# By John Sammons The Basics Of Digital Forensics Second Edition The Primer For Getting Started In Digital Forensics 2nd Second Edition Paperback





## SCHWARTZ POWELL

Forensic Analytics John Wiley & Sons
Digital Forensics with Open Source Tools is the definitive book on investigating and analyzing computer systems and media using open source tools. The book is a technical procedural guide, and explains the use of open source tools on Mac, Linux and Windows systems as a platform for performing computer forensics. Both well-known and novel forensic methods are demonstrated using command-line and graphical open source computer forensic tools for examining a wide range of target systems and artifacts. Written by world-renowned forensic practitioners, this book uses the most current examination and analysis techniques in the field. It consists of 9 chapters that cover a range of topics such as the open source examination platform; disk and file system analysis; Windows systems and artifacts; Linux systems and artifacts; Mac OS X systems and artifacts; Internet artifacts; and automating analysis and extending capabilities. The book lends itself to use by students and those entering the field who do not have means to purchase new tools for different investigations. This book will appeal to forensic practitioners from areas including incident response teams and computer forensic investigators; forensic technicians from legal, audit, and consulting firms; and law enforcement agencies. Written by world-renowned forensic practitioners Details core concepts and techniques of forensic file system analysis Covers analysis of artifacts from the Windows, Mac, and Linux operating systems
*Digital Forensics Processing and Procedures* Newnes
Build your organization's cyber defense system by effectively implementing digital forensics and incident management techniques Key Features Create a solid incident response framework and manage cyber incidents effectively Perform malware analysis for effective incident response Explore real-life scenarios that effectively use threat intelligence and modeling techniques Book DescriptionAn understanding of how digital forensics integrates with the overall response to cybersecurity incidents is key to securing your organization's infrastructure from attacks. This updated second edition will help you perform cutting-edge digital forensic activities and incident response. After focusing on the fundamentals of incident response that are critical to any information security team, you’ll move on to exploring the incident response framework. From understanding its importance to creating a swift and effective response to security incidents, the book will guide you with the help of useful examples. You’ll later get up to speed with digital forensic techniques, from acquiring evidence and examining volatile memory through to hard drive examination and network-based evidence. As you progress, you’ll discover the role that threat

intelligence plays in the incident response process. You'll also learn how to prepare an incident response report that documents the findings of your analysis. Finally, in addition to various incident response activities, the book will address malware analysis, and demonstrate how you can proactively use your digital forensic skills in threat hunting. By the end of this book, you'll have learned how to efficiently investigate and report unwanted security breaches and incidents in your organization.What you will learn Create and deploy an incident response capability within your own organization Perform proper evidence acquisition and handling Analyze the evidence collected and determine the root cause of a security incident Become well-versed with memory and log analysis Integrate digital forensic techniques and procedures into the overall incident response process Understand the different techniques for threat hunting Write effective incident reports that document the key findings of your analysis Who this book is for This book is for cybersecurity and information security professionals who want to implement digital forensics and incident response in their organization. You will also find the book helpful if you are new to the concept of digital forensics and are looking to get started with the fundamentals. A basic understanding of operating systems and some knowledge of networking fundamentals are required to get started with this book.

