 字节)、可用次数(2 字节)、分隔符 00 00(2 字节) 重复构成的，那么地址加 6、加 12....就分别修改下一表项。注意，若物品没有实时变化，只须退出物品功能再重新进入，让游戏程序重读数据即可。还有，通常 0 代表没有物品。

1.6.3 还是修改物品表

也许您会问，那么那些没有量值的游戏怎么办呢？没有问题。

拿《失落的维克战士》开刀。任选一人先拣一个随便什么物品，调出 GB4 分析，选模糊分析，输入 1，然后把东西给别人再次调出 GB4，输入 0，重复这个过程直到找到一个地址。由于每样物品只能使用一次，因此只有物品代码地址，而没有使用次数地址。由 GB4 得到的地址就是物品代码地址，修改地址内容，就能得到不同的物品。若该地址被 GB4 锁定，就会有使不完的物品。游戏共有 3 人，每个人限带 4 样物品，每样物品按双字节变量存放，故此链表共 24 字节。如此便轻易得到了所有开门钥匙和食物。修改其他类似的游戏，只要使主角的物品不断地发生变化即可。

很多游戏都可以按方法 2 和方法 3 修改。要考虑的问题是，存不存在链表、链表代码的位数(如功夫的代码是 1 字节还是 2 字节)，是否有间隔符，最重要的是随时查看修改的结果。

1.6.4 使用任务切换

GB4 本身没有任务切换功能，不过我们可以利用 GB4 的游戏进度存储、载入功能实现一些简单的任务切换。即当实现任务切换时，先用 GB4 保护现场，然后用 GB4 退回到 DOS，执行其他程序任务，只要您需要，可以保存无数个进度，需要时用 GB4 取回。不过值得注意的是，有些程序会用到 640KB 以上的内存，这时要先执行该程序，恢复其数据区，然后才能用 GB4 取回进度。

> 注意：该方法不是对所有游戏有效。

1.6.5 实现老板屏幕

在某些特殊场合下，需要暂时关闭屏幕，GB4 没有提供老板屏幕功能，容易使玩家身陷囹圄。若使用其他攻关工具作老板屏幕，则容易被行家识破，而这些攻关工具提供的老板屏幕，都是单一不能活动的屏幕。由于缺乏可操作性，时间一长不免露出马脚。下面介绍一个方法，配合 PCTOOLS，可使玩家暂保性命。

1. 先驻留 PCTOOLS

在 DOS 提示符下键入如下命令：

PCTOOLS /R/F9

其中参数 R 表示使 PCTOOLS 驻留内存，参数 F9 表示使用 CTRL+F9 作为 PCTOOLS 激活的热键，您可以用其他功能键来代替 F9，范围是 F1—F10。省略该参数则激活的热键为 CTRL+ESC。

2. 驻留 GB4。

3. 使用时，先激活 GB4，再激活 PCTOOLS，即可进行各种 DOS 操作，好象什么事情都没有发生，使操作者不至于无事可做而令人怀疑。退出时顺序退出 PCTOOLS 和 GB4，就能回到游戏画面，继续玩游戏。

注意：您可不用 PCTOOLS，而用任何能用热键激活的 TSR 程序。

1.6.6 修改内存

由于游戏的一些相关数据较为集中，比如存放金钱、体力、法术等数据的地址不会相距很远，我们可通过 GB4 的“Modify Memory”(修改内存)选项，查看所选地址附近的地址，改改试试，十有八九可以如愿。这可以帮助我们加快数据的修改而不用老作分析，此外，对等级之类变化周期长的数据的修改也变得十分快捷。

以《妖魔道》为例。先分析李大侠的“负担”值(买一样物品此值就会变

化)，内存地址是 2000：A4F4，再在附近寻找，就不难发现攻击力的地址 2000：A4F7，接下来就是防御力的地址 2000:A4F9，依次类推，生命、等级以及法力的地址都可以找到了。

另外，在输入数据出现“＊”后，可以用＊＋n(n 为数字)来查看所选地址的前 n 个地址或用＊－n(n 为数字) 查看后 n 和地址，有时修改其后一个地址的数值可使想要增加的数值成倍增长。

仍以《妖魔道》为例。将 2000：A4F4 的地址的内容改为 FF，这时“负担”的数字将变为 255，那么 2000:A4F4 的下一个地址是多少？是 2000：A4F5，再将它的数值改为 FF，若它和前一个地址表示的是同一个数据，则刚才的数值又会改变，FFFF 算算会是多少？是 65535！再察看“负担”的数值，真的变成了 65535。

现在大部分游戏的数据都由两个双字节组成(如上例中的攻击力、法力、生命等数值也是如此)，有的数据甚至由三个或更多的双字节组成。若一个数据的三个双字节全变成 FF，则就变成了 16777215 了！

1.6.7 跟踪地址数制自动转换

GB4 在跟踪地址时，要求输入 16 进制数，而且不能大于 FFH。您只要在输入数字之前打个“/”再输入 10 进制数(可大于 FFH)，按回车键后，10 进制数便会自动转换为 16 进制数(取低位)。

1.6.8 跟踪数据地址妙法

当您跟踪到数据地址后，在 Game Table 中用 ALT＋(编号)登记完后，若想此数字不再变化，只要按 SHIFT＋(编号)，这时对应的编号将变为高亮度，表示成功，退回游戏，这时 GB4 将在后台不停将数字改回原值，如此便不用使用拖慢速度而且不安全的 Trace 功能了。

1.7 GB4 实例技巧分析

1.7.1 利用 GB4 修改“生命值”

1. 安装 GB4。

2. 运行游戏。

3. 当屏幕显示出“生命值”时，连续按第二次 CTRL 键后激活 GB4。选择功能[1]进行地址分析，这时屏幕提示“Level(H/L)?”。若您要找的是可确切得知的数值，请选择“H”，即高级分析。若要寻找的数据是以图形方式显示的，不知道其确切值，请选择“L”，即低级分析。

选择完分析方式后，屏幕显示“Analysis Value 01：”，要求您输入要寻找的“生命值”的数值。若是选择低级分析，不能确定其具体数值，则可自动地估计一个大约数值代替。GB4 便可依照您所提供的数据，找到内存中的“生

命值”的地址。

若需要重新分析新的数据，可在输入分析值时输入英文字母“X”，这时分析功能重新回到初始状态，您就可进行下一个“生命值”的分析。

4. 使用“地址分析”功能分析三次以上后，可用“List Addrsss”查看所要寻找的“生命值”地址。若所列地址太多，应使用功能[1]继续分析。等到列出的地址少于4个以下时，便会出现一个高亮度标条，您可选定最有可能的地址，被选定的地址前会出现一个“*”号，而在输入地址时便可用“*”还来代替选定的地址。

5. 找到“生命值”地址后，使用功能[0]将所选的地址及其注释填入地址表，若要使该地址的数值保持不变，则按[Shift]+[1]-[8]锁定该地址的内容。另外还可将地址表保存在磁盘上，下次游戏时再调入。

6. 找到正确的“生命值”后，使用功能[4]可找到改变“生命值”的指令，并加以修改，使此“生命值”保持不变，若修改达到了目的，则可修改原执行程序。您可使用UNP将原程序还原，再用PCTOOLS等工具进行修改。

7. 若游戏内容太多，不能够在短时间内完成，或是难度太高，经常有“一失足成千古恨”的情况发生，而游戏本身又没有进度存储功能，则在紧急关头，就可利用功能[7]将进度保存在磁盘上，等到下次游戏时再装入所存的进度。

1.7.2 用GB4攻克F117战斗机

F117战斗机最大难点在于在飞机中稍有闪失，便会机毁人亡，前功尽弃，先前的记录全部作废，只能从头再来。因此，想升到最高军衔直到爆机绝非易事。但是利用GB4就可使读者在玩该游戏时死而复生，步步高升、战功卓著。

首先介绍F117主要操作：“+”加油门，“-”减油门，SHIFT+“+”最大油门，SHIFT+“-”关闭发动机。“1”放锈导火球，“2”放铝泊，“3”红外干扰，“4”电磁干扰，“5”放假目标，“6”收起起落架，“7”自动导航，“8”开关舱门，“9”收起升降翼，ENTER发射导弹，SPACE选武器，BACKSPACE开炮。

其中假目标可以防一切武器，但只有3个。另外导弹、炸弹也有限！用GB4可将它们修改到无穷。具体作法如下：

1. 先使GB4驻留内存。

2. 然后运行F117。

3. 进入游戏后，先建立一个新成员，起飞后，连续按两下CTRL键呼出GB主菜单，选择Address analysus(地址分析)，选H(高级分析)，分析有确定值的量，L为低级分析，分析无确定值的量。输入/18(当前锈导火球数)，注意：GB4将输入量认为是16进制数，输入10进制数以“/”开头，GB4可自动转换，之后，每放一次火球，输入一次，三次之后，就可以选择Address List(地址表)，一般此时只有一个地址，回车地址前出现“*”，今后就可以用“*”代替它。

4. 选择Trace(跟踪)，输入*，退出菜单。此时游戏变慢，再按“1”放火球，GB4马上弹出一个菜单，列出此时要修改*地址的操作码，用“自动修改”使

其变为空操作(90H),此后火球数就不会减少了。

5. *存储着火球数，*－4,*－2 分别存放假目标数和铝泊数,*＋2 存第一种武器，*＋4 存第二种武器等,但只需跟踪修改*和*＋2 地址,就可使以上所有物品均变为无穷。

另外，可以使用低级分析分析油量,但较繁杂,不如开始就带一个附加油箱,反正所有武器都变为无穷。降落较难,可使用 GB4 的"Save/Load"存盘。

1.8 利用 GB4 实现 UCDOS 5.0 的备份

UCDOS 5.0 正式版是通过在并行口挂上软件狗才能安装。一旦软件狗出现问题，就无法安装。为了您安装和使用的方法,我们发现,可使用 GAMEB USTER 软件正常备份 UCDOS 5.0 系统，在安装时不需要软件狗。下面我们就来介绍这种方法。

1.8.1 GAME BUSTER 的加载

在 MS DOS 提示符下运行 GB4.EXE 命令,则出现下面的屏幕信息。

```
GAME BUSTER4
DESIGNED & PROGRAMMED BY NEIL HO
PRESENTED BY KINGFORMATION INC.
COPYRIGHT (C) 1988,89,90,91,92

Base memory used : 11 K
Ext. memory used : 250 K
Graphic adaptor : Tseng 3000 SVGA

386 memory control program exists,
trace speed will be slow.

EMM386 detected.
Hotkey intercept ability low.
```

该屏幕信息表明 GB4 已经加载到内存中，使用了 11KB 的常规内存和 250KB 的扩展内存。

您直接按左 CTRL 键两次就可呼出 GB4。

1.8.2 存储 UCDOS 5.0 的安装环境

在 MS DOS 提示符下键入 INSTALL 命令,出现图 1－1 所示的屏幕。

图 1－1

该屏幕的出现说明软件狗已经读过了。UCDOS 5.0 的安装程序只在 INSTALL 程序运行的开始读一次，以后就不再需要读了。此时，我们就可利用 GB4 将读后的微机环境保存在文件中，以后需要再安装 UCDOS 5.0 时直接装载该环境，就可不需要软件狗了。

按左 CTRL 键两次，则出现图 1－2 所示的屏幕。

图 1－2

在图 1－2 中，我们选择“7. LOAD/SAVE GAME”菜单，则出现图 1－3 所示的画面。

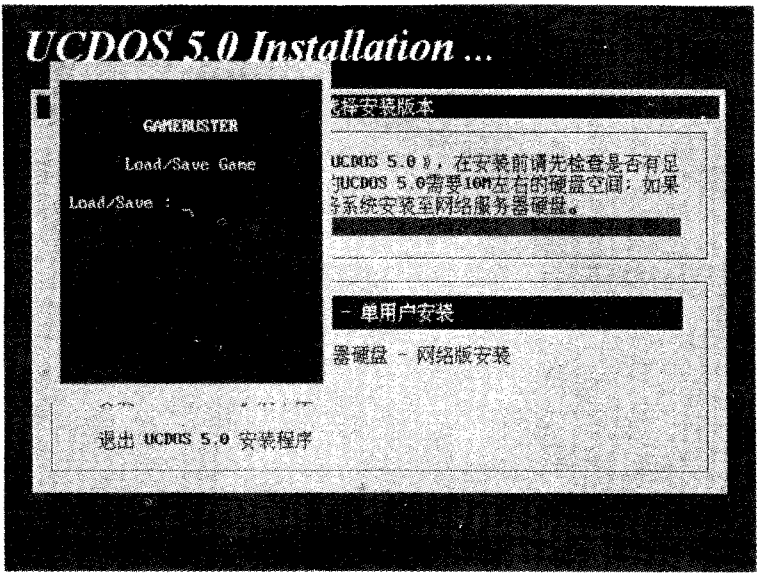


图 1－3

在该屏幕中我们选择“SAVE”，则出现图 1－4 所示的屏幕。

图 1－4

您可在输入存储微机环境的文件名字。例如，我们可输入“UCDOS50”。若出现图 1－5 所示的信息“PRESS ANY KEY”，则说明保存环境信息是成功的。

图 1－5

我们通过上面的系列步骤就将 UCDOS 5.0 读过软件狗的微机环境保存在文件中。

微机的环境信息系列文件及文件长度参见下表 1－1。

表 1－1：微机环境信息文件信息表

文件名	文件长度(单位：字节)
UCDOS50. SG0	2048
UCDOS50. SG1	27984
UCDOS50. SGH	65536
UCDOS50. SG2	288144
UCDOS50. SG3	262144
UCDOS50. SG4	315392
GB4. EXE	34128
(合计)	995376

您可以上表中的所有文件拷贝到一张 1.2MB 的软盘中，然后，再编制如下的批处理文件 SETUP. BAT。

```
@ECHO OFF
ECHO UCDOS 5.0 Installation Decryled!!!
GB4 > nul
echo You Press left CTRL Key twice to enter GB4!!!
@echo on
```

1.8.3 利用保存微机环境安装 UCDOS 5.0

在本段中，我们利用在 2.2 中保存的微机环境信息来安装 UCDOS 5.0 系统。

执行 SETUP 程序，然后，按左 CTRL 键两次就可呼出 GB4，参见下图 1—6。

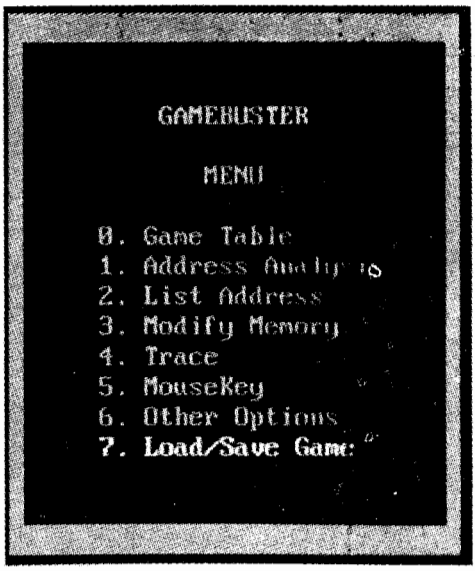


图 1—6

在图 1—6 中选择 7，则出现图 1—7 的画面。

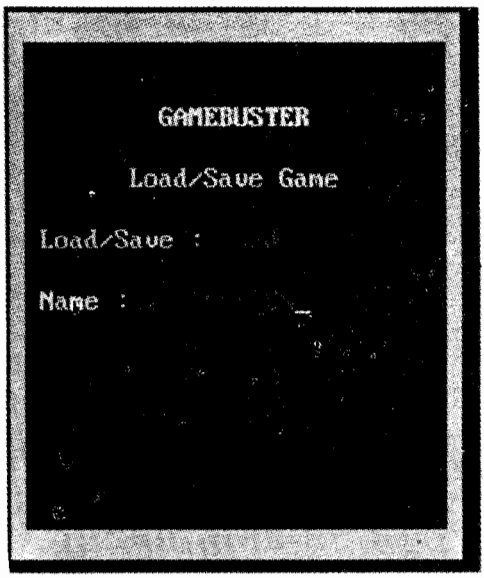


图 1—7

在图 1—7 中按“L”键，则输入装载微机环境的文件名 UCDOS50。如图 1—8。

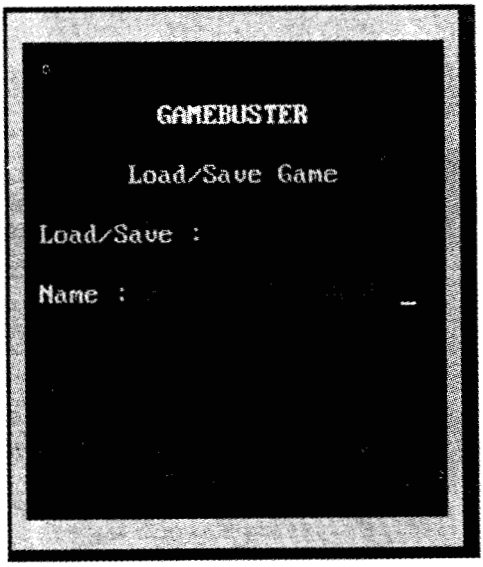


图 1－8

此时，屏幕上出现了 UCDOS 5.0 的安装程序的画面。参见下图 1－9。

图 1－9

在图 1－9 中，出现“PRESS ANY KEY”提示信息，则说明微机环境装载成功。

若在出现图 1－10 所示的屏幕，并出现“ALLOCATION ERROR”的提示信息，则说明微机环境没有正确地装载。

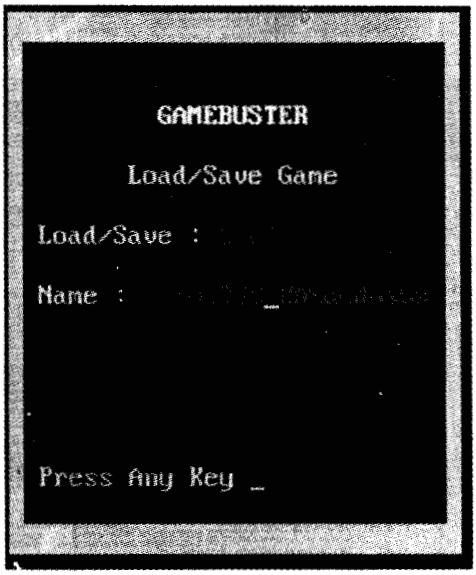


图 1－10

这有以下几个方面的原因：

· 您将本机备份的微机环境文件拿到其它微机上使用。

因为这两台微机的环境信息不完全一样，将导致该错误信息的出现。

· 该微机中有压缩盘程序驻留内存。

若您使用了压缩盘驱动程序 DBLSPACE. SYS 或 DRVSPACE. SYS，则可能会出现这样的信息。

为了解决这个问题，您可暂时将压缩盘驱动程序从微机中卸掉。您可用 PCTOOLS 工具将启动盘中的 DBLSPACE. INI 文件换名（例如，可换为 DBLSPACE Ⅱ 等），这样就可将压缩盘驱动程序从内存中卸掉。

在图 1－9 中按任意键，则出现图 1－11 所示的画面。

图 1－11

在图 1－11 中，按 ESC 键，则出现 1－12 所示的安装程序的屏幕。

图 1－12

此时，您就可正常安装 UCDOS 5.0 系统，而不再需要软件狗了。

1.9 GB4 比 GB3 之改进之处

我们在附录 A 中介绍了 GB2、GB3 的特点及其使用方法。那么，GB4 比 GB3 或 GB2 有哪些过人之处呢？

1. 大幅度地减少常规内存的量。若您拥有有足够的扩展内存或是硬盘空间，则 GB4 只占用常规内存 11KB，

2. 增加锁定地址的功能，可以向选定的地址不断地填入指定的数值。

3. 提供了以鼠标器模拟键盘的功能。

4. 提供了重新定义控制键的功能。

5. 提供了具有特技效果的电视墙功能。

6. 与抓图程序配合使用时，自动修正使用特殊 VGA 模式的游戏画面，使得抓下来的图不会错乱(如《红公爵》、《喷射战斗机 I 》等)。

7. 与游戏程序的兼容性极高。

1.10 使用 GB4 常见问题及解答

问 1：为什么当执行 GB4 时，GB4 要吃掉一百多 KB 的系统内存，不是说只占用 11KB 吗？

答：主板一定没有扩展内存(Extented Memory)，或者早就已经将它挪作它用了(象某些速度异常的 AT 主板，就将其用作影子内存(SHADOW RAM))。

这时只好运行 GB4 所带的 EXTDISK 程序，使用您的硬盘空间来模拟 Extended Memory 了。

问 2：确定主板上拥有 1MB 内存，而且后面的 384KB 也就是 Extenede Memory(扩展内存)，为什么执行 GB4 时仍需要吃掉一百多 KB 的内存？

答：请检查一下是否在 CONFIG. SYS 中指定了 RAMDRIVE. SYS(或 VDISK. SYS) 或者 SMARTDRV，这两种 SYS 程序将会把您的 384KB 当作磁盘来使用，因此，GB4 当然没有办法和它们来抢了。

问 3：在使用低级分析时，老是有"DISK FULL"的问题出现？

答：低级地址原本就比较难找的。若是给的数据有太多相同的数值，则就会造成"DISK FULL"问题。

问 4：已经找到了地址，也已经修改，可是为什么没有效果？

答：效果？试一下死掉一只看看。若有效可以看到画面上的只数不会改变。若是改变了，那就表示找错了。

问 5：使用了指令跟踪的功能，可是游戏的速度变得很慢，是不是有问题？

答：在指令跟踪的过程中，游戏速度变得很慢是很正常的事情。

问 6：为什么启动了"电视墙"，结果画面只能选择"MODE 3"，这是什么原因？

答：某些游戏软件使用了特殊显示模式，因此在启动"电视墙"时并没有出现预期效果，因为 GB4 的"电视墙"功能只支持标准的 VGA 320X200。若不是用标准的显示模式可能会有问题。

问 7：使用了鼠标器模拟键盘的功能，但是为什么一点效果都没有？

答：首先要执行鼠标器驱动程序，GB4 的模拟程序是要配合鼠标驱动程序才能使用的。

问 8：使用了键盘自定义的功能，结果不但新定义的键不能使用，甚至原来的键都不能使用了，这是为什么？

答：使用了键盘自定义功能只能对付使用 ASCII CODE 的程序，若是这个程序是用自己的键盘扫描程序(象《破坏神传说》)，那就没有办法了。

第二章 游戏巫师 Game Wizard PRO 2.30

Game Wizard Pro 是由意大利 Enchanced Software Design 公司研制的游戏工具。在许多地方比 GB4 有过人之处。

本章将介绍这一游戏工具，并给出应用实例。

2.1 系统要求与文件

2.1.1 系统要求

要运行 Game Wizard Pro(下称 GW)需要如下硬件和软件环境。

- 80286 或更好的处理器
- DOS3.1 或更高的版本
- VGA 图形卡
- 100%IBM 兼容机器
- 硬盘

2.1.2 GW 文件

完整的 GW 需要如下文件：

gw.bos	Game Wizard Pro 的老板(BOSS)屏幕
gw.exe	Game Wizard Pro 主执行文件
gw.ov1	Game Wizard Pro 辅助文件
gw.ov2	Game Wizard Pro 辅助文件
gw.ov3	Game Wizard Pro 辅助文件
gw.sch	Game Wizard Pro 屏幕保护文件
gwtutor.exe	Game Wizard Pro 使用的演示执行文件
gwtutor.ov1	Game Wizard Pro 使用的演示辅助文件

2.2 使用说明

2.2.1 GW 的启动与驻留

在 DOS 提示符下键入 GW，则首先出现有关系统信息屏幕，如下显示：

Game Wizard Pro V2.30b Copyright (C) 1994 by Ray Hsu & Genald Ryckman

General Information	
Main Processor Type:	80486
Math Co-Processor Type:	Present
Video Adapter Type:	VGA(VESA not present)
Mouse Type:	None
Sound Card Type:	PC Speaker or other

System Memory Available
Conventional Memory: 614K Expanded Memory: None Extended Memory: 6900K

Game Wizard Pro Information
Swap Memory To: XMS Video Swapping Speed: Fast Screen Blanking Time: 3 Min

上面的屏幕显示了如下内容：

· 微机一般信息(General Information)，如微处理器、数学协处理器、显示适配器、鼠标器类型、声音卡类型等。

· 系统可用内存(System Memory Available)，如常规内存、扩充内存和扩展内存剩余情况。

· GW 信息(Game Wizard Pro Information)，如交换内存、显示交换速度、屏幕保护时间等。

此时，按任意键或者过 3 分钟(由 Screen Blanking Time 决定)该屏幕消失，出现如下的提示信息：

Press ' key (the key to the left of 1 & above Tab) to activate Game Wizard Pro.

