ORLANDO POLICE DEPARTMENT POLICY AND PROCEDURE

1630.3, COMPUTER/DIGITAL EVIDENCE AND THE DIGITAL FORENSIC LAB

EFFECTIVE:	11/12/13
RESCINDS:	1630.2
DISTRIBUTION:	ALL EMPLOYEES
REVIEW RESPONSIBILITY:	PROPERTY SECTION COMMANDER
ACCREDITATION CHAPTERS:	27
CHIEF OF POLICE:	JOHN W. MINA

CONTENTS

POLICY:

It is the policy of the Orlando Police Department to preserve, collect, and examine any computer-related or digital evidence linked to criminal activity. The Digital Forensic Lab has been established to provide specially trained digital forensic examiners to assist the assigned officers and detectives. The digital forensic examiners are trained in the collection and examination of various types of magnetic and electronic media found within computer systems, cellular telephones, digital cameras, and other electronic storage media. The digital forensic examiners are able to provide sworn and non-sworn personnel with technical advice for the preparation of search warrants, the seizure of computers, digital storage media, and the recovery and examination of relevant evidence.

PROCEDURES:

1. DIGITAL EVIDENCE

Digital Evidence: Evidence contained within any form of magnetic or electronic media. Digital evidence is found in, but not limited to, hard drives, USB drives, compact disks (CD), digital versatile disks (DVD), floppy disks, Zip disks, Jaz disks, flash memory cards, magnetic tape, Secure Digital (SD) cards, digital cameras, Subscriber Identity Module (SIM) cards, cellular telephones, Personal Data Assistants (PDA) and any other memory developed for the storage of electronic data or information.

a. Any first responder who encounters a computer or data storage device that he or she believes may contain evidence of a crime should establish probable cause or consent for the seizure of the system or device.

b. Once probable cause has been established, a search warrant or Digital Evidence Consent to Search Form (Attachment B) should be completed for the seizure of the data to be examined. If there is a danger that electronic evidence may be destroyed, altered or overwritten, the evidence should be safeguarded and secured pending a search warrant or warrant exception (e.g., exigent circumstances).

c. A Digital Forensic Examiner should be consulted to ensure a properly structured and worded search warrant is drafted.

d. Unless exigent circumstances require it, digital and electronic media should not be accessed without first consulting a digital forensic examiner. Such evidence should, whenever possible, be maintained in the condition it was at the time of the seizure.

If circumstances require access to evidence prior to a forensic examination, the member shall document the date, time and description of evidence viewed or accessed, and shall provide that written detail to the digital forensic examiner.

e. Electronic evidence voluntarily provided by bystanders and uninvolved witnesses may be secured as reasonably necessary under the circumstances at the discretion of the officer (in the spirit of accommodating helpful citizens). If a bystander or witness wishes to email or permit the member to extract the relevant data via a CelleBrite Universal Forensic Extraction Device (UFED), follow the procedure outlined in Section 3. The member must document the witness' involvement and the collection method to facilitate the witness' authentication of the evidence later.

2. STORAGE DEVICES

If a first responder encounters a data storage device and has probable cause to believe it contains evidence of a crime, he or she should seize the device.

a. The disk, tape, or other form of digital media should be handled so as to not damage the data. Some storage media utilize a magnetic medium. The storage device should be kept away from any magnetic fields or high temperatures.

b. The storage devices should be packaged separately from peripherals, cables or other evidence to facilitate later examination. Do not place evidence tape directly onto any disk, tape, or CD: these items should be placed into appropriate storage containers.

A basic guide for the seizure of all computer-related evidence, entitled "Electronic Crime Scene Investigation: A Guide for First Responders," is available at OPD Online under Training References.

Digital forensic examiners are available to give advice, instruction and assistance when appropriate. Refer to the current issue of OPD P&P 1103, Call-Out Procedures, for after-hours procedures and contact information.

3. HAND-HELD COMMUNICATION DEVICES

This section encompasses a variety of hand-held devices that are used for or have the potential to be used for communication. These devices include cellular telephones, personal data devices, and hand-held tablets such as the iPad, Samsung Galaxy or Microsoft Surface. Within this policy, all of these devices will be referred to as cellular telephones.

