


PLACING THE SUSPECT BEHIND THE KEYBOARD

Using Digital Forensics and Investigative Techniques to Identify
Cybercrime Suspects

Brett Shavers



Placing the Suspect Behind the Keyboard

Using Digital Forensics and
Investigative Techniques to
Identify Cybercrime Suspects

Brett Shavers

Harlan Carvey, Technical Editor



ELSEVIER

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

Syngress is an Imprint of Elsevier

SYNGRESS

Acquiring Editor: *Chris Katsaropoulos*

Development Editor: *Heather Scherer*

Project Manager: *Malathi Samayan*

Designer: *Matthew Limbert*

Syngress is an imprint of Elsevier
225 Wyman Street, Waltham, MA 02451, USA

© 2013 Elsevier, Inc. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher. Details on how to seek permission, further information about the Publisher's permissions policies and our arrangements with organizations such as the Copyright Clearance Center and the Copyright Licensing Agency, can be found at our website: www.elsevier.com/permissions.

This book and the individual contributions contained in it are protected under copyright by the Publisher (other than as may be noted herein).

Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods or professional practices, may become necessary. Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information or methods described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

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.

For information on all Syngress publications
visit our website at <http://store.elsevier.com>

ISBN: 978-1-59749-985-9

Printed in the United States of America
13 14 15 16 12 11 10 9 8 7 6 5 4 3 2 1

Working together to grow
libraries in developing countries

www.elsevier.com | www.bookaid.org | www.sabre.org

ELSEVIER

BOOK AID
International

Sabre Foundation

Acknowledgments

The forensic community has grown in size in the past years, so to give thanks to the many that have kept me focused, encouraged me, and shared their knowledge is a longer list than I could share in a few pages. There are some that cannot go without public acknowledgement, for without their support as friends and confidants, this book would not have been but a fleeting thought.

I cannot thank Harlan Carvey enough for agreeing to be the Tech Editor for this book. Harlan is the rare person that not only has legendary expertise in the field, but also has a great heart as a person and family man. Troy Larson, another digital forensics legend, for his foreword to my book. Dave Stenhouse, one of the best persons I know to bounce ideas on the tough cases. Going back a few years, I thank the finest partner a detective could have, Mark Klinke. Mark is one of those investigators that will dig and not stop until the case is finished, all the while doing an absolute great job. I tend to think his tenacity in purpose rubbed off a bit on me. I'd also like to thank a dear friend, Brad Toftshagen, who constantly reminds me through his actions, that personal integrity and honor is something to keep strong, no matter the cost or effort. My constant calls, emails, and bothersome requests over the years, and in particular for this book, are appreciated.

As for my number one supporter, I thank my wife Chikae, as she has endured my endless discussions of computer jargon and excitement of finding forensic artifacts in my cases. Her limitless support was instrumental and probably the main reason I started and finished this book. I attribute my success and the success of our children to her tireless efforts and patience to encourage all of us to drive on.

About the Author

Brett Shavers is a former law enforcement officer of a municipal police department. He has been an investigator assigned to state and federal task forces. Besides working many specialty positions, Brett was the first digital forensics examiner at his police department, attended over 2000 hours of forensic training courses across the country, collected more than a few certifications along the way, and set up the department's first digital forensics lab in a small, cluttered storage closet.

Brett has been an adjunct instructor at the University of Washington's Digital Forensics Program, an expert witness and digital forensics consultant, a prolific speaker at conferences, a blogger on digital forensics, and is an honorary member of the Computer Technology Investigators Network. Brett has worked cases ranging from child pornography investigations as a law enforcement investigator to a wide range of civil litigation cases as a digital forensics expert consultant. And even though it's been more than two decades since wearing the uniform, he's still a Marine.

