


# FORT SMITH POLICE DEPARTMENT

## POLICIES AND PROCEDURES

<b>SUBJECT</b>	<b>Collection and Preservation of Evidence – Computer Related Equipment</b>		
<b>NUMBER</b>	<b>1106.15</b>	<b>EFFECTIVE DATE</b>	<b>March 1, 2002</b>
<b>SCHEDULED REVIEW DATE</b>	<b>Annually beginning November 1</b>	<b>ISSUE DATE</b>	<b>March 1, 2002</b>
<b>DATE REVIEWED</b>	<b>March 20, 2025</b>	<b>REVISION DATE</b>	<b>October 27, 2016</b>
<b>APPROVED BY</b>		<b>CALEA STANDARDS</b>	<b>LE 83.2.5</b>

### I. Purpose and Scope

- A. The purpose of this policy is to establish guidelines for the secure field seizure of computers, peripherals, handheld devices, computer-related equipment, and the potential digital evidence contained within such devices. This policy shall apply to all members of the Fort Smith Police Department (FSPD).

### II. Policy

- A. As computers, their related storage devices, and other types of electronic communications devices proliferate in our society, so does their use in conducting criminal activity. Criminals employ technology as a means of communications, a tool for theft and extortion, and as a means to hide incriminating evidence or contraband material. **Personnel specifically trained in computer forensics techniques and data recovery should be used when appropriate.**
- B. It shall be the policy of the FSPD to utilize every lawful means available to identify, investigate, and prosecute individuals and organizations that use these technologies in support of their illicit activities.

### III. Definitions

- A. Computer - an electronic, magnetic, optical, electrochemical, or other high-speed data processing device that performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, or communication facilities that are connected or related to the device.
- B. Computer network - the interconnection of two or more computer systems by satellite, microwave, line, or other communication medium with the capability to transmit information among the computers.
- C. Computer forensics - the application of computer investigation and analysis techniques to gather evidence suitable for presentation in a court of law.

Page 1 of 10	Effective Date: 3/1/2002
Subject: Collection and Preservation of Evidence – Computer Related Equipment	Number: 1106.15

- D. Computer system - the product of the use of a computer, the information stored in the computer, or the personnel supporting the computer, including computer time, data processing, and storage functions.
- E. Computer software - a set of computer programs, procedures, and associated documentation related to the operation of a computer, computer system, or computer network.
- F. Data - a representation of information, knowledge, facts, concepts, or instructions that is being prepared or has been prepared in a formalized manner and is intended to be stored or processed, is being stored or processed, or has been stored or processed in a computer.
- G. Dongle - a small piece of hardware that connects to a computer. Originally used to refer only to software-protection dongles; however, currently “dongle” is used to refer to any small piece of hardware that plugs into a computer.
- H. Faraday container – an enclosure formed by conductive material or by a mesh of such material, used to block electric fields and protect sensitive electronic equipment from external radio frequency interference.
- I. Handheld device – a device such as a smart phone, tablet, mp3 player, etc.
- J. Peripherals - any device on the outside of a computer used in conjunction with a computer for the purpose of processing, manipulating, storing, transmitting, printing or displaying the product of a computer. (e.g., monitors, modems, keyboards, printers, disk drives, media storage drives, mouse, or cables).
- K. Removable media – digital storage media such as CDs, DVDs, Zip disks, Jazz disks, floppy disks, external hard drives, memory cards, thumb drives, SIM cards, etc.
- L. SIM – a Subscriber Identity Module (SIM) card is a portable memory chip used mostly in cell phones.
- M. UPS - an uninterruptible power source that provides power to the computer in the event of a power failure.
- N. PC card – a type of peripheral interface designed for laptop computers.

#### **IV. Other Electronic Devices and Digital Evidence**

- A. Electronic devices, such as the ones in the list below, may have the capability to store digital data and therefore may contain potential digital evidence associated with criminal activity. Unless an emergency exists, the device should not be operated. Should it be necessary to access information from the device, all actions associated with the manipulation of the device should be documented to preserve the integrity of the data. Many of the items listed below may contain data that could be lost if not handled properly.
- B. Examples of other electronic devices, including computer peripherals:
  - 1. Audio recorders;
  - 2. Handheld devices;

Page 2 of 10	Effective Date: 3/1/2002
Subject: Collection and Preservation of Evidence – Computer Related Equipment	Number: 1106.15

3. Chips;
4. Copy machines;
5. Digital cameras;
6. Dongles;
7. Drive duplicators;
8. External drives;
9. Fax machines;
10. Memory cards;
11. Floppies, diskettes, CD-ROMs;
12. GPS devices;
13. Pagers;
14. Palm Pilots/electronic organizers;
15. PC cards;
16. Printers (if active, allow to complete printing);
17. Removable media;
18. Scanners;
19. Smart cards/secure ID tokens;
20. Telephones;
21. Video game consoles;
22. Wireless access points.

