"Keep Orlando a safe city by reducing crime and maintaining livable neighborhoods."

ORLANDO POLICE DEPARTMENT POLICY AND PROCEDURE

1630.4, COMPUTER/DIGITAL EVIDENCE AND THE DIGITAL FORENSIC LAB

EFFECTIVE:	12/15/2020
RESCINDS:	1630.3
DISTRIBUTION:	ALL EMPLOYEES
REVIEW RESPONSIBILITY:	PROPERTY SECTION COMMANDER
ACCREDITATION CHAPTERS:	27
CHIEF OF POLICE:	ORLANDO ROLÓN

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), computers, hand held computers (tablets), 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 aside from actions described in Section 3.

   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 forensic tool, 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 (e.g. thumb drive, external hard drive, secure device (SD) card) 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. Contact any digital forensic examiner or the Economic Crimes Unit's Supervisor for after-hours procedures and contact information.

3. HAND-HELD COMMUNICATION DEVICES

Industry best practices will be followed when collecting handheld communication devices. These handheld communication devices may include but not limited to cellphones, smartphones, personal digital assistance (PDA) and handheld computer (tablet). Within this policy, all these handheld communication devices will be referred to as device(s).

The Florida Supreme Court ruled a warrantless search of a mobile phone or any other form of digital media, incident to 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 law enforcement officers rightly seized the mobile device, but a search of the data required a search warrant or a warrant exception.

For a search of a device(s) there must be probable cause to believe evidence of the crime is within the device, along with the existence of a signed search warrant or a recognized exception to the search warrant requirement (e.g. consent, exigent circumstances, and destruction of evidence).

A warrant exception, such as consent or exigent circumstances, must exist for a Digital Forensic Examiner to search a device(s) without a warrant. The US Supreme court stated, "Such exigencies could include the need to prevent the imminent destruction of evidence in individual cases, to pursue a fleeing suspect, and to assist persons who are seriously injured or are threatened with imminent injury*." Riley v. California, 134 S. Ct. 2473 (2014).*

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:

a. Seize and secure the device(s) in a way which prevents destruction, if possible
b. Have the device(s) downloaded by a Digital Forensic Examiner utilizing a forensic tool, pending a search warrant
c. Have the device(s) examined by a Digital Forensic Examiner utilizing "Best Practices" to obtain the evidence from which the exigencies apply.

When a device(s) is lawfully collected from witnesses, victims and suspects in order to recover necessary evidence and intelligence information, best practices will be followed to ensure the safe collection of the device(s).

a. Photograph the device(s) and scene
b. If the device(s) is located "powered off" leave it off
d. If the device(s) is located "powered on", keep it on and immediately "shield" the device(s) from the network:
    a. This can be done by placing the device(s) in airplane mode, disconnecting the wireless connection (Wi-Fi) and turning off Bluetooth. For Global System for Mobile Communications (GSM) phones the removal of a Subscriber Identity Module (SIM) card can be removed from the device(s) to keep the device(s) from connecting to the cellular network.
    b. Devices which cannot be "shielded" from the network by the above method, need to be immediately placed in a "Faraday" solution. A Faraday solution may be a Faraday bag, box or room. The Faraday solution is used to block electromagnetic fields reaching the device, as well as stopping any electromagnetic fields being sent by the device. Any device(s) in a Faraday solution must be provided a power source to ensure the device(s) battery is not depleted.
    c. If a Faraday bag is being used to shield the device(s) from the network a battery pack contained inside the Faraday bag must be used to ensure the battery life of the device. The power source provided to the device(s) cannot come from outside the Faraday bag used, as this will break the Faraday shielding.
    d. All Crime Scene Investigators (CSI) are equipped with Faraday bags for the collection of devices.
    e. Digital forensic examiners can provide advice and instruction if needed.

Upon collection of the device(s), any device(s) "powered off" shall be entered into OPD Property and Evidence. If a search of the device(s) is needed follow instructions provided in Section 9.

