Samsung Intercept Rooting Guide

In their Second Edition of Cases in Intelligence Analysis: Structured Analytic Techniques in Action, accomplished instructors and intelligence practitioners Sarah Miller Beebe and Randolph H. Pherson offer robust, class-tested cases studies of events in foreign intelligence, counterintelligence, terrorism, homeland security, law enforcement, and decision-making support. Designed to give analysts-in-training an opportunity to apply structured analytic techniques and tackle real-life problems, each turnkey case delivers a captivating narrative, discussion questions, recommended readings, and a series of engaging analytic exercises.

CISSP Study Guide, Third Edition provides readers with information on the CISSP certification, the most prestigious, globally-recognized, vendor-neutral exam for information security professionals. With over 100,000 professionals certified worldwide, and many more joining their ranks, this new third edition presents everything a reader needs to know on the newest version of the exam's Common Body of Knowledge. The eight domains are covered completely and as concisely as possible, allowing users to ace the exam. Each domain has its own chapter that includes a specially-designed pedagogy to help users pass the exam, including clearly-stated exam objectives, unique terms and definitions, exam warnings, "learning by example" modules, hands-on exercises, and chapter ending questions. Provides the most complete and effective study guide to prepare users for passing the CISSP exam, giving them exactly what they need to pass the test Authored by Eric Conrad who has prepared hundreds of professionals for passing the CISSP exam through SANS, a popular and well-known organization for information security professionals Covers all of the new information in the Common Body of Knowledge updated in January 2015, and also provides two exams, tiered end-of-chapter questions for a gradual learning curve, and a complete self-test appendix

The fourth edition of this bestselling book explains how to combine professional weather forecasts with information from self-assessment of the signs in the sky, as well as from websites and apps, to arrive at a local forecast of coming weather. The Weather Handbook is the essential guide to how the weather is formed, providing readers with the ability to look at the sky and interpret its signs. This handbook has been the standard reference for over 20 years for skippers and crews of cruising and racing yachts. The fourth edition has been updated and expanded with new photos and explanatory text, addressing new sources of weather information. There are countless websites and apps providing forecast data, and The Weather Handbook guides users in how to use and interpret this information for themselves, taking a general forecast for a wide area to provide a local forecast for a specific location. "The perfect introduction to understanding weather" - Practical Boat Owner

Alternative Investments: A Primer for Investment Professionals provides an overview of alternative investments for institutional asset allocators and other overseers of portfolios containing both traditional and alternative assets. It is designed for those with substantial experience regarding traditional investments in stocks and bonds but limited familiarity regarding alternative assets, alternative strategies, and alternative portfolio management. The primer categorizes alternative assets into four groups: hedge funds, real assets, private equity, and structured products/derivatives. Real assets include vacant land, farmland, timber, infrastructure, intellectual property, commodities, and private real estate. For each group, the primer provides essential information about the characteristics, challenges, and purposes of these institutional-quality alternative assets in the context of a well-diversified institutional portfolio. Other topics addressed by this primer include tail risk, due diligence of the investment process and operations, measurement and management of risks and returns, setting return expectations, and portfolio construction. The primer concludes with a chapter on the case for investing in alternatives.

This book is the poetic journey of a human being, going crazy in love. One of the most powerful reason for someone to go crazy is being in intense love. This book is the description of everything a human can possible feel and think of, in the different phases of his insanity in love. The different phases that has been described in the book are mergence, collision, mess, overthinking and then patience. Going crazy (that is a phrase I used for someone experiencing all of the above phases in sequence, is obviously an irregular phase of life that isn't static and where things doesn't make sense). Everything written in this book are the overwhelming thoughts, intense feelings, overthinking and chaotic scenarios one makes up in his mind while going crazy. But it always ends with a sunrise, always patience has its way to hug us and even though we aren't okay, we act okay. We have to, because going crazy for so long can kill us. Book is published with Auraq Publications. About Author Abu Bakr Zafar is a literature enthusiast, residing in Lahore. With immense hurdles in the way to be a student of literature before starting the journey as a writer, just like many other hurdles in his way due to absence of his father & being a one-man army in his life, he still made it happen for himself as he has always been passionate about studying literature not for studying it but to be a part of the literary world and consuming more knowledge about writing and reading. He published his first book "the speaking psycho" in late 2018 and continued his six books journey till the middle of 2020. All of those books were read by thousands of people that was unexpected for him. He did it all without any guidance and support. He had his failures, a lot of them, in the way since the first publication but he aimed to master all of them instead of giving up. He writes about the matters and things people prefer to overlook. Everyone talks about the viral topics, but there are some that are rarely spoken about. He chooses the rarely discussed topics that is hard to write about but what's the fun in writing about things everyone talks about. In August 2020, he founded Aspiring Pens, a literary organization that helps aspiring and emerging writers with writing and publishing. He as a founder, works at aspiring pens as a visual architect to design every idea that comes out as a publication as well as a teacher to teach courses of writing, publishing and editing. At that organization, he aimed to provide writers with everything he couldn't have or being taught. He doesn't want anyone to make the same mistakes and learn the hard way. According to him; he wanted to play his part in spreading literature anyway he could. So he turned his passion into his field and then profession. He published this book almost after one year of his recent book release. His literary organization kept him captivated, as people supposed but there were reason he thinks aren't authentic for him to talk about.

