View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Embry-Riddle Aeronautical University

Publications

1-2002

Computer Forensics: The Issues and Current Books in the Field

Gary C. Kessler
Champlain College - Burlington, kessleg1@erau.edu

Michael Schirling

Follow this and additional works at: https://commons.erau.edu/publication

 Part of the Digital Communications and Networking Commons

Scholarly Commons Citation

Kessler, G. C., & Schirling, M. (2002). Computer Forensics: The Issues and Current Books in the Field. , (). Retrieved from https://commons.erau.edu/publication/426

This Review is brought to you for free and open access by Scholarly Commons. It has been accepted for inclusion in Publications by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

Computer Forensics: The Issues and Current Books in the Field

Gary C. Kessler
Michael Schirling
January 2002

An edited version of this paper appeared with the title "Cracking the Books, Cracking the Case: A Review of Computer Forensics Texts" in the April 2002 issue of *Information Security Magazine* (www.infosecuritymag.com). **Copyright © 2002. All rights reserved.**

In June 2000, when the home of alleged serial killer John Robinson was searched, five computers were collected as evidence. Robinson used the Internet to find victims and persuade them into meeting him, at which time he allegedly sexually assaulted some and killed others. More recently, several hard drives were seized from the home of FBI spy Robert Hanssen. In addition to searching private government computer systems to ensure that he was not under investigation, Hanssen hid and encrypted data on floppy disks that he allegedly passed to the KGB, and used handheld devices to communicate securely with his collaborators.

While executing a warrant to search the basement office/bedroom of a suspected double-murderer, police found a computer along with several peripheral devices. Upon inspection, they found that the computer was on a network and it was subsequently discovered that the network included a computer upstairs in the same structure and a third computer in an adjacent structure. This computer was in hibernation mode, so that police investigators had to carefully power down the suspect's machine. After ascertaining that all three computers had open file and print shares, additional search warrants were obtained, as was consent from the other computers' owners for an analysis of those computers. The original thrust of the search was to find e-mails between the victims and the suspect to establish a motive in the murder case. During this examination, investigators found suspiciously named folders and files on one of the other networked computers, such as LOLITA and BOYS2.JPG; upon examination of these and other files, they discovered a collection of approximately 10,000 child pornographic images and video clips. Upon being presented with this evidence, the suspect told investigators where he had gotten the images and even asked if it was possible to delete these files from his computer. The investigators had to provide affidavits and testimony, demonstrating that the e-mail and pornographic files really came from these computers and could be tied to the suspect, and that the handling of the evidence was consistent with all legal requirements.

Those two scenarios, described in more detail in Eoghan Casey's computer forensics text, are less than the tip of the iceberg of how computers and crime today often go hand-in-hand. Consider also these examples

- Local and federal law enforcement officers were somewhat surprised to find evidence of attempts at online fraud along side collections of child pornography as they executed a search warrant at the home of a self-described heroin addict in rural Vermont, while looking for evidence in an armed bank robbery.

- The exchange of child pornography via traditional mail was almost entirely wiped out in the last decade by the vigilance of postal service inspectors. Internet e-mail and the World Wide Web have given trafficking in child pornography new life by providing almost instantaneous access to these images and a nearly infinite number of Web-based repositories.

- People — mostly men — seeking underage and other vulnerable males and females for illicit sexual activity used to be limited to the geographic area in which they lived or traveled. With Internet chat rooms and e-mail, trolling for potential victims has an almost unlimited population and geographic scope.

- Illegal gambling generally requires a bookie or other intermediary with whom to place bets, and the operation often operates outside of the boundaries of the country of the person placing the bet. Online Web-based virtual casinos make such gambling quick, simple, and obviates the need for a person in the middle. But it is still illegal — and a one trillion dollar industry around the world.

From preferential sex offenders to disgruntled corporate insiders, street level con men to members of organized crime, well-respected businessmen to clergy, people you would never have suspected of high technology crime are being convicted regularly. Since the early 1990s, law enforcement agencies at every level have become increasingly aware that the threats they face as they endeavor to protect the public come not only from the dark alleys and cold basements in which criminals have historically operated, but from the new landscape of computers and the Internet that is so much a part of the way we live today.

Dramatic growth of the Internet and sales of personal computers, migration from tapes to compact discs (CDs) to digital versatile discs (DVDs), the Walkman to the MP3 player, and the Polaroid camera to high resolution digital imagery, has changed lives at a pace never before seen. Likewise, crime and mischief have evolved from days past when the threats were from a few highly motivated and well "educated" hackers attacking our bulletin board systems to today where innumerable hacker, crackers, and script kiddies utilizing highly automated, easy to use utilities seize control of systems remotely, alter Web sites, and send viruses and worms worldwide with surprising precision. Additionally, offenders seeking to exploit our most valuable and precious resource, children, have found new ways to exploit emerging technology to their own benefit.

