FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Forensische Untersuchung von Social Media Apps

Carsten Crampen
Lehrgebiet Datennetze

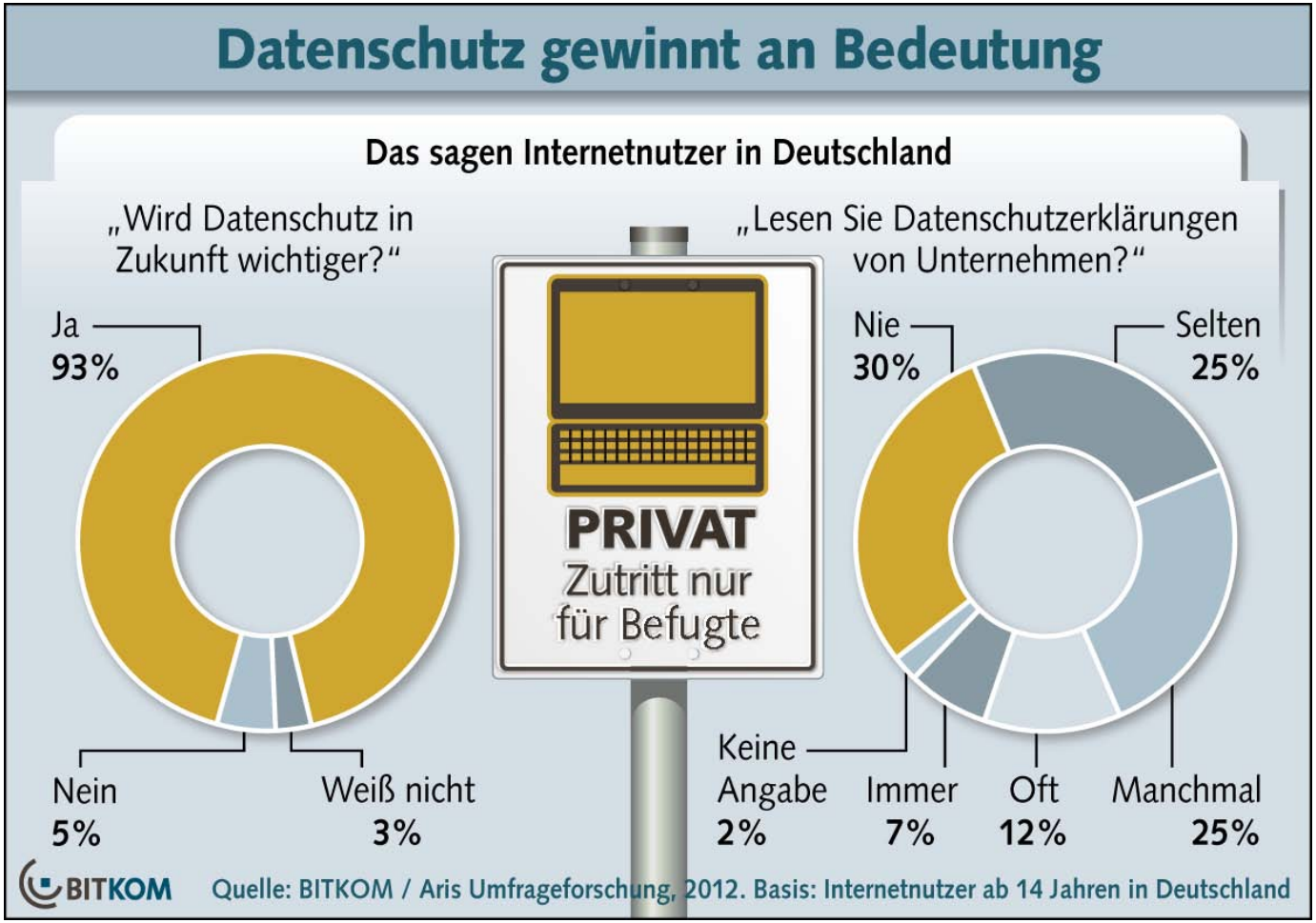
IT Forensik
FH Aachen

Gliederung

- Einleitung
- Aufgabenstellung
- Herangehensweise
- Vorgehensweise
- Ergebnisse
- Fazit

Einleitung

- Datenschutz auf Smartphones?



Aufgabenstellung

Was speichert mein Smartphone?

- Nachrichten, Bilder, Status, Standorte, usw.

