RheinlandPfalz
POLIZEIPRÄSIDIUM KOBLENZ

Analyse und Interpretation von Geolokalisationsdaten in modernen Smartphones

Andreas Dhein

Polizeipräsidium Koblenz / Universität Koblenz

PG Technische Ermittlungsunterstützung

Über den Vortragenden

1977

1985

2001

2005

ATELCO Computer

2009 2010 2011 2012

startseite → campus koblenz → fachbereich 4: informatik → wissenschaftliche einrichtungen → institut für wirtschafts- und verwaltungsinformatik → professur grimm → personen → prof. dr. rüdiger grimm

IWVI

PROF. DR. RÜDIGER GRIMM

Promotion

Leiter der Professur IT-Risk-Management (Institut für Wirtschafts- und Verwaltungsinformatik)

Über den Vortrag

- Motivation

- Untersuchung iOS
  - iPhoneTracker (Warden/Allan)
  - iPhoneTrackerLE
  - Erfahrungen/Probleme
  - Natives GPS (harvesting-Tabellen)

- Untersuchung Android
  - AndroidTrackerLE
  - Erfahrungen/Probleme

- Ausblick
  - Aktueller Forschungsstand

MOTIVATION

PG Technische Ermittlungsunterstützung

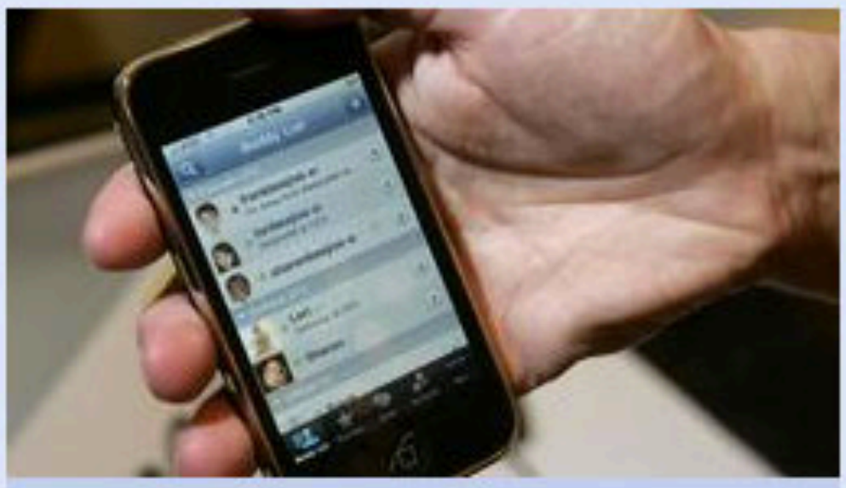
Smartphone speichert Bewegungsprofile

Das iPhone als Spitzel

Ohne Wissen der Nutzer haben Apples Smartphones aufgezeichnet, wann sich die Nutzer wo aufgehalten haben. Zwei britische Experten analysierten die Daten und zeigten: Damit lassen sich detaillierte Bewegungsprofile erstellen. Jeder iPhone-Besitzer kann das nach einem Download selbst überprüfen.

Von Fiete Stegers, tagesschau.de

Nur 184 KiloByte ist das Programm iPhoneTracker groß, das die britischen Informatiker Pete Warden und Alasdair Allan geschrieben haben. Aber wer es aus dem Internet herunterlädt und auf dem Computer installiert, mit dem er normalerweise via iTunes sein iPhone mit Musik bestückt oder seinen Kalender sychronisiert, erlebt Erstaunliches: Das Programm liest die von Apples iTunes-Software automatisch erstellten Sicherungskopien der Handy-Daten aus. Dann zeigt es auf einer Weltkarte mit



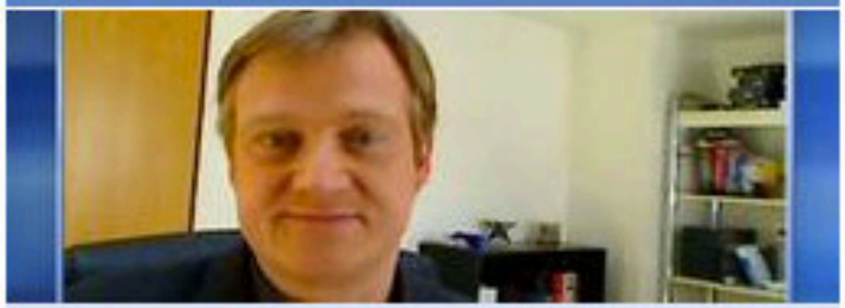
iPhones speichern mehr Informationen über ihre Besitzer, als vielen von ihnen lieb sein dürfte.

Nachrichten-Weltatlas

Deutschland

Landkarte, weitere Nachrichten aus der Region und viele Hintergrundinformationen. [Flash|HTML]

Video



Computerexperte Jörg Schieb zu den iPhone-Datenschutzproblemen [mehr]

Video

Apple in der Kritik: iPhone und iPad speichern Bewegungsprofile

Johannes Jolmes, NDR [tagesschau 15:00 Uhr 21.04.2011]

Audio

Apple-Affäre: Aigner und Schaar verlangen Aufklärung [Stephan Ueberbach (SWR), ARD Berlin]

Quelle: tagesschau.de

... aus forensischer Sicht

- Ganz viele Fragen!!!!!
  - Wann werden Geodaten vom Gerät erhoben ?
  - Wo befinden sich die Ortungsdienstdaten ?
  - Warum gibt es mehrere Einträge pro Zeitstempel ?
  - Wie sind die Zeitstempel zu interpretieren ?
  - Wie werden die Daten interpretiert ?
  - Wie sieht es mit der Genauigkeit der Daten aus ?
  - Wie bekomme ich das „Ganze“ in Berichtsform ?
  - ... ?
  - ... ?

PG Technische Ermittlungsunterstützung

Untersuchungen an

APPLE IOS

PG Technische Ermittlungsunterstützung

locationDaemon /-Datenbank

RheinlandPfalz
POLIZEIPRÄSIDIUM KOBLENZ

- Speicherort: /private/var/root/Library/Caches/locationd
  - seit iOS 4.0 bis iOS 4.3.2
    - **consolidated.db** (im iTunes-Backup, keine Speicherfrist)
  - seit iOS 4.3.3
    - consolidated.db (im iTunes-Backup) (leer)
    - **cache.db** (im physical-Backup, bis zu 7 Tage)
  - in iOS 5
    - **cache_encryptedA.db** (unverschlüsselt!)
- SQLite3-Datenbank als Puffer-Speicher

PG Technische Ermittlungsunterstützung

GeoDaten von Apple

RheinlandPfalz
POLIZEIPRÄSIDIUM KOBLENZ

- **CellLocation**
- **WiFiLocation**

MCC	MNC	LAC	CI	Timestamp	Latitude	Longitude	HorizontalAccuracy	Altitude	VerticalAccuracy	Speed	Course	Confidence
262	1	38855	1914859	336687527.233497	50.34313845	7.56175976	1912.0	0.0	-1.0	-1.0	-1.0	70
262	1	38855	1931383	336687527.233497	50.34281909	7.56195545	1418.0	0.0	-1.0	-1.0	-1.0	70
262	1	10527	1931383	336687527.233497	50.34196454	7.56106489	1460.0	0.0	-1.0	-1.0	-1.0	60

MAC	Timestamp	Latitude	Longitude	HorizontalAccuracy	Altitude	VerticalAccuracy	Speed	Course	Confidence
0:1c:f0:5d:d:a7	336728358.030818	50.34228074	7.55155771	50.0	75.0	21.0	-1.0	-1.0	50
0:1f:3f:55:e8:2b	336728358.030818	50.34220075	7.55158233	50.0	71.0	5.0	-1.0	-1.0	50
c0:25:6:e:f0:39	336728358.030818	50.34215962	7.55156248	50.0	67.0	6.0	-1.0	-1.0	50
bc:5:43:4f:32:c0	336728358.030818	50.34209638	7.55162566	50.0	76.0	5.0	-1.0	-1.0	50
0:1c:10:42:d0:ac	336728358.030818	50.3424949	7.55142909	50.0	83.0	18.0	-1.0	-1.0	50
78:ca:39:48:db:23	336728358.030818	50.34199208	7.55166333	50.0	76.0	13.0	-1.0	-1.0	50
0:15:c:a:ed:be	336728358.030818	50.34257471	7.55142003	50.0	78.0	11.0	-1.0	-1.0	50
0:1a:4f:3a:42:9	336728358.030818	50.34196728	7.55159574	119.0	81.0	19.0	-1.0	-1.0	50
f0:7d:68:4e:83:12	336728358.030818	50.34210222	7.55109912	50.0	84.0	17.0	-1.0	-1.0	50

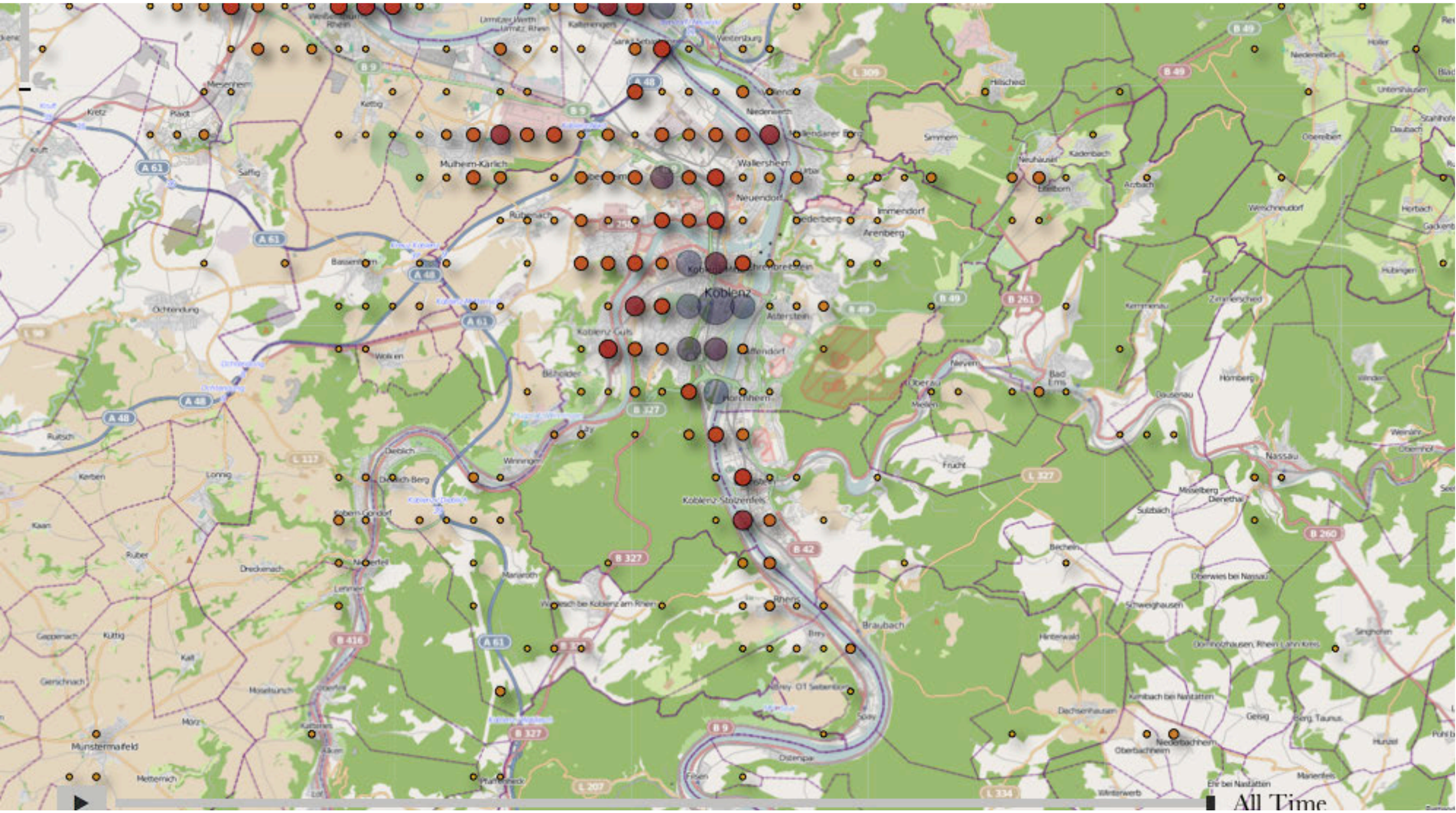
- Individuelle Repräsentation der Quelle
  - MCC, MNC, LAC, CI (Funkzellen)
  - MAC (WLAN)
- Datum des Abrufs der Daten von Apple
  - Zeitstempel in CFAbsoluteTime
- Geo-Position der Quelle
  - Längen- und Breitengrad
- Sendereichweite der Quelle
  - Horizontale- und Vertikale Akkuratesse
- Verlässlichkeit der Ortsgenauigkeit