Among the most prevalent challenges facing law enforcement as we enter the 21st century is education and training to respond to computer and Internet crimes, and the emerging field known as *computer forensics*. *Forensics* is the use of science to investigate and establish facts in criminal or civil courts of law, so that computer forensics is squarely a branch of law enforcement just as forensic medicine. But forensic computing also includes the activities that many information security professionals do every day in managing corporate IT resources, protecting servers and computers, and tracking intruders on their networks.

Computer crime investigation is a multidisciplinary profession and almost no one today has been trained purely as a *computer forensic analyst*. Most police officers receive traditional training in legal issues, law enforcement procedures, and investigative techniques, so that those who get into computer forensics do so as their criminal investigation background and an interest in computers combine as the need emerges in their community. Most independent computer investigators, on the other hand, are either former police officers or computer professionals who have learned something about the law or have been called upon as law enforcement or other participants in the legal system require technical assistance. Forensic scientists and technicians trained in the analysis of digital media now play a critical role in law enforcement and corporate investigations. All of these professionals need to know about computer and network technology, analysis tools, and the law, and subsequently present what they have found so that a judge and jury can understand how it relates the crime(s) alleged to have occurred.

Toward that end, investigators need professional reference guides and texts that cover the major points of computer forensics. In this article, we discuss some broad issues related to forensic computing and include a review of four texts on the subject:

- *Computer Forensics: Incident Response Essentials*, Warren G. Kruse II & Jay G. Heiser
- *Computer Forensics & Privacy*, Michael Caloyannides
- *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, edited by Albert J. Marcella Jr. & Robert S. Greenfield
- *Handbook of Computer Crime Investigation*, edited by Eoghan Casey

Forensics Procedures and Analysis Tools

Forensic analysis of a computer, whether for a criminal investigation or as part of a more general security incident response, requires that there be a set of well-defined procedures that comply with appropriate laws, organizational policies, and best industry practices that cover issues such as when (and how) to notify law enforcement and the physical seizure of the computer(s) to obtaining and protecting evidence and performing an orderly search of the system. It doesn't matter, really, whether the evidence gathering is for legal purposes or just to understand an incident so as to avoid it in the future; analysis requires tools and processes.

Computer forensics involves the "preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis," a point made specifically by Kruse & Heiser but echoed in all of the books. In addition, all of the books agree on some fundamentals of the analysis:

1. The analysis should be performed on a copy of the media and never, except under the most extraordinary circumstances, on the original.
2. The copy should be made in such a way as to not alter the original information in any way and the copy must be authenticated as an exact duplicate of the original.
3. The analysis process should not alter the information in any way.

This latter point is trickier than it might first appear. Consider that many operating systems, such as Linux and Windows 2000, maintain a number of timestamps associated with every file, including the last access date. Using ordinary operating system tools to examine the contents of files will probably cause the last-access date to be changed while specialized analysis tools can examine files without modifying this date. It is important to maintain the integrity of the original data so that you can be sure that the results of the analysis are legally and technically valid.

Troy Larson in Casey notes that the most well-publicized uses of forensics tools are for "finding hidden data, recovering long-forgotten deleted files or otherwise proving through bits and bytes that the adverse party is a liar and a cheat." Forensic computing, he goes on to say, also has a defensive side and that is to examine one's own systems when involved in a criminal or civil discovery process. The same tools and procedures that police use to prepare a prosecution can be used by security administrators and private investigators to defend themselves and their clients.

Regardless of the purpose of the analysis, then, forensic computing is as much art as it is science. There are a large number of tools that the analyst has available but the first thing is to determine what evidence is to be gathered based upon the activity that is being investigated. In a child pornography case, for example, the investigator will naturally be looking for JPEG, GIF, and other image files. Since users can easily change file extensions, however, simply looking for .jpeg and .gif file names is not sufficient; the contents of all files need to be examined. All non-text files contain a header within the file that identifies the type of contents and good forensics software can find files where the file type extension doesn't match the file header to cause a so-called *signature mismatch*.

The heart of the actual forensic analysis, of course, is examining the computer(s) and/or network, recovering all possible information, and reconstructing the activity related to the incident being investigated. One of the most well-known computer forensics tools is the Windows-based analysis software package EnCase, used to perform a thorough analysis of the contents of a system's hard drive. The relative coverage of this tool by the four books is somewhat indicative of the different books' coverage of tools, in general. Casey, for example, provides a detailed chapter on the use of EnCase, covering the entire process from media acquisition to analysis to reporting. The other three books discuss EnCase at a much higher level and show it to be one of several tools that can be used to examine the contents of media.

