TECHNISCHE UNIVERSITÄT DRESDEN

UNIVERSITÄT MANNHEIM

ICSI INTERNATIONAL COMPUTER SCIENCE INSTITUTE

Multimedia-Forensik als Teildisziplin der digitalen Forensik

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

[†] Technische Universität Dresden [‡] Universität Mannheim [*] ICSI Berkeley

39. GI Jahrestagung Informatik — Digitale Multimedia-Forensik

Lübeck · 28. September 2009

Gliederung

Multimedia-Forensik

Wissenschaft zur Feststellung der Authentizität von digitalen Mediendaten

Ziele: **Entdeckung von Manipulationen** und **Rückschlüsse auf das Eingabegerät**

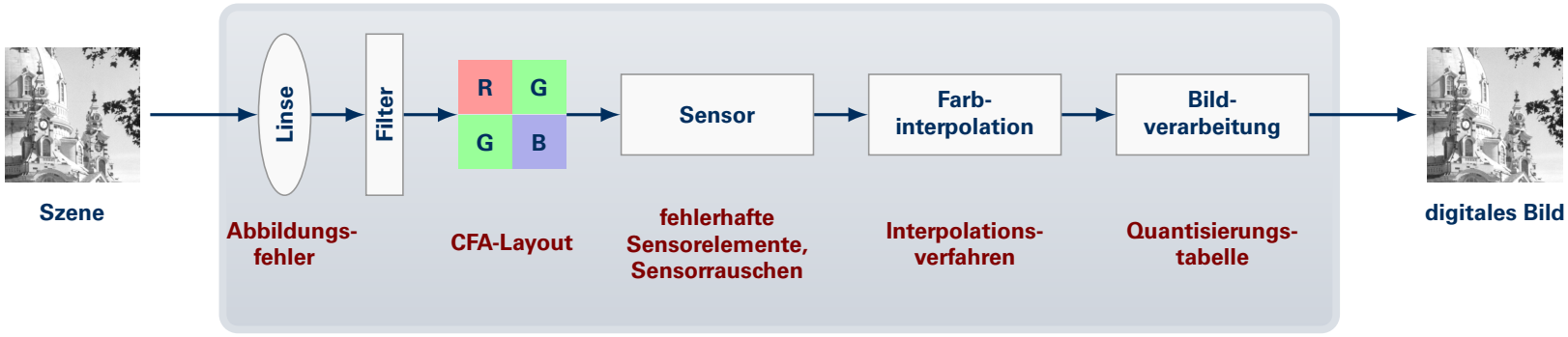
Analyseansätze:

- *Manipulationsartefakte*

  Resampling · Copy & Paste · Inkonsistenzen der Beleuchtung · Mehrfachkompression

- *Charakteristiken des Eingabegeräts*

  z. B. Digitalkamera:



Beispiele für Multimedia-Forensik

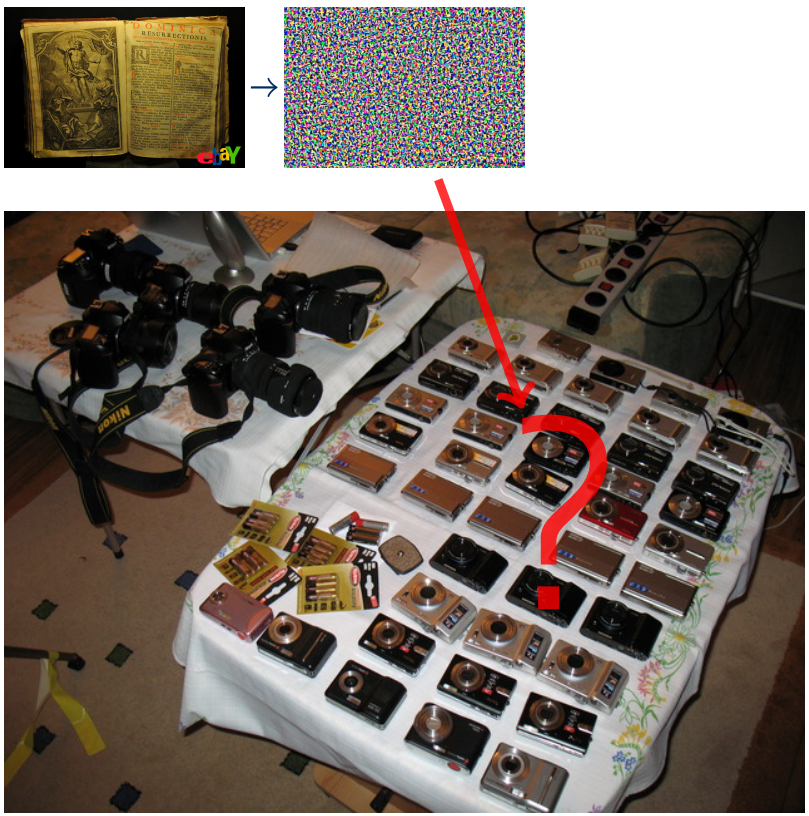
- Identifikation einer Digitalkamera anhand von Sensorrauschen

Beispiele für Multimedia-Forensik

- Identifikation einer Digitalkamera anhand von Sensorrauschen

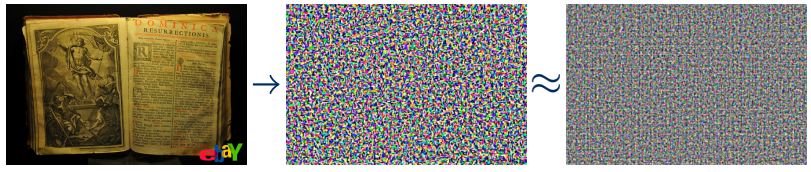
Beispiele für Multimedia-Forensik

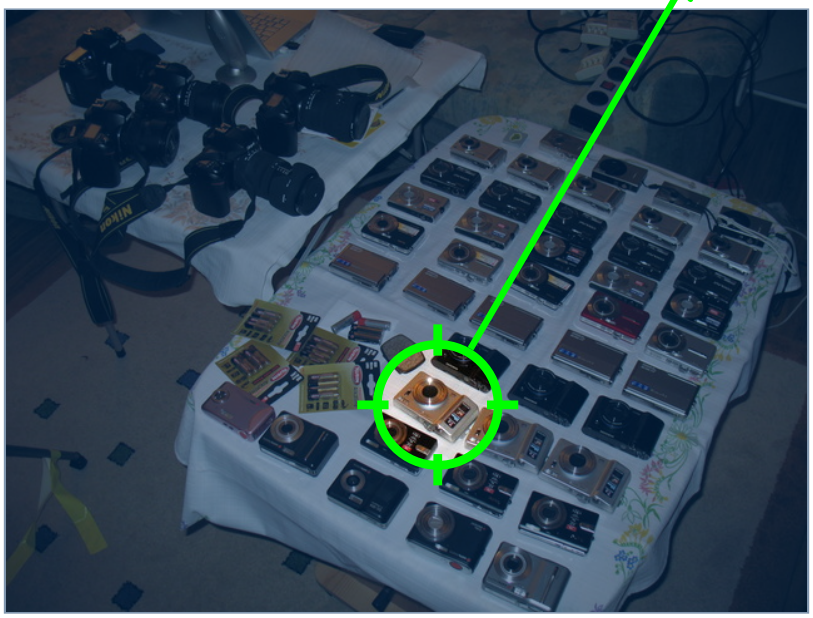
- Identifikation einer Digitalkamera anhand von Sensorrauschen



Beispiele für Multimedia-Forensik

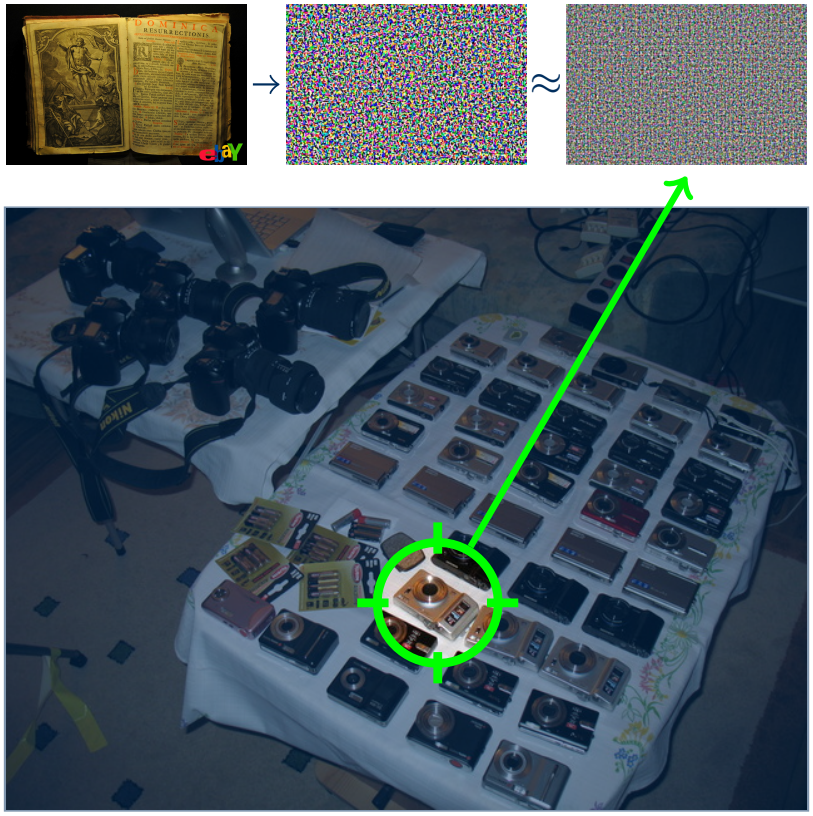
- Identifikation einer Digitalkamera anhand von Sensorrauschen





Beispiele für Multimedia-Forensik

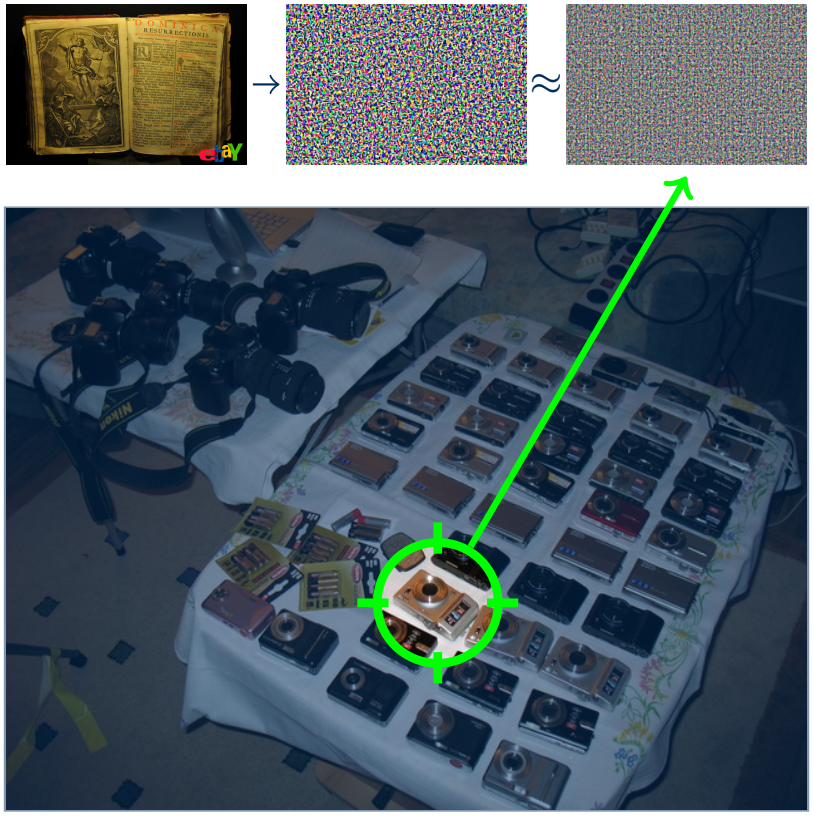
- Identifikation einer Digitalkamera anhand von Sensorrauschen