Forensic Digital Imaging and Photography Syngress

Over 60 recipes to help you learn digital forensics and leverage Python scripts to amplify your examinations About This Book Develop code that extracts vital information from everyday forensic acquisitions. Increase the quality and efficiency of your forensic analysis. Leverage the latest resources and capabilities available to the forensic community. Who This Book Is For If you are a digital forensics examiner, cyber security specialist, or analyst at heart, understand the basics of Python, and want to take it to the next level, this is the book for you. Along the way, you will be introduced to a number of libraries suitable for parsing forensic artifacts. Readers will be able to use and build upon the scripts we develop to elevate their analysis. What You Will Learn Understand how Python can enhance digital forensics and investigations Learn to access the contents of, and process, forensic evidence containers Explore malware through automated static analysis Extract and review message contents from a variety of email formats Add depth and context to discovered IP addresses and domains through various Application Program Interfaces (APIs) Delve into mobile forensics and recover deleted messages from SQLite databases Index large logs into a platform to better query and visualize datasets In Detail Technology plays an increasingly large role in our daily lives and shows no sign of stopping. Now, more than ever, it is paramount that an investigator develops programming expertise to deal with increasingly large datasets. By leveraging the Python recipes explored throughout this book, we make the complex simple, quickly extracting relevant information from large datasets. You will explore, develop, and deploy Python code and libraries to provide meaningful results that can be immediately applied to your investigations. Throughout the Python Digital Forensics Cookbook, recipes include topics such as working with forensic evidence containers, parsing mobile and desktop operating system artifacts, extracting embedded metadata from documents and executables, and identifying indicators of compromise. You will also learn to integrate scripts with Application Program Interfaces (APIs) such as VirusTotal and PassiveTotal, and tools such as Axiom, Cellebrite, and EnCase. By the end of the book, you will have a sound understanding of Python and how you can use it to process artifacts in your investigations. Style and approach Our succinct recipes take a no-frills approach to solving common challenges faced in investigations. The code in this book covers a wide range of artifacts and data sources. These examples will help improve the accuracy and efficiency of your analysis—no matter the situation.

XBOX 360 Forensics Academic Press

An explanation of the basic principles of data This book explains the basic principles of data as building blocks of electronic evidential matter, which are used in a cyber forensics investigations. The entire text is written with no reference to a particular operation system or environment, thus it is applicable to all work environments, cyber investigation scenarios, and technologies. The text is written in a step-by-step manner, beginning with the elementary building blocks of data progressing upwards to the representation and storage of information. It inlcudes practical examples and illustrations throughout to guide the reader.

**Digital Methods** Syngress

Conduct repeatable, defensible investigations with EnCase Forensic v7 Maximize the powerful tools and features of the industry-leading digital investigation software. Computer Forensics and Digital Investigation with EnCase Forensic v7 reveals, step by step, how to detect illicit activity, capture and verify evidence, recover deleted and encrypted artifacts, prepare court-ready documents, and ensure legal and regulatory compliance. The book illustrates each concept using downloadable evidence from the National Institute of Standards and Technology CFReDS. Customizable sample procedures are included throughout this practical guide. Install EnCase Forensic v7 and customize the user interface Prepare your investigation and set up a new case Collect and verify evidence from suspect computers and networks Use the EnCase Evidence Processor and Case Analyzer Uncover clues using keyword searches and filter results through GREP Work with bookmarks, timelines, hash sets, and libraries Handle case closure, final disposition, and evidence destruction Carry out field investigations using EnCase Portable Learn to program in EnCase EnScript

Digital Forensics and Incident Response Createspace Independent Publishing Platform

This fourth edition covers the fundamentals of discrete-time signals, systems, and modern digital signal processing. Appropriate for students of electrical engineering, computer engineering, and computer science, the book is suitable for undergraduate and graduate courses and provides balanced coverage of both theory and practical applications.

*Digital Signal Processing Fundamentals* Elsevier

A NEW YORK TIMES, USA TODAY, and WASHINGTON POST BESTSELLER! A 2021 Alex Award winner! The 2021 RUSA Reading List: Fantasy Winner! An Indie Next Pick! One of Publishers Weekly's "Most Anticipated Books of Spring 2020" One of Book Riot's "20 Must-Read Feel-Good Fantasies" Lambda Literary Award-winning author TJ Klune's bestselling, breakout contemporary fantasy that's "1984 meets The Umbrella Academy with a pinch of Douglas Adams thrown in." (Gail Carriger) Linus Baker is a by-the-book case worker in the Department in Charge of Magical Youth. He's tasked with determining whether six dangerous magical children are likely to bring about the end of the world. Arthur Parnassus is the master of the orphanage. He would do anything to keep the children safe, even if it means the world will burn. And his secrets will come to light. The House in the Cerulean Sea is an enchanting love story, masterfully told, about the profound experience of discovering an unlikely family in an unexpected place—and realizing that family is yours. "1984 meets The Umbrella Academy with a pinch of Douglas Adams thrown in." —Gail Carriger, New York Times bestselling author of Soulless At the Publisher's request, this title is being sold without Digital Rights Management Software (DRM) applied.

