



Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes

By Albert J. Marcella Jr & Robert S. Greenfield
Paperback / January 2002 / 0849309557
[Link to Amazon](#)

Table of Contents

Disclaimer
Introduction
Background
Dimensions of the Problem
Computer Forensics
Works Cited

Section I: Cyber Forensics
Chapter List

Chapter 1: The Goal of the Forensic Investigation
Overview
Why Investigate
Internet Exceeds Norm
Inappropriate E.mail
Non.Work.Related Usage of Company Resources
Theft of Information
Violation of Security Parameters
Intellectual Property Infraction
Electronic Tampering
Establishing a Basis or Justification to Investigate
Determine the Impact of Incident
Who to Call/Contact
If You Are the Auditor/Investigator
Resources
Authority
Obligations/Goals
Reporting Hierarchy

Escalation Procedures
Time Frame
Procedures
Precedence
Independence

Chapter 2: How to Begin a Non.Liturgical Forensic Examination

Overview
Isolation of Equipment
Cookies
Bookmarks
History Buffer
Cache
Temporary Internet Files
Tracking of Logon Duration and Times
Recent Documents List
Tracking of Illicit Software Installation and Use

Chapter 2: How to Begin a Non.Liturgical Forensic Examination

The System Review
The Manual Review
Hidden Files
How to Correlate the Evidence
Works Cited

Chapter 3: The Liturgical Forensic Examination: Tracing Activity on a Windows.Based Desktop

Gathering Evidence For Prosecution Purposes
Gathering Evidence Without Intent to Prosecute
The Microsoft Windows.Based Computer
General Guidelines To Follow
Cookies
Bookmarks/Favorites
Internet Explorer's History Buffer
Temporary Storage on the Hard Drive
Temporary Internet Files
System Registry
Enabling and Using Auditing via the Windows Operating System
Confiscation of Computer Equipment
Other Methods of Covert Monitoring

Chapter 4: Basics of Internet Abuse: What is Possible and Where to Look Under the Hood

Terms
Types of Users
E.Mail Tracking
IP Address Construction
Browser Tattoos
How an Internet Search works
Swap Files
ISPs
Servers

Works Cited

Chapter 5: Tools of the Trade: Automated Tools Used to Secure a System Throughout the Stages of a Forensic Investigation

Overview

Detection Tools

Protection Tools

Analysis Tools

Chapter 6: Network Intrusion Management and Profiling

Overview

Common Intrusion Scenarios

Intrusion Profiling

Creating the Profile

Conclusion

Chapter 7: Cyber Forensics and the Legal System

Overview

How the System Works

Issues of Evidence

Hacker, Cracker, or Saboteur

Best Practices

Notes

Acknowledgments

Section II: Federal and International Guidelines

Chapter List

References

Chapter 8: Searching and Seizing Computers and Obtaining Electronic Evidence

Recognizing and Meeting Title III Concerns in Computer Investigations

Computer Records and the Federal Rules of Evidence

Proposed Standards for the Exchange of Digital Evidence

Recovering and Examining Computer Forensic Evidence

International Principles for Computer Evidence

Chapter 9: Computer Crime Policy and Programs

The National Infrastructure Protection Center Advisory 01.003

The National Information Infrastructure Protection Act of 1996

Distributed Denial of Service Attacks

The Melissa Virus

Cybercrime Summit: A Law Enforcement/Information Technology Industry Dialogue

Chapter 10: International Aspects of Computer Crime

Council of Europe Convention on Cybercrime

Council of Europe Convention on Cybercrime Frequently Asked Questions

Internet as the Scene of Crime

Challenges Presented to Law Enforcement by High.Tech and Computer Criminals

Problems of Criminal Procedural Law Connected with Information Technology

Combating High.Tech and Computer.Related Crime

Vienna International Child Pornography Conference

OECD Guidelines for Cryptography Policy

Fighting Cybercrime: What are the Challenges Facing Europe

Chapter 11: Privacy Issues in the High.Tech Context

Law Enforcement Concerns Related to Computerized Databases

Enforcing the Criminal Wiretap Statute

Referring Potential Privacy Violations to the Department of Justice for Investigation and Prosecution

