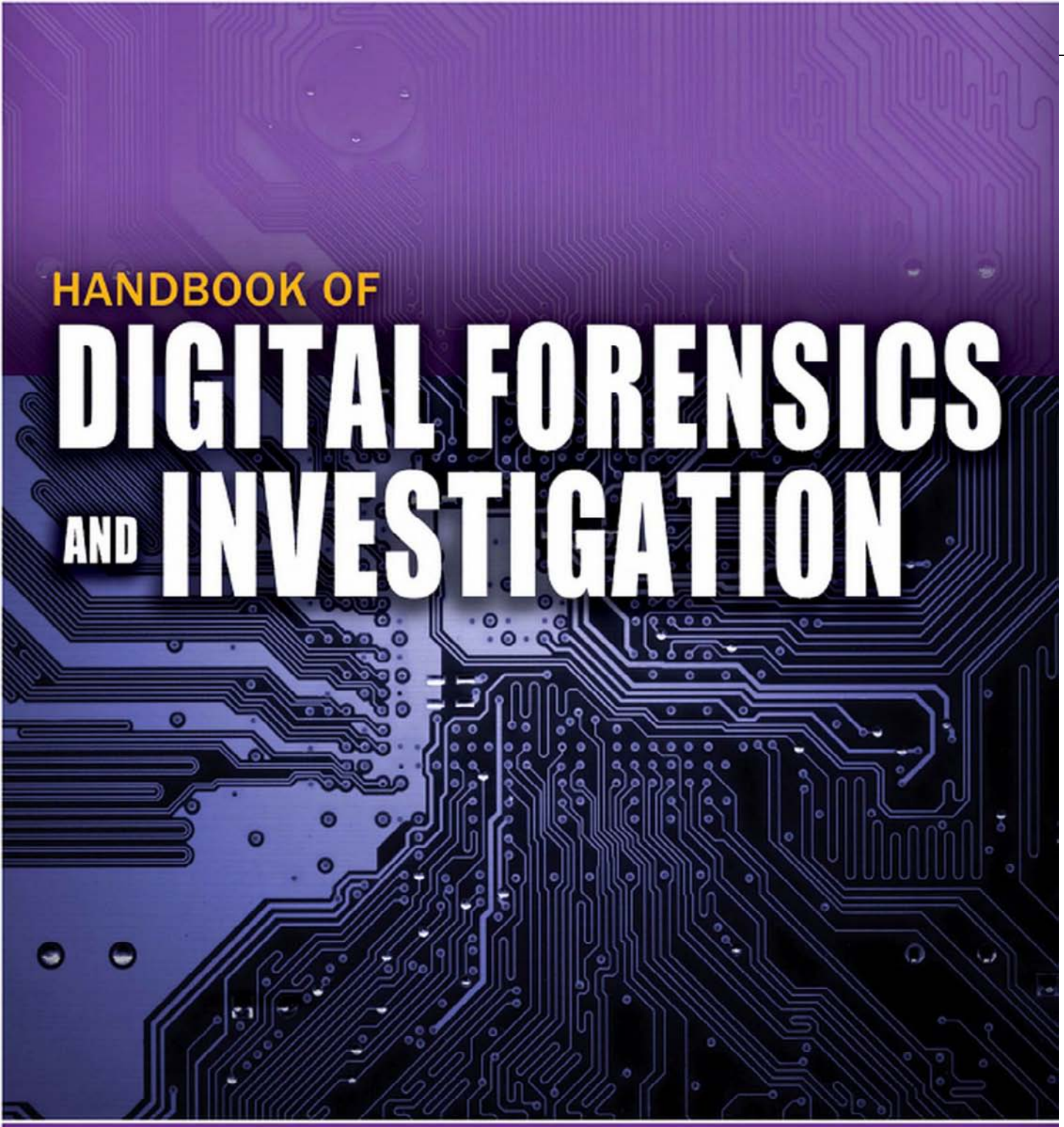


EDITED BY

EOGHAN CASEY

# Handbook of Digital Forensics and Investigation

This page intentionally left blank

# Handbook of Digital Forensics and Investigation

Edited by

**Eoghan Casey**

With contributions from

**Cory Altheide**
**Christopher Daywalt**
**Andrea de Donno**
**Dario Forte**
**James O. Holley**
**Andy Johnston**
**Ronald van der Knijff**
**Anthony Kokocinski**
**Paul H. Luehr**
**Terrance Maguire**
**Ryan D. Pittman**
**Curtis W. Rose**
**Joseph J. Schwerha IV**
**Dave Shaver**
**Jessica Reust Smith**

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Academic Press is an imprint of Elsevier

Elsevier Academic Press
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA
525 B Street, Suite 1900, San Diego, California 92101-4495, USA
84 Theobald's Road, London WC1X 8RR, UK

This book is printed on acid-free paper.



**Library of Congress Cataloging-in-Publication Data**
Application Submitted

**British Library Cataloguing in Publication Data**
A catalogue record for this book is available from the British Library

ISBN 13: 978-0-12-374267-4

For all information on all Elsevier Academic Press publications
visit our Web site at www.elsevierdirect.com

Printed in the United States of America

09 10 9 8 7 6 5 4 3 2 1

*To Genevieve, Roisin and Hesper*

This page intentionally left blank

# Contents

# Contributors

**Eoghan Casey** cmdLabs, Baltimore, MD
**Curtis W. Rose** Curtis W. Rose & Associates, Laurel, MD
**Cory Altheide** Mandiant Highlands Ranch, CO
**James O. Holley** Ernst & Young LLP, New York, NY
**Paul H. Luehr** Stroz Friedberg, Minneapolis, MN
**Jessica Reust Smith** Stroz Friedberg, Washington, DC
**Joseph J. Schwerha IV** TraceEvidence, Charleroi, PA
**Christopher Daywalt** cmdLabs, Baltimore, MD
**Andy Johnston** University of Maryland, Baltimore County, Baltimore, MD
**Ryan D. Pittman** U.S. Army CCIU, Fort Belvoir, VA
**Dave Shaver** U.S. Army, Woodbridge, VA
**Anthony Kokocinski** CSC, Chicago, IL
**Ronald van der Knijff** Netherlands Forensic Institute, Den Haag, The Netherlands
**Terrance Maguire** cmdLabs, Baltimore, MD
**Dario Forte** DFLabs, Crema (CR), Italy
**Andrea de Donno** Lepta Milano (MI), Italy

This page intentionally left blank

