

IT-forensische Analyse von App-Daten auf Android-Smartphones

Jens Weidhase

Absolvent B.Sc. FH-Aachen

Master ITS (RUB)



- Motivation / Ziel
- App-Entwicklung
- Analyse der App-Daten
- Vorstellung Android-Forensic-Toolkit
- Zusammenfassung

- Smartphones bieten eine Vielzahl von Daten
- Klassische Daten
 - Kontakte
 - Anrufliste
 - SMS
- Moderne Daten
 - GPS (Geo-Daten)
 - WLAN
 - Internet Cache
 - Kennwörter
 - Bilder
 - etc.
 - Daten unterschiedlichster Apps



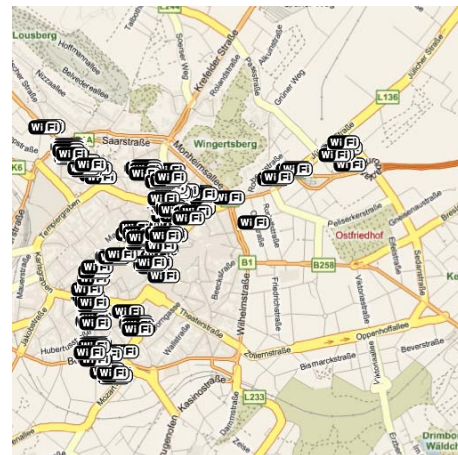
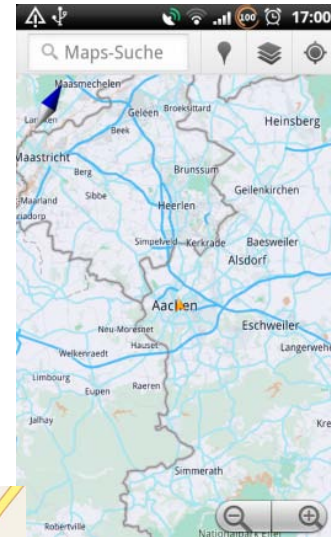
■ Ziel:

- Geo-Daten finden
- Geo-Daten exportieren
- Geo-Daten auswerten



■ Wichtig dabei:

- Erweiterbarkeit
 - neue Apps, die Geo-Daten speichern, sollen einfach zu integrieren sein

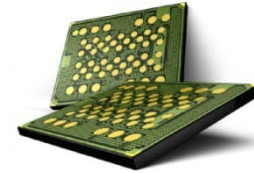


- Motivation / Ziel
- App-Entwicklung
- Analyse der App-Daten
- Vorstellung Android-Forensic-Toolkit
- Zusammenfassung



■ Speichermöglichkeiten

- Interner Speicherplatz
- Externer Speicherplatz
- Shared Preferences
- SQLite Datenbanken
- Netzwerkverbindungen



- Motivation / Ziel
- App-Entwicklung
- Analyse der App-Daten
- Vorstellung Android-Forensic-Toolkit
- Zusammenfassung

- Wetter (com.htc.provider.weather)
 - Automatische Aktualisierungen
 - Speichert in einer SQLite Datenbank

```
tree /data/data/com.htc.provider.weather/  
|-- databases  
|  |-- weather.db          SQLite V3  
'-- files  
    |-- WP_0407GER.db      SQLite V3  
    '-- WP_0409WWE.db      SQLite V3
```

```
sqlite> select * from location where app = "com.htc.htclocationservice";  
  _id = 221  
  app = com.htc.htclocationservice  
  type = 1  
  code =  
  name = Aachen  
  state = Nordrhein-Westfalen  
  country = Deutschland  
  latitude = 50.77  
  longitude = 6.08  
  timezone =  
  timezoneId = Europe/Amsterdam
```


- Browser (com.android.browser)
 - „databases/browser.db“



```
sqlite> .tables
android_metadata      delicious_bookmarks  oma
bookmark_tag         delicious_tag        searches
bookmarks             htctopbookmarks     tags
```

```
sqlite> select * from bookmarks where _id=154;
_id = 154
title = http://m.zdnet.com/blog/security/ted-talk-fighting-2
viruses-defending-the-net/9099
url = http://m.zdnet.com/blog/security/ted-talk-fighting-2
viruses-defending-the-net/9099
visits = 1
date = 1311500436075
```

- Browser (com.android.browser)
 - „databases/browser.db“

```
sqlite> .tables
android_metadata      delicious_bookmarks  oma
bookmark_tag         delicious_tag        searches
bookmarks             htctopbookmarks     tags
```

```
sqlite> select * from searches;
_id = 1
search = waffen mp5 zusammenbauen
date = 1310299266414
```



- Browser (com.android.browser)
 - „databases/webview.db“



```
sqlite> .table
android_metadata  formdata          httpauth
cookies           formurl           password
```

```
sqlite> select * from httpauth;
  _id = 1
  host = deine-url.de
  realm = Geschützer Bereich
  username = deinbenutzername
  password = deinpasswort

  _id = 2
  host = andereseite.org
  realm = Geheimer Bereich
  username = username
  password = pwd
```

