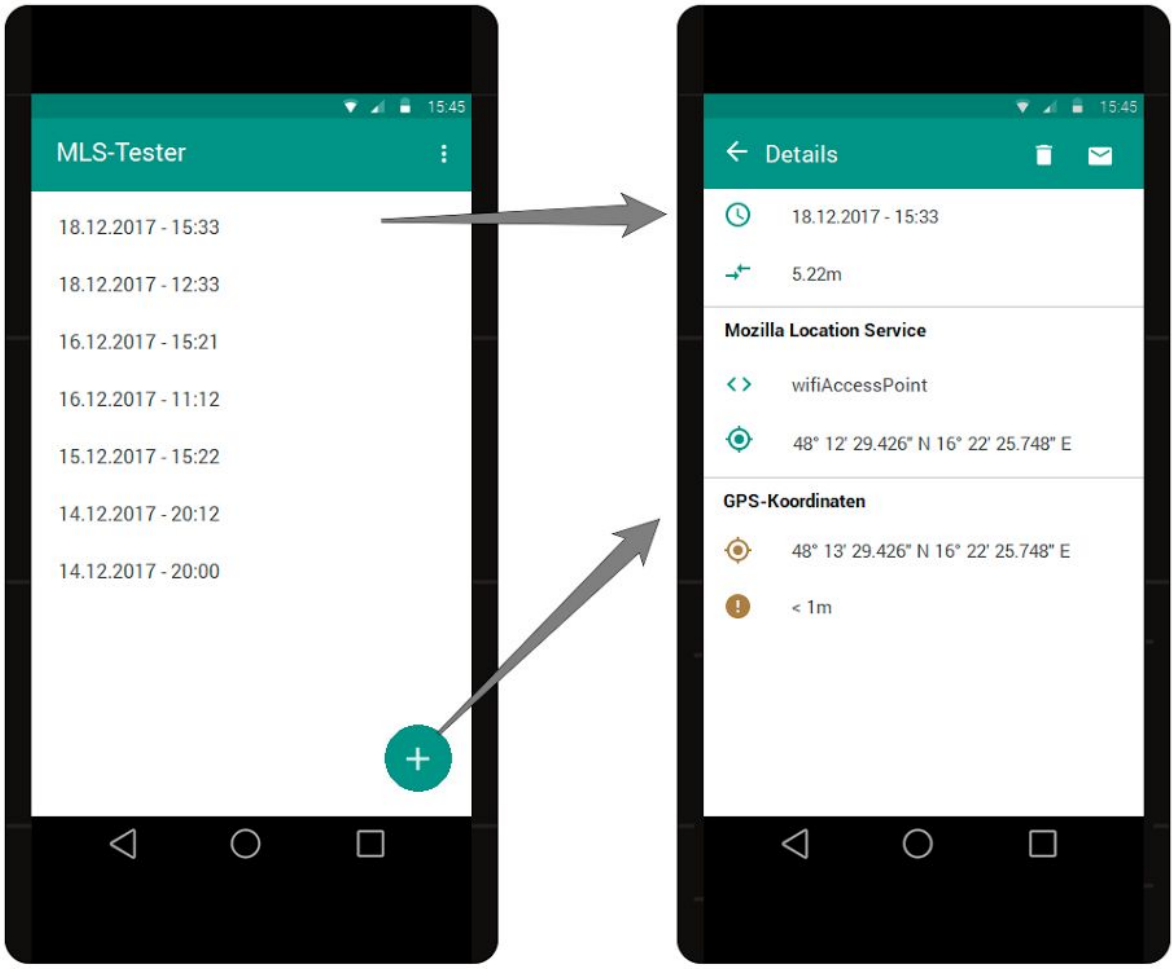
# Übung 3: Geolocation

Marton Bartal – Dominik Schwarz – Johannes Vass

## Mockups:

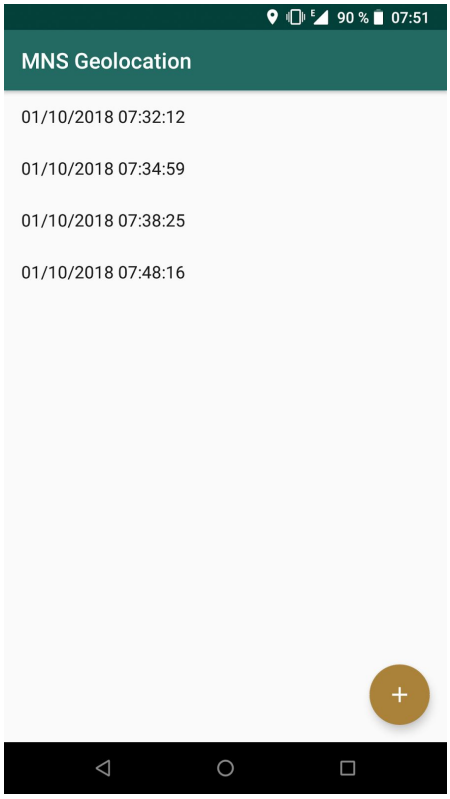


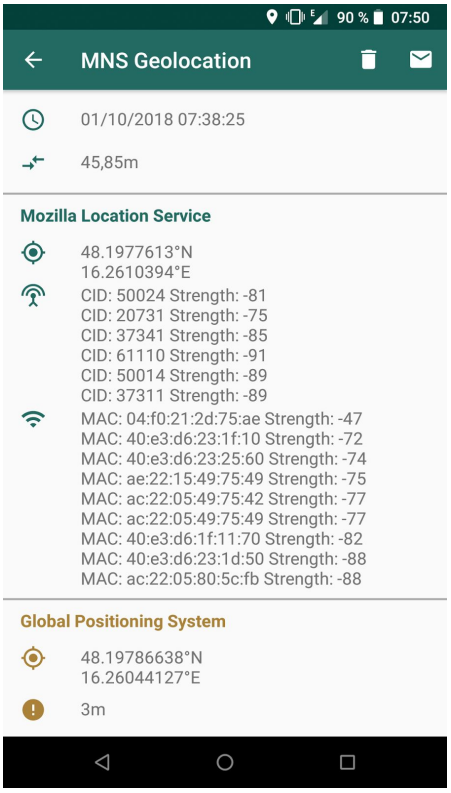

Wir verwenden für die Geolocation-App eine Activity mit zwei Fragments, nach dem Start der App wird ein Fragment mit einer Liste aller bisherigen Messungen sortiert nach Zeitpunkt und einem FAB zur Erstellung neuer Messung angezeigt. Klickt der User nun auf eine bereits erstellte Messung in der Liste oder den FAB öffnet sich das Detail-Fragment mit folgenden Informationen:

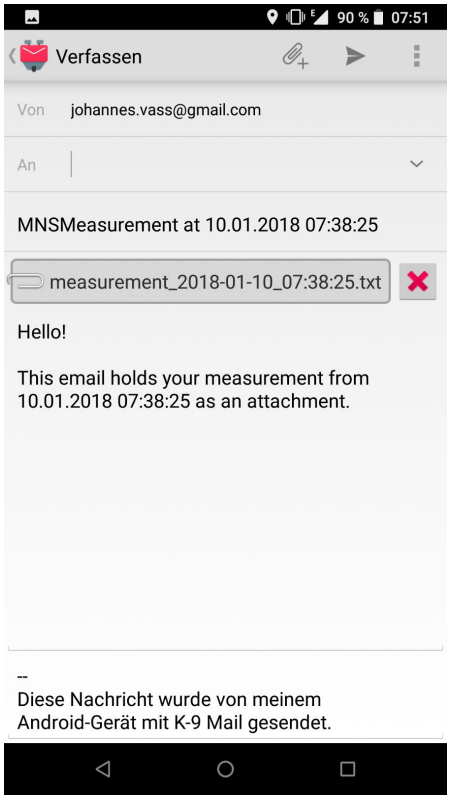
- Zeitpunkt der Messung
- Unterschied zwischen MLS und GPS Position (Distanz in m)
- Parameter sowie Ergebnis des MLS API Requests
- Tatsächliche Koordinaten (GPS)
- Genauigkeit der GPS-Position (in m)

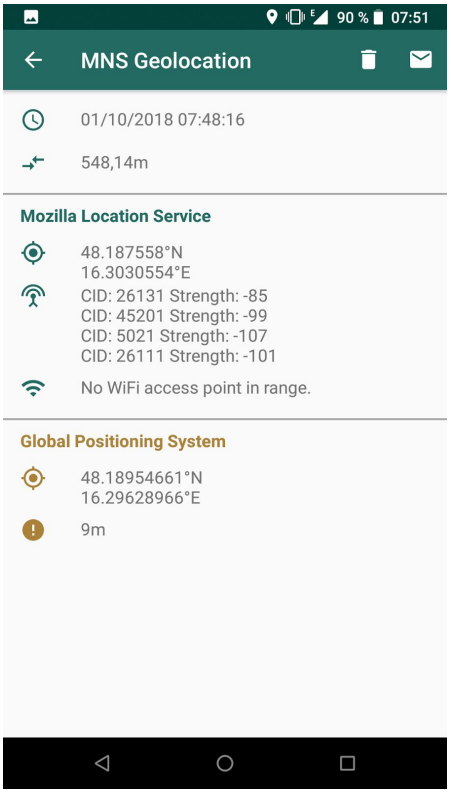
In der Toolbar hat der User nun die Möglichkeit wieder in die Listenansicht zu wechseln (Back-Icon), den geöffneten Messbericht zu löschen (Delete-Icon) oder den Bericht als Anhang zu versenden.

