# Practical Forensic Imaging Securing Digital Evidence With Linux Tools

Computer ForensicsShore EnoughGame HackingIntroductory Computer ForensicsDigital Forensics and Incident ResponseDigital Forensics with Kali LinuxMultimedia Security Technologies for Digital Rights ManagementPractical Forensic Digital ImagingMorton HallFood, Faith, and Facing My FearsComputer Forensics : A Practical GuidePractical Forensic ImagingPractical Mobile ForensicsDigital Forensics and Forensic Investigations: Breakthroughs in Research and PracticeWindows Forensics CookbookComputer ForensicsDigital and Document ExaminationForensic Examination of Windows-Supported File SystemsImaging for Forensics and SecurityConquering BabelRedNetwork ForensicsA Practical Guide to Computer Forensics InvestigationsA Practical Guide to Computer Forensics InvestigationsGuide to Computer Forensics and InvestigationsDigital Forensics WorkbookLearn Computer ForensicsSmall BallDigital Forensics and Incident ResponseAdvances in Communications, Computing, Networks and SecurityPractical Forensic ImagingDigital Image ForensicsThe Adventures of Tom Sawyer & Huckleberry Finn - Complete EditionPractical Forensic ImagingTitanicSuddenly Today We Can DreamDigital Forensics with Open Source ToolsScene of the Cybercrime: Computer Forensics HandbookGuide to Digital ForensicsReal digital forensics

## Computer Forensics

Become well-versed with forensics for the Android, iOS, and Windows 10 mobile platforms by learning essential techniques and exploring real-life scenarios Key Features Apply advanced forensic techniques to recover deleted data from mobile devices Retrieve and analyze data stored not only on mobile devices but also on the cloud and other connected mediums Use the power of mobile forensics on popular mobile platforms by exploring different tips, tricks, and techniques Book Description Mobile phone forensics is the science of retrieving data from a mobile phone under forensically sound conditions. This updated fourth edition of Practical Mobile Forensics delves into the concepts of mobile forensics and its importance in today's world. The book focuses on teaching you the latest forensic techniques to investigate mobile devices across various mobile platforms. You will learn forensic techniques for multiple OS versions, including iOS 11 to iOS 13, Android 8 to Android 10, and Windows 10. The book then takes you through the latest open source and commercial mobile forensic tools, enabling you to analyze and retrieve data effectively. From inspecting the device and retrieving data from the cloud, through to successfully documenting reports of your investigations, you'll explore new techniques while building on your practical knowledge. Toward the end, you will understand the reverse engineering of applications and ways to identify malware. Finally, the book guides you through parsing popular third-party applications, including Facebook and WhatsApp. By the end of this book, you will be proficient in various mobile forensic techniques to analyze and extract data from mobile devices with the help of open source solutions. What you will learn Discover new data extraction, data recovery, and reverse engineering techniques in mobile forensics Understand iOS, Windows, and Android security mechanisms Identify sensitive files on every mobile platform Extract data from iOS, Android,

and Windows platforms Understand malware analysis, reverse engineering, and data analysis of mobile devices Explore various data recovery techniques on all three mobile platforms Who this book is for This book is for forensic examiners with basic experience in mobile forensics or open source solutions for mobile forensics. Computer security professionals, researchers or anyone looking to gain a deeper understanding of mobile internals will also find this book useful. Some understanding of digital forensic practices will be helpful to grasp the concepts covered in the book more effectively.

## Shore Enough

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 Description An 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.

## Game Hacking

Well-documented scenes can prove to be invaluable pieces of evidence at trial, and the ability to take compelling photographs is a critical skill for forensic

scientists and investigators. Practical Forensic Digital Imaging: Applications and Techniques is an up-to-date and thorough treatment of digital imaging in the forensic sciences. Balancing pr

## Introductory Computer Forensics

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.

## Digital Forensics and Incident Response

It is a short story by Mrs. Gaskell. In the novel she explores different kinds of love, and her observations about human nature are as acute here as in her longer works. In this particular attempt she especially identifies motherhood and mother's feelings for her children. An awakening attempt!