即驻留 Game Wizard 内存，且可按[']键激活 Game Wizard，执行 GWTWTOR.EXE 可演示 GW 的使用(GWTUTOR 的使用方法在下面介绍)。

2.2.2 GW 的使用

在任何时刻您都可以按"'"键激活 GW，下面为 GW 激活的屏幕。

Game Wizard Pro V2.30b Copyright (C) 1994 by Ray Hsu & Genald Ryckman

Game Wizard Pro.
Main Menu

Memory Address Search
Result of Memory Address
Table of Memory Location
Edit Memory Contents
File View(Display Text File)
Game Playing Speed
Protect Screen(Screen Blanker)
BOSS Screen With Password Option
View Current Program Screen
Load Previous Saved Program From Disk
Save Current Program to Disk
Crash Back to DOS(Exit the Current Program)
DOS Shell

ESC to Quit　　Registered to:Game Star

下面详细介绍上述屏幕的主菜单各项。

1. Memory Address Search(内存地址查找)

该选项用于查找游戏中的"生命值"、"金钱数"等项目。有三种方式：基

本(Basic)、中级(Intermediate)和高级(Advanced)。中高级选项只能在注册版本使用。

选择该选项后,输入你要查找的数值然后按回车开始查找。

(1) 功能键

Ctrl+E 结束当前查找开始一个新的查找。

Ctrl+P 用于重新输入上次查找的值,但不能递归。当上次输入值有误时可使用该功能。

(2) 查找方法

① 基本方式

基本方式用于查找确切知道的值,如钱、子弹等。

当找到的地址个数为 8 个或更少时,它自动转到"Result of Memory Search"屏幕并等待你作决定。

在查找一项目时,Game Wizard 还将查找比你输入值小 1 的值。这是由于有时存放在内存中的值比显示的值小 1。一些游戏开发者经常用这种方法存放数据。

② 中高级方式

用于查找模糊值,如能量条等。有时编程人员有意用非传统方式存放数据。用中高级方式还能确定这些数据的类型。

2. Result of Memory Address Searth(内存地址查找结果)

使用"内存地址查找"功能找到可能的地址后必须选择该功能确定正确的地址。当使用基本方式查找时,通常只有几个地址找到。不过,当使用中高级方式查找时往往有更多可能地址。

该功能允许你查看最多 100 个内存地址。用光标条选择一个最有可能的地址后,按回车键,则该地址可在"Table of Memory Locations"和"Edit MemoryContents"功能中使用。

有时可能有多个地址满足查找要求。这时,只能一个一个地尝试。

3. Table of Memory Locations(内存地址表)

选择可能的地址后,应将该地址放入内存地址表中。在内存地址表中建一项目后,该地址的值就可修改或锁定。每个项目由四列组成:Freeze(锁定列)显示该项是否被锁;Description(说明列),用于标识项目;Address(地址列)即项目的地址;Value(值列)显示当前值。

注意:地址以十六进制显示而值以十进制格式显示。

有如下按键:

- O 编辑表中项目的值
- C 从表中清除一项目
- E 建立或修改一项目。进入编辑方式后,可用下列命令:

TAB 得到下一列

CTrl+S 输入项目地址(仅当地址非 0000:0000 时需要)。

Enter 保存修改后的数据

ESC 放弃全部修改

· F　锁定/解锁某一指定项目。锁定某一内存地址后，该地址的内容不会被修改。被锁定时，该项目高亮度白色，并且在 Freeze 列的括号内显示一个点。

Ctrl+L　装入以前保存的地址表。只能在运行游戏时装入地址表。装入地址表后，Game Wizard 自动根据游戏的 PSP 值调整地址。如果地址超出游戏的范围，则该地址表不起作用。

Ctrl+S　将地址表保存到磁盘。只能在运行游戏时保存地址表，否则在装入时可能不起作用。当保存地址表时，要求输入文件名和简要说明。

ESC　回到主菜单。

4. Edit Memory Contents(编辑内存的内容)

该选项用于修改选择的一片内存区域。当有大量数据需要修改时特别有用。它还可用于确定和修改游戏中的名字、说明、模式等等。

(1)　按键

E　编辑当前屏幕上显示的内存数据。一旦在编辑方式，可用下列命令：

TAB　十六进制和 ASCII 码之间切换。

Ctrl+S　保存修改后的数据。

ESC　退出编辑方式。

G　将光标直接移至指定地址。

H　转化十六进制到十进制或十进制到十六进制。进入转换器后，可用下列命令：

TAB　十六制/十进制输入项切换

ENTER　转换输入的数据

ESC　退出转换器

N　重复上一次查找

S　从当前位置开始查找十六进制或 ASCII 串。在查找时，可用下列命令：

TAB　十六进制和 ASCII 之间切换

Ctrl+S　大小写敏感切换。当显示点时，表示大小写敏感。

ENTER　开始查找

ESC　退出查找

Ctrl+G　转到在"Result of Memory Address Search"中选择的地址。

ESC　返回到主菜单

5. File Viewer—Display Text File(文件查看器——显示文本文件)

该功能用于查看任何文本文件。

6. Game Playing Speed(游戏速度)

Game Wizard 可以降低 或加快游戏速度。该项用于增加老游戏在现代高速电脑上的可玩性。用光标键调整速度，然后按回车确定。

该功能不一定对全部游戏可用。大部分游戏的速度可降低，而只有少数游戏的速度可增加。

速度能否调整由游戏怎么编写决定。一些游戏设计为只能在一定速度上运行，改变速度可能引起系统错误或不正常。

只能在第一次激活 Game Wizard 时调整速度。要调整速度条的延迟因子，在命令行中加/recalc 选项。当使用不同的内存管理器时，这可能是必须的。

7. Protect Screen(保护屏幕)

该选项用于使屏幕变黑防止烧坏。Game Wizard 还有自动保护屏幕功能。如果在指定时间内没有按键，Game Wizard 自动保护屏幕。默认时间是 3 分钟。允许范围是 1～60 分钟。默认的延迟时间可以用命令行/b＝选项调整并保存。

例如要设置延迟时间为 10 分钟，使用如下命令：

```
GW/b=10
```

8. Boss Screen(老板屏幕)

可以用任何文本屏幕和口令隐蔽当前的游戏画面。这可用于躲过老板或者防止别人在你离开时使用你的机器。要建一个新的老板屏幕，首先得删除 Game Wizard 目录下的 GW. BOS 文件。然后抓取当前显示的文本屏幕(通过激活 Game Wizard 并选择 Boss Screen 选项)。这样每次使用该功能时都显示该屏幕。要退出老板屏幕，必须记住正确的口令。默认口令是“Game Wizard”(输入口令后必须按回车键)。要调整或保存新的默认口令(最多 8 个字符)，使用命令行的/P＝选项。

例如，要设置默认的口令为“book”，使用如下命令：

```
GW/P=book
```

9. View Current Program Screen(查看当前程序屏幕)

在游戏紧张的时刻，可能来不及看游戏的详细情况(如生命、能量等)。该选项可帮你了解游戏详情。在查找或编辑内存之前，用该功能确认一下你要查找或编辑的项目是个好想法。

10. Save & Load(保存和装入)

Game Wizard 允许保存和装入程序。但这并不能替代游戏中的保存/装入功能。这用于不具有保存/装入进度的游戏，或者只允许在某一时间或地点保存/装入进度的游戏。

11. Crach back to DOS(退到 DOS)

该功能将结束当前运行的程序并返回到 DOS 提示符。它主要用于程序本身没有退出功能的场合，还可用于由于编程错误系统出错时退到 DOS。选择该功能后，在 GameWizard 之后使用的全部内存和设备都将被复位并且系统返回到其原始配置状态。该功能不能中止批文件，但它清除正在运行的程序，然后继续处理批文件中的下一个命令。

12. DOS Shell(转到 DOS 外壳)

该功能允许程序转到 DOS 外壳，通过将当前执行的程序转换到 EMS/XMS/DISK。这将腾出大部分基本内存，允许你进行日常的工作。用户可从 DOS 外壳返回到游戏。

13. 其他命令

在主菜单中，还有几个隐藏的命令可用于增加与某些程序的兼容性。现例举如下：

· 数字键盘上的减号(－)

在某些慢速的机器上，从 Game Wizard 返回游戏后可能会变慢。为了解决这个问题，激活 Game Wizard，然后按[－]键若干次可将游戏速度调回到原速度。

· 数字键盘上的星号（*）

这等同于主菜单中的 ESC 键。这是由于有些游戏在用 ESC 键退出 Game Wizard 后还能被游戏截获(这可能引起游戏退出)。

在有些游戏中，你可能希望自动重复某一按键。在激活 Game Wizard 时按住那键就可实现这一功能。如果要取消该特性，可再按"autorepeat"键。

14. 查找技术

对于知道精确值的游戏，使用"基本的内存地址查找"功能可很快找到。最有效的办法是只找上次查找后已改变的值。在某些游戏中，在地址内容修改或锁定后，其值在屏幕上不改变。这时你就只能等到屏幕上的值改变之后查找。

2.2.3 GW 的命令行选项

Game Wizard 的命令行选项很多，可同时使用多个命令行选项。

当您在 DOS 提示符下键入 GW/? 时，将显示 GW 的命令行帮助屏幕：

Game Wizard Pro v2.30b (c) Copyright 1994 by Ray Hsu & Gerald Ryckman.

Licensed to: Enhanced Software Design Inc.

Phone No. (416)492－0157 BBS No. (416)497－8337

Usage: GW [options]

Common Options:

/b# －Set the screen blanking delay in minutes; # is from 1 to 60.

/i# － Alternate interrupt setting; # is from 1 to 9.

/kN － Use a different activation key; N is the new KEYNAME.

i.e. to use F1 as the activation key use: GW /kf1

Refer to the manual for a complete list of the key names.

/p= －Set a new password for boss screen. Maximum length is 8 characters.

i.e. to set the password to cloud use: GW /p=cloud

/sN — Set swapping to (d)isk, (e)ms, or (x)ms. Where N is d,e or x.

i.e. to swap to disk use: GW /sd

/t — Stop the system time from being updated while inside Game Wizard Pro.

/vN — Set video swapping to (f)ast or (s)low. Where N is f or s.

i.e. to use slow video swapping: GW /vs

/u — Uninstall Game Wizard Pro from memory.

/x — Enhanced DOS Extended support; may be necessary for certain programs.

我们在 GW 的命令行中可用的命令行选项如下：

1. 基本命令行选项

• /b=#

设置黑屏延迟时间(单位:分钟)。范围:1～60。

• /i=#

改变中断设置,范围:1～9。

例如要将中断改为 5,则可执行下面的命令：

```
GW        /i=5
```

• /k=N

使用其他热键。N 是新的键名。例如,要改变热键为 F1,则执行下面的命令：

```
GW        /k=f1
```

下表列出了 GW 中可使用的键名及其对应功能。

表　GW 中可使用的键名及其对应功能

键名	实际键
RSHIFT	右 Shift
GMINUS	数字键盘上的减号(－)
GPLUS	数字键盘上的加号(＋)
CTRL	右或左 Ctrl
ALT	右或左 Alt
TAB	Tab
F1	F1
F2	F2
F3	F3
F4	F4
F5	F5
F6	F6
F7	F7

F8	F8
F9	F9
F10	F10

• /P

设置老板屏幕的口令。最多为 8 个字符。

例如要设置口令为“cloud”,使用下面的命令:

```
GW        /P=cloud
```

• /SN

设置交换到 d(磁盘),e(EMS)还是 x(XMS)。N 是 d、e 或 x。

例如要交换到磁盘,使用下面的命令:

```
GW        /sd
```

• /t

该选项用于防止进入 Game Wizard 后系统时间被改变(对某些游戏是必要的)。

• /vN

设置显示交换为(f) 快或(s)慢。这里 N 是 f 或 s。如果出现显示问题,试一试另一

选项。

2. 高级命令行选项

• /delay

该选项用于设置新的游戏速度延迟因子,以防在 Game Wizard 初始安装时不能正

确计算。对不同的微机系统,下表列出合适的延迟因子。

系统与延迟因子的关系表

系统	延迟因子
286/20 386/25	784(不同的标准) 336
486/33 486/66	1344 3584

286 的延迟因子比 386 大,这是由于 286 所用的计算方法与 386/486 和 Pentium 的不一样。由于 286 慢,因此使用特定的数字进行计算。通过调整这些数字,可获得经验。

• /install

该选项用于安装 Game Wizard,而不管它是否已在内存中。

• /recalc

该选项用于重新计算一个新的延迟因子。当运行不同的内存管理器时,这是必要的。

• /sbirg

用于设置与声霸卡的兼容声卡的 IRQ(中断请求),以防 Game Wizard 不能正确识别。这值将被存放在配置文件中。例如,要放置 IRQ 为 7:GW/sbirq

=7

· /sbport

用于设置声霸兼容卡的端口地址以防 Game Wizard 不能正确识别。这值将被存入配置文件中。

例如，设置端口地址为 220，使用下面的命令：

```
GW        /sbport=220
```

2 /trident=N

该选项用于纠正在某些 Trident VGA 卡中的硬件错误。当使用 Game Wizard 时若游戏屏幕的顶部遭破坏，则应该用该选项。N 可以是 on 或 off。一旦使用/trident 选项，Game Wizard 将用该选项永久配置自身。如不想使该特性起作用，必须使用 /trident=off 选项。

2.2.4 利用 GW 修改 Wolfensein 3—D 游戏为天下无敌手

1. 驻留 GW。

2. 运行 Wolfensein 3—D 游戏。

3. 开始游戏，等到屏幕显示 100%健康值时按[']键激活 GW。这时屏幕出现 GW 的主菜单。

选择"1. Memory Address Search"(内存地址查找)，并使用中级或高级查找功能。当提示"Search for:"时输入健康值 100，然后回到游戏。

4. 当健康值发生变化时再次激活 GW。选择"内存地址查找"，并输入新的健康值。

5. 重复步骤 4，直到找到的地址不多于 8 个，这时 GW 自动显示找到的地址。若找到的地址不止一个，则可输入新的健康值继续分析，或者判断哪个地址可能是确切地址。

6. 进入"Table of Memory Location"(内存地址表)选项，按[E]键编辑一个表项，输入注释"Health"，按回车键或 TAB 键将光标移到地址列。若该表原先没有地址，则 GW 会自动填入您所选择的地址，否则，按[Ctrl]+[S]填入地址。然后输入值 100 或参照对应于 100%的值进行确定。按回车保存该项值。

8. 为了不让程序修改该值，可用[F]键锁定。

9. 回到游戏后，您将是天下无敌手了。

2.2.5 在 DOSV 环境下使用 GW

GW 游戏工具软件还是不能真正地支持 DOSV 环境（虽然软件开发者都说可支持）。不过，您可采用如下方法使 GW 可真正地支持 DOSV 环境。

1. 首先将 CONFIG.SYS 中有关 DOSV 配置的下面一行注释掉：

```
REM     device=C:\JDOS\$DISP.SYS
```

2. 用 DOSV 重新启动，此时，屏幕并未进入日文屏幕。

3. 调入 GW。

4. 使用 PC DOS 7.0 提供的 DEVLOAD.EXE 工具将 $DISP.SYS 调入内存，其命令行调入命令如下：

```
DEVLOAD C:\JDOS\$DISP.SYS
```

此时，屏幕进入了日文状态。

这样您就可随时调入 GW 了。

DEVLOAD 的详细使用方法参见附录 F。

2.2.6 GW 系列技巧集锦

1. 使用 GW 时应记住如下几个常用的汇编指令(详细介绍参见附录 C)。

- JMP 指令代码为 0EBH。
- JZ 指令代码为 74H
- JNZ 指令代码为 75H

2. GW 与声霸卡、特殊模式

GW 与声霸卡、一些特殊显示模式不兼容。

3. GW 与 XMS 内存

GW 不支持对 XMS 内存的读写方式。虽说 GW 不能锁定 XMS 内存，但这也是为保持兼容性。它存档时能把 XMS 的内存也存进盘中，只有少数保护模式的游戏存不了。

在 32 位保护模式的游戏中不能直接编辑内存，也不能使用带 * 号的 20 位地址，否则会死机。

4. GW 的测地址算法

GW 具有十分优秀的测地址算法，假如游戏中的值是 1、2、3，而您在 Intermediate 方式里输入 6、5、4，仍能测出正确的地址，但其他软件的低级分析就测不出来。

另外，当您数错值时，可用 CTRL+P 修改，这也是 GW 的过人之处。

有些游戏用 GB4 等锁定后血还是减少，但 GW 就能锁住。

5. 用 GW 对付《三国志Ⅳ》(不是增强版)

若您在使用 GB4 时改 SAN4 鼠标器会死掉，您不妨使用 GW。

有的机器在 SAN4 中用 GW 会使屏幕上面变色，用 GW/trident=on 就可解决稳妥。

用 GW 一个城一个城地改钱很麻烦，您可以在分配“内政”资金时测剩余资金的地址，经过反复试验您会得到这样一个地址：用 GW 锁定功能把这个地址加 1 的地址锁为 255 后，不论到哪一个城，一修改任何一项内政资金此城的钱就会变成 6 万多。这样您就可以用鼠标轻松地把每个城市加满钱而不再调用 GW。注意此方法只能用于 GW，其他软件锁定不住。

2.3 GW 的演示软件

在 GW 工具软件中还包括了 GW 的演示软件，其执行程序名为 GWTUTOR.EXE(辅助文件为 GWTUTOR.OV1)。

当您在 DOS 中装入了 GW 后，就可以执行 GWTUTOR.EXE 程序来

运行 GW 的演示软件。

若您在执行 GWTUTOR 时出现了下面的错误信息：

```
ERROR : V86 mode without VCPI. This is usually caused by a memory manager
        which has its EMS services disabled. Please refer to the manual for
        more detailed information.
```

说明您的微机处于 V8086 环境(虚拟 8086)，因为 GWTUTOR 不能在此环境下运行，必须在 EMS 内存的环境下运行。因此，下面两行必须出现在您的 CONFIG. SYS 文件中。

```
DEVICE=D:\PWIN\HIMEM. SYS
DEVICE=D:\PWIN\EMM386. EXE RAM FRAME=E000
```

用此配置的 CONFIG. SYS 重新启动后，GWTUTOR 就可运行了。运行的初始画面如下。

```
Game Wizard Pro V2. 30b Copyright (C) 1994 by Ray Hsu & Genald Ryckman

        General Information
    Welcome to the interactive tutor for Game Wizard. This
    Program attempts to illuatrate how to use the Memory
    Address Search function to locate items within Game.
    Other features demonstrated in this demo are the
    Result of Memory Address and editing/Freezing data
    using options within the Table of Meaning Locations.
    Please make sure Game Wizard is resident in meaning
    or you will not not be able to take part in the last
    section of this interaction demo.

    Press ESC to quit or any other key to continue.
```

上面屏幕的中文意思说明 GWTUTOR 演示程序可以向您介绍如何使用“Memory Address Search”功能定位到游戏中的项目。另外还演示了 GW 的其他特性，如“Result of Memory Address”及“Table of Meaning Locations”。在启动 GWTUTOR 之前，必须装入 GW 程序，否则您将无法参与该交互演示的最后部分。按 ESC 键退出 GWTUTOR，按其他键将继续 GWTUTOR。

在演示过程中，您可按下面的热键进行您的演示过程：

- N=Next Screen(下一个屏幕)
- P=Previous Screen(前一个屏幕)
- CTRL+A=Abort SlideShow(放弃演示)

第三章 整人专家 FPE 4.0 使用

您曾经为了游戏不能破关而烦恼吗？在市面上常可见到专门修改游戏的程序，例如：电动克星（由台湾陈伟谷先生编写），游戏克星（即 GAME BUSTER 4.0）等...玉树临风的整人专家就是属于这一类的程序。整人专家是"调整游戏人数之专家"，使用扫描技巧修改像生命、经验值等数值，完成破关的神圣使命，解救为游戏废寝忘食、抛妻弃子的玩家. 唉，GAME 海无边，回头是岸，阿弥陀佛 !!

本章将介绍 FPE 4.0 详细使用与实例分析。

3.1 整人专家 FPE 4.0 主要特点

FPE 4.0 具有以下特点：

1. 超强扫描功能。
2. 完整内存编辑功能。
3. 100% 有效的表格记录功能，不论内存变动与否。
4. 支持 XMS.（扩展内存，需安装驱动程序，如 HIMEM. SYS，QEMM386. SYS 等）。
5. 支持 VGA，Super VGA 各种模式。
6. 只占用 10KB 左右的基本内存，并且可以进驻高内存能不占用基本内存。
7. 操作简便，相容性高，不会和 EMM386. EXE、抓图程序 等...冲突。
8. 拦截能力超强。
9. 支援 DOS Extender 的游戏！如《绝地大反攻》、《毁灭战士》(DOOM)、《模拟城市 2000》(SC2000)、《毁灭战士 2》(DOOM 2)、《快乐天堂》(THEME PARK)及 FPE3.0 无法改的例如《雷电》等游戏。
10. 支持日文 DOS/V，可修改日文游戏。
11. 支持鼠标呼叫功能，能拦截的游戏几乎达到 100% !!
12. 内置抓图接口，并附抓图专家，用整人专家也可以抓图罗！且可以抓 SVGA 的图片。
13. 内置 Game Speed 功能，包含 Turbo 及 Delay。
14. 键盘及鼠标热键可调，即 Hot Write 热键。
15. 支援各种 Super VGA 卡，包括 VESA 标准，Tseng，Trident 系列等。
16. 老板屏幕保护按键。
17. 加强表格功能，合并 Lock 功能并增加注释（Comment），开关自动锁定(Switch)、修改位址(Addr) 等 功能。
18. 超大十进位扫描范围由 0 至 4294967295 (FFFFFFFFh)。
19. 快速方便的 SETUP 程序。

3.2 FPE 4.0 的使用环境与文件

3.2.1 FPE 4.0 的使用环境

1. 适用机型

286 以上兼容机型，以及 1MB 以上的内存。

2. 屏幕模式

VGA，Super VGA 支援的有：VESA 标准（S3，ET4000/W32. .），Tseng 系列（ET3000，ET4000/AX），Trident 系列（TR8800，TR8900，TR9000）... 等等，只支持 VGA 以上的显示卡。

3. 软件环境

建议使用 DOS 5.0 以上，亦支持日文 DOS/V。

3.2.2 FPE 4.0 的文件

FPR 4.0 应有下列文件：

INSTALL.EXE	.... FPE 4.0 安装程序
FPE.BAT	.... FPE 4.0 安装程序
FPE.BAT	.... FPE 4.0 安装程序
FPE.BAT	.... FPE 4.0 执行批处理文件
FPEMAIN.COM	.... FPE 3.0 一般游戏执行程序
FPE32M.COM	.... FPE 4.0 32M 执行程序
FPESETUP.EXE	.... FPE 4.0 参数设定程序
BATC.EXE	.... FPE.BAT 控制程序
CBOOT.EXE	.... 建立开机磁盘的程序
GPE.COM	.... 抓图专家 2.0，需配合 FPE 4.0
SPE.EXE	.... 秀图专家 2.0
AL.COM	.... 自动锁定程序.
FPE.LOG	.... FPE LOGO 画面

3.3 FPE 4.0 的安装与设定

3.3.1 FPE 4.0 的安装

将 FPE 4.0 系统 磁盘放入软盘驱动器 A 或 B 中，执行 INSTALL.EXE。一切完成后，就大功告成了，不过装入的文件只有在这台电脑中才能使用，若以后你想要换主板或 VGA 等显示卡或想要拿到另一台电脑使用，请重新安装整人专家。INSTALL.EXE 不会对硬盘做任何不正常的写入，请安心使用.

