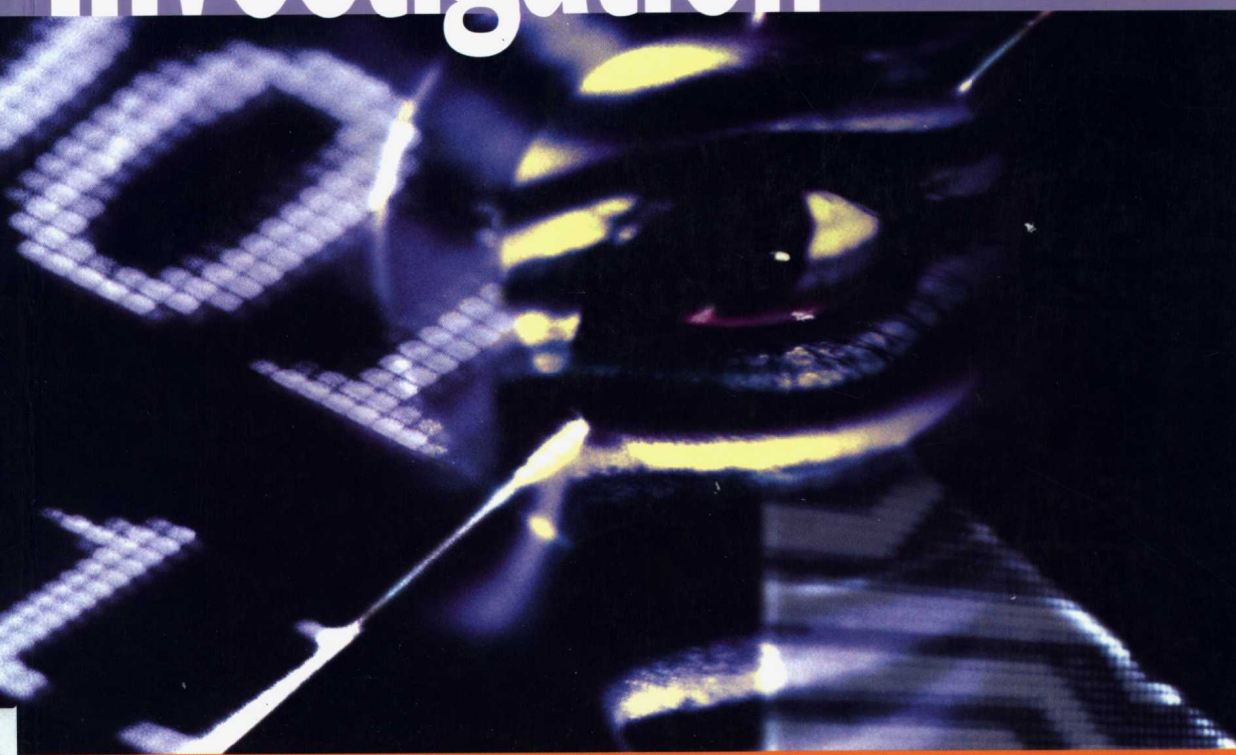
HANDBOOK OF Computer Crime Investigation



Forensic Tools and Technology

Edited by **Eoghan Casey**

HANDBOOK OF COMPUTER CRIME INVESTIGATION

FORENSIC TOOLS AND TECHNOLOGY

Edited by Eoghan Casey

ACADEMIC PRESS

A Division of Harcourt, Inc.

San Diego San Francisco New York Boston

London Sydney Tokyo

This book is printed on acid-free paper.

ACADEMIC PRESS
A division of Harcourt, Inc.
Harcourt Place, 32 Jamestown Road, London NW1 7BY, UK
http://www.academicpress.com

ACADEMIC PRESS
A division of Harcourt, Inc.
525 B Street, Suite 1900, San Diego, California 92101-4495, USA
http://www.academicpress.com

