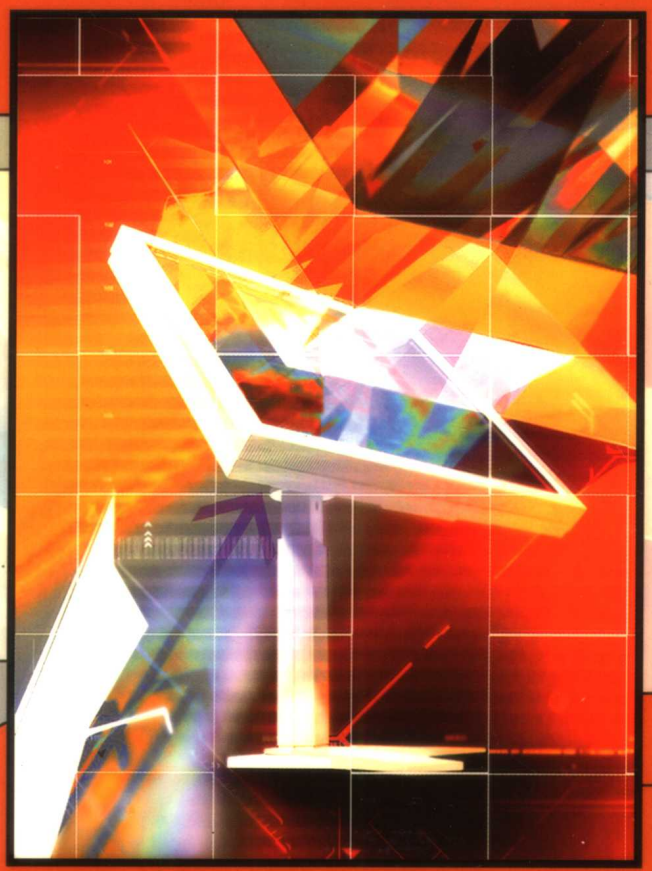
Borland In-Depth Series \ Borland 大系

Broadview
WWW.BROADVIEW.COM.CN

Delphi 源代码分析



周爱民 著

CD-ROM Included

電子工業出版社
PUBLISHING HOUSE OF ELECTRONIC INDUSTRY
http://www.phei.com.cn

Delphi

数据分析

Borland In-Depth Series\Borland 大系

Delphi 源代码分析

周爱民 著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书通过对 Delphi 内核(RTL)源代码进行分析，深入阐述了 Delphi 内核(RTL)的原理及其实现。全书从 Nico Bendlin 编写的著名最小化内核示例程序 MiniDExe 讲起，基于 MiniDExe 分析 Delphi 在编译器一级的技术内幕，带领读者一窥 Delphi 的核心。随后作者基于这个内核逐层地包装代码，将 Delphi 的各种功能的具体实现一一展现，通过列出关键性代码并进行系统性分析的方式，全面分析对象结构、VCL 和 COM 等在源代码中的实现。全书内容详实，阐述精辟、深入，主要议题包括：Delphi 的编译器在 Windows、Delphi RTL 和用户代码之间的交互；Delphi RTL 内核代码的完整实现；与 Delphi 内核相关的操作系统机制；初始(入口)代码、模块、内存、线程、资源、异常处理机制等。

本书是一本不可多得的高端技术图书，适合中、高级 Delphi 开发人员研读。

图书在版编目(CIP)数据

Delphi 源代码分析 / 周爱民著. —北京：电子工业出版社，2004.9
（Borland In-Depth Series\Borland 大系）

ISBN 7-121-00303-1
Ⅰ.D... Ⅱ.周... Ⅲ.软件工具—程序设计—代码—程序分析 Ⅳ.TP311.56
中国版本图书馆 CIP 数据核字（2004）第 088925 号

责任编辑：周 筠 张兴田
责任校对：陈元玉
印 刷：北京智力达印刷公司印刷
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
经 销：各地新华书店
开 本：787×980 1/16 印张：23.5 字数：550 千字
印 次：2004 年 9 月第 1 次印刷
印 数：5 000 册 定价：40.00 元（含光盘 1 张）

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

序

第一次和 Aimingoo 见面是 2003 年底 Borland Conference 2003 在北京举行之际，Aimingoo 宏亮的声音、诚恳的态度立刻引发了我的好感。在 BorCon 排练时 Aimingoo 努力不懈，一直坚持到最后，我当时心中就想，这位年轻人真是不错。到了 BorCon 结束之后，我和 Aimingoo 有更多机会可以聊天，让我了解了 Aimingoo 的专长领域，也很佩服 Aimingoo 这么年轻就拥有这么多的开发经验。