3.3.2 设定 SETUP

FPESETUP.EXE 是参数设定程序，可以辅助您设定参数，你可以不用键入任何参数。(除了 R 及一些不常用的参数) FPESETUP.EXE 会在本身所在的目录下自动产生 FPE.BAT 执行批处理文件。

执行 FPESETUP.EXE 后，您可以上下移动红棒或鼠标，选择要设定的项目，并按下 [Enter] 或鼠标的右键，就可以设定此项目的开启或按键了。另外，功能键 [F3]为储存并结束，[F4] 或 [Esc]为结束但不储存。

FPESETUP 的屏幕画面如下：

```
Fix People Expert Setup                    Version 4.0

                        Setup
        Use FPEMan ver =                    Off
        LoadHigh to UMB =                   On
        A:Auto Lock Quickly=                On
        V:Check VGA card =                  On
        M:Mouse Calling =                   Mode 1
        C:System Clock =                    Off
        X:Reserved XMS(MB) =                [04]
        H:Hot key =                         [Prts * ](37)
        L:Hot Load key =                    [-](4A)
        W:Hot Write Key =                   [+](4E)
        Load GPE =                          Off
        File Name: E:\CGJ\FPE\FPE.BAT

        F3:Save and Exit      ESC or F4:Exit without Save

                                    Designed by Li Guoo.jaw
```

下面详细地介绍 FPESETUP 的配置。

第一项选项 "Use FPEMAIN ver" 询问你是否要使用 FPEMAIN 版本、FPE32M 版本及 FPEMAIN 版本(这些在后面说明)。如果你对如何判别是否为 DOS Extender(DOS/4GW) 的游戏不是很了解的话，请设定为 OFF，整人专家会自己辨认。但是如果你有下面情况时，请设成 ON，自行选用 FPEMAIN 版本或 FPE32M 版本。

1. 你的电脑是 286

笔者尚未见过使用 286 DOS Extender 的游戏，请完全使用 FPEMAIN 版本即可。

2. 你没有足够的高端内存 (UMB)

FPE32M 必须使用基本内存 22kB，而 FPE32M 只需要 12kB 基本内存 + 76kB XMS。所以如果是一般的游戏，可以选用 FPEMAIN 版本以节省基本内存的使用。

3. 兼容性问题

FPE32M 版本由于硬件的特性，锁定值必须为偶数个字节，如果你只输

入 1 个字节，如 "01"，它会自动帮你补上 00，如 "01 00"成为偶数个字节，但是这样在某些游戏上可能造成问题，所以遇上这种问题时请选用 FPE-MAIN 版本。

对于 A，C，X，H，L，W，M 等各项参数的使用方法及说明，请参考下面的参数说明。

> 注意：如果你不想让 FPE32M 版本吃掉你的 XMS 内存，可把 X 参数后的值设为 0。

最后一项选项 "Load GPE" 询问你是否载入抓图专家，载入抓图专家后，整人专家就有抓图功能了！如果要，请把红棒移到这个选项，并按下 [Enter]，键入所要存放影像文件 *.GPE 的路径就可以了，如果想直接存在游戏的那个目录下，请输入路径时直接按 [Enter]。

3.4 执行方式

3.4.1 游戏设计的两种方式

> 注意：如果你对游戏是否使用 DOS Extender (DOS/4GW) 不很了解的话，请直接把 FPESETUP.EXE 中的选项 "Use FPEMAIN ver" 设为 OFF，就可以跳过下面 FPE 两个版本的说明。

一般来说，游戏的设计方式分成如下两种：

· 一是使用 DOS Extender(DOS 扩展程序，一种新发展的技术，介于保护模式应用程序与 DOS 之间的一个中介程序，DOS4GW.EXE 就是这种程序)。

· 一是不使用 DOS Extender 的，也就是传统的一般游戏。

所以，整人专家载入的方式也分为两种：FPEMAIN 版本和 FPE32M 版本。

如果你知道这个游戏是否使用了 DOS Extender 的话，正确选择载入的整人专家版本将会提升您修改的效率！但是 FPE32M 版本也是能够修改传统一般游戏的！

以下将以 FPEMAIN 版本来代表可修改一般游戏的整人专家一般游戏版本。以 FPE32M 版本来代表整人专家扫描范围可达 32M 并且可修改 DOS/4GW 等 DOSExtender 游戏的版本。目前使用 DOS Extender 的游戏大多使用 DOS/4GW，所以以下将以 DOS/4GW 来代表 DOS Extender，但是 FPE32M 应可支持绝大多数的 DOSExtender !!

3.4.2 使用 FPE 4.0 的有关注意事项

· 执行 FPEMAIN 版本必须先安装 XMS 驱动程序，如 HIMEM.SYS、QEMM386.SYS 等，而且最少必须有 14kB 可用的 XMS 供整人专家使用。

· 执行 FPE32M 版本是不需要任何内存的驱动程序的，也就是说就算

你把 CONFIG.SYS 整个删除也能工作!! 不过笔者不建议您这样做。并且请您在载入 FPE32M 后就立刻进入游戏，中间请不要执行其他会占用 XMS/EMS 的常驻程序，否则 FP32M 的 Load/Save 与 FPE 自动计算地址的功能可能会失效。

· 因为 DOS/4GW 的游戏工作方式特殊，所以如果您只有 4MB 内存，而没有空出最大的扩展内存时，内存可能会不够用，笔者建议您最好用 DOS 6.0 写个多重配置，移去 CONFIG.SYS 及 AUTOEXEC.BAT 中的内存常驻程序及内存管理程序（如：SMARTDRV、NCACHE、4DOS、NDOS、EMM386、QEMM386、386MAX 等）

· 如果您觉得上述的修改太复杂或懒得修改的话，当然您也可以制作"开机磁盘"，CBOOT，EXE 可以帮您建立开机磁盘，它会帮你写 CONFIG.SYS 以及 AUTOEXEC. BAT。若您已经建立了开机磁盘，可以直接以此磁盘开机，然后再载入 FPE，玩 DOS/4GW 的游戏。

· 如果您只有 4MB 内存的话，想要玩 DOS/4GW 的游戏时，笔者强烈建议您用开机磁盘或上述配置开机；但是如果您有 8 MB 以上内存的话，您可以加挂其他内存管理程序、高速缓存程序；笔者建议您加挂高速缓存程序以提高整体效率。

3.4.3 FPE 4.0 使用及参数说明

1. 当 "Use FPEMAIN ver" 选项为 OFF 时
在 DOS 提示符号下键入如下命令：

```
C:>FPE [A C Xnn Mn Hnn Tnn Wnn R ?]
```

然后就可以了。

2. 当 "Use FPEMAIN ver" 选项为 ON 时
在 DOS 提示符号下键入如下命令：

```
C:>FPE [A C Bnn/Xnn Mn Hnn Tnn Wnn R ?]
```

会出现下列的画面：

```
1. Fix People Expert normal version
2. Fix Peolpe Expert 32M version

                    by Li Guoo—jaw
```

假如你要玩的游戏是一般游戏，就是没有使用 DOS/4GW 的游戏时，请选择第一个 "1. Fix Peolpe Expert normal version" 并按下 [Enter]；就会自动载入 FPEMAIN 版本；假如您要玩的游戏是 DOS/4GW 的游戏时，请选择第二个 "2. FixPeolpe Expert 32M version" 并按下 [Enter]；就会自动载入 FPE32M 版本。

[A C Bnn/Xnn Mn Hnn Tnn Wnn R ?] 是参数，请用空格隔开；没有键入的参数会使用内定值；参数可以重复使用，若参数有重复使用，则以较后面的为准。设定错误时会显示 "整人专家参数辅助说明" (Param Help)，并在右上方显示错误原因。

整人专家载入完成后，会把内存、热键、开关、Super VGA 状态显示出来，若装载不成功的话，则会出现"WARNING!!....."的警告信息。

如果内存（MEMORY）状态中显示为"Use UMB memory. . ...."的话，表示 LoadHigh 成功了，将不会占用传统 640kB 内存空间；如果显示"Use MAIN memory....."的话，表示没有可用的 UMB，它将使用基本内存。

下面对上面的参数作些说明。

· A(Auto Lock quickly)

设定快速自动锁定修改，约 1/18.2 秒就修改一次。假如您没有设定这个参数时，内定为 2 秒修改一次。

假如您发现整人专家还来不及修改时 主角就死了，例如在"WOLF3D"主角遭到机枪连续射击时，您就可以在事先载入"整人专家"时使用此参数，以加快修改速度。

但是您设定这个参数时，有时会因为修改速度太快，而导致游戏无法顺利进行（例如《PRINCE 2》〈波斯王子 2〉，王子掉下陷阱却不会死。），所以，请斟酌设定。

· C (System Clock)

设定 Clock 为 OFF；至于 Clock 功能请参考下面的功能说明。

· Hnn(Hot Key)

设定"热键＃1"为 nn。"nn" 是键盘扫描码，用十六进制表示；热键＃1 内定为[*](37)，即 nn＝37。

假如您想要更改热键时，建议使用 FPESETUP. EXE 会比较方便，使用 FPESETUP. EXE 更改热键时只需要直接按下该键，不需要知道扫描码！热键的用途请阅读下面的热键说明。

· Lnn (Hot Load key)

设定"读取热键"为 nn。"nn" 是键盘扫描码，用十六进制表示，读取热键内定为 [－](4A)，即 nn＝4A。

· Wnn (Hot Write key)

设定"修改热键"为 nn。"nn" 是键盘扫描码，用十六进位制表示，修改热键内定为 [＋](4E)，即 nn＝4E。

· Xnn(Reserved XMS)

此参数为 FPE32M 版本专用，只键入"X" 或"X0" 时设定完全不占内存，"nn"＝ 欲保留给游戏的空间。例如："X4" 保留 4MB XMS 给游戏使用，"X6" 保留 6MBXMS 给游戏使用。缺省值 nn＝4(即 4MB)。

如果你有 8MB 以上的内存，为了低级扫描的需要，FPE32M 会帮你占据多的内存，让游戏只用 4MB XMS，笔者目前尚未看过需要 XMS 超过 4MB 的游戏，如果您发现执行游戏时出现内存空间不足的信息，您可以使用 X 参数调整保留大小，不过如果您想要低级分析时，请准备足够的硬盘空间。

· Mn(Mouse Call)

使用此参数时，FPE 可用鼠标呼叫。"n" 表示鼠标呼叫的模式。内定 n＝1，目前根据笔者的测试，并无 M1 鼠标呼叫不能叫出整人专家的游戏，所

以您可以不需更动此参数。

n＝0 时，不使用鼠标呼叫。

n＝1 时，呼叫方法为把鼠标移到最左边（就是 X 轴等於零），然后左右两键一起按下，就可以呼叫出整人专家主菜单了。直接同时按下滑鼠左右两个按键，整人专家会自动根据表格修改目标一次，此参数不影响游戏支持鼠标。

n＝2 时，呼叫方法为同时按下鼠标的左右两键，就可以呼叫出整人专家主选单了。如果在此模式只按下鼠标的左键或是右键，FPE 会自动根据表格，修改目标一次。此参数不影响游戏支持鼠标。

n＝3 时，使用此参数时，整人专家会让游戏不能发现鼠标驱动程序的存在，这样使用鼠标呼叫整人专家，就能达到 100% 的拦截力！但相对的，游戏将不能支持鼠标。呼叫方法为同时按下鼠标的左右两键，就可以呼叫出整人专家主选单了；如果在此模式只按下鼠标的左键或是右键，FPE 会自动根据表格，修改目标一次。

> 注意：使用此参数请先载入鼠标驱动程序；若整人专家找不到鼠标驱动程序，会忽略此参数。

· V (Check VGA card)

设定载入时不检查 VGA 卡(内定的是要检查 VGA 卡)。假如您的 VGA 卡太旧，而和 "整人专家" 不兼容时，可以设定此参数，不过整人专家可能无法正常执行，建议更新您的 VGA 卡。

· R

把 "整人专家" 从内存中移除。这参数和其他参数一起使用时，其他参数全部失效。

· ?

显示 "整人专家" 参数辅助说明。这参数和其他参数一起使用时，其他参数全部失效。

下面介绍 FPE 4.0 的较特殊的参数。(在 FPESETUP.EXE 不提供下列参数的设定)

· Bnn(Buffer size，FPE32M 版本无此参数)

设定分析地址缓冲区的大小；"nn" 表示欲设定之 KB 数，用越大之 KB 数，程序占用的内存就越大，但可分析的址也会相对的提高。设定"nn"＝14 时，可以记录大约 14,000 个址；而设定"nn"＝37 时，可以记录大约 37,000 个址。如果不用此参数时，缓冲区内定为 62kB。

关于内存占用，FPEMAIN 版本会占用基本内存 12kB，占用 XMS（扩展内存）"14 ＋ 设定之 KB 数"，所以 "nn"＝0 时，整人专家只使用 14kB 的 XMS，但就无法进行高级扫描了；而低级扫描则没有此限（低级扫描完全使用磁盘空间），但"nn" 小于 62 时，会增加 64kB 的磁盘使用空间。FPE32M 版本为了获得最大执行空间，完全不用 XMS。

· S

此参数是为了配合 DOS/V 版的游戏在某些 VGA 卡时发生屏幕不正常时用的；整人专家已经支持 DOS/V 的游戏了，但如果玩游戏时屏幕发生不正常现象时，请加上此参数。

下面我们给出三个例子。

1. C:\>FPE A M1 V X5
   设定快速自动锁定修改；(A)
   设定可以使用鼠标呼叫模式 1；(M1)
   不要检查 VGA 卡；(V)
   设定保留给游戏使用的 XMS 为 5MB。(X5)
2. C:\>FPE H02 L03 W04
   设定 热键 (Hot key) 为 [1] (02)；(H02)
   设定 读取热键 (Hot Load key) 为 [2] (03)；(L03)
   设定 修改热键 (Hot Write key)为 [3] (04)；(W04)
   "[1] (02)" 的意思是 "[键名] (扫描码)"
3. C:\>FPE R
   把 "整人专家" 从内存中移除。

3.4.4 FPE 4.0 热键

热键是用来呼叫整人专家的，只要硬盘不在运转中，您就可以执行下面的动作。

1. 按 [热键] 然后放开，就可以呼叫出整人专家主菜单。

2. 按 [读取热键] 然后放开，整人专家会自动载入 "AUTO. FPE" 这个锁定文件，并自动算出正确目标地址，自动修改；如果发出"哔"一声，表示整人专家目前无法载入 "AUTO. FPE"，可能是文件不存在或驱动器门没关。

3. 按 [修改热键] 然后放开，不论自动修改功能有没有关掉 (AUTO 或 Switch)，整人专家都会自动根据表格，修改目标一次。这个功能是适用于只想要修改一次那些使用 Edit rooms 的 Auto [OFF] 或 Switch 关掉的地址。

某些游戏会把时钟中断向量按管理，而导致整人专家无法自动锁定写入，(就是整人专家不会自己自动修改成您想要的值) 这时您也可以使用这个功能 3。或下面 #2 的方式修改，手动写入，按一次改一次。

当您遇到键盘无法呼叫整人专家时，可以使用鼠标呼叫来尝试呼叫出整人专家。(下面范例是对内定参数 M1 而言的，其他 M? 参数呼叫方法请参考上面参数说明)

#1. 把鼠标往左移，如果您看不见鼠标时，往左移多一点，然后同时按下左右两个按键，就可以呼叫出整人专家主选单。

#2. 直接同时按下鼠标左右两个按键，整人专家会自动根据表格，修改目标一次。

举个例子：在未修改热键时，您可按下面的热键执行相应的操作。

按 "键盘右边灰色的 [*] 键" 然后放开，可以呼叫出整人专家主菜单。

按 "键盘右边灰色的 [－] 键" 然后放开，可以自动载入 "AUTO. FPE"。

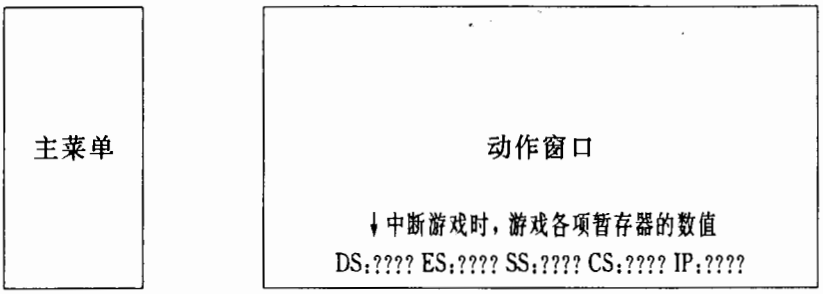
按 "键盘右边灰色的 [＋] 键" 然后放开，可以自动根据表格，修改目标一次。

把鼠标往左移 (移多一点) 然后同时按下左右两个按键，呼叫出整人专家主菜单。

不用移动鼠标，直接按下鼠标左右两个按键，可以自动根据表格，修改目标一次。

3.4.5 功能说明

当您按呼叫出整人专家主选单后，屏幕会出现如下样子的画面：



"ESC" 这个键可使用于整人专家的任何时候，在动作窗口按下此键，则退回到主菜单，如果在主菜单按下此键，则脱离主菜单回到游戏中。在主菜单有 11 个可使用功能，下面详细说明。

1. Scan memory (扫描内存)

这个功能依据扫描方法，分为 High level 和 Low level 两个等级。

· 高级扫描 (High level)

> 注意：由于 FPE32M 版本所需要扫描的空间太大，所以它会用磁盘来存放资料，请在一开始时输入工作驱动器名。FPEMAIN 版本则不用。

使用此功能时，整人专家会要求输入一组数值，这个数值就是目前欲修改的目标之值，然后您可以离开整人专家，继续游戏，等到这个目标之数值有所变化时，再呼叫整人专家使用这功能重新输入目前之值，整人专家会告诉您找到的地址个数；如此重复做几次，等到整人专家找出地址数在十个以内，整人专家会显示出"List ? (Y/N)" 问您要不要列出地址，假如要，请按 [Y]，整人专家会自动呼叫 "2. List addresss" 这功能，您就可以锁住或修改了。建议找出地址数在一、二个以内才列出地址修改比较可靠。

假如想要分析另一个新的目标，中途可以按 [F2] 来清除上次分析的数据，以便重新分析。假如输入错误，则会出现错误信息，而且央标会停在错误的地方。如果扫描后出现 "Buffer Full" 或 "Disk full" 的信息，表示相同数据太多(请不要在第一次扫描时输入 0)，您可以继续分析资料，不过有可能会因为太多而找不到！

假如您玩的是 RPG 或战略游戏或其他有数个数据连续排在一起的程序，因为目标在内存中极可能是连续的，您就可以很好的使用字串扫描的功能。例如主角的列表是"HP:500，MP:600"，您就可以直接输入" > 500，600 "，这样一次就找到的机率就很大了。

· 低级扫描 (Low level)

使用这功能时，请确定有足够的磁盘空间；FPEMAIN 版本最好有 1.2M 以上可用空间，假如您设定扫描缓冲区 (参数 B) 大於 62k 时，FPEMAIN 版本会使用比较少的磁盘空间。

FPE32M 版本则需要庞大的磁盘空间，需要 (内存大小－1) * 4 的空

间，例如您有 4MB 内存，(4－1) * 4 = 12MB，所以你最大需要 12MB 的硬盘空间，不过通常分析需要的大小为最大的一半，所以如果您有 4MB 的内存，最少也得准备 6MB 的硬盘空间。

如果您有 8MB 以上的内存，为了以上的理由，FPE32M 会帮您吃掉多的内存，让游戏只用 4MB XMS，笔者目前尚未看过需要 XMS 超过 4MB 的游戏，如果您发现执行游戏时出现内存空间不够的提示，您可以使用 X 参数设定保留空间，不过如果您想要低级分析时，请准备足够的硬盘空间。

使用这功能时，整人专家会先要求输入工作驱动器，并进行储存；第二次使用这功能之后，您就可以依据目标大小的变化，按方向键，上下选择 "＞"（大于），"＝"（等于）或 "＜"（小于）了。

例如，在 "XENON2" 中，您可以在一开始时先呼叫整人专家，使用这功能输入工作驱动器，然后回到游戏，故意去撞敌机减少保护罩的能源，再呼叫整人专家，因为这次（第二次）比第一次时的数值少，所以选择 "＜"（小于），整人专家会告诉您找到的地址个数；假如您第三次吃到补充能源的心脏，因为这次（第三次）比第二次时的数值多，就可以选择 "＞"（大于）；您也可以趁着保护罩的能源没有改变时选择 "＝"（等于）；如此重复做几次，等到整人专家找出地址数在十个以内，您就可以锁住或修改了。

在第二次扫描及第三次扫描时请千万不要选择 "＝"（等于），否则您将可以看到您的硬盘灯闪个不停，扫描时间超久，而且会吃掉庞大的硬盘空间。

2. List address（列出可能地址）

这功能是要配合 "1. Scan memory" 列出找到的可能地址。假如可能地址是在十个以内，就可以列出。

例如：

```
1234:0001   77
1234:0002   63
  ↑          ↑
地址         目前这个地址的值(十六进制)
```

列出之后您可以上下移动红棒选择可能地址，然后可以执行下面的操作：

按 [Enter] 执行 "3. View table" 锁住可能地址。

或按 [E]（Edit）执行 "4. Edit memory" 编辑内存。

所谓 "锁住地址"，就是在每间隔 2 秒或 1/18.2 秒之后就在这个地址自动写入锁定值，时间的长短由设定时的参数 A 决定。

在 FPE32M 版本中，地址 001234h 所指的是 "物理地址"（Physical address）。

3. View table（编辑表格）

执行这功能时会出现如下屏幕。

```
Free Room                                    ← 没有使用的空间
Free Room                                    ← 没有使用的空间
1234:ABCD     01 02 0A 0F    [test1]         ← 锁定数据列表
2222:3333     01 02 0A 0F    [test2]         ← 锁定数据列表
```

↑ 地址　　↑ 锁定值(字串)　　↑ 注释

您可以上下移动红棒查看，

或按 [A] (Addr)　　设定锁定地址，

或按 [V] (Value)　　设定锁定值，请输入和 Scan 功能相同语法的字串。

或按 [C] (Comment)　　设定注释，

或按 [U] (Unlock)　　删除锁定，

或按 [S] (Switch)　　设定是否要自动修改，按一次会关掉这个地址的自动修改，关掉时会在地址前面会出现 "—" 并成紫色，这个地址就不会自动修改；再按一次[S] 则会打开自动修改。

