

LET'S GET LEGAL!!!

*R*OCKY *M*OUNTAIN *D*IVISION
OF THE
*I*NTERNATIONAL *A*SSOCIATION FOR *I*DENTIFICATION

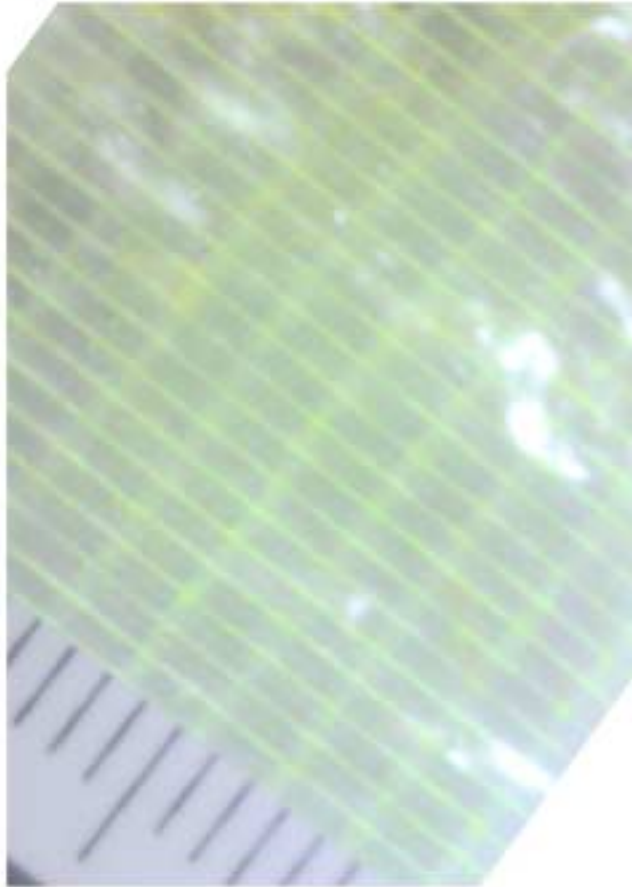
Breckenridge, Colorado
September 18 - 20, 2002

David "Ski" Witzke
Vice President, Sales & Marketing
PC Pros *MORE HITS*®

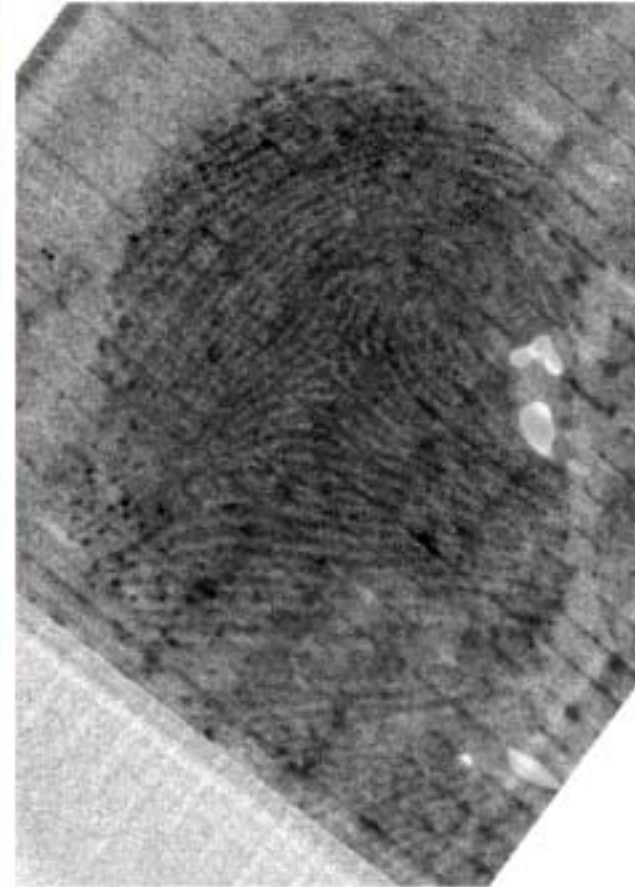


Making the invisible visible!

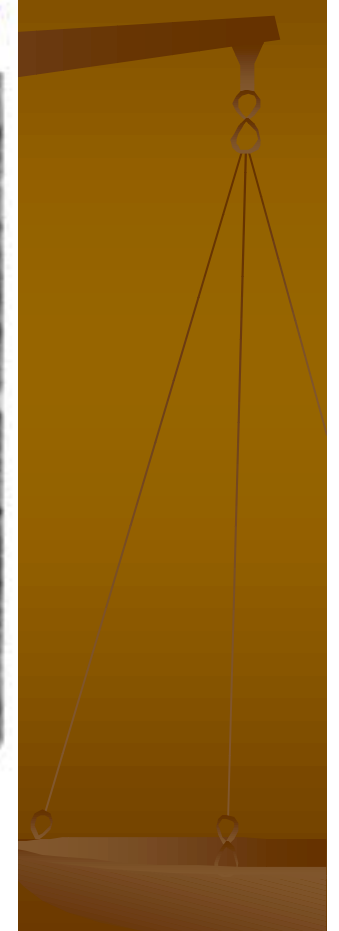
**LATENT PRINT ON DUCT TAPE
PROCESSED WITH BASIC YELLOW**



