TECHNISCHE UNIVERSITÄT DRESDEN

UNIVERSITÄT MANNHEIM

Multimedia Forensics is not Computer Forensics

Rainer Böhme[†], Felix Freiling[‡], Thomas Gloe[†], Matthias Kirchner[†]

[†] Technische Universität Dresden [‡] Universität Mannheim

International Workshop on Computational Forensics 2009 (IWCF'09)

The Hague · 2009/8/14

Outline

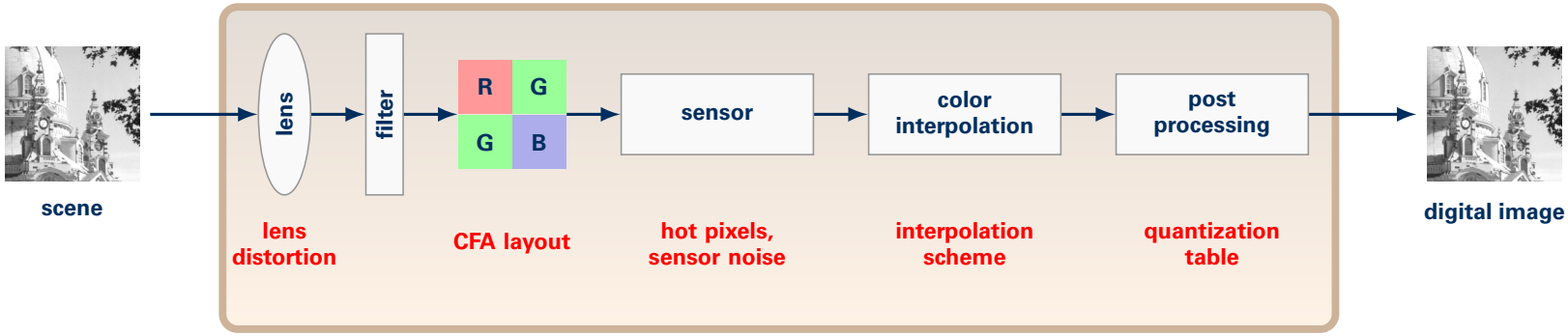
1. Multimedia forensics and computer forensics
2. Multimedia forensics is not computer forensics
3. Counter-forensics
4. And how does this all relate to practice?

Multimedia forensics

A science to assess the authenticity of digital media objects

manipulation detection and **source device identification** based on

- *artifacts of processing operations*
  resampling · copy & paste · inconsistent lightning · double compression
- *characteristics of the source device*
  e. g. digital camera



Multimedia forensics: Examples

- digital camera identification
  based on sensor noise

Multimedia forensics: Examples

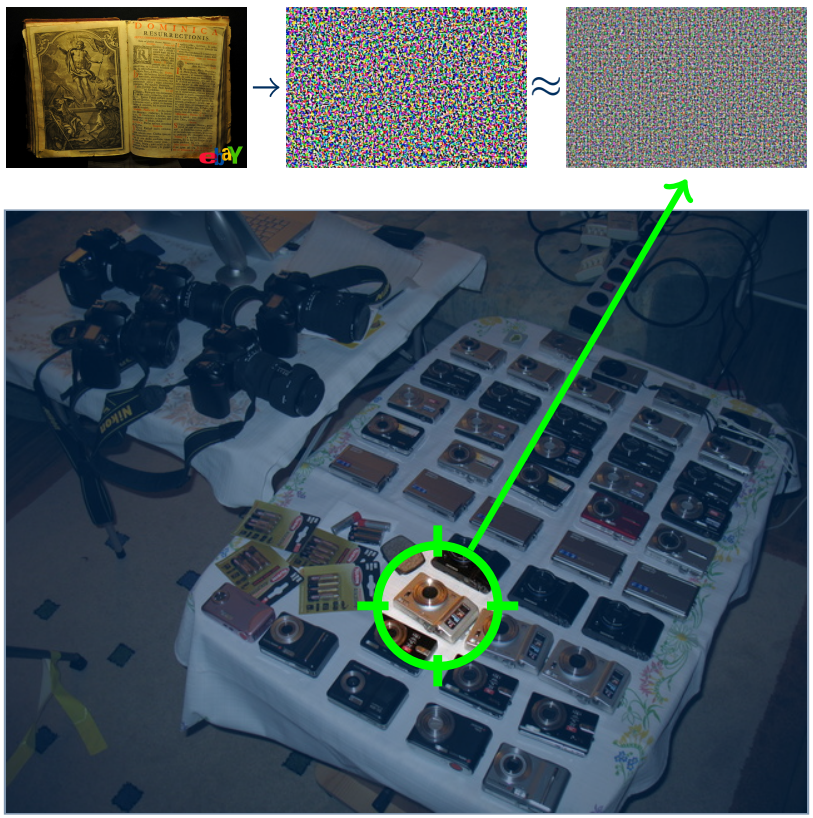
- digital camera identification
  based on sensor noise

Multimedia forensics: Examples

- digital camera identification
  based on sensor noise

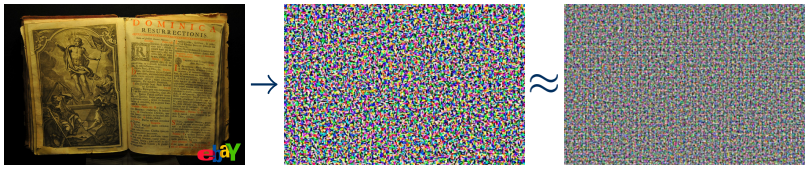
Multimedia forensics: Examples

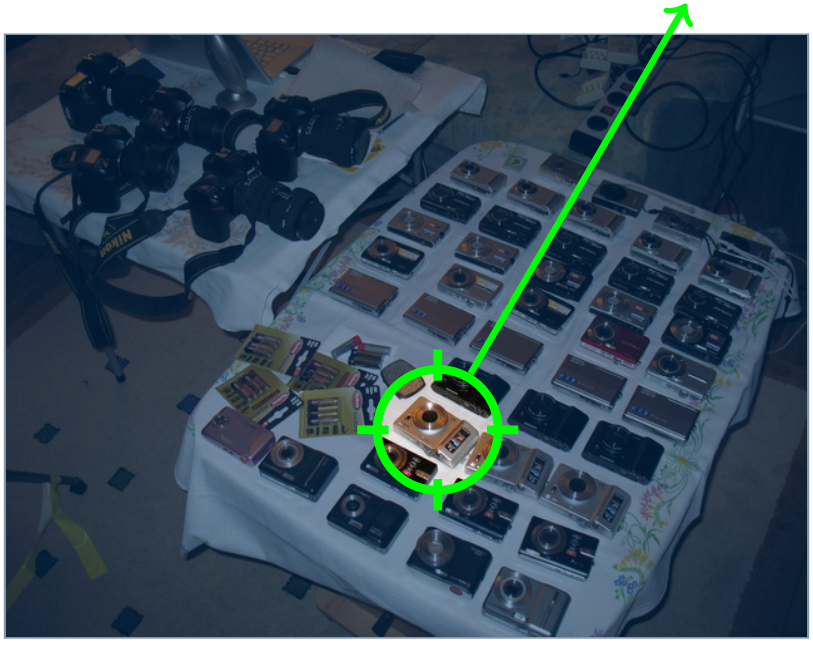
- digital camera identification
  based on sensor noise



Multimedia forensics: Examples

- digital camera identification based on sensor noise

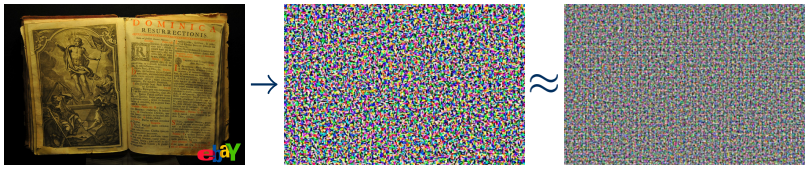


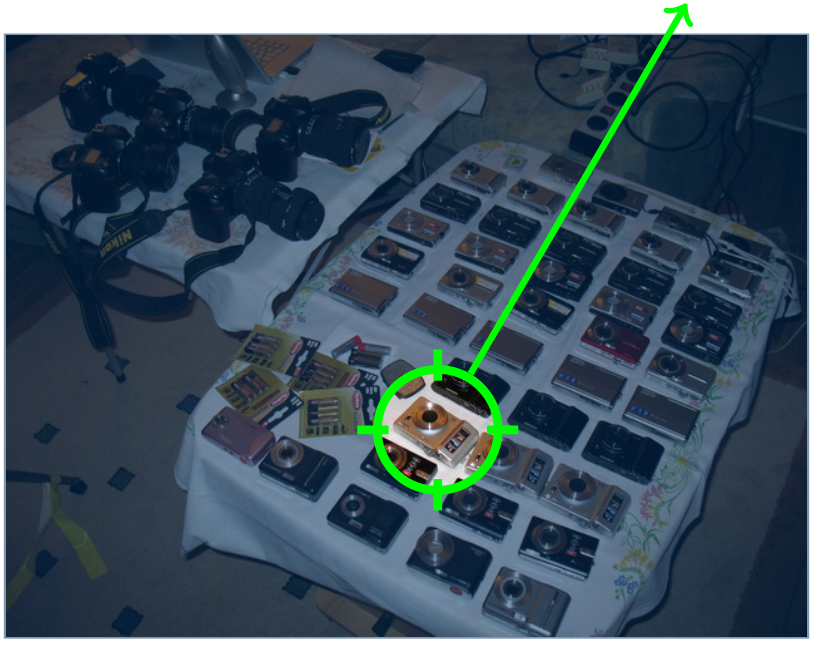


- copy & paste detection

Multimedia forensics: Examples

- digital camera identification based on sensor noise





- copy & paste detection

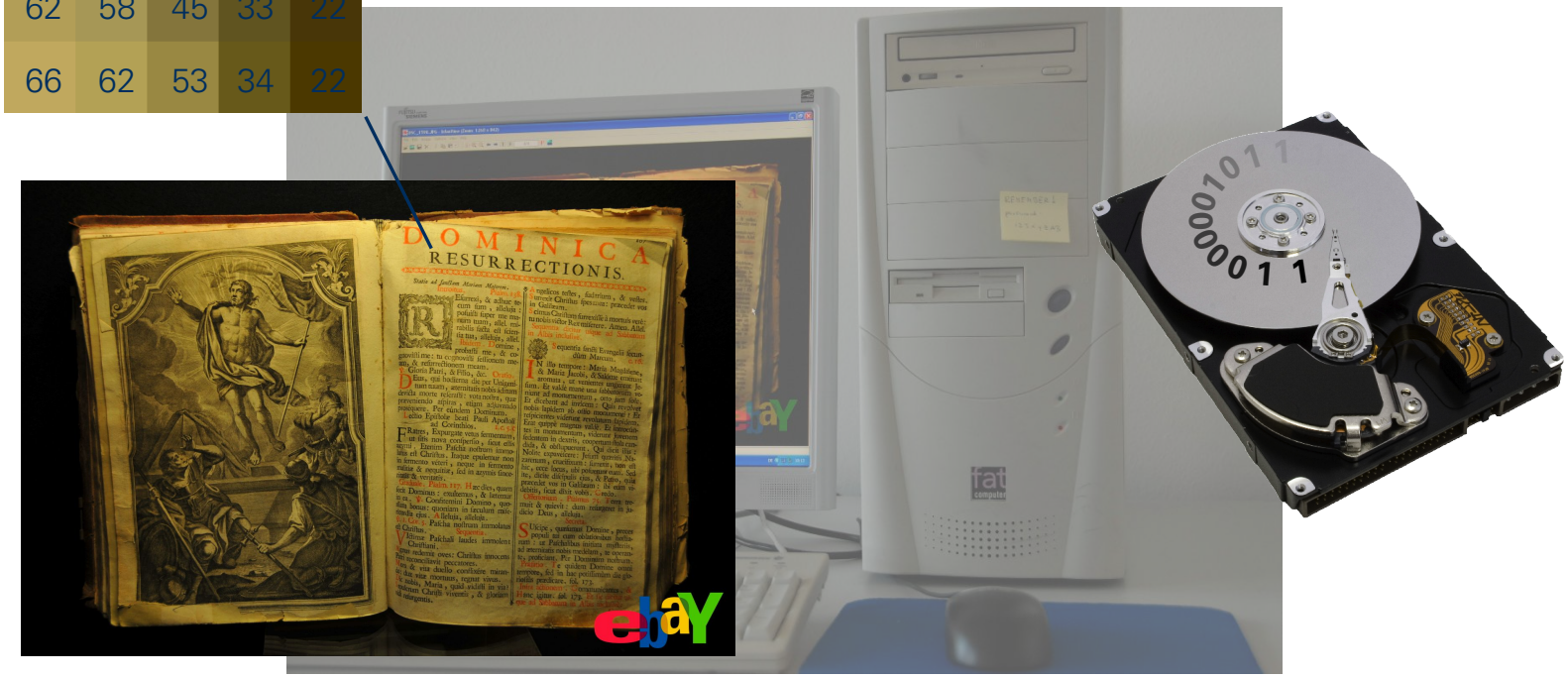
By the way,
what is computer forensics?

