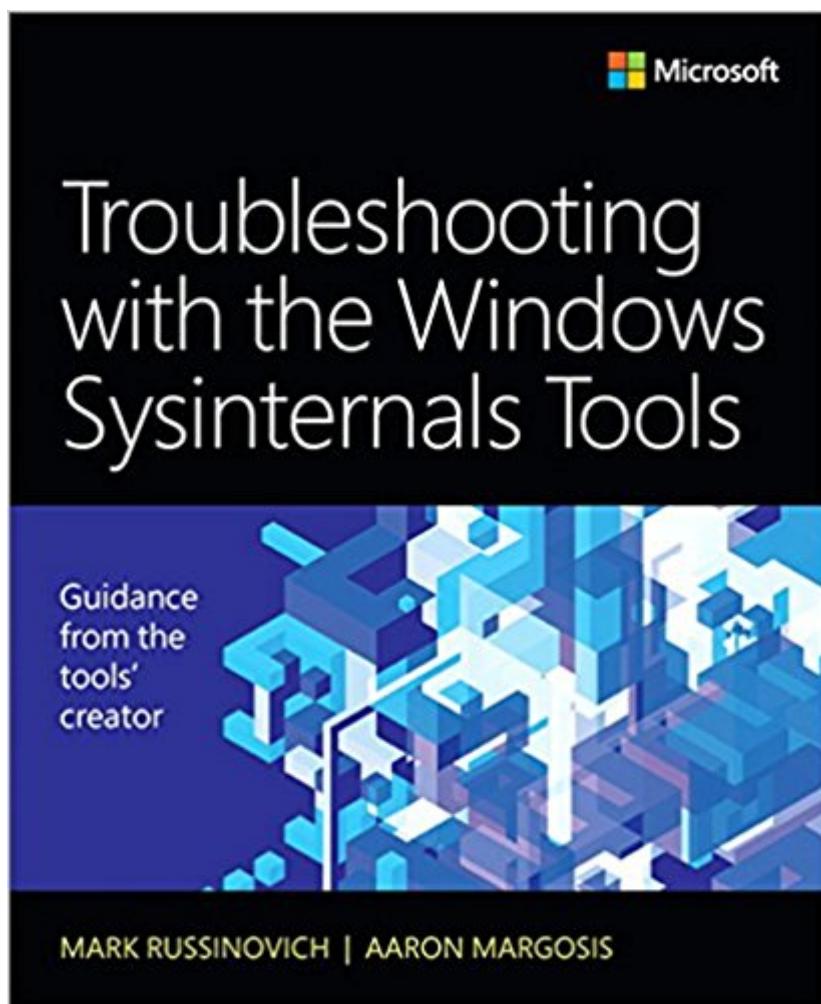


The book was found

# Troubleshooting With The Windows Sysinternals Tools (2nd Edition)



## Synopsis

Optimize Windows system reliability and performance with Sysinternals. IT pros and power users consider the free Windows Sysinternals tools indispensable for diagnosing, troubleshooting, and deeply understanding the Windows platform. In this extensively updated guide, Sysinternals creator Mark Russinovich and Windows expert Aaron Margosis help you use these powerful tools to optimize any Windows system's reliability, efficiency, performance, and security. The authors first explain Sysinternals' capabilities and help you get started fast. Next, they offer in-depth coverage of each major tool, from Process Explorer and Process Monitor to Sysinternals' security and file utilities. Then, building on this knowledge, they show the tools being used to solve real-world cases involving error messages, hangs, sluggishness, malware infections, and much more. Windows Sysinternals creator Mark Russinovich and Aaron Margosis show you how to: Use Process Explorer to display detailed process and system information Use Process Monitor to capture low-level system events, and quickly filter the output to narrow down root causes List, categorize, and manage software that starts when you start or sign in to your computer, or when you run Microsoft Office or Internet Explorer Verify digital signatures of files, of running programs, and of the modules loaded in those programs Use Autoruns, Process Explorer, Sigcheck, and Process Monitor features that can identify and clean malware infestations Inspect permissions on files, keys, services, shares, and other objects Use Sysmon to monitor security-relevant events across your network Generate memory dumps when a process meets specified criteria Execute processes remotely, and close files that were opened remotely Manage Active Directory objects and trace LDAP API calls Capture detailed data about processors, memory, and clocks Troubleshoot unbootable devices, file-in-use errors, unexplained communication, and many other problems Understand Windows core concepts that aren't well-documented elsewhere

## Book Information

Paperback: 688 pages

Publisher: Microsoft Press; 2 edition (October 27, 2016)

Language: English

ISBN-10: 0735684448

ISBN-13: 978-0735684447

Product Dimensions: 7.4 x 1.5 x 9 inches

Shipping Weight: 3.2 pounds (View shipping rates and policies)

