
CYBER FORENSICS

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

OTHER AUERBACH PUBLICATIONS

ABCs of IP Addressing

Gilbert Held
ISBN: 0-8493-1144-6

Application Servers for E-Business

Lisa M. Lindgren
ISBN: 0-8493-0827-5

Architectures for E-Business Systems

Sanjiv Purba, Editor
ISBN: 0-8493-1161-6

A Technical Guide to IPSec Virtual Private Networks

James S. Tiller
ISBN: 0-8493-0876-3

Building an Information Security Awareness Program

Mark B. Desman
ISBN: 0-8493-0116-5

Computer Telephony Integration

William Yarbbery, Jr.
ISBN: 0-8493-9995-5

Cyber Crime Investigator's Field Guide

Bruce Middleton
ISBN: 0-8493-1192-6

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

Albert J. Marcella and Robert S. Greenfield, Editors
ISBN: 0-8493-0955-7

Information Security Architecture

Jan Killmeyer Tudor
ISBN: 0-8493-9988-2

Information Security Management Handbook, 4th Edition, Volume 1

Harold F. Tipton and Micki Krause, Editors
ISBN: 0-8493-9829-0

Information Security Management Handbook, 4th Edition, Volume 2

Harold F. Tipton and Micki Krause, Editors
ISBN: 0-8493-0800-3

Information Security Management Handbook, 4th Edition, Volume 3

Harold F. Tipton and Micki Krause, Editors
ISBN: 0-8493-1127-6

Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management

Thomas Peltier
ISBN: 0-8493-1137-3

Information Security Risk Analysis

Thomas Peltier
ISBN: 0-8493-0880-1

Information Technology Control and Audit

Frederick Gallegos, Sandra Allen-Senft, and Daniel P. Manson
ISBN: 0-8493-9994-7

New Directions in Internet Management

Sanjiv Purba, Editor
ISBN: 0-8493-1160-8

New Directions in Project Management

Paul C. Tinnirello, Editor
ISBN: 0-8493-1190-X

A Practical Guide to Security Engineering and Information Assurance

Debra Herrmann
ISBN: 0-8493-1163-2

The Privacy Papers: Managing Technology and Consumers, Employee, and Legislative Action

Rebecca Herold
ISBN: 0-8493-1248-5

Secure Internet Practices: Best Practices for Securing Systems in the Internet and e-Business Age

Patrick McBride, Jody Patilla, Craig Robinson, Peter Thermos, and Edward P. Moser
ISBN: 0-8493-1239-6

Securing and Controlling Cisco Routers

Peter T. Davis
ISBN: 0-8493-1290-6

Securing E-Business Applications and Communications

Jonathan S. Held and John R. Bowers
ISBN: 0-8493-0963-8

Securing Windows NT/2000: From Policies to Firewalls

Michael A. Simonyi
ISBN: 0-8493-1261-2

TCP/IP Professional Reference Guide

Gilbert Held
ISBN: 0-8493-0824-0

AUERBACH PUBLICATIONS

www.auerbach-publications.com

To Order Call: 1-800-272-7737 • Fax: 1-800-374-3401

E-mail: orders@crcpress.com

CYBER FORENSICS

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

**ALBERT J. MARCELLA, Ph.D.
ROBERT S. GREENFIELD**

Editors



AUERBACH PUBLICATIONS

A CRC Press Company

Boca Raton London New York Washington, D.C.

Library of Congress Cataloging-in-Publication Data

Cyber forensics : a field manual for collecting, examining, and preserving evidence of computer crimes / Albert J. Marcella, Robert Greenfield, editors.

p. cm.

Includes bibliographical references and index.

ISBN 0-8493-0955-7 (alk. paper)

1. Computer crimes--Investigation--Handbooks, manuals, etc. I. Marcella, Albert J. II. Greenfield, Robert, 1961-

HV8079.C65 C93 2001

363.25'968--dc21

2001053817

This book contains information obtained from authentic and highly regarded sources. Reprinted material is quoted with permission, and sources are indicated. A wide variety of references are listed. Reasonable efforts have been made to publish reliable data and information, but the authors and the publisher cannot assume responsibility for the validity of all materials or for the consequences of their use.

