Encyclopedia of Crash Dump Analysis Patterns
Detecting Abnormal Software Structure and Behavior in Computer Memory

Third Edition

Dmitry Vostokov
Software Diagnostics Institute
Encyclopedia of Crash Dump Analysis Patterns
Third Edition

Detecting Abnormal Software Structure and Behavior in Computer Memory

Dmitry Vostokov
Software Diagnostics Institute

OpenTask
<table>
<thead>
<tr>
<th>Summary of Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary of Contents</td>
</tr>
<tr>
<td>Detailed Table of Contents</td>
</tr>
<tr>
<td>Preface to the Third Edition</td>
</tr>
<tr>
<td>Preface to the Second Edition</td>
</tr>
<tr>
<td>Preface to the First Edition</td>
</tr>
<tr>
<td>Acknowledgements</td>
</tr>
<tr>
<td>About the Author</td>
</tr>
<tr>
<td><strong>A</strong></td>
</tr>
<tr>
<td>Abridged Dump</td>
</tr>
<tr>
<td>Accidental Lock</td>
</tr>
<tr>
<td>Activation Context</td>
</tr>
<tr>
<td>Active Space</td>
</tr>
<tr>
<td>Active Thread</td>
</tr>
<tr>
<td>Activity Resonance</td>
</tr>
<tr>
<td>Affine Thread</td>
</tr>
<tr>
<td>Aggregate Snapshot</td>
</tr>
<tr>
<td>Aggregated Frames</td>
</tr>
<tr>
<td>Anchor Region</td>
</tr>
<tr>
<td>Annotated Disassembly</td>
</tr>
<tr>
<td><strong>B</strong></td>
</tr>
<tr>
<td>Blocked DPC</td>
</tr>
<tr>
<td>Term</td>
</tr>
<tr>
<td>-------------------------------</td>
</tr>
<tr>
<td>Blocked Queue</td>
</tr>
<tr>
<td>Blocked Thread</td>
</tr>
<tr>
<td>Blocking File</td>
</tr>
<tr>
<td>Blocking Module</td>
</tr>
<tr>
<td>Broken Link</td>
</tr>
<tr>
<td>Busy System</td>
</tr>
<tr>
<td>C</td>
</tr>
<tr>
<td>C++ Exception</td>
</tr>
<tr>
<td>Caller-n-Callee</td>
</tr>
<tr>
<td>Changed Environment</td>
</tr>
<tr>
<td>Clone Dump</td>
</tr>
<tr>
<td>Cloud Environment</td>
</tr>
<tr>
<td>CLR Thread</td>
</tr>
<tr>
<td>Coincidental Error Code</td>
</tr>
<tr>
<td>Coincidental Frames</td>
</tr>
<tr>
<td>Coincidental Symbolic Information</td>
</tr>
<tr>
<td>Constant Subtrace</td>
</tr>
<tr>
<td>Context Pointer</td>
</tr>
<tr>
<td>Corrupt Dump</td>
</tr>
<tr>
<td>Corrupt Structure</td>
</tr>
<tr>
<td>Coupled Machines</td>
</tr>
<tr>
<td>Coupled Modules</td>
</tr>
</tbody>
</table>
Coupled Processes
Crash Signature
Crash Signature Invariant
Crashed Process
Critical Region
Critical Section Corruption
Critical Stack Trace
Custom Exception Handler