**Digital Forensics and Incident Response** Packt Publishing Ltd

The fifth edition of Mayhall's Hospital Epidemiology and Infection Prevention has a new streamlined focus, with new editors and contributors, a new two-color format, and a new title. Continuing the legacy of excellence established by Dr. C. Glen Mayhall, this thoroughly revised text covers all aspects of healthcare-associated infections and their prevention and remains the most comprehensive reference available in this complex field. It examines every type of healthcare-associated (nosocomial) infection and addresses every issue relating to surveillance, prevention, and control of these infections in patients and in healthcare personnel, providing unparalleled coverage for hospital epidemiologists and infectious disease specialists.

*Digital Forensics with Open Source Tools* Packt Publishing Ltd

Use this hands-on, introductory guide to understand and implement digital forensics to investigate computer crime using Windows, the most widely used operating system. This book provides you with the necessary skills to identify an intruder's footprints and to gather the necessary digital evidence in a forensically sound manner to prosecute in a court of law. Directed toward users with no experience in the digital forensics field, this book provides guidelines and best practices when conducting investigations as well as teaching you how to use a variety of tools to investigate computer crime. You will be prepared to handle problems such as law violations, industrial espionage, and use of company resources for private use. Digital Forensics Basics is written as a series of tutorials with each task demonstrating how to use a specific computer forensics tool or technique. Practical information is provided and users can read a task and then implement it directly on their devices. Some theoretical information is presented to define terms used in each technique and for users with varying IT skills. What You'll Learn Assemble computer forensics lab requirements, including workstations, tools, and more Document the digital crime scene, including preparing a sample chain of custody form Differentiate between law enforcement agency and corporate investigationsGather intelligence using OSINT sources Acquire and analyze digital evidence Conduct in-depth forensic analysis of Windows operating systems covering Windows 10–specific feature forensicsUtilize anti-forensic techniques, including steganography, data destruction techniques, encryption, and anonymity techniques Who This Book Is For Police and other law enforcement personnel, judges (with no technical background), corporate and nonprofit management, IT specialists and computer security professionals, incident response team members, IT military and intelligence services officers, system administrators, e-business security professionals, and banking and insurance professionals

*Forensic Science* Firewall Media

The field of computer forensics has experienced significant growth recently and those looking to get into the industry have significant opportunity for upward mobility. Focusing on the concepts investigators need to know to conduct a thorough investigation, Digital Forensics Explained provides an overall description of the forensic practice from a practitioner's perspective. Starting with an overview, the text describes best practices based on the author's decades of experience conducting investigations and working in information technology. It illustrates the forensic process, explains what it takes to be an investigator, and highlights emerging trends. Filled with helpful templates and contributions from seasoned experts in their respective fields, the book includes coverage of: Internet and email investigations Mobile forensics for cell phones, iPads, music players, and other small devices Cloud computing from an architecture perspective and its impact on digital forensics Anti-forensic techniques that may be employed to make a forensic exam more difficult to conduct Recoverability of information from damaged media The progression of a criminal case from start to finish Tools that are often used in an examination, including commercial, free, and open-source tools; computer and mobile tools; and things as simple as extension cords Social media and social engineering forensics Case documentation and presentation, including sample summary reports and a cover sheet for a cell phone investigation The text includes acquisition forms, a sequential process outline to guide your investigation, and a checklist of supplies you'll need when responding to an incident. Providing you with the understanding and the tools to deal with suspects who find ways to make their digital activities hard to trace, the book also considers cultural implications, ethics, and the psychological effects that digital forensics investigations can have on investigators.

