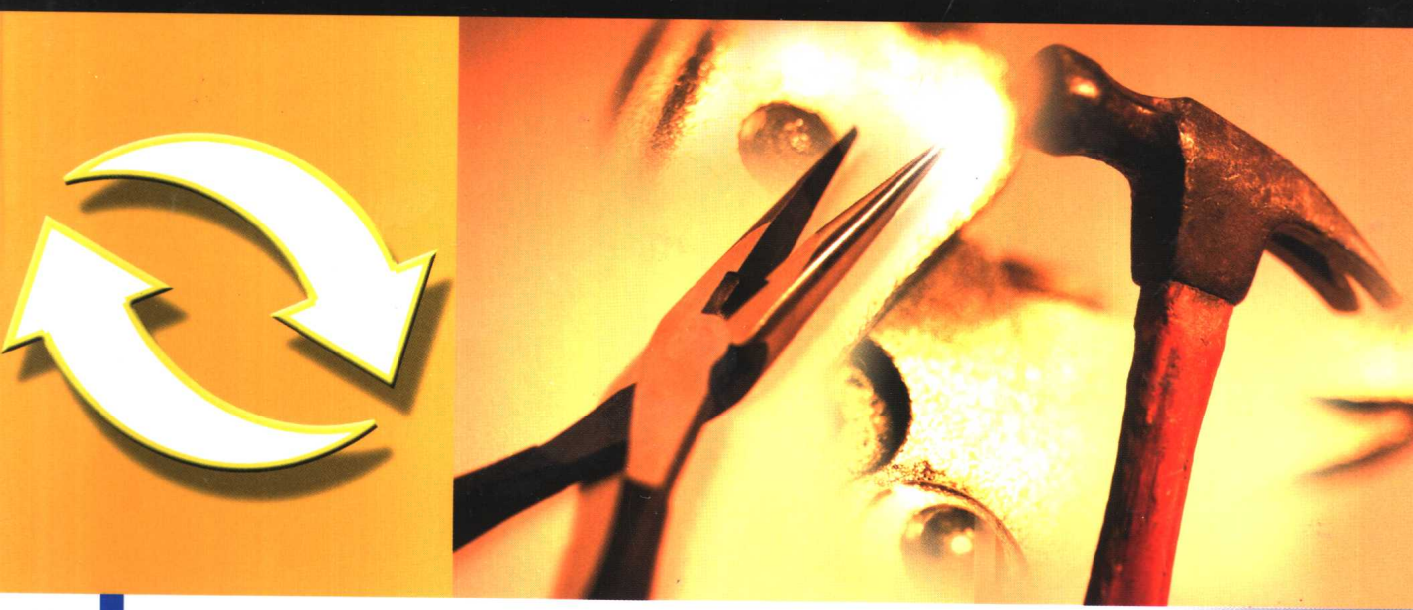
21世纪计算机高职高专系列教材



常用工具软件的使用

康耀红　黄健青　魏应彬　主编
杜育宽　张　晋　编著

北京大学出版社
http://cbs.pku.edu.cn

符合高职高专教学大纲

21世纪计算机高职高专系列教材

常用工具软件的使用

康耀红　黄健青　魏应彬　主编

杜育宽　张　晋　编著

北京大学出版社

北　京

内 容 提 要

本书是“21 世纪计算机高职高专系列教材”之一。全书分别以最新版本的工具软件为例，向读者详尽地介绍了目前国内外广泛流行的常用工具软件的特点、使用方法、注意事项和操作技巧。全书共分五章，内容包括：杀毒工具、图形图像工具、压缩工具、系统工具和软件备份等。附录中附有本书的教学大纲。

本书内容丰富、结构清晰、实用性强。适合作为高等职业与高等专科教育、成人教育的常用工具软件使用教材，也可作为大学非计算机专业的教材，并适合广大读者自学。

图书在版编目(CIP)数据

常用工具软件的使用/杜育宽等编著. —北京：北京大学出版社，2001.12
(21 世纪计算机高职高专系列教材)
ISBN 7-301-05030-5
I. 常… II. 杜… III. 软件工具－高等学校：技术学校－教材 IV. TP311.56

