

Memory Dump Analysis Anthology

Color Supplement for Volumes 4-5

Dmitry Vostokov

Published by OpenTask, Republic of Ireland

Copyright © 2011 by Dmitry Vostokov

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.

Microsoft, MSDN, Visual C++, Visual Studio, Win32, Windows, Windows Server and Windows Vista are registered trademarks of Microsoft Corporation. Citrix is a registered trademark of Citrix Systems. Other product and company names mentioned in this book may be trademarks of their owners.

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

ISBN-13: 978-1-908043-04-7 (Paperback)

First printing, 2011

Preface	9
Acknowledgements	11
Volume 4	13
<i>Data Ordering</i>	13
<i>Clean Raw Stack Execution Residue</i>	29
<i>Pattern Interaction: Stack Trace Collection, Suspended Threads, Not My Version, Special Process, Main Thread and Blocked LPC Chain Threads</i>	37
<i>Pattern Interaction: Wait Chain, Blocked Thread, Waiting Thread Time, IRP Distribution Anomaly and Stack Trace Collection</i>	45
<i>Memoidealism as Monistic Aspect Pluralism</i>	49
<i>Metaphorical Bijectionism: A Method of Inquiry</i>	51
<i>Manifold Memory Space</i>	58
<i>MemD Category</i>	60
<i>Operating Closure of Memory</i>	63
<i>Experiments on Poor Bugs</i>	65
<i>The Tsar of Memory Dump Analysis</i>	66
<i>Bugs in Passing</i>	67
<i>After Volume 3</i>	70
<i>RADII Process Illustrated</i>	71

<i>Debugware Patterns: A Case Study</i>	73
<i>Workaround Patterns: Hidden Output</i>	78
<i>Extending Multithreading to Multibraiding (Adjoint Threading)</i>	81
<i>Software Trace Analysis Patterns: Characteristic Message Block</i>	85
<i>Software Trace Analysis Patterns: Activity Region</i>	88
<i>Software Trace Analysis Patterns: Inter-Correlation</i>	89
<i>Fiber Bundle of Memory Space</i>	91
<i>Pictures from Memory Space</i>	92
<i>Large-scale Structure of Memory Space</i>	94
<i>Advanced Memory Visualization</i>	96
<i>3D Memory Visualization</i>	108
<i>Memory Dump and Minidumps</i>	121
<i>Hot Issues from Physicalist Artist Perspective</i>	122
<i>Memory Dumps from Physicalist Artist Perspective</i>	123
<i>Memory Hot Spot and The Illusion of Fix</i>	124
<i>Shared Section</i>	125
<i>Memory Space Road to the Ultimate Fix</i>	126
<i>Structure and Noise</i>	127
<i>2 Great Windows Software Engineering Magazines</i>	128

Volume 5	129
<i>Architecture of CARE</i>	129
<i>Crash Dump Analysis Patterns: Coupled Processes (Weak)</i>	131
<i>Memory Systems Language</i>	134
<i>Collective Pointer</i>	135
<i>Archaeological Foundations for Memory Analysis</i>	138
<i>On God and Miracles</i>	140
<i>On Unconscious</i>	141
<i>General Memory Analysis</i>	142
<i>Category Theory and Troubleshooting</i>	143
<i>Software Chorography and Chorology: A Definition</i>	145
<i>Dr. DebugLove and Nature</i>	147
<i>Sailing Memory Spaces under an RGB Flag</i>	151
<i>Memory Dump Analysis Services Cap and T-Shirt</i>	152
<i>Basic Software PLOTs</i>	153
<i>Two Readings of a Software Trace</i>	155
<i>Presenting a Software Story</i>	157
<i>Software Trace Analysis Patterns: Trace Acceleration</i>	159

<i>Software Trace Analysis Patterns: Background and Foreground Components</i>	161
<i>Software Trace Analysis Patterns: Defamiliarizing Effect</i>	165
<i>Software Trace Analysis Patterns: Anchor Messages</i>	168
<i>Software Trace Analysis Patterns: Trace Partition</i>	171
<i>Software Trace Analysis Patterns: Layered Periodization</i>	174
<i>More on Demystifying First-chance Exceptions</i>	178
<i>Decomposing Memory Dumps via DumpFilter</i>	184
<i>Can a Memory Dump be Blue?</i>	188
<i>Virtual to Physical Memory Mapping</i>	189
<i>The Memory Visualization Question</i>	191
<i>Sweet Oil of Memory</i>	202
<i>Night Sky</i>	203
<i>Component Trace</i>	204
<i>Ana-Trace-Log-Lyzer and Closed Session</i>	205
<i>Computer Memory Gardens</i>	207
<i>Debugging Venue</i>	208
<i>Inside a Memory File</i>	209
<i>Fabric of Memory Dumps</i>	210
<i>Race Condition in a Kernel Pool</i>	221

<i>Memory Interfaces</i>	222
<i>Bleeding Memory</i>	223
<i>Picture Frame for Memory Dumps</i>	225
<i>Front Cover Glitch</i>	226
<i>Chance Exceptions in a Turing Machine</i>	227
<i>User/Kernel Diagramming Styles</i>	228