

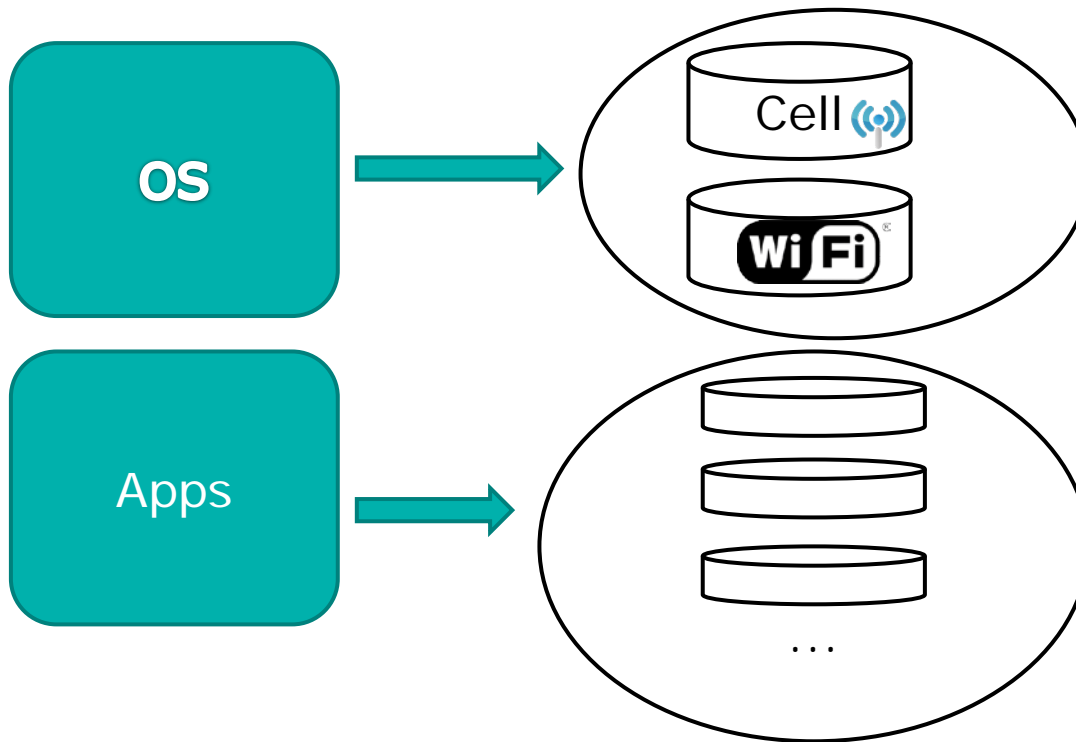
Android Forensik App – Geo Daten Analyse

