ILLINOIS STATE POLICE DIRECTIVE
OPS-202, EVIDENCE – COLLECTING AND PACKAGING COMPUTER AND DIGITAL/MULTIMEDIA FORENSIC EVIDENCE

RESCINDS: OPS-202, 2011-052, revised 07-18-2011	**REVISED:** 04-30-2015 **2015-016**
RELATED DOCUMENTS: OPS-200, Evidence Custodian's Manual	**RELATED CALEA STANDARDS:** 42.2.1, 42.2.2, 42.2.3, 55.2.4, 61.2.3, 82.2.5, 82.3.2, 83.1.2, 83.2.1, 83.2.2, 83.2.3, 83.2.5, 83.2.6, 83.3.1, 83.3.2, 84.1.1, 84.1.2, 84.1.3, 84.1.4, 84.1.5, 84.1.6, 84.1.7

I. POLICY

The Illinois State Police (ISP) will establish guidelines to collect, preserve, package, document, and transfer digital evidence and related items in a standard and consistent manner.

II. DEFINITIONS

For definitions, refer to ISP directive OPS-200, "Evidence - Definitions and Responsibilities."

I. PROCEDURES

II.A. Vaults and processing laboratories controlled by the Digital Crimes Unit (DCU), Intelligence Command, Division of Operations (DOO) are the receiving facilities for computer-related evidence only, but are to be considered storage facilities only for the length of time necessary to complete the required analysis. A high level of security with a controlled/protected environment, and immediate access to specialized computer processing equipment and forensic analysis software are required.

II.B. The Colonel, DOO, may authorize an exemption to the receipting and logging procedures specified in this directive in special or unusual circumstances.

II.C. Seizing electronic evidence

II.C.1. Planned seizures

II.C.1.a. Officers planning an operation that may result in the seizure of computer-related evidence should attempt to obtain the service of personnel who have had formal computer seizure training approved and/or conducted by DCU.

II.C.1.b. When personnel with formal training are not available, officers planning the seizure will contact DCU for technical guidance prior to the seizure.

II.C.1.c. Search Warrants:

II.C.1.c.1) DCU will provide advisory services in the preparation of search warrants for computer equipment and data.

II.C.1.c.2) The search warrant must specify the items to be seized and searched. All computer hardware and software should be included, keeping in mind the entire system is necessary to replicate the suspect's use of it and to enable forensic examination of the system.

II.C.1.d. Officers will consult with a department legal advisor and DCU in the event the computer or electronic storage media to be seized may involve legitimate business records or business "work products."

II.C.2. Non-planned seizures

II.C.2.a. Officers encountering computer equipment and/or electronic storage media that may be of evidentiary value should attempt to obtain the services of formally trained personnel in the physical seizure and handling of computers and related items.

II.C.2.b. Officers may contact DCU for advice.

II.C.2.c. If assistance is not readily available, and the possible evidentiary value of the equipment/storage media may be compromised by leaving it in its current location, the officer should take the following steps:

NOTE: The following is extremely basic guidance subject to rapidly changing technologies. All officers should consult and follow the guidelines listed in the booklet "Best Practices for Seizing Electronic Evidence, version 3.0" or the latest version (the guide is available online at http://www.forwardedge2.com/pdf/bestpractices.pdf).

II.C.2.c.1) Stand alone computer (Non-network)

II.C.2.c.1)a) Computer equipment that appears to be turned off:

II.C.2.c.1)a)(1) Move people away from the computer.

II.C.2.c.1)a)(2) Under no circumstances will the officer switch on the computer.

II.C.2.c.1)a)(3) Record the configuration of the device and all connections via photographs, hand-drawn diagrams, or notes.

II.C.2.c.1)a)(4) Unplug the power cord from the back of the computer not from the wall.

II.C.2.c.1)a)(5) Collect the power cord as not all power supplies are interchangeable.

II.C.2.c.1)b) Computer equipment that appears to be turned on:

II.C.2.c.1)b)(1) Move people away from the computer.

II.C.2.c.1)b)(2) Do not touch the keyboard or mouse.

II.C.2.c.1)b)(3) Record what is on the screen, as well as the configuration of the device and all connections, via photographs, hand-drawn diagrams, or notes.

II.C.2.c.1)b)(4) If no formally trained personnel are readily available, remove the power cord from the back of the computer not from the wall.

II.C.2.c.1)b)(5) If the computer is a laptop, unplug the power cord from the back of the computer and remove the battery.

II.C.2.c.1)b)(6) Collect the power cord and battery, as not all power supplies are interchangeable.

II.C.2.c.2) Network or business computers

II.C.2.c.2)a) Officers will consult with DCU or other personnel with formal training and expertise when dealing with network or business computers, a computer network, mainframe, or mainframe terminal.

II.C.2.c.2)b) Pulling the power cord could damage the system and/or disrupt legitimate business. Without approval from a formally trained officer, do not disturb the power cord.

II.D. Packaging/labeling electronic evidence

Each item seized/recovered must be properly marked, labeled, and packaged.

II.D.1. Large items such as monitors, keyboards, and system units (normally containing the hard drive) may be tagged or labeled rather than bagged.

II.D.1.a. If the system unit is not bagged, the electrical plug will also be covered with evidence tape.

II.D.1.b. The officer seizing the system will place his/her initials and identification number on the tape. The officer will place the tape so power may not be supplied to the machine without disrupting the tape.

II.D.2. If a large item is bagged, clear, static free bags, or a large paper bag (such as a lawn/leaf bag) will be used. If a large paper bag is used, the officer will seal the bag with evidence tape.

II.D.3. Small items such as loose media (CDs, DVDs, SD cards, Flash drives, etc.) must be bagged/boxed, tagged, and sealed.

II.E. Protecting electronic evidence

II.E.1. During transportation and storage of computers and related electronic devices, avoid external magnetic sources (i.e. placing the item near the police radios), extreme temperatures, and other possible contaminants.

II.E.2. Do not use fingerprint powder on compact discs, or other computer media as the presence of fingerprint powder may render forensic data examination impossible.

II.E.3. If forensic evidence is present on these items, contact the DCU.

II.F. Temporary storage in work unit DCU offices:

II.F.1. Work unit offices may be used for periods exceeding one day while evidence is being processed and/or pending transfer to DFS laboratory facilities' evidence vault or the agency managing the case.

II.F.2. DCU offices may be used for temporary storage exceeding one day while evidence is being processed and/or pending transfer to the DCU vault for retention until processing of the evidence is complete.

II.F.3. The Colonel, DOO, will approve written procedures to ensure proper security for such temporary storage areas.

II.G. The evidence vault at DCU will not provide drop lockers.

II.G.1. Evidence may be submitted to the section during regular business hours.

II.G.2. It is advisable to schedule an appointment to deliver or retrieve evidence from DCU.

II.H. Prior to submitting evidence to DCU, officers should first contact the section to receive appropriate procedures for transport and transfer.

II.I. Officers seizing computer systems should contact the appropriate State's Attorney prior to seizing any work product of documentary materials from a suspect if it is reasonably believed the materials are intended for public dissemination or publication.

II.J. DCU will provide and maintain formal, written procedures addressing the handling of computer crime evidence as well as computer forensic procedures.

Indicates new or revised items.

-End of Directive-