SPRINGFIELD POLICE DEPARTMENT

Standard Operating Guideline

Effective Date: 04/04/2017	Supersedes Policy Dated: 05/31/2014	Rescinds:	SOG Number: 413.3
Accreditation Index:			
Part Title: Operations	**Chapter Title:** Evidence		
Chief of Police:			

Computer Evidence

I Policy

It is the policy of the Springfield Police Department to pursue the identification, investigation, and prosecution of persons who use computers and other digital devices in the furtherance of criminal activity. To ensure computer evidence is seized properly, only department employees who are trained in digital evidence collection shall seize computer systems for evidence. Only department employees who are trained in forensic data recovery and analysis shall process computer systems, computer storage media, mobile electronic devices, digital records, and gaming consoles for evidence, unless otherwise provided for herein. The Criminal Investigations Division shall be responsible for maintaining employees trained in computer forensic investigations. [1]

II Definitions [2]

Access – To instruct, communicate with, store data in, retrieve or extract data from, or otherwise make any use of any resources of a computer, computer system, or computer network.

Computer – The box that houses the central processing unit, along with any internal storage devices, such as internal hard drives, and internal communication devices, such as internal modems capable of sending or receiving electronic mail or fax cards, along with any other hardware stored or housed internally. Thus, computer refers to hardware, software, and data contained in the main unit.

1 Policy Statement revised, unnecessary word removed, per Policy Change Order 16-038.
2 Definitions revised; formatting corrected, minor punctuation and wording changes; per PCO 16-038.

Computer Forensic Examiner – A member of the department specifically trained in the techniques of forensic data recovery and analysis. Successful completion of at least one digital forensic certification, program, or undergraduate field of study in digital forensics shall constitute the required training.

Computer Program – A set of instructions, statements, or related data that directs or is intended to direct a computer to perform certain functions.

Computer Storage Media – Internal or external hard drive, micro or mini hard drive, network attached storage device, tape backup system, CD, DVD, HD DVD (High Density DVD), BD (Blu-ray Disk), floppy disk, jazz disk, zip disk, tape, flash memory card, USB drive, or other types of physical media used to store data magnetically, optically, or electronically.

Computer System – A set of related, connected or unconnected, computer equipment, data, or software.

Data – A representation of information, facts, knowledge, concepts, or instructions prepared in a formalized or other manner and intended for use in a computer or computer network.

Digital Record – Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

Gaming Console – Home video game consoles such as Microsoft Xbox, or handheld game consoles such as Sony PSP, which contain internal computer hard drives or removable flash memory cards for data storage.

Hardware – All computer equipment with the capability to collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data.

Mobile Electronic Device – PDA (Personal Digital Assistant), cellular phone, digital camera, digital video camera, MP3 / MP4 or other audio/video player such as Apple iPod, or other mobile data storage devices.

Software – Digital information which can be interpreted by a computer and any of its related components to direct the way they work.

III Procedure

1 WHEN COMPUTER FORENSIC EXAMINER SHALL BE UTILIZED

1.1 This policy shall apply in those cases where data residing on computer systems, computer storage media, mobile electronic devices, digital records, or gaming consoles are being sought as evidence in an investigation. [3]

1.1.1 Computers, storage media and other devices seized by department personnel as fruits of crimes (e.g. burglary, retail theft, etc.) shall be treated as normal evidence and processed according to the procedures in SOG 413.1 – Collection and Preservation of Evidence.

1.1.1(a) This type of seizure will not normally require the services of the Computer Forensic Examiner.

2 SEIZURE AND PRESERVATION OF COMPUTER EVIDENCE

2.1 No department member, except those who have been trained, shall power off, disconnect, power on, or access a computer system that is to be seized.

2.2 No department member, except those who have been trained, shall access computer storage media, mobile electronic devices, digital records, or gaming consoles which are to be seized.

2.3 Computer systems can and have been found to contain destructive computer programs which can alter file access dates and file content that can be critical evidence.

