电脑实用工具精粹

刘建新 崔维娜 等编著

北京航空航天大学出版社
http://www.buaapress.com.cn

电脑实用工具精粹

刘建新 崔维娜 等编著

北京航空航天大学出版社
http://www.buaapress.com.cn

内 容 简 介

工具软件是任何计算机用户必不可少的帮手。本书以通俗易懂的语言、简洁明了的实例、图文并茂的风格、深入浅出地详细展示了一些工作和学习中必用的优秀计算机工具软件的使用方法。本书共由9章组成，每章讲解一类工具。本书特别适合于计算机初级用户使用，对计算机中级用户也有很大的帮助。

图书在版编目(CIP)数据

电脑实用工具精粹/刘建新等编著. —北京：
北京航空航天大学出版社，2000.9
ISBN 7-81012-998-8

Ⅰ.电… Ⅱ.刘… Ⅲ.软件工具-基本知识
Ⅳ.TP311.56

中国版本图书馆CIP数据核字(2000)第47487号

电脑实用工具精粹

刘建新 崔维娜 等编著

责任编辑 张光斌 范曼华

北京航空航天大学出版社出版发行

北京市学院路37号(100083)发行部电话：82317024 发行部传真：82328026

http://www.buaapress.com.cn

E-mail:pressell@publica.bj.cninfo.net

河北省涿州市新华印刷厂印刷 各地书店经销

*

开本：787×1092 1/16 印张：22 字数：600千字

2000年11月第1版 2000年11月第1次印刷 印数：5000册

ISBN 7-81012-998-8/TP·411 定价：33.00元

前　言

近年来，计算机在各个领域的应用迅速发展，相应的计算机软件也日新月异，功能越来越强大，种类越来越齐全。作为应用软件的一个重要组成部分，工具软件也犹如雨后春笋，新的软件层出不穷。

工具软件对计算机用户而言，就如同日常生活中的工具，随时随地都有可能使用。各种各样的工具软件在平时使用计算机时将成为用户的良师益友，同时也会使得复杂繁重的工作变得轻松愉快。但工具软件的种类浩瀚如烟海，一个人要掌握所有的工具软件，既不可能也没有必要。笔者编写该书的目的主要在于帮助广大计算机用户迅速了解相关的主流计算机工具软件，并在较短时间内熟练使用这些工具，在平时的工作中收到事半功倍的效果。在本书中将最常用的工具软件分为9类，每一类讲述几个主流的软件，旨在帮助计算机用户迅速找到并掌握所需要的工具软件。在本书的编写过程中，本着支持民族产业的原则，同类软件中优先选择国产软件。

本书覆盖面广，讲述软件的种类多，而工具软件尤其是一些小的软件，发展更新速度很快，用不了几个月就有新的版本推出。因此，尽管在编写时所有的软件都是最新的版本，但在本书出版后可能很多的软件已经升级。但这并不影响本书的参考价值，因为软件的升级不是跳跃式的，而是循序渐进的。大部分软件的新版本和前一版本使用方法差别不大，只是功能有所增强。会使用该软件的前一版本，则使用后一版本也不成问题。

本书由刘建新、崔维娜等负责编写。全书共分9章，第1章杀毒工具由刘建新编写；第2章图形图像工具由崔维娜编写；第3章媒体播放工具由史建刚、付　云编写；第4章翻译工具由杨学海、徐兴良编写；第5章解压压缩工具由戴佳毅编写；第6章网络工具由高泽华、孙　虹、孔林昱编写；第7章测试工具由刘钦恩编写；第8章桌面工具由李　伟编写；第9章其他工具由孔林昱、韦冠男编写。

本书约定：按钮一律使用【】括起，窗口、对话框、选项菜单一律使用引号“”引起，“菜单|选项”表示某菜单下的某个选项；对于层次，先用1，2，3……，其下使用(1)，(2)，(3)……，再下层次使用①，②，③……表示。对于并列的项目如特点等用项目符号表示。

