



Windows Memory Dump Analysis **Advanced** with Data Structures

Version 3.0

Dmitry Vostokov
Software Diagnostics Services

Published by OpenTask, Republic of Ireland

Copyright © 2017 by OpenTask

Copyright © 2017 by Software Diagnostics Services

Copyright © 2017 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.

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

ISBN-13: 978-1-908043-84-9 (Paperback)

Version 3, 2017

Revision 3.00 (June 2017)

Contents

About the Author	5
Presentation Slides and Transcript	7
Practice Exercises	13
Exercise 0: Download, setup and verify your WinDbg installation.....	18
Exercise C1: Stack Trace Collection (64-bit)	25
Exercise C2: Memory Search (64-bit).....	66
Exercise C3: Linked Lists (64-bit).....	80
Exercise C4A: WinDbg Built-in Scripting (64-bit).....	133
Exercise C4B: WinDbg JavaScript Scripting (64-bit)	151
Exercise C5: Registry (64-bit)	167
Exercise C6: Module Variables (64-bit)	176
Exercise C7: System Objects (64-bit)	181
Exercise C8: Network (64-bit)	191
Exercise C9: Device Drivers (64-bit)	205
Exercise C10: Storage and File System (64-bit)	221
Exercise C11: Window Messaging (64-bit).....	226
Legacy Exercises	239
Exercise Legacy.0: Download, setup and verify your WinDbg installation	241
Exercise Legacy.C1: Stack Trace Collection (64-bit)	246
Exercise Legacy.C2: Memory Search (64-bit)	271
Exercise Legacy.C3: Linked Lists (64-bit)	282
Exercise Legacy.C4: Scripting (64-bit)	311
Exercise Legacy.C5: Registry (64-bit)	328
Exercise Legacy.C6: Module Variables (64-bit)	336
Exercise Legacy.C7: System Objects (64-bit).....	340
Exercise Legacy.C8: Network (64-bit)	346
Exercise Legacy.C9: Device Drivers (64-bit)	354
Selected Q&A	365