

Forensische Untersuchung von Social Media Apps

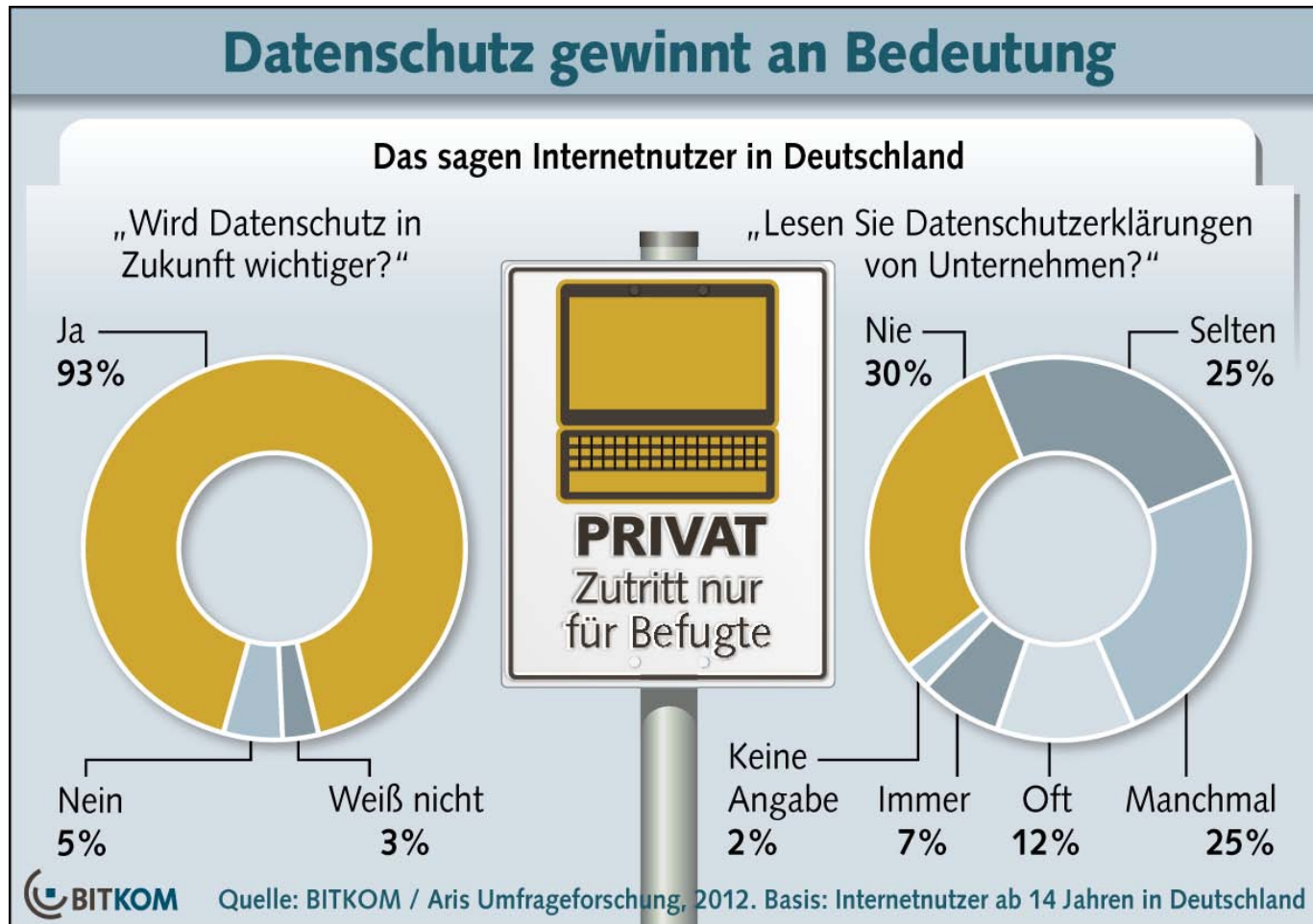
Carsten Crampen
Lehrgebiet Datennetze



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



■ Datenschutz auf Smartphones?



Was speichert mein Smartphone?

