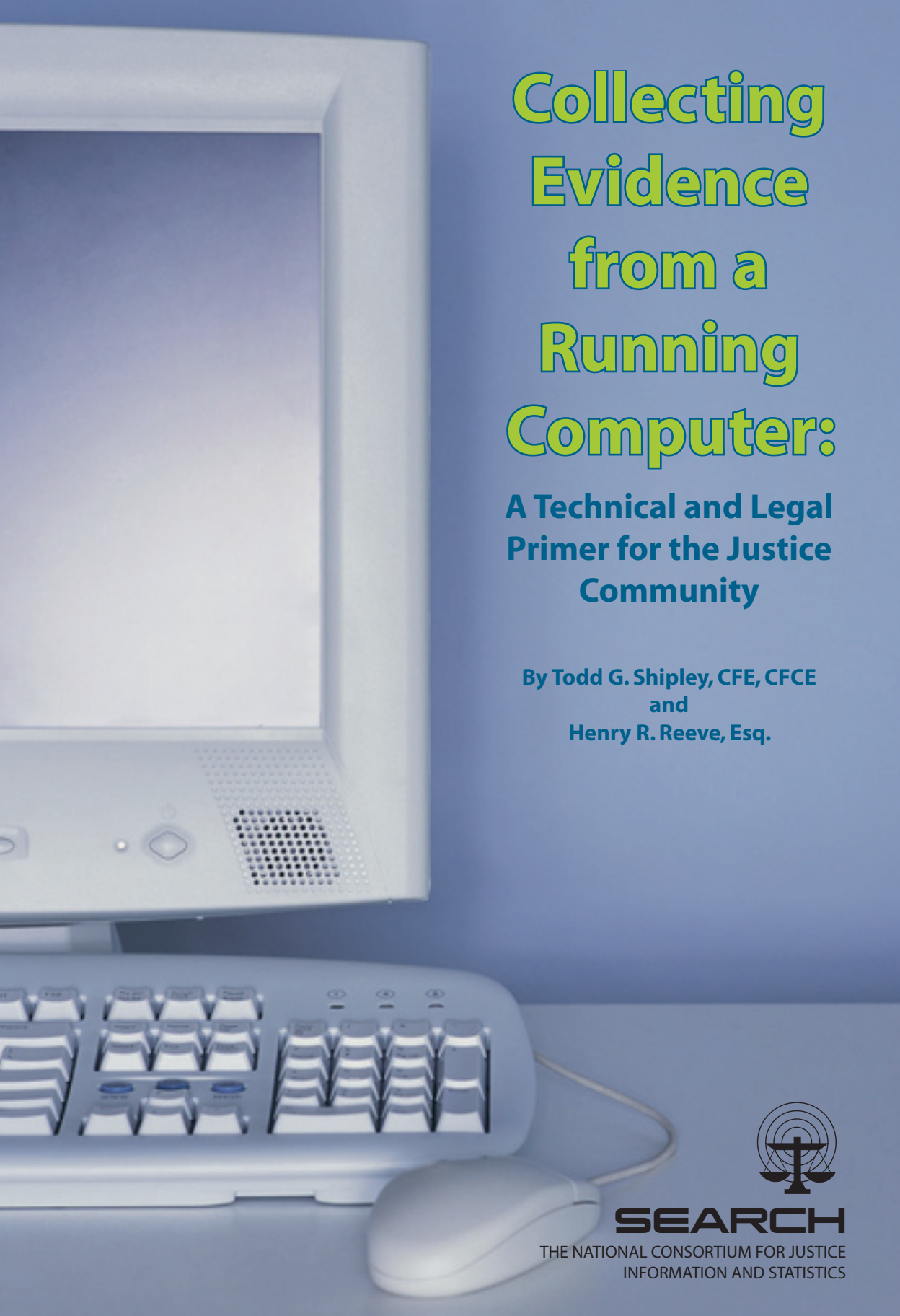


Collecting Evidence from a Running Computer:

A Technical and Legal Primer for the Justice Community

By Todd G. Shipley, CFE, CFCE
and
Henry R. Reeve, Esq.

