



MILWAUKEE POLICE DEPARTMENT

STANDARD OPERATING PROCEDURE

740 – FORENSIC EVIDENCE COLLECTION

GENERAL ORDER: 2024-23
ISSUED: April 15, 2024

EFFECTIVE: April 15, 2024

REVIEWED/APPROVED BY:
Assistant Chief Nicole Waldner
DATE: March 13, 2024

ACTION: Amends General Order 2023-16 (April 21, 2023)

WILEAG STANDARD(S): 11.1.1, 11.1.2, 11.1.3, 11.1.4, 11.1.5, 11.1.6, 11.1.7, 11.1.8, 11.2.1

740.00 PURPOSE

The purpose of this standard operating procedure is to establish guidelines regarding the collection, preservation, and documentation of forensic evidence and the utilization of forensic services. These duties include but are not limited to the following:

- providing photographic services for the department and other agencies,
- providing crime scene examinations in the area of evidence collection and latent print development;
- obtaining, comparing and identifying fingerprints from dead human bodies;
- identifying prisoners through fingerprint comparisons;
- retrieval and processing of forensic video evidence;
- process document evidence;
- comparison and identification of crime scene latent prints to known persons;
- providing testimony regarding forensic analysis or examination in court proceedings;
- records management regarding forensic services, criminal records, fingerprint databases, latent, mug shot and photographic evidence;
- retrieval of digital evidence;
- collection and preservation of DNA and biological evidence.

740.05 GENERAL (WILEAG 11.1.1, 11.1.2, 11.1.5, 11.1.6, 11.1.7, 11.1.8)

A. TRAINING

The department will provide or authorize training regarding the detection, collection, preservation and documentation of physical, DNA, and computer / electronic evidence in conformity to established laws and department guidelines. Specialized training will be provided for crime scene trained (CST) officers, community service officers, forensic investigators, crime scene investigators, and other personnel assigned to the Forensics Division and High Technology Unit. Updated training will be provided as necessary.

(WILEAG 11.1.5.4, 11.1.6.3, 11.1.6.4)

B. AVAILABILITY

Forensic services by trained forensic investigators, crime scene investigators,

community service officers, and/or CST officers shall be accessible for 24 hours/7 days a week.

- C. First responders and investigators shall safeguard the integrity of the scene and relevant physical, DNA, and computer / electronic evidence in accordance with SOP 725 (Crime Scene Investigations). All firearms shall be unloaded prior to being transported, placed on inventory, or submitted for processing. The member shall provide a copy of the *Gun Recovery Report* with the firearm submitted for processing. (WILEAG 11.1.5.1, 11.1.6.1, 11.2.1.5)

D. EVIDENCE COLLECTION AND PRESERVATION

Evidence collected from a scene shall be packaged in such a way as to safeguard the integrity of the evidence, and prevent damage and contamination. Evidence shall subsequently be placed on inventory in accordance with SOP's 560 (Property) and 725 (Crime Scene Investigations). (WILEAG 11.2.1.4)

1. Biological / DNA evidence shall be dried and individually packaged in paper envelopes/bags or other "breathable" material. Plastic or other airtight materials/containers shall not be utilized as they may retain moisture and damage evidence. (WILEAG 11.1.5.2)
2. Forensic investigators and crime scene investigators are responsible for inventorying items of evidence that they collect (e.g., latent lifts, DNA swabs, footwear impressions).

E. EVIDENCE INVENTORY AND TRANSFER

In order to maintain an effective chain of custody, all evidence submitted for analysis shall be properly inventoried prior to processing. Any additional property transfers shall be documented on the property inventory in accordance with SOP 560. (WILEAG 11.1.5.2, 11.1.8.4)

F. DOCUMENTATION

1. An incident report, supplementary report or *Department Memorandum* (form PM-9E) shall be completed documenting relevant details regarding the detection, collection, preservation and documentation of physical and electronic evidence. Documentation regarding the transfer of custody of physical evidence shall include the date and time of transfer, name of person transferring property, name/title/agency of person receiving property, laboratory name and location (if applicable), reason for the transfer, if any processing is required, and a brief synopsis of the case.
2. The investigating officer or detective shall document the name and PeopleSoft number of the member taking photographs of the scene, including the number of photographs and the date and time the photographs were taken.

