



# Windows Memory Dump Analysis **Accelerated**

Dmitry Vostokov  
Memory Dump Analysis Services

Published by OpenTask, Republic of Ireland

Copyright © 2011 by OpenTask

Copyright © 2011 by Memory Dump Analysis Services

Copyright © 2011 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 catalogue record for this book is available from the British Library.

ISBN-13: 978-1-908043-29-0 (Paperback)

First printing, 2011

## Contents

Presentation Slides and Transcript.....	5
Practice Exercises .....	27
Exercise 0: Download, setup and verify your WinDbg installation .....	31
Exercise P1: Analysis of a normal application process dump (32-bit notepad) .....	38
Exercise P2: Analysis of a normal application process dump (64-bit notepad) .....	57
Exercise P3: Analysis of a normal application process dump (32-bit IE) .....	75
Exercise P4: Analysis of an application process dump (ApplicationK, no symbols) .....	91
Exercise P5: Analysis of an application process dump (ApplicationK, with application symbols) .....	102
Exercise P6: Analysis of application process dump (ApplicationL, 32-bit) .....	108
Exercise P7: Analysis of an application process dump (ApplicationL, 64-bit) .....	115
Exercise P8: Analysis of an application process dump (ApplicationM, 32-bit).....	121
Exercise P9: Analysis of an application process dump (ApplicationN, 64-bit) .....	132
Exercise P10: Analysis of an application process dump (ApplicationO, 64-bit) .....	142
Exercise P11: Analysis of an application process dump (ApplicationP, 32-bit).....	149
Exercise P12: Analysis of an application process dump (ApplicationR, 32-bit).....	161
Exercise P13: Analysis of an application process dump (ApplicationA, 32-bit).....	172
Exercise P14: Analysis of an application process dump (ApplicationS, 32-bit) .....	181
Exercise K1: Analysis of a normal kernel dump (32-bit).....	193
Exercise K2: Analysis of a kernel dump with pool leak (32-bit).....	231
Exercise K3: Analysis of a kernel dump with pool corruption (32-bit) .....	246
Exercise K4: Analysis of a kernel dump with code corruption (32-bit) .....	253
Exercise K5: Analysis of a kernel dump with hang I/O (32-bit) .....	263
Exercise C1: Analysis of a normal complete dump (32-bit).....	276
Exercise C2: Analysis of a problem complete dump (32-bit).....	296
Application Source Code .....	338
ApplicationA .....	339
ApplicationB .....	341
ApplicationC.....	343
ApplicationE.....	345
ApplicationK.....	347
ApplicationL.....	348
ApplicationM .....	349
ApplicationN .....	350

ApplicationO.....	351
ApplicationP.....	352
ApplicationR .....	353
ApplicationS.....	354
Selected Q&A.....	355