Memory Dump Analysis Anthology

Volume 7

Dmitry Vostokov
Software Diagnostics Institute

OpenTask

Published by OpenTask, Republic of Ireland

Copyright © 2014 by Dmitry Vostokov

Copyright © 2014 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: 978-1-908043-51-1 (Paperback)

ISBN-13: 978-1-908043-52-8 (Hardback)

First printing, 2014

Revision 2 (July 2015)

Summary of Contents

Preface 23

Acknowledgements 25

PART 1: Professional Crash Dump Analysis and Debugging 27

PART 2: Crash Dump Analysis Patterns 65

PART 3: Core Dump Analysis Patterns (Mac OS X) 201

PART 4: Malware Analysis Patterns 239

PART 5: A Bit of Science and Philosophy 259

PART 6: Software Trace Analysis Patterns 279

PART 7: Fun with Crash Dumps 355

PART 8: Software Narratology 383

PART 9: Software Diagnostics, Troubleshooting, and Debugging 399

PART 10: Art and Visualization 451

PART 11: Miscellaneous 497

Appendix 505

Index of WinDbg Commands 519

About the Author 521

Notes 522

Cover Images 523

```
0:007> !address

Mapping file section regions...
Mapping parts regions...
Mapping page regions...
Mapping appendix regions...
Mapping WinDbg commands regions...

    BaseAddress     EndAddress+1        RegionSize     Protect
------------------------------------------------------------------------
    0`00000000      0`0020B000          0`0020B000     PAGE_EXECUTE_READ


0:007> !address -summary

--- Usage Summary ---------------- RgnCount %ofTotal
crash dump analysis patterns             66   24.44%
log and trace analysis patterns          48   17.77%
core dump analysis patterns              18    6.66%
malware analysis patterns                10    3.70%
other patterns                            7    2.59%
and more                                120   44.84%

7: kd> !memusage
 loading PFN database
loading (100% complete)
Compiling memory usage data (99% Complete).
        Crash dump analysis patterns:  135
     Trace and log analysis patterns:   75
         Core dump analysis patterns:   38
           Malware analysis patterns:   20
  Software diagnostics and debugging:   90
                Software narratology:   16
                          Philosophy:   20
                                 Art:   45
                                 Fun:   30
                          Transition:   36
                                Zero:   18
                             Unknown:    0
                               TOTAL:  523
```

Contents

Preface 23

Acknowledgements.. 25

PART 1: Professional Crash Dump Analysis and Debugging.. 27

WinDbg Shortcuts 27

.ecxr.. 27

!heap -x -v 29

!sw and !k.. 31

Two WinDbg Scripts That Changed the World.. 32

Raw Stack Dump of All Threads (Kernel Space) 37

The Design of Memory Dump Analysis: 7 Steps of Highly Successful Analysts........... 38