Data Alignment
Data Contents Locality
Data Correlation
Deadlock
Debugger Bug
Debugger Omission
Design Value
Deviant Module
Deviant Token
Diachronic Module
Dialog Box
Directing Module
Disassembly Ambiguity
<table>
<thead>
<tr>
<th>Issue Type</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disconnected Network Adapter</td>
<td>257</td>
</tr>
<tr>
<td>Disk Packet Buildup</td>
<td>259</td>
</tr>
<tr>
<td>Dispatch Level Spin</td>
<td>262</td>
</tr>
<tr>
<td>Distributed Exception</td>
<td>265</td>
</tr>
<tr>
<td>Distributed Spike</td>
<td>267</td>
</tr>
<tr>
<td>Distributed Wait Chain</td>
<td>275</td>
</tr>
<tr>
<td>Divide by Zero</td>
<td>277</td>
</tr>
<tr>
<td>Double Free</td>
<td>282</td>
</tr>
<tr>
<td>Double IRP Completion</td>
<td>302</td>
</tr>
<tr>
<td>Driver Device Collection</td>
<td>303</td>
</tr>
<tr>
<td>Dry Weight</td>
<td>304</td>
</tr>
<tr>
<td>Dual Stack Trace</td>
<td>305</td>
</tr>
<tr>
<td>Duplicate Extension</td>
<td>306</td>
</tr>
<tr>
<td>Duplicated Module</td>
<td>310</td>
</tr>
<tr>
<td>Dynamic Memory Corruption</td>
<td>315</td>
</tr>
<tr>
<td>Early Crash Dump</td>
<td>335</td>
</tr>
<tr>
<td>Effect Component</td>
<td>338</td>
</tr>
<tr>
<td>Embedded Comments</td>
<td>343</td>
</tr>
<tr>
<td>Empty Stack Trace</td>
<td>344</td>
</tr>
<tr>
<td>Environment Hint</td>
<td>347</td>
</tr>
<tr>
<td>Error Reporting Fault</td>
<td>348</td>
</tr>
</tbody>
</table>
Evental Dumps
Exception Module
Exception Reporting Thread
Exception Stack Trace
Execution Residue

Fake Module
False Effective Address
False Frame
False Function Parameters
False Memory
False Positive Dump
Fat Process Dump
Fault Context
First Fault Stack Trace
Foreign Module Frame
FPU Exception
Frame Pointer Omission
Frame Regularity
Frame Trace
Frozen Process
<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ghost Thread</td>
<td>459</td>
</tr>
<tr>
<td>Glued Stack Trace</td>
<td>461</td>
</tr>
<tr>
<td>Handle Leak</td>
<td>464</td>
</tr>
<tr>
<td>Handle Limit</td>
<td>466</td>
</tr>
<tr>
<td>Handled Exception</td>
<td>477</td>
</tr>
<tr>
<td>Hardware Activity</td>
<td>486</td>
</tr>
<tr>
<td>Hardware Error</td>
<td>490</td>
</tr>
<tr>
<td>Hidden Call</td>
<td>499</td>
</tr>
<tr>
<td>Hidden Exception</td>
<td>504</td>
</tr>
<tr>
<td>Hidden IRP</td>
<td>514</td>
</tr>
<tr>
<td>Hidden Module</td>
<td>515</td>
</tr>
<tr>
<td>Hidden Parameter</td>
<td>517</td>
</tr>
<tr>
<td>Hidden Process</td>
<td>519</td>
</tr>
<tr>
<td>Hidden Stack</td>
<td>521</td>
</tr>
<tr>
<td>Hidden Stack Trace</td>
<td>524</td>
</tr>
<tr>
<td>High Contention</td>
<td>527</td>
</tr>
<tr>
<td>Historical Information</td>
<td>543</td>
</tr>
<tr>
<td>Hooked Functions</td>
<td>544</td>
</tr>
<tr>
<td>Hooked Modules</td>
<td>550</td>
</tr>
<tr>
<td>Hooking Level</td>
<td>552</td>
</tr>
<tr>
<td>Hyperdump</td>
<td>555</td>
</tr>
</tbody>
</table>
I

Incomplete Stack Trace
Inconsistent Dump
Incorrect Stack Trace
Incorrect Symbolic Information
Injected Symbols
Inline Function Optimization
Instrumentation Information
Instrumentation Side Effect
Insufficient Memory
Internal Stack Trace
Interrupt Stack
Invalid Exception Information
Invalid Handle
Invalid Parameter
Invalid Pointer

