



# Windows Memory Dump Analysis **Accelerated**

**Version 5.0**

**Part 1: Process User Space**

Dmitry Vostokov  
Software Diagnostics Services

Published by OpenTask, Republic of Ireland

Copyright © 2019 by OpenTask

Copyright © 2019 by Software Diagnostics Services

Copyright © 2019 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](mailto:press@opentask.com).

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

ISBN-13: 978-1-912636-05-1 (Paperback)

Version 5, 2019

Revision 5.00 (November 2019)

# Contents

About the Author.....	5
Presentation Slides and Transcript.....	7
Practice Exercises .....	33
Exercise 0: Download, setup and verify your WinDbg or WinDbg Preview installation .....	38
Exercise P1: Analysis of a normal application process dump (64-bit notepad) .....	48
Exercise P2: Analysis of a normal application process dump (32-bit notepad) .....	72
Exercise P3: Analysis of a normal application process dump (64-bit Microsoft Edge) .....	74
Exercise P4: Analysis of an application process dump (64-bit AppK, no symbols).....	114
Exercise P5: Analysis of an application process dump (64-bit AppK, with application symbols).....	128
Exercise P6: Analysis of an application process dump (AppL, 64-bit) .....	134
Exercise P7: Analysis of an application process dump (AppL2, 64-bit) .....	148
Exercise P8: Analysis of an application process dump (AppM, 64-bit) .....	168
Exercise P9: Analysis of an application process dump (AppN, 64-bit) .....	178
Exercise P10: Analysis of an application process dump (AppO, 64-bit) .....	192
Exercise P11: Analysis of an application process dump (AppP, 64-bit).....	202
Exercise P12: Analysis of an application process dump (AppR, 32-bit).....	218
Exercise P13: Analysis of an application process dump (AppA, WOW64) .....	242
Exercise P14: Analysis of an application process dump (AppS, 64-bit).....	252
Exercise P15: Analysis of an application process dump (notepad, 32-bit).....	272
Exercise P16: Analysis of an application process dump (notepad, 64-bit).....	278
Exercise P17: Analysis of an application process dump (AppQ, 32-bit) .....	286
Exercise P18: Analysis of an application process dump (AppQ, 64-bit) .....	300
Exercise P19: Analysis of an application process dump (AppT, 64-bit).....	314
Application Source Code .....	335
AppA .....	337
AppK .....	339
AppL.....	340
AppL2.....	341
AppM .....	342
AppN.....	343
AppO.....	344
AppP .....	346
AppR .....	347

AppS.....	348
AppQ.....	350
AppT.....	354
Selected Q&A.....	357
Triple Dereference.....	383
Large Heap Allocations.....	385