Digital Forensics

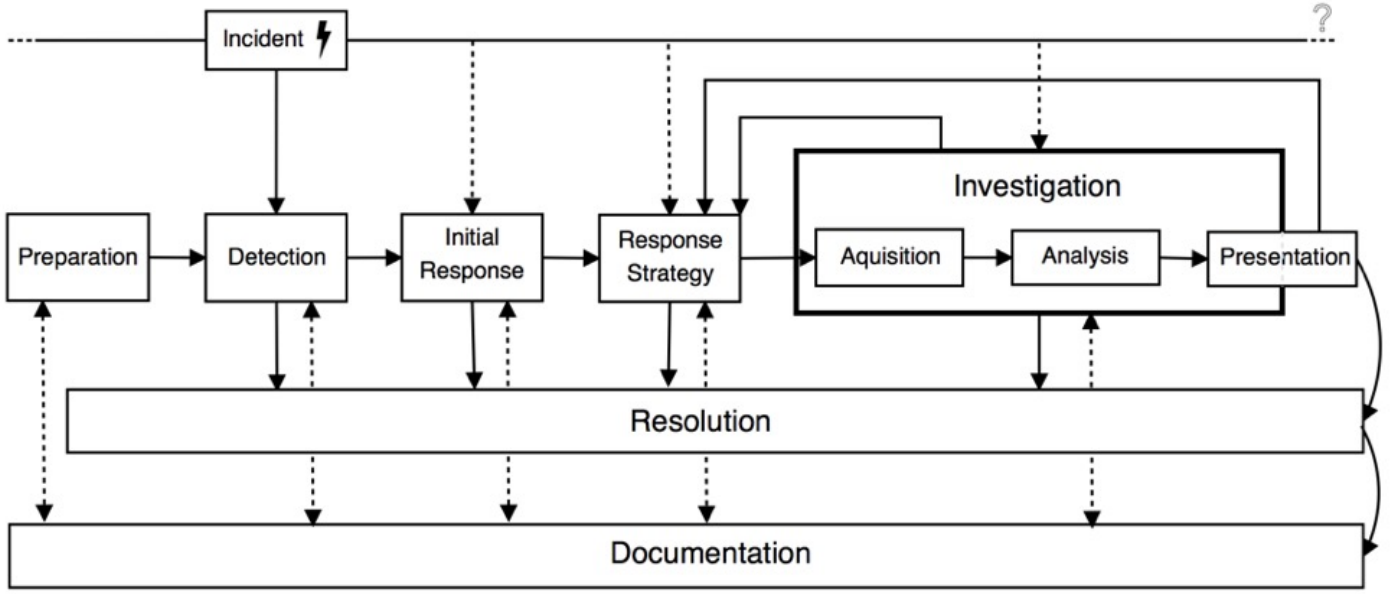
Rosario Giustolisi

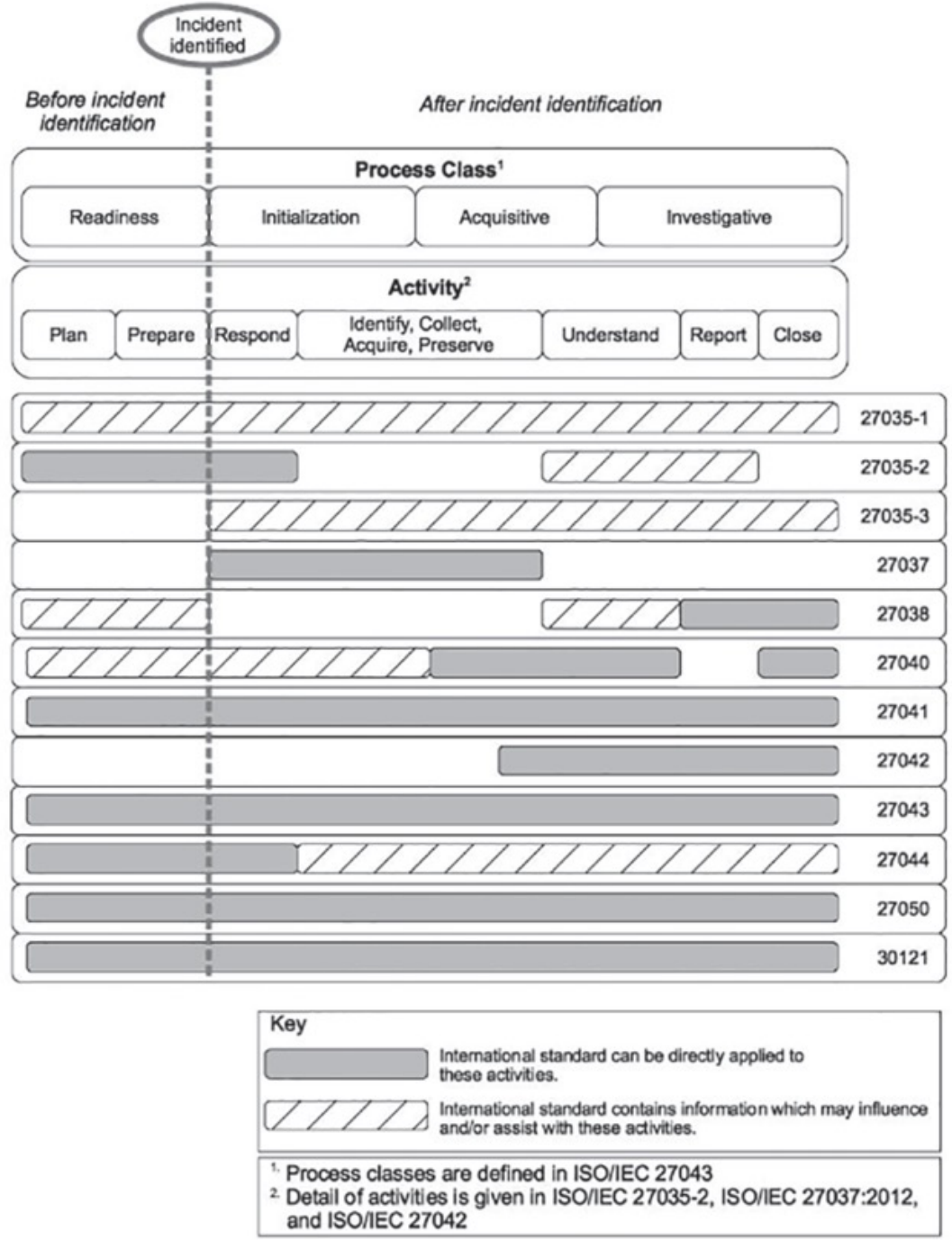
Plan

- Incident Response
- Computer Forensics
- Disk Forensics
- Image/Video Forensics

Incident Response

- Security Incident: illegal or unauthorized action which might involve a computer system or network
- Incident Response: **process** to address and manage security incidents