Convert Android to a powerful pentesting platform. Key Features Get up and running with Kali Linux NetHunter Connect your Android device and gain full control over Windows, OSX, or Linux devices Crack Wi-Fi passwords and gain access to devices connected over the same network collecting intellectual data Book Description Kali NetHunter is a version of the popular and powerful Kali Linux pentesting platform, designed to be installed on mobile devices. Hands-On Penetration Testing with Kali NetHunter will teach you the components of NetHunter and how to install the software. You’ll also learn about the different tools included and how to optimize and use a package, obtain desired results, perform tests, and make your environment more secure. Starting with an introduction to Kali NetHunter, you will delve into different phases of the pentesting process. This book will show you how to build your penetration testing environment and set up your lab. You will gain insight into gathering intellectual data,

exploiting vulnerable areas, and gaining control over target systems. As you progress through the book, you will explore the NetHunter tools available for exploiting wired and wireless devices. You will work through new ways to deploy existing tools designed to reduce the chances of detection. In the concluding chapters, you will discover tips and best practices for integrating security hardening into your Android ecosystem. By the end of this book, you will have learned to successfully use a mobile penetration testing device based on Kali NetHunter and Android to accomplish the same tasks you would traditionally, but in a smaller and more mobile form factor. What you will learn Choose and configure a hardware device to use Kali NetHunter Use various tools during pentests Understand NetHunter suite components Discover tips to effectively use a compact mobile platform Create your own Kali NetHunter-enabled device and configure it for optimal results Learn to scan and gather information from a target Explore hardware adapters for testing and auditing wireless networks and Bluetooth devices Who this book is for Hands-On Penetration Testing with Kali NetHunter is for pentesters, ethical hackers, and security professionals who want to learn to use Kali NetHunter for complete mobile penetration testing and are interested in venturing into the mobile domain. Some prior understanding of networking assessment and Kali Linux will be helpful.

Over the last few years, interest in the industrial applications of AI and learning systems has surged. This book covers the recent developments and provides a broad perspective of the key challenges that characterize the field of Industry 4.0 with a focus on applications of AI. The target audience for this book includes engineers involved in automation system design, operational planning, and decision support. Computer science practitioners and industrial automation platform developers will also benefit from the timely and accurate information provided in this work. The book is organized into two main sections comprising 12 chapters overall: •Digital Platforms and Learning Systems •Industrial Applications of AI

This is the only book actuaries need to understand generalized linear models (GLMs) for insurance applications. GLMs are used in the insurance industry to support critical decisions. Until now, no text has introduced GLMs in this context or addressed the problems specific to insurance data. Using insurance data sets, this practical, rigorous book treats GLMs, covers all standard exponential family distributions, extends the methodology to correlated data structures, and discusses recent developments which go beyond the GLM. The issues in the book are specific to insurance data, such as model selection in the presence of large data sets and the handling of varying exposure times. Exercises and data-based practicals help readers to consolidate their skills, with solutions and data sets given on the companion website. Although the book is package-independent, SAS code and output examples feature in an appendix and on the website. In addition, R code and output for all the examples are provided on the website.

Tailored to mirror the AP Statistics course, "The Practice of Statistics" became a classroom favorite. This edition incorporates a number of first-time features to help students prepare for the AP exam, plus more simulations and statistical thinking help, and instructions for the TI-89 graphic calculator."