整人专家会在锁住的地址每 2 秒(或 1/18.2 秒)自动写入锁定值，以达到无敌版的效果。

这功能可以配合 "2. List address"，假如您是使用功能 2. List address 按 [Enter] 跳到这功能的则会自动执行 Addr 副功能，而且会自动设定锁定地址为 List address 列出的地址。

整人专家共有 12 个表格空间；每个空间最多可以连续锁住 9 个地址。因为一般的战略游戏或 RPG 经常把相似的资料放在一起（例如体力 "HP" 和魔法力 "MP" 就经常放在一起)，而连续锁住地址可以一次就锁住好几个目标（例如您已经找到 HP 和 MP 的地址，您想要都修改成 1000，输入锁定值时就可以输入" > 1000,1000 ")，所以玩战略游戏或 RPG 时，可以好好利用这个功能。

4. Edit memory (编辑内存)

这功能可以配合 "2. List address" 编辑找到的地址或自己输入编辑地址。

这个功能会要求输入一个地址，输入之后会把这地址之后的 8 * 8 个地址内容全部印出并且会不断更新它的内容。这时您就可以执行下面的操作：

按 [F1] 重新输入地址，

或按 [F2] 编辑内存，

或按 [Pg Up]、[Pg Dn] 上下翻页。

编辑内存时您可以藉着按 [TAB] 切换十六进制，只要您一改变内容，相对的内存就会跟着改变。

5. File record (文件记录)

这功能请在载入游戏之后使用，因为假如不在游戏中使用，程序无法算出正确的地址。

在 FPE32M 版本中，请载入 FPE32M 后就立刻进入游戏，中间请不要执行其他会占用 XMS/EMS 的常驻程序，否则 FP32M 的自动计算地址的功能可能会失效；而如果你本来只安装 HIMEM.SYS，没有安装内存管理程序时，也请不要把在你电脑上记录的 *. FPE 拿到有安装内存管理程式的电脑上用，FPE32M 无法正确的算出地址。

使用这功能请先选择储存 (Save) 或 读取 (Load) *.FPE 文件，并且

输入文件名(FPE 不用输入)，就可以了。第一次储存了之后，以后只要读取记录就可以了，这样可以避免每玩一次就改一次的麻烦。

但是假如您用的文件名称是"AUTO. FPE"的话，就可以使用读取键(HotLoadkey)直接读取，而不用呼叫主功能表了。FPEMAIN 版本的 *. FPE 文件和 整人专家 2.5 的是兼容的；FPE32M 版本的 *. FPE 则和 FPEMAIN 版本的 *. FPE 文件不相容。

不过这功能和其他的 GB4 等的工具程序不相同的是它会自动计算内存变动后的正确地址，这样使 FPE 能够成为无敌手。

另外，不论 AUTOEXEC. BAT 或 CONFIG. SYS 是不是有修改过，甚至在另一台电脑上，这个功能将可以 100% 有效的依据以前的 .FPE 记录文件，自动计算目前地址。

也就是说只要在第一次修改游戏时，把游戏修改的数据用这个功能记录下来，之后再玩这个游戏时就可以直接使用这个功能把记录读出，整人专家会自动算出正确的地址，而不用考虑 AUTOEXEC. BAT 或 CONFIG. SYS 是否和上次玩这个游戏时相同。

6. Game screen (游戏原来的画面)

这功能会回到游戏原来的画面，按任何键可以回到整人专家。这功能可以配合抓图程序抓图。整人专家 4.0 附有一个抓 VGA 模式的抓图程序——抓图专家，它可以抓几乎所有的 VGA 模式，包含自定的模式，例如 320 * 200 256 色 (市面上游戏大多用此模式，含 mode X) 及 640 * 480 16 色 (DOS/V 游戏大多用此模式)的图形；抓图专家只占 1.6k 的内存；而使用方法只要用这个功能"Game screen"回到游戏原来的画面，并按下 [G] 键就可以了；关于详细使用方法，请参阅下面抓图专家说明。

7. Exit game (跳离游戏)

这功能会跳离游戏回到 DOS。请尽量不要使用这个功能跳离支持 XMS 或 EMS 或直接使用保护模式的游戏，整人专家无法释放游戏所占用的 XMS 或 EMS！如果

游戏有支持音效卡时，请先关掉音乐及音效。

8. Game Speed (调整游戏速度)

这功能可以调整游戏速度。使用时会出现一个红色光标，把光标往右移，游戏速度会增快；把游标往左移，游戏速度会减慢；中间则是原来游戏速度；要恢复原速时请把游标移回中间。

9. Auto [ON] (表格开关)

这个功能是全部表格的自动修改开关，假如您想要关掉全部自动修改，您可以移动红棒到这里，并且按下 [Enter]，就会关掉全部的自动修改；再按一次[Enter]则会打开全部的自动修改。

10. Clock [OFF] (保留时钟装置切换)

当你把此项设为 ON 时，可能会造成某些游戏的兼容性问题，如有问题发生时，请设回 OFF！

这功能可以设定是否要保留时钟装置。ON = 要，OFF = 不要。内定为 OFF。当你设成 ON 时，在您呼叫整人专家之后，仍然可以听到游戏的音乐不会停止，这是因为整人专家并没有完全停止游戏的执行，整人专家保留了时钟装置；所以如果你觉得暂停时太吵的话，可以设成 ON，这样即使没有在游戏中，也可以听到优美的音乐。但是，在某些游戏用时钟装置来处理时间跳动或敌人移动，所以您可能在不知不觉中时间就到了或被敌人砍死。为了避免这种惨剧发生，所以遇上这种游戏时，请设定为 OFF。

11. Quit FPE（跳离整人专家）

这功能可以跳离整人专家回到游戏。

另外，FPE 还有一些功能未在主菜单，现列出来，供读者参考。

· 自动按键功能

整人专家有一个功能可以辅助您一直按着某些键；您只要在呼叫整人专家主选单之前，把这些键一直按着不放，等到呼叫整人专家主菜单出现之后，再放掉这些键，再跳离整人专家回到游戏，这些键就有一直被按着的效果，直到这些键又被按为止。

· 老板来了按键兼屏幕保护按键功能 — F10

你如果在玩游戏当中突然发现老板回来了，但又不想重新开机，可以马上呼叫出整人专家并在主菜单中按下 [F10]，屏幕会清除并出现 "C:\>" 的字样，可以暂时骗过你的老板。等老板走了的时候，可以再按 [F10] 回到主菜单，也可以按[F1] 回到 DOS 下。因为画面会清除，所以当你想暂时去上厕所，也可以按下此键以保护屏幕。

· FPE32M 版本的设定扫描范围 — F1，F2

当你使用 FPE32M，并在游戏中呼叫出它时，它会自动判断目前是否为 DOSExtender 的游戏，如有误判时，或者一直扫描不到目标时，可以按 [F1] 切换为扫描 640kB 内或 1MB 以外的内存，这样应该就可以扫描到了。

当你载入 FPE32M 版本时，它会自动计算出未使用的 XMS 起始地址及终点地址，以便以后能够扫描游戏，但是为了最大的兼容性，你可以更改这两个地址到 32M 内任何地方，除非你对游戏的内存配置很了解，否则笔者不建议你更动此二地址，适合进阶者使用。按 [F2] 可设定，并且在你设定后，Load/Save *.FPE 自动计算正确地址的功能将会失效。

3.5 抓图专家 & 秀图专家

3.5.1 抓图专家 GPE (Get Picture Expert)

整人专家提供一套抓图用的工具程序，只占 1.6kB 的抓图专家 GPE.COM 及秀图专家 SPE.EXE；可以在载入整人专家后再载入 GPE，整人专家就有抓图功能了！

GPE 可以抓下列模式的图形(GPE 目前不提供抓 Super VGA 的图形)。

1. 256 色图形：320 x 200。大部份的游戏都用此模式。

2. 16 色图形：320 x 200，640 x 200，640 x 350，640 x 480。日文 DOS/V 的游戏及 16 色游戏大多用此模式。

3. 特殊 VGA 模式：mode X、320 x 200、320 x 240，及其他游戏作者自订的解析度。如：《毁灭战士 DOOM》、《爆笑躲避球》、《超级卡曼契》、《PINBALL》、《SerfCity》等游戏。

GPE 的使用方法为：

在载入整人专家后再载入 GPE.COM (可 LoadHigh)，语法如下：

```
GPE [!] [path]
```

其中：

参数"!"强迫设定为 mode 13h，当你要抓超级卡曼契的图时，请加上此参数！

参数 [path] 设定 *.GPE 图形文件存放路径，如果空白，则直接存入游戏的目录下。

另外 FPESETUP.EXE 中也有个选项可供选择是否要载入抓图专家，如果有需要，可在载入整人专家时一并载入抓图专家。

下面举个例子说明。

```
C:\>fpe                    //载入整人专家
C:\>lh gpe c:\fpe
```

第二个命令 LoadHigh GPE，并且存放路径文件为 C:\FPE\PIC#00.GPE

载入完了后，在游戏中看到要抓的图时呼叫整人专家，使用 Game screen 功能回到游戏原来的画面，并按下 [G] 键，假如听到"哔"一声，表示图已经抓下来了，按任何键可以回到整人专家；假如听到"哔"两声，可能是有错误。若是磁盘空间不够的问题，请先更正再抓图。

而想要移除时再键入一次"C:>gpe"就可以了。

3.5.2 秀图专家 SPE (Show Picture Expert)

"秀(Show)"图专家 SPE 可以秀出 GPE 抓下来的 PIC#??.GPE 图形文件，其用法为：

```
C:\>spe
```

SPE 是支持鼠标，菜单式的程序，把红棒移到想要看的图形文件上，按[Enter]就可以秀出来了；按[D]（Delete）可以删除该文件；按[R]（Rename）可以更改形文件名（扩展名自动设成 .GPE）；按[Enter]可连续秀出图形文件；按[Esc]离开 SPE。

3.5.3 特殊 VGA 模式说明

有时候游戏设计师为了画面美观，会自己订立一个解析度，如 340 x 200，这种解析度并不是标准的解析度，所以普通抓图程序抓下来可能得到扭曲的画面；抓图专家 GPE 为了解决这种问题，特别储存了特殊资料，故可以抓几乎各种解析度的 VGA 图形。

3.6 AL.COM 自动锁定程序

AL.COM 只支持 FPEMAIN 版本的记录文件，而不支持 FPE32M 版本的记录文件。

AL.COM 是一个会读取 AUTO.FPE 记录档并自动修改游戏的程序；本程序需先载入鼠标驱动程序。只要你先用 FPE 扫描修改一个游戏，并用 File record 功能把表格存成 AUTO.FPE 记录文件，以后只需载入只占用 1k 内存的 AL.COM 就能达到修改这个游戏的目的了。

AL.COM 的呼叫方法和用鼠标呼叫整人专家的方式大致相同，不过把鼠标往左移并同时按下左右两个按键的方法变成载入 AUTO.FPE。AL.COM 必须先载入 AUTO.FPE 才能修改游戏。

1. 把鼠标往左移并同时按下左右两个按键，就可以载入 AUTO.FPE。

2. 直接同时按下鼠标左右两个按键，AL.COM 会自动根据表格，修改目标一次。

想要移除时再执行一次 AL.COM 就可以了。

使用本程序对于会占用大内存的游戏特别有效，例如 Comanche（超级卡曼契）在只有 4MB 的内存下执行，就可以利用本程序进行锁定（此游戏无法自动锁定，必须同时按下鼠标左右两个按键才能修改），玩完所有任务。

3.7 游戏修改实例

以下实例均把 FPESETUP.EXE 中的 "Use FPEMAIN ver" 选项设为 OFF。

3.7.1 Comanche：Maximum Overkill 超级卡曼契

超级卡曼契是由松岗公司在台湾发行的保护模式下的游戏。这个游戏会把键盘完全拦死，所以我们必须使用鼠标来呼叫整人专家。

首先请照着超级卡曼契使用手册，把内存管理程序拿掉重新开机。

接下来直接在 DOS 的提示符号下键入 "C> FPE" 并按下[Enter]。

(FPE 已内定使用鼠标 M1 呼叫，但如果你用了 FPESETUP.EXE 更改鼠标呼叫模式为 OFF，请键入 "C>FPE M1")

接下来请照着超级卡曼契使用手册，进入游戏。

步骤 1

首先我们以卡曼契训练 "Oil Tank Holiday" 任务来开刀。出现驾驶舱画面后先切换武器，可以看到画面左下方 HELLFIRE 有 0008 枚，此时把鼠标往左移(移多一点) 并同时按下左右两个按键，呼叫出整人专家主菜单；选择第一个功能"Scan memory"，然后选择高级扫描 "High Level"，输入 "8" (因为有 8 枚) 按[Enter]，整人专家会把找到的内存个数印在屏幕上，然后按 [ESC] 脱离 Scanmemory，按 [ESC] 脱离整人专家。

步骤 2.

继续游戏故意射出一枚 HELLFIRE，看到画面左下方变成 "0007"，此时再把鼠标往左移并按下左右两个按键，出现整人专家主菜单后，选择第一个功能 "Scan memory"，然后输入 "7" (变成 7 枚了) 按 [Enter]，然后按 [ESC] 脱离 Scan memory，再按 [ESC] 脱离整人专家，继续游戏。

步骤 3.

重复步骤 2. 照目前 HELLFIRE 数输入 8，..7，..6，...等数值，直到整人专家找到的个数变成 0001 时，就可以在 "List ?(Y/N)" 下按 [Y] 跳到功能二"List address"。

步骤 4.

在功能二 "List address" 中直接选择第一个地址 (只有一个地址) 并按下[Enter] 跳到功能三 "View table"。

步骤 5.

在功能三 "View table" 中输入你想要的 HELLFIRE 数目，例如 9999，就直接输入 9999 并按 [Enter]，并输入注释 "FIRE"，按 [ESC] 回到游戏。

步骤 6.

因为这个游戏拦死很多设备，所以整人专家在这个游戏中无法自动修改，我们必须以手动来修改；手动修改的方式是直接同时按下鼠标左右两个按键 (鼠标不用往左移)；所以扫描完毕按 [ESC] 回到游戏后，把鼠标往右移一点，同时按下鼠标左右两个按键，然后再故意射出一枚 HELLFIRE，你就可以看到 HELLFIRE 变成 9998 枚了！以后重新开始新的任务时也要同时按下鼠标左右两个按键，整人专家才会修改你所锁定的目标。

当然，你也可以用 "File record" 功能把找到的地址写成文件，以后再玩这个游戏时只要用 "File record" 功能把文件读回来就不用重找了！

3.7.2 REBEL ASSAULT 绝地大反攻 CD

绝地大反攻 CD 是由美国 LucasArts 授权台湾松岗公司在台湾发行，由于它必须至少 4MB 的内存，而且我们可以在此片 CD 中发现 DOS4GW，EXE 这个文件，所以它是个 DOS Extender 的游戏。如果你只有 4MB 的内存，别忘记用系统盘或上述配置 (别忘了加入 CD－ROM 驱动程序) 开机；键入 "C:>FPE" 按下 [Enter]。

接下来请照着绝地大反攻使用手册载入绝地大反攻。

步骤 1.

等到任务介绍完毕，开始飞行时，可以看到画面下方 "PILOTS 表示目前飞行员有三个人，此时最好按空格键暂停，然后再按右边灰色的 [*] 键，放开，呼叫出整人专家主菜单；选择第一个功能 "Scan memory"，选择高级扫描 (Highlevel) 并且在 "Input work device：" 下直接按 [C] 输入工作磁盘驱动器 C：，(因为 CD－ROM D：不能写入)，然后输入 "3" (因为飞行员有三个人) 按 [Enter]，整人专家会把找到的个数印在屏幕上，然后按 [ESC] 脱离 Scan memory，按 [ESC]脱离整人专家。

步骤 2.

继续游戏故意去撞墙，等爆炸重来后可以看到画面下方 "PILOTS "表示目前飞行员剩下两个人，此时再按空格键暂停，按右边灰色的 [*] 键再放开，出现整人专家主菜单并选择第一个功能 "Scan memory"，然后输入 "2" (因为飞行员剩下二个人) 按 [Enter]，然后按 [ESC] 脱离 Scan memory，按 [ESC] 脱离整人专家，继续游戏。

步骤 3.

重复步骤 2. 照目前飞行员人数输入 3，2，1. 等数值，直到整人专家找到的个数变成 0001 时，就可以在 "List ? (Y/N)" 下按 [Y] 跳到功能二"Listaddress"。

步骤 4.

在功能二 "List address" 中直接选择第一个地址 (只有一个地址) 并按下[Enter] 跳到功能三 "View table"。

步骤 5.

在功能三 "View table" 中输入你想要飞行员的数目，例如 5，就直接输入 5 并按 [Enter]，并输入注释 "PILOTS" 就完成修改啦！

按 [ESC] 回到游戏中玩一阵子后你就会发现飞行员一直都是五个人，死不完啦！

当然，你也可以用 "File record" 功能把找到的地址写成文件，以后再玩就不用重找了！

> 注意!! 绝地大反攻是个动作型的 CD－ROM 的游戏，欲呼叫整人专家时请先按暂停，否则不要中断游戏时间太久，以免发生不可预期的后果。

3.8 FPE 4.0 使用中的问题与解决

3.8.1 Super VGA 卡问题

SVGA 状态栏显示的是您的 SVGA chip 的名称，如果是 "normal VGA"，表示整人专家无法辨认您的 SVGA 卡，将使用标准 VGA 模式；您可以在载入整人专家之前先挂入您 SVGA 卡的 VESA 驱动程序，那么整人专家侦测到 VESA 标准后会显示出 "VESA Standard"，就可以使用于 SVGA 的模式了！

3.8.2 鼠标问题

整人专家支持较新版的鼠标驱动程序，所以如果您玩游戏时有发现呼叫整人专家后，鼠标光标会消失或不正常的移动时，请更新您的鼠标驱动程序，或者直接使用 MS－DOS 所附的 MOUSE.COM 驱动程序。

3.8.3 找不到目标

可能原因是储存数据的方式不一样，虽然大部份的数据都是依十六进制排列，但也有其它的排列方式，如时间的 BCD 排列、十进位制排列、十位数和个位数分开排等多种排法，这是属于资料结构的范围，笔者建议您参考资料结构相关书籍。

3.9 FPE 4.0 使用中各种错误信息及警告信息

Your config changed! Please re－run INSTALL.EXE!!
您的配置改变了，请重新执行 INSTALL.EXE。

Error!!I can't find FPEDATA.DAT, please re－run INSTALL.EXE!
您的 FPE 目录改变了，请重新执行 INSTALL.EXE。

MOUSE DEVICE not install!
找不到鼠标驱动程序，鼠标呼叫功能关闭。

Fix People Expert has installed !!
整人专家已经载入，想要移除时请键入 "fpe r"。

Fix People Expert can't be removed, NOW !!
整人专家现在不能被移除，请先移除后来载入的常驻程序。

WARNING!! BIOS only !!
你可能没有载入任何内存驱动程序，Load/Save *.FPE 自动计算正确地址的功能及 X 参数的功能会失效，请至少载入 HIMEM.SYS。

WARNING!! EMM too old!!
你可能用的是附在 DOS 5.0，DOS 6.0，Windows 3.1 的旧版 EMM386.EXE，Load/Save *.FPE 自动计算正确地址的功能及 X 参数的功能会失效，请改用 DOS 6.2 的 EMM386.EXE 或者是 QEMM386 或者干脆只用 HIMEM.SYS 就好了。

WARNING!! Address is over 32M, maybe I will miss some target !!
你可能内存太多了，以至于超过 FPE32M 的定址能力，请移除一些会占非常多 XMS 的程序，如 Cache，虚拟磁盘等，并且用 Xn 参数叫 FPE32M

帮你吃掉一点内存。(内定的 X4 应该就足够了)

WARNING!! XMS isn't continuous, you maybe should REBOOT your PC!

你可能在载入 FPE32M 前做了太多 XMS 的操作,以致 free XMS 不连续,请重新开机,尽快载入 FPE32M,尽快执行游戏。

3.10 重要游戏使用 FPE 提示

3.10.1 DOOM (毁灭战士)

DOOM 是个比较特殊的游戏,它每一关卡都会重新读数据到内存,也就是说 DOOM 每过一关,储存健康值的地方就会变动,所以如果您想要一直无敌呢,就要每过一关就重新找一次健康值才行。

3.10.2 Ⅱ 轩辕剑

轩辕剑Ⅰ也是比较特殊的游戏,它在战斗时会检查经验值,也就是说它的经验值不能被锁定!所以当您找到经验值地址时,请用 [S]witch 功能把他设成不自动锁定,然后按"右边灰色的 [+] 键"来修改经验值,再去战斗,就可以升级了。

其它的体力和法力是可以被锁定的。

3.11 重要参考资料

3.11.1 如何判断 一般游戏 或 DOS/4GW 的游戏

DOS/4GW 的游戏会需要 4MB 以上的内存,而且通常在一开始时出现 DOS/4GW 或是 DOS/16M 的如下版权宣告画面。

```
DOS/4GW Protected Mode Run—time Version X.XX
Copyright (c) Rational System, Inc。1990—xxxx
```

其他如毁灭战士,Raptor 一开始有各项资料的初始画面时,也是 DOS/4GW 的游戏。

目前 DOS/4GW 的游戏有:

- 绝地大反攻 CD
- 极道枭雄
- DOOM (毁灭战士)
- Shadow Caster (救世圣主)
- Sim City 2000 (模拟城市 2000)
- Raptor

- UFO
- 真人快打
- Serf City

等等。

Comanche（超级卡曼契）虽然是保护模式的游戏但它并不使用 DOS/4GW！如果自行选择版本时，请用 FPEMAIN 版本配合鼠标下呼叫来修改它。

日文 DOS/V 目前并未出现使用 DOS/4GW 的游戏。

如果您无法确定某游戏是否要用 DOS Extender 时，不妨用 FPE32M 版本找找看，FPE32M 会帮助你判断是否为 DOS Extender 的游戏 并且自动设定扫描范围。

下面我们给出只有 4MB RAM 的多重系统配置范例，供读者参考。

```
[menu]
menuitem=HIMEM, Only HIMEM.SYS
.....
[HIMEM]
DOS=HIGH
DEVICE=C:\DOS\HIMEM.SYS
DEVICE= (CD-ROM 驱动程序或网路驱动程序)
SHELL=C:\COMMAND.COM /P

[...]
....
```

上面的范例中并没有载入内存管理程序，或许您会疑惑的说"如果游戏需要 EMS 怎么办?"，请放心，一个真正的 DOS Extender 的游戏（特别是 DOS/4GW 的）是不需要任何内存驱动程序的，包括 EMS、XMS、VCPI、DPMI 内存程序，如果您在游戏说明书发现要求需要 EMS 或 XMS 的话，那笔者认为，这如果不是个 DOS Extender 的游戏就是说明书写错！笔者发现市面上有不少的说明书写错了，

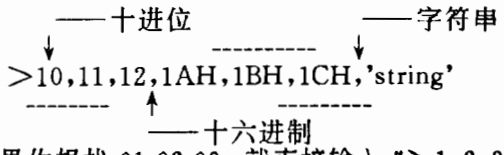
可参考笔者在上面所列的 DOS/4GW 游戏，都是连 HIMEM.SYS 都可以不用载入就能执行的游戏。