SEARCH
THE NATIONAL CONSORTIUM FOR JUSTICE
INFORMATION AND STATISTICS

This report was prepared by SEARCH, The National Consortium for Justice Information and Statistics, Francis X. Aumand III, Chairman, and Ronald P. Hawley, Executive Director. This report was produced as a product of a project funded by the Office of Juvenile Justice and Delinquency Prevention (OJJDP), Office of Justice Programs, U.S. Department of Justice, under Cooperative Agreement No. 2005-MC-CX-K021, awarded to SEARCH Group, Incorporated, 7311 Greenhaven Drive, Suite 145, Sacramento, California 95831. Contents of this document do not necessarily reflect the views or policies of the OJJDP or the U.S. Department of Justice.

Acknowledgments

This primer was prepared by Todd G. Shipley, CFE, CFCE, Director of Systems Security and High Tech Crime Training for SEARCH, The National Consortium for Justice Information and Statistics, and Henry R. "Dick" Reeve, General Counsel and Deputy District Attorney, Denver, Colorado.

This paper was written under the direction of the Legal Committee of the Working Group of the Internet Crimes Against Children Task Forces.

SEARCH
THE NATIONAL CONSORTIUM FOR JUSTICE INFORMATION AND STATISTICS

7311 Greenhaven Drive, Suite 145
Sacramento, California 95831

Phone: (916) 392-2550

Fax: (916) 392-8440

www.search.org

Traditional Computer Search and Seizure Methodology

The traditional method for law enforcement when dealing with the search and seizure of computers at a crime scene is to simply unplug the computer and book it into the evidence facility. From there, the investigator requests that the computer be examined by a trained digital evidence examiner. The examiner then makes a "forensically sound" copy of the computer's hard drive(s)[1] and reviews the copy for evidence or contraband. Upon completion, the examiner reports the findings back to the investigator.

Traditionally, computer forensics has focused on researching, developing, and implementing proper techniques, tools, and methodologies to collect, store, and preserve sensitive data that is left on a system's hard drive(s).

***—First Responders Guide to Computer Forensics* (CERT Training and Education Handbook)**

This methodology was developed in the early days of computer forensics to ensure that the data was not changed in any way. It was developed in light of a number of considerations, including defending against later challenges in court that the investigator or examiner altered or created evidence found on the device. Since the early 1990s, this methodology has been central to law enforcement's response in handling computers found at a crime scene. As stated in a 2001 National Institute of Justice (NIJ) publication titled *Electronic Crime Scene Investigation: A Guide for First Responders*:

> "Each responder must understand the fragile nature of electronic evidence and the principles and procedures associated with its collection and preservation. Actions that have the

1 A forensically sound copy of a computer hard drive is one that is a bit-for-bit copy.

potential to alter, damage, or destroy original evidence may be closely scrutinized by the courts."[2]

A more recent NIJ document, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, further states:

> "When dealing with digital evidence, the following general forensic and procedural principles apply:
>
> - Actions taken to secure and collect digital evidence should not affect the integrity of that evidence.
> - Persons conducting an examination of digital evidence should be trained for that purpose.
> - Activity relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved, and available for review.
>
> Through all of this, the examiner should be cognizant of the need to conduct an accurate and impartial examination of the digital evidence."[3]

What this means simply is that law enforcement officers generally should not do anything that changes electronic evidence unless the circumstances of a particular situation justify something different. Inadvertent or accidental changing of evidence

could be caused by simply looking through files on a running computer or by booting up the computer to "look around" or play games on it. This strict methodology has historically provided for original evidence that, if relevant, is difficult for defense counsel to successfully challenge when it is introduced in court. However, we must remember that every crime scene is changed by the action of law enforcement being there. In fact, the NIJ research report *Crime Scene Investigation: A Guide for Law Enforcement* acknowledges that contamination occurs, and describes methods to limit that contamination.[4]

It is important to note that **potential evidence may be lost or destroyed if a running computer is encountered by law enforcement and seized as part of an investigation using the historical methodology described above**. (A "running computer" is defined as a computer that is already "powered on" when encountered at a crime scene.)