由于水平所限，本书中的错误疏漏之处在所难免，请读者批评指正。

编　者

2000年9月

目 录

第1章　杀毒工具

计算机病毒能将自身传染给其他的程序，并能破坏计算机系统的正常工作程序。

它们都具有如下共同的特性：

- 传染性

传染性是所有病毒程序都具有的一大特性。通过传染，病毒就可以扩散。病毒程序通过修改磁盘扇区信息或文件内容并把自身嵌入到其中的方法达到病毒的传染和扩散。

- 破坏性

大多数计算机病毒在发作时都具有不同程度的破坏性，有的干扰计算机系统的正常工作，有的占用系统资源，有的则修改和删除磁盘数据或文件内容，更有甚者，能破坏计算机的硬件。

- 隐蔽性

计算机病毒的隐蔽性表现在两个方面：一是传染的隐蔽性，大多数病毒在进行传染时速度是极快的，一般不具有外部表现，不易被人发现；二是病毒程序存在的隐蔽性，一般的病毒程序都夹在正常程序之中，很难被发现，而一旦病毒发作出来，往往已经给计算机系统造成了不同程度的破坏。

- 寄生性

病毒程序嵌入到宿主程序中，依赖于宿主程序的执行而生存，这就是计算机病毒的寄生性。病毒程序在侵入到宿主程序中后，一般对宿主程序进行一定的修改，宿主程序一旦执行，病毒程序就被激活，从而可以进行自我复制和繁衍。

- 潜伏性

计算机病毒侵入系统后，一般不立即发作，而是具有一定的潜伏期。病毒不同，其潜伏期的长短就不同，有的潜伏期为几个星期，有的潜伏期为几年。在潜伏期中病毒程序只要在可能的条件下就会不断地进行自我复制、繁衍和传染。一旦条件成熟，病毒就开始发作。

近年来，计算机病毒的危害越来越大，仅1999年4月26日爆发的CIH病毒就使至少100万台电脑受到破坏，2000年4月26又同样造成了严重损失。因此，在日常使用中杀毒防毒具有重要的意义。但是，几乎每一天都有新的病毒出现，因此杀毒软件的病毒库也要随时更新，但核心的东西和使用方法却不会改变。本章介绍几个国产的杀毒软件。

1.1　KV300杀毒软件

1.1.1　KV300的特点

KV300是由北京江民新技术有限责任公司开发的计算机杀病毒软件，该软件可以检测清

除计算机病毒。KV300 具有很强的查毒、杀毒功能，是一个较好的 DOS 杀毒软件。它具有下列特点：

- 采用独特的开放式系统，不需编程就可以方便地不断增加 KV300 检测和清除计算机病毒的数量。在发现新病毒后，可以自行抽取新病毒特征码来扩充查毒和增加杀毒代码，还可以通过有关报刊来获取新病毒特征码和杀毒代码来升级 KV300，提高 KV300 的查毒和杀毒能力。
- KV300 是目前惟一的具备扩展开放式和封闭式两项功能的杀毒软件。扩展开放式使得 KV300 具有扩展功能。
- KV300 首次设计出独特的特征代码过滤器，很容易查出部分变种和变换自身代码的变形病毒，也可以很容易地查出 WORD 宏病毒。
- KV300 具有多种查毒方法，如“特征代码过滤法”、“步步跟踪法”、“逻辑判断法”和“逆转显影法”等。如此多的查毒方法可以保证 KV300 具有足够的能力来查杀各种复杂病毒。
- KV300 可以直观地查看硬盘的物理扇区的主引导和 BOOT 引导信息是否正常。
- KV300 能够安全地杀除所有主引导区病毒，在杀主引导区病毒时，KV300 可以将主引导信息保存到软盘上，防止万一破坏主引导信息时可以安全恢复。
- KV300 采用广谱智能检测系统可查出许多引导区和文件类未知新病毒。
- KV300 一次启动就可以很方便地检查和杀除许多软(硬)盘中的病毒，能解除交叉感染的多层病毒。
- KV300 具有自我检查和修复功能，能够自我解除自身感染的病毒。
- KV300 能够检测、修复和重构硬盘分区表，能够恢复丢失的硬盘。
- KV300 能够方便地升级，及时杀除最新病毒。
- KV300 具有简单的操作界面，可以方便地用于 DOS、Windows 9X、Windows NT 和 UNIX 操作系统。

