SYNGRESS®

FREE E-BOOK DOWNLOAD

Techno Security's™ Guide to E-Discovery and Digital Forensics

A Comprehensive Handbook for Investigators, Examiners, IT Security Managers, Lawyers, and Academia

- Internationally known experts in computer forensics share their decades of hard-learned wisdom
- Tips, tricks, and specific procedures to use in building your high-tech forensics lab
- A must read for all cyber cops, digital forensic examiners, attorneys, and those directing IT resources and policy

Jack Wiles Lead Author

thetrainingco. LLC

Tammy Alexander
Stevee Ashlock
Susan Ballou
Larry Depew
Greg Dominguez
Art Ehuan
Ron Green
Johnny Long
Kevin Reis
Amber Schroader
Karen Schuler
Eric Thompson

FOREWORD BY JIM CHRISTY

DIRECTOR OF FUTURES EXPLORATION, DEFENSE CYBER CRIME CENTER (DC3)

Visit us at

www.syngress.com

Syngress is committed to publishing high-quality books for IT Professionals and delivering those books in media and formats that fit the demands of our customers. We are also committed to extending the utility of the book you purchase via additional materials available from our Web site.

SOLUTIONS WEB SITE
To register your book, visit www.syngress.com/solutions. Once registered, you can access our solutions@syngress.com Web pages. There you may find an assortment of value-added features such as free e-books related to the topic of this book, URLs of related Web sites, FAQs from the book, corrections, and any updates from the author(s).

ULTIMATE CDs
Our Ultimate CD product line offers our readers budget-conscious compilations of some of our best-selling backlist titles in Adobe PDF form. These CDs are the perfect way to extend your reference library on key topics pertaining to your area of expertise, including Cisco Engineering, Microsoft Windows System Administration, CyberCrime Investigation, Open Source Security, and Firewall Configuration, to name a few.

DOWNLOADABLE E-BOOKS
For readers who can't wait for hard copy, we offer most of our titles in downloadable Adobe PDF form. These e-books are often available weeks before hard copies, and are priced affordably.

SYNGRESS OUTLET
Our outlet store at syngress.com features overstocked, out-of-print, or slightly hurt books at significant savings.

SITE LICENSING
Syngress has a well-established program for site licensing our e-books onto servers in corporations, educational institutions, and large organizations. Contact us at sales@syngress.com for more information.

CUSTOM PUBLISHING
Many organizations welcome the ability to combine parts of multiple Syngress books, as well as their own content, into a single volume for their own internal use. Contact us at sales@syngress.com for more information.

SYNGRESS®

SYNGRESS®

Techno Security's™ Guide to E-Discovery and Digital Forensics

Jack Wiles Lead Author

Tammy Alexander
Stevee Ashlock
Susan Ballou
Larry Depew
Greg Dominguez
Art Ehuan
Ron Green
Johnny Long
Kevin Reis
Amber Schroader
Karen Schuler
Eric Thompson

KEY	SERIAL NUMBER
001	HJIRTCV764
002	PO9873D5FG
003	829KM8NJH2
004	BPOQ48722D
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

PUBLISHED BY
Syngress Publishing, Inc.
Elsevier, Inc.
30 Corporate Drive
Burlington, MA 01803

Printed in the United States of America
1 2 3 4 5 6 7 8 9 0
ISBN 13: 978-1-59749-223-2

Publisher: Amorette Pedersen
Acquisitions Editor: Patrice Rapalus
Technical Editor: Jack Wiles
Cover Designer: Michael Kavish
Project Manager: Gary Byrne
Page Layout and Art: Patricia Lupien
Copy Editors: Audrey Doyle, Adrienne Rebello
Indexer: Richard Carlson

For information on rights, translations, and bulk sales, contact Matt Pedersen, Commercial Sales Director; email m.pedersen@elsevier.com.

Technical Editor

Jack Wiles is a security professional with over 30 years' experience in security-related fields, including computer security, disaster recovery, and physical security. He is a professional speaker and has trained federal agents, corporate attorneys, and internal auditors on a number of computer crime-related topics. He is a pioneer in presenting on a number of subjects that are now being labeled "Homeland Security" topics. Well over 10,000 people have attended one or more of his presentations since 1988. Jack is also a cofounder and president of TheTrainingCo. He is in frequent contact with members of many state and local law enforcement agencies as well as special agents with the U.S. Secret Service, FBI, U.S. Customs, Department of Justice, the Department of Defense, and numerous members of high-tech crime units. He was also appointed as the first president of the North Carolina InfraGard chapter, which is now one of the largest chapters in the country. He is also a founding member and "official" MC of the U.S. Secret Service South Carolina Electronic Crimes Task Force.