PG Technische Ermittlungsunterstützung

iPhoneTracker

http://petewarden.github.com/iPhoneTracker/

RheinlandPfalz
POLIZEIPRÄSIDIUM KOBLENZ

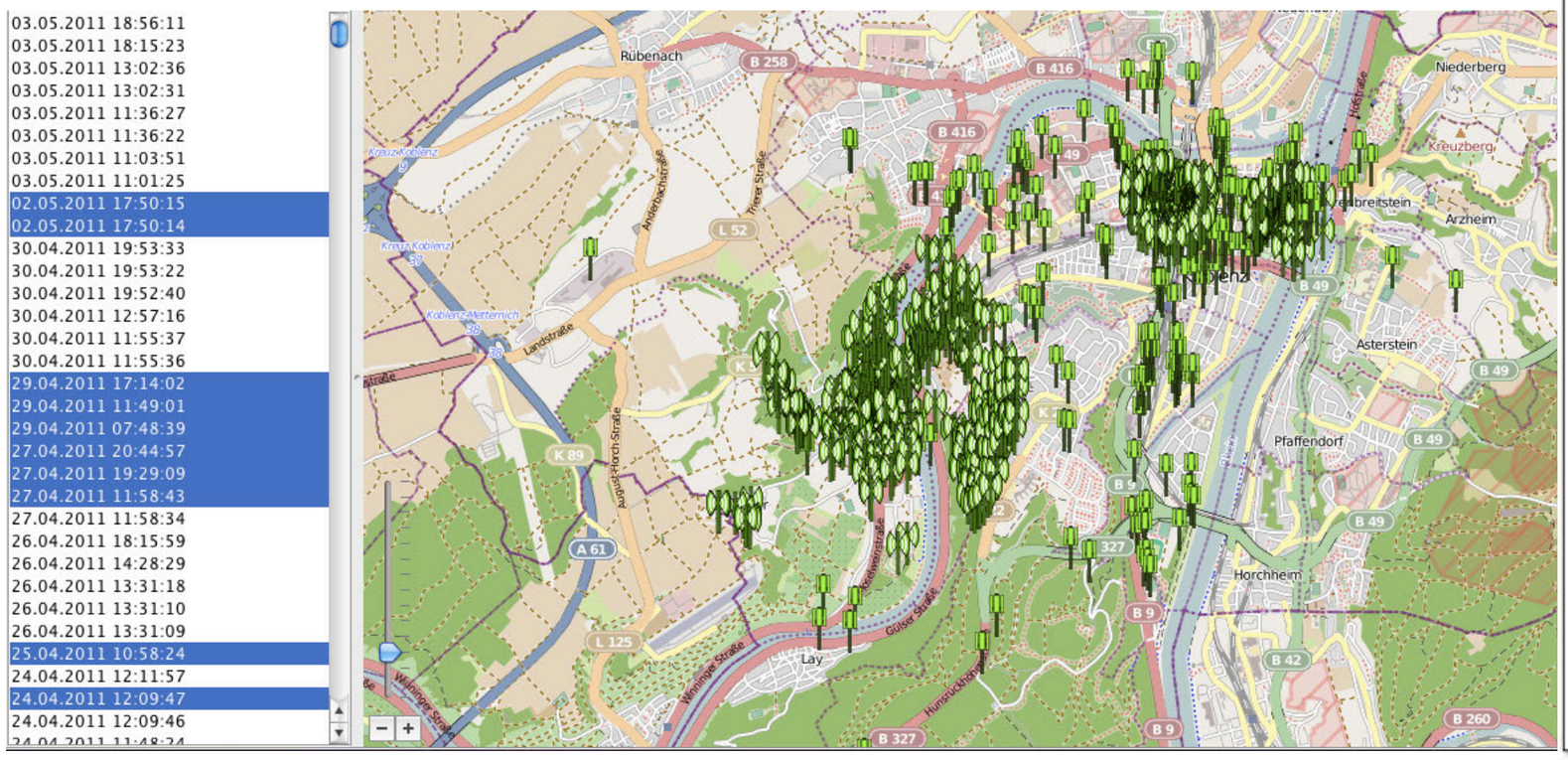


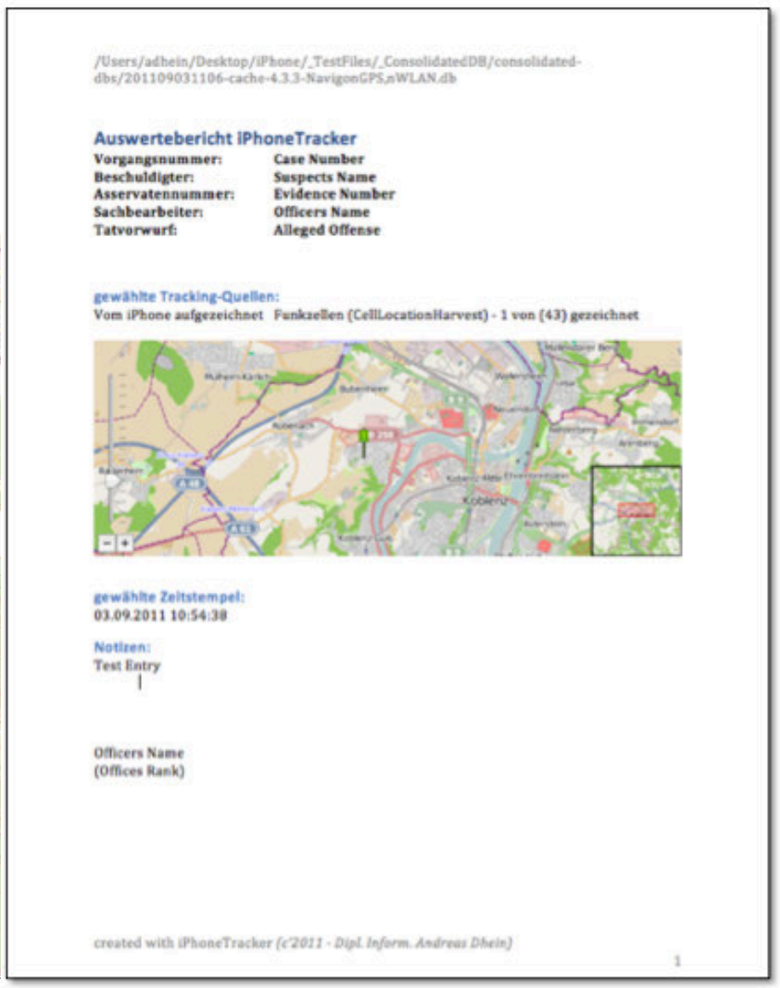
iPhoneTrackerLE

(Eigenentwicklung)

RheinlandPfalz
POLIZEIPRÄSIDIUM KOBLENZ

- Keine Rasterung !!!
- Unterscheidung zw. Funkzellen- und WiFi- Daten
- Einzelne Zeitstempel auswählbar
- Bericht generieren




/Users/adhein/Desktop/iPhone/_TestFiles/_ConsolidatedDB/consolidated-dbs/201109031106-cache-4.3.3-NavigonGPS,nWLAN.db

Auswertebericht iPhoneTracker

Vorgangsnummer:	**Case Number**
Beschuldigter:	**Suspects Name**
Asservatennummer:	**Evidence Number**
Sachbearbeiter:	**Officers Name**
Tatvorwurf:	**Alleged Offense**

gewählte Tracking-Quellen:
Vom iPhone aufgezeichnet Funkzellen (CellLocationHarvest) - 1 von (43) gezeichnet

gewählte Zeitstempel:
03.09.2011 10:54:38

Notizen:
Test Entry

Officers Name
(Offices Rank)

created with iPhoneTracker *(c'2011 - Dipl. Inform. Andreas Dhein)*

Apple iOS

ERFAHRUNGEN/PROBLEME

PG Technische Ermittlungsunterstützung

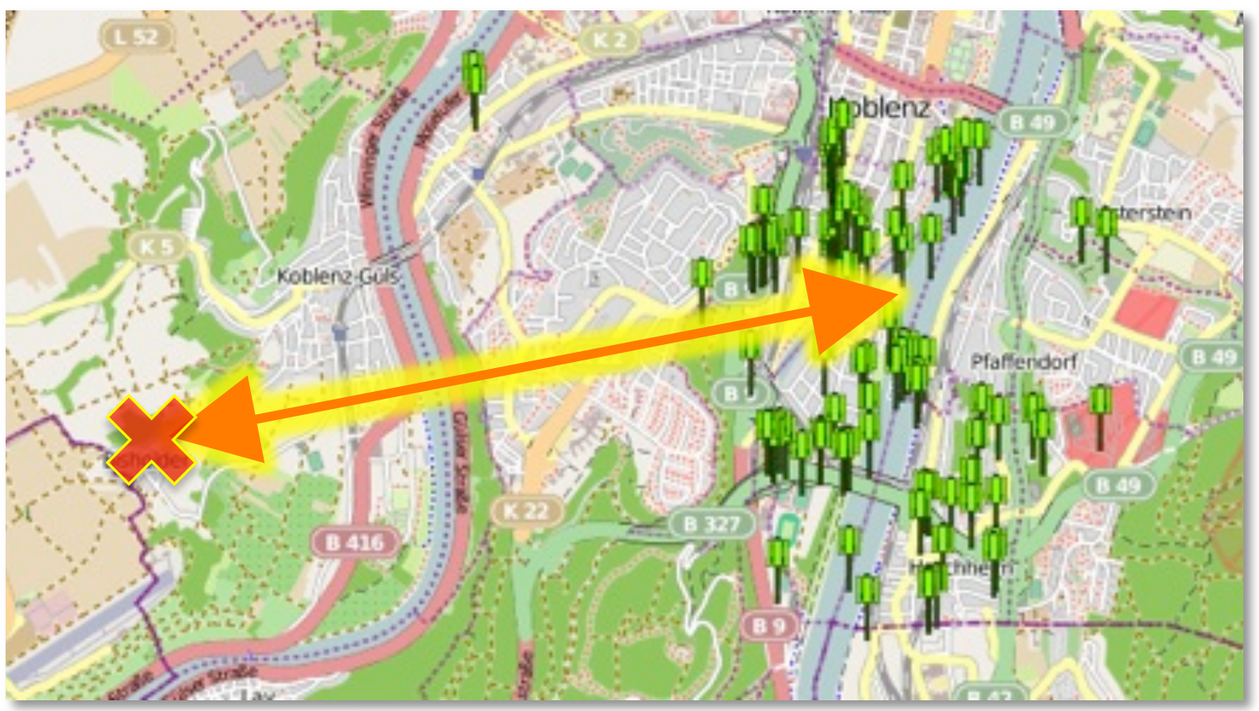
Erfahrungen / Probleme

» Mehrere Quellen für einen Zeitstempel

» Wo war das iPhone ?

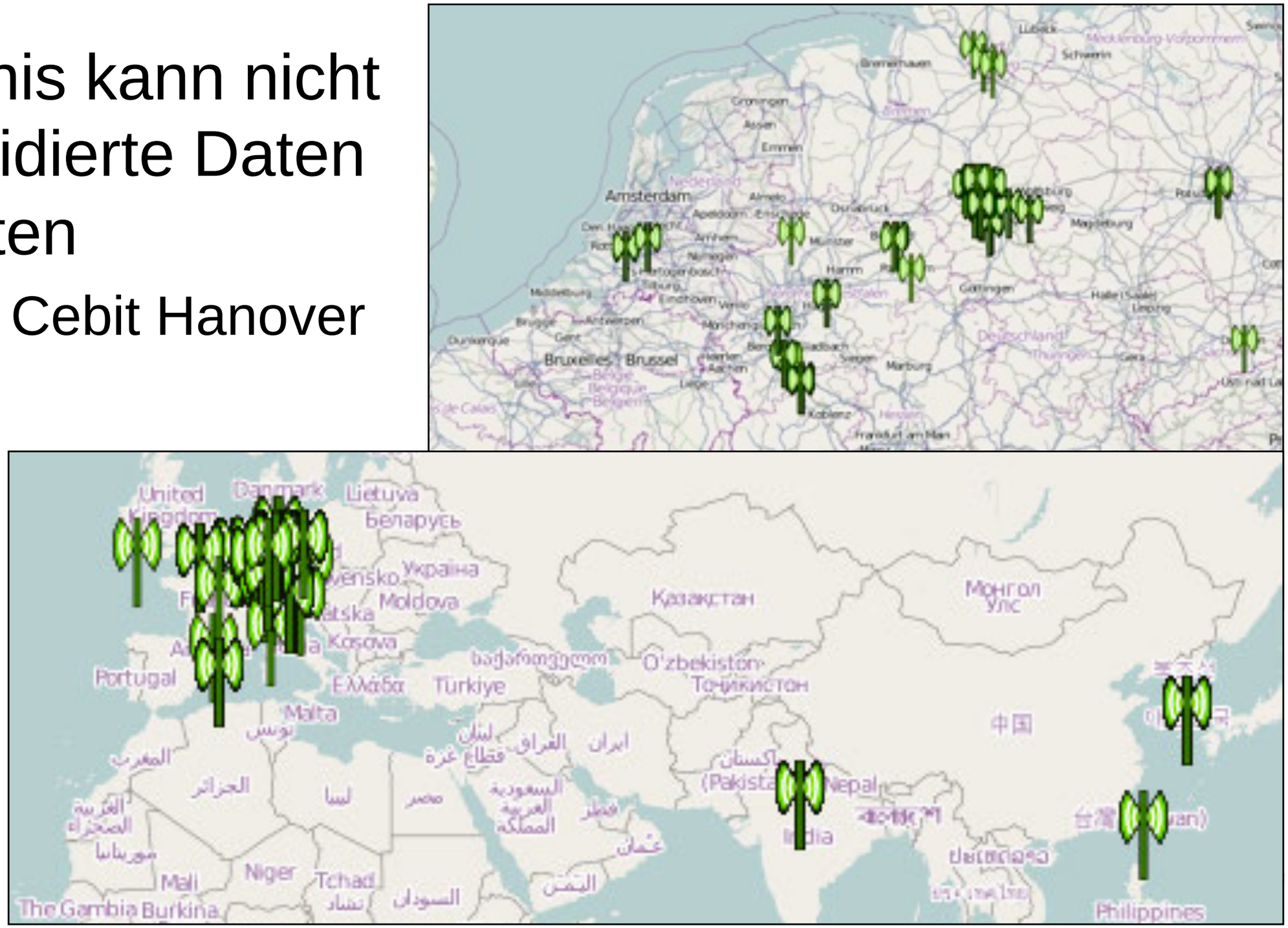
» i.d.R. im „Mittel“

» Kann schief gehen !



