Absicherung der analytischen Interpretation von Geolokalisierungsdaten in der Mobilfunkforensik

von

Andreas Dhein

Genehmigte Dissertation zur Erlangung des akademischen Grades eines
Doktors der Naturwissenschaften (Dr. rer. nat.)
Fachbereich 4: Informatik
Universität Koblenz-Landau

Vorsitzende des Promotionsausschusses:
Prof. Dr. habil. Maria A. Wimmer, Universtität Koblenz-Landau

Vorsitzender der Promotionskommission:
Prof. Dr.-Ing. Dietrich Paulus, Universtität Koblenz-Landau

Berichterstatter:
Prof. Dr. phil.-nat. Rüdiger Grimm, Universtität Koblenz-Landau
Prof. Dr.-Ing. Felix Freiling, Friedrich-Alexander Universität Erlangen-Nürnberg
Prof. Dr.-Ing. Utz Roedig, University College Cork

Datum der Einreichung: 04.07.2018
Datum der wissenschaftlichen Aussprache: 25.10.2019

Erklärung

Ich versichere, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

	Ja	Nein
Mit der Einstellung der Arbeit in die Bibliothek bin ich einverstanden.	☒	☐
Der Veröffentlichung der Arbeit im Internet stimme ich zu.	☒	☐

. . . . . .

(Ort, Datum) (Unterschrift)

Um manche Dinge zu verstehen, reicht es nicht aus, sich nur theoretisch mit ihnen zu beschäftigen. Erst durch praktische Erfahrungen und die Implementierung von Werkzeugen lassen sich bestimmte Zusammenhänge richtig begreifen.

Hierbei haben mich über die letzten Jahre hinweg einige, für mich sehr spezielle, Menschen unterstützt. Zunächst gilt mein Dank meinen Vorgesetzten, Kollegen sowie meinem Doktorvater. Ihrem Rückhalt, ihren Anregungen und einer Vielzahl an Diskussionen und Vorträgen habe ich es zu verdanken, dass sich diese Arbeit über die bloße Reflexion von Beweismitteln hinaus entwickeln konnte. Ebenso möchte ich den zahlreichen Lektoren und Kritikern meinen Dank aussprechen. Durch jeden einzelnen ist die Arbeit immer wieder ein Stück besser geworden.

Ebenso möchte ich meiner Familie, vor allem meiner Frau und meinen Kindern, danken. Der Weg hierhin war auch für Sie eine Herausforderung.

Ich widme diese Arbeit meiner Familie!

Zusammenfassung

Lokalisierungsdienste gehören mit zu den wesentlichen Merkmalen moderner mobiler Endgeräte. Neben der Tatsache, dass Standortdaten zur Rekonstruktion eines Bewegungsprofils genutzt werden können, steigt der Anteil der zu untersuchenden Geräten mit entsprechender Ausstattung im Rahmen von polizeilichen Ermittlungen enorm an.

Motivation

Ziel dieser Arbeit ist es, tiefergehendes Wissen um Geolokalisierungsfragen im Bereich der Mobilfunkforensik aufzubauen, um die in den Geräten gespeicherten Standortdaten forensisch auswertbar zu machen. Darüber hinaus sollen Werkzeuge entwickelt werden, die die spezifischen Bedürfnisse der Strafverfolgungsbehörden berücksichtigen.

Probleme

Die Prozesse der Geolokalisierung in Smartphones sind komplex. Um seine Position zu lokalisieren zu können, müssen verschiedene Referenzsysteme wie z. B. GPS, Funkzellen oder WLAN-hotspots in unterschiedlicher Art und Weise verknüpft werden. Der gesamte Lokalisierungsmechanismus ist geistiges Eigentum der Hersteller und nicht mit dem Ziel forensischer Auswertungen entstanden. Ein grundlegendes Problem der forensischen Untersuchung ist, dass hauptsächlich Referenzpunkte anstelle reeller Gerätepositionen gespeichert werden. Darüber hinaus bestehen die Geolokalisierungsinformationen aus Bits und Bytes bzw. numerischen Werten, die zuverlässig an ihre Bedeutung geknüpft werden

müssen. Die gewonnenen Lokalisierungsdaten sind ferner lückenhaft und stellen lediglich einen Teil des gesamten Prozesses bzw. der Gerätenutzung dar. Dieser Datenverlust muss bestimmt werden, um eine zuverlässige Aussage hinsichtlich der Vollständigkeit, Integrität und Genauigkeit der Daten zu ermöglichen. Zu guter Letzt muss, wie für jedes Beweismittel einer kriminalistischen Untersuchung, gesichert sein, dass eine Manipulation der Daten bzw. Fehler bei der Positionsschätzung des Gerätes keinen nachteiligen Einfluss auf die Auswertung haben.

Forschungsfragen

Im Zusammenhang mit Lokalisierungsdiensten in modernen Smartphones kommt es im forensischen Alltag immer wieder zu ähnlichen Fragestellungen:

1. Lassen sich Standorte zu jedem beliebigen Zeitpunkt ermitteln?
2. Wie genau sind die ermittelten Geodaten des Smartphones?
3. Werden Standortdaten aus Smartphones vor Gericht Bestand haben?

Forschungsansatz

Zur besseren Nachvollziehbarkeit der Prozesse in modernen Smartphones und um die Qualität und Zuverlässigkeit von Geolokalisierungsdaten zu bewerten, sollen Standortdaten verschiedener Plattformen sowohl theoretisch analysiert als auch praktisch während der Lokalisierung betrachtet werden. Der Zusammenhang zwischen Daten und Entstehungskontext wird mithilfe experimenteller Live-Untersuchungen sowie Desktop- und nativen Anwendungen auf den mobilen Endgeräten untersucht werden.

Ergebnis

Im Rahmen dieser Arbeit konnten mithilfe der entwickelten Werkzeuge die forensische Untersuchung verbessert sowie die analytische Interpretation von Geodaten von- bzw. direkt auf modernen Smartphones durchgeführt werden. Dabei hat sich ein generisches Modell zur Beurteilung der Qualität von Standortdaten herauskristallisiert, das sich allgemein auf die ermittelten Geodaten aus mobilen Endgeräten anwenden lässt.

Abstract

Location based services maybe are within one of the most outstanding features of modern mobile devices. Despite the fact, that cached geolocation data could be used to reconstruct motion profiles, the amount of devices capable to provide these information in the field of criminal investigations is growing.

Motivation

The aim of this work is to generate in-depth knowledge to questions concerning geolocation in the field of mobile forensics, making especially somehow cached geolocation data forensically valuable. On top, tools meeting the specific requirements of law enforcement personnel shall be developed.

Problems

Geolocation processes within smartphones are quite complex. For the device to locate its position, different reference systems like GPS, cell towers or WiFi hotspots are used in a variety of ways. The whole mobile geolocation mechanism is proprietary to the device manufacturer and not build with forensic needs in mind. One major problem regarding forensic investigations is, that mainly reference points are being extracted and processed instead of real life device location data. In addition, these geolocation information only consist of bits and bytes or numeric values that have to be securely assigned to their intended meaning. The location data recovered are full of gaps providing only a part of the process or device usage. This possible loss of data has to be determined deriving a reliable measurement for the completeness, integrity and accuracy of data. Last but not

least, as for every evidence within a criminal investigation, it has to be assured, that manipulations of the data or errors in position estimation have no disadvantageous effect on the analysis.

Research Questions

In the context of localisation services in modern smartphones, it always comes back to similar questions during forensic everyday life:

1. Can locations be determined at any time?
2. How accurate is the location of a smartphone?
3. Can location data from smartphones endure in court?

Approach

For a better understanding of geolocation processes in modern smartphones and to evaluate the quality and reliability of the geolocation artefacts, information from different platforms shall be theoretically analysed as well as observed in-place during the geolocation process. The connection between data points and localisation context will be examined in predefined live experiments as well as desktop- and native applications on smartphones.

Results

Within the scope of this thesis self developed tools have been used for forensic investigations as well as analytical interpretation of geodata from modern smartphones. Hereby a generic model for assessing the quality of location data has emerged, which can be generally applied to geodata from mobile devices.

Inhaltsverzeichnis

1 Einleitung **1**

1.1 Motivation 1

1.1.1 Ortungsdienste in Smartphones 2

1.1.2 Geolokalisierung als Systemdienst 4

1.1.3 Skandale um Ortungsdaten in der Presse 11

1.1.4 Standortdaten als forensisches Beweismittel 14

1.2 Probleme in der IT-Forensik 16

1.2.1 Veränderung der Beweismittellage 16

1.2.2 Datenextraktion von mobilen Endgeräten 18

1.2.3 Abweichungen von Ortungsdaten 22

1.2.4 Gezielte Manipulation von Standortdaten 24

1.3 Forschungsfragen 29

1.3.1 Completeness: Wie vollständig sind die Daten? 30

1.3.2 Integrity: Wie verlässlich sind die Daten? 31

1.3.3 Accuracy: Wie genau sind die Daten? 32

1.3.4 Existiert ein generisches Bewertungsmodell? 33

1.4 Eigener Ansatz und Struktur der Arbeit 34

2 Stand der Technik **36**

2.1 Verwandte Arbeiten 36

2.1.1 Andrew Hoog 36

2.1.2 Jonathan Zdziarski 37

2.1.3 Fachhochschule Aachen 38

2.1.4 Universität Erlangen 38

2.1.5 Eigene Veröffentlichungen 40

2.2 Softwaretechnische Umsetzungen 41

2.2.1 iPhoneTracker 41

2.2.2 MyPhoneTracker 43

2.2.3 Oxygen Forensic Suite 44

2.2.4 Micro Systemation XRY 45

2.2.5 Cellebrite UFED / Physical Analyzer 47

2.2.6 Öffentliche Funknetz-Datenbanken 51

2.3 Zusammenfassung 52

3 Forschungsmethodik **55**

3.1 Design Science Research Method 56

3.2 Problemidentifikation und Motivation 58

3.3 Mögliche Lösungsansätze 59

3.4 Design & Entwicklung 59

3.5 Demonstratoren 61

3.6 Evaluation 63

3.7 Kommunikation 64

4 Forensische Untersuchung von Standortdaten aus Smartphones 65

4.1 Apple iOS 66

4.1.1 Die Ortungsdatenbank 66

4.1.2 Ortungsdaten von Apple 76

4.1.3 Ortungsdaten für Apple 87

4.1.4 Zusammenfassung 106

4.2 Google Android 109

4.2.1 Die Ortungsdatendateien 110

4.2.2 Ortungsdaten von Google 114

4.2.3 Ortungsdaten für Google 119

4.2.4 Google Location History 125

4.2.5 Zusammenfassung 129

5 Absicherung der analytischen Interpretation durch native Apps 131

5.1 Eigenentwicklungen für iOS und Android 132

5.2 Einstellmöglichkeiten für Entwickler 136

5.3 Retrogrades Datentracking 139

5.4 Auswirkungen von LocationFaker-Apps 140

5.5 Zusammenfassung 141

5.5.1 Erkenntnisgewinn durch Live-Untersuchungen 141

5.5.2 Generisches Modell zur Beurteilung von Geodaten 143

5.5.3 Schwarmkartierung bei Apple 145

5.5.4 Forensische Standortermittlung bei Apple 148

5.5.5 Forensische Standortermittlung bei Google 149

6 Diskussion und Ausblick **150**

6.1 Beantwortung der Forschungsfragen 151

6.2 Vergleich der Eigenentwicklung mit kommerziellen Produkten . . 156

6.3 Absicherung der Erkenntnisse durch Apps 157

6.4 Bewertung der Ermittlungsmöglichkeiten 158

6.5 Ausblick 159

Anhang **167**

Literaturverzeichnis 167

Internetquellen 171

Abbildungsverzeichnis 183

Tabellenverzeichnis 187

Terminalausgaben 188

Abkürzungsverzeichnis 189

Begriffserläuterungen 190

Teil 1

Einleitung

1.1 Motivation

Zur forensischen Aufklärung kriminalpolizeilicher Vorgänge sind Informationen zu Aufenthaltsorten verdächtiger Personen zu bestimmten Zeitpunkten häufig unabdingbar. Standortdaten aus elektronischen Geräten, wie z. B. Smartphones, könnten hierfür wichtige Hinweise liefern, sofern der Betroffene das Gerät zum Tatzeitpunkt bei sich getragen hat. In der forensischen Praxis hingegen wird die Beweiskraft von Ortungsdaten mobiler Endgeräte aufgrund möglicher Fehler bei der Verortung regelmäßig angezweifelt.

Mithilfe dieser Arbeit soll durch die Absicherung der analytischen Interpretation von Geolokalisierungsdaten in der Mobilfunkforensik für mehr Klarheit bei der Auswertung von Standortdaten gesorgt werden.

Potentiell sind in aktuellen Computersystemen Unmengen an Standortinformationen gespeichert. Insbesondere Smartphones mit Assistenzfunktionen sammeln und werten permanent Informationen über die Umgebung des Gerätes aus. Hierdurch hinterlassen diese elektronischen Assistenten, oftmals ohne aktive Nutzung durch den Anwender, digitale Spuren, die sich für kriminalpolizeiliche Ermittlungen nutzbar machen lassen. Die Sicherung und Bereitstellung solcher Beweise aus digitalen Geräten fällt der Mobilfunkforensik als Teilgebiet der IT-Forensik innerhalb des Aufgabenbereiches der kriminaltechnischen Untersuchung zu.

Ließen sich Standortdaten aus Smartphones in Strafverfahren als verlässliches Beweismittel zur Beantwortung kriminalpolizeilicher Fragestellungen einbringen, fiele der Mobilfunkforensik nicht mehr nur in den für sie typischen Deliktsbereichen der IT-Forensik, wie Computerbetrug, Datenveränderung oder Hacking, sondern auch in der allgemeinen Kriminalitätsaufklärung eine feste Rolle zur.

Zur Feststellung der Gerichtsverwertbarkeit gilt es, die Qualität von Geodaten aus mobilen Endgeräten zu bewerten und anschaulich darzustellen. Hierzu muss zusätzlich zur forensischen Analyse der extrahierten Ortungsinformationen die Entstehung der Daten während der Verortung des mobilen Endgerätes wissenschaftlich untersucht werden. Im Rahmen dieser Arbeit soll darüber hinaus mithilfe eines induktiven Ansatzes und Untersuchungen an aktuellen Smartphones ein allgemein gültiges Modell zur Qualitätsbewertung von Ortungsdaten abgeleitet werden. Für die Praxis entstehen so zusätzliche Werkzeuge, die Standortdaten aus mobilen Endgeräten für die Mobilfunkforensik nutzbar machen und die Entstehung von Ortungsdaten auf mobilen Endgeräten veranschaulichen.

1.1.1 Ortungsdienste in Smartphones

Um verständlich zu machen, warum auf mobilen Endgeräten Standortdaten in großer Zahl zu finden sind und wodurch sie entstehen, werden im Folgenden einige typische Nutzungsszenarien aufgezeigt.

Um die bestmögliche Funktionalität zu entfalten, erheben Assistenzsysteme in Smartphones regelmäßig ortsbezogene Informationen ihrer Umgebung. Hierzu zählen exemplarisch der nächstgelegene Parkplatz, das beste Restaurant oder die günstigste Tankstelle in der Umgebung. Damit aber nicht genug. Durch die Verknüpfung des Aufenthaltsortes mit Ereignissen im Kalender oder typischen Verhaltensweisen des Nutzers (z. B. die Fahrt zur Arbeitsstätte) gewinnen die elektronischen Helfer immer mehr an Bedeutung. So erhält der Nutzer z. B. direkt nach dem Aufstehen einen Hinweis, wie lange die Fahrt zur Arbeit unter den aktuellen verkehrstechnischen Bedingungen voraussichtlich dauern wird. Bei Termineinträgen mit zusätzlicher Ortsangabe werden ebenfalls rechtzeitig Hinweise angezeigt, die sowohl die reine Fahrzeit als auch die zu erwartende Verkehrssituation berücksichtigen.

Ein weiteres Beispiel für die Verwendung von Ortungsdiensten sind Kartenanwendungen. Aufgrund kontraststarker und hochauflösender Farbdisplays, die Informationen auch bei ungünstigen Lichtverhältnissen gut erkennen lassen, konnten sich Kartenanwendungen bereits sehr früh etablieren. Insbesondere, da jeder Gerätehersteller zusammen mit dem mobilen Betriebssystem auch eine proprietäre Kartensoftware ausliefert. Zusätzlich zur Kartenansicht mit Anzeige des eigenen Standortes ist die Nutzung des Smartphones als Navigationsgerät dank schneller Internetverbindungen und Datenflatrates sowie der Lokalisierung im Meterbereich mittlerweile zum Standard geworden. Durch Optimierungen beim Energieverbrauch lassen sich auch längere Routen heutzutage problemlos ohne externe Stromversorgung bewältigen. Dazu mehr in Abschnitt 1.1.2 auf Seite 8.

Darüber hinaus werden die Möglichkeiten zur Verortung mobiler Endgeräte für die Anzeige von ortsbezogenen Werbeeinblendungen ebenso eingesetzt wie zur Standortbestimmung innerhalb von augmented-reality Spielen, wie z. B. PokémonGo. Die aktuelle Position kann mit anderen geteilt, über Messenger verschickt oder innerhalb von Social-Media-Anwendungen mit den sogenannten Posts verknüpft werden. Suchergebnisse im Webbrowser oder Shopping-Apps können abhängig von der Geräteposition sortiert bzw. gefiltert werden. Es gibt noch unzählige weitere Beispiele für die Nutzungsmöglichkeiten der Ortungsdienste in Smartphones. Viel interessanter ist jedoch, dass sich bei der forensischen Untersuchung solcher Apps eine Menge gespeicherter Standortdaten feststellen lassen.

Verortung von Mediendateien

Am Beispiel von Metadaten in Bildern wird ebenfalls deutlich wie wertvoll die forensische Untersuchung der Exchangeable Image File Format (Exif)-Daten für die kriminaltechnische Betrachtung ist. Die Auswertung von Aufnahmedatum und Kameramodell von Bildaufnahmen ist gängige Praxis in der IT-Forensik. Hierbei lassen sich Bilder sowohl chronologisch in eine Reihenfolge bringen, als auch bestimmten Aufnahmegeräten zuordnen.

Mithilfe von Standortdaten ist es dann zusätzlich möglich den Zusammenhang zwischen Bildinhalt, Aufnahmedatum, dem Photographen (über die Gerätebezeichnung) und dem Aufnahmeort noch konkreter darzustellen.

Allerdings gelten Ortsinformationen aus Exif-Daten als nicht sehr verlässlich. Zum einen, weil in der Vergangenheit bisweilen Abweichungen von mehreren hundert Metern zum realen Aufnahmeort aufgezeigt werden konnten (vgl. Abschnitt 1.2.3 auf Seite 22). Aber vor allem, da die Informationen mithilfe von Computerprogrammen manipulierbar sind. Die detaillierte Diskussion zu Möglichkeiten der gezielten Manipulation bzw. Simulation von Geodaten sowie weitere, kritisch zu betrachtende elektronische Beweismittel im Zusammenhang mit Adressdaten aus Smartphones wird in Abschnitt 1.2.4 auf Seite 24 weitergeführt. Neben der Darstellung der technischen Möglichkeiten zur Manipulation soll der Leser zudem dafür sensibilisiert werden elektronische Beweismittel grundsätzlich zu hinterfragen.

1.1.2 Geolokalisierung als Systemdienst

Um die Geräteposition möglichst energiesparend zu ermitteln und anschließend allen Anwendungen gleichzeitig zur Verfügung zu stellen, verwenden die Geräte einen zentralen Systemdienst. Die Betrachtung dieser sog. Ortungsdienste ist notwendig zum Verständnis der Entstehung von Ortungsdaten. Mithilfe dieses Wissens lassen sich Unregelmäßigkeiten bzw. Abweichungen von gespeicherten Standortdaten erklären und bewerten. Hierzu werden im Folgenden Aspekte der als assisted Global Positioning System (aGPS) bekannten Technik beschrieben. Der Fokus liegt zunächst noch auf den Erwartungen der Anwender, den technischen Herausforderungen für die Hersteller sowie der Umsetzung im Detail und nicht der Bedeutung für die Forensik. AGPS ist seit Jahrzehnten verfügbar, wurde aber erst mit Einführung von Smartphones in den letzten Jahren populär.

Erwartungen des Benutzers

Für die Nutzer mobiler Endgeräte dürfte von besonderer Bedeutung sein, die Geräteposition möglichst direkt und so präzise wie möglich an jedem beliebigen Ort der Welt zu erhalten. Nach persönlicher Einschätzung sollte die Ermittlung der eigenen Position dabei möglichst effizient, d.h. schnell und energiesparend ablaufen.

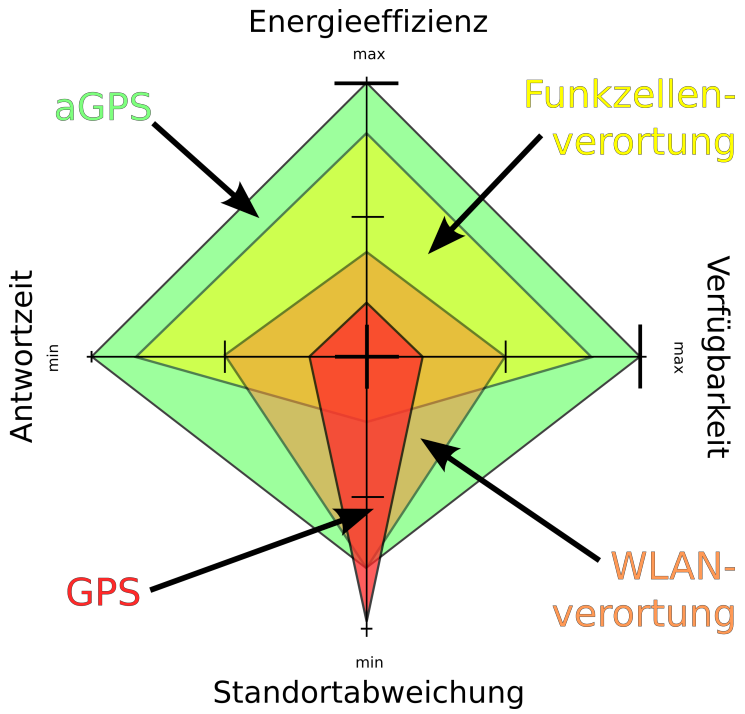


Abb. 1.1: Vergleich der Verortungsmethoden GPS, WLAN-verortung, Funkzellenverortung und aGPS hinsichtlich der Dimensionen Standortabweichung, Antwortzeit, Energieeffizienz sowie Verfügbarkeit. Weitere Details im Text. Quelle: Eigene Darstellung.

Die Dimensionen für verschiedene Ortungstechniken bei der Smartphonelokalisierung können sehr anschaulich mithilfe eines Kiviat-Graphen verglichen werden (siehe Abb. 1.1). Die optimalen Faktoren zur Verbesserung des Nutzerempfindens bei der Standortbestimmung auf einem aktuellen Smartphone werden hierbei definiert durch eine möglichst:

- minimale Antwortzeit,
- maximale Verfügbarkeit,
- maximale Energieeffizienz sowie
- minimale Standortabweichung.

Wie in Abb. 1.1 dargestellt, liegt das Ziel von aGPS primär in der Beseitigung der Unzulänglichkeiten des Global Positioning System (GPS) (rötliche Einfärbung). Für ein ideales Nutzererleben gilt es, eine möglichst maximale Ausdehnung aller Dimensionen herzustellen.

In der Praxis wird ein Maximum aller vier Dimensionen nicht erreicht werden können. A-GPS (grün eingefärbte Fläche in Abb. 1.1 auf der vorherigen Seite) deckt die Parameter Effizienz, Antwortzeit sowie Verfügbarkeit im Ideal und die Standortabweichung zumindest annähernd ideal ab. Gegenüber dem GPS-Verfahren muss hierfür, zumindest initial bei der Verortung, eine höhere Standortabweichung in Kauf genommen werden.

Bei aGPS werden Verortungstechniken verschiedener Funkempfänger kombiniert und i. d. R. hintereinander ausgeführt. So lässt sich z.B. die erste, noch grobe Lokalisierung über Funkzellen sehr schnell erreichen (in Abb. 1.1 auf der vorherigen Seite gelblich dargestellt). Eine genauere Bestimmung der Geräteposition (z. B. über WLAN-Sender in der Umgebung, in Abb. 1.1 auf der vorherigen Seite orangefarben gezeichnet) benötigt nur unwesentlich mehr Zeit. Die präzise Standortbestimmung über GPS dauert potentiell am längsten, wenn überhaupt verfügbar. Durch die Kombination von Lokalisierungstechniken beim aGPS lassen sich die für den Nutzer maßgeblichen Faktoren Antwortzeit und Standortabweichung minimieren. Durch die Speicherung der letzten bekannten Position lässt sich das Verfahren zusätzlich beschleunigen.

Für die Mobilfunkforensik ergibt sich hieraus, dass die Standortabweichung der jeweils verwendeten Verortungsmöglichkeit für jeden Einzelfall zu betrachten ist. Ziel dieser Arbeit ist es, eine Generalisierung und Qualitätsbewertung von Standortdaten unabhängig von Herstellern, Geräten etc. zu ermöglichen (vgl. Abb. 5.13 auf Seite 143 in Abschnitt 5.5.2 auf Seite 143).

Zusammenfassend erwartet der Benutzer eines mobilen Endgerätes heutzutage, dass möglichst alle zuvor genannten Faktoren der Standortlokalisierung optimal umgesetzt sind. Die Reaktionszeiten sollen sich im Sekundenbereich bewegen, die Verfügbarkeit muss auch an Orten ohne GPS-Signal gewährleistet sein, und darüber hinaus soll die Akkuleistung den ganzen Tag überdauern. Wird umgekehrt die Geräteposition nicht ausreichend schnell und genau ermittelt, läuft der Hersteller Gefahr, dass der Anwender den Ortungsdienst deaktiviert und keine Standortdaten mehr ermittelt werden können. Hiervon ist dann nicht nur der kriminalpolizeiliche Ermittler betroffen. Vielmehr wirkt sich die Deaktivierung der Ortungsdienste negativ auf die Möglichkeit der Hersteller aus, diese Dienste überhaupt anzubieten. Mehr dazu in Abschnitt 5.5.3 auf Seite 145.

Technische Herausforderungen

Hinsichtlich der bestmöglichen Genauigkeit ist die Positionsbestimmung über GPS zu bevorzugen. Allerdings ergeben sich auch einige Nachteile.

So steigt z. B. der Energieverbrauch des Smartphones durch die Nutzung des GPS-Sensors um ca. 500mW an (vgl. [na13]). In der Praxis führte dieser Wert in der Anfangszeit der mobilen Ortung ohne zusätzliche Optimierungen zu einer prozentualen Abnahme der Batterieladung um beinahe ein Prozent pro Minute aufgrund der dauerhaften Verwendung des GPS-Sensors. Der Energiebedarf der Drahtlosempfänger für Mobilfunk oder Wireless Local Area Network (WLAN) ist mit ca. 500-1200mW (vgl. [na13]) zwar nicht niedriger, allerdings sind die Empfänger bzw. Schnittstellen ohnehin fast permanent in Benutzung. Das Mobilfunkmodem muss z. B. ständig aktiv sein, um Anrufe entgegen zu nehmen bzw. den Wechsel zu anderen Funkzellen durchzuführen. Die WLAN-Schnittstelle dürfte ebenfalls dauerhaft in Betrieb sein, um die Vorteile des schnelleren und günstigeren Internetzugangs via WLAN auszunutzen.

Ein weiterer Nachteil beim Einsatz von GPS zur Standortbestimmung liegt in der Reaktionszeit des Systems. Für die Berechnung der Geräteposition müssen die Positionen aller Satelliten im Orbit, die sogenannten Ephemeriden, vorab bekannt sein. Werden diese Informationen ausschließlich aus dem GPS-Signal ermittelt, kann die Standortbestimmung bis zu 12,5 Minuten betragen (vgl. [Zog11]). Selbst wenn der sogenannte Almanach (Laufbahninformationen aller Satelliten) über das Internet abgerufen wird, liegen die Zeiten bis zur Positionsermittlung häufig oberhalb der erwartbaren Antwortzeiten von wenigen Sekunden.

Die Lokalisierung mittels GPS ist zudem nicht überall möglich. Voraussetzung für die Standortbestimmung auf Basis von GPS ist eine freie Sicht auf mindestens vier GPS-Satelliten. So verwundert es auch nicht weiter, dass in Gebieten mit steilen Schluchten oder in Stadtzentren mit einer Vielzahl an Hochhäusern (bei [Gor11] auch »urban canyons« genannt) die Standortbestimmung gestört wird. Innerhalb geschlossener bzw. abgeschirmter Räume sind GPS-Signale mitunter gar nicht erst zu empfangen. Insbesondere hier versprechen die Hersteller über alternative Stützsysteme wie Mobilfunksender oder WLAN-Access-Points Abhilfe. Was die bessere Verfügbarkeit von Mobilfunk sowie WLAN gegenüber GPS angeht, so steht dies in urbanen Gebieten außer Frage.

Funksender in der unmittelbaren Umgebung des Gerätes als Stützsysteme für die Lokalisierung einzusetzen ist allerdings ebenfalls problematisch.

Zunächst verfügen sowohl Mobilfunk- als auch WLAN-Sender gemeinhin nicht über Informationen zum eigenen Standort. Darüber hinaus ist die Übertragung von Geodaten kein direkter Bestandteil der gängigen Übertragungsprotokolle (vgl. [nay14]). Zusätzlich kann sich die Position oder Verfügbarkeit der Funksender im Laufe der Zeit verändern. Insbesondere die geringe Größe von WLAN-Routern machen den Transport einfach. Zuweilen werden die Geräte zur Optimierung der Funkabdeckung neu positioniert, tageszeitabhängig oder bei längeren Abwesenheiten abgeschaltet oder bei einem Umzug mitgenommen. Neben stationären AccessPoints sind auch Smartphones in der Lage WLAN-Hotspots für andere Geräte zur Verfügung zu stellen. Und mobile Endgeräte sind schon von ihrem Verwendungszweck nicht ortsgebunden.

Aber auch Mobilfunkmasten können unter bestimmten Umständen an unterschiedlichen Standorten auftauchen. Hierbei wechselt allerdings nicht der Sender selbst die Position, sondern es ändert sich lediglich die Kennung des Senders, die sogenannte FunkzellenID. Durch die Verwendung der CellID für die Lokalisierung scheint es dann, dass der Sender seine Position verändert hat. Auf die forensischen Implikationen dieser Problematik wird später in Abschnitt 5.5.3 auf Seite 147 noch detailliert eingegangen.

Lösungen der Hersteller

Um aGPS oder Standortdaten aus Smartphones zu verstehen ist es notwendig, sich mit den technischen Umsetzungen der Hersteller zu den oben beschriebenen technischen Schwierigkeiten auseinanderzusetzen.

Die technischen Probleme bei der Verortung über GPS lassen sich hinsichtlich der Reaktionszeit verbessern, indem die Positionsdaten der orbitalen Satelliten über das Internet heruntergeladen werden. Bei den aktuellen Übertragungsraten sind die hierzu benötigten maximal 100kb (vgl. [Zog11]) in wenigen Sekunden übertragen. Um den Energieverbrauch zu senken setzen Smartphonehersteller auf moderne Sensoren zur Reduktion der Leistungsaufnahme. Darüber hinaus deaktivieren adaptive Algorithmen den GPS-Sensor je nach Aktivität des Gerätenutzers so häufig wie möglich.

Damit aGPS in aktuellen Smartphones funktionieren kann, müssen die Bezeichner und Standorte möglichst vieler Sendestationen bekannt sein. Zum Glück versenden Mobilfunksender und WLAN-AccessPoints permanent technische Informationen. Konkret übertragen Mobilfunkstationen die sogenannten Paging-Informationen und WLAN-Access-Points Beacons mit der BSSID (Geräte-Adresse) und falls nicht unterdrückt SSID (Netzwerkbezeichner) (vgl. [Komb], [Koma]). Diese Daten dienen zwar primär dem Verbindungsaufbau mit mobilen Endgeräten, können aber auch rein passiv mitgelesen werden. Eine tatsächliche Verbindung mit einem der Netze ist für die Aufzeichnung dieser Informationen nicht notwendig.

Das zu lösende Problem für die Gerätehersteller besteht darin zu den technischen Informationen der Sender die jeweiligen Standorte zu ermitteln. Hierzu bauen Apple (vgl. [App11] Absatz 4) und andere Hersteller, wie Google oder Microsoft (vgl. [Goo17a], [Mic17]), sog. crowd-sourced Datenbanken auf, welche die erhobenen Informationen zu Funksendern in der Umgebung mit aktuellen Positionsdaten der Geräte anreichern. Die Daten werden schlussendlich von den Herstellern dazu genutzt, die Standorte der Funksender zu errechnen. Wie dieses Verfahren im Detail abläuft wird später in Abschnitt 5.5.3 auf Seite 145 für Apple genauer beschrieben. Mithilfe der Standortdaten aus diesen Datenbanken ist es dann umgekehrt auch an Orten ohne GPS-Empfang und obendrein wesentlich schneller möglich, auf Basis der Identifikationsmerkmale von Sendern (CellID, Media-Access-Control (MAC)-Adresse oder SSID) den Standort des Funksenders abzufragen und die Positionsbestimmung des Gerätes durchzuführen. Abb. 1.2 auf der nächsten Seite zeigt, wie die Geräteposition über aktive Mobilfunksender in der Umgebung bestimmt werden kann. Die so durchgeführte Initialverortung kann hierbei sehr schnell erfolgen, da für die Teilnahme am Mobilfunknetz mindestens die Verbindung zu einer Funkzelle gegeben sein muss. Sind die Informationen von drei oder mehr Funksendern (in Abb. 1.2 auf der nächsten Seite grün eingefärbt) verfügbar, lässt sich die Position des mobilen Endgerätes recht präzise bestimmen. In zahlreichen Live-Untersuchungen (siehe Abschnitt 5.1 auf Seite 132) wurden Standortabweichungen von unter 1km (selbst in ländlichen Regionen Deutschlands) festgestellt.

Nach der initialen Positionsbestimmung lässt sich der Gerätestandort durch die Einbeziehung weiterer Funksender (insbesondere solche mit geringerer Sende-

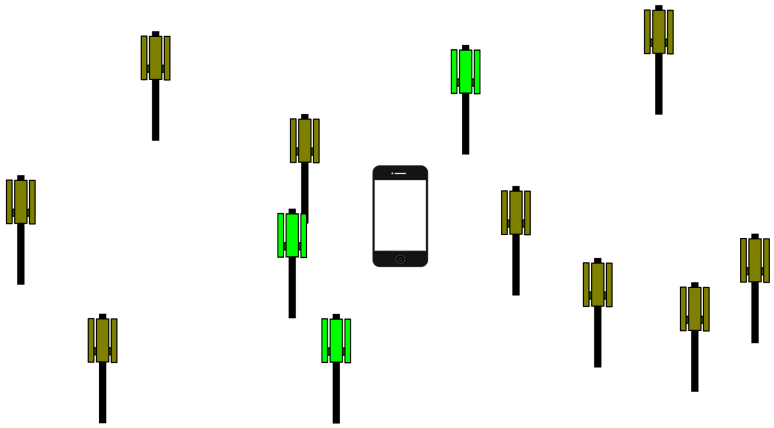


Abb. 1.2: Verortung eines Smartphones auf Basis der von Apple übertragenen Mobilfunksendern in der Umgebung. Exemplarisch sind die zur Verortung genutzten Sender grün markiert. Quelle: Eigene Darstellung.

leistung wie z. B. WLAN) beliebig verfeinern. Die Hersteller sind aktuell in der Lage, unter Einbeziehung weiterer Funktechnologien wie z. B. Near Field Communication, deu: Nahbereichskommunikation (NFC) (Bluetooth, RFID, etc.) und durch Priorisierung der Datenquellen hinsichtlich bestimmter Qualitätsmerkmale, die Position des Gerätes so präzise zu bestimmen wie dies mithilfe von GPS unter idealen Bedingungen möglich gewesen wäre. Wie genau die Verortung auf Basis von aGPS bei Apple bzw. für Google funktioniert wird ebenfalls später in Abschnitt 4.1.3 auf Seite 87 bzw. Abschnitt 5.5.3 auf Seite 145 für Apple und in Abschnitt 4.2.3 auf Seite 119 für Google ausgeführt. Die Methodik zur Positionsberechnung (Lateration, Angulation etc.) sowie die Vorgehensweise der Hersteller zur Standortbestimmung auf Basis von Umgebungsinformationen ist nicht öffentlich zugänglich dokumentiert. Fest steht allerdings, dass durch die Verwendung mehrerer Funksender eine Verfeinerung der Positionsschätzung von wenigen Kilometern, im Idealfall hin zu wenigen Metern möglich ist (vgl. Abschnitt 5.5.2 auf Seite 143).

Spuren dieser Datenbanken (Apple) bzw. Dateien (Android) lassen sich mitunter auch auf den Smartphones finden. Die ausführliche Diskussion dieser Spuren bei Apple wird in Abschnitt 4.1 auf Seite 66 geführt, für Google erfolgt die Darstellung in Abschnitt 4.2 auf Seite 109.

1.1.3 Skandale um Ortungsdaten in der Presse

Überwachungsvorwürfe und der Datenschutz sind attraktive Themen für die Medien. Das Interesse steigt dabei um so mehr, wenn sich die Vorwürfe gegen Global Player richten. Um die Aufmerksamkeit der Leser zu steigern, hängen die Ersteller von Skandalbeiträgen im Zusammenhang mit Apple in Anlehnung an die amerikanische Watergate-Affäre von 1974 ihren Überschriften sehr gerne das Suffix -gate an. So werden auch die mittlerweile 11 skandalträchtigsten Probleme von Apple mit dem medienwirksamen Postfix versehen.

Die bekanntesten Beispiele aus der Geschichte von Apple sind: Antennagate [App10], Bendgate und eben die Affäre um die Speicherung von Ortungsdaten auf Apple Geräten, in den Medien als Locationgate [App11] bezeichnet.

Locationgate

Mithilfe der Neuen Medien verbreitet sich die Nachricht zum Locationgate von Apple sehr schnell. Am 20.04.2011 veröffentlichen die Briten Alasdair Allen und Pete Warden einen Artikel im Technologieradar des O'Reilly Verlages [AW11] und bereits am nächsten Tag entsteht ein globaler Hype um die Erkenntnisse der beiden Engländer (vgl. [Sch11], [AVD11]).

Bei Untersuchungen zur Speicherung von Geoinformationen in Smartphones sind die beiden Wissenschaftler auf eine Datenbank mit Unmengen gespeicherter Geokoordinaten bei Apple gestoßen. Der Vorwurf des vermeintlich bewussten Überwachens, das Aufzeichnen und Übersenden von Aufenthaltsorten der iPhone-Besitzer durch Apple (tracking) war vielleicht nicht das Ziel der Untersuchungen, aber das Ergebnis der Veröffentlichung.

iPhoneTracker

Die zusätzlich zur Veröffentlichung entwickelte Software zur Visualisierung der von iTunes synchronisierten Geodaten trägt den skandalträchtigen Namen iPhoneTracker und kann bei github auch heute noch heruntergeladen werden (Download über [War11]).

In der Hauptsache projiziert die Software, wie in 1.3 dargestellt, Standortdaten auf Kartenmaterial von OpenStreetMaps. Darüber hinaus kann der Anwender mithilfe eines Zeitstrahls die Visualisierung auf einzelne Datensätze zu einem bestimmten Zeitpunkt einschränken. Erste eigene Erkenntnisse zum iPhoneTracker ergaben sehr schnell, dass die Software nicht für forensische Zwecke eingesetzt werden sollte (hierzu später in Abschnitt 2.2.1 auf Seite 41 mehr).

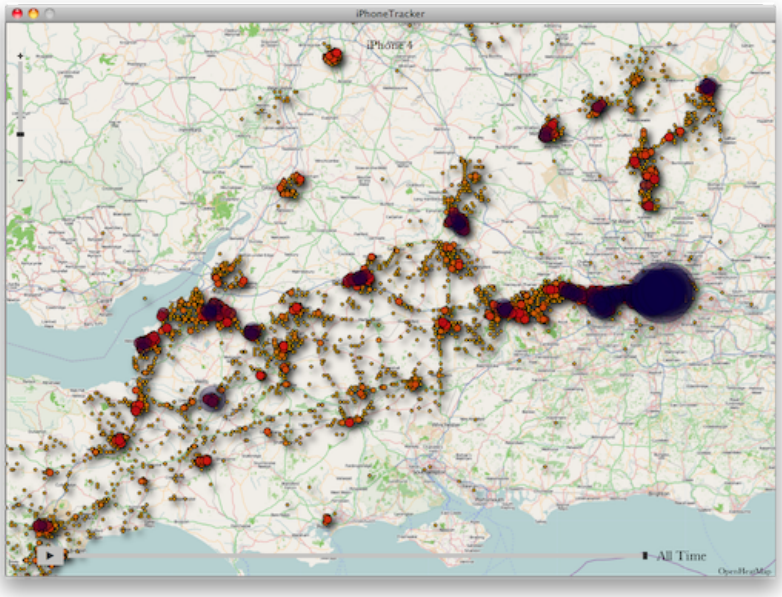


Abb. 1.3: Screenshot der Anwendung iPhoneTracker - Standortdaten eines iPhone4 mit Geodaten einer Reise durch Südengland. Quelle: [War11]. Kartenmaterial: © OpenStreetMap Mitwirkende 2011.

Programmiert wurde die Software iPhoneTracker von Pete Warden, populär in den Medien platziert, dann später von Alasdair Allan. An die Diskussion im Technik-Blog des O'Reilly Verlages [AW11] schließen sich mehrere TV-Interviews sowie Fernsehbeiträge diverser Berichterstatter an. Bald beherrscht das Thema sämtliche Medienkanäle. Zusätzlich entstehen diverse Deutungsversuche mit teilweise abstrusen Unterstellungen gegenüber Apple.

Allerdings waren Warden und Allen nicht die Ersten, die nachgewiesen haben, dass Apple-Geräte Positionsdaten ihrer Benutzer speicherten. So berichtete am 15.09.2010 bereits der Franzose Paul Courbis in seinem Internet-Blog detailliert über die »Indiskretion des iPhones« (vgl. [Cou10]).

Apples Stellungnahme

Apple weist den Vorwurf der Überwachung in einer öffentlichen Stellungnahme entschieden zurück (vgl. [App11]). Z. B. heißt es in der Antwort auf die Frage nach dem »Warum überwacht Apple die Position meines iPhones«: »Apple is not tracking the location of your iPhone. Apple has never done so and has no plans to ever do so.« [App11].

Im Weiteren beschreibt Apple die Technik hinter aGPS. Bezüglich der Verortung und dem technischen Vorgang beim Sammeln der Daten wird in Abschnitt 3 ausgeführt, dass »These calculations are performed live on the iPhone using a crowd-sourced database of Wi-Fi hotspot and cell tower data that is generated by tens of millions of iPhones sending the geo tagged locations of nearby Wi-Fi hotspots and cell towers in an anonymous and encrypted form to Apple«. Bezüglich des Umfangs der bei Apple gespeicherten Daten wird lediglich angegeben, dass die gesamte Lokalisierungsdatenbank viel zu groß sei, um sie komplett auf dem Gerät zu speichern.

Zur Frage, warum die Daten auf dem Computersystem des Anwenders gespeichert würden, wird keine Angabe gemacht. Es erfolgt lediglich der Hinweis, dass die Datenbank mit Ortungsdaten in Zukunft (mit Einführung von iOS5) verschlüsselt gespeichert werden wird. Hinsichtlich der Daten von mehr als einem Jahr in der Vergangenheit erklärte Apple, dass es sich hierbei um einen Softwarefehler handele, der in kommenden Versionen behoben werden wird. »The reason the iPhone stores so much data is a bug we uncovered and plan to fix shortly (see Software Update section below). We don't think the iPhone needs to store more than seven days of this data.«. Die Speichergrenze soll demnach zukünftig bei sieben Tagen liegen.

Zusammenfassend lässt sich festhalten, dass Apple offensichtlich ungern mit Überwachungsvorwürfen in Verbindung gebracht wird. Die Medienberichte führten dazu, dass der Speicherumfang der Daten auf den Geräten reduziert wurde. Ebenso werden die Daten nicht mehr über iTunes synchronisiert. Inwiefern und unter welchen Umständen Datenbestände der Ortungsdienste für forensische Untersuchungen auch heute noch herangezogen werden können, wird später in Abschnitt 4.1 auf Seite 66 und Abschnitt 4.2 auf Seite 109 weiter betrachtet.

Google Streetview

Aber nicht nur Apple geriet wegen Überwachungsvorwürfen um Standortdaten in die Schlagzeilen. Ein Jahr zuvor (Mai 2010) sorgte Google für Aufregung um die Verletzung der Privatsphäre von WLAN-Betreibern durch das vermeintlich heimliche Aufzeichnen des Funkverkehrs durch Streetview-Fahrzeuge. Google hat sich seinerzeit öffentlich entschuldigt und zugegeben, dass neben Daten zur Geräteidentifikation für den Google Kartendienst auch Nutzungsdaten von unverschlüsselten WLAN Netzwerken aufgezeichnet wurden (vgl. [San10]).

1.1.4 Standortdaten als forensisches Beweismittel

In der Forensik ist es die Aufgabe des Ermittlers auf Basis der zur Verfügung stehenden Beweismittel ein für das Gericht nachvollziehbares Gesamtbild einer Straftat zu erstellen (forensisch = gerichtsverwertbar). Hierbei erhöht jeder hergestellte Kausalzusammenhang der untersuchten Indizien die Möglichkeit zur objektiven Klärung des Tathergangs.

So können z. B. Reiserouten bzw. Häufungen von Informationen zu bestimmten Örtlichkeiten tragende Indizien für ein Verfahren sein. Darüber hinaus lassen sich in den sogenannten Metadaten zu Bildern, Videos oder Beiträgen in den sozialen Medien generell Zeitangaben und manchmal auch Ortsinformationen zusätzlich zu den Inhalten finden. Neben der Analyse und Rekonstruktion nativer Apps gewinnen Zeitstrahlanalysen (engl. timeline analysis) verschiedener Datentypen und Apps immer mehr an Bedeutung für die heutige Mobilfunkforensik.

Zum Zeitpunkt der Veröffentlichung von Allan und Warden im Jahr 2011 war die Erstellung, Betrachtung und Auswertung von timelines bzw. Standortdaten ein selten genutztes Mittel. Die Eigenentwicklung iPhoneTrackerLE soll hier Abhilfe schaffen. Ziel ist es, die Positionsdaten relevanter Zeitpunkte auf einer Karte zu visualisieren und direkt innerhalb der Anwendung in einem forensischen Bericht zu dokumentieren. Wie in Abb. 1.4 auf der nächsten Seite dargestellt, lassen sich so Geokoordinaten der Ortungsdatenbank von Apple (ausgewählte Zeitpunkte im linken Bereich der Abbildung) sehr anschaulich in der Kartenansicht (Mitte) darstellen, mit Notizen versehen (unterer Bereich der Software) und abschließend in Berichtsform bringen.

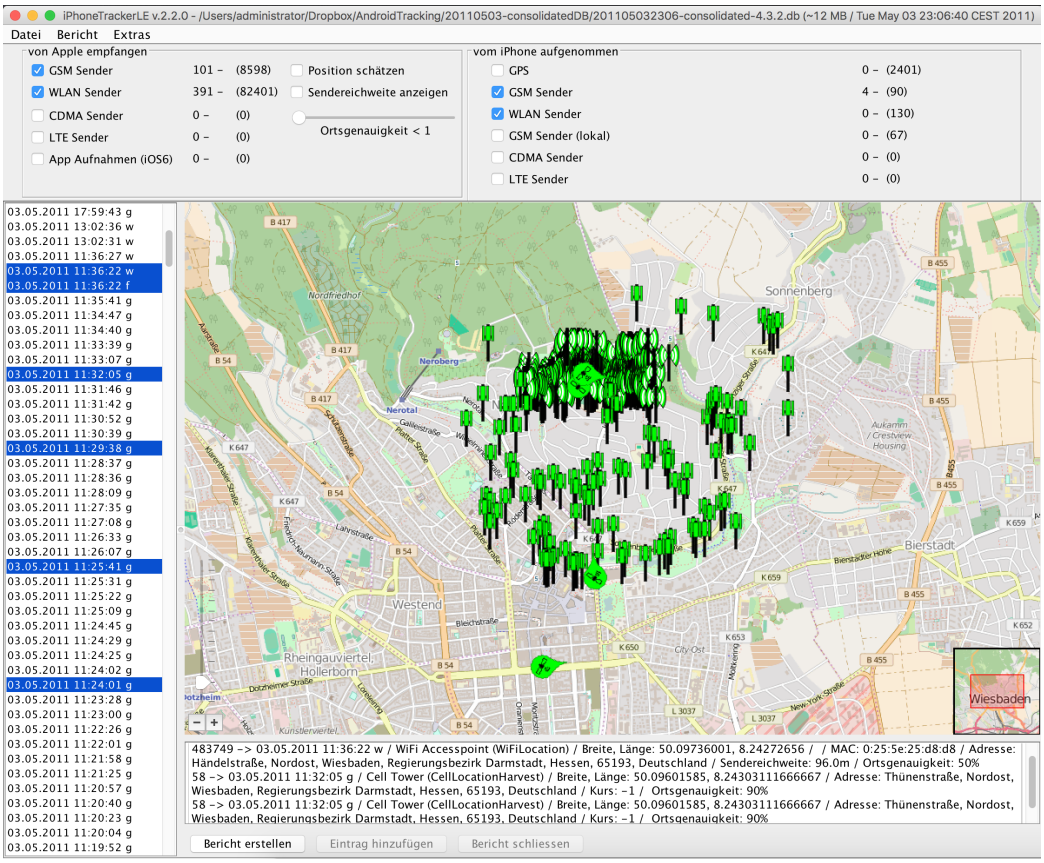


Abb. 1.4: Screenshot der Eigenentwicklung iPhoneTrackerLE - Darstellung der Benutzeroberfläche und Testdaten (GPS und Mobilfunksender); weitere Details im Text. Quelle: Eigene Darstellung. Kartenmaterial: © OpenStreetMap Mitwirkende 2011.

Hierbei muss nach hiesiger Einschätzung der Datenursprung zur Bewertung der Qualität der Standortdaten genau unterschieden werden. In der Anwendung wird der Datenursprung deshalb immer mit zum Zeitstempel angegeben. Ein »g« hinter der Zeitangabe steht z. B. für GPS, ein »w« für WiFI und das »f« steht für Standortdaten auf Basis von Funkzelleninformationen.

Zusätzlich zu den Standortdaten und einem Screenshot von der Kartenansicht lassen sich im finalen Ermittlungsbericht noch zusätzliche forensische Aspekte, wie z. B. der Datenursprung und weitere Freitextinformationen ergänzen. Durch einen Klick auf die Symbole der Geokoordinaten werden zusätzlich zur Adresse weitere forensisch relevante Aspekte (u.a. Standortabweichung) ermittelt und direkt im Textfeld unten hinterlegt.

1.2 Probleme in der IT-Forensik

Der Arbeitsbereich der IT-Forensik und insbesondere die Mobilfunkforensik sind geprägt durch ständige Veränderungen. Hierbei erschwert nicht nur die stetig steigende Anzahl der zu untersuchenden Geräte die Arbeit sondern vielmehr die immer fortschrittlicheren Sicherheitsfunktionen der Gerätehersteller.

In diesem Abschnitt wird neben der Betrachtung einer akuten Entwicklung weg vom reinen Desktop-Anwender hin zum mobilen Endgerätenutzer der Fokus auf die Herausforderungen bei der Datensicherung / -extraktion von Smartphones gelegt. Darüber hinaus soll auf Probleme im Umgang mit der Datenintegrität im Allgemeinen bzw. Möglichkeiten zur Manipulation von Beweismitteln im Speziellen hingewiesen werden.

1.2.1 Veränderung der Beweismittellage

Wie Abb. 1.5 zu entnehmen ist, steigt der Trend zur Smartphonenutzung in der Gesellschaft immer weiter an. Aktuell verwenden knapp 75% aller Deutschen zumindest hin und wieder ein Smartphone. Analog hierzu nimmt der weltweite Absatz an mobilen Endgeräten ebenfalls stetig zu (vgl. Abb. 1.6). Die Verkäufe steigen annähernd linear um ca. 200 Millionen Geräte pro Jahr, wohingegen der Absatz bei stationären Computersystemen mit rund 400-500 Millionen Geräten jährlich stagniert.

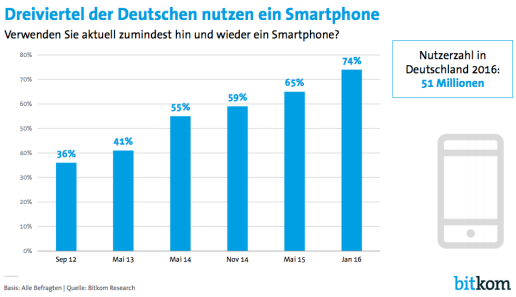


Abb. 1.5: Die Smartphonenutzung in Deutschland wird immer populärer, Quelle: [Ame16]

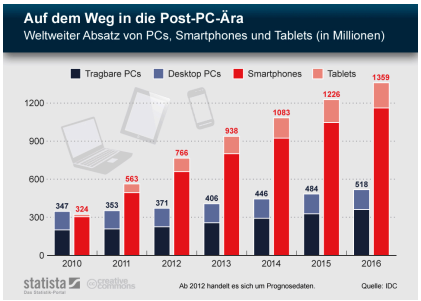


Abb. 1.6: Mobile Endgeräte dominieren den weltweiten Markt ab 2011, Quelle: [Ric16]

Demzufolge ist zu vermuten, dass auch Straftäter Smartphones besitzen und bei konspirativen Aktivitäten oder für vertrauliche Unterhaltungen einsetzen.

Traditionell befasst sich die IT-Forensik mit der gerichtsverwertbaren Sicherung und Aufbereitung der Inhalte von elektronischen Datenträgern in Dateiform, der Extraktion sowie Bereitstellung von Emailverkehr bzw. Kommunikationsspuren allgemein. Die Mobilfunkforensik hingegen war lange Zeit beschränkt auf die Extraktion von Adressbuchinformationen, Anrufprotokollen und Informationen von SIM-Karten. Mit der Verfügbarkeit von Smartphones hat sich dies verändert. Es folgt ein Rückgang der Menge verfahrensrelevanter Beweismittel auf Personal Computer (PC)s und die Verlagerung auf mobile Systeme oder in die Cloud.

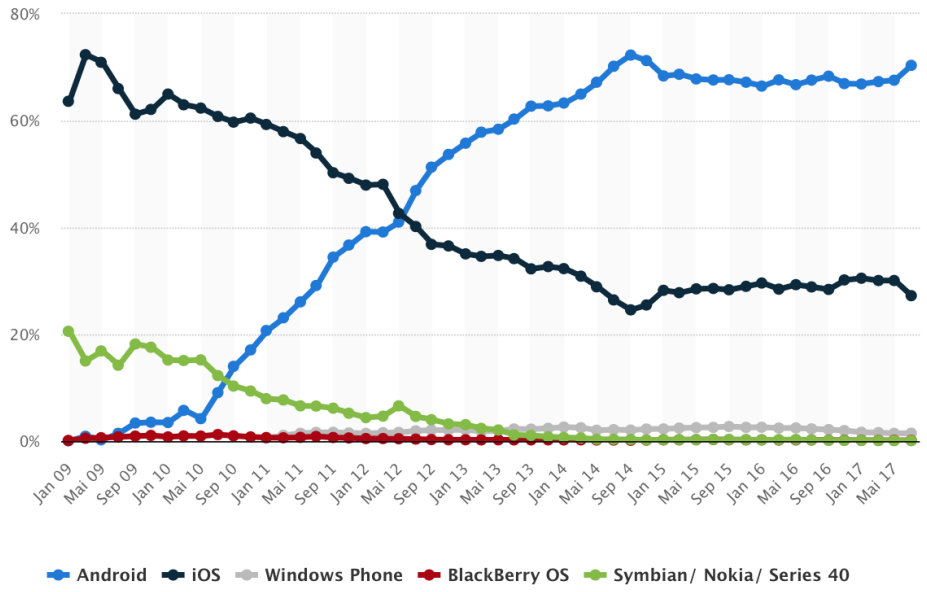


Abb. 1.7: Veränderung der prozentualen Marktanteile von Android (hellblau), iOS (dunkelblau), WindowsPhone (grau), BlackberryOS (rot) und Symbian/Nokia/Series 40 (grün) zwischen 2009 und 2017, Quelle: [Sta17].

Bezüglich der Marktanteile von Herstellern mobiler Betriebssysteme ist ebenfalls eine Verlagerung zu erkennen (vgl. Abb. 1.7). Während Apples Marktdominanz in 2009 noch bei über 70% gegenüber einem Anteil von 20% bei Google Android lag, nimmt ab 2010 der Marktanteil von Android stetig zu und löst Apple im Mai 2012 als Marktführer ab. Seitdem hält sich Apple halbwegs stabil bei ca. 30%, während Android die Führung mit knapp 70% für sich beansprucht. Mitbewerber wie Windows Phone, Blackberry OS oder Symbian spielen in der Mobilfunkforensik daher kaum eine Rolle.

1.2.2 Datenextraktion von mobilen Endgeräten

Nach der Maxime der Unveränderlichkeit der Daten in der IT-Forensik ist das Ziel einer forensischen Datensicherung eine 1:1-Kopie aller Daten des Asservates im Sinne einer physischen Sicherung inkl. gelöschter Bereiche. Hierzu wird der Datenträger ausgebaut und über eine schreibgeschützte Schnittstelle mit dem Sicherungsrechner verbunden. Ein solches Vorgehen ist in der Mobilfunkforensik nicht praktikabel, da die Speicherbausteine i. d. R. fest mit der Hauptplatine verlötet sind und die Software der Hersteller zum Synchronisieren der Benutzerdaten ein eingeschaltetes Gerät voraussetzen.

Der Fokus bei der Datenextraktion in der Mobilfunkforensik liegt daher mehr auf der Vertraulichkeit, Reproduzierbarkeit und einer möglichst vollständigen Extraktion von Daten als dem bitweisen Kopieren vom internen Datenspeicher ohne Veränderung am Gerät selbst. Darüber hinaus spielt es für den Analysten aufgrund wirtschaftlicher Gründe eine nicht unerhebliche Rolle, mit möglichst günstigen Tools und Methoden möglichst viele unterschiedliche Plattformen zu unterstützen und jeweils das Maximum an Daten zu extrahieren (vgl. Abschnitt 2.2 auf Seite 41).

In der nachfolgenden Tabelle werden verschiedene Extraktionsmethoden und die daraus resultierende Datenmenge verglichen. Die zu erwartende Datenmenge steigt dabei proportional zum Aufwand und den Kosten für den Ermittler.

Extraktionsmethode	**resultierende Datenmenge**	**Aufwand/Kosten**
Kopieren von Multimediadaten / einzelner Dateien über USB	einzelne Bilder, Videos bzw. Dateiinhalte aber keine Anwendungs- oder Systemdaten	gering / keine
Datensicherung über Hersteller- oder Drittanbietersoftware	beschränkte logische Datensicherung von Teilen der Anwendungsdaten inkl. Multimediadaten i. d. R. ohne Systemdaten	gering / keine
Datenextraktion über kommerzielle Drittanbietersoftware	erweiterte logische Datensicherung aller Nutzerdaten inkl. Multimedia- und tlw. Systemdaten	gering / niedrig
Datenextraktion über Open-Source-Tools und Community-Methoden	logische oder physische Dateisystemsicherung einer beschränkten Anzahl von Geräten / OS-Versionen	erhöht / keine
Datenextraktion über kommerzielle forensische Produktanbieter	logische oder physische Dateisystemsicherung einer großen Anzahl unterschiedlicher Plattformen	variiert / hoch
Chipextraktion und Auslesen der Speicherstrukturen	vollständige physische Datensicherung (aber oftmals verschlüsselt)	hoch / hoch

Tab. 1.1: Vergleich verschiedener Extraktionsmethoden in der Mobilfunkforensik hinsichtlich der resultierenden Datenmenge sowie dem Aufwand der Methode.

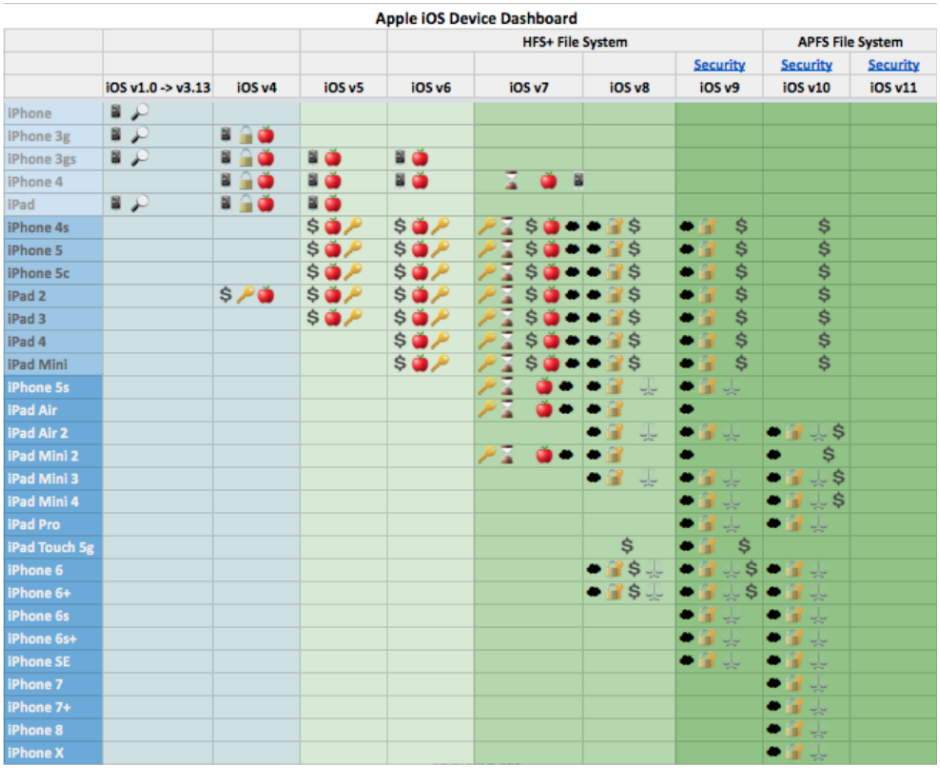


Abb. 1.8: Möglichkeiten von Ermittlungsbehörden für den Zugriff auf gesperrte Apple Geräte. Quelle: [Ack16]. Legende: siehe Seitenende ff..