3.11.2 技术资料

1. 扫描字串语法

这个字串的语法是类似「汇编语言的资料定义方式」；字串中字节（或字符）之间请用「逗号」分开；十进制的数值请直接输入，十六进制的数值请在数值后面加一个"H"，字符串请用「'字符串'」这种格式。

举个例子：



如果你想找 01 02 03，就直接输入"＞1,2,3"就行了。

因为程序设计师通常都会把性质类似的数值放在数组里，如属性啦、物品啦，而数组又是连续排列的，所以这个功能将会相当有用。你又可以用[F1]切换 byte 或 word，以扫描字符数组（char：1 byte）或整数数级（int：1 word）。

2. 扫描原理

一个游戏通常有很多相同的数据，整人专家的 Scan 功能就是把和您输入相同数据地址放入缓冲区，再根据您多次输入的值，过滤找出最可能之地址。

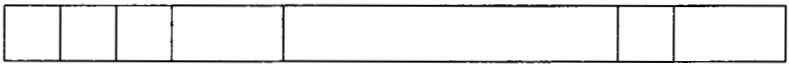
3. FPE32M 的工作方式

DOS Extender 的工作方式是把 GAME 本身完全放在 1MB 内存以上，而 DOSExtender 本身则放在基本内存中；由于 DOS Extender 并不会很庞大，所以通常基本内存都还剩下许多未使用，这也就是为什么 DOS Extender 通常只需要四百多 K 的基本内存就能执行的原因；所以 FPE32M 就完全不占 XMS，空出最大空间给 Game 执行，而把自己放在基本内存，占 22kB。

4. 抓图程序支持

整人专家 4.0 增加了抓图接口，只要用"Game screen"功能回到游戏原来的画面，按下[G]键，整人专家会呼叫中断 61h (int 61h)；因此只要写个抓图程序拦截中断 61h 即可，不需要再写呼叫热键及拦截技巧，而且不用考虑 INDOS(DOS 函数重入）及转换 DTA 的问题！你只需要把 VIDEO RAM 写成文件就能写出自己的抓图程序了！

5. *.GPE 文件格式



3 1 1 26 320x200 or 640x480 or .... 17 256x3 bytes

：辨识字符串 'GPE'。3 bytes

：VGA BIOS 显示模式：mov ah，0fh int 10h bh＝显示模式，如 320 x 200x 256 色时为 13h。1 byte

：是否为连续定址：连续定址＝' '；不是连续定址＝'X'。1 byte 如

'GPE',13h,' ' 为 标准 320 x 200 x 256 色。
'GPE',13h,'X' 为 mode X 320 x 270 x 256 色 4 页。

: CRTC 0－18h 暂存器 + 杂项输出暂存器：回复原游戏模式用的。26 bytes

: 未压缩影像资料：连续定址时直接由 A000:0000 抓到 A000:FA00;不连续定址时，先存层面 0，然后层面 1..2..3。如 mode 12h,先层面 0 640 x 480 / 8 (因为每点 1 bit，8 点 1 byte),然后层面 1 640 x 480 / 8，层面 2...层面 3....。Mode X 大小均为 320 x 270。

: 16 个色盘值及一个过扫暂存器值：17 bytes，256 色图形无此栏。

: 256 色彩值：每个 3 bytes，共 256 x 3 bytes，16 色图形也有此栏，DOS/V 图形 "可能" 也会修改色彩暂存器。

第四章 游戏工具 GAMETOOLS 3.22

游戏工具 Game Tools 3.22（下称 GTS）是由香港软件专家 Wang WingKin 研制的，在内地占有一定的用户，其最新版本在性能上有了一个较大的提高。

4.1 GTS 的运行要求与启动

4.1.1 GTS 的运行要求

1. 内存

要求基本内存

G3.EXE(只用基本内存)	76208B
G3X.EXE(只用扩展内存)	2784B
G3E.EXE(只用扩充内存)	11696B

> 注意：由于机器配置不同，上面数据稍有区别。

2. CPU 为 386 以上的处理器。

4.1.2 GTS 的启动

在 DOS 提示符下键入 G3，则出现下面的四行信息：

```
GAME TOOLS Version 3.22N3 30/12/93
Copyright (C) 1990,91,92,93. by Wong Wing Kin. All Right Reserved.

Hot Keys－[PrtSc＊] to Pop up GAMETOOLS.
          [ALT－PrtSc＊] to stop the game and restore other POP－UP program
```

若在 DOS 提示符下键入 G3X，则出现下面的四行信息：

```
GAME TOOLS Version 3.22X3 30/12/93
Copyright (C) 1990,91,92,93. by Wong Wing Kin. All Right Reserved.

Hot Keys－ [PrtSc＊] to Pop up GAMETOOLS.
          [ALT－PrtSc＊] to stop the game and restore other POP－UP program
```

若在 DOS 提示符下键入 G3E，则出现下面的四行信息：

```
GAME TOOLS Version 3.22E3 30/12/93
Copyright (C) 1990,91,92,93. by Wong Wing Kin. All Right Reserved.

Hot Keys－ [PrtSc＊] to Pop up GAMETOOLS.
          [ALT－PrtSc＊] to stop the game and restore other POP－UP program
```

也就是说，G3、G3X、G3E 的热键都是一样的，只是，它们占用内存方式不同而已。

4.2 GTS 的使用

4.2.1 热键

按[PtrScr＊]键(即同时按下 PrtScreen 和＊键)弹出 GAMETOOLS。

[ALT]＋[PtrScr＊]暂停游戏，恢复所有中断，以便弹出在 GAMETOOLS 之前装入的程序。

4.2.2 输入数字的方式

1. 十六进制数字必须在数字前加“$”。

2. 可使用简写 CPU 的寄存器代码，因为 GAMETOOLS 可识别 CS、DS、ES、SS、PS(PSP)、AX、BX、CX、DS、SI、BP、SP。

3. 在输入地址时按[TAB]可弹出地址表供选择。在分析列表和内部调试器时按[TAB.将保存高亮度光标所在的地址到地址表。

4.2.3 各选项介绍

当您按[PrtSc＊]热键时，将在屏幕弹出如下画面。

GAME TOOLS Version 3.22E3 30/12/93 Written by Wong Wing Kin
AX=1100 BX=0392 CX=0001 DX=0001 SP=2000 BP=2222 SI=200 DI=2000 DS=2000 ES=2000 SS=2000 CS=2200 IP=2220 FLAGS=odItsZaPc PSP=DA12

MAIN MENU

[A] Global Analysis	[T] Hardware Break Point
[V] Internal Debugger	[D] External Debugger
[K] Keep Memories Contant	[I] Interrupt Monitor
[E] User Screen	[B] Restore Keyboard & Video
[S] DOS Shell	[Q] Quit to DOS
[C] Clock Frequency	[U] Uninstall

ESC — Abort & Exit

在画面的最上面显示出 GAME TOOLS 的版本信息、版权信息及 CPU 各个寄存器的数值。

在画面的下面显示了 GAME TOOLS 的主菜单(MAIN MENU)。若按 ESC 键则退出该画面。下面我们对该画面中提到的各个菜单项进行详细解释。

1. [A]Global Analysis(全局分析)

根据您的指定找出内容增加或减少的地址。它用于查找游戏中“生命值”

或“功力值”存放的地址。

它有二个子功能。

[B] 字节分析

[W] 字分析

要找出地址至少要分析二次。例如，要找存放“生命值”的地址，在主菜单中选择 [A]，然后输入 GAMETOOLS 存放临时文件的路径。退出 GAMETOOLS 继续游戏直到“生命值”减少。按[Ptrscr *] 弹出 GAMETOOLS 再次分析。至少重复二次后，选择菜单中的[L]列出全部找到的地址。如果不是严格减少，在每次分析时可用箭头键选择[increase]或[decrease]，然后按回车开始分析。

子功能[L]列出分析得到的地址。

通过二次分析就可能得到结果。您可用箭头键前后查看地址，然后按[TAB]键将当前光标所在的地址存入地址表。

分析结果的格式如下：

分析的次数；第一次是 0。只保存最近的 20 次。

	V	V	V	V	
ANALYSIS	03	02	01	00	←第一次
1234:0012	13	12	10	09	←每次分析的内容
1234:0019	31	30	2F	20	

↑

找到的地址

分析后，可能找到的地址不止一个。选择一个最有可能的地址，然后用功能[V]检验内容看是否确实是您想找的那一个。

子功能[K] 将当前光标条所在的地址存放在 KEEP 列表中。字节分析存放 1 字节，而字分析存放 2 字节。

子功能[A] 在当前地址设置硬件中断。一旦游戏修改该地址的内容，GAMETOOLS 将自动弹出并且询问您是否将游戏修改为不死。（它将该代码改为若干个 NOP 指令。）

子功能[R]初始化分析过程并忽略前面的结果。

2. [T]Hardware Break Point(硬件中断点设置)

用于找出修改您指定地址的内容的代码。首先输入一个地址，然后回到游戏。一旦游戏试图修改该地址的内容，GAMETOOLS 将自动弹出并且告诉您改变该内容的代码地址。还可用于跟踪游戏，直到该地址的内容被改为指定值。该功能可用于找出游戏中修改“生命值”或“功力值”的代码。

对于 386 的 4 个调试寄存器有下列的子功能：

· 子功能[0]

表示内存执行方式。当 CPU 执行到断点地址时，GAMETOOLS 中断游戏并弹出。

· 子功能[1]

表示内存写方式。当 CPU 写到断点地址时，GAMETOOLS 中断游戏并

弹出。

· 子功能[2]

表示内存读或写方式。当 CPU 读/写断点地址时,GAMETOOLS 中断游戏并弹出。

· 子功能[3]

表示内存写并且减少。当 CPU 改变断点地址的内容为更小的值时,GAMETOOLS 中断游戏并弹出。

· 子功能[4]

表示内存写并且改变:当 CPU 修改断点地址的内容为不同的值时,GAMETOOLS 中断游戏并弹出。

· 子功能[5]

表示内存写并且增加。当 CPU 修改断点地址的内容为更大的值时,GAMETOOLS 中断游戏并弹出。

· 子功能[6]

表示内存改变为某一值。当 CPU 改变断点地址的内容为某一指定值时,GAMETOOLS 中断游戏并弹出。

对于子功能[0]到[2],必须输入断点地址的大小。大小可以是 1,2,4。如果断点大小为 4,则在程序计数和断点地址比较时,相对不重要的 2 位将被忽略。

另外,Auto modify(自动修改)的功能可在当前地址放置硬件断点。一旦游戏修改该地址的内容,GAMETOOLS 自动弹出并询问是否修改游戏为不死。它将该代码改为若干个 NOP 指令。

注意:断点 0 可能被 GAMETOOLS 本身使用。

3. [V]Internal Debugger(内部调试器)

该功能很容易使用。可用箭头键、PgUp、PgDn、Home、End 前后左右移动查看内存地址的内容。

汇编码以不同的颜色显示。

下面是各按键的功能:

U 在 HEX/ASCII 代码和汇编代码之间切换。

F 查找字符串。可以是十六进制串,或字符串,但长度最长为 16 字节。

N 找下一个匹配的串。

C 改变查看地址。

T 单步跟踪。

P 每次执行一个指令码。它不跟进 'CALL', 'INT', 'LOOP' 等指令内部。

H 运行到光标所在地址。

R 改变寄存器内容。

L 装入程序进行调试。请不要在运行另一程序时使用该命令。

S 保存部分内存到一个文件。

Tab 将光标所在的地址存入地址表。

E 看用户屏幕。

4. [D]External Debugger(外部调试器)

GAMETOOLS 执行 INT3 转到在游戏之前装入的 Debug 或 SYMDEB 中。

子功能[3]转到 DEBUG。首先,在 DOS 下装入 DEBUG,然后在 DEBUG 中装入并执行 GAMETOOLS。接着,装入 COMMAND.COM 并执行。现在可以进入游戏了。当使用子功能[3]转到 DEBUG 后,你可以反汇编在跟踪时找到的代码,修改代码看看效果。

> 注意:现在你仍然在 GAMETOOLS 内部,并且寄存器内容没有改变;如果用 Q 命令退到 DOS,系统将死机。完成修改后,输入 G 返回到 GAMETOOLS。

如想在您中断的地方跟踪游戏,请选择子功能[4],它在当前中断的位置调试游戏,这样在退出 GAMETOOLS 时将返回到 DEBUG,你可使用 DEBUG 的跟踪功能进行跟踪。但如果你在执行 DOS 功能时按[PtrScr *],有时可能在该点生成 INT3。这是因为 DEBUG 再次调用 DOS 功能引起 DOS 重入。

子功能[0] 用于恢复 INT3 地址为在 GAMETOOLS 第一次装入时的地址。有时游戏可能改变了 INT3 的地址避免你设断点。

子功能[1]在 INT3 最近改变的地址和当前地址之间切换。

5. [K]Keep memory constant(保持内存数据不变)

指定地址和其值后,GAMETOOLS 将周期性地写该地址的内容,使其值保持不变。最多可指定 9 个地址。0000:0000 表示没有指定地址。

当难以找到修改"生命值" 或"动力值"的全部代码时,这功能是很有用的。你可先用[A] 分析找出"生命值"地址。然后,用[K]使该地址的内容不变。这不需要任何汇编语言的知识。

6. [I]Interrupt monitor(中断监控)

当调用你指定的中断时,GAMETOOLS 自动弹出。在弹出时 GAMETOOLS 显示在中断调用前和后的各寄存器内容。

选择该选项后,要求输入要监控的中断号,然后确定从 DOS 调用该中断时是否跟踪。如果你要求条件跟踪,即只有寄存器的内容满足指定条件时才弹出 GAMETOOLS,那么你可以输入各寄存器的内容,这样当寄存器值与你输入的值一致时,GAMETOOLS 将弹出。输入[*]表示全部匹配。例如输入 AH=0 时,GAMETOOLS 将只在执行 INT 之前 AH=0 时弹出。

7. [E]USER Screen(用户屏幕)

查看用户屏幕。

8. [B]Restore Keyboard & Video(恢复键盘和显示状态)

它有如下子功能:

· 子功能[0]

恢复 INT8、9、16 为在 GAMETOOLS 第一次装入时的中断地址,并将

显示方式改为文本方式。

· 子功能[1]

将 INT8,9,16 和显示状态改为上次用[Debugging]－[Debug the game]功能保存的地址和状态。当使用[Debug the game]功能时用 GAMETOOLS 改变并保存键盘和显示状态，以便你可用键盘或屏幕进行调试。如你想继续游戏，请使用该功能恢复键盘和显示为最近保存的状态。

9. [S]Shell to DOS(转到 DOS 外壳)

> 注意：在使用该功能时，不要改变各驱动器的当前目录，否则游戏可能找不到相关文件。

有时，由于 GAMETOOLS 和游戏有冲突，系统可能会死机。

10. [Q]Quit to DOS(退出游戏回到 DOS)

有时，由于 GAMETOOLS 和游戏之间有冲突，系统可能会死机。

11. [C]Change the frequency of clock(改变时钟频率)

也就是改变 INT8 的中断发生次数。

当前频率显示在屏幕上方。

子功能[0]将频率改为 0。

子功能[1]将频率改为正常(18.2Hz)。

子功能[2]将频率改为你输入的值。

该功能用于改变游戏的速度。通常，增加频率将增加游戏的速度。

12. [U]Uninstall GAMETOOLS(卸下 GAMETOOLS)

如果在 GAMETOOLS 之后装入了其它 TSR 程序，将不能卸下 GAMETOOLS。请首先卸下

GAMETOOLS 之后装入的 TSR 程序。

4.2.4 利用 GAME TOOLS 修改游戏为不死版

GAME TOOLS 的强大功能使修改游戏为不死版成为十分容易的事情。本节将给出具体操作方法。

1. 驻留 GAME TOOLS。

2. 运行游戏。

3. 按[Prtsc＊]调出 GAME TOOLS，选择“Global Analysis”(全局分析)，根据需要选择分析字节或字，同时确定临时文件存放的目录，然后按 ESC 回到游戏。

4. 当“生命值”发生变化时，再次调出 GAME TOOLS，并使用全局分析功能，这时屏幕提示：

> [D]ecrase[N]O Change [I]ncrease [E]xtract [L]isting [R]eAnalyse

根据实际情况确定是 D(减少)、N(没有改变)、I(增加)或 E(输入精确

值)。

分析完成后，可能找到的值不止一个，这时，可重复该步骤直到只剩下一个地址。也可以选一到三个您认为最有可能的地址。

5. 使用 Internal Debugger(内部调试器)功能修改所选地址的内容，看看这里是否有您真正要找的地址。

6. 使用 Hardware Breakpoint 功能在找到的地址处设置硬件断点。GAMETOOLS 允许设置三个硬件断点（另外还有一个由 GAME TOOLS 本身使用)，输入"生命值"地址，中断方式一般选择"Write"方式即可。甚至断点后回到游戏。

7. 当"生命值"再次发生变化时，看看是否自动调出 GAME TOOLS。若没有，说明您所确定的地址有误，应再次分析。若发生了中断，看看是哪个地址发生了中断，发生中断的地址就是您要找的地址。

8. 使用内部调试器功能进行反汇编，并调试游戏。

4.2.5 注意事项

GAMETOOLS 不能在 DV 下运行。如果在 GAMETOOLS 后装入 DV，则在 DV 运行时 GAMETOOLS 不能激活。执行完 DV 后，可使用 GAMETOOLS。

如果在 DOSPRMPT. PIF 中放置了 EMS 内存锁，那么可以在 WINDOWS3. 1 的 DOS 提示符下运行。在 WINDOWS3. X 下，不能使用硬件断点功能。

4.3 GAME TOOLS 两个实用工具

4.3.1 TSRCrack 1.00 使用说明

TSRCrack 是一个用于破解软件保护(如口令保护)的 TSR 实用程序，它还可以用于修改游戏使游戏更容易完成。

为什么不直接修改文件呢？这是因为文件经常被压缩和加密，不能还原和修改。这时你就需要有一个 TSR 程序去修改文件被调入内存后的代码。

该程序可根据给出的有关在哪里和如何修改代码的信息，生成一个 TSR 程序。

当您在 DOS 提示符下输入 TSTCRACK 时，将在屏幕上出现如下信息：

```
TSTCRACK Version 1.0 10/02/93—TST Generator
Copyright (C) 1993. by Wong Wing Kin. All right reserved.

Usage: TSRCRACK <Infile> <OutFile>
```

其中 Infile 的输入文件格式如下所示。

```
[program <startup program name> ]
int <which interrupt to hook>
```

```
<conditions>?

<conditions> :- if <segreg>:<seg offset>:<offset>:<codes>
                (then <segreg>:<seg offset>:<offset>:<codes>)?
<segreg> :- ds | es | cs | ss
<seg offset> :- signed/unsigned hex numbers (word)
<offset> :- unsigned hex numbers (word)
<codes> :- space separated hex numbers (byte)
```

其中：? 表示 1 或更多的次数。

[] 表示任选。

例如我们要破解 INDARK 的口令，可输入如下的内容。

```
program tatou.com
int 21
if cs:0000:25bc = 3b 86 d0 fd 75 28 a0 8e
then cs:0000:25c0 = eb 1a
```

上面的程序将截获 INT21。每次调用 INT21，它将检查在地址 CS+0000:25bc 的字节序列是否为 3b 86 d0 fd 75 28 a0 8e。如相等，则改变 CS+0000:25co 为 eb 1a。

4.3.2 UNP 4.10 使用说明

1. UNP 帮助屏幕

UNP 是个通用的被压缩运行程序还原工具。它有许多命令和选项，它们都以“－”开头。不带参数运行 UNP 可得到命令和选项的简要说明，如下显示：

```
usage: UNP command [options] [[d:][\path]Infile] [[d:][\path]Outfile]

c = convert to COM file                    m = MarkEXE, insert a file in header
d = make current options default           o = copy overlay
e = expand compressed file (default)       s = search for compressed files
i = show info only                         t = trace executable
l = load and save                          x = convert to EXE file

-? -= help (this screen)                   -l-= use large memoryblock
-a-= automatic retry                       -m-= MORE alike output
-b-= make backup .BAK file of original     -n-= numbered Outfiles
-c-= ask for confirmation before action    -o-= overwrite output file if it exists
-f-= optimize fixups (like HDROPT.EXE)     -p-= align header data on a page
-g-= merge overlay into image              -r-= remove overlay data
-h-= remove irrelevant header data         -u+= update file time/date
-i+= interception of I/O interrupts        -v-= verbose
-k+= [-|+|?] pklite signature handling     -- = program's commandline
```

2. UNP 命令用法

UNP 的命令长度必须为一个字符，但可放在任何位置。默认命令是 E。各命令的用法如下：

· C－转化 COM 文件

有些.EXE 文件可转化为.COM 文件。但转化结果并不自动带.COM 扩展名。只有你确切知道其原理时才能转化文件。

· D－ 设置默认命令。

将当前指定的命令设置为默认命令。

例如要让 UNP 永远建一备份，使用下面的命令：

```
UNP D －B+
```

· E － 还原压缩文件(默认)。

如果用该选项但不带文件名，将还原当前目录下的全部压缩文件。

· I－ 显示信息。

UNP 象 E 命令那样显示全部信息但不还原。

· L－ 装入和保存。

该命令装入.COM 或.EXE 文件但不展开。它将与还原文件一样被写回。

当你想去掉覆盖部分，无关的头部数据或优化重定位项时非常有用。

· M MARKEXE，在文件头部插入一个文件。

MARKEXE 是由 PROTECT! EXE/COM V5.0 提供的实用程序。用该选项在 EXE 文件中加入一段文本，当文件在屏幕上显示时可看到那段文本。'M' 命令其实与 MARKEXE 不完全相同。首先，它在重定位项之前插入，这样在重定位项中的结束标记(EOF)不会影响它。其次，UNP 不在代码的结尾入放相同的文本，因此它或多或少地会受影响。

· O－ 拷贝覆盖部分。

用该命令可以从一些.EXE 文件中取得覆盖部分并将它加到一些其它的.EXE 文件中。当用 LZEXE 压缩时，它会删除文件覆盖部分。用该命令可将覆盖部分加回去。

· S－ 查找压缩文件。

UNP 自动查找压缩文件进行处理。为节省屏幕空间，UNP 不显示路径名。由于 UNP 不循环查找，因此不应成为问题。

· T－ 跟踪可执行文件。

单步跟踪程序的执行。

· X－ 转化为 EXE 文件。

有些压缩工具(如 LZEXE)只能压缩.EXE 文件。用该命令可将.COM 文件转化为.EXE 文件。

> 注意，结果文件不会默认带.EXE 扩展名存效。在进行.COM 和.EXE 转化时，你应知道其原理。但不是所有程序都能转化。

UNP 除了命令参数外，还有许多选项，它们可以单独写(如－A －B －C)；也可以连在一起(如－ABC)。每个选项后可跟字符“－”，“＋”或“?”。“－”表示关，“＋”表示开。而“?”强迫 UNP 询问(要求你证实)，目前只有－K

选项支持。如选项后不带字符表示切换，即使用第二次将放弃前一次(如－A－A 没有影响)。但一旦用"?"设置了一个选项，你可用后跟'－'来关掉它，如(－A－)。

3. UNP 的各选项

各选项的用法如下：

－?　帮助。显示各命令和选项的简要功能

－A　自动重试。当要还原由 CPAV 免疫的文件时有用。

－B　为原文件作备份(.BAK 文件)。

－C　在动作前要求证实。这将强迫 UNP 询问你是否确实清除由 UNP 在文件中找到的例程。

－F　优化重定位项(类似于 HDROPT.EXE)。—EXE 文件头中的重定位项由二部分组成：16 位段址和 16 位偏移。由于 DOS 只使用 20 位地址，重定位项中包含有冗余数据。通过优化尽可能将地址作为偏移而段值为 0。这与 PKLITE 所提供的 HDROPT.EXE 是一样的。