## V. Procedures

These procedures should be adapted as necessary based upon the situation. The Computer Forensics Unit (CFU) is available for call out to respond to crime scenes to seize and/or process digital evidence when requested by a supervisor. The supervisor will contact a Criminal Investigations Division (CID) supervisor, who will determine the necessity of sending out a Computer Forensics Analyst. If adequate direction can be given remotely, the Computer Forensics Analyst may direct field personnel to seize the equipment. **Any actions taken should not add, modify, or destroy data stored on a computer or other media.**

- A. Legal - it is the responsibility of the case investigator, whether assigned to the CFU or not, to ensure digital evidence submitted is properly seized. The CFU will not process digital evidence seized outside the boundaries of the Arkansas Rules of Criminal Procedure. Before

Page 3 of 10	Effective Date: 3/1/2002
Subject: Collection and Preservation of Evidence – Computer Related Equipment	Number: 1106.15

an investigator can use evidence obtained from a computer in a legal proceeding, the following legal requirements must be met:

1. The investigator must establish probable cause for the issuance of a search warrant or develop a lawful exception to the warrant requirement;
2. The investigator must use appropriate collection techniques so as not to alter unnecessarily or destroy any potential evidence;
3. The investigator should ensure trained personnel, in a speedy fashion, with expert testimony available at the time of trial, complete the forensic examination of the evidence.

B. General

1. Ensure the safety of all individuals at the scene and secure the crime scene in a manner consistent with FSPD Policy 1106.14.
2. Ensure all persons are removed from the immediate area from which evidence is to be collected.
3. Evaluate the scene and formulate a search plan.
4. Identify potential evidence. The recognition of potential electronic evidence is of primary importance to the investigator. The investigator must be able to answer the following questions:
  - a. Is the device contraband or fruit of a crime? (e.g., Was the software or hardware stolen?);
  - b. Is the device a tool of the offense? (e.g., Was the equipment actively used to commit the offense, such as making fake IDs or other counterfeit documents?);
  - c. Is the device incidental to the offense? (e.g., Was the equipment being used to store evidence of the crime?);
  - d. Is the computer equipment integral to the offense *and* to storing evidence of that offense? (e.g., Was the computer used to attack other systems and store the stolen information?);
  - e. Keyboards, the computer mouse, diskettes, CDs, or other components may have latent fingerprints or other physical evidence that should be preserved. Chemicals used in processing latent prints can damage equipment and data. Therefore, latent prints should be collected after electronic evidence recovery.
5. Once a computer or device's role in the crime is identified, the investigator should evaluate the following questions:
  - a. Does probable cause exist to seize the hardware;
  - b. Does probable cause exist to seize the software;

Page 4 of 10	Effective Date: 3/1/2002
Subject: Collection and Preservation of Evidence – Computer Related Equipment	Number: 1106.15

- c. Does probable cause exist to seize data;
  - d. Where will the search be conducted;
  - e. Is it practical to search the computer system on site or must the examination be conducted at a laboratory?
  - f. If the system is removed from the premises to conduct the search, must the computer system or copies of the seized data be returned to the owner/user before trials?
6. Protect the integrity of the evidence. 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 ensure its admission in court.
7. All potential evidence should be secured, documented, and/or photographed.
- a. The first responding investigator assigned should secure the computer or device as evidence.
  - b. Documentation of the scene is an ongoing process throughout the investigation. It is important to accurately record the location and condition of computers, storage media, other electronics devices, and related conventional devices. The investigator should document the following in detail:
    - 1. Observe and document the physical scene, such as the position of the mouse and the location of the components relative to each other;
    - 2. Document the condition and location of the computer system, including power status of the computer;
    - 3. Identify and document related electronic components that will not be collected;
    - 4. Photograph the entire scene to create a visual record as noted by the first officer to arrive on the scene; and
    - 5. Photograph the front of the computer as well as the monitor screen and other components. Also, take written notes as to what appears on the monitor screen.
8. Conduct interviews. Investigators should obtain as much information 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 applications in use.
  - g. Type of internet access.
  - h. Any offsite storage.

