IT-Sachverständigenbüro • IT-Consulting • Datenrettung

Anwendertag IT-Forensik
„Big Data – Big Evidence?“

IT-Forensik im Strafprozesskontext – Umgang mit großen Datenmengen

Werner Poppitz
September 2014

Abgrenzung / Haftungsausschluss / Copyright

Abgrenzung

Dieser Foliensatz stellt teilweise sehr komplexe Sachverhalte sehr verkürzt und plakativ (teilweise überspitzt) dar. Insbesondere bei juristischen und technischen Aussagen erhebt er keinen Anspruch auf Vollständigkeit oder Korrektheit.

Die in diesem Foliensatz enthaltenen Informationen können durch die FAST-DETECT GmbH ohne vorherige Ankündigung geändert werden.

Haftungsausschluss

Die FAST-DETECT GmbH übernimmt keinerlei Haftung für Fehler oder Unvollständigkeiten in diesem Foliensatz. Aus den in diesem Foliensatz enthaltenen Informationen ergibt sich auch keine weiterführende Haftung.

© Copyright 2014 FAST-DETECT GmbH

Dieser Foliensatz wurde durch Mitarbeiter der FAST-DETECT GmbH erstellt und präsentiert. Er wird Teilnehmern der Präsentation zur Verfügung gestellt und dient als Begleit-, Informations- und Nachlesematerial. Eine weitergehende Nutzung wird nicht gestattet. Insbesondere sind die Weitergabe (auch Vorführung, Sendung, Vermietung oder Leihe) sowie die Vervielfältigung dieses Foliensatzes oder von Teilen daraus, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung durch die FAST-DETECT GmbH nicht gestattet und ziehen straf- oder zivilrechtliche Folgen nach sich. Alle Rechte bleiben vorbehalten.

Inhalt

1. Die FAST-DETECT GmbH
2. „Big-Data“ in der Sicherstellung
   - Sicherung von Daten im Unternehmen
   - Sicherung von Daten in der Cloud
3. Rechtliche Probleme
4. „Big-Data“ in der IT-Forensik-Auswertung
   - Wie sieht die Toolseite aus?
   - Auswertung großer Datenmengen im Wirtschaftsstrafverfahren

Die FAST-DETECT GmbH

Größtes Sachverständigenbüro für **IT-Forensik** in Deutschland

Die FAST-DETECT GmbH

Berufssachverständige für IT-Forensik

- Unternehmensgründung 2003 mit stetigen Wachstum.
- Derzeit 3 Berufssachverständige für IT-Forensik und 16 weitere IT-Forensik-Analysten.

Berufssachverständige für IT-Forensik		Erfahrung in der IT-Forensik	
	**Thomas Salzberger**, 1963 Diplom-Informatiker (Univ.)	**Seit 2002**	**Weit über 3.000 Gutachten** für über 70 Staatsanwaltschaften in allen 16 Bundesländern **Mehr als 400 Gerichtsverhandlungen** **Breites Spektrum an IT-Forensik-Aufträgen**
	**Werner Poppitz**, 1968 Fachinformatiker (IHK)	**Seit 2004**	
	**Fabian Unucka**, 1981 Diplom-Informatiker (Univ.)	**Seit 2004**	

- Weitere Sachverständige für IT-Forensik werden ausgebildet.
- **Wir suchen ständig neues Personal im Bereich IT-Forensik!**

„Big Data“ in der Sicherstellung

Auswirkungen der Datenzunahme auf die Daten- und Beweissicherung

Sicherung von Daten im Unternehmen

Rapide Zunahme der in Unternehmen anfallenden Daten

Sicherstellungsunterstützung

Vorbereitung Planung

Dinge die im Vorfeld einer Sicherstellung benötigt werden:

- **möglichst detaillierte** Informationen zum Durchsuchungsobjekt, zu der Art des Verfahrens und zu den Vorermittlungserkenntnissen
- je nach „Größe des Durchsuchungsobjekts“ 1 bis 5 Tage zur **Vorbereitung** (evtl. Beschaffung):

Micro-SD-Karte

Laptop

Serverraum

Rechenzentrum

Sicherstellungsunterstützung

Das FAST-DETECT Field-Forensic-Equipment

- Schreibschutzsysteme für alle gängigen Festplatten (IDE, SATA, SCSI, USB und SAS)
- 6 Field-Forensic Rechner und 2 UFED, um u.a. **live Daten auszuwerten.**
- 50 x IDE-/SATA-Adapter für das gleichzeitigte Sichern von bis zu 50 Rechnern.
- Alle gängigen Software-Imagelösungen (auch Linux)
  - EnCase von Guidance Software
  - FTK Imager von Access Data
    NT-Backup von Microsoft

- Festplattenkapazitäten nach Bedarf

Sicherstellungsunterstützung

Das 8-Stunden-Zeitfenster als Wettrennen gegen die Zeit!

