Review of the book

"Forensic Computing : A Practitioner's Guide"
by Sammes, A.J., Jenkinson, Brian
Springer, 2007

ISBN: 978-1-84628-732-9

Nishant Doshi
MEFGI, Gauridad Campus, India

1 Summary of the review

With the advancement of the digital era, the digital crime (aka cyber crime) increasing day-by-day. This lead to the era of forensic computing in which expert look and analyzed the digital data of criminal and gets the clues from it. Indeed, this book discuss about forensic computing and analysis from its origin to present. As the forensic computing deals with cyber crime, this book very well discussed various case studies regarding crime and related forensics. One thing that I like and recommend to others that, after each chapter put the list of references that will help the readers. I suggest to add the further finding and list of softwares/tools for doing the forensic analysis at the personal/organizational/researcher level.

For the researchers, this book gives the fundamentals understanding of the forensic computing and its workings in the various environments. I will recommend this book to the UG students to strengthen their fundamentals on forensic analysis. For the PG student (and researchers too) to get the well depth understanding with further scope of improvements in the methods of forensic analysis.

2 Summary of the book

Chapter 1 This chapter starts with introduction about what is forensic as well as why this book named by forensic computing but not "computer forensic". It is well defined the origin of this from their postgraduate course called *forensic computing foundation course (FCFC).* Finally this discussion ends with well structured organization of book as discussed in last section.

Chapter 2 I suggests the readers to read this chapter if they are not familiarize with forensic terms. In our daily life, we are using devices like laptop, PC, PDA, tablet, mobile and so on. This chapter focuses on the type of information that is used by these devices, like humans use *English* as communication. When we get information from any devices than it may be not in human readable form, thus this chapter will help to understand the basics of communication language used between them. This chapter also explains the addressing modes (little and big-endian), various systems like binary (0-1), decimal (0-9), hex (0-F) and so on. Afterward, it discusses the various file formats like txt,rtf,gif,png, jpg and so on. Using the naive text editor, the authors have nicely shown the corresponding hex value and how it changed in the respective file formats. It is nice to see that authors have given productive exercise at the end of chapter to test and improve the grasping of readers.

Chapter 3 In almost all chapters, the authors nicely started whats covered in previous chapter, whats is in this chapter and whats next in upcoming chapter. After getting depth of different file systems and communication systems, in this chapter, the authors have examined the memory, processor, address and data bus, instructions and software in this digital world. It start with, what is bus and how it used to carry information from one place to another. Afterward, analysis of instruction like fetch, update and so on are discussed. In general we may write like A=B+C, but in computer it converts in instruction and than into binary string. It is admirable that authors have started from vary basic like fetch instruction and lead to the evolution of software and how it worked in the computer. Finally, this black box model lead to the today's computer system.

Chapter 4 After developing the black box model of computer, this chapter deals with different peripherals like motherboard, socket, processor, expansion card, hard disk and so on. It is nice to see having photographic description of each of this component. As we may have seen (and touch too) this components but not knows the internals of it. This chapter will surely help to fill this gaps.

Chapter 5 After getting viewpoint of different component of computer, this chapter discusses the important component of forensic analysis called hard disk. This is the device which stores the data in permanent form and thus very helpful in forensic analysis. This chapter start with brief history of hard disk and lead to five main issue which important for forensic analysis. Afterward, it discusses this five issues in depth. This is one of the plus point of this book to discusses only analysis which is useful for forensic experts. This analysis start with physical construction of the disk including motor, rotor, sector etc. Then it continues with different encoding methods to store this data into floppy or hard-disk. One can see that this chapter is important in this book as it covers more than 100 pages which is about 1/4 of the entire book.

After discussing methods for floppy disk, this chapter focus on the main course called hard disk drive, It explains the encoding methods, interfaces, formatting process etc. in it. As today's hard disk is on SATA cable, this chapter has nicely covered the problems in previous interfaces and how it lead to the SATA interfaces. From the viewpoint of processor, the hard disk is slower in terms of data transfer thus one of researcher's goal is to improve the transfer speed for better performance, time utilization etc. Afterward, it discusses the boot sequence and where it stored in hard disk. It also explains the master boot record and partitions (logical in nature).Finally it discusses the different file system including FAT and the associated directories and file structures. It ends with the RAID architecture which is used in the hard disk.

Chapter 6 After getting depths of geometry of hard disk and FAT system. This chapter focuses on the today's file system called NTFS (New Technology File System). After evolving of networks and thus internet , there is a need of file system which is more friendly to users for networking and at the same time more secure and structured too. This lead to the evolution of NTFS by the Microsoft after getting concepts and idea from HPFS project (joint venture of Microsoft and IBM). This chapter discusses the meta-data information for files like log, volume, boot etc. In this file system, many attributes like (name, resident,unnamed,non-residential, etc.) is attached with file. Based on it this chapter divided into sub chapters and shows the in depth analysis (with example) for each of the scenario

Chapter 7 After getting depths of hardware in the computer, this chapter discusses the steps that is required during forensic investigation. it discusses the steps during pre-search, pre-seizure. live seizure, shutdown of servers and so on. In crisp, this chapter discusses the step-by-step procedure of handling the situation during forensic analysis. The final section discusses about the copying and imaging. Imaging is useful for prove of any non-alteration with seized data while copy is fast (in time) but makes alteration in data's history.

Chapter 8 After getting the knowledge of step-by-step procedure for forensic investigation in different situation, this chapter discusses the real time analysis of PDA and other resources constrained devices. This chapter nicely covered the various software for palm OS devices and shows the ways to retrieve password and other useful information data from it.

Chapter 9 Int this final chapter, the authors had discussed the advancement in technology and thus lead to a more challenging jobs for forensic experts like today's companies using hiding technology to hide files/folders, encryption technology to protest from unauthorized persons and so on. Also with bigger and bigger size hard disk, this task is more time consuming and require more research efforts from forensic experts.

3 Comments and Recommendations

With the increasing involvement of digital technology in our daily life, it seems that soon we become dependent on devices like mobile, laptop, tablet and so on. Attacker can use these devices for their malafide intentions on the victims. Forensic computing is the technology suing which we can analyzed the data and find the attacker. I likes about this book is to considering graphical way of explanation for various peripherals and analysis. Also, in-depth discussion of some tools by which one can do such kind of analysis as it also handful for the students and the researchers. This book is the bridge for students to learn about what is forensic computing and how to use it using various methods, thus from study to the research. One advancement in this book that I suggest is to add the further findings section in each chapter which specially used by researchers for motivation or guide the further scope in that field. As digital information security and thus the forensic analysis is in-demand topic in today's world.

On an average, this book gives the undergraduate students (of pre-final year), postgraduate students, researchers, scientists and so on to motivate and also to study further in the forensic world and how to use it to capture and stop malicious intentions. Surely, I will not only suggest this book as first hand book in forensic computing for UG, PG and the researchers, but to offer courses like this in UG and PG level. There will be plenty of job choices in this field in recent years.

The reviewer is a faculty at Department of Computer Engineering, MEFGI, India.