DIRECTIVE 83.2
COLLECTION AND PRESERVATION OF EVIDENCE OPERATIONS

Issue Date: 05/28/2020	By Order of Chief of Police
Rescinds: (Issue: 08/11/2015) Pages: 15	CALEA Standards Referenced: 83.2.1; 83.2.2; 83.2.3; 83.2.4; 83.2.5 & 83.2.6

This directive consists of the following sections:

POLICY AND PROCEDURE:

It is the policy of the Miami Township Police Department to thoroughly investigate crime and traffic collision scenes. Thorough investigations include the collection, processing, handling, preservation and documentation of physical evidence in an efficient manner.

83.2.1 Guidelines and Procedures

First Responder Responsibilities and Precautions

It is the responsibility of the first officer at the scene to secure that scene from all non-essential personnel. The scene must be secured as soon as possible to prevent contamination of the scene and/or loss of evidence. The officer securing the scene should initiate a crime scene entry log, listing the time, name and reason for all personnel who enter the crime scene. All personnel at the scene will not disturb, touch or handle physical evidence; unless a danger exists that the evidence will be lost or destroyed prior to it being processed. Should such a situation arise, it will be the responsibility of the officer securing such evidence to mark, seal, tag and preserve the evidence.

Officers responsible for processing a scene will be responsible for preparing a written report, photographing, crime scene sketch, collecting, packaging, preserving, transporting and submitting all evidence to a Department designated property storage area.

Scene Sketches

Generally, the processor of the scene will make rough sketches with measurements, including sufficient additional information so a final drawing, to scale, can be made at a later time, if needed. These rough sketches are evidence and shall be kept by the case Detective. When crime scene sketches are drawn pursuant to the collection and preservation of evidence, they will contain the following information:

- Dimensions
- Relation of the crime scene to other buildings, geographical features or roads.
- Address, floor or room number as appropriate.
- Location of significant features of the scene, including the victim.
- Date and time of preparation.
- Name of person preparing the sketch.
- Direction of North
- Location of items of physical evidence recovered.

If evidence is transferred to another person prior to being logged in to the department designated property storage area, documenting the transfer is critical to maintaining the chain of custody. The record of transfer shall be indicated on the property submission form.

If a specialist is called to the scene, i.e. staff from BCI & I, accident reconstruction specialist, the date and time of the request and the requesting officer's name will be added to the report. All information obtained by the specialist will be documented and included with the report.

Should physical analysis be required of all or a part of the evidence obtained from a scene, the person who submitted such evidence shall be responsible for informing the assigned case Detective of that information and the type of analysis requested.

The procedures used for the collection and preservation of all evidence will be consistent with accepted practices for the collection of physical evidence.

If an officer responsible for processing a scene decides that no evidence can be collected and/or photographs taken at a scene, the offense report and/or supplement will outline the reasons.

Procedures for the Collection, Storage and Transportation of Evidence

Collection of Blood and Other Bodily Fluids

Employees must use protective gear when handling biological evidence.

Biological Evidence is defined as the contents of a sexual assault kit, blood, semen, hair, saliva, tissue or any other biological material that was collected as part of a criminal investigation or delinquent child investigation that be exculpatory or incriminatory. This

includes evidence present separately (such as on a slide or a swab) or other evidence such as clothing, bedding or cigarettes.

Biological Evidence from certain criminal investigation must be retained for 30 years or longer. [ORC 2933.82]

ORC SECTION	OFFENSE	UNSOLVED	CONVICTED
2903.01	**Aggravated Murder**	Indefinitely	Until released from prison, parole, community control, registration requirements, etc. or until the person dies but no less than thirty years
2903.02	**Murder**	Indefinitely	
2903.03	**Voluntary Manslaughter**	30 Years	
2903.04	**Involuntary Manslaughter**	30 Years	
2903.06	**Aggravated Vehicular Homicide (F1 or F2)**	30 Years	
2903.06	**Vehicular Homicide (F1 or F2)**	30 Years	
2903.06	**Vehicular Manslaughter (F1 or F2)**	30 Years	
2923.02/2907.02	**Attempted Rape**	30 Years	
2907.02	**Rape**	30 Years	
2907.03	**Sexual Battery**	30 Years	
2907.05(A)(4) or (B)	**Gross Sexual Imposition (Less than 13 yoa)**	30 Years	

Blood, urine, semen and other body fluids will be collected at a scene only be personnel who have received training in the collection and preservation of such substances.