Jens Weidhase



- Problemstellung
- Vorgehensweise
- Ergebnis

- Mobiles Gerät
 - Geo Daten vorhanden



- Entwickler der App entscheidet über die Daten

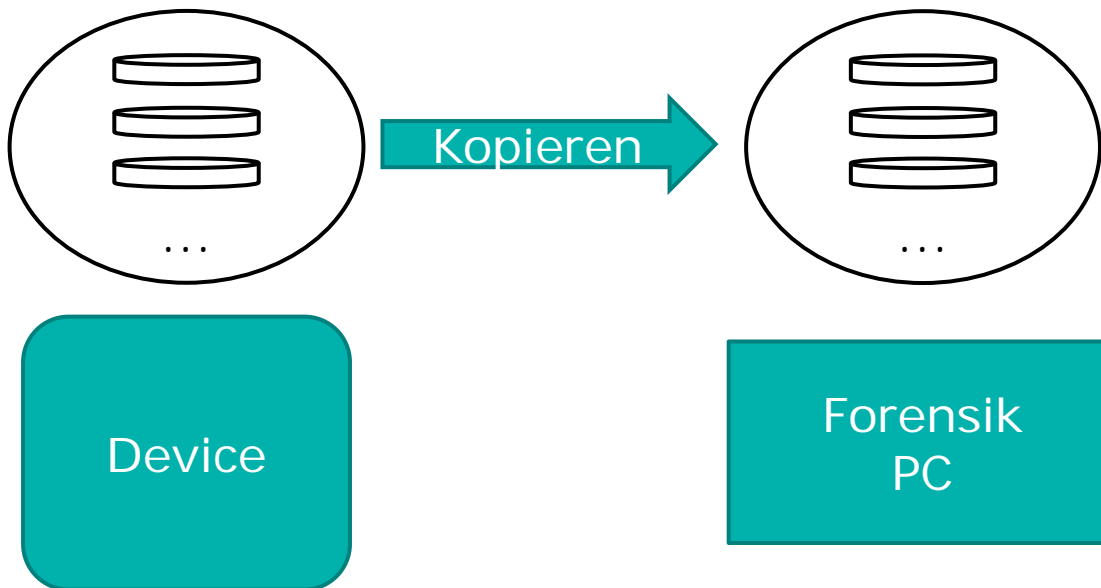
Table:

id	address	address2	time stamp	location	longitude	latitude
1	1 Martinstrasse 17	52062 Aachen, Aachen (Stadt)	1292586413117	NK		
2	4 Kettwiger Strasse 2	45127 Essen, Essen	1292676475380	NK		
3	5 B67	46395 Bocholt, Borken	1292680241216	NK		
4	6 Erfstrasse	52249 Eschweiler, Aachen (Landkreis)	1292845999454	NK		
5	7 Flachsbleiche 27	41179 Mönchengladbach, Mönchengladbach	1293096062782	NK		
6	8 Stadionring 24	44791 Bochum, Bochum	1293384022755	NK		
7	9 Total	Frechen, 50226 Frechen, Rhein-Erft-Kreis	1293377443783	NK		

