NIJ

APR. 08

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

Chapter 3. Securing and Evaluating the Scene

NCJ 219941

Chapter 3. Securing and Evaluating the Scene

The first responder's primary consideration should be officer safety and the safety of everyone at the crime scene. All actions and activities carried out at the scene should be in compliance with departmental policy as well as Federal, State, and local laws.

After securing the scene and all persons at the scene, the first responder should visually identify all potential evidence and ensure that the integrity of both the digital and traditional evidence is preserved. Digital evidence on computers and other electronic devices can be easily altered, deleted, or destroyed. First responders should document, photograph, and secure digital evidence as soon as possible at the scene.

When securing and evaluating the scene, the first responder should—

- Follow departmental policy for securing crime scenes.
- Immediately secure *all* electronic devices, including personal or portable devices.
- Ensure that no unauthorized person has access to any electronic devices at the crime scene.
- Refuse offers of help or technical assistance from any unauthorized persons.
- Remove all persons from the crime scene or the immediate area from which evidence is to be collected.
- Ensure that the condition of any electronic device is not altered.

- Leave a computer or electronic device off if it is already turned off.

Components such as keyboard, mouse, removable storage media, and other items may hold latent evidence such as fingerprints, DNA, or other physical evidence that should be preserved. First responders should take the appropriate steps to ensure that physical evidence is not compromised during documentation.

If a computer is on or the power state cannot be determined, the first responder should—

- Look and listen for indications that the computer is powered on. Listen for the sound of fans running, drives spinning, or check to see if light emitting diodes (LEDs) are on.
- Check the display screen for signs that digital evidence is being destroyed. Words to look out for include "delete," "format," "remove," "copy," "move," "cut," or "wipe."
- Look for indications that the computer is being accessed from a remote computer or device.
- Look for signs of active or ongoing communications with other computers or users such as instant messaging windows or chat rooms.
- Take note of all cameras or Web cameras (Web cams) and determine if they are active.

Developments in technology and the convergence of communications capabilities have linked even the most conventional devices and services to each other, to computers, and to the Internet. This rapidly changing environment makes it essential for the first responder to be aware of the potential digital evidence in telephones, digital video recorders, other household appliances, and motor vehicles.

Preliminary Interviews

First responders should separate and identify all adult persons of interest at the crime scene and record their location at the time of entry onto the scene.

No one should be allowed access to any computer or electronic device.

Within the parameters of the agency's policies and applicable Federal, State, and local laws, first responders should obtain as much information from these individuals as possible, including:

- Names of all users of the computers and devices.
- All computer and Internet user information.
- All login names and user account names.
- Purpose and uses of computers and devices.
- All passwords.
- Any automated applications in use.
- Type of Internet access.
- Any offsite storage.
- Internet service provider.
- Installed software documentation.
- All e-mail accounts.
- Security provisions in use.
- Web mail account information.
- Data access restrictions in place.
- All instant message screen names.
- All destructive devices or software in use.

- MySpace, Facebook, or other online social networking Web site account information.
- Any other relevant information.