Section 4/700 ◆ Criminal Investigation		
4 / 707	Seizure of Computer Equipment	2/20/01
Accreditation Standards	83.2.5	

4 / 707.05 GENERAL

Computers and digital media are increasingly involved in unlawful activities. The computer may be contraband, fruits of the crime, a tool of the offense, or a storage container holding evidence of the offense. Investigation of any criminal activity may produce electronic evidence.

Computers and related evidence range from the mainframe computer to the pocket-sized personal data assistant to the floppy diskette, CD or the smallest electronic chip device. Images, audio, text and other data on these media are easily altered or destroyed. It is imperative that law enforcement officers recognize, protect, seize and search such devices in accordance with applicable statutes, policies and best practices and guidelines.

The below procedures were developed from the guide "Best Practices for Seizing Electronic Evidence." A copy of this guide is issued to each supervisor for reference.
.

4 / 707.10 LEGAL REQUIREMENTS

Using evidence obtained from a computer in a legal proceeding requires:

- Probable cause for issuance of a warrant or an exception to the warrant requirement. Caution: If you encounter potential evidence that may be outside the scope of your existing warrant or legal authority, contact your agency's legal advisor or prosecutor as an additional warrant may be necessary.

- Use of appropriate collection techniques so as not to alter or destroy evidence.

- Forensic examination of the system completed by trained personnel in a speedy fashion, with expert testimony available at trial.

In order to apply for a warrant for the seizure of computer equipment, the following questions must be answered:

- Is there probable cause to seize hardware?
- Is there probable cause to seize software?
- Is there probable cause to seize data?
- Where will this search be conducted?

4 / 707.15 PROCEDURES

Once legal requirements have been met, the procedures for seizing the computer equipment are as follows:

1. Secure the Scene

- Officer safety is paramount.
- Preserve area for potential fingerprints.
- Immediately restrict access to computer(s).
- Isolate from phone lines (because data on the computer can be accessed remotely).

2. Secure the Computer as Evidence

If computer is "OFF", do not turn "ON".
If computer is "ON":

- Stand-alone computer (non-networked)

Contact the City's Office of Information Technology, the FBI or the Maryland State Police for assistance. Officers are prohibited from examining any computer or electronic equipment regardless of their level of training. If a technician is not available, then:

- Photograph screen, then disconnect all power sources; unplug from the wall AND the back of the computer.
- Place evidence tape over each drive slot.
- Photograph/diagram and label back of computer components with existing connections.
- Label all connectors/cable ends to allow reassembly as needed.
- If transport is required, package components and transport/store components as fragile cargo.
- Keep away from magnets, radio transmitters and otherwise hostile environments.

- Networked or business computers

Contact the City's Office of Information Technology, the FBI or the Maryland State Police for assistance.

- Pulling the plug could:
  a) Severely damage the system
  b) Disrupt legitimate business
  c) Create officer and department liability

END OF ORDER