Social Media Apps

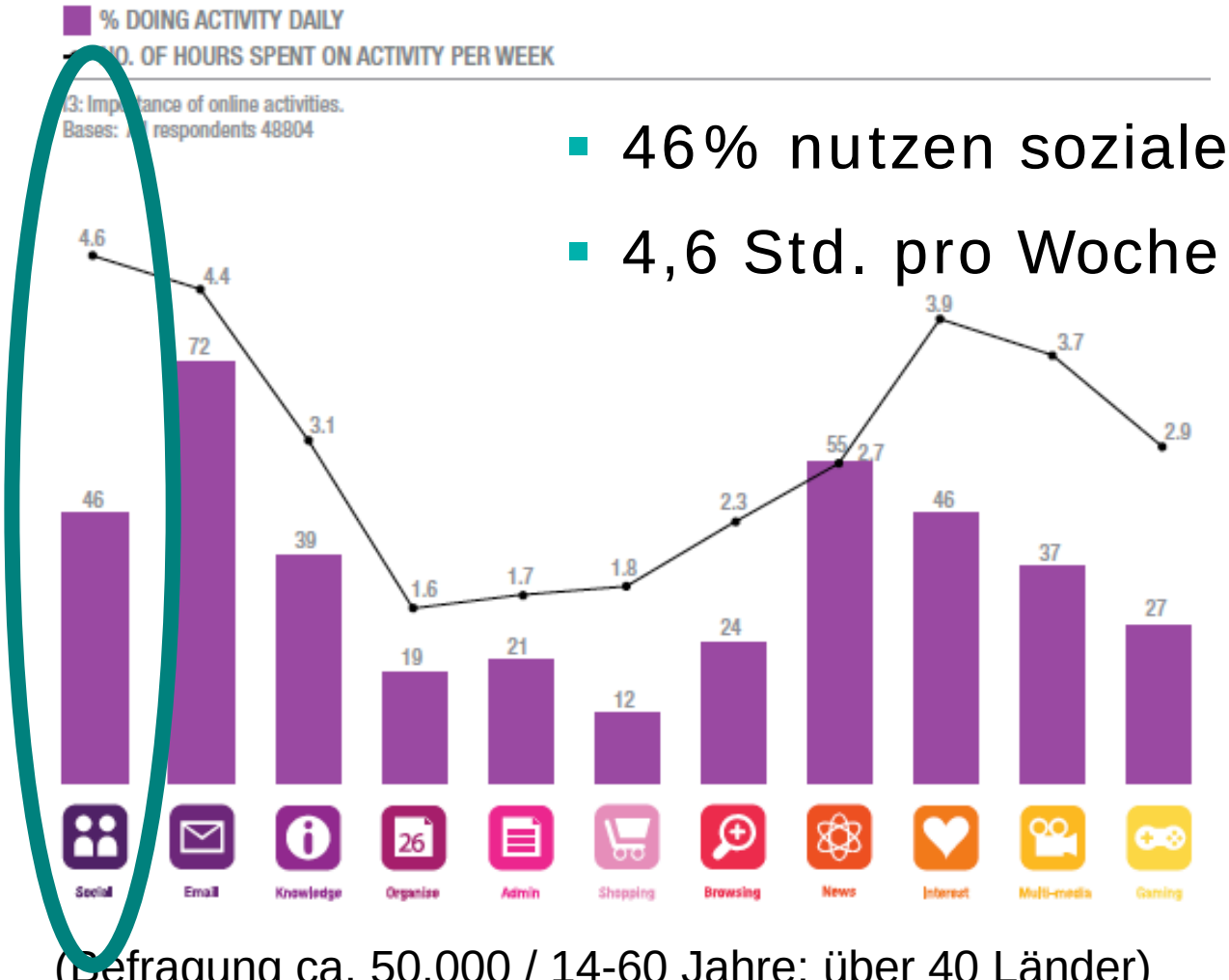
Aufgabenstellung

Wie bzw. welche Daten finde ich auf dem Smartphone?

- erwartete Daten
  - Benutzernamen, E-Mail-Adressen, Passwörter
  - Handynummern
  - Statusmitteilungen, Nachrichten-Verläufe
  - Bilder

Aufgabenstellung

Übersicht: Internet-Nutzung auf Smartphones



- 46% nutzen soziale Netzwerke täglich
- 4,6 Std. pro Woche

(Befragung ca. 50.000 / 14-60 Jahre; über 40 Länder)