## Screenshots:



## Securitymaßnahmen:

**Absicherung der Nutzerdaten:**

- Speicherung der Nutzerdaten in einer verschlüsselten Sqlite-Datenbank
- Beim ersten Start wird ein Passwort generiert und verschlüsselt gespeichert in den Shared Prefs
- Ver-/Entschlüsselung des Passworts mittels Key aus dem Android Keystore

→ Entschlüsselung ist an das Gerät gebunden. Datenbank kann kopiert werden, aber da man den Key nicht (einfach) extrahieren kann fängt man damit nichts an.

**Absicherung des API-Key:**

Einen statischen API-Key zu schützen ist nicht so einfach (mit dynamischen Keys sollte man den Keystore benutzen). Ohne backend server kann man nur durch Security through Obscurity statische Keys schützen. Was natürlich sehr einfach angreifbar ist. Folgende Möglichkeiten gibt es statische Keys zu schützen:

1. In der Client Applikation den Code mit Proguard unlesbar machen und den plain Key in zB. Base64-Format speichern. (Alle diese Herangehensweisen können ganz einfach bei einem Angriff rückgängig gemacht werden -> Key ist nicht wirklich geschützt)
2. Den Key auf einem Server speichern und eine Schnittstelle an dem Server zu verfügung stellen. Diese Schnittstelle wird dann den Key im Hintergrund benutzen. Der Client hat in diesem Fall mit dem Key nicht zu tun. Um den Key zu bekommen muss der Angreifer unseren Back End Server hacken.

## Einschränkungen

- Da die meisten Verschlüsselungsalgorithmen und -methoden mit API-Level 23 umgestaltet/eingeführt wurden, haben wir diese Version als Mindeststandard definiert → siehe TUWEL-Thread
- Wir haben die Messungen im 2G Netz ausgeführt, weil das die einzige Einstellung ist, wo wir zuverlässig die Cell Ids von Nachbarzellen bekommen (--> Triangulation) und die MLS-Datenbank mit den Positionen der Masten neuerer Technologien noch nicht so vertraut zu sein scheint.

# Messbericht:

## Messpunkte:

<u>Vor dem Bahnhof Hütteldorf:</u>

An dieser Position wurden 6 GSM Sendepunkte und 9 WiFi Netzwerke in der Umgebung gefunden, wir konnten daher eine gute MLS Genauigkeit von 124 Metern erzielen. Das GPS Signal war mit eine Genauigkeit von 3 Metern ebenfalls sehr gut. Durch diese effektiven Bedingungen wurde eine Distanz zwischen der GPS Position und der MLS Position von lediglich 45 Metern gemessen.

```
GPS vs MLS measurement from 10.01.2018 07:38:25:

GPS:
  Location: 48.19786638°N / 16.26044127°E
  Accuracy: 3.0 m

MLS:
  Location: 48.1977613°N / 16.2610394°E
  Accuracy: 124.404205 m
  Parameters:
    Cell Towers:
      - CellTower(mobileCountryCode=232, mobileNetworkCode=1, locationAreaCode=17008, cellId=50024, radioType='gsm', signalStrength=-81,
      - CellTower(mobileCountryCode=232, mobileNetworkCode=1, locationAreaCode=17008, cellId=20731, radioType='gsm', signalStrength=-75,
      - CellTower(mobileCountryCode=232, mobileNetworkCode=1, locationAreaCode=17008, cellId=37341, radioType='gsm', signalStrength=-85,
      - CellTower(mobileCountryCode=232, mobileNetworkCode=1, locationAreaCode=17004, cellId=61110, radioType='gsm', signalStrength=-91,
      - CellTower(mobileCountryCode=232, mobileNetworkCode=1, locationAreaCode=17008, cellId=50014, radioType='gsm', signalStrength=-89,
      - CellTower(mobileCountryCode=232, mobileNetworkCode=1, locationAreaCode=17008, cellId=37311, radioType='gsm', signalStrength=-89,
    WIFI Access Points:
      - WifiAccessPoint(macAddress='04:f0:21:2d:75:ae', channel=11, frequency=2462, signalStrength=-47, signalToNoiseRatio=null, age=null
      - WifiAccessPoint(macAddress='40:e3:d6:23:1f:10', channel=100, frequency=5500, signalStrength=-72, signalToNoiseRatio=null, age=nul
      - WifiAccessPoint(macAddress='40:e3:d6:23:25:60', channel=1, frequency=2412, signalStrength=-74, signalToNoiseRatio=null, age=null)
      - WifiAccessPoint(macAddress='ae:22:15:49:75:49', channel=6, frequency=2437, signalStrength=-75, signalToNoiseRatio=null, age=null)
      - WifiAccessPoint(macAddress='ac:22:05:49:75:42', channel=112, frequency=5560, signalStrength=-77, signalToNoiseRatio=null, age=nul
      - WifiAccessPoint(macAddress='ac:22:05:49:75:49', channel=6, frequency=2437, signalStrength=-77, signalToNoiseRatio=null, age=null)
      - WifiAccessPoint(macAddress='40:e3:d6:1f:11:70', channel=52, frequency=5260, signalStrength=-82, signalToNoiseRatio=null, age=null
      - WifiAccessPoint(macAddress='40:e3:d6:23:1d:50', channel=108, frequency=5540, signalStrength=-88, signalToNoiseRatio=null, age=nul
      - WifiAccessPoint(macAddress='ac:22:05:80:5c:fb', channel=48, frequency=5240, signalStrength=-88, signalToNoiseRatio=null, age=null

Distance: 45.84623785166273 m
```