BEFORE

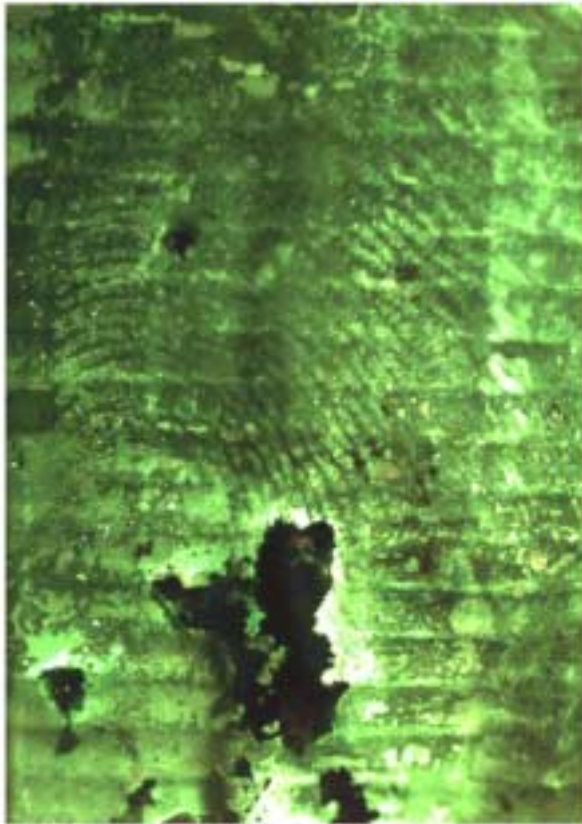


AFTER



Making the invisible visible!

LATENT PRINT ON DUCT TAPE PROCESSED WITH BASIC YELLOW



BEFORE



AFTER

Making the invisible visible!

**LATENT PRINT ON NEWSPRINT
PROCESSED WITH NINHYDRIN**



BEFORE



AFTER

Making the invisible visible!

**LATENT PRINT ON SODA CAN
PROCESSED WITH RHODAMINE**



BEFORE



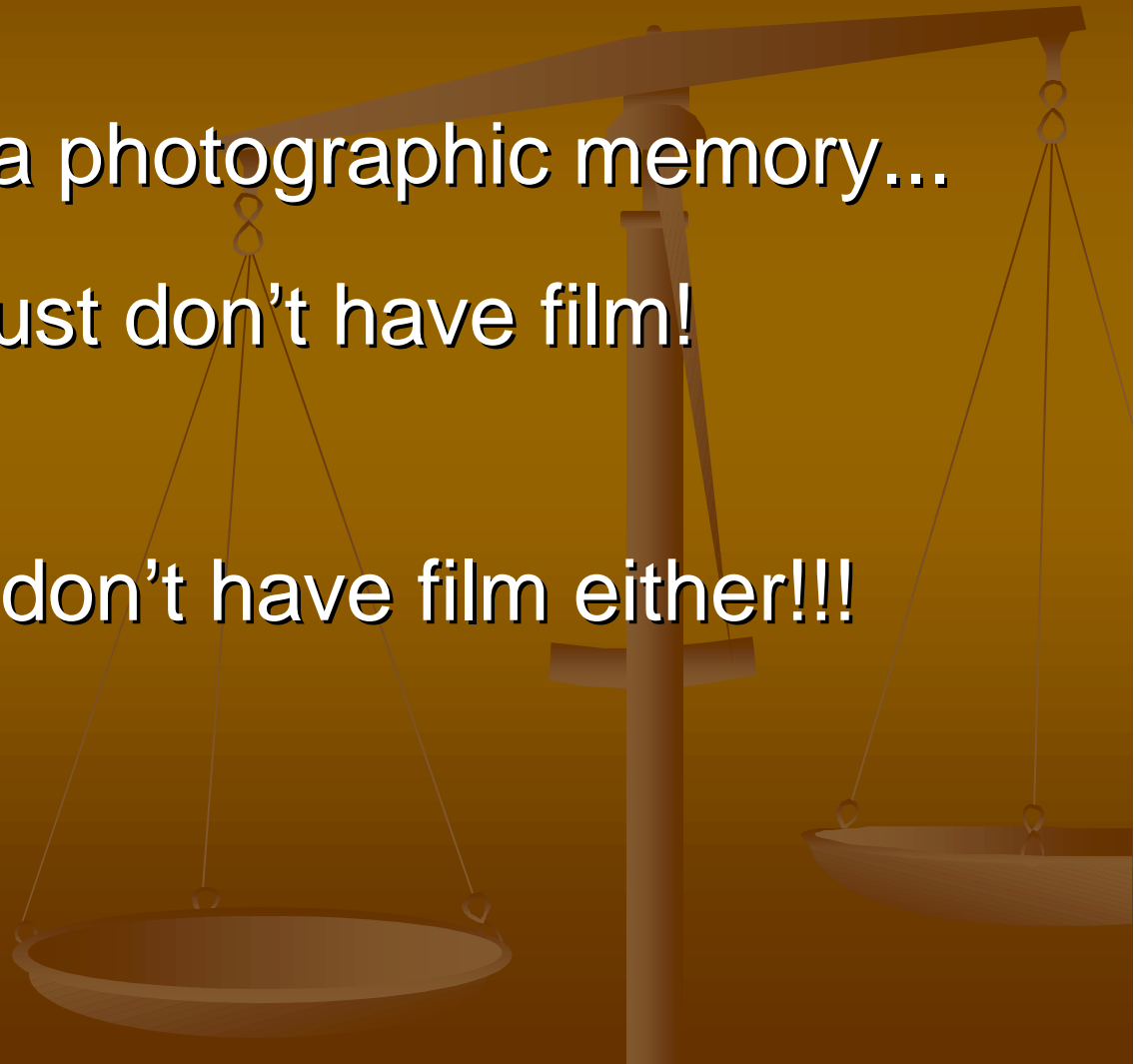
AFTER

A thought to ponder ...

Everyone has a photographic memory...

Some people just don't have film!

Digital images don't have film either!!!



So what do
YOU
do for
image security?



