



## **Digital Evidence and Computer Crime, 2nd Edition**

By Eoghan Casey

*Paperback* / February 2004 / 0121631044

[Link to Publisher](#)

[Link to Amazon](#)

## Table of Contents

### Part 1

#### Chapter 1: Digital Evidence and Computer Crime

- 1.1) Digital Evidence
- 1.2) Increasing Awareness of Digital Evidence
- 1.3) Challenging Aspects of Digital Evidence
- 1.4) Following the Cybertrail
- 1.5) Challenging Aspects of the Cybertrail
- 1.6) Forensic Science and Digital Evidence
- 1.7) Summary

#### Chapter 2: History and Terminology of Computer Crime Investigation

- 2.1) Brief History of Computer Crime Investigation
- 2.2) Evolution of Investigative Tools
- 2.3) Language of Computer Crime Investigation
  - 2.3.1) The Role of Computers in Crime
- 2.4) Summary

#### Chapter 3: Technology and Law

##### Part A: Technology and Law – A United States Perspective

Robert Dunne

- A.1) Jurisdiction
- A.2) Pornography and Obscenity
- A.3) Privacy
- A.4) Copyrights and the “Theft” of Digital Intellectual Property

##### Part B: Computer Misuse in America

Eoghan Casey

##### Part C: Technology and Criminal Law – A European perspective

Tessa Robinson

- C.1) Overview of Criminal Offenses
- C.2) Search and Seizure
- C.3) Jurisdiction and Extradition

- C.4) Penalties
- C.5) Privacy
- C.6) Summary

## Chapter 4: The Investigative Process

Eoghan Casey and Gary Palmer

- 4.1) The Role of Digital Evidence
- 4.2) Investigative Methodology
  - 4.2.1) Accusation or Incident Alert
  - 4.2.2) Assessment of Worth
  - 4.2.3) Incident/Crime Scene Protocols
  - 4.2.4) Identification or Seizure
  - 4.2.5) Preservation
  - 4.2.6) Recovery
  - 4.2.7) Harvesting
  - 4.2.8) Reduction
  - 4.2.9) Organization and Search
  - 4.2.10) Analysis
  - 4.2.11) Reporting
  - 4.2.12) Persuasion and Testimony
- 4.3) Summary

## Chapter 5: Investigative Reconstruction

Eoghan Casey and Brent Turvey

- 5.1) Equivocal Forensic Analysis
  - 5.1.1) Reconstruction
  - 5.1.2) Temporal Analysis
  - 5.1.3) Relational Analysis
  - 5.1.4) Functional Analysis
- 5.2) Victimology
  - 5.2.1) Risk Assessment
- 5.3) Crime Scene Characteristics
  - 5.3.1) Method of Approach and Control
  - 5.3.2) Offender Action, Inaction and Reaction
- 5.4) Evidence Dynamic and Introduction of Error
- 5.5) Reporting
- 5.6) Summary

## Chapter 6: Modus Operandi, Motive & Technology

Brent Turvey

- 6.1) Axes to Pathological Criminals, and Other Unintended Consequences
- 6.2) Modus Operandi
- 6.3) Technology and Modus Operandi
- 6.4) Motive and Technology
  - 6.4.1) Power Reassurance (Compensatory)
  - 6.4.2) Power Assertive (Entitlement)
  - 6.4.3) Anger Retaliatory (Anger or Displaced)
  - 6.4.4) Anger Excitation (Sadistic)
  - 6.4.5) Profit Oriented

- 6.5) Current Technologies
- 6.5.1) Computer Virus
- 6.5.2) Public Email Discussion List
- 6.6) Summary

## Chapter 7: Digital Evidence in the Courtroom

- 7.1) Admissibility – Warrants
- 7.2) Authenticity and Reliability
- 7.3) Casey's Certainty Scale
- 7.4) Best Evidence
- 7.5) Direct versus Circumstantial Evidence
- 7.6) Hearsay
- 7.6.1) Hearsay Exceptions
- 7.7) Scientific Evidence
- 7.8) Presenting Digital Evidence
- 7.9) Summary