中国版本图书馆 CIP 数据核字(2001)第 040298 号

书　　名：常用工具软件的使用
著作责任者：杜育宽　张　晋
责 任 编 辑：杨锡林
标 准 书 号：ISBN 7-301-05030-5/TP·0538
出　版　者：北京大学出版社
地　　址：北京市海淀区中关村北京大学校内　100871
电　　话：出版部 62752015　发行部 62750672　编辑部 62765013
网　　址：http://cbs.pku.edu.cn
电 子 信 箱：xxjs@pup.pku.edu.cn
印　刷　者：北京大学印刷厂
发　行　者：北京大学出版社
经　销　者：新华书店
787 毫米×1092 毫米　16 开本　10.625 印张　227 千字
2002 年 1 月第 1 版　2002 年 1 月第 1 次印刷
定　　价：16.00 元

21世纪计算机高职高专系列教材
编委成员名单

前　言

扩大教育规模成为国家为实施科教兴国战略采取的重要措施。如何完善我国高等教育体系，适应新经济发展的需要，是中国教育界十分关注的问题。高职高专教育已经成为一种具有中国特色的教育模式，是我国多元化教育模式的重要组成部分，重视和发展高职高专教育对于完善我国现行教育体系具有十分重要的意义。

高职高专教育需要一定的职业基础理论和实用的职业技能，必须打破以学科为特征的传统教学内容，不应过度强调理论的深度和系统性，而应注重面向应用型人才的专业技能和实用技术。

本套丛书的作者对高职高专教育具有丰富的教学经验。在本套丛书编写过程中，编委会经过多次讨论，首先制定了全套丛书的编写风格，然后针对高职高专教育的特点确定了每本书的编写大纲，在初稿完成后，集体从正确性、条理性、通俗性等方面进行了多次加工和修订。

本套丛书共 11 本，分别为《计算机应用基础》、《计算机办公应用》、《网页设计与制作》、《多媒体计算机的组装与维护》、《计算机图形图像处理》、《多媒体技术及应用》、《Visual FoxPro 6.0 数据库设计》、《Visual Basic 程序设计》、《计算机网络基础与应用》、《常用工具软件的使用》、《会计电算化教程》，这是根据计算机科学的特点和高职高专教育的现状精心安排的。学生经过这些课程的学习，一方面能够获得计算机科学技术专业的基本知识，另一方面能够快速掌握一些基本的实用技能，为未来的自我发展奠定良好基础。

本书第 1、2 章由杜育宽执笔，第 3、4、5 章由张晋执笔。由杜育宽、张晋统稿。

高职高专教育仍在蓬勃发展之中，关于高职高专教育的研究也是一个新兴的课题，本套丛书虽经艰苦努力，但仍难免存在不足和谬误之处，恳请广大读者批评指正。

编　者

2001 年 11 月

目　录

第 1 章　计算机病毒及杀毒软件

本章要点：

- 了解和认识计算机病毒
- 常用杀毒软件

随着计算机技术和信息技术的迅猛发展，计算机在国民经济和社会发展的各个方面所起的作用已经越来越显著。这样，计算机安全问题自然就显得非常重要。在计算机安全方面最为突出的问题就是计算机病毒问题，计算机病毒就像幽灵一样无时无刻不伴随在计算机左右，不断地制造麻烦，给人们的工作和生活带来了极大的不便。因此，对于广大计算机用户来说，认识和了解计算机病毒，采取有效的安全防范措施以防止病毒的侵害是很有必要的。所以，本章先对计算机病毒做简要阐述，然后，介绍计算机病毒的预防及常用杀毒软件的使用方法和技巧等。

1.1　计算机病毒的定义

大家知道，一个完整的计算机系统包括硬件系统和软件系统。计算机硬件只是一个执行者，做什么、怎么做，都需要人来预先设计好程序，这些程序就是些计算机软件。人可以编制出让计算机硬件为大家服务的程序，当然也可以设计出让计算机硬件完成一些人们不愿看到的程序，如破坏计算机系统的程序，这个程序除了破坏计算机系统之外，还有一些其他的特点，如它能在计算机系统内部自我复制等。由于这一特殊的计算机程序具有与生物学病毒相类似的特征（传染性、潜伏性、寄生性等），所以人们借用了生物学上病毒的名字来称呼它，即计算机病毒。