- Copy & Paste-Detektor

Beispiele für Multimedia-Forensik

- Identifikation einer Digitalkamera anhand von Sensorrauschen



- Copy & Paste-Detektor

mutmaßliches Original

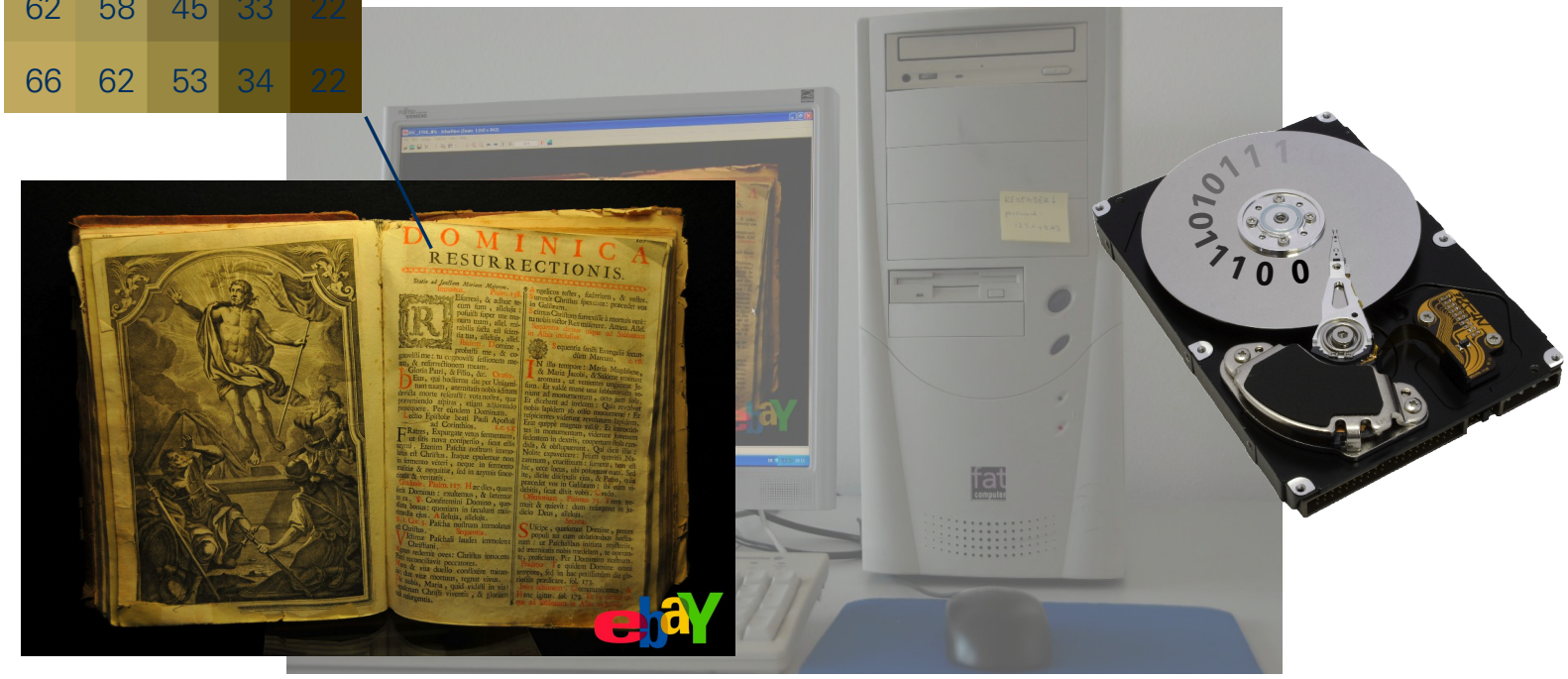
Was ist eigentlich *Computer-Forensik* ?

