

## 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) 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 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, evidence sheet 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.

## *Computers and Digital Evidence*

---

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.

Some resources to consider include, but are not limited to:

- (a) RCFL - Regional Computer Forensic Lab (FBI)
- (b) FBI Cyber Task Force
- (c) San Diego District Attorney's Office CATCH - Computer and Technology Crimes High Tech Task Force
- (d) San Diego ICAC - Internet Crimes Against Children
- (e) Secret Service Cyber Task Force

### **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) An exact duplicate of the hard drive or disk will be made using a forensic computer and a forensic software program by someone trained in the examination of computer storage devices for evidence.

### **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.

## *Computers and Digital Evidence*

---

- (b) Do not review, access or open digital files prior to submission. If the information is needed for immediate investigation request the Property and Evidence Section 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 plastic cases designed to protect the media, or other protective packaging, to prevent damage (Faraday bags).
- (f) Never insert any portable storage or seized device into a work related network computer/drive not specifically designed for device/imaging or review.

### **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) Officers should not 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.
- (b) Do not turn the device on or off. The device 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.
- (c) When seizing the devices, also seize the charging units and keep them plugged in to the chargers until they can be examined. If the batteries go dead all the data may be lost.

### **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. 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:

## *Computers and Digital Evidence*

---

- (a) The recording media (smart card, compact flash card or any other media) shall be brought to the Property and Evidence Section as soon as possible for submission into evidence.
- (b) Officers are not authorized to review or copy memory cards. The evidence technicians are the only employees authorized to copy and/or distribute digital media made from the memory cards.
- (c) As soon as possible following the collection of evidence, the camera operator is to remove the memory card from their digital camera and place the card into a plastic carrier. The card and carrier are then to be placed into a zip-lock type baggie. The camera operator shall write their name and the related case number on the outside of the baggie before placing in the film drop box along with the evidence form. This does not prohibit saving/copying pictures of accident scenes, crime scenes, etc. that will be attached to a report.
- (d) Evidence technicians will make a copy of the memory card using appropriate storage media. Once they have verified that the images properly transferred to the storage media, the technicians will erase the memory card for re-use. The storage media will be marked as the original.
- (e) Officers requiring a copy of the digital files must request a copy on the evidence form when submitted to evidence.

### 808.5.3 DOWNLOADING OF DIGITAL FILES

Digital information such as video or audio files recorded on devices (other than BWC footage) using internal memory must be downloaded to 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 directly from the computer directory or downloaded to a folder on the host computer for copying to the storage media.

### 808.5.4 PRESERVATION OF DIGITAL EVIDENCE

- (a) Only evidence technicians 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.