Jack is also a Vietnam veteran who served with the 101st Airborne Division in Vietnam in 1967-68. He recently retired from the U.S. Army Reserves as a lieutenant colonel and was assigned directly to the Pentagon for the final seven years of his career. In his spare time, he has been a senior contributing editor for several local, national, and international magazines.

Contributors

Tammy Alexander is the director of Fountainhead College of Technology's Center for Information Assurance & Cybersecurity Training (IACT) in Knoxville, TN. She also serves as the vice president of the Knoxville InfraGard East Tennessee Chapter and was recently awarded the FBI Director's Community Leadership Award for her contributions to area cyber security efforts.

Tammy holds a bachelor's degree in network security and forensics and is currently pursuing a master's degree at Capella University. She also holds the following certifications: MCSE: Security, CompTIA Security+, CIW Security Analyst, CompTIA Project+, CNA (Certified Novell Administrator), and CNSS (4011, 4012, 4013, 4014A). She is a member of several security organizations. Her research interests include security awareness training, IA curriculum development, cyber crime, and cyber law. She has conducted numerous local, regional, and national lectures and student workshops in the areas of information assurance and cyber security.

Stevee Ashlock is an international speaker, trainer, and consultant appearing at universities, conventions, conferences, and associations. As a keynote speaker, Stevee facilitates corporate seminars and interactive workshops concentrating on professional presentation. Stevee has participated in numerous high-profile criminal trials, working side by side with the defense team, coaching and refining important strategies used in the courtroom to elevate jury awareness and comprehension of evidence.

Stevee provides legal clients with a fresh insight and unique trial consulting service specializing in the effective preparation of expert witnesses. Understanding that a trial often is made or broken on key witness testimony and demeanor, she guides the way expert witnesses deliver their testimonies and evidence. She blends science and art into effective communication that will be vitally important to how the jury perceives the expert witness's credibility. Additionally, she strategizes one-on-one with her clients to perfect their effectiveness and dynamics in the courtroom.

Stevee is a member of the Toastmasters International, an instructor for the Knowledge Shop, an author, and a syndicated columnist. She is honoree of the Madison Who's Who of Executives and Professionals Registry for signification accomplishments, contribution to society, and dedication toward exemplary goals.

Susan M. Ballou is program manager for forensic science in the Office of Law Enforcement Standards at the National Institute of Standards and Technology (NIST) and liaison to Department of Justice and DHS for forensic attribution. In this capacity she has evaluated scientific research under numerous forensic disciplines to ensure that the end product applies

to the bench forensic examiner. Susan has established contacts with various federal forensic laboratories, including the U.S. Secret Service, Department of Defense, FBI, DEA, ATF, and U.S. Postal Inspection Service, to reduce research duplication and obtain vital input.

Her forensic laboratory experience spans almost 20 years and includes forensic toxicology, drug analysis, serology, hairs, fibers and DNA. She is a charter member of TWGFibe, now known as SWGMAT, and was the chair of the quality control/quality assurance subgroup for several years. Susan holds fellow status with the American Academy of Forensic Science (AAFS) and was past chair of the criminalistics section. She has Diplomate certification with the American Board of Criminalistics and is a member and past president of the Mid-Atlantic Association of Forensic Scientists (MAAFS). She is chair of the E30 Forensic Science Committee of the American Society for Testing and Materials (ASTM) and recently joined the International High Technology Crime Investigation Association (HTCIA) to stay current with developments in computer forensics.

Larry Depew, PMP, is the director of the New Jersey Regional Computer Forensic Laboratory (NJRCFL), a partnership between the FBI and State of New Jersey that provides forensic examinations and training to law enforcement in the field of digital forensics. He retired from the Federal Bureau of Investigation (FBI) as a supervisory special agent after nearly 32 years and is currently employed by the State of New Jersey. Larry leads a laboratory of 24 forensic examiners from nine law enforcement agencies servicing more than 550 federal, state, and local law enforcement agencies in New Jersey and the surrounding region.

Larry oversaw the overall construction of the NJRCFL's physical laboratory space and implemented a quality system for laboratory operations to meet client quality requirements for digital forensic examinations, law enforcement training, and expert testimony.