Image storage and management

- Store both images
 - Original image
 - Proprietary file format
 - Data encryption
 - Enhanced image
 - Image
 - Processing data



Image storage and management

- Manual processes
 - Naming conventions
 - Directory
 - Subdirectory
 - File name
- Automated processes
 - Image tracking systems



Image processing guidelines

- Develop guidelines for digital image capture, storage and transmission of digital images retained as evidence
 - Image format
 - Image size
 - Physical dimensions
 - Resolution
- Establish procedures to preserve image integrity



Image processing guidelines

- Develop guidelines for digital image capture, storage and transmission of digital images retained as evidence
- Establish procedures to preserve image integrity
 - Image identity
 - Image authenticity
 - Image security
 - Image privacy



Image processing guidelines

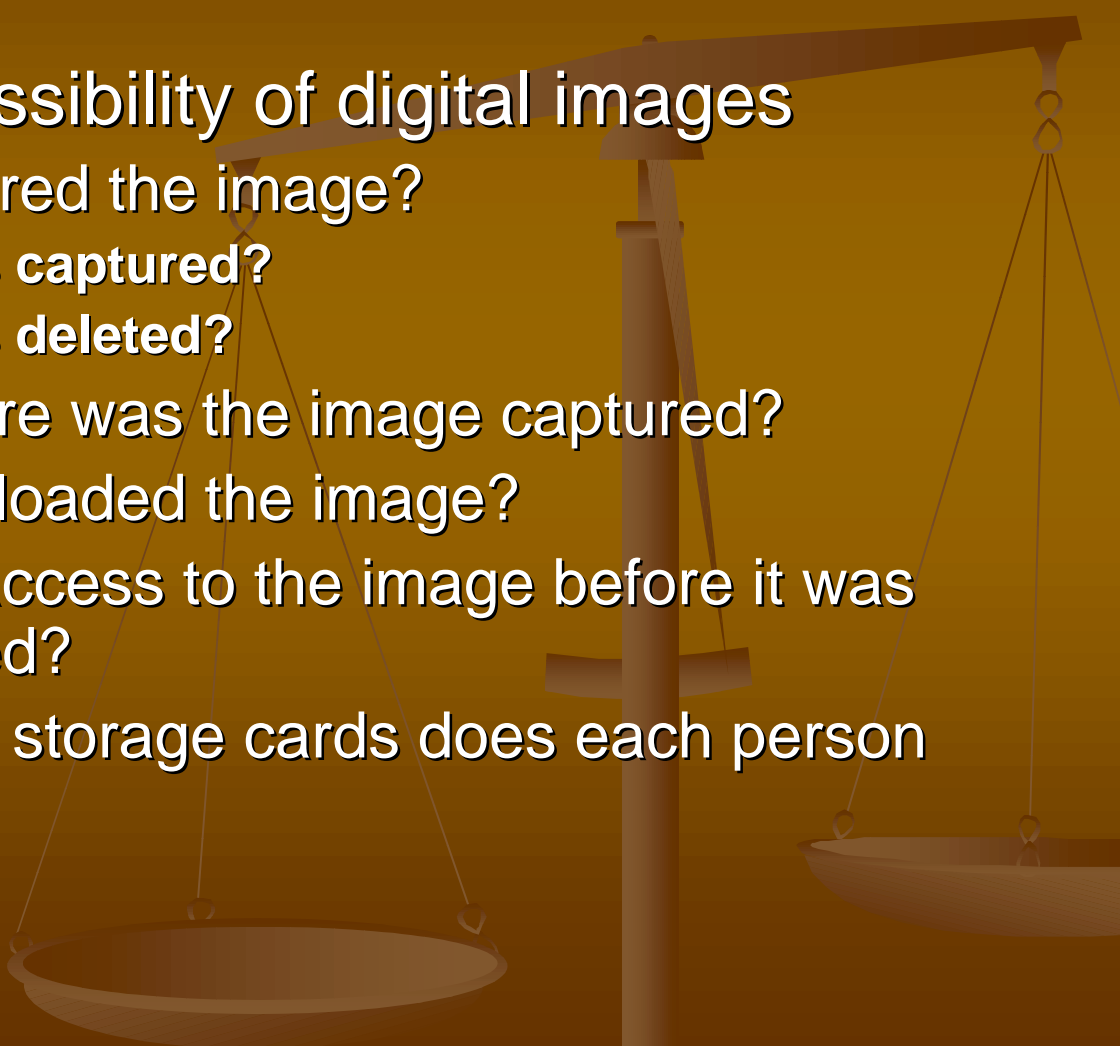
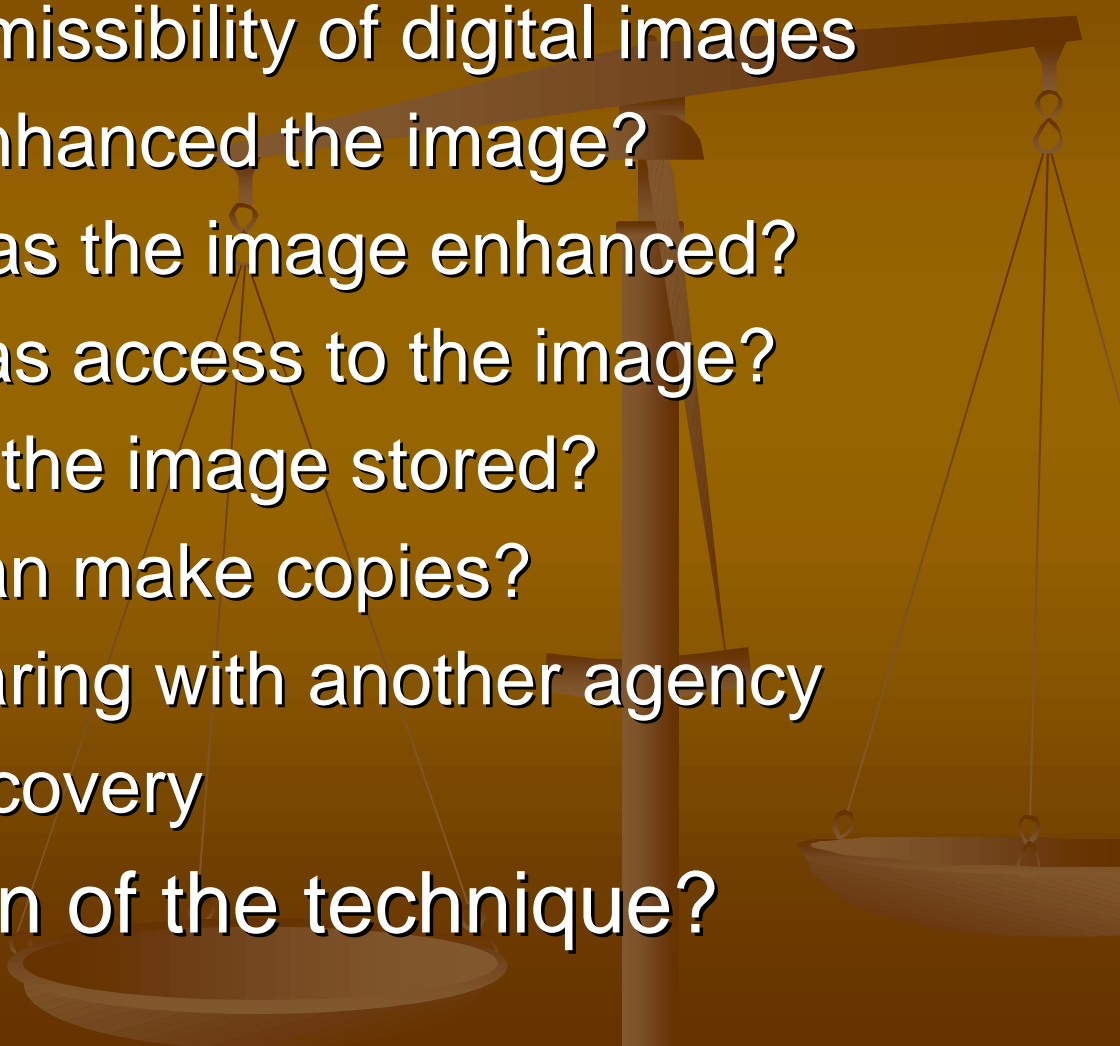
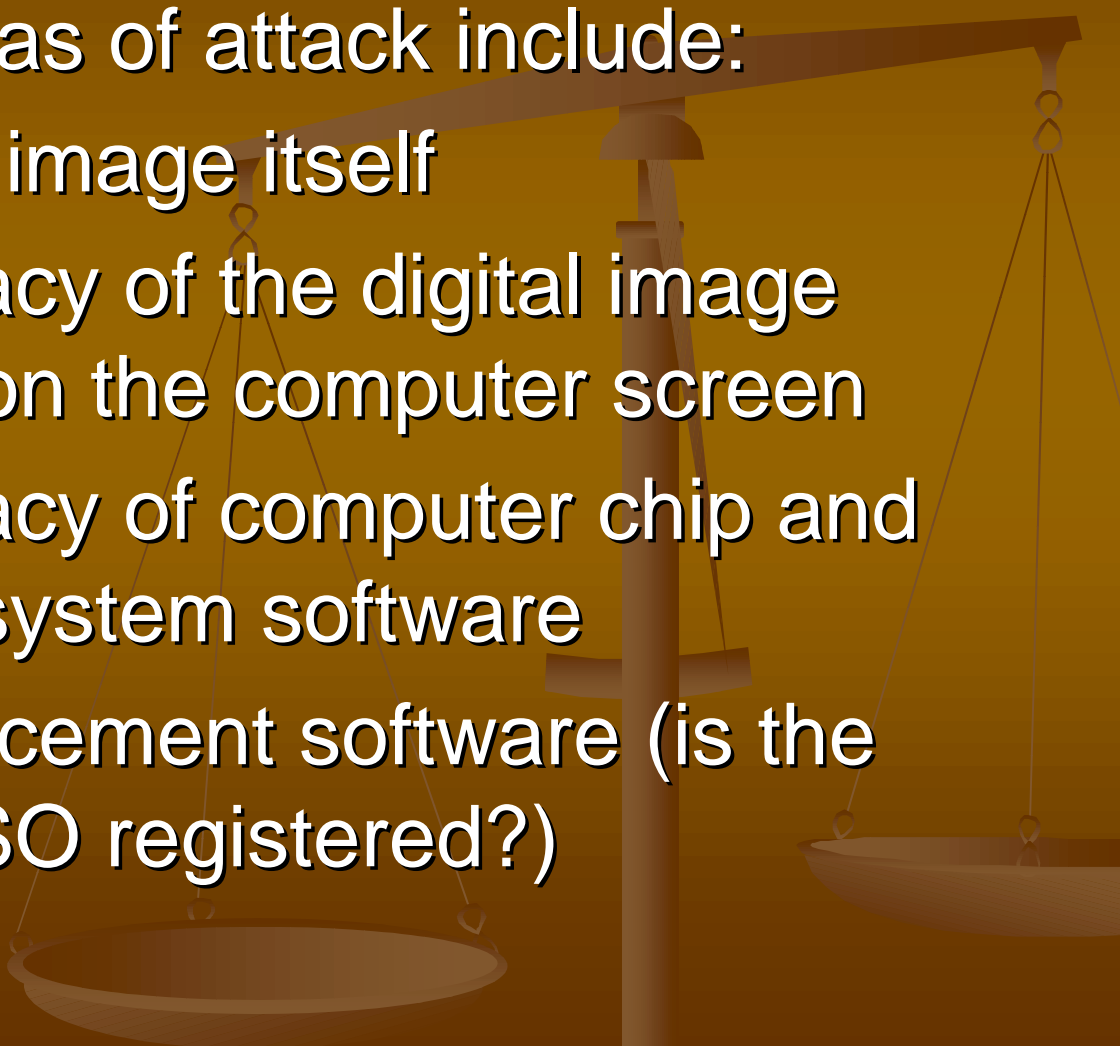
- Ensure admissibility of digital images
 - Who captured the image?
 - What is captured?
 - What is deleted?
 - When/where was the image captured?
 - Who downloaded the image?
 - Who had access to the image before it was downloaded?
 - How many storage cards does each person have?
- 