- Nachrichten, Bilder, Status, Standorte, usw.

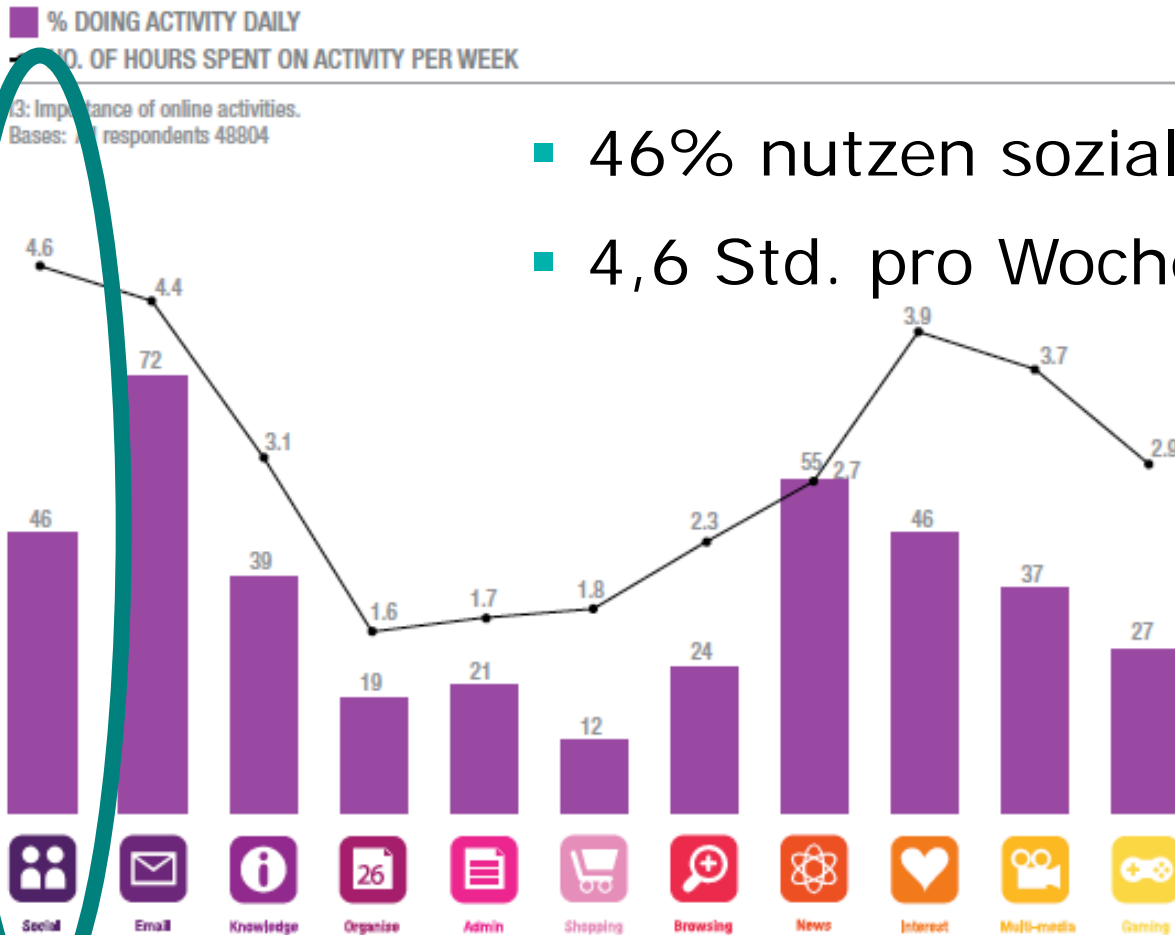
Social Media Apps



Wie bzw. welche Daten finde ich auf dem Smartphone?

