Intel X86 X64 Debugger

This is the third edition of this assembly language programming textbook introducing programmers to 64 bit Intel assembly language. The primary addition to the third edition is the discussion of the new version of the free integrated development environment, ebe, designed by the author specifically to meet the needs of assembly language programmers. The new ebe is a C++ program using the Qt library to implement a GUI environment consisting of a source window, a data window, a register, a floating point register window, a backtrace window, a console window, a terminal window and a project window along with 2 educational tools called the "toy box" and the "bit bucket." The source window includes a full-featured text editor with convenient controls for assembling, linking and debugging a program. The project facility allows a program to be built from C source code files and assembly source files. Assembly is performed automatically using the yasm assembler and linking is performed with ld or gcc. Debugging operates by transparently sending commands into the gdb debugger while automatically displaying registers and variables after each debugging step. Additional information about ebe can be found at http: //www.rayseyfarth.com. The second important addition is support for the OS X operating system. Assembly language is similar enough between the two systems to cover in a single book. The book discusses the differences between the systems. The book is intended as a first assembly language book for programmers experienced in high level programming in a language like C or C++. The assembly programming is performed using the yasm assembler automatically from the ebe IDE under the Linux operating system. The book primarily teaches how to write assembly code compatible with C programs. The reader will learn to call C functions from assembly language and to call assembly functions from C in addition to writing complete programs in assembly language. The gcc compiler is used internally to compile C programs. The book starts early emphasizing using ebe to debug programs, along with teaching equivalent commands using gdb. Being able to single-step assembly programs is critical in learning assembly programming. Ebe makes this far easier than using gdb directly. Highlights of the book include doing input/output programming using the Linux system calls and the C library, implementing data structures in assembly language and high performance assembly language programming. Early chapters of the book rely on using the debugger to observe program behavior. After a chapter on functions, the user is prepared to use printf and scanf from the C library to perform I/O. The chapter on data structures covers singly linked lists, doubly linked circular lists, hash tables and binary trees. Test programs are presented for all these data structures. There is a chapter on optimization techniques and 3 chapters on specific optimizations. One chapter covers how to efficiently count the 1 bits in an array with the most efficient version using the recently-introduced popcnt instruction. Another chapter covers using

SSE instructions to create an efficient implementation of the Sobel filtering algorithm. The final high performance programming chapter discusses computing correlation between data in 2 arrays. There is an AVX implementation which achieves 20.5 GFLOPs on a single core of a Core i7 CPU. A companion web site, http: //www.rayseyfarth.com, has a collection of PDF slides which instructors can use for in-class presentations and source code for sample programs.

The purpose of this text is to provide a reference for University level assembly language and systems programming courses. Specifically, this text addresses the x86-64 instruction set for the popular x86-64 class of processors using the Ubuntu 64-bit Operating System (OS). While the provided code and various examples should work under any Linux-based 64-bit OS, they have only been tested under Ubuntu 14.04 LTS (64-bit). The x86-64 is a Complex Instruction Set Computing (CISC) CPU design. This refers to the internal processor design philosophy. CISC processors typically include a wide variety of instructions (sometimes overlapping), varying instructions sizes, and a wide range of addressing modes. The term was retroactively coined in contrast to Reduced Instruction Set Computer (RISC3).

This book provides an overview of modern boot firmware, including the Unified Extensible Firmware Interface (UEFI) and its associated EFI Developer Kit II (EDKII) firmware. The authors have each made significant contributions to developments in these areas. The reader will learn to use the latest developments in UEFI on modern hardware, including open source firmware and open hardware designs. The book begins with an exploration of interfaces exposed to higher-level software and operating systems, and commences to the left of the boot timeline, describing the flow of typical systems, beginning with the machine restart event. Software engineers working with UEFI will benefit greatly from this book, while specific sections of the book address topics relevant for a general audience: system architects, pre-operating-system application developers, operating system vendors (loader, kernel), independent hardware vendors (such as for plug-in adapters), and developers of end-user applications. As a secondary audience, project technical leaders or managers may be interested in this book to get a feel for what their engineers are doing. The reader will find: An overview of UEFI and underlying Platform Initialization (PI) specifications How to create UEFI applications and drivers Workflow to design the firmware solution for a modern platform Advanced usages of UEFI firmware for security and manageability

