WHITE PAPER

CDW·G PEOPLE WHO GET IT™

DIGITAL EVIDENCE MANAGEMENT

New technologies to manage, enhance and distribute evidence are helping law enforcement agencies improve their processes.

Table of Contents:

Executive Summary

A few decades ago, detectives were encouraged to limit the number of photos taken at a crime scene because of the high cost of film and processing. That's not the case anymore. The cost for law enforcement agencies to capture images and sound has significantly decreased, and as a result, the amount of evidentiary data produced has expanded exponentially.

The cost of cameras has also dropped, putting them in the hands of more people. Cameras that take high-resolution photos are now available for less than $100, and millions are sold each year.

Meanwhile, the research organization Nielsen Company expects smartphone sales to surpass feature phone sales by the end of 2011. Many smartphones have a camera that can record high-resolution still and video images, as well as audio. So in addition to video from police cars, surveillance camera footage and crime scene photos, there's a good chance a civilian with a camera may capture crime scene evidence as well.

All of this points to the challenge for law enforcement today: it isn't capturing the evidence, but how to collect it, enhance it and, most important, control it. That requires systems and policies to manage photo, video and associated audio evidence.

The process of digital evidence management consists of four elements:

1) **COLLECTING:** Whether physically gathering evidence at the scene or pulling data back to the lab across a network

2) **STORING:** As evidence or in archives

3) **SECURING:** From intentional or unintentional contamination or deletion

4) **DISSEMINATING:** As evidence or property, to internal sources, external agencies, defense, prosecution or the media

Rules for evidence were originally established for audio and video, which at that time were in analog (tape) format. Current processes now include converting analog into digital format for management, enhancement and distribution.

Digital evidence isn't new. Computer forensics has existed for more than 20 years. Early on, courts struggled with defining digital evidence and how it should be managed, which is how best-evidence rules came about. These rules dictated that evidence had to be original, not a copy, but this pertained primarily to facsimiles and photocopies.

Eventually, the courts realized that copies of digital evidence, if gathered correctly, are as good as and maybe even better than the original analog data because the digital media can be frozen in time and preserved indefinitely.

File Formats

There are many different types of digital evidence — crime scene photos, audio recordings, video surveillance or other video footage, and more. Within these categories, evidence can take many different file formats.

Digital cameras are available from a variety of manufacturers. The resolution quality of the image is a function of how many megapixels the camera has, while capacity is a function of the memory card. Depending on the brand, digital cameras use a variety of file formats.

With the exception of the proprietary RAW formats, most file formats have been standardized among camera manufacturers. Most current photo viewing/editing software can also view the more common RAW formats. The RAW format is considered the best format for recording and storing digital images because it retains the greatest amount of digital information that the camera can capture.

Then there's video evidence, which may be collected from regular video surveillance, fixed covert surveillance or an in-car system. Investigators may struggle with proprietary formats when collecting video evidence.

Most systems have an export feature, but the majority of them export in a compressed format, which causes some loss of video data. Though there are certainly video cameras and digital video recorders that can capture images in high resolution and export data in an uncompressed format, users typically avoid these because of cost and the logistical limitations of storing large data files.

Proprietary or not, video formats are numerous and varied. Some recording devices even have multiple codecs (code-decode programs) and can be played only with a specific version of video player.

Law enforcement agencies sometimes create their own video for surveillance and crime scenes. Proper camera setup requires the user to choose the format in which the

images will be captured. There may be circumstances in which the original file must be altered.

When this happens, any conversion process must be addressed in an organization's standard operating policies, indicating how files will be managed and verifying that the process or procedure has been tested and validated to cause minimal or zero data loss.

The use of in-car video surveillance systems is also on the rise. Such systems include a camera, video and audio recorder, and wireless microphone, and are often integrated with vehicle-rugged notebooks.

Handling and storing video files created by in-car surveillance systems can be a challenge for public safety departments. In the past, most systems required the officer to enter the tape into an in-house cataloging system on a daily, weekly or monthly basis. Some agencies keep only video that might be needed for a criminal investigation or prosecution, or for liability reasons.

Whatever the type of evidence, video and audio media come from a variety of sources, and management of this media depends on where it comes from. In other words, it depends on whether the agency itself has created the audio or video files (at the crime scene or through surveillance, for example) or if it comes from an outside organization (such as commercial security camera images).

