Memory Dump Analysis Anthology

Volume 2

Dmitry Vostokov
Software Diagnostics Institute

OpenTask

Published by OpenTask, Republic of Ireland

Copyright © 2008 by Dmitry Vostokov

Copyright © 2015 by Software Diagnostics Institute

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, without the prior written permission of the publisher.

You must not circulate this book in any other binding or cover, and you must impose the same condition on any acquirer.

OpenTask books are available through booksellers and distributors worldwide. For further information or comments send requests to press@opentask.com.

Product and company names mentioned in this book may be trademarks of their owners.

A CIP catalog record for this book is available from the British Library.

ISBN-13: 978-0-9558328-7-1 (Paperback)

ISBN-13: 978-1-906717-22-3 (Hardback)

First printing, 2008

Revision 3 (April, 2015)

Exception “is what we see at a glance”.

Blaise Pascal

Crash dump analysis “does not consist merely in” **peeking** “the memory and enlightening the understanding. Its main business should be to direct the” **Customer**.

Joseph Joubert

[This page is intentionally left blank]

Summary of Contents

Preface 15

Acknowledgements 17

PART 1: Crash Dumps for Beginners 19

PART 2: Professional Crash Dump Analysis 29

PART 3: Crash Dump Analysis Patterns 147

PART 4: Crash Dump Analysis AntiPatterns 343

PART 5: A Bit of Science 347

PART 6: Fun with Crash Dumps 351

PART 7: Data Recovery 375

PART 8: Software Troubleshooting 377

PART 9: Security 397

PART 10: The Origin of Crash Dumps 401

PART 11: Miscellaneous 425

Appendix A 443

Appendix B 445

Appendix C 447

Appendix D 451

Appendix E 455

Index 459

Notes 465

About the Author 469

Cover Images 470

[This page is intentionally left blank]