Erfahrungen / Probleme

- Ergebnis kann nicht konsolidierte Daten enthalten
  - Bsp. Cebit Hanover



Assisted GPS (aGPS)

- Ziel
  - immer und überall verfügbar
  - ressourcenschonend, schnell

- Problem
  - GPS (nicht in Gebäuden, „frisst“ Batterien)
  - Funkzellen (keine Geokoordinaten)
  - WiFi (keine Geokoordinaten)

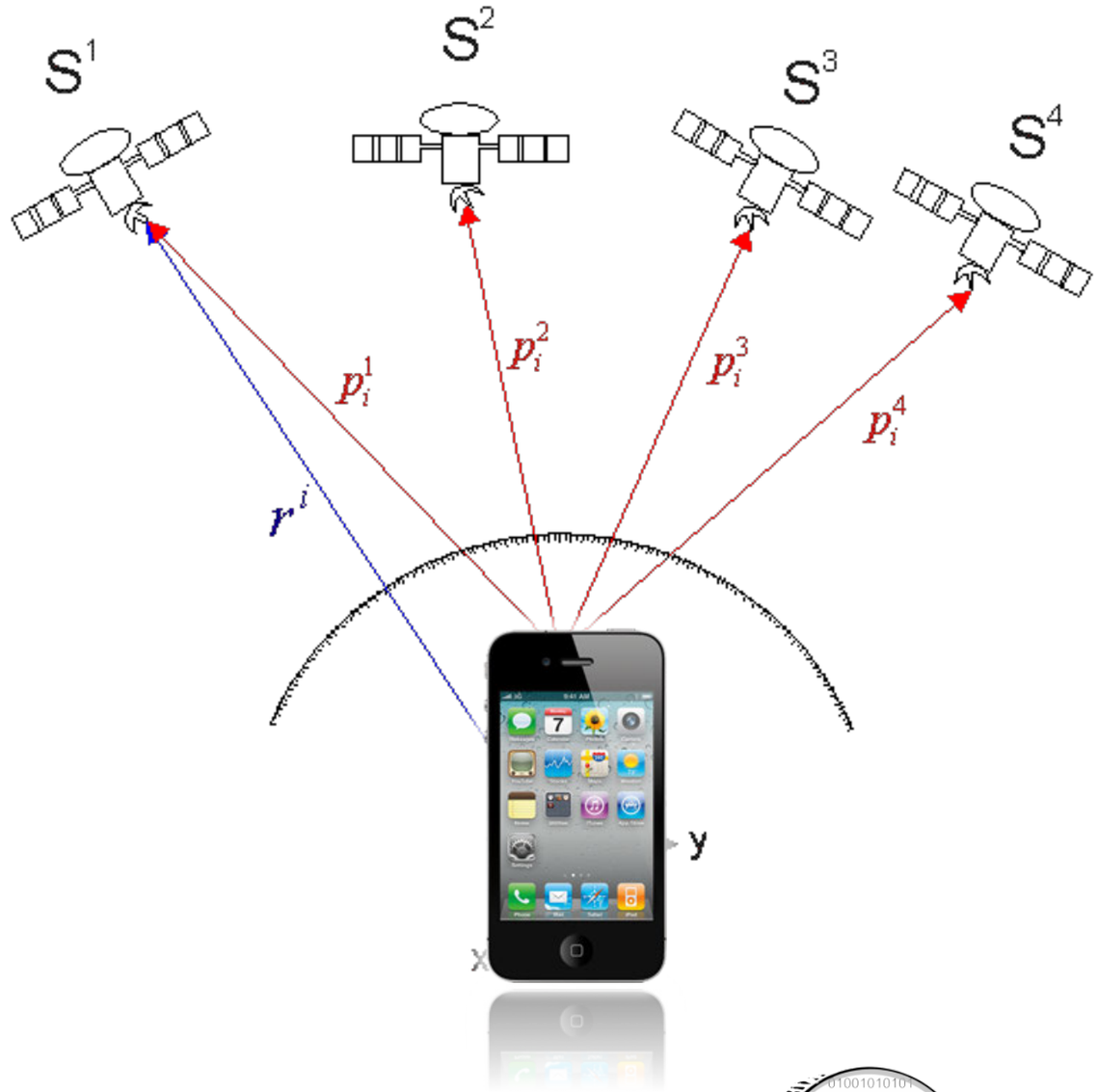
- Lösung
  - „Schwarm-Kartierung“

PG Technische Ermittlungsunterstützung

Schwarm-Kartierung (iPhone)

RheinlandPfalz
POLIZEIPRÄSIDIUM KOBLENZ

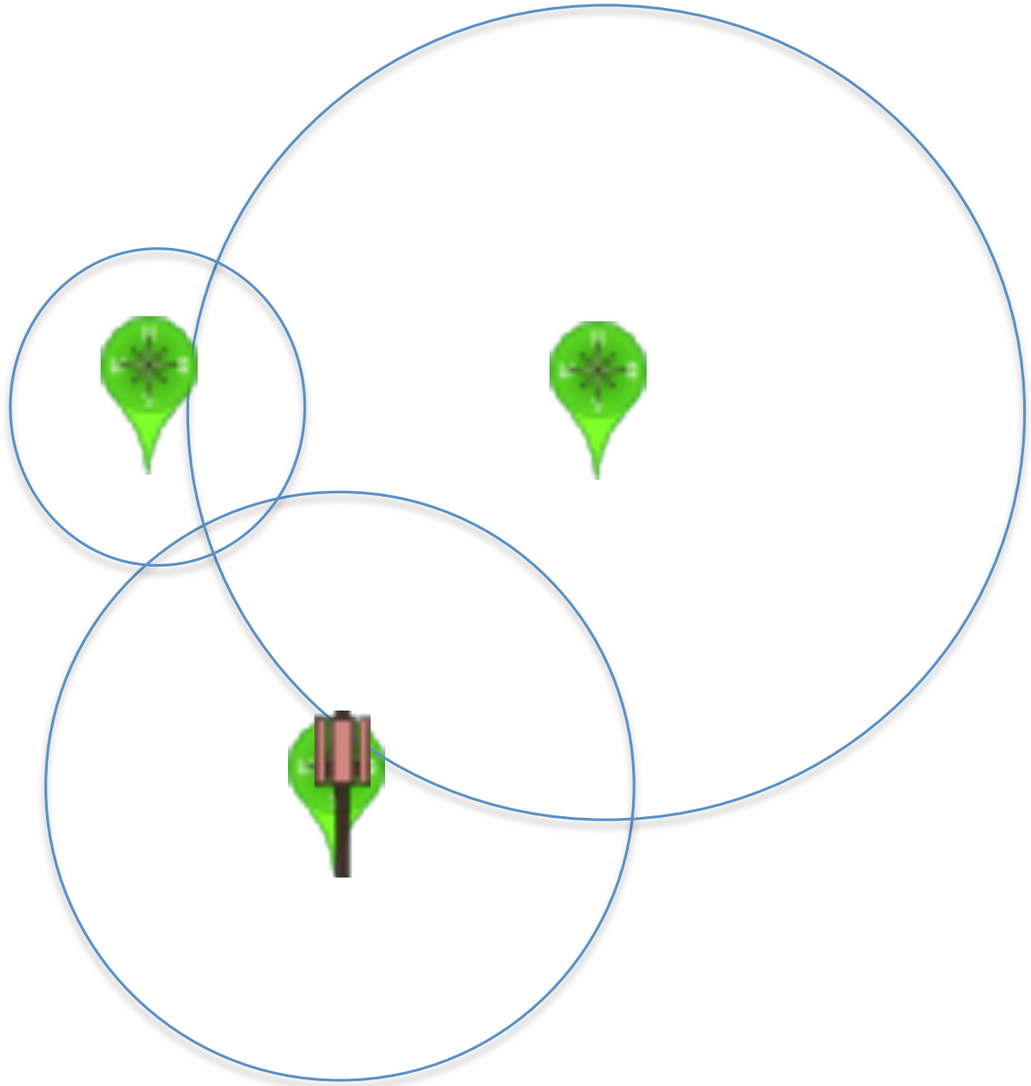
1. Daten sammeln
   - » auf dem iPhone
2. Daten übermitteln
   - » Daten „consolidieren“
3. Daten abrufen
   - » von Apple



PG Technische Ermittlungsunterstützung

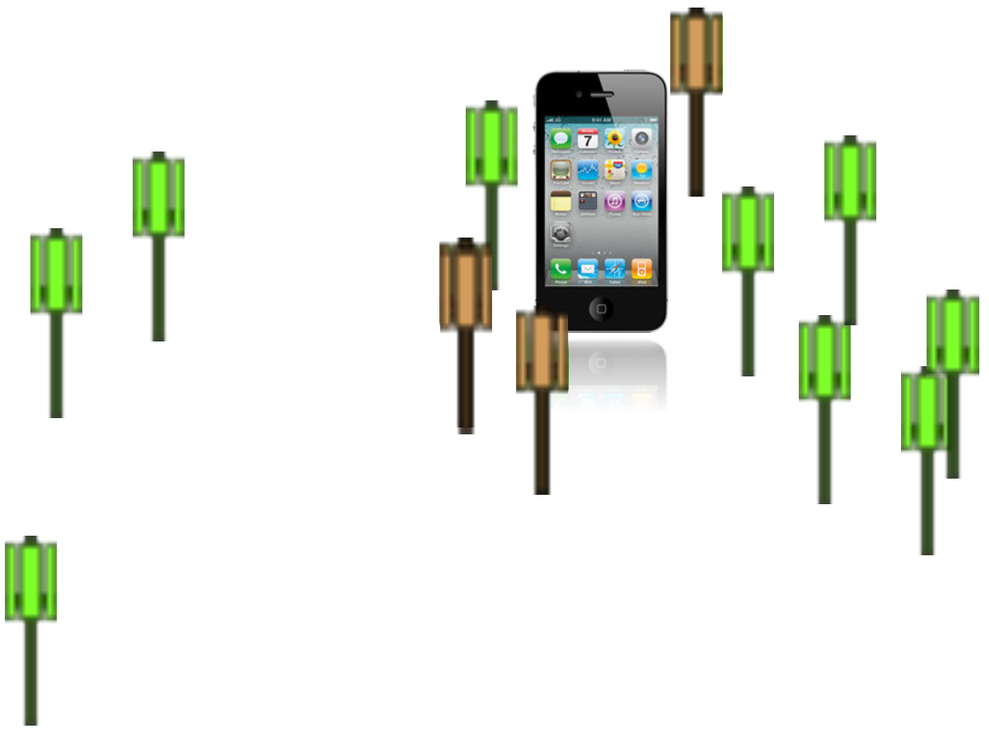
Schwarm-Kartierung (iPhone)

1. Daten sammeln
   - » auf dem iPhone
2. Daten übermitteln
   - » Daten „consolidieren“
3. Daten abrufen
   - » von Apple



Schwarm-Kartierung (iPhone)

1. Daten sammeln
   - » auf dem iPhone
2. Daten übermitteln
   - » Daten „consolidieren“
3. Daten abrufen
   - » von Apple



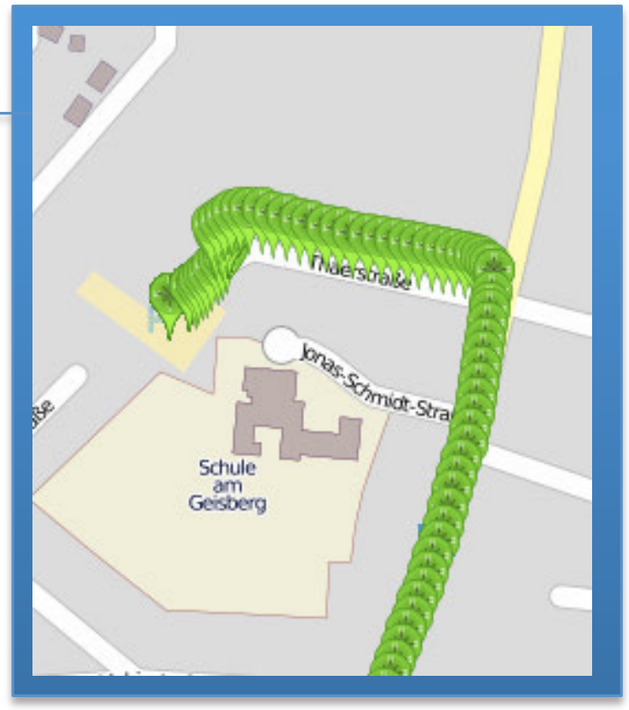
Es muss also auch irgendwo GPS-Daten geben?!

