COUNTY OF MONROE
OFFICE OF THE SHERIFF
ROCHESTER, NEW YORK

GENERAL ORDER POLICE BUREAU	DATE OF ISSUE NOVEMBER 29, 2022	EFFECTIVE DATE NOVEMBER 29, 2022	NO. 058-22
SUBJECT: GENERAL ORDER Digital Forensics Unit		DISTRIBUTION Police Bureau Personnel	AMENDS
REFERENCE:			RESCINDS PBGO-058-17

PURPOSE: To establish policy and procedure for conducting digital forensic examinations by the Monroe County Sheriff's Office Digital Forensics Unit.

POLICY: It shall be the policy of the Monroe County Sheriff's Office (MCSO) to provide digital forensic examinations, digital evidence recovery services and expert witness testimony of digital evidence seized during the course of a criminal investigation to this and other law enforcement agencies. Digital forensic examinations shall only be conducted by trained examiners and administered consistent with all applicable federal, state and local laws within the guidelines set forth in this order while also following current best practices for digital forensics.

Definitions: Digital forensics – the identification, acquisition, authentication, reconstruction, examination and analysis of digital information on electronic media. It often involves creating a faithful copy of the media in a manner that does not alter the original.

* Digital Evidence - Internal or external hard drives, solid state drives (SSD), USB flash drives, compact discs/DVDs, floppy disks, smart cards, tape, computers (desktop, laptop, servers), personal digital assistants (PDAs), media players, digital cameras, tablets, global positioning system (GPS) devices, mobile communication devices (cellular telephones, "smartphones"), wearable devices (smart watches, fitness trackers), drones or other devices designed to hold, interpret or manipulate information stored in digital format.

Digital Evidence Collection Specialist -- A sworn or civilian member of the Monroe County Sheriff's Office trained in the collection of digital evidence.

Digital Forensics Examiner – A sworn or civilian member of the Monroe County Sheriff's Office trained in digital evidence seizure and recovery.

I. Authorization

Digital forensic examination may be authorized when consistent with federal, state and local laws and MCSO policy.

II. Who may Request Digital Forensic Services

A. Police Bureau members of the Monroe County Sheriff's Office Patrol or Criminal Investigation Section (CIS) may initiate a request for digital forensic services

B. District Attorney's Office.

C. Outside law enforcement agencies.

III. Procedures for Requesting Digital Forensic Services

A. Police Bureau Road Patrol Personnel

* 1. A deputy should have his/her request for digital forensic services reviewed by a CIS Sergeant or Digital Forensic Unit designee.

* 2. When the CIS Sergeant/Digital Forensic Unit designee decides that digital forensic services are in order, the deputy will contact an agency examiner or the unit supervisor.

3. Upon being advised for the need of digital forensic services, the examiner will review the specifics of the investigation and may direct that other investigative attempts be conducted prior to beginning forensic services.

B. CIS Personnel

1. Members of the Criminal Investigation Section may contact the unit supervisor or a Forensic Examiner directly for digital forensic services.

2. The specifics of the investigation will be reviewed with the Forensic Examiner to determine if digital forensic services are feasible.

C. How to Handle Requests by Outside Agencies or Other MCSO Bureaus

1. Any examination requests from outside agencies require the approval of the Captain of the Criminal Investigation Section (CIS) or his/her designee.

2. Upon approval for services, the specifics of the investigation will be reviewed with the examiner to determine if digital forensic services are feasible.

IV. Procedures for Digital Forensic Services

This policy shall apply only in those cases where data residing on computer systems, recording devices and media are being sought as evidence in an investigation.

A. Seizure

Seizure is a vital part of digital evidence collection. It may involve the process of capturing live, volatile data (such as data existing in a computer's memory while powered on) that could be lost if not captured at the time of collection. It could also include preserving data on a device so that it cannot be altered at a later time, such as placing a mobile communication device in "airplane mode" to prevent outside communication to/from the device. In addition, if data encryption is discovered on a powered-on device, imaging the device at the time of seizure may be the only chance one has of obtaining any data from it. Properly seizing data will ensure that the evidence is not altered or lost

1. No member, except those designated employees who are properly trained in handling digital evidence or who are acting under the direction of such employees, shall power-off, disconnect, power-on or access a computer system, recording device or recording media that is to be seized.

2. When it is determined that digital evidence is to be seized and processed, and neither an examiner nor collection specialist is available,

MCSO personnel shall contact the digital forensic examiner or unit supervisor for assistance. This assistance may be provided verbally to those personnel located on-site.

3. With prior approval, digital forensic examiners from the Monroe County Crime Lab may be contacted to assist with seizure of digital evidence if a MCSO digital forensic examiner or evidence collection specialist is not available.

4. Any questions regarding equipment seizure (wording of search warrants, etc.) can be addressed by contacting the digital forensic examiner or unit supervisor.

B. Transport

1. The digital forensic examiner or digital evidence collection specialist tasked with the seizure in question will handle the transportation of the seized equipment, unless other approved arrangements are made. A qualified digital forensic examiner or digital collection specialist must give approval in these instances.

2. If a digital forensic examiner or evidence collection specialist is unable to physically assist in the transportation of the seized items, then the following precautions must be adhered to:

a. All items should be packaged in a manner suitable for safe/secure transport;

* b. All items should be attempted to be preserved in a manner that does not effect their potential for data recovery through a forensic process - always follow current "best practices", i.e – if powered on typically device should remain powered on;

b. All items shall be labeled so they are readily identifiable; and,

d. At no time should items be placed on or near devices that produce strong magnetic fields (i.e. radio equipment in the trunk of a patrol vehicle, etc.).