1.1.2 KV300 的使用

下面讲述 KV300 的使用步骤。

1. 利用引导盘启动计算机

为了确保内存中没有驻留病毒，在使用 KV300 清杀病毒之前，应该使用干净无毒系统盘从软盘引导计算机(必须采用冷启动)。

如果计算机上的系统为 Windows 95(OSR2)或 Windows 98、NT 等 32 位版本，若采用 DOS 7.0 以下的系统软盘引导，硬盘将不会被确认。采用 FAT16 格式化的硬盘，安装 Windows 98 后，利用 DOS 7.0 以下的系统软盘或 KV300 软盘引导，有些文件可能会无法打开。可以采用 DOS 7.1 以上版本或 Windows 98 启动盘启动计算机，计算机启动后重新插入 KV300 软盘，在“A:>”提示符下键入“KV300”启动 KV300。

可以按照如下方式快速制作一张 DOS 7.1 系统引导盘。

将一张格式化过的软盘放在一台装有相应操作系统并且无病毒的机器软驱内，启动 MS-DOS 快捷方式，在 C 盘提示符下键入“SYS A:”即可自行制作一张引导盘。

也可以按照如下步骤制作引导盘：

第 1 步：将一张格式化过的软盘放在一台装有 Windows 98 操作系统并且无病毒的机器软

驱内。

第 2 步:打开 Windows 98 的开始菜单,单击“运行”选项,弹出如图 1.1 所示对话框。

第 3 步:在命令行内键入“SYS A:”,单击【确定】按钮,计算机就会制作出一张该系统的引导盘。

尽量避免使用 KV300 原盘来引导计算机,这样会降低 KV300 盘片的使用寿命,应该在使用其他相应引导盘引导后,再运行 KV300。

2. 运行 KV300

计算机启动以后,进入 DOS 环境。首先将 KV300 的原盘插入软驱内,在“A:>”提示符下键入“KV300”,回车后即可启动 KV300,如图 1.2 所示为 KV300 的启动画面。按下任意键后,即可进入 KV300 的工作界面,如图 1.3 所示。下面详细叙述其各项功能及操作方法。

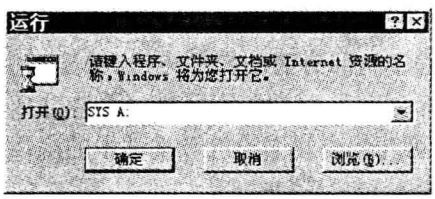

图 1.1　运行“SYS A:”对话框

图 1.2　KV300 的启动画面

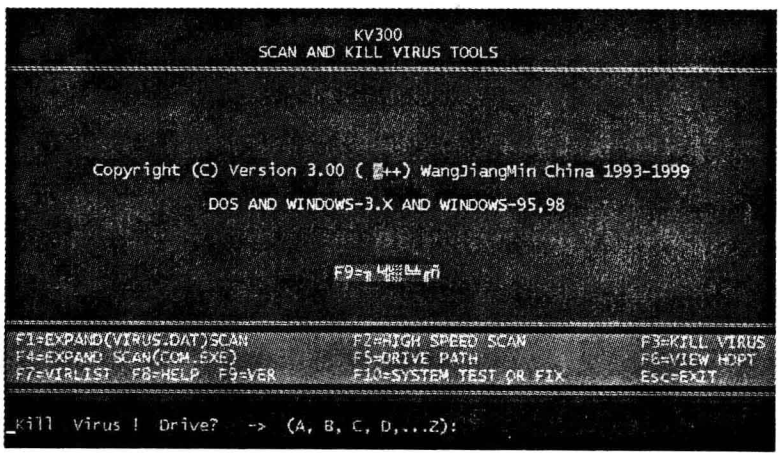

图 1.3　KV300 的工作界面

该工作界面为 KV300 的缺省状态(功能键 F3),即清杀硬盘中的已知名病毒。选取相应分区如 A,B,C,D…等,KV300 即可以查找并杀除该分区内所检测到的病毒。