PG Technische Ermittlungsunterstützung

Schwarmkartierung (Praxis)

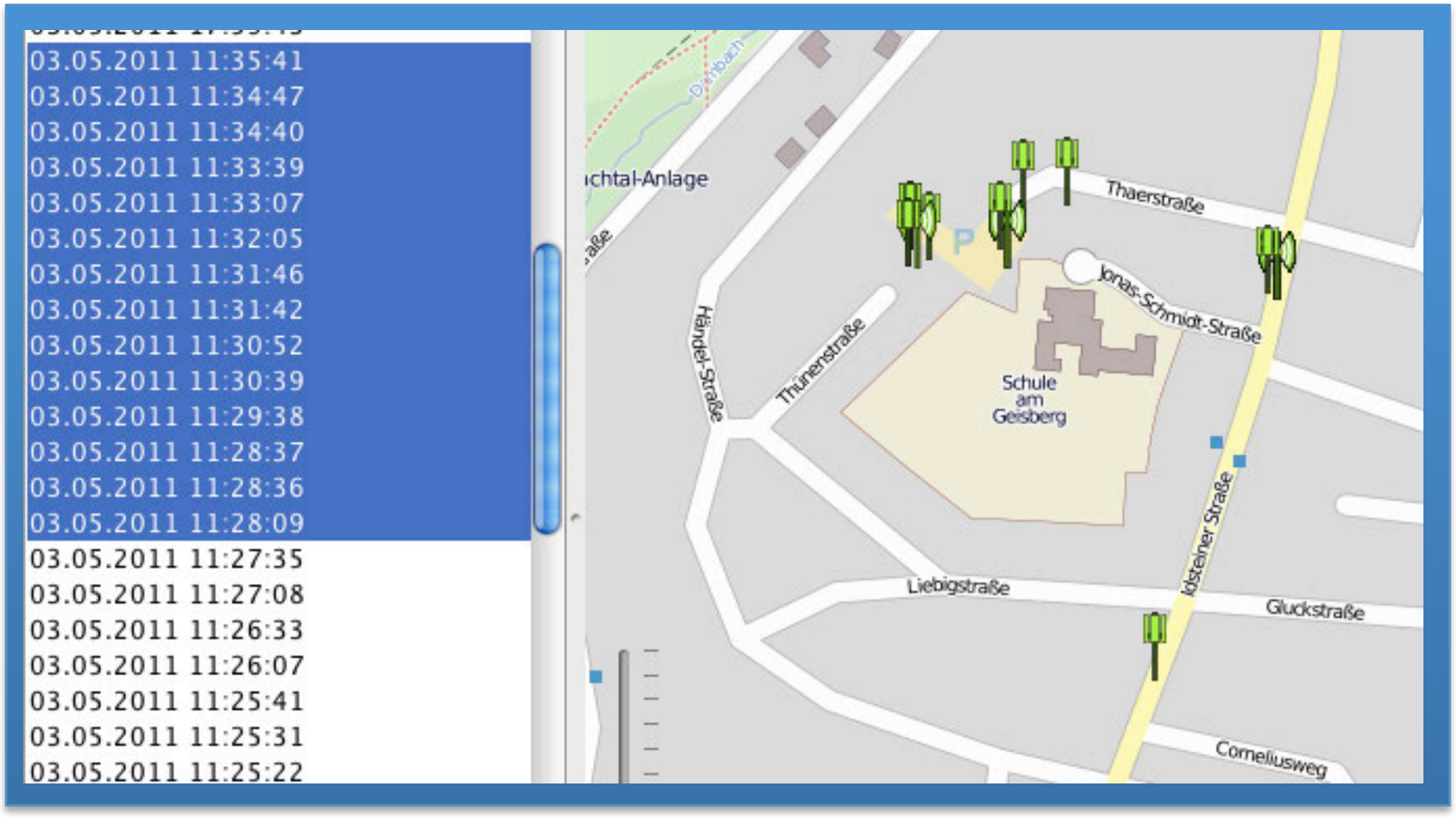
RheinlandPfalz
POLIZEIPRÄSIDIUM KOBLENZ

- Das iPhone verfügt über einen GPS-Sensor
  - kann als Navi verwendet werden (z.B. Navigon)
  - kein Bezug für Andere
  - zu viele Datensätze!!!



Schwarmkartierung (Praxis)

» Interessante Informationen (Funkzellen und WiFi)
  » Echte GPS-Daten des iPhones
  » führt zu einer erheblichen Datenreduktion



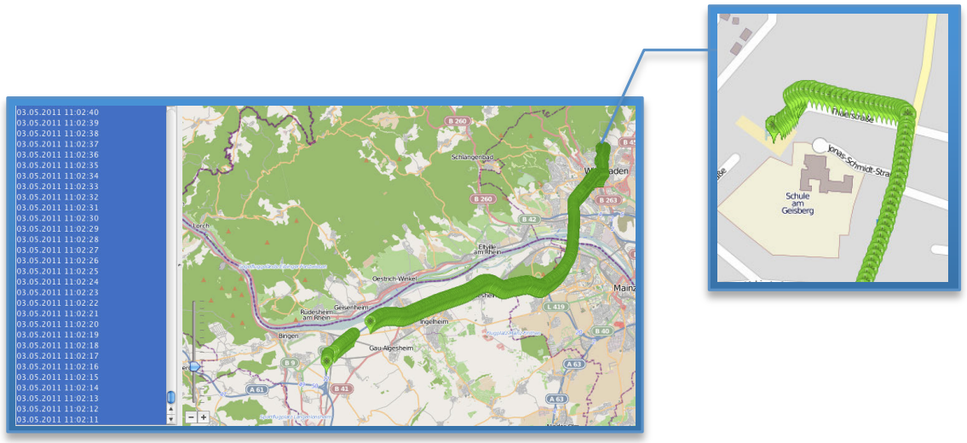
PG Technische Ermittlungsunterstützung

LocationHarvest

RheinlandPfalz
POLIZEIPRÄSIDIUM KOBLENZ

Timestamp	Latitude	Longitude	HorizontalAccuracy	Altitude	VerticalAccuracy	Speed	Course	Co...	TripId	Context
326107824.847468	50.0959116833333	8.24361396666667	47.421633549...	191.230...	70.281001375...	0.0	216.0	90	508DDB35-3823-404D-A08D-F158E5C19E44	402
326107825.842139	50.0959116833333	8.24361396666667	47.421633549...	191.230...	70.281001375...	0.0	216.0	90	508DDB35-3823-404D-A08D-F158E5C19E44	402
326107826.842839	50.0959116833333	8.24361396666667	47.421633549...	191.230...	70.281001375...	0.0	216.0	90	508DDB35-3823-404D-A08D-F158E5C19E44	402
326131212.522883	50.08654815	8.2440175	162.95795319...	132.225...	228.34367325...	2.36644444444444	94.0	90	48C1CCD4-26B7-40A3-BA63-3D5CD48B9BD1	502
326131213.533959	50.0865217833333	8.24409906666667	162.95795319...	132.225...	228.34367325...	2.46933333333333	96.0	90	48C1CCD4-26B7-40A3-BA63-3D5CD48B9BD1	502

- » Datumsangabe zu dem gespeicherten Wegpunkt
  - » Zeitstempel in CFAbsoluteTime (lokal)
- » Geo-Position des iPhones
  - » Längen- und Breitengrad, Höhenangabe
- » Genauigkeit der Positionsbestimmung
  - » Horizontale- und Vertikale Akkuratesse
- » Navigationsinformationen
  - » Geschwindigkeit in m/s
  - » Kurs in Grad
    - » 000 = Norden
    - » 090 = Osten
    - » 180 = Süden
    - » 270 = Westen
- » Verlässlichkeit der Ortsgenauigkeit
  - » confidence immer 90 (höchste Genauigkeit)
- » TripId and Context
  - » Nutzen bisher unbekannt, wird nicht weiter benutzt



PG Technische Ermittlungsunterstützung

CellLocationHarvest

Rheinland-Pfalz
POLIZEIPRÄSIDIUM KOBLENZ

MCC	MNC	LAC	CI	RSSI	ARFCN	PSC	RSCP	ECN0	Operator	Tran...	BundleId	Timestamp	Latitude	Longit...	Horiz...	Altitude	Vertica...	Speed	Course	Confic
262	1	26891	12807	-82	-1	-1	-1	-1	T-Mobile D	-1	com.navigon.NavigonSelectTmoD	32610752...	50.082...	8.244...	17.06...	145.2...	23.16...	9.56...	354.0	90
262	1	26891	12783	-73	-1	-1	-1	-1	T-Mobile D	-1	com.navigon.NavigonSelectTmoD	32610754...	50.083...	8.244...	17.06...	142.2...	23.16...	11.8...	354.0	90
262	1	26891	12752	-88	-1	-1	-1	-1	T-Mobile D	-1	com.navigon.NavigonSelectTmoD	32610756...	50.086...	8.243...	17.06...	139.2...	23.16...	12.4...	316.0	90
262	1	26891	12752	-65	-1	-1	-1	-1	T-Mobile D	-1	com.navigon.NavigonSelectTmoD	32610762...	50.088...	8.243...	47.42...	135.2...	70.28...	7.35...	28.0	90
262	1	26891	12752	-70	-1	-1	-1	-1	T-Mobile D	-1	com.navigon.NavigonSelectTmoD	32610768...	50.093...	8.245...	17.06...	143.2...	23.16...	9.77...	20.0	90

- Individuelle Repräsentation der Quelle
  - MCC, MNC, LAC, CI (wie in CellLocation)
  - zusätzlich: ARFCN, PSC, RSCP, ECN0, Operator, Transmit, BundleId
- Datumsangabe zu dem gespeicherten Wegpunkt
  - Zeitstempel in CFAbsoluteTime (lokal)
- Geo-Position der Quelle
  - Längen- und Breitengrad, Höhenangabe
- Genauigkeit der Positionsbestimmung
  - Horizontale- und Vertikale Akkuratesse
- Navigationsinformationen
  - Geschwindigkeit in m/s
  - Kurs in Grad
    - 000 = Norden
    - 090 = Osten
    - 180 = Süden
    - 270 = Westen
- Verlässlichkeit der Ortsgenauigkeit
  - confidence immer 90 (höchste Genauigkeit)

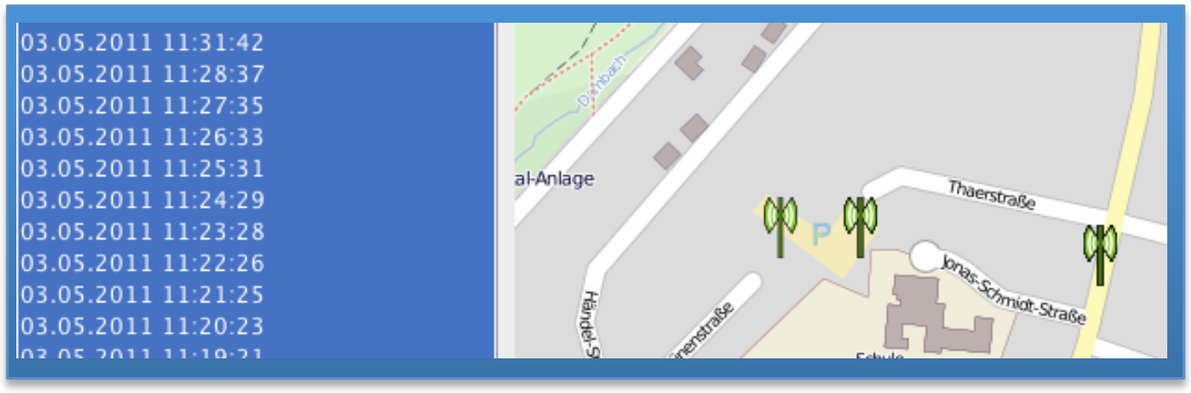
PG Technische Ermittlungsunterstützung

WiFiLocationHarvest

Rheinland-Pfalz
POLIZEIPRÄSIDIUM KOBLENZ

MAC	Channel	Hidden	RSSI	Age	BundleId	Timestamp	Latitude	Longitude	Horizontal...	Altitude	Vertical...	Speed	Course	Confidence
0:24:fe:4a:f1:cb	10	0	-76	0.0	com.navigon.NavigonSelectTmoD	326107099.844842	50.066...	8.22258...	17.0684...	150.216...	23.164...	6.27...	46.0	90
0:22:b0:62:f8:3d	1	0	-95	0.0	com.navigon.NavigonSelectTmoD	326107161.842851	50.069...	8.22608...	17.0684...	165.217...	23.164...	0.0	34.0	90
0:25:5e:25:ac:c8	6	0	-91	0.0	com.navigon.NavigonSelectTmoD	326107161.842851	50.069...	8.22608...	17.0684...	165.217...	23.164...	0.0	34.0	90
0:1d:19:d6:9a:8c	1	0	-99	1.662	com.navigon.NavigonSelectTmoD	326107223.847171	50.071...	8.22902...	47.4216...	171.218...	70.281...	9.26	36.0	90
0:24:fe:d1:17:1f	1	0	-98	1.662	com.navigon.NavigonSelectTmoD	326107223.847171	50.071...	8.22902...	47.4216...	171.218...	70.281...	9.26	36.0	90