Besondere Problemstellung bei der Sicherstellung im Strafprozess:

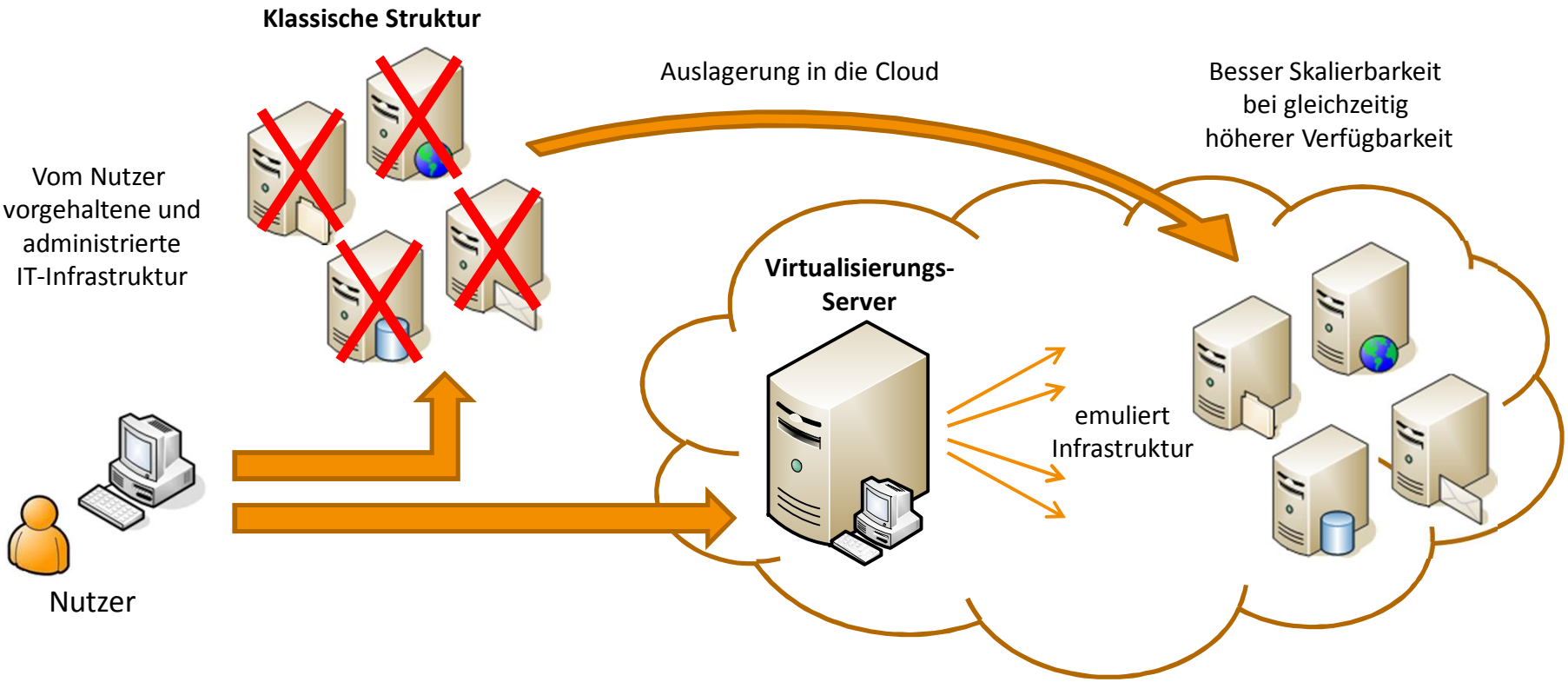
- Als Zeitraum für die Datensicherung steht i.d.R. nur ein Arbeitstag zur Verfügung:
  - Datensicherungen über mehr als 24 Stunden erfordern die Versiegelung von Büro- und Serverräumen
  - Eventuell Schichtablösungen von Polizeibeamten und Sachverständigen
- Selbst modernste Festplatten unterstützen nur Transferraten von bis zu 150 MByte pro Sekunde (= 0,5 TByte pro Stunde)
- Identifizierung des schnellsten Transferweges:
  - Ausbauen der Festplatten und an eigenem Equipment sichern
  - Anschluss mitgebrachter Platten an die Systeme des Beschuldigten
  - Sicherung über das Netzwerk
- Eventuell Filterung vor Ort zur Eingrenzung und Reduktion der zu sichernden Datenmenge