The Florida Supreme Court ruled that a warrantless search of a mobile phone incident to the arrest of an individual violates the Fourth Amendment of the U.S. Constitution, *Smallwood v. Florida, 113 So.3d 724 (Fla 2013)*. The Court said that law enforcement officers rightly seized the cell phone, but a search of the data required a search warrant or a warrant exception.

Officers may not search an arrestee's mobile phone incident to arrest: there must be probable cause to believe that evidence of a crime is within the phone, along with the existence of either a signed search warrant or a recognized exception to the search warrant requirement (e.g., consent, exigent circumstances).

If a delay to obtain a search warrant is likely to result in destruction of evidence, the officer must articulate the basis for that belief, and may: 1) download device data via an available Universal Forensic Extraction Device (UFED) pending a search warrant; and/or 2) examine the phone to obtain the evidence for which the exigencies apply.

Cellular telephones are widely used and collected from witnesses, victims and suspects in order to recover necessary evidence and intelligence information. Assuming a proper factual basis exists to examine it, there are many levels of processing that can be performed to obtain the information from a cellular telephone. If an officer, detective or crime

scene investigator (CSI) collects a cellular telephone and needs to obtain basic phone data, the device telephone number or the phonebook, the officer/detective/CSI can utilize an authorized CelleBrite UFED to process the telephone. In some cases, depending on the cellular telephone model, the standard CelleBrite system may be able to also extract text messages, call history, pictures, video and audio data. The CelleBrite UFED system fielded for agency use outside of the Digital Forensic Lab is located in the Drug Enforcement Division building. The CelleBrite UFED system is easy to use and the instructions are within the case.

a. Members shall ensure that there is a factual and legal basis to support data extraction and subsequent search of the cellular telephone.

b. To process the cellular telephone, the member may need to log into the device. If the device is password-protected and the password is not obtainable, the member may attempt to acquire the device data with the CelleBrite UFED anyway. If the CelleBrite UFED cannot acquire the data without the password, the member should power-off the device and submit it to Property and Evidence. A Digital Evidence Examination Request form (Attachment A) should be completed. The processing request and legal search authority documentation should be submitted to the Digital Forensic Lab for further processing.

c. The member should turn off the telephone's ability to communicate with its service provider. This procedure will prevent new data or calls from being received by the telephone and altering or overwriting existing data. The menu to turn off this capability is normally located within the settings area of the device. Place the telephone into "airplane" mode. If the device has WiFi or other transmitters listed, they should also be turned off.

d. The member should disable any password, pattern or PIN lock setting immediately. When possible, obtain the password, pass code, or pattern from the person in possession of the phone. If this is not possible, set the phone so that it will not automatically lock. This will allow the member to transport the telephone to a location where the processing will be conducted without the lock engaging.

e. The CelleBrite UFED system will display a listing of what type of information it is capable of extracting from each specific model. The cellular telephone model is normally listed within the settings menu area under the device or phone information menu. If not, the model is written on the product label under the battery. If the phone is powered off, to remove the battery, the password lock may be engaged. Prior to powering off the telephone, the password or PIN should be disabled. If all of the information required for the investigation is not supported by the CelleBrite UFED system, the member can run the process to obtain the supported information. The telephone should then be powered off and submitted into evidence and a processing request submitted.

f. If the member is unable to obtain the required data (to include deleted data, if required) from the cellular telephone using the CelleBrite UFED, the telephone should be submitted to Property and Evidence, and a request for processing should be submitted to the Digital Forensic Lab.

g. When submitting any cellular telephone to Property and Evidence, if the cell phone is not locked, the member should navigate through the setting and ensure that the pass code or PIN lock is disabled, if possible. The cell phone should then be powered off. Remove the battery and submit both handset and battery together to Property and Evidence.

h. All media viewed or settings changed must be documented in the member's statement, supplement or report. If the CelleBrite UFED is utilized, the member shall thoroughly document the procedure within their report. Copies of the electronic data extracted from a telephone should be saved/burned to disk, submitted into evidence and a copy provided to the State Attorney's Office.

i. If the member notices that the CelleBrite UFED system or data cables are damaged or missing, they shall notify the Digital Forensic Lab so that a replacement can be obtained.

j. If a member wishes to take a CelleBrite device to the field for use, they must first sign it out on the property form as its current custodian. The property form is in the storage area with the CelleBrite UFED system. The CelleBrite UFED must be returned as soon as practical after the member completes the current operation.

k. Training on the use of the CelleBrite UFED system is coordinated through the Digital Forensic Unit.