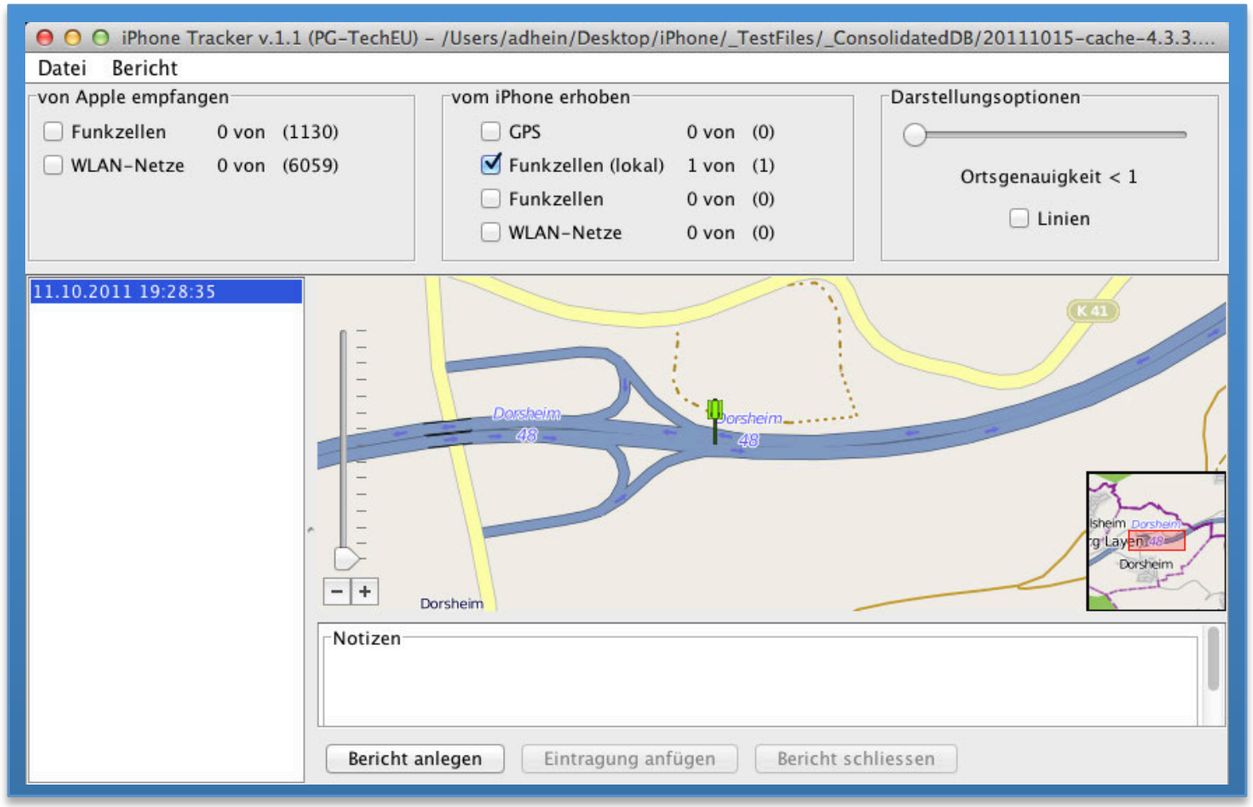
- Individuelle Repräsentation der Quelle
  - MAC-Adresse (wie in WifiLocation)
  - zusätzlich: Channel, Hidden, RSSI (db), Age, BundleId
- Datumsangabe zu dem gespeicherten Wegpunkt
  - Zeitstempel in CFAbsoluteTime (lokal)
- Geo-Position der Quelle
  - Längen- und Breitengrad, Höhenangabe
- Genauigkeit der Positionsbestimmung
  - Horizontale- und Vertikale Akkuratesse
- Navigationsinformationen
  - Geschwindigkeit in m/s
  - Kurs in Grad
    - 000 = Norden
    - 090 = Osten
    - 180 = Süden
    - 270 = Westen
- Verlässlichkeit der Ortsgenauigkeit
  - confidence immer 90 (höchste Genauigkeit)

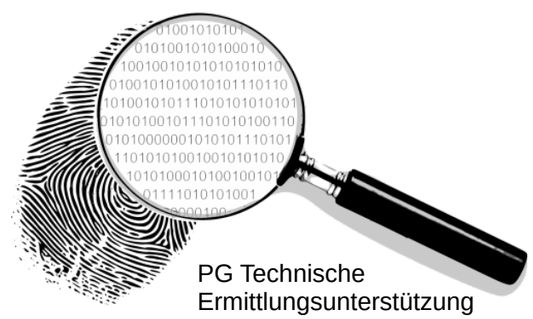


PG Technische Ermittlungsunterstützung

CellLocationLocal

- Dem Namen nach „Heimatfunkzelle“ (…)
- Übersteht i.d.R. die Datenübertragung an Apple
  - für einen schnelleren GPS-fix (?)



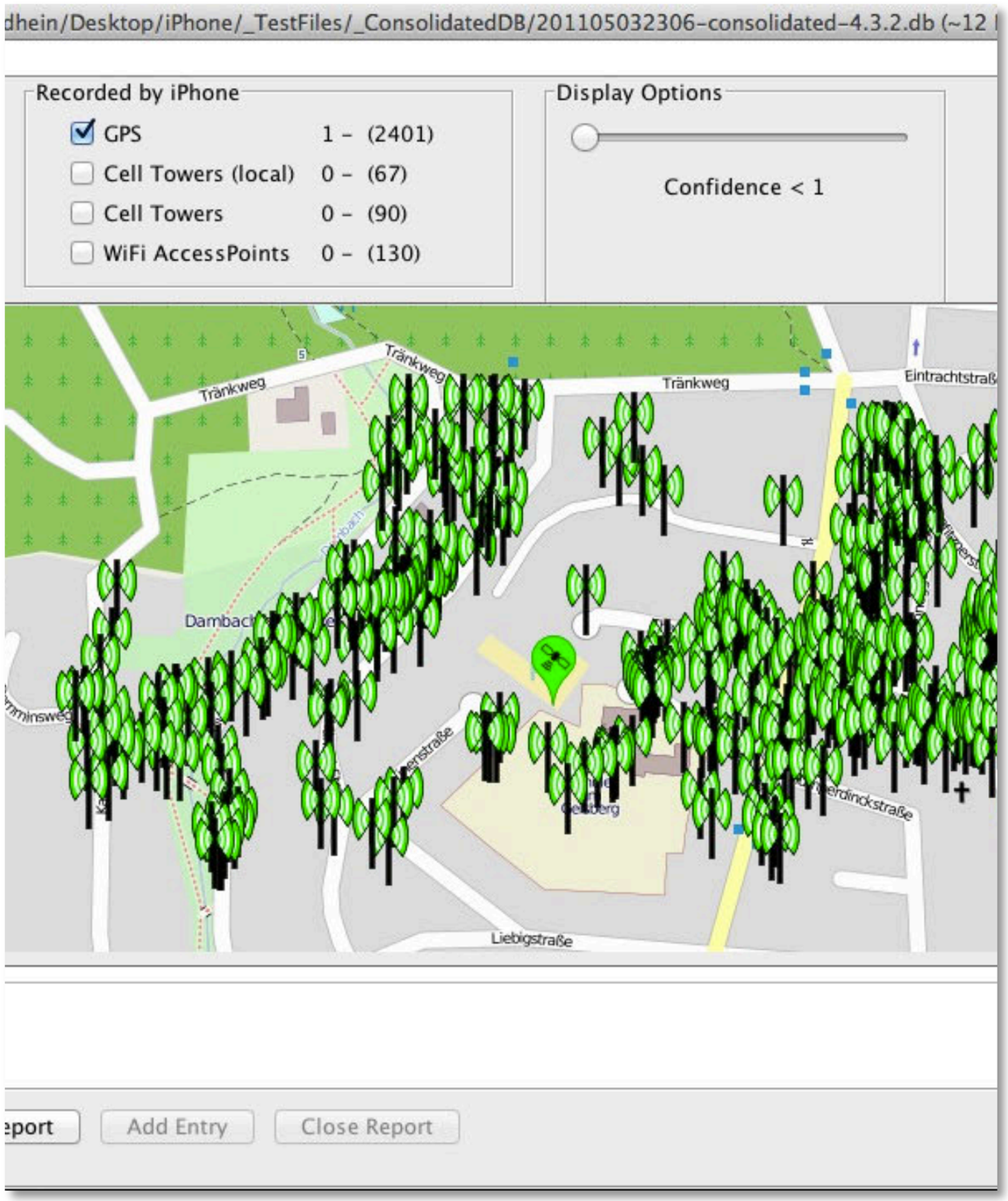


APPLE – iOS

POSITIONSBESTIMMUNG UND GENAUIGKEIT

PG Technische Ermittlungsunterstützung

Positionsbestimmung I



» Reduktion auf eine Position pro Zeitstempel

» Erster Eintrag

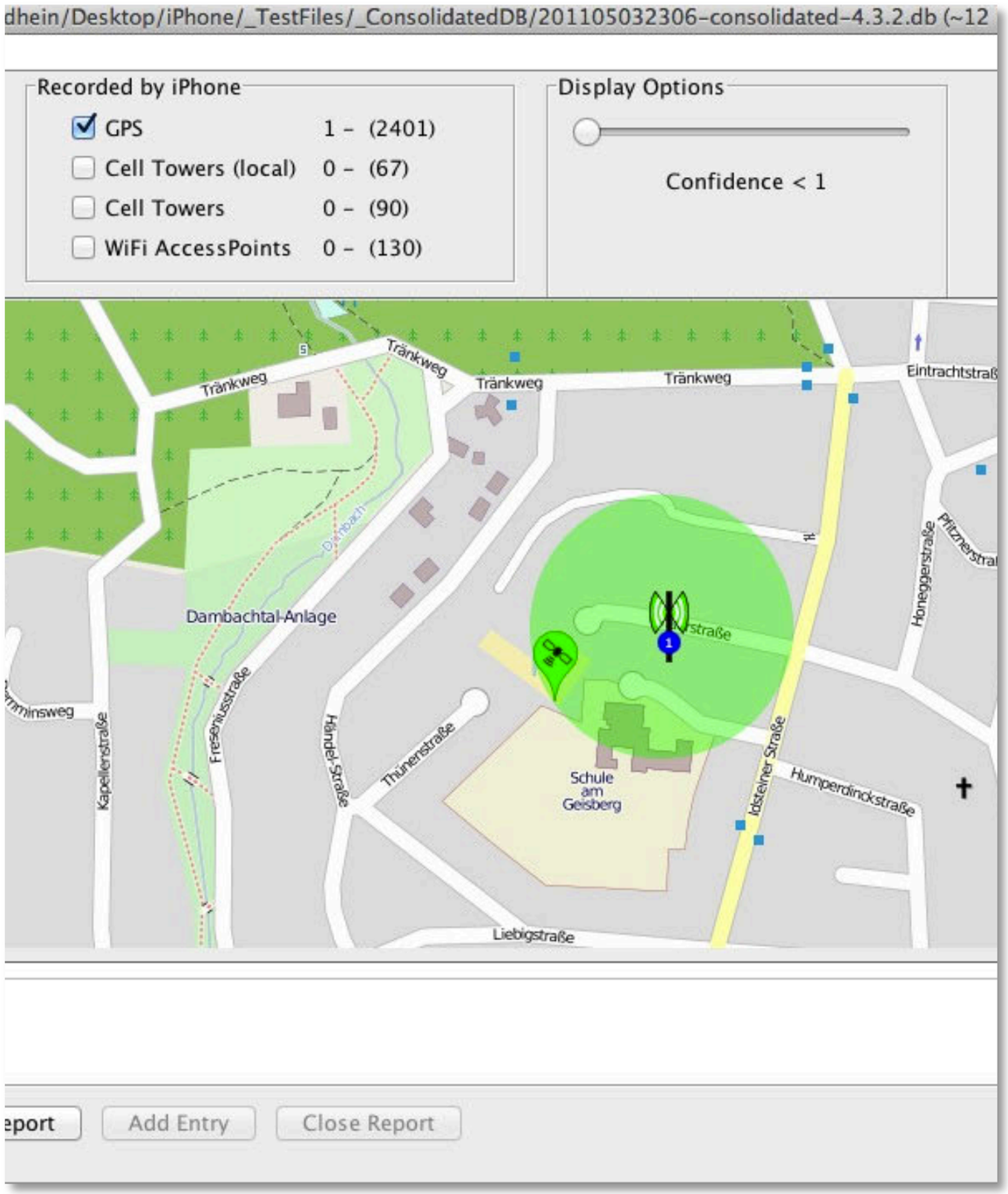
» *Mittelwert/Schwerpunkt*

» Letzter Eintrag

» forensisch notwendig!