No single tool can perform all aspects of a computer forensics analysis and all of the books discuss other tools to aid the investigator:

- Create disk images
- Recover passwords
- Perform file access, modification, and creation time analysis
- Create file catalogs
- View system and application logs
- Determine the activity of users and/or applications on a system
- Recover "deleted" files and/or examine unallocated file space
- Obtain network information such as IP addresses and host names, network routes, and Web site information

The analyst must be familiar with the myriad of command line system utilities and specialized forensics tools so that they can prepare their own toolkit with which to perform an examination related to a specific incident.

The analyst's toolkit, though, is primarily reactive. There are additional tools that system and information security managers might employ to protect themselves from having a security incident and/or to simplify information gathering should an incident occur. These tools, primarily for defense rather than analysis and investigation, include anti-virus software, digital signature protection of critical system file, intrusion detection systems (IDS), firewalls, proxy servers, and desktop/network surveillance software.

There are also tools that end users might employ for defense of their own system, including anti-virus software, IDS, and firewalls. But end users might also deploy tools that make forensics difficult, such as file scrubbers that really do delete files and purge the browser cache, and encryption and steganography software that make the examination of file contents next to impossible without a crypto key. Corporate policies may or may not prohibit use of these tools on a corporate computing resource, but these anti-forensics tools are well known to criminals as well as benign users.

The coverage of the tools clearly distinguishes these books from each other. Kruse & Heiser and Caloyannides provide the best high-level discussions of the broad spectrum of tools that are available for analysis and defense, and both spend a major portion of their pages on this topic. Their descriptions give the reader a very good idea of what information can be obtained from a computer system, what tools and utilities are available, what tools would be useful for what tasks, and what the tool interface looks like. There are two primary differences in the how these two books cover this subject matter, however.

First, Kruse & Heiser is clearly written for the forensics investigator and takes that perspective. Caloyannides, on the other hand, is written from the perspective that users/administrators need to know how to protect themselves from a thief or other unscrupulous individual who might want to steal data from their computer, which includes an forensic investigation; the key word in the book title here really is "privacy." If Kruse & Heiser would write "when you delete a file it isn't really

removed from the disk, here's how to recover the data," for example, Caloyannides would write "when you delete a file it isn't really removed from the disk, here's how the data might be recovered, and here's how to really delete it." Caloyannides also covers many tools that might be used to invade one's privacy such as keystroke monitors and spyware; these are hardly forensics tools, per se, but well within the scope of the "privacy defense."

Second, Kruse & Heiser address tools that run on, and can analyze, both Windows and Unix/Linux systems, whereas Caloyannides only covers Windows software because, in the author's words, "...most computers today utilize Windows." This difference in operating system coverage is undoubtedly due to the different perspectives in approach, but lack of Unix coverage is a significant weakness.

Casey provides very detailed coverage about four specific forensics tools, spending a chapter on each (about 20% of the book) to provide in-depth descriptions on the functionality and use of these Windows and Unix/Linux tools. There is, however, very little broad coverage of other tools. While what the authors of these chapters offer is excellent information, there might be a nagging voice in the back of the reader's mind that these chapters are advertisements for the respective software since the authors are all directly affiliated with the vendor or developer of the software that they write about. The good news is that the choice of tools is excellent but the bad news is that the reader is not presented with a spectrum of choices.

Finally, Marcella & Greenfield's coverage of tools is sparse but that may not be surprising given its focus on forensics guidelines and policies. There is passing mention of different tools and the one chapter with the most information merely is a list of different software. This book, too, only discusses tools for Windows systems.

The absence of coverage of Unix/Linux tools is a major deficiency for the professional investigator. Given the large percentage of Internet servers that run Linux/Unix and are, therefore, the target of computer crimes, knowledge of tools with which to analyze these systems is essential.

Computer and Network Technology

To testify as an expert computer forensic analyst, one cannot merely be aware of the analysis tools; an individual must also be able to speak to the efficacy of the information gleaned from the tools (which is why only fingerprint and DNA specialists testify about these types of evidence). The investigator, then, needs to know the rudimentary basics about the computer's hardware and software, operating system, and underlying file system. The professional investigator needs to be comfortable with both Windows and Unix/Linux, including the command line interfaces of both; how each operating system moves, manipulates, and "deletes" files; and how to examine areas of the storage media beyond the file structure, such as unallocated space, file slack, and a host of other areas; in the words of Kruse & Heiser, "The operating system sees all, but it may not tell you about it." The analyst even needs to know how to properly power down and power up a computer, as well as how to disconnect peripherals and network connections, without destroying any of the information on the computer.