ISBN 0-12-163103-6

Library of Congress Catalog Number:
2001095720

A catalogue record for this book is available from the British Library

Typeset by M Rules
Printed and bound in Great Britain by Bath Press, Bath

02 03 04 05 06 07 **BP** 9 8 7 6 5 4 3 2 1

ABOUT THE AUTHORS

Curt Bryson spent 11 years in the U. S. Air Force. He was originally responsible for the security of some of the Air Force's most highly guarded Top Secret information while assigned in Berlin. Curt was later selected as a Special Agent in the U. S. Air Force Office of Special Investigations. He is experienced in a wide variety of investigations including high-tech and telecommunications crime, procurement fraud, homicide, child pornography, espionage, terrorism, hate crimes, and counter-intelligence. Curt is federally certified by the Department of Defense in computer forensics and has extensive knowledge of computer networks, computer security, Internet topography and architecture. He is also the lead instructor for NTI's Internet Investigations Course and articles written by him have been published in ISSA's publication, PASSWORD; as well as ISACA's Information Management magazine. He has also conducted training courses at the national conventions of ISACA, ACFE and ASIS. His instruction at California State University in Sacramento led to Curt being named as a preferred member of the Criminal Justice Scholastic Speaker's Bureau.

Eoghan Casey earned his Master of Arts in Educational Communication and Technology at NYU's School of Education. He received his Bachelor of Science in Mechanical Engineering from the University of California, Berkeley. Working on a research satellite project for four years, along with subsequent computer programming and network administration positions, developed his understanding of satellite operations, computer automation, and communication networks and their misuses. Eoghan is currently a System Security Administrator for Yale University, where he investigates computer intrusions, cyberstalking reports, and other computer-related crimes, and assists in the research and implementation of university wide security solutions. He is author of *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* and *Cyberpatterns: Criminal Behavior on the Internet in*

Criminal Profiling: An Introduction to Behavioral Evidence Analysis and is a full partner and instructor with Knowledge Solutions LLC.

David F. Clark received his B.S. engineering degree with electrical option in 1987 from LeTourneau University in Texas. Subsequently he spent three and a half years in the Middle East working in RF engineering. He then moved to Finland where he spent six and a half years in various positions in the wireless technology industry involving quality, manufacturing, marketing, and engineering. He is currently working in the area of wireless network technology testing. He resides with his wife in the Dallas area and can be reached at mr@clarkcorner.com

Karen Frederick is a senior security engineer for the Rapid Response Team at NFR Security. She holds a bachelor's degree in Computer Science from the University of Wisconsin-Parkside, and she is currently completing her master's degree in Computer Science, focusing in network security, through the University of Idaho's Engineering Outreach program. Karen has over 10 years of experience in technical support, system administration and information security. She holds several certifications, including Microsoft Certified Systems Engineer + Internet, Check Point Certified Security Administrator, SANS GIAC Certified Intrusion Analyst, GIAC Certified Unix Security Administrator, and GIAC Certified Incident Handler. Karen is one of the authors and editors of *Intrusion Signatures and Analysis* and regularly writes articles on intrusion detection for SecurityFocus.com

K. Edward Gibbs has over 12 years in the computing industry and has spent the last six years focused on internetworking and Internet security - mainly firewalls and VPN, although he has recently been involved in various aspects of wireless technologies. Previously, he spent most of his time developing real-time, mission-critical software for various Fortune 500 companies. He currently lives in California with his wife and three children. He can be contacted at e_gibbs@hotmail.com

Troy Larson is a forensic computing and electronic evidence consultant based out of Seattle, Washington. Troy focuses primarily on electronic evidence and legal support matters, as well as research and development of advanced forensic computing and investigative techniques and training. He specializes in assisting attorneys handle electronic evidence throughout all facets of litigation, including discovery and expert testimony. He is a frequent speaker to attorney information systems, and information security groups on issues related to electronic evidence and forensic computing. Mr. Larson is an active member of the Washington State

Bar. He received his undergraduate and law degrees from the University of California at Berkeley. He can be contacted at ntevidence@home.com

H. Morrow Long is the Director of the Information Security Office at Yale University. He holds a B.S. in Communications from the Boston University School of Communication (1981) and a M.S. C.I.S. (Computing and Information Systems) from the University of New Haven (1986). Morrow is a UNIX, NT and TCP/IP security expert, an author, consultant and educator with more than 17 years of experience with the IP (Internet Protocol) networking protocols and over 10 years of experience designing Internet/Intranet firewalls and information security solutions. Morrow has written and released several software programs into the public domain. Prior to working at Yale University Mr. Long was a Member Technical Staff at the ITT Advanced Technology Labs in Stratford and Shelton (1984–6) and a Lead Programmer Analyst developing INVESTWARE(TM) at New England Management Systems (NEMS 1982–84).