Die größten Probleme für die Mobilfunkforensik entstehen durch den Einsatz von Kryptoverfahren, Sperrcodes auf den Geräten sowie weiterer Beschränkungen der Gerätehersteller beim Zugriff über den Universal Serial Bus (USB).

Der Zugriff auf den Datenbestand gesperrter kryptierter Smartphones ist ohne Kenntnis des Zugangscodes nur über Umwege möglich. Die unterschiedlichen Methoden zur Datenextraktion von solchen Geräten des Herstellers Apple ist in Abb. 1.8 dargestellt. So ist der mögliche Zugriff auf gesperrte Geräte im Einzelfall zusätzlich zur Verschlüsselung abhängig vom Gerätetyp, der Architektur des Prozessors sowie der Betriebssystemversion.

Wie in Abb. 1.8 zu sehen, existieren bis zur ersten Version des iPads kommerzielle Lösungen, um die Gerätedaten vollständig zu extrahieren (iPhone-Symbol). Die Lupe verspricht darüber hinaus die Rekonstruktion gelöschter Daten bis iOS4. Seit der Version iOS4 ist das Dateisystem standardmäßig verschlüsselt. Anfänglich ist die Kryptierung allerdings noch zu umgehen (siehe geöffnetes Schloss).

Das Apfel-Symbol steht weiter für Apple selbst, da es bis zur Einführung von iOS8 möglich ist, iPhones per richterlichem Beschluss (Symbol der Gerechtigkeitswaage vgl. [App17c]) entsperren zu lassen. Das Sanduhr-Symbol in Abb. 1.8 auf der vorherigen Seite gibt an, dass 4-stellige numerische Sperrcodes bestimmter Geräte bzw. iOS-Versionen mithilfe des Bruteforce-Verfahrens, durch das Ausprobieren aller möglichen Kombinationen teilweise zeitaufwendig, zu ermitteln sind. Darüber hinaus ist es möglich, Apple-Geräte mithilfe sogenannter Pairing-Records von zugehörigen Computersystemen zu entsperren. Diese Schlüsselpaare (daher das Schlüssel-Symbol) entstehen bei der Synchronisierung mit dem Computer und werden auf diesem gespeichert. Mit der Integration der iCloud-Dienste seit iOS8 zur Online-Speicherung von Gerätedaten gewinnt die Sicherstellung bzw. Beschlagnahme von Gerätedaten aus der Cloud (hierfür steht das Wolkensymbol in Abb. 1.8 auf der vorherigen Seite) immer mehr an Bedeutung.

Die Möglichkeiten der Datenextraktion gesperrter Android Geräte lassen sich nicht so komprimiert darstellen, wie dies bei iOS möglich ist. Neben der großen Vielzahl an Herstellern mit unterschiedlichen Produktlinien/Gerätevarianten ermöglicht die Quelloffenheit von Android den Firmen Anpassungen, welche die Zugriffsmöglichkeiten auf die Geräte ggf. noch weiter einschränken. Das Ziel hierbei ist die Erhöhung der Privatsphäre des Kunden bei Verlust bzw. gegen einen unbefugten Zugriff und nicht die Unterstützung forensischer Methoden. Dementgegen ermöglichen speziell angepasste Bootloader für Android-Geräte sehr häufig die Möglichkeit selbst gesperrte Geräte physisch auszulesen.

Aber selbst mit Zugang zum Gerät lassen sich je nach gewählter Methode nur bestimmte Datenbestände extrahieren. Wie der Abb. 1.9 auf der nächsten Seite zu entnehmen ist, lassen sich die vom Benutzer generierten Daten, wie z. B. persönliche Informationen aus Adressbüchern, Kalendern, Anruflisten oder den Notizen ermitteln. Darüber hinaus können häufig noch die Datenbanken von Messengerprogrammen sowie weiterer Applikationen extrahiert werden. Der Datenumfang entspricht somit dem einer Apple iTunes Sicherung. Mithilfe der sogenannten Filesystem-Sicherung (hier am Beispiel von Apple-iOS dargestellt) ist es möglich, zusätzlich hierzu noch die Mediendaten vom Gerät zu sichern. Bei diesen Varianten zur Datensicherung handelt es sich um sogenannte logische Sicherungen, d.h. es werden ausschließlich logisch lesbare Daten über vom Hersteller vorgesehene Softwareschnittstellen erlangt.

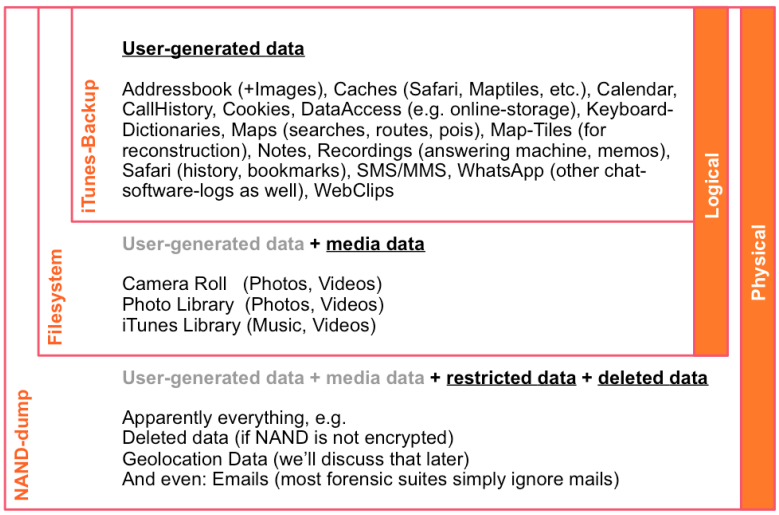


Abb. 1.9: Datenumfang möglicher Methoden zur forensischen Datenextraktion bei Apple. Die logische Extraktion (Logical) ermöglicht die Sicherung nutzergenerierter Daten sowie Mediendateien. Die aufwändigere und nicht immer mögliche physische Extraktion (Physical) ermöglicht darüber hinaus die Sicherung geschützter Systembereichen (z.B. der Ortungsdatenbank) sowie Rekonstruktion gelöschter Dateien.

Erst die vollständige Datenextraktion mittels NAND-dump bzw. dem physischen Auslesen des Speicherchips nach dem »Chip-Off« (Auslöten des Bausteins und Datenextraktion über spezielle Chip-Lesegeräte) machen es möglich, auch Daten aus nicht frei zugänglichen Systembereichen und logisch gelöschte Dateien zu rekonstruieren. Die Vielfalt an Smartphones mit unterschiedlichen Speicherbausteinen und proprietären wear-leveling Lösungen sowie spezieller Dateisystemen auf mobilen Plattformen (YAFFS) stellen die Mobilfunkforensik bei der logischen Filesystem-Extraktion bzw. physischen Spiegelung (NAND-dump vgl. Abb. 1.9) von Asservaten immer wieder vor neue Herausforderungen. Und das auch nur, wenn die Daten nicht verschlüsselt abgespeichert sind (siehe Apple-iOS). Die Problematik der Verschlüsselung bei Android führt häufig auch bei Inhalten auf externen Speicherkarten zu Problemen.

Bei iOS-Geräten mit aktivem Jailbreak besteht unter Umständen die Möglichkeit, über bestimmte Dienste wie SSH, auch auf systembeschränkte Daten zuzugreifen. Hierzu muss allerdings der Dienst zuvor vom Benutzer installiert worden und zum Zeitpunkt der forensischen Untersuchung aktiv sein. In der Praxis kommt dieser Fall sehr selten vor.

Darüber hinaus ist im Rahmen eines Strafverfahrens nach deutschem Recht die Beachtung der Verhältnismäßigkeit im Umgang mit den Beweismitteln in Bezug auf die Schwere der Straftat geboten. Demnach ist es gar nicht immer möglich bzw. erlaubt, alle Möglichkeiten der Datenextraktion auszuschöpfen. Darüber hinaus ergibt sich aus der Menge an zu untersuchenden Geräten bei der Polizei eine Beschränkung der aufgewendeten Zeit pro Extraktion/Aufbereitung bzw. Auswertung eines jeden Asservates.

Zusammenfassend begegnet der Mobilfunkforensiker bei der Datenextraktion je nach mobilem Endgerät und Zustand des Gerätes gleich mehreren Herausforderungen. Neben der Fragestellung zur geeigneten Extraktionsmethode und der Probleme einer anschließenden Aufbereitung/Rekonstruktion von Inhalten nach der Datensicherung muss der Forensiker zur Umgehung von Gerätesperren die Schwachstellen mobiler Betriebssysteme ausnutzen. Apples Ortungsdatenbank bzw. die Ortungsdateien bei Google lassen sich ebenfalls nur von gerooteten Smartphones extrahieren (mit Ausnahme von Apple iOS 4.0-4.3.2).

1.2.3 Abweichungen von Ortungsdaten

Wie bereits zu Beginn dieser Arbeit auf Seite 3 angedeutet, sowie später noch in Abschnitt 2.2.5 auf Seite 48 weiter ausgeführt werden wird, ergeben sich häufiger Abweichungen zwischen dem angezeigten und dem tatsächlichen Aufnahmeort von Bildern. Aber auch in anderen Artefakten aus mobilen Endgeräten wird offensichtlich, dass die Genauigkeit der Geoinformationen mitunter fragwürdig ist.

Zu diesem Thema stellte der bedeutende deutsche Computerforensikexperte Alexander Geschonneck 2011 im Internet eine Quizfrage (vgl. [Ges11]). Er bot demjenigen eine aktuelle Ausgabe seines Buches zur Computerforensik an, der in den Kommentaren zum Artikel den tatsächlichen Aufnahmeort eines Bildes angeben kann, bei dem die zugehörigen Geokoordinaten aus den Metadaten der Datei offensichtlich nicht dem Aufnahmeort entsprechen. Wie in Abb. 1.10 auf der nächsten Seite dargestellt, weicht die Position des Fotografen zum Standort aus den Metadaten (siehe roter Kreis auf der Karte) sehr stark ab. Diese und auch andere Abweichungen lassen sich allerdings recht simpel erklären, wenn man die Umstände der Lokalisierung betrachtet.

Abb. 1.10: Aus der Vorlesung »Mobile Systems Security« von R. Grimm. Quelle: [Gri15] zu fehlerhaften Standortdaten aus Exif-Daten in Bildern. Quelle: Geschonneck [Ges11].

Im Fall Geschonneck's wurde die Lokalisierung des Apple iPhone 3GS über aGPS sehr wahrscheinlich auf Basis von Funkzelleninformationen durchgeführt. Aufgrund der Sendereichweiten im Mobilfunk können so Abweichungen im Kilometerbereich zum tatsächlichen Gerätestandort auftreten, ohne das der Fehler im Bild vermerkt ist. Wie später in Abschnitt 6.5 auf Seite 164 beschrieben, sind die Angaben sehr wohl verfügbar, werden aber schlicht nicht gespeichert.

Abweichungen wie diese werfen ein schlechtes Licht auf die Beweiskraft von Geodaten in der Forensik. Ferner könnten Straftäter versuchen, Standortdaten zu manipulieren. So könnte die Kombination falscher Positionsdaten und Zeitstempel ein schlüssiges Alibi aufzeigen und so von der eigenen Schuld ablenken. Ohne konkrete, verlässliche Beweise heißt es dann: »in dubio pro reo« (lat. »Im Zweifel für den Angeklagten«).

In beiden Fällen gilt es die Qualität von Standortdaten verlässlich zu untersuchen und objektiv und eindeutig darzustellen.

1.2.4 Gezielte Manipulation von Standortdaten

Wann immer Daten erhoben oder gemessen werden, könnten diese Daten auch manipuliert worden sein. Im Folgenden werden ein eher akademischer Ansatz (extrinsisch – durch gezielte Veränderungen in der Umgebung) sowie eine in der Praxis leicht umzusetzende Möglichkeit (intrinsisch – durch den Einsatz sogenannter LocationFaker-Software) zur gezielten Manipulation von Ortungsdaten vorgestellt. Abschließend folgt noch ein kurzer Hinweis bezüglich gezielter Veränderungen von Standortinformationen in Bildern sowie der Synthetisierung von Adressdaten und den hieraus resultierenden Problemen in der Praxis.

Extrinsische Manipulation

Forscher der ETH Zürich beschreiben 2012 in ihrer Arbeit zum Thema »Location Spoofing: Attacks on Public WLAN-based Positioning Systems« [TRPC12] eine Möglichkeit, die Ermittlung von Standortinformationen in Apple Geräten gezielt zu manipulieren. Im Rahmen ihrer Forschung konnten die Wissenschaftler durch »AP-impersonating« (Vortäuschen einer dem Endgerät bekannten SSID) dafür sorgen, dass die Geräte einen falschen Standort anzeigen. Ein ähnliches Ergebnis entsteht mitunter, wenn WLAN-Stationen mit bestimmten generischen SSID Namen à la »Linksys«, »Telekom«, »Airport« etc. zur Standortbestimmung verwendet werden.

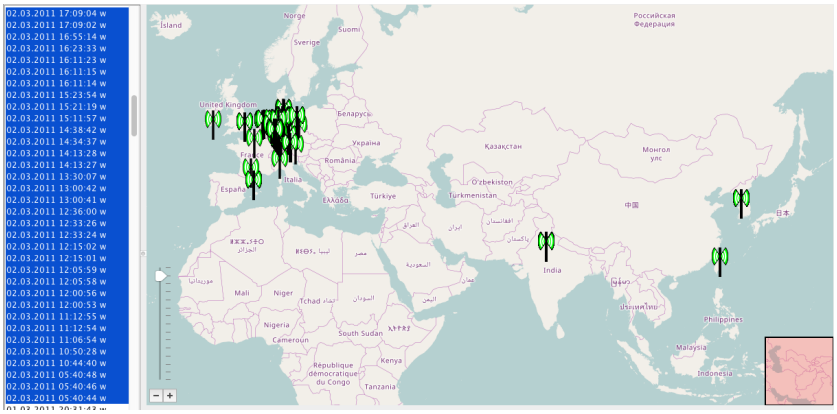


Abb. 1.11: Kartenansicht fehlerhaft verorteter WLAN-AccessPoints während eines Cebit-Besuchs in Hannover 2011. Quelle: Eigene Darstellung. Kartenmaterial: © OpenStreetMap Mitwirkende 2011.

Noch vor der Arbeit der Schweizer Kollegen fiel bei eigenen Untersuchungen auf, dass sich WLAN-Stationen nach einem Umzug negativ auf die Lokalisierung von Smartphones auswirken. So führte z. B. der WLAN-AccessPoint des zugezogenen Nachbarn dazu, dass der Gerätestandort einmalig und auch nur sehr kurz falsch angezeigt wurde. WLAN-Sender auf der Technikmesse Cebit im Jahr 2011 führten hingegen dazu, dass über den ganzen Tag verteilt falsche Standorte auf der ganzen Welt ermittelt wurden (vgl. Abb. 1.11 auf der vorherigen Seite mit Standorten aus einer iOS4.3.2-Ortungsdatenbank vom 02.03.2011).

In der Zwischenzeit haben Gerätehersteller reagiert. Anstelle der SSID werten Smartphones heutzutage die MAC-Adressen der Netzwerkadapter aus. Da sich auch MAC-Adressen manipulieren lassen, versuchen Hersteller seit neuestem Manipulationen bzw. Ortsveränderungen von Funksendern über Informationen zum Alter der Signale (sog. »ageing«) zu erkennen, um zweifelhafte Sender von der Positionsbestimmung auszuschließen.

Intrinsische Manipulation

Apples Entwickler-Richtlinien verbieten Funktionen zur Manipulation von Standortinformationen. Demnach lassen sich sogenannte LocationFaker zur Manipulation von Ortungsdaten auf Apple-Geräten auch nur über alternative Installationsanbieter, wie z. B. Cydia [(sa16] installieren. Hierzu ist es notwendig, Apples Betriebssystem zu modifizieren (sog. jailbreak).

Wie in Abb. 1.12 auf der nächsten Seite links dargestellt, lässt sich nach dem Start der Applikation »LocationFaker« (vgl. [Cun17]) eine beliebige Position auf der Welt einstellen. Anschließend wird in jeder Anwendung, auch in der »Find My Phone«-App von Apple (vgl. [App17a]), ein manipulierter Standort angezeigt (Mitte). Nur auf die in der Ortungsdatenbank von Apple korrekt gespeicherten Standortdaten hat die Manipulation keinen Einfluss (siehe Screenshot rechts).

Bedauerlicherweise konnte nicht abschließend geklärt werden, wie die iOS-App LocationFaker genau arbeitet. Eine Mailanfrage beim Autor der »LocationFaker«-App bzgl. der Arbeitsweise der Software LocationFaker blieb unbeantwortet. Es dürfte sich hierbei aber um eine Technik zur Manipulation des Datenstroms vom Dienst locationd handeln (sogenanntes function hooking), um so gefälschte Informationen als quasi-Antwort vom System einzustreuen.

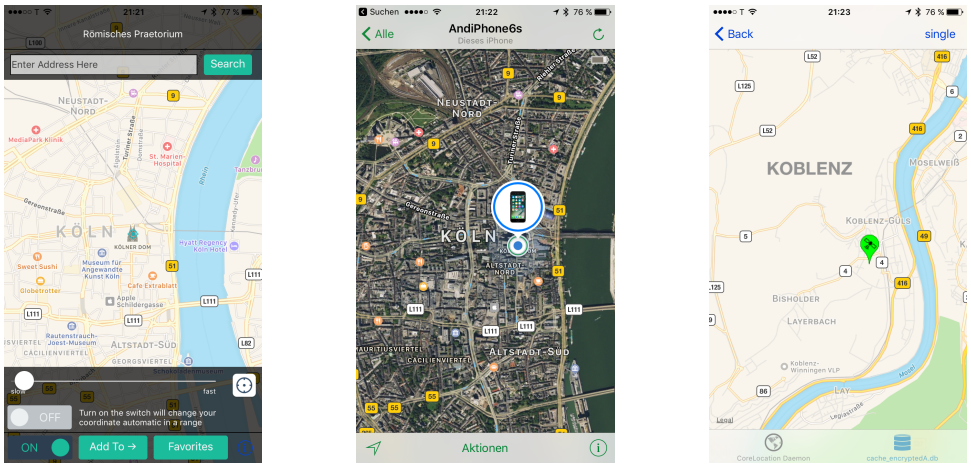


Abb. 1.12: Untersuchung von LocationFaker unter iOS. Links: Einstellen der Fake-Position. Kartenmaterial: © OpenStreetMap Mitwirkende 2017. Mitte: Manipulierter Standort in der App »Find My Phone«. Kartenmaterial © Apple 2017. Rechts: Korrekte Verortung in der Eigenentwicklung »iOSTracker« auf Basis der Standortdaten aus der Ortungsdatenbank. Kartenmaterial © Apple 2017.

Unter Google Android ist die Manipulation von Standortinformationen ohne Modifikation des Betriebssystems möglich. Android sieht von Haus aus vor, dass Entwickler sogenannte »mock locations« (auf deutsch Schein-Positionen bzw. simulierte Standorte) zu Testzwecken verwenden dürfen.

Nach der Freischaltung der Entwickleroptionen in den Systemeinstellungen lässt sich, wie in Abb. 1.13 auf der nächsten Seite links zu sehen, eine Anwendung für den Empfang simulierter Standortdaten einstellen. In der gleichen Abb. ist in der Mitte ein Screenshot der App »Fake GPS Location Spoofer Free« dargestellt (vgl. [Inc17]). Mithilfe dieses oder anderer Tools ist es ebenfalls und ohne Einstellung in den Entwickleroptionen möglich, beliebig ausgewählte Standorte in mobilen Anwendungen zu simulieren. Programme, wie z. B. Google Maps (in Abb. 1.13 auf der nächsten Seite rechts dargestellt), zeigen so die zuvor ausgewählte Position als vermeintlich tatsächlichen Gerätestandort an.

Die Möglichkeiten zur Simulation von Standorten sind allerdings begrenzt. So war es z. B. bei eigenen Untersuchungen weder durch Simulation der Standorte über die Entwickleroptionen noch mithilfe der App »Fake GPS« möglich, unter Android6 auf einem Huawei P8 Lite, gefakte Standorte auch in den Metadaten zu Fotos zu speichern. Trotz aktivierter Simulation weisen die Aufnahmen nach wie vor den tatsächlichen Gerätestandort als Aufnahmeort aus.

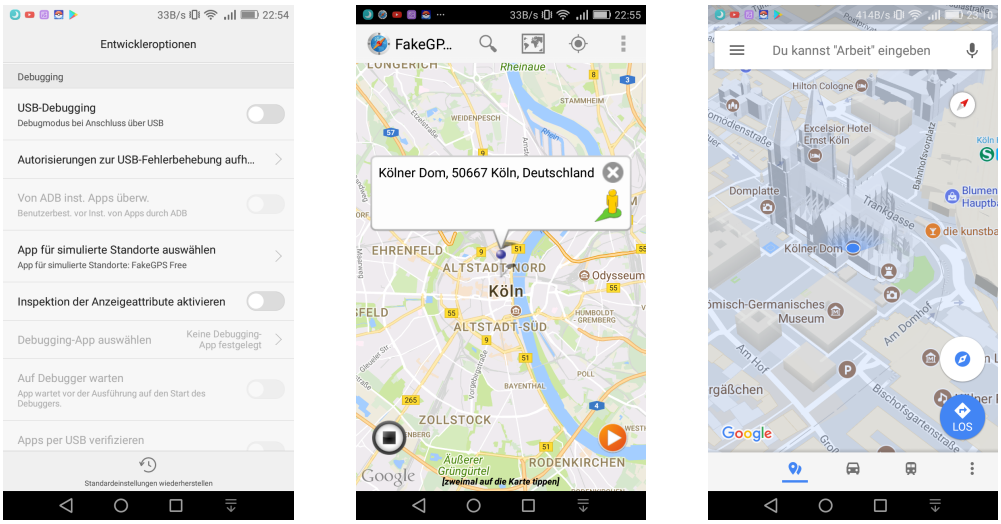


Abb. 1.13: Untersuchung simulierter/gefakter Standortdaten unter Android. Links: Simulierte Standorte via Entwickleroptionen. Mitte: Manipulation mithilfe der App »Fake GPS« [Inc17]. Rechts: Anzeige in GoogleMaps. Kartenmaterial © Google 2017.

Andere Tools zur Manipulation von Standorten funktionieren mitunter ebenfalls nicht wie gewünscht. So existieren z. B. Programme, die nicht mehr kompatibel zu aktuellen Android Versionen zu sein scheinen oder solche, bei denen der simulierte Standort in der Kartenanwendung permanent zwischen dem tatsächlichen Gerätestandort und dem simulierten Standort hin und her wechselt.

Manipulation von EXIF-Daten

Zusätzlich zu den eben beschriebenen Methoden zur Manipulation von Standortinformationen lassen sich Aufnahmeorte von Bilddateien retrograd mithilfe von Standardsoftware zur Bildverarbeitung /-verwaltung auf einem Computer oder auch dem Smartphone bearbeiten.

Hierbei wird in den Metadaten des Bildes der originäre Standort durch neue Geokoordinaten in Dezimalform ersetzt. Diese Art der Manipulation stellt die einfachste Form der Veränderung von Ortungsdaten dar. Ferner ist diese Art der Veränderung leicht zu erkennen, da sich bei der Anpassung des Standortes der Zeitstempel der letzten Änderung der Datei ändert. In der Folge stimmt dieser nicht mehr mit dem Erstellzeitpunkt der Ursprungsdatei überein und lässt auf eine Bearbeitung des Bildinhaltes oder eben der Metadaten schließen.

Extraktion synthetischer Adressdaten

Aktuelle Tools zur Mobilfunkforensik extrahieren häufiger auch Adressen in Textform, wie sie z. B. unter iOS und Android in diversen Datenbanken, Emails, Dokumenten, Googleanfragen etc. gespeichert sein können.

So lassen sich zwar unter Umständen interessante Standorte aus Suchanfragen im Web, Emails mit Adressdaten bzw. ortsabhängigen Einträgen im Kalender ermitteln. Deren Authentizität ist allerdings besonders kritisch zu prüfen. Denn selbst Daten aus vermeintlich gesicherten Quellen des Systemdienstes (consolidated.db) können tatsächlich vom Nutzer frei gewählt werden (vgl. Abb. 1.14).

#	Straßenposition	Info	Konfidenz	Kategorie	Gelöschte
1	(50.6 , 7.0)	**Beschreibung** com.google.GoogleMobile **Zeit** 20.01.2017 12:34:55(UTC+1) **Quelldatei** /var/root/Library/Caches/locationd/consolidated.db : 0x4F83 (Tabelle: Fences, Größe: 45056 Bytes) **Quelldatei:** /var/root/Library/Caches/locationd/consolidated.db : 0x4F83 (Tabelle: Fences, Größe: 45056 Bytes)		Reminder Locations	
2	(50.6 , 7.0)	**Beschreibung** com.google.GoogleMobile **Zeit** 20.01.2017 12:34:55(UTC+1) **Quelldatei** /var/root/Library/Caches/locationd/consolidated.db : 0x4D9D (Tabelle: Fences, Größe: 45056 Bytes) **Quelldatei:** /var/root/Library/Caches/locationd/consolidated.db : 0x4D9D (Tabelle: Fences, Größe: 45056 Bytes)		Reminder Locations	

Abb. 1.14: Ausgabe von Geoinformationen zu nutzergenerierten Standorten aus Apples ehemaliger Ortungsdatenbank »consolidated.db« in einem forensischen Bericht der Firma Cellebrite (vgl. Abschnitt 2.2.5 auf Seite 47).

Manipulationen von Daten durch Tatverdächtige fallen i. d. R. bei den weiteren Ermittlungen aufgrund von Widersprüchen in der Beweisführung auf. Mitunter ist es jedoch für technisch weniger versierte Ermittler schwierig, die Qualität und Vertrauenswürdigkeit der einzelnen Datenquellen richtig einzuschätzen.

Kurzum: Es existieren sowohl Möglichkeiten, um Geodaten in digitalen Beweismitteln zu manipulieren, als auch neue Standorte zu generieren. Die Techniken zur Manipulation des Ortungssystems im Live-Betrieb sind allerdings nur mit erweiterten Systemrechten umsetzbar. Hierzu müssen Android-Geräte gerootet und Apple Smartphones mit einem Jailbreak versehen sein. Solche Eingriffe sind ebenso erkennbar wie unstimmige Zeitstempel von Bilddateien.

1.3 Forschungsfragen

Für die forensische Arbeitsweise ist schlussendlich die Gerichtsverwertbarkeit das Ziel (vgl. [DF16], [fSidI11]). Hierbei besteht die Aufgabe des Forensikers darin, die Zuverlässigkeit der Untersuchungsergebnisse zu gewährleisten. Somit lautet die zentrale Frage für diese Arbeit: »Wie lässt sich die Verlässlichkeit von Geolokationsdaten gerichtsverwertbar feststellen?«

Die Verteidigung hingegen wird versuchen die Beweiskraft von Geodaten aus Smartphones dadurch zu schmälern, indem sie die Genauigkeit der Verortung in Frage stellt (vgl. Abschnitt 1.2.3 auf Seite 22). Aber »Verlässlichkeit« ist mehr als nur Genauigkeit. Im Rahmen dieser Arbeit versteht sich »verlässlich« als die Summe aus Integrität, d.h. unverfälscht von der Erhebung bis zur Würdigung, Eindeutigkeit und Vollständigkeit.

Inspiriert durch die CIA-Triade der IT-Sicherheit (vgl. [BA10]) sollen hierzu im Rahmen dieser Arbeit Fragen zur Vollständigkeit, Integrität und Genauigkeit von Ortungsdaten aus mobilen Endgeräten untersucht werden. Hierbei ergibt sich für die Betrachtung der Forschungsaspekte so z. B. folgende Reihenfolge:

- C ompleteness: Wie vollständig sind die Datenbestände?
- I ntegrity: Wie verlässlich sind die Datenquellen?
- A ccuracy: Wie genau sind die Standortdaten?

Im Weiteren gilt es konkrete Aspekte der Forschungsfragen zu bestimmen, um die Datenbestände der gängigen mobilen Betriebssysteme Apple iOS und Google Android später in Teil 4 ab Seite 65 daraufhin zu untersuchen.

Aus Sicht der Forschung und für die Mobilfunkforensik ist es zudem wichtig, neben der Absicherung der Analyse von Ortungsdaten aus iOS und Android ein möglichst allgemeines, unabhängiges und leicht nachvollziehbares Modell zur Beurteilung der Qualität von Geodaten aus Smartphones zu entwickeln (vgl. Abschnitt 5.5.2 auf Seite 143). Hierzu erfolgt neben der forensischen Analyse der erhobenen Daten später in Teil 5 ab Seite 131 die Diskussion der Entstehung von Ortungsdaten mithilfe nativer Smartphone-Anwendungen für Apple iOS und Google Android. Darüber hinaus muss die Darstellung der Standortdaten auch für Laien nachvollziehbar sein und darf keinen Zweifel an der Objektivität in der Beweisführung aufkommen lassen.

1.3.1 Completeness: Wie vollständig sind die Daten?

Für den polizeilichen Ermittler sind lückenlose Bewegungsprofile eines jeden Smartphones die ideale Arbeitsgrundlage. Dementgegen stehen die Forderungen von Datenschützern und Erklärungen der Hersteller, die gemäß ihrer Datenschutzbestimmungen (vgl. [App16e], [Goo17a]) Standortinformationen nur mit der Zustimmung der Nutzer ermitteln, ggf. speichern und oder online zum Hersteller übertragen dürfen.

Also konkret: »In welchem Umfang werden Standortdaten tatsächlich erhoben?«, bzw. »Existieren überhaupt zu jedem beliebigen Zeitpunkt der Gerätenutzung Geodaten?« Ferner stellt sich die Frage: »Werden Geolokalisierungsdaten auch ohne aktive Gerätenutzung im Hintergrund erhoben?« Schließlich ist bekannt, dass aktuelle Assistenzsysteme für ortsbezogene Dienste (engl. location based services) im Hintergrund die eigene Position ermitteln, um bei Bedarf schnellstmöglich gezielte Angebote in der Umgebung präsentieren zu können. Darüber hinaus muss bzgl. der Vollständigkeit von Geodaten aus Systemdiensten die nächste Frage beantwortet werden. »Existieren Unterschiede im Speicherumfang der Betriebssysteme von Google und Apple bzw. deren Versionen?« Dies ist nach der Ankündigung seitens Apple, den Speicherumfang der Ortungsdatenbank in iOS nach dem Skandal in den Medien rigoros zu begrenzen, stark zu vermuten (vgl. Abschnitt 1.1.3 auf Seite 13 no »more than seven days of this data« [App11] Frage 6). Umgekehrt lässt sich nach dem Wegfall der Speicherung von Ortungsdaten auf Android-Geräten bei Googles eine gewisse »Sammelwut« aufzeigen (siehe Abschnitt 4.2.4 auf Seite 125). Die Frage hierzu lautet: »Lassen sich Geodaten im Standortverlauf überhaupt löschen?«

Davon abgesehen ist bei der Sicherstellung von Smartphones darauf zu achten, dass neben der Gewährleistung der Zugriffsmöglichkeit auf das Endgerät durch das Deaktivieren der Gerätesperre möglichst keine Datenveränderungen mehr vorgenommen werden können; z. B. durch Aktivierung des Flugzeug-Modus. Das wirft die Frage auf: »Welche Automatismen bzgl. der Löschung gespeicherter Ortungsdaten sind auf Smartphones generell zu erwarten?« Und: »Lassen sich gelöschte Standorte beliebig rekonstruieren?« bzw. »Sind diese rekonstruierten Geodaten dann überhaupt noch gerichtsverwertbar?« Hierzu später mehr in Abschnitt 4.1.4 auf Seite 108.

1.3.2 Integrity: Wie verlässlich sind die Daten?

Wurden zum fraglichen Zeitpunkt Geodaten erhoben und konnten diese auch vom mobilen Endgerät extrahiert werden, so stellt sich die nächste Frage: »Besitzen die Daten die notwendige Integrität?« Denn Geoinformationen, die vor Gericht Zweifel aufkommen lassen, sind angreifbar. Wie bereits erwähnt, reicht bei Gericht bzw. der freien Beweiswürdigung mitunter die Unsicherheit im Einzelfall aus, um die Relevanz von Beweismitteln allgemein zu schmälern. Mit der Erhebung von Geodaten ist bzgl. der Frage zur Integrität allerdings nicht die Datenextraktion vom Gerät gemeint. Vielmehr ist zu klären: »Wie führen mobile Betriebssysteme die Standortbestimmung im Detail durch?« bzw.: »Wie integer sind die erhobenen bzw. gespeicherten Geodaten?«

Bezogen auf die Integrität der Analyse von Geolokalisierungsdaten aus mobilen Endgeräten in der Mobilfunkforensik muss so zunächst untersucht werden, ob Manipulationen der Ortungsdienste auszuschließen oder zumindest erkennbar sind. Ferner ist bekannt, dass Metadaten von Bildern im Nachhinein bearbeitet werden können. Hierzu existieren Anwendungen, die auch die Anpassung des Aufnahmeortes erlauben. Mitunter verfügen bereits die vom Hersteller mitgelieferten Betrachtungsprogramme über Funktionen, die auch die Möglichkeit zur Korrektur des Aufnahmeortes eines Bildes bieten (vgl. Abschnitt 1.2.4 auf Seite 24). Darüber hinaus existieren mobile Apps zur gezielten Manipulation des Gerätestandortes. »Wie wirken sich diese sogenannten LocationFaker (vgl. Seite 140) auf die protokollierte Position des Gerätes aus?« odee »Lässt sich auf diese Weise ein falsches Alibi generieren?« Falls ja: »Wie und unter welchen Umständen ist eine solche bewusste Manipulation zu erkennen?« Hierbei ist ebenfalls zu untersuchen, ob vorsätzliche Veränderungen immer und überall möglich sind. »Oder existieren bestimmte Datenquellen, bei denen eine Manipulation weniger wahrscheinlicher oder schwieriger zu bewerkstelligen ist?« Die Antwort hierauf wird später in Abschnitt 6.1 auf Seite 153 gegeben.

Ohne der Frage zur Genauigkeit von Ortungsdaten aus mobilen Endgeräten zu sehr vorwegzugreifen, spielt im Bezug zur Verlässlichkeit von Geodaten auch die Präzision der Standorte eine wesentliche Rolle. So ist die Frage zu stellen: »Welche Umstände bei der Geolokalisierung führen zu Abweichungen bei der Genauigkeit und wie lässt sich die Fehlertoleranz zuverlässig ermitteln?«

1.3.3 Accuracy: Wie genau sind die Daten?

Hinsichtlich der Genauigkeit von Ortungsdaten in der Mobilfunkforensik stellt sich zunächst die Frage: »Sind die Daten überhaupt ungenau?« GPS gilt gemein hin als präzise Methode zur Geolokalisierung. Unter guten Bedingungen beträgt die zu erwartende Standortabweichung nach dem sog. GPS-Fix i. d. R. nur wenige Meter (vgl. [Zog11] und [DG16]). Aber: »Wie präzise sind die Messwerten bis zum initialen GPS-Fix?«

Darüber hinaus wirken sich, wie bereits in Abschnitt 1.1.2 auf Seite 7 erwähnt, Umgebungsfaktoren, wie z. B. das »urban canyoing«, negativ auf die Präzision der Lokalisierung aus (vgl. [Gor11]). Hierzu wird später in Teil 5 ab Seite 131 mithilfe nativer Anwendungen für Android und iOS folgende Frage untersucht: »Wie reagieren die Hersteller auf Verortungsfehler im Allgemeinen und der zeitlichen Problematik bis zum initialen GPS-Fix im Speziellen?«

Die Verortung mittels aGPS auf Basis von Drahtlossendern lässt sich umgekehrt sehr schnell bewerkstelligen und ermöglicht die Positionsbestimmung auch dann, wenn kein GPS-Signal verfügbar ist. Dafür ist bei der Lokalisierung über Funkzellen im Mobilfunkbereich mit Standortfehlern im Kilometerbereich zu rechnen. Ferner ist noch die Frage zu klären: »Woher stammen die Standorte zu Stützsystemen wie Mobilfunk, WLAN oder NFC und mit welcher Häufigkeit werden die Daten aktualisiert?«

Zusammenfassend gilt es im Rahmen der vorliegenden Arbeit insbesondere die folgende Frage zu klären: »Wie lässt sich die Standortbestimmung über GPS durch Verwendung zusätzlicher Stützsysteme verbessern?« bzw.: »Gelingt den Herstellern die Optimierung der Geolokalisierung in jedem Fall?« Zudem scheint sich die Präzision der erhobenen Daten zur Laufzeit zu verändern. Hier stellt sich die Frage: »Wie schnell lässt sich eine möglichst exakte Positionsberechnung in unterschiedlichen Szenarien durchführen?« Für die Genauigkeit von Ortungsinformationen im Rahmen des Strafverfahrens ist ferner entscheidend: »Wie lassen sich etwaige Abweichungen zum tatsächlichen Standort ermitteln und nachvollziehbar darstellen?« Hierzu wurde bei der Entwicklung der Tools im Rahmen dieser Arbeit darauf zu achten, dass die potentiellen Abweichungen bzw. Sendebereiche der Drahtlossender zunächst dem Ermittler bzw. später dem Richter auch angezeigt werden können.

1.3.4 Existiert ein generisches Bewertungsmodell?

Ein weiteres Ziel dieser Arbeit liegt in der Erstellung eines generischen Modells zur Bewertung der Qualität von Ortungsdaten aus mobilen Endgeräten.

In diesem Modell sollen die Dimensionen für die Vollständigkeit, die Integrität sowie die Genauigkeit von Standortdaten aus mobilen Endgeräten falls möglich generisch abgebildet werden. »Existiert ein solches Modell, welches in der Interpretation nicht nur auf Daten aus iOS bzw. Android beschränkt ist?« Und wenn ja: »Ist es nachvollziehbar bzw. sind damit auch technische Laien in der Lage, die Bewertung von Ortungsdaten aus mobilen Systemen vorzunehmen?«

»Wie wirken sich die größeren Sendereichweiten von Mobilfunk gegenüber den geografisch stärker begrenzten Reichweiten bei WLAN-Netzen bis hin zu NFC-Sendern auf die zu erwartende Fehlerrate von Ortungsdaten für aGPS ohne GPS-Verfügbarkeit aus?« Und: »Lassen sich ggf. noch weitere Kriterien bei der Ausgestaltung des Modells erkennen?« In jedem Fall ist zu erwarten, dass die Zeit eine wesentliche Komponente innerhalb des Models zur Bewertung der Qualität von Ortungsdaten einnehmen wird (vgl. Abb. 5.13 auf Seite 143 bzw. Abb. 5.14 auf Seite 144).

Um der Forderung nach einer objektiven Darstellung in der Forensik gerecht zu werden, gilt es ferner von den unterschiedlichen Darstellungen kommerzieller Anbieter forensischer Produkte sowie proprietären Lösungen zu abstrahieren. Denn nur so lässt sich ein allgemeines Verständnis für die Interpretation und Nachvollziehbarkeit von Standortdaten ungeachtet der eingesetzten Software schaffen.

Schlussendlich soll im Rahmen dieser Arbeit auf induktivem Wege der Versuch unternommen werden, anhand der Bestrebungen einzelner Hersteller beim Aufbau von Ortungsdatenbanken eine möglichst generell gültige Aussage bzgl. der Entwicklung der Genauigkeit von Standortdaten abzuleiten. Hierzu werden neben qualitativen Studien Quasi-Experimente mit Realdaten verwendet, um von den speziellen Einzelfällen bzw. simulierten Labordaten auf ein universelles und herstellerunabhängiges Modell für Ortungsdaten zu verallgemeinern.

1.4 Eigener Ansatz und Struktur der Arbeit

Der Kern der Arbeit liegt in der Analyse und Interpretation von Artefakten der iOS- und Android Ortungsdienste sowie der gerichtsverwertbaren Darstellung von Ortungsdaten in der Mobilfunkforensik. Hierauf basierend und mithilfe von Erkenntnissen aus der Entwicklung nativer Anwendungen für Smartphones soll so ein allgemein gültiges Modell zur Bewertung der Qualität von Geodaten abgeleitet werden. Beides gilt es, durch Untersuchungen mit Apps für Apple iOS und Google Android zur Veranschaulichung der Entstehung von Ortungsdaten auf mobilen Endgeräten abzusichern.

Bisher wurden hierfür neben der Notwendigkeit zur Untersuchung und Analyse von Standortdaten in der Forensik (vgl. Abschnitt 1.1.1 auf Seite 2) bereits verschiedene Szenarien angeführt, die mit einer unterschiedlichen Menge an gespeichertern Standortdaten auf Smartphones einhergehen. Darüber hinaus sind ab Seite 16ff. wesentliche Herausforderungen der IT-Forensik beschrieben sowie Forschungsfragen hierzu aufgestellt worden (vgl. Abschnitt 1.3 auf Seite 29).

In Teil 2 ab Seite 36 sollen ausgewählte Abhandlungen sowie ab Seite 41 gängige Softwarelösungen mit Bezügen zur kriminalforensischen Arbeit und Auswertung von Standortdaten vorgestellt und diskutiert werden. Nach der Erläuterung der Forschungsmethode DSRM (Design Science Research Method) in Teil 3 ab Seite 55 folgt dann der Theorieteil mit den Grundlagen und forensischen Untersuchungen von Standortdaten aus Apple- sowie Google-Geräten von Seite 66 bis 130. In Teil 5 ab Seite 131 wird dann die zuvor durchgeführte Interpretation der Daten mithilfe nativer Anwendungen abgesichert, bevor in Teil 6 ab Seite 150 auf die Reflexion der Forschungsfragen sowie weiteren Grenzen und Möglichkeiten mobiler Geolokalisierung eingegangen wird. Neben einer Diskussion der Erkenntnisse aus dieser Arbeit soll in diesem Kapitel u.a. noch ein Ausblick auf potentielle Weiterentwicklungen der entstandenen Werkzeuge sowie Möglichkeiten der Erweiterung bei der Speicherung von Metadaten gegeben werden.

Für die forensische Untersuchung von Standortdaten aus Smartphones wurden eine Vielzahl von Datensätzen aus diversen Experimenten unter realen Bedingungen analysiert. Insbesondere wurde das Verhalten der Ortungssysteme auf Reisen sowie ungünstigen Umständen für die Standortbestimmung untersucht. Die hierbei festgestellten Unterschiede bei der Qualität der Standortdaten wer-

den in Abschnitt 5.5.2 auf Seite 143 zusammengefasst und eruiert. Darüber hinaus wurden zur Absicherung der forensischen Untersuchungen und zur analytischen Interpretation von Standortdaten unmittelbar während der Entstehung auf dem Smartphone mehrere native Anwendungen für iOS und Android programmiert. Die Applikationen werden in Teil 5 ab Seite 131 detailliert vorgestellt. Unter anderem ermöglichen die Apps den Prozess der Geolokalisierung unmittelbar auf dem mobilen Endgerät live mitzuverfolgen und auch retrograd zu analysieren.

Der Theorieteil der Arbeit wurde bewusst in zwei Kapitel aufgeteilt, um sowohl die forensische Untersuchung von Standortdaten als auch die praktischen Teile der Analyse zur Entstehung von Geolokalisierungsdaten auf mobilen Endgeräten unabhängig von einander darzustellen. Zwar wirkt sich die praktische Erfahrung der Implementierung nativer Anwendungen zur Geolokalisierung hilfreich auf die Analyse und Interpretation von Standortdaten aus, nichts desto trotz müssen kriminalpolizeiliche Ermittlungen jedoch objektiv und unabhängig von Optimierungen bei der Programmierung einzelner Anwendungen durchgeführt werden.

Neben der analytischen Interpretation von Standortdaten liegt der Fokus der Arbeit auf der praktischen Anwendung der entwickelten Werkzeuge innerhalb der Mobilfunkforensik (vgl. Abschnitt 1.1.4 auf Seite 14). Mithilfe der Desktop-Anwendungen iPhoneTrackerLE und GoogleTrackerLE können die Daten von Apple iOS- sowie Google Android-Geräten aber auch Daten der Google-LocationHistory eingelesen und grafisch auf einer Karte visualisiert werden. Für den polizeilichen Ermittler war hierbei die Unterscheidung des Datenursprungs (stammen die Daten direkt vom Gerät oder dem Hersteller?) sowie die Betrachtung der potentiellen Standortabweichung (farbliche Radien um die Standorte) von besonderem Interesse.

Zudem erfolgt im Rahmen dieser Arbeit eine Unterscheidung der Ortungsdaten aus Systemdiensten von Google und Apple zu Standortdaten gegenüber Metadaten von Bildern oder gar Adressinformationen aus Anwendungen der Hersteller, wie z. B. Apple Mail, Kontakte etc.. Viele forensische Lösungen, welche in Abschnitt 2.2 auf Seite 41 ausführlich vorgestellt werden, schließen in ihre Berichte hingegen potentiell jede Information mit ein, die zu einem Standort oder einer Adresse aufgelöst werden kann. Einige Hersteller von Forensiklösungen setzen darüber hinaus zusätzlich auf synthetisch erzeugte Standortdaten anhand verbundener Drahtlosnetzwerke auf Basis von Drittanbieterdatenbanken.

Teil 2

Stand der Technik

2.1 Verwandte Arbeiten

Das Thema »Ortungsdaten in mobilen Endgeräten« ist Gegenstand zahlreicher, vorwiegend forensischer Abhandlungen. Im Folgenden sollen, ohne Anspruch auf Vollständigkeit, die Werke bekannter Forensiker sowie Wissenschaftlern zum Thema aufgezählt werden. Die Tiefe der Werke im Umgang mit der Materie ist hierbei vor allem abhängig vom untersuchten Betriebssystem. Auffallend ist gleichwohl, dass es bereits vor 2011 Literatur zum Thema Smartphone Forensik gibt (s.u. Hoog, Zdziarski). Eine Zunahme des Interesses plus die Spezialisierung der Mobilfunkforensik ist inzwischen deutlich zu spüren. Neben amerikanischen Forensikexperten beschäftigen sich mittlerweile auch deutsche Wissenschaftler wie Spreitzenbarth oder Schuba et al. mit der Betrachtung von Geodaten in mobilen Endgeräten.

2.1.1 Andrew Hoog

Der Mitbegründer und CEO von NowSecure (alt viaforensics) gilt als Experte für Mobilfunkforensik und Sicherheit in mobilen Systemen. Andrew Hoog nimmt als Sprecher an Sicherheitskonferenzen [wtwts17] teil und tritt als Gutachter vor Gericht auf [Now17]. In seinen Büchern »Android Forensics« und »iPhone and

iOS Forensics« wird das gesamte Spektrum der Mobilfunkforensik vorgestellt, von der Datenextraktion bis hin zur Auswertung (vgl. [Hoo11] und [HS11]).

Die Werke sind sehr allgemein gehalten und geben bezogen auf die Auswertung von Geodaten den Stand der Forschung 2011 wieder. Konkret wird nur im Hinblick auf Apple iOS in [HS11] ab Seite 172ff. auf die systemimmanenten GPS Daten des Ortungsdienstes mit Verweis auf die iOS4-Datenbank consolidated.db eingegangen.

2.1.2 Jonathan Zdziarski

Zdziarski gilt ebenfalls als international renommierter Experte in Sachen Smartphone Forensik und Sicherheit in mobilen Systemen. Seine ersten Beiträge zum Thema Sicherheit in iOS erschienen noch unter dem Pseudonym »nervegas« als Teil der Jailbreaking-community. Unter dem Begriff des Jailbreak'ens versteht man Sicherheitslücken in Apples Betriebssystem so auszunutzen, dass auch ein nicht von Apple signierter Programmcode ausgeführt werden kann. Zunächst ist das Ziel der Entwickler, den erweiterten Systemzugriff dazu zu nutzen, das Mobilfunkmodem zu manipulieren, um Providersperren (den sog. SIM-Lock) auszuhebeln. Später verwendet Zdziarski die Techniken dazu über erweiterte Systemrechte ein vollständiges Abbild des internen Datenspeichers zu extrahieren.

Dem Thema Geodaten widmet Zdziarski in seinem Buch [Zdz13] »iOS Forensic Investigative Methods« zwei Abschnitte. Zunächst beschreibt er im Abschnitt »Extracting Image Geo-Tags« auf Seite 71 anhand der Software exifprobe [Fig11], wie sich Geodaten aus Bildern ermitteln lassen. Später beschreibt er im Abschnitt »Consolidated GPS Cache« auf Seite 83, wie sich Positionsdaten aus der Apple-Datenbank »consolidated.db« bzw. genauer den Tabellen »wifilocation« sowie »celllocation« extrahieren lassen. Zdziarki liefert allerdings noch keine Ansätze hinsichtlich der Bewertung von Standortdaten. Er stellt lediglich Methoden zur Extraktion von Artefakten aus iOS dar und überlässt die Bewertung der Daten dem Ermittlern.

Darüber hinaus trägt Jonathan Zdziarski zum Thema Geodaten hin und wieder über Kanäle der sozialen Medien (twitter-Account) sowie seinem persönlichen Blog bei.

2.1.3 Fachhochschule Aachen

Der Lehrstuhl IT-Forensik von Professor M. Schuba sowie Dipl.-Ing. H-W. Höfken an der FH Aachen hat sich als feste Größe im Umfeld der Forensik in Deutschland etabliert. So veranstaltet die FH Aachen z. B. jährlich den IT-Forensik Workshop in Aachen.

In »Forensic Analysis of Geodata in Android Smartphones« [MHS11] beschäftigen sich S. Maus, Höfken und Schuba erstmals öffentlich mit Geodaten in Android Smartphones. Auf Seite 3 beschreiben die Autoren z. B. eine Tabelle mit potentiell zu erwartenden Genauigkeiten verschiedener Ortungssysteme. Darüber hinaus wird die Bedeutung der Herkunft der Geodaten hervorgehoben und als Basis für die Genauigkeit der Verortung beschrieben. Eine solche Betrachtung ist, wie sich später in Abschnitt 5.5.2 auf Seite 144 zeigen wird, essentiell für die Absicherung der Qualität von Standortdaten allgemein. Im weiteren Verlauf des Papiers wird dann allerdings mehr auf die Extraktion der Daten sowie deren Speicherung und Repräsentation eingegangen, als auf die eingangs beschriebene Genauigkeit. Letztlich lässt sich nur aus der Angabe der App, von der die Daten stammen, noch ein Rückschluss auf die Präzision gewinnen. So kann z. B. bei Daten aus der dargestellten Applikation Garmin Navigon aufgrund der Funktionsweise zur Navigation auf eine höhere Genauigkeit der erhobenen Standortdaten geschlossen werden. Die entsprechende Angabe bzw. grafische Darstellung der Abschätzung fehlt indes.

2.1.4 Universität Erlangen

Michael Spreitzenbarth war bis 2013 Mitarbeiter bei Professor Felix Freiling an der Friedrich-Alexander Universität in Erlangen. Im Rahmen seiner Forschung zur forensischen Extraktion von Daten aus Android Geräten mithilfe des Android Data Extractor Lite (ADEL) veröffentlichte er zusammen mit Sven Schmitt einen Beitrag zum Thema Ortungsdaten in Android. Die beiden stellen anhand einer Technik zur automatisierten Extraktion und Darstellung von Geoinformationen aus Multimediadateien dar wie wichtig Seitenkanäle für die kriminalistischen Ermittlungen sein können. In dem Artikel »IS DATA RETENTION STILL NECESSARY IN THE AGE OF SMARTPHONES?« [SS12] wird neben der reinen

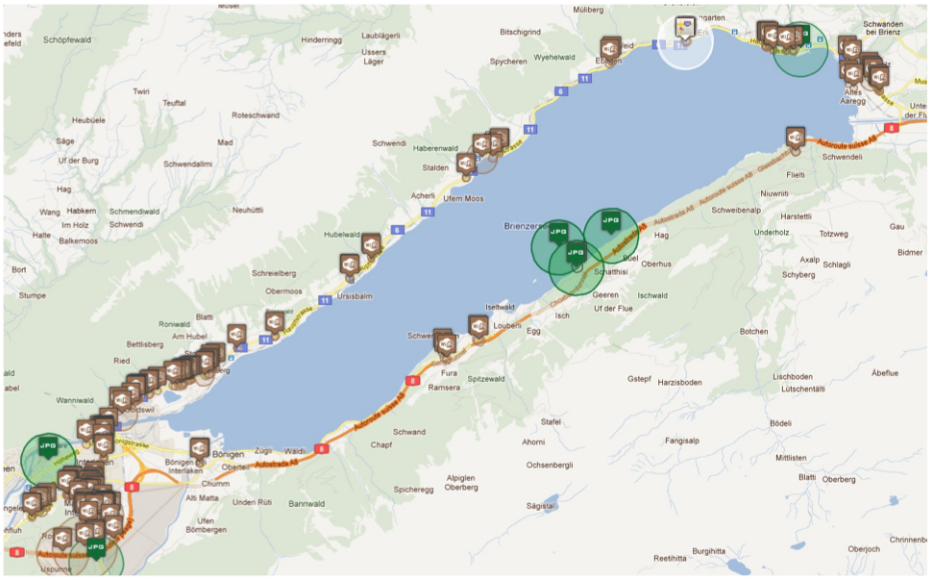


Abb. 2.1: Kartenansicht verschiedener Standortdaten zu WiFi-, Bild- sowie Karteninformationen inkl. Standortabweichungen in ADEL. Quelle: [Spr13] S.88. Kartenmaterial: © OpenStreetMap Mitwirkende 2012

Darstellung von Geodaten auch die Reflexion bzgl. Genauigkeit und Gerichtsverwertbarkeit von Android Ortungsdaten angeführt. Wie in Abb. 2.1 dargestellt, werden Standortinformationen inklusive einer möglichen Fehlertoleranz in Form von Umgebungsradien zur Position angegeben. Bei den Datenpunkten mit dem Label »wifi« dürfte es sich um den Senderadius der Funksender handeln. Bei den Radien um die Label »JPG« sowie dem Kartensymbol ist jedoch unklar, wie die Größe des Radius ermittelt wurde. Nach derzeitigem Stand der Technik weisen Metadaten in Bildern keine Informationen zur möglichen Abweichung des Aufnahmeortes aus.

In seiner Dissertation mit dem Titel »Dissecting the Droid: Forensic Analysis of Android and its malicious Applications« [Spr13] geht Spreitzenbarth dann nochmals auf die Thematik Ortungsdaten aus Androidgeräten ein. Wieder wird der Vorteil einer potentiell höheren Genauigkeit von Ortsangaben, welche vom Smartphone extrahiert werden, festgestellt. Darüber hinaus führt Spreitzenbarth Untersuchungen zur Fehleranfälligkeit von Geoinformationen aus Smartphones innerhalb von Gebäuden durch. Hierzu wurden nach den Angaben auf Seite 97 seiner Abhandlung rund 1000 Fotos aufgenommen und gegen Ortsinformationen eines hochempfindlichen GPS-Empfängers evaluiert.

Zusammenfassend wird im Gegensatz zu den vorherigen Veröffentlichungen in den letzten beiden Arbeiten erstmals eine Repräsentation von Ortungsdaten mit mehr als nur der Angabe von Geokoordinaten vorgestellt. Im Gegensatz zur vorliegenden Arbeit fehlt allerdings noch die Betrachtung der Entstehung von Ortungsdaten in mobilen Endgeräten.

2.1.5 Eigene Veröffentlichungen

Im Vorfeld zu dieser Arbeit wurden bereits 2011 und 2012 unter dem Pseudonym »4rensiker« die ersten Beiträge im Internet veröffentlicht:

- »iPhone Tracking – from a forensic point of view« [(4r11]
- »Android Tracking – from a forensic point of view« [(4r12]

Ziel der beiden englischsprachigen Artikel war die Schärfung des Bewusstseins im Bereich der Mobilfunkforensik und weniger die Unterstützung des medialen Hypes hinsichtlich der Apple-Affäre. Später wurden dann im Rahmen dieser Arbeit noch zwei weitere Artikel in deutschsprachigen Fachzeitschriften zum Thema veröffentlicht:

- »Ortungsdaten in modernen Smartphones«
  <kes> Die Zeitschrift für Informationssicherheit [Dhe13]
- »Standortlokalisierung in modernen Smartphones«
  Informatik-Spektrum (Springer Verlag) [DG16]

Darüber hinaus lassen sich teilweise noch Folien zu Beiträgen zum Thema Smartphone-Tracking auf diversen Konferenzen, Vorlesungen, Workshops etc. finden, sofern diese online bereitgestellt wurden (z. B. [Dhe12], [Gri13], [Gri15]).

Bei den Veranstaltungen handelt es sich um:

- Vorlesung »Sicherheit in mobilen Anwendungen« an der Uni Koblenz
- IT-Forensik Anwendertagung beim Fraunhofer SIT
- DV-Sachbearbeitertagung der Polizei in RLP (mehrfach)
- Nationale IT-Ermittlertagung in der Schweiz (mehrfach)

Zusammenfassend wurden die Inhalte und Ergebnisse dieser Arbeit sowohl mit Akademikern, als auch kriminalpolizeilichem Fachpublikum diskutiert.

2.2 Softwaretechnische Umsetzungen

Neben schriftlichen Arbeiten zum Thema Ortungsdaten aus mobilen Endgeräten existieren ferner Anwendungen zur Aufbereitung von Geolokalisierungsdaten. Die Programme iPhoneTracker und MyPhoneTracker beschränken sich hierbei ausschliesslich auf die Darstellung der Ortungsdaten aus den Systemdiensten während die Tools kommerzieller Hersteller wie Oxygen Forensics, MSAB und Cellebrite sowohl Standortdaten der Systemdienste als auch Ortsinformationen anderer Quellen verarbeiten können.

2.2.1 iPhoneTracker

Die von Pete Warden und Alasdair Allen entwickelte Software iPhoneTracker legte 2011 den Grundstein für die globale Diskussion um die Speicherung von Ortungsdaten in Apple Geräten. Die Abbildungen 2.2 und 2.3 zeigen Screenshots der Software mit Standortdaten aus mehreren Eigenversuchen unter iOS 4.3.2. Auffällig ist hierbei a) die potentiell unbegrenzte Speichermenge (Abb. 2.2) sowie b) Fehler in der Darstellung der Standortdaten (vgl. Abb. 2.3 auf der nächsten Seite).

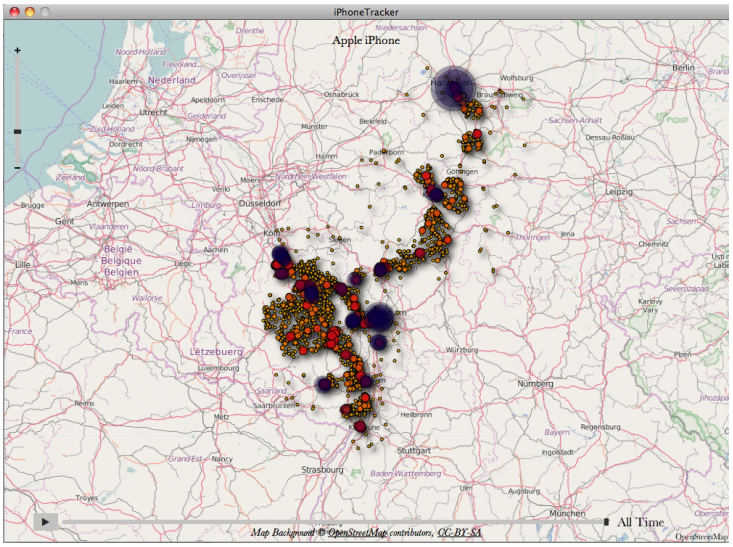


Abb. 2.2: Kartenansicht mit enormen Mengen an Standortdaten aus eigenen Untersuchungen unter iOS 4.3.2. im iPhoneTracker von [War11]. Quelle: Eigene Darstellung, Kartenmaterial: © OpenStreetMap Mitwirkende 2011

Die ausschließlich unter MacOSX lauffähige Software ermittelt hierfür zunächst die via iTunes synchronisierte Ortungsdatenbank »consolidated.db«. Anschliessend werden die Inhalte der Datenbank aufbereitet und mittels Projektion auf das Kartenmaterial von OpenStreetMap übertragen (siehe Screenshots).

Am unteren Ende des Programmfensters kann dann über einen Schieberegler Einfluss auf die angezeigten Ortsinformationen genommen werden. Ferner ist die Interaktion mit der Karte selbst (zoomen, verschieben etc.) vorgesehen. Die Darstellung der Ortsinformationen selbst ist in ihrer Größe und Färbung davon abhängig, wie viele Datenpunkte verarbeitet wurden. Demnach geben kleinere, gelbe Kreise an, dass sich 1-2 Datenpunkte in der Umgebung und bei größeren, dunkelblauen, einige Dutzend Punkte in der näheren Umgebung befinden. Gezählt werden hierbei wie viele Punkte sich innerhalb eines Hundertstel eines Quadratgrades befinden (vgl. [War11]).

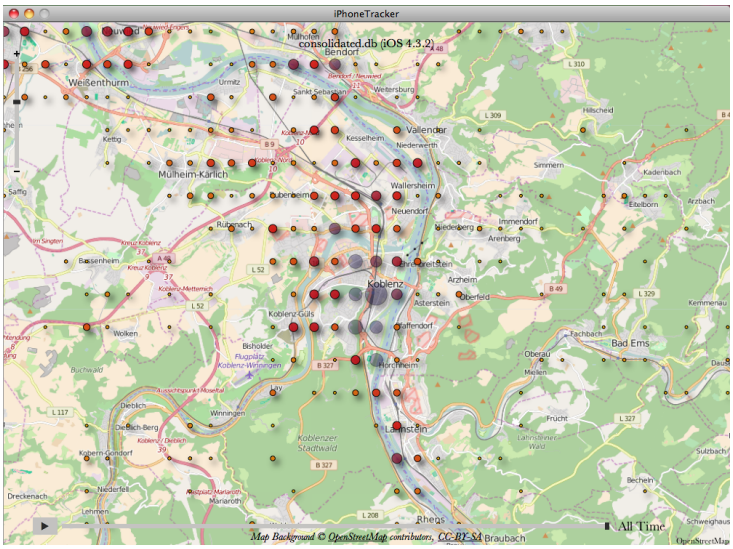


Abb. 2.3: Fehlerhafter Darstellung (Rasterung) von Standortinformationen durch Rundung der Koordinaten im iPhoneTracker von [War11]. Quelle: Eigene Darstellung. Kartenmaterial: © OpenStreetMap Mitwirkende 2011.