Most agencies know how to handle audio and video that comes from outside sources because it's easy for them to assume it is evidence and handle it appropriately. Crime scene video and images plus surveillance and audio recordings created by undercover officers should also be handled as evidence (property) and tracked accordingly.

Digital Evidence Collection Workflow

- **RESPONSE:** Respond to the scene to acquire media or have it shipped to agency lab
- **INTAKE:** Enter media into evidence system
- **ANALYST PROCESSING:** Enhancing and editing of media
- **REPORT:** Analyst completes report
- **PEER/SUPERVISOR REVIEW:** Peer review and supervisor approval
- **DISTRIBUTION:** Copies of results released to appropriate entities
- **ARCHIVE:** Media, reports and notes are archived

Maintaining Chain of Custody

Once law enforcement agencies obtain digital evidence, they must properly track and maintain control of it at all times so the data cannot be tampered with.

Fixed and in-car surveillance systems make it easy to access remote video and audio (or even stream it live) and to store it for later retrieval. However, organizations should place a priority on securing access so files can't be mishandled. Software is available that can limit and control access while providing for collaboration among those with the proper authority.

Court challenges to the validity of data (because of the potential for data modification, such as image editing) are of concern, making the ability to control the original file imperative. Another potential problem occurs when videos that shouldn't be shown to the public appear on the nightly news or YouTube because of a lack of controls that would prevent files from being copied.

Video, still images and audio files created by agencies themselves should be controlled in the same way that evidence is controlled. Software and hardware is available that can lock down files, log those who access files and track what they did with them, as well as identify original image and audio files.

There are cameras and audio equipment available today that can apply a digital fingerprint to an original file. All image files have a numeric value, commonly referred to as the hash value. Any evidence processing system should include a method for obtaining the hash value of an original image both before and after enhancement techniques have been used.

This doesn't mean that law enforcement must work only with the original file. In fact, it's just the opposite. These types of marking systems, along with good notes from the investigator, will show that the original file has not been altered and that the enhancement techniques were performed using an exact copy of the original file.

Organizations need to establish guidelines that control how audio and video files are handled, with all files being entered into the agency's property or evidence system. Evidence specialists must be thoroughly trained in handling audio and video media so that the files can be properly secured and stored. Most law enforcement agencies have strong property and evidence policies in place.

Mobile Video Considerations

The International Association of Chiefs of Police's report, *In-Car Video Camera Systems, Performance Specifications: Digital Video Systems Module*, establishes minimum requirements for in-car video systems. When choosing a mobile video solution, organizations should address the following factors regarding chain of custody:

- Does the manufacturer provide physical security for vehicle equipment?
- Are there mechanisms for proving that the digital multimedia evidence (DME) is original?
- Does the manufacturer include the CPU or hardware ID of the vehicle recorder in the DME Audit Log?
- Is there an ability to indicate where and when the DME was captured?
- Does the equipment provide electronic validation of location and time synchronization between recorders through the use of GPS equipment?
- Are the time and date on the records synchronized to back-office equipment?
- Does the manufacturer provide evidence that system components are time-synchronized?
- Can the manufacturer provide a recording stream that is unalterable?
- Does the manufacturer provide the capability of assigning authorization for media access?
- Does the manufacturer provide the capability of protecting the DME on removable media so that it cannot be accessed by unauthorized equipment?
- Does the manufacturer provide synchronization between the record streams and the telemetry streams from one or more mobile systems for playback?
- Does the manufacturer provide a method for the user of the vehicle recorder to log in and authenticate?

Storage Management

Storage and archiving have always been challenging. The latest wrinkle is how to apply analog processes to the digital world. Doing so requires the right technologies.

Write-once, read-many (WORM) secure digital memory cards have proven to be a popular storage media for law enforcement organizations bound to strict retention requirements. WORM SD storage is tamperproof, making it useful for storing unalterable, permanent photographic records and guaranteeing the legitimacy of evidence.

Digital cameras with compatible interfaces can write to the card, while any compatible computing device can read it.

Another type of storage media, solid-state drives (SSDs), use flash memory and deliver high performance. SSDs have no moving parts, making them more rugged and less susceptible to shock, vibration and extreme environments. They are well suited to surveillance applications that require ruggedness and reliability. What's more, they use less power than traditional hard disks, decreasing the drain on the battery or the amount of electricity required to run the notebook or surveillance system.