Specimens collected which require refrigeration will be maintained in the property room refrigerator.

Specimens collected will be marked, sealed and tagged as appropriate to identify and preserve them for analysis.

Fresh wet blood will be collected in an appropriate evidence container.

Wet blood-stained items must be allowed to dry before packaging. Only secure areas will be used to hang a blood-stained item for drying. Once the blood-stained item is dry it will be placed in an appropriate evidence container. All blood-stained items will be packaged in separate containers to avoid contamination.

When possible, dry blood-stained objects should be collected in their entirety. If this is not possible, the dried blood should be collected with moistened gauze fibers. Gauze fibers will be moistened with distilled water solution and the gauze pad will be used to swab the blood. Once the gauze has soaked up the blood, it will be allowed to dry. Once dry, the container will be properly marked, sealed and tagged and placed in the property room. Dry blood does not require refrigeration.

Fluids and stains other than blood can be collected by the same procedure as blood.

Body Tissues will be placed in an appropriate container, sealed, marked and refrigerated. Blood and urine specimens for OVI and drug screens will be packaged according to the procedures enclosed in the OVI kits. The kit will be marked, sealed and refrigerated.

Sexual Assault Kits shall be sealed and marked after hospital staff releases them to the Miami Township Police Department.

Other Items Collected as Evidence

Wet clothing and wet documents collected as evidence shall be air-dried. A temporary storage locker will be utilized if the clothing will fit in the locker and will allow for proper drying. Should this method not be suitable, a property room custodian shall be contacted and provide for secured storage of the item while they air dry. As soon as the evidence is dried it will be marked, packaged, tagged and submitted to the property system.

Firearms, dangerous drugs, currency and volatile fluids of evidentiary value will be submitted in accordance with property submission procedures outlined in Directive 84.1.

Stolen vehicles that are recovered will be towed to and placed in the Large Property Containment area. The recovering officer shall as soon as practical, have a Detective process the vehicle.

DNA Evidence Collection

A DNA (deoxyribonucleic acid) match is a major factor in solving cases where the identity of the offender is not known. The Miami Township Police Department has DNA evidence collection capabilities.

DNA and other biological evidence must be retained for crimes of aggravated murder, murder, voluntary manslaughter, first and second-degree involuntary manslaughter, first and second degree aggravated vehicular homicide, rape, attempted rape, sexual battery or underage gross sexual imposition.

In the case of aggravated murder or murder, biological evidence must be maintained for as long as the crime remains unsolved. In unsolved cases involving other offenses, biological evidence must be maintained for thirty (30) years from the time of collection.

If the accused is convicted of the crime but did not plead guilty, the evidence must be maintained for 30 years or until the expiration of the latest period of time (whichever comes first) that the accused is:

- Incarcerated;
- Under community control sanction;
- Under any order of disposition for the offense;
- On probation or parole for the offense;

- Under post-release control for the offense;
- Involved in civil litigation or subject to registration.

If the offender is still incarcerated after thirty (30) years, the evidence must be kept until the offender is released from incarceration or dies.

In short, the offender must have fully completed his/her sentence, including probation. The offender must not be subject to any registration requirements such as sex offender registration. There must be no pending civil litigation stemming from the offense. If all these criteria are met, the biological evidence may be disposed of. Otherwise the thirty (30) year wait applies.

A request to dispose biological evidence prior to the above-mentioned time frames may be made by certified mail to all the following:

- The offender;
- The attorney of record for the offender;
- The Ohio public defender;
- The county prosecutor;
- The Ohio Attorney General.