运行 KV300 后,系统将程序装入内存。KV300 运行后可以取出原盘,这样可以利用 KV300 清杀软盘上的病毒。此外 KV300 还可以查找光盘中的病毒,但不能杀除,一般可以将光盘中的数据拷贝到硬盘上,然后用 KV300 进行清杀。

F1 键——用 KV300 的第一套查毒方式,即采用外部开放式可扩展的病毒特征库(VIRUS.DAT)和扫描过滤法对引导区和所有的文件进行全代码扫描搜索病毒,这种方式灵敏度和准确度极高,但扫描速度稍慢,如图 1.4 所示。进入该界面后,选择相应分区,即按相应键,如果要

杀除 C 区病毒，键入“C”键，KV300 即可开始查找引导区和文件中的病毒。

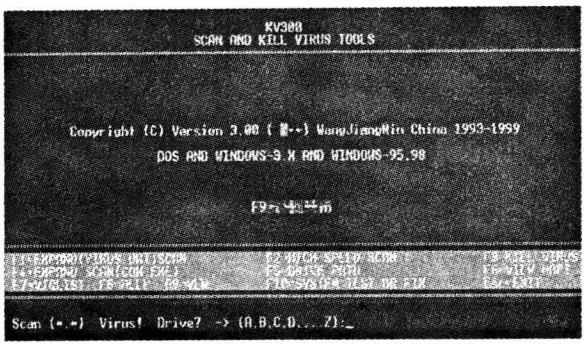

图 1.4　用病毒特征库 VIRUS. DAT 查找病毒

F2 键——用 KV300 的第二套查毒方式，即采用程序内部封闭的扫描方法，快速对引导区和所有文件中的病毒进行扫描，速度较快，如图 1.5 所示。进入该界面后，选择相应分区，即按相应键，如果要杀除 C 区病毒，键入“C”键，KV300 即可开始查找引导区和文件中的病毒。

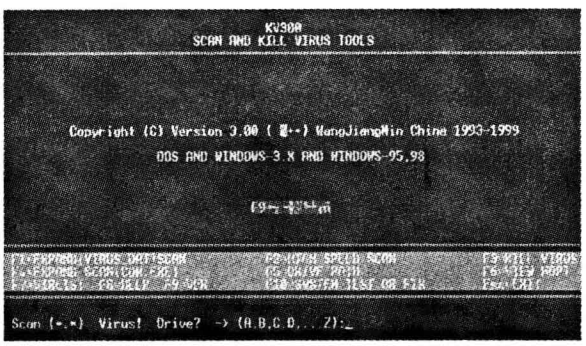

图 1.5　用程序内部封闭的扫描法查找病毒

F3 键——快速清杀文件中的病毒，该功能是 KV300 启动后的缺省功能。进入该界面后，选择相应分区，即按相应键，如果要杀除 C 区病毒，键入“C”键，KV300 即可开始查找并清杀文件中的病毒。

F4 键——用 KV300 的第一套查毒方式，即采用外部开放式可扩展的病毒特征库（VIRUS. DAT）和扫描过滤法对引导区和所有. com 和. exe 文件进行全代码扫描搜索病毒，这种方式灵敏度和准确度极高，但扫描速度稍慢，如图 1.6 所示。此种方法适用于搜索网络服务器。进入该界面后，选择相应分区，即按相应键，如果要杀除 C 区病毒，键入“C”键，KV300 即可开始查找引导区和文件中的病毒。

F5 键——对某一子目录内的所有文件进行扫描和清除，如图 1.7 所示。在命令行中输入相应的目录，如“c:\windows”。回车后，KV300 即可开始查杀该目录内所有文件的病毒。