Computer forensics

Computer forensics

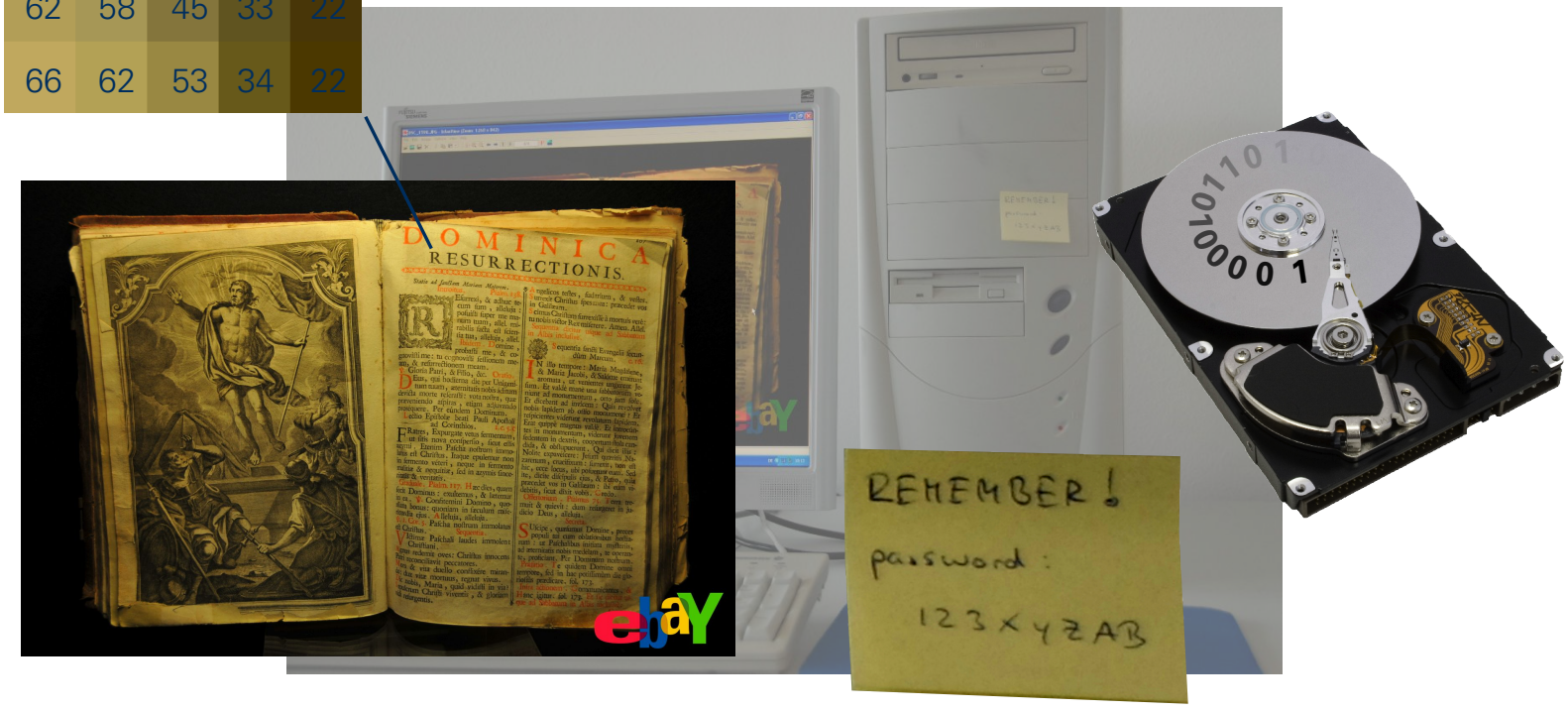
Computer forensics

52	51	51	51	49
49	40	36	34	33
55	48	40	33	23
62	58	45	33	22
66	62	53	34	22



Computer forensics

52	51	51	51	49
49	40	36	34	33
55	48	40	33	23
62	58	45	33	22
66	62	53	34	22



Outline

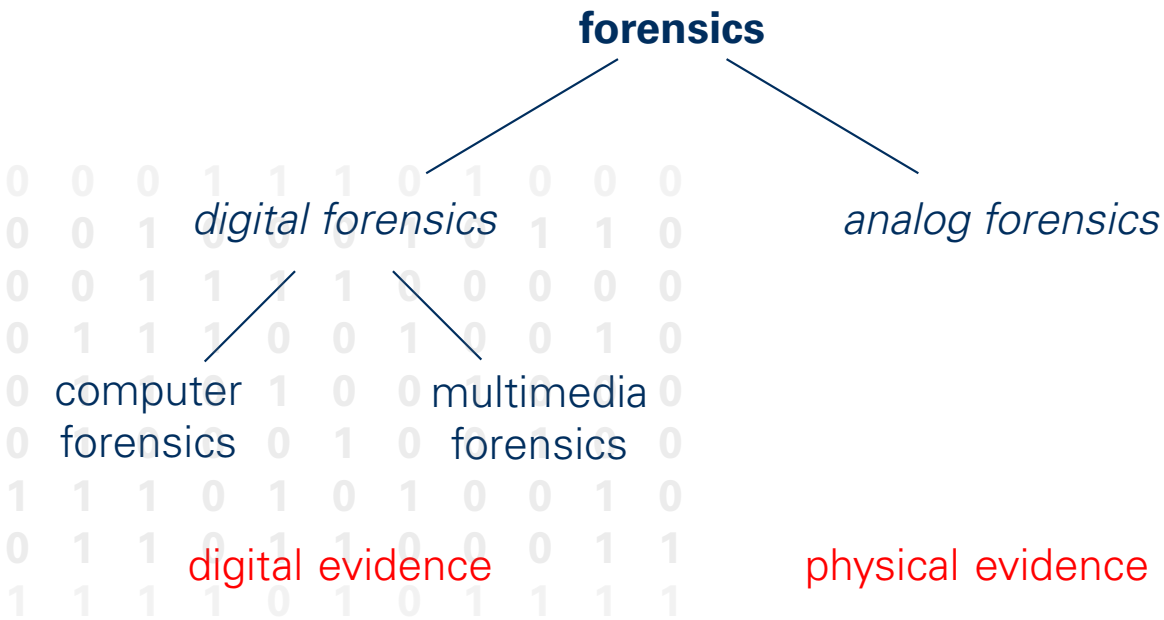
1 Multimedia forensics and computer forensics

2 **Multimedia forensics is not computer forensics**

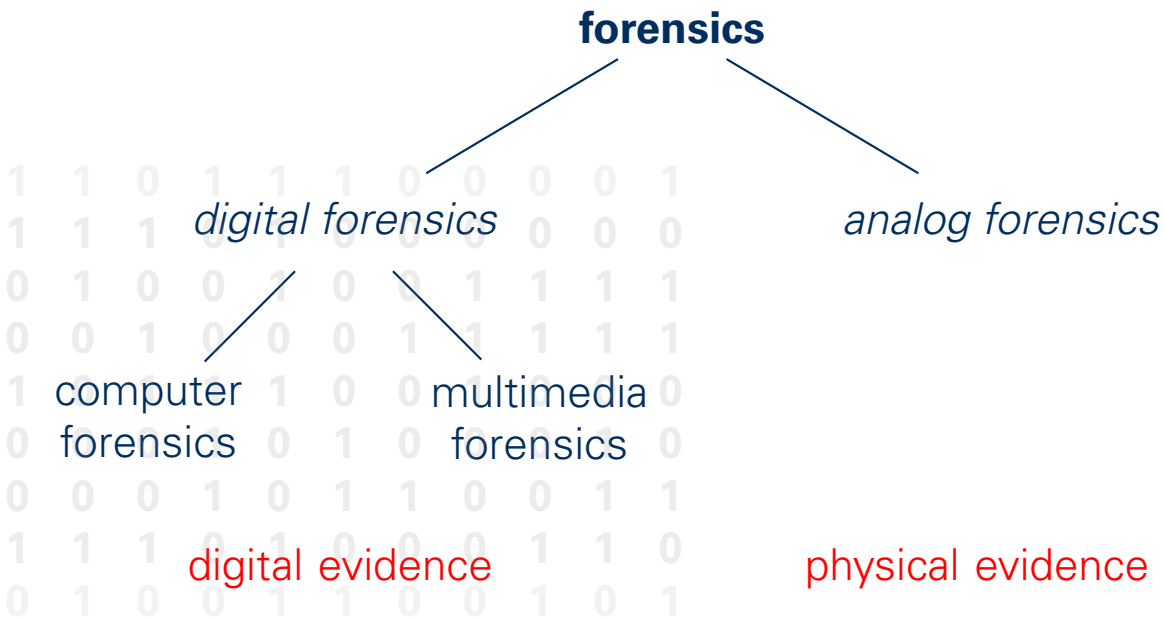
3 Counter-forensics

4 And how does this all relate to practice?

Digital forensics: proposed ontology



Digital forensics: proposed ontology



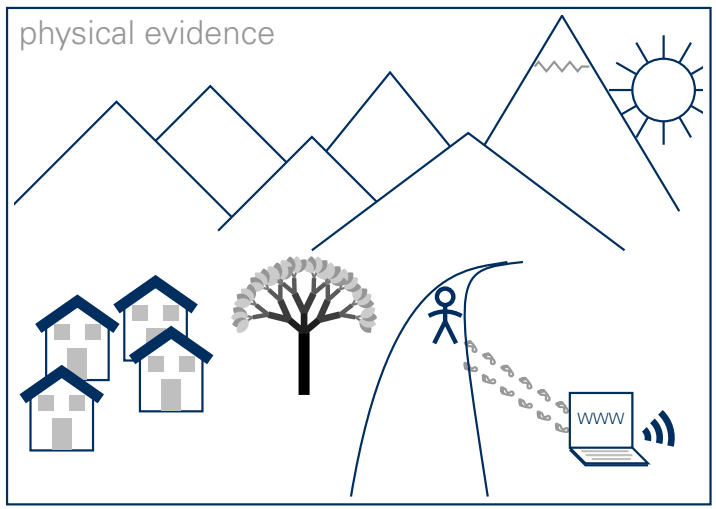
finite sequence of discrete and perfectly observable symbols

WARNING!

The following slides intentionally draw a very black-and-white picture

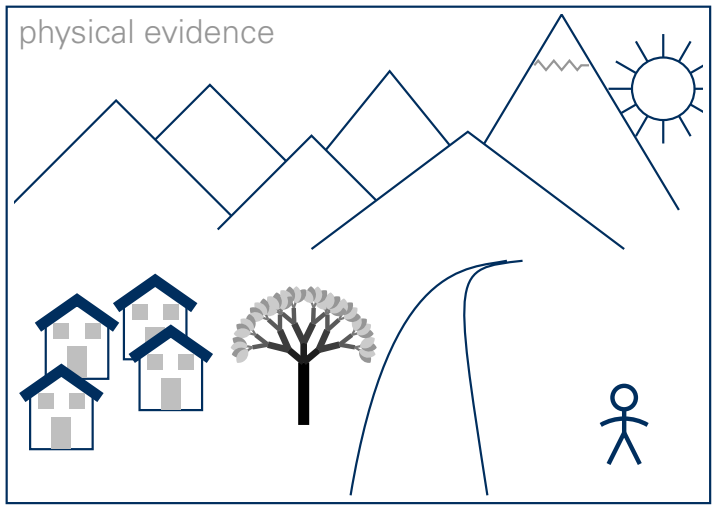
Computer forensics ≠ Multimedia forensics