J

JIT Code

L

Last Error Collection
Last Object
<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Late Crash Dump</td>
<td>677</td>
</tr>
<tr>
<td>Lateral Damage</td>
<td>678</td>
</tr>
<tr>
<td>Least Common Frame</td>
<td>684</td>
</tr>
<tr>
<td>Livelock</td>
<td>686</td>
</tr>
<tr>
<td>Local Buffer Overflow</td>
<td>688</td>
</tr>
<tr>
<td>Lost Opportunity</td>
<td>692</td>
</tr>
<tr>
<td>Main Thread</td>
<td>694</td>
</tr>
<tr>
<td>Managed Code Exception</td>
<td>697</td>
</tr>
<tr>
<td>Managed Stack Trace</td>
<td>704</td>
</tr>
<tr>
<td>Manual Dump</td>
<td>705</td>
</tr>
<tr>
<td>Memory Fibration</td>
<td>714</td>
</tr>
<tr>
<td>Memory Fluctuation</td>
<td>715</td>
</tr>
<tr>
<td>Memory Hierarchy</td>
<td>717</td>
</tr>
<tr>
<td>Memory Leak</td>
<td>718</td>
</tr>
<tr>
<td>Memory Region</td>
<td>743</td>
</tr>
<tr>
<td>Memory Snapshot</td>
<td>744</td>
</tr>
<tr>
<td>Message Box</td>
<td>745</td>
</tr>
<tr>
<td>Message Hooks</td>
<td>748</td>
</tr>
<tr>
<td>Mirror Dump Set</td>
<td>751</td>
</tr>
<tr>
<td>Missing Component</td>
<td>753</td>
</tr>
<tr>
<td>Missing Process</td>
<td>767</td>
</tr>
</tbody>
</table>
Missing Thread 768
Mixed Exception 773
Module Collection 778
Module Hint 781
Module Product Process 783
Module Stack Trace 784
Module Variable 786
Module Variety 788
Multiple Exceptions 791

Namespace 807
Nested Exceptions 808
Nested Offender 815
Network Packet Buildup 818
No Component Symbols 819
No Current Thread 822
No Data Types 824
No Process Dumps 826
No System Dumps 827
Not My Thread 828
Not My Version 829
NULL Pointer 831
Object Distribution Anomaly
OMAP Code Optimization
One-Thread Process
Optimized Code
Optimized VM Layout
Origin Module
Out-of-Module Pointer
Overaged System
Packed Code
Paged Out Data
Parameter Flow
Paratext
Pass Through Function
Passive System Thread
Passive Thread
Past Stack Trace
Patched Code
Pervasive System
Place Trace
Platform-Specific Debugger
Relative Memory Leak 935
RIP Stack Trace 938
Rough Stack Trace 940
Same Vendor 943
Screwbolt Wait Chain 944
Self-Diagnosis 945
Self-Dump 953
Semantic Split 955
Semantic Structure 962
Shared Buffer Overwrite 966
Shared Structure 974
Small Value 975
Snapshot Collection 977
Software Exception 978
Source Stack Trace 980
Special Process 981
Special Stack Trace 986
Special Thread 987
Spike Interval 988
Spiking Thread 989
Stack Overflow 999
<table>
<thead>
<tr>
<th>Stack Trace</th>
<th>1024</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack Trace Change</td>
<td>1041</td>
</tr>
<tr>
<td>Stack Trace Collection</td>
<td>1042</td>
</tr>
<tr>
<td>Stack Trace Motif</td>
<td>1061</td>
</tr>
<tr>
<td>Stack Trace Race</td>
<td>1062</td>
</tr>
<tr>
<td>Stack Trace Set</td>
<td>1064</td>
</tr>
<tr>
<td>Stack Trace Signature</td>
<td>1067</td>
</tr>
<tr>
<td>Stack Trace Surface</td>
<td>1069</td>
</tr>
<tr>
<td>Step Dumps</td>
<td>1070</td>
</tr>
<tr>
<td>Stored Exception</td>
<td>1071</td>
</tr>
<tr>
<td>String Hint</td>
<td>1072</td>
</tr>
<tr>
<td>String Parameter</td>
<td>1074</td>
</tr>
<tr>
<td>Subsystem Modules</td>
<td>1076</td>
</tr>
<tr>
<td>Suspended Thread</td>
<td>1077</td>
</tr>
<tr>
<td>Swarm of Shared Locks</td>
<td>1079</td>
</tr>
<tr>
<td>System Call</td>
<td>1084</td>
</tr>
<tr>
<td>System Object</td>
<td>1086</td>
</tr>
<tr>
<td>Tampered Dump</td>
<td>1089</td>
</tr>
<tr>
<td>Technology-Specific Subtrace</td>
<td>1102</td>
</tr>
<tr>
<td>Template Module</td>
<td>1112</td>
</tr>
<tr>
<td>Thread Age</td>
<td>1116</td>
</tr>
</tbody>
</table>
Thread Cluster
Thread Poset
Thread Starvation
Top Module
Translated Exception
Truncated Dump
Truncated Stack Trace
Ubiquitous Component
Unified Stack Trace
Unknown Component
Unloaded Module
Unrecognizable Symbolic Information
Unsynchronized Dumps
User Space Evidence
Value Adding Process
Value Deviation
Value References
Variable Subtrace
Version-Specific Extension
Virtualized Process
Virtualized System