Testimony on Digital Privacy

Chapter 12: Critical Infrastructure Protection

Attorney General Janet Reno's Speech on Critical Infrastructure Protection

Protecting the Nation's Critical Infrastructures: Presidential Decision Directive 63

The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential

Chapter 12: Critical Infrastructure Protection

Decision Directive 63

Foreign Ownership Interests in the American Communications Infrastructure

Carnivore and the Fourth Amendment

Chapter 13: Electronic Commerce: Legal Issues

Overview

Guide for Federal Agencies on Implementing Electronic Processes

Consumer Protection in the Global Electronic Marketplace

The Government Paperwork Elimination Act

Internet Gambling

Sale of Prescription Drugs Over the Internet

Guidance on Implementing the Electronic Signatures in Global And National Commerce Act (E.SIGN)

Part I: General Overview of the E.SIGN Act

The Electronic Frontier: the Challenge of Unlawful Conduct Involving the Use of the Internet

Internet Health Care Fraud

Jurisdiction in Law Suits

Electronic Case Filing at the Federal Courts

Notes

Chapter 14: Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies

Executive Summary

Introduction

I. Why Agencies Should Consider Legal Risks

II. Legal Issues to Consider in "Going Paperless"

III. Reducing The Legal Risks in "Going Paperless"

Conclusion

Notes

Chapter 15: Encryption

Department of Justice FAQ on Encryption Policy (April 24, 1998)

Interagency and State and Federal Law Enforcement Cooperation

Law Enforcement's Concerns Related to Encryption

Privacy in a Digital Age: Encryption and Mandatory Access

Modification of H.R. 695

Security and Freedom Through Encryption Act
OECD Guidelines for Cryptography Policy
Recommended Reading

Chapter 16: Intellectual Property
Prosecuting Intellectual Property Crimes Guidance
Deciding Whether to Prosecute an Intellectual Property Case
Government Reproduction of Copyrighted Materials
Federal Statutes Protecting Intellectual Property Rights
IP Sentencing Guidelines
Intellectual Property Policy and Programs
Copyrights, Trademarks and Trade Secrets

Section III: Forensics Tools
Chapter List

Chapter 17: Forensic and Security Assessment Tools
Detection, Protection, and Analysis
Detection and Prevention Tools for the PC Desktop
Analysis Tools
Applications
Additional Free Forensics Software Tools

Chapter 18: How to Report Internet-Related Crime
Overview
The Internet Fraud Complaint Center (IFCC)

Chapter 19: Internet Security: An Auditor's Basic Checklist
Firewalls
Supported Protocols
Anti-Virus Updates
Software Management Systems
Backup Processes and Procedures
Intra-Network Security

Section IV: Appendices
Appendix List
Appendix A: Glossary of Terms
A.C
D
E.G
H.I
K.Q
R.S
T.W

Appendix B: Recommended Reading List
Books
Articles
Web Sites

List of Exhibits

Chapter 2: How to Begin a Non.Liturgical Forensic Examination
Chapter 3: The Liturgical Forensic Examination: Tracing Activity on a Windows.Based Desktop
Chapter 4: Basics of Internet Abuse: What is Possible and Where to Look Under the Hood
Chapter 5: Tools of the Trade: Automated Tools Used to Secure a System Throughout the Stages of a Forensic Investigation
Chapter 6: Network Intrusion Management and Profiling
Chapter 8: Searching and Seizing Computers and Obtaining Electronic Evidence

List of Exhibits

Chapter 9: Computer Crime Policy and Programs
Chapter 11: Privacy Issues in the High.Tech Context
Chapter 12: Critical Infrastructure Protection
Chapter 13: Electronic Commerce: Legal Issues
Chapter 14: Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies
Chapter 18: How to Report Internet.Related Crime