Neither this book nor any part may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, microfilming, and recording, or by any information storage or retrieval system, without prior permission in writing from the publisher.

All rights reserved. Authorization to photocopy items for internal or personal use, or the personal or internal use of specific clients, may be granted by CRC Press LLC, provided that \$1.50 per page photocopied is paid directly to Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923 USA The fee code for users of the Transactional Reporting Service is ISBN 0-8493-0955-7/02/\$0.00+\$1.50. The fee is subject to change without notice. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

The consent of CRC Press LLC does not extend to copying for general distribution, for promotion, for creating new works, or for resale. Specific permission must be obtained in writing from CRC Press LLC for such copying.

Direct all inquiries to CRC Press LLC, 2000 N.W. Corporate Blvd., Boca Raton, Florida 33431.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation, without intent to infringe.

Visit the Auerbach Publications Web site at www.auerbach-publications.com

© 2002 by CRC Press LLC

Auerbach is an imprint of CRC Press LLC

No claim to original U.S. Government works

International Standard Book Number 0-8493-0955-7

Library of Congress Card Number 2001053817

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

Printed on acid-free paper

Editors and Contributors

Albert J. Marcella, Jr., Ph.D., CFSA, COAP, CQA, CSP, CDP, CISA, is an associate professor of Management in the School of Business and Technology, Department of Management, at Webster University, in Saint Louis, Missouri. Dr. Marcella remains the president of Business Automation Consultants, an information technology and management-consulting firm he founded in 1984. Dr. Marcella has completed diverse technical security consulting engagements involving disaster recovery planning, site and systems security, IT, financial and operational audits for an international clientele. He has contributed numerous articles to audit-related publications and has authored and co-authored 18 audit-related texts.

Robert S. Greenfield, MCP, has over 16 years of experience as a programmer/analyst, with the past five years as a systems consultant and software engineer in the consulting field. He has extensive experience designing software in the client/server environment. In addition to mainframe experience on several platforms, his background includes systems analysis, design, and development in client/server GUI and traditional environments. His client/server expertise includes Visual Basic, Access, SQL Server, Sybase, and Oracle 7.3 development. Mr. Greenfield has created intranet Web sites with FrontPage and distributing applications via the Internet. He currently holds professional accreditation as a Microsoft Certified Professional and continues self paced training to achieve MCSE, MCSD, and MCSE/D + Internet ratings.

Abigail Abraham is an Assistant State's Attorney, prosecuting high-technology crimes for the Cook County State's Attorney's Office in Chicago, Illinois. She was awarded her J.D. from The University of Chicago Law School and served as an editor on the law review. Following law school, she clerked for one year for the Honorable Danny J. Boggs, U.S. Court of Appeals for the Sixth Circuit. She is an adjunct law professor at The University of Chicago Law School. In addition, she has designed training for lawyers and for police officers, and lectures around the country on high-technology legal issues.

Brent Deterdeing graduated from the University of Missouri with a degree in computer science and a minor in economics. Brent's involvement with SANS is extensive. He is an author of an upcoming book on firewalls through SANS, as well as chairing the SANS/GIAC Firewalls Advisory Board. He has mentored both small and large classes through SANS/GIAC Security Essentials Training & Certification (GSEC). Brent also authors, revises, and edits SANS courseware, quizzes, and tests. He has earned the SANS/GIAC GSEC (Security Essentials), GCFW (Firewall Analyst — HONORS), GCIA (Intrusion Analyst), and GCIH (Incident Handling) certifications, as well as being a Red Hat Certified Engineer (RHCE). Brent participates in the St. Louis InfraGard chapter.

John W. Rado is a geospatial analyst at National Imagery and Mapping Agency (NIMA) in St. Louis, Missouri. John has worked for NIMA since January of 1991.

William J. Sampias has been involved in the auditing profession for the past decade, with primary emphasis on audits of information systems. Mr. Sampias has published several works in the areas of disaster contingency planning, end-user computing, fraud, effective communications, and security awareness. Mr. Sampias is currently director of a state agency information systems audit group.

