Introductory Computer Forensics

Xiaodong Lin

Introductory Computer Forensics

A Hands-on Practical Approach

Springer

Xiaodong Lin
Department of Physics and Computer Science
Faculty of Science
Wilfrid Laurier University
Waterloo, ON, Canada

ISBN 978-3-030-00580-1 ISBN 978-3-030-00581-8 (eBook)
https://doi.org/10.1007/978-3-030-00581-8

Library of Congress Control Number: 2018957125

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

In deep appreciation and endless memory, this book is dedicated to my dear forever beloved grandmother Xiulin Li who raised me up.

Preface

Internet technology is advancing at a speed beyond comprehension. With ever-advancing Internet technology, we truly are living in a digital age. It will certainly improve our quality of life, as it can offer the speed, the capabilities, to handle endless different types of transactions at relatively low cost. Things we take for granted in our daily activities are an excellent example: transferring money, surfing, emailing, sharing information, etc. On the other hand, we will become handicap in our daily life if without Internet. Simply put it, we all depend on the capabilities of Internet technology to run our daily errands more efficiently, even when we do not directly notice it.

Unfortunately, one of Murphy's more applicable axioms becomes apparent with this technology: "with every solution comes a new set of problems." This marvelous new technology will also provide golden opportunities for organized crime groups, as well as other individuals who want to abuse the technology and maximize their profit illegally. Activities like denial of service attacks, website vandalism, online fraud, money laundering, and more have surfaced. We have all read headlines from around the world about companies being hacked and losing personal information; cybercrimes have become a rampant reality that we must all face, and according to the forecast, the cybercrime trends will worsen globally, and billions of dollars will be lost every year in the global conflict against it.

In order to fight against cybercrime effectively, public prosecutors need to be able to do more than simply match a crime to a suspect; they must be able to produce convincing digital evidence in a court of law, before a judge who may not even know what a USB drive is, in order to put the criminals behind bars. This evidence may include all computer log files, corresponding emails, accounting information, spreadsheets, and other related records, regardless of whether or not these files were deleted or not. According to the study, the majority of digital evidence presented in court is obtainable from all sorts of the daily used electronic devices such as computer, digital camera, BlackBerry, and 3G cell phones.

In one case, former Alaska Governor Sarah Palin's e-mail account was hacked by a Tennessee student. After the suspect reset Governor Palin's e-mail account

password and posted the new password on a forum, the FBI was able to trace the suspect's digital footprint or trail, particularly his email address, leading to the suspect's apartment. This evidence was vital in helping the federal prosecutor to acquire further necessary digital evidence and arrest the suspect, even while the suspect removed, altered, concealed, and covered up files on his laptop computer.

No individual alone can effectively fight with online criminals, and technology is evolving much faster than the law can adapt. Traditional forensic science, while still invaluable, will not be able to deal with this new wave of cybercrimes. As a result, an exciting new branch of forensic science—digital forensics—is emerging.

Digital forensic investigation is a sequence of interdependent and linked procedures, employing technology to study and recreate chains of events that lead to the current state of digital objects. Digital objects may include (but are not limited to) computer systems, such as software applications and databases; data storage devices, such as hard disks, CDs, DVDs, and USB drives; electronic document such as spreadsheets, documents, emails, and images. Digital objects could be as large as an entire network or as small as a single byte. By using technology to examine the digital objects, the investigator can present trustworthy, satisfactory, and legally acceptable evidence to a court of law and provide answers to the questions raised about criminal events.

Unlike established traditional forensic analysis, digital forensics, as a new subject, must overcome many challenges before it becomes widely acceptable in courts of law internationally. The major challenges include the following:

(a) The process of collecting the digital evidence may alter the evidence itself, as it can easily be deleted or altered and become inadmissible to the court; hence, the prosecutor must preserve it in the state it was collected in and provide proof that the digital evidence has not suffered any alteration between the time of collection and the time of admission to the court.
(b) As the complexity of digital forensic analysis techniques continues to increase and the size of forensic target grows rapidly, you will experience the need for hundreds of gigabytes, or even terabytes of hard drive space to store all the necessary evidence.
(c) As technology is always advancing more quickly than the law can compensate for, there is no shortage of new opportunities for online criminals to take advantage of "holes in the legal system" and use new technology to perform activities that are clearly immoral; however, technically speaking, these activities may be "legal," as the law does not, or there is no law to deal with the new situation/environment created by the new technology and that may become a stumbling block between the prosecutors and the lawyers.

As a new subject, digital forensics is not well known to the general public, but interest in it is booming, as more companies and individuals seek the truth about what has happened to their network infrastructure. Even as a growing number of court cases (civil, criminal, and otherwise) involve digital evidence (or electronic evidence), trained digital forensic professionals are in short supply, and cybercrime

can be committed anywhere in the world. It has become essential for universities and colleges to offer digital forensics to their students so that the students are well prepared with the proper tools to fight against cybercrime.