Computer-Forensik

Computer-Forensik

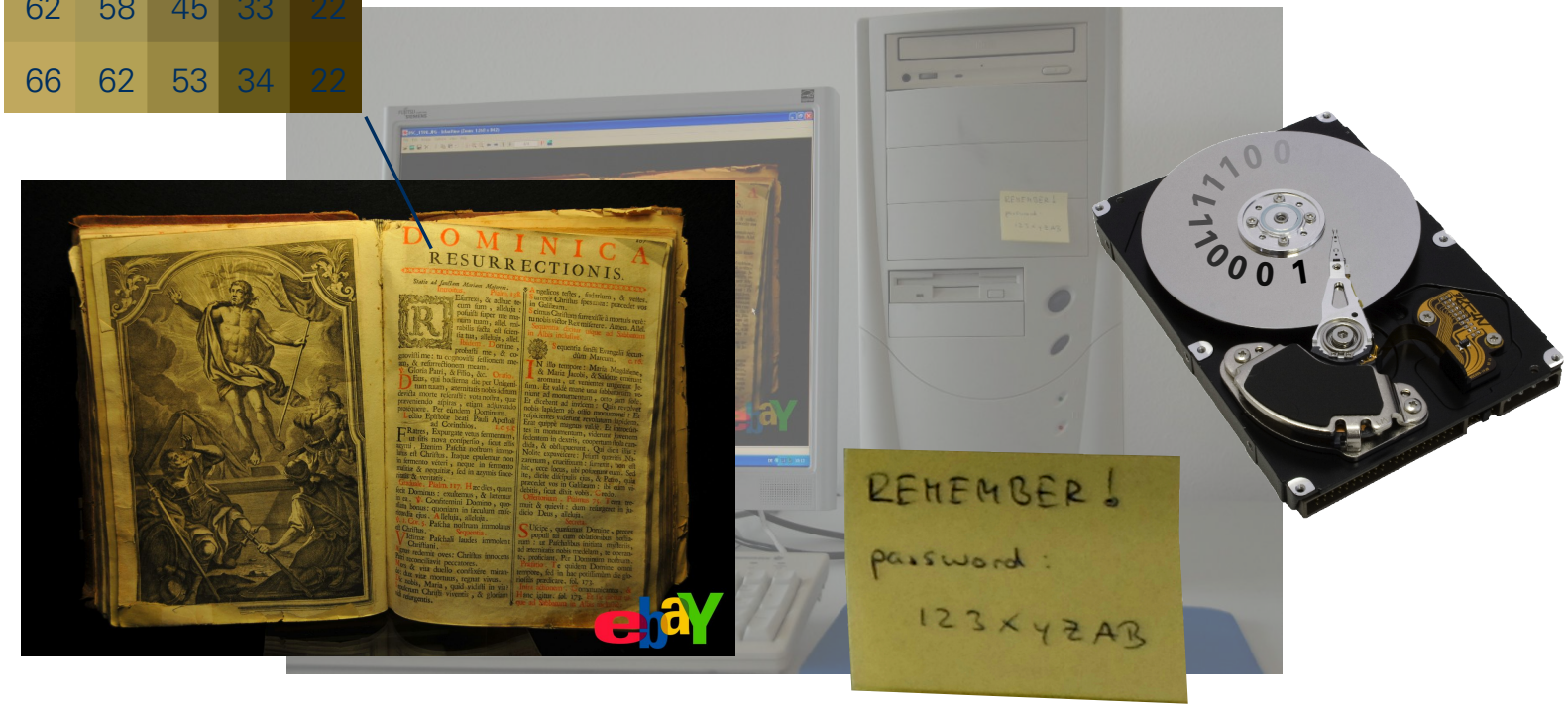
Computer-Forensik

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



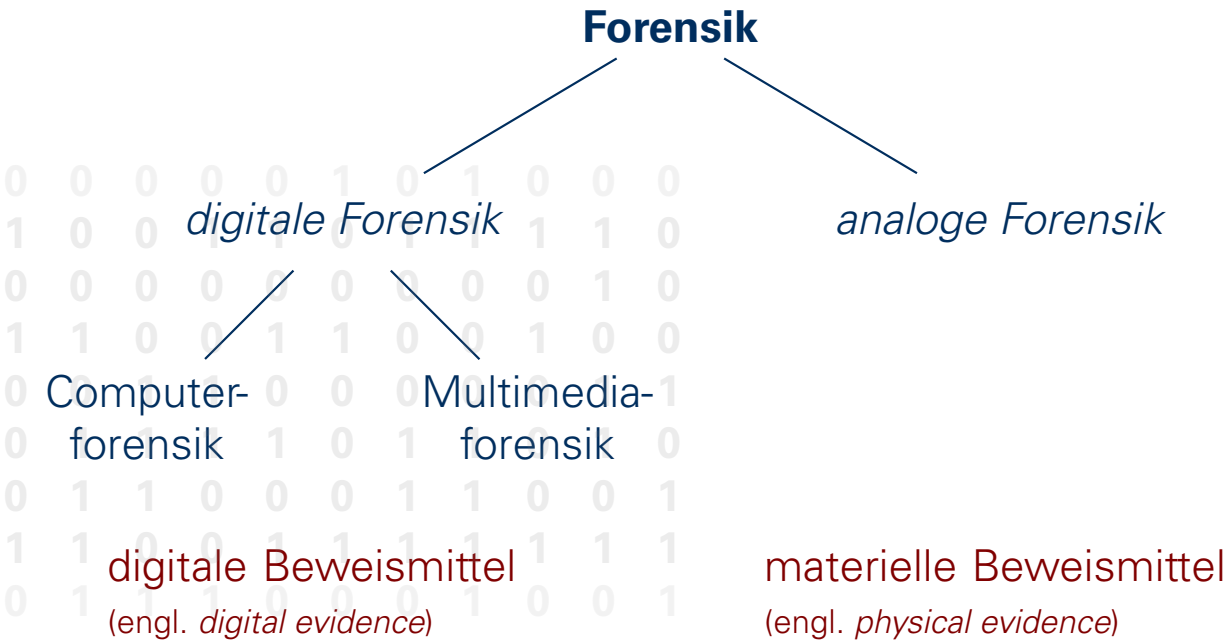
Computer-Forensik

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

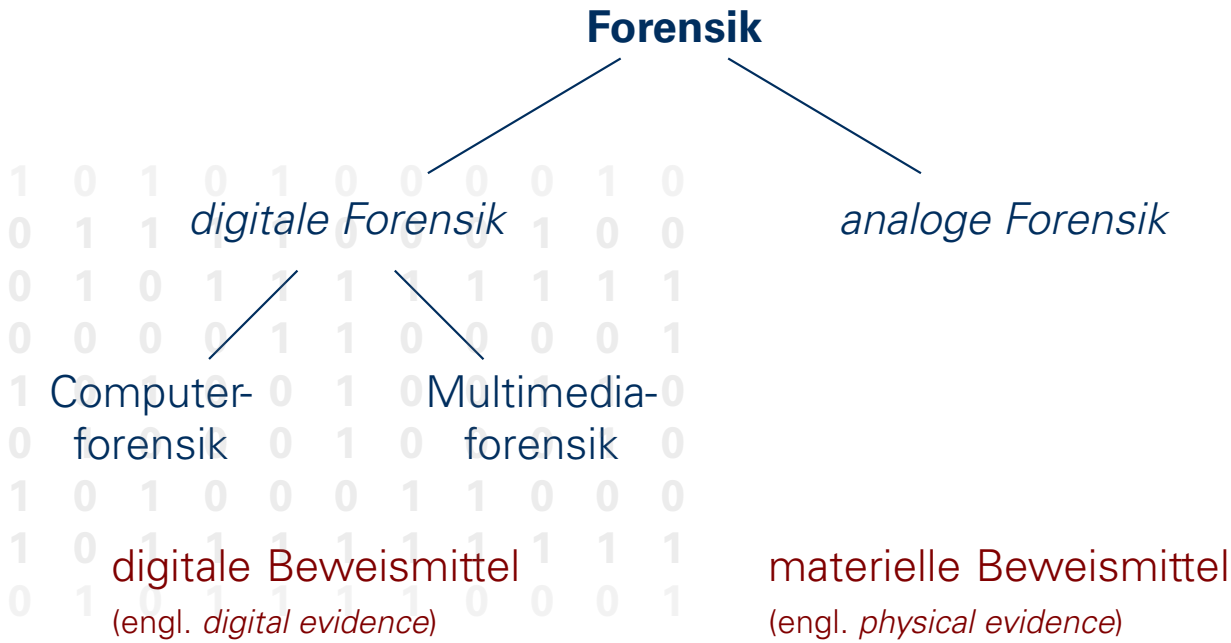


Gliederung

Strukturierungsvorschlag für digitale Forensik



Strukturierungsvorschlag für digitale Forensik

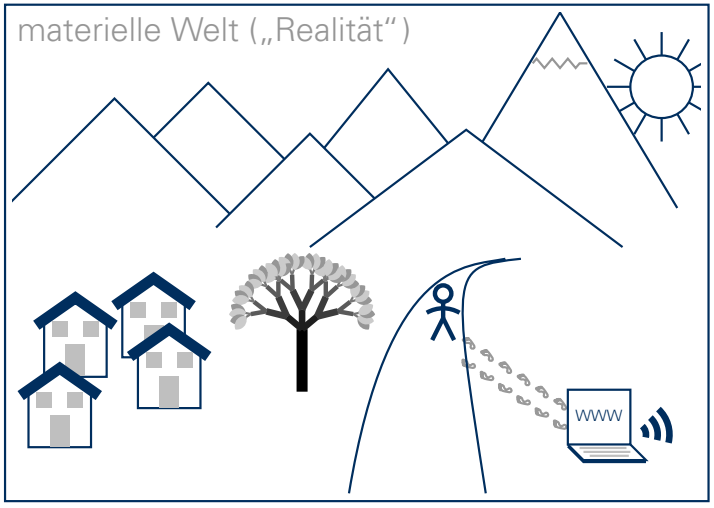


ACHTUNG

Die folgenden Argumente zeichnen bewusst ein Schwarz-Weiß-Bild

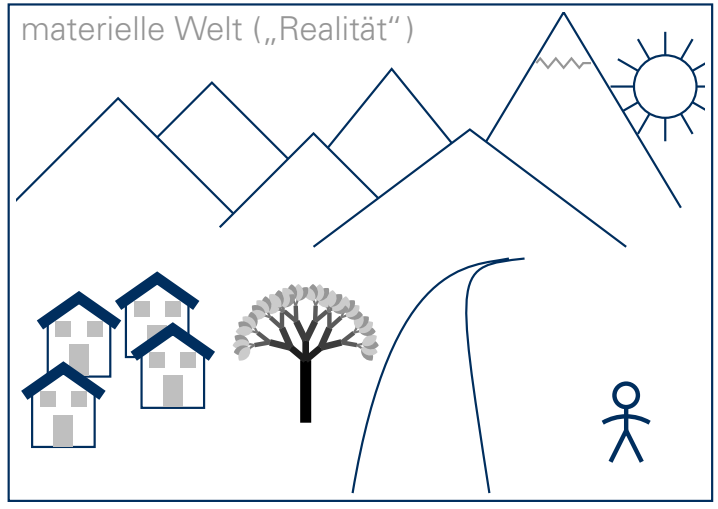
Computer-Forensik ≠ Multimedia-Forensik

Computer-Forensik



digitale Beweismittel

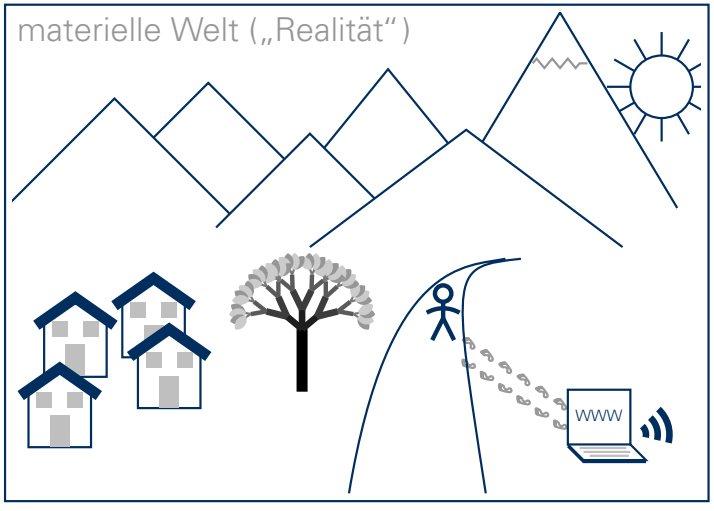
Multimedia-Forensik

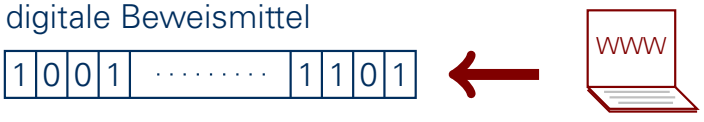


digitale Beweismittel

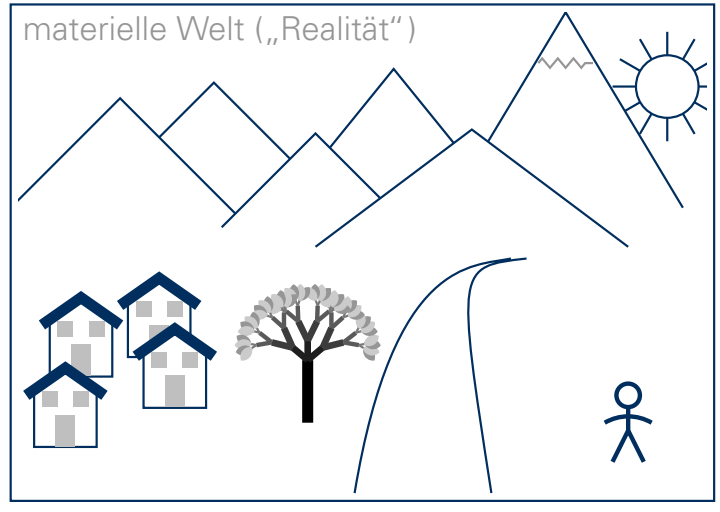
Computer-Forensik ≠ Multimedia-Forensik

Computer-Forensik



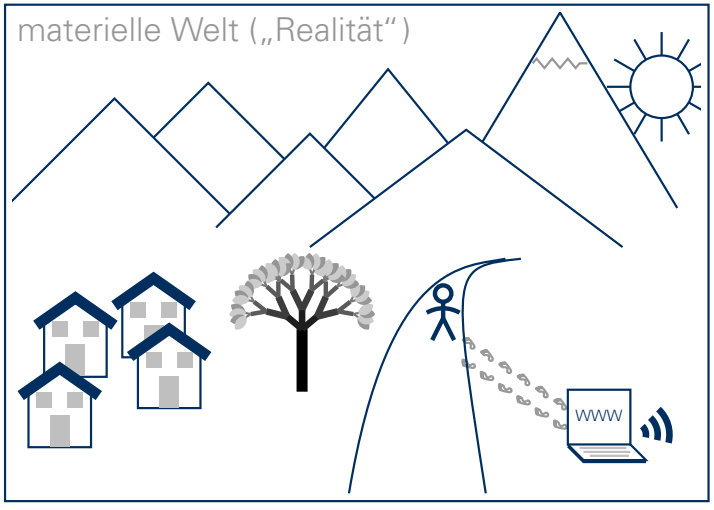


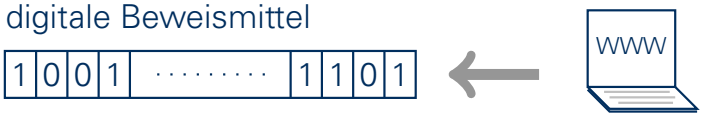
Multimedia-Forensik



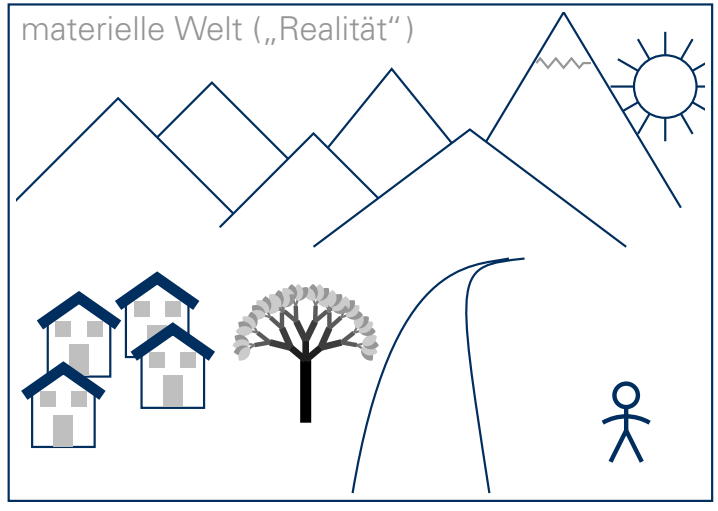
Computer-Forensik ≠ Multimedia-Forensik

Computer-Forensik





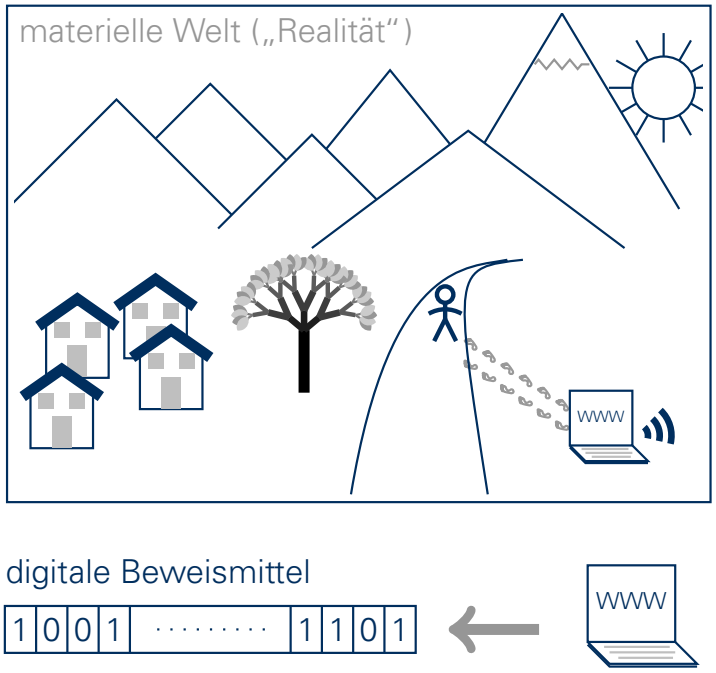
Multimedia-Forensik



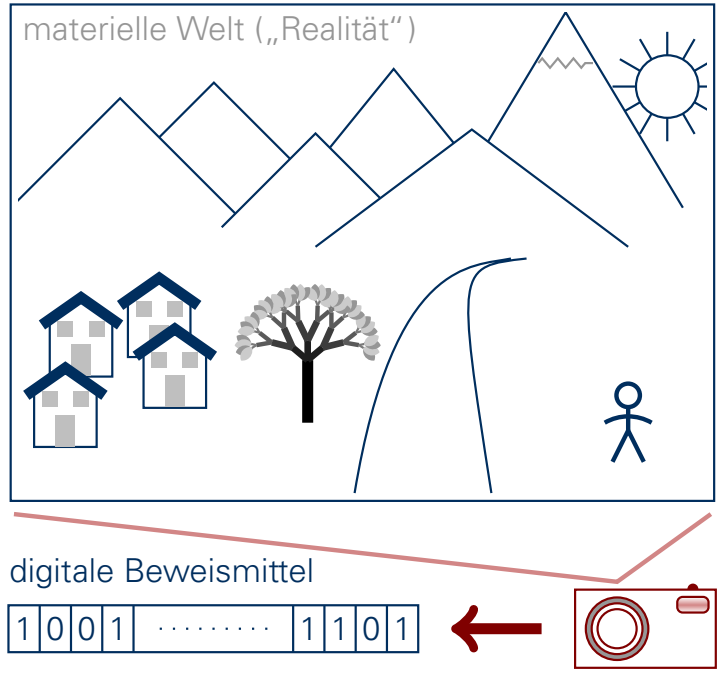
- Digitale Beweismittel **sind isoliert** von der materiellen Welt.

Computer-Forensik ≠ Multimedia-Forensik

Computer-Forensik



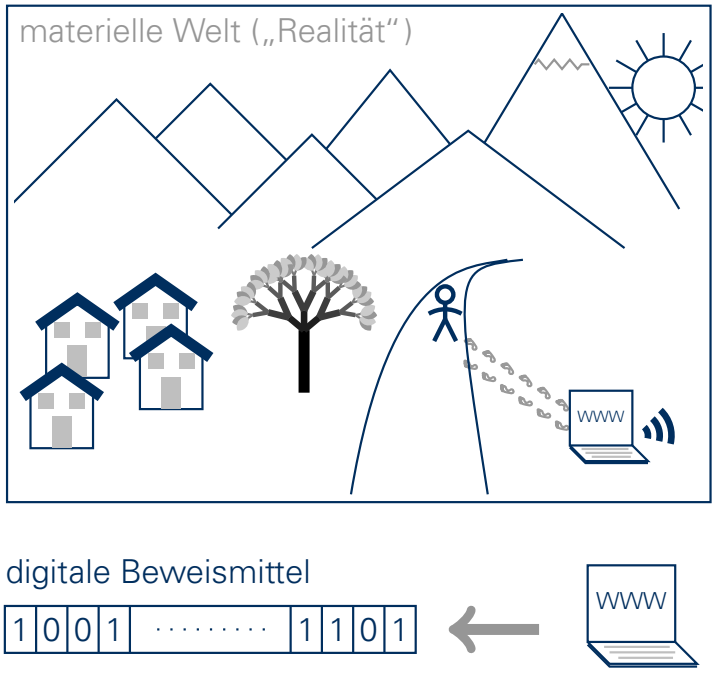
Multimedia-Forensik



- Digitale Beweismittel **sind isoliert** von der materiellen Welt.