Steven Schlarman, CISSP, is a security consultant with PricewaterhouseCoopers. Since joining the firm in 1998, Steve has covered a number of roles, mainly as the lead developer of the Enterprise Security Architecture System and Services. He has published articles on the subject as well as being one of the major thought leaders in the PricewaterhouseCoopers' Enterprise Security Architecture Service line. Prior to joining the firm, Steve had worked on multiple platforms including PC applications, networking, and midrange and mainframe systems. His background includes system security, system maintenance, and application development. Steve has completed numerous technical security consulting engagements involving security architectures, penetration studies ("hacking studies"), network and operating system diagnostic reviews, and computer crime investigation. He has participated in both PC computer forensic analysis and network intrusion management and investigation. Prior to PricewaterhouseCoopers, Steve worked at a U.S. state law enforcement agency in the information systems division.

Carol Stucki is working as a technical producer for PurchasePro.com, a rapidly growing dot.com company that is an application service provider specializing in Internet-based procurement. Carol's past experiences include working with GTE, Perot Systems, and Arthur Andersen as a programmer, system analyst, project manager, and auditor.

Dedication

Erienne, Kristina, and Andy

Michael Jordan said it best, thus, what more can I say...

I approached practices the same way I approached games. You can't turn it on and off like a faucet. I couldn't dog it during practice and then, when I needed that extra push late in the game, expect it to be there. But that's how a lot of people fail. They sound like they're committed to being the best they can be. They say all the right things, make all the proper appearances. But when it comes right down to it, they're looking for reasons instead of answers. If you're trying to achieve, there will be roadblocks. I've had them; everybody has had them. But obstacles don't have to stop you. If you run into a wall, don't turn around and give up. Figure out how to climb it, go through it, or work around it.

You are each important, special and unique for so many reasons. Always remain close, protect, respect, and love each other. Always know that I love each of you with all my heart.

Thank you Diane, for your constant support and love. My life is a far better one with you in my world. Today, tomorrow, forever...

Al

This book is dedicated to my mother and father who always believed in me, gave me love, guidance, and support in all of my pursuits. A son could not hope for better parents. Thank you both and know that your love gives me strength every day.

To my wife for her patience, and love through it all. And a special thank you goes out to my daughter Hannah, for your understanding, patience, love, wit, and unwavering support.

You are all the best and I love you.

I also would like to recognize Dr. Marcella for giving me this opportunity. Thank you.

Bob

Contents

Introductionxv

SECTION I: CYBER FORENSICS

1 The Goal of the Forensic Investigation3
Carol Stucki

2 How to Begin a Nonliturgical Forensic Investigation..... 19
Carol Stucki

**3 The Liturgical Forensic Examination:
Tracing Activity on a Windows-Based Desktop**..... 47
Robert S. Greenfield

**4 Basics of Internet Abuse: What Is Possible and Where
to Look Under the Hood**.....79
John W. Rado

**5 Tools of the Trade: Automated Tools Used to Secure a System
Throughout the Stages of a Forensic Investigation**97
Brent Deterdeing

6 Network Intrusion Management and Profiling 117
Steven Schlarman

7 Cyber Forensics and the Legal System..... 133
Abigail Abraham

SECTION II: FEDERAL AND INTERNATIONAL GUIDELINES

**8 Searching and Seizing Computers and Obtaining Electronic
Evidence**..... 149

9 Computer Crime Policy and Programs 179

10 International Aspects of Computer Crime..... 205

11	Privacy Issues in the High-Tech Context	221
	The Department of Justice Privacy Council	
12	Critical Infrastructure Protection	227
13	Electronic Commerce: Legal Issues	249
	The Electronic Commerce Working Group (ECWG), Department of Justice	
14	Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies	287
15	Encryption	335
16	Intellectual Property	361

SECTION III: FORENSICS TOOLS

17	Forensic and Security Assessment Tools	375
18	How to Report Internet-Related Crime	389
19	Internet Security: An Auditor's Basic Checklist	391

SECTION IV: APPENDICES

Appendix A	Glossary	399
Appendix B	Recommended Reading List	415
Index	425

Disclaimer

As always with texts of this nature, here is the disclaimer....