# Foreword

Everywhere around you, you can find a digital storage device within arm's reach. We have "Electronic Attention Deficit Disorder:" our concentration being pulled from one device to another.

You use a mobile device where you make your phone calls, send text messages, post on Twitter, all while surfing the web. You use a computer to communicate, pay bills, order groceries, or even watch television. You probably also use one or more of the following devices on a daily basis: GPS, video game system, eReader, MP3 player, digital video recorder, or more.

For better or worse, our lives—our personal/private data—are recorded on these devices moment-by-moment. As a result, we are seeing the rise in crimes, civil litigation cases, and computer security incidents that exploit your data found on these devices. This Handbook is a powerful resource for investigating these cases and analyzing evidence on computers, networks, mobile devices and other embedded systems.

The demand for digital forensic professionals to analyze these devices has increased due to the sheer number of cases that organizations now face. Major incidents such as TJX, Heartland, and Hannaford may have drawn the most media attention, but attacks against small, medium, and large businesses that include data breaches, fund transfers, and intellectual property theft are no longer rare. And these security breaches are costing organizations millions of dollars. For the digital forensic investigator, he or she must be able to effectively respond, investigate, and ultimately answer difficult questions. As criminal cases continue collecting a subject's or victim's cell phone, computer, and other electronic devices to solve a crime, and as civil lawsuits introduce electronically stored evidence, the investigator's role is crucial.