740.10 FORENSIC IMAGING LAB / PHOTOGRAPHIC EVIDENCE (WILEAG 11.1.3)**A. CARE AND MAINTENANCE OF EQUIPMENT**

All crime scene trained and sergeant digital cameras shall be supplied by the Forensics Division and maintained by the respective work locations.

1. Work location supervisors shall conduct periodic inspections of the cameras for serviceability. When a camera is found to be defective, the camera shall be conveyed to the Forensics Division for service. An investigation shall be initiated if negligence is involved by a work location supervisor. The work location supervisor conducting the investigation shall submit a *Department Memorandum* (form PM-9E) documenting the reason for the negligence prior to the Forensics Division repairing or replacing the camera.
2. Prior to using the camera, members shall inspect it for serviceability and shall immediately report any problems with the camera to his/her shift commander or shift supervisor.
3. Commanding officers at each work location shall be responsible for the retention and distribution of digital camera(s) assigned to their respective work locations.
4. The Forensics Division may assign digital cameras to individual members and the member receiving the camera shall be responsible for maintaining the camera.

B. IMAGE / PHOTOGRAPHIC STORAGE

Original images shall be imported in an unaltered state to Evidence.com.

C. PHOTO REQUESTS

1. Request for photographs by department members shall be made by emailing [REDACTED]. Members shall carbon copy (cc) the supervisor authorizing the request and must include the case number; needed by date; and reason for why the photographs are being requested (e.g., District Attorney's Office review, pre-trial, jury trial, investigation).
2. All other requests for photographs must be made following existing open records procedures.

740.15 SCENE AND INCIDENT PHOTOGRAPHY (WILEAG 11.1.3)**A. REQUEST FOR SERVICES FROM FORENSICS DIVISION PERSONNEL**

1. If a member needs a forensic investigator or crime scene investigator, the member shall notify their shift commander. Shift commanders shall then notify the Criminal Investigation Bureau (CIB) at extension [REDACTED], and the CIB shift commander shall determine if a forensic investigator or crime scene investigator will respond to the scene.

2. The CIB shift commander shall notify the Forensics Division if a forensic investigator or crime scene investigator will need to respond to the scene.

B. TYPES OF INCIDENTS - RESPONSIBILITIES

1. Forensics Division

Forensics Division personnel shall photograph major crime scenes, fatal accidents, etc. and may be requested when more sophisticated photography skills and equipment are needed. They may also be requested in accordance with SOP 740.15(A)(1) when a supervisor or other authorized member is not available to photograph an incident.

2. Sergeants and Other Supervisors

Sergeants and other supervisors authorized by the Forensics Division shall photograph the following incidents:

- a. Property damage traffic crashes involving city-owned vehicles.
- b. Scenes at which forced entry by department members resulted in property damage.
- c. District level internal investigations or use of force complaints.
- d. Those scenes in which a department owned camera can adequately document the pertinent information.

Note: A forensic investigator or crime scene investigator may also be utilized to photograph the above incidents in accordance with the approval procedures in SOP 740.15(A)(1).

3. Crime Scene Trained Officers (CST) and Community Service Officers

District CST's and community service officers have been trained to assist officers in the processing of certain crime scenes as they have received limited specialized training in crime scene photography, processing latent prints, and DNA collection. However, a CST or community service officer does not replace a forensic investigator or crime scene investigator in those situations where the nature of the investigation requires more specialized training and equipment. In addition, sergeants are still required by SOP 740.15(B)(2) to take certain photographs; a CST or community service officer cannot take the photographs that SOP 740.15(B)(2) requires of sergeants.

- a. CST's, community service officers, or on scene supervisors should be utilized to photograph scenes in which the CST or community service officer assigned camera can adequately document the pertinent information in accordance with departmental training and guidelines. Absent special circumstances, a forensic investigator or crime scene investigator will not respond to photograph death

investigations in which the following circumstances exist:

1. Non-suspicious death of an individual under long-term medical treatment in a facility (e.g., nursing home, hospital).
2. Non-suspicious death following facility-based or in-home hospice care.
3. Non-suspicious death of an adult over 65.