- Browser (com.android.browser)
 - „app_geolocation/webview.db“



```
sqlite> select * from CachedPosition;  
latitude = 50.7754893  
longitude = 6.0861394  
altitude =  
accuracy = 722.0  
altitudeAccuracy =  
heading =  
speed =  
timestamp = 1311382576208
```



- Maps (com.google.android.apps.maps)
 - „databases/search_history.db“

```
sqlite> SELECT * FROM suggestions;  
...  
      _id = 4  
      data1 = hiltrop , bochum  
singleResult =  
displayQuery = Hiltrop , Bochum  
  
      _id = 5  
      data1 = werne , bochum  
singleResult =  
displayQuery = Werne, Bochum  
  
...  
  
      _id = 11  
      data1 = burger king  
singleResult =  
displayQuery = Burger King  
  
      _id = 12  
      data1 = kortumstraße 46, 44787 bochum @51.478850,7.217084  
singleResult =
```

- Maps (com.google.android.apps.maps)
 - „databases/da_destination_history“

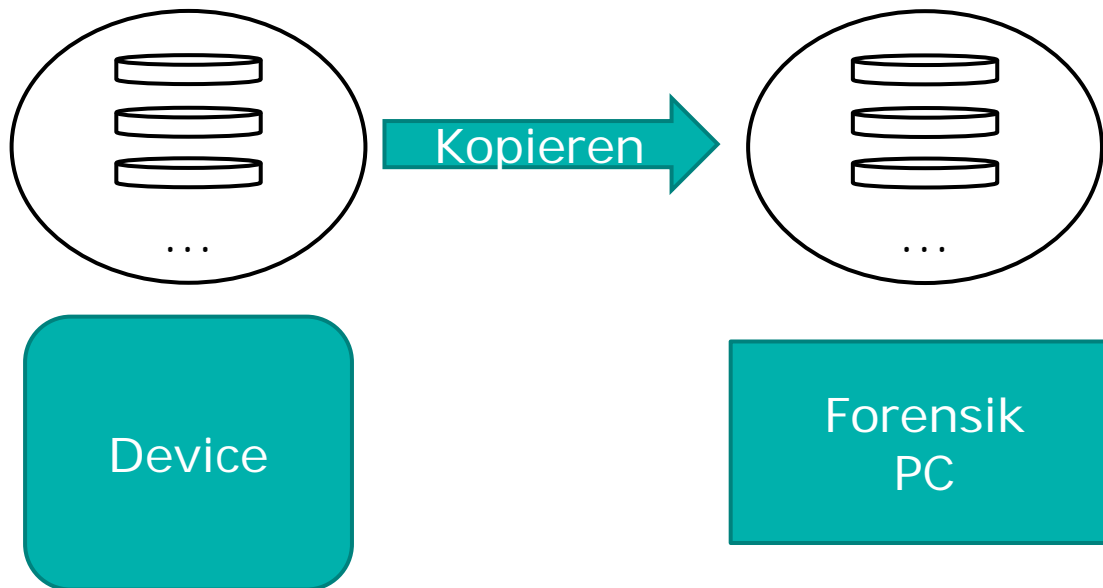
```
time = 1311853729570
dest_lat = 50759490
dest_lng = 6082690
dest_title = Fachhochschule Aachen Fachbereich 05 Elektrotechnik und I
Informationstechnik
dest_address = Eupener Straße 70
52066 Aachen
dest_token = FUKHBgMdgTbcACGPDWMrSHjFgykDflFPxZvARzHMIluBYng5-w
source_lat = 50779152
source_lng = 6088283
day_of_week = 5
hour_of_day = 13
```

