

St. Helens Police Department

Policy Manual

Computers and Digital Evidence

814.2.1 BUSINESS OR NETWORK COMPUTERS

If the computer belongs to a business or is part of a network, it may not be feasible to seize the entire computer. Cases involving networks require specialized handling. Officers should contact a certified forensic computer examiner for instructions or a response to the scene. It may be possible to perform an on-site inspection, or to image the hard drive only of the involved computer. This should only be done by someone specifically trained in processing computers for evidence. Cases involving networks require specialized training which is available through the Northwest Regional Computer Forensic Lab, the Oregon State Police or another agency having certified examiners.

814.2.2 FORENSIC EXAMINATION OF COMPUTERS

If an examination of the contents of the computer's hard drive, or floppy disks, compact discs, or any other storage media is required, forward the following items to the Computer Forensic Examiner:

- (a) Copy of report(s) involving the computer, including the Evidence/Property sheet.
- (b) Copy of a consent to search form signed by the computer owner or the person in possession of the computer, or a copy of a search warrant authorizing the search of the computer hard drive for evidence relating to investigation.
- (c) A listing of the items to search for (e.g., photographs, financial records, e-mail, documents).
- (d) An exact duplicate of the hard drive or disk will be made using a forensic computer and a forensic software program by someone trained in the examination of computer storage devices for evidence.

814.3 SEIZING DIGITAL STORAGE MEDIA

Digital storage media, to include hard discs, floppy discs, CDs, DVDs, tapes, memory cards, or flash memory devices should be seized and stored in a manner that will protect them from damage.

- (a) If the media has a write-protection tab or switch, it should be activated.
- (b) Do not review, access or open digital files prior to submission. If the information is needed for immediate investigation request Property Control to copy the contents to an appropriate form of storage media.
- (c) Many kinds of storage media can be erased or damaged by magnetic fields. Keep all media away from magnetic devices, electric motors, radio transmitters or other sources of magnetic fields.
- (d) Do not leave storage media where they would be subject to excessive heat such as in a parked vehicle on a hot day.
- (e) Use plastic cases designed to protect the media, or other protective packaging, to prevent damage.

814.4 SEIZING PERSONAL COMMUNICATION DEVICES

Personal communication devices such as cell phones, PDAs or other hand-held devices connected to any communication network must be handled with care to preserve evidence that may be on the device including messages, stored data and/or images.

- (a) Officers should not attempt to access, review or search the contents of such devices prior to examination by a forensic expert. Unsent messages can be lost, data can be inadvertently deleted and incoming messages can override stored messages.

St. Helens Police Department

Policy Manual

Computers and Digital Evidence

- (b) Do not turn the device on or off. The device should be placed in a solid metal container such as a paint can or in a faraday bag, to prevent the device from sending or receiving information from its host network.
- (c) When seizing the devices, also seize the charging units and keep them plugged in to the chargers until they can be examined. If the batteries go dead all the data may be lost.

814.5 DIGITAL EVIDENCE RECORDED BY OFFICERS

Officers handling and submitting evidence recorded by officers and stored digitally using digital cameras, audio or video recorders will comply with these procedures to ensure the integrity and admissibility of such evidence.

814.5.1 COLLECTION OF DIGITAL EVIDENCE

Once evidence is recorded it shall not be erased, deleted or altered in any way prior to submission. All photographs taken will be preserved regardless of quality, composition or relevance. Video and audio files will not be altered in any way.

814.5.2 SUBMISSION OF DIGITAL MEDIA

The following are required procedures for the submission of digital media used by cameras or other recorders:

- (a) The recording media (smart card, compact flash card or any other media) shall be brought to the Property and Evidence Section as soon as possible for submission into evidence.
- (b) Officers are not authorized to review or copy memory cards. The property officers are the only employees authorized to copy and/or distribute digital media made from the memory cards.
- (c) As soon as possible following the collection of evidence, the officer should remove the memory card from their digital camera and place the card into a plastic carrier or container. Officers shall write their name and the related case number on a memo or note and deposit the media in the criminal detective's desk or in box for processing.
- (d) The property officer will make a copy of the memory card using appropriate storage media. Once it is verified that the images are properly transferred to the storage media, the property officer will erase the memory card for re-use. The storage media will be returned to the appropriate police vehicle.
- (e) Officers requiring a copy of the digital files should make the request through the detective division.

814.5.3 DOWNLOADING OF DIGITAL FILES

Digital information such as video or audio files recorded on devices using internal memory must be downloaded to storage media. The following procedures are to be followed:

- (a) Files should not be opened or reviewed prior to downloading and storage.
- (b) Where possible, the device should be connected to a computer and the files accessed directly from the computer directory or downloaded to a folder on the host computer for copying to the storage media.

St. Helens Police Department

Policy Manual

Computers and Digital Evidence

814.5.4 PRESERVATION OF DIGITAL EVIDENCE

- (a) Only evidence technicians are authorized to copy original digital media that is held as evidence. The original digital media shall remain in evidence and shall remain unaltered.
- (b) Digital images that are enhanced to provide a better quality photograph for identification and investigative purposes must only be made from a copy of the original media.
- (c) If any enhancement is done to the copy of the original, it shall be noted in the corresponding incident report.