The Basics of Digital Forensics

The Basics of Digital Forensics

The Primer for Getting Started in Digital Forensics

John Sammons

Technical Editor

Jonathan Rajewski

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: Danielle S. Miller
Designer: Alisa Andreola

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

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
Sammons, John.
The basics of digital forensics : the primer for getting started in digital forensics / John Sammons.
p. cm.
ISBN 978-1-59749-661-2
1. Computer crimes–Investigation. I. Title.
HV8079.C65S35 2012
363.25'968–dc23
2011047052

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

Typeset by: diacriTech, Chennai, India

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

Dedication

For Lora, Abby, and Rae for making me a truly
blessed and lucky man.

To my mother Juanita, and my grandmother Grace.
For the many sacrifices you made and
the example you set … I miss you.

Contents

PREFACE xv
ACKNOWLEDGMENTS xix
ABOUT THE AUTHOR xxi
ABOUT THE TECHNICAL EDITOR xxiii

CHAPTER 1 Introduction 1
Introduction 1
What Is Forensic Science? 2
What Is Digital Forensics? 2
Uses of Digital Forensics 3
Criminal Investigations 3
Civil Litigation 4
Intelligence 5
Administrative Matters 6
Locard's Exchange Principle 7
Scientific Method 7
Organizations of Note 7
Scientific Working Group on Digital Evidence 8
American Academy of Forensic Sciences 8
American Society of Crime Laboratory Directors/
Laboratory Accreditation Board 9
National Institute of Standards and Technology (NIST) 9
American Society for Testing and Materials (ASTM) 9
Role of the Forensic Examiner in the Judicial System 10
The CSI Effect 10
Summary 10
References 11

CHAPTER 2 Key Technical Concepts 13
Introduction 13
Bits, Bytes, and Numbering Schemes 13
Hexadecimal 14
Binary to Text: ASCII and Unicode 14

File Extensions and File Signatures 15
Storage and Memory 16
Magnetic Disks 17
Flash Memory 18
Optical Storage 18
Volatile versus Nonvolatile Memory 18
Computing Environments 19
Cloud Computing 19
Data Types 20
Active Data 20
Latent Data 21
Archival Data 21
File Systems 21
Allocated and Unallocated Space 22
Data Persistence 22
How Magnetic Hard Drives Store Data 23
Page File (or Swap Space) 25
Basic Computer Function—Putting it All Together 26
Summary 27
References 27

CHAPTER 3 Labs and Tools 29
Introduction 29
Forensic Laboratories 29
Virtual Labs 30
Lab Security 30
Evidence Storage 31
Policies and Procedures 32
Quality Assurance 32
Tool Validation 33
Documentation 34
Digital Forensic Tools 35
Tool Selection 36
Hardware 36
Software 39
Accreditation 40
Accreditation versus Certification 42
Summary 43
References 43

CHAPTER 4 Collecting Evidence 45
Introduction 45
Crime Scenes and Collecting Evidence 46
Removable Media 46
Cell Phones 47
Order of Volatility 49
Documenting the Scene 49
Photography 50
Notes 51
Chain of Custody 52
Marking Evidence 52
Cloning 52
Purpose of Cloning 54
The Cloning Process 54
Forensically Clean Media 55
Forensic Image Formats 55
Risks and Challenges 55
Value in eDiscovery 56
Live System versus Dead System 56
Live Acquisition Concerns 56
Advantage of Live Collection 57
Principles of Live Collection 58
Conducting and Documenting a Live Collection 58
Hashing 59
Types of Hashing Algorithms 59
Hashing Example 59
Uses of Hashing 60
Final Report 61
Summary 61
References 62

CHAPTER 5 Windows System Artifacts 65
Introduction 65
Deleted Data 66
Hibernation File (Hiberfile.sys) 66
Sleep 67
Hibernation 67
Hybrid Sleep 67
Registry 67
Registry Structure 68

Attribution 69
External Drives 70
Print Spooling 70
Recycle Bin 70
Metadata 72
Removing Metadata 74
Thumbnail Cache 75
Most Recently Used (MRU) 76
Restore Points and Shadow Copy 76
Restore Points 76
Shadow Copies 77
Prefetch 78
Link Files 78
Installed Programs 79
Summary 79
References 80