Die Software ist aus forensischer Sicht allerdings unbrauchbar, da die Standortdaten bei der Verarbeitung manipuliert werden. Durch die Rundung der Geokoordinaten auf zwei Nachkommastellen entsteht eine Rasterung, wie sie in Abb. 2.3 zu sehen ist. Zusammenfassend wird die Software maximal einem Proof-Of-Concept gerecht, da sie weder Funktionen für Datenim- noch -export bietet.

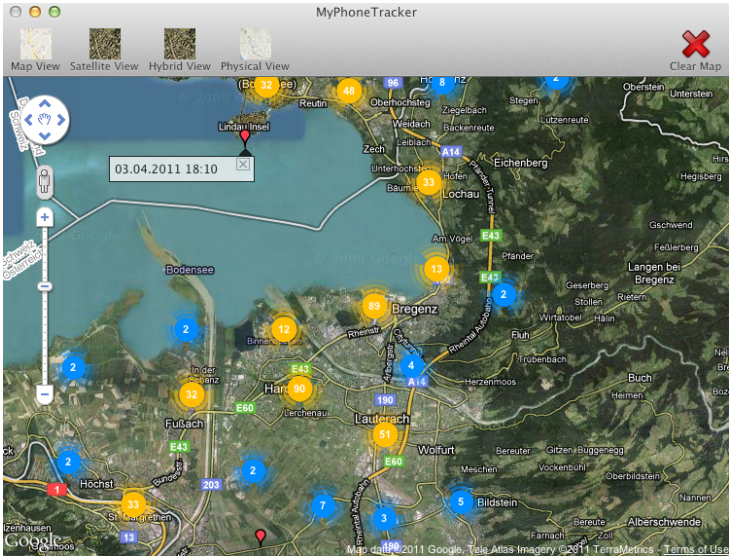


Abb. 2.4: Korrekte Verortung von Standortinformationen im MyPhoneTracker. Legende: blaues Icon: bis zu 10 Standorte, oranges Icon: mehr als 10 Standorte. Quelle: [Ano11], Kartenmaterial © Google 2011.

2.2.2 MyPhoneTracker

Die Software MyPhoneTracker bietet Lösungen zu einigen Einschränkungen des iPhoneTrackers. So erfolgt z. B. keine Manipulation der Daten und es ist möglich, eigene Daten zu laden bzw. zu verarbeiten. Darüber hinaus erlaubt die Software das Laden von Daten des Google-Ortungsdienstes bzw. den Dateien cache.cell und cache.wifi (vgl. Abschnitt 4.2.1 auf Seite 110). Eine zeitliche Navigation mittels Zeitstrahl existiert hingegen nicht. Dafür werden beim Klicken auf die jeweiligen Datenpunkte mit der Maus in einem Popup-Fenster die zugehörigen Zeiten angezeigt (vgl. Abb. 2.4). Die Darstellung mehrerer Datenpunkte zu einer bestimmten Position ist ebenfalls abhängig von der Menge an Einträgen. Wie in Abb. 2.4 zu erkennen, werden die Positionsdaten entweder in blauen (< 10 Einträge) oder ansonsten gelben Icons bei mehr als 10 Einträgen angezeigt.

Zusammenfassend wirkt die Umsetzung im MyPhoneTracker ausgereifter als im iPhoneTracker. Grundsätzlich bietet aber auch diese Software keinerlei weitergehende forensischen Funktionen, wie z. B. die Erstellung eines Berichtes. Für den Datenexport existiert lediglich die Möglichkeit, den Bildschirmausschnitt zu drucken bzw. den angezeigten Kartenausschnitt als Bitmap-Grafik zu exportieren.

2.2.3 Oxygen Forensic Suite

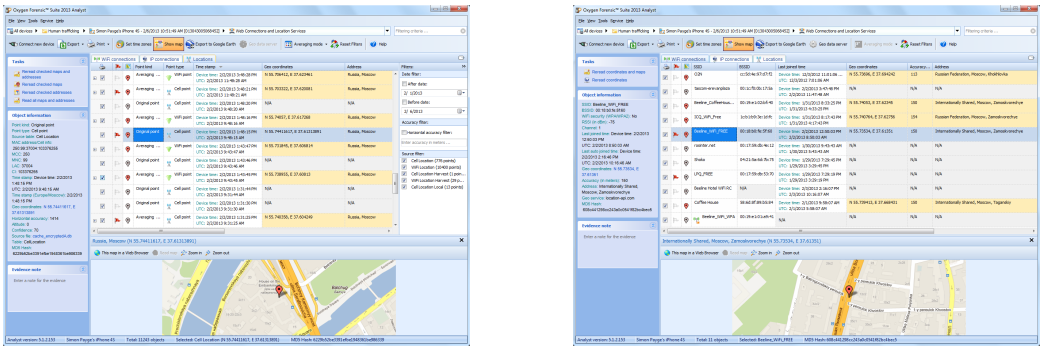


Abb. 2.5: Darstellung von Standorten aus einer Ortungs-DB (links) bzw. verbundenen WLAN-APs (rechts) bei Oxygen. Quelle: [For16], Kartenmaterial © Google 2016.

Noch vor der Etablierung der Mobilfunkforensik als eigenständigem Teilgebiet der IT-Forensik war die russische Firma Oxygen bereits darauf spezialisiert, Daten aus Mobiltelefonen zu extrahieren. Neben der reinen Speicherung persönlicher Informationen (Kontakte, SMS, Kalenderinformationen etc.) verschob sich der Fokus der Software mit der Zeit immer mehr in Richtung vernetzter Darstellung hin zum aggregierten Gesamtbild aller Nutzerdaten.

Bei der Verarbeitung von Standortinformationen verfolgt Oxygen ebenfalls einen kombinierten Ansatz. Um die größtmögliche Datenmenge zu generieren, werden Ortungsdaten aus unterschiedlichen Quellen kombiniert. Wie in den Screenshots in Abb. 2.5 dargestellt, lassen sich über den Menüpunkt »Web Connections and Location Services« Positionsdaten aus Ortungsdatenbanken, auf Basis ehemals verbundener WLAN-AccessPoints sowie weiterer Datenquellen ermitteln (vgl. [For16]). Erwähnenswert ist auch die Exportfunktion eines forensischen Berichtes bzgl. der Ortungsdaten (siehe Abb. 2.6 auf der nächsten Seite). Während andere kommerzielle Anwendungen häufig die rein tabellarische Ansicht wählen, werden bei Oxygen die Positionsdaten auf einer Karte mit zusätzlichen textlichen Informationen dargestellt.

Im Ergebnis lässt sich festhalten, dass die Softwarelösung der Firma Oxygen mittlerweile zu den Marktführern im Bereich Mobilfunkforensik aufgeschlossen hat. Was die Verarbeitung von Geoinformationen betrifft, so liegt die Stärke der Oxygen Forensic Suite in der Kombination unterschiedlicher Standortdaten und der anschaulichen Darstellung nebst Berichterstellung für den Ermittler.

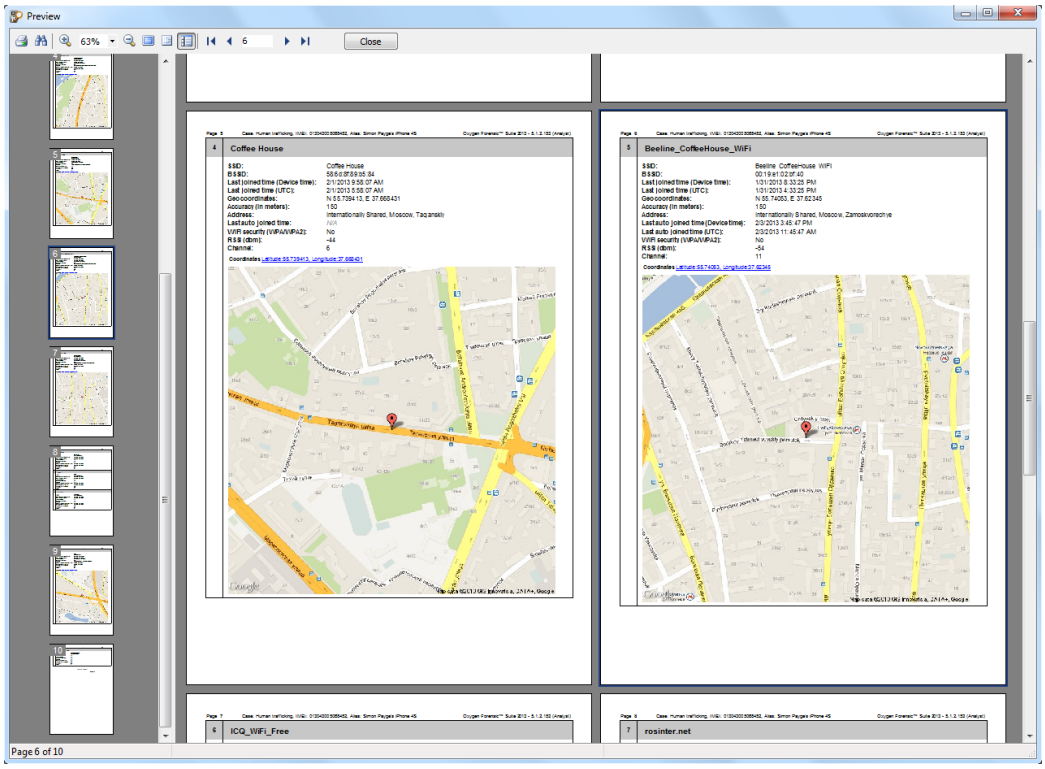


Abb. 2.6: Generierter Bericht zu Ortungsdaten aus Oxygen Forensic Detective. Quelle: [For16], Kartenmaterial © Google 2016.

2.2.4 Micro Systemation XRY

Der schwedische Hersteller Micro Systemation AB (seit 2015 kurz MSAB) gilt neben Cellebrite als einer der zwei führenden Anbieter kommerzieller Lösungen im Bereich der Mobilfunkforensik. Die Abkürzung AB im Namen steht für die schwedische Bezeichnung »aktiebolag«, zu deutsch: Aktiengesellschaft.

Über eine Hardwarelösung (siehe Abb. 2.8 auf der nächsten Seite) zum Anschluss an den PC können Telefone, Speicherkaten und SIM-Karten angeschlossen und mitunter parallel ausgelesen werden.

Im Rahmen dieser Arbeit wurden u.a. die folgenden Geräte untersucht:

- ein aktuelles Sony Xperia Z3 LTE-A D6603 mit Android 6.0 und
- ein älteres Samsung Galaxy S3 mit Android in der Version 2.3.

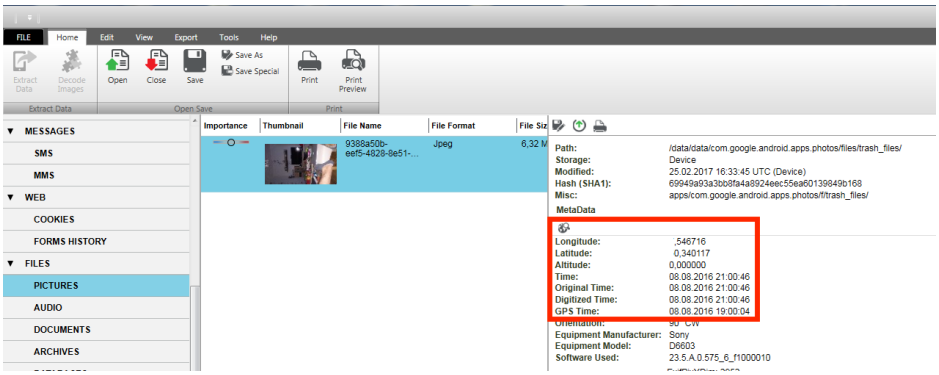


Abb. 2.7: Screenshot: MSAB XRY v7.3. Anzeige von Ortungsdaten aus Metainformationen von Bildern in Textform. Quelle: Eigene Darstellung.

Ortungsdaten können hierbei theoretisch aus Systemdienstdateien aber auch Metainformationen von Multimediadaten sowie Konfigurationsdateien ermittelt werden; nicht so bei den untersuchten Smartphones. Dies liegt zum einen daran, dass entsprechende Systemdaten nur bis Android 2.3 auf den Geräten gespeichert werden und selbst dann muss die Option zur Nutzung von Drahtlosnetzwerken für die Lokalisierung explizit aktiviert werden (vgl. Abschnitt 4.2.1 auf Seite 110). Hier bleibt dem Ermittler nur, wie in Abb. 2.7 zu sehen, die Auswertung von Geoinformationen auf Basis von Exif-Daten aus Bilddateien.

Abb. 2.8: MSAB XRY: Hardware-Kit zur Datensicherung. Quelle: [Tar12]

Zusammenfassend sind die Ergebnisse der Software von MSAB in Bezug auf die Extraktion und Analyse von Ortungsdaten aus Android-Geräten ernüchternd. Obwohl vorhanden und während der Extraktion explizit ausgewiesen, konnten keine Geoinformationen auf Basis von Standortdateien unter Android gewonnen werden. Die ermittelten Geoinformationen werden lediglich als Längen- und Breitengradangaben in Textform im forensischen Bericht wiedergegeben und nicht, wie bei Oxygen Forensics, auf einer Karte dargestellt.

2.2.5 Cellebrite UFED / Physical Analyzer

Das forensische Produktportfolio der aus Israel stammenden Firma Cellebrite ist sehr umfangreich. Die Produktpalette ist abgestimmt auf den voraussichtlichen Einsatzort und die technischen Fähigkeiten der Ermittler. Hierbei variieren die Bedienung aber auch die forensischen Extraktionsmöglichkeiten von möglichst einfach benutzbar (zur schnellen Gewinnung der gängigsten Artefakte) bis hin zur Rekonstruktion physischer Datenabbilder zerstörter oder gesperrter Geräte im Labor. Einen guten Überblick hierzu liefert die aktuellen Produktbroschüre auf der Internetseite von Cellebrite [Cel17].

Abb. 2.9: Cellebrites Universal-Forensic-Extraction-Device in der mobilen Ausführung, kurz UFED-touch mit über 100 Adapterkabel und angeschlossenem iPhone 4GSM. Quelle: Eigene Aufnahme 2011.

Ortungsdaten können beim Physical Analyzer aus den verschiedensten Quellen aus iOS- und Android-Daten gewonnen werden. Die meisten Positionsangaben lassen sich bei den durchgeführten Untersuchungen am eigenen iPhone wieder im Bereich der Mediadaten ermitteln, gefolgt von Standorten aus Emails, der verbundenen WLAN-Netze, Erinnerungen, eMails bzw. weiteren Apps.

Nachfolgend ist exemplarisch die Anzahl der Häufigkeiten von Ortungsdaten eines über Jahre genutzten iPhones aufgeführt:

- Media (4696)
- Mail Content (100)
- Wireless Networks (63)
- Apple Maps (58)
- Erinnerungen (9)
- Threema (2)

Abb. 2.10 zeigt die Software Cellebrite Physical Analyzer in der Version 4.2.1.7. In der Kartenansicht ist eine Vielzahl an Positionen dargestellt. Teilweise kommen die Standorte mehrfach vor, zu sehen an den Zahlen in den Beschriftungslabels. Rechts unten im Screenshot ist ein mit dem iPhone aufgenommenes Bild zu sehen. Direkt darüber sind die Positionsdaten der Aufnahme angegeben.

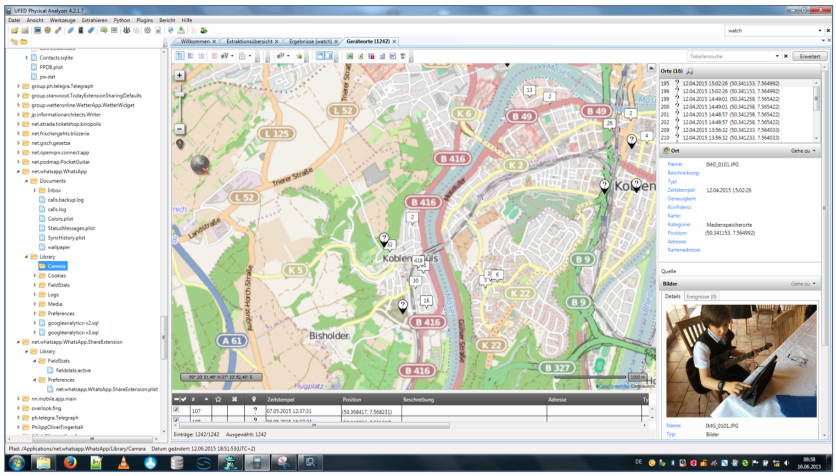


Abb. 2.10: Cellebrite Physical Analyzer v.4.2.1.7: Darstellung von Ortungsdaten aus Multimediadateien inklusive Darstellung auf einer Karte. Quelle: Eigene Darstellung. Kartenmaterial: © OpenStreetMap Mitwirkende 2015.

Mithilfe von Google Maps lässt sich anhand der Koordinate »50.341153,7.564992« die vermeintliche Position des Aufnahmeortes ermitteln. In Abb. 2.11 (unten) ist die Fehlerabweichung des aGPS-Standortes rechts (»iPhone«) zum tatsächlichen Aufnahmeort des Bildes links (»Photo«) dargestellt (vgl. Abb. 2.11). Die Distanz zwischen dem angenommenen und dem tatsächlichen Aufnahmeort beträgt in dem Versuch mehr als 1km.

Abb. 2.11: Die Abweichung des Aufnahmeortes (links: »Photo«) zur vermeintlichen Geräteposition (rechts: »iPhone«) kann hierbei mitunter beträchtlich sein. Quelle: Google Maps (Maßstab auf der Karte unten rechts). Kartenmaterial: © Google 2017.

Die Abweichung wird dadurch erklärbar, dass das Bild im Inneren eines alten Winzergebäudes mit dicken Außenwänden (und somit bestens gegen GPS-Signalen abgeschirmt) erstellt wurde (vgl. Abb. 2.10 auf der vorherigen Seite). Zudem spielt das Aufnahmedatum eine Rolle. Damals, im Jahr 2013, waren die Sensoren im iPhone und die Standortdatenbank von Apple noch nicht optimiert bzw. hinreichend befüllt.

Unter idealen Bedingungen, das heißt außerhalb von Gebäuden mit freiem Blick zum Himmel und nach einigen Bildaufnahmen bzw. Ortungsaktivitäten, sieht die Situation besser aus. Abb. 2.12 auf der nächsten Seite zeigt eine Aufnahme aus dem Jahr 2015 (wieder im Physical Analyzer, diesmal Version 5.4.7.5). Der Abstand zum tatsächlichen Aufnahmeort beträgt nur noch wenige Meter.

Bezogen auf den Fokus dieser Arbeit ist von besonderer Bedeutung, dass vom Physical Analyzer keine Standortdaten aus Apples Ortungsdatenbanken mehr ermittelt werden, obwohl der Firma die Forschungsergebnisse und Tools dieser Arbeit zugänglich gemacht worden sind.

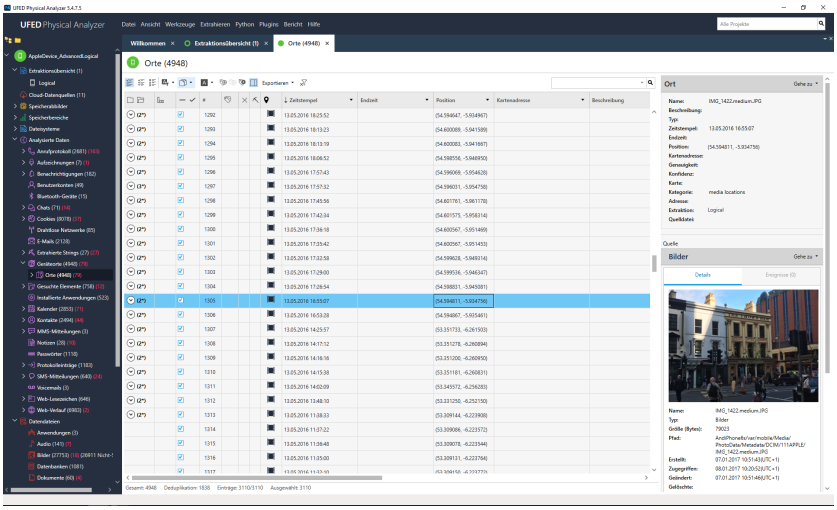
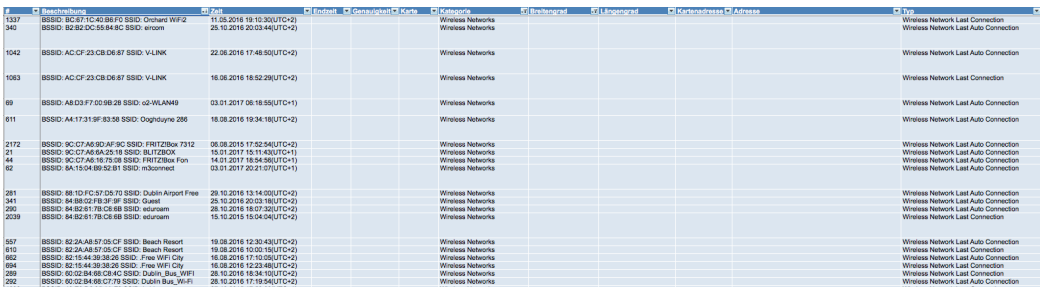


Abb. 2.12: Auswertung eigener Aufnahmen unter günstigen Bedingungen im Freien mithilfe des Physical Analyzers v.5.4.7.5. Die Abweichung beträgt i.d.R. wenige Meter. Eine Angabe hierzu fehlt jedoch bei Cellebrite. Quelle: Eigene Darstellung.

Bei den Ortungsdaten aus Emails ist generell unklar, welchem Kontext die Daten zuzuordnen sind. Darüber hinaus dürften Geoinformationen in ortsabhängigen Erinnerungen ebenfalls willkürlich durch den Benutzer angelegt worden sein.

Im Standortbericht von Cellebrite befinden sich mitunter auch Datensätze ohne Geoinformationen. Wie in Abb. 2.13 zu erkennen, fehlen dort die Standortdaten zu WLAN-Funksendern. Dies liegt daran, dass vor der Berichtgenerierung auf die Möglichkeit verzichtet wurde, fehlende Ortsinformationen über externe Quellen zu erheben. Solche künstlich generierten Informationen sind generell mit Vorsicht zu genießen, wie in Abschnitt 2.2.6 auf der nächsten Seite ausgeführt wird.



#	Beschreibung	Zeit	Endzeit	Genauigkeit	Karte	Kategorie	Breitengrad	Längengrad	Kartenadresse	Adresse	Typ
1337	BSSID: BC:67:1C:40:B6:F0 SSID: Orchard WiFi2	11.05.2016 19:10:30(UTC+2)				Wireless Networks					Wireless Network Last Connection
340	BSSID: B2:B2:DC:55:84:8C SSID: ercom	25.10.2016 20:03:44(UTC+2)				Wireless Networks					Wireless Network Last Auto Connection
1042	BSSID: AC:CF:23:CB:D6:87 SSID: V-LINK	22.06.2016 17:48:50(UTC+2)				Wireless Networks					Wireless Network Last Auto Connection
1063	BSSID: AC:CF:23:CB:D6:87 SSID: V-LINK	16.06.2016 18:52:29(UTC+2)				Wireless Networks					Wireless Network Last Connection
69	BSSID: A8:D3:F7:00:9B:28 SSID: o2-WLAN49	03.01.2017 06:18:55(UTC+1)				Wireless Networks					Wireless Network Last Auto Connection
611	BSSID: A4:17:31:9F:83:58 SSID: Ooghduyne 286	18.08.2016 19:34:18(UTC+2)				Wireless Networks					Wireless Network Last Auto Connection
2172	BSSID: 9C:C7:A6:9D:AF:9C SSID: FRITZ!Box 7312	06.08.2015 17:52:54(UTC+2)				Wireless Networks					Wireless Network Last Auto Connection
21	BSSID: 9C:C7:A6:9A:25:18 SSID: BLITZBOX	15.01.2017 15:11:43(UTC+1)				Wireless Networks					Wireless Network Last Auto Connection
44	BSSID: 9C:C7:A6:16:75:08 SSID: FRITZ!Box Fon	14.01.2017 18:54:56(UTC+1)				Wireless Networks					Wireless Network Last Auto Connection
62	BSSID: 8A:15:04:89:52:81 SSID: m3connect	03.01.2017 20:21:07(UTC+1)				Wireless Networks					Wireless Network Last Auto Connection
281	BSSID: 88:1D:FC:57:D5:70 SSID: Dublin Airport Free	29.10.2016 13:14:00(UTC+2)				Wireless Networks					Wireless Network Last Auto Connection
341	BSSID: 84:B8:02:FB:3F:9F SSID: Guest	25.10.2016 20:03:18(UTC+2)				Wireless Networks					Wireless Network Last Auto Connection
290	BSSID: 84:B2:61:78:C6:6B SSID: eduroam	28.10.2016 18:07:32(UTC+2)				Wireless Networks					Wireless Network Last Auto Connection
2039	BSSID: 84:B2:61:78:C6:6B SSID: eduroam	15.10.2015 15:04:04(UTC+2)				Wireless Networks					Wireless Network Last Connection
557	BSSID: 82:2A:A8:57:05:CF SSID: Beach Resort	19.08.2016 12:30:43(UTC+2)				Wireless Networks					Wireless Network Last Auto Connection
610	BSSID: 82:2A:A8:57:05:CF SSID: Beach Resort	19.08.2016 10:03:15(UTC+2)				Wireless Networks					Wireless Network Last Connection
662	BSSID: 82:15:44:39:38:26 SSID: .Free WiFi City	16.08.2016 17:10:05(UTC+2)				Wireless Networks					Wireless Network Last Auto Connection
694	BSSID: 82:15:44:39:38:26 SSID: .Free WiFi City	16.08.2016 12:23:48(UTC+2)				Wireless Networks					Wireless Network Last Connection
289	BSSID: 60:02:B4:68:C8:4C SSID: Dublin_Bus_WIFI	28.10.2016 18:34:10(UTC+2)				Wireless Networks					Wireless Network Last Connection
292	BSSID: 60:02:B4:68:C7:79 SSID: Dublin Bus_Wi-Fi	28.10.2016 17:19:54(UTC+2)				Wireless Networks					Wireless Network Last Auto Connection

Abb. 2.13: Weiteres Problem bei Cellebrite: Geodaten von WLAN-MAC-Adressen werden anhand von Drittanbieterdatenbanken ermittelt. Ohne Online-Zugriff auf diese fehlen die Standortdaten bei der Ausgabe im Bericht. Quelle: Eigene Darstellung.

Zusammenfassend ist die Darstellung von Ortungsdaten im Physical Analyzer durch die Visualisierung der extrahierten Standorte auf einer Karte anschaulicher als in Textform, welche ebenfalls möglich ist. Wie die übrigen Tools bietet auch die Software von Cellebrite keine Hinweise auf die Fehlerrate der dargestellten Standortdaten. Dass die Abweichung von Aufnahmeort zur angegebenen Position in den Metadaten von Bildern mitunter beträchtlich sein kann, zeigt Abb. 2.11 auf Seite 49.

2.2.6 Öffentliche Funknetz-Datenbanken

Neben Apple und Google sind weitere Diensteanbieter an Standortdaten zu Funksendern interessiert. Webseiten wie OpenCellID [Ena16] laden dazu ein, die über entsprechende Smartphone-Apps gesammelten Daten mit anderen Nutzern zu teilen. Abb. 2.14 zeigt einen Kartenausschnitt des Anbieters OpenCellID mit Mobilfunksendern in Koblenz. Zusätzlich sind die Standorte der mitteilenden Nutzer (rosa Farbpunkte) zur T-Mobile Funkzelle 10543 dargestellt.

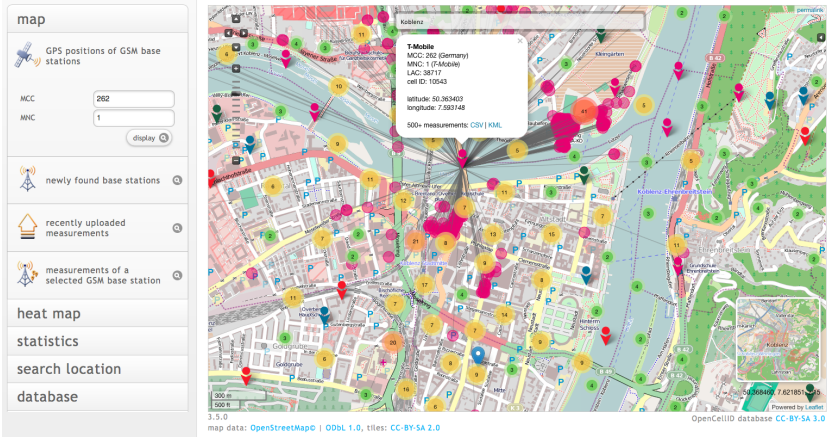


Abb. 2.14: Crowd-Sourced Funkzellenvermessung am Beispiel des Anbieters OpenCellID [Ena16]. Quelle: Eigene Darstellung. Kartenmaterial: © OpenStreetMap Mitwirkende 2016.

Ähnliche Projekte existieren auch für WLAN-Funknetze. Der bekannteste Diensteanbieter betreibt die Webseite wigle.net ([bau17]) mit Standortinformationen zu WLAN-MAC-Adressen. Die Genauigkeit der Daten schwankt von Anbieter zu Anbieter, ist aber mitunter sehr hoch. So wird z. B. der WLAN-Access-Point mit der BSSID: 00:1F:7D:B0:1C:83 bzw. der SSID: »Hotel Grebel« unmittelbar vor

dem gleichnamigen Hotel dargestellt (siehe Abb. 2.15 links, rote Markierung). Beim nächsten Anbieter ([Myl17]) wird der WLAN-AccessPoint hingegen 50m vom tatsächlichen Standort entfernt angezeigt (siehe Abb. 2.15 rechts).

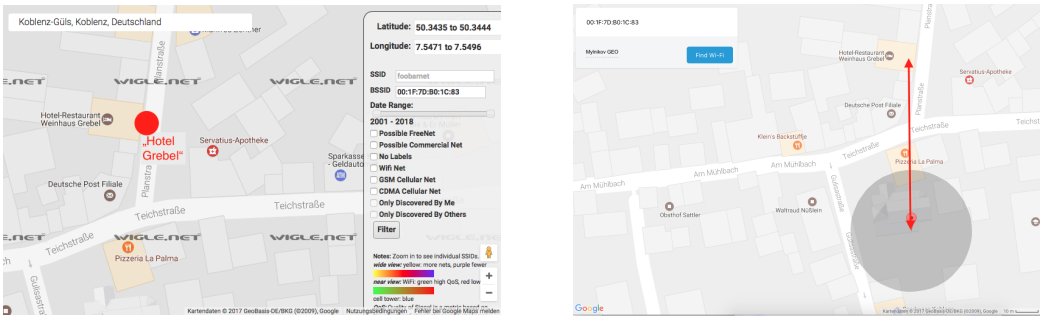


Abb. 2.15: Verortung der WLAN-BSSID 00:1F:7D:B0:1C:83 am Beispiel der Anbieter wigle.net [bau17] (links) und mylnikov [Myl17] (rechts). Kartenmaterial © Google 2017.

Mit den im Rahmen dieser Arbeit durchgeführten Untersuchungen und durch die Verwendung nativer Apps ist es möglich gewesen, die Verlässlichkeit und Genauigkeit von Geodaten der zuvor dargestellten Funknetzdatenbanken zu beurteilen. Ohne die Vorteile der Standortbestimmung anhand von Funksendern zu diskreten Standorten inkl. Fehlerabschätzung zu schmälern, ist festzuhalten, dass die Qualität der Ortsangaben im Zweifelsfall durch eigene Messungen vor Ort zu verifizieren ist. Ein solches Vorgehen ist bei Ermittlungen auf Basis von Funksendern im Bereich der Mobilfunkforensik ohnehin üblich.

Die theoretisch maximale Abweichung verschiedener Funksender wird später im Abschnitt Genauigkeitskompass ab Seite 144 weiter ausgeführt.

2.3 Zusammenfassung

Die in diesem Abschnitt vorgestellten Produkte und Lösungen verschiedener Entwickler und Hersteller sind allesamt mehr oder weniger gut dazu geeignet, Standortinformationen aus Smartphones zu verarbeiten bzw. zu visualisieren. Allerdings trifft die Aussage »Je teurer desto besser« nicht auf die Darstellung von Standortdaten im Allgemeinen zu. Jede Software hat, wie in Tab. 2.1 auf der nächsten Seite dargestellt, ihre unterschiedlichen Stärken und Schwächen.

Anwendung	Stärken	Schwächen
iPhoneTracker	erste Software zur Visualisierung von Ortungsdaten aus iOS kostenlos und Open-Source	Rasterung der Daten Umständliche Bedienung stark eingeschränkter Funktionsumfang keine Exportfunktionen keine Fehlerabschätzung
MyPhoneTracker	erste Software zur Visualisierung von Ortungsdaten aus Android kostenlos keine Rasterung der Standorte	stark eingeschränkter Funktionsumfang keine Exportfunktionen keine Fehlerabschätzung
ADEL	Fehlerabschätzung in Form von Radien um die Standorte	erste Ansätze der Betrachtung der Entstehung von Geodaten
Oxygen Forensic Suite	gute Darstellung von Standortdaten in den exportierten Berichten	teuer in der Anschaffung keine Fehlerabschätzung
Microsystemation Xry	forensische, oftmals physische, Datenextraktion aus mobilen Endgeräten	sehr teuer in der Anschaffung keine Visualisierung von Standortdaten auf einer Karte keine Fehlerabschätzung
Cellebrite Physical Analyzer	forensische, oftmals physische, Datenextraktion aus mobilen Endgeräten	sehr teuer in der Anschaffung keine Fehlerabschätzung
Online Funknetzdatenbanken	einfach zugänglich	keine Fehlerabschätzung

Tab. 2.1: Vergleich verschiedener Anwendungen zur Verarbeitung von Geodaten aus mobilen Endgeräten mit Fokus auf die Stärken und Schwächen des jeweiligen Tools.

Insgesamt verfügt nur ein einziges der im Rahmen dieser Arbeit getesteten Tools über die Funktion, Abweichungen von Geoinformationen auszugeben. Darüber hinaus sind die generierten Berichte oftmals nicht dazu geeignet, ohne weitere Bewertung von Experten, vor Gericht präsentiert zu werden.

Im Rahmen dieser Arbeit wurde dementgegen versucht, diese Probleme durch die Desktopanwendungen iPhoneTrackerLE und GoogleTracker zu lösen. So ist es insbesondere bei der Berichterstellung möglich, zu jedem ausgewählten Standort die Fehlerabschätzung mit anzugeben. Zusätzlich wird zu den Positionsdaten in jedem Fall auch eine Kartenansicht zur besseren Visualisierung sowie weitere forensisch relevante Informationen für jeden Standort auf jeweils einer gedruckten Seite ausgegeben. Mithilfe der Notizfunktion innerhalb der Software und durch den Export des Berichtes als Word-Dokument ist der Ermittler ferner in der Lage, fehlende Informationen für die spätere Würdigung vor Gericht unkompliziert zu ergänzen.

Darüber hinaus wird deutlich, dass in den meisten Werken zum Thema Geodaten in der Forensik keine hinreichende Absicherung der Untersuchungen durchgeführt wird. Die Autoren der nicht-wissenschaftlich geprägten Arbeiten legen den Fokus lediglich auf die Erhebung der GPS-Koordinaten. Ohne Angabe zur Entstehung bzw. dem Ursprung der Daten werden diese unreflektiert wiedergegeben. Die Forscher der FH Aachen liefern in ihrem Paper zwar eine Abschätzung der zu erwartenden Genauigkeit von Geodaten unterschiedlicher Verortungsmethoden, wenden diese Erkenntnis aber letztlich nicht auf die ermittelten Standortdaten aus mobilen Endgeräten an. Lediglich in der Arbeit von M. Spreitzenbarth von der Universität Erlangen wird die Fehlertoleranz von Standortinformationen dann erstmals grafisch dargestellt.

Ziel dieser Arbeit ist es, Standortdaten möglichst allgemein zu betrachten und auf Basis des Datenursprungs entsprechend reflektiert inkl. Angabe einer möglichen Standortabweichung wiederzugeben. Hierzu ermöglichen z. B. die entwickelten Desktopanwendungen bei der forensischen Auswertung von Standortdaten die Unterscheidung hinsichtlich des Ursprungs der Daten durch entsprechende Angaben in der Zeitstrahlübersicht. Darüber hinaus wird die Qualitätsbewertung anhand der Entstehung von Geolokalisierungsdaten und mithilfe nativer Anwendungen für iOS und Android durchgeführt. Die bei dieser Analyse und Interpretation von Standortdaten gewonnenen wissenschaftlichen Erkenntnisse werden dann induktiv in ein universelles Modell zu Standortdaten aus mobilen Endgeräten überführt (vgl. Abschnitt 5.5.2 auf Seite 143).

Teil 3

Forschungsmethodik

Zu Beginn der Untersuchungen im Rahmen dieser Arbeit 2011/2012 existierten noch keine brauchbaren Lösungen zur Verarbeitung von Standortdaten in der Mobilfunkforensik. Um hier zeitnah Abhilfe zu schaffen galt es eine Methode zu finden, die es erlaubt schnell einsetzbare Werkzeuge zu entwickeln.

Die Vorgehensweise nach der Design Science Research Methode (DSRM) bietet hierzu einen zweckmäßig orientierten Ansatz für die Forschung, um Softwareentwicklung inkrementell durchzuführen. Die in Abb. 3.1 skizzierte Methodik ist so auch für die zeitnahe Lösung von Problemen innerhalb der Polizei geeignet. Insbesondere die Rückkopplung während der Evaluierungsphase, etwa durch Anwendung im Rahmen der polizeilichen Praxis und der damit einhergehenden Möglichkeit das Design für die anstehende Implementierung anzupassen, erzeugt einen wichtigen Mehrwert für die die Entwicklung im Allgemeinen.

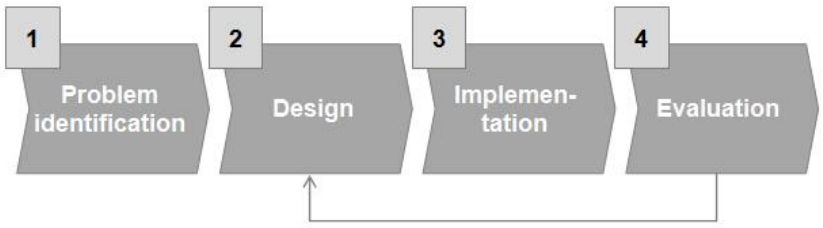


Abb. 3.1: Übersicht zur Design Science Research Methode. Quelle: [BV11].

Zusätzlich unterstützt DSRM das induktive Vorgehen bei der Erforschung unklarer Sachverhalte. So werden im Rahmen dieser Arbeit mithilfe selbst entwickel-

ter Apps für Apple iOS und Google Android gezielt Messungen zur Verortung von Smartphones durchgeführt und so unter nachvollziehbaren Begebenheiten Standortdaten erhoben. Die iOS-Apps zeichnen hierbei nach dem Aktivieren des Ortungsdienstes innerhalb der App die während der Verortung entstehenden Standortdaten auf. Diese lassen sich während oder nach Abschluss der Messung entweder direkt innerhalb der App betrachten oder retrograd mit den Daten der Ortungsdatenbank von Apple korrelieren (vgl. Abb. 3.3 auf Seite 62). Die hierbei gewonnenen Erkenntnisse ermöglichen später in Teil 5 ab Seite 131 die Klärung vieler der offenen Fragen rund um die Geolokalisierung auf Smartphones.

Bevor der konkrete Bezug zur Thematik der Arbeit hergestellt wird, soll zunächst aber noch die Forschungsmethode detailliert vorgestellt werden. An dieser Stelle ist anzumerken, dass auch andere Forschungsmethoden, z. B. solche mit deduktiven oder eher hypothetischen Ansätzen in Betracht gezogen wurden. Aufgrund der hohen Relevanz der Arbeit für die polizeiliche Praxis sowie der Notwendigkeit zur schnellen Verfügbarkeit von Werkzeugen und Ergebnissen wurde schlussendlich die Forschungsmethode nach DSRM gewählt.

3.1 Design Science Research Method

Wie Ken Pfeffers und seine Kollegen in [PRK12] ab Seite 32ff. ausführen, besteht DSRM massgeblich darin, mögliche Lösungsansätze zu finden, die als Artefakt der Phase Design&Entwicklung im Rahmen einer Demonstration während der Phase Evaluation bewertet werden. Ergänzend zur Abb. 3.1 auf der vorherigen Seite werden zwei weitere Phasen ergänzt, um den akademischen Maximen der Motivation sowie der Veröffentlichung nachzukommen. Ebenso lassen sich, wie in Abb. 3.2 auf der nächsten Seite dargestellt, mögliche Einstiegspunkte für die Wissenschaft ergänzen. Im Folgenden werden die einzelnen Phasen der Abb. 3.2 auf der nächsten Seite und die zu erkennenden Abweichungen zu Abb. 3.1 auf der vorherigen Seite weiter ausgeführt.

Die Start- und Endprozesse »Problemidentifikation« und »Evaluation« aus Abb.3.1 bleiben erhalten. Hinzugefügt werden die Prozesse »Lösungsansatz«, »Demonstration« sowie »Kommunikation« Dafür werden die Einzelprozesse »Design« und »Implementierung« in einem Prozess (»Design & Entwicklung«)

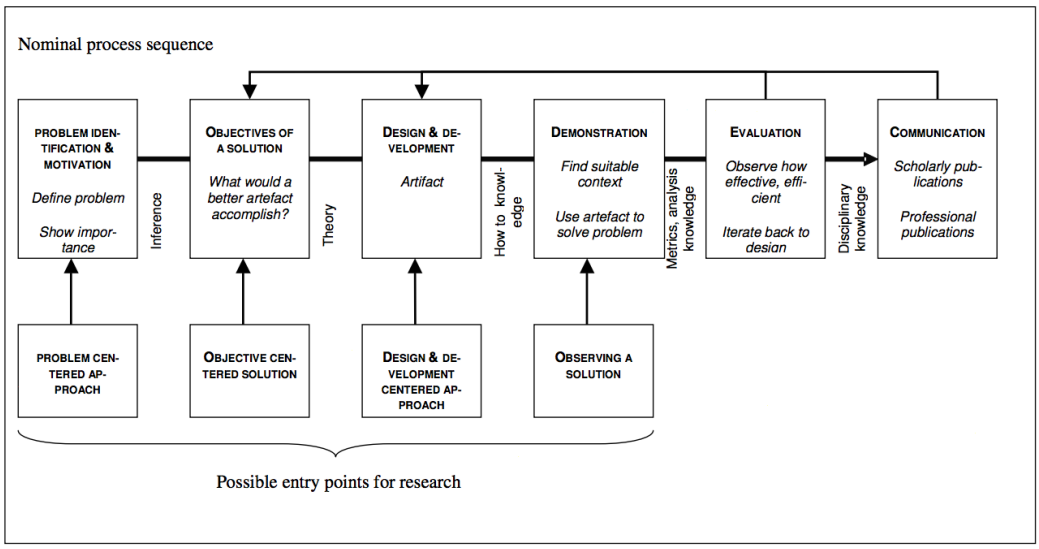


Abb. 3.2: Detaillierter Prozessablauf der DSRM mit möglichen Einstiegspunkten für die Wissenschaft. Quelle: [PTG+06]. Konkreter Bezug zur Arbeit im Text.

zusammengefasst. So verschiebt sich der Fokus von der Implementierung in Richtung Reflexion auf Basis einer Schlussfolgerung für die Grundproblematik (»Lösungsansatz«) über die »Demonstration« im Kontext der Kernproblematik hin zur abschließenden Veröffentlichung, sprich dem Diskurs innerhalb der jeweiligen Domäne. Zudem bleibt das Paradigma von durch Rückkopplung der Prozesse »Evaluation« bzw. »Kommunikation« mit dem »Lösungsansatz« bzw. dem Prozess »Design & Entwicklung« konstruktiv iterativ (vgl. [VK15]).

Neben der akademisch-theoretischen Herangehensweise durch wissenschaftliche Forschungsmethoden werden bei DSRM zusätzlich weitere Anforderungen aus der Praxis berücksichtigt. Die grundlegende Idee von DSRM wird ohnehin in der Praxis häufig intuitiv angewandt. Viele der Elemente von DSRM lassen sich auch in anderen agilen Softwareentwicklungsmethoden, wie z. B. SCRUM finden. Ferner spielen nach Meinung von Pfeffer et. al. insbesondere die Modularität basierend auf definierten Programmierschnittstellen (Application Programming Interface (API)s) und die Anwendung sogenannter Entwurfsmuster (»design pattern«) eine bedeutende Rolle (vgl. [PRK12]).

Im Folgenden werden die einzelnen Phasen der Methode mit Fokus auf die forensische Auswertung und Präsentation von Geolokalisierungsdaten in der Mobilfunkforensik beschrieben.

3.2 Problemidentifikation und Motivation

Die Extraktion, Verarbeitung bzw. Auswertung von Standortdaten bildet eine der wesentlichen Grundlagen für kriminalpolizeiliche Ermittlungen. Zu Beginn der Untersuchung von Geodaten sind die forensischen Tools und somit auch Ermittler darauf beschränkt, Exif-Daten aus Bildern zum fraglichen Zeitpunkt zu bewerten. Mit der Veröffentlichung von Allen und Warden zum Thema Speicherung von Standortdaten in Systemdateien ändert sich hier die potentielle Beweislage.

Aufgrund der Menge an gespeicherten Standortdaten erwächst zunächst die Hoffnung, ein lückenloses Bewegungsprofil des Nutzers zu erhalten. Schnell wird jedoch klar, dass die im iPhoneTracker dargestellten Geokoordinaten aus Ortungsdatenbanken von Apple viele Fragen aufwerfen:

- Was bedeuten die unterschiedlichen Punktgrößen / -farben?
- Warum existieren nicht zu jedem Datum Geoinformationen?
- Wieso werden die Daten bei starkem Zoom gerastert dargestellt?

Grundsätzlich fehlt dem Ansatz von Allen und Warden das tiefere Verständnis zur Entstehung der Daten sowie die forensische Darstellung. Andere Entwickler, wie der Franzose Paul Courbis, berichten ebenfalls zum Thema. In seinem blog [Cou10] geht Courbis auf die »Indiskretion« von Apple-Geräten im Hinblick auf datenschutzrechtliche Aspekte ein. In der forensischen Literatur wird das Problemfeld allenfalls oberflächlich betrachtet. Wie bereits in Abschnitt 2.1.1 auf Seite 36 und Abschnitt 2.1.2 auf Seite 37 ausführlich beschrieben, gehen Zdziarski und Hoog lediglich auf die Existenz der Ortungsdatenbank consolidated.db ein, nicht aber auf die Auswertung der Daten selbst.

Mithilfe dieser Arbeit sollen diese Probleme gelöst werden. So gilt es neben der Betrachtung von Standortdaten unter forensischen Gesichtspunkten forensische Tools für den praktischen Einsatz zu entwickeln. Daneben soll auf Basis nativer Anwendungen und Live-Untersuchungen der Ortungsdienste auf Smartphones ein Verständnis für die Lokalisierung mobiler Systeme geschaffen werden.

3.3 Mögliche Lösungsansätze

Zur Beantwortung der durch den iPhoneTracker aufgeworfenen Fragen (siehe oben) muss der Quellcode der Software untersucht werden. Anschließend gilt es, die Quelldaten genauer zu analysieren. Mittels deduktiver Vorgehensweise (Quellcodestudium) sollte es möglich sein, die vorliegenden Datenbestände auf besondere Merkmale hin zu untersuchen. Nachdem dann geklärt ist, ob die Daten lückenlos verarbeitet wurden, soll der Frage nachgegangen werden, ob weitere Informationen eine Präzisierung hinsichtlich Zeit und Ort bzw. Entstehung der Daten ermöglichen.

Abschließend soll in möglichst vielen praktischen Tests das Verhalten und die Genauigkeit der Ortungsdienste auf verschiedenen Endgeräten mit unterschiedlichen Betriebssystemversionen nachgestellt werden. Hierzu bieten sich native Smartphone-Applikationen an. Denn nur so lässt sich der Ortungsprozess ohne weitere Hilfsmittel live auf dem Gerät mitverfolgen.

3.4 Design & Entwicklung

Für die Phase der Konzeptionierung und Implementierung der verschiedenen Tools und Anwendungen liegt der Fokus der Arbeit weniger auf der Verwendung einschlägiger Entwurfsmuster der Informatik als vielmehr den besonderen Erfordernissen der forensischen Arbeit, damit die erhobenen bzw. später dargestellten Daten auch einem Gerichtsverfahren standhalten.

In der IT-Forensik wird nach dem S-A-P-Stufenprinzip verfahren (siehe Geschonneck in Computer Forensik [Ges16]).

1. S-ichern
2. A-nalysieren
3. P-räsentieren

Diese Vorgehensweise muss demnach auch für die forensische Untersuchung und Auswertung von Ortungsdaten aus Mobiltelefonen beachtet werden. Das S-A-P-Stufenmodell stellt an die Phase Design und Entwicklung der DSRM eini-

ge Anforderungen, die nun im Folgenden betrachtet und hinsichtlich ihrer Relevanz für die Umsetzung im Rahmen dieser Arbeit zu bewerten sind.

S-ichern

Die Extraktion der Daten vom Gerät ist nicht Gegenstand dieser Arbeit sein. Dafür sind die notwendigen Schritte (vgl. Abschnitt 1.2.2 auf Seite 18) zu komplex und je nach Gerät zu unterschiedlich. Es wird aber davon ausgegangen, dass bei der Sicherstellung des Smartphones alle bekannten Maßnahmen zur Vermeidung von Datenmanipulationen berücksichtigt werden (z.B. Aktivieren des sog. Flugmodus).

Für die Durchführung der bereits angesprochenen eigenen Messungen ist es ebenfalls notwendig, daß die Daten vor der Extraktion eingefroren werden bzw. ohne größere Umstände vom Gerät extrahiert werden können, denn nur so lassen sich Datenverluste durch automatisierte Löschroutinen der mobilen Betriebssysteme verhindern.

A-nalysieren

Das Hauptaugenmerk dieser Arbeit liegt in der Erforschung und Analyse der Datenbasis von Ortungsdiensten. Hierzu ist es unabdingbar, die Datenstrukturen genau zu untersuchen, um so die Analyse der Inhalte abzusichern.

Im Zusammenhang mit den SQLite3-Datenbanken auf Apple-iOS-Geräten ist die Analyse leicht zu bewerkstelligen. Zum einen existieren Tools zum Betrachten von SQLite3-Datenbanken (Firefox SQLiteManager, SQLiteBrowser2003, SQLiteSpy, etc.) bzw. Bibliotheken für alle gängigen Programmiersprachen zur Verarbeitung der Inhalte von Datenbanken. Nicht zuletzt lassen sich SQLite3-Datenbanken über ein vorkompiliertes Kommandozeilentool auf allen gängigen Betriebssystemen öffnen (herunterzuladen unter `https://www.sqlite.org/download.html`).

Die Auswertung der Daten von Android-Geräten ist komplizierter. Aber auch hier lassen sich durch das Quellenstudium bzw. frei verfügbare Tools und Skripte Aussagen zur Vollständigkeit bzw. Interpretation der Daten geben. So lieferte z.B. Magnus Eriksson 2011 auf seinem github-Account eine erste Beschreibung der Struktur der Daten (vgl. [Eri11b]).

Hier bietet es sich an, spezielle Applikationen zur konkreten Untersuchung und Aufbereitung der jeweiligen Datenquellen zu entwickeln.

P-räsentieren

Für die abschließende Berichterstellung gilt es dann, die verfahrensrelevanten Daten leicht verständlich und zweifelsfrei nachvollziehbar darzustellen. Die Reduktion der Standorte auf die für die polizeilichen Ermittlungen relevanten Informationen ist hierbei ebenso wichtig, wie Erklärungen sowie eine lückenlose Darstellung der zeitlichen Zusammenhänge. Neben all den technischen Informationen muss die Präsentation aber auch anschaulich umgesetzt werden. Eine Kartendarstellung mit individuellem Ausschnitt ist hierfür ebenso unabdingbar wie die Ausgabe in druckbarer Form für die Aktenführung.

3.5 Demonstratoren

Nach dem Aufbau des Wissens um Ortungstechniken müssen in der DSRM die Datenbestände zur Demonstration im Kontext der Systemumgebung betrachtet werden. Hierbei ist die Kartendarstellung von Standortdaten zum Verständnis enorm hilfreich. Ebenso ist es für die forensische Endbearbeitung erforderlich, die spezifischen Anforderungen von Ermittlungsbehörden zu verstehen. So ist es z.B. notwendig, die anzuzeigenden Ortungsdaten auf einen einzigen Standort inkl. potentieller Fehlerrate pro untersuchten Zeitstempel zu reduzieren.

Ergänzend zu den eben beschriebenen Aspekten für die forensische Nutzung bietet es sich für die wissenschaftliche Untersuchung von Ortungsdiensten an, Standortdaten direkt auf dem Endgerät während der Entstehung erfahrbar zu machen. Hierzu wurden im Rahmen der Arbeit mobile Anwendungen entwickelt (in DSRM auch als Demonstratoren bezeichnet) welche später in Teil 5 ab Seite 131 detailliert vorgestellt werden. Mithilfe der App iOSTracker lässt sich z. B. direkt oder auch retrograd auf die Ortungsdatenbank von Apple zugreifen, während die Apps WatchTracker und DroidTracker dazu entwickelt wurden, Positionsdaten live während der Entstehung zu bewerten.

Zusätzlich zu den in Java programmierten Desktopanwendungen iPhoneTrackerLE und GoogleTrackerLE für Ermittler existiert eine speziell angepasste Version des iPhoneTrackersLE, die nur für die Verwendung im Rahmen der Dissertati-

on bestimmt ist. Das besondere Merkmal, neben der Freischaltung aller Restriktionen bei ungültiger Lizenzierung, ist die Möglichkeit der Korrelation aufgezeichneter Messdaten aus der nativen App iOSTracker mit Standorten aus der Ortungsdatenbank von Apple.

Wie in Abb. 3.3 dargestellt, lassen sich so Geodaten aus der Ortungsdatenbank mit aufgezeichneten Daten des IOSTrackers korrelieren. Im Ergebnis lässt sich sehr gut nachvollziehen, dass sich der WLAN-Sender zum fraglichen Zeitpunkt innerhalb des orange gekennzeichneten Senderadius des Trackers befunden hat. Wählt der Benutzer zusätzlich die Programmoption »Estimate Position« aus, werden nur noch die entsprechenden Sender auf der Karte dargestellt.

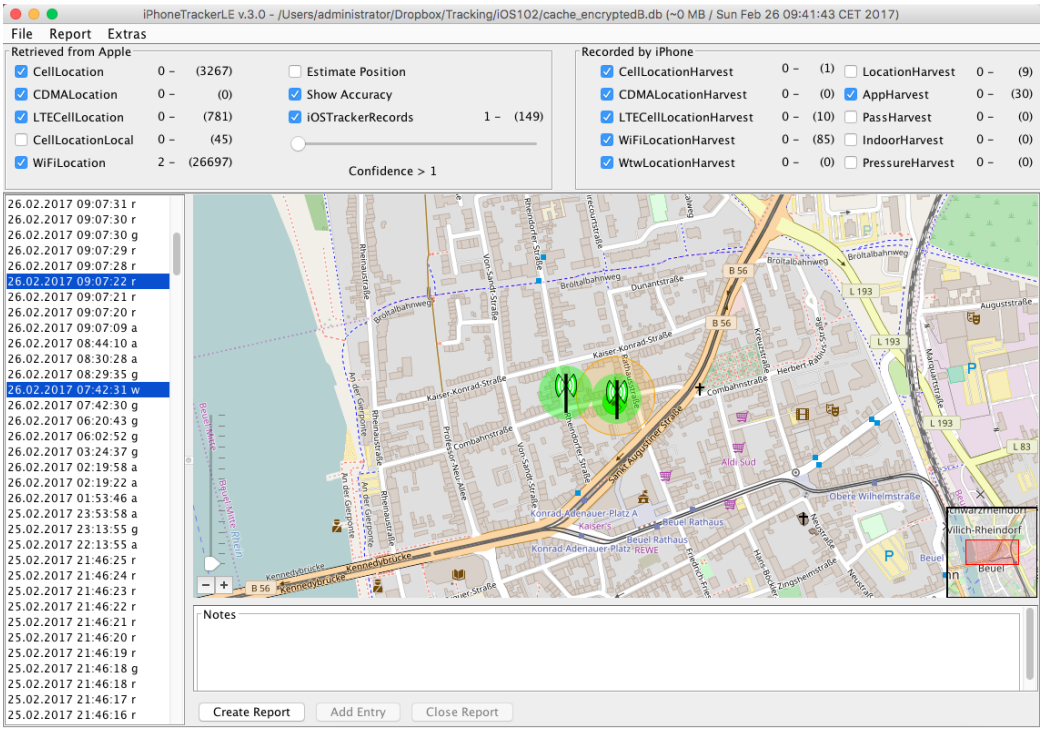


Abb. 3.3: Angepasste Version des iPhoneTrackersLE mit der Option zur Korrelation aufgezeichneter Standorte mit Einträgen aus der Ortungsdatenbank. Weitere Details im Text. Quelle: Eigene Darstellung. Kartenmaterial: © OpenStreetMap Mitwirkende 2017.

3.6 Evaluation

Auf die Implementierung folgt bei der Design Science Research Methode, wie bei vielen anderen wissenschaftlichen Vorgehensweisen auch, eine Bewertung bzw. Evaluation des Designs sowie des Ergebnisses der Entwicklung.

Bezogen auf die forensische Praxis bei der Strafverfolgung ist die Effektivität der Auswertung i. d. R. niedriger priorisiert als die Einhaltung spezieller Vorgaben der Ermittlungsbehörden. Oberstes Gebot hierbei ist das Erreichen des Maximums an Verlässlichkeit. Neben der Integrität, d.h. unverfälscht von der Erhebung bis zur Würdigung (keine Manipulation der Daten) müssen die Standorte möglichst präzise (Accuracy oder Standortdatenmodell) und vollständig sein.

Darüber hinaus bildet die Möglichkeit zur Darstellung der Ergebnisse auf Papier in lückenlos nachvollziehbarer Form mit allen verfahrensrelevanten Fakten wie Datenquellen, Geokoordinaten, Zeitstempel etc. inkl. einer Kartendarstellung die Grundvoraussetzung, um vor Gericht zu bestehen.

Für eine hinreichende wissenschaftliche Reflektion muss ferner die Auseinandersetzung mit der zugrundeliegenden Thematik stattfinden, wenn möglich anhand eines unabhängigen Modells zur Erklärung der Ortungsdienste in modernen Smartphones. Die Erstellung eines solchen Modells muss demnach ebenso Ziel dieser Arbeit sein, wie die Schaffung einer Erklärungsgrundlage für bestimmte Einzelfälle (vgl. Abschnitt 5.5.2 auf Seite 143).

Die im Rahmen der vorliegenden Arbeit entwickelten Anwendungen werden daran zu messen sein, wie sie sich in der Praxis einsetzen lassen. Hierfür lässt sich zunächst auf die Erfahrungen und das Feedback von Kollegen hinsichtlich der beiden Desktopanwendungen zurückgreifen, die bereits seit Jahren weltweit im Einsatz sind. Ferner ist die Bewertung der Arbeit durch Erkenntnisse aus den nativen Apps zur Veranschaulichung von Standortdaten für iOS und Android zu ergänzen. Mithilfe der mobilen Anwendungen lässt sich die Entstehung von Ortungsdaten live mitverfolgen. So ist es möglich, die forensische Analyse von Standortdaten in ein generisches Qualitätsmodell zu überführen, um so den für die Wissenschaft wichtigen universellen Modellansatz zu schaffen.

Zusätzlich müssen die Forschungsfragen aus Abschnitt 1.3 auf Seite 29 und in Teil 6 ab Seite 150 aufgegriffen und abschließend beantwortet werden.

3.7 Kommunikation

Während die erzielten Ergebnisse von Untersuchungen in der freien Wirtschaft häufig nicht veröffentlicht werden, sind in der Wissenschaft Veröffentlichungen sowie der öffentliche Diskurs von Forschungsergebnissen erklärtes Ziel. Das ist im Umfeld von forensischen Analysen ähnlich. Zumindest vor Gericht sind die Untersuchungsmethoden regelmäßig offen zu legen.

Eine Ausnahme zu Aussagen vor Gericht stellen Inhalte um kriminaltaktische Methoden dar. Denn mit der Offenlegung spezieller Untersuchungsmethoden ist stets zu vermuten, dass die Erkenntnisse hieraus umgekehrt zur Verschleierung von Beweismitteln angewandt werden könnten (Stichwort: Antiforensik).

Selbstredend müssen aber auch Forensiker ihr Wissen von irgendwoher beziehen, ein Dilemma also.

In der polizeilichen Praxis werden in Folge dessen allgemeine Darstellungen von Ermittlungserfolgen oder Untersuchungsmethoden ohne Verfahrensbezug über öffentliche Informationskanäle verbreitet und spezifische Details nur intern im Kreise der Ermittlungsbehörden diskutiert.

Teil 4

Forensische Untersuchung von Standortdaten aus Smartphones

Im Rahmen dieser Arbeit wird die Untersuchung mobiler Betriebssysteme auf die Analyse der beiden Plattformen Android und iOS beschränkt. Die Entscheidung hierzu basiert auf der enormen Verbreitung von Android sowie der Bedeutung von iOS im Umfeld kriminaltechnischer Untersuchungen (vgl. Abschnitt 1.2.1 auf Seite 16 bzw. konkret Abb. 1.7 auf Seite 17).

Die Vorgehensweise bei der forensischen Analyse von Standortdaten ist für die beiden mobilen Betriebssysteme ähnlich. Zunächst werden die Datendateien auf den Geräten ermittelt, anschließend ihre Datenstrukturen analysiert und in der Folge möglichst detailliert und soweit möglich generisch für die beiden Betriebssystemversionen beschrieben. Bei der weitergehenden Untersuchung bietet es sich an, die Entstehung der Standortdaten ebenfalls zu betrachten. Hierbei soll, nicht zuletzt durch die Unterscheidung des Datenursprungs (stammen die Geodaten vom Gerät oder vom Hersteller), eine Bewertung der Qualitätskriterien für Standortdaten anhand der Genauigkeit, Verlässlichkeit sowie Vollständigkeit der Daten durchgeführt werden.