About the Technical Editor

Harlan Carvey (CISSP) is Vice President of Advanced Security Projects with Terremark Worldwide, Inc. Terremark is a leading global provider of IT infrastructure and “cloud computing” services, based in Miami, FL. Harlan is a key contributor to the Engagement Services practice, providing disk forensics analysis, consulting, and training services to both internal and external customers. Harlan has provided forensic analysis services for the hospitality industry, financial institutions, as well as federal government and law enforcement agencies. Harlan’s primary areas of interest include research and development of novel analysis solutions, with a focus on Windows platforms.

Harlan holds a bachelor’s degree in electrical engineering from the Virginia Military Institute and a master’s degree in the same discipline from the Naval Postgraduate School. Harlan resides in Northern Virginia with his family.

Foreword

I first met Brett Shavers several years ago at a training event that he had organized. At the time, Brett was a police officer—one of a handful among the local jurisdictions with the training and skill to take on digital forensic investigations. I had no idea then how often our paths would cross or how valuable his support could be. Brett has since become a leader in the digital forensic community of the Pacific North West, presiding over our local professional organization (www.ctin.org), running his own consulting company, writing papers and training materials, and maintaining websites devoted to Windows FE and RegRipper. In fact, that the world knows anything of my little internal project, Windows FE, has more to do with Brett's work and enthusiasm than my own efforts. I am, therefore, quite honored that Brett asked me to write a foreword to this book.

To best describe the value of *Placing the Suspect Behind the Keyboard*, I need to put the book in context. When I started my career many years ago, there was only one book available on the subject of what we now call digital forensics. That book was primarily focused on how to investigate certain types of computer crime under the laws that existed two decades ago. Its emphasis was law, with very little presented regarding technical detail, investigative techniques, or, strictly speaking, digital forensics.

In the late 1990s, a few technical books about “computer forensics” began trickling out, and then, slowly, more have trickled out every year since. The early books presented the digital forensics more as a collection of generally applicable tips and tricks than technical deep dives into the varieties of electronic evidence. Over time, however, articles and books on forensics adopted a more solid and scientific approach, and began taking on a broader range of forensics topics with greater detail and systematic focus on particular subject matters. Thus, we have moved from those early books on “computer forensics” to books about the forensics particularities of specific platforms,

e.g., “windows forensics,” to books that focus on specific parts of specific platforms, e.g., “registry forensics.” This has been a good thing.

Particularly valuable over the past few years has been the evolving trend of books and articles to focus on distinct “artifacts,” that is, the trace evidence that computer or user activities create in memory, leave on disk, or send over the network. Armed with a good knowledge of artifacts, a competent forensics investigator can develop a surprisingly accurate and detailed account of what has happened on a computer system or digital device. Internet history, file usage, data deletion, program execution, IP addresses, even geolocation of devices, are all facts available to the digital investigator to decipher a blow-by-blow account what has been done with a computer or device. Despite all this, there is a limit to the conclusions that can be supported by digital evidence alone.

Putting a specific person at the keyboard at a specific time, often one of the most critical issues to be proved, just happens to be one of those things that digital evidence rarely can accomplish on its own. This is not as obvious as it should be, since it is deceptively easy to confuse the computer owner or an account name for a real person behind the keyboard when a deed was done. But account names are not people, and computer owners are not the only people who use their computers. Thus, confusion can have catastrophic consequences when it leads to people being prosecuted or punished in error. It can also lead to investigators being sued for defamation. New forensics investigators are therefore frequently admonished to confine their conclusions to what is supported by the digital evidence they know well, and avoid making unsupported assumptions about the person behind the keyboard, about whom they often know very little to nothing.

Placing the Suspect Behind the Keyboard shows how to bridge the gap between digital and physical evidence to “make the connection between the act and the actor” and establish the person responsible for what was found on the computer. As the book illustrates, sometimes this connect can be made by interviewing witness who can place a person at a place and a specific time. Sometimes the connection must be reconstructed from physical evidence, such as other records gathered from the suspect or third parties. Sometimes, establishing the connection may even require surveillance. Non-law enforcement investigators might consider many of these suggestions as out-of-scope, but this would ignore that all these investigative techniques are important tools to understand, as they all have a place in particular investigations. An investigator who limits the world of evidence to the confines of a hard drive is going to miss evidence. To miss evidence, particular important evidence, is to fail at investigation.

