Sheridan Police Department
Policies and Procedures
12.2
Chapter 12 – Evidence & Property
Section 2 – Seizing Computers & Other Electronic Devices

Date: January 1, 2013
Updated: 9/27/2021

Signature:

Computers and other electronic technology that is taken as evidence can be a valuable source of criminal evidence. Seizure of these devices requires special consideration.

12.2.1 General Principles

A. All seizures require a legal basis to seize the item. (Sections 10.4.1, 10.4.2)
B. If the officer planning a search and seizure knows in advance that computer equipment is to be seized, he or she should consider enlisting the aid of someone trained in the area of forensic computer seizures. Particularly for networked or business computers where the business or network proprietor is not involved in the criminal activity, officers should seek the assistance of a computer specialist before disconnecting a computer.
C. Suspects must not be allowed to remain near any computers. A single keystroke could launch a program that would permanently destroy digital evidence. In addition, some computers can be controlled through remote devices, such as a wireless mouse. Therefore, suspects should not be allowed to retain any electronic devices during the search.
D. Consider the need for processing for physical evidence such as fingerprints and handle accordingly.
E. When seizing a computer for analysis, if the computer is off, leave it off.
F. If the computer is on, depending on the facts of the case and skill level of those involved in the seizure, it may be appropriate to carefully gather some volatile evidence in RAM that will be lost upon shutdown. Do not start searching through the computer.
G. If it is reasonably believed that the computer is destroying evidence, immediately shut down the computer by pulling the power cord from the back of the computer and removing the battery if necessary.
H. If a camera is available, and the computer is on, take pictures of the computer screen. If the computer is off, take pictures of the computer, the location of the computer, the connections and any electronic media attached.
I. When supported by the legal basis for the seizure (warrant, consent, plain view, etc.) all printouts (officers should be observant for user names and passwords), components and peripherals including cables, power cords, keyboards, mice, manuals and storage media should be collected with the computer.

12.2.2 Stand-Alone Home Personal Computer

For proper evidence preservation, follow these procedures in order.

A. If networked (attached to router and modem), see instructions in 12.2.3.
B. Do not use a computer or attempt to search for evidence except per 12.2.1F.

C. Photograph computer front and back as well as cords and connected devices, as found. Photograph the surrounding area prior to moving any evidence.
D. If the computer is off, do not turn on.
E. If the computer is on and something is displayed on the monitor, photograph the screen.
F. If the computer is on and the screen is blank, move the mouse or press space bar (this will display the active image on the screen). After image appears, photograph the screen.
G. Unplug power cord from back of computer.
    1. For laptops, if the laptop does not shutdown when the power cord is removed, locate and remove the battery.
    2. The battery is commonly placed on the bottom, and there is usually a button or switch that allows for the removal of the battery.
    3. Once the battery is removed, do not return it to or store it in the laptop. Removing the battery will prevent accidental start-up of the laptop.
H. Diagram and label cords to later identify connected devices.
I. Disconnect all cords and devices from the computer.
J. Package components and transport as fragile cargo.
K. Seize additional storage media.
L. Keep computer and all media away from magnets, radio transmitters and other potentially damaging elements.
M. Collect instruction manuals, documentation and notes.

12.2.3 Networked Home Personal Computer

For proper evidence preservation, follow these procedures in order.
A. Unplug power to router and/or modem.
B. Do not use computer or attempt to search for evidence except per 12.2.1F.
C. Photograph computer front and back as well as cords and connected devices, as found. Photograph surrounding area prior to moving any evidence.
D. If computer is off, do not turn on.
E. If computer is on and something is displayed on the monitor, photograph the screen.
F. If computer is on and the screen is blank, move mouse or press space bar (this will display the active image on the screen). After image appears, photograph the screen.
G. Unplug power cord from back of computer.
H. Diagram and label cords to later identify connected devices.
I. Disconnect all cords and devices from computer.
J. Package components (including router and modem) and transport as fragile cargo.
K. Seize additional storage media.
L. Keep computer and all media away from magnets, radio transmitters and other potentially damaging elements.
M. Collect instruction manuals, documentation and notes.

12.2.4 Network Server / Business Network

A. Consult a computer specialist for further assistance.
B. Secure the scene and do not let anyone touch except personnel trained to handle network systems.
C. Pulling the plug could:
    1. Severely damage the system;

2. Disrupt legitimate business;
3. Create officer and department liability

12.2.5 Cell Phone & Digital Camera

A. Cell phones, smartphones and digital cameras may store data directly to internal memory or may contain removable media.

B. The following details the proper seizure and preservation of these devices and associated removable media.
   1. If the device is off, do not turn on.
   2. With PDAs or cell phones, if device is on, leave on. Powering down device could enable a password, thus preventing access to evidence.
   3. Photograph device and screen display (if available).
   4. Label and collect all cables (to include power supply) and transport with device.
   5. Keep the device charged. They may store information in RAM type memory - if the battery dies data can be lost.
   6. If the device cannot be kept charged, analysis by a specialist must be completed prior to battery discharge or data may be lost.

12.2.6 Processing and Storage of Digital Evidence Collected by Officers

A. This policy will apply to all personnel who collect, handle, and process digital evidence. Digital evidence, in this policy, refers to digital files collected as evidence in police investigations such as videos and phone downloads.
   1. If during the course of an investigation an officer collects a piece of digital evidence the officer should use portable hardware such as a USB Drive to store the evidence. The officer shall then take the item and place it in an envelope. On the outside of the envelope, the officer should write the corresponding case number and the collecting officer's name. The officer shall then place that envelope in the pass-through evidence lockers. There is no need to seal the envelope or affix any barcode or other labels. The officer will also log the item as evidence in Spillman, following already established procedures for evidence item entry.
   2. The evidence technician will take the digital file and transfer it from the temporary portable hardware to a hard drive. This hard drive will be used exclusively for the storage and management of digital evidence. The evidence technician will then return the portable hardware back to be used again by officers.
   3. The evidence technician will remain the point of contact for any other agencies or persons who wish to have access to the evidence. The evidence technician will maintain the evidence and document access following established procedures.
   4. Patrol Sergeants and the Special Operations Lieutenant will maintain a supply of USB drives for officers to use.

B. Any deviation from this procedure needs to be granted in writing by a bureau commander or above. The one set exception to this procedure are items with digital evidence containing child pornography. Those items will be stored and sealed separately.