*Digital Forensic Education* CRC Press

Operating System Forensics is the first book to cover all three critical operating systems for digital forensic investigations in one comprehensive reference. Users will learn how to conduct successful digital forensic examinations in Windows, Linux, and Mac OS, the methodologies used, key technical concepts, and the tools needed to perform examinations. Mobile operating systems such as Android, iOS, Windows, and Blackberry are also covered, providing everything practitioners need to conduct a forensic investigation of the most commonly used operating systems, including technical details of how each operating system works and how to find artifacts. This book walks you through the critical components of investigation and operating system functionality, including file systems, data recovery, memory forensics, system configuration, Internet access, cloud computing, tracking artifacts, executable layouts, malware, and log files. You'll find coverage of key technical topics like Windows Registry, /etc directory, Web browers caches, Mbox, PST files, GPS data, ELF, and more. Hands-on exercises in each chapter drive home the concepts covered in the book. You'll get everything you need for a successful forensics examination, including incident response tactics and legal requirements. Operating System Forensics is the only place you'll find all this covered in one book. Covers digital forensic investigations of the three major operating systems, including Windows, Linux, and Mac OS Presents the technical details of each operating system, allowing users to find artifacts that might be missed using automated tools Hands-on exercises drive home key concepts covered in the book. Includes discussions of cloud, Internet, and major mobile operating systems such as Android and iOS

Python Digital Forensics Cookbook Tor Books

FORENSIC SCIENCE Forensic Science: Current Issues, Future Directions presents a comprehensive, international discussion of key issues within the forensic sciences. Written by accomplished and respected specialists in distinct areas of the forensic sciences, this volume examines central issues within each discipline, provides perspective on current debate and explores current and proposed research initiatives. The forensic sciences represent dynamic and evolving fields, presenting new challenges to a rapidly expanding cohort of international practitioners. This book acquaints readers with the complex issues involved and how they are being addressed. The academic treatment by experts in the fields ensures comprehensive and thorough understanding of these issues and paves the way for future research and progress. Draws on the knowledge and expertise of the prestigious American Academy of Forensic Sciences Written by key experts in the diverse disciplines of forensic science An international approach Each chapter carefully integrated throughout with key themes and issues covered in detail Includes discussion of future directions of

forensic science as a discipline

**Mayhall's Hospital Epidemiology and Infection Prevention** Syngress

A proposal to repurpose Web-native techniques for use in social and cultural scholarly research. In Digital Methods, Richard Rogers proposes a methodological outlook for social and cultural scholarly research on the Web that seeks to move Internet research beyond the study of online culture. It is not a toolkit for Internet research, or operating instructions for a software package; it deals with broader questions. How can we study social media to learn something about society rather than about social media use? Rogers proposes repurposing Web-native techniques for research into cultural change and societal conditions. We can learn to reapply such "methods of the medium" as crawling and crowd sourcing, PageRank and similar algorithms, tag clouds and other visualizations; we can learn how they handle hits, likes, tags, date stamps, and other Web-native objects. By "thinking along" with devices and the objects they handle, digital research methods can follow the evolving methods of the medium. Rogers uses this new methodological outlook to examine such topics as the findings of inquiries into 9/11 search results, the recognition of climate change skeptics by climate-change-related Web sites, and the censorship of the Iranian Web. With Digital Methods, Rogers introduces a new vision and method for Internet research and at the same time applies them to the Web's objects of study, from tiny particles (hyperlinks) to large masses (social media).

*The Basics of Cyber Safety* Academic Press

The Basics of Cyber Safety: Computer and Mobile Device Safety Made Easy presents modern tactics on how to secure computer and mobile devices, including what behaviors are safe while surfing, searching, and interacting with others in the virtual world. The book's author, Professor John Sammons, who teaches information security at Marshall University, introduces readers to the basic concepts of protecting their computer, mobile devices, and data during a time that is described as the most connected in history. This timely resource provides useful information for readers who know very little about the basic principles of keeping the devices they are connected to—or themselves—secure while online. In addition, the text discusses, in a non-technical way, the cost of connectedness to your privacy, and what you can do to it, including how to avoid all kinds of viruses, malware, cybercrime, and identity theft. Final sections provide the latest information on safe computing in the workplace and at school, and give parents steps they can take to keep young kids and teens safe online. Provides the most straightforward and up-to-date guide to cyber safety for anyone who ventures online for work, school, or personal use Includes real world examples that demonstrate how cyber criminals commit their crimes, and what users can do to keep their data safe