computer forensics



digital evidence

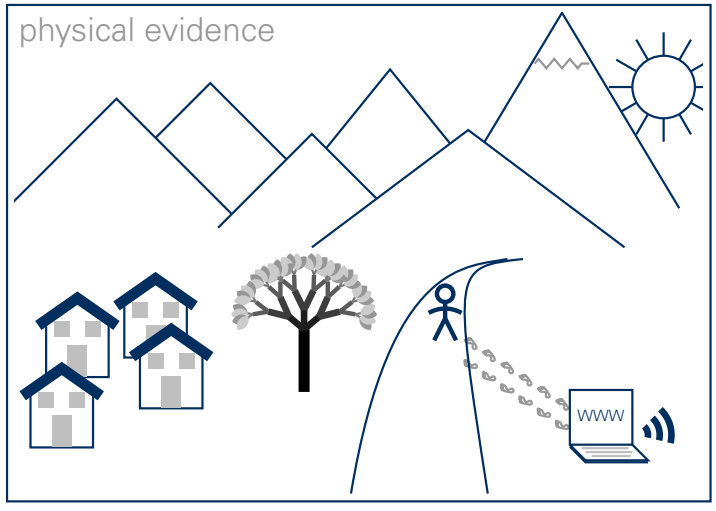
multimedia forensics



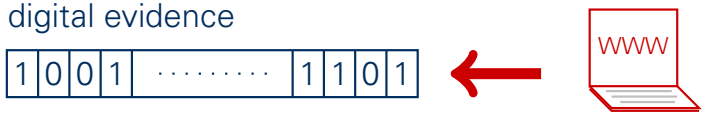
digital evidence

Computer forensics ≠ Multimedia forensics

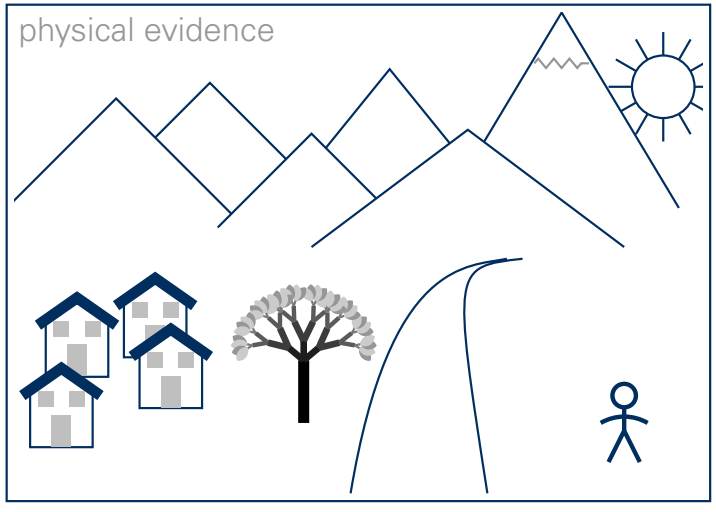
computer forensics



digital evidence



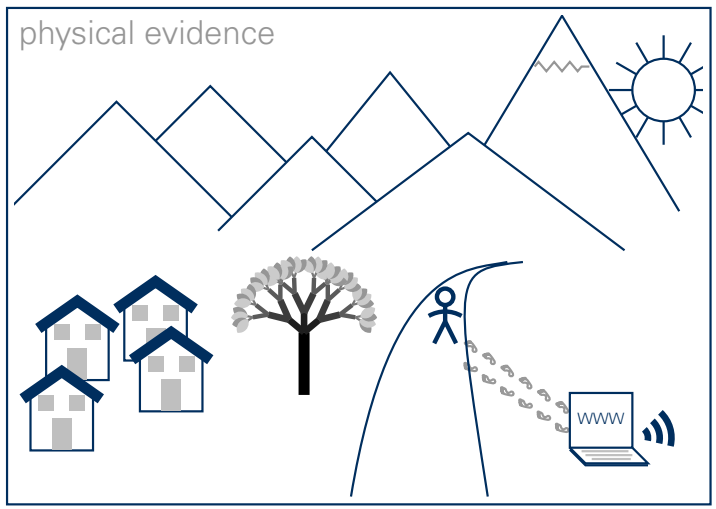
multimedia forensics



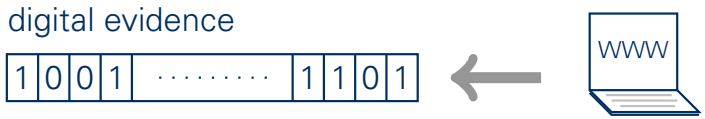
digital evidence

Computer forensics ≠ Multimedia forensics

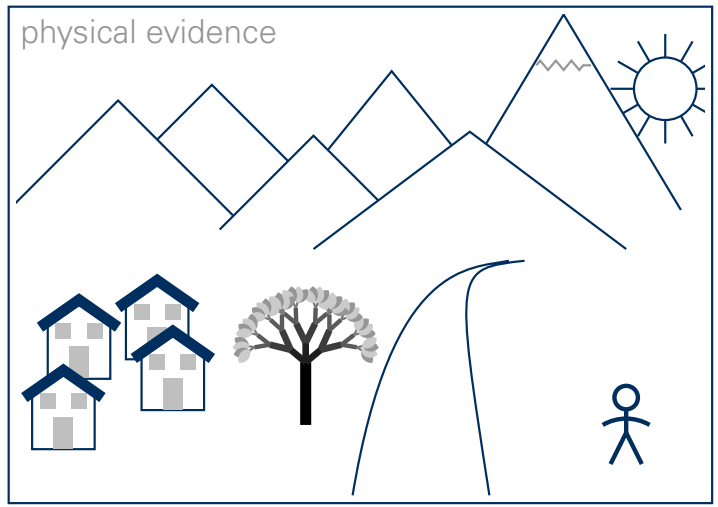
computer forensics



digital evidence



multimedia forensics

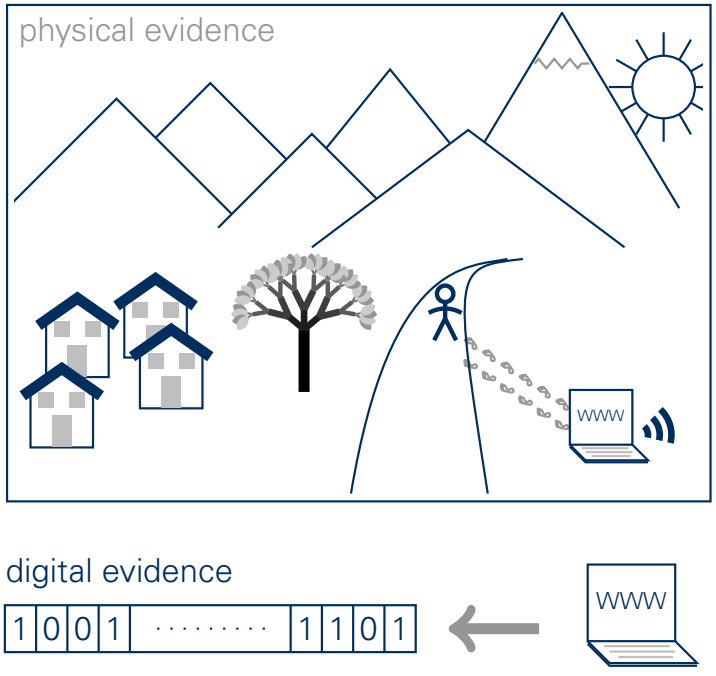


digital evidence

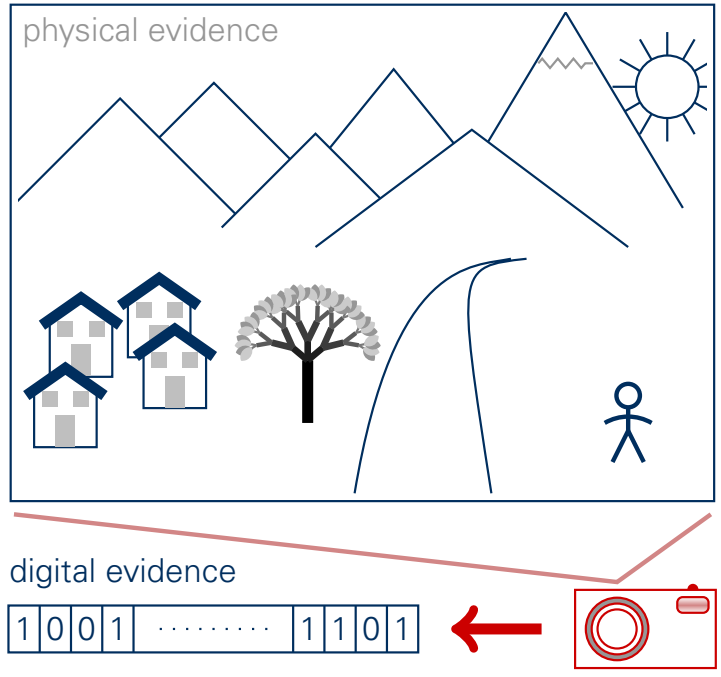
- digital evidence **is not** linked to the outside world

Computer forensics ≠ Multimedia forensics

computer forensics



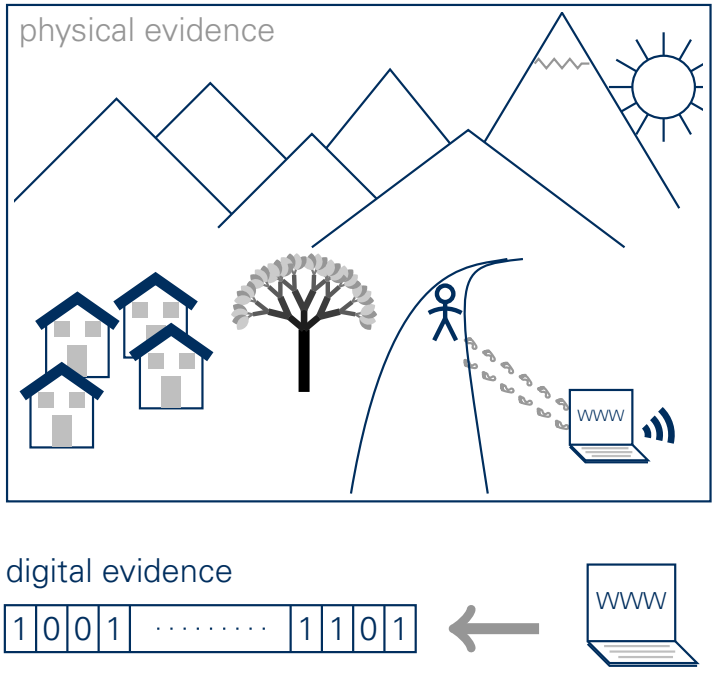
multimedia forensics



- digital evidence **is not** linked to the outside world

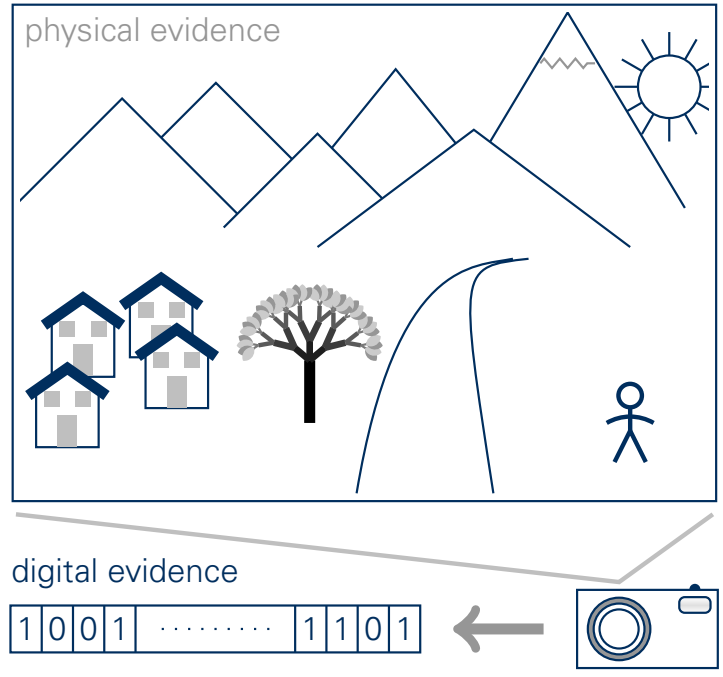
Computer forensics ≠ Multimedia forensics

computer forensics



- digital evidence **is not** linked to the outside world

multimedia forensics



- digital evidence **is** linked to the outside world

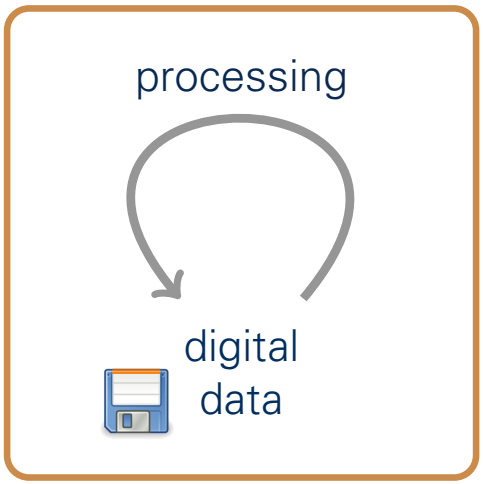
Computer forensics: A closer look

Computer forensics: A closer look

suspicious traces?

Computer forensics: A closer look

suspicious traces?

