

---

# Inside Windows Debugging A Practical Guide To Debugging And Tracing Strategies In Windows Paperback 2012 Tarik Soulami

---

Gray Hat Python

Learning Malware Analysis

Old New Thing

Hands-On Penetration Testing on Windows

Effective Debugging

Debugging Microsoft .NET 2.0 Applications

Windows Internals, Part 1

Windows 10 Inside Out (includes Current Book Service)

Debugging Applications for Microsoft .NET and Microsoft Windows

Practical Foundations of Linux Debugging, Disassembling, Reversing

Mastering Visual Studio .NET  
Advanced Windows Memory Dump Analysis with Data Structures  
X64 Windows Debugging  
Advanced R  
Practical Debugging for .NET Developers  
Windows Internals, Part 2  
Debugging Windows Programs  
Security Warrior  
Advanced .NET Debugging  
Automate the Boring Stuff with Python, 2nd Edition  
Practical Malware Analysis  
Windows PowerShell Step by Step  
Windows Debugging  
Windows Debugging Notebook  
Practical Foundations of Windows Debugging, Disassembling, Reversing  
Practical Mod\_perl  
Troubleshooting Finite-Element Modeling with Abaqus  
Windows Sysinternals Administrator's Reference  
Windows Server 2019 & PowerShell All-in-One For Dummies  
Practical Reverse Engineering

Learning DCOM  
Windows Internals  
The Art of Debugging with GDB, DDD, and Eclipse  
Windows Internals  
Developing Drivers with the Windows Driver Foundation  
Accelerated Windows Debugging 3  
Advanced Windows Debugging  
Windows Runtime via C#  
Inside Windows Debugging

*Inside Windows  
Debugging A Practical  
Guide To Debugging  
And Tracing Strategies  
In Windows Paperback  
2012 Tarik Soulami*

Downloaded from  
[business.itu.edu.tr](http://business.itu.edu.tr) by guest

---

**ERICK CORTEZ**

---

**Gray Hat Python** Addison-Wesley  
Professional  
Every software developer and IT  
professional understands the crucial

importance of effective debugging.  
Often, debugging consumes most of a  
developer's workday, and mastering the  
required techniques and skills can take a  
lifetime. In *Effective Debugging*,  
Diomidis Spinellis helps experienced  
programmers accelerate their journey to  
mastery, by systematically categorizing,  
explaining, and illustrating the most  
useful debugging methods, strategies,

techniques, and tools. Drawing on more than thirty-five years of experience, Spinellis expands your arsenal of debugging techniques, helping you choose the best approaches for each challenge. He presents vendor-neutral, example-rich advice on general principles, high-level strategies, concrete techniques, high-efficiency tools, creative tricks, and the behavioral traits associated with effective debugging. Spinellis's 66 expert techniques address every facet of debugging and are illustrated with step-by-step instructions and actual code. He addresses the full spectrum of problems that can arise in modern software systems, especially problems caused by complex interactions among components and services running on hosts scattered

around the planet. Whether you're debugging isolated runtime errors or catastrophic enterprise system failures, this guide will help you get the job done—more quickly, and with less pain. Key features include High-level strategies and methods for addressing diverse software failures Specific techniques to apply when programming, compiling, and running code Better ways to make the most of your debugger General-purpose skills and tools worth investing in Advanced ideas and techniques for escaping dead-ends and the maze of complexity Advice for making programs easier to debug Specialized approaches for debugging multithreaded, asynchronous, and embedded code Bug avoidance through improved software design, construction,

and management

Learning Malware Analysis "O'Reilly  
Media, Inc."

DCOM -- the Distributed Component Object Model -- is a recent upgrade of a time-honored and well-tested technology promoted by Microsoft for distributed object programming. Now that components are playing a larger and larger part in Windows 98, Windows NT 4.0, and Windows 2000, every Windows programmer will want to understand the technology. DCOM competes with CORBA as a rich and robust method for creating expandable and flexible components, allowing you to plug in new parts conveniently and upgrade without the need for code changes to every program that uses your component. This book introduces C++ programmers to