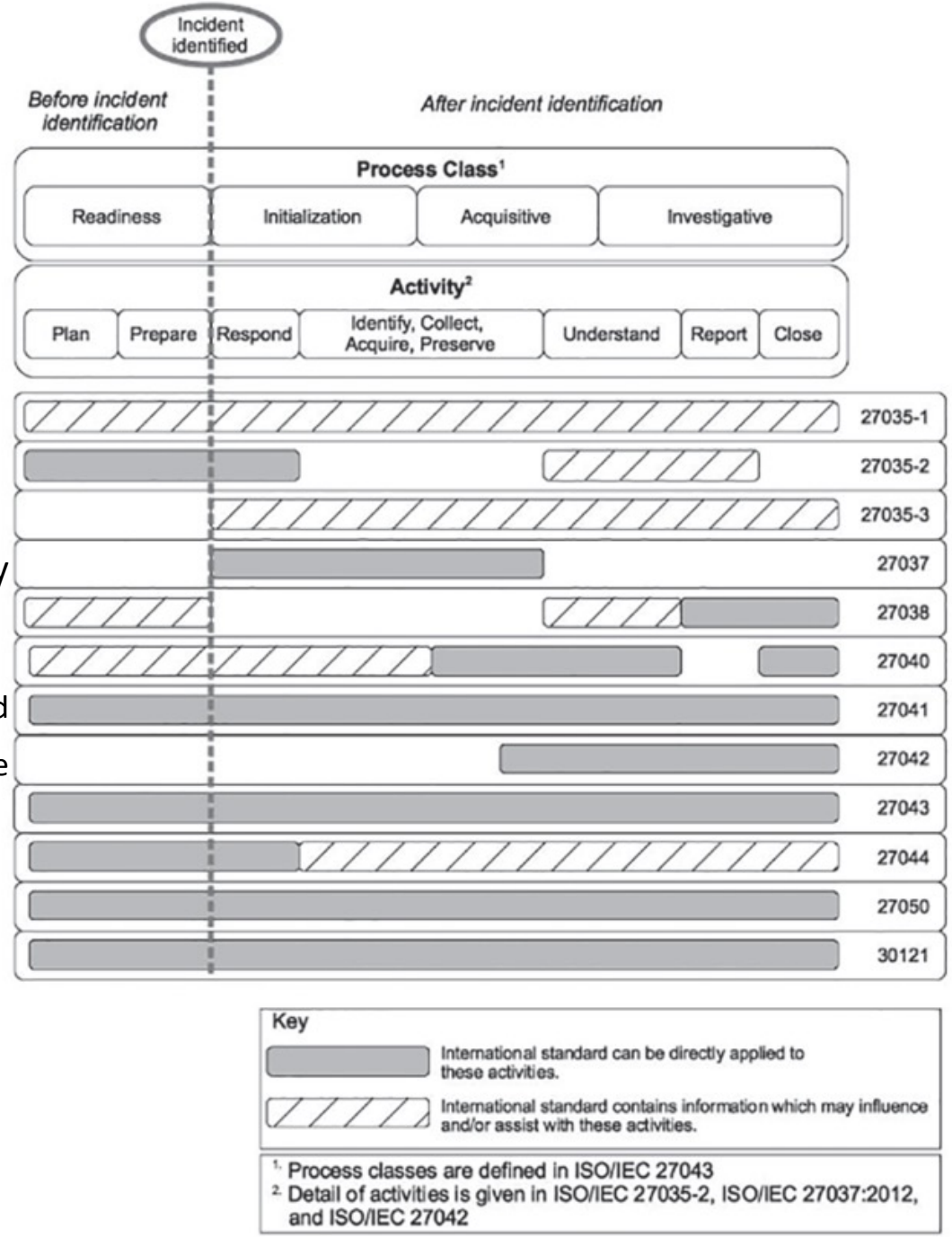



Incident identified
Before incident identification
After incident identification
Process Class[1]
Readiness
Initialization
Acquisitive
Investigative
Activity[2]
Plan
Prepare
Respond
Identify, Collect, Acquire, Preserve
Understand
Report
Close
27035-1
27035-2
27035-3
27037
27038
27040
27041
27042
27043
27044
27050
30121
Key
International standard can be directly applied to these activities.
International standard contains information which may influence and/or assist with these activities.
1. Process classes are defined in ISO/IEC 27043
2. Detail of activities is given in ISO/IEC 27035-2, ISO/IEC 27037:2012, and ISO/IEC 27042

chain of custody

Evaluation of incident investigative method

Analysis and interpratation of digital evidence



Incident Response

- CERT (Computer Emergency Response Team) established in 1988 in response to the *Morris worm*.

- DKCERT established in 1991 after someone tried to access computers at NASA from Roskilde University.

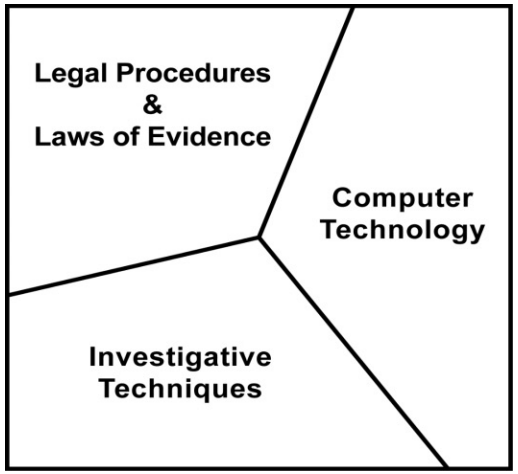
  - Jørgen Bo Madsen, *The greatest cracker-case in Denmark: The detecting, tracing and arresting of two international crackers*

Terminology

- Computer Forensics: process with the goal of investigating digital media, often in relation to criminal events.
- Focus: sound and correct reconstruction of a security incident
- Goal: use the acquired data for law enforcement

Terminology

- Computer Forensics: **process** with the goal of investigating digital media, often in relation to criminal events.
- Focus: sound and correct reconstruction of a security incident
- Goal: use the acquired data for law enforcement



Computer Forensics

Computer Forensics vs Risk Assessment vs Information Gathering

Computer Forensics

Computer Forensics vs Risk Assessment vs Information Gathering

Enforce law vs Identify threats vs Find vulnerabilities

Similar techniques, different goals.

Process

1. Acquisition of data
   - Identification
   - Collection
   - Preservation
2. Analysis of artifacts
   - Interpretation
   - Validation
3. Presentation of evidence
   - Documentation

Artifact: Object of **potential** computer forensics interest

Remember: Must be forensically sound!

Acquisition

- Identify objects useful for the investigation
  - *E.g. IT systems, network systems, external drives, post-it, paper documents, …*

Obtain as much as possible relevant pieces of data

- Collect data from the identified objects
  - Live data collection *e.g. dump RAM, network connections, …*
  - Forensics duplication *e.g. bit-by-bit images, hash-verified copies, …*

Avoid downtime

- Preserve the object to be investigated
  - *e.g. restrict logical and physical access to the object, enforce chain of custody*

Make the procedure repeteable

Chain of Custody

- Handling of artifacts must follow the 3 C's of artifacts: care, control, and chain of custody

- Chain of custody procedures
  - Keep an artifacts **log** that shows when an artifact was received and seized, and where it is located
  - **Record** dates
  - **Restrict** access to artifacts
  - Place original objects in an evidence **locker**
  - Perform all forensics on a **mirror-image** copy, never on the original data

Presentation

- Document
  - **What** was done
  - **How** it was done
  - What data emerged
  - What is the **meaning** of resulting data

- Adapt the document to the recipient (technical-jurist)

Computer Forensics

- Computer forensics includes
  - Disk forensics
  - Image forensics
  - Video forensics
  - Network forensics
  - Mobile device forensics
  - Database forensics
  - Social network forensics
  - …