If no response is received after one (1) year the evidence may be disposed of. If any of those parties' request that the evidence be retained, the evidence must be maintained.

If the offender pleads guilty or no contest, biological evidence can be destroyed five (5) years after the plea and any appeals from the plea have been exhausted unless the offender requests retention and the court finds good cause to retain the evidence.

Evidence that is too large to retain (i.e. car, boat, etc.) for a long period of time may be disposed of. In those cases, the agency must remove and preserve portions of the evidence that are likely to contain biological evidence. The evidence must be maintained in a manner and amount sufficient to develop a DNA profile.

The agency is required to provide an inventory of the biological evidence it possesses in connection with a case if requested to do so in writing by the defendant.

Every officer should be aware of important issues involved in the identification, collection, transportation, and storage of DNA evidence. Because extremely small samples of DNA can be used as evidence, greater attention to contamination issues is necessary. Evidence can be contaminated when DNA from another source gets mixed with DNA relevant to the case. This can happen when someone sneezes or coughs over the evidence, or touches his/her mouth, nose or other part of the face, and then touches the area of the evidence containing the DNA.
Procedures for the Collection, Storage and Transportation of DNA Evidence

When transporting and storing DNA evidence, keep the evidence dry and at room temperature. Once the evidence has been secured in paper bags or paper envelopes, it must be sealed, labeled, and transported in a way that ensure proper identification of where it was found and proper chain of custody.

- Never place DNA evidence in plastic bags as moisture retained in the bags can be damaging to the DNA.
- Direct sunlight and hot conditions also may be harmful to DNA.

To avoid contamination of evidence that may contain DNA, always take the following precautions:

- Wear disposable latex gloves.
- Use disposable instruments or clean them thoroughly before or after handling each sample.
- Avoid touching the area of the evidence where DNA is believed to exist.
- Avoid talking, sneezing, scratching and coughing over evidence.
- Avoid touching your face, nose and mouth when collecting and packaging evidence.
- Air-dry evidence thoroughly before packaging (not in direct sunlight).
- Put evidence into new paper bags or paper envelopes. Do not use plastic bags or staples.

As with fingerprints, the effective use of DNA may require the collection and analysis of 'elimination samples'. These samples are necessary to determine whether the evidence came from the suspect or from someone else.

Only persons trained in the collection of DNA evidence shall do so. DNA evidence training is available through several outside courses. i.e. Crime Scene and Evidence Collection. Investigative personnel who have received training in DNA collection may train other personnel.

Once packaged and submitted to the property room, DNA evidence will be transported to an accredited laboratory for DNA analysis. The transfer shall be in accordance with Directive 83.3, Section 83.3.2.

Evidence Collection Training Requirements for Persons Collecting Evidence

Officers will utilize their knowledge from their Ohio Peace Officer Training Academy and experience to properly collect evidentiary items. Only persons trained in the collection of evidence shall do so. Evidence training is available through several outside courses. i.e. Crime Scene and Evidence Collection.

Procedures for the Submission of Evidence to Accredited Laboratories

Once packaged and submitted to the property room, evidence will be transported to an accredited laboratory for analysis if requested/required. The transfer shall be in accordance with Directive 83.3, Section 83.3.2.

Transfer of Custody of Physical Evidence

If evidence is transferred to another person prior to being logged in to the department designated property storage area, documenting the transfer is critical to maintaining the chain of custody. The record of transfer shall be indicated on the property submission form. If evidence is transferred to another person after being logged in to the department property room. The record of transfer shall be indicated on the property submission form.

83.2.2 Photography, Video and Audio Evidence

Photographs and video tapes of crime scenes, serious traffic collisions and other incidents which may require the use of photographs or video tapes for recording the scene will be the responsibility of the investigating officer or officer assigned to process the scene.

Photographing of all aspects of the crime scene, traffic collision or incident will be required in the following instances.

