Ios 11 2 Jailbreak Pangu

Yatharth, an intelligent ïover-achiever' is very clear about his life's goal ? research. However, he faces a new challenge ? a girl! Will Yatharth be able to face this challenge and continue with his life's goal? With friends such as Mr. intelligent Sudeep, Mr. handsome-funny-But still not datable Vikalp, the style icon Samantha and the counselor friend Prathishtha, Yatharth has all the support that he doesn't need!Sanchita, a sentimental girl is all beauty but takes life seriously. Will she be able to handle the challenges she is about to face with love entering her life? ïMy Ex fell in love!' is a hilarious tale of growing up and dealing with the consequent challenges of life in a unique way. Enjoy the light, humorous and witty story of these youngsters, which will bring a smile on your face.

A practical guide to analyzing iOS devices with the latest forensics tools and techniques About This Book This book is a comprehensive update to Learning iOS Forensics This practical book will not only cover the critical aspects of digital forensics, but also mobile forensics Whether you're a forensic analyst or an iOS developer, there's something in this book for you The authors, Mattia Epifani and Pasquale Stirparo, are respected members of the community, they go into extensive detail to cover critical topics Who This Book Is For The book is for digital forensics analysts, incident response analysts, IT security experts, and malware analysts. It would be beneficial if you have basic knowledge of forensics What You Will Learn Identify an iOS device between various models (iPhone, iPad, iPod Touch) and verify the iOS version installed Crack or bypass the protection passcode chosen by the user Acquire, at the most detailed level, the content of an iOS Device (physical, advanced logical, or logical) Recover information from a local backup and eventually crack the backup password Download back-up information stored on iCloud Analyze system, user, and third-party information from a device, a backup, or iCloud Examine malicious apps to identify data and credential thefts In Detail Mobile forensics is used within many different domains, but is chiefly employed in the field of information security. By understanding common attack vectors and vulnerability points, security professionals can develop measures and examine system architectures to harden security on iOS devices. This book is a complete manual on the identification, acquisition, and analysis of iOS devices, updated to iOS 8 and 9. You will learn by doing, with various case studies. The book covers different devices, operating system, and apps. There is a completely renewed section on third-party apps with a detailed analysis of the most interesting artifacts. By investigating compromised devices, you can work out the identity of the attacker, as well as what was taken, when, why, where, and how the attack was conducted. Also you will learn in detail about data security and application security that can assist forensics investigators and application developers. It will take hands-on approach to solve complex problems of digital forensics as well as mobile forensics. Style and approach This book provides a step-by-step approach that will guide you through one topic at a time. This intuitive guide focuses on one key topic at a time. Building upon the acquired knowledge in each chapter, we will connect the fundamental theory and practical tips by illustrative visualizations and hands-on code examples.

Become an effective cyber forensics investigator and gain a collection of practical, efficient techniques to get the job done. Diving straight into a discussion of anti-forensic techniques, this book shows you the many ways to effectively detect them. Now that you know what you are looking for, you'll shift your focus to network forensics, where you cover the various tools available to make your network forensics process less complicated. Following this, you will work with cloud and mobile forensic techniques by considering the concept of forensics as a service (FaSS), giving you cutting-edge skills that will future-proof your career. Building on this, you will learn the process of breaking down malware attacks, web attacks, and email scams with case studies to give you a clearer view of the techniques to be followed. Another tricky

technique is SSD forensics, so the author covers this in detail to give you the alternative analysis techniques you'll need. To keep you up to speed on contemporary forensics, Practical Cyber Forensics includes a chapter on Bitcoin forensics, where key crypto-currency forensic techniques will be shared. Finally, you will see how to prepare accurate investigative reports. What You Will Learn Carry out forensic investigation on Windows, Linux, and macOS systems Detect and counter anti-forensic techniques Deploy network, cloud, and mobile forensics Investigate web and malware attacks Write efficient investigative reports Who This Book Is For Intermediate infosec professionals looking for a practical approach to investigative cyber forensics techniques.