## Digital Forensics with Kali Linux

## Multimedia Security Technologies for Digital Rights Management

## Practical Forensic Digital Imaging

Forensic image acquisition is an important part of postmortem incident response and evidence collection. Digital forensic investigators acquire, preserve, and manage digital evidence to support civil and criminal cases; examine organizational policy violations; resolve disputes; and analyze cyber attacks. Practical Forensic Imaging takes a detailed look at how to secure and manage digital evidence using Linux-based command line tools. This essential guide walks you through the entire forensic acquisition process and covers a wide range of practical scenarios and situations related to the imaging of storage media. You'll learn how to: Perform forensic imaging of magnetic hard disks, SSDs and flash drives, optical discs, magnetic tapes, and legacy technologies Protect attached evidence media from accidental modification Manage large forensic image files, storage capacity, image format conversion, compression, splitting, duplication, secure transfer and storage, and secure disposal Preserve and verify evidence integrity with cryptographic and piecewise hashing, public key signatures, and RFC-3161 timestamping Work with newer drive and interface technologies like NVME, SATA Express, 4K-native sector drives, SSHDs, SAS, UASP/USB3x, and Thunderbolt Manage drive security such as ATA passwords; encrypted thumb drives; Opal self-encrypting drives; OS-encrypted drives using BitLocker, FileVault,

and TrueCrypt; and others Acquire usable images from more complex or challenging situations such as RAID systems, virtual machine images, and damaged media With its unique focus on digital forensic acquisition and evidence preservation, Practical Forensic Imaging is a valuable resource for experienced digital forensic investigators wanting to advance their Linux skills and experienced Linux administrators wanting to learn digital forensics. This is a must-have reference for every digital forensics lab.

## Morton Hall

## Food, Faith, and Facing My Fears

There once were two sisters who were like the two rose-trees. One was called Snow-white and the other Rose-Red. Twenty years after the treaty of the Wicked Witches was signed, odd events began occurring in the town of Thistle Grove, a small village on the edge of the Woods. Bears started to appear in the Woods and small children disappeared. Was Paulina the Malevolent breaking the peace and up to no good? But when Red's beloved, Griffin, goes missing she knows she has to help rescue him. With the help of wolf in sheriff's clothing and their friend Ruby, Snow and Red begin a journey that will take them in conflict with Wicked Witches, Goblins, and bear shifters. Will they be able to solve the disappearance of their friends and town people? Or will the Treaty of the Wicked Witches be smashed and the peace of Thistle Grove destroyed forever?

## Computer Forensics : A Practical Guide

This textbook provides an introduction to digital forensics, a rapidly evolving field for solving crimes. Beginning with the basic concepts of computer forensics, each of the book’s 21 chapters focuses on a particular forensic topic composed of two parts: background knowledge and hands-on experience through practice exercises. Each theoretical or background section concludes with a series of review questions, which are prepared to test students’ understanding of the materials, while the practice exercises are intended to afford students the opportunity to apply the concepts introduced in the section on background knowledge. This experience-oriented textbook is meant to assist students in gaining a better understanding of digital forensics through hands-on practice in collecting and preserving digital evidence by completing various exercises. With 20 student-directed, inquiry-based practice exercises, students will better understand digital forensic concepts and learn digital forensic investigation techniques. This textbook is intended for upper undergraduate and graduate-level students who are taking digital-forensic related courses or working in digital forensics research. It can also be used by digital forensics practitioners, IT security analysts, and security engineers working in the IT security industry, particular IT professionals responsible for digital investigation and incident handling or researchers working in these related fields as a reference book.

