IAPE STANDARDS SECTION 16 – DIGITAL EVIDENCE

IAPE STANDARD SECTION 16.1 – DIGITAL EVIDENCE

Standard: Digital evidence is a critical element of modern criminal investigation that should be maintained in strict adherence to the basic principles of evidence management from acquisition through disposition, chain of custody, preservation, storage, security, and limited access.

Definition:
Digital evidence refers to digital information that has probative value in either tending to prove or disprove a material fact in a criminal or civil case.

Digital information is any type of electronic file containing text, data, signal, image, video, or voice recording stored on magnetic, optical, or flash media.

Reasoning: Digital evidence generally consists of digital information from many different sources. The range of what is considered digital evidence continues to expand at a rate that corresponds with the growth in technology. The following sources are commonly encountered:

audio data may come from these sources:
- pocket digital voice recorders
- cellular phone voice recorders
- in-car audio recorders
- victim provided telephone communications
- 911 call data
- court approved wiretaps
- message centers
- interrogation audio
- internet feed
- baby monitor feed
- parabolic antenna surveillance feed

still images may come from these sources:
- digital cameras
- cellular phones
- internet feed
- traffic cameras
- automated teller machines

moving video image may come from these sources:
- digital cameras
- cellular phones
- surveillance video
- security cameras
- body worn video

- in-car cameras
- interrogation video
- internet feed
- traffic cameras
- nanny cams

digital data may come from these sources:

- automobile computer data, aka “black box data”.
- fleet management monitoring
- GPS tracking location and speed data
- email
- letters, memos, reports, or other text files

Standard 16.2 Digital Evidence Preservation

Standard: Digital evidence should be preserved in a manner that retains the original content and format of the files, ensures the integrity of the digital information stored, and documents any changes to the files for the duration of its storage as evidence.

Definition: Digital evidence preservation refers to specific standardized procedures that are used to govern the acquisition, storage, backup, duplication, access, distribution, and final disposition of digital information with evidentiary value.

Reasoning: The appropriate handling and management of digital evidence ensures the integrity and availability of the digital information throughout the duration of its custody.

The original file should retain the authentic content and format of the source information. The digital information may require its translation or storage in a usable format and condition that is capable of retrieval for the duration of the required retention of the digital asset.

Digital information files preserved as evidence must retain the authentic content and format of the original file. That is not to say that only original assets may be preserved as evidence, nor should this be misconstrued to mean that assets transferred from a primary source (i.e. camera SD card) to permanent storage (i.e. optical media) are not authentic assets. Digital evidence assets must be verifiable as an authentic and true rendering of the originally submitted evidence.

One method of verifying the authenticity of a digital asset is through the generation of an MD5, SHA-2 or similar algorithm using an application designed for authenticating files or assets. This should only be performed by a high technology investigations expert.

Another critical component of preservation is simply the ability to retain and retrieve a required asset using the agency's digital management system. If a digital asset cannot be retained, or is retained but cannot be retrieved, the evidentiary value of the digital asset is non-existent. Any preservation or storage method employed by an agency must provide authorized users with the ability to access the information contained.

Consumer quality DVDs/CDs have not demonstrated that they are capable of reliably storing digital information for long-term under all storage conditions. Some DVDs/CDs may only preserve digital information for as little as five years if exposed to improper storage, such as heat, humidity, dust, or sunlight. It is critical to use media that is designed and intended for long-term storage.

Standard 16.3 Digital Evidence Security

Standard: Digital evidence should be stored in a secure environment, with appropriate safeguards to ensure the security of individual digital assets, storage locations and systems used to facilitate the management of digital evidence.

Definition: Digital evidence security is a systematic process designed to protect the digital file from unauthorized access, alteration or removal. Digital evidence security often involves a combination of traditional physical evidence security and computer security processes and systems to accomplish the task of securely storing digital evidence and keeping a paper or computerized trail, with signatures, of who had access to the item and when.