The multicore revolution has reached the deployment stage in embedded systems ranging from small ultramobile devices to large telecommunication servers. The transition from single to multicore processors, motivated by the need to increase performance while conserving power, has placed great responsibility on the shoulders of software engineers. In this new embedded multicore era, the toughest task is the development of code to support more sophisticated systems. This book provides embedded engineers with solid grounding in the skills required to develop software targeting multicore

processors. Within the text, the author undertakes an in-depth exploration of performance analysis, and a close-up look at the tools of the trade. Both general multicore design principles and processor-specific optimization techniques are revealed. Detailed coverage of critical issues for multicore employment within embedded systems is provided, including the Threading Development Cycle, with discussions of analysis, design, development, debugging, and performance tuning of threaded applications. Software development techniques engendering optimal mobility and energy efficiency are highlighted through multiple case studies, which provide practical “how-to advice on implementing the latest multicore processors. Finally, future trends are discussed, including terascale, speculative multithreading, transactional memory, interconnects, and the software-specific implications of these looming architectural developments. Table of Contents Chapter 1 - Introduction Chapter 2 – Basic System and Processor Architecture Chapter 3 – Multi-core Processors & Embedded Chapter 4 –Moving To Multi-core Intel Architecture Chapter 5 – Scalar Optimization & Usability Chapter 6 – Parallel Optimization Using Threads Chapter 7 - Case Study: Data Decomposition Chapter 8 - Case Study: Functional Decomposition Chapter 9 – Virtualization & Partitioning Chapter 10 – Getting Ready For Low Power Intel Architecture Chapter 11 - Summary, Trends, and Conclusions Appendix I Glossary References *This is the only book to explain software optimization for embedded multi-core systems *Helpful tips, tricks and design secrets from an Intel programming expert, with detailed examples using the popular X86 architecture *Covers hot topics, including ultramobile devices, low-power designs, Pthreads vs. OpenMP, and heterogeneous cores

This highly relevant and up-to-the-minute book constitutes the refereed proceedings of the Third International Conference on High Performance Embedded Architectures and Compilers, HiPEAC 2008, held in Göteborg, Sweden, January 27-29, 2008. The 25 revised full papers presented together with 1 invited keynote paper were carefully reviewed and selected from 77 submissions. The papers are organized into topical sections on a number of key subjects in the field.

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.

The less-experienced engineer will be able to apply Ball's advice to everyday projects and challenges immediately with amazing results. In this new edition, the author has expanded the section on debug to include avoiding common hardware, software and interrupt problems. Other new features include an expanded section on system integration and debug to address the capabilities of more recent emulators and debuggers, a section about combination microcontroller/PLD devices, and expanded information on industry standard embedded platforms. * Covers all 'species' of embedded system chips rather than specific hardware * Learn how to cope with 'real world' problems * Design embedded systems products that are reliable and work in real applications

Android on x86: an Introduction to Optimizing for Intel® Architecture serves two main purposes. First, it makes the case for adapting your applications onto Intel’s x86 architecture, including discussions of the business potential, the changing landscape of the Android marketplace, and the unique challenges and opportunities that arise from x86 devices. The fundamental idea is that extending your applications to support x86 or creating new ones is not difficult, but it is imperative to know all of the technicalities. This book is dedicated to providing you with an awareness of these nuances and an understanding of how to tackle them. Second, and most importantly, this book provides a one-stop detailed resource for best practices and procedures associated with the installation issues, hardware optimization issues, software requirements, programming tasks, and performance optimizations that emerge when developers consider the x86 Android devices. Optimization discussions dive into native code, hardware acceleration, and advanced profiling of multimedia applications. The authors have collected this information so that you can use the book as a guide for the specific requirements of each application project. This book is not dedicated solely to code; instead it is filled with the information you need in order to take advantage of x86 architecture. It will guide you through installing the Android SDK for Intel Architecture, help you understand the differences and similarities between processor architectures available in Android devices, teach you to create and port applications, debug existing x86 applications, offer solutions for NDK and C++ optimizations, and introduce the Intel Hardware Accelerated Execution Manager. This book provides the most useful information to help you get the job done quickly while utilizing best practices. What you’ll learnThe development-relevant