Explore real-world threat scenarios, attacks on mobile applications, and ways to counter them About This Book Gain insights into the current threat landscape of mobile applications in particular Explore the different options that are available on mobile platforms and prevent circumventions made by attackers This is a step-by-step guide to setting up your own mobile penetration testing environment Who This Book Is For If you are a mobile application evangelist, mobile application developer, information security practitioner, penetration tester on infrastructure web applications, an application security professional, or someone who wants to learn mobile application security as a career, then this book is for you. This book will provide you with all the skills you need to get started with Android and iOS pen-testing. What You Will Learn Gain an in-depth understanding of Android and iOS architecture and the latest changes Discover how to work with different tool suites to assess any application Develop different strategies and techniques to connect to a mobile device Create a foundation for mobile application security principles Grasp techniques to attack different components of an Android device and the different functionalities of an iOS device Get to know secure development strategies for both iOS and Android applications Gain an understanding of threat modeling mobile applications Get an in-depth understanding of both Android and iOS implementation vulnerabilities and how to provide counter-measures while developing a mobile app In Detail Mobile security has come a long way over the last few years. It has transitioned from "should it be done?" to "it must be done!"Alongside the growing number of devises and applications, there is also a growth in the volume of Personally identifiable information (PII), Financial Data, and much more. This data needs to be secured. This is why Pen-testing is so important to modern application developers. You need to know how to secure user data, and find vulnerabilities and loopholes in your application that might lead to security breaches. This book gives you the necessary skills to security test your mobile applications as a beginner, developer, or security practitioner. You'll start by discovering the internal components of an Android and an iOS application. Moving ahead, you'll understand the inter-process working of these applications. Then you'll set up a test environment for this application using various tools to identify the loopholes and vulnerabilities in the structure of the applications. Finally, after collecting all information about these security loop holes, we'll start securing our applications from these threats. Style and approach This is an easy-to-follow guide full of hands-on examples of real-world attack simulations. Each topic is explained in context with respect to testing, and for the more inquisitive, there are more details on the concepts and techniques used for different platforms.

This book constitutes the thoroughly refereed roceedings of the 13th International Conference on Security and Privacy in Communications Networks, SecureComm 2017, held in Niagara Falls, ON, Canada, in October 2017.The 31 revised regular papers and 15 short papers were carefully reviewed and selected from 105 submissions. The topics range from security and privacy in machine learning to differential privacy, which are currently hot research topics in cyber security research.

Develop the capacity to dig deeper into mobile device data acquisitionAbout This Book*A mastering guide to help you overcome the roadblocks you face when dealing with mobile

forensics*Excel at the art of extracting data, recovering deleted data, bypassing screen locks, and much more*Get best practices to how to collect and analyze mobile device data and accurately document your investigationsWho This Book Is ForThe book is for mobile forensics professionals who have experience in handling forensic tools and methods. This book is designed for skilled digital forensic examiners, mobile forensic investigators, and law enforcement officers.What You Will Learn*Understand the mobile forensics process model and get guidelines on mobile device forensics*Acquire in-depth knowledge about smartphone acquisition and acquisition methods*Gain a solid understanding of the architecture of operating systems, file formats, and mobile phone internal memory*Explore the topics of of mobile security, data leak, and evidence recovery*Dive into advanced topics such as GPS analysis, file carving, encryption, encoding, unpacking, and decompiling mobile application processesIn DetailMobile forensics presents a real challenge to the forensic community due to the fast and unstoppable changes in technology. This book aims to provide the forensic community an in-depth insight into mobile forensic techniques when it comes to deal with recent smartphones operating systemsStarting with a brief overview of forensic strategies and investigation procedures, you will understand the concepts of file carving, GPS analysis, and string analyzing. You will also see the difference between encryption, encoding, and hashing methods and get to grips with the fundamentals of reverse code engineering. Next, the book will walk you through the iOS, Android and Windows Phone architectures and filesystem, followed by showing you various forensic approaches and data gathering techniques.You will also explore advanced forensic techniques and find out how to deal with third-applications using case studies. The book will help you master data acquisition on Windows Phone 8. By the end of this book, you will be acquainted with best practices and the different models used in mobile forensics.

We are pleased to present herein the proceedings of the 13th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2018) held in Incheon, Korea, June 4-8, 2018. ASIACCS 2018 is organized by AsiaCCS 2018 organizing committee, supported by ACM SigSAC, Korea Institute of Information Security &Cryptography (KIISC). We received 310 submissions. This year's Program Committee comprising 103 security researchers from 24 countries, helped by 73 external reviewers, evaluated these submissions through thoughtful discussion and rigorous review procedure. The review process resulted in 52 full papers being accepted to the program, representing an acceptance rate of about 17%. In addition, 10 short papers and 15 posters are also included in the program. Once again we have a very strong technical program along with 5 specialized pre-conference workshops: CPSS'18, APKC'18, RESEC'18, BBC'18, and SCC'18. We are also fortunate to have distinguished invited speakers, Dr. Cliff Wang, Dr. Jaeyeon Jung, and Prof. Kevin Fu, who will provide various insights into Cyber Deception: an emergent research area, Securing a large scale IoT ecosystem, and Analog Sensor Cybersecurity and Transduction Attacks, respectively. These valuable and insightful talks can and will guide us to a better understanding on both fundamental and emerging topic areas in the field of information, computer and communications security.