Disk Forensics

Source: DTI Data Recovery

Urban Legends

Data recovery impossible

Source: DTI Data Recovery

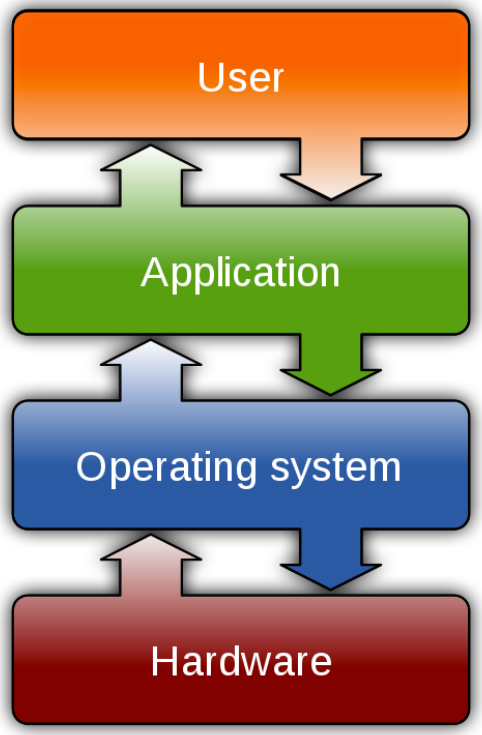
Urban Legends

Data recovery possible

Source: DTI Data Recovery

Disk Forensics

Why?



Disk

Volume

Metadata

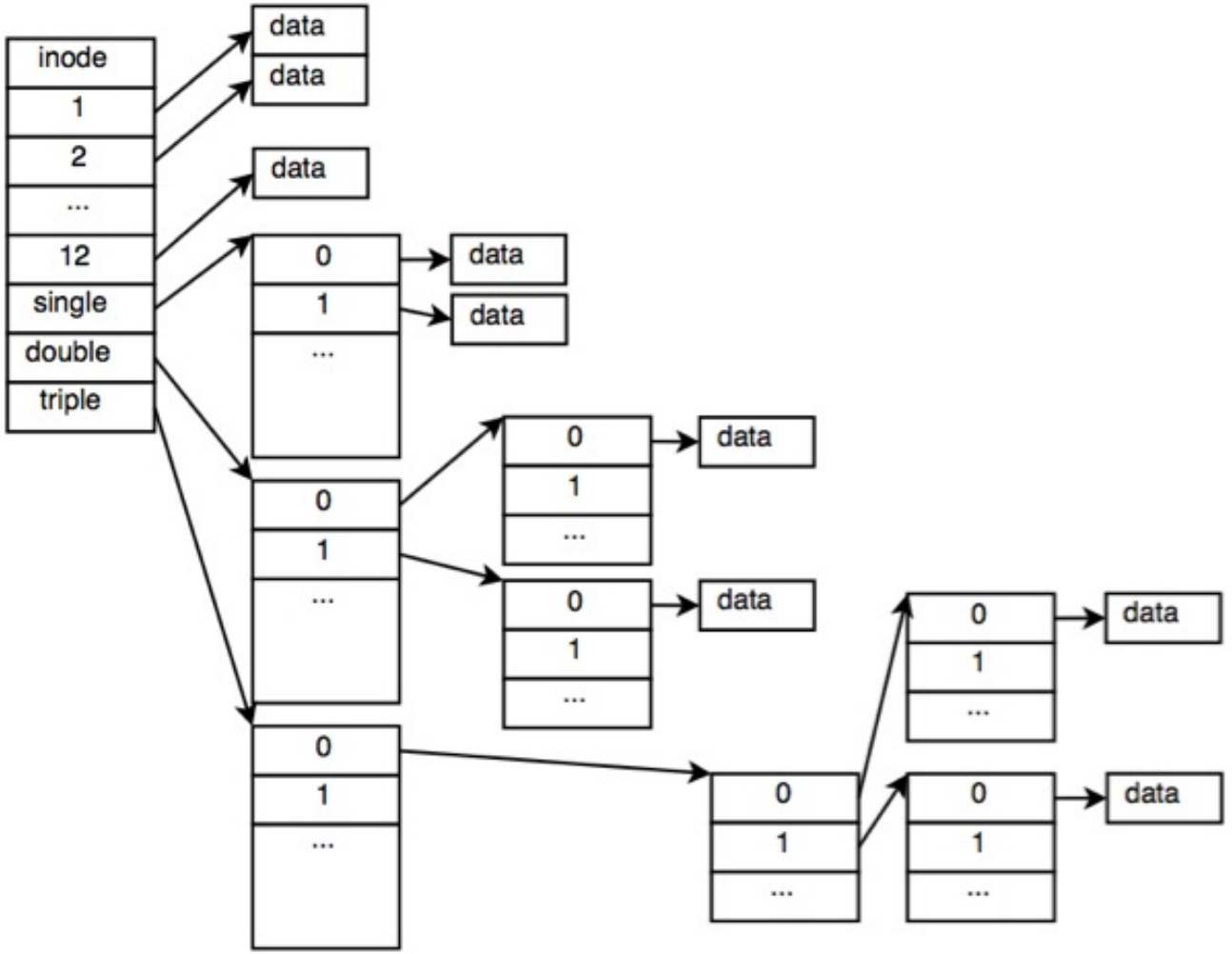
File system

Block

Linux file systems: Ext2 / Ext3 / Ext4

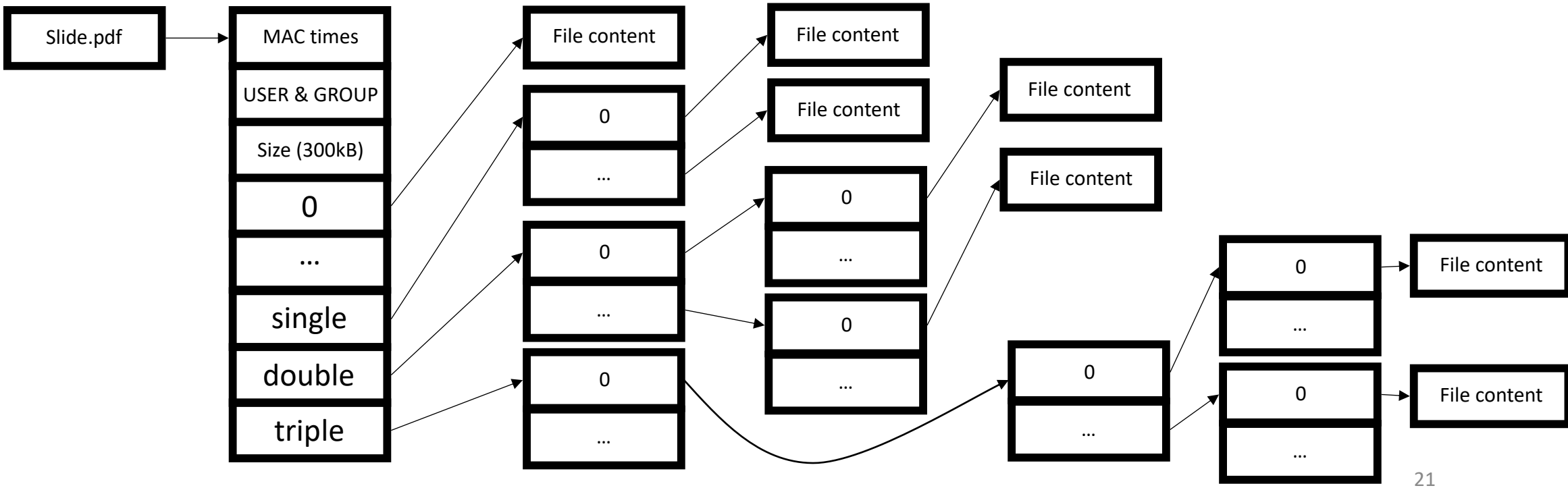
Inode

- Inodes store four time stamps
  1. **M**odified
  2. **A**ccessed
  3. **C**hanged
  4. Deleted