For all of us, the digital forensic profession grows more challenging. We no longer analyze just a desktop system for evidence. In many cases, we examine an enterprise network with more than 1,000 nodes, a mobile device, or even a portable game system. The skills and the knowledge required to meet the

increasing demands placed on a digital forensic investigator today are immense. That is why this Handbook helps us all. It sets the mark for an in-depth examination of the diversity that encompasses today's digital forensic field.

Digital Forensics is undergoing a transition from a perceived ad hoc field into a scientific one that requires detailed analysis combined with a variety of sound and proven methods. One of the main themes that struck me while reading this Handbook is the strong case made for why a scientific foundation is crucial to analyze a case successfully. The Handbook is organized by the old and new disciplines in the digital forensic field where the new breakthroughs are occurring daily. From network and mobile device forensics to traditional forensics using the latest techniques against UNIX, Apple Macintosh, and Microsoft Windows operating systems, this Handbook offers details that are extremely cutting edge and provides new approaches to digital based investigations—from data theft breaches to intellectual property theft. I particularly enjoy the sections that provide detailed explanations in straightforward terms; they offer good ideas that I hope to use in my own forensic reports.

When I first picked up the Handbook, I was impressed with the depth and scope of expertise of the assembled author team. Many led the investigations noted above and those that made national headlines in the past ten years. If you had the ability to truly call a digital forensic "A-Team" together to help with a case, these authors would comprise the majority of that team. We are fortunate that they bring their hard-core practical experiences to each and every chapter.

It is clear that this Handbook will become a must read for new and seasoned investigators alike.

I urge you to read and understand the principles presented in the following pages. True scientific analyses that use the techniques presented here will allow you to solve your cases. I hope you enjoy the Handbook as much as I have. My hat is off to the authors for their continued contributions to the digital forensic field and for coming together to produce this Handbook.

**Rob Lee**
*Director, MANDIANT, Inc.*
*Digital Forensic Curriculum Lead and Faculty Fellow, The SANS Institute*

## BIO:

Rob Lee is a Director for MANDIANT (http://www.mandiant.com), a leading provider of information security consulting services and software to Fortune 500 organizations and the U.S. Government. Rob is also the Curriculum Lead for Digital Forensic Training at the SANS Institute (http://forensics.sans.org).

Rob has more than 13 years experience in computer forensics, vulnerability and exploit discovery, intrusion detection/prevention, and incident response. After graduating from the U.S. Air Force Academy, he served in the U.S. Air Force as a founding member of the 609th Information Warfare Squadron, the first U.S. military operational unit focused on Information Operations. Later, he served as a member of the Air Force Office of Special Investigations where he conducted computer crime investigations, incident response, and computer forensics. Prior to joining MANDIANT, Rob worked directly with a variety of U.S. government agencies in the law enforcement, Department of Defense, and intelligence communities. He provided the technical lead for a vulnerability discovery and exploit development team, ran a cyber forensics branch, and led a computer forensic and security software development team. Rob is coauthor of the bestselling book, *Know Your Enemy, 2nd Edition*, and was named "Digital Forensic Examiner of the Year" by the Forensic 4Cast 2009 Awards. Rob holds a bachelor's degree from the U.S. Air Force Academy and his MBA from Georgetown University.

This page intentionally left blank

# About the Authors

## Eoghan Casey

Eoghan Casey is founding partner of cmdLabs, author of the foundational book *Digital Evidence and Computer Crime*, and coauthor of *Malware Forensics*. For over a decade, he has dedicated himself to advancing the practice of incident response and digital forensics. He helps client organizations handle security breaches and analyzes digital evidence in a wide range of investigations, including network intrusions with international scope. He has testified in civil and criminal cases, and has submitted expert reports and prepared trial exhibits for computer forensic and cyber-crime cases.