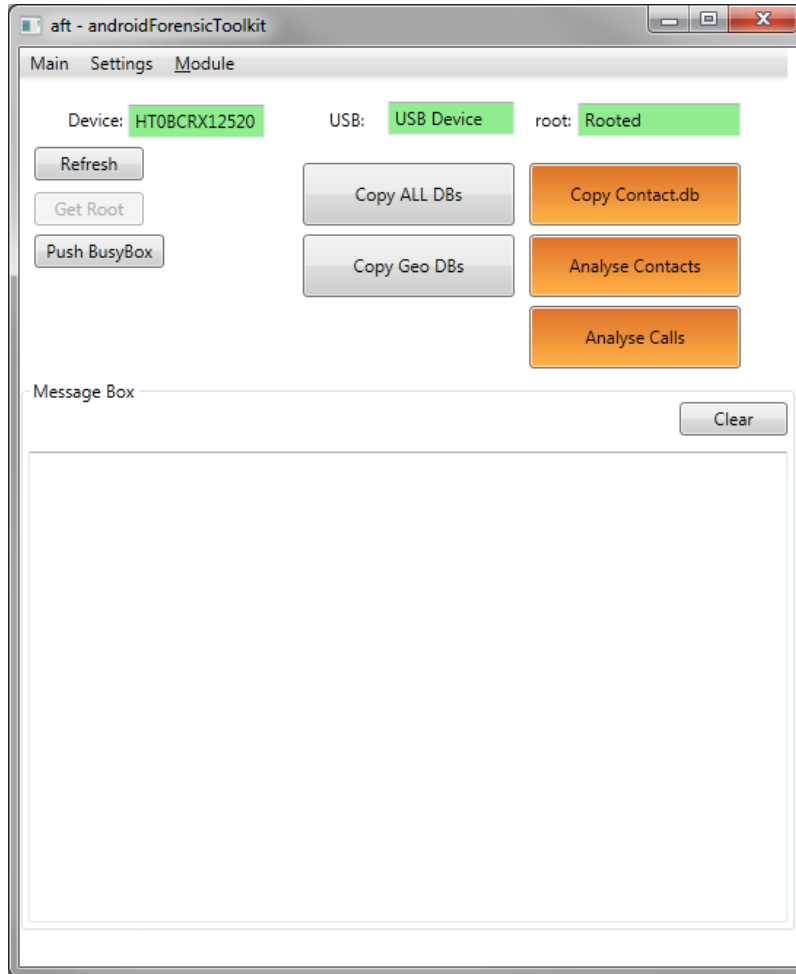
- Motivation / Ziel
- App-Entwicklung
- Analyse der App-Daten
- **Vorstellung Android-Forensic-Toolkit**
- Zusammenfassung