Note: A forensic investigator or crime scene investigator may only be utilized to photograph the above incidents in accordance with the approval procedures in SOP 740.15(A)(1).

- b. A CST officer or community service officer should not be utilized to process any firearms or any extensive crime scene requiring specialized evidence collection (e.g., footwear, chemical processes). All abandoned firearms and firearms involved in a crime shall be processed at the Forensics Division.
4. District Stations and Other Work Locations

Supervisors shall authorize the use of a digital camera to include, but not limited to, scenes in which the camera can adequately document the pertinent information in accordance with departmental training and guidelines.

Note: Only members who have received training from the Forensics Division shall be allowed to photograph scenes.

C. IMAGES TO BE TAKEN

1. In an effort to accurately depict the details and locations of pertinent evidence and crime scenes the following photographs should be taken:
 - a. Overall Scene

Panoramic photo taken of a scene from multiple vantage points to depict spatial relationship of persons/objects within a scene.
 - b. Mid-Range

Photo taken of entire person/object to depict the overall view of person/object for identification purposes.
 - c. Close Up

Photo taken within six to twelve inches of person/object to depict details of the person/object.

2. Review images at the scene

Digital images shall be reviewed prior to leaving the scene. In the event the images do not adequately depict the necessary detail, are blurred or are otherwise of poor quality, the images shall be retaken.

Note: No images shall be deleted from the camera or secure digital (SD) cards.

3. Document all photographs

All department members who photograph an incident shall complete a *Photographic Record Sheet* (PP-52). All relevant information must be noted on the incident report or envelope, which shall be reviewed by a work location supervisor.

- a. Complete the narrative portion of the PP-52, providing a brief summary of the photographs that were taken.
- b. In order to indicate the end of an incident the final photograph shall be of a completed PP-52.
- c. Evidence.com shall be reviewed to ensure the images were properly imported.
- d. Complete a supplemental report; *Forensics – FI Supplemental*; or a *Forensics – CST/CSO Supplemental* report in the Records Management System (RMS) describing the photographs taken.
- e. Once imported into Evidence.com, one copy of the PP-52 shall be forwarded for imaging to the Records Management Division, and the original shall be retained by the work location for 31 days and then destroyed in accordance with SOP 680.10(E)(5), as it relates to data protection and security.

D. VIDEO

1. Crime scene and/or items of evidence can be video recorded by a forensic investigator or crime scene investigator to document the crime scene and/or the location of evidence found to produce a permanent record. Video shall be taken in a manner consistent with training.
2. Information pertaining to all video, including the date, time, and location the video was recorded shall be documented in a supplemental report by the member recording the video. The recorded video shall be imported to Evidence.com.

E. The Training Division shall maintain a list of supervisors, CSTs, and community service officers that are authorized and trained to take photographs of scenes.

740.20 LATENT PRINT COLLECTION (WILEAG 11.1.4, 11.1.7)

A. Latent print processing is intended to develop hidden or invisible fingerprint

impressions. This processing is intended to establish an individualized forensic linkage or exclusion between suspects, victims, witnesses, and physical evidence through the collection and examination of latent fingerprint evidence. These duties shall be performed by authorized personnel who have been trained by the Forensics Division, in conformity to established laws, and department guidelines.

- B. Fingerprints shall be processed, developed, photographed, lifted, labeled, and stored in a manner consistent with basic and specialized training and in accordance with the Department of Justice *Physical Evidence Handbook*, which is located on the directives intranet homepage under [Handbooks, Manuals, and How-To's](#). The recovery of latent prints shall be documented in a supplemental report by the member recovering the latent print.

C. ON-SCENE PROCESSING

1. Members shall request a CST officer, community service officer, or with supervisory approval in accordance with SOP 740.15(A)(1), a forensic investigator or crime scene investigator during any investigation that requires the processing of a scene for latent fingerprints. CST and community service officers shall be utilized at scenes in accordance with 740.15(B)(3).
2. A *Forensics Division Case Folder* (PE-13) must be completed and a latent case number must be assigned to all cases regarding latent print collection regardless of positive or negative results.