differences between Android on ARM and Android on Intel x86 How to set up the SDK for an emulated Intel Android device How to build the Android OS for the Intel Mobile Processor How to create new x86 based Android applications, set up testing and performance tuning, and port existing Android applications to work with the x86 processor How to debug problems they encounter when working on the x86 Android test platform Intricacies of the Intel Hardware Accelerated Execution Manager. The reader will also gain significant insight into the OpenGL Android support. Who this book is for Android developers Hardware designers who need to understand how Android will work on their processorsCIOs and CEOs of technology-based companies IT staff who may encounter or need to understand the issues New startup founders and entrepreneurs Computer science students Table of ContentsChapter 1: History & Evolution of Android OS Chapter 2: Mobile Device Applications – Uses and Trends Chapter 3: Why x86 on Android? Chapter 4: Android Development – Business Overview andConsiderations Chapter 5: Android Devices with Intel Processors Chapter 6: Installing the Android SDK for IntelApplication Development Chapter 7: The Intel Mobile Processor Chapter 8: Creating and Porting NDK-based AndroidApplications Chapter 9: Debugging Android Chapter 10: Performance Optimization for AndroidApplications on x86 Chapter 11: x86 NDK and C++ Optimizations Chapter 12: Intel Hardware Accelerated Execution Manager Appendix: References

If you want to master the art and science of reverse engineering code with IDA Pro for security R&D or software debugging, this is the book for you. Highly organized and sophisticated criminal entities are constantly developing more complex, obfuscated, and armored viruses, worms, Trojans, and botnets. IDA Pro’s interactive interface and programmable development language provide you with complete control over code disassembly and debugging. This is the only book which focuses exclusively on the world’s most powerful and popular took for reverse engineering code. *Reverse Engineer REAL Hostile Code To follow along with this chapter, you must download a file called !DANGER!INFECTEDMALWARE!DANGER!... ‘nuff said. *Portable Executable (PE) and Executable and Linking Formats (ELF) Understand the physical layout of PE and ELF files, and analyze the components that are essential to reverse engineering. *Break Hostile Code Armor and Write your own Exploits Understand execution flow, trace functions, recover hard coded passwords, find vulnerable functions, backtrace execution, and craft a buffer overflow. *Master Debugging Debug in IDA Pro, use a debugger while reverse engineering, perform heap and stack access modification, and use other debuggers. *Stop Anti-Reversing Anti-reversing, like reverse engineering or coding in assembly, is an art form. The trick of course is to try to stop the person reversing the application. Find out how! *Track a Protocol through a Binary and Recover its Message Structure Trace execution flow from a read event, determine the structure of a protocol, determine if the protocol has any undocumented messages, and use IDA Pro to determine the functions that process a

particular message. *Develop IDA Scripts and Plug-ins Learn the basics of IDA scripting and syntax, and write IDC scripts and plug-ins to automate even the most complex tasks.

The Metasploit Framework makes discovering, exploiting, and sharing vulnerabilities quick and relatively painless. But while Metasploit is used by security professionals everywhere, the tool can be hard to grasp for first-time users. Metasploit: The Penetration Tester's Guide fills this gap by teaching you how to harness the Framework and interact with the vibrant community of Metasploit contributors. Once you've built your foundation for penetration testing, you'll learn the Framework's conventions, interfaces, and module system as you launch simulated attacks. You'll move on to advanced penetration testing techniques, including network reconnaissance and enumeration, client-side attacks, wireless attacks, and targeted social-engineering attacks. Learn how to: –Find and exploit unmaintained, misconfigured, and unpatched systems –Perform reconnaissance and find valuable information about your target –Bypass anti-virus technologies and circumvent security controls –Integrate Nmap, NeXpose, and Nessus with Metasploit to automate discovery –Use the Meterpreter shell to launch further attacks from inside the network –Harness standalone Metasploit utilities, third-party tools, and plug-ins –Learn how to write your own Meterpreter post exploitation modules and scripts You'll even touch on exploit discovery for zero-day research, write a fuzzer, port existing exploits into the Framework, and learn how to cover your tracks. Whether your goal is to secure your own networks or to put someone else's to the test, Metasploit: The Penetration Tester's Guide will take you there and beyond.