DCOM and gives them the basic tools they need to write secure, maintainable programs. While using Visual C++ development tools and wizards where appropriate, the author never leaves the results up to magic. The C++ code used to create distributed components and the communications exchanged between systems and objects are described at a level where the reader understands their significance and can use the insights for such tasks as debugging and improving performance. The first few chapters explain both the remote procedure calls that underlie DCOM's communication and the way DCOM uses C++ classes. Readers become firmly grounded in the relation between components, classes, and objects, the ways objects are created and destroyed, how clients find

servers, and the basics of security and threading. After giving you a grounding in how DCOM works, this book introduces you to the Microsoft tools that make it all easy. By showing what really happens each time you choose a button in a wizard, Learning DCOM makes it possible for you to choose what you need. This book is for anyone who wants to understand DCOM. While thoroughly practical in its goals, it doesn't stint on the background you need to make your programs safe, efficient, and easy to maintain. Topics include: MIDL (Microsoft Interface Definition Language, the language for defining COM interfaces) COM error and exception handling Custom, dispatch, and dual interfaces Standard and custom factories Management of in-process versus out-of-

process servers Distributed memory management Pragmatic explanation of the DCOM wire protocol Standard, custom, handler, and automation marshaling Multithreading and apartments Security at the system configuration and programming level Active Template Library (ATL), ATL wizards -- and what they don't do Writing a component that can be invoked from Visual Basic Techniques for using distributed components Creating an ActiveX control and embedding it in a Web client Authentication and the use of Windows NT security features Techniques for merging marshaling code Connection and distributed events management An introduction to COM+ features *Old New Thing* Microsoft Press

This training course is a combined and reformatted version of the two previous books Windows Debugging: Practical Foundations and x64 Windows Debugging: Practical Foundations. The new format makes it easy to switch between and compare x86 and x64 versions. The book also has a larger format similar to other training courses from Software Diagnostics Services, punctuation and code highlighting improvements, the output and screenshots from the latest WinDbg 10, and consistently uses WinDbg (X86) for 32-bit examples and WinDbg (X64) for 64-bit examples. The book contains two separate sets of chapters and corresponding illustrations. They are named Chapter x86.NN and Chapter x64.NN respectively. There is some

repetition of content due to the shared nature of x64 and x86 platforms. Both sets of chapters can be read independently. We included x86 chapters because many Windows applications are still 32-bit and executed in 32-bit compatibility mode on x64 Windows systems. This introductory training course can complement the more advanced course Accelerated Disassembly, Reconstruction and Reversing (ISBN: 978-1908043672). Hands-On Penetration Testing on Windows No Starch Press  
“Mario Hewardt’s Advanced .NET Debugging is an excellent resource for both beginner and experienced developers working with .NET. The book is also packed with many debugging tips and discussions of CLR internals, which

will benefit developers architecting software.” –Jeffrey Richter, consultant, trainer, and author at Wintellect “Mario has done it again. His *Advanced Windows Debugging* (coauthored with Daniel Pravat) is an invaluable resource for native code debugging, and *Advanced .NET Debugging* achieves the same quality, clarity, and breadth to make it just as invaluable for .NET debugging.” –Mark Russinovich, Technical Fellow, Microsoft Corporation *The Only Complete, Practical Guide to Fixing the Toughest .NET Bugs* *Advanced .NET Debugging* is the first focused, pragmatic guide to tracking down today’s most complex and challenging .NET application bugs. It is the only book to focus entirely on using powerful native debugging tools, including

WinDBG, NTSD, and CDB, to debug .NET applications. Using these tools, author Mario Hewardt explains how to identify the real root causes of problems—far more quickly than you ever could with other debuggers. Hewardt first introduces the key concepts needed to successfully use .NET’s native debuggers. Next, he turns to sophisticated debugging techniques, using real-world examples that demonstrate many common C# programming errors. This book enables you to Make practical use of postmortem debugging, including PowerDBG and other “power tools” Understand the debugging details and implications of the new .NET CLR 4.0 Master and successfully use Debugging Tools for Windows, as well as SOS, SOSEX, CLR

Profiler, and other powerful tools Gain a deeper, more practical understanding of CLR internals, such as examining thread-specific data, managed heap and garbage collector, interoperability layer, and .NET exceptions Solve difficult synchronization problems, managed heap problems, interoperability problems, and much more Generate and successfully analyze crash dumps A companion web site ([advanceddotnetdebugging.com](http://advanceddotnetdebugging.com)) contains all sample code, examples, and bonus content.