- Homicide
- Rape, Abduction or Kidnapping
- Death Scene
- Investigation of Excessive Force
- Injuries to a Police Officer or Citizen During Arrest
- Fatal or Serious Injury Traffic Collisions
- Damage or Injury to Township Property
- Serious Property Damage Accidents in Excess of $5,000.00 Damages
- Burglaries Where Loss May Exceed $3,000.00
- Arson or Suspected Arson
- Discharge of a Firearm by a Police Officer in Relationship with Use of Force
- Aggravated or Felonious Assaults Involving a Weapon
- Any Crime Scene Upon Request of the Reporting of Investigating Officer

Photographing to Demonstrate Scale – When the exact size of an item being photographed is required, a scale will be placed next to the item to add dimension and aid in development for ‘to scale’ prints. A second photograph of the item will be taken without the scale, using the same camera settings, position and lighting in the event the court desires photographs of evidence in which nothing has been introduced into the field of view.

Recording Photography Information – The photography of any crime scene or traffic collision scene is the responsibility of the investigating officer or officer assigned to process the scene.

The officer photographing any crime scene or traffic collision scene utilizing digital photography shall download the digital photography to the Miami Township Police secure 'G' drive, year appropriate Records folder, to a file with the assigned CAD Number or Report Number. The officer shall submit an email to Records personnel advising them of the download, along with significant identifiers such as victim name, location, time of event, etc. to allow records personnel to place the photographs in a 'G' drive folder utilizing the event number. Records personnel shall also download the photographs into the Miami Township records management software Interbadge.

Digital Video Taping of a scene may be used as a supplement to but shall not replace still photography as visual documentation of a scene. Digital video of a crime or traffic collision scene that has evidentiary value shall be transferred to a digital medium (CR-R or DVD). The officer shall enter the digital medium as evidence into the department property room and document this piece of evidence on the NIBRS report as well as in the narrative.

The use of personally owned devices will not be used when photographing or recording evidence at a scene.

83.2.3 Fingerprinting

Latent Fingerprints

Only officers trained to collect latent fingerprints will do so. The following guidelines will be followed when processing a crime scene for latent prints:

- Latent impressions developed with fingerprint powder should be photographed on the original object. After being photographed, they should be lifted.
- The process of lifting latent prints follows these guidelines (ref: FBI Publication "The Science of Fingerprints"):

    - Observe and identify the surface bearing the suspected latent. A flashlight held at an angle can enhance visualization.
    - If the surface is non-porous, oxide powder can be used.
    - Lightly dip the fiber brush into the powder and tap the excess off on the inside of the powder jar.
    - Lightly stroke the surface in the area of the suspected latent.
    - Once the print begins to visualize, continue to apply light strokes with a minimal use of powder until the print is fully enhanced.
    - Once the print is visual, select lifting tape and peel the necessary amount to cover the latent plus three inches.

- Place the tape over the latent from the outside edge and work inward, pressing the tape down uniformly over the entire area.
- Peel the tape up from one side and immediately place down on lifting card of contrasting color.

The lifted print is to be placed on a latent fingerprint card with the following information listed in the offense report/supplement:

- Place of Occurrence
- Complainant
- Complainant Address
- Type of Offense
- Date of Offense
- Name of Officer Making Lift
- Diagram, noting the location on the item that the lift was made from.

The officer shall enter the latent prints as evidence into the department property room and document this piece of evidence on the NIBRS report as well as in the narrative.

Should the officer have a potential suspect, the officer shall include the information in a supplemental/narrative report requesting a comparison of the latent lifts to prints of the known suspect. It shall be the responsibility of the person assigned to the case to have such comparison conducted, if prints are available for the suspect.

83.2.4 Equipment and Supplies

It is the policy of the Miami Township Police Department to thoroughly investigate crime scenes and traffic collision scenes and to ensure that such duties are performed in an efficient manner on a 24-hour basis by qualified personnel.

It is the responsibility of the Investigations Supervisor to maintain a call out schedule of investigative personnel for the purpose of processing crime scenes.