2 U.S. Department of Justice, Office of Justice Programs, National Institute of Justice (Washington, DC: July 2001) at page 1. The guide was written and approved by the Technical Working Group for Electronic Crime Scene Investigation.

3 U.S. Department of Justice, Office of Justice Programs, National Institute of Justice (Washington, DC: April 2004) at page 1.

4 U.S. Department of Justice, Office of Justice Programs, National Institute of Justice (Washington, DC: January 2000). This report was written and approved by the Technical Working Group on Crime Scene Investigation.

Volatile Data on Running Computers can Provide Crucial Evidence

Computers require that a certain amount of computer memory called "random access memory" (RAM)[5] be used by the operating system and its applications when the computer is in operation. The computer utilizes this RAM to write the current processes it is using as a form of a virtual clipboard. The information is there for immediate reference and use by the process. This type of data is called "volatile data" because it simply goes away and is irretrievable when the computer is off.[6] Volatile data stored in the RAM can contain information of interest to the investigator. This information could include, for example:

1. Running processes.
2. Executed console commands.
3. Passwords in clear text.
4. Unencrypted data.
5. Instant messages (IMs).
6. Internet Protocol (IP) addresses.
7. Trojan Horse(s).

There are other types of volatile data that could be considered evidence of interest to an investigation. This potentially exculpatory information may also simply "go away" when the system is turned off or loses power. This type of volatile data as potential evidence can also be collected from a running Microsoft Windows computer. Some of the additional data that can be collected may include:

1. Who is logged into the system.
2. Open ports and listening applications.
3. Lists of currently running processes.
4. Registry information.
5. System information.
6. Attached devices (this can be important if you have a wireless-attached device not obvious at the crime scene).

5 RAM is the most common type of memory found in computers. It is a type of memory that can be accessed randomly. RAM is synonymous with the term "main memory," which is memory available for applications to use.

6 The United States Computer Emergency Readiness Team (US-CERT) defines "volatile data" as "... any data that is stored in memory, or exists in transit, that will be lost when the computer loses power or is turned off."

Analyzing a Running Computer: A Different Approach to Evidence Collection

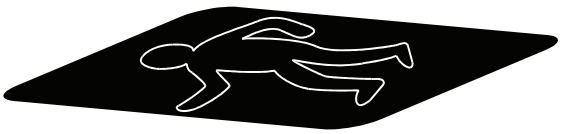
The traditional digital evidence collection methodology described earlier still holds true for many law enforcement applications. Ensuring the integrity of evidence is paramount to any investigation conducted by a law enforcement agency. Preserving digital evidence by collecting a system and conducting a forensic examination later will be the standard for many years to come. However, there are also exceptions to the rule.

There can be circumstances during an investigation involving a computer that can require the examination of a running system. Circumstances when this technique is of potential use are becoming more frequent. **The single greatest factor pushing law enforcement into this direction is the advancement of home networking technology**. The ability of the home and small office user to set up small wired or wireless networks has been simplified to the "plug-and-play" standard. Now it is more likely that in any investigative situation involving a computer, the investigator may find a small network.

Network crime scenes traditionally have been treated by investigators as a big STOP sign that says "call for help." However, the current ranks of trained computer forensics personnel are inadequate to support the ever-growing amount of digital evidence that should be collected at crime scenes. It is fairly common for investigators to wait months for their reports due to the resulting backlog. In many jurisdictions, such backlogs limit the support that forensics examiners can provide to field operations. Therefore, the ability of investigators to collect potential evidence from running computers at the crime scene has never been more critical. Providing investigators with new crime scene collection skills will be paramount in dealing with the workload and challenges presented by small networks.