*The Basics of Digital Forensics, Second Edition* Apress

This is the first digital forensics book that covers the complete lifecycle of digital evidence and the chain of custody. This comprehensive handbook includes international procedures, best practices, compliance, and a companion web site with downloadable forms. Written by world-renowned digital forensics experts, this book is a must for any digital forensics lab. It provides anyone who handles digital evidence with a guide to proper procedure throughout the chain of custody--from incident response through analysis in the lab. A step-by-step guide to designing, building and using a digital forensics lab A comprehensive guide for all roles in a digital forensics laboratory Based on international standards and certifications

**Digital Forensics Workbook** Lippincott Williams & Wilkins

Written by experts on the frontlines, Investigating Internet Crimes provides seasoned and new investigators with the background and tools they need to investigate crime occurring in the online world. This invaluable guide provides step-by-step instructions for investigating Internet crimes, including locating, interpreting, understanding, collecting, and documenting online electronic evidence to benefit investigations. Cybercrime is the fastest growing area of crime as more criminals seek to exploit the speed, convenience and anonymity that the Internet provides to commit a diverse range of criminal activities. Today's online crime includes attacks against computer data and systems, identity theft, distribution of child pornography, penetration of online financial services, using social networks to commit crimes, and the deployment of viruses, botnets, and email scams such as phishing. Symantec's 2012 Norton Cybercrime Report stated that the world spent an estimated $110 billion to combat cybercrime, an average of nearly $200 per victim. Law enforcement agencies and corporate security officers around the world with the responsibility for enforcing, investigating and prosecuting cybercrime are overwhelmed, not only by the sheer number of crimes being committed but by a lack of adequate training material. This book provides that fundamental knowledge, including how to properly collect and document online evidence, trace IP addresses, and work undercover. Provides step-by-step instructions on how to investigate crimes online Covers how new software tools can assist in online investigations Discusses how to track down, interpret, and understand online electronic evidence to benefit investigations Details guidelines for collecting and documenting online evidence that can be presented in court

Digital Forensics McGraw Hill Professional

God intends nothing less than sainthood for you! The early Church held that all believers could achieve holiness. Over time, this conviction was largely forgotten. Sainthood seemed to be an honor only intended for a select few among the priests and religious. Eric Sammons tells how twentieth century Spanish priest and canonized saint Josemaria Escriva, the founder of Opus Dei, recovered the message of the universal call to holiness. Declared the saint of ordinary life by Pope John Paul II, St. Josemaria developed a spirituality directed toward the sanctity of every man and woman. His legacy is the belief that each of us can, by God's grace, achieve holiness through the course of our ordinary life and work. The heart of Sammons' practical guide to the spiritual life is a detailed examination of the steps in St. Josemaria's thoughtful plan for building a saintly life in spite of your hectic work and home life in a world filled with distractions and temptations. Strive for your own personal holiness as you implement your daily plan to: --Be a Contemplative in the Midst of a Busy World --Live a Life of Prayer --Recognize the Presence of God --Make a Plan of Life --Make Your Work a Way to Heaven Holiness for Everyone will inspire you as it sets your feet on the path to sainthood. "Eric Sammons shows that St. Josemaria has recovered the most powerful truth of classic Christianity and restated it in a way that is compelling for men and women of our time." --- From the Foreword by Scott Hahn

**Digital Forensics Basics** John Wiley & Sons

XBOX 360 Forensics is a complete investigation guide for the XBOX game console. Because the XBOX 360 is no longer just a video game console — it streams movies, connects with social networking sites and chatrooms, transfer files, and more — it just may contain evidence to assist in your next criminal investigation. The digital forensics community has already begun to receive game consoles for examination, but there is currently no map for you to follow as there may be with other digital media. XBOX 360 Forensics provides that map and presents the information in an easy-to-read, easy-to-reference format. This book is organized into 11 chapters that cover topics such as Xbox 360 hardware; XBOX LIVE; configuration of the console; initial forensic acquisition and examination; specific file types for Xbox 360; Xbox 360 hard drive; post-system update drive artifacts; and XBOX Live redemption code and Facebook. This book will appeal to computer forensic and incident response professionals, including those in federal government, commercial/private sector contractors, and consultants. Game consoles are routinely seized and contain evidence of criminal activity Author Steve Bolt wrote the first whitepaper on XBOX investigations

