Basic Training Module Specifications

Functional Area:	I.	Investigation
Subject Area:	F.	Crime Scene Process
Module Title:	3.	COLLECTION AND PRESERVATION OF EVIDENCE
Hours:	Not less than 8 hours	

Note to Instructor:

MCOLES encourages using problem-based learning techniques and simulated crime scene scenarios to deliver the Collection and Preservation of Evidence training. Using a mock crime scene with various types of evidence (e.g., impressions, latent prints, digital media, electronic devices, etc.) is recommended.

Module Objectives:

I.F.3.1. Collect Information and Evidence at Scene of a Preliminary Investigation.

a. Gathers information leading to the identification of complainant, suspect(s), witnesses, and any other related investigative facts (e.g., who, what, why, where, when, how).

b. Interviews complainant and/or witnesses to obtain additional information (e.g., suspect's name, nature of the crime, etc.).

c. Collects and records any evidence related to the crime.

I.F.3.2. Collect Evidence and Personal Property from a Crime Scene.

a. Uses appropriate techniques for collecting evidence and personal property from crime scene in conformance with the following principles:
(1) protects the crime scene to prevent the destruction of evidence;
(2) searches crime scene systematically to locate evidence;
(3) identifies potential evidence;
(4) records location of evidence before collection (e.g., crime scene diagram, photograph, videotape, etc.);
(5) collects evidence without destroying or contaminating it; and
(6) preserves evidence for analysis and courtroom presentation.

b. Secures evidence according to department policy.

I.F.3.3. Cast Impressions.

a. Evaluates impressions at crime scene for evidentiary value (e.g., checks for cut in tire, wear spot on shoe, tire track pattern, pattern of shoe sole, tool marks, etc.).

b. Protects the impression to be cast.

I.F.3.4. Locate and Evaluate Latent Fingerprints.

a. Identifies the type of objects that can be dusted for prints (e.g., smooth, clean surfaces).

b. Examines prints for any ridge structure.

I.F.3.5. Secure Digital Media Evidence.

a. Defines digital media as any electronic technology or device potentially capable of storing information in a binary or virtual manner.

b. Identifies various types of digital media as:
(1) computer systems, components, and access control devices;
(2) telephones, cellular phones, answering machines, digital cameras, handheld devices, gaming box devices, and MP3 players;
(3) hard drives, memory cards, modems, thumb drives, routers, hubs, and network components;
(4) pagers, printers, scanners, and removable storage devices;
(5) miscellaneous electronic items (e.g., copiers, credit card skimmers, digital watches, facsimile machines, global positioning systems, iPods, etc.);
(6) CD's, DVD's, magnetic tape, and removable disks; and
(7) easily concealed in non-typical USB devises.

c. Considers the sensitive nature and evidentiary value of digital media by recognizing that it:
(1) is often hidden (latent) in the same sense as fingerprints or DNA;
(2) can transcend borders with ease and speed;
(3) is fragile and can be easily altered, damaged, or destroyed;
(4) is sometimes time-sensitive; and
(5) could contain evidence of a crime (e.g., child porn, I.D. theft, etc.).

d. Recognizes the technical capabilities of digital devices, including:
(1) direct access, both active and passive (e.g., wireless, infrared, etc.);
(2) remote access; and
(3) system/network connections.

I.F.3.5. Secure Digital Media Evidence. (continued)

e. Takes the proper steps to secure digital media as potential evidence by:
(1) considering the presence of digital photographs and data prior to disabling connections;
(2) documenting, photographing and/or video recording the computer configuration and all connections prior to disabling;
(3) labeling cables before disabling connections and peripheral devices;
(4) documenting which programs are running (if computer is active);
(5) shutting down equipment (using proper shut down procedure per operating system);
(6) considering the fragile nature of digital evidence; and
(7) sending power cords and/or power charging devices with certain electronic devices (laptops, cell phones, x-boxes, PDA's, etc.) to forensic lab (this does not apply to desktop type computers, printers, monitors, etc.).

f. Transports and stores digital media evidence by considering:
(1) temperature and humidity;
(2) physical shock;
(3) static electricity and magnetic sources; and
(4) placing cell phones in "Faraday bag" or other protective covering to block incoming signals.

Note to Instructor:

Although I.F.3.5. is intended for the first responder (i.e., patrol officer) and not evidence technicians or computer experts, MCOLES designed this material to be taught by an instructor with basic expertise in digital media evidence. First responders should be familiar with department policy, as well as state and federal laws that regulate the seizing of electronic devices. The improper access of data stored in electronic devices may violate provisions of certain Federal laws, including the Electronic Communications Privacy Act. Legal instructors familiar with digital media should address these issues during the appropriate legal blocks of instruction under *Substantive Criminal Law* and *Criminal Procedure*. The legal instruction should also cover relevant case law, consent search issues and the specific language of search warrants as it relates to digital media.

The U.S. Department of Justice published a resource guide for first responders entitled "Electronic Crime Scene Investigation." This document contains relevant information and lists many useful references, organizations, and training resources in the appendices. This document is available at: https://www.ncjrs.gov/pdffiles1/nij/219941.pdf . The Federal Trade Commission also maintains a web site regarding Identity Theft and related issues at http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html .

I.F.3.6. Tag Evidence and Confiscated Property.

a. Determines where to mark evidence or confiscated property by considering:
(1) how to preserve its value as evidence, and
(2) how to protect the article's value to owner.

b. Places identifying marks on evidence or confiscated property, if possible, which may include:
(1) complaint number,
(2) officer initials, and
(3) date.

c. Completes evidence tag by recording all pertinent information about the evidence or confiscated property.

I.F.3.7. Package Evidence and Personal Property.

a. Determines how to package evidence and personal property by considering physical characteristics of the evidence or personal property.

b. Places evidence and personal property in the appropriate container to secure and protect it (e.g., envelope, box, wrapping paper, packet, etc.).

c. Determines proper preservation techniques for evidence and personal property (e.g., refrigerating it, drying it, etc.).

I.F.3.8. Transport Evidence and Property.

a. Handles evidence and property in such a way as to preserve and secure it while being transported (e.g., not placing firearm in plastic bag).

b. Documents chain of custody of evidence by recording where the evidence or property is transported, who transported it, etc.

I.F.3.9. Document the Chain of Custody for Evidence.

a. Documents chain of custody of evidence by recording the following information about the evidence:
(1) description,
(2) dates,
(3) times,
(4) location,
(5) name of recovering officer, and
(6) where transported and stored.

b. Documents the deposit, removal, or return of evidence on appropriate forms.

I.F.3.10. Witness Autopsies.

a. Verifies identity of body of deceased upon which the autopsy is to be performed.

b. Collects evidence from the body of the deceased which will assist in the investigation (e.g., photograph fingerprints, obtain nail scrapings, collect clothing, etc.).

c. Takes custody of evidence collected by the pathologist during the autopsy.

d. Records (in field notes) facts contributing to death, as determined by the pathologist during the autopsy.

Module History

Revised	01/10
Reviewed	09/21