CHAPTER 6 Antiforensics 81
Introduction 81
Hiding Data 83
Encryption 83
What Is Encryption? 83
Early Encryption 84
Algorithms 85
Key Space 86
Some Common Types of Encryption 86
Breaking Passwords 88
Password Attacks 89
Brute Force Attacks 89
Password Reset 90
Dictionary Attack 90
Steganography 92
Data Destruction 94
Drive Wiping 94
Summary 100
References 100

CHAPTER 7 Legal 103
Introduction 103
The Fourth Amendment 104

Criminal Law—Searches without a Warrant 104
Reasonable Expectation of Privacy 104
Private Searches 105
E-mail 105
The Electronic Communications Privacy Act (ECPA) 105
Exceptions to the Search Warrant Requirement 105
Searching with a Warrant 108
Seize the Hardware or Just the Information? 109
Particularity 109
Establishing Need for Off-Site Analysis 109
Stored Communications Act 110
Electronic Discovery (eDiscovery) 111
Duty to Preserve 111
Private Searches in the Workplace 112
Expert Testimony 113
Summary 114
References 115

CHAPTER 8 Internet and E-Mail 117
Introduction 117
Internet Overview 117
Peer-to-Peer (P2P) 119
The INDEX.DAT File 120
Web Browsers—Internet Explorer 120
Cookies 120
Temporary Internet Files, a.k.a. web Cache 121
Internet History 122
Internet Explorer Artifacts in the Registry 123
Chat Clients 124
Internet Relay Chat (IRC) 125
ICQ "I Seek You" 125
E-Mail 126
Accessing E-mail 126
E-mail Protocols 126
E-mail as Evidence 126
E-mail—Covering the Trail 127
Tracing E-mail 127
Reading E-mail Headers 128
Social Networking Sites 129
Summary 129
References 130

CHAPTER 9 Network Forensics 131
Introduction 131
Social Engineering 132
Network Fundamentals 132
Network Types 133
Network Security Tools 135
Network Attacks 135
Incident Response 137
Network Evidence and Investigations 139
Network Investigation Challenges 141
Summary 141
References 142

CHAPTER 10 Mobile Device Forensics 145
Introduction 145
Cellular Networks 146
Cellular Network Components 147
Types of Cellular Networks 148
Operating Systems 149
Cell Phone Evidence 150
Call Detail Records 151
Collecting and Handling Cell Phone Evidence 152
Subscriber Identity Modules 154
Cell Phone Acquisition: Physical and Logical 155
Cell Phone Forensic Tools 155
Global Positioning Systems (GPS) 157
Summary 161
References 161

CHAPTER 11 Looking Ahead: Challenges and Concerns 163
Introduction 163
Standards and Controls 164
Cloud Forensics (Finding/Identifying Potential Evidence Stored in the Cloud) 165
What Is Cloud Computing? 165
The Benefits of the Cloud 166
Cloud Forensics and Legal Concerns 166
Solid State Drives (SSD) 167
How Solid State Drives Store Data 167
The Problem: Taking out the Trash 168

Speed of Change 169
Summary 170
References 171

INDEX 173

Preface

Seal Team Six tore the hard drives from Osama bin Laden's computers. Some of Michael Jackson's final words were captured on an iPhone. Google searches for chloroform played a central role in the trial of Casey Anthony. This list could go on and on. Digital forensics is used to keep us safe, to ensure justice is done and company and taxpayer resources aren't abused. This book is your first step into the world of digital forensics. Welcome!

Digital forensics is used in a number of arenas, not just in catching identity thieves and Internet predators. For example, it's being used on the battlefields of Afghanistan to gather intelligence. The rapid exploitation of information pulled from cell phones and other devices is helping our troops identify and eliminate terrorists and insurgents.

It's being used in the multibillion-dollar world of civil litigation. Gone are the days when opposing parties exchanged boxes of paper memos, letters, and reports as part of the litigation process. Today, those documents are written in 1s and 0s rather than ink. They are stored on hard drives and backup tapes rather than in filing cabinets.

Digital forensics helps combat the massive surge in cybercrime. Identity thieves, child pornographers, and "old school" criminals are all using and leveraging technology to facilitate their illegal activities.

Finally, it's being used in the workplace to help protect both companies and government entities from the misuse of their computer systems.