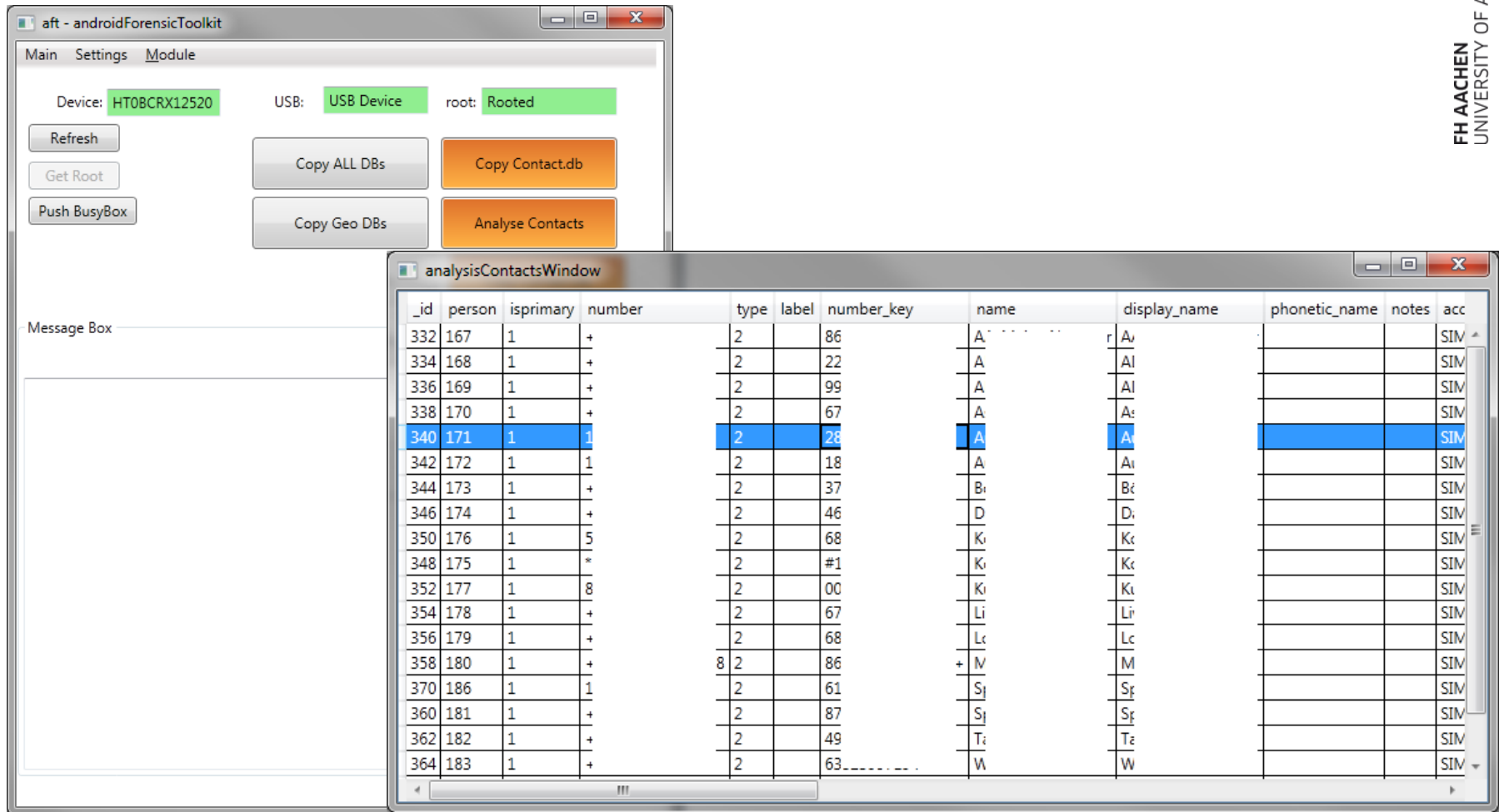


- Wurde von Stefan Maus (ehemaliger Student, FH-Aachen) entwickelt
- Läuft auf Windows Betriebssystem (Voraussetzung .NET Framework)
- Dient der logischen Analyse von Android Smartphones
- Weiterentwickelt um Ortsinformationen darzustellen

- Voraussetzungen
 - Root-Zugriff
 - USB Treiber
 - SDK
- Kopieren der Datenbanken



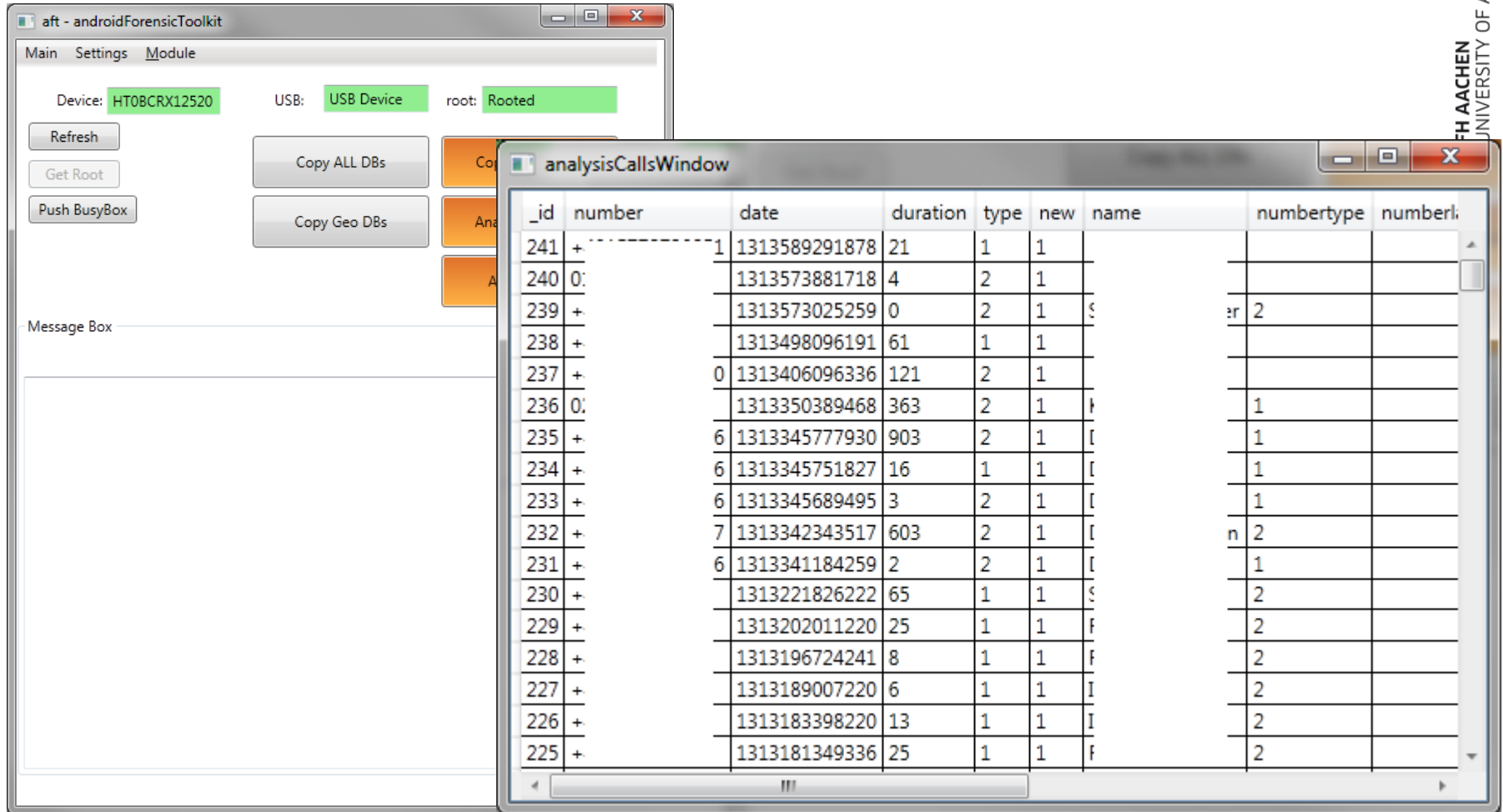




The screenshot displays the 'aft - androidForensicToolkit' application interface. The main window shows device information: Device: HT0BCRX12520, USB: USB Device, and root: Rooted. Below this are buttons for 'Refresh', 'Get Root', 'Push BusyBox', 'Copy ALL DBs', 'Copy Contact.db', 'Copy Geo DBs', and 'Analyse Contacts'. A 'Message Box' is visible at the bottom left.