W

Wait Chain

Waiting Thread Time

Well-Tested Function

Well-Tested Module

Wild Code

Wild Pointer

Window Hint

Y

Young System

Z

Zombie Processes

Bibliography

Appendix A

Reference Stack Traces

Appendix B

.NET / CLR / Managed Space Patterns

Contention Patterns

Deadlock and Livelock Patterns

DLL Link Patterns

Dynamic Memory Corruption Patterns
<table>
<thead>
<tr>
<th>Pattern Name</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Resource Patterns</td>
<td>1292</td>
</tr>
<tr>
<td>Exception Patterns</td>
<td>1293</td>
</tr>
<tr>
<td>Falsity and Coincidence Patterns</td>
<td>1294</td>
</tr>
<tr>
<td>Frame Patterns</td>
<td>1295</td>
</tr>
<tr>
<td>Hidden Artifact Patterns</td>
<td>1296</td>
</tr>
<tr>
<td>Hookware Patterns</td>
<td>1297</td>
</tr>
<tr>
<td>Memory Consumption Patterns</td>
<td>1299</td>
</tr>
<tr>
<td>Meta-Memory Dump Patterns</td>
<td>1300</td>
</tr>
<tr>
<td>Module Patterns</td>
<td>1301</td>
</tr>
<tr>
<td>Optimization Patterns</td>
<td>1302</td>
</tr>
<tr>
<td>Pointer Patterns</td>
<td>1303</td>
</tr>
<tr>
<td>Process Patterns</td>
<td>1304</td>
</tr>
<tr>
<td>RPC, LPC and ALPC Patterns</td>
<td>1305</td>
</tr>
<tr>
<td>Stack Overflow Patterns</td>
<td>1306</td>
</tr>
<tr>
<td>Stack Trace Patterns</td>
<td>1307</td>
</tr>
<tr>
<td>Structural Memory Patterns</td>
<td>1309</td>
</tr>
<tr>
<td>Symbol Patterns</td>
<td>1310</td>
</tr>
<tr>
<td>Thread Patterns</td>
<td>1311</td>
</tr>
<tr>
<td>Wait Chain Patterns</td>
<td>1313</td>
</tr>
</tbody>
</table>

**Appendix C**

Crash Dump Analysis Checklist 1314

Index 1317
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary of Contents</td>
<td>3</td>
</tr>
<tr>
<td>Detailed Table of Contents</td>
<td>20</td>
</tr>
<tr>
<td>Preface to the Third Edition</td>
<td>50</td>
</tr>
<tr>
<td>Preface to the Second Edition</td>
<td>51</td>
</tr>
<tr>
<td>Preface to the First Edition</td>
<td>52</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>53</td>
</tr>
<tr>
<td>About the Author</td>
<td>54</td>
</tr>
<tr>
<td>A</td>
<td>55</td>
</tr>
<tr>
<td>Abridged Dump</td>
<td>55</td>
</tr>
<tr>
<td>Accidental Lock</td>
<td>59</td>
</tr>
<tr>
<td>Activation Context</td>
<td>66</td>
</tr>
<tr>
<td>Active Space</td>
<td>69</td>
</tr>
<tr>
<td>Active Thread</td>
<td>71</td>
</tr>
<tr>
<td>Linux</td>
<td>71</td>
</tr>
<tr>
<td>Mac OS X</td>
<td>72</td>
</tr>
<tr>
<td>Windows</td>
<td>74</td>
</tr>
<tr>
<td>Activity Resonance</td>
<td>78</td>
</tr>
<tr>
<td>Affine Thread</td>
<td>80</td>
</tr>
<tr>
<td>Aggregate Snapshot</td>
<td>83</td>
</tr>
<tr>
<td>Aggregated Frames</td>
<td>84</td>
</tr>
<tr>
<td>Anchor Region</td>
<td>85</td>
</tr>
</tbody>
</table>
Annotated Disassembly 86

