I. Policy

It is the policy of this Division to train members to seize evidence in a manner designed to minimize the potential loss of any electronic data stored within the devices.

II. Purpose

This Directive establishes guidelines and procedures for the seizure of computers, computer related equipment, electronic devices and supplies.

III. Securing and Seizing Computers

A. Securing a Computer

1. Document and take a photograph of the computer, wiring schematic and surrounding area before doing anything. This should include making a diagram and labeling all wires connected to the computer.

2. If the computer is off - simply disconnect the power cord. NEVER TURN THE COMPUTER ON, IF IT IS OFF.

3. If the computer is running, simply disconnect the power cord. NEVER PUSH THE POWER BUTTON ON THE MACHINE as it could be hard wired to reformat the hard drive.

4. If the computer is on, do not open any files on the computer.

5. Under no circumstances should anyone, other than trained law enforcement representatives, be allowed to manipulate the computer in any way, other than described in this order.

B. Seizing the Computer

1. Prior to searching the site, gather as much intelligence on the system to be seized as possible. Attempt to ascertain the user's level of computer knowledge and the environment in which the computer components are located.

2. Once on the scene, protect the computer from the suspect(s) and others at the scene including other law enforcement personnel and preserve the area for processing.

3. If the computer operating system is unknown, NOTHING SHOULD BE DONE WITH THE COMPUTER and assistance should be requested from qualified personnel at the Montgomery County Police Department (MCPD) Computer Crimes Unit.

4. The following language may be used as a guide when describing items to be seized in a search and seizure warrant regarding computers.

   a. Computer and Electronic Equipment: Any and all information and/or data stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer or with the aid of computer related equipment. This media includes floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, DVDs, videocassettes and other media which are capable of storing magnetic or electronic coding.

   b. Any and all electronic devices which are capable of analyzing, creating, displaying, converting or transmitting electronic or magnetic computer impulses or data. These devices include computers, computer components, computer peripherals, word processing equipment, modems, monitor, printer, plotters, encryption circuit boards, optical scanners, external hard drives and other computer related electronic devices.

   c. Any and all instructions or programs stored in the form of electronic or magnetic media, which are capable of being interpreted by a computer or related component. The items to be seized could include operating systems, application software, utility programs, compilers, interpreters and other programs or software used to communicate with the computer hardware or peripherals either directly or indirectly via telephones lines, radio or other means of transmission.

   d. Any and all written or printed material which provides instructions or examples concerning the operation of a computer system, computer software and/or any related device.

   e. This warrant is for the seizure of the above described computer data and for the authorization to read, retrieve, copy and seize information stored and contained on the above described computer systems and magnetic storage devices and for the authorization to present these items to persons capable of conducting such examinations and recoveries.

5. Seize everything related to the computer. This includes external modems or drives, monitors, printers, scanners, diskettes, instruction manuals and any printed documentation.

6. If possible, all computers and components should be packaged in original cartons and boxes if available on the scene.

IV. Securing and Seizing Electronic Devices

A. Electronic devices may contain viable evidence associated with criminal activity. Unless an emergency exists, the device should not be accessed. Should it be necessary to access the device all actions associated with the manipulation of the device should be noted in order to document the chain of custody and ensure its admission in court.

1. Wireless telephones

a. The phone should be left on until a search warrant can be obtained.

b. Officers should be aware that continued access to electronic communications over a phone without proper authorization could be construed as unlawful interception of electronic communications.

c. Potential evidence contained in wireless devices includes the following:
1) Phone and pager numbers
2) Names and addresses
3) Personal Identification Numbers (PIN)
4) Voice mail access number
5) Voice mail password
6) Debit card numbers
7) Calling card number
8) E-mail/Internet access information
9) Other valuable information on the screen image

2. Electronic paging devices

a. The pager should be left on until a search warrant can be obtained.

b. Officers should be aware that continued access to electronic communications over a pager without proper authorization could be construed as unlawful interception of electronic communications

c. Numeric pagers receive only numeric digits. These number or sequence of number can be used to communicate codes as well as phone numbers.

d. Alphanumeric pagers receive numbers and letters and can carry full text messages.

e. Voice pagers transmit voice communications in addition to alphanumeric messages

f. 2-way pagers combine incoming and outgoing messages

3. Facsimile machines

a. If the FAX machine is found “on,” powering down may cause loss of last number dialed and/or stored faxes.

b. Officers should contact a MCPD computer expert assistance.

c. Facsimile machines may contain the following evidence:

1) Speed dial lists.
2) Stored faxes, both incoming and outgoing.
3) FAX transmission logs, both incoming and outgoing.
4) Header line.
5) Clock setting

4. Caller ID device - Caller ID devices may contain telephone and subscriber information from incoming calls. Officers should:

a. Protect internal battery back up to ensure uninterrupted power supply to the device so no data will be lost.

b. Document all stored data prior to seizure to prevent loss of data.

5. Smart Cards - A smart card is a plastic card the size of a standard credit card that holds a microprocessor (chip) that can store monetary value and other information. Smart cards can be for point of sale transactions, direct exchange of value between cardholders and exchange value over the Internet, ATM capabilities and storing other data and files similar to a computer. When encountering a smart card, officers should;

a. Photograph the card
b. Attempt to detect possible alterations or tampering
c. Document who the card is issued to

V. Computer Forensics

A. The Montgomery County Police Computer Crimes Lab will be the primary agency used by this Division for computer forensics.

1. The MCPD Computer Crimes Unit is available 24 hours a day by calling ECC.

2. For MAJOR CASES or if intelligence on the suspect or computer system indicates there could be a problem, the MCPD Computer Crimes Unit can be called for assistance or advice. If enough notification is given, computer forensic personnel from the MCPD Computer Crimes Lab can respond to the location of the seizure, help secure the computers and transport the computers directly to the MCPD Computer Crime Lab for analysis.

3. When a seizure is made and MCPD is not present - Arrangements should then be made with MCPD Computer Crimes Unit to deliver the seized computer for analysis. This should include any magnetic storage devices such as disks or CD-ROM's needing analysis.

4. If more than one floppy disk, CD-ROM or any other type of computer magnetic storage device are seized an computer forensics are necessary, each item must be identified separately.

5. Division evidence procedures will be followed.

6. When delivering a computer for analysis the following items will be supplied to MCPD:

    a. Copies of any police reports.
    b. Copies of search warrants.
    c. A list of key words or the information being sought.

B. Another resource is the Maryland State Police (MSP) Computer Crime Lab, which is available 24 hours a day.

Approved Park Police Document
Signed Original on File

End of Directive