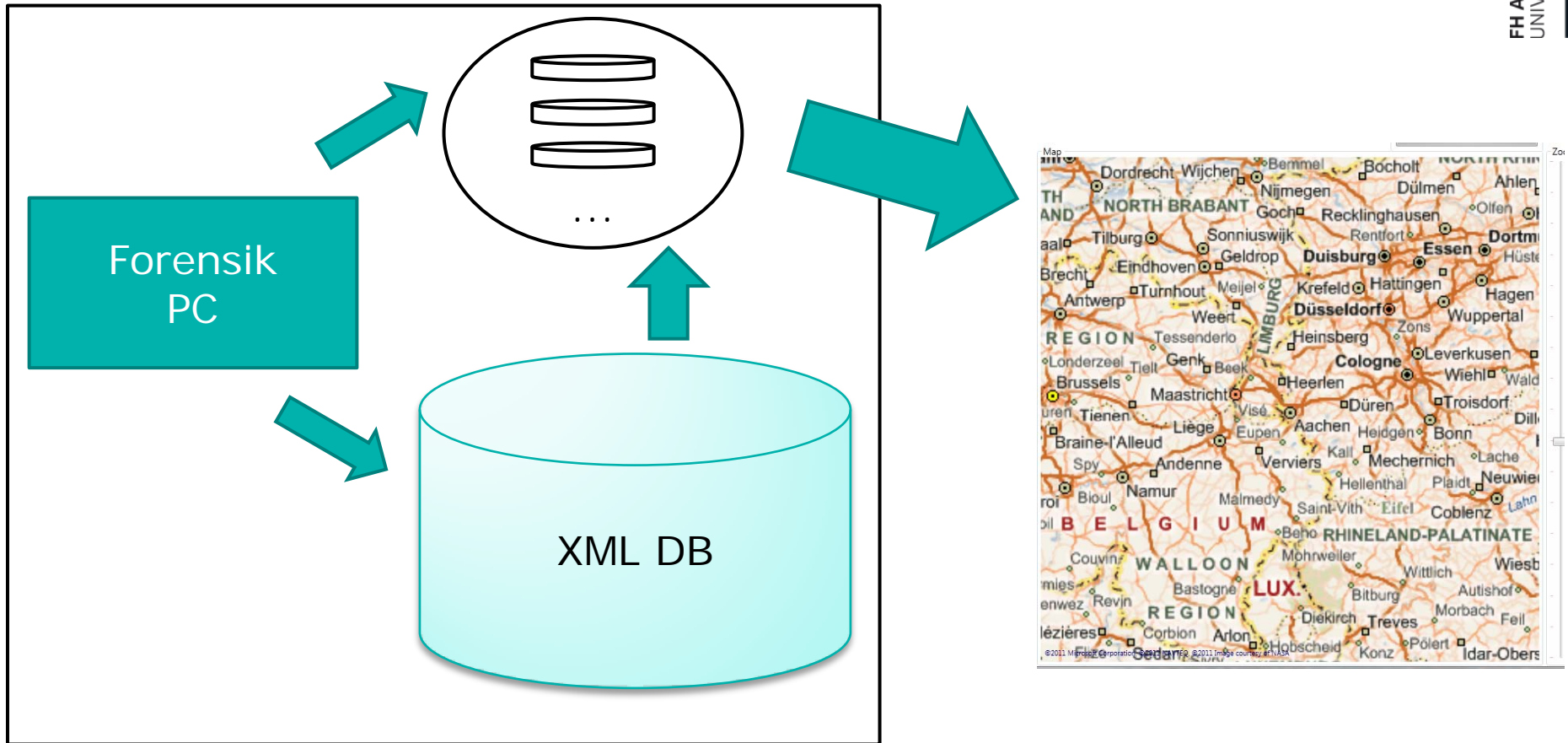
content	source	latitude	longitude	place_name	place_bounding
@ [redacted] Training at 9am?	Twitter for Android	50.7791362	6.08831245	Aix-la-Chapelle, Aix-la-Chapelle	[[50.6621438,5.9748467],[50.6621438,6.218106],[50.8