## Practical Forensic Imaging

Maximize the power of Windows Forensics to perform highly effective forensic investigations About This Book Prepare and perform investigations using powerful tools for Windows, Collect and validate evidence from suspects and computers and uncover clues that are otherwise difficult Packed with powerful recipes to perform highly effective field investigations Who This Book Is For If you are a forensic analyst or incident response professional who wants to perform computer forensics investigations for the Windows platform and expand your took kit, then this book is for you. What You Will Learn Understand the challenges of acquiring evidence from Windows systems and overcome them Acquire and analyze Windows memory and drive data with modern forensic tools. Extract and analyze data from Windows file systems, shadow copies and the registry Understand the main Windows system artifacts and learn how to parse data from them using forensic tools See a forensic analysis of common web browsers, mailboxes, and instant messenger services Discover how Windows 10 differs from previous versions and how to overcome the specific challenges it presents Create a graphical timeline and visualize data, which can then be incorporated into the final report Troubleshoot issues that arise while performing Windows forensics In Detail Windows Forensics Cookbook provides recipes to overcome forensic challenges and helps you carry out effective investigations easily on a Windows platform. You will begin with a refresher on digital forensics and evidence acquisition, which will help you to understand the challenges faced while acquiring evidence from Windows systems. Next you will learn to acquire Windows memory data and analyze Windows systems with modern forensic tools. We also cover some more in-depth elements of forensic analysis, such as how to analyze data from Windows system artifacts, parse data from the most commonly-used web browsers and email services, and effectively report on digital forensic investigations. You will see how Windows 10 is different from previous versions and how you can overcome the specific challenges it brings. Finally, you will learn to troubleshoot issues that arise while performing digital forensic investigations. By the end of the book, you will be able to carry out forensics investigations efficiently. Style and approach This practical guide filled with hands-on, actionable recipes to detect, capture, and recover digital artifacts and deliver impeccable forensic outcomes.

## Practical Mobile Forensics

## Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice

The Digital Forensics Workbook is a filled with over 60 hands-on activities using over 40 different tools for digital forensic examiners who want to gain practice acquiring and analyzing digital data. Topics include analysis of media, network traffic, memory, and mobile apps. By becoming proficient in these activities, examiners can then focus on the recovered data and conduct in-depth analyses. This workbook was designed to augment existing digital forensics learning, whether it be formalized academic courses, industry training classes, on-the-job learning, or independent studying. The hands-on activities include step-by-step procedures for the reader so they obtain the identical results presented in the workbook. Activities include over 150 questions and answers to reinforce content.

Additional exercises with answers are also provided so readers can apply what they have learned.

## Windows Forensics Cookbook

Every computer crime leaves tracks–you just have to know where to find them. This book shows you how to collect and analyze the digital evidence left behind in a digital crime scene. Computers have always been susceptible to unwanted intrusions, but as the sophistication of computer technology increases so does the need to anticipate, and safeguard against, a corresponding rise in computer-related criminal activity. Computer forensics, the newest branch of computer security, focuses on the aftermath of a computer security incident. The goal of computer forensics is to conduct a structured investigation to determine exactly what happened, who was responsible, and to perform the investigation in such a way that the results are useful in a criminal proceeding. Written by two experts in digital investigation, Computer Forensics provides extensive information on how to handle the computer as evidence. Kruse and Heiser walk the reader through the complete forensics process–from the initial collection of evidence through the final report. Topics include an overview of the forensic relevance of encryption, the examination of digital evidence for clues, and the most effective way to present your evidence and conclusions in court. Unique forensic issues associated with both the Unix and the Windows NT/2000 operating systems are thoroughly covered. This book provides a detailed methodology for collecting, preserving, and effectively using evidence by addressing the three A's of computer forensics: Acquire the evidence without altering or damaging the original data. Authenticate that your recorded evidence is the same as the original seized data. Analyze the data without modifying the recovered data. Computer Forensics is written for everyone who is responsible for investigating digital criminal incidents or who may be interested in the techniques that such investigators use. It is equally helpful to those investigating hacked web servers, and those who are investigating the source of illegal pornography.

## Computer Forensics

As computer and internet technologies continue to advance at a fast pace, the rate of cybercrimes is increasing. Crimes employing mobile devices, data embedding/mining systems, computers, network communications, or any malware impose a huge threat to data security, while cyberbullying, cyberstalking, child pornography, and trafficking crimes are made easier through the anonymity of the internet. New developments in digital forensics tools and an understanding of current criminal activities can greatly assist in minimizing attacks on individuals, organizations, and society as a whole. Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice addresses current challenges and issues emerging in cyber forensics and new investigative tools and methods that can be adopted and implemented to address these issues and counter security breaches within various organizations. It also examines a variety of topics such as advanced techniques for forensic developments in computer and communication-link environments and legal perspectives including procedures for cyber investigations, standards, and policies. Highlighting a range of topics such as cybercrime, threat detection, and forensic science, this publication is an ideal

reference source for security analysts, law enforcement, lawmakers, government officials, IT professionals, researchers, practitioners, academicians, and students currently investigating the up-and-coming aspects surrounding network security, computer science, and security engineering.