与生物病毒类似，计算机病毒是一种能够自我复制的计算机程序，这种程序是能够修改程序并把自身“传染”给其他程序的程序，这种传染往往是在违背用户意愿的情况下隐蔽进行的。病毒通过传染可能扩散侵入很多计算机系统，当条件被满足时就会破坏计算机的正常工作，给用户造成巨大损失。

计算机病毒最大的特点是具有主动传染性。病毒可以侵入到整个系统，使其受到感染，而每个受感染的程序又可能成为一个病毒，继续将病毒传染给其他程序。携带计算机病毒的程序被称为计算机病毒载体或被感染程序。这些寄生于应用程序或系统其他部分的病

毒，一方面不断自我复制，传染其他正常程序；另一方面在宿主程序执行的某个阶段，能够取得控制权。然而，正常的计算机程序是不会将自身的代码强行连接到其他程序之上的，即不会传染给其他程序，当然更不会有控制权易主问题的存在。

从广义上讲，凡是能够引起计算机故障，破坏计算机数据的程序统称为计算机病毒。依此，诸如特洛伊马、逻辑炸弹等均可称为计算机病毒。但从狭义上确切地定义计算机病毒，许多专家和研究者对其做过不尽相同的定义，却没有公认的明确定义。一种定义是能够实现自我复制且借助一定的载体存在的具有潜伏性、传染性和破坏性的程序。另一种定义是一种人为制造的通过不同的途径潜伏或寄生在存储媒体或程序里的程序，当条件或时机成熟时，它会自身复制并传播，使计算机的资源受到不同程度的破坏等等。

确切地说，计算机病毒就是那些能够通过某种途径潜伏在计算机系统内部不断自我繁殖，危及计算机系统正常工作，浪费和破坏系统资源的一种特殊的计算机程序。

1.2　计算机病毒的基本特征

计算机病毒主要具有以下特征：

（1）潜伏性

病毒进入计算机系统之后并不是马上就破坏计算机资源的，而是要潜伏一段时间，这就是病毒的潜伏性。从病毒感染某计算机系统开始到该病毒发作为止的这段时间，就是病毒的潜伏期。在潜伏期，其隐藏在合法文件中，对其他系统进行传染，而不会被人发现。潜伏性愈好，在系统中的存在时间就会愈长，病毒的传染范围就会愈大。一旦发作，造成的破坏性也就愈大。如 1999 年 4 月 26 日 CIH 病毒大爆发，据报道，国内有近 40 万台计算机遭到破坏，这是因为病毒可能在此之前早已感染了计算机，但是由于不满足发作条件，因而许多用户并未意识到，到了 26 日满足了病毒发作的条件，于是就有如此众多的计算机遭到了破坏。假如病毒一感染就马上发作的话，也许 26 日以前病毒发作的事例会引起其他用户的警觉，在 26 日也就可能不会遭到如此大的损失。

一般来说，计算机病毒的潜伏性主要表现在两方面：一方面是如不用相关的专用检测查毒软件，病毒是很难检查出来的，因此病毒可以隐藏在合法文件中肆意繁殖，一旦时机成熟，得到运行机会，就进行破坏，并四处繁殖、扩散，继续为害。另一方面是指计算机病毒的内部往往有一种触发机制，不满足触发条件时，病毒除了传染外不做什么破坏。触发条件一旦得到满足，计算机病毒就会发作，造成破坏。比如以时间作为发作条件的耶路撒冷病毒、CIH 病毒等。此外，还有以计数器、键盘字符输入等作为触发条件的。

（2）传染性

传染性是病毒的基本特征。生物学上的病毒会通过各种途径进行传染，计算机病毒也

一样，也能通过各种途径在计算机之间传播。与生物病毒不同的是，计算机病毒是一段人为编制的计算机程序代码，这段程序代码一旦进入计算机并得以执行，它就会搜索其他符合其传染条件的程序或存储介质，确定目标后再将自身代码插入其中，达到自我繁殖的目的。一台计算机一旦染毒，如不及时处理，那么病毒会在这台机器上迅速扩散，其中的大量文件会被感染。而被感染的文件又成了新的传染源，再与其他机器进行数据交换或通过网络接触，病毒会继续进行传染。