An 'analysisContactsWindow' is overlaid on top, displaying a table of contact data. The table has the following columns: _id, person, isprimary, number, type, label, number_key, name, display_name, phonetic_name, notes, and acc. The row with _id 340 is highlighted in blue.

_id	person	isprimary	number	type	label	number_key	name	display_name	phonetic_name	notes	acc
332	167	1	+	2		86	A	A			SIM
334	168	1	+	2		22	A	Al			SIM
336	169	1	+	2		99	A	Al			SIM
338	170	1	+	2		67	A	Ae			SIM
340	171	1	1	2		28	A	A			SIM
342	172	1	1	2		18	A	Ai			SIM
344	173	1	+	2		37	B	Be			SIM
346	174	1	+	2		46	D	D			SIM
350	176	1	5	2		68	K	Kc			SIM
348	175	1	*	2		#1	K	Kc			SIM
352	177	1	8	2		00	Ki	Ki			SIM
354	178	1	+	2		67	Li	Li			SIM
356	179	1	+	2		68	Lc	Lc			SIM
358	180	1	+	8 2		86	+ M	M			SIM
370	186	1	1	2		61	Sj	Sj			SIM
360	181	1	+	2		87	Sj	Sj			SIM
362	182	1	+	2		49	Ti	Te			SIM
364	183	1	+	2		63	W	W			SIM

