

Memory Dump Analysis Anthology

Volume 1

Dmitry Vostokov

Published by OpenTask, Republic of Ireland

Copyright © 2008 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: 978-0-9558328-0-2 (Paperback)

ISBN-13: 978-0-9558328-1-9 (Hardcover)

First printing, 2008

To my mother, wife and children.

SUMMARY OF CONTENTS

Preface	19
Acknowledgements.....	21
About the Author	23
PART 1: Crash Dumps for Beginners	25
PART 2: Professional Crash Dump Analysis	43
PART 3: Crash Dump Analysis Patterns	251
PART 4: Crash Dump Analysis AntiPatterns	483
PART 5: A Bit of Science	491
PART 6: Fun with Crash Dumps.....	503
PART 7: WinDbg For GDB Users and Vice Versa	553
PART 8: Software Troubleshooting	579
PART 9: Citrix.....	583
PART 10: Security.....	589
PART 11: The Origin of Crash Dumps	595
PART 12: Tools	625
PART 13: Miscellaneous.....	639
Appendix A.....	695
Appendix B	697
Index	699
Notes.....	705

CONTENTS

Preface	19
Acknowledgements.....	21
About the Author	23
PART 1: Crash Dumps for Beginners	25
Crash Dumps Depicted	25
Right Crash Dumps	26
Crashes Explained	28
Hangs Explained	30
Symbol Files Explained	33
Crashes and Hangs Differentiated.....	35
Proactive Crash Dumps	38
PART 2: Professional Crash Dump Analysis.....	43
Minidump Analysis.....	43
Scripts and WinDbg Commands.....	43
Component Identification.....	46
Raw Stack Data Analysis.....	53
Symbols and Images.....	62
Interrupts and Exceptions Explained.....	67
Exceptions Ab Initio.....	67
X86 Interrupts	68

X64 Interrupts	75
Interrupt Frames and Stack Reconstruction	82
Trap Command on x86.....	91
Trap Command on x64.....	99
Exceptions in User Mode	103
How to Distinguish Between 1st and 2nd Chances	108
Who Calls the Postmortem Debugger?	111
Inside Vista Error Reporting	115
Another Look at Page Faults	130
Bugchecks Depicted	133
NMI_HARDWARE_FAILURE.....	133
IRQL_NOT_LESS_OR_EQUAL.....	134
KERNEL_MODE_EXCEPTION_NOT_HANDLED	139
KMODE_EXCEPTION_NOT_HANDLED.....	141
SYSTEM_THREAD_EXCEPTION_NOT_HANDLED	142
CAFF	148
CF.....	150
Manual Stack Trace Reconstruction.....	155
WinDbg Tips and Tricks	165
Looking for Strings in a Dump.....	165
Tracing Win32 API While Debugging a Process	166
Exported NTDLL and Kernel Structures.....	168

Easy List Traversing	176
Suspending Threads	179
Heap Stack Traces	180
Hypertext Commands	181
Analyzing Hangs Faster	185
Triple Dereference	186
Finding a Needle in a Hay.....	189
Guessing Stack Trace.....	191
Coping with Missing Symbolic Information	197
Resolving Symbol Messages.....	202
The Search for Tags.....	204
Old Dumps, New Extensions	210
Object Names and Waiting Threads	212
Memory Dumps from Virtual Images	217
Filtering Processes	218
WinDbg Scripts.....	219
First Encounters	219
Yet Another WinDbg Script	220
Deadlocks and Critical Sections.....	221
Security Problem	222
Hundreds of Crash Dumps	225
Parameterized Scripts	227

Security Issues and Scripts	228
Raw Stack Dump of All Threads (Process Dump).....	229
Raw Stack Dump of All Threads (Complete Dump).....	234
Case Study	239
Detecting Loops in Code	242
Crash Dump Analysis Checklist.....	248
Crash Dump Analysis Poster (HTML version)	250
PART 3: Crash Dump Analysis Patterns.....	251
Multiple Exceptions.....	251
Dynamic Memory Corruption	253
False Positive Dump	255
Lateral Damage	259
Optimized Code.....	260
Invalid Pointer	262
Inconsistent Dump	264
Hidden Exception	266
Deadlock (Critical Sections).....	271
Changed Environment.....	278
Incorrect Stack Trace.....	283
OMAP Code Optimization	289
No Component Symbols.....	293
Insufficient Memory (Committed Memory).....	297
Spiking Thread.....	300

Module Variety	305
Stack Overflow (Kernel).....	309
Deadlock (Executive Resources).....	318
Insufficient Memory (Handle Leak).....	322
Managed Code Exception	326
Truncated Dump	334
Waiting Thread Time.....	337
Deadlock (Mixed Objects)	342
Memory Leak (Process Heap).....	350
Missing Thread	356
Unknown Component	361
Memory Leak (.NET Heap)	365
Double Free (Process Heap).....	372
Double Free (Kernel Pool)	381
Coincidental Symbolic Information	384
Stack Trace	389
Virtualized Process (WOW64).....	393
Stack Trace Collection	402
Coupled Processes	411
High Contention	413
Accidental Lock	415
Passive Thread (User Space)	422
Main Thread.....	428