－G　合并覆盖部分为影像文件。它将覆盖部分并入一个.EXE 文件。一般不需要用。

－H　删除无关的头数据。许多连接程序在.EXE 文件头加入了无用数据。它可删除这些无用信息，从而压缩文件头部大小。它还象 PKLITE 一样跳过文件头重建代码。

－I　I/O 中断异常(interception)

通常 UNP 检查几个 DOS 中断看看是程序是否正常运行。如果发现有异常调用，UNP 将放弃处理。如果有 TSR 驻留，可使用该选项。

－K　PKLITE 标志处理，有三种可能：

－K－不加 PKLITE 标志。如果只用－K(保持 DISLITE 兼容)，也将是这种情况。

－K＋永远加 PKLITE 标志。这是 UNP 的默认情况。

－K?　这时，每次 UNP 发现一个标志都将询问你是否加。

－L　使用大内存块。当 UNP 装入程序时，为安全起见，它将分配比实际要求大 32K 的内存。

有些程序实际要求的内存可能比它告诉 DOS 的多得多。如果 UNP 要还原这样的文件肯定会出错。这时可能会出现二种情况。程序发现内存不够，试图通知用户，导致"(INT21) Uexepeeted call to DOS"错误，并且 UNP 终止。更坏的是，程序不进行检查，继续还原，这可能导致系统蹦溃或内存分配错。如果你要处理的文件，该文件需要的内存比它告诉 DOS 的要多，这时用该选项。

－M　类似于 MORE 的输出。用该选项后，信息满屏后暂停。

－N　输出文件编号。用于给输出文件编号。若文件已编号，它将往后编。否则编号为 1。

－O　如果输入文件已存在，则覆盖。如果用该选项，UNP 将不提示你证实是否要覆盖。

－P　文件头数据以页对齐。也就是文件头大小是 512 字节的整数倍，这样装入时速度可更快些。

—R　删除覆盖数据。这将删除附加在文件后面的数据。这可能会删除有用数据。

—A　更新文件时间/日期

通用 UNP 不改变目标文件的时间和日期。用该选项将时间和日期改为当前时间或日期。

—V　详细。用该选项，UNP 将给出一些附加的信息。它主要用于调试。

——　程序命令行。该选项之后的内容将被传送到被解压的程序。这样你就可以带任何所需要的参数(象口令)作为跟踪命令。

4. UNP 修复的错误

UNP 能修复的错误有：

- COMPACK V4.4 486 死机
- EXEPACK 的"PACKED FILES CORRUPT"错误
- PKLITE V1.00a
- SHRINK V1.00

5. UNP 还原的压缩程序

UNP 能还原的有：

- AINEXE V2.1
- ANTIBODY
- AVPACK V1.20
- AXE V2.2
- CENTRAL POINT ANTI—VIRUS V1, V1.1
- COM2CRP V1.0
- COMLOCK V0.10
- COMPACK V4.4, V4.5
- CRYPTA V1.00
- CRYPTCOM
- DELTAPACKER V0.1
- DIET V1.00, V1.00d, V1.02b, V1.10a, V1.20, V1.44, V1.45f
- ENCRCOM V2.0
- EPW V1.2, V1.21, V1.30
- EXELITE V1.00aF
- EXEPACK V4.00, V4.03, V4.05, V4.06
- F—XLOCK V1.16
- ICE V1.00
- IMPLODE V1.0 Alpha
- KVETCH V1.02a
- LINK /EXEPACK V3.60, V3.64, V3.65, V3.69, V5.01.21
- LZEXE V0.90, V0.91, V1.00a
- MCLOCK V1.2, V1.3
- MEGALITE V1.18a, V1.20a
- OPTLINK
- PACKEXE V1.0

- PASSCOM V2.0
- PGMPAK V0.13, V0.14, V0.15
- PKLITE V1.00a, V1.00, V1.03, V1.05, V1.12, V1.13, V1.14, V1.15, V1.20
- POJCOM V1.0
- PRO－PACK V2.08, V2.14
- PROCOMP V0.82
- PROTECT! EXE/COM V1.0, V1.1, V2.0, V3.0, V3.1, V4.0, V5.0
- SELF－DISINFECT V0.90a
- SHRINK V1.0
- SCRNCH V1.00, V1.02
- SYRINGE
- TINYPROG V1.0, V3.0, V3.3, V3.6, V3.8, V3.9
- TURBO ANTI－VIRUS V7.02A
- USERNAME V2.00, V2.10, V3.00
- WWPACK V3.00, V3.01

6. UNP 无法还原的程序

UNP 不能还原的：

- SPACEMAKER V1.03
- EPW V1.2, V1.21, V1.30, EXE only

第五章 解拆大全 CM386

CM386 是一种基于 DOS DEBUG 的游戏软件解拆工具，对于汇编语言比较熟悉的用户来说，它是十分优美的游戏工具。

本章将介绍现今流行较广的 CM386 V1.0 和 V2.0，希望读者能对该工具软件有一个深入的了解。

5.1 CM386 由来

CM386 V1.0 的全称是 CRACKMATE V1.0，它是 Computing Age Publisher 于 1992 年 3 月出版发行的。

5.1.1 CM386 V1.0 的系统要求

因 CM386 V1.0 是一种基于 DOS DEBUG 程序的游戏工具，因此，它对计算机的系统资源的要求是：

- 386 以上的 CPU。
- VGA 以上的显示器。
- DOS 版本要求在 3.0 以上。

5.1.2 CM386 V1.0 的内存占用

CM386 的源程序全部采用汇编程序编写，其文件长度仅有 10 多 KB，对基本内存的占用小于 10KB，并且不占用任何扩充内存或扩展内存，这一点要比 GB4 强，GB4 占用 11KB 的基本内存和 180～250KB 的扩展内存。

5.2 CM386 V1.0 的使用

5.2.1 CM386 V1.0 功能介绍

若要充分发挥 CM386 的全部功能，首先用如下方法装入 CM386 及游戏程序(例如：西洋封神榜 GODS)。

```
C:\>DEBUG CM386.EXE
-G <ENTER>                    ; CM386 驻留程序
```

```
Crack Mate
Version 1.00
Copyright (C) 1992
by ChanWaiWong Wilfred
All Right reserved.
```

这里执行 CM386.EXE 的结果

```
Program terminated normally
```

```
-N GODS.EXE <ENTER>        ; 游戏程序名
-L <ENTER>                 ; 装载游戏
-G <ENTER>                 ; 启动游戏
```

此后就可在游戏中可随时用 NUMLOCK 键激活 CM386。

CM386 的主菜单显示如下：

Main Menu
0. Data analysis
1. Start another analysis
2. List address
3. Hardware breakpoint
4. Return to Debugger
5. Return to game

下面对上面的各个菜单项作分析。

1. Data analysis(数据分析)

在该菜单项中有两个选择：Increase(增加)或 Decrease(减少)。我们在分析时一般选择减少，例如，生命数、体力、能量等。。在游戏过程中都是下降的，经过数次分析，就可以得到地址。也许分析出的地址不止一个，则选择与分析数最为接近的一组数据的地址。

2. Start another analysis(重新进行分析)

选择该菜单项后，清除已有的分析结果，并开始新的一轮分析。

3. List address(列地址)

根据数据分析情况，列出相关地址及各次分析时该存储单元的数据。

4. Hardware breakpoint(硬件中断)

该菜单项用于某一内存单元进行监视，一旦发现对该单元的访问，则立刻弹出 CM386，以便修改。

5. Return to Debugger(切换到 Debugger)

允许用户使用 Debugger 对游戏程序分析、修改和调试。

6. Return to game(切换到游戏)

从 Debugger 切换到游戏时，必须注意，在呼出 CM386 以前，必须用 Debugger 的"G" 命令运行游戏，之后才能呼出 CM386，切换到游戏画面，否则会使游戏程序挂起而死机。

5.2.2 具体使用例子

1. 用前述方法驻留 CM386，并启动游戏。进入游戏后，呼出 CM386，选择数据分析，并且是"减少"选项。此时，CM386 要求用户输入两个供分析用的临时文件名，而后按"ESC"键返回游戏。

2. 继续游戏，一旦能量或生命减少，立即呼出 CM386，并选择数据分析，此时不要求用户输入，只要求用户耐心等待，CM386 在 386 机器上分析的最

长时间为 15 秒，分析结束后，按“ESC”键返回游戏。

3. 进行数次分析后，选择列地址，也许 CM386 分析的地址值不止一个，此时可继续分析（地址值太多），或者选择一个与分析数据最接近的地址，如 GODS 中的棕色液体加满时，其值为 24，依次选择地址。

4. 知道地址后，立即将该地址设置为硬件中断，应注意段地址和偏移地址都输入完整，一般的游戏都是对该地址进行覆盖，故选择写存储器选项，这样设置断点后，在游戏过程中，一旦对该地址有写操作时，CM386 发现覆写该地址的代码地址后会立即弹出主菜单，可以再次选择硬件断点项区观察地址，然后再按 R 键选择切换到 Debugger，观察并修改那段地址的代码。必须注意的是，断点地址是修改数据实际代码之后的立即数地址，因此，在分析程序代码时，应从该地址前数个字节起，以得到完整的命令。

在这一项中，应特别注意输入代码的精确地址、段地址和偏移地址的每一位都不能输错。

5. 代码修改结束后，应键入 G 命令继续执行游戏程序，然后再次激活 CM386，按 ESC 键恢复游戏画面，这一点非常重要，在激活 CM386 前应先恢复继续执行游戏程序，否则，可能会不能继续游戏或死机。

若在修改的过程中，将整个修改过程记录下来，然后利用 DEBUG 或 PCTOOLS 之类的工具软件对游戏程序进行修改，则能将游戏永久地修改，治成不死版，此后直接运行游戏程序，必须借助于 CM386 了。

5.2.3 破译游戏密码

一般游戏开发者为了保护其权益，一般都设置了密码，如无密码，则不能进入游戏。大多数的游戏在开始时要密码，极少数游戏是在游戏中段要密码，用 CM386 可以较方便地破译密码。在游戏提示输入密码时，激活 CM386，选择切换到 Debugger，此时，Debugger 各个寄存器的值为游戏口令代码的现场，可对该段进行分析、修改，使其绕过密码。

5.2.4 与 GB4 的比较

GB4.0(GB4) 是相当不错的游戏分析工具，与其类似的工具软件还有 GAMETOOL，它们共同特点就是对具体数值的分析、修改极为方便，虽然它们也能进行指令跟踪，但只能跟踪对某一个确切地址进行写操作的指令，GB4 还能自动将对指定地址进行写操作的指令修改为 NOP（空指令），而 CM386 的指令分析功能则远比 GB4 强，它不仅能设置断点，而且可以跟踪整个游戏，例如，在 Debugger 下启动 CM386 后，任何时候只要按下 CM386 的热键 NUMLOCK，就可呼出 CM386 主菜单，选 R 切换到 Debugger 就能对游戏现场的操作指令进行分析。

需要说明的是，CM386 要求使用者对 8086 汇编语言具有一定的知识，才能对游戏现场的指令进行分析、修改。此外，目前许多游戏加入防 Debugger 跟踪功能，此时，就应当用其它的程序分析工具，如 SOFT－ICE 等。

5.3 CM386 V2.0

CM386 V2.0 是由陈伟光先生继 CM386 V1.0 后于 1992 年 12 月开发的游戏解拆程序。它可用来修改"生命值"等，也可用来解拆密码。，特别是出现在游戏中间的口令。Cm386V2.0 的主要特点就是具有设置硬件断点功能，但要修改"生命值"等数据只能通过代码来实现。

5.3.1 CM386 V2.0 系统要求与启动

1. 系统要求

CM386V2.0 的系统要求如下：

- 386 以上处理器
- VGA 显示器
- DOS 3.0 以上版本的操作系统

2. 启动

CM386 V2.0 同 CM386 V1.0 不一样，它是一个独立的驻留内存程序，不需要外部调试器 DEBUG 的支持。按键执行 CM386 命令后，将在屏幕上出现如下信息：

```
Crack Mate
Version 2.00
Copyright (C) 1992
by ChanWaiWong Wilfred
All Right reserved.

Memory used:10239 Byte (Hex)
Hot Key is NumLock
```

当您按住热键 NumLock 时，将在屏幕上弹出主菜单，显示如下：

```
Main Menu

[D] Data analysis
[S] Start another analysis
[L] List address
[H] Hardware breakpoint
[U] Uninstall
[R] Return to Debugger
[ESC] Return to game
```

5.3.2 CM386 V2.0 基本使用

下面对 CM386 V2.0 的主菜单中各个菜单项进行解释。

1. Data analysis(数据分析)。

在第一次分析时输入二个临时文件名。在以后分析时要求指定 Incease (增加)或 Decreas (减少)表示与前一数据相比当前数据是增加还是减少。

2. Seart anather analysis(开始另一个分析)

放弃当前分析结果,开始下一次分析。

3. List address(列地址)

列出由"数据分析"功能找到的地址。

4. Hardware breakpoint(硬件断点)

无论何时从"列地址"中取地址,都可在该地址放置硬件断点。通常断点是"写内存"类型,这是因为"生命值"被游戏修改为一个更小的值。然后,在下次"生命减少"时可立即找到代码。接着用选项"Return to debugger"修改代码 (应具有一定的汇编语言知识)。在输入地址时,必须输满四位数字,如要输入 123,改输 0123。

5. Uninstall(卸下 CM386)

用该选项释放由 CM386 V2.0 占有用的内存。

6. Return to debugger(转到调试器)

将控制交给调试器,以便调试游戏。

7. Return to game(返回到游戏)

退出 CM386 V2.0 系统回到游戏。

5.3.3 CM386 V2.0 实际用法

我们在本节介绍 CM386 V2.0 系统的实际用法。

1. 如何找"生命值"

(1)运行游戏,然后调出解拆大全。选择数据分析(Data Analysis),按提示输入两个临时文件名。然后按 ESC 键回到游戏。

(2)当生命值发生变化时(如减少),再次调出解拆大全,并选择数据分析。在提示"Increase or Decrease: [I/D]"时输入 D 表示减少。分析完成后,按 ESC 键回到游戏。

(3)重复步骤 2 若干次。选择"List address"查看可能的地址。若只有一个地址,或者其中只有一个地址所列各次分析的值与您每次分析时记录下的实际值一致,那么这地址就是"生命值"的地址。。数据分析过程到此完成。

(4)得到"生命值" 地址后,选择"Hardware Breakpoint"设置硬件断点。由于"生命值" 是在"写" 时被修改的,因此,在提示"Instruction fetch/Read-Memory/Write Memory[I/R/W]:"时选择 W。然后输入找到的地址。注意:在输入地址时必须输满 4 位数字。如 123 时应输入 0123,设置了硬件断点后,按 ESC 回到游戏。

(5)当修改"生命值" 时,CM386 V2.0 自动弹出。这时选择"HardWare-

Breakpoint"可看到中断地址。然后按[R]进入调试器,可看到修改的"生命值"的代码。这时您就可以修改这段代码了。

(6)修改完代码后,按 G 回到主菜单,再按 ESC 回到游戏。

(7)继续玩一段时间,若修改达到了自己的要求,请记住修改的代码及其地址。退出游戏后,可以修改游戏程序使它永远不变,也可以每次玩游戏前驻留 CM386 V2.0,进入游戏后计算要修改的地址、临时修改。

2. 如何解拆密码

(1)运行游戏,在提示输入口令时调出 CM386 V2.0,并进入调试器(下面以 TURTLES 为例说明)。

(2)这时执行的指令为 JMP 858D,地址是 1CC7:859E。再用 U (UNASSSEMBLE) 看一看后面的指令,就可看到在 1CC7:85B2 位置有一个 RET 指令。

从这段指令可看到 JMP 858D 指令是一个循环读取密码的指令,而 RET 正是读取密码程序回调程序的指令。

(3)按[G]退出调试器回到主菜单,选择"Hardware Breakpoint"在 1CC7:85B2 处设置取指令中断。

(4)按 ESC 回到游戏继续输入密码,当只输入 1 个数字时便发生了硬件中断,自动弹出 CM386 V2.0,这时按[R]进入调试器看一看,果然是停在 RET 指令。

(5)执行 RET 指令回到调用程序,再查看下面的指令,可看出下面是用来读取密码、进行比较、条件转移的代码。只要把 JZ 8513 改为 JMP 8513 即可。按 ESC 回到游戏,可看到输入任何密码都正确。

5.3.4 CM386 V2.0 使用注意事项

在使用解拆大全 2.0 时,有下面的几个问题必须注意:

1. 解拆大全 2.0 不能与 EMM386.EXE 一起使用,因此,不要在 CONFIG.SYS 中安装这个驱动程序。

2. 不能在网络下使用解拆大全 2.0。

3. 不能在 386 以下机器上使用。

第六章 类 GB 游戏工具 SGB 和 DGB

我们在前面详细地介绍了 GAME BUSTER 4.0 游戏工具，该游戏工具软件在破解游戏时起到了很大的作用。但是，随 GB 4.0 而来的，产生了 SGB 和 DGB，前者克服了 GB 4.0 保存内存地址少的情况，现在能保存达到 40 个内存地址。后者针对磁盘和 DOS/V 的游戏软件有独到之处。本章将着重介绍这两个游戏工具软件。

6.1 超级游戏克星 SGB 2.1

修改游戏的工具软件 SGB 的全称为 SUPER GAME BUSTER2.1(超级游戏克星 2.1)。

6.1.1 SGB 的硬件软件环境

SGB 同 GB 4.0 一样，可在 286 以上机器上运行。MS DOS 在 3.1 以上版本，最好使用 MS DOS 5.0 以上版本。

当在 DOS 提示符下键入 SGB 时，显示一段版权信息文字，SGB 便驻留内存了。

SGB 驻留内存后，只占用 6KB 的常规内存。若您的机器有上位内存(uMB)的话，则可将 SGB 放在 UMB 中运行，不占用常规内存，这要比 GB 4.0 优越多了(GB 4.0 至少占用 11KB 的常规内存和 250KB 左右的 EMS 内存)。

6.1.2 SGB 的显著特点

SGB 比 GB 4.0 的一个显著不同就是可记录多达 40 个内存地址。另外，SGB 中还设有 DEBUG 调试功能，而且在每一项功能中有在线帮助。

6.1.3 SGB 的使用

当 SGB 驻留内存后，连续按两次 ALT 键就可呼出 SGB 的主菜单。SGB 的主菜单如下。

```
Main Menu

0. Edit Memory
1. Game Table
2. Analyze Memory
3. View Picture
4. Debug
5. Unload
```

下面详细地介绍以上菜单功能。

1. Edit Memory(编辑内存地址)

找到要修改的地址后,可以直接在内存中修改:

(1)按 A 可填入要编辑的地址。

(2)按 S 可搜索几个连续的数值(16 进制)。

(3)按空格键可输入 16 进制数。

2. Game Table(地址记录)

找出游戏在内存中存储资料的地址之后,便可将您所选定的地址及其注解填

入表内,以便以后使用。

(1)按 F1 键可进行 10 进制和 16 进制的转换。

(2)按空格键可输入数值。

(3)按回车键可确定地址。

(4)按 D 可删除锁定的地址。

(5)按 N 可输入新地址。

(6)按 L 可从磁盘上装入表格。

(7)按 S 可将表格存入磁盘中。

3. Analyze Memory(分析内存)

(1)让使用者输入要寻找地址的数值,以便根据这些数值来进行分析查找工作。在第一次选择这项功能时,屏幕上会询问您要进行高级分析或低级分析 (STRICT/RELAXED)。

(2)若寻找的数据是确切得知的数值,如现存人数、关数等,您便可选择高级分析。若要寻找的数据是以图形方式来表示,而不知道其确切的数值(如游戏中能源的长度、主角的体力等),便可选择低级分析的工作方式。

当选择完分析方式之后,会询问您是数值还是字符串(TYPE/WORD),然后会让您输入要分析的第一个数值,然后您可以离开 SGB,继续游戏等到这个目标数值有所变化时,再呼出 SGB 使用这功能。接着输入目标之数值,按 F1 键可方便地进行 10 进制和 16 进制的转换。

(3)当输入三个以上的分析值后,便可利用 List Address 功能列出所要寻找的数据地址。若所列出的地址太多时,表示使用进行分析的次数不够,应继续进行分析,直到列出的地址少于四个,用回车键选定最可能的一个。

4. View Picture(观察图片)

这个功能可以回到游戏原来的画面,按任意键可以回到 SGB 主菜单,它可以配合抓图程序使用。

5. Debug(静态跟踪调试)

这个功能可以在游戏中进行跟踪、修改,类似于 DEBUG 程序的一些功能。

6. Unload(退出 SGB)

这个功能可退出 SGB,并且把 SGB 占用的内存释放出来。

6.2 磁盘/DOSV 游戏克星 DGB 3.0

磁盘/DOSV 游戏克星 DGB 全称为 Disk/DosV GAME BUSTER Ⅰ，它是可用于磁盘或 DOSV 的游戏软件。

6.2.1 DGB 的运行环境

DGB 可在 286 以上微机上运行，操作系统为 DOS 3.1 以上，最好为 DOS 5.0 以上版本。

DGB 特别适于磁盘或 DOSV 的软件环境，这是对 GB3 游戏软件功能的扩充。

6.2.2 建立磁盘或 DOSV 的环境

目前许多游戏基于 DOSV 开发的，而 DGB 正是该环境的最好的游戏工具。下面我们给出 DOSV 的配置，供读者参考。

CONFIG.SYS 配置文件内容如下：

```
[menu]
menuitem=NOTHING
menuitem=HIMEM
menuitem=XMS—NOEMS
menuitem=EMS
menuitem=DOSV
menudefault=XMS—NOEMS,3
menucolor=07,0

[common]
numlock=off
files=40
buffers=40,0
lastdrive=Z

[NOTHING]

[HIMEM]
device=c:\dos\himem.sys
dos=high,umb

[XMS—NOEMS]
device=c:\dos\himem.sys
device=c:\dos\emm386.exe noems
dos=high,umb

[EMS]
device=c:\dos\himem.sys
device=c:\dos\emm386.exe ram
```

```
dos=high,umb

[DOSV]                                          ┐
COUNTRY=081,932,C:\DOSV\COUNTRY.SYS             │
DEVICE=C:\DOSV\$FONT.SYS /P=C:\DOSV             │
DEVICE=C:\DOS\HIMEM.SYS                         │ 用于 DOSV 环境的配置
DEVICE=C:\DOS\EMM386.EXE RAM                    │
SHELL=C:\COMMAND.COM C:\ /P /E:512              │
DEVICE=C:\DOSV\$DISP.SYS                        ┘
```

AUTOEXEC.BAT 批处理文件内容如下：

```
@echo off
lh c:\dos\doskey.com /bufsize=1024
lh C:\DOS\mouse.COM /Y
goto %config%
:DOSV
lh c:\dos\SMARTDRV.EXE /x
goto end
:HIMEM
lh c:\dos\SMARTDRV.EXE /x
goto end
:XMS—NOEMS
lh c:\dos\SMARTDRV.EXE /x
goto end
:EMS
lh c:\dos\SMARTDRV.EXE /x
goto end
:NOTHING
:end
PATH C:\DOS;
SET TEMP=C:\
```

6.2.3 DGB 文件构成

完整的 DGB 游戏工具软件由以下四个文件组成的：

· DGB.COM(长度为 7231 字节)