F6 键——可查看硬盘的引导区记录和硬盘的分区表，可以查找移动过的主引导记录和硬盘的分区表，并向 A 盘备份保存。

F7 键——显示病毒名及其基本性质。使用该功能时首先应该启动汉字环境。

F8 键——显示使用说明，使用该功能时也需要启动汉字环境。

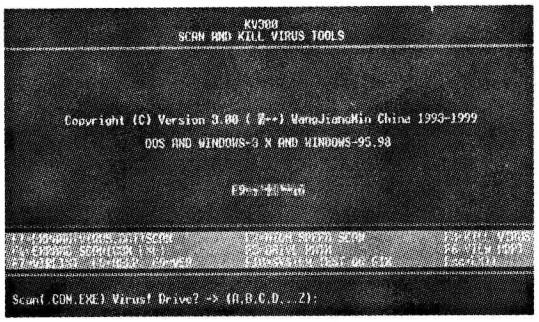

图 1.6　用病毒特征库 VIRUS. DAT 和扫描过滤法查找引导区和. com、. exe 文件中的病毒

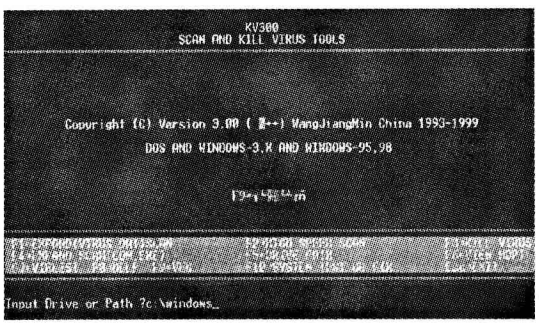

图 1.7　查找和清除指定目录中的病毒

F9 键——显示版本号和简易说明，该功能也要启动汉字环境。

F10 键——该功能可以自动测试和快速修复硬盘分区表。当由于硬盘分区表受到病毒或人为破坏而无法启动时，利用该功能一般可以修复硬盘分区表，恢复丢失的硬盘。

3. 退出 KV300

清杀完硬盘中的病毒后，按“Esc”键可以退出 KV300。在任何功能内只要按“Esc”键，就可以退出 KV300。KV300 杀毒过程中按“Esc”键可以停止当前的动作，返回操作界面。

如果 KV300 查到 Word 的宏病毒时，一般要提示是否杀除。此时应该注意，有些染有宏病毒的文档杀毒后不能打开，因此在杀除这些病毒之前，应该对这些文档进行处理，可以按照如下方法进行处理。

当 KV300 查到 Word 宏病毒，要求选择杀除（按“Y”键）或不杀除（按“N”键）时，应该按“N”键，暂时不杀除该病毒。等到 KV300 检查完整个硬盘后，按“Esc”键，退出 KV300。重新启动 Windows，用 Word 打开带有宏病毒的文档，如图 1.8 所示。单击“编辑”菜单，在下拉菜单中单击“全选”选项，Word 将选中所有文档，然后打开“编辑”菜单单击“复制”选项，将所有文档拷贝到剪贴板中。

然后，打开“开始”菜单，鼠标指向“程序”选项，打开该子菜单后指向“附件|选项”，运行 Windows 自带的写字板软件，将剪贴板中的内容拷贝到写字板内，将该文件存为文本文件格式（*.txt）或（*.rtf）格式。因为 Word 宏病毒不能感染这两种文档格式。

如果选择“Y”，即杀除了该宏病毒而导致打不开该文档时，可以采用下面的方法进行

恢复：

• 利用写字板软件打开该文档。有些带有 Word 宏病毒的文档在杀完毒后，Word 无法打开该文档，此时可以用写字板打开该文档。

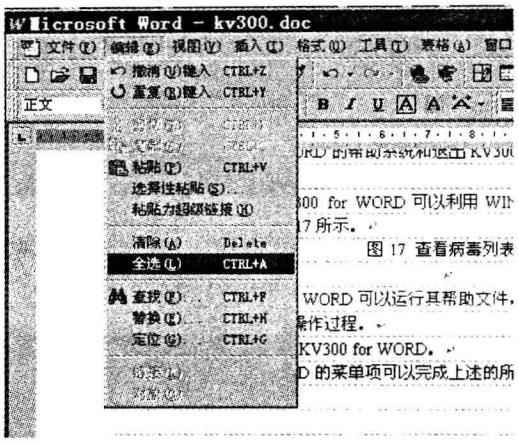

图 1.8　拷贝带有 Word 宏病毒的文档内容

• 如果写字板也无法完全打开，此时系统一般提示是否尝试恢复该文档，如果选择恢复，一般很难打开此文档，此时应该选择不恢复，这样可以恢复文档中的所有文本内容。

4. 保存和恢复硬盘主引导信息

如果硬盘的主引导信息受到病毒或人为破坏时，计算机将无法启动，利用 KV300 可以向 A 盘备份一个硬盘的主引导信息档案，其名为：hdpt. dat。具体操作过程如下：