If an investigation involves more than a single computer, the analyst may also have to examine network activity along the suspected path of the attack. Since a large number of attacks and compromises occur via the Internet or local area network (LAN) rather than from a human at the local keyboard, investigators must understand:

- System logs, such as those from Unix or Windows Event Viewer, that describe operating system activity and events
- Application logs, such as those from the e-mail or Web server, for example, that describe events and activities related to specific applications

- Packet traces from sniffers such as tcpdump, showing the protocol traffic for host-to-host communication
- Intrusion detection system reports, such as those from Snort or BlackICE, that signal possible security events based upon network traffic patterns

Taken together, these logs and reports allow an analyst to get a full picture of an particular event, from the packets on the network to the specific events that took place on a given computer. To this end, investigators need to understand the rudiments of network protocols, particularly TCP/IP.

But that's not all. Casey and Seglem (in Casey) make the point that "[t]he proliferation of handheld devices connected to wireless networks has ushered in an era of pervasive computing." In this context, part of the difficulty is just obtaining all of the systems from which evidence can be obtained; it's not just the desktop or laptop computer system anymore. In addition, encryption software for everything from e-mail to PDAs is becoming routine, even for the casual user.

The networked environment not only involves communications protocols but the network operating system (NOS) environment, such as Linux/Unix, NetWare, and Windows NT/2000. If a computer on a network is to be examined, then the entire operating environment must be examined which includes the file and print server, e-mail server, remote access and communications server, etc. This is also important when examining multi-user systems. Windows 98, for example, supports multiple user logons but the operating system does nothing to protect one user from another on the local system, or even to enforce the use of usernames and passwords. Windows 2000 and Unix, on the other hand, can allow multiple users to share the same computer and protect one user's files from another user. This adds a new wrinkle to the analysis of the computer — if you are investigating User A, can you look at User B's files? And what if User A knows User B's password and is secretly storing files in another user's file space?

This plethora of technologies coming together adds to the complexity of any analysis. As Casey and Seglem observe, "[b]ecause every network is different, combining different technologies in unique ways, no single individual is equipped to deal with every situation." Indeed, the person being investigated doesn't need to be a computer and network whiz to hide information; the very complexity of the today's interconnected world may obfuscate things sufficiently, including making it very difficult to prove that an individual actually is responsible for a specific computer or network activity.

Casey provides the broadest coverage of computer and network technology, spending over 50% of the book in this space. Two chapters are devoted to the analysis of Windows and Unix systems, and this is supplemented by a chapter on the analysis of networks (with nice coverage of Unix and Windows log files, TCP/IP, packet sniffing, and intrusion detection) and another devoted to wireless network technologies. A final really interesting technology chapter covers embedded systems, which are basically computers that are part of some "appliance" and cannot be programmed by the user; these would include computers in office systems (e.g., telephones, fax machines, and copiers), communications systems (e.g., routers, hubs, and data and voice switches), transport systems (e.g., air traffic control, automobiles, and parking meters), household equipment (e.g., microwave ovens, smart house managers, and air conditioning systems), building management equipment (e.g., emergency systems, elevators, and secure ingress/egress systems), and a lot more. This chapter teaches the reader how to access embedded systems' read-only memory (ROM), random access memory (RAM), and processor. This is an important perspective; consider that a "secret" document on someone's computer might have been printed and, therefore, there might be traces of it on a file server, in the print queue on the print server, and within the memory of the printer itself.

While Casey provides a broad coverage of technology, it is not deep. Kruse & Heiser provides narrower and deeper coverage of computer technology, covering such topics as the basics of storage media, encryption and steganography, hiding data, and hostile code. The authors also cover Windows and Unix forensics in detail, providing four times as many pages on Unix as on Windows.

This provides an excellent introduction to these operating systems for the forensics investigator while assuming no prior knowledge of the operating systems and file systems. The book is much lighter on the network side, but does offer an introduction to the Internet and how one would track down intruders over the Internet. Casey provides excellent coverage of Windows and Unix, as well, but assumes that the reader has a better *a priori* understanding than Kruse & Heiser.

Caloyannides also provides detailed coverage of technology that will be of interest to the forensics analyst, covering similar topics as Kruse & Heiser. Much of the Windows discussion, however, is a long set of tips on how make Windows more secure and private — such as disabling the built-in microphone and not using virtual memory — but doesn't fully explain the underlying rationale for the steps that are recommended. Despite the absence of Unix, Caloyannides provides detailed and broad coverage of a variety of network and computer technologies. Consistent with the emphasis of his book, the strength of his presentation is with respect to privacy-related technologies, providing detailed coverage of how data is stored in the memory, registry, and hard drive of computers; modes of data insertion and self-protection, including keystroke logging software, telephone taps, spyware, and even Van Eck radiation; the application and detection of encryption and steganography software; and two long chapters about achieving and protecting on-line privacy covering such topics as the browser, e-mail, secure protocols, firewalls, and encryption.