计算机病毒具有很强的传染性，可以说是无孔不入，到处渗透。比如 1998 年 11 月 2 日晚，ARPA 网上所有正在运行的计算机突然停止了正常工作，屏幕显示一片混乱，这个连接全美约三百所大学、公司、研究中心、军用基地的网络系统及与之相连的军用、民用及其他计算机网络系统都同时出现了类似的故障，整个网络瘫痪近一天。

除了病毒故意传染外，有时候人们也会在有意无意之中促成病毒的传播，甚至成为传播病毒的“工具”或者“通道”。比如把一个感染了病毒的程序拷贝到一台没有感染该病毒的计算机中，那么这台计算机就会感染上该病毒。现在，随着计算机网络的广泛应用，病毒传播的途径越来越多。

（3）破坏性

计算机病毒的目的，就是要让他人的计算机系统不能正常工作，对计算机用户造成不同程度的破坏。如 CIH 病毒对硬盘进行格式化破坏用户数据和应用程序等。当然，病毒的破坏性有大有小，这取决于入侵系统的计算机病毒其设计者的目的。如果病毒设计者的目的在于彻底破坏系统的正常运行的话，那么这种病毒对于计算机系统进行攻击造成的后果是难以设想的，它可以毁掉系统的部分数据，也可以破坏全部数据并使之无法恢复。但并非所有的病毒都对系统产生极其恶劣的破坏作用。有时几种本没有多大破坏作用的病毒交义感染，也会导致系统崩溃等重大恶果。所以，常常根据其破坏力的大小把病毒分成破坏性不大的一般病毒和破坏性极大的恶性病毒。

一般而言，计算机病毒的破坏性主要表现为：占用 CPU 时间和内存开销，从而造成进程堵塞；对数据或文件进行破坏；干扰外围设备正常工作等。

（4）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，很难被发觉，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。

（5）多样性

计算机病毒的多样性也表现在两个方面：一是指病毒有很多种。据不完全统计，目前已有几万种计算机病毒，而且每天都有新的病毒产生，威胁着计算机系统和数据的安全。二是指某些病毒有很多变种，使人防不胜防。如 CIH 病毒至少已经发现了五个变种。这就像感冒病毒一样，具有多种变种，因此使得很多感冒药使用周期很短，迫使加快新感冒

药的研制。

1.3　计算机病毒的类型

按照计算机病毒的特点及特性，计算机病毒的分类方法有许多种。因此，同一种病毒可能有多种不同的分法。有按照计算机病毒攻击的系统分类；按照病毒的攻击机型分类；按照计算机病毒的破坏情况分类；按照计算机病毒的寄生部位或传染对象分类等等。就目前来说，习惯按照病毒的寄生方式来分类。依此，计算机病毒基本上可分为四类：即引导型、文件型、混合型和宏病毒。

（1）引导型病毒

引导型病毒侵染磁盘上引导扇区（BOOT SECTOR）的内容，或感染硬盘上的分区表（FAT）。引导型病毒按其寄生对象的不同又可分为两类，主引导区（MBR）病毒、引导区（BR）病毒。一旦主引导区被病毒侵染，病毒就试图侵染每一个插入计算机从事访问的软盘引导区。

引导型病毒是利用操作系统的引导模块放在某个固定的位置，并且控制权的转交方式是以物理地址为依据，因而病毒占据该物理位置即可获得控制权，而将真正的引导区内容转移或替换。这样，病毒可以在系统文件装入存储器之前，先进入存储器，从而使它获得对操作系统扰乱的完全控制，这就使它得以传播和造成危害。

（2）文件型病毒

文件型病毒主要是感染文件。这类病毒通常感染带有COM、EXE、DRV、BIN、OVL等扩展名的可执行文件。当它们激活时，感染文件又把自身复制到其他可执行文件中，并能在存储器里保存很长时间，直到病毒又被激活。感染病毒的文件执行速度会减缓，甚至完全无法执行。

