Review of the book *"Computer Forensics - Evidence Collection and Management"* by Robert C. Newman Auerbach Publications, 2007 Taylor & Francis Group ISBN: 978-0-8493-0561-0

Jannik Pewny

1 What the book is about

Computer forensics means the acquisition, preservation and presentation of evidence, where the evidence is of an electronical nature. The electronic devices, which provide these evidences can be an object in the case, like in a computer intrusion, or they can be a subject, for example if a computer is used as a tool in an identity fraud. There are also cases, where the device is unrelated to the actual crime, e.g. where the offender in a battery took pictures with his cellphone. The neccessity for such evidence can occur in legal cases as well as in violations of computer-use policies in a company.

This books touches a lot of topics around this complex matter. It should be noted that it does not give real technical details. Instead, it gives an overview of a topic.

It is divided into two main parts. The first part covers the basics of computer forensics. The first chapter gives an introduction with definition of computer forensics, electronic evidence, the process of evidence collection and such things. Then there is a chapter about laws and legal processes, followed by one about the different categories an investigation might be neccessary in. The fourth chapter handles different types of crimes in the context of the internet, while the fifth chapter handles the different devices, which can be subject to examinations, like computers, cellphones, PDAs and peripheral devices. This part closes with a chapter on the tools and training for an investigator in the field of computer forensics.

The second part is supposed to handle the actual crime scene investigation and the management of evidence. It begins with a chapter on the numerous administrative things when handling an incident scene, followed by a chapter on the specialties of the investigation in computer centers. The next chapter is about data carriers and file systems. Chapter ten gives information on the equipment of a laboratory for computer forensics and the possibilities for training and certification. While chapter eleven gives general information on the collection of electronic evidence, the chapters twelve and thirteen handle the specifics of investigation on *eMail and Internet* respectively *Mobile phones and PDAs*. The last chapter handles the preparation and presentation of the collected material in a court case.

2 What the book is like

The book seems like there has been paid attention to compiling the "bulletpoints" for the content. A lot of topics get handled and the skeleton of the content is quite appealing, even though some elements seem to be a little missorted. Headlines of the chapters and the introductionary texts are usually interesting and make the reader want to continue reading. The continous text on the other hand is often too shallow to satisfy the expectations, but it is written quite pleasantly, which makes it easy to read and understand.

Each chapter starts with the objectives of the chapter and a short introduction to the handled topic. Both can usually be skipped without loss of information. Also, each chapter ends with a short summary, a list of used terms and some review questions. The summary itself is not of much use, and one has recently read about all the terms. The review questions are mostly of the *fill-in-a-word*-type, which can be seen in Appendix C of the book.
The mentioned non-technicality of the book is not annoying most of the time, but some sentences actually do indicate that they were written without technical knowledge. While *It is common for a laptop to contain one megabyte of RAM and 80 gigabytes of disk storage* might be a typing error, the sentence *scripting languages like perl or linux* is incosiderate.

It has to be noted that the book is full of lists. For example on the different sources of information in computers or PDAs, the equipment of a computer for forensic needs or the steps to process a crime scene. These list do not help most of the time, since they are often vague, incomplete or scattered over the chapters.

3 Recommendation

This book gives you an overview of the topics of computer forensics and does not leave out the parts like law, the chain-of-custody or the forensics expert's role in a court case, which are actually really important in the actual work of computer forensics.

This book will not fit your needs, if you look for details on where electronic evidence can be found, how it can be found and extracted or how to use the tools to do so. Actual Instructions, e.g. on how to scan certain file-types or cached information of a device for information, is not covered here.

On the other hand, if you want an overview of the topic, e.g. if you have to manage the people doing the dirty technical work, this book might be handy. The quite big scope of computer forensics will be known to you, once you have read it. You will in most cases know *what* has to be done, to do the work. The actual *how* does require another book, though.

The reviewer is a student of IT-Security
at the Ruhr-University of Bochum (Horst Görtz Institute)