

	Policy & Procedures				No. 2.09	
	Subject: Searching & Seizing Electronic Devices					
	Issuing Authority: Chief of Police			Effective Date: 10/02/2014	Review Date: 11/13/2023	
					References:	
Review						
Revision	02/21/2016					
Reissued	1/28/2018					
Dates:	11/03/2020					

CALEA STANDARDS

83.2.5

1. Policy

The Canton Police Department recognizes the frequent use of computer equipment in criminal activity. All offices shall consider the evidentiary nature of computer related equipment and handle it according to this procedure unless directed by specially trained personnel consulted for a particular case either from within the department, the Massachusetts State Police or the District Attorney's Office.

The intent of this written directive is to provide guidelines to officers, when searching for and/or seizing computers and other electronic equipment or devices, which are capable of storing data in electronic format.

2. Seizure of Computer Equipment 83.2.5(1)

- A. Data contained on computer systems can be damaged, altered, or destroyed if proper procedures are not followed. Officers should be aware that the seizure of computer equipment is a process at times more complicated than the seizure of typical physical evidence and specialized knowledge and procedures may be required.
- B. If during the course of an investigation, officers become aware that evidence of a crime may be contained within a computer, computer related system, or another type of digital storage device, they shall whenever possible, seek the advice of a specialist.

In all cases, the officer's actions shall be in compliance with applicable State and Federal laws, as well as Department policies, including Collection and Preservation of Evidence Policy.

In circumstances where time does not allow for consultation with a specialist prior to the incident, the following procedures shall be followed during seizure of computer equipment and similar devices: **83.2.5(1)**

- Initially, assess what action is necessary to prevent the destruction or alteration of such evidence;
- Prevent the removal, shut down, or start-up of the equipment;
- Prevent computer equipment and/or digital storage devices from being connected or disconnected from such things as power sources, telephone lines, cable modems, networks, or other peripheral devices;
- Prevent the removal, destruction, or alteration of computer equipment programs or files stored on any type of digital storage media;
- Notify a member of our CIU who in turn will notify an agent from the MSP or the DA's office who are computer investigation specialists or forensic examiners.

3. Search for Computer Equipment 83.2.5(1)

- A. All searches for computer equipment shall be made in accordance with pertinent Federal and State law, as well as other existing Department directives.
- B. When initially preparing to search for computer equipment, under the proper authority of a warrant or an exigency exception, officers shall:
 - Secure the scene and not allow anyone to manipulate the computer system in any way.
 - Photograph, videotape, and/or diagram the entire computer system so that connections, screen settings, etc. may be replicated at a later date and note the computer display of date/time in comparison to actual date/time.
 - Disconnect modems and communication devices at their source; (Note: In some cases, depending on the nature of the investigation, it may be necessary to allow the computer system to remain attached to the network or communication devices to facilitate the investigation);
 - Disconnect power sources from their source (see note in above paragraph);
 - Label all connections in order to replicate the setup of the system;
 - Label and package all items in non-static (i.e.: no plastic bags) containers for transportation;
 - Seize all books, manuals, software, diskettes, and other information or storage devices related to the computer system; **83.2.5(1)**

- Seize any and all information relative to the possible passwords, indicators of ownership, or other items pertinent to the investigation; **83.2.5(1)**
- Transport all computer related items, ensuring that they are kept away from electromagnetic sources to include radio transmitters (i.e. the trunk of a patrol car where the radio is mounted in the trunk);
- When securing all computer evidence, be certain special notations are placed on the items that are not to be handled, turned on, or “booted” unless by authorized computer forensic personnel.

4. Search of Computer Equipment 83.2.5(1)

- All searches of computer equipment shall be made in accordance with pertinent Federal and State law, as well as other existing department directives.
- Computer and/or digital storage equipment seized during the course of an investigation shall be examined only by personnel with specialized training. **83.2.5(1)**
- Such examinations shall be done in accordance with accepted contemporary computer forensic procedures as trained, which may include precautions to preserved all programs, data and files, and prevent the activation of any destructive programs.

5. Wireless or Cellular Devices 83.2.5(1)

A. Potential evidence contained in wireless and cellular devices:

- Numbers called
- Numbers stored for speed dial
- Caller ID for incoming calls
- Incriminating photos
- Other information contained in the memory of cell phones could include:
 - o Phone numbers
 - o Names and addresses
 - o PIN numbers
 - o Voice mail access number
 - o Voice mail password
 - o Debit card numbers
 - o Calling card numbers
 - o E-mail/Internet access information
 - o The on-screen image may contain other valuable information
 - o Pictures/videos

B. ON/OFF Rule

- If the device is “on”, do not turn it “off”.
 - o Turning it off could activate a lockout feature
 - o Write down all the information on display or take a photo
 - o Take any power supply cords, if present.

- If the device is “off”, leave it “off”.
 - o Turning it on could alter evidence on the device
 - o Upon seizure, be sure to hand it over to trained personnel.
 - o Make every effort to locate any ownership information and service provider information for the device.

6. Facsimile (Fax) Machines 83.2.5(1)

- A. Fax machines can contain:
 - Speed dial lists
 - Stored faxes- both incoming and outgoing
 - Fax transmission logs – both incoming and outgoing
 - Header line
 - Clock setting
- B. If a fax machine is found “on”, powering it down may cause loss of the last number dialed and/or stored faxes.
- C. Search procedures and issues:
 - Record the telephone number that the fax line is plugged into
 - Header line should be the same as the phone line; user sets the header line.
 - All manuals should be seized with the equipment, if possible.

7. Caller ID Devices 83.2.5(1)

- A. May contain telephone numbers and subscriber information from incoming telephone calls.
- B. Interruption of the power supply to the device may cause loss of data if it is not protected by an internal battery backup.
- C. Document all stored data prior to seizure, or a loss of data may occur.

8. Other Storage Devices 83.2.5(2)

Electronic storage is constantly evolving and advancing rapidly. Offices should learn to recognize other devices and objects capable of storing data in an electronic format (such as PDA’s) which may contain chips, external drives, USB flash media, etc., so that these items may be seized and analyzed as the other categories listed previously. Similar care and protective measures should be used to prevent any loss of data prior to analysis by trained personnel.