NEW ORLEANS POLICE DEPARTMENT OPERATIONS MANUAL

CHAPTER: 83.2

TITLE: COMPUTERS AND DIGITAL EVIDENCE

EFFECTIVE: 01/14/2018
REVISED: Replaces Policy 814

PURPOSE

This Chapter establishes guidelines for the seizure and storage of mobile devices, computers, and other electronic devices capable of storing digital information. The Chapter also establishes guidelines for the preservation and storage of digital evidence.

POLICY STATEMENT

1. The New Orleans Police Department will adhere to all state and federal laws and regulations of the Louisiana Bureau of Criminal Identification and Information related to the access, use and dissemination of sensitive information received via a law enforcement telecommunications network (R.S. 15:579).

DEFINITIONS

Faraday Bag—A faraday bag is a bag composed of radio signal deflecting material.

Hardware—Physical parts of a digital item such as a memory chip or hard drive.

Laptop computer—A portable computer suitable for use while traveling. Not to be confused with mobile device.

Mobile Device—A mobile device, also referred to as a handheld device or handheld computer, are portable data devices which provide communications, digital photography, navigation, web access, personal information management, and data storage.

FIRST RESPONDER AND INVESTIGATING OFFICER RESPONSIBILITIES

2. The officer or detective must have the legal authority to seize the mobile device, computer, hardware, software or electronic media with a signed warrant and/or valid consent. The officer or detective shall obtain the appropriate permission prior to seizing the equipment and prior to forensic examination by the Digital Forensic Unit. (See: **Chapter 1.2.4 – Search and Seizure** and **Chapter 1.2.4.2 – Search Warrant, Content, Forms and Reviews**).

3. Secure the devices containing the digital evidence by:
   (a) As a general rule of thumb, if the laptop or mobile device is powered off, leave it

off; if the device is on, leave it on.
(b) Isolate the device from communicating with any network (Faraday bag).

4. Officers can obtain Faraday bags from Central Evidence and Property. In the event that a Faraday bag is not available, aluminum foil will prohibit the device from accessing wireless networks.

5. Consider non-electronic evidence on the device such as fingerprints or biological or trace evidence and contact the Scientific Criminal Investigation Section (Crime Lab) to process and analyze this evidence. The device and evidence shall be collected and processed prior to the device being processed by the Digital Forensics Unit.

6. If there is an articulable reason to believe that the computer or mobile device is utilizing encryption mechanisms, authentication mechanisms, pass locks, pass codes, or other security features, the officer should consult with the detectives of the Digital Forensics Unit prior to seizing the electronic device.

7. If the electronic device is powered on and will be placed in storage for any period of time, the investigator shall consult with the Digital Forensic Unit to determine the best method to secure such a device.

8. Upon confiscating the electronic device, the investigating officer or detective shall complete the **Digital Forensic Unit Work Request Form** to have the device processed by the Digital Forensics Unit. The following forms shall be used:
(a) Cellular/Mobile Device Work Request - Form 320
(b) Video Work Request - Form 321
(c) Computer Work Request - Form 322

9. In order for the seized evidence to be examined by a Digital Forensic Examiner, the Digital Forensic Work Order shall be completed and attached to a copy of the applicable Search Warrant or signed Consent to Search when submitted for examination. The Digital Forensics Unit shall be notified about the pending devices at Central Evidence and Property.

VIDEO SURVEILLANCE EVIDENCE

10. The first responder and/or case detective shall attempt to obtain video from the surveillance system while on scene to ensure that video evidence will not be overwritten.

11. If the first responder cannot obtain the video while on scene, he/she shall document the steps taken to obtain the video and contact the Digital Forensics Unit for assistance. It is important to note what steps were taken so that the Digital Forensics Unit can prepare the necessary equipment for extraction. If the first responder was successful in obtaining the surveillance video and the video is stored on removable media such as CD, DVD, or flash drive, follow current departmental guidelines for storing evidence (see: **Chapter 83.1 – Collection and Preservation of Evidence**).

RECEIVING, STORING, AND PROCESSING EVIDENCE

12. Digital Forensics Unit Detectives (forensics examiners) shall retrieve evidence from Central Evidence and Property upon notification and receipt of the appropriate work request form and search authority (warrant). The detectives will process evidence in a timely manner using equipment/procedures accepted by the forensics community for obtaining evidence from electronic and data storage devices.