As a Director of Digital Forensics and Investigations at Stroz Friedberg, he maintained an active docket of cases and co-managed the firm's technical operations in the areas of computer forensics, cyber-crime response, incident response, and electronic discovery. He also spearheaded Stroz Friedberg's external and in-house forensic training programs as Director of Training. Eoghan has performed thousands of forensic acquisitions and examinations, including Windows, UNIX, and Macintosh systems, Enterprise servers, smart phones, cell phones, network logs, backup tapes, and database systems. He also has extensive information security experience, as an Information Security Officer at Yale University and in subsequent consulting work. He has performed vulnerability assessments, deployed and maintained intrusion detection systems, firewalls and public key infrastructures, and developed policies, procedures, and educational programs for a variety of organizations.

Eoghan holds a B.S. in Mechanical Engineering from the University of California at Berkeley, and an M.A. in Educational Communication and Technology from New York University. He conducts research and teaches graduate students at Johns Hopkins University Information Security Institute, and is Editor-in-Chief of *Digital Investigation: The International Journal of Digital Forensics and Incident Response.*

## Cory Altheide

Cory Altheide has been performing forensics and incident response for eight years. He has responded to numerous incidents for a variety of clients and is constantly seeking to improve the methodologies in use in the incident response field. Mr. Altheide is currently a principal consultant at Mandiant, an information security consulting firm that works with the Fortune 500, the defense industrial base and the banks of the world to secure their networks and combat cyber-crime.

Prior to joining Mandiant, Mr. Altheide worked at IBM, Google and the National Nuclear Security Administration (NNSA). Mr. Altheide has authored several papers for the computer forensics journal *Digital Investigation* and co-authored *UNIX and Linux Forensic Analysis* (2008). Additionally, Mr. Altheide is a recurring member of the program committe of the Digital Forensics Research Workshop (DFRWS).

## Christopher Daywalt

Christopher Daywalt is a founding partner of cmdLabs, and has considerable experience conducting digital investigations within large enterprises and handling security incidents involving persistent information security threats. He is dedicated to providing consistent, quality work that directly addresses the needs of organizations that experience information security events.

Before working at cmdLabs, Chris was an instructor and course developer at the Defense Cyber Investigations Training Academy, where he authored and delivered instruction in digital forensics and investigation to Federal law enforcement and counter intelligence agents. While there he produced advanced material in specific areas such as live network investigation, Windows and Linux intrusion investigation, log analysis and network exploitation techniques. During this work he frequently served as the lead for development and delivery.

Prior to that, he worked as an incident handler in the CSC Computer Investigations and Incident Response group, where he performed investigation, containment and remediation of enterprise-scale security incidents for large corporations. Through these endeavors he gained experience responding to a variety of events, including massive PCI/PII data breaches at corporate retailers and persistent intrusions into government-related organizations. Chris also worked as a global security architect at CSC, conducting assessment and design of security technologies and architectures for deployment in enterprise information systems.

Chris earned his bachelor's degree from UMBC, and holds an MS in Network Security from Capitol College.

## Andrea de Donno

Andrea De Donno was born in Milan, Italy in 1975. His education focused on science. After a brief stint with the Carabinieri, in 1998 he began working for one of the major intelligence firms, providing technical investigation services and technology to the Italian Military Operations Units. In 2002, he became Managing Director of the company, increasing the company's revenues and expanding it throughout Italy with the creation of new Operations Centers. That same year, he was also named Managing Director of an Italian consulting firm offering specialized risk analysis and risk management services to medium and large companies.

## Dario Forte

Dario Forte, former police detective and founder and CEO of DFLabs has worked in information security since 1992. He has been involved in numerous international conferences on information warfare, including the RSA Conference, Digital Forensic Research Workshops, the Computer Security Institute, the U.S. Department of Defense Cybercrime Conference, and the U.S. Department of Homeland Security (New York Electronic Crimes Task Force). He was also the keynote speaker at the Black Hat conference in Las Vegas. Mr. Forte is Associate Professor at UAT and Adjunct Faculty at University of Milano, Crema Research Center. With more than 50 papers and book chapters written for the most important scientific publishers worldwide, he provides security consulting, incident response and forensics services to several government agencies and global private companies.

