[美] Matt Pietrek 著
米东 王森 等译

美国IDG“奥秘”丛书

# Windows 95 系统编程 奥秘

## Windows 95 System Programming SECRETS

**了解内部：**
包括Windows 95系统和存储结构、进程、线程、Win16模式和任务等。

**掌握底层：**
如User和GDI子系统、KERNEL32、PE和COFF OBJ格式。

**达到新高度：**
通过研究Win32平台的内部行为和数据结构，可以使你在Windows开发方面达到一个新高度。

IDG BOOKS
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

美国 IDG“奥秘”丛书

# Windows 95 系统编程奥秘

[美]Matt Pietrek 著

米东 王森 等译

电子工业出版社

# 内 容 简 介

本书属于美国 IDG 环球出版公司的“奥秘”丛书之一。

本书详细揭示了 Windows 95 系统的核心技术，解剖了 Windows 95 的存储结构、进程、线程、模块、任务以及有关函数。

本书共有十章，第一章展望了 Windows 95 的未来，与 Windows NT 等工具软件进行了综合比较。第二章论述了 Windows 95 的新特点，与 Windows 3.1 进行了详细的比较。第三章详细论述了 Windows 95 中的模块、进程和线程。第四章和第五章分别揭示了 Windows 95 中 USER 和 GDI 两个子系统，以及 Windows 95 的内存管理。第六章详细分析了 Windows 95 的三个核心部件(VWIN32. VXD、KERNEL32. DLL 和 KRNL386. EXE)。第七章论述了 WIN16 模块和任务。第八章考察了 Windows 95 中可移植的执行模块和通用目标文件格式。第九章教读者自身去探索 Windows 95 奥秘的方法。第十章作者介绍了自己编写的一个 WIN32 API 侦探程序，读者可在此基础上进行扩展。

**Windows 95 System Programming SECRETS　　by Matt Pietrek**



美国 IDG “奥秘” 丛书

Windows 95系统编程奥秘

米东　王森　等译

责任编辑：郭庆睿

*

电子工业出版社出版（北京市万寿路）

电子工业出版社总发行　各地新华书店经售

北京市顺义县天竺颖华印刷厂印刷

*

开本：787 × 1092 毫米 1/16　印张：38.25　字数：976 千字

1996 年 8 月第一版　1996 年 8 月第一次印刷

印数：5000 册　　定价：85.00 元

ISBN 7-5053-3278-3/TP·1226

著作权合同登记号　图字：01-95-940 号

# IDG Books 奥秘系列丛书的优势

奥秘系列丛书的宗旨很简单：给专家作者设一个论坛，把他或她的经验传授给读者。奥秘系列丛书的作者(而不是出版公司)直接组织、精选和处理该课题的材料。作者们通过文章的反馈、培训班、e-mail 交换、参加用户组织及咨询工作与最终用户保持密切联系。由于作者们了解计算机日常使用的现状，我们的奥秘系列丛书具有一个战略优势：奥秘系列丛书的作者们与读者们是紧密结合的。

奥秘系列丛书的作者们具有以最有效的方式处理某一课题的经验，并且我们知道您——亲爱的读者，会从与作者一对一的关系中受益。我们的调查表明，读者们之所以要购买计算机书籍是想就某一产品听取专家们的意见，读者们想从作者的经验中受益，而奥秘系列丛中自始至终都有作者的声音。有些人将阅读该丛书比喻成在休息时间与作者聊天，并得到作者充分的关注。

此外，在奥秘系列丛书中，作者还免费提供或推荐一些有用的软件。随书所附的软件是经过精心挑选的，与书中的内容、主题或步骤有密切的关联。我们相信您会从所附的软件中获益匪浅。

无论您是从头到尾一段段地阅读，还是一次只读一个专题，您都会从本书中发现您所需要的内容。作为一位计算机用户，您应该获得全面解答的资源。IDG 书籍出版公司荣幸地以《Windows 95 系统编程奥秘》为您提供这一资源。

# 译 者 序

Windows 工具软件可以说是目前最优秀的软件之一，Windows 95 又是 Microsoft 公司最新推出的功能极丰富的产品，市场需求前景是非常可观的，在相当一段时间内必定是广大计算机软件工作者所青睐的产品，同行们若对 Windows 95 想有一个较深入地了解，请参阅本书。