Get the only official guide to the GRE® General Test that comes straight from the test makers! If you're looking for the best, most authoritative guide to the GRE General Test, you've found it! The Official Guide to the GRE General Test is the only GRE guide specially created by ETS--the people who actually make the test. It's packed with everything you need to do your best on the test--and move toward your graduate or business school degree. Only ETS can show you exactly what to expect on the test, tell you precisely how the test is scored, and give you hundreds of authentic test questions for practice! That makes this guide your most reliable and accurate source for everything you need to know about the GRE revised General Test. No other guide to the GRE General Test gives you all this: • Four complete, real tests--two in the book and two on CD-ROM • Hundreds of authentic test questions--so you can study with the real thing • In-depth descriptions of the Verbal Reasoning and Quantitative Reasoning measures plus valuable tips for answering each question type • Quantitative Reasoning problem-solving steps and strategies to help you get your best score • Detailed overview of the two types of Analytical Writing essay tasks including scored sample responses and actual raters' comments Everything you need to know about the test, straight from the test makers!

Sidestep VoIP Catastrophe the Foolproof Hacking Exposed Way "This book illuminates how remote users can probe, sniff, and modify your phones, phone switches, and networks that offer VoIP services. Most importantly, the authors offer solutions to mitigate the risk of deploying VoIP technologies." --Ron Gula, CTO of Tenable Network Security Block debilitating VoIP attacks by learning how to look at your network and devices through the eyes of the malicious intruder. Hacking Exposed VoIP shows you, step-by-step, how online criminals perform reconnaissance, gain access, steal data, and penetrate vulnerable systems. All hardware-specific and network-centered security issues are covered alongside detailed countermeasures, in-depth examples, and hands-on implementation techniques. Inside, you'll learn how to defend against the latest DoS, man-in-the-middle, call flooding, eavesdropping, VoIP fuzzing, signaling and audio manipulation, Voice SPAM/SPIT, and voice phishing attacks. Find out how hackers footprint, scan, enumerate, and pilfer VoIP networks and hardware Fortify Cisco, Avaya, and Asterisk systems Prevent DNS poisoning, DHCP exhaustion, and ARP table manipulation Thwart number harvesting, call pattern tracking, and conversation eavesdropping Measure and maintain VoIP network quality of service and VoIP conversation quality Stop DoS and packet flood-based attacks from disrupting SIP proxies and phones Counter REGISTER hijacking, INVITE flooding, and BYE call teardown attacks Avoid insertion/mixing of malicious audio Learn about voice SPAM/SPIT and how to prevent it Defend against voice phishing and identity theft scams

An in-depth exploration of the inner-workings of Android: In Volume I, we take the perspective of the Power User as we delve into the foundations of Android, filesystems, partitions, boot process, native daemons and services.

Provides a professional-level reference to the Samsung ARTIK API, as well as to other aspects of interest to developers such as the file systems, the operating system internals, various available interfaces, input/output, and the hardware itself. This is the perfect book for experienced programmers and developers who want to jump in and work with Samsung's new ARTIK product line to create Internet of Things devices and applications. It is also a perfect follow-up resource for new-to-the-field developers who are just getting past the beginning stages of learning the ARTIK. Samsung ARTIK Reference begins with a concise overview of the hardware and the various developer reference boards that are available. Attention then shifts to operating system internals, modes such as sleep and startup, and the various file systems and their parameters that are available for developers to adjust. Also included is a reference of API calls, guidance on input and output, documentation of serial, audio, graphic, and other interfaces. There is extensive reference to online resources with annotation and commentary guiding the learning process in many directions for further study. What You Will Learn Install the ARTIK toolkit and prepare to develop Manipulate the inner workings of the ARTIK operating system Look up and refer to details of the ARTIK API specification Perform input and output over the peripheral interface

buses Build embeddable applications in support of IoT devices Embed the ARTIK modules into your own hardware products Who This Book Is For Samsung ARTIK Reference is for experienced developers wanting to understand and begin working with ARTIK. The book is especially of interest to those wishing to interact with ARTIK modules from within their own applications and web services.

