Electronic Evidence Collection and Preservation

A. Initial Response

1. Secure the scene. As with any aspect of evidence collection, officer safety is paramount.
   a) Move suspects, witnesses, and by-standers away from electronic evidence and keep them away.
      Destructive processes can be initiated by a single keystroke or mouse click.
   b) Ensure the above-listed personnel are not in possession of potential evidence. Secure all electronic
      devices, including portable handheld devices. Some handheld devices have the ability to connect to
      the Internet or to the local network and may be used to initiate destructive processes.
   c) Preserve the condition of the electronic evidence. Some evidence may require processing for latent
      prints or DNA, therefore appropriate evidence handling procedures should be followed.

2. If the system or device is ON:
   a) The power state may be determined by listening for cooling fans, spinning drives, or lighted power
      indicators.
   b) NO files should be accessed, open dialog boxes clicked on, or screensavers stopped, or the system
      otherwise perused. Any active applications on the system or device shall be documented if they are
      viewable without any user interaction and, if possible, the display should be photographed. If the
      display screen is blank, the screen should not be “awakened.”
   c) If there are indications a destructive program or process is running and data is being destroyed
      (“wipe,” “format,” “delete,” “remove,” “erase”), the power cord should be pulled from the back of the
      computer immediately. If the device is a notebook/laptop/netbook computer, the battery should be
      removed first and then the power disconnected. The specific program or process that was running
      and required an immediate shut down shall be documented in the DR.

3. If the system or device is OFF: Leave it off. Powering on a system or device will likely alter the date and
   time stamps, access dates, and login information, and may trigger a destructive process or encryption.

4. All actions taken shall be documented in a DR.

B. Seizure of Electronic Evidence

1. Prior to collection, verification should be made that proper search authority exists (i.e., search warrant,
   consent search, plain view, or exigency).

2. Identify what items may be lawfully seized. If additional evidence items outside the scope of the search
   authority are identified, the appropriate search authority to seize those items shall be obtained.

3. Suspects, witnesses, and system administrators should be interviewed to determine their knowledge of the
   system or device, including the operating system(s), user account names, login names, passwords,
   encryption/security, offsite storage, and network.

4. The scene and evidence will be documented by video, photographs, or diagrams. This should include the
   back of the evidence item, any attached power cords, cables, or peripheral devices, and the area
   surrounding the evidence item.

5. It should be documented whether the system or device is powered ON or OFF. The powered state will
   determine the appropriate steps for proper evidence collection.

6. The area surrounding the system or device will be systematically searched for additional evidence.
a) User names, login names, passwords, and Internet addresses may be written on scraps of paper or in user manuals.

b) Storage media can be hidden and easily missed – MicroSD cards are about the size of a fingernail.

C. Collection of Electronic Evidence – System or Device is Already OFF

1. In most circumstances, a computer or electronic evidence should not be powered on or accessed unless directed by a computer forensic examiner.

2. The power cord shall be disconnected from the back of the computer. For notebook/laptop computers, the battery will be removed first and then the power disconnected from the computer.

3. Once the power is disconnected, make, model, serial number, service tag number, and/or any owner-applied marking or numbers shall be obtained.

4. All power cords, power supply adapters, batteries, and docking cradles will be collected.

D. Collection of Electronic Evidence – System or Device Already ON

1. Pulling the plug on a running system could result in lost data or lost evidence. Encryption may be in use, which may require the collection of volatile memory by forensic techniques. Volatile memory may also contain passwords or other evidentiary material that would be lost once power is disconnected. If available, the assistance of a certified electronic evidence collection specialist or a certified forensic computer examiner should be requested through the on-call Investigations supervisor.

2. Operating systems such as UNIX, Linux, and Macintosh are dependent on being shutdown using normal procedures otherwise data may become irrecoverable. Upon encountering UNIX, Linux, Macintosh, or any unfamiliar operating system, a certified electronic evidence collection specialist or a certified forensic computer examiner should be contacted.

3. If a certified electronic evidence collection specialist or a certified forensic computer examiner has been requested to respond, the computer system should be kept from going into hibernation or locked prior to their arrival. This may be accomplished by periodically moving the mouse, taking care NOT to click any of the mouse buttons or scroll wheel, or by pressing the “SHIFT” key on the keyboard. Any action taken shall be documented in the DR.