大多数的文件型病毒都会把自己的程序代码复制到其宿主文件的开头或结尾处，这会造成已感染病毒文件的长度变长，但用户很难发现其变化。也有部分病毒是直接改写受害文件的程序代码，因此感染病毒后文件的长度仍然维持不变。

（3）混合型病毒

顾名思义，混合型病毒综合引导型病毒和文件型病毒的特性，它比引导型病毒和文件型病毒更具有破坏性。此种病毒往往通过这两种方式来传染，更增加了病毒的传染性和存活率。因此，只要感染该类病毒，就会经开机或执行程序而感染其他的磁盘或文件，此类病毒也是最难消灭的。

（4）宏病毒

宏病毒不像以前的病毒，它是通过使用应用程序自己的宏程序语言来扰乱应用程序本

身。它并不是感染程序，而是感染文档文件；它不特别关联于操作系统，但能通过电子邮件、软盘、Web 下载、文件传输和应用很容易地得以蔓延。在各个文件应用操作上，如打开文件、存储文件、关闭文件或清除文件，它们都能侵染。

宏病毒大多是用 Visual Basic 写出的，比较容易制作，在计算机历史上它是发展最快的病毒。据统计，该病毒目前占全部病毒的 80%。

宏病毒主要是随着 Microsoft 的办公自动化软件 Office 的流行开始慢慢流行起来的。为了减少用户的重复劳动，比如要进行相似的操作，Office 提供了一种所谓“宏”的功能。利用这个功能用户可以把一系列操作全部记录下来，作成一个宏，之后只要运行这个宏，计算机就能自动重复执行那些定义在“宏”中的所有操作。这种“宏”机制一方面方便了普通的计算机用户，但这也给病毒制造者提供了可乘之机。

以 Word 为例，当打开一个文档时，Word 首先查找现有的 Auto Open 宏。如果有这么一个宏，Word 便会自动去执行它。同样地，当 Word 关闭文档时就去执行 Auto Close 宏。即完成不同的操作（如打开文档、保存文档、退出保存等），Word 首先查找执行相应自动宏的运行，而宏病毒往往就是通过这种机制加载进来的。当含有宏病毒的文档一旦被打开，其中的自动运行的宏病毒就抢先运行了，并驻留在 Normal 模板上。从此以后，所有自动保存的文档都会感染上这种宏病毒，而且如果其他用户打开了感染病毒的文档，宏病毒又会传染到他的计算机上。

1.4　计算机病毒的主要症状

计算机感染病毒后，往往会表现出一些异常现象。及时发现异常情况，使病毒危害尽可能降到最低，并对病毒发作的症状予以注意。此外，病毒的发作症状和所感染病毒的种类直接相关，由此可采取相应的处理措施消灭病毒。

从目前发现的病毒来看，使计算机出现的主要症状有：

（1）运行速度减慢。

（2）系统出现异常现象，如：突然死机或死机频繁。

（3）输入、输出设备有异常现象，如：显示器时常花屏等。

（4）文件、数据丢失。

（5）文件的大小、内容、属性、日期等无故改变。

（6）系统引导变慢。

（7）程序运行出现异常现象或不合理的结果。

（8）系统不认磁盘或硬盘，不能引导系统等。

（9）没做写保护时屏幕上出现软盘写保护的提示。

（10）异常要求用户输入口令。
（11）计算机系统的指示灯、蜂鸣器等出现异常现象。
（12）计算机存储系统的存储容量异常，时常显示内存不够等提示。
（13）文件夹里出现许多乱码。

1.5　计算机病毒的预防和数据安全

预防和阻止病毒的侵入比病毒侵入后再去发现和排除它重要得多。计算机病毒的预防是保证系统和数据安全的前提，因为病毒一旦侵入系统，就会影响系统和数据的安全运行。因此，每一位计算机用户应该时刻防范病毒的侵入，做到以下几点：

（1）谨慎使用公共和共享的软件。

由于这种软件使用的人多而杂，它们携带病毒的可能性较大。一个学校或公司的公共软件每天可能都有许多人在使用，如有一人不注意使一张软盘感染病毒，其结果可能会使整个单位的计算机系统或公共软件感染病毒。