Unleash your creative potential and start producing hip hop music today. This beginner’s guide breaks down the basics of music production and gives you the tools to start creating. Beat making isn’t a linear process, and there’s no exact science or method. Slime Green Beats provides a complete overview of the equipment, strategy, and mentality that you need to produce mind-blowing music, all without stifling your creativity. Whether you’re looking to produce your own music or start a career in music production, this handbook is a must-have. Learn beat making rules for different genres and musical styles, including hip hop, trap, R&B, and rap. You’ll learn: Setup - How to set up your home beat making studio - Tips for sound selection and melody creation - What drum layers make up a hip-hop beat - The stylistic

difference between 808s and basslines Finishing - An introduction to mixing instrumentals - How to create vibrant, clean beats without over-compressing - Music theory rules for arranging - How to find and implement reliable feedback Sharing - Online marketing strategies for self-promotion - Email marketing tips to build industry connections - How to license, lease, and sell your beats - What to expect when selling exclusive beats, including track outs …And more! How to Make Beats explains music theory and technical software in easy-to-understand terms. The language of music production often feels elite, but Slime Green Beats breaks down barriers for new creators. Learn the lingo with an extensive terminology section in the back of the handbook and links to suggested resources. About the authors Slime Green Beats is led by 3E Wave and Stunna, two highly acclaimed music producers with an extensive fanbase on YouTube. With nearly a decade of beat making experience between them, their technical tips and recommendations are proven to work in the real world.

Unearth some of the most significant attacks threatening iOS applications in recent times and learn methods of patching them to make payment transactions and personal data sharing more secure. When it comes to security, iOS has been in the spotlight for a variety of reasons. Although a tough system to manipulate, there are still critical security bugs that can be exploited. In response to this issue, author Kunal Relan offers a concise, deep dive into iOS security, including all the tools and methods to master reverse engineering of iOS apps and penetration testing. What you will learn: • Get a deeper understanding of iOS infrastructure and architecture• Obtain deep insights of iOS security and jailbreaking• Master reverse engineering techniques for securing your iOS Apps• Discover the basics of application development for iOS• Employ security best practices for iOS applications Who is this book for: Security professionals, Information Security analysts, iOS reverse engineers, iOS developers, and readers interested in secure application development in iOS.

This open access book provides the first comprehensive collection of papers that provide an integrative view on cybersecurity. It discusses theories, problems and solutions on the relevant ethical issues involved. This work is sorely needed in a world where cybersecurity has become indispensable to protect trust and confidence in the digital infrastructure whilst respecting fundamental values like equality, fairness, freedom, or privacy. The book has a strong practical focus as it includes case studies outlining ethical issues in cybersecurity and presenting guidelines and other measures to tackle those issues. It is thus not only relevant for academics but also for practitioners in cybersecurity such as providers of security software, governmental CERTs or Chief Security Officers in companies.

Covering up-to-date mobile platforms, this book focuses on teaching you the most recent tools and techniques for investigating mobile devices. Readers will delve into a variety of mobile forensics techniques for iOS 11-13, Android 8-10 devices, and Windows 10.

iPhone and iOS Forensics is a guide to the forensic acquisition and analysis of iPhone and iOS devices, and offers practical advice on how to secure iOS devices, data and apps. The book takes an in-depth look at methods and processes that analyze the iPhone/iPod in an official legal manner, so that all of

the methods and procedures outlined in the text can be taken into any courtroom. It includes information data sets that are new and evolving, with official hardware knowledge from Apple itself to help aid investigators. This book consists of 7 chapters covering device features and functions; file system and data storage; iPhone and iPad data security; acquisitions; data and application analysis; and commercial tool testing. This book will appeal to forensic investigators (corporate and law enforcement) and incident response professionals. Learn techniques to forensically acquire the iPhone, iPad and other iOS devices Entire chapter focused on Data and Application Security that can assist not only forensic investigators, but also application developers and IT security managers In-depth analysis of many of the common applications (both default and downloaded), including where specific data is found within the file system

Mobile Endgeräte, vor allem Smartphones und Tablets der Hersteller Apple und Google, sind inzwischen in fast jedem Haushalt vertreten. Auch in der Firmenwelt nehmen diese Geräte einen immer größeren Stellenwert ein und verarbeiten hochsensible Daten. Diese neuen Einsatzszenarien, gepaart mit Tausenden von Applikationen, schaffen neue Angriffsvektoren und Einfallstore in diese Geräte. Dieses Buch stellt die einzelnen Angriffsszenarien und Schwachstellen in den verwendeten Applikationen detailliert vor und zeigt, wie Sie diese Schwachstellen aufspüren können. Am Beispiel der aktuellen Betriebssysteme (Android, iOS und Windows Mobile) erhalten Sie einen umfassenden Einblick ins Penetration Testing von mobilen Applikationen. Sie lernen typische Penetration-Testing-Tätigkeiten kennen und können nach der Lektüre Apps der großen Hersteller untersuchen und deren Sicherheit überprüfen. Behandelt werden u.a. folgende Themen: - Forensische Untersuchung des Betriebssystems, - Reversing von mobilen Applikationen, - SQL-Injection- und Path-Traversal-Angriffe, - Runtime-Manipulation von iOS-Apps mittels Cycript, - Angriffe auf die HTTPS-Verbindung, - u.v.m. Vorausgesetzt werden fundierte Kenntnisse in Linux/Unix sowie erweiterte Kenntnisse in Java bzw. Objective-C.