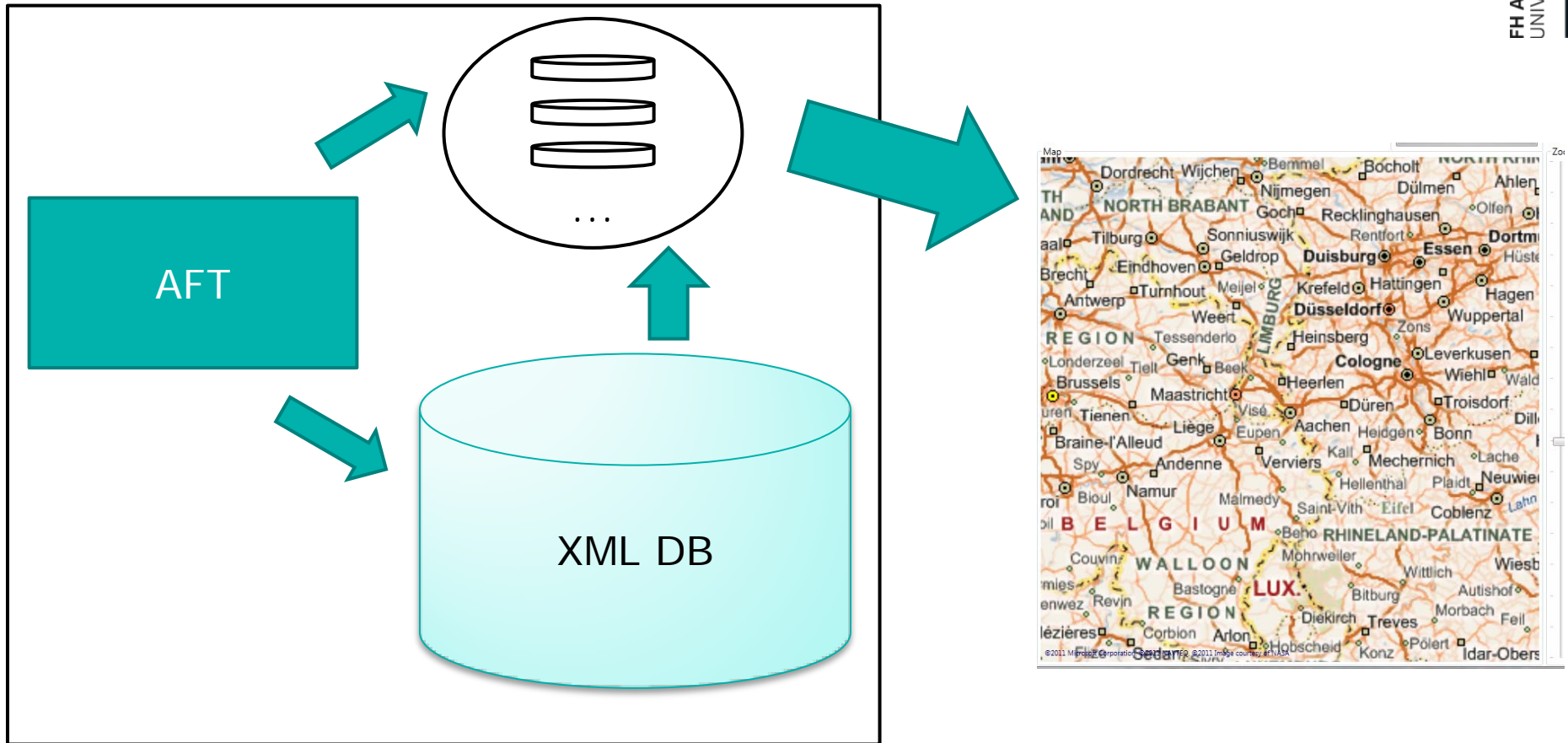


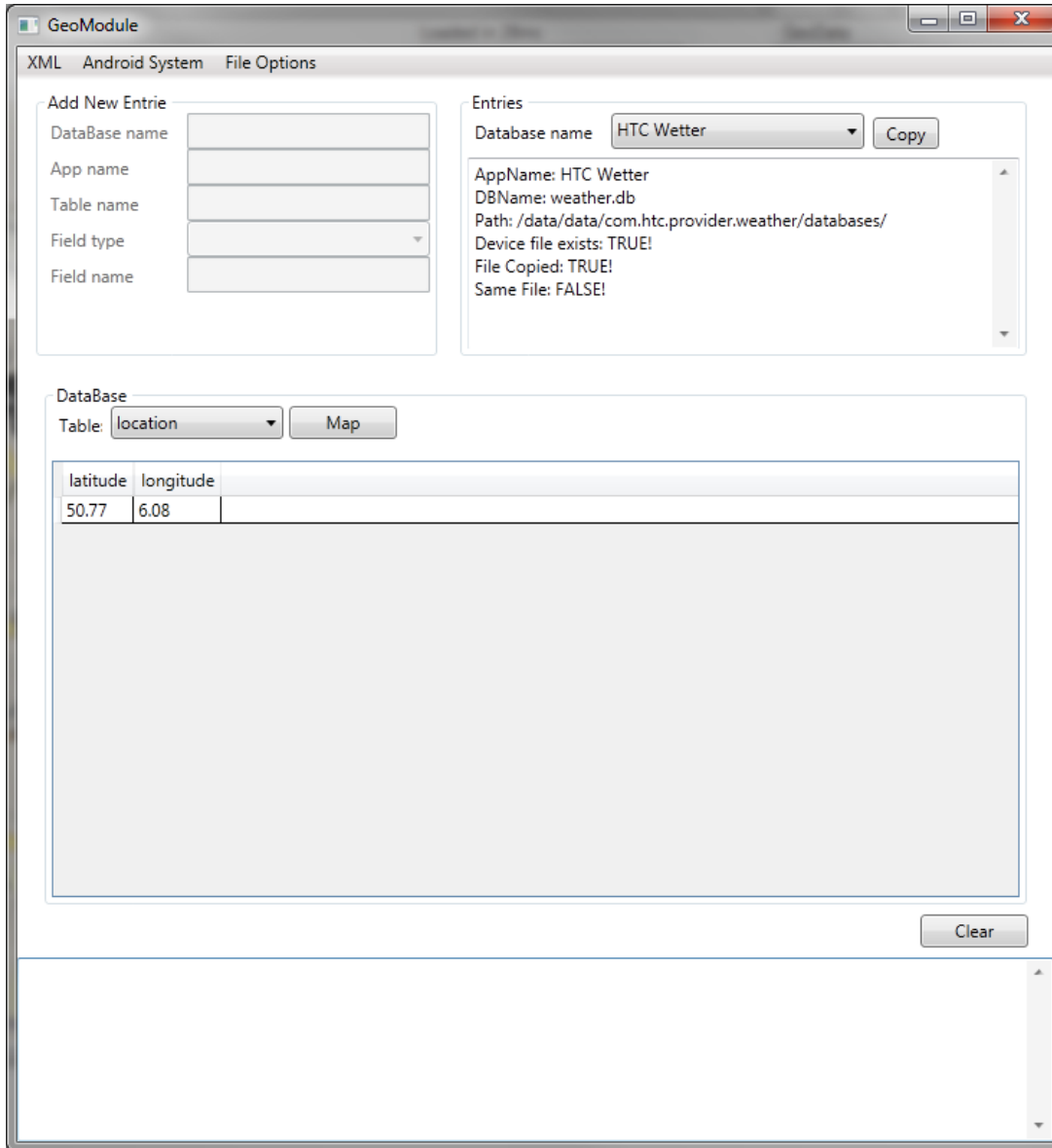
The screenshot shows the 'aft - androidForensicToolkit' application interface. The main window has a menu bar with 'Main', 'Settings', and 'Module'. Below the menu, there are fields for 'Device: HT0BCRX12520', 'USB: USB Device', and 'root: Rooted'. There are several buttons: 'Refresh', 'Get Root', 'Push BusyBox', 'Copy ALL DBs', 'Copy Geo DBs', and a partially visible 'Copy' button. A 'Message Box' is located at the bottom left.