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

Übersicht: Internet-Nutzung auf Smartphones



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

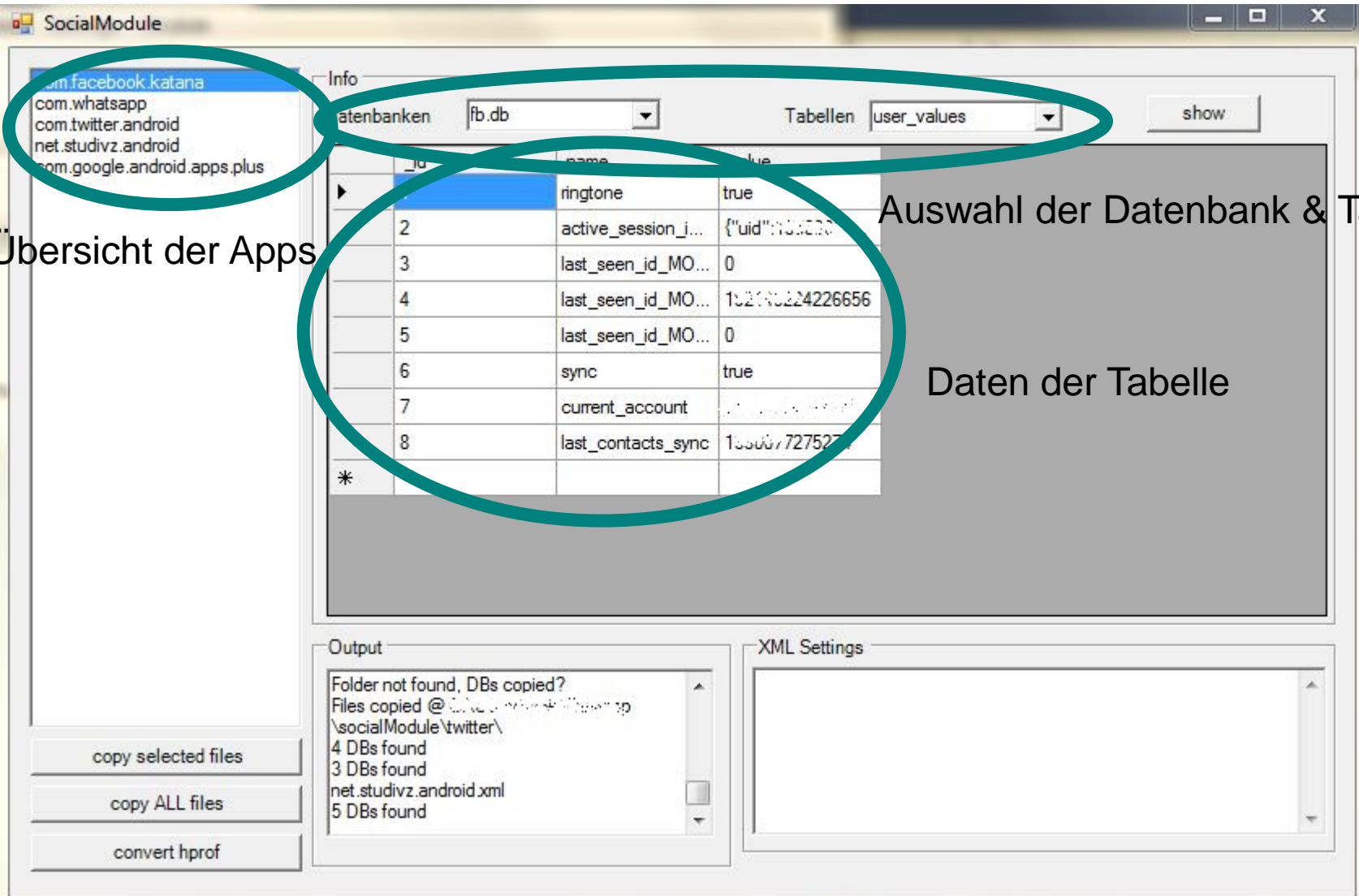
(Befragung ca. 50.000 / 14-60 Jahre; über 40 Länder)

Quelle: Digital Life (NeedScope)

- 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

- 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

Android Forensic Toolkit



The screenshot shows the SocialModule application interface. On the left, a list of applications is displayed, with several entries circled in green. The main area shows the selected database 'fb.db' and table 'user_values'. Below this, a table of data is shown, also circled in green. At the bottom, there are sections for 'Output' and 'XML Settings'.