这是 DGB 主执行文件。它采用 PKLITE 1.15 版压缩。若您要分析 DGB.COM 游戏，不妨使用 UNP 或 UP 等还原软件。

· DGB.KEY(长度为 50 字节)

这是 DGB 的热键定义文件。

· DGB.PTN(长度为 48 字节)

这是 DGB 的辅助文件。

· DGB.TLP(长度为 35332 字节)

这是 DGB 的辅助文件。

6.2.4 DGB 启动与热键配置

当您在 DOS 提示符下键入 DGB 时，将在屏幕上显示如下信息：

```
Disk/DosV GameBuster
Version 3.0
COPYRIGHT (C)1994 DEROW COMPUTER STUDIO.
BBS Tel: 886-2-761-0045 , 886-2-763-1164

Automatic Resident in UMB !!!
HOT KEY : Ctrl+Left Shift
```

另外，若您在 DGB 命令后面带? 参数，则可给出 DGB 的命令行参数：

```
Syntax: DGB [ R | D K(0..3) ]
```

其中：

R(Remove)参数将 DGB 从内存中撤离。当您在内存中加载了 DGB 时，可使用该参数卸载 DGB，当出现下面的信息说明卸载成功。

```
<< Disk/DosV GameBuster Ⅲ >> Has been REMOVED !!!
```

D K(0..3)用于定义 DGB 的呼出热键。下表列出 K(0..3)对应的热键。

表 K(0..3)对应的热键

K(0..3)取值	对应热键
K0	Ctrl+Left Shift(默认)
K1	Left Shift+Right Shift
K2	Alt+Right Shift
K3	Ctrl+Alt

例如，当您执行下面的命令时：

```
DGB D K1
```

将出现下面的提示信息，此时，DGB 的热键变为左 Shift+右 Shift。

```
Disk/DosV GameBuster
Version 3.00
COPYRIGHT (C)1994 DEROW COMPUTER STUDIO.
BBS Tel: 886-2-761-0045 , 886-2-763-1164

Automatic Resident in UMB !!!
HOT KEY : Left Shift + Right Shift
```

6.2.5 DGB 的使用

当您使用 Ctrl+Left Shift 呼出 DGB 时，将在屏幕上出现下面的画面：

Main Menu
[1] Analysis
[2] List Address
[3] Edit Memory
[4] Game Table
[5] Print
[6] DEC→HEX
[7] Show Screen
[8] Capture PCX

下面介绍这些菜单项。

1. Analysis(分析)

此菜单让使用者输入欲寻找地址的数值，以便让 DGB 跟据这些分析值来展开寻找的工作。在第一次选择这项功能时，屏幕上会询问您是要进行高级分析或低级分析“LEVEL (H/L)?”，若您要寻找的变数是可以确切得知的数值，如现存的球数、人数、关数等，您便可键入 [H]；也就是要选择高级分析；如果要寻找的数据是以图形方式来表示，而不知道其确切的数值(例如游戏中能源的长度、主角的体力等等)，我们便可键入 [L]，也就是选择低级分析的工作方式。

当选择完分析方式之后，游戏克星便会问您：“ANALYSIS VALUE 01:?”，也就是第一个分析的数值是多少，您就要输入当时游戏中您所要寻找的变数数值。若您所选择的是低级分析的工作方式，不能确定其具体数值，您可自行估计一个大约的数值代替。随着游戏的进行，您要输入几次分析值，这样一来，GB4 便可依照您所提供的数据，找到内存中变数的地址。

若您要重新分析新的数据，可在输入分析值的时候输入英文字母“X”，此时 GB4 的分析功能会重新回到初始状态，您便可以进行下一个变数的分析。

DGB 的输入系统为十六进制，故您所填入的数值范围应为 00－FF。若您要输入的数值为十进制，则数值的范围应为 0－255，并请在数值前加一“/”号，游戏克星便会自动将其转换为十六进制数值。

低级分析的原则为：变数越大，则输入的分析值也要越大；变数越小，则输入的分析值也要越小；变数不变时，其间输入的分析值是一样的。

另外，低级分析的原则是分析值间的大小关系，而分析值间大小的比例则不予考虑。

2. List Address(显示地址)

当您使用功能 [1] 输入三个以上的分析值之后，便可利用此功能列出您所要寻找的变数地址。如果所列出的地址太多时，表示使用者进行分析的次数不够，此时应再使用功能 [1]，多输入几个分析值，便可滤去许多不相干的地址。等到列出的地址减少到 4 个以下时，便会出现一个以亮度表示的光标，让使用者选定最有可能的地址，被选定的地址前会出现一个“*”号，而在输

入地址时便可用“*”号来代替选定的地址。

例：
```
2000：31A9   02   01   01   00   03
2000：4529   02   01   00   00   04
3000：1928   02   01   01   00   03
```

3. Edit Memory(编辑内存地址)

找到要修改的地址后，可以直接在内存中修改：

(1)按 A 可填入要编辑的地址。

(2)按 S 可搜索几个连续的数值(16 进制)。

(3)按空格键可输入 16 进制数。

4. Game Table(地址记录表)

该菜单找出游戏中储存资料的地址之后，便可将您所选定的地址及其注解填入表内，以便以后使用。

例：
```
01—BALL     3000：6B5A     02
02—LEVEL    3000：6BC4     04
03          0000：0000     5B
04          0000：0000     5B
```

在使用该菜单时，应注意下面的问题：

(1)按 [ALT]+<1>—<8> 便可将选定的地址及其注解填入表格中。

(2)按 <1>—<8> 则能把数值写入该项选定的地址位中。

(3)按 SHIFT] +<1>—<8> 锁定该地址的内容，使得该地址的数值保持不变，再按一次便可解除锁定。

(4)[S] 键可将表格存入磁盘中；[L] 键则从磁盘上载入表格。

(5)在输入地址表格文件名时不必加扩展名.

(6)填入地址栏时，若键入“*+1”则为选定地址的下一个地址。

(7)填入地址栏时，若键入“*-1”则为选定地址的上一个地址。

(8)若您欲使用上次所储存的记录表格，请使用与上次执行游戏时相同的 CONFIG. SYS 以及 AUTOEXEC. BAT 文件(或其它的常驻程序)，这样游戏程序载入内存中的位置才会与上次相同，才能避免表格内的地址因变动而失效。

5. Print(打印)

利用该菜单，可将分析的地址数据打印出来，供进一步地址分析。

6. DEC→HEX(10 进制转化 16 进制)

该菜单可让用户在分析地址数据时，将输入数据转换为 16 进制数。

7. Show Screen(显示屏幕)

该菜单用于查看用户游戏屏幕。

8. Capture PCX(抓图 PCX)

该菜单可将游戏屏幕抓图为 PCX，并保存起来。

附录 A：

游戏克星 GB2、GB3 简介

A.1 游戏克星第二代 GAME BUSTER Ⅱ

相信大家在玩一些游戏时，除非有该游戏的不死版或攻略秘技之类，否则便要花不少时间去“钻研”。例如笔者为了完成“怒”，花上了几个月时间，这使得我不敢去玩“怒Ⅰ”！如果不幸的话，甚至可能会饮恨而回。笔者玩了“变形金刚”几个月，也只是到第三关，而该游戏共有十多关呢！

一套最新由广大电脑引进的功能强劲实用工具将令你永不落空－Game Buster Ⅰ，使你成为电脑游戏中的不死英雄。它可以用来修改游戏的程序（当然不是 PCTOOLS 那样简单！）。以下向大家介绍一下，好让各位软件世界用家一尝自己修改无敌版的滋味。

1. 程序介绍

Game Buster 是一个驻留内存程序，它能在任何时间呼叫出来，从内存中找出、记录和修改游戏中的所需资料。即使游戏所占用的内存多至 512KB，仍可使用本程序，而且用法简单方便，大家可以用它来修改游戏中的人数、武器、能量和金钱等。你们听了也跃跃欲试吧！

而且游戏克星还拥有时间延迟（Delay）这一个功能，如果大家认为电脑的速度太快，这实在是一大福音了。

2. 启动程序

（1）启动机器后，将 Game Buster 放入 A 驱动器，输入 GB，这时程序程式已驻留内存。

（2）接着替换磁盘，把 DOS 系统盘或直接启动的游戏磁盘放入，按任何一键 REBOOT（重新启动）。

其输入的其它方法如下：

[2]代表软件占 256K。

[3]代表软件占 384K。

[5]代表软件占 512K。

举个例，修改需用 512K 内存的游戏，在输入时只需在 A:\>提示符下键入：GB/5，便可有 512K 的空间。

如果使用 EGA 的用户，或游戏需要使用 EGA 的话，请使用 GBEGA 来启动游戏克星，否则屏幕显示将会不正常。

3. 键盘控制

由于 GB Ⅰ是针对 CGA 用户而设计的，所以在其他屏幕上有可能出现看不见的问题。因此以下数个功能是给其他屏幕用的：

- CTRL－C 颜色切换。
- CTRL－Q 返回 DOS。
- CTRL－E 画面切定。单色屏幕使用 CGA 模拟程序专用，用来放大或缩小画面。
- ＜或＞键调整频率：单色屏幕模拟 CGA 时常会有整个画面上下跳动的现象发生，此时便可以用此键来调整频率，使画面不再跳动，而不需调整

屏幕后方的旋钮。

4. 使用方法

在进行游戏时，连按 TAB 或 F10 两次，便可呼叫出 Game Buster，第一次看到标头时，按 Spacebar，您会看到七个选择(0－6)，分别是：

· USE TABLE

若您已经利用下面的功能找出了数值地址，便可利用这功能把地址记下，并加上注解(最多可记下八个)，储存到磁盘文件上。

具体方法是在选择了这项功能后，按 Alt－1(1－8)，然后输入注解和地址，再按 Enter，以后要修改地址数值时，只要按 1－8 选择地址，便可输入想要的数值。

只要在这功能项下按 S，再输入文件名称，Game Buster 便人地把输入了的地址和注解存档。下次要用时，只要在启动 Game Buster 时，键入 GB [Filename]便可。

· PROCEED ANALISYS

您可以使用这个功能，输入 reference value1，让电脑记下存在被寻找的数值地址之现时数值，然后继续进行游戏，让这数值改变，跟着又进入 GB 再输入那个变更了的数值，如是者三次或以上，便可用接着的功能找出该个资料的地址。

例如您要寻找能量的地址，便输入现时的能量值，待用去了一些时再输入新的值，三次后便可利用下一项功能，找出相对的地址。

要注意的便是输入的数值应为十六进制，例如原本是 100，输入便为 $64，原本是 10，则为 $0A。另外，这功能最多可作 15 次的分析。

· LIST ADDRESS

当利用了以上的功能后，便可选择用 high level 或 low level 来检查可能的地址。

High level 是从内存中找出与输入数据完全相同的数值与其地址。例如您输入 10、11 和 12，电脑便会找出所出有变化为 10－11－12 的地址，并列出来。

如果用 high level 找不到，便可用 low level 来尝试。它的寻找方式是按数值变化的方向来比较。例如输入为 32、37、3C 和 37，其中第二、三项上升，第四项下降，于是电脑便列出所有数值上升两次及下降一次的地址。使用 lowlevel 来寻找地址，可能会有很多地址被列出来，所以应该尽量输入多些数据，以分析得详细点。

一旦您找到可疑的地址时，便应把它们抄下，然后使用下面的修改功能来试一下。

· MODIFY MEMORY

这一项有两个选择，一个是 Read，读取某地址的数值。另一个则是 Write，用来修改你所指定的地址的数值。

例如您怀疑一个地址是记忆金钱的数目，那么便可使用 Write 这个功能来更改这个地址的数值，然后看一看结果，满意与否。如果发现修改成功或有一些问题出现时，应该把它抄下来慢慢研究。

· REINIT

当您想重新分析，可选择这一项，原先输入的数据便会清除，让您重新分析。

· ADJUST SPEED

如果游戏的速度太快，您可以使用这个功能调慢游戏的速度。输入的数值越大，游戏的速度越慢，各位可以调校至理想的速度。

· TRACE

追踪：通常能源、生命等的减少都会由某一个指令来控制；例如在《波动拳》的游戏，中波就扣四分之一，全空就输一个 ROUND 等。如果能找出这指令并将它弃掉，以后能源或生命便不会减少，形同无敌。而这功能就是找出这种指令，以便改为无版。

· LOAD/SAVE GAME

存取游戏：有许多游戏本身并未提供储存游戏－[续关]的功能，而不储存游戏又很难玩得完。因此这功能可以随时存取游戏的进度。当游戏玩不下去或生命不够时可以重新载入，这样就不需重头开始了，只需从上次 SAVE GAME 的地方开始就可以了。

· ESC：EXIT

按 ESC 键可让您继续游戏。

巧妙地使用上面的功能，相信任何一个游戏都会被击破。

5. 其他应用

《游戏克星Ⅰ》不单是一个游戏工具，它还是一个十分不错的实用工具，笔者举一个例：假如您有一个 DBASE Ⅱ 排序的程序，它需要很长时间才可以搞完，那么您可以用《游戏克星》把它当游戏一样 SAVE 入磁盘，保留现场，等下一班回来时再继续运行。另外它对于实用软件的调试也很有用。

《游戏克星Ⅰ》由于有更多的商业性，所以它离实用软件还有一段距离，以笔者个人意见以为：《游戏克星Ⅰ》+DEBUG 或《游戏克星Ⅰ》+TURBO DEBUG 岂不是更加实用？

不过，笔者在此给各位一个衷心的建议，千万不要滥用无敌的功能，那将会失去许多游戏的乐趣。

总之，笔者认为《游戏克星》是每一个 IBM pc 用户所必须拥有的实用工具盘，值得您第一时间购买。

A. 2 GAME BUSTER 3. 0

1. 安装方法

以 DOS 3. 3 开机，将 GAME BUSTER 3 磁盘放入 A 驱(勿贴上防写标签)，键入 GBINST，按下＜ENTER＞键。驱动器停止转动后，磁盘上会出现 GB. EXE、MAINHC. EXE 及 MAINEV. EXE 三个文件。

请注意：在安装过程中请勿按 RESET 键，否则会破坏整个程序！GB3 只能安装一次，并且只能在安装时的机器上使用。请自行备份安装过后的三个文件，以免有任何意外发生而无法挽救。

2. 装入方式

在 DOS 提示符下键入 GB 以执行之，经过显示一段版权文字信息后，GB3 程序便以常驻方式存于内存中。此外亦可加入下列的参数：

－ GB/H 执行单色版本。

－ GB/C：执行 CGA 版本。

－ GB/E：执行 EGA 版本。

— GB/V：执行 VGA 版本。

— GB XXXX：执行并载入 XXXX.GB 的表格档。

此外，它会自动侦测电脑上是否有扩展内存(EXTENDED MEMORY)并自动使用扩展内存，以增大常规内存的剩余空间。故有 1024K 的 AT 及 386 机器应避免载入虚拟磁盘(VDISK)或其他占用全部扩展内存的程序。

3. 功能介绍

载入 GB3 后，任何时候，只要按两次 CTRL 键，便会出现 GB3 的主目录(第一次进入还会显示作者等资料)，而各项选择的功能介绍如下：

· USE TABLE

当您分析出某些位置后，可利用此功能记录下来。

· ADDRESS ANALYSIS

作数值的分析，输入方法与 GB2 相同。

· LIST ADDRESS

将分析结果列出。比旧版本新增了一个功能，能够让使用者选定最可能的位置，被选定的位置前会出现一个 * 号，而在使用 0、3、5 这些功能时便可使用 * 号来取代所选定的位置。(等到所列出的位置减至 4 个以下时才可以用 * 号。)

· MODIFY MEMORY

供使用者对电脑内的任意位置作观看或修改。

· CLEAR ANALYSIS

把所有分析资料清除，以便作下一次分析。

· TRACE

跟踪指令，以便您作不死版的修改，同时亦可自动为
您修改。

· ADJUST SPEED

作游戏速度的调校。

· SAVE & LOAD GAME

存储和调用的戏

3. 新增控制键说明

以下的控制键均在【游戏克星 3】的主菜单下使用：

· CTRL — S

此功能可配合抓图程序使用，按 CTRL — S，【游戏克星】会把主目录隐藏起来，此时屏幕上所呈现的是完整的游戏画面。使用者便可将屏幕的图形用先前所载入的抓图长驻程序抓下来。完成之后按 ESC 键回到主目录。抓图驻留程序应在【游戏克星】程序之前先载入。

· CTRL — H

由于【游戏克星】是以连续两次 CTRL 叫出，而有些游戏也使用 CTRL 键，为了避免冲突，此功能可将召唤键由 CTRL 改换成 TAB 键，当下次欲叫出【游戏克星】时，改按 TAB 两次。

· CTRL — Q

强迫结束游戏，跳回 DOS，而不是 WARM BOOT。

附录 B：

GAMETOOL 1.0 版简介

GAME TOOLS 1.0 版是一个以 TURBO PASCAL5.5 编写的软件破解系统。它除了可代替 GAME BUSTER 的功能外，其最大的优点是它只占约 40KB 的内存，但容许用户使用更多的功能，如显示内存内容、选择作分析之内存范围、呼叫 DEBUG 来把软件修改或监察及使用更强的系统追踪功能。

除了 GAMETOOL 及 GAME BUSTER Ⅱ外，无敌工具箱还包括一系列工具系统，内容包括磁盘保护之破解、文件的加密、EXE 文件之处理、屏幕之捕捉及增加磁盘容量等等。

比游戏克星更强的系统－GAMETOOL 是一个驻留程序，可由 DOS 载入，最多用了 38016 BYTES，但却有更多功能。

因为 GAMETOOL 是用 TURBO PASCAL 5.5 编写的，所以所有数字输入格式都是跟着 TURBO PASCAL 的格式。例如，十六进制数字之前要加上“$”。注意，GAMETOOL 应在 DOS 3.×系统下动作及在装入之前不可以装入任何 TSR。另外，GAMETOOL 只可以完全在 CGA 或 MGA 上执行，另外它也可支持部分的 EGA 模式。

装入 GAMETOOL 后，用户可按热键“PRTSCR”呼叫 GAMETOOL。进入 GAMETOOL 后，书面上端会印出刚进入 GAMETOOL 前 DS、CS、ES、SS、IP 的值及 PSP、INT8、INT9 的地址。

GAMETOOL 有十二个功能：

0－TRACE

追踪软件的执行，当 GAMETOOL 发现某地址的值有改变时返回 GAMETOOL。有两种追踪方式：

(1)追踪软件直至由用户指定地址内的值有改变。

(2)追踪程序直至指定地址被改成用户指定的值。

若用户发觉使用这功能时，电脑暂停，可选择当遇到机器码 CLI 暂停跟踪直至遇到 STI 才恢复。

1－ANALYSE

这功能和游戏克星Ⅱ的差不多，不同的是可在任何 PATH 开启临时文件，及输入 REFERENCE VALUE 时则有三种选择：

(1)由使用者输入。

(2)自动增加。

(3)自动减少。

因为要简化系统及减少占用的内存，GAMETOOL 只是分析指定的 SEGMENT，不分析所有内存。而 REFERENCE SEGMENT 通常都是被跟踪软件的 DS 或 ES。

2－LIST

分析完三次后便可将地址列出，可按“↑”，“↓”，“PgUp”，“PgDn”，去观看那些地址。按“R”将所有最后分析出来的地址恢复为某次 ANALYST 时

的值。

3—KEEP

将10个地址维持成特定的值，这是方便用户的分析，而不需每次改变后都要自行修改内存。若没有地址要维持，可输入地址0:0。

4—DUMP

把内存内容显示。按"G"，输入地址及显示。按"W"，修改内存。按"S"，找寻字串或数值，长度不可超过16 BYTES。按"N"，继续找寻。按"↑"、"↓"、"PgUp"、"PgDn"向前或向后显示。

5—INT3

发出一个INT3。如在执行软件前先执行DEBUG，在GAMETOOL发出INT3后，回到DEBUG，这时可作机器语言修改。完成后，将DEBUG的IP设成IP+1，再输入"G"，便可返回GAMETOOL。

6—CLOCK

每次进入该功能时，GAMETOOL会检查现时发出中断8的FREQUENCY及使用者可将FREQUENCY设成0，则可正常或自行输入。

7—REINIT ANALYSIS

放弃以前分析的结果重新分析。

8—EXIT

返回被跟踪软件。

9—QUIT

放弃现时执行的软件并返回DOS。

U—UNINSTALL

卸载GAMETOOL。

D—DIRECTVIDEO IS TRUE/FALSE

选择是否直接显示(不使用BIOS)。

R—RETURN TO MODE

用户可按R选择返回被跟踪软件之屏幕模式。这里已包括所有的CGA及MGA或HERCULES输出模式。

附录 C：

超级 DEBUG 调试程序 SDEBUG

在使用本书介绍的游戏工具软件时，适当地使用 DEBUG 是有好处的。MSDOS 提供的 DEBUG 功能太弱，不能满足调试特殊游戏程序(如反跟踪、反拷贝等)的要求。

SDEBUG 就是在此情况下诞生的超级 DEBUG 程序，它增加或增强了 DEBUG 的许多功能。

1. SDEBUG 的基本功能(与 DEBUG 相似)。

- 汇编　　A [地址]
- 比较　　C 比较地址范围
- 查看　　D [地址范围]
- 填写　　E 地址 [列表]
- 填充　　F 地址范围
- 运行　　G [=起始地址 1] [启始地址 2..]
- 十六制运算　H 值 1，值 2
- 读口地址　I 端口号
- 调文件　　L [地址] [驱动器] [起始扇区] [数量]
- 移动内存　M 范围 地址
- 命名　　N [路径名] [文件名]
- 写口地址　O 端口号
- 跟踪过程　P [=地址] [数量]
- 退出　　Q
- 显示寄存器　R [寄存器]
- 搜索　　S 范围 列表
- 单步跟踪　T [=地址] [数量]
- 反汇编　　U [范围]
- 写文件　　W [地址] [驱动器] [起始扇区] [数量]
- 分配扩充内存　　XA [#页号]
- 取消扩充内存　　XD [句柄]
- 显示扩充内存页映像　　XM [L 页] [P 页] [句柄]
- 显示扩充内存状态　　XS

2. SDEBUG 增设命令简介

(1) [B 命令]

格式：　B nn (如：B 1C) —— nn 表示两位 16 进制数

意义：　自动定时断点，当完成指定的 nn 次断点后自动停止执行。(其定时间隔可由"KB nn"命令修改)

(2) [Y 命令]

格式：　Y nn (如：Y 2)

意义：　当完成指定的 nn 次功能调用后自动停止执行。

(默认的功能调用号为 30H,其值可由"KY nn"命令重新设定)

(3)[Z 命令]

格式: Z filename (如:Z MY.TXT)

意义: 自动连续执行指定的文本文件 filename 中的命令。

(4)[X 命令]

格式: 1) XW nnnn [nnnn] [....] (如:XW CD13 CD10)

意义: 在"T"命令时,当遇到该命令指定的 2 字节指令码时自动判停。(最多允许 10 个双字节指令)

格式: 2) XB nn [nn] [....] (如:XB FA A5 C3)

意义: 在"T"命令时,当遇到该命令指定的 1 字节指令码时自动判停。(最多允许 10 个单字节指令)

格式: 3) XW

意义: 取消所有的自动判停双字节指令。

格式: 4) XB

意义: 取消所有的自动判停单字节指令。

格式: 5) XI

意义: 在"T"命令时,若遇到中断向量表有变化,则自动判停。

格式: 6) XS

意义: 在"T"命令时,若遇到程序堆栈和(SS,SP)溢出时,则自动判停。

格式: 7) X

意义: 在"T"命令时,取消"XI","XS"命令设置的自动判停功能。

(5)[J 命令]

格式: 1) JC

意义: 在"T"命令时,自动跳过 CALL 指令。

格式: 2) JI

意义: 在"T"命令时,自动跳过 INT n 指令。

格式: 3) J

意义: 在"T"命令时,取消"JC"、"JI"命令设置的自动判跳功能。

(6)[V 命令]

格式: 1) VI

意义: 在"T"命令时,仅当遇到 INT n 指令时才显示。

格式： 2) VE

意义： 在"T"命令时，仅当单步结束时才显示. 即关闭 CRT。

格式： 3) V

意义： 在"T"命令时，取消"VI"，"VE"命令设置的关闭 CRT 功能。恢复正常显示。

(7) [K 命令]

格式： 1) KB nn （如：KB 4）

意义： 修改"B"命令定时间隔，即修改步距，控制自动断点精度。(nn=0 步距最小)

格式： 2) KY nn （如：KY 09）

意义： 修改"Y"命令功能调用号。

格式： 3) KG nn （如：KG 15）

意义： 修改"G"命令断点中断号，(默认为 INT 80H)

格式： 4) KN nn （如：KN 3）

意义： 设定"G"命令某断点自动重复计数的次数。

(注意：此时在"G"命令中必需同时提供两个相关的断点地址. 如：G 120 124)。

格式： 5) KK

意义： 在"G"命令时，自动保存并恢复中断向量地址，并强行打开键盘和 CRT 中断。

格式： 6) K

意义： 取消上述"KK"设置，恢复正常的断点中断情况。

附录 D：

8088/8086 汇编速查简明手册

一、数据传输指令

它们在存储器和寄存器、寄存器和输入输出端口之间传送数据。

1. 通用数据传送指令

MOV	传送字或字节
PUSH	把字压入堆栈
POP	把字弹出堆栈
XCHG	交换字或字节
XLAT	字节查表转换

BX 指向一张 256 字节的表的起点，AL 为表的索引值（0－255，即 0－FFH）；返回 AL 为查表结果。（[BX+AL]－>AL）

2. 输入输出端口传送指令.