（2）防范光盘上的病毒。

从光驱引导和安装软件，是方便了用户，但同时也带来了问题：光盘中可能隐藏着病毒，主要是因为盗版光盘的存在。盗版过程是导致这些盗版光盘染上病毒的主要途径，该过程可能有两种情况，一是制作光盘母盘时所使用的计算机系统有病毒活动，导致光盘中有病毒，由此制作出的所有光盘都会有病毒存在；二是制作光盘的软件本身有病毒，由于是盗版，来源不正规，导致来源中可能含有病毒。因此在光盘中，特别是盗版光盘中很可能含有病毒，故应少用盗版光盘。

（3）防范网络病毒。

随着计算机网络的广泛应用，网上病毒也就到处蔓延。因特网以其信息量大而著称，从中可以下载大量的应用程序和各种文档资料。如果下载的的应用程序染有病毒，那么当用户运行这些带毒程序就会使本地计算机染上病毒；如果下载的 Word 文档含有宏病毒，用户在阅读这些资料时很可能使自己的计算机染上该病毒。因此，对下载的程序和资料在使用前务必先用正版杀毒软件对它们进行检查和处理。

另外，收发电子邮件时，应慎重打开陌生人发来的邮件中所带有的附件。

（4）慎用不知来源的程序。
（5）限制网上可执行代码的交换。
（6）对不知来源的磁盘和机器在使用前用正版杀毒软件先清查。
（7）注意观察系统是否有异常情况并时常用杀毒软件检查。
（8）备份重要数据。

如果不能防止病毒侵入，至少应该尽早发现它的侵入；如果能在病毒产生危害前发现和排除它，则可以使系统免受危害；如果能在病毒广泛传播之前发现它，则可以使系统中修复的任务较轻和较容易；如果能时刻防范，不麻痹大意，做到经常把重要数据和资料备份，这样就会减少因病毒危害而产生的损失。

1.6　常用杀毒软件

病毒是防不胜防的，可以说哪里有计算机哪里就可能有病毒的侵入。为了对付计算机病毒，人们设计了许多杀毒软件。一般每一种病毒都会有所谓的特征码，当被它感染后，病毒就会把特征码标识上去，这样病毒在感染文件和系统时，先检查被感染者有无这个标识，如果有，说明已经被感染过了，就不会再感染了；如果没有标识则感染。一般的杀毒软件就是通过查找病毒的特征码和病毒的一些特殊性质来查毒杀毒的。下面介绍几种常用杀毒软件的使用和注意事项。

1.6.1　KV3000 杀毒软件

KV3000 软件是一种集防、查、杀、修、扩五位一体的功能强大的实时检测防火墙。防杀 DOS 病毒、Windows 病毒、宏病毒、网络蠕虫、黑客有害程序、网络炸弹、恶性 CIH 病毒等，能防杀国际上数万种病毒和国内数千种病毒。尤其是独树一帜的强大的硬盘救护工具箱和灾难修复功能是电脑用户的必备工具。最新的 KV3000 杀毒软件所包含的内容有 2 张软盘和一张光盘。2 张软盘中的 A 盘是 KV3000 的主文件、升级说明及查杀病毒列表等，B 盘是带光驱启动系统的软盘、KVW3000 和 KVD3000 升级的库文件 KV3000.LIB。而光盘上含有 KV3000 系列所必须的所有文件，其中包括制作解锁紧急启动盘、制作驱动光驱启动盘、恢复影像文件等工具，使用 KV3000 可使计算机用户免受病毒的侵害。

1. KV3000 主要功能

（1）KV3000 杀毒软件分为 DOS、Windows 9X/ ME/ 2000 以及 Windows NT 4.0 版。在不同的操作平台上能防能查能杀，同时它采用了独特的开放式系统，即用户自己不需编程序就可简单方便地不断增加该软件检测和清除计算机病毒的数量，克服了以往的查毒软件难以增加查解新病毒的能力而不断被淘汰。发现新病毒后，用户可立即自行抽取新病毒特征码扩充查毒或增加杀毒代码，也可随时在有关专业报刊上获取新病毒特征码和杀毒代码，不必为不能自形升级扩充查解新病毒而发愁。

