UNIVERSITÄT MANNHEIM

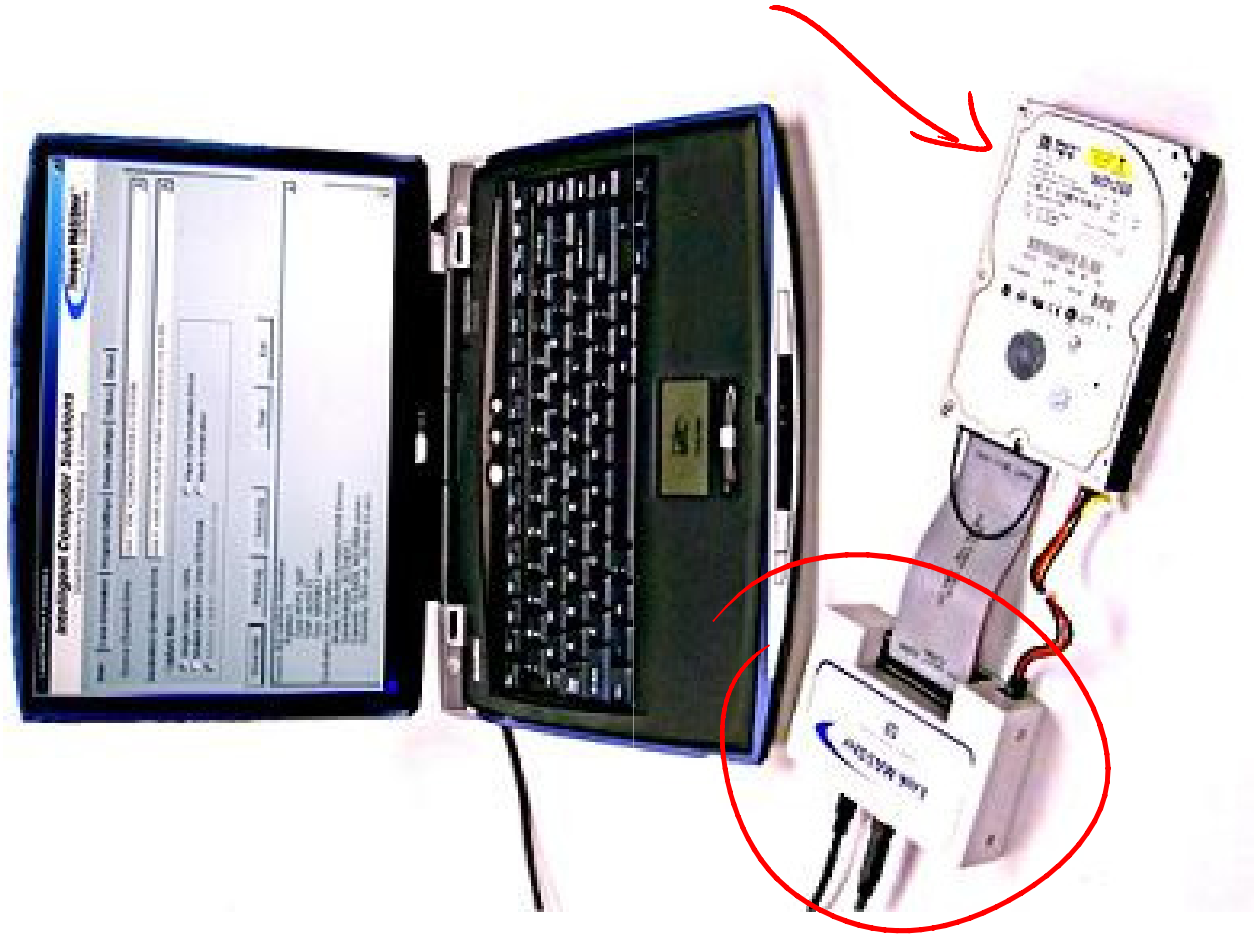
Selektion vor der Sicherung

Methoden zur effizienten forensischen Sicherung digitaler Speichermedien

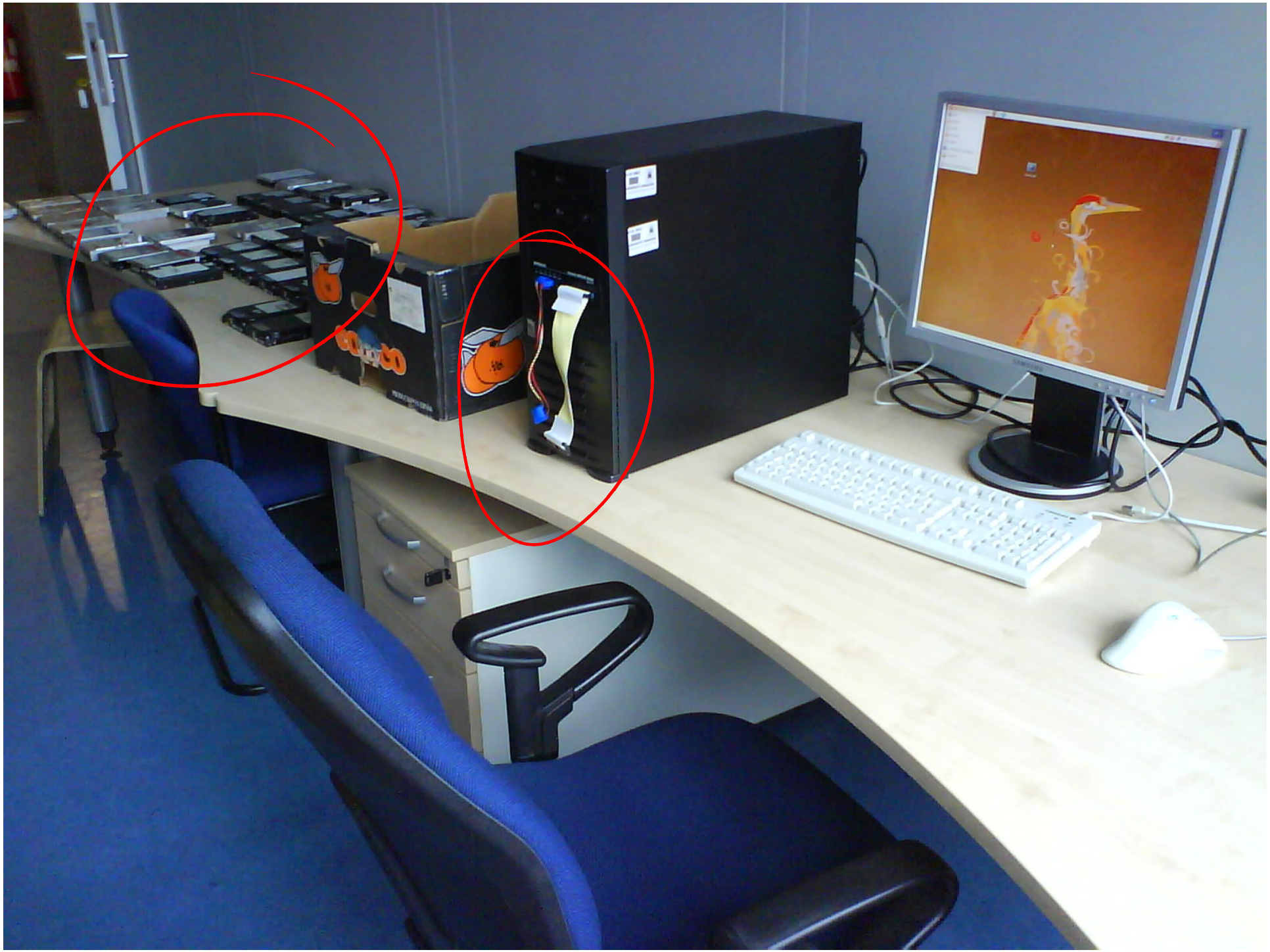
Felix C. Freiling
Universität Mannheim
Lehrstuhl für Praktische Informatik 1

Anwendertag IT-Forensik, Fraunhofer SIT, Darmstadt, 23.2.2010

Quelle: http://abcusinc.com/ICS_Linkmasster.html




ROUTET
WURST
FUJITSU
SIEMENS



Die bitweise 1:1-Kopie

- Forensischer Grundsatz: Nichts verändern!
- Natur digitaler Spuren:
  - Können vollständig dupliziert werden
  - Sind leicht zu manipulieren
- Standardmäßiger Schritt im forensischen Prozess (bisher):
  - Vollständige bitweise 1:1-Kopie der beschlagnahmten Datenträger
  - Sicherung der Integrität des Originals durch Hardware-Write-Blocker
  - Integritätskonrolle durch kryptographische Checksummen

Datenüberlastung

- Digitale Speichermedien sind heute in vielen Strafverfahren von Bedeutung
- (Private) Speicherkapazität steigt deutlich schneller als die der Ermittlungsbehörden
- Quantität an gesicherten Daten übersteigt die Kapazität der Ermittler