A field manual to the technologies that are transforming our lives Everywhere we turn, a startling new device promises to transfigure our lives. But at what cost? In this urgent and revelatory excavation of our Information Age, leading technology thinker Adam Greenfield forces us to reconsider our relationship with the networked objects, services and spaces that define us. It is time to re-evaluate the Silicon Valley consensus determining the future. We already depend on the smartphone to navigate every aspect of our existence. We're told that innovations—from augmented-reality interfaces and virtual assistants to autonomous delivery drones and self-driving cars—will make life easier, more convenient and more productive. 3D printing promises unprecedented control over the form and distribution of matter, while the blockchain stands to revolutionize everything from the recording and exchange of value to the way we organize the mundane realities of the day to day. And, all the while, fiendishly complex algorithms are operating quietly in the background, reshaping the economy, transforming the fundamental terms of our politics and even redefining what it means to be human. Having successfully colonized everyday life, these radical technologies are now conditioning the choices available to us in the years to come. How do they work? What challenges do they present to us, as individuals and societies? Who benefits from their adoption? In answering these questions, Greenfield's timely guide clarifies the scale and nature of the crisis we now confront —and offers ways to reclaim our stake in the future.

This book constitutes the refereed proceedings of the 33rd Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy, DBSec 2019, held in Charleston, SC, USA, in July 2018. The 21 full papers presented were carefully reviewed and selected from 52 submissions. The papers present high-quality original research from academia, industry, and government on theoretical and practical aspects of information security. They are organized in topical sections on attacks, mobile and Web security, privacy, security protocol practices, distributed systems, source code security, and malware.

Research Methods and Statistics for Public and Nonprofit Administrators: A Practical Guide is a comprehensive, easy-to-read, core text that thoroughly prepares readers to apply research methods and data analysis to the professional environments of public and non-profit administration. The authors expertly incorporate original case examples to demonstrate concepts using "real actors," facing specific scenarios, in which research methods must be applied. This unique approach—presented in language accessible to both students new to research as well as current practitioners—guides the reader in fully understanding the research options detailed throughout the text.

Infrastructure for Homeland Security Environments Wireless Sensor Networks helps readers discover the emerging field of low-cost standards-based sensors that promise a high order of spatial and temporal resolution and accuracy in an ever-increasing universe of applications. It shares the latest advances in science and engineering paving the way towards a large plethora of new applications in such areas as infrastructure protection and security, healthcare, energy, food safety, RFID, ZigBee, and processing. Unlike other books on wireless sensor networks that focus on limited topics in the field, this book is a broad introduction that covers all the major technology, standards, and application topics. It contains everything readers need to know to enter this burgeoning field, including current applications and promising research and development; communication and networking protocols; middleware architecture for wireless sensor networks; and security and management. The straightforward and engaging writing style of this book makes even complex concepts and processes easy to follow and understand. In addition, it offers several features that help readers grasp the material and then apply their knowledge in designing their own wireless sensor network systems: * Examples illustrate how concepts are applied to the development and application of * wireless sensor networks * Detailed case studies set forth all the steps of design and implementation needed to solve real-world problems * Chapter conclusions that serve as an excellent review by stressing the chapter's key concepts * References in each chapter guide readers to in-depth discussions of individual topics This book is ideal for networking designers and engineers who want to fully exploit this new technology and for government employees who are concerned about homeland security. With its examples, it is appropriate for use as a coursebook for upper-level undergraduates and graduate students.

The first comprehensive guide to discovering and preventingattacks on the Android OS As the Android operating system continues to increase its shareof the smartphone market, smartphone hacking remains a growingthreat. Written by experts who rank among the world's foremostAndroid security researchers, this book presents vulnerabilitydiscovery, analysis, and exploitation tools for the good guys.Following a detailed explanation of how the Android OS works andits overall security architecture, the authors examine howvulnerabilities can be discovered and exploits developed forvarious system components, preparing you to defend againstthem. If you are a mobile device administrator, security researcher,Android app developer, or consultant responsible for evaluatingAndroid security, you will find this guide is essential to yourtoolbox. A crack team of leading Android security researchers explainAndroid security risks, security design and architecture, rooting,fuzz testing, and vulnerability analysis Covers Android application building blocks and security as wellas debugging and auditing Android apps Prepares mobile device administrators, security researchers,Android app developers, and security consultants to defend Androidsystems against attack Android Hacker's Handbook is the first comprehensiveresource for IT professionals charged with smartphonesecurity.