INTENDED AUDIENCE

As the title suggests, this is a beginner's book. The only assumption is that you have a fundamental understanding or familiarity of computers and other digital devices. If you have a moderate or advanced understanding of digital forensics, this book may not be for you. As part of Syngress's "Basics" series, I wrote this book more as a broad introduction to the subject rather than an all-encompassing tome. I've tried to use as much "plain English" as possible, making it (hopefully) an easier read.

I'd like to emphasize that this is an introductory book that is deliberately limited in length. Given that, there is much that couldn't be covered in depth or even covered at all. Each chapter could be a book all by itself. There are many wonderful books out there that can help further your understanding. I sincerely hope you don't stop here.

ORGANIZATION OF THIS BOOK

The book is organized in a fairly straightforward way. Each chapter covers a specific type of technology and begins with a basic explanation of the technology involved. This is a necessity in order to really understand the forensic material that follows.

To help reinforce the material, the book also contains stories from the field, case examples, and Q and A with a cryptanalyst as well as a specialist in cell phone forensics.

Chapter 1 – Introduction

What exactly is digital forensics? Chapter 1 seeks to define digital forensics and examine how it's being used. From the battlefield to the boardroom to the courtroom, digital forensics is playing a bigger and bigger role.

Chapter 2 – Key Technical Concepts

Understanding how computers create and store digital information is a perquisite for the study of digital forensics. It is this understanding that enables us to answer questions like "How was that artifact created?" and "Was that generated by the computer itself, or was it a result of some user action?" We'll look at binary, how data are stored, storage media, and more.

Chapter 3 – Labs and Tools

In "Labs and Tools," we look at the digital forensic environment and hardware and software that are used on a regular basis. We will also examine standards used to accredit labs and validate tools. Those standards are explored along with quality assurance, which is the bedrock of any forensic operation. Quality assurance seeks to ensure that results generated by the forensic examination are accurate.

Chapter 4 – Collecting Evidence

How the digital evidence is handled will play a major role in getting that evidence admitted into court. Chapter 4 covers fundamental forensically sound practices that you can use to collect the evidence and establish a chain of custody.

Chapter 5 – Windows System Artifacts

The overwhelming odds are that you have a Windows-based computer on your desk, in your briefcase, or both. It's a Windows world. (No disrespect, Mac people. I'm one of you.) With over a 90% market share, it clearly represents the bulk of our work. Chapter 5 looks at many of the common Windows artifacts and how they are created.

Chapter 6 – Antiforensics

The word is out. Digital forensics is not the secret it once was. Recovering digital evidence, deleted files, and the like is now common place. It's regularly seen on such shows as NCIS and CSI. The response has been significant. They are now many tools and techniques out there that are used to hide or destroy data. These are examined in Chapter 6.

Chapter 7 – Legal

Although a "forensic" science, the legal aspects of digital forensics can't be divorced from the technical. In all but certain military/intelligence applications, the legal authority to search is a perquisite for a digital forensics examination. Chapter 7 examines the Fourth Amendment, as well as reasonable expectations of privacy, private searches, searching with and without a warrant, and the Stored Communications Act.

Chapter 8 – Internet and E-Mail

Social networks, e-mail, chat logs, and Internet history represent some of the best evidence we can find on a computer. How does this technology work? Where is this evidence located? These are just a few of the questions we'll answer in Chapter 8.

Chapter 9 – Network Forensics

We can find a network almost anywhere, from small home networks to huge corporate ones. Like computers and cell phones, we must first understand how things work. To that end, Chapter 9 begins with networking basics. Next, we start looking at how networks are attacked and what role digital forensics plays in not only the response, but how perpetrators can be traced.

Chapter 10 – Mobile Device Forensics

Small-scale mobile devices such as cell phones and GPS units are everywhere. These devices are in many respects pocket computers. They have a huge potential to store evidence. Digital forensics must be as proficient with these devices as they are desktop computers. We'll look at the underlying technology powering cell phones and GPS units as well as the potential evidence they could contain.

Chapter 11 – Looking Ahead: Challenges and Concerns

There are two "game-changing" technologies that are upon us that will have a huge impact on not only the technical aspect of digital forensics but the legal piece as well. The technology driving solid state hard drives negates much of the traditional "bread and butter" of digital forensics. That is our ability to recover deleted data. As of today, there is no answer to this problem.