Image processing guidelines

- Ensure admissibility of digital images
 - Who enhanced the image?
 - How was the image enhanced?
 - Who has access to the image?
 - How is the image stored?
 - Who can make copies?
 - Sharing with another agency
 - Discovery
 - application of the technique?
- 

Admissibility of digital evidence

Potential areas of attack include:

- The digital image itself
 - The accuracy of the digital image displayed on the computer screen
 - The accuracy of computer chip and operating system software
 - The enhancement software (is the software ISO registered?)
- 

Admissibility of digital evidence

Potential areas of attack include:

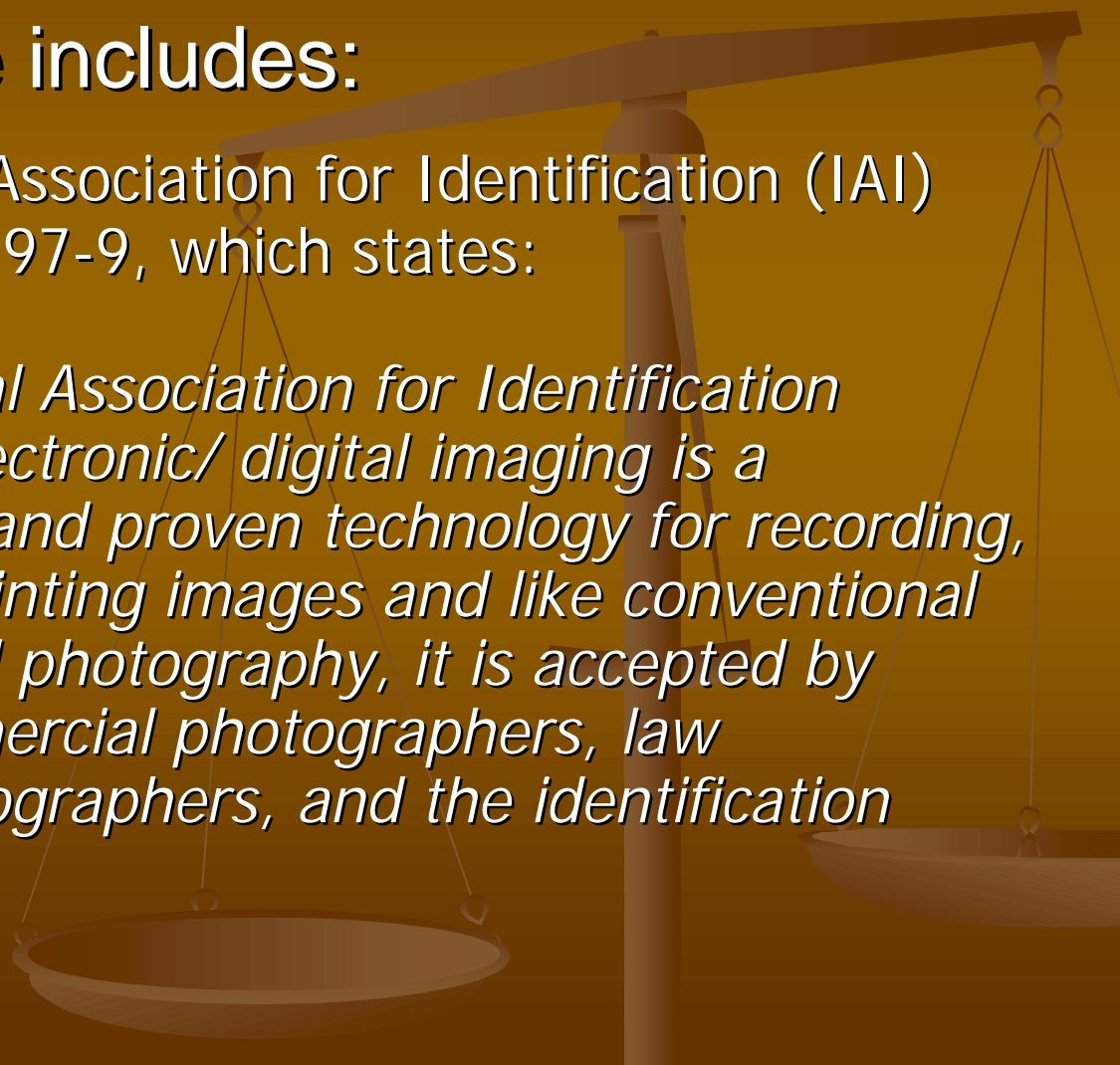
- The accuracy of specialized software that is used to enhance the image on the screen
- The ability to accurately account for multiple enhancements
- The quality of the output (does it accurately represent the enhanced image?)

Admissibility of digital evidence

Potential defense includes:

The International Association for Identification (IAI) passed Resolution 97-9, which states:

... the International Association for Identification recognizes that electronic/ digital imaging is a scientifically valid and proven technology for recording, enhancing, and printing images and like conventional silver-halide based photography, it is accepted by professional commercial photographers, law enforcement photographers, and the identification community.



Admissibility of digital evidence

Potential defense includes:

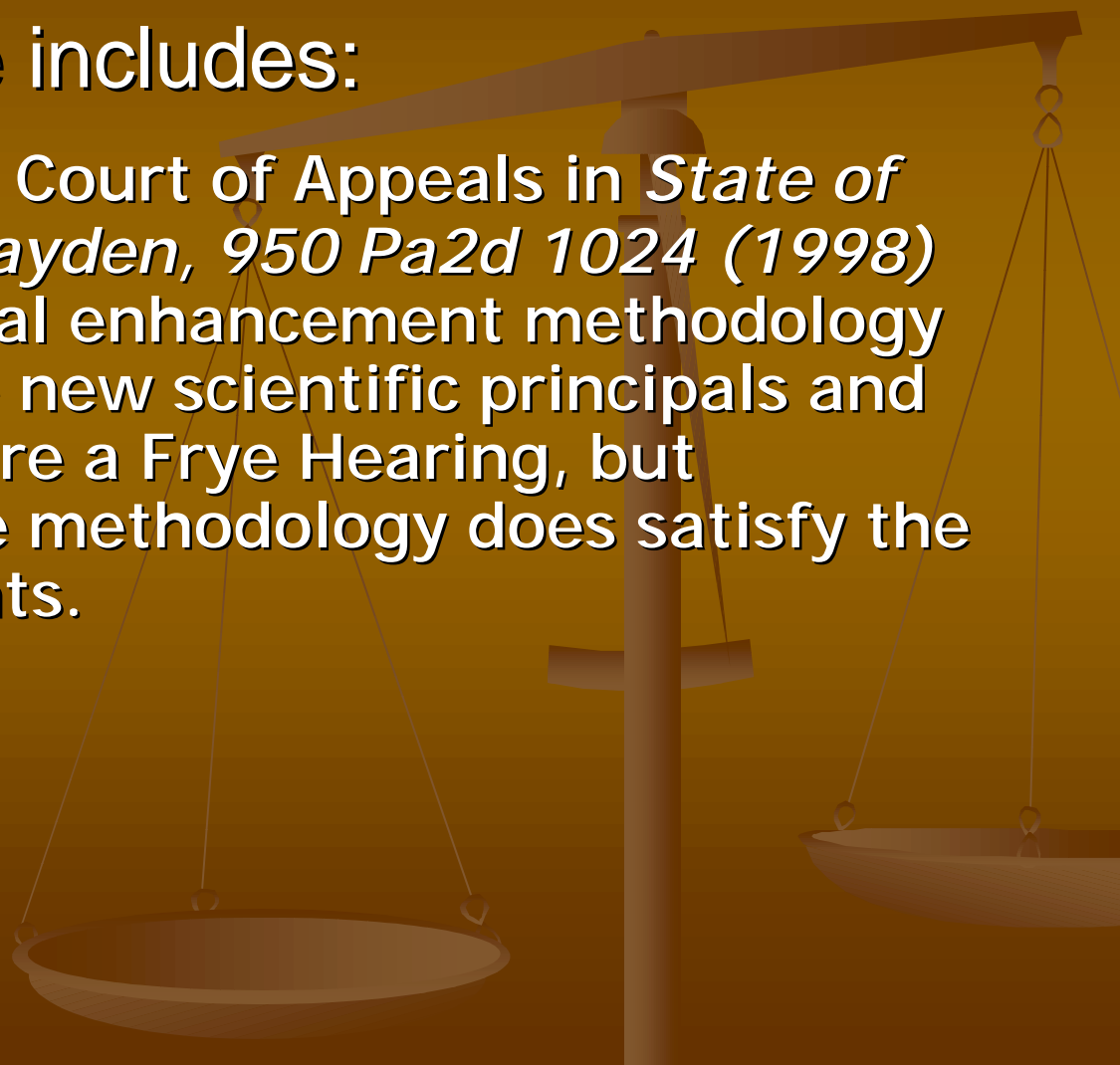
You follow Standard Operating Procedures for digital image processing, which states that:

...all enhancements shall be performed on exact copies of the original image, and that at no time during the enhancement process will any area of an image be deleted or altered in any way. All enhancement processes shall be accomplished by adjusting the values of each pixel that make up the total image. Each of these processes shall then be recorded for purposes of authenticating the image enhancement process.

Admissibility of digital evidence

Potential defense includes:

The Washington Court of Appeals in *State of Washington v Hayden, 950 Pa2d 1024 (1998)* stated that digital enhancement methodology does not involve new scientific principals and should not require a Frye Hearing, but nevertheless the methodology does satisfy the Frye requirements.



Admissibility of digital evidence

Potential defense includes:

Three other decisions that support this position were decided in State of Florida:

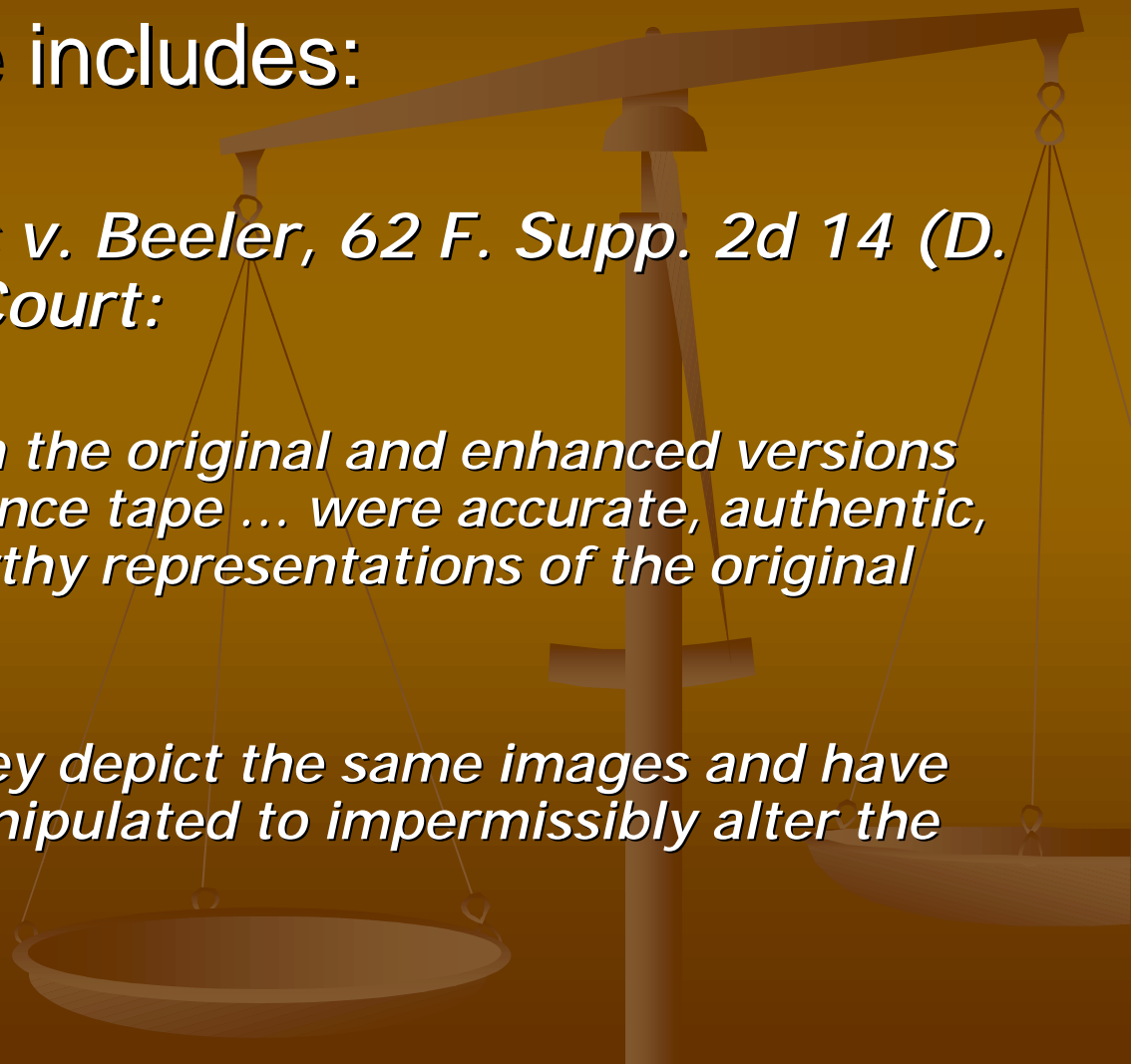
- (1) State of Florida versus Veleka Bryant, a First District case cited at 810 So.2d 532 (Fla. 1st DCA 2002)*
- (2) the State of Florida versus Roger Dolan, a Fourth District case cited at 743 So.2d 544, 546 (Fla. 4th DCA 1999)*
- (3) the State of Florida versus Lucious Boyd, Case No. 99-5809CF10A, Broward County, Florida, Circuit Court.*