About mid-way through the book, *Placing the Suspect Behind the Keyboard* expands beyond the topic of the title to the all-important program of building a good case. Although there is a research-like aspect to digital forensics, forensics is ultimately about proving or disproving things, not simply dissecting artifacts or building timeline. To succeed at digital forensics, one must be able to do more than pick apart the details. A good investigator must be able to marshal the facts to an end, which involves a bit of organization, an eye for relevancy, and the ability to present technical data to a non-technical audience. All of these topics are addressed, and Mr. Shavers suggestions are practical and useful.

Don't let the word "suspect" in the title make you think this is a book primarily for law enforcement. Although the burdens of proof and rules of evidence collection may differ between criminal and civil investigations (which includes internal corporate investigation), the burden of finding and making sense of the facts does not, particularly when it comes to placing a person behind the keyboard. *Placing the Suspect Behind the Keyboard* is full of useful guidance for digital forensics investigators of all types.

Troy Larson
Microsoft Network Security

Preface

This book was inspired over a decade ago when I was a new detective. The biggest obstacle I faced was that of attribution. In every case to which I was assigned, attributing a crime to a suspect was the main focus. Some cases were easy. Other cases, seemingly impossible. Even just the identification of a suspect was next to impossible in some cases. But in every case, I did my best to identify the suspect and attribute criminal behavior appropriately.

I'm probably no different than most investigators; in that experiencing a horrific crime scene has some effect on the effort I put forth in investigations. After recovering evidence in the first child pornography case assigned to me, I was determined and driven to follow the evidence, identify the suspect, and collect enough evidence to close the case with charges. Seeing the personal damage caused to victims by the sliver of darkness in human nature is more than enough motivation to make sure a case is done right, the first time.

In this age of technology, where the Internet has increased the ease of crime through enabling transfer of contraband, harassment, bullying, intrusions, and facilitating terrorism through electronic communication, investigators need to accomplish the very important goal of *Placing the Suspect Behind the Keyboard*. The identification of a crime and victim does not further our justice system if we do not also identify the suspects.

The intention of this book is to be a guide to that end of placing the suspect behind the keyboard through a combination of digital forensics techniques and more traditional, non-technical investigative methods. Throughout the book, consider that the investigator and the forensic examiner may be the same person or more than two separate people, depending upon the size of their organization. However, their goal is the same and their cooperation with each other should not have half an inch of light between them or their common goal of a successful case conclusion.

Each chapter in this book is independent of the others, but all are interconnected through the same theme and purpose. The principles and concepts cover the best case scenarios and the worst case scenarios. Sometimes, the best evidence is out front in plain sight and the investigator has all the legal authority to seize it. Other times, the evidence may not exist, or be accessible, or able to be interpreted. Rather than giving in, take a step back and reflect on your investigation. There is a clue waiting for you to find it, and follow it. *This is a book of clues.*

Although the theme of this book primarily supports criminal investigations, many of the same methods and processes can be used in civil litigation and internal corporate matters. The primary differences being the legal authority in certain methods of investigations may be different between civil and criminal cases.

I also intentionally focused on the mindset of conducting an investigation, as it is your ideas and intuition that solve cases. Using software and hardware just helps you exploit your ideas eventually into physical evidence. Considering that my first forensic lab was literally a small storage closet converted into a cramped digital forensic lab, remember that it is the person, not the gear, which solves cases. Think of your ability as becoming the Pablo Picasso of forensics. Picasso's art and skill in painting didn't rely upon the kind of paint brush or the number of colors he used. He relied upon his mind. You as the examiner or investigator can do the same.

The principals outlined in the book are meant to be principals, not an absolute checklist, but a guide. The principals can be applied today just as much as they can be applied tomorrow. It is my sincerest intention that by reading this book, you have found one thing that will make your work easier and one thing that makes a case. If you learned one thing that saves you many hours of time, that will have been worth the time reading the book.