GPU Parallel Program Development using CUDA teaches GPU programming by showing the differences among different families of GPUs. This approach prepares the reader for the next generation and future generations of GPUs. The book emphasizes concepts that will remain relevant for a long time, rather than concepts that are platform-specific. At the same time, the book also provides platform-dependent explanations that are as valuable as generalized GPU concepts. The book consists of three separate parts; it starts by explaining parallelism using CPU multi-threading in Part I. A few simple programs are used to demonstrate the concept of dividing a large task into multiple parallel sub-tasks and mapping them to CPU threads. Multiple ways of parallelizing the same task are analyzed and their pros/cons are studied in terms of both core and memory operation. Part II of the book introduces GPU massive parallelism. The same programs are parallelized on multiple Nvidia GPU platforms and the same performance analysis is repeated. Because the core and memory structures of CPUs and GPUs are different, the results differ in interesting ways. The end goal is to make programmers aware of all the good ideas, as well as the bad ideas, so readers can apply the good ideas and avoid the bad ideas in their own programs. Part III of the book provides pointer for readers who want to expand their horizons. It provides a brief introduction to popular CUDA libraries (such as cuBLAS, cuFFT, NPP, and Thrust),the OpenCL

programming language, an overview of GPU programming using other programming languages and API libraries (such as Python, OpenCV, OpenGL, and Apple’s Swift and Metal,) and the deep learning library cuDNN.

The start-to-finish tutorial and reference for Windows 2000 kernel debugging! The expert guide to Windows 2000 kernel debugging and crash dump analysis Interpreting Windows 2000 stop screens--in depth! Making the most of WinDbg and KD Debugging hardware: ports, BIOS, PCI and SCSI buses, and chipsets Advanced coverage: remote debugging, Debugging Extensions, Driver Verifier, and more Step-by-step crash dump analysis and kernel debugging How to interpret every element of a Windows 2000 stop screen Using WinDbg: configuring options, symbol paths, DLLs, and more Debugging hardware: ports, BIOS, PCI and SCSI buses, chipsets, and more Configuring local and remote kernel debugging environments Includes extensive code samples This comprehensive guide to Windows 2000 kernel debugging will be invaluable to anyone who must analyze and prevent Windows 2000 system crashes--especially device driver authors and debuggers. Renowned kernel debugging expert Steven McDowell covers every aspect of kernel debugging and crash dump analysis--including advanced hardware debugging and other techniques barely addressed in Microsoft's documentation. Discover what Microsoft's WinDbg debugger can (and can't) do for you, and how to configure both local and remote kernel debugging environments. Learn to use Windows 2000's crash dump feature, step by step. Learn how to start and stop errant drivers, pause target systems, retrieve system and driver state, and step through source code using breakpoints and source-level debugging. McDowell demonstrates techniques for taking control of target systems,including finding "lost" memory blocks, setting process and thread contexts, and reviewing I/O system error logs. You'll learn how to use Microsoft's powerful Debugger Extensions to run virtually any command you choose, and master the new Driver Verifier, which can detect common mistakes in driver code with unprecedented speed and accuracy.

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 2, you’ll examine: Core subsystems for I/O, storage, memory management, cache manager, and file systems Startup and shutdown processes Crash-dump analysis, including troubleshooting tools and techniques

Android on x86: an Introduction to Optimizing for Intel® Architecture serves two main purposes. First, it makes the case for adapting your applications onto Intel’s x86 architecture, including discussions of the business potential, the changing

landscape of the Android marketplace, and the unique challenges and opportunities that arise from x86 devices. The fundamental idea is that extending your applications to support x86 or creating new ones is not difficult, but it is imperative to know all of the technicalities. This book is dedicated to providing you with an awareness of these nuances and an understanding of how to tackle them. Second, and most importantly, this book provides a one-stop detailed resource for best practices and procedures associated with the installation issues, hardware optimization issues, software requirements, programming tasks, and performance optimizations that emerge when developers consider the x86 Android devices. Optimization discussions dive into native code, hardware acceleration, and advanced profiling of multimedia applications. The authors have collected this information so that you can use the book as a guide for the specific requirements of each application project. This book is not dedicated solely to code; instead it is filled with the information you need in order to take advantage of x86 architecture. It will guide you through installing the Android SDK for Intel Architecture, help you understand the differences and similarities between processor architectures available in Android devices, teach you to create and port applications, debug existing x86 applications, offer solutions for NDK and C++ optimizations, and introduce the Intel Hardware Accelerated Execution Manager. This book provides the most useful information to help you get the job done quickly while utilizing best practices.