With iPhone Hacks, you can make your iPhone do all you'd expect of a mobile smartphone -- and more. Learn tips and techniques to unleash little-known features, find and create innovative applications for both the iPhone and iPod touch, and unshackle these devices to run everything from network utilities to video game emulators. This book will teach you how to: Import your entire movie collection, sync with multiple computers, and save YouTube videos Remotely access your home network, audio, and video, and even control your desktop Develop native applications for the iPhone and iPod touch on Linux, Windows, or Mac Check email, receive MMS messages, use IRC, and record full-motion video Run any application in the iPhone's background, and mirror its display on a TV Make your iPhone emulate old-school video game platforms, and play classic console and arcade games Integrate your iPhone with your car stereo Build your own electronic bridges to connect keyboards, serial devices, and more to your iPhone without "jailbreaking" iPhone Hacks explains how to set up your iPhone

the way you want it, and helps you give it capabilities that will rival your desktop computer. This cunning little handbook is exactly what you need to make the most of your iPhone.

An in-depth look into Mac OS X and iOS kernels Powering Macs, iPhones, iPads and more, OS X and iOS are becoming ubiquitous. When it comes to documentation, however, much of them are shrouded in mystery. Cocoa and Carbon, the application frameworks, are neatly described, but system programmers find the rest lacking. This indispensable guide illuminates the darkest corners of those systems, starting with an architectural overview, then drilling all the way to the core. Provides you with a top down view of OS X and iOS Walks you through the phases of system startup—both Mac (EFi) and mobile (iBoot) Explains how processes, threads, virtual memory, and filesystems are maintained Covers the security architecture Reviews the internal Apis used by the system—BSD and Mach Dissects the kernel, XNU, into its sub components: Mach, the BSD Layer, and I/o kit, and explains each in detail Explains the inner workings of device drivers From architecture to implementation, this book is essential reading if you want to get serious about the internal workings of Mac OS X and iOS.

A collection of large—scale problems for “learning by doing.” With detailed and careful analysis of the real world situations surrounding common programming problems. -- Back cover.

Practical Mobile ForensicsForensically investigate and analyze iOS, Android, and Windows 10 devices, 4th EditionPackt Publishing Ltd

This book provides authoritative information on the theory behind the Macintosh 'look and feel' and the practice of using individual interface components. It includes many examples of good design and explains why one implementation is superior to another. Anyone designing or creating a product for Macintosh computers needs to understand the information in this book.

If you’re an app developer with a solid foundation in Objective-C, this book is an absolute must—chances are very high that your company’s iOS applications are vulnerable to attack. That’s because malicious attackers now use an arsenal of tools to reverse-engineer, trace, and manipulate applications in ways that most programmers aren’t aware of. This guide illustrates several types of iOS attacks, as well as the tools and techniques that hackers use. You’ll learn best practices to help protect your applications, and discover how important it is to understand and strategize like your adversary. Examine subtle vulnerabilities in real-world applications—and avoid the same problems in your apps Learn how attackers infect apps with malware through code injection Discover how attackers defeat iOS keychain and data-protection encryption Use a debugger and custom code injection to manipulate the runtime Objective-C environment Prevent attackers from hijacking SSL sessions and stealing traffic Securely delete files and design your apps to prevent forensic data leakage Avoid debugging abuse, validate the integrity of run-time classes, and make your code harder to trace

Secure your iOS applications and uncover hidden vulnerabilities by conducting

penetration tests About This Book Achieve your goal to secure iOS devices and applications with the help of this fast paced manual Find vulnerabilities in your iOS applications and fix them with the help of this example-driven guide Acquire the key skills that will easily help you to perform iOS exploitation and forensics with greater confidence and a stronger understanding Who This Book Is For This book is for IT security professionals who want to conduct security testing of applications. This book will give you exposure to diverse tools to perform penetration testing. This book will also appeal to iOS developers who would like to secure their applications, as well as security professionals. It is easy to follow for anyone without experience of iOS pentesting. What You Will Learn Understand the basics of iOS app development, deployment, security architecture, application signing, application sandboxing, and OWASP TOP 10 for mobile Set up your lab for iOS app pentesting and identify sensitive information stored locally Perform traffic analysis of iOS devices and catch sensitive data being leaked by side channels Modify an application's behavior using runtime analysis Analyze an application's binary for security protection Acquire the knowledge required for exploiting iOS devices Learn the basics of iOS forensics In Detail iOS has become one of the most popular mobile operating systems with more than 1.4 million apps available in the iOS App Store. Some security weaknesses in any of these applications or on the system could mean that an attacker can get access to the device and retrieve sensitive information. This book will show you how to conduct a wide range of penetration tests on iOS devices to uncover vulnerabilities and strengthen the system from attacks. Learning iOS Penetration Testing discusses the common vulnerabilities and security-related shortcomings in an iOS application and operating system, and will teach you to conduct static and dynamic analysis of iOS applications. This practical guide will help you uncover vulnerabilities in iOS phones and applications. We begin with basics of iOS security and dig deep to learn about traffic analysis, code analysis, and various other techniques. Later, we discuss the various utilities, and the process of reversing and auditing. Style and approach This fast-paced and practical guide takes a step-by-step approach to penetration testing with the goal of helping you secure your iOS devices and apps quickly.