But if you learned just one small thing, just that one small *Eureka!* moment which blasts your case wide open, then your time reading this book was more than worthwhile to you. It was worthwhile to the victims in that one case, whether it be a child, a parent, or a business. *And it definitely will impact the suspect, that same suspect you placed behind the keyboard.*

Contents

ACKNOWLEDGMENTS	xi
ABOUT THE AUTHOR	xiii
ABOUT THE TECHNICAL EDITOR	xv
FOREWORD	xvii
PREFACE	xxi
CHAPTER 1	
Introduction.....	1
Digital Evidence Collection.....	2
Simple File Copying.....	4
“Dead Box” Approaches	5
“Live Box” Approaches.....	10
Decision-Making FlowChart	19
Preview/Triage	20
SmartPhones and Cellular Devices	24
GPS	24
Summary.....	25
Bibliography.....	25
CHAPTER 2	
High Tech Interview.....	27
Introduction.....	27
The Main Goal of Questioning a Suspect	28
The Line of Questions for Suspects	30
Computer Skills, Ability, and Knowledge.....	30
Password, Encryption, Steganography, and Deletion	31
Control of the Device(s) in Question.....	33
Other Devices Used by Suspect	34
Software Used by Suspect	35
Internet Use by Suspect.....	36
Online Chat, Email, Forums, Boards, Online Social Networking.....	37
Peer-to-Peer Networking	40
File Storage	42
Crime Specific—Child Pornography.....	44

	Crime Specific—Identity Theft	46
	Other Alleged Crimes	47
	Questions for Victims	48
	Computer Crime Victim Questions—Identity Theft	48
	Computer Crime Victim Questions—Harassment Via Email/Text/Online Postings	49
	Questions for Network Administrators	50
	Customer Accounts—Internet Service Provider, Online Data Hosting, Other Online Services	50
	Summary	51
	Bibliography	51
CHAPTER 3	Physical Investigations	53
	Introduction	53
	Hazards of Acting Upon Minimal Information	54
	Physical Surveillance	56
	Mobile Surveillance	57
	Aerial Surveillance	59
	Video Surveillance	61
	Covertly Installed Cameras	65
	Other Sources of Surveillance Records	66
	Surveillance Notes and Timelines	67
	Electronic Surveillance	69
	Oral Intercepts	70
	Dialed Number Recorders	70
	Trash Runs	72
	Tracking Cell Phones	73
	Vehicle Tracking	75
	Keystroke Logging	76
	Consumer Purchase Records	77
	Obtaining Personal Information	78
	Undercover and Informant Operations	79
	Witnesses	81
	Neighbors as Surveillance Agents	82
	Deconfliction	82
	Summary	83
	Bibliography	84
	Further Reading	84
CHAPTER 4	Technical Investigations	85
	Introduction	85
	Digital Investigative Techniques	86

What is a Person?	87
Who? What? When? Why? Where? And How?	89
Location	89
Time	90
Wireless Connections	94
Network (Cloud) Connections	95
Photos and Videos	97
Internet Evidence (Mobile Devices, Computers, and Game Systems)	103
Texts and Emails	110
Calendar Evidence	111
"Other" Device Forensics	112
Online Social Networking	113
User Activity	114
User logins	114
User-Specific Computer Activity	115
Digital Authorship	116
Profiling	117
Biological Forensic Evidence	118
Triage and Previews	118
Summary	121
Bibliography	121
Further Reading	121
 CHAPTER 5	
Putting It All Together	123
"2 + 2 = Putting It All Together"	123
The Evidence as a Whole	124
Avoiding Assumptions	124
Who Did It?	125
Timelines	129
Follow the Evidence	132
Computer User Activity	133
Rabbit Holes	133
Summary	134
Bibliography	135
 CHAPTER 6	
Investigative Case Management	137
Introduction	137
Basic Case Tracking	138
The Case Name	139
Note Taking	141