Anhand dieser Untersuchungen wird dann später in Abschnitt 5.5.1 auf Seite 141 auf Basis von Erkenntnissen aus Untersuchungen mithilfe nativer Applikationen ein generisches Modell der Standortlokalisierung auf mobilen Systemen (vgl. Abschnitt 5.5.2 auf Seite 143) abgeleitet und ausführlich dargelegt werden.

4.1 Apple iOS

Die ersten forensischen Untersuchungen an der Apple Ortungsdatenbank im Rahmen dieser Arbeit wurden, bedingt durch die Medienberichte im März 2011, für ein Verfahren der Kriminaldirektion Koblenz durchgeführt. Hierbei wurde sehr schnell klar, dass neben den Daten aus den bekannten Tabellen, die Warden und Allen beschrieben hatten, forensisch wertvollere Daten in anderen Tabellen gespeichert sind (vgl. Abschnitt 4.1.1 auf Seite 73).

4.1.1 Die Ortungsdatenbank

Die Ortungsdatenbank von Apple iOS baut auf das bei mobilen Plattformen weit verbreitete relationale Datenbanksystem SQLite3 auf. Die Extraktion sowie forensische Auswertung solcher Inhalte gehört zum Standardrepertoire in der IT-Forensik. Zur Betrachtung der Daten existieren zahlreiche Programme sowie Plugins für bereits installierte Applikationen, wie z. B. Mozilla Firefox [laz18].

Problematisch gestaltet sich in der forensischen Praxis hingegen die Analyse bzw. Interpretation der in Tabellen gespeicherten Daten, da proprietäre Flags sowie Datenformate innerhalb der Datenbank ohne weitere Erklärungen oder Maßeinheiten abgespeichert sind. Für die Interpretation solcher Informationen sind häufig weitere Untersuchungen bzw. Tests und Erfahrungen aus praktischen Versuchen um die Entstehung von Geolokalisierungsdaten notwendig.

Bevor aber die Erläuterung der Inhalte aus der Ortungsdatenbank von Apple vorgenommen wird, soll zunächst der Speicherort der SQLite3-Datenbank sowie deren Extraktion vom Gerät beschrieben werden.

Pfad im Dateisystem

Um an die Inhalte der Datenbank zu gelangen, muss diese zunächst vom Gerät extrahiert werden. Hierzu war bis iOS 4.3.2 aufgrund eines Programmierfehlers von Apple eine simple Synchronisierung der Daten des Gerätes über Apples Software iTunes ausreichend. Im Folgenden werden die vier notwendigen Schritte im Detail und mit entsprechenden Screenshots beschrieben.

Um dem forensischen Grundsatz der Vermeidung von Datenveränderungen nachzukommen, muss vor der Verbindung des Gerätes mit dem Computer die Software Apple iTunes umkonfiguriert werden. Standardmäßig veranlasst iTunes ansonsten die Synchronisation mit dem Gerät. Hierbei gilt der Computer als Basis für den Datenabgleich, was zur Folge hat, dass alle Daten auf dem Gerät gelöscht würden. Dies gilt es zu verhindern.

Wie in Abb. 4.1 zu sehen, lässt sich durch das Setzen einer entsprechenden Option in iTunes (Schritt 1) die automatische Synchronisation verhindern.

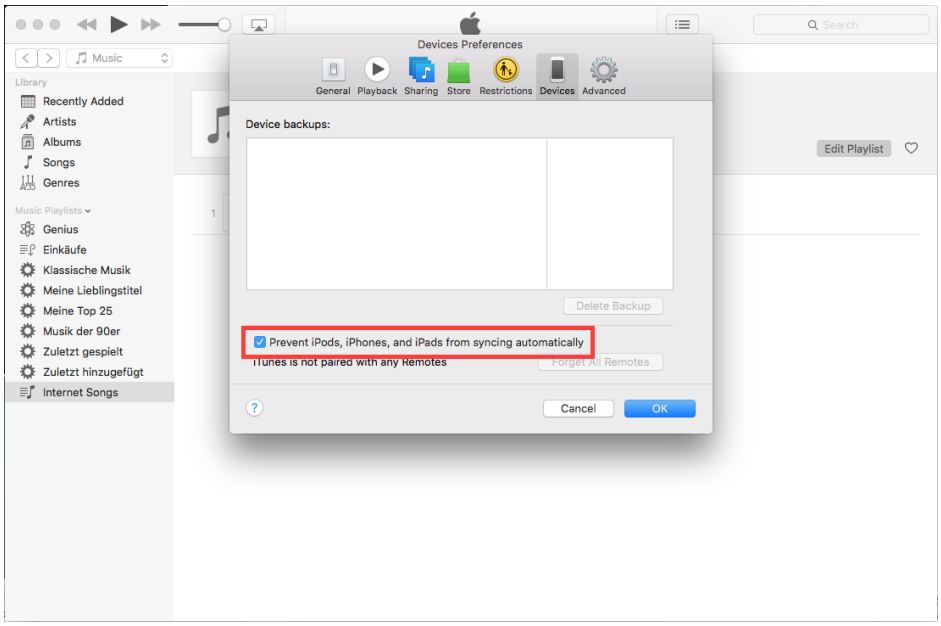


Abb. 4.1: Schritt 1 der logischen Datensicherung bei Apple: Automatische Synchronisierung in den iTunes-Einstellungen verhindern (siehe rote Umrandung). Quelle: Eigene Darstellung.

Nachdem das Gerät von iTunes z. B. als iPhone erkannt wurde, erscheint es als kleines Icon neben der Quellenauswahl und lässt sich darüber aufrufen. In der dann erscheinenden Übersicht (vgl. Abb. 4.2 auf der nächsten Seite) kann durch Betätigen des Knopfes »Back Up Now« die Sicherung des Gerätes veranlasst werden (Schritt 2). Nach nur wenigen Minuten ist die logische Sicherung der Inhaltsdaten vom Gerät bereits abgeschlossen. Ganz im Gegensatz zu einer physischen Sicherung elektronischer Beweismittel, welche i. d. R. mehrere Stunden in Anspruch nimmt.

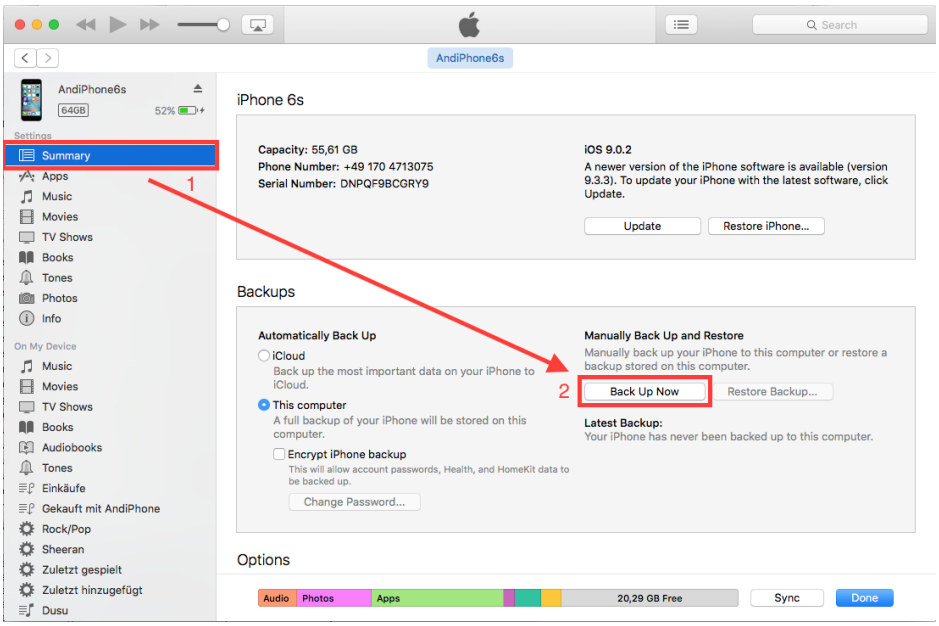


Abb. 4.2: Schritt 2 der logischen Datensicherung bei Apple: Auswahl des Gerätes (1) und Backup (2) in iTunes durchführen. Quelle: Eigene Darstellung.

Die extrahierten Daten befinden sich nach erfolgreicher Sicherung in Abhängigkeit des verwendeten Betriebssystems unterhalb folgender Ordnerstrukturen:

- `~/Library/Application Support/MobileSync/Backup/UDID/...` auf Mac-basierten Betriebssystemen
- `C:\Users\[username]\AppData\Roaming\Apple Computer\Mobile Sync\Backup\UDID\...` unter Microsoft Windows

Für die Speicherung ist insbesondere zu beachten, dass Apple die Geräte nicht anhand der Klarnamen, sondern auf Basis des UDIDs unterscheidet (vgl. [iW16], [iW17]).

Die Dateinamen der Sicherung werden ebenfalls nicht im Klartext, sondern als SHA1-Hash des Dateinamens inkl. Pfad gespeichert (siehe Abb. 4.4 auf der nächsten Seite). Eine Suche nach Dateinamen scheidet so aus. Um die Datenbank zu ermitteln, bietet sich stattdessen eine Dateiheaderanalyse zur Identifikation der Ortungsdatenbank an. Der Header von SQLite3-Datenbanken beginnt nämlich immer mit der Zeichenfolge `SQLITE3`. Im Anschluss kann die Datenbank durch eine Sortierung der Dateigrößen von groß nach klein ermittelt werden (Ortungsdatenbanken sind in der Regel mehrere Megabyte groß).

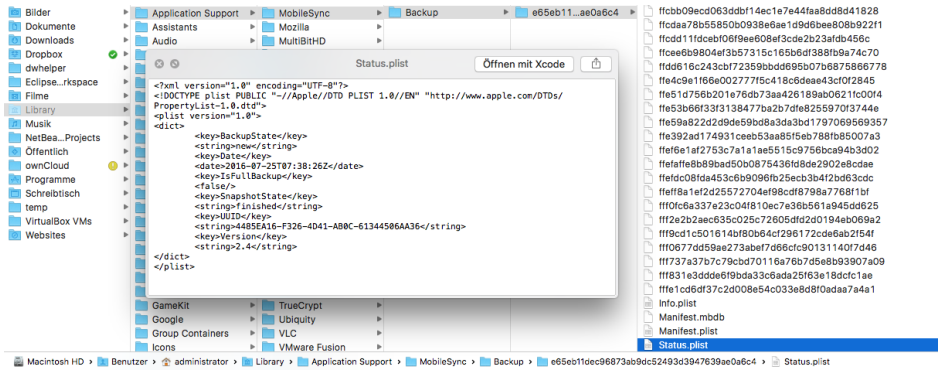


Abb. 4.3: Schritt 3 der logischen Datensicherung bei Apple: Sicherungsdaten im Dateisystem des Sicherungsrechners ermitteln. Quelle: Eigene Darstellung.

Alternativ existieren im Internet Python-Skripte (vgl. [gal15]) zum Parsen der Backup-Datei manifest.mbdb, die neben der SHA1-Repräsentation der Pfad- und Dateinamen auch menschenlesbare Dateinamen sowie weitere Informationen ähnlich einem unix ls-Befehl zum Auflisten von Verzeichnisinhalten ausgeben.

Die einfachste Methode zur Extraktion der Ortungsdatenbank bietet die im Internet kostenfrei zum Download angebotene Software iPhoneBackupExtractor [Pad16]. Mithilfe der Anwendung lassen sich die Daten einzelner Applikationen sowie Systemdateien (»IOS Files«) extrahieren (Schritt 4). Die Dateinamen werden nach der Extraktion direkt dekodiert im Klartext angezeigt (vgl. Abb. 4.4).

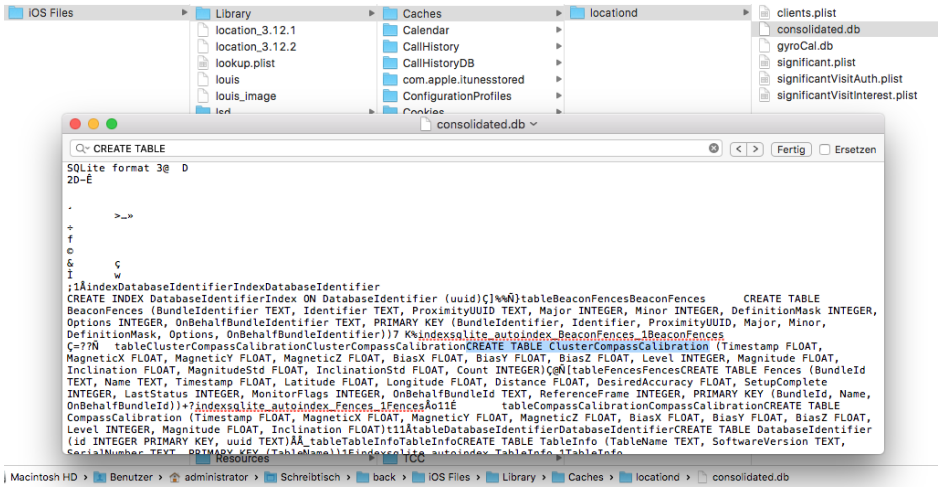


Abb. 4.4: Schritt 3 der logischen Datensicherung bei Apple: Ortungsdatenbank mithilfe der Software iPhoneBackupExtractor exportieren und aufrufen. Quelle: Eigene Darstellung.

Seit Apple iOS 4.3.3 ist die Extraktion der Datenbank nur noch direkt über das Smartphone selbst möglich. Hierzu muss zuvor eine passende Jailbreak-Methode angewandt werden, um Zugriff auf den Datenbestand des Systemdienstes (root) zu erlangen. Ohne genauer auf die Details der unterschiedlichen Jailbreak-Methoden einzugehen, wird hierbei eine temporäre oder dauerhafte Eskalation der Rechte erreicht. So lassen sich neben der Installation von Apps aus Drittanbieterquellen tiefgreifende Modifikationen bzw. Einblicke in iOS bewerkstelligen.

Auf einem jailbroken iPhone kann über den alternativen AppStore Cydia [(sa16] weitere Software für den externen Zugriff auf dem Gerät installiert werden. Um z. B. die entsprechenden Daten via SSH-Verbindung vom Gerät zu extrahieren, muss zuvor das Paket OpenSSH inkl OpenSSH-Server (siehe Abb. 4.5) installiert werden. Nach der Installation wird der SSH-Dienst automatisch gestartet und ermöglicht so den Zugang via SSH über eine bestehende WLAN- oder USB-Verbindung [Dhe14].

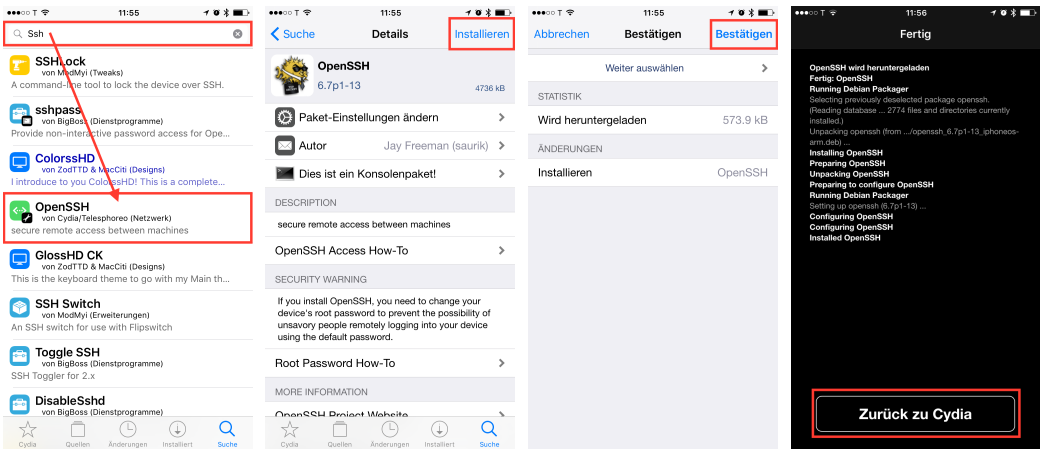


Abb. 4.5: Installation zusätzlicher Software (hier z.B. OpenSSH für den Dateizugriff) über alternativen AppStore auf einem jailbroken iPhone. Quelle: Eigene Darstellung

Zur Anmeldung des Benutzers »root« via SSH lautet das Standardpasswort durchgängig für alle Apple iOS Versionen »alpine«. Die Ortungsdatenbank des Systemdienstes lässt sich anschliessend im Verzeichnis `/private/var/root/Caches/locationd/` finden.

Die unterschiedlichen Dateinamen und Veränderungen der verschiedenen iOS-Versionen werden später in Abschnitt 4.1.1 auf Seite 73 ausführlich beschrieben.

Aufbau und Struktur

Nach der erfolgreichen Extraktion der Datenbank lassen sich die Daten via SQL-Statement abfragen und weiterverarbeiten. So kann z. B. über die Konsole, wie in Ausgabe 4.1 durchgeführt, mithilfe der Software `sqlite3` nach folgendem Schema vorgegangen werden:

1. Ermitteln aller Tabellen der Datenbank (`.tables`)
2. Export aller Inhalte der relevanten Tabelle (`SELECT * FROM <table>;`).

Konkret wird in Zeile 1 zunächst die Datenbank geöffnet. Anschließend wird eine Übersicht aller Tabellen erzeugt (Z.3). Der Befehl `.output celllocation.csv` in Zeile 24 leitet die Ausgabe des Ergebnisses der SQLite-Abfrage in eine CSV-Datei um. Durch Eingabe des Befehls `.headers on` (Z.25) werden zusätzlich zu den Werten die Spaltenüberschriften mit ausgegeben. Die Abfrage `SELECT * FROM CellLocation;` in Zeile 26 erzeugt dann die Ausgabe auf Festplatte (in die Datei »celllocation.csv«). Mittels `.exit` wird die Datenbank verlassen und die Anwendung SQLite3 geschlossen.

```
1  $ SQLite version 3.8.10.2 2015-05-20 18:17:19
2  Enter ".help" for usage hints.
3  sqlite> .tables
4  CdmaCellLocation   CellLocationCounts
5  CdmaCellLocationBoxes              CellLocationHarvest
6  CdmaCellLocationBoxes_node         CellLocationHarvestCounts
7  CdmaCellLocationBoxes_parent       CellLocationLocal
8  CdmaCellLocationBoxes_rowid        CellLocationLocalBoxes
9  CdmaCellLocationCounts             CellLocationLocalBoxes_node
10 CdmaCellLocationHarvest            CellLocationLocalBoxes_parent
11 CdmaCellLocationHarvestCounts      CellLocationLocalBoxes_rowid
12 CdmaCellLocationLocal              CellLocationLocalCounts
13 CdmaCellLocationLocalBoxes         CompassCalibration
14 CdmaCellLocationLocalBoxes_node    Fences
15 CdmaCellLocationLocalBoxes_parent  Location
16 CdmaCellLocationLocalBoxes_rowid   LocationHarvest
17 CdmaCellLocationLocalCounts        LocationHarvestCounts
18 Cell                               TableInfo
19 CellLocation                       Wifi
20 CellLocationBoxes                  WifiLocation
21 CellLocationBoxes_node             WifiLocationCounts
22 CellLocationBoxes_parent           WifiLocationHarvest
23 CellLocationBoxes_rowid            WifiLocationHarvestCounts
24 sqlite> .output celllocation.csv
25 sqlite> .headers on
26 sqlite> SELECT * FROM CellLocation;
27 sqlite> .quit
```

Terminalausgabe 4.1: Befehlsübersicht zur Auflistung der SQLite-Tabellen einer iOS 4.3.2 Ortungsdatenbank sowie zusätzlichem Export der Tabelle CellLocation in eine CSV-Datei mithilfe der Konsolenanwendung sqlite3.

Das Resultat von Ausgabe 4.1 auf der vorherigen Seite ist eine Tabelle, wie die Folgende (limitiert auf 5 Einträge mit gekürzten Überschriften):

MCC	MNC	LAC	CI	timestamp	Latitude	Longitude	HAcc	Alt	VAcc	Speed	Course	Conf
262	1	26369	43695	300958520.283397	49.8314321	7.67494863	1655.0	0.0	-1.0	-1.0	-1.0	70
262	1	25118	557887	300958520.283397	49.78332656	7.65151941	500.0	0.0	-1.0	-1.0	-1.0	70
262	1	26375	61085	300958520.283397	49.81101763	7.69869554	2885.0	0.0	-1.0	-1.0	-1.0	70
262	1	26375	30194	300958520.283397	49.82029122	7.71951216	1219.0	0.0	-1.0	-1.0	-1.0	70
262	1	26146	496028	300958520.283397	49.81847596	7.72168356	500.0	0.0	-1.0	-1.0	-1.0	70
...	...	...	...	...	...	...	...	0.0	-1.0	-1.0	-1.0	70

Tab. 4.1: Ergebnis der Datenbankabfrage
SELECT * FROM CellLocation;
einer iOS 4.3.2-Ortungsdatenbank

Die detaillierte Beschreibung der unterschiedlichen Tabellen aus Ausgabe 4.1 auf der vorherigen Seite und deren Inhalten wird ab Seite 76 fortgeführt.

Vorab ist aber festzuhalten, dass die Tabellennamen den Datenursprung der Inhalte wiedergeben. So steht das englische Wort »Cell« im Namen für Funkzellentabellen und die Abkürzung »Wifi« taucht in Tabellen mit WLAN-Daten auf.

Ferner lassen sich noch Tabellen mit dem Suffix »harvest« finden. Die Tabellen beinhalten keine bzw. maximal wenig Daten. Wie später in Abschnitt 4.1.3 auf Seite 87 weiter ausgeführt, sind diese Tabellen für die forensische Auswertung von besonderem Interesse. Umgekehrt werden die Inhalte dieser Tabellen von den kommerziellen Tools entweder nicht oder nur selten verarbeitet.

Weitergehende Untersuchungen haben ergeben, dass die meisten Tabellen keine externen Verweise beinhalten. Lediglich Tabellen mit dem Suffix »_boxes« am Ende des Tabellennamens enthalten externe Schlüssel (sogenannte foreign keys) zu den primären Einträgen in der korrespondierenden Tabelle ohne Suffix. Die Referenztabellen beinhalten Koordinaten zu Standorten aus den Tabellen ohne Suffix. So wird anstatt eines Radius um den Standort eine Box definiert, welche eine wesentlich schnellere Prüfung darauf erlaubt, ob ein Punkt innerhalb einer Box anstelle eines Kreises liegt.

Darüber hinaus existieren noch Tabellen mit dem Suffix »count«. Diese Tabellen beinhalten lediglich eine Zeile mit nur einer Spalte, welche die Anzahl der Einträge der Tabellen ohne Suffix wiedergibt.

Ortungsdaten im Wandel von iOS

Wie in Abschnitt 4.1.1 auf Seite 69 bereits erwähnt, hat Apple den Dateinamen und den Aufbau der Ortungsdatenbank im Laufe der Zeit häufiger geändert. In Tab. 4.2 sind die Änderungen aller iOS-Versionen dargestellt.

Die aus den Medien bekannte Datei »consolidated.db« (vgl. [AW11]) existiert nach wie vor (auch im iTunes Backup). Die Datei hat allerdings nichts mehr mit der ursprünglichen Version der Ortungsdatenbank gemeinsam. Ob die Beibehaltung der Datei der Verschleierung sowie zur Beruhigung der Medien und Nutzer dienen soll, ist zwar nur Spekulation, aber dennoch auffällig.

	vor iOS 4.x	**bis iOS 4.3.2**	**ab iOS 4.3.3**
Dateiname(n)	h-cells.plist	consolidated.db	cache.db
Besonderheiten	nicht untersucht	Backup via iTunes möglich	Zugriff nur noch via SSH möglich (Jailbreak nötig)
	iOS 5.x	**iOS 6.x**	**iOS 7.x**
Dateiname(n)	cache_encryptedA.db	cache_encryptedA.db	cache_encryptedA.db
Besonderheiten	neue Tabellen: AppHarvest	neue Tabellen: PassHarvest	
	iOS 8.x	**iOS 9.x**	**iOS 10.x**
Dateiname(n)	cache_encryptedA.db cache_encryptedC.db	cache_encryptedA.db cache_encryptedB.db cache_encryptedC.db	cache_encryptedB.db cache_encryptedC.db
Besonderheiten	cache_encryptedC.db enthält Fitnessdaten	cache_encryptedB.db enthält jetzt WLAN-Daten entfernte Tabellen: WifiLocation	

Tab. 4.2: Benennung und Veränderungen an den Ortungsdatenbanken verschiedener iOS-Versionen von iOS 4 bis iOS 10

Kategorisierung von Standortdaten aus Apples Ortungsdiensten

Innerhalb von Apples Ortungsdatenbank existieren verschiedene Tabellen mit Standortdaten unterschiedlicher Bestimmung, Genauigkeit, Granularität etc. Wie später in Abschnitt 5.5.3 auf Seite 145 detailliert ausgeführt, lassen sich die Tabellen zunächst hinsichtlich des Datenursprungs (von Apple) bzw. Verwendungszweckes (für Apple) der Positionsdaten unterscheiden (vgl. Tab. 4.3 auf der nächsten Seite).

Standortdaten werden sowohl von Apple an das Smartphone übermittelt, als auch nach der Erhebung auf dem Gerät zu Apple hin versandt. Wie in Tab. 4.3 dargestellt, werden die Daten entweder von außen (extrinsisch) über den Hersteller zur Verfügung gestellt oder über die im Gerät verbauten Sensoren (intrinsisch) ermittelt.

Die Kategorisierung der Standortdaten lässt sich anhand der Namensgebung der Tabellen vornehmen. So beinhalten z. B. alle Tabellen mit dem Suffix »Harvest« Daten für Apple, wohingegen Tabellen ohne Suffix mit Daten aus Apples crowdsourced Datenbank befüllt sind.

Daten von Apple (extrinsisch)	**Daten vom Endgerät (intrinsisch)**
	AppHarvest (>iOS5),
CdmaCellLocation,	CdmaCellLocationHarvest (>iOS7),
CdmaCellLocationLocal (>iOS7),	CdmaCellNeighborsLocationHarvest (>iOS9),
CellLocation, CellLocationLocal,	CellLocationHarvest, CellNeighborsLocationHarvest (>iOS9),
	IndoorLocationHarvest (>iOS9), IndoorWifiHarvest (>iOS9),
LteCellLocation,	LocationHarvestLteCellLocationHarvest,
LteCellLocationLocal (>iOS7),	LteCellNeighborsLocationHarvest (>iOS9),
	PassHarvest (>iOS7),
	PoiHarvestLocation, PoiHarvestMUID, PoiHarvestWifi (>iOS10),
	PressureLocationHarvest (>iOS9),
SCDMA,	PressurePressureHarvest (>iOS10),
ScdmaCellLocation (>iOS9),	ScdmaCellNeighborsLocationHarvest (>iOS9),
UnknownCellLocation (iOS7),	UnknownCellLocationHarvest (iOS7),
WifiAWD (>iOS10),	
WifiLocation(!iOS9)	WifiLocationHarvest,
	WtwLocationHarvest (>iOS9)

Tab. 4.3: Übersicht aller Tabellen der iOS Ortungsdatenbank(en) von iOS4 bis iOS10.2 mit Unterscheidung des Datenursprungs vgl. [DG16]

In der ergänzenden Auflistung zum Datenursprung auf der nächsten Seite wird im Rahmen dieser Arbeit zusätzlich eine Zuordnung hinsichtlich verschiedener Lokalisierungstechniken seit iOS4 vorgenommen. Wie später in Abschnitt 5.5.2 auf Seite 143 ausführlich dargelegt und konkret in Tab. 5.1 auf Seite 144 aufgelistet, lassen sich so weitere Hinweise zur potentiellen Genauigkeit von Ortungsdaten ableiten. Darüber hinaus sollen die angegebenen Seitenverweise das punktuelle Nachschlagen der einzelnen Datenquellen vereinfachen.

In den folgenden Abschnitten werden dann die für eine forensische Auswertung interessanten Tabellen auf Basis von iOS Version 9.3.3 vorgestellt und analysiert. Die Informationen der unterschiedlichen Spalten scheinen hierbei über alle iOS

Versionen hinweg gleichbedeutend, dafür kommen mit jeder neuen iOS Version weitere Tabellen mit potentiell neuen Datenquellen hinzu.

- **Ortungsdaten von Apple (extrinsisch)**
  mit niedriger Genauigkeit und Verlässlichkeit, dafür viele Dateneinträge
  - Mobilfunk-Tabellen
    - CellLocation S. 76, LteCellLocation S. 82,
    - CdmaCellLocation, CdmaCellLocationLocal (>iOS7), SCDMA, ScdmaCellLocation (>iOS9) S. 83ff.
    - CellLocationLocal, LteCellLocationLocal (>iOS7) S. 85
  - WLAN-Tabellen
    - WifiLocation generell S. 80 außer iOS9 siehe S. 86
- **Ortungsdaten für Apple (intrinsisch)**
  mit hoher Genauigkeit und Verlässlichkeit, dafür selten Dateninhalte
  - Bei GPS-Verfügbarkeit siehe S. 87ff.
    - LocationHarvest S. 89
    - CellLocationHarvest S. 93,
    - WifiLocationHarvest S. 95
  - Ohne GPS-Verfügbarkeit aber hinreichender Genauigkeit siehe S. 97ff.
    - AppHarvest (>iOS5) S. 97
    - PassHarvest (>iOS7) S. 98
  - Nicht vollständig geklärt oder keine Daten festgestellt, siehe S. 100ff.
    - WtwLocationHarvest (>iOS9)
    - CellNeighborsLocationHarvest (>iOS9), LteCellNeighborsLocationHarvest (>iOS9),
    - CdmaCellLocationHarvest (>iOS7), CdmaCellNeighborsLocationHarvest (>iOS9),
    - ScdmaCellNeighborsLocationHarvest (>iOS9)
    - vermutlich für eine zukünftige Nutzung geplant
      - IndoorLocationHarvest (>iOS9), IndoorWifiHarvest (>iOS9),
      - PressureLocationHarvest (>iOS9), PressurePressureHarvest (>iOS10)
      - UnknownCellLocationHarvest (iOS7)

4.1.2 Ortungsdaten von Apple

Wie bereits von Warden und Allen korrekt erkannt und dargelegt, beinhaltet die Ortungsdatenbank von Apple Informationen zu Positionsdaten, die von Apple stammen. Wobei dies nicht notwendigerweise bedeutet, dass Apple die Gerätenutzer »trackt« bzw. überwacht, wie von den Medien proklamiert (vgl. [(4r11]) wurde. Vielmehr dienen die Daten dazu, das Nutzererlebnis während der Lokalisierung unter ungünstigen Umständen zu verbessern (vgl. Abschnitt 4.1.3 auf Seite 87 bzw. Abschnitt 5.5.3 auf Seite 145).

CellLocation, WiFiLocation

Ausgehend von den Berichten in den Medien bilden die Tabellen »Celllocation« bzw. »WifiLocation« zunächst auch für diese Arbeit die Basis für die durchgeführten forensischen Untersuchungen. Wie die Namen vermuten lassen, handelt es sich bei den Inhalten um Koordinaten zu den Positionen von Funkzellen der Mobilfunkbetreiber bzw. Drahtlosnetzwerken genauer WLAN.

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
262	1	38855	1959037	336687527.233497	50.34167772	7.56277644	1414.0	0.0	-1.0	-1.0	-1.0	70
262	1	10241	39110	336687527.233497	50.3410446	7.56211131	3415.0	0.0	-1.0	-1.0	-1.0	70
262	1	10527	1946113	336687527.233497	50.34122639	7.56364428	2093.0	0.0	-1.0	-1.0	-1.0	70
262	1	10527	43208	336687527.233497	50.34501749	7.56381779	2059.0	0.0	-1.0	-1.0	-1.0	50
262	1	38855	1957133	336687527.233497	50.34612059	7.56118327	1875.0	0.0	-1.0	-1.0	-1.0	70
262	1	10527	1957133	336687527.233497	50.34651505	7.56146174	2066.0	0.0	-1.0	-1.0	-1.0	70
262	1	10527	1938707	336687527.233497	50.34652614	7.56180667	1812.0	0.0	-1.0	-1.0	-1.0	70

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

Abb. 4.6: Darstellung der Spalten der Tabellen CellLocation (oben) bzw. WiFiLocation (unten) ohne Konvertierung der Datentypen. Quelle: [(4r11].

Wie in Abb. 4.6 bewusst ohne Konvertierung dargestellt, beinhalten die Tabellen viele Informationen in einem nicht-menschenlesbaren Format. So werden z.B. Zeitstempel (engl. »timestamp«) in einem Dezimalformat und fehlerhafte Werte mit »-1« angegeben. Die Umrechnung der Zeitstempel wird in Abschnitt 4.1.2 auf der nächsten Seite beschrieben. Die Zahl »-1« ist ein gängiger Rückgabewert bei Fehlern in der Programmierung.

Beide Tabellen beinhalten Spalten mit den annähernd gleichen Informationen:

- Eine individuelle Repräsentation der Datenquelle
  in einer (Wifi-) bzw. mehreren Spalten (CellLocation)
  - **MCC, MNC, LAC, CI** (für Funkzellen) **bzw.**
    (UARFCN, PSC vgl. Abschnitt 4.1.2 auf Seite 80)
  - **MAC** (für WLAN-Accesspoints)
- Eine Zeitangabe, welche den Zeitpunkt der Datenerhebung angibt
  - **Timestamp (im CFAbsolute-Time Datenformat vgl. Abschnitt 4.1.2)**
- Den Standort der Senderquelle
  - **Latitude, Longitude** (in Grad mit Dezimalstellen)
- Die Genauigkeit der Datenquelle
  - **Horizontal- und Vertical- Accuracy** (max. Sendebereich in Meter)
  - »-1« für Funkzellen, da nicht relevant bzw. Abstand i. d. R. zu groß
- Die Höhe des Senders
  - **Altitude** (in Meter über NN)
  - 0 für Funkzellen (nicht relevant)
- Eine Geschwindigkeits- bzw. Kursangabe
  - **Speed / Course** (-1 für invalid bzw. nicht erfasst)
- Und zuletzt eine Verlässlichkeitsangabe bzgl. des Datenursprungs
  - **Confidence**
    - 50-70% für Funkzellen,
    - 50% für WLAN-Sender
    - vermutlich bezogen auf die Position der Senderquelle

Zusammenfassend dürften für forensische Untersuchungen insbesondere folgende Informationen von Interesse sein:

- ***Timestamp (Datum mit Zeitangabe)***
- ***Location (Der Ort als Geookordinaten)***
- Accuracy (Genauigkeit) und
- Confidence (Verlässlichkeit)

Im Folgenden werden die einzelnen Datenformate sowie Wertebereiche (bzw. die Konvertierung falls möglich) einmalig für die ganze Arbeit beschrieben.

Zunächst gilt es, die CFAbsolute-Time der Zeitstempel Angabe (Timestamp) zu konvertieren. Es ist bekannt, dass Computer in vergangenen Zeitintervallen ab einem bestimmten Zeitpunkt rechnen. Wie in [App16h] beschrieben, bezieht sich das CFAbsolute-Time Zeitformat auf eine Zeitspanne in Sekunden seit dem 1.ten Januar 2001 00:00:00 GMT. Das ist insofern ungewöhnlich, als das UNIX-Zeitformat in Sekunden ab dem 1.1.1970 gebräuchlicher ist.

Eine Begründung, warum Apple ein eigenes Datumsformat bevorzugt, konnte nicht gefunden werden. Eine mögliche Ursache liegt in der Verringerung der Ungenauigkeit für zukünftige Datumswerte nach dem 1.1.2001. Hierfür spricht obendrein die Verwendung des Datentyps »double« mit einer Genauigkeit von 64-bit anstatt 32-bit gegenüber dem Datentyp »long« in dem unix Zeitstempel oftmals gespeichert werden.

In SQL lassen sich Zeitstempel mithilfe der integrierten Umrechnungsfunktion »datetime« in ein menschenlesbares Format umwandeln. Hierzu muss allerdings zunächst noch die Differenz in Sekunden zwischen dem 01.01.2001 und dem 01.01.1970 (978307200 Sekunden) auf den Wert in der Zelle addiert werden. Der Aufruf zur Umrechnung aller Zeitstempel einer Spalte lautet demnach:

```
datetime((COLUMN + 978307200), 'unixepoch', 'localtime').
```

Die Darstellung von Geokoordinaten in Dezimalform wird als bekannt vorausgesetzt. Für die Durchführung eigener Untersuchungen hat es sich als sehr nützlich erwiesen, dass über Googles Kartendienst (Google Maps) unter Verwendung einer Uniform Resource Locator (URL) in Form von

```
http://maps.google.de/maps?q=latitude,longitude
```

jede beliebige Geokoordinate innerhalb der Ortungsdatenbank auf einer Karte dargestellt werden kann (vgl. Abb. 4.7 auf der nächsten Seite). Für die Darstellung ganzer Positionsblöcke ist dieses Vorgehen hingegen nicht geeignet.

Die Angabe von Sendereichweiten (Accuracy) und Verlässlichkeit (Confidence) wird später zum Verständnis der Verortung von mobilen Endgeräten noch von elementarer Bedeutung sein. Die Genauigkeit oder besser die max. Ungenauigkeit, die sich aus dem Wert Accuracy in Metern ablesen lässt, beschreibt hierbei den Senderadius von Funkzellen sowie WLAN-Sendern. Der Wert gibt an, dass sich das Gerät zum Zeitpunkt *t* (Timestamp) der Geolokalisierung innerhalb des Senderadius des angegebenen Funksenders befunden hat.

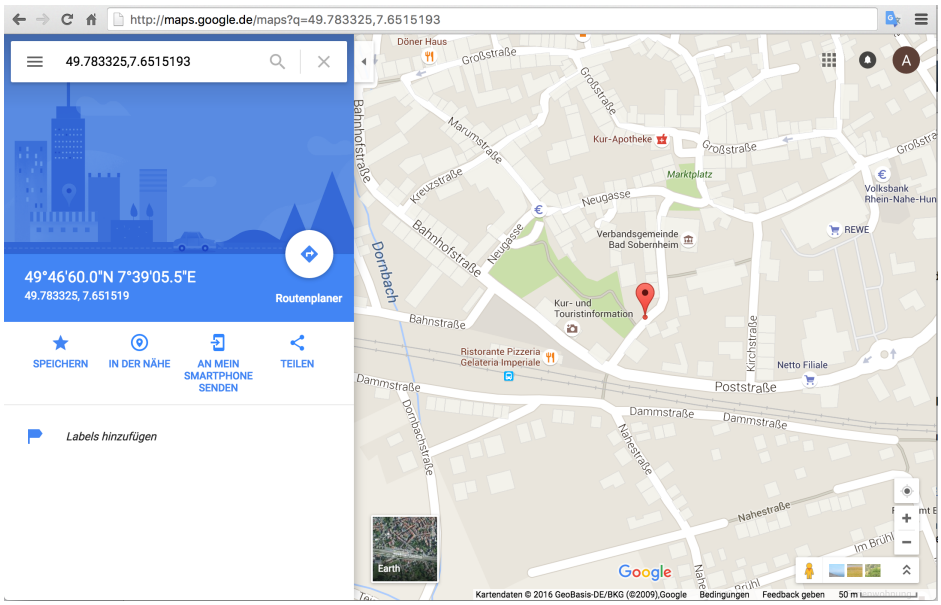


Abb. 4.7: Kartendarstellung von Geokoordinaten mithilfe von Goolge Maps via URL: http://maps.google.de/maps?q=49.783325,7.6515193. Quelle: Google Maps. Kartenmaterial: © Google 2017.

Die Verlässlichkeit der Sendestandorte wird für WLAN-Stationen mit 50% -, für Mobilfunksender mit 70% Verlässlichkeit angegeben (vgl. Abb. 4.6 auf Seite 76). Diese Werte erscheinen zunächst nicht besonders vertrauenswürdig. Eine fünfzigprozentige Verlässlichkeit dürfte, wenn man die Prozentangabe alleine für sich betrachtet, in der forensischen Praxis als ungenügend gelten.

Aufgrund der beschränkten Verwendung der Werte (50 bzw. 70 bei WLAN, bzw. [0 .. 30 .. **50** .. **70** .. 100] auf einer Prozentskala im Bereich Mobilfunk) und durch die Erfahrung aus zahlreichen Untersuchungen im Rahmen dieser Arbeit lässt sich die Bewertung leicht zum Positiven hin korrigieren. So beschreiben 50% bei WLAN-Sendern tatsächlich mehr als nur eine Mindestverlässlichkeit bezogen auf die Standorte von WLAN-Accesspoints und 70% bei Mobilfunksendern lassen hier bereits eine höhere Verlässlichkeit bzgl. der Beständigkeit der Standorte von Mobilfunkantennen gegenüber WLAN-Sendern erkennen.

Wie bereits zu Beginn dieses Kapitels auf S. 76 beschrieben, handelt es sich bei den Standortdaten in den »...«*Location*-Tabellen nicht um Ortsinformationen des Gerätes, sondern um Ortsinformationen von Funksendern in der vermeintlichen Umgebung zum eigenen Standort.

So wird auch nachvollziehbar, warum zu den Positionsdaten aus Tabellen mit Mobilfunkinformationen auch eindeutige Identifikationsmerkmale von Funkzellen gespeichert werden. Durch Angabe des MobileCountry- (MCC), des MobileNetworkCode (MNC), des LocationAreaCode (LAC) und der CellIdentification (CI) lässt sich jede GSM sowie UMTS Funkzelle auf der Welt exakt und vor allem eindeutig beschreiben. So ist z. B. Deutschland der MCC »262« zugeordnet. Der MNC »1« steht für den Mobilfunkbetreiber Deutsche Telekom. T-Mobile unterteilt ihr Mobilfunknetz wiederum in Areale, welche durch die sogenannten LACs unterschieden werden. Innerhalb dieser Bereiche werden dann die Funkzellen betrieben, die jeweils eine für die LAC eindeutige Bezeichnung (die sogenannte CellID, kurz CI) besitzen.

Mit der Einführung neuer iOS-Versionen tauchen auch immer wieder weitere Spalten innerhalb einzelner Tabellen auf. In der Tabelle *CellLocation* sind dies z. B. die Spalten UARFCN (in iOS8) oder auch ARFCN und PSC. Die Angabe weiterer Merkmale, wie UARFCN und PSC, erlaubt die Unterscheidung von UMTS bzw. LTE Funksender. Über die Funkzellenidentifikationsnummer (CI) hinaus können Sender auf der physikalischen Ebene mittels Ganzzahl basierend auf der Trägerfrequenz (UARFCN, Kurzform für UTRA Absolute Radio Frequency Channel Number) bzw. dem primären Synchonisierungscode (PSC) (vgl. [Gö09]) unterschieden werden. In der Praxis kommen diese Identifikationsmerkmale jedoch aktuell (noch) nicht zum Tragen. Bei den durchgeführten Analysen wurde immer nur der Wert »-1« festgestellt.

Ein weiteres Problem für die Auswertung der Tabellen *Cell-* bzw. *WiFiLocation*: Sehr häufig existieren zu einem Zeitstempel eine Vielzahl an Positionsangaben mit unterschiedlichen Standorten zu verschiedenen Sendern. Für eine eindeutige forensische Aussage sind »mehrere potentielle Aufenthaltsorte zu einem einzigen Zeitpunkt« nicht geeignet! Wie später in Abschnitt 5.5.4 auf Seite 148 beschrieben, lässt sich die »Punktewolke« für iOS-Versionen bis iOS10 sehr zuverlässig auf einen einzigen Eintrag reduzieren.

Zum Zeitstempel der Ortungsdaten ist zu sagen, dass es sich hierbei um den Zeitpunkt der Nutzung des Systemdienstes am Gerät handelt und nicht etwa um den Zeitpunkt der Erhebung der Daten durch Apple. Diese Aussage lässt sich leicht mittels Untersuchungen und der nativen App iOSTracker zeigen. Weitere Details hierzu folgen in Abschnitt 5.1 auf Seite 132.

Die Spalteninhalte der Tabelle WifiLocation verhalten sich analog zur Tabelle CellLocation. Der einzige Unterschied besteht darin, dass hier an Stelle von Mobilfunksendern Angaben zu Drahtlosnetzwerken (WLAN) gespeichert sind. Demnach werden als eindeutige Bezeichner von WLAN-Accesspoints deren MAC-Adressen in der hexadezimalen Form mit Doppelpunkten als Trennzeichen gespeichert. Informationen zur Genauigkeit finden sich in diesen Tabellen ebenso wie (naturgemäß) geringere Sendereichweiten. Auf die Genauigkeitsangaben für die Vertical-Accuracy wurde bereits in Abschnitt 4.1.2 auf Seite 77 hingewiesen.

Erfahrungen und Probleme

Die Geokoordinaten der von Apple übertragenen Ortungsdaten lassen sich, wie in Abschnitt 4.1.2 auf Seite 78 beschrieben bzw. Abb. 4.7 auf Seite 79 zu sehen, am besten auf einer topographischen Karte darstellen. Für die kriminalpolizeilichen Ermittlungen sind hierbei insbesondere Standortdaten zu speziellen Zeitpunkten von Interesse. Hierzu gilt es, die Anzahl der darzustellenden Punkte zunächst bestmöglich einzuschränken und vor allem keine Zweifel an der Eindeutigkeit der Daten aufkommen zu lassen.

Bei der Auswertung von Funkzellen- und WLAN-Daten zu den durchgeführten eigenen Untersuchungen mit vorgegebenen Routen oder bekannten Standorten zu bestimmten Zeitpunkten hat sich gezeigt, dass zu einem Zeitstempel immer Standortdaten zu mehr als einem Funksender gespeichert sind. Aus forensischer Sicht stellt sich die Frage, ob sich aus der Vielzahl von Standortdaten immer ein einziger Standort zuverlässig bestimmen lässt. Erste Tests zeigten, dass der Standort regelmäßig im Bereich des Schwerpunktes der Punktewolken zu liegen scheint (vgl. Abb. 4.8 auf der nächsten Seite). Allerdings gab es auch Abweichungen, die diese Theorie widerlegten. Wie zum Beispiel in Abb. 4.8 auf der nächsten Seite zu sehen, kommt es vor, dass die Position des Gerätes mitunter außerhalb der Punktwolke liegt. Diese, teilweise erheblichen, Abweichungen (vgl. Abb. 4.8 auf der nächsten Seite rechts) zum Zentrum der Standortdaten machten noch weitere Untersuchungen bzw. Hypothesen zur Standortverlässlichkeit notwendig.

Dabei hat hat sich recht schnell gezeigt, dass die Abweichung zwar unerfreulich, aber zumindest im Ansatz erklärbar wird. So ist z. B. in Abb. 4.8 auf der nächsten Seite zu sehen, dass der Sendebereich des ersten Eintrages der Funkzellenda-

Abb. 4.8: Erfahrungen und mögliche Ungereimtheiten bei der Auswertung von Apples Ortungsdaten. Links: Endgerät im Zentrum der umgebenden Funksender (Regelfall). Rechts: Standort außerhalb des Zentrums aber innerhalb des Senderadius des ersten Funksenders (Ausnahmefall). Quelle: Eigene Darstellung. Kartenmaterial: © OpenStreetMap Mitwirkende 2011.

ten zum gegeben Zeitstempel eine große Ausbreitung aufweist. Betrachtet man die örtlichen Begebenheiten zum Zeitpunkt der Gerätelokalisierung so lässt sich nachvollziehen, dass die Mobilfunkverbindung des Gerätes (in der Abb. 4.8 mit einem roten Kreuz markiert) von dem einem erhöhten Standort auf der linken Moselseite über den mit einer blauen »1« markierten Funksender auf der gegenüberliegenden Moseltalseite stattgefunden haben muss. Das wiederum bedeutet, dass sich das Gerät für die Standortbestimmung über Mobilfunk innerhalb des Sendebereiches des Funkmastes befunden hat. Darum erstreckt sich der grüne Bereich (Senderadius) auch über die gesamte rechte Abbildung oben.

In Abschnitt 5.5.3 auf Seite 145 sowie Abschnitt 5.5.4 auf Seite 148 werden die besondere Bedeutung des ersten Eintrags zu jedem Zeitstempel sowie weitere Optionen zur Erkennung von Sonderfällen zu Ende geführt. Mithilfe der nativen Apps lässt sich die besondere Bedeutung zur Einschätzung der Verlässlichkeit und Qualität des ersten Eintrages im Rahmen von Live-Untersuchungen erhärten.

LteCellLocation (ab iOS5)

Mit der Einführung von LTE-fähigen Apple Geräten (ab iPhone5 bzw. iPad3 vgl. [App16g]) wurde in iOS5 die Tabelle *LteCellLocation* eingeführt. Zwar lassen sich aktuelle iOS Versionen auch auf älteren iPhone Modellen, wie z. B. dem iPhone4S noch betreiben, die Tabellen werden aber nur befüllt, wenn der entsprechende

Empfänger (iPhone4S hat kein LTE [iPh13]) im Gerät verbaut ist und so aktiv genutzt werden kann.

In der Tabelle *LteCellLocation* wurden die Spalten **LAC und PSC** ersetzt durch:

- **TAC** (Tracking Area Code)
- **NID** (Network (Cell) IDentification)

Die Ersetzung von LAC durch **TAC** bei LTE ist auf den Terminus »Tracking Area Code« anstatt »Location Area Code« zurückzuführen. Darüber hinaus besitzen LTE-Funkzellen ab jetzt eine physische Identifikationsnummer **(PID)** zusätzlich zur **CID**. Wie die Spalte **PSC** in der Tabelle *CellLocation* scheint auch die Spalte **PID** für eine zukünftige Verwendung (zur Differenzierung von Funkzellen beim Übergang von homogenen großflächigen Funkzellen zu kleineren heterogenen Netzen nach [SB14]) vorgesehen zu sein. Aktuell beinhalten die Einträge in der Spalte PID durchgängig den Wert »-1«. Was die Darstellung der Daten auf einer Karte betrifft, so ergibt sich kein Unterschied zu den Erfahrungen der Ortungsdaten von Apple allgemein.

CdmaCellLocation (ab iOS7)

Code Division Multiple Access (CDMA) steht für einen vorwiegend in Amerika sowie in Teilen Asiens gebräuchlichen Mobilfunkstandard der dritten Generation (3G). Daten innerhalb der Tabelle *CdmaCellLocation* sind im Rahmen forensischer Untersuchungen von Geräten mit CDMA-Empfängern allerdings nur dann zu erwarten, wenn das Gerät auch aktiv in den CDMA-Netzen der USA bzw. Asien genutzt worden ist.

Die Tabelle *CdmaCellLocation* beinhaltet zur Identifikation eines CDMA-Funksenders folgende Merkmalsspalten (vgl. [rGPPG04]):

- **MCC** (Mobile Country Code)
- **SID** (Subscriber Identifier)
- **NID** (Network Identifier)
- **BSSID** (Billing oder BREW [Gro09] Subscriber Identity)
- **ZONEID** (Zone Identification)
- **BANDCLASS** (Bandwidth Class)
- **CHANNEL** (Channel within Band Class)

Die oben aufgeführten Merkmale spielen insofern eine Rolle, da sich Überschneidungen mit den Termini des GSM Mobilfunknetzes ergeben (vgl. [(ms14]). Die CDMA-typischen Merkmale sind **BSSID, ZONEID, BANDCLASS bzw. PNOFFSET**. Für die Darstellung von Standortdaten spielen diese Informationen indes keine Rolle, sie lassen sich aber ggf. für einen Abgleich mit Providerdaten heranziehen.

Die übrigen Spalten mit Zeitangaben, Standortdaten, Genauigkeit und Verlässlichkeit entsprechen der gebräuchlichen Repräsentation für Funkzellen in den Ortungsdatenbanken (vgl. Abschnitt 4.1.2 auf Seite 76). Für die Darstellung auf einer Karte ergibt sich kein Unterschied zu den Erfahrungen bzgl. der Ortungsdaten von Apple allgemein.

ScdmaCellLocation (seit iOS9)

Der Synchronous-CDMA-Mobilfunkstandard (kurz SCDMA oder TD-SCDMA für Time-Division-Synchronous Code Division Multiple Access) bezeichnet die Weiterführung des CDMA2000 Mobilfunkstandards, hervorgegangen aus dem WCDMA (Wideband Code Division Multiple Access) Mobilfunkstandard (vgl. [na12]). Laut heise wird dieser Standard nur vom größten chinesischen Mobilfunkbetreiber (China Mobile) eingesetzt (vgl. [Suh06]).

Zur Identifikation eines SCDMA Funksenders beinhaltet die *ScdmaCellLocation*-Tabelle folgende Merkmalsspalten:

- **MCC** (Mobile Country Code)
- **MNC** (Mobile Network Code)
- **LAC** (Location Area Code)
- **CI** (Cell Identifier)
- **UARFCN** (UTRA Absolute Radio Frequency Channel Number)
- **PSC** (Primary Synchronization Code)

Wie bereits in Abschnitt 4.1.2 auf Seite 80 beschrieben, scheint der chinesische 3G-Standard CDMA dem europäischen Mobilfunkstandard bei der Identifikation der Funksender angepasst worden zu sein. Demnach dürfte die Tabelle Apple dazu dienen, offensichtliche Überschneidungen in der Benennung der einzelnen Merkmale abzufangen.

Die übrigen Spalten entsprechen der bekannten Repräsentation für Funkzellen, wie bereits in Abschnitt 4.1.2 auf Seite 76 beschrieben. Was die Darstellung der Daten auf einer Karte betrifft, so dürfte sich ebenfalls kein Unterschied zu den Erfahrungen der Ortungsdaten von Apple ergeben.

CellLocationLocal, LTECellLocationLocal

In der iOS-Ortungsdatenbank befinden sich auch Tabellen mit ungewöhnlichen Ortsangaben sowie auffällig identischen Sendereichweiten. Der Bezeichnung nach gehören die Tabellen CellLocationLocal und LTECellLocationLocal zu den von Apple übersandten Datentabellen. Entsprechend der Spaltenbezeichner handelt es sich bei den Datensätzen um Funkzellenstandorte.

Das Suffix »Local« deutet zunächst auf eine mögliche Verbindung zu privaten oder häufigen Standorten des Nutzers hin. Tatsächlich wurden im Rahmen von Untersuchungen aber auch Datenpositionen festgestellt, die nicht zu dieser Annahme passen. So existieren z. B. Standorte direkt an Autobahnabfahrten oder sehr weit entfernt vom Heimatort des Gerätenutzers. Bei den Daten dürfte es sich um Rückfallpositionen im Falle fehlender Internetverbindung handeln. So könnte zumindest eine grobe Verortung unmittelbar durchgeführt werden (z. B. während einer Autobahnfahrt).

Aufgrund der konstant großen Reichweiteangaben von 5005m spielen die Daten für eine forensische Betrachtung allerdings keine all zu große Rolle. Erstens ist davon auszugehen, dass die Angabe der Ungenauigkeit nicht vom Senderadius eines Funksenders stammt und zweitens dürfte der Bereich häufig zu groß sein, um einen konkreten Aufenthaltsort eines Tatverdächtigen nachzuweisen.

UnknownCellLocation (iOS7)

Die Tabelle mit der Bezeichnung UnknownCellLocation existiert nur in iOS7. Sie dürfte Apple dazu dienen, Probleme bei der Verortung von bis dato unbekannter Mobilfunktechnologien zu verhindern. So lassen sich Sendestationen mit unbekannten oder gleich lautenden Bezeichnungen von Basisstationen zur Ortung nutzen. Etwa zeitgleich wurde Ende 2013 weltweit begonnen, dass LTE-Netz aufzubauen.

Die Einträge in der Tabelle entsprechen den Spalten mit Zeitangaben, Standortdaten sowie Genauigkeit und Verlässlichkeit der bekannten Repräsentation für Funkzellen (vgl. Abschnitt 4.1.2 auf Seite 76). Auch hier lässt sich hinsichtlich der Darstellung der Standorte auf einer Karte kein Unterschied zu den bereits beschriebenen Erfahrungen erkennen.

WifiLocation (Besonderheiten ab iOS9)

Mit der Einführung von Apple iOS9 ist die Tabelle WifiLocation innerhalb der Datenbank cache_encryptedA.db verschwunden. Dafür existiert seit iOS9 eine neue Datenbankdatei mit der Bezeichnung cache_encryptedB.db im selben Verzeichnis. Offensichtlich versucht Apple ein neues System zur WLAN-Verortung zu etablieren.

Zumindest erklärt sich durch die neue Datenbankdatei mit dem Suffix »B« die Lücke in der Benennung der Datenbank der Bewegungsdaten (cache_encrypted<u>C</u>.db) und der Ortungsdatendatenbank (cache_encrypted<u>A</u>.db). Mit der Einführung von iOS10 verschiebt Apple auch die übrigen Spalten aus der Datei cache_encryptedA.db in die neue Datenbank und verzichtet fortan auf die »A«-Datei.

Die auffälligste Änderung liegt in der Speicherung der MAC-Adressen im Integer-Format anstelle der gebräuchlicheren Darstellung im hex-Format. So wird beispielsweise aus 00:1a:f0:5d:0d:a7 (hex) die MAC-Adresse 115701779879 (int) (vgl. [Ass16]). Der Vorteil dieser Art der Speicherung dürfte darin liegen, die direkte Referenzierung mit den übrigen Tabellen als primary-Key zu den foreign-Keys der anderen Tabellen zu ermöglichen.

Darüber hinaus hat Apple zwei weitere Spalten mit den Bezeichnern Score und Reach ergänzt. Erste Analysen der Werte aus der Spalte Reach lassen erkennen, dass die Werte größer oder gleich dem Wert in der Spalte HorizontalAccuracy sind. Eine Vermutung zu diesem Zusammenhang ist, dass der Wert in der Spalte Reach die maximale Sendereichweite aus Apples crowd-source Datenbank darstellt, wohingegen der Wert HorizontalAccuracy einer vom Gerät aktuell berechneten (mitunter geringeren) Sendereichweite entspricht.

4.1.3 Ortungsdaten für Apple

Wie in Abschnitt 1.1.2 auf Seite 8 beschrieben, müssen die Positionsdaten möglichst vieler Sender bei Apple vorliegen, damit Lokalisierung auf Basis von aGPS funktionieren kann. Auf iOS-Geräten existieren hierfür spezielle Tabellen in der Ortungsdatenbank, die im Folgenden beschrieben werden.

Harvesting-Tabellen

Bereits Ende 2011 wurden während eigener Untersuchungen noch vor Beginn dieser Arbeit neben den Tabellen CellLocation und WifiLocation jeweils eine zweite Tabelle mit der Endung »harvest« festgestellt (vgl. [(4r11]). Offensichtlich speichern Apple-Smartphones häufiger Geoinformationen zu Funksendern in der Umgebung. Die Daten werden unterwegs geerntet und später an Apple gesendet. Ins Englische übersetzt bedeutet ernten »to harvest«, daher auch der Suffix »harvest« an dieser Art von Tabellen.

Der Zugriff auf den Datenbestand der »harvest«-ing Tabellen ist aus forensischer Sicht sehr viel interessanter, als die Daten der zuvor beschriebenen Tabellen mit Ortungsdaten von Apple. Die Problematik der vielen unterschiedlichen Standorte zu einem Zeitpunkt in den von Apple übertragenen Standortdaten (vgl. Abschnitt 4.1.2 auf Seite 81) existiert bei dieser Art von Tabellen nämlich nicht. Zwar kommt es vor, dass mehrere Tabelleneinträge den selben Zeitstempel aufweisen, der Standort der unterschiedlichen Sender aus der Umgebung bleibt aber gleich. Zusätzlich zur Position ermittelt das Gerät noch Merkmale zur Identifizierung (MCC, MNC, LAC und CellID oder die MAC-Adresse) sowie Informationen zur Sendereichweite und der Empfangsstärke (RSSI).

Die Genauigkeitsangabe der Accuracy-Werte liegt im Bereich von unter 60m und damit weit unter den im Kilometerbereich liegenden Werten der CellLocation-Tabelle. Die Werte zur Verlässlichkeit bewegen sich ebenfalls mit 90% oberhalb der 70% der WiFiLocation- und 50% der CellLocation-Tabellen.

Dafür ist die Anzahl der Einträge in dieser Art von Tabellen leider viel geringer, wenn überhaupt noch Daten zum Zeitpunkt der Auswertung existieren. Zudem variiert die Anzahl der Datensätze pro Tabelle je nach iOS Version (vgl. Tab. 4.4 auf der nächsten Seite). Die dort angegebenen Werte sind jeweils nach längeren

Autofahrten (min. 300km) bei dauerhafter Nutzung der Ortungsdienste durch Navigationssoftware ermittelt worden. Die Daten wurden anschließend erhoben, bevor die Daten nach der Übertragung an Apple bereinigt werden konnten. Die Tabelle *LocationHarvest*, in welche bei der Navigation sehr viele Daten gespeichert werden, sticht mit einer enorm hohen Anzahl an Einträgen hervor.

	bis iOS 4.3.2	**ab iOS 4.3.3**	**iOS 5.x**	**ab iOS 6.x**	**ab iOS 10**
CellLocation	>8500	~ 1000	~ 500	~ 2000	~ 3500
WiFiLocation	>80000	~ 10000	~ 5000	~ 500	~ 27000
AppHarvest (>iOS6)	na	na	na	~ 20	~ 80
LocationHarvest	~2400	~ 1400	0	~ 17000	~ 18000
CellLocationHarvest	~ 90	1	~ 30	~ 500	~ 300
WifiLocationHarvest	~ 130	~ 130	~ 80	~ 300	~ 180

Tab. 4.4: Anzahl der Einträge verschiedener Harvesting-Tabellen in iOS bei gezielter Nutzung der Ortungsdienste und ohne WLAN-Verbindung.

Die Harvest-Tabellen beinhalten sehr häufig keine Daten, da die Dateninhalte nach der erfolgreichen Übertragung an Apple umgehend gelöscht werden. Die Übertragung zum Hersteller findet allerdings nur statt, wenn eine WLAN-Verbindung besteht. Zur Konservierung dieser Daten ist es deshalb äußerst wichtig, den Flugmodus bei der Sicherstellung von mobilen Endgeräten direkt zu aktivieren.

Der Datenumfang bzw. die Vollständigkeit der Daten wurde mit der Einführung von iOS4.3.3 durch Apple sehr stark beschränkt (vgl. Tab. 4.5). Nach Ablauf von mittlerweile nur noch 5 Tagen werden die alten Datenbestände gelöscht. Die Nachvollziehbarkeit von retrograden Ortungsdaten auf Basis von Apple-Geräten wird dadurch für die Mobilfunkforensik äußerst nachteilig beeinflusst.