Postmortem Effects of -g 39

Event Owners.. 42

Improbable Occurrence 48

Pattern Cooperation 49

Page Heap Implementation 54

More Common Mistakes in Memory Analysis 60

Memory Dump Analysis Best Practices.. 63

PART 2: Crash Dump Analysis Patterns.. 65

FPU Exception 65

Hidden Parameter 67

Memory Leak (Page Tables) 69

Unrecognizable Symbolic Information 76

Network Packet Buildup 82

Disconnected Network Adapter 83

Problem Module 85

Empty Stack Trace 86

Debugger Bug 90

Value References 92

Self-Diagnosis (Registry) 93

System Object 95

Module Variable 98

Stack Trace Collection (Predicate) 100

Stack Trace Collection (I/O Requests) 101

Regular Data 106

Translated Exception 107

Blocked DPC 108

Late Crash Dump 109

Blocked Thread (Timeout) 110

Punctuated Memory Leak 111

Insufficient Memory (Reserved Virtual Memory) 114

Coincidental Error Code 117

Stored Exception 119

Activity Resonance 120

Value Adding Process 122

Memory Leak (I/O Completion Packets) 123

No Current Thread 124

Unloaded Module 126

Stack Trace Change 131

Spike Interval 132

Deviant Module 133

Hidden Exception (Kernel Space) 140

Handled Exception (Kernel Space) 141

High Contention (.NET CLR Monitors) 142

Frozen Process 145

Incomplete Session 150

Error Reporting Fault 152

First Fault Stack Trace 155

Hidden Process 156

Disk Packet Buildup 158

Deviant Token 161

Module Collection 162

Handle Leak 164

Critical Stack Trace 165

Debugger Omission 166

Broken Link 168

Wait Chain (Pushlocks) 170

Insufficient Memory (Session Pool) 172

Step Dumps 173

Reduced Symbolic Information 174

Injected Symbols 175

Glued Stack Trace 178

Distributed Wait Chain 182

Ubiquitous Component (Kernel Space) 184

One-Thread Process 187

Module Product Process 189

Crash Signature Invariant 190

Small Values 191

Shared Structure 193

Wait Chain (CLR Monitors) 194

Thread Cluster 195

Module Collection (Predicate) 196

False Effective Address 197

Screwbolt Wait Chain 198

PART 3: Core Dump Analysis Patterns (Mac OS X) 201

GDB for WinDbg Users 201

Stack Trace 203

GDB Annoyances: Incomplete Stack Trace 205

NULL Pointer (Data) 206

Shared Buffer Overwrite 207

Multiple Exceptions 211

Double Free (Process Heap) 213

Dynamic Memory Corruption (Process Heap) 214

Spiking Thread 216

NULL Pointer (Code) 218

Execution Residue 220

Coincidental Symbolic Information 223

Paratext 225

Truncated Dump 227

C++ Exception 228

Local Buffer Overflow 229

Divide by Zero (User Mode) 231

Stack Overflow (User Mode) 232

Active Thread 236

PART 4: Malware Analysis Patterns 239

Malware: A Definition 239

Fake Module 240

RIP Stack Trace 244

Driver Device Collection 246

Pre-Obfuscation Residue 247

Packed Code 248

Raw Pointer 251

Out-of-Module Pointer 252

Patched Code 253

String Hint 254

Namespace 257

PART 5: A Bit of Science and Philosophy 259

On Matter 259

Commodities as Memories 260

Software as Means of Production 261

Notes on Memoidealism 262

The Confluence of Computers, Philosophy, and Religion 264

Analytic Memory Dump - A Mathematical Definition 265

Sorting and Early Greek Philosophers 266

General Abnormal Patterns of Structure and Behavior 267

On Matter and Substances 268

M-Memory 269

Ontology of Memoidealism 270

Philosophies of Persistence 273

Information as Arrow 275

Dialectical Triad in Memoidealism 276

PART 6: Software Trace Analysis Patterns 279

Software Trace Diagrams (STDiagrams) 279

Macrofunction 283

Linked Messages 284

Marked Message 285

Trace Frames 286

Counter Value 288

Message Context 289

Error Distribution 290

Break-in Activity 291

Resume Activity 292

Fiber Bundle 294

Data Flow 296

Empty Trace 298

Error Message 299

Periodic Message Block 300

Visibility Limit 301

Relative Density 302

Sparse Trace 303

Opposition Messages 304

Split Trace 305

Message Interleave 306

Sheaf of Activities 307

Indexical Trace 310

Abnormal Value 311

Dominant Event Sequence 313

Pivot Message 314

Traces of Individuality 318

Indirect Facts 319

Hidden Error 320

Last Activity 322

State and Event 324

Dialogue 326

Motif 329

Exception Stack Trace (Java) 330

Correlated Discontinuity 332

Piecewise Activity 333

Density Distribution 335

Factor Group 336

Silent Messages 339

Shared Point 341

Meta Trace 343

Data Association 344

State Dump 346

Message Cover 347

Message Set 349

Error Thread 351

Activity Divergence 352

PART 7: Fun with Crash Dumps 355

Debugging Slang 355

LoL 355

Watching a Movie 356

PonOS 357

Typology, Typological 358

Memorandum 359

HELL 360

FBI 361

poo 362

STaMPs 363

A NoSQL Problem 364

Matrix 365

Fool 366

B2B, B2C, H2H 367

New Year Eve Debugging 368

Happy New Spiking Year of Software Trace Analysis 369

Happy New Year (from Windows 8) 370

Music for Debugging 372

Going Romantic 372

Make It through This Trace 373

Fiction for Debugging 374

The Problem and The Solution 374

Pilgrimage to Harvard University 375

Welcome to Ki* and Ke* 376

I Memory Dump 377

A Blue Screen Watch 379

Poetry 380

Surfaces in Nature 381

PART 8: Software Narratology 383

Software Anti-Narrative 383

Software Narratology Helps Fiction Writers 384

Narremes in Software Narratology 386

Narralog - A Software Trace Modeling Language 387

What is a Software Narrative? 388

Software Narrative Planes 389

Software Narratology Square 391

Writing and Validation of Historical Narratives 392

Software Trace Analysis Patterns Domain Hierarchy 393

Process Monitor as Modeling Tool 394

Generalized Software Narrative and Trace 395

Unified Computer Diagnostics: Incorporating Hardware Narratology 396

Introducing Software Narratology of Things (Software NT) 397

PART 9: Software Diagnostics, Troubleshooting, and Debugging................................. 399