Insufficient Memory (Kernel Pool)	432
Busy System	440
Historical Information	449
IRP Distribution Anomaly	450
Local Buffer Overflow.....	452
Passive System Thread (Kernel Space)	453
Early Crash Dump	457
Hooked Functions	460
Custom Exception Handler.....	462
Deadlock (LPC)	465
Special Stack Trace	469
Manual Dump (Kernel)	470
Wait Chain (General).....	472
Manual Dump (Process)	477
Wait Chain (Critical Sections)	480
PART 4: Crash Dump Analysis AntiPatterns	483
Alien Component	483
Zippocrisy	484
Word of Mouth	485
Wrong Dump	486
Fooled by Description	487
Need the crash dump.....	488
Be Language	489

Foiled by Abbreviation	490
PART 5: A Bit of Science	491
Memory Dump - A Mathematical Definition	491
Threads as Braided Strings in Abstract Space	492
What is Memory Dump Analysis?	495
Memorillion and Quadrimemorillion	496
Four Causes of Crash Dumps.....	497
Complexity and Memory Dumps	499
What is a Software Defect?	500
PART 6: Fun with Crash Dumps.....	503
Dump Analysis and Voice Recognition	503
Sending SMS Messages via Dumps	504
WinDbg as a Big Calculator	505
Dumps, Debuggers and Virtualization.....	506
Musical Dumps.....	508
Debugging the Debugger	509
Musical Dumps: Dump2Wave.....	511
Dump Tomography	512
The Smallest Program	513
Voices from Process Space.....	516
Crash Dump Analysis Card	518
Listening to Computer Memory	519
Visualizing Memory Dumps.....	522

Visualizing Memory Leaks	534
Picturing Computer Memory	546
Unicode Illuminated	549
Teaching Binary to Decimal Conversion	550
Crash Dumps and Global Conspiracy	551
PART 7: WinDbg For GDB Users and Vice Versa	553
AT&T and Intel Syntax	553
Installation	555
Disassembler	558
Stack Trace (Backtrace)	563
Local Variables	571
PART 8: Software Troubleshooting	579
Four Pillars	579
Five Golden Rules	580
Critical Thinking	581
Troubleshooting as Ddebugging	582
PART 9: Citrix	583
Pooltags	583
The List of Citrix Services	584
Reverse Engineering Citrix ThinWire	586
PART 10: Security	589
Memory Visualization	589
WinDbg is Privacy-Aware	590

Crash Dumps and Security	594
PART 11: The Origin of Crash Dumps	595
JIT Service Debugging.....	595
Local Crash Dumps in Vista	596
COM+ Crash Dumps	597
Correcting Microsoft Article about Userdump.exe	602
Where did the Crash Dump Come from?	606
Custom Postmortem Debuggers in Vista	608
Resurrecting Dr. Watson in Vista	611
Process Crash - Getting the Dump Manually	614
Upgrading Dr. Watson.....	617
Savedump.exe and Pagefile	618
Dumping Vista	619
Dumping Processes Without Breaking Them	621
Userdump.exe on x64	622
NTSD on x64 Windows	623
Need a Dump? Common Use Cases	624
PART 12: Tools	625
Memory Dump Analysis Using Excel	625
TestDefaultDebugger.NET	626
Cons of Symbol Server	627
StressPrinters: Stressing Printer Autocreation	628
InstantDump (JIT Process Dumper).....	629

TestDefaultDebugger	631
DumpAlerts	633
DumpDepends	634
Dump Monitor Suite	635
SystemDump	636
PART 13: Miscellaneous.....	639
What is KiFastSystemCallRet?.....	639
Understanding I/O Completion Ports.....	643
Symbol File Warnings.....	646
Windows Service Crash Dumps in Vista	648
The Road to Kernel Space	654
Memory Dump Analysis Interview Questions.....	656
Music for Debugging	657
PDBFinder.....	658
When a Process Dies Silently	659
ASLR: Address Space Layout Randomization	664
Process and Thread Startup in Vista	669
Race Conditions on a Uniprocessor Machine.....	671
Yet Another Look at Zw* and Nt* Functions.....	674
Programmer Universalis.....	677
Dr. Watson Logs Analysis	678
Post-Debugging Complications	681
The Elements of Crash Dump Analysis Style	682

Crash Dump Analysis in Visual Studio	683
32-bit Stack from 64-bit Dump.....	685
Asmpedia.....	686
How WINE Can Help in Crash Dump Analysis.....	687
Horrors of Debugging Legacy Code	688
UML and Device Drivers	690
Statistics: 100% CPU Spread over all Processes	693
Appendix A.....	695
Crash Dump Analysis Portal	695
Appendix B	697
Reference Stack Traces	697
Index	699
Notes.....	705