**Digital Archaeology** Springer Science & Business Media

About the Book : - Digital Signal Processing Fundamentals Digital Signal Processing (DSP), as the term suggests, is the processing of signals using digital computers. These signals might be anything transferred from an analog domain to a digital form (e.g., temperature and pressure sensors, voices over a telephone, images from a camera, or data transmittal though computes). As a result, understanding the whole spectrum of DSP technology can be a daunting task for electrical engineering professionals and students alike. Digital Signal Processing Fundamentals provides a comprehensive look at DSP by introducing the important mathematical processes and then providing several application-specific tutorials for practicing the techniques learned. Beginning with general theory, including Fourier Analysis, the mathematics of complex numbers, Fourier transforms, differential equations, analog and digital filters, and much more; the book then delves into Matlab and Scilab tutorials with examples on solving practical engineering problems, followed by software applications on image processing and audio processing - complete with all the algorithms and source code. This is an invaluable resource for anyone seeking to understand how DSP works. Features: Provides a comprehensive overview and introduction of digital signal processing technology. Provides application with software algorithms Explains the concept of Nyquist frequency, orthogonal functions and method of finding Fourier coefficients Includes a CD-ROM with the source code for the projects plus Matlab and Scilab that generate graphs, figures in the book, and third party application software Discusses the techniques of digital filtering and windowing of input data, including: Butterwoth, Chebyshev, and elliptic filter formulation. Table Of Contents : Fourier Analysis Complex Number Arithmetic The Fourier Transform Solutions of Differential Equations Laplace Transforms and z-Tranforms Filter Design Digital Filters The FIR Filters Appendix A : Matlab Tutorial Appendix B : Scilab Tutorial Appendix C : Digital Filter Applications Appendix D : About the CD-ROM Appendix E : Software Licenses Appendix F : Bibliography Index About Author :- Ashfaq A. Khan (Baton Rouge, LA) is a senior software engineer for LIGO Livingston Observatory, with over 20 years of experience in system design. He has conducted several workshop and is the author of Practical Linux Programming: Device Drivers, Embedded Systems, and the Internet.

*Investigating Internet Crimes* John Wiley & Sons

The definitive text for students of digital forensics, as well as professionals looking to deepen their understanding of an increasingly critical field Written by faculty members and associates of the world-renowned Norwegian Information Security Laboratory (NisLab) at the Norwegian University of Science and Technology (NTNU), this textbook takes a scientific approach to digital forensics ideally suited for university courses in digital forensics and information security. Each chapter was written by an accomplished expert in his or her field, many of them with extensive experience in law enforcement and industry. The author team comprises experts in digital forensics, cybercrime law, information security and related areas. Digital forensics is a key competency in meeting the growing risks of cybercrime, as well as for criminal investigation generally. Considering the astonishing pace at which new information technology – and new ways of exploiting information technology – is brought on line, researchers and practitioners regularly face new technical challenges, forcing them to continuously upgrade their investigatory skills. Designed to prepare the next generation to rise to those challenges, the material contained in Digital Forensics has been tested and refined by use in both graduate and undergraduate programs and subjected to formal evaluations for more than ten years. Encompasses all aspects of the field, including methodological, scientific, technical and legal matters Based on the latest research, it provides novel insights for students, including an informed look at the future of digital forensics Includes test questions from actual exam sets, multiple choice questions suitable for online use and numerous visuals, illustrations and case example images Features real-word examples and scenarios, including court cases and technical problems, as well as a rich library of academic references and references to online media Digital Forensics is an excellent introductory text for programs in computer science and computer engineering and for master degree programs in military and police education. It is also a valuable reference for legal practitioners, police officers, investigators, and forensic practitioners seeking to gain a deeper understanding of digital forensics and cybercrime.