Übersicht der Apps

Auswahl der Datenbank & Tabellen

Daten der Tabelle

ID	name	value
1	ringtone	true
2	active_session_j...	{\"uid\":\"000000
3	last_seen_id_MO...	0
4	last_seen_id_MO...	152190224226656
5	last_seen_id_MO...	0
6	sync	true
7	current_account	...
8	last_contacts_sync	155007727527...

Output:
Folder not found, DBs copied?
Files copied @ ...
4 DBs found
3 DBs found
net.studivz.android.xml
5 DBs found



■ Facebook:



Profilbild

Name & Status

Uhrzeit & Ort

- Facebook:

- Speicherabbild

java.lang.String @ 0x41d206f8	https://fbcdn-profile-a.akamaihd.net/hprofile-ak-ash2/	
java.lang.String @ 0x41d20558	SO 15 Stunden gefeiert, davon 5 Stunden "I sing a Lied f	
java.lang.String @ 0x41d20508	Tim H\u00f6	
java.lang.String @ 0x41d204c0	H\u00f6	
java.lang.String @ 0x41d20480	Tim	
java.lang.String @ 0x41d20340	https://fbcdn-profile-a.akamaihd.net/hprofile-ak-snc4/	
java.lang.String @ 0x41d20280	irjenswie isset mir nit so jut... :-)	
java.lang.String @ 0x41d20270	Andreas	Name & Status
java.lang.String @ 0x41d20230		
java.lang.String @ 0x41d201e8	Andreas	Profilbild
java.lang.String @ 0x41d201b0	https://fbcdn-profile-a.akamaihd.net/hprofile-ak-snc4/	
java.lang.String @ 0x41d1ffd8	gleich mit Jacqueline , Nikolai , Jan usw nach Olfen & sp'	
java.lang.String @ 0x41d1ff80	Deborah	

- nicht** zusammenhängende Nachrichten

- Facebook:
 - Datenstruktur:

```
tree /data/data/com.facebook.katana/
```

```
|--cache
```

```
  |-- webViewCache (Bilder)
```

```
    |-- 0b27c63f
```

```
    [...]
```

Navigationssicons

```
|--databases (SQLite-Dateien)
```

```
|  |-- fb.db
```

```
|  |-- uploadmanager.db
```

```
|  |-- webView.db
```

```
|  |-- webViewCache.db
```

Datenbank-Dateien

```
|--files (Bilder)
```

```
  |-- 8PLw
```

```
  [...]
```

Profilbilder

■ Facebook:

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

▫ AccessToken:

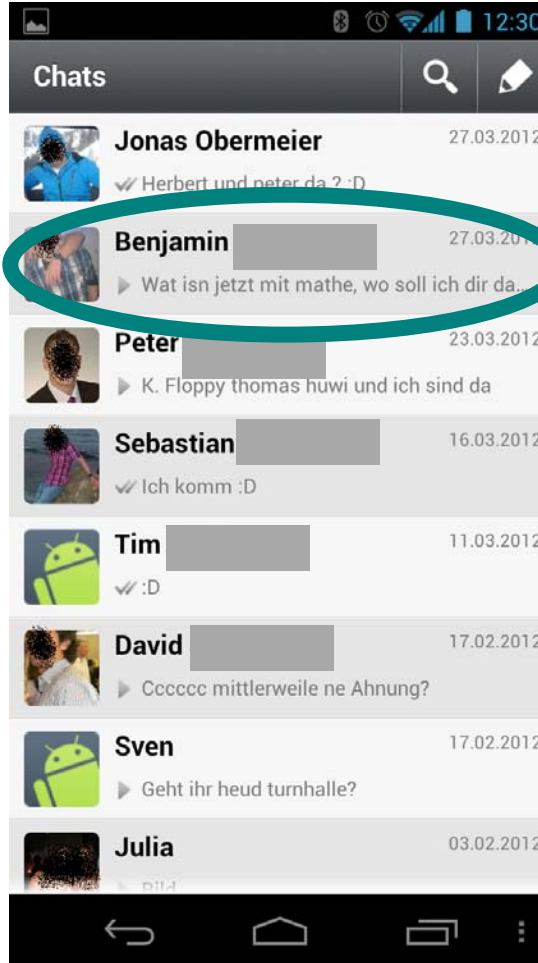
```

{
  "data": [
    {
      "id": "2361000017789",
      "from": {
        "name": "Facebook Webservice",
        "id": "1558985060"
      },
      "tags": {
        "data": [
          {
            "id": "100000134636747",
            "name": "Daniel Gernsbein",
            "created_time": "2011-09-22T21:59:34+0000"
          },
          {
            "id": "1623001370",
            "name": "Facebook User",
            "created_time": "2011-09-22T19:19:21+0000"
          },
          {
            "id": "1558985060",
            "name": "Patrick Weisler",
            "created_time": "2011-09-22T19:18:55+0000"
          }
        ]
      }
    }
  ]
}