The information contained within this field manual is intended to be used as a reference, and not as an endorsement of the included providers, vendors, and informational resources. Reference herein to any specific commercial product, process, or service by trade name, trademark, service mark, manufacturer, or otherwise does not constitute or imply endorsement, recommendation, or favoring by the authors or the publisher.

As such, users of this information are advised and encouraged to confirm specific claims for product performance as necessary and appropriate.

The legal/financial materials and information that are available for reference through this manual are not intended as a substitute for legal/financial advice and representation obtained through legal/financial counsel. It is advisable to seek the advice and representation of legal/financial counsel as may be appropriate for any matters to which the legal/financial materials and information may pertain.

Web sites included in this manual are intended to provide current and accurate information; neither the authors, publisher, nor any of its employees, agencies, and officers can warranty the information contained on the sites and shall not be held liable for any losses caused on the reliance of information provided. Relying on information contained on these sites is done at one's own risk. Use of such information is voluntary, and reliance on it should only be undertaken after an independent review of its accuracy, completeness, efficacy, and timeliness.

Throughout this manual, reference links to other Internet addresses have been included. Such external Internet addresses contain information created, published, maintained, or otherwise posted by institutions or organizations independent of the authors and the publisher. The authors and the publisher do not endorse, approve, certify, or control these external Internet addresses and do not guarantee the accuracy, completeness, efficacy, timeliness, or correct sequencing of information located at such addresses. Use of such information is voluntary, and reliance on it should only be undertaken after an independent review of its accuracy, completeness, efficacy, and timeliness.

Acknowledgments

As senior editor for this text, the responsibility to acknowledge and thank all the individuals who have contributed their expertise, time, energies, and efforts to the successful development of this text falls to me. This is no easy task. It is difficult to put into words the appreciation and gratitude I have for each of their efforts and to express appropriately to each of them my sincere thanks for giving their time and themselves to make this text a better product. Simply mentioning each by name here seems a bit inadequate in comparison to their individual and collective contributions.

Given the continual shifting technological landscape in which we all live and work, attempting to harness even for a moment in time, this very technology, and to “look under the hood” so-to-speak, was a daunting assignment. Those professionals whose insights and comments on the critically important field of cyber forensics are included in this text, and deserve substantial credit and our thanks for taking up this challenge and for their spot-on examination and evaluation of key cyber forensics issues.

I wish to formally recognize each contributing author here, although briefly, and have included a more extensive personal profile for each author. To each of you, please know that you have my heartfelt gratitude and personal thanks for your willingness to contribute your talents and expertise to this text.

Thank You:

To my co-editor Bob Greenfield; thank you for contributing your talents in the technical systems arena and for your piece on “The Liturgical Forensic Examination: Tracing Activity on a Windows-Based Desktop.”

Thanks to Steve Schlarman, security consultant at PricewaterhouseCoopers, who wrote the chapter on “Network Intrusion Management and Profiling,” and to Brent Deterdeing, network security manager, enabling technologies at Solutia, Inc., for insights and comments on “Tools of the Trade: Automated Tools Used to Secure a System Throughout the Stages of a Forensic Investigation.”

John Rado, geospatial analyst at National Imagery and Mapping Agency; thank you for sharing your thoughts (and your extensive security/forensics background and library with me), and for developing the focused piece on “Basics of Internet Abuse: What is Possible and Where to Look Under the Hood.”

From the Financial and Computer Crime Department of the State Attorney’s office of Cook County, Illinois, Attorney Abigail Abraham; thank you for your engaging examination into “Cyber Forensics and the Legal System.”

To my long-time colleagues and collaborators Carol Stucki, for your presentations on the “The Goal of the Forensic Investigation” and “How to Begin a Nonliturgical Forensic Examination;” and Bill Sampias for your efforts in developing the areas of guidelines and tools, including the list of critical recommended readings.

Additionally, I would like to thank Carol for all the work she did in compiling the exhaustive reference materials from the Federal Bureau of Investigation, computer examinations library, which appeared in successive issues of the Bureau’s *Handbook of Forensic Services*.