Mark E. Luque is a computer forensics practitioner for the DoD Computer Forensics Laboratory. He spent the past four years performing computer forensics analysis and studying the process of Unix analysis. He developed a comprehensive intrusion analysis program focusing on post-mortem analysis of victim and subject file systems and performed dozens of media analysis studies supporting defense and federal investigations. Mark is a Master Sergeant for the United States Air Force and a Computer Information Science undergraduate with the University of Maryland.

John McLean holds a Bachelor and Master of Science in Criminal Justice from Northeastern University. He has an exceptional background in Law Enforcement with specialization in the areas of Computer Crime Investigation, Computer Forensics, Computer Child Exploitation and Computer Security. His past assignments include the U.S. Marine Corps, U.S. Secret Service, U.S. Attorney's Office, and Massachusetts Attorney General's Office. Sergeant McLean is currently with the Medford Police Department in Massachusetts where he is Supervisor of Investigation for the Computer Crime and Forensic Investigation Unit. John has investigated hundreds of diverse, technically challenging computer crime cases and has assisted numerous Federal, State & Local Police Agencies with computer crime investigations. He is also an instructor for the Department of Justice, Massachusetts Criminal Justice Training Council, Northeastern University, and other private and public organizations.

Sigurd E. Murphy, a government contractor from Veridian Information Solutions, is currently a Computer Forensic Examiner with the U.S. Department of Defense Computer Forensic Laboratory (DCFL). He focuses on computer intrusions and investigations in the Windows NT environment. Sig received his Bachelor of Arts in Psychology with a minor in Computer Science from Georgetown University. Previous to his employment at the DCFL, he worked as a Senior Technology Consultant, and later as Manager of Lab and Network security for Georgetown University.

John Patzakis joined Guidance Software as general counsel in January 2000 from the law firm of Corey & Patzakis, of which he was a founder. A senior partner practicing primarily in the areas of insurance and business litigation, his focus shifted in 1998 to issues relating to the discovery and admissibility of electronic evidence. Guidance Software presented an excellent opportunity for John to combine his legal talents with his knowledge of technology at the leading computer forensics software company. Upon receiving his juris doctorate from Santa Clara University School of Law, John was admitted to the California State Bar in December 1992. Prior to receiving his law degree, John received a bachelor of arts in political science from the University of Southern California in 1989. He began his legal career at the Los Angeles, California civil litigation firm of Cotkin & Collins, where he served as an associate in the firm's business litigation department.

Steve Romig is in charge of the Ohio State University Incident Response Team, which provides incident response assistance, training, consulting, and security auditing service for The Ohio State University community. He is also working with a group of people from Central Ohio businesses to improve Internet security response and practices in the Ohio area. Steve received his Bachelor's degree in Math (Computer Science Track) from Carnegie Mellon University in 1983. In years past Steve has worked as lead UNIX system administrator at one site with 40,000 users and 12 hosts and another site with 3000 users and over 500 hosts. Most recently Steve has been working on tools to make it easier to investigate network-related evidence of computer security incidents, such as the Review package for viewing the contents of tcpdump logs, and the flow-tools package from Mark Fullmer for looking at Cisco net flow logs. He can be reached at romig@acm.org

Keith Seglem, a government contractor from Veridian Information Solutions, has been a Senior Computer Forensic Examiner with the U.S. Department of Defense Computer Forensic Laboratory since its inception over 3 years ago. He focuses on Unix and computer intrusion investigation

and analysis. Keith began programming during high school in 1975 and went on to major in Computer Science with a minor in Psychology at New Mexico Tech. He worked as an engineers assistant at the National Radio Astronomy Observatory, VLA, in New Mexico, and later as a programmer at what is now the Energetic Materials Research and Testing Center in Socorro. After a serious case of burnout, he joined the U.S. Air Force. He began his Air Force career in Electronic Warfare, progressed into digital signal intelligence, and retired as a Computer Security Officer. While on active duty, he completed AAS and BSED degrees. Since retiring he has been involved with and received commendations from various law enforcement organizations including the FBI, DEA, AFOSI and DCIS.