第 1 步：准备一张干净无病毒、格式化过的软盘。

第 2 步：用一张干净的引导盘引导计算机启动，进入 DOS 环境。

第 3 步：插入 KV300 原盘，在命令行中键入：KV300/B，按“Enter”键后计算机开始运行该程序，出现如下提示。

Backup Hard Disk Partition Table.

并要求输入要保存的硬盘。如果系统只有一个硬盘，可直接按“Enter”键，KV300 进一步提示是否继续操作。此时需要按照提示进行第 4 步操作。

第 4 步：取出 KV300 原盘，插入准备好的干净软盘，按“Y”键后，KV300 即可在软盘上备份硬盘的主引导信息，文件名为 hdpt. dat。

第 5 步：取出软盘，在软盘的选项卡上写明该机器的机器型号、硬盘容量和分区大小，再设置为写保护后长期保存。

注意：当计算机的硬盘重新分区或该计算机换了新的硬盘后，原来备份的硬盘主引导信息将不能再使用，应该按照上述方法重新备份一个。

当硬盘的主引导信息受到破坏而需要恢复时，取出上面所制作的备份盘，利用软盘引导并启动计算机后，将该盘放入软驱内，在命令行内键入 KV300/HDPT. DAT 即可将引导信息恢复到该硬盘中。

上述 2 种命令配合使用，可以解决大部分硬盘主引导信息受到破坏计算机无法启动的现象。

提示:使用这种格式时,千万不可搞错硬盘!也必须证明该硬盘以后没有重新分区和格式化过。

5. 清除所有引导区型病毒

KV300 可以清除引导区型病毒,在清除引导区型病毒之前,可以将硬盘的主引导信息(带毒或不正常)保存在软盘上。与上面所提到的保存和恢复硬盘主引导信息不同,前者是保存无毒的主引导信息,在硬盘的主引导信息受到破坏后可以正常恢复,而后者是为了防止 KV300 在清除主引导信息型病毒时万一破坏了硬盘的主引导信息,可以利用该备份来恢复。因此在清除病毒之前需要保存当前的主引导信息。

清除主引导信息型病毒的操作过程如下:

第 1 步:用无毒的 DOS 启动盘引导计算机(一定要冷启动机器)。

第 2 步:插入 KV300 原盘,在命令行内键入 KV300/K,按"Enter"键后计算机开始运行该程序。

第 3 步:在提示符"Kill All Boot Virus. (A,B,C):"下键入"C"键,运行一段时间后,KV300 会提示插入一张格式化过的软盘,并选择是否进一步操作。

第 4 步:取出 KV300 原盘,插入一张格式化过的软盘,在提示符下键入"Y"键,KV300 即可保存当前主引导信息并清除硬盘主引导信息型病毒。

KV300 将硬盘当前的主引导信息保存在软盘上,并取名为 HDPT. VIR。生成该文件的目的是防止万一原硬盘的主引导信息中有某种加锁的密码也被解除了而不能工作时,可以利用该文件恢复硬盘的主引导信息。其具体过程如下:

利用 DOS 系统盘引导计算机,插入备份有硬盘主引导信息的软盘,在命令行内键入:KV300/HDPT. VIR 即可恢复硬盘的主引导信息。

提示:恢复主引导信息之前,应该将主板的 CMOS 中的"BIOS Features Setup"选项的"PBUA - Virus Protection"项设为"DISABLE"。