Sicherung von Daten in der Cloud

Verschiebung der Daten und Ressourcen in die Netzwerk-Wolke

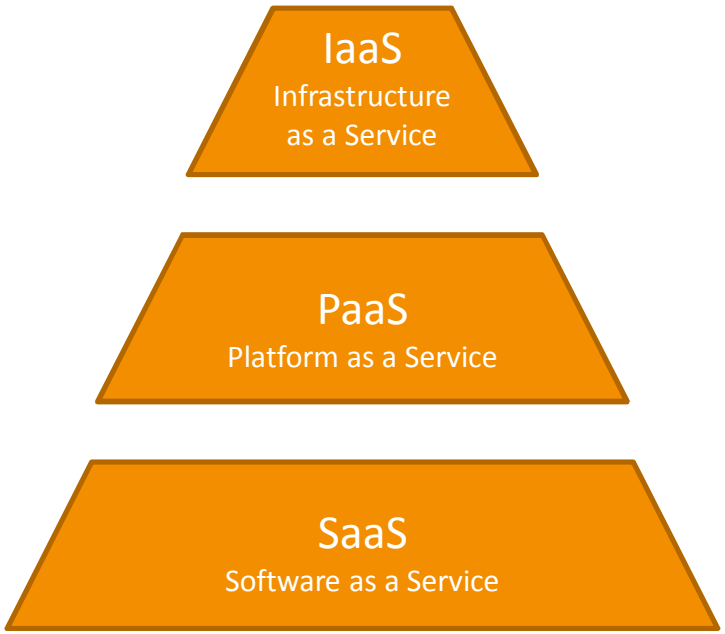
Sicherung von Daten in der Cloud

Virtualisierung als Motor des Cloud-Computing-Hypes



Sicherung von Daten in der Cloud

Die unterschiedlichen Arten des Cloud-Computings



- Virtualisierte Hardware
  (Speicher, CPU-Leistung, Bandbreite)
- Framework-System zur Realisierung eigener Anwendungen
  (Datenbanken, File- und Webserver, etc.)
- Fertige Anwendungen als Internetdienst
  (Webmailer, Kalender, Fotoalben etc.)

Sicherung von Daten in der Cloud

Cloud-Computing – Unterschiedliches Vorgehen, abhängig vom Service

Die unterschiedlichen Cloud-Computing-Service-Arten erfordern neu angepasste Vorgehen zur IT-forensischen Beweismittelsicherung:

- **Infrastructure as a Service (IaaS)**
  I.d.R. Sicherung der zugrunde liegenden virtuellen Maschinen über das Netz.
- **Platform as a Service (PaaS)**
  Sicherung der Dienstdaten über vorhandene Schnittstellen abhängig von der verwendeten Plattform (z.B. Sicherung von Datenbankdaten über SQL-Befehle). Erfordert zur Auswertung häufig die Rekonstruktion des Systems im IT-Forensik-Labor.
- **Software as a Service (SaaS)**
  Sicherungsmöglichkeit ist sehr stark vom angebotenen Service abhängig.
  Mitunter kann die Mitwirkung des Dienstanbieters erforderlich sein, da es u.U. keine Datensicherungsschnittstellen für den Endanwender.
  Im Extremfall Abfotografieren/Mitschnitt der Bildschirminhalte als letztes Mittel.

Sicherung von Daten in der Cloud

Cloud-Computing – Die besonderen Herausforderungen

- **Problem der ungenauen Geo-Lokalisation der Daten**
  Wo liegen die Daten? Bei einigen Providern nur über Vertragsunterlagen bestimmbar!
  Standorte der Server und/oder Daten möglicherweise im In- und Ausland.
- **Einschränkung des Zugriffs auf Cloud-Daten während/nach der Sicherung**
  - Verhindern, dass der Beschuldigte die Daten während der Sicherung von einem beliebigen Internet-Rechner aus löschen kann.
  - Verhindern, dass der Beschuldigte nach der Sicherstellung noch auf inkriminierte Daten zugreifen kann, welche der Besitzstrafbarkeit unterliegen.
- **Die Internetleitung als Flaschenhals**
  Bestehende Internetverbindungen eignen sich zwar für den Zugriff auf Cloud-Dienste, nicht aber zur Sicherung großer Cloud-Datenspeichermengen.
  (Evtl. Sicherung auf Server im Internet mit schnellerer Netzwerkanbindung)