4. PERSONAL COMPUTER AND LAPTOP SYSTEMS

A desktop computer, laptop or other data storage device that a member has probable cause to believe contains evidence of a crime may be seized with a search warrant or warrant exception. (35.05c)

The following guidelines are directed toward both laptop and stand-alone desktop computer systems (not to include networked computers). Only properly-trained agency members should collect a computer system that is in a powered-on state. All Crime Scene Investigators (CSIs) are trained on the proper procedures for collecting a computer system.

a. If the computer is **ON,** it **SHOULD NOT BE TOUCHED**. If information is displayed on the monitor, the monitor should be photographed. If there is a "screen saver" program running, the member collecting the computer may jiggle the mouse or press the SHIFT key to deactivate the screen saver. Do not push any other key/buttons or click any desk icons. Digital photographs should be taken of the items displayed on the system's monitor and connected devices. If needed, a digital forensic examiner may be contacted for further instructions.

b. If the computer is **OFF, DO NOT** turn it on. If needed, contact a digital forensic examiner for further instructions.

c. The member may label cables and device ports to which each cable is connected.

d. Laptop computers should be packaged with their main batteries removed. The battery and power cable should be placed into a separate container (bag or envelope) within the same evidence package as the laptop.

e. Devices to be electronically processed should be packaged separately from the other evidence, peripherals and cables.

f. To maintain the integrity of any evidence, only persons properly trained in the seizure of a computer should collect a computer system containing evidence to be processed.

g. Digital forensic examiners will provide advice and instruction when appropriate. When necessary, the digital forensic examiners will respond to the scene and collect the computer system in accordance with accepted standards of digital forensic procedure.

5. RELATED DOCUMENTATION

During the seizure of computer-related evidence, the digital forensic examiner, officer or CSI may attempt to find and photograph (before collection) all related documentation and materials on or in the area of the system. Items to be seized include software, manuals, printouts, check stock, Post-It Notes, notebooks, day planners, rolodex, and any other items associated with the equipment. These items are frequently related to the criminal activity and may contain additional evidence and passwords to files or programs. Any information contained within these documents that have investigative use should be copied prior to the item being submitted to the Property and Evidence Section. The copies should be forwarded to the examiner along with the examination request.

6. NETWORKED SYSTEMS AND SERVERS

Properly-trained digital forensic examiners are the only agency personnel authorized to seize corporate network and server-based systems.

a. With limited exceptions, servers shall be **powered down properly** to avoid any system damage or loss of information. Damage to the system may disrupt legitimate business and create potential liability. When practical, the digital forensic examiner will coordinate with on-site personnel familiar with the server in order to determine the most appropriate course of action. In cases requiring a deviation from a normal server shutdown, the digital forensic examiner will specify the reasons within the examination report.

b. A legitimate business' computer system should only be seized when necessary and then only with the appropriate warrant or warrant exception.

c. Digital forensic examiners will strive to minimize the impact of the computer examination on the legitimate operation of a business. This can often be accomplished through execution of a search warrant or lawful warrantless examination during the hours of the least computer usage.

d. The examination should be only as intrusive as is necessary and proper for the investigation (e.g., if the suspect only had access to his computer workstation and specific network drives, the entire company's computer network should not be seized).

e. If an entire system must be seized from an entity with legitimate business operation, it should be returned as soon as practical and appropriate.