This is an easy-to-follow guide, full of hands-on and real-world examples of applications. Each of the vulnerabilities discussed in the book is accompanied with the practical approach to the vulnerability, and the underlying security issue. This book is intended for all those who are looking to get started in Android security or Android application penetration testing. You don't need to be an Android developer to learn from this book, but it is highly recommended that developers have some experience in order to learn how to create secure applications for Android.

Take a practioner's approach in analyzing the Internet of Things (IoT) devices and the security issues facing an IoT architecture. You'll review the architecture's central components, from hardware communication interfaces, such as UARTand SPI, to radio protocols, such as BLE or ZigBee. You'll also learn to assess a device physically by opening it, looking at the PCB, and identifying the chipsets and interfaces. You'll then use that information to gain entry to the device or to perform other actions, such as dumping encryption keys and firmware. As the IoT rises to one of the most popular tech trends, manufactures need to take necessary steps to secure devices and protect them from attackers. The IoT Hacker's Handbook breaks down the Internet of Things, exploits it, and reveals how these devices can be built securely. What You'll Learn Perform a threat model of a real-world IoT device and locate all possible attacker entry points Use reverse engineering of firmware binaries to identify security issues Analyze,assess, and identify security issues in exploited ARM and MIPS based binaries Sniff, capture, and exploit radio communication protocols, such as Bluetooth Low Energy (BLE), and ZigBee Who This Book is For Those interested in learning about IoT security, such as pentesters working in different domains, embedded device developers, or IT people wanting to move to an Internet of Things security role.

This book presents a selection of papers representing current research on using field programmable gate arrays (FPGAs) for realising image processing algorithms. These papers are reprints of papers selected for a Special Issue of the Journal of Imaging on image processing using

FPGAs. A diverse range of topics is covered, including parallel soft processors, memory management, image filters, segmentation, clustering, image analysis, and image compression. Applications include traffic sign recognition for autonomous driving, cell detection for histopathology, and video compression. Collectively, they represent the current state-of-the-art on image processing using FPGAs.

Are we alone? asks the writeup on the back cover of the dust jacket. The contributors to this collection raise questions that may have been overlooked by physical scientists about the ease of establishing meaningful communication with an extraterrestrial intelligence. By drawing on issues at the core of contemporary archaeology and anthropology, we can be much better prepared for contact with an extraterrestrial civilization, should that day ever come. NASA SP-2013-4413.

Focusing on developing practical R skills rather than teaching pure statistics, Dr. Kurt Taylor Gaubatz's A Survivor's Guide to R provides a gentle yet thorough introduction to R. The book is structured around critical R tasks, and focuses on applied knowledge, rather than abstract concepts. Gaubatz's easy-to-read approach helps students with little or no background in statistics or programming to develop real-world R skills through straightforward coverage of R objects and functions. Focusing on real-world data, the challenges of dataset construction, and the use of R's powerful graphing tools, the guide is written in an accessible, sympathetic, even humorous style that ensures students acquire functional R skills they can use in their own projects and carry into their work beyond the classroom.

Linux® is being adopted by an increasing number of embedded systems developers, who have been won over by its sophisticated scheduling and networking, its cost-free license, its open development model, and the support offered by rich and powerful programming tools. While there is a great deal of hype surrounding the use of Linux in embedded systems, there is not a lot of practical information. Building Embedded Linux Systems is the first in-depth, hard-core guide to putting together an embedded system based on the Linux kernel. This indispensable book features arcane and previously undocumented procedures for: Building your own GNU development toolchain Using an efficient embedded development framework Selecting, configuring, building, and installing a target-specific kernel Creating a complete target root filesystem Setting up, manipulating, and using solid-state storage devices Installing and configuring a bootloader for the target Cross-compiling a slew of utilities and packages Debugging your embedded system using a plethora of tools and techniques Details are provided for various target architectures and hardware configurations, including a thorough review of Linux's support for embedded hardware. All explanations rely on the use of open source and free software packages. By presenting how to build the operating system components from pristine sources and how to find more documentation or help, this book greatly simplifies the task of keeping complete control over one's embedded operating system, whether it be for technical or sound financial reasons.Author Karim Yaghmour, a well-known designer and speaker who is responsible for the Linux Trace Toolkit, starts by discussing the strengths and weaknesses of Linux as an embedded operating system. Licensing issues are included, followed by a discussion of the basics of building embedded Linux systems. The configuration, setup, and use of over forty different open source and free software packages commonly used in embedded Linux systems are also covered. uClibc, BusyBox, U-Boot, OpenSSH, thttpd, tftp, strace, and gdb are among the packages discussed.