```

(Rückgabe direkt durch Facebook)

■ WhatsApp:



Profilbild

Uhrzeit
Name & Nachricht

Handynummer Absender

Zeitstempel

6	491632877783@s.whats...	1	1324850...	5	0	so aber noch kurz	1324852438532
7	491632877783@s.whats...	1	1324850...	5	0	Stehen Grade drin;	1324852455021
8	491632877783@s.whats...	0	1324762...	0	0	h' meinste ? ^{ET} Ja kommen gleich	1324852495216

Nachrichten

■ WhatsApp:

```
tree /data/data/com.whatsapp/
|--databases (SQLite-Dateien)
|   |-- msgstore.db
|   |-- msgstore.db-journal
|   |-- wa.db
|--files (Textdateien)
```

Datenbank-Dateien

```
    |-- Logs
        |-- whatsapp.log
        [...]
    |--shared_prefs (XML-Dateien)
```

Log-Datei

```
        |-- _has_set_default_value.xml
        |-- com.whatsapp_preferences.xml
        |-- RegisterPhone.xml
```

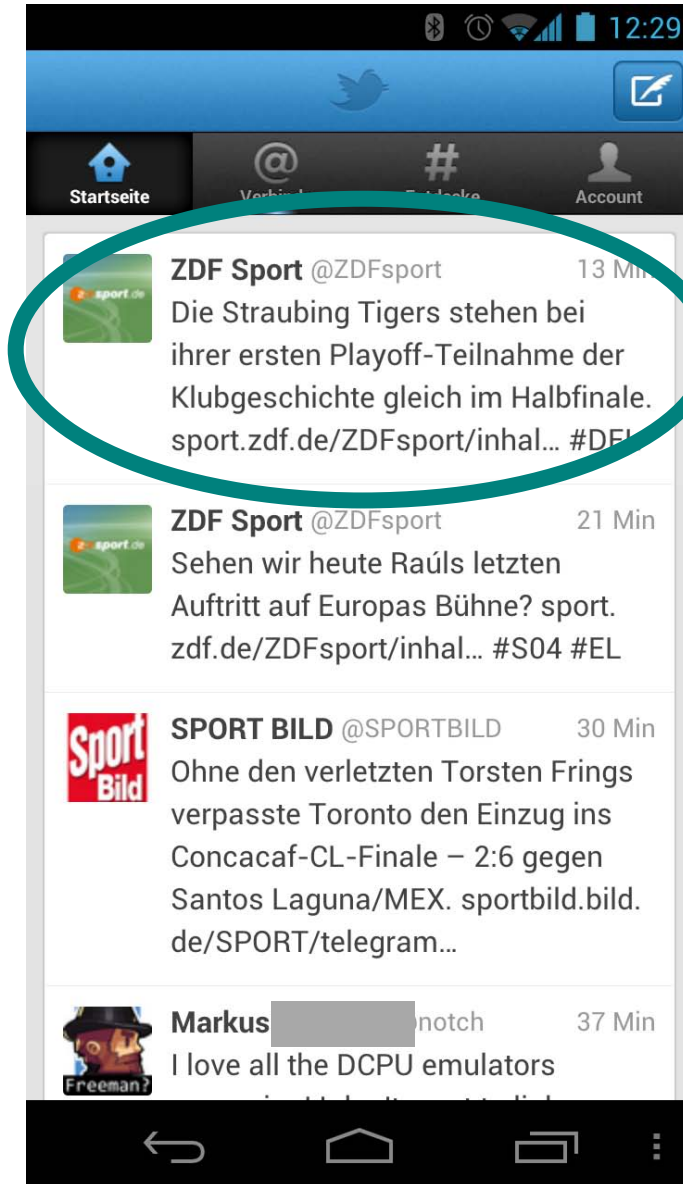
Konfiguration

■ Nutzen:

- Handynummern
- Nachrichtenverläufe
- Telefoninfos

- Twitter:

Profilbild



Uhrzeit

Name & Status

■ Twitter:

Datenbank-Dateien

Konfiguration

Ordnerstruktur & Dateien

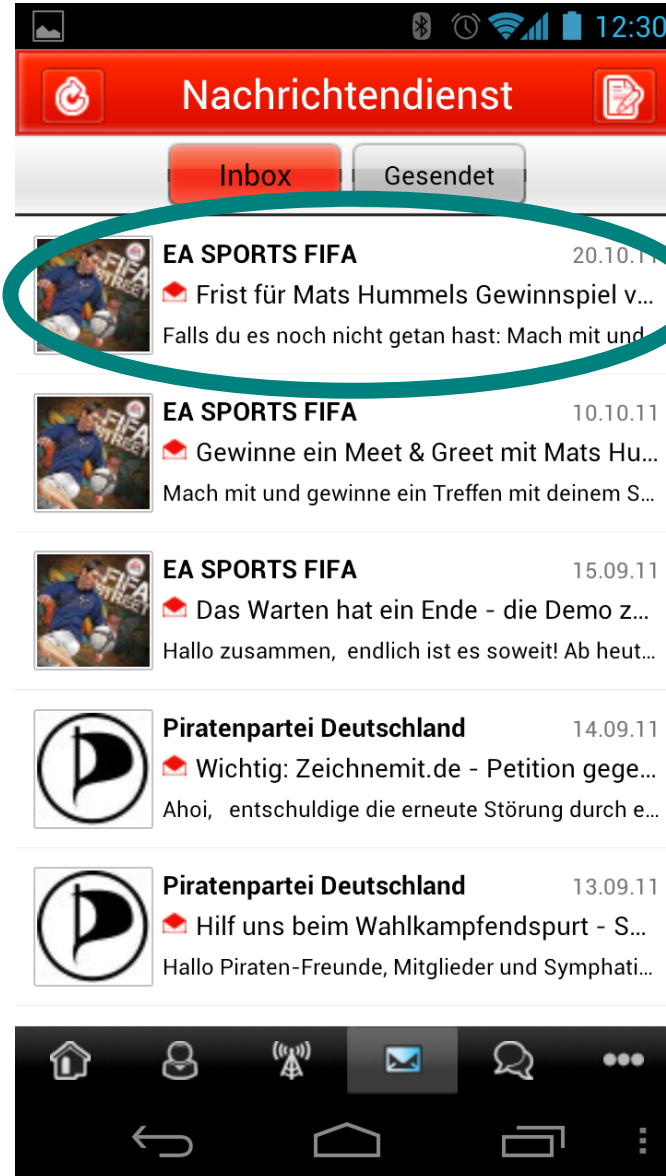
```
tree /data/.../twitter.android/
|--databases
|   |-- 0.db
|   |-- 0.db-journal
|   |-- 82657022.db
|   |-- 82657022.db-journal
|   |-- 460623142.db
|   |-- 460623142.db-journal
|   |-- global.db
|   |-- global.db-journal
|--shared_prefs
|   |-- c2dm.xml
|   |-- com.twitter.android.preferences.xml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

■ Nutzen:

- Nachrichtenverläufe (offline)
- Eingerichtete Benutzer

■ StudiVZ:

Profilbild



Datum

Name, Betreff, Nachricht

■ StudiVZ:

Profilbilder