‘Don’t cry.’ Christoph uncurled her clenched fingers. ‘You know why you must work for him: to keep your real work away from your family, to keep them safe so that, if you get caught, they won’t be taken. One day you’ll be able to tell them all of that.’ Germany 1940. As secretary to an influential businessman, Magda Aderbach spends her days sending party invitations to high-ranking Nazis, and her evenings distributing pamphlets for the resistance. When she is approached about a job by the leader of the SS, Magda embarks upon a dangerous double life smuggling secrets out of his office. It’s a deadly game, and eventual exposure is a certainty, but Magda is driven by a need to keep the man she loves safe as he fights against the Nazis… Forty years later. Nina Dahlke’s heart pounds as she leaves everything she has ever known and steps into an uncertain future carrying a forged passport, a few Deutschmarks, and the image of an ornate stone villa, The Tower House, seared into her memory. She has never forgotten the fear in her grandmother’s voice when Nina found the drawing of the elegant building hidden in her wardrobe. And now, with nothing left to lose, Nina is determined to uncover the past her grandmother ran from. But not even Nina’s wildest imaginings come close to the truth that she discovers when she reaches her

destination… A haunting and poignant novel about bravery, loss and redemption during the second World War. A beautiful read for fans of The Tattooist of Auschwitz, We Were the Lucky Ones and The Alice Network. What readers are saying about Catherine Hokin: ????? ‘The best historical fiction book I’ve read this year! I was awake until the early morning hours finishing it, because I could not put it down!… Heartbreaking.’ Goodreads reviewer ????? ‘What an amazing read… I was totally absorbed in the story and I would love to give it 10 stars. One of my best reads this year. I can’t begin to say how much I loved this book, I couldn’t put it down, absolutely brilliant.’ Goodreads reviewer ????? ‘If I could give this book more than a five-star rating, I surely would! It is absolutely the best WW2 historical fiction I’ve read in a long time!… I couldn’t bear to put it down.’ Goodreads reviewer ????? ‘Can I give a rating higher than 5 stars?!… I really loved this book.’ Goodreads reviewer ????? ‘Have you ever read a book that has torn at your heartstrings so much that you just know it’s going to leave a lasting impression for the rest of time?… This book is going on that list!’ Goodreads reviewer ????? ‘This story just swept me away… I was left speechless… just wow!!… I do recommend a box of tissues… This book will have you turning the pages.’ Red Headed Book Lady blog ????? ‘The more I read of this book, the more I had to read! What a fantastic story this is touching just about every emotion there is.’ Goodreads reviewer ????? ‘A wonderfully heartbreaking story of life, love and above all survival. A truly emotional book and very hard to put down. 5*.’ Goodreads reviewer ????? ‘Captivating. Sobering. Unflinching. 5+ stars.’ Goodreads reviewer ????? ‘Squeezed my cold heart… I was turned inside out yet completely invested and unwilling to put my Kindle down while compelled to read late into the night.’ Goodreads reviewer ????? ‘What an extraordinary, engaging story. It moved me to undiscovered heights of understanding and compassion. A novel that will stay in my mind forever.’ Goodreads reviewer

DON’T JUNK IT, FIX IT--AND SAVE A FORTUNE! The only reference & tutorial of its kind--in full color! Fix your own iPhone, iPad, or iPod with secret repair knowledge Apple doesn’t want you to have! This groundbreaking, full-color book shows you how to resurrect expensive Apple mobile iDevices you thought were dead for good, and save a fortune. Apple Certified Repair Technician Timothy L. Warner demystifies everything about iDevice repair, presenting simple, step-by-step procedures and hundreds of crisp, detailed, full-color photos. He’ll walk you through safely taking apart your iDevice, replacing what’s broken, and reliably reassembling it. You’ll learn where to get the tools and exactly how to use them. Warner even reveals sources for broken Apple devices you can fix at low cost--for yourself, or even for resale! Replace All These iDevice Components: • Battery • Display • SIM card • Logic board • Dock connector Take Apart, Fix, and Reassemble: • iPod nano (5th & 7th Gen) • iPod touch (4th & 5th Gen) • iPhone (3GS, 4, 4S, & 5) • iPad (iPad 2, iPad 4th Gen, & iPad mini) Fix Common Software-Related Failures: • Emergency data recovery • Jailbreaking • Carrier unlocking Do What Apple Never Intended: • Resurrect a waterlogged iDevice • Prepare an iDevice for resale • Install non-Apple Store apps • Perform out-of-warranty repairs All technical content reviewed & approved by iFixit, world leader in iDevice parts, tools, and repair tutorials!

