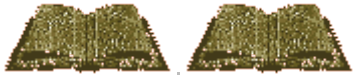
ANIL AGGRAWAL'S
Internet Journal of
Forensic Medicine and Toxicology
The world's first online journal devoted entirely to forensic medicine and toxicology · Published 1 January and 1 July

VOL. 3, NO. 2
Downloaded from www.anilaggrawal.com · ISSN 0972-8074 (Online) · https://www.anilaggrawal.com/ij/vol_003_no_002/reviews/tb/page007.html

# Book Reviews: Technical Books Section



**OTHER REVIEWS IN THIS ISSUE**
[Technical Books Section] Pages: |1| 2| 3| 4| 5| 6| 7| 8| 9| 10| 11| 12| 13| 14| 15| 16| 17| 18| 19| 20|
[Popular Books Section] Pages: |1| 2| 3| 4| 5| 6|

[Books on CD/Audio Tapes] Pages: |1|

[Software/Multimedia] Pages: |1|

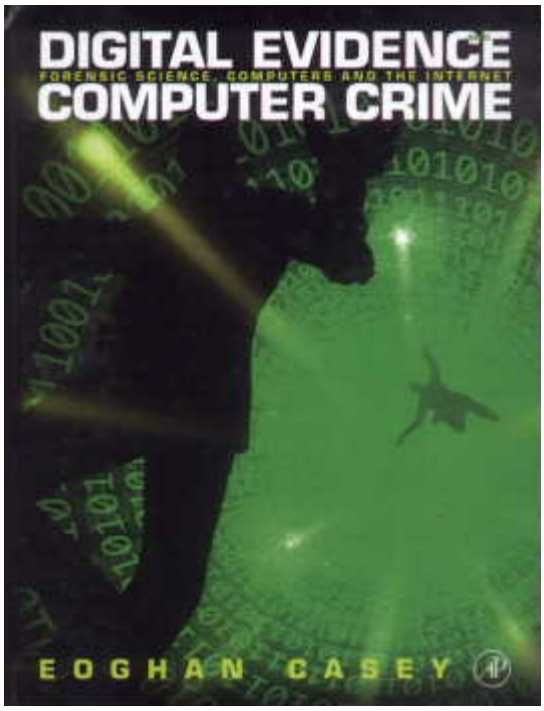
[Online Courses] Pages: |1|

**REVIEWS IN THE PREVIOUS ISSUE | NEXT ISSUE**

## INVESTIGATING COMPUTER CRIME

Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, (with Multimedia CD) 1st Edition (third printing 2001), *by* Eoghan Casey. Hard Bound, 7.5" x 10". Academic Press, Harcourt Place, 32 Jamestown Road, London NW1 7BY, UK. xvi + 279 pages, ISBN 0-12-162885-X. Price $69.95

**Click cover to buy from amazon**




Last year (2001) two devastating acts of terrorism took place - the September 11 attack on the World Trade Centre and the December 13 attack on the Indian Parliament. It is suspected that in both, computers played a vital part. It is believed that the culprits of the September 11 attack used steganography to transmit messages. Steganography is the method of hiding text or even programs inside pictures.

View this book on Amazon

After the December 13 attack, a laptop was recovered from some of the arrested militants, and it proved a goldmine of information regarding their links with their parent terrorist organizations. The laptops also revealed the details of how the attack was to be executed.

Recent years have seen the phenomenal rise of computer use and the internet. So much so that even criminals have begun using them for their nefarious activities. Using computers and internet for perpetration of crime has given rise to a new word - cybercrime.

