

A PRACTICAL GUIDE TO  
**COMPUTER  
FORENSICS**  
INVESTIGATIONS



DR. DARREN R. HAYES

# **A Practical Guide to Computer Forensics Investigations**

Dr. Darren R. Hayes

**PEARSON**

800 East 96th Street, Indianapolis, Indiana 46240 USA

# Practical Guide to Computer Forensics Investigations, A

## Table of Contents

### Table of Contents

#### Introduction

#### Chapter 1: The Scope of Computer Forensics

##### Introduction

Popular Myths about Computer Forensics

##### Types of Computer Forensics Evidence Recovered

Electronic Mail (Email)

Images

Video

Websites Visited and Internet Searches

Cellphone Forensics

##### What Skills Must a Computer Forensics Investigator Possess?

Computer Science Knowledge

Legal Expertise

Communication Skills

Linguistic Abilities

Continuous Learning

An Appreciation for Confidentiality

##### The Importance of Computer Forensics

Job Opportunities

##### A History of Computer Forensics

1980s: The Advent of the Personal Computer

1990s: The Impact of the Internet

# Table of Contents

Training and Education

Law Enforcement Training

Summary

## Chapter 2: Windows Operating and File Systems

Introduction

Physical and Logical Storage

File Storage

File Conversion and Numbering Formats

Conversion of Binary to Decimal

Hexadecimal Numbering

Conversion of Hexadecimal to Decimal

Conversion of Hexadecimal to ASCII (American Standard Code for  
Information Interchange)

Unicode

Operating Systems

The Boot Process

Windows File Systems

Windows Registry

Registry Data Types

FTK Registry Viewer

Microsoft Windows Features

Windows Vista

Windows 7

Windows 8.1

Summary

## Chapter 3: Handling Computer Hardware

Introduction

Hard Disk Drives

# Table of Contents

Small Computer System Interface (SCSI)

Integrated Drive Electronics (IDE)

Serial ATA (SATA)

## Cloning a PATA or SATA Hard Disk

Cloning Devices

## Removable Memory

FireWire

USB Flash Drives

External Hard Drives

MultiMedia Cards (MMCs)

## Summary

## References

## Chapter 4: Acquiring Evidence in a Computer Forensics Lab

### Introduction

### Lab Requirements

American Society of Crime Laboratory Directors

American Society of Crime Laboratory Directors/Lab Accreditation Board (ASCLD/LAB)

ASCLD/LAB Guidelines for Forensic Laboratory Management Practices

Scientific Working Group on Digital Evidence (SWGDE)

### Private Sector Computer Forensics Laboratories

Evidence Acquisition Laboratory

Email Preparation Laboratory

Inventory Control

Web Hosting

### Computer Forensics Laboratory Requirements

Laboratory Layout

Laboratory Management

# Table of Contents

Laboratory Access

Extracting Evidence from a Device

Using the dd Utility

Using Global Regular Expressions Print (GREP)

Skimmers

Summary

## Chapter 5: Online Investigations

Introduction

Working Undercover

Generate an Identity

Generate an Email Account

Mask Your Identity

Website Evidence

Website Archives

Website Statistics

Background Searches on a Suspect

Personal Information: Mailing Address, Email Address, Telephone  
Number, and Assets

Personal Interests and Membership of User Groups

Searching for Stolen Property

Online Crime

Identity Theft

Credit Cards for Sale

Electronic Medical Records

Cyberbullying

Social Networking

Capturing Online Communications

Using Screen Captures

Using Video

# Table of Contents

Viewing Cookies

Using Windows Registry

Summary

## Chapter 6: Documenting the Investigation

Introduction

Obtaining Evidence from a Service Provider

Documenting a Crime Scene

Seizing Evidence

Crime Scene Examinations

Documenting the Evidence

Completing a Chain of Custody Form

Completing a Computer Worksheet

Completing a Hard Disk Drive Worksheet

Completing a Server Worksheet

Using Tools to Document an Investigation

CaseNotes

FragView

Helpful Mobile Applications (Apps)

Network Analyzer

System Status

The Cop App

Lock and Code

Digital Forensics Reference

Federal Rules of Civil Procedure (FRCP)

Federal Rules of Evidence (FREvidence)

Writing Reports

Time Zones and Daylight Saving Time (DST)

Creating a Comprehensive Report

Using Expert Witnesses at Trial

# Table of Contents

The Expert Witness

The Goals of the Expert Witness

Preparing an Expert Witness for Trial

Summary

## Chapter 7: Admissibility of Digital Evidence

Introduction

History and Structure of the United States Legal System

Origins of the U.S. Legal System

Overview of the U.S. Court System

In the Courtroom

Evidence Admissibility

Constitutional Law

First Amendment

First Amendment and the Internet

Fourth Amendment

Fifth Amendment

Sixth Amendment

Congressional Legislation

Rules for Evidence Admissibility

Criminal Defense

When Computer Forensics Goes Wrong

Pornography in the Classroom

Structure of the Legal System in the European Union (E.U.)