*Effective Debugging* No Starch Press  
The First In-Depth, Real-World, Insider's Guide to Powerful Windows Debugging For Windows developers, few tasks are more challenging than debugging--or more crucial. Reliable and realistic

information about Windows debugging has always been scarce. Now, with over 15 years of experience two of Microsoft's system-level developers present a thorough and practical guide to Windows debugging ever written. Mario Hewardt and Daniel Pravat cover debugging throughout the entire application lifecycle and show how to make the most of the tools currently available--including Microsoft's powerful native debuggers and third-party solutions. To help you find real solutions fast, this book is organized around real-world debugging scenarios. Hewardt and Pravat use detailed code examples to illuminate the complex debugging challenges professional developers actually face. From core Windows operating system concepts to security,

Windows® Vista™ and 64-bit debugging, they address emerging topics head-on—and nothing is ever oversimplified or glossed over!

*Debugging Microsoft .NET 2.0*

Applications Microsoft Press

Python is fast becoming the programming language of choice for hackers, reverse engineers, and software testers because it's easy to write quickly, and it has the low-level support and libraries that make hackers happy. But until now, there has been no real manual on how to use Python for a variety of hacking tasks. You had to dig through forum posts and man pages, endlessly tweaking your own code to get everything working. Not anymore. Gray Hat Python explains the concepts behind hacking tools and techniques like

debuggers, trojans, fuzzers, and emulators. But author Justin Seitz goes beyond theory, showing you how to harness existing Python-based security tools—and how to build your own when the pre-built ones won't cut it. You'll learn how to: -Automate tedious reversing and security tasks -Design and program your own debugger -Learn how to fuzz Windows drivers and create powerful fuzzers from scratch -Have fun with code and library injection, soft and hard hooking techniques, and other software trickery -Sniff secure traffic out of an encrypted web browser session -Use PyDBG, Immunity Debugger, Sulley, IDAPython, PyEMU, and more The world's best hackers are using Python to do their handiwork. Shouldn't you? *Windows Internals, Part 1* Microsoft Press

Drill down into Windows architecture and internals, discover how core Windows components work behind the scenes, and master information you can continually apply to improve architecture, development, system administration, and support. Led by three renowned Windows internals experts, this classic guide is now fully updated for Windows 10 and 8.x. As always, it combines unparalleled insider perspectives on how Windows behaves "under the hood" with hands-on experiments that let you experience these hidden behaviors firsthand. Part 2 examines these and other key Windows 10 OS components and capabilities: Startup and shutdown The Windows Registry Windows management mechanisms WMI System mechanisms

ALPC ETW Cache Manager Windows file systems The hypervisor and virtualization UWP Activation Revised throughout, this edition also contains three entirely new chapters: Virtualization technologies Management diagnostics and tracing Caching and file system support

**Windows 10 Inside Out (includes Current Book Service)** Microsoft Press Delve inside Windows architecture and internals—and see how core components work behind the scenes. Led by three renowned internals experts, this classic guide is fully updated for Windows 7 and Windows Server 2008 R2—and now presents its coverage in two volumes. As always, you get critical insider perspectives on how Windows operates. And through hands-on experiments,

you'll experience its internal behavior firsthand—knowledge you can apply to improve application design, debugging, system performance, and support. In Part 1, you will:

- Understand how core system and management mechanisms work—including the object manager, synchronization, Wow64, Hyper-V, and the registry
- Examine the data structures and activities behind processes, threads, and jobs
- Go inside the Windows security model to see how it manages access, auditing, and authorization
- Explore the Windows networking stack from top to bottom—including APIs, BranchCache, protocol and NDIS drivers, and layered services
- Dig into internals hands-on using the kernel debugger, performance monitor, and other tools

*Debugging Applications for Microsoft*

*.NET and Microsoft Windows* Pearson Education

The second edition of this best-selling Python book (over 500,000 copies sold!) uses Python 3 to teach even the technically uninclined how to write programs that do in minutes what would take hours to do by hand. There is no prior programming experience required and the book is loved by liberal arts majors and geeks alike. If you've ever spent hours renaming files or updating hundreds of spreadsheet cells, you know how tedious tasks like these can be. But what if you could have your computer do them for you? In this fully revised second edition of the best-selling classic *Automate the Boring Stuff with Python*, you'll learn how to use Python to write programs that do in minutes what would

take you hours to do by hand--no prior programming experience required. You'll learn the basics of Python and explore Python's rich library of modules for performing specific tasks, like scraping data off websites, reading PDF and Word documents, and automating clicking and typing tasks. The second edition of this international fan favorite includes a brand-new chapter on input validation, as well as tutorials on automating Gmail and Google Sheets, plus tips on automatically updating CSV files. You'll learn how to create programs that effortlessly perform useful feats of automation to:

- Search for text in a file or across multiple files
- Create, update, move, and rename files and folders
- Search the Web and download online content
- Update and format data in

Excel spreadsheets of any size

- Split, merge, watermark, and encrypt PDFs
- Send email responses and text notifications
- Fill out online forms

Step-by-step instructions walk you through each program, and updated practice projects at the end of each chapter challenge you to improve those programs and use your newfound skills to automate similar tasks. Don't spend your time doing work a well-trained monkey could do. Even if you've never written a line of code, you can make your computer do the grunt work. Learn how in Automate the Boring Stuff with Python, 2nd Edition.

[Practical Foundations of Linux Debugging, Disassembling, Reversing](#)  
Pearson Education

Your one-stop reference for Windows

Server 2019 and PowerShell know-how  
 Windows Server 2019 & PowerShell All-in-One For Dummies offers a single reference to help you build and expand your knowledge of all things Windows Server, including the all-important PowerShell framework. Written by an information security pro and professor who trains aspiring system administrators, this book covers the broad range of topics a system administrator needs to know to run Windows Server 2019, including how to install, configure, and secure a system. This book includes coverage of: Installing & Setting Up Windows Server  
 Configuring Windows Server 2019  
 Administering Windows Server 2019  
 Configuring Networking Managing Security Working with Windows

PowerShell Installing and Administering Hyper-V Installing, Configuring, and Using Containers If you're a budding or experienced system administrator looking to build or expand your knowledge of Windows Server, this book has you covered.

*Mastering Visual Studio .NET* No Starch Press

This resource helps technical support, escalation engineers, and Windows software testers master necessary prerequisites to understand and start debugging and crash dump analysis on Windows platforms.

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

Fastprint Publishing

This training course is a Linux version of the previous Practical Foundations of

Windows Debugging, Disassembly, Reversing book. It also complements Accelerated Linux Core Dump Analysis training course. Although the book skeleton is the same as its Windows predecessor, the content was revised entirely because of a different operating system, debugger (GDB), toolchain (GCC, assembler, linker), application binary interface, and even an assembly language flavor, AT&T. The course is useful for: Software technical support and escalation engineers Software engineers coming from JVM background Software testers Engineers coming from non-Linux environments, for example, Windows or Mac OS X Linux C/C++ software engineers without assembly language background Security researchers without assembly language

background Beginners learning Linux software reverse engineering techniques This book can also be used as x64 assembly language and Linux debugging supplement for relevant undergraduate level courses.

*X64 Windows Debugging* Microsoft Press Malware analysis is big business, and attacks can cost a company dearly. When malware breaches your defenses, you need to act quickly to cure current infections and prevent future ones from occurring. For those who want to stay ahead of the latest malware, *Practical Malware Analysis* will teach you the tools and techniques used by professional analysts. With this book as your guide, you'll be able to safely analyze, debug, and disassemble any malicious software that comes your way. You'll learn how to:

-Set up a safe virtual environment to analyze malware -Quickly extract network signatures and host-based indicators -Use key analysis tools like IDA Pro, OllyDbg, and WinDbg -Overcome malware tricks like obfuscation, anti-disassembly, anti-debugging, and anti-virtual machine techniques -Use your newfound knowledge of Windows internals for malware analysis -Develop a methodology for unpacking malware and get practical experience with five of the most popular packers -Analyze special cases of malware with shellcode, C++, and 64-bit code Hands-on labs throughout the book challenge you to practice and synthesize your skills as you dissect real malware samples, and pages of detailed dissections offer an

over-the-shoulder look at how the pros do it. You'll learn how to crack open malware to see how it really works, determine what damage it has done, thoroughly clean your network, and ensure that the malware never comes back. Malware analysis is a cat-and-mouse game with rules that are constantly changing, so make sure you have the fundamentals. Whether you're tasked with securing one network or a thousand networks, or you're making a living as a malware analyst, you'll find what you need to succeed in Practical Malware Analysis.