PG Technische Ermittlungsunterstützung

Positionsbestimmung II



» Auswertungen haben ergeben:

» **Erster Eintrag**

» ~~*Mittelwert/Schwerpunkt*~~

» Letzter Eintrag

» am häufigsten.

PG Technische Ermittlungsunterstützung

Zusammenfassung Apple

- Wichtigster Grundsatz:
  - Es geht nicht um die Sender, sondern um das Gerät!!!

- Datenumfang
  - Häufig viele Daten in CellLocation, WiFiLocation
  - Meistens weniger bis keine Daten in den Harvesting Tabellen

- Genauigkeit
  - Harvesting-Daten sind zu bevorzugen

- Forensik
  - Positionsschätzung bietet brauchbare Ergebnisse
  - Positionsdaten sind in jedem Fall zu validieren

PG Technische Ermittlungsunterstützung

GOOGLE ANDROID

PG Technische Ermittlungsunterstützung

Keine Ortungsdaten?

» Standardmäßig ist Assisted-GPS deaktiviert

» Folglich keine Cachingdaten ☹

» Pfad

» /data/data/com.google.android.location/files/

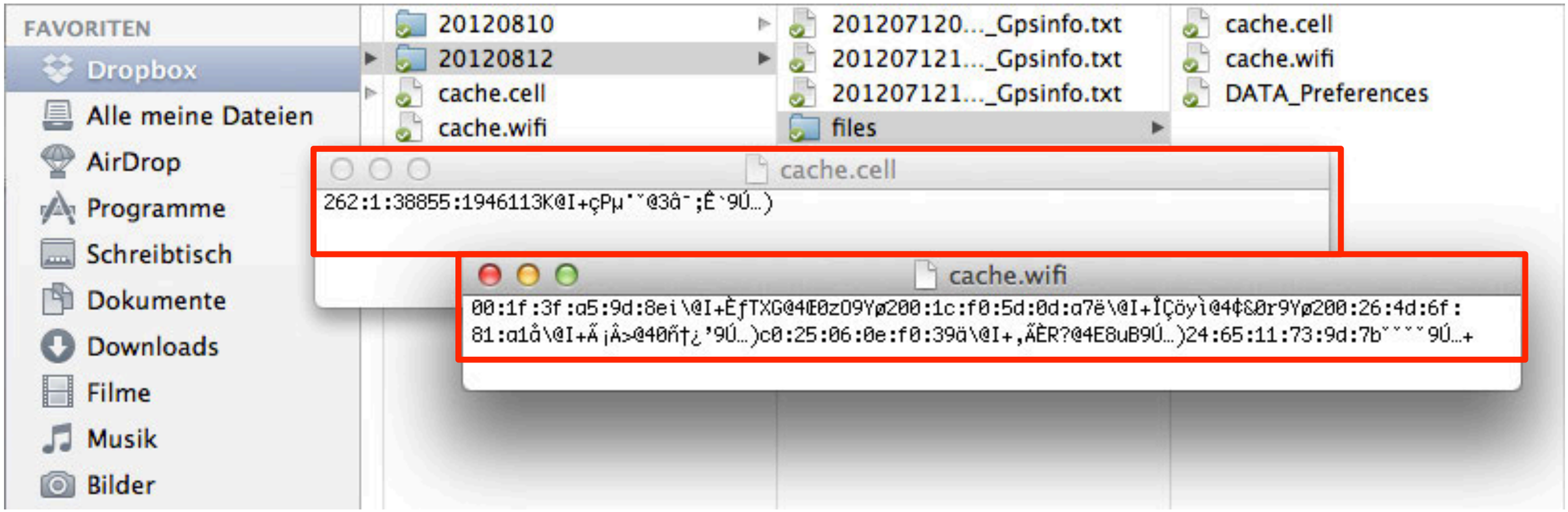
» cache.cell

» cache.wifi

PG Technische Ermittlungsunterstützung

cache.cell, cache.wifi

» Daten liegen als Bytestream vor



» Informationen in Nicht ASCII Zeichen ☹

PG Technische Ermittlungsunterstützung

Bytestream interpretieren

RheinlandPfalz
POLIZEIPRÄSIDIUM KOBLENZ

- **Header Information**
  - **2 byte** **Version** 1 bislang immer „1“
  - **2 byte** **Einträge** n Anzahl der Datensätze

- **Location Entry(ies)**
  - **n bytes** **Schlüssel** [mcc:mnc:lac:cid] cell [xx:xx:xx:xx:xx:xx] wifi
  - **4 byte** **Sendebereich** [-1:2^{31}] m
  - **4 byte** **Verlässlichkeit** [0:100] %
  - **8 byte** **Breitengrad** [-90:90]
  - **8 byte** **Längengrad** [-180:180]
  - **8 byte** **Zeitstempel** [-2^{63}:2^{63}] s UNIX-timestamp

https://github.com/packetlss/android-locdump/blob/master/parse.py

PG Technische Ermittlungsunterstützung

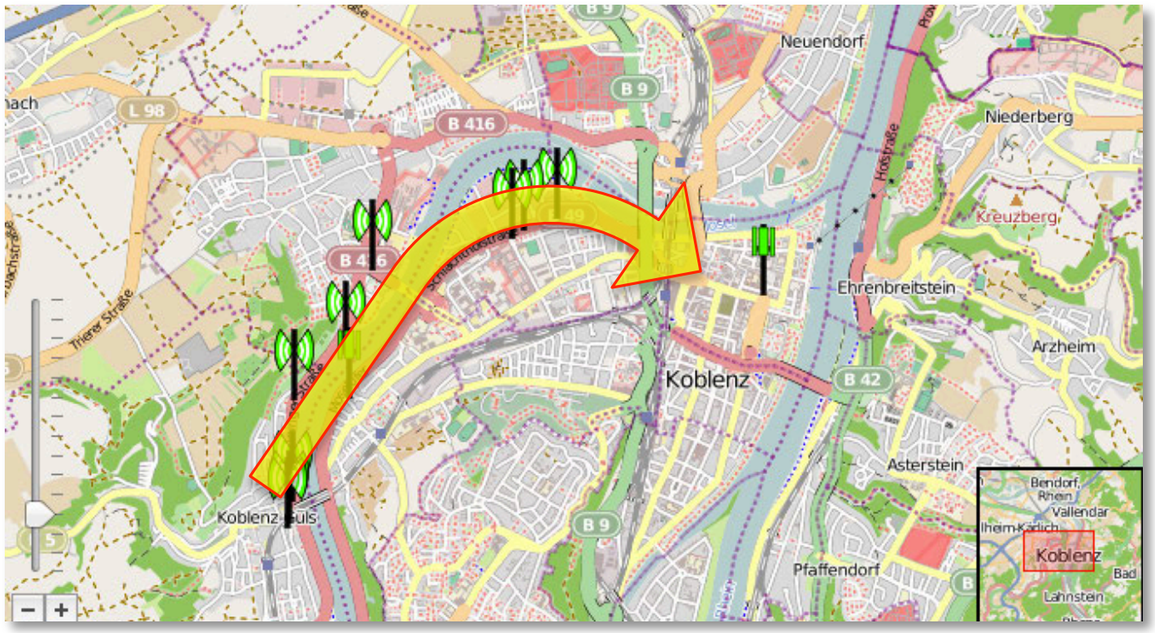
Google Android

ERFAHRUNGEN/PROBLEME

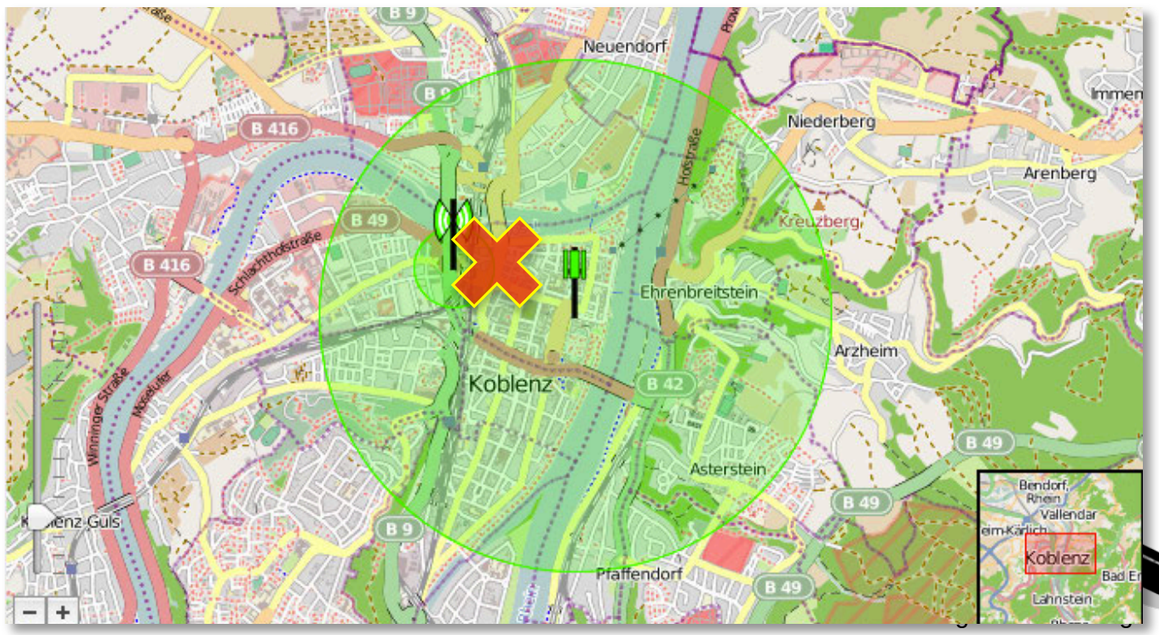
PG Technische Ermittlungsunterstützung

Positionsbestimmung

» *Zeitstempel für* Mobilfunk und WLAN *unterscheiden sich*
  » Gerät war in Bewegung



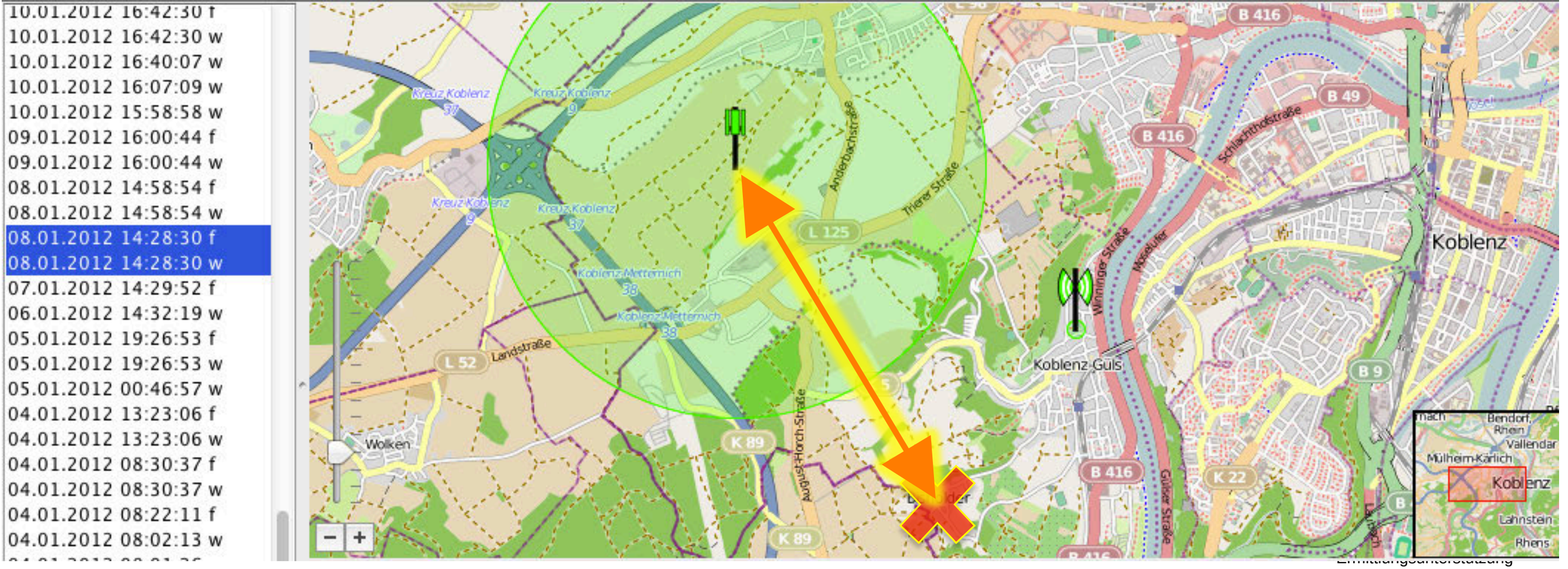
» *Zeitstempel für* Mobilfunk und WLAN *sind gleich*
  » Gerät befindet sich im Bereich des WLAN



Genauigkeit der Daten

RheinlandPfalz
POLIZEIPRÄSIDIUM KOBLENZ

- Wenn WLAN-Sendebereich außerhalb des Senderadius der Funkzelle liegt, dann
  - Aufenthaltsort nicht bestimmbar
  - Sendebereich der Funkzelle zu klein



Zusammenfassung Android

» Alle Positionsdaten werden (von Google) berechnet und müssen daher validiert werden!

