



# Windows Memory Dump Analysis **Accelerated**

**Version 4.0**

Dmitry Vostokov  
Software Diagnostics Services

Published by OpenTask, Republic of Ireland

Copyright © 2016 by OpenTask

Copyright © 2016 by Software Diagnostics Services

Copyright © 2016 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.

You must not circulate this book in any other binding or cover, and you must impose the same condition on any acquirer.

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](mailto:press@opentask.com).

A CIP catalog record for this book is available from the British Library.

ISBN-13: 978-1-908043-46-7 (Paperback)

Version 4, 2016

## Contents

About the Author .....	7
Presentation Slides and Transcript .....	9
Practice Exercises .....	35
Exercise 0: Download, setup and verify your WinDbg installation .....	40
Exercise P1: Analysis of a normal application process dump (32-bit notepad) .....	47
Exercise P2: Analysis of a normal application process dump (64-bit notepad) .....	72
Exercise P3: Analysis of a normal application process dump (64-bit Microsoft Edge) .....	84
Exercise P4: Analysis of an application process dump (64-bit ApplicationK, no symbols).....	113
Exercise P5: Analysis of an application process dump (64-bit ApplicationK, with application symbols) .....	126
Exercise P6: Analysis of application process dump (ApplicationL, 32-bit).....	131
Exercise P7: Analysis of an application process dump (ApplicationL, 64-bit) .....	140
Exercise P8: Analysis of an application process dump (ApplicationM, 64-bit) .....	148
Exercise P9: Analysis of an application process dump (ApplicationN, 64-bit) .....	162
Exercise P10: Analysis of an application process dump (ApplicationO, 64-bit) .....	174
Exercise P11: Analysis of an application process dump (ApplicationP, 64-bit) .....	184
Exercise P12: Analysis of an application process dump (ApplicationR, 32-bit) .....	199
Exercise P13: Analysis of an application process dump (ApplicationA, 64-bit) .....	217
Exercise P14: Analysis of an application process dump (ApplicationS, 64-bit).....	225
Exercise P15: Analysis of an application process dump (notepad, 32-bit) .....	238
Exercise P16: Analysis of an application process dump (notepad, 64-bit) .....	242
Exercise P17: Analysis of an application process dump (ApplicationQ, 32-bit).....	249
Exercise K1: Analysis of a normal kernel dump (64-bit) .....	262
Exercise K2: Analysis of a kernel dump with pool leak (64-bit).....	308
Exercise K3: Analysis of a kernel dump with pool corruption (64-bit) .....	326
Exercise K4: Analysis of a kernel dump with code corruption (64-bit).....	335
Exercise K5: Analysis of a kernel dump with hang I/O (64-bit) .....	359
Exercise C1: Analysis of a normal complete dump (64-bit).....	379
Exercise C2: Analysis of a problem complete dump (64-bit).....	400
Exercise C3: Analysis of a problem complete dump (64-bit).....	424
Exercise C4: Analysis of a problem complete dump (64-bit).....	441
Exercise A1: Analysis of a problem active dump (64-bit) .....	463
Legacy Exercises .....	485
Exercise Legacy.0 .....	487

Exercise Legacy.P1: Analysis of a normal application process dump (32-bit notepad) .....	492
Exercise Legacy.P2: Analysis of a normal application process dump (64-bit notepad) .....	513
Exercise Legacy.P3: Analysis of a normal application process dump (32-bit IE).....	522
Exercise Legacy.P4: Analysis of an application process dump (32-bit ApplicationK, no symbols).....	537
Exercise Legacy.P5: Analysis of an application process dump (32-bit ApplicationK, with application symbols) .....	547
Exercise Legacy.P6: Analysis of application process dump (ApplicationL, 32-bit) .....	551
Exercise Legacy.P7: Analysis of an application process dump (ApplicationL, 64-bit) .....	558
Exercise Legacy.P8: Analysis of an application process dump (ApplicationM, 32-bit) .....	562
Exercise Legacy.P9: Analysis of an application process dump (ApplicationN, 64-bit) .....	572
Exercise Legacy.P10: Analysis of an application process dump (ApplicationO, 64-bit) .....	580
Exercise Legacy.P11: Analysis of an application process dump (ApplicationP, 32-bit).....	586
Exercise Legacy.P13: Analysis of an application process dump (ApplicationA, 32-bit) .....	597
Exercise Legacy.P14: Analysis of an application process dump (ApplicationS, 32-bit) .....	605
Exercise Legacy.P15: Analysis of an application process dump (notepad, 32-bit) .....	614
Exercise Legacy.P16: Analysis of an application process dump (notepad, 64-bit) .....	618
Exercise Legacy.P17: Analysis of an application process dump (ApplicationQ, 32-bit) .....	624
Exercise Legacy.K1: Analysis of a normal kernel dump (32-bit) .....	633
Exercise Legacy.K2: Analysis of a kernel dump with pool leak (32-bit) .....	670
Exercise Legacy.K3: Analysis of a kernel dump with pool corruption (32-bit).....	689
Exercise Legacy.K4: Analysis of a kernel dump with code corruption (32-bit) .....	701
Exercise Legacy.K5: Analysis of a kernel dump with hang I/O (32-bit).....	715
Exercise Legacy.C1: Analysis of a normal complete dump (32-bit) .....	728
Exercise Legacy.C2: Analysis of a problem complete dump (32-bit) .....	748
Application Source Code .....	783
ApplicationA .....	785
ApplicationB .....	787
ApplicationC .....	789
ApplicationE .....	791
ApplicationK .....	793
ApplicationL.....	794
ApplicationM .....	795
ApplicationN .....	796
ApplicationO.....	797
ApplicationP .....	798
ApplicationR .....	799

ApplicationS.....	800
ApplicationQ.....	801
Selected Q&A .....	805
Minidump Analysis .....	849
Scripts and WinDbg Commands .....	849
Component Identification.....	852
Raw Stack Data Analysis .....	857
Symbols and Images .....	866
Wait Chain (Executive Resources) .....	869