**Table of Contents**


| S.no. | Topic | page |
|---|---|---|
| 1 | Introduction to digital evidence | 1 |
| 2 | The language of cybercrime | 15 |
| 3 | *Modus Operandi*, motive and technology | 25 |
| 4 | Applying forensic science to computers | 41 |
| 5 | Digital evidence on computer networks | 75 |
| 6 | Digital evidence on the internet | 99 |
| 7 | Digital evidence at the transport and network layers | 121 |
| 8 | | 145 |

| S.no. | Topic | page |
|---|---|---|
| | **Digital evidence on the data-link and physical layers** | |
| **9** | **Using digital evidence and behavioral evidence analysis in an investigation** | **161** |
| **10** | **Computer Crackers** | **171** |
| **11** | **Cyberstalking** | **187** |
| **12** | **Digital evidence as alibi** | **199** |
| **13** | **Laws, jurisdiction, search and seizure** | **207** |
| **14** | **Thoughts for the future** | **223** |
| **Appendix 1** | **Summary of resources** | **231** |


If the investigating agencies recover their computers and laptops, can they unearth information about their plans, their accomplices, their resources, their addresses, other contact information and so on? Fortunately it can be done, if one knows how to wade through the zillions of files on the computer's hard disk. Investigators have to do, what me may call a "post-mortem on their computers" to get the requisite information. How do we unearth this "hidden information" from criminals' computers? How can we prove in a court of law that their wicked plans were indeed hatched on their computers and with the help of the internet?

The book under review attempts to explain answers to questions like these. This new branch has variously been called forensic computing, cyberforensics or computer forensics.

One may imagine that one has to be "computer savvy" to be able to understand this book. But this is not necessarily true. The book starts from the basics. Even a novice can follow the book, if he begins from the beginning. An expert however may wish to leave out some of the introductory text in the beginning.

I thoroughly enjoyed reading this book, and I am sure you will too. The book comes with a CD, with 7 cases on it, which are roughly based on actual cases. The cases included in this CD are (i) Email rape (ii) Internet murder (iii) IRC child pornography (iv) Hit and Run alibi (v) Computer intrusion (vi) Web graffiti and (vii) boastful cracker. You can spend hours solving these cases, and in the process will gain useful insights in computer forensics.

...The exercises [on the accompanying CD] are pure fun. And by the time you are through with them, you would know a lot about computer forensics. The book will provide all necessary backup information in case you need to solve any case. I would very highly recommend this book to all those professionals who want to venture into the new and exciting branch of computer forensics. This book is good value for money, and should adorn the bookshelves of all computer experts, especially those who are in computer forensics...

To give you an idea of what I am talking about, let us talk about the first case - that of Email rape. As we click on this case, we are shown a small movie clip with a voice in the background explaining the problem. Susan Langer, a 20 year old college student was raped in Central park by a man she

met on the internet. The only clue was an Email message which that mysterious man sent her with detailed directions where to meet him. Our mission is to find the sender of the message, and of course we have access to Susan Langer's computer from where the message was presumably retrieved.

Well, what do you learn from solving this case? Five things at least, and here they are (i) How to find the suspect's address from the Email header (ii) How to read your own Email headers (iii) How to obtain information about viewed web pages (iv) How to obtain a more complete list of web pages and (v) How to search swap space for Email.

Or consider the case of "Boastful cracker" in which a person broke into a corporation (the author calls it Corporation X) and stole a valuable file called "tradesecrets". He also destroyed all of the digital evidence on the computer, except for an account that he created called "ezrobber". Our mission is to catch the thief. Solving this puzzle explains three more concepts. These are (i) How to search for an individual on IRC (ii) How to determine a person's IP address on IRC and (iii) How to find the stolen file without seeing its contents.

The exercises are pure fun. And by the time you are through with them, you would know a lot about computer forensics. The book will provide all necessary backup information in case you need to solve any case.

I would very highly recommend this book to all those professionals who want to venture into the new and exciting branch of computer forensics. This book is good value for money, and should adorn the bookshelves of all computer experts, especially those who are in computer forensics.

To know more about this book, and about computer forensics in general, the linked page (career).

Order *Academic Press* Books by clicking here.

Request a PDF file of this review by clicking here. (If your screen resolution can not be increased, or if printing this page is giving you problems like overlapping of graphics and/or tables etc, you can take a proper printout from a pdf file. You will need an Acrobat Reader though. You can also create a pdf file yourself by clicking here.)