Without the contributions of these talented professionals, this text would have been a lesser product.

Last, but by far certainly not the least, I want to acknowledge and thank Christian Kirkpatrick, Acquisitions Editor at Auerbach Publications, for her constant confidence that this text would emerge from a simple concept into a viable product.

Christian, thank you for your steadfast support throughout the lengthy development process that has led to the creation of this viable cyber forensics field manual.

Introduction

As an auditor as well as researcher and author, I realize and value the importance of timely, well-focused, accurate information. It is with this philosophy in mind that the development of this project was undertaken.

To the reader, a note of explanation.... This is not a text, but rather a field manual. It has been written — better yet, compiled — and edited in a manner that will allow you to rapidly access a specific area of interest or concern and not be forced to sequentially wade through an entire text, chapter by chapter, to get to what is important to you.

In the true sense of a field manual, each “chapter” (and we use that term loosely) stands on its own and presents focused, timely information on a specific topic related to cyber forensics. The author of each “chapter” was selected for his or her expertise in a specific area within the very broad field of cyber forensics.

Often a limiting aspect of most projects, especially those written on emerging technical topics, is the inability to cover every aspect of the topic in a single all-inclusive text. This truth befalls this field manual that you are about to use.

Initial research into this growing discipline proved that it would be next to impossible to include all the areas of both interest and importance in the field of cyber forensics that would be needed and required by all potential readers and users in a single text. Thus, this field manual presents specific and selected topics in the discipline of cyber forensics, and addresses critical issues facing the reader who is engaged in or who soon will be (and you will!) engaged in the preservation, identification, extraction, and documentation of computer evidence.

As a user of this field manual, you will see that this manual’s strength lies with the inclusion of an exhaustive set of chapters covering a broad variety of forensic subjects. Each chapter was thoroughly investigated; examined for accuracy, completeness, and appropriateness to the study of cyber forensics; reviewed by peers; and then compiled in a comprehensive, concise format to present critical topics of interest to professionals working in the growing field of cyber forensics.

We finally had to select several key areas and put pen to paper, entice several colleagues to share their ideas, and resign ourselves to the fact that we cannot say all that needs to be said in one text, book, or manual. We trust the material

we have included will serve as a starting point for the many professionals who are beginning their journey into this exciting discipline.

We begin our journey into the realm of this relatively new discipline by opening with a brief discussion as to the current state of the environment relating to the need for this new field of forensics and then a brief examination of the origins of cyber forensics. Along the way, we will establish several basic definitions designed to assist the reader in moving easily through what could be difficult and confusing terrain.

Although e-mail is becoming more mission-critical for enterprises, it also has the ability to haunt a company in times of trouble, because records of e-mail messages remain in the company systems after deletion — a feature highlighted during the Microsoft anti-trust trial. The case has featured critical testimony derived from old Microsoft e-mail messages.

— *InfoWorld*, 10/25/99

Background

The ubiquitous use of computers and other electronic devices is creating a rapidly rising wave of new and stored digital information. The massive proliferation of data creates ever-expanding digital information risks for organizations and individuals. Electronic information is easy to create, inexpensive to store, and virtually effortless to replicate. As a result, increasingly vast quantities of digital information reside on mass storage devices located within and without corporate information systems. Information risks associated with this data are many. For example, electronic data can often show — with a high degree of reliability — who said, knew, took, shared, had and did what, and who else might be involved in the saying, knowing, taking, sharing, having, and doing. For the corporation, the free flow of digital information means that the backdoor is potentially always open to loss.

To put the explosive growth of electronic data in perspective, consider that Americans were expected to send and receive approximately 6.8 trillion e-mail messages in 2000 — or about 2.2 billion messages per day.¹ Although some of this e-mail is sent and received by individuals, most of it is being created by and sent from corporate mail servers.

In 2000, the World Wide Web consisted of 21 terabytes of static HTML pages and is growing at a rate of 100 percent per year.¹ There are now about 2.5 billion indexed Web pages, increasing at the rate of 7.3 million pages per day.