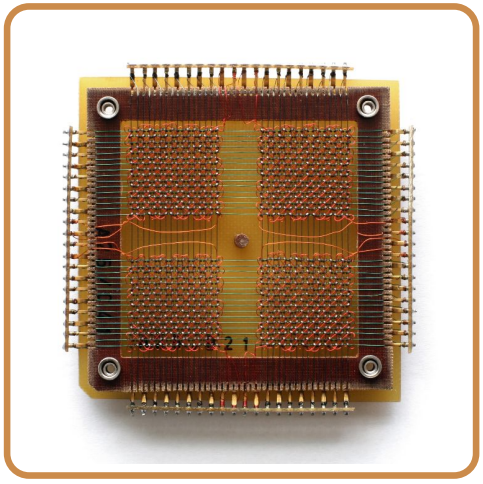


reality

- digital evidence is stored in the finite automaton each computer represents
- number of states in a closed system is finite

Computer forensics: A closer look

suspicious traces?

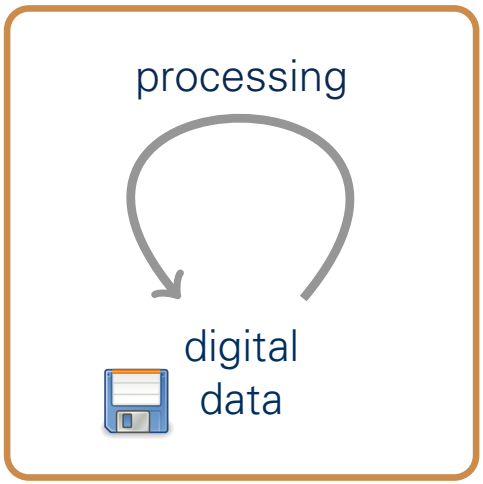


reality

- digital evidence is stored in the finite automaton each computer represents
- number of states in a closed system is finite

Computer forensics: A closer look

suspicious traces?



reality

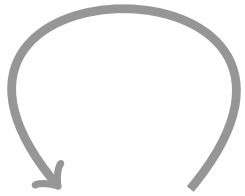
- digital evidence is stored in the finite automaton each computer represents
- number of states in a closed system is finite
- non-negligible chance that a computer is left in a state which **perfectly** erases all traces

Multimedia forensics: A closer look

Multimedia forensics: A closer look

original?

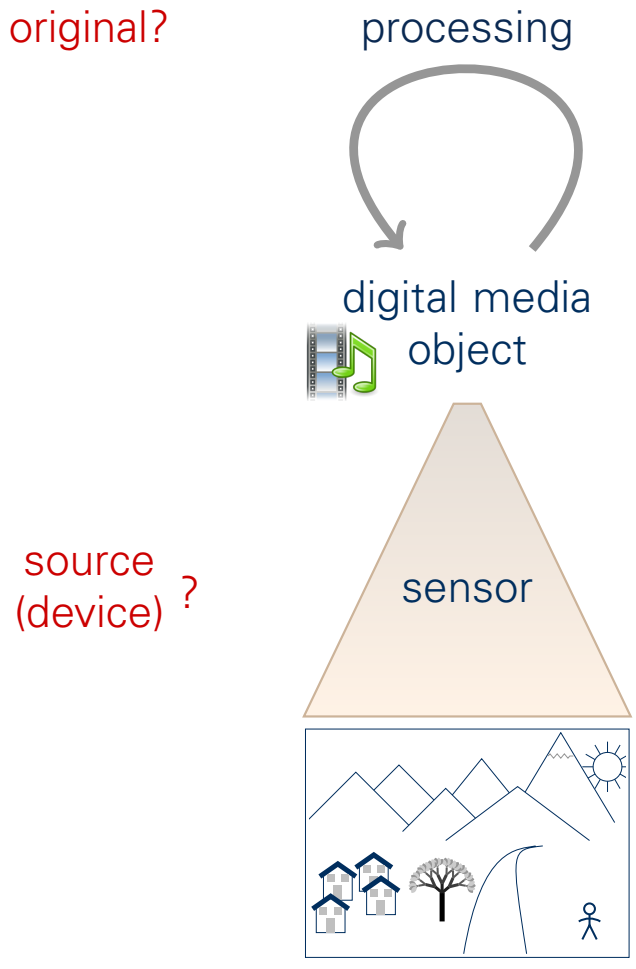
processing



digital media object

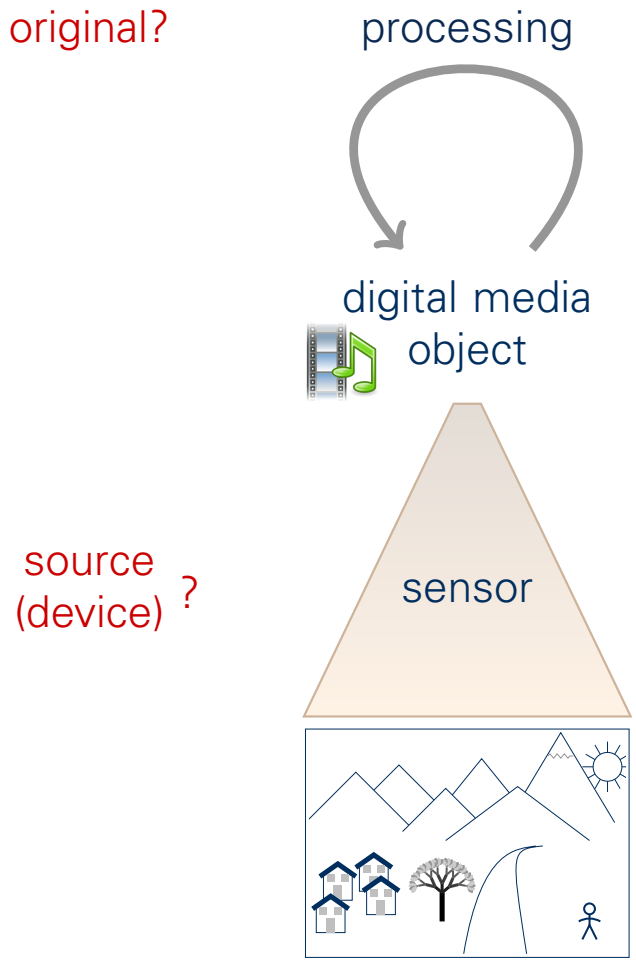
source (device) ?

Multimedia forensics: A closer look



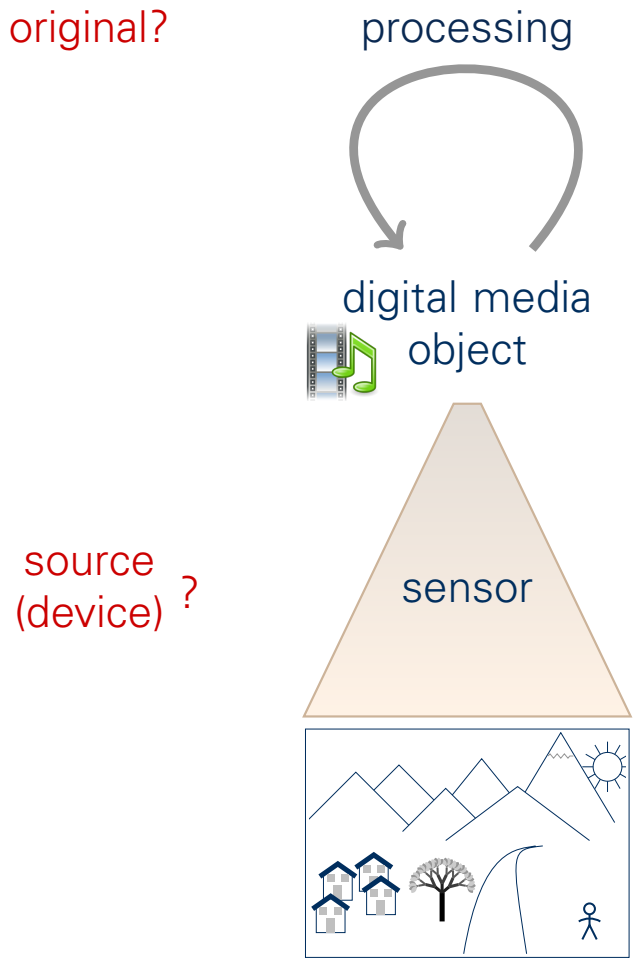
- sensors capture parts of the reality and transform them into digital representations

Multimedia forensics: A closer look



- sensors capture parts of the reality and transform them into digital representations
- reality is incognizable: ultimate knowledge whether a piece of digital media reflects reality or not cannot exist

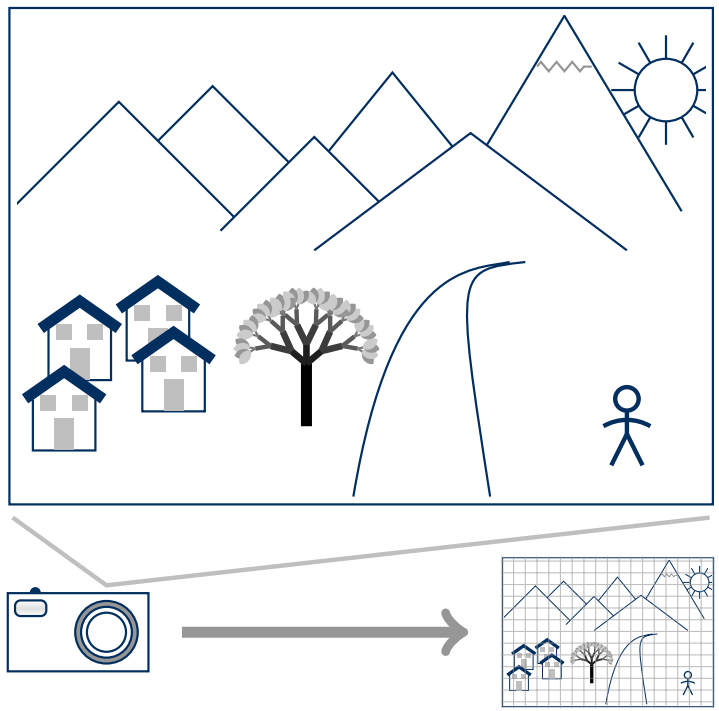
Multimedia forensics: A closer look



- sensors capture parts of the reality and transform them into digital representations
- reality is incognizable: ultimate knowledge whether a piece of digital media reflects reality or not cannot exist
- multimedia forensics = empirical science

Sensors: A source of uncertainty

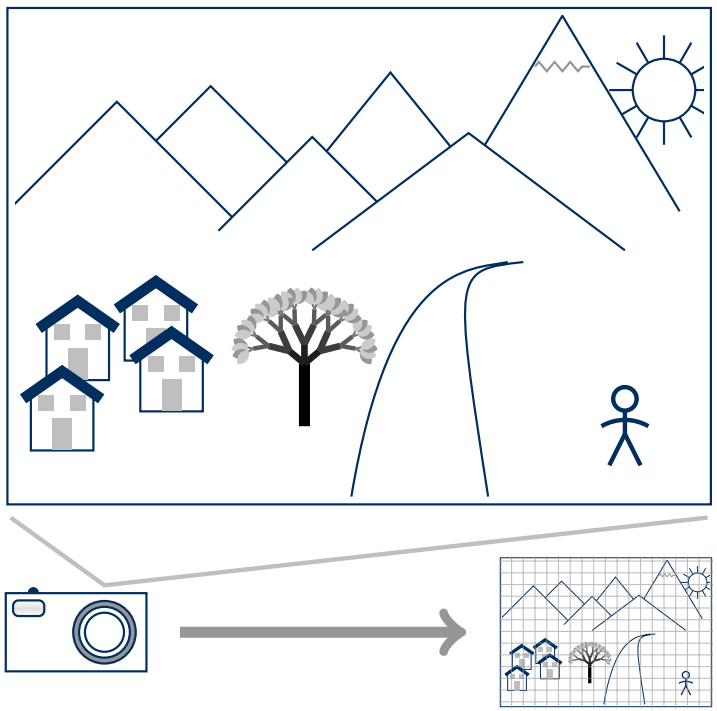
- projection of reality to discrete symbols means a dimensionality reduction