（2）KVW3000（KV3000W）在线式“实时监测”病毒，即病毒防火墙，可时刻“实时监测”和查杀外来软盘、光盘和 Internet 网的病毒及其有关黑客程序。可时刻“实时监

测”最常见的十多种压缩病毒文件和识别多种可执行程序的压缩格式，让那些隐藏极深的病毒也不得不原形毕露。另外，它也可以“实时监测”或搜寻到电子信箱中夹带在 E-mail 中的病毒，可以支持 Foxmail、Outlook 等常见的 E-mail 软件生成的信箱格式，阻止网上病毒的进入。

（3）KV3000 是目前惟一具有扩展开放式和封闭式两项功能的杀毒软件。其一，采用了具有扩充功能的开放式外部病毒光谱特征库过滤法查病毒和接口编程加载法杀新病毒原理和方式。其二，采用了以往常规的封闭式内部定位法的查毒原理和方式，用户可任选其一或分别使用，查毒细致、准确广泛。

（4）在国际上首次设计有独特的病毒特征代码过滤器，很容易查出部分变种和变换自身代码的变形病毒。也很容易地查出 Word 宏病毒。特别是光谱代码过滤功能，能查出名为“G2、IVP、VCL 等多种病毒生产机”生产出的“各自血型”的千万种病毒。

（5）在对抗病毒时，具有“光谱特征代码过滤法”、“步步跟踪法”、“逻辑判断法”等多套不同的查毒方法，使病毒难以逃脱。

（6）能按用户意愿主动在软盘上保存硬盘正常的引导区信息，以防日后被病毒破坏后硬盘不能启动时，即可用该软盘再恢复。

（7）能直观地查看硬盘物理扇区主引导和 BOOT 引导信息是否正常。用户可一个不漏地查看出所有的主引导病毒。KV3000 可以尽收眼底，直观地看到它们的代码真面目。

（8）能安全杀除所有主引导区病毒。在杀主引导区新病毒前，会先备份原主引导信息到软盘，以防不测时可安全恢复原样。

（9）该软件最有特点的高效光谱智能检测系统、虚拟跟踪技术、神经网络敏感系统可查出大多数的未知名引导区和文件类病毒。

（10）KV3000.EXE 具有自我检查、自我修复、自我解除感染自身的病毒，即具有金蝉脱壳之功能，以保自身清洁和完整。

（11）测试、修复和重建硬盘分区表功能，使丢失了分区表的硬盘能在几秒钟内就可起死回生，使硬盘上被封闭的重要数据存取如意。这对存有大量信息的硬盘来说，尤为重要。

（12）增加硬盘救护箱工具、使得维护、备份、修复硬盘数据变得得心应手。

（13）简单的界面，适应各种显示器，兼容中西文。DOS、Windows 9X/ME、windows NT 4.0、Windows 2000、Novell 网络等。

（14）版本升级方便。为了紧跟追杀新病毒，适应不同层次用户的要求，KV3000 还将扩充查解新病毒的接口留给了用户或按照通告扩充查解新病毒的代码。

用该软件在对抗新的计算机病毒中，有了快速反应能力，可用来紧紧跟踪新病毒，把新病毒及早地消灭在初期状态。使用这一软件后，还会发现，世界上现有的上千种引导区病毒和以后不断出现的新引导区病毒，几乎没有能逃脱 KV3000 的查解。并且，许多文件型新病毒和几千种感染 Word 文档的宏病毒及新宏病毒，也难以逃脱 KV3000 高效查杀。

2. 查杀毒前注意事项

（1）不要使用未经授权许可的杀毒软件，更不要使用解密、盗版杀毒软件，否则会有很多不良结果。

（2）使用该软件查解病毒时，必须使用无病毒的系统软盘引导机器（冷启动），以确保内存无病毒。

（3）购买软件后，不应用复制密码的方式来备份 KV3000。

（4）使用该软件时，用户应自备一张无病毒的系统引导软盘，在要查毒的情况下，用自备盘来引导系统，这样，能更好地延长 KV3000 原盘的使用寿命，一般不要用 KV3000 原版引导系统，否则，会降低原盘的使用寿命。