Average Customer Review: 4.8 out of 5 stars 22 customer reviews

Best Sellers Rank: #39,281 in Books (See Top 100 in Books) #7 in Books > Computers & Technology > Business Technology > Windows Server #9 in Books > Computers & Technology > Networking & Cloud Computing > Data in the Enterprise > Client-Server Systems #22 in Books > Computers & Technology > Operating Systems > Windows > Windows Desktop

## Customer Reviews

Mark Russinovich is Chief Technology Officer of Microsoft Azure, where he oversees the technical strategy and architecture of Microsoft's cloud computing platform. He is a widely recognized expert in distributed systems, operating system internals, and cybersecurity. He is the author of the Jeff Aiken cyberthriller novels, Zero Day, Trojan Horse, and Rogue Code, and co-author of the Microsoft Press Windows Internals books. Russinovich joined Microsoft in 2006 when Microsoft acquired Winternals Software, the company he cofounded in 1996, as well as Sysinternals, where he authors and publishes dozens of popular Windows administration and diagnostic utilities. He is a featured speaker at major industry conferences, including Microsoft Ignite, Microsoft //build, RSA Conference, and more. Aaron Margosis is a Principal Consultant with Microsoft's Global Cybersecurity Practice, where he has worked with security-conscious customers since 1999. Aaron specializes in Windows security, least-privilege, application compatibility, and the configuration of locked-down environments. He is a top speaker at Microsoft conferences, and created many of the tools commonly used by organizations implementing high-security environments, including LUA Buglight, Policy Analyzer, IE Zone Analyzer, LGPO.exe (Local Group Policy Object utility), and MakeMeAdmin, which can be downloaded through his blog ([https://blogs.msdn.microsoft.com/aaron\\_margosis](https://blogs.msdn.microsoft.com/aaron_margosis)) or through two team blogs for which he is a primary author

(<https://blogs.technet.microsoft.com/fdcc> and <https://blogs.technet.microsoft.com/SecGuide>)

Extremely useful whether you are a sysadmin or developer. Really grok the internals of Windows by exploring them in a hands on manner.

Amazing invaluable book keep up the awesome work mark

useful tool book

Helpful documentation and explanation of tools.

It's the ultimate resource for troubleshooting windows systems in depth and gain a better knowledge.

AWESOME!

Excellent book, great read!

Very practical, really great book. I call it "Windows Internals missing chapters".

[Download to continue reading...](#)

Troubleshooting with the Windows Sysinternals Tools (2nd Edition) Windows 10: The Ultimate 2 in 1 User Guide to Microsoft Windows 10 User Guide to Microsoft Windows 10 for Beginners and Advanced Users (tips and tricks, ... Windows, softwares, guide Book 7) Windows 10: The Best Guide How to Operate New Microsoft Windows 10 (tips and tricks, 2017 user manual, user guide, updated and edited, Windows for beginners) Windows 10: The Best Guide How to Operate New Microsoft Windows 10 (tips and tricks, user manual, user guide, updated and edited, Windows for beginners) Windows 10: The Ultimate 2017 Updated User Guide to Microsoft Windows 10 (2017 updated user guide, tips and tricks, user manual, user guide, Windows 10) Windows 10 Manual and Windows 10 User Guide (Windows 10 Guide for Beginners) Windows 10: User Guide and Manual: Microsoft Windows 10 for Windows Users Easy Thermostat Wiring & Troubleshooting Guide: Simple HVAC, Furnace, and Air Conditioning; Thermostat Wiring and Troubleshooting Guide for Homeowners (HelpItBroke.com - Easy HVAC Guides Book 3) Troubleshooting LC Systems: A Comprehensive Approach to Troubleshooting LC Equipment and Separations Windows Registry Forensics, Second Edition: Advanced Digital Forensic Analysis of the Windows Registry Windows 10: Pros and Cons (Windows 10 for beginners Kindle ebooks Edition Book 2) Windows Forensic Analysis Toolkit, Fourth Edition: Advanced Analysis Techniques for Windows 8 Save America's Windows: Caring for older and historic wood windows. Working Windows: A Guide To The Repair And Restoration Of Wood Windows Windows 10: Complete Beginners Guide To Microsoft WINDOWS 10 (Tips And Tricks, User Manual, 2017 Updated User Guide) Microsoft Specialist Guide to Microsoft Windows 10 (Exam 70-697, Configuring Windows Devices) Emergency Care and Transportation of the Sick and Injured (Book with Mini-CD-ROM for Windows & Macintosh,

Palm/Handspring, Windows CE/Pocket PC, Electric Motor Maintenance and Troubleshooting, 2nd Edition (Electronics) 55 Smart Apps to Level Up Your Brain: Free Apps, Games, and Tools for iPhone, iPad, Google Play, Kindle Fire, Web Browsers, Windows Phone, & Apple Watch Windows 10 Inside Out (includes Current Book Service) (2nd Edition)

[Contact Us](#)

[DMCA](#)

[Privacy](#)

[FAQ & Help](#)