Admissibility of digital evidence

Potential defense includes:

In United States v. Beeler, 62 F. Supp. 2d 14 (D. Me. 1999), the Court:

- *“viewed both the original and enhanced versions of a surveillance tape ... were accurate, authentic, and trustworthy representations of the original tape.”*
- *And “that they depict the same images and have not been manipulated to impermissibly alter the images.”*

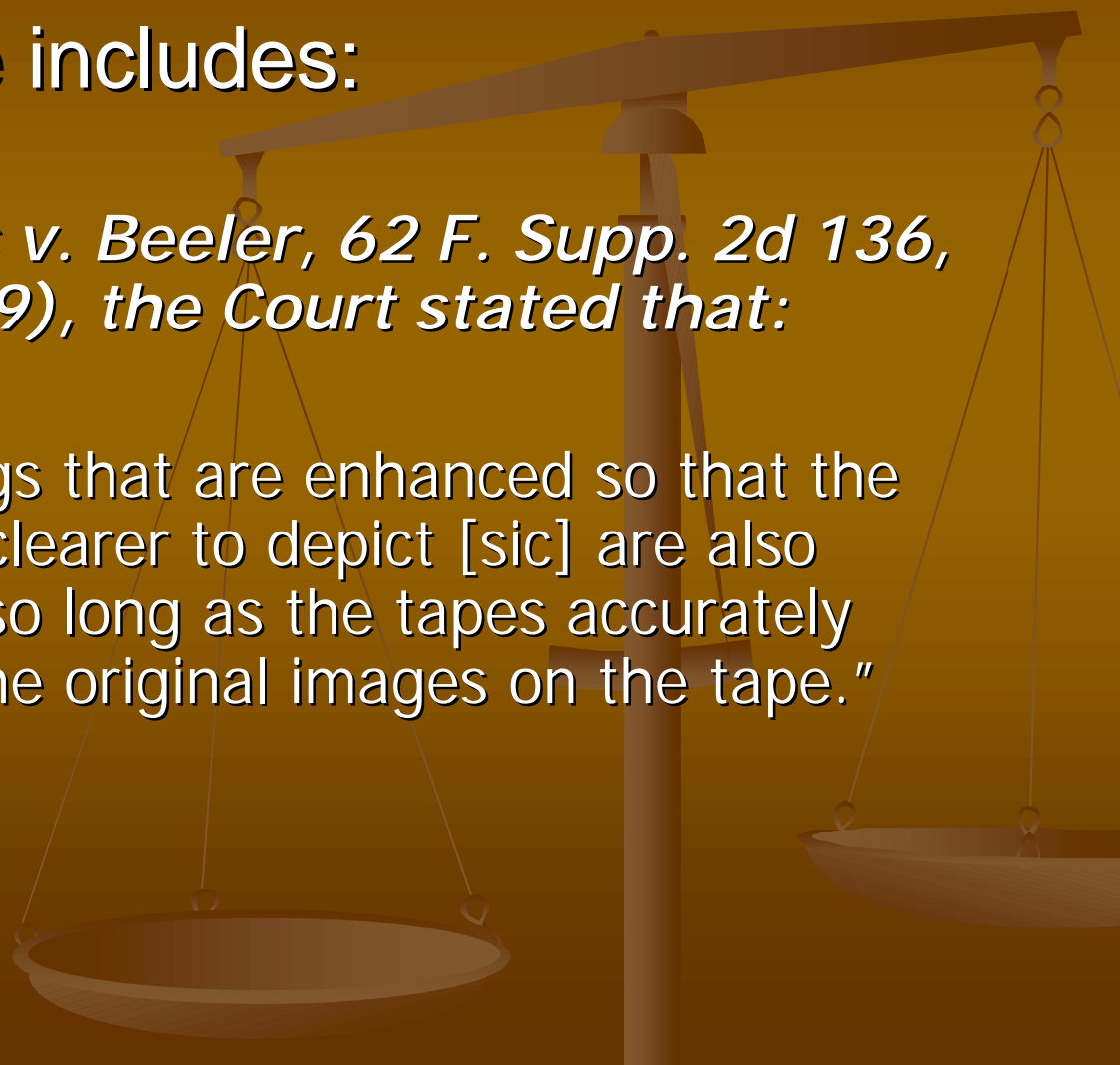


Admissibility of digital evidence

Potential defense includes:

In United States v. Beeler, 62 F. Supp. 2d 136, 148 (D. Me. 1999), the Court stated that:

- “Rerecordings that are enhanced so that the images are clearer to depict [sic] are also ‘duplicates’ so long as the tapes accurately reproduce the original images on the tape.”