IN	I/O 端口输入.（语法：IN 累加器，{端口号mDX}）
OUT	I/O 端口输出.（语法：OUT {端口号mDX}，累加器）

输入输出端口由立即方式指定时，其范围是 0－255；由寄存器 DX 指定时，其范围是 0－65535。

3. 目的地址传送指令。

LEA　　装入有效地址。

例：LEA DX,string ；把偏移地址存到 DX。

LDS　　传送目标指针，把指针内容装入 DS。

例：LDS SI,string ；把段地址：偏移地址存到 DS:SI。

LES　　传送目标指针，把指针内容装入 ES。

例：LES DI,string ；把段地址：偏移地址存到 ES:DI。

4. 标志传送指令

LAHF	标志寄存器传送，把标志装入 AH。
SAHF	标志寄存器传送，把 AH 内容装入标志寄存器。
PUSHF	标志入栈。
POPF	标志出栈。

二、算术运算指令

ADD	加法
ADC	带进位加法
INC	加 1
AAA	加法的 ASCII 码调整
DAA	加法的十进制调整
SUB	减法
SBB	带借位减法
DEC	减 1

NEC　　求反(以 0 减之)

CMP　　比较.(两操作数作减法,仅修改标志位,不回送结果)

AAS　　减法的 ASCII 码调整

DAS　　减法的十进制调整

MUL　　无符号乘法

IMUL　　整数乘法

以上两条,结果回送 AH 和 AL(字节运算),或 DX 和 AX(字运算)

AAM　　乘法的 ASCII 码调整

DIV　　无符号除法

IDIV　　整数除法

以上两条,结果回送:

商回送 AL,余数回送 AH,(字节运算)

或　商回送 AX,余数回送 DX,(字运算)

AAD　　除法的 ASCII 码调整

CBW　　字节转换为字.(把 AL 中字节的符号扩展到 AH 中去)

CWD　　字转换为双字 (把 AX 中的字的符号扩展到 DX 中去)

三、逻辑运算指令

AND　　与运算

OR　　或运算

XOR　　异或运算

NOT　　取反

TEST　　测试(两操作数作"与运算",仅修改标志位,不回送结果)

SHL　　逻辑左移

SAL　　算术左移(=SHL)

SHR　　逻辑右移

SAR　　算术右移(=SHR)

ROL　　循环左移

ROR　　循环右移

RCL　　通过进位的循环左移

RCR　　通过进位的循环右移

以上八种移位指令,其移位次数可达 255 次

移位一次时,可直接用操作码. 如 SHL AX,1

移位>1 次时,则由寄存器 CL 给出移位次数

如　MOV CL,04

SHL AX,CL

四、串指令

DS:SI　　源串段寄存器 :源串变址

ES:DI　　目标串段寄存器:目标串变址

CX　　重复次数计数器

AL/AX　　扫描值

D 标志　　0 表示重复操作中 SI 和 DI 应自动增量；1 表示应自动减量。

Z 标志　　用来控制扫描或比较操作的结束。

MOVS　串传送

（MOVSB　传送字符.　　MOVSW　传送字.）

CMPS　串比较

（CMPSB　比较字符.　　CMPSW　比较字.）

SCAS　串扫描

把 AL 或 AX 的内容与目标串作比较，比较结果反映在标志位、

LODS　装入串

把源串中的元素(字或字节)逐一装入 AL 或 AX 中。

STOS　保存串

是 LODS 的逆过程。

REP/REPE/REPNE/REPZ/REPNZ　重复

五、程序转移指令

1>无条件转移指令（长转移）

JMP　无条件转移指令

CALL　过程调用

RET/RETF过程返回

2>条件转移指令（短转移，－128 到＋127 的距离内）

JA/JNBE 不小于或不等于时转移

JAE/JNB 大于或等于转移

JB/JNAE 小于转移

JBE/JNA 小于或等于转移

以上四条，测试无符号整数运算的结果(标志 C 和 Z)。

JG/JNLE 大于转移

JGE/JNL 大于或等于转移

JL/JNGE 小于转移

JLE/JNG 小于或等于转移

以上四条，测试带符号整数运算的结果(标志 S,O 和 Z)。

JE/JZ　等于转移

JNE/JNZ　不等于时转移

JC　有进位时转移

JNC　无进位时转移

JNO　不溢出时转移

JNP/JPO　奇偶性为奇数时转移

JNS　符号位为 "0" 时转移

JO　溢出转移

JP/JPE　奇偶性为偶数时转移

JS　符号位为 "1" 时转移

3>循环控制指令(短转移)

LOOP　CX 不为零时循环

LOOPE/LOOPZ　CX 不为零且标志 Z=1 时循环
LOOPNE/LOOPNZ CX 不为零且标志 Z=0 时循环
JCXZ　CX 为零时转移

4>中断指令

INT　中断指令
INTO　溢出中断
IRET　中断返回

5>处理器控制指令

HLT　处理器暂停，直到出现中断或复位信号才继续
WAIT　当芯片引线 TEST 为高电平时使 CPU 进入等待状态
ESC　转换到外处理器
LOCK　封锁总线
NOP　空操作
STC　置进位标志位
CLC　清进位标志位
CMC　进位标志取反
STD　置方向标志位
CLD　清方向标志位
STI　置中断允许位
CLI　清中断允许位

六、伪指令

DB　定义字节
DW　定义字(2 字节)
PROC　定义过程
ENDP　过程结束
SEGMENT 定义段
ASSUME 建立段寄存器寻址
ENDS　段结束
END　程序结束

七、系统和 BIOS,DOS 占用的中断向量

.中断 0：除数为 0 错
.中断 1：单步中断
.中断 2：不可屏蔽中断 NMI
.中断 3：断电中断 (CCH)
.中断 4：溢出中断
.中断 5：屏幕打印中断
.中断 6-7：保留
.中断 8：计时器中断(18.2/秒)
.中断 9：键盘中断
.中断 A-D：保留
.中断 E：软盘机中断
.中断 19：引导装入程序
.中断 1A：日时调用
.中断 1B：键盘阻断时得到控制权
.中断 1C：时钟中断时得到控制权
.中断 1D：指向 CRT 初始参数表
.中断 1E：指向盒带参数表
.中断 1F：1KB 图形模式 CRT 用第 128 至 256 号字符
.中断 20：结束 DOS 程序
.中断 21：DOS 功能调用
.中断 22：结束地址 (建议用 EXEC 功能调用)
.中断 23：DOS Ctrl-Break 退出地址

.中断 F：保留
.中断 10：屏幕 I/O 调用
.中断 11：设备检查调用
.中断 12：存贮器检查调用
.中断 13：软盘机 I/O 调用
.中断 14：RS-232 I/O 调用
.中断 15：盒带机 I/O 调用
.中断 16：键盘 I/O 调用
.中断 17：打印机 I/O 调用
.中断 18：ROM-BASIC 入口
.中断 24：DOS 致命错向量
.中断 25：DOS 绝对磁盘读
.中断 26：DOS 绝对磁盘写
.中断 27：结束程序并贮留(建议用 31H 功能调用)
.中断 28-3F：DOS 保留
.中断 40-7F：未用
.中断 80-85：BASIC 保留
.中断 86-F0：BASIC 解释程序用
.中断 F1-FF：未用

八、IBM PC 的中断 INT 10：

.00H 屏幕方式设置

入口：AH＝0，AL＝显示方式代码.(0－6)

0：40x25 黑白 1：40x25 彩色 2：80x25 黑白 3：80x25 彩色文本方式

4：320x200 彩色 5：320x200 黑白 6：640x200 黑白图形方式

7：80x25 单色字符（单色显示器）

.01H 设光标大小

入口：AH＝1，CH＝光标起始行号(00－0C)，CL＝光标结束行号(00－0C)，且 CH＜CL。

.02H 光标定位

入口：AH＝2，BH＝页号，DH:DL＝起始行:列。

.03H 读光标位置

入口：AH＝3，BH＝页号。返回：DH:DL＝起始行:列。

.06H 窗口上卷

入口：AH＝6，AL＝窗口上卷行数(AL＝0 卷动整个窗口)；

CH:CL －DH:DL 窗口坐标

.07H 窗口下卷

入口：AH＝7，AL＝窗口下卷行数

CH:CL －DH:DL 窗口坐标

.08H 读当前光标处字符和属性

入口：AH＝8，BH＝页号。返回：AH:AL＝字符的颜色:字符的 ASCII 码

显示字符的颜色定义如下：

1	2	3	4	5	6	7	8
BL	R	G	B	I	R	G	B

B－兰 G－绿 R－红

闪烁　字符底色　加亮　字符显示色

.09H 在当前光标处写字符和属性(光标不下移).

入口：AH＝9，BH＝页号，BL:AL＝字符的颜色:字符的 ASCII 码，CX＝重复次数。

.0AH 在当前光标处写字符(原有属性)

入口：AH＝0A，BH＝页号，AL＝字符的 ASCII 码，CX＝重复次数。

.0BH 色彩设置

入口：AH＝0B，BL＝0　　设背景色，BH＝0－15

BL＝1　　设调色码，BH＝0－1

.0CH 写图形点

入口：AH＝0C，CX:DX＝列号:行号，AL＝颜色。

.0DH 读图形点

入口：AH＝0D，CX:DX＝列号:行号. 返回：AL＝颜色，

.0EH 在当前页、当前光标处写字符

入口：AH＝0E，AL＝字符的 ASCII 码，BL＝前景色。

.0FH 显示器状态

入口：AH＝0F. 返回：AL＝当前显示器方式，AH＝屏幕列数，BH＝当前页号

九、IBM PC 的键盘中断 INT 16：

.00H 读一个键盘键入字符

入口：AH＝0. 返回：AL＝字符的 ASCII 码，AH＝扫描码.

.01H 确认键盘是否键入字符

入口：AH＝1.　　返回:ZF＝1 (Z) 未键入字符；

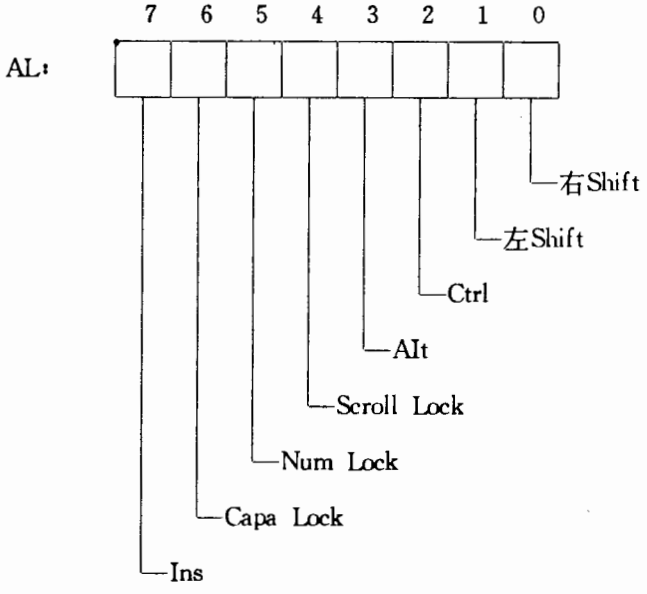
ZF＝0 (NZ)键入字符，AL＝字符的 ASCII 码，AH＝扫描码。

键入字符同时留在键盘缓冲区.

.02H 读当前移位键状况

入口：AH＝2。

返回：AL＝状态。



十、ROM 中断 INT 13：

A. 软盘机 I/O 调用(360K)

.00H 复位盘系统

入口：AH =0

返回：AH =磁盘状态

0—坏命令，1—盘上地址找不到，3—写保护，4—扇区找不到，...

.01H 读磁盘状态

入口：AH =1

返回：AH =磁盘状态

.02H 磁盘读

入口：AH =2，DL =驱动器号(0—3)，0=A，1=B，2=C

DH =头号(0 或 1)，CH =道号(0—39H)，CL =起始扇区号(1—9)

AL =欲读扇区数(1—9)，ES:BX =内存缓冲区首址.

返回：AL =实际读入扇区数，AH =磁盘状态；进位标志 CF =0，出错；=1，成功.

.03H 磁盘写

入口：AH =3，DL =驱动器号(0—3)，0=A，1=B，2=C

DH =头号(0 或 1)，CH =道号(0—39H)，CL =起始扇区号(1—9)

AL =欲写扇区数(1—9)，ES:BX =内存缓冲区首址.

返回：AL =实际写入扇区数，AH =磁盘状态；进位标志 CF =0，出错；=1，成功。

B. 硬盘机 I/O 调用

入口：AH =0—3，DL =驱动器号(硬盘 80H，81H)，80=C，81=D

DH =头号(硬盘 0—15)，CH =道号(0—1023)，CL =起始扇区号(1—17)

AL =欲读写扇区数，ES:BX =内存缓冲区首址.

返回：AL =实际读入扇区数，AH =磁盘状态；进位标志 CF =0，出错；=1，成功。

十一、绝对磁盘读写 (中断 25，中断 26)

A. INT 25 绝对磁盘读

B. INT 26 绝对磁盘写

入口：AL =驱动器号(0—2)，0=A，1=B，2=C

DX =起始扇区的逻辑扇区号

CX =欲读写扇区数(1—80H)

DS:BX =内存缓冲区首址。

十二、IBM PC 功能调用（中断 INT 21）

.00H 程序结束

.01H 键盘输入一个字符(回显)

入口：AH＝01，　　返回：DL＝输入字符。

对扩展键，要求两次功能调用。

.02H 显示一个字符。

入口：AH＝02，DL＝字符.(07 响铃，08 退格，0D 回车，0A 换行)

.05H 打印一个字符。

入口：AH＝05，DL＝字符.(0D 回车，0A 换行)

.08H 键盘输入一个字符(不回显)

入口：AH＝08。　　返回：DL＝输入字符.

对扩展键，要求两次功能调用。

.09H 显示一串字符

入口：AH＝09，DS:DX＝字符串首址。(字符串必须以字符'$'结尾.)

.0AH 键盘输入一串字符

入口：AH＝0A，DS:DX＝字符串首址，字节 DS:[DX]＝缓冲区长(最多容纳字符数)

(输入字符串必须以回车结尾.)

返回：字符串首址在 DS:DX＋2，字符数＝DS:[DX＋1]。

.0CH 清键盘缓冲区，并调用键盘功能(01H，06H，07H，08H 或 0AH)

入口：AH＝0C，AL＝调用键盘功能号(01H，06H，07H，08H 或 0AH)。

.30H 取得 DOS 版本号

返回：AL－主版本号，AH－次版本号

.42H 移动文件读写指针

AL＝0　　指针从文件开始移动 CX:DX 个字节

AL＝1　　指针从当前位置开始移动 CX:DX 个字节

AL＝2　　指针从文件尾向前移动 CX:DX 个字节

.43H 改变文件属性

.4CH 结束 DOS 程序，并保留代码可用于批处理中

附录 E：

游戏软件存档跟踪实用工具 TRACE

在电脑上需要了解游戏软件的存档数据文件，使这些游戏软件也能在光盘上直接运行。另外，该程序对于了解游戏软件的流程及文件之间的关系有指导作用。为此，我编制了一个游戏软件存档跟踪实用工具 TRACE，它驻留内存后，就可跟踪游戏软件在运行期间的文件之间的相互调用关系，以便决定哪些文件是游戏软件的存档文件。

TRACE 采用汇编语言编制的，经 MASM、LINK、EXE2BIN 编译、连接和转换，最终程序为 TRACE.COM，该文件长度只有 143 字节。

在执行 TRACE 后，必须将打印机打开，然后运行游戏软件，此时，就在打印机上打印出游戏软件中必需使用的文件名。

程序 TRACE.ASM 的清单如下：

```
code segment
    assume cs:code,ds:code,es:code,ss:code
    org 100h
start:
    jmp setup
old21 dd 0
ssss dw 0
sspp dw 0
mess1  db '游戏软件存档跟踪实用工具 TRACE',13,10
       db '国家医药管理局重庆医药设计院 曹国钧编制 ',13,10
       db '日期:1996 年 4 月 8 日 ',13,10,'$'
new21  proc far          ;建立新的 INT 21H 中断向量
       pushf
       cmp ah,3dh        ;DOS 系统功能调用的打开文件子功能 3DH
       je loc—9
       cmp ah,4bh        ;DOS 系统功能调用的执行文件子功能 4BH
       je loc—9
       popf
       jmp cs:old21      ;不是,执行原来的 INT21H 功能调用
       cmp al,7ch
       je loc—9
       popf
       jmp cs:old21
loc—9:push ax           ;新的 INT 21H 功能调用
       push bx
       push cx
       push dx
```

```
        push di
        push si
        push es
        push ds
        push bp
        mov ax,ss
        mov cs:ssss,ax      ;保存堆栈段地址到 CS:SSSS
        mov ax,sp
        mov cs:sspp,ax      ;保存堆栈偏移地址到 CS:SSSP
loc—10:
    mov si,dx
loc—11:
        lodsb
        cmp al,0
        je loc—12
        mov ah,5
        mov dl,al
        int 21h         ;打印机上打印出执行或打开的文件名
        jmp short loc—11
loc—12:
        mov dl,0ah
        int 21h
        mov dl,0dh
        int 21h         ;换行
        mov ah,0
        mov al,2
        int 16h          ; 按任意键,执行下一个 INT 21H 功能调用。
        mov ax,cs:ssss      ;恢复堆栈段地址到 CS:SSSS
        mov ss,ax
        mov ax,cs:sspp      ;恢复堆栈偏移地址到 CS:SSSP
        mov sp,ax
        pop bp
        pop ds
        pop es
        pop si
        pop di
        pop dx
        pop cx
        pop bx
        pop ax
        popf
        jmp cs:old21
```

```
new21 endp
    setup:
        push cs
        pop ds
        mov dx,offset mess1
        mov ah,09h
        int 21h
        mov ax,3521h          ;获取 INT 21H 的中断向量地址
        int 21h
        mov si,offset old21
        mov [si],bx
        mov [si+2],es         ; 保存 INT 21H 中断向量到 OLD21 中
        mov dx,offset new21
        mov ax,2521h
        int 21h           ;安装新的 INT 21H 中断向量
        mov dx,offset setup+1
        int 27h            ; 驻留退出
code ends
        end start
```

附录 F：

动态装载设备驱动程序命令 DEVLOAD

在 PC DOS 7.0 新提供了一个动态装载设备驱动程序命令 DEVLOAD.EXE，它有以下两种使用格式：

格式 1：(基本内存)

```
DEVLOAD  设备驱动程序  [参数 1 参数 2  参数 3...]  [/?]
```

格式 2：(高端内存)

```
LOADHIGH DEVLOAD  设备驱动程序  [参数 1 参数 2  参数 3...]  [/?]
```

说明：设备驱动程序应含必要的全路径，如 C:\PCDOS7\HIMEM.SYS 等。

参数 1 参数 2 参数 3. . .是设备驱动程序所携带的参数，如对于 HIMEM.SYS 可带/INT15=384K 等。

/? 提供 DEVLOAD 的命令列表。

下面以两个例子说明 DEVLOAD 的使用方法。

【例子 1】CCBIOS 2.13H 在 286 以上可将显示字库放在虚拟盘中使用，若在 CONFIG.SYS 未装载虚拟盘驱动程序 RAMDRIVE.SYS，则可用 DEVLOAD.EXE 命令直接加载，而需要重新启动系统。下面就是具体步骤。

(1) DEVLOAD C:\DOS\HIMEM.SYS 装载 HIMEM.SYS 驱动程序

(2) DEVLOAD C:\DOS\RAMDRIVE.SYS 384 512 32/E 装载 RAMDRIVE.SYS 驱动程序，并在扩展内存(XMS)中设置了 384KB 的虚拟盘 D(若微机中只有一个 C 分区)。

(3) 执行启动 2.13H 的批处理文件 213.BAT，选择 3 即可。

【例子 2】在工作站上网或使用不同版本的 DOS 外部命令，如在 MS DOS 6.2 中使用 MS DOS 5.0 的 EDLIN. EXE 程序，一般需要用 MS DOS 6.2 的版本模拟驱动程序 SETVER.EXE 将 EDLIN.EXE 设置为 MS DOS 6.2 的运行环境，但启动微机时未在 CONFIG.SYS 中设置 DEVICE=C:\DOS\SETVER.EXE，并且需要重新启动微机，修改 SETVER.EXE 版本表才可使用 EDLIN. EXE，十分麻烦。现在 PC DOS 7.0 中有了 DEVLOAD 命令就方便许多。下面就是这方面的两个应用实例。

1. 将 MS DOS 5.0 的 EDLIN.EXE 放在 MS DOS 6.2 中运行。

(1) SETVER EDLIN.EXE 5.0 将 EDLIN.EXE 设置为 MS DOS 6.2 运行环境。

(2) LOADHIGH DYNALOD C:\DOS\SETVER.EXE 加载 SETVER.EXE。

(3) EDLIN CGJ.CCC 此时用 MS DOS 5.0 的 EDLIN.EXE 可在 MS DOS 6.2 中编辑文件 CGJ.CCC 了。

2. 将 MS DOS 4.0 的 NET4.COM 放在 MS DOS 5.0 中运行

(1) SETVER NET4.COM 4.0 将 NET4.COM 设置为 MS DOS 5.0 运行环境。

(2) LOADHIGH DYNALOD C:\DOS\SETVER.EXE 加载 SETVER.EXE。

(3) 执行 IPX.COM 和 NET4.COM 就能正常入网了。

同样,用户利用 DYNALOD 命令,也可将 MS DOS 5.0 的 BACKUP.EXE 命令移植到 MS DOS6.0 以上版本中。