## Part 2: Computers

## Chapter 8: Computer Basics for Digital Evidence Examiners

- 8.1) A Brief History of Computers
- 8.2) Basic Operation of Computers
- 8.2.1) Central Processing Unit (CPU)
- 8.2.2) Basic Input and Output System (BIOS)
- 8.2.3) Power-on Self Test and CMOS Configuration Tool
- 8.2.4) Disk Boot
- 8.3) Representation of Data
- 8.4) Storage Media and Data Hiding
- 8.5) File Systems and Location of Data
- 8.6) Overview of Encryption
- 8.6.1) Private Key Encryption
- 8.6.2) Public Key Encryption
- 8.6.3) Pretty Good Privacy
- 8.7) Summary

## Chapter 9: Applying Forensic Science to Computers

- 9.1) Authorization and Preparation
- 9.2) Identification
- 9.2.1) Recognizing Hardware
- 9.2.2) Identifying Digital Evidence
- 9.3) Documentation
- 9.3.1) Message Digests and Digital Signatures
- 9.4) Collection and Preservation
- 9.4.1) Collecting and Preserving Hardware
- 9.4.2) Collecting and Preserving Digital Evidence
- 9.5) Examination and Analysis
- 9.5.1) Filtering/Reduction
- 9.5.2) Class/Individual Characteristics and Evaluation of Source
- 9.5.3) Data Recovery/Salvage

- 9.6) Reconstruction
  - 9.6.1) Functional Analysis
  - 9.6.2) Relational Analysis
  - 9.6.3) Temporal Analysis
  - 9.6.4) Digital Stratigraphy
- 9.7) Reporting
- 9.8) Summary

## Chapter 10: Forensic Examination of Windows Systems

- 10.1) Windows Evidence Acquisition Boot Disk
- 10.2) File Systems
- 10.3) Overview of Digital Evidence Processing Tools
- 10.4) Data Recovery
  - 10.4.1) Windows-based Recovery Tools
  - 10.4.2) Unix-based Recovery Tools
  - 10.4.3) File Carving with Windows
  - 10.4.4) Dealing with Password Protection and Encryption
- 10.5) Log Files
- 10.6) File System Traces
- 10.7) Registry
- 10.8) Internet Traces
  - 10.8.1) Web Browsing
  - 10.8.2) Usenet Access
  - 10.8.3) E-mail
  - 10.8.4) Other Applications
  - 10.8.5) Network Storage
- 10.9) Program Analysis
- 10.10) Summary

## Chapter 11: Forensic Examination of Unix Systems

- 11.1) Unix Evidence Acquisition Boot Disk
- 11.2) File Systems
- 11.3) Overview of Digital Evidence Processing Tools
- 11.4) Data Recovery
  - 11.4.1) Unix-based Tools
  - 11.4.2) Windows-based Tools
  - 11.4.3) File Carving with Unix
  - 11.4.4) Dealing with Password Protection and Encryption
- 11.5) Log Files
- 11.6) File System
- 11.7) Internet Traces
  - 11.7.1) Web Browsing
  - 11.7.2) E-mail
  - 11.7.3) Network Traces
- 11.8) Summary

## Chapter 12: Forensic Examination of Macintosh Systems

- 12.1) File Systems
- 12.2) Overview of Digital Evidence Processing Tools

- 12.3) Data Recovery
- 12.4) File System Traces
- 12.5) Internet Traces
  - 12.5.1) Web Activity
  - 12.5.2) E-mail
  - 12.5.3) Network Storage
- 12.6) Summary

## Chapter 13: Forensic Examination of Handheld Devices

- 13.1) Overview of Handheld Devices
  - 13.1.1) Memory
  - 13.1.2) Data Storage and Manipulation
  - 13.1.3) Exploring Palm Memory
- 13.2) Collection and Examination of Handheld Devices
  - 13.2.1) Palm OS
  - 13.2.2) Windows CE Devices
  - 13.2.3) RIM Blackberry
  - 13.2.4) Mobile Phones
- 13.3) Dealing with Password Protection and Encryption
- 13.4) Related Sources of Digital Evidence
  - 13.4.1) Removable Media
  - 13.4.2) Neighborhood Data
- 13.5) Summary

