
Encyclopedia of Crash Dump Analysis Patterns

Second Edition

Detecting Abnormal Software Structure and Behavior in Computer Memory

Dmitry Vostokov
Software Diagnostics Institute

Published by OpenTask, Republic of Ireland

Copyright © 2017 by Dmitry Vostokov

Copyright © 2017 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: 978-1-908043-83-2 (Paperback)

First printing, 2017

Version 1.04 (March 2017)

Summary of Contents

Summary of Contents	3
Detailed Table of Contents	18
Preface to the First Edition	45
Preface to the Second Edition	46
Acknowledgements	47
About the Author	48
A	49
Abridged Dump	49
Accidental Lock	53
Activation Context	60
Active Thread	63
Activity Resonance	70
Affine Thread	72
Annotated Disassembly	75
B	76
Blocked DPC	76
Blocked Queue	77
Blocked Thread	80
Blocking File	93
Blocking Module	96
Broken Link	97

Busy System	99
C	108
C++ Exception	108
Caller-n-Callee	111
Changed Environment	114
Clone Dump	118
Cloud Environment	122
CLR Thread	124
Coincidental Error Code	128
Coincidental Frames	130
Coincidental Symbolic Information	134
Constant Subtrace	141
Corrupt Dump	142
Corrupt Structure	144
Coupled Machines	146
Coupled Modules	147
Coupled Processes	148
Crash Signature	153
Crash Signature Invariant	155
Crashed Process	156
Critical Region	157
Critical Section Corruption	161

Critical Stack Trace	168
Custom Exception Handler	169
D	174
Data Alignment	174
Data Contents Locality	175
Data Correlation	180
Deadlock	182
Debugger Bug	219
Debugger Omission	220
Design Value	221
Deviant Module	222
Deviant Token	229
Diachronic Module	230
Dialog Box	232
Directing Module	235
Disconnected Network Adapter	236
Disk Packet Buildup	238
Dispatch Level Spin	241
Distributed Exception	243
Distributed Spike	245
Distributed Wait Chain	253
Divide by Zero	255

Double Free	260
Double IRP Completion	279
Driver Device Collection	280
Dry Weight	281
Dual Stack Trace	282
Duplicate Extension	283
Duplicated Module	287
Dynamic Memory Corruption	292
E	312
Early Crash Dump	312
Effect Component	315
Embedded Comments	320
Empty Stack Trace	321
Environment Hint	324
Error Reporting Fault	325
Evental Dumps	328
Exception Module	361
Exception Stack Trace	363
Execution Residue	365
F	385
Fake Module	385
False Effective Address	389

False Function Parameters	390
False Positive Dump	393
Fat Process Dump	395
Fault Context	396
First Fault Stack Trace	397
Foreign Module Frame	398
FPU Exception	401
Frame Pointer Omission	403
Frozen Process	407
G	411
Ghost Thread	411
Glued Stack Trace	413
H	416
Handle Leak	416
Handle Limit	417
Handled Exception	428
Hardware Activity	437
Hardware Error	441
Hidden Call	450
Hidden Exception	455
Hidden IRP	462
Hidden Module	463

Hidden Parameter	465
Hidden Process	467
Hidden Stack Trace	469
High Contention	472
Historical Information	483
Hooked Functions	484
Hooked Modules	490
Hooking Level	492
I	495
Incomplete Stack Trace	495
Incomplete Session	496
Inconsistent Dump	498
Incorrect Stack Trace	499
Incorrect Symbolic Information	505
Injected Symbols	510
Inline Function Optimization	512
Instrumentation Information	516
Instrumentation Side Effect	520
Insufficient Memory	523
Internal Stack Trace	568
Invalid Exception Information	570
Invalid Handle	574

Invalid Parameter	586
Invalid Pointer	589
J	591
JIT Code	591
L	596
Last Error Collection	596
Last Object	599
Late Crash Dump	601
Lateral Damage	602
Least Common Frame	604
Livelock	606
Local Buffer Overflow	608
Lost Opportunity	612
M	614
Main Thread	614
Managed Code Exception	617
Managed Stack Trace	624
Manual Dump	625
Memory Fluctuation	634
Memory Leak	636
Message Box	660
Message Hooks	663

