

Forensik Generator für mobile Systeme

Benedikt Bauer
Lehrgebiet Datennetze



- Fragestellung und Zielsetzung
- Motivation und (mögl.) Einsatzzweck
- Analyse der Gegebenheiten
- Umsetzung
- Ergebnisse / Zusammenfassung

Problem: Forensische Methoden/Tools testen

- Beweismittel mehrfach untersuchen,
Ergebnisse vergleichen
 - Zeitaufwändig
 - Vollständigkeit der Untersuchung nicht gewährleistet
 - Woher bekommt man geeignete Beweismittel?
 - Zerstört man evtl. noch benötigte Beweismittel?
 - Bei neuen Geräten gibt es u.U. noch gar keine Methodik

➤ Deshalb: Beweismittel selbst generieren

Generieren von Daten unter Bedingungen:

- Automatisiert
- Schnell
- Realitätsnah
- Nachvollziehbar
- Mit geringem Aufwand

Hier im Fokus: **Android**-Smartphones,
insbesondere Kontakte, Anruflisten, Nachrichten

- Forensiker
Schulung, Tests,
Beweisführung
- Studenten,
Auszubildende,
angehende Forensiker
Ausbildung,
Prüfungsszenarien
- Entwickler
forensischer Software
Basis, Tests,
Funktionsbeweis
- Zertifizierungsstellen
Ergebnisse von
Untersuchungen vergleichen

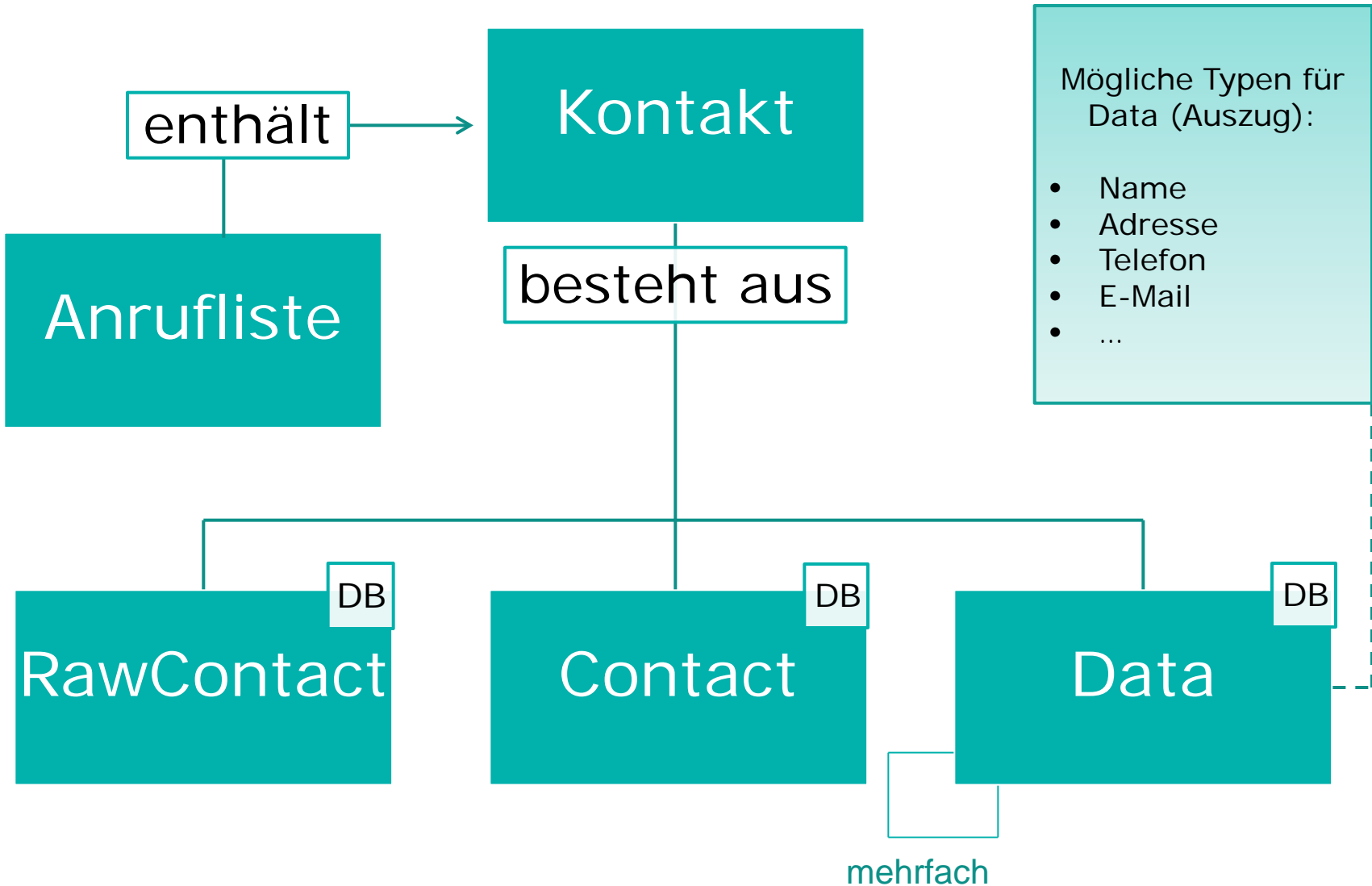
- Grundfunktionen des Telefons sind auch Apps
- Apps speichern Daten in SQLite Datenbanken
- Auslesen innerhalb Android liefert nur Ausschnitt
- Schreibzugriff in Android nur eingeschränkt
- Vollzugriff über Debugging-Schnittstelle aus SDK