## Part 3: Networks

### Chapter 14: Network Basics for Digital Evidence Examiners

- 14.1) A Brief History of Computer Networks
- 14.2) Technical overview of networks
- 14.3) Network Technologies
  - 14.3.1) Attached Resource Computer Network (ARCNET)
  - 14.3.2) Ethernet
  - 14.3.3) Fiber Distributed Data Interface (FDDI)
  - 14.3.4) Asynchronous Transfer Mode (ATM)
  - 14.3.5) IEEE 802.11 (Wireless)
  - 14.3.6) Cellular Networks
  - 14.3.7) Satellite Networks
- 14.4) Connecting Networks Using Internet Protocols
  - 14.4.1) Physical and Data-Link Layers (Layers 1 & 2)
  - 14.4.2) Network and Transport Layers (Layers 3 & 4)
  - 14.4.3) Session Layer (Layer 5)
  - 14.4.4) Presentation Layer (Layer 6)
  - 14.4.5) Application Layer (Layer 7)
  - 14.4.6) Synopsis of the OSI Reference Model
- 14.5) Summary

### Chapter 15: Applying Forensic Science to Networks

- 15.1) Preparation and Authorization
- 15.2) Identification

- 15.3) Documentation, Collection, and Preservation
- 15.4) Filtering and Data Reduction
- 15.5) Class/Individual Characteristics and Evaluation of Source
- 15.6) Evidence Recovery
- 15.7) Investigative Reconstruction
- 15.7.1) Behavioral Evidence Analysis
- 15.8) Summary

## Chapter 16: Digital Evidence on Physical and Data-Link Layers

- 16.1) Ethernet
  - 16.1.1) 10Base5
  - 16.1.2) 10/100/1000BaseT
  - 16.1.3) CSMA/CD
- 16.2) Linking the Data-Link and Network Layers—Encapsulation
  - 16.2.1) Address Resolution Protocol (ARP)
  - 16.2.2) Point to Point Protocol and Serial Line Internet Protocol
- 16.3) Ethernet versus ATM Networks
- 16.4) Documentation, Collection, and Preservation
  - 16.4.1) Sniffer Placement
  - 16.4.2) Sniffer Configuration
  - 16.4.3) Other Source of MAC Addresses
- 16.5) Analysis Tools and Techniques
  - 16.5.1) Keyword Searches
  - 16.5.2) Filtering and Classification
  - 16.5.3) Reconstruction
- 16.6) Summary

## Chapter 17: Digital Evidence on Network and Transport Layers

- 17.1) TCP/IP
  - 17.1.1) Internet Protocol and Cellular Data Networks
  - 17.1.2) IP Addresses
  - 17.1.3) Domain Name System
  - 17.1.4) IP Routing
  - 17.1.5) Servers and Ports
  - 17.1.6) Connection Management
  - 17.1.7) Abuses of TCP/IP
- 17.2) Setting up A Network
  - 17.2.1) Static versus Dynamic IP Address Assignment
  - 17.2.2) Protocols for Assigning IP Addresses
- 17.3) TCP/IP Related Digital Evidence
  - 17.3.1) Authentication Logs
  - 17.3.2) Application Logs
  - 17.3.3) Operating System Logs
  - 17.3.4) Network Device Logs
  - 17.3.5) State Tables
  - 17.3.6) Random Access Memory Contents
- 17.4) Summary