If you are a security professional, pentester, or anyone interested in getting to grips with wireless penetration testing, this is the book for you. Some familiarity with Kali Linux

and wireless concepts is beneficial.

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.

See your app through a hacker's eyes to find the real sources of vulnerability The Mobile Application Hacker's Handbook is a comprehensive guide to securing all mobile applications by approaching the issue from a hacker's point of view. Heavily practical, this book provides expert guidance toward discovering and exploiting flaws in mobile applications on the iOS, Android, Blackberry, and Windows Phone platforms. You will learn a proven methodology for approaching mobile application assessments, and the techniques used to prevent, disrupt, and remediate the various types of attacks. Coverage includes data storage, cryptography, transport layers, data leakage, injection attacks, runtime manipulation, security controls, and cross-platform apps, with vulnerabilities highlighted and detailed information on the methods hackers use to get around standard security. Mobile applications are widely used in the consumer and enterprise markets to process and/or store sensitive data. There is currently little published on the topic of mobile security, but with over a million apps in the Apple App Store alone, the attack surface is significant. This book helps you secure mobile apps by demonstrating the ways in which hackers exploit weak points and flaws to gain access to data. Understand the ways data can be stored, and how cryptography is defeated Set up an environment for identifying insecurities and the data leakages that arise Develop extensions to bypass security controls and perform injection attacks Learn the different attacks that apply specifically to cross-platform apps IT security breaches have made big headlines, with millions of consumers vulnerable as major corporations come under attack. Learning the tricks of the hacker's trade allows security professionals to lock the app up tight. For better mobile security and less vulnerable data, The Mobile Application Hacker's Handbook is a practical, comprehensive guide.

"This book is a must for anyone attempting to examine the iPhone. The level of forensic detail is excellent. If only all guides to forensics were written with this clarity!"-Andrew Sheldon,

Director of Evidence Talks, computer forensics experts With iPhone use increasing in business networks, IT and security professionals face a serious challenge: these devices store an enormous amount of information. If your staff conducts business with an iPhone, you need to know how to recover, analyze, and securely destroy sensitive data. iPhone Forensics supplies the knowledge necessary to conduct complete and highly specialized forensic analysis of the iPhone, iPhone 3G, and iPod Touch. This book helps you: Determine what type of data is stored on the device Break v1.x and v2.x passcode-protected iPhones to gain access to the device Build a custom recovery toolkit for the iPhone Interrupt iPhone 3G's "secure wipe" process Conduct data recovery of a v1.x and v2.x iPhone user disk partition, and preserve and recover the entire raw user disk partition Recover deleted voicemail, images, email, and other personal data, using data carving techniques Recover geotagged metadata from camera photos Discover Google map lookups, typing cache, and other data stored on the live file system Extract contact information from the iPhone's database Use different recovery strategies based on case needs And more. iPhone Forensics includes techniques used by more than 200 law enforcement agencies worldwide, and is a must-have for any corporate compliance and disaster recovery plan.

The book is an easy-to-follow guide with clear instructions on various mobile forensic techniques. The chapters and the topics within are structured for a smooth learning curve, which will swiftly empower you to master mobile forensics. If you are a budding forensic analyst, consultant, engineer, or a forensic professional wanting to expand your skillset, this is the book for you. The book will also be beneficial to those with an interest in mobile forensics or wanting to find data lost on mobile devices. It will be helpful to be familiar with forensics in general but no prior experience is required to follow this book.

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Networked computing, wireless communications and portable electronic devices have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence. Digital forensics also has myriad intelligence applications. Furthermore, it has a vital role in information assurance -- investigations of security breaches yield valuable information that can be used to design more secure systems. Advances in Digital Forensics XI describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: Themes and Issues Internet Crime Investigations Forensic Techniques Mobile Device Forensics Cloud Forensics Forensic Tools This book is the eleventh volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and prac tice in digital forensics. The book contains a selection of twenty edited papers from the Eleventh Annual IFIP WG 11.9 International Conference on Digital Forensics, held in Orlando, Florida in the winter of 2015. Advances in Digital Forensics XI is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities. Gilbert Peterson, Chair, IFIP WG 11.9 on Digital Forensics, is a Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA. Sujeet Shenoi is the F.P. Walter Professor of Computer Science and a Professor of Chemical Engineering at the University of Tulsa, Tulsa, Oklahoma, USA.

Core Animation is the technology underlying Apple's iOS user interface. By unleashing the full power of Core Animation, you can enhance your app with impressive 2D and 3D visual effects

and create exciting and unique new interfaces. In this in-depth guide, iOS developer Nick Lockwood takes you step-by-step through the Core Animation framework, building up your understanding through sample code and diagrams together with comprehensive explanations and helpful tips. Lockwood demystifies the Core Animation APIs, and teaches you how to make use of Layers and views, software drawing and hardware compositing Layer geometry, hit testing and clipping Layer effects, transforms and 3D interfaces Video playback, text, tiled images, OpenGL, particles and reflections Implicit and explicit animations Property animations, keyframes and transitions Easing, frame-by-frame animation and physics Performance tuning and much, much more! Approximately 356 pages.