- Datenbankstruktur zunächst undurchsichtig (Felder heißen data1, data2,... werden mehrfach verwendet)

mimetype...	raw_co...	data1	data2	data3
1	1	mastach...		
4	2			
8	2	Guido B...	Guido	Bauer

- Bedeutung von Feldern ist abhängig von Eintragstyp, dazu: Beispiel Kontakte

Beispiel: Kontakte



Beispiel: Kontakte

enthält → Kontakt

Mögliche Typen für Data (Auszug):

- Name
- Adresse
- Telefon

data1	data2	data3	data4
Thomas Engel	Thomas	Engel	
SusanneSchreiner@dodgit.com	3	Accord Investments	
Budapester Straße 70Belgweiler...	2	Spaceage Stereo	Budapester Straße 70
0395 46 85 87	1		7858645930

DB
RawContact

DB
Contact

DB
Data

mehrfach

Simulation

1. Datenbank auslesen
2. Neue Daten generieren und in Datenbank einfügen
3. Daten auslesen und verändern
4. Datensatz löschen
5. Datenbank zurück übertragen

Entspricht realer Aktion

- Keine Entsprechung
- Neuer Telefonbucheintrag / Anruf tätigen
- Eintrag ändern, Nachricht ändern
- Eintrag (Telefonbuch / Anrufliste) löschen
- Keine Entsprechung

✓ Aktionen simulieren:

- ✓ Exakte Abbildung der Realität
- ✓ Erfasst auch Änderungen im Hintergrund

– Kontra:

- Zeitaufwändig
- Teilweise unmöglich (autom. Anrufen geht, Annehmen nicht)
- Schwer dokumentierbar
- U.U. kostenintensiv