要求本书的读者对 Windows 的使用比较熟悉，至少对 Windows 3.1 有比较强的编程能力，同时对 C 语言有一定的编程经验，那么你读起这本书来会更有情趣。

正如作者比喻的，Windows 95 是一个扑朔迷离的洞穴，则此书是为那些洞穴探索者所准备的。本书不是教你如何去编写 Windows 95 程序，而是带你走进其内部，详细考察 Windows 95 的本质，认清其本来面目，以便更好地使用 Windows 95 开展有关工作，但愿本书会给你带来较大帮助。

参加本书翻译的有：米东（第一章、第二章、第三章（前 11 节）），郝杰成（第四章），崔新军（前言及序部分，第三章（后 8 节）、第五章），朱金钧（第六章），齐剑峰（第七章），卢凌云（第八章、第九章），王森、董永乐（第十章、附录 A），米东、王森作了全书统校。

由于译者水平有限，错译之处在所难免，敬请读者指正。

1996 年 4 月 于石家庄

# 序

《Windows 95 系统编程奥秘》是 Matt Pietrek 有关如何真正了解 Microsoft Windows 的第三项主要工作。Matt 从事 Windows 方面的工作已有多年。1988 年从 Santa Cruz 大学毕业后，他就开始逐渐显露了他的这方面的技术才华，尽管当时他获得的是物理学学位而且只拿到了二门计算机学科方面的学分。在进入 Borland 的技术保障部之后，他很快获得了客户的高度评价。

之后，他在 Borland 的 R&D 室取得了更大的成绩。他编写了 TDUMP 和 WinSpector，甚至在 OS/2 Turbo Debugger 上也卓有成效。其后，由于 Borland 的多次裁员，他离开了 Borland 而最后来到了他自己的 Nu-Mega 公司。今天，他已经成为了 Bounds-Checker 系列产品的主要设计者。

我第一次与 Matt 相遇是在 1991 年春天召开的软件开发会议(Software Development conference)上，那时我们所倡导的 Windows 尚未引起关注。Charles Petzold 和我是 Windows 与 OS/2 辩论会的小组成员，当时我们已是四面楚歌，公众都已认定未来必是属于 PC OS 的了。

然而，事实却如 Matt、Charles 和我所预料的——今天，Windows 已经远远超出纯技术的王国而成为大众文化的一个部分。在 Windows 95 展示周里，其盛况超过了“侏罗纪公园”首映的场面。但事实上，在您为此欢欣鼓舞之际，尚有许多问题等待解决。完成最后一个从 Windows 3.x 向 Windows 95 的升级尚需多年的努力，只有到那时我们才算真正地进入了 32 位世界。

如果将 Windows 比做一个扑朔迷离的洞穴，那么这本书就是为那些洞穴探索者所准备的，而且要比 Win32 API 更合适。Matt 是进入 Windows 95 洞底的第一人。(事实上，按本书的工作性质讲，可称做“Windows 洞穴探险”。)许多其它“当今的”Windows 95 书籍曾承诺向您展示所有的黑盒子，但实际上一、二年前就已不再“黑”了。为了抢到先机，那些书本的作者往往会不合时宜地走在了前面，而对 Chicago 的探险也不会超过 1994 年 5 月份公诸于世的内容。甚至，有些工作还在被那些过时了的信息和错误的假设搞得头绪皆无。

与此相反，Matt 则深入洞察了 Chicago 的一切——包括 Windows 95 的零售版本——因而给您带来了真正时新的信息。还在等什么？亲爱的读者！还不戴上您的安全盔，点起手中的火把，开始您的洞穴探险！

Eric J. Maffei
Microsoft 系统杂志主编
1995 年 9 月于纽约

# 引　言

近来，Microsoft 一直在问，“今天你又想到哪儿去？”现在，公司已不再介意推出 Windows 95 是我们达到目的的一种手段的观念了。我们作为编程者需要知道的是，Windows 95 是不是真正地如我们所预期的那样有效。几乎所有的人都会同意，Windows NT 如凯迪拉克一样漂亮（如果你更愿意的话，你也可以称它是奔驰），因为它有着近乎完美的设计和安装。但问题是，Windows 95 会不会成为雪弗莱或其它跑车呢？唯一的验证办法是打开车盖自己去看个究竟。这也正是我写此书的目的。只有在考察了像 Windows 95 之类的操作系统的本质之后，我们才有可能自己认清它是否有排气管和火花塞，以及它的安全性，舒适性如何。