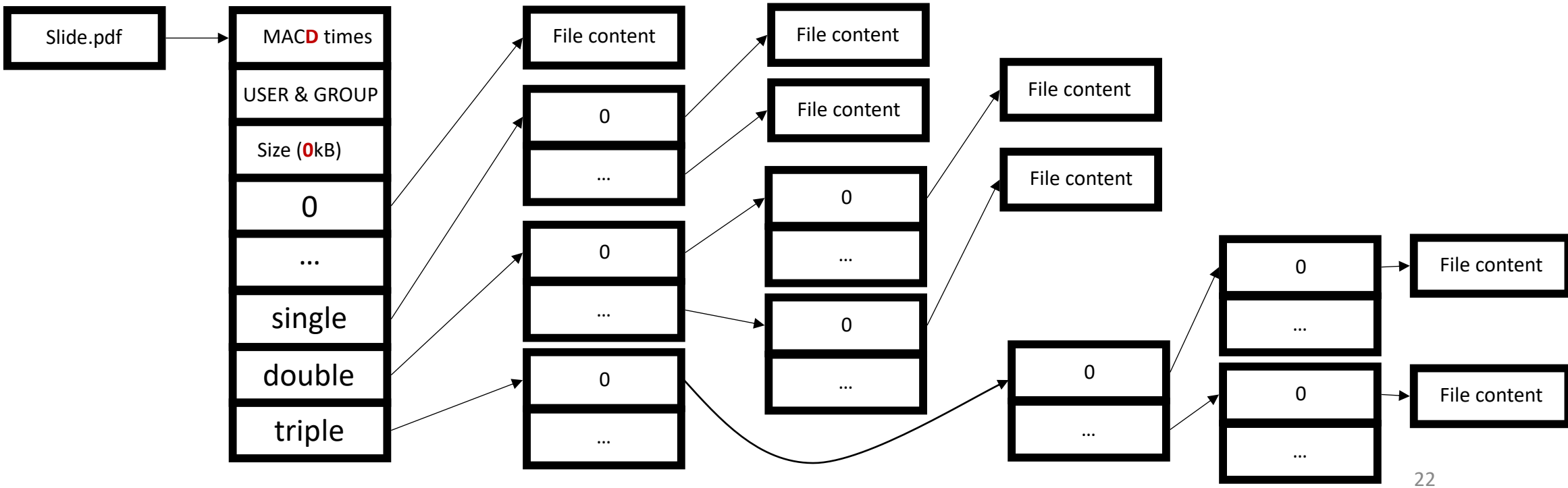
Deleting Data

- Deleting a block or inode *freezes* that item until it is reused



Deleting Data

- Deleting a block or inode *freezes* that item until it is reused
  - **Ext2**: Block pointers are not zeroed



Deleting Data

- Deleting a block or inode *freezes* that item until it is reused
  - **Ext3/4**: Block pointers are zeroed but content on block is still present
  - *Journaling* and *carving* can help reconstructing the file

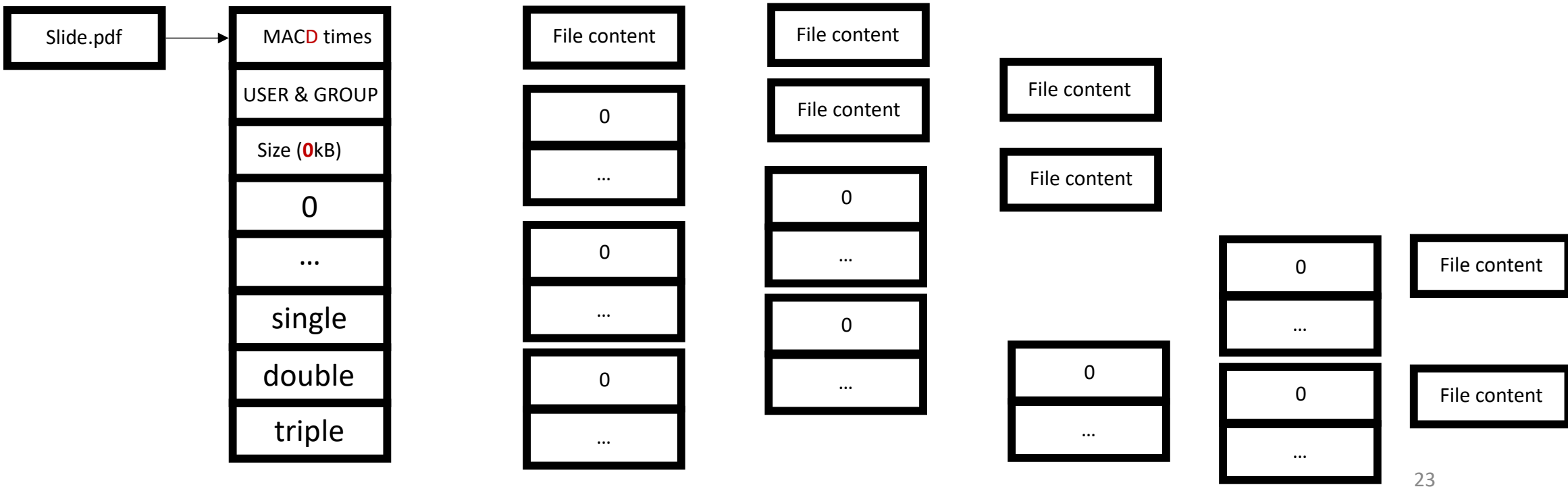


Image and Video Forensics

Urban Legends

Data recovery impossible

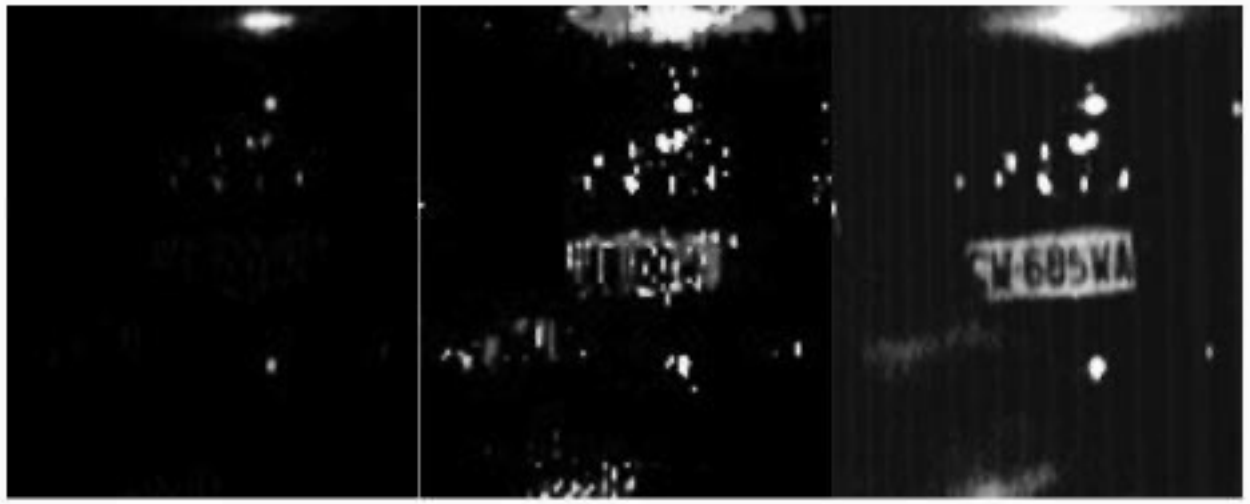
- Cannot: create new pieces of information
- Can: emphasise and extract hidden information

