# Memory Dump Analysis Anthology

## Volume 8b

**Dmitry Vostokov**
**Software Diagnostics Institute**

OpenTask

Published by OpenTask, Republic of Ireland



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



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

ISBN-13: 978-1-908043-54-2 (Paperback)

First printing, 2015

Revision 1.02

# Table of Contents

**Preface** ..... **7**

**About the Author** ..... **9**

**PART 1: Professional Crash Dump Analysis and Debugging** ..... **11**

Win32 Start Address Fallacy ..... 11
Multidimensionality of Exceptions ..... 13

**PART 2: Crash Dump Analysis Patterns** ..... **15**

Reference Leak ..... 15
Origin Module ..... 19
Hidden Call ..... 21
Corrupt Structure ..... 26
Software Exception ..... 29
Crashed Process ..... 30
Variable Subtrace ..... 31
User Space Evidence ..... 37
Technology-Specific Subtrace (COM Client Call) ..... 38
Internal Stack Trace ..... 39
Distributed Exception (Managed Code) ..... 41
Thread Poset ..... 43

**PART 3: Pattern Interaction** ..... **45**

Virtualized Process, Stack Trace Collection, COM Interface Invocation Subtrace, Active Thread, Spiking Thread, Last Error Collection, RIP Stack Trace, Value References, Namespace, and Module Hint ..... 45

**PART 4: A Bit of Science and Philosophy** ..... **57**

Cantor Operating System ..... 57
Metaphor of Memory as a Directed Container ..... 57
Praxiverse ..... 58
When Universe is Going to End? ..... 58

Notes on Memoidealism ..... 59

**PART 5: Software Trace Analysis Patterns ..... 61**

Timeout ..... 61
Activity Overlap ..... 65
Adjoint Space ..... 67
Indirect Message ..... 70
Watch Thread ..... 75
Punctuated Activity ..... 77
Trace Mask ..... 78
Trace Viewpoints ..... 81
Data Reversal ..... 83
Recovered Messages ..... 85
Palimpsest Messages ..... 87
Message Space ..... 90
Interspace ..... 92
Translated Message ..... 94
Activity Disruption ..... 96

**PART 6: Fun with Debugging, Crash Dumps, and Traces ..... 99**

The Dump from the Future ..... 99
Exchange Rate on 16.12.14 ..... 99
Check the Plug ..... 100
Debugging Slang ..... 101

*YAWE ..... 101*
*Embedded Software Engineer ..... 101*
*Minute-wise ..... 101*
*Developer ..... 101*
*Multidigitalist ..... 101*
*KgB ..... 102*
*CIQ (Crash IQ) ..... 102*
*Pat Ching ..... 102*
*Explosive Mixture ..... 102*
*POEM ..... 102*
*YearNormous Day ..... 103*
*eNormous ..... 103*

2015 - The Year of RAM ..... 104
Diagnostics and Debugging in Science Fiction ..... 105
Software and Hardware Exceptions ..... 108
Logging for Kids ..... 110
Find the Bug ..... 111
Music for Debugging ..... 112
Tracing and Counting Book ..... 113
The Last Error ..... 114
Patching the Hardware Defect ..... 115
Pattern Match ..... 116

**PART 7: Software Narratology ..... 117**

Coding and Articoding ..... 117

**PART 8: Software Diagnostics, Troubleshooting, and Debugging ..... 119**

Special and General Trace and Log Analysis ..... 119
Projective Debugging ..... 123
Pattern! What Pattern? ..... 132
I Didn't See Anything ..... 135

**PART 9: Art and Photography ..... 137**

Diagnostics Designer Glasses ..... 137
Pattern Diagnostics Logo ..... 138
Happy Valentine's Day ..... 139
50 Shades of Crash Dump ..... 140
Computer Universe ..... 141
Failed Surveillance ..... 142
Debugging Allegory on FEB 23 ..... 143
Object in Signaled State ..... 144
Kernel Space Starts with 8 ..... 145
The Day of ST. P. The Elimination of Snakes ..... 146
The Fifth Column ..... 147
Proportionate Disproportionate Proportion ..... 148
Autoportrait in 5 Objects ..... 149
Kernel Works ..... 150
Chip Forensics ..... 151

Industrial Windows ..... 152
The Meaning of Life ..... 153
Hidden Bug ..... 154

**PART 10: Memory Forensics ..... 155**

Artifact-Malware and its Primary and Secondary Effects ..... 155

**PART 11: Miscellaneous ..... 161**

Quotes ..... 161
Status Updates ..... 163
Execution Residue ..... 164

**Appendix ..... 165**

Patterns are Weapons for Massive Debugging ..... 165
Crash Dump Analysis Checklist ..... 166

**Index of WinDbg Commands ..... 169**