7. LOCAL SEARCH WARRANTS

Digital evidence search warrants should be written in accordance with current OPD guidelines (current issue of P&P 1402, Search Warrants). The officer must ensure that there is an articulated link between the electronic data and criminal activity or evidence.

a. If an officer who is otherwise lawfully on the premises develops probable cause to believe that a computer or other data storage device contains evidence of a crime, the device may be seized pursuant to a separate search warrant or warrant exception (e.g., plain view). If the computer or data storage device is located in an area in which an individual has a reasonable expectation of privacy, a search warrant (or warrant exception) will be required to enter and seize said evidence. A forensic examination of the evidence requires a search warrant where the device(s) are known, or which may require a separate search warrant post-seizure.

b. A digital forensic examiner shall be consulted during the preparation of any search warrant intended to seize computers or digital evidence that will be forensically examined.

c. The digital forensic examiner will ensure that the search warrant meets the current accepted format and structure necessary to accomplish a forensic examination..

d. The Police Legal Advisor will review all search warrants prior to obtaining a judge's signature.

e. When an officer is planning to conduct a search warrant involving the seizure of a computer or computer system, the officer will notify a digital forensic examiner or the Technology and Forensics Unit supervisor at least 24 hours prior to the execution of the warrant, when possible.

Templates for a Computer Search Warrant and a Cellular Telephone Search Warrant are provided in the Microsoft Word Add-Ins Investigative Forms/Warrants menu.

8. INTERNET SERVICE PROVIDERS

Valuable information can be obtained through any of the Internet Service Providers (ISP). Depending on the type of information sought, different court documents are required.

These requests will typically be generated from the Investigative Services Bureau. Patrol officers who intend to submit a subpoena or search warrant to an ISP should consult with any digital forensic examiner, a CID detective assigned to the type of crime being investigated, or a member of DED (as applicable).

a. INVESTIGATIVE SUBPOENA: An investigative subpoena will allow the member to obtain basic subscriber information and detailed account and billing information.

b. COURT ORDER: A court order is typically used to obtain transactional information such as cellular tower information. A court order will also permit the member to obtain the detailed subscriber, account and billing information.

c. SEARCH WARRANT: A search warrant will allow the investigator to obtain detailed subscriber, account, and billing information, transactional information, and any stored user files as well as emails and Internet history.

d. Depending on the ISP and the court order required, the court order may need to be issued by a court having geographic jurisdiction for the ISP.

e. ISP data and items may be time sensitive, so preservation and prompt application is required.

f. For specifics on obtaining information from an ISP, contact a digital forensic examiner.

9. EXAMINATION REQUESTS

During any investigation, if an officer or detective requires a computer or other electronic data storage device examined, a Digital Evidence Examination Request form (Attachment A) shall be completed.

a. The examination request will be submitted to a digital forensic examiner or the Technology and Forensics Unit supervisor. The submitting officer should provide detailed information describing what information they believe to be contained within the data.

b. The submitting officer will attach a copy of the signed Digital Evidence Consent to Search form (Attachment B), search warrant or detailed warrant exception.

c. The submitting officer shall also attach a copy of any pertinent documentation or possible passwords with the request.

d. The submitting officer shall indicate the priority of the examination and when he or she expects the examination to be completed. **This is only a request.** Once an examination has begun, it can take from one day to several weeks to complete. An emergency request must be approved by a lieutenant or higher.

e. If the examination cannot be completed by the time requested, the assigned digital forensic examiner shall notify the submitting officer, who may need to obtain an extension by the court.

10. EXAMINATION PROCEDURES

All examinations will be conducted in accordance with accepted computer forensic standards. All examinations, except those conducted under Section 3, will be conducted by, or under the supervision of, a properly trained or certified Digital Forensic Examiner. Only properly-licensed software will be utilized during an examination.

COMPUTER EXAMINATION LOG: A listing of examinations conducted will be maintained in the Computer Examination Log. The assigned examinations will be completed according to the priority of all cases assigned.

11. DIGITAL FORENSIC EXAMINERS

Each digital forensic examiner will be trained and/or certified in the seizure of computers and digital evidence, digital forensic examinations, and in the use of the primary examination software. (35.05a) During the certification process, a newly assigned digital forensic examiner may conduct examinations under the supervision of a certified examiner.

The City of Orlando, or the examiner, will be licensed to use all the software utilized in the Digital Forensic Lab. This does not include software contained on or extracted from the target device and used to examine that same target device or data.