## Chapter 18: Digital Evidence on the Internet

- 18.1) Role of the Internet in Criminal Investigations
- 18.2) Internet Services: Legitimate versus Criminal Uses
  - 18.2.1) The World Wide Web
  - 18.2.2) E-mail
  - 18.2.3) Newsgroups
  - 18.2.4) Synchronous Chat Networks
  - 18.2.5) Peer-To-Peer Networks and Instant Messaging
- 18.3) Using the Internet as an Investigative Tool
  - 18.3.1) Search Engines
  - 18.3.2) Online Databases (the Invisible Web)
  - 18.3.3) Usenet Archive versus Actual Newsgroups
- 18.4) Online Anonymity and Self-Protection
  - 18.4.1) Overview of Exposure
  - 18.4.2) Proxies
  - 18.4.3) IRC "bots"
  - 18.4.5) Encryption
  - 18.4.5) Anonymous and Pseudonymous E-mail and Usenet
  - 18.4.6) Freenet
  - 18.4.7) Anonymous Cash
- 18.5) E-mail Forgery and Tracking
  - 18.5.1) Interpreting E-mail Headers
- 18.6) Usenet Forgery and Tracking
  - 18.6.1) Interpreting Usenet Headers
- 18.7) Searching and Tracking on IRC
- 18.8) Summary

#### Part 4: Investigating Computer Crime

#### Chapter 19: Investigating Computer Intrusions

- 19.1) How Computer Intruders Operate
- 19.2) Investigating Intrusions
  - 19.2.1) Processes as a Source of Evidence (Windows)
  - 19.2.2) Processes as a Source of Evidence (Unix)
  - 19.2.3) Windows Registry
  - 19.2.4) Acquisition over Network
  - 19.2.5) Classification, Comparison, and Evaluation of Source
- 19.3) Investigative Reconstruction
  - 19.3.1) Parallels between Arson and Intrusion Investigations
  - 19.3.2) Crime Scene Characteristics
  - 19.3.3) Automated and Dynamic Modus Operandi
  - 19.3.4) Examining the Intruder's Computer
- 19.4) Detailed Case Example
- 19.5) Summary

#### Chapter 20: Sex Offenders on the Internet

Eoghan Casey, Monique Mattei Ferraro, Michael McGrath

- 20.1) Window to the World
- 20.2) Legal Considerations
- 20.3) Identifying and Processing Digital Evidence

## 20.4) Investigating Online Sexual Offenders

### 20.4.1) Undercover Investigation

## 20.5) Investigative Reconstruction

### 20.5.1) Analyzing Sex Offenders

### 20.5.2) Analyzing Victim Behavior

### 20.5.3) Crime Scene Characteristics

### 20.5.4) Motivation

## 20.6) Summary

## Chapter 21: Investigating Cyberstalking

### 21.1) How Cyberstalkers Operate

#### 21.1.1) Acquiring Victims

#### 21.1.2) Anonymity and Surreptitious Monitoring

#### 21.1.3) Escalation and Violence

### 21.2) Investigating Cyberstalking

#### 21.2.1) Interviews

#### 21.2.2) Victimology

#### 21.2.3) Risk Assessment

#### 21.2.4) Search

#### 21.2.5) Crime Scene Characteristics

#### 21.2.6) Motivation

### 21.3) Cyberstalking Case Example

## 21.4) Summary

## Chapter 22: Digital Evidence as Alibi

### 22.1) Investigating an Alibi

### 22.2) Time as Alibi

### 22.3) Location as Alibi

## 22.4) Summary

## Part 4: Guidelines

## Chapter 23: Handling the Digital Crime Scene

### 23.1) Identification or Seizure

#### 23.1.1) When the Entire Computer is Required

### 23.2) Preservation

#### 23.2.1) If Only a Portion of the Digital Evidence on a Computer is Required

#### 23.2.2) Sample Preservation Form

## Chapter 24: Digital Evidence Examination Guidelines

Eoghan Casey and Troy Larson

### 24.1) Preparation

### 24.2) Processing

#### 24.2.1) DOS/Windows Command Line – Maresware

#### 24.2.2) Windows GUI – EnCase

#### 24.2.3) Windows GUI - FTK

### 24.3) Identify and Process Special Files



#### 24.4) Summary