Prior to becoming director of the NJRCFL, Larry worked on several information technology projects at the FBI in Washington, D.C., including developing user requirements for case management systems, and as project manager for the deployment of the Investigative Data Warehouse (IDWv1.0). Larry is an experienced digital forensic examiner who has conducted more than 100 examinations and reviewed the output of more than

1,000 examinations performed by NJRCFL examiners. His digital forensic certifications include the FBI CART Forensic Examiner (Windows, Linux, and personal data assistants) and steganography investigator.

Larry chaired the FBI's Computer Analysis Response Team's (CART) first Standard Operating Procedure and Quality System committee, which formed the basis for today's RCFL National Program and CART Standard Operating Procedures.

Larry is an adjunct professor in digital forensics at The College of New Jersey (TCNJ). He has also taught digital forensics at the New Jersey Institute of Technology (NJIT). Larry is a project management professional certified through the Project Management Institute. He has lectured at many government and private sector conferences on topics relating to data management, workflow, computer security, and digital forensics. He has appeared on the Fox network and the Philadelphia ABC affiliate as an expert regarding digital evidence and Internet safety. He has been interviewed by several national publications and regional newspapers regarding digital evidence analysis, computer security, and Internet safety.

Greg Domínguez is the director of Forensic Computers, Inc. He is a retired U.S. Air Force Office of Special Investigations computer crime investigator. As an Air Force special agent he was the first chief of the Air Force Computer Forensic Lab, which later became the Department of Defense Computer Forensics Lab (DCFL). Since retiring from the Air Force in October 1997, he has held positions in information security at Trident Data Systems; as the director of the National Computer Forensics Lab at Ernst & Young LLP; and as director of computer forensics at Fiderus, Inc. In these positions he has worked computer crime cases involving multimillion-dollar fraud, computer intrusions, child exploitation, and matters involving national security. In his current position at Forensic Computers, he manages the day-to-day operations, including the development and manufacture of forensic systems.

Art Ehuan (CISSP, CFCE, EnCE) is a digital forensic expert with senior management experience in developing and implementing digital forensic facilities for corporations and the United States government.

Art previously managed the Information Security Department for USAA, a Fortune 200 financial services company, where he developed and implemented policies, process, and technology for a state-of-the-art digital forensic facility for handling computer forensics and electronic discovery. Art was previously the deputy chief information security officer at Northrop Grumman, where he developed and implemented three digital forensic facilities for the company. He also developed and implemented Cisco Systems' first digital investigative facility.

Art also has extensive government experience in digital forensics. He was formerly an FBI special agent certified as a Computer Analysis Response Team member and Air Force Office of Special Investigations special agent certified as a computer crime investigator.

Art was formerly an adjunct professor at Georgetown University, Duke University, and George Washington University, where he taught undergraduate and graduate courses on computer forensics, incident response, and computer crime.

Ron Green (CISSP, ISSMP), a senior vice president at the Information Security Business Continuity division of Bank of America, currently serves as an information security business continuity officer supporting the Bank's Network Computing Group. He formerly managed a bank team dedicated to handling cyber investigations, computer forensics, and electronic discovery. Prior to joining Bank of America, Ron was a Secret Service agent and part of the agency's Electronic Crimes Agent Program (ECSAP). In addition to the investigative and protection work all agents perform, ECSAP agents perform cyber investigations and computer forensics for the agency. Ron started with the Secret Service in its Phoenix Field Office, and he then transferred to the agency's headquarters to become part of the Electronic Crimes Branch (ECB). While part of ECB he provided support to the ECSAP agents in the field. He also worked on national and international cyber crimes cases, initiatives, and laws. He was the project manager for Forward Edge and the Best Practice Guides for Seizing Electronic Evidence, version 2.0.

Ron graduated from the United States Military Academy at West Point, earning a bachelor's degree in mechanical engineering, and he earned a graduate certificate from George Washington University in computer security and information assurance. Ron currently serves as the treasurer/secre-

tary for the Financial Services Information Sharing and Analysis Center (FS/ISAC) and as a board member for the Institute for Computer Forensic Professionals. Ron currently lives in North Carolina with his wife, Cheryl, and their four children.

Johnny Long is a Christian by grace, a family guy by choice, a professional hacker by trade, a pirate by blood, a ninja in training, a security researcher, and an author. His home on the Web is http://johnny.ihackstuff.com.

Johnny wrote Appendix A.

