OVERVIEW
[83.2.5] 1. Computer equipment, cell phones, video evidence, and other electronic storage devices may be severely damaged or destroyed due to improper handling.

2. The device may be pre-programmed to erase or destroy data if certain start-up or shutdown procedures are not followed.

3. Improper handling may result in loss of data rendering the device or media useless for evidentiary value.

4. Since technology can change daily, best practices in the seizure, storage, and examination of electronic equipment is a dynamic process, so direct any questions to the Computer Crimes Unit (CCU).

TRAINING and ACCEPTED PRACTICES
1. Forensic examinations of seized computers, electronic media, cellular telephones and video equipment including digital and analog images should only be conducted by individuals who have formal training in Computer Forensics or Forensic Video Examinations and are authorized by the department to conduct those examinations.

2. Examinations of seized computer equipment and related digital evidence should be conducted within established and accepted practices and procedures recommended by organizations such as International Association of Computer Investigative Specialists (IACIS) and/or the Law Enforcement Emergency Services Video Association (LEVA).

DIGITAL EVIDENCE
1. If available, request Certified Electronic Evidence Collection Specialist (CEECS) or Certified Computer Forensic Examiner to assist.

2. If there is any uncertainty during the seizure process, report your concerns to the supervisor and request a CEECS.

3. Document and note the time of any actions during the seizure process.
4. If seizing COMPUTER SYSTEMS:
   - Isolate the computer and/or digital evidence.
   - Photograph the displayed screen, regardless of what is displayed, and determine if immediate power disconnection is necessary.
   - If the computer appears to be running an unfamiliar operating system or there is an indication of system/file encryption, request a CEECS.
   - Do NOT pull the power plug on business networks, mainframes, and/or UNIX systems. Contact a CEECS.
   - If acquiring volatile memory is necessary given the nature of the seizure, contact a Certified Computer Forensic Examiner for assistance.
   - If a CEECS has been requested:
     - Ensure the system does not lock prior to CEECS arrival.
     - Disconnect any external network connections.
   - Disconnect power. To disconnect, unplug the power connection directly from the back of the computer – NOT from the wall or surge protector/power source. For laptop type devices, remove the battery supply.
   - Photograph the surrounding area and document all connections to/from the computer system, including peripheral devices and network connections.
   - Search for and/or ask related persons about passwords, network configurations, and additional users.
   - Seize all books, manuals, software, hardware, and information related to the system.

5. If seizing CELLULAR TELEPHONES or PERSONAL DIGITAL ASSISTANTS (PDAs):
   - Seize the charging cord/cradle along with any software that may be related to the device.
   - These devices may have to stay charged to ensure evidence is not lost, so contact CCU to ensure the device is charged and securely stored.

6. Do NOT use standard plastic bags for packaging/storing electronic media. Use only paper bags, cardboard boxes, or anti-static bags and other containers made specifically for
electronic media.

7. Transport evidence, keeping it away from all electromagnetic sources, including the mobile radio. Prevent rough handling or dropping.

8. Impound seized equipment into evidence.

9. For evidence needing immediate analysis:
   - Document removing the property from the Property and Evidence Section.
   - Complete the Forensic Analysis Request form.
   - Document in the supplement the steps taken before depositing the evidence.
   - Place the evidence in the secured drop box located within the CCU office.
   - Notify the CCU Sergeant or OIC of the evidence drop, the DR number, and the criminal charge or case title. The CCU Detective assigned the case, documents actions taken in a supplement and notifies the case detective when the process is complete.
   - Complete the impound process and subsequent disposition.

VIDEO PROCEDURE

RECOVERING DETECTIVE/OFFICER

1. Should review the video on its home system to ensure the video is cued to the relevant position, when possible. If the media is electronic, ensure the data actually is on the media and that all players/codec’s are recovered or acquired at the source.

2. Include in the supplement:
   - The brand of the video system including model and serial numbers.
   - The time stamp on the system and any discrepancy with real time
   - If the system is electronic, the software name and version.

3. Immediately impound the video or electronic media under the correlating report number.

4. If use and recovery procedure on the system is not readily known because of the media on the system, seize the equipment following these guidelines and impound the equipment for CCU examination.

REQUEST for EXAMINATION ASSIGNED CASE DETECTIVE/OFFICER
1. Request examination of the evidence via a CCU Forensic Analysis Request form. Copies of the form are available in CCU and also are located on the department shared in the CCU folder.

2. Give a detailed description of the evidence to be recovered on the form to include:
   - Suspect descriptions.
   - Descriptions of suspect actions.
   - Descriptions of what files and folders to search for.
   - Images requested to be recovered.

3. Forward the request to the CCU Sergeant for assignment to an examiner. If the item needs immediate attention, notify the CCU Sergeant or a CCU member to make appropriate arrangements and follow steps in DIGITAL EVIDENCE #9., above.

4. Attach copies of any search warrants and/or consent forms for the examination to the form. CCU detectives will review the documents to ensure they are compliant with the latest in evidentiary rulings concerning the examination of digital media/video evidence. CCU detectives are available to assist with form information as needed.

EXAMINATION

See Investigations Order 4022/Computer Crimes Unit for responsibilities of the assigned examiner during an examination.

◆ ◆ ◆