在知道 Aimingoo 要写有关 Delphi Run Time Library 的书时，心中又惊又喜。惊的是这可是一个浩大的工程，喜的则是 Aimingoo 愿意花时间写这方面的书籍，造福想要一窥究竟的 Delphi 使用者。当 Aimingoo 把他的书籍目录和初稿给我过目时，我又不禁羡慕他的成果以及 Aimingoo 的书籍和拙作《Inside VCL》是如此地相辅相成，Aimingoo 的书籍叙述了驱动 Delphi 应用程序的引擎动力，《Inside VCL》则说明了 Delphi 应用程序使用的系统框架。

Aimingoo 请我为他的新书写序实在是我的荣幸，除了他丰富的知识和精湛的技术之外，Aimingoo 做事的态度更令人敬佩。结合技术和努力的结晶，Aimingoo 为广大的 Delphi 使用者写出了另一本 Delphi 领域的著作，对于想要深入了解 Delphi 执行时期运作细节的 Delphi 使用者而言，这是值得阅读和珍藏的一本好书。

最后我个人也要谢谢 Aimingoo 又为**李维工作室**产生了一本高质量的技术书籍，让**李维工作室**系列书籍更为丰富和充实。希望 Aimingoo 能够继续写出好书，不断帮助我们这群 Delphi 使用者更上一层楼。

李维 2004/3

前　言

关于本书

在用 Delphi1.0 时，我便开始阅读 Delphi 的源代码了。大约是在五年前，我曾试图做一个名为“Delphi 源代码深入分析”的网站，后来终于放弃了这个计划。而自此，写现在这样一本书的想法便积蓄至今。

真正激发我做这样一件事的，是 Nico Bendlin 写的 MiniDExe。这是我所见过的用 Delphi 写的最小版本的可执行程序，它使我得以一窥 Delphi 的核心。于是，我开始基于 MiniDExe 分析 Delphi 在编译器一级上的真相。随后，我分析了对象结构、VCL 和 COM 等在源代码中的实现。至此，本书的基本知识框架组织完成。

本书的知识结构

本书以内核的原理及其实现为主，主要讲述：

- Delphi 的编译器在 Windows、Delphi RTL 和用户代码之间的交互；
- Delphi RTL 内核代码的完整实现；
- 与 Delphi 内核相关的操作系统机制；
- 初始(入口)代码、模块、内存、线程、资源、异常处理机制等。

所有在本书中使用到的术语、参考资料等将以附录的形式列出。

本书基于 Delphi 7.0 所提供的源程序分析。

什么是“内核”

通常意义上的开发工具“内核”，指的是 RTL(RunTime Library)。在 Delphi 中，RTL 是指源码的*$(Source)\RTL* 目录中的全部代码。但以纯粹的 RTL 的概念来理解的话，事实上它应当是指 *System.pas* 和 *SysInit.pas* 中的全部代码(包括 *GetMem.inc*)——这甚至不包括 *SysUtils.pas* 这个单元。

在本书中所讨论的内核，基本上是指*$(Source)\RTL\Sys* 目录中的代码。此外，还包括：

- *$(Source)\RTL\Win*：*Windows.pas* 的部分代码。
- *$(Source)\RTL\Common*：*Classes.pas* 和 *SyncObjs.pas* 中的部分代码。

如何阅读这本书

写这本书的过程中，我几乎无时不在问自己“Delphi 如何实现这个”或者“Delphi 如何实现那个”。所以这本书在很大程度上都是在描述“Delphi 如何做到”，而不是“用 Delphi 如何做”。因此，我建议你以技术探索的角度来读这本书。你不要指望在本书中发现太多能直接在工程中使用的技术与技巧。

本书虽然是立足于 Delphi 源代码分析，但书中并不会大段地给出 Delphi 产品中的源码。因为 Borland 并没有这样的授权。通常情况下，我会列出关键性的代码，并进行系统的分析。因此，如果需要，读者可能必须自行对照源码中的*.pas* 文件来阅读一些章节。

本书不包含内核源码的哪些内容

本书立足于对 Delphi 内核(RTL)源代码的深入分析，但为了叙述的必要，仍剔除了部分内容。这些内容主要是指：

一、 BCB 兼容代码

我不是太了解 BCB。因此除非必要，我不会在本书的章节中讨论与 BCB 相关的内容。基于同样的原因，在 Delphi 内核源码中与 BCB 相关的(绝大多数)代码也被我忽略了。

二、 调试代码

除了在讲述异常机制时，其它绝大多数情况下我都不会讨论在 Delphi 内核源码中与调试相关的代码。那的确是相当复杂的一套代码。不过在读完本书之后，我相信读者已经有能力自行开始分析这些代码了。

