



## Computer Forensics: Computer Crime Scene Investigation

By John Vacca

Firewall/Laxmi Publications (P) Ltd., New Delhi, 2015. N.A. Condition: New. First. 731pp.



**READ ONLINE**  
[ 4.22 MB ]

**DOWNLOAD**



### Reviews

*A must buy book if you need to adding benefit. It really is writer in easy terms instead of difficult to understand. I found out this ebook from my dad and i advised this publication to find out.*

-- **Prof. Elton Gibson I**

*I just began reading this pdf. It is actually writer in straightforward words instead of hard to understand. Once you begin to read the book, it is extremely difficult to leave it before concluding.*

-- **Jensen Bins**

Documentation of a crime scene creates a record for the investigation. It is important to accurately record the location of the scene; the scene itself; the state, power status, and condition of computers, storage media, wireless network devices, mobile phones, smart phones, PDAs, and other data storage devices; Internet and network access; and other electronic devices. The first responder should be aware that not all digital evidence may be in close proximity to the computer or other devices. Record any network and wireless access points that may be present and capable of linking computers and other devices to each other and the Internet. The existence of network and wireless access points may indicate that additional evidence exists beyond the initial scene. This article explains Computer Forensics and Digital Investigation Resources. Learn about digital analysis tools for computers, tablets and mobile devices. Computer forensics is a branch of digital forensic science that combines the elements of law and computer science. It involves collecting and analyzing data and information obtained from computer systems, networks, wireless networks, and communications. In addition, it involves data stored in various mediums such as hard drives, storage drives, thumb drives, CD-ROMs and even archaic floppy disks. Computer Crime Investigation Books. If you would like to learn more about the tools and techniques used by the experts, start with one of the following books. Computer Forensics For Dummies. View on Amazon.

Investigating a crime scene is not an easy job. It requires years of study to learn how to deal with hard cases, and most importantly, get those cases resolved. This applies not only to real-world crime scenes, but also to those in the digital world. Search Blog. —. Cybercrime investigators must be experts in computer science, understanding not only software, file systems and operating systems, but also how networks and hardware work. Known as OCFA, Open Computer Forensics Architecture is a forensic analysis framework written by the Dutch National Police Agency. They developed this software in pursuing the main goal of speeding up their digital crime investigations, allowing researchers to access data from a unified and UX-friendly interface. This article explains Computer Forensics and Digital Investigation Resources. Learn about digital analysis tools for computers, tablets and mobile devices. Computer forensics is a branch of digital forensic science that combines the elements of law and computer science. It involves collecting and analyzing data and information obtained from computer systems, networks, wireless networks, and communications. In addition, it involves data stored in various mediums such as hard drives, storage drives, thumb drives, CD-ROMs and even archaic floppy disks. Computer Crime Investigation Books. If you would like to learn more about the tools and techniques used by the experts, start with one of the following books. Computer Forensics For Dummies. View on Amazon.