Marcella & Greenfield provide the weakest coverage of technology, again not surprising given its focus. There are a number of chapters covering a variety of relevant topics; a chapter on Windows discusses how files are stored on the computer with particular emphasis on the Internet Explorer history buffer, cache, and temporary files, the registry, and Event Viewer, while the chapter on Internet abuse primarily describes browsers' cookies, bookmarks, and swap files. A chapter on the tools of the trade covers vulnerability detection tools such as nmap and nessus, protection tools such as BlackICE and swatch, and analysis tools such as The Coroners Toolkit (TCT) and Encase. Finally, there is a nice chapter on tracking and profiling network intrusions. Each of these chapters, however, are too short and spend insufficient time to really develop the topic; instead, the reader gets only a glimpse into these important topics.

Laws Related to Computer Forensics

Carol Stucki, in a chapter in Marcella & Greenfield, suggests that while most computer forensic investigations are not initially headed for court, analysts "should always conduct the investigation as if you are going to trial, just in case you have to." By following a rigorous law-based procedural framework, all of the evidence necessary for litigation will be available without having to backtrack and redo any work — and without having to explain to a judge why proper procedures weren't followed in the first place.

Investigators, particularly law enforcement officers and their agents, need to be aware of applicable local and federal legislation as they relate to obtaining warrants and subpoenas, conducting a legal search, determining what to seize, securing the evidentiary chain, obtaining affidavits and testimony, etc. In some cases, investigators may also need to be aware of applicable international laws and treaties. System and network administrators within private organizations also need to be aware of certain legal issues, including when to call for law enforcement assistance and their responsibilities once they do report a computer crime. Ignorance of the law or a lapse in protecting the evidence, in either criminal or civil matters, can make the entire analysis moot.

In addition to the 4th Amendment of the U.S. Constitution and the plethora of case law associated with it, such legislation as the Electronic Communications Privacy Act (ECPA) and the Privacy Protection Act (PPA) are critical to an investigator's understanding of the legal environment that the field of computer forensic exists within. Knowing when a subpoena, court order, or search warrant is needed to obtain specific evidence is critical to conducting an investigation. Without proper implementation of these legal tools, the collection of evidence is simply not possible in many cases. Investigators must be aware what types of evidence are available utilizing the varied means of legal

process. For example, subscriber information from an Internet service provider is available via a subpoena, while content, depending on where it is stored, whether it has been opened by the end user or not, or whether it is in the midst of transmission, requires varying court orders and search warrants. In addition to the federal legislation noted, each state may offer additional protections of privacy that state and local investigators must be aware of.

Marcella & Greenfield devote more than half their book to a collection of relevant laws and guidelines covering the search and seizure of computers, computer crime policies, U.S. national critical infrastructure protection, privacy issues, legal aspects of e-commerce, and international computer crime laws. Providing such a collection is the *raison d'etre* for this book which is specifically intended to be "not a text, but rather a field manual." Much of this material has been drafted by Federal Law Enforcement workgroups, which is important because these are the documents that will guide everyday forensics analysis of computers that might have been used as the tool of a criminal. Many of these documents, however, are available freely on the Internet so while it is very useful to have all of these documents available together in one place, it is unclear that an agency couldn't put much of this information together themselves; in fact, one chapter ("Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations") supercedes the contents of another chapter ("Federal Guidelines for Searching and Seizing Computers"). Since a large portion of this part of the book contains reprints of previously-published material, the book suffers from the absence of an author's voice giving expert analysis and guidance about the applicability of the legal material.

An additional twist on forensic investigation, of course, is that of privacy. Expectations of privacy and consent to search often go hand-in-hand. Most corporate policies explicitly state that company computers are owned by the company and are not to be used for personal purposes, limit corporate network connectivity to company-owned systems, and state that users of the corporate network should have no expectation of privacy with respect to their computer, files, or e-mail. This pretty much gives the investigator a free hand to examine any aspect of network hosts and servers without individual consent; all that is required is consent of appropriate corporate management.