Let's look at a scenario where evidence, if collected on-scene, can be critical to solving that crime:

Scenario



Investigators respond to a homicide on a street corner. The victim was shot once in the chest, and there are no witnesses. The victim is identified and a search is conducted of his residence in an attempt to determine a suspect or motive. A computer is found at his residence. The computer is already turned on and is running Windows XP. The investigators follow the traditional method of computer evidence collection by shutting down the system and collecting the computer. The computer is booked into evidence for review by a computer forensics examiner.

Had the investigators been trained in the collection of volatile evidence, they could have collected the RAM from the running system. Had they collected this evidence, they might have found instant message traffic between the victim and another individual detailing a drug deal. The IM traffic would have quickly led them to the suspect.

This scenario is based on a real case in which investigators did, in fact, collect the volatile evidence and identify a suspect through the IMs, thereby leading to his arrest. Had the investigators not recovered the IM traffic, they would have had little evidence to tie the suspect to the crime.

This type of scenario is becoming more common. Live system information can, in some cases, mean the difference between solving a crime and not. It can be the difference between proving someone's guilt or their innocence. The shift here is not a large technological leap; it is more one of philosophy and training. The traditional method of "Do Not Touch" the running machine leads to the potential of losing this kind of evidence. These methods have been commonly used in the investigation of intrusion attempts on larger networks for years. In chapter 9 of the book *Incident Response: Investigating Computer Crime*, the authors describe their view of the best process for collecting volatile data as evidence.[7] Most of the more current incident response texts offer a similar method for collecting RAM and volatile evidence.

Learning how to properly collect volatile evidence requires investigators to take additional training to supplement the basic computer seizure courses conducted nationally. However, with additional training in volatile evidence collection methods, an investigator can develop the skills necessary to collect evidence that traditionally may have been overlooked or lost. Again, it is important to understand that *volatile data will be lost forever if not collected while the computer is running*.

7 Kevin Mandia and Chris Prosise (Berkeley, CA: Osborne/McGraw-Hill, 2001).

A Methodology for the Law Enforcement Collection of Digital Evidence from a Running Computer

Presently, there are a number of different tools in use to collect volatile data.[8] Given how rapidly technology changes, any tools or methodologies described here today could be obsolete by tomorrow. What is offered here is a suggested practice for investigators to follow at the crime scene that allows volatile evidence to be collected in a manner consistent with principles of evidence preservation and collection and the law.

Some guidance on a possible methodology is provided in a CERT Training and Education handbook, *First Responders Guide to Computer Forensics*. It describes this six-step methodology for volatile data collection:[9]

Step 1: Incident Response Preparation.

Step 2: Incident Documentation.

Step 3: Policy Verification.

Step 4: Volatile Data Collection Strategy.

Step 5: Volatile Data Collection Setup.

Step 6: Volatile Data Collection Process.

These steps are designed to be used by an investigator to investigate intrusion cases common to larger networks. For purposes of this document, our focus is on Step 6.

Steps in the Volatile Data Collection Process

Step 6, Volatile Data Collection Process, involves the following five steps:

1. Collect uptime, date, time, and command history for the security incident.
2. As you execute each forensic tool or command, generate the date and time to establish an audit trail.
3. Begin a command history that will document all forensic collection activities.
4. Collect all types of volatile system and network information.

8 Some of the currently used tools include Helix, a bootable CD that is a collection of incident response tools, and "dd," a tool written by George Garner to capture RAM.

9 Richard Nolan, Colin O'Sullivan, Jake Branson, and Cal Waits, CMU/SEI-2005-HB-001 (Pittsburgh, PA: Carnegie-Mellon Software Engineering Institute, March 2005) at pp. 94–102.

5. End the forensic collection with date, time, and command history.

These basic steps provide general guidance regarding what to collect. Of importance to this discussion is the need to document the actions of the investigator. CERT suggests the use of audit trails as documentation. The CERT method also describes in general terms the types of volatile evidence to collect.