It is the responsibility of the Patrol Division Supervisor to have scheduled traffic safety unit personnel for the purpose of providing for the processing of traffic collision scenes. Should a traffic safety unit member be unavailable, a district patrol car will respond to process the scene.

Miami Township Police Department maintains in each marked patrol unit and Detectives vehicle, equipment for the collection of evidence. Each vehicle is equipped with equipment and supplies used for the processing of scenes for the following purposes:

- Recovery of Latent Fingerprints – Latent Fingerprint Kit
- Photography – Digital Camera/District Phone
- Sketch of the Scene – Forms and Diagramming Materials

- Collection and Preservation of Physical Evidence – Barrier Tape and Evidence Collection Materials

Miami Township Traffic Safety unit vehicles shall be equipped with additional items needed to conduct technical accident investigations, including:

- Measuring Wheels
- Spray Paint & Chalk
- Portable Breath Testing Equipment

Miami Township Police Department maintains more extensive crime scene processing equipment in the Crime Scene Response Trailer which may be utilized at scene investigations as needed. These items are maintained by the Investigations Division and shall be made available as needed.

83.2.5 Procedures, Seizure of Electronic Equipment

Computers and digital media are increasingly involved in unlawful activities. The computer may be contraband, fruits of a crime, a tool of the offense or a storage container holding evidence of the offense.

It is not always a computer with the hard drive contained inside that will be the focus of a search. If you can store digital information to a device, it is potentially capable of holding evidence. Therefore, any item that can contain digital media must be handled and examined as a computer. The following is a definition of a computer system: all computers, central processing units, all data drivers, hard drives, floppy drives, optical drives, tape drives, digital audio tape drives, and/or any other internal or external storage devices such as magnetic tapes and/or disks. Any terminals and/or video display units and/or receiving devices and/or peripheral equipment such as, but not limited to printers, digital scanning equipment, automatic dialers, modems, acoustic couplers and/or direct line couplers, peripheral interface boards, and connecting cables and/or ribbons. Any computer software, programs and source documentation, computer logs, magnetic audio tapes, and recorders, digital audio discs and/or recorders, any memory devices such as but not limited to, memory modules, memory chips, bubble memory, and any other form of memory device utilized by the computer or its peripheral devices.

When to Obtain a Warrant or Consent

Guidelines outlined in the US Department of Justice Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations suggest the following rules in determining when a warrant or consent is feasible. These are only guidelines based upon district and federal court rulings.

- To determine whether an individual has a reasonable expectation of privacy in information stored in a computer, it helps to treat the computer like a closed container such as a briefcase or file cabinet. The Fourth Amendment generally prohibits law enforcement from accessing and viewing information stored in a

computer without a warrant if it would be prohibited from opening a closed container and examining its contents in the same situation.

- Individuals may lose Fourth Amendment protection in their computer files if they lose control of the files.
- The Fourth Amendment does not apply to searches conducted by private parties who are not acting as agents of the government. Such as computer repair shops, friends or family who uses the computer and find illegal material on the computer.
- The permitted scope of consent searches depends on the facts of each case. Officers should be especially careful about relying on consent as the basis for a search of computer when they obtain consent for one reason but wish to conduct a search for another reason. Be specific about the need for consent if an off-site examination needs to be done advise the owner of the computer or electronic evidence the reason for the need of consent and the criminal investigation. Any investigations outside the scope of consent may be unconstitutional and may be challenged through appeal.
- Co-users of a computer will generally have the ability to consent to search of its files. However, when an individual protects his/her files with passwords, and has not shared the passwords with others who also use the computer, the authority of those other users to consent to search of the computer will not extend to the password protected files. Conversely, if the co-user has been given the password by the suspect, then he/she probably has the requisite common authority to consent to a search of the files.
- Absent an affirmative showing that the consenting spouse has no access to the property searched, the courts generally hold that either spouse may consent to search all the couple's property.
- In some computer crime cases, the perpetrators are relatively young and reside with their parents. When the perpetrator is a minor, parental consent to search the perpetrator's property and living space will almost always be valid. When officers would like to search an adult child's room or other private areas, however, officers cannot assume that the adult's parents have authority to consent. Although courts have offered divergent approaches, they have paid particular attention to three factors:

    - The suspects age
    - Whether the suspect pays rent; and
    - Whether the suspect has taken affirmative steps to deny his or her parents' access to the suspects room or private are.