12. EVIDENCE STORAGE

The Digital Forensic Lab is an authorized evidence storage location. All evidence stored within the lab will be checked out from the Property and Evidence Section indicating the reason why it is out to the Digital Forensic Lab. The Property and Evidence Section will enter and maintain the chain of custody log and indicate that the item(s) are being temporarily stored in the Digital Forensic Lab. (35.05b)

a. Once the forensic images have been acquired and all the systems information is annotated, if there is no longer a need for the system, it should be returned to the Property and Evidence Section.

b. Items stored within the Digital Forensic Lab will be kept separate from other items to ensure the integrity of each case and its evidence.

c. After the examination is completed, the digital evidence file will be archived onto electronic storage media. The archived data will be maintained in accordance with current evidence disposal policy. Evidence requiring long-term storage (more than five years) will be archived to storage disks and submitted to the Property and Evidence Section under a separate evidence number. Items requiring short-term storage (five years or less) may be archived to electronic storage system within the Digital Forensic Lab.

ATTACHMENT A

Digital Examination Request Form

Agency Case #(s)	Orlando Police Department Digital Forensic Lab	Date Received in Lab	By (initials)

Request Date	Date Needed	Priority	Case Status	Manager's Signature (Emergency Only)
		Normal ☐ Priority ☐		
		Emergency ☐	10-15 ☐	

Examination Requested by Name - PLEASE PRINT:	ID #	Rank/Position	Unit	Contact Phone #s

Suspect(s) – Last, First, MI	Race/Sex	DOB	Victim(s) – Last, First MI	Race/Sex	DOB
PLEASE PRINT:	/		PLEASE PRINT:	/	
PLEASE PRINT:	/		PLEASE PRINT:	/	

Offense	Offense Location	Date of Seizure

Please identify the types of evidence/information to be searched for/recovered:

	X		X	
Financial Records	☐	Word Processing/Text Documents	☐	[Other – Please be specific]
* Internet History and log files	☐	Credit card info/Check-writing programs	☐	
* Email/IM/ Text Messages	☐	Child Porn	☐	
Contact Lists	☐	Images	☐	
Call History	☐	Owner Info	☐	

* Note: For Internet- and email-related investigations, please identify any known screen names, ISPs (Internet Service Providers) and other pertinent information for suspects and victims.

Item #	Evidence ID/ Bar Code #	Item Description	Special Instructions

Upon completion of forensic examination, OPD evidence items will be returned to the OPD Property and Evidence Section for secure storage.

ATTACHMENT A Continued

Digital Examination Request Form

Upon completion of forensic examination, OPD evidence items will be returned to the OPD Property and Evidence Section for secure storage.

Case overview, notes and **Key Words** to search for:

General Instructions – Completion of Digital Exam Request Form

- All seized evidence must be appropriately processed and submitted to the Property and Evidence Section.
- Please do not place evidence tape directly on CPUs or any other seized media such as floppy disks, backup tapes, CDs, etc. These items should be bagged and labeled in accordance with crime scene/evidence handling guidelines.
- It is important to **identify what you expect/hope to find** as evidence on the computer or media. Please be as detailed as possible when completing this form. Attach additional sheets if necessary.
- **Please attach a copy of your Search Warrant, Digital Evidence Consent to Search Form or detailed warrant exception, e.g., abandoned property.**
- Attach any **other documentation or passwords,** if applicable.

Orlando Police Department – Digital Forensic Lab
100 South Hughey Avenue
P. O. Box 913
Orlando, FL 32802-0913
407.246.3743

Page 2 of 2

ATTACHMENT B

COMPUTER CONSENT TO SEARCH

Date: _____ Case Number _____

I, _____ hereby freely and voluntarily authorize _____ or any law enforcement agent, State or Federal, to conduct a complete search of the property listed below in which I have or may claim a possessory or other privacy interest.

This property is described as _____

and is under the control of _____

and is located at _____

The items to be searched and seized include any electronic data processing and storage devices, computers and computer systems including central processing units, internal and peripheral storage devices such as fixed discs, external and internal hard drives, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices or other memory storage devices; peripheral input and output devices such as keyboards, printers, video display monitors, optical readers and related communication devices such as modems; together with documentation, operating logs and documentation, software and instruction manuals.

I am giving this written permission to the above named persons voluntarily and without threats or promises of any kind.

_____
Signature

_____
Witness

_____
Witness