Preface

Purpose of This Book

This book is part of the Information Systems Security & Assurance Series from Jones & Bartlett Learning (*www.jblearning.com*). Designed for courses and curriculums in IT Security, Cybersecurity, Information Assurance, and Information Systems Security, this series features a comprehensive, consistent treatment of the most current thinking and trends in this critical subject area. These titles deliver fundamental information-security principles packed with real-world applications and examples. Authored by Certified Information Systems Security Professionals, they deliver comprehensive information on all aspects of information security. Reviewed word for word by leading technical experts in the field, these books are not just current, but forward-thinking—putting you in the position to solve the cybersecurity challenges not just of today, but of tomorrow, as well.

Computer crimes call for forensics specialists—people who know how to find and follow the evidence. But even aside from criminal investigations, incident response requires forensic skills. This book begins by examining the fundamentals of system forensics: what forensics is, an overview of computer crime, the challenges of system forensics, and forensics methods and labs. The second part of this book addresses the tools, techniques, and methods used to perform computer forensics and investigation. These include collecting evidence, investigating information hiding, recovering data, and scrutinizing email. It also discusses how to perform forensics in the Windows, Linux, and Macintosh operating systems; on mobile devices; and on networks. Finally, the third part explores incident and intrusion response, emerging technologies and future directions of this field, and additional system forensics resources.

Learning Features

The writing style of this book is practical and conversational. Each chapter begins with a statement of learning objectives. Step-by-step examples of information security concepts and procedures are presented throughout the text. Illustrations are used both to clarify the material and to vary the presentation. The text is sprinkled with Notes, Tips, FYIs, Warnings, and sidebars to alert the reader to additional helpful information related to the subject under discussion. Chapter Assessments appear at the end of each chapter, with solutions provided in the back of the book.

Chapter summaries are included in the text to provide a rapid review or preview of the material and to help students understand the relative importance of the concepts presented.

Audience

The material is suitable for undergraduate or graduate computer science majors or information science majors, students at a two-year technical college or community college who have a basic technical background, or readers who have a basic understanding of IT security and want to expand their knowledge.

This book is dedicated to all the forensic analysts who work diligently to extract the evidence necessary to find the truth in criminal and civil cases.