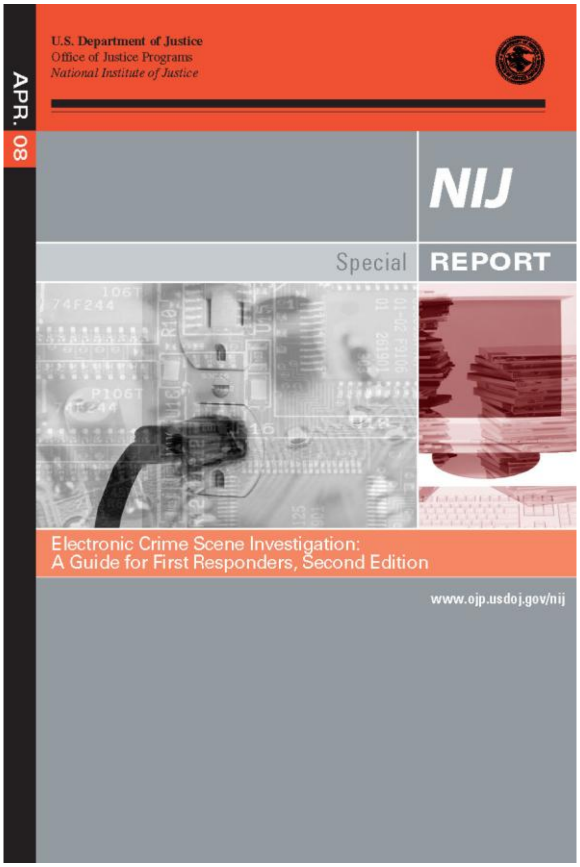
Electronic Crime Scene Investigation[1]

Reviewed by M. E. Kabay, PhD, CISSP-ISSMP
CTO & Program Director, MSIA / School of Graduate Studies
Associate Professor of Information Assurance / School of Business & Management
Norwich University, Northfield, Vermont


APR. 08
U.S. Department of Justice
Office of Justice Programs
National Institute of Justice
NIJ
Special
REPORT
Electronic Crime Scene Investigation:
A Guide for First Responders, Second Edition
www.ojp.usdoj.gov/nij

The *Electronic Crime Scene Investigation: A Guide for First Responders*, issued by the Technical Working Group for Electronic Crime Scene Investigation at the Office of Justice Programs, National Institute of Justice of the US Department of Justice has been issued in its second edition in April 2008.[2]

The free document, 74 pages long, is packed with valuable, practical information for everyone responsible for collecting evidence of a crime directed against computers and networks or mediated through such equipment.

- The introduction reviews the applicability of the instructions and advice and defines digital evidence for law enforcement and other investigators: "Digital evidence is information and data of value to an investigation that is stored on, received, or transmitted by an electronic device. This evidence is acquired when data or electronic devices are seized and secured for examination. The authors add that "Digital evidence
    - Is latent, like fingerprints or DNA evidence.
    - Crosses jurisdictional borders quickly and easily.
    - Is easily altered, damaged, or destroyed.
    - Can be time sensitive."
- Chapter 1 provides a brief overview of concepts and terminology applying to computers and networks. It includes updated photos of PCs and Apple computers, hard drives, removable media including concealed or disguised flash (thumb) drives and memory cards, and a reminder that devices such as mobile phones and personal digital assistants (PDAs) and music players can carry a great deal of evidence.

[1] This review was updated in January 2009

[2] DoJ (2001). *Electronic Crime Scene Investigation: A Guide for First Responders.* xi + 62. PDF & HTM versions available from < http://www.ojp.usdoj.gov/nij/pubs-sum/219941.htm >

- Chapter 2 describes investigative tools and equipment such as cameras, gloves, screwdrivers, pliers, plastic bags and so on – obvious for investigators but less so for information technology geeks.

- Chapter 3 discusses how to secure and evaluate the scene of a putative crime. The guide warns that in the initial phase of the investigation, it's important to "Ensure that the condition of any electronic device is not altered." In particular, "Leave a computer or electronic device off it is already turned off." The new edition also suggests using all available resources in the preliminary interviews, including details of computer applications, Internet connections and Service Providers, Web mail, instant-messaging accounts, and social networking accounts.

- Chapter 4 explains how to document the scene for use in possible prosecutions or cases under civil law. Photographs are useful in this phase of the data gathering. The authors remind investigators to be thorough: "All activity and processes on display screens should be fully documented." Furthermore, "Documentation of the scene should include the entire location, including the type, location, and position of computers, their components and peripheral equipment, and other electronic devices. The scene may expand to multiple locations; first responders should document all physical connections to and from the computers and other devices." Wireless connectivity is also an issue that should be investigated.

- Chapter 5 reviews evidence collection. In particular, the guide provides a step-by-step diagnostic procedure for deciding how to treat equipment that may or may not be powered on. The purpose of the procedures is to capture as much information as possible from the systems being seized, including photographs of volatile data on screens, in RAM and in swap files on disk.

- Chapter 6 gives instructions on safe packaging, transportation, and storage of evidence. It is critically important that a proper chain of custody be established and documented for evidence at all stages of handling.

- Chapter 7 and several appendices provide checklists of the types of evidence that are particularly useful in investigating different types of crimes. For example, in auction fraud, accounting data and address books are on the list whereas in child exploitation cases, chat logs are particularly valuable. Other types of crimes specifically addressed include computer intrusion, counterfeiting, homicide, domestic violence, threats, extortion, e-mail threats, stalking, gambling, identity theft, narcotics trafficking, online or economic fraud, prostitution, software piracy, telecommunications fraud, and terrorism.

This guide is written simply and clearly. It is a good resource for anyone who is writing policy and procedures on the collection and safe handling of evidence in computer crime investigations.