JIT .NET Code 86

B 87

Blocked DPC 87

Blocked Queue 88

LPC/ALPC 88

Comments 90

Blocked Thread 91

Hardware 91

Software 93

Comments 101

Timeout 103

Blocking File 104

Blocking Module 107

Comments 107

Broken Link 108

Busy System 110

C 119

C++ Exception 119

Linux 119

Mac OS X 120

Windows 121

Comments 121
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caller-n-Callee</td>
<td>122</td>
</tr>
<tr>
<td>Changed Environment</td>
<td>125</td>
</tr>
<tr>
<td>Comments</td>
<td>128</td>
</tr>
<tr>
<td>Clone Dump</td>
<td>129</td>
</tr>
<tr>
<td>Cloud Environment</td>
<td>133</td>
</tr>
<tr>
<td>CLR Thread</td>
<td>135</td>
</tr>
<tr>
<td>Comments</td>
<td>138</td>
</tr>
<tr>
<td>Coincidental Error Code</td>
<td>139</td>
</tr>
<tr>
<td>Coincidental Frames</td>
<td>141</td>
</tr>
<tr>
<td>Comments</td>
<td>144</td>
</tr>
<tr>
<td>Coincidental Symbolic Information</td>
<td>145</td>
</tr>
<tr>
<td>Linux</td>
<td>145</td>
</tr>
<tr>
<td>Mac OS X</td>
<td>146</td>
</tr>
<tr>
<td>Windows</td>
<td>148</td>
</tr>
<tr>
<td>Comments</td>
<td>152</td>
</tr>
<tr>
<td>Constant Subtrace</td>
<td>153</td>
</tr>
<tr>
<td>Context Pointer</td>
<td>154</td>
</tr>
<tr>
<td>Corrupt Dump</td>
<td>155</td>
</tr>
<tr>
<td>Comments</td>
<td>156</td>
</tr>
<tr>
<td>Corrupt Structure</td>
<td>157</td>
</tr>
<tr>
<td>Coupled Machines</td>
<td>159</td>
</tr>
<tr>
<td>Coupled Modules</td>
<td>160</td>
</tr>
</tbody>
</table>
Disassembly Ambiguity 256
Disconnected Network Adapter 257
Disk Packet Buildup 259
  Comments 261
Dispatch Level Spin 262
Distributed Exception 265
  Managed Code 265
Distributed Spike 267
  Comments 274
Distributed Wait Chain 275
Divide by Zero 277
  Kernel Mode 277
  User Mode 279
    Linux 279
    Mac OS X 280
    Windows 281
Double Free 282
  Kernel Pool 282
    Comments 284
  Process Heap 289
    Windows 289
    Comments 298
  Mac OS X 301
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Double IRP Completion</td>
<td>302</td>
</tr>
<tr>
<td>Driver Device Collection</td>
<td>303</td>
</tr>
<tr>
<td>Dry Weight</td>
<td>304</td>
</tr>
<tr>
<td>Dual Stack Trace</td>
<td>305</td>
</tr>
<tr>
<td>Duplicate Extension</td>
<td>306</td>
</tr>
<tr>
<td>Comments</td>
<td>309</td>
</tr>
<tr>
<td>Duplicated Module</td>
<td>310</td>
</tr>
<tr>
<td>Comments</td>
<td>314</td>
</tr>
<tr>
<td>Dynamic Memory Corruption</td>
<td>315</td>
</tr>
<tr>
<td>Kernel Pool</td>
<td>315</td>
</tr>
<tr>
<td>Comments</td>
<td>320</td>
</tr>
<tr>
<td>Managed Heap</td>
<td>324</td>
</tr>
<tr>
<td>Process Heap</td>
<td>327</td>
</tr>
<tr>
<td>Linux</td>
<td>327</td>
</tr>
<tr>
<td>Mac OS X</td>
<td>328</td>
</tr>
<tr>
<td>Windows</td>
<td>330</td>
</tr>
<tr>
<td>Comments</td>
<td>331</td>
</tr>
<tr>
<td><strong>E</strong></td>
<td>335</td>
</tr>
<tr>
<td>Early Crash Dump</td>
<td>335</td>
</tr>
<tr>
<td>Effect Component</td>
<td>338</td>
</tr>
<tr>
<td>Embedded Comments</td>
<td>343</td>
</tr>
<tr>
<td>Empty Stack Trace</td>
<td>344</td>
</tr>
<tr>
<td>Comments</td>
<td>346</td>
</tr>
</tbody>
</table>
Environment Hint 347
   Comments 347
Error Reporting Fault 348
Evental Dumps 351
Exception Module 384
Exception Reporting Thread 386
Exception Stack Trace 387
   Comments 388
Execution Residue 389
   Linux 389
   Mac OS X 391
   Windows 393
      Managed Space 393
         Comments 394
      Unmanaged Space 395
         Comments 407
     F 409
      Fake Module 409
      False Effective Address 413
      False Frame 414
      False Function Parameters 416
      False Memory 419
      False Positive Dump 428
Fat Process Dump
Fault Context
First Fault Stack Trace
Foreign Module Frame
FPU Exception
Frame Pointer Omission
Frame Regularity
Frame Trace
Frozen Process
Ghost Thread
Glued Stack Trace
Handle Leak
Comments
Handle Limit
GDI
Kernel Space
User Space
Handled Exception
.NET CLR
Comments
Critical Sections 535
Executive Resources 537
 Comments 539
 Processors 540
 Historical Information 543
 Comments 543
 Hooked Functions 544
 Kernel Space 544
 Comments 547
 User Space 548
 Comments 549
 Hooked Modules 550
 Comments 551
 Hooking Level 552
 Hyperdump 555
 Incomplete Stack Trace 559
 GDB 559
 Incomplete Session 560
 Comments 561
 Inconsistent Dump 562
 Comments 562
 Incorrect Stack Trace 563
Comments