Mirror Dump Set	666
Missing Component	668
Missing Process	682
Missing Thread	683
Mixed Exception	688
Module Collection	693
Module Hint	696
Module Product Process	698
Module Stack Trace	699
Module Variable	701
Module Variety	703
Multiple Exceptions	706
N	722
Namespace	722
Nested Exceptions	723
Nested Offender	730
Network Packet Buildup	733
No Component Symbols	734
No Current Thread	737
No Data Types	739
No Process Dumps	740
No System Dumps	741

Not My Thread	742
Not My Version	743
NULL Pointer	745
O	756
Object Distribution Anomaly	756
OMAP Code Optimization	761
One-Thread Process	765
Optimized Code	767
Optimized VM Layout	769
Origin Module	771
Out-of-Module Pointer	773
Overaged System	774
P	775
Packed Code	775
Paged Out Data	778
Parameter Flow	780
Paratext	783
Pass Through Function	787
Passive System Thread	789
Passive Thread	793
Past Stack Trace	800
Patched Code	802

Pervasive System	803
Place Trace	804
Platform-Specific Debugger	806
Pleiades	808
Pre-Obfuscation Residue	809
Problem Exception Handler	810
Problem Module	812
Problem Vocabulary	813
Process Factory	814
Punctuated Memory Leak	819
Q	823
Quiet Dump	823
Quotient Stack Trace	824
R	825
Random Object	825
Raw Pointer	828
Reduced Symbolic Information	829
Reference Leak	830
Regular Data	833
Relative Memory Leak	834
RIP Stack Trace	837
Rough Stack Trace	839

S	842
Same Vendor	842
Screwbolt Wait Chain	843
Self-Diagnosis	844
Self-Dump	850
Semantic Split	853
Semantic Structure	860
Shared Buffer Overwrite	864
Shared Structure	872
Small Value	873
Software Exception	875
Special Process	877
Special Stack Trace	882
Special Thread	883
Spike Interval	884
Spiking Thread	885
Stack Overflow	895
Stack Trace	917
Stack Trace Change	932
Stack Trace Collection	933
Stack Trace Set	952
Stack Trace Signature	955

Stack Trace Surface	957
Step Dumps	958
Stored Exception	959
String Hint	960
String Parameter	962
Suspended Thread	964
Swarm of Shared Locks	966
System Object	971
T	974
Tampered Dump	974
Technology-Specific Subtrace	987
Template Module	997
Thread Age	1001
Thread Cluster	1003
Thread Poset	1004
Thread Starvation	1006
Top Module	1012
Translated Exception	1013
Truncated Dump	1014
Truncated Stack Trace	1017
U	1020
Ubiquitous Component	1020

Unified Stack Trace	1035
Unknown Component	1037
Unloaded Module	1041
Unrecognizable Symbolic Information	1045
Unsynchronized Dumps	1050
User Space Evidence	1051
V	1052
Value Adding Process	1052
Value Deviation	1053
Value References	1057
Variable Subtrace	1058
Version-Specific Extension	1064
Virtualized Process	1068
Virtualized System	1076
W	1082
Wait Chain	1082
Waiting Thread Time	1137
Well-Tested Function	1146
Well-Tested Module	1147
Wild Code	1148
Wild Pointer	1151
Window Hint	1153

Y	1156
Young System	1156
Z	1158
Zombie Processes	1158
Bibliography	1165
Appendix A	1166
Reference Stack Traces	1166
Appendix B	1167
.NET / CLR / Managed Space Patterns	1167
Contention Patterns	1168
Deadlock and Livelock Patterns	1169
DLL Link Patterns	1170
Dynamic Memory Corruption Patterns	1171
Executive Resource Patterns	1172
Exception Patterns	1173
Falsity and Coincidence Patterns	1174
Hooksware Patterns	1175
Memory Consumption Patterns	1177
Meta-Memory Dump Patterns	1178
Module Patterns	1179
Optimization Patterns	1180
Process Patterns	1181

RPC, LPC and ALPC Patterns	1182
Stack Overflow Patterns	1183
Stack Trace Patterns	1184
Symbol Patterns	1186
Thread Patterns	1187
Wait Chain Patterns	1188
Appendix C	1189
Crash Dump Analysis Checklist	1189
Index	1192

Detailed Table of Contents

Summary of Contents	3
Detailed Table of Contents	18
Preface to the First Edition	45
Preface to the Second Edition	46
Acknowledgements	47
About the Author	48
A	49
Abridged Dump	49
Accidental Lock	53
Activation Context	60
Active Thread	63
Linux	63
Mac OS X	64
Windows	66
Activity Resonance	70
Affine Thread	72
Annotated Disassembly	75
JIT .NET Code	75
B	76
Blocked DPC	76
Blocked Queue	77