» Im Idealfall betrachtet man Kombinationen von WLAN und Mobilfunkdaten pro Zeitstempel

» Wenn
  » Sendebereich Drahtlosnetzwerk innerhalb
  » Sendebereich Mobilfunknetzwerk
» dann
  » liegt die aktuelle Position innerhalb des WLAN-Bereiches

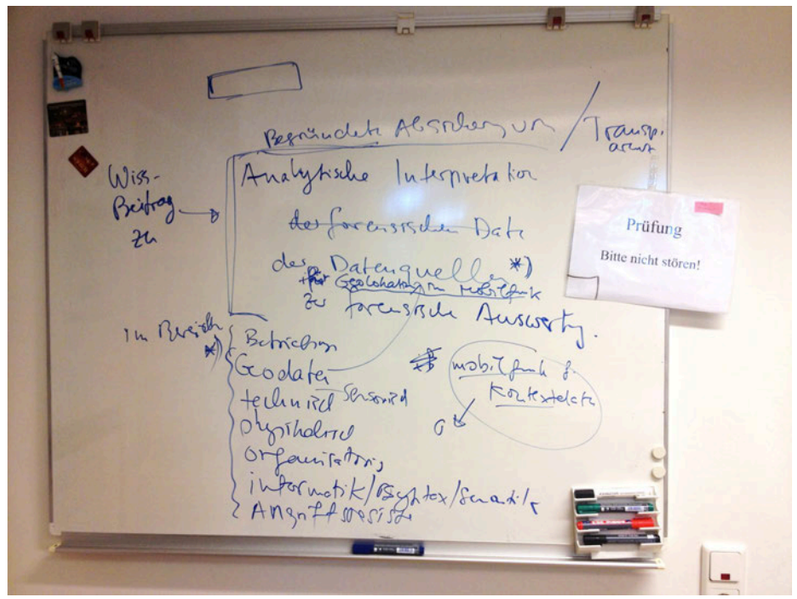
PG Technische Ermittlungsunterstützung

AKTUELLE FORSCHUNGSARBEIT

PG Technische Ermittlungsunterstützung

Promotionsvorhaben

- An der Universität Koblenz
  - Bei Prof. Grimm
  - seit 03.05.2012

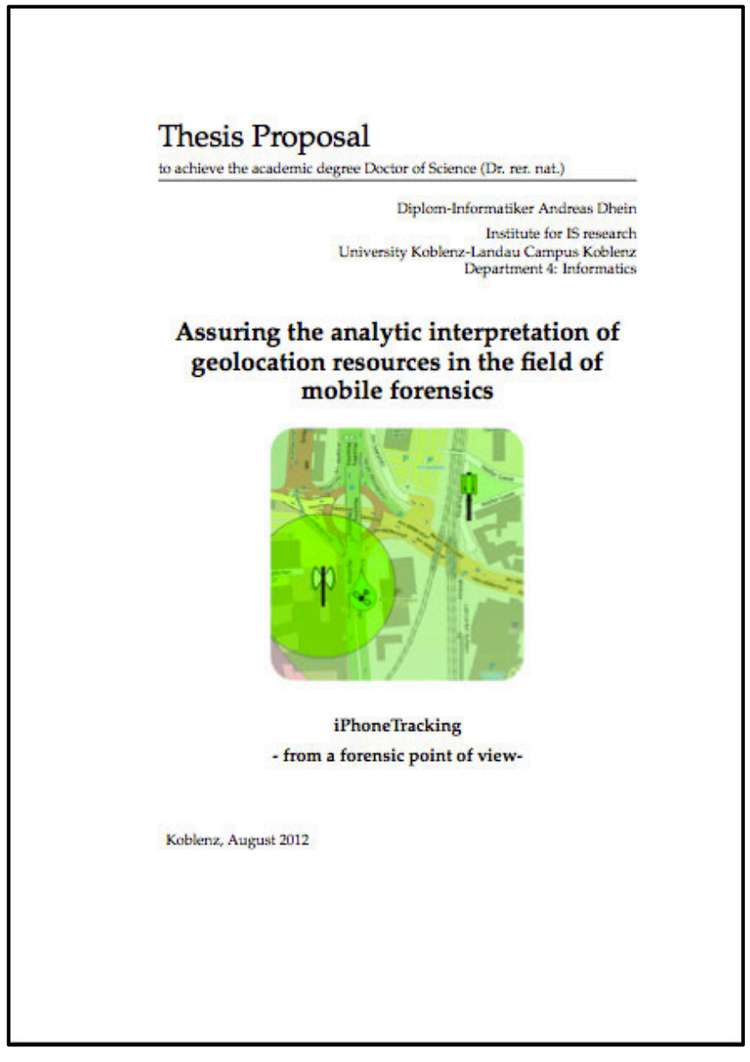


- Arbeitstitel
  - Begründete Absicherung der analytischen Interpretation der Datenquellen für Geolokalisation im Mobilfunk zur forensischen Auswertung
  - **Assuring the analytic interpretation of geolocation resources in the field of mobile forensics**


PG Technische Ermittlungsunterstützung

Forschungsfragen

- **How *accurate* are the data?** i.e. is there a measurement of accuracy for the mapping of the data (i.e. geographical data) regarding the reality the data is about (i.e. geographical place)?
- **How *complete* are the data?** i.e. is there a measurement of completeness for the mapping of the data available from the context the device was in, when the location data were produced?
- **How *reliable* are the data with respect to errors and manipulations?** What are the dimensions for proof of quality for these data in court: **are completeness, accuracy, reliability sufficient?**
- **Is there a model for proof of quality that is independent from a concrete operation system and hardware?** i.e. may the experiences from analysing iOS data be transferred to other mobile systems like Android?



Thesis Proposal

to achieve the academic degree Doctor of Science (Dr. rer. nat.)

Diplom-Informatiker Andreas Dhein

Institute for IS research
University Koblenz-Landau Campus Koblenz
Department 4: Informatics

Assuring the analytic interpretation of geolocation resources in the field of mobile forensics

iPhoneTracking
- from a forensic point of view-

Koblenz, August 2012

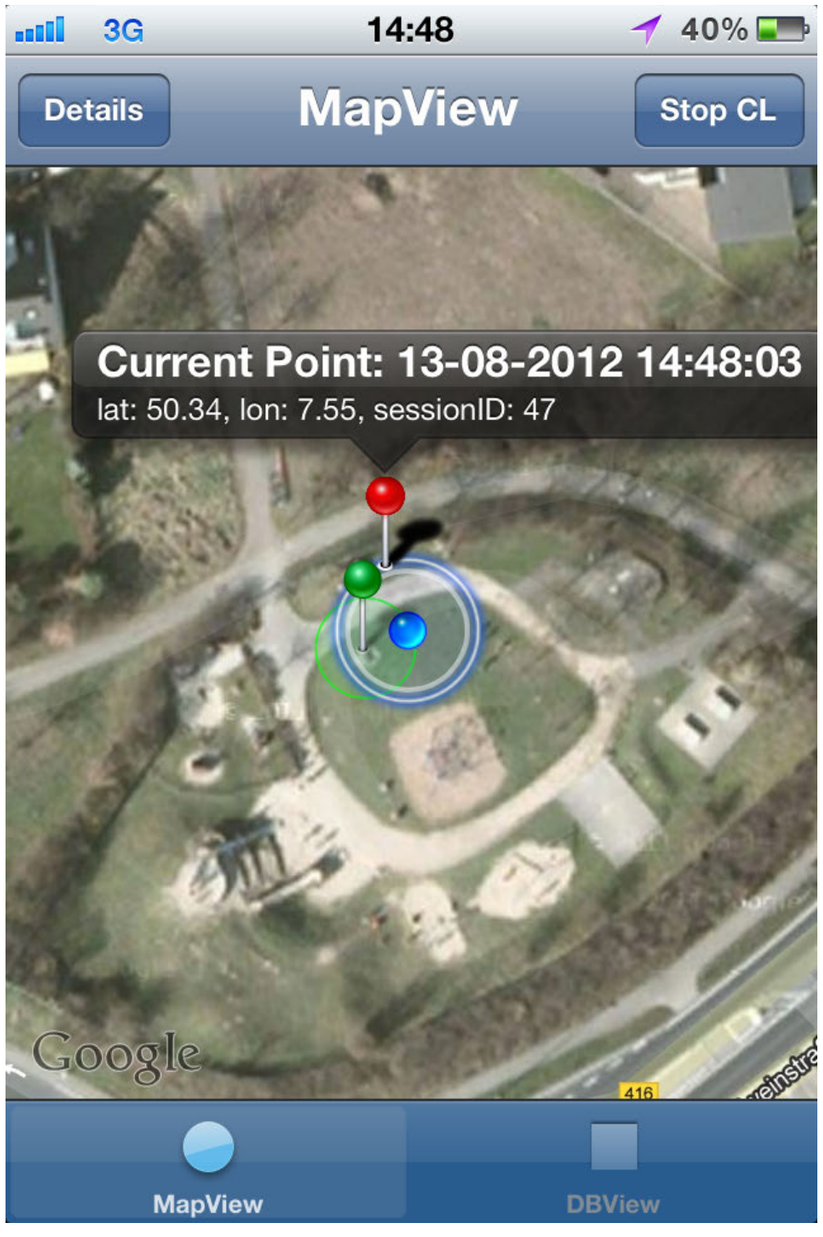
PG Technische Ermittlungsunterstützung

iOSTracker

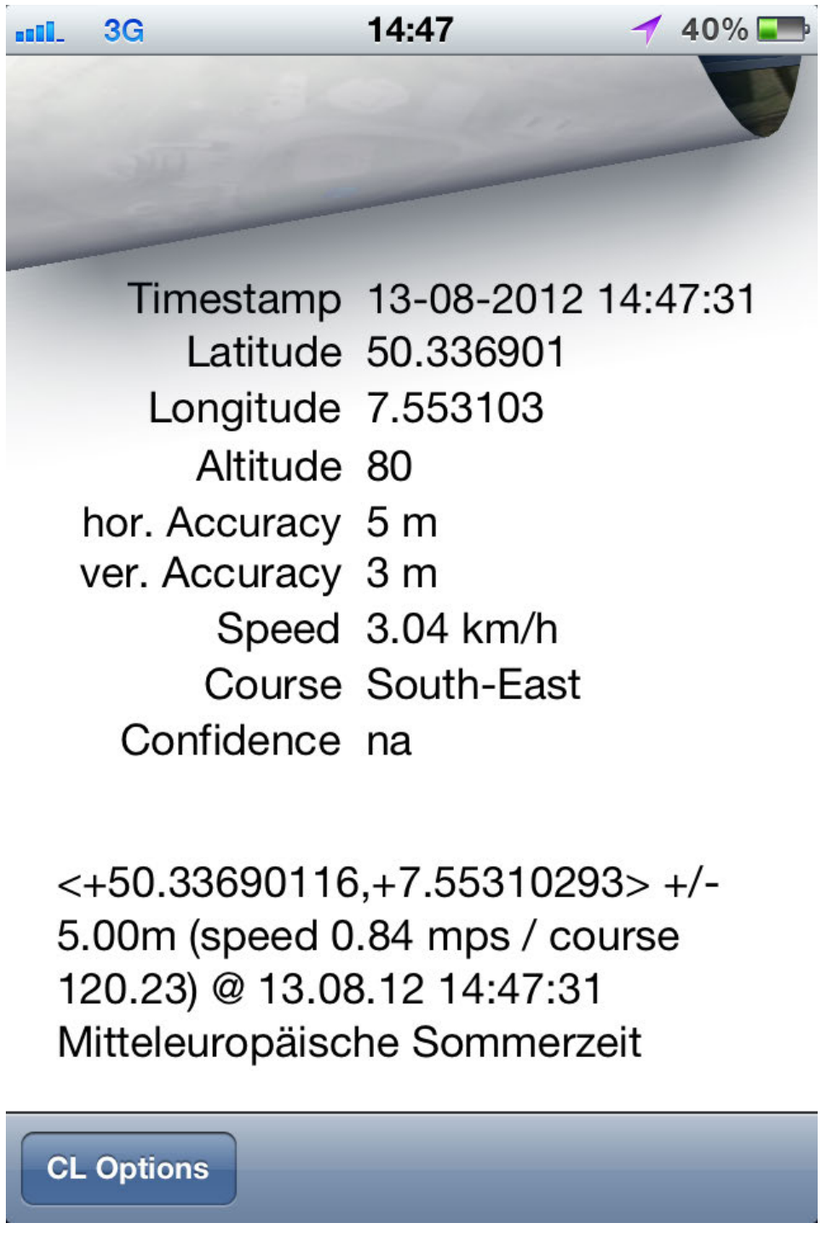
- iPhoneTrackerLE als iPhone-App
  - Erforschen verschiedener Einstellungsmöglichkeiten des CLFramework
  - Live-Betrachtung der Daten der cache_encryptedA.db sowie separate Protokollierung
  - Korrelation der protokollierten Daten in Bezug zu den Daten der cache-Datenbank
  - Evaluation der Genauigkeit der „GPS-Daten“
  - Wann werden welche Daten an Apple übermittelt
  - …