Rechtliche Probleme

„Big Data“ und die Strafprozessordnung

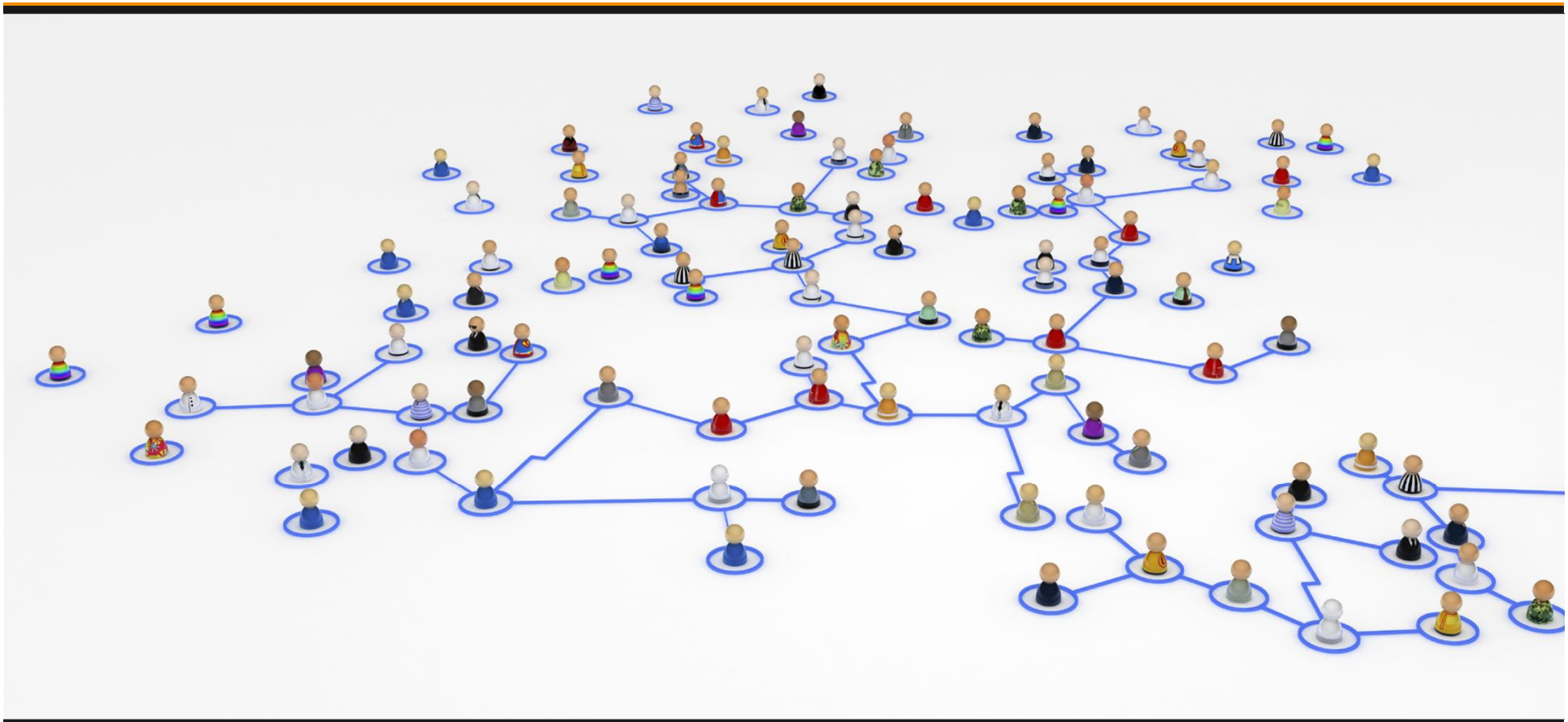
Mögl. Rechtliche Probleme

Fragen an die Justiz!

Die Strafprozessordnung kann die aktuelle Technik nicht abbilden

Der Gesetzgeber spricht noch von „Fernmeldegeheimnis“ und „Postbeschlagnahme“ während alle Welt schon von „Big Data“ spricht!

- **§110 Abs. 3 StPO** erlaubt die Datensicherung räumlich getrennter Speichermedien soweit auf sie vom Durchsuchungsort aus zugegriffen werden kann.
- **Grenzüberschreitender Datenverkehr = internationales Rechtshilfeersuchen**
  - Daten auf ausländischen Servern können nur bei „Gefahr in Verzug“ im Rahmen der Durchsuchung gesichert werden (=nachgeschobenes Rechtshilfeersuchen).
  - Schwierig wird es, wenn selbst der Provider nicht mehr sagen kann in welchem Land die Daten liegen (Stichwort: Elastic Cloud) – Welches Land ist in solchen Fällen für einen möglichen Beschlagnahmebeschluss zuständig?
  - Manchmal genügt aber auch schon der Rückgriff auf Proxyserver im Inland oder die Auswertung zwischengespeicherter Daten auf dem Clientrechner bzw. dem Mobiltelefon.