```
tree /data/data/net.studivz.android/
```

```
|--cache (Bilder)
```

```
    |-- 1-0a528bea5119bcb6-s.jpg
```

```
    [ ]
```

Datenbank-Dateien

```
|--databases (SQLite-Dateien)
```

```
    |-- content.db
```

```
    |-- content.db-journal
```

```
    |-- conversations.db
```

```
    |-- conversations.db-journal
```

```
    |-- messages.db
```

```
    |-- messages.db-journal
```

Konfiguration

```
|--shared_prefs (XML-Datei)
```

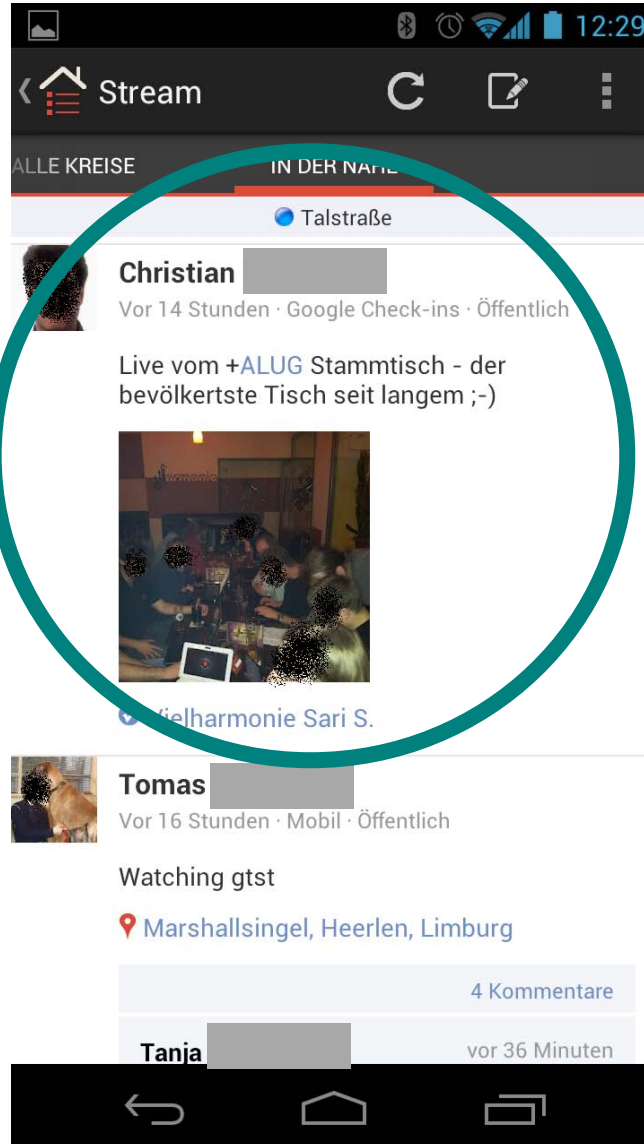
```
    |-- net.studivz.android.xml
```

■ Nutzen:

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

■ Google+ :

Profilbild



Uhrzeit & Ort

Name & Status

■ Google+ :

```

tree /data/data/com.google.android.app.plus/
| databases (SQLite-Dateien)
|   |-- people-registrierteE-Mail.db
|   |-- realtime-registrierteE-Mail"'.db
|-- files (unbekannt, aber lesbar)
|   |-- notifications_v2
|       |-- registrierteE-Mail
|           |-- eingestellte Sprache
|               |-- data
|   |-- stream (unbekannt)
|   |-- preferences
|       |-- registrierteE-Mail
|-- shared_prefs (XML-Dateien)
|   |-- com.google.android.apps.circles.accounts.SettingsV2.xml
|   |-- com.google.android.apps.plus_preferences.xml
|   |-- PlusOneSettings.xml
  
```

Datenbank-Dateien

Nutzen fraglich

Konfiguration

■ Nutzen:

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

- lokale Datenspeicherung bei allen Apps
- fraglich, warum Daten gespeichert werden
-  Facebook & StudiVZ – Datenzugriff durch Dritte möglich
- Smartphone-Verlust bedeutet „Sperrern“
 - 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!