## Digital and Document Examination

Learn the skills you need to take advantage of Kali Linux for digital forensics investigations using this comprehensive guide Key Features Master powerful Kali Linux tools for digital investigation and analysis Perform evidence acquisition, preservation, and analysis using various tools within Kali Linux Implement the concept of cryptographic hashing and imaging using Kali Linux Perform memory forensics with Volatility and internet forensics with Xplico. Discover the capabilities of professional forensic tools such as Autopsy and DFF (Digital Forensic Framework) used by law enforcement and military personnel alike Book Description Kali Linux is a Linux-based distribution used mainly for penetration testing and digital forensics. It has a wide range of tools to help in forensics investigations and incident response mechanisms. You will start by understanding the fundamentals of digital forensics and setting up your Kali Linux environment to perform different investigation practices. The book will delve into the realm of operating systems and the various formats for file storage, including secret hiding places unseen by the end user or even the operating system. The book will also teach you to create forensic images of data and maintain integrity using hashing tools. Next, you will also master some advanced topics such as autopsies and acquiring investigation data from the network, operating system memory, and so on. The book introduces you to powerful tools that will take your forensic abilities and investigations to a professional level, catering for all aspects of full digital forensic investigations from hashing to reporting. By the end of this book, you will have had hands-on experience in implementing all the pillars of digital forensics—acquisition, extraction, analysis, and presentation using Kali Linux tools. What you will learn Get to grips with the fundamentals of digital forensics and explore best practices Understand the workings of file systems, storage, and data fundamentals Discover incident response procedures and best practices Use DC3DD and Guymager for acquisition and preservation techniques Recover deleted data with Foremost and Scalpel Find evidence of accessed programs and malicious programs using Volatility. Perform network and internet capture analysis with Xplico Carry out professional digital forensics investigations using the DFF and Autopsy automated forensic suites Who this book is for This book is targeted at forensics and digital investigators, security analysts, or any stakeholder interested in learning digital forensics using Kali Linux. Basic knowledge of Kali Linux will be an advantage.

## Forensic Examination of Windows-Supported File Systems

A practical guide to deploying digital forensic techniques in response to cyber security incidents About This Book Learn incident response fundamentals and create an effective incident response framework Master forensics investigation utilizing digital investigative techniques Contains real-life scenarios that effectively use threat intelligence and modeling techniques Who This Book Is For This book is targeted at Information Security professionals, forensics practitioners, and

students with knowledge and experience in the use of software applications and basic command-line experience. It will also help professionals who are new to the incident response/digital forensics role within their organization. What You Will Learn Create and deploy incident response capabilities within your organization Build a solid foundation for acquiring and handling suitable evidence for later analysis Analyze collected evidence and determine the root cause of a security incident Learn to integrate digital forensic techniques and procedures into the overall incident response process Integrate threat intelligence in digital evidence analysis Prepare written documentation for use internally or with external parties such as regulators or law enforcement agencies In Detail Digital Forensics and Incident Response will guide you through the entire spectrum of tasks associated with incident response, starting with preparatory activities associated with creating an incident response plan and creating a digital forensics capability within your own organization. You will then begin a detailed examination of digital forensic techniques including acquiring evidence, examining volatile memory, hard drive assessment, and network-based evidence. You will also explore the role that threat intelligence plays in the incident response process. Finally, a detailed section on preparing reports will help you prepare a written report for use either internally or in a courtroom. By the end of the book, you will have mastered forensic techniques and incident response and you will have a solid foundation on which to increase your ability to investigate such incidents in your organization. Style and approach The book covers practical scenarios and examples in an enterprise setting to give you an understanding of how digital forensics integrates with the overall response to cyber security incidents. You will also learn the proper use of tools and techniques to investigate common cyber security incidents such as malware infestation, memory analysis, disk analysis, and network analysis.