IT-Forensik (= Digitale Forensik, Computerforensik)

„Big Data“ in der IT-Forensik-Auswertung

Auch IT-Forensik-Sachverständige sind „Big Data“ Anwender!

Der IT-Forensiker als „Big Data“ Anwender

Wie sieht die Toolseite aus?

„Big-Data“-Lösungen für den IT-Forensiker

Welche Lösungsansätze und Markttrends gibt es?

- Guidance Software:
  - Verabschiedung vom „Single-Case-All-In-Memory“-Konzept
  - Ansätze für Multirechner-Support in Form von „Processing-Nodes“ (jedoch derzeit nur begrenztes Parallel-Computing)
- Access-Data:
  - Trend zum Multi-User-System mit „AD-Labs“ (mehrere Auswerter arbeiten an einem Fall)
- NUIX:
  - Skalierbare „Parallel-Processing“-Lösung für „Big-Data“ mit integrierter grafischer Visualisierung (jedoch mit Schwächen in der Nutzungsspurenanalyse)
- IBM / I2Group:
  - Analyst‘s Notebook zur Visualisierung von unstrukturierten Daten in der Kriminalistik (fehlende Integration bzw. noch ungenügende Schnittstellen zu bestehenden IT-Forensik-Lösungen - erfordert häufig manuelle Datenkonvertierungen)
- Die Verarbeitung der Beweismitteldaten in der „Cloud“ stellt im Strafprozess aufgrund geltender Sicherheitsanforderungen keine Option dar!

Der IT-Forensiker als „Big Data“ Anwender

Die Auswertung großer Datenmengen im Wirtschaftsstrafverfahren

Auswertungsvorgehen bei Wirtschaftskriminalität

Knowledge Discovery Prozess

1. Vorbereitung des Knowledge Discovery Prozesses
2. Datenauswahl
3. **Datenbereinigung / Datennormalisierung** *Wird kurz beschrieben.*
4. Datenreduktion (Filterung, De-Duplizierung, Textextraktion)
5. Suchen nach relevanten Dokumenten (Schlüsselwort- vs. Indexsuche)
6. **Data-Mining** (Erkenntnisgewinnung) *Wird kurz beschrieben.*
7. Interpretation der Erkenntnisse und Überführung ins Gutachten

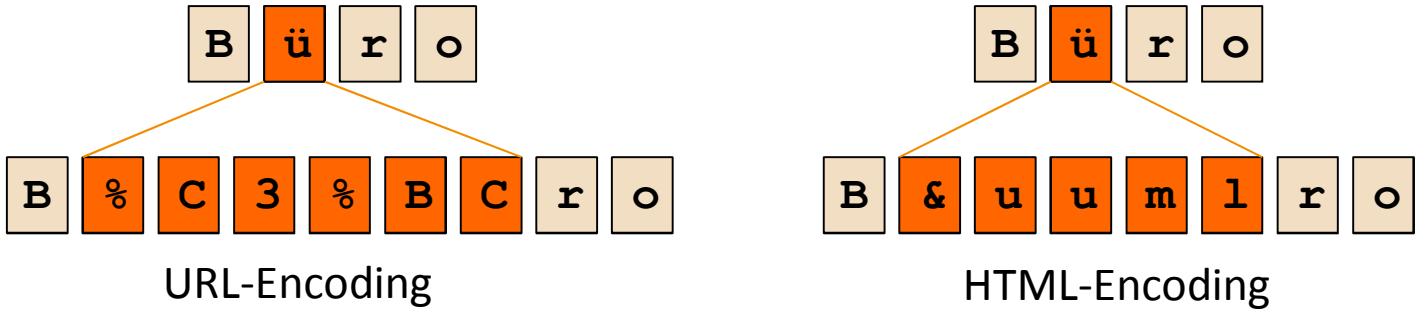
Auswertungsvorgehen bei Wirtschaftskriminalität