Bob Sheldon is vice president of Guidance Software, holds a bachelor's degree in economics, is certified in applications programming, and has completed coursework in network and Internet operations. Having served in law enforcement for 20 years, Bob's last assignment prior to joining the company was as supervisor for the computer forensics team of the California Department of Insurance, Fraud Division. He has been conducting computer-based investigations on seized computers since 1988 and has received more than 350 hours of formal training. Bob is certified to instruct on both the specialties of computer and economic crime and seizure and the examination of microcomputers at the California Commission on Peace Officer Standards and Training Institute for Criminal Investigation. He has testified regarding computer evidence in cases involving fraud, narcotics and homicide.

Todd G. Shipley is a Detective Sergeant with the Reno, Nevada Police Department. He has over 22 years experience as a police officer with 16 of those years conducting and managing criminal investigations. He currently supervises his department's Financial Crimes and Computer Crimes Units. For the past ten years he has been actively involved in developing law enforcement response to technology crime. He speaks and teaches regularly on technology crime investigations. He holds certification in Computer Forensics as a Certified Forensic Computer Examiner from the International Association of Computer Investigative Specialists and is a Certified Fraud Examiner. He can be reached at renocybercop@yahoo.com

Scott Stevens graduated with a Bachelor of Science Degree in Business Administration from Fort Lewis College in Durango, Colorado. Scott has been with NTI since 1998 and is currently Vice President of Marketing. While at NTI he has dealt extensively with hundreds of law enforcement and military computer forensics specialists. He has completed NTI's forensic

training program and has lectured concerning automated computer forensic processes and software tools at the Los Alamos National Laboratory in New Mexico and for numerous professional organizations.

Ronald van der Knijff received his BSc degree in electrical engineering in 1991 from the Rijswijk Institute of Technology. After performing military service as a Signal Officer he obtained his MSc degree in Information Technology in 1996 from the Eindhoven University of Technology. Since then he has worked at the Digital Technology department of the Netherlands Forensic Institute as a scientific investigator and is currently responsible for the embedded systems group. He also lectures on 'Smart Cards and Biometrics' at the EUFORCE Masters Program 'Information Technology' at the Technical University of Eindhoven, and on 'Cards & IT' at the 'Dutch Police Academy'.

ACKNOWLEDGEMENTS

Eoghan Casey – My highest commendation and appreciation goes to the authors for their commitment to creating this book and their tolerance of the demands it placed on them. I would also like to thank Nick Fallon for making this book possible and Linda Beattie, Roopa Baliga, and the others at Academic Press for their efforts. Thanks to my family and friends for their steady support, particularly my mother Ita O'Connor for her guidance and wisdom. And to my wife Genevieve, thank you for everything, again.

Karen Frederick – I am grateful for all of the teaching, guidance and assistance that I've received from my colleagues at NFR Security. Special thanks go to Marcus Ranum, Tim Collins, Dodge Mumford, and Bill Bauer.

Edward Gibbs & David F. Clark – Special thanks to Lt. Ron Ramlan of the San Francisco Police Department, CSI, Computer Analysis Unit for his input and review of content in Chapter 10. Special thanks also to Lorin Rowe of AT&T Wireless Services for his insight and help with this interesting subject. Additionally, special thanks to Steve Coman for reviewing Chapter 10.

Troy Larson – I would like to express my sincere appreciation for the assistance, creativity, leadership and expertise of my coworkers, particularly David Morrow, Greg Dominguez and James Holley. The past several years that I have had the pleasure of working with David, Greg and James have been the most rewarding professional experience I could have had. They also gave my efforts in this book considerable attention and they must share credit for whatever value the reader might find in my contributions. I would also like to thank Dan Mares and Gordon Mitchell for their editorial assistance. Their comments and suggestions have helped make my portions of this book much clearer and more informative than they might otherwise have been. I must also thank Ron Peters, who helped me make forensic computing my

profession. Finally, I must thank my wife for her unfailing encouragement and my daughters for their patience.

John McLean – Special thanks to the Massachusetts State Police – CPAC unit – Middlesex, Cambridge PD, and the Middlesex District Attorney's Office.

John Patzakis – Thank you to my beautiful wife Andrea, whom with I have spent far too little time in recent months.