Admissibility of digital evidence

Potential defense includes:

The Texas Rule of Evidence 1001 is typical of how most States have chosen to adopt Rule 1001 from the Federal Rules of Evidence :

An original of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. An original of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an original.

Admissibility of digital evidence

Potential defense includes:

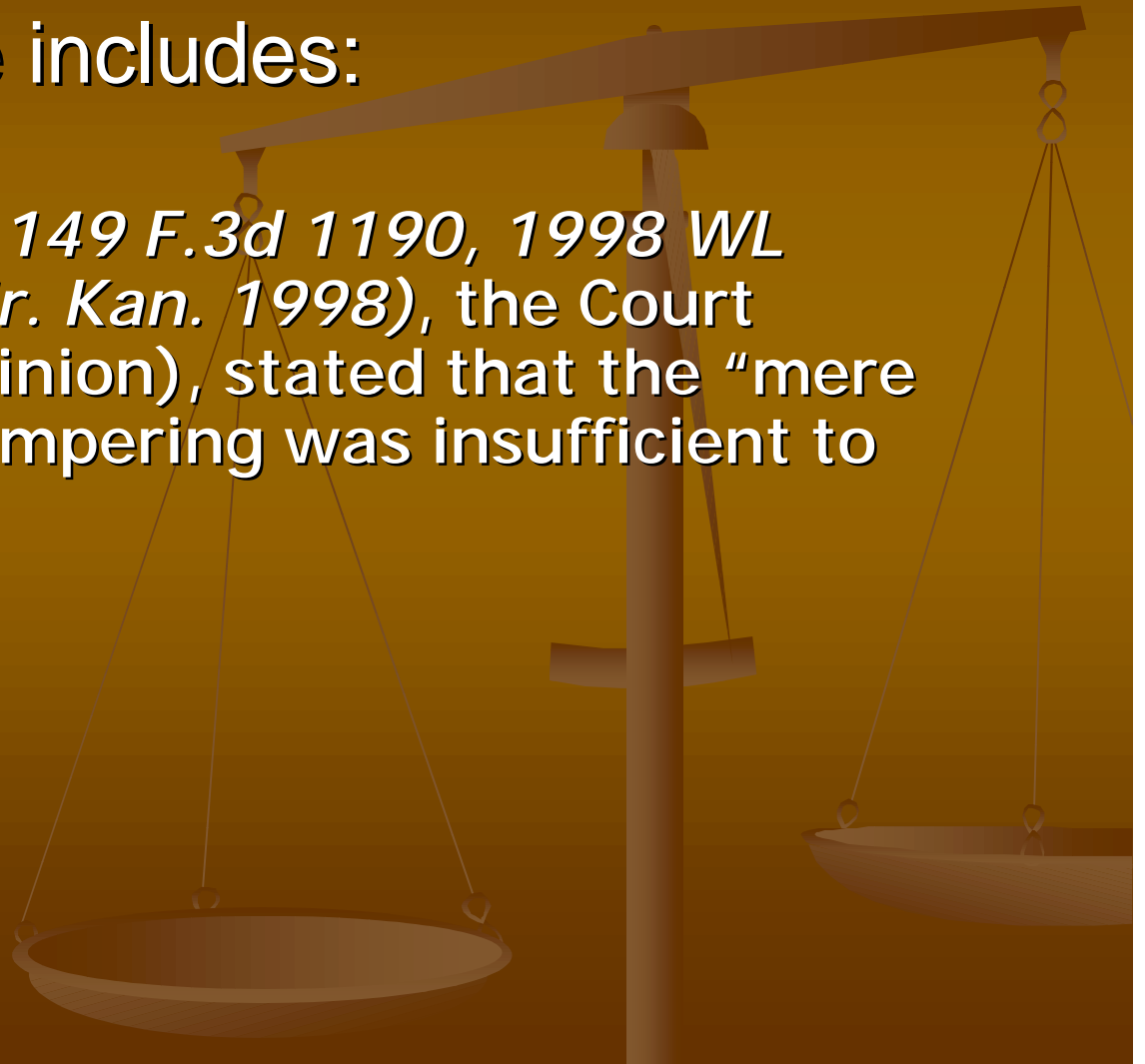
Texas Rule of Evidence 1001, Section 1550.6, added in August of 1996, defines originality of video and digital images by stating:

Images stored on video or digital media, or copies of images stored on video or digital media, shall not be rendered inadmissible by the best evidence rule. Printed representations of images stored on video or digital media shall be presumed accurate representations of the images they purport to represent.

Admissibility of digital evidence

Potential defense includes:

In *Cross v. U.S.*, 149 F.3d 1190, 1998 WL 255054 (10th Cir. Kan. 1998), the Court (unpublished opinion), stated that the “mere possibility” of tampering was insufficient to prove bad faith.



Admissibility of digital evidence

Forensic Digital Imaging and Photography,
by Herbert L. Blitzer and Jack Jacobia, page 201:

Anyone who has seen a movie made in the past five years is well aware that it is possible to do almost anything you want to do with digital images—change which items are in the picture, change their coloration or texture, move things around, etc.; thus it is generally believed that the digital images are easily manipulated. At the same time, there is a belief that film images are much less susceptible to manipulation. The facts of the matter are that the first statement is true and the second is, to a large degree, false.