Knowledge Discovery Prozess: Datenbereinigung / Datennormalisierung

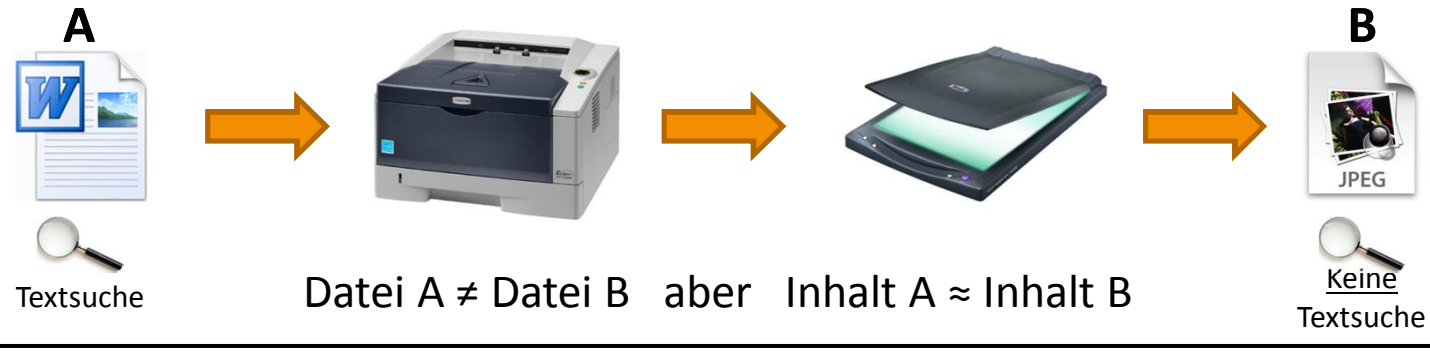
Computer speichern häufig die selbe Information auf unterschiedliche Weise.

Für die Auswertung müssen diese jedoch so umgewandelt werden, dass sie auf eine einheitliche Weise durchsucht werden können.