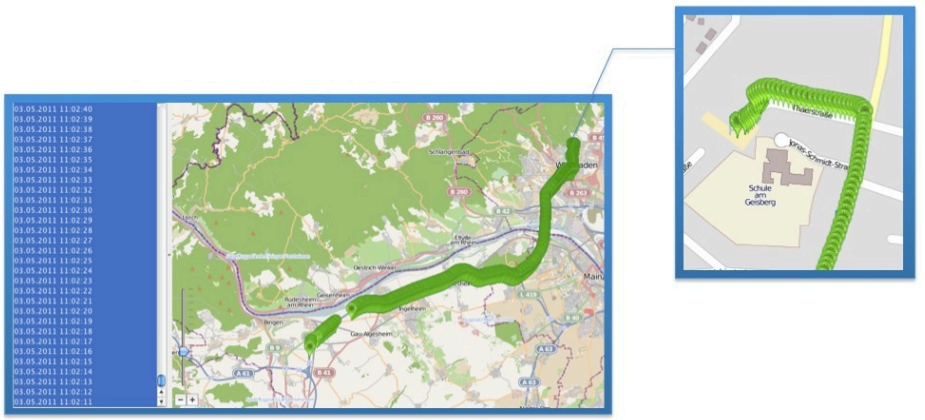
	bis iOS 4.3.2	**ab iOS 4.3.3**	**ab iOS 5.x**	**iOS 10**
Dateiname	consolidated.db	cache.db	cache_encryptedA.db	cache_encryptedB.db
Speicherort	Sync per iTunes auf PC/Mac	nur noch auf dem Gerät	nur noch auf dem Gerät, verschlüsselt (wenn gesperrt)	nur noch auf dem Gerät, verschlüsselt (wenn gesperrt)
Dateigröße (exemplarisch)	12,8 mb	1,4 mb	0,5 mb	24,7 mb
Speicherumfang	9 Monate (unbegrenzt)	<7 Tage	<5 Tage	<5 Tage

Tab. 4.5: Speicherumfang verschiedener Ortungsdatenbanken in iOS 4.x - iOS 10.

LocationHarvest

In der Tabelle LocationHarvest lassen sich je nach Dauer der Reise und iOS-Version mehr als 15000 Einträge feststellen. Die in Abb. 4.9 dargestellten Wegpunkte stammen z. B. aus einer Testfahrt von unter 1h mit dem Auto auf dem Weg nach Wiesbaden zum Hauptsitz des BKAs im Jahre 2012. Auffallend und aus forensischer Sicht erfreulich ist die hohe Dichte an Wegpunkten mit einer beinahe sekündlichen Erhebung von Positionsdaten.

Neben der hohen Genauigkeit, zu erkennen an den kleinen Zahlenwerten der horizontalen- sowie vertikalen Accuracy-Spalten (siehe Abb. 4.9), ist der Grad der Verlässlichkeit mit 90% (in Abb. 4.9 Spalte »Co..«) ebenfalls sehr hoch. Zusätzlich können noch weitere wertvolle Informationen für die forensische Untersuchung gewonnen werden. So werden zu sehr vielen Einträgen Informationen zur aktuellen Geschwindigkeit sowie der Richtung der Bewegung gespeichert.



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...	2.366444444444444	94.0	90	48C1CCD4-26B7-40A3-BA63-3D5CD48B9BD1	502
326131213.533959	50.0865217833333	8.24409906666667	162.95795319...	132.225...	228.34367325...	2.469333333333333	96.0	90	48C1CCD4-26B7-40A3-BA63-3D5CD48B9BD1	502

Abb. 4.9: Auszugsweise Spaltenauflistung der Tabelle LocationHarvest (iOS4.3.2) inkl. Darstellung der Wegpunkte auf einer Karte. Quelle: Eigene Darstellung. Kartenmaterial: © OpenStreetMap Mitwirkende 2011.

Die Spalten der Tabelle **LocationHarvest** beinhalten folgende Informationen:

- Eine Zeitangabe, welche den Zeitpunkt der Datenerhebung festhält
  - **Timestamp** (im CFAbsolute-Time Datenformat vgl. S. 77)
- Den Standort des Gerätes
  - **Latitude, Longitude** (in Grad mit Dezimalstellen)

- Die Genauigkeit der aktuellen Verortung
  - **Horizontal- und Vertical- Accuracy** (in Meter)
- Die Höhe des Gerätes in Meter über NN
  - **Altitude**
- Eine Geschwindigkeits- sowie Kursangabe
  - **Speed** (in Meter/Sekunde)
  - **Course** (in math. Gradangabe mit 0 = Nord, »-1« für nicht verfügbar)
- Eine Verlässlichkeitsangabe bzgl. des Datenursprungs
  - **Confidence** (entspricht mit 90% einer sehr hohen Genauigkeit)
- Ungeklärte Angaben
  - **TripId**
  - **Context**

Der Aufbau und die Bedeutung der Zeichenketten **TripId** sowie die Werte für **Context** konnten bislang nicht abschließend geklärt werden. Es dürfte sich hierbei um anonymisierte Hinweise auf das Gerät oder einen bestimmten Routentyp handeln. Apple scheint bemüht, stets weitere Merkmale hinsichtlich des Umstandes der Erhebung der Ortungsinformation zu erheben. Mithilfe solcher Informationen ist es z. B. möglich die Aktualisierungsintervalle so anzupassen, dass sich die Akkulaufzeit des Gerätes erhöht.

Bis iOS 9 sind noch folgende Spalten hinzugekommen:

- **RAT** (Radio Access Type (s.u.), deu: Mobilfunk Zugangsmethode)
- **MCC** (Mobile Country Code, deu: Länderkennung)
- **MNC** (MobileNetwork Code, deu: Netzwerkkennung)
- **BundleId** (kanonischer Projektname)
- **BundleIds** (verschiedene BundleIds, zur Unterscheidung von Applikationen)
- **MotionActivityType** (Aktivitätstyp der Bewegung, siehe nächste Seite)
- **MotionActivityConfidence** (Erkennungsrate bzgl. der Bewegungsart)
- **MotionVehicleConnectedStateChanged** (?)
- **MotionVehicleConnected** (Verbindung mit einem Fahrzeug? vgl. S. 92)

Die Spalte **Radio Access Type** dürfte Apple zur Unterscheidung verschiedener Mobilfunkstandards dienen (vgl. [Rev12]). So lassen sich z. B. die Funkzellen

diverser Mobilfunkanbieter in unterschiedlichen Mobilfunknetzen oder Mobilfunkgenerationen (UMTS, LTE, CDMA etc.) anhand des RAT unterscheiden.

In der Spalte **BundleId** wird der Name der Ortungs-App gespeichert. Die von Apple vorgeschriebene kanonische Kennung folgt dem Schema eines Uniform Type Identifier (UTI)s (vgl. [App16b]: com.organization.application). Anhand dieser Informationen der verwendeten App zum Zeitpunkt der Datenerhebung lassen sich weitere Rückschlüsse auf die zu erwartende Genauigkeit der Standortdaten ableiten. Wie bereits mehrfach angeführt, setzen Navigationsanwendungen eine höhere Präzision voraus als z. B. Unterhaltungs-Apps.

In iOS7 werden darüber hinaus erstmals konkret Bewegungsdaten gespeichert. In Geräten mit entsprechendem Sensor (ab iPhone5s mit M7 Ko-Prozessor [Bal13]) ist es fortan möglich, anhand von Bewegungsmustern verschiedene Arten der Fortbewegung zu unterscheiden (vgl. Spalte **MotionActivityType** auf S. 89).

Wie in Apples Entwicklerdokumentation [App16a] beschrieben, lassen sich die folgenden Bewegungsarten unterscheiden:

- **stationary** (stationär, keine Bewegung)
- **walking** (gehen)
- **running** (laufen)
- **automotive** (mit dem Auto unterwegs)
- **cycling** (während des Radfahrens)
- **unknown** (unbekannt).

Insbesondere unter dem Gesichtspunkt der Energieeinsparung ist es von Vorteil, wenn das System in der Lage ist zu beurteilen, in welchen Zeitintervallen der Nutzer auf aktuelle Positionsdaten angewiesen ist. Gar keine Positionsupdates dürfte z. B. ein Gerät benötigen, dass über eine längere Zeit keine Bewegung erfahren hat. Hier kann der Ortungsdienst entsprechend länger deaktiviert bleiben, um keine unnötige Energie zu verbrauchen. Dementgegen benötigen Läufer regelmäßig, aber noch weniger häufig als ein Radfahrer aktualisierte Daten. Ein Autofahrer auf der Autobahn hingegen wird sehr häufig neue Standortdaten benötigen, da sich sein Standort sehr schnell und darüber hinaus mehrere Meter pro Sekunde ändert.

Entgegen der oben getroffenen Feststellung, dass ein Autofahrer mehr Energie für häufige Standortupdates benötigt, zeigt die Praxis aktuell eine andere Ten-

denz: 1 Stunde Laufen verbraucht mehr Akku als 1h im Auto navigieren. Denn im Gegensatz zum Autofahrer, der sich aller Wahrscheinlichkeit nach auf einer befestigten Straßen und gestützt auf eine Navigationssoftware befindet, kann ein Radfahrer auch auf »ungeführten« Strecken (ohne zusätzliche Stützmöglichkeit einer Straßenkarte) unterwegs sein. Der Läufer wird sogar sehr wahrscheinlich auf ungeführten Routen unterwegs sein und benötigt von daher regelmäßiger Updates zur Position über das Ortungssystem des iPhones.

Die Spalten **BundleId**, **MotionActivityType** und **MotionActivityConfidence** könnten Apple ferner dazu dienen, die Erkennung der Bewegungsmuster durch Korrelation der aktiven App zur angenommenen Bewegungsart nach der Übertragung der Daten an Apple retrograd zu verbessern.

Bezüglich der in iOS9 hinzugekommenen Spalten **MotionVehicleConnected** und **MotionVehicleConnectedStateChanged** lassen sich derzeit nur Vermutungen anstellen. Hinweise auf die Intention Apples können sich allenfalls auf die Entwicklerdokumentation zum Core Motion Framework stützen (siehe [App16d]). Aufgrund der Bezeichnung der beiden Spalten kann ggf. davon ausgegangen werden, dass die Bestrebung seitens Apple drahtgebundene Schnittstellen in Fahrzeugen zu nutzen, auch einen Einfluss auf die Ortungsdienste haben könnte. Die Verortung in Kraftfahrzeugen mithilfe von permanent mit Strom versorgten mobilen Endgeräten könnten den Fokus wieder von der Energieeinsparung in Richtung Erhöhung der Präzision lenken und hierzu wieder mehr Sensoren sowie kleinere Abfrageintervalle nutzen.

Aufgrund der restriktiven Datenspeicherung seit iOS4.3.2 und der Tatsache, dass die Datenbestände der Harvest-Tabellen sofort nach der Übertragung gelöscht werden (vgl. Abschnitt 4.1.3 auf Seite 88) können nur in begrenztem Maße Untersuchungen bzgl. der Inhalte der Tabelle LocationHarvest durchgeführt werden. Darüber hinaus ließen sich in iOS5 keine Hinweise auf die Speicherung von Daten in der Tabelle LocationHarvest feststellen (vgl. Tab. 4.4 auf Seite 88). So hatte es zunächst den Anschein, Apple verzichte nach dem Locationgate-Skandal (vgl. [App11]) fortan auf die Speicherung der Reisedaten von iOS-Benutzern. Mit Einführung von iOS6 und insbesondere nach dem Erscheinen von iOS7 scheint die Sammel- und Speicherwut aber wieder zugenommen zu haben.

CellLocationHarvest

Der Datenumfang der Tabelle **CellLocationHarvest** tendiert ebenfalls gegen Null. Sofern sich hier jedoch Daten erheben lassen, weisen diese, wie in Abb. 4.10 zu erkennen, ebenfalls den tatsächlichen Gerätestandort aus. Wie auf Seite 87 zu Beginn dieses Kapitels beschrieben, sammeln die Apple-Geräte in dieser Tabelle gezielt Informationen zu den umliegenden Mobilfunksendern. Die Genauigkeit sowie Verlässlichkeit der Daten kann als sehr gut angenommen werden. Dieser Umstand begründet sich insbesondere in der Tatsache, dass Ortsinformationen nur dann erhoben und gespeichert werden, wenn die Präzision der Verortung annähernd der Qualität von GPS entspricht.

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

Abb. 4.10: Kartendarstellung einzelner Wegpunkte inkl. Inhalte der Tabelle CellLocationHarvest einer iOS4.3.2 Ortungdatenbank. Quelle: Eigene Darstellung. Kartenmaterial: © OpenStreetMap Mitwirkende 2011.

Die Spalten der Tabelle **CellLocationHarvest** enthalten folgende Informationen:

- Eine individuelle Repräsentation der Datenquelle mit weiteren Merkmalen
  - **MCC, MNC, LAC, CI,** (zur Identifikation der Funkzelle)
  - **RSSI** (Feldstärke in dBm vgl. [DG16] S.3 unten)
  - **Operator** (Mobilfunkanbieter)
  - **Transmit** (ungeklärt, s.u.)
  - **BundleId** (kanonischer Projektname)
- Eine Zeitangabe, welche den Zeitpunkt der Datenerhebung festhält
  - **Timestamp** (im CFAbsolute-Time Datenformat vgl. S. 77)
- Den Standort des Gerätes
  - **Latitude, Longitude** (in Grad mit Dezimalstellen)

- Die Genauigkeit der aktuellen Verortung
  - **Horizontal- und Vertical- Accuracy** (in Meter)
- Die Höhe des Gerätes in Meter über NN
  - **Altitude**
- Eine Geschwindigkeits- sowie Kursangabe
  - **Speed** (in Meter/Sekunde)
  - **Course** (in math. Gradangabe mit 0 = Nord, »-1« für nicht verfügbar)
- Eine Verlässlichkeitsangabe bzgl. des Datenursprungs
  - **Confidence** (entspricht mit 90% einer sehr hohen Genauigkeit)

Bezüglich der Bedeutung der Einträge in der Spalte **Transmit** können maximal Vermutungen angestellt werden. Dem Namen nach dürften die Werte mit einer nicht näher bestimmten Übertragung (engl. transmission) zusammenhängen. Alles weitere wäre ohne entsprechende Werte (bisher nur »-1«-Werte) reine Spekulation und dürfte bei der forensischen Betrachtung von Ortungsdaten ohnehin nicht weiterhelfen. Bis iOS9 kommen noch folgende Spalten hinzu:

- **ARFCN** (Absolute Radio Frequency Channel Number vgl. S. 80)
- **PSC** (Primary Synchronization Code)
- **RSCP** (Received Signal Code Power)
- **ECNo** (Received Energy per Chip divided by total Noise power density)
- **RAT** (Radio Access Type, deu: Mobilfunk Zugangsmethode)
- **MotionActivityType** (Aktivitätstyp der Bewegung, siehe Seite 91)
- **MotionActivityConfidence** (Erkennungsrate bzgl. der Bewegungsart)
- **MotionVehicleConnectedStateChanged** (?)
- **MotionVehicleConnected** (Verbindung mit einem Fahrzeug? vgl. S. 92)

Bei den weiteren Parametern handelt es sich nach [BS09] um interferenzfreie Werte zur Abschätzung der Sende- bzw. Empfangsleistung im UMTS Mobilfunknetz. So berechnet sich z. B. die Energie pro Chip ohne Störeinflüsse als **ECNo = RSCP / RSSI**. Die Angaben sind für die Berechnung von tatsächlichen Empfangsstärken im UMTS- bzw. LTE-Netz von Bedeutung, da Nachbarzellen auf der gleichen Frequenz strahlen wie der aktuell genutzte Sender (vgl. [BS09]). Anhand dieser Werte dürfte Apple in der Lage sein, die realen Standortdaten der Funksender noch genauer zu bestimmen als zuvor.

WifiLocationHarvest

In der Tabelle **WiFiLocationHarvest** werden bei entsprechender Genauigkeit und Verlässlichkeit der Positionsschätzung WLAN-Sender in der Umgebung des iOS-Gerätes erhoben und gespeichert. Verglichen mit der Tabelle CellLocation-Harvest ist die Anzahl an Einträgen leicht erhöht. Dieser Umstand ist dadurch zu erklären, dass die WLAN-Abdeckung (in urbanen Gegenden) höher ist als die Abdeckung im Bereich Mobilfunk.

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

Abb. 4.11: Darstellung ausgewählter Wegpunkte inkl. Kartendarstellung und Inhalte der Tabelle WiFiLocationHarvest (iOS4.3.2)

Die Spalten der Tabelle **WifiLocationHarvest** beinhalten folgende Informationen:

- Eine individuelle Repräsentation der Datenquelle mit weiteren Merkmalen
  - **MAC** (zur Identifikation des Accesspoints)
  - **Channel** (Sendekanal auf dem der AP überträgt)
  - **Hidden** (ist der AccessPoint versteckt? 0=nein, 1=ja)
  - **RSSI** (Feldstärke in dBm vgl. [DG16] S.3 unten)
  - **Age** (unbekannt s.u.)
  - **BundleId** (kanonischer Projektname)
- Eine Zeitangabe, welche den Zeitpunkt der Datenerhebung festhält
  - **Timestamp** (im CFAbsolute-Time Datenformat vgl. S. 77)
- Den Standort des Gerätes
  - **Latitude, Longitude** (in Grad mit Dezimalstellen)
- Die Genauigkeit der aktuellen Verortung
  - **Horizontal- und Vertical- Accuracy** (in Meter)

- Die Höhe des Gerätes in Meter über NN
  - **Altitude**
- Eine Geschwindigkeits- sowie Kursangabe
  - **Speed** (in Meter/Sekunde)
  - **Course** (in math. Gradangabe mit 0 = Nord, »-1« für nicht verfügbar)
- Eine Verlässlichkeitsangabe bzgl. des Datenursprungs
  - **Confidence** (entspricht mit 90% einer sehr hohen Genauigkeit)

In der Spalte **Age** werden kleine Dezimalwerte gespeichert. Dem Namen nach könnte die Bedeutung dieser Einträge einen Rückschluss auf das Zeitintervall für die Empfangsdauer des jeweiligen WLAN-AccessPoints in Sekunden geben. Im Umfeld von BigData könnte Apple versuchen mithilfe weiterer Kennzahlen (vgl. **Transmit** Abschnitt 4.1.3 auf Seite 94) die Empfangsbereiche der Senders besser zu verorten. Für die forensische Betrachtung dürfte die Spalte hingegen ohne Bedeutung sein.

Bis iOS 9 kommen wieder folgende Spalten hinzu:

- **MotionActivityType** (Aktivitätstyp der Bewegung, siehe Seite 91)
- **MotionActivityConfidence** (Erkennungsrate bzgl. der Bewegungsart)
- **MotionVehicleConnectedStateChanged** (?)
- **MotionVehicleConnected** (Verbindung mit einem Fahrzeug? vgl. S. 92)

Die Bedeutung der **Motion***-Spalten wurde bereit in Abschnitt 4.1.3 auf Seite 91 ausführlich erläutert.

Zusammenfassend lässt sich festhalten, dass die erhobenen Standortdaten zwar nur punktuell und teilweise auch nur unter ganz bestimmten Umständen, z. B. während einer Reise, erhoben werden. Dafür weisen die Daten aber die für die forensische Untersuchung so wichtige Eindeutigkeit und Genauigkeit auf.

Der Vergleich zu den Harvest-Tabellen wurde bewusst an ein und derselben Versuchsfahrt dargestellt. So lässt sich sehr gut erkennen, dass sich je nach Fokus der jeweiligen Tabelle die zeitliche Auflösung, die Anzahl der erhobenen Standorte und auch die Präzision der gespeicherten Ortsinformationen unterscheidet (vgl. Abb. auf Seite 89, 93 sowie Seite 95). Dementgegen sind die forensischen Implikationen bzgl. der Harvest-Tabellen für jede Tabelle und in allen bisherigen iOS-Versionen gleichermaßen als sehr gut zu bewerten.

Weitere Harvest-Tabellen in Apples Ortungsdatenbank

Im Laufe der Entwicklung von iOS hat Apple immer wieder Änderungen an der Ortungsdatenbank vorgenommen. Was die Qualitätskriterien bzgl. Genauigkeit, Verlässlichkeit und Vollständigkeit angeht, so gelten die bislang beschriebenen Erkenntnisse auch für die zusätzlichen Tabellen neuerer iOS-Versionen.

AppHarvest (ab iOS5) Apple erhebt seit iOS5 mitunter zusätzlich Standortdaten, wenn iOS-Anwendungen auf die Ortungsdienste zugreifen. Obendrein werden die Daten nicht sofort nach der Übertragung an Apple gelöscht. Insofern ist die Tabelle AppHarvest für die Mobilfunkforensik von besonderem Interesse, da sich in ihr häufiger noch Datenspuren ermitteln lassen, als dies in den anderen Harvesting-Tabellen möglich ist.

Zudem scheint die Erhebung von Standortdaten ungeachtet der Verfügbarkeit von GPS ab einer gewissen Genauigkeit der Positionsberechnung zu erfolgen. Bei eigenen Untersuchungen im Rahmen von Live-Auswertungen an Orten ohne GPS-Verfügbarkeit (z. B. innerhalb von Gebäuden) konnte festgestellt werden, dass trotzdem Positionsdaten erhoben werden. Die Genauigkeit sowie Verlässlichkeit entspricht dabei immer noch GPS-Niveau.

Zusätzlich zu den typischen Merkmalen anderer Harvesting-Tabellen enthält die Tabelle AppHarvest noch folgende Spalten (vgl. Abschnitt 4.1.3 auf Seite 93):

- **State** (aktiv oder im Hintergrund laufend)
- **Age** (hohe Werte, Angabe in Sekunden?)
- **RoutineMode** (0)
- **LocationOfInterestType** (-1)
- **Sig** (byte-array len:57)

Von den oben aufgeführten Informationen ist besonders die Spalte Status (engl. state) hervorzuheben. Es ist bekannt, dass mobile Anwendungen je nach Berechtigung auch im Hintergrund und ohne Zutun des Nutzers Ortungsdaten erheben können. Für solche Apps dürfte dann der Status auf inaktiv gesetzt sein. Interessant ist die Speicherung des Status insofern, dass iOS bei einer App im Hintergrund die Genauigkeit der Positionsberechnung verringern könnte, um Energie zu sparen.

PassHarvest (ab iOS7) Die Tabelle PassHarvest besitzt die gleichen Spalten wie die Tabelle AppHarvest (vgl. Abschnitt 4.1.3 auf der vorherigen Seite). Zusätzlich werden in der Tabelle neben dem Standort potentiell noch weitere Daten zum Diensteanbieter gespeichert:

- PassTypeId (»0«)
- AssociatedStoreIds (»na«)
- PassSource (»-1«)
- Age (»-1«)
- Sig (»-1«)

Die Tatsache, dass die Spalten bislang noch nicht sinnvoll belegt sind, lässt zwar auf eine zukünftige Verwendung schließen, erlaubt aber aktuell keine konkrete Aussage zur tatsächlichen Bedeutung der Informationen. Je nach Fall ließe sich im Rahmen der Mobilfunkforensik anhand der Daten in AssociatedStoreIDs und Age spekulieren, ob ein Nutzer einen bestimmten Apple-Partner zum fraglichen Zeitpunkt für wie lange besucht hat.

LteCellLocationHarvest (ab iOS5) Die Tabelle LteCellLocationHarvest wurde mit iOS5 eingeführt. Zusätzlich zu den typischen Harvesting-Merkmalen (siehe Abschnitt 4.1.3 auf Seite 93) existieren folgende Spalten:

- CellLatitude (0.000000)
- CellLongitude (0.000000)

Der Bezeichnung nach könnte sich Apple darauf vorzubereiten, dass einige Provider in Zukunft die Standorte der Mobilfunkantennen übertragen. Bis zuletzt konnten allerdings nur float-Werte von 0.000000 (s.o.) festgestellt werden.

LteCellLocationNeighborsHarvest (seit iOS9) In der Tabelle LteCellLocationNeighborsHarvest wurden ergänzende Informationen von LTE-Funksender in der Umgebung (Neighbors) gespeichert. Die Tabelle dürfte Apple dazu dienen, Interferenzen bei der Funkzellenkartierung zu eliminieren. In iOS10 wurde die Tabelle umbenannt in LteCellNeighborsLocationHarvest und enthält fortan nur noch die Spalten: Timestamp, ECN0, PID, RSCP, UARFCN und BAND_INFO. Ohne Geokoordinaten ist die Tabelle so für die forensische Untersuchung von Standortdaten uninteressant geworden.

CdmaCellLocationHarvest (ab iOS7) Die Tabelle CdmaCellLocation-Harvest besitzt keine nennenswerten Spaltenbezeichner, außer den zuvor im Rahmen der Beschreibung der Tabelle CelllocationHarvest bereits diskutierten Spalten (vgl. Abschnitt 4.1.3 auf Seite 93). Ohnehin ließen sich auf den untersuchten Geräten bzw. in Europa aufgrund fehlender Sender keine CDMA-Daten ermitteln. Es ist aber zu vermuten, dass die Qualität der Dateneinträge der Genauigkeit, Verlässlichkeit sowie Vollständigkeit den Erfahrungen der übrigen Harvest-Tabellen folgt.

CdmaCellNeighborsLocationHarvest (seit iOS9) Wie eben dargestellt dürfte die Tabelle CdmaCellNeighborsLocationHarvest für Nutzer europäischer Netze nicht relevant sein, da in ihr keine Ortsinformationen zu erwarten sind. Wie in Abschnitt 4.1.3 ausgeführt, senden CDMA bzw. UMTS Mobilfunkstationen auf denselben Frequenzen. So sind Tabellen zu Nachbarzellen im CDMA-Netz zwar für Apple sinnvoll zur Konsolidierung von Daten, jedoch weniger relevant für die Mobilfunkforensik.

CellNeighborsLocationHarvest (seit iOS9) Wie bei der Beschreibung der Tabelle CdmaCellNeighborsLocationHarvest bereits ausgeführt, dürfte auch die Tabelle CellNeighborsLocationHarvest Apple bei der Konsolidierung von UMTS-Funknetzen helfen. In der Praxis wurden in dieser Tabelle allerdings zu keiner Zeit Ortungsdaten festgestellt. Eine Aussage zur Qualität der Ortungsdaten kann so nicht getroffen werden, dürfte sich aber nicht wesentlich von den Merkmalen anderer Harvesting-Tabellen unterscheiden.

PressureLocationHarvest (seit iOS9) Bisher konnten in dieser Tabelle bei keiner Untersuchung Daten festgestellt werden. Zusätzlich zu den bislang beschriebenen Harvesting-Merkmalen (siehe Abschnitt 4.1.3 auf Seite 93) enthält die Tabelle ferner noch die Spalten: BundleId, Provider und Floor. Durch die Integration eines Barometers im iPhone6 und neuer (vgl. [App16g]) ist es für Apple möglich, Höhenangaben bzw. -unterschiede auch ohne GPS-Verfügbarkeit zu bestimmen. So kann Apple insbesondere die Schätzung des Stockwerks (vgl. floor) im Innenbereich (engl. indoor) und somit die Kartierung von Gebäuden verbessern.

IndoorWifiHarvest (seit iOS9) Auffällig bei der Tabelle IndoorWifiHarvest ist, dass die typischen Harvesting-Merkmale (siehe Abschnitt 4.1.3 auf Seite 93) wie auch in der oben beschriebenen Tabelle LteCellLocationNeighborsHarvest fehlen. Zudem konnten in der Tabelle bislang noch keine Einträge festgestellt werden. Die Bewertung der Genauigkeit der Dateneinträge für eine forensische Untersuchung erübrigt sich ohnehin, da keine Standortdaten existieren.

IndoorLocationHarvest (seit iOS9) Bisher konnten bei Untersuchungen der Tabelle PressureLocationHarvest ebenfalls noch keine Daten festgestellt werden. Analog zur Tabelle PressureLocationHarvest (siehe vorige Seite) beinhaltet sie ferner noch die Spalten: BundleId, Provider und Floor. Demnach könnte die Spalte Floor unter Umständen für eine forensische Betrachtung von Interesse sein, um den Aufenthaltsort bezüglich des Stockwerkes zu präzisieren.

UnknownCellLocationHarvest (iOS7) Wie bereits in Abschnitt 4.1.2 auf Seite 85 beschrieben, existierten UnknownCellLocation-Tabellen nur unter iOS7. Die Spalten mit Zeitangaben, Standorten sowie Genauigkeit und Verlässlichkeit folgen dem typischen Harvesting-Schema (siehe Abschnitt 4.1.3 auf Seite 93).

Es ist nachvollziehbar, dass Apple immer wieder darum bemüht ist, Informationen zu bislang unbekannten Funksendern zu erheben. Ein durchgängiges Schema scheint allerdings bislang noch nicht gefunden.

WtwLocationHarvest (seit iOS9) In der recht neuen Tabelle WtwLocationHarvest lassen sich regelmäßig unerwartet viele Einträge feststellen. Ferner löscht der Ortungsdienst die Daten auch bei bestehender Internetverbindung über WLAN nicht unmittelbar. In ersten Untersuchungen konnten mehrere hundert Einträge nach einem Tag Gerätenutzung festgestellt werden.

Der Sinn und Zweck dieser Tabelle ist bislang ungeklärt. Aus dem Tabellennamen lassen sich ebenfalls keine Hinweise auf Senderquellen, Applikationen oder sonstige Apple-Ambitionen ableiten. Diverse Verzeichnisse zu Akronymen lassen ggf. zwei Optionen für »Wtw« vermuten:

1. Well-to-Wheels: Im Kontext von Hybrid-Fahrzeugen
2. What-the-What: Unbekannte Sender (vgl. UnknownCellLocationHarvest)

Zusätzlich zu den Harvesting-Merkmalen (vgl. Abschnitt 4.1.3 auf Seite 93) sind in der Tabelle WtwLocationHarvest noch folgende Spalten enthalten:

- **MAC** (zur Identifikation des Accesspoints)
- **Channel** (Sendekanal auf dem der AP überträgt)
- **Hidden** (ist der AccessPoint versteckt? 0=nein, 1=ja)
- **RSSI** (Feldstärke in dBm vgl. [DG16] S.3 unten)
- **Age** (kleine Age Zeiten <2.0s)
- **BundleId** (kanonischer Projektname)
- **MotionActivityType** (Aktivitätstyp der Bewegung, siehe Seite 91)
- **MotionActivityConfidence** (Erkennungsrate bzgl. der Bewegungsart)
- **MotionVehicleConnectedStateChanged** (?)
- **MotionVehicleConnected** (Verbindung mit einem Fahrzeug? vgl. S. 92)

Die Verwendung der Daten im Kontext mit Hybrid-Fahrzeugen ergibt Sinn, wenn man die Spalten MotionActivity* bzw. MotionVehicle* betrachtet. Allerdings spricht auch sehr viel für die Erhebung von Geoinformationen zu bislang unbekannten Funksendern (What-the-What). Insbesondere die drei Spalten MAC, Hidden und Channel lassen sich häufig in WLAN-Tabellen finden. Die Genauigkeit der Geokoordinaten folgt den Erfahrungen der übrigen Harvesting-Tabellen und weist eine geringe Fehlertoleranz der Standorte aus.

Auffälligkeiten in iOS9 bzw. iOS10

Während der Weiterentwicklung der nativen Applikation iOSTracker bzw. der Untersuchung aktueller Veränderungen in iOS9.3.3 und 10.2 im Rahmen dieser Arbeit wurden weitere Datenbankdateien ermittelt, in denen Apple offensichtlich Daten des Systemdienstes (locationd) speichert. Die Dateien befinden sich wie immer im Verzeichnis `/private/var/root/Library/Caches/locationd` auf dem Gerät.

Mithilfe der nativen App iOSTracker und einem jailbroken Apple iPhone ist es möglich gewesen, die Unterschiede sowie die aktuellen Entwicklungen von Apple zu untersuchen. Im Folgenden sollen die hinzugekommen Dateien kurz vorgestellt sowie sowie deren Inhalte forensisch analysiert werden.

cache_encryptedB.db Wie bereits in Abschnitt 4.1.1 auf Seite 73 beschrieben, hat Apple den Dateinamen der Ortungsdatenbank mehrfach geändert. In iOS9 wurde die Tabelle WifiLocation aus der Datei cache_encryptedA.db entfernt und in eine eigene Datenbank (cache_encryptedB.db) verschoben.

Die Gründe hierfür lassen sich nur vermuten: So könnte ein Beweggrund in der Übersichtlichkeit liegen. Denn anstatt nur Positionsdaten zu WLAN-AccessPoints zu speichern, befinden sich in der Datenbank eine Vielzahl an Tabellen mit weiteren Informationen zu WLAN-Sendern. Die Tabellennamen folgen dabei dem Schema: wifi_tile_TILEy_TILEx (siehe Ausgabe 4.2).

```
sqlite> .tables
DatabaseIdentifier         wifi_tile_1403000_1874500
TableInfo                  wifi_tile_1403000_1875000
WifiLocation               wifi_tile_1403000_1875500
WifiLocationBoxes          wifi_tile_1403000_1876000
WifiLocationBoxes_node     wifi_tile_1403000_1876500
WifiLocationBoxes_parent   wifi_tile_1403000_1877000
WifiLocationBoxes_rowid    wifi_tile_1403500_1873000
WifiLocationCounts         wifi_tile_1403500_1873500
WifiTileHeader             wifi_tile_1403500_1874000
wifi_tile_1401500_1873000  wifi_tile_1403500_1874500
wifi_tile_1401500_1873500  wifi_tile_1403500_1875000
wifi_tile_1401500_1874000  wifi_tile_1403500_1875500
wifi_tile_1401500_1874500  wifi_tile_1403500_1876000
wifi_tile_1401500_1875000  wifi_tile_1403500_1877000
wifi_tile_1401500_1875500  wifi_tile_1404000_1873000
wifi_tile_1401500_1876000  wifi_tile_1404000_1873500
wifi_tile_1402000_1873000  wifi_tile_1404000_1874000
wifi_tile_1402000_1873500  wifi_tile_1404000_1874500
wifi_tile_1402000_1874000  wifi_tile_1404000_1875000
wifi_tile_1402000_1874500  wifi_tile_1404000_1875500
wifi_tile_1402000_1875000  wifi_tile_1404000_1876000
wifi_tile_1402000_1875500  wifi_tile_1404000_1876500
wifi_tile_1402000_1876000  wifi_tile_1404000_1877000
wifi_tile_1402000_1876500  wifi_tile_1404500_1873000
wifi_tile_1402000_1877000  wifi_tile_1404500_1873500
wifi_tile_1402500_1873000  wifi_tile_1404500_1874000
wifi_tile_1402500_1873500  wifi_tile_1404500_1874500
wifi_tile_1402500_1874000  wifi_tile_1404500_1875000
wifi_tile_1402500_1874500  wifi_tile_1404500_1875500
wifi_tile_1402500_1875000  wifi_tile_1404500_1876500
wifi_tile_1402500_1875500  wifi_tile_1404500_1877000
wifi_tile_1402500_1876000  wifi_tile_1405000_1874000
wifi_tile_1402500_1876500  wifi_tile_1405000_1874500
wifi_tile_1402500_1877000  wifi_tile_1405000_1875000
wifi_tile_1403000_1873000  wifi_tile_1405000_1875500
wifi_tile_1403000_1873500  wifi_tile_1405000_1876000
wifi_tile_1403000_1874000  wifi_tile_1405000_1877000
```

Terminalausgabe 4.2: Tabellenauflistung der cache_encryptedB.db Ortungsdatenbank. Nur in iOS9 existiert diese Ortungsdatenbank in der ausschließlich WLAN-Informationen gespeichert sind.

Die Tabelle WifiLocation der Ortungsdatenbank cache_encryptedB.db beinhaltet neben den bereits in Abschnitt 4.1.2 auf Seite 80 angegebenen Parametern für WLAN-AccessPoints folgende Merkmale:

- **glsmac** gespeichert als Integer (erlaubt Nutzung als foreign key)
- **score** in Prozent(?) (starke Zunahme zw. 30-50, schwache Steigung ab 60)
- **reach** in Meter(?) (30-300 schwach steigend, 300-2000 sehr starke Zunahme)

Die Tabelle **WifiTileHeader** enthält Informationen zu den **tile-**Tabellen:

- **tilex** (int)
- **tiley** (int)
- **southwestlatitude** (Grad)
- **southwestlongitude** (Grad)
- **deltalatitude** (0.05)
- **deltalongitude** (0.05)
- **Altitude** (in Meter) minimumAltitude $<$ Altitude $\leq$ maximumAltitude
- **minimumAltitude** (in Meter)
- **maximumAltitude** (in Meter)
- **generationtimestamp** (CFAbsolute-Time)
- **expirationage** (0; Bedeutung unbekannt)
- **version** (318; Bedeutung unbekannt)
- **flags** (0; Bedeutung unbekannt)
- **numberofindextiles** Anzahl der Tiles in der jeweiligen tile-Tabelle
- **accesstimestamp** in CFAbsolute-Time ($\geq$ generationtimestamp)
- **gizmosynctimestamp** in CFAbsolute-Time
  (generationtimestamp $\leq$ gizmosynctimestamp $\leq$ accesstimestamp)

Exemplarisch für die tiles-Tabellen enthält z. B. die Tabelle wifi_tile_x_y folgende zwei Spalten:

- **macaddress** (Integer Wert) und
- **accesspointdata** (ca. -2mio bis ca. 2mio).

Gemeinhin lässt sich aus den Tabellen WifiTileHeader bzw. den einzelnen Tiles bislang kein konkreter forensischer Ansatz ableiten. Da es sich vermutlich um eine Übergangslösung in iOS9 handelt, dürfte die Betrachtung dieser Daten keine Rolle in der Mobilfunkforensik spielen.

lockCache_encryptedA.db Zusätzlich zur Datenbank cache_encryptedA.db werden in iOS9 sog. SQLite-write-ahead-logs (kurz -wal Dateien) mitgeführt. Ziel dieser Daten ist es, die Konsistenz und Performance der SQLite-Datenbank zu verbessern. In früheren Versionen (vor iOS9.1) war diese Option nicht aktiviert, folglich existieren keine solchen Dateien.

Die Datenbank lockCache_encryptedA.db enthält häufig sehr viele Daten, was die forensische Auswertung der Standortdaten so interessant macht. Zudem ist der Bekanntheitsgrad der Datenbank sehr gering, da sie zum einen nur in iOS9 existiert und darüber hinaus nicht dem sonstigen Vorgehen Apples folgt. Die nachfolgende Terminalausgabe zeigt eine Übersicht aller Tabellen.

```
1
2  sqlite> .tables
3  CdmaCellLocation                   CellLocationLocalCounts
4  CdmaCellLocationBoxes              DatabaseIdentifier
5  CdmaCellLocationBoxes_node         DatabaseIdentifierCounts
6  CdmaCellLocationBoxes_parent       LteCellLocation
7  CdmaCellLocationBoxes_rowid        LteCellLocationBoxes
8  CdmaCellLocationCounts             LteCellLocationBoxes_node
9  CdmaCellLocationLocal              LteCellLocationBoxes_parent
10 CdmaCellLocationLocalBoxes         LteCellLocationBoxes_rowid
11 CdmaCellLocationLocalBoxes_node    LteCellLocationCounts
12 CdmaCellLocationLocalBoxes_parent  LteCellLocationLocal
13 CdmaCellLocationLocalBoxes_rowid   LteCellLocationLocalBoxes
14 CdmaCellLocationLocalCounts        LteCellLocationLocalBoxes_node
15 CellLocation                       LteCellLocationLocalBoxes_parent
16 CellLocationBoxes                  LteCellLocationLocalBoxes_rowid
17 CellLocationBoxes_node             LteCellLocationLocalCounts
18 CellLocationBoxes_parent           TableInfo
19 CellLocationBoxes_rowid            WifiLocation
20 CellLocationCounts                 WifiLocationBoxes
21 CellLocationLocal                  WifiLocationBoxes_node
22 CellLocationLocalBoxes             WifiLocationBoxes_parent
23 CellLocationLocalBoxes_node        WifiLocationBoxes_rowid
24 CellLocationLocalBoxes_parent      WifiLocationCounts
25 CellLocationLocalBoxes_rowid
```

Terminalausgabe 4.3: Die Ortungsdatenbank lockCache_encryptedA.db mit von Apple übersandten Daten existiert nur unter iOS9.

Von forensischem Interesse sind jedoch nur die nachfolgenden Tabellen, da nur diese Geokoordinaten enthalten:

- CdmaCellLocation
- CellLocation
- CellLocationLocal
- LteCellLocation
- WifiLocation

In Tab. 4.6 sind die Anzahl der Einträge pro Tabelle für iOS9.3.3 nach rund vier Tagen Nutzung aufgeführt. Neben der Anzahl der Gesamteinträge pro Tabelle sind in Klammern die Anzahl unterschiedlicher Zeitstempel sowie die maximale Speicherdauer in Tagen angegeben ($\forall\ n > 1 < 7$ Tagen). Werte, die sich aufgrund fehlender Empfänger nicht ermitteln ließen, sind mit »na« gekennzeichnet. Wenn keine Entsprechung in den Tabellennamen der unterschiedlichen Datenbanken vorliegt, ist dies durch die Verwendung von »–« gekennzeichnet.

Darüber hinaus ist in Tab. 4.6 erkennbar, dass in der lockCache_encryptedA.db-Datenbank im Vergleich zur cache_encryptedA.db-Datenbank zum einen mehr Informationen gespeichert werden und darüber hinaus ggf. aktuellere Werte zu erwarten sind, als in der Ortungsdatenbank cache_encryptedA.db.

	cache_encryptedA.db	**cache_encryptedB.db**	**lockCache_encryptedA.db**
CdmaCellLocation	na	na	na
CellLocation	100 (1) (1)	–	320 (3) (1)
CellLocationLocal	1 (1) (1)	–	1 (1) (1)
LteCellLocation	267 (3) (n)	–	112 (6) (n)
WifiLocation	–	503 (2) (1)	913 (6) (n)

Tab. 4.6: Übersicht des Speicherumfanges verschiedener Ortungsdatenbanken in iOS9. Auffällig ist die getrennte Speicherung von Funkzellen- und WLAN-Daten in unterschiedlichen Datenbanken.

In iOS10.2 werden die beiden Ortungsdienst-Datenbanken cache_encryptedA.db und cache_encryptedB.db dann wieder zusammengeführt. So existiert unter iOS10 nur noch die Datei cache_encryptedB.db. Die Datenbank lockCache_encryptedA.db wurde ebenfalls entfernt.

Die Datei cache_encryptedB.db beinhaltet dabei folgende Tabellen:

```
1
2  sqlite> .tables
3  AppHarvest                            MicroLocationConfiguration            WifiLocationHarvest
4  AppHarvestCounts                      MicroLocationConfigurationCounts      WifiLocationHarvestCounts
5  CdmaCellLocation                      MicroLocationMeasurements             WifiTileHeader
6  CdmaCellLocationCounts                MicroLocationMeasurementsCounts       WtwLocationHarvest
7  CdmaCellLocationHarvest               MicroLocationModels                   WtwLocationHarvestCounts
8  CdmaCellLocationHarvestCounts         MicroLocationModelsCounts             wifi_tile_1400500_1874000
9  CdmaCellLocationLocal                 MicroLocationRecordingEvents          wifi_tile_1400500_1874500
10 CdmaCellLocationLocalCounts           MicroLocationRecordingEventsCounts    wifi_tile_1401000_1874000
11 CdmaCellNeighborsLocationHarvest      PassHarvest                           wifi_tile_1401000_1874500
12 CdmaCellNeighborsLocationHarvestCounts PassHarvestCounts                    wifi_tile_1401000_1875000
13 CellLocation                          PoiHarvestLocation                    wifi_tile_1401000_1875500
14 CellLocationCounts                    PoiHarvestLocationCounts              wifi_tile_1401000_1876000
15 CellLocationHarvest                   PoiHarvestMUID                        [...]
16 CellLocationHarvestCounts             PoiHarvestMUIDCounts
17 CellLocationLocal                     PoiHarvestWifi
18 CellLocationLocalCounts               PoiHarvestWifiCounts
```

```
CellNeighborsLocationHarvest            PressureLocationHarvest
CellNeighborsLocationHarvestCounts      PressureLocationHarvestCounts
DatabaseIdentifier                      PressurePressureHarvest
DatabaseIdentifierCounts                PressurePressureHarvestCounts
IndoorLocationHarvest                   SCDMA
IndoorLocationHarvestCounts             SCDMACounts
IndoorWifiHarvest                       ScdmaCellLocation
IndoorWifiHarvestCounts                 ScdmaCellLocationCounts
LocationHarvest                         ScdmaCellNeighborsLocationHarvest
LocationHarvestCounts                   ScdmaCellNeighborsLocationHarvestCounts
LteCellLocation                         TableInfo
LteCellLocationCounts                   WifiAWD
LteCellLocationHarvest                  WifiLocation
LteCellLocationHarvestCounts            WifiLocationBoxes
LteCellLocationLocal                    WifiLocationBoxes_node
LteCellLocationLocalCounts              WifiLocationBoxes_parent
LteCellNeighborsLocationHarvest         WifiLocationBoxes_rowid
LteCellNeighborsLocationHarvestCounts   WifiLocationCounts
```

Terminalausgabe 4.4: Auflistung der Tabellen einer iOS10-Ortungsdatenbank (cache_encryptedB.db). In iOS 10 speichert Apple Funkzellen- und WLAN-Daten wieder in einer Datenbank.

4.1.4 Zusammenfassung

Der in der Einleitung erwähnte erste kriminalpolizeiliche Vorgang konnte mit den Erkenntnissen seinerzeit nur durch die Betrachtung der Daten in der Tabelle CellLocationHarvest erfolgreich gelöst werden. Der erwirkte richterliche Beschluss zur Hausdurchsuchung wäre ansonsten auf Basis einer Datenwolke (wie bei den Ortungsdaten von Apple der Fall) und der hohen Ungenauigkeit der Daten von Apple nicht zu begründen gewesen. Abgesehen von der Tatsache, dass zum fraglichen Zeitpunkt ohnehin keine Daten in den Tabellen CellLocation bzw. WifiLocation zu ermitteln waren. Darüber hinaus lieferte die Analyse der Ortungsdatenbank(en) zu Beginn dieser Arbeit wesentliche Grundlagen zum Verständnis der mobilen Ortung aus forensischer Sicht (vgl. [(4r11] und [(4r12]).

Apples Ortungsdienst ist einem ständigen Wandel unterworfen (vgl. Abschnitt 4.1.1 auf Seite 73). Die Datenbanken erhalten immer wieder neue Tabellen und, oder Spalten wobei sich die Erkenntnisse vergangener Untersuchungen auf neuere iOS-Versionen übertragen lassen. So ändern sich z.B. die Wertebereiche der einzelnen Spalten nicht, wohingegen die Genauigkeit und Differenzierung einzelner Datenquellen mit jeder neuen iOS- bzw. Geräte-Version zunehmen.

In der Praxis sind harvest-ing Tabellen sehr gut für die forensische Auswertung von Standortdaten aus Apple-Geräten geeignet. Allerdings macht die Tatsache,

dass die Daten der Harvesting-Tabellen regelmäßig gelöscht und überschrieben werden, die Auswertung dieser Daten häufig schwierig bzw. unmöglich.

Aber auch Ortsinformationen aus den Tabellen CellLocation und WifiLocation können hilfreiche Ansätze für kriminalpolizeiliche Ermittlungen liefern. So gibt der erste Funksender zu einem bestimmten Zeitpunkt zuverlässig die Position des Gerätes innerhalb eines Fehler- bzw. Senderadius an. Im Falle von Mobilfunkantennen ist der Senderadius mitunter zu groß, um eine ausreichend genaue Position zu ermitteln. WLAN-Sender hingegen liefern hier i. d. R. hinreichend genaue Angaben.

Einer Veröffentlichung der untersuchten Ortungsdatenbanken und aufgezeichneten Messergebnisse kann nicht entsprochen werden. Zum einen handelt es sich mitunter um kriminalpolizeiliche Verfahrensdaten, des Weiteren um persönliche Daten inkl. Standortinformationen Dritter deren Einverständnis zur Veröffentlichung nicht vorliegt. Die gesicherten Daten können allerdings bei Bedarf einem kritischen Leser demonstriert werden.

In der Summe sind zwei Erkenntnisse bzgl. Ortungsdaten von Apple essentiell:

Funkzellendaten bei Apple sind nicht providerbezogen. Wie in Abschnitt 4.1.2 auf Seite 76 bereits beschrieben, stammen die Positionsangaben zu Mobilfunkmasten nicht von den Providern. Vielmehr wird die Position des Funksenders auf Basis einer Vermessung durch Endgeräte der Nutzer vom Hersteller (hier Apple) selbst durchgeführt. Es ist von daher auch nicht verwunderlich, dass ein Abgleich mit von Providern stammenden Daten zu Abweichungen bei der Verortung führen würde.

WLAN-Daten sind genauer als die von Mobilfunksender. Was den Umfang an Daten angeht, so ist dies antiproportional zu der Feststellung um die Sendereichweiten zu sehen. Das bedeutet, dass wesentlich mehr WLAN-Sendestationen zur Abdeckung des gleichen Areals notwendig sind als dies z. B. bei Mobilfunksendern der Fall ist. Demzufolge lassen sich auch wesentlich mehr Einträge in den WLAN-Tabellen als in den CellLocation Tabellen finden.

Exkurs: Rekonstruktion gelöschter Standortdaten.

Eine Rekonstruktion gelöschter Standortdaten in iOS ist prinzipiell möglich. In mehreren Posts beschreibt z. B. Richard Drinkwater in seinem Forensik-Blog »Forensics from the sausage factory« [Dri11a] den Aufbau von SQLite3-Datenbanken sowie Möglichkeiten der Erkennung von Bereichen mit gelöschten Datensätzen.

Demnach sind SQLite3-Datenbanken in sog. Pages mit einer fest vorgegebenen Größe organisiert. Zu Beginn wird im Header einer jeden Page der Typ der Seite angegeben. Hieran anschliessend folgen Pointer auf die Inhalte der Datensätze, die sich vom Ende der Seite in Richtung der Positionspointer hin füllen. Durch die Korrelation der Pointer zu den Inhaltsdaten lassen sich dann die gelöschten Datensätze erkennen und mittels Schema der regulär gespeicherten Datensätze rekonstruieren (vgl. [Dri11b]).

Die Rekonstruktion gelöschter Einträge in Apples Ortungsdatenbanken erscheint zunächst sehr interessant, zumal Harvesting-Daten bekanntermaßen direkt nach der Übertragung an Apple gelöscht werden. Demzufolge müssten Unmengen an gelöschten Datensätzen zu rekonstruieren sein. In der Praxis ist die Zuordnung der Daten allerdings nicht immer zweifelsfrei möglich. Denn die gelöschten Daten werden intern als »freier Speicher« deklariert und könnten komplett oder auch nur teilweise überschrieben worden sein. Eine forensische Nutzung gebietet sich hingegen nur, wenn Daten zweifelsfrei zu rekonstruieren sind.

Zudem besitzen SQLite3-Datenbanken eine Option, die sich »auto vacuum« nennt. Wird diese Option in der Konfiguration der Datenbank gesetzt, werden vollständig gelöschte Datenbereiche, die sog. »free pages« ans Ende der Datenbank verschoben und dann dort abgeschnitten. Durch die Vollverschlüsselung des Dateisystems von iOS-Geräten lassen sich solche Speicherbereiche danach nicht mehr rekonstruieren. Das Wiederherstellen der so gelöschten Datensätze ist dann nicht mehr möglich.

Zusammenfassend ist es möglich, gelöschte Standortdaten der Ortungsdienste bei Apple zu rekonstruieren. In der forensischen Praxis werden die Verfahren dagegen nur selten angewandt. Der Aufwand sowie die Anzahl fälschlich wiederhergestellter Datensätze (sog. false-positives) machen das Vorgehen unwirtschaftlich und ggf. angreifbar.

4.2 Google Android

Neben Apple existieren weitere Hersteller die Ortungsdienste auf ihren Geräten verwenden. Aufgrund der bestimmenden Marktlage von Googles Betriebssystem Android ist insbesondere eine forensische Untersuchung der Ortungsfunktionen von Google geboten. Ferner gilt es zu klären, ob sich Erkenntnisse aus Analysen von iOS-Daten auf die Qualität und Quantität der von Google gespeicherten Daten übertragen lassen.

Darüber hinaus setzt Google Lokalisierungstechniken nicht nur zur Positionsbestimmung auf Android-Smartphones ein. Standortdaten lassen sich bei Google zusätzlich über deren Online-Dienste finden und sogar unter Apple iOS [Goo16e] mithilfe der Software GoogleNow erheben. Hierauf wird später insbesondere in Bezug zu Google Now in Abschnitt 4.2.3 auf Seite 119 genauer eingegangen.

Zunächst soll aber, wie im Abschnitt zu Apples iOS (vgl. Abschnitt 4.1.1 auf Seite 66), auch für Android eine forensische Betrachtung der vom System gespeicherten Ortungsdaten erfolgen.

Kategorisierung der Datenquellen in Android

Im Gegensatz zu den in Abschnitt 4.1.1 auf Seite 73 beschriebenen Kategorien der extrinsischen bzw. intrinsischen Erhebung von Standortdaten bei Apple existiert in Android nur eine Kategorie. So werden alle auswertbaren Ortungsdateien von außen, also extrinsisch motiviert.

- **Ortungsdaten auf dem Gerät** bis Android 2.3
  - cache.cell, cache.wifi (siehe S. 110)
- **Ortungsdaten nur noch bei Google** ab Android 3.0 (siehe S. 125)

Bekanntermaßen existieren Android-Smartphones mit GPS-Sensoren. Bei den ersten eigenen Untersuchungen mit einem Samsung S3mini und Android 2.3 konnte die Geräteposition auch ohne Netzwerkunterstützung ermittelt werden. Bei späteren Tests (ohne Mobilfunk oder Internetverbindung) mit einem Sony Xperia Z5 und Android 6.0 war die Verortung auf Basis des GPS-Empfängers trotz hinreichend guter GPS-Signale selbst nach mehr als 15 Minuten nicht mehr möglich. Reine GPS- Standortdaten konnten nicht mehr festgestellt werden.

4.2.1 Die Ortungsdatendateien

Wie bereits beschrieben speichert Google Standortdaten. Außer in Metadaten zu Bildern etc. speichert(e) Android bis zur Version 2.3 Ortungsdaten des Systemdienstes in zwei unterschiedlichen Dateien auf dem Gerät. Daneben speichert Google Standortdaten online im sog. Standortbericht [Goo16d], aber hierzu später in Abschnitt 4.2.4 auf Seite 125 mehr.

Die erste Beschreibung der Datendateien im Rahmen dieser Arbeit um Android 2.x inkl. Analyse und Interpretation der Standortdaten wurde im November 2011 in englischer Sprache online veröffentlicht (siehe [(4r12]). Seitdem gibt es keine nennenswert neueren Erkenntnisse zum Thema. Das hängt damit zusammen, dass nach Android 2.3 keine durch das Betriebssystem gepufferten Ortungsdaten mehr ermittelt werden konnten.

Pfad im Dateisystem

Um die vom Android Ortungsdienst gepufferten Cache-Daten untersuchen zu können, müssen die Daten zunächst vom Gerät extrahiert werden. Eine Option zur Erstellung eines lokalen Gerätebackups (analog zu iOS) existiert bei Google so nicht. Dafür bietet Android die Möglichkeit, über die sog. Android Debugging Bridge (ADB) auf das Gerät via USB zuzugreifen. Der Zugriff auf das Gerät über USB ist allerdings standardmäßig deaktiviert und muss zuvor eingeschaltet werden (siehe hierzu [Goo16a]). Bis Android v.4.2 konnte die entsprechende Einstellung in den Systemeinstellungen unter »Einstellungen - System - Entwickleroptionen« gesetzt werden. Nach Android v.4.3 muss der Nutzer nach Aufruf des Menüpunktes »Über das Telefon« sieben mal auf den Eintrag »Build number« tippen (vgl. [Goo16a] »how to enable ADB«). Anschließend lässt sich der Entwicklermodus wie gewohnt aktiveren.

Die Android-Ortungsdateien befinden sich nach [Sch11] auf dem Gerät in:

- `/data/data/com.google.android.location/files/cache.cell`
- `/data/data/com.google.android.location/files/cache.wifi`

Um die beiden Dateien vom Gerät zu extrahieren, muss der Zugang zum Gerät über ein USB-Kabel hergestellt werden. Zusätzlich müssen auf dem Hostsystem

die »platform-tools« aus dem Goggle Android-SDK installiert sein. Anschließend lassen sich die Daten mittels Aufruf auf der Kommandozeile wie folgt vom Gerät herunter kopieren:

```
$ adb pull /data/data/com.google.android.location/files/cache.* .
```

Terminalausgabe 4.5: adb-Kommando zur logischen Extraktion der Ortungsdaten aus dem Android-Dateisystem.

Der Aufruf des Kommandos folgt dem Schema: `adb pull <remote> <local>`. Für den Zugriff auf diese Ordnerstruktur innerhalb des Dateisystems von Android sind, wie auch unter iOS, erweiterte Systemrechte erforderlich.

Aufbau und Struktur Die Standortdaten in Android v.2.2/2.3 sind in einem binären Datenformat abgespeichert. Diese Art der Speicherung von Daten in Form von Bytestreams wird in Java sehr häufig eingesetzt. Eine Beschreibung der Struktur dieser Daten liefert Magnus Eriksson auf github (vgl. [Eri11b]):

```
Leading Information (4 bytes sequence)
  * 2 bytes: Unsigned Short (version)
  * 2 bytes: Unsigned Short (Entry Count)
Location Entry(ies) (loop sequence)
  * x bytes: UTF-String (Cell-Information or \gls{mac}-adress)
  * 4 bytes: Integer (transmission range)
  * 4 bytes: Integer (gls{confidence})
  * 8 bytes: Double (gls{lat})
  * 8 bytes: Double (gls{lon})
  * 8 bytes: Long (UNIX-timestamp)
```

Jede der beiden Dateien beginnt mit einem vier Byte langen Dateiheader. Der Header besteht aus zwei Byte für die Versionsinformation gefolgt von zwei Byte für die Anzahl der Standortdaten. Die anschließend gespeicherten Positionsdaten beinhalten in der Folge Informationen zum Funksender, dem Senderadius, einer Angabe zur Verlässlichkeit, der Position mit Breiten- und Längengradangabe und den Zeitstempel.

Die erste Bytefolge nach dem Header dient der Identifikation des Funksenders. Die Sequenz selbst besteht aus einem UTF8-String variabler Länge. Access Points werden so z. B. durch die MAC Adresse mit führenden Nullen in hex Notation beschrieben:

- 7c:4f:b5:df:0f:cf (als Beispiel)

Für Funkzellen folgt die UTF8-Zeichenkette dem Schema:

- MCC (Mobile Network Code; Landeskennung, z. B. »262« für Deutschland)
- MNC (Mobile Network Code; Netzwerkkennung, z. B. »1« für T-Mobile)
- LAC (Location Area Code; die sogenannte Bereichskennung)
- CI (Cell Identifier; zu deutsch: Funkzellenkennung)

Sodann folgt jeweils dieselbe Bytefolge zur Beschreibung des Standortdaten:

- Senderadius in Meter, (als Integer-Ganzzahl ohne Angabe zur Einheit)
- Verlässlichkeit in Prozent (als Ganzzahl ohne Prozentangabe)
- Breiten- und Längengradangabe (im Dezimalformat als Double-Wert)
- Zeitstempel im unix-Format (Sekunden seit dem 01.01.1970 00:00:00h)

Dekodierung des Bytestreams Zur Dekodierung der Daten stellt Eriksson online auf github ein Python-Skript (»android-locdump/parse.py« [Eri11b]) zur Verfügung. Ein Beispiel der Ausführung gibt er ebenfalls mit an (siehe [Eri11a]). Insbesondere werden hierdurch die Unix-Zeitstempel in ein menschenlesbares Format inkl. Zeitzonenangabe (0200 entspricht plus 2 Stunden Mitteleuropäische Sommerzeit (MESZ)) überführt.

```
$ python parse.py cache.wifi
db version:  1
total:   47

key                    accuracy  conf.   latitude    longitude  time
50:63:13:57:42:7e             80     92   57.689354   11.994763  04/11/11 10:03:51  0200
e0:cb:4e:7e:cc:53             75     92   57.689340   11.994495  04/11/11 10:03:51  0200
4c:54:99:14:47:68             57     92   57.708979   11.916581  04/11/11 01:14:53  0200
00:26:18:0a:ad:cb             60     92   57.709699   11.917637  04/13/11 08:40:36  0200
00:22:15:28:3f:7a             60     92   57.699467   11.979340  04/13/11 11:52:16  0200
00:22:3f:a7:d9:fd             65     92   57.699442   11.979343  04/13/11 11:52:16  0200

$ python parse.py cache.cell
db version:  1
total:       41

key                    accuracy  conf.   latitude    longitude  time
240:5:15:983885             1186     75   57.704031   11.910801  04/11/11 20:03:14  0200
240:5:15:983882              883     75   57.706322   11.911692  04/13/11 01:41:29  0200
240:5:75:4915956             678     75   57.700175   11.976824  04/13/11 11:52:16  0200
240:5:75:4915953             678     75   57.700064   11.976629  04/13/11 11:53:09  0200
240:7:61954:58929           1406     75   57.710205   11.921849  04/15/11 19:46:31  0200
240:7:15:58929                -1      0    0.000000    0.000000  04/15/11 19:46:32  0200
240:5:75:4915832              831     75   57.690024   11.998419  04/15/11 16:13:53  0200
```

Terminalausgabe 4.6: Gekürzte exemplarische Ausgabe des locdump-parser-Skriptes von Magnus Eriksson (android-locdump/parse.py).

Eigenentwicklung eines Bytestream-Parsers Zur weiteren Untersuchung sowie besseren Nachvollziehbarkeit wurde im Rahmen dieser Arbeit das Tool BytestreamAnalyzerLE entwickelt. Hiermit sollte u.a. untersucht werden, ob sich ggf. weitere Daten innerhalb der Ortungsdateien von Android (z. B. am Ende der Datei bzw. andere Versionsnummern von Android) ermitteln lassen.

Wie in Abb. 4.12 auf der nächsten Seite dargestellt, ist es mithilfe dieser Software möglich, Bytestromdateien einzulesen, diese zu untersuchen und mithilfe eines »parsing-Pattern« (deu. Analysemuster) automatisiert in eine menschenlesbare Darstellung zu überführen. Durch die Anwendung des Erkennungsmusters (vgl. Abb. 4.12 auf der nächsten Seite Schritt 3) lassen sich die Inhalte der beiden Dateien cache.cell bzw. cache.wifi in eine Berichtsform für den forensischen Analysten überführen.