Memory forensics provides cutting edge technology to help investigate digital attacks Memory forensics is the art of analyzing computer memory (RAM) to solve digital crimes. As a follow-up to the best seller Malware Analyst's Cookbook, experts in the fields of malware, security, and digital forensics bring you a step-by-step guide to memory forensics—now the most sought after skill in the digital forensics and incident response fields. Beginning with introductory concepts and moving toward the advanced, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory is based on a five day training course that the authors have presented to hundreds of students. It is the only book on the market that focuses exclusively on memory forensics and how to deploy such techniques properly. Discover memory forensics techniques: How volatile memory analysis improves digital investigations Proper investigative steps for detecting stealth malware and advanced threats How to use free, open source tools for conducting thorough memory forensics Ways to acquire memory from suspect systems in a forensically sound manner The next era of malware and security breaches are more sophisticated and targeted, and the volatile memory of a computer is often overlooked or destroyed as part of the incident response process. The Art of Memory Forensics explains the latest technological innovations in digital forensics to help bridge this gap. It covers the most popular and recently released versions of Windows, Linux, and Mac, including both the 32 and 64-bit editions.

"John Robbins has done for Windows debugging what Charles Petzold did for Windows programming." -Jeffrey Richter,

author, Programming Applications for Microsoft Windows How can you prevent bugs from creeping into your programs-even before you begin writing code? What practices separate the debugging gods from the mere mortals? DEBUGGING APPLICATIONS describes a powerful, Windows-focused methodology for debugging on the offensive-starting at the requirements phase-so you catch and fix bugs at the source, before customers ever see your software. Expert bugslayer John Robbins reveals lethally effective real-world techniques for resolving just a bout any debugging problem-from memory bugs and disappearing threads to the hairiest multithreaded deadlock. * Learn the coding techniques that help you introduce fewer errors into your program and spend less time debugging * Use version control systems, bug tracking software, and other infrastructure tools to maximize product quality * Exploit the advanced debugging capabilities in the Microsoft Visual C++ and Visual Basic development systems so you debug faster and more effectively * Cushion crashes with structured exception handling and C++ exception handling * Decipher the x86 assembly language you see in the Disassembly window * Master the tools and tactics for debugging multithreaded deadlocks, cross-machine processes, multilanguage problems, Windows 2000 services and dynamic-link libraries (DLLs) that load into services, and other challenging situations Along with John's expert guidance, you also get eight of his battle-tested, professional-level utilities for solving many of the nastiest bugs you'll encounter. In all, the CD-ROM packs over 2.5 megabytes of source code to study and reuse. With DEBUGGING APPLICATIONS, you'll learn the proven practices the industry's best developers use to eradicate bugs at the source-and deliver better software faster!

"Writing Windows 8 apps with C# and XAML"--Cover.

Assembly Language for x86 Processors, 6/e is ideal for undergraduate courses in assembly language programming and introductory courses in computer systems and computer architecture. Written specifically for the Intel/Windows/DOS platform, this complete and fully updated study of assembly language teaches students to write and debug programs at the machine level. Based on the Intel processor family, the text simplifies and demystifies concepts that students need to grasp before they can go on to more advanced computer architecture and operating systems courses. Students put theory into practice through writing software at the machine level, creating a memorable experience that gives them the confidence to work in any OS/machine-oriented environment. Proficiency in one other programming language, preferably Java, C, or C++, is recommended.

Are you an Android Java programmer who needs more performance? Are you a C/C++ developer who doesn’t want to bother with the complexity of Java and its out-of-control garbage collector? Do you want to create fast intensive multimedia applications or games? If you’ve answered yes to any of these questions then this book is for you. With some general knowledge of C/C++ development, you will be able to dive headfirst into native Android development.

Learn to find software bugs faster and discover how other developers have solved similar problems. For intermediate to advanced iOS/macOS developers already familiar with either Swift or Objective-C who want to take their debugging skills to the next level,

this book includes topics such as: LLDB and its subcommands and options; low-level components used to extract information from a program; LLDB's Python module; and DTrace and how to write D scripts.