Demand for digital storage is expected to grow by more than 1800 percent between 1998 and 2003. A midrange estimate of the amount of data currently stored on magnetic tape is 2.5 exabytes (an exabyte is 1 million terabytes), with another 2.5 exabytes stored on computer hard drives.¹

Contrasting the growth of paper pages and electronic documents adds additional perspective. The growth of recorded information doubles every three to four years. Over 93 percent of all information produced in 1999 was in digital format. About 80 percent of corporate information currently exists in digital form.

Companies are expected to generate some 17.5 trillion electronic documents by 2005, up from approximately 135 billion in 1995.² Some 550 billion documents now exist online.

There is more to this explosive growth than just “documents.” Additional forms of electronic data originate from:

- Internet-based electronic commerce, online banking, and stock trading
- Corporate use and storage of phone mail messages and electronic logs
- Personal organizers, such as the Palm Pilot (worldwide PDA sales were expected to total about 6 million units in 2000 rising to 17 million in 2004.)
- Wireless devices such as cell phones and pagers with contacts and task list storage (worldwide mobile phone sales were expected to total about 400 million in 2000, rising to 560 million in 2004¹)
- Digital cameras
- Corporate use and storage of graphic images, audio, and video

These are several of the factors now at work in corporations that increase the risk of litigation and loss of confidential corporate data (from www.fios-inc.com/digital_risk.html, Fios, Inc. (877) 700-3467, 921 S.W. Washington Street, Suite 850, Portland, Oregon 97205)

It is best to state up-front that the emphasis in any cyber forensic examination must be on the forensic element, and it is vital to understand that forensic computing, cyber forensics, or computer forensics is not solely about computers. It is about rules of evidence, legal processes, the integrity and continuity of evidence, the clear and concise reporting of factual information to a court of law, and the provision of expert opinion concerning the provenance of that evidence:

Companies are very concerned about the notion that anything they write electronically can be used again at any time. If you have to discipline yourself to think, “can this be misconstrued?” that greatly hampers your ability to communicate and introduces a huge level of inefficiency.

— *David Ferris, president of Ferris Research (San Francisco)*

Dimensions of the Problem

Crime: an act committed in violation of the law.

Much of today’s computer-related crime is not a violation of formal law. In 1979, the Justice Department defined computer crime as any illegal act for which knowledge of computer technology is essential for its perpetration, investigation, or prosecution.

Criminal law is a crime, which is a wrong against society, typically leading to a conviction, which normally results in jail term or probation. The main purpose is punishment of the offender. Most computer crimes in United States today go unpunished (which weakens deterrence of law).

Evidence must be gathered by law enforcement in accordance with court guidelines governing search and seizure (Fourth Amendment):

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but on probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Computer crime is escalating!

The FBI's caseload is increasing dramatically. In FY 1998, the FBI opened 547 computer intrusion cases; in FY 1999, that jumped to 1154. At the same time, because of opening the National Infrastructure Protection Center (NIPC) in February 1998 and the FBI's improving ability to fight cyber crime, the Bureau closed more cases. In FY 1998, the closed case file increased to 399 intrusion cases; and in FY 1999 it increased to 912 such cases.

However, given the exponential increase in the number of cases opened, cited above, the FBI's actual number of pending cases has increased by 39 percent, from 601 at the end of FY 1998 to 834 at the end of FY 1999. In short, although the FBI has markedly improved its capabilities to fight cyber intrusions, the problem is growing even faster.

The Computer Security Institute released its fifth annual "Computer Crime and Security Survey" for 2001, confirming the alarming facts cited above. Eighty-five percent of respondents detected security breaches over the past 12 months.

At least 64 percent of respondents reported financial losses, including theft of proprietary information, financial fraud, system penetration by outsiders, data or network sabotage, and denial-of-service attacks. Information theft and financial fraud caused the most severe financial losses, put at \$151 million and \$93 million, respectively. The losses from 186 respondents totaled just over \$377 million.

