

	ANDOVER POLICE DEPARTMENT GENERAL ORDER		Number: O2508
			Page: 1 of 7
			Distribution: All
Title: SEIZURE OF ELECTRONIC EVIDENCE		Section: Investigations	
Issued: 03/29/2011	Effective: 04/07/2011	Revised: 04/10/2014	
Rescinds: All Previous		Amends:	
CALEA References: 83.2.5			
Review: Annual	Authority: Chief Michael A. Keller <i>M.A.K.</i>		

I. Purpose

The purpose of this General Order is to provide guidance for officers responsible for preserving an electronic crime scene and for recognizing, collecting and safeguarding digital evidence.

II. Policy

In order to maintain compliance with accepted electronic evidence collection and forensic examination procedures, department members will follow the procedures outlined in this General Order to guide them through identification and collection of electronic evidence. Furthermore, forensic examination of electronic storage devices will only be conducted by qualified forensic computer examiners.

III. Definitions

- A. Computer System:** A computer system consists of hardware and software that process data and is likely to include a case that contains circuit boards, microprocessors, hard drive, memory and interface connections; a monitor or video display device; a keyboard; a mouse; and peripheral or externally connected drives, devices and components. Computer systems can take many forms, such as laptops, desktops, tower computers, rack-mounted systems, minicomputers, and mainframe computers. Additional components and peripheral devices include modems, routers, printers, scanners and docking stations.
- B. Hard Drives:** Hard drives are data storage devices that consist of an external circuit board; external data and power connections; and internal magnetically charged glass, ceramic, or metal platters that store data. Hard drives may or may not be connected to a computer when found at a scene.
- C. External Hard Drives:** External hard drives installed in an external drive case increase the computer's data storage capacity and provide the user with portable data. Generally, external hard drives require a power supply and a universal serial bus (USB), FireWire, Ethernet, or wireless connection to a computer system.
- D. Removable Media:** Removable media are cartridges and disk-based storage devices. They are typically used to store, archive, transfer, and transport data and other information. These devices help users share data, information, applications and utilities among different computers and other devices.
- E. Thumb Drives:** Thumb drives are small, lightweight, removable data storage devices with USB connections. These devices, also referred to as flash drives, are easy to conceal and transport. They can be found as part of, or disguised as, a wristwatch, a



ANDOVER POLICE DEPARTMENT
GENERAL ORDER

Title: SEIZURE OF ELECTRONIC EVIDENCE

Number: O2508

Page: 2 of 7

Section: Investigations

pocket-size multitool such as a Swiss Army knife, a keychain fob, or any number of common and unique devices.

- F. **Memory Cards:** Memory cards are small data storage devices commonly used with digital cameras, computers, mobile phones, digital music players, personal digital assistants (PDAs), video game consoles, and handheld and other electronic devices.
- G. **Handheld Devices:** Handheld devices are portable data storage devices that provide communications, digital photography, navigation systems, entertainment, data storage, and personal information management.
- H. **Peripheral Devices:** Peripheral devices are equipment that can be connected to a computer or computer system to enhance user access and expand the computer's functions.
- I. **Computer Networks:** A computer network consists of two or more computers linked by data cables or by wireless connections that share or are capable of sharing resources and data. A computer network often includes printers, other peripheral devices, and data routing devices such as hubs, switches and routers.

IV. Regulations

(This section intentionally left blank.)

V. Procedures

A. Recognizing Potential Evidence

Officers must be able to recognize potential sources of electronic evidence and understand the evidentiary value of those sources. The following serves as a general guide:

1. Computer system – A computer system and its components can be valuable evidence in an investigation. The hardware, software, documents, photos, image files, email and attachments, databases, financial information, Internet browsing history, chat logs, buddy lists, event logs, data stored on external devices and identifying information associated with the computer system and components are all potential evidence.
2. Storage devices – Storage devices such as hard drives, external hard drives, removable media, thumb drives, and memory cards may contain information such as email messages, Internet browsing history, Internet chat logs and buddy lists, photographs, image files, databases, financial records, and event logs that can be valuable evidence in an investigation.
3. Handheld devices – Handheld devices such as mobile phones, smart phones, PDAs, digital multimedia (audio and video) devices, pagers, digital cameras, and global positioning system (GPS) receivers may contain software applications, data, and information such as documents. Concerning handheld devices, it is important to note that data or digital evidence may be lost if power is not maintained; data or digital evidence on some devices such as mobile or smart



ANDOVER POLICE DEPARTMENT
GENERAL ORDER

Title: SEIZURE OF ELECTRONIC EVIDENCE

Number: O2508

Page: 3 of 7

Section: Investigations

phones can be overwritten or deleted while the device remains activated; and software is available for mobile and smart phones that can be activated remotely to render the device unusable and make the data it contains inaccessible if the phone is lost or stolen. Officers should take precautions to prevent the loss of data on handheld devices they seize as evidence.