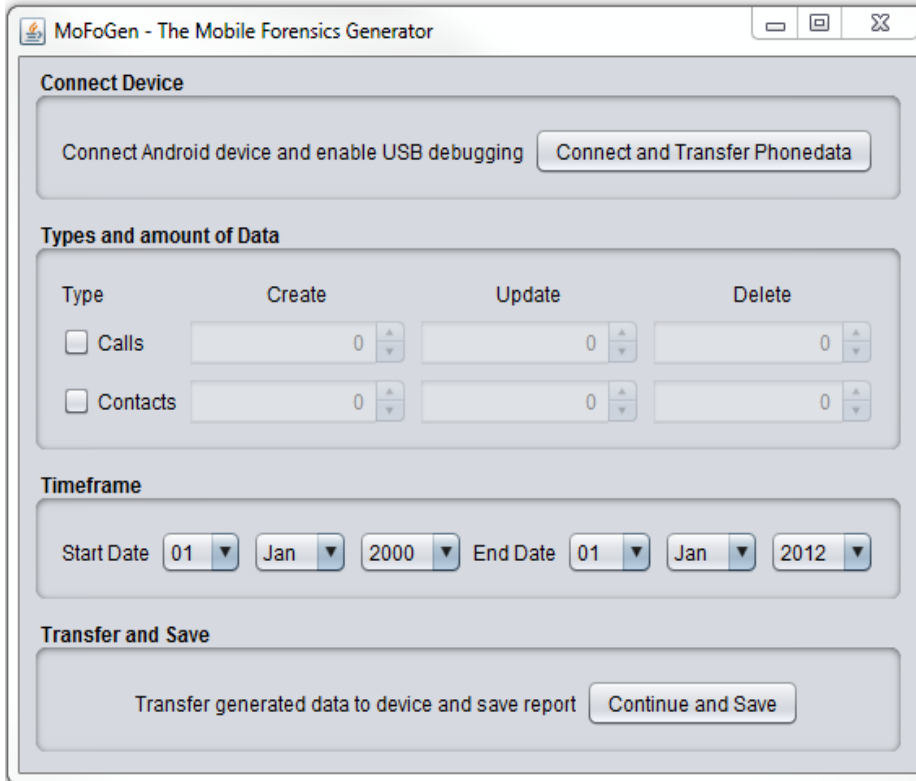
✓ Datenbank erzeugen:

- ✓ Schnell (200 Anrufe in ~10 Sek)
- ✓ Einfach (Daten liegen in SQLite DB)
- ✓ Leicht dokumentierbar (Änderungen bekannt)
- ✓ Kostenfrei

– Kontra:

- Synchronisationsdaten fehlen unter Umständen
- Echtzeiteingaben werden nicht erfasst

MoFoGen – The Mobile Forensics Generator



The screenshot shows the MoFoGen application window with the following sections:

- Connect Device:** A text box with the instruction "Connect Android device and enable USB debugging" and a button labeled "Connect and Transfer Phonedata".
- Types and amount of Data:** A table with columns for "Type", "Create", "Update", and "Delete".

Type	Create	Update	Delete
<input type="checkbox"/> Calls	0	0	0
<input type="checkbox"/> Contacts	0	0	0
- Timeframe:** Fields for "Start Date" (01, Jan, 2000) and "End Date" (01, Jan, 2012).
- Transfer and Save:** A text box with the instruction "Transfer generated data to device and save report" and a button labeled "Continue and Save".

- Anwendung fragt Rahmenbedingungen ab und erstellt passende Datenbank
 - Art der erzeugten Daten (Anrufe, Kontakte etc.)
 - Anzahl der Datensätze je Typ und Aktion (bspw.: 10 erstellen, 5 ändern, 3 löschen)
 - Zeitraum für generierte Daten (bspw.: 1.1.–1.4.2012)

- Anwendung erstellt 100 Datensätze in 5-10 Sek.
- Vergleich generierter und echter Daten:
 - In der Benutzeroberfläche (nach Neustart) nicht unterscheidbar
 - Zeitstempel der Datenbankdateien beziehen sich auf Zeitpunkt der Übertragung
 - Synchronisationsinformationen werden bei nächstem Abgleich eingetragen, fehlen bei Übertragung noch
 - Herstellerspezifische Zusatzfelder werden nicht ausgefüllt
 - Basisfelder des Android Systems werden identisch gefüllt

- Android-Schnittstellen sind universell einsetzbar um weitere Daten auszulesen und zu verändern
 - Meine Arbeit befasst sich nur mit zentralen Android Komponenten (Kontakte, Anrufe, Nachrichten)
 - Erweiterungsmöglichkeit: Drittanbieter App-Daten (bspw.: Soziale Netzwerke, Messenger, Notizen)
- Automatisierte Tests durch Kombination aus Generator und Untersuchungssoftware
- Szenarios erstellen
 - Inhalte vorgeben um realistische Fälle für Schulung zu konstruieren
 - Person A kontaktiert Person B über 4 Wochen täglich per SMS und E-Mail

Vielen Dank für Ihre Aufmerksamkeit