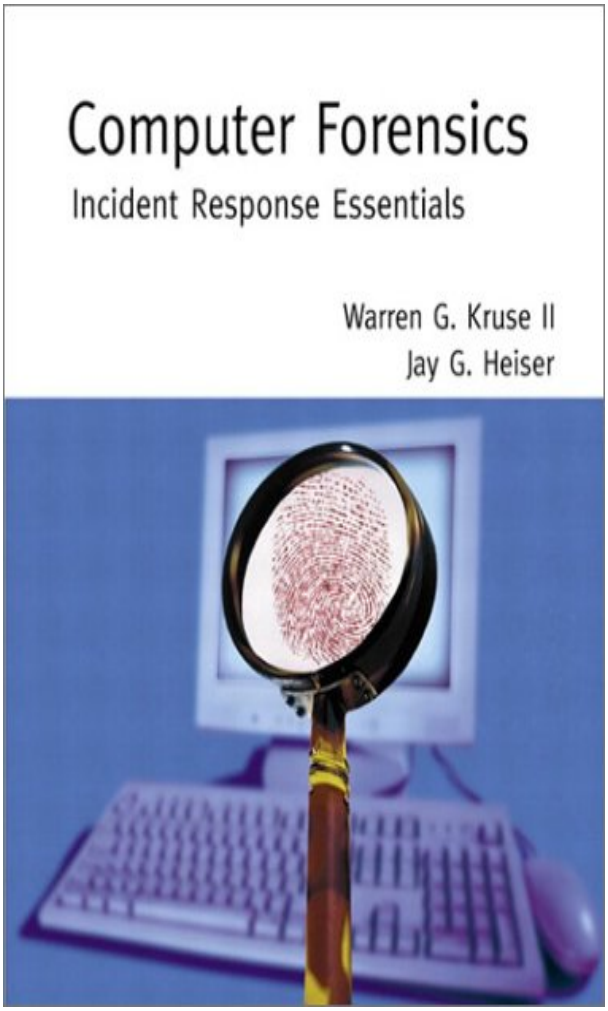
Kruse & Heiser and Caloyannides both provide a general overview of applicable laws that guide investigators. Rather than cite the individual laws, Kruse & Heiser provide a brief overview of the legal system for the non-law enforcement professional, including such issues as what happens after a law enforcement agency is notified, how search warrants are obtained and executed, how suspects are charged, the chain of custody of evidence, and tips for dealing with law enforcement agencies. In fact, the only specific laws cited are the U.S. wiretap statute (18 U.S.C. 10-25) and 18 U.S.C. 1029 Amended which, among other things, makes possession of computer passwords potentially illegal. By contrast, Caloyannides' coverage of legal issues provides detailed discussion about such topics as civil legal discovery, e-mail, criminal evidence collection and handling, federal guidelines for searching and seizing computers, and how businesses (and individuals) can protect themselves. Where relevant, specific laws are cited in the discussion, with particular attention to the Digital Millennium Copyright Act (DMCA) and Uniform Computer Information Transactions Act (UCITA). The book also covers some of the emerging privacy legislation, particularly the differences in views of data privacy in North America versus the European Union.

Casey takes a different approach by using case studies to present some of the legal aspects of forensic computing. A case study by McLean, for example, discusses how privacy extends to a premises without specific privacy policies, such as a private residence. As the case study demonstrates, a homeowner or parent may not be able to give permission for the search of every computer in a household; unless an investigator can prove that a computer is in common use by multiple users without any restrictions to access (real or implied) and that there is no real expectation of privacy by an individual, each respective owner must provide their consent for a search. In the absence of such permission, search warrants must be obtained. This is rather dry stuff to read statute by statute and, indeed, various specific laws are cited, but the case studies cover the

entire aspect of the analysis and the "case," and are, therefore, interesting and compelling reading. The coverage of legal aspects is slight compared even to Kruse & Heiser, although the coverage is the best at showing the specific application of relevant laws to the investigation, analysis, and prosecution.

The issue of protecting the privacy of files on your own computer is, of course, a very hot issue in the aftermath of the September 11 terrorist attacks in the U.S. One result of the "war on terrorism" has been what some critics suggest is an erosion of personal privacy and civil rights. In any case, criminals and some civil libertarians alike are adopting a posture of privacy at almost any cost and this is of increasing concern to forensics analysts.

The Books



Computer Forensics: Incident Response Essentials
Warren G. Kruse II & Jay G. Heiser
(Addison Wesley, published 2001)

Summary: This book is designed by the authors as an incident response handbook for investigators, and meets the needs of basic and intermediate level field officers, detectives, and information systems investigators well. The book focuses on the forensics, providing an overview of the different types of tools available in the field and supplies the reader with invaluable citations to other texts, articles, and Web sites where more detailed and advanced information can be obtained. (In the spirit of complete disclosure, we note that Jay Heiser is a columnist for *Information Security Magazine*.)