Whatever type of storage media is used, it must be connected to a computing device. There are several models for achieving this. One of the most simple is direct-attached storage, or DAS. This usually refers to storage attached to a local desktop computer or notebook, and can be a second hard drive or perhaps a few hard drives configured to appear as one large drive.

This type of storage is appropriate for small labs that have one or two analysts. DAS provides basic capability and is limited both in expansion and in sharing resources. The biggest downside to a DAS system is that when there's an equipment failure, the user or agency can lose all its data.

Another type of storage is network-attached storage, or NAS. This storage option is usually associated with smaller deployments in which all storage devices have their own IP addresses. NAS is easy to manage and usually comes with software that enables the administrator to schedule backups to other devices.

A third type of storage is a storage area network, or SAN. This is an enterprise option generally seen in larger departments. The scalability offered by being able to add more storage easily and higher speed performance makes a SAN a good option for large agencies.

Storage system selection directly relates to space and the cost of purchasing and then maintaining that space. Evidence room size has always been an issue in departments. One of the main problems is that once a department has built a room, eventually they'll outgrow it. Physical expansion isn't easy to do.

Unlike building costs, which seem to increase every year, digital storage has dropped in price every year. It used to cost around $2 per gigabyte. Now a gigabyte of storage costs about 10 cents, and a terabyte can be had for less than $100. So the cost of storage is becoming less of an issue every year.

Keep in mind that storing audio and video files can require an enormous amount of storage. A single video file can be as large as 6 to 10 gigabytes. A number of large cases can quickly overwhelm a server.

Here are some of the questions that need to be answered when establishing server size for managing audio and video files:

- How many cases a year will the server handle?
- How much data per case is anticipated?
- How is this data going to be stored for processing — on a local computer or a server?
- How is the data going to be archived — onsite, offsite or both?

When building a storage system, it's important to include both short- and long-term archiving systems in the plan. Organizations may want to consider information lifecycle management to rotate infrequently accessed data to less expensive types of storage.

Of course, data protection measures such as backup and proper continuity of operations planning are also critical. Archiving can be done to tape or disk and requires some form of redundancy. Data should also be archived offsite for disaster recovery — in case of a building fire, for example, or or a flood. However and wherever an organization stores its data, a high level of security should be in place to protect that data wherever it goes.

Securing Digital Evidence

Every day in the news, headlines blare about hackers or physical security problems and internal and external threats. Strong physical protection and cybersecurity are crucial to safeguarding digital evidence.

Just as law enforcement organizations store evidence in a locked room, systems containing image files should be separated from the department's normal production network. Guidelines and permissions need to be in place so that even support personnel can't access image evidence files without permission, logging and supervision.

Any outside workers coming onsite to repair computers, including government staff, still need to be supervised while they are accessing the system. It's too easy for someone working on the server to download or even mistakenly export or damage important files. Child pornography files are contraband, and anyone outside the investigation is essentially committing an illegal act if they view, export or erase the images.

A Cautionary Tale

A local agency received a DVR from a criminal investigation. The DVR worked its way through normal evidence channels, but because it was coming from far away, it didn't arrive in the lab and into the hands of the analyst for a few weeks.

The analyst hooked up the DVR and started the process to export the video using dates and times given to him from a source at the scene. The DVR appeared to be working well, so the analyst left it to run overnight. When the analyst got back into the lab the next morning, he found that the DVR had stopped exporting soon after it had started.

Most DVRs have a rollover period, meaning that after a predetermined amount of time — usually seven to 30 days — the DVR will begin recording over whatever is on the hard drive. In this case, it had been only about 12 hours, so the video files should still have been present.

But when the analyst checked the settings the next morning, he found that the DVR was set to clear out the database altogether and start over every 14 days — and he had begun the export on the 14th day. At midnight, the DVR had reset itself and started over, dumping the video evidence before it could be exported.

There are two problems here. First, the DVR was set incorrectly; it should not have been set to dump the entire database and start over. Second, the analyst should have checked the DVR settings prior to starting the export process. If he had done so, he could have unchecked the radio button that instructed the DVR to start over and would have had plenty of time to export the video.

