

# Windows® Debugging Notebook

---

Essential Concepts, WinDbg Commands and  
Tools

**Roberto Alexis Farah**  
**Dmitry Vostokov**

Published by OpenTask, Republic of Ireland

Copyright © 2008 by Roberto Alexis Farah, 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](mailto: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, 2008





## SUMMARY OF CONTENTS

Preface .....	11
Acknowledgements .....	13
About the Author .....	15
32 (0x20) Essential Concepts .....	17
64 (0x40) WinDbg Commands .....	81
16 (0x10) Tools .....	207
Appendix A: Checklists .....	239
Appendix B: Further Reading .....	245
Bibliography .....	247
Index .....	252
Notes .....	253



# CONTENTS

Preface .....	11
Acknowledgements .....	13
About the Authors .....	15
32 (0x20) Essential Concepts .....	17
01 (0x01): Memory / Crash Dump Types .....	17
02 (0x02): Virtual / Physical Memory.....	19
03 (0x03): Crash / Hang .....	21
04 (0x04): Exception / Breakpoint .....	23
05 (0x05): Heap / Pool / Paged / NonPaged .....	25
06 (0x06): Stack / Stack Trace / Raw Stack / FPO.....	27
07 (0x07): Execution Context.....	29
08 (0x08): First Chance / Second Chance Exceptions .....	31
09 (0x09): SEH / Exception Handlers.....	33
10 (0x0A): PE / Import / Export Tables.....	35
11 (0x0B): Virtual Function Call.....	37
12 (0x0C): OMAP / Disassembly.....	39
13 (0x0D): IDT / ISR / Trap Frame.....	41
14 (0x0E): Critical Section / Executive Resource .....	43
15 (0x0F): Synchronization / Dispatcher Object.....	45
16 (0x10): Calling Convention .....	47
17 (0x11): (Un)Managed / Native Code.....	49

18 (0x12): IRQL .....	51
19 (0x13): Thread Priority / Scheduling.....	53
20 (0x14): Postmortem / Live Debugger.....	55
21 (0x15): APC / DPC / ISR.....	57
22 (0x16): Deadlock .....	59
23 (0x17): File / Device / Driver Object .....	60
24 (0x18): IRP / Completion / Cancellation.....	62
25 (0x19): User / Kernel Mode / Space .....	64
26 (0x1A): Module / DLL / EXE / SYS .....	66
27 (0x1B): LPC / RPC .....	68
28 (0x1C): FSD / File System Filter .....	70
29 (0x1D): PDO / FDO / FiDO.....	72
30 (0x1E): Objects and Handles .....	74
31 (0x1F): PDE / PTE / PFN .....	75
32 (0x20): Session ID / CID / PID / TID .....	77
64 (0x40) WinDbg Commands .....	81
Common .....	81
version.....	81
!analyze -v (-hang).....	83
User Space .....	94
Kernel / Complete Space .....	126
16 (0x10) Tools .....	207
01 (0x01): Gflags.....	207
02 (0x02): Application Verifier .....	209

03 (0x03): NTSD / CDB / Dr. Watson .....	211
04 (0x04): WER.....	213
05 (0x05): Userdump .....	215
06 (0x06): Exception Monitor.....	217
07 (0x07): DebugDiag .....	219
08 (0x08): ADPlus.....	221
09 (0x09): SystemDump .....	223
10 (0x0A): DumpCheck .....	225
11 (0x0B): InstantDump .....	227
12 (0x0C): Driver Verifier .....	229
13 (0x0D): Process Monitor.....	231
14 (0x0E): Traceview / XPerf .....	233
15 (0x0F): WindowHistory .....	235
16 (0x10): MessageHistory.....	237
Appendix A: Checklists .....	239
Appendix B: Further Reading.....	245
Bibliography.....	247
Index.....	252
Notes.....	253