Reasoning:
Regardless of whether digital evidence is physically stored on electronic media inside the property room, or stored on network storage or a single computer workstation; digital evidence must be protected from unauthorized access, alteration or removal.

Maintaining the security of digital evidence is of paramount importance. Security measures should begin at the time the first employee comes into the possession of the digital information. This first employee, "Employee zero," must make a determination on how best to preserve the original data. Is it possible to upload the data to a server, or should the entire device on which the recording was made be seized? Department policy, not an individual officer's judgment should guide when to seize the original recording equipment, and when copying the data to a duplicate original will suffice.

Once the original digital information data has been preserved, it should be uploaded to a dedicated digital information server or copied to media capable of preserving the information for the duration of its custody.

A decision should be made to place the server where it can be secure, and where uninterrupted power is available. Once the server is located and functioning, policy should direct staff on how and when to fill requests for duplicate originals. Ideally, the assigned investigating officer, or the detail supervisor, should approve all requests for digital information before it is copied. All completed data requests should go back to the assigned investigating officer for delivery to the requesting party, as one point of contact.

Who should be responsible for the data? Some options are having the server located in IT, Records, or Evidence, depending on the size of the agency and the technical computer ability of the assigned staff. Assigning the digital information server to Evidence is preferable, unless the evidence custodian(s) have limited computer skills. Placing the server in IT or Records is not discouraged if the staff is appropriately trained in chain of evidence issues and documentation of requests for copies made, and orders filled.

Security of original digital evidence data is maintained by:

- limiting access to files to only authorized persons
- ensuring that original image files never leaves the server or storage facility unless the item is formally released from custody or disposed following departmental policy
- running software that detects changes to content
- making automatic uploads of body camera data without user input.
- having in-car camera data uploaded by automatic activation, not selectively downloaded by operator input to eliminate claims of user tampering.
- having the main server backed up to cloud storage, or other third party (off-site) storage to guarantee access to the court and transparency on a daily basis
- ensuring that the original files are only accessed in a read only format and duplicate originals preserved to guarantee access and transparency; no "lost" or "misplaced" files

Standard 16.4 Digital Evidence Infrastructure

Standard: Agencies utilizing digital evidence should maintain the technological capacity to appropriately manage and store digital evidence, and adopt measures to accommodate future demands in digital evidence technology.

Definition: Digital evidence infrastructure refers to physical storage of digital evidence; as well as any software, storage media, hardware and network or cloud storage used to acquire, manage or store digital evidence.

Reasoning: Digital evidence management practices should be supported by the department's information technology infrastructure to ensure compatibility between digital evidence storage and existing and future information technology systems. Planning and decision making for digital evidence management processes and systems should account for future technology needs.

Digital evidence practices should support requirements and processes for the forensic analysis of digital evidence.

Departments should ensure that digital evidence management systems provide a clearly defined set of procedures and utilize a user interface that makes the process convenient and understandable to the end user. For example, providing a link to "read only" copies of all digital evidence in a case could simplify discovery and increase security. Numbered copies of photos could be provided under subpoena, and also identify where unauthorized copies, if any, may originate.

Digital images come in a variety of formats, some are common and some are proprietary. There is a need to convert one master copy to a common user-friendly format in order to store and duplicate the images on the department's designated digital evidence server. The original data (tape, flash memory drive, or optical storage in user-unfriendly format) should be booked into evidence as an archive copy, if needed. Law enforcement agencies should be prepared to store images in different common formats, or convert a duplicate original to a user-friendly format master copy.

Proprietary formats used for un-coding surveillance cameras in stores or from ATMs can create a critical need. It is always useful to know what the forensic digital capabilities of the local, county, or state crime labs are before seeking commercial assistance.

Agencies should have equipment available to copy and upload digital information from many different sources when the need arises. Digital data comes from many sources and should be uploaded to the designated digital evidence server to properly manage its distribution.