Die Erstellung eines Parsing-Musters läuft schematisch wie folgt ab:

1. Nach dem Einlesen des Bytestreams muss das Datenformat an der Cursorposition (roter Kasten in »Input«) zunächst mithilfe des Datendolmetschers (rote Kästen in »Data«) analysiert werden (SCHRITT1).
2. Zusätzlich zur Darstellung des Datentyps erfolgt hierbei automatisch die Konvertierung in ein menschenlesbares Format. So wird z.B. aus 1326872247659 (long) das Datum 18.01.2012 08:37:27 (SCHRITT2).
3. Anhand des im vorigen Schritt ermittelten Datenformates gilt es nun, das »Parsing-Pattern« zu beschreiben (SCHRITT3). In Abb. 4.12 auf der nächsten Seite resultiert so z. B. aus dem abzulesenden Datentyp long ein »L« im Parsing-Pattern.

Generell ermöglicht die Anwendung BytestreamAnalyzersLE die Zuordnung nachfolgender Datentypen zu den fettgedruckten Lettern:

- **S** = unsigned-short (2 Byte)
- **I** = integer (4 Byte)
- **F** = float (4 Byte)
- **L** = long (8 Byte)
- **D** = double (8 Byte)
- **U** = utf-string (n Byte) und
- **{x}n** = führt das Pattern »x« n-mal aus, bzw. ohne Angabe von n solange, bis keine weiteren Daten mehr erkannt werden.

Ist das Pattern vollständig beschrieben (SCHRITT4), lässt sich zum Schluss im Ausgabefenster (»Output«) die Dekodierung des Bytestreams betrachten (5).

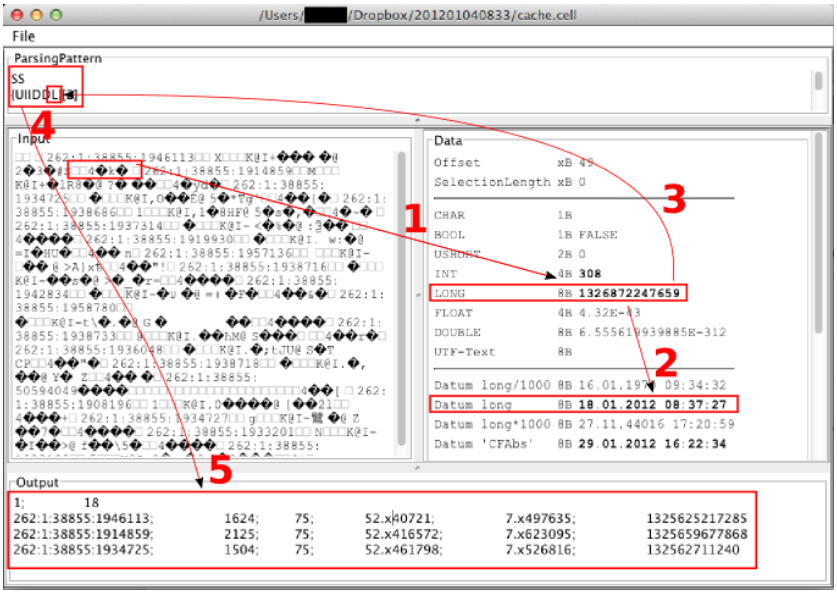


Abb. 4.12: Mithilfe der Eigenentwicklung (BytestreamAnalyzerLE) lassen sich die Daten eines Bytestream im Datendolmetscher (1,2) untersuchen und durch Eingabe der Datenstrukturen (3,4) menschenlesbar ausgeben (5). Quelle: Eigene Darstellung.

4.2.2 Ortungsdaten von Google

Ohne den späteren Ausführungen ab Seite 119ff. vorzugreifen, ist offensichtlich, dass die Ortungsfunktionalität von Google weitaus weniger detailliert durch Analyse der Ortungsdaten beschrieben werden kann, als dies bei iOS der Fall ist.

Außer Standortinformationen zu umliegenden Funksendern speichert Android keine zusätzlichen Hinweise, die eine Analyse oder Interpretation hinsichtlich der Erhebung von Standortdaten seitens Google zulassen. Mit Einführung von Android Honeycomb (3.0) scheint Google keine persistenten Cache-Dateien des Ortungsdienstes mehr auf den Geräten zu speichern. Bevor die Problematik in Abschnitt 4.2.2 auf Seite 118 weiter ausgeführt wird, gilt es im nachfolgenden Abschnitt zunächst noch die Erfahrungen und Probleme aus forensischer Sicht hinsichtlich der gespeicherten Ortungsdaten in Android 2.x zu beschreiben.

Erfahrungen und Probleme

Bei den Informationen innerhalb der Dateien **cache.cell** und **cache.wifi** handelt es sich um Standortdaten von Funksendern in der Umgebung des Gerätes. Wie bei Apple (vgl. Abschnitt 4.1.2 auf Seite 81 - Erfahrungen und Probleme) lassen sich auch bei Android mehrere Einträge bzgl. Drahtlossender zu einem Zeitpunkt feststellen. So gelten unter forensischen Gesichtspunkten die gleichen einschränkenden Bedingungen wie für iOS.

Aus den bisherigen Erfahrungen bzgl. der forensischen Analyse von Apple iOS-Ortungsdaten und der Vielzahl durchgeführter Tests mit Google-Daten konnte auch für Android ermittelt werden, dass der jeweils erste Eintrag einer Serie von Zeitstempeln die Position des Gerätes beschreibt; wieder mit der angegebenen Ungenauigkeit auf Basis der Sendereichweite des betreffenden Senders.

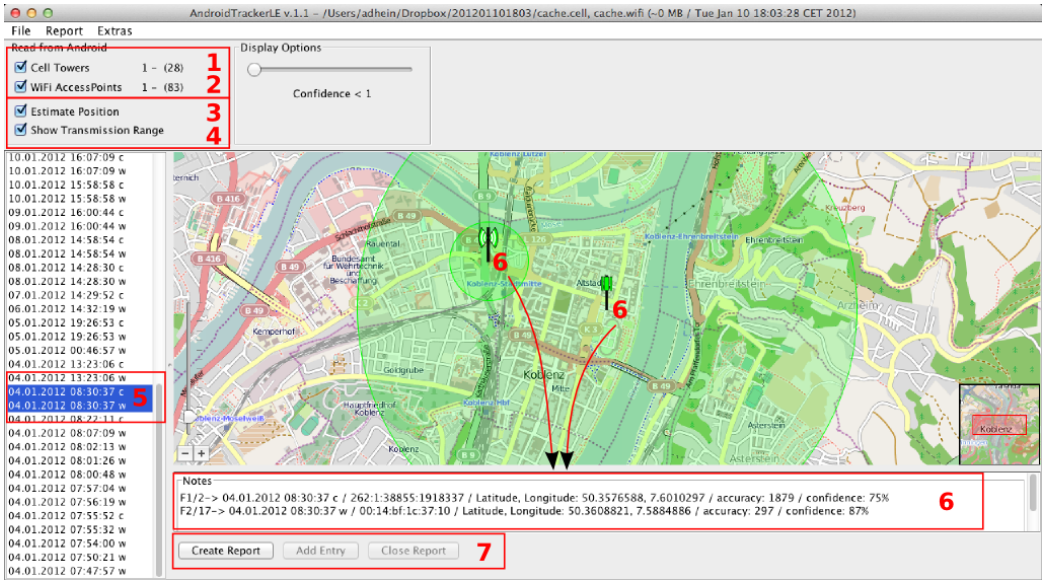


Abb. 4.13: Beispiel einer korrekten Verortung von Google-Standorten im AndroidTrackerLE v1.1. Wenn nach dem Laden und Anzeigen der Daten (1,2,3,4) bei gleichen Zeitstempeln (5) von Funkzellen- und WLAN-Sendern der WLAN-Sender innerhalb des Senderadius der Funkzelle liegt (6) gilt die Verortung des Gerätes im WLAN-Bereich als sehr zuverlässig. Zusätzlich können mithilfe der Anwendung noch Notizen (6 unten) sowie ein forensischer Bericht (7) erstellt werden.
Quelle: Eigene Darstellung. Kartenmaterial: © OpenStreetMap Mitwirkende 2011.

Regelmäßig lässt sich darüber hinaus feststellen, dass Standorte zu Funkzellen und WLAN-Accesspoints zu ein und demselben Zeitstempel existieren. Wie in

Abb. 4.13 auf der vorherigen Seite zu erkennen, liegt hierbei der Standort sowie die Sendereichweite des WLAN-Senders sehr häufig innerhalb des Funkradius des Mobilfunksenders.

Für diese Konstellation der Standorte zu einem fixen Zeitpunkt konnte durch zahlreiche Tests zuverlässig ermittelt werden, dass die Geräteposition innerhalb des Sendebereichs des WLAN-Senders liegt. In Abb. 4.13 auf der vorherigen Seite z. B. am Sitz des Polizeipräsidiums in Koblenz. Ferner hat sich herausgestellt, dass die Position des Gerätes zum Zeitpunkt der Verortung immer innerhalb des Radius einer der Funkquellen liegt (wenn die WLAN-Funkquelle innerhalb des Sendebereichs des Mobilfunksenders liegt).

Umgekehrt ist für die Betrachtung und Bewertung der Genauigkeit wichtig, dass die Standortinformationen zweier identischer Zeitstempel nicht völlig »daneben« liegen (wie z. B. in Abb. 4.14 zu sehen). In einem solchen Fall konnte die Ortung nicht präzise durchgeführt werden. Wie mehrere Tests gezeigt haben, kann hier der tatsächliche Aufenthaltspunkt zum Zeitpunkt der Datenerhebung nicht nur außerhalb des Sendebereiches des WLAN-Senders, sondern auch weiter entfernt von der Mobilfunkantenne liegen.

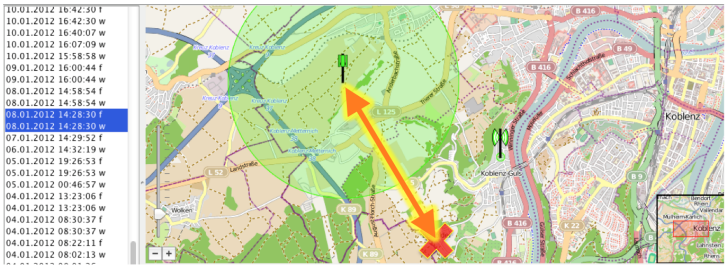


Abb. 4.14: Beispiel einer gescheiterten Verortung. Befindet sich der WLAN-Sender außerhalb des Senderadius der Funkzelle, ist die Verortung des Gerätes nicht verlässlich. Das rote »X« markiert den tatsächlichen Aufenthaltsort. Quelle: Eigene Darstellung. Kartenmaterial: © OpenStreetMap Mitwirkende 2012.

In puncto Genauigkeit der Standortdaten stehen die Daten von Google hingegen, trotz der bereits erwähnten stark reduzierten Anzahl an gespeicherten Einträgen, der Genauigkeit der Apple-Daten in nichts nach. Die Senderadien der Mobilfunkmasten bewegen sich im Durchschnitt um die 1,5km. Die Reichweiten der WLAN-Sender liegen im Bereich von 50-300m.

Vollständigkeit des Standortberichtes

Auf den ersten Blick scheinen auf Android-Geräten viel weniger Ortungsdaten gespeichert zu werden, als dies bei Apple der Fall ist. Im Durchschnitt beläuft sich die Gesamtmenge an Daten auf weniger als 1 Kilobyte.

- cache.cell (<100bytes)
- cache.wifi (<900bytes)

Magnus Eriksson zitiert hierzu in seinem Beitrag auf github [Eri11a] aus dem Android-Sourcecode einen Abschnitt, der die maximale Anzahl an Einträgen für Funkzellen bzw. WLAN-AccessPoints festlegt:

```
1 // Maximum time (in millis) that a record is valid for, before it needs
2 // to be refreshed from the server.
3     private static final long MAX_CELL_REFRESH_RECORD_AGE = 12 * 60 * 60 * 1000; // 12 hours
4     private static final long MAX_WIFI_REFRESH_RECORD_AGE = 48 * 60 * 60 * 1000; // 48 hours
5
6 // Cache sizes
7     private static final int MAX_CELL_RECORDS = 50;
8     private static final int MAX_WIFI_RECORDS = 200;
```

Demnach beläuft sich die maximale Anzahl an Einträgen zu Funksendern auf

- max. 50 Einträge für Funkzellen und
- max. 250 Einträge im Bereich WLAN.

Ferner lässt sich dem Quellcode-Ausschnitt oben entnehmen, dass die maximale Zeitspanne für valide Einträge von Ortungsdaten wie folgt definiert ist:

- Funkzellen: 12h
- WiFisender: 48h.

Auf Basis eigener Untersuchungen konnte bestätigt werden, dass Inhaltsdaten der beiden Dateien (cache.cell, cache.wifi) nur dann überschrieben werden, wenn die maximale Anzahl an Einträgen erreicht wurde. Umgekehrt erscheinen zuverlässig neue Standorte, wenn die Positionsdaten älter als die vorgegebenen Zeiträume sind. Beim Deaktivieren des Ortungsdienstes in Android 2.3 werden die gespeicherten Daten des Systemdienstes gelöscht. Unter Android 2.2 werden die Inhalte der Dateien cache.cell und cache.wifi zwar nicht gelöscht, es werden aber auch keine weiteren Standorte mehr erhoben.

Zusammengefasst ist die Vollständigkeit der Standortdaten auf Google-Geräten mit Android 2.x nicht zeitlich, sondern durch die maximale Anzahl an Record-Einträgen beschränkt. In der Praxis spielen die Daten älterer Androidversionen in der Mobilfunkforensik aktuell nur noch eine untergeordnete Rolle. Darüber hinaus bereitet die Extraktion der gepufferten Geolokalisierungsdaten älterer Versionen von Android mitunter auch den kommerziellen Anbietern von Mobilfunkforensiklösungen Schwierigkeiten (vgl. MSAB in Abschnitt 2.2.4 auf Seite 45).

Kein Standortbericht mehr seit Android 3.0?

Wie bereits mehrfach beschrieben, lassen sich unter Android in der Version 3.0 (Honeycumb) keine gepufferten Standortdaten des Google-Ortungsdienstes mehr finden. Die Ordnerstruktur `/data/data/com.google.android.location/files/` existiert zwar nach wie vor, das Verzeichnis beinhaltet allerdings keine Dateien mehr.

Da Ortungsdienste nach Android v.2.x weiterhin verfügbar sind, müssen die Standortdaten hierfür auf den Geräten erhoben und auch dort gespeichert werden. Bisher verliefen alle Untersuchungen zum Auffinden von Standortdaten des Systemdienstes in Android Smartphones negativ. Es ist zu vermuten, dass die komplette Verortung nunmehr ausschliesslich online über Google-Dienste durchgeführt wird. Demnach stammen Standortdaten, welche von den Forensik-Tools aus späteren Android Versionen ermittelt werden auch nicht mehr aus den Cache-Dateien sondern aus Metadaten von Bild- oder Multimediadateien bzw. auch aus gespeicherten Standortdaten in Apps. Allgemein ist festzuhalten, dass diese Daten in der Regel keine Angaben zur Genauigkeit mehr beinhalten. Zudem ist der Ursprung der erhobenen Ortungsinformationen nicht mehr klar zu ermitteln. Es ist sehr wahrscheinlich, dass die Daten zur Verortung über einen Online-Dienst von Google (https://loc.google.com) durch eine Anfrage auf Basis diverser möglicher Sender oder auch anderer technischer Informationen zurück geliefert werden. Leider läuft diese Übertragung Ende-zu-Ende-verschlüsselt ab. Eine Auswertung der Inhaltsdaten der übertragenen sowie der empfangenen Daten ist von daher nicht möglich.

4.2.3 Ortungsdaten für Google

Um Ortungsdienste anbieten zu können muss Google, wie jeder andere Anbieter auch, im Vorfeld Informationen und Standorte zu Funksendern erheben. Im Gegensatz zu Apple lässt sich aufgrund fehlender harvesting-Daten die Datenerhebung auf Android-Smartphones nicht konkret darstellen. Dafür nutzt Google viele andere Wege zur Erhebung von Standortdaten, die im Folgenden beschrieben werden sollen.

Google Maps und Reverse-Geocoding

Seit mittlerweile mehr als 10 Jahren bietet Google seinen Kartendienst an. Neben unterschiedlicher Darstellmöglichkeiten der Kartenansicht sowie Suchoptionen für Adressen und Fahrtrouten ist es ferner möglich, Adressdaten mittels der sog. Reverse-Geocoding-Technik in Breiten- und Längengradangaben umrechnen zu lassen.

Der Aufruf der URL `https://www.google.com/maps/place/Universität-Koblenz:GebäudeA,Universiätsstrasse1,-56070Koblenz,Deutschland` führt z. B. zu folgender Kartenansicht:

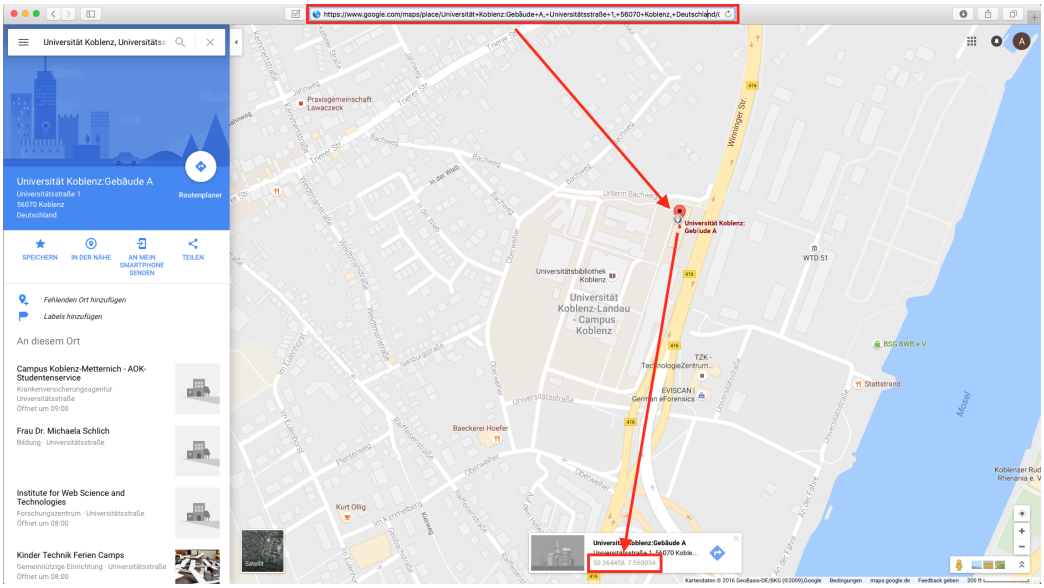


Abb. 4.15: Auflösen einer Adresse zu einer geographischen Position mithilfe von Googles Kartendienst. Quelle: Google Maps 2016.

Neben der Kartenansicht erhält der Anwender weitere geographische Angaben zur ermittelten Position. So lässt sich die Geoposition (50.364482,7.560061) zur Adresse bzw. dem Marker auf der Karte (roter Pin) im roten Kasten unten in Abb. 4.15 auf der vorherigen Seite ablesen. Das sog. Reverse-Geocoding ist aber nur ein Beispiel, wie Google Standortdaten aus Quellen ableiten kann, die originär keine Geokoordinaten ausweisen.

Hinter dem Kartendienst steckt noch mehr. Für die Erweiterung von Google Maps um Streetview setzt Google spezielle Kamerawagen ein, die zusätzlich zu den Bildaufnahmen gezielt Standortdaten zu WLAN-Accesspoints sammeln. In Deutschland wird diese Tatsache höchst kontrovers diskutiert. Der Skandal um die Aufzeichnungen privater WLAN-Daten wird durch Anschuldigungen der Landes- bzw. Bundesdatenschützer 2010 öffentlich [Bri10]. Der Problematik um die Erhebung privater SSID-Informationen unbenommen, ging es Google sehr wahrscheinlich mehr um die Erhebung von Positionsdaten zu den umliegenden WLAN-Endgeräten. Als Nebenprodukt zu Googles Streetview-Bildern wäre es so möglich gewesen, eine gezielte weltweite Kartierung der bestehenden WLAN-Accesspoints ohne Smartphones zu generieren. Gewissermaßen eine recht frühe und sehr spezielle Art des Harvestings von Standortdaten durch Google.

Ortungsdaten aus IP-Adressen

Das Ermitteln von Standortdaten zu IP-Adressen lässt sich sehr anschaulich am Beispiel einer Sicherheitswarnung von Google darstellen. Nach der Anmeldung zum Google-Konto mit einem bislang unbekannten Gerät erhält der Inhaber des Accounts diverse Sicherheitsmeldungen im Kundenkonto, via Email oder auf dem Android-Smartphone. Die Ortsinformation des Gerätes (in Abb. 4.16 auf der nächsten Seite ist ein Anmeldeversuch mit einem bislang unbekannten Apple iPhone zu sehen) ermittelt Google hierbei anhand der IP-Adresse. Im Beispiel wurde die Internetverbindung über eine WLAN-Verbindung von innerhalb der Universität Koblenz hergestellt (IP: 141.26.x.x).

Vereinfacht dargestellt passieren zwei Dinge:

1. Ermitteln der Adresse des Internetproviders (Uni Koblenz)
2. Lokalisieren des Standortes durch Reverse-Geocoding (siehe oben)

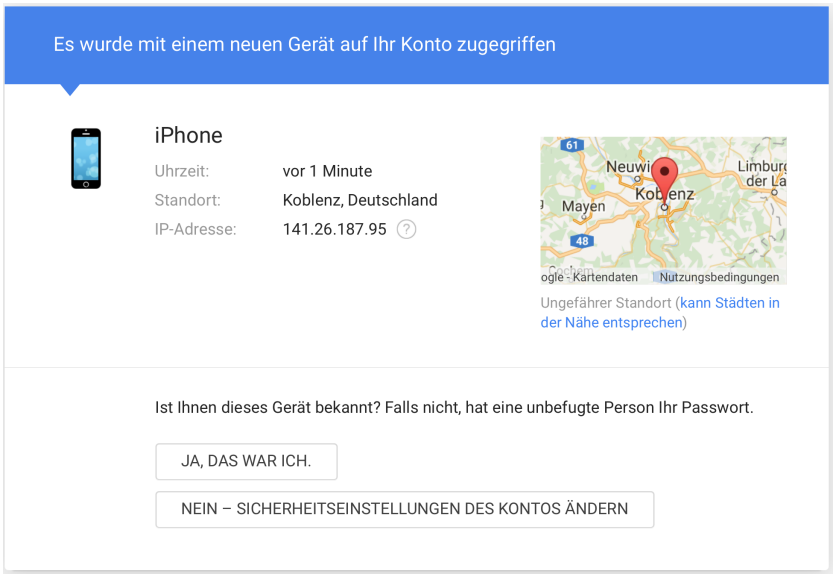


Abb. 4.16: Screenshot Google-Anmeldung: Google stellt geographische Abweichungen bei der Anmeldung anhand der IP-Adresse fest. Quelle: Google 2017.

Das Verfahren bzw. auch die Anwendung auf Computersystemen zur Auflösung eines Providers hinter einer IP Adresse nennt sich WHOIS (vgl. Ausgabe 4.7). Für die Verortung sind insbesondere die Einträge aus den Feldern »address« für das Reverse-Geocoding (siehe Abschnitt 4.2.3 auf Seite 119) von Interesse.

```
$ whois 141.26.185.153
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/public/whoisinaccuracy/index.xhtml
[...]
inetnum:        141.26.0.0 - 141.26.255.255
netname:        UKLA
descr:          Universitaet Koblenz-Landau (Abt. Koblenz) GHRKO, Koblenz
country:        DE
[...]
address:        Universitaet Koblenz
address:        Rechenzentrum
address:        Rheinau 1
address:        D-56075 Koblenz
address:        Germany
[...]
```

Terminalausgabe 4.7: Ergebnis der WHOIS-Abfrage zur IP 141.26.185.153

Wie in Ausgabe 4.7 auf der vorherigen Seite zu entnehmen, ist für die Universität Koblenz hier noch der alte Campus auf dem Oberwerth (ca. 2km vom heutigen Campus im Stadtteil Metternich) angegeben. An dem Beispiel wird deutlich, dass die Genauigkeit bei der automatisierten Verarbeitung sehr von der Aktualität der Informationen von Drittanbietern abhängt.

Die Technik lässt sich auch bei Internetverbindungen über das Mobilfunknetz anwenden. Hierbei entstehen allerdings nicht weniger Probleme. Da die Mobilfunkprovider sehr häufig ein nationales Netz bzw. mittels Roaming auch internationale Netzzugänge anbieten, dürfte die Positionsbestimmung weitaus ungenauer als 2km (wie im Beispiel eben) sein.

Zur Generierung qualitativ hochwertiger Standortdaten ist dieses Verfahren nicht geeignet. Die Genauigkeit sowie Verlässlichkeit ist unter bestimmten Umständen mangelhaft und mitunter irreführend, wenn z. B. Anonymisierungsdienste verwendet werden. Weitere Informationen zur Genauigkeit der IP-Tracking-Methode lassen sich auf einer der zahlreichen Hilfe Seiten zum Thema bei Google finden (z. B. [Goo18d]).

Ortungsdaten via Geolocation API

Über die Geolokalisierungsschnittstelle (API) bei Google lassen sich ebenfalls und nicht nur auf Android-Smartphones Standorte ermitteln. Wie in der Entwicklerdokumentation [Goo16g] beschrieben, wird die Verortung hierbei wie folgt durchgeführt:

1. Übersenden der Funksender aus der Umgebung an Google
   (vgl. Ausgabe 4.2.3 auf der nächsten Seite).
2. Google berechnet den Gerätestandort inkl. möglicher Fehlerabweichung
3. Die Positionsschätzung wird zum Gerät zurückgesendet
   (vgl. Ausgabe 4.2.3 auf der nächsten Seite)

Neben eindeutigen Identifikationsmerkmalen der Funksender sind dem Datensatz im JSON-Format aus Schritt 1 im Idealfall noch weitere Informationen bzgl. Empfangsstärke etc. beigefügt. Anhand dieser Informationen errechnet Google dann auf Basis von bereits gesammelten Geodaten (interne Datenbestände bei Google) die Geräteposition und sendet diese zurück ans Gerät.

Konkret könnte ein solcher POST-request an `https://www.googleapis.com/geolocation/v1/geolocate?key=**YOUR_API_KEY**` wie folgt aussehen:

```
{
 "homeMobileCountryCode": 310,
 "homeMobileNetworkCode": 260,
 "radioType": "gsm",
 "carrier": "T-Mobile",
 "cellTowers": [
  {
   "cellId": 39627456,
   "locationAreaCode": 40495,
   "mobileCountryCode": 310,
   "mobileNetworkCode": 260,
   "age": 0,
   "signalStrength": -95
  }
 ],
 "wifiAccessPoints": [
  {
   "macAddress": "01:23:45:67:89:AB",
   "signalStrength": 8,
   "age": 0,
   "signalToNoiseRatio": -65,
   "channel": 8
  },
  {
   "macAddress": "01:23:45:67:89:AC",
   "signalStrength": 4,
   "age": 0
  }
 ]
}
```

Vorab ist es allerdings erforderlich, bei Google [Goo18b] einen sog. API-Key zu erstellen, da nur über einen solchen personalisierten Schlüssel auf den Online-Ortungsdienst von Google zugegriffen werden kann. Die Generierung des Schlüssels ist zwar kostenlos, aber dann mit einigen Einschränkungen (z. B. einem Abfragelimit) verbunden.

Die Antwort der Verortung durch Google erfolgt ebenfalls im JSON-Format:

```
{
  "location": {
    "lat": 51.0,
    "lng": -0.1
  },
  "accuracy": 1200.4
}
```

Bei aktuellen Untersuchungen musste zur Verortung auf einem Google Android Smartphone über Apps, wie z. B. Google Maps, immer auch eine Verbindung

zum Internet bestehen. Diese Beobachtung wird dadurch erklärbar, dass immer mehr Android-Entwickler von der älteren Android-Lokalisierung zu den moderneren Google-Play-Services migrieren (Hintergründe und Anwendung siehe [Pat15]). Es ist davon auszugehen, dass die Verortung mittlerweile und zukünftig immer stärker über Googles Online Dienste stattfinden wird und das Gerät keine weiteren lokalen Datenbestände zur Verortung mehr speichern muss.

Ortungsdaten via Systemdienst

Mithilfe des Dienstes Google Now verfolgt Google das Ziel, dem Anwender nur Informationen anzuzeigen, die aktuell von Interesse für ihn sein könnten. Google bewirbt die native iOS-Anwendung bzw. die Android-App inkl. Systemdienst mit Funktionen wie der Darstellung des Wetters zum momentanen Aufenthaltsortes, der aktuellen Fahrzeit zur Arbeitsstelle auf Basis von Google Verkehrsinformationen oder der Speicherung der Parkposition des Fahrzeugs (vgl. [Goo16c]).

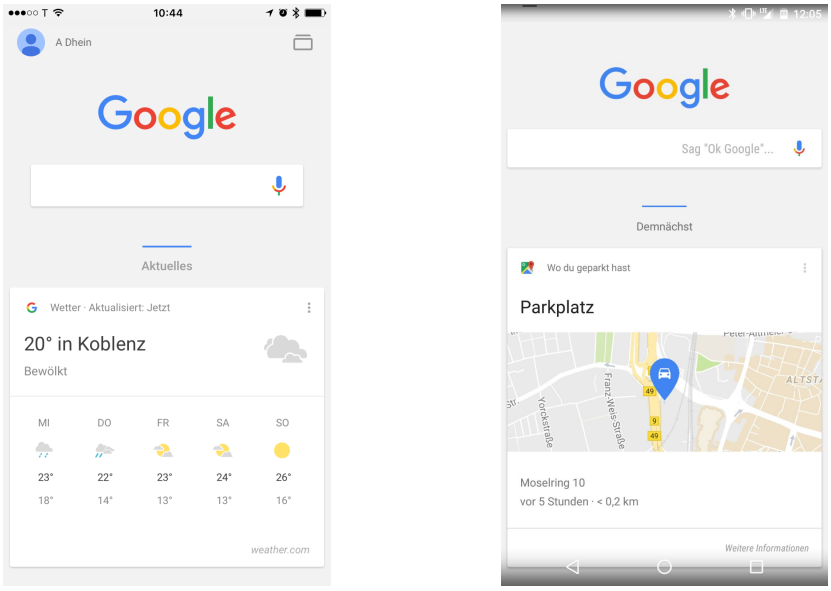


Abb. 4.17: Google Now unter iOS (links) und Android (rechts). Das Assistenzsystem präsentiert nach dem Start mithilfe sogenannter Karten z.B. das Wetter und kann sich auf Wunsch Orte von Interesse, wie bsplw. den Parkplatz, merken.
Quelle: Eigene Darstellung. Kartenmaterial © Google 2017.

Zur Nutzung muss sich der Anwender zunächst bei Google anmelden. Zudem müssen die Standortdienste aktiviert sein. Wie dies zu bewerkstelligen ist, bzw.

welche Probleme bei der Verortung auftreten können, ist online bei Google in [Goo16e] beschrieben. Zur Personalisierung der Informationen (sog. Karten) werden Standortdaten auch im Hintergrund an Google übertragen. Der Standortbericht (alt [Goo16d]) bzw. Standortverlauf [Goo16f], wie sich die Google-Technik neuerdings nennt, steht aber auch anderen Diensten zur Verfügung. So werden die übertragenen Standortdaten z. B. noch für Navigationsvorschläge in Google Maps bzw. die Google Suche allgemein verwendet.

4.2.4 Google Location History

Die Ortungsdaten aller Google Dienste werden zentral im sog. Standortverlauf (engl. locationhistory) im Internet gespeichert. Der Verlauf lässt sich über einen Webbrowser unter `http://www.google.com/locationhistory` betrachten. Wie in Abb. 4.18 unten rechts zu erkennen, muss für die Datenerhebung die Standortfreigabe aktiv sein. Denn nur dann werden auch Standorte gespeichert, obwohl im Verlauf (Abb. 4.18 oben rechts) alle Jahre seit dem Anlegen des Accounts existieren.

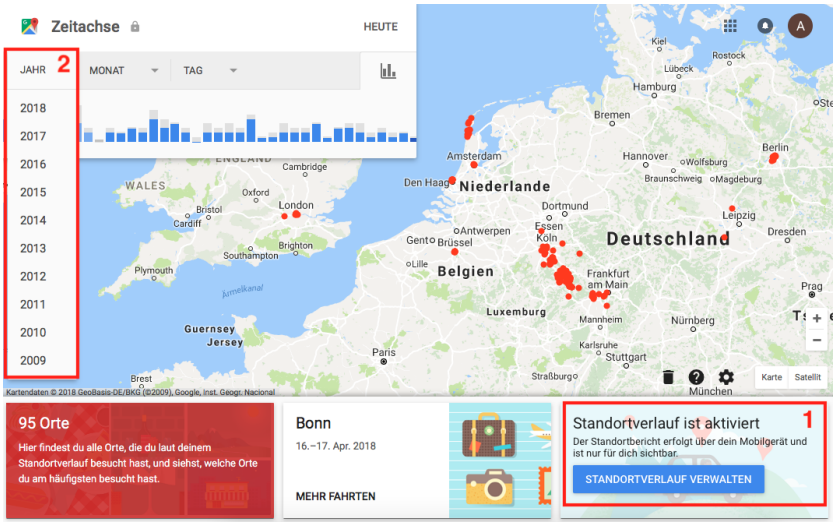


Abb. 4.18: Screenshot der Google Location History. Unten rechts (1) zu erkennen, der Dienst wurde auf dem Smartphone aktiviert. Oben rechts dargestellt (2), es können beinahe beliebig viele Standorte seit Anlegen des Benutzeraccounts gespeichert sein. Quelle: Eigene Darstellung. Kartenmaterial © Google 2018.

Wie in Abb. 4.19 dargestellt, existieren vielfältige Möglichkeiten, die Daten nach der Erhebung zu betrachten. Über einen Klick auf das Zahnradsymbol (unten rechts) lassen sich die »Rohdaten einblenden«. Anschließend werden zusammen mit den Routeninformationen (in der Abbildung links) alle Datenpunkte auf der Karte dargestellt. Bewegt der Anwender die Maus über einen Datenpunkt, so erscheint zusätzlich zum Datum die Genauigkeitsangabe der Verortung in Form eines Kreises bzw. einer Ellipse um den Standort. Der sehr blasse rote Rahmen wurde aus Darstellungsgründen nachträglich hervorgehoben.

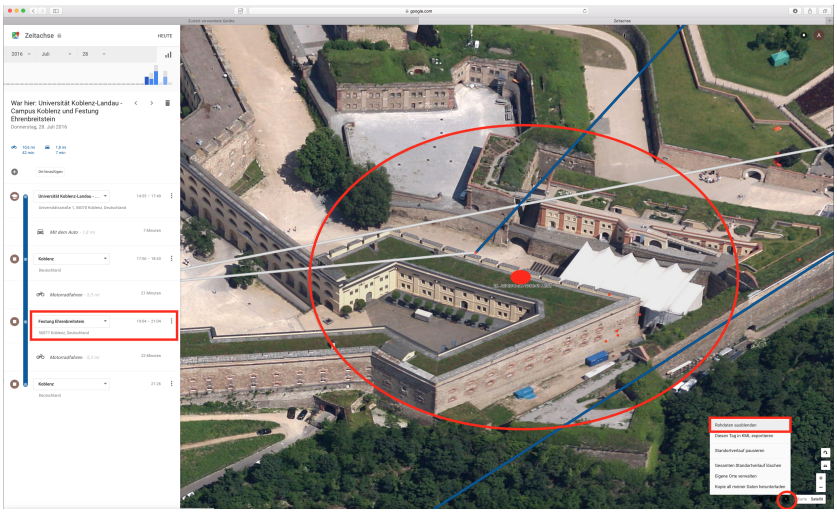


Abb. 4.19: Screenshot Google Location History. Nach dem Einblenden der Rohdaten (unten rechts) lässt sich die Abweichung der Positionsschätzung anzeigen. Quelle: Eigene Darstellung. Kartenmaterial © Google 2016.

Ferner lassen sich die gespeicherten Daten bearbeiten. Der Editiervorgang ist durch simples Auswählen plus einem weiteren Mausklick zu bewerkstelligen. In der Abbildung oben ist hierfür der aktuelle Datensatz markiert (roter Kasten). Über die drei Punkte rechts der Ortsangabe des von Google erkannten Standorts (»Festung Ehrenbreitstein«) lässt sich dieser bearbeiten. Drüber hinaus kann über die Auswahloption rechts der Standort auch komplett aus dem Verlauf gelöscht werden. Die Möglichkeit der forensischen Nutzung potentiell manipulierbarer Daten wird hierdurch angreifbar. Der Ermittler ist demnach gehalten, die Daten sorgfältig auf ihre Kausalität hin zu überprüfen und durch weitere Erkenntnisse zum Aufenthaltsort des Betroffenen im Verfahren zu untermauern.

Umgekehrt hält sich der Aufwand zur Extraktion bzw. Speicherung der Daten durch den Forensiker in Grenzen. Über das zuvor erwähnte Zahnradsymbol (vgl. Abb. 4.19 auf der vorherigen Seite) lässt sich eine Kopie der Daten herunterladen. Die genaue Vorgehensweise ist im Internet unter `http://www.google.com/locationhistory` detailliert beschrieben. Nach dem Klick auf den Download-Button öffnet sich ein neues Browserfenster zur Festlegung des Datenformates. Zur Auswahl stehen JSON und KML. Im Ergebnis stellt der Google-Dienst ein Archiv zusammen, dass nach Fertigstellung heruntergeladen werden kann. Selbstverständlich funktioniert diese Form der Beweissicherung nur, wenn die Zugangsdaten des Benutzers bekannt sind.

Aus forensischer Sicht ist es ebenfalls erfreulich, dass sich beim Datenexport im JSON-Format mitunter weitere Angaben zum Standort ermitteln lassen. Wie in Ausgabe 4.8 dargestellt, sind allerdings nicht immer alle möglichen Parameter wie Höhe (altitude), horizontale und vertikale Fehlerabweichung (accuracy, vertical-Accuracy), Geschwindigkeit (velocity), Richtung (heading) und Verlässlichkeit (confidence) in jedem Datensatz gespeichert.

```
{
  "locations" : [ {
    "timestampMs" : "1470222047464",
    "latitudeE7" : 503401372,
    "longitudeE7" : 75467271,
    "accuracy" : 26
  }, {
    "timestampMs" : "1470221808000",
    "latitudeE7" : 503402825,
    "longitudeE7" : 75464066,
    "accuracy" : 10,
    "velocity" : 0,
    "altitude" : 87,
    "verticalAccuracy" : 4
  }, {
    "timestampMs" : "1470221650000",
    "latitudeE7" : 503425770,
    "longitudeE7" : 75459492,
    "accuracy" : 10,
    "velocity" : 6,
    "heading" : 181,
    "confidence" : 83,
    "verticalAccuracy" : 4
}
```

Terminalausgabe 4.8: Auszug aus der Datei Standortverlauf.json. Neben Geokoordinaten speichert Google zusätzliche Standortinformationen, wie z. B. Standortgenauigkeit (accuracy), Geschwindigkeit (velocity), Richtung (heading) oder Verlässlichkeit (confidence) zum Standort.

Um nach dem Wegfall gespeicherter Ortungsdaten auf Android-Geräten >3.0 wieder auswertbare Standortinformationen verarbeiten zu können, wurde im Rahmen dieser Arbeit die Desktop-Anwendung AndroidTrackerLE (vgl. [(4r12]) zum GoogleTrackerLE weiterentwickelt. Neben Standortinformationen aus Google-Suchanfragen im RAM (vgl. Abb. 4.20: »RoastLamb GPS Positionen«) lassen sich mithilfe der Software Ortungsdaten aus dem Standortverlauf von Google auf einer Karte darstellen. Der in der Abbildung unten ausgewählte Datensatz (siehe Zeitleiste links), ist in der Kartenansicht rechts mit einem roten Kreis markiert. Das besondere hierbei ist die Auswertung der Richtung und auch Geschwindigkeit zum Zeitpunkt der Positionsbestimmung (vgl. roter Kasten im Notizfeld der Anwendung unten). So kann das GPS-Symbol im richtigen Winkel gedreht angezeigt werden.

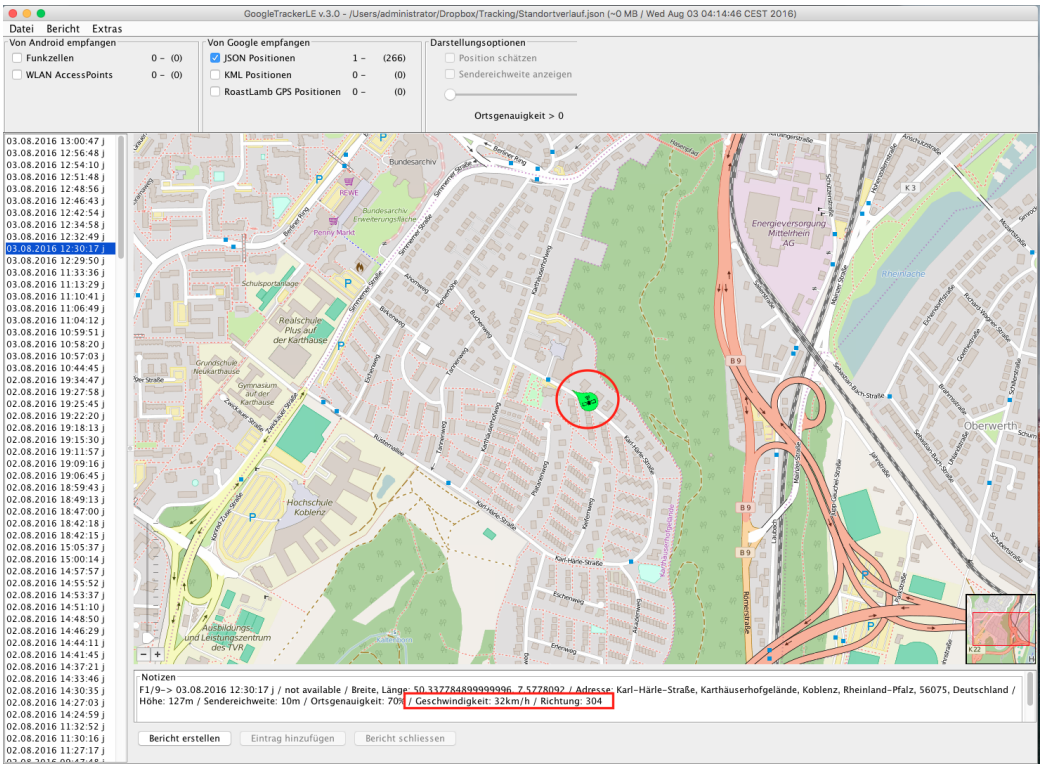


Abb. 4.20: AndroidTrackerLE: Darstellung des JSON Standortverlaufes von Google. Für die kriminalistische Betrachtung sind vor allem die Standortabweichung (accuracy) aber auch weitere Detailinformationen wie Geschwindigkeit und Kursangabe von Interesse (siehe rote Umrandungen).
Quelle: Eigene Darstellung. Kartenmaterial: © OpenStreetMap Mitwirkende 2011.

4.2.5 Zusammenfassung

Es existieren keine GPS-Ortungsdaten

Alle im Rahmen dieser Arbeit untersuchten Cache-Dateien bis Android v.2.3 beinhalten ausschließlich Standortinformationen zu Mobilfunk- bzw. Drahtlosnetzwerken. Der Ortungsdienst in späteren Android-Versionen speichert dann keine Positionsdaten mehr auf dem Gerät.

Zusätzlich sorgt Google mit der Einführung der Google Location-Services-API (vgl. [Goo17d]) dafür, dass bei jeder Verortung Informationen zu Funksendern in der Umgebung des Gerätes an Google übersandt werden (vgl. Abschnitt 4.2.3 auf Seite 122). Die Verortung über GPS, wie sie noch mit der Android Location-API möglich gewesen ist, wird von Google aus Performancegründen nicht mehr empfohlen (siehe [Pat15]).

Bei keiner Untersuchung ließen sich auf dem Gerät Harvesting-Daten, wie sie bei Apple (vgl. Abschnitt 4.1.3 auf Seite 87) existieren, bei Google feststellen.

Neue Wege der Datenakquise

Durch die fehlenden Ortungsdateien des Systemdienstes seit Android 3.0 scheint die forensische Auswertung von Standortdaten zunächst auf Informationen aus Metadaten zu Bildern etc. begrenzt. Dafür bieten sich durch die vielfältige Online-Speicherung von Daten bei Google neue Ermittlungsansätze.

Interessant ist der Zugriff auf den Online-Datenpool bei Google vor allem, weil hier potentiell auch Standortinformationen aus anderen Plattformen (iOS, macOS, Windows, Linux, etc.) über Google-Apps gespeichert sein könnten. Wie in Abschnitt 4.2.3 auf Seite 124 ausgeführt, erfolgt die Generierung von Daten für die Google Location History (siehe Abschnitt 4.2.4 auf Seite 125) erwiesenermaßen auch bei iOS Geräten und sogar über mobile oder stationäre Computersysteme. Die Datenakquise vom Google-Konto des Betroffenen sowie die Untersuchung der exportierten Daten innerhalb des im Rahmen dieser Arbeit entwickelten Forensik-Tools GoogleTrackerLE gestaltet sich sehr einfach. Für die Zukunft könnte so die fehlende Speicherung von Ortsinformationen auf Google-Geräten

den Ermittlungsbehörden, wenn rechtlich zulässig, durch die Akquise und Verarbeitung anderer Datenquellen zugute kommen?!

Bewertung der Qualität von Standortdaten bei Google

Die Standortinformationen der Cache-Dateien von Android scheinen zunächst weniger anfällig für Störungen zu sein, als dies bei Apple-Daten mitunter der Fall ist. Aber auch bei Android konnten Konstellationen bei der aGPS-Verortung festgestellt werden, die falsche Positionsangaben nach sich gezogen haben (vgl. Abschnitt 4.2.2 auf Seite 115). Dadurch, dass bei Android noch keine vom Gerät selbst erhobenen GPS-Informationen während der Untersuchungen im Rahmen dieser Arbeit ermittelt werden konnten, lässt sich eine Bewertung von GPS-Daten unter Android schlicht nicht vornehmen.

Wie in Abschnitt 4.2.4 auf Seite 125 ausgeführt, beinhalten die heruntergeladenen Geodaten der Google Location History sowohl die Angabe der Genauigkeit als auch die maximale Standortabweichung (accuracy) sowie eine Prozentangabe bzgl. der Verlässlichkeit (confidence) des Datensatzes. Zahlreiche Vergleiche mit Apple iOS lassen erkennen, dass Standortdaten von Google eine höhere Präzision sowie Verlässlichkeit aufweisen, als entsprechende Einträge in Apples Ortungsdatenbank (vgl. Ausgabe 4.2.4 auf Seite 127 bzw. Abschnitt 4.1.2 auf Seite 76).

Dementgegen steht die Möglichkeit, Einträge im Google Standortverlauf bewusst zu manipulieren. Hierdurch wird die Qualität hinsichtlich der Integrität von Standortdaten bei Google gemindert. Bezogen auf die Vollständigkeit der Daten ist hingegen anzumerken, dass keinerlei Beschränkung hinsichtlich der Speicherfristen existiert. Dieser Umstand kommt insbesondere Ermittlungen zu Straftaten zugute, die längere Zeit zurückliegen. Umgekehrt besteht immer die Gefahr, dass gezielt einzelne Datensätze oder auch der gesamte Standortverlauf gelöscht wird. Die Datenlöschung ist auch nach Sicherstellung des Gerätes online über den Google-Account durch den Betroffenen möglich.

Wie bereits in Abschnitt 4.1.4 auf Seite 107 ausgeführt, kann der Veröffentlichung der untersuchten Daten bei Google aus den genannten Gründen ebenfalls nicht entsprochen werden. Einem kritischen Leser können aber auch die von Google gesicherten Daten demonstriert werden.

Teil 5

Absicherung der analytischen Interpretation durch native Apps

Bei der Erstellung von Gutachten oder zur Absicherung von Erkenntnissen bzgl. unbekannten Datenquellen wird in der Forensik häufig die zu untersuchende Software auf einem Referenzsystem installiert. Anschliessend lassen sich sowohl das Verhalten des Systems als auch die generierten Artefakte gezielt analysieren. Dieses Vorgehen ist für die Untersuchung von mobilen Apps und insbesondere mobiler Systemdienste so nicht anwendbar. Zwar ist es möglich, im Rahmen der forensischen Untersuchungen Artefakte von Herstellertools wie Apple Maps zu untersuchen. Auf die Inhalte von Apples Ortungsdatenbank erhält der Analyst hingegen ohne erweiterte Systemrechte keinen Zugriff.

Mithilfe einer nativen App zur Untersuchung systembezogener Standortdaten kann, entsprechende Systemrechte durch einen Jailbreak vorausgesetzt, direkt auf die Rohdaten der Datenbank zugegriffen werden. So ist es dann möglich, die Analyse der Ortungsdienste und die Entstehung von Standortdaten gezielt nachzuvollziehen und zusätzlich Einfluss auf bestimmte Parameter der Lokalisierung zu nehmen (siehe später in Abschnitt 5.2 auf Seite 136).

Darüber hinaus lassen sich die Ergebnisse der Untersuchungen speichern und für spätere Analysen konservieren. Die Problematik des Löschens von Ortungsdaten bei Apple kann z. B. dadurch umgangen werden, dass die Datenbanken vor der Verbindung mit dem heimischen WLAN in einem Archiv gesichert werden.

5.1 Eigenentwicklungen für iOS und Android

Für die Untersuchung der Entstehung von Ortungsdaten direkt auf den Geräten wurden insgesamt drei mobile Apps entwickelt (iOSTracker, WatchTracker und DroidTracker), die im Folgenden vorgestellt werden.

Mit dem iOSTracker entstand bereits sehr früh die erste native Anwendung zur tiefergehenden Analyse von Ortungsdaten im Rahmen dieser Arbeit. Die App ist in der Programmiersprache Objective-C für iOS ab Version 4 implementiert. Bis heute sind nur Anpassungen aufgrund geänderter Darstellungstechniken in iOS7 vorgenommen worden. Der Hauptteil der App (CLLocationManager [App16f]) funktioniert unverändert bis einschließlich iOS10. Darüber hinaus ermöglicht eine eigene Implementierung, verschiedene Präzisionsanforderungen zu testen. Weitere Details hierzu siehe Abschnitt 5.2 auf Seite 136.

Die Software erlaubt sowohl die gezielte Steuerung der Ortungsdienste durch Ein- bzw. Ausschalten als auch das Betrachten der Inhalte der Ortungsdatenbank. In der Kartenansicht (MapView; in Abb. 5.1) lässt sich der Ortungsdienst starten

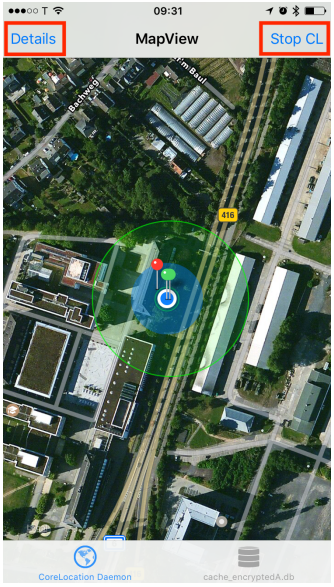


Abb. 5.1: Screenshot iOSTracker: Die Positionsschätzung wird inkl. der maximalen Abweichung dargestellt. Kartenmaterial © Apple 2016.

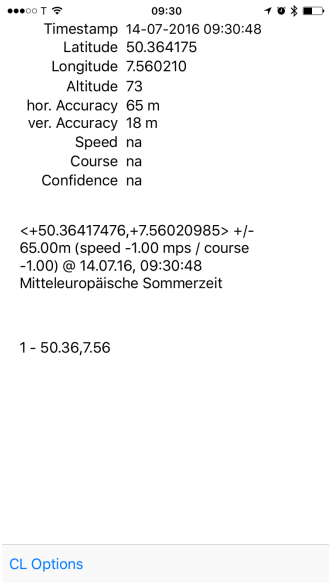


Abb. 5.2: Screenshot iOSTracker: Über eine Detailseite lassen sich weitere Informationen zur Verortung ablesen.

und die Verortung live mitverfolgen. Hierbei wird zu Beginn jeder Verortung eine Stecknadel inkl. der Accuracy in Metern auf die initiale Position gesetzt. Während der laufenden Verortung kann in der Detailansicht (vgl. Abb. 5.2 auf der vorherigen Seite) die Ausgabe des CoreLocationDaemons (ein String mit Angabe der Geokoordinate, Genauigkeit (in Metern), Geschwindigkeit (Meter pro Sekunde) und zusätzlich Richtung (in Grad; 0=Nord) inkl. Datum und der aktuellen Uhrzeit) sowie zusätzlich die Interpretation der Werte angezeigt werden.

Zur Betrachtung der Inhalte der Ortungsdatenbank, wie in Abb. 5.3 dargestellt, ist ein Jailbreak bzw. Zugriff mit speziellen Systemrechten erforderlich. Mithilfe der erweiterten Zugriffsrechte durch den Jailbreak lassen sich dann die Einträge aller Tabellen mit Geodaten betrachten. Dargestellt wird hierbei immer der erste Eintrag aller Einträge mit validen Ortungsdaten zum Zeitpunkt der Datenerhebung, falls mehrere Einträge zum gleichen Zeitpunkt existieren. Nach der Auswahl einer Zeile (rote Markierung in Abb. 5.3) öffnet sich eine Kartenansicht (vgl. Abb. 5.4) mit weiteren Details zu dem ausgewählten Eintrag. Hier lassen sich dann über einen Button oben rechts in der Ansicht wahlweise alle Standorte (»all«) oder nur der Erste (»single«) zum ausgewählten Eintrag darstellen.

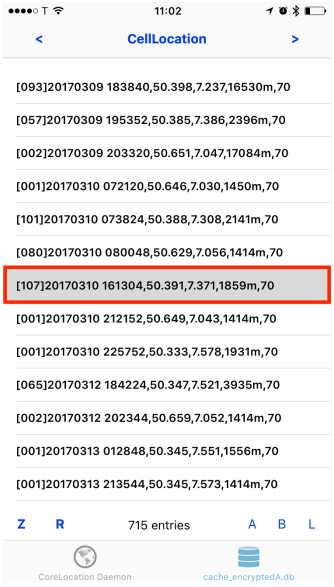


Abb. 5.3: Screenshot iOSTracker: Auflistung gespeicherter Ortsinformationen in der Ortungsdatenbank von Apple.

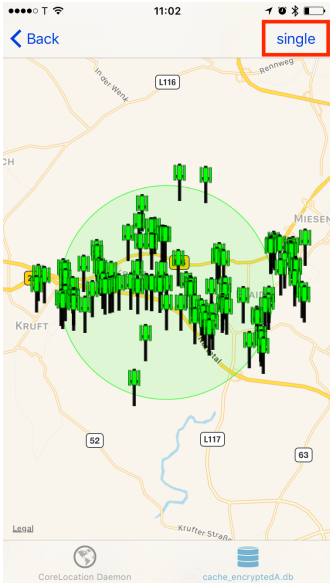


Abb. 5.4: Screenshot iOSTracker: Betrachtung gespeicherter Positionsdaten in einer Kartenansicht. Kartenmaterial © Apple 2017.

Die zweite Anwendung (WatchTracker) befindet sich noch in der Entwicklung. Neben dem Umstieg auf die aktuelle Programmiersprache Swift ist die Idee zu dieser App, Ortungsfunktionen auf Wearables zu untersuchen. Es ist geplant, Ortungsdaten auf der Apple Watch aufzuzeichnen und anschließend auf dem iPhone retrograd zu betrachten. Die App muss auch ohne Jailbreak vollumfänglich nutzbar sein, da bislang noch kein Jailbreak für die Apple Watch veröffentlicht wurde. Der Funktionsumfang beschränkt sich aktuell auf das Aufzeichnen bzw. Betrachten von Standortdaten auf dem Smartphone (siehe rote Kästen unten in Abb. 5.5). Über die Schaltfläche unten links in wird die Verortung mit Standardparametern des Systemdienstes gestartet und kann nach dem Beenden über den Slider (unten rechts) retrograd wiedergegeben werden. Über den Knopf oben rechts (Ordnersymbol) kann der Anwender in die Übersicht zu den aufgezeichneten Positionsdaten wechseln (vgl. Abb. 5.6). Auffällig ist, dass Positionsdaten i. d. R. nicht fortlaufend erhoben werden. Dafür existieren häufiger mehrere Positionsdaten zu einem Zeitpunkt (vgl. auch Abschnitt 4.1.2 auf Seite 81). Weitere Informationen hierzu folgen in Abschnitt 5.2 auf Seite 136.

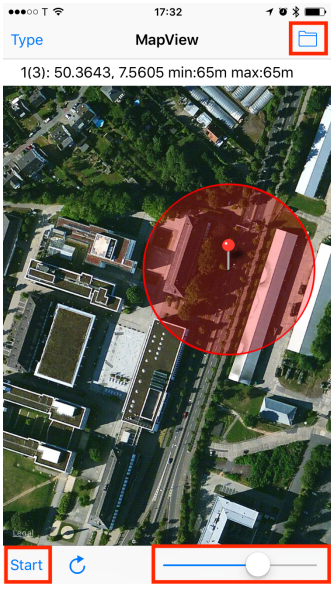


Abb. 5.5: Screenshot WatchTracker: Die App ermöglicht über eine Zeitschiene (unten) das Nachvollziehen der Verfeinerung der Lokalisierung. Kartenmaterial © Apple 2016.

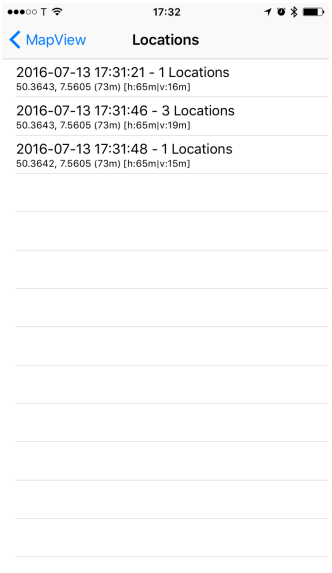


Abb. 5.6: Screenshot WatchTracker: Aufgezeichnete Ortungsdaten in einer Liste. Auffällig: es werden mitunter mehrere Datensätze zu einem Zeitpunkt ermittelt.

Zur praktischen Untersuchung der Ortungsfunktionen unter Android wurde im Rahmen dieser Arbeit analog zu den oben beschriebenen Anwendungen auch eine native App für Google Android entwickelt. Die Anwendung ermöglicht es, den Ortungsdienst von Android ein- bzw. wieder auszuschalten und dabei die Verbesserung der Positionsschätzung zu beobachten (siehe Abb. 5.7). Darüber hinaus lassen sich über die Detail-View die aGPS-Funkempfänger, wie in Abb. 5.8 zu sehen, gezielt ein- bzw. ausschalten. Hierdurch besteht (anders als bei iOS) die Möglichkeit, unmittelbar Einfluss auf die maximal mögliche Genauigkeit der Standortlokalisierung zu nehmen. Hierzu mehr in Abschnitt 5.5.2 auf Seite 144.

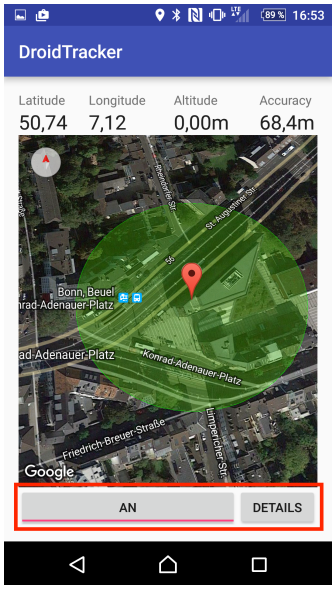


Abb. 5.7: Screenshot DroidTracker: Positionsschätzung nach dem Starten des Ortungsdiensten in einer Kartenansicht. Kartenmaterial © Google 2017.

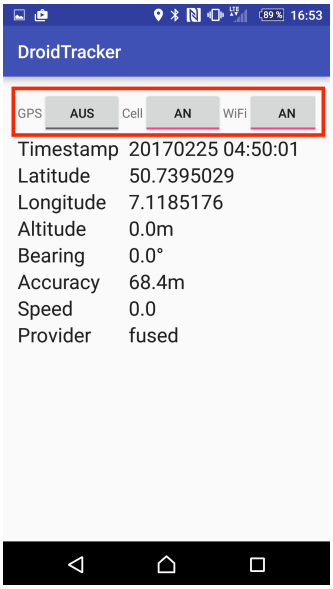


Abb. 5.8: Screenshot DroidTracker: Über die Detailansicht lassen sich weitere Informationen zur Verortung ablesen sowie unterschiedliche Positionsprovider einstellen

Der DroidTracker wurde in Java zunächst für API Level 21 (Lollipop bzw. A5) als Zielplattform entwickelt. Unter A5 war der Standardweg zur Verortung noch die Android Location API. Mit der Umstellung auf API Level 23 (Marshmallow bzw. A6) wurde dann auch auf die neue Methode zur Verortung über Google Play Services umgestellt. Wie im Folgenden weiter ausgeführt, existieren verschiedene Wege zur Verortung bei Google (vgl. [Pat15]) bzw. beeinflussende Faktoren bei Google und Apple, die mithilfe von eigenen Implementierungen nativer Apps sehr gut analysiert werden können.

5.2 Einstellmöglichkeiten für Entwickler

Entwickler nativer Applikationen für mobile Endgeräte können eine Vielzahl energetischer Einstellmöglichkeiten nutzen damit die Akkuleistung aktueller Smartphones mindestens den Tag überdauert. Hier unterliegt die Genauigkeit von Standortinformationen unter Umständen der Nutzungsdauer. Online sind die Best-Practices in den entsprechenden Entwicklerdokumentationen bei Apple [App18] bzw. Google [Goo18a] nachzulesen.