Unified and Generative Debugging... 399

Analysis, Architectural, Design, Implementation and Usage Debugging Patterns 399

Software Problem Description Language... 401

What are Software Trace and Memory Dump Analysis? A One Sentence Definition402

Software Problem Solving Tools as a Service... 403

Software Problem Description Patterns 404

Software Behavior Pattern Prediction 405

Patterns of Software Diagnostics.. 406

First Fault 406

Highly Effective Diagnostics 407

Network Trace Analysis Patterns 408

Software Diagnostics Services... 411

Architecture of Process Memory Dump Capture Done Right 412

An Introduction to General Systems Thinking (Book Review) 413

Software Diagnostics Institute Logo 414

User Interface Problem Analysis Patterns.. 415

Unresponsive Window.. 415

Pattern-Based Software Diagnostics 418

Software Diagnostics Discipline 419

Architecture of memCPU 420

Phenomenology of Software Diagnostics: A First Sketch 421

Software Diagnostics Report Schemes 422

Missing Cause Trace 422

Software Diagnostics Training: Two Approaches 423

Software Disruption Patterns 425

Space Precondition 425

Static Code Analysis Patterns 426

Loop Construct 426

The Structure of Software Problem Solving Organization 427

Bridging the Great Divide 428

Elementary Software Diagnostics Patterns 429

Zero Fault Software Diagnostics 430

Agile Software Diagnostics 432

ADDR Pattern Catalogue 433

Thinking-Based Software Diagnostics 434

Memory Acquisition Pattern Catalog 436

Trace Acquisition Pattern Catalog 437

Patterns of Software Diagnostics Architecture 438

Detecting and Predicting the Unknown 440

Software Diagnostics Metaphors 442

Software Diagnostics as Psychology 442

Software Diagnostics as Literary Criticism 443

Rapid Software Diagnostics Process (RSDP) 444

Right First Time Software Diagnosis 445

Software Diagnosis Codes 446

Vulnerability Analysis Patterns (VAP) 447

Versioned Namespace 449

PART 10: Art and Visualization 451

2012 (Pessimistic) 451

2012 (Optimistic) 452

A Bug in a Bag (Collections, Ex-hi-bit 1) 453

A Bug Meets a Bug (The Clash of Civilizations) 454

A Bug Catcher 455

The Second Generation of CARE System (Trademark) 456

RawStackGram 457

A Memory Window 458

Liquid Memory 459

Computer Brain 460

Computer Evolution 461

M Spaces 462

Happy Hellowin! 463

Pointers in Nature 464

Drink Sensibly Before The End Of The World! 465

MM=DD=YY 466

Process Monitor Log Visualized 468

Holes Infinity (HI OS) 472

Cyber Vostok Missions 473

A Dump Machine 474

The Power of Simplicity 475

Happy St. Patrick's Screen 476

Happy New Year 2014! 477

I Love Software Diagnostics 478

Puree Windows Cooking 479

  Salad Winterminal 479

  Kernel Soup 481

  Neolithic Soup 482

  Food Subsystems 483

An Accident of Creation 484

So Chi Salad, 2014 485

Self-Organized Window-ed soup 486

Political Computicarts 487

Needs Non-Invasive Debugging! 487

Russian Spaces 488

The Day I Quit 489

Hero of Dump Analysis, a Medal for Labor Day 490

Diagnosed by Vostokov®™ 491

Stack Trace Shapes 492

The Art of Internals 494

Threadinking 495

PART 11: Miscellaneous 497

C and C++ Programming Books That Made a Great Impression on the Author 497

Outside 499

After Debugging 500

Crash Dumps, Acquisitions, and Layoffs 501

Cadaver Worm: An Exercise in Malware Fiction 502

WinDbg as UNICODE to ASCII Converter 504

Appendix 505

- Falsity and Coincidence Patterns 505
- Process Patterns 506
- Thread Patterns 507
- Optimization Patterns 508
- Exception Patterns 509
- Module Patterns 510
- RPC, LPC and ALPC Patterns and Case Studies 511
- ERESOURCE Patterns and Case Studies 513
- Meta-Memory Dump Patterns 515
- Crash Dump Analysis Checklist 516

Index of WinDbg Commands 519

About the Author 521

Notes 522

Cover Images 523