An 'analysisCallsWindow' is overlaid on the main window, displaying a table of call records. The table has the following columns: '_id', 'number', 'date', 'duration', 'type', 'new', 'name', 'numbertype', and 'numberl'. The data is as follows:

_id	number	date	duration	type	new	name	numbertype	numberl
241	+	1 1313589291878	21	1	1			
240	0:	1313573881718	4	2	1			
239	+	1313573025259	0	2	1		er 2	
238	+	1313498096191	61	1	1			
237	+	0 1313406096336	121	2	1			
236	0:	1313350389468	363	2	1		1	
235	+	6 1313345777930	903	2	1		1	
234	+	6 1313345751827	16	1	1		1	
233	+	6 1313345689495	3	2	1		1	
232	+	7 1313342343517	603	2	1		n 2	
231	+	6 1313341184259	2	2	1		1	
230	+	1313221826222	65	1	1		2	
229	+	1313202011220	25	1	1		2	
228	+	1313196724241	8	1	1		2	
227	+	1313189007220	6	1	1		2	
226	+	1313183398220	13	1	1		2	
225	+	1313181349336	25	1	1		2	

- Auswertung der Geo-Daten





GeoModule

XML Android System File Options

Add New Entry

DataBase name:

App name:

Table name:

Field type:

Field name:

Entries

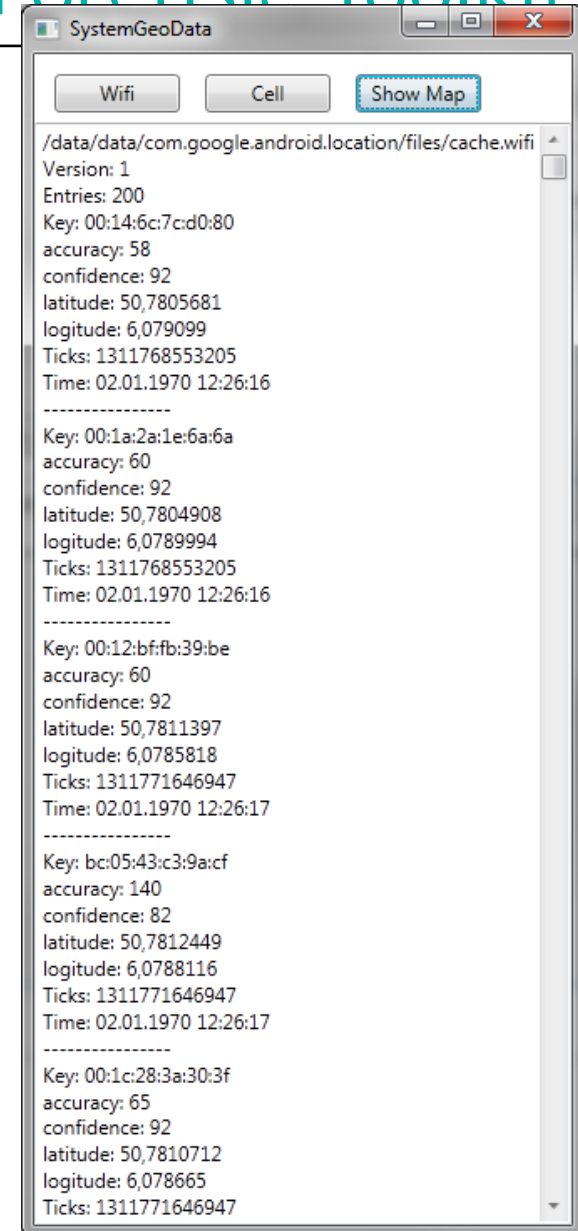
Database name: HTC Wetter

AppName: HTC Wetter
DBName: weather.db
Path: /data/data/com.htc.provider.weather/databases/
Device file exists: TRUE!
File Copied: TRUE!
Same File: FALSE!