  When suspects are older, pay rent, and/or deny access to parents, courts have generally held that parents may not consent.
- When Detectives suspect that a network account contains relevant evidence, they may feel inclined to seek the system administrator's consent to search the contents of that account. As a practical matter, the primary barrier to searching a network account pursuant to a system administrator's consent is statutory, not constitutional. System administrators typically serve as agents of "provider(s) of electronic communication service" under the Electronic Communications Privacy

Act ("ECPA"), 18 U.S.C. §§2701-2712. ECPA regulates law enforcement efforts to obtain the consent of a system administrator to search an individuals ACCOUNT. See 18 U.S.C. § 2702-2703. Accordingly, any attempt to obtain a system administrator's consent to search an account must comply with ECPA. To the extent that ECPA authorizes system administrators to consent to searches, the resulting consent searches will, in most cases, comply with the Fourth Amendment. Most fundamentally, it may be that individuals retain no reasonable expectation of privacy in the remotely stored files and records that their network accounts contain. Check with the company or governmental agency policy to decide if all files stored on company network servers are private.

- When possible, it is best to obtain a search warrant over consent. If consent is obtained a search warrant should be obtained as soon as contraband is located on a computer or computer system.
- A municipal court search warrant is sufficient to seize computer systems from a residence.
- To view any computer system a search warrant from Common Pleas Court is required.

Exigent Circumstances

Under the "exigent circumstances" exception to the warrant requirement, officers can search without a warrant if the circumstances "would cause a reasonable person to believe that entry…was necessary to prevent physical harm to the officer or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts. In determining whether exigent circumstances exist, members should consider:

- The degree of urgency involved.
- Whether the evidence is about to be removed or destroyed.
- The possibility of danger at the site.
- The ready destructibility of the contraband.

It is rare that exigent circumstances will apply in computer or cyber crime offenses. Because of the fact that it is rarely necessary to access a computer system to protect life or the destruction of evidence officers should not access computer systems without a warrant or consent unless a life is at risk by failing to do so. Officers must also be cognizant that they can not create the exigent circumstances. If an officers' presence at the scene requires the urgency, then exigent circumstances do not apply as relates to the destruction of evidence.

Plain View

Evidence of a crime may be seized without a warrant under the plain view exception to the warrant requirement. To rely on this exception, the officer must be in a lawful position to observe and access the evidence, and its incriminating character must be immediately apparent. For example, if an officer conducts a valid search of a hard drive

and comes across evidence of an unrelated crime while conducting the search, the officer may seize the evidence under the plain view doctrine. The plain view doctrine does not authorize officers to open and view the contents of a computer file that they are not otherwise authorized to open and review.