With the understanding that computer systems contain potential evidence that could be destroyed if traditional computer evidence collection methods are employed, investigators can use the following basic steps when collecting volatile evidence:

1. Maintain a log of all actions conducted on a running machine.
2. Photograph the screen of the running system to document its state.
3. Identify the operating system running on the suspect machine.
4. Note date and time, if shown on screen, and record with the current actual time.
5. Dump the RAM from the system to a removable storage device.
6. Check the system for the use of whole disk or file encryption.
7. Collect other volatile operating system data and save to a removable storage device.
8. Determine evidence seizure method (of hardware and any additional artifacts on the hard drive that may be determined to be of evidentiary value).
9. Complete a full report documenting all steps and actions taken.

These basic steps allow the on-scene investigator to collect data that was previously overlooked as unnecessary or simply lost out of ignorance. Open source and commercial tools are currently available that easily allow for this methodology to be followed on a running system. The RAM is dumped first to capture the greatest amount of evidence available. It must be noted that inserting any device into the running system (flash drive, removable drive, or CD) will make minor changes to the system, albeit very small changes. The proper use of these tools does not add evidence or contraband to the system. Running a program to dump the RAM requires that a very small amount of RAM be occupied by the tool to conduct the RAM dump. Inserting a removable drive into a USB port adds an entry to the Microsoft Registry. All of these changes have no effect on the overall state of the evidence and can be further documented at a later time by a traditional forensic examination. Some small changes are made during the process of using some of the available tools that require interaction with the Windows operating system. These changes however, occur to the operating system files only and do not fundamentally change the content of the data saved on the system.

Legal Considerations of Live Analysis and Collecting Evidence from a Running Computer: An Overview

Current practice in many jurisdictions utilize either—

- one search warrant that authorizes both the initial seizure of a computer and the subsequent forensic examination, or
- two search warrants in which the first warrant authorizes the initial seizure and the second (usually obtained at a later time) authorizes the forensic examination.

The on-scene live analysis described in this primer is of a limited nature and scope and should not require specific authorization in a warrant unless the additional time required for execution materially lengthens or broadens the execution of the warrant. The boundaries for this determination will be established by reference to local case law. To date, there is no reported appellate decision on this question; however, the authors submit that live analysis, when performed by properly trained personnel, usually does not add significant time to the warrant execution process and also should not broaden the scope of the search. Rather, the collection and preservation of volatile data should be viewed simply as a regular, integral component of the proper seizure of many computer systems. The constitutional need to be more particular in such circumstances seems a dubious argument.

If properly drafted, a search warrant should have at least the implied authority to conduct a live analysis, when circumstances merit. It is suggested that the warrant or its attachments contain the following language:

1. Electronically document and preserve the state of the computer network and electronic storage media, and
2. Conduct preview screening of the computer data storage media for contraband utilizing data recovery software.

The steps for live analysis, as described earlier, are merely designed to capture, preserve, and record evidence that may already be present at an electronic crime scene and which may be lost if not properly collected. A live analysis should be structured to be a directed effort, conducted in an efficient manner, by trained personnel. If conducted otherwise, the likelihood of other legal challenges being raised seems substantial.

A live analysis should be structured to be a directed effort, conducted in an efficient manner, by trained personnel. If conducted otherwise, the likelihood of other legal challenges being raised seems substantial.

In cases where no search warrant was needed or used (for example, where consent or exigent circumstances were present), the above legal considerations may not prove of relevance. In light of a recent decision in *Georgia v. Randolph*[10] by the United States Supreme Court on the question of consent, however, the ability to quickly and effectively conduct a live analysis may contribute to establishing probable cause prior to the time consent is revoked when the authority to conduct a full forensic examination might otherwise be lost.

The accuracy and reliability of any evidence collection process, as well as the various tools or utilities used in the collection, may be challenged by a criminal defendant. In order to best assure admissibility in court, law enforcement officers and prosecutors who use live system analysis in a case need to be prepared to establish the skills and knowledge of the investigator, as well as the validity of the tools used. Again, to date, there are no reported appellate opinions that address these issues.