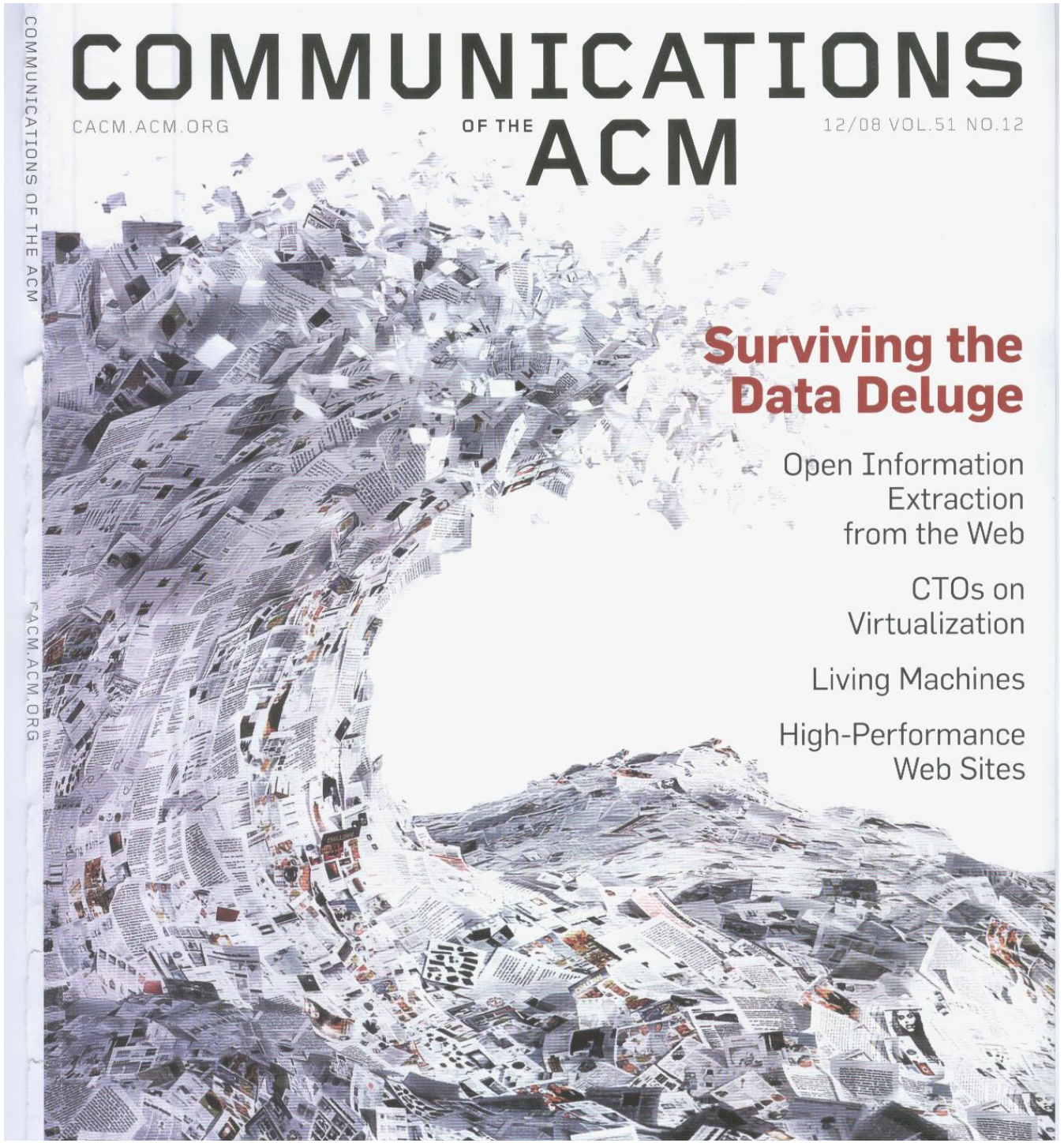

COMMUNICATIONS OF THE ACM
CACM.ACM.ORG
COMMUNICATIONS OF THE ACM
CACM.ACM.ORG
12/08 VOL.51 NO.12
Surviving the Data Deluge
Open Information Extraction from the Web
CTOs on Virtualization
Living Machines
High-Performance Web Sites

Foto: Thomas Herbrich (vgl. auch Titelbild CACM 12/2008)

