CHAPTER 4  Forensics Methods and Labs  57

Forensic Soundness  58

Forensic Frameworks and Processes  60

The DFRWS Framework  60
An Event-Based Digital Forensic Investigation Framework  60

Building a Business Case for Creating a Forensics Lab  62

Setting Up a Forensics Lab  64

The Duties of a Lab Manager and Staff  65
Planning a Forensics Lab Budget  65
Determining Physical Requirements for a Computer Forensics Lab  69
Stocking a Forensics Lab  74

Policies, Processes, and Procedures for Maintaining a Lab  77

Creating a Disaster Recovery Plan  77
Planning for Equipment Upgrades  78

CHAPTER SUMMARY  79

KEY CONCEPTS AND TERMS  79

CHAPTER 4 ASSESSMENT  80

PART TWO  Technical Overview:
System Forensics Tools, Techniques, and Methods  81

CHAPTER 5  System Forensics Technologies  82

How the Military Uses System Forensics  83

Which Technologies Law Enforcement Agencies Use  83

Evidence Preservation  84
Trojan Horse Programs  84
Documentation of Methodologies and Findings  85
Disk Structure  85
File Slack Searching  85
Data-Hiding Techniques  85
Fuzzy Logic Tools for Identifying Unknown Text  88
Data Encryption  88
Disk-to-Computer Matching  88
Data Compression  88
Recovery of Erased Files  89
Internet Abuse Identification and Detection  89
The Boot Process and Memory-Resident Programs  89
Flash Memory Media Processing  89
How Businesses Use System Forensics Technologies 89
Remote Monitoring of Target Computers 92
Trackable Electronic Documents 92
Theft Recovery Software for Laptops and PCs 92
Handling Evidence 93
Encryption Methods and Vulnerabilities 95
Security and Wireless Technologies 98
Firewall Forensics 100
Commonly Used System Forensics Tools 102
EnCase 102
Forensic Toolkit (FTK) 102
Helix 102
AnaDisk Disk Analysis Tool 103
CopyQM Plus Disk Duplication Software 103
TextSearch Plus 103
Filter_G Intelligent Forensic Filter 104
UFED 104
Device Seizure 104
The Zdziarski Technique 105
CHAPTER SUMMARY 106
KEY CONCEPTS AND TERMS 106
CHAPTER 5 ASSESSMENT 106

CHAPTER 6 Controlling a Forensic Investigation 108
Preserving a Digital Crime Scene 109
Considerations in Collecting Evidence 111
Securing the Physical Evidence 112
Volatile Data: Two Schools of Thought 112
Determining How Much to Duplicate 113
Making a Bit Stream Backup 114
Booting a Computer 116
Examining Evidence 116
Physical Analysis and Logical Analysis 118
Physical Analysis 118
Logical Analysis 121
Legal Aspects of Acquiring Evidence 122
The Fourth Amendment 123
Processing and Logging Evidence 124
The Computer Evidence Collection Process 126
CHAPTER SUMMARY 128
KEY CONCEPTS AND TERMS 128
CHAPTER 6 ASSESSMENT 129
CHAPTER 7 Collecting, Seizing, and Protecting Evidence 130

Collecting Forensic Evidence 131
Obstacles to Data Collection 132
Types of Forensic Evidence 133
The Rules of Evidence 133
Do’s and Don’ts of Data Collection 134
Logging and Monitoring 136
Methods of Data Collection: Freezing the Scene and Honeypotting 136

The Steps in Seizing Forensic Evidence 138
Shutting Down the Computer 138
Documenting the Hardware Configuration of the System 139
Transporting the Computer System to a Secure Location 139
Mathematically Authenticating Data on All Storage Devices 139
Making a List of Key Search Words 140
Searching Files, File Slack, and Unallocated Space for Keywords 141
Documenting Filenames, Dates, and Times 142
Identifying File, Program, and Storage Anomalies 142
Evaluating Program Functionality 143
Documenting Findings 143
Retaining Copies of Software Used 143

Protecting Evidence: Controlling Contamination 143
Creating a Timeline 144
Forensic Analysis of Backups 145
Reconstructing an Attack 145

CHAPTER SUMMARY 146
KEY CONCEPTS AND TERMS 146
CHAPTER 7 ASSESSMENT 147

CHAPTER 8 Understanding Information-Hiding Techniques 148

History of Data Hiding 149
Alternate Data Streams (ADS) 151
Risks Associated With ADS 151
Executing Code From ADS 153
Rootkits 154
Steganography Concepts and Tools 155
Types of Steganography 155
Steganography Algorithms 156
Steganography Software 158

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.
## Contents

Defeating Steganography 161  
Detecting the Use of Steganography Software 161  
Strengths and Weaknesses of Today’s Detection Methods 163  
Steganalysis 164  
Extracting Hidden Information 165  
Steganalysis Software 166

**CHAPTER SUMMARY** 167  
**KEY CONCEPTS AND TERMS** 168  
**CHAPTER 8 ASSESSMENT** 168

<table>
<thead>
<tr>
<th>CHAPTER 9</th>
<th>Recovering Data</th>
<th>170</th>
</tr>
</thead>
<tbody>
<tr>
<td>What Is Data Recovery?</td>
<td>171</td>
<td></td>
</tr>
</tbody>
</table>
| Disk Structure and Recovery Techniques | 172  
  Recovering Data After Physical Damage | 172  
  Recovering Data After Logical Damage | 174 |
| Data Backup and Recovery | 176  
  Obstacles to Data Backup | 177  
  Key Elements of Data Backup | 178  
  The Role of Backups in Data Recovery | 182 |
| Data Recovery Today | 183  
  Handling Failures | 184  
  Critical Thinking and Creative Problem Solving | 184  
  Preparing for Recovery | 185 |