LPC/ALPC	77
Comments	79
Blocked Thread	80
Hardware	80
Software	82
Comments	90
Timeout	92
Blocking File	93
Blocking Module	96
Comments	96
Broken Link	97
Busy System	99
C	108
C++ Exception	108
Linux	108
Mac OS X	109
Windows	110
Comments	110
Caller-n-Callee	111
Changed Environment	114
Comments	117
Clone Dump	118
Cloud Environment	122

CLR Thread	124
Comments	127
Coincidental Error Code	128
Coincidental Frames	130
Comments	133
Coincidental Symbolic Information	134
Linux	134
Mac OS X	135
Windows	137
Constant Subtrace	141
Corrupt Dump	142
Comments	143
Corrupt Structure	144
Coupled Machines	146
Coupled Modules	147
Coupled Processes	148
Semantics	148
Strong	149
Comments	150
Weak	151
Crash Signature	153
Crash Signature Invariant	155
Crashed Process	156

Critical Region	157
Linux	157
Critical Section Corruption	161
Critical Stack Trace	168
Custom Exception Handler	169
Kernel Space	169
User Space	171
D	174
Data Alignment	174
Page Boundary	174
Data Contents Locality	175
Data Correlation	180
Function Parameters	180
Deadlock	182
Critical Sections	182
Comments	189
Executive Resources	194
LPC	197
Managed Space	202
Mixed Objects	205
Kernel Space	205
User Space	210
Comments	217

Self	218
Comments	218
Debugger Bug	219
Debugger Omission	220
Design Value	221
Deviant Module	222
Comments	228
Deviant Token	229
Diachronic Module	230
Dialog Box	232
Directing Module	235
Disconnected Network Adapter	236
Disk Packet Buildup	238
Comments	240
Dispatch Level Spin	241
Distributed Exception	243
Managed Code	243
Distributed Spike	245
Comments	252
Distributed Wait Chain	253
Divide by Zero	255
Kernel Mode	255

User Mode	257
Linux	257
Mac OS X	258
Windows	259
Double Free	260
Kernel Pool	260
Comments	262
Process Heap	267
Windows	267
Comments	276
Mac OS X	278
Double IRP Completion	279
Driver Device Collection	280
Dry Weight	281
Dual Stack Trace	282
Duplicate Extension	283
Comments	286
Duplicated Module	287
Comments	291
Dynamic Memory Corruption	292
Kernel Pool	292
Comments	297
Managed Heap	301

Process Heap	304
Linux	304
Mac OS X	305
Windows	307
Comments	308
E	312
Early Crash Dump	312
Effect Component	315
Embedded Comments	320
Empty Stack Trace	321
Comments	323
Environment Hint	324
Comments	324
Error Reporting Fault	325
Evental Dumps	328
Exception Module	361
Exception Stack Trace	363
Comments	364
Execution Residue	365
Linux	365
Mac OS X	367
Windows	369
Managed Space	369

Comments	370
Unmanaged Space	371
Comments	382
F	385
Fake Module	385
False Effective Address	389
False Function Parameters	390
False Positive Dump	393
Fat Process Dump	395
Fault Context	396
First Fault Stack Trace	397
Foreign Module Frame	398
FPU Exception	401
Frame Pointer Omission	403
Frozen Process	407
G	411
Ghost Thread	411
Glued Stack Trace	413
H	416
Handle Leak	416
Handle Limit	417
GDI	417

Kernel Space	417
User Space	423
Handled Exception	428
.NET CLR	428
Kernel Space	433
User Space	434
Comments	436
Hardware Activity	437
Hardware Error	441
Comments	446
Hidden Call	450
Hidden Exception	455
Kernel Space	455
Comments	456
User Space	457
Comments	461
Hidden IRP	462
Hidden Module	463
Comments	464
Hidden Parameter	465
Hidden Process	467
Hidden Stack Trace	469
High Contention	472