Fragestellung

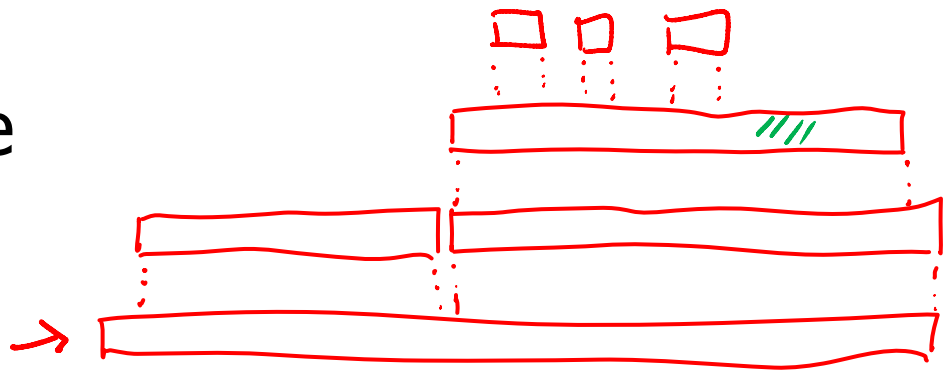
- Welche Alternativen zur 1:1-Kopie gibt es?

Analogie: Identifikation physischer Beweismittel

- Bei einer (klassischen) Durchsuchung wird vor Ort gesichtet und selektiert
  - Aufschriften auf Ordnerrücken
  - Inhalt der ersten Seiten eines Notizbuches
  - ...
- Training und Erfahrung des Ermittlers geben den Ausschlag
- Bei einer (digitalen) Durchsuchung wird bereits heute selektiert
  - Musik-CDs und Installationsmedien werden nicht kopiert
  - Aber was ist mit dem Rest?

Abstraktionsebenen Speichermedien

- Dateiebene
- Dateisystemebene
- Partitionsebene
- Physische Ebene



Arten der Sicherung

- Sicherung auf physischer Ebene
  - Entspricht vollständiger 1:1-Kopie
- Sicherung auf Partitionsebene
  - Selektion auf Ebene der Partitionen möglich
  - Beispiel: Systempartitionen oder Swap-Space ausschließen
- Sicherung auf Dateisystemebene
  - Selektion auf Ebene der Dateisysteme möglich
- Sicherung auf Dateiebene
  - Selektion auf Dateiebene möglich
  - Beispiel: nur Bilddateien sichern oder nur E-Mail-Dateien

Live-Analyse

- Sicherung unter Nutzung des Rechners des Beschuldigten
  - Booten von LiveCD
- Sicherung unter Nutzung des Rechners und des Betriebssystems des Beschuldigten (Live-Analyse)
  - Wenigstens Programme von vertrauenswürdiger Quelle verwenden (CD)
  - Vorsicht vor Rootkits und logischen Sprengfallen

Techniken und Werkzeuge

HELIX 3 ENTERPRISE

F.I.R.E.

- LiveCDs
  - HELIX (www.e-fense.com)
  - F.I.R.E. (fire.dmzs.com)
- Spezialhardware:
  - Shadow Drive (www.voomtech.com)
  - Reborn Card (www.signalnet.de)

Grundsätzliche juristische Einschätzung

- Freie richterliche Beweiswürdigung
- Inbetriebnahme und Sichtung fremder EDV-Anlagen wird durch Befugnis zur Durchsuchung abgedeckt
- Vertrauenswürdigkeit limitierender Faktor bleibt der Zeuge/Sachverständige
- Manipulations- und Fehlerrisiko abschätzbar machen durch Dokumentation

Manipulations- und Fehlerrisiko

- Sehr gering:
  - Zugriff auf Datenträger mit Hardware-Write-Blocker
  - Booten des Rechners mittels LiveCD, Montierung des Datenträgers als Read-Only-Device
- Abschätzbar:
  - Untersuchung am laufenden System (Live-Analyse) mit vertrauenswürdigen Programmen von CD

Verhältnismäßigkeit des Umfangs der Datenerhebung

- IT-Grundrecht schützt die Vertraulichkeit der persönlichen IT
- Zugriffe müssen auf das notwendige Maß beschränkt sein
- Zusätzlicher Vorteil der Selektion vor der Sicherung

Ausblick: verschlüsselte Festplatten

- Notwendige kryptographische Schlüssel liegen im RAM
- Live-Analyse wird die Regel sein

Handlungsempfehlung

- „Nichts verändern“ heißt nicht automatisch „alles mitnehmen“

- Begründete Selektion kann Datenüberlastung eindämmen
- Gefahr, etwas zu übersehen, von Fall zu Fall abwägen

Dank

Matthias Bäcker, Felix Freiling, Sven Schmitt: Selektion vor der Sicherung. In: Datenschutz und Datensicherheit, 4/2010

- Prof. Dr. Matthias Bäcker, Universität Mannheim

- Dipl.-Wirtsch.-Inf. Sven Schmitt, Universität Mannheim

Kontakt

Prof. Dr. Felix Freiling
Universität Mannheim
Lehrstuhl für Praktische Informatik 1
68131 Mannheim

https://pi1.informatik.uni-mannheim.de