



Windows Memory Dump Analysis **Accelerated**

Version 5.0

Part 2: Kernel and Complete Spaces

Dmitry Vostokov
Software Diagnostics Services

Published by OpenTask, Republic of Ireland

Copyright © 2021 by OpenTask

Copyright © 2021 by Software Diagnostics Services

Copyright © 2021 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.

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

OpenTask books and magazines 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: 978-1-912636-08-2 (Paperback)

Revision 5.00 (October 2021)

Contents

| | |
|---|-----|
| About the Author..... | 5 |
| Presentation Slides and Transcript..... | 7 |
| Practice Exercises | 37 |
| Exercise 0: Download, setup and verify your WinDbg or WinDbg Preview installation | 42 |
| Exercise K1: Analysis of a normal kernel dump (64-bit)..... | 52 |
| Exercise K2: Analysis of a kernel dump with pool leak (64-bit)..... | 107 |
| Exercise K3: Analysis of a kernel dump with pool corruption (64-bit) | 122 |
| Exercise K4: Analysis of a kernel dump with code corruption (64-bit) | 128 |
| Exercise K5: Analysis of a kernel dump with hang I/O (64-bit) | 145 |
| Exercise K6: Analysis of a kernel dump with stack overflow (64-bit)..... | 165 |
| Exercise K7: Analysis of a kernel dump with stack overwrite (64-bit) | 179 |
| Exercise C1: Analysis of a normal complete dump (64-bit)..... | 196 |
| Exercise C2: Analysis of a problem complete dump (64-bit)..... | 216 |
| Exercise C3: Analysis of a problem complete dump (64-bit)..... | 248 |
| Exercise C4: Analysis of a problem complete dump (64-bit)..... | 261 |
| Application Source Code | 285 |
| AppA | 287 |
| AppB | 289 |
| AppC | 291 |
| AppE..... | 293 |
| AppK | 295 |
| Selected Q&A..... | 296 |
| Minidump Analysis | 320 |
| Scripts and WinDbg Commands | 320 |
| Component Identification | 323 |
| Raw Stack Data Analysis | 328 |
| Symbols and Images | 337 |
| Wait Chain (Executive Resources) | 340 |