D. COUNTER CASE

1. Portable items of evidence, as defined in SOP 560.10 (Property), that have not been processed at a crime scene may be submitted to the Forensics Division for examination in accordance with the procedures listed herein.
2. Property shall be transferred on a property inventory to personnel assigned to the Forensics Division for processing.
3. A *Forensics Division Case Folder* (PE-13) must be completed by the submitting member.
4. When all forensic processing is completed, all items of evidence shall be secured at the Forensics Division until it can be properly transferred to the custody of the Property Control Division.
5. A latent case number must be assigned to all cases regarding latent print collection regardless of positive or negative results.

E. LATENT PRINT EXAMINATION

1. All latent cases with actual latent print evidence shall be analyzed by a latent print examiner or chief latent print examiner in order to determine the quality of the lifts. Lifts may then be compared manually and/or processed utilizing the departmental

Automated Fingerprint Identification System (AFIS). The member conducting the latent print examination shall document their analysis in a *Forensics – Latent Print Examiner Supplemental* report in the Records Management System.

2. Latent cases shall be retained by the Forensics Division in accordance with departmental record retention schedules.
3. In accordance with state and federal open records and discovery laws, defense attorneys may be allowed to have their own experts review latent fingerprint evidence provided it has been approved by the district attorney's office or by court order. All latent fingerprint evidence to be subjected to external examination shall remain in the custody of the Milwaukee Police Department. This evidence is not to be removed by or released to defense experts for review. Defense experts are allowed to conduct forensic examinations on departmental premises by appointment only.

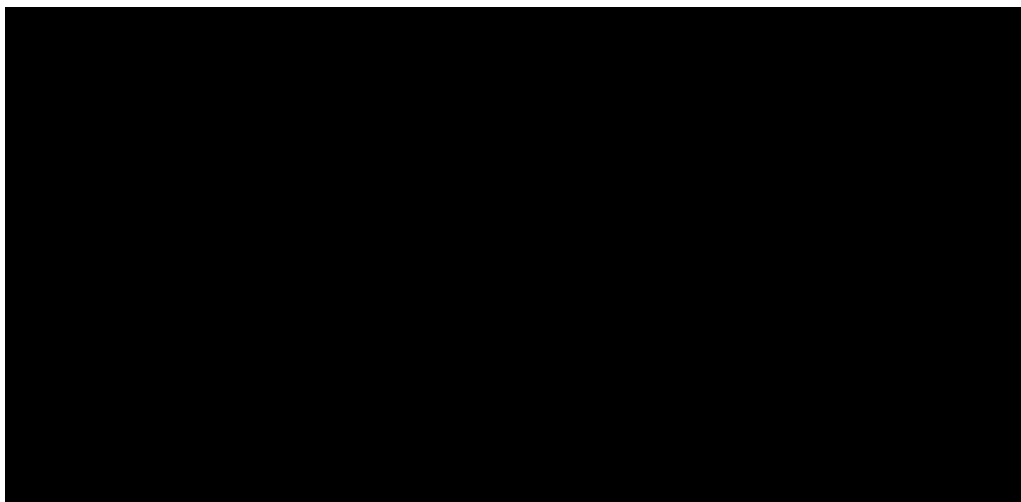
740.25 DNA and BIOLOGICAL MATERIALS (WILEAG 11.1.5)

- A. DNA processing is intended to collect visible or trace biological samples. This processing is intended to establish an individualized forensic linkage or exclusion between suspects, victims, witnesses, and physical evidence through the collection and examination of various forms of biological material, including but not limited to, blood, sweat, saliva, semen, and other biological materials. These duties shall be performed by authorized personnel, in conformity to established laws and department guidelines.

(WILEAG 11.1.5.2)

B. DETECTION

1. It is imperative that members closely examine all scenes and pertinent items for the presence of biological evidence. Members should take care to protect against destruction and/or contamination of biological materials. Consideration should be taken to determine the most likely location of DNA evidence by asking the following questions:



(WILEAG 11.1.5.1)

2. If a department member needs clothing/fabric or casings to be processed for DNA by the Forensics Division, they shall obtain approval from a Forensics Division supervisor prior to bringing the items to the Forensics Division. If a Forensics Division supervisor does not approve the request, the items must be submitted directly to the Wisconsin State Crime Lab for analysis.
(WILEAG 11.1.5.3)

740.30 OTHER FORENSIC EVIDENCE AND SERVICES

Forensic investigators, crime scene investigators, and latent print examiners assist with the collection of various forms of forensic evidence, including but not limited to the following:

- Trace evidence collection (e.g., hairs, fibers, glass fragments, soil).
- Tool, tire and footwear impressions.
- Prisoner fingerprint identification and classification.
- Identification of unknown or deceased persons through fingerprint comparisons.
- Presumptive testing (human blood).
- Trajectory marking.