Files should be locked down from read/write privileges as a normal course of procedure, with the privilege given only to the investigator or analyst. Again, consider digital files akin to paper files: Paper files are usually stored in a locked container where only people who have permission to access the file are allowed to do so. Evidence system software can be housed on the internal network, but no links to the actual digital evidence should be in the evidence tracking software.

It's important to remember that CDs, DVDs and DVRs seized from a suspect or obtained from outside surveillance cameras may contain viruses. Using imaging techniques learned from computer forensic processes can help departments isolate problems that might arise from media containing viruses. Such files can be imaged in a way that won't affect the department's system.

Forensics software can place the suspect media into a "container" that allows an analyst to look at the data without having a virus infect the analyst's computer. Video, audio and still images can be exported from these containers for further analysis by audio/visual analysts. At the very least, it's a good idea to keep virus software up to date.

In most analyst shops, it's a hard-and-fast rule that analysts work only one case per analyst computer. Every time a new case is started, a clean (cloned) operating system and tools are loaded back onto the analyst's computer. This ensures that there is no cross-contamination from previous cases.

The downside is that such careful attention to keeping computers untainted can be expensive for an audiovisual (A/V) forensics shop. Good, experienced analysts can work four to six cases at a time, and thus would need four to six computers to perform their duties. Forensic computers and software can be pricey — about $20,000 at a minimum to get two analysts up and running.

Also, even with a separate internal network for handling digital evidence, it's important to put proper security controls in place, with logging turned on, separate user accounts and established guidelines for users. Controlling who has access to what data and logging activities will help secure digital evidence and any casework that is being done. Use passwords and encryption for extra-sensitive data.

It's possible to have a digital evidence network that doesn't touch the outside world and still have Internet access in the lab. A separate, access-controlled Internet connection is a must for analysts and will provide them with the necessary access to codecs, software updates and other resources needed in the day-to-day operation of a functioning A/V lab.

Agency Policy Development

Every agency should develop a standard operating policy (SOP) for handling digital media. Due to the dynamic nature of technologies and procedures, the policy should be reviewed and updated periodically.

The policy should include normal evidence handling procedures that document who had custody and control of the evidence from the time the digital media was captured to final archiving. Establishing retention periods as part of the SOP will help the agency manage large files by determining when the media can be removed from its storage and archiving system.

Because some digital media begins life as analog media, the SOP should detail how the analog media will be converted to digital. Don't forget to define how the media should be authenticated to ensure that the original data was not altered and that copies of the original media were used for editing and enhancement during the conversion.

From a historical standpoint, it's good to remember that most of the hardware and software now used for analyzing digital media was used first by the general public. It was only recently that technology manufacturers began rewriting software or adding plug-ins aimed at addressing the specific needs of law enforcement. Therefore, the SOP should include techniques to validate hardware and software used throughout the audio and video collection and handling processes.

The SOP for digital media should also cover these elements:

- Proper collection techniques, taking care not to alter the original data
- Problems noted when DVRs compress digital files while exporting data to another source
- Proper handling techniques for digital media
- Proper techniques for analysis
- Storage and archiving
- Distribution to prosecution, defense and news media
- Roles and responsibilities of those who have access to the media, including managers, analysts and technicians
- The type of evidence system used to track the digital media, including evidence coming from outside as well as digital media and its copies in the lab
- The ability to track subnumbers, which are numbers attached to digital media that may have come from inside another piece of evidence, such as a second drive found in a computer or a disk found in a camera
- How to handle notes and reports, including peer review, supervisory and distribution systems (No reports should leave the lab until at least two sets of eyes have reviewed it.)
- How to handle subpoenas and discovery requests
- How to render conclusions and opinions in reports
- How to prepare courtroom presentations
- How to handle audit and review processes and who has signature authority

Meeting the Needs of the News Media

Law enforcement works with the news media on almost a daily basis. Much of what police departments are involved in is considered newsworthy, and so part of this process includes the release of digital evidence.

Video and audio files distributed by the news media come from numerous sources, including the public and news media staff themselves. Often, though, video or audio files captured by law enforcement (or captured by surveillance cameras and now controlled by law enforcement) need to be distributed, at least in part, to the news media.

It's best to develop policies for distribution of audio and video files and to appoint a specific person or group to serve as a primary point of contact with the press.

