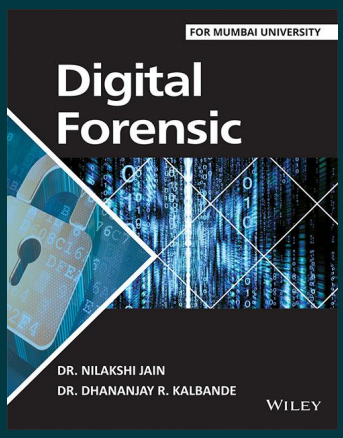

Digital Forensic: For Mumbai University

By Dr. Nilakshi Jain, Dr. Dhananjay R. Kalbande

Paperback 9788126578399 **₹1,050.00**

Pages: 320

Description

Digital Forensic is for those who desire to learn more about investigating and fighting digital crimes. This book will also help for computer professionals who want to move into the rapidly growing security field and who are considering shifting their career focus to law enforcement and criminal investigation. It is important that computer security personnel expand their knowledge of forensic processes and keep their understanding of investigative and preventive procedures up-to-date. To complete this goal, this book covers latest challenges faced in digital forensic. This book sequentially explains disk forensic, network forensic, and memory forensic.

About the Author

Dr. Nilakshi Jain, Dr. Dhananjay R. Kalbande

Dr. Nilakshi Jain is currently working as an Associate Professor at the Shah & Anchor Kutchhi Engineering College in the Information Technology Department, Mumbai, India. She is a Certified Ethical Hacker CEH (EC-Council-USA). She has a rich experience of working in Digital Forensic field. Her areas of research include Artificial Intelligence, Human Computer Interaction and Usability Engineering. She has many publications in international conference proceedings and journals, including IEEE, ACM, and Springer, etc.

Table of Contents

Preface

About the Authors

Acknowledgments

Chapter 1 Introduction to Computer Crimes and Ethical Hacking

1.1 Introduction to Cybercrime

1.2 Categories of Cybercrimes

1.3 Types of Cybercrimes

1.4 The Internet Spawns Crime

1.5 Worms Versus Viruses

1.6 Computer’s Role in Crimes

1.7 Cybercrime Statistics in India

1.8 Prevention of Cybercrime

1.9 Definition of Hacker

1.10 Definition of Crackers

1.11 Definition of Phreakers
1.12 Ethical Hacking
1.13 Difference between Hacking and Ethical Hacking
1.14 Steps of Ethical Hacking
1.15 Exploring Some Tools for Ethical Hacking
1.16 What to Do if Been Hacked?
Chapter 2 Introduction to Digital Forensics and Digital Evidences
2.1 Introduction to Digital Forensic
2.2 Need of Digital Forensic
2.3 Rules of Computer/Digital Forensic
2.4 Types of Digital Forensics
2.5 Ethical Issues
2.6 Digital Forensic Investigations
2.7 Introduction to Digital Evidences
2.8 Rules of Digital Evidence
2.9 Characteristics of Digital evidence
2.10 Types of Evidence
2.11 Challenges in Evidence Handling
Chapter 3 Incidence Response Process
3.1 Introduction
3.2 People Involved in Incident Response Process
3.3 Incident Response Process
3.4 Incident Response Methodology
3.5 Activities in Initial Response
3.6 Phases after Detection of an Incident
Chapter 4 Live Data Collection
4.1 Introduction
4.2 The Facts in a Criminal Case
4.3 People Involved in Data Collection Techniques
4.5 Live Data collection from UNIX System
Chapter 5 Forensic Duplication
5.1 Introduction to Forensic Duplication
5.2 Rules of Forensic Duplication (Thumb Rule)
5.3 Necessity of Forensic Duplication
5.4 Forensic Duplicates as Admissible Evidence
5.5 Important Terms in Forensic Duplicate
5.6 Forensic Image Formats
5.7 Traditional Duplication

5.8 Live System Duplication
5.9 Forensic Duplication Tool Requirements
5.10 Creating a Forensic Duplicate of a Hard Drive
5.11 Creating a Qualified Forensic Duplicate of a Hard Drive
Chapter 6 Disk and File System Analysis
6.1 Media Analysis Concepts
6.2 Partitioning and Disk Layouts
6.3 Special Containers
6.4 Hashing
6.5 Carving
6.6 Forensic Imaging
Chapter 7 Data Analysis
7.1 Preparation Steps for Forensic Analysis
7.2 Investigating Windows Systems
7.3 Investigating UNIX Systems
7.4 Investigating Applications
7.5 Malware Handling
Chapter 8 Network Forensic
8.1 Introduction to Network Forensic
8.2 Understanding Password Cracking
8.3 Understanding Technical Exploits
8.4 Introduction to Intrusion Detection System
8.5 Types of Intrusion Detection System
8.6 Understanding Network Intrusions and Attacks
8.7 Analyzing Network Traffic
8.8 Collecting Network-Based Evidence
8.9 Evidence Handling
8.10 Investigating Routers
8.12 Using Routers as Response Tools
Chapter 9 Report Writing
9.1 Goals of Report
9.2 Layout of an Investigative Report
9.3 Guidelines for Writing a Report
9.4 Sample for Writing a Report
Chapter 10 Computer Forensics Tools
10.1 Introduction to Computer Forensic Tools
10.2 Needs of Computer Forensics Tool
10.3 Types of Computer Forensics Tools

10.4 Tasks Performed by Computer Forensics Tools

10.5 Study of Digital Forensic Tools

Summary

Key Terms

Review Questions

Further Readings

Appendix A: Lab Experiments

Appendix B: Questions and Answers

To purchase this product, please visit:
https://www.wileyindia.com/digital-forensic-for-mumbai-university.html

Scan to buy