Windows Debugging Notebook

Essential User Space WinDbg Commands

Roberto Alexis Farah
Dmitry Vostokov
Mario Hewardt
(Foreword)

OpenTask

Published by OpenTask, Republic of Ireland

WinDbg Commands section Copyright © 2011 by Roberto Alexis Farah

Interior and cover design Copyright © 2008 by Dmitry Vostokov

A Note about Heap section Copyright © 2008 by Dmitry Vostokov

Troubleshooting and Debugging Notebooks series editor: 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.

OpenTask books are available through booksellers and distributors worldwide. For further information or comments send requests to press@opentask.com.

Microsoft, MSDN, Visual C++, Visual Studio, Win32, Windows, Windows Server and Windows Vista are registered trademarks of Microsoft Corporation. Citrix is a registered trademark of Citrix Systems. Other product and company names mentioned in this book may be trademarks of their owners.

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

ISBN-13: 978-1-906717-00-1 (Paperback)

ISBN-13: 978-0-9558328-5-7 (Hardcover)

First printing, 2011

Table of Contents

Table of Contents 5

Series Editor's Preface 7

Preface 9

Acknowledgements 11

About the Author 13

A Note about Heap 15

WinDbg Commands 17

.dump/.dumpcab 17

.writemem 19

!runaway 21

!lmi 23

!dlls 25

!dh 32

wt 37

u, ub, uf 43

Editing memory (a, eb, ed, ew, eza, ezu) 52

*k** 85

kL 1000 86

kpn 1000 87

kbn 1000 88

kvn 1000 89

kPn 1000 90

kf 1000 91

kpM 92

*d** 93

dd 94

db 95

du 96

da 97

dc *98*
dyb *99*
.formats *100*
*dp** *101*
dpa *102*
dpu *103*
dps *104*
dpp *106*
dv *107*
!for_each_frame *109*
*~** *111*
*x** *122*
??, @@c++() and poi() *132*
z *134*
!address *136*
.foreach *139*
.shell *146*
.cmdtree *153*
Pseudo-registers *155*
.if and j *157*
ln *159*
Logging and History *161*
!uniqstack *164*
Breakpoints: bp, bm, ba, bu *168*
dt *171*
*lm** *212*
!findstack *225*
s *228*
Scripting *236*
!chksym/!itoldyouso *241*
*244*

Notes 249