Loyalty is one of the main assets of a brand. In today's markets, achieving and maintaining loyal customers has become an increasingly complex challenge for brands due to the widespread acceptance and adoption of diverse technologies by which customers communicate with brands. Customers use different channels (physical, web, apps, social media) to seek information about a brand, communicate with it, chat about the brand and purchase its products. Firms are thus continuously changing and adapting their processes to provide customers with agile communication channels and coherent, integrated brand experiences through the different channels in which customers are present. In this context, understanding how brand management can improve value co-creation and multichannel experience—among other issues—and contribute to improving a brand's portfolio of loyal customers constitutes an area of special interest for academics and marketing professionals. This Special Issue explores new areas of customer loyalty and brand management, providing new insights into the field. Both concepts have evolved over the last decade to encompass such concepts and practices as brand image, experiences, multichannel context, multimedia platforms and value co-creation, as well as relational variables such as trust, engagement and identification (among others).

There are more than one billion Android devices in use today, each one a potential target. Unfortunately, many fundamental Android security features have been little more than a black box to all but the most elite security professionals—until now. In Android Security Internals, top Android security expert Nikolay Elenkov takes us under the hood of the Android security system. Elenkov describes Android security architecture from the bottom up, delving into the implementation of major security-related components and subsystems, like Binder IPC, permissions, cryptographic providers, and device administration. You'll learn: –How Android permissions are declared, used, and enforced –How Android manages application packages and employs code signing to verify their authenticity –How Android implements the Java Cryptography Architecture (JCA) and Java Secure Socket Extension (JSSE) frameworks –About Android's credential storage system and APIs, which let applications store cryptographic keys securely –About the online account management framework and how Google accounts integrate with Android –About the implementation of verified boot, disk encryption, lockscreen, and other device security features –How Android's bootloader and recovery OS are used to perform full system updates, and how to obtain root access With its unprecedented level of depth and detail, Android Security Internals is a must-have for any security-minded Android developer.

Lecturers - request an e-inspection copy of this text or contact your local SAGE representative to discuss your course needs. Watch Andy Field's introductory video to Discovering Statistics Using R Keeping the uniquely humorous and self-deprecating style that has made students across the world fall in love with Andy Field's books, Discovering Statistics Using R takes students on a journey of statistical discovery using R, a free, flexible and dynamically changing software tool for data analysis that is becoming increasingly popular across the social and behavioural sciences throughout the world. The journey begins by explaining basic statistical and research concepts before a guided tour of the R software environment. Next you discover the importance of exploring and graphing data, before moving onto statistical tests that are the foundations of the rest of the book (for example correlation and regression). You will then stride confidently into intermediate level analyses such as ANOVA, before ending your journey with advanced techniques such as MANOVA and multilevel models. Although there is enough theory to help you gain the necessary conceptual understanding of what you're doing, the emphasis is on applying what you learn to playful and real-world examples that should make the experience more fun than you might expect. Like its sister textbooks, Discovering Statistics Using R is written in an irreverent style and follows the same ground-breaking structure and pedagogical approach. The core material is

augmented by a cast of characters to help the reader on their way, together with hundreds of examples, self-assessment tests to consolidate knowledge, and additional website material for those wanting to learn more. Given this book's accessibility, fun spirit, and use of bizarre real-world research it should be essential for anyone wanting to learn about statistics using the freely-available R software.