In order to best assure admissibility in court, law enforcement officers and prosecutors who use live system analysis in a case need to be prepared to establish the skills and knowledge of the investigator, as well as the validity of the tools used.

As described in this primer, live analysis is directed at being used in a home or small office environment and not in a large commercial or corporate network setting. Further, this process does not contemplate the real-time capture of content of communications on a computer or network. The issues associated with corporate networks or the capture of content in real-time are outside of the scope of this document.

Conclusion

This document describes a methodology for the law enforcement collection of volatile data. The collection of this data can be of substantial use in the investigation of various criminal activities. The current legal restriction of this type of investigation has yet to be determined. What can be controlled by law enforcement is the proper implementation of a process by which we collect this evidence consistent with prevailing legal authority and generally accepted practice. Volatile data is evidence that can—and should—be collected at crime scenes. With training in proper collection techniques and an understanding of its value, this evidence can be successfully collected.

10 126 S.Ct. 1515 (2006)

References

Brown, Christopher L.T., *Computer Evidence Collection & Preservation* (Hingham, MA: Charles River Media, 2006). Available at http://www.delmarlearning.com/charlesriver/.

Carrier, Brian, *File System Forensic Analysis* (Boston, MA: Addison-Wesley Professional, 2005). Available at http://www.awprofessional.com/bookstore/product.asp?isbn=0321268172&rl=1.

Carvey, Harlan, *Windows Forensics and Incident Recovery* (Boston, MA: Addison-Wesley Professional, 2004). Available at http://www.awprofessional.com/bookstore/product.asp?isbn=0321200985&rl=1.

e-fense™, Inc., *Helix Live CD-ROM*. Available at http://www.e-fense.com/helix/.

Garner, George M. Jr., *Forensic Acquisition Utilities* (August 17, 2004). Available at http://users.erols.com/gmgarner/forensics/.

Jones, Keith J., Richard Bejtlich, and Curtis W. Rose, *Real Digital Forensics: Computer Security and Incident Response* (Boston, MA: Addison Wesley Professional, 2005). Available at http://www.awprofessional.com/bookstore/product.asp?isbn=0321240693&rl=1.

Kenneally, Erin E. and Christopher L.T. Brown, "Risk Sensitive Digital Evidence Collection," Volume 2, Issue 2 *Digital Investigation 101* (June 2005). Available at http://www.sciencedirect.com/science/journal/17422876 (fee applies).

Mandia, Kevin, and Chris Prosise, *Incident Response: Investigating Computer Crime* (Berkeley, CA: Osborne/McGraw Hill, 2001). Available at http://books.mcgraw-hill.com/getbook.php?isbn=0072194510&template=osborne.

Nolan, Richard, Colin O'Sullivan, Jake Branson, and Cal Waits, *First Responders Guide to Computer Forensics*, CERT Training and Education Handbook, CMU/SEI-2005-HB-001 (Pittsburgh, PA: Carnegie-Mellon Software Engineering Institute, March 2005). Available at http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

Remote-exploit.org, *Auditor Security Collection CD-ROM*. Available at http://www.remote-exploit.org/index.php/Auditor_main.

Technical Working Group for Electronic Crime Scene Investigation, *Electronic Crime Scene Investigation: A Guide for First Responders*, NIJ Guide series, NCJ 187736 (Washington, DC: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, July 2001). Available at http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm.

Technical Working Group on Crime Scene Investigation, *Crime Scene Investigation: A Guide for Law Enforcement*, Research Report series, NCJ 178280 (Washington, DC: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, January 2000). Available at http://www.ncjrs.gov/pdffiles1/nij/178280.pdf.

U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, NIJ Special Report series, NCJ 199408 (Washington, DC: April 2004). Available at http://www.ojp.usdoj.gov/nij/pubs-sum/199408.htm.

United States Computer Emergency Readiness Team (US-CERT), *Computer Forensics*, 2005. Available at http://www.us-cert.gov/reading_room/forensics.pdf.