U4 Braunschweiggasse:

Bei einer Messung in einem U-Bahn-Zug nahe der Station Braunschweiggasse wurden nur 4 GSM Sendepunkte und kein WiFi Netzwerk gefunden. Die Genauigkeit von MLS wird mit 1000 Metern angegeben und wir erreichen eine Entfernung zum GPS Standort von 540 Metern. Es wird hier ersichtlich, dass durch eine Messung nur über ein paar GSM Sendepunkte die genaue Position des Gerätes nur sehr unzuverlässig ermittelt werden kann.

```
GPS vs MLS measurement from 10.01.2018 07:48:16:

GPS:
  Location: 48.18954661°N / 16.29628966°E
  Accuracy: 9.0 m

MLS:
  Location: 48.187558°N / 16.3030554°E
  Accuracy: 1000.0 m
  Parameters:
    Cell Towers:
      - CellTower(mobileCountryCode=232, mobileNetworkCode=1, locationAreaCode=17008, cellId=26131, radioType='gsm', signalStrength=-85,
      - CellTower(mobileCountryCode=232, mobileNetworkCode=1, locationAreaCode=17008, cellId=45201, radioType='gsm', signalStrength=-99,
      - CellTower(mobileCountryCode=232, mobileNetworkCode=1, locationAreaCode=17008, cellId=5021, radioType='gsm', signalStrength=-107,
      - CellTower(mobileCountryCode=232, mobileNetworkCode=1, locationAreaCode=17008, cellId=26111, radioType='gsm', signalStrength=-101,
    WIFI Access Points:

Distance: 548.1359455184282 m
```

Vor dem Hauptgebäude der TU Wien:

Die letzte Messung wurde vor dem Hauptgebäude der TU Wien am Karlsplatz durchgeführt. Ähnlich zur ersten Messung wurde an dieser Position eine Vielzahl an GSM Sendepunkten und WiFi Netzwerken gefunden. Die Genauigkeit der MLS Position (fast 126 Meter) und die Distanz zur GPS Position (51 Meter) sind daher ebenfalls mit der ersten Messung vergleichbar.

```
GPS vs MLS measurement from 10.01.2018 18:02:19:

GPS:
  Location: 48.19968609°N / 16.37045098°E
  Accuracy: 11.0 m

MLS:
  Location: 48.1994354°N / 16.3710302°E
  Accuracy: 125.867775 m
  Parameters:
    Cell Towers:
      - CellTower(mobileCountryCode=232, mobileNetworkCode=1, locationAreaCode=4101, cellId=31710, radioType='gsm', signalStrength=-61,
      - CellTower(mobileCountryCode=232, mobileNetworkCode=1, locationAreaCode=17005, cellId=32304, radioType='gsm', signalStrength=-71,
      - CellTower(mobileCountryCode=232, mobileNetworkCode=1, locationAreaCode=17005, cellId=30611, radioType='gsm', signalStrength=-71,
      - CellTower(mobileCountryCode=232, mobileNetworkCode=1, locationAreaCode=4101, cellId=54594, radioType='gsm', signalStrength=-77,
      - CellTower(mobileCountryCode=232, mobileNetworkCode=1, locationAreaCode=17007, cellId=37230, radioType='gsm', signalStrength=-79,
      - CellTower(mobileCountryCode=232, mobileNetworkCode=1, locationAreaCode=4101, cellId=56701, radioType='gsm', signalStrength=-79,
      - CellTower(mobileCountryCode=232, mobileNetworkCode=1, locationAreaCode=17005, cellId=50421, radioType='gsm', signalStrength=-75,
    WIFI Access Points:
      - WifiAccessPoint(macAddress='e4:aa:5d:3e:aa:72', channel=1, frequency=2412, signalStrength=-70, signalToNoiseRatio=null, age=null
      - WifiAccessPoint(macAddress='e4:aa:5d:3e:aa:73', channel=1, frequency=2412, signalStrength=-71, signalToNoiseRatio=null, age=null
      - WifiAccessPoint(macAddress='e4:aa:5d:3e:aa:70', channel=1, frequency=2412, signalStrength=-77, signalToNoiseRatio=null, age=null
      - WifiAccessPoint(macAddress='f0:9f:c2:7a:59:1f', channel=6, frequency=2437, signalStrength=-72, signalToNoiseRatio=null, age=null
      - WifiAccessPoint(macAddress='f2:9f:c2:7a:59:1f', channel=6, frequency=2437, signalStrength=-74, signalToNoiseRatio=null, age=null
      - WifiAccessPoint(macAddress='f0:9f:c2:7d:5c:1a', channel=6, frequency=2437, signalStrength=-76, signalToNoiseRatio=null, age=null
      - WifiAccessPoint(macAddress='2c:3f:38:aa:90:b3', channel=1, frequency=2412, signalStrength=-77, signalToNoiseRatio=null, age=null
      - WifiAccessPoint(macAddress='88:51:fb:8a:8d:d0', channel=1, frequency=2412, signalStrength=-79, signalToNoiseRatio=null, age=null
      - WifiAccessPoint(macAddress='f2:9f:c2:7d:5c:1a', channel=6, frequency=2437, signalStrength=-79, signalToNoiseRatio=null, age=null
      - WifiAccessPoint(macAddress='4c:5e:0c:82:10:9f', channel=120, frequency=5600, signalStrength=-81, signalToNoiseRatio=null, age=nu
      - WifiAccessPoint(macAddress='00:20:a6:61:ff:bd', channel=136, frequency=5680, signalStrength=-84, signalToNoiseRatio=null, age=nu
      - WifiAccessPoint(macAddress='b4:a4:e3:cb:c2:9d', channel=36, frequency=5180, signalStrength=-84, signalToNoiseRatio=null, age=nul
      - WifiAccessPoint(macAddress='b4:a4:e3:cb:c2:9f', channel=36, frequency=5180, signalStrength=-85, signalToNoiseRatio=null, age=nul
      - WifiAccessPoint(macAddress='f4:0f:1b:bf:56:5c', channel=48, frequency=5240, signalStrength=-87, signalToNoiseRatio=null, age=nul
      - WifiAccessPoint(macAddress='02:9f:c2:7b:59:1f', channel=48, frequency=5240, signalStrength=-89, signalToNoiseRatio=null, age=nul

Distance: 51.18555886235954 m
```

# Projektbericht:

Diese Aufgabe war am aufwendigsten aber hat sehr viel Spaß gemacht. Wir mussten viele Herausforderungen lösen, aber weil wir die einzelne Aufgaben sehr gut aufteilen konnten, waren wir mit dem Beispiel ganz schnell fertig. Wir haben sehr viel über Android Programmierung durch diese Aufgabe gelernt. Ein paar Beispiele: wie man Services mocken kann, wie man mit Fragments umgeht, wenn wir nur ein Activity haben oder wie man IntentServices/Services erfolgreich mit Event Broadcasting benutzt bzw. wie Eventbased- und Reactive Programmierung unterscheidet. Man kann schon sehen, dass die Android System Services sehr gut aufgebaut und einfach benutzbar sind, weil die Implementation für die GPS/Wifi/CellTower Scanner war schnell erledigt. Wo wir ein bisschen länger diskutiert haben, waren die Sicherheitsmaßnahmen. Man würde denken, dass statische Keys zu schützen ist einfach, aber wenn man ein bisschen überlegt sieht man sofort, dass es nicht mal trivial ist und nur Clientseite geht es gar nicht (man muss natürlich wissen, dass statische Keys muss anders behandelt werden, wie dynamische Keys).