740.35 TRANSMITTAL OF EVIDENCE TO OUTSIDE AGENCY (WILEAG 11.1.8)

With the exception of the analysis listed herein, the Milwaukee Police Department does not provide scientific analysis of physical evidence. Request for these levels of analysis must be submitted to a qualified external agency, such as the Wisconsin State Crime Lab or other processing agency, in accordance with SOP 560.45.

740.40 SCENE RECOVERY OF SURVEILLANCE VIDEO EVIDENCE

A. ON-SCENE RETRIEVAL/CAPTURE

1. The member retrieving the video shall import the video to Evidence.com. If the member is unable to retrieve the video and needs the Forensics Division to obtain the video, this request shall be made utilizing a *Forensic Video Request* form (PI-60).
2. In the event that another member responds to a location independent of the investigating officer, the investigator will be notified of the retrieval and the member retrieving the video shall import the video to Evidence.com and complete a supplemental report in RMS. If the video is unable to be imported to Evidence.com, the member shall make a DVD copy of the video and place it on inventory in accordance with SOP 560 Property.

B. THIRD PARTY RECOVERY

1. Video evidence retrieved or recovered by a third party (e.g., non-department person such as a property owner or business employee) may be submitted for analysis. These items must be imported to Evidence.com by the receiving member who shall complete a supplemental report in RMS.
2. Video or photographic evidence retrieved by a member from a resident regarding an incident through Axon Citizen in Evidence.com shall complete a supplemental report in RMS.

740.45 IN-HOUSE/COUNTER CASE VIDEO REQUEST**A. REQUEST FORM**

Members requesting in-house forensic video analysis (enhancements, still images, or format conversions) shall complete a *Forensic Video Request* form (PI-60). The form and the original video evidence shall then be submitted to the Forensics Division.

B. CHAIN OF CUSTODY

In order to maintain chain of custody, all video evidence submitted for analysis shall be properly inventoried prior to submission for processing. Any additional property transfers shall be documented on the property inventory.

C. MEDIA RELEASES

The Public Information Office or a member authorized by a supervisor may prepare video images intended for public release to media outlets for the purpose of clarification of events, identification or location of relevant individuals. These files will be released at the approval of the Chief of Police.

D. NOTIFICATION OF COMPLETION

Upon completion of the forensic video analysis, the forensic investigator or crime scene investigator shall notify the requesting investigator. The finished product and any original video evidence not initially turned over to the investigating member shall be imported to Evidence.com.

E. OTHER REQUESTS

All other requests for forensic video images must be made following existing open records procedures.

740.50 COMPUTER / ELECTRONIC EVIDENCE (WILEAG 11.1.6)

- A. Digital evidence is evidence which is contained within any form of magnetic or electronic media, which can include, but is not limited to, hard drives, USB drives, compact discs (CD), digital versatile discs (DVD), floppy disks, flash memory cards,

magnetic tape, secure digital (SD) cards, digital cameras, cellular phones, global positioning systems (GPS), digital audio recorders, etc. Members shall use caution when they seize electronic devices as improperly accessing data stored on electronic devices may violate federal and/or state laws. In addition to the legal ramifications of improperly accessing data that is stored on electronic devices, members must understand that electronic data is fragile and easily altered. Only properly trained members shall attempt to examine and analyze digital evidence. Members shall contact the High Technology Unit through their shift commander for assistance if they have questions or concerns related to the recovery of any computer / electronic evidence.