## Imaging for Forensics and Security

Get up and running with collecting evidence using forensics best practices to present your findings in judicial or administrative proceedings Key Features Learn the core techniques of computer forensics to acquire and secure digital evidence skillfully Conduct a digital forensic examination and document the digital evidence collected Analyze security systems and overcome complex challenges with a variety of forensic investigations Book Description A computer forensics investigator must possess a variety of skills, including the ability to answer legal questions, gather and document evidence, and prepare for an investigation. This book will help you get up and running with using digital forensic tools and techniques to investigate cybercrimes successfully. Starting with an overview of forensics and all the open source and commercial tools needed to get the job done, you'll learn core forensic practices for searching databases and analyzing data over networks, personal devices, and web applications. You'll then learn how to acquire valuable information from different places, such as filesystems, e-mails, browser histories, and search queries, and capture data remotely. As you advance, this book will guide you through implementing forensic techniques on multiple platforms, such as Windows, Linux, and macOS, to demonstrate how to recover valuable information as evidence. Finally, you'll get to grips with presenting your findings efficiently in judicial or administrative proceedings. By the end of this book, you'll have developed a clear understanding of how to acquire, analyze, and present digital evidence like a proficient computer forensics investigator. What you

will learn Understand investigative processes, the rules of evidence, and ethical guidelines Recognize and document different types of computer hardware Understand the boot process covering BIOS, UEFI, and the boot sequence Validate forensic hardware and software Discover the locations of common Windows artifacts Document your findings using technically correct terminology Who this book is for If you're an IT beginner, student, or an investigator in the public or private sector this book is for you.This book will also help professionals and investigators who are new to incident response and digital forensics and interested in making a career in the cybersecurity domain.

## Conquering Babel

Learners will master the skills necessary to launch and complete a successful computer investigation with the updated fourth edition of this popular book, GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS. This resource guides readers through conducting a high-tech investigation, from acquiring digital evidence to reporting its findings. Updated coverage includes new software and technologies as well as up-to-date reference sections. Learn how to set up a forensics lab, how to acquire the proper and necessary tools, and how to conduct the investigation and subsequent digital analysis. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

## Red

Provides an overview and case studies of computer crimes and discusses topics including data recovery, evidence collection, preservation of digital evidence, information warfare, and the cyber underground.

## Network Forensics

## A Practical Guide to Computer Forensics Investigations

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

## A Practical Guide to Computer Forensics Investigations

"The Adventures of Tom Sawyer" – Tom Sawyer lives with his Aunt Polly and his half-brother Sid. He skips school to swim and is made to whitewash the fence the next day as punishment. Tom falls in love with Becky Thatcher, a new girl in town, but shortly after Becky shuns him, he accompanies Huckleberry Finn to the graveyard at night, where they witness a trio of body snatchers getting into a fight. Tom and Huck run away to an island. While enjoying their new-found freedom, they become aware that the community is sounding the river for their bodies… "Adventures of Huckleberry Finn" – Huck Finn and his friend Tom Sawyer have each come into a considerable sum of money as a result of their earlier adventures. Huck is placed under the guardianship of the Widow Douglas, who is attempting to "sivilize" him. Finding civilized life confining, his spirits are raised somewhat when Tom helps him to escape one night, but his alcoholic father turns up and kidnaps him… "Tom Sawyer Abroad" – Tom, Huck, and their friend Jim set sail to Africa in a futuristic hot air balloon, where they survive encounters with lions, robbers, and fleas to see some of the world's greatest wonders, including the Pyramids and the Sphinx. "Tom Sawyer, Detective" – Tom attempts to solve a mysterious murder in this burlesque of the immensely popular detective novels of the time. Samuel Langhorne Clemens (1835-1910), better known by his pen name Mark Twain, was an American writer, humorist, entrepreneur, publisher, and lecturer.

