OVERVIEW

1. If not handled properly, computer equipment, cell phones, video evidence, and other electronic storage devices may be damaged or destroyed causing the loss of digital evidence.

2. Digital evidence can be easily lost by unplugging the power source or allowing the battery to discharge.
   - Many computers, phones, and other electronic devices contain memory that requires continuous power to maintain digital information.

3. Many computers, phones, and other electronic devices encrypt data when powered down. Passwords are required to decrypt the data.

4. Devices may be pre-programmed to erase or destroy data if specific startup or shutdown procedures are not followed.

5. Contact the Digital Forensics Unit (DFU) for assistance when seizing digital devices, especially when devices are powered on, to reduce the risk of lost digital evidence.

TRAINING and ACCEPTED PRACTICES

1. Based on time constraints and circumstances, investigators may conduct physical examinations of electronics containing digital evidence.

2. When time permits, utilize DFU for evidence preservation and forensically sound analysis.
   a. Only personnel who have successfully completed the DFU Training Program and have been authorized by the department may conduct forensic examinations of seized computers, phones, other electronic devices, and video equipment.

   b. Examinations of seized computer equipment and related digital evidence are conducted within established and accepted practices and procedures recommended by organizations such as the International Association of Computer Investigative Specialists (IACIS), Scientific Working Group on Digital Evidence (SWGDE), and/or the Law Enforcement Emergency Services Video Association

(LEVA).

COMPUTER-RELATED EVIDENCE

DEFINITION

Computer Evidence: For this section only, computer evidence includes:

- Cartridges.
- Computers and computer systems.
- Electronic and magnetic data processing and storage devices such as central processing units.
- External hard disks.
- Fixed disks.
- Input/output devices such as keyboards, printers, monitors, and optical reader/write devices (scanners).
- Networking devices such as routers, modems, Wi-Fi adapters, and air cards.
- Optical storage devices or other memory storage devices.
- Related communications devices such as cellular telephones, modems, and facsimile devices; together with system documentation, operating logs and documentation, handwritten notes, logs, usernames and lists, software and instruction manuals, and related connectors and connecting cables.
- Tape drives and tapes.
- USB memory sticks (e.g., thumb drives).

DIGITAL EVIDENCE

1. If available, request a DFU member to assist with powered on devices.

2. If you are uncertain during the seizure process, report your concerns to your supervisor and contact a DFU member.

3. Document and note the time of any actions during the seizure process.

4. If seizing **COMPUTER SYSTEMS**:
   a. Photograph and label any wires or cables using tags or a permanent ink marking pen before disconnecting them.

   b. Photograph the display screen.

   c. If visible on the display screen, document the computer time and actual time (from your smartphone).

   d. Seize all cables along with digital evidence.

   e. Search for and/or ask related persons about passwords, network configurations, and additional

users.

f. Determine if the computer is powered on or off. If powered on and a DFU member is unavailable to assist, disconnect the power.
- To disconnect, unplug the power directly from the back of the computer, not from the wall or surge protector/power supply.
- For laptop-type devices, remove the battery. (Digital evidence may be lost upon power down, especially if passwords are unknown.)
- Do NOT pull the power on business networks, mainframes, and/or UNIX systems. Contact DFU.

5. If seizing **CELLULAR TELEPHONES or TABLET DEVICES**, determine if the phone or tablet is powered on or off.
   a. Best practice for a powered on phone or tablet is to place the device in airplane mode, turn off Wi-Fi and Bluetooth, connect it to a battery pack, and place it and the battery pack in a radio frequency blocking bag or enclosure. Thoroughly document each step. Contact DFU.

   b. If powered on, a DFU member is unavailable to assist, and the best practice procedure above is not possible, power down and/or remove the battery. (Digital evidence may be lost upon power down without a password to unlock the phone or tablet.)

6. Do NOT use standard plastic bags for packaging/storing electronic media. Use only paper bags, cardboard boxes, 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, contact DFU.

VIDEO PROCEDURE – **Recovering Detective/Officer**

1. 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 is on the media and that all players/codecs 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 DFU examination.

REQUEST for EXAMINATION

ASSIGNED CASE DETECTIVE/OFFICER

1. Request an examination of the evidence via a Crime Lab Request form.

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 DFU Sergeant for assignment to an examiner. If the item needs immediate attention, notify the DFU Sergeant or a DFU member to make appropriate arrangements.

4. Attach copies of any search warrants and/or consent forms for the examination to the form. DFU detectives:
   a. Will review the documents to ensure they comply with the latest evidentiary rulings concerning the examination of digital media/video evidence.

   b. Are available to assist with form information as needed.

EXAMINATION

See Forensic Services Division (FSD) Order 8120/Digital Forensics Unit for the responsibilities of the assigned examiner during an examination.

◆ ◆ ◆