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



- Auswertung der Daten



- XML Datenbank

```

<Database Type="GEO">
  <DBName>weather.db</DBName>
  <DBPath>/data/data/com.htc.provider.weather/databases/</DBPath>
  <AppName>HTC Wetter</AppName>
  <Tables>
    <Table>
      <TBName>location</TBName>
      <Fields>
        <Field Type="lat">latitude</Field>
        <Field Type="lng">longitude</Field>
      </Fields>
    </Table>
  </Tables>
</Database>

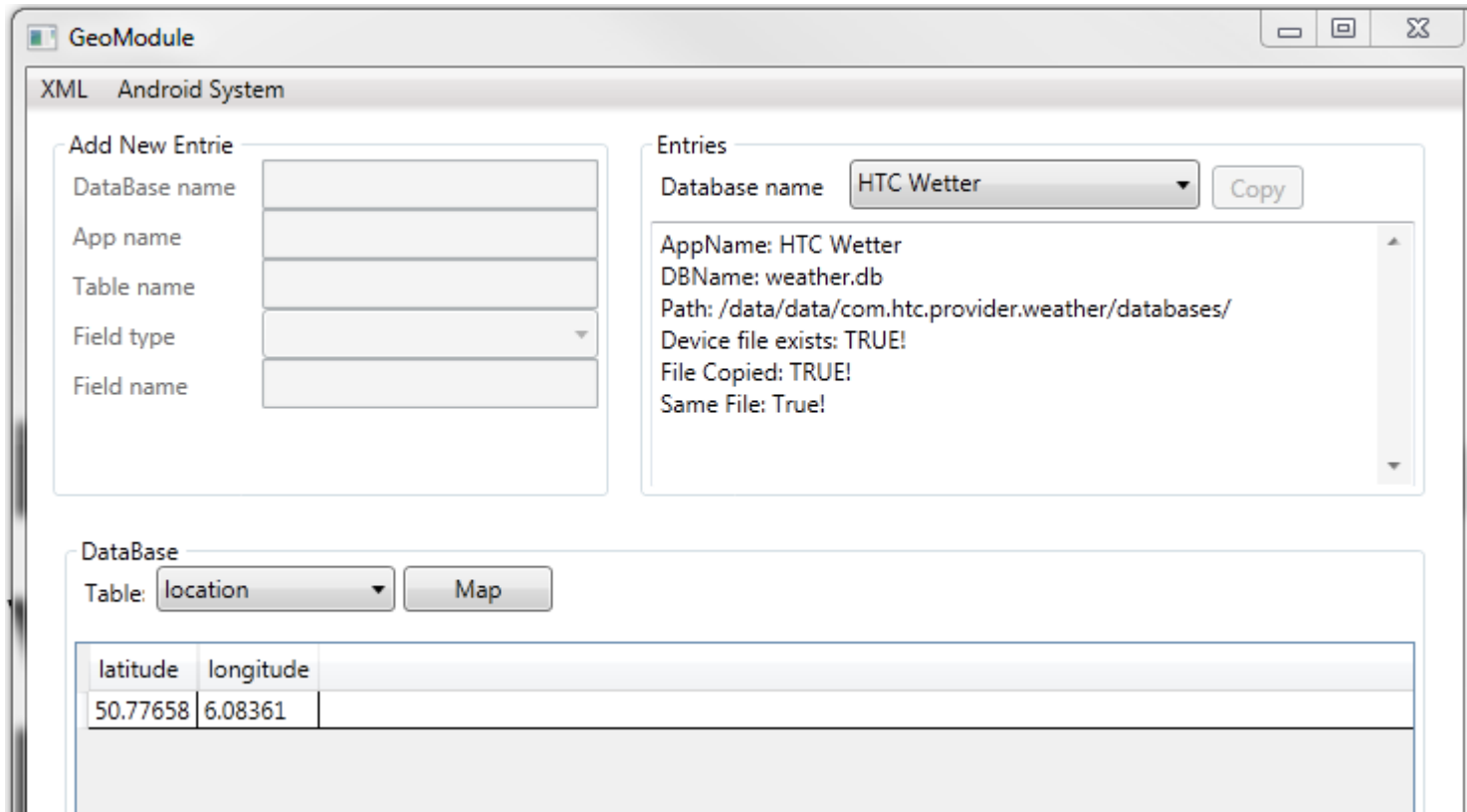
<Table>
  <TBName>adress_example</TBName>
  <Fields>
    <Field Type="string">city</Field>
    <Field Type="string">code</Field>
    <Field Type="string">street</Field>
  </Fields>
</Table>

```

- Vorteile

- Erweiterbar (neue Apps)
- Anpassbar (App Versionen)

- Daten auswerten



The screenshot shows the GeoModule application interface. It has a title bar with 'GeoModule' and standard window controls. The main content area is divided into several sections:

