Computers and Digital Evidence

808.1 PURPOSE AND SCOPE

This policy establishes procedures for the seizure and storage of computers, personal communications devices (PCDs) digital cameras, digital recorders and other electronic devices that are capable of storing digital information; and for the preservation and storage of digital evidence. All evidence seized and/or processed pursuant to this policy shall be done so in compliance with clearly established Fourth Amendment and 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 utilize the most knowledgeable available resources. When seizing 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) The circumstances of the case should dictate the appropriate action to take with a powered computer. Generally, a normal shutdown should be performed to preserve log files, histories, open files, etc. If anti-forensics techniques are suspected, do not shut down the computer 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 box or if a portable notebook style, disconnect any power cable from the case and remove the battery).

(e) Label each item with case number and item number.

(f) Handle and transport the computer and storage media (e.g., tape, discs, memory cards, flash memory, external drives) with care so that potential evidence is not lost.

(g) Lodge all computer items in the Property Room. Do not store computers where normal room temperature and humidity is not maintained.

(h) 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.

(i) 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.

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 the computer's hard drive, or floppy disks, compact discs, or any other storage media is required, forward the following items to a computer forensic examiner:

(a) Copy of report(s) involving the computer, including the Evidence/Property sheet.

(b) Copy of a consent to search form signed by the computer owner or the person in possession of the computer, or a copy of a search warrant authorizing the search of the computer hard drive for evidence relating to investigation.

(c) A listing of the items to search for (e.g., photographs, financial records, e-mail, documents).

(d) A forensic image, or authenticated duplicate of the hard drive or disk will be made using a forensic computer and/or a forensic software program by someone trained in the examination of computer storage devices for evidence. The needs of the case will dictate whether or not a forensic preview is appropriate before or in place of forensic imaging.

808.3 SEIZING DIGITAL STORAGE MEDIA

Digital storage media including hard drives, floppy discs, CD's, DVD's, tapes, memory cards, or flash memory devices should be seized and stored in a manner that will protect them from damage.

(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 a copy of the data should be used.

(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) Whenever possible, use plastic cases designed to protect the media, or other protective packaging, to prevent damage.

808.4 SEIZING PCDS

Personal communication devices such as cell phones, PDAs 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) Generally, officers should not attempt to access, review or search the contents of such devices through the device's interface prior to examination by a forensic expert or other personnel trained in data extraction. Unsent messages can be lost, data can be inadvertently deleted and incoming messages can override stored messages. The needs and severity of the case, experience of the officer, and exigency are all determining factors in how the PCD is handled.

(b) If off, do not turn the device on.

(c) If on, attempt to place the device in "airplane" mode or otherwise disconnect it from wireless networks. If the device cannot be placed in airplane mode, it should 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.

(d) When seizing the devices, also seize the charging units. If the batteries go dead all the data may be lost. Notify the Property Clerk if a powered device has been booked and the status of its battery so that it can be placed on a charger in a secure location, if appropriate.

(e) If the device is password/pin code protected, attempt to obtain the password or pin from the device owner and document.

808.5 DIGITAL EVIDENCE RECORDED BY OFFICERS

Officers handling and submitting recorded and digitally stored evidence from digital cameras and audio or video recorders will comply with these procedures to ensure the integrity and admissibility of such evidence.

808.5.1 COLLECTION OF DIGITAL EVIDENCE

Once evidence is recorded it shall not be erased, deleted or altered in any way prior to submission. All photographs taken will be preserved regardless of quality, composition or relevance. Original video and audio files will not be altered in any way.

808.5.2 SUBMISSION OF DIGITAL MEDIA

The following are required procedures for the submission of digital media used by cameras or other recorders:

(a) The recording media (smart card, compact flash card or any other media) shall be brought to the booking area as soon as practical for submission into evidence.

(b) Officers shall create an evidence entry in the RMS system that accurately defines the evidence. Officers shall create a folder, named after the case number and RMS item number, in the designated digital evidence storage location and shall copy the digital media into that folder. Excessively large files may need to be copied to external media rather than a folder. The property officer should be consulted in such circumstances..

(c) After the evidence has been copied, the officer shall make reasonable efforts to verify that the copied data is the same as the original data. Upon verification, the original storage media should be prepared for the next recording by deleting data on the device and/or reformatting the device.

(d) Upon receipt of the digital evidence, the Property Clerk will move the digital evidence to a secure storage location under his/her control.

(e) Officers requiring a copy of the digital files must request a copy from the Property Clerk or a supervisor in the Property Clerks absence..

808.5.3 DOWNLOADING OF DIGITAL FILES

Digital information such as video or audio files recorded on devices using internal memory must be written to external storage media. The following procedures are to be followed:

(a) Files should not be opened or reviewed prior to downloading and storage.

(b) Where possible, the device should be connected to a computer and the files accessed through the computer's operating system for download to a folder on the host computer.

(c) Investigations utilizing the recording devices in the Investigations Interview rooms shall be downloaded to a CD and booked into evidence.

808.5.4 PRESERVATION OF DIGITAL EVIDENCE

(a) Only the Property Clerk or a designated alternate are authorized to copy original digital media that is held as evidence. The original digital media shall remain in evidence and shall remain unaltered.

(b) Digital images that are enhanced to provide a better quality photograph for identification and investigative purposes must only be made from a copy of the original media.

(c) If any enhancement is done to the copy of the original, it shall be noted in the corresponding incident report.