4. If it is determined a certified electronic evidence collection specialist or a certified forensic computer examiner will not respond to the scene, the computer’s power cord will be disconnected from the back of the computer. For notebook/laptop computers, the battery shall be removed first and then the power connector disconnected from the computer.

5. After disconnecting the power, the make, model, serial number, service tag number, and/or any owner-applied marking or numbers shall be obtained.

6. All power cords, power supply adapters, batteries, and docking cradles shall be collected.

E. Collection of Electronic Evidence – Business or Residential Server Already ON

1. Contact a certified electronic evidence collection specialist or a certified forensic computer examiner.

2. Pulling the power plug on a server or disconnecting network connections may result in the disruption of legitimate business, data corruption, and potential civil liability. It may be necessary to image the data on-site using forensic techniques.

F. Collection of Electronic Evidence – Cell Phones and other Handheld Devices

1. If the device is OFF, leave it OFF and remove the battery. Obtain the make, model, and all serial/equipment numbers, which are typically located underneath the battery. Collect the battery, docking cradle, connection cable(s), and power supply adapter. User manuals and device software should be collected if the search authority allows.
2. If the device is ON, the investigating officer should determine whether the device should be left ON or powered OFF. Some cell phones and handheld devices are password-protected, which activate once the device is powered OFF. Leaving the device ON creates some challenges such as disconnecting the device from network connectivity and keeping the device powered until the device can be forensically examined.

3. If the device will be collected ON:
   a) As soon as possible, disconnect the network connectivity of the device. Cell phones and networked handheld devices typically communicate with a network. Leaving the device connected to the network can result in the intentional or unintentional deletion or overwriting of data. Some devices can only store a set amount of data and incoming data will overwrite old data. Additionally, some cell phones have a “remote wiping” ability where a person could send a command to the device which causes the deletion of data.
      (1) The device may be disconnected from the network by contacting the cell phone provider and requesting they remove the device from the network.
      (2) If the collecting officer has the requisite training or knowledge, the officer may attempt to navigate through the device’s menu settings to place the device into “airplane” mode or disconnect it from the network. If this is done, document the specific actions taken (step-by-step details of how the appropriate menu was accessed and what selections were made) in the departmental report.
      (3) The device may also be shielded from the network through the use of a Faraday bag or radio frequency (RF) shielding device. If neither is available, either a metal evidence can or aluminum foil may be used. Disconnect all cables and wrap the foil completely around the device several times ensuring the antenna does not poke through.
   b) The docking cradle, connection cable(s), and power supply adapter. User manuals and device software should be collected if the search authority allows.
   c) Ensure the device remains powered on and charged through an electrical outlet until the device can be forensically examined. Plugging the device into a computer via a USB cable or other data cable should be avoided as this can alter data on the device. Notify the forensic examiner immediately.

G. Packaging Computers and Electronic Evidence

1. In order to protect electronic evidence and storage media, proper packaging procedures should be followed. Do NOT use plastic bags to package or store electronic devices or storage media. Electrostatic Discharge can damage electronic components and possibly result in the loss of data. Instead use PAPER BAGS, CARDBOARD BOXES, or ANTI-STATIC BAGS.
   a) Loose CD’s, DVD’s, and floppy disks may be packaged together in one evidence bag in a manner that prevents the media from being scratched or bent. Ensure the exterior of the packaging is bound securely to prevent the media from rubbing against each other during handling and transport. Do NOT affix tape/labels or write directly on the disc surface with a permanent marker or ball-point pen.
   b) USB flash drives and memory cards should be packaged separately.
   c) When packaging computers and peripheral equipment, ensure the computer case is securely shut. If the computer case or peripheral equipment will not close or is missing a panel, securely package the case in a PAPER BAG or CARDBOARD BOX.

2. If the electronic evidence contains latent, trace, or biological evidence, contaminated with biological fluids, drugs, or other hazardous material, or requires special handling, clearly mark the packaging as such. Forensic computer examination should be performed prior to latent, trace, or biological testing.
H. Transporting, Impounding, and Storing Electronic Evidence

1. Care should be taken while transporting and storing electronic evidence. The following should be avoided:
   a) Vibration
   b) Electromagnetic fields and radio signals (avoid transporting in patrol vehicle trunk)
   c) Static electricity
   d) Extreme temperature and humidity changes

2. All electronic evidence items must be issued a property item number prior to submitting a request for forensic examination.