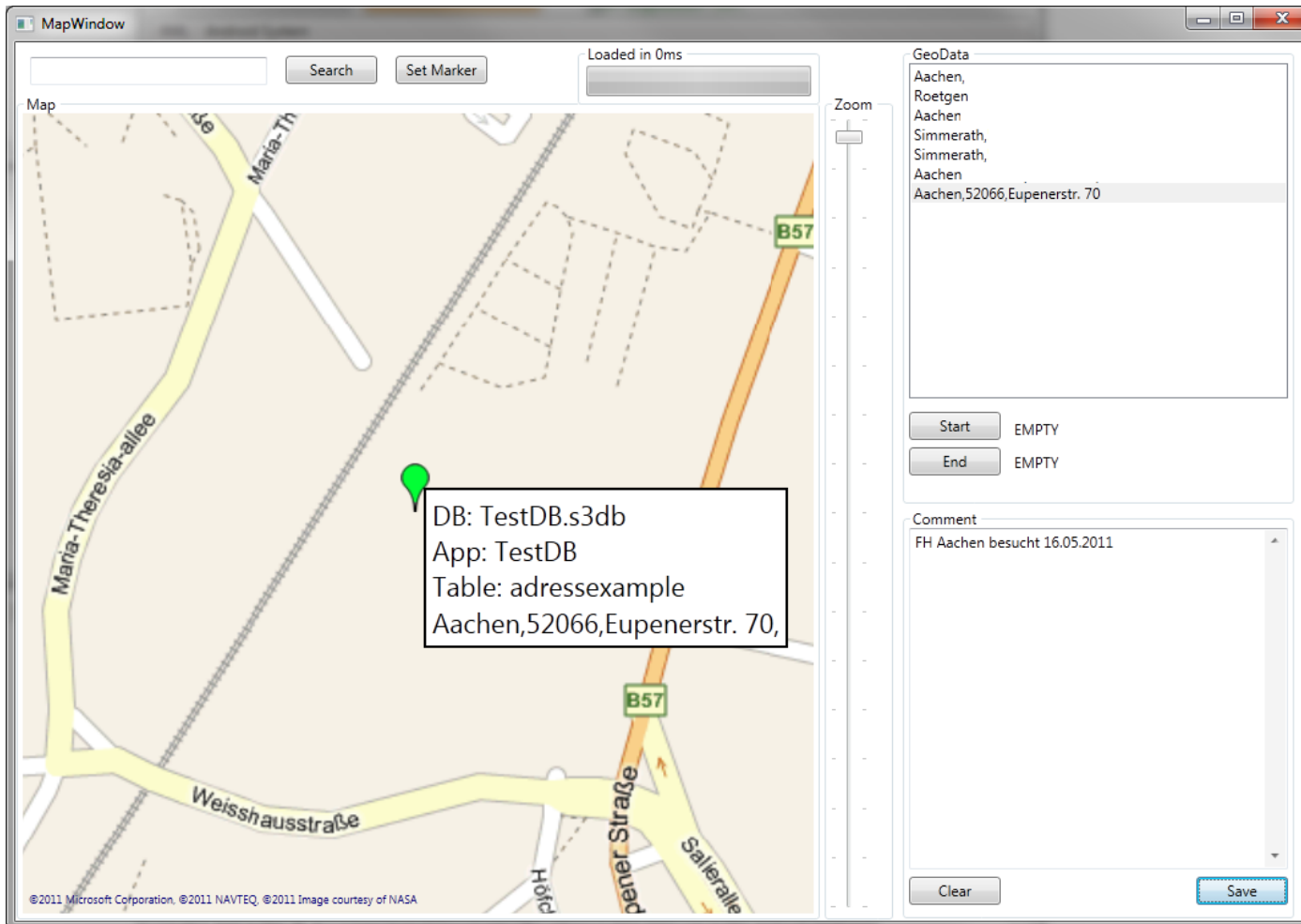
- XML Android System**: A header for the current view.
- Add New Entry**: A form with input fields for 'DataBase name', 'App name', 'Table name', 'Field type' (a dropdown menu), and 'Field name'.
- Entries**: A section containing a dropdown menu for 'Database name' (set to 'HTC Wetter') and a 'Copy' button. Below this is a text area displaying the following information:


```

      AppName: HTC Wetter
      DBName: weather.db
      Path: /data/data/com.htc.provider.weather/databases/
      Device file exists: TRUE!
      File Copied: TRUE!
      Same File: True!
      
```
- DataBase**: A section with a dropdown menu for 'Table' (set to 'location') and a 'Map' button.
- Table View**: A table with two columns, 'latitude' and 'longitunde', and one data row:

latitude	longitunde
50.77658	6.08361

- Veranschaulichung der Daten



Abschließende Fragen?

Jens.Weidhase@alumni.fh-aachen.de

Vielen Dank für Ihre
Aufmerksamkeit!