Incorrect Symbolic Information

Injected Symbols

Inline Function Optimization

Managed Code

Unmanaged Code

Instrumentation Information

Instrumentation Side Effect

Comments

Insufficient Memory

Committed Memory

Control Blocks

Handle Leak

Comments

Kernel Pool

Comments

Module Fragmentation

Comments

Physical Memory

PTE

Comments

Region

Reserved Virtual Memory

Session Pool
Stack 627
Stack Trace Database 633
Internal Stack Trace 638
Interrupt Stack 640
Invalid Exception Information 642
Invalid Handle 646
General 646
Comments 649
Managed Space 650
Comments 657
Invalid Parameter 658
Process Heap 658
Runtime Function 661
Invalid Pointer 663
General 663
Objects 665

J 667

JIT Code 667
.NET 667
Comments 669
Java 670

L 672

LastError Collection 672
Kernel 705
Comments 706
Process 710
Comments 713
Memory Fibration 714
Memory Fluctuation 715
Process Heap 715
Comments 716
Memory Hierarchy 717
Memory Leak 718
.NET Heap 718
Comments 724
I/O Completion Packets 725
Page Tables 726
Process Heap 732
Comments 738
Regions 740
Memory Region 743
Memory Snapshot 744
Message Box 745
Comments 747
Message Hooks 748
Comments 750
Module Variety 788
Multiple Exceptions 791
  Mac OS X 791
  Windows 793
    Kernel Mode 793
    Managed Space 798
    Stowed 799
    User Mode 805