Bob Sheldon – I would like to thank John Colbert for his research and development and editorial assistance, and the Guidance Software training support staff, including Tracy Simmons, for all their hard work.

Todd Shipley – Thank you to my wife who put up with the laptop and to my daughter who is too young to know I wasn't playing with her as much as I should have been.

Ronald van der Knijff would like to thank the people within the Dutch government supporting forensic embedded system analysis, and all the people from law-enforcement organizations willing to share information. Thanks also to my colleagues for reviewing the embedded systems analysis chapter.

CONTENTS

CASE EXAMPLES

CHAPTER 1

INTRODUCTION

Eoghan Casey and Keith Seglem

In June 2000, when the home of alleged serial killer John Robinson was searched, five computers were collected as evidence. Robinson used the Internet to find victims and persuade them into meeting him, at which time he allegedly sexually assaulted some and killed others (McClintock 2001). More recently, several hard drives were seized from the home of FBI spy Robert Hanssen. In addition to searching private government computer systems to ensure that he was not under investigation, Hanssen hid and encrypted data on floppy disks that he allegedly passed to the KGB, and used handheld devices to communicate securely with his collaborators as detailed in the following communication that he sent to them.

> *As you implied and I have said, we do need a better form of secure communication – faster. In this vein, I propose (without being attached to it) the following: One of the commercial products currently available is the Palm VII organizer. I have a Palm III, which is actually a fairly capable computer. The VII version comes with wireless internet capability built in. It can allow the rapid transmission of encrypted messages, which if used on an infrequent basis, could be quite effective in preventing confusions if the existance [sic] of the accounts could be appropriately hidden as well as the existance [sic] of the devices themselves. Such a device might even serve for rapid transmittal of substantial material in digital form.* (US vs Hanssen)

As more criminals utilize technology to achieve their goals and avoid apprehension, there is a developing need for individuals who can analyze and utilize evidence stored on and transmitted using computers. This book grew out of the authors' shared desire to create a resource for forensic examiners[1] who deal regularly with crimes involving networked computers,

1 For the purposes of this text, the term 'forensic examiner' is used to refer to any individual who is responsible for examining digital evidence in the context of a legal dispute.

wireless devices, and embedded systems. This work brings together the specialized technical knowledge and investigative experience of many experts, and creates a unique guide for forensic scientists, attorneys, law enforcement, and computer professionals who are confronted with digital evidence of any kind.

To provide examiners with an understanding of the relevant technology, tools, and analysis techniques, three primary themes are treated: *Tools*, *Technology*, and *Case Examples*. Chapter 2 (The Other Side of Civil Discovery) unites all three themes, detailing tools and techniques that forensic examiners can use to address the challenges of digital discovery. The *Tools* section presents a variety of tools along with case examples that demonstrate their usefulness. Additionally, each chapter in this section contains valuable insights into specific aspects of investigating computer-related crime.

The *Technology* section forms the heart of the book, providing in-depth technical descriptions of digital evidence analysis in commonly encountered situations, starting with computers, moving on to networks, and culminating with embedded systems. This section demonstrates how forensic science is applied in different technological contexts, providing forensic examiners with technical information and guidance that is useful at the crime scene. Demonstrative case examples are provided throughout this section to convey complex concepts.

In the final *Case Examples* section, experienced investigators and examiners present cases to give readers a sense of the technical, legal, and practical challenges that arise in investigations involving computers and networks.

There are several dichotomies that examiners must be cognizant of before venturing into the advanced aspects of forensic examination of computer systems. These fundamental issues are introduced here.

LIVE VERSUS DEAD SYSTEMS

> *It is accepted that the action of switching off the computer may mean that a small amount of evidence may be unrecoverable if it has not been saved to the memory but the integrity of the evidence already present will be retained.* (ACPO 1999)

Individuals are regularly encouraged to turn a computer off immediately to prevent deletion of evidence. However, the unceremonious cutting of a computer's power supply incurs a number of serious risks. Turning off a computer causes information to be cleared from its memory; processes that were running, network connections, mounted file systems are all lost. This loss of evidence may not be significant when dealing with personal computers – some information may even be retained on disk in RAM slack (NTI 2000) or

virtual memory in the form of swap and page files.[2] However, shutting down a system before collecting volatile data can result in major evidence loss when dealing with systems that have several gigabytes of random access memory or have active network connections that are of critical importance to an investigation. Additionally, an abrupt shutdown may corrupt important data or damage hardware, preventing the system from rebooting. Shutting down a system can also mean shutting down a company, causing significant disruption and financial loss for which the investigator may be held liable. Finally, there is the physical risk that the computer could be rigged to explode if the power switch is toggled.[3] Therefore, attention must be given to this crucial stage of the collection process.