In order to understand hackers and protect the network infrastructure you must think like a hacker in today's expansive and eclectic internet and you must understand that nothing is fully secured.This book will focus on some of the most dangerous hacker tools that are favourite of both, White Hat and Black Hat hackers.If you attempt to use any of the tools discussed in this book on a network without being authorized and you disturb or damage any systems, that would be considered illegal black hat hacking. So, I would like to encourage all readers to deploy any tool described in this book for WHITE HAT USE ONLY.The focus of this book will be to introduce some of the best well known software that you can use for free of charge, furthermore where to find them, how to access them, and finally in every chapter you will find demonstrated examples step-by-step.Your reading of this book will boost your knowledge on what is possible in today's hacking world and help you to become an Ethical Hacker.BUY THIS BOOK NOW AND GET STARTED TODAY!IN THIS BOOK YOU WILL LEARN: -Common mobile platform terminologies-Attack Vectors & Countermeasures-How to Install Android in Hyper-V-Android Architecture-Android Hardware Function Basics-Android Root Level Access-How to Root Android Devices-Android Attack Types-Securing Android Devices-IOS Architecture Basics-IOS Hardware Security-IOS App Security-IOS Jailbreak Types-IOS Jailbreaking-Securing IOS Devices-Windows Phone Architecture-BlackBerry Architecture-Mobile Device Management-Security Recommendations-Spiceworks & Solarwinds-Malware & Spyware on IOS-Malware & Spyware on Android and much more...BUY THIS BOOK NOW AND GET STARTED TODAY!

Explore fundamental to advanced Python 3 topics in six steps, all designed to make you a worthy practitioner. This updated version’s approach is based on the “six degrees of separation” theory, which states that everyone and everything is a maximum of six steps away and presents each topic in two parts: theoretical concepts and practical implementation using suitable Python 3 packages. You’ll start with the fundamentals of Python 3 programming language, machine learning history, evolution, and the system development frameworks. Key data mining/analysis concepts, such as exploratory analysis, feature dimension reduction, regressions, time series forecasting and their efficient implementation in Scikit-learn are covered as well. You’ll also learn commonly used model diagnostic and tuning techniques. These include optimal probability cutoff point for class creation, variance, bias, bagging, boosting, ensemble voting, grid search, random search, Bayesian optimization, and the noise reduction technique for IoT data. Finally, you’ll review advanced text mining techniques, recommender systems, neural networks, deep learning, reinforcement learning techniques and their implementation. All the code presented in the book will be available in the form of iPython notebooks to enable you to try out these examples and extend them to your advantage. What You'll Learn Understand machine learning development and frameworks Assess model diagnosis and tuning in machine learning Examine text mining, natuarl language processing (NLP), and recommender systems Review reinforcement learning and CNN Who This Book Is For Python developers, data engineers, and machine learning engineers looking to expand their knowledge or career into machine learning area.

Build HTML5-based hybrid applications for Android with a mix of native Java and JavaScript components, without using third-party libraries and wrappers such as PhoneGap or Titanium. This concise, hands-on book takes you through the entire process, from setting up your development environment to deploying your product to an app store. Learn how to create apps that have access to native APIs, such as location, vibrator, sensors, and the camera, using a JavaScript/Java bridge—and choose the language that gives you better performance for each task. If you have experience with HTML5 and JavaScript, you’ll quickly discover why hybrid app development is the wave of the future. Set up a development environment with HTML, CSS, and JavaScript tools Create your first hybrid Android project, using Eclipse IDE Use the WebView control to host your hybrid application Explore hybrid application architecture, including JavaScript/Java communication Build single-page applications, using JavaScript libraries such as Backbone and Underscore Get optimization tips and useful snippets for CSS, DOM, and JavaScript Distribute your application to Google Play and the Amazon Appstore

Protect your organization from scandalously easy-to-hack MFA security “solutions” Multi-Factor Authentication (MFA) is spreading like wildfire across digital environments. However, hundreds of millions of dollars have been stolen from MFA-protected online accounts. How? Most people who use multifactor authentication (MFA) have been told that it is far less hackable than other types of authentication, or even that it is unhackable. You might be shocked to learn that all MFA solutions are actually easy to hack. That’s right: there is no perfectly safe MFA solution. In fact, most can be hacked at least five different ways. Hacking Multifactor Authentication will show you how MFA works behind the scenes and how poorly linked multi-step authentication steps allows MFA to be hacked and compromised. This book covers over two dozen ways that various MFA solutions can be hacked, including the methods (and defenses) common to all MFA solutions. You’ll learn about the various types of MFA solutions, their strengthens and weaknesses, and how to pick the best, most defensible MFA solution for your (or your customers') needs. Finally, this book reveals a simple method for quickly evaluating your existing MFA solutions. If using or developing a secure MFA solution is important to you, you need this book. Learn how different types of multifactor authentication work behind the scenes See how easy it is to hack MFA security solutions—no matter how secure they seem Identify the strengths and weaknesses in your (or your customers’) existing MFA security and how to mitigate Author Roger Grimes is an internationally known security expert whose work on hacking MFA has generated significant buzz in the security world. Read this book to learn what decisions and preparations your organization needs to take to prevent losses from MFA hacking.