"The Antivirus Hacker's handbook shows you how to hack your own system's defenses to discover its weaknesses, so you can apply the appropriate extra protections to keep you network locked up tight."-- Back cover.

No source code? No problem. With IDA Pro, the interactive disassembler, you live in a source code-optional world. IDA can automatically analyze the millions of opcodes that make up an executable and present you with a disassembly. But at that point, your work is just beginning. With The IDA Pro Book, you'll learn how to turn that mountain of mnemonics into something you can actually use. Hailed by the creator of IDA Pro as "profound, comprehensive, and accurate," the second edition of The IDA Pro Book covers everything from the very first steps to advanced automation techniques. You'll find complete coverage of IDA's new Qt-based user interface, as well as increased coverage of the IDA debugger, the Bochs debugger, and IDA scripting (especially using IDAPython). But because humans are still smarter than computers, you'll even learn how to use IDA's latest interactive and scriptable interfaces to your advantage. Save time and effort as you learn to: –Navigate, comment, and modify disassembly –Identify known library routines, so you can focus your analysis on other areas of the code –Use code graphing to quickly make sense of cross references and function calls –Extend IDA to support new processors and filetypes using the SDK –Explore popular plug-ins that make writing IDA scripts easier, allow collaborative reverse engineering, and much more –Use IDA's built-in debugger to tackle hostile and obfuscated code Whether you're analyzing malware, conducting vulnerability research, or reverse engineering software, a mastery of IDA is crucial to your success. Take your skills to the next level with this 2nd edition of The IDA Pro Book.

This volume constitutes the refereed proceedings of the Third International Conference on Contemporary Computing, IC3 2010, held in Noida, India, in August 2010.

This easy to read textbook provides an introduction to computer architecture, while focusing on the essential aspects of hardware that programmers need to know. The topics are explained from a programmer’s point of view, and the text emphasizes consequences for programmers. Divided in five parts, the book covers the basics of digital logic, gates, and data paths, as well as the three primary aspects of architecture: processors, memories, and I/O systems. The book also covers advanced topics of parallelism, pipelining, power and energy, and performance. A hands-on lab is also included. The second edition contains three new chapters as well as changes and updates throughout.

This book is about programming the Intel(R) X86-X64 in assembly language using the "free" version of Microsoft(R) Visual Studio 17 software. The X86 implies the 16-bit legacy Intel(R) 8086 processor up through the 64-bit Intel(R) core i7 and even beyond. Program in assembly starting with simple and basic programs, all the way up to AVX programming. By the end of this book, you will be able to write and read assembly code, mix assembly with higher level languages, know what AVX is, and a lot more than that. The code used in Beginning x64 Assembly Programming is kept as simple as possible, which means: no graphical user interfaces or whistles and bells or error checking. Adding all these nice features would distract your attention from the purpose:

learning assembly language. The theory is limited to a strict minimum: a little bit on binary numbers, a short presentation of logical operators, and some limited linear algebra. And we stay far away from doing floating point conversions. The assembly code is presented in complete programs, so that you can test them on your computer, play with them, change them, break them. This book will also show you what tools can be used, how to use them, and the potential problems in those tools. It is not the intention to give you a comprehensive course on all of the assembly instructions, which is impossible in one book: look at the size of the Intel Manuals. Instead, the author will give you a taste of the main items, so that you will have an idea about what is going on. If you work through this book, you will acquire the knowledge to investigate certain domains more in detail on your own. The majority of the book is dedicated to assembly on Linux, because it is the easiest platform to learn assembly language. At the end the author provides a number of chapters to get you on your way with assembly on Windows. You will see that once you have Linux assembly under your belt, it is much easier to take on Windows assembly. This book should not be the first book you read on programming, if you have never programmed before, put this book aside for a while and learn some basics of programming with a higher-level language such as C. What You Will Learn Discover how a CPU and memory works Appreciate how a computer and operating system work together See how high-level language compilers generate machine language, and use that knowledge to write more efficient code Be better equipped to analyze bugs in your programs Get your program working, which is the fun part Investigate malware and take the necessary actions and precautions Who This Book Is For Programmers in high level languages. It is also for systems engineers and security engineers working for malware investigators. Required knowledge: Linux, Windows, virtualization, and higher level programming languages (preferably C or C++).