2.3.1 Only members of the Computer Forensics Unit may attempt to access computer systems, computer storage media, mobile electronic devices, digital records, and gaming consoles in any way, in any type of attempt to validate the presence of files or computer programs which may contain evidentiary content or aid in the development of further probable cause. [4]

2.4 When it is determined that a computer system and/or digital records are to be seized and processed, department personnel should immediately contact the Crimes Against Persons Lieutenant to request a computer forensic examiner. [5]

2.4.1 In most cases, a computer forensic examiner will respond to seize computer systems and/or digital records. Upon being contacted and well informed of an investigation involving computer evidence, the examiner will retain sole discretion in determining whether on-scene personnel may seize a computer system.

2.5 If a department computer forensic examiner is unavailable, the Crimes Against Persons Lieutenant may contact an outside agency for assistance. [6]

2.6 Exigent circumstances may necessitate immediate seizure of computer systems by officers on-scene. A department computer forensic examiner should be

3 Section 1.1 revised, subsections reorganized, per Policy Change Order 16-038.
4 Section 2.3.1(a) deleted regarding search of mobile communications devices incident to arrest, per PCO 16-038.
5 Section 2.4 revised, contact person when seizing a computer specified, per Policy Change Order 16-038.
6 Section 2.5 revised, procedure for outside agency assistance clarified, per Policy Change Order 16-038.

notified as soon as possible to assist. [7]

2.7 When it is determined that computer storage media, mobile electronic devices or gaming consoles are to be seized and processed by on-scene personnel, the following guidelines shall be adhered to.

2.7.1 Computer storage media:

2.7.1(a) Ensure write-protect tabs (if present) are placed in the locked position on floppy and zip disks, USB drives, flash memory cards, and other media.

2.7.2 Mobile electronic devices and gaming consoles: [8]

2.7.2(a) If a device is found “on”, document and photograph the information on the display screen.

2.7.2(b) If a device is found “off”, do not turn it on. Seize power cables and charging cradles, if present.

2.7.2(c) Ensure mobile communication devices are in airplane mode and all other wireless communications are disabled immediately. After communications are disabled, security measures including personal identification numbers, passphrases, patterns, or other equipment that may prevent future access to the device should be removed, if possible. Finally, remove the battery from the device, if possible.

2.7.2(d) Ensure game consoles are powered off and all applicable input/output devices are collected along with their power cords.

2.7.3 When seizing and transporting computer evidence, personnel should be aware of environmental factors such as electromagnetic interference, electrostatic discharge, moisture and excessive temperatures, all of which contribute to an increased potential for data damage or destruction.

2.7.3(a) Computer evidence should be transported on the rear floorboard of police vehicles to avoid electromagnetic interference created by police radio and mobile dispatch systems.

2.7.3(b) Avoid transporting storage media in uniform pockets due to potential static electricity.

2.8 Once potential computer evidence has been located, on-scene personnel should prevent victims, witnesses, suspects, and any other persons from accessing or tampering with any of the evidence to be seized.

---

7 Section 2.6 revised, minor wording change, per Policy Change Order 16-038.
8 Section 2.7.2 revised; capitalization changes and rewording, per Policy Change Order 16-038.

3 RESPONSIBILITIES OF THE COMPUTER FORENSIC EXAMINER [9]

3.1 The computer forensic examiner shall make all efforts to accomplish the following during the examination of the seized system and media.

3.1.1 Ensure the computer equipment, computer hardware, and digital records are maintained in their original unaltered state.

3.1.2 Ensure no unauthorized alterations are made to any seized computer evidence by viruses, defense schemes, the operating system, write back applications or other inadvertent means prior to and during data acquisition.

3.1.3 Ensure data analysis is performed on a validated, forensic duplication of the original media.

3.1.3(a) Forensic previews of storage media may be performed using a write blocking device or application.

3.1.4 Examine unallocated disk space and file slack for relevant data.

3.1.5 Recover, unlock and access deleted files, hidden data, password protected data and encrypted files.

3.1.6 Provide a report of the findings to the case investigator as soon as practical.

4 TRAINING

4.1 All major crime investigators should be trained in the proper methods to preserve and seize computer systems, computer storage media, mobile electronic devices, digital records, and gaming consoles. This training shall be conducted in accordance with the current lesson plan on file with the Training Unit.

IV Attachments

9 Section 3.1 revised, minor reorganization, per Policy Change Order 16-038.