你可能不理解，像我这样的编程人员，为什么一直会对 Windows 95 之类的操作系统的根本细节情有独钟。如果把更多的精力投入像 OLE、MFC、或最新的图象或是多媒体 API 之类的新科技上去，不会更好吗？当然，对一些编程者来讲，只要了解得够用就行了，但也有一些编程者则更喜欢刨根问底，把代码层搞得透透彻彻，也或许我们并不想把自己的代码运行于不大了解的其它代码之上。无论什么原因，《Windows 95 系统编程奥秘》一书是为这些人所准备的。知识就是力量，你对 Windows 95 这样的系统掌握得越多，你对它的控制就会越强。

《Windows 95 系统编程奥秘》并不想透视 Windows 95 设计与执行的各个方面，我选择了自己深感兴趣的内容。希望本书能为您自己的 Windows 95 编程工作中提供一些有益的参考。

## 关于您和读者的假定

从全书的背景考虑，这里对读者作一定的知识假定。当然，确切地讲，本书的读者应当具有较强的 Windows 编程能力，至少为 Windows 3.x 编过程。本书并不是一本有关“如何为 Windows 95 编写程序”之类的书籍，我想这方面的书已彼彼皆是了。

因此，《Windows 95 系统编程奥秘》一书的出发点是认定您已知道了在 Windows 3.1 和 Windows 95 中的编程方法，而且您现在正想继续走下一步：想了解为什么 Windows 95 会如其所设计的那样工作。

通过了解 Windows 95 内部的理论黑盒子的工作方式，您就可以按照 Windows 95 的工作方式来达到自己的目的而不会陷于盲目。这样，您的程序当中出现了故障时（这当然是我们应尽力避免的），如果您已经了解了 Windows 95 的工作原理，那么调试过程就会非常迅速。为什么会这样？因为如果您掌握着 Windows 95 的一举一动，您通常可以在调试过程中尽早地明确程序是在何处中断的。

本书的示例是以 C 语言的形式写出的，并混入了一些汇编语言。我所提供的各种 Windows 95 伪码也是以 C 语言为基础的。因此，为了有效地掌握本书内容，您应当了解有关 C/C++ 的知识。如果您在其它编译语言，如 Borland Pascal/Delphi 上有一定的编程经验，则也可以。

## 伪码

由于本书的目的是首先要展示 Windows 95 的工作机理，我需为 DLL 系统中的各种函数提供伪码，这类伪码通常与可编译的 C 代码相似。但为了不破坏 C 语言的语法规则，我单独给出了伪码。这里的伪码是以 Windows 95 的调试版本为基础的，它提供了许多有用的诊断字符和其它信息，可以使我们更容易精确察看到 Windows 所作的一切。如果您运行的不是 Windows 95 的调试版本，应当改变过来。在有错误出现时，Windows 95 的调试 DLL 会给出非常有用的信息。如果您不用调试版本，而想用零售版本，那么您的调试程序的内容与本书的伪码会有一定的区别。

## 样本程序

《Windows 95 系统编程奥秘》有几个程序可供您考察 Windows 95，它们均附于本书的磁盘上（包括 .EXE 程序和源程序）。由于这些源代码要一次占去 30 多页，除了第十章的 APISPY32 程序外，在书中正文基本没给出。第十章的重点是建立一个 Win32 API 的侦探程序，因而在论述有关概念时需对源代码进行深入的考察。

如果您读过《Microsoft 系统杂志》或《PC 杂志》，您在这些杂志上会发现与本书相类似的某些程序。事实上，书中的一些章节在上述杂志上已经讨论过。但是，如果您已经读过这些杂志，在看本书时也不要跳过相应的章节，因为书中的程序已较以前大有改进。而且，由于当时篇幅所限，有些内容并未涉及。

例如，第八章的 PEDUMP 程序在功能方面已比当时发表于《Microsoft 系统杂志》上的程序大了一倍。与此类似，在《Microsoft 系统杂志》上出现过的 APISPY32 程序也比 Windows 95 中的情况差得远。本书的 APISPY32 程序是以船载 Windows 95 形式工作的，NT 3.51 中的 .EXE 程序也有类似的情况。

# 目　录