B. FIRST RESPONDER RESPONSIBILITIES AND PRECAUTIONS

1. Investigators are responsible for maintaining the integrity of the crime scene. This responsibility starts with the first officer(s) on scene.
2. Members shall ensure that no unauthorized person(s) has access to any electronic devices at the crime scene, and shall refuse all offers of help or technical assistance from any unauthorized persons.
3. Sworn members shall remove any persons from the crime scene or the immediate area from which evidence is to be collected.
4. Members shall ensure that the condition of any electronic device is not altered.
5. Members shall leave a computer or electronic device off if it is already turned off. Members shall have photographs of the computer screen taken as necessary if the computer is already on. However, members shall not attempt to access any computer files if the computer is on.
6. Members shall collect all power supplies and adapters associated with any electronic devices seized.
7. Members shall document the scene prior to securing electronic evidence and have photographs taken as necessary. Members shall document the entire location, including the type, location, and position of computers, their components and peripheral equipment, and other electronic devices.
(WILEAG 11.1.6.1, 11.1.6.2)

740.55 COLLECTION OF COMPUTER / ELECTRONIC EVIDENCE (WILEAG 11.1.6)

- A. Members shall ensure that all digital evidence is documented and photographed (if necessary) before it is packaged and inventoried.
- B. Members shall package all digital evidence in antistatic packaging. Only paper bags and envelopes, cardboard boxes, and antistatic containers should be used for packaging digital evidence. Plastic materials shall not be used when collecting and storing digital evidence.

- C. Members shall ensure all digital evidence is packaged in a manner that will prevent it from being bent, scratched, or otherwise deformed.
- D. Members need to remove the power source from electronic devices that are in an “on” state. Desktop computers should have the power cord pulled from the back of the computer. Laptops and mobile computers should also have the battery removed and then the power cords removed and collected (if applicable). Cell phones should be placed into “airplane mode.” The sim card should be removed and taped to the back of the device when possible.

Note: Subsection D does not apply to members of the High Technology Unit while performing procedures for live analysis and preservation of volatile data.

- E. Members shall collect all power supplies and adapters for all electronic devices seized.
(WILEAG 11.1.6.1, 11.1.6.2)

740.60 TRANSPORTATION AND STORAGE OF COMPUTER / ELECTRONIC EVIDENCE
(WILEAG 11.1.6, 11.1.7)

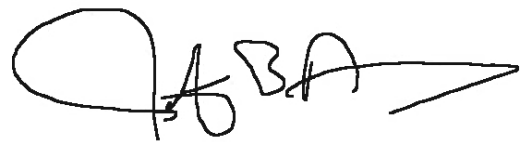
- [REDACTED]
- [REDACTED]
- B. Members should avoid keeping digital evidence in a squad car for prolonged periods of time. Heat, cold, and humidity can damage or destroy digital evidence.
 - C. Members shall ensure that computers and electronic evidence are packaged and secured during transportation to prevent damage.
 - D. Members shall inventory all computer / electronic evidence in accordance with SOP 560.
(WILEAG 11.1.6.2)

740.65 SUBMISSION OF COMPUTER / ELECTRONIC EVIDENCE TO HIGH TECHNOLOGY UNIT FOR ANALYSIS (WILEAG 11.1.6)

- A. Electronic evidence requiring analysis shall be submitted to the High Technology Unit. Requests for service by the High Technology Unit shall include the following:
 - 1. Members shall submit electronic evidence for analysis by utilizing the online analysis request on the High Technology Unit’s Share Point page.
 - 2. One copy of all property inventories related to the evidence submitted for analysis.
 - 3. A search warrant is required and must include appropriate language that specifically allows for the examination of the digital evidence submitted. Other forms of legal authority, such as written consent signed by the owner, usage agreement, or documented company policies, shall be acceptable. Oral consent is

acceptable, but it must be documented.

4. More information regarding the submission of electronic evidence can be found on the High Technology Unit's [Share Point page](#).
- B. All computer components, peripherals, or other electronic evidence that is necessary to support a criminal case in court shall be seized. The seized property shall be fingerprinted and/or DNA processed if applicable, prior to requesting analysis by the High Technology Unit.
- C. The High Technology Unit will not accept keyboards, mice, monitors, printers, scanners, web cams, etc., which do not normally contain electronic evidence.
(WILEAG 11.1.6.3)

A handwritten signature in black ink, appearing to read 'J.B.N.' followed by a long horizontal stroke.

JEFFREY B. NORMAN
CHIEF OF POLICE

JBN:mfk