To Save and Protect

Handling video evidence is a tricky business. Like any other piece of evidence, it is vitally important that it be handled correctly so that your results are credible in court. To that end, we've put together some tips and hints to make sure your video evidence puts criminals behind bars for good!

Retrieval – Master and Working Copies

A crime has been committed at a local gas station with a CCTV surveillance system. The system has recorded events that may be evidence to the crime. Now you must figure out how to retrieve and properly handle the video to ensure that, if it comes to it, the evidence will be credible in court.

The first step is to create a **master copy** of the video from the surveillance system recording. When it comes to the courtroom, this master copy is critical because it's what the court will look to in confirming the integrity of images presented during a trial. So you must be sure to both create a master and document your steps while doing so. The master should be copied from the CCTV system in the native file format, regardless of the format. There are several ways to create the master copy from the CCTV system, but your ultimate goal is to have it on a Write Once, Read Many times or WORM media (such as a CD-R or a DVD±R). Once you have created the master, store it securely. Its only use will be in court to protect the integrity of images produced as evidence.

Next you will need to create a **working copy**. The working copy is what you will use in the investigation. *Any enhancement of the video will be done to this copy only.* It's usually preferable to create the working copy in the native file format, but due to the large amount of proprietary CCTV formats out there, that won't always be possible. If that's the case, a format conversion will be necessary.

There are four main methods for format conversion:

Digital media with a proprietary file format. In this situation, direct conversion of the data is available by using functionality available from within the proprietary software that plays the video. Additional screen recording software is typically employed to complete the conversion process.

Digital media with a common file format. Some common file formats need conversion. This conversion can be performed by acquiring the correct video CODEC and employing it with a video player.

Output from an analog connection, such as a NTSC monitor output from a DVR, or connection via a VGA cable either from the DVR or from the replay PC.

Digital connections (such as network, USB or FireWire) typically provide either a proprietary or common file format. These formats can be converted via proprietary player or CODEC.

The end goal of each method is to create a video that can be easily played back and worked on without losing any data from the original format. Each of these options has benefits and limitations. It's important to consider these as you work through a digital video retrieval.

With your master and working copy of the video, you are now ready to use your evidence to work the case. *Here are a couple of things to keep in mind about the video:*

Make sure the original recording of the crime is not erased without authorization. This may leave your evidence open to be challenged in court.

Try to store your media in a clean, dry environment and keep it away from strong magnetic fields, strong light and chemical contamination to prevent damaging the video.

Keep your DVDs and CDs in individual cases to prevent scratching and damaging them.

Make sure you define and label the master and working copies of the video.

Audit Log

One of the best tips we can provide you is: *keep a detailed log of everything concerning the evidence.* From the moment you come in contact with the video to the moment the evidence is disposed of or stored, be sure to log every action taken on the video. In fact, if not already in place, it's a great idea to create a procedure that generates an audit log for every video. *Some key details to include in the audit log are:*

Details of the case.

Information about retrieving the evidence from the crime scene.

Details about the capture equipment used for retrieval.

Descriptions of the images captured.

Creation, storage and access to the master copy of the video.

Details on any analysis or clarification applied to the video.

Any copying of the master copy of the video.

Disposal details of the video and retention time of the video.

Keep in mind, when creating your audit log, make sure you have a date and time for every action in the log. Also, if you use software to enhance or process the video, check to see if the program creates an electronic log of the actions you take on the video. This may save you some time in creating your own audit log. Another helpful tool for creating an audit trail is having a Location, Equipment, and Incident Details Form to fill out while retrieving the video (see our example). Filling out a form like this at the crime scene will ensure that all of the pertinent information of the retrieval is accurately captured as soon as possible.

Location/Equipment/Incident Details Form

Location Details			
Contact Name:		Contact Numbers:	
Address:			
Installer/Provider:			

Equipment/Device Details	
Make/Model of Equipment:	
Serial No:	
Software Version:	
Total Number of Cameras:	
Recording Audio:	□ Yes □ No
Networked:	□ Yes □ No

Current Time:		Device Clock vs. Real Time:	
Device Clock:			
Date and Time Evidence Will be Overwritten			

Incident Details							
Description of Events and Offenders:							
Camera Number:		Date:		Time Start:		Time End:	
Camera Number:		Date:		Time Start:		Time End:	
Camera Number:		Date:		Time Start:		Time End:	
Camera Number:		Date:		Time Start:		Time End:	
Camera Number:		Date:		Time Start:		Time End:	
Camera Number:		Date:		Time Start:		Time End:	