When preparing image files to release to the news media, file format for still images or video is generally not a concern. Most files can be exported in .png or .jpeg file formats, which can be easily provided to the press. However, control over distribution of images, whether stills or video, is a valid concern for most agencies. Although most images don't reach the level of contraband, the "how" and "to whom" of image distribution should be well documented.

Once an image is released to the news media or even to another agency, control of the image and how it can be used is lost for all intents and purposes. If a department wants to maintain strict control over the images they distribute, software tools are available that can apply a digital signature to the image, limiting copying and printing of the image to some extent.

In some instances, when an image needs to be released to the news media, there is also a need to protect some of the people in the image, such as undercover officers or victims. Analysts can use image-editing software to blur out identifiable features. Care should be taken to save the file in a format that prevents reversing the steps taken to protect the people in the image.

It's also good practice to have the metadata (which can contain a tremendous amount of information about the photo, such as location, the type of camera used and the owner of the camera) stripped from the image before distribution.

There is some debate about adding data that would mark a video or image in some sort of way — for example, inserting a frame with a control word. But with today's technology, such editing is too easy to remove or alter by whoever might have control of the files, so time spent on this type of project would be of little use.

CD/DVD duplicators have proven very useful for distributing information to multiple news media outlets. The duplicators have the ability to copy data to many CD/DVDs at once with only the push of a button. They also come in handy when law enforcement has seized a large number of CDs or DVDs because they can automatically create an ISO image of the original CD/DVD and handle a large stack of CDs or DVDs simultaneously.

When working with the news media, another set of eyes on a file is a must. Law enforcement also needs the ability to review and edit videos in a collaborative way. Large video wall installations are available that fuse several small displays into a cohesive unit for an impressive visual experience. Be sure a public information officer reviews and edits videos before distributing to the media.

Also, remember that any data given to the news media should be target-specific. That is, distribute only the minimum amount of information needed to assist an investigation. Never assume the media, if asked, will agree to use only portions of a video it's been given. This also applies to any audio that may be attached.

Future Trends

Going forward, two areas related to video and audio that need to be addressed are speed and quality. The upside to digital files is the ability to quickly access and distribute them in a timely manner. Editing and releasing files to prosecutors can be done in minutes as opposed to months. For simple cases, creating kiosks where both the prosecution and defense can review video files can lead to quick plea arrangements and speed up the judicial process.

There are newly developed cameras that will record in very high resolution and export with little or no compression. Some of the crime scene investigation techniques depicted on television can actually be done with the high-resolution images provided by these new devices.

Unfortunately, due to budget considerations, many legacy systems are still being used in state, local and federal agencies around the country. High resolution also brings large files, so having software and hardware capable of handling and storing these large files is a must.

In the future, interactive maps that include geographic location as well as internal floor plans with links to video cameras will enable investigators to logically and quickly access data needed to proactively or reactively investigate a crime.

Another nascent law enforcement tool is intelligent hardware and software. Right now, for the most part, a pair of eyes following hundreds if not thousands of video feeds is the standard approach to proactively monitoring for criminal or terrorist activities.

Software is currently being developed that, when configured, can monitor for things out of the ordinary, such as a crowd gathering, or a car stopped at a certain place on the road, or a briefcase or bag left sitting in a particular location. Facial recognition software is slowly becoming reality. When it identifies a suspect, the software sets off an alarm that calls a real person to respond to the situation.

For larger cases, software manufacturers can improve case management by developing tools that will allow teams of analysts to collaboratively attack a case. Today, a single analyst typically handles a case, no matter how much data it involves. But expecting one analyst to review all the data from numerous media sources is like asking one person to walk into a library and organize, clean up and enhance the entire library with no help.

That's not practical and makes it easy to overlook valuable information, especially as it relates to intelligence work. Public safety organizations need a case management tool that enables a lead analyst to assign selected portions of digital media to each team member and to target certain events for concentration while working as a team to better process very large media files.

All of this is within reach today. Concentrating resources in the form of money, people, hardware and software will enable organizations to reach the next level, realizing some very exciting audio and video evidence management capabilities.

Where to Go for Help

There is much work being done regarding video and audio evidence files. The Scientific Working Group on Imaging Technologies (SWGIT) is a good resource for guidelines and processes. Law Enforcement & Emergency Services Video Association (LEVA) and the National Technical Investigators' Association (NATIA) are useful resources for training and all things audio and video related.