I am a strong believer in active learning. A Chinese proverb says: "Tell me, I will forget. Show me, I may remember. Involve me, and I will understand." I strongly believe that theoretical knowledge and practical hands-on experience are necessary to function independently to reach each individual student's full potential, particularly in computer security education. Also, they should be integrated into a coherent whole. Such kinds of educational excursions have been proved very attractive and informative to students in my computer security and forensics classes. It is crucial to let students know why they need to study one subject, what they need to know about the subject, and most importantly, how they can apply knowledge and skills learned in classes to some real-life situations. I am trying to tie the theory with the practical, real world through case studies and practice exercises to help the students learn the material better, because they literally make more connections as opposed to only learning theory and how to apply a formula to get a result. Holistic learning including hands-on experience and theory is what is needed more. For example, man-in-the-middle (MITM) attacks using address resolution protocol (ARP) spoofing in the switched network environment are classic but complicated network attacks. A decent theoretical illustrations help, but may not gain enough classroom attention or cooperation. Thus, in order to improve student learning and encourage cooperation among students, after a theoretical explanation of ARP spoofing and man-in-the-middle attacks, a live demonstration of ARP spoofing and man-in-the-middle attacks can be conducted in class to show students how ARP protocol works before and after the attacks through captured network traffic and how the participating computers will behave as attacks proceed by showing their ARP tables at different stages of the attacks. By doing so, students are able to reflect on knowledge that they just have learned in the classroom. Hence, gaining hands-on experience through live lab experiment is as vital to a student as one is to a medical student. I have taught courses on computer forensics, cyberattack and defense techniques, and software security in several Canadian universities over the past decade. In my teaching, I developed a lot of hands-on practice exercises to enhance understanding of concepts/theories of information security and forensics introduced in my classes and increase student interest in information security and forensics. This book is the first edition of an experience-oriented textbook that stems from the introductory digital forensics course I developed at the University of Ontario Institute of Technology (UOIT), Canada. The objective of this book is to help students gain a better understanding of digital forensics, gaining hands-on experience in collecting and preserving digital evidence by completing various practice exercises. This experience-oriented textbook contains 20 student-directed, inquiry-based practice exercises to help students better understand digital forensic concepts and learn digital forensic investigation techniques. This hands-on, experience-oriented textbook is a great way to introduce people to the world of computer forensics, a fast-evolving field for solving crimes.

Practice Exercise Environment

While all the practice exercises in this book can be conducted in a physical computer, we use virtualization and build a forensics workstation using a publically available Kali Linux virtual machine for your use while working on the exercises in this book. Virtualization is a technology to use a computer hardware to run operating system (s) within an operating system, and it has the potential to be within an operating system within an operating system. It is a way to run multiple operating systems at the same time on one computer hardware, and each operating system runs separately and could do something completely different.

In virtualization, there are two main components, the first being the host machine, the physical machine on which the virtualization takes place, and the second being the guest machine, i.e., the virtual machine (VM).

The benefits of using virtualization or a preconfigured Kali Linux virtual machine include the following:

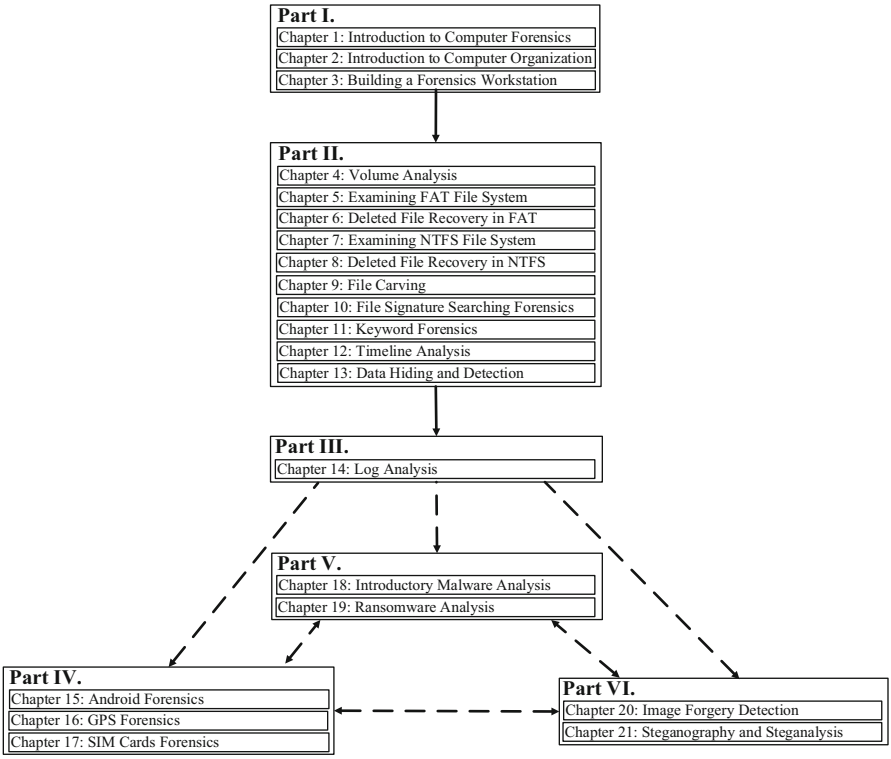
First, we can save a lot of time from configuring the devices and software. If thing does not work out, we can always roll back to a snapshot and start over again until it works. In other words, we can have an environment that can be saved, deleted, backed up, etc., on demand. By using virtualization, we can always have a copy of clean and workable image, which is very good for the purpose of teaching.