	Analyzing Your Notes	142
	Analysis with Spreadsheets	144
	Analysis with Databases	147
	Analysis Using Charts	149
	Analysis Using Maps	153
	Fresh Set of Eyes	154
	Summary	154
	Bibliography	155
CHAPTER 7	Case Presentation.....	157
	Introduction	157
	It's Not Whether You Win or Lose.....	158
	Investigative Mindset.....	158
	Your Audience	159
	Preparation	160
	Organizing Case Information	160
	Value of Visuals	162
	Presentation Media	162
	Slideshows and Animations	165
	Charts and Diagrams	167
	The Suspect's Machine	173
	Analogies	175
	Avoid TMI (Too Much Information)	179
	Your Presentation.....	180
	Summary	180
	Bibliography	181
CHAPTER 8	Cheat Sheets and Quickstart Guides	183
	Introduction	183
	Cheat Sheets and Quickstart Guides	184
	Turnover Folders	186
	Visual Aids.....	187
	Investigative Aids	188
	Study Guides.....	189
	Make Your Own	190
	Checklists.....	191
	Summary	192
	Bibliography	192
CHAPTER 9	Some Things Will Become Easier, Others	
	Not So Much	193
	Introduction	193

It Will Become Easier to Place a Suspect Behind	
the Keyboard.....	193
Operating Systems Will Make It Easier	194
Computer Hardware and Software Applications	
Will Make It Easier	195
New and Innovative Computing Devices Will Make	
It Easier	197
Data Storage and Access Will Make It Easier	197
Public Awareness and Education Will Make	
It Easier	199
The Suspect Will Make It Easier.....	199
Pre-Placed Surveillance Systems Will Make It Easier....	200
New Laws and Employer Rights Will Make It Easier....	201
It Will Become More Difficult to Place a Suspect Behind	
the Keyboard.....	201
Encryption Will Make It More Difficult	201
Public awareness Will Make It More Difficult	204
Remote Control of Systems Will Make It More	
Difficult.....	204
Open Wi-Fi Hotspots Will Make It More Difficult.....	205
Massive and Duplicate Data Will Make It More	
Difficult.....	205
Virtual Machines Will Make It More Difficult	206
Even More Techniques Will Make It Difficult.....	208
Summary	208
Bibliography	209
CHAPTER 10 Online Investigations	211
Introduction	211
Online Investigations	211
Why the Internet?	212
What Can Be Found Online?.....	212
How to Build Your “Super” Browser.....	213
Internet Search Engines and Directories	214
Usernames.....	215
Social Networking Websites	216
Blogs, Forums, and Wikis.....	217
The Dark Web.....	219
Following the Bread Crumbs	220
Capturing Webpages as Evidence	221
Be Careful of Your Visits Online	222
Summary	222
Bibliography	223

CHAPTER 11	Case Studies	225
	Introduction	225
	A Day in the Life of a Cybercriminal	226
	Backdating Documents	226
	False Names and Disposable Email Accounts	229
	Evidence Leads to More Evidence	230
	Searching for All the Bad Things.....	231
	Scenario—Threatening Blog Posts	233
	Making the Wrong Kind of Friends Online.....	234
	A Break in the Case, Otherwise Known as a Suspect's Mistake.....	235
	Altered Evidence and Spoliation	237
	Spoofed Call Harassment	240
	Disgruntled Employee Steals and Deletes Employer's Data	242
	Missing Evidence.....	245
	Bomb Threats by Email.....	246
	ID the Suspect	247
	Online Extortion.....	249
	Placing Suspect at a Location	250
	Placing the Suspect in the Office at a Specific Location	251
	Stolen Property.....	252
	IP Addresses Aren't Enough	253
	Planted Evidence	254
	The Life and Casework of a Cyber Investigator.....	255
	Technical Knowledge and Skills	256
	This Case is Different from That Case	257
	Testifying to Your Work.....	258
	Summary.....	259
	Bibliography	260
	INDEX.....	261