N 807
  Namespace 807
  Nested Exceptions 808
    Managed Code 808
      Comments 810
      Unmanaged Code 811
    Nested Offender 815
  Network Packet Buildup 818
  No Component Symbols 819
  No Current Thread 822
  No Data Types 824
    Comments 825
  No Process Dumps 826
  No System Dumps 827
    Comments 827
Not My Thread
Not My Version
Hardware
Software
NULL Pointer
Linux
Code
Data
Mac OS X
Code
Data
Windows
Code
Comments
Data
Comments
Object Distribution Anomaly
.NET Heap
IRP
Comment
OMAP Code Optimization
Comments
One-Thread Process
Optimized Code 853

Comments 854

Optimized VM Layout 855

Origin Module 857

Comments 858

Out-of-Module Pointer 859

Overaged System 860

Comments 860

P 861

Packed Code 861

Paged Out Data 864

Parameter Flow 866

Paratext 869

Linux 869

Mac OS X 871

Comments 872

Pass Through Function 873

Comments 874

Passive System Thread 875

Kernel Space 875

Passive Thread 879

User Space 879
Spiking Thread

Linux

Mac OS X

Windows

Comments

Stack Overflow

Linux

Mac OS X

Windows

Kernel Mode

Comments

Insufficient Memory

Software Implementation

User Mode

Comments

Stack Trace

Linux

Mac OS X

Windows

Database

File System Filters

General

I/O Devices

I/O Request
Stack Trace Change 1041
Stack Trace Collection 1042
CPUs 1042
  Comments 1044
I/O Requests 1045
Managed Space 1049
Predicate 1052
  Comments 1052
Unmanaged Space 1053
  Comments 1060
Stack Trace Motif 1061
Stack Trace Race 1062
Stack Trace Set 1064
Stack Trace Signature 1067
Stack Trace Surface 1069
Step Dumps 1070
Stored Exception 1071
String Hint 1072
String Parameter 1074
Subsystem Modules 1076
Suspended Thread 1077
  Comments 1078
Swarm of Shared Locks 1079
System Call

Comments

System Object

Tampered Dump

Technology-Specific Subtrace

COM Client Call

COM Interface Invocation

Comments

Dynamic Memory

JIT .NET Code

Template Module

Thread Age

Thread Cluster

Thread Poset

Thread Starvation

Normal Priority

Realtime Priority

Top Module

Translated Exception

Truncated Dump

Mac OS X

Windows
Truncated Stack Trace

Comments

U

Ubiquitous Component

Kernel Space

User Space

Unified Stack Trace

Unknown Component

Unloaded Module

Comments

Unrecognizable Symbolic Information

Unsynchronized Dumps

User Space Evidence

V

Value Adding Process

Value Deviation

Stack Trace

Structure Field

Value References

Comments

Variable Subtrace

Version-Specific Extension
Virtualized Process

WOW64

Comments

Virtualized System

Wait Chain

C++11, Condition Variable

CLR Monitors

Comments

Critical Sections

Executive Resources

General

Comments

LPC/ALPC

Modules

Comments

Mutex Objects

Named Pipes

Nonstandard Synchronization

Process Objects

Pushlocks

RPC

RTL_Resource

SRW Lock

Thread Objects
Window Messaging

Waiting Thread Time

Kernel Dumps

Comments

User Dumps

Comments

Well-Tested Function

Well-Tested Module

Wild Code

Comments

Wild Pointer

Comments

Window Hint

Y

Young System

Comments

Z

Zombie Processes

Comments

Bibliography

Appendix A

Reference Stack Traces
Appendix B

.NET / CLR / Managed Space Patterns

Contention Patterns

Deadlock and Livelock Patterns

DLL Link Patterns

Dynamic Memory Corruption Patterns

Executive Resource Patterns

Exception Patterns

Falsity and Coincidence Patterns

Frame Patterns

Hidden Artifact Patterns

Hookware Patterns

Memory Consumption Patterns

Meta-Memory Dump Patterns

Module Patterns

Optimization Patterns

Pointer Patterns

Process Patterns

RPC, LPC and ALPC Patterns

Stack Overflow Patterns

Stack Trace Patterns

Structural Memory Patterns
Symbol Patterns 1310
Thread Patterns 1311
Wait Chain Patterns 1313

Appendix C 1314

Crash Dump Analysis Checklist 1314

Index 1317