C. Storage

* 1. All digital evidence seized for the purposes of analysis will be secured in the Property Management Office, CIS Technician's Lab or in the Digital Forensic Unit's evidence storage room by a digital forensics collection specialist (unless directed by a member of the digital forensics unit) prior to the end of the member's tour of duty. If the Property Management Office is closed, the evidence will be secured in accordance with MCSO general orders. Digital evidence may be stored in an approved area until analysis is complete.

2. If a computer, or related media, is collected solely for the purposes of determining ownership, it is not necessary for a digital forensic examiner or digital evidence collection specialist to assist. In these instances, the assigned member may handle the collection and subsequent submission of the item(s) to the Property Management Office through normal procedures. The member may contact the digital forensic examiner for assistance at his/her convenience.

D. Reviews and Examinations/Analysis

1. All requests for reviews, examinations and analysis must include a copy of the search warrant or signed consent form before a digital forensic examiner can take action. Absent a search warrant, the decision to go forward with an examination is at the

discretion of the digital forensic examiner, per MCSO guidelines. In the event of abandoned property or the owner is otherwise unknown, a search warrant or consent form may not be required.

2. A request form must also be submitted to the digital forensic unit. The request should include a reason for the examination as well as a description of the particular evidence the member is seeking to locate (photographs, financial records, email, documents, etc.). The request should also include possible search terms to target the evidence sought.

   In addition, any usernames, passwords, encryption keys, personal identification number (PIN), swipe patterns or other types of security information should be included, if known. Deputies should make every effort to ascertain passwords or other security information prior to the collection of devices.

3. Other relevant documentation such as reports, FIFs, etc., may be submitted to assist with the examination.

4. The time frame for completion will depend on the volume of materials seized in combination with the reason for seizure. Reasons for seizure will generally fall within one of the following categories:

   a. Reviews- These are the least obtrusive investigations and generally involve an overall look at the system type, size and operating system. They are often done for the purposes of determining the existence of such things as pornography or Internet access to unauthorized sites. As stated above, they may also be done to determine ownership on lost and found or stolen property.

   b. Examinations- These are normally done in an effort to locate a specific file or piece of data, involving a specific crime or activity, which is known or highly suspected to exist on the media in question.

   c. Analysis- Involves a complete and detailed review of the submitted media. This is the most obtrusive investigation and will generally take the longest period of time to complete.

5. Priority for reviews/examinations/analysis will be given to MCSO investigations. Digital evidence may be submitted by other agencies, but they will be subject to the needs of the MCSO.

6. With prior approval from the Captain of CIS or his designee, digital evidence may be taken to the Monroe County Crime Lab, the Regional Computer Forensics Laboratory (RCFL), the New York State Police digital forensics unit or any vendor with expertise in digital forensics for examination.

E. Dissemination

Upon completion of analysis, the digital forensic examiner will:

1. Send a report of the findings to the requesting deputy/investigator or other agency representative.

2. Maintain a copy of the findings in the digital forensics unit.

* 3. The deputy/investigator is responsible for materials needed for discovery; If an arrest is made, a request for forensic evidence/materials to be submitted to the District Attorney's Office can be made to the Digital Forensic Unit at which point that transfer will be initiated.

F. Disposition

1. Final dispositions or destruction of evidence shall be done in accordance with general orders or, when applicable, at the discretion of the court or the District Attorney's office.

2. Evidence released by the court or District Attorney's office shall be returned to the owner as soon as practical.

3. If the evidence contains contraband (such as child pornography), the original evidence item(s) and all copies will be disposed of according to best practices for data sterilization/destruction prior to returning to the owner, at the discretion of the Captain of CIS or his designee.

V. Roles and Responsibilities

A. Deputy/Investigator

1. It is the responsibility of the officer or investigator on-scene to notify his/her immediate supervisor in those instances where handling digital media is required.

2. Any deputy or investigator who knows that digital media may be encountered on a search warrant is responsible for making arrangements before the execution of the warrant to have a person trained in proper handling techniques available as set forth in this general order.

B. Supervisor

In those instances where digital media is encountered and no on-scene personnel are trained in the seizure of such media, it is the responsibility of the digital forensics unit supervisor to contact the digital evidence collection specialist.

C. Digital Evidence Collection Specialist

1. The digital evidence collection specialist will ensure that all procedures set forth in this general order and any unit procedures are adhered to with regards to the seizure, transportation, preservation and analysis of digital media.

2. In those circumstances where it is necessary to have a digital evidence collection specialist called out, it will be the responsibility of the digital forensics unit supervisor to coordinate a response to the scene or to make other arrangements for the proper handling of the media under the guidelines set forth in this general order.

VI. Training and Maintenance

A. The Monroe County Sheriff's Office shall maintain the equipment, tools, software, licenses and supplies necessary to collect and preserve electronic evidence and to conduct forensic examinations of the digital evidence.

B. Digital forensic examiners will be trained and certified by an accredited digital forensics training program. Examiners will work within the scope of their training and certification(s).

C. Departmental digital forensic examiners will ensure they adhere to guidelines required to maintain their certification with the organization that certified him/her.

D. Departmental digital forensic examiners shall maintain proficiency and knowledge of current forensic practices by receiving continuing education. This can be accomplished through attendance at digital forensics conferences or training courses, or through online digital forensics training offered via the Internet, or through any other means deemed appropriate. The forensic examiner will ensure he/she attains at least the minimum number of continuing education credits/hours set forth by the organization granting his/her certification.

E. Training of digital evidence collection specialists shall be conducted by a digital forensic examiner or via an approved training program (such as the NW3C).

By Order of the Sheriff,

Todd K. Baxter