三、 面向 Linux 的移植：CLX

要讨论 CLX，则必须进一步深入了解 Kylix 和 Linux 操作系统。如果在本书中以大量篇幅出现这些内容，将会降低本书在主流的桌面开发平台(当然，你知道我指的是什么)上的实用性，同时，也将使关于 RTL 的分析显得混乱。

本书的示例源码

我绝不想用大量源码来充斥书页。因此，本书中大多数地方的源码引用只是点到即止。很多时候，你会看类似于“...”的省略。或许有部分读者会认为在光盘中(而不是书中)阅读源码是件痛苦的事，但是我相信，如果与使用数页甚至十数页的源码来充填内容、增加厚度相比，将这些东西放在光盘中还是更对得起读者的钱包的☺

两本书

这里提到两本书。提及这两本书，是因为在底层以及原理的分析方面，这两本书当属扛鼎之作。因此本书会在内容上尽量避免与它们重复。

其一是 Ray Liscbner 著、中国电力出版社出版的《Delphi 技术手册》。这本书基于 Delphi 5，用 130 页的内容概述了 Delphi 的基本语言特征，其后的 500 页则是一个完整的语言参考。基本语言特征部分言简意赅但直指核心，句句发人深省；语言参考部分十分详尽，且附有精彩的示例。

其二是李维先生著、电子工业出版社出的《Inside VCL》。

鉴于《Inside VCL》一书卷帙浩繁，解析深湛，因此本书剔除了与 VCL 部分有关的内容(原定计划中是有的)，至于 OOP 在 Delphi 中的实现以及可能的一些 VCL 和 COM 方面的补遗，我会放在其它书中单独去讲。而《Delphi 技术手册》一书中对 RTL 的过程、函数描述详尽，因此本文在这些例程的功能方面，也不多费笔墨。

.NET 相关问题

本书不讲.NET Framework。在绝大多数读者看来，.NET 的出现，意味着 Delphi 的终结，很多朋友甚至对写这样一本 Delphi 内核分析的书的必要性提出质疑。然而在我看来，即便是.NET，在内核结构上仍与 Win32 内核存在千丝万缕的联系，更何况.NET 中的非托管代码，还需要用 Win32 原生应用开发工具来实现。所以 Delphi 7.x 与 Delphi .NET 是两条不同的产品线，也有着不同的发展方向。

即使是在.NET 大行其道的时候，Win32 开发以及 Win32 应用的维护仍然要持续很长一段时间，正如至今还有人在用汇编写驱动程序一样。

免责声明

本书中许多内容都是未见于 Delphi 的标准文档的。这意味着某些结论是非官方的，在更新(或者更旧)的版本中，不会得到认可和支持。我只是从源代码中得到了这些结论，并通过实例来证实了它们。如果你需要在其他版本的 Delphi 中实现相应的功能，你应当重新编译并运行测试程序。

如非必须，你不应当在商业软件中使用某些技巧。这不是授权问题，而是安全性的问题。通常，如果你发现“必须使用技巧来解决问题”，那么你应当考虑“是否方案设计错误”。我建议你在商业化软件中应用这技巧时，应当做出详尽的源码注释，并在项目中添加一个专用的测试程序。

我保证在本书中的所有结论和技巧都经过验证和测试。但如果读者未经过进一步的测试而使用它们，所导致的问题，是我所不负责任的。

随书光盘

本书附随书光盘一张，包含了书中所有示例程序源代码以及相关工具。光盘基本目录结构如下：

- *\Book* ：本书各章节中所使用的示例程序的完整源代码。
- *\third* ：本书在正文中介绍过的第三方代码/开发项目。
- *\tool* ：本书编写过程中使用过的一些分析工具。

在绝大多数目录下都将包含一个文件“说明.txt”，该文件描述了该目录中的代码或工具的

相关资料。如果本目录下未包含该文件，则相关的说明应当在上一级目录的“说明.txt”文件中。

在本书正文中，如果必须指明光盘中的文件位置，通常以如下格式给出(其中$(CD)表示光盘所在驱动器)：

```
$(CD)\third\chapter 1\MiniDExe.zip
```

本书所附的光盘中不带有任何 Delphi 产品光盘中的源代码。但是，部分程序会用到这些源代码，这需要读者自行提供——它们应在你的 Delphi 安装目录中。[①]

排版格式与惯例

通常情况下，我不会在书的正文部分包含注释，而会写成脚注。仅在不影响阅读的情况下，我会在正文中加入由“()”包含的可省略语言，通常它们是用于强调、限定或者极少量的注释。

