EXPORTING VIDEO FOR EVIDENCE

ABS Technologies

Not long ago video tape, the original tape was used for play back in a court room. Digital media is different. Today video surveillance is recorded to a fixed digital media. For convenience the video evidence is usually copied from the original source to other media such as DVD, Blu-ray, or even a solid state (flash) drive. In many countries, a proven chain of custody is required. For example, the transfer needs to be documented and witnessed to prove it is an exact copy of the original recording.

Therefore, following are three critical considerations to prove that the evidence to be presented can be deemed admissible in a court of law:

1. How was the video captured?

2. Has the video data been altered?

3. Has the seizure, control, transfer of the video evidence been chronologically documented and witnessed?

To answer questions 1 and 2 above, our IP camera provides two methods for securing and authenticating recorded images. This is extremely important for the end user to understand what each of these things are:

Digital Image Fingerprint

The digital image fingerprint is actually contained within the JPEG file header of images taken from our camera. It contains important information about the camera and the given image sequence.

NOTE: Digital ‘Fingerprinting’ is not the primary system for preventing image tampering as it is unencrypted data, so in itself employs no methods of protection. However it is part of the image sequence data which is protected by the Digital Signing. So when Digital Signing is enabled, using our *state-of-the-art* software, the Digital Image Fingerprint is protected against tampering.

Digital Signing

The primary system that protects the integrity of video recording data is the “Digital Signing” of the data with a video security surveillance camera, a certification process that is commonly used for online banking.

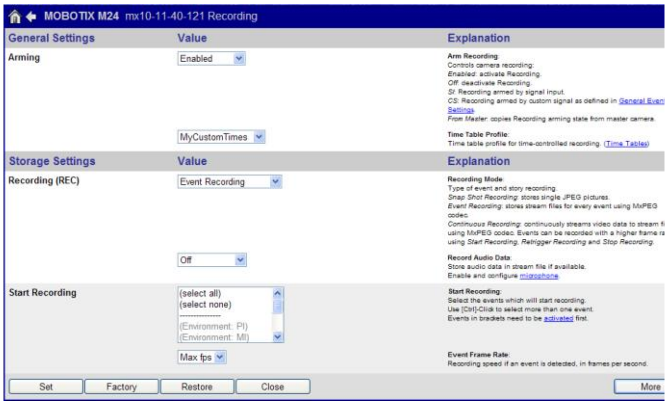
All data recorded by the camera is signed with the camera’s X.509 Certificate using public key cryptography to protect against tampering. This is a highly secure asymmetric method of encryption.

Enabling Digital Signing Using Our Software

By using our sophisticated world-class software, all you need to do is open a web browser and enter the IP address we provide. We make it so easy and convenient and can also guide you through the process over the phone.

Enabling Digital Signing (*continued*)

To enable Digital Signing, using our sophisticated software, access the IP address we provide with your system, Click Setup Menu >> Event Control >>Recording (click More). Now enable Digital Signing by selecting "On", then Set >> Close >> OK.


MOBOTIX M24 mx10-11-40-121 Recording

General Settings	Value	Explanation
Arming	Enabled	**Arm Recording:** Controls camera recording: *Enabled:* activate Recording. *Off:* deactivate Recording. *SI:* Recording armed by signal input. *CS:* Recording armed by custom signal as defined in General Even Settings. *From Master:* copies Recording arming state from master camera.
	MyCustomTimes	**Time Table Profile:** Time table profile for time-controlled recording. (Time Tables)
Storage Settings	**Value**	**Explanation**
Recording (REC)	Event Recording	**Recording Mode:** Type of event and story recording. *Snap Shot Recording:* stores single JPEG pictures. *Event Recording:* stores stream files for every event using MxPEG codec. *Continuous Recording:* continuously streams video data to stream fi using MxPEG codec. Events can be recorded with a higher frame ra using *Start Recording*, *Retrigger Recording* and *Stop Recording*.
	Off	**Record Audio Data:** Store audio data in stream file if available. Enable and configure microphone.
Start Recording	(select all) (select none) --------------- (Environment: PI) (Environment: MI)	**Start Recording:** Select the events which will start recording. Use [Ctrl]-Click to select more than one event. Events in brackets need to be activated first.
	Max fps	**Event Frame Rate:** Recording speed if an event is detected, in frames per second.

The camera will now use a Self-Signed X.509 certificate. The self-signed certificate is one signed with its own private key. A customized X.509 Certificate can be created within the camera's web interface by clicking into the Admin Menu >> Network Setup >>Web Server page. This is available as an option however, the camera's Self-Signed certificate is the fastest option in terms of setup time.

Checking Data Integrity

Our software control center has the ability to verify both the authenticity and data integrity of the Digital Signature. This is really useful to ensure, that the timing of events recorded have not been changed to distort the evidence, by showing the sequence of events out of their original context in order to do this, connect to a camera or recording path, in Playback or Search mode, and click the "Export" button. The pictured dialog will appear (top right). When you export your video for evidentiary purposes, please make sure that you export it from your application software control panel using the following steps:

1. **Set the Time Range**

This will determine the export time range and also allow an integrity check for the data in that time range.

2. **Select File Server Structure**

Please make sure that you select "Export as: File Server Structure", because this will export the video in its exact original format while preserving the data integrity. It also provides the ability to check the digital signature.

3. **Copy Application File**

Checking this option enables the control center to create a folder that includes the recordings and the X.509 certificate (cert.pem). The file exported can also be played back as a playable MxCC file.

4. **Select Digital Structure**

This feature is especially useful for verifying whether or not a copy of an original recording is an exact replication of the original.

5. **Click Check**

This step will perform a data integrity check. If the integrity check fails, the data has either been tampered with or become corrupted.

6. **Export**

Now you are ready to export the recorded sequences as a ready-to-play video player.