Contents

Preface 15

Acknowledgements 17

PART 1: Crash Dumps for Beginners 19

The Time of the Crash 19

Stack Trace 20

EasyDbg 22

Citrix Symbol Server 27

PART 2: Professional Crash Dump Analysis 29

WinDbg Scripts 29

Introduction for C/C++ Users 29

Generating File Name for .dump Command 37

All at Once: Postmortem Logs and Dump Files 38

Common Mistakes 39

Not Looking at Full Stack Traces 39

Not Seeing Semantic and Pragmatic Inconsistencies 41

Pattern Interaction 43

Heuristic Stack Trace 43

Multiple Patterns 50

Exception and Deadlock 55

Heap and Spike 59

Hooksware 63

Heap and Early Crash Dump 65

WinDbg Shortcuts 67

WinDbg as a Binary Editor 67

Command Autocompletion 70

!envvar 71

.quit_lock 72

.dumpcab 73

.f+, .f- 74

.exptr 75

WinDbg as a Simple PE Viewer 76

.sound_notify 79

Signaled Objects 80

Memory Search Revisited 87

WDF and PNP BSOD: Case Study 95

Exploring NDIS Extension 105

The Hunt for the Debugger 109

Complete Dump: User Space Critical Sections 115

Microsoft DLL Help Database 116

What Does This Function Do? 118

What Was This Process Doing? 119

STL and WinDbg 122

WinDbg Cheat Sheet 125

How Old Is Your Application or System? 126

Demystifying First-chance Exceptions 129

.NET Managed Code Analysis in Complete Memory Dumps 131

Who Opened That File? 134

In Search of Lost CID 136

Large Heap Allocations 137

First-order and Second-order Memory Leaks 140

Hooked Modules 145

PART 3: Crash Dump Analysis Patterns 147

Wait Chain (Executive Resources) 147

Corrupt Dump 151

Dispatch Level Spin 154

No Process Dumps 157

No System Dumps 158

Insufficient Memory (PTE) 159

Suspended Thread 161

Special Process 164

Frame Pointer Omission 169

False Function Parameters 173

Message Box 177

Self-Dump 181

Blocked Thread 184

Zombie Processes 196

Wild Pointer 202

Dynamic Memory Corruption (Kernel Pool) 204

Insufficient Virtual Memory 210

Wild Code 219

Hardware Error 221

Handle Limit (GDI) 226

Missing Component 233

NULL Pointer (Code) 237

Execution Residue 239

Optimized VM Layout 267

Invalid Handle 269

Overaged System 273

Thread Starvation 274

Stack Overflow (User Mode) 279

Missing Component (Static Linkage) 283

Duplicated Module 294

Not My Version 299

Data Contents Locality 300

Nested Exceptions (Unmanaged Code) 305

Nested Exceptions (Managed Code) 310

Affine Thread 314

Self-Diagnosis 318

Waiting Thread Time (User Dumps) 319

Inline Function Optimization 322

Critical Section Corruption 324

Lost Opportunity 332

Young System 335

Last Error Collection 337

Hidden Module 339

High Contention (Critical Sections) 341

PART 4: Crash Dump Analysis AntiPatterns 343

Debugging Architects 343

Symbolless Analysis 344

Myopic Troubleshooting and Debugging 345

PART 5: A Bit of Science 347

Memoretics 347

Memory Analysis 348

Memoidealism 349

Memiotics 350

PART 6: Fun with Crash Dumps 351

Music for Debugging 351

The Glory of Debugging 351

Memory Analysis Album 352

Biography of a Bug 354

Visual Computer Memories 355

The First Defect 356

The Songs for Remote Debugging 357

Thinking Out of the Box 358
Crash Dumps and Science Fiction 359
Colorimetric Computer Memory Dating 360
On CSI Abbreviation 362
The First Memory Dump Book 363
On SOS Abbreviation 365
Software Exceptions: a Paranormal View 366
Bug Entanglement (Bugtanglement) 367
The Standard Model of Debugging 368
Physics of Debugging 369
Can Computers Debug? 371
PART 7: Data Recovery 375
With the Help of Memory Dump Analysis 375
PART 8: Software Troubleshooting 377
Troubleshooter's Block 377
Causal Models 378
Object-Oriented Debugging and Troubleshooting 379
Component-Based Debugging and Troubleshooting 380
Domain-Driven Debugging and Troubleshooting 381
Myths and Facts about Software Support 382
Ceteris Paribus in Comparative Troubleshooting 383
Dancing in Software Support Environment 384
PARTS: Problem Solving Power of Thought 385

The Hidden Tomb in Pyramid of Software Change 386

Tracing 387

CDF Traces: Analyzing Process Launch Sequence 387

ETW Tracing Tools 389

Lean Tracing 390

Debugware Patterns 391

API Query 391

Tool Façade 392

Configuration Wrapper 393

Dual Interface 394

Tool Chain 395

Tool Box 396

PART 9: Security 397

Data Hiding in Crash Dumps 397

Hardening Dump Security: Beware of PEB Data 400

PART 10: The Origin of Crash Dumps 401

Memory Dumps from Xen-virtualized Windows 401

Bugchecks: SYSTEM_SERVICE_EXCEPTION 402

Bugcheck Callbacks 406

Application Verifier on x64 Platforms 413

Who Saved the Dump File? 414

ADPlus in 21 Seconds and 13 Steps 416

PART 11: Miscellaneous 425

Three Main Ideas of Debugging 425

Pseudo-corrupt Memory Dumps 426

Win32 Exception Frequencies 427

Bugcheck Frequencies 429

Time Travel Debugging 440

I/O and Memory Priority in Vista 441

Appendix A 443

Crash Dump File Examples 443

Appendix B 445

WinDbg.Org: WinDbg Quick Links 445

Appendix C 447

Dump2Wave Source Code 447

Appendix D 451

Dump2Picture Source Code 451

Appendix E 455

Crash Dump Analysis Checklist 455

CMDTREE.TXT 457

Index 459

Notes 465

About the Author 469

Cover Images 470