## Guide to Computer Forensics and Investigations

“This is a must-have work for anybody in information security, digital forensics, or involved with incident handling. As we move away from traditional disk-based analysis into the interconnectivity of the cloud, Sherri and Jonathan have created a framework and roadmap that will act as a seminal work in this developing field.” – Dr. Craig S. Wright (GSE), Asia Pacific Director at Global Institute for Cyber Security + Research. “It’s like a symphony meeting an encyclopedia meeting a spy novel.” –Michael Ford, Corero Network Security On the Internet, every action leaves a mark–in routers, firewalls, web proxies, and within network traffic itself. When a hacker breaks into a bank, or an insider smuggles secrets to a competitor, evidence of the crime is always left behind. Learn to recognize hackers’ tracks and uncover network-based evidence in Network Forensics: Tracking Hackers through Cyberspace. Carve suspicious email attachments from packet captures. Use flow records to track an intruder as he pivots through the network. Analyze a real-world wireless encryption-cracking attack (and then crack the key yourself). Reconstruct a suspect’s web surfing history–and cached web pages, too–from a web proxy. Uncover DNS-tunneled traffic. Dissect the Operation Aurora exploit, caught on the wire. Throughout the text, step-by-step case studies guide you through the analysis of network-based evidence. You can download the evidence files from the authors’ web site (lmgsecurity.com), and follow along to gain hands-on experience. Hackers leave footprints all across the Internet. Can you find their tracks and solve

the case? Pick up Network Forensics and find out.

## Digital Forensics Workbook

## Learn Computer Forensics

Imaging for Forensics and Security: From Theory to Practice provides a detailed analysis of new imaging and pattern recognition techniques for the understanding and deployment of biometrics and forensic techniques as practical solutions to increase security. It contains a collection of the recent advances in the technology ranging from theory, design, and implementation to performance evaluation of biometric and forensic systems. This book also contains new methods such as the multiscale approach, directional filter bank, and wavelet maxima for the development of practical solutions to biometric problems. The book introduces a new forensic system based on shoeprint imagery with advanced techniques for use in forensics applications. It also presents the concept of protecting the originality of biometric images stored in databases against intentional and unintentional attacks and fraud detection data in order to further increase the security.

## Small Ball

Forensic science is the branch of science that deals to investigate crimes using scientific methods. Whereas digital or computer forensic is the branch of forensic science that used to investigate electronic crimes. Computer forensics involves some techniques to capture important data that would be useful in your reports and reports should be admissible evidence to court. Electronic crimes involves electronic data including money laundering, espionage, piracy theft, extortion, malware attacks, spoofing, key logging. These crimes can be investigated using scientific methods. In this book, data acquisition described, that is the first step in computer forensics. Data acquisition involves bit-streaming which means you can create an image file of your data with the same date and time because using bit-streaming you can’t compromise your evidence. In this book, we described bit-streaming with advance tools and techniques. We used more than three tools to acquire data only. Here’s the question, why we acquire data and why bit-streaming is important for computer forensics and investigation. When a cyber-incident happens, it is very important for a cybercrime analyst to use standard ways to response against that incident. Incident response based on logical as well as physical. When cybercrime analyst responses against cyber-attack, one thing must be understand to diagnose system states (described in this book also) and actions, what he/she must do if system is alive or dead. In this book we explained not only acquisition but we also explored advance methods to acquire data. Data acquisition is applied when you want to get whole image of suspect machine. You can also acquire data using live acquisition method or offline method. Live acquisition can be done using universal live acquisition tool Helix or using your server also. In this book we also elaborated different tools used in Helix.

## Digital Forensics and Incident Response

You don’t need to be a wizard to transform a game you like into a game you love. Imagine if you could give your favorite PC game a more informative heads-up display or instantly collect all that loot from your latest epic battle. Bring your knowledge of Windows-based development and memory management, and Game Hacking will teach you what you need to become a true game hacker. Learn the basics, like reverse engineering, assembly code analysis, programmatic memory manipulation, and code injection, and hone your new skills with hands-on example code and practice binaries. Level up as you learn how to: *Scan and modify memory with Cheat Engine *Explore program structure and execution flow with OllyDbg *Log processes and pinpoint useful data files with Process Monitor *Manipulate control flow through NOPing, hooking, and more *Locate and dissect common game memory structures You’ll even discover the secrets behind common game bots, including: *Extrasensory perception hacks, such as wallhacks and heads-up displays *Responsive hacks, such as autohealers and combo bots *Bots with artificial intelligence, such as cave walkers and automatic looters Game hacking might seem like black magic, but it doesn’t have to be. Once you understand how bots are made, you’ll be better positioned to defend against them in your own games. Journey through the inner workings of PC games with Game Hacking, and leave with a deeper understanding of both game design and computer security.