Searches Incident to Lawful Arrest

Pursuant to a lawful arrest, officers may conduct a "full search" of the arrested person, and a more limited search of his surrounding area, without a warrant. Due to the increasing use of handheld and portable computers and other electronic storage devices, officers often encounter computers when conducting searches incident to lawful arrests. Suspects may be carrying pagers, cellular telephones, tablets, smart watched, Personal Digital assistants (such as Palm Pilots), or even laptop computers when they are arrested. Does the search-incident-to-arrest exception permit an officer to access the memory of an electronic storage device found on the arrestee's person during a warrantless search incident to arrest? In the case of electronic pagers, the answer clearly is "yes". Relying on Robinson, courts have uniformly permitted officers to access electronic pagers carried by the arrested person at the time of arrest. Courts have not yet addressed whether Robinson will permit warrantless searches of electronic storage devices that contain more information than pagers. The limit on this argument is that any search incident to an arrest must by reasonable. While a search of physical items found on the arrestee's person may always be reasonable, more invasive searches in different circumstances may violate the Fourth Amendment (holding that Robinson does not permit strip searches incident to arrest because such searches are not reasonable in context). For example, the increasing storage capacity of handheld computers suggests that Robinson's bright line rule may not always apply in the case of electronic searches. Because most cell phones have the capacity of a computer or computer system they need to be regarded as such. Although pagers fall under a search incident to arrest the information contained on those devices differs form information stored on cell phones. As a result, cell phones, digital media cards, or other devices capable of storing information as a computer are not an exception to a search warrant requirement. These devices fall under the same guidelines as a computer. If probable cause exists to seize these items, they may be taken but not viewed. To view these items specific consent of the owner or a Common Pleas Search Warrant is required to view any of this information.

Seizing Electronic Evidence

Upon establishing probable cause for a search warrant, obtaining consent or an exception to the warrant rule, members must use appropriate collection techniques provided through training or policy so as not to destroy, alter or compromise electronic evidence.

When a situation arises where the electronic evidence to be seized is too complicated to properly determine the best method of collection, RECI or a computer seizure expert shall be called on for their knowledge and training.

- Secure the scene; remove anyone on or near any computers, cameras or other electronic or digital evidence.

- Isolate Network devices connected to computers i.e. routers, modems, wireless access points. Disconnect power from the back of network devices.
- Photograph and document the scene to be seized. Include the monitor screen if it is on.

    - Do not press any key on the keyboard or move the mouse to wake the computer or to turn on the monitor screen.

- Do not turn computer on if it is off. When finding a computer that is on, remove the power cord from the back of the computer. If you are unable to unplug the power cord from the rear of the computer unplug the power cord from the wall.
- Photograph PC to show condition and all connections. Use numbering or color-coded labels to show what wire goes to which connection. Mark ports with an X that are not connected to anything.
- Upon securing PC in a safe area, search the rest of the area for other electronic or non-electronic evidence, i.e. notepads with passwords, email address list, cell phone bills, floppy disks, CD-R, DVD-R, USB flash drives, IPods, Digital Cameras or any other possible device that can store digital information and that is within the scope of the search warrant or consent.
- Before releasing the suspect or incarcerating them, do a thorough search for digital evidence.

    - Be aware of digital storage devices in or disguised as watches, key fobs, sunglasses, pens, bracelets, etc.

- When transporting digital evidence treat it as fragile cargo.

    - If possible, use the original boxes or containers to package evidence.
    - Transport evidence in the rear floorboard of police vehicles.
    - Keep away from radios or any other electromagnetic devices and any other hostile environments for electronic components.
    - Do not store computers in plastic bags or other media such as Styrofoam that can cause static electricity to accumulate. This can damage property and destroy evidence.

<u>Internet Investigations</u>

When determining whether the electronic evidence needing to be seized is stored on an Internet Service Provider's or Internet Web Site's network, the investigating officer will send a letter by mail or fax on departmental letterhead to the Internet Service Provider to preserve the electronic evidence as soon as possible under 18 U.S.C. 2703(f) until a subpoena or warrant for the information can be obtained.

<u>Examinations</u>

Forensic examinations of all electronic and digital evidence will be done by persons who are trained Computer Forensic Specialists. These persons will require a copy of the

search warrant or consent form upon transfer of the evidence. When possible, RECI will perform all forensic computer examinations.

83.2.6 Report Preparation

An officer charged with processing a crime scene will prepare a supplemental report to the NIBRS report describing the sequence of events associated with a scene investigation. The report shall contain the following:

- Time of Notification;
- Date and Time of Arrival at the Scene;
- Narrative of the Officers Action at the Scene, to Include Evidence Collection Procedures Taken.

An officer charged with processing a traffic collision scene will complete all Traffic Collision Forms required by the State of Ohio.