PG Technische Ermittlungsunterstützung

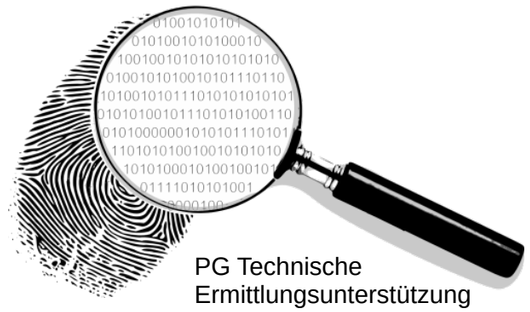
MapView (CoreLocationDaemon)



Kartenansicht

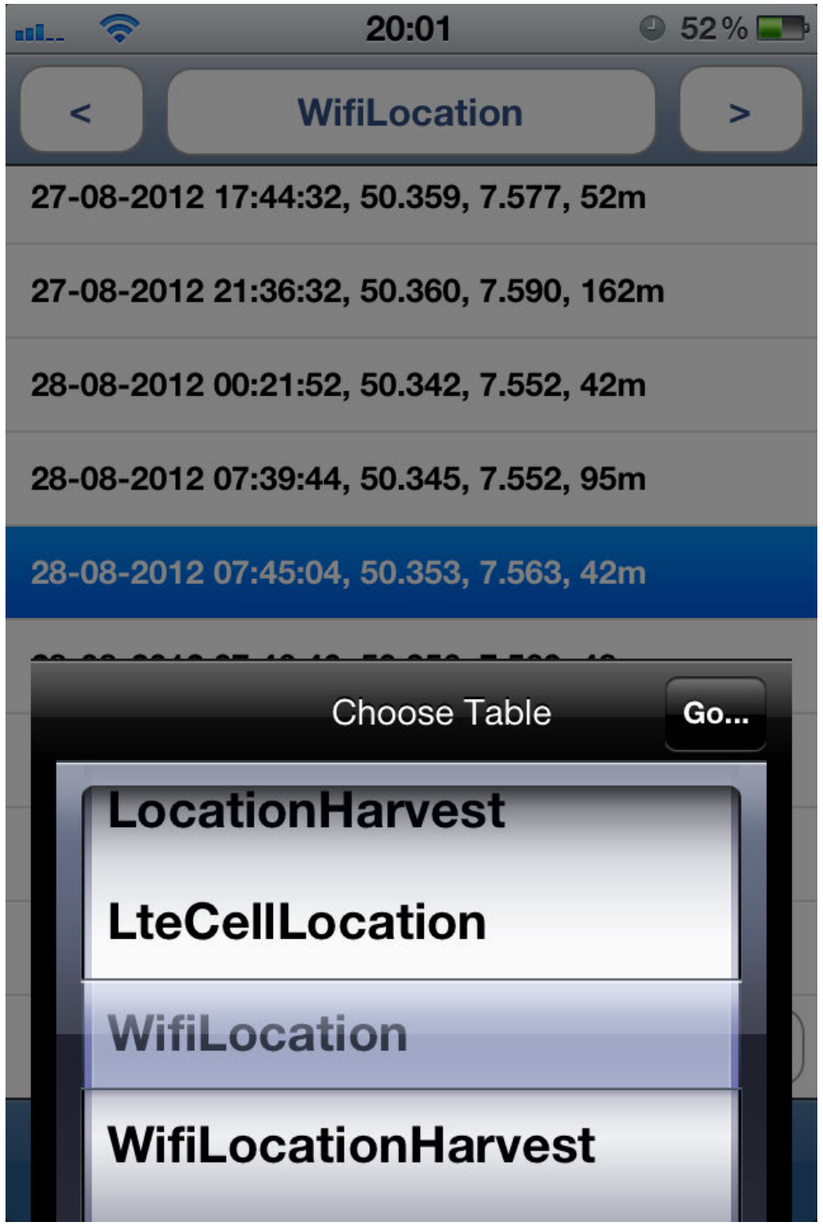


Detailansicht



PG Technische Ermittlungsunterstützung

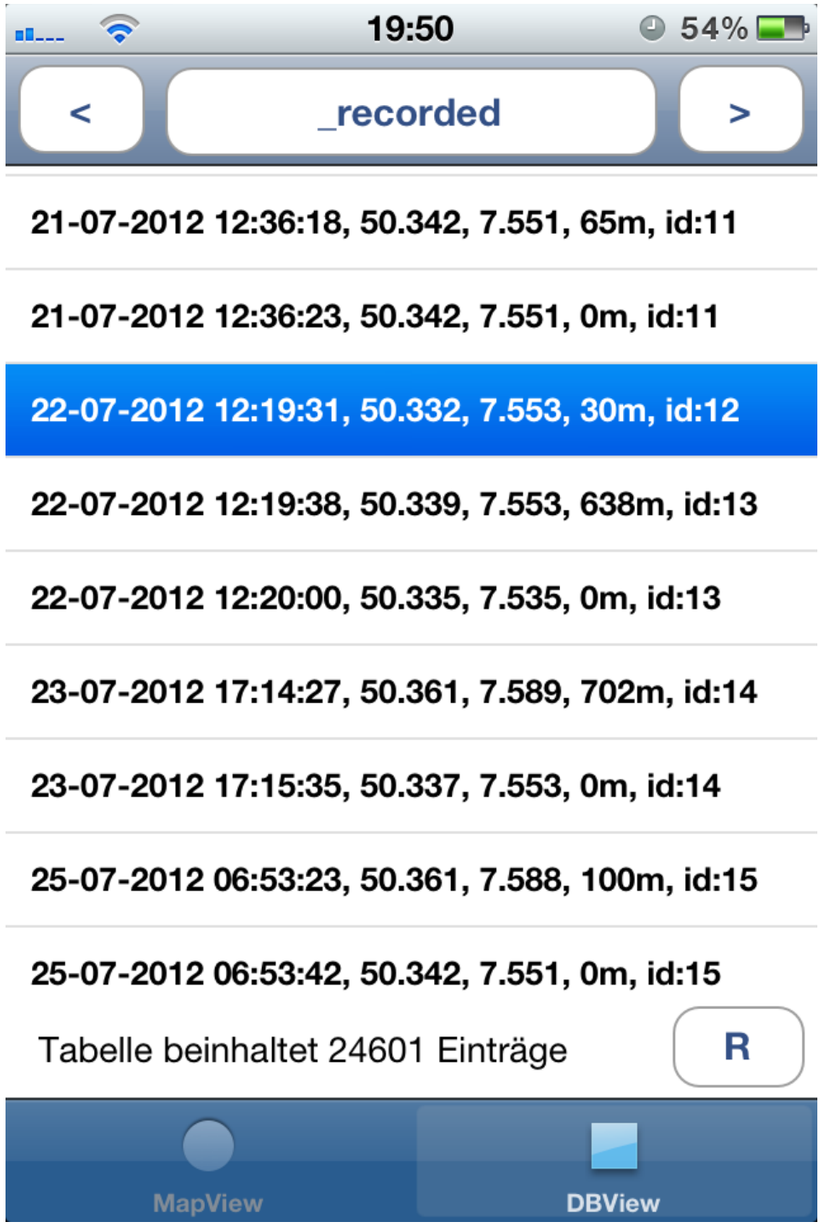
DBView (cache_encryptedA.db)



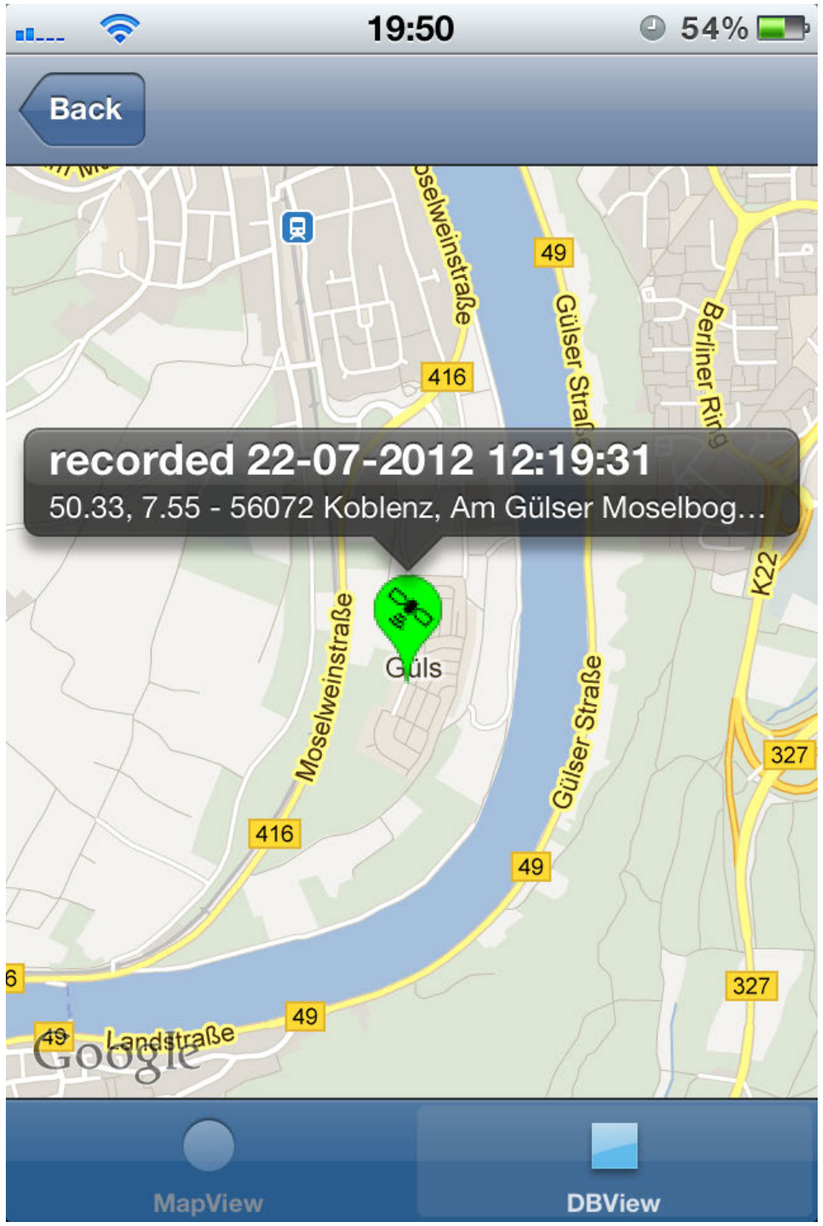
Tabellenansicht

Kartenansicht

Recorded Data (eigene Aufz.)



Tabellenansicht



Kartenansicht

PG Technische Ermittlungsunterstützung

Artikel zum Vortrag

http://articles.forensicfocus.com/2011/11/20/iphone-tracking-from-a-forensic-point-of-view/
http://articles.forensicfocus.com/2012/02/27/android-tracking-from-a-forensic-point-of-view/

Software zum Vortrag

http://it.dhein.com

PG Technische Ermittlungsunterstützung

Dipl.-Inform. Andreas Dhein
Moselring 10-12
56068 Koblenz
+49 261 103 2489

4rensics@gmx.de

andreas.dhein@polizei.rlp.de

adhein@uni-koblenz.de