Kevin Reis (CISSP, CFE, GCFA, EnCE) has extensive public and private sector experience in the fields of computer forensics, network investigations, financial fraud investigations, and electronic discovery. Kevin began his career conducting counterintelligence investigations as a special agent with the Federal Bureau of Investigation (FBI), but he soon joined the FBI Computer Analysis Response Team (CART). As a CART field examiner, Kevin provided computer forensics support and technical consultation to investigations ranging from financial institution fraud and child pornography to espionage. Kevin then joined the National Aeronautics and Space Administration (NASA) Office of Inspector General (OIG) as a computer crime investigator (CCI), where he investigated computer and network intrusions at the Goddard Space Flight Center. Following his tenure at NASA, Kevin entered the private sector, working as a computer intrusion analyst at Aegis Research Corporation and then as a senior associate with the Forensic Technology Services practice of the Big Four accounting firm KPMG. While at KPMG, Kevin provided computer forensics, data analysis, e-discovery, and investigative services on financial fraud and civil litigation engagements. Following the events of September 11, 2001, Kevin reentered public service with the Department of Justice OIG as a special agent to build the OIG's computer forensics program. Kevin is currently a special agent with the Federal Deposit Insurance Corporation OIG Electronic Crimes Unit and a reserve Air Force Office of Special Investigations CCI.

Amber Schroader has been involved in the field of computer forensics for the past 17 years. Amber has developed and taught numerous training courses for the computer forensic arena, specializing in the field of wireless

forensics as well as mobile technologies. Amber is the CEO of Paraben Corporation and continues to act as the driving force behind some of the most innovative forensic technologies. As a pioneer in the field, Amber has been key in developing new technology to help investigators with the extraction of digital evidence from hard drives, e-mail, and handheld and mobile devices. Amber has extensive experience in dealing with a wide array of forensic investigators ranging from federal, state, local, and foreign government as well as corporate investigators. With an aggressive development schedule, Amber continues to bring new and exciting technology to the computer forensic community worldwide and is dedicated to supporting the investigator through new technologies and training services that are being provided through Paraben Corporation. Amber is involved in many different computer investigation organizations, including The Institute of Computer Forensic Professionals (ICFP) as the chairman of the board, HTCIA, CFTT, and FLETC.

Amber currently resides in Utah and Virginia with her two children, Azure and McCoy.

Karen Schuler is vice president of ONSITE^3's Consulting Practice Group. She brings over 15 years of management, technology, forensics, and electronic discovery experience to ONSITE^3's team of experts and specialists. Karen's experience ranges from the migration of data, enterprisewide technology planning and implementation, forensic investigations to large and complex litigation matters involving electronic discovery. As a former owner of a boutique computer forensics and security firm as well as a contracted computer forensic examiner for the U.S. Securities and Exchange Commission, she is an expert at understanding the intricate details involved in providing admissible and defensible evidence.

Karen has a wide range of experience in dealing with change management, technology assessments, and investigations as they relate to large corporate entities in the financial services industry, pharmaceutical, retail, manufacturing, health care, and technology fields. In addition, she has routinely been engaged on large, unwieldy electronic discovery projects where an expert is required to oversee the methodologies as well as provide recommendations for better practices.

Eric Thompson is responsible for setting the company's strategic direction and leading its growth as a global provider of computer forensics, cryptography, and password recovery software and services. An award-winning expert on the topic of encryption, decryption, and computer forensics, Eric has presented research on cryptography and code breaking to Congress and other groups in Washington, D.C. He has also worked with the U.S. Department of Defense, where he was recognized for his code-breaking expertise that led to the largest drug arrest in Bolivian history. He is a frequent guest instructor at the Federal Law Enforcement Training Center (FLETC) and at High Tech Criminal Investigation Association (HTCIA) events. Eric is an honorary lifetime member of the International Association of Computer Investigative Specialists (IACIS).

Foreword Contributor

Jim Christy is currently the director of futures exploration for the Defense Cyber Crime Center (DC3). Christy is a recently retired special agent, with 35 years of federal service, specializing in cyber crime investigations and digital evidence. From November 2003 to November 2006, Christy was the director of the Defense Cyber Crime Institute (D.C.C.I.), responsible for researching, developing, testing, and evaluating forensic and investigative tools for the Department of Defense Law Enforcement and Counterintelligence organizations. In October 2003, the Association of Information Technology Professionals voted Jim the winner of the 2003 Distinguished Information Science Award for his outstanding contribution through distinguished services in the field of information management.

Contents