Urban Legends

Data recovery possible

Urban Legends

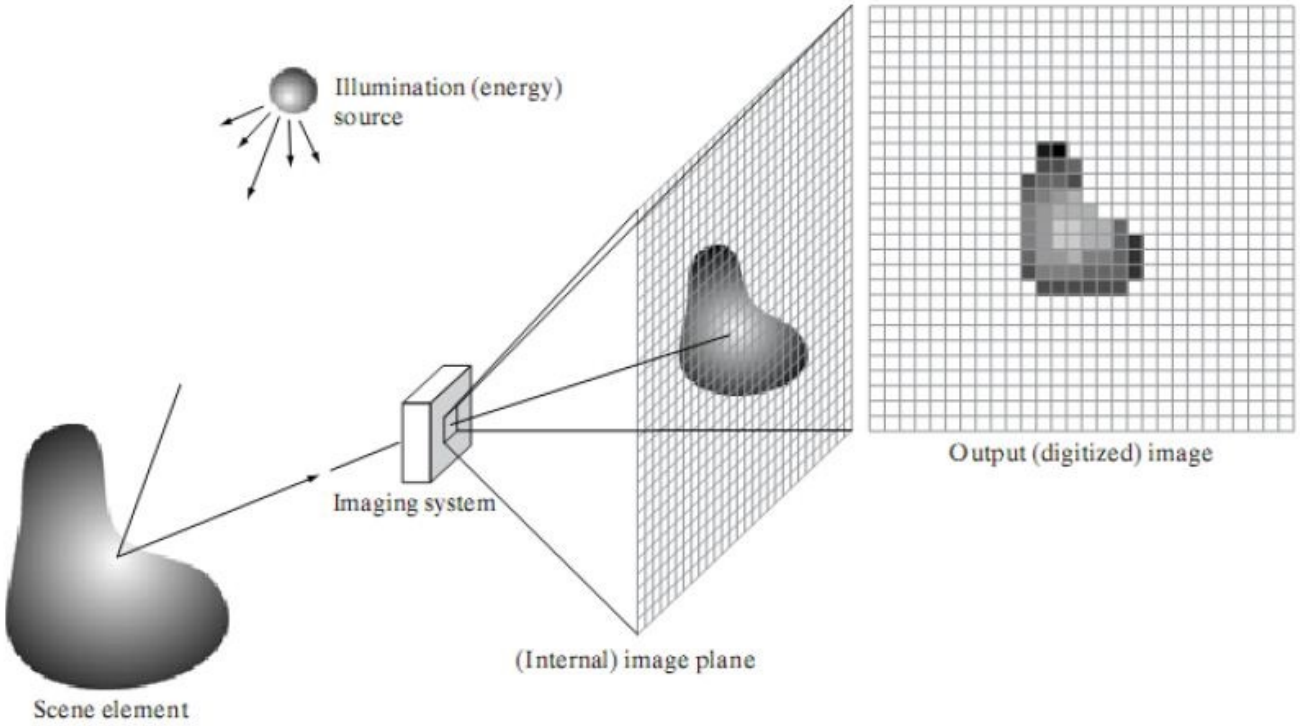
Data recovery possible



Contrast enhancement + Stabilization + Frame Averaging

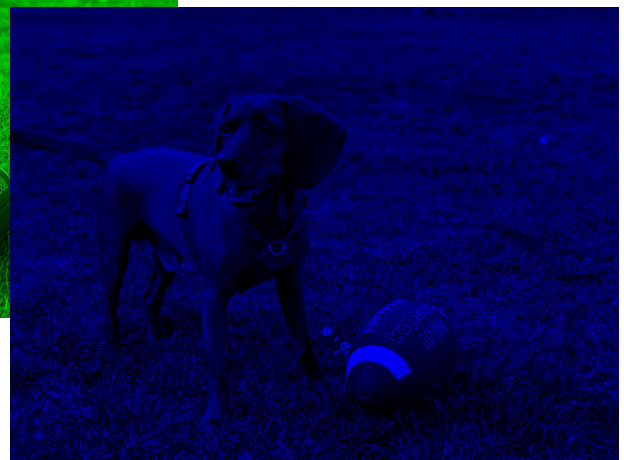
Motion deblurring

Image Acquisition



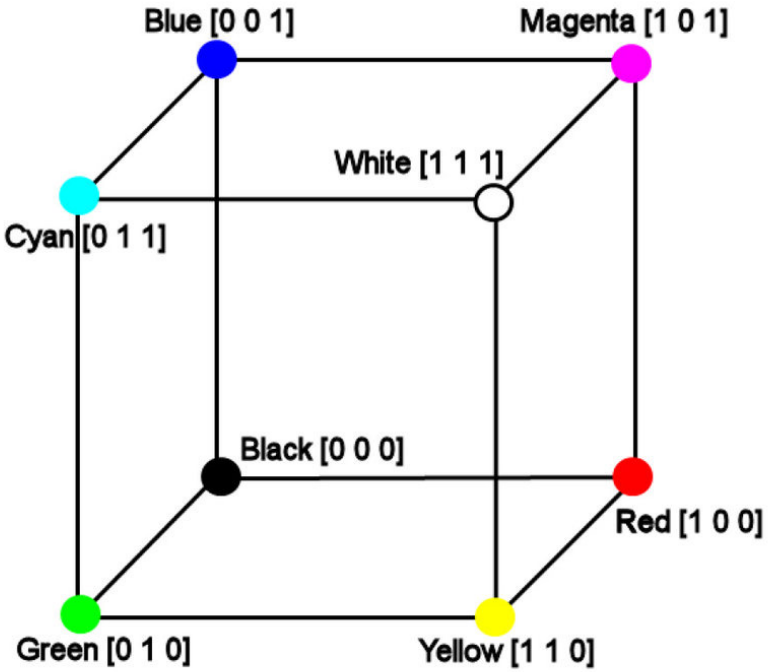
RGB

RGB

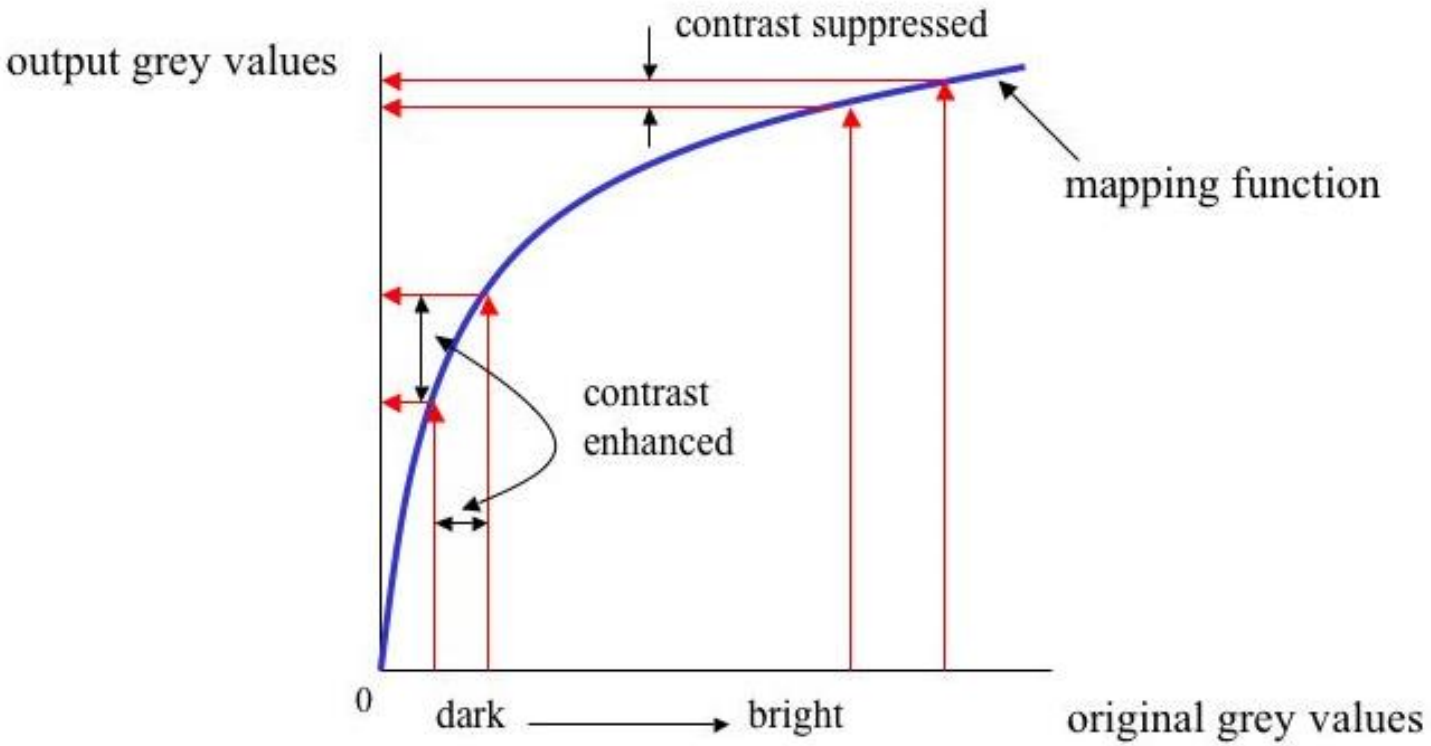


RGB

RGB


Blue [0 0 1]
Magenta [1 0 1]
White [1 1 1]
Cyan [0 1 1]
Black [0 0 0]
Red [1 0 0]
Green [0 1 0]
Yellow [1 1 0]

Contrast Enhancement



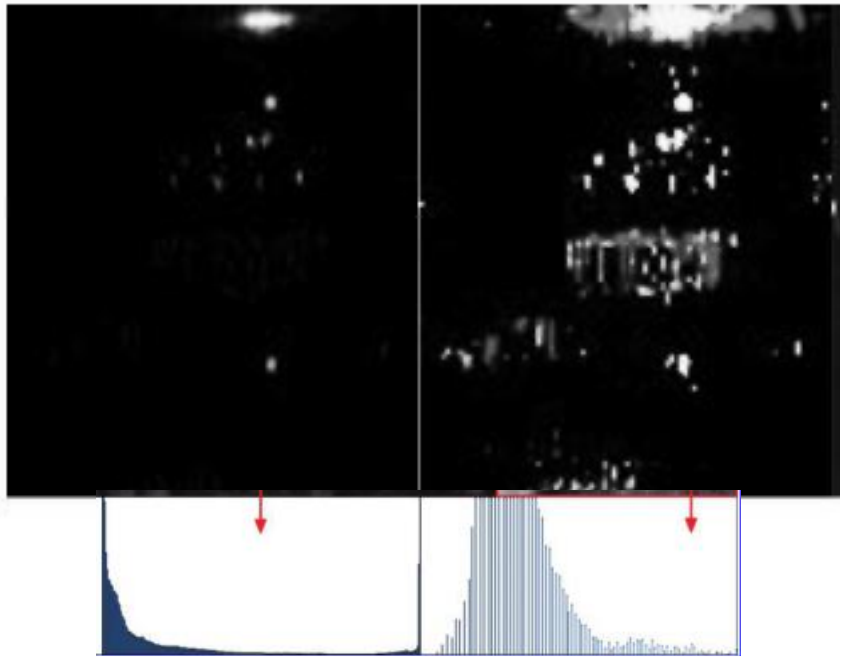
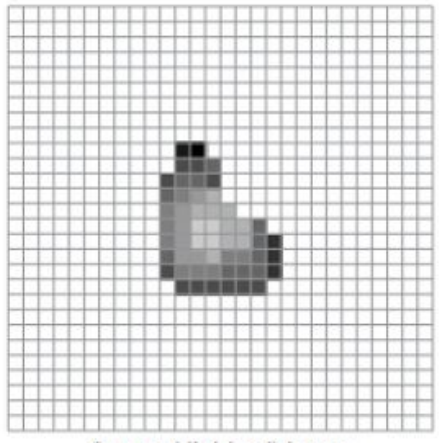


Image Filters

Convolution matrix

Kernel-mask values define filter behaviour



Identity

$$* \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} =$$

Image Filters

*

Mean