Mac OS X was released in March 2001, but many components, such as Mach and BSD, are considerably older. Understanding the design, implementation, and workings of Mac OS X requires examination of several technologies that differ in their age, origins, philosophies, and roles. Mac OS X Internals: A Systems Approach is the first book that dissects the internals of the system, presenting a detailed picture that grows incrementally as you read. For example, you will learn the roles of the firmware, the bootloader, the Mach and BSD kernel components (including the process, virtual memory, IPC, and file system layers), the object-oriented I/O Kit driver framework, user libraries, and other core pieces of software. You will learn how these pieces connect and work internally, where they originated, and how they evolved. The book also covers several key areas of the Intel-based Macintosh computers. A solid understanding of system internals is immensely useful in design, development, and debugging for programmers of various skill levels. System programmers can use the book as a reference and to construct a better picture of how the core system works. Application programmers can gain a deeper understanding of how their applications interact with the system. System administrators and power users can use the book to harness the power of the rich environment offered by Mac OS X. Finally, members of the Windows, Linux, BSD, and other Unix communities will find the book valuable in comparing and contrasting Mac OS X with their respective systems. Mac OS X Internals focuses on the technical aspects of OS X and is so full of extremely useful information and programming examples that it will definitely become a mandatory tool for every Mac OS X programmer.

In his landmark bestseller Listening to Prozac, Peter Kramer revolutionized the way we think about antidepressants and the culture in which they are so widely used. Now Kramer offers a frank and unflinching look at the condition those medications treat: depression. Definitively refuting our notions of "heroic melancholy," he walks readers through groundbreaking new research—studies that confirm depression's status as a devastating disease and suggest pathways toward resilience. Thought-provoking and enlightening, Against Depression provides a bold revision of our understanding of mood disorder and promises hope to the millions who suffer from it.

Recently, mobile security has garnered considerable interest in both the research community and industry due to the popularity of smartphones. The current smartphone platforms are open systems that allow application development, also for malicious parties. To protect the mobile device, its user, and other mobile ecosystem stakeholders such as network operators, application execution is controlled by a platform security architecture. This book explores how such mobile platform security architectures work. We present a generic model for mobile platform security architectures: the model illustrates commonly used security mechanisms and techniques in mobile devices and allows a systematic comparison of different platforms. We analyze several mobile platforms using the model. In addition, this book explains hardware-security mechanisms typically present in a mobile device. We also discuss enterprise security extensions for mobile platforms and survey recent research in the area of mobile platform security. The objective of this book is to provide a comprehensive overview of the current status of mobile platform security for students, researchers, and practitioners. Table of

Contents: Preface / Introduction / Platform Security Model / Mobile Platforms / Platform Comparison / Mobile Hardware Security / Enterprise Security Extensions / Platform Security Research / Conclusions / Bibliography / Authors' Biographies

Given today’s fast paced world of tweets, texts and barely scratching the surface news reporting inside an ever increasing deluge of information, the average individual investor faces the growing challenge of having to cut through the clutter and decipher what it means to understand how, where and why they should be investing given the current environment and what lies ahead. This book will teach readers how to: Read the economy like a professional investor Filter out all the useless and misleading data Recognize the investable signal and identify which company or companies stand to benefit Identify both cyclical and structural changes—like the Internet, mobility, social media and other forces—that have drastically altered business models This book will give you readers a lens through which they will be able to clearly see the actionable, observable and recognizable trends that surround them every day and help them build a profitable portfolio for the long run.

In this book, the editors explain how students enrolled in two digital forensic courses at their institution are exposed to experiential learning opportunities, where the students acquire the knowledge and skills of the subject-matter while also learning how to adapt to the ever-changing digital forensic landscape. Their findings (e.g., forensic examination of different IoT devices) are also presented in the book. Digital forensics is a topic of increasing importance as our society becomes “smarter” with more of the “things” around us been internet- and inter-connected (e.g., Internet of Things (IoT) and smart home devices); thus, the increasing likelihood that we will need to acquire data from these things in a forensically sound manner. This book is of interest to both digital forensic educators and digital forensic practitioners, as well as students seeking to learn about digital forensics.

Looks at the native environment of the iPhone and describes how to build software for the device.

