



## Video and audio systems

### *Principles*

Never alter the contents of the original data or the digital reference copy you have made.  
Be aware that image processing methods can alter images, and know the filters that are used in this software.  
Document your process.

### *Practices & Procedures*

#### **Stored data**

Know that your information can get lost when digitizing analog audio and video material. The number of lines might be altered, and you might have skipped frames in the video. Furthermore the quality of the audio and video might degrade when digitising.

Check the status of the media, and depending on the condition of the media,

Identify the format of the audio and video evidence (eg. Compression standard, file formats, NTSC, PAL, SECAM).

If you are working with equipment with volatile memories, have a regime for systematic replacing of batteries.

Be aware of tape material that could be installed back to front for the purpose of deception.

Make a digital copy of the part for investigation and compute a hash code (if possible)

Use validated software, when available or software with which you know what happens, also for conversions of file formats.

The forensic examiner should be able to explain to court what kind of image and sound-processing method has been used.

Presentation of the evidence.

- Video prints

- Transcripts

- Digital Media (eg. CD-ROMs, DVDs)

Be aware that distribution of certain kinds of images (child pornography) is illegal in some countries, also in forensic reports.

#### **Real time data collection**

Ensure that you have filed the right data that is intercepted.

You should keep track of the sender and receiver data (eg the telephone number it was received from).

Follow your laws.

Store the adequate data that is allowed by law and some sort of system for authenticating (eg timestamps and hashes).