$$\frac{1}{9}\begin{bmatrix}1 & 1 & 1\\ 1 & 1 & 1\\ 1 & 1 & 1\end{bmatrix}$$

=

Image Filters

Mean

$$* \quad \frac{1}{81}\begin{bmatrix} 1&1&1&1&1&1&1&1&1\\ 1&1&1&1&1&1&1&1&1\\ 1&1&1&1&1&1&1&1&1\\ 1&1&1&1&1&1&1&1&1\\ 1&1&1&1&1&1&1&1&1\\ 1&1&1&1&1&1&1&1&1\\ 1&1&1&1&1&1&1&1&1\\ 1&1&1&1&1&1&1&1&1\\ 1&1&1&1&1&1&1&1&1 \end{bmatrix} \quad =$$

Image Filters

Horizontal Edge Enhancer

$$* \quad \begin{bmatrix} -1 \\ 2 \\ -1 \end{bmatrix} \quad =$$

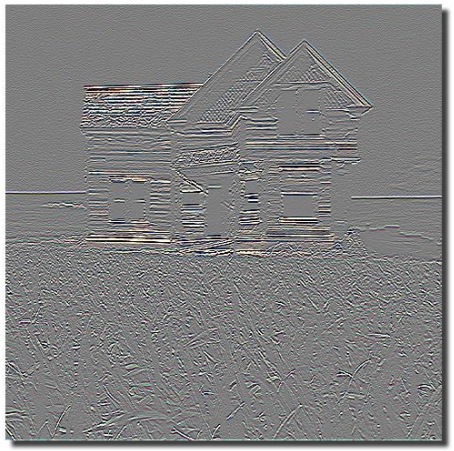


Image Filters

Edge Enhancer

$$* \quad \begin{bmatrix} 0 & -1 & 0 \\ -1 & 4 & -1 \\ 0 & -1 & 0 \end{bmatrix} \quad =$$

Image Restoration

- Linear degradation can be modelled in general as

$$g(i,j) = \sum_{k=1}^{K} \sum_{l=1}^{K} \boldsymbol{f}(\boldsymbol{k},\boldsymbol{l}) h(k,l,i,j)$$