Page 5 of 10	Effective Date: 3/1/2002
Subject: Collection and Preservation of Evidence – Computer Related Equipment	Number: 1106.15

- i. Internet service provider.
- j. Hardware and software documentation.
- k. All e-mail accounts.
- l. Security provisions in use.
- m. Webmail account information.
- n. Data access restrictions in place.
- o. All instant message screen names.
- p. All destructive devices or software in use.
- q. MySpace, Facebook, or other online, social networking website account information.
- r. Any other relevant information.

C. PCs, desktops, all-in-ones, laptops, Macs, etc

1. The scene should be searched to determine if any wireless networks or networking devices exist. **For networked or business computers, the investigator shall consult a computer specialist for assistance prior to seizing the computer or any component thereof. The investigator should not pull the plug on a networked or business computer as this could result in:**
  - a. **Severe damage to the system;**
  - b. **Disruption of legitimate business; and**
  - c. **Unnecessary liability for the FSPD and the officer.**
2. If the evidence computer or device is connected to a network:
  - a. Assistance should be sought from the system administrator in isolating the computer or device from the network, presuming the administrator is not a suspect in the case. *Note: If the system administrator is a suspect in the case, assistance should be sought from personnel knowledgeable in the network's operation;*
  - b. Isolate and remove the evidence computer or device from the network immediately.
3. Document the location and condition of all computers and/or devices. Photograph the entire scene.
4. Document any open file(s) on the computer. Photograph the computer monitor screen or any other displays.
5. The examiner may choose to capture live memory. See Live Capture Module.
6. Shutdown procedures:
  - a. **STOP! If data encryption is in use on a computer, data storage device, or other electronic device and it is improperly powered off during digital evidence collection, the data it contains may become inaccessible. Consult a CFU member for guidance.**

Page 6 of 10	Effective Date: 3/1/2002
Subject: Collection and Preservation of Evidence – Computer Related Equipment	Number: 1106.15

- b. **Unplug the device from the back of the computer, then the wall. Macs are an exception to this rule. Power them down normally via the operating system (OS).**
  - c. If the device is powered by an internal battery, remove it. If this is not possible, power the device down normally via the OS.
  - d. Place evidence tape over any drive slots.
  - e. Remove any connected external media after device is powered down.
- 7. Document all connections to the computer. Photograph all wired connections.
- 8. Search the scene for passwords, account numbers, or other pertinent information.
- 9. Document all actions taken.
  
- D. Removable Media
  - 1. Document and photograph the location and condition of all removable media.
  - 2. Remove any connected external media (e.g., external drives or thumb drives) after the computer has been powered down.
  
- E. Handheld Devices
  - 1. Document and photograph the location and condition of all handheld digital devices, including on-screen data.
  - 2. If the device is on, do not turn it off, especially fingerprint-protected devices.
  - 3. Turning the device off could activate lockout procedures.
  - 4. Handheld devices may lose data or activate security measures if the battery is allowed to fully discharge. If you suspect the battery will die before the device is processed by the CFU, contact a CFU member for guidance.
  - 5. If the phone is off, remove the battery if possible. It's okay to store the battery in the same evidence container as the phone. Leave SIM and memory cards in the phone so they don't get lost.
  - 6. Photograph the screen(s).
  - 7. Interview suspects/witnesses to attempt to obtain PINs, pattern codes, or other security codes.
  - 8. Put the device into "Airplane Mode" or similar function.
  - 9. If this is not an option, Faraday containers are available from the CFU.
  - 10. If you obtain the security code, go into the settings menu and disable the security pass code requirement.
  - 11. The courts have held actions taken to preserve data generally are not 4<sup>th</sup> Amendment violations and do not constitute searches.
  - 12. Do not look at any other data on the phone unless an emergency exists. Do not attempt to obtain the phone's number.
  - 13. Search the scene for any removable media, passwords, or other data and evidence. In cases of water submerged devices, contact the CFU immediately so we can start the process of cleaning/drying and minimize corrosion and data loss.
  - 14. Document all actions taken.
  
- F. Evidence - Any item to be removed from the scene should be properly packaged and

Page 7 of 10	Effective Date: 3/1/2002
Subject: Collection and Preservation of Evidence – Computer Related Equipment	Number: 1106.15

secured. Special precautions should be taken when packaging, transporting, and storing electronic evidence. To maintain chain of custody of electronic evidence, document its packaging, transportation, and storage. The electronic evidence will be packaged, transported, and stored in the following manner:

1. Packaging procedure:

- a. Ensure all collected electronic evidence is properly documented, labeled, and inventoried before packaging;
- b. Pay special attention to latent or trace evidence and take actions to preserve it;
- c. Pack magnetic media in antistatic packaging. Avoid using packaging materials that can produce static electricity;
- d. Avoid folding, bending, or scratching computer media such as diskettes, CD-ROMs, and tapes;
- e. Ensure all containers used to hold evidence are properly labeled.