Cloud computing creates another major hurdle. In the cloud, data are stored in a complex virtual environment that could physically be located anywhere in the world. This creates two problems; from a technical standpoint, there is an alarming lack of forensic tools that work in this environment. Deleted files are also nearly impossible to recover. Legally, it's a nightmare. With data potentially being scattered across the globe, the legal procedures and standards vary wildly. Although steps are being taken to mitigate this legal dilemma, the situation still persists today.

Being in its infancy, the digital forensics community still has work to do regarding how it conducts its business, especially in relation to the other more traditional disciplines. Chapter 11 will explore this issue.

Acknowledgments

Although my name may be on the cover, this book would not have been possible without the help and support of many people. First, I'd like to thank my family, particularly my wife Lora, and my two girls, Abby and Rae. Their patience, understanding, and willingness to "pick up my slack" while I wrote was invaluable. Thank you, ladies.

Next I'd like to thank Nick Drehel, Rob Attoe, Lt. Lannie Hilboldt, Chris Vance, and Nephi Allred for sharing their expertise and experiences. I have no doubt their contributions made this a better book.

My Chair, Dr. Mike Little, and my Dean, Dr. Charles Somerville, also helped make this book a reality. It would have been impossible for me to write this book and still do my "day job" without their support and assistance. Thank you, gentlemen.

I'd like to thank my Editor, Heather Scherer, and my Tech Editor, Jonathan Rajewski, for keeping me on task and on point. Danielle Miller, my Project Manager at Syngress, deserves my thanks as well for putting up with my last minute editing.

Many thanks go to Jennifer Rehme and Jonathan Sisson. Jennifer, as my GA, helped keep me afloat during the semester handling much of my grading and research for this book and other projects. Jonathan, a digital forensics student here at Marshall, created most of the graphics for this book. I have no doubt that each will be wildly successful and real contributors to the forensic science community. I wish you both nothing but continued success after graduation.

Finally, I'd like to thank Angelina Ward for giving me this opportunity.

About the Author

John Sammons is an Assistant Professor at Marshall University in Huntington, West Virginia. John teaches digital forensics, electronic discovery, information security and technology in the Department of Integrated Science and Technology. He is also the founder and Director of the Appalachian Institute of Digital Evidence. AIDE is a non-profit organization that provides research and training for digital evidence professionals including attorneys, judges, law enforcement and information security practitioners in the private sector. Prior to joining the faculty at Marshall, John co-founded Second Creek Technologies, a digital forensics and electronic discovery firm. While at Second Creek, John served as the Managing Partner and CEO. John is a contract instructor for AccessData and is certified by them as both an instructor and examiner. He is a former Huntington Police officer and currently serves as an investigator for the Cabell County (WV) Prosecutors Office. As an investigator, he focuses on Internet crimes against children and child pornography. John is a member of the FBI WV Cybercrime Task Force. John routinely provides training for the legal and law enforcement communities in the areas of digital forensics and electronic discovery. He is an Associate Member of the American Academy of Forensic Sciences, the High Technology Crime Investigation Association, the Southern Criminal Justice Association, and Infragard.

About the Technical Editor

Jonathan Rajewski (EnCe, CCE, CISSP, CFE, CSI, SANS Lethal Forensicator) is an Assistant Professor in the Computer & Digital Forensic program at Champlain College. Aside from his teaching responsibilities he is member of the Vermont Internet Crimes Task Force serving law enforcement and governmental entities. He is also a Director and Principle Investigator with the Senator Patrick Leahy Center for Digital Investigation. In his prior life he was a Global Senior Digital Forensic Consultant with Protiviti. He was recently honored as 2011 Digital Forensic Examiner of the Year by www.forensic4cast.com.

His high degree of professionalism, passion, and experience in the detection and prevention of white-collar crime complements his ability to teach, manage, and conduct digital forensic investigations. Jonathan has a keen ability to articulate very technical topics and present in such way that's understandable to both experienced and nontechnical audiences. Jonathan is also the author of the 2011->future Undergraduate Digital Forensic curriculum at Champlain College.

Jonathan has served many high profile confidential clients and has worked alongside many governmental and corporate teams. Jonathan holds a B.S. in Economic Crime Investigation from Hilbert College and an M.S. in Managing Innovation & Information Technology from Champlain College. Jonathan resides in Vermont with his family.