Source: Interpol

Image Restoration

- Linear degradation can be modelled in general as

$$g(i,j) = \sum_{k=1}^{K}\sum_{l=1}^{K} \boldsymbol{f}(\boldsymbol{k},\boldsymbol{l})h(k,l,i,j)$$

$$f = h^{-1}g$$

Source: Interpol

Image Restoration

- Linear degradation can be modelled in general as

$$g(i,j) = \sum_{k=1}^{K}\sum_{l=1}^{K} \boldsymbol{f}(\boldsymbol{k},\boldsymbol{l})h(k,l,i,j)$$

$$f = h^{-1}g$$

Whirl transform

$$\mathrm{i}(t) = i_0 + \alpha t\cos(\beta t)$$
$$\mathrm{j}(t) = j_0 + \alpha t\sin(\beta t)$$

Source: Interpol

Image Restoration

- Linear degradation can be modelled in gene

$$g(i,j) = \sum_{k=1}^{K}\sum_{l=1}^{K} \boldsymbol{f}(\boldsymbol{k},\boldsymbol{l})h(k,l,i,j)$$

$$f = h^{-1}g$$

Whirl transform

$$\mathrm{i}(t) = i_0 + \alpha t\cos(\beta t)$$
$$\mathrm{j}(t) = j_0 + \alpha t\sin(\beta t)$$

Source: Interpol

Digital Forgery

Source: Autodesk

Digital Forgery

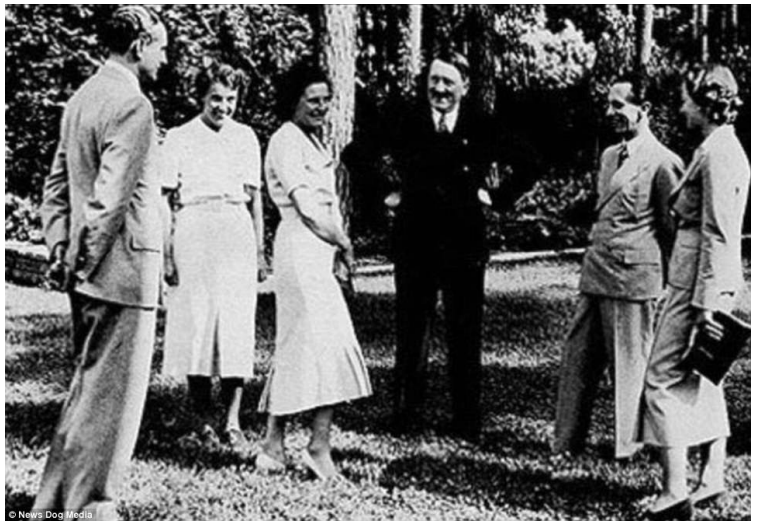
Source: Autodesk

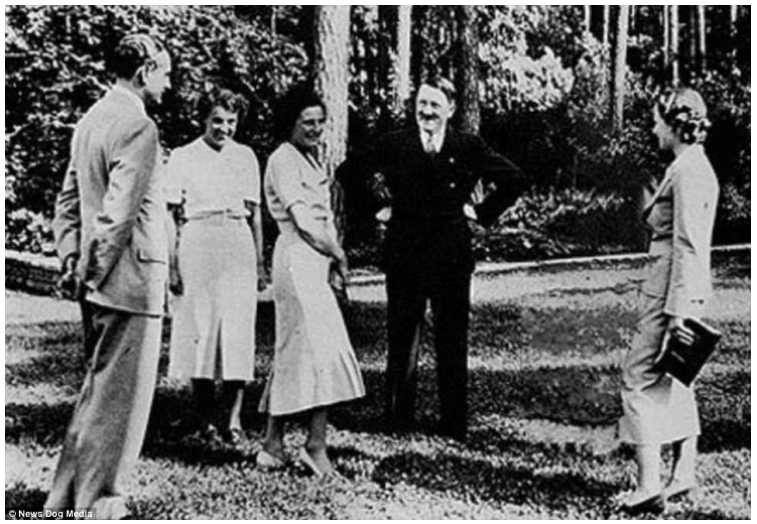
Digital Forgery

Digital Forgery

- https://thispersondoesnotexist.com/

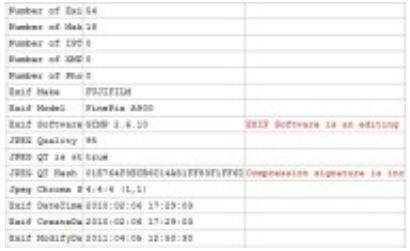
Digital Forgery

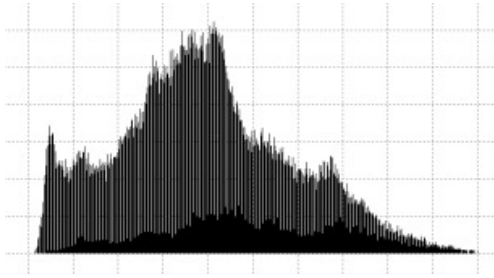




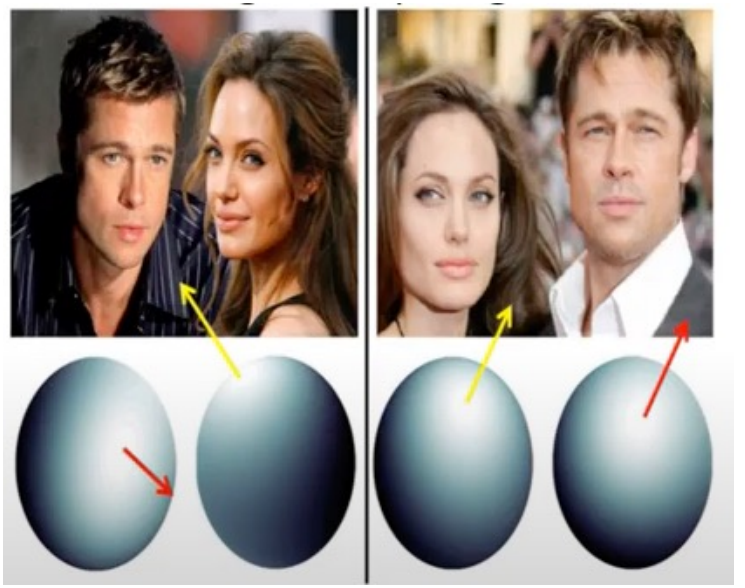
Digital Forgery

- How to authenticate an image?
  - Visual Inspection
  - File Analysis
    - File format and structures
    - Metadata
    - Compression Parameters (Quantization Tables)
  - Global Analysis
    - Pixel and compressed data statistics
  - Local Analysis
    - Inconsistencies of pixel statistics across the image