Standardmäßig, d.h. ohne expliziten Parameter beim Aufruf des CLLocation-Managers, verwendet Apple die Einstellung `kCLLocationAccuracyBest`. Allerdings gilt diese Einstellung bei Apple ohnehin nur als Best-»wenn-möglich«-Genauigkeit. In der Entwicklerdokumentation heißt es hierzu »When requesting high Accuracy location data, the initial event delivered by the location service may not have the Accuracy you requested.« [App16f]. Darüber hinaus haben sich die Parameter seit der Einführung von iOS2.0 kaum verändert (vgl. [App16c]):

- `kCLLocationAccuracyBest` (seit iOS2.0)
  - Use the highest-level of Accuracy.
- `kCLLocationAccuracyNearestTenMeters` (seit iOS2.0)
  - Accurate to within ten meters of the desired target.
- `kCLLocationAccuracyHundredMeters` (seit iOS2.0)
  - Accurate to within one hundred meters.
- `kCLLocationAccuracyKilometer` (seit iOS2.0)
  - Accurate to the nearest kilometer.
- `kCLLocationAccuracyThreeKilometers` (seit iOS2.0)
  - Accurate to the nearest three kilometers.
- `kCLLocationAccuracyBestForNavigation` (seit iOS4.0)
  - Use the highest possible Accuracy and combine it with additional sensor data. This level of Accuracyy is intended for use in navigation applications that require precise position information at all times and are intended to be used only while the device is plugged in.

Hinweise auf die verwendeten Funkempfänger zur Verortung gibt Apple nicht.

Google verfolgt bei der Bezeichnung eine gegenteilige Strategie und bezieht sich auf die Verortungsmethode bzw. den Daten-Provider anstelle der angestrebten Genauigkeit bei der Standortbestimmung.

Darüber hinaus existieren unter Android zwei APIs zur Verortung:

- Android Location API (alt - Standard bis Android 5)
  - `android.location.LocationListener`
- Google Play Services APIs (neu - seit Android 6 bevorzugt)
  - `com.google.android.gms.location.LocationListener`

Die ältere Android Location API kennt so z. B. drei Location-Provider [Goo17d]:

- `LocationManager.GPS_PROVIDER` - This provider determines location using satellites. Depending on conditions, this provider may take a while to return a location fix.
- `LocationManager.NETWORK_PROVIDER` - This provider determines location based on availability of cell tower and WLAN access points. Results are retrieved by means of a network lookup.
- `LocationManager.PASSIVE_PROVIDER` - This provider will return locations generated by other providers. You passively receive location updates when other applications or services request them without actually requesting the locations yourself.

Die aktuellere und laut Google zu bevorzugende Variante (vgl. [Goo18c]) zur Geolokalisierung über die Google Play Services verspricht dem Entwickler durch die Verwendung der `FusedLocationProviderApi` ressourcenschonender zu arbeiten (vgl. [Goo17c]). Im Rahmen der Entwicklung der nativen Anwendung DroidTracker wurde zunächst die Android API und später bzw. aktuell nur noch die Google Play Services API zur Standortbestimmung verwendet.

Seit Android 6 (Codename Marshmallow bzw. API Level 23) wird ferner dem Datenschutz verstärkt Rechnung getragen. So müssen nunmehr in der Datei `AndroidManifest.xml` zwingend die Berechtigungen für die erwünschte maximale Genauigkeit `ACCESS_COARSE_LOCATION` bzw. `ACCESS_FINE_LOCATION` hinterlegt werden [Goo17b].

Generell lässt sich festhalten, dass die iOS Implementation besser abstrahiert, Google dafür auf den ersten Blick mehr Einstellmöglichkeiten bietet.

Mit der Integration des M7-Koprozessors im Jahr 2013 bietet sich für Apple die Gelegenheit, die Verortung anhand des aktuellen Aktivitätstyps (vgl. [Bal13]) zu beeinflussen. Bereits ein Jahr zuvor hat Apple im September 2012 mit iOS6 die nachfolgenden Parameter hinzugefügt, welche sich direkt auf die Aktualisierung des LocationManagers bzw. den Energieverbrauch auswirken.

Gemäß [App16f] lassen sich so vier Aktivitätstypen unterscheiden:

- `CLActivityTypeOther` (Standard)
  - The location manager is being used for an unknown activity.
- `CLActivityTypeAutomotiveNavigation`
  - The location manager is being used specifically during vehicular navigation to track location changes to the automobile. This activity might cause location updates to be paused only when the vehicle does not move for an extended period of time.
- `CLActivityTypeFitness`
  - The location manager is being used to track fitness activities such as walking, running, cycling, and so on. This activity might cause location updates to be paused only when the user does not move a significant distance over a period of time.
- `CLActivityTypeOtherNavigation`
  - The location manager is being used to track movements for other types of vehicular navigation that are not automobile related. For example, you would use this to track navigation by boat, train, or plane. Do not use this type for pedestrian navigation tracking. This activity might cause location updates to be paused only when the vehicle does not move a significant distance over a period of time.

Standardmäßig, d.h. ohne explizite Angabe eines Aktivitätstyps, wird zunächst die Option `CLActivityTypeOther` angenommen. Hier ist zu erwarten, dass keine Energiesparoptionen greifen und der Standort häufig aktualisiert wird. Bei allen anderen Aktivitäten ist dem Ortungsdienst programmatisch vorgegeben, die Ortung auszusetzen (`pausesLocationUpdatesAutomatically: TRUE`), wenn keine Bewegung mehr erkannt wird. Die Pause dürfte je nach Aktivität variieren. Und wenn keine neuen Standorte mehr erhoben werden, ist mit Lücken in den Ortungsdaten zu rechnen.

5.3 Retrogrades Datentracking

Zusätzlich zur Betrachtung von Standortdaten zeichnet die App iOSTracker auch selbst Standortdaten auf. Anhand der erhobenen Daten lässt sich so zunächst die Verbesserung der Ortungsgenauigkeit im Verlauf der Lokalisierung belegen. Des Weiteren können die gespeicherten Ortungsdaten in späteren Auswertungen am PC mit Daten der Ortungsdatenbank korreliert werden (vgl. Abb. 5.9). Hierbei lässt sich mithilfe einer Kennzeichnung der Datensätze (r=recorded, g=gps, c=cell, w=wifi) in der Zeitleiste sehr anschaulich nachvollziehen, wann der Ortungsdienst durch die App genutzt wurde.

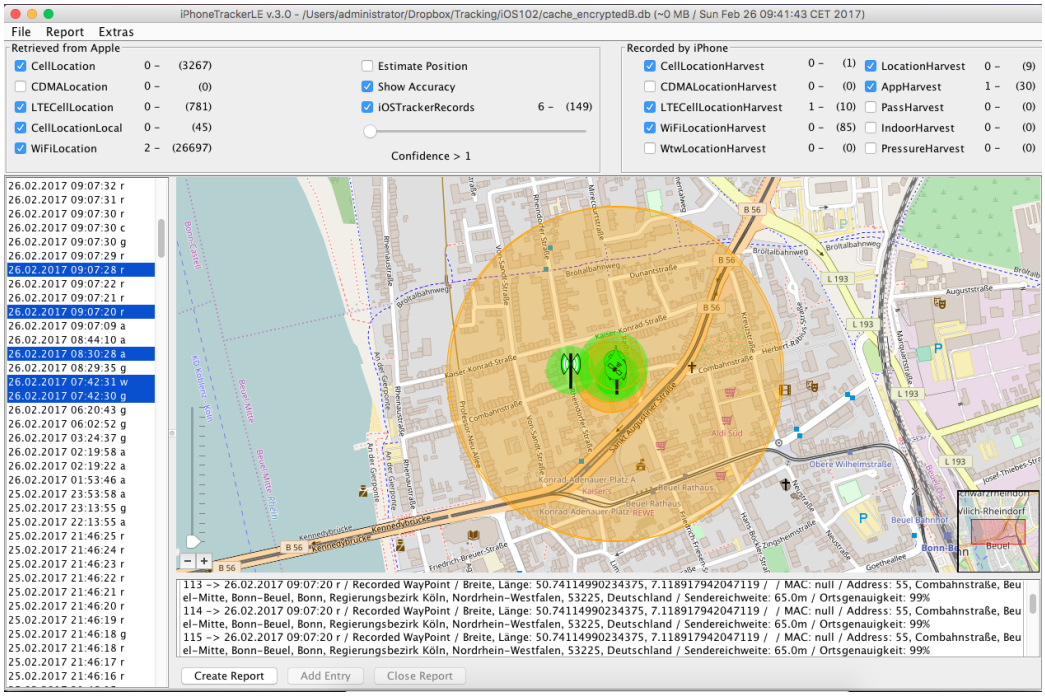


Abb. 5.9: Screenshot iPhoneTrackerLE: Möglichkeit der Korrelation aufgezeichneter Messdaten aus dem iOSTracker mit Daten aus der cache_encryptedB.db. Quelle: Eigene Darstellung. Kartenmaterial: © OpenStreetMap Mitwirkende 2017.

Im Rahmen dieser Arbeit wurden vielfältige Tests durchgeführt. So wurden auch Versuche unter außergewöhnlichen Umständen, wie z.B. anlässlich einer Flugreise unternommen. Hierbei konnte festgestellt werden, dass während des Fluges der GPS-Empfang besonders gut funktioniert und auch Mobilfunk-Signale noch in großer Höhe zu empfangen sind. Dementgegen konnten keine WLAN-Signale festgestellt werden.

Technisch ermöglichen es alle im Zusammenhang mit dieser Arbeit entwickelten mobilen Applikationen Daten für eine spätere Auswertung am Computer zu konservieren. Wie in Abb. 5.9 auf der vorherigen Seite zu sehen, bieten aber nur die Softwarekombination iOSTracker (auf dem Smartphone) und iPhoneTrackerLE (auf dem Computer) die Möglichkeit, die erhobenen Positionsdaten der Testläufe retrograd mit den von der App aufgezeichneten Daten zu korrelieren.

Insgesamt führte das retrograde Datentracking zu einem besseren Verständnis der Ergebnisse der durchgeführten Untersuchungen. Ohne Tracking wäre die Rekonstruktion des Standortverlaufs sonst nur auf Basis von Erinnerungen oder im besten Fall sonstiger schriftlicher Aufzeichnungen möglich gewesen.

5.4 Auswirkungen von LocationFaker-Apps

Aufgrund der strikten Kapselung von Applikationen sowie der Trennung von System- und Anwenderebene mobiler Plattformen lassen sich Systemdienste, wie der Ortungsdienst, nicht durch andere Anwendungen beeinflussen. Sollen Ortungsdaten gezielt manipuliert werden, ist unter Apple-iOS ein privilegierter Zugriff auf das System erforderlich. Hierfür muss das Gerät jailbroken sein.

Tests mit der iOS-App LocationFaker (vgl. [Cun17]) zeigen, dass es auf einem jailbroken-iPhone ohne großen Aufwand möglich ist, Standortdaten z. B. in Bildaufnahmen zu fälschen. Darüber hinaus lässt sich so der eigene Standort in Karten- wie auch Navigationsanwendungen fälschen, ja selbst die Apple-eigene iPhone-Suche lässt sich auf diese Weise manipulieren (vgl. Abb. 1.12 auf Seite 26). Nur die Daten in der Apple Ortungsdatenbank waren von der Manipulation nicht betroffen.

Bedauerlicherweise konnte nicht abschließend geklärt werden, wie die Software LocationFaker [Cun17] arbeitet. Diverse Anfragen beim Entwickler bzgl. der Arbeitsweise der Anwendung blieben unbeantwortet. Es dürfte sich um eine Technik analog zum Einhängen (sogenanntes hooking) in den Datenstrom des location deamons handeln. Hierbei arbeitet der Ortungsdienst nach wie vor, aber anstelle der Informationen vom Systemdienst erhalten Anwendungen gefälschte Standortinformationen vom LocationFaker.

5.5 Zusammenfassung

5.5.1 Erkenntnisgewinn durch Live-Untersuchungen

Mithilfe der entwickelten Tools konnte die Ortung auf mobilen Endgeräten direkt nachvollzogen sowie anschaulich dargestellt werden. Hierfür wurde zudem die später in Abschnitt 5.5.4 auf Seite 148 ausführlicher beschriebene Funktion zur Reduktion der Funksender implementiert (vgl. Abb. 5.10 rechts), um zu zeigen, dass der Standort des Gerätes zum Zeitpunkt der Verortung tatsächlich innerhalb des Senderadius des initialen Funksenders liegt.

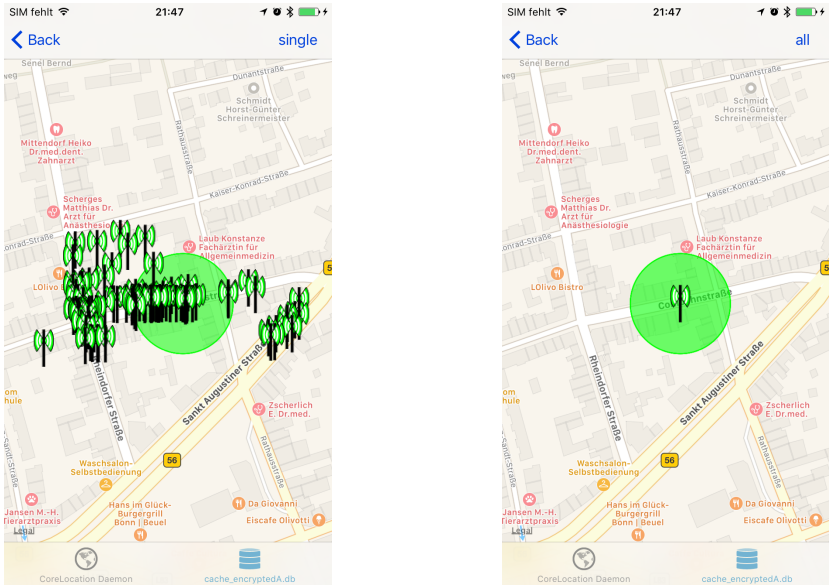


Abb. 5.10: Screenshots iOSTracker. Links: Darstellung aller Funksender zum ausgewählten Zeitpunkt. Rechts: Filterung der Daten und Anzeige des ersten Standorts zum gegebenen Zeitpunkt. Quelle: Eigene Darstellung. Kartenmaterial: © Apple 2017.

Wie in den Abbildungen 5.11 und 5.12 zu erkennen, verläuft die Verortung bei Apple und Google ähnlich. Beide Dienste starten, je nach vorhandenen Daten, zunächst mit der Positionsbestimmung auf Basis von Funkzelleninformationen in der Umgebung und verbessern die Standortgenauigkeit durch Verwendung von Standortdaten umliegender WLAN-Access-Points. Hierdurch verbessert sich die Lokalisierung in Abb. 5.11 auf der nächsten Seite unter Apple iOS von einer initialen Ungenauigkeit von 226m hin zu einer Genauigkeit von 30m innerhalb weniger Sekunden.

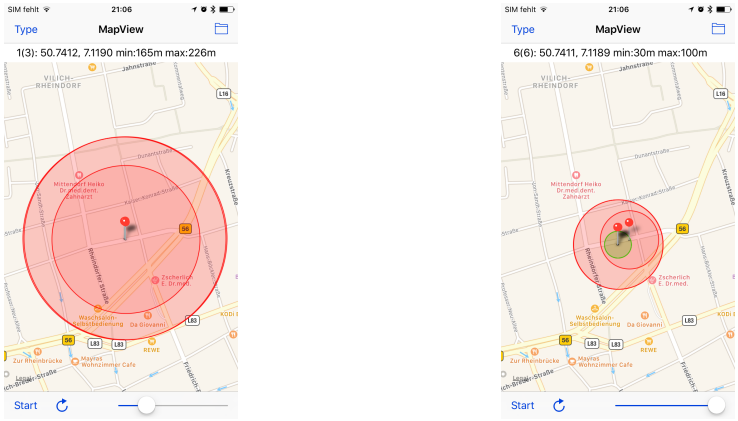


Abb. 5.11: Screenshots WatchTracker. Die Verbesserung der Positionsschätzung (rechts) nach der initial groben Lokalisierung (links) lässt sich über einen Schieberegler retrograd sehr gut nachvollziehen. Quelle: Eigene Darstellung. Kartenmaterial: © Apple 2017.

Die Verortung bei Google in Abb. 5.12 zeigt die Verbesserung der Lokalisierung noch eindrucksvoller. So verbessert sich die initial recht grobe Verortung anhand von Funkzelleninformationen mit einer Ungenauigkeit von knapp einem Kilometer hin zu einer Genauigkeit von ca. 50m bei der letzten Messung ebenfalls innerhalb nur weniger Sekunden.

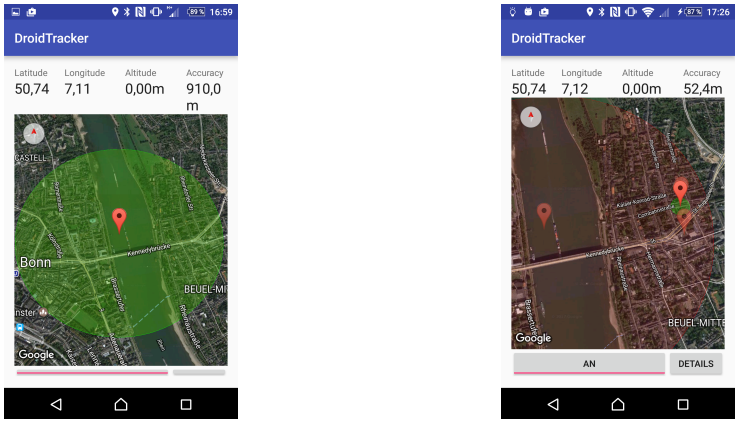


Abb. 5.12: Screenshots DroidTracker: Die Verfeinerung der Lokalisierung über die Zeit lässt sich auch bei Google Android sehr gut nachvollziehen. Links: relativ grobe Initialverortung (910m). Rechts: genauere Positionsbestimmung (52,4m) nach einiger Zeit. Quelle: Eigene Darstellung. Kartenmaterial: © Google 2017.

5.5.2 Generisches Modell zur Beurteilung von Geodaten

Wie in Abschnitt 1.3.4 auf Seite 33 bereits gefordert, soll mithilfe dieser Arbeit ein möglichst unabhängiges Modell zur Entstehung von Ortungsdaten in aktuellen Smartphones skizziert werden. Hierzu wurde zunächst die Geolokalisierung auf Apple Geräten untersucht, welche in Abb. 5.13 grafisch in Form einer Spirale dargestellt ist. Ist die Geräteposition nicht bekannt, überträgt das Smartphone in einer Anfrage an den Provider diverse Funksender aus der Umgebung. Der Provider antwortet entweder mit einer Menge an weiteren Funksendern in der Umgebung (Apple) oder direkt mit einem ersten groben Standort auf Basis von Funkzellenstandorten (Google). Bei beiden Herstellern wird die Positionsbestimmung immer weiter verfeinert, bis eine exakte Position über GPS vorliegt.

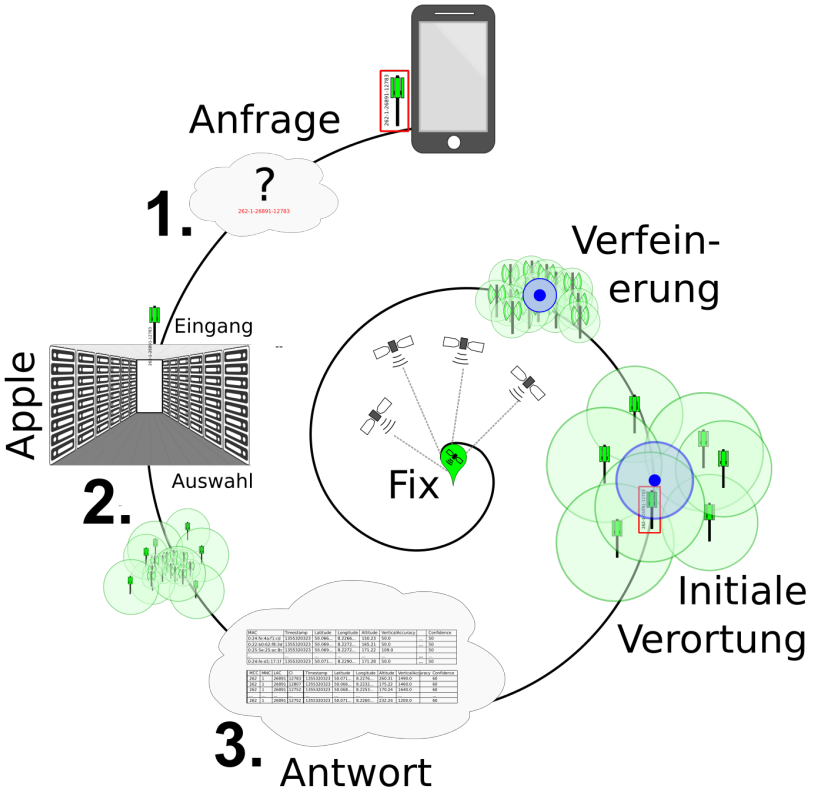


Abb. 5.13: Schematische Darstellung der Verbesserung der Genauigkeit über die Zeit unter Apple iOS in Form einer Ortungsspirale (vgl. [DG16])

Der Prozess der Geolokalisierung unter Android verläuft weitgehend analog. Google beschreibt die Verortung online in der Entwicklerdokumentation in Form eines Zeitstrahls (vgl. [Goo16b]).

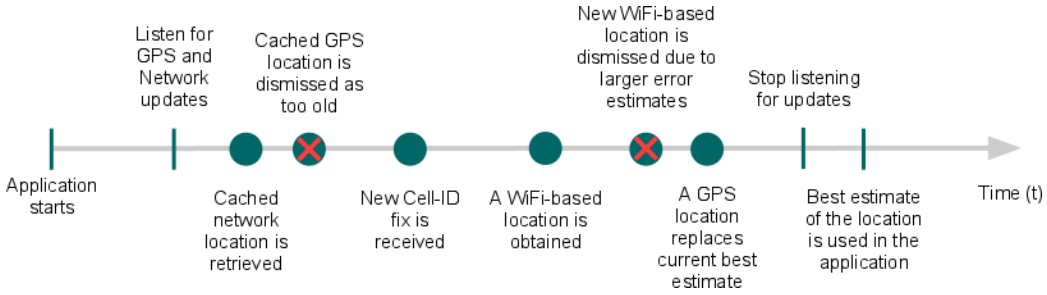


Abb. 5.14: Schematische Darstellung der Verortung unter Android in Form eines Zeitstrahls. Quelle: Entwicklerdokumentation von Google (vgl. [Goo16b])

Die Geräteposition wird so für aGPS auf Basis von Funknetzen in der Umgebung und falls verfügbar und aktiviert über GPS berechnet.

Hierbei wird die Steigerung der Genauigkeit durch Kaskadieren verschiedener Ortungstechniken auf Basis von Funksendern in der unmittelbaren Umgebung und deren Sendereichweite bzw. Empfangsstärke erreicht. Je nach Zeitpunkt seit der Initialverortung und der Verfügbarkeit von Funksendern in der Umgebung dürfte als Modell für die Geolokalisierung die in Abb. 5.13 auf der vorherigen Seite dargestellte Ortungsspirale anwendbar sein.

Genauigkeitskompass

Wie bereits beschrieben, steht die Genauigkeit bei der Geolokalisierung mittels aGPS in unmittelbarem Zusammenhang zur verwendeten Verortungstechnik. In Tab. 5.1 sind hierzu die zu erwartenden maximalen Standortabweichungen (»worst case«) sowie in der Praxis anzunehmende Werte (»Mittlere Genauigkeit«) für unterschiedliche Sensoren angegeben. Die Spalte »Datenbankwerte« bezieht sich auf die untersuchten Ortungsdatenbanken von Apple.

Sensor	Mittlere Genauigkeit	worst case Genauigkeit	Datenbankwerte bei Apple
GPS	1 bis 10m	10 bis 30m	-1 bis 5
WLAN	100m	300m	-1 bis 300
Mobilfunk	100 bis 1800m	34880m [Koma]	-1 bis 38000

Tab. 5.1: Genauigkeit verschiedener Funksender unter Ideal- bzw. schlechten Umgebungsbedingungen im Vergleich zu Werten aus der iOS Ortungsdatenbank.

Umgekehrt sind Rückschlüsse hinsichtlich der Standortgenauigkeit möglich, wenn sich bei fehlenden Accuracy-Angaben die Dichte von Funksendern bzw. Verfügbarkeit von GPS abschätzen lässt.

Darüber hinaus hat sich im Verlauf der im Rahmen dieser Arbeit durchgeführten Untersuchungen seit 2011 gezeigt, dass die Verortung auf mobilen Endgeräten immer verlässlicher wird und Ausreißer bei der Geolokalisierung (vgl. Abschnitt 1.2.3 auf Seite 22) immer seltener werden. Zurückzuführen sein ist diese Erkenntnis auf die zum einen stetig anwachsende Zahl an Funksendern sowie die permanente Optimierung der Ortungsdatenbanken bei Apple, Google und Co..

5.5.3 Schwarmkartierung bei Apple

Die Erfahrungen der zuvor beschriebenen Untersuchungen lassen sich allgemein zur Beschreibung des gemeinschaftlichen (crowd-sourced) Kartierens der Welt durch den Hersteller Apple (aber auch andere) heranziehen.

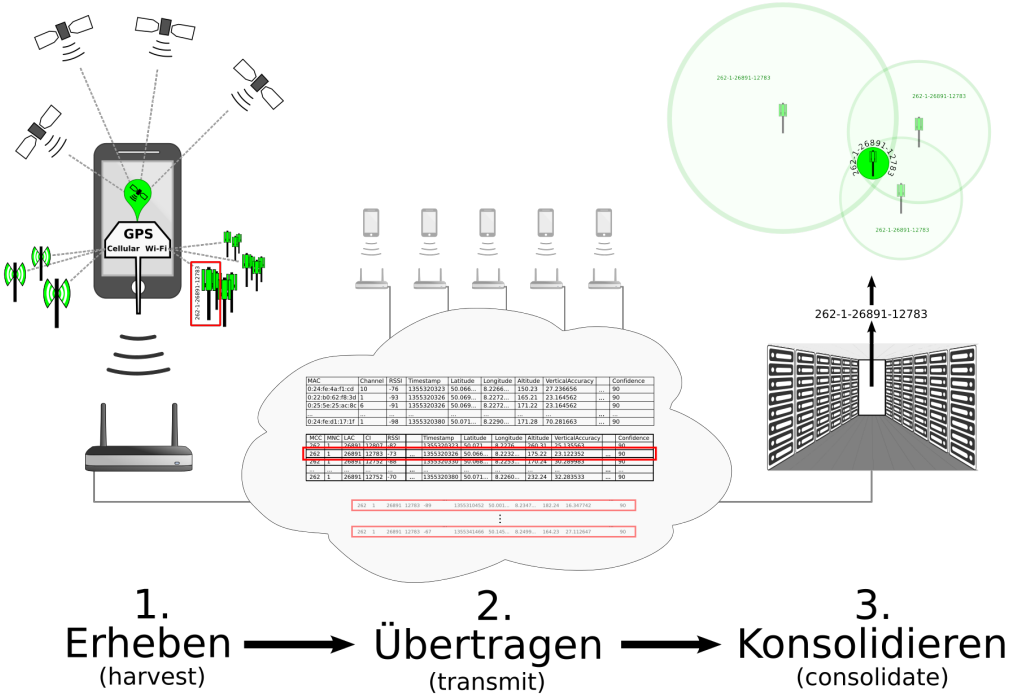


Abb. 5.15: Ablauf der Schwarmkartierung (eigene Wortkreation) bei Apple von der Datenerhebung bis zur Konsolidierung der Daten bei Apple im Überblick.

Wie in Abb. 5.15 auf der vorherigen Seite dargestellt, verläuft der Prozess zur Erstellung und Optimierung der sogenannten crowd-sourced Datenbanken bei Apple in drei Schritten:

1. Daten erheben (harvest)
2. Daten übertragen (transmit)
3. Daten konsolidieren (consolidate).

Im ersten Schritt werden möglichst exakte Gerätepositionen mit eindeutigen Merkmalen (Cell-ID bzw. MAC-Adresse) von Drahtlossendern in der Umgebung erhoben, bevor sie in Schritt zwei zum Hersteller (Apple) übertragen werden. Abschließend werden die Daten dann in der Gesamtdatenbank mit den bereits erhobenen Standorten anderer Nutzer abgeglichen und ggf. zur Konsolidierung (siehe Abb. 5.16) der Standortdaten verwendet.

Hierbei werden die Standortdaten verschiedener Datensätze ($S_{M1}\, bis\, S_{Mn}$) von ein und demselben Funksender so kombiniert, dass die konsolidierte Position des Senders im Schnittpunkt aller Funksender liegt. Wie die Standorte der Funksender bei der Konsolidierung durch Apple tatsächlich berechnet werden, ist ein Betriebsgeheimnis und somit nicht öffentlich bekannt.

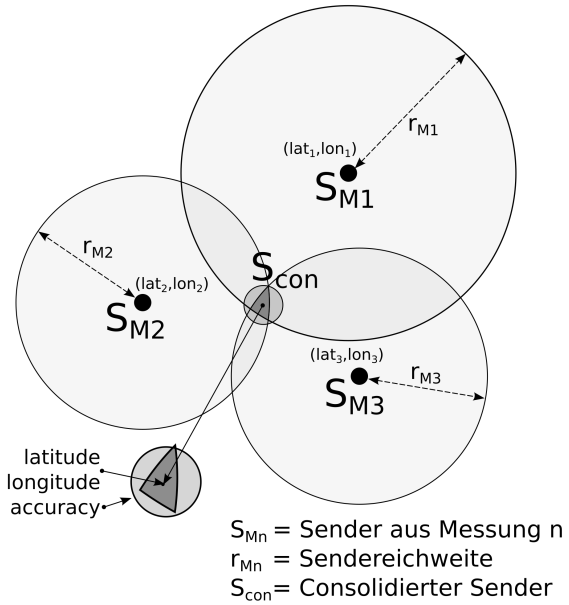


Abb. 5.16: Schwarmkartierung: Schematische Darstellung der Konsolidierung eines Senders auf Basis von drei Datenpunkten aus unterschiedlichen Messungen.

Durch die permanente Aktualisierung des Datenbestandes bei Apple mit ständig neuen Datensätzen lassen sich zwei grundlegende Dinge für die aGPS-Verortung erreichen:

1. Die Positionsschätzung der Drahtlossender wird stetig verbessert.
2. Etwaige Veränderungen der Senderquellen können erkannt werden.

Speziell Veränderungen an Senderquellen stellen, wie bereits in Abschnitt 1.1.2 auf Seite 8 beschrieben, ein großes Problem bei der Verortung mittels aGPS dar. Durch Neuschaltungen, Abschaltungen bzw. Umbenennen von Funkzellen kam es in der Vergangenheit ebenso zu Fehlern bei der Standortbestimmung, wie durch die vorübergehende Nutzung von WLAN-Accesspoints auf Reisen (vgl. [(4r11] - »a day at the Cebit fair 2011 in Hannover« bzw. in Abb. 1.11 auf Seite 24).

Und auch die stetige Verbesserung der Positionsschätzung von Drahtlossendern (siehe oben Punkt Eins) bedeutet nicht, dass die Ortungsdaten den tatsächlichen Standorten der Sender wiedergegeben. Wie in Abb. 5.17 zu erkennen, wird so z. B. ein Mobilfunkmast inmitten des Rheins bei Bonn angegeben.

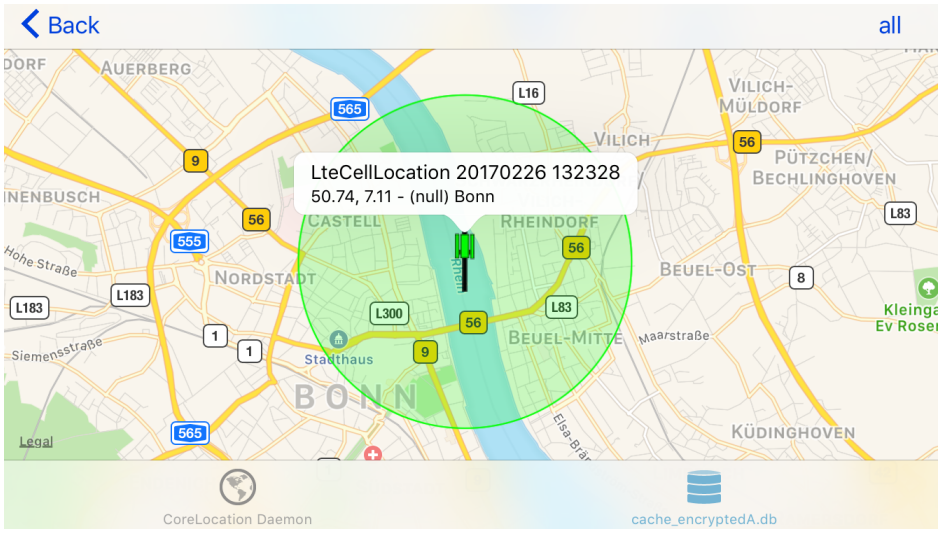


Abb. 5.17: Screenshot iOSTracker: Beispiel einer fehlerhaften Verortung eines Funksenders in der Mitte des Rheins bei Bonn. Quelle: Eigene Darstellung. Kartenmaterial: © Apple 2017.

Selbstverständlich ist dies nicht der Fall. Vielmehr dürfte die kuriose Verortung aus ähnlich vielen Messungen von beiden Seiten des Rheins mit entsprechender Empfangsstärke zum Abstand resultieren.

Tatsächlich spielt die fehlerhafte Positionierung bei der Verortung der Geräte keine große Rolle. Durch die Vielzahl an unterschiedlichen Funksendern, die von Apple an die Geräte übertragen werden, fallen solche Ausreißer nicht weiter ins Gewicht. Einzig die Tatsache, dass das iPhone des Besitzers mitunter vor dem Haus anstelle im Haus verortet wird, lässt sich auf die Schwarmkartierung zurückführen. Bislang wurden nämlich mehr Daten auf Basis von GPS im outdoor-Bereich erhoben als zukünftig möglich, wenn die Daten von indoor-Funksendern vermehrt Eingang in den Datenpool von Apple finden.

5.5.4 Forensische Standortermittlung bei Apple

Der Schlüssel für eine forensische Positionsbestimmung liegt darin, verlässlich den *einen* Standort zu ermitteln, an dem sich das Gerät zum fraglichen Zeitpunkt der Verortung befunden hat. Bei der Verortung über aGPS lässt sich die Position über den Funksender bestimmen, in dessen Empfangsradius sich das Gerät zum Zeitpunkt der Positionsbestimmung befunden hat. Wie bereits in Abschnitt 4.1.2 auf Seite 76ff. beschrieben, existieren allerdings i. d. R. eine Vielzahl möglicher Sender zum Zeitpunkt der Datenerhebung. Und die sind sehr häufig nicht dazu geeignet, einen konkreten Standort anzugeben (vgl. Abschnitt 4.1.2 auf Seite 81).

Im Rahmen der Untersuchung offensichtlicher Möglichkeiten der Reduktion auf nur einen Sender wurden folgende Einträge zum Datensatz / Zeitpunkt in den Tabellen *CellLocation* und *WiFiLocation* untersucht:

- Erster Eintrag
- Letzter Eintrag
- Median der zurückgelieferten Ortsinformationen
- Schwerpunkt der Punktewolke (mit einer Standardabweichung?)

Diskussionen mit Kollegen sowie die Auswertung eigener Tests haben ergeben, dass der Erste Eintrag zu einem bestimmten Zeitpunkt bis iOS10 verlässlich die Senderquelle angibt, in dessen Sendebereich sich das Gerät zum angegebenen Zeitpunkt befunden hat. Diese Erkenntnis ließ sich mithilfe der nativen iOS-App bestätigen (vgl. Abb. 5.10 auf Seite 141).

5.5.5 Forensische Standortermittlung bei Google

Wie in Abschnitt 5.5.4 auf der vorherigen Seite beschrieben, besteht für die Standortbestimmung bei Android unter forensischen Gesichtspunkten ebenfalls die Notwendigkeit, eine konkrete und verlässliche Position zu ermitteln. Analog zu Apple ließen sich auch bei Google in den gespeicherten Ortsinformationen aus Android v2.x zunächst Punktewolken ermitteln. Die hierbei durchgeführten Untersuchungen sowie Erfahrungen mit Apple iOS haben schnell gezeigt, dass die Beschränkung auf den ersten Eintrag zum Zeitpunkt der Datenerhebung auch bei Google zum gewünschten forensischen Ergebnis führt. Weitere Probleme bei der Verortung können zwar noch auftreten, lassen sich aber zuverlässig erkennen (vgl. Abschnitt 4.2.2 auf Seite 115).

Die Verlagerung der Speicherung von Informationen bei Google weg vom Gerät hin in die Cloud verbessert die Situation insofern, dass im sog. Standortverlauf (vgl. Abschnitt 4.2.4 auf Seite 125) nur noch eine Position für jeden Zeitstempel gespeichert wird. Dementgegen sind die Möglichkeiten der Einflussnahme über den Google-Account gegenüber dem forensischen Gesichtspunkt der Sicherheit gegen Veränderungen von Beweismitteln kritisch zu bewerten. So lassen sich z. B. Datensätze gezielt löschen oder bearbeiten. Die hierzu notwendigen Schritte können, wie ebenfalls in Abschnitt 4.2.4 auf Seite 126 beschrieben, sehr einfach über die Weboberfläche von Google durchgeführt werden. So empfiehlt es sich immer, bei der Beweisführung mehrere unterschiedliche Beweismittel kausal in einen Zusammenhang zu bringen und solche mit zweifelhafter Beweiskraft weniger stark zu favorisieren.

Teil 6

Diskussion und Ausblick

In der Diskussion werden zunächst die in Abschnitt 1.3 auf Seite 29 aufgeführten Forschungsfragen hinsichtlich Genauigkeit, Integrität und Vollständigkeit der Daten beantwortet.

Anschließend gilt es, die im Rahmen dieser Arbeit entwickelten Tools und Apps zur Analyse von Geolokalisierungsdaten aus mobilen Endgeräten am Stand der Technik zu messen. Zusätzlich soll diskutiert werden, welche Erfahrungen sich speziell durch die native Untersuchung von Geolokalisierungsdaten auf mobilen Endgeräten ergeben haben bzw. wie sich diese Erkenntnisse auf die kriminalpolizeilichen Ermittlungsmöglichkeiten, insbesondere im Zusammenhang mit dem generischen Modell zur Beurteilung von Ortungsdaten vgl. Abschnitt 5.5.2 auf Seite 143, auswirken.

Im Ausblick werden dann schlussendlich alternative Wege bei der Lokalisierung mobiler Systeme sowie Sigmabereiche als vielversprechende Möglichkeiten zur Verbesserung der Verlässlichkeit bei der Erhebung bzw. späteren Auswertung von Geodaten vorgestellt. Ferner werden mit Windows Mobile, Wearables sowie einer Erweiterung von Exif-Informationen potentiell lohnende Themenfelder für zukünftige Untersuchungen aufgezeigt. Unabhängig davon ist geplant, die Weiterentwicklung bzw. Nutzung der entstandenen Tools durch die Polizei zu ermöglichen.

6.1 Beantwortung der Forschungsfragen

Vollständigkeit von Ortungsdaten aus Smartphones

Zur Beantwortung der Forschungsfrage zur Vollständigkeit von Geodaten aus mobilen Endgeräten (vgl. Abschnitt 1.3.1 auf Seite 30) wird im Folgenden nur auf Ortungsdaten der Systemdienste von Apple und Google eingegangen, da sie die Grundlage für alle auf dem Gerät gespeicherten Geolokalisierungsdaten bilden. Davon abgesehen ist festzuhalten, dass mobile Systeme nur dann auch Geodaten erheben, wenn die Ortungsdienste aktiviert und tatsächlich genutzt werden. Umgekehrt reicht eine Hintergrundnutzung entsprechender Apps aus, damit Ortungsdaten entstehen und ggf. gespeichert werden.

Für Google ist die Frage bezüglich der auf dem Gerät gespeicherten Ortungsdaten kurz und knapp zu beantworten. Vom Systemdienst gepufferte Standortdaten existieren nur in Android 2.2 (froyo) und 2.3 (gingerbread). Darüber hinaus sind die Dateien cache.cell und cache.wifi auf maximal 50 Mobilfunkeinträge sowie 250 Einträge zu Drahtlosnetzwerken beschränkt (vgl. [Eri11a]). Zeitlich ist der Datenumfang durch einen sogenannten Ringspeicher begrenzt, der den ältesten Eintrag löscht, wenn neue Standorte abgerufen bzw. gespeichert werden sollen. Darüber hinaus aktualisiert Android Funkzellenstandorte nach max. 12h und WLAN-Daten nach 48h (vgl. Abschnitt 4.2.2 auf Seite 117). Somit lässt sich sagen, dass die Vollständigkeit der gepufferten Daten auf Google-Geräten, wenn überhaupt verfügbar, sehr stark beschränkt ist.

Dementgegen lassen sich im Internet bei Google potentiell alle jemals vom Gerät erhobenen Standortdaten finden. Abhängig von den Systemeinstellungen zum Standortbericht und der Möglichkeit zur Datenlöschung durch den Anwender speichert Google ansonsten alle Standorte in der Location-History. Die Daten müssen dabei nicht notwendigerweise auf einem Android-Smartphone erhoben worden sein. Wie in Abschnitt 4.2.3 auf Seite 119 beschrieben, ist es Google möglich Standortinformationen auf Basis verschiedenster Google-Dienste zu generieren. Das Sammeln der Daten kann nach der Anmeldung am Google-Konto ebenso bei der Verwendung von Google Now unter iOS geschehen, wie beim Surfen über die Google-Suchseite oder durch Nutzung der Anwendung Google Maps

auf dem Computer. Es lassen sich lediglich keine Daten des Systemdienstes mehr von Google auf Geräten mit aktuellen Android Versionen ermitteln.

Bei Apple iOS hängt die Bewertung zur Vollständigkeit der Ortungsdaten rein von der installierten iOS-Version ab, da Apple im Gegensatz zu Google keine nutzerspezifische Onlinespeicherung vornimmt.

Von iOS4 bis iOS4.3.1 wurden Standortdaten auf Apple-Geräten in einer SQLite3-Datenbank (consolidated.db) ohne jegliche zeitliche Beschränkung gespeichert. Der Umfang an hochwertigen Standortdaten des Systemdienstes entspricht so der Nutzung des Ortungsdienstes bzw. der Übertragung von Funksenderdaten von Apple an das Gerät. Harvesting-Daten werden nach der Übertragung zum Hersteller automatisch gelöscht (vgl. Abschnitt 4.1.3 auf Seite 87).

Mit der Einführung von iOS4.3.3 werden die Daten in einer anderen Datenbank (cache.db) gespeichert. Der Name der Ortungsdatenbank ändert sich bis iOS10 auch noch mehrfach (cache_encrypted*.db, vgl. Abschnitt 4.1.1 auf Seite 73), die Speicherfristen hingegen liegen seitdem stabil bei unter 7 Tage bzw. selten mehr als ein paar tausend Einträgen pro Tabelle (vgl. Tab. 4.4 auf Seite 88).

Daten werden darüber hinaus nur dann erhoben und gespeichert, wenn die entsprechenden Funkchips verwendet werden. In Phasen der Erprobung neuer Methoden zur Verortung führt Apple mitunter zusätzliche bzw. neue Datenbanken ein. So existiert in iOS9.x vorübergehend die Datenbank lockCache_encryptedA.db zur Speicherung von unmittelbar aufgenommenen Ortungsdaten ebenso wie die SQLite3-Datenbank-Datei cache_encrypted**B**.db zur Speicherung von WLAN-Daten. In iOS10 wird die Speicherung von Ortungsdaten dann wieder in einer SQLite-Datenbank (cache_encryptedB.db) mit write-ahead-log WAL und aktivem auto-vacuum konsolidiert.

Ferner könnten gelöschte Ortungsdaten rekonstruiert werden (vgl. Abschnitt 4.1.4 auf Seite 108). Aufgrund der auto-vacuum Problematik (siehe S. 108) verliert die Methode allerdings immer mehr an Bedeutung. Moderne SQLite3-Datenbanken werden so konfiguriert, dass regelmäßig zum Löschen vorgesehene Datensätze ans Ende der Datei verschoben und dann schlussendlich abgeschnitten werden. Anschließend sind die Daten auf vollverschlüsselten Dateisystemen, wie sie Apple einsetzt, unwiederbringlich verloren.

Integrität von Ortungsdaten aus Smartphones

Anhand der im Rahmen dieser Arbeit entwickelten Werkzeuge sowie der durchgeführten Datenauswertung mithilfe kommerzieller forensischer Tools konnten die Erkenntnisse zur Integrität von Geodaten aus mobilen Endgeräten systematisch vertieft werden. So ermöglichte z.B. die native App iOSTracker die Betrachtung der Ortungsdatenbank live während der Ausführung einer sog. LocationFaker-App (vgl. Abschnitt 1.2.4 auf Seite 24ff. bzw. konkret in Abb. 1.12 auf Seite 26). Hierbei hat sich gezeigt, dass die Standorte in der Ortungsdatenbank von Apple dem tatsächlichen Gerätestandort entsprechen, während die Apps auf dem Gerät die in der LocationFaker-App eingestellte Position anzeigen. Dieses Beispiel und die Tatsache, dass Systembereiche mobiler Betriebssysteme sehr gut geschützt sind, lässt auf ein Maximum an Integrität von Ortsinformationen aus Systemdaten schließen.

	Systemdaten >	**Anwendungsdaten >**	**Multimediainhalte >**	**Dokumente**
Beispieldateien	consolidated.db, cache.db, cache_encryptedA.db, cache_encryptedB.db, cache.cell, cache.wifi	com.apple.wifi.plist, Facebook_session.plist, GeoHistory.mapsdata, ThreemaData.sqlite, com.google.Maps.plist	Photos.sqlite, IMG1234.JPG, IMG1234.MOV	Mail Recents: Treffpunkt.eml
Integrität	Standortdaten mit Genauigkeitsangaben, sehr schlecht manipulierbar	Standortdaten nach dem best-effort-Prinzip (siehe unten), manipulierbar	Standortdaten ohne Genauigkeitsangaben, leicht (insb. retrograd) manipulierbar	Adressdaten im Klartext, selbst erstellt, manipulierbar

Tab. 6.1: Übersicht der Integrität unterschiedlicher Artefakte in der Mobilfunkforensik in Form einer Verlässlichkeitsmatrix

Wie in Tab. 6.1 von links nach rechts angeordnet sind Daten aus Systembereichen der Betriebssysteme durchweg als verlässlicher einzustufen, als Anwendungsdaten, Standorte aus Multimediadateien oder gar vom Nutzer generierten Inhalten. Insbesondere bei Anwendungsdaten ist nicht immer nachvollziehbar, ob die angezeigten Standorte integer sind. Zwar dürfte das Bestreben einer jeden Anwendung sein (best-effort), verlässliche Standortdaten zu speichern, aber ohne durchgängige Absicherung lassen sich Standortdaten retrograd (ggf. sogar direkt in der App z.B. bei Bildbearbeitungsprogrammen) verändern. Demnach ist bei nutzergenerierten Daten, wie Emails, Terminen etc., besondere Vorsicht geboten, weil diese Inhalte direkt bei der Eingabe korrumpiert worden sein könnten.

Genauigkeit von Ortungsdaten aus Smartphones

Wie im ersten Kapitel (u.a. auf Seite 14) bereits ausgeführt, gilt in der Forensik nach wie vor die Regel: Beweise, welche nicht zweifelsfrei und nachvollziehbar dargestellt werden können, haben vor Gericht nur Indizcharakter. Aus diesem Grund ist es wichtig, die Genauigkeit von Standortdaten explizit mit anzugeben. Die im Rahmen dieser Arbeit entwickelten Programme und Apps ermöglichen die Darstellung der Genauigkeitsangabe von Ortungsdaten durch Anzeige der bei Apple- und Google-Ortungsdiensten verfügbaren Accuracy-Werte als grünen Kreis mit dem Radius in Metern um den Standort.

Das die Abweichungen von Ortungdaten zum Teil beträchtlich sein können, zeigt das Beispiel zur Fehleranfälligkeit von Standortinformationen aus Metadaten in Bildern aus der forensischen Praxis (vgl.Abschnitt 1.2.3 auf Seite 22). Umgekehrt lässt sich auf Basis der in den letzten Jahren durchgeführten Untersuchungen feststellen, dass die Genauigkeit von Ortungsdaten in mobilen Endgeräten seit dem Jahr 2011 kontinuierlich zugenommen hat. Waren seinerzeit noch Abweichungen von einigen Kilometern möglich, so reduzierten sich diese je nach Technik auf einige hundert Meter (Mobilfunk) bzw. einige wenige Meter (WLAN/GPS).

Darüber hinaus hat sich gezeigt, dass die Positionsschätzungen über die Zeit der aktiven Nutzung am gleichen Ort immer genauer werden (vgl. Abschnitt 5.5.2 auf Seite 143). Google macht hierzu konkrete Angaben in Googles Entwicklerdokumentation [Goo16b], woher auch die Abb. 5.14 auf Seite 144 stammt. In der Folge kann so eine Steigerung der Qualität dadurch erreicht werden, dass elektronische Beweismittel im zeitlichen Kontext betrachtet werden. Sehr gut lässt sich dieser Umstand mithilfe der im Rahmen dieser Arbeit entwickelten mobilen Applikation Watchtracker nachvollziehen. Die App erlaubt das Aufzeichnen einer Selbstlokalisierung von Apple-Geräten und ermöglicht so die Darstellung der Verbesserung der initialen Grobverortung hin zu einer genaueren Positionsschätzung (vgl. Abb. 5.6 auf Seite 134).

Während Untersuchungen von Google Android mithilfe der Desktopanwendung GoogleTrackerLE bzw. der mobilen App DroidTracker ist aufgefallen, dass sich bei Google die gesamte Lokalisierungs-API über die Jahre verändert hat. Neben der Tatsache, dass mittlerweile zwei völlig unterschiedliche Implementierungen existieren (vgl. Abschnitt 5.2 auf Seite 137), scheint die Menge der übertragenen

Standorte beinahe willkürlich zu bzw. wieder abzunehmen. Dies hat sekundär auch Auswirkungen auf die Bewertung der Genauigkeit von Google-Standorten. So lassen sich aktuell viel weniger Daten zu Untersuchungen heranziehen, als dies noch vor einigen Jahren möglich gewesen ist. Bezüglich der Genauigkeit weisen die angegebenen Senderadien im Vergleich zu Apple um den Faktor 10 kleinere Accuracy-Werte aus. Subjektiv wird dadurch die Genauigkeit erhöht, in der Praxis muss diese Frage noch hinsichtlich der Bewertung der Qualität der Daten in Abschnitt 6.1 auf Seite 153 untersucht werden.

Die Genauigkeit bei der Verortung in geschlossenen Räumen gilt es gesondert zu betrachten. So kommt es z. B. häufiger vor, dass trotz Aufenthalt innerhalb von Gebäuden, die Standortdaten auf einen Punkt außerhalb verweisen. Dies liegt mitunter am schlechten bis unmöglichen GPS-Empfang (vgl. Abschnitt 2.2.5 auf Seite 48) aber auch an der fehlerhaften Verortung von Drahtlossendern. Wie in Abschnitt 5.5.3 auf Seite 147 beschrieben, werden bei der Standortvermessung durch Apple und Google häufiger Standorte errechnet, an denen faktisch kein Sender installiert ist (vgl. Abb. 5.17 auf Seite 147). Hierdurch werden Ortsinformationen auf Basis von WLAN-Sendern häufig vor, anstelle innerhalb von Gebäuden angezeigt (vgl. Abb. 5.6 auf Seite 134). Die Ursache hierfür liegt darin begründet, dass in der Vergangenheit (zumindest für iOS sehr gut nachvollziehbar) nur dann Standortdaten für den harvesting-Prozesses erhoben wurden, wenn ein GPS-fix vorlag (vgl. Abschnitt 4.1.3 auf Seite 87). Mittlerweile sammelt Apple auch dann Daten zu Funksendern in der Umgebung, wenn eine hinreichende Genauigkeit gegeben ist (vgl. Abschnitt 4.1.3 auf Seite 97). Durch die größere Menge an Funksendern dürfte sich die Verortung, insbesondere über WLAN-Accesspoints in Gebäuden, deutlich verbessern.

Falls keine Genauigkeitsangaben bzw. Accuracy-Werte vorliegen, bietet es sich an die allgemein bekannten Größen entsprechend der in Tab. 5.1 auf Seite 144 aufgeführten Sendereichweiten von Funksystemen anzunehmen, je nachdem ob der Standort unter freiem Himmel (GPS), in dichtbesiedeltem Gebiet (WLAN) oder eher ländlichen Gegenden (Mobilfunk) liegt. Bei der qualitativen Abschätzung von Ortungsdaten über die Zeit sind spätere Positionsangaben derselben Verortung stets zu bevorzugen, da sich die Standortbestimmung aktueller Geräte rasch auf wenige Meter verbessert (vgl. Abschnitt 5.5.2 auf Seite 143).

6.2 Vergleich der Eigenentwicklung mit kommerziellen Produkten

Im Unterschied zu den kommerziellen Produkten der Mobilfunkforensik liegt der Fokus von iPhoneTrackerLE bzw. GoogleTrackerLE allein auf der Darstellung und Verarbeitung von Standortdaten der Ortungsdienste von Apple und Google. So verarbeiten die Programme z. B. keine Standorte aus Bildern oder sonstigen Datenbeständen mobiler Endgeräte. Dafür existieren Funktionen, die sich bei den kommerziellen Pendants nicht finden lassen.

Für die Bewertung von Standortdaten durch Laien ist es hilfreich, ihnen eine möglichst leicht nachvollziehbare sowie eindeutige Schätzung zur Präzision und Integrität der Daten zu liefern. Beide Tools bieten hierfür zunächst einmal die Möglichkeit zur Reduktion der Punktwolken (vgl. Abschnitt 4.1.2 auf Seite 81) der Drahtlossender in der Umgebung des Gerätes auf einen einzigen Standort je ausgewählten Zeitpunkt (Estimate Position). Zusätzlich lässt sich die maximale Standortabweichung in der Kartenansicht durch einen farbflächigen Radius um den Funksender bzw. die GPS-Position anzeigen (Show Accuracy). Über einen Schieberegler (Confidence) lassen sich die Daten dann ggf. noch weiter filtern. Die Unterscheidung des Datenursprungs (vom Gerät bzw. Hersteller) sowie der zu erwartenden Fehlertoleranzen von Funkzellen-, WLAN- bzw. GPS-Signalen (vgl. Abb. 5.9 auf Seite 139) rundet den Funktionsumfang hinsichtlich der Standortdarstellung ab.

Für die Benutzung der Desktopanwendungen durch den polizeilichen Ermittler sind die Implementierung einer Zeitleiste zur gezielten Auswahl von Ortungsdaten sowie Funktionen zur einfachen Berichterstellung zwei der wesentlichen Funktionsmerkmale. Sofern tatrelevante Zeitstempel existieren, lassen sich diese über die Schaltflächen »Create Report«, »Add Entry« sowie »Close Report« in die für deutsche Gerichtsverfahren notwendige Darstellung in Papierform bringen. Im Unterschied zu den kommerziellen Tools ist die Intention hierbei eine interaktive Zusammenführung der relevanten Informationen inkl. Beschreibung der Dateiquellen, einer Darstellung der Standortabweichung im Kartenausschnitt als Screenshot für jeden Zeitraum inkl. Adresse. Diese lässt sich über einen simplen Mausklick in der Kartenansicht bzw. auf die einzelnen Pins der Standorte über das Internet abrufen und im Bereich der Notizen mit ausgeben.

6.3 Absicherung der Erkenntnisse durch Apps

Neben der Implementierung von Desktopanwendungen zur Untersuchung von Standortdaten in der Mobilfunkforensik liegt ein weiterer Schwerpunkt dieser Arbeit in der Entwicklung nativer mobiler Applikationen zur Veranschaulichung der Geolokalisierung auf mobilen Endgeräten. So führte die Implementierung unterschiedlicher Methoden zur Verortung auf Smartphones mit Apples iOS bzw. Google Android zusätzlich zur retrograden Analyse bereits erhobener Standortdaten zu einem besseren Verständnis der Arbeitsweise von Ortungsdiensten in Smartphones im Allgemeinen.

Mithilfe der selbstentwickelten nativen Apps für iOS und Android war es so z. B. möglich, die verschiedenen Einstellmöglichkeiten für Entwickler direkt beim Aufruf der entsprechenden Programmierschnittstellen unter iOS und Android systematisch zu beeinflussen (vgl. Abschnitt 5.5.1 auf Seite 141). Hierbei ließen sich durch Setzen der gewünschten Präzision bei der Verortung Unterschiede in der Häufigkeit der Abfragen bzw. eine Veränderung der Anzahl an Einträge in den Ortungsdaten feststellen bzw. gezielt steuern.

Darüber hinaus lässt sich in der App iOSTracker die Ortungsdatenbank von iOS und insbesondere die Inhalte der harvesting-Tabellen mit den erhobenen Daten für Apple direkt auf dem Gerät betrachten und einzelne Einträge hieraus in einer Kartenansicht darstellen (vgl. Abb. 5.3 bzw. 5.4 auf Seite 133). Hierdurch wird es einfach und ohne komplizierte Sicherungsmaßnahmen möglich, eine verlässliche Interpretation der Daten der harvesting-Tabellen zu ergründen, bevor die Daten zu Apple übersandt und auf dem Gerät gelöscht werden.

Schlussendlich ermöglichen alle Anwendungen, den Geolokalisierungsprozess gezielt zu starten bzw. zu beenden und den Vorgang der Verortung dann live auf dem Gerät zu beobachten. Hierzu wird der Ortungsprozess auch nicht, wie sonst bei Apps mit Ortungsfunktionalität üblich, bereits beim Initialisieren der App gestartet, sondern erst durch bewusste Aktivierung des Ortungsdienstes. Die Android-App DroidTracker ermöglicht ferner das gezielte Deaktivieren bzw. Aktivieren der unterschiedlichen Sensoren zur Verortung. So ließ sich zeigen, dass die Funkempfänger für Mobilfunk, WLAN bzw. GPS zu einem bestimmten Maß an Genauigkeit bei der Verortung führen (vgl. Abschnitt 5.5.2 auf Seite 144).

6.4 Bewertung der Ermittlungsmöglichkeiten

Mithilfe des in Abschnitt 5.5.2 auf Seite 143 dargestellten Modells zur Verortung auf Basis von aGPS konnte gezeigt werden, dass Standortdaten in Smartphones im Verlauf der Verortung immer präziser werden. So erlauben die Erfahrungen zu Positionsschätzungen aktueller Geräte mit modernen Sensoren sowie aktuellen mobilen Betriebssystemen eine durchweg positive Einschätzung hinsichtlich der Genauigkeit sowie Integrität der extrahierten Standortdaten.

Die technischen Entwicklungen der letzten Jahre bei Apple und Google führen zu einer deutlich gesunkenen Fehlerrate bzgl. der gespeicherten Standortdaten in Multimediadateien gegenüber älterer Aufnahmen aus dem Jahre 2011 wie in [Gri15] bzw. Abb. 1.10 auf Seite 23 beschrieben. So ließ sich auch in Abschnitt 2.2.5 auf Seite 48 feststellen, dass sich die Standortabweichung einer Aufnahme aus dem Jahr 2013 von ca. 1km hin zu einer Genauigkeit von unter 10m bei einer Aufnahme aus Mitte 2016 verbessert hat (vgl. Abb. 2.12 auf Seite 50).

Die Aussagen zur Beurteilung der Qualität von Geolokationsdaten in iOS (vgl. Abschnitt 5.5.2 auf Seite 143) konnten in dieser Arbeit empirisch untersucht und gestützt werden. Das ist ein wesentlicher Fortschritt gegenüber den bisherigen Annahmen, die sich auf die Herstellerangaben stützten. In der Online-Dokumentation gewähren die Hersteller i. d. R. lediglich Einblick in die Arbeitsweise und Wertebereiche ihrer APIs. Nur bei Google lassen sich auch Angaben zur Entwicklung der Standortgenauigkeit über die Laufzeit der Verortung finden (vgl. [Goo16b] bzw. Abb. 5.14 auf Seite 144). Im Zweifelsfall kann es somit hilfreich sein, bei der Bewertung von Ortungsdaten weitere Erkenntnisse aus polizeilichen Ermittlungen zu ergänzen.

Umgekehrt lassen sich die allgemein bekannten Reichweiten von Funksendern, wie in Tab. 5.1 auf Seite 144 aufgezählt, durchaus zur Schätzung der maximalen Abweichung zum extrahierten Standort heranziehen, sofern explizite Angaben zur Accuracy nicht verfügbar sind.

Insgesamt ist festzuhalten, dass die vielfältigen Möglichkeiten des entwickelten Modells zur Genauigkeit von Standortdaten aus mobilen Endgeräten (vgl. Abschnitt 5.5.2 auf Seite 143) in Kombination und ergänzt durch die Wissensbasis

aus Teil 3 ab Seite 55 ausreichend sein sollten, um die Qualität von Ortungsdaten in der Mobilfunkforensik abzuschätzen und nachvollziehbar darzulegen.

6.5 Ausblick

Aufgrund der sich ständig verändernden technischen Entwicklung im Bereich der Sensorik mobiler Endgeräte, sowie neuer Verfahren zur Standortbestimmung im Zuge regelmäßiger Systemupdates, ist eine hundertprozentige Bewertung von Standortdaten aus Ortungsdiensten in Smartphones nicht möglich.

Grundsätzlich wird die Smartphonelokalisierung aber weiterhin auf externe Stützsysteme über Funksender angewiesen sein. Im nächsten Abschnitt sollen hierzu aktuelle sowie neue Hintergründe bzw. Methoden zur Geolokalisierung aufgezeigt werden, die nicht mehr im Rahmen dieser Arbeit betrachtet werden konnten. Im Ergebnis lässt sich festhalten, dass die Standortbestimmung mobiler Endgeräte stetig weiterentwickelt bzw. verbessert wird. Darüber hinaus wird in Abschnitt 6.5 auf Seite 161 eine mathematische Methode skizziert, die sich in die Desktopanwendungen iPhoneTrackerLE bzw. GoogleTrackerLE integrieren ließe und zur Maximierung der Zuverlässigkeit von Geodaten genutzt werden könnte.

Im Anschluss ab Seite 161 werden dann noch Ortungsdaten bei Microsoft sowie Wearables betrachtet und der Frage nachgegangen, inwiefern eine Betrachtung aus forensischer Sicht machbar und interessant ist. Lohnenswert dürfte eine Ergänzung der Metadaten in Bildern um die Angabe des Accuracy-Wertes zur maximalen Fehlerabschätzung sein, die auf Seite 164 kurz vorgestellt wird.

Schlussendlich wird im letzten Abschnitt dieser Arbeit ab Seite 164 noch die Idee einer integrierten Gesamtanwendung aus iPhoneTrackerLE / GoogleTrackerLE unter Berücksichtigung der Erkenntnisse des herstellerunabhängigen Standortdatenmodells aus Abschnitt 5.5.2 auf Seite 143 in Form eines Expertensystems für den forensischen Sachbearbeiter für zukünftige Entwicklungen vorgestellt.