All device(s), which are "powered on" will be brought to the Digital Forensics lab upon collection. The device(s) does not need to be entered into OPD Property and Evidence, prior to bringing it to the Digital Forensic Lab.

a. If a "powered on" device(s) is collected after-hours, the device(s) will be stored in the CSI lab's cellphone collection area on a power supply. All device(s) will be packaged, labeled and written on the Control Log. An email shall be sent to the digitalforensiclab@cityoforlando.net immediately upon securing the device(s).
b. If the "powered on" device(s)cannot be shielded from the network, the device(s)shall be placed in the Faraday Box located in the CSI lab's cellphone collection area:
    a. <u>Faraday Box Use</u>
        i. All devices need to be kept powered on.
            1. If device(s) are on and unlocked, but the security code is unknown set display to never lock
        ii. Attempt to set device(s)to Airplane Mode:
            1. Airplane Mode should be set ASAP
            2. Verify Wi-Fi is OFF
            3. Verify Bluetooth is OFF
            4. **If Airplane Mode is set the phone shall not be placed in the Faraday Box**.
        iii. If Airplane Mode cannot be set place the device(s) and proper labeled evidence envelope into the Faraday Box and connect the device(s) to a charging cable.

iv. If the device(s) is already in a Faraday bag, place the entire unopened Faraday Bag into the Faraday Box, along with the proper labeled evidence envelope.
    1. Close and seal the lid. You can turn the light on within the box to see.
        1. Open the Faraday Bag
        2. Attach device(s)to charging cable
        3. Slide device(s) into the envelope.
        4. **DO NOT OPEN THE FARADAY BOX TO REMOVE THE FARDAY BAG**

ii. If the **FARADAY BOX LID IS CLOSED** and you cannot put the device(s)into Airplane Mode
    1. **DO NOT OPEN THE FARADAY BOX**
    2. Place device(s)in a Faraday Bag on a battery pack and notify the Digital Forensic Lab immediately
    3. If no battery packs are available call the Economic Crimes Supervisor or Digital Forensic Examiner.

iii. **For all devices placed in the Faraday Box you must send an Email to digitalforensiclab@cityoforlando.net advising the case number and the items are in the Faraday Box.**

During the collection process, whenever possible the member should try to obtain the password, passcode or pattern from the person in possession of the phone. If the device owner is in custody, Miranda must be administered. If consent is denied, passcodes cannot be compelled, even with a court order; however, bio-metric security such as fingerprints, or touch ID can be compelled with a court order. In some cases, if the passcode is not obtained the data cannot be retrieved from the device.

If the password, passcode or pattern for the device has been obtained, it should be verified by the member and documented.

A detailed guide for device collection procedures is available on OPD Online within the Training Reference Guides. Proper device collection procedures should be followed or the ability to extract the device data could be lost. Digital forensic examiners will provide advice and instruction when appropriate.

Only properly trained members may conduct extractions of the device(s). Training is coordinated through the Digital Forensic Lab.

Members shall document all procedures completed, media viewed, or settings changed in the member's statement, supplement, examination notes or report. Copies of the electronic data extracted from a device shall be stored according to Section 12.

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.

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 in a powered off state.

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. A digital forensic examiner should 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. Powered off 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 powered on 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 Economic Crimes 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 SED (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 in person or via electronic mail (digitalforensiclab@cityoforlando.net). 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 digital forensics best practices. All examinations, except those conducted under Section 1, 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. 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, unless meeting the exceptions listed in Section 3. 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. If a device is delivered directly to the Digital Forensic Lab, or submitted to the CSI storage area for charging / use of the Faraday

Box (see Section 3) a log shall be maintained within the Digital Forensic Lab maintaining the chain of custody until such device is properly submitted into Property and Evidence.

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, or properly submitted 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 to the electronic storage system within the Digital Forensic Lab. The archived data will be maintained in accordance with current evidence disposal policy.

P&P 1630.4 12/15/2020

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	ID #	Rank/Position	Div/Unit	Contact Phone #s
Name - PLEASE PRINT:				

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/Time of Incident

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 apps	☐		
* Email/IM/ Text Messages	☐	Child Porn	☐		
Contact Lists	☐	Images	☐		
Call History	☐	Owner Info	☐	Provide UFED Reader ONLY	☐

* 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.

Device Description	Device Location	Password (If Known)

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

- 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.
- All seized evidence must be appropriately processed and submitted to the Property and Evidence Section.
- Please do not place evidence tape directly on seized media such as backup tapes, CDs/DVDs, etc. These items should be bagged and labeled in accordance with current evidence handling guidelines.
- Requests and documents can be emailed to digitalforensiclab@cityoforlando.net. **Please attach a copy of your Search Warrant, Digital Evidence Consent to Search Form or specify the warrant exception, e.g., abandoned property.**
- . Attach any **other documentation or passwords,** if applicable.

Orlando Police Department – Digital Forensic Lab
185 George DeSalvia Way, Suite B
Orlando, FL 32807
407.246.3444

ATTACHMENT B

Digital Evidence Consent to Search

DATE_____ CASE #_____

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 in 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, cellular telephones and other electronic communication devices 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, flash memory devices, secure digital cards, SIM cards 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)