Second, all students have the same practice exercise environments, which can be well controlled. As a result, it could become easy to troubleshoot and diagnose problems in the exercise environments of students.

Book Organization

The book consists of 21 chapters, which are organized into 6 parts. Chapter 1 discusses basic concepts of computer forensics. As for the rest, each of them is composed of two parts, background knowledge and hands-on experience through practice exercises. Each theoretical or background section concludes with a series of review questions, which are prepared to test students' understanding of the materials, while the practice exercises are intended to afford students the opportunity to apply the concepts introduced in the section of background knowledge.

The below flowchart illustrates the chapter organizations that instructors can follow to achieve their course plans. The arrow means the order of chapters and sections which the instructors are suggested to follow. The dashed lines indicate that the pointing-to parts are optional for an introductory computer forensics course. For an introductory course, the instructors are suggested to cover the first three parts. Depending on course length and level, the instructor will be able to choose and determine the order of the rest parts, as each of them is self-standing and does not require knowledge from the other sections.



The summary of the book parts is given below:

The first part, or Part I (Chaps. 1–3), is focused on basic computer skill required before studying computer forensics and completing practice exercises in the book. In Chap. 1, we will introduce you to the fundamentals of computer forensics and why computer forensics skills are important to our society. In Chap. 2, we will review some basic concepts in computer organization, which are essential for you to know how computer forensics techniques work. If you are familiar with computer organization, you can skip ahead to the next chapter. In Chap. 3, you will build your own forensics workstation using some open-source digital forensics tools.

Part II (Chaps. 4–13) discusses file system forensics analysis. It is concerned with the most common source of digital evidence, computer storage devices such as hard drives, which can be divided into multiple sections known as partitions. Then each partition is formatted with a file system such as FAT and NTFS before data can be stored into it. It is worth mentioning that this part can be used in conjunction to *File System Forensics Analysis* by Brian Carrier. *File System Forensics Analysis* is an excellent reference for anyone that studies analysis techniques of file systems for investigative purposes. However, this part of our book can be used as extra hands-on exercises to enhance student learning and improve skills and knowledge for file system forensics, thereby helping them gain a more detailed understanding of file

system analysis for investigative purposes. In Chap. 4, we will discuss the concept of disk partitioning and study volume analysis techniques. Chap. 5 describes analysis of FAT file system. In this chapter, we also provide an introduction to the concepts of file system. Then in Chap. 6, the discussion focuses on how to recover deleted files in FAT file system based on remaining file system metadata. Chapter 7 describes analysis of NTFS file system. Then in Chap. 8, the discussion focuses on how to recover deleted files in NTFS file system based on remaining file system metadata. Chapter 9 describes file carving techniques, which can recover deleted files when file system metadata is missing. Chapter 10 covers keyword searching forensic technique. Chapter 11 discusses file signature searching forensic technique. Chapter 12 discusses timeline analysis. In Chap. 13, we discuss data hiding and detection techniques.

Part III (Chap. 14) covers log forensic analysis. Chapter 14 is concerned with forensic analysis of log files in computer systems, which are another important source of digital evidence.

Part IV (Chaps. 15–17) covers mobile device forensics. Chapter 15 discusses android-based device forensics. Chapter 16 studies Global Positioning System (GPS) forensics. Chapter 17 covers forensic analysis of SIM card data.

Part V (Chaps. 18 and 19) is concerned with the study of malware analysis. Chapter 18 provides an introduction to malware analysis. Then in Chap. 19, the study of ransomware, a new breed of malware, is considered.

The last part, or Part VI (Chaps. 20 and 21), is focused on multimedia forensics. In Chap. 20, we will introduce you to the fundamentals of digital image forgery and detection techniques. In Chap. 21, we discuss the principles of image steganography and steganalysis.

Supplements

An Instructor's Solutions Manual
Solutions for all questions in the end of background knowledge section, as well as the textbook practice exercises, are provided. The solutions can be downloaded from the publisher.

Data Files
Data files are provided for the practice exercises, which are required in most of the chapters to complete these hands-on exercises. They are available for download from the publisher.

Waterloo, ON, Canada Xiaodong Lin

Acknowledgments

After several years of teaching an introductory digital forensics course, particularly, receiving positive feedback in extensive lab exercises for hands-on experience, an idea just came to my mind: why not put together the course materials I developed as a textbook, an experience-based textbook in particular.

I realized how much work was involved only after I started to write the book. Finishing the book would be impossible without the help, advice, and support of people. I am greatly grateful to many of my former students and particularly to Corey Knecht, Khalid Alharbi, Muhammad Ali Raffay, Zhenxing Lei, and Aiqing Zhang for their invaluable feedback and suggestion for improvement, especially from their points of view as students, after carefully reviewing parts of the manuscript.

Contents