## Advances in Communications, Computing, Networks and Security

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.

## Practical Forensic Imaging

"Cybercrime and cyber-terrorism represent a serious challenge to society as a whole." - Hans Christian Krüger, Deputy Secretary General of the Council of Europe Crime has been with us as long as laws have existed, and modern technology has given us a new type of criminal activity: cybercrime. Computer and network related crime is a problem that spans the globe, and unites those in two disparate fields: law enforcement and information technology. This book will help both IT pros and law enforcement specialists understand both their own roles and those of the other, and show why that understanding and an organized, cooperative effort is necessary to win the fight against this new type of crime. 62% of US companies reported computer-related security breaches resulting in damages of $124 million dollars. This data is an indication of the massive need for Cybercrime training within the IT and law enforcement communities. The only book that covers Cybercrime from forensic investigation through prosecution. Cybercrime is one of the battlefields in the war against terror.

## Digital Image Forensics

"Food, Faith & Facing My Fears" plunges into my lifelong pursuit of perfection and the inevitable eating disorder that accompanied it. It uncorks the intimate details of a journey bubbling with pain and isolation, as well as self-love and resurrection. As a sixteen year old girl I, along with many others, fell victim to the body-image pressures of society. After finally claiming the rights of a toned, thin, "dream" body, I soon figured out that it wasn't as great as I'd expected - it was actually much worse.Leaked are my raw insecurities and the peculiar ways I found security in the mayhem my life becomes. This book proves that, in a world that promotes the opposite, our appearances do not cradle the keys to our happiness. This is a story of tears, tenacity, and testimony. This is my story of how I transformed my rocky relationship with food, my body, and my wealth of fears into a sovereign, overflowing Faith in God.

## The Adventures of Tom Sawyer & Huckleberry Finn - Complete Edition

This work introduces the reader to the world of digital forensics in a practical and accessible manner. The text was written to fulfill a need for a book that introduces forensic methodology and sound forensic thinking, combined with hands-on examples for common tasks in a computer forensic examination. The author has several years of experience as a computer forensics examiner and is now working as a university-level lecturer. Guide to Digital Forensics: A Concise and Practical Introduction is intended for students that are looking for an introduction to computer forensics and can also be used as a collection of instructions for practitioners. The aim is to describe and explain the steps taken during a forensic examination, with the intent of making the reader aware of the constraints and considerations that apply during a fo rensic examination in law enforcement and in the private sector. Upon reading this book, the reader should have a proper overview of the field of digital forensics, starting them on the journey of becoming a computer forensics expert.

## Practical Forensic Imaging

## Titanic

September 11th, 2001 was America's wake up call to terrorism. Unfortunately, we hit the snooze alarm. The next wave of terror attacks won't be nation shaking, cataclysmic events. We're ready for that. Instead, they'll be minor, localized nightmares. Mere pinpricks to our country, but catastrophic to the small towns that find themselves in the crosshairs. Worst of all, there's nothing we can do to stop it from happening - or is there? A gritty novel extrapolated from real world events, this fast-paced, riveting thriller will leave you alarmed, angry, and awestruck at America's unpreparedness for the next wave of terror attacks. Some might refer to it as death by a thousand cuts, but the counterterrorism community calls it Small Ball. Small Ball is an indictment of our woefully wrongheaded security infrastructure and a testament to the resilience, resourcefulness, and integrity of

the average American. You'll wonder why it hasn't happened already. Perhaps it's happening right now

## Suddenly Today We Can Dream

This was one of the first books to appear after the sinking of the Titanic, published just 37 days after the disaster, and despite the haste it is one of the most stylish and well-written of the early works. Its author, Filson Young, was a respected journalist who had already used his columns in the London Saturday Review and the Pall Mall Gazette to call for better safety at sea, and for all ships to have properly-manned radios. Having sailed the Atlantic himself, and knowing several of the passengers on board the doomed liner, his book combines an imaginative telling of the first few days on board, with a vivid account of the sinking based on early survivor interviews. In 1932 the BBC asked Filson to dramatise the book for radio, but a public outcry forced them to reconsider: even after twenty years, his recreation of the sinking was still too powerful for many of their audience.