4. Peripheral devices: The devices themselves and the functions they perform or facilitate are all potential evidence. Information stored on the device regarding its use also is evidence, such as incoming and outgoing phone and fax numbers; recently scanned, faxed or printed documents; and information about the purpose for or use of the device. In addition, these devices can be sources of fingerprints, DNA and other identifiers.
5. Computer networks – The networked computers and connected devices themselves may be evidence that is useful to an investigation or prosecution. The data they contain may also be valuable evidence and may include software, documents, photos, image files, email messages and attachments, databases, financial information, Internet browsing history, log files, event and chat logs, buddy lists, and data stored on external devices. The device functions, capabilities, and any identifying information associated with the computer system; components and connections, including Internet Protocol (IP) and local area network (LAN) addresses associated with the computers and devices; broadcast settings; and media access card (MAC) or network interface card (NIC) addresses may all be useful evidence.

B. Securing and Evaluating the Scene

The responding officers primary consideration should be officer safety and the safety of everyone at the crime scene. All actions and activities carried out at the scene should be in compliance with departmental policy as well as Federal, State, and local laws. When securing and evaluating the scene, officers should:

1. Follow departmental policy for securing crime scenes (General Order O2516);
2. Immediately secure all electronic devices, including personal or portable devices (mobile phones);
3. Ensure that no unauthorized person has access to any electronic devices at the crime scene;
4. Refuse offers of help or technical assistance from any unauthorized persons;
5. Remove all persons from the crime scene or the immediate area from which evidence is to be collected;
6. Ensure that the condition of any electronic device is not altered;
7. Leave a computer or electronic device off if it is already turned off;
8. Take appropriate steps to ensure that physical evidence (DNA, fingerprints, etc.) is not compromised during documentation;
9. If a computer is on or the power state cannot be determined, officers should:



ANDOVER POLICE DEPARTMENT
GENERAL ORDER

Title: SEIZURE OF ELECTRONIC EVIDENCE

Number: O2508

Page: 4 of 7

Section: Investigations

- a. Look and listen for indications that the computer is powered on (e.g. sound of fans running, drives spinning, LED lights are on, etc.);
 - b. Check the display screen for signs that digital evidence is being destroyed;
 - c. Look for indications that the computer is being accessed from a remote computer or device;
 - d. Look for signs of active or ongoing communication with other computers or users such as instant messaging windows or chat rooms; and
 - e. Take note of all cameras or web cameras and determine if they are active.
10. Document any activity on the computer, components, or devices.

C. Preliminary Interviews

1. Officers should separate and identify all persons of interest at the crime scene and record their location at the time of entry onto the scene.
2. No one should be allowed access to any computer or electronic device.
3. Within the parameters of the department's policies and applicable laws, officers should obtain as much information from these individuals as possible, including:
 - a. Names of all users of the computers and devices;
 - b. All computer and Internet user information;
 - c. All login names and user account names;
 - d. Purpose and uses of computers and devices;
 - e. All passwords;
 - f. Any automated application in use;
 - g. Type of Internet access and Internet Service Provider (ISP);
 - h. Any offsite storage;
 - i. Installed software documentation;
 - j. All email accounts;
 - k. Security provisions in use;
 - l. Data access restrictions in place;
 - m. All instant message screen names; and
 - n. All destructive devices or software in use.

D. Evidence Collection

1. Officers must have proper authority – such as consent or court order – to search for and collect evidence at an electronic crime scene. If an officer is unsure if they have the authority to search for or collect evidence at an electronic crime scene they should consult a supervisor or prosecutor.
2. If the desktop, tower or minicomputer is off (refer to APD FORM 30 - Collecting Digital Evidence Flow Chart):
 - a. Document, photograph, and sketch all wires, cables and other devices connected to the computer.