Sensors: A source of uncertainty

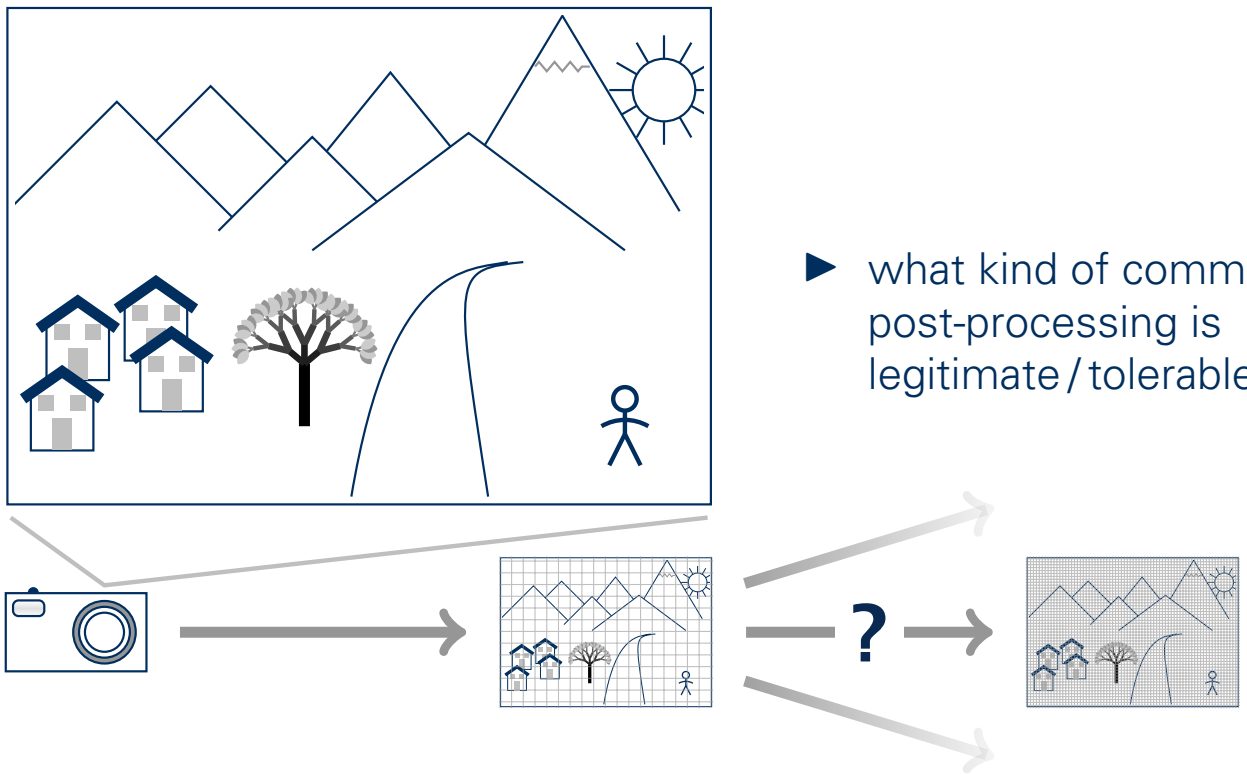
degrees of freedom

- projection of reality to discrete symbols means a dimensionality reduction
- multimedia forensics has to cope with an additional source of uncertainty



Sensors: A source of uncertainty

- projection of reality to discrete symbols means a dimensionality reduction
- multimedia forensics has to cope with an additional source of uncertainty



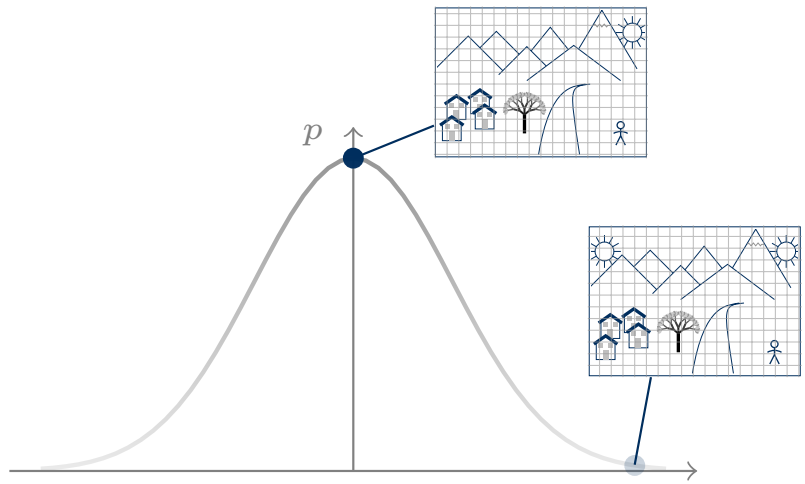
- what kind of common post-processing is legitimate / tolerable?

Models: Yet another dimensionality reduction

- **models** make projection of reality to discrete symbols tractable with formal methods
- typical models in multimedia forensics:
  - sensor noise follows a Gaussian distribution
  - connected regions of identical pixel values are unlikely to occur in original images

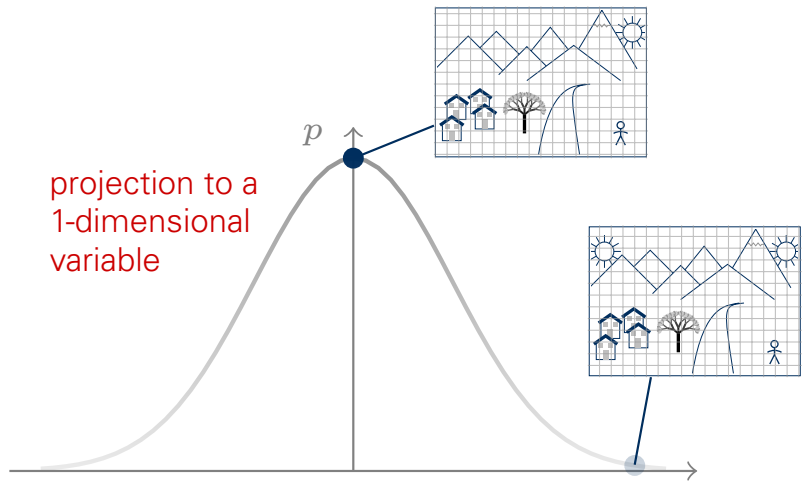
Models: Yet another dimensionality reduction

- **models** make projection of reality to discrete symbols tractable with formal methods
- typical models in multimedia forensics:
  - sensor noise follows a Gaussian distribution
  - connected regions of identical pixel values are unlikely to occur in original images



Models: Yet another dimensionality reduction

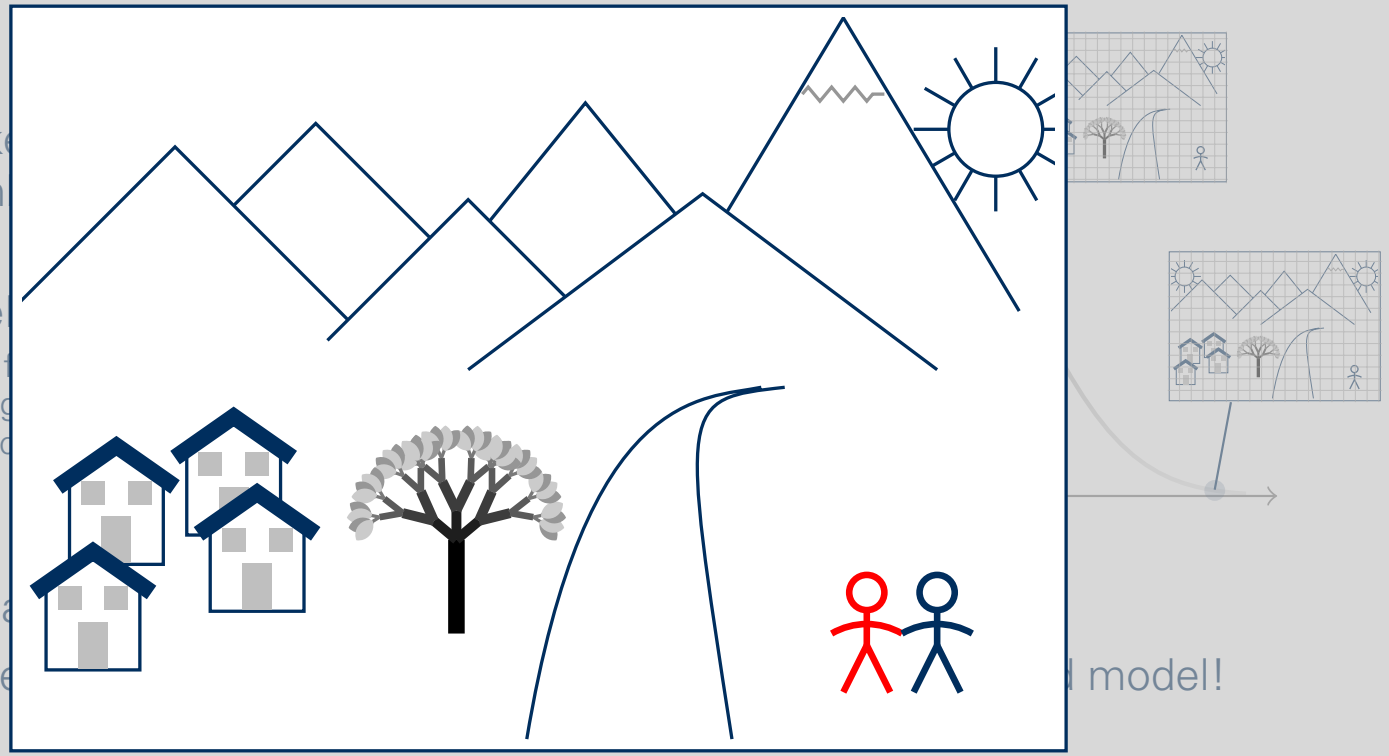
- **models** make projection of reality to discrete symbols tractable with formal methods
- typical models in multimedia forensics:
  - sensor noise follows a Gaussian distribution
  - connected regions of identical pixel values are unlikely to occur in original images



- models of reality function as yet another dimensionality reduction
- quality of forensic methods depends on the quality of the employed model!

Models: Yet another dimensionality reduction

- **models** mak
  discrete sym
  methods
- typical mode
  - ▷ sensor noise
  - ▷ connected reg
    unlikely to occ
- models of rea
- quality of fore



model!

Outline

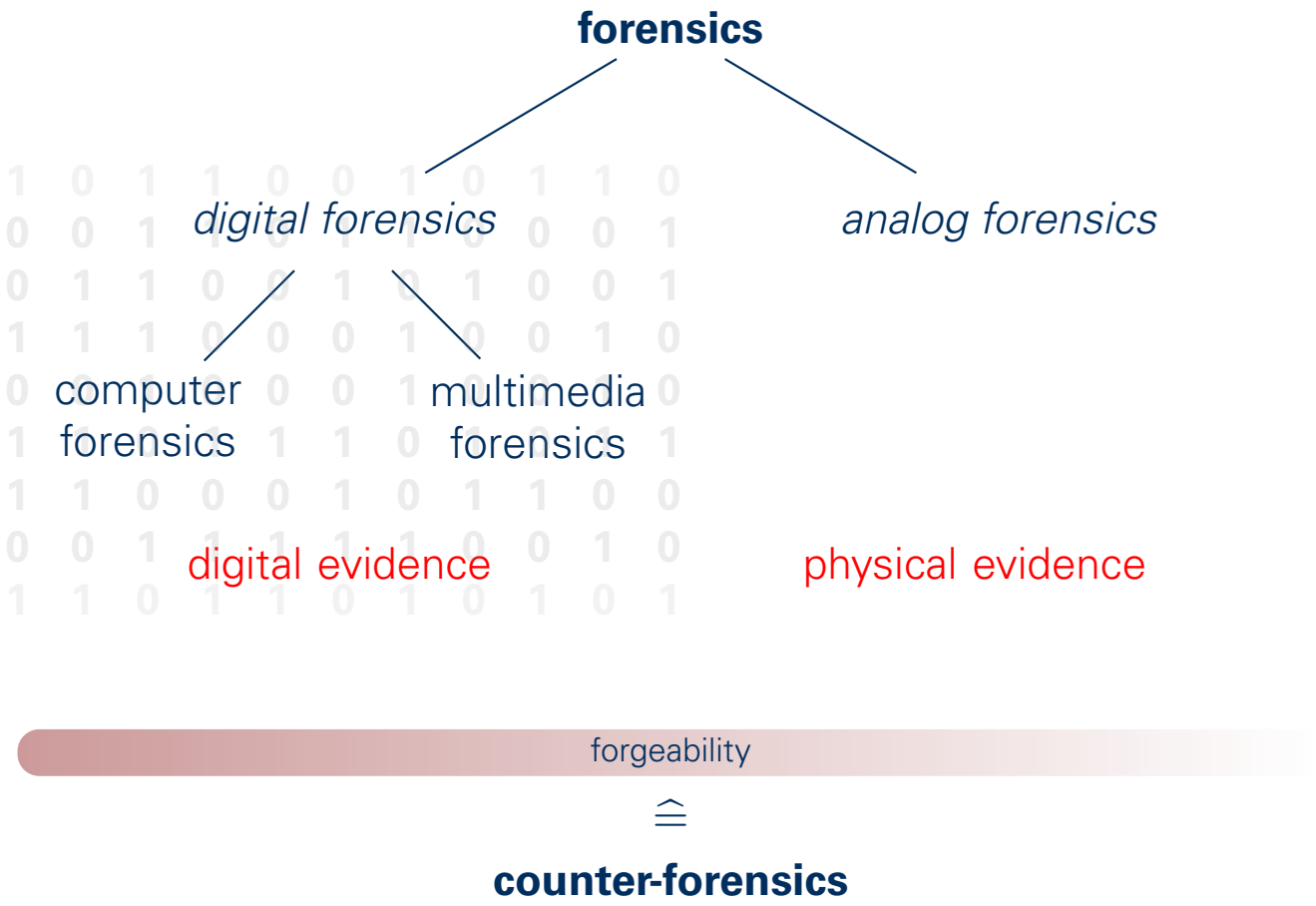
1 Multimedia forensics and computer forensics

2 Multimedia forensics is not computer forensics

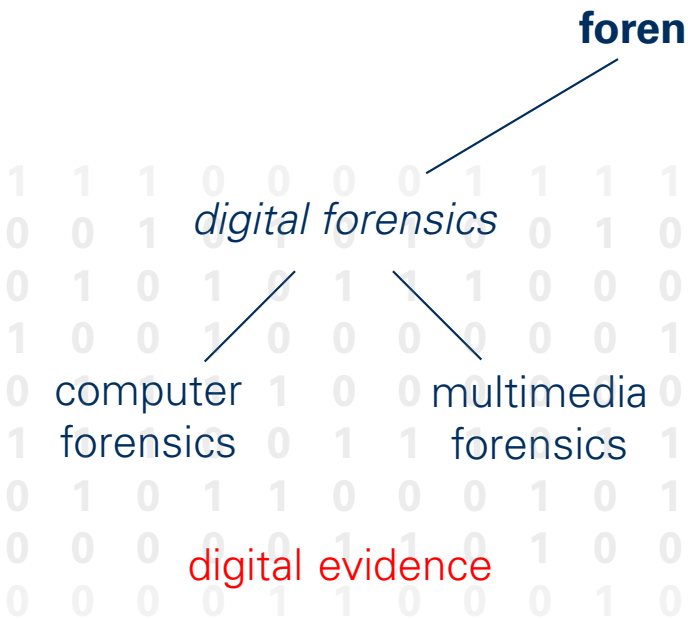
3 **Counter-forensics**

4 And how does this all relate to practice?

Digital forensics: proposed ontology



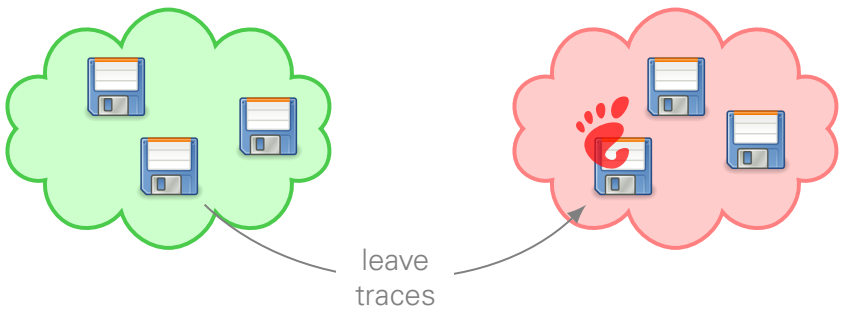
Digital forensics: proposed ontology



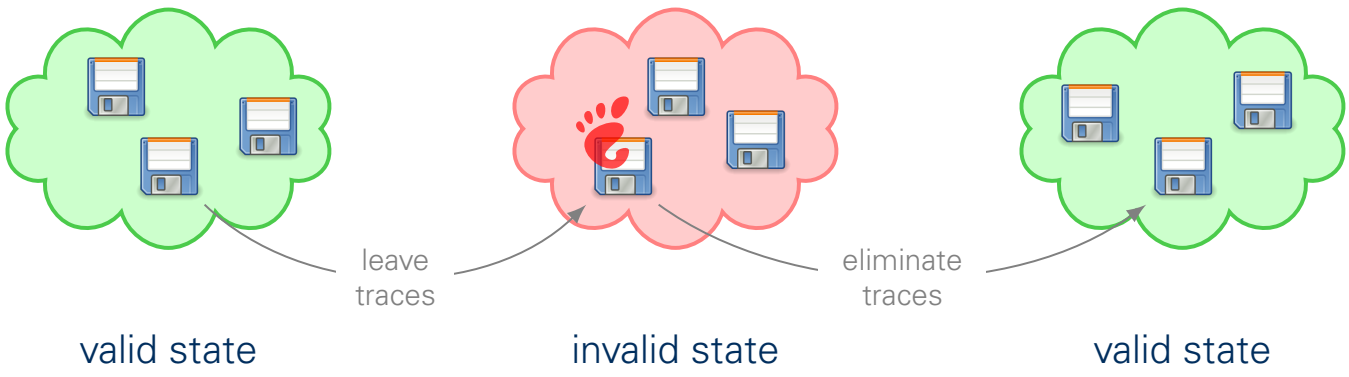
"physical evidence cannot be wrong,
it cannot perjure itself,
it cannot be wholly absent"

Kirk (1953)

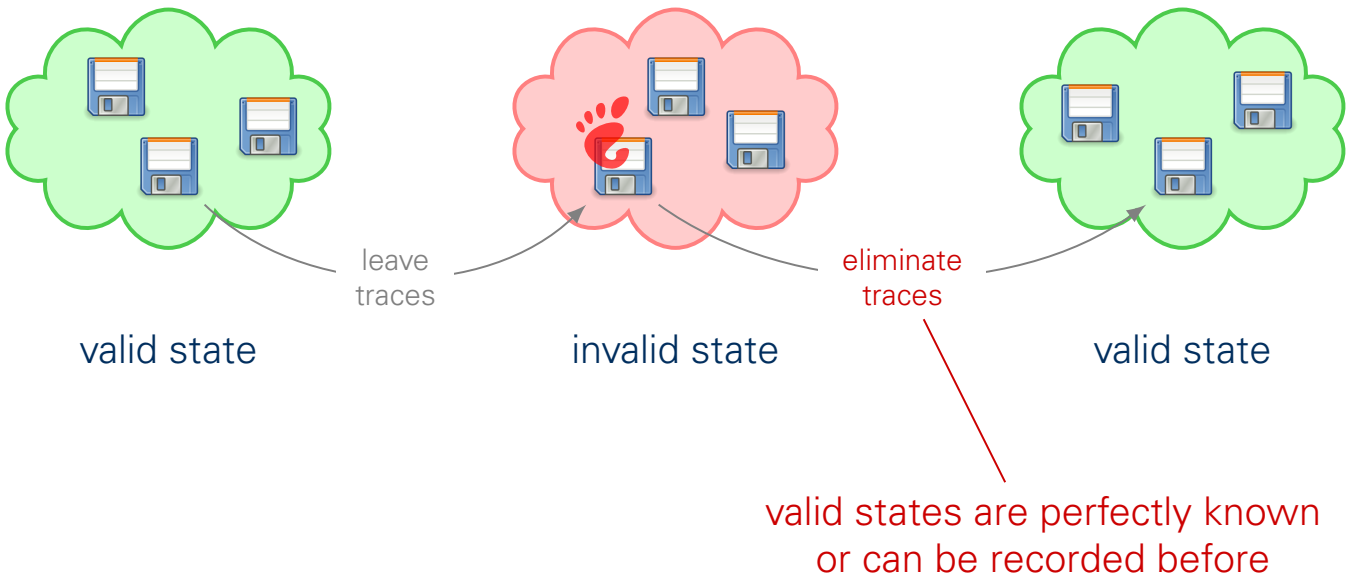
Counter-forensics: Computer forensics



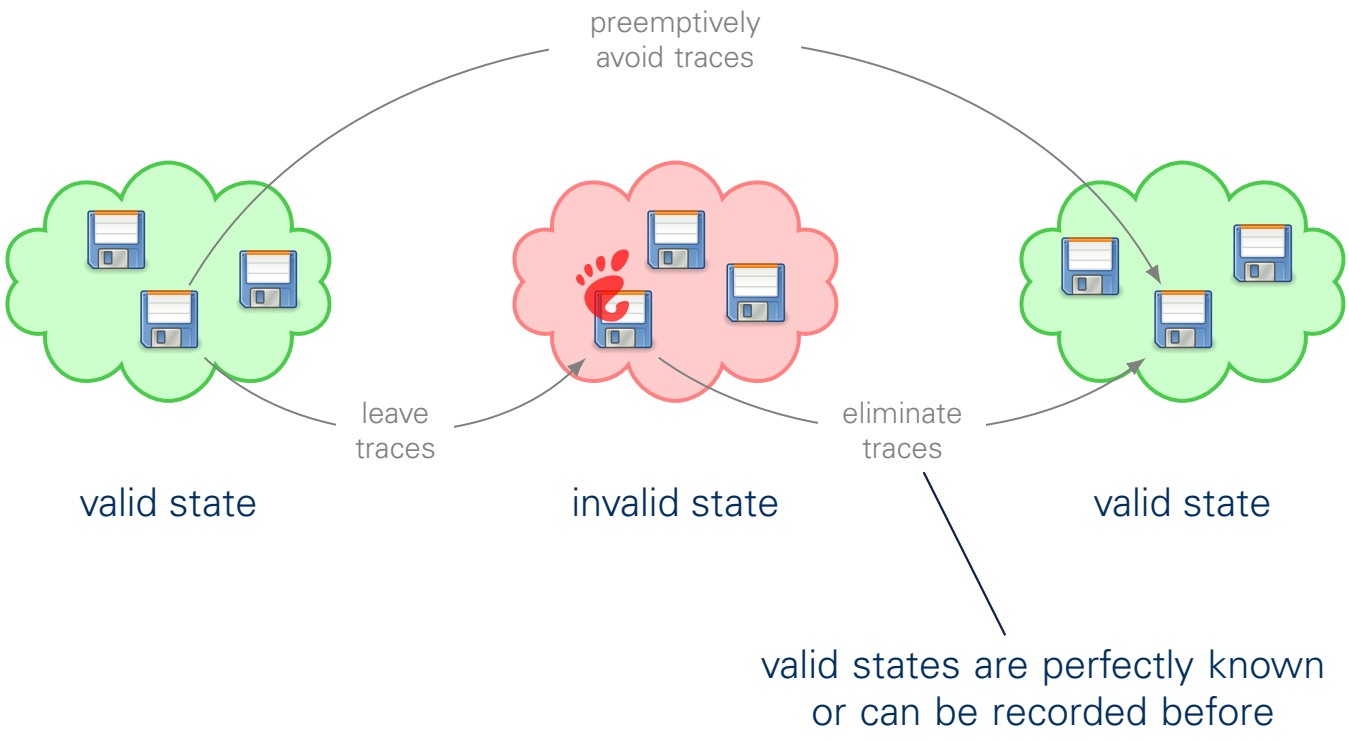
Counter-forensics: Computer forensics



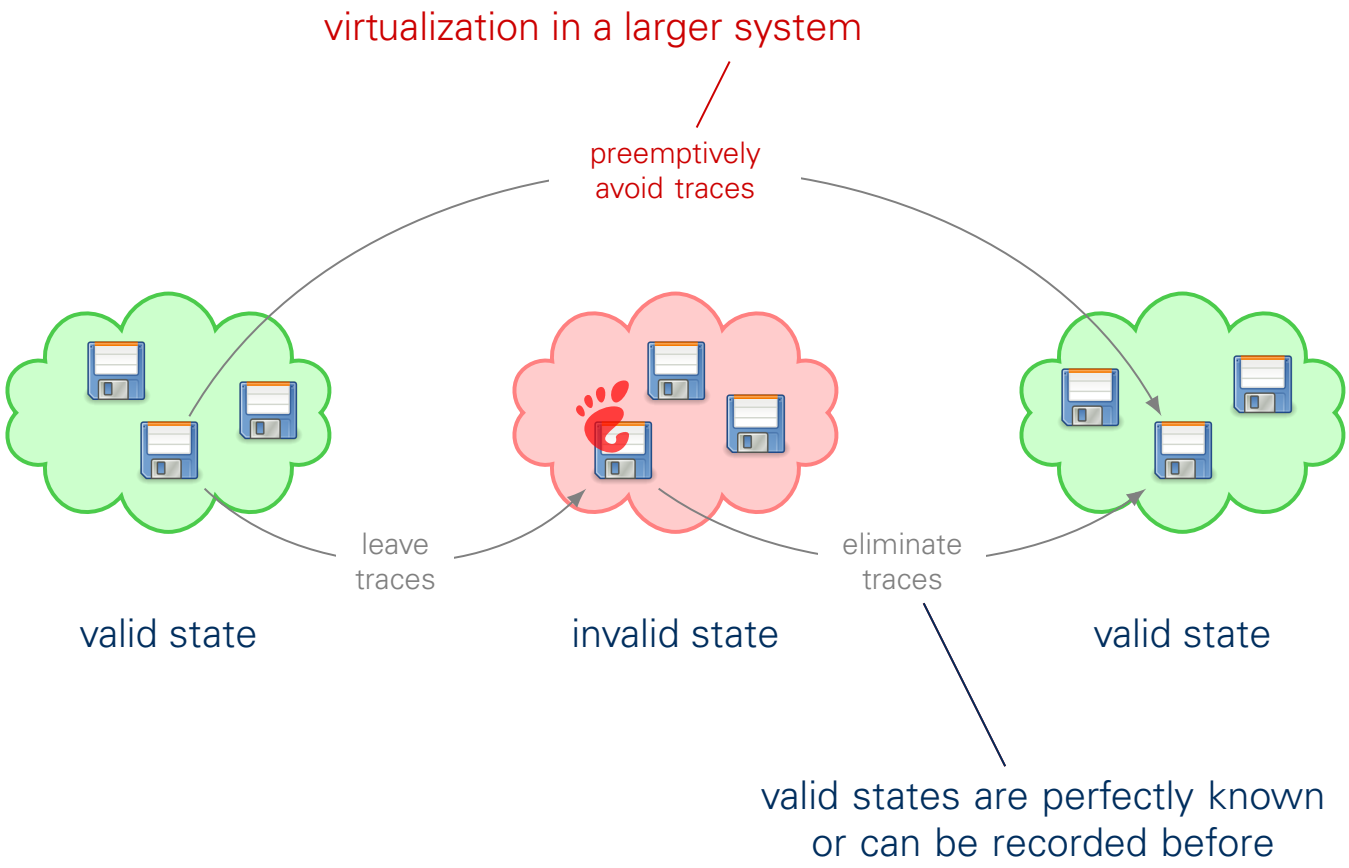
Counter-forensics: Computer forensics



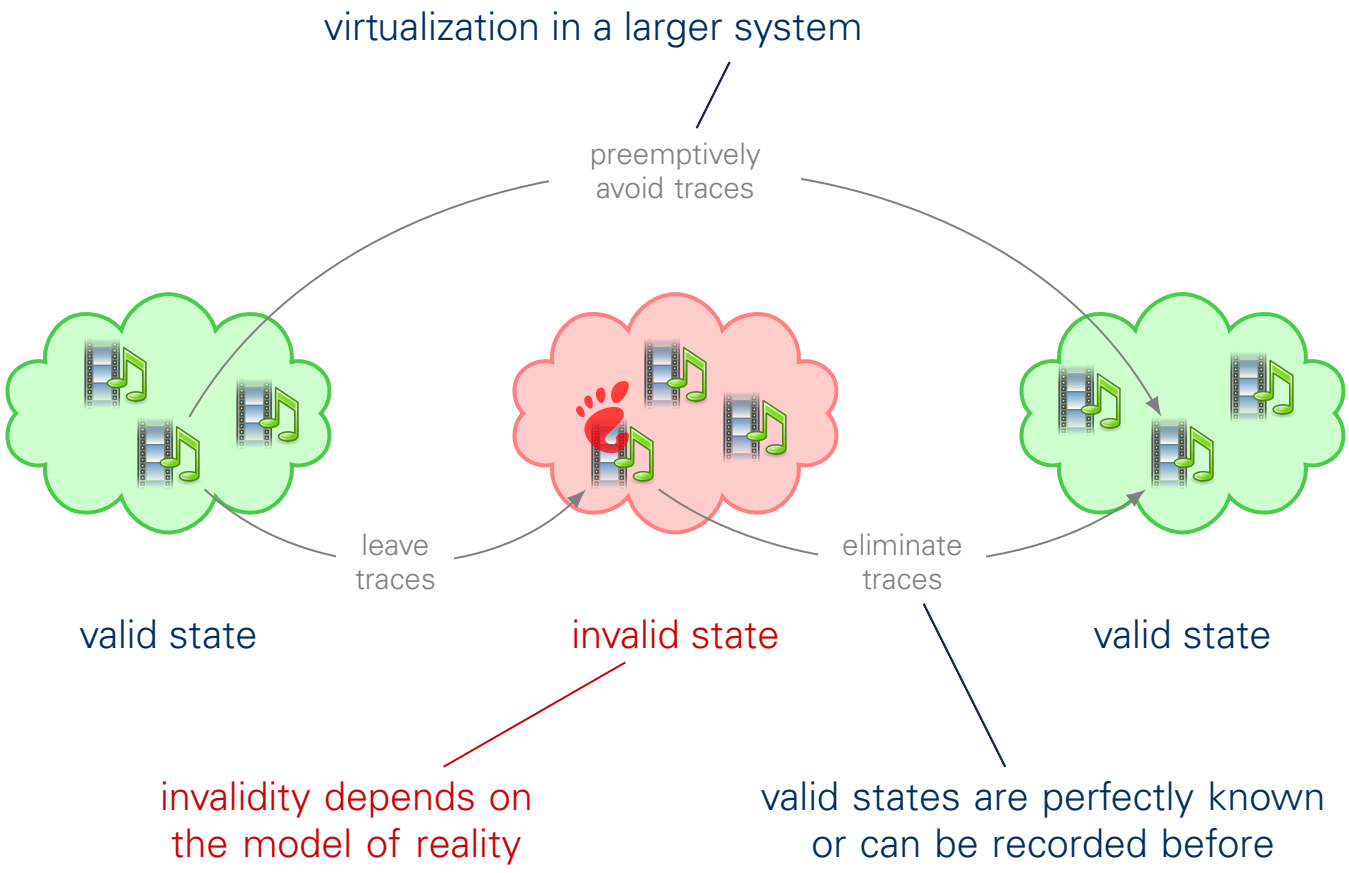
Counter-forensics: Computer forensics



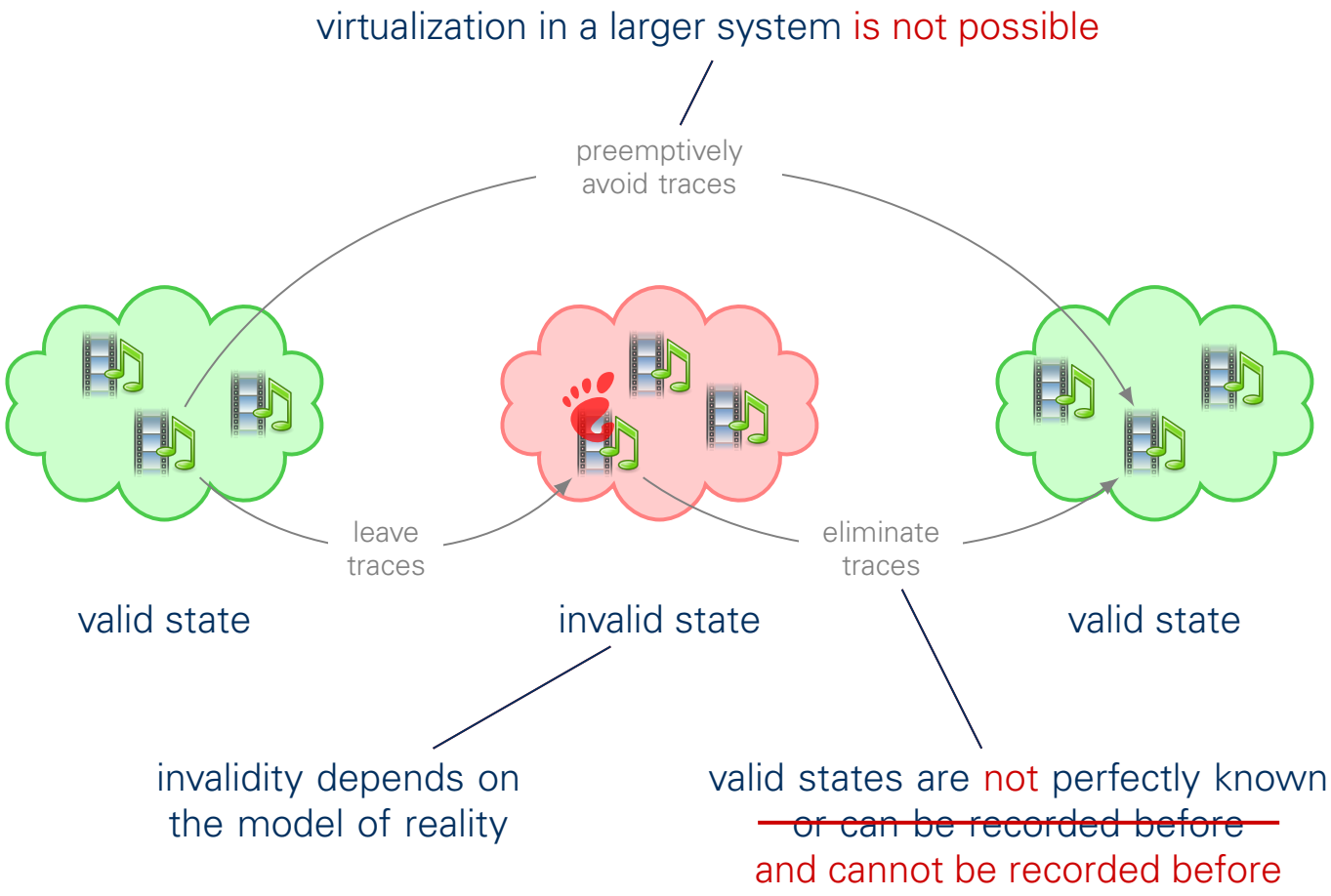
Counter-forensics: Computer forensics



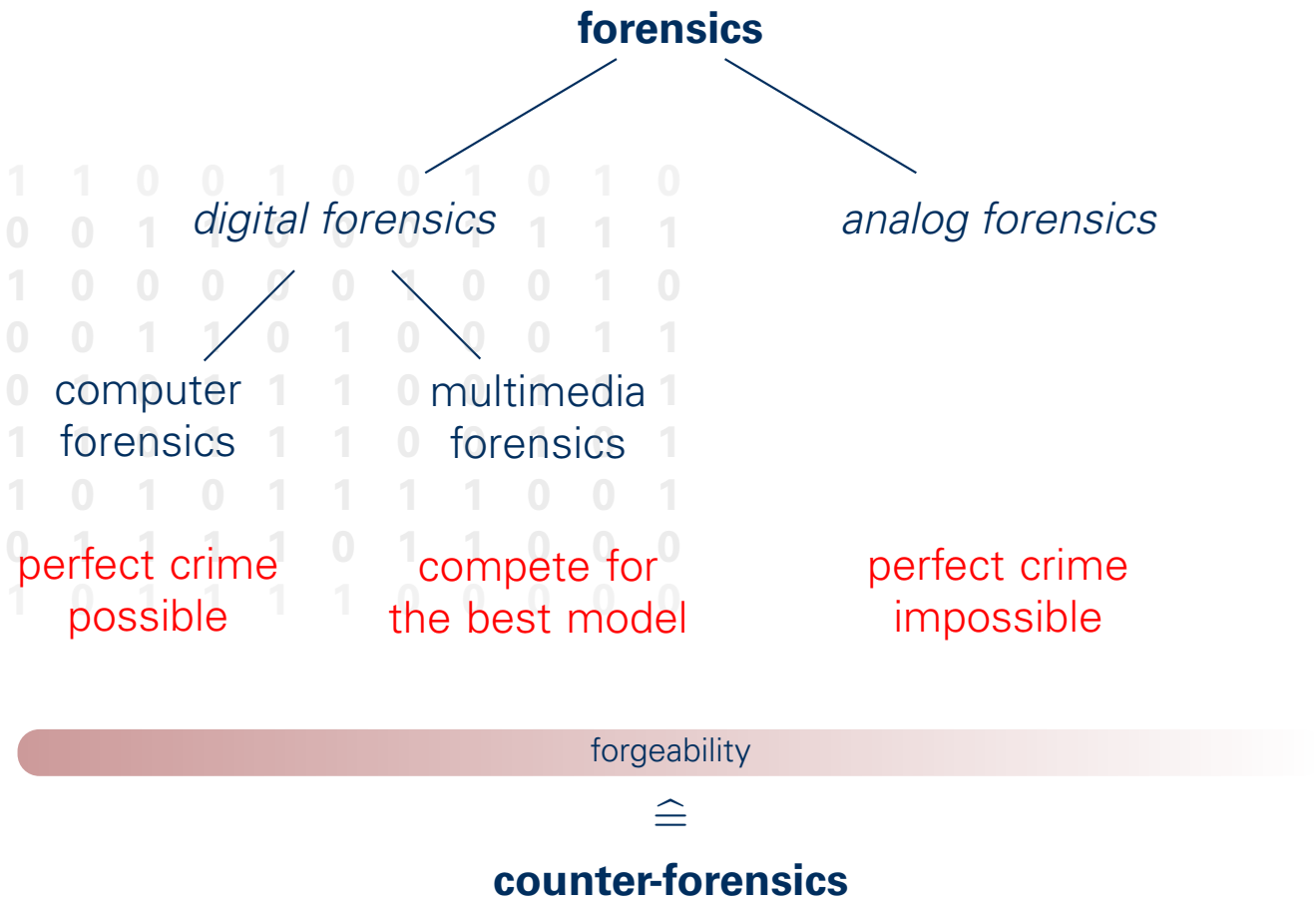
Counter-forensics: Multimedia forensics



Counter-forensics: Multimedia forensics



Digital forensics: proposed ontology

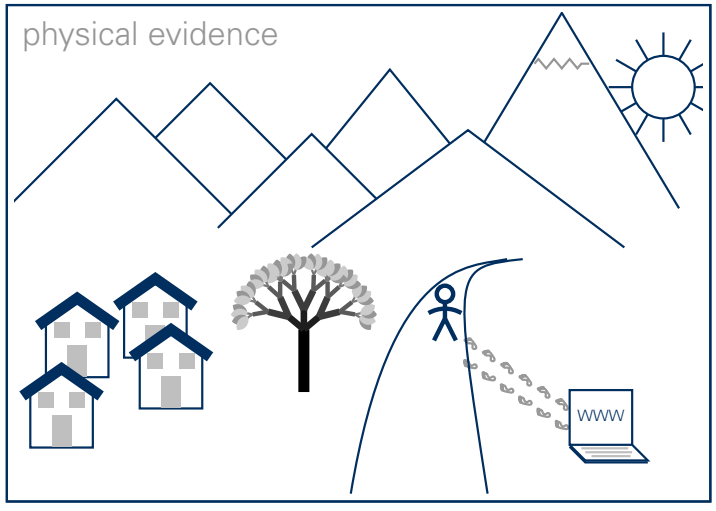


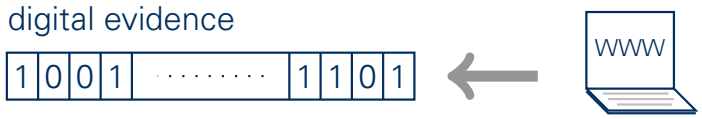
Outline

1. Multimedia forensics and computer forensics
2. Multimedia forensics is not computer forensics
3. Counter-forensics
4. **And how does this all relate to practice?**

Computer forensics in a broader sense

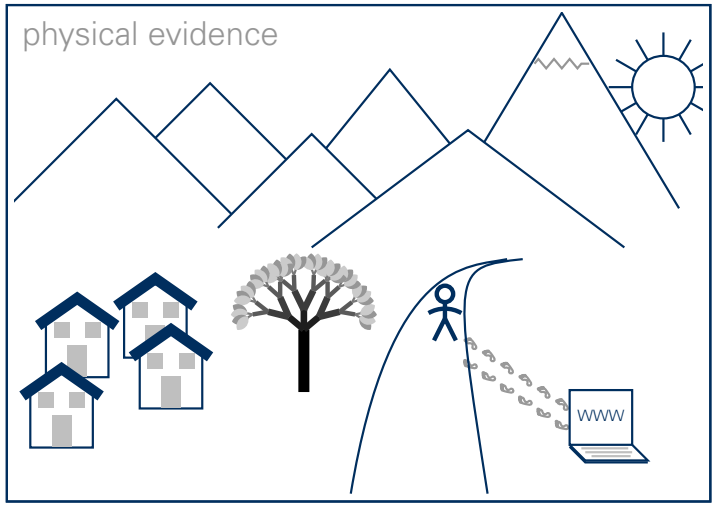
- computers interact with their environment



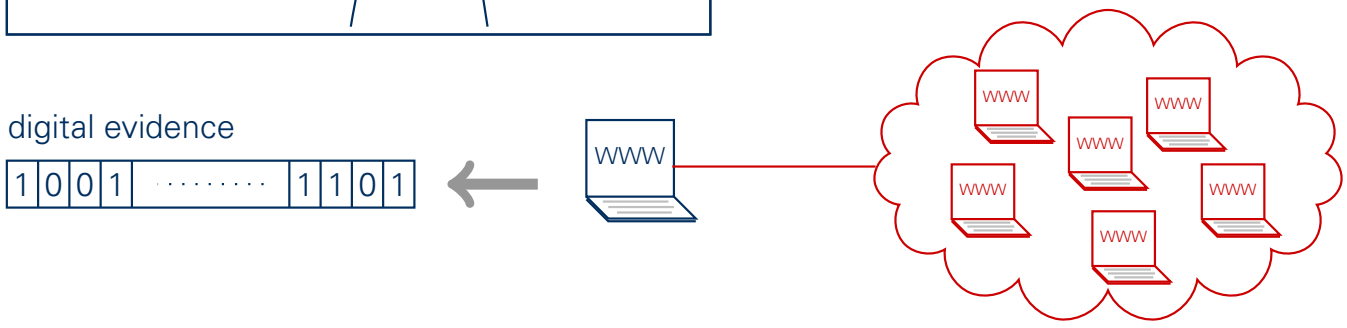


Computer forensics in a broader sense

- computers interact with their environment

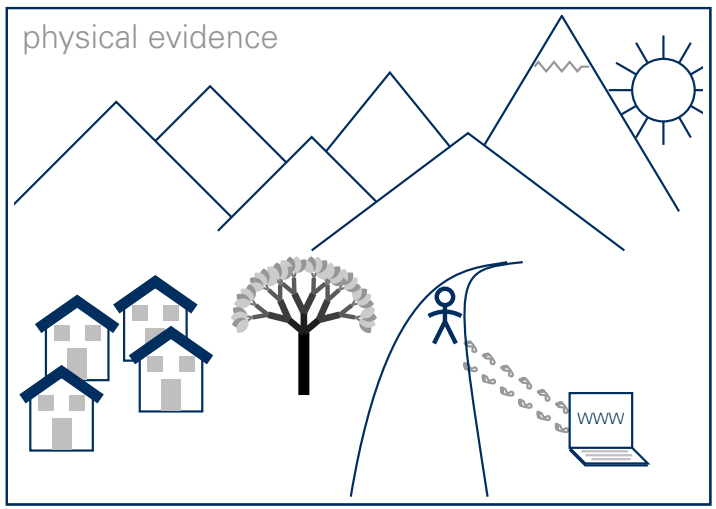


- computers can be part of a network

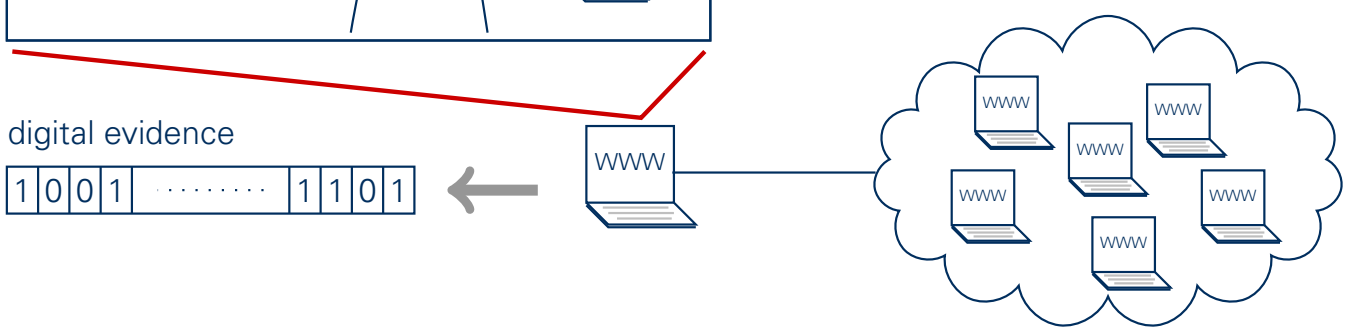


Computer forensics in a broader sense

- computers interact with their environment

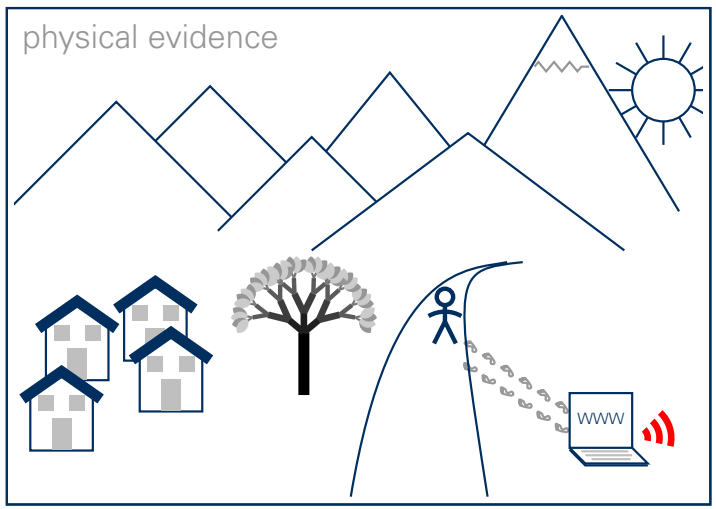


- computers can be part of a network
- computers can be sensors itself

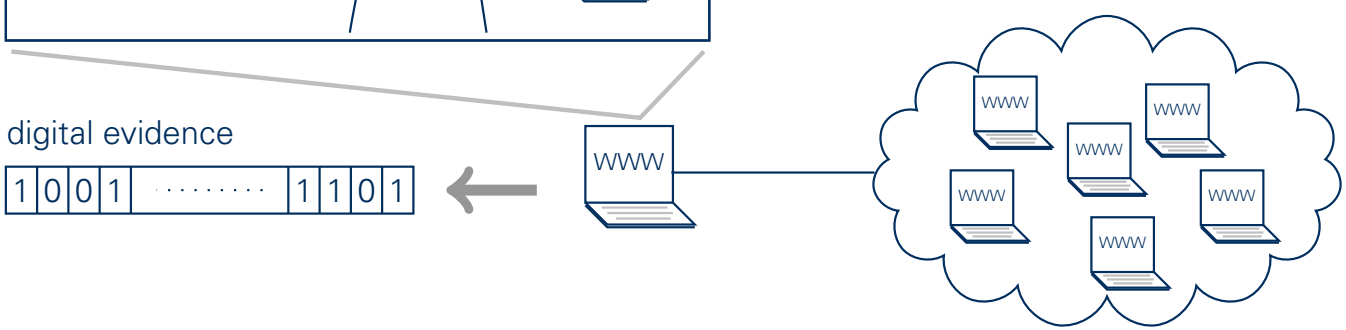


Computer forensics in a broader sense

- computers interact with their environment



- computers can be part of a network
- computers can be sensors itself
- computers leave physical evidence



(Finally) A more practical view

Concluding remarks

- forensic examinations include techniques from a variety of forensic sciences
- important differences in the underlying assumptions between different methods are blurred by practice
- **in particular:** digital evidence $\neq$ digital evidence ($\neq$ physical evidence):
  - digital evidence in computer forensics is not linked to the outside world whereas in multimedia forensics it is
  - effects the reliability of forensic methods

- **furture work:** rigorous probabilistic modeling

Concluding remarks

- forensic examinations include techniques from a variety of forensic sciences
- important differences in the underlying assumptions between different methods are blurred by practice
- **in particular:** digital evidence $\neq$ digital evidence ($\neq$ physical evidence):
  - digital evidence in computer forensics is not linked to the outside world whereas in multimedia forensics it is
  - effects the reliability of forensic methods

- **furture work:** rigorous probabilistic modeling

reality is ultimately incognizable, but

Concluding remarks

- forensic examinations include techniques from a variety of forensic sciences
- important differences in the underlying assumptions between different methods are blurred by practice
- **in particular:** digital evidence ≠ digital evidence (≠ physical evidence):
  - digital evidence in computer forensics is not linked to the outside world whereas in multimedia forensics it is
  - effects the reliability of forensic methods

- **furture work:** rigorous probabilistic modeling

reality is ultimately incognizable, but
your comments will help to gain a more comprehensive view on it

TECHNISCHE UNIVERSITÄT DRESDEN

UNIVERSITÄT MANNHEIM

Thanks for your attention

Questions?

Rainer Böhme[†], Felix Freiling[‡], Thomas Gloe[†], Matthias Kirchner[†]

[†] Technische Universität Dresden [‡] Universität Mannheim

Matthias Kirchner gratefully receives a doctorate scholarship from Deutsche Telekom Stiftung, Bonn, Germany.

Image sources

- Iranian missile test (4) http://www.spiegel.de
- hard drive (6) http://commons.wikimedia.org/wiki/File:Open_hard-drive.jpg
- floppy disk (11,17) http://commons.wikimedia.org/wiki/GNOME_Desktop_icons
- core memory (11) http://commons.wikimedia.org/wiki/File:KL_CoreMemory.jpg
- multimedia (12,18) http://commons.wikimedia.org/wiki/GNOME_Desktop_icons
- fingerprints (22) http://www.lanl.gov/news/albums/chemistry/fingerprint.jpg
- handcuffs (22) http://commons.wikimedia.org/wiki/File:Handcuffs01_2003-06-02.jpg