*Advanced R* No Starch Press

This book gives detailed instructions on how to use, optimize, and troubleshoot mod\_perl. It shows how to get this Apache module running quickly and

easily.

*Practical Debugging for .NET Developers*  
No Starch Press

Stop manually analyzing binary!

Practical Binary Analysis is the first book of its kind to present advanced binary analysis topics, such as binary instrumentation, dynamic taint analysis, and symbolic execution, in an accessible way. As malware increasingly obfuscates itself and applies anti-analysis techniques to thwart our analysis, we need more sophisticated methods that allow us to raise that dark curtain designed to keep us out--binary analysis can help. The goal of all binary analysis is to determine (and possibly modify) the true properties of binary programs to understand what they really do, rather than what we think they should do.

While reverse engineering and disassembly are critical first steps in many forms of binary analysis, there is much more to be learned. This hands-on guide teaches you how to tackle the fascinating but challenging topics of binary analysis and instrumentation and helps you become proficient in an area typically only mastered by a small group of expert hackers. It will take you from basic concepts to state-of-the-art methods as you dig into topics like code injection, disassembly, dynamic taint analysis, and binary instrumentation. Written for security engineers, hackers, and those with a basic working knowledge of C/C++ and x86-64, Practical Binary Analysis will teach you in-depth how binary programs work and help you acquire the tools and

techniques needed to gain more control and insight into binary programs. Once you've completed an introduction to basic binary formats, you'll learn how to analyze binaries using techniques like the GNU/Linux binary analysis toolchain, disassembly, and code injection. You'll then go on to implement profiling tools with Pin and learn how to build your own dynamic taint analysis tools with libdft and symbolic execution tools using Triton. You'll learn how to:

- Parse ELF and PE binaries and build a binary loader with libbfd
- Use data-flow analysis techniques like program tracing, slicing, and reaching definitions analysis to reason about runtime flow of your programs
- Modify ELF binaries with techniques like parasitic code injection and hex editing
- Build custom

disassembly tools with Capstone - Use binary instrumentation to circumvent anti-analysis tricks commonly used by malware - Apply taint analysis to detect control hijacking and data leak attacks - Use symbolic execution to build automatic exploitation tools

With exercises at the end of each chapter to help solidify your skills, you'll go from understanding basic assembly to performing some of the most sophisticated binary analysis and instrumentation. Practical Binary Analysis gives you what you need to work effectively with binary programs and transform your knowledge from basic understanding to expert-level proficiency.

*Windows Internals, Part 2* Pearson Education

This is the eBook of the printed book and may not include any media, website access codes, or print supplements that may come packaged with the bound book. Conquer today's Windows 10—from the inside out! Dive into Windows 10—and really put your Windows expertise to work. Focusing on the most powerful and innovative features of Windows 10, this supremely organized reference packs hundreds of timesaving solutions, tips, and workarounds—all fully reflecting the major Windows 10 Anniversary Update. From new Cortana and Microsoft Edge enhancements to the latest security and virtualization features, you'll discover how experts tackle today's essential tasks—and challenge yourself to new levels of mastery. Install, configure, and

personalize the newest versions of Windows 10 Understand Microsoft's revamped activation and upgrade processes Discover major Microsoft Edge enhancements, including new support for extensions Use today's improved Cortana services to perform tasks, set reminders, and retrieve information Make the most of the improved ink, voice, touch, and gesture support in Windows 10 Help secure Windows 10 in business with Windows Hello and Azure AD Deploy, use, and manage new Universal Windows Platform (UWP) apps Take advantage of new entertainment options, including Groove Music Pass subscriptions and connections to your Xbox One console Manage files in the cloud with Microsoft OneDrive and OneDrive for Business Use the improved

Windows 10 Mail and Calendar apps and the new Skype app Fine-tune performance and troubleshoot crashes Master high-efficiency tools for managing Windows 10 in the enterprise Leverage advanced Hyper-V features, including Secure Boot, TPMs, nested virtualization, and containers In addition, this book is part of the Current Book Service from Microsoft Press. Books in this program will receive periodic updates to address significant software changes for 12 to 18 months following the original publication date via a free Web Edition. Learn more at <https://www.microsoftpressstore.com/cbs>.