Beispiel 1



Beispiel 2

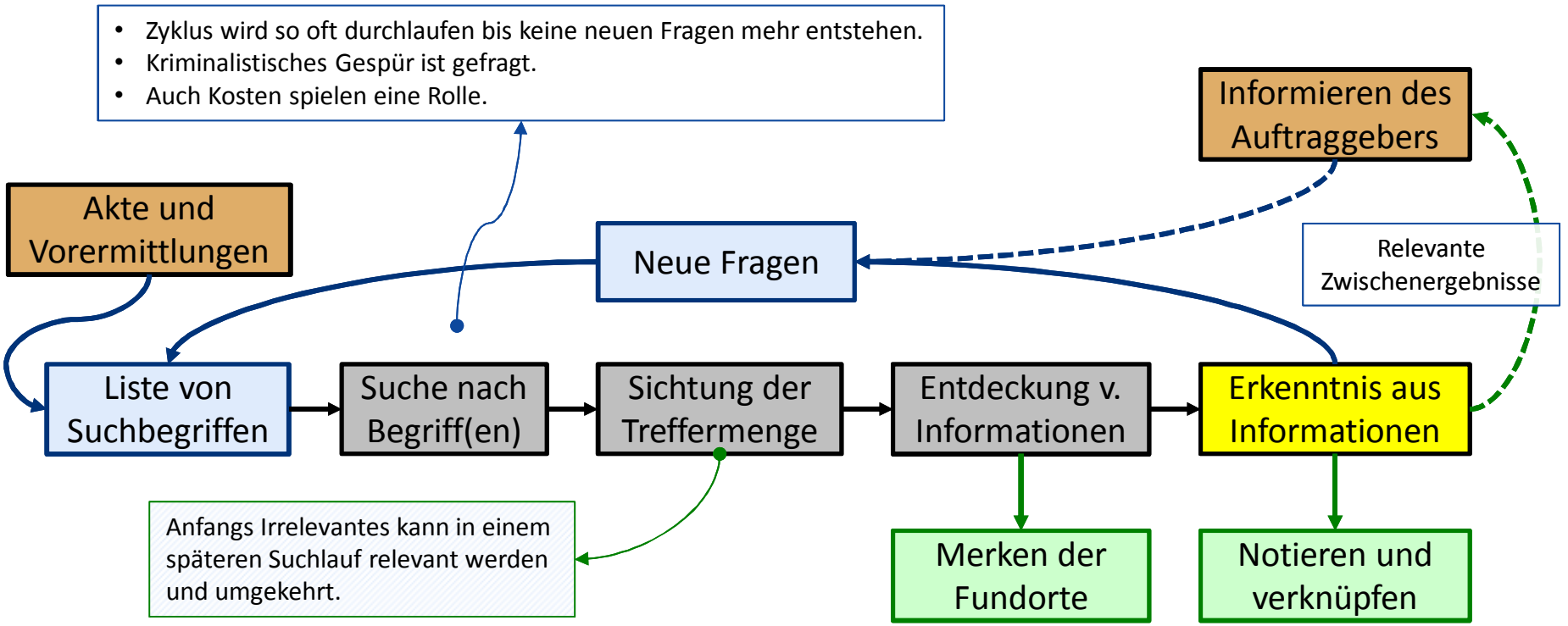


Auswertungsvorgehen bei Wirtschaftskriminalität

Knowledge Discovery Prozess: Data-Mining

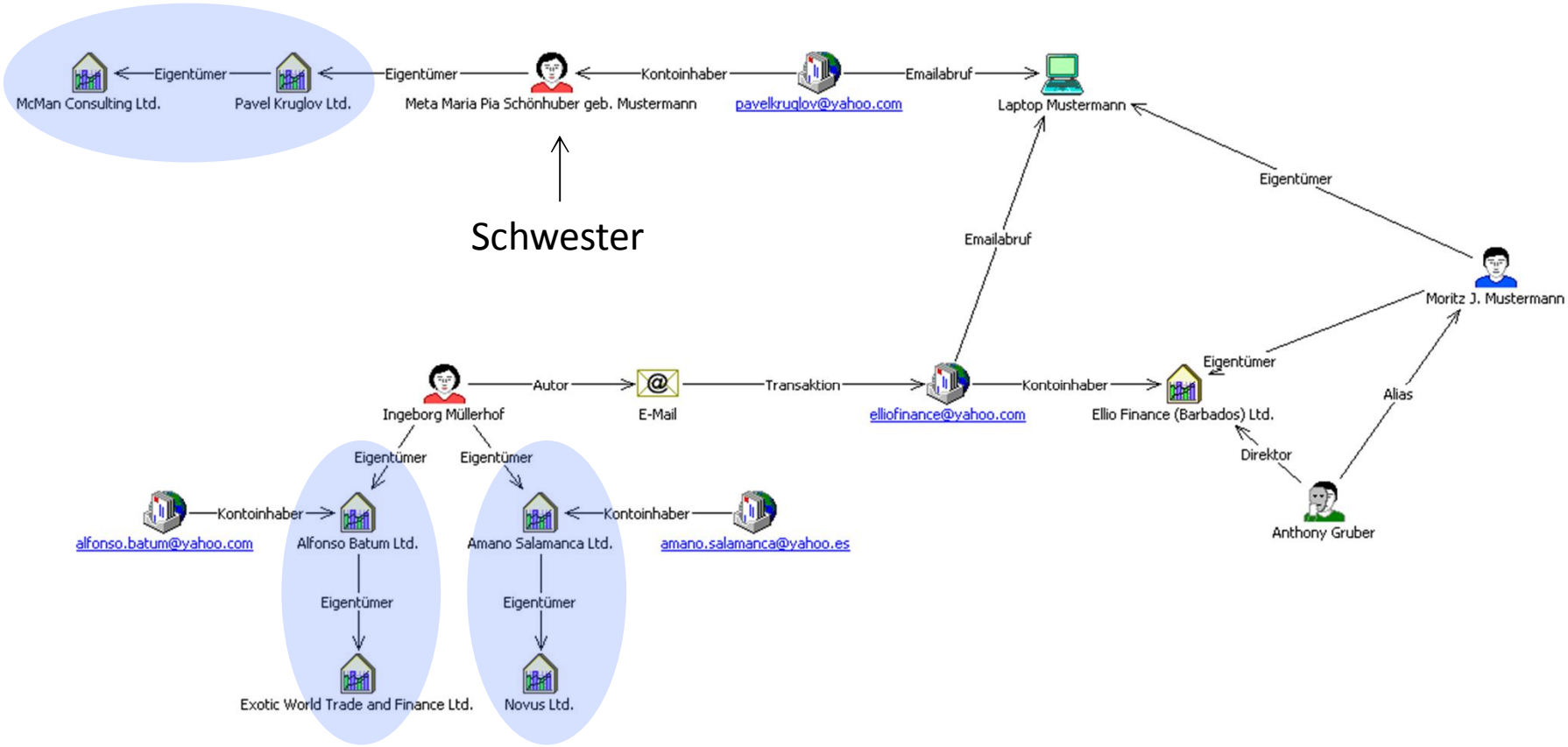
Data-Mining dient dem Erkennen von Mustern zur Erkenntnisgewinnung.