Quelle: Digital Life (NeedScope)

Herangehensweise

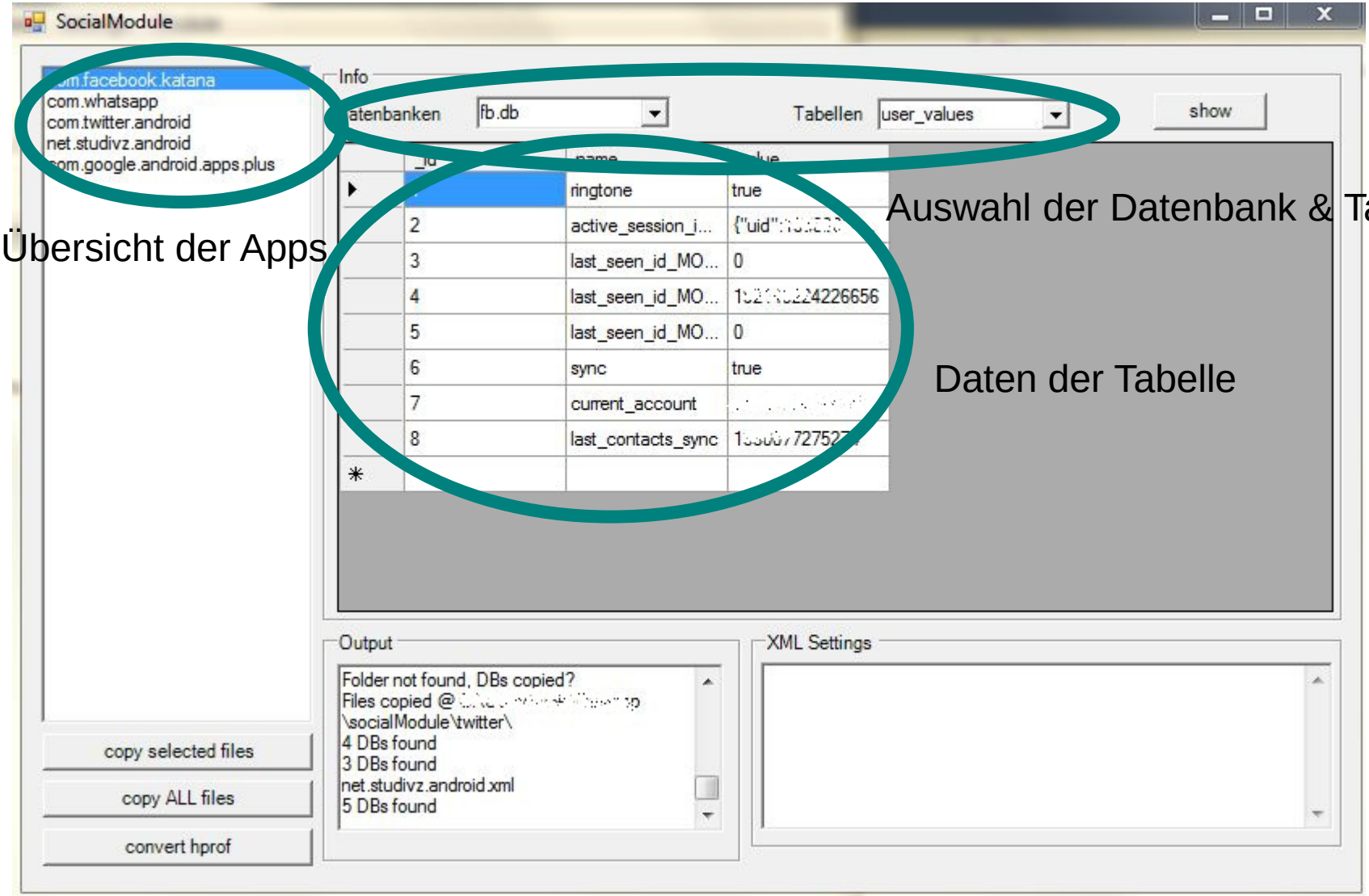
- Untersuchungen auf anderen Plattformen
- forensische Untersuchung sozialer Netzwerke
  - öffentliches Profil
  - Browserverlauf & Cookies
  - Arbeitsspeicher- & Festplattenanalyse
- Untersuchung auf Smartphone
  - der Speicherabbilder
  - der gespeicherten Daten / Datenbanken (/data/ - Partition)
- Administratorberechtigungen werden auf dem Smartphone benötigt