The eagerly anticipated new edition of the bestselling introduction to x86 assembly language The long-awaited third edition of this bestselling introduction to assembly language has been completely rewritten to focus on 32-bit protected-mode Linux and the free NASM assembler. Assembly is the fundamental language bridging human ideas and the pure silicon hearts of computers, and popular author Jeff Dunteman retains his distinctive lighthearted style as he presents a step-by-step approach to this difficult technical discipline. He starts at the very beginning, explaining the basic ideas of programmable computing, the binary and hexadecimal number systems, the Intel x86 computer architecture, and the process of software development under Linux. From that foundation he systematically treats the x86 instruction set, memory addressing, procedures, macros, and interface to the C-language code libraries upon which Linux itself is built. Serves as an ideal introduction to x86 computing concepts, as demonstrated by the only language directly understood by the CPU itself Uses an approachable, conversational style that assumes no prior experience in programming of any kind Presents x86 architecture and assembly concepts through a cumulative tutorial approach that is ideal for self-paced instruction Focuses entirely on free, open-source software, including Ubuntu Linux, the NASM assembler, the Kate editor, and the Gdb/Insight debugger Includes an x86 instruction set reference for the most common machine instructions, specifically tailored for use by programming beginners Woven into the presentation are plenty of assembly code examples, plus practical tips on software design, coding, testing, and debugging, all using free, open-source software that

may be downloaded without charge from the Internet.

If you're a developer or system administrator lured to Mac OS X because of its Unix roots, you'll quickly discover that performing Unix tasks on a Mac is different than what you're accustomed to. Mac OS X for Unix Geeks serves as a bridge between Apple's Darwin OS and the more traditional Unix systems. This clear, concise guide gives you a tour of Mac OS X's Unix shell in both Leopard and Tiger, and helps you find the facilities that replace or correspond to standard Unix utilities. You'll learn how to perform common Unix tasks in Mac OS X, such as using Directory Services instead of the standard Unix /etc/passwd and /etc/group, and you'll be able to compile code, link to libraries, and port Unix software using either Leopard and Tiger. This book teaches you to: Navigate the Terminal and understand how it differs from an xterm Use Open Directory (LDAP) and NetInfo as well as Directory Services Compile your code with GCC 4 Port Unix programs to Mac OS X with Fink Use MacPorts to install free/open source software Search through metadata with Spotlight's command-line utilities Build the Darwin kernel And there's much more. Mac OS X for Unix Geeks is the ideal survival guide to tame the Unix side of Leopard and Tiger. If you're a Unix geek with an interest in Mac OS X, you'll soon find that this book is invaluable.

Simulation of computer architectures has made rapid progress recently. The primary application areas are hardware/software performance estimation and optimization as well as functional and timing verification. Recent, innovative technologies such as retargetable simulator generation, dynamic binary translation, or sampling simulation have enabled widespread use of processor and system-on-chip (SoC) simulation tools in the semiconductor and embedded system industries. Simultaneously, processor and SoC simulation is still a very active research area, e.g. what amounts to higher simulation speed, flexibility, and accuracy/speed trade-offs. This book presents and discusses the principle technologies and state-of-the-art in high-level hardware architecture simulation, both at the processor and the system-on-chip level.

What people are saying about C# 4.0 in a Nutshell "C# 4.0 in a Nutshell is one of the few books I keep on my desk as a quick reference. It is a book I recommend."--Scott Guthrie, Corporate Vice President, .NET Developer Platform, Microsoft Corporation "A must-read for a concise but thorough examination of the parallel programming features in the .NET Framework 4."--Stephen Toub, Parallel Computing Platform Program Manager, Microsoft "This wonderful book is a great reference for developers of all levels."--Chris Burrows, C# Compiler Team, Microsoft When you have questions about how to use C# 4.0 or the .NET CLR, this highly acclaimed bestseller has precisely the answers you need. Uniquely organized around concepts and use cases, this fourth edition includes in-depth coverage of new C# topics such as parallel programming, code contracts, dynamic programming, security, and COM interoperability. You'll also find updated information on LINQ, including examples that work with both LINQ to SQL and Entity Framework. This book has all the essential details to keep you on track with C# 4.0. Get up to speed on C# language basics, including syntax, types, and variables Explore advanced topics such as unsafe code and preprocessor directives Learn C# 4.0 features such as dynamic binding, type parameter variance, and optional and named parameters Work with .NET 4's rich set of features for parallel programming, code contracts, and the code security model Learn .NET topics, including XML, collections, I/O

and networking, memory management, reflection, attributes, security, and native interoperability