**Debugging Windows Programs** Packt Publishing Ltd  
A detailed handbook for experienced

developers explains how to get the most out of Microsoft's Visual Studio .NET, offering helpful guidelines on how to use its integrated development environment, start-up templates, and other features and tools to create a variety of applications, including Web services. Original. (Advanced)

*Security Warrior* CRC Press

A guide to debugging Windows applications for professional developers covers resource leaks, memory corruption, stack problems, release build problems, multithreading problems, and finding crash locations.

*Advanced .NET Debugging* Addison-Wesley Professional

The definitive guide—fully updated for Windows 10 and Windows Server 2016 Delve inside Windows architecture and

internals, and see how core components work behind the scenes. Led by a team of internals experts, this classic guide has been fully updated for Windows 10 and Windows Server 2016. Whether you are a developer or an IT professional, you'll get critical, insider perspectives on how Windows operates. And through hands-on experiments, you'll experience its internal behavior firsthand—knowledge you can apply to improve application design, debugging, system performance, and support. This book will help you:

- Understand the Windows system architecture and its most important entities, such as processes and threads
- Examine how processes manage resources and threads scheduled for execution inside processes
- Observe how Windows

- manages virtual and physical memory
- Dig into the Windows I/O system and see how device drivers work and integrate with the rest of the system
- Go inside the Windows security model to see how it manages access, auditing, and authorization, and learn about the new mechanisms in Windows 10 and Server 2016

[Automate the Boring Stuff with Python, 2nd Edition](#) Inside Windows Debugging Master the art of identifying vulnerabilities within the Windows OS and develop the desired solutions for it using Kali Linux. Key Features Identify the vulnerabilities in your system using Kali Linux 2018.02 Discover the art of exploiting Windows kernel drivers Get to know several bypassing techniques to gain control of your Windows

environment Book Description Windows has always been the go-to platform for users around the globe to perform administration and ad hoc tasks, in settings that range from small offices to global enterprises, and this massive footprint makes securing Windows a unique challenge. This book will enable you to distinguish yourself to your clients. In this book, you'll learn advanced techniques to attack Windows environments from the indispensable toolkit that is Kali Linux. We'll work through core network hacking concepts and advanced Windows exploitation techniques, such as stack and heap overflows, precision heap spraying, and kernel exploitation, using coding principles that allow you to leverage powerful Python scripts and shellcode.

We'll wrap up with post-exploitation strategies that enable you to go deeper and keep your access. Finally, we'll introduce kernel hacking fundamentals and fuzzing testing, so you can discover vulnerabilities and write custom exploits. By the end of this book, you'll be well-versed in identifying vulnerabilities within the Windows OS and developing the desired solutions for them. What you will learn Get to know advanced pen testing techniques with Kali Linux Gain an understanding of Kali Linux tools and methods from behind the scenes See how to use Kali Linux at an advanced level Understand the exploitation of Windows kernel drivers Understand advanced Windows concepts and protections, and how to bypass them using Kali Linux Discover Windows

exploitation techniques, such as stack and heap overflows and kernel exploitation, through coding principles Who this book is for This book is for penetration testers, ethical hackers, and individuals breaking into the pentesting

role after demonstrating an advanced skill in boot camps. Prior experience with Windows exploitation, Kali Linux, and some Windows debugging tools is necessary

Best Sellers - Books :

- [How To Win Friends & Influence People \(dale Carnegie Books\)](#)
- [The Summer I Turned Pretty \(summer I Turned Pretty, The\)](#)
- [A Soul Of Ash And Blood: A Blood And Ash Novel \(blood And Ash Series\) By Jennifer L. Armentrout](#)
- [Fast Like A Girl: A Woman's Guide To Using The Healing Power Of Fasting To Burn Fat, Boost Energy, And Balance Hormones By Dr. Mindy Pelz](#)
- [Twisted Hate \(twisted, 3\)](#)
- [Lessons In Chemistry: A Novel](#)
- [The Democrat Party Hates America By Mark R. Levin](#)
- [I'm Glad My Mom Died By Jennette Mccurdy](#)
- [Lord Of The Flies](#)
- [Icebreaker: A Novel \(the Maple Hills Series\)](#)