This comprehensive exam guide offers 100% coverage of every topic on the CompTIA PenTest+ exam Get complete coverage of all the objectives included on the CompTIA PenTest+ certification exam PT0-001 from this comprehensive resource. Written by an expert penetration tester, the book provides learning objectives at the beginning of each chapter, hands-on exercises, exam tips, and practice questions with in-depth answer explanations. Designed to help you pass the exam with ease, this definitive volume also serves as an essential on-the-job reference. Covers all exam topics, including: •Pre-engagement activities •Getting to know your targets •Network scanning and enumeration •Vulnerability scanning and analysis •Mobile device and application testing •Social engineering •Network-based attacks •Wireless and RF attacks •Web and database attacks •Attacking local operating systems •Physical penetration testing •Writing the pen test report •And more Online content includes: •Interactive performance-based questions •Test engine that provides full-length practice exams or customized quizzes by chapter or by exam domain

Fearlessly change the design of your iOS code with solid unit tests. Use Xcode's built-in test framework XCTest and Swift to get rapid feedback on all your code - including legacy code. Learn the tricks and techniques of testing all iOS code, especially view controllers (UIViewControllers), which are critical to iOS apps. Learn to isolate and replace dependencies in legacy code written without tests. Practice safe refactoring that makes these tests possible, and watch all your changes get verified quickly and automatically. Make even the boldest code changes with complete confidence. Manual code and UI testing get slower the deeper your navigation hierarchy goes. It can take several taps just to reach a particular screen, never mind the actual workflow tests. Automatic unit testing offers such rapid feedback that it can change the rules of development. Bring testing to iOS development, even for legacy code. Use XCTest to write unit tests in Swift for all your code. iOS developers typically reserve unit tests for their

model classes alone. But that approach skips most of the code common to iOS apps, especially with UIViewControllers. Learn how to unit test these view controllers to expand your unit testing possibilities. Since good unit tests form the bedrock for safe refactoring, you're empowered to make bold changes. Learn how to avoid the most common mistakes Swift programmers make with the XCTest framework. Use code coverage to find holes in your test suites. Learn how to identify hard dependencies. Reshape the design of your code quickly, with less risk and less fear.

The perfect supplement to CEH Certified Ethical Hacker All-in-One Exam Guide, this practice exams book provides valuable test preparation for candidates preparing to pass the exam and achieve one of the fastest-growing information security credentials available. Designed as an exam-focused study-self aid and resource, CEH Certified Ethical Hacker Practice Exams offers practice test items from each domain of the latest CEH exam, and provides knowledge and scenario-based questions plus one case study-based Lab Question per chapter. In-depth answer explanations for both the correct and incorrect answers are included. The book contains more than 400 practice exam questions (in the book and electronic content) that match the actual exam questions in content and feel. The CEH Program certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective. A Certified Ethical Hacker is a skilled IT professional responsible for testing the weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker. Covers all exam topics, including intrusion detection, policy creation, social engineering, ddos attacks, buffer overflows, virus creation, and more Based on the 2011 CEH exam update Electronic content includes two complete practice exam simulations Market / Audience The Certified Ethical Hacker certification certifies the application knowledge of security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure. DOD 8570 workforce requirements include CEH as an approved commercial credential US-CERT's EBK and Certified Computer Security Incident Handler (CSIH) standards map to CEH CEH is an international, vendor-neutral certification that can be taken at any Prometric or VUE testing center worldwide. The exam costs $250. The Ethical Hacker is usually employed with the organization and can be trusted to undertake an attempt to penetrate networks and/or computer systems using the same methods as a Hacker. Hacking is a felony in the United States and most other countries. When it is done by request and under a contract between an Ethical Hacker and an organization, it is legal. The most important point is that an Ethical Hacker has authorization to probe the target. Matt Walker, CCNA, CCNP, MCSE, CEH, CNDA, CPTS (Ft. Lauderdale, FL) is the IA Training Instructor Supervisor and a Sr. IA Analyst at Dynetics, Inc., in Huntsville, Alabama. An IT education professional for over 15 years, Matt served as the Director of Network Training Center and the Curriculum Lead and Senior Instructor for the local Cisco Networking Academy on Ramstein AB, Germany. After leaving the US Air Force, Matt served as a Network Engineer for NASA's Secure Network Systems, designing and maintaining secured data, voice and video networking for the agency.

Discover all the security risks and exploits that can threateniOS-based mobile devices iOS is Apple's mobile operating system for the iPhone and iPad.With the introduction of iOS5, many security issues have come tolight. This book explains and discusses them all. The award-winningauthor team, experts in Mac and iOS security, examines thevulnerabilities and the internals of iOS to show how attacks can bemitigated. The book explains how the operating system works, itsoverall security architecture, and the security risks associatedwith it, as well as exploits, rootkits, and other payloadsdeveloped for it. Covers iOS security architecture, vulnerability hunting,exploit writing, and how iOS jailbreaks work Explores iOS enterprise and encryption, code signing and memoryprotection, sandboxing, iPhone fuzzing, exploitation, ROP payloads,and baseband attacks Also examines kernel debugging and exploitation

Companion website includes source code and tools to facilitateyour efforts iOS Hacker's Handbook arms you with the tools needed toidentify, understand, and foil iOS attacks.