Pros:

- Very good coverage on basic computer and Internet technology
- Detailed coverage of Unix and Windows
- Excellent overview of the computer forensics analysis process and forensics tools

Cons:

- Only a high-level coverage on the laws and applying them

Computer Forensics & Privacy
Michael Caloyannides
(Artech House, published 2001)

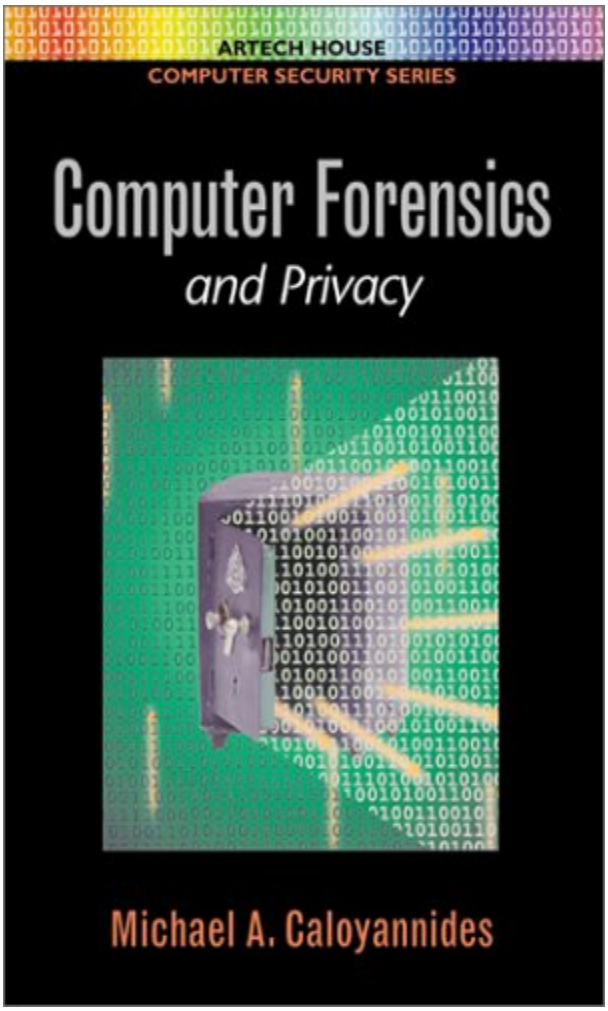
Summary: This books is written from an "information is your best defense" posture, designed primarily as a resource for users/administrators who want to protect themselves from someone who might want to analyze their computer, such as a data thief — or law enforcement officer. This is a good resource for the end user looking to safeguard their own system.

Pros:

- Good description of basic computer technology
- Good coverage of available forensics tools
- Excellent coverage of privacy invasion and other surveillance tools — and defenses

Cons:

- No coverage of Unix/Linux
- High-level discussion of legal aspects



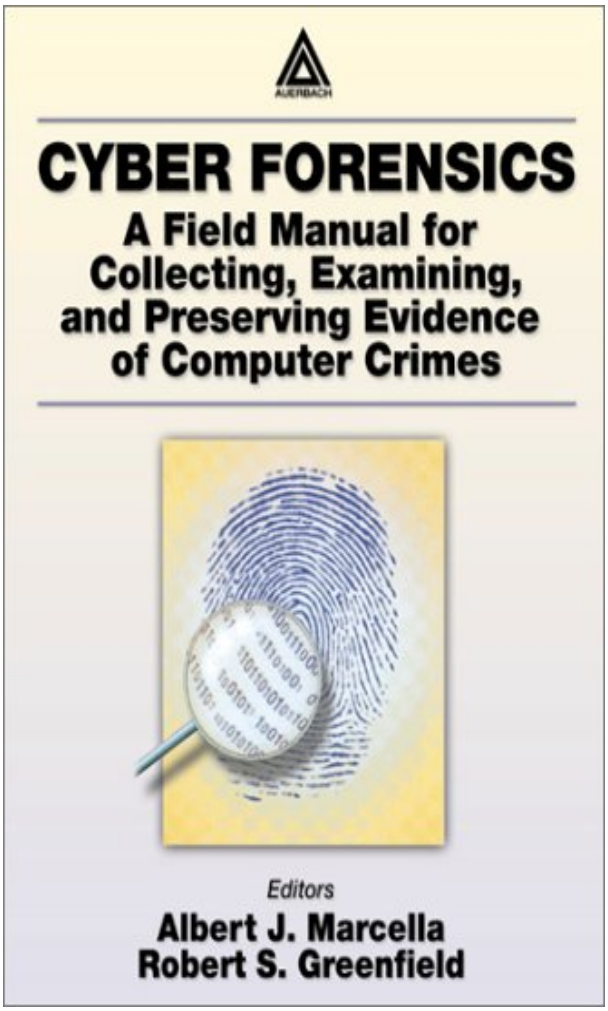
Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes
Edited by Albert J. Marcella Jr. & Robert S. Greenfield
(Auerbach, publication expected 2002)

Summary: This book is a field manual containing rules and guidelines governing the legal aspects of computer forensic investigations. (We should note that we were working with a prepublication draft of this book.)