Vorgehensweise

- Anschluss und „Rooten“ des Smartphones
- Zugriff auf /data/ - Partition über Android Debug Bridge (Konsole)
- Speicherorte der Apps:
  z.B. /data/data/com.facebook.katana
- Auslesen der Datenbank-Files (SQLite-Dateien), Konfigurationsdateien (XML-Dateien)
- Auslesen automatisiert und im Android Forensic Toolkit integriert

Vorgehensweise

Android Forensic Toolkit



Übersicht der Apps

Auswahl der Datenbank & Tabellen

Daten der Tabelle

Untersuchung der Apps

Untersuchung der Apps

- Facebook:

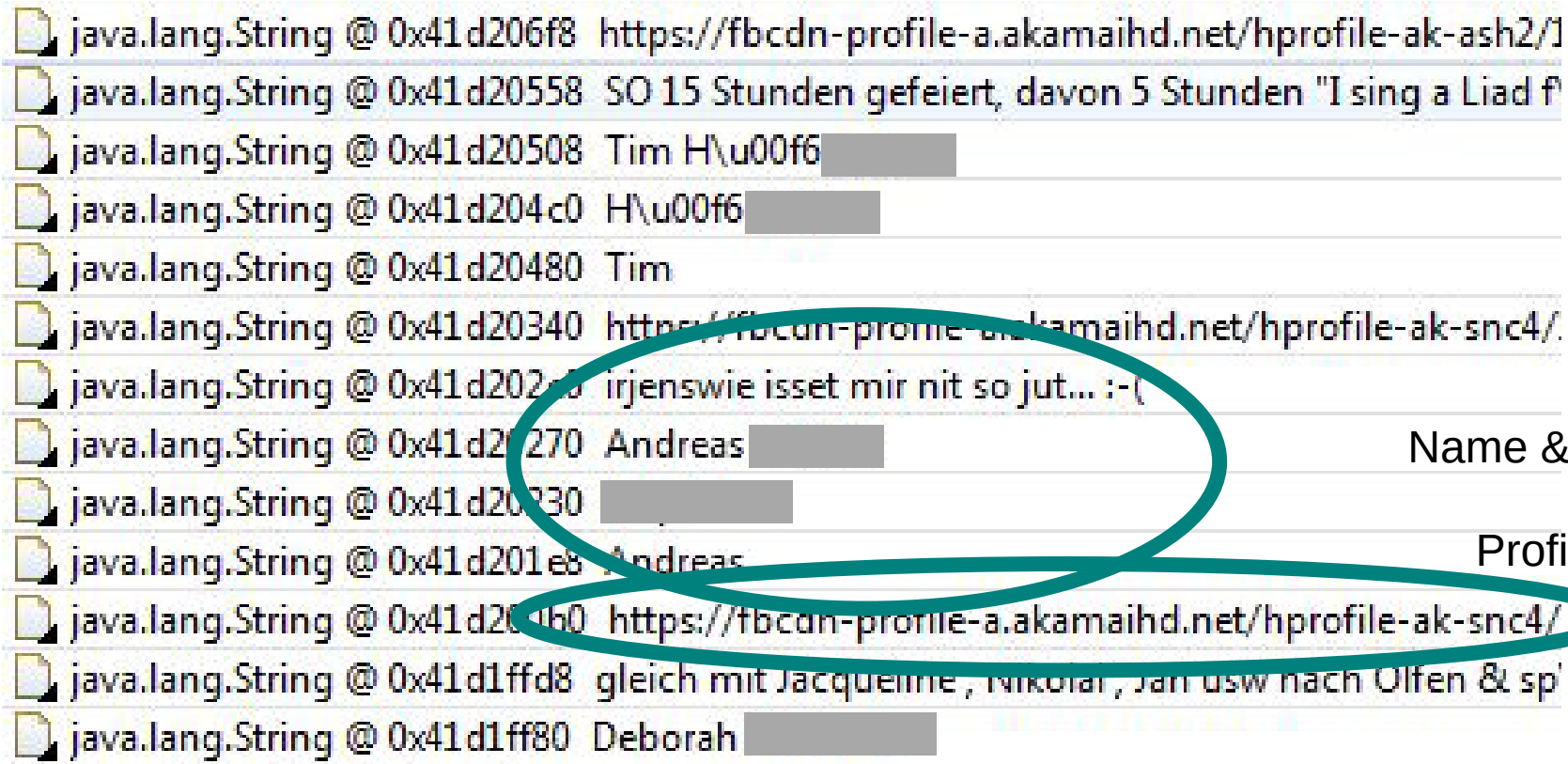
Profilbild

Name & Status

Uhrzeit & Ort

Untersuchung der Apps

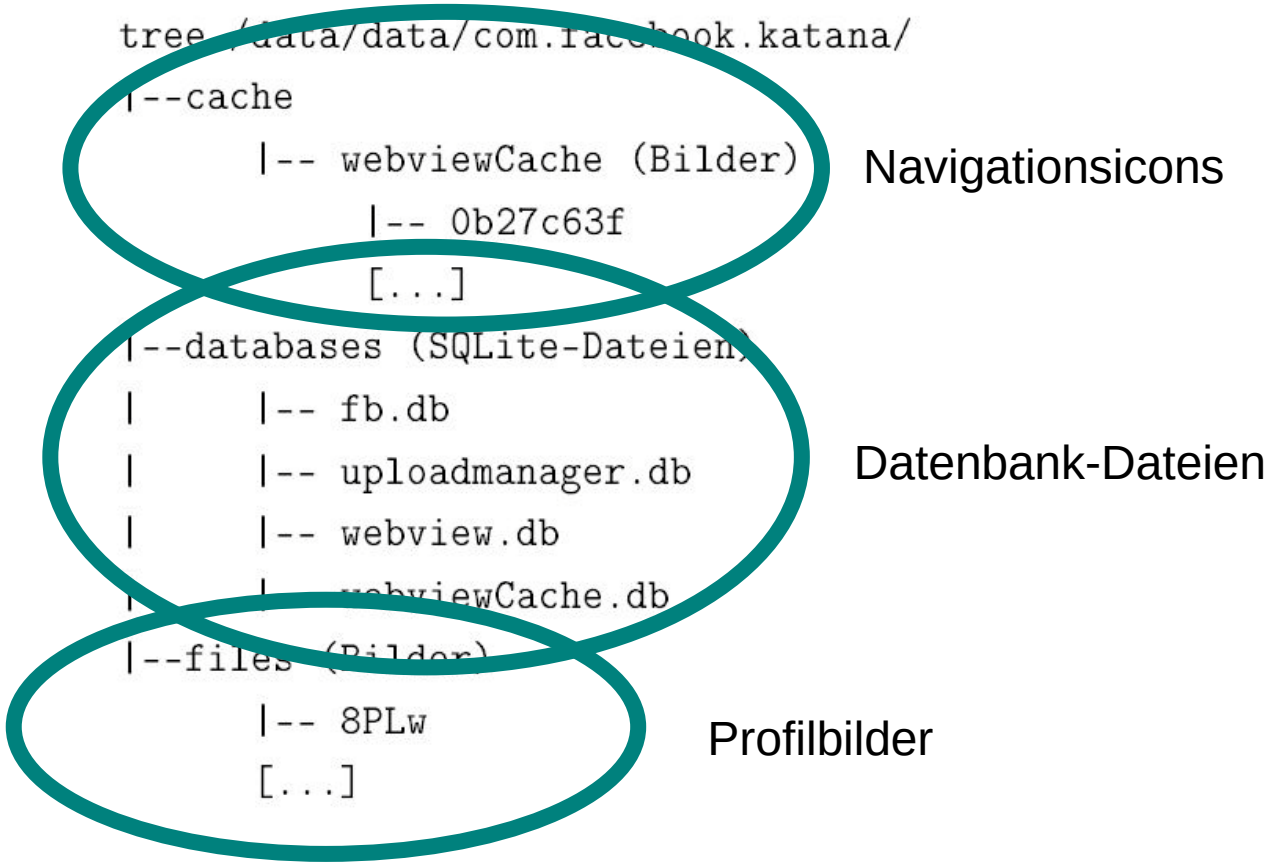
- Facebook:
  - Speicherabbild



  - **nicht** zusammenhängende Nachrichten

Untersuchung der Apps

- Facebook:
  - Datenstruktur:



Untersuchung der Apps

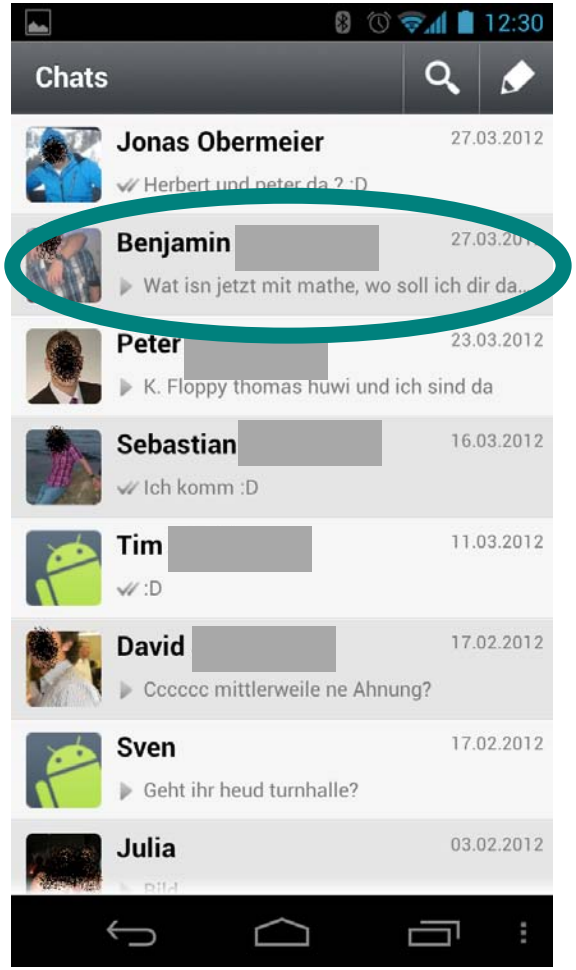
- Facebook:
  - Freundesliste mit Benutzernamen, Geburtstagen, registrierten E-Mail-Adresse
  - hochzuladene Bilder
  - AccessToken:


```
{
   "data": [
      {
         "id": "2361[illegible]017789",
         "from": {
            "name": "[illegible]",
            "id": "1558[illegible]5060"
         },
         "tags": {
            "data": [
               {
                  "id": "100003134636747",
                  "name": "Daniel [illegible]",
                  "created_time": "2011-09-22T21:59:34+0000"
               },
               {
                  "id": "162[illegible]370",
                  "name": "[illegible]",
                  "created_time": "2011-09-22T19:19:21+0000"
               },
               {
                  "id": "155[illegible]060",
                  "name": "Patrick [illegible]",
                  "created_time": "2011-09-22T19:18:55+0000"
               },
```


(Rückgabe direkt durch Facebook)

Untersuchung der Apps

- WhatsApp:



Profilbild

Uhrzeit

Name & Nachricht

Handynummer Absender

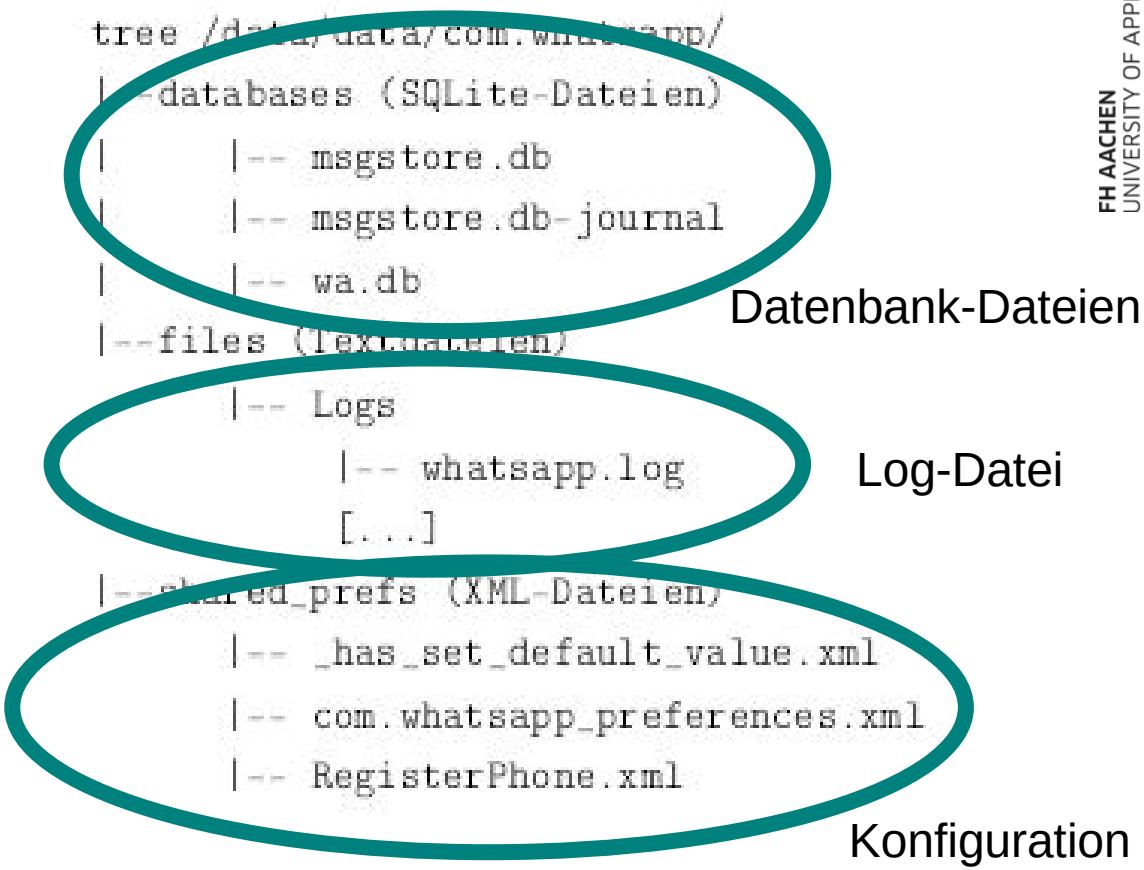
Zeitstempel

6	491632877783@s.whats...		1324850...	5	0	jo aber noch kurz	1324852438532
7	491632877783@s.whats...	1	1324850...	5	0	Stehen Grade drin;	1324852455021
8	491632877783@s.whats...		1324762...	0	0	ch' meinste ? Ja kommen gleich	1324852495216

