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.