Origins of European Law

Structure of European Union Law

Structure of the Legal System in Asia

China

India

Summary

# Table of Contents

## Chapter 8: Network Forensics

Introduction

The Tools of the Trade

Networking Devices

Proxy Servers

Web Servers

DHCP Servers

SMTP Servers

DNS Servers

Routers

IDS

Firewalls

Ports

Understanding the OSI Model

The Physical Layer

The Data Link Layer

The Network Layer

The Transport Layer

The Session Layer

The Presentation Layer

The Application Layer

Advanced Persistent Threats

Cyber Kill Chain

Indicators of Compromise (IOC)

Investigating a Network Attack

Summary

## Chapter 9: Mobile Forensics

Introduction

The Cellular Network

# Table of Contents

Base Transceiver Station

Mobile Station

Cellular Network Types

SIM Card Forensics

Types of Evidence

## Handset Specifications

Memory and Processing

Battery

Other Hardware

## Mobile Operating Systems

Android OS

Windows Phone

## Standard Operating Procedures for Handling Handset Evidence

National Institute of Standards and Technology

Preparation and Containment

Wireless Capabilities

Documenting the Investigation

## Handset Forensics

Cellphone Forensic Software

Cellphone Forensics Hardware

Logical versus Physical Examination

## Manual Cellphone Examinations

Flasher Box

## Global Satellite Service Providers

Satellite Communication Services

## Legal Considerations

Carrier Records

## Other Mobile Devices

Tablets

# Table of Contents

GPS Devices

Summary

## Chapter 10: Photograph Forensics

Introduction

Understanding Digital Photography

File Systems

Digital Photography Applications and Services

Examining Picture Files

Exchangeable Image File Format (EXIF)

Evidence Admissibility

Federal Rules of Evidence (FRE)

Analog vs. Digital Photographs

Case Studies

Worldwide Manhunt

NYPD Facial Recognition Unit

Summary

## Chapter 11: Mac Forensics

Introduction

A Brief History

Macintosh

Mac Mini with OS X Server

iPod

iPhone

iPad

Apple Wi-Fi Devices

Macintosh File Systems

Forensic Examinations of a Mac

IOReg Info

# Table of Contents

PMAP Info

Epoch Time

Recovering Deleted Files

Journaling

DMG File System

PList Files

SQLite Databases

## Macintosh Operating Systems

Mac OS X

Target Disk Mode

## Apple Mobile Devices

iOS

iOS 7

iOS 8

Security and Encryption

iPod

iPhone

Enterprise Deployment of iPhone and iOS Devices

## Case Studies

Find My iPhone

Wanted Hactivist

Michael Jackson

Stolen iPhone

Drug Bust

## Summary

## Chapter 12: Case Studies

Introduction

Zacharias Moussaoui

Background

# Table of Contents

Digital Evidence

Standby Counsel Objections

Prosecution Affidavit

Exhibits

Email Evidence

## BTK (Bind Torture Kill) Killer

Profile of a Killer

Evidence

## Cyberbullying

Federal Anti-harassment Legislation

State Anti-harassment Legislation

Warning Signs of Cyberbullying

What Is Cyberbullying?

Phoebe Prince

Ryan Halligan

Megan Meier

Tyler Clementi

## Sports

## Summary

## Index

## Bonus Chapter

### Answers to Multiple-Choice and Fill in the Blanks Questions

#### Chapter 1 Answers

Multiple-Choice

Fill in the Blanks

#### Chapter 2 Answers

Multiple-Choice

Fill in the Blanks

#### Chapter 3 Answers

Multiple-Choice

# Table of Contents

Fill in the Blanks

## Chapter 4 Answers

Multiple-Choice

Fill in the Blanks

## Chapter 5 Answers

Multiple-Choice

Fill in the Blanks

## Chapter 6 Answers

Multiple-Choice

Fill in the Blanks

## Chapter 7 Answers

Multiple-Choice

Fill in the Blanks

## Chapter 8 Answers

Multiple-Choice

Fill in the Blanks

## Chapter 9 Answers

Multiple-Choice

Fill in the Blanks

## Chapter 10 Answers

Multiple-Choice

Fill in the Blanks

## Chapter 11 Answers

Multiple-Choice

Fill in the Blanks

## Chapter 12 Answers

Multiple-Choice

Fill in the Blanks