## James O. Holley

James Holley leads a team of computer forensics and electronic evidence discovery professionals in the New York Metropolitan Area providing a wide range of dispute resolution services to clients, including Computer Forensics, Forensic Text and Data Analytics, Electronic Discovery/Discovery Response Services, and Electronic Records Management/Legal Hold services.

With Ernst & Young for ten years, James is the technology leader for their U.S. Computer Forensics team. He also leads EY's New York office of Forensic Technology and Discovery Services, a specialty practice in Fraud Investigation and Dispute Services. James has provided expert testimony in deposition and trial and has testified in arbitration proceedings.

Prior to joining EY, James spent nearly ten years as a federal agent with the U.S. Air Force Office of Special Investigations. As a special agent, he gained

experience conducting general criminal investigations prior to beginning a career in counterintelligence. He spent six years as an AFOSI counterintelligence case officer planning, developing and executing offensive counterintelligence operations and teaching new case officers. In his final assignment, he was an AFOSI computer crime investigator focused on integrating computer forensics and incident response capabilities into counterintelligence operations.

James holds a bachelors' degree from the United States Air Force Academy, a Master's of Science in Computer Science from James Madison University, and is a Certified Computer Examiner (CCE).

## Andy Johnston

Andy Johnston has been a software developer, scientific programmer, and a Unix system administrator in various capacities since 1981. For the last ten years, he was worked as IT security coordinator for the University of Maryland, Baltimore County specializing in network intrusion detection, anti-malware computer forensics, and forensic log analysis.

## Ronald van der Knijff

Ronald van der Knijff received his B.Sc. degree in electrical engineering in 1991 from the Rijswijk Institute of Technology. After performing military service as a Signal Officer he obtained his M.Sc. degree in Information Technology in 1996 from the Eindhoven University of Technology. Since then he works at the Digital Technology and Biometrics department of the Netherlands Forensic Institute as a forensic scientist.

He is responsible for the embedded systems group and is also court-appointed expert witness in this area. He is author of the (outdated) cards4labs and TULP software and founder of the TULP2G framework. He is a visiting lecturer on 'Cards & IT' at the Dutch Police Academy, a visiting lecturer on 'Smart Cards and Biometrics' at the Masters Program 'Information Technology' of TiasNimbas Business School and a visiting lecturer on 'Mobile and Embedded Device Forensics' at the Master's in 'Artificial Intelligence' of the University in Amsterdam (UvA).

## Anthony Kokocinski

Anthony Kokocinski started his forensic career working for the Illinois Attorney General directly out of college. His passion for Macintosh computers quickly led him to research and continue work on this from the number of "it's a Mac,

you do it" cases that came across his desk. During this tenure he began to work with the Macintosh Electronic Search and Seizure Course for the RCMP's Canadien Police College. When he became tired of the very well traveled roads in Illinois he fell in with CSC on a government contract for the DoD. One of the many duties there was to design the first Macintosh Forensics Examinations course. This became very popular for both the DoD as well as Federal Law Enforcement. He takes great credit and pleasure of having converted over half of the on-staff instructors at DCITA to the Macintosh. After leaving the DoD he can now be found residing happily in the finest city in the world (Chicago), where he is still doing security design, implementation, and testing as well as litigation support for CSC and their clients. He can usually be seen regularly at conferences talking at least once about Macintosh related topics.

## Paul H. Luehr, Esq.

Paul Luehr is Managing Director and General Counsel of Stroz Friedberg, a technical consulting firm. Mr. Luehr specializes in complex e-discovery, computer forensics, data breaches, and consumer protection issues. He is a former federal cybercrimes prosecutor and FTC Assistant Director who worked on matters ranging from national Internet fraud to the post-9/11 investigation of terrorist Zacarias Moussaoui. Mr. Luehr has lectured before the National Academy of Sciences, the FBI Academy, the U.S. Justice Department, and has traveled abroad as a U.S. State Department Speaker on e-commerce and cybercrime. He is a graduate of Harvard University and the UCLA School of Law.

