Computers, Mobile Communication Devices, and Digital Evidence

808.1 PURPOSE AND SCOPE

This policy establishes procedures for the seizure, storage adn analysis of computers, mobile communication devices, digital cameras, digital recorders, and other electronic devices that are capable of storing digital information. All evidence seized or processed pursuant to this policy shall be done so in compliance with clearly established search and seizure provisions.

808.2 SEIZING COMPUTERS AND RELATED EVIDENCE

Computer equipment requires specialized training and handling to preserve its value as evidence. Officers should be aware of the potential to destroy information through careless or improper handling, and, whenever possible, only those trained should physically handle the device. For those not trained, evidence collection on the device should be limited to observations, photographing, and documenting. When others must seize a computer and accessories, the following steps should be taken:

(a) Photograph each item, front and back, specifically including cable connections to other items. Look for a phone line or cable to a modem for internet access.

(b) Do not overlook the possibility of the presence of physical evidence on and around the hardware relevant to the particular investigation such as fingerprints, biological or trace evidence, and/or documents.

(c) If the computer is off, do not turn it on.

(d) If the computer is on, do not shut it down normally, and do not click on anything or examine any files.

    1. Photograph the screen, if possible, and note any programs or windows that appear to be open and running.
    2. Disconnect the power cable from the back of the computer or, if a laptop or portable notebook-style computer, disconnect any power cable from the case and remove the battery.

(e) Handle and transport the computer and storage media with care so that potential evidence is not lost.

(f) Lodge and tag all computer items as per normal procedures. Do not store computers where normal room temperature and humidity is not maintained.

(g) At minimum, officers should document the following in related reports:

    1. Where the computer was located and whether or not it was in operation.
    2. Who was using it at the time.
    3. Who claimed ownership
    4. If it can be determined, how it was being used.

(h) In most cases when a computer is involved in criminal acts and is in the possession of the suspect, the computer itself and all storage devices (hard drives, tape drives, and disk drives) should be seized along with all media. Accessories (printers, monitors, mouse, scanner, keyboard, cables, software and manuals) should not be seized unless as a precursor to forfeiture or they are capable of storing data.

808.2.1 BUSINESS OR NETWORKED COMPUTERS

If the computer belongs to a business or is part of a network, it may not be feasible to seize the entire computer. Cases involving networks require specialized handling. Officers should contact a certified forensic computer examiner for instructions or a response to the scene. It may be possible to perform an on-site inspection, or to image the hard drive only of the involved computer. This should only be done by someone specifically trained in processing computers for evidence.

808.2.2 FORENSIC EXAMINATION OF COMPUTERS

If an examination of the contents of a computer's hard drive or any other storage media is required, forward the following items or information to a computer forensic examiner:

(a) Copy of report(s) involving the computer.

(b) Description of the circumstances authorizing the search (e.g. consent, search warrant, etc.).

(c) Suggestions and items for which to search (e.g. photographs, financial records, e-mail, documents).

808.3 SEIZING DIGITAL STORAGE MEDIA

Digital storage media, including hard drives, should be seized and stored in a manner that will protect them from damage. An exact duplicate of the hard drive may ultimately be made using a forensic computer and a forensic software program by someone trained in the examination of computer storage devices for evidence.

(a) If the media has a write-protection tab or switch, it should be activated.

(b) Do not review, access, or open digital files prior to submission. If the information is needed for immediate investigation, request the department's computer forensic examiner to copy the contents to an appropriate form of storage media.

(c) Many kinds of storage media can be erased or damaged by magnetic fields. Keep all media away from magnetic devices, electric motors, radio transmitters, or other sources of magnetic fields.

(d) Do not leave storage media where they would be subject to excessive heat such as in a parked vehicle on a hot day.

(e) Use protective packaging to secure the media.

808.4 SEIZING MOBILE COMMUNICATION DEVICES

Mobile communication devices such as cell phones, tablets, or other hand-held devices connected to any communication network must be handled with care to preserve evidence that may be on the device including messages, stored data and/or images.

(a) Officers should not, as a matter of routine, attempt to access, review or search the contents of such devices prior to examination by a forensic expert. Unsent messages can be lost, data can be inadvertently deleted, and incoming messages can override stored messages. However, this does not preclude officers from ever searching contents of such devices: circumstances and resources may warrant such action.

(b) Do not turn the device on or off. The device should be isolated from any network. The preferred methods to accomplish this 'isolation' is to put the device into "airplane mode" or by removing the SIM card. As a last resort, the device may be placed in a solid metal container such as a paint can or in a Faraday bag to prevent the device from sending or receiving information from its host network.

(c) When seizing devices, also seize the charging units.