Pros:

- Contains an excellent set of appropriate and relevant documents for the investigator

Cons:



- No coverage of Unix
- No analysis or advice in the applicability of the laws and guidelines
- Limited coverage of tools and technology

Handbook of Computer Crime Investigation: Forensics Tools and Technology
Edited by Eoghan Casey
(Academic Press, published 2002)

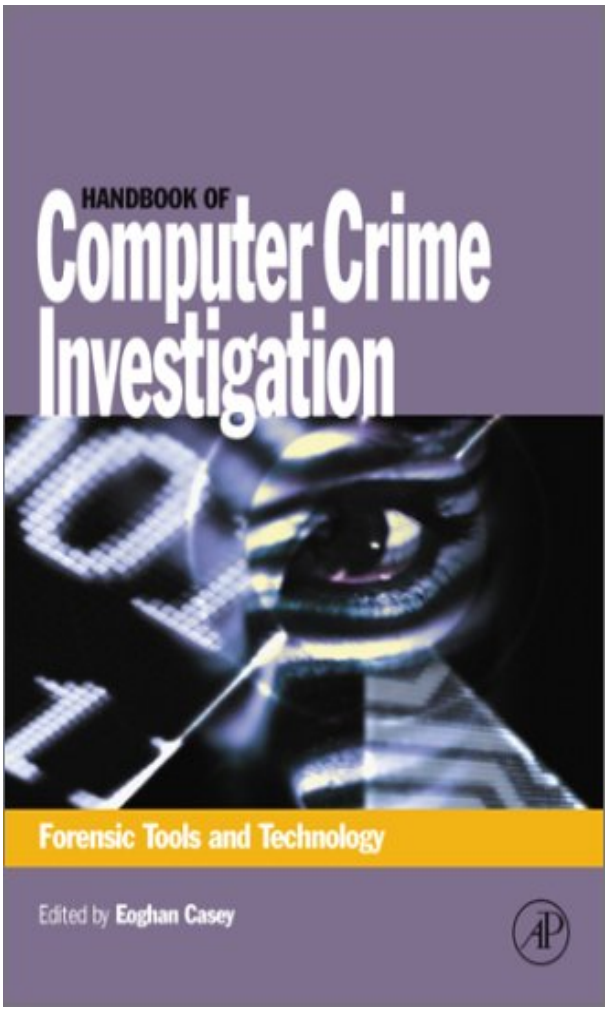
Summary: This book is a compilation of chapters by a number of authors and primarily focuses on available tools and procedures to analyze Windows and Unix systems, as well as providing information on other technical topics such as wireless networks, network protocols, and embedded systems. Detailed coverage on a few tools brings the reader further into the actual analysis of digital media utilizing specific tools and procedures than other books, but discusses relatively few tools. This book is very practical for the investigator, particularly the neophyte to computer and network technologies.

Pros:

- Describes Unix/Linux and Windows
- Case study approach to legal aspects
- Good coverage of computer and network technologies

Cons:

- Covers only a few forensics tools (although those are covered in detail)



Bottom-line: If you're trying to learn about the broad field of investigations and computer forensics, and want to concentrate on the computer aspects and tools, and step-by-step procedures relative to examining media, Kruse & Heiser is our favorite. Casey is also a very good choice and it provides a nice treatment of the law. If you are an end user or system administrator in a Windows environment looking to learn about how computer investigations — legal or illegal — might affect you, then Caloyannides provides a lot of useful information. If you need have the most relevant set of laws and guidelines at your fingertips, then Marcella & Greenfield is a good fit.

Report Card

	Caloyannides	Casey	Kruse & Heiser	Marcella & Greenfield
Technology				
Computer	B	B+	A	C+
Internet	B-	B+	B+	C+
Network	B	A	B	C
Tools				
Windows	A-	B	B	C+
Unix	—	B+	A-	—
Analysis process	B	A-	A	C+
Legal Aspects	B-	C+	B-	A

The laws Application of law	B-	B	B	B+
Overall Grade	B-	B+	B+	C+

ABOUT THE AUTHORS: Gary C. Kessler is an Associate Professor and program director of the Computer Networking major at Champlain College in Burlington, Vermont, and an independent consultant and writer. His e-mail address is *kumquat@sover.net*. Michael Schirling is a lieutenant on the Burlington Police Department, directs the Vermont Internet Crimes Against Children Task Force, and is an adjunct instructor at Champlain College. His e-mail address is *mschirli@dps.state.vt.us*.