## Digital Forensics with Open Source Tools

Security is a major concern in an increasingly multimedia-defined universe where the Internet serves as an indispensable resource for information and entertainment. Digital Rights Management (DRM) is the technology by which network systems protect and provide access to critical and time-sensitive copyrighted material and/or personal information. This book equips savvy technology professionals and their aspiring collegiate protégés with the latest technologies, strategies and methodologies needed to successfully thwart off those who thrive on security holes and weaknesses. Filled with sample application scenarios and algorithms, this book provides an in-depth examination of present and future field technologies including encryption, authentication, copy control, tagging, tracing, conditional access and media identification. The authors present a diversified blend of theory and practice and focus on the constantly changing developments in multimedia applications thus providing an admirably comprehensive book. * Discusses state-of-the-art multimedia authentication and fingerprinting techniques * Presents several practical methodologies from industry, including broadcast encryption, digital media forensics and 3D mesh watermarking * Focuses on the need for security in multimedia applications found on computer networks, cell phones and emerging mobile computing devices

## Scene of the Cybercrime: Computer Forensics Handbook

Photographic imagery has come a long way from the pinhole cameras of the nineteenth century. Digital imagery, and its applications, develops in tandem with contemporary society’s sophisticated literacy of this subtle medium. This book examines the ways in which digital images have become ever more ubiquitous as legal and medical evidence, just as they have become our primary source of news and have replaced paper-based financial documentation. Crucially, the contributions also analyze the very profound problems which have arisen alongside the digital image, issues of veracity and progeny that demand systematic and detailed response: It looks real, but is it? What camera captured it? Has it been

doctored or subtly altered? Attempting to provide answers to these slippery issues, the book covers how digital images are created, processed and stored before moving on to set out the latest techniques for forensically examining images, and finally addressing practical issues such as courtroom admissibility. In an environment where even novice users can alter digital media, this authoritative publication will do much so stabilize public trust in these real, yet vastly flexible, images of the world around us.

## Guide to Digital Forensics

Forensic image acquisition is an important part of postmortem incident response and evidence collection. Digital forensic investigators acquire, preserve, and manage digital evidence to support civil and criminal cases; examine organizational policy violations; resolve disputes; and analyze cyber attacks. Practical Forensic Imaging takes a detailed look at how to secure and manage digital evidence using Linux-based command line tools. This essential guide walks you through the entire forensic acquisition process and covers a wide range of practical scenarios and situations related to the imaging of storage media. You'll learn how to: –Perform forensic imaging of magnetic hard disks, SSDs and flash drives, optical discs, magnetic tapes, and legacy technologies –Protect attached evidence media from accidental modification –Manage large forensic image files, storage capacity, image format conversion, compression, splitting, duplication, secure transfer and storage, and secure disposal –Preserve and verify evidence integrity with cryptographic and piecewise hashing, public key signatures, and RFC-3161 timestamping –Work with newer drive and interface technologies like NVME, SATA Express, 4K-native sector drives, SSHDs, SAS, UASP/USB3x, and Thunderbolt –Manage drive security such as ATA passwords; encrypted thumb drives; Opal self-encrypting drives; OS-encrypted drives using BitLocker, FileVault, and TrueCrypt; and others –Acquire usable images from more complex or challenging situations such as RAID systems, virtual machine images, and damaged media With its unique focus on digital forensic acquisition and evidence preservation, Practical Forensic Imaging is a valuable resource for experienced digital forensic investigators wanting to advance their Linux skills and experienced Linux administrators wanting to learn digital forensics. This is a must-have reference for every digital forensics lab.

## Real digital forensics