SAN MARCOS POLICE DEPARTMENT
POLICIES AND PROCEDURES MANUAL

Section Title: Computer Seizures **General Order:** 304

Date Issued: January 17, 2004 **Date Revised:** January 1, 2006

Effective Date: January 14, 2006

Issuing Authority: Howard E. Williams

Howard E. Williams, Chief of Police

I. POLICY

Images, audio, text and other data on computers and electronic media are easily altered or destroyed. It is imperative that the Department recognize, protect and seize such devices in accordance with applicable Texas statutes, and utilizing the best practices and guidelines for the seizure of computer related evidence. Generally, computer hardware can serve one of two roles in a criminal case. The computer hardware can be a storage device for evidence of criminal activity, or it can be contraband, mere evidence, or an instrumentality or fruit of a crime. Regardless, the goal is to obtain evidence in a form admissible in court and that is free from any inadvertent alteration or destruction of the evidence. It is imperative that computer data be examined only by personnel specifically trained in computer data forensics using law enforcement specific software to preserve the evidence.

II. PURPOSE

The purpose of General Order 304 is to establish responsibilities and guidelines for the investigation of incidents involving computers and the seizure of computer hardware and software.

III. PRE-SEIZURE

A. When the assigned Investigator anticipates the recovery of computer-related evidence, it is imperative that personnel who have been trained in computer forensics be consulted during the initial stages of a preparing a search warrant affidavit.

1. Search Warrants requesting the seizure of computers and related peripherals are very specific in nature and require language within the Affidavit to ensure that the items identified in the warrant are properly connected to the facts of the case.

2. Several key questions must be addressed in preparing the composition of a search warrant for the seizure of computer evidence.

   a. Is there probable cause to seize the hardware?

   b. Is there probable cause to seize the software?

   c. Where will this search be conducted?

B. It is preferable that the computer system be examined by a qualified forensic examiner, so the warrant should authorize the removal of the seized evidence to the lab.

C. If the data within the computer is identified as evidence, the warrant should specifically describe the type of information that is being sought. It is also helpful to request the seizure of the computer manuals and original software to provide guidance to the computer examiner during the forensic data recovery procedure if the software is unfamiliar or foreign to the examiner.

D. If it is suspected that the computer may be the fruit of an illegal activity, the entire system – monitor, printer, scanner, and other peripherals and connecting cables should also be seized.

E. Generally, the Department will only seize and perform forensic examination on non-networked personal computers used by individuals in their residences. Seizure of computers used in business can expose the Department to loss-of-business liability. A network seizure will be done with the assistance of the appropriate network administrator so that the entire network is not adversely affected by the removal of a single computer.

IV. EVIDENCE COLLECTION

A. Trained Department personnel should accompany the search team during the execution of a computer-related search warrant. During the initial stages of the execution of the warrant, it is important to identify the specific location of the computer(s) to be seized.

B. Everyone should be removed from all computers. Allowing a suspect to continue using a computer may result in the destruction of the computerized evidence by predefined keystrokes called "hotkeys" or "macros," which can activate a total erasure of the evidence files in just seconds.

C. Photograph everything, including the computer screen.

D. It is important to photograph and mark cables before disconnecting them. The computer may need to be reassembled later. If the computer is OFF, unplug it. If it is ON, photograph the screen and then unplug it.

E. Although unlikely, computers can be booby-trapped with explosives.

1. First, examine bookshelves in the vicinity of the computer, and if there are any books or manuals on explosives or related subjects DO NOT PROCEED WITH EVIDENCE COLLECTION.

2. Contact ATF to examine the computer for possible booby-traps.

F. If there is no suspected booby-trap, verify the system is OFF and that no drive lights are active. If the computer is ON, look for another power source, possibly an uninterrupted power supply, or UPS.

G. Seize any additional computer related materials working outward from the computer, such as printouts or notes, and examine notebooks and manuals for passwords.

H. Mark and disconnect cables and their respective ports.

1. Hand drawings and/or photographs will document specific cable placements.

2. Seized items should be properly tagged and marked in accordance with Department procedures for evidence collection.

3. Diskettes that appear to be new, unlabelled or unused can also contain deleted evidence that is recoverable.

4. If diskettes are not sealed in the original shrink-wrap, officers should seize them also.

G. Prior to packaging, remove all storage media from the CPU drives or peripheral devices, noting what was removed and from where.

H. Pack system pieces carefully in boxes, blankets and bubble wrap. Do not use Styrofoam packaging material.

I. The CPU should be marked "EVIDENCE – DO NOT BOOT" and a DEPARTMENT floppy disk should be inserted into the diskette drive to prevent accidental booting of the machine. ZIP and floppy diskettes should be transported in paper bags or boxes because plastic may generate static electricity that can damage the disks.

J. An inventory should be completed of all items that were seized pursuant to the search warrant and left at the location searched or with the suspects themselves, before leaving the scene.

VI. TRANSPORTATION AND STORAGE

A. Care should be taken that seized computer systems or disks are not placed on or near the radio transmitter in the trunk of transport vehicles or left in dramatic temperature extremes. If possible, items should be placed within the passenger compartment of a vehicle to prevent excessive vibrations or damage.

B. Computer evidence items will be submitted to the Department Evidence and Property Technician pursuant to applicable section of Department policy.

C. Computers and computer-related items should be stored in a secure, dry, cool environment away from generators, magnets or any sources of direct sunlight or electromagnetic fields.

D. The assigned Investigator should fill out a Department Computer Forensic Analysis form, and transfer custody of the seized CPU and other original storage media to the department's computer data forensic analyst as soon as possible.