6. 在 Windows 下查杀 Word 宏病毒

在 KV300 的原盘中带有安装文件"kvwsetup. exe"。进入 Windows 后,运行该文件,按照安装向导的提示可以很方便地安装 KV300 for WORD 软件,并在桌面上自动建立一个图标,同时将快捷方式加入 Windows 的开始菜单内,如图 1.9 所示。

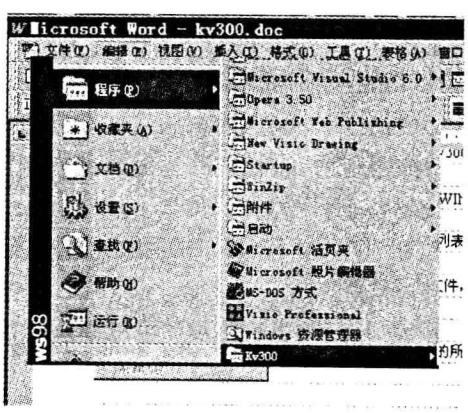

图 1.9 加有 KV300 for WORD 的开始菜单

KV300 for WORD 可以查找并清除 Word 文档中的宏病毒，查杀宏病毒时，可以只选择软盘、硬盘的一个分区或硬盘中的某一个文件夹。

安装完毕后，单击 KV300 for WORD 图标，计算机即可以启动该 KV300 for WORD，其主界面如图 1.10 所示。KV300 for WORD 的主界面主要包括菜单项、工具栏、磁盘图标行、路径编辑框、扫描信息窗口和状态栏 6 个部分。

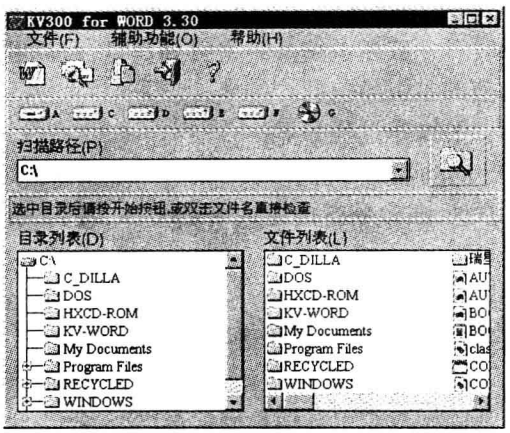

图 1.10　KV300 for WORD 的主界面

7. KV300 for WORD 的使用

（1）设置扫描路径。在查杀病毒之前，需要先设置扫描路径。KV300 for WORD 提供了多种设置方式，以满足特定的需要。

选择整盘——在磁盘图标行相应磁盘图标上单击，即选定相应磁盘，如单击 C 盘图标即可以选择 C 盘。KV300 for WORD 可以同时选择多个磁盘进行扫描，方法是在单击时按下“Ctrl”或“Shift”键，操作方法与 Windows 多项选择操作相同。或者在磁盘图标上右击，选择相应选项。如果检查整个硬盘，则无需选择目录。

（2）选择目录。在目录列表框内选择目录。带有“+”号图标的目录项表示有下级目录，可以双击展开。如果检查该目录，则无需再选择文件。

（3）选择文件。有时可能需要检查某个文件是否有毒，在文件列表框内双击文件名，即可直接检查。

此外，还可以在路径编辑框内直接输入扫描路径。如果想要一次扫描多个路径，可以都输入进去，在每两个路径之间以分号分隔。输入结束后按回车键进行扫描。

（4）开始检查。设置好扫描路径后，在扫描路径编辑框右侧【开始】按钮上单击，或者在查杀宏病毒按钮上单击，即开始扫描检查。图 1.11 列出了 KV300 for WORD 的常用命令按钮。

【查毒】按钮——单击该按钮，KV300 for WORD 可以检查选定的硬盘或目录中的 Word 文档，该功能只检查病毒，而不进行杀除。

【杀毒】按钮——单击该按钮，KV300 for WORD 可以清杀选定的硬盘或目录中的 Word 文档，该功能可以杀除文档中的病毒。

【扫描】按钮——单击该按钮，KV300 for WORD 可以扫描并检查文件中的病毒。在该按钮上右击，会弹出一个菜单，如图 1.12 所示。