Analyzing how hacks are done, so as to stop them in thefuture Reverse engineering is the process of analyzing hardware orsoftware and understanding it, without having access to the sourcecode or design documents. Hackers are able to reverse engineersystems and exploit what they find with scary results. Now the goodguys can use the same tools to thwart these threats. PracticalReverse Engineering goes under the hood of reverse engineeringfor security analysts, security engineers, and system programmers,so they can learn how to use these same processes to stop hackersin their tracks. The book covers x86, x64, and ARM (the first book to cover allthree); Windows kernel-mode code rootkits and drivers; virtualmachine protection techniques; and much more. Best of all, itoffers a systematic approach to the material, with plenty ofhands-on exercises and real-world examples. Offers a systematic approach to understanding reverseengineering, with hands-on exercises and real-world examples Covers x86, x64, and advanced RISC machine (ARM) architecturesas well as deobfuscation and virtual machine protectiontechniques Provides special coverage of Windows kernel-mode code(rootkits/drivers), a topic not often covered elsewhere, andexplains how to analyze drivers step by step Demystifies topics that have a steep learning curve Includes a bonus chapter on reverse engineering tools Practical Reverse Engineering: Using x86, x64, ARM, WindowsKernel, and Reversing Tools provides crucial, up-to-dateguidance for a broad range of IT professionals.

Use Windows debuggers throughout the development cycle—and build better software Rethink your use of Windows debugging and tracing tools—and learn how to make them a key part of test-driven software development. Led by a member of the Windows Fundamentals Team at Microsoft, you'll apply expert debugging and tracing techniques—and sharpen your C++ and C# code analysis skills—through practical examples and common scenarios. Learn why experienced developers use debuggers in every step of the development process, and not just when bugs appear. Discover how to: Go behind the scenes to examine how powerful Windows debuggers work Catch bugs early in the development cycle with static and runtime analysis tools Gain practical strategies to tackle the most common code defects Apply expert tricks to handle user-mode and kernel-mode debugging tasks Implement postmortem techniques such as JIT and dump debugging Debug the concurrency and security aspects of your software Use debuggers to analyze interactions between your code and the operating system Analyze software behavior with Xperf and the Event Tracing for Windows (ETW) framework

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!

Advanced Windows DebuggingPearson Education

Written by the founder of DumpAnalysis.org, this resource can help technical support and escalation engineers and Windows software testers without the knowledge of assembly language master necessary prerequisites to understand and start debugging and crash dump analysis on X64 Windows platforms.

Rootkits and Bootkits will teach you how to understand and counter sophisticated, advanced threats buried deep in a machine's boot process or UEFI firmware. With the aid of numerous case studies and professional research from three of the world's leading security experts, you'll trace malware development over time from rootkits like TDL3 to present-day UEFI implants and examine how they infect a system, persist through reboot, and evade security software. As you inspect and dissect real malware, you'll learn: • How Windows boots—including 32-bit, 64-bit, and UEFI mode—and where to find vulnerabilities • The details of boot process security mechanisms like Secure Boot, including an overview of Virtual Secure Mode (VSM) and Device Guard • Reverse engineering and forensic techniques for analyzing real malware, including bootkits like Rovnix/Carberp, Gapz, TDL4, and the infamous rootkits TDL3 and Festi • How to perform static and dynamic analysis using emulation and tools like Bochs and IDA Pro • How to better understand the delivery stage of threats against BIOS and UEFI firmware in order to create detection capabilities • How to use virtualization tools like VMware Workstation to reverse engineer bootkits and the Intel Chipsec tool to dig into forensic analysis Cybercrime syndicates and malicious actors will continue to write ever more persistent and covert attacks, but the game is not lost. Explore the cutting edge of malware analysis with Rootkits and Bootkits. Covers boot processes for Windows 32-bit and 64-bit operating systems.