**CHAPTER SUMMARY** 187  
**KEY CONCEPTS AND TERMS** 187  
**CHAPTER 9 ASSESSMENT** 188

<table>
<thead>
<tr>
<th>CHAPTER 10</th>
<th>Investigating and Scrutinizing E-mail</th>
<th>189</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Roles of Mail Servers and E-mail Clients</td>
<td>190</td>
<td></td>
</tr>
</tbody>
</table>
| Understanding E-mail Headers | 192  
  Viewing an E-mail Header | 193  
  Interpreting an E-mail Header | 194 |
| E-mail Tracing | 195  
  Faking E-mail | 196  
  E-mail Tracing in Forensic Investigations | 200  
  An E-mail Tracing Example | 201 |
| Legal Considerations in Investigating E-mail | 203  
  The Fourth Amendment to the U.S. Constitution | 204  
  The Electronic Communications Privacy Act | 204 |

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.
CHAPTER 11 Performing Network Analysis 207
Network Basics 208
  Wireless Networks 209
  Common Network Protocols 211
Types of Network-Related Attacks 211
  Types of Router Attacks 213
  DoS Attacks 213
  Web Attacks 214
Investigating Network Traffic 215
  Using Log Files as Evidence 216
  Firewall Forensics 217
  Using Sniffers and Other Traffic Analysis Tools 221
Investigating Router Attacks 221
  Collecting Router Evidence 223
  Router Logs 224
CHAPTER SUMMARY 226
KEY CONCEPTS AND TERMS 226
CHAPTER 11 ASSESSMENT 227

CHAPTER 12 Searching Memory in Real Time with Live System Forensics 228
The Need for Live System Forensics 229
Live System Forensics Versus Dead System Analysis 230
  Problems with Dead System Forensics 231
  Live Forensic Acquisition 232
  Benefits and Limitations of Live Acquisition 235
Live System Forensics Consistency Issues 237
  Understanding the Consistency Problem 238
  Locating Different Memory Segments in UNIX 240
Tools for Analyzing Computer Memory 240
  Live Response 241
  Volatile Memory Analysis 243
  Analysis of Live Response Versus Volatile Memory Analysis 245
CHAPTER SUMMARY 247
KEY CONCEPTS AND TERMS 248
CHAPTER 12 ASSESSMENT 248
CHAPTER SUMMARY 287
KEY CONCEPTS AND TERMS 287
CHAPTER 14 ASSESSMENT 288

CHAPTER 15 System Forensics Resources 289
System Forensics Certification and Training 290
  International Association of Computer Investigative Specialists (IACIS) 290
  High Tech Crime Network (HTCN) 291
  EnCase Certified Examiner (EnCE) Certification 291
  AccessData Certified Examiner (ACE) 291
  Defense Cyber Investigations Training Academy (DCITA) 292
Other Training Programs and Certifications 292
User Groups 293
Online Resources 293
  System Forensics Organizations and Information 293
  Discussion List Servers 294
  Forensic Journals 295
  Conferences 295
  Forensic Tools 296
CHAPTER SUMMARY 305
KEY CONCEPTS AND TERMS 305
CHAPTER 15 ASSESSMENT 305

APPENDIX A Answer Key 307
APPENDIX B Standard Acronyms 309
  Glossary of Key Terms 311
References 323
Index 329

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.
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 (CISSPs), 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. 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, scrutinizing e-mail, and searching memory in real time. 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.
The authors would like to thank the following individuals and organizations for granting permission to re-use materials in this book:


The publisher wishes to extend special thanks to Kitty Wilson, whose yeoman efforts made this book possible.
About the Authors

JOHN R. VACCA is an information technology consultant and internationally known best-selling author based in Pomeroy, Ohio. Since 1982, John has written 62 books and more than 600 articles in the areas of advanced storage, computer security, and aerospace technology. John was also a configuration management specialist, computer specialist, and the computer security official (CSO) for NASA’s space station program (Freedom) and the International Space Station Program from 1988 until his retirement from NASA in 1995. In addition, John is an independent online book reviewer. He was also one of the security consultants for the MGM movie AntiTrust, which was released in 2001.

K RUDOLPH is a Certified Information Systems Security Professional (CISSP) with a degree from Johns Hopkins University. She is the primary author of the chapter on security awareness from the Computer Security Handbook, Vol. 5, and is also the author of the chapter on security awareness in the Handbook of Information Security published in 2006 and 2009. K is a named contributor to and participant in the work group that created NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model. K has presented at conferences that include the Computer Security Institute Security Exchange (CSI SX) Conference in 2008, the New York Cyber Security Conference (2006 and 2007), the Annual CSI Computer Security Conferences (2005, 2007), and Information Assurance and Security Conferences held by FISSEA, FIAC, and eGOV. In March 2006, K was honored by the Federal Information Systems Security Educators’ Association (FISSEA) as the Security Educator of the Year.