ANDOVER POLICE DEPARTMENT
GENERAL ORDER

Title: SEIZURE OF ELECTRONIC EVIDENCE

Number: O2508

Page: 5 of 7

Section: Investigations

Rev. 04092014

- b. Uniquely label the power supply cord and all cables, wires, or USB drives attached to the computer as well as the corresponding connection each cord, cable, wire or USB drive occupies on the computer.
 - c. Photograph the uniquely labeled cords, cables, wires, and USB drives and the corresponding labeled connections.
 - d. Remove and secure the power supply cord from the back of the computer and from the wall outlet, power strip or battery backup device.
 - e. Disconnect and secure all cables, wires, and USB drives from the computer and document the device or equipment connected at the opposite end.
 - f. Make sure the CD or DVD drive trays are retracted into place; note whether these drives are empty, contain disks, or are unchecked.
 - g. Record the make, model, serial numbers, and any user-applied markings or identifiers.
 - h. Record or log the computer and all its cords, cables, wires, devices, and components according to department policy.
 - i. Package all evidence collected following department procedures to prevent damage or alteration during transportation and storage.
 - j. For laptop computers secure all batteries from the laptop.
3. If the computer is found on, for practical purposes, removing the power supply from the back of the computer (not from the wall outlet) is generally the safest option. If evidence of a crime is visible on the computer display, however, officers may need to request the assistance from personnel who have experience in volatile data capture and preservation.
 4. In the following situations, if the computer is found on, immediate disconnection of power is recommended:
 - a. Information or activity onscreen indicates that data is being deleted or overwritten.
 - b. There is indication that a destructive process is being performed on the computer's data storage devices.
 - c. The system is powered on in a typical Microsoft Windows environment. Pulling the power cord from the back of the computer will preserve information about the last user to login and at what time the login occurred, most recently used documents, most recently used commands and other valuable information.
 5. In the following situations, if the computer is found on, immediate disconnection of power is NOT recommended and personnel who have experience and training in capturing and preserving volatile data should be immediately contacted:
 - a. Data of apparent evidentiary value is in plain view onscreen.
 - b. Indications exist that any of the following are active or in use:
 - (1) Chat rooms.
 - (2) Open text documents.

	ANDOVER POLICE DEPARTMENT GENERAL ORDER	Number: O2508
	Title: SEIZURE OF ELECTRONIC EVIDENCE	Page: 6 of 7
		Section: Investigations

- (3) Remote data storage.
 - (4) Instant message windows.
 - (5) Child pornography.
 - (6) Contraband.
 - (7) Financial documents.
 - (8) Data encryption.
 - (9) Obvious illegal activities.
6. For mainframe computers, servers, or a group of networked computers, officers should secure the scene and request assistance from personnel who have training in collecting digital evidence from large or complex computer systems.
 7. Officers should collect, when lawful authority allows and when applicable, pieces of paper with possible passwords, handwritten notes, blank pads of paper with impressions from prior writings, hardware and software manuals, calendars, literature, and text or graphic material printed from the computer that may reveal information relevant to the investigation.
 8. Officers should not alter the power state of a handheld device and should immediately wrap the device in radio frequency-shielding material (faraday isolation bags or aluminum foil) to prevent the device from receiving a call, text message, or other communications signal that may alter the evidence.
 9. Computers and devices should not be accessed directly (i.e. mouse clicks, keyboard presses, etc.) except in emergency situations or by trained forensic computer technicians. If a situation warrants accessing computers immediately, all actions taken should be thoroughly documented. Data may be lost if a device is not properly handled or its data properly accessed.

E. Computers in a Business Environment

Business environments frequently have complicated configurations of multiple computers networked to each other, to a common server, to network devices, or a combination of these. Improperly shutting down these systems may result in lost data, lost evidence and potential civil liability. Officers should seek the assistance of personnel experienced and trained with these types of systems before taking any action.

F. Packaging, Transportation, Storage and Release of Digital Evidence

1. Package all digital evidence in antistatic packaging. Only paper bags and envelopes, cardboard boxes, and antistatic containers should be used for packaging digital evidence. Plastic material should not be used when collecting digital evidence because plastic can produce or convey static electricity and allow humidity and condensation to develop, which may damage or destroy evidence.



ANDOVER POLICE DEPARTMENT
GENERAL ORDER

Title: SEIZURE OF ELECTRONIC EVIDENCE

Number: O2508

Page: 7 of 7

Section: Investigations

2. Ensure that all digital evidence is packaged in a manner that will prevent it from being bent, scratched or otherwise deformed.
3. When transporting digital evidence, officers should:
 - a. Keep digital evidence away from magnetic fields such as those produced by radio transmitters, speaker magnets, and magnetic mount emergency lights. Other potential hazards include heated seats and any device or material that can produce static electricity.
 - b. Avoid keeping digital evidence in a vehicle for prolonged periods of time. Heat, cold and humidity can damage or destroy digital evidence.
 - c. Document the transportation of the digital evidence and maintain the chain of custody in compliance with department policy.
4. When storing evidence, officers should:
 - a. Ensure each piece of evidence is entered into the department's evidence management system according to department policy.
 - b. Ensure the evidence is stored in a climate controlled environment away from extreme temperatures or humidity.
 - c. Ensure that the evidence is not exposed to magnetic fields, moisture, dust, vibration or any other elements that may damage or destroy it.
5. When electronic evidence is returned to the owner, the releasing officer shall have the owner power on the device and ensure that it is working properly prior to release.
6. Electronic evidence containing child pornography shall not be released unless, at a minimum, the pornography has been removed and the storage media forensically cleaned (wiped).

Rev. 04092014

G. Forensic Analysis

1. Analysis of electronic evidence should only be done by technicians trained and experienced in the forensic examination of this type of evidence. If the department does not have qualified forensic computer examiners on staff, the electronic evidence shall be sent to a qualified laboratory for examination (Kansas Bureau of Investigation, Heartland Regional Computer Forensic Laboratory, Wichita Police Department, etc.).
2. Department procedures for submission of evidence to a laboratory should be followed.