## Terrance Maguire

Terrance Maguire is a partner at cmdLabs, conducting cyber-crime investigations, including those involving network intrusions, insider attacks, anonymous and harassing e-mails, data destruction, electronic discovery and mobile devices. He has nearly 20 years of experience in physical and digital forensic investigations, has developed and led training programs in varied areas of law enforcement and digital evidence, and has experience implementing counter-intelligence intrusion detection programs.

Before working at cmdLabs, Terry was Assistant Director of Digital Forensics at Stroz Friedberg, where he was responsible for casework, lab management, and internal training efforts. His prior experience includes senior-level Forensic Computer Analyst the U.S. State Department, where he was responsible for conducting analysis on digital evidence. As a cyber operations specialist for the Department of Defense, he implemented network

surveillance, network packet analysis, wireless surveys, and intrusion detection. In addition, at the Defense Computer Investigations Training Program (DCITP), Terry developed and presented a broad range of instruction to federal law enforcement on topics such as computer search and seizure, incident response, digital evidence, computer forensic examinations, and intrusion investigations.

Earlier in his investigative career, as a forensic detective with the Chesterfield County Police Department in Virginia, Terry collected, evaluated, and processed evidence from crime scenes, prepared comprehensive case reports, and trained department personnel in forensic techniques. Subsequently, as a Forensic Scientist for the Virginia Division of Forensic Science, he conducted bloodstain pattern analysis in criminal cases and testified in court as an expert witness, and he was the Principal Instructor at the Forensic Science Academy.

Terry is a professorial lecturer at the George Washington University where he teaches graduate-level courses focusing on incident response and computer intrusion investigations involving network-based attacks. He received an M.S. in Communication Technology from Strayer University and a B.S. in Chemistry from James Madison University. He is qualified as an ASCLD/LAB inspector in digital evidence, and is a member of the Virginia Forensic Science Academy Alumni Association.

## Ryan D. Pittman

Ryan Pittman is currently a Criminal Investigator (1811) for the U.S. Army Criminal Investigation Command's Computer Crime Investigative Unit (CCIU) near Washington, DC, continuing a career of more than 12 years in law enforcement and forensic science. Special Agent Pittman previously served as a Digital Forensic Examiner for Stroz Freidberg, LLC; a Master Instructor for Guidance Software, Inc.; a Senior Forensic Analyst for Sytex, Inc.; and a Computer Crime Coordinator (as an active duty soldier) for the U.S. Army Criminal Investigation Command. He is currently a Ph.D. candidate with Northcentral University, after receiving his Master of Forensic Sciences from National University, his Master of Science in Management in Information Systems Security from Colorado Technical University, and his Bachelor of Science in Criminal Justice from the University of Maryland University College. Special Agent Pittman has taught for George Washington University, University of Maryland University College, and Central Texas College, among others, and has been invited to teach or speak about incident response, digital investigations, and computer forensics on five continents.

## Curtis W. Rose

Curtis W. Rose is the President and founder of Curtis W. Rose & Associates LLC, a specialized services company which provides computer forensics, expert testimony, litigation support, computer intrusion response and training to commercial and government clients. Mr. Rose is an industry-recognized expert in computer security with over 20 years' experience in investigations, computer forensics, technical and information security. Mr. Rose was also a founding member of the Mandiant Corporation, where he served as the Vice President of Research, Chief Technology Officer, and led technical teams which conducted research & development, computer intrusion investigations, forensic examinations, and provided technical support to criminal investigations and civil litigation. Prior to joining Mandiant, Mr. Rose was the Director of Investigations and Forensics, and Principal Forensic Scientist, for The Sytex Group, Inc. where he helped develop and manage the company's investigations, incident response and forensics programs. Prior to joining Sytex, Mr. Rose was a Senior Counterintelligence Special Agent with the United States Army's Military Intelligence Branch where he specialized in technical investigations and computer forensics.