（5）当电脑硬盘上装的是新版 Windows95(OSR2)或 Windows98/ WindowsNT4，即 32 位系统，这时，如果用 DOS 7.0 以下的系统软盘引导机器后，硬盘不会被确认。应制作一张 DOS 7.1（即 Windows 98 版）的系统引导盘。其方法如下：

将一张格式化的软盘，放入有上述操作系统并证明无病毒的机器中的软驱，在 C 盘提示符下键入 SYS　A：即可制作成一张引导盘。

（6）使用该软件查解病毒时，为了安全，应先使用本软件的扫描功能，如果查出有引导区病毒，那么，在使用本软件的杀毒功能前，应先使用本软件的备份功能，将硬盘主引导信息先备份到软盘中保存，然后再使用杀毒功能。如果查出文件中有病毒，也应做到先备份，后杀毒。

（7）光盘上的病毒不能查杀，只能将病毒文件拷贝下后，再查杀。

3. 直接使用 KV3000

直接用 KV3000 软件中的 A 盘启动机器，这是 KV3000 常用格式。在出现提示符后键入主程序名 KV3000 后，回车。即可看到如图 1.1 所示的界面。

图 1.1　KV3000 窗口界面

使用这种格式后，KV3000 自动将当前盘下的病毒特征库文件 VIRUS.DAT 读入内存，当使用 F1、F4 定义的功能时，就是用此特征库中的病毒代码来搜索病毒。

根据主画面的菜单，选择并按一下功能定义键（F1 至 F10），然后再连续选择 A、B、C...Z 盘对病毒进行行扫描或清杀，若要中途退出，只要按一下【Esc】键即可。

在 KV3000 界面中定义了很多功能键，用户可以根据不同的功能进行系统的相应操作，表 1.1 列出了这些功能键的详细功能。

表 1.1　功能键的作用

功 能 键	功　　能
F1	用 KV3000 的第一套查毒方式，即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，灵敏度和准确度极高，速度稍慢
F2	用 KV3000 的第二套查毒方式，即用程序内部封闭的另一套扫描方法，快速对引导区和所有文件的病毒进行扫描，速度较快
F3	快速清杀已经知名病毒
F4	用 KV3000 的第一套查毒方式，即用外部扩展的病毒特征库（VIRUS.DAT）和扫描过滤法对引导区和.COM、.EXE 文件进行全代码扫描搜索病毒，灵敏度和准确度极高，速度稍慢，适应搜索网络服务器
F5	对某一子目录内全部文件中的病毒进行扫描或清除。例如：C：\DOS 或输入 C：\UCDOS　回车
F6	硬盘急救工具箱。可查看、分析、修复硬盘所有扇区，有较强的数据修复功能，是了解和学习硬盘逻辑结构的有力帮手。可查看不归 DOS 管理的硬盘隐含扇区，查看硬盘 0 面 0 柱 1 扇区主引导记录及分区表，可在硬盘隐含扇区内查找被搬家的主引导记录及分区表，并可向 A 盘备份保存。备份后，可用 KV3000/HDPT.DAT 的格式再恢复到硬盘 0 面 0 柱 1 扇区主引导区中，但事先应先用 KV3000/B 的格式将当前 0 面 0 道 1 扇区主引导区备份到某一软盘上保存，以防不对时，再原样恢复回去
F7	可查看硬盘主引导区、BOOT 区、FAT1FAT2、ROOT 等扇区
F8	病毒演示，无任何负作用
F9	显示版本号和简易说明等，但事先应启动汉字
F10	自动测试和快速修复硬盘分区表等
Esc	任何状态中，按下此键可返回、终止、或退出

功能键定义说明：

（1）F1、F4 定义使用开放式的病毒特征库 VIRUS.DAT 文件中的病毒特征代码来扩展搜索病毒。

（2）F2 定义用常规的内部封闭式的查毒原理和方法，快速查找已知名的病毒。

（3）启动 KV3000 后的默认状态是 F3=KILL，快速清杀全盘引导区病毒和所有文件中的病毒。

（4）启动 KV3000 后的默认状态下再按 F5，可快速清杀某一子目录内全部文件中的病毒。其使用格式：C:\DOS 〈回车〉。