

<<格蠹汇编>>

图书基本信息

书名：<<格蠹汇编>>

13位ISBN编号：9787121196072

10位ISBN编号：7121196077

出版时间：2013-3

出版时间：电子工业出版社

作者：张银奎

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<格蠹汇编>>

### 内容概要

《格蠹汇编:软件调试案例集锦》以案例形式讨论了使用调试技术解决复杂软件问题的工具和方法。全书共36章，分为四篇。

前两篇每章讲述一个有代表性的真实案例。

第三篇讨论了调试工具和调试系统的设计方法。

第四篇收录了使用调试器探索计算机世界的若干学习笔记，包括在调试器中细品CPU，通过调试器观察和解码堆块结构，透视Windows8的新类型应用以及使用调试器监视启动、睡眠和唤醒三大基本过程等。

## 书籍目录

笃行第一 第1章 从堆里抢救丢失的博客 第2章 修复因误杀而瘫痪的系统 第3章 徒手战木马 第4章 调试笔记之侦查广告插件 第5章 拯救“发疯”的Windows 第6章 再解电源服务溢出崩溃 第7章 三解电源服务溢出崩溃 第8章 拯救挂死的PowerPoint 第9章 经典阅读器的经典死锁 明辨第二 第10章 转储分析之双误谜团 第11章 混乱数据何处来——标准文件流有关的陷阱 第12章 解救即将被断网的系统——调试补丁安装失败 第13章 SDK安装程序卡壳之谜——兼谈函数的异常出口 第14章 是谁动了我的句柄 第15章 转储分析之系统挂在DPC 第16章 转储分析之探寻唤醒失败原因 第17章 解救陷入死循环的MSN 第18章 寻找系统中的“耗电大王”器用第三 第19章 Windows 8的内核调试增强 第20章 漫谈Android系统的调试模型 第21章 趣谈托管程序的辅助调试线程 第22章 漫谈SOS扩展 第23章 趣谈CLR4的调试模型重构 第24章 如何跟踪ACPI代码 第25章 如何调试窗口大总管 第26章 嵌入式系统调试浅谈 第27章 海森伯效应一例 致知第四 第28章 使用调试器来认识计算机世界 第29章 在调试器中细品CPU 第30章 系统启动系列 第31章 在调试器中观察计算机的睡眠过程 第32章 在调试器中观察计算机的唤醒过程 第33章 使用调试器探索托管程序的执行起点 第34章 解读编码后的HEAP\_ENTRY结构 第35章 在调试器中看Win7打电话回家 第36章 使用调试器透视Windows 8的METRO应用 附录A 准备试验环境 附录B 设置内核调试环境 附录C 面向问题的索引 附录D 英文术语索引 附录E WinDbg命令索引 附录F 常用的汇编指令 (x86)

## 章节摘录

版权页：插图：是谁杀了关键服务 简单的方法没能奏效后，我开始思考如何对付这个问题。

系统重启的直接原因是关键的系统服务意外终止了（serviceterminated unexpectedly）。

因为有些系统服务（service）承担着重要的职责，它们的“健康”关系到整个系统是否能正常运行，所以系统会监视这些服务，如果发现它们意外退出（终止）了，那么便像有国家政要被谋杀了一样，进入紧急状态，强制“戒严”——关闭登录会话，退出窗口系统，强制重启系统……因为有很多个重要服务，比如日志服务、PnP服务、电源服务、DCOM等，都居住（host）在SvcHost进程中，在那里办公，所以一旦这个进程意外终止，那么很多个关键服务都会受影响。

从上面描述的现象来看，很可能是SvcHost进程意外终止了，导致运行在这个进程中的系统服务全完了，可谓“城门失火，殃及池鱼”。

那么是谁杀了这个重要的服务进程呢？

选择方法 接下来应该选用什么方法来调试呢？

我开始评估各种方法。

1.很多进程意外终止是因为未处理异常导致进程被强行终止，即通常说的应用程序崩溃（Application Crash）。

对付应用程序崩溃的常用方法是JIT调试，也就是当程序在被终止前，自动启动JIT调试器（参见第4章以及《软件调试》12.5节）。

但对于本例，出问题的进程运行在不可见的Session 0中，因此，当JIT调试器被启动后，默认是不可见的。

我们必须想办法让JIT调试器可见或者想办法与它通信。

2.第二种方法是使用双机内核调试，也就是通过串口、1394或者USB 2.0电缆来调试出问题的系统。尽管本例中问题发生在用户态，但是仍可以通过内核方式设置断点，或者等待发生未处理异常时中断到内核调试器，然后进行调试。

3.第三种方法是使用转储文件（dump file），也就是在SvcHost进程崩溃时产生转储文件，然后分析这个转储文件。

通常系统的WER机制（参见《软件调试》第14章）会自动产生转储文件，因此只需要找到并复制出来。

比较以上三种方法，第三种相对来说简单一些，但是只能看到崩溃时的“瞬间快照”，前两种方法都需要两台机器，相对来说比较麻烦，但是可以进行交互式调试。

不妨先尝试第三种方法，不行再用其他两种方法（见补记部分）。

于是面临的问题便是如何找到转储文件并复制出来。

眼下系统反复重启，每次只能使用几秒钟，要在那几秒钟时间内找到转储文件，然后复制出来难度太大了。

怎么办呢？

Win7的一个新功能刚好可以完美地解决这个问题。

WinRE派用场 很多普通用户可能根本不注意，一个典型的Win7系统中，其实有两个Windows，一个是用户通常使用的，另一个是正常系统出故障时用来紧急恢复用的，后者通常被称为WinRE（Windows Recovery Environment）。

简单来说，WinRE是个简化了的Windows，它很小，占用大约200MB的磁盘空间。

如何进入WinRE呢？

与进入安全模式的方法是类似的，也就是在高级启动菜单中选择Repair Your Computer。

进入WinRE后，启动一个命令行窗口，然后切换到Win7的系统盘。

值得注意的是，WinRE映射的盘符与正常系统中看到的盘符很可能是不一样的，C盘一般是所谓的系统保留分区，D盘一般是Win7的系统盘，可以通过文件来确定。

在本例中，D盘是Win7的系统盘，于是切换到D盘后，执行dir\*.mdmp / s以下命令来寻找WER机制产生的转储文件。



## <<格蠹汇编>>

### 编辑推荐

《格蠹汇编:软件调试案例集锦》是《软件调试》一书的姊妹篇，延续了《软件调试》的深入严谨风格。但与《软件调试》重在系统介绍调试原理不同，《格蠹汇编:软件调试案例集锦》重在实践，通过一个个有代表性的真实问题“现身说法”，在软件大背景下介绍调试，通过调试技术解剖软件。《格蠹汇编:软件调试案例集锦》适合广大程序员、软件测试工程师、软件架构师以及相关专业的高年级学生阅读，也可供信息安全领域的工程师或者研究者参考。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>