## Dave Shaver

Dave Shaver is currently serving as a Criminal Investigator (1811) for the U.S. Army Criminal Investigation Command's Computer Crime Investigative Unit (CCIU) near Washington DC, continuing a career of more than 13 years in law enforcement and forensic science. He is a graduate of Ohio University, with a Bachelor of Arts degree in sociology/criminology. Dave is a frequent presenter at national and international events, sharing his research and experiences in incident response and network intrusion investigations, and has been intimately involved in the development of incident response and investigation tools and practices that are in wide-spread use by the digital forensic community.

## Joseph J. Schwerha IV

Joseph J. Schwerha IV is a professor, prosecutor and private attorney. Mr. Schwerha has the unique experience of having served in both the private and public sectors for several years. As an Associate Professor within the Department of Business and Economics at California University of Pennsylvania, he is responsible for instruction on all aspects of business law, as well as for development of new curriculum in the areas of privacy, cybercrime and information law. While not teaching, Mr. Schwerha primarily splits his time between his law firm, Schwerha & Associates (a boutique law firm concentrating in the

areas of privacy, information security and electronic discovery law), and Trace Evidence, LLC. (his computer forensics and e-discovery consulting business).

Mr. Schwerha holds a Juris Doctor from the University of Pittsburgh, as well as both a Bachelors' and Masters' of Science from Carnegie Mellon University. He has published numerous articles in various publications, including law reviews.

## Jessica Reust Smith

Jessica Reust Smith is the Assistant Director of Digital Forensics at Stroz Friedberg's Washington, DC office, where she conducts digital forensic acquisitions and analyses on media pertinent to civil, criminal and regulatory matters, internal investigations and computer incident response efforts. Ms. Smith also assists with the strategic development of Stroz Friedberg's e-discovery methodologies and is responsible for supervising and performing the preservation, processing and production of data for complex, global electronic discovery projects. Ms. Smith has a Master of Forensic Sciences and Master of Arts in Computer Fraud Investigation from George Washington University, and a Bachelor of Science and Bachelor of Arts from the University of Queensland in Brisbane, Australia.

# Acknowledgements


## Eoghan Casey

Working with the contributing authors on this Handbook has been a deep honor and learning experience. Thanks to all involved for their commitment to advancing the field of digital forensics and investigation, and their willingness to share their knowledge. I have deepest gratitude for Christopher Daywalt for being smarter, better, faster, and repeatedly rescuing this book by lifting us over seemingly insurmountable hurdles. Thanks for the tireless support and patience of Liz Brown, Renske van Dijk, Nikki Levy, and everyone else at Elsevier who worked on bringing this book to print. Special thanks to Genevieve, Roisin and Hesper for their infinite love and reminding me what is important in life.

## Cory Altheide

There are a lot of people I owe a debt of gratitude with regards to Linux & UNIX forensics. First and foremost among these people is Brian Carrier – without the Sleuthkit we'd still be using stone knives and bearskins to examine any non-Windows file systems. I'd like to thank Eoghan Casey for encouraging me to share my knowledge with the community, first through Digital Investigation, then the Digital Forensics Research Workshop, and most recently this handbook. Thanks go to Rob Lee for his continued advice and support over the years, and to Andy Rosen for being the vanguard of our industry as well as a good friend. An enormous amount of gratitude goes to Avery Brewing for Mephistopheles Stout, Dogfish Head for Theobroma, and New Belgium for La Folie. Finally, to my incredible wife Jamie and my two amazing daughters for always reminding me why it is I do what I do – I love you.

## Chris Daywalt

I would like to thank Eoghan Casey for the opportunity to make my modest contribution to this excellent text.