NIJ

APR. 08

# Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition

## Introduction



NCJ 219941

# Introduction

This guide is intended to assist State and local law enforcement and other first responders who may be responsible for preserving an electronic crime scene and for recognizing, collecting, and safeguarding digital evidence. It is not all inclusive but addresses situations encountered with electronic crime scenes and digital evidence. All crime scenes are unique and the judgment of the first responder, agency protocols, and prevailing technology should all be considered when implementing the information in this guide. First responders to electronic crime scenes should adjust their practices as circumstances—including level of experience, conditions, and available equipment—warrant. The circumstances of individual crime scenes and Federal, State, and local laws may dictate actions or a particular order of actions other than those described in this guide. First responders should be familiar with all the information in this guide and perform their duties and responsibilities as circumstances dictate.

When dealing with digital evidence, general forensic and procedural principles should be applied:

- The process of collecting, securing, and transporting digital evidence should not change the evidence.
- Digital evidence should be examined only by those trained specifically for that purpose.
- Everything done during the seizure, transportation, and storage of digital evidence should be fully documented, preserved, and available for review.

First responders must use caution when they seize electronic devices. Improperly accessing data stored on electronic devices may violate Federal laws, including the Electronic Communications Privacy Act of 1986 and the Privacy Protection Act of 1980. First responders may need to obtain additional legal authority before they proceed. They should consult the prosecuting attorney for the appropriate jurisdiction

to ensure that they have proper legal authority to seize the digital evidence at the scene.

In addition to the legal ramifications of improperly accessing data that is stored on a computer, first responders must understand that computer data and other digital evidence are fragile. Only properly trained personnel should attempt to examine and analyze digital evidence.

**NOTE:** Officer safety and the safety of others should remain the primary consideration of first responders. Nothing in this guide is intended to be, or should be construed as being, a higher priority than officer safety or the safety of others.

## Using This Guide


When the STOP sign is encountered in this guide, the first responder is advised to STOP, review the corresponding information, and proceed accordingly.


When the YIELD sign is encountered in this guide, the first responder is advised to review the corresponding information and proceed accordingly.

## Intended Audience for This Guide

- Anyone who may encounter a crime scene that might involve digital evidence.
- Everyone who processes a crime scene that includes digital evidence.
- Everyone who supervises personnel who process such crime scenes.
- Everyone who manages an organization that processes such crime scenes.

# What Is Digital Evidence?

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.

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.

**NOTE:** First responders should remember that digital evidence may also contain physical evidence such as DNA, fingerprints, or serology. Physical evidence should be preserved for appropriate examination.

## Handling Digital Evidence at the Scene

Precautions should be taken in the collection, preservation, and transportation of digital evidence. First responders may follow the steps listed below to guide their handling of digital evidence at an electronic crime scene:

- Recognize, identify, seize, and secure all digital evidence at the scene.
- Document the entire scene and the specific location of the evidence found.
- Collect, label, and preserve the digital evidence.
- Package and transport digital evidence in a secure manner.

Before collecting evidence at a crime scene, first responders should ensure that—


- Legal authority exists to seize evidence.
- The scene has been secured and documented.
- Appropriate personal protective equipment is used.


First responders without the proper training and skills should not attempt to explore the contents of or to recover information from a computer or other electronic device other than to record what is visible on the display screen. Do not press any keys or click the mouse.

## Is Your Agency Prepared to Handle Digital Evidence?

Every agency should identify personnel—before they are needed—who have advanced skills, training, experience, and qualifications in handling electronic devices and digital evidence. These experts should be available for situations that exceed the technical expertise of the first responder or agency. This preparation and use is similar to the provisions in place for biohazard and critical incident responses. It is recommended that protocols for how to handle electronic crime scenes and digital evidence be developed in compliance with agency policies and prevailing Federal, State, and local laws and regulations. In particular, under the Privacy Protection Act of 1980, with certain exceptions, law enforcement is prohibited from seizing material from a person who has a legal right to disseminate it to the public. For example, seizure of first amendment material such as drafts of newsletters or Web pages may violate the Privacy Protection Act of 1980.

This guide was developed to assist law enforcement and other first responders when they encounter electronic crime scenes. These guidelines will help first responders—

- Ensure that officer safety and the safety of others remain the highest priority.
- Recognize the investigative value of digital evidence.
- Assess available resources.
- Identify the equipment and supplies that should be taken to electronic crime scenes.
- Assess the crime scene and the digital evidence present.
- Designate the assignments, roles, and responsibilities of personnel involved in the investigation.