.NET CLR Monitors	472
Critical Sections	475
Executive Resources	477
Comments	479
Processors	480
Historical Information	483
Comments	483
Hooked Functions	484
Kernel Space	484
Comments	487
User Space	488
Comments	489
Hooked Modules	490
Comments	491
Hooking Level	492
I	495
Incomplete Stack Trace	495
GDB	495
Incomplete Session	496
Comments	497
Inconsistent Dump	498
Comments	498
Incorrect Stack Trace	499

Comments	504
Incorrect Symbolic Information	505
Injected Symbols	510
Inline Function Optimization	512
Managed Code	512
Unmanaged Code	514
Instrumentation Information	516
Instrumentation Side Effect	520
Comments	522
Insufficient Memory	523
Committed Memory	523
Control Blocks	525
Handle Leak	526
Comments	530
Kernel Pool	535
Comments	543
Module Fragmentation	544
Comments	551
Physical Memory	552
PTE	555
Comments	556
Region	557
Reserved Virtual Memory	559
Session Pool	562

Stack Trace Database	563
Internal Stack Trace	568
Invalid Exception Information	570
Invalid Handle	574
General	574
Comments	577
Managed Space	578
Comments	585
Invalid Parameter	586
Process Heap	586
Invalid Pointer	589
General	589
J	591
JIT Code	591
.NET	591
Comments	593
Java	594
L	596
Last Error Collection	596
Comments	597
Last Object	599
Comments	600
Late Crash Dump	601

Lateral Damage	602
Linux	602
Windows	603
Comments	603
Least Common Frame	604
Livelock	606
Local Buffer Overflow	608
Linux	608
Mac OS X	609
Windows	611
Comments	611
Lost Opportunity	612
M	614
Main Thread	614
Managed Code Exception	617
Managed Stack Trace	624
Manual Dump	625
Kernel	625
Comments	626
Process	630
Comments	633
Memory Fluctuation	634
Process Heap	634

Comments	635
Memory Leak	636
.NET Heap	636
Comments	642
I/O Completion Packets	643
Page Tables	644
Process Heap	650
Comments	656
Regions	657
Message Box	660
Comments	662
Message Hooks	663
Comments	665
Mirror Dump Set	666
Missing Component	668
General	668
Static Linkage	672
User Mode	672
Comments	681
Missing Process	682
Comments	682
Missing Thread	683
Comments	687

Mixed Exception	688
Comments	692
Module Collection	693
General	693
Predicate	695
Module Hint	696
Comments	697
Module Product Process	698
Module Stack Trace	699
Linux	699
Windows	700
Module Variable	701
Module Variety	703
Multiple Exceptions	706
Mac OS X	706
Windows	708
Kernel Mode	708
Managed Space	713
Stowed	714
User Mode	720
N	722
Namespace	722
Nested Exceptions	723

Managed Code	723
Comments	725
Unmanaged Code	726
Nested Offender	730
Network Packet Buildup	733
No Component Symbols	734
No Current Thread	737
No Data Types	739
No Process Dumps	740
No System Dumps	741
Comments	741
Not My Thread	742
Not My Version	743
Hardware	743
Software	744
NULL Pointer	745
Linux	745
Code	745
Data	746
Mac OS X	747
Code	747
Data	749
Windows	750

Code	750
Data	752
Comments	752
O	756
Object Distribution Anomaly	756
.NET Heap	756
IRP	759
Comment	760
OMAP Code Optimization	761
Comments	764
One-Thread Process	765
Optimized Code	767
Comments	768
Optimized VM Layout	769
Origin Module	771
Out-of-Module Pointer	773
Overaged System	774
Comments	774
P	775
Packed Code	775
Paged Out Data	778
Parameter Flow	780

Paratext	783
Linux	783
Mac OS X	785
Comments	786
Pass Through Function	787
Comments	788
Passive System Thread	789
Kernel Space	789
Passive Thread	793
User Space	793
Comments	799
Past Stack Trace	800
Patched Code	802
Pervasive System	803
Place Trace	804
Comments	805
Platform-Specific Debugger	806
Pleiades	808
Pre-Obfuscation Residue	809
Problem Exception Handler	810
Comments	811
Problem Module	812

Comments	812
Problem Vocabulary	813
Process Factory	814
Punctuated Memory Leak	819
Q	823
Quiet Dump	823
Quotient Stack Trace	824
R	825
Random Object	825
Raw Pointer	828
Reduced Symbolic Information	829
Reference Leak	830
Regular Data	833
Relative Memory Leak	834
RIP Stack Trace	837
Rough Stack Trace	839
S	842
Same Vendor	842
Screwbolt Wait Chain	843
Self-Diagnosis	844
Kernel Mode	844
Comments	844