A major new exploration of the refugee crisis, focusing on how borders are formed and policed Forty thousand people

have died trying to cross between countries in the past decade, and yet international borders only continue to harden. The United Kingdom has voted to leave the European Union; the United States elected a president who campaigned on building a wall; while elsewhere, the popularity of right-wing antimigrant nationalist political parties is surging. Reece Jones argues that the West has helped bring about the deaths of countless migrants, as states attempt to contain populations and limit access to resources and opportunities. “We may live in an era of globalization,” he writes, “but much of the world is increasingly focused on limiting the free movement of people.” In Violent Borders, Jones crosses the migrant trails of the world, documenting the billions of dollars spent on border security projects and the dire consequences for countless millions. While the poor are restricted by the lottery of birth to slum dwellings in the ailing decolonized world, the wealthy travel without constraint, exploiting pools of cheap labor and lax environmental regulations. With the growth of borders and resource enclosures, the deaths of migrants in search of a better life are intimately connected to climate change, environmental degradation, and the growth of global wealth inequality. Newly updated with a discussion of Brexit and the Trump administration.

This fully revised and updated new edition of the definitive text/reference on computer network and information security presents a comprehensive guide to the repertoire of security tools, algorithms and best practices mandated by the technology we depend on. Topics and features: highlights the magnitude of the vulnerabilities, weaknesses and loopholes inherent in computer networks; discusses how to develop effective security solutions, protocols, and best practices for the modern computing environment; examines the role of legislation, regulation, and enforcement in securing computing and mobile systems; describes the burning security issues brought about by the advent of the Internet of Things and the eroding boundaries between enterprise and home networks (NEW); provides both quickly workable and more thought-provoking exercises at the end of each chapter, with one chapter devoted entirely to hands-on exercises; supplies additional support materials for instructors at an associated website.

This practical, conceptual introduction to statistical analysis by award-winning teacher Andrew N. Christopher uses published research with inherently interesting social sciences content to help students make clear connections between statistics and real life. Using a friendly, easy-to-understand presentation, Christopher walks students through the hand calculations of key statistical tools and provides step-by-step instructions on how to run the appropriate analyses for each type of statistic in SPSS and how to interpret the output. With the premise that a conceptual grasp of statistical techniques is critical for students to truly understand why they are doing what they are doing, the author avoids overly formulaic jargon and instead focuses on when and how to use statistical techniques appropriately.

An exquisite strand of pale pink pearls, worth more than the Hope Diamond, has been bought by a Hatton Garden broker. Word of the 'Mona Lisa of Pearls' spreads around the world, captivating jewellers as well as thieves. In transit to London from Paris, the necklace vanishes without a trace. Thoroughly researched, compellingly colourful, The Great Pearl Heist is a gripping narrative account of this little-known, yet extraordinary crime. In the spirit of The Great Train Robbery and the tales of Sherlock Holmes, this is the true story set in London's golden Edwardian era.

MQ Telemetry Transport (MQTT) is a messaging protocol that is lightweight enough to be supported by the smallest devices, yet robust enough to ensure that important messages get to their destinations every time. With MQTT devices such as smart energy meters, cars, trains, satellite receivers, and personal health care devices can communicate with each other and with other systems or applications. This IBM® Redbooks® publication introduces MQTT and takes a scenario-based approach to demonstrate its capabilities. It provides a quick guide to getting started and then shows how to grow to an enterprise scale MQTT server using IBM WebSphere® MQ Telemetry. Scenarios demonstrate how to integrate MQTT with other IBM products, including WebSphere Message Broker. This book also provides typical usage patterns and guidance on scaling a solution. The intended audience for this book ranges from new users of MQTT and telemetry to those readers who are looking for in-depth knowledge and advanced topics.

A Practical Guide to Computer Forensics Investigations introduces the newest technologies along with detailed information on how the evidence contained on these devices should be analyzed. Packed with practical, hands-on activities, students will learn unique subjects from chapters including Mac Forensics, Mobile Forensics, Cyberbullying, and Child Endangerment. This well-developed book will prepare students for the rapidly-growing field of computer forensics for a career with law enforcement, accounting firms, banks and credit card companies, private investigation companies, or government agencies.