

Memory Dump Analysis Anthology Volume 1

Revised Edition

Dmitry Vostokov
Software Diagnostics Institute

Published by OpenTask, Republic of Ireland

Copyright © 2020 by Dmitry Vostokov

Copyright © 2020 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.

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

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: 978-1912636211 (Paperback)

Revision 4.01 (April 2020)

Dedicated to the memory of my mother.

[This page is intentionally left blank]

Summary of Contents

Preface	19
Acknowledgments	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	255
PART 4: Crash Dump Analysis AntiPatterns	493
PART 5: A Bit of Science	501
PART 6: Fun with Crash Dumps	513
PART 7: WinDbg For GDB Users and Vice Versa	563
PART 8: Software Troubleshooting	589
PART 9: Reversing and Reconstruction	593
PART 10: Security	599
PART 11: The Origin of Crash Dumps	605
PART 12: Tools	635
PART 13: Miscellaneous	649
Appendix	703
Index of WinDbg Commands	707
Cover Images	711

[This page is intentionally left blank]

Contents

Preface	19
Acknowledgments	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	31
Symbol Files Explained	34
Crashes and Hangs Differentiated.....	36
Proactive Crash Dumps	39
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.....	63
Interrupts and Exceptions Explained.....	68
Exceptions Ab Initio.....	68
X86 Interrupts	69
X64 Interrupts	76

Interrupt Frames and Stack Reconstruction	83
Trap Command on x86	92
Trap Command on x64	100
Exceptions in User Mode	104
How to Distinguish Between 1st and 2nd Chances	109
Who Calls the Postmortem Debugger?	113
Inside Vista Error Reporting	117
Another Look at Page Faults	132
Bugchecks Depicted	135
NMI_HARDWARE_FAILURE	135
IRQL_NOT_LESS_OR_EQUAL	136
KERNEL_MODE_EXCEPTION_NOT_HANDLED	141
KMODE_EXCEPTION_NOT_HANDLED	143
SYSTEM_THREAD_EXCEPTION_NOT_HANDLED	144
CAFF	150
CF	152
Manual Stack Trace Reconstruction	157
WinDbg Tips and Tricks	167
Looking for Strings in a Dump	167
Tracing Win32 API While Debugging a Process	168
Exported NTDLL and Kernel Structures	170
Easy List Traversing	178
Suspending Threads	181

Heap Stack Traces	182
Hypertext Commands	183
Analyzing Hangs Faster	187
Triple Dereference	188
Finding a Needle in a Hay	191
Guessing Stack Trace	193
Coping with Missing Symbolic Information	199
Resolving Symbol Messages	204
The Search for Tags	206
Old Dumps, New Extensions	212
Object Names and Waiting Threads	214
Memory Dumps from Virtual Images	219
Filtering Processes	220
WinDbg Scripts	221
First Encounters	221
Yet another WinDbg Script	222
Deadlocks and Critical Sections	223
Security Problem	224
Hundreds of Crash Dumps	227
Parameterized Scripts	229
Security Issues and Scripts	230
Raw Stack Dump of All Threads (Process Dump)	231
Raw Stack Dump of All Threads (Complete Dump)	236

Case Study	241
Detecting Loops in Code	244
Crash Dump Analysis Checklist.....	251
Crash Dump Analysis Poster (HTML version)	254
PART 3: Crash Dump Analysis Patterns.....	255
Multiple Exceptions.....	255
Dynamic Memory Corruption	257
False Positive Dump	259
Lateral Damage	264
Optimized Code.....	265
Invalid Pointer	267
Inconsistent Dump	269
Hidden Exception (User Space)	271
Deadlock (Critical Sections).....	276
Changed Environment.....	283
Incorrect Stack Trace.....	288
OMAP Code Optimization	294
No Component Symbols.....	298
Insufficient Memory (Committed Memory).....	302
Spiking Thread.....	305
Module Variety	310
Stack Overflow (Kernel Mode)	314
Deadlock (Executive Resources).....	323

Insufficient Memory (Handle Leak).....	327
Managed Code Exception	331
Truncated Dump	340
Waiting Thread Time (Kernel Dumps).....	343
Deadlock (Mixed Objects, User Space)	348
Memory Leak (Process Heap).....	356
Missing Thread	362
Unknown Component	367
Memory Leak (.NET Heap)	371
Double Free (Process Heap).....	378
Double Free (Kernel Pool)	387
Coincidental Symbolic Information	390
Stack Trace	395
Virtualized Process (WOW64).....	400
Stack Trace Collection (Unmanaged Space).....	409
Coupled Processes (Strong).....	419
High Contention (Executive Resources)	421
Accidental Lock	423
Passive Thread (User Space)	430
Main Thread	437
Insufficient Memory (Kernel Pool).....	441
Busy System	449
Historical Information	458