Alternative Wege in der Lokalisierung mobiler Systeme

Zunächst versprechen Hersteller wie Google und Apple durch neue Methoden bei der Routenführung eine verlässlichere Navigation in urbanen Gegenden (vgl.

Abschnitt 1.1.2 auf Seite 7). So orientieren sich die Standortdaten bei Apple z. B. an bekannten Strukturen (Straßen, Wege, Gebäude etc.) des zugrundeliegenden vektorbasierten Kartenmaterials, wie im Video zur Apple-Entwicklerkonferenz WWDC [App12] ab Minute 4:15 zu sehen.

Zusätzlich soll eine Optimierung des Energiebedarfs auf Apple-Geräten durch Komprimierung und Übertragung größerer Datenmengen von Funksendern aus der weiteren Umgebung, weniger häufiges Nachladen sowie die Verringerung der notwendigen Bandbreite zur Folge haben. Ferner scheint Apple in neueren iOS-Versionen Funksender um Standorte von besonderem Interesse zu ergänzen und ebenfalls vorab an die Geräte zu übertragen. Dies führt bei forensischen Untersuchungen von iOS10 und neuer zu Problemen, wenn in der Ortungsdatenbank von Apple weit entfernte Standorte an mehreren potentiell möglichen Aufenthaltsorten zu ein und demselben Zeitpunkt ermittelt werden. Nach der Aktivierung der Positionsschätzung wird dann mitunter ein Standort angezeigt, der weiter entfernt ist als der Senderadius der Funkquelle reicht. Für die Verortung des Geräts selbst stellt dies kein Problem dar. Hierfür werden schliesslich nur die sichtbaren Sender in der Umgebung verwendet und die Standortinformationen weiter entfernter Geräte ignoriert. Die forensische Auswertung schlägt hingegen fehl.

Darüber hinaus versuchen die Hersteller stets die Verortung in geschlossenen Räumen zu verbessern bzw. um neue Funktechnologien zu erweitern. Entgegen der Lokalisierung unter freiem Himmel über GPS ist die Standortbestimmung innerhalb von Gebäuden (ohne Verfügbarkeit von GPS-Signalen) fehleranfällig. So wirken sich bauliche Begebenheiten wie Mauern, Decken und Wassersysteme spürbar auf den Empfang von Funksendern und somit auch auf die Positionsschätzung aus. Umgekehrt ist es z. B. auf Google Maps schon länger möglich, das Innere bestimmter Gebäude zu erkunden. Diese Karten lassen sich ebenso zur Verbesserung der Verortung nutzen, wie es Google und Apple möglich ist, über Nachbereichs-Funksender in der unmittelbaren Umgebung der Geräte die Erschließung von Innenräumen voranzutreiben. Wie in Abschnitt 4.1.3ff. ab Seite 99 beschrieben, arbeitet zumindest Apple an der Erfassung und Integration von Nahbereichs- oder auch Microlocation-Sendern wie NFC.

Demnach wird zukünftig die Genauigkeit von Geolokalisierungsdaten in der Mobilfunkforensik durch eine Verbesserung der Empfangschips ebenso weiter stei-

gen, wie dies durch die permanente Aktualisierung und Konsolidierung der Datenbanken bei Apple und Google sowie der Nutzung neuer Funktechnologien mit kleineren Senderadien der Fall sein wird.

Automatische Sigmabereiche für Senderadien

Wie in Abschnitt 4.2.2 auf Seite 115 beschrieben, treten unter Android 2.x Fälle auf, bei denen der tatsächliche Gerätestandort etwas außerhalb des Senderadius liegt. Bei Apple konnten solche Unstimmigkeiten zunächst nicht festgestellt werden. Erst die Untersuchung von Ortungsdaten aus iOS9 hat ergeben, dass auch unter iOS Datensätze existieren, für die der tatsächliche Standort des Gerätes außerhalb des Senderadius des angezeigten Funksenders liegt.

Um diesem Problem zu begegnen, ermöglicht die sogenannte Sigma-Umgebung (vgl. [Bri08]) laienhaft ausgedrückt, durch Maximierung der Wahrscheinlichkeit eines gegebenen Umgebungsradius die Berechnung eines größeren Radius zur Erhöhung der Chance dafür, dass sich der gesuchte Punkt dann innerhalb des neuen Radius befindet. Übertragen auf Ortungsdaten in der Mobilfunkforensik könnte, wie in Abb. 6.1 auf der nächsten Seite dargestellt, die »confidence« als Basisbezugsgröße zur Accuracy genommen werden. Durch Erhöhung der Prozentangabe lässt sich so die Wahrscheinlichkeit dafür erhöhen, dass der tatsächliche Standpunkt innerhalb des geringfügig größeren Senderadius liegt.

Für eine erste Implementierung wäre es z. B. eine Möglichkeit, die confidence-Werte der Einträge aller Tabellen auf den maximal ermittelten Wert von 90% zu bringen. Hierdurch würden sich die Radien in den Tabellen CellLocation (von 70% auf 90%) sowie WifiLocation (von 50% auf 90%) geringfügig vergrößern und die tatsächlichen Standorte dürften wieder innerhalb des Senderadius liegen.

Windows Mobile

Zusätzlich zu den in dieser Arbeit untersuchten Geräten existieren eine Vielzahl weiterer Hersteller im Bereich von Mobiltelefonen. Ortungsdienste lassen sich mittlerweile auf allen mobilen sowie einigen Desktop-Plattformen finden.

Aus forensischer Sicht ist es sicherlich legitim, den Fokus auf die Marktführer im Segment Smartphones zu legen. Die Marktverteilung in Abb. 1.7 auf Seite 17 zeigt

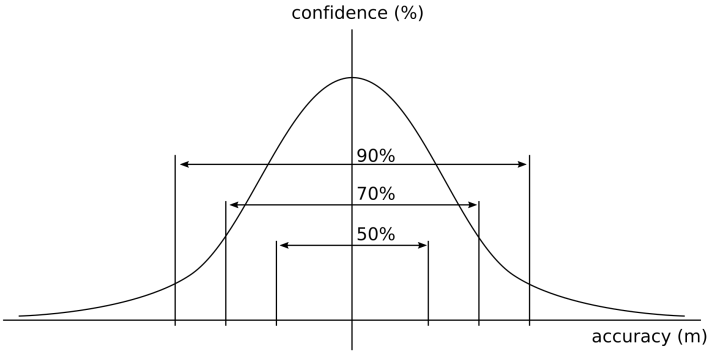


Abb. 6.1: Ausblick: Implementierung einer Sigma-Umgebung zur Maximierung der confidence von Senderadien von Ortungsdaten unter Android und iOS in iPhoneTrackerLE und GoogleTrackerLE. Quelle: Eigene Darstellung.

eine klare Dominanz von Android mit knapp 80% vor Apple auf Platz zwei mit über 15% noch vor Windows Mobile mit 5,6% Marktanteil. Die fehlende akademische Auseinandersetzung mit Windows Mobile lässt sich dadurch aber nicht unmittelbar ableiten.

Tatsächlich hat es auch Überlegungen gegeben, Microsofts mobile Plattform im Rahmen dieser Arbeit zu untersuchen. Hierzu ist anzumerken, dass Windows Mobile im Vergleich zu den Betriebssystemen von Apple und Google erst spät und nur für kurze Zeit Verbreitung gefunden hat. Zudem berichteten Kollegen der Mobilfunkforensik immer wieder von großen Schwierigkeiten beim Zugriff auf die Geräte bzw. bei der Datenextraktion von Windows-Phones. Ebenso ließen sich seinerzeit keinerlei Zugriffsmöglichkeiten auf Clouddaten von Microsoft ermitteln, über die sich eine Extraktion von Ortungsdaten hätte bewerkstelligen lassen. Literatur zum Thema war ebenfalls nicht verfügbar.

Es ist zwar anzunehmen, dass Microsoft ähnliche Techniken zur Geolokalisierung anwendet wie die Konkurrenz. In der Praxis konnten diese im Rahmen dieser Arbeit schlichtweg nicht untersucht werden. Nichts desto trotz ist zu vermuten, dass in den Metainformationen zu Bildern sowie den Konfigurationsdateien von Apps auch unter Windows Mobile Geodaten gespeichert sind. Die Abschätzung zur Genauigkeit, Integrität etc. dürfte dem in Abschnitt 5.5.2 auf Seite 143 beschriebenen generischen Modell zur Beurteilung von Geodaten aus mobilen

Endgeräten folgen. Sprich, es werden Ortsinformationen erhoben und die bestmöglichen bzw. hinreichend exakten Daten im jeweiligen Kontext gespeichert.

Die konkrete Beurteilung von Standortdaten aus Windows Mobile Geräten oder bei Microsoft im Internet wird im Falle eines forensischen Ersuchens oder einer gesonderten Arbeit hierzu durchzuführen sein.

Ortungsdaten in Wearables

Eine weitere interessante Abwandlung mobiler Endgeräte für die IT-Forensik dürfte zukünftig in der Sparte der sogenannten Wearables zu finden sein. Insbesondere Fitnesstracker, aber auch Smartwatches oder andere Hilfsmittel zur Erweiterung der Funktionalität von Smartphones nutzen Geoinformationen (vgl. [Coo16]). Und wo immer Standortdaten erhoben werden, besteht auch die Chance, dass diese nachvollziehbar gespeichert sind.

Über die Sensoren in der Apple Watch (1st Generation nur WLAN und Bluetooth, 2nd Generation GPS und 3rd Generation dann inkl. Mobilfunk) ist eine Verortung über aGPS unter Verwendung gepufferter Standortinformationen analog zu iOS auch ohne iPhone möglich. Es ist explizit vorgesehen, die Uhr autark beim Sport zu tragen und Informationen zum Training zu speichern (vgl. [App17b]).

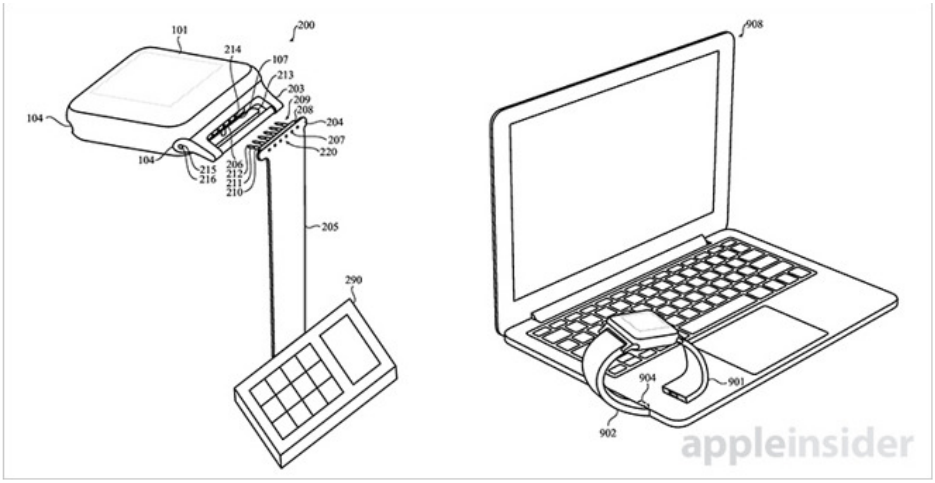


Abb. 6.2: Patentskizze der Apple Watch Diagnoseschnittstelle. Quelle: [app16i].

Bei den Recherchen zu diesem Thema konnte bislang keine Methode ermittelt werden, um Standortdaten direkt von der Apple Watch zu extrahieren. Über die

von außen zugänglichen Kontaktpunke, wie in Abb. 6.2 auf der vorherigen Seite zu erkennen, scheint nur Apple selbst über spezielle Geräte (links) oder besondere (USB-)Armbändern (rechts) mit der Uhr kommunizieren zu können. Und solange keine Möglichkeit existiert, um Standortdaten von der Uhr zu extrahieren und aufzubereiten, kann über die Qualität der Ortungsdaten auf der Apple Watch nur spekuliert werden. Sie dürfte aber, den Ausführungen Apples in [App17b] folgend, der Qualität von denen bei iOS bzw. der von Smartphone entsprechen.

Fehlertoleranz in Exif Daten

Im Rahmen der in Abschnitt 5.1 auf Seite 132 beschriebenen Implementierungen der nativen Apps konnte gezeigt werden, dass die Ortungsdienste unter Apple iOS sowie Google Android immer auch die Genauigkeit der Positionsschätzung im Datenstrom der location-API beinhalten (vgl. Abb. 5.2 auf Seite 132). Hieraus folgt, dass es jeder Anwendung (so auch der Kamera-App) möglich ist, den aktuellen Verortungsfehler innerhalb der Metadaten von Bildern etc. zu dokumentieren.

Im Exif-Standard v.2.3 existiert ein Exif-Tag um die Fehlerabweichung zur GPS-Position in Metern abzuspeichern (vgl. [Ass12] S. 68, 77). Allerdings scheint die optionale Angabe zum »GPSHPositioningError« bislang nicht genutzt bzw. nicht ausgewertet zu werden. Ferner existiert die Möglichkeit, mittels Angabe zur »GPSProcessingMethod« zu beschreiben, mit welcher Methode die Verortung durchgeführt wurde. Durch die Angabe von »CELLID« bzw. »WLAN« anstelle von »GPS« lässt sich so auf Basis des Genauigkeitskompasses (vgl. Abschnitt 5.5.2 auf Seite 144) zumindest eine grobe Schätzung bzgl. der maximalen Fehlerrate bei der Verortung erreichen (vgl. [Ass12] S. 75).

Durch die Nutzung bzw. Auswertung der im Exif-Standard möglichen Tags ließe sich ein Mehrwert für die Mobilfunkforensik erreichen.

Weiterentwicklung der Desktop-Anwendungen

In Diskussionen mit Kollegen sind einige interessante Ideen entstanden, wie sich die Desktop-Programme erweitern lassen. So wurde beispielsweise der Wunsch

geäußert die Desktopanwendungen iPhoneTrackerLE und GoogleTrackerLE zu einem Produkt zusammenzufassen, um so Daten aus iOS- und Android-Geräten gleichzeitig darstellen zu können. Neben der Angleichung der unterschiedlichen Parameter bezüglich Präzision und Integrität läge ein weiterer Vorteil in der Möglichkeit, die forensische Auswertung auf Basis einer gemeinsamen Zeitlinie über alle einem Tatverdächtigen zuzuordnenden elektronischen Beweismitteln mit Standortinformationen durchführen zu können.

Ferner sollte die Option zur Erweiterung der Senderadien (Sigma-Umgebung) zur Verbesserung der Zuverlässigkeit von Standortdaten aus mobilen Endgeräten in die Desktopanwendungen integriert werden (vgl. Abschnitt 6.5 auf Seite 161).

Zusätzlich ist immer wieder der Wunsch geäußert worden, weitere Datenformate zu unterstützen. Als lohnenswerte Formate gelten Geokoordinaten aus Metadaten von Bildern, aus reverse-geocoding-Abfragen von IP- und MAC-Adressen sowie alles, was sich in eine Geokoordinate überführen lässt. Der Hintergedanke hierbei ist stets, zusätzlich zur Darstellung auf einer Karte immer auch eine maximale Abweichung aufgrund der zu erwartenden Fehlertoleranzen in Form von Radien um die Ortsangaben mit anzugeben.

Bislang konnte noch nicht entschieden werden, wie mit dem Quellcode der Tools und Anwendungen nach dem Fertigstellen der Dissertation weiter verfahren werden soll. Zumindest ist aber geplant, den Programmcode innerhalb der Polizei für die Weiterentwicklung /Pflege zur Verfügung zu stellen.

Zu erwartende Verlässlichkeit im Bereich Geodaten

Gegenüber 2011 hat sich die Verlässlichkeit im Zusammenhang mit Geodaten bzgl. der Vollständigkeit bzw. Speicherdauer von Standortdaten stark verändert. Die Ergebnisse dieser Arbeit zeigen, dass Apple und Google zwar hinsichtlich des Speicherumfangs von Geodaten auf dem Gerät bzw. online beim Hersteller gegensätzliche Vorstellungen haben, die Nutzung von location-based services auf Smartphones aber mittlerweile zum Standard geworden ist. Die Integrität der Ortungsdienste auf Smartphones mit unverändertem Betriebssystem war und ist durch das hohe Sicherheitsniveau der mobilen Plattformen gewährleistet. Die Hersteller geben zudem ihr Bestes, damit extrinsische Faktoren keine negativen Auswirkungen auf die Geräteverortung haben. Dessen ungeachtet müssen elek-

tronische Beweise immer objektiv kritisch auf vorsätzliche Manipulationen überprüft werden. Schlussendlich hat sich die Genauigkeit von Standortdaten aus mobilen Endgeräten im Verlauf der letzten Jahre stetig verbessert. So ist auch in Zukunft davon auszugehen, dass die Präzision, Integrität und Vollständigkeit, kurzum die Verlässlichkeit von Geolokalisierungsdaten in der Mobilfunkforensik einen Mehrwert in der Beweisführung bringen wird.

Literaturverzeichnis

[(4r11] Andreas Dhein (4rensiker). iPhone Tracking – from a forensic point of view. *Forensic Focus*, 2011. Online, letzter Zugriff: 13.07.2016. URL: https://articles.forensicfocus.com/2011/11/20/iphone-tracking-from-a-forensic-point-of-view.

[(4r12] Andreas Dhein (4rensiker). Android Tracking – from a forensic point of view. *Forensic Focus*, 2012. Online, letzter Zugriff: 13.07.2016. URL: https://articles.forensicfocus.com/2012/02/27/android-tracking-from-a-forensic-point-of-view.

[Ass16] IEEE Standards Association. Guidelines for Use Organizationally Unique Identifier (OUI) and Company ID (CID). https://standards.ieee.org/develop/regauth/tut/eui.pdf, Juli 2016. Online, letzter Zugriff: 26.07.2016.

[AVD11] Julia Angwin and Jennifer Valentino-Devries. What they know - Apple, Google Collect User Data. *Wallstreet Journal*, 2011. Online, letzter Zugriff: 05.07.2016. URL: http://www.wsj.com/articles/SB10001424052748703983704576277101723453610.

[AW11] Alasdair Allan and Pete Warden. Got an iPhone or 3G iPad? Apple is recording your moves. *O'Reilly*, 2011. Online, letzter Zugriff: 05.07.2016. URL: http://radar.oreilly.com/2011/04/apple-location-tracking.html.

[BA10] Mark Bedner and Tobias Ackermann. Schutzziele der IT-Sicherheit. *Datenschutz und Datensicherheit - DuD*, 34(5):323–328, 2010. Online, letzter Zugriff: 22.01.2017. URL:

http://dx.doi.org/10.1007/s11623-010-0096-1, doi:10.1007/s11623-010-0096-1.

[BS09] Mathew Backer and Stefania Sesia. *LTE, The UMTS Long Term Evolution: From Theory to Practice*. Wiley, 1st edition, April 2009. https://onlinelibrary.wiley.com/doi/book/10.1002/9780470742891, Online, letzter Zugriff: 01.12.2019.

[BV11] Mark Bilandzic and John Venable. Towards Participatory Action Design Research: Adapting Action Research and Design Science Research Methods for Urban Informatics. *The Journal of Community Informatics*, 7(3), 2011. Online, letzter Zugriff: 05.07.2016. URL: http://ci-journal.net/index.php/ciej/article/view/786.

[DF16] Andreas Dewald and Felix C. Freiling. Forensische Prinzipien: von digital zu cyber. https://www1.informatik.uni-erlangen.de/filepool//projects/openc3s/mikromodul-forensische-prinzipien.pdf, 2016. Online, letzter Zugriff: 17.06.2018.

[DG16] Andreas Dhein and Rüdiger Grimm. Standortlokalisierung in modernen Smartphones. *Informatik-Spektrum*, pages 1–10, 2016. Online, letzter Zugriff: 04.07.2016. URL: http://dx.doi.org/10.1007/s00287-016-0964-7, doi:10.1007/s00287-016-0964-7.

[Dhe13] Andreas Dhein. Ortungsdaten in modernen Smartphones. *kes*, 2013. Online, letzter Zugriff: 13.07.2016. URL: https://www.kes.info/archiv/heft-archiv/jahrgang-2013/ausgabe-2013-3/.

[Dri11a] Richard Drinkwater. An analysis of the record structure within SQLite databases. *Forensics from the sausage factory*, 2011. Online, letzter Zugriff: 05.11.2017. URL: http://forensicsfromthesausagefactory.blogspot.de/2011/05/analysis-of-record-structure-within.html.

[Dri11b] Richard Drinkwater. Carving SQLite databases from unallocated clusters. *Forensics from the sausage factory*, 2011. Online, letzter Zugriff:

05.11.2017. URL:
http://forensicsfromthesausagefactory.blogspot.de/2011/04/carving-sqlite-databases-from.html.

[fSidI11] Bundesamt für Sicherheit in der Informationstechnik. Leitfaden »IT-Forensik«. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=2, 2011. Online, letzter Zugriff: 17.06.2018.

[Ges16] Alexander Geschonneck. *Computer Forensik*. dpunkt.verlag GmbH, Heidelberg, 2016. Online, letzter Zugriff: 05.07.2016, https://books.google.de/books?ISBN=3864914906.

[Hoo11] Andrew Hoog. *Android forensics: investigation, analysis, and mobile security for Google Android*. Syngress, Waltham, MA, 2011. Online, letzter Zugriff: 01.12.2019, https://dl.acm.org/citation.cfm?id=2021191.

[HS11] Andrew Hoog and Katie Strzempka. *iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices*. Syngress Publishing, Rockland, Massachusetts, 1st edition, 2011. Online, letzter Zugriff: 01.12.2019, https://dl.acm.org/citation.cfm?id=2021199.

[MHS11] Stefan Maus, Hans Höfken, and Marko Schuba. Forensic Analysis of Geodata in Android Smartphones. Technical report, FH Aachen, University of Applied Sciences, 52066 Aachen, Germany, 2011. Online, letzter Zugriff: 05.01.2017. URL: https://www.fh-aachen.de/fileadmin/people/fb05_schuba/IT-Forensik/download/PDF_s/Forensic_Analysis_of_Geodata_in_Android_Smartphones.pdf.

[PRK12] K. Peffers, M. Rothenberger, and B. Kuechler. *Design Science Research in Information Systems: Advances in Theory and Practice: 7th International Conference, DESRIST 2012, Las Vegas, NV, USA, May 14-15, 2012, Proceedings*. Lecture Notes in Computer Science. Springer Berlin

Heidelberg, 2012. Online, letzter Zugriff: 05.07.2016, https://books.google.de/books?id=DSe7BQAAQBAJ.

[PTG+06] Ken Peffers, Tuure Tuunanen, Charles E. Gengler, Matti Rossi, Wendy Hui, Ville Virtanen, and Johanna Bragge. The Design Science Research Process: a model for producing and presenting information systems research. *DESRIST 2006. February 24-25, 2006, Claremont, CA.*, 7, 2006. Online, letzter Zugriff: 12.03.2017. URL: http://www.wrsc.org/sites/default/files/documents/000designscresearchproc_desrist_2006.pdf.

[San10] Ralf Sander. Wlan-Daten ausspioniert: Google setzt sich die Datenkraken-Krone auf. *Stern*, Mai 2010. Online, letzter Zugriff: 30.12.2016. URL: http://www.stern.de/digital/MISC/wlan-daten-ausspioniert-google-setzt-sich-die-datenkraken-krone-auf-3100188.html.

[Sch11] Ben Schwan. Wirbel um Aufzeichnung von Ortungsdaten im iPhone. *Mac & I*, 2011. Online, letzter Zugriff: 30.11.2017. URL: https://www.heise.de/mac-and-i/meldung/Wirbel-um-Aufzeichnung-von-Ortungsdaten-im-iPhone-1231573.html.

[Spr13] Michael Spreitzenbarth. *Dissecting the Droid: Forensic Analysis of Android and its malicious Applications*. PhD thesis, Universität Erlangen, 2013. https://opus4.kobv.de/opus4-fau/frontdoor/deliver/index/docId/3286/file/MichaelSpreitzenbarthDissertation.pdf. Online, letzter Zugriff: 04.01.2017.

[SS12] Michael Spreitzenbarth and Sven Schmitt. Is data retention still necessary in the age of smartphones? *Hakin9*, pages 20–24, März 2012. Online, letzter Zugriff: 05.07.2016. URL: https://www1.cs.fau.de/filepool/publications/Hakin9_Forensics.pdf.

[TRPC12] Nils Ole Tippenhauer, Kasper Bonne Rasmussen, Christina Pöpper, and Srdjan Capkun. iPhone and iPod Location Spoofing: Attacks on Public WLAN-based Positioning Systems. Technical report,

Department of Computer Science, ETH Zurich, 8092 Zurich, Switzerland, 2012. Online, letzter Zugriff: 30.12.2016. URL: http://e-collection.library.ethz.ch/eserv/eth:4990/eth-4990-01.pdf.

[VK15] V.K. Vaishnavi and W. Kuechler. *Design Science Research Methods and Patterns: Innovating Information and Communication Technology, 2nd Edition*. CRC Press, 2015. Online, letzter Zugriff: 05.07.2016, https://books.google.de/books?id=OOE_CQAAQBAJ.

[Zdz13] Jonathan Zdziarski. *iOS Forensic Investigative Methods*. Self published, technical draft edition, 2013. Online, letzter Zugriff: 05.07.2016, http://www.zdziarski.com/blog/wp-content/uploads/2013/05/iOS-Forensic-Investigative-Methods.pdf.

[Zog11] Jean-Marie Zogg. GPS essentials to satellite navigation, 2011. Online, letzter Zugriff: 03.02.2018, http://zogg-jm.ch/Dateien/Update_Zogg_Deutsche_Version_Jan_09_Version_Z4x.pdf.

Internetquellen

[Ack16] Devon Ackerman. Forensics - Apple iOS & Watch OS Artifacts. https://docs.google.com/spreadsheets/d/1zAqSSiLZ-Fw6RrXg7qegkxbE7ejXI_mpxQre_ybWRWw/edit#gid=0, Juni 2016. Online, letzter Zugriff: 13.02.2018.

[Ame16] Hannes Ametsreiter. Smartphone-Markt: Konjunktur und Trends. https://www.bitkom.org/Presse/Anhaenge-an-PIs/2016/Bitkom-Pressekonferenz-Smartphone-Markt-Konjunktur-und-Trends-16-02-2016-Praesentation-final.pdf, 2016. Online, letzter Zugriff: 11.07.2016.

[Ano11] Anonym. MyPhoneTracker, 2011. Online, letzter Zugriff: 05.07.2016. URL: http://www.mac-and-i.net/2011/04/myphonetracker-analyze-iphone.html.

[App10] Apple. Apple Antennendesign und Testlabors. http://www.apple.com/de/antenna, 2010. Online, letzter Zugriff: 25.07.2010.

[App11] Apple. Apple Q&A on Location Data. http://www.apple.com/pr/library/2011/04/27Apple-Q-A-on-Location-Data.html, 2011. Online, letzter Zugriff: 10.02.2018.

[App12] Apple. Staying on Track with Location Services. https://developer.apple.com/videos/play/wwdc2012/303/, 2012. Online, letzter Zugriff: 14.04.2017.

[App16a] Apple. CMMotionActivity Class Reference. https://developer.apple.com/library/ios/documentation/CoreMotion/Reference/CMMotionActivity_class, 2016. Online, letzter Zugriff: 27.07.2016.

[App16b] Apple. Configuring Your Xcode Project for Distribution. https://developer.apple.com/library/ios/documentation/IDEs/Conceptual/AppDistributionGuide/ConfiguringYourApp/ConfiguringYourApp.html, 2016. Online, letzter Zugriff: 27.07.2016.

[App16c] Apple. Core Location Constants Reference. https://developer.apple.com/library/ios/documentation/CoreLocation/Reference/CoreLocationConstantsRef/index.html#//apple_ref/doc/constant_group/Accuracy_Constants, 2016. Online, letzter Zugriff: 20.07.2016.

[App16d] Apple. Core Motion Framework. https://developer.apple.com/reference/coremotion, 2016. Online, letzter Zugriff: 27.07.2016.

[App16e] Apple. Informationen zum Datenschutz und zu den Ortungsdiensten. https://support.apple.com/de-de/HT203033, 2016. Online, letzter Zugriff: 03.08.2016.

[App16f] Apple. Klassenbeschreibung des CLLocationManager. https://developer.apple.com/library/ios/documentation/CoreLocation/Reference/CLLocationManager_Class/index.html#//apple_ref/occ/cl/CLLocationManager, 2016. Online, letzter Zugriff: 20.07.2016.

[App16g] Apple. Technische Spezifikationen iPhone. https://support.apple.com/specs/iphone, Juli 2016. Online, letzter Zugriff: 27.07.2016.

[App16h] Apple. Time Utilities Reference. https://developer.apple.com/library/mac/documentation/

CoreFoundation/Reference/CFTimeUtils/, 2016. Online, letzter Zugriff: 25.07.2016.

[app16i] appleinsider. Apple invents modular Apple Watch accessories that link togLocation Spoofinger, connect via diagnostics port. *appleinsider.com*, März 2016. Online, letzter Zugriff: 26.02.2017. URL: http://appleinsider.com/articles/16/03/31/apples-modular-apple-watch-strap-invention-connects-via-diagnostics-port-supports-battery-pack-gps-receiver-more.

[App17a] Apple. App Store Preview: Find My iPhone. https://apps.apple.com/us/app/find-my-iphone/id376101648, Februar 2017. Online, letzter Zugriff: 26.01.2017.

[App17b] Apple. Apple Watch ohne Ihr iPhone in der Nähe verwenden. https://support.apple.com/de-de/HT205547, 2017. Online, letzter Zugriff: 27.05.2018.

[App17c] Apple. Government Information Requests. http://www.apple.com/privacy/government-information-requests, 2017. Online, letzter Zugriff: 26.03.2017.

[App18] Apple. Optimize Location and Motion. https://developer.apple.com/library/content/documentation/Performance/Conceptual/EnergyGuide-iOS/LocationBestPractices.html, 2018. Online, letzter Zugriff: 01.05.2018.

[Ass12] Camera & Imaging Products Association. Exchangeable image file format for digital still cameras: Exif Version 2.3. http://www.cipa.jp/std/documents/e/DC-008-2012_E.pdf, 2012. Online, letzter Zugriff: 14.04.2017.

[Bal13] Paul Balzer. Aktivitätenerkennung – Apple iPhone 5s mit M7 Motionprozessor. http://mechlab-engineering.de/2013/10/aktivitaetenerkennung-apple-iphone-5s-mit-m7-motionprozessor/, Oktober 2013. Online, letzter Zugriff: 27.07.2016.

[bau17] bobzilla, arkasha, and uhtu. WIGLE: Wireless Network Mapping. https://www.wigle.net/map, Januar 2017. Online, letzter Zugriff: 21.01.2017.

[Bri08] R. Brinkmann. Wahrscheinlichkeiten von Umgebungen. http://www.brinkmann-du.de/mathe/gost/stoch_01_13.htm, 2008. Online, letzter Zugriff: 14.04.2017.

[Bri10] Volker Briegleb. Datenschützer: Street-View-Autos scannen private Funknetze. *heise.de*, April 2010. Online, letzter Zugriff: 01.08.2016. URL: http://www.heise.de/newsticker/meldung/Datenschuetzer-Street-View-Autos-scannen-private-Funknetze-Update-984118.html.

[Cel17] Cellebrite. Mobile Forensics Solution Brochure. http://www.cellebrite.com/Media/Default/Files/Forensics/Solution-Briefs/Mobile-Forensics-Solution-Brief.pdf, 2017. Online, letzter Zugriff: 04.02.2017.

[Coo16] Pricewaterhouse Coopers. The Wearable Life 2.0 - Connected living in a wearable world. http://www.pwc.com/us/en/industry/entertainment-media/assets/pwc-cis-wearables.pdf, 2016. Online, letzter Zugriff: 26.02.2017.

[Cou10] Paul Courbis. Localisation iPhone : votre téléphone est indiscret. http://www.courbis.fr/Localisation-iPhone-votre.html, September 2010. Online, letzter Zugriff: 18.12.2016.

[Cun17] Cunstuck. LocationFaker(8,9,10). http://apt.thebigboss.org/onepackage.php?bundleid=org.thebigboss.locationfaker8, Februar 2017. Online, letzter Zugriff: 26.01.2017.

[Dhe12] Andreas Dhein. Analyse und Interpretation von Geolokalisationsdaten in modernen Smartphones. https://www.sit.fraunhofer.de/fileadmin/dokumente/Anwendertag_IT-Forensik/2012/Vortrag_Dhein.pdf?_=1463500589, 2012. Online, letzter Zugriff: 02.01.2017.

[Dhe14] Andreas Dhein. ssh Zugang zum iPhone über USB (ohne WiFi). *dhein-pc.de*, 2014. Online, letzter Zugriff: 12.03.2017. URL: http://www.dhein-pc.de/wie-erhalte-ich-einen-ssh-zugang-zum-iphone-ueber-usb-ohne-wifi/.

[Ena16] Enaikoon. OpenCellID. http://wwww.opencellid.org, 2016. Online, letzter Zugriff: 21.01.2017.

[Eri11a] Magnus Eriksson. android-locdump README. https://github.com/packetlss/android-locdump, 2011. Online, letzter Zugriff: 01.08.2016.

[Eri11b] Magnus Eriksson. android-locdump/parse.py. https://github.com/packetlss/android-locdump/blob/master/parse.py, 2011. Online, letzter Zugriff: 13.07.2016.

[Fig11] Hubert Figuière. github-hfiguiere/exifprobe. https://github.com/hfiguiere/exifprobe, Oktober 2011. Online, letzter Zugriff: 30.12.2016.

[For16] Oxygen Forensics. Oxygen Forensic Detective - Geo Locations. https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective/analyst/web-connnections-locations, 2016. Online, letzter Zugriff: 15.01.2017.

[gal15] galloglass. Python Skript zum Parsen der iTunes Manifest.mbdb Datei. http://stackoverflow.com/questions/3085153/how-to-parse-the-manifest-mbdb-file-in-an-ios-4-0-itunes-backup, August 2015. Online, letzter Zugriff: 26.07.2016.

[Ges11] Alexander Geschonneck. iPhone Forensics Tools und Quizfrage!, 2011. Online, letzter Zugriff: 12.07.2016. URL: https://www.computer-forensik.org/blog/2011/05/30/iphone-forensics-tools-und-quizfrage/.

[Goo16a] Google. Android Debug Bridge. https://developer.android.com/studio/command-line/adb.html, 2016. Online, letzter Zugriff: 01.08.2016.

[Goo16b] Google. Google Developers - Location Strategies. https://developer.android.com/guide/topics/location/strategies.html, 2016. Online, letzter Zugriff: 04.09.2016.

[Goo16c] Google. Google Now - Die richtigen Informationen zur richtigen Zeit. https://www.google.com/intl/de/landing/now, 2016. Online, letzter Zugriff: 28.07.2016.

[Goo16d] Google. Standortbericht unter Android 2.3 und niedriger. https://support.google.com/accounts/answer/6179389, 2016. Online, letzter Zugriff: 28.07.2016.

[Goo16e] Google. Standortverlauf für iPhone & iPad. https://support.google.com/accounts/answer/4388034, 2016. Online, letzter Zugriff: 28.07.2016.

[Goo16f] Google. Standortverlauf verwalten. https://support.google.com/accounts/answer/3118687, 2016. Online, letzter Zugriff: 28.07.2016.

[Goo16g] Google. The Google Maps Geolocation API. https://developers.google.com/maps/documentation/geolocation/intro, 2016. Online, letzter Zugriff: 02.08.2016.

[Goo17a] Google. Datenschutzerklärung von Google. https://www.google.com/policies/privacy/, 2017. Online, letzter Zugriff: 05.03.2017.

[Goo17b] Google. Google Android - Manifest.permission. https://developer.android.com/reference/android/Manifest.permission.html#ACCESS_COARSE_LOCATION, 2017. Online, letzter Zugriff: 25.02.2017.

[Goo17c] Google. Google APIs for Android - LocationRequest. https://developers.google.com/android/reference/com/google/android/gms/location/LocationRequest, 2017. Online, letzter Zugriff: 25.02.2017.

[Goo17d] Google. Google Developers: android.location. https://developer.android.com/reference/android/location/package-summary.html, 2017. Online, letzter Zugriff: 16.11.2017.

[Goo18a] Google. Best Practices Using Google Maps APIs Web Services. https://developers.google.com/maps/documentation/geolocation/web-service-best-practices, 2018. Online, letzter Zugriff: 01.05.2018.

[Goo18b] Google. Get a Key/Authentication. https://developers.google.com/maps/documentation/javascript/get-api-key?hl=de, 2018. Online, letzter Zugriff: 05.01.2018.

[Goo18c] Google. Migrate to location and context APIs. https://developer.android.com/guide/topics/location/migration, 2018. Online, letzter Zugriff: 01.05.2018.

[Goo18d] Google. Wie Google den letzten Standort Ihres Geräts ermittelt. https://support.google.com/accounts/answer/6076654, 2018. Online, letzter Zugriff: 26.04.2018.

[Gor11] Adam Gorski. Understanding GPS performance in urban environments. http://blogs.agi.com/agi/2011/01/04/understanding-gps-performance-in-urban-environments, Januar 2011. Online, letzter Zugriff: 30.12.2016.

[Gri13] Rüdiger Grimm. Sicherheit und Zuverlässigkeit für mobile Anwendungen. https://www.uni-koblenz-landau.de/de/koblenz/fb4/iwvi/aggrimm/lehre-en/archiv/sose13/sicherheitmobianwendungen, 2013. Online, letzter Zugriff: 15.03.2017.

[Gri15] Rüdiger Grimm. Mobile System Security (Sicherheit für mobile Systeme). https://www.uni-koblenz-landau.de/de/koblenz/fb4/iwvi/aggrimm/lehre-en/sose15/mobsec, 2015. Online, letzter Zugriff: 15.03.2017.

[Gro09] CDMA Development Group. Open Market Handsets (OMH) R-UIM Specification - CDG Document 166. `http://www.cdg.org/members_only/refdocs/166.zip`, 2009. Online, letzter Zugriff: 27.07.2016.

[Gö09] Joachim Göller. Über Signalisierung im UMTS, ein Lehrbrief. `http://www2.informatik.hu-berlin.de/~goeller/isdn/UeberSignalisationImUMTS.pdf`, 2009. Online, letzter Zugriff: 27.07.2016.

[Inc17] IncorporateApps. Fake GPS Location Spoofer Free. `https://play.google.com/store/apps/details?id=com.incorporateapps.fakegps.fre`, August 2017. Online, letzter Zugriff: 08.08.2017.

[iPh13] iPhoneFAQ. Does the iPhone 4S support 4G / LTE? `http://www.iphonefaq.org/archives/971577`, 2013. Online, letzter Zugriff: 27.07.2016.

[iW16] The iPhone Wiki. iTunes Backup. `https://www.theiphonewiki.com/wiki/ITunes_Backup`, September 2016. Online, letzter Zugriff: 09.01.2018.

[iW17] The iPhone Wiki. UDID. `https://www.theiphonewiki.com/wiki/UDID`, März 2017. Online, letzter Zugriff: 09.01.2018.

[Koma] Elektronik Kompendium. Grundlagen Mobilfunk. `https://www.elektronik-kompendium.de/sites/kom/0406221.htm`. Online, letzter Zugriff: 30.11.2017.

[Komb] Elektronik Kompendium. Wlan-beacons. `https://www.elektronik-kompendium.de/sites/net/2010231.htm`. Online, letzter Zugriff: 30.11.2017.

[laz18] lazierthanthou. SQLite Manager Plugin für Mozilla Firefox. `https://addons.mozilla.org/de/firefox/addon/sqlite-manager/`, 2018. Online, letzter Zugriff: 04.04.2018.

[Mic17] Microsoft. Datenschutz bei Microsoft. https://privacy.microsoft.com/de-de/, 2017. Online, letzter Zugriff: 05.03.2017.

[(ms14] Markus (msemm). CDMA. http://wiki.opencellid.org/wiki/Public:CDMA, 2014. Online, letzter Zugriff: 27.07.2016.

[Myl17] Alexander Mylnikov. Find WiFi - Mylnikov GEO. http://find-wifi.mylnikov.org, Januar 2017. Online, letzter Zugriff: 21.01.2017.

[na12] na. TD-SCDMA vs WCDMA vs CDMA2000. http://www.rfwireless-world.com/Terminology/difference-between-TD-SCDMA-WCDMA-CDMA2000.html, 2012. Online, letzter Zugriff: 27.07.2016.

[na13] na. Wir räumen gängige Akku-und Strom-Mythen auf! https://www.android-user.de/wir-raeumen-gaengige-akku-und-strom-mythen-auf/, August 2013. Online, letzter Zugriff: 28.01.2018.

[nay14] nayarasi. 802.11 Mgmt : Beacon Frame. https://mrncciew.com/2014/10/08/802-11-mgmt-beacon-frame/, Oktober 2014. Online, letzter Zugriff: 30.12.2016.

[Now17] NowSecure. Andrew Hoog Biography. https://www.nowsecure.com/team/andrew-hoog/, Januar 2017. Online, letzter Zugriff: 02.01.2017.

[Pad16] Padraig. SuperCrazyAwesome: iPhoneBackupExtractor. http://supercrazyawesome.com/downloads/iPhoneBackupExtractor.app.zip, 2016. Online, letzter Zugriff: 25.07.2016.

[Pat15] Pranay Patel. Stack Overflow: Android LocationManager vs Google Play Services. https://stackoverflow.com/questions/33022662/

android-locationmanager-vs-google-play-services, 2015. Online, letzter Zugriff: 05.01.2018.

[Rev12] Reverb. Multi-Radio Access Technology (RAT) Self-Optimizing Networks, 2012. Online, letzter Zugriff: 27.07.2016. URL: http://www.reverbnetworks.com/wp-content/uploads/2014/06/Reverb_wp_MultiRAT-SON_Aug12rs.pdf.

[rGPPG04] 3rd Generation Partnership Project 2 3GPP2. Interoperability Specification for cdma2000 Air Interface. http://www.3gpp2.org/public_html/specs/C.S0044-0_v1.0_040929.pdf, 2004. Online, letzter Zugriff: 27.07.2016.

[Ric16] Felix Richter. Auf dem Weg in die Post-PC-ära. https://de.statista.com/infografik/275/absatz-von-pcs-smartphones-und-tablets-bis-2016/, 2016. Online, letzter Zugriff: 11.07.2016.

[(sa16] Jay Freeman (saurik). Cydia: an alternative AppStore. https://cydia.saurik.com/, 2016. Online, letzter Zugriff: 25.07.2016.

[SB14] Hendrik Schmidt and Brian Butterly. LTE vs. Darwin. http://2014.hackitoergosum.org/slides/day1_ERNW_LTEvsDarwin_HES.pdf, 2014. Online, letzter Zugriff: 27.07.2016.

[Sch11] Christian Scharten. Android Location Cache Viewer: auf dem Handy gespeicherte Standortdaten einsehen. *cnet*, 2011. Online, letzter Zugriff: 04.01.2018. URL: http://www.cnet.de/41552226/android-location-cache-viewer-auf-dem-handy-gespeicherte-standortdaten-einsehen/.

[Sta17] Statista. Anteile der Betriebssysteme an der mobilen Internetnutzung in Deutschland bis 2017. https://de.statista.com/statistik/daten/studie/184332/umfrage/marktanteil-der-mobilen-

betriebssysteme-in-deutschland-seit-2009/, 2017. Online, letzter Zugriff: 23.09.2017.

[Suh06] Sven-Olaf Suhl. China ernennt TD-SCDMA zum 3G-Mobilfunkstandard. *heise.de*, 2006. Online, letzter Zugriff: 27.07.2016. URL: http://www.heise.de/newsticker/meldung/China-ernennt-TD-SCDMA-zum-3G-Mobilfunkstandard-167873.html.

[Tar12] Andrew Tarantola. The XRY Cracking Tool Is Unimpressed With Your iPhone's Defenses. *gizmodo*, 2012. Online, letzter Zugriff: 14.06.2017. URL: https://www.gizmodo.com.au/2012/03/the-xry-cracking-tool-is-unimpressed-with-your-iphones-defenses/.

[War11] Pete Warden. iPhone Tracker. http://petewarden.github.io/iPhoneTracker/, 2011. Online, letzter Zugriff: 08.08.2017.

[wtwts17] RSA Conference where the world talks security. Andrew's session at RSA. https://www.rsaconference.com/speakers/andrew-hoog, Januar 2017. Online, letzter Zugriff: 02.01.2017.

Abbildungsverzeichnis

1.1 Vergleich verschiedener Methoden bei der Smartphoneverortung . 5
1.2 Verortung eines Smartphones auf Basis von Mobilfunksendern . . 10
1.3 Anzeige von Standortdaten im iPhoneTracker (Warden) 12
1.4 Anzeige von Standortdaten im iPhoneTrackerLE (Dhein) 15
1.5 Statistik zur Smartphonenutzung in Deutschland 16
1.6 Statistik zur Martverteilung stationärer-/mobiler Systeme weltweit 16
1.7 Statistik zur Marktverteilung mobiler Betriebssysteme weltweit . . 17
1.8 Zugriffsmöglichkeiten auf gesperrte Apple Geräte 19
1.9 Datenumfang verschiedener Methoden zur iOS Datenextraktion . . 21
1.10 Fehlerhafte Standortdaten in Metadaten von Bildern 23
1.11 Fehlerhaft verortete WLAN-AccessPoints 24
1.12 Untersuchung von LocationFaker unter iOS 26
1.13 Untersuchung von LocationFaker unter Android 27
1.14 Ausgabe von Standortdaten in forensischen Berichten 28

2.1 Anzeige von Standortabweichungen in ADEL 39
2.2 iPhoneTracker: Enormer Datenumfang unter iOS 4.3.2. 41
2.3 iPhoneTracker: Fehlerhafte Darstellung von Geokoordinaten 42
2.4 MyPhoneTracker: Korrekte Darstellung von Standortdaten 43

2.5 Oxygen Forensic Detective: Darstellung von Ortungsdaten 44
2.6 Oxygen Forensic Detective: Berichtsexport zu Standortdaten 45
2.7 MSAB XRY: Ortungsdaten in Bilddateien 46
2.8 MSAB XRY: Hardware-Kit zur Datensicherung 46
2.9 Cellebrite UFED-touch: Lieferumfang und Auslesen eines iPhones 47
2.10 Cellebrite PA v.4.2.1.7: Ortungsdaten aus Metadaten 48
2.11 Problem 1 bei Cellebrite: Mögliche Abweichung von Ortungsdaten 49
2.12 Cellebrite PA v.5.4.7.5: Ortungsdaten unter guten Bedingungen . . 50
2.13 Problem 2 bei Cellebrite: Standortdaten von Drittanbietern 50
2.14 OpenCellID: Crowd-Sourced Funkzellenvermessung 51
2.15 wigle.net&mylnikov: WLAN-Verortung im Internet 52

3.1 Design Science Research Methode: Prozessüberblick 55
3.2 Design Science Research Methode: Detaillierter Prozessablauf . . . 57
3.3 Korrelation von Messdaten mit Standorten aus Apples Ortungs-DB 62

4.1 Datenextraktion bei Apple 1: iTunes-Synchronisierung verhindern 67
4.2 Datenextraktion bei Apple 2: Gerätesicherung durchführen 68
4.3 Datenextraktion bei Apple 3: Sicherungsdaten ermitteln 69
4.4 Datenextraktion bei Apple 4: Ortungsdatenbank finden 69
4.5 Installation von OpenSSH über alternativen AppStore cydia 70
4.6 Forensic Focus: CellLocation- und WiFiLocationtabelle 76
4.7 Kartendarstellung von Geokoordinaten mithilfe von GoogleMaps . 79
4.8 Erfahrungen und Probleme i.Z.m. Apples Ortungsdaten 82
4.9 Kartendarstellung und Tabellenwerte: LocationHarvest 89
4.10 Kartendarstellung und Tabellenwerte: CellLocationHarvest 93
4.11 Kartendarstellung und Tabellenwerte: WiFiLocationHarvest 95

4.12 BytestreamAnalyzerLE: Analyse von Ortungsdaten aus Android 2.3 114
4.13 AndroidTrackerLE: Beispiel einer korrekten Verortung 115
4.14 AndroidTrackerLE: Beispiel einer fehlerhaften Verortung 116
4.15 Reverse-Geocoding mithilfe von Google Maps 119
4.16 Google ermittelt Ortsinformationen aus IP Adressen 121
4.17 Google Now Screenshots unter iOS und Android 124
4.18 Google Location History: Status und Datenumfang 125
4.19 Google Location History: Rohdaten zeigen mögliche Abweichungen 126
4.20 AndroidTrackerLE: Darstellung des Standortverlaufs von Google . 128

5.1 iOSTracker: Kartenansicht zur Verortung 132
5.2 iOSTracker: Detailangaben zur aktuellen Position 132
5.3 iOSTracker: Ansicht der Einträge in der Ortungsdatenbank 133
5.4 iOSTracker: Betrachten der gespeicherten Positionsdaten 133
5.5 WatchTracker: Ortungsverlauf in der Kartenansicht 134
5.6 WatchTracker: Aufgezeichnete Ortungsdaten 134
5.7 DroidTracker: Positionsschätzung in der Kartenansicht 135
5.8 DroidTracker: Detailinformationen zur Verortung 135
5.9 iPhoneTrackerLE: rKorrelation mit Daten aus dem iOSTracker . . . 139
5.10 iOSTracker: Filterung von Funksendern zur Positionsbestimmung . 141
5.11 WatchTracker: Darstellung der Lokalisierung über die Zeit 142
5.12 DroidTracker: Verfeinerte Lokalisierung über die Zeit 142
5.13 Schematische Darstellung der Geolokalisierung bei Apple 143
5.14 Schematische Darstellung der Geolokalisierung bei Google 144
5.15 Schwarmkartierung bei Apple im Überblick 145
5.16 Schwarmkartierung: Konsolidierung verschiedener Messpunkte . . 146
5.17 Screenshot iOSTracker: Fehlerhafte Verortung von Funksendern . . 147

6.1 Ausblick: Sigma-Umgebung zur Maximierung der confidence . . . 162

6.2 Patentskizze der Apple Watch Diagnoseschnittstelle 163

Tabellenverzeichnis

1.1 Vergleich von Extraktionsmethoden in der Mobilfunkforensik . . . 18

2.1 Stärken und Schwächen von Tools zur Darstellung von Geodaten aus mobilen Endgeräten 53

4.1 Spaltenübersicht der Tabelle CellLocation unter iOS 4.3.2 72
4.2 Veränderungen der Ortungsdatenbank neuerer iOS-Versionen . . . 73
4.3 Übersicht aller Tabellen der Ortungsdatenbanken von iOS4 - iOS10 74
4.4 Speicherumfang verschiedener Harvesting-Tabellen in iOS 88
4.5 Speicherumfang verschiedener Ortungsdatenbanken 88
4.6 Speicherumfang der Ortungsdatenbanken unter iOS9 105

5.1 Genauigkeit verschiedener Funksender 144

6.1 Integrität unterschiedlicher Artefakte in der Mobilfunkforensik . . 153

Terminalausgaben

4.1 Tabellenübersicht einer iOS 4.3.2 Ortungsdatenbank anzeigen . . . 71
4.2 Tabellenauflistung der Datenbank cache_encryptedB.db (iOS9) . . 102
4.3 Tabellenauflistung der Datenbank lockCache_encryptedA.db (iOS9) 104
4.4 Tabellenauflistung der Datenbank cache_encryptedB.db (iOS10) . . 106
4.5 adb-Kommando zur logischen Extraktion von Android-Daten . . . 111
4.6 Exemplarische Ausgabe des locdump-parser Skriptes von Magnus Eriksson 112
4.7 Ergebnis der WHOIS-Abfrage zur IP 141.26.185.153 121
4.8 Auszug aus der Datei Standortverlauf.json 127

Abkürzungsverzeichnis

ADB Android Debugging Bridge. 110

aGPS assisted Global Positioning System. 4–6, 8–10, 13, 23, 32, 33, 49, 87, 130, 135, 144, 147, 148, 158, 163

API Application Programming Interface. 57, 122, 123, 135, 137, 158, 164

DSRM Design Science Research Methode. 55–57, 59, 61

Exif Exchangeable Image File Format. 3, 4, 23, 46, 58, 150, 164

GPS Global Positioning System. 5–8, 10, 15, 32, 33, 37, 39, 49, 54, 97, 128, 130, 137, 143–145, 148, 154–157, 160, 163, 164

MAC Media-Access-Control. 9, 25, 51, 77, 81, 86, 87, 95, 101, 111, 146, 165, 190

MESZ Mitteleuropäische Sommerzeit. 112

NFC Near Field Communication, deu: Nahbereichskommunikation. 10, 33, 160

PC Personal Computer. 17, 45, 88

URL Uniform Resource Locator. 78, 79, 119

USB Universal Serial Bus. 19, 70, 110

UTI Uniform Type Identifier. 91

WLAN Wireless Local Area Network. 7–10, 14, 24, 25, 32, 33, 44, 48, 50–52, 70, 72, 73, 75–79, 81, 86, 88, 95, 96, 100–103, 105, 107, 115–117, 120, 131, 137, 139, 141, 144, 147, 151, 152, 154–157, 163, 183, 184, 193

Begriffserläuterungen

Accuracy Genauigkeit, besser: maximale Fehlertoleranz; ist als Radius in Metern zu verstehen, innerhalb dessen sich das Smartphone zum Zeitpunkt der Verortung befunden hat. 77, 78, 81, 86, 87, 89, 90, 94, 95, 133, 136, 145, 154–156, 158, 159, 161, 190

Altitude Höhe in Metern über NN. 77, 90, 94, 96, 103

ARFCN Absolute Radio Frequency Channel Number, dient zur Berechnung der Up- und Downlinkfrequenzen eines Kanalpaars. 80, 94, 193

BANDCLASS Bandwidth Class, gibt die Bandbreite einer Klasse im CDMA Mobilfunkstandard an. 83, 84

Beacon Beacons bezeichnen sowohl Managementinformationen im WLAN-Standard als auch Drahtlossender im NFC-Umfeld. 9

BSSID Basic Service Set Identifier, entspricht i.d.R. der MAC-Adresse. 9, 83, 84

BundleId kanonischer Projektname, d.h. eindeutige Bezeichnung einer nativen iOS App. 90–93, 95, 99–101

CDMA Code Division Multiple Access, Mobilfunkstandard der dritten Generation (3G), vgl. UMTS. 83, 84, 91, 99, 190–193

CellID eindeutige Funkzellenkennung. 9, 80, 87, 190

CFAbsolute-Time Apple-spezifisches Zeitformat; rechnet in Sekunden seit dem 01.01.2001 00:00:00h. 77, 78, 89, 93, 95, 103

CI Abkürzung für Cell Identifier, siehe CellID. 77, 80, 84, 93, 112

Cloud Synonym für beim Anbieter gespeicherte Daten im Internet. 17, 149, 162

Confidence Verlässlichkeitsangabe, abhängig von der Empfängerquelle; verhält sich antiproportional zur Accuracy Angabe. 77, 78, 90, 92, 94, 96, 101, 156

Course Kursangabe in mathematischer Richtung von 0=Nord über 90=Ost, 180=Süd bis 270=West. 77, 90, 94, 96

Cydia Alternativer Appstore zur Installation und Nutzung von Drittanbietersoftware. Häufig einhergehend mit der Verbreitung von Applikationen, die gegen Apples restriktive Softwareprüfung verstoßen. 25

dB dB (Dezibel) ist die Einheit des Leistungspegels LP, der das Verhältnis einer Leistung P im Vergleich zu einer Bezugsleistung P0 beschreibt: $L_P = 10lg(P/P_0)dB$. 93, 95, 101, 192

DV Datenverarbeitung, historisch geprägter Begriff bei der Polizei. Steht u.a. für die IT-Forensik. 40

ECNo Received Energy per Chip divided by total Noise power density, entspricht der RSCP - RSSI im WCDMA Mobilfunkstandard. 94

ID eindeutiger Bezeichner, Identifikator. 8, 51

IP Internet Protocol, hier allerdings in Form der IP-Adresse (z.B. 84.2.44.2) gemeint. 165, 193

Jailbreak Technik um durch Ausnutzen von Exploits Software vorbei am Apple AppStore zu installieren. Geht für gewöhnlich mit einer Rechteeskalation einher. 21, 37, 70, 73, 131, 133, 134

KML Keyhole Markup Language, ist eine Auszeichnungssprache zur Beschreibung von Geodaten, basierend auf XML. 127

LAC Location Area Code, eine 2 Byte große Kennung, deutsch Aufenthaltsbereichskennzahl im Mobilfunk. 77, 80, 83, 84, 87, 93, 112

Latitude Geografische Breite; der Wertebereich im Dezimalformat liegt zwischen 0 Grad=Äquator und $\pm$90 Grad an den Polen. 77, 89, 93, 95

Longitude Geografische Länge; ger Wertebereich im Dezimalformat liegt zwischen 0 Grad=Greenwich und $\pm$180 Grad Richtung Westen oder Osten. 77, 89, 93, 95

LTE Long Term Evolution, Mobilfunkstandard der vierten Generation (4G); ermöglicht Übertragungsraten bis zu 300mbit/s. 80, 82, 83, 85, 91, 94

MCC Mobile Country Code, 3-stellige eindeutige Landeskennung im Mobilfunk. 77, 80, 83, 84, 87, 90, 93, 112

MNC Mobile Network Code, i.d.R. 2-stellige Netzwerkcode im Mobilfunk für die Zuordnung zum Anbieter. 77, 80, 84, 87, 90, 93, 112

NAND-dump Bei der Datenextraktion mittels NAND-dump werden die Dateninhalte der auf in Smartphones häufig anzutreffenden NAND-Technik basierenden Speicherchips bitweise als 1:1 Abbild extrahiert. 21

NID Network Identifier, dient der Identifikation des Netzes im CDMA Mobilfunkstandard. 83

OpenSSH Opensourceimplementierung des SSH Protokolls. 70

Operator hier: Mobilfunkanbieter. 93

Paging Paging im Kontext zum Mobilfunk bezeichnet einen Rundruf an alle verfügbaren Teilnehmer innerhalb der Sendereichweite der Basisstation. 9

PID Physical (cell) IDentification, dient der Identifikation des physischen Funksenders. 83, 98

PNOFFSET Pseudo Noise Offest, gibt den zufälligen Rauschabstand im CDMA Mobilfunkstandard an. 84

PSC Primary Synchronisation Code, dient der Synchronisierung von Zeitslots im Mobilfunk, gleich für die gesamte Zelle. 77, 80, 83, 84, 94

RAT Radio Access Type, deu: Mobilfunk Zugangsmethode. 90, 91, 94

reverse-geocoding Unter reverse-geocoding versteht man die Überführung von Adressdaten in Geokoordinaten. 165

RLP Rheinland-Pfalz. 40

RSCP Received Signal Code Power, gemessene Leistung in dB eines Empfängers auf einem bestimmten physikalischen Kommunikationskanal im WCDMA Mobilfunkstandard. 94, 98, 191

RSSI Received Signal Strength Indication, Feldstärke in dB pro Milliwatt (dBm). 87, 93–95, 101, 191

SCRUM Agile Softwareentwicklungsmethode. Inkrementell getrieben wird Software in kurzen, sog. Sprints mit dem Ziel entwickelt, dem Kunden nach jedem Inkrement ein minimal lebendes Produkt demonstrieren zu können. 57

Seitenkanäle Unter Seitenkanälen sind in der IT-Forensik Artefakte zu verstehen, die nicht unmittelbar zu dem Zweck der Informationsgewinnung entstanden sind. Als Beispiel bringen Standortdaten in Bilddateien keinen Vorteil für die Bilddarstellung. 38

SHA1 Secure Hash Algorithm 1, dient zur Berechnung eines eindeutigen Prüfwerts für beliebige elektronische Daten. 68, 69, 193

SIM Subscriber Identity Module; Chipkarte für Mobiltelefone. 37, 45

Speed Geschwindigkeit in Metern pro Sekunde. 77, 90, 94, 96

SQLite3 Ein dateibasiertes Datenbanksystem; sehr populär auf Geräten mit geringer Rechenleistung, da kein eigenständiger Datenbankserver benötigt wird. 60, 66, 68, 71, 108, 152

SSH Secure SHell bezeichnet sowohl ein Netzwerkprotokoll als auch entsprechende Programme, mit deren Hilfe man auf sichere Art und Weise eine Verbindung zu einem Gerät im Netzwerk herstellen kann. 21, 70, 73, 191

SSID Service Set Identifier, entspricht i.d.R. dem Namen des WLAN Netzwerkes. 9, 24, 25

TAC Tracking Area Code, dient der Zuordnung von Funkzellen im Mobilfunk zu einem Areal. 83

Timestamp Zeitstempel, speziell im Zusammenhang mit Ortungsdaten in Smartphones wird hierbei der Zeitpunkt des Empfangs bzw. der Speicherung in der Datenbank bezeichnet. 77, 78, 89, 93, 95, 98

UARFCN UTRA Absolute Radio Frequency Channel Number, Variante der ARFCN im UMTS Mobilfunknetz. 77, 80, 84, 98

UDID steht als Abkürzung für Unique Device Identifier. 40-Zeichen langer SHA1-Wert aus UDID = SHA1(serial + [ECID | IMEI] + wifiMac + bluetoothMac). 68

UMTS Universal Mobile Telecommunications System ist ein Mobilfunkstandard der dritten Generation (3G) und ermöglicht Übertragungsraten bis zu 42mbit/s. 80, 91, 94, 99, 190

WAL Mittels write ahead logs soll die Atomarität und Beständigkeit von Datenbankeinträgen gewährleistet werden. Hierzu werden die Daten vor dem eigentlichen Eintragen in die Datenbank vorab gespeichert und anschließend kontrolliert überführt. 152

wear-leveling Verfahren zur Optimierung der Speicherung von Daten auf flash-Speichern. Aufgrund der beschränkten Lebensdauer der Speicherzellen von flash-Bausteien werden Daten blockweise und möglichst gleichmäßig über alle Zellen verteilt, gespeichert. 21

WHOIS Eine WHOIS Abfrage ermittelt zu einer IP-Adresse weitergehende Detailinformationen zum verantwortlichen Betreiber des Systems. 121

YAFFS YAFFS steht für Yet Another Flash File System. Fand bei älteren Android-Versionen oftmals Verwendung. 21

ZONEID Zone Identification, dient der Identifikation einer Zone im CDMA Mobilfunkstandard. 83, 84