2. Transportation procedure:

- a. Keep electronic evidence away from magnetic sources. Radio transmitters, speaker magnets, and heated seats are examples of items that can damage electronic evidence;
- b. Avoid storing electronic evidence in vehicles for prolonged periods of time. Conditions of excessive heat, cold, or humidity can damage electronic evidence;
- c. Ensure computers and other components are packaged in containers and secured in vehicles to avoid shock;
- d. Maintain the chain of custody of all evidence transported.

3. Storage procedure:

- a. Ensure evidence is inventoried and submitted consistent with FSPD Policy 1102.02;
- b. Any digital evidence seized shall be transported to the evidence vault or Computer Forensics Lab as soon as practical, using the proper chain of evidence form;
- c. Store evidence in a secure area away from temperature and humidity extremes;  
Protect it from magnetic sources, moisture, dust and other harmful particles or contaminants;
- d. The CFU will retrieve the evidence for processing at a later time.

G. Special Considerations

1. Criminals have been known to sabotage their computers with small explosive charges or voltage surges meant to destroy the computer and all data. This should be a concern for anyone who suspects a computer system has been tampered with.

Page 8 of 10	Effective Date: 3/1/2002
Subject: Collection and Preservation of Evidence – Computer Related Equipment	Number: 1106.15



2. Even unsophisticated criminals can rig a computer to purge all of its data in an instant if the wrong key is pushed or if other inputs occur locally or from a remotely networked site. There are several scenarios that will render all evidence on-site useless and destroy links to any data being stored or accessed off-site.
3. When there is a legitimate business use for a computer being seized, any improper command could destroy legitimate business records, leaving the seizing agency and individual possibly liable for any business lost while these records are reconstructed.

## VI. Limitations

### A. Computers

1. Networked:
  - a. Unplugging a suspect computer from a network may cause data loss and could potentially damage other computers on the network;
  - b. Computer networks can be technically complex and may prevent collection of evidence in a timely manner. *Note: If the system administrator is a suspect in the case, assistance should be sought from other personnel knowledgeable in the network's operation.*
2. Non-networked:
  - a. Powering down a suspect's computer may cause data loss and potentially damage the operating system;
  - b. If, while securing the computer, the analyst believes evidence may be destroyed or manipulated, the computer should be forcibly shut down.

### B. Removable Media

1. Most removable media is very small, often hard to locate, and often overlooked;
2. Thumb drives may be disguised or obfuscated to thwart detection;
3. Some removable media is susceptible to immediate physical destruction.

### C. Handheld Devices

1. Active devices are susceptible to data destruction due to network communication;
2. Mobile devices may lose data or initiate additional security measures once discharged or shut down;
3. Blocking radio frequency (RF) signals: may drain the battery; may be expensive; is not always successful; and may result in the alteration of data;
4. Some components and devices are susceptible to immediate physical destruction and should be physically secured;
5. A device may be protected with a password, PIN, token, or other authentication mechanism. The suspect may be queried for this information during the initial interview.

## VII. Evidence Preservation: Crime Scene/Field Response

Page 9 of 10	Effective Date: 3/1/2002
Subject: Collection and Preservation of Evidence – Computer Related Equipment	Number: 1106.15

- A. The purpose of this procedure is to secure digital evidence located at a non-laboratory location to preserve its integrity for further forensic processing. When requested, the CFU will assist any case investigator with the proper drafting and execution of search warrants or consensual searches for digital evidence to ensure the evidence is properly seized.
- B. This module describes procedures to follow when providing digital forensics assistance at non-laboratory locations. The physical seizure of evidence from any crime scene can be conducted by any peace officer following the current guidelines for seizing electronic evidence. The CFU will conduct training in the proper seizure procedures as requested and as necessary. All standard procedures regarding evidence handling apply.
- C. A digital forensics field response kit may contain some of the following
  - 1. Digital camera;
  - 2. Sterilized removable media;
  - 3. Forensic computer or laptop;
  - 4. Hardware and software write-blockers;
  - 5. Forensically sound boot disks;
  - 6. Mobile device acquisition tools;
  - 7. Tool kit (screw drivers, flashlight, etc.);
  - 8. Evidence packaging materials;
  - 9. Notepads;
  - 10. Gloves;
  - 11. Evidence logs;
  - 12. Anti-static bags;
  - 13. Radio frequency shielding material.