In many cases, it may not be desirable or necessary to shut a system down as the first step. For example, volatile data may need to be collected before a suspect system is shut down. Some disk editing programs (e.g. Norton Diskedit) can capture the entire contents of RAM, and various tools are available for collecting portions of memory. For instance, `fport` (www.foundstone.com), `handleex` (www.sysinternals.com), `ps` and `pulist` from the Windows 2000 resource kit all provide information about the processes that are running on a system. Also, tools such as `carbonite`(www.foundstone.com) have been developed to counteract loadable kernel modules on Linux. Additionally, applications such as The Coroner's Toolkit (TCT) are being developed to formalize and automate the collection of volatile information from live computer systems.[4]

Once volatile information has been collected, it is generally safe to unplug the power cord from the back of the computer. Except in the context of networks and embedded systems, this book presumes that examiners are dealing with dead systems that have been delivered to them for examination.

LOGICAL VERSUS PHYSICAL ANALYSIS

From an examination standpoint, the distinction between the physical media that holds binary data and the logical representation of that information is extremely important. In certain instances, forensic examiners will want to

2 Virtual memory enables more processes to run than can fit within a computer's physical memory. This is achieved by either swapping or paging data from disk into and out of physical memory as required. Swapping replaces a complete process with another in memory whereas paging removes a 'page' (usually 2–4 kbytes) of a process and replaces it with a page from another process.

3 In 1994, while investigating satellite transceiver sales via Bulletin Board System, Mike Menz encountered a computer with explosives connected to the power switch.

4 Although components of The Coroner's Toolkit are presented in this book, it is not covered in detail. Additional information about TCT is available at www.porcupine.org/forensics.

perform their analysis on the raw data and in other instances they will want to examine the data as they are arranged by the operating system. Take a Palm V handheld device as an example. An examination of the full contents of the device's physical RAM and ROM can reveal passwords that are hidden by the Palm OS interface. On the other hand, viewing the data logically using the Palm OS or Palm Desktop enables the examiner to determine which data were stored in the Memo application and the category in which they were stored.

Take the Linux operating system as another example. When instructed to search for child pornography on a computer running Linux, an inexperienced examiner might search at the file system (logical) level for files with a GIF or JPG extension (`find / -iname *.jpg -print`). In some cases this may be sufficient to locate enough pornographic images to obtain a search warrant for a more extensive search or to discipline an employee for violation of company policy. However, in most cases, this approach will fail to uncover all of the available evidence. It is a simple matter to change a file extension from JPG to DOC, thus foiling a search based on these characteristics. Also, some relevant files might be deleted but still resident in unallocated space. Therefore, it is usually desirable to search every sector of the physical disk for certain file types (`strings - /dev/hda | grep JFIF`).

Searching at the physical level also has potential pitfalls. For instance, if a file is fragmented, with portions in non-adjacent clusters, keyword searches may give inaccurate results.

> *if an examiner were to enter the keyword 'Manhattan Project' and a file containing that text was arranged in several fragmented data clusters, it is very possible that the search would fail to register a 'hit' on that file. Even worse, if a cluster ends, for example, with the text phrase 'Tomorrow we'll go to Manhattan' and the next physical cluster begins with 'project supervision,' the search will register a false hit.* (Guidance Software 2000)

Fortunately, some tools will search each sector of the drive and are simultaneously aware of the logical arrangement of the data, giving the examiner the best of both worlds.[5]

NETWORKS, ENCRYPTION, AND STEGANOGRAPHY

The proliferation of handheld devices connected to wireless networks has ushered in an era of pervasive computing. One of the most significant

5 Another aspect of physical disk examination is the restoration of damaged media and recovery of overwritten data (NTI 2001). Although this level of examination is beyond the scope of this book, guidelines are provided for preserving damaged media later in this chapter.