DEPARTMENT GENERAL ORDER 07-50

OFFICE of the CHIEF OF POLICE DATE: February 9, 2007
REPLACES: General Order 99-40
SOP 502.18.00

SEIZURE/EXAMINATION OF COMPUTER EQUIPMENT

I. PURPOSE.

Computer equipment may be severely damaged and the data contained in the system lost due to improper seizure/examination procedures. As such, the following shall constitute a general guideline to govern the seizure of computer hardware and software and its subsequent examination by department personnel.

DEFINITIONS.

Computer - Pursuant to 18 U.S.C. § 1030(e)(1), an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

Computer hardware - All equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

Computer software - Digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

III. GENERAL.

When a seizure of computer equipment is deemed necessary, Field Investigators, detectives, or other uniformed officer(s) at the scene shall note the operating status of the equipment which shall influence seizure proceedings.

A. Should the computer system be off and its various parts disconnected from one another and a power source, the area shall be photographed by a Field Investigator, at which time the equipment may be removed and packaged.

B. Should a computer system be connected to other unit components and a source of power, the scene shall be secured from unauthorized access, and the system and surrounding area photographed by a Field Investigator. No attempt shall be made by uniformed personnel to access the system or otherwise power same down. CID personnel shall then be requested to respond to the scene to manage the seizure proceedings. Upon their arrival, the computer equipment will be subsequently powered down, disassembled, and seized in accordance with the standards established by the Department of Justice Cyber Crime Division. A brief synopsis of those procedures is presented elsewhere in this order.

IV. PROCEDURAL STEPS FOR SEIZURE.

In an effort to maximize the potential for meaningful data retrieval, the following procedural steps have been established in regard to the physical seizure of computer equipment.

A. Photograph the general scene, computer monitor (including any on-screen display), and electrical connections.

B. Power system down and disconnect from electrical outlets.

C. Label all connectors prior to disassembly.

D. Seize all available software and computer discs.

E. Keep hardware units and connectors together.

F. Record equipment identification numbers/descriptions.

G. Return hardware/software to this agency.

H. Package software and tag hardware.

I. Complete evidence sheet(s) and store items in a secure and cool environment (evidence vault).

V. START-UP/SEARCH PROCESS.

CID personnel will contact the Computer Crime Task Force or appropriate entity for assistance in reactivating seized computer equipment and/or to perform a search of the system's software. Should task force technicians be unavailable to assist in this process, appropriate outside personnel will be contacted by CID to provide the technical expertise required.

Information which may be obtained by a search of computer equipment will be secured and documented as evidence according to the situation. Other data will be held with the computer until released by proper authorization.

VI. LEGAL CONSULTATION.

In those instances where a question exists as to the legal justification regarding the seizure of computer components, or documentation derived therefrom, consultation should be made with the St. Louis County Prosecuting Attorney's office or the United States Attorney's office prior to any seizure being initiated.

BY ORDER OF:

THOMAS J. BYRNE
Chief of Police

TJB:dld

CALEA Reference: 83.2.5