Nachrichten

Untersuchung der Apps

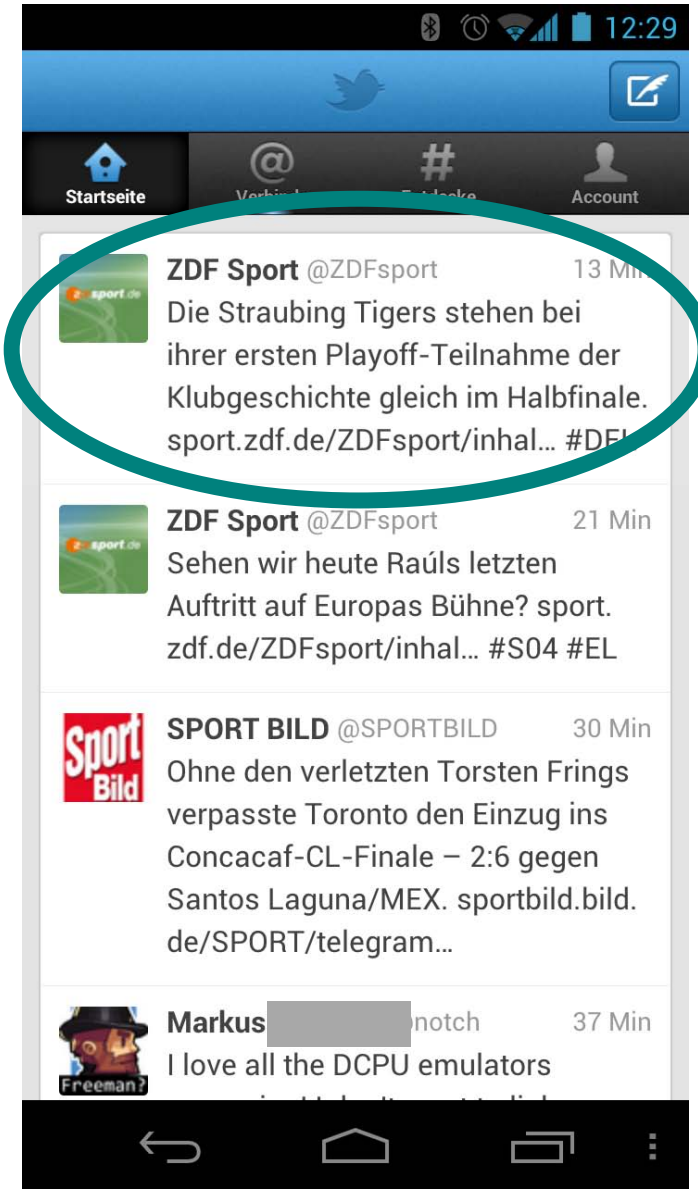
- WhatsApp:



- Nutzen:
  - Handynummern
  - Nachrichtenverläufe
  - Telefoninfos

Untersuchung der Apps

- Twitter:



Profilbild

Uhrzeit

Name & Status

Untersuchung der Apps

- Twitter:

Ordnerstruktur & Dateien

```
tree /data/data/com.twitter.android/
|--databases
|      |-- 0.db
|      |-- 0.db-journal
|      |-- 82657022.db
|      |-- 82657022.db-journal
|      |-- 460623142.db
|      |-- 460623142.db-journal
|      |-- global.db
|      |-- global.db-journal
|      |-- c2dm.xml
|      |-- com.twitter.android_preferences.xml
|      |-- ConnectActivity.xml
|      |-- discover_prefs.xml
|      |-- HomeActivity.xml
|      |-- HomeTabActivity.xml
|      |-- PostActivity.xml
|      |-- profile_prefs.xml
|      |-- search_prefs.xml
```

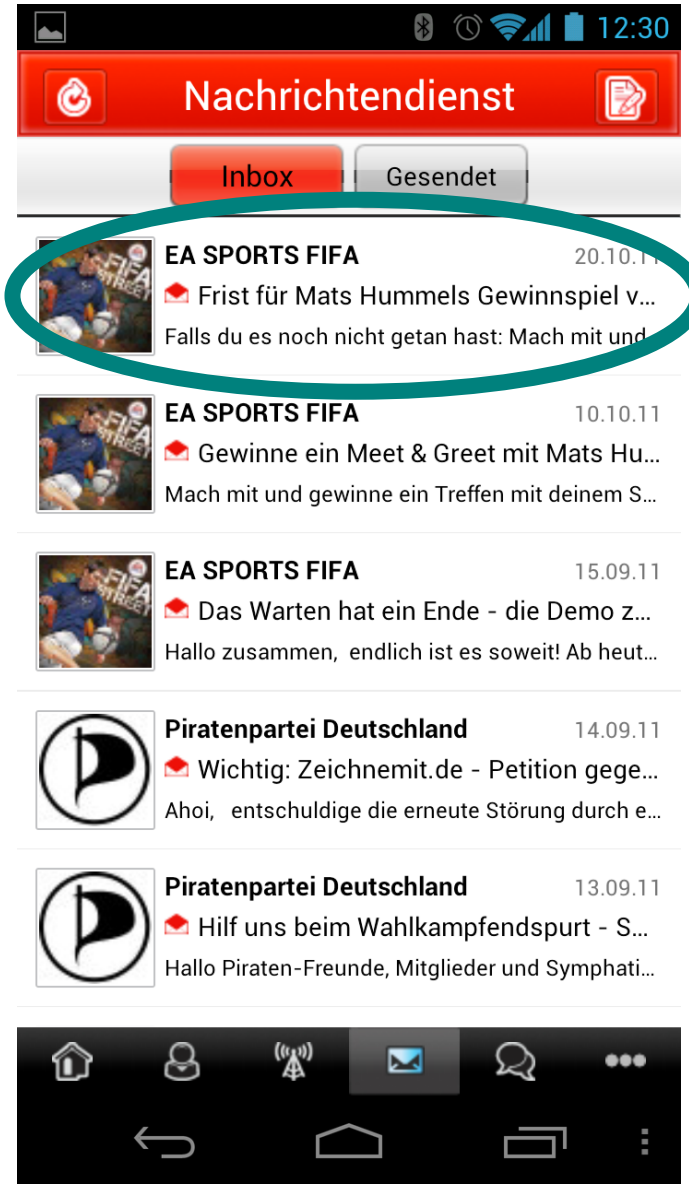
Datenbank-Dateien

Konfiguration

- Nutzen:
  - Nachrichtenverläufe (offline)
  - Eingerichtete Benutzer

Untersuchung der Apps

- StudiVZ:



Profilbild

Datum

Name, Betreff, Nachricht

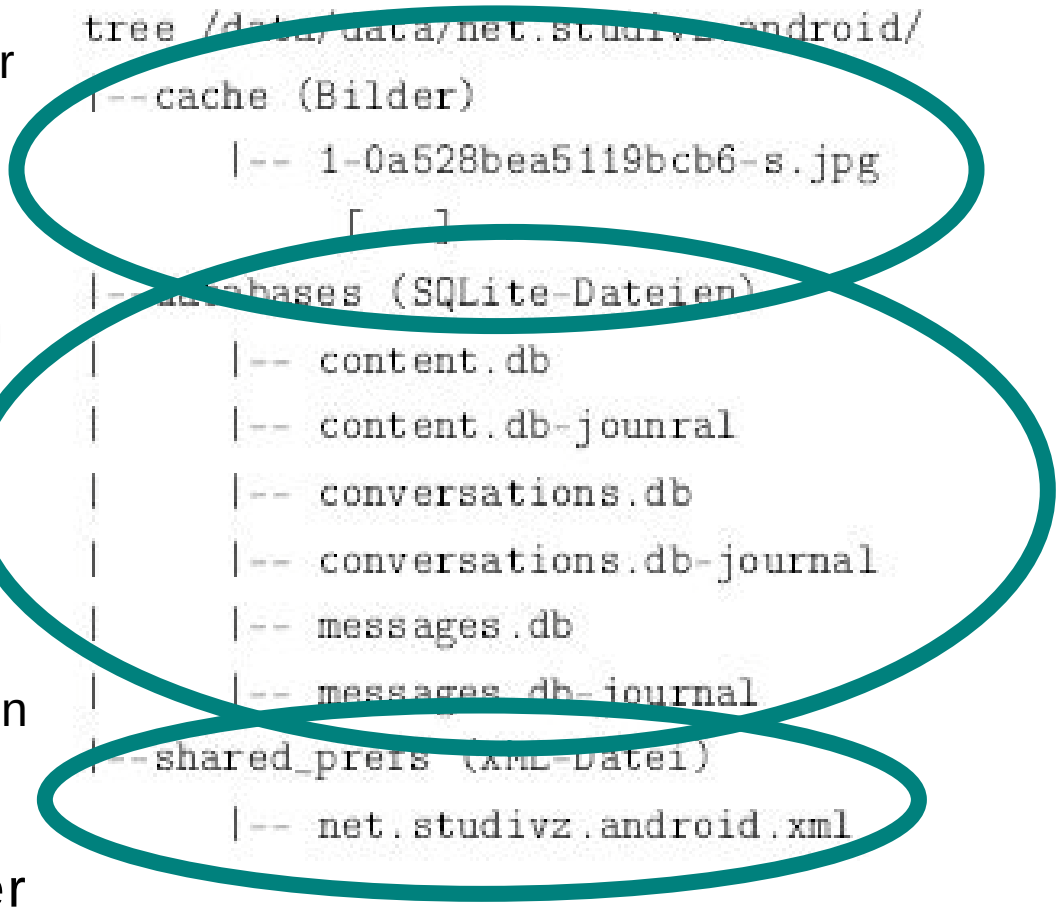
Untersuchung der Apps

- StudiVZ:

Profilbilder

Datenbank-Dateien

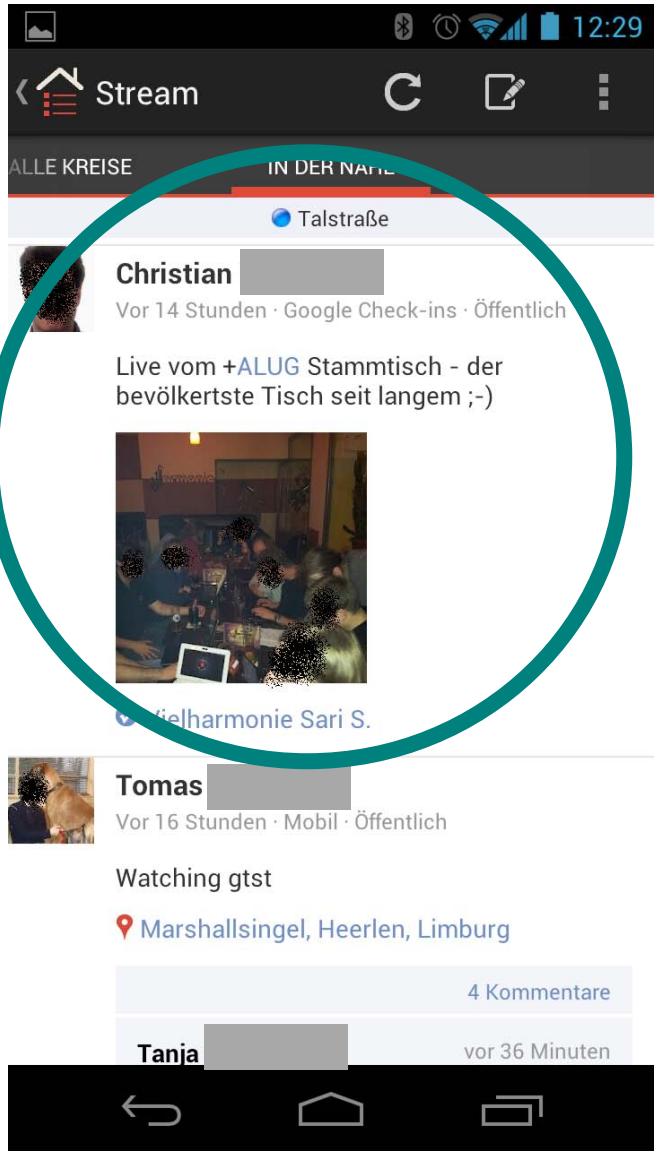
Konfiguration



- Nutzen:
  - Keine Infos, nur Bilder
  - Benutzername / Passwort im Klartext in Konfigurationsdatei

Untersuchung der Apps

- Google+:



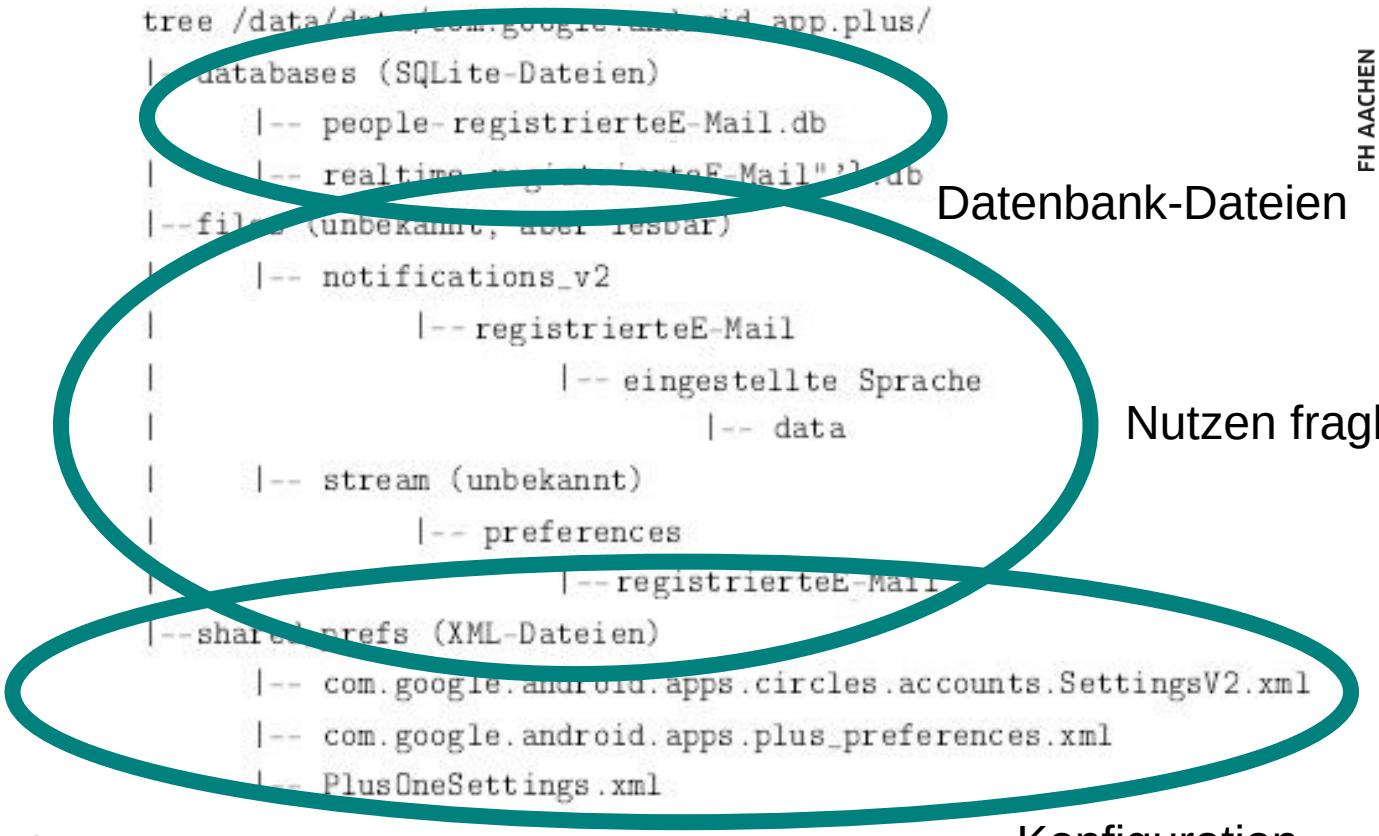
Profilbild

Uhrzeit & Ort

Name & Status

Untersuchung der Apps

- Google+:



- Nutzen:
  - Freundeslisten
  - Kontakte (auch außerhalb der App)
  - Nachrichtenverläufe

Fazit

- lokale Datenspeicherung bei allen Apps
- fraglich, warum Daten gespeichert werden
-  Facebook & StudiVZ – Datenzugriff durch Dritte möglich
- Smartphone-Verlust bedeutet „Sperren“
  - Sperren beim Netzbetreiber, Passwort-Änderungen in Netzwerken, Schließen aktiver Sessions in Netzwerken
- schnelllebiger Bereich
  - Versionsunterschiede der Apps und Betriebssysteme bedeuten evtl. unterschiedliche Untersuchungsergebnisse

Danke für Ihre Aufmerksamkeit!