Object Distribution Anomaly (IRP)	459
Local Buffer Overflow.....	461
Passive System Thread (Kernel Space)	462
Early Crash Dump	466
Hooked Functions (User Space)	469
Custom Exception Handler (User Space).....	471
Deadlock (LPC)	474
Special Stack Trace	479
Manual Dump (Kernel)	480
Wait Chain (General).....	482
Manual Dump (Process)	487
Wait Chain (Critical Sections)	490
PART 4: Crash Dump Analysis AntiPatterns	493
Alien Component	493
Zippocrisy	494
Word of Mouth	495
Wrong Dump	496
Fooled by Description	497
Need the Crash Dump	498
Be Language	499
Fooled by Abbreviation	500
PART 5: A Bit of Science	501
Memory Dump - A Mathematical Definition	501

Threads as Braided Strings in Abstract Space	503
What is Memory Dump Analysis?	506
Memorillion and Quadrimemorillion	507
Four Causes of Crash Dumps.....	508
Complexity and Memory Dumps	510
What is a Software Defect?	511
PART 6: Fun with Crash Dumps.....	513
Dump Analysis and Voice Recognition	513
Sending SMS Messages via Dumps	514
WinDbg as a Big Calculator	515
Dumps, Debuggers, and Virtualization.....	516
Musical Dumps.....	518
Debugging the Debugger	519
Musical Dumps: Dump2Wave.....	521
Dump Tomography	522
The Smallest Program	523
Voices from Process Space.....	526
Crash Dump Analysis Card	528
Listening to Computer Memory	529
Visualizing Memory Dumps.....	532
Visualizing Memory Leaks	544
Picturing Computer Memory	556
Unicode Illuminated	559

Teaching Binary to Decimal Conversion	560
Crash Dumps and Global Conspiracy	561
PART 7: WinDbg For GDB Users and Vice Versa	563
AT&T and Intel Syntax	563
Installation	565
Disassembler	568
Stack Trace (Backtrace)	573
Local Variables	581
PART 8: Software Troubleshooting	589
Four Pillars.....	589
Five Golden Rules.....	590
Critical Thinking.....	591
Troubleshooting as Debugging.....	592
PART 9: Reversing and Reconstruction	593
Pooltags.....	593
The List of Services	594
Reverse Engineering Component Dependencies	596
PART 10: Security.....	599
Memory Visualization	599
WinDbg is Privacy-Aware	600
Crash Dumps and Security	604
PART 11: The Origin of Crash Dumps	605
JIT Service Debugging.....	605

Local Crash Dumps in Vista	606
COM+ Crash Dumps	607
Correcting Microsoft Article about Userdump.exe	612
Where did the Crash Dump Come from?	616
Custom Postmortem Debuggers in Vista	618
Resurrecting Dr. Watson in Vista	621
Process Crash - Getting the Dump Manually	624
Upgrading Dr. Watson.....	627
Savedump.exe and Pagefile	628
Dumping Vista	629
Dumping Processes without Breaking Them.....	631
Userdump.exe on x64	632
NTSD on x64 Windows	633
Need a Dump? Common Use Cases	634
PART 12: Tools	635
Memory Dump Analysis Using Excel	635
TestDefaultDebugger.NET	636
Cons of Symbol Server	637
StressPrinters: Stressing Printer Autocreation.....	638
InstantDump (JIT Process Dumper).....	639
TestDefaultDebugger	641
DumpAlerts	643
DumpDepends	644

Dump Monitor Suite	645
SystemDump	646
PART 13: Miscellaneous	649
What is KiFastSystemCallRet?	649
Understanding I/O Completion Ports.....	653
Symbol File Warnings	656
Windows Service Crash Dumps in Vista	658
The Road to Kernel Space	664
Memory Dump Analysis Interview Questions.....	665
Music for Debugging	666
PDBFinder.....	667
When a Process Dies Silently	668
ASLR: Address Space Layout Randomization	673
Process and Thread Startup in Vista	678
Race Conditions on a Uniprocessor Machine.....	680
Yet Another Look at Zw* and Nt* Functions.....	683
Programmer Universalis.....	686
Dr. Watson Logs Analysis	687
Post-Debugging Complications	690
The Elements of Crash Dump Analysis Style	691
Crash Dump Analysis in Visual Studio	692
32-bit Stack from 64-bit Dump.....	694
Asmpedia.....	695

How WINE Can Help in Crash Dump Analysis	696
Horrors of Debugging Legacy Code	697
UML and Device Drivers	699
Statistics: 100% CPU Spread over all Processes	702
Appendix	703
Crash Dump Analysis Portal	703
Reference Stack Traces	706
Index of WinDbg Commands	707
Cover Images.....	711

ISBN 978-1-912636-21-1



90000

9 781912 636211