DataBase

Table: location

latitude	longitude
50.77	6.08



SystemGeoData

```

/data/data/com.google.android.location/files/cache.wifi
Version: 1
Entries: 200
Key: 00:14:6c:7c:d0:80
accuracy: 58
confidence: 92
latitude: 50,7805681
logitude: 6,0790999
Ticks: 1311768553205
Time: 02.01.1970 12:26:16
-----
Key: 00:1a:2a:1e:6a:6a
accuracy: 60
confidence: 92
latitude: 50,7804908
logitude: 6,0789994
Ticks: 1311768553205
Time: 02.01.1970 12:26:16
-----
Key: 00:12:bf:fb:39:be
accuracy: 60
confidence: 92
latitude: 50,7811397
logitude: 6,0785818
Ticks: 1311771646947
Time: 02.01.1970 12:26:17
-----
Key: bc:05:43:c3:9a:cf
accuracy: 140
confidence: 82
latitude: 50,7812449
logitude: 6,0788116
Ticks: 1311771646947
Time: 02.01.1970 12:26:17
-----
Key: 00:1c:28:3a:30:3f
accuracy: 65
confidence: 92
latitude: 50,7810712
logitude: 6,078665
Ticks: 1311771646947

```

Vorstellung Android-Forensic-Toolkit

GeoModule

XML Android System File Options

Add New Entry

DataBase name

App name

Table name

Field type

Field name

DataBase

Table: loc

latitude

50.77

SystemGeoData

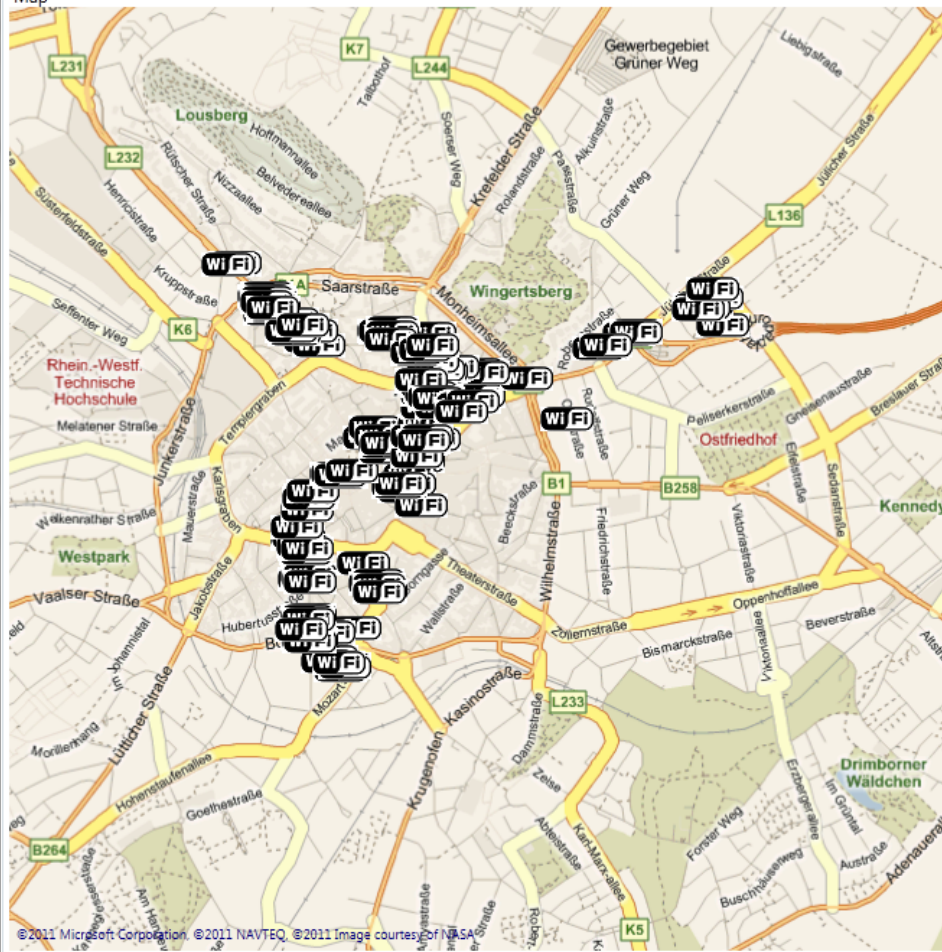
Wifi Cell **Show Map**

/data/data/com.google.android.location/files/cache.wifi

MapWindow

Loaded in 28ms

Search



Zoom

GeoData

Key: 00:14:6c:7c:d0:80
 Key: 00:1a:2a:1e:6a:6a
 Key: 00:12:bf:fb:39:be
 Key: bc:05:43:c3:9a:cf
 Key: 00:1c:28:3a:30:3f
 Key: 00:a0:57:16:50:63
 Key: 00:a0:57:16:52:34
 Key: 00:1c:28:05:1e:18

Routing

Start EMPTY

End EMPTY

walking Add Waypoint 0 Get Routes!

Routes

Comment

Clear Save

- Motivation / Ziel
- App-Entwicklung
- Analyse der App-Daten
- Vorstellung Android-Forensic-Toolkit
- Zusammenfassung

- Untersuchung der bekannten Speicherorte
 - Bilder, Passwörter, Ortsinformationen
- Root-Zugriff ist von der Android Version abhängig
- Ortsinformationen können dargestellt werden (Online Modus)
- ADB eignet sich, um eine logische Analyse der Daten anzufertigen

Vielen Dank für Ihre Aufmerksamkeit