在书中包含的源代码中存在大量的“// ...”，这些被省略掉的部分可能存在于 Delphi 自己的源代码或者随书光盘中。这取决于你正在阅读的是哪一部分代码。但在极少数的情况下，它们表明是在前文中出现过的代码，这时我通常会补充一行注释，表明你可以在什么位置看到这些代码。例如：

```
// ...
// (参见上例)
```

在源代码的第一行可能出现一个单行的注释。这个注释表明其后的代码引用自哪个单元，以及该单元中的哪个例程(如果随后的源码中没有给出例程名字)。但是，如果源代码出自 *System.pas* 单元，这一行注释将不会存在。此外，这个单行注释还有一种特殊的情况：如果随后的代码是改写自 Delphi 源代码而非直接复制，那么注释将以“code referenced by”开始，而不是通常的“code form”。例如：

```
// code referenced by System.pas, _InitResStrings()

TResStringInitItem = record
  variableAddress: String;
  resStringAddress: PResStringRec;
end;
```

① 请注意这些源程序只包含在某些版本中，如果你的 Delphi 中不包含它们，请安装更高级别的商业版本。

一些代码并不是*.pas*中的源代码，而是从 Delphi IDE 的 CPU 窗口中复制出来的汇编代码[①]。通常这些代码会包括源代码行、运行期地址、二进制码和反汇编代码行。这些代码以类似如下的形式提供：

```
Project1.dpr.5: ShowMessage('Test');
00451F6C B8841F4500      mov eax,$00451f84
00451F71 E8D2FBFFFF      call ShowMessage
```

很多时候，我习惯于使用 DOS 命令行来做一些事情(事实上，本书中的绝大多数代码都是我用 *Notepad.exe* 书写并用 DCC32.EXE 编译的)，因此本书中会有一些 DOS 命令行。为了区分它们，我使用了加粗的文字，而且它们通常将以类似于“*C:\>*”这样的形式开始。而紧接其后的内容，则是执行该命令行后的屏幕显示(可能是部分的显示结果)。例如：

```
C:\>tdump E:\Delphi7\Bin\tregsvr.exe
#   Name      VirtSize   RVA      PhysSize  Phys off  Flags
--  --------  --------  --------  --------  --------  --------
08  .rsrc     00001800  0001B000  00001800  00015A00  50000040 [IRS]
09  .debug    000E1AAC  0001D000  000E1AAC  00017200  50000040 [IRS]
```

另外，对于本书中出现的英文，采用了不同的字体表达不同的概念，概列如下：

- ✧ 正文中一般的英文采用 Times New Roman
- ✧ 行文中的代码采用 Lucida Sans Typewriter
- ✧ 大段代码采用 Courier New 字体
- ✧ 代码中的注释采用楷体_GB2312 字体
- ✧ 具有特定含义的概念或人名采用 Arial 字体
- ✧ 超级链接采用 Arial Narrow
- ✧ 正文中文件名/磁盘路径采用 *Arial* 斜体

致　谢

我当然得感谢 Nico Bendlin(nicode@gmx.net)，尽管我从未见过、也没有联系过他，但是如果没有他的 MiniDExe，我可能永远也不能开始写这本书。

① 在随书光盘中提供了一个笔者编写的 IDE 专家工具 CpuWHelper，可以方便地从 CPU 窗口中复制汇编代码。

我得感谢那个著名的 Delphi 大富翁论坛(http://www.delphibbs.com/)。感谢 yysun 创建了这个论坛，感谢 Soul 近三年来不辞辛劳地无偿维护着这个论坛，并以本书的出版纪念五年前离开论坛的 dwwang。在此也感谢活跃其中的诸多朋友，我的工作离不开大家的支持和帮助。谢谢。

我得感谢 CSDN 与电子工业出版社的朋友，这包括蒋涛、周筠、韩磊、方舟、张兴田，以及所有关注本书的编写、出版、发行的朋友。感谢我的老朋友王寒松先生向蒋涛推荐了本书，尽管那时这本书还没有写到 100 页。

感谢李维先生在百忙之中为本书作序。他对我的赞誉之词既令我深感荣幸亦令我不胜惶恐，以致于作每段文字时都倍加小心，生怕出现任何疏漏差错，而有负于李维先生对我的信任和对本书的推介。

我还得感谢我身边的她(Joy Xie)。尽管经过长达数年之久的斗争，她仍然未能迫使我改掉昼伏夜出的作息习惯。但是我得承认，如果没有她，我无法写完这本书(中途死于饥饿或本书终结于我觅食的过程中)。此外，在写这本书的过程中，我们结婚了☺

感谢给予我支持和帮助的所有朋友！

目 录