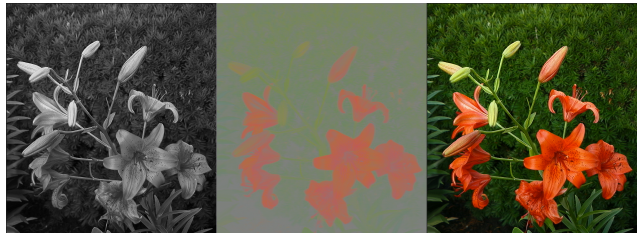




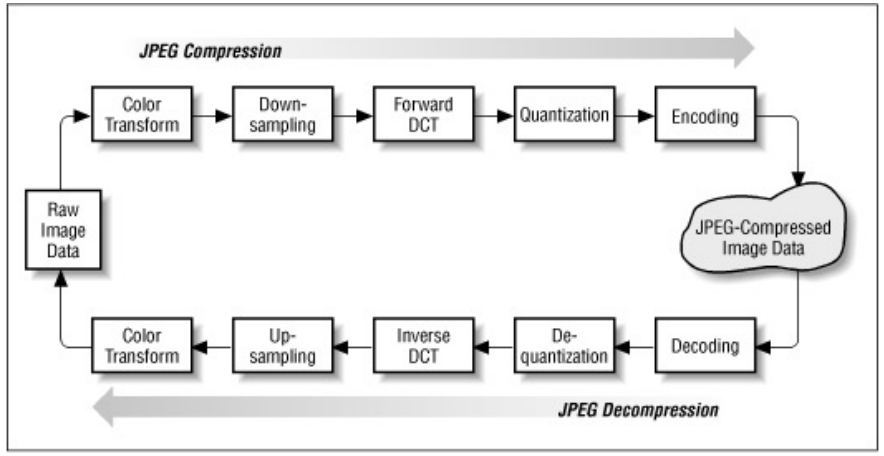
Visual Inspection

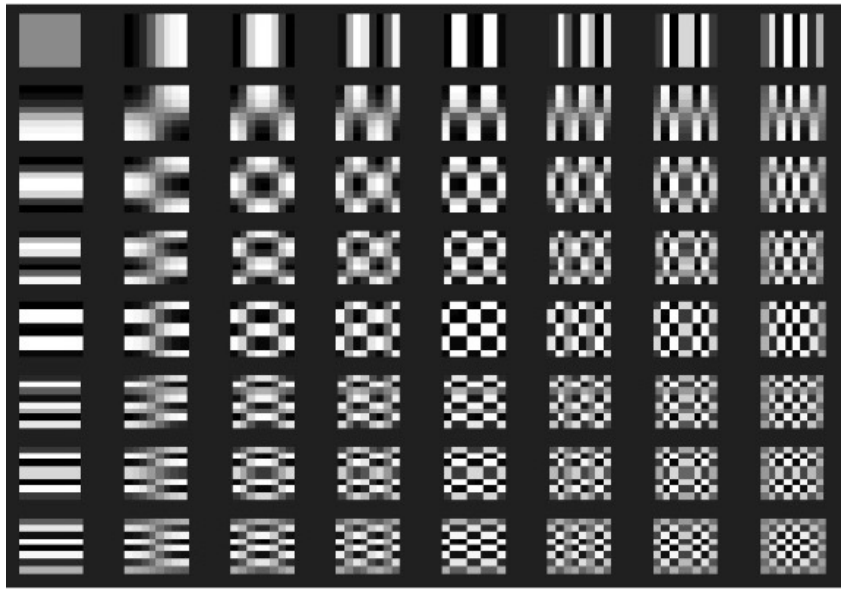


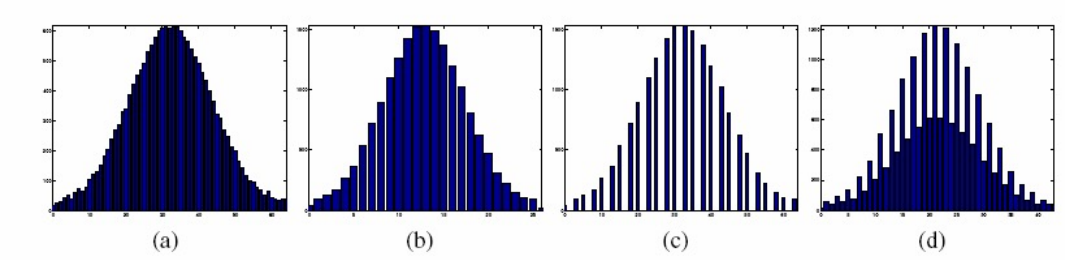
Digital Forgery



- JPEG images are lossy
- Manufactures offer different *Quantization Tables*



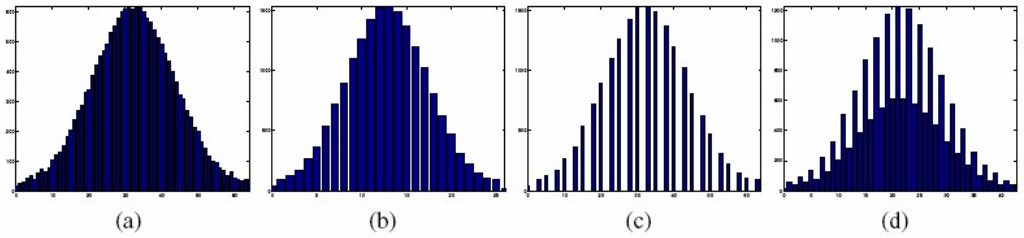


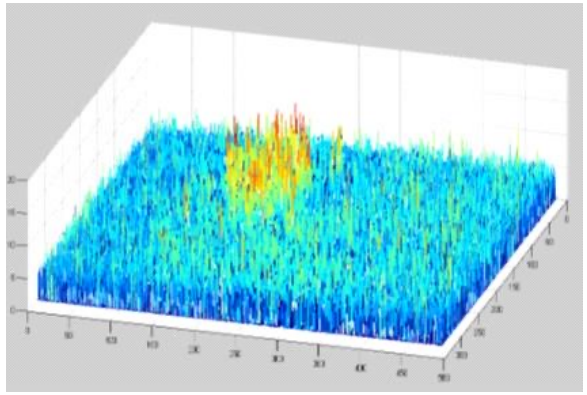


DCT Histograms

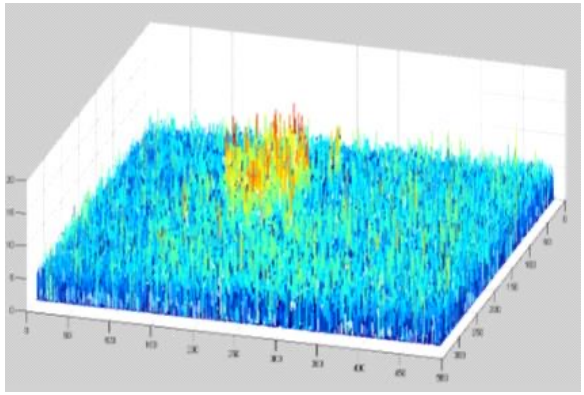
Digital Forgery

DCT Histograms





Digital Forgery



Limits of Computer Forensics

- Hardness of avoiding artifact alteration
  - Digital data is easy (and inexpensive) to manipulate
- Hardness of linking artifacts to real authors
- Easyness of creating ad-hoc probative values
  - Image enhancing vs Image alteration
  - Digital forgery: what's the original and what's the processed artifact?

Limits of Computer Forensics

- Hardness of avoiding artifact alteration
  - Digital data is easy (and inexpensive) to manipulate
- Hardness of linking artifacts to real authors

  - Take care of the original artifact
  - Ensure safe and non-repudiable acquisition
  - Do analysis on copies
  - Document to ensure reproducibility

- Easyness of creating ad-hoc probative values
  - Image enhancing vs Image alteration
  - Digital forgery: what's the original and what's the processed artifact?

Summary

- Incident Response: complex process that includes CF
- Computer Forensics: multidisciplinary process that require method application
- Disk Forensics: Ext2/3/4 + journaling + carving
- Image/Video Forensics: Image restoration vs image enhancement vs image forgery