Es handelt sich um einen dynamischen, sich wiederholenden Prozess:



Visualisierung unstrukturierter Daten

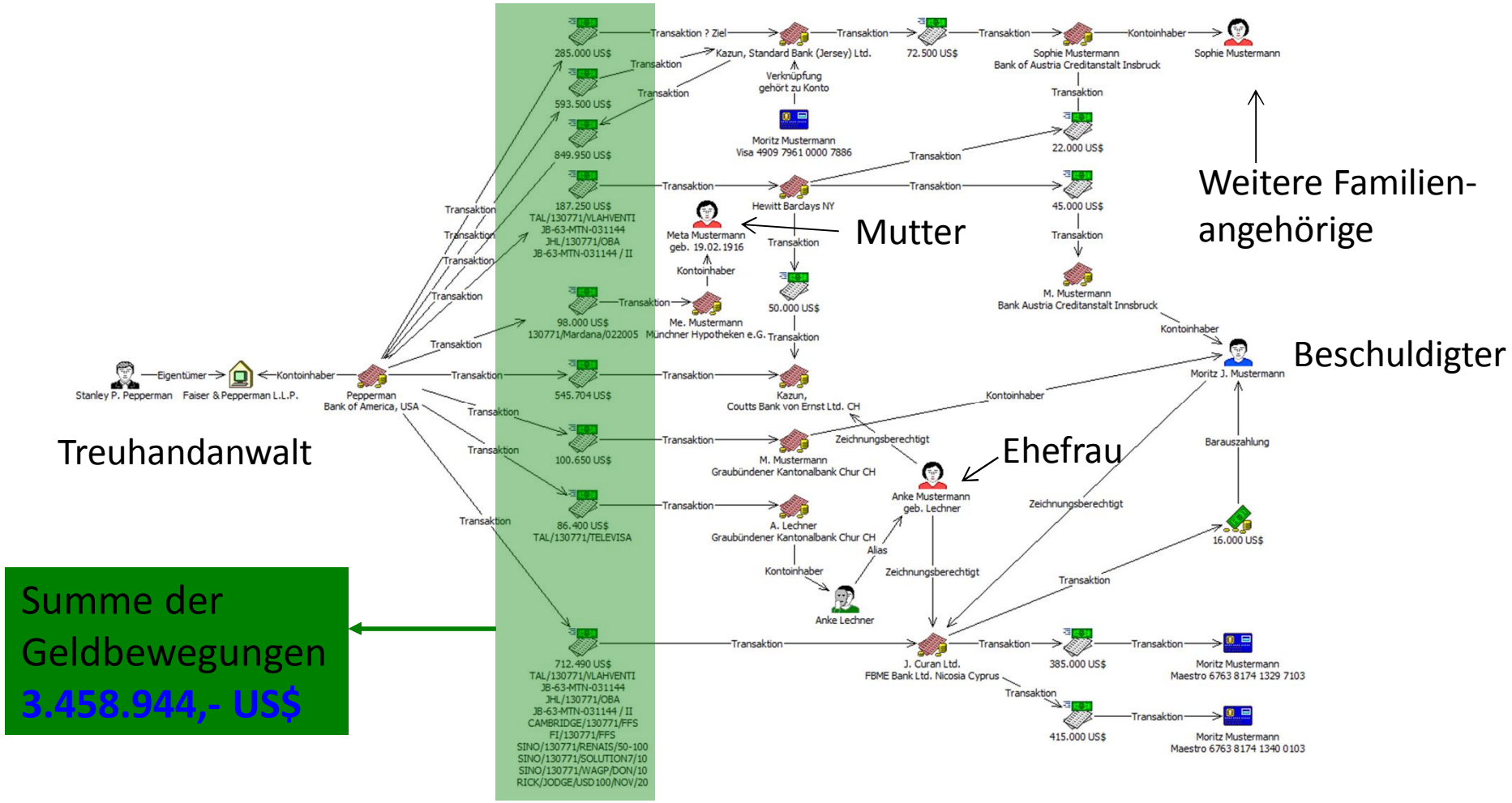
Grafische Darstellungen helfen beim Erkennen von Mustern



z.B. Tochterfirmenverschachtelungen zur Verschleierung der wahren Identität der Täter-gruppe.

Visualisierung unstrukturierter Daten

z.B. Darstellung aller **Geldbewegungen** in Richtung des Beschuldigten



Vielen Dank für Ihre Aufmerksamkeit

FAST-DETECT GmbH

Ehrengutstr. 1
80469 München

Tel. +49 89 461358-0
Fax +49 89 461358-29
info@fast-detect.de
www.fast-detect.de

Geschäftsführer

Thomas Salzberger

Thomas.Salzberger@fast-detect.de