Registry	845
User Mode	847
Comments	848
Self-Dump	850
Comments	852
Semantic Split	853
Semantic Structure	860
PID.TID	860
Comments	863
Shared Buffer Overwrite	864
Mac OS X	864
Windows	868
Shared Structure	872
Small Value	873
Comments	874
Software Exception	875
Comments	875
Special Process	877
Comments	881
Special Stack Trace	882
Comments	882
Special Thread	883

.NET CLR	883
Spike Interval	884
Spiking Thread	885
Linux	885
Mac OS X	886
Windows	888
Comments	893
Stack Overflow	895
Linux	895
Mac OS X	897
Windows	900
Kernel Mode	900
Comments	908
Software Implementation	910
User Mode	912
Comments	915
Stack Trace	917
Linux	917
Mac OS X	918
Windows	919
Database	919
File System Filters	924
General	926
I/O Request	930

Stack Trace Change	932
Stack Trace Collection	933
CPUs	933
I/O Requests	936
Managed Space	940
Predicate	943
Comments	943
Unmanaged Space	944
Comments	951
Stack Trace Set	952
Stack Trace Signature	955
Stack Trace Surface	957
Step Dumps	958
Stored Exception	959
String Hint	960
String Parameter	962
Suspended Thread	964
Swarm of Shared Locks	966
System Object	971
T	974
Tampered Dump	974
Technology-Specific Subtrace	987
COM Client Call	987

COM Interface Invocation	988
Comments	991
Dynamic Memory	992
JIT .NET Code	994
Template Module	997
Thread Age	1001
Thread Cluster	1003
Thread Poset	1004
Thread Starvation	1006
Normal Priority	1006
Realtime Priority	1008
Top Module	1012
Translated Exception	1013
Truncated Dump	1014
Mac OS X	1014
Windows	1015
Truncated Stack Trace	1017
Comments	1017
U	1020
Ubiquitous Component	1020
Kernel Space	1020
User Space	1023
Unified Stack Trace	1035

Unknown Component	1037
Unloaded Module	1041
Unrecognizable Symbolic Information	1045
Unsynchronized Dumps	1050
User Space Evidence	1051
V	1052
Value Adding Process	1052
Value Deviation	1053
Stack Trace	1053
Value References	1057
Comments	1057
Variable Subtrace	1058
Version-Specific Extension	1064
Virtualized Process	1068
WOW64	1068
Comments	1075
Virtualized System	1076
W	1082
Wait Chain	1082
C++11, Condition Variable	1082
CLR Monitors	1085
Critical Sections	1086

Executive Resources	1089
General	1092
Comments	1096
LPC/ALPC	1097
Modules	1103
Comments	1103
Mutex Objects	1104
Named Pipes	1106
Nonstandard Synchronization	1108
Process Objects	1111
Pushlocks	1116
RPC	1118
RTL_RESOURCE	1122
Thread Objects	1128
Window Messaging	1132
Waiting Thread Time	1137
Kernel Dumps	1137
Comments	1142
User Dumps	1144
Comments	1145
Well-Tested Function	1146
Well-Tested Module	1147
Wild Code	1148
Comments	1149

Wild Pointer	1151
Comments	1152
Window Hint	1153
Y	1156
Young System	1156
Comments	1157
Z	1158
Zombie Processes	1158
Comments	1164
Bibliography	1165
Appendix A	1166
Reference Stack Traces	1166
Appendix B	1167
.NET / CLR / Managed Space Patterns	1167
Contention Patterns	1168
Deadlock and Livelock Patterns	1169
DLL Link Patterns	1170
Dynamic Memory Corruption Patterns	1171
Executive Resource Patterns	1172
Exception Patterns	1173
Falsity and Coincidence Patterns	1174
Hooksware Patterns	1175

Memory Consumption Patterns	1177
Meta-Memory Dump Patterns	1178
Module Patterns	1179
Optimization Patterns	1180
Process Patterns	1181
RPC, LPC and ALPC Patterns	1182
Stack Overflow Patterns	1183
Stack Trace Patterns	1184
Symbol Patterns	1186
Thread Patterns	1187
Wait Chain Patterns	1188
Appendix C	1189
Crash Dump Analysis Checklist	1189
Index	1192