Losses traced to denial-of-service attacks were only \$77,000 in 1998, and by 1999 had risen to just \$116,250. Further, the new survey reports on numbers taken before the high-profile February 2000 attacks against Yahoo!, Amazon, and eBay. Finally, many companies are experiencing multiple attacks; 19 percent of respondents reported ten or more incidents.

Attorney Deanne Siemer says she tells judges that digital technology "takes one-third out of the trial time." And that's a huge factor for courts with their enormous backlogs.

— *Rebecca Ganzel*,
"Digital Technology in the Courtroom,"
Presentations, November 1999

Computer Forensics

Computer Forensics deals with the preservation, identification, extraction, and documentation of computer evidence. The field is relatively new to the private

sector but it has been the mainstay of technology-related investigations and intelligence gathering in law enforcement and military agencies since the mid-1980s.

Like any other forensic science, computer forensics involves the use of sophisticated technology tools and procedures that must be followed to guarantee the accuracy of the preservation of evidence and the accuracy of results concerning computer evidence processing.

What evidence is needed?

- All physical evidence (computer, peripherals, notepads, documentation, etc.)
- Visual output on the monitor
- Printed evidence on a printer
- Printed evidence on a plotter
- Film recorder (magnetic representations)

It is extremely important to realize that evidence must have been gathered in accordance with the Fourth Amendment and the Electronic Communications Privacy Act (ECPA), and that computer-generated evidence is considered “hearsay” with some exclusions. Depending on your role or responsibility in the computer forensics investigation, you may be subject to differing sets of rules and regulations. Internal investigators, for example, are not subject to the Fourth Amendment stipulations; however, they are subject to the ECPA.

Typically, computer forensic tools exist in the form of computer software. Computer forensic specialists guarantee accuracy of evidence processing results through the use of time-tested evidence processing procedures and through the use of multiple software tools, developed by separate and independent developers. The use of different tools that have been developed independently to validate results is important to avoid inaccuracies introduced by potential software design flaws and software bugs.

The introduction of the personal computer in 1981 and the resulting popularity came with a mixed blessing. Society in general benefited, but so did criminals using personal computers in the commission of crimes. Today, personal computers are used in every facet of society to create and share messages, compute financial results, transfer funds, purchase stocks, make airline reservations, and access bank accounts and a wealth of worldwide information on essentially any topic.

Computer forensics is used to identify evidence when personal computers are used in the commission of crimes or in the abuse of company policies. Computer forensic tools and procedures are also used to identify computer security weaknesses and the leakage of sensitive computer data. In the past, documentary evidence was typically stored on paper and copies were made with carbon paper or photocopy machines.

Most documents are now stored on computer hard disk drives, floppy diskettes, Zip disks, and other forms of removable computer storage media. Computer forensics deals with finding, extracting, and documenting this form of “electronic” documentary evidence (www.forensics-intl.com/def4.html).

Along the way, prior to formally pursuing a cyber forensics investigation, several important and critical questions must be asked:

- What is the policy in the organization to report and deal with computer crime? (It may be nonexistent, or it may be not well thought out or tested, or it may even be incompetent.)
- Do you “really” want to prosecute?
- Who do you call in law enforcement and what will be their reaction?

Additional questions that should be considered and appropriate answers well thought out include:

- Can you afford to be without the evidence?
- Are you willing to see this go public?
- Was a thorough investigation conducted?
- Did you violate the ECPA or any privacy issues?
- How will you prove the crime?
- Is there any likelihood of the suspect doing damage prior to arrest? (Dr. Rayford Vaughn, vaughn@cs.msstate.edu)

Obtaining concrete answers to these questions prior to embarking on a cyber forensics audit or investigation is critical. Doing so may help shield the organization (as well as the investigator/auditor/security personnel, etc.) from civil or criminal liabilities.

The material presented in the following pages of this field manual has been selected, developed, and shared with the specific objective of providing the reader with a resource with which to become better prepared to undertake and participate in the cyber forensics audit of a suspect system.

Works Cited

1. University of California at Berkeley, School of Information Management and Systems, October 2000, <http://www.sims.berkeley.edu/how-much-info/>.
2. *Designing a Document Strategy: Documents...Technology...People*. Craine, K., MC2 Books, 2000.