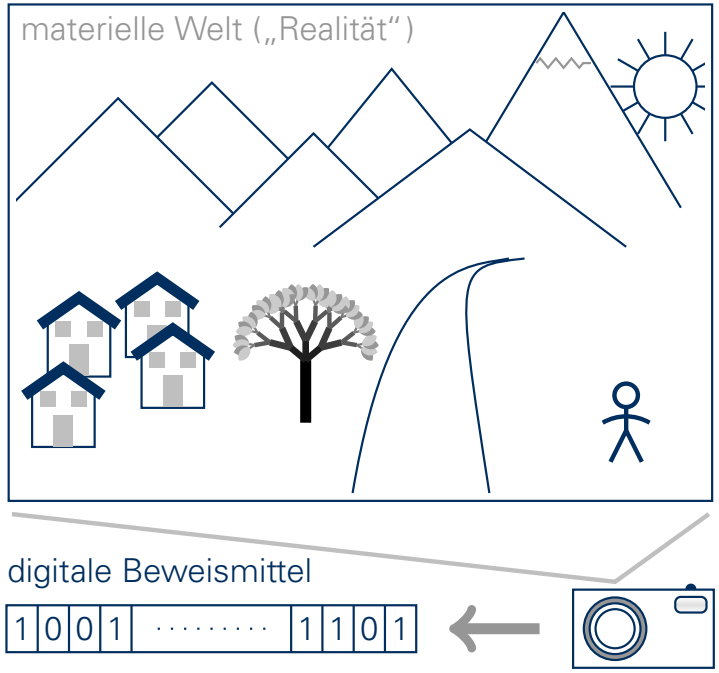
Computer-Forensik ≠ Multimedia-Forensik

Computer-Forensik



- Digitale Beweismittel **sind isoliert** von der materiellen Welt.

Multimedia-Forensik



- Digitale Beweismittel **stehen im Bezug** zur materiellen Welt.

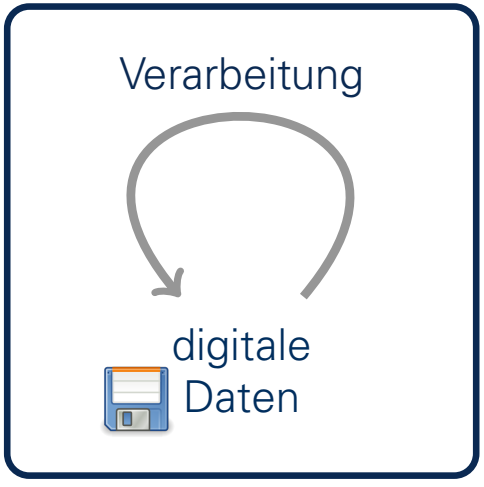
Besonderheiten der Computer-Forensik

Besonderheiten der Computer-Forensik

verdächtige Spuren?

Besonderheiten der Computer-Forensik

verdächtige Spuren?

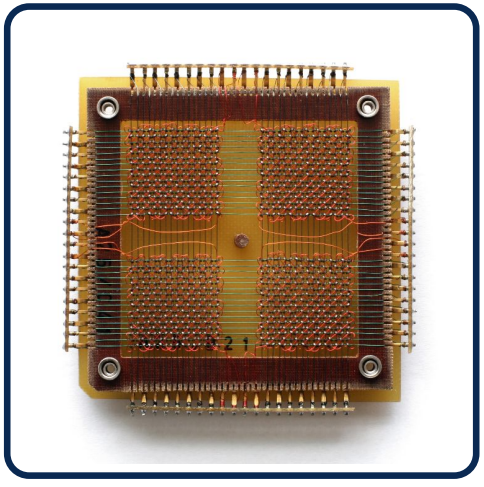


Realität

- Digitale Beweismittel ergeben sich aus dem Zustand eines Automaten.
- Die Anzahl möglicher Zustände in einem geschlossenen System ist endlich.

Besonderheiten der Computer-Forensik

verdächtige Spuren?

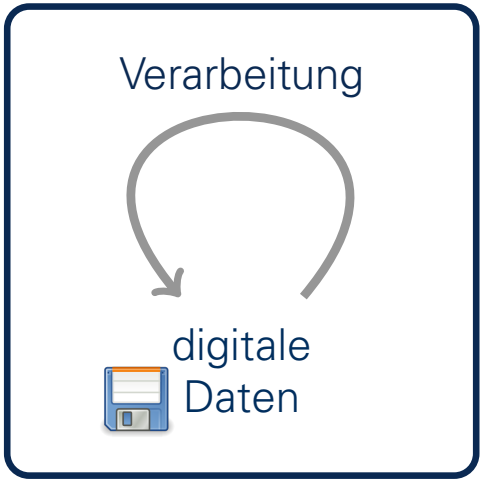


Realität

- Digitale Beweismittel ergeben sich aus dem Zustand eines Automaten.
- Die Anzahl möglicher Zustände in einem geschlossenen System ist endlich.

Besonderheiten der Computer-Forensik

verdächtige Spuren?



Realität

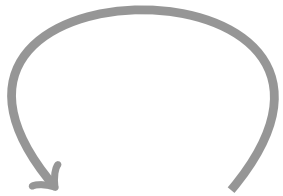
- Digitale Beweismittel ergeben sich aus dem Zustand eines Automaten.
- Die Anzahl möglicher Zustände in einem geschlossenen System ist endlich.
- Realistische Chance, den Computer gezielt in einen Zustand zu versetzen, der alle Spuren perfekt verwischt.

Besonderheiten der Multimedia-Forensik

Besonderheiten der Multimedia-Forensik

Original?

Verarbeitung



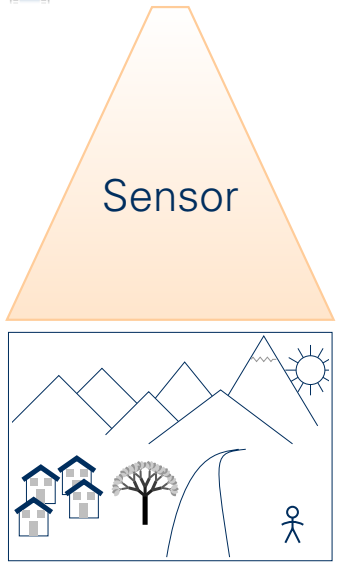
digitales Medien-objekt

Herkunft?

Besonderheiten der Multimedia-Forensik

Original?

Herkunft?

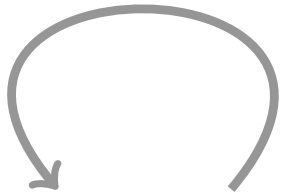


- Sensoren bilden Teile der Realität in digitalen Repräsentationen ab.

Besonderheiten der Multimedia-Forensik

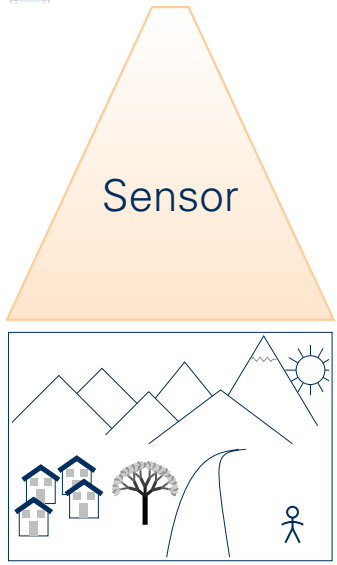
Original?

Verarbeitung



digitales Medien-objekt

Herkunft?

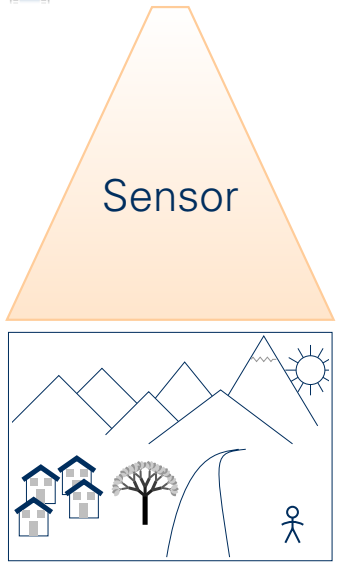


- Sensoren bilden Teile der Realität in digitalen Repräsentationen ab.
- Die Realität ist nicht endgültig erkennbar: Es ist nicht mit Sicherheit entscheidbar, ob eine digitale Repräsentation der Realität entspricht (d. h. „wahr“ ist) oder nicht.

Besonderheiten der Multimedia-Forensik

Original?

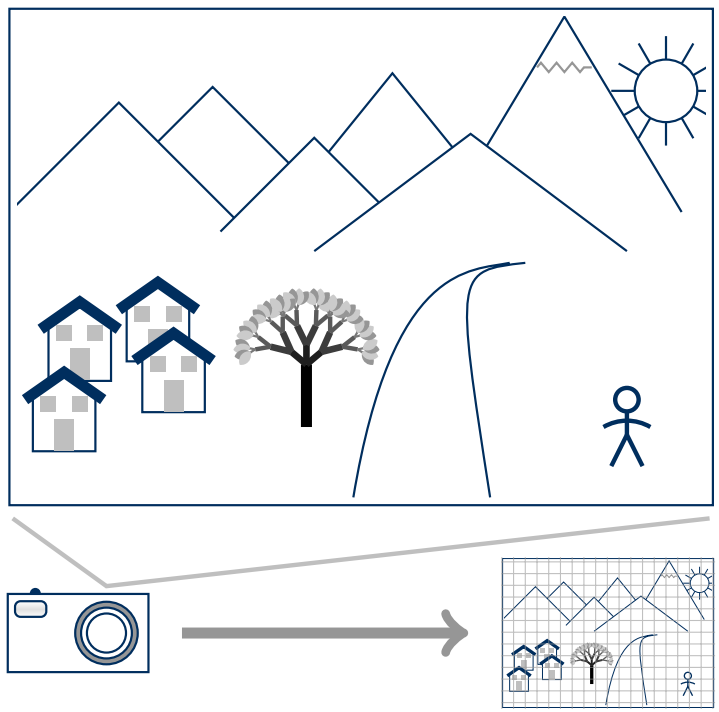
Herkunft?



- Sensoren bilden Teile der Realität in digitalen Repräsentationen ab.
- Die Realität ist nicht endgültig erkennbar: Es ist nicht mit Sicherheit entscheidbar, ob eine digitale Repräsentation der Realität entspricht (d. h. „wahr“ ist) oder nicht.
- Multimedia-Forensik ist also eine empirische Wissenschaft.

Sensor als Quelle von Unsicherheit

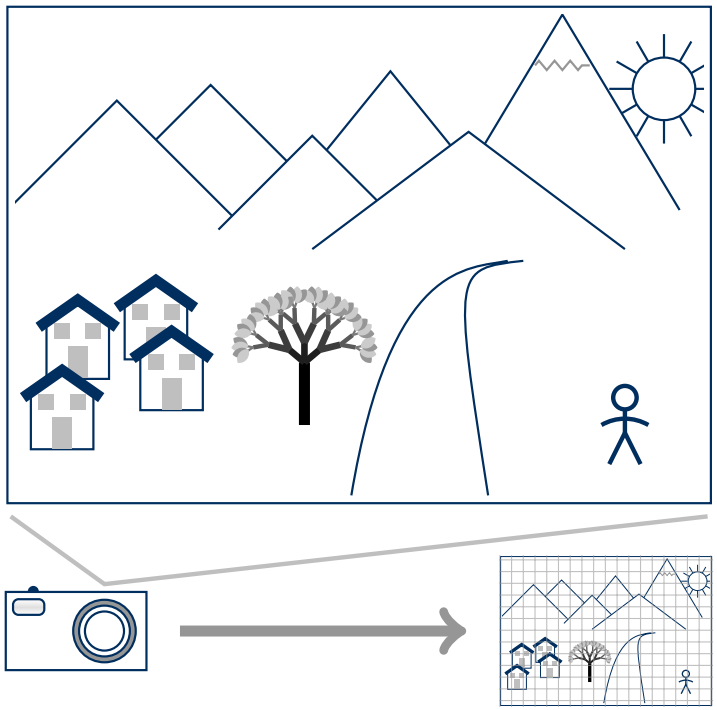
- Dimensionsreduktion durch Projektion der Realität auf diskrete Symbole



Sensor als Quelle von Unsicherheit

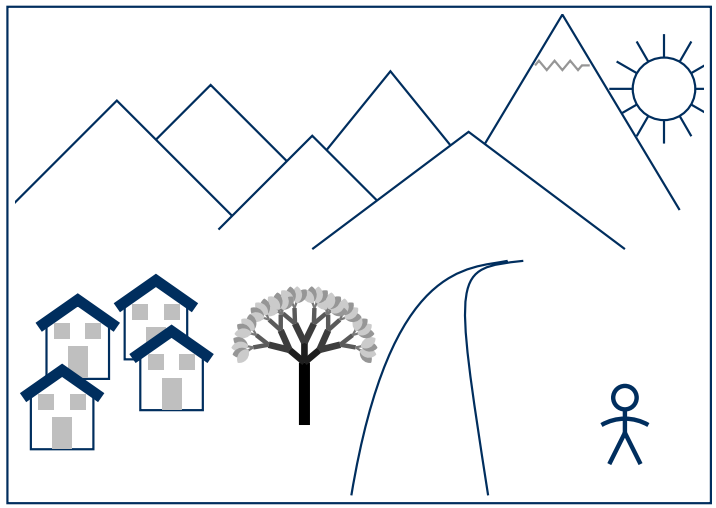
Freiheitsgrade

- Dimensionsreduktion durch Projektion der Realität auf diskrete Symbole
- Unsicherheitsquelle schränkt Aussagekraft der Multimedia-Forensik ein
  (im Gegensatz zur Computer-Forensik).

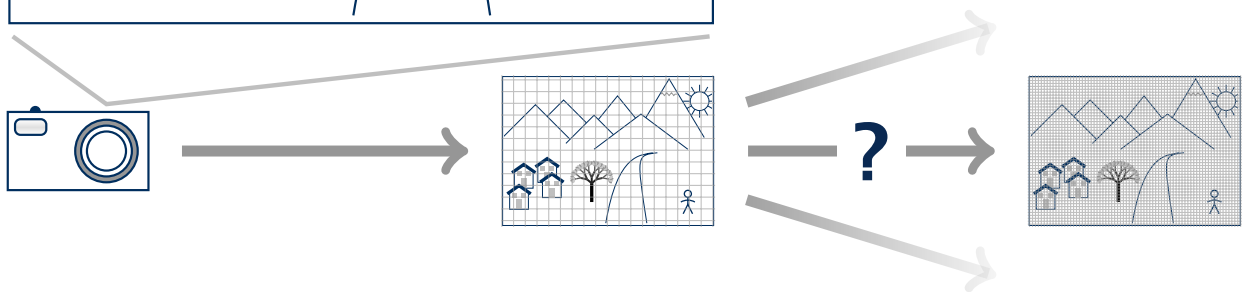


Sensor als Quelle von Unsicherheit

- Dimensionsreduktion durch Projektion der Realität auf diskrete Symbole
- Unsicherheitsquelle schränkt Aussagekraft der Multimedia-Forensik ein
  (im Gegensatz zur Computer-Forensik).



- zusätzliche Unsicherheit durch standardmäßige oder „zulässige“ Nachbearbeitung

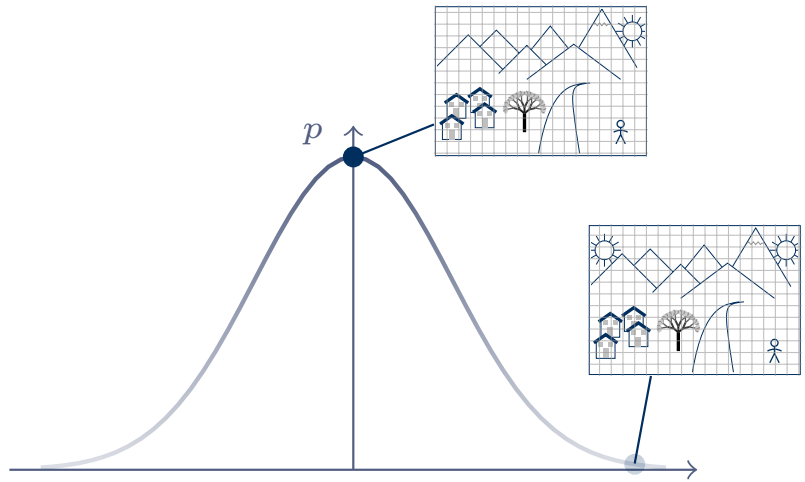


Weitere Dimensionsreduktion durch Modelle

- **Modelle** helfen, digitalisierte Abbilder der Realität formal zu fassen.
- Typische Modellannahmen:
  - Sensorrauschen folgt einer Normalverteilung;
  - zusammenhängende Regionen identischer Pixel treten in Originalbildern nicht auf.

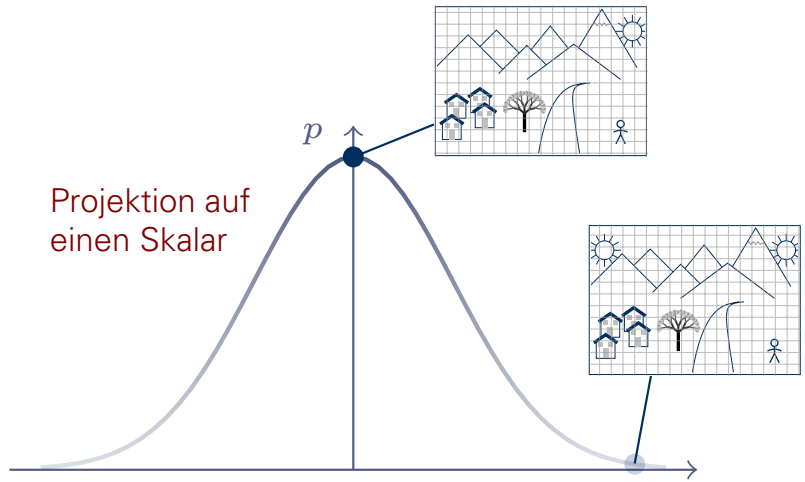
Weitere Dimensionsreduktion durch Modelle

- **Modelle** helfen, digitalisierte Abbilder der Realität formal zu fassen.
- Typische Modellannahmen:
  - Sensorrauschen folgt einer Normalverteilung;
  - zusammenhängende Regionen identischer Pixel treten in Originalbildern nicht auf.



Weitere Dimensionsreduktion durch Modelle

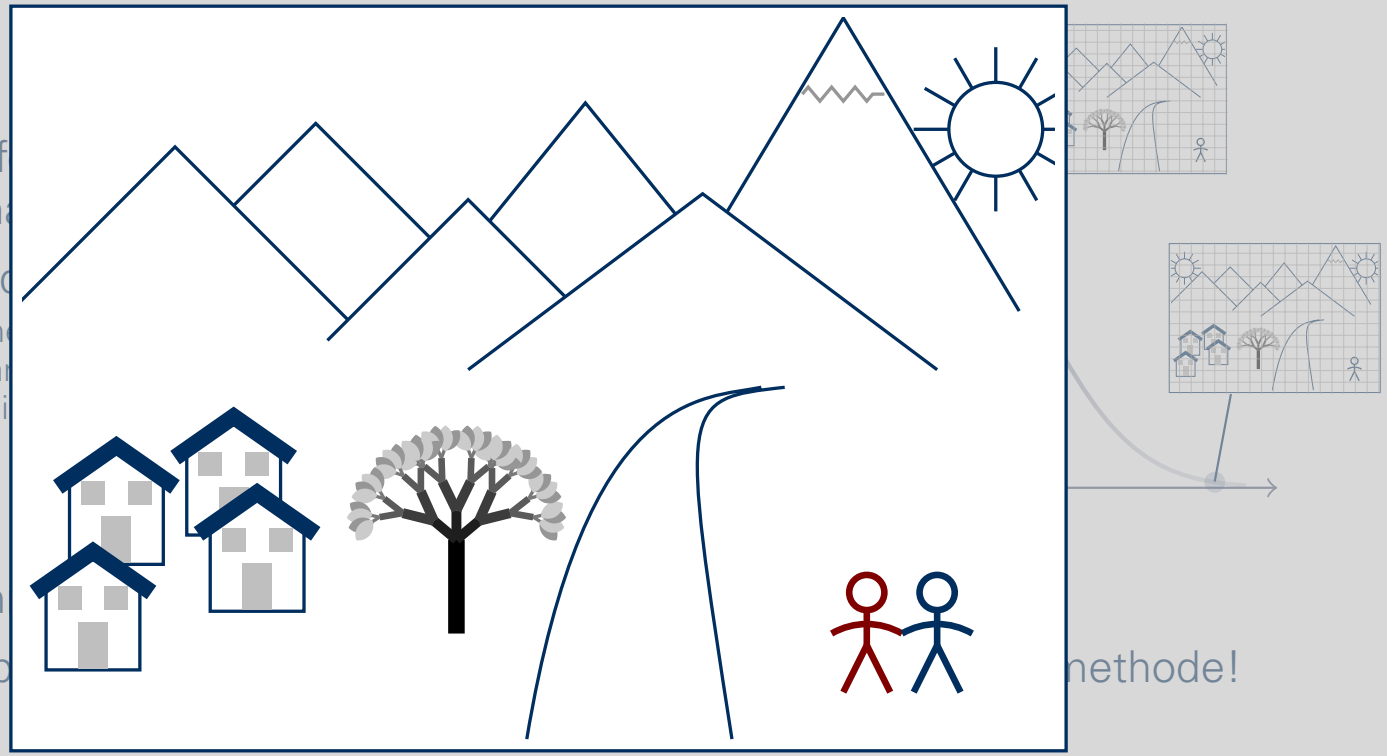
- **Modelle** helfen, digitalisierte Abbilder der Realität formal zu fassen.
- Typische Modellannahmen:
  - Sensorrauschen folgt einer Normalverteilung;
  - zusammenhängende Regionen identischer Pixel treten in Originalbildern nicht auf.



- Modellannahmen implizieren weitere Dimensionalitätsreduktion.
- Modellgüte bestimmt die Aussagekraft jeder forensischen Analysemethode!

Weitere Dimensionsreduktion durch Modelle

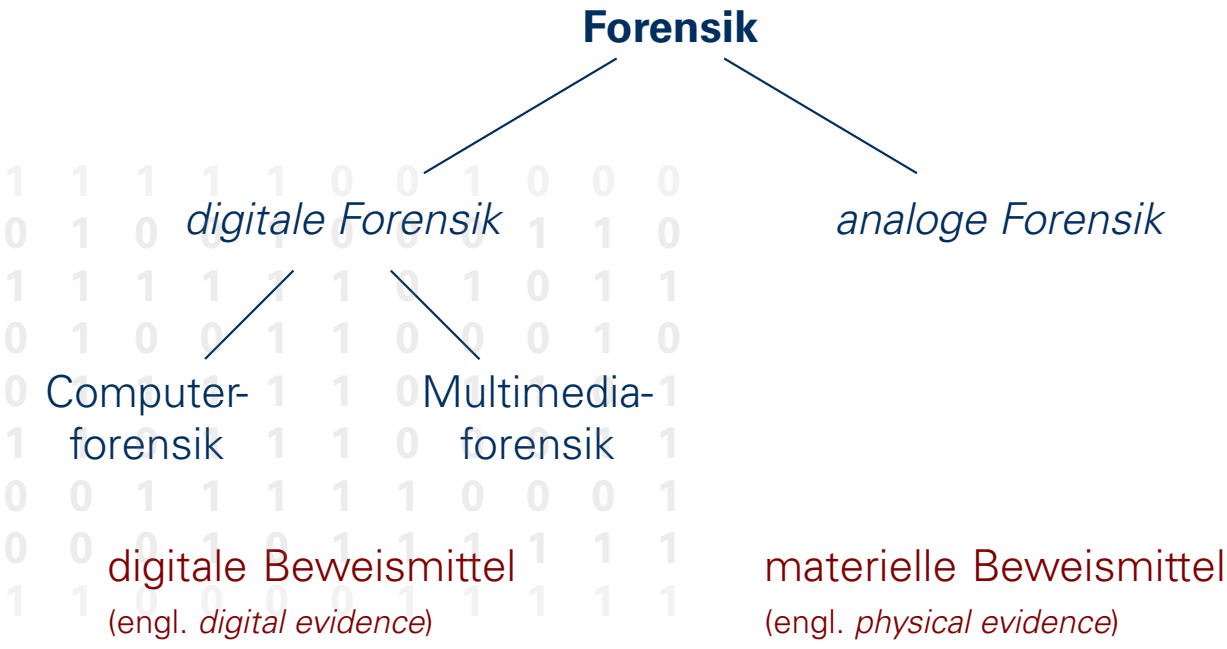
- **Modelle** helf
  Realität forma
- Typische Mod
  - ▷ Sensorrausch
  - ▷ zusammenhä
    treten in Origi
- Modellannah
- Modellgüte b



nethode!

Gliederung

Strukturierungsvorschlag für digitale Forensik



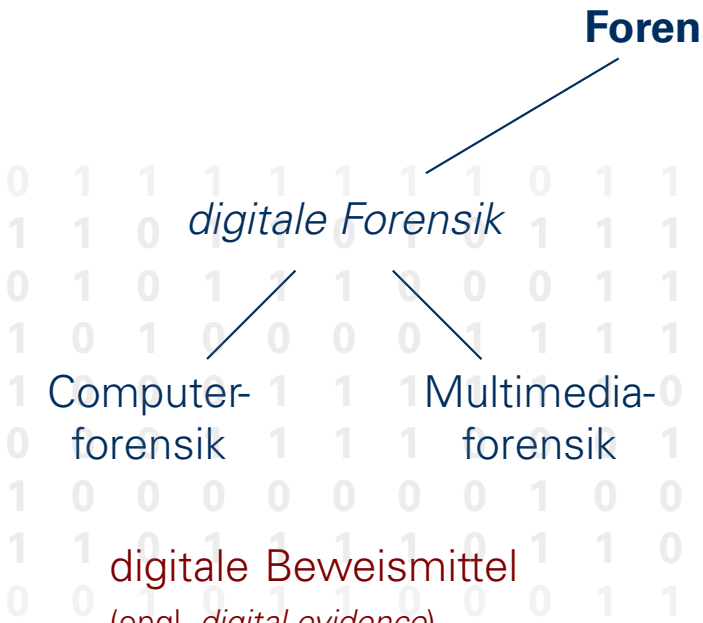
Fälschbarkeit

$\widehat{=}$

Techniken zur Vereitelung forensischer Erfolge

(engl. *counter-forensics*)

Strukturierungsvorschlag für digitale Forensik



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

Kirk (1953)

digitale Beweismittel
(engl. *digital evidence*)

materielle Beweismittel
(engl. *physical evidence*)

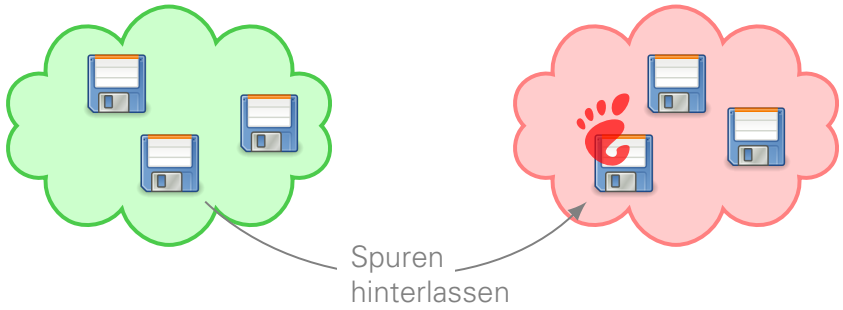
Fälschbarkeit

$\widehat{=}$

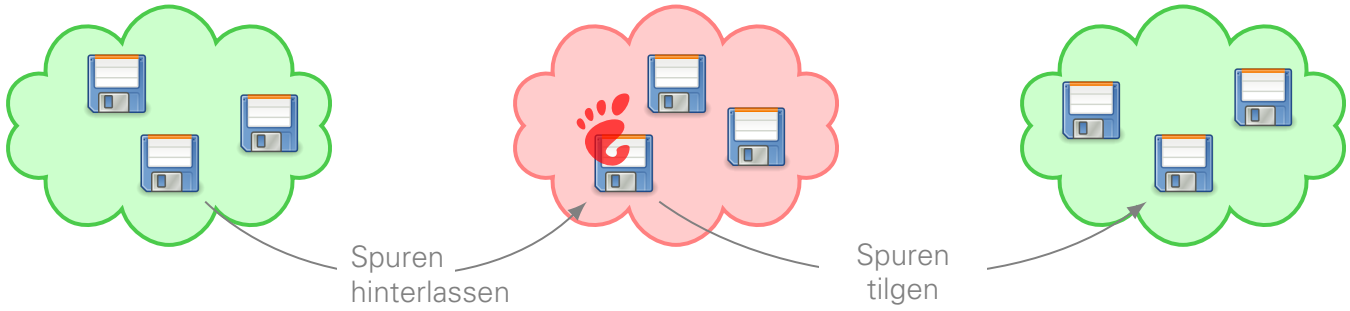
Techniken zur Vereitelung forensischer Erfolge

(engl. *counter-forensics*)

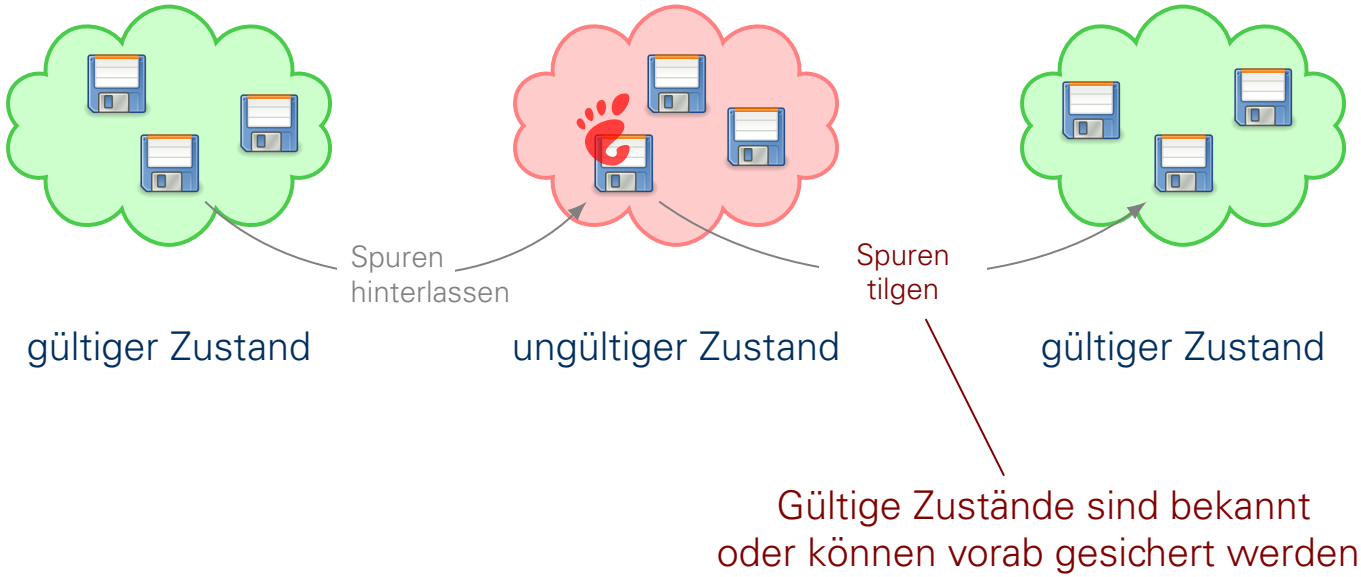
Vereitelungstechniken bei Computer-Forensik



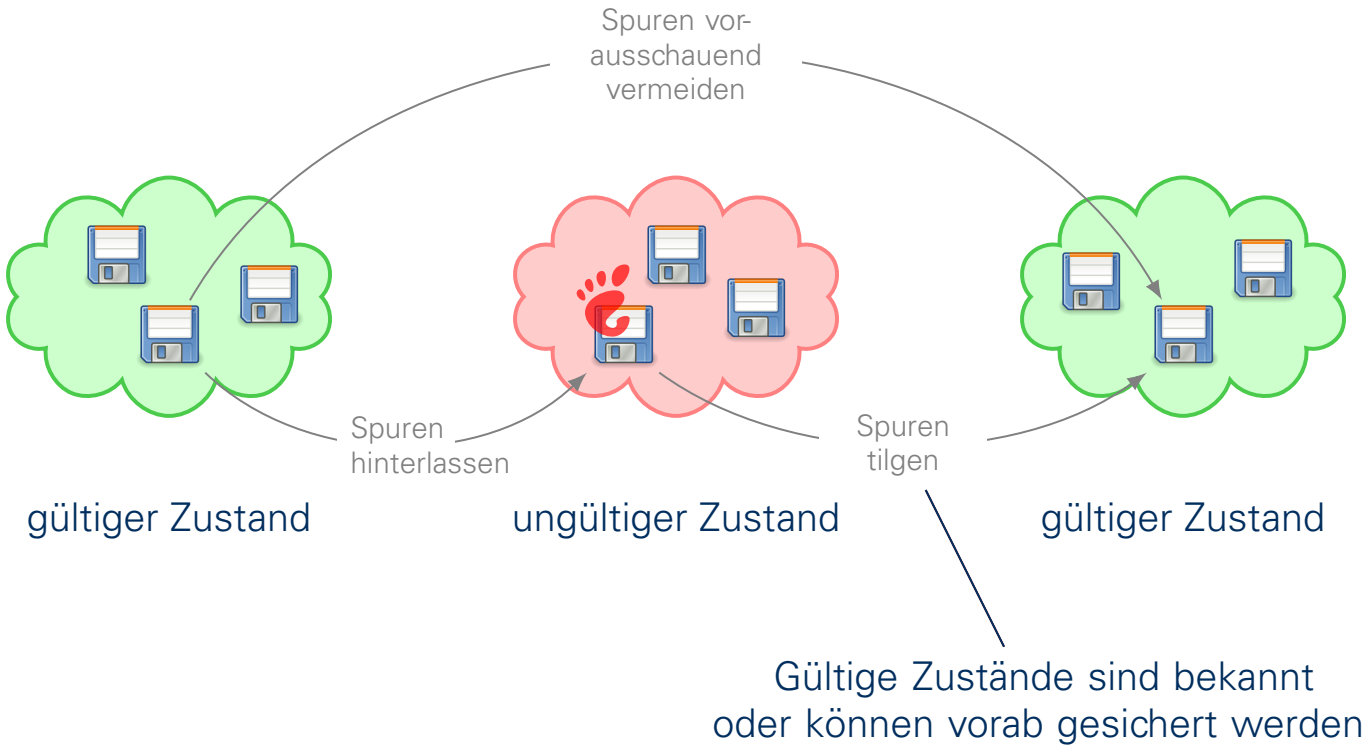
Vereitelungstechniken bei Computer-Forensik



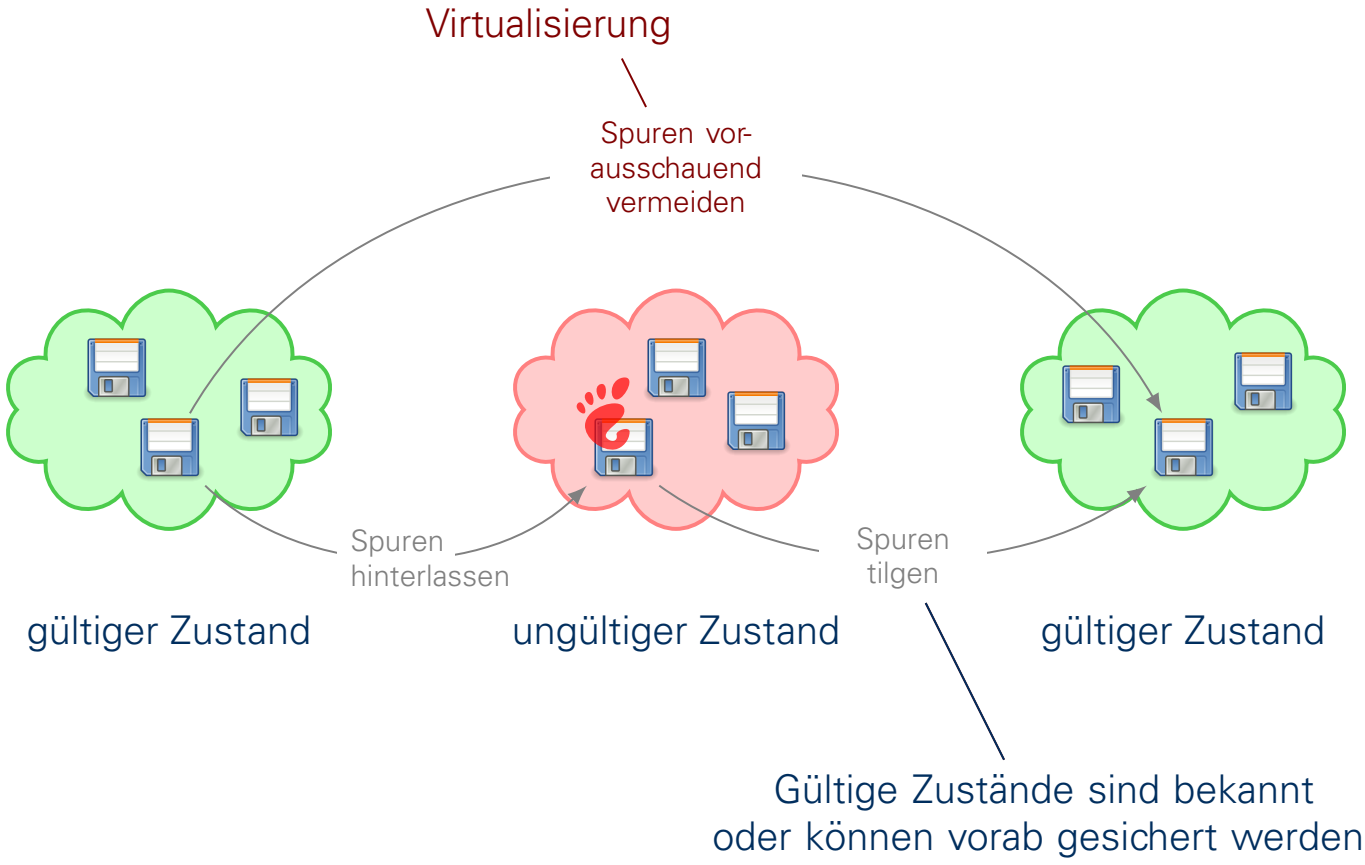
Vereitelungstechniken bei Computer-Forensik



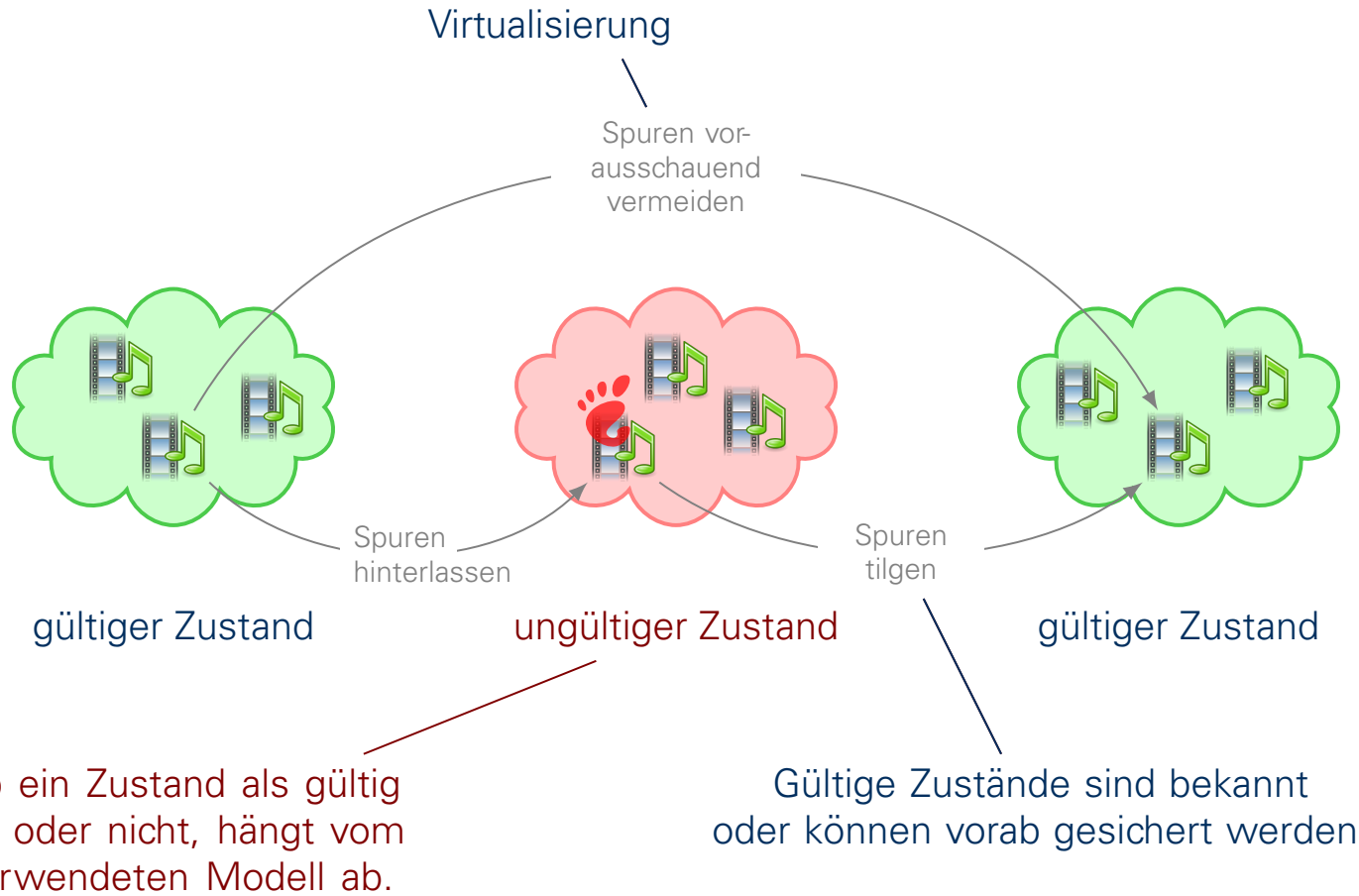
Vereitelungstechniken bei Computer-Forensik



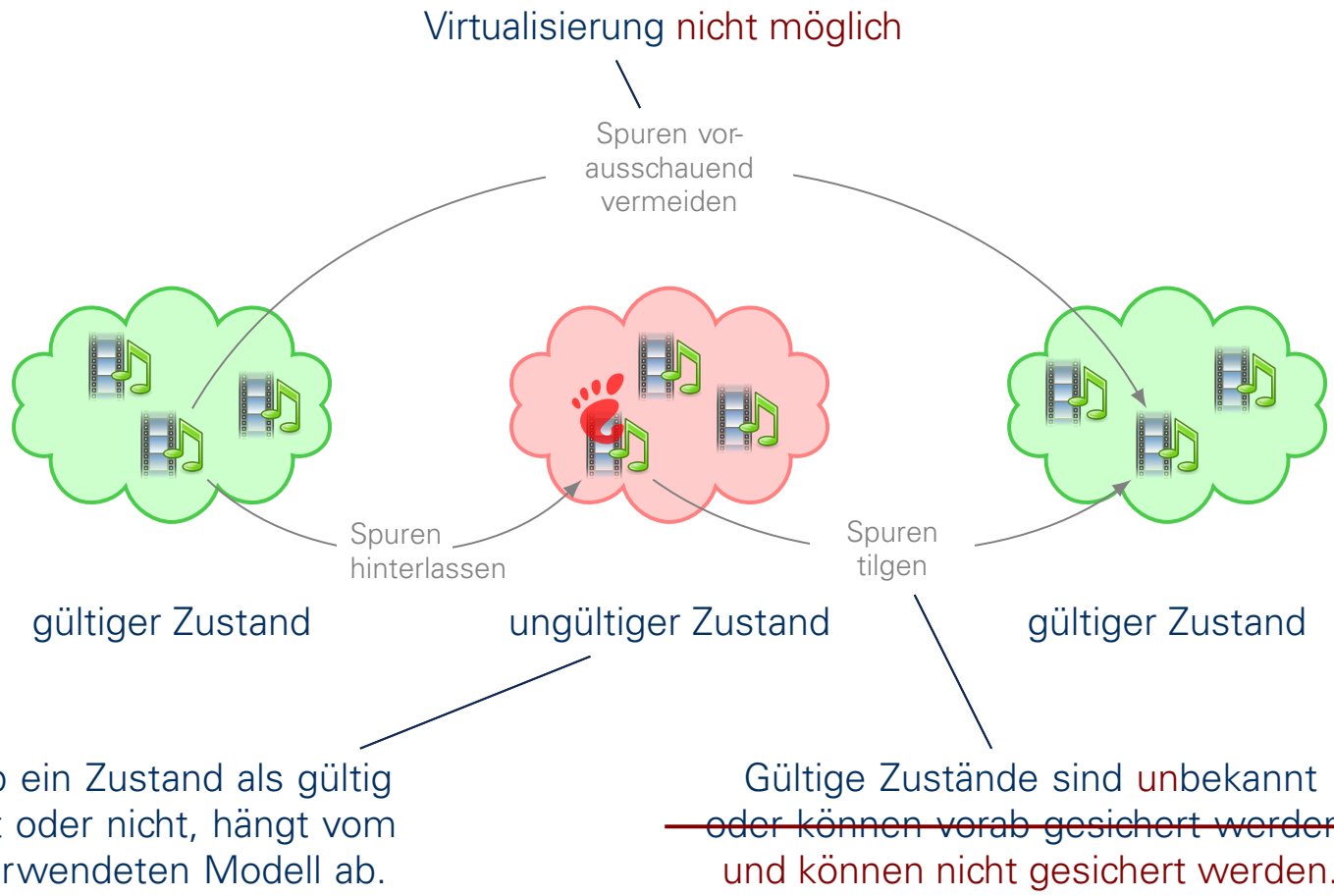
Vereitelungstechniken bei Computer-Forensik



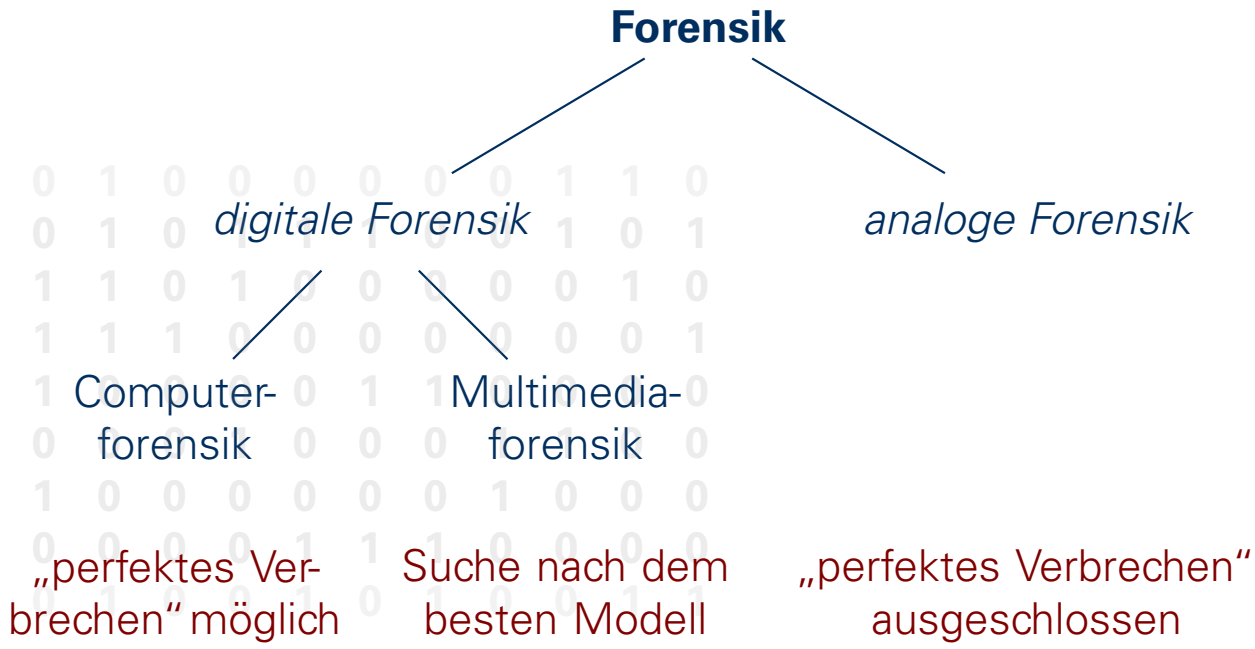
Vereitelungstechniken bei Multimedia-Forensik



Vereitelungstechniken bei Multimedia-Forensik



Strukturierungsvorschlag für digitale Forensik



$\widehat{=}$

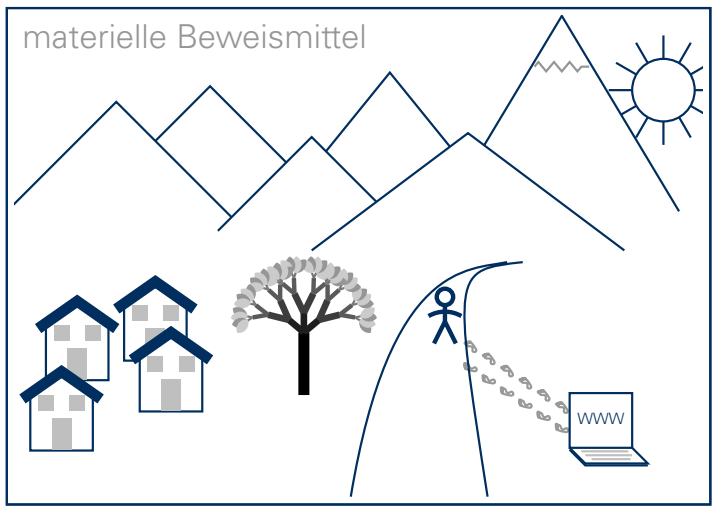
Techniken zur Vereitelung forensischer Erfolge

(engl. *counter-forensics*)

Gliederung

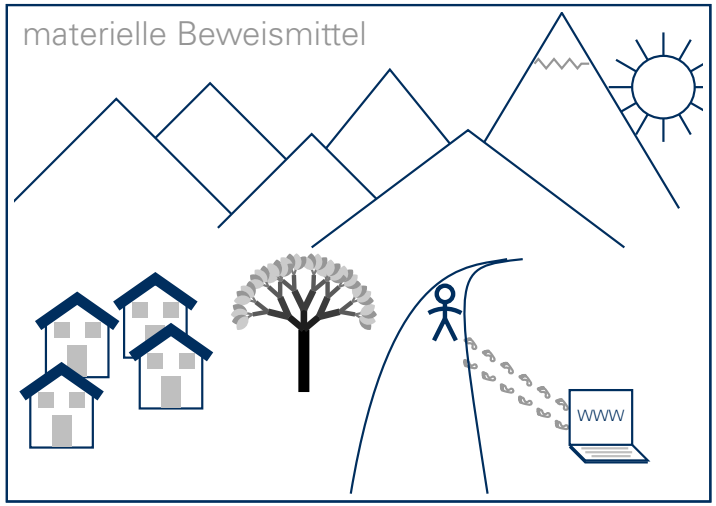
Computer-Forensik im weiteren Sinne

- Rechner interagieren mit ihrer Umgebung.

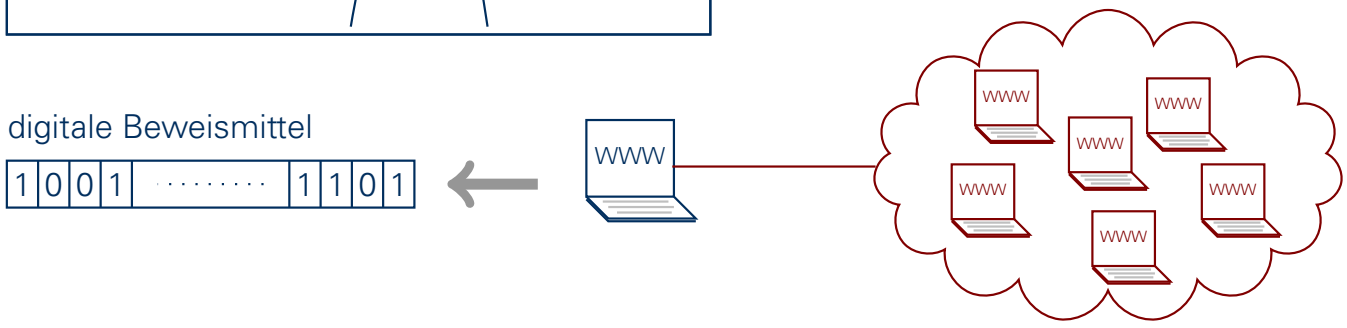


Computer-Forensik im weiteren Sinne

- Rechner interagieren mit ihrer Umgebung.

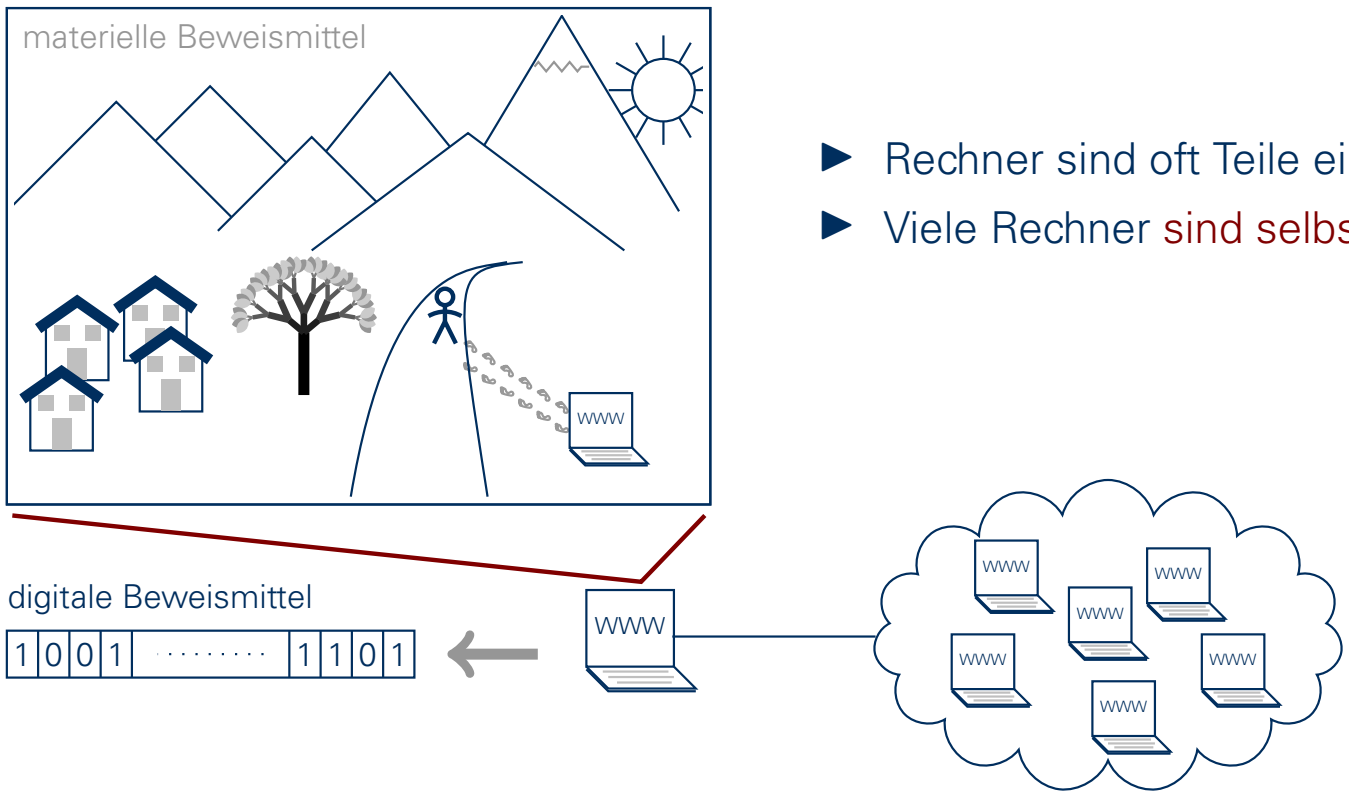


- Rechner sind oft Teile eines Netzes.



Computer-Forensik im weiteren Sinne

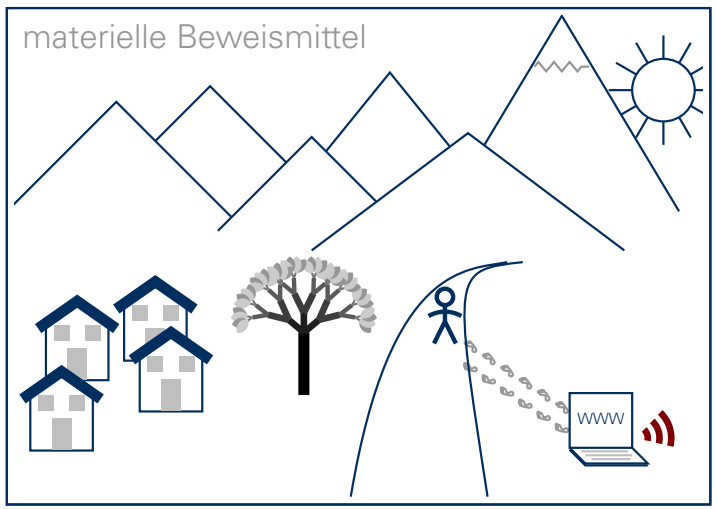
- Rechner interagieren mit ihrer Umgebung.



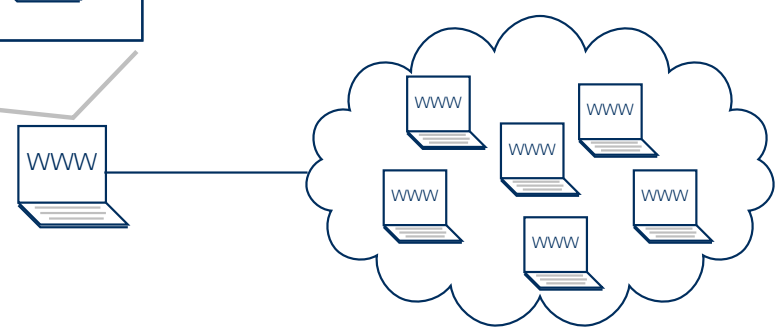
- Rechner sind oft Teile eines Netzes.
- Viele Rechner sind selbst Sensoren.

Computer-Forensik im weiteren Sinne

- Rechner interagieren mit ihrer Umgebung.



- Rechner sind oft Teile eines Netzes.
- Viele Rechner sind selbst Sensoren.
- Rechner hinterlassen Spuren in der materiellen Welt (z. B. elektromagn. Abstrahlung).



Zu guter Letzt: Ein Blick in die Praxis

Schlussbemerkungen

- Ermittler kombinieren in der Regel verschiedene forensische Wissenschaften.
- Dies „vernebelt“ den Blick auf wichtige Unterscheidungen bzgl. der jeweiligen zugrunde liegenden Annahmen.

- **Denn:** digitale Beweismittel $\neq$ digitale Beweismittel ($\neq$ materielle Beweismittel):
  - Digitale Beweismittel in der Computer-Forensik weisen einen schwächeren Bezug zur Realität auf, als in der Multimedia-Forensik.
  - Dies hat Konsequenzen auf die Aussagekraft forensischer Analysen.

- **Forschungsbedarf:** formalere Beschreibung auf Grundlage der Wahrscheinlichkeitslehre

Schlussbemerkungen

- Ermittler kombinieren in der Regel verschiedene forensische Wissenschaften.
- Dies „vernebelt“ den Blick auf wichtige Unterscheidungen bzgl. der jeweiligen zugrunde liegenden Annahmen.

- **Denn:** digitale Beweismittel $\neq$ digitale Beweismittel ($\neq$ materielle Beweismittel):
  - Digitale Beweismittel in der Computer-Forensik weisen einen schwächeren Bezug zur Realität auf, als in der Multimedia-Forensik.
  - Dies hat Konsequenzen auf die Aussagekraft forensischer Analysen.

- **Forschungsbedarf:** formalere Beschreibung auf Grundlage der Wahrscheinlichkeitslehre

Die Realität ist nicht endgültig erkennbar, . . .

Schlussbemerkungen

- Ermittler kombinieren in der Regel verschiedene forensische Wissenschaften.
- Dies „vernebelt“ den Blick auf wichtige Unterscheidungen bzgl. der jeweiligen zugrunde liegenden Annahmen.

- **Denn:** digitale Beweismittel $\neq$ digitale Beweismittel ($\neq$ materielle Beweismittel):
  - Digitale Beweismittel in der Computer-Forensik weisen einen schwächeren Bezug zur Realität auf, als in der Multimedia-Forensik.
  - Dies hat Konsequenzen auf die Aussagekraft forensischer Analysen.

- **Forschungsbedarf:** formalere Beschreibung auf Grundlage der Wahrscheinlichkeitslehre

Die Realität ist nicht endgültig erkennbar, . . .
aber Ihre Anregungen helfen, einen vollständigeren Blick auf sie zu erlangen.

TECHNISCHE UNIVERSITÄT DRESDEN

UNIVERSITÄT MANNHEIM

ICSI INTERNATIONAL COMPUTER SCIENCE INSTITUTE

Danke für Ihre Aufmerksamkeit

Fragen ? Kommentare ?

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

[†] Technische Universität Dresden [‡] Universität Mannheim [*] ICSI Berkeley

Rainer Böhme ist Postdoktorand am ICSI Berkeley, seine Reise nach Lübeck wurde freundlicherweise vom DAAD unterstützt. Matthias Kirchner ist Stipendiat der Deutschen Telekom Stiftung, Bonn.

Quellennachweis

- Iranischer Raketentest (4) http://www.spiegel.de
- Festplatte (6) http://commons.wikimedia.org/wiki/File:Open_hard-drive.jpg
- Diskette (11,17) http://commons.wikimedia.org/wiki/GNOME_Desktop_icons
- Kernspeicher (11) http://commons.wikimedia.org/wiki/File:KL_CoreMemory.jpg
- Multimedia (12,18) http://commons.wikimedia.org/wiki/GNOME_Desktop_icons
- Fingerabdrücke (22) http://www.lanl